Cisco CDA Visual Quality Experience Application User Guide, Release 3.2

January, 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-14115-05

Cisco CDA Visual Quality Experience Application User Guide, Release 3.2

CONTENTS

Preface

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services. This preface contains the following sections:

Objectives

This document describes Cisco CDA Visual Quality Experience Application (VQE), Release 3.2, and explains how to set up and use the VQE software.

Document Revision History

Table 1 records technical changes to this document. The table shows the document revision number for the change, the date of the change, and a brief summary of the change.

Table 1 Document Revision History

Revision	Date	Change Summary
OL-14115-05	January, 2009	Document for VQE Release 3.2
OL-14115-04	October, 2008	Document for VQE Release 3.1
OL-14115-03	August, 2008	Document for VQE Release 3.0
OL-14115-02	December, 2007	Document for VQE Release 2.1
OL-14115-01	August, 2007	Document for VQE Release 2.0

For information on the content and enhancements of each VQE release, see the relevant VQE release notes.

Document Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Introduction to Cisco CDA Visual Quality Experience Application	Provides an introduction to Cisco CDA Visual Quality Experience (VQE) Application.
Chapter 2	Getting Started with the VQE Startup Configuration Utility	Explains how to use the Cisco VQE Startup Configuration Utility to perform the initial configuration tasks for the Cisco CDE110 that hosts VQE-S and the CDE110 that hosts VQE Tools.
Chapter 3	Using the VQE Channel Provisioning Tool	Describes how to use Cisco VQE Channel Provisioning Tool (VCPT).
Chapter 4	Using the VQE-S Application Monitoring Tool	Describes how to use Cisco VQE-S Application Monitoring Tool (VQE-S AMT or AMT)
Chapter 5	Troubleshooting VQE Software Components	Describes how to identify and remedy problems related to Cisco VQE Server, VQE-S Application Monitoring Tool, and VQE Channel Provisioning Tool. The chapter also explains how to stop, start, and restart the VQE-S and VQE Client Channel Configuration Delivery Server (VCDS) services.
Chapter 6	Configuring VQE Server and VQE Tools	Describes these VQE Configuration Management System software components: VQE Configuration Tool, Configuration Engine, and the VCDB Parser. The chapter also provides information on using Configuration Tool, manually editing the VCDB file, and using **vqe_cfgtool** command.
Appendix A	VQE, System, and Network Parameters	Provides descriptions of the VQE-S Configuration Database (VCDB) parameters.
Appendix B	Using Net-SNMP	Gives information about using Net-SNMP on the Cisco CDE110 that hosts VQE-S and on the CDE110 that hosts VQE Tools.
Appendix C	VQE System Messages	Provides information on the Cisco VQE system messages.
Appendix D	Manual Initial VQE System Configuration	Explains how to perform manual initial configuration on the CDE110 that hosts VQE-S and on the CDE110 that hosts VQE Tools.
Appendix E	Configuring DHCP and DNS Servers for VCDS	Provides information on configuring the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers so that they work correctly with VCDS or another RTSP server.
Appendix F	Changing the Boot Sequence to Start from the CD/DVD Drive	Explains how to change the BIOS setting on the Cisco CDE110 server so that the server boots first from the CD/DVD Combo drive.

Related Documentation

The following is a list of documents and URLs for the Cisco CDE110 and the Cisco CDA Visual Quality Experience Application, Release 3.2:

- *Release Notes for Cisco CDA Visual Quality Experience Application, Release 3.2*
  http://www.cisco.com/en/US/docs/video/cds/cda/vqe/3_2/release/notes/vqe_notes3_2.html
- *Cisco CDA Visual Quality Experience Application User Guide, Release 3.2* (this document)
  http://www.cisco.com/en/US/docs/video/cds/cda/vqe/3_2/user/guide/vqe_guide3_2.html
- *Cisco Content Delivery Engine 110 Hardware Installation Guide*
  http://www.cisco.com/en/US/docs/video/cds/cde/cde110/installation/guide/cde110_install.html
- *Regulatory Compliance and Safety Information for the Cisco Content Delivery Engine 110*
  http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/cde110_rcsi.pdf

The VQE Client (VQE-C) documentation is included in the VQE-C software TAR file. If you are a registered Cisco.com user, the file can be downloaded from the following location:

http://www.cisco.com/kobayashi/sw-center/content-delivery/cda.shtml

Table 2 lists the VQE Client documentation that is provided.

Table 2 VQE Client Documentation

VQE-C Document	Description
VQE-C Release Notes	Provides release-specific information on VQE-C.
VQE-C System Integration Reference	Provides information on VQE-C components, architecture, integration, and APIs. Also includes a VQE-C quick-start guide.
VQE-C System Configuration Guide	Explains certain factors to consider when configuring and deploying VQE-C. Also provides reference information on the VQE-C configuration file parameters.
VQE-C CLI Command Reference	Provides reference information on the VQE-C command-line interface.

Conventions

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

Table 3 Command Syntax and Emphasis Conventions

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{*x* | *y* | *z*}	Alternative, mutually exclusive, keywords are grouped in braces and separated by vertical bars.

Table 3 Command Syntax and Emphasis Conventions (continued)

Convention	Description
[*x* | *y* | *z*]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Arguments for which you supply values are in *`italic screen`* font.
^	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.
< >	Nonprinting characters, such as passwords, are in angle brackets in contexts where italics are not available.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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.

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Introduction to Cisco CDA Visual Quality Experience Application

This chapter provides information on Cisco CDA Visual Quality Experience Application (VQE), Release 3.2, and contains the following major topics:

VQE Overview

This VQE overview has the following sections:

Introduction to VQE

Cisco CDA Visual Quality Experience Application (VQE) offers service providers a set of technologies and products associated with the delivery of IPTV video services. VQE is designed to improve the quality of IPTV services and subscribers' viewing experiences. VQE is part of a Cisco end-to-end solution that builds video awareness into the network infrastructure. For Cisco VQE, Release 3.2, VQE technology is intended for wireline operators who offer managed broadcast (multicast) IPTV services using xDSL.

IPTV subscribers expect high video quality. Because many subscribers are migrating from existing analog or digital cable services, their quality expectation has already been set. To attract subscribers, IPTV providers must meet or exceed the video experience of existing services. VQE technology and products provide that capability.

Video is less tolerant of network factors such as jitter, delay, and especially packet loss because a single IP packet carries up to seven MPEG transport frames. Therefore, IP networks require additional functionality to deliver the video quality expected by subscribers. The accepted industry benchmark for quality is to deliver a maximum of one video "artifact" or perceived distortion during the viewing of a one-hour movie. This level of quality translates into a network-layer requirement of less than 7.8E-7 video packets loss. Most xDSL networks are not optimized to deliver such low levels of packet loss.

A second issue that affects IPTV video quality is channel change time (CCT). Consumers have become used to the current CCT—which is less than two seconds—offered by digital cable and digital satellite services. A number of factors can contribute to longer IPTV channel change times, including Internet Group Management Protocol (IGMP) delays, MPEG decoding delays, and I-frame acquisition time. Non-optimized IPTV channel change times can take several seconds. Channel change times as long as five seconds have been observed.

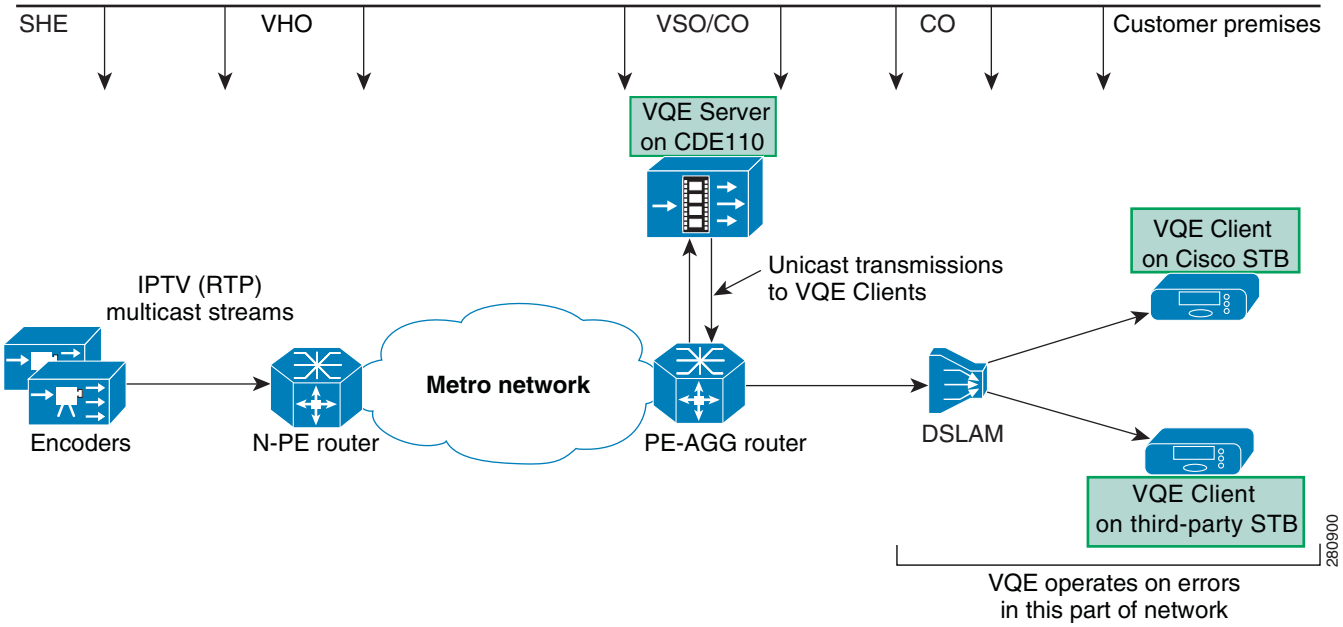
VQE addresses the issue of video quality from both a network infrastructure and a video technology perspective. VQE provides the linkage to optimize video delivery over next-generation carrier networks. Based on industry standards, including Real-Time Transport Protocol (RTP) and RTP Control Protocol (RTCP), Cisco VQE provides these mechanisms to help in delivering entertainment-grade services to subscribers:

- Unicast Retransmission—Optimized, selective retransmission of dropped IPTV packets caused by noisy DSL lines or errors in the home network caused by poor quality wiring. The set-top box receiver (VQE Client) sends NACK packets to VQE Server to request retransmission of the lost packets.
- Forward Error Correction (FEC)—Extra information is sent along with the video data at the application layer. The additional information is used by the VQE Client on the set-top box to detect and correct lost packets.
- Rapid Channel Change (RCC)—When the subscriber requests a channel change, the VQE Client on the set-top box sends VQE Server a request for the new channel's IPTV packets. The VQE Server sends the VQE Client an optimized unicast burst of IPTV packets and other channel information from the VQE Server's cached video data for the new channel. This greatly reduces the time needed to display the new channel.
- IPTV Packet Loss Monitoring—Facilities such as VQE-S RTCP Exporter help operators measure, baseline, and pinpoint problem areas of the video infrastructure, including transmission lines and home networks.

The two error-repair options, Unicast Retransmission and FEC, can be used separately or together for *Hybrid Error Repair*. Each repair mechanism has its own advantages and limitations. Whether Unicast Retransmission or FEC or both are used, the subscriber does not detect the error repair and no video artifact results.

Figure 1-1 shows the location of the major network and VQE components in the service-provider network and in the subscriber's customer premises equipment (CPE).

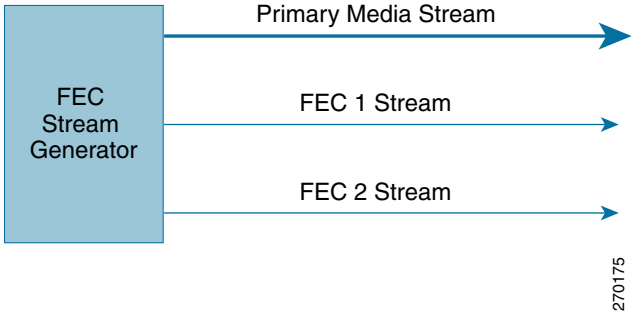
Figure 1-1 VQE Major Components



If FEC is used for error repair, an SMPTE 2022 compatible FEC stream generator, such as the Cisco Digital Content Manager (DCM), is required. The FEC stream generator (shown in Figure 1-2) is often located in the headend and transmits application-layer FEC packets. Real-Time Transport Protocol (RTP) encapsulation is a prerequisite for FEC.

The FEC stream generator, which is connected to the real-time encoders, subscribes to video channels from the headend and encodes FEC for each channel. It is responsible for originating FEC packets associated with individual channels and with primary multicast streams. For each FEC-enabled channel, a primary media stream and two encoded FEC streams are sent over multicast addresses (Figure 1-2).

Figure 1-2 FEC Stream Generator



VQE Major Software Components

The two major VQE software components that implement Unicast Retransmission, FEC, Rapid Channel Change, and IPTV Packet Loss Monitoring are:

- VQE Client (VQE-C)—Software embedded in the subscriber's CPE—typically a set-top box. VQE-C provides the CPE interface to VQE Server to support Unicast Retransmission, Rapid Channel Change, and IPTV Packet Loss Monitoring statistics. VQE Client receives the primary media data packets and, if FEC is enabled, one or two streams with FEC packets. When VQE Client software detects packet loss on a channel that is configured for FEC and Unicast Retransmission, the following occurs:
  - If there are packet losses in the primary media stream, VQE Client first tries to repair the lost packets using the FEC streams.
  - If some packet losses cannot be corrected by FEC, VQE Client requests a Unicast Retransmission of the missing packets from VQE Server.
- VQE Server (VQE-S)—Software that runs on a Linux-based Cisco Content Delivery Engine 110 (CDE110) appliance located in the intelligent edge of the service provider's network. For Unicast Retransmission and Rapid Channel Change, VQE Server caches primary video packets from an encoder or other headend device.
  - For Unicast Retransmission, working with VQE Client, VQE Server monitors the subscriber's reception of video packets and uses its cached video data to service Unicast Retransmission requests from the VQE Client on the set-top box.
  - For Rapid Channel Change, when the subscriber requests a channel change, VQE Client on the set-top box sends a request for a new channel to VQE Server. To service the Rapid Channel Change request, VQE Server sends the VQE Client a unicast burst of video packets from its cached video data for the channel and also sends some MPEG priming information to facilitate immediate decoding.

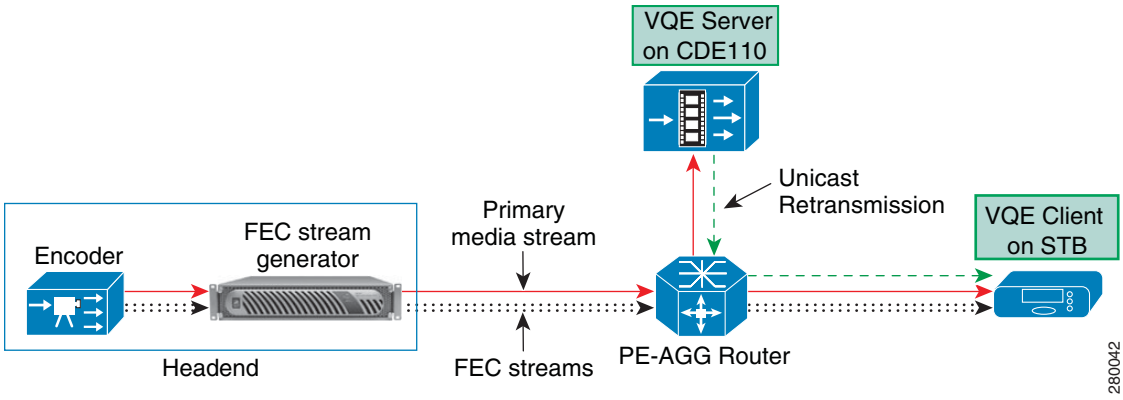
With both Unicast Retransmission and FEC, the missing packets are resequenced by the set-top box without interruption.

VQE Client is available with certain Cisco set-top boxes running Scientific-Atlanta IPTV Layer (SAIL) 1.x and 2.x. Please contact your Cisco sales representative for further information. VQE Client can also be integrated into set-top boxes from third-party vendors. The VQE Client code and Software Development Kit (SDK) is available to third-party vendors through an open-source program.

VQE Hybrid Error Repair

VQE Hybrid Error Repair occurs when Unicast Retransmission and FEC are used together. The devices used for Hybrid Error Repair are shown in Figure 1-3, which for simplicity omits some of the network elements. Hybrid Error Repair allows the service provider to customize VQE error repair to match the error characteristics of a given access network.

Figure 1-3 Hybrid Error Repair



In an IPTV system, video data is very sensitive to packet losses due to the interdependence of encoded data. One packet loss could cause quality degradation of several successive frames in a group of pictures (GOP). Selective retransmission and FEC are two methods to protect channels from packet losses.

With selective retransmission (Unicast Retransmission), NACK packets are sent to VQE Server to request retransmission of the lost packets whenever the receiver (VQE Client) detects dropped packets. Selective retransmission is very efficient in terms of bandwidth utilization in a unicast scenario, but may flood the network with control packets when errors are highly correlated in nature.

The application-layer FEC method of error repair is usually used for controlling errors in a one-way communication system. The FEC stream generator (for example, the Cisco DCM) sends FEC information along with the primary media stream. VQE Client uses the FEC data to detect and correct the lost packets. No feedback to VQE Server is needed. FEC is optimized for non-bursty, correlated errors. Unicast Retransmission is better for bursty, uncorrelated errors.

In addition to providing a flexible solution for error repair, VQE Hybrid Error Repair is also able to correct more lost-packet errors than when FEC is used alone. If VQE Client tries but is unable to retrieve lost packets using FEC, it can request that VQE Server selectively retransmit the dropped packets.

The VQE Hybrid Error Repair solution provides the flexibility to customize an error-repair scheme that best suits the network error characteristics and available access-link bandwidth.

VQE Rapid Channel Change

Channel change time is defined as the time from when a subscriber initiates a channel change to the time the video for the new channel is displayed. The Rapid Channel Change (RCC) functionality built into VQE Server and VQE Client reduces channel change time from several seconds to approximately one second.

There are several factors that contribute to channel change time:

- Multicast latency for “leaving” the old channel (IGMP leave latency)
- The time it takes for the set-top box to receive the information it needs to begin demultiplexing, decoding, decrypting and displaying the video stream. This time includes how long it takes to receive the following:
  - Program Association Tables (PAT), Program Map Tables (PMT), and Entitlement Control Messages (ECM) if decryption is required
  - Program Clock Reference (PCR) and sequence header information (for example, frame rate)
  - Random access point (such as I-frame) acquisition delay

  - Network buffer delays, including delays caused by error-mitigation techniques (Unicast Retransmission or FEC)
  - MPEG decoder buffer delay
- Multicast latency for "joining" the new channel (IGMP join latency)

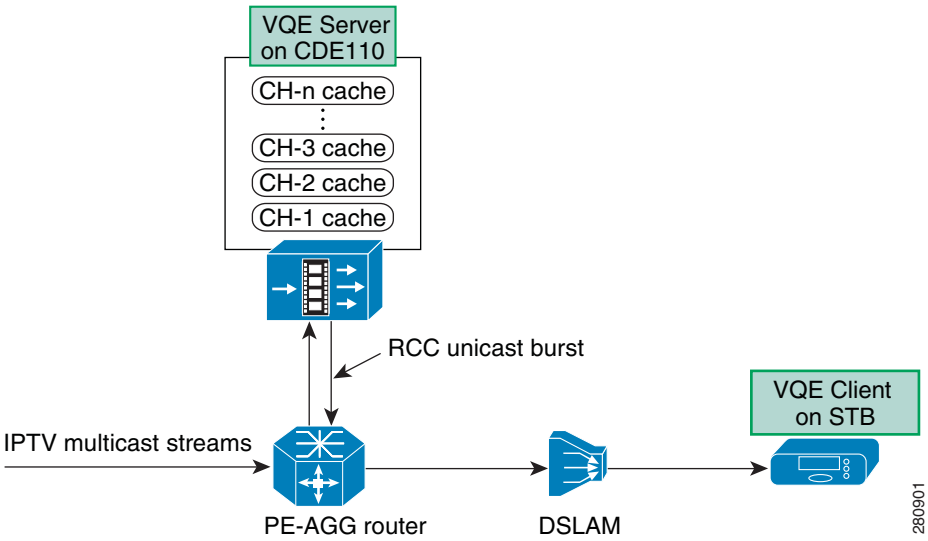
Not all of the above factors need to be addressed by RCC functionality. For example, many Digital Subscriber Line Access Multiplexers (DSLAMs) can provide fast leave for IGMP, which addresses the multicast leave latency factor.

The goal of RCC is to reduce or eliminate the main sources of channel change delay. With RCC, the resulting channel-change delay should be similar to or better than the delay observed in a typical digital broadcast.

For RCC, VQE Server caches multicast IPTV packets corresponding to each channel (Figure 1-4). Each cache holds a few GOPs of video data as well as PAT, PMT, ECM, PCR, and sequence information.

When the subscriber requests a channel change, VQE Client on the set-top box requests the IPTV packets for the new channel from its target VQE Server, using a specific RTCP message. After it has sent the RTCP message, the VQE Client issues an IGMP join for the new channel at an optimum point in time.

Figure 1-4 VQE Server Caches Multicast IPTV Packets for Rapid Channel Change



Upon receipt of the request, the VQE Server locates the appropriate channel cache, identifies the location of the IPTV packet carrying the beginning of a recent I-frame, and transmits a short unicast burst of packets starting with the I-frame to the requesting VQE Client.

Prior to sending the unicast burst, the VQE Server originates an RTCP message to the requesting VQE Client "priming" it with video parameters such as PAT, PMT, and ECM.

Because the incoming burst from the VQE Server contains an I-frame, the set-top box decoder can immediately start processing the MPEG information. This greatly reduces the time a subscriber waits before the image is rendered on the TV screen. Other VQE optimizations, such as Fast Decoder Buffer Fill, shorten channel change time by reducing MPEG decoder buffer delay.

After a short period of time, multicast packets for the new channel start to arrive at the set-top box. The VQE Client monitors RTP sequence numbers from both unicast and multicast streams. It is likely that VQE Client will see a few packets with duplicate RTP sequence numbers before the unicast stream ends. During this period, the VQE Client will only forward one copy of the RTP packet to the MPEG demultiplexing stage.

The VQE Client is responsible for managing the seamless transition between unicast and multicast IPTV packets. The RCC unicast burst continues for up to the full duration of the IGMP join or until it is explicitly stopped by a message sent from the VQE Client to the VQE Server.

RTP and RTCP

VQE relies on Real-Time Transport Protocol (RTP) and RTP Control Protocol (RTCP). RTP is used to carry video packets over multicast streams from the video headend to the VQE Clients on the set-top boxes. It is also used to transport specific video packets between the VQE Server and a VQE Client. RTCP is a signaling protocol used between VQE devices. RTP is the transport baseline for application-layer FEC, Unicast Retransmission, and Rapid Channel Change.

RTP encapsulation is typically the responsibility of real-time encoders and specialized video products, such as a Cisco DCM. These devices often reside in the video headend office (VHO) or super headend (SHE). RTP sequence numbers are assigned to IPTV packets and are unique within a given multicast group or channel.

A growing number of real-time encoders support native RTP and SMPTE 2022 FEC. For those that support UDP only or RTP encapsulation, the Cisco DCM product is recommended. For FEC support, the DCM requires the GbE I/O Board with a FEC daughter card, and DCM software version 5 or higher.

VQE Web Browser-based Tools

VQE also provides two web browser-based tools: VQE Channel Provisioning Tool (VCPT) and VQE-S Application Monitoring Tool (AMT).

- VQE Channel Provisioning Tool is an optional channel-provisioning utility to aid with the channel lineup configuration required by both the VQE Server and VQE Client. The channel information is in Session Description Protocol (SDP) format. VQE Channel Provisioning Tool sends the channel information to the VQE Servers and VQE Client Channel Configuration Delivery Servers. The VQE Client Channel Configuration Delivery Servers provide the channel lineup to the VQE Clients on the set-top boxes.
- VQE-S Application Monitoring Tool is a browser-based GUI that displays configuration, status, and statistics on the VQE-S processes, the channel lineup, Unicast Retransmission, Rapid Channel Change, Multicast Load Balancer, and VQE-S RTCP Exporter. VQE-S Application Monitoring Tool also allows you to configure debugging and logging facilities.

VQE Server and VQE Channel Provisioning Tool are bundled software and hardware solutions. VQE Server and VQE Channel Provisioning Tool run on separate Cisco Content Delivery Engine 110 (CDE110) appliances. A typical network might consist of multiple CDE110s hosting VQE Server and one or two CDE110s hosting VQE Channel Provisioning Tool and VQE Client Channel Configuration Delivery Server.

Lookaside Mode and the Cisco CDE110

The VQE-S software functions in *lookaside mode* where the VQE Server is not directly in the video data path. Lookaside mode has these advantages:

- If the Cisco CDE110 appliance or VQE-S software should fail, there is no loss of IPTV service to the customer.
- Because no multicast forwarding is provided by VQE-S, more IPTV customers can be serviced by each VQE-S instance.
- The number of Cisco CDE110 appliances hosting VQE-S can be easily scaled up as subscriber count and the demand for VQE services increase.

The Cisco Content Delivery Engine 110 is a standalone, carrier-hardened appliance running the Linux operating system. The Cisco CDE110 is NEBS-compliant and suitable for central office lights-out locations. The Cisco CDE110 comes with the required software pre-installed: VQE Server or VQE Channel Provisioning Tool, Linux, Apache web server, and other software.

VQE Benefits

Cisco VQE, Release 3.2, provides the following benefits to the service provider:

- Supports Hybrid Error Repair allowing use of Unicast Retransmission or FEC or both
- Addresses noise issues associated with lossy DSL lines and home network wiring
- Reduces or eliminates the need for outside plant optimization, such as pair swapping, joint renewals, and drop-cable re-runs
- Increases addressable market consumer base because Hybrid Error Repair technology enables video service over noisier transmission lines, thus extending available footprint
- Reduces or eliminates the need to fragment video service into consumers that can and cannot receive service based on line quality attributes
- Supports Rapid Channel Change to effectively reduce or eliminate the main sources of channel-change delay
- Employs much of the same infrastructure and the same technology (RTCP) for Unicast Retransmission and Rapid Channel Change—thereby reducing service-provider training time
- Reduces or eliminates quality-related service-center calls
- Establishes a video quality baseline for all consumers with granularity per set-top box
- Provides an end-to-end view of network characteristics from an IPTV delivery perspective
- Uses open, standards-based protocols

Cisco VQE also provides the subscriber with an enhanced video experience with higher and consistent visual and audio quality. Subscribers with noisier transmission lines or longer loop lengths can take advantage of the service provider's video offerings, bundles, and unique content.

VQE Server

The VQE Server (VQE-S) software is hosted on a Cisco CDE110 appliance running a standard Linux operating system. The Cisco CDE110 comes with the required software pre-installed: VQE-S, VQE-S Application Monitoring Tool, Linux, Apache web server, and other software.

VQE-S is responsible for the following functions:

- Creating a channel configuration database using the channel configuration information sent by the VQE Channel Provisioning Tool
- Maintaining per-channel and per-component state information
- Handling Unicast Retransmission by caching RTP data streams for channels and sending repair packets to the requesting VQE Clients on the set-top boxes
- Handling Rapid Channel Change by caching RTP data streams as well as PAT, PMT, ECM, PCR, and sequence information and sending RCC unicast bursts to requesting VQE Clients when a channel change occurs
- Load balancing VQE-S services across the Cisco CDE110 Ethernet interfaces
- Providing detailed statistics on IPTV delivery down to the set-top box VQE Client level
- Monitoring the health of VQE-S application processes

Like a regular IP host, VQE-S joins multicast groups using Internet Group Management Protocol (IGMP). VQE-S maintains a dedicated buffer for each channel. VQE-S receives the multicast stream for each channel from upstream, caching a few seconds of the most recently received program content from each. VQE-S can use the same cache of video to service both Unicast Retransmission requests and Rapid Channel Change requests.

For Unicast Retransmission, when a VQE Client requests retransmission of missing packets, VQE-S locates them in its cache and, if found, delivers them to the set-top box through an associated RTP retransmission stream. A single VQE Server can process up to 10,000 inbound repair requests per second. A repair request may support up to 17 packet retransmissions in a single transaction.

A number of factors affect how many errors a single VQE Server can repair for a single VQE Client. These factors include the distribution of errors, the bandwidth of the channel, and the size of the jitter buffer in the set-top box. The VQE-S software includes global and per-client policers to provide sensible rate limits for the traffic associated with Unicast Retransmission.

For Rapid Channel Change, VQE Server uses much the same infrastructure as Unicast Retransmission with some major additions. VQE-S can use the same cache of video data for both Unicast Retransmission and Rapid Channel Change. Instead of requesting repair of a specific packet, the VQE Client sends VQE-S an RTCP message requesting a unicast burst of IPTV packets for a new channel.

In addition, VQE-S uses its MPEG Parser component to choose the start point of the RCC burst for the new channel. To properly form the RCC burst, the MPEG Parser examines the video data for several pieces of crucial information, caches the information, and provides it to other VQE-S components upon receipt of an RCC request. Before play-out can begin, VQE Client must receive this information (for example, PAT, PMT, and PCR) to properly display the video. This additional data is sent out of band of the RCC burst and is used to prime the MPEG decoder on the client side.

VQE Server supports setting Differentiated Services Code Point (DSCP) values on IPTV-related packets so that specific levels of service can be assigned to different types packets. The service provider can configure DSCP values with the VQE Configuration Tool for RTCP and RTP traffic types.

The number of channels supported by single VQE Server is determined by the ingest capacity of the CDE110 server. Currently, the CDE110 provides 1 Gbps of ingest bandwidth. In practical terms, the number of channels currently supported by a single VQE Server is, for example, approximately 500 channels at 2 Mbs each, or 250 channels at 4 Mbs each.

VQE-S High Availability

VQE-S provides a number of high-availability mechanisms for resiliency and redundancy:

- The VQE-S processes (Control Plane, Data Plane, Multicast Load Balancer, and STUN Server) are constantly monitored by the VQE monitoring process—Process Monitor. If a VQE-S process fails, Process Monitor automatically attempts to restart it.
- If Process Monitor itself fails, the Linux initialization process detects this failure and restarts the VQE-S service (Process Monitor).
- If a Cisco CDE110 running VQE-S fails and there is a redundant, backup CDE110 running VQE-S that is configured to receive the same multicast streams, the backup VQE-S takes over servicing the streams.
- The use of anycast IP addresses and equal-cost multi-path routing allows multiple VQE Servers in a single facility to be loaded balanced between servers and to provide failover protection in case of a server failure. For more information, see the "Load Balancing and Redundancy with Multiple VQE-S Servers" section on page 2-14.

For Multicast Load Balancing, when a multicast stream used for caching on the VQE-S host starts or stops, VQE-S determines the best Cisco CDE110 Ethernet interface on which to join or leave the multicast group. The VQE-S software distributes the joins across available Ethernet interfaces to avoid oversubscription. VQE-S also monitors the status of these interfaces, moving the streams to other interfaces in case of interface failure.

VQE-S uses Linux system and network services for system initialization, network access, interface status monitoring, and multicast stream reception.

VQE-S and VQE-C Support for All NAT Mapping Types

VQE supports all Network Address Translation (NAT) mapping types, including address and port-dependent mapping (symmetric NAT). Symmetric NAT is the most restrictive form of NAT behavior.

Deployments where a CPE device is behind a NAT device require a NAT transversal mechanism, such as a Simple Traversal of UDP (User Data Protocol) through NATs (STUN) Server. The STUN Server is included with the VQE-S software, and a STUN Client is included with VQE-C. When VQE-C tunes to a new channel, it sends STUN binding requests to the STUN Server on the VQE-S host. VQE-C sends the requests to the channel's feedback target IP address and RTP/RTCP retransmission ports as configured on the VQE Server. VQE-C uses the STUN Server responses to determine whether it is behind a NAT device and what type of NAT device it is.

VQE-C is optimized to handle a variety of NAT configurations. For example, if VQE-C determines from the initial STUN responses that it is not behind a NAT device, it turns off NAT mode so that VQE-C does not send further STUN messages.

The STUN Server that is included with VQE-S can be turned on or off using a configurable option in the VQE-S configuration file. Unless it is certain that no set-top boxes being serviced by VQE-S are behind a NAT device, we recommend that you enable the STUN Server. For information on enabling the STUN Server, see the "VQE STUN Server Is Enabled By Default" section on page D-14.

VQE Client

The VQE Client (VQE-C) software runs on customer premises equipment (CPE), such as a set-top box. VQE Client supports Unicast Retransmission, FEC, Rapid Channel Change, and video-quality statistics by providing the following:

- CPE interface to VQE-S for Unicast Retransmission and Rapid Channel Change
- FEC functionality to receive and decode FEC packets for error repair
- RTP packet reordering
- RTP data plane jitter buffer and de-jittering
- IPTV Packet Loss Monitoring

For Unicast Retransmission, if an error in video transmission occurs, the VQE-C software detects the packet loss and requests a retransmission while holding the video sequence in queue. VQE Server automatically repairs the error by transmitting the missing packet, which is resequenced by the set-top box without interruption. The entire error-repair cycle is imperceptible to the viewer.

For Rapid Channel Change, when a subscriber selects a new channel, VQE-C sends to the VQE Server a special RTCP packet requesting a unicast burst of the IPTV packets for the new channel. As soon as the unicast IPTV packets arrive, the VQE-C software is responsible for sending the packets to the decoder. When the multicast IPTV packets for the new channel begin to arrive, VQE-C manages the seamless transition between unicast packets from VQE Server and multicast packets from the headend encoder.

VQE Clients can get channel configuration information from a VQE Client Channel Configuration Delivery Server (VCDS) or from a centralized network management/configuration server that supports the DESCRIBE request of the RTSP protocol. For information on the interactions between a VQE Client and a VQE Client Channel Configuration Delivery Server, see the "VQE Client Channel Configuration Delivery Server" section on page 1-17.

VQE Client supports setting Differentiated Services Code Point (DSCP) values on IPTV-related packets it sends so that specific levels of service can be assigned to packets. DSCP values can be configured with the rtcp_dscp_value parameter in the VQE-C system configuration file. The setting of rtcp_dscp_value applies to both the RTCP messages and the STUN messages.

VQE Client is available in two deployment models:

- VQE Client is integrated into selected Cisco set-top boxes.
- The VQE-C code is offered through an open-source program for integration with set-top boxes from third-party vendors.

For information on VQE-C deployment models, see the "VQE Deployment Options and Requirements" section on page 1-13.

VQE-C Forward Error Correction

VQE Client supports both one-dimension FEC (one FEC stream) and two-dimension FEC streams (two FEC streams). The Cisco DCM or other SMPTE 2022 compliant FEC stream generator sends one primary media stream and one or two FEC streams over different UDP ports to VQE-C. The VQE-C receives and processes these FEC streams to provide packet-level error repair.

Before receiving the FEC packets, the VQE-C must learn some basic information about the FEC session, such as the IP address and port numbers of FEC streams. This information is obtained through the channel configuration file that is sent to the VQE-C from the channel provisioning server, such as VQE Client Channel Configuration Delivery Server. The FEC streams are configured on a per-channel basis.

When a VQE Client detects packet loss on a channel that is configured for FEC and Unicast Retransmission, the following occurs:

- VQE Client first tries to repair the lost packets using the FEC streams.
- If some packet losses cannot be corrected by FEC, VQE Client requests a Unicast Retransmission of the missing packets from VQE Server.

The use of one-dimension (1-D) or two-dimension (2-D) FEC is configured when the channel is defined. 1-D FEC uses one FEC stream, and 2-D FEC uses two FEC streams. While 2-D FEC can correct more packet losses than 1-D FEC, 2-D FEC sometimes requires more intensive processing of both FEC streams to maximize the number of packets recovered. FEC bandwidth overheads may be too high in some deployments for full FEC-based error repair deployment. FEC can be turned on or off on a per-channel basis through the VQE-C channel configuration file.

VQE-C supports a number of extensions to the SMPTE 2022 standard. VQE-C autodetects L (column) and D (row) values, and allows any combination of L and D sizes where L*D <= 256. This is an extension of the SMPTE 2022 limit of L*D <= 100. VQE-C also allows any payload value to identify FEC packets where the standard says the value must be equal to 96.

VQE-C supports SMPTE 2022 Annex A and Annex B stream orderings. For detailed information on 1-D and 2-D FEC, see the SMPTE standard *Forward Error Correction for Real-Time Video/Audio Transport Over IP Networks* (SMPTE 2022-1-2007). The standard is available for purchase at this URL:

http://www.smpte.org/standards

VQE-C IPTV Packet Loss Monitoring

When used with VQE-S RTCP Exporter, the VQE-C software also provides the instrumentation for IPTV Packet Loss Monitoring and valuable “last hop” analysis. VQE Clients generate RTP packet-level statistics for packet loss, jitter, delay, and other quality measurements. VQE Clients provide statistics on both Unicast Retransmission and FEC. For the RTCP reports, VQE Clients transmit RTCP compound packets to their target VQE-S. Each compound packet contains an RTCP receiver report as well as other information.

For more information on IPTV Packet Loss Monitoring, see the “VQE-S RTCP Exporter for Video-Quality Monitoring” section on page 1-21.

VQE-C Software Development Kit and Documentation

VQE-C consists of a software development kit (SDK), which can be used for VQE-C integration into set-top boxes from third-party vendors. The VQE-C code and SDK is available to third-party vendors through an open-source program. The VQE-C code resembles a standard Linux software component. The VQE-C source code is currently supported for the Linux operating system. For information on support for other operating systems, contact your Cisco account representative.

The VQE-C library provides a set of high-level APIs designed to support easy integration into an existing set-top box (STB) software base. The programmatic interface provides a “socket replacement” interface, which is used to get packets from a repaired VQE Server-enhanced video stream. VQE-C also provides APIs for updating its channel configuration data and acquiring statistics on error repairs.

The integrator configures the VQE-C through system configuration file parameters. The parameters allow customizing of many elements of the VQE-C system (for example, number of concurrent streams and client policing). The configuration of a VQE Client must be coordinated with the configuration of VQE Server. Certain features are operational only when they are enabled on both VQE-C and VQE-S.

The VQE-C command-line interface (CLI), based on the open source library libcli (http://sourceforge.net/projects/libcli), is designed primarily for testing and debugging the VQE-C software on the set-top box. The scope of the CLI is limited to the VQE-C software only. The CLI is accessible by Telnet.

The VQE-C SDK and documentation can be downloaded from Cisco.com. Table 1-1 lists the VQE-C documentation that is provided.

Table 1-1 VQE-C Documentation

VQE-C Document	Description
VQE-C Release Notes	Provides release-specific information on VQE-C.
VQE-C System Integration Reference	Provides information on VQE-C components, architecture, integration, and APIs. Also includes a VQE-C quick-start guide.
VQE-C System Configuration Guide	Explains certain factors to consider when configuring and deploying VQE-C. Also provides reference information on the VQE-C configuration file parameters.
VQE-C CLI Command Reference	Provides reference information on the VQE-C command-line interface.

VQE Deployment Options and Requirements

The two basic deployment options for VQE are as follows:

- VQE reference architecture model—For existing IPTV deployments or new IPTV deployments that do not use Cisco set-top boxes
- Cisco end-to-end IPTV solution model—For new IPTV opportunities

With both deployment options, VQE Server is deployed on a Cisco CDE110 appliance running Linux.

VQE Reference Architecture Model

The VQE reference architecture model is designed for existing IPTV deployments or new IPTV deployments that do not use Cisco set-top boxes. Cisco offers VQE-C as open-source software. VQE-C is implemented so that service providers and CPE device vendors can integrate the VQE-C software with third-party set-top boxes. Appropriate development-level documentation is available along with the VQE-C code.

With this model, the service provider uses the VQE Channel Provisioning Tool to define channels and servers and to create channel lineups for different subscriber regions. The VQE Channel Provisioning Tool sends the channel information to the VQE Servers and to the VQE Client Channel Configuration Delivery Servers from which each VQE Client gets its channel information. The channel information is in the Session Description Protocol (SDP) format required by VQE-S and VQE Client Channel Configuration Delivery Server.

Cisco End-to-End IPTV Solution Model

The Cisco end-to-end IPTV solution model is designed for new or "greenfield" IPTV opportunities. VQE technology is included as an integral part of the Cisco end-to-end video solution.

In this model, VQE-C is integrated with selected Cisco set-top boxes. The main difference between the Cisco end-to-end IPTV solution and the VQE reference architecture models lies with the integration responsibility of VQE-C.

- For the Cisco end-to-end IPTV solution model, Cisco is responsible for the integration and testing of VQE-C.
- For the VQE reference architecture model, the third-party vendor is responsible for the integration and testing of VQE-C.

For the Cisco end-to-end IPTV solution, contact your Cisco representative for details of the set-top box models and software versions supported.

VQE Deployment Requirements

To deploy VQE, the following prerequisites must be met:

- Real-Time Transport Protocol (RTP) support—Video streams from the headend must be encapsulated in RTP. Service providers can deploy products such as the Cisco Digital Content Manager (DCM) to provide RTP encapsulation capabilities at the video headend.
- VQE-C and CPE integration—VQE-C must be integrated with the software of the CPE device (set-top box).
- TV channel information—VQE-C and VQE-S require details of network-level TV channel lineup information. This includes per-channel IP multicast addresses, port numbers, and some other parameters. The information must be presented to the VQE-C and VQE-S components in Session Description Protocol (SDP) format. The VQE Channel Provisioning Tool is designed specifically for this purpose.
- If forward error correction is used, an SMPTE 2022 compatible device, such as an encoder or Cisco DCM, is required to transmit FEC streams to VQE-C.
- VQE-S network connectivity— VQE-S requires a connection to the edge router for the purposes of joining and receiving Internet Group Management Protocol (IGMP) multicast groups (channels). A direct, Layer 3 connection between VQE-S and the edge router is preferred.
- VQE-C network connectivity—VQE-C requires an IP unicast path to and from its designated VQE-S. The path is used for RTP Control Protocol (RTCP) signaling between the VQE-C and VQE-S, and for sending RTP data packets from VQE-S to VQE-C.
- All versions of IGMP are supported by VQE-S and VQE-C.

VQE Channel Provisioning Tool and Channel Information

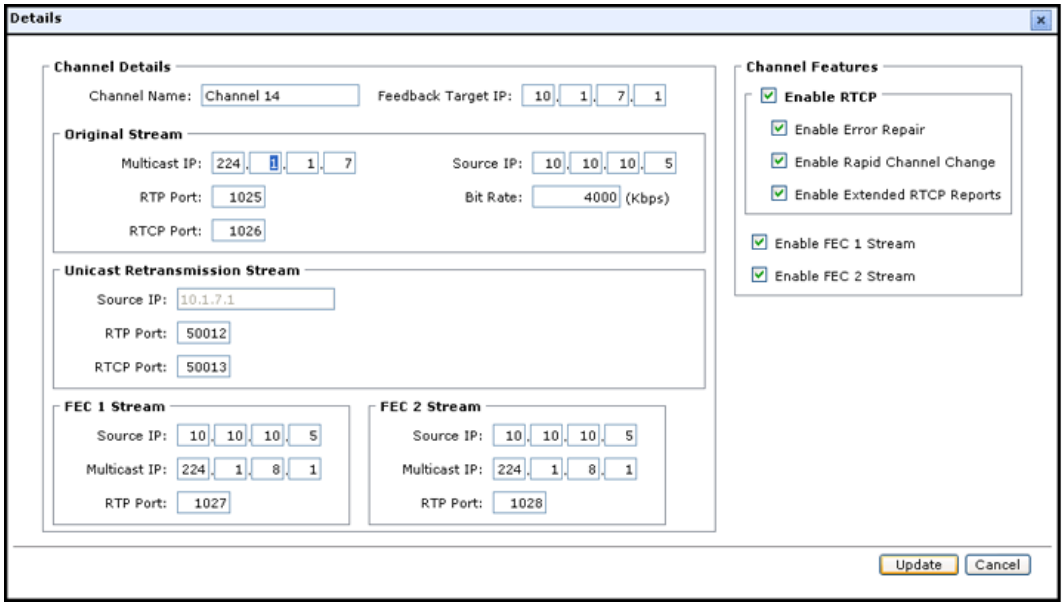
The VQE Channel Provisioning Tool (VCPT) is responsible for the creation, maintenance, and distribution of the channel information containing channel-lineup data. VCPT includes a browser-based GUI that allows the service provider to provision the following:

- Channel definitions—Information on the channels that will be serviced by VQE

- Server definitions—Information on each VQE Server and VQE Client Channel Configuration Delivery Server that will receive the channel information
- Channel lineups—Associations between channels and the VQE Servers and VQE Client Channel Configuration Delivery Servers

Figure 1-5 shows the details that the service provider defines for each channel using VCPT. The channel details include information that is used for VQE error repair—both Unicast Retransmission and FEC—and for Rapid Channel Change.

Figure 1-5 VCPT Channel Definition



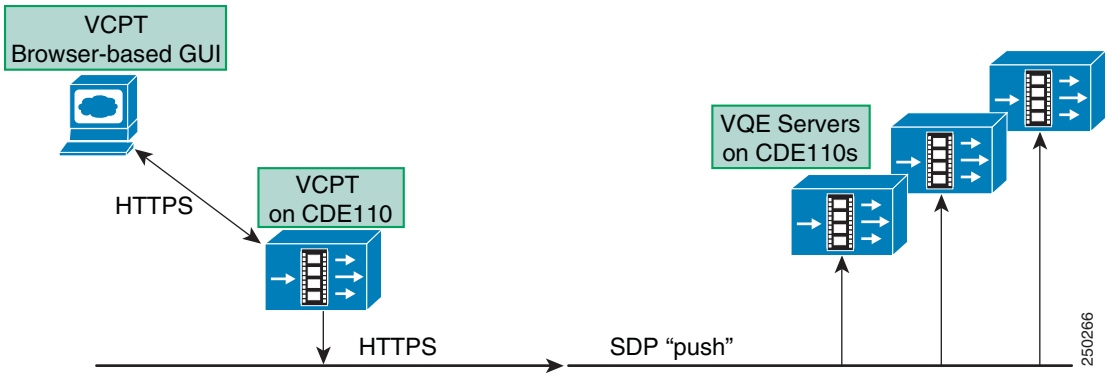
The VCPT GUI has a clone capability to simplify and expedite channel information. When the service provider uses VCPT to define the set of VQE Servers that receive the channel information, the VQE Servers can be grouped based on channel lineups. Using separate VCPT configuration files makes it possible to manage multiple deployments. For example, one VCPT configuration file might be for the channel lineup in one metro region, and another VCPT configuration file might be for the channel lineup in another metro region.

The VCPT channel-provisioning process creates a persistent local database, which is stored on the Cisco CDE110 appliance. When the Cisco CDE110 or VCPT is restarted, channel data and server grouping information is read from the local database.

When the user completes channel, server, and channel-lineup configuration and initiates the VCPT send operation, VCPT sends the channel information in Session Description Protocol (SDP) format to the set of VQE Servers and to the VQE Client Channel Configuration Delivery Server.

VCPT sends or “pushes” the channel information to all VQE Servers that are defined in the current VCPT configuration file. The channel information is sent to the VQE Servers over secure HTTPS. VCPT contains a secure HTTPS client, and each VQE Server has an embedded web server running. Each VQE Server stores it own local copy of the channel information. Figure 1-6 shows the interactions between VCPT and the VQE Servers. For information on the VQE Servers, see the “VQE Server” section on page 1-8.

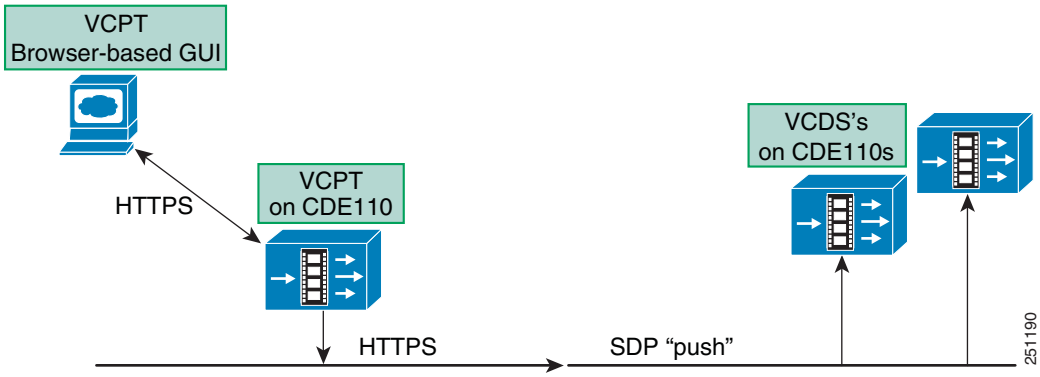
Figure 1-6 VCPT: Sending Channel Information to VQE Servers



VCPT is also responsible for sending channel information to each VQE Client Channel Configuration Delivery Server (VCDS). VCDS is a software component installed on each VQE Tools server, the Cisco CDE110 that also hosts VCPT. When the service-provider operator initiates the VCPT send operation, VCPT "pushes" the channel information to one or more VQE Client Channel Configuration Delivery Servers. VCPT sends the channel information in SDP format through HTTPS similar to the way it is sent to the VQE Servers.

Figure 1-7 shows the interactions between VCPT and the VCDS's. Each VQE Tools server includes both VCPT and VCDS. VCPT can also send channel information to the VCDS on the same CDE110 on which the VCPT resides. This interaction within a single VQE Tools server (CDE110) is not shown in Figure 1-7.

Figure 1-7 VCPT: Sending Channel Information to VCDS's



VQE Client Channel Configuration Delivery Server

VQE Client Channel Configuration Delivery Server (VCDS) is a software component on the VQE Tools server that can be used to deliver the channel configuration file to the VQE Clients on the set-top boxes. This VCDS function is explained in the following section:

- VCDS Delivery of the Channel Configuration File, page 1-17

VCDS Delivery of the Channel Configuration File

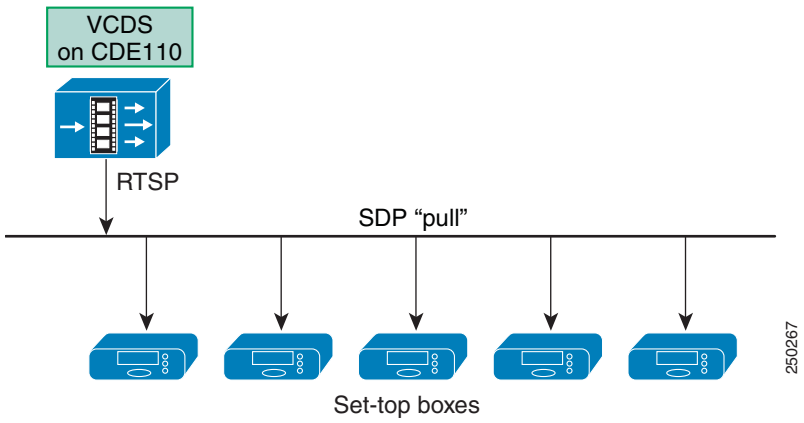
When the VCDS receives information on the channel lineup from VCPT, VCDS creates a channel configuration file and stores it on the local disk.

Each VQE Client running in a CPE device, such as a set-top box, uses a Real Time Streaming Protocol (RTSP) "pull" operation to receive the channel configuration file from VCDS. VCDS is a simplified RTSP server that supports the VQE Client RTSP "pull" operation. The VQE Client learns the name of the VCDS through a Domain Name System (DNS) server using a SRV lookup.

After the VQE Client learns the VCDS name, it sends out an RTSP DESCRIBE request asking for the change status of the channel configuration. If there is new information on channels, the VQE Client asks the VCDS to send the channel configuration file. In response, the VCDS sends the channel configuration file for the entire channel set in SDP format. Figure 1-8 shows the interaction between a VCDS and the VQE Clients on the subscriber set-top boxes.

For information on the interactions between the VCDS and the other components in the channel delivery infrastructure, see Appendix E, "Configuring DHCP and DNS Servers for VCDS."

Figure 1-8 VQE-C on Set-Top Box: Receiving Channel Information File from VCDS



The VQE Client requests the channel configuration file from VCDS when the set-top box is started and VQE-C is initialized. After the initialization, VQE-C can receive an updated channel configuration file by the following mechanisms:

- Periodic polls—VQE-C periodically polls VCDS to determine whether a new channel configuration file is available. If a new version of the channel configuration file is detected during a poll, the VQE-C requests the updated channel configuration file.

- Triggered polls—When the set-top box attempts to tune to a channel that is not present in the VQE-C channel lineup, VQE-C attempts to retrieve a new channel configuration file from VCDS. As it does in a periodic-poll update, the VQE-C first determines whether an updated version of the file is available. If so, the VQE-C requests the updated channel configuration file.

With both periodic polls and triggered polls, the VQE-C uses the new channel configuration file to update the channel lineup that is in use and writes the channel configuration to the file specified in the VQE-C channel-lineup system configuration.

VQE-S Application Monitoring Tool

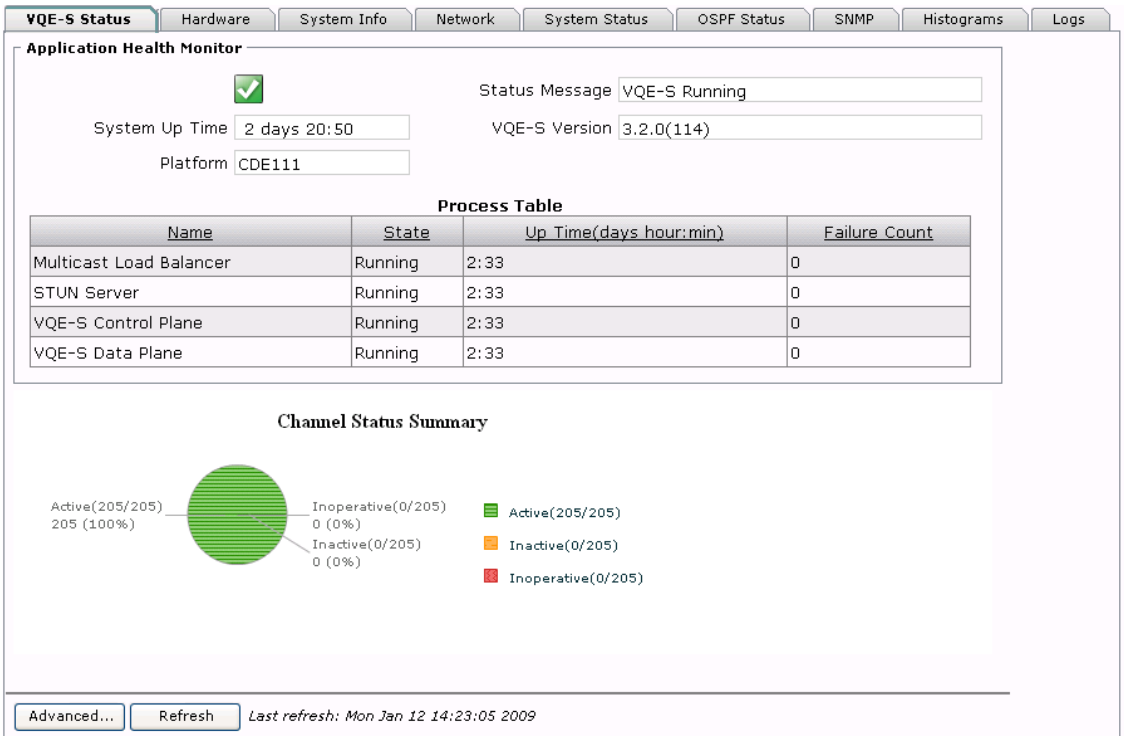
The VQE-S Application Monitoring Tool (VQE-S AMT or AMT) is a browser-based GUI that allows the service-provider operator to do the following:

- Monitor the health of the VQE-S processes
- View channel configuration details, status, and statistics
- Monitor statistics for Unicast Retransmission and Rapid Channel Change
- Monitor statistics for STUN Server usage
- View configuration details, status, and statistics for:
  - Multicast Load Balancer
  - VQE-S RTCP Exporter
- Configure VQE-S logging levels and debugging options

The next paragraphs provide a few examples of VQE-S AMT functionality.

When you log in to VQE-S AMT, the initial window (Figure 1-9) shows the health of VQE-S processes and other status information.

Figure 1-9 Monitoring VQE-S Processes



With VQE-S AMT, you can view the channel lineup that was sent from the VQE Channel Provisioning Tool. Figure 1-10 shows a partial example of the channel lineup with usage statistics that VQE-S AMT displays.

Figure 1-10 Viewing Channel Lineups with Usage Statistics

Channel Lineups *Last update: 2008-07-08T14:44:14, Total Channels: 250, Active Channels: 240 Aggregated Bandwidth: 1215000(kbits/sec), Total Receivers: 1040*

Name	Status	Original Multicast	Feedback Target	Bit Rate (Kbps)	Repair Enabled	RCC Enabled	Member Receiver Population
Channel 229.1.1.1	✓	229.1.1.1:53170	11.112.1.1:53171	4000	true	true	400
Channel 229.1.1.10	✓	229.1.1.10:53206	11.112.1.10:53207	13000	true	true	0
Channel 229.1.1.11	✓	229.1.1.11:53210	11.112.1.11:53211	4000	true	true	0
Channel 229.1.1.12	✓	229.1.1.12:53214	11.112.1.12:53215	4000	true	true	0
Channel 229.1.1.13	✓	229.1.1.13:53218	11.112.1.13:53219	4000	true	true	0
Channel 229.1.1.14	✓	229.1.1.14:53222	11.112.1.14:53223	4000	true	true	0
Channel 229.1.1.15	✓	229.1.1.15:53226	11.112.1.15:53227	2000	true	true	0

281142

In Figure 1-10, the channel-lineup summary data indicates when the lineup was last updated (for example, with VCPT) and provides totals for all channels and active channels as well as aggregated bandwidth and total receivers:

```
Last update: 2008-07-08T14:44:14, Total Channels: 250, Active Channels: 240
Aggregated Bandwidth: 1215000 (kbits/sec), Total Receivers: 1040
```

In the channel-lineup summary data, the rightmost column, Member Receiver Population, is the number of VQE Clients that are currently receiving this multicast stream.

VQE-S AMT uses the Unicast Retransmission and Rapid Channel Change counters kept by the VQE Server to display a variety of data. For Unicast Retransmissions, the counters include NACK messages received from VQE Clients, RTP packets requested and sent, and error repair rates. For Rapid Channel Change, the counters are for RCCs requested, accepted, and refused.

For Cisco VQE AMT provides limited configuration capabilities. The items that can be configured with AMT include parameters for the following:

- Logging priority level for VQE-S processes
- Debugging options for VQE-S-related functions, including RTP/RTCP packets, events, and errors

The VQE Server channel lineup is stored locally on the Cisco CDE110 appliance. If VQE-S is restarted, the channel lineup is read from the local repository. The VQE-S counters for statistics that AMT displays are reset to zero when VQE-S is restarted.

VQE-S AMT is a web application that uses the application server and web server that are pre-installed on the Cisco CDE110 where VQE-S runs. VQE-S AMT has an XML-RPC client that communicates with multiple internal applications, such as VQE-S processes, to send and receive application management data.

VQE-S RTCP Exporter for Video-Quality Monitoring

VQE-S provides a variety of data for monitoring IPTV packet delivery and for fault isolation. VQE-S receives RTCP reports from VQE Clients on the CPE devices and from reports generated by the VQE-S itself. In those reports, VQE Clients provide statistics for RTP packet loss, jitter, delay, and other quality measurements. VQE Clients also provide statistics on Unicast Retransmission.

For the RTCP reports, each VQE Client periodically transmits RTCP compound packets to its target VQE-S. Each compound packet contains an RTCP receiver report as well as other information. Each VQE Client sends additional RTCP reports every time a Unicast Retransmission request is made.

The service provider can use VQE-S RTCP Exporter to export the RTCP compound packets to a video-quality monitoring (VQM) application. The VQM application can collect the exported data in a database for use in video-quality analysis. The video-quality monitoring application is outside the scope of the VQE solution. The VQE documentation set includes detailed information on the data collected and the formats used in the RTCP reports.

VQE-S RTCP Exporter is responsible for sending the RTCP compound packets to an external device, which typically hosts the video-quality monitoring application. The compound packets are sent over a TCP socket to a configurable location. The monitoring application is identified by IP address or Internet domain name and a TCP port number.

The data in the RTCP compound packets are very useful for determining the quality of video service and for isolating faults. The data help the service provider to measure, baseline, and pinpoint problem areas of the video infrastructure, including transmission lines and home networks. The granularity of the data is per set-top box. The data could be stored in a database and searched for answers to questions of interest, such as whether packet loss and jitter events have occurred in the network and, if so, where and when the events have occurred.

Starting with VQE, Release 3.0, RTCP Extended Reports and the Extended Report (XR) packet type are supported. Three XR report block types are supported:

- Loss RLE (run-length encoded)
- Statistics Summary
- Post-Repair Loss RLE

Extended Reports provide information that supplements the statistics contained in the report blocks used by the RTCP sender and receiver reports. For example, the Loss RLE report block type provides much more detailed reporting on individual packets and loss events than is provided in standard RTCP reports. VQE Channel Provisioning Tool allows the service provider to specify whether or not RTCP Extended Reports will be used for each channel.

The following documents, which are available from the Internet FAQ Archives, provide more information on RTCP reports:

- RTCP reports are described in RFC 3550.
- RTCP Extended Reports are described in RFC 3611

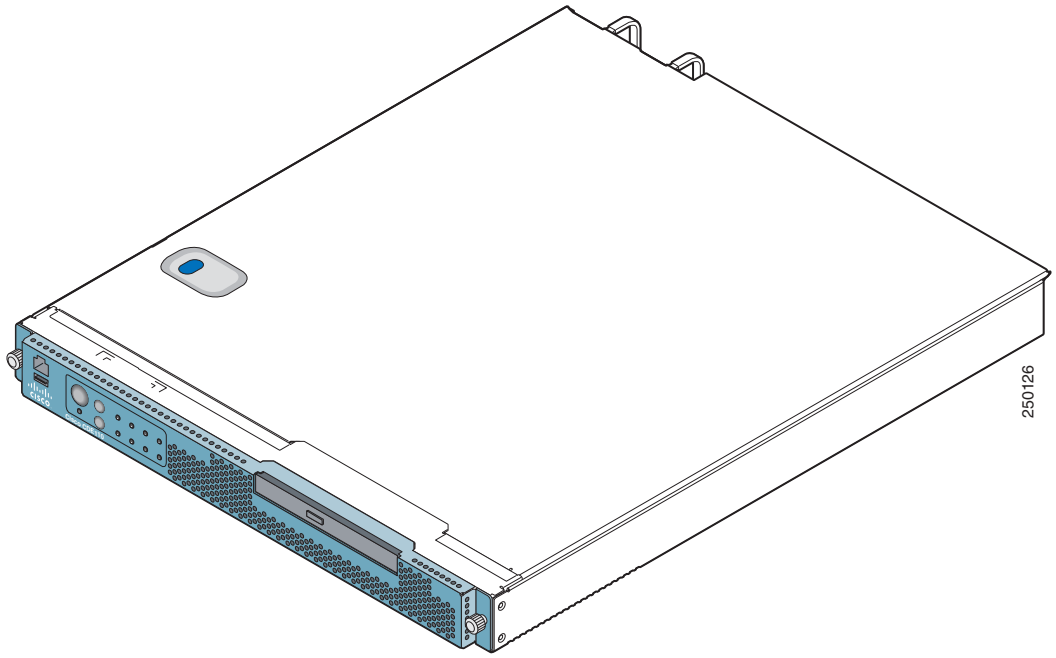
The new Post-Repair Loss RLE report block type contains information on individual packet receipt and loss events, after packet recovery techniques (Unicast Retransmission or FEC or both) have been applied. For more information, see the document *Post-Repair Loss RLE Report Block Type for RTCP XR* at:

http://tools.ietf.org/html/draft-begen-avt-post-repair-rtcp-xr-01

Content Delivery Engine 110

Each VQE Server runs on one Cisco Content Delivery Engine 110 (CDE110). If VQE Channel Provisioning Tool and VQE Client Channel Configuration Deliver Server are used, another Cisco CDE110 hosts these two facilities. The Cisco CDE110 (Figure 1-11) comes with the Red Hat Enterprise Linux 5.1 operating system and either the VQE-S or VCPT and VQE Client Channel Configuration Deliver Server software pre-installed.

Figure 1-11 Content Delivery Engine 110



Note The descriptions of hardware given in the following paragraphs are for the latest CDE110 models (CDE111-2-146TXA-K9 and CDE111-2-146TXD-K9). For complete information on all CDE110 models, see the *Cisco Content Delivery Engine 110 Hardware Installation Guide*.

The Cisco CDE110 appliance is a NEBS-3 and ETSI-compliant carrier-grade rack server. It is powered by two 64-bit Quad-Core Intel Xeon L5410 processors with 12 MB of shared L2 cache. For maximized bandwidth, it contains 8 GB of dual-channel Fully Buffered DIMM (FB-DIMM) memory at 667 MHz. For storage, the Cisco CDE110 has one 36-GB simple-swap, serial attached SCSI (SAS) hard disk drive. The optical drive is a CD/DVD RW combination drive.

The Cisco CDE110 has six 10/100/1000 Mb Ethernet ports and a serial port for the system console. Earlier CDE110 models have four 10/100/1000 Mb Ethernet ports. The Ethernet ports can be load-balanced for incoming multicast IPTV streams and for outgoing Unicast Retransmission and Rapid Channel Change streams to the VQE Clients.

The Cisco CDE110 has a 1-RU form factor and is available with redundant AC or DC hot-swappable power supplies. The Cisco CDE110's Telco Alarm Management features provide visual, audible (optional), and SNMP event indications of faults, consistent with the rigid requirements of the telecom central office environment.

CHAPTER 2

Getting Started with the VQE Startup Configuration Utility

This chapter explains how to use the Cisco VQE Startup Configuration Utility to perform the initial configuration tasks needed to get the two categories of Cisco CDE110 servers running with the Cisco VQE software:

- VQE-S server—CDE110 hosting VQE Server
- VQE Tools server—CDE110 hosting VQE Channel Provisioning Tool (VCPT) and VQE Client Channel Configuration Delivery Server (VCDS)

In a VQE deployment, use of the VQE Tools server with VCPT and VCDS is optional.

Note We recommend that you use the VQE Startup Configuration Utility rather than try to do the initial configuration manually because the utility simplifies your work and is known to produce correct results.

For information on the manual initial VQE configuration tasks, see Appendix D, "Manual Initial VQE System Configuration."

Read the following sections for information on CDE110 configuration and on using the VQE Startup Configuration Utility:

Note The configuration instructions in this chapter are intended for new installations of Cisco VQE, Release 3.2, software, where the Cisco CDE110 has the Cisco VQE, Release 3.2, software preinstalled.

For information on upgrading a Cisco CDE110 from Cisco VQE Release 2.1, 3.0, or 3.1 to Release 3.2, see the *Release Notes for Cisco CDA Visual Quality Experience Application, Release 3.2*.

This chapter assumes that the Cisco CDE110 hardware has been installed as described in the *Cisco Content Delivery Engine 110 Hardware Installation Guide*, including connecting cables and connecting power.

Web Browser, Screen Resolution, and Other Requirements

To access the VQE-S Application Monitoring Tool (VQE-S AMT or AMT) or the VQE Channel Provisioning Tool (VCPT), you need a web browser. For these tools, the following web browsers are supported:

- Microsoft Internet Explorer version 6.0 or later
- Mozilla Firefox version 2.0 or later

The minimum screen resolution required for VQE-S AMT and VCPT is 1024 x 768 pixels.

For VQE-S AMT, Adobe Flash Player must be installed on the computer that hosts the browser accessing AMT. Adobe Flash Player is required to display the Channels Status Summary graph of active, inoperative, and inactive channels in the AMT VQE-S Status window. Adobe Flash Player is free and can be found at this URL:

http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash

Configuring Terminal Emulation Software

The RJ-45 serial ports on the Cisco CDE110 front and back panels can be used for administrative access to the CDE110 through a terminal server. Terminal emulation software must be configured as follows:

- Bits per second: 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Hardware flow control: ON

Security Restrictions for Logins and Root Privileges

For security reasons, the following restrictions apply to VQE:

- The root user cannot use Secure Shell (SSH) to log in to a CDE110 that hosts VQE-S or VCPT, or to log in to VQE-S AMT or VCPT. The vqe username should be used instead. The vqe username is a pre-created Linux user ID and has its password set during CDE110 initial system configuration.

- Only users in the wheel group can use the **su** or **sudo** commands. By default, the vqe username is in the wheel group.

If you want to add user accounts to the wheel group so that additional users can use **su** and **sudo**, log in as root and issue the following command:

```
[root@system]# usermod -G wheel username
```

In the preceding, *username* specifies the user who will be added to the wheel group.

Prerequisites

Before you start the initial VQE software configuration, the following items should be accomplished for the CDE110 that hosts VQE-S and the CDE110 that hosts the VQE Tools:

- Connect cables to the CDE110—See the "Connecting Cables to the CDE110" section on page 2-3.
- Determine how you will set up Secure Sockets Layer (SSL) certificates—For information on the alternatives available to you, see the "Setting Up SSL Certificates with the VQE Startup Configuration Utility" section on page 2-4.

Connecting Cables to the CDE110

The following cable connections are used on the Cisco CDE110 that hosts VQE-S and on the CDE110 that hosts the VQE Tools:

- Depending on whether the host is for VQE-S or VQE Tools, do one of the following:

Note Earlier models of the CDE110 have four Ethernet ports. The latest models of the CDE110 include the Intel PRO/1000 PT Dual Port Server Adapter that provides two additional Ethernet ports.

  - On a VQE-S server, use Category 5 UTP cables to connect up to six Ethernet interfaces on the back of the Cisco CDE110 to Ethernet interfaces on the edge router that is providing multicast streams for each IPTV channel. For optimal VQE-S performance, all Ethernet interfaces on the Cisco CDE110 should have a direct Layer 3 connection to the edge router.

Note For OSPF routing on the VQE-S server, the Ethernet interfaces used for VQE-S traffic *must have* a direct Layer 3 connection to the edge router.

  - On a VQE Tools server, use Category 5 UTP cable to connect at least one of the Ethernet interfaces on the back of the CDE110 to the same network that the CDE110s that host VQE-S are on. If you use additional Ethernet interfaces for link redundancy, connect Category 5 UTP cables for those interfaces also.

- If a terminal server is used, the RJ-45 cable from the terminal server is connected to an RJ-45 serial port on the front or back of the Cisco CDE110. Only one serial port can be used because it is one shared serial port.
- If a PC is directly connected to the CDE110 serial port, the cable from the PC is connected to an RJ-45 serial port on the front or back of the Cisco CDE110. Only one serial port (front or back) can be used because it is one shared serial port. The PC end of the cable connected to the CDE110 serial port varies depending on the type of ports supported by the PC.

Note The serial port is used for the system console. A system console is typically used rather than a monitor, keyboard, and mouse directly attached to the Cisco CDE110.

- If a monitor, keyboard, and mouse are used, the cables for the devices are connected to the appropriate connectors on the Cisco CDE110.

For the location of connectors on the Cisco CDE110 front and back panels, see the *Cisco Content Delivery Engine 110 Hardware Installation Guide*.

Setting Up SSL Certificates with the VQE Startup Configuration Utility

Secure Sockets Layer (SSL) certificates must be deployed on the CDE110s for HTTPS to operate. You can let the Cisco VQE Startup Configuration Utility do most of the creation and deployment, or you can do the creation and deployment tasks yourself. For information on your options for SSL certificates with the startup utility, see the "Using the Cisco VQE Startup Configuration Utility for SSL Certificates" section on page 2-4.

Setting Up SSL Certificates

VQE-S Application Monitoring Tool (VQE-S AMT or AMT) and VQE Channel Provisioning Tool (VCPT) require Secure Sockets Layer (SSL) certificates from a certificate authority (CA). The CA can be you or someone in your company, or can be a commercial CA, such as VeriSign.

On the CDE110s hosting VQE-S and VCPT, the HTTP server is not usable until the SSL certificates and other required SSL files are created and deployed.

Before AMT and VCPT can be used, you need to either deploy your own SSL certificate or deploy a commercial SSL certificate. The procedures that you use are explained in the following sections:

- Using the Cisco VQE Startup Configuration Utility for SSL Certificates, page 2-4
- Creating Your Own Certificate Authority, page 2-7
- Generating and Deploying Your Own SSL Certificates, page 2-8
- Deploying Commercial SSL Certificates, page 2-11

You perform the procedures for deploying CA certificates on the VQE-S hosts and the VCPT hosts. As an alternative if you are setting up the certificates manually, you can create the needed files on one host and copy them to the other hosts.

The Open Source toolkit from the OpenSSL Project collaborative is used to generate, sign, and install your own CA certificates and to generate the Certificate Signing Request for commercial certificates. The Open Source toolkit is installed on the VQE-S and VCPT hosts. For more information on the Open Source toolkit and for documentation on toolkit commands, go to the following URL:

http://www.openssl.org

Using the Cisco VQE Startup Configuration Utility for SSL Certificates

If you use the Cisco VQE Startup Configuration Utility, the utility allows you to choose different ways to create and deploy SSL certificates:

- Option 1: The Cisco VQE Startup Configuration Utility creates and deploys a self-signed SSL certificate (vqe.cert), private key (server.key), and stackedChain.pem file.

  For an explanation of the tasks involved with using Option 1, see the "Step-by-Step Example: VQE Startup Configuration Utility's Option 1 for Preparing SSL Certificates" section on page 2-5.

- Option 2: The Cisco VQE Startup Configuration Utility generates only a Certificate Signing Request file (server.csr).
  - The VQE Startup Configuration Utility creates the Certificate Signing Request file in the /etc/opt/certs directory.
  - You sign the Certificate Signing Request as described one of the following sections:
  - If you are signing the Certificate Signing Request with a self-created certificate authority, see the "Signing the Certificate Signing Request" section on page 2-9.
  - If you are submitting the Certificate Signing Request to a commercial CA for signing, see the "Deploying Commercial SSL Certificates" section on page 2-11. You can omit the first step in this section (generating a Certificate Signing Request) as the VQE Startup Configuration Utility does this for you.
  - You install the certificates, private key, and keystore as described in the "Installing the Certificates, Private Key, and Keystore" section on page 2-10.

- Option 3: You manually deploy SSL certificates. Follow the directions in these sections for the needed information.
  - For overview information of the SSL tasks, see the "Setting Up SSL Certificates" section on page 2-4.
  - For deploying your own SSL certificates, see the "Creating Your Own Certificate Authority" section on page 2-7 and the "Generating and Deploying Your Own SSL Certificates" section on page 2-8.
  - For deploying commercial SSL certificates, see the "Deploying Commercial SSL Certificates" section on page 2-11.

Step-by-Step Example: VQE Startup Configuration Utility's Option 1 for Preparing SSL Certificates

This section provides a step-by-step example of the tasks that you perform when you choose Option 1 for SSL certificates preparation with the VQE Startup Configuration Utility. With Option 1, the utility creates and deploys a self-signed SSL certificate (vqe.cert), private key (server.key), and stackedChain.pem file on the CDE110 server.

To use the VQE Startup Configuration Utility to create and deploy self-signed SSL certificates, do the following:

Step 1 On the CDE110 hosting VQE-S, when the VQE Startup Configuration Utility runs and displays "Prepare SSL certificate for HTTPS service," select Option 1 to create a self-signed SSL certificate.

```
Prepare SSL certificate for HTTPS service. Choose from following options:

1. Generate a self-signed SSL certificate and deploy now. You will need to manually copy
the certificate to the trusted VCPT host later and import it into its truststore.
2. Generate a certificate signing request and proceed. No SSL certificate will be
deployed, you will need to sign the generated CSR file externally and manually deploy it.
3. Skip this step now and manually deploy SSL certificate later. Refer to VQE-S User's
Guide for instructions. VCPT host will not be able to push SDP configurations to VQE-S
without SSL certificate in place.
```

```
Please enter your choice: [1|2|3]  1
Generating a 2048 bit RSA private key
...
```

The utility creates these files in the /etc/opt/certs directory:

- Server certificate file (vqe.cert)
- Private key file (server.key)
- stackedChain.pem file

The VQE Startup Configuration Utility continues to execute until the initial configuration is completed. Finish the initial system configuration and verification of the CDE110 hosting VQE-S before performing the next step.

Step 2 On the CDE110 hosting VCPT, when the VQE Startup Configuration Utility runs and displays "Prepare SSL certificate for HTTPS service," select Option 1 to create a self-signed SSL certificate.

```
Prepare SSL certificate for HTTPS service. Choose from following options:

1. Generate a self-signed SSL certificate and deploy now. You will need to manually copy
the certificate to the trusted VCPT host later and import it into its truststore.
2. Generate a certificate signing request and proceed. No SSL certificate will be
deployed, you will need to sign the generated CSR file externally and manually deploy it.
3. Skip this step now and manually deploy SSL certificate later. Refer to VQE-S User's
Guide for instructions. VCPT host will not be able to push SDP configurations to VQE-S
without SSL certificate in place.

Please enter your choice: [1|2|3]  1
Generating a 2048 bit RSA private key
...
```

The utility creates these files in the /etc/opt/certs directory:

- Server certificate file (vqe.cert)
- Private key file (server.key)
- stackedChain.pem file

An empty trustedca file is also created in the /etc/opt/certs directory. This file will be used on the VCPT host.

The VQE Startup Configuration Utility continues to execute until the initial configuration is completed. Finish the initial system configuration and verification of the CDE110 hosting VCPT before performing the next step.

Step 3 On the CDE110 hosting VCPT, copy the /etc/opt/certs/vqe.cert file from the VQE-S host to /etc/opt/certs/vqe.cert on the VCPT host. Use an appropriate Linux command (for example, **scp**) for the copy operation.

Step 4 On the CDE110 hosting VCPT, use the **keytool** command to create the keystore (trustedca) file. For example:

```
$ cd /etc/opt/certs
$ keytool -import -keystore trustedca -alias vqe1 -file vqe.cert
```

Note The vqe.cert file that was copied from the VQE-S host is specified in the **-file** argument when invoking the **keytool** command.

When **keytool** runs, it asks for a keystore password (enter any arbitrary password you want) and asks if you trust this certificate (answer yes).

The trustedca file, where **keytool** writes it output, is used only on the VCPT host and must be located in the /etc/opt/certs directory.

Step 5 On the VQE-S and VCPT hosts, restart the httpd daemon by logging in as root and stopping and restarting the httpd service as follows:

```
[root@system]# service httpd restart
```

Step 6 After the VQE-S and VCPT hosts are configured and VQE services are started, you can verify that the SSL certificates are created and deployed correctly by doing the following:

Note HTTPS must be used to access VQE-S AMT and VCPT.

a. To verify that VQE-S AMT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE-S:

`https://ip_address_of_VQES_host`

The VQE-S Application Monitoring Tool login screen should be displayed.

b. To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VCPT:

`https://ip_address_of_VCPT_host`

The VQE Channel Provisioning Tool login screen should be displayed.

c. To verify that VCPT is able to send channel information to VQE-S, use VCPT to define channels, and one or more VQE Servers with the needed channel associations. (The VQE Servers have SSL certificates deployed.) Then use VCPT to send the channel information to the VQE Servers.

The send operation should be successful if the SSL certificates were created and deployed correctly.

Creating Your Own Certificate Authority

Note This task is *not needed* if you are using certificates *that are signed by a commercial CA*.

This task to create your own certificate authority (CA) is only performed once for all instances of VQE-S and VCPT. The CA that you create can be used to sign server certificates on all CDE110 servers hosting VQE-S or VCPT.

To create a CA certificate, follow these steps:

Step 1 Log in using a valid Linux username and password.

Step 2 To generate an encrypted RSA private key, issue the following command:

```
$ openssl genrsa -des3 -out ca.key 4096
```

The command prompts you to enter a pass phrase to protect the private key. The pass phrase will be needed every time this CA signs a certificate request.

The **openssl genrsa** command saves the ca.key file in your current working directory.

The generated key is a 4096-bit RSA key, which is encrypted using Triple-DES and stored in PEM format so that it is readable as ASCII text.

Step 3 To generate the CA certificate, issue the following command:

```
$ openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

The command prompts for the following X.509 attributes of the certificate. It is recommended that you provide valid input for X.509 information. Use a period (.) to indicate blank input.

- Country Name—The country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- State or Province—The state or province where your company resides. Spell out the state completely (for example, California). Do not abbreviate the state or province name.
- Locality or City—The city or town where your company resides (for example, Berkeley).
- Company—Your company's name (for example, XYZ Corporation). If your company or department name has an &, @, or any other symbol that requires using the Shift key in its name, you must spell out the symbol or omit it to enroll.
- Organizational Unit—The organization within the company. This field is optional but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press Enter.
- Common Name—The Common Name is the host plus the domain name (for example, www.company.com or company.com).

The **openssl req** command saves the ca.crt file in your current working directory.

Generating and Deploying Your Own SSL Certificates

When you act as your own certificate authority, you can sign multiple Certificate Signing Requests for the VQE-S hosts and the VCPT hosts. Generating and deploying your own SSL certificates involves three tasks:

1. Generate a Certificate Signing Request.
2. Sign the Certificate Signing Request.
3. Install the certificates, private key, and keystore.

These tasks are explained in the following three sections. *We recommend that these tasks be repeated for each CDE110 host so that there is a unique set of files generated for each host.* You can create the needed sets of files on one host and copy them to the other hosts.

Generating a Certificate Signing Request

To generate a Certificate Signing Request, follow these steps:

Step 1 To generate a server private key, issue the following command:

```
$ openssl genrsa -des3 -out server.key 1024
```

To bypass the pass-phrase requirement, omit the **-des3** option when generating the private key. Bypassing the pass phrase is desirable when you want the Apache web server to be autostarted without human intervention. Otherwise, someone must enter a pass phrase on every restart.

The **openssl genrsa** command saves the server.key file in your current working directory.

Note We recommend that access to the Cisco CDE110 host be restricted so that only authorized server administrators can access or read the private key file.

Step 2 To generate the Certificate Signing Request (CSR), issue the following command:

```
$ openssl req -new -key server.key -out server.csr
```

The command prompts for the same X.509 attributes that were specified when you created your CA certificate in the "Creating Your Own Certificate Authority" section on page 2-7. It is recommended that you provide valid input for X.509 information. Use a period (.) to indicate blank input.

Note The Common Name (CN) of the CA and the server certificates *should not match* or else a naming collision occurs and you get errors when the certificates are used.

The **openssl req** command saves the server.csr file in your current working directory.

The command creates a public/private key pair. The private key (server.key) is stored locally on the server machine and is used for decryption. The public portion, in the form of a Certificate Signing Request (server.csr), is used for certificate enrollment with the CA.

Tip If you are creating Certificate Signing Requests for multiple VQE-S or VCPT hosts and want to reuse most of the X.509 attributes, you can save the information to a file (openssl.cnf) and pass the information to the **openssl req** command by specifying **-config openssl.cnf** on the command line.

Signing the Certificate Signing Request

The Certificate Signing Request (CSR) can be signed by commercial CA entities, such as VeriSign, or by your own CA as created in the "Creating Your Own Certificate Authority" section on page 2-7.

Note If you will use a self-created (non-commercial) CA, signing the Certificate Signing Request must be done *on the same CDE110 server* where the CA was created.

We recommend that the system time of each CDE110 be synchronized with Network Time Protocol (NTP). The system time when the signing of the Certificate Signing Request occurs must be later than the system time when the CA was created.

To sign the Certificate Signing Request with the self-created certificate authority, issue the following command:

```
$ openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01
-out server.crt
```

The **openssl x509** command saves server.crt in your current working directory.

In the example above, the serial number of the signed server certificate is set to 01. *Each time you execute this command, you must change the serial number, especially if you sign another certificate before a previously-signed certificate is expired.*

Installing the Certificates, Private Key, and Keystore

The certificate needs to be in a certain format and reside in a designated directory to be used by the VQE Server-related or the VCPT-related software.

To install the server and CA certificates, the private key and the keystore, follow these steps:

Step 1 To create a "stacked PEM" file, concatenate the contents of the server certificate file (server.crt) and all CA certificate files (ca.crt) in the CA chain to a file named stackedChain.pem. The safest way to create the stackedChain.pem file is to use the Linux **cat** command. For example:

```
$ cat server.crt ca.crt > stackedChain.pem
```

Note Using a text editor and a cut-and-paste operation to concatenate the server and CA certificates can produce *unusable results* because the text editor may add extraneous characters.

The stackedChain.pem file content must be in this order:

```
-----BEGIN CERTIFICATE-----
<SSL Server Cert Contents>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<CA Cert Contents>
-----END CERTIFICATE-----
```

The stackedChain.pem file looks something like the following:

```
-----BEGIN CERTIFICATE-----
MIIDvjCCAaYCAQEwDQYJKoZIhvcNAQEFBQAwZTELMAkGA1UEBhMCVVMxDTALBgNV
... Omitted contents ...
/kzgDk5wO1CbTwuxPIY1piy0Os1Q5EWk3VVAmv4tNMT9bANeKDUiVyYyOi1NIiHA
36w=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGGDCCBACgAwIBAgIJAPtvlrCRokk4MA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
... Omitted contents ...
KV+sxNECGE40iWIvd1dXDA1O34qhAwkVD6/bxw==
-----END CERTIFICATE-----
```

Note If you are creating stackedChain.pem files for multiple VQE-S or VCPT hosts, the server.crt file should be different for each host.

Step 2 For VCPT only, to create a trust-store file for the SSL Java client, issue the following command:

```
$ keytool -import -keystore trustedca -alias rootca -file ca.crt
```

The CA certificate (ca.crt) specified in the **-file** argument is the CA certificate that you created in the "Creating Your Own Certificate Authority" section on page 2-7.

The **keytool** command creates a new keystore with the CA certificate. The resulting file is named trustedca.

Step 3 Do one of the following:

- On a VQE-S host, copy the following files to the directory /etc/opt/certs:
  - server.key
  - stackedChain.pem

- On a VCPT host, copy the following files to the directory /etc/opt/certs:
  - server.key
  - stackedChain.pem
  - trustedca

Deploying Commercial SSL Certificates

As an alternative to acting as your own certificate authority (CA), commercial certificate authorities, such as VeriSign, can issue and sign Secure Sockets Layer (SSL) certificates.

Deploying a commercial certificate involves these steps:

1. Generate a Certificate Signing Request. See the "Generating a Certificate Signing Request" section on page 2-8.
2. Submit the Certificate Signing Request to the commercial CA for signing.
3. Install the certificates, private key, and keystore. See the "Commercial CA: Installing the Certificates, Private Key, and Keystore" section that follows.

Commercial CA: Installing the Certificates, Private Key, and Keystore

When you get the signed certificates back from the commercial CA, you need to install them and the private key and keystore.

To install the certificates, private key, and keystore, follow these steps:

Step 1 To create a "stacked PEM" file, concatenate the contents of the server certificate file (server.crt) and all CA certificate files (ca.crt) in the CA chain to a file named stackedChain.pem. The safest way to create the stackedChain.pem file is to use the Linux **cat** command. For example:

```
$ cat server.crt ca.crt > stackedChain.pem
```

Note Using a text editor and a cut-and-paste operation to concatenate the server and CA certificates can produce *unusable results* because the text editor may add extraneous characters.

The stackedChain.pem file content must be in this order:

```
-----BEGIN CERTIFICATE-----
<SSL Server Cert Contents>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<CA Cert Contents>
-----END CERTIFICATE-----
```

The stackedChain.pem file looks something like the following:

```
-----BEGIN CERTIFICATE-----
MIIDvjCCAaYCAQEwDQYJKoZIhvcNAQEFBQAwZTELMAkGA1UEBhMCVVMxDTALBgNV
... Omitted contents ...
/kzgDk5wO1CbTwuxPIY1piy0Os1Q5EWk3VVAmv4tNMT9bANeKDUiVyYyOi1NIiHA
36w=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

```
MIIGGDCCBACgAwIBAgIJAPtvlrCRokk4MA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
... Omitted contents ...
KV+sxNECGE40iWIvd1dXDA1O34qhAwkVD6/bxw==
-----END CERTIFICATE-----
```

Note If you are creating stackedChain.pem files for multiple VQE-S or VCPT hosts, the server.crt file should be different for each host.

Step 2 For VCPT only, to create a trust-store file for the SSL Java client, issue the following command:

```
$ keytool -import -keystore trustedca -alias rootca -file ca.crt
```

The CA certificate (ca.crt) specified in the **-file** argument is the commercial CA certificate that you get from the vendor.

The **keytool** command creates a new keystore with the CA certificate. The resulting file is named trustedca.

Step 3 Do one of the following:

- On a VQE-S host, copy the following files to the directory /etc/opt/certs:
  - server.key
  - stackedChain.pem
- On a VCPT host, copy the following files to the directory /etc/opt/certs:
  - server.key
  - stackedChain.pem
  - trustedca

VQE-S Server: Routing Configuration Overview

For a VQE-S server, the VQE Startup Configuration Utility supports two routing types: static routes and OSPF routing. This section provides overview information on how you can configure static routes or OSPF routing on a VQE-S server. It includes these topics:

At initial system startup, the VQE Startup Configuration Utility can be used to configure static routes or Open Shortest Path First (OSPF) routing. After initial system startup, the VQE Configuration Tool can be used to modify the routing implementation.

Types of Routes on a VQE-S Server

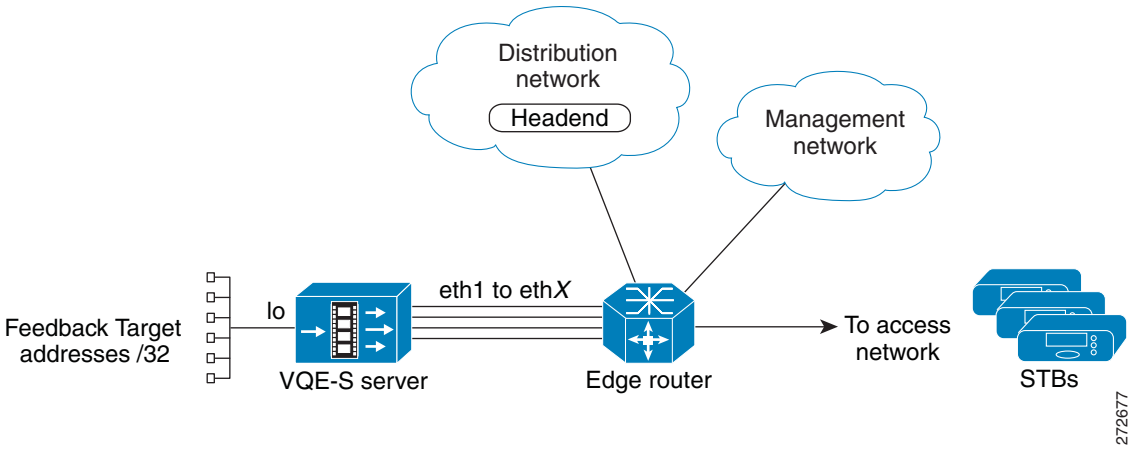
On the VQE-S server, three types of routes are used:

- Management route—A route on the VQE-S server through a directly attached edge router to the management network, where the VQE-S management applications, such as AMT and VCPT, reside.
- Access routes—Routes on the VQE-S server through a directly attached edge router to the access network, where the VQE Clients on the set-top boxes live.
- Feedback target routes—Routes on a directly attached edge router to the VQE-S server that advertise reachability of the VQE-S feedback targets (FBTs) into the access network, where the set-top boxes reside. Each FBT is associated with a channel. VQE Clients on the set-top boxes send requests for Unicast Retransmission and Rapid Channel Change services to the feedback target addresses. VQE-S configures each channel's FBT address as a host address on the VQE-S server loopback interface.

The VQE-S also joins the multicast RTP streams from the distribution network. This interaction is between the VQE-S server and the edge router. It takes place through the use of IGMP joins and does not involve routing with the local routing daemon on the VQE-S server. This interaction is outside the scope of this discussion.

Figure 2-1 shows the types of routes used on a VQE-S server.

Figure 2-1 Routes Used on a VQE-S Server



Static Routes on a VQE-S Server

Prior to Cisco VQE, Release 3.1, the routes on a VQE-S server were configured using static routes. Though static routes can still be chosen as the routing type, the use of static routes for the access routes and feedback target routes has some limitations.

For the access routes, use of static routes requires that the VQE-S server be configured for the static routes to the access network. In contrast, with OSPF routing, the edge router advertises a default route to the access network through a routing protocol, allowing load balancing across the VQE-S interfaces and not requiring an extra configuration step.

For the feedback target routes, the use of static routes on the edge router means that repair services on the VQE-S for all feedback targets are assumed to always be available as long as the VQE-S interfaces are up. In some cases, although the interfaces are up, the VQE-S may not be able to handle requests for one or more feedback targets. The VQE-S itself can not add or withdraw the routes as services become available or unavailable for particular feedback targets. Another limitation of the use of static routes for

feedback targets is that it requires the customer to take the extra step of configuring the edge router for feedback target addresses. In the worst case, this approach can require that each feedback target have a separate static route configured on the router if the feedback target addresses are not summarizable.

For information on static route configuration on the edge router, see the "For Static Routes: Guidance for Configuring Feedback Targets on the Attached Router" section on page 2-34.

OSPF Routing on a VQE-S Server

Starting with Release 3.1, Cisco VQE supports a dynamic routing feature, which uses OSPF, on the VQE-S server. The use of OSPF routing eliminates the limitations of static routing, which are described in the preceding section, "Static Routes on a VQE-S Server". Specifically, OSPF routing can be used on the VQE-S for the following:

- To learn routes to the access network out the VQE-S interfaces to the edge router
- To advertise feedback target routes to the edge router and access network

With dynamic routing, the feedback target routes can be advertised based on the actual capabilities of the VQE-S to process requests for services sent to those targets by adding and removing feedback target routes as needed.

On the VQE-S server, the Quagga routing package provides the OSPF routing capability. The VQE Startup Configuration Utility and the VQE Configuration Tool simplify the OSPF configuration on the VQE-S server. After you enter values for OSPF configuration parameters, such as the OSPF area and router ID, these tools perform the configuration tasks for you. For information on the OSPF configuration parameters for the VQE-S server, see the "OSPF Configuration (VQE-S Host Only)" section on page 2-20.

For information on OSPF configuration on the edge router, see the "For OSPF Routing: Guidance for Configuring the Attached Router" section on page 2-32.

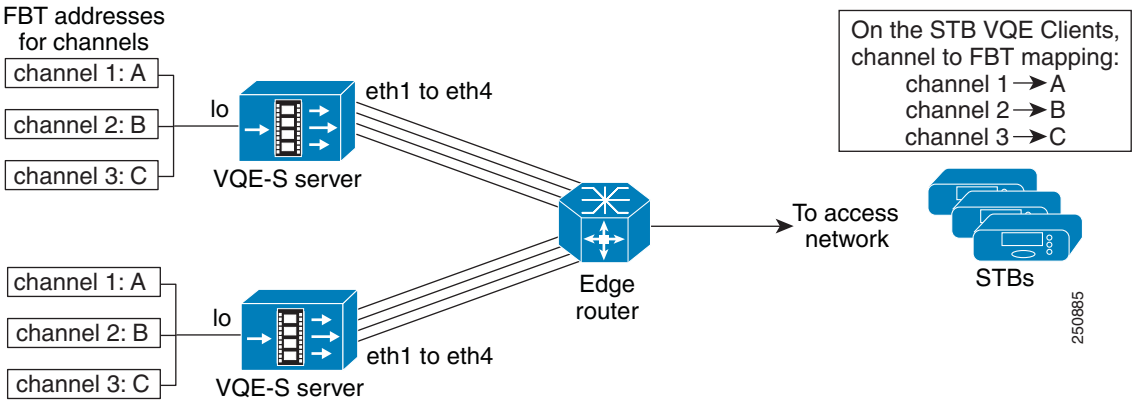
Load Balancing and Redundancy with Multiple VQE-S Servers

When more than one VQE-S server provides Unicast Retransmission and Rapid Channel Change or both services for a set of channels, the VQE-S servers and edge router can load balance the requests from VQE Clients on the set-top boxes and provide failover protection if a VQE-S server fails.

In the VCPT channel definition, each channel is associated with a unique feedback target (FBT) IP address. The VQE Clients on the set-top boxes use the FBT addresses to request Unicast Retransmission and RCC services for a particular channel. The FBT address is a unique IP anycast address that VQE Server configures on its host Cisco CDE110 based on the channel information that is sent to it by VCPT or another channel-provisioning server. An *anycast address* is a unicast address that is assigned to multiple interfaces. With the appropriate routing topology, packets addressed to an anycast address are delivered to a single interface (in this case, the nearest VQE Server's Ethernet interface that is identified by the address).

The use of anycast IP addresses and Equal Cost Multipath (ECMP) routing allows multiple VQE Servers in a single facility to balance the load among themselves and to provide failover protection in case of a server failure. As an example, Figure 2-2 shows a redundant pair of VQE-S servers, each providing Unicast Retransmission and RCC services for the same set of three channels. On both VQE-S servers, each channel is defined to have the same anycast IP address: A for channel 1, B for channel 2, and C for channel 3.

Figure 2-2 Redundant VQE-S Servers for Service Failover and Load Balancing



When OSPF routing is configured on the VQE-S servers, the FBT routes are advertised from the VQE-S to the edge router. In this example, both VQE-S servers advertise FBT routes for a particular channel. If the services for that channel become unavailable on one VQE-S, that VQE-S withdraws the route. This allows the other VQE-S to take over services for that channel. If one VQE-S server fails, the second VQE-S server services the requests directed to the three feedback target addresses.

With OSPF routing and ECMP on the edge router, the router uses multi-interface load splitting on different interfaces with equal cost paths. ECMP provides load balancing of output traffic on the edge router interfaces that are attached to the VQE-S traffic interfaces on the CDE110 server. If three Ethernet interfaces on each of the two VQE-S servers were configured for VQE-S traffic, the edge router would load balance set-top box requests for VQE-S services over the six available Ethernet interfaces.

VQE Tools Server: Routing Configuration Overview

On the VQE Tools server, the following routes are used:

- Management route—A route on the VQE Tools server through an edge router to the management network.
- External access—Proper route configuration is needed to provide external access to the VQE Tools server. This access allows VQE Client Channel Configuration Delivery Server (VCDS) to send channel information to the VQE Clients on the set-top boxes and for VCPT to send channel information to each VQE-S.

The VQE Tools server uses one or more static routes to the management network. The static route to the management network can also be used to provide the external access. The VQE Startup Configuration Utility and VQE Configuration Tool can be used to configure one or more static routes.

Using the VQE Startup Configuration Utility

The Cisco VQE Startup Configuration Utility runs automatically the first time you log in to a CDE110 server. The CDE110 server has the VQE software pre-installed. The utility is available on the CDE110 that hosts VQE-S and on the CDE110 that hosts VQE Tools. We recommend that you use the VQE Startup Configuration Utility rather than try to do the initial configuration manually because the utility simplifies your work and is known to produce correct results.

Caution The Cisco VQE Startup Configuration Utility runs once the first time a CDE110 boots normally. Do *not* attempt to use the utility a second time because this will produce incorrect and unpredictable results.

Before using the VQE Startup Configuration Utility, do the following so that you understand how the startup configuration utility works and what information you need to collect before powering on the VQE-S or VCPT server:

- Read the "VQE-S Server: Routing Configuration Overview" section on page 2-12.
- Read the "VQE Tools Server: Routing Configuration Overview" section on page 2-15.
- Read the "Configuration Parameters" section on page 2-16.
- Complete the "Pre-Configuration Worksheets" section on page 2-22.
- Read the "VQE Startup Configuration Utility Root Menu" section on page 2-25.

When it is started, the VQE Startup Configuration Utility displays the following choices:

```
Please choose one of the following:
1) I have all the information needed and want to proceed.
2) I do not have all the information and want to shutdown the system.
3) Skip configuration wizard and directly enter the system.
```

If you select choice 1, the VQE Startup Configuration Utility begins prompting you for configuration values.

If you select choice 2, the system is shutdown. The next time the system is started the VQE Startup Configuration Utility is launched.

After you finish entering configuration values, the VQE Startup Configuration Utility displays the Root Menu. The Root Menu allows you to view the values that you have specified and to change values that are not correct.

After using the VQE Startup Configuration Utility, perform the verification tasks in the following sections:

- On the VQE-S Host: Verifying Status of VQE and System Services, page 2-27
- On the VQE Tools Host: Verifying Status of VQE and System Services, page 2-29

Configuration Parameters

This section provides information on the configuration parameters present in the VQE Startup Configuration Utility. Before using the VQE Startup Configuration Utility, read the descriptions of the configuration parameters in this section.

Tip For many configuration parameters, you will need to gather some information prior to booting the CDE110 for the first time and using the VQE Startup Configuration Utility. The worksheets in the "Pre-Configuration Worksheets" section on page 2-22 may be helpful in organizing the information.

In the explanations that follow, these conventions are used for the configuration parameters:

- For the parameters that are for a VQE-S host only, *VQE -S Host Only* appears in parentheses after the item name.
- For optional parameters, *Optional* appears in parentheses after the item name.

Note To not enter data for an optional item, press **Enter** without entering any data at the VQE Startup Configuration Utility prompt.

Passwords for root and the vqe User IDs

The password for root is set when the CDE110 boots normally for the first time (when you log in as root) and before the VQE Startup Configuration Utility executes.

The vqe username is a predefined Linux user ID that the system administrator can use to log in to VQE-S AMT and VCPT.

The root and vqe user passwords have the following requirements: A valid password should be a mix of uppercase and lowercase letters, digits, and other characters. You can use an eight-character long password with characters from at least three of these four classes, or a seven-character long password containing characters from all the classes. An uppercase letter that begins the password and a digit that ends it do not count towards the number of character classes used.

The password can be a passphrase. A passphrase should be at least three words with a combined total length of 12 to 40 characters.

Hostname for the CDE110

The hostname is used in multiple Linux configuration files. Allowed range is 3 to 200 characters.

Domain Name System (DNS) IP Addresses and a Search Domain

The IP addresses of one or more DNS servers and an optional search domain. Allowed range for the search domain is 3 to 200 characters.

System Timezone

The timezone and current system time that will be used for this CDE110. The VQE Startup Configuration Utility prompts for the needed information.

NTP Server IP Addresses

The IP addresses of one or more Network Time Protocol (NTP) servers.

Note We recommend that the system time of each CDE110 be synchronized with NTP. Problems (for example, with Session Description Protocol [SDP] updates) can occur if the server time is not synchronized with NTP.

Current System Time

The current system time that will be used for this CDE110. The VQE Startup Configuration Utility prompts for the needed information.

SNMP Read-only Community String, Location, Contact, and Trap-Listener IP Addresses or Hostnames (Optional)

If your deployment will use SNMP, you specify the following:

- Read-only community string—Password for read-only access to the VQE-S or VQE Tools server
- Location information—Physical location of the VQE-S or VQE Tools server
- Contact information—Username of a contact person who has management information for the CDE110 server

- Trap listeners—IP addresses or fully qualified hostnames of the management hosts that will receive the SNMP messages

For more information on SNMP for the CDE110, see Appendix B, "Using Net-SNMP."

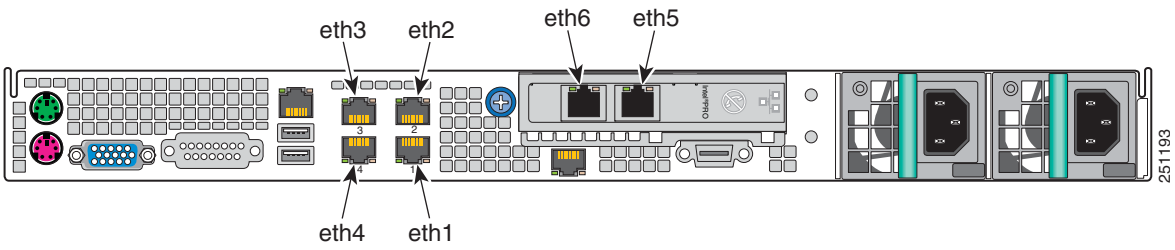
Ethernet Interface Configurations IP Addresses and Prefix Lengths

For one or more of the Ethernet ports on the Cisco CDE110, you specify an IP address and prefix length (for example, 1.2.3.4/32). The Ethernet ports are named eth1 to eth6 as shown in Figure 2-3.

Note Earlier models of the CDE110 have four Ethernet ports (eth1 to eth4). These models did not have the Intel PRO/1000 PT Dual Port Server Adapter that provides the eth5 and eth6 ports.

- On a VQE-S host, up to six Ethernet interfaces are typically configured and used for incoming multicast streams, outgoing Unicast Retransmissions, and other VQE-S traffic.
- On a VQE Tools host, at least one Ethernet interface is typically configured and used for VCPT and VQE Client Channel Configuration Delivery Server (VCDS) traffic.
- Optionally on both the VQE-S host and VQE Tools host, one Ethernet interface may be used for a management network, that interface *should be included* in the set for which you provide IP addresses and prefix lengths.

Figure 2-3 Ethernet Port Numbering for Software Configuration



IP Address and Prefix Length and Gateway Address for a Static Route to a Management Network (Optional)

Note If you configure a static route for a management network using the VQE Startup Configuration Utility, see "Static Route for a Management Network Is Missing on CDE110 Hosting VQE-S or VQE Tools" section on page 5-7 for some important additional information.

If your deployment will make use of a management network, the VQE Startup Configuration Utility can configure static routes to the management network. You specify the following:

- Management subnet IP address and prefix length for the management network. The following example shows the allowed format for the subnet IP address and prefix length:

  10.1.0.0/16

- Gateway (next hop) IP address of the interface on the router that is directly attached to the CDE110 Ethernet interface that will be used for the management network.

As an example of gateway (next hop) IP address, if Ethernet interface eth4 were used for the management network, you would specify the IP address of the router interface that is directly attached to eth4.

Note On the VQE Tools server, proper route configuration is needed for external access to the VQE Tools server. You can use the static management route created by this parameter to configure this access.

SSL Certificates Options

Secure Sockets Layer (SSL) certificates must be created and deployed for VQE-S AMT or VCPT to be accessed using HTTPS. The VQE Startup Configuration Utility gives you three options for creating and deploying the certificates. For information on the three options and using the utility for creating and deploying SSL certificates, see the "Using the Cisco VQE Startup Configuration Utility for SSL Certificates" section on page 2-4.

Trusted Provisioning Clients

The use of this parameter varies depending on the VQE server type:

- For a VQE Server host, if your IPTV deployment will use VCPT or another channel-provisioning server to send channel information to the VQE Servers, you specify the IP addresses of the trusted channel-provisioning servers. If VCPT is the channel-provisioning server, the IP addresses of all Ethernet interfaces (that have been assigned IP addresses) on the VCPT host must be configured as trusted HTTPS clients on the VQE-S host.
- For a VQE Tools host where a VCDS receives channel information from VCPT, *all Ethernet interfaces* (that have been assigned IP addresses) on the VCPT host sending the channel information must be specified as addresses in Trusted Provisioning Client(s). This requirement applies even when the VCDS is in the same VQE Tools server as the VCPT.
- For a VQE Tools host, if a VQE-C system configuration provisioning server sends network configuration information to the VCDS, you specify the IP address of the trusted VQE-C system configuration provisioning server. This type of provisioning server is not currently used in most deployments.

This parameter is for enhanced communications security beyond HTTPS. The VQE-S server or VQE Tools server is configured so that only trusted HTTPS clients (as specified in the Trusted Provisioning Client(s) parameter) can send information to, respectively, the VQE-S server or VQE Tools server using HTTPS.

VQE-S Traffic Routing Type (VQE-S Host Only)

Specifies whether static routes or OSPF routing will be used as the routing type for VQE-S traffic.

- If static routes are chosen, the VQE-S host is configured for one or more default gateway (next hop) router interfaces. See the "Default Gateway IP Addresses for Multipath Static Routes (VQE-S Host Only)" section on page 2-19.
- If OSPF routing is chosen, the set of OSPF parameters can be configured. For descriptions of these OSPF configuration parameters, see the "OSPF Configuration (VQE-S Host Only)" section on page 2-20.

For information about routing on the VQE-S host, see the "VQE-S Server: Routing Configuration Overview" section on page 2-12.

Default Gateway IP Addresses for Multipath Static Routes (VQE-S Host Only)

If static routes are chosen as the routing type, you specify the IP addresses for the interfaces on the router that is directly attached to the VQE-S host. Specify as many gateway (next hop) router interfaces as are reachable through the CDE110 Ethernet interfaces that have been configured with an IP address and prefix length.

Note If one Ethernet interface is used for a management network, that interface *should not be included* in the set for which gateway router interfaces are specified.

VQE-S uses Equal Cost Multipath (ECMP) to load-balance its output traffic across all the gateway router interfaces that are specified. If a default route (the gateway IP address) is configured for each Ethernet interface that is available to VQE-S for Unicast Retransmissions, RCC, and other VQE-S traffic, ECMP load balances output traffic across all of the listed gateway interfaces.

For more information on ECMP configuration, see the "Configuring Static Routes for VQE-S Traffic" section on page D-6.

OSPF Configuration (VQE-S Host Only)

If OSPF is chosen as the routing type, Table 2-1 describes the parameters that can be configured. For detailed information on the OSPF parameters, see the following Quagga documentation:

http://www.quagga.net/docs/quagga.pdf

Table 2-1 OSPF Parameters

Parameter	Description
Area Type	Type for the OSPF area that the VQE-S traffic interfaces and feedback target host addresses will reside in. You can choose either normal or nssa (Not So Stubby Area). If no value is specified, the default value is normal.
Area ID	Integer ID value for the OSPF area that the VQE-S Ethernet interfaces and feedback target addresses will reside in. If no value is specified, the default value is 0. Allowed range is 0 to to 4,294,967,295.
Router ID	IP address used as the router ID to uniquely identify the VQE-S server in the OSPF network. The router ID must not be the same as the IP address of one of the CDE110 Ethernet interfaces because the router ID will be added as an internal address to the loopback interface.
Enable MD5	Specifies whether Message Digest 5 (MD5) authentication is enabled on the Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, specifying an MD5 key and MD5 key ID are required.
MD5 Key	If MD5 authentication is enabled, specifies a key (a string) that will be configured for all Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, an MD5 key and MD5 key ID are required. Allowed length for the string is 1 to 16 characters.
MD5 Key ID	If MD5 authentication is enabled, specifies an MD5 key ID (an integer) that will be used for all Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, an MD5 key and MD5 key ID are required. Allowed range of integer values is 1 to 255.

Table 2-1 OSPF Parameters (continued)

Parameter	Description
Hello Interval	Interval (in seconds) at which OSPF Hello packets are sent. This value must be the same for all interfaces running OSPF in the network. The hello interval will be set for all VQE-S interfaces running OSPF. If no value is specified, the default value is 10. Allowed range is 1 to 65,535.
Dead Interval	OSPF dead interval (in seconds). The dead interval is the maximum amount of time allowed to receive a Hello packet from a neighbor before that neighbor is declared down. This value must be the same for all interfaces running OSPF in the network. The dead interval will be set for all VQE-S interfaces running OSPF. If no value is specified, the default value is 40. Allowed range is 1 to 65,535.

Ethernet Interfaces That Will Be Used for VQE-S Traffic (VQE-S Host Only)

You specify which of the CDE110 Ethernet interfaces will be available for VQE-S traffic. The interface names are eth1 to eth6.

Note If one Ethernet interface is used for a management network, that interface *should not be included* as one of the interfaces that will be available for VQE-S traffic.

Automatic Start of VQE Services on a Reboot

After you finish specifying values for the configuration items, the VQE Startup Configuration Utility displays the following menu:

```
VQE Configuration Tool Root Menu:

     1) System Parameters
     2) Network Parameters
     3) Configure VQE Password
     4) Generate SSL Certificate
     5) VQE-S Parameters
     S) Save/Apply and reboot system

Enter your choice:
```

When you have completed the configuration items, you choose `S) Save/Apply and reboot system`. The VQE Startup Configuration Utility saves your configuration in the VCDB file, applies the VCDB values to the configuration files under /etc, and reboots the CDE110 system. Each time the VQE-S or VQE Tools host reboots, the services listed in Table 2-2 and Table 2-3 will be started.

Table 2-2 VQE-S and System Services for CDE110 That Hosts VQE-S

Service	Description
vqes	The VQE-S service (process_monitor process) starts and monitors the other VQE-S processes—Control Plane, Data Plane, Multicast Load Balancer, and STUN Server.
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.

Table 2-2 VQE-S and System Services for CDE110 That Hosts VQE-S (continued)

Service	Description
snmpsa	(Optional) The SNMP subagent.
ntpd	(Optional) The NTP daemon.
check_daemons	A script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a **cron** job owned by root.
	If OSPF is selected as the routing type
watchquagga	The Quagga watchdog process. If the ospfd or zebra daemon crashes or hangs, watchquagga restarts it automatically.
ospfd	The OSPF daemon.
zebra	The zebra daemon.

Table 2-3 VCDS and System Services for CDE110 That Hosts VQE Tools

Service	Description
vcds	VQE Client Channel Configuration Delivery Server (VCDS) service
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.
snmpsa	(Optional) The SNMP subagent.
ntpd	(Optional) The NTP daemon.
check_daemons	A script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a **cron** job owned by root.

Note On the VQE Tools host, VCPT is a web application and has no dedicated processes associated with it. The processes needed for the VCPT web application to work (for example, the web server) are started automatically when the Cisco CDE110 is started.

Pre-Configuration Worksheets

Before using the VQE Startup Configuration Utility, complete the pre-configuration worksheets in Table 2-4 for a VQE-S host and Table 2-5 for a VQE Tools host before the first normal boot. The use of a VQE Tools server and VCPT is optional.

For information on the configuration items in Table 2-4 and Table 2-5, see the "Configuration Parameters" section on page 2-16.

Table 2-4 VQE-S CDE110: Pre-Configuration Worksheet

Configuration Item	Value for Your Deployment
Password for root	
Password for the vqe username (a pre-defined Linux user ID)	
Hostname of the CDE110 for VQE-S	
Domain Name System (DNS) IP addresses and a search domain	DNS IP address: DNS IP address: Search domain:
System timezone	
NTP server IP addresses	
SNMP read-only community string Location for SNMP Contact for SNMP SNMP trap-listener IP addresses or hostnames	community string: location: contact: IP addresses or hostnames:
Ethernet interface configurations (IP address and prefix lengths)	eth1: eth2: eth3: eth4: eth5: eth6:
For static routes for a management network—subnet IP address and prefix length, and gateway (next hop) IP address	IP address and prefix length: Gateway (next hop) IP address:
SSL certificate option	
Trusted provisioning clients IP addresses	
Routing type (static or ospf)	
If static is chosen as the routing type, default gateway (next hop) IP addresses for multipath static routes	IP addresses:

Table 2-4 VQE-S CDE110: Pre-Configuration Worksheet (continued)

Configuration Item	Value for Your Deployment
If OSPF is chosen as the routing type, the OSPF parameters required by your networking implementation can be configured.	area type: area ID: router ID: Enable MD5 authentication? MD5 key: MD5 key ID: Hello interval: Dead interval:
Ethernet interface names that will be used for VQE-S traffic	

Table 2-5 VQE Tools CDE110: Pre-Configuration Worksheet

Configuration Item	Value for Your Deployment
Password for root	
Password for the vqe username (a pre-defined Linux user ID)	
Hostname of the CDE110 for VCPT	
Domain Name System (DNS) IP addresses and a search domain	DNS IP address: DNS IP address: Search domain:
System timezone	
NTP server IP addresses	
SNMP read-only community string Location for SNMP: Contact for SNMP: SNMP trap-listener IP addresses or hostnames	community string: location: contact: IP addresses or hostnames:

Table 2-5 VQE Tools CDE110: Pre-Configuration Worksheet (continued)

Configuration Item	Value for Your Deployment
Ethernet interface configurations (IP address and mask)	eth1: eth2: eth3: eth4: eth5: eth6:
For static routes for a management network—subnet IP address and prefix length, and gateway (next hop) IP address	IP address and prefix length: Gateway (next hop) IP address:
SSL certificate option	
Trusted provisioning clients IP addresses	

VQE Startup Configuration Utility Root Menu

After you have used the VQE Startup Configuration Utility to specify values for the configuration items, the utility displays the Root Menu. The Root Menu allows you to view the values that you have specified and to change values that are not correct. The Root Menu on a VQE-S server is as follows:

```
VQE Configuration Tool Root Menu:

     1) System Parameters
     2) Network Parameters
     3) Configure VQE Password
     4) Generate SSL Certificate
     5) VQE-S Parameters
     S) Save/Apply and reboot system

Enter your choice:
```

This Root Menu and its behavior are similar to the standard VQE Configuration Tool Root Menu and behavior. The two differences are that the numbered choices 3 and 4 are only present in the VQE Startup Configuration Utility, and the Save/Apply choice in the VQE Startup Configuration Utility includes a reboot of the system.

Note For information on how to use the VQE Configuration Tool Root Menu and the other menu choices, see the "Using the VQE Configuration Tool" section on page 6-4. *The information in the "Using the VQE Configuration Tool" section is applicable to the Root Menu and other menu choices presented at the end of the VQE Startup Configuration Utility.*

The Root Menu choices allow you to do the following:

- View and change the parameter or password values that you have set (choices 1, 2, 3, and 5)
- Generate and deploy SSL certificates (choice 4)
- Save the parameter values to the VQE Configuration Database (VCDB), and apply the values to the VQE-S server or VQE Tools server (choice S)

To view and change parameter values, you can select choices 1, 2, 3, and 5 as many times as you wish.

Note *When you are finished specifying parameter values, you must select choice* `S) Save/Apply and reboot system` to save the parameter values to the VQE Configuration Database (VCDB), and apply the values to the VQE-S server or VQE Tools server.

Table 2-6 provides more information about the choices on the Root Menu. You enter the number or letter for your choice.

Table 2-6 Root Menu Choices (for a VQE -S Server)

Root Menu Choice	Menu Description
1) System Parameters	Allows you to view the current system parameter values that you have set, and to change or set the system parameters values: 1) Hostname 2) DNS Server(s) 3) DNS Search Domain 4) Timezone 5) NTP Server(s) 6) SNMP RO Community String 7) SNMP System Location 8) SNMP System Contact 9) SNMP Trap Listener(s) 10) Trusted Provisioning Client(s)
2) Network Parameters	Allows you to view the current network parameter values that you have set, and to change or set the network parameters values: 1) Eth1 Interface 2) Eth2 Interface 3) Eth3 Interface 4) Eth4 Interface 5) Eth5 Interface 6) Eth6 Interface 7) Management Route(s) 8) VQE-S Traffic Routing Type 9) Static Routing Parameters 10) OSPF Parameters
3) Configure VQE Password	Allows you to set the password for the vqe username. Once you select this menu choice, you must enter the password value even if you choose to keep the current password.
4) Generate SSL Certificate	Allows you to create and deploy a Secure Sockets Layer (SSL) certificate for VQE-S AMT or VCPT, or to generate a Certificate Signing Request file (server.csr).

Table 2-6 Root Menu Choices (for a VQE -S Server) (continued)

Root Menu Choice	Menu Description
5) VQE-S Parameters	Allows you to view the current VQE-S parameter values that you have set, and to change or set the VQE-S parameters values: 1) Log Priority * 2) Excess Bandwidth Fraction * 3) VQE-S Traffic Interfaces * The VQE Startup Configuration Utility does not allow you to set the values of these parameters in the set of parameters that were previously displayed. You can supply values at this point if you want or accept the defaults. For more information on these values, see the vcdb.conf.sample file and Appendix A, "VQE, System, and Network Parameters."
6) Save/Apply and reboot the system	Saves the changes you have made to the parameters in the VQE Configuration Database (VCDB), applies parameter values to the configuration files under /etc, and reboots the CDE110 system.

On the VQE-S Host: Verifying Status of VQE and System Services

After the VQE Startup Configuration Utility finishes and the CDE110 that hosts VQE-S reboots, it is recommended that you perform some quick checks to ensure that VQE and system services are running.

To verify the status of VQE services on the VQE-S host, follow these steps:

Step 1 If needed, log in as root.

Step 2 To verify that the SSH service is running, issue the following command:

```
[root@system]# service sshd status

sshd (pid 21165 21110 20595 20569 2777) is running...
```

Step 3 To verify that the HTTP service is running, issue the following command:

```
[root@system]# service httpd status

httpd (pid 9665 9664 9663 9661 9660 9658 9657 9656 3978) is running...
```

Step 4 To verify that the Tomcat 5 service is running, issue the following command:

```
[root@system]# service tomcat5 status

Tomcat is running...
```

Step 5 If you configured SNMP, to verify that the SNMP service is running, issue the following command:

```
[root@system]# service snmpd status

snmpd (pid 2754) is running...
```

Step 6 If you configured SNMP, to verify that the SNMP subagent service is running, issue the following command:

```
[root@system]# service snmpsa status

The SNMP subagent is running.
```

Step 7 If you enabled OSPF routing, to verify that the three OSPF-related services are running, issue the following commands:

```
[root@system]# service watchquagga status

watchquagga (pid 2513) is running...

[root@system]# service ospfd status

ospfd (pid 7104) is running...

[root@system]# service zebra status

zebra (pid 7072) is running...
```

Step 8 To verify that the VQE-S service is running, issue the following command:

```
[root@system]# service vqes status

process_monitor (pid 21853) is running...
```

Step 9 To check that the VQE-S processes are running, issue the following command:

```
[root@system]# ps -ef | grep vqe

root     17928 17896  0 Jun02 pts/1    00:00:00 tail -f vqe.log
root     21853     1  0 Jun03 ?        00:00:00 /opt/vqes/bin/process_monitor
vqes     21903 21853  0 Jun03 ?        00:00:00 mlb --interface eth1 eth2 eth3 eth4
--xmlrpc-port 8052 --unicast-reservation 20 --ssm --log-level 4
root     21914 21853  0 Jun03 ?       00:00:04 vqes_dp --max-pkts 1000000 --log-level
4 --rtp-inactivity-tmo 300
vqes     21944 21853  0 Jun03 ?        00:00:00 vqes_cp --cp-uid 499 --cp-gid 499
--xmlrpc-port 8051 --cfg /etc/opt/vqes/vqe_channels.cfg --er-cache-time 3000
--rtp-hold-time 100 --client-er-policing --client-er-tb-rate-ratio 5
--client-er-tb-depth 10000 --log-level 4 --rcc-mode conservative
--igmp-join-variability 100 --max-client-bw 0 --max-idr-penalty 0 --rap-interval 2000
--excess-bw-fraction 20 --excess-bw-fraction-high-def 12 --rcc-burst-delay-to-send 10
--rtp-dscp 0 --rtcp-dscp 24
```

In the preceding output, the VQE-S processes to check for are as follows:

- process_monitor—Process Monitor
- stun_server—STUN Server
- mlb—Multicast Load Balancer
- vqes_dp—Data Plane
- vqes_cp—Control Plane

Step 10 Issue the following command to check that the STUN Server process is running:

```
[root@system]# ps -elf | grep stun

4 S vqes     21972 21959  0  75   0 -  3745 322792 Jul15 pts/1    00:00:00 stun_server
--ss-uid 499 --ss-gid 499 --xmlrpc-port 8054 --log-level 4
```

Step 11 If you configured an IP address for an NTP server, to verify that the NTP service is running, issue the following command:

```
[root@system]# service ntpd status

ntpd (pid 2790) is running...
```

Step 12 To use the VQE-S Application Monitoring Tool from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE-S:

```
https://ip_address_of_VQES_host
```

Log in using the vqe username and password. (Any valid Linux username and password can be used to log in to the VQE-S Application Monitoring Tool.)

If you click **System** in the left pane, the VQE-S Application Monitoring Tool displays information on the VQE-S processes and channels. Figure 4-2 on page 4-4 shows an example. Because at this point no channel information has been sent to the VQE-S, no channels will be displayed.

Step 13 Do one of the following:

- If the preceding checks indicate that all is well, you are ready to start using VQE-S and VQE-S AMT. For information, see Chapter 4, "Using the VQE-S Application Monitoring Tool."
- If one of the preceding checks fails, inspect the configuration of the item that failed and make any needed adjustments. You can get more information on VQE-S host configuration in Appendix D, "Manual Initial VQE System Configuration."

On the VQE Tools Host: Verifying Status of VQE and System Services

After the VQE Startup Configuration Utility finishes and the CDE110 that hosts VQE Tools reboots, it is recommended that you perform some quick checks to ensure that VQE and system services are running.

To verify the status of VQE services on the VQE Tools host, follow these steps:

Step 1 If needed, log in as root.

Step 2 To verify that the SSH service is running, issue the following command:

```
[root@system]# service sshd status

sshd (pid 21165 21110 20595 20569 2777) is running...
```

Step 3 To verify that the HTTP service is running, issue the following command:

```
[root@system]# service httpd status

httpd (pid 9665 9664 9663 9661 9660 9658 9657 9656 3978) is running...
```

Step 4 To verify that the Tomcat 5 service is running, issue the following command:

```
[root@system]# service tomcat5 status

Tomcat is running...
```

Step 5 If you configured SNMP, to verify that the SNMP service is running, issue the following command:

```
[root@system]# service snmpd status

snmpd (pid 2754) is running...
```

Step 6 If you configured SNMP, to verify that the SNMP subagent service is running, issue the following command:

```
[root@system]# service snmpsa status

The SNMP subagent is running.
```

Step 7 If you configured an IP address for an NTP server, to verify that the NTP service is running, issue the following command:

```
[root@system]# service ntpd status

ntpd (pid 2790) is running...
```

Step 8 To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VCPT:

```
https://ip_address_of_VCPT_host
```

Log in with a Linux username and password.

If you are able to log in successfully, VCPT is running correctly.

Step 9 Do one of the following:

- If the preceding checks indicate that all is well, you are ready to start using VCPT. For information, see Chapter 3, "Using the VQE Channel Provisioning Tool."
- If one of the preceding checks fails, inspect the configuration of the item that failed and make any needed adjustments. You can get more information on VCPT host configuration in Appendix D, "Manual Initial VQE System Configuration."

Configuring VQE-S RTCP Exporter

VQE-S RTCP Exporter is the VQE-S software component responsible for sending the RTCP reports to an external device that hosts the video-quality monitoring (VQM) application. Use of RTCP Exporter is optional.

To monitor the RTCP Exporter, use the VQE-S Application Monitoring Tool (AMT). This tool displays RTCP Exporter configuration details and status as well as counters of exported packets. The VQE-S Application Monitoring Tool can also be used to enable or disable RTCP Exporter debugging.

To troubleshoot the RTCP Exporter, examine the Exporter syslog messages, which are sent to the VQE-S log file (/var/log/vqe/vqe.log). If more detailed troubleshooting is needed, enable RTCP Exporter debugging using VQE-S AMT and examine the debug messages, which are also sent to the VQE-S log file.

To configure and enable the RTCP Exporter on the Cisco CDE110 that hosts VQE-S, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file and use the **vqe_cfgtool** command.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file and add to the file the three key-value pairs for the RTCP Exporter parameters listed in Table 2-7. Specify values for each of the parameters.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-12. The parameters used for enabling the RTCP Exporter are not available in the VQE Configuration Tool.

Step 3 Save the vcdb.conf file.

Table 2-7 RTCP Exporter Parameters

Parameter	Value Required
vqe.vqes.vqm_host="*IP_addr_or_domain_name*"	IP address or fully qualified Internet domain name of the host on which the VQM application resides. There is no default value.
vqe.vqes.vqm_port="*vqm_port_no*"	TCP port number on which the VQM application listens for video quality data from RTCP Exporter. Allowed range is 1024 to 65535. There is no default value.
vqe.vqes.exporter_enable="*true_or_false*"	Either true or false. The value true enables RTCP exports, and false disables RTCP exports. The default value is false.

RTCP Exporter remains disabled unless both vqe.vqes.vqm_host and vqe.vqes.vqm_port are configured and are valid.

By default, the vcdb.conf file contains no RTCP Exporter parameters and RTCP Exporter is disabled.

Step 4 To apply the RTCP Exporter parameter values to the /etc configuration files and restart VQE-S, issue the following command:

```
[root@system]# vqe_cfgtool -apply
```

For more information on the **vqe_cfgtool** command and the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 6-16.

Note The **vqe_cfgtool** command with **-apply** asks you if you want to restart VQE-S. When RTCP Exporter parameters are added or modified, this restart is required for the new or changed parameter values to take effect.

Configuring Other Parameters for the VQE-S Host

The set of parameters for the VQE-S host includes many parameters that are not configurable with the VQE Startup Configuration Utility. Many additional parameters are used, for example, to make adjustments to the VQE-S software facilities that perform Unicast Retransmission and Rapid Channel Change.

Read the following to get information on these additional parameters:

- Chapter 6, "Configuring VQE Server and VQE Tools" describes the tools and procedures to used to configure all parameters for a VQE-S or VQE Tools system.
- Appendix A, "VQE, System, and Network Parameters" describes the VQE-S, system, and network parameters.

- The file /etc/vqes/vcdb.conf.sample provides additional information on the VQE-S, system, and network parameters.

Configuring the Edge Router for VQE-S

This section provides some guidance on configuring the edge router that will be directly attached to the VQE-S host. Depending on whether OSPF routing or static routes are used on the VQE-S host, refer to one of the following sections:

- For OSPF Routing: Guidance for Configuring the Attached Router, page 2-32
- For Static Routes: Guidance for Configuring Feedback Targets on the Attached Router, page 2-34

For OSPF Routing: Guidance for Configuring the Attached Router

If OSPF routing is used for VQE-S traffic, the following sections provide guidance on configuring the edge router that is directly attached to VQE-S:

- VQE-S in Separate OSPF Area, page 2-32
- VQE-S in Area 0, page 2-33
- General Guidelines, page 2-33

For detailed information on OSPF and the Cisco IOS commands used to configure the routing protocol, see the OSPF resources at:

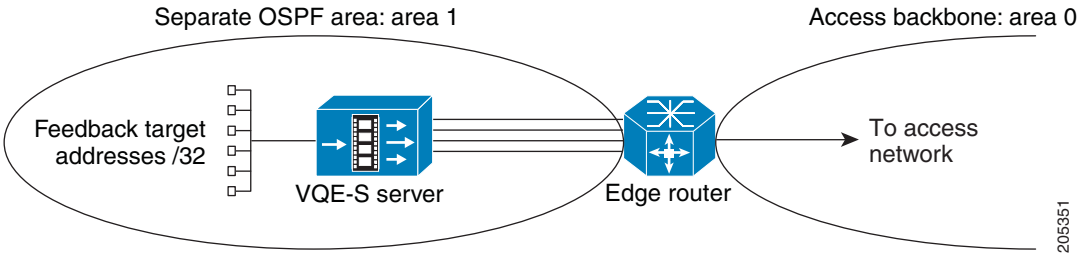
http://www.cisco.com/en/US/tech/tk365/tk480/tsd_technology_support_sub-protocol_home.html

Note In the following sections, Cisco IOS commands are used for some of the configuration examples. However, there is no requirement that a Cisco router be used as the edge router.

VQE-S in Separate OSPF Area

The VQE-S server can be configured to be in a separate OSPF area by specifying the VCDB parameter network.ospf.area to be a non-zero value. With the VQE Startup Configuration Utility or VQE Configuration Tool, this separate area with the VQE-S server can be defined as a normal area or a Not So Stubby Area. Figure 2-4 shows the VQE-S server in a separate OSPF area: area 1.

Figure 2-4 VQE-S Server in a Separate OSPF Area



When the VQE-S server is configured in a separate OSPF area, these guidelines for configuring the directly attached edge router apply:

- Configure the edge router interfaces attached to the VQE-S server in the same OSPF area as the VQE-S host.
- To keep the routing table on the VQE-S server small in size, configure the separate area (in Figure 2-4, area 1) to be a Not So Stubby Area (NSSA). The VQE-S server must also be configured so that its OSPF area type is a NSSA by specifying the VCDB parameter network.ospf.area_type to have the value “nssa”.

With a NSSA, the edge router generates a default route to the access network and advertises the default route in the NSSA (in Figure 2-4, area 1). This default-route mechanism reduces the size of the VQE-S server routing table.

To configure the NSSA and to configure the edge router to advertise the default route in the NSSA, issue the following Cisco IOS commands on the edge router:

router ospf *process-id*
  area *area-id* **nssa no-summary**

When **no-summary** is specified with **area nssa**, the edge router advertises the default route in the NSSA but does not inject summary routes into the area.

VQE-S in Area 0

When the VQE-S server is configured within OSPF area 0 (that is, when the network.ospf.area VCDB parameter value is zero, the default), these guidelines for configuring the directly attached edge router apply:

- Configure the edge router interfaces to the VQE-S host to be within OSPF area 0.
- With this configuration, the VQE-S host routing table may be very large depending on the size of the network visible in area 0. If this is a concern, one suggestion is to configure the VQE-S host interfaces to be in a separate OSPF area, as described in the previous section, “VQE-S in Separate OSPF Area”.

General Guidelines

The following are general edge router configuration guidelines:

- Feedback target routes—The feedback target (FBT) routes that are advertised from the VQE-S to the edge router *should not* be summarized by the edge router if multiple VQE-S servers exist in the network and high availability of VQE-S services is desired. The reason for this is that each FBT route advertises VQE-S services for a particular channel, and if the services for that channel become unavailable on a VQE-S, that VQE-S withdraws the route. This allows another VQE-S in the network to take over services for that channel. However, if the FBT routes are summarized by the edge router, the FBT routes cannot be added and withdrawn individually. Thus redundancy is lost because a VQE-S may still get service requests for a channel that is not available.
- Fast convergence—If fast convergence in the case of link failure or other causes in the network is a concern, set the VCDB parameter network.ospf.hello_interval on the VQE-S server to the lowest possible setting, which is one second. Also, set the same hello interval value for each VQE-S interface on the edge router. This allows a link failure to be detected as quickly as possible between the VQE-S and the edge router. A general rule of thumb when changing the default hello interval is to set the dead interval to be four times the hello interval. Therefore, the VCDB parameter network.ospf.dead_interval should be set to four seconds, and a corresponding change must be made on the edge router for each VQE-S traffic interface. For each interface, the Cisco IOS commands on the edge router are as follows:

interface *name*
ip ospf hello-interval 1
ip ospf dead-interval 4

- Interface authentication—If MD5 authentication is desired between OSPF peers, all VQE-S traffic interfaces *must have the same key value and key ID* when the VCDB parameters network.ospf.md5_key and network.ospf.md5_keyid are set. Therefore, the same MD5 key value and MD5 key ID must be configured on the edge router for all traffic interfaces to the VQE-S.
- VQE-S redundancy—All VQE-S servers in the network must be configured to use the same routing type: either all must be static or all must be ospf. This is required for anycast ECMP across multiple VQE-S servers to work properly.
- Forwarding table—The size of the forwarding table on the edge router may be restricted, which will limit the number of VQE-S servers that can participate in anycast ECMP properly. On a Cisco 7600 router, the size of the forwarding table can be increased to allow more VQE-S servers and more traffic interfaces per VQE-S using the following commands:

  router ospf *process-id*
  maximum-paths *maximum-paths*

- Directly connected VQE-S—The VQE-S server *must be directly connected* to the edge router on all VQE-S traffic interfaces. Specifically, OSPF virtual links are not allowed.
- For information on configuring the edge router to generate and advertise a default route into a Not So Stubby Area, see the "VQE-S in Separate OSPF Area" section on page 2-32.

For Static Routes: Guidance for Configuring Feedback Targets on the Attached Router

When channels are configured with a channel-provisioning tool such as VQE Channel Provisioning Tool, it is required that you specify a unique feedback target (FBT) address for each channel. If static routes are used for VQE-S traffic, the router that is directly attached to the VQE-S host must have a static route configured for the FBT address so that the router can reach the target. If the FBT addresses are allocated within a contiguous address range, this configuration piece can be done with a single aggregated route.

For example, if the FBT addresses for the channels are assigned to be 8.86.1.1, 8.86.1.2, 8.86.1.3, ..., 8.86.1.250, then the single static route 8.86.1.0/24 configured on the directly attached router allows any of these FBT addresses to be reached. The commands on the router for the FBT addresses would be as follows:

```
configure terminal
ip route 8.86.1.0 255.255.255.0 11.2.9.2
ip route 8.86.1.0 255.255.255.0 11.2.10.2
ip route 8.86.1.0 255.255.255.0 11.2.11.2
ip route 8.86.1.0 255.255.255.0 11.2.12.2
```

For the preceding configuration example, the IP addresses 11.2.9.2, 11.2.10.2, 11.2.11.2, and 11.2.12.2 have been assigned to the Ethernet interfaces on the VQE-S host. See Figure D-3 on page D-6. These Ethernet interfaces are used for VQE-S traffic, including Unicast Retransmission and Rapid Channel Change traffic.

CHAPTER 3

Using the VQE Channel Provisioning Tool

This chapter describes how to use Cisco VQE Channel Provisioning Tool (VCPT). The tasks that you perform with VCPT are listed in Table 3-1. When you use VCPT for the first time, the required tasks are performed in the order shown in the table.

Table 3-1 VCPT Tasks

VCPT Task	Section Where Described
1. Log in to VCPT	Logging in to VCPT, page 3-1
2. Create a new VCPT configuration file	Working with VCPT Configuration Files, page 3-2
3. Provision VQE channels	Provisioning VQE Channels, page 3-5
4. Create VQE Servers and VQE Client Channel Configuration Delivery Servers	Defining VQE Servers and VQE Client Channel Configuration Delivery Servers, page 3-12
5. Specify channel associations for the VQE Servers and VQE Client Channel Configuration Delivery Servers	Defining Channel Associations, page 3-16
6. Send the channel information file to the VQE Servers and VQE Client Channel Configuration Delivery Servers	Working with VCPT Configuration Files, page 3-2

Logging in to VCPT

Before logging in to VCPT, you need a valid UNIX username and password on the Cisco CDE110 hosting VCPT. The username does not have to belong to any special group. Creation of the username is the responsibility of the Cisco CDE110 system administrator.

VCPT supports two web browsers: Microsoft Internet Explorer version 6.0 or later, and Mozilla Firefox version 2.0 or later. VCPT uses secure HTTPS. The minimum screen resolution required for VCPT is 1024 x 768 pixels.

To log in to VCPT, follow these steps:

Step 1 Point your web browser to the Cisco CDE110 that hosts VCPT using an IP address or fully qualified domain name:

```
https://ip_address
```

or

```
https://fully_qualified_domain_name
```

The VQE login dialog box is displayed.

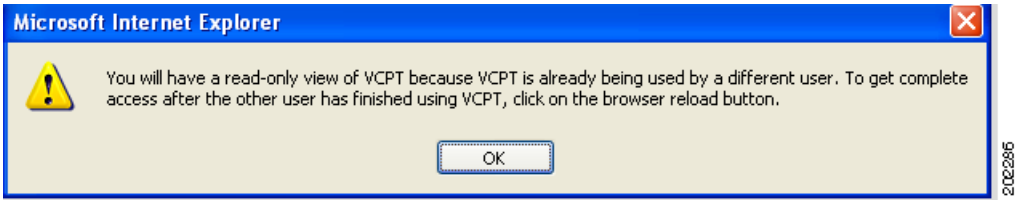
Step 2 Enter a UNIX username and password.

Step 3 Click **OK**.

If the username and password are valid, the VQE Channel Provisioning Tool main window is displayed.

If you log in to VCPT when another person is using the same VCPT, the message shown in Figure 3-1 is displayed and your access to VCPT is a read-only view. To get read-write access, wait and try to open a VCPT session at a later time when no one else is using the tool.

Figure 3-1 Read-only View Message



With certain versions of Microsoft Internet Explorer 6, if you close a read-write session and try to open it again immediately, you get a read-only view. In this case, wait a minute and open another session to get read-write access.

When you are finished using VCPT, click the **Logout** button on the right side of the banner so that another user can get read-write access to the tool.

VCPT sessions are timed out after 25 minutes of inactivity. If VCPT detects a network failure or server failure, the session is timed out after one minute.

Working with VCPT Configuration Files

The VCPT channel, server, and association provisioning information is stored in a persistent local database on the Cisco CDE110 server. When the Cisco CDE110 or VCPT is restarted, channel, server, and association data are read from the local database. The VCPT configuration file can be saved at any time and should be saved frequently to store your work.

Caution If a VCPT session times out because of inactivity or because of a server or network failure, unsaved data is lost. Therefore, you should save the VCPT configuration file frequently.

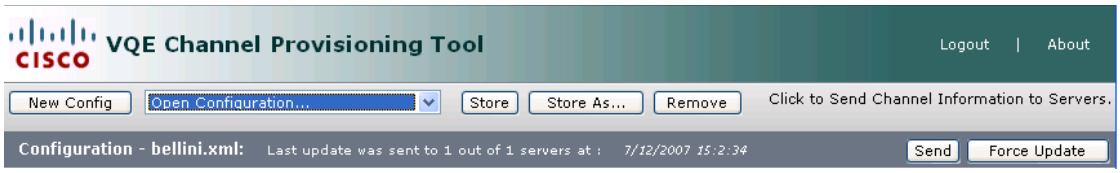
VCPT configuration files are stored in the /etc/opt/vcpt/data directory on the Cisco CDE110. File management tasks for VCPT are the responsibility of the VCPT user.

Caution The VCPT configuration files must be backed up in a safe location that is not on the local Cisco CDE110 disk. If a server or software failure occurs, the latest VCPT configuration file must be retrievable from the backup location.

When the user completes channel and server configuration and initiates the VCPT send operation, VCPT sends the channel information in Session Description Protocol (SDP) format to the set of VQE Servers and VQE Client Channel Configuration Delivery Servers.

Figure 3-2 shows the buttons that you use for working with VCPT configuration files and for sending channel information.

Figure 3-2 VCPT Configuration File Operations



The following sections explain the configuration file and channel information operations:

- Performing Non-Push Configuration-File Operations, page 3-3
- Sending or Pushing Channel Information to Servers, page 3-4
- Sending Channel Information to a Subset of Servers, page 3-5

Performing Non-Push Configuration-File Operations

The VCPT configuration file buttons used for non-push operations are:

- **New Config**—Clears the current configuration (if any) so that you can start a new one. The new configuration is not saved until you click **Store**, specify a file name, and click **OK**.
- **Open Configuration**—Allows you to choose an existing configuration file from the pull-down menu and open it. If needed, you should save the current configuration file before opening another one because any unsaved data in the current configuration file is lost.
- **Store**—Saves the current configuration file on the Cisco CDE110 that hosts VCPT.
- **Store As**—Saves the current file under a new file name that you specify.
- **Delete**—Deletes the current configuration file and clears the configuration.

When the current VCPT configuration is changed but the changes have not been saved, an asterisk is displayed beside the configuration filename (for example, bellini.xml*).

Names for VCPT Configuration Files

The name for a VCPT configuration file can be up to 60 characters long and use lowercase a to z, uppercase A to Z, numeric characters 0 to 9, and the underscore (_), hyphen (-) and period (.) characters. No spaces are allowed in the name.

Sending or Pushing Channel Information to Servers

The VCPT buttons used to send or push channel information to VQE Servers and VQE Client Channel Configuration Delivery Servers are the **Send** and **Force Update** buttons.

Send Button

Use the **Send** button to send channel information in the current configuration file to the VQE Servers and VQE Client Channel Configuration Delivery Servers that have been defined.

Note Use the **Send** button for "normal" configuration file changes where the changes modify the base file that was most recently pushed to the servers.

Note Using the **Send** button causes temporary disruption to Unicast Retransmission services *for modified channels* while the VQE-S cache used for packet retransmission on the modified channels is flushed.

The channel information to send is based on the channel associations that have been defined for the VQE Servers and VQE Client Channel Configuration Delivery Servers. When channel information is sent to a set of servers, VCPT saves the current configuration file. The send operation does not succeed if any channel has misconfiguration issues. When channel information is sent to servers, VCPT displays the following:

- The status line next to the configuration file name is updated (for example, `Last update was sent to 1 out of 2 servers at: 5/11/2007 14:47:20`).
- A status message is displayed: either "Send Complete" or, if the send operation fails, the message text shown in Figure 3-3.
- On the Servers tab, the Status of Last Send column is updated with information on the send operation. For a description of the status values that can appear in this column, see the "Viewing or Updating Server Information" section on page 3-15.

You can get more details on a send failure by examining the VCPT log file, which is located in /usr/share/tomcat5/logs/vcpt.log.

Figure 3-3 Status Message for Failed Send Operation

Force Update Button

Note Using the **Force Update** button causes temporary disruption to Unicast Retransmission and Rapid Channel Change? services *for all channels* while the VQE-S cache used for packet retransmission is flushed.

For the following types of configuration file changes, use the **Force Update** button to send the channel information to the VQE Servers and VQE Client Channel Configuration Delivery Servers.

- Configuration file changes where you are reverting to an old version of the configuration file (older that the most recently pushed configuration file)
- Configuration file changes where the changes modify some file other than the base file that was most recently pushed to the servers
- Configuration file changes when you are not certain whether the file used was the base file that was most recently pushed to the servers

If configuration information is sent to the servers and the changes to channel information are not present on the servers after the send, you can use the **Force Update** button to force the channel information changes to be accomplished on the servers.

Sending Channel Information to a Subset of Servers

To send a channel information file to a subset of servers, follow these steps:

Step 1 Open an existing VCPT configuration file that has the needed server, channel, and association information.

Step 2 Click **Save As** to save the VCPT configuration file *using a new file name*.

Step 3 On the Servers tab, adjust the servers list by deleting the VQE Servers and VQE Client Channel Configuration Delivery Servers that are not wanted.

Step 4 Click **Store** to save the VCPT configuration file.

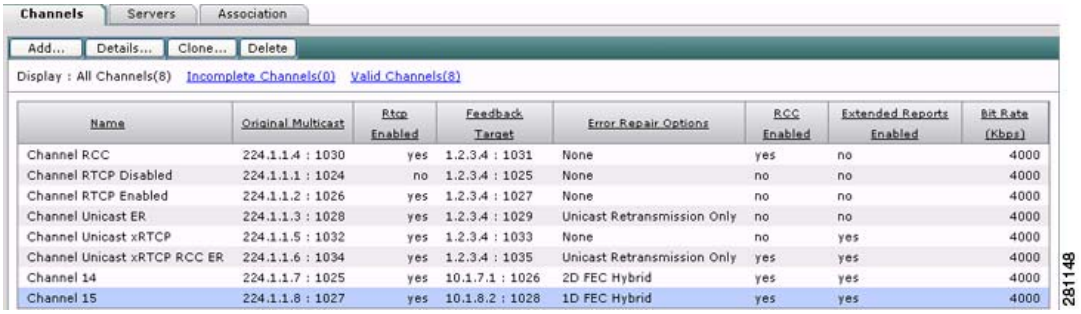
Step 5 Click **Send** to send the channel information file to the adjusted list of VQE Servers and VQE Client Channel Configuration Delivery Servers.

Provisioning VQE Channels

In the Cisco VQE Channel Provisioning Tool, use the Channels tab to add a new channel, clone an existing channel, delete an existing channel, and get detailed information on an existing channel. The number of channels supported by single VQE Server is determined by the ingest capacity of the CDE110 server. Currently, the CDE110 provides 1 Gbps of ingest bandwidth. In practical terms, the number of channels currently supported by a single VQE Server is, for example, approximately 500 channels at 2 Mbs each, or 250 channels at 4 Mbs each.

When you click the Channels tab, VCPT displays summary information (Figure 3-4) on all channels that have been created. An incomplete channel is displayed in red.

Figure 3-4 Channels Summary



Name	Original Multicast	Rtcp Enabled	Feedback Target	Error Repair Options	RCC Enabled	Extended Reports Enabled	Bit Rate (Kbps)
Channel RCC	224.1.1.4 : 1030	yes	1.2.3.4 : 1031	None	yes	no	4000
Channel RTCP Disabled	224.1.1.1 : 1024	no	1.2.3.4 : 1025	None	no	no	4000
Channel RTCP Enabled	224.1.1.2 : 1026	yes	1.2.3.4 : 1027	None	no	no	4000
Channel Unicast ER	224.1.1.3 : 1028	yes	1.2.3.4 : 1029	Unicast Retransmission Only	no	no	4000
Channel Unicast xRTCP	224.1.1.5 : 1032	yes	1.2.3.4 : 1033	None	no	yes	4000
Channel Unicast xRTCP RCC ER	224.1.1.6 : 1034	yes	1.2.3.4 : 1035	Unicast Retransmission Only	yes	yes	4000
Channel 14	224.1.1.7 : 1025	yes	10.1.7.1 : 1026	2D FEC Hybrid	yes	yes	4000
Channel 15	224.1.1.8 : 1027	yes	10.1.8.2 : 1028	1D FEC Hybrid	yes	yes	4000

From the Channels tab, you can do the following:

- Click **Incomplete Channels** or **Valid Channels** to display only the corresponding subsets of channels.
- Click a column heading to reorder the channels in the list. For example, clicking **Feedback Target** orders the entries by feedback target: the combination of IP address and RTCP port number.
- Double-click any item in a channel's row to display the full details for the channel in a new window. You can update the channel information.
- Click **Add** to display a dialog box so that you can create a new channel.
- Click a channel to select it and then use one of the following buttons:
  - **Details**—Displays a dialog box with detailed information on an existing channel and allows you to update the information.
  - **Clone**—Displays a dialog box with appropriate cloned information from an existing channel so that you can use the information to create a new channel.
  - **Delete**—Deletes an existing channel.

On the Channels summary, the Error Repair Options column indicates the types of repair (see Table 3-2) that have been configured for the channel.

Table 3-2 Error Repair Options

Option	Description
None	No Error Repair
Unicast Retransmission Only	VQE-S provides selective retransmission of dropped IPTV packets to repair errors.
1-D FEC Only	VQE-C provides 1-dimension FEC.
2-D FEC Only	VQE-C provides 2-dimension FEC.
1-D FEC Hybrid	Unicast retransmission and 1-dimension FEC are provided.
2-D FEC Hybrid	Unicast retransmission and 2-dimension FEC are provided.

The sections that follow provide more information on the tasks that can be performed from the Channels tab.

Adding a Channel

In the VCPT channel definition, each channel is associated with a unique feedback target (FBT) IP address. The feedback target address is a unique IP anycast address that VQE Server configures on its host Cisco CDE110 based on the channel information that is sent to it by VCPT.An anycast address is a unicast address that is assigned to multiple interfaces. With the appropriate routing topology, packets addressed to an anycast address are delivered to a single interface (in this case, the nearest VQE Server's CDE110 interface that is identified by the address). The use of anycast addresses to identify feedback targets is useful for VQE Server redundancy.

Note When channels are configured with VCPT, it is required that you specify a unique feedback target (FBT) address for each channel. *The router that is directly attached to the VQE-S host must have a static route configured for the FBT address so that the router can reach the target.*

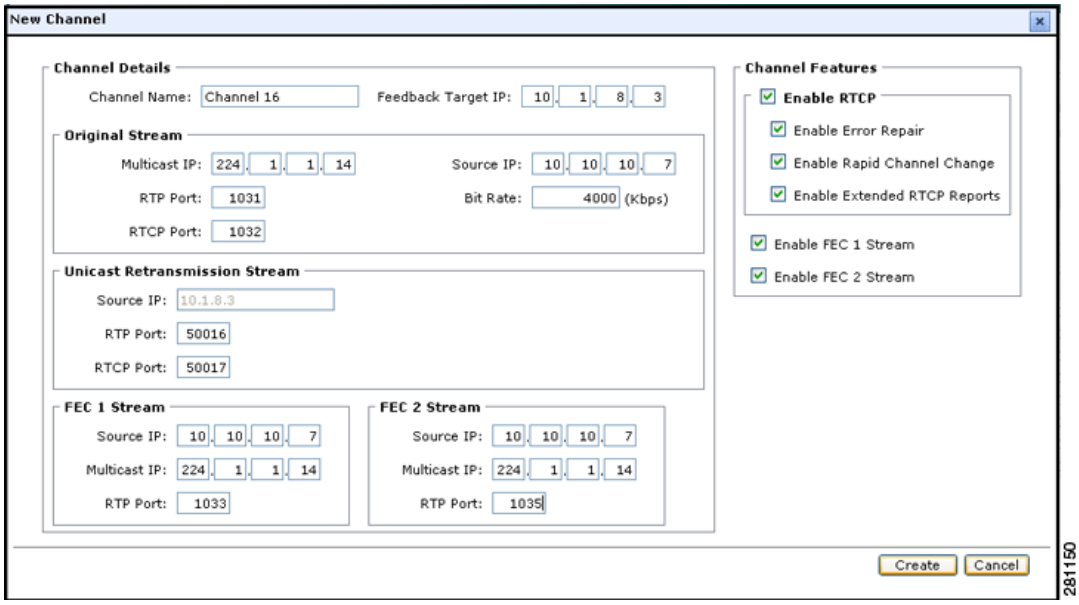
For information on configuring the FBT IP addresses on the router that is attached to the CDE110 hosting VQE-S, see "Configuring OSPF Routing for VQE-S Traffic" section on page D-8.

To add a channel, follow these steps:

Step 1 On the Channels tab, click **Add**.

The New Channel dialog box (Figure 3-5) is displayed.

Figure 3-5 New Channel Dialog Box



Step 2 Fill in the information for the new channel. Table 3-3 has information on the fields that you need to complete.

Table 3-3 VQE Channel Details

VCPT Field	Description
Channel Name	String having 1 to 40 alphanumeric characters.
Feedback Target IP	A unique anycast IP address on the VQE Servers that provide services for this channel. Using the Feedback Target IP address that is sent to it by VCPT in the channel information, VQE Server automatically configures the specified address on one of its Cisco CDE110 interfaces.
Channel Features	
Enable RTCP	RTCP must be enabled to use Error Repair (Unicast Retransmission), Rapid Channel Change, Video-Quality Monitoring (RTCP Exporter and RTCP Extended Reports), or to have VQE-S display video-monitoring statistics. If Enable RTCP is not checked, the Enable Error Repair, Enable Rapid Channel Change, and Enable RTCP Extended Reports check boxes are greyed out.
Enable Error Repair	Check to enable Error Repair (Unicast Retransmission). You also need to complete the Unicast Retransmission Stream fields.
Enable Rapid Channel Change	Check to enable Rapid Channel Change.
Enable Extended RTCP Reports	Check to enable RTCP Extended Reports.
Enable FEC 1 Stream	Check to enable 1-dimension FEC. You also need to complete the FEC 1 Stream fields.
Enable FEC 2 Stream	Check to enable 2-dimension FEC. You also need to complete the FEC 2 Stream fields.
Original Stream	
Multicast IP	Multicast IP address for the channel's original source stream. The first octet must be within the range of a valid multicast address. The multicast address must be unique for each channel.
RTP Port	RTP port number of the channel's original source stream.
RTCP Port	The RTCP port number of the channel's original source stream. By default, RTCP Port is the (RTP/UDP) port number plus one.
Source IP	IP address of the channel's original source stream.
Bit Rate	Bit rate of the channel's original source stream in Kbits per second. This parameter defines how many packets VQE Server will accept and send for this multicast stream. **Note** The specified bit rate should be equal to the primary stream bandwidth but *should not* include bandwidth used for FEC.
Unicast Retransmission Stream	
Source IP	IP address of the Unicast Retransmission stream. The IP address must be the same as is defined for Feedback Target IP.
RTP Port	RTP port number of the unicast retransmission stream. By default, RTP Port is a valid port number.

Table 3-3 VQE Channel Details (continued)

VCPT Field	Description
RTCP Port	RTCP port number of the unicast retransmission stream. By default, RTCP Port is a valid port number.
FEC 1 Stream and FEC 2 Stream	
Source IP	IP address of the channel's source stream. By default, this is the IP address of the Source IP specified for the Original Stream.
Multicast IP	IP address of the channel's multicast stream. By default, this is the IP address of the Multicast IP specified for the Original Stream.
RTP Port	RTP port number of the FEC stream. The port number specified cannot be the same as the port number used for the RTP or RTCP port for the Original Stream.

Rules When Adding a Channel. The following rules apply when adding a channel:

- The Feedback Target IP address must be unique for each channel.
- For the Original Stream, the Multicast IP address must be unique for each channel. That is, the address cannot be used by another channel as its Original Stream Multicast IP address.
- For the Original Stream, the Source IP address must not be equal to the Feedback Target IP address.
- The FEC 1 Stream and FEC 2 Stream RTP port numbers cannot be the same as the port numbers used for the Original Stream RTP or RTCP ports.
- In any given stream, the RTP port number must not be equal to the RTCP port number.
- Configuring a FEC 1 Stream or a FEC 2 Stream provides 1-dimension FEC for the channel.
- Configuring a FEC 1 Stream and a FEC 2 Stream provides 2-dimension FEC for the channel.
- If you enter invalid data, the field name is displayed in red. You must correct the invalid data before creating or updating the channel.
- If you enter incomplete data, you can create or update the channel, but it will be marked incomplete.
- A channel configuration file with an incomplete channel definition cannot be sent to VQE Servers or VQE Client Channel Configuration Delivery Servers.

Port Usage Recommendations. When the STUN Server is enabled on a VQE-S server (the default and recommended mode), one set of four unique port numbers can be used for all channels for the following:

- Original Source RTP Port
- Original Source RTCP Port
- Unicast Retransmission Stream RTP Port
- Unicast Retransmission Stream RTCP Port

Note If the STUN Server is not enabled, each channel must be configured with unique port numbers for the each of the preceding items. The STUN server is not enabled only when no set-top boxes being serviced by VQE-S are behind NAT devices.

Step 3 When you have specified all required values, click **Create** to create the new channel, or click **Cancel** to exit the dialog box without creating the new channel.

Viewing or Updating Channel Information

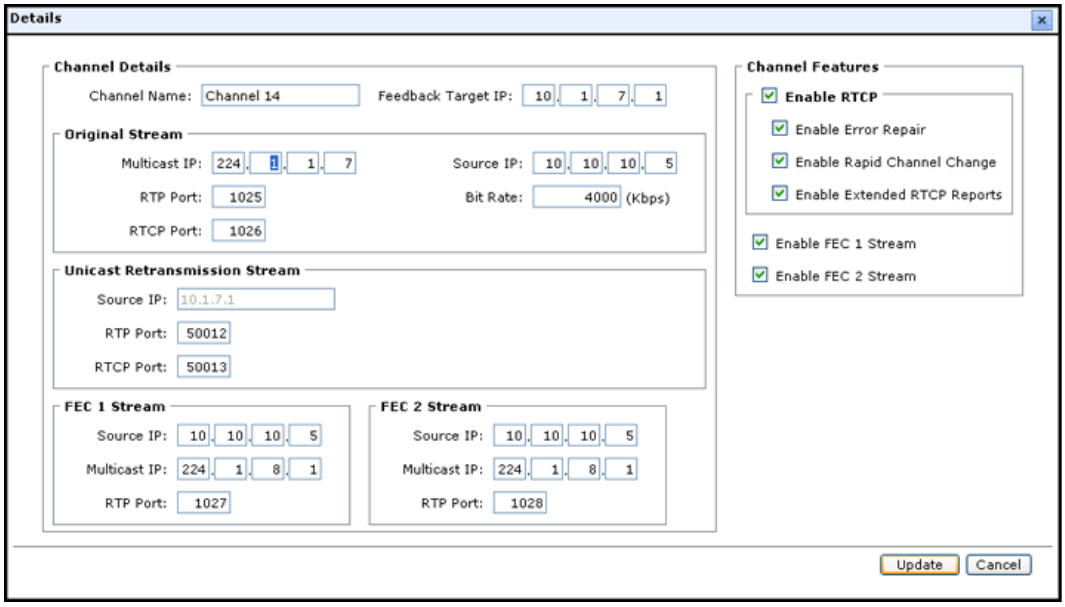
To view or update channel information, follow these steps:

Step 1 On the Channels tab, click the channel you want to view or update.

Step 2 Click **Details**.

The Details dialog box (Figure 3-6) is displayed.

Figure 3-6 Details Dialog Box



Step 3 If needed, change or add channel information.

Step 4 Do one of the following:

- Click **Update** to update the channel information.
- Click **Cancel** to close the dialog box without updating the channel information.

Cloning a Channel

To clone a channel, follow these steps:

Step 1 On the Channels tab, click the channel you want to clone.

Step 2 Click **Clone**.

The Clone dialog box is displayed. Only appropriate information from the existing channel is cloned.

Step 3 Verify that the cloned values are what you require. Where needed, change the values and add channel information where that is required.

Step 4 Do one of the following:

- Click **Create** to create the new channel.
- Click **Cancel** to close the dialog box without creating the new channel.

Deleting a Channel

To delete a channel, follow these steps:

Step 1 On the Channels tab, click the channel you want to delete.

Step 2 Click **Delete**.

A dialog box asking if you want to delete the channel is displayed.

Step 3 Do one of the following:

- Click **Delete** to delete the channel.
- Click **Cancel** to close the dialog box without deleting the channel.

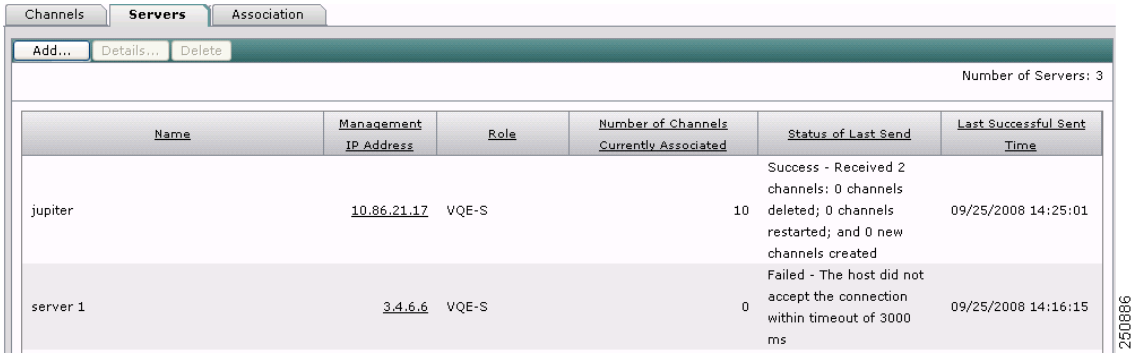
Step 4 If you clicked Delete, a confirmation dialog box is displayed. Click **OK**.

Defining VQE Servers and VQE Client Channel Configuration Delivery Servers

The Cisco VQE Channel Provisioning Tool requires that you provide information on each VQE Server and each VQE Client Channel Configuration Delivery Server that will receive channel configuration information from the VQE Channel Provisioning Tool.

In the VQE Channel Provisioning Tool, use the Servers tab to add a new server, delete an existing server, and get information on an existing server. When you click the Servers tab, VCPT displays summary information (Figure 3-7) on all servers that have been created.

Figure 3-7 Servers Summary



From the Servers tab, you can do the following:

- Click a column heading to reorder the servers in the list. For example, clicking **Status of Last Send** orders the servers by their channel configuration file status.
- Double-click any item in a server's row to display the full details for the server in a new window. You can update the server information.
- Click **Add** to display a dialog box so that you can create a new server.
- Click a channel to select it and then use one of the following buttons:
  - **Details**—Displays a dialog box with detailed information on an existing server and allows you to update the information.
  - **Delete**—Deletes an existing server.

On the Servers tab, the following columns provide useful information on the servers.

- The Number of Channels Currently Associated column shows how many channels are currently associated with a server in the current configuration—whether or not that configuration has been saved. If the current channel information in VCPT has not been sent to the server, the Number of Channels Currently Associated can be different from the number shown as "Received" in the Status of Last Send Column.
- The Status of Last Send column provides information on the last attempt by VCPT to send channel configuration information to the server. Table 3-4 lists the possible messages. The result will either be Success or Failed plus some additional information. The following examples explain some of the additional information that can be provided in the Status of Last Send column.

  ```
  Success - Received 4 channels: 0 channels deleted; 1 channels restarted; and 0 new
  channels created
  ```

The preceding Success status indicates the send operation succeeded: A VQE Server received four channel definitions; zero channels were deleted; one channel definition was modified and the channel was restarted; zero new channels were created.

```
Failed - 0 out of 4 channels failed to validate; 1 channels having the old version;
and 0 channels having the same version but contents being changed
```

The preceding Failed status indicates the send operation failed: all channel definitions have valid SDP format; one channel definition is an older version of the channel; zero channels have the same version (when compared to the VQE Server or VCPT server's current version) but with a changed channel definition.

Note The "channels having the same version but contents being changed" error condition is present only when the SDP definition for the channels has been incorrectly coded by manual modifications or by a channel-provisioning tool other than VCPT.

Table 3-4 Status of Last Send Messages

Message	Explanation
Success - *additional_information*	The send operation succeeded, and *additional_information* provides details on the send operation.
Failed - *additional_information*	The send operation failed, and *additional_information* provides details on the reasons for the failure.
Failed - Network Error	VCPT did not receive any error message back from VQE-S or VQE Client Channel Configuration Delivery Server.
Failed - Connection refused	See the "Channel-Provisioning Server Cannot Send Channel Information to VQE Server: Trusted Provisioning Client(s) Problem" section on page 5-12.
Failed - Unable to find valid certification path to requested target	See the "Channel-Provisioning Server Cannot Send Channel Information to VQE Server: SSL Certificates Problems" section on page 5-12.
Failed - Unable to connect with Server	See the "Unable to Connect Error When VCPT Tries to Send Channel Information" section on page 5-13.
Failed - Security Exception	An exception occurred while VCPT was authenticating the server SSL certificate.
Failed - Invalid EMS Address	Incorrect server URL format
Failed - VCPT Server Error	A generic internal VCPT coding error has occurred. This may be because of a coding bug or because VCPT failed to read a file.
Failed - Channel config file is not writable	The channel configuration file could not be written to disk on the VQE-S or VQE Client Channel Configuration Delivery Server host.
Failed - File failed to open	VQE-S or VQE Client Channel Configuration Delivery Server could not open the channel configuration file.
Failed - Tomcat Service Unavailable	The Tomcat application server has failed on the VCPT host.

Table 3-4 Status of Last Send Messages (continued)

Message	Explanation
Failed - Unable to store the SDP data on VCPT Server	The SDP data could not be generated or saved on the VCPT host.
Failed - VCPT:AMT IO Exception: Connection Refused	VCPT was not able to deliver the channel configuration information. One possible cause of the failure is that VQE services were not running on the server to which the information was sent.

- The Status of Last Send Time column shows the date and time of the last successful send operation for this server, or shows "None." None indicates one of the following:
  - That the server is new and channel information has never been successfully sent to it
  - That the VCPT configuration file that is currently open is from a previous version of VQE

The sections that follow provide more information on the tasks that can be performed from the Servers tab.

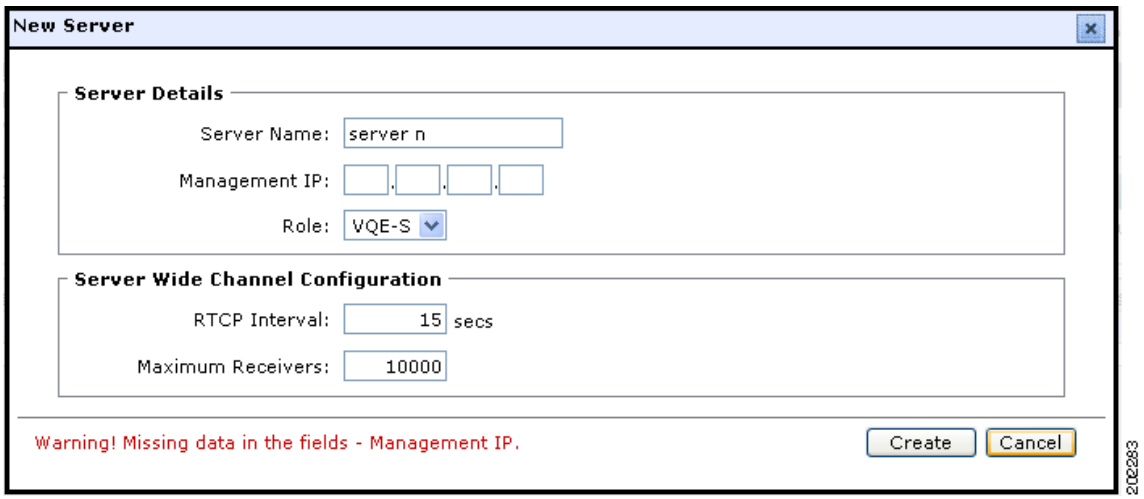
Adding a Server

To add a server, follow these steps:

Step 1 On the Servers tab, click **Add**.

The New Server dialog box (Figure 3-8) is displayed.

Figure 3-8 New Server Dialog Box



Step 2 Fill in the information for the new server. For descriptions of the fields that you need to fill in, see Table 3-5.

Table 3-5 VQE Server and VQE Client Channel Configuration Delivery Server Information

VCPT Field	Description
Server Details	
Server Name	String having 1 to 40 alphanumeric characters.
Management IP	IP address of an Ethernet interface on the server's Cisco CDE110.
Role	One of the following: • VQE-S (VQE Server) • VCDS (VQE Client Channel Configuration Delivery Server)
Server Wide Channel Configuration	
Maximum Receivers	Total number of VQE Clients that are expected to tune in this channel. This value is used by VQE-S to calculate how often VQE-S sends an RTCP report to the video source for this channel.
RTCP Interval	Defines how often VQE Clients send an RTCP report. By default, RTCP Interval is five seconds.

Step 3 Do one of the following:

- Click **Create** to create the new server.
- Click **Cancel** to close the dialog box without creating the new server.

Viewing or Updating Server Information

To view or update server information, follow these steps:

Step 1 On the Servers tab, click the server you want to view or update.

Step 2 Click **Details**.

The Details dialog box is displayed.

Step 3 If needed, change the server information.

Step 4 Do one of the following:

- Click **Update** to update the server information.
- Click **Cancel** to close the dialog box without changing server information.

Deleting a Server

To delete a server, follow these steps:

Step 1 On the Servers tab, click the server you want to delete.

Step 2 Click **Delete**.

A dialog box asking if you want to delete the server is displayed.

Step 3 Do one of the following:

- Click **Delete** to delete the server.
- Click **Cancel** to close the server dialog box without deleting the server.

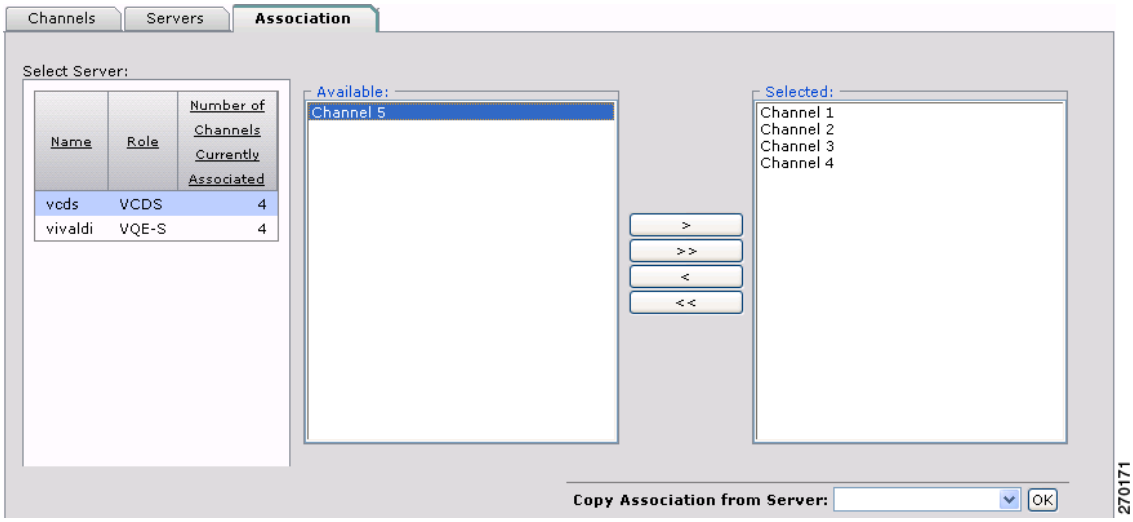
Step 4 If you clicked Delete, a confirmation dialog box is displayed. Click **OK**.

Defining Channel Associations

After VQE channels and the VQE Servers and VQE Client Channel Configuration Delivery Servers have been defined, you associate a set of channels with the servers. When the channel information file is sent to the VQE Servers and VQE Client Channel Configuration Delivery Servers, only the channels associated with the server are included in the file.

In the VQE Channel Provisioning Tool, use the Association tab (Figure 3-9) to associate servers with channels or copy an existing channel association.

Figure 3-9 Association Tab



The following sections explain how to associate channels with servers:

- Defining Channel Associations for a Server, page 3-16
- Copying Channel Associations from Another Server, page 3-18

Defining Channel Associations for a Server

To define channel associations for a server, follow these steps:

Step 1 From the Select Server pull-down menu, select the server for which you want to define channel associations.

VCPT displays the IP address and role for the server.

Step 2 Select one or more channels to associate or disassociate with the server by using the arrow buttons. For example:

- The > button moves a single available channel or group of available channels to the Selected group.
- The >> button moves all available channels to the Selected group.

The associations for the channel are updated.

Copying Channel Associations from Another Server

To copy channel associations for a server, follow these steps:

Step 1 From the Select Server pull-down menu, select the server for which you want to define channel associations.

VCPT displays the IP address and role for the server.

Step 2 From the Copy Association from Server pull-down menu, select the server whose channel associations you want to copy.

Step 3 Click **OK**.

The associations for the channel are updated.

CHAPTER 4

Using the VQE-S Application Monitoring Tool

This chapter describes how to use Cisco VQE-S Application Monitoring Tool (VQE-S AMT or AMT). The tasks that you can perform with VQE-S AMT are listed in Table 4-1.

Table 4-1 VQE-S AMT Tasks

VQE-S AMT Task	Section Where Described
Logging in to VQE-S AMT	Logging in to and Navigating in VQE-S AMT, page 4-1
Monitor the health of the VQE-S processes	Monitoring the Health of the VQE-S Processes, page 4-4
View channel configuration details, status, and statistics	Viewing Channel Configuration and Status, page 4-6
Monitor statistics for Unicast Retransmission and RCC	Monitoring Unicast Retransmission and RCC, page 4-11
View configuration details, status, and statistics for Multicast Load Balancer	Monitoring Multicast Load Balancer, page 4-14
View configuration details, status, and statistics for VQE-S RTCP Exporter	Monitoring RTCP Exporter, page 4-16
View STUN Server Statistics	Monitoring the STUN Server, page 4-17
Configure VQE-S logging levels	Configuring VQE-S Logging, page 4-18
Configure VQE-S debugging levels	Configuring VQE-S Debugging, page 4-19

Note VQE-S AMT supports configuration capabilities for logging levels and debugging options. However, the configured values do not persist when AMT is restarted.

Logging in to and Navigating in VQE-S AMT

Before logging into VQE-S AMT, you need a valid Linux username and password on the Cisco CDE110 hosting AMT. The username does not have to belong to any special group. Creation of the username is the responsibility of the Cisco CDE110 system administrator.

VQE-S AMT supports two web browsers: Microsoft Internet Explorer version 6.0 or later, and Mozilla Firefox version 2.0 or later. The minimum screen resolution required for VQE-S AMT is 1024 x 768 pixels.

VQE-S AMT uses secure HTTPS. Access by multiple simultaneous browsers is supported.

To display the Channels Status Summary graph of active, inoperative, and inactive channels in the AMT VQE-S Status window, Adobe Flash Player must be installed on the computer that hosts the browser accessing AMT. Adobe Flash Player is free and can be found at this URL:

http://get.adobe.com/flashplayer/

To login to VQE-S AMT, follow these steps:

Step 1 Point your web browser to the Cisco CDE110 that hosts VQE-S AMT using an IP address or fully qualified domain name:

```
https://ip_address
```

or

```
https://fully_qualified_domain_name
```

The AMT login dialog box is displayed.

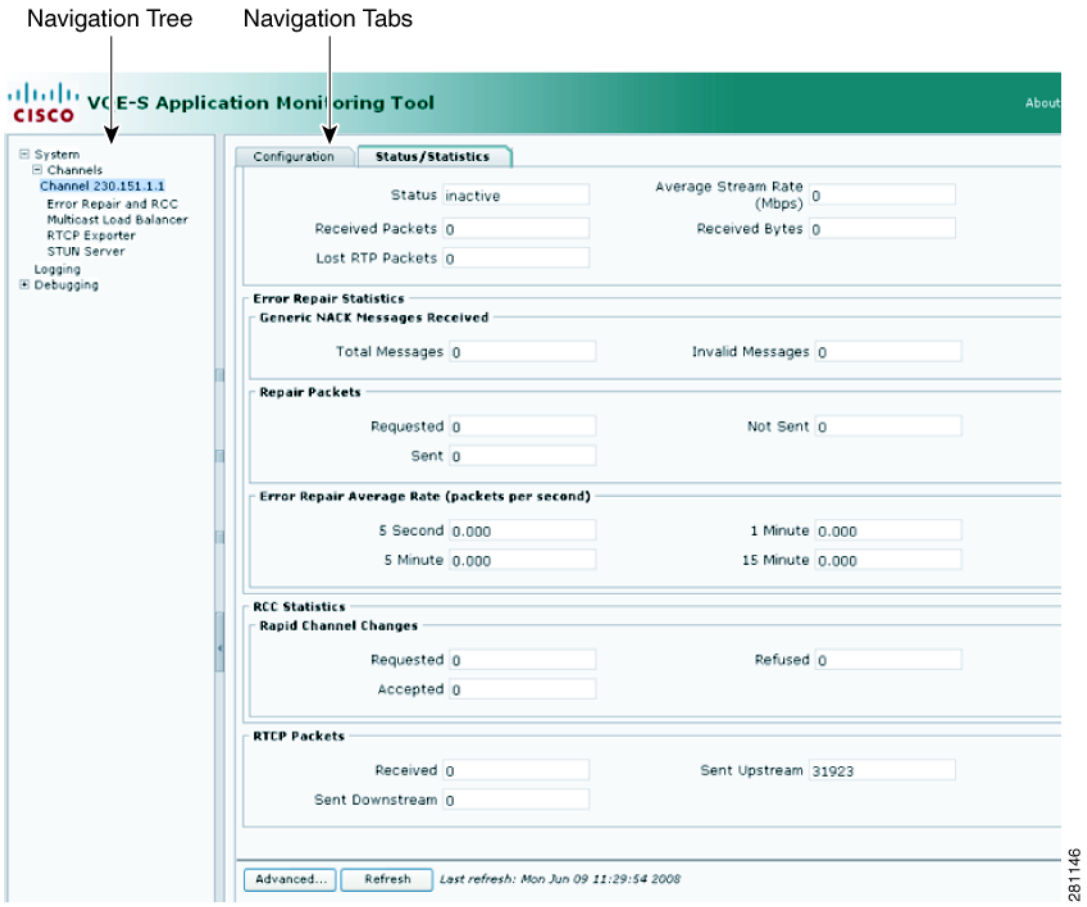
Step 2 Enter a Linux username and password.

Step 3 Click **OK**.

If the username and password are valid, the AMT VQE-S Status window is displayed.

Figure 4-1 shows the VQE-S AMT navigation controls and buttons.

Figure 4-1 VQE-S AMT Navigation



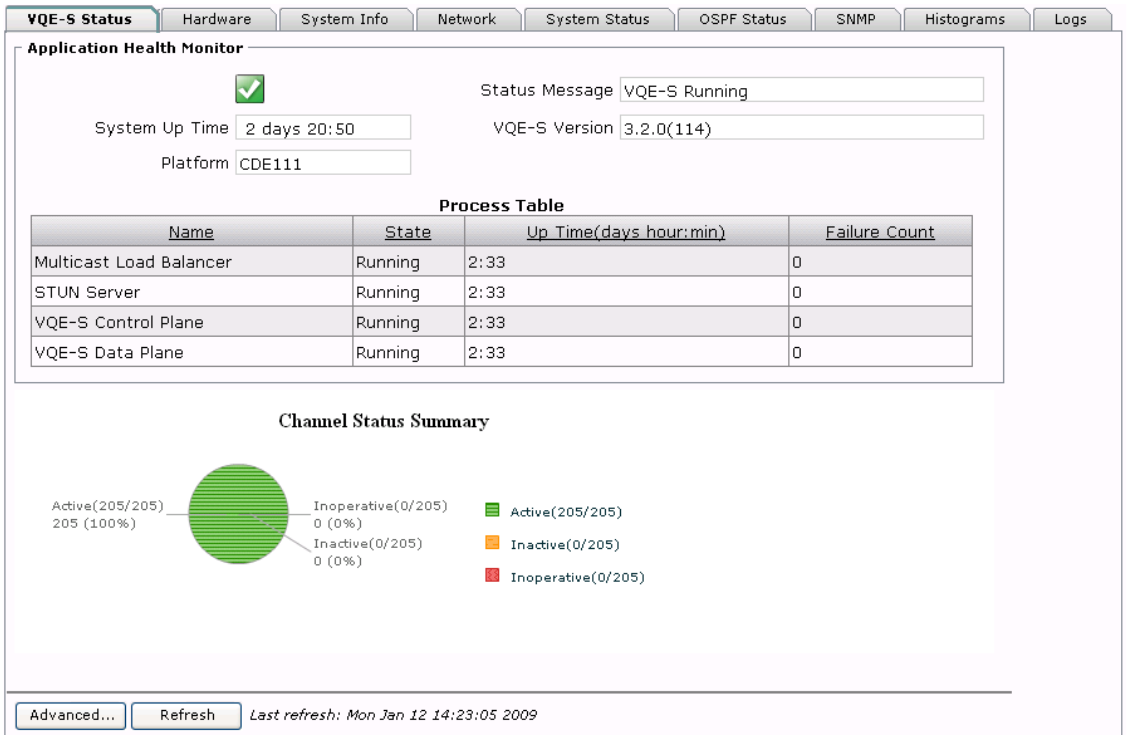
VQE-S AMT (Figure 4-1) provides these controls and buttons for navigating and displaying VQE data:

- **Navigation tree**—Use the collapsible and expandable tree to display the VQE-S AMT items that can be viewed or configured. The navigation tree can be hidden by clicking the < arrow in its right border.
  - A parent node in the tree (such as Channels) usually provides summary data.
  - A child node in the tree (such as an individual channel name) provides data on the specific child node.
- **Navigation Tabs**—Click the tabs to display VQE data for viewing or VQE parameters for configuring in the main window. Some but not all VQE items have Configuration and Statistics tabs that display the relevant data or parameters.
- **Advanced**—Click to get additional, detailed information on the current VQE-S AMT items. The advanced data is intended for Cisco Technical Support and are not described in this document.
- **Refresh** —Click to update the displayed data. VQE-S AMT statistical data are not automatically updated when VQE-S real-time counters are incremented. The Last refresh date-and-time information to the right of the **Refresh** button indicates when the last update of displayed data occurred.

Monitoring the Health of the VQE-S Processes

When you click the **System** node in the navigation tree and the **VQE-S Status** tab, VQE-S AMT displays the VQE-S Status window (Figure 4-2). The Application Health Monitor and a Channel Status Summary are displayed in the VQE-S Status window.

Figure 4-2 VQE-S Status Window



In the Application Health Monitor, a green icon with a checkmark indicates the VQE-S system is running and healthy. A red icon with an X indicates one or more problems with the VQE-S processes.

Using the Application Health Monitor, you can view the following status information:

- System Up Time—Time that Cisco CDE110 hosting VQE-S has been running.
- Platform—Cisco CDE110 hardware platform that is hosting this VQE-S. Platform can be one of the following:
  - Cisco CDE110 (models CDE110-1-036TXA-K9 and CDE110-1-036TXD-K9)
  - Cisco CDE111 (models CDE111-2-146TXA-K9 CDE111-2-146TXD-K9)
  - UNKNOWN if the hardware platform cannot be determined
- Status Message—Current status of the VQE-S software or information on problems (for example, the message “Config File Parsing Failed”)
- VQE-S Version—Current version of the VQE-S software.
- Process Table—Information on these VQE-S processes:
  - Multicast Load Balancer
  - STUN Server

- Data Plane
- Control Plane

In the Process Table, Failure Count is the number of times the process has failed and been restarted by VQE-S Process Monitor. Process Monitor is responsible for starting and monitoring the preceding processes.

The Channels Status Summary section provides the number of and a graph for active, inoperative, and inactive channels.

In addition to the VQE-S Status tab, you can get information on the VQE-S system on the five other tabs. Table 4-2 lists the information that is available from each tab accessible from the System node.

Table 4-2

System Node Tab	Information Provided
VQE-S Status	Application Health Monitor and Channel Status Summary
Hardware	Processor and memory on the Cisco CDE110 that hosts VQE-S Each CDE110 has two physical processors and four virtual processors.
System Info	Hostname, operating system version, date and time, Network Time Protocol servers, Domain Name System servers, and **iptables** information (trusted channel-provisioning servers).
Network	Output from the **ifconfig** and **ip addr show lo** commands. • The configuration information displayed by **ifconfig** is for the four CDE110 Ethernet interfaces and the CDE110 loopback addresses. • The loopback addresses displayed by **ip addr show lo** are the feedback target addresses for the configured channels.
System Status	Detailed information on host uptime, currently running processes, and file system disk space.
OSPF Status	Output from a number of commands that show OSPF information, including status, neighbors, interfaces, database, and routes.
SNMP	SNMP information on the VQE-S host taken from the snmpd.conf file.
Histograms	Set-top box IGMP latency data is displayed in graphs and tables.
Logs	Most recent 300 lines from the following VQE-related log files are displayed: • VQE-S log (/var/log/vqe/vqe.log) • System messages log (/var/log/messages) • HTTPD error log (/var/log/httpd/error_log) • SSL error log (/var/log/httpd/ssl_error_log) • Tomcat log (/usr/share/tomcat5/logs/catalina.out)

Viewing Channel Configuration and Status

When you click the **Channels** node in the navigation tree, VQE-S AMT displays the Channel Lineups window (Figure 4-3).

Figure 4-3 Channel Lineups Window

Channel Lineups *Last update: 2008-07-08T14:44:14, Total Channels: 250, Active Channels: 240*
Aggregated Bandwidth: 1215000(kbits/sec), Total Receivers: 1040

Name	Status	Original Multicast	Feedback Target	Bit Rate (Kbps)	Repair Enabled	RCC Enabled	Member Receiver Population
Channel 229.1.1.1	✓	229.1.1.1:53170	11.112.1.1:53171	4000	true	true	400
Channel 229.1.1.10	✓	229.1.1.10:53206	11.112.1.10:53207	13000	true	true	0
Channel 229.1.1.11	✓	229.1.1.11:53210	11.112.1.11:53211	4000	true	true	0
Channel 229.1.1.12	✓	229.1.1.12:53214	11.112.1.12:53215	4000	true	true	0
Channel 229.1.1.13	✓	229.1.1.13:53218	11.112.1.13:53219	4000	true	true	0
Channel 229.1.1.14	✓	229.1.1.14:53222	11.112.1.14:53223	4000	true	true	0
Channel 229.1.1.15	✓	229.1.1.15:53226	11.112.1.15:53227	2000	true	true	0

281142

Using the Channel Lineups window, you can do the following:

- Click on a column heading to reorder the channels in the list. For example, clicking on **Feedback Target** orders the entries by feedback target: the combination of an IP address and RTCP port number.
- Double-click on any item in a channel's row to display the full details for the channel in a new window.
- Click the **Re-Activate** button to cause VQE-S to create all channels that are not currently created in the VQE-S software.

In Figure 4-3, the channel-lineup summary data indicates when the lineup was last updated (for example, with VCPT) and provides totals for all channels and active channels as well as aggregated bandwidth and total receivers:

```
 Last update: 2007-08-06T14:15:31, Total Channels: 10, Active Channels: 9
Aggregated Bandwidth: 88000 (kbits/sec), Total Receivers: 0
```

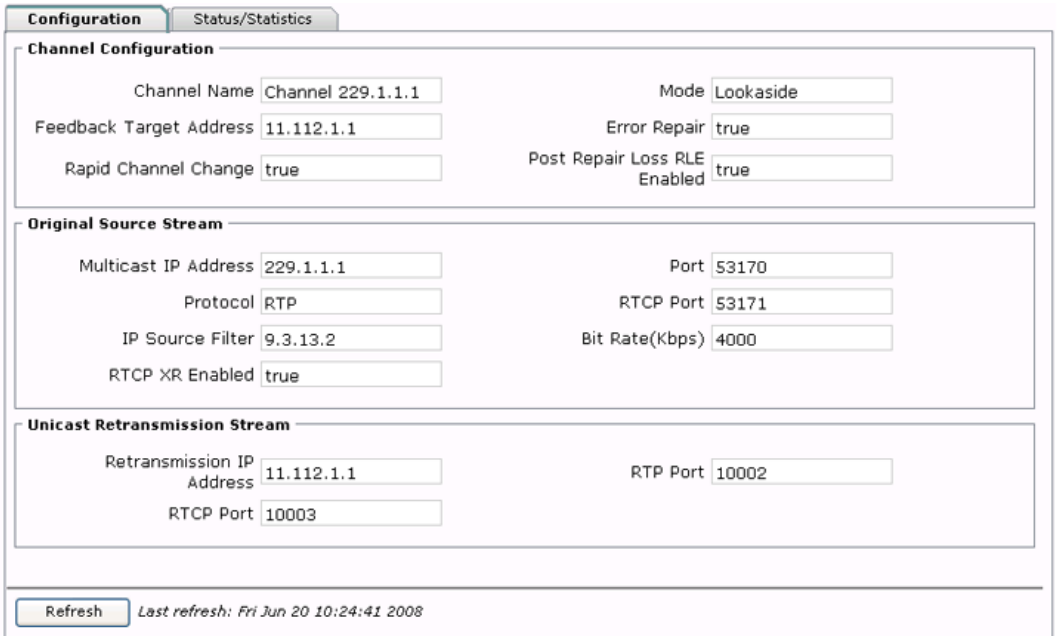
The Channel Lineups window has the same information that is defined for channels using VCPT but has the following additions. For information on the other data that appears in the Channel Lineups table, see Table 3-3 on page 3-8.

- Status—Indicates channel status as follows:
  - Green with a checkmark—Channel is active. VQE-S is receiving the multicast stream.
  - Yellow with exclamation mark (!)—Channel is inactive. The channel is successfully initialized, but VQE-S is not receiving the multicast stream.
  - Red with an X—Channel is inoperative (for example, the channel is not configured correctly).
- Member Receiver Population—Provides the number of VQE Clients that are currently receiving this multicast stream.

Viewing Channel Configuration

When you click on a channel name in the navigation tree and then click the **Configuration** tab, VQE-S AMT displays the Channel Configuration window (Figure 4-4).

Figure 4-4 Channel Configuration Window



The Channel Configuration window has the information listed in Table 4-3.

Table 4-3 Channel Configuration

Field	Description
Channel Configuration	
Channel Name	Name of the channel.
Feedback Target Address	Feedback Target IP address assigned on the VQE-S host.
Rapid Channel Change	• true—RCC is enabled for this channel. • false—RCC is not enabled for this channel.
Mode	Currently only Lookaside mode is supported.
Error Repair	• true—Unicast Retransmission is enabled for this channel. • false—Unicast Retransmission is not enabled for this channel.
Post Repair Loss RLE Enabled	• true—RTCP Extended Reports will include the Loss RLE (run-length encoded) report block type. • false—RTCP Extended Reports will not include the Loss RLE report block type.
Original Source Stream	
Multicast IP Address	Multicast IP address for the channel's original source stream.

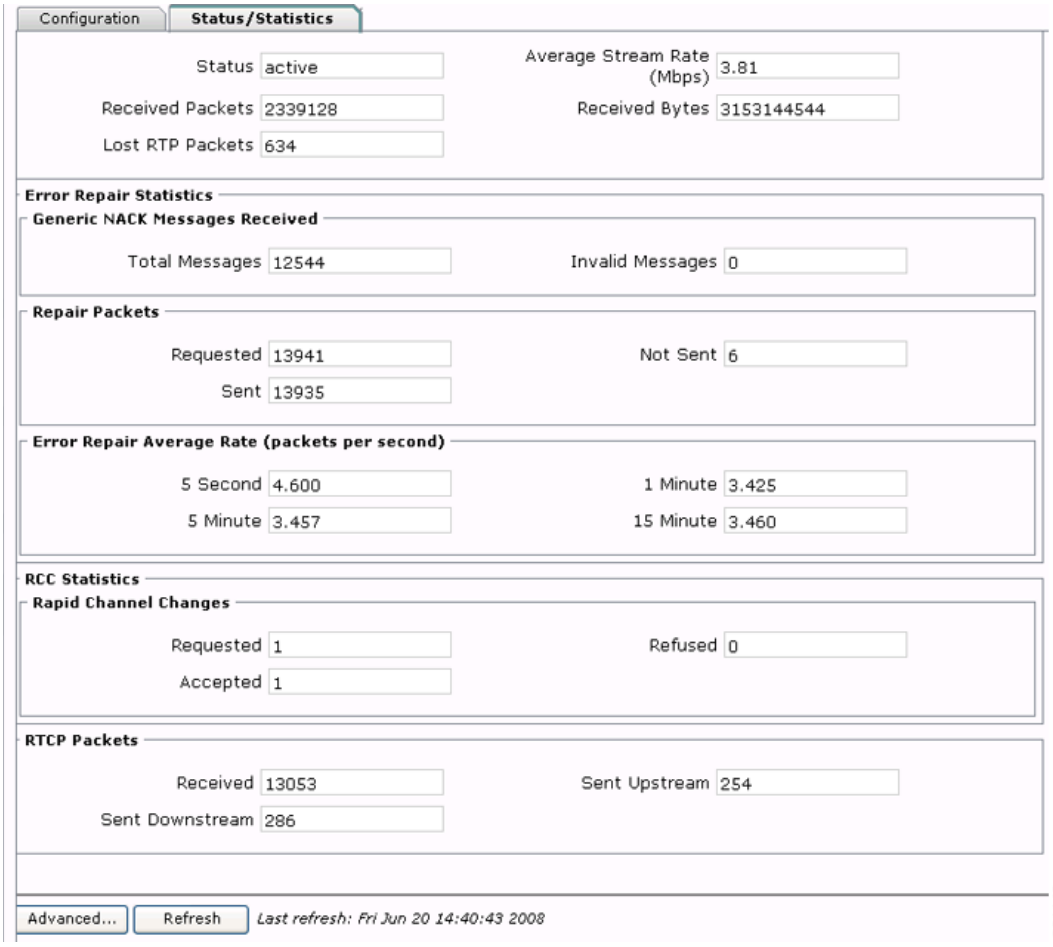
Table 4-3 Channel Configuration (continued)

Field	Description
Protocol	Currently only RTP is supported.
IP Source Filter	Source IP address of the channel's original source stream.
RTCP XR Enabled	• true—RTCP Extended Reports are enabled. • false—RTCP Extended Reports are not enabled.
Port	Number of the port for the original source stream. When the protocol is RTP, this is the RTP port number.
RTCP Port	Number of the RTCP port for the original source stream.
Bit Rate (Kbps)	Bit rate configured for the original source stream.
Unicast Retransmission Stream	
Retransmission IP Address	IP address of the Unicast Retransmission stream.
RTCP Port	Number of the RTCP port for the Unicast Retransmission stream.
RTP Port	Number of the RTP port for the Unicast Retransmission stream.

Viewing Channel Statistics

When you click on a channel name in the navigation tree and then click the Statistics tab, VQE-S AMT displays the Channel Statistics window (Figure 4-5).

Figure 4-5 Channel Statistics Window



The Channel Statistics window has the information listed in Table 4-4.

Table 4-4 Channel Statistics

Field	Description
Channel Input Stream	
Status	• active—VQE-S is receiving the multicast stream. • inactive—The channel is successfully initialized, but VQE-S is not receiving the multicast stream. • inoperative—The channel is not, for example, configured correctly.
Received Packets	Number of RTP packets received by VQE-S for this multicast stream.

Table 4-4 Channel Statistics (continued)

Field	Description
Lost RTP Packets	Number of RTP packets sent but not received by VQE-S for this multicast stream. Lost RTP Packets, in general, specifies the number of missing input RTP packets for a channel, as determined by missing sequence numbers. Some lost packets can occur when a channel is first received because a few packets may be dropped internally by the VQE-S in the course of initializing the channel. Once the channel has been initialized (typically less than a one second delay), further increments in this counter may reflect lost packets in the network between the source of the RTP stream and the VQE-S.
Average Stream Rate (Mbps)	Average megabits per second received by VQE-S for this multicast stream.
Received Bytes	Number of bytes received by VQE-S for this multicast stream.
Error Repair Statistics—Generic NACK Messages Received	
Total Messages	Number of NACK messages received by VQE-S from VQE-C for this multicast stream.
Invalid Messages	Number of invalid messages received by VQE-S from VQE-C for this multicast stream. Invalid messages are received messages that, for example, cannot be parsed.
Repair Packets	
Requested	Number of RTP packets VQE Clients have requested for Error Repair for this multicast stream.
Sent	Number of RTP packets sent by VQE-S that have succeeded in repairing an error for this multicast stream.
Not Sent	Number of failed RTP packets that were not repaired by VQE-S for this multicast stream. VQE-S may not be able to send an Error Repair packet for the following reasons: • The most likely cause is that the Error Repair requests were bursty and exceeded the Error Repair rate-policer limit at one point. • The requested RTP packets were not found in the VQE-S memory cache. • The VQE-S failed to send the RTP packets because of a socket sendto() failure.
Error Repair Average Rate (packets per second)	
5 second, 5 minute, 1 minute, 15 minute	For each time interval, the average number of packets per second that VQE-S has sent to VQE Clients to repair errors for this multicast stream. Averages are calculated for each time interval over a period of time that is greater than the interval. For example, the five second calculation might be an average of 12 five-second intervals over a one minute period.
RCC Statistics—Rapid Channel Changes	
Requested	Number of Rapid Channel Changes requested for this channel.
Accepted	Number of Rapid Channel Changes requested for this channel where the VQE-S has accepted the request and sent IPTV packets and other channel data to a VQE Client on the set-top box.

Table 4-4 Channel Statistics (continued)

Field	Description
Refused	Number of Rapid Channel Changes requested for this channel where VQE-S refused the request. For example, VQE-S may refuse an RCC request for the following reasons: • If the VQE-S did not find an I-frame that is a suitable starting point for the RCC burst • If the VQE-S exceeded the output interface bandwidth limit or CPU load limit If the CPU load limit is exceeded, the Advanced Channel Debug Stats counter "Refused RCC - no core resources on DP" shows when the limit is exceeded.
Failed	Number of Rapid Channel Changes that have failed. A VQE-C has made an RCC request, and VQE-S has accepted the request and sent IPTV packets and other channel data to a VQE Client. But the RCC failed. For example, an RCC can fail if the VQE-C stops receiving the packets from the VQE-S earlier than expected.
RTCP Packets	
Received	Number of RTCP packets received by VQE-S for this multicast stream.
Sent Downstream	Number of RTCP packets that VQE-S sent downstream for this multicast stream.
Sent Upstream	Number of RTCP packets that VQE-S sent upstream for this multicast stream.

Monitoring Unicast Retransmission and RCC

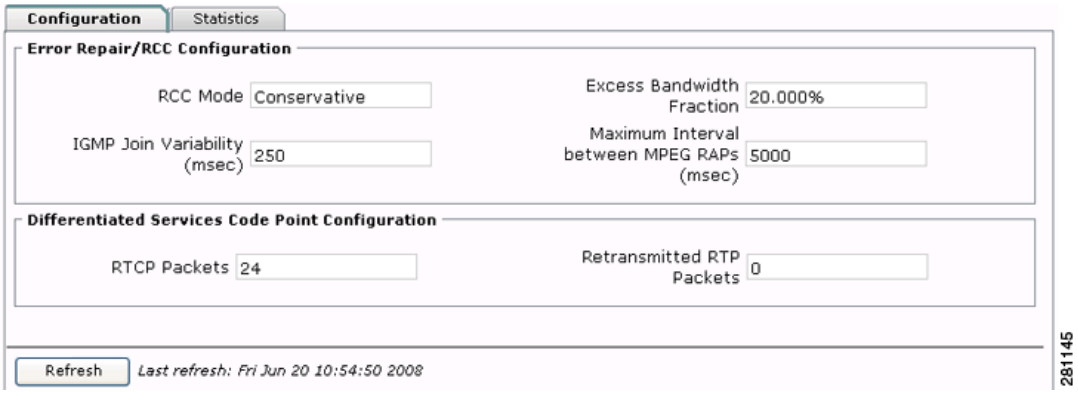
Note In VQE-S AMT, Error Repair is the term used for Unicast Retransmission.

You can use VQE-S AMT to view Error Repair and RCC statistics.

Viewing Error Repair and RCC Configuration

When you click **Error Repair and RCC** in the navigation tree and click the **Configuration** tab, VQE-S AMT displays the Error Repair and RCC Configuration window (Figure 4-6).

Figure 4-6 Error Repair and RCC Configuration Window



The Error Repair and RCC Configuration window has the information listed in Table 4-5. Each of the parameters listed in the table can be configured with the VQE Configuration Management System. For information on configuring VQE-S, see Chapter 6, "Configuring VQE Server and VQE Tools."

Table 4-5 Error Repair and RCC Configuration

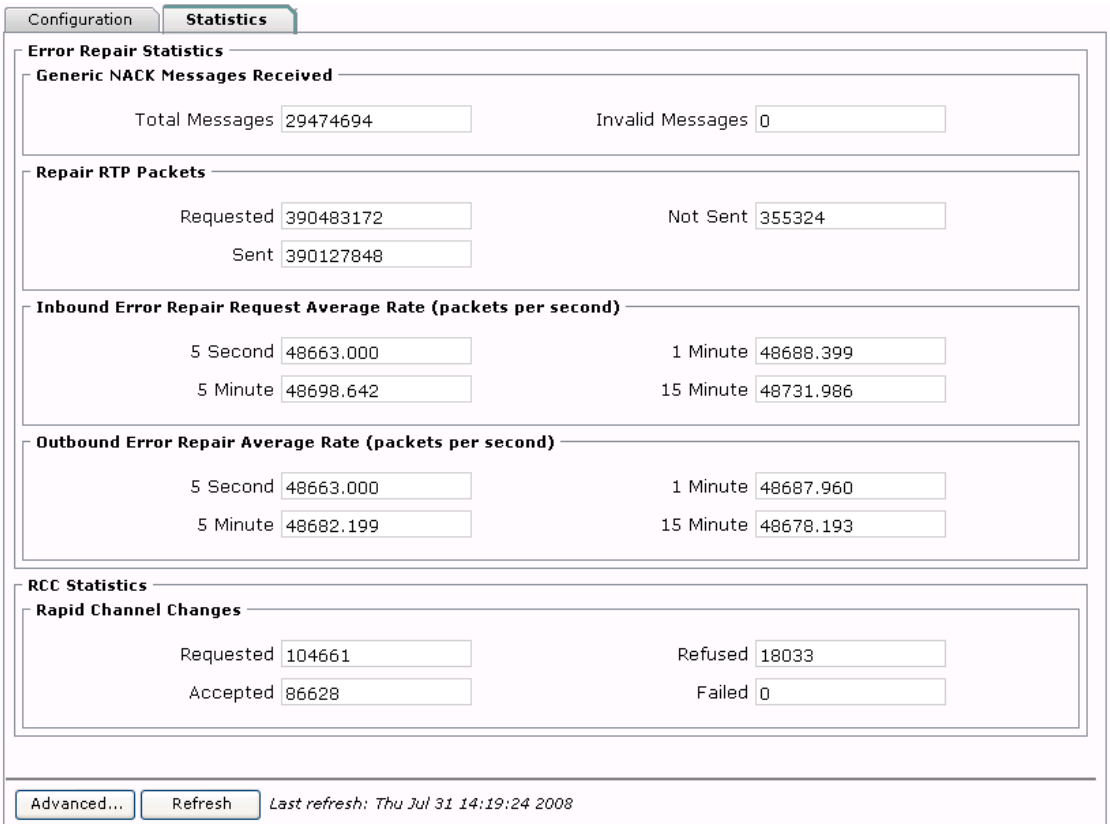
Field	Description
Error Repair/RCC Configuration	
RCC Mode	RCC mode can be aggressive or conservative. This value is configured with the vqe.vqes.rcc_mode parameter in VCDB. For information on this parameter, see Table A-3 on page A-4.
IGMP Join Variability (msec)	Amount of variability (in milliseconds) between the fastest and slowest IGMP joins for RCC. This value is configured with the vqe.vqes.igmp_join_variability parameter. For information on this parameter, see Table A-3 on page A-4.
Excess Bandwidth Fraction	Percent of channel bandwidth that will be available on the access link for Unicast Retransmission and Rapid Channel Change. This value is configured with the vqe.vqes.excess_bw_fraction parameter. For information on this parameter, see Table A-4 on page A-6.
Maximum Interval between MPEG RAPs (msec)	Maximum time interval (in milliseconds) between MPEG RAPs (random access points) for the entire channel lineup. This value is configured with the vqe.vqes.rap_inteval parameter in VCDB. For information on this parameter, see Table A-3 on page A-4.
Differentiated Services Code Point Configuration	
RTCP Packets	DCSP value for RTCP packets that VQE-S transmits. This value is configured with the vqe.vqes.rtcp_dscp parameter in VCDB. For information on this parameter, see Table A-1 on page A-2.
Retransmitted RTP Packets	DCSP value for RTP packets that VQE-S transmits. This value is configured with the vqe.vqes.rtp_trans_dscp parameter in VCDB. For information on this parameter, see Table A-1 on page A-2.

Viewing Error Repair and RCC Statistics

When you click **Error Repair and RCC** in the navigation tree and click the **Statistics** tab, VQE-S AMT displays the Error Repair and RCC Statistics window (Figure 4-7). The statistics are for this VQE-S and are similar to the Error Repair and RCC statistics displayed for individual channels but are for all channels in the current channel lineup.

The Error Repair and RCC statistics are reset to 0 when VQE-S restarts or when the channel lineup changes.

Figure 4-7 Error Repair and RCC Statistics Window



The Error Repair and RCC Statistics window has the information listed in Table 4-6.

Table 4-6 Error Repair and RCC Statistics

Field	Description
Generic NACK Messages Received	
Total Messages	Number of NACK messages received by this VQE-S from VQE Clients.
Invalid Messages	Number of invalid messages received by this VQE-S from VQE Clients. Invalid messages are received messages that, for example, cannot be parsed.
Repaired RTP Packets	
Requested	Number of RTP packets VQE Clients have requested for Error Repair from this VQE-S.

Table 4-6 Error Repair and RCC Statistics (continued)

Field	Description
Sent	Number of RTP packets sent by this VQE-S that have succeeded in repairing an error.
Not Sent	Number of failed RTP packets that were not repaired by VQE-S. VQE-S may not be able to send an Error Repair packet for the following reasons: • The most likely cause is that the Error Repair requests were bursty and exceeded the Error Repair rate-policer limit at one point. • The requested RTP packets were not found in the VQE-S memory cache. • The VQE-S failed to send the RTP packets because of a socket sendto() failure.
Inbound and Outbound Error Repair Average Rate (packets per second)	
5 second, 5 minute, 1 minute, 15 minute	For each time period, the average number of packets per second that VQE-S has received (inbound) or sent (outbound) to VQE Clients to repair errors (Unicast Retransmission).
RCC Statistics—Rapid Channel Changes	
Requested	Number of Rapid Channel Changes requested for this channel.
Accepted	Number of Rapid Channel Changes requested for this channel where the VQE-S has accepted the request and sent IPTV packets and other channel data to a VQE Client on the set-top box.
Refused	Number of Rapid Channel Changes requested for this channel where VQE-S has refused the request. For example, VQE-S may refuse an RCC request for the following reasons: • If the VQE-S did not find an I-frame that is a suitable starting point for the RCC burst • If the VQE-S exceeded the output interface bandwidth limit or CPU load limit If the CPU load limit is exceeded, the Advanced Channel Debug Stats counter "Refused RCC - no core resources on DP" shows when the limit is exceeded.
Failed	Number of Rapid Channel Changes that have failed. A VQE-C has made an RCC request, and VQE-S has accepted the request and sent IPTV packets and other channel data to a VQE Client. But the RCC failed. For example, an RCC can fail if the VQE-C stopped receiving RCC packets from the VQE-S earlier than was expected.

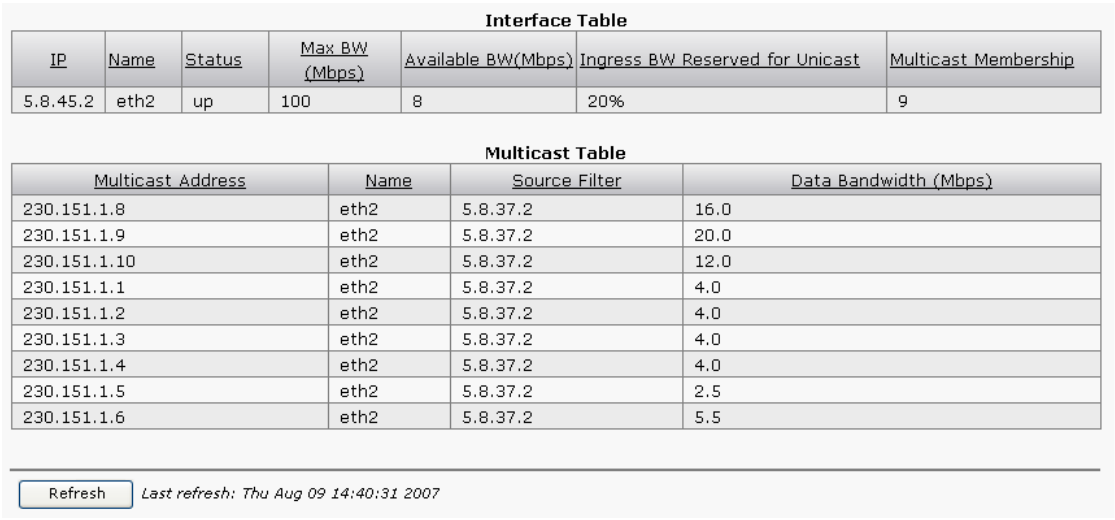
Monitoring Multicast Load Balancer

When you click **Multicast Load Balancer** in the navigation tree, VQE-S AMT displays two tables associated with the Multicast Load Balancer component of VQE-S: the Interface Table and the Multicast Table. Figure 4-8 shows both tables.

Multicast Load Balancer distributes traffic for incoming multicast streams and outgoing Error Repair over the Ethernet interfaces on the Cisco CDE110 that hosts VQE-S. The interfaces must be correctly configured and operational (up) to participate in this load balancing.

Multicast Load Balancer determines the best interface on which to join or leave the multicast group, distributing the joins across available interfaces to avoid oversubscription. Load Balancer also monitors the status of these interfaces, moving the streams to other interfaces in case of interface failure.

Figure 4-8 Interface Table and the Multicast Table



Interface Table

IP	Name	Status	Max BW (Mbps)	Available BW(Mbps)	Ingress BW Reserved for Unicast	Multicast Membership
5.8.45.2	eth2	up	100	8	20%	9

Multicast Table

Multicast Address	Name	Source Filter	Data Bandwidth (Mbps)
230.151.1.8	eth2	5.8.37.2	16.0
230.151.1.9	eth2	5.8.37.2	20.0
230.151.1.10	eth2	5.8.37.2	12.0
230.151.1.1	eth2	5.8.37.2	4.0
230.151.1.2	eth2	5.8.37.2	4.0
230.151.1.3	eth2	5.8.37.2	4.0
230.151.1.4	eth2	5.8.37.2	4.0
230.151.1.5	eth2	5.8.37.2	2.5
230.151.1.6	eth2	5.8.37.2	5.5

Refresh *Last refresh: Thu Aug 09 14:40:31 2007*

202276

The Interface Table (Figure 4-8) has the information listed in Table 4-7. The information is about the Ethernet interfaces on the Cisco CDE110 that are currently participating in multicast load balancing.

Table 4-7 Interface Table

Column	Description
IP	IP address assigned to this Ethernet interface.
Name	Name that is assigned to this Ethernet interface by Linux. For information on these names, see "Configuring the Linux Operating System for VQE-S" section on page D-3.
Status	Either up or down.
Max BW	Maximum speed of the interface.
Available BW	Interface bandwidth that is currently not being used.
Ingress BW Reserved for Unicast	Percent of the interface's ingress bandwidth that is reserved for Error Repair requests from VQE Clients. This value is configured by the burst-rate option in the VQE-S configuration file.
Multicast Membership	Number of channels that are currently using this interface for Error Repair.

The Multicast Table (Figure 4-8) has the information listed in Table 4-8. The information is about the multicast streams on this VQE-S that are currently participating in multicast load balancing.

Table 4-8 Multicast Table

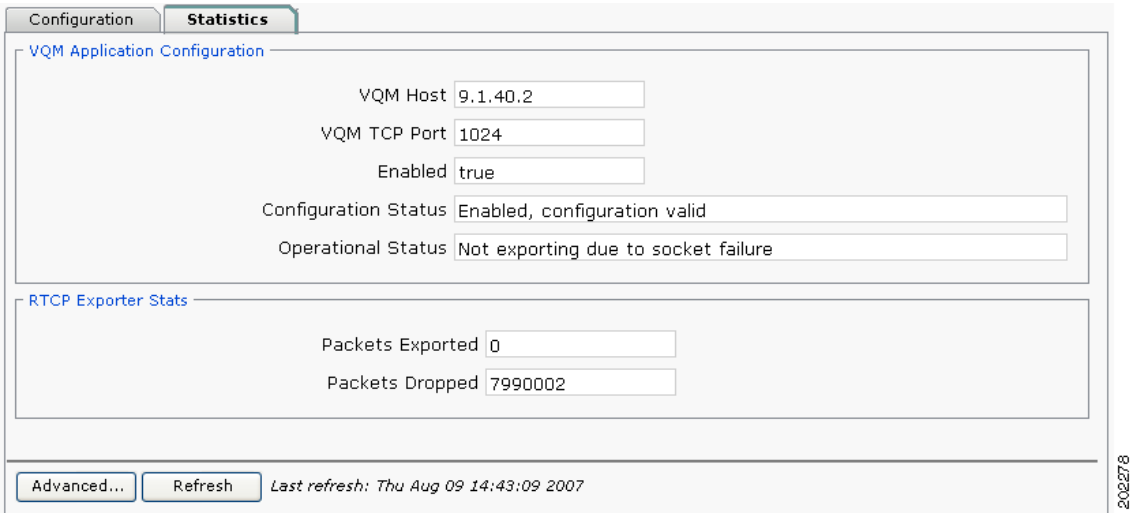
Column	Description
Multicast Address	IP address for this multicast group.
Name	Name of the interface that is being used for this multicast stream.
Source Filter	IP address of the multicast group's original source stream.
Data Bandwidth	Bandwidth specified for this multicast steam in VCPT's Bit Rate field.

Monitoring RTCP Exporter

When you click **RTCP Exporter** in the navigation tree and click the **Configuration** tab, VQE-S AMT displays the VQE-S RTCP Exporter parameters. RTCP Exporter currently has no parameters that can be configured with VQE-S AMT, and the parameters are for viewing only. For information on configuring RTCP Exporter, see the "Configuring VQE-S RTCP Exporter" section on page 2-30.

When you click **RTCP Exporter** in the navigation tree and click the **Statistics** tab, VQE-S AMT displays the RTCP Exporter Statistics window (Figure 4-9).

Figure 4-9 RTCP Exporter Statistics Window



The RTCP Exporter Statistics window has the information listed in Table 4-9. The statistics are for this VQE Server's RTCP Exporter.

Table 4-9 RTCP Exporter Statistics

Field	Description
VQM Application Configuration	
VQM Host	IP address of the host on which the video-quality monitoring (VQM) application resides.
VQM TCP Port	TCP port number on which the VQM application listens for video quality data from RTCP Exporter.

Table 4-9 RTCP Exporter Statistics

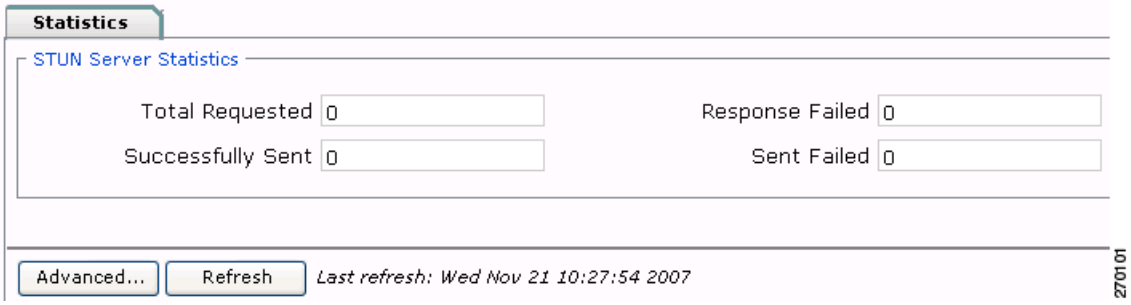
Field	Description
Enabled	Either true (enabled) or false (not enabled).
Configuration Status	Either enabled or not enabled. It is possible for the value in the Enabled field to be true, and the value in the Configuration Status field to be not enabled (for example, if the host IP address or TCP port are not valid).
Operational Status	Message providing information on the operational status of RTCP Exporter.
RTCP Exporter Stats	
Packets Exported	Number of RTCP compound packets that have been exported to a VQM host.
Packets Dropped	Number of RTCP compound packets that have been dropped rather than exported to a VQM host. In heavy load situations, RTCP Exporter may intentionally drop RTCP packets. Details on dropped packets (number of dropped packets and the position and time where this loss occurred) is contained in the collection of reports exported by this VQE-S.

For information on RTCP Exporter and the video-quality monitoring application, see the "VQE-S RTCP Exporter for Video-Quality Monitoring" section on page 1-21.

Monitoring the STUN Server

When you click **STUN Server** in the navigation tree, VQE-S AMT displays the STUN Server Statistics window (Figure 4-10).

Figure 4-10 STUN Server Statistics Window



The STUN Server Statistics window has the information listed in Table 4-10.

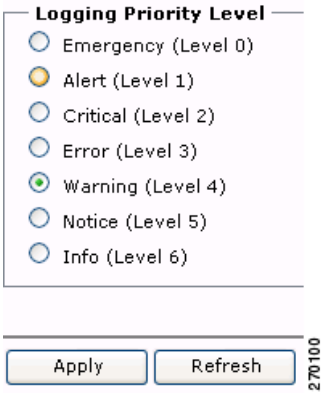
Table 4-10 STUN Server Statistics

Field	Description
Total Requested	Number of STUN binding requests that the VQE-C STUN Client sent to the STUN Server.
Successfully Sent	Number of responses to STUN binding requests that the STUN Server successfully sent to the VQE-C STUN Client.
Response Failed	Number of instances where the STUN Server fails to generate a binding response because of an internal error.
Sent Failed	Number of instances where the STUN Server successfully generates a binding response but fails to send it to the VQE-C STUN Client (for example, because of a socket error).

Configuring VQE-S Logging

When you click **Logging** in the navigation tree, VQE-S AMT displays the logging priority levels (Figure 4-11) for VQE-S. The priority levels allow you to control the logging level for system messages for all VQE-S processes (Process Monitor, Control Plane, Data Plane, and Multicast Load Balancer). By default, all VQE-S system messages are written to the file /var/log/vqe/vqe.log.

Figure 4-11 Logging Priority Levels



To configure a VQE-S logging priority level, click the button next to the level you want and click **Apply**.

In VQE-S AMT, the logging priority levels are listed from least verbose to most verbose. The Emergency level generates the smallest number of messages, and the Info level generates the greatest number of messages. The default value is Warning.

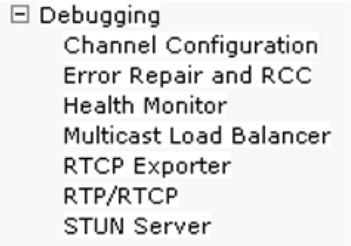
When you select a logging level, log messages are generated for the levels below that level. For example, when the level is set to Error, messages are generated for Emergency, Alert, Critical, and Error.

The selected logging priority level does not persist when VQE-S is stopped. When VQE-S restarts, the logging priority level goes back to the default (Warning). To set a logging priority level that does persist, use the VQE-S parameter vqe.vqes.log_priority. For information on this parameter, see Table A-1 on page A-2.

Configuring VQE-S Debugging

When you click **Debugging** in the navigation tree and click a debug component, the debugging options for that component are displayed. Figure 4-12 shows the debug components. The options allow you to control the types of debugging messages that are written to the syslog file. By default, debug messages are written to the file /var/log/vqe/vqe.log.

Figure 4-12 Debug Components

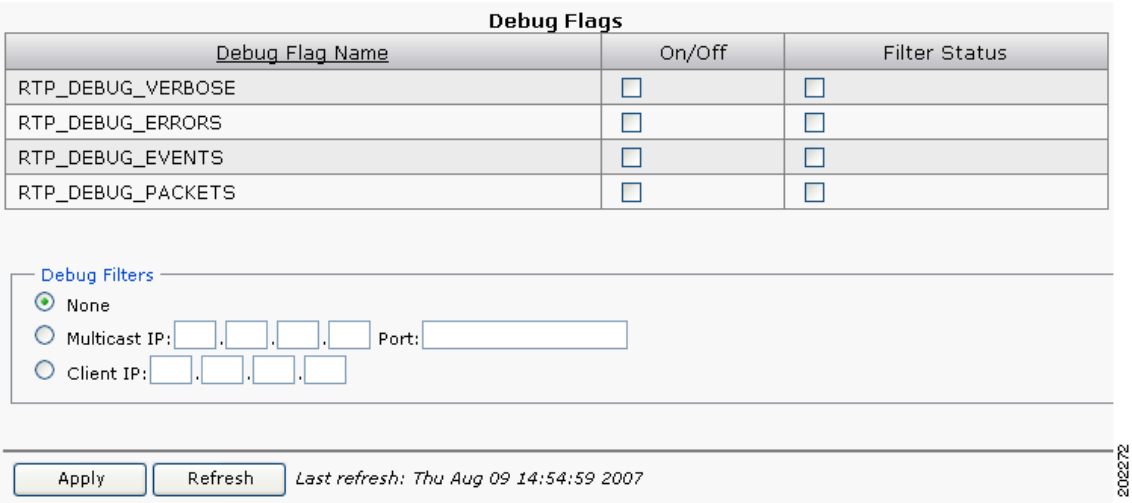


To configure VQE-S debugging, follow these steps:

Step 1 In the VQE-S AMT navigation tree, click the + sign next to **Debugging** and click the component for which you want debug messages.

The debug flags and filters for that component are displayed. For example, Figure 4-13 shows the flags and filters for the RTP/RTCP category.

Figure 4-13 RTP/RTCP Flags and Filters



Note In the Debug Filters for the STUN Server, only the Client IP filter is supported. The Multicast IP filter is not supported because the STUN Server has no knowledge of channels. Filtering on the Client IP address will provide debug messages for the specified client.

Step 2 To enable a debugging flag, click the check box in the On/Off column, or to disable an enabled flag click the check box to uncheck it.

Note For the next step, be aware that not all debug flags support debug filters (in the Filter Status column). If debug filters are not supported, the check box next to the flag is grayed out.

Step 3 For an enabled debugging flag, if you want to filter debugging messages by a specific channel or VQE Client, do the following:

a. In the Filter Status column, click the check box for the option.

b. In the Debug Filters section, click either **Multicast IP** or **Client IP**:

- For Multicast IP, enter the channel's source stream IP address and (RTP/UDP) port number.
- For Client IP, enter the VQE Client's IP address.

Step 4 Click **Apply**.

The selected debugging options are enabled.

The selected debugging options do not persist when VQE-S is stopped. When VQE-S restarts, debugging goes back to the default—no options are enabled.

CHAPTER 5

Troubleshooting VQE Software Components

This chapter describes how to identify and remedy problems related to Cisco VQE Server (VQE-S), VQE-S Application Monitoring Tool (VQE-S AMT or AMT), and VQE Channel Provisioning Tool (VCPT). This chapter contains the following major topics:

Useful Linux Tools

Table 5-1 provides information on some Linux commands that are particularly useful for troubleshooting VQE software components.

Table 5-1 Useful Linux Commands

Command	Description	Notes
arp	Manipulates the kernel's ARP cache	—
ethtool	Displays or changes Ethernet card settings	Detailed status on an Ethernet interface
ifconfig	Configures a network interface	Traditional interface configuration and status
ip	Shows or manipulates routing, devices, policy routing and tunnels	Most useful interface to all Linux networking
netstat	Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships	Provides traditional network state information
ping	Sends ICMP ECHO_REQUEST to network hosts	—
tcpdump	Dumps and analyzes traffic on a network	Captures packet data

VQE Logging and Log Files

VQE-related log entries can provide useful information for troubleshooting. The VQE-related log files are described in these sections:

VQE Server and VQE Tools Logging and Log Files

VQE Server logging is based on the Berkeley syslogd utility, which is part of the inetutils package in Linux. The following is a typical VQE-S log entry:

```
Oct 22 08:42:03 minnie vqes_mlb: <<%VQES_MLB-3-MLB_NIC_DOWN>> Network interface eth3 went down.
```

Every logged message contains five fields in this order:

- Timestamp (Oct 22 08:42:03)
- Host name (minnie)
- Name of process logging the message (vqes_mlb)
- Identity string (<<%VQES_MLB-3-MLB_NIC_DOWN>>)
- Log message (Network interface eth3 went down.)

For information on VQE system messages, see Appendix C, “VQE System Messages.”

By default, VQE-S and VQE Tools system messages are written to the file /var/log/vqe/vqe.log. The location of the file is configured in the /etc/syslog.conf file. For information on configuring VQE-S logging, see the “Configuring VQE-S Logging” section on page 4-18.

VQE-S and VQE Tools log files are rotated by logrotate. The logrotate facility is configured to rotate a log file when it is larger than 20 MB. The old versions of the log files are rotated up to 20 times before being removed.

Note If you move the VQE log file to another directory, be sure to stop the syslogd daemon before moving the vqe.log file. If syslogd is started with no vqe.log file in the /var/log/vqe directory, syslogd creates the vqe.log file.

VQE-S AMT and VCPT Logging and Log Files

VQE-S AMT and VCPT are both web applications that make use of the Apache Tomcat application server. Apache Tomcat uses the log4j logging system. For AMT and VCPT, the logging output is configured by these log4j configuration files:

- For AMT, the configuration file is located at /usr/share/tomcat5/webapps/ems/WEB-INF/classes/log4j.properties.
- For VCPT, the configuration file is located at /usr/share/tomcat5/webapps/vcpt/WEB-INF/classes/log4j.properties.

By default, the log files for AMT and VCPT are saved in these locations:

- For AMT, the log files (vqe.log) are saved in the /usr/share/tomcat5/logs directory.
- For VCPT, the log files (vcpt.log) are saved in /usr/share/tomcat5/logs directory.

Table 5-2 lists the most important default log4j configuration settings for AMT and VCPT logging.

Table 5-2 Log4j Default Configuration for AMT and VCPT

Configuration Property	Default Setting
Logging priority level	Warning
Logging output	Log messages are written to both the console and the log file
Maximum size of the log file before it rotates	100 KB
Maximum number of backup files	4

For information on configuring the log4j.properties file, see the log4j documentation at these URLs:

http://tomcat.apache.org/tomcat-5.5-doc/logging.html

http://logging.apache.org/log4j/1.2/manual.html

VQE Files, Directories, and Permissions

If you encounter a problem related to VQE-related files, directories, or permissions, use the information in the following tables to resolve the issues.

- Table 5-3 provides information for the CDE110 that hosts VQE-S.
- Table 5-4 provides information for the CDE110 that hosts VCPT and VQE Client Channel Configuration Delivery Server.

These sections provide additional information on resolving problems:

- Changing Permissions, page 5-5
- Replacing a Lost or Corrupt VQE File, page 5-5

Table 5-3 VQE-S Files, Directories, and Permissions

File or Directory	Required Permissions, Owner, and Group	Description
/etc/opt/vqes (directory)	drwx------ vqes vqes	--
/etc/opt/vqes/vcdb.conf	-rw-r--r-- root root	VCDB configuration file
/etc/opt/vqes/vcdb.conf.sample	-r-------- vqes vqes	VCDB sample configuration file
/etc/opt/vqes/vqe_channels.cfg	-rw-r--r-- vqes vqes	VQE-S channel configuration file
/etc/opt/vqes/vqes_syslog.conf	-rw-r--r-- vqes vqes	VQE-S syslog configuration file
/opt/vqes (directory)	drwxr-xr-x vqes vqes	--
/opt/vqes/bin (directory)	drwxr-xr-x vqes vqes	VQE-S binary directory
/opt/vqes/bin/fbt_flush.sh	-r-xr----- root vqes	VQE-S feedback target flush script

Table 5-3 VQE-S Files, Directories, and Permissions (continued)

File or Directory	Required Permissions, Owner, and Group	Description
/opt/vqes/bin/mlb	-r-xr-xr-x root root	VQE-S Multicast Load Balancer process
/opt/vqes/bin/mlb_ethtool	-r-sr-x--- root vqes	VQE-S Ethernet utility for Multicast Load Balancer
/opt/vqes/bin/process_monitor	-r-xr-xr-x root root	VQE-S Process Monitor process
/opt/vqes/bin/stun_server	-r-xr-xr-x root root	VQE-S STUN Server process
/opt/vqes/bin/vqe_cfgtool	-r-x------ vqes vqes	**vqe_cfgtool** command
/opt/vqes/bin/vqereport	-r-x------ root root	**vqereport** command
/opt/vqes/bin/vqes_cp	-r-x------ root root	VQE-S Control Plane process
/opt/vqes/bin/vqes_dp	-r-xr-xr-x root root	VQE-S Data Plane process
/opt/vqes/bin/vqes_bin.sha1sum	-r--r----- vqes vqes	SHA-1 checksums list
/opt/vqes/bin/vqes_syslogd	-r-xr-xr-x vqes vqes	VQE-S syslogd process
/opt/vqes/bin/xmlrpc	-r-xr-xr-x vqes vqes	XML-RPC client utility
/var/log/vqe (directory)	drwxr-xr-x vqes vqes	VQE log file directory
/var/log/vqe/vqe.log	-rw------- vqes vqes	VQE system messages log file

Table 5-4 VQE Tools Files, Directories, and Permissions

File or Directory	Required Permissions, Owner, and Group	Description
/etc/opt/vqes (directory)	drwx------ root root	--
/etc/opt/vqes/vcdb.conf	-rw-r--r-- root root	VCDB configuration file
/etc/opt/vqes/vcdb.conf.sample	lrwxrwxrwx root root	A link to the VCDB sample configuration file
/etc/opt/vqes/vcdb.conf.tools.sample	-r-------- vqes vqes	VCDB sample configuration file
/etc/opt/vqes/VCDServer.cfg	-rw-r--r-- root root	VQE Client Channel Configuration Delivery Server (VCDS) configuration file
/etc/opt/vqes/vqec_channels.cfg	-rw--r--r-- root root	VCDS channel configuration file
/etc/opt/vcpt (directory)	drwxr-xr-x root root	--
/etc/opt/vcpt/data (directory)	drwxr-xr-x root root	Directory for VCPT configuration files
VCPT configuration files in /etc/opt/vcpt/data	-rw-r--r-- root root	VCPT configuration files (Filenames are user-defined and vary.)
/opt/vqes (directory)	drwxr-xr-x vqes vqes	--
/opt/vqes/bin (directory)	drwxr-xr-x vqes vqes	--
/opt/vqes/bin/vqe_cfgtool	-r-x------ vqes vqes	**vqe_cfgtool** command
/opt/vqes/bin/vqereport	-r-x------ root root	**vqereport** command
/var/log/vqe (directory)	drwxr-xr-x vqes vqes	VQE log directory
/var/log/vqe/vqe.log	-rw------- vqes vqes	VQE system messages log file

Changing Permissions

To change permissions on a file or directory, use the **chmod** command:

Step 1 If needed, log in as root on the CDE110 that hosts VQE-S or that hosts VCPT.

Step 2 To change permissions, issue the following command:

chmod *mode file_or_dir_name*

In the preceding command, the two arguments are as follows:

- *mode* specifies the correct permissions.
- *file_or_dir_name* specifies the file or directory whose permissions will be set.

For example:

```
[root@system]# chmod 555 /opt/vqes/bin/vqes_cp
```

For information on setting permissions, see the man page for the **chmod** command.

Replacing a Lost or Corrupt VQE File

If a required VQE file that has not been backed up becomes lost or corrupt, you must reinstall the version of the VQE software that the CDE110 server is running. To preserve the current VQE configuration, the software reinstallation should be an ISO full upgrade. For information on VQE software installation, see the *Release Notes for Cisco CDA Visual Quality Experience Application, Release 3.2*.

If a configuration file located in the directories under /etc becomes lost or corrupt file and was not backed up, you can do one of the following:

- Use the **vqe_cfgtool** command with the **-fix_config** option to discard the current copy of each /etc configuration file where there is a checksum mismatch and replace it with the original copy of the file that comes with the RPM package. Then apply the current VCDB configuration to the /etc configuration files using the **vqe_cfgtool** command and the **-apply** option.
- Get a copy of the factory default version of the configuration file from the /vqe-etc/etc-pristine directory. To restore the lost or corrupt file, copy the factory default configuration file to its correct location under /etc, and apply the current VCDB configuration to the /etc configuration files using the **vqe_cfgtool** command and the **-apply** option.

For information on the **vqe_cfgtool** command, see the "Using the VQE Configuration Tool Command-Line Options" section on page 6-16.

VQE-S and VQE Tools Server Troubleshooting

This section provides information on troubleshooting the following specific problems that can occur with a VQE-S or VQE Tools server. Table 5-5 lists the troubleshooting topics by the category of the problem.

Table 5-5 Troubleshooting Topics by Problem Category

Problem Category	Troubleshooting Topics
Monitoring a VQE-S server	Monitoring Received Multicast Streams, page 5-6
VQE-S and VQE Tools servers	Static Route for a Management Network Is Missing on CDE110 Hosting VQE-S or VQE Tools, page 5-7
	Repeated Message on CDE110 Hosting VQE-S or VQE Tools, page 5-8
VQE-S server	Repeated Message on CDE110 Hosting VQE-S or VQE Tools, page 5-8
VQE-S AMT	VQE-S AMT or VCPT Unavailable, page 5-10
	Channels Are Not Displayed in VQE-S AMT, page 5-11
	VQE-S AMT Channels Status Summary Has No Graphs, page 5-11
VCPT or other channel-provisioning servers*	VQE-S AMT or VCPT Unavailable, page 5-10
	Channel-Provisioning Server Cannot Send Channel Information to VQE Server: Trusted Provisioning Client(s) Problem, page 5-12
	Channel-Provisioning Server Cannot Send Channel Information to VQE Server: SSL Certificates Problems, page 5-12
	Unable to Connect Error When VCPT Tries to Send Channel Information, page 5-13
	Internal Server Error When VCPT Tries to Send Channel Information to VQE-S, page 5-14

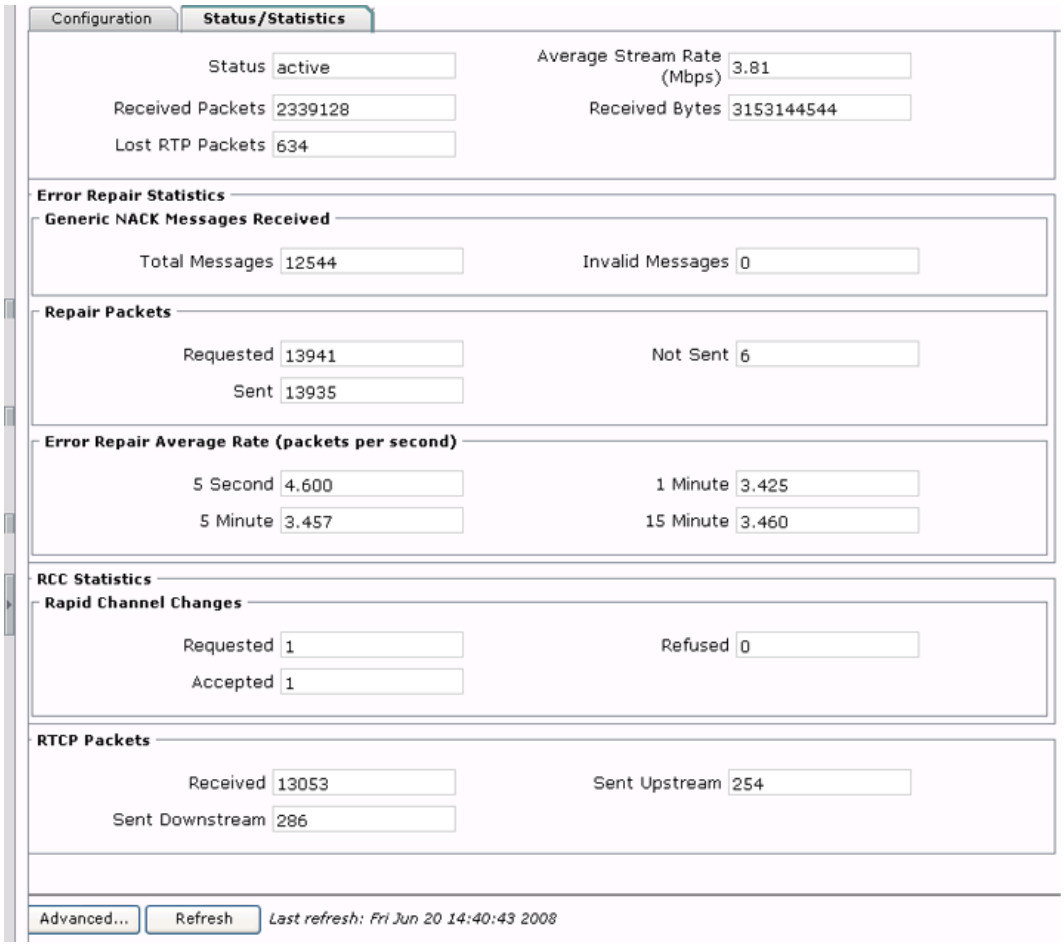
* Some VCPT troubleshooting topics apply to other channel-provisioning servers, such as Cisco IPTV Services Delivery Server (ISDS).

Monitoring Received Multicast Streams

For troubleshooting VQE-S, using VQE-S AMT to monitor received multicast streams is recommended.

We recommend that you use AMT to monitor received multicast streams. In the AMT Channel Statistics window for each channel (Figure 5-1), the Lost RTP Packets field for the Channel Input Stream is a per-channel counter that provides the number of missing RTP packets. The Lost RTP Packets counter increments when an RTP packet is sent for the channel's original source stream but is not received by the VQE Server.

Figure 5-1 Lost RTP Packets



Static Route for a Management Network Is Missing on CDE110 Hosting VQE-S or VQE Tools

Symptom: A static route for a management network, which was configured in /etc/sysconfig/static-routes-iputil, are missing, and the VQE-S host or VQE Tools host can no longer reach the management network.

Explanation: This condition can occur when CDE110 interfaces are manually shutdown by the operator using the Linux **ifdown** *ifname* command and then manually brought back up using the **ifup** *ifname* command. This condition can also occur when the CDE110 interfaces are reset for any reason.

If the next hop routers for a static route configured in /etc/sysconfig/static-routes-iputil become unreachable due to CDE110 interfaces being manually shut down in this manner, the corresponding routes are removed from the routing table and will not be reinstalled even when one or more of the CDE110 interfaces are brought back up.

(The VQE Startup Utility and the VQE Configuration Tool can be used to configure a static route for a management network. These facilities use /etc/sysconfig/static-routes-iputil for the static route to a management network.)

Remedy: To reinstall a management-network static route that has been removed from the routing table, use the **route add** command:

route add -net *management-network-addr/prefix-length* **gw** *gateway-addr*

For example:

```
[root@system]# route add -net 192.0.2.0/16 gw 10.86.21.1
```

In the preceding, the *management-network-addr/prefix-length* is the IP address and prefix length for the management network. The *gateway-addr* is the IP address of the router interface that is directly attached to the CDE110 Ethernet port that will be used for management network traffic.

To avoid this problem in the future, instead of using the **ifup** *ifname* command to bring each of the interfaces up individually, bring them all back up at once using the **service network start** command. This will bring up all interfaces that were shut down, and will also reinstall all of the routes contained in the file /etc/sysconfig/static-routes-iputil.

Repeated Message on CDE110 Hosting VQE-S or VQE Tools

Symptom: During initial system configuration, a new Cisco CDE110 hosting VQE-S or VQE Tools boots successfully, the root password is set successfully, but the following message displays repeatedly:

```
SIOCGIFADDR: Cannot assign requested address
SIOCGIFADDR: Cannot assign requested address
SIOCGIFADDR: Cannot assign requested address
SIOCGIFADDR: Cannot assign requested address
SIOCGIFADDR: Cannot assign requested address
SIOCGIFADDR: Cannot assign requested address
```

Explanation: This error can occur when you configure the CDE110 server manually (rather than use the VQE Startup Configuration Utility). The message may display so frequently that it is difficult to edit a file to continue the initial system configuration.

The message can be caused by an Ethernet interface configuration issue in the ifcfg-eth# files (ifcfg-eth1, ifcfg-eth2, and so on).

Remedy: Look for Ethernet interface address or other errors in the four ifcfg-eth# files. Use a text editor to correct any errors.

Use the following command to verify that the addresses specified in the ifcfg-eth# files have been assigned to the interfaces:

ifconfig -a

Continue with the initial configuration tasks.

Changing the System Time Causes Unicast Retransmission and RCC Disruptions

Symptom: When the system time is changed on a VQE-S server that is actively repairing network errors, all Unicast Retransmissions stop indefinitely, and output gaps are seen on the VQE Clients.

Explanation: When the system time is changed, the behavior of the VQE-S is as follows:

- When the system time is moved forward, the VQE-S receives requests for Unicast Retransmission and Rapid Channel Change (RCC) but does not send the repairs/RCCs to the VQE Clients on the set-top boxes.

- When the system time is moved backward, all channels go to an inactive state and the VQE-S does not perform Unicast Retransmission and RCC operations.

For a VQE-S server that is actively repairing network errors, an explicit system time change (that is, by using the **date** command) always results in the failure of Unicast Retransmission and RCC operations until corrective action is taken.

Remedy: Any time change performed on the VQE-S system should be done during a maintenance window. The procedures for changing the date and time vary depending on whether Network Time Protocol (NTP) or the Linux **date** command is used. See one of the following sections:

- "Performing a Date and Time Change with NTP" section on page 5-9
- "Performing a Date and Time Change with the Linux date Command" section on page 5-10

Note Using the local clock *is not* the recommended procedure for running with accurate time. Using NTP is recommended to keep the VQE-S services operational.

Performing a Date and Time Change with NTP

When performing a date and time change with NTP, do the following:

Step 1 Log in as root.

Step 2 Stop the VQE-S services by issuing the following command:

```
[root@system]# service vqes stop
```

Step 3 Stop the ntpd service by issuing the following command:

```
[root@system]# service ntpd stop
```

Step 4 If needed, set the time zone with the **vqe_cfgtool** command's **-config** option. Use the Configuration Tool's System Parameters menu and the Timezone choice.

Step 5 Set the system date and time to a date and time close to the NTP server date and time by issuing the following command:

date -s "*date_time_string*"

For example:

```
[root@system]# date -s "16:55:30 July 7, 2008"
```

Step 6 Synchronize the clock to the configured NTP servers by issuing the following command:

```
[root@system]# ntpd -q
```

If the system clock is off by a lot, the command will take considerable time to return.

Step 7 Start the ntpd service by issuing the following command:

```
[root@system]# service ntpd start
```

Step 8 Synchronize the hardware clock by issuing the following command:

```
[root@system]# /sbin/hwclock --systohc
```

Step 9 Check NTP synchronization

```
[root@system]# ntpq -p
```

Step 10 Reboot the VQE-S server by issuing the following command:

```
[root@system]# init 6
```

Performing a Date and Time Change with the Linux date Command

When performing a time/date change with the Linux **date** command only, perform the following commands:

Step 1 Log in as root.

Step 2 Stop the VQE-S services by issuing the following command:

```
[root@system]# service vqes stop
```

Step 3 If needed, set the time zone with the **vqe_cfgtool** command's **-config** option. Use the Configuration Tool's System Parameters menu and the Timezone choice.

Step 4 Set the system date and time by issuing the following command:

date -s "*date_time_string*"

For example:

```
[root@system]# date -s "16:55:30 July 7, 2008"
```

Step 5 Synchronize the hardware clock by issuing the following command:

```
[root@system]# /sbin/hwclock --systohc
```

Step 6 Reboot the VQE-S server by issuing the following command:

```
[root@system]# init 6
```

VQE-S AMT or VCPT Unavailable

Symptom: To browse to VQE-S AMT or VCPT, you enter a valid IP address or fully qualified domain name, but the browser displays the message "Page Cannot Be Found" (status code 404) or "Service Temporarily Unavailable" (status code 503).

Explanation: Both AMT and VCPT require the Apache HTTP server service (httpd) and the Apache Tomcat application server service (tomcat5) to be running. When you attempt to browse to AMT or VCPT and one of these services is not running, the status codes are typically as follows:

- "Page Cannot Be Found" (status code 404) indicates that httpd is not running.
- "Service Temporarily Unavailable" (status code 503) indicates that tomcat5 is not running.

To check whether the httpd service is running, log in as root and issue following command:

```
[root@system]# /sbin/service httpd status

httpd (pid 15836 13179 2593 2592 2591 2590 2589 2588 2587 2586 2576) is running...
```

To check whether the tomcat5 service is running, log in as root and issue following command:

```
[root@system]# service tomcat5 status
Tomcat is running...
```

Remedy: If either httpd or tomcat5 is not running, log in as root and start the services that are stopped as follows:

```
[root@system]# service httpd start

[root@system]# service tomcat5 start
```

Verify that the httpd and tomcat5 services are running as shown earlier in the Explanation. If the httpd or tomcat5 processes continue to fail, check the log files for the services to determine the cause.

- The httpd log file is /etc/httpd/logs/error_log.
- The tomcat5 log files are /var/log/tomcat5/catalina.*date*.log.

For information on the log files for each service, see the vendor documentation for the Apache HTTP server or for the Apache Tomcat application server.

Channels Are Not Displayed in VQE-S AMT

Symptom: After channels are defined in VCPT and channel information is pushed to servers, VQE-S AMT does not display the channels.

Explanation: The most likely reason why AMT does not display the channels is that the VQE Server was not associated with the channels in VCPT.

To determine whether the channels are associated with this VQE Server, follow these steps:

Step 1 Log in to VCPT.

Step 2 Click the **Association** tab

Step 3 Select the VQE Server in the Select Server pull-down menu.

The channels should be in the Selected group. Also, make sure the VQE Server is defined with the role VQE-S. If the role is wrong, correct it with VCPT from the Servers tab. For information on updating server information, see the "Viewing or Updating Server Information" section on page 3-15.

If the channels are correctly associated with the VQE Server, it is possible that there were problems when VQE Server attempted to process the channels. Check the VQE Server log files for errors in channel processing. For information on these log files, see the "VQE Server and VQE Tools Logging and Log Files" section on page 5-2.

Remedy: If the channels have not been associated with the VQE Server in VCPT, associate the channels with VCPT from the Association tab. For information on associating channels with servers, see the "Defining Channel Associations for a Server" section on page 3-16.

VQE-S AMT Channels Status Summary Has No Graphs

Symptom: In the AMT VQE-S Status window (Figure 4-2 on page 4-4), the Channels Status Summary does not have graphs for the channels.

Explanation: If one or more channels are successfully created in AMT, the channels should appear in a Channels Status Summary graph of active, inoperative, and inactive channels in the VQE-S Status window. To be displayed, the graphs require that Adobe Flash Player be installed on the computer that hosts the browser accessing AMT.

Remedy: Download and install Adobe Flash Player on the computer that hosts the browser used to access AMT. The software is free and can be found at this URL:

http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash

It is recommended that you close all other open browser windows before performing the installation.

Channel-Provisioning Server Cannot Send Channel Information to VQE Server: Trusted Provisioning Client(s) Problem

Symptom: The channel-provisioning server (for example, VCPT or Cisco IPTV Services Delivery Server [ISDS]) cannot send channel information to a VQE Server.

Explanation: When the channel-provisioning server attempts to send channel information to a VQE Server, the send operation fails. On the VQE-S server, the VQE Configuration Tool parameter Trusted Provisioning Client(s) is not configured with the IP addresses for the channel-provisioning server.

If VCPT is the channel-provisioning server and the send operation fails because the Trusted Provisioning Client(s) parameter is not configured with the IP addresses of the Ethernet interfaces on the VCPT host, VCPT displays the following in the Status of Last Send column in its VCPT Servers Summary window:

```
Failed - Connection refused
```

In addition, the following error message is written to the VCPT log file (/usr/share/tomcat5/logs/vcpt.log):

```
ERROR: Unable to send the SDP File java.net.ConnectException: Connection refused
```

Remedy: Use the VQE Configuration Tool to configure the System Parameter > Trusted Provisioning Client(s) with the IP addresses of the channel-provisioning servers. For information on using the Configuration Tool, see the "Using the VQE Configuration Tool" section on page 6-4.

Note If VCPT is the channel-provisioning server, the IP addresses of all Ethernet interfaces (that have been assigned IP addresses) on the VCPT host must be configured as trusted provisioning clients on the VQE-S host.

Note If ISDS is the channel-provisioning server, for the Trusted Provisioning Clients(s), use the Broadcast System IP Address, which is configured on the ISDS VASP List. The VASP List can be found on the ISDS Administrative Console under ISDS -> Network Element Provisioning -> VASP.

Channel-Provisioning Server Cannot Send Channel Information to VQE Server: SSL Certificates Problems

Symptom: The channel-provisioning server (for example, VCPT or ISDS) cannot send channel information to a VQE Server.

Explanation: When the channel-provisioning server attempts to send channel information to a VQE Server, the send operation fails. On the VQE-S server or the channel-provisioning server or both, the Secure Sockets Layer (SSL) certificates are not valid or the needed items have not been copied to the correct locations.

If VCPT is the channel-provisioning server and the send operation fails because of SSL certificate problems, VCPT displays the following in the Status of Last Send column in its VCPT Servers Summary window:

```
Failed - Unable to find valid certification path to requested target
```

In addition, the following error message is written to the VCPT log file (/usr/share/tomcat5/logs/vcpt.log):

```
ERROR: Unable to send the SDP File javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target
```

Remedy: Make sure all SSL certificate-related items have been created correctly and the needed items have been copied to the correct locations on the VQE-S server and on the channel-provisioning server. For information on setting up SSL certificates, see the "Setting Up SSL Certificates" section on page 2-4.

Once the certificate-related items have been copied to the correct locations on the VQE-S server and on the channel-provisioning server, restart the httpd and tomcat5 services on both servers. For example, login as root and issue the following commands on both servers:

```
[root@system]# service httpd restart
[root@system]# service tomcat5 restart
```

Note If the tomcat5 service is not running when you try to restart it, an exception is displayed on the console when the attempt is made to stop the service. The exception can be ignored.

Unable to Connect Error When VCPT Tries to Send Channel Information

Symptom: When VCPT tries to send channel information to a VQE Server or VCDS, the send operation fails. In VCPT, the Servers tab displays "Failed - Unable to connect with Server" in the Status of Last Send column.

Explanation: Possible causes for the failed send operation are that the Apache HTTP server service (httpd) or the Apache Tomcat application server service (tomcat5) on the target VQE-S or VQE Tools server (hosting VCDS) is not running.

To check whether the httpd service is running, log in as root and issue following command:

```
[root@system]# service httpd status

httpd (pid 15836 13179 2593 2592 2591 2590 2589 2588 2587 2586 2576) is running...
```

To check whether the tomcat5 service is running, log in as root and issue following command:

```
[root@system]# service tomcat5 status

Tomcat is running...
```

Remedy: If either httpd or tomcat5 is not running, log in as root and start the services that are stopped as follows:

```
[root@system]# service httpd start

[root@system]# service tomcat5 start
```

Verify that the httpd and tomcat5 services are running as shown earlier in the Explanation. If the httpd or tomcat5 processes continue to fail, check the log files for the services to determine the cause.

- The httpd log file is /etc/httpd/logs/error_log.
- The tomcat5 log files are /var/log/tomcat5/catalina.*date*.log.

For information on the log files for each service, see the vendor documentation for the Apache HTTP server or for the Apache Tomcat application server.

Internal Server Error When VCPT Tries to Send Channel Information to VQE-S

Symptom: When VCPT tries to send channel information to VQE Server, you get an "Internal Server Error." Java exceptions in the catalina.out file indicate that there is an address conflict or unreachable address.

Explanation: The Internal Server Error is displayed when you use VCPT to send channel information to a VQE Server. The Status of Last Send column on the VCPT Servers tab shows the error.

From the CDE110 that hosts VQE-S, you are able to successfully **ping** the machine running the web browser used for VQE-S AMT, and **ping** the CDE110 hosting VCPT.

In the /usr/share/tomcat5/logs/catalina.out file of the Apache Tomcat application server, there are Java exceptions indicating an address conflict or unreachable address. For example:

```
java.net.BindException: Address already in use
at java.net.PlainSocketImpl.socketBind(Native Method)
at java.net.PlainSocketImpl.bind(Unknown Source)
...
java.net.SocketException: Network is unreachable
at java.net.PlainSocketImpl.socketConnect(Native Method)
at java.net.PlainSocketImpl.doConnect(Unknown Source)
```

Remedy: The Internal Server Error can be caused by one or more errors in the /etc/hosts file on the CDE110 that hosts VQE-S. Check the /etc/hosts file for typing or syntax errors, correct them, and save the file. Reboot the CDE110.

If you still receive the same Internal Server Error and Java exceptions, check the following files to see if you can find some indication for what is causing the error.

- /var/log/vqe/vqe.log
- /var/log/httpd/error_log
- /var/log/httpd/access_log
- /usr/share/tomcat5/logs/catalina.out
- /var/log/messages

Using the vqereport Command

The **vqereport** command can be useful for VQE troubleshooting. You can use the **vqereport** command to gather information on the VQE system's software configuration and hardware. The information can be used by the VQE administrator or Cisco technical support personnel to diagnose problems with VQE software or with the Cisco Content Delivery Engine 110 (CDE110) hardware.

Caution The **vqereport** command can take up to 15 minutes to complete and may cause VQE services (such as Unicast Retransmission) to be degraded for the duration of the execution.

The syntax for the **vqereport** command is as follows:

vqereport [-h | -help]

Syntax Description

-h | -help	Displays help information.

Usage Guidelines

The **vqereport** command generates a report file that, when the command finishes, is located in /root/*hostname.dateandtime*.tar.bz2. If appropriate, the report file can be attached to field issue reports for Cisco technical support.

Note You must log in as root to execute the **vqereport** command.

The **vqereport** command can be executed on the CDE110 that hosts VQE Server or on the CDE110 that hosts VCPT. The **vqereport** executable is located at /opt/vqes/bin/vqereport.

To have the operating system find the **vqereport** executable, you must set the PATH environment variable to include the location of the /opt/vqes/bin directory, or use the full path to **vqereport** when executing the command.

All information gathered is considered confidential, and Cisco will use this information for diagnostic purposes only.

Examples

The following example shows the execution of the **vqereport** command and some abbreviated output.

```
[root@system ~]# /opt/vqes/bin/vqereport

This utility will go through and collect some detailed information about the hardware and
setup of your VQE system. This information will be used to diagnose problems with your
system and will be considered confidential information. Cisco will use this information
for diagnostic purposes ONLY.
Please wait while we collect information about your system.
This process may take a while to complete....
No changes will be made to your system during this process.
NOTE: You can safely ignore a failed message. This only means a file we were checking for
did not exist.

Press ENTER to continue, or CTRL-C to quit.

**********************************************************************
Collect Redhat sysreport
```

```
**********************************************************************
Collect information of installed RPM packages
...
output omitted
...
Report file /root/<hostname>.20071115164635.tar.bz2 has been generated, please send it to
Cisco support.
```

Stopping, Starting, and Restarting VQE-S

The VQE-S application is a service that is started with the Linux **service** command.

To stop, start, or restart the VQE-S application, follow these steps:

Step 1 Log in as root.

Step 2 Depending on what is required, issue one of the following commands:

- To stop VQE-S, issue the following command:

  ```
  [root@system]# service vqes stop
  ```

- To start VQE-S, issue the following command:

  ```
  [root@system]# service vqes start
  ```

- To restart (stop and then start) VQE-S, issue the following command:

  ```
  [root@system]# service vqes restart
  ```

Stopping, Starting, and Restarting VCDS

The VQE Client Channel Configuration Delivery Server (VCDS) application is a service that is started with the Linux **service** command.

To stop, start, or restart the VCDS application, follow these steps:

Step 1 Log in as root.

Step 2 Depending on what is required, issue one of the following commands:

- To stop VCDS, issue the following command:

  ```
  [root@system]# service vcds stop
  ```

- To start VCDS, issue the following command:

  ```
  [root@system]# service vcds start
  ```

- To restart (stop and then start) VCDS, issue the following command:

  ```
  [root@system]# service vcds restart
  ```

CHAPTER 6

Configuring VQE Server and VQE Tools

This chapter describes these VQE Configuration Management System software components: VQE Configuration Tool, Configuration Engine, and the VCDB Parser. The chapter also provides task-based information on the following topics:

The chapter also provides information on the VQE Configuration Engine and the VCDB Parser.

Note This chapter describes VQE configuration management facilities that are used *after the VQE-S or VQE Tools server has been initially configured* (on first power on). For information on initial configuration, see Chapter 2, "Getting Started with the VQE Startup Configuration Utility."

Table 6-1 provides acronyms or terms and descriptions for the major components of the VQE Configuration Management System that you need to be familiar with.

Table 6-1 VQE Configuration Management System Components

Acronym or Term	Expansion and Description
VCDB	*VQE Configuration Database* stores key-value pairs with the parameters and values you have specified with Configuration Tool or by manually editing the vdcb.conf file (the VCDB file).
CT	VQE *Configuration Tool* provides a menu-driven user interface that you use to display VCDB parameters and their values, add parameters to VCDB, and specify values for VCDB parameters needed for the operation of a VQE Server or VQE Tools system. See the "Using the VQE Configuration Tool" section on page 6-4.
CE	VQE *Configuration Engine* is used to apply the configuration values in VCDB (vcdb.conf) to the running VQE-S or VQE Tools server. CE also ensures that the configuration values in the VCDB and the configuration on the CDE110 server are synchronized. See the "VQE Configuration Engine" section on page 6-10.

Table 6-1 VQE Configuration Management System Components

Acronym or Term	Expansion and Description
CMS	VQE *Configuration Management System* includes CT, CE, and the VCDB Parser.
/etc configuration files	Configuration files in the directories under /etc. This is the set of configuration files for the CDE110 that hosts VQE Server or VQE Tools. These files include the existing VCDB file, all history VCDB backup files, the password file, the SDP file, and so on.

Managing /etc Configuration Files Using the VQE CMS Versus Editing the Files Manually

Starting with Cisco VQE Release 3.0, the configuration files under the /etc directory can be managed in two ways:

- Managing /etc Configuration Files with the VQE CMS, page 6-2
- Managing /etc Configuration Files by Manually Editing the Files, page 6-3

On both the VQE-S and VQE Tools hosts, the /etc configuration files are used for VQE software configuration and for CDE110 system and network configuration. For information on VQE, system, and network parameters, see Appendix A, "VQE, System, and Network Parameters."

Note Using the VQE CMS is the recommended method for managing VQE, system, and network configuration files.

For some deployments, it may be necessary to manage one or more /etc configuration files by manually editing the files because the set of CDE110 system and network parameters that can be managed by the VQE CMS does not include all system and network parameters that your implementation requires. *Those /etc configuration files that you manage manually are removed from the control of the VQE CMS.*

Managing /etc configuration files by manually editing the /etc configuration files has this *disadvantage*: When it becomes necessary to upgrade the VQE software to a later release, changes to the /etc files that you have made by manual file editing (outside the control of the VQE Configuration Management System) will, in most cases, be lost.

Managing /etc Configuration Files with the VQE CMS

Managing /etc configuration files with the VQE CMS consists of using the Configuration Tool or manual editing of the vcdb.conf file to set parameter values, and using the Configuration Engine to apply parameter values to the CDE110 server. Using the VQE CMS is the recommended method for managing VQE, system, and network configuration files. The VQE CMS automates much of the work related to configuring a VQE system. If you manage /etc files with the VQE CMS, the CMS automatically does the following:

- Provides the correct syntax for each /etc file parameter
- Checks for the allowed set of values for each /etc file parameter
- Restarts the appropriate system processes or reboots the CDE110 server so that changed parameter values take effect

- When a VQE software upgrade is required, automatically preserves your deployment's configuration in the upgraded software

In addition to this automation, using the VQE CMS to manage /etc configuration files makes it possible to efficiently setup multiple CDE110 servers. With the exception of some server-specific parameter values, the same VCDB set of parameter values (the vcdb.conf file) may be appropriate for multiple CDE110 servers.

Managing /etc Configuration Files by Manually Editing the Files

You can manage one or more /etc configuration files manually by editing them with a text editor. *In this scenario, those /etc configuration files that you manage manually are removed from the control of the VQE CMS.* For some deployments, it may be necessary to manage one or more /etc configuration files manually because the set of CDE110 system and network parameters that can be managed by the VQE CMS does not include all system and network parameters that your implementation requires.

For the VQE software itself, all user-configurable parameters can be managed with the VQE CMS. The essential VQE software parameters can be configured with VQE Configuration Tool. All VQE software parameters can be configured by manually editing the VCDB file (vcdb.conf).

With the VQE CMS, the Configuration Engine is used to apply VCDB values to the set of /etc configuration files. Each time VQE Configuration Engine runs, it performs a checksum comparison to determine which /etc configuration files have been manually edited. If an /etc configuration file has been manually edited, the Configuration Engine assumes that you (the VQE administrator) are managing the files manually, and Configuration Engine does not apply VCDB values to that /etc configuration file. When the Configuration Engine detects a checksum mismatch for an /etc configuration file, CE logs a warning message and, if CE is being used interactively, CE also displays the message on standard output.

Note The configuration parameters for the VQE software (and all system and network components) are contained in the vcdb.conf file, which can be manually edited. *If you manually edit the VQE parameters in vcdb.conf, you must use the VQE Configuration Engine to apply the VQE parameters to the VQE configuration files under /etc.* For the list of user-configurable VQE parameters, see Appendix A, "VQE, System, and Network Parameters."

When you manually manage some /etc configuration files and you later decide you would like the VQE CMS to start managing one or more such files, you can use the **vqe_cfgtool** command with the **-fix_checksum** option to have the checksum recomputed so that the manually edited /etc configuration files pass the checksum verification. This will allow these manually edited files to be managed through the VQE CMS, while at the same time preserving the manually edited sections of the file.

When you manually manage some /etc configuration files and you later decide you would like to return to using the factory default version of the /etc file, you can use the **vqe_cfgtool** command with the **-fix_config** option. When -**fix_config** is specified, **vqe_cfgtool** discards each /etc configuration file where there is a checksum mismatch and replaces it with the factory default /etc configuration file from the RPM package. **vqe_cfgtool** then recomputes the checksum using the factory default file

Using the VQE Configuration Tool

VQE Configuration Tool (CT) provides a menu-driven user interface that you use to display VCDB parameters and their values, add parameters to VCDB, and specify values for VCDB parameters needed for the operation of a VQE Server or VQE Tools system. Only essential parameters required for a VQE-S or VQE Tools system are configurable with CT. For those parameters that are not configurable with CT, you can use a text editor to manually modify the vcdb.conf file, which holds the VCDB. For information on editing vcdb.conf, see the "Manually Editing the VCDB File" section on page 6-12.

From the Linux command line, you start CT using the **vqe_cfgtool** command with the **-config** option. You must have root privileges to invoke **vqe_cfgtool**. For information on the **vqe_cfgtool** command, see the "Using the VQE Configuration Tool Command-Line Options" section on page 6-16.

Note This section provides information on using CT when it is started with **vqe_cfgtool -config**. For information on the Cisco VQE Startup Configuration Utility, see Chapter 2, "Getting Started with the VQE Startup Configuration Utility."

Starting the Configuration Tool and Using the Root Menu

When CT is started with **vqe_cfgtool -config**, it calls the VCDB Parser to parse existing VCDB contents.

- If the Parser finds errors, CT displays the Parser output and quits. The Parser also logs the errors in the /var/log/vqe/vqe.log file.

Note To correct the parsing errors, you must use a text editor to manually edit the vcdb.conf file. You modify the file to correct parameter errors and remove parameters not recognized by the Parser.

- If the Parser finds no errors, CT displays the VQE Configuration Tool Root Menu:

```
VQE Configuration Tool Root Menu:

     1) System Parameters
     2) Network Parameters
     3) VQE-S Parameters
     S) Save and Exit
     A) Save/Apply and Exit
     E) Exit without saving
```

Table 6-2 describes the choices on the CT Root Menu. You enter the number or letter for your choice.

Table 6-2 CT Root Menu Choices

Choice	Description
1) System Parameters	Configures the system parameters
2) Network Parameters	Configures the network parameters
3) VQE-S Parameters	Configures the VQE-S parameters. This choice is present only on the VQE-S system.
S) Save and Exit	Saves the changes you have made to the VCDB parameters and exits CT. Any new parameter values *are not applied* to the configuration files under /etc.

Table 6-2 CT Root Menu Choices (continued)

Choice	Description
A) Save/Apply and Exit	Saves the changes you have made to the VCDB parameters, applies any new parameter values to the configuration files under /etc, restarts services (as needed), and exits CT.
E) Exit without saving	Exits CT. Any changes you have made to the VCDB parameters *are not saved*.

Using the Configuration Tool Menus

The System Parameters, Network Parameters, and VQE-S Parameters menus and prompts are self-documenting and do not require line-by-line explanation. The System Parameters menu, which is typical of the menu format, is as follows:

```
VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          vqe_server1
   2) DNS Server(s):                     []
   3) DNS Search Domain:                 []
   4) Timezone:                          [America/New_York]
   5) NTP Server(s):                     []
   6) SNMP RO Community String:          []
   7) SNMP System Location:              []
   8) SNMP System Contact:               []
   9) SNMP Trap Listener(s):             []
   10) Trusted Provisioning Client(s)    []
   R) Go to Root Menu

   Enter a number choice followed by a letter 'd'(eg. 3d) will reset the
   corresponding parameter to its factory default value.

Enter your choice:
```

To the right of the VQE Configuration Tool menu choice, one of the following is displayed:

- If a value is displayed, it is the current user-defined value for the parameter in VCDB. In the preceding example, vqe_server1 is the current user-defined value in VCDB for the Hostname parameter.
- If a value enclosed by brackets is displayed, this is the default value—the value used when no user-defined value has been specified. In the preceding example, America/New York is a default value.
- If empty brackets ([ ]) are displayed, there is no current user-defined value and no default value for the parameter.

For the default values used for specific parameters, see the file /etc/opt/vqes/vcdb.conf.sample.

In the System Parameters menu and similar menus, the numbered menu choices allow you to configure the set of relevant parameters. The lettered menu choice “R) Go to Root Menu” returns you to the Root menu.

CT allows you to specify values for the system, network, and VQE parameters that require configuration as well as some of the most common optional parameters. Table 6-3 tells you where to find guidance on the system, network, and VQE-S parameters that are configurable with CT.

Note When a VCDB parameter is not configurable with Configuration Tool, you can specify the parameter and a value for it by manually editing the /etc/opt/vqes/vcdb.conf file. For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-12.

Table 6-3 Where To Find Information on Configuration Tool Parameters

Configuration Tool Parameter	Where To Find Information
System Parameters	
Hostname	Hostname for the CDE110, page 2-17
DNS Server(s) DNS Search Domain	Domain Name System (DNS) IP Addresses and a Search Domain, page 2-17
Timezone	System Timezone, page 2-17
NTP Server(s)	NTP Server IP Addresses, page 2-17
SNMP RO Community String SNMP System Location SNMP System Contact SNMP Trap Listeners	SNMP Read-only Community String, Location, Contact, and Trap-Listener IP Addresses or Hostnames (Optional), page 2-17
Trusted Provisioning Client(s)	Trusted Provisioning Clients, page 2-19
Network Parameters	
Eth1 Interface Eth2 Interface Eth3 Interface Eth4 Interface Eth5 Interface Eth6 Interface	Ethernet Interface Configurations IP Addresses and Prefix Lengths, page 2-18 **Note** Earlier models of the CDE110 have four Ethernet ports (eth1 to eth4). These models did not have the Intel PRO/1000 PT Dual Port Server Adapter that provides the eth5 and eth6 ports.
Management Route(s)	IP Address and Prefix Length and Gateway Address for a Static Route to a Management Network (Optional), page 2-18
VQE-S Traffic Routing Type	VQE-S Traffic Routing Type (VQE-S Host Only), page 2-19
Static Routing Parameters	Default Gateway IP Addresses for Multipath Static Routes (VQE-S Host Only), page 2-19
OSPF Parameters	OSPF Configuration (VQE-S Host Only), page 2-20
VQE-S Parameters (for VQE-S Host Only)	
Log Priority	vqe.vqes.log_priority parameter in Table A-1
Excess Bandwidth Fraction	vqe.vqes.excess_bw_fraction parameter in Table A-4
VQE-S Traffic Interface(s)	Ethernet Interfaces That Will Be Used for VQE-S Traffic (VQE-S Host Only), page 2-21

Entering Data for Configuration Parameters

In the CT menus, when you enter a number for your choice, a set of prompts asks you for the required parameter information. This section provides information on using the System Parameters menu. Using the other CT menus is similar.

VCDB additions are appended to the end of the vcdb.conf file. That is, VCDB additions are added after the parameters that are already in the file.

The procedures for entering configuration data varies slightly depending on whether the parameter can have only one definition or multiple definitions.

Entering Data for Parameters That Can Have Only One Definition

To enter data for a VCDB configuration parameter *that can have only one definition*, do the following:

Step 1 When the System Parameters menu is displayed, enter the number for the parameter you want to configure and press **Enter**. In this example, a single definition is specified for the Hostname parameter.

```
VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          [localhost]
   2) DNS Server(s):                     []
   3) DNS Search Domain:                 []
   4) Timezone:                          [America/New_York]
   5) NTP Server(s):                     []
   6) SNMP RO Community String:          []
   7) SNMP System Location:              []
   8) SNMP System Contact:               []
   9) SNMP Trap Listener(s):             []
   R) Go to Root Menu

   Enter a number choice followed by a letter 'd'(eg. 3d) will reset the
   corresponding parameter to its factory default value.

Enter your choice: 1
```

Step 2 At the Hostname prompt, enter a hostname and press **Enter**.

```
Enter the Hostname of this server: vqe_server1 <Enter>
```

For a parameter that allows only one definition, enter the needed data for the parameter and press **Enter**. Hostname allows only one definition. In this case, CT does not prompt for a multiple entries.

The System Parameters menu is displayed with the newly entered parameter value displayed to the right of the menu choice.

```
VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          vqe_server1
   2) DNS Server(s):                     []
   3) DNS Search Domain:                 []
 ...
```

Entering Data for Parameters That Can Have Multiple Definitions

To enter data for a VCDB configuration parameter *that can have multiple definitions*, do the following:

Step 1 When the System Parameters menu is displayed, enter the number for the parameter you want to configure and press **Enter**. In this example, multiple definitions are specified for the DNS Server(s) parameter.

```
VQE Configuration Tool <System Parameters> Menu:
```

```
   1) Hostname:                          vqe_server1
   2) DNS Server(s):                     []
   3) DNS Search Domain:                 []
   4) Timezone:                          [America/New_York]
   5) NTP Server(s):                     []
   6) SNMP RO Community String:          []
   7) SNMP System Location:              []
   8) SNMP System Contact:               []
   9) SNMP Trap Listener(s):             []
   10) Trusted Provisioning Client(s)    []
   R) Go to Root Menu

   Enter a number choice followed by a letter 'd'(eg. 3d) will reset the
   corresponding parameter to its factory default value.

Enter your choice: 2
Configure DNS Server(s). Enter one DNS server on each subsequent line.
Hit Enter at the prompt will complete this configuration.
```

Step 2 For a parameter that allows multiple definitions, enter one or more definitions on separate lines. To complete the configuration, press **Enter** at the prompt without entering data. For example, DNS Server(s) allows multiple definitions. In this case, CT prompts for multiple entries.

```
Enter a DNS server IP address: 1.2.3.4 <Enter>
Enter a DNS server IP address: 5.6.7.8 <Enter>
Enter a DNS server IP address: <Enter>
```

The System Parameters menu is displayed with the newly entered parameter values displayed to the right of the menu choices.

```
VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          vqe_server1
   2) DNS Server(s):                     1.2.3.4, 5.6.7.8
   3) DNS Search Domain:                 []
 ...
```

Entering New Values for Parameters That Have a Currently Defined Value

For a parameter that has one or more currently defined values in VCDB, the Configuration Tool does not allow you to add additional values or delete a subset of the existing parameter values. When you add a new value for a parameter, all old values for that parameter are deleted.

Note When you specify a value for a parameter that already has a user-defined value specified, the old value for that parameter is deleted and the value you have entered becomes the current value.

If there are multiple existing definitions for a parameter and you specify a value for that parameter, all existing definitions are deleted and the value you have entered becomes the current value.

To enter a new value for a parameter that currently has a value defined in VCDB, do the following:

Step 1 At the System Parameters menu, enter the number of the parameter. For example:

```
Enter your choice: 2
```

The prompt for the parameter is displayed:

```
Configure DNS Server(s). Enter one DNS server on each subsequent line.
Hit Enter at the prompt will complete this configuration.

Enter a DNS server IP address:
```

Step 2 Enter the new parameter value and press **Enter**. For example:

```
Enter a DNS server IP address: 9.9.9.9
```

Repeat this step if you want to add more parameter values. Each parameter value that you enter is added to VCDB in a cumulative manner.

Step 3 If you have no further parameter values to add, press **Enter**.

```
Enter a DNS server IP address: <Enter>
```

When the System Parameters menu is displayed, the new parameter value (9.9.9.9) replaces any existing definitions and values.

As an example, assume that prior to entering a new value for a parameter, the DNS Server(s) parameter had two definitions, one with the value 1.2.3.4 and one with the value 5.6.7.8:

```
VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          vqe_server1
   2) DNS Server(s):                     1.2.3.4, 5.6.7.8
   ...
```

After the new value (9.9.9.9) is entered, the DNS Server(s) parameter has one definition with the value 9.9.9.9:

```
VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          vqe_server1
   2) DNS Server(s):                     9.9.9.9
   ...
```

Reverting to the Default VCDB Values

To revert to the default VCDB value when an existing user-defined value has been specified, do the following:

When the System Parameters menu is displayed, enter the number of the parameter followed by the letter "d" and press **Enter**. For example:

```
VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          vqe_server1
   2) DNS Server(s):                     9.9.9.9
   3) DNS Search Domain:                 []
   4) Timezone:                          []
   5) NTP Server(s):                     []
   6) SNMP RO Community String:          []
   7) SNMP System Location:              []
   8) SNMP System Contact:               []
   9) SNMP Trap Listener(s):             []
   10) Trusted Provisioning Client(s)    []
   R) Go to Root Menu

   To reset a parameter to its factory default, enter
   its number choice followed by the letter 'd' (e.g. 3d).
```

```
   Default values are displayed inside square brackets [].

Enter your choice: 1d <Enter>
```

Any existing values for the parameter that have been set in VCDB are deleted. The default value for the parameter is in effect.

In this example, when the System Parameters menu is displayed, the default value (localhost) is listed to the right of the parameter name (Hostname).

```
VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          [localhost]
   2) DNS Server(s):                     9.9.9.9
   ...
```

VQE Configuration Engine

Configuration Engine (CE) is used to apply the configuration values in VCDB (vcdb.conf) to the running VQE-S or VQE Tools server. CE also ensures that the configuration values in vcdb.conf and the configuration on the server are synchronized.

CE is invoked in the following ways:

- Each time the VQE-S or VQE Tools server reboots, CE runs automatically.
- From the Configuration Tool root menu, choose menu choice A—Save/Apply and Exit.
- From the Linux command line, use the **vqe_cfgtool** command with the **-apply** option to start CE.

For information on the **vqe_cfgtool** command, see the "Using the VQE Configuration Tool Command-Line Options" section on page 6-16.

When CE is invoked, it does the following:

1. CE (by calling the VCDB Parser) parses the entire vcdb.conf file for parameter validity. A line in vcdb.conf is invalid if it has unknown parameter keywords or syntax errors. If any invalid lines are found, CE logs an error for each invalid line and completes file parsing, but does not proceed to update the /etc configuration files. Instead, CE quits after parsing is complete. CE logs any invalid lines to the /var/log/vqe/vqe.log file on the VQE-S server or on the VQE Tools server. CE also displays parsing errors on standard output when run interactively.

   If CE quits because of invalid lines in the vcdb.conf file, *you must manually edit vcdb.conf to correct the invalid lines*. Then issue the command **vqe_cfgtool -apply** to apply the values in vcdb.conf to the server's /etc configuration files.

Note When CE is automatically invoked during system reboot, no interactive questions are displayed. You are not prompted on whether to continue if CE detects a checksum mismatch for an /etc configuration file, or before changes are made to the running configuration and services restarted if a restart is needed to put a new parameter value into effect.

When CE is invoked using the **vqe_cfgtool** command and the **-apply prompt-off** option, no interactive questions are displayed before changes are made to the running configuration.

2. CE verifies the checksum of each /etc configuration file managed by the CMS. If a checksum is different, this usually means that changes outside of VCDB control (manual changes) have been made to this /etc file since the last CE update. If such a file is found, CE logs the file name and

checksum mismatch to /var/log/vqe/vqe.log. CE does not apply VCDB values to /etc files where there is a checksum mismatch. To fix a checksum mismatch so that the /etc configuration file is again managed by the CMS, use **vqe_cfgtool** with the option **-fix_checksum**.

If CE cannot find or cannot read an /etc file, CE logs the error and does nothing. *In this case, you must replace the missing file before normal VQE-S operations can continue.* You can use **vqe_cfgtool** with **-fix config** to replace missing or unreadable /etc configuration files with the factory default configuration files.

Note Copies of the factory default configuration files are in the /vqe-etc/etc-pristine directory.

3. For synchronization, CE checks that all parameters in VCDB exist in the files under /etc, and that these parameters are effective within the running application. If there is a difference between the configuration values in VCDB and a configuration file under /etc, CE applies the VCDB values to the /etc configuration file where the differences exist.

   VCDB is the authority for overall system configuration. If there is a conflict between VCDB and the configuration on the running system, the VCDB value always overrides the value in the /etc file.

4. CE backs up the VCDB files. The current running VCDB configuration is saved in the file /etc/opt/vqes/vcdb-running.conf. When CE finds a difference between the VCDB file (vcdb.conf) and the vcdb-running.conf file, it does the following:

   - Updates the latest running configuration file with the values in vcdb.conf.
   - Saves a copy of vcdb.conf in the archive directory (/etc/opt/vqes/archive/).

   The name of the archived file contains the software version, date, and time stamp (for example, vcdb-3.2.0-20080204.1150.conf). Up to 100 VCDB archived backup files can be saved. Backup files over the 100 file limit are deleted based on the time stamp in the filename. Oldest files are deleted first.

5. After applying the VCDB values, CE (if needed) restarts the associated services or reboot the system. CE restarts only those services that had a VCDB value applied to the corresponding /etc configuration file and that require a service restart or reboot for the changed value to take effect.

Note In interactive mode, CE warns you when service interruptions are required to put a VCDB value into effect for the service, or when a reboot is required to put a VCDB value into effect. You can choose to apply the changes and restart services, or to terminate CE processing.

- If the system.hostname parameter value has changed, CE reboots the server, and all services are restarted.
- If the system.hostname parameter value has not changed, CE restarts individual services in the following order:

  1. network and routing
  2. iptables
  3. Domain Name System (DNS)
  4. Network Time Protocol (NTP)
  5. Net-SNMP
  6. VQE-S Process Monitor (VQE-S server only)

VCDB Parser

When the VCDB Parser starts, it reads the /etc/opt/vqes/vcdb.conf.sample file. This file contains information on all the valid VCDB parameters and their syntax. Next the VCDB Parser reads the /etc/opt/vqes/vcdb.conf file line by line, validates the syntax and parameter keywords, and outputs messages as it proceeds. The VCDB Parser writes its output informing you about any problems to the /var/log/vqe/vqe.log file and to standard output (if the Parser is used in an interactive mode). The VCDB Parser does not stop when it finds an error but finishes parsing the whole VCDB file.

There are several categories of VCDB Parser output messages: debug, info, warning, error. The format for the log messages is the same as is used for VQE-S logging. For information on log entry format, see "VQE Server and VQE Tools Logging and Log Files" section on page 5-2.

In addition to checking syntax and parameter keywords, the VCDB Parser also performs limited semantic checks. For example, if identical values are specified for a parameter that requires unique values, the VCDB Parser logs a warning and continues.

The VCDB Parser is invoked in the following ways:

- Each time the Configuration Tool runs, the VCDB Parser is automatically invoked.
- Each time the Configuration Engine runs, the VCDB Parser is automatically invoked.
- From the Linux command line, use the **vqe_cfgtool** command with the **-parse** option to start the VCDB Parser.

For information on the **vqe_cfgtool** command, see the "Using the VQE Configuration Tool Command-Line Options" section on page 6-16.

Manually Editing the VCDB File

The VQE Configuration Tool allows you to specify values for the required system, network, and VQE parameters. It also allows you to configure some of the most common optional parameters. When a VCDB parameter is not configurable with Configuration Tool, you can specify the parameter and a value for it by manually editing the /etc/opt/vqes/vcdb.conf file.

This section provides information on how you specify parameters in the vcdb.conf file and how you use the reference information in the vcdb.conf.sample file to edit vcdb.conf:

- Using VCDB File Syntax, page 6-13
- Understanding the vcdb.conf.sample File, page 6-14

For information on the VCDB parameters, see Appendix A, "VQE, System, and Network Parameters."

Note When you manually edit the vcdb.conf file to modify, add, or remove parameters, *you must apply the parameter values in vcdb.conf to the server /etc configuration files in order for the changed parameters to take effect.* To apply the values, use the **vqe_cfgtool** command with the **-apply** option. For information on **vqe_cfgtool**, see the "Using the VQE Configuration Tool Command-Line Options" section on page 6-16.

Tip After you manually edit and save the vcdb.conf file, use the **vqe_cfgtool** command with the **-parse** option to check that your changes have not created any errors in the file.

Using VCDB File Syntax

This section provides information on the syntax rules you need to follow when editing the vcdb.conf file.

The vcdb.conf file contains a list of key-value pairs. Each key-value pair is associated with a system, network, or VQE parameter that is used to configure a VQE-S or VQE Tools system. Each key-value pair has the following syntax:

section.subsection.parameter = "*value*"

Each key is associated with a section and subsection. Section names are vqe, system, and network. Some key-value pair examples are as follows:

```
vqe.vqes.exporter_enable = "TRUE"

system.global.hostname = "iptv_host"

network.eth1.addr = "11.2.9.2/24"
```

The syntax rules for the vcdb.conf file are as follows:

- Allowed VCDB keys and their syntax are defined in the vcdb.conf.sample file.
- Each key is case-sensitive.
- The key and its value are separated by an equal sign (=).
- The value is enclosed by quotation marks ("*value*").
- A comment line starts with #. The VCDB Parser ignores these lines.
- The following are allowed but ignored:
  - Leading space before a key
  - Leading space before and trailing space after a value
  - Spaces before or after the equal sign (=)

Multiple Definitions

If a parameter definition appears more than once in vcdb.conf when multiple definitions of the parameter are not allowed, the VCDB Parser logs an error and terminates. None of the values in vcdb.conf are applied to the /etc configuration files.

When this multiple definition error occurs, you must edit vcdb.conf manually to correct the items that are in error.

Parameter Order

For those parameters that can only appear once in VCDB, parameter order is not important.

If a parameter can have multiple values, it requires multiple lines of definition. Each line defines one value. The order of these definitions in the vcdb.conf file is important because the same order is kept in the /etc configuration files. Consider the following vcdb.conf file items:

```
system.snmp.trap_listener = "1.2.3.4"

system.snmp.trap_listener = "5.6.7.8"
```

When the Configuration Engine applies these two `system.snmp.trap_listener` items to the /etc/snmp/snmpd.conf file, listener 1.2.3.4 is defined in the snmpd.conf file before listener 5.6.7.8 because 1.2.3.4 is specified first in the vcdb.conf file.

Understanding the vcdb.conf.sample File

For each VQE release, the vcdb.conf.sample file provides user reference information on the parameters recognized by the VCDB Parser. For each VCDB parameter, vcdb.conf.sample contains the key-value pair, syntax rules, range of allowed values, and other information. The vcdb.conf.sample file is located in /etc/opt/vqes/vcdb.conf.sample. It is a read-only file and should not be moved.

To determine how to specify a VCDB parameter in vcdb.conf, you read about the parameter and its usage in vcdb.conf.sample. Some parameter examples from vcdf.conf.sample are as follows:

```
# system.global.hostname="localhost"
# Description: "Fully Qualified Domain Name (FQDN) or hostname of the system."
# Type: String, minimum length 3 characters, maximum length 200 characters
# Default value: localhost
# Required: N
# Service interruption: "System reboot. "
# Allow multiple definitions: N
# Target /etc file: ""127.0.0.1" in /etc/hosts and "HOSTNAME" in /etc/sysconfig/network"

# network.eth1.addr=""
# Description: "IP address and network mask length for interface eth1 in the for
m ""1.2.3.4/24""
# Type: IP_Prefix
# Default value:
# Required: N
# Service interruption: "Potential network traffic interruption. "
# Allow multiple definitions: N
# Target /etc file: ""IPADDR" and "NETMASK" in /etc/sysconfig/network-scripts/if
cfg-eth1"

# vqe.vqes.log_priority="4"
# Description: "Global logging priority level for all VQE applications. Valid va
lues are 0-6. 0 - EMERGENCY, system is unusable, 1 - ALERT, action must be taken
 immediately, 2 - CRITICAL, critical conditions, 3 - ERROR, error conditions, 4
- WARNING, warning conditions, 5 - NOTICE, normal but significant condition, 6 -
 INFO, informational. Levels less than or equal to log-level will be logged.",
# Type: Integer, minimum value is 0, maximum value is 6
# Default value: 4
# Required: N
# Service interruption: "VQE Process Monitor restart."
# Allow multiple definitions: N
# Target /etc file: ""log-level" in /etc/opt/vqes/.vqes.conf"
```

In vcdb.conf.sample, the first line of an entry is the key-value pair for the parameter. Table 6-4 lists the vcdb.conf.sample reference information that describes each VCDB parameter.

Table 6-4 Parameter Information in the vcdb.conf.sample File

Field	Description
Description	Explains how the parameter is used.
Type	Specifies one of the following data types and, if applicable, the range of values allowed. • Integer—A whole number. • Float—A floating-point number (for example, 10.25 or –5.75 or .50). The allowed floating-point numbers correspond to those allowed by the Perl float type. • String —One or more characters. The set of characters allowed varies depending on the parameter. • Boolean—Either true or false. • IP—An IPv4 address in dotted-decimal form (for example, 10.0.0.1). The IP address must be in the range allowed for an IPv4 address. • IP_PREFIX—An IP address and prefix length in the form *ip-address*/*prefix-length* (for example, 10.0.0.0/8). The *ip_address* is the same as in IP. The *prefix-length* must be in the range 0 to 32. • Route—A route in the format *ip-address*/*prefix-length* via *ip-address* (for example, 10.0.0.0/8 via 11.2.9.1). Each *ip_address* is the same as in IP. The *prefix-length* must be in the range 0 to 32. • Host—Either an IP address or a string representing a fully qualified domain name (for example, myhost.company.com). The IP address is the same as in IP.
Default value	Specifies a default value. If there is no default value, this field is blank.
Required	Specifies one of the following: • Y—The parameter must be defined, and there is no default value. • N—The parameter does not have to be defined. You can define a parameter by using the Configuration Tool or by manually editing the vcdb.conf file with a text editor.
Service interruption	Indicates whether VQE services will be interrupted when the parameter definition is applied to the relevant configuration file (for example, when you invoke the **vqe_cfgtool** command with the **-apply** option).
Allow multiple definition	Specifies one of the following: • Y—The parameter can be specified more than once in the vcdb.conf file. • N—The parameter can be specified only once in the vcdb.conf file.
Target /etc file	Specifies the configuration file under /etc that will be written to when the parameter is applied. Also indicates the configuration items that will be written to the /etc configuration file. In the `system.global.hostname` parameter example preceding this table, "Target /etc file" indicates that a line 127.0.0.1 *host_name* will be written to the file /etc/hosts, and a line HOSTNAME=*host_name* will be written to the /etc/sysconfig/network file. The *host_name* is the value specified for `system.global.hostname`. The exact syntax for the line that will be added to the /etc file is not specified in the "Target /etc file" field.

Using the VQE Configuration Tool Command-Line Options

The **vqe_cfgtool** command performs a variety of configuration tasks related to the VQE Configuration Database (VCDB) and the configuration files under the /etc directory on a VQE-S or VQE Tools server.

The syntax for the **vqe_cfgtool** command is as follows:

vqe_cfgtool [**-apply** [**prompt-off**] | **-backup** | **-config** | **-fix_checksum** | **-fix_config** | **-help** | **-parse** [*full_pathname*] | **-restore** *full_pathname* | **-sanity_check** | **-version**]

Syntax Description

-apply [**prompt-off**]	Launches the Configuration Engine to apply the values in VCDB to the server /etc configuration files. If you specify **prompt-off**, no interactive questions are displayed before changes are made to the running configuration.
-backup	Copies all files under /etc into a tar file and saves the tar file in /vqe-etc/vqe-*release-hostname-timestamp*.tar.gz.
-config	Launches the Configuration Tool so that you can modify the VQE configuration parameter values that are stored in VCDB.
-fix_checksum	Recomputes the checksum for each /etc configuration file that has a checksum mismatch.
-fix_config	Discards the current copy of each /etc configuration file where there is a checksum mismatch and replaces it with the original copy of the file that comes with the RPM package.
-help	Displays information on how to use the **vqe_cfgtool** command and its options. If no valid option is specified when **vqe_cfgtool** is invoked, **-help** is the default.
-parse [*full_pathname*]	Performs validation of the VCDB contents (parameters, values, syntax, and so on) for the current vcdb.conf file. If *full_pathname* is specified, that file is parsed rather than the current vcdb.conf file.
-restore *full_pathname*	Extracts the contents of the tar file specified in *full_pathname*, and replaces all /etc configuration files with the tar file contents. The tar file is typically created with **vqe_cfgtool -backup**.
-sanity_check	Compares the parameter values in VCDB with the values in the /etc configuration files, and displays any differences on the command line.
-version	Displays software version information.

Usage Guidelines

The **vqe_cfgtool** command is available on the VQE-S or VQE Tools server. The tool is located in the /opt/vqes/bin directory. You must have root privileges to invoke **vqe_cfgtool**. The **vqe_cfgtool** command does not respond to Ctrl-C and cannot be exited prematurely once execution has started.

The **vqe_cfgtool** command writes its output to standard output (by default, it is displayed on the command line) and to the /var/log/vqe/vqe.log file.

-apply Option

When **-apply** is specified, **vqe_cfgtool** invokes the Configuration Engine to apply the VCDB values to the server /etc configuration files. After applying the VCDB values, CE (if needed) will restart the associated services or reboot the system. CE restarts only those services that had a VCDB value applied to the corresponding /etc configuration file and that require a service restart or reboot for the changed value to take effect. For a detailed description of Configuration Engine processing, see the "VQE Configuration Engine" section on page 6-10.

If **prompt-off** is specified with the **-apply** option, you are not prompted on whether to continue for these two situations:

- If the Configuration Engine detects a checksum mismatch for an /etc configuration file. If a checksum is different, this usually means that unauthorized changes (that is, changes outside of VCDB control) have been made to this file after the last CE update.
- Before changes are made to the running configuration and services restarted (if a restart is needed to put any new parameter values into effect).

-backup and -restore Options

When **-backup** is specified, **vqe_cfgtool** saves all files under /etc into a tar file and saves the tar file in /vqe-etc/vqe-*release-hostname-timestamp*.tar.gz. After **vqe_cfgtool** saves the tar file, it displays the location of the tar file and reminds you to use the **scp** command to copy the file to a remote server. The **-backup** option is typically used before **-config** or **-apply** so that a backup copies of the /etc configuration files are available for rollback purposes.

When **-restore** *full_pathname* is specified, **vqe_cfgtool** extracts the contents of the tar file specified in *full_pathname*, and replaces all /etc configuration files with the tar file contents. The *full_pathname* argument usually gives the path to a tar file that has been created with **-backup**.

-config Option

When **-config** is specified, **vqe_cfgtool** parses the vcdb.conf file and, if there are no errors, runs the Configuration Tool so you can modify parameter values in VCDB. For information on how Configuration Tool works, see the "Using the VQE Configuration Tool" section on page 6-4.

-fix_checksum Option

VQE Configuration Engine does not apply VCDB values to /etc configuration files where there is a checksum mismatch. Use the **-fix_checksum** option to fix the checksum of one or more /etc configuration files that have a checksum mismatch.

When **-fix_checksum** is specified, **vqe_cfgtool** loops through /etc configuration files that have checksum mismatches and, for each, asks if you want the VQE CMS to manage the file again. If you answer yes, **vqe_cfgtool** recomputes the checksum for the file.

For information on how the Configuration Engine works, see the "VQE Configuration Engine" section on page 6-10.

-fix_config Option

When **-fix_config** is specified, **vqe_cfgtool** discards each /etc configuration file where there is a checksum mismatch and replaces it with the factory default /etc configuration file from the RPM package. **vqe_cfgtool** then recomputes the checksum using the factory default file.

A missing or unreadable /etc configuration file is considered a checksum mismatch and **–fix_config** copies the default factory file into the appropriate directory below /etc.

-parse Option

When **-parse** is specified, **vqe_cfgtool** parses the vcdb.conf file or, if the optional *full_pathname* is given, it parses the indicated file. This option is typically used to check the validity of offline VCDB configuration files. For information on the VCDB Parser, see the "VCDB Parser" section on page 6-12.

-sanity_check Option

When **-sanity_check** is specified, **vqe_cfgtool** checks the following:

- Whether the files under /etc have been manually edited (changes made not using VCDB)
- Whether the RPM software on the server is intact and no piece is missing
- Whether the vqe user account exists on the server

If **vqe_cfgtool** finds a problem with any of the preceding checks, it displays information about the issue on standard output.

Tip You can use the **cron** command to execute **vqe_cfgtool -sanity_check** periodically to check VQE-S or VQE Tools system sanity.

APPENDIX A

VQE, System, and Network Parameters

This appendix provides descriptions of the VQE Configuration Database (VCDB) parameters.

The essential VCDB parameters—the subset typically required for a VQE-S or VQE Tools system—can be configured by using the VQE Configuration Tool (CT) or by manually editing the vcdb.conf file. For information on using the VQE Configuration Tool, see Chapter 6, "Configuring VQE Server and VQE Tools."

All VCDB parameters can be configured by manually editing the vcdb.conf file. For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-12

The VQE-S, system, and network parameters are described in the following tables:

- Table A-1—VQE-S global parameters
- Table A-2—VQE-S Unicast Retransmission parameters
- Table A-3—VQE-S Rapid Channel Change parameters
- Table A-4—VQE-S Unicast Retransmission and Rapid Channel Change parameters (parameters that affect the behavior of both Unicast Retransmission and Rapid Channel Change)
- Table A-5—VQE-S RTCP Exporter parameters
- Table A-6—System parameters
- Table A-7—Network parameters

For all parameters intended to be user-configurable, the preceding tables provide the parameter name, default value (if any), description, and allowed range of values. The parameter default value (if any) is in quotation marks following the parameter name. For example:

vqe.vqes.log_priority="4"

For vqe.vqes.log_priority, 4 is the default value. Empty quotation marks indicate that there is no default value.

For more information on the VQE, system, and network parameters, see the /etc/vqes/vcdb.conf.sample file. *The vcdb.conf.sample file provides the above information and additionally the parameter type, service interruption information, whether multiple definitions are allowed, and the target /etc files where the parameter value is applied.*

Note In the following tables, if a parameter is configurable with Configuration Tool, the Description lists the CT menu and menu choice for the parameter in the brackets as follows: [CT: *menu* > *menu_choice(s)*].

Table A-1 VQE-S Global Parameters

Parameter and Default Value (if any)	Description
vqe.vqes.log_priority="4"	Logging level for all VQE-S processes. Allowed range is 0 to 6. Logging levels are as follows: • 0—Emergency (System is unusable.) • 1—Alert (Action must be taken immediately.) • 2—Critical (critical condition) • 3—Error (error condition) • 4—Warning (warning condition) • 5—Notice (normal but significant condition) • 6—Info (informational condition) Logging levels go from least verbose to most verbose. The Emergency level generates the smallest number of messages, and the Informational level generates the greatest number of messages. By default, VQE-S logging messages are written to the file /var/log/vqe/vqe.log. When you select a logging level, log messages are generated for that level and the levels below that level. For example, when the level is set to Error, messages are generated for Emergency, Alert, Critical, and Error. For information on configuring VQE-S debugging messages, see the "Configuring VQE-S Debugging" section on page 4-19. [CT: VQE-S Parameters > Log Priority]
vqe.vqes.vqe_interfaces="eth1,eth2,eth3,eth4, eth5,eth6"	Names of the interfaces to be used for incoming multicast streams, outgoing Unicast Retransmission and RCC traffic, and other non-management VQE-S traffic. Multiple interfaces should be separated by a comma without any space between names. Allowed values are eth1 to eth6. Interfaces eth5 and eth6 are available only on CDE110 servers that include the Intel PRO/1000 PT Dual Port Server Adapter. [CT: VQE-S Parameters > VQE-S Traffic Interface(s)]
vqe.vqes.rtcp_dscp="24"	Differentiated Services Code Point (DSCP) value for transmitted RTCP packets. The default value (24) is for the CS3 selector, which is used for broadcast video. Allowed range is 0 to 63.
vqe.vqes.rtp_retrans_dscp="0"	Differentiated Services Code Point (DSCP) value for transmitted RTP packets sent for Unicast Retransmission or RCC. Allowed range is 0 to 63.
vqe.vqes.rtp_inactivity_timeout="300"	Amount of time (in milliseconds) for the inactivity timeout on received RTP streams. If no packets are received on an input channel for this amount of time, the channel will be declared inactive until the next input packet is received for that stream. Allowed range is 10 to 900.
vqe.vqes.stun_enable="true"	Specifies whether the STUN Server is enabled. The value true enables the STUN Server, and false disables the STUN Server. Unless you are sure that no set-top boxes being serviced by VQE-S are behind NAT devices, we recommend that the STUN Server is enabled.
vqe.iptables.trusted_vcpt=""	Starting with Cisco VQE Release 3.2, this parameter is deprecated. Use the system.iptables.trusted_provisioner parameter.

Table A-2 VQE-S Unicast Retransmission (Error Repair) Parameters

Parameter and Default Value (if any)	Description
vqe.vqes.client_er_policing="true"	Specifies whether per-VQE Client policing is enabled for Unicast Retransmission (error repair) packets. The value true enables per-VQE Client policing, and false disables per-VQE Client policing. The VQE Client policing mechanism is intended to limit the fraction of VQE-S error-repair resources that can be consumed by a single VQE Client on the set-top box. When per-VQE Client policing is enabled, the policer is tuned by two parameters: vqe.vqes.client_er_tb_rate_ratio and vqe.vqes.client_er_tb_depth.
vqe.vqes.client_er_tb_rate_ratio="5"	Per-client policing token rate (percent of stream rate) for each VQE Client for Unicast Retransmission. Allowed range is 1 to 100. Per-client policing uses token bucket policers. A token is the equivalent of a packet. The token rate for the policers is defined as a percent of a stream's packet rate. For example, assume an RTP stream with a packet rate of 350 packets per second, the default rate of five percent will set the per-client policer token rate to 18 packets per second. Increasing this parameter will increase the maximum load that a single set-top box can put on the VQE-S. By default, each VQE Client is permitted to request up to five percent of the overall stream bandwidth for whatever channel it is watching. In a situation with only a few VQE Clients, some or all of which have very high error rates, it may be desirable to increase this parameter in order to allow each client to get more errors repaired. In a situation with a large number of VQE Clients, it may be necessary to decrease this parameter in order to prevent a small proportion of misbehaving or very error-prone client connections from consuming a disproportionate fraction of the VQE Server error-repair resources. The VQE-S AMT channel statistics for each channel provide data that you can use to tune the VQE Client policing mechanism. In the Channel Statistics window, click **Advanced**. The Advanced Channel Debug Stats include the following parameters that indicate how many error-repair requests were refused because the VQE Server is overloaded and how many were refused because of per-client policing. • Dropped repair pkts by Packet Policer—If the server is overloaded with error repairs, this statistic may be an indication that the per-client policing should be lowered. • Aggregated dropped pkts by client policers—If many repairs are being refused because of per-client policing, but the server is not overloaded, this statistic may be an indication that the per-client policing can be raised.

Table A-2 VQE-S Unicast Retransmission (Error Repair) Parameters (continued)

Parameter and Default Value (if any)	Description
vqe.vqes.client_er_tb_depth="10000"	Length of time (in milliseconds) needed to fill the per-VQE Client policer bucket for Unicast Retransmission (error repair). Allowed range is 1 to 60,000. The bucket "depth" of the per-client packet policers is expressed as a duration over which the token limit would be reached if the bucket was initially empty and filled at the token rate with no tokens drained. Therefore, the maximum number of tokens ("depth") of the policer bucket is calculated as follows: maximum number of tokens = (client_er_tb_rate_ratio * stream packet rate * client_er_tb_depth) The bucket size should be set large enough to cover the maximum burst loss that may ordinarily occur on a client set-top box. In most cases, the default value for vqe.vqes.client_er_tb_depth should be adequate.
vqe.vqes.er_cache_time="3000"	Maximum time interval (in milliseconds) to cache the original source stream packets for Unicast Retransmission (error repair). Allowed range is 100 to 5000.

Table A-3 VQE-S Rapid Channel Change Parameters

Parameter and Default Value (if any)	Description
vqe.vqes.rcc_burst_delay_to_send="10"	Amount of time (in milliseconds) to delay before the Data Plane schedules an RCC repair burst. This parameter may be set to a larger value to compensate for lags in the IGMP "fast leave" mechanism in the access node (for example, a DSLAM). Allowed range is 0 to 100.
vqe.vqes.igmp_join_variability = "100"	Amount of variability (in milliseconds) between the fastest and slowest IGMP joins for RCC. Allowed range is 0 to 500. **Note** This parameter can have a large impact on the amount of bandwidth consumed by RCC. It needs to be carefully tuned for a deployment.
vqe.vqes.rtp_hold_time="20"	Amount of time (in milliseconds) to delay before making a packet in the Data Plane cache available for RCC in order to allow for reordering of received packets. Allowed range is 0 to 500. This parameter is needed to allow for reordering of received packets in case they were received out of order from the source (headend). The parameter should be set as small as possible but large enough to cover the maximum arrival time jitter of received packets. Setting the parameter too small may cause some RCC operations to fail or be degraded if packets are received out of order. Setting the parameter too large causes RCC operations to use more network bandwidth, on average, than is necessary.
vqe.vqes.rap_max_interval="2000"	Maximum time interval (in milliseconds) between MPEG random access points (RAPs) that VQE-S will support for RCC operations. Allowed range is 500 to 5000.

Table A-3 VQE-S Rapid Channel Change Parameters (continued)

Parameter and Default Value (if any)	Description
vqe.vqes.rcc_mode="conservative"	RCC mode. Can be specified as either of these values: • aggressive—Conserves bandwidth if all DSLAMs that may receive an RCC burst from VQE-S are configured to give priority to the primary multicast video traffic over the unicast RCC burst traffic. • conservative—Use when the DSLAM does not have the required QoS capability for aggressive mode. Use of aggressive mode in a situation where one or more access nodes (DSLAMs) in the network have not been configured to give preference to the primary multicast traffic over the unicast stream will cause degraded video quality during RCC operations for customers attached to DSLAMs that are not properly configured for aggressive mode RCC. **Caution** Use of aggressive mode may cause brief, transient congestion of the access links during the RCC operation and therefore should not be used in situations where such congestion may have undesirable side effects, such as loss of data or voice traffic on the access link.
vqe.vqes.fastfill_enable=”true”	Specifies whether Fast Decoder Buffer Fill (FDBF) is enabled for RCC to reduce decoder buffering time. The value true enables FDBF, and false disables FDBF.
vqe.vqes.max_idr_penalty="0"	For MPEG-4 only, the maximum penalty (in milliseconds) that will be permitted in order to begin an RCC burst with an instantaneous decoding refresh (IDR) frame rather than I-frame. Allowed range is 0 to 10000. In cases where there are several MPEG random access points (RAPs) from which an RCC could be performed, the RCC is normally started from the most recent feasible RAP. If vqe.vqes.max_idr_penalty is specified as greater than zero, then the RCC will be started with an IDR frame instead of an I-frame provided that the IDR is within vqe,vqes.max-idr-penalty milliseconds of the most recent feasible I-frame.

Note Table A-4 lists parameters that affect the behavior of both Unicast Retransmission and Rapid Channel Change.

Table A-4 VQE-S Unicast Retransmission and Rapid Channel Change Parameters

Parameter and Default Value (if any)	Description
vqe.vqes.unicast_reservation-"20"	Percent of network bandwidth reserved for inbound Unicast Retransmission and RCC requests. This parameter specifies the amount of inbound bandwidth that *will not be allocated* to receiving multicast streams. Allowed range is 0 to 100. **Note** Recommended value range is 20 to 40. The percent value should not be anywhere close to 0 or 100.
vqe.vqes.max_client_bw = “0”	Maximum access link bandwidth (in bits per second) available for each VQE Client for Unicast Retransmission and RCC. Allowed range is 0 to 30,000,000. • If a non-zero value is specified, the vqe.vqes.excess_bw_fraction is ignored. Instead each time the set-top box tunes to a new channel, the implicit excess_bw_fraction for the client on the channel is calculated using vqe.vqes.max_client_bw. • If zero is specified or the parameter is not explicitly configured, VQE-S uses the configured vqe.vqes.excess_bw_fraction parameter in the Unicast Retransmission or RCC computation.
vqe.vqes.excess_bw_fraction="20"	Specifies the rate e (e = excess_bw_fraction / 100) that determines the rate at which packets are sent during Unicast Retransmission and Rapid Channel Change. Allowed range is 3 to 500. • For Unicast Retransmission, the VQE-S sends packets at rate (e). • During RCC, the VQE-S initially sends packets at rate (1+e). [CT: VQE-S Parameters > Excess Bandwidth Fraction]

Table A-4 VQE-S Unicast Retransmission and Rapid Channel Change Parameters (continued)

Parameter and Default Value (if any)	Description
vqe.vqes.excess_bw_fraction_high_def=""	For high definition channels, specifies the rate e (e = excess_bw_fraction_high_def / 100) that determines the rate at which packets are sent during Unicast Retransmission and Rapid Channel Change. Allowed range is 3 to 500. • For Unicast Retransmission, the VQE-S sends packets at rate (e). • During RCC, the VQE-S initially sends packets at rate (1+e). VQE-S uses the value configured in the vqe.vqes.high_def_min_bw parameter to determine what constitutes a high-definition channel. If either vqe.vqes.excess_bw_fraction_high_def or vqe.vqes.high_def_min_bw is not explicitly configured, VQE-S uses vqe.vqes.excess_bw_fraction for all channels.
vqe.vqes.high_def_min_bw=""	Minimum bit rate (in bits per second) for a channel to be considered a high definition channel. Allowed range is 0 to 40,000,000. For high definition channels, the vqe.vqes.high_def_min_bw value determines whether the vqe.vqes.excess_bw_fraction_high_def value is used for the bandwidth that will be available on the access link for Unicast Retransmission and Rapid Channel Change. For more information, see vqe.vqes.excess_bw_fraction_high_def. If either vqe.vqes.excess_bw_fraction_high_def or vqe.vqes.high_def_min_bw is not explicitly configured, VQE-S uses vqe.vqes.excess_bw_fraction for all channels.

Table A-5 VQE-S RTCP Exporter Parameters

Parameter and Default Value (if any)	Description
vqe.vqes.exporter_enable = "false"	Specifies whether RTCP exports are enabled. The value true enables RTCP exports, and false disables RTCP exports. If vqe.vqes.exporter-enable equals true, both vqe.vqes.vqm_host and vqe.vqes.vqm_port must be provided. For information on configuring VQE-S RTCP Exporter, see the "Configuring VQE-S RTCP Exporter" section on page 2-30.
vqe.vqes.vqm_host = ""	Specifies the IP address or fully qualified Internet domain name of the host on which the video-quality monitoring (VQM) application resides. For information on configuring RTCP Exporter, see the "Configuring VQE-S RTCP Exporter" section on page 2-30.
vqe.vqes.vqm_port= ""	Specifies the TCP port number on which the VQM application listens for video-quality data from RTCP Exporter. For information on configuring RTCP Exporter, see the "Configuring VQE-S RTCP Exporter" section on page 2-30.

Table A-6 System Parameters

Parameter and Default Value (if any)	Description
system.global.hostname="localhost"	A fully qualified domain name (FQDN) or hostname of the system. Hostname is used in multiple Linux configuration files. Allowed range is 3 to 200 characters. [CT: System Parameters > Hostname]
system.dns.server="" system.dns.search_domain=""	VQE-S host only—IP address of a DNS server and an optional search domain. Allowed range for the search domain is 3 to 200 characters. [CT: System Parameters > DNS Server(s) and DNS Search Domain]
system.ntp.server=""	IP address of a Network Time Protocol (NTP) server. [CT:System Parameters > NTP Server(s)]
system.snmp.ro_community_string="" system.snmp.location="" system.snmp.contact="" system.snmp.trap_listener=""	• Read-only community string—Password for read-only access to the VQE-S or VQE Tools server. Allowed range is 3 to 200 characters. • Location information—Physical location of the VQE-S or VQE Tools server. Allowed range is 3 to 200 characters. • Contact information—User name of a contact person who has management information for the CDE110 server. Allowed range is 3 to 200 characters. • Trap listener —IP address or fully qualified hostname of a management host that will receive the SNMP messages. [CT: System Parameters > SNMP RO Community String and SNMP System Location, SNMP System Contact, and SNMP Trap Listener(s)]

Table A-6 System Parameters (continued)

Parameter and Default Value (if any)	Description
system.clock.timezone="America/New York"	The time zone that will be used for this CDE110 server. [CT: System Parameters > Timezone]
system.iptables.trusted_provisioner=""	Depending on the hardware platform, specifies the IP addresses of the following trusted provisioners: • On a VQE-S host, specifies IP addresses of one or more trusted channel-provisioning servers (such as VCPT). – If VCPT is the channel-provisioning server, the IP addresses of all Ethernet interfaces (that have been assigned IP addresses) on the VCPT host must be configured as trusted HTTPS clients on the VQE-S host. • On a VQE Tools host where a VCDS receives channel information from VCPT, specifies the IP addresses of *all Ethernet interfaces* (that have been assigned IP addresses) on the VCPT host sending the channel information. This requirement applies even when the VCDS is in the same VQE Tools server as the VCPT. • On a VQE Tools host, specifies IP addresses of one or more trusted VQE-C system configuration provisioning servers. This type of provisioning server is not currently used in most deployments. Multiple system.iptables.trusted_provisioner parameters are used when there is more than one Ethernet port IP address that must be specified. This parameter is used for enhanced communications security beyond HTTPS. The VQE-S server or VQE Tools server is configured so that only trusted HTTPS clients (as specified in system.iptables.trusted_provisioner) can send information to, respectively, the VQE-S server or VQE Tools server. [CT: System Parameters > Trusted Provisioning Client(s)]

Table A-7 Network Parameters

Parameter and Default Value (if any)	Description
network.eth1.addr="" network.eth2.addr="" network.eth3.addr="" network.eth4.addr="" network.eth5.addr="" network.eth6.addr=""	For one or more of the Ethernet ports on the Cisco CDE110, an IP address and prefix length (for example, 1.2.3.4/24). • On a VQE-S host, four Ethernet interfaces are typically configured and used for VQE-S traffic. • On a VQE Tools host, at least one Ethernet interface is typically configured and used for VCPT and VQE Client Channel Configuration Delivery Server (VCDS) traffic. **Note** If one Ethernet interface is used for a management network, that interface *should be included* in the set for which you provide IP addresses and prefix-lengths. The VCDB parameters for eth5 and eth6 are used only on CDE110 servers that include the Intel PRO/1000 PT Dual Port Server Adapter. [CT: Network Parameters > Eth1 Interface, Eth2 Interface, Eth3 Interface, Eth4 Interface, Eth5 Interface, and Eth6 Interface]
network.route.mgmt_route=""	If your deployment will make use of a management network, you specify a static route for the management network: • Subnet IP address and prefix-length for the management network. The following example shows the allowed format for the subnet IP address and prefix-length: 10.1.0.0/16 • Gateway (next hop) IP address of the interface on the router that is directly attached to the CDE110 Ethernet interface that will be used for the management network. For example: network.route.mgmt_route="10.1.0.0/16 via 5.6.7.8" In this example, • 10.1.0.0/16 is the subnet IP address and prefix-length for the management network. • 5.6.7.8 is the IP address of the interface on the router directly attached to the CDE110 Ethernet interface that will be used for the management network. **Note** On the VQE Tools server, proper route configuration is needed for external access to the VQE Tools server. You can use the static management route created by this parameter to configure this access. [CT: Network Parameters > Management Route(s)]

Table A-7 Network Parameters (continued)

Parameter and Default Value (if any)	Description
network.route.type="static"	VQE-S host only—Specifies whether static routes or OSPF routing are enabled for VQE-S traffic. Allowed values are static or ospf. If static routes are enabled, the network.route.default_gateway parameter is configured for one or more default gateway (next hop) router interfaces. If OSPF routing is enabled, the following parameters can be configured: • network.ospf.router_id • network.ospf.area • network.ospf.area_type • network.ospf.md5_enable • network.ospf.md5_key • network.ospf.md5_keyid • network.ospf.hello_interval • network.ospf.dead_interval For descriptions of the preceding parameters, see Table A-7 (this table). [CT: Network Parameters > Routing Type]
network.route.default_gateway=""	VQE-S host only—If static routes are enabled, specifies the IP address for the interface on the router that is directly attached to the VQE-S host. Specify as many gateway (next hop) router interfaces as are reachable through all of the configured CDE110 Ethernet interfaces. **Note** If one Ethernet interface is used for a management network, that interface *should not be included* in the set for which gateway router interfaces are specified. The same number (usually one) of next hop gateways should be specified for each CDE110 interface that is to be used for VQE-S traffic. This will ensure that output is equally balanced across all interfaces and none will be overloaded. VQE-S uses Equal Cost Multipath (ECMP) to load-balance its output traffic across all the gateway router interfaces that are specified. If a default route (the gateway IP address) is configured for each Ethernet interface that is available to VQE-S for Unicast Retransmissions, RCC, and other traffic, ECMP load-balances output traffic across all of the listed gateway interfaces. If you later configure another Ethernet interface for VQE-S traffic, be sure to also configure an associated default gateway for that interface. [CT: Network Parameters > Default Gateway(s)]
network.ospf.router_id=""	VQE-S host only—If OSPF routing is enabled, specifies the IP address used as the router ID to uniquely identify the VQE-S server in the OSPF network. The router ID must not be the same as the IP address of one of the CDE110 Ethernet interfaces because the router ID will be added as an internal address to the loopback interface. [CT: Network Parameters > OSPF Parameters > Router ID]

Table A-7 Network Parameters (continued)

Parameter and Default Value (if any)	Description
network.ospf.area_type="normal"	VQE-S host only—If OSPF routing is enabled, specifies the type of OSPF area that the VQE-S traffic interfaces and feedback target host addresses will reside in. Allowed values are normal or nssa (Not So Stubby Area). [CT: Network Parameters > OSPF Parameters > Area Type]
network.ospf.area="0"	VQE-S host only—If OSPF routing is enabled, specifies the OSPF area that the VQE-S Ethernet interfaces and feedback target addresses will reside in. Allowed range of integer values is 0 to 4,294,967,295. [CT: Network Parameters > OSPF Parameters > Area ID]
network.ospf.md5_enable="false"	VQE-S host only—If OSPF routing is enabled, specifies whether Message Digest 5 (MD5) authentication is enabled on the Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, specifying an MD5 key and MD5 key ID are required. Allowed values are true or false. (Ethernet interfaces used for VQE-S traffic are configured with the vqe.vqes.vqe_interfaces parameter.) [CT: Network Parameters > OSPF Parameters > Enable MD5]
network.ospf.md5_key=""	VQE-S host only—If OSPF routing and MD5 authentication are enabled, specifies the key (a string) that will be configured for all Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, specifying an MD5 key and MD5 key ID are required. [CT: Network Parameters > OSPF Parameters > MD5 Key]
network.ospf.md5_keyid="1"	VQE-S host only—If OSPF and MD5 authentication are enabled, specifies an MD5 key ID (an integer) that will be used for all Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, an MD5 key and MD5 key ID are required. Allowed range of integer values is 1 to 255. [CT: Network Parameters > OSPF Parameters > MD5 Key ID]
network.ospf.hello_interval="10"	VQE-S host only—If OSPF routing is enabled, specifies the interval at which OSPF Hello packets are sent (in seconds). This value must be the same for all interfaces running OSPF in the network. The hello interval will be set for all VQE-S interfaces running OSPF. Allowed range is 1 to 65,535. [CT: Network Parameters > OSPF Parameters > Hello Interval]
network.ospf.dead_interval="40"	VQE-S host only—If OSPF routing is enabled, specifies the OSPF dead interval (in seconds). The dead interval is the maximum amount of time allowed to receive a Hello packet from a neighbor before that neighbor is declared down. This value must be the same for all interfaces running OSPF in the network. The dead interval will be set for all VQE-S interfaces running OSPF. Allowed range is 1 to 65,535. [CT: Network Parameters > OSPF Parameters > Dead Interval]

APPENDIX B

Using Net-SNMP

The CDE110 servers that host VQE-S and VQE Tools use Net-SNMP, a third-party product, for Simple Network Management Protocol (SNMP) support for some basic, non-VQE system services. Net-SNMP offers a set of built-in MIBs for Linux platforms. This appendix provides information about using Net-SNMP on the Cisco CDE110 that hosts VQE-S and on the CDE110 that hosts VQE Tools.

Net-SNMP provides tools and libraries relating to the Simple Network Management Protocol including an extensible agent, an SNMP library, tools to request or set information from SNMP agents, and tools to generate and handle SNMP traps. For information on configuring and using Net-SNMP, see the Net-SNMP web site:

http://www.net-snmp.com/docs/

Net-SNMP provides a set of built-in MIBs for Linux platforms, but no VQE-specific MIBs are included in the set. The built-in MIBs cover GETs and TRAPs for some areas of the Linux distribution, such as interface status and statistics, SNMP protocol-related counters, and host resources.

On the CDE110s that host VQE-S and VCPT, only the SNMPv2 client is supported. Also, configuration through the SNMP interface is disabled.

The sysDescr and sysObjectID objects in the SNMPv2-MIB identify a VQE system. The following values can be used to identify a CDE110 hosting VQE-S or VCPT:

- SNMPv2-MIB::sysDescr.0 = STRING: "Cisco VQE (Video Quality Experience) offers service providers a set of technologies and products associated with the delivery of IPTV video services."
- SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.942

Table B-1 lists the MIBs that are supported on the CDE110s that host VQE-S and VCPT. For information on the supported MIBs, see the MIB area of the Net-SNMP web site:

http://www.net-snmp.com/docs/mibs/

Table B-1 MIBs for CDE110s That Host VQE-S and VCPT

MIB/Table	Description
SNMPv2-MIB/system	System contact, location, etc.
SNMPv2-MIB/snmp	SNMP protocol-related counters, including cold/warm start and authentication failure traps
SNMP-NOTIFICATION-MIB/snmpNotifyTable	Used to configure TRAP listeners
IF-MIB	Interface status and statistics
RMON/etherStatsTable	Statistics for each Ethernet interface

Table B-1 MIBs for CDE110s That Host VQE-S and VCPT (continued)

MIB/Table	Description
RMON/alarmTable	Stores configuration entries that each define a variable, polling period, and threshold parameters
RMON/eventTable	Controls the generation and notification of events from this device
HOST-RESOURCE-MIB (except hrPrinterTable)	System, memory, storage, device, processor, network, disc, partition, FS, and software version information about Linux host
INTEL-SERVER-BASEBOARD5	Supports the Intel Server Baseboard SNMP subagent for monitoring baseboard components, providing SNMP access to GET information for baseboard components, SET sensor thresholds and support events through the NOTIFICATION-TYPE construct. See: http://people.redhat.com/peterm/IPMI/sw/basebrd5.mib

APPENDIX C

VQE System Messages

This appendix provides information on the Cisco VQE system messages. The VQE software writes these messages to these locations:

- VQE-S system messages are written to the /var/log/vqe/vqe.log file.
- VQE Client Channel Configuration Delivery Server (VCDS) system messages are also written to the /var/log/vqe/vqe.log file.

Not all system messages indicate problems with VQE. Some messages are purely informational, while others may help diagnose problems with communications links or the operating system (for example, file permission problems). Only critical messages are displayed on the CDE110 console.

For information on VQE-S AMT and VCPT logging output, see the "VQE-S AMT and VCPT Logging and Log Files" section on page 5-2.

System Message Structure

System messages are structured as follows:

```
FACILITY-SEVERITY-MNEMONIC: Message-text
```

- FACILITY code

  The facility code consists of two or more uppercase letters that indicate the facility to which the message refers. Table C-1 lists the VQE facility codes.

Table C-1 VQE Facility Codes

Code	VQE Facility
STUN_SERVER	STUN Server (VQE-S)
VQES_CP	VQE-S Control Plane
VQES_DP_CLIENT	VQE-S Data Plane Client
VQES_DP	VQE-S Data Plane
VQES_MLB_Client	VQE-S Multicast Load Balancer Client
VQES_MLB	VQE-S Multicast Load Balancer
VQES_PM	VQE-S Process Monitor
VQE_CFGTOOL	VQE Configuration Tool (**vqe_cfgtool** command)
VQE_CFG	VQE channel configuration

Table C-1 VQE Facility Codes (continued)

Code	VQE Facility
VQE_UTILS	VQE utilities, such as hash table
VQE_RPC	VQE-S Remote Procedure Calls
VQE_RTP	VQE Real-Time Transport Protocol (Many of these messages are related to RTP Control Protocol (RTCP)).
VQE_RTSP	VQE Real Time Streaming Protocol (VCDS related)

- SEVERITY level

  The severity level is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation. Table C-2 lists the message severity levels. Messages of severity 7 (Debugging) are not described in this appendix.

Table C-2 Message Severity Levels

Severity Level	Name	Description
0	Emergency	System is unusable.
1	Alert	Immediate action is required.
2	Critical	Critical condition
3	Error	Error condition
4	Warning	Warning condition
5	Notification	Normal but significant condition
6	Informational	Information message only
7	Debugging	Message that appear during debugging only

- MNEMONIC code

  The combination of the facility code and the mnemonic code uniquely identifies the error message.

- Message-text

  Message-text is a text string that describes the condition. The text string sometimes contains detailed information about the event, including port numbers and network addresses. Because variable fields change from message to message, they are represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec]. Table C-3 lists the variable fields in messages.

Table C-3 Representations of Variable Fields in Messages

Representation	Type of Information
[chars] or [char]	Character string
[dec]	Decimal
[hex]	Hexadecimal integer

Table C-3 Representations of Variable Fields in Messages

Representation	Type of Information
[int]	Integer
[num]	Number

System Message Example

The following is an example of a VQE system message:

```
VQES_CP-3-CP_CHANNEL_DELETE_ERR: Failed to delete a channel due to [chars]
```

- VQES_CP is the facility code.
- 3 is the severity level.
- CP_CHANNEL_DELETE_ERR is the mnemonic code.
- "Failed to delete a channel due to [chars]" is the message text.

Basic Recovery Procedures

In the Recommended Actions of the system messages, certain recovery procedures that VQE users should perform are referred to numerous times. Table C-4 provides references to where you can find more information on these recovery procedures.

Table C-4 Recovery Procedures in Recommended Actions

Recovery Procedure in Recommended Action	Notes and Where to Find Information
Reboot the VQE-S server.	Restarting the System and Verifying System and VQE-S Status, page D-21
Restart the VQE-S application.	Stopping, Starting, and Restarting VQE-S, page 5-16
Restart the VQE-S channels.	In VCPT, use the Force Update button to send the channel information to the VQE Server. See the "Force Update Button" section on page 3-5.
Modify the channel configuration and resend it to the VQE Servers and/or VCDS servers.	Chapter 3, "Using the VQE Channel Provisioning Tool"
Modify vcdb.conf and apply the configuration.	For VQE configuration (vcdb.conf) information, see Chapter 6, "Configuring VQE Server and VQE Tools." For information on applying a VQE configuration with the **–apply** option to **vqe_cfgtool**, see the "Using the VQE Configuration Tool Command-Line Options" section on page 6-16.
Issue the **vqereport** command to gather data that may help identify the nature of the error.	"Using the vqereport Command" section on page 5-15

VQE System Messages Reference Information

Starting with VQE Release 3.0, reference information for the VQE system messages is listed in HTML format in a file that is available for each release in the VQE software download area on Cisco.com.

Tip The online system messages file with reference and recovery information is located with the VQE software installation file. When you click on a specific VQE-S or VQE Tools software installation file, the system messages link is System Messages and Recovery Procedures for *X.X(X)* and is listed under Additional Information.

For each system message, the HTML file contains the message text, an explanation of the message, and a recommended action describing what (if anything) you need to do. For example:

Error Message `STUN_SERVER-2-SS_INIT_FAILURE_CRIT: STUN Server initialization failed due to [chars]`

Explanation A software error has occurred during the initialization of the STUN Server process and the process will not start.

Recommended Action Restart the VQE-S application. If this message recurs, copy the error message exactly as it appears in the VQE-S system log. Contact your Cisco technical support representative, and provide the representative with the gathered information.

Note The Recommended Action frequently involves a recovery procedure (for example, "Restart the VQE-S application.") that is described in the "Basic Recovery Procedures" section on page C-3.

APPENDIX D

Manual Initial VQE System Configuration

This appendix explains how to perform manual initial configuration on the two categories of CDE110 servers running the VQE software:

- VQE-S server—CDE110 hosting VQE Server
- VQE Tools server—CDE110 hosting VQE Channel Provisioning Tool (VCPT) and VQE Client Channel Configuration Delivery Server (VCDS)

In a VQE deployment, use of a VQE Tools server and VCPT is optional.

The alternative to manual configuration is to use the Cisco VQE Startup Configuration Utility. For information on using the utility, see the "VQE-S Server: Routing Configuration Overview" section on page 2-12.

Note We recommend that you use the VQE Startup Configuration Utility rather than try to do the initial configuration manually because the utility simplifies your work and is known to produce correct results.

The manual initial configuration procedures are explained in these sections:

Setting Up a Cisco CDE110 That Hosts VQE-S

This section explains how to perform the initial configuration tasks for a Cisco CDE110 hosting VQE-S.

When performed manually, the initial configuration tasks involve editing the /etc/opt/vqes/vcdb.conf file to configure the essential VCDB parameters. The use of the vcdb.conf file simplifies the configuration tasks. Because the VQE Configuration Tool automatically applies the VCDB values to the /etc configuration files on system reboot, mistakes in configuration file syntax are unlikely.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-12.

Perform these initial configuration tasks in the order shown:

1. Prerequisites for a Cisco CDE110 That Hosts VQE-S, page D-2
2. Configuring the Linux Operating System for VQE-S, page D-3
3. Configuring a Static Route for a Management Network (VQE-S Host), page D-5
4. Configuring Static Routes for VQE-S Traffic, page D-6
5. Configuring OSPF Routing for VQE-S Traffic, page D-8
6. Configuring Ethernet Interfaces for VQE-S Traffic, page D-13
7. Synchronizing the Time and Configuring Network Time Protocol, page D-14
8. VQE STUN Server Is Enabled By Default, page D-14
9. Configuring SNMP (Optional), page D-14
10. Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS, page D-15
11. Starting VQE-S System Services and Verifying Status, page D-16
12. Starting the VQE-S Processes and Verifying Status, page D-20
13. Restarting the System and Verifying System and VQE-S Status, page D-21

Note The configuration instructions in this section are intended for new installations of Cisco VQE Release 3.2 software, where the Cisco CDE110 has the Cisco VQE Release 3.2 software preinstalled.

For information on *upgrading an already configured* Cisco CDE110 from Cisco VQE Release 2.1, 3.0, or 3.1 to Release 3.2, see the *Release Notes for Cisco CDA Visual Quality Experience, Release 3.2*

For information on configuring VQE-S RTCP Exporter, see the "Configuring VQE-S RTCP Exporter" section on page 2-30.

Prerequisites for a Cisco CDE110 That Hosts VQE-S

This section explains tasks that should be performed before setting up a Cisco CDE110 that hosts VQE-S.

Connecting Cables for VQE-S

For information on connecting cables on the VQE-S server, see the "Connecting Cables to the CDE110" section on page 2-3.

For the location of connectors on the Cisco CDE110 front and back panels, see the *Cisco Content Delivery Engine 110 Hardware Installation Guide*.

Setting Up SSL Certificates for VQE-S

It is recommended that you deploy your own Secure Sockets Layer (SSL) certificates or commercial SSL certificates prior to beginning the tasks for setting up a Cisco CDE110 that hosts VQE-S. For information on setting up the certificates, see the "Setting Up SSL Certificates" section on page 2-4.

Configuring the Linux Operating System for VQE-S

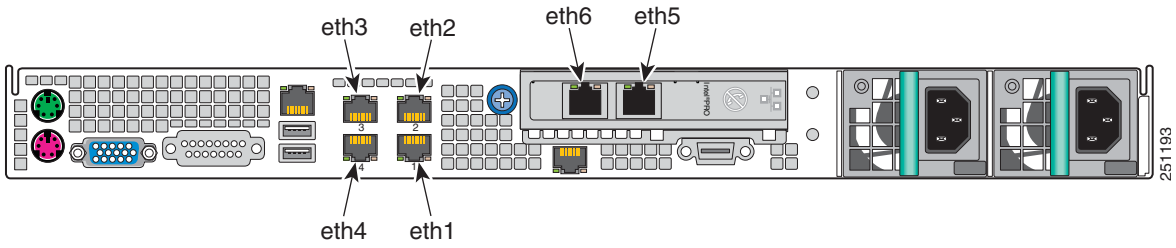
This section explains the initial Linux configuration tasks needed for a Cisco CDE110 appliance that will run VQE-S software. The explanation assumes that the needed software for Linux and VQE-S has been pre-installed on the Cisco CDE110 appliance. For Red Hat Enterprise Linux 5.1 documentation, go to the following web site:

http://www.redhat.com/docs/manuals/enterprise/

For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE110 back panel are specified as eth1 to eth6 as shown in Figure D-1.

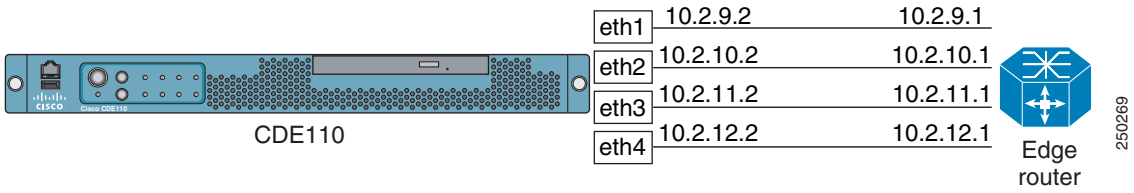
Note Earlier models of the CDE110 have four Ethernet ports (eth1 to eth4). These models did not have the Intel PRO/1000 PT Dual Port Server Adapter that provides the eth5 and eth6 ports.

Figure D-1 NIC Port Numbering for Software Configuration



For the configuration examples in this section, Figure D-2 shows the IP addresses for interfaces eth1, eth2, eth3, and eth4 and the corresponding interfaces on the edge router.

Figure D-2 IP Addresses for VQE-S Configuration Examples



To configure the Linux operating system and other software for VQE-S, follow these steps:

Step 1 If needed, login as root. You must have root privileges to modify the vcdb.conf file.

Step 2 To create the password for the vqe username (a pre-created Linux user ID), issue the following command:

```
[root@system]# passwd vqe
```

Enter a password that follows the password guidelines:

```
A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use an 8 character long
password with characters from at least 3 of these 4 classes, or
a 7 character long password containing characters from all the
classes.  An upper case letter that begins the password and a
digit that ends it do not count towards the number of character
classes used.

A passphrase should be of at least 3 words, 12 to 40 characters
long and contain enough different characters.
```

This username and password can be used to log in to Linux directly using SSH. The vqe username and password can also be used log in to the VQE-S Application Monitoring Tool.

Step 3 To configure CDE110 Ethernet interfaces eth1 to eth6, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.eth*x*.addr parameters, where eth*x* is eth1, eth2, and so on. Specify an IP address and prefix length for each interface. The following example shows four vcdb.conf lines for the four Ethernet interfaces:

```
network.eth1.addr="10.2.9.2/24"
network.eth2.addr="10.2.10.2/24"
network.eth3.addr="10.2.11.2/24"
network.eth4.addr="10.2.12.2/24"
```

Step 4 To configure the hostname for the CDE110 server, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the system.global.hostname parameter and specifying a hostname. The following example specifies the hostname as starfire-iptv:

```
system.global.hostname="starfire-iptv"
```

Step 5 To configure a DNS server, edit the /etc/opt/vqes/vcdb.conf file by adding the VCDB parameters for the IP address and optionally for the search domain of a DNS server and specifying the needed values:

- system.dns.server="*IP_address*"
- system.dns.search_domain="*search_domain*"

For example:

```
system.dns.server="192.0.20.53."
system.dns.search_domain="domain.com"
```

Step 6 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-21. You reboot once when all VCDB configuration tasks are completed.

After the VQE-S host is rebooted, you can verify that the eth1 to eth6 interfaces are configured correctly and up and running by issuing the following commands:

- Use the **ifconfig** *interface* command to verify that each Ethernet interface is up and running and the IP address and netmask for each are set correctly. The following example is for eth1:

```
[root@system]# ifconfig eth1

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:C6:F3:0F
          inet addr:10.2.10.2  Bcast:10.2.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fec6:f30f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:192 (192.0 b)  TX bytes:2700 (2.6 KiB)
          Base address:0x3000 Memory:b8800000-b8820000
```

- Use the **ip link show eth#** command (where # is the Ethernet interface number) to check that the link is up. The following example is for eth1:

```
[root@system]# ip link show eth1

eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0e:0c:c6:e4:fe brd ff:ff:ff:ff:ff:ff
```

- Use the **ping** command to check that the Cisco CDE110 can reach the connected edge router. For example:

```
[root@system]# ping 10.2.9.1
```

Configuring a Static Route for a Management Network (VQE-S Host)

If your deployment makes use of a management network, a static route for the management network can be configured using the VCDB parameter network.route.mgmt_route. The configuration example in this section assumes that one CDE110 Ethernet interface will be used to connect to the VQE network.

Note If you configure a static route for a management network as described in this section, see the "Static Route for a Management Network Is Missing on CDE110 Hosting VQE-S or VQE Tools" section on page 5-7 for some additional information.

To configure a static route for a management network, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file by adding to the file a network.route.mgmt_route parameter and specifying the needed values using the following format:

network.route.mgmt_route="*management-network-addr/prefix-length* via *gateway-addr* "

The *management-network-addr/prefix-length* is the IP address and prefix length for the management network. The *gateway-addr* is the IP address of the router interface that is directly attached to the CDE110 Ethernet port that will be used for management network traffic.

For this example, assume the following:

- CDE110 Ethernet interface eth1 (10.2.9.2) will be used for the management network.
- The management network is 192.0.0.0/8.

The line in the vcdb.conf file is as follows:

```
network.route.mgmt_route="192.0.0.0/8 via 10.2.9.1"
```

In the preceding example, 10.2.9.1 is the *gateway-addr*—the router interface that is directly attached to eth1. Figure D-3 shows the IP addresses used in this example for the eth1 interface and the directly attached router.

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-21. You reboot once when all VCDB configuration tasks are completed.

After the VQE-S host is rebooted, you can verify that the static route for the management network is present in the routing table by issuing the following command:

```
[root@system]# ip route show
```

The output will be similar to the following:

```
192.0.0.0/8 via 10.2.9.1 dev eth1
default
    nexthop via 10.2.10.1 dev eth2 weight 1
    nexthop via 10.2.11.1 dev eth3 weight 1
    nexthop via 10.2.12.1 dev eth4 weight 1
```

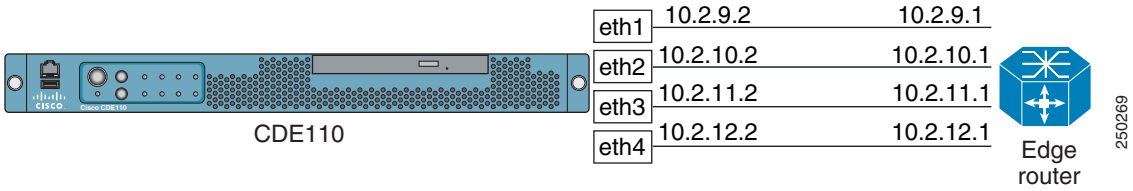
Configuring Static Routes for VQE-S Traffic

This section provides information on configuring static routes for VQE-S traffic on the CDE110 that hosts VQE-S.

Note For information on configuring static routes for feedback targets on the directly attached router, see the "For Static Routes: Guidance for Configuring Feedback Targets on the Attached Router" section on page 2-34.

For the configuration examples in this section, Figure D-3 shows the IP addresses for interfaces eth1, eth2, eth3, and eth4 and the corresponding interfaces on the edge router.

Figure D-3 IP Addresses for VQE-S Configuration Examples



On the Cisco CDE110 that hosts VQE-S, multiple Ethernet interfaces are used for VQE-S traffic, including incoming multicast streams, outgoing Unicast Retransmissions and RCC unicast transmissions, and other VQE-S traffic. In addition, some VQE deployments may use one of the Ethernet ports as the interface to a management network.

If default gateway (next hop) route is configured for each Ethernet interface that is available for VQE-S traffic, Equal Cost Multipath (ECMP) is used to load balance output traffic across all of the listed next hop interfaces.

Note A single default gateway should be configured for each interface used for VQE-S traffic. Otherwise, output load will not be balanced and some interfaces may be overloaded.

To configure a default gateway for multiple CDE110 Ethernet interfaces, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 To choose static routes for VQE-S traffic, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the network.route.type parameter and specifying the value static for the parameter:

```
network.route.type="static"
```

Step 3 To configure default gateways for each Ethernet interface that is available for VQE-S traffic, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.route.default_gateway parameters and specifying values for each of the parameters. The following example shows four vcdb.conf lines that add default gateways for the four CDE110 Ethernet interfaces.

```
network.route.default_gateway=”10.2.9.1”
network.route.default_gateway=”10.2.10.1”
network.route.default_gateway=”10.2.11.1”
network.route.default_gateway=”10.2.12.1”
```

In the preceding example, 10.2.9.1, 10.2.10.1, 10.2.11.1 , and 10.2.12.1 are the gateway (next hop) addresses on the router that is directly attached to the VQE-S host.

Note If one Ethernet interface is used for a management network, that interface *should not be included* in the set for which gateway router interfaces are specified.

Step 4 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the “Restarting the System and Verifying System and VQE-S Status” section on page D-21. You reboot once when all VCDB configuration tasks are completed.

After the VQE-S host is rebooted, you can verify that the default gateway routes are present in the routing table of the CDE110 by issuing the following command:

```
[root@system]# ip route show
```

The output will be similar to the following:

```
default
    nexthop via 10.2.9.1 dev eth1 weight 1
    nexthop via 10.2.10.1 dev eth2 weight 1
    nexthop via 10.2.11.1 dev eth3 weight 1
    nexthop via 10.2.12.1 dev eth4 weight 1
```

Configuring OSPF Routing for VQE-S Traffic

This section provides information on configuring OSPF routing for VQE-S traffic on the CDE110 that hosts VQE-S.

Note For guidance on configuring the attached router for OSPF routing, see the "For OSPF Routing: Guidance for Configuring the Attached Router" section on page 2-32.

To configure OSPF routing for the CDE110 Ethernet interfaces that will be used for VQE-S traffic, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 To choose OSPF routing for VQE-S traffic, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the network.route.type parameter and specifying the value ospf for the parameter:

```
network.route.type="ospf"
```

Step 3 To configure OSPF routing for the VQE-S traffic interface, edit the /etc/opt/vqes/vcdb.conf file by adding one or more of the following parameters to the file. The OSPF parameters that you choose to use depend on your network implementation.

Note Some of the OSPF parameters have a default value if you do not add the parameter to and specify a value in the vcdb.conf file.

- network.ospf.router_id
- network.ospf.area
- network.ospf.area_type
- network.ospf.md5_enable
- network.ospf.md5_key
- network.ospf.md5_keyid
- network.ospf.hello_interval
- network.ospf.dead_interval

For information on each of the preceding parameters and default values, see Table A-7 on page A-10.

Step 4 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-21. You reboot once when all VCDB configuration tasks are completed.

When the system is rebooted, the VQE Configuration Tool applies the OSPF configuration that you have specified to the VQE-S traffic interfaces.

On the VQE-S Server

After the VQE-S host is rebooted, you can verify that the OSPF configuration is present on the CDE110 by issuing the following commands where:

- 8.31.200.1 is the OSPF router ID of the VQE-S server.
- 8.31.1.1. is a feedback target address.
- 0.0.0.0/0 is the default route in the routing table on the VQE-S server.
- The VQE-S traffic interfaces are eth2 (10.1.1.2) and eth3 (10.1.2.2).

```
[root@system]# show ip ospf

vqe-s# show ip ospf
 OSPF Routing Process, Router ID: 8.31.200.1
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 OpaqueCapability flag is disabled
 Initial SPF scheduling delay 200 millisec(s)
 Minimum hold time between consecutive SPFs 1000 millisec(s)
 Maximum hold time between consecutive SPFs 10000 millisec(s)
 Hold time multiplier is currently 1
 SPF algorithm last executed 1m00s ago
 SPF timer is inactive
 Refresh timer 10 secs
 This router is an ASBR (injecting external routing information)
 Number of external LSA 1. Checksum Sum 0x0000efb2
 Number of opaque AS LSA 0. Checksum Sum 0x00000000
 Number of areas attached to this router: 1

 Area ID: 0.0.0.1 (NSSA)
   Shortcutting mode: Default, S-bit consensus: no
   Number of interfaces in this area: Total: 3, Active: 3
   It is an NSSA configuration.
   Elected NSSA/ABR performs type-7/type-5 LSA translation.
   It is not ABR, therefore not Translator.
   Number of fully adjacent neighbors in this area: 2
   Area has no authentication
   Number of full virtual adjacencies going through this area: 0
   SPF algorithm executed 4 times
   Number of LSA 6
   Number of router LSA 2. Checksum Sum 0x0000a03d
   Number of network LSA 2. Checksum Sum 0x00010556
   Number of summary LSA 1. Checksum Sum 0x0000519e
   Number of ASBR summary LSA 0. Checksum Sum 0x00000000
   Number of NSSA LSA 1. Checksum Sum 0x0000693e
   Number of opaque link LSA 0. Checksum Sum 0x00000000
   Number of opaque area LSA 0. Checksum Sum 0x00000000


[root@system]# show ip ospf database

       OSPF Router with ID (8.31.200.1)

                Router Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Link count
8.31.20.1       8.31.20.1       1120 0x80000012 0x1707 2
8.31.200.1      8.31.200.1      1120 0x8000001b 0x8936 3

                Net Link States (Area 0.0.0.1 [NSSA])
```

```
Link ID         ADV Router      Age  Seq#       CkSum
25.1.1.1        8.31.20.1       1125 0x80000001 0x08a6
25.1.2.1        8.31.20.1       1120 0x80000001 0xfcb0

                Summary Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         8.31.20.1        159 0x8000000c 0x4f9f 0.0.0.0/0

                NSSA-external Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route
8.31.1.1        8.31.200.1      1125 0x80000003 0x693e E2 8.31.1.1/32 [0x0]

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route
8.31.1.1        8.31.200.1      1125 0x80000003 0xefb2 E2 8.31.1.1/32 [0x0]


[root@system]# show ip ospf route

============ OSPF network routing table ============
N IA 0.0.0.0/0              [2] area: 0.0.0.1
                            via 25.1.1.1, eth2
                            via 25.1.2.1, eth3
N    8.31.200.1/32          [10] area: 0.0.0.1
                            directly attached to lo
N    25.1.1.0/24            [1] area: 0.0.0.1
                            directly attached to eth2
N    25.1.2.0/24            [1] area: 0.0.0.1
                            directly attached to eth3

============ OSPF router routing table =============
R    8.31.20.1              [1] area: 0.0.0.1, ABR, ASBR
                            via 25.1.1.1, eth2
                            via 25.1.2.1, eth3

============ OSPF external routing table ===========


[root@system]# show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>*   0.0.0.0/0 [110/2] via 25.1.1.1, eth2, 00:01:40
                      via 25.1.2.1, eth3, 00:01:40
C>* 8.31.1.1/32 is directly connected, lo
O   8.31.200.1/32 [110/10] is directly connected, lo, 00:01:49
C>* 8.31.200.1/32 is directly connected, lo
O   25.1.1.0/24 [110/1] is directly connected, eth2, 00:01:45
C>* 25.1.1.0/24 is directly connected, eth2
O   25.1.2.0/24 [110/1] is directly connected, eth3, 00:01:44
C>* 25.1.2.0/24 is directly connected, eth3
C>* 127.0.0.0/8 is directly connected, lo
K>* 224.0.0.0/4 is directly connected, eth1
```

On the Cisco 7600 Edge Router

After the VQE-S host is rebooted, you can verify that the OSPF configuration is present on the Cisco 7600 edge router by issuing the following commands where:

- 8.31.20.1 is the OSPF router ID on the edge router.
- In the **show ip route** command output, 8.31.1.1. is accessible from two interfaces, indicating the ECMP is configured correctly.
- The configuration on the edge router is as follows:

```
router ospf 100
 router-id 8.31.20.1
 log-adjacency-changes
 area 1 nssa no-summary
 traffic-share min across-interfaces
 network 25.1.1.0 0.0.0.255 area 1
 network 25.1.2.0 0.0.0.255 area 1
 network 26.1.1.0 0.0.0.255 area 0
 maximum-paths 8


c7600> show ip ospf
 Routing Process "ospf 100" with ID 8.31.20.1
 Start time: 00:00:04.540, Time elapsed: 06:07:33.560
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 It is an area border and autonomous system boundary router
 Redistributing External Routes from,
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x002F1B
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 2. 1 normal 0 stub 1 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm last executed 06:07:24.744 ago
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x012D0C
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 1
```

```
        Number of interfaces in this area is 2
        It is a NSSA area
        Perform type-7/type-5 LSA translation
        Area has no authentication
        SPF algorithm last executed 00:18:18.804 ago
        SPF algorithm executed 10 times
        Area ranges are
        Number of LSA 6. Checksum Sum 0x025E70
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 2
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

c7600> show ip ospf database

            OSPF Router with ID (8.31.20.1) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
8.31.20.1       8.31.20.1       288         0x8000000D 0x001B73 1

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
8.31.200.1      8.31.20.1       1239        0x80000001 0x009B69
25.1.1.0        8.31.20.1       1244        0x80000011 0x004292
25.1.2.0        8.31.20.1       1234        0x80000013 0x00339E

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
8.31.20.1       8.31.20.1       1249        0x80000012 0x001707 2
8.31.200.1      8.31.200.1      1250        0x8000001B 0x008936 3

                Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
25.1.1.1        8.31.20.1       1254        0x80000001 0x0008A6
25.1.2.1        8.31.20.1       1250        0x80000001 0x00FCB0

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
0.0.0.0         8.31.20.1       289         0x8000000C 0x004F9F

                Type-7 AS External Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Tag
8.31.1.1        8.31.200.1      1256        0x80000003 0x00693E 0

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
8.31.1.1        8.31.20.1       1240        0x80000001 0x002F1B 0

c7600> show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

     8.0.0.0/32 is subnetted, 2 subnets
O N2    8.31.1.1 [110/20] via 10.1.2.2, 00:20:45, GigabitEthernet0/2
                 [110/20] via 10.1.1.2, 00:20:45, GigabitEthernet0/1
O       8.31.200.1 [110/11] via 10.1.2.2, 00:20:45, GigabitEthernet0/2
                   [110/11] via 10.1.1.2, 00:20:45, GigabitEthernet0/1
     25.0.0.0/24 is subnetted, 2 subnets
C       25.1.1.0 is directly connected, GigabitEthernet0/1
C       25.1.2.0 is directly connected, GigabitEthernet0/2
     26.0.0.0/24 is subnetted, 1 subnets
C       26.1.1.0 is directly connected, GigabitEthernet0/3
```

Configuring Ethernet Interfaces for VQE-S Traffic

On the VQE-S host, the vqe.vqes.vqe_interfaces parameter in the /etc/vqes/vcdb.conf file allows you to specify the Ethernet interfaces that will be available to Multicast Load Balancer (MLB) for incoming multicast streams and outgoing Unicast Retransmission and RCC traffic, and other non-management VQE-S traffic. You manually edit the vcdb.conf file and specify the Ethernet interfaces that will be used.

Note If the vqe.vqes.vqe_interfaces parameter is not specified in the vcdb.conf file, all four Ethernet interfaces are available for VQE-S traffic.

To configure the Ethernet interfaces for VQE-S traffic on the Cisco CDE110 that hosts VQE-S, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file. Add the vqe.vqes.vqe_interfaces parameter to the file and specify the CDE110 Ethernet interface names that will be used for MLB. For example:

```
vqe.vqes.vqe_interfaces="eth2,eth3,eth4"
```

For the preceding example, assume that the implementation uses eth1 for management network traffic. Therefore, eth1 is not included in the set of interfaces that will be available to MLB.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-12.

Note If your deployment uses one Ethernet interface for a management network, be sure *not to include* that interface as one of the interfaces that will be available to Multicast Load Balancer.

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-21. You reboot once when all VCDB configuration tasks are completed.

Synchronizing the Time and Configuring Network Time Protocol

To keep system time correct and synchronized, we recommend that you use Network Time Protocol (NTP) on the VQE-S host. To synchronize the time and configure NTP, follow these steps:

Step 1 If needed, log in as root.

Step 2 To set the time zone, issue the **tzselect** command and follow the prompts:

```
[root@system]# /usr/bin/tzselect
```

Step 3 To set the date and time, issue the **date** command as follows:

date -s "*date_time_string*"

For example:

```
[root@system]# date -s "16:55:30 July 7, 2008"
```

Step 4 Edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more system.ntp.server parameters and specifying the IP address of an NTP server for each of the parameters. For example:

```
system.ntp.server="10.2.26.2"
```

In the preceding example, the IP address of the NTP server is 10.2.26.2.

Step 5 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-21. You reboot once when all VCDB configuration tasks are completed.

For information on starting the NTP service (ntpd daemon), see the "Starting VQE-S System Services and Verifying Status" section on page D-16.

VQE STUN Server Is Enabled By Default

Starting with Cisco VQE Release 3.0, the VQE STUN Server is enabled by default. The STUN Server allows set-top boxes behind NAT devices to be supported by VQE-S. Unless you are sure that no set-top boxes being serviced by VQE-S are behind NAT devices, we recommend that you leave the STUN Server enabled.

Configuring SNMP (Optional)

The CDE110 that hosts VQE-S uses Net-SNMP, a third-party product, for SNMP support for some basic, non-VQE system services. Net-SNMP offers a set of built-in MIBs for Linux platforms. The use of Net-SNMP is optional. For more information on Net-SNMP support, see Appendix B, "Using Net-SNMP."

To configure SNMP on the Cisco CDE110 that hosts VQE-S, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file by adding the following VCDB parameters and specifying the needed values for each:

- system.snmp.ro_community_string="*community_string*"
- system.snmp.location="*server_location*"
- system.snmp.contact="*contact_person*"
- system_snmp_trap_listener="*listener_IP_or_host_name*"

For more information on the SNMP-related VCDB parameters, see Table A-6 on page A-8.

The following example shows the four vcdb.conf lines that specify the SNMP parameters:

```
system.snmp.ro_community_string="XXYYZZ"
system.snmp.location="Building 6 San Francisco"
system.snmp.contact="Helen_Lee@company.com"
system_snmp_trap_listener="192.0.2.25"
```

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-21. You reboot once when all VCDB configuration tasks are completed.

Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS

In your IPTV deployment, VQE Channel Provisioning Tool (VCPT) or another channel-provisioning server sends channel information to the VQE Servers. You must configure each CDE110 that hosts VQE-S so that only trusted HTTPS clients (the channel-provisioning servers) can send the channel information to the CDE110. If VCPT is the channel-provisioning server, the IP addresses of all Ethernet interfaces (that have been assigned IP addresses) on the VCPT host must be configured as trusted HTTPS clients on the VQE-S host.

For more information on VCPT and how it sends channel information, see the "VQE Channel Provisioning Tool and Channel Information" section on page 1-14.

The system.iptables.trusted_provisioner parameter is for enhanced communications security beyond HTTPS. The VQE-S server is configured so that only trusted HTTPS clients (as specified in system.iptables.trusted_provisioner) can send it information using HTTPS.

To allow only traffic from trusted HTTPS clients on the CDE110 port used for HTTPS, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more vqe.iptables.trusted_provisioner parameters and specifying the IP address of a trusted channel-provisioning server, such as VCPT. For example:

```
system.iptables.trusted_provisioner="10.86.17.200"
```

In the preceding example, `10.86.17.200` is the IP address of a trusted channel-provisioning server.

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-21. You reboot once when all VCDB configuration tasks are completed.

Starting VQE-S System Services and Verifying Status

For the CDE110 that hosts VQE-S, Table D-1 lists the system services that you configure and start. Use of the SNMP and NTP services are optional depending on your deployment requirements.

Table D-1 System Services for CDE110 That Hosts VQE-S

Service	Description
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.
snmpsa	(Optional) The SNMP subagent.
ntpd	(Optional) The NTP daemon.
check_daemons	A script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a **cron** job owned by root.
If OSPF Is Selected as the Routing Type	
watchquagga	The Quagga watchdog process. If a Quagga daemon crashes or hangs, watchquagga restarts it automatically.
ospfd	The OSPF daemon.
zebra	The zebra daemon.

To start the VQE-S system services and verify their status, follow these steps:

Note In the following procedure, abbreviated output is shown for some commands.

Step 1 If needed, log in as root on the CDE110 that hosts VQE-S.

Step 2 To configure the system services to be managed by **chkconfig** and started automatically at run levels 2, 3, 4, and 5, and to start the services, issue the following commands:

```
[root@system]# chkconfig --add sshd
[root@system]# chkconfig sshd on
[root@system]# service sshd start

[root@system]# chkconfig --add httpd
[root@system]# chkconfig httpd on
[root@system]# service httpd start
```

```
[root@system]# chkconfig --add tomcat5
[root@system]# chkconfig tomcat5 on
[root@system]# service tomcat5 start
```

The following commands for the Quagga routing package and OSPF are optional depending on whether these services for Quagga and OSPF are used in your deployment:

```
[root@system]# chkconfig --add ospfd
[root@system]# chkconfig ospfd on
[root@system]# service ospfd start

[root@system]# chkconfig --add zebra
[root@system]# chkconfig zebra on
[root@system]# service zebra start

[root@system]# chkconfig --add watchquagga
[root@system]# chkconfig watchquagga on
[root@system]# service watchquagga start
```

The following commands for SNMP, SNMP subagent, and NTP are optional depending on whether these services are used in your deployment:

```
[root@system]# chkconfig --add snmpd
[root@system]# chkconfig snmpd on
[root@system]# service snmpd start

[root@system]# chkconfig --add snmpsa
[root@system]# chkconfig snmpsa on
[root@system]# service snmpsa start

[root@system]# chkconfig --add ntpd
[root@system]# chkconfig ntpd on
[root@system]# service ntpd start
```

Step 3 To configure the check_daemons script to run as a **cron** job under root, issue the following command:

```
[root@system]# /usr/bin/check_daemons >> /var/spool/cron/root
```

Step 4 To verify the sshd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep sshd

sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service sshd status

sshd (pid 2772) is running...

[root@system]# ps -ef | grep sshd

root      2772     1  0 Jul23 ?        00:00:00 /usr/sbin/sshd
```

Step 5 To verify the httpd run levels and that the services and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep httpd

httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service httpd status

httpd (2894) is running...
```

```
[root@system]# ps -ef | grep httpd

apache     447  2894  0 Jul23 ?        00:00:00 /usr/sbin/httpd
root      2894     1  0 Jul02 ?        00:00:00 /usr/sbin/httpd
apache   30078  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30079  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30080  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30082  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30083  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30084  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30085  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30087  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
```

Step 6 To verify the tomcat5 run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep tomcat5

tomcat5         0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service tomcat5 status

Tomcat is running...

[root@system]# ps -ef | grep tomcat5

root     19800     1  0 Jul23 ?        00:00:08 /usr/java/default/bin/java
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.util.logging.config.file=/usr/share/tomcat5/conf/logging.properties
-Djava.endorsed.dirs=/usr/share/tomcat5/common/endorsed -classpath
:/usr/share/tomcat5/bin/bootstrap.jar:/usr/share/tomcat5/bin/commons-logging-api.jar
-Dcatalina.base=/usr/share/tomcat5 -Dcatalina.home=/usr/share/tomcat5
-Djava.io.tmpdir=/usr/share/tomcat5/temp org.apache.catalina.startup.Bootstrap start
```

Step 7 If you have configured OSPF and started the ospfd service, to verify the ospfd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep ospfd

ospfd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service ospfd status

ospfd (pid 6173) is running...

[root@system]# ps -ef | grep ospfd

quagga    6173     1  0 Sep22 ?        00:00:07 /usr/sbin/ospfd -d -A 127.0.0.1 -f
/etc/quagga/ospfd.conf
```

Step 8 If you have configured OSPF and started the zebra service, to verify the zebra run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep zebra

zebra           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service zebra status

zebra (pid 6139) is running...

[root@system]# ps -ef | grep zebra

quagga    6139     1  0 Sep22 ?        00:00:00 /usr/sbin/zebra -d -A 127.0.0.1 -f
```

```
/etc/quagga/zebra.conf
```

Step 9 If you have configured OSPF and started the watchquagga service, to verify the watchquagga run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep watchquagga

watchquagga     0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service watchquagga status

watchquagga (pid 2513) is running...

[root@system]# ps -ef | grep watchquagga

root      2513     1  0 Sep15 ?        00:00:00 /usr/sbin/watchquagga -Az -d -b_
-r/sbin/service_%s_restart -s/sbin/service_%s_start -k/sbin/service_%s_stop zebra
ospfd
```

Step 10 If you have configured and started the SNMP service, to verify the snmpd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep snmpd

snmpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service snmpd status

snmpd (pid 17654) is running...

[root@system]# ps -ef | grep snmpd

root     17654     1  0 Jul25 ?        00:09:24 /usr/sbin/snmpd -Lsd -Lf /dev/null -p
/var/run/snmpd.pid -a
```

Step 11 If you have configured and started the SNMP subagent service, to verify the snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep snmpsa

snmpsa          0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service snmpsa status

The SNMP subagent is running.

[root@system]# ps -ef | grep snmpsa

root     17678     1  0 Jul25 ttyS1    00:09:14 /usr/local/snmpsa/bin/smSubagent
```

Step 12 If you have configured and started the NTP service, to verify that the ntpd service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep ntpd

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

[root@system]# service ntpd status

ntpd (pid 17219) is running...

[root@system]# ps -ef | grep ntpd
```

```
ntp      17219     1  0 Jul25 ?        00:00:06 ntpd -u ntp:ntp -p /var/run/ntpd.pid
-g
```

Starting the VQE-S Processes and Verifying Status

To start the VQE-S service and processes and verify status, follow these steps:

Step 1 If needed, log in as root on the CDE110 that hosts VQE-S.

Step 2 To configure the VQE-S service to be managed by **chkconfig** and started automatically at run levels 2, 3, 4, and 5, and to start the service, issue the following commands:

```
[root@system]# chkconfig --add vqes
[root@system]# chkconfig vqes on
[root@system]# service vqes start
```

Note System error messages are displayed indicating that the VQE-S processes are starting without a channel configuration file. *This is normal behavior* because a channel configuration file from the VQE Channel Provisioning Tool (VCPT) has not yet been sent to VQE-S. Creating and sending the file is done when the Cisco CDE110 that hosts VCPT is configured, and VCPT is used to create and send the file.

Step 3 To verify that the VQE-S service is running, issue the following command:

```
[root@system]# service vqes status

process_monitor (pid 15189) is running...
```

Step 4 To check that the VQE-S processes are running, issue the following commands:

```
[root@system]# ps -ef | grep vqe

root     15189     1  0 11:46 ttyS1    00:00:00 /opt/vqes/bin/process_monitor
vqes     15202 15189  0 11:46 ttyS1    00:00:00 stun_server --ss-uid 499 --ss-gid 499
--xmlrpc-port 8054 --log-level 6
root     15226 15189 99 11:46 ttyS1    06:31:33 vqes_dp --group vqes --max-pkts
1000000 --log-level 6 --rtp-inactivity-tmo 300 --max-core-bw 900000000
--reserved-core-rcv-bw 350000000 --reserved-core-er-bw 200000000
vqes     15280 15189 28 11:46 ttyS1    00:35:04 vqes_cp --cp-uid 499 --cp-gid 499
--xmlrpc-port 8051 --cfg /etc/opt/vqes/vqe_channels.cfg --er-cache-time 3000
--rtp-hold-time 20 --max-channels 500 --max-clients 32000 --exporter-enable --vqm-host
11.8.1.2 --vqm-port 8312 --client-er-tb-rate-ratio 5 --client-er-tb-depth 10000
--log-level 6 --rcc-mode conservative --igmp-join-variability 100 --max-client-bw 0
--max-idr-penalty 0 --rap-interval 2000 --excess-bw-fraction 20
--rcc-burst-delay-to-send 10 --rtp-dscp 0 --rtcp-dscp 24 --overlap-loss 0
--intf-output-allocation 75

[root@system]# ps -ef | grep mlb

root     15206 15189  0 11:46 ttyS1    00:00:04 mlb --interface eth2 eth3 eth4
--add-routes 0.0.0.0/0~10.2.15.1,0.0.0.0/0~10.2.16.1,0.0.0.0/0~10.2.17.1 --xmlrpc-port
8052 --unicast-reservation 20 --poll-interval 1 --ssm --log-level 6
```

In the preceding output, the VQE-S processes to check for are as follows:

- process_monitor—Process Monitor

- stun_server—STUN Server
- vqes_dp—Data Plane
- vqes_cp—Control Plane
- mlb—Multicast Load Balancer

Step 5 To use the VQE-S Application Monitoring Tool from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE-S:

```
https://ip_address_of_VQES_host
```

Log in using the vqe username and password. (Any valid Linux username and password can be used to log in to the VQE-S Application Monitoring Tool.)

If you click **System** in the left pane, the VQE-S Application Monitoring Tool displays information on the VQE-S processes. Figure 4-2 on page 4-4 shows an example.

Restarting the System and Verifying System and VQE-S Status

To restart the Cisco CDE110 and verify system and VQE-S status, follow these steps:

Note The output for the commands issued in this section has been omitted. For example output, see the previous sections in this chapter where the same commands were issued.

Step 1 If needed, log in as root on the CDE110 that hosts VQE-S.

Step 2 To restart the system, issue the following command:

```
[root@system]# reboot
```

The operating system boots.

Note Syslog error messages are displayed indicating that the VQE-S processes are starting without a channel configuration file. *This is normal behavior* because a channel configuration file from the VQE Channel Provisioning Tool (VCPT) has not yet been sent to VQE-S. Creating and sending the file is done when the Cisco CDE110 that hosts VCPT is configured, and VCPT is used to create and send the file.

Step 3 Log in as root.

Step 4 To verify that interfaces eth1 to eth6 are up and running and the IP address and netmask for each are set correctly, issue the following command:

```
[root@system]# ifconfig -a

... Output omitted
```

Step 5 To check that the vqes service is running, issue the following command:

```
[root@system]# service vqes status

... Output omitted
```

Step 6 To check that the STUN Server process is running, issue the following command:

```
[root@system]# ps -ef | grep stun

... Output omitted
```

Step 7 To verify that the sshd service is running, issue the following command:

```
[root@system]# service sshd status

... Output omitted
```

Step 8 To verify that the httpd service is running, issue the following command:

```
[root@system]# service httpd status

... Output omitted
```

Step 9 To verify that the tomcat5 service is running, issue the following command:

```
[root@system]# service tomcat5 status

... Output omitted
```

Step 10 If you have configured OSPF, to verify the ospfd service is running, issue the following command:

```
[root@system]# service ospfd status

... Output omitted
```

Step 11 If you have configured OSPF, to verify the zebra service is running, issue the following command:

```
[root@system]# service zebra status

... Output omitted
```

Step 12 If you have configured OSPF, to verify the watchquagga service is running, issue the following command:

```
[root@system]# service watchquagga status

... Output omitted
```

Step 13 If you have configured SNMP, to verify that the snmpd service is running, issue the following command:

```
[root@system]# service snmpd status

... Output omitted
```

Step 14 If you have configured SNMP, to verify that the snmpsa service is running, issue the following command:

```
[root@system]# service snmpsa status

... Output omitted
```

Step 15 If you have configured an NTP server, to verify that the ntpd service is running, issue the following command:

```
[root@system]# service ntpd status

... Output omitted
```

Step 16 Do one of the following:

- If the preceding checks indicate that all is well, proceed to the "Setting Up a Cisco CDE110 That Hosts VQE Tools" section on page D-24.

- If one of the preceding checks fails, inspect the configuration of the item that failed and make any needed adjustments.

Setting Up a Cisco CDE110 That Hosts VQE Tools

This section explains how to perform the initial configuration tasks for a Cisco CDE110 hosting VQE Tools (VQE Channel Provisioning Tool [VCPT] and VQE Client Channel Configuration Delivery Server).

When performed manually, the initial configuration tasks involve editing the /etc/opt/vqes/vcdb.conf file to configure the essential VCDB parameters. The use of the vcdb.conf file simplifies the configuration tasks. Because the VQE Configuration Tool automatically applies the VCDB values to the /etc configuration files on system reboot, mistakes in configuration file syntax are unlikely.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-12.

Perform these initial configuration tasks in the order shown:

1. Prerequisites for a Cisco CDE110 That Hosts VQE Tools, page D-24
2. Configuring the Linux Operating System for VQE Tools, page D-25
3. Configuring a Static Route for a Management Network (VQE Tools Host), page D-27
4. Synchronizing the Time and Configuring Network Time Protocol, page D-28
5. Configuring SNMP (Optional), page D-29
6. Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS, page D-29
7. Starting VQE Tools System Services and Verifying Status, page D-30
8. Starting the VCDS Service and Verifying VCDS and VCPT Status, page D-33
9. Restarting the System and Verifying System, VCPT, and VCDS Status, page D-34

On the VQE Tools server, proper route configuration is needed for external access to the VQE Tools server. You can use the static management route explained in the "Configuring a Static Route for a Management Network (VQE Tools Host)" section on page D-27 to configure this access.

Note The configuration instructions in this section are intended for new installations of Cisco VQE Release 3.2 software, where the Cisco CDE110 has the Cisco VQE Release 3.2 software preinstalled.

For information on *upgrading an already configured* Cisco CDE110 from Cisco VQE Release 2.1, 3.0, or 3.1 to Release 3.2, see the *Release Notes for Cisco CDA Visual Quality Experience, Release 3.2*.

Prerequisites for a Cisco CDE110 That Hosts VQE Tools

This section explains tasks that should be performed before setting up a Cisco CDE110 that hosts VQE Tools.

Connecting Cables

For information on connecting cables on the VQE Tools server, see the "Connecting Cables to the CDE110" section on page 2-3.

For the location of connectors on the Cisco CDE110 front and back panels, see the *Cisco Content Delivery Engine 110 Hardware Installation Guide*.

Setting Up SSL Certificates for VCPT

It is recommended that you deploy your own or commercial Secure Sockets Layer (SSL) certificates prior to beginning the tasks for setting up a Cisco CDE110 that hosts VCPT. For information on setting up the certificates, see the "Setting Up SSL Certificates" section on page 2-4.

Configuring the Linux Operating System for VQE Tools

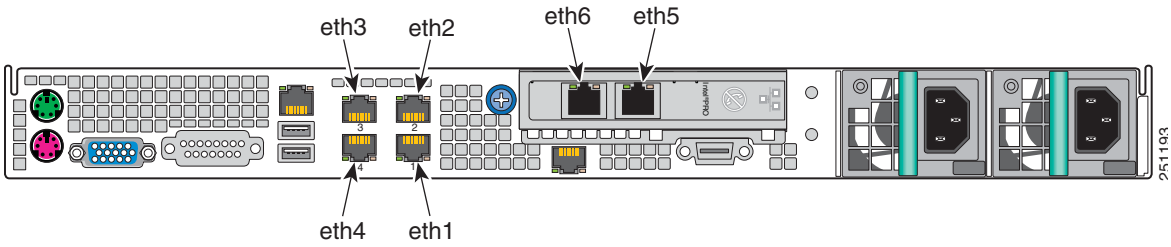
This section explains the initial Linux configuration tasks needed for a Cisco CDE110 appliance that will run the VQE Tools (VCPT and VQE Client Channel Configuration Delivery Server) software. The explanation assumes that the needed software for Linux, VCPT, and VQE Client Channel Configuration Delivery Server have been pre-installed on the Cisco CDE110 appliance. For Red Hat Linux 5.1 documentation, go to the following web site:

http://www.redhat.com/docs/manuals/enterprise/

For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE110 back panel are specified as eth1 to eth6 as shown in Figure D-4.

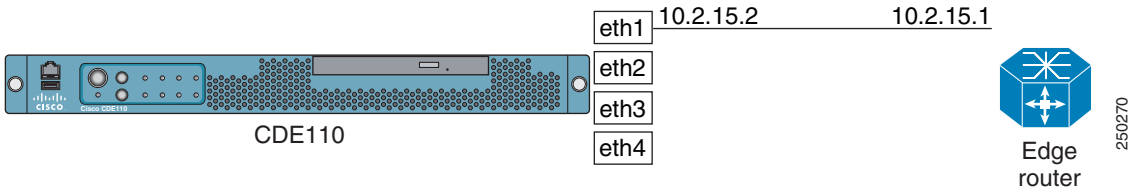
Note Earlier models of the CDE110 have four Ethernet ports (eth1 to eth4). These models did not have the Intel PRO/1000 PT Dual Port Server Adapter that provides the eth5 and eth6 ports.

Figure D-4 NIC Port Numbering for Software Configuration



For the configuration examples in this section, Figure D-5 shows the IP addresses for interface eth1 and the corresponding interface on the edge router.

Figure D-5 IP Addresses for VQE Tools Configuration Examples



Note The configuration examples in this section assume that one CDE110 Ethernet interface (eth1) will be used to connect to the VQE network.

To configure the Linux operating system and other software for the VQE Tools (VCPT and VQE Client Channel Configuration Delivery Server [VCDS]), follow these steps:

Step 1 If needed, login as root. You must have root privileges to modify the vcdb.conf file.

Step 2 To create the password for the vqe username (a pre-created Linux user ID), issue the following command:

```
[root@system]# passwd vqe
```

Enter a password that follows the password guidelines:

```
A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use an 8 character long
password with characters from at least 3 of these 4 classes, or
a 7 character long password containing characters from all the
classes.  An upper case letter that begins the password and a
digit that ends it do not count towards the number of character
classes used.

A passphrase should be of at least 3 words, 12 to 40 characters
long and contain enough different characters.
```

This username and password can be used to log in to Linux directly using SSH. The vqe username and password can also be used log in to the VQE Channel Provisioning Tool.

Step 3 To configure CDE110 Ethernet interfaces eth1 to eth6, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.eth*x*.addr parameters, where eth*x* is eth1, eth2, and so on. Specify an IP address and prefix length for each interface. The following example shows one vcdb.conf line for the eth1 Ethernet interface:

```
network.eth1.addr="10.2.15.2/24"
```

Step 4 To configure the hostname for the CDE110 server, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the system.global.hostname parameter and specifying a hostname. The following example specifies the hostname as starfire1-iptv:

```
system.global.hostname="starfire1-iptv"
```

Step 5 To configure a DNS server, edit the /etc/opt/vqes/vcdb.conf file by adding the VCDB parameters for the IP address and optionally for the search domain of a DNS server and specifying the needed values:

- system.dns.server="*IP_address*"
- system.dns.search_domain="*search_domain*"

For example:

```
system.dns.server="192.0.20.53."
system.dns.search_domain="domain.com"
```

Step 6 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System, VCPT, and VCDS Status" section on page D-34. You reboot once when all VCDB configuration tasks are completed.

After the VQE Tools host is rebooted, you can verify that the eth1 interface is configured correctly and up and running.

- Use the **ifconfig** *interface* command to verify that the Ethernet interface is up and running and the IP address and netmask is set correctly. The following example is for eth1:

```
[root@system]# ifconfig eth1

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:C6:F3:0F
          inet addr:10.2.15.2  Bcast:10.2.15.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fec6:f30f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:192 (192.0 b)  TX bytes:2700 (2.6 KiB)
          Base address:0x3000 Memory:b8800000-b8820000
```

- Use the **ip link show eth#** command (where # is the Ethernet interface number) to check that the link is up. For example:

```
[root@system]# ip link show eth1

eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0e:0c:c6:e4:fe brd ff:ff:ff:ff:ff:ff
```

- Use the **ping** command to check that the Cisco CDE110 can reach the connected edge router. For example:

```
[root@system]# ping 10.2.15.1
```

Configuring a Static Route for a Management Network (VQE Tools Host)

If your deployment makes use of a management network, a static route for the management network can be configured using the VCDB parameter network.route.mgmt_route. The configuration example in this section assumes that one CDE110 Ethernet interface (eth1) will be used to connect to the VQE network.

On the VQE Tools server, proper route configuration is needed for external access to the VQE Tools server. You can use the static management route to configure this access.

Note If you configure static route for a management network as described in this section, see "Static Route for a Management Network Is Missing on CDE110 Hosting VQE-S or VQE Tools" section on page 5-7 for some additional information.

To configure a static route for a management network, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file by adding to the file a network.route.mgmt_route parameter and specifying the needed values using the following format:

network.route.mgmt_route="*management-network-addr/prefix-length* via *gateway-addr* "

The *management-network-addr/prefix-length* is the IP address and prefix length for the management network. The *gateway-addr* is the IP address of the router interface that is directly attached to the CDE110 Ethernet port that will be used for management network traffic.

For this example, assume the following:

- CDE110 Ethernet interface eth1 (10.2.15.2) will be used for the management network.
- The management network is 192.0.0.0/8.

The line in the vcdb.conf file is as follows:

```
network.route.mgmt_route="192.0.0.0/8 via 10.2.15.1"
```

In the preceding example, 10.2.15.1 is the *gateway-addr*—the router interface that is directly attached to eth1. Figure D-5 shows the IP addresses used in this example for the eth1 interface and the directly attached router.

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System, VCPT, and VCDS Status" section on page D-34. You reboot once when all VCDB configuration tasks are completed.

After the VQE Tools host is rebooted, you can verify that the static route for the management network is present in the routing table by issuing the following command:

```
[root@system]# ip route show
```

The output will be similar to the following:

```
192.0.0.0/8 via 10.2.9.1 dev eth1
```

Synchronizing the Time and Configuring Network Time Protocol

To keep system time correct and synchronized, we recommend that you use Network Time Protocol (NTP) on the VQE Tools host. To synchronize the time and configure NTP, follow these steps:

Step 1 If needed, log in as root on the CDE110 that hosts VQE Tools.

Step 2 To set the time zone, issue the **tzselect** command and follow the prompts:

```
[root@system]# /usr/bin/tzselect
```

Step 3 To set the date and time, issue the **date** command as follows:

date -s "*date_time_string*"

For example:

```
[root@system]# date -s "16:55:30 July 7, 2008"
```

Step 4 Edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more system.ntp.server parameters and specifying the IP address of an NTP server for each of the parameters. For example:

```
system.ntp.server="10.2.26.2"
```

In the preceding example, the IP address of the NTP server is 10.2.26.2.

Step 5 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System, VCPT, and VCDS Status" section on page D-34. You reboot once when all VCDB configuration tasks are completed.

For information on starting the NTP service (ntpd daemon), see the "Starting VQE Tools System Services and Verifying Status" section on page D-30.

Configuring SNMP (Optional)

The CDE110 that hosts VQE Tools uses Net-SNMP, a third-party product, for SNMP support for some basic, non-VQE system services. Net-SNMP offers a set of built-in MIBs for Linux platforms. The use of Net-SNMP is optional. For more information on Net-SNMP support, see Appendix B, "Using Net-SNMP."

To configure SNMP on the Cisco CDE110 that hosts VQE Tools, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file by adding the following VCDB parameters and specifying the needed values for each:

- system.snmp.ro_community_string="*community_string*"
- system.snmp.location="*server_location*"
- system.snmp.contact="*contact_person*"
- system_snmp_trap_listener="*listener_IP_or_host_name*"

For more information on the SNMP-related VCDB parameters, see Table A-6 on page A-8.

The following example shows the four vcdb.conf lines that specify the SNMP parameters:

```
system.snmp.ro_community_string="XXYYZZ"
system.snmp.location="Building 6 San Francisco"
system.snmp.contact="Helen_Lee@company.com"
system_snmp_trap_listener="192.0.2.25"
```

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System, VCPT, and VCDS Status" section on page D-34. You reboot once when all VCDB configuration tasks are completed.

Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS

The system.iptables.trusted_provisioner parameter must be configured for both of the following:

- For a VQE Tools host where a VCDS receives channel information from VCPT, *all Ethernet interfaces* (that have been assigned IP addresses) on the VCPT host sending the channel information must be specified as addresses using the system.iptables.trusted_provisioner parameter. This requirement applies even when the VCDS is in the same VQE Tools server as the VCPT.

- For a VQE Tools host, if a VQE-C system configuration provisioning server sends network configuration information to the VCDS, you specify the IP address of the trusted VQE-C system configuration provisioning server. This type of provisioning server is not currently used in most deployments.

The system.iptables.trusted_provisioner parameter is for HTTPS communications security. The VQE Tools server is configured so that only trusted HTTPS clients (as specified in system.iptables.trusted_provisioner) can send it information using HTTPS.

To allow only traffic from trusted HTTPS clients on the CDE110 port used for HTTPS, follow these steps:

Step 1 If needed, log in as root. You must have root privileges to modify the vcdb.conf file.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more vqe.iptables.trusted_provisioner parameters and specifying the IP addresses as explained in the preceding discussion. For example, when VCPT send channel information to one of more VCDS's, you specify the IP addresses of *all Ethernet interfaces* that has been assigned an IP address on the VQE Tools host.

```
system.iptables.trusted_provisioner="10.2.15.2"
```

In the preceding example, `10.2.15.2` is the IP address of the only Ethernet interface that has been assigned an IP address on the VQE Tools host.

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-21. You reboot once when all VCDB configuration tasks are completed.

Starting VQE Tools System Services and Verifying Status

For the CDE110 that hosts VQE Tools, Table D-2 lists the system services that you configure and start. Use of the SNMP and NTP services are optional depending on your deployment's requirements.

Table D-2 System Services for CDE110 That Hosts VQE Tools

Service	Description
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.
snmpsa	(Optional) The SNMP subagent.
ntpd	(Optional) The NTP daemon.
check_daemons	A script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a **cron** job owned by root.

To start the VQE Tools system services and verify their status, follow these steps:

Note In the following procedure, abbreviated output is shown for some commands.

Step 1 If needed, log in as root on the CDE110 that hosts VQE Tools.

Step 2 To configure the system services to be managed by **chkconfig** and started automatically at run levels 2, 3, 4, and 5, and to start the services, issue the following commands:

```
[root@system]# chkconfig --add sshd
[root@system]# chkconfig sshd on
[root@system]# service sshd start

[root@system]# chkconfig --add httpd
[root@system]# chkconfig httpd on
[root@system]# service httpd start

[root@system]# chkconfig --add tomcat5
[root@system]# chkconfig tomcat5 on
[root@system]# service tomcat5 start
```

The following commands for SNMP and NTP are optional depending on whether these services are used in your deployment:

```
[root@system]# chkconfig --add snmpd
[root@system]# chkconfig snmpd on
[root@system]# service snmpd start

[root@system]# chkconfig --add snmpsa
[root@system]# chkconfig snmpsa on
[root@system]# service snmpsa start

[root@system]# chkconfig --add ntpd
[root@system]# chkconfig ntpd on
[root@system]# service ntpd start
```

Step 3 To configure the check_daemons script to run as a **cron** job under root, issue the following command:

```
[root@system]# /usr/bin/check_daemons >> /var/spool/cron/root
```

Step 4 To verify the sshd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep sshd

sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service sshd status

sshd (pid 2772) is running...

[root@system]# ps -ef | grep sshd

root      2772     1  0 Jul23 ?        00:00:00 /usr/sbin/sshd
```

Step 5 To verify the httpd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep httpd

httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service httpd status
```

```
httpd (2894) is running...

[root@system]# ps -ef | grep httpd

apache     447  2894  0 Jul23 ?        00:00:00 /usr/sbin/httpd
root      2894     1  0 Jul02 ?        00:00:00 /usr/sbin/httpd
apache   30078  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30079  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30080  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30082  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30083  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30084  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30085  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30087  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
```

Step 6 To verify the tomcat5 run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep tomcat5

tomcat5         0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service tomcat5 status

Tomcat is running...

[root@system]# ps -ef | grep tomcat5

root     19800     1  0 Jul23 ?        00:00:08 /usr/java/default/bin/java
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.util.logging.config.file=/usr/share/tomcat5/conf/logging.properties
-Djava.endorsed.dirs=/usr/share/tomcat5/common/endorsed -classpath
:/usr/share/tomcat5/bin/bootstrap.jar:/usr/share/tomcat5/bin/commons-logging-api.jar
-Dcatalina.base=/usr/share/tomcat5 -Dcatalina.home=/usr/share/tomcat5
-Djava.io.tmpdir=/usr/share/tomcat5/temp org.apache.catalina.startup.Bootstrap start
```

Step 7 If you have configured and started the SNMP daemon, to verify the snmpd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep snmpd

snmpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service snmpd status

snmpd (pid 17654) is running...

[root@system]# ps -ef | grep snmpd

root     17654     1  0 Jul25 ?        00:09:24 /usr/sbin/snmpd -Lsd -Lf /dev/null -p
/var/run/snmpd.pid -a
```

Step 8 If you have configured and started the SNMP subagent, to verify the snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep snmpsa

snmpsa          0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service snmpsa status

The SNMP subagent is running.
```

```
[root@system]# ps -ef | grep snmpsa

root     17678     1  0 Jul25 ttyS1    00:09:14 /usr/local/snmpsa/bin/smSubagent
```

Step 9 If you have configured and started the NTP service, to verify run levels and that the ntpd service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep ntpd

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

[root@system]# service ntpd status

ntpd (pid 17219) is running...

[root@system]# ps -ef | grep ntpd

ntp      17219     1  0 Jul25 ?        00:00:06 ntpd -u ntp:ntp -p /var/run/ntpd.pid
-g
```

Starting the VCDS Service and Verifying VCDS and VCPT Status

This section explains how to start the VQE Client Channel Configuration Delivery Server (VCDS) service and verify that the process is running and that VCPT is available.

Note VCPT is a web application and has no dedicated processes associated with it. The processes needed for the VCPT web application to work (for example, the web server) are started automatically when the Cisco CDE110 is started.

To start the VCDS service and verify VCDS and VCPT status, follow these steps:

Step 1 If needed, log in as root on the CDE110 that hosts VQE Tools.

Step 2 To configure the VCDS service to be managed by **chkconfig** and started automatically at run levels 2, 3, 4, and 5, and to start the service, issue the following commands:

```
[root@system]# chkconfig --add vcds
[root@system]# chkconfig vcds on
[root@system]# service vcds start
```

Step 3 To verify that the VCDS service is running, issue the following command:

```
[root@system]# service vcds status

VQECCfgDeliveryServer (pid 29860) is running...
```

Step 4 To check that the VCDS process (VQECCfgDeliveryServer) is running, issue the following command:

```
[root@system]# ps -ef | grep VQECCfg

root     29860     1  0 Jul25 ?        00:00:00 /opt/vqes/bin/VQECCfgDeliveryServer -d
-f /etc/opt/vqes/VCDServer.cfg
```

Step 5 To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VCPT:

```
https://ip_address_of_VCPT_host
```

Log in using the vqe username and password. (Any valid Linux username and password can be used to log in to VCPT.)

If you are able to log in successfully, VCPT is running correctly.

Restarting the System and Verifying System, VCPT, and VCDS Status

To restart the Cisco CDE110 and verify system, VCPT, and VQE Client Channel Configuration Delivery Server (VCDS) status, follow these steps:

Note The output for the commands issued in this section has been omitted. For example output, see the previous sections in this chapter where the same commands were issued.

Step 1 If needed, log in as root on the CDE110 that hosts VQE Tools.

Step 2 To restart the system, issue the following command:

```
[root@system]# reboot
```

The operating system boots.

Step 3 To verify that interface eth1 is up and running and the IP address and netmask is set correctly, issue the following command:

```
[root@system]# ifconfig -a

... Output omitted
```

Step 4 To verify that the sshd service is running, issue the following command:

```
[root@system]# service sshd status

... Output omitted
```

Step 5 To verify that the httpd service is running, issue the following command:

```
[root@system]# service httpd status

... Output omitted
```

Step 6 To verify that the tomcat5 service is running, issue the following command:

```
[root@system]# service tomcat5 status

... Output omitted
```

Step 7 If you have configured SNMP, to verify that the snmpd service is running, issue the following command:

```
[root@system]# service snmpd status

... Output omitted
```

Step 8 If you have configured SNMP, to verify that the snmpsa service is running, issue the following command:

```
[root@system]# service snmpsa status

... Output omitted
```

Step 9 If you have configured an NTP server, to verify that the ntpd service is running, issue the following command:

```
[root@system]# service ntpd status

... Output omitted
```

Step 10 To check that the vcds service is running, issue the following command:

```
[root@system]# service vcds status

... Output omitted
```

Step 11 To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VCPT:

```
https://ip_address_of_VCPT_host
```

Log in with a Linux username and password.

If you are able to log in successfully, VCPT is running correctly.

Step 12 Do one of the following:

- If the preceding checks indicate that all is well, you are ready to start using VCPT. For information, see Chapter 3, "Using the VQE Channel Provisioning Tool."
- If one of the preceding checks fails, inspect the configuration of the item that failed and make any needed adjustments.

APPENDIX E

Configuring DHCP and DNS Servers for VCDS

The VQE configuration delivery infrastructure (CDI) is used to deliver channel configuration information to the VQE Clients in a VQE system. VQE Client Channel Configuration Delivery Server (VCDS) or an RTSP server sends the channel configuration file to the VQE Client on the set-top box.

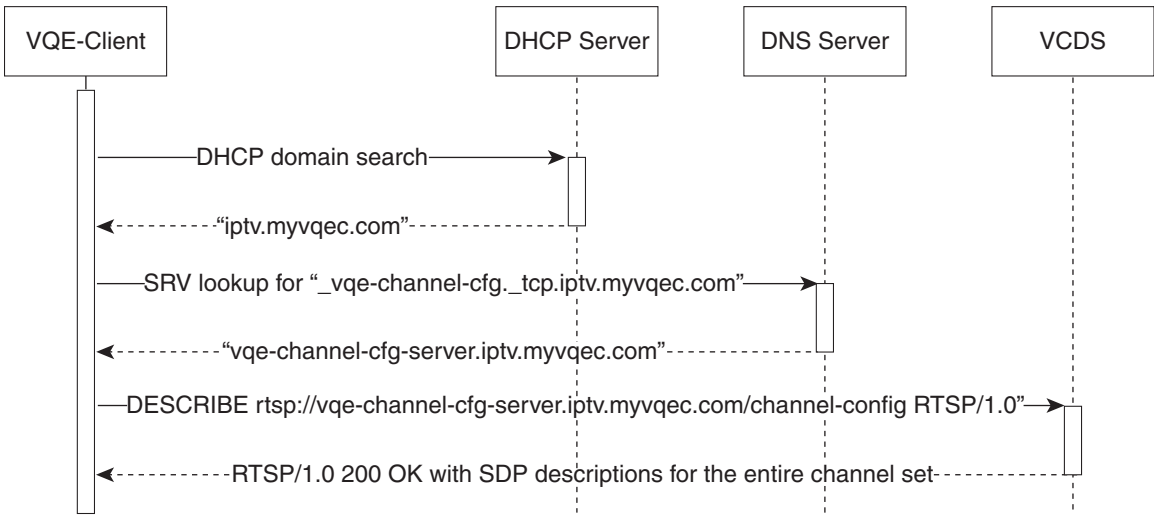
This appendix provides information on configuring the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers so that they work correctly with VCDS or an RTSP server compatible with the VQE CDI. This appendix assumes you have knowledge of DHCP and DNS configuration.

Note The VQE-C parameter cdi_enable must be set to “true” to enable VQE-C to use the configuration delivery infrastructure. For information on the VQE-C system configuration parameters, see the VQE-C documentation that is provided in the VQE-C software TAR file.

The components and interactions of the configuration delivery infrastructure are shown in Figure E-1. In this example, VCDS sends the channel configuration file to the VQE Client. The example provides guidance on the following VQE requirements for the DHCP and DNS server configuration.

- For a domain search request, the DHCP server must be configured to provide the domain of the VCDS to the VQE-C.
- For a DNS service request, the DNS server must be configured to return the VCDS server name to VQE-C when the service lookup is for _vqe-channel-cfg._tcp (*exact string required*) with the VCDS domain name appended.

Figure E-1 VQE Configuration Delivery Infrastructure



As shown in Figure E-1, the interactions between the VQE Client and the other components of the configuration delivery infrastructure are as follows:

1. The VQE-C on the set-top box sends out a DHCP domain search request.
2. The DHCP Server returns the domain (in this example, iptv.myvqec.com) that the VCDS is part of. The domain is user-defined and configured in the DHCP server.
3. After receiving the domain name from the DHCP server, VQE-C makes a DNS service request for the following string:

   _vqe-channel-cfg._tcp.iptv.myvqec.com

Note The _vqe-channel-cfg._tcp part of the string is hardcoded in VQE-C and is not configurable. *The DNS server must be configured for this exact string (_vqe-channel-cfg._tcp) with the domain name appended.*

4. The DNS server responds with the VCDS server name defined in SRV records.
5. If the query is successful, VQE-C parses out the VCDS server name from the DNS server response. VQE-C sends out an RTSP DESCRIBE request for the channel configuration data to the VCDS server.
6. VCDS receives the request and sends back the channel configuration data for the entire channel set in SDP format.

If the RTSP DESCRIBE operation succeeds, the VQE-C attempts to update the local channel_lineup file.

If the DNS query or the RTSP DESCRIBE operation fails, the VQE-C attempts to retrieve the channel configuration locally if a channel_lineup file is specified in the VQE-C system configuration file. If the appropriate channel configuration cannot be obtained, the VQE-C does not perform error repair.

APPENDIX F

Changing the Boot Sequence to Start from the CD/DVD Drive

This appendix explains how to change the BIOS setting on the Cisco CDE110 server so that the server boots first from the CD/DVD Combo drive.

For VQE Server and VQE Tools hosts, the CD for an ISO installation of VQE software works correctly only when the BIOS of the Cisco CDE110 server is configured so that the server boots first from the CD/DVD Combo drive.

Note A Cisco CDE110 server with VQE Release 3.0 or later software preinstalled is configured at the factory so that the server boots first from the CD/DVD Combo drive. Therefore, unless someone has changed the BIOS setting for boot sequence or the CDE110 server was delivered with software earlier than VQE Release 3.0, changing the boot sequence should not be needed.

For information on installing VQE software, see the release notes for your version of the VQE software.

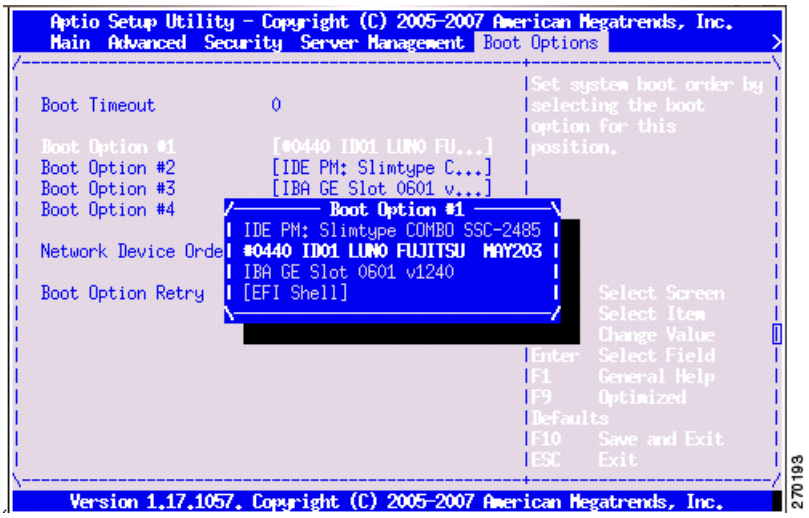
If your CDE110 server is set up so that it boots from something other than the CD/DVD Combo drive, to change the BIOS setting so that the server boots first from the CD/DVD Combo drive, do the following:

Step 1 Power on or power cycle the CDE110.

Step 2 When the system boots and displays “Press <F2> to enter SETUP,” press F2 to go enter BIOS Setup.

Step 3 When the BIOS Setup utility is displayed, use the arrow keys to move to the **Boot Options** menu (Figure F-1).

Figure F-1 Boot Options Menu



Step 4 So that the CD/DVD Combo drive is first in the boot order, you need to change the boot sequence to the following:

1. IDE PM: SlimType COMBO SSC-2485
2. #0440 ID01 LUN0 FUJITSU MAY203
3. IBA GE Slot 0600
4. [EFI SHELL]

Note Because the components used in the CDE110 can vary, the name of the CD/DVD Combo drive may be different from what is shown in the preceding list.

To change the boot sequence, use the arrow keys to move to the boot option you will change (for example, Boot Option #1) and press Enter. Then use the arrow keys to move to the required boot device and press Enter.

The updated Boot Option is displayed.

Step 5 To save and exit the BIOS Setup, press F10. (As an alternative to pressing F10, use the arrow keys to move to **Exit** in the BIOS Setup menu and select **Save Changes and Exit**.)

The Setup Confirmation message “Save Configuration Changes and exit now?” is displayed.

Step 6 Select Yes and press Enter.

The CDE110 restarts.

INDEX

Symbols

A

B

C

D

E

F

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z