



## **Cisco CDA Visual Quality Experience Application User Guide Release 3.5**

October 2010

### **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-14115-10

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*Cisco CDA Visual Quality Experience Application User Guide, Release 3.5*  
©2007–2011 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface ix**

Objectives	ix
Document Revision History	ix
Document Organization	x
Related Documentation	xi
Document Conventions	xii
Obtaining Documentation and Submitting a Service Request	xiii
3-xiii	

---

## **CHAPTER 1**

### **Introduction to Cisco CDA**

#### **Visual Quality Experience Application 1-1**

VQE Overview	1-1
Introduction to VQE	1-2
VQE Major Software Components	1-4
VQE Hybrid Error Repair	1-4
VQE RCC	1-5
RTP and RTCP	1-7
VQE Web Browser-based Tools	1-7
Lookaside Mode and the Cisco CDE110	1-8
VQE Benefits	1-8
VQE-S	1-9
VQE-S High Availability	1-10
Support for All NAT Mapping Types	1-10
VQE-C	1-11
VQE-C Forward Error Correction	1-12
VQE-C IPTV Packet Loss Monitoring	1-13
VQE-C Software Development Kit and Documentation	1-13
VQE Deployment Options and Requirements	1-14
VQE Reference Architecture Model	1-14
Cisco End-to-End IPTV Solution Model	1-14
VQE Deployment Requirements	1-14
VCPT and Channel Information	1-15
VCDS	1-17

- VCDS Delivery of the Channel Configuration File 1-17
- VCDS Delivery of the Per-Client Network Configuration File 1-18
  - VQE-C System Configuration Provisioning Server Role 1-20
  - VCDS Role 1-20
  - VQE-C Role 1-20
- VQE-S AMT 1-21
- VQE-S RTCP Exporter for Video-Quality Monitoring 1-23
- VCDS AMT 1-24
- Content Delivery Engine 110 1-26

**CHAPTER 2**

- Getting Started with the VQE Startup Configuration Utility 2-1**
  - Web Browser, Screen Resolution, and Other Requirements 2-2
  - System Port Numbers 2-3
  - Configuring Terminal Emulation Software 2-3
  - Security Restrictions for Logins and Root Privileges 2-4
  - Prerequisites 2-4
    - Connecting Cables to the CDE110 2-4
    - Setting Up SSL Certificates with the VQE Startup Configuration Utility 2-5
  - Setting Up SSL Certificates 2-5
    - Using the Cisco VQE Startup Configuration Utility for SSL Certificates 2-6
      - Step-by-Step Example: Creating and Deploying Self-Signed Certificates Using the Cisco VQE Startup Configuration Utility 2-7
    - Creating Your Own Certificate Authority 2-9
    - Generating and Deploying Your Own SSL Certificates 2-10
      - Generating a Certificate-Signing Request 2-10
      - Signing the Certificate-Signing Request 2-11
      - Installing the Certificates, Private Key, and Keystore 2-12
    - Deploying Commercial SSL Certificates 2-13
      - Commercial CA: Installing the Certificates, Private Key, and Keystore 2-13
  - VQE-S: Routing and Interface Configuration Overview 2-14
    - Bond Interfaces on a VQE-S 2-15
    - Types of Routes on a VQE-S 2-16
    - Static Routes on a VQE-S 2-16
    - OSPF Routing on a VQE-S 2-17
    - Using Dedicated or Shared Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic 2-17
    - Routing Configuration for Dedicated Interfaces and Shared Interfaces 2-18
      - Configuring Static Routes 2-19
    - Interface for a Management Network 2-20

Load Balancing and Redundancy with Multiple VQE-S	2-21
VQE Tools Server: Routing Configuration Overview	2-22
Using the VQE Startup Configuration Utility	2-23
Configuration Parameters	2-24
Preconfiguration Worksheets	2-33
VQE Configuration Tool Root Menu	2-36
On the VQE-S Host: Verifying the Status of the VQE and System Services	2-38
On the VQE Tools Host: Verifying the Status of the VQE and System Services	2-40
Configuring the VQE-S RTCP Exporter	2-42
Configuring the Other Parameters for the VQE-S Host	2-43
Configuring the Edge Router for VQE-S	2-44
For Bond Interfaces: Guidance for Configuring Bond Interface on the Attached Router	2-44
For OSPF Routing: Guidance for Configuring the Attached Router	2-45
VQE-S in a Separate OSPF Area	2-45
VQE-S in Area 0	2-46
General Guidelines	2-46
For Static Routes: Guidance for Configuring the Feedback Targets on the Attached Router	2-47

**CHAPTER 3****Using the VQE Channel Provisioning Tool 3-1**

Logging into VCPT	3-2
Working with VCPT Configuration Files	3-3
Performing Configuration-File Operations	3-4
Importing a Configuration	3-4
Exporting a Configuration	3-5
Sending or Pushing Channel Information to Servers	3-5
Send Button	3-5
Force Update Button	3-6
Sending Channel Information to a Subset of Servers	3-7
Provisioning VQE Channels	3-7
Adding a Channel	3-8
Viewing or Updating Channel Information	3-12
Cloning a Channel	3-13
Deleting a Channel	3-13
Defining VQE-Ss, VCDs, or Remote Servers	3-14
Adding a Server	3-16
Viewing or Updating Server Information	3-17
Deleting a Server	3-18
Defining Channel Associations	3-18

Defining Channel Associations for a Server 3-19  
 Copying Channel Associations from Another Server 3-19  
 Setting-up a SSH Certificate on a Remote Server 3-19

**CHAPTER 4**

**Using the VQE-S AMT 4-1**

Logging into and Navigating in the VQE-S AMT 4-2  
 Monitoring the Health of the VQE-S Processes 4-4  
 Viewing Channel Configuration and Status 4-7  
     Viewing Channel Configuration 4-8  
     Viewing Channel Statistics 4-10  
     Viewing Channel Histograms 4-14  
     Viewing RCC Troubleshooting 4-15  
 Monitoring Unicast Retransmission and RCC 4-16  
     Viewing Error Repair and RCC Configuration 4-16  
     Viewing Error Repair and RCC Statistics 4-17  
     Viewing Excess Bandwidth 4-21  
     Viewing Channel Change Times 4-22  
     Viewing Error Repair and RCC Capacity Statistics 4-23  
 Monitoring Interfaces 4-26  
 Monitoring RTCP Exporter 4-28  
 Monitoring the STUN Server 4-30  
 Resetting VQE-S Counters 4-31  
 Restoring VQE-S Counters 4-32  
 Change VQE-S Logging 4-33  
 Change VQE-S Debugging 4-33

**CHAPTER 5**

**Using the VCDS AMT 5-1**

Logging into and Navigating in VCDS AMT 5-2  
 Monitoring the Health of the VCDS Process and VQE Tools Server 5-3  
 Viewing VCDS Configuration and Statistics 5-4  
     Viewing VCDS Configuration 5-5  
     Viewing VCDS Statistics 5-7  
 Change VCDS Logging 5-7  
 Change VCDS Debugging 5-9

**CHAPTER 6**

**Troubleshooting VQE Software Components 6-1**

Useful Linux Tools 6-1

VQE Logging and Log Files	6-2
VQE Server and VQE Tools Logging and Log Files	6-2
VQE-S AMT, VCDS AMT, and VCPT Logging and Log Files	6-3
VQE Files, Directories, and Permissions	6-3
Changing Permissions	6-5
Replacing a Lost or Corrupt VQE File	6-5
VQE-S and VQE Tools Server Troubleshooting	6-7
Monitoring Received Multicast Streams	6-8
Repeated Message on CDE110 Hosting VQE-S or VQE Tools	6-9
Performing a Date and Time Change with NTP	6-9
Performing a Date and Time Change with the Linux date Command	6-10
VQE-S AMT, VCDS AMT, or VCPT Unavailable	6-10
Channels Are Not Displayed in VQE-S AMT	6-11
VQE-S AMT Channels Status Summary Has No Graphs	6-12
VCPT Fails to Initialize	6-12
Channel-Provisioning Server Cannot Send Channel Information to VQE-S: Trusted Provisioning Client Problem	6-13
Channel-Provisioning Server Cannot Send Channel Information to VQE-S: SSL Certificates Problems	6-13
Unable to Connect Error When VCPT Tries to Send Channel Information	6-14
Internal Server Error When VCPT Tries to Send Channel Information to VQE-S	6-15
RCC Troubleshooting	6-15
VQE-S RCC Troubleshooting	6-16
Channel is not configured on the VQE-S	6-16
Channel is not active on the VQE-S	6-16
RCC is disabled on the channel	6-17
No connectivity between the VQE-C and the FBT on the VQE-S	6-18
No connectivity between the VQE-C and the VQE-S	6-18
RCC refused by the VQE-S control or data planes	6-18
RCC refused by the VQE-S—invalid e-factor	6-19
RCC refused by the VQE-S—insufficient bandwidth	6-19
MPEG Parser is unable to locate the burst start point	6-20
VQE-S MPEG Parser is unable to locate the ECM PID	6-21
Burst start point not found within the backfill range	6-21
No burst start point found—stream is invalid	6-22
VQE-C RCC Troubleshooting	6-23
RCC not enabled on the VQE-C	6-24
Problem with priming information sent from the VQE-S	6-24
First packets from repair burst not received within expected time period	6-25
No multicast stream	6-25

- Output loss during RCC 6-25
- Output packets dropped 6-28
- Using the vqereport Command 6-29
- Gathering Information for a Service Request 6-30
- Stopping, Starting, and Restarting VQE-S 6-30
- Stopping, Starting, and Restarting VCDS 6-31
- Resetting the Root Password on the VQE-S or VQE Tools Server 6-31

**CHAPTER 7**

**Configuring VQE Server and VQE Tools 7-1**

- Managing /etc Configuration Files Using the VQE CMS 7-2
  - Managing /etc Configuration Files with the VQE CMS 7-2
- Using the VQE Configuration Tool 7-3
  - Starting the Configuration Tool and Using the Root Menu 7-3
  - Using the Configuration Tool Menus 7-4
  - Entering Data for Configuration Parameters 7-6
    - Entering Data for Parameters That Can Have Only One Definition 7-6
    - Entering Data for Parameters That Can Have Multiple Definitions 7-7
    - Entering New Values for Parameters That Have a Currently Defined Value 7-8
    - Reverting to the Default VCDB Values 7-10
- VQE Configuration Engine 7-11
- VCDB Parser 7-13
- Manually Editing the VCDB File 7-14
  - Using VCDB File Syntax 7-14
    - Multiple Definitions 7-15
    - Parameter Order 7-15
  - Understanding the vcdb.conf.sample File 7-15
- Using the VQE Configuration Tool Command-Line Options 7-18

**APPENDIX A**

**VQE, System, and Network Parameters A-1**

**APPENDIX B**

**SNMP MIBs B-1**

- SNMP Overview B-1
  - MIB Objects B-1
  - SNMP Notifications B-2
  - Object Identifiers B-2
- VQE MIB Support B-2
  - Net-SNMP B-3
  - Standard Linux MIBs B-4

Syslog MIB	B-5
VQE-Specific MIBs	B-5
CISCO-VQES-MIB	B-5
CISCO-VQE-TOOLS-MIB	B-8
Compiling VQE-Specific MIBs	B-9

**APPENDIX C****VQE System Messages C-1**

System Message Structure	C-1
System Message Example	C-3
Basic Recovery Procedures	C-3
VQE System Messages Reference Information	C-4

**APPENDIX D****Manual Initial VQE System Configuration D-1**

Setting Up a Cisco CDE110 That Hosts VQE-S	D-2
Prerequisites for a Cisco CDE110 That Hosts the VQE-S	D-3
Connecting Cables for the VQE-S	D-3
Setting Up SSL Certificates for the VQE-S	D-3
Configuring the Linux Operating System for the VQE-S	D-3
Configuring Bond Interfaces	D-5
Configuring a Static Route for a Management Network (VQE-S Host)	D-6
Configuring Static Routes for VQE-S Traffic or VQE-S Services Traffic (VQE-S Host)	D-8
Enabling OSPF Routing for VQE-S Traffic or VQE-S Services Traffic	D-10
Configuring Interfaces for VQE-S Traffic (Ingest and Services) and VQE-S Services Traffic	D-15
Configuring Dedicated Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic	D-16
Configuring Shared Interfaces for All VQE-S Traffic	D-17
Synchronizing the Time and Configuring Network Time Protocol	D-19
VQE STUN Server Is Enabled By Default	D-20
Configuring SNMP	D-20
Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS	D-21
Configuring Remote Syslog Servers	D-22
Starting VQE-S System Services and Verifying Status	D-22
Starting the VQE-S Processes and Verifying Status	D-27
Restarting the System and Verifying System and VQE-S Status	D-28
Setting Up a Cisco CDE110 That Hosts VQE Tools	D-30
Prerequisites for a Cisco CDE110 That Hosts VQE Tools	D-32
Connecting Cables	D-32
Setting Up SSL Certificates for VCPT	D-32
Configuring the Linux Operating System for VQE Tools	D-32
Configuring a Static Route for a Management Network (VQE Tools Host)	D-34

Synchronizing the Time and Configuring Network Time Protocol **D-36**  
 Configuring SNMP **D-37**  
 Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS **D-38**  
 Configuring Remote Syslog Servers **D-39**  
 Starting VQE Tools System Services and Verifying Status **D-39**  
 Starting the VCDS Service and Verifying VCDS, VCDS AMT and VCPT Status **D-43**  
 Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status **D-44**

**APPENDIX E**

**Configuring DHCP and DNS Servers for VCDS E-1**

**APPENDIX F**

**Using the vcds\_send\_file Command F-1**

VQE CDI and VQE-C Network-based Per-Client Configuration **F-1**  
 The vcds\_send\_file Command **F-2**

**APPENDIX G**

**Changing the Boot Sequence to Start from the CD/DVD Drive G-1**

**CHAPTER H**

**VQE Server Performance and Scaling Limits H-1**

Ingress and Egress Bandwidth Limits **H-1**  
 Scaling and Performance Summary **H-2**  
 VQE-S Capacity Statistics **H-3**

**APPENDIX I**

**VCPT Configuration Files I-1**

Introduction **I-1**  
 VCPT Configuration File Data Rules **I-2**  
 VCPT Configuration in XML Format **I-8**  
     XML Schema **I-8**  
     XML Data Elements and Attributes **I-16**  
     XML Example **I-17**  
 VCPT Configuration in CSV Format **I-21**  
     CSV Example **I-24**  
     How to create the CSV format **I-25**

**INDEX**



## 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, page ix](#)
- [Document Revision History, page ix](#)
- [Document Organization, page x](#)
- [Related Documentation, page xi](#)
- [Document Conventions, page xii](#)
- [Obtaining Documentation and Submitting a Service Request, page xiii](#)

## Objectives

This document describes Cisco CDA Visual Quality Experience (VQE) Application, Release 3.5, 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-14115-10	October 2010	Document for Cisco VQE Release 3.5.5
OL-14115-09	June 2010	RCC Troubleshooting section added
OL-14115-08	February 2010	Document for Cisco VQE Release 3.5
OL-14115-07	August 2009	Document for Cisco VQE Release 3.4
OL-14115-06	April 2009	Document for Cisco VQE Release 3.3
OL-14115-05	January 2009	Document for Cisco VQE Release 3.2
OL-14115-04	October 2008	Document for Cisco VQE Release 3.1
OL-14115-03	August 2008	Document for Cisco VQE Release 3.0

**Table 1 Document Revision History**

Revision	Date	Change Summary
OL-14115-02	December 2007	Document for Cisco VQE Release 2.1
OL-14115-01	August 2007	Document for Cisco VQE Release 2.0

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

## Document Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	<a href="#">Introduction to Cisco CDA Visual Quality Experience Application</a>	Provides an introduction to the VQE Application.
Chapter 2	<a href="#">Getting Started with the VQE Startup Configuration Utility</a>	Explains how to use the Cisco VQE Startup Configuration Utility to perform the initial configuration tasks for the Cisco CDE110 that hosts the VQE-S <sup>1</sup> and the CDE110 that hosts the VQE Tools.
Chapter 3	<a href="#">Using the VQE Channel Provisioning Tool</a>	Describes how to use the Cisco VCPT <sup>2</sup> .
Chapter 4	<a href="#">Using the VQE-S AMT</a>	Describes how to use the Cisco VQE-S AMT <sup>3</sup> .
Chapter 5	<a href="#">Using the VCDS AMT</a>	Describes how to use the Cisco VCDS AMT.
Chapter 6	<a href="#">Troubleshooting VQE Software Components</a>	Describes how to identify and remedy problems related to the Cisco VQE Server, the VQE-S AMT, and the VCPT. The chapter also explains how to stop, start, and restart the VQE-S and VCDS <sup>4</sup> services.
Chapter 7	<a href="#">Configuring VQE Server and VQE Tools</a>	Describes these VQE Configuration Management System software components: the VQE Configuration Tool, the Configuration Engine, and the VCDB Parser. The chapter also provides information on using the Configuration Tool, manually editing the VCDB file, and using the <code>vqe_cfgtool</code> command.
Appendix A	<a href="#">VQE, System, and Network Parameters</a>	Provides descriptions of the VQE-S Configuration Database parameters.
Appendix B	<a href="#">SNMP MIBs</a>	Gives information about the VQE-specific and standard Linux MIBs on the Cisco CDE110 that hosts the VQE-S and on the CDE110 that hosts VQE Tools.
Appendix C	<a href="#">VQE System Messages</a>	Provides information on the Cisco VQE system messages.
Appendix D	<a href="#">Manual Initial VQE System Configuration</a>	Explains how to perform manual initial configuration on the CDE110 that hosts VQE-S and on the CDE110 that hosts VQE Tools.
Appendix E	<a href="#">Configuring DHCP and DNS Servers for VCDS</a>	Provides information on configuring the DHCP <sup>5</sup> and DNS <sup>6</sup> servers so that they work correctly with the VCDS or another RTSP server.

Chapter	Title	Description
Appendix F	<a href="#">Using the <code>vcds_send_file</code> Command</a>	Gives overview information on the network-based per-client configuration of the VQE-C <sup>7</sup> . Also, explains how to use the <code>vcds_send_file</code> command to send the client database file and group attribute file to one or more VCDSs.
Appendix G	<a href="#">Changing the Boot Sequence to Start from the CD/DVD Drive</a>	Explains how to change the BIOS setting on the Cisco CDE110 server so that the server boots first from the CD/DVD Combo drive.
Appendix H	<a href="#">VQE Server Performance and Scaling Limits</a>	Summarizes performance information of the Cisco VQE-Ss, and provides information on how to access the VQE-S capacity statistics.
Appendix I	<a href="#">VCPT Configuration Files</a>	Describes the VCPT import and export configuration file formats, and provides examples of both formats.

1. VQE-S = VQE Server
2. VCPT = VQE Channel Provisioning Tool
3. AMT = Application Monitoring Tool.
4. VCDS = VQE Client Configuration Delivery Server.
5. DHCP = Dynamic Host Configuration Protocol.
6. DNS = Domain Name System.
7. VQE-C = VQE Client.

## Related Documentation

The following is a list of documents and Cisco.com URLs for the Cisco CDE110 and the Cisco CDA Visual Quality Experience Application, Release 3.5:

- *Release Notes for Cisco CDA Visual Quality Experience Application, Release 3.5*  
[http://www.cisco.com/en/US/docs/video/cds/cda/vqe/3\\_5/release/notes/vqe\\_notes3\\_5.html](http://www.cisco.com/en/US/docs/video/cds/cda/vqe/3_5/release/notes/vqe_notes3_5.html)
- *Cisco CDA Visual Quality Experience Application User Guide, Release 3.5* (this document)  
[http://www.cisco.com/en/US/docs/video/cds/cda/vqe/3\\_5/user/guide/vqe\\_guide3\\_5.html](http://www.cisco.com/en/US/docs/video/cds/cda/vqe/3_5/user/guide/vqe_guide3_5.html)
- *Cisco CDA Visual Quality Experience Client System Configuration Guide*  
[http://www.cisco.com/en/US/docs/video/cds/cda/vqe/vqec/configuration/guide/vqec\\_cnfg.html](http://www.cisco.com/en/US/docs/video/cds/cda/vqe/vqec/configuration/guide/vqec_cnfg.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](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](http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/cde110_rcsi.pdf)
- Open Source Used in Visual Quality Experience 3.5.5  
[http://www.cisco.com/en/US/products/ps7127/products\\_licensing\\_information\\_listing.html](http://www.cisco.com/en/US/products/ps7127/products_licensing_information_listing.html)

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
<i>VQE-C Release Notes</i>	Provides release-specific information on the VQE-C.
<i>VQE-C System Integration Reference</i>	Provides information on the VQE-C components, architecture, integration, and APIs. Also includes a VQE-C quick-start guide.
<i>Cisco CDA Visual Quality Experience Client System Configuration Guide</i> *	Explains certain factors to consider when configuring and deploying VQE-C. Also provides reference information on the VQE-C configuration file parameters.
<i>VQE-C CLI Command Reference</i>	Provides reference information on the VQE-C command-line interface.

\* This guide is available only on Cisco.com. See the URL in the list preceding [Table 2](#).

## Document Conventions

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

Convention	Description
<b>boldface</b> font	Commands and keywords are in <b>boldface</b> .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{x   y   z}	Alternative, mutually exclusive, keywords are grouped in braces and separated by vertical bars.
[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.
<i>screen</i> font	Terminal sessions and information the system displays are in <i>screen</i> font.
<b>boldface screen</b> font	Information you must enter is in <b>boldface screen</b> font.
<i>italic screen</i> font	Arguments for which you supply values are in <i>italic screen</i> 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 (VQE) Application and contains the following major topics:

- [VQE Overview, page 1-1](#)
- [VQE Benefits, page 1-8](#)
- [VQE-S, page 1-9](#)
- [VQE-C, page 1-11](#)
- [VQE Deployment Options and Requirements, page 1-14](#)
- [VCPT and Channel Information, page 1-15](#)
- [VCDS, page 1-17](#)
- [VQE-S AMT, page 1-21](#)
- [VQE-S RTCP Exporter for Video-Quality Monitoring, page 1-23](#)
- [VCDS AMT, page 1-24](#)
- [Content Delivery Engine 110, page 1-26](#)

### VQE Overview

This VQE overview has the following sections:

- [Introduction to VQE, page 1-2](#)
- [VQE Major Software Components, page 1-4](#)
- [VQE Hybrid Error Repair, page 1-4](#)
- [VQE RCC, page 1-5](#)
- [RTP and RTCP, page 1-7](#)
- [VQE Web Browser-based Tools, page 1-7](#)
- [Lookaside Mode and the Cisco CDE110, page 1-8](#)

## Introduction to VQE

Cisco CDA Visual Quality Experience (VQE) Application offers service providers a set of technologies and products associated with the delivery of Internet Protocol television (IPTV) video services. VQE is designed to improve the quality of IPTV services and viewing experiences of the subscriber. VQE is part of a Cisco end-to-end solution that builds video awareness into the network infrastructure. For Cisco VQE Release 3.5, 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 a loss of fewer than  $7.8E-7$  video packets. Most xDSL networks are not optimized to deliver such low levels of packet loss.

The second issue that affects IPTV video quality is channel change time (CCT). Consumers have become used to the current CCT—which is less than 2 seconds—offered by digital cable and digital satellite services. Several 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 5 seconds have been observed.

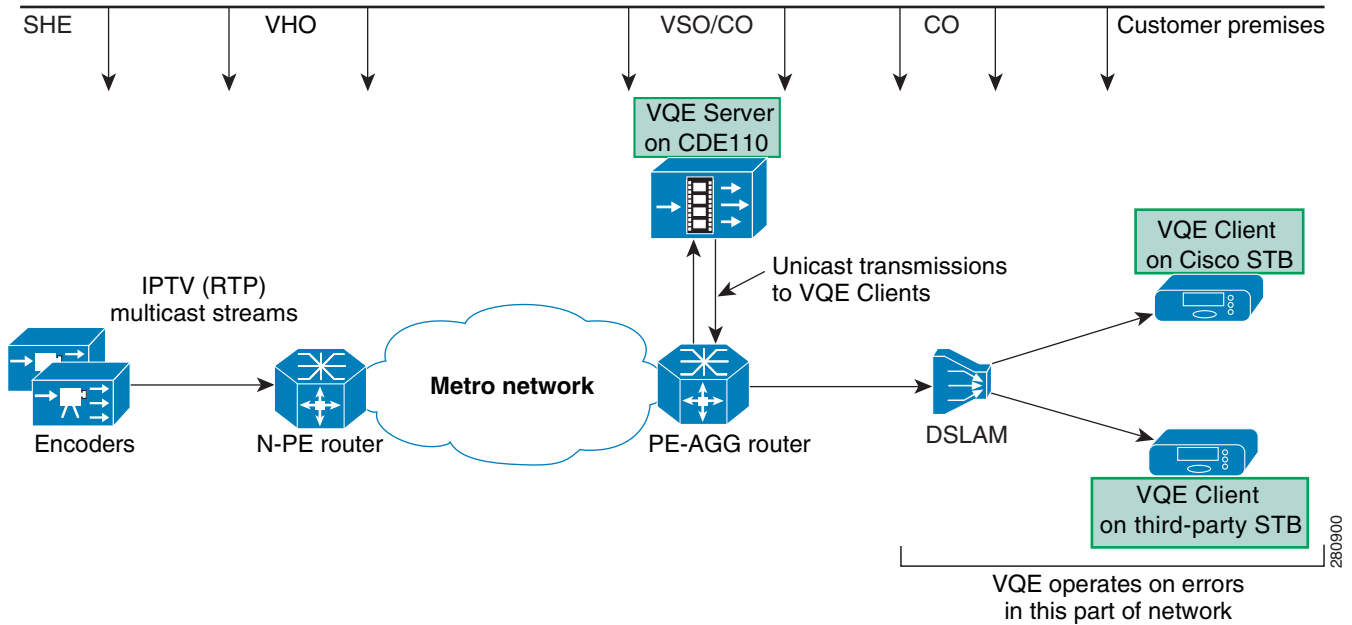
VQE addresses the issue of video quality from both a network infrastructure and a video technology perspective. VQE provides the linkage to optimize video delivery over next-generation carrier networks. Based on industry standards, including Real-Time Transport Protocol (RTP) and RTP Control Protocol (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 (STB) receiver, the VQE Client (VQE-C), sends non-acknowledgement (NACK) packets to the VQE-S 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-C on the STB to detect and correct lost packets.
- Rapid Channel Change (RCC)—When the subscriber requests a channel change, the VQE-C on the STB sends the VQE-S a request for the IPTV packets of the new channel. The VQE-S sends the VQE-C an optimized unicast burst of IPTV packets and other channel information for the new channel from the cached video data of the VQE-S. 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 Forward Error Correction (FEC), can be used separately or together for Hybrid Error Repair (see [“VQE Hybrid Error Repair”](#) section on page 4). 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 customer premises equipment (CPE) of the subscriber.

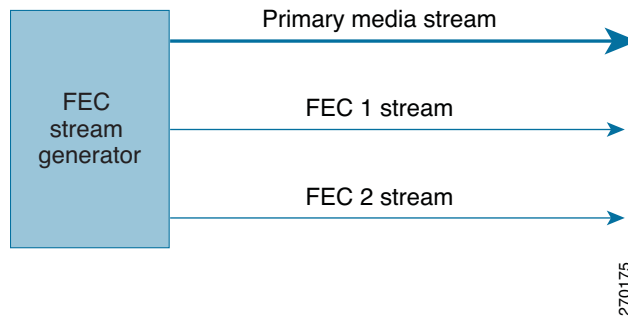
Figure 1-1 VQE Major Components



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 sends application-layer FEC packets. 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 (see Figure 1-2).

Figure 1-2 FEC Stream Generator



## VQE Major Software Components

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

- VQE-C—Software embedded in the CPE of the subscriber—typically a STB. The VQE-C provides the CPE interface to the VQE Server (VQE-S) to support Unicast Retransmission, RCC, and IPTV Packet Loss Monitoring statistics. The VQE-C receives the primary media data packets and, if FEC is enabled, one or two streams with FEC packets. When the VQE-C 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, the VQE-C first tries to repair the lost packets using the FEC streams.
  - If some packet losses cannot be corrected by FEC, the VQE-C requests a Unicast Retransmission of the missing packets from the VQE-S.
- 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 RCC, the VQE-S caches primary video packets from an encoder or other headend device.
  - For Unicast Retransmission, working with the VQE-C, the VQE-S monitors the subscriber’s reception of video packets and uses its cached video data to service Unicast Retransmission requests from the VQE-C on the STB.
  - For RCC, when the subscriber requests a channel change, the VQE-C on the STB sends a request for a new channel to the VQE-S. To service the RCC request, the VQE-S sends the VQE-C 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.

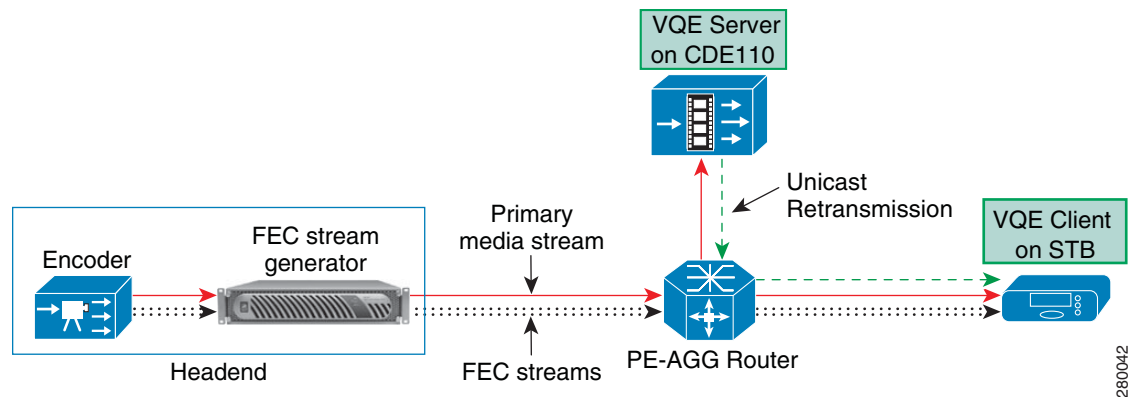
With both Unicast Retransmission and FEC, the missing packets are resequenced by the STB without interruption.

The VQE-C is available with certain Cisco STBs running Scientific-Atlanta IPTV Layer (SAIL) 1.x and 2.x. Please contact your Cisco sales representative for further information. The VQE-C can also be integrated into a STB from third-party vendors. The VQE-C 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 because of the interdependence of the 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), RTCP NACK compound packets are sent to the VQE-S to request retransmission of the lost packets whenever the receiver (VQE-C) 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. Starting with Cisco VQE Release 3.5.5, it is possible to configure the VQE-C on a per-channel basis to send RTCP NACK compound packets without Receive Reports (RRs) to reduce the bandwidth consumed by RTCP NACK compound packets on the access link.

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. The VQE-C uses the FEC data to detect and correct the lost packets. No feedback to the VQE-S 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 the VQE-C tries but is unable to retrieve lost packets using FEC, it can request that the VQE-S 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 RCC

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 RCC functionality built into the VQE-S and the VQE-C 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).
- Time it takes for the STB 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).

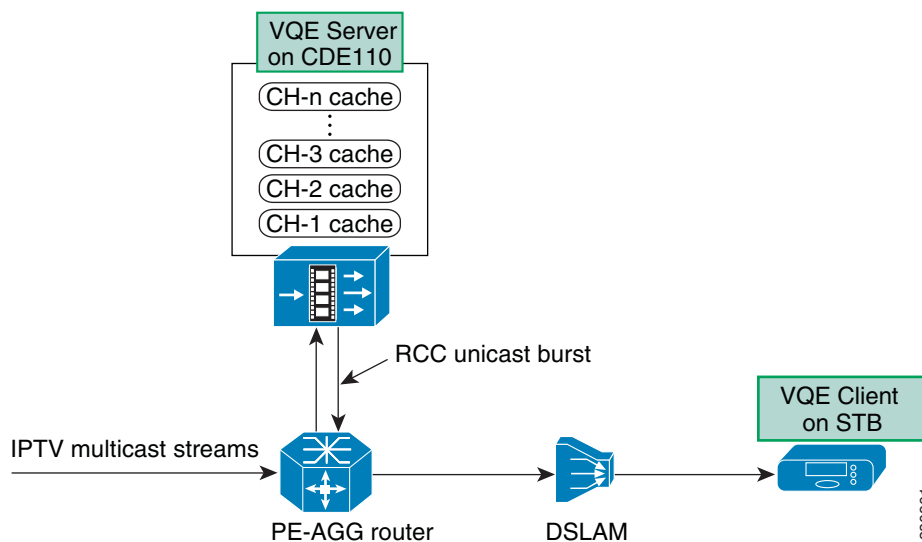
Not all of the above factors need to be addressed by RCC functionality. For example, many Digital Subscriber Line Access Multiplexers (DSLAMs) can provide fast leave for IGMP, which addresses the multicast leave latency factor.

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, the VQE-S caches multicast IPTV packets corresponding to each channel (see [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, the VQE-C on the STB requests the IPTV packets for the new channel from its target the VQE-S, 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 RCC**



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

Before sending the unicast burst, the VQE-S 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-S contains an I-frame, the STB 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 for RCC, 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 STB. The VQE-C monitors RTP sequence numbers from both unicast and multicast streams. It is likely that the VQE-C sees a few packets with duplicate RTP sequence numbers before the unicast stream ends. During this period, the VQE-C only forwards one copy of the RTP packet to the MPEG demultiplexing stage.

The VQE-C 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-C to the VQE-S.

## RTP and RTCP

VQE relies on RTP and RTCP. RTP is used to carry video packets over multicast streams from the video headend to the VQE-Cs on the STBs. It is also used to transport specific video packets between the VQE-S and a VQE-C. RTCP is a signaling protocol used between VQE devices. RTP is the transport baseline for application-layer FEC, Unicast Retransmission, and RCC.

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 three web browser-based tools: VQE Channel Provisioning Tool (VCPT), VQE-S Application Monitoring Tool (AMT), and VQE Client Configuration Delivery Server (VCDS) AMT.

- VCPT is an optional channel-provisioning utility to aid with the channel lineup configuration required by both the VQE-S and the VQE-C. The channel information is in Session Description Protocol (SDP) format. The VCPT sends the channel information to the VQE-Ss and VCDSs. The VCDS servers provide the channel lineup or network configuration to the VQE-Cs on the STBs.
- VQE-S AMT is a browser-based GUI that displays configuration, status, and statistics on the VQE-S processes, the channel lineup, Unicast Retransmission, RCC, Ethernet interfaces, and VQE-S RTCP Exporter. The VQE-S AMT also allows you to configure debugging and logging facilities.
- VCDS AMT is a browser-based GUI that displays configuration, status, and statistics on the VCDS and VQE Tools server. The VCDS AMT also allows you to configure debugging and logging facilities.

The VQE-S and the VCPT are bundled software and hardware solutions. The VQE-S and the VCPT run on separate Cisco Content Delivery Engine 110 (CDE110) appliances. A typical network might consist of multiple CDE110s hosting the VQE-S and one or two CDE110s hosting the VCPT, the VCDS AMT, and the VCDS.

## Lookaside Mode and the Cisco CDE110

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

- If the Cisco CDE110 appliance or the VQE-S software should fail, there is no loss of IPTV service to the customer.
- Because no multicast forwarding is provided by the VQE-S, more IPTV customers can be serviced by each VQE-S instance.
- Number of Cisco CDE110 appliances hosting the 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 preinstalled: VQE-S or VCPT, Linux, Apache web server, and other software.

## VQE Benefits

Cisco VQE Release 3.5 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 reruns
- 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 RCC 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 RCC—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 STB
- 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 video offerings, bundles, and unique content of the service provider.

# VQE-S

The VQE-S software is hosted on a Cisco CDE110 appliance running a standard Linux operating system. The Cisco CDE110 comes with the required software preinstalled: VQE-S, VQE-S AMT, Linux, Apache web server, and other software.

The VQE-S is responsible for the following functions:

- Creating a channel configuration database using the channel configuration information sent by the VCPT
- 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-Cs on the STBs
- Handling RCC by caching RTP data streams as well as PAT, PMT, ECM, PCR, and sequence information and sending RCC unicast bursts to requesting VQE-Cs when a channel change occurs
- Load balancing VQE-S services across the Cisco CDE110 Ethernet or bond interfaces
- Providing detailed statistics on IPTV delivery down to the STB VQE-C level
- Monitoring the health of VQE-S application processes

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

For Unicast Retransmission, when a VQE-C requests retransmission of missing packets, the VQE-S locates them in its cache and, if found, delivers them to the STB through an associated RTP retransmission stream. See [Table H-3 on page H-2 in Appendix H, “VQE Server Performance and Scaling Limits”](#) for information on the VQE-S inbound repair request limits.

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

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

In addition, the 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, the VQE-C 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.

The VQE-S separates the bandwidth resources that are dedicated to Unicast Retransmission and RCC. A VQE-S configuration parameter (`vqe.vqes.reserved_er_bw`) controls the bandwidth resources that are dedicated to Unicast Retransmission. The parameter allows the amount of resources dedicated to Unicast Retransmission to be reduced so that the resources are available for RCC instead. The VQE-S provides capacity statistics to indicate when Unicast Retransmission and RCC capacity limits have been exceeded. For more information on the VQE-S capacity statistics, see the [“VQE-S Capacity Statistics” section on page H-3 of Appendix H, “VQE Server Performance and Scaling Limits”](#).

The VQE-S supports setting Differentiated Services Code Point (DSCP) values on IPTV-related packets so that specific levels of service can be assigned to RTCP and RTP packets. For RTP traffic, the service provider can configure separate DSCP values for Unicast Retransmission and RCC. DSCP values are set using the VQE Configuration Tool.

For VQE-S performance information, see [Appendix H, “VQE Server Performance and Scaling Limits”](#).

## VQE-S High Availability

The VQE-S provides several high-availability mechanisms for resiliency and redundancy:

- 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, the Process Monitor automatically attempts to restart it.
- If the Process Monitor itself fails, the Linux initialization process detects this failure and restarts the VQE-S service (Process Monitor).
- If a Cisco CDE110 running a VQE-S fails and there is a redundant, backup CDE110 running a VQE-S that is configured to receive the same multicast streams, the backup VQE-S takes over servicing the streams.
- Use of anycast IP addresses and equal-cost multi-path routing allows multiple VQE-Ss in a single facility to be load 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” section on page 2-21](#).

For Multicast Load Balancing, when a multicast stream used for caching on the VQE-S host starts or stops, the 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 interfaces to avoid oversubscription. The VQE-S also monitors the status of these interfaces, moving the streams to other interfaces in case of interface failure.

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

## 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 the VQE-C. When the VQE-C tunes to a new channel, it sends STUN binding requests to the STUN Server on the VQE-S host. The VQE-C sends the requests to the feedback target IP address of the channel and RTP and RTCP retransmission ports as configured on the VQE-S. The VQE-C uses the STUN Server responses to determine whether it is behind a NAT device and what type of NAT device it is.

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

The STUN Server that is included with the VQE-S can be turned on or off using a configurable option in the VQE-S configuration file. Unless it is certain that no STBs 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-20](#).

## VQE-C

The VQE-C software runs on customer premises equipment (CPE), such as a STB. The VQE-C supports Unicast Retransmission, FEC, RCC, and video-quality statistics by providing the following:

- CPE interface to the VQE-S for Unicast Retransmission and RCC
- 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 by sending a RTCP NACK compound packet to the VQE-S while holding the video sequence in queue. The VQE-S automatically repairs the error by transmitting the missing packet, which is resequenced by the STB without interruption. The entire error-repair cycle is imperceptible to the viewer. The RTCP NACK compound packet consists of an RR (Receiver Report) message, an SDES (source description) message, a PUBPORTS (publish ports) message, if applicable, and a generic RTP feedback (RTPFB) NACK message. Starting with Cisco VQE Release 3.5.5, the RR packets may be omitted to reduce the bandwidth utilized by the RTCP NACK compound packets on the access link.

For RCC, when a subscriber selects a new channel, the VQE-C sends to the VQE-S 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, the VQE-C manages the seamless transition between unicast packets from the VQE-S and multicast packets from the headend encoder.

The VQE-Cs can get channel configuration information and per-client network configuration from a 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-C and a VCDS, see the [“VCDS” section on page 17](#) section.

Each VQE-C can communicate client-specific information to a VQE-S so that some VQE-S services can be optimized for the particular client. Two examples of this capability are as follows:

- **Maximum Receive Bandwidth**—Each VQE-C can communicate a maximum receive bandwidth on the STB to the VQE-S so that VQE-S can precisely set the excess bandwidth available for Unicast Retransmission and RCC. This information is specified with VQE-C system parameters and is used to determine the rate at which VQE-S sends packets to this VQE-C.
- **Decoder Buffer Burst Shaping**—Each VQE-C can communicate the size of the STB decoder hardware buffer using the VQE-C system parameter `max_fastfill`. This size is used for RCC and allows a STB with limited memory to perform RCC. Using the buffer size provided by the VQE-C, the VQE-S modifies the shape of the RCC burst to take advantage of fast decoder fill capabilities.

The VQE-C 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. For information on VQE-C system parameters, see *Cisco CDA Visual Quality Experience Client System Configuration Guide*.

Starting with Cisco VQE Release 3.5.5, the VQE-C provides a data path for packets from UDP MPEG2-TS streams and RTPv2 streams that are not configured in the VQE-C channel line up. No VQE services (that is, Error Repair and RCC) are provided for these streams. For UDP streams, the VQE-C acts as a pass-through device. For RTP streams not configured in the channel line up, the VQE-C provides reordering of packets.

The VQE-C supports the monitoring and reporting of a subset of TR-135 statistics. The technical report *TR-135—Data Model for a TR-069 Enabled STB* defines a hierarchical model of statistics that may be collected by remote management stations for the purposes of monitoring and troubleshooting STB services. The VQE-C is in an ideal position to support the collection of the subset of these statistics that correspond to the IPTV and VoD streams that the VQE-C buffers. For more information on configuring the VQE-C to collect TR-135 statistics, see *VQE-C System Integration Guide*. For information on TR-135 data model statistics, the TR-135 data model can be found at this url: <http://www.broadband-forum.org/technical/download/TR-135.pdf>

The VQE-C supports statistics counters that can be utilized to implement SNMP MIB views. The VQE-C provides APIs to export tuner and channel cumulative MIB-compatible counters. For more information on creation of SNMP MIB Views of VQE-C counters, see *VQE-C System Integration Guide*.

The VQE-C is available in two deployment models:

- VQE-C is integrated into selected Cisco STBs.
- VQE-C code is offered through an open-source program for integration with STBs from third-party vendors.

For information on VQE-C deployment models, see “[VQE Deployment Options and Requirements](#)” section on page 14.

## VQE-C Forward Error Correction

The VQE-C 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 VCDS. The FEC streams are configured on a per-channel basis.

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

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

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.

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

The VQE-C supports SMPTE 2022 Annex A and Annex B stream orderings. For detailed information on 1-D and 2-D FEC, see 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.smpite.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. The VQE-C generates RTP packet-level statistics for packet loss, jitter, delay, and other quality measurements. The VQE-C provides statistics on both Unicast Retransmission and FEC. For the RTCP reports, the VQE-C sends 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 23.

## VQE-C Software Development Kit and Documentation

The VQE-C consists of a software development kit (SDK), which can be used for VQE-C integration into STBs 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 STB software base. The programmatic interface provides a *socket replacement* interface, which is used to get packets from a repaired VQE-S server-enhanced video stream. The 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-C must be coordinated with the configuration of the VQE-S. Certain features are operational only when they are enabled on both the VQE-C and the 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 STB. 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. See the “[Related Documentation](#)” section on page -xi for a list of the VQE-C documentation that is available.

# 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 STBs
- Cisco end-to-end IPTV solution model—For new IPTV opportunities

With both deployment options, the VQE-S 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 STBs. Cisco offers the VQE-C as open-source software. The VQE-C is implemented so that service providers and CPE device vendors can integrate the VQE-C software with third-party STBs. Appropriate development-level documentation is available along with the VQE-C code.

With this model, the service provider uses the VCPT to define channels and servers and to create channel lineups for different subscriber regions. The VCPT sends the channel information to the VQE-Ss, and to the VCDSs or a remote server from which each VQE-C gets its channel information. The channel information is in the Session Description Protocol (SDP) format required by the VQE-S and the VCDS.

## 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, the VQE-C is integrated with selected Cisco STBs. The main difference between the Cisco end-to-end IPTV solution and the VQE reference architecture models lies with the integration responsibility of the VQE-C.

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

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

## VQE Deployment Requirements

To deploy VQE, the following prerequisites must be met:

- 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 (STB).

- TV channel information—VQE-C and the 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 the VQE-S components in Session Description Protocol (SDP) format. The VCPT 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 send FEC streams to the 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 the 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 the VQE-S, and for sending RTP data packets from the VQE-S to the VQE-C.
- All versions of IGMP are supported by the VQE-S and the VQE-C.

## VCPT and Channel Information

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

- Channel definitions—Information on the channels that is serviced by VQE
- Server definitions—Information on each VQE-S, VCDS, and Remote Server that receives the channel information
- Channel lineups—Associations between channels, the VQE-Ss, and the VCDSs

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 RCC. The option to enable reduced-size RTCP messages is available in Cisco VQE Release 3.5.5 and later releases.

**Figure 1-5** VCPT Channel Definition

The screenshot displays the 'Details' window for a VCPT channel definition. The window is divided into two main sections: 'Channel Details' and 'Channel Features'.

**Channel Details:**

- Channel Name:** Channel 14
- Feedback Target IP:** 10.1.7.1
- Original Stream:**
  - Multicast IP: 224.1.1.7
  - Source IP: 10.10.10.5
  - RTP Port: 1025
  - RTCP Port: 1026
  - Bit Rate: 4000 (kbps)
- Unicast Retransmission Stream:**
  - Source IP: 10.1.7.1
  - RTP Port: 50012
  - RTCP Port: 50013
- FEC 1 Stream:**
  - Source IP: 10.10.10.5
  - Multicast IP: 224.1.8.1
  - RTP Port: 1027
- FEC 2 Stream:**
  - Source IP: 10.10.10.5
  - Multicast IP: 224.1.8.1
  - RTP Port: 1028

**Channel Features:**

- Enable RTCP
  - Enable Error Repair
  - Enable Rapid Channel Change
  - Enable Extended RTCP Reports
  - Enable Reduced Size RTCP
- Enable FEC 1 Stream
- Enable FEC 2 Stream

At the bottom right of the window are 'Update' and 'Cancel' buttons. A small vertical number '254375' is visible on the right edge of the window frame.

The VCPT GUI has a clone capability to simplify and expedite channel information. When the service provider uses the VCPT to define the set of the VQE-Ss that receive the channel information, the VQE-Ss 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.

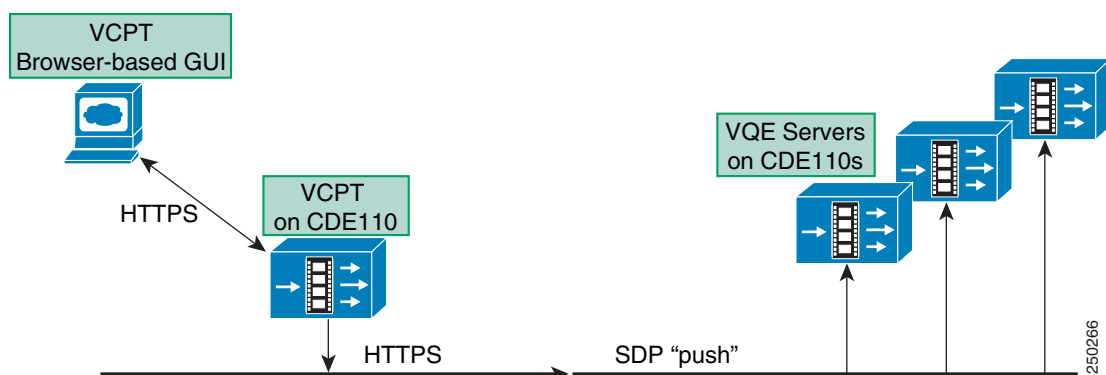
The VCPT GUI has the capability to import a configuration from a file. The file must be in either XML or CSV format, and must comply with the data rules and definitions specified in [Appendix I, “VCPT Configuration Files”](#). The VCPT GUI also has the capability to export a configuration to an XML or CSV file.

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 starts the VCPT send operation, the VCPT sends the channel information in Session Description Protocol (SDP) format to the set of VQE-Ss, to the VCDS, or to a Remote Server.

The VCPT sends or *pushes* the channel information to all VQE-Ss that are defined in the current VCPT configuration file. The channel information is sent to the VQE-Ss over secure HTTPS. The VCPT contains a secure HTTPS client, and each VQE-S has an embedded web server running. Each VQE-S stores its own local copy of the channel information. [Figure 1-6](#) shows the interactions between the VCPT and the VQE-Ss. For information on the VQE-Ss, see the “VQE-S” section on page 9.

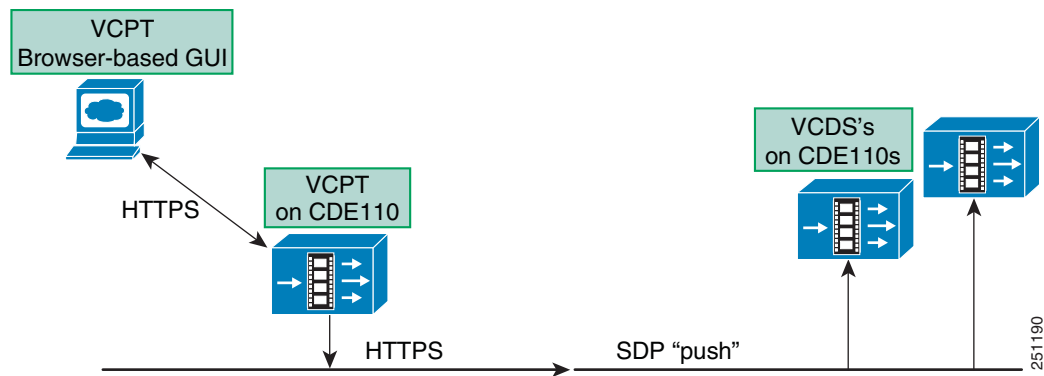
**Figure 1-6 VCPT: Sending Channel Information to VQE Servers**



The VCPT is also responsible for sending channel information to each VCDS. The VCDS is a software component installed on each VQE Tools server, the Cisco CDE110 that also hosts the VCPT. When the service-provider operator initiates the VCPT send operation, the VCPT *pushes* the channel information to one or more VCDSs. The VCPT sends the channel information in SDP format through HTTPS similar to the way it is sent to the VQE-Ss.

[Figure 1-7](#) shows the interactions between the VCPT and the VCDSs. Each VQE Tools server includes both the VCPT and the VCDS. The 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 VCDSs**



An alternative VQE-C Configuration Delivery Server to the VCDS can be used to deploy network and channel information to the access network. The service-provider may have a multicast-based STB file delivery solution already in place. The VCPT can send channel information to a remote server, once the service-provider defines the remote server in the VCPT by providing the following information:

- Management IP address of the remote server.
- Transfer port number to use.
- Full path and filename of the configuration file on the remote server.
- Name of the person with the authority to access this path.

The remote server is treated as another server role, with channels being associated with the remote server. The VCPT *pushes* a channel configuration to the remote server using the password-less secure copy protocol (SCP). From the remote server, you can distribute network and channel configuration data to STBs by integrating your deployment with customized middleware from a third-party vendor.

## VCDS

The VCDS is a software component on the VQE Tools server that can be used to deliver the channel configuration file to the VQE-Cs on the STBs, and per-client network configuration files to the VQE-Cs on the STBs. This VCDS function is explained in the following section:

- [VCDS Delivery of the Channel Configuration File, page 1-17](#)
- [VCDS Delivery of the Per-Client Network Configuration File, page 1-18](#)

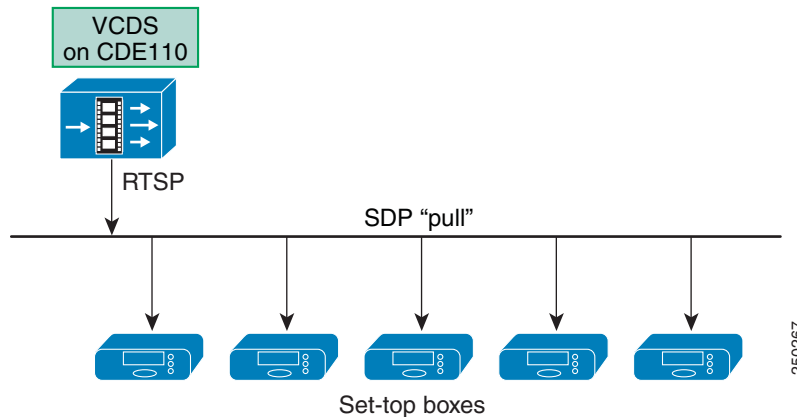
## VCDS Delivery of the Channel Configuration File

When the VCDS receives information on the channel lineup from the VCPT, the VCDS creates a channel configuration file and stores it on the local disk. Each VQE-C running in a CPE device, such as a STB, uses a Real Time Streaming Protocol (RTSP) *pull* operation to receive the channel configuration file from the VCDS. The VCDS is a simplified RTSP server that supports the VQE-C RTSP *pull* operation. The VQE-C learns the name of the VCDS through a Domain Name System (DNS) server using a SRV lookup.

After the VQE-C 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-C 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-Cs on the subscriber STBs.

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 STB: Receiving Channel Information File from VCDS**



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

- **Periodic polls**—VQE-C periodically polls the 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 STB attempts to tune to a channel that is not present in the VQE-C channel lineup, the VQE-C attempts to retrieve a new channel configuration file from the 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.

## VCDS Delivery of the Per-Client Network Configuration File

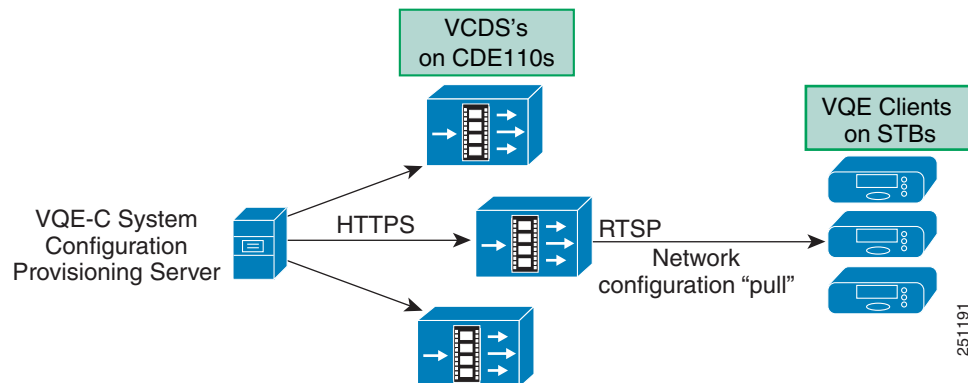
The VCDS can provide customized per-client network configuration to the VQE-C on the STB after the VQE-C has been initialized. The VQE-C network configuration might, for example, specify whether RCC or Forward Error Correction is enabled on the VQE-C, or specify some configuration parameters for the VQE-C.

Updates to the VQE-C network configuration occur because of periodic polls. The VQE-C polls the VCDS to check whether the VQE-C network configuration file has been updated. If a new network configuration file is detected during a poll, the VQE-C requests the file from VCDS and overwrites the network configuration file it has stored in flash memory. The new network configuration does not apply until the next STB reboot.

The three major components involved in the delivery of per-client network configuration are the VQE-C system configuration provisioning server, the VCDS, and the VQE-C on the STB. [Figure 1-9](#) shows the interactions between these components. A simplified description of these interactions is as follows:

- VQE-C system configuration provisioning server sends or pushes the client database file and group attribute file to the VCDSs.
- In response to a request from the VQE-C on the STB, the VCDS sends the updated per-client network configuration file to the VQE-C.
- VQE-C receives the updated network configuration file, merges the attributes into its running configuration, and initializes the system using the merged running configuration on the next reboot.

**Figure 1-9 Major Components for Delivering the Per-Client Network Configuration File**



The following sections provide information on the role of the major components used to deliver the per-client network configuration file for VQE-C system configuration:

- [VQE-C System Configuration Provisioning Server Role, page 1-20](#)
- [VCDS Role, page 1-20](#)
- [VQE-C Role, page 1-20](#)

For information on the interactions between the VCDS and the other components in the VQE configuration delivery infrastructure, see [Appendix E, “Configuring DHCP and DNS Servers for VCDS.”](#)

An alternative to VCDS and CDI may be required for deploying configuration to the access network if the service provider already has a solution in place for multicasting network and channel configuration files to the access network or if the service provider wishes to unicast per-subscriber configuration changes to STBs.

The delivery of the network and channel configuration files may be handled externally to the VQE-C on the STB. The VQE-C provides a set of APIs to receive per-client network configuration data, channel configuration data, and per-subscriber configuration data (that is, an override configuration) from an external client. Deploying network, channel and override configurations to the VQE-C without using VCDS and CDI requires integrating the Cisco’s VQE solution with customized middleware from a third-party vendor.

## VQE-C System Configuration Provisioning Server Role

The VQE-C system configuration provisioning server sends or pushes the client database file and group attribute file to one or more VCDSs using HTTPS. The service provider can provide a VQE-C system configuration provisioning server that meets the specific requirements of the deployment.

As an alternative to a VQE-C system configuration provisioning server, the VQE Tools software includes the **vcds\_send\_file** command that can be used to send the client database file and group attribute file to a VCDS. For information on this command, see [Appendix F, “Using the vcds\\_send\\_file Command.”](#)

The VQE-C system configuration provisioning server has a different role than the channel-provisioning server (for example VCPT or ISDS). The VQE-C system configuration provisioning server delivers the following files to the VCDSs:

- *Client database file*—In this file, each STB VQE-C has a unique identity (for example, MAC address) that is associated with a group identifier (group ID) for the specific network configuration that should be applied to the VQE-C system. Each VQE-C is associated with one group ID. The client database file can be a complete set or superset of all STBs or a subset which adds to or modifies a previous set that exists on the VCDS.
- *Group attribute file*—In this file, different sets of per-client network configurations are defined. Each set of attributes is identified by a group ID.

The client database file and the group attribute file are XML-based and follow a schema specified by a specification defined by Cisco. On a VQE Tools server, the XML schema and examples of the two files are included with the software. See [Appendix F, “Using the vcds\\_send\\_file Command”](#) for the locations of the files on a VQE Tools server.

For information on getting specifications for the client database file, group attribute file, and the VQE-C system configuration provisioning server, contact your Cisco account representative.

## VCDS Role

When the VQE-C system configuration provisioning server sends or pushes the client database file and the group attribute file to one or more VCDSs, each VCDS does the following:

- Accepts a push of the client database file and the group attribute file from the VQE-C system configuration provisioning server
- Parses the files for validity
- Updates its local copies of the client database file and group attribute file
- Services VQE-C requests for an updated per-client network configuration file

## VQE-C Role

To obtain and process the per-client network configuration file, the VQE-C on the STB performs the following tasks:

- By a periodic poll, determines whether an updated network configuration file is available
- Retrieves the updated network configuration file from the VCDS
- Writes the updated network configuration file to local flash memory
- Derives a *running configuration* in memory by merging its existing network configuration file using the attributes in the updated network configuration file
- On the next STB reboot, initializes the VQE-C network configuration using the merged running configuration

For more information on VQE-C's use of a per-client network configuration file, see *Cisco CDA Visual Quality Experience Client System Configuration Guide*.

## VQE-S AMT

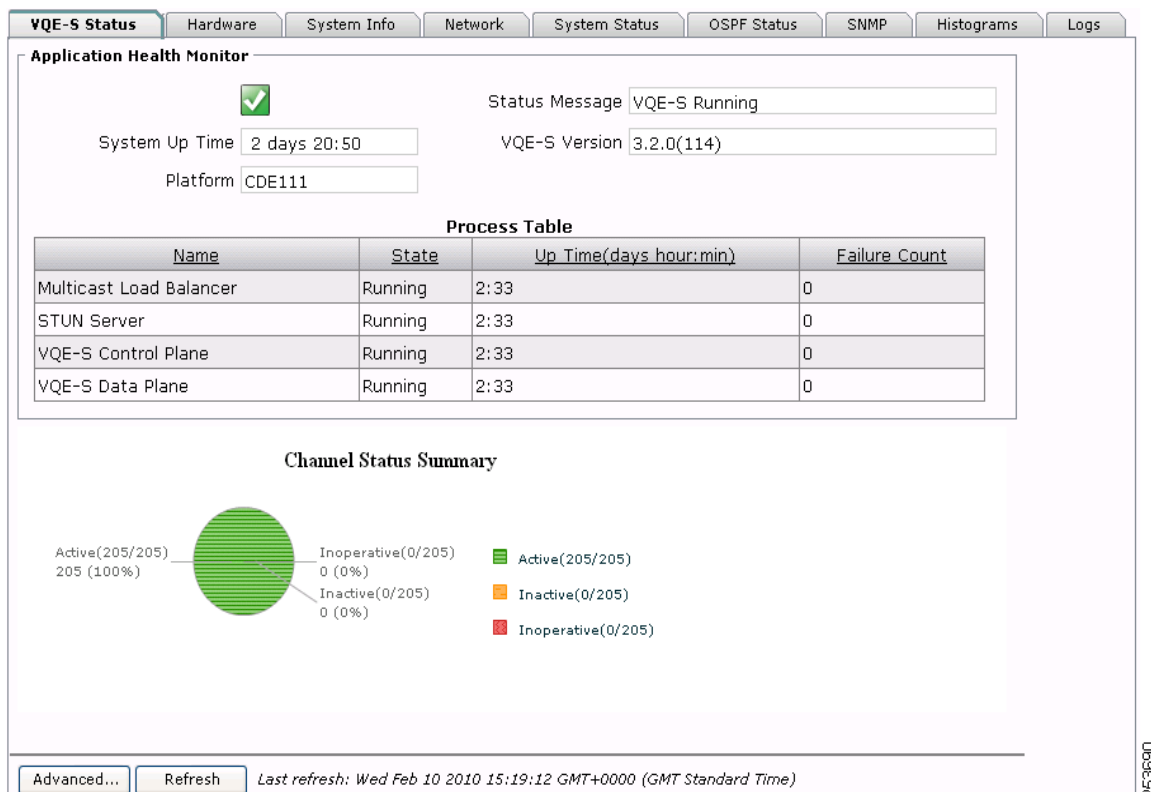
The VQE-S AMT is a browser-based GUI that allows the service-provider operator to do the following:

- Monitor the health of the VQE-S processes
- View channel configuration details, status, and statistics
- Monitor statistics for Unicast Retransmission and RCC
- Monitor statistics for STUN Server usage
- View configuration details, status, and statistics for:
  - Multicast Load Balancer
  - VQE-S RTCP Exporter
- Change 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 (see [Figure 1-10](#)) shows the health of VQE-S processes and other status information.

**Figure 1-10** Monitoring VQE-S Processes



253690

With VQE-S AMT, you can view the channel lineup that was sent from the VCPT. Figure 1-11 shows a partial example of the channel lineup with usage statistics that VQE-S AMT displays.

**Figure 1-11 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

In Figure 1-11, the channel-lineup summary data indicates when the lineup was last updated (for example, with the 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-Cs that are currently receiving this multicast stream.

The VQE-S AMT uses the Unicast Retransmission and RCC counters kept by the VQE-S to display a variety of data. For Unicast Retransmissions, the counters include non-acknowledgement (NACK) messages received from VQE-Cs, RTP packets requested and sent, error repair rates, and requests exceeding Unicast Retransmission capacity limits. For RCC, the counters include the number of RCCs requested, accepted, and refused, as well as the number of requests exceeding RCC capacity limits.

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

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

These configuration changes are temporary in nature, and only remain in effect until the VQE-S restarts.

In addition, the VQE-S AMT allows you to reset a subset of VQE-S counters to zero and subsequently, to restore these counters to their true values.

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

The VQE-S AMT is a web application that uses the application server and web server that are preinstalled on the Cisco CDE110 where the VQE-S runs. The 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

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

For the RTCP reports, each VQE-C periodically sends RTCP compound packets to its target VQE-S. Each compound packet contains an RR, an SDES, PUBPORTs, if present, and a generic RTP feedback NACK, if present. The VQE-C sends additional RTCP reports every time a Unicast Retransmission request is made. Starting with Cisco VQE Release 3.5.5, the service provider may omit RRs from the RTCP NACK compound packet for each channel using the VCPT. In addition to the RTCP compound packet, each VQE-C may transmit pre- and post-repair RTCP XR reports to its target VQE-S if the option to enable XR reports is enabled for each channel using the VCPT.

The service provider can use VQE-S RTCP Exporter to export the RTCP compound packets and the XR reports to a video-quality monitoring (VQM) application. Starting with Cisco VQE Release 3.5.5, the service provider can exclude RTCP NACK compound packets from being exported to the VQM application by setting the VCDB parameter `vqe.vqes.exporter_filter_nack` to TRUE. The VQM application collects 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.

The 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 STB. 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.

On the VQE-S, RTCP Extended Reports and the Extended Report (XR) packet type are supported. The following XR report block types are supported:

- Loss RLE (run-length encoded)
- Statistics Summary
- Post-Repair Loss RLE
- Multicast Acquisition
- Diagnostic Counters (available in Cisco VQE Release 3.5.5 and later releases)

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. The VCPT allows the service provider to specify whether or not RTCP Extended Reports are used for each channel.

The following documents, which are available from <http://www.faqs.org/faqs/>, provide more information on RTCP reports:

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

The 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 *Post-Repair Loss RLE Report Block Type for RTCP XR* at:

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

The Multicast Acquisition report block type is also capable of supporting information on the total channel change time, the expected RCC presentation timestamp and the actual RCC presentation timestamp. The availability of this timing information is dependent on the specific VQE-C platform integration. For more information, see *Multicast Acquisition Report Block Type for RTCP XR* at:

<http://tools.ietf.org/id/draft-begen-avt-rapid-sync-rtcp-xr-01.txt>

Starting with Cisco VQE Release 3.5.5, the Diagnostic Counters XR report block type contains information on cumulative overruns and underruns, post-repair loss events, late packet drops, and output queue drops per channel.

## VCDS AMT

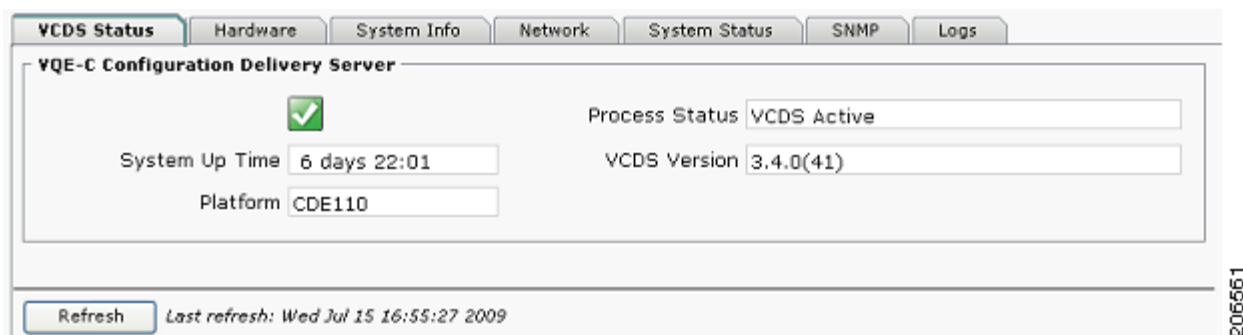
The VCDS AMT is a browser-based GUI that allows the service-provider operator to do the following:

- Monitor the health of the VCDS process and the VQE Tools Server
- View configuration details and statistics for the VCDS
- Configure VCDS logging levels and debugging options

The next paragraphs provide a few examples of the VCDS AMT functionality.

When you log into VCDS AMT, the initial window (see [Figure 1-12](#)) shows the health of the VCDS process, the VQE Tools server, and other status information.

**Figure 1-12** VCDS Status Information



The VCDS AMT displays status and configuration on the VCDS configuration, and on the VQE-C channel configuration, the client database, and the group attribute files (see [Figure 1-13](#)).

Figure 1-13 VCDS Configuration Window

Section	Parameter	Value
VCDS Configuration	TCP Port	8554
	Max Connections Allowed	2000
	Inactive Connection Timeout (sec)	10
VQE-C Channel Lineup	Validation Check	Pass
	No. of Channels in Lineup	1
	Lineup Filename	/etc/opt/vqes/vqec_channels.cfg
	Last Modified	Thu, 9 Jul 2009 15:27:15 EDT
VQE-C Group Map	Validation Check	Pass
	No. of CNames in Map	2
	Map Filename	/etc/opt/vqes/vqec_group_map
	Last Modified	Mon, 13 Jul 2009 16:26:27 EDT
VQE-C Network Configuration	Validation Check	Pass
	No. of Groups in Network Configuration File	2
	Network Configuration Filename	/etc/opt/vqes/vqec_attributes.cfg
	Last Modified	Mon, 13 Jul 2009 17:20:30 EDT

The VCDS AMT displays configuration and status information for the channel configuration, the client database, and the group attribute files. For the channel configuration file, the VCDS AMT indicates whether the file contents are valid. It displays the full pathname of the file, the number of channels contained in the channel lineup and the timestamp of the last modification to the file. For the client database file, the VCDS AMT indicates whether the file contents are valid. It displays the full pathname of the file, the number of CNames (VQE-C unique identifier) in the file and the timestamp of the last modification to the file. For the group attribute file, the VCDS AMT indicates whether the file contents are valid. It displays the full pathname of the file, the number of attribute groups in the file and the timestamp of the last modification to the file.

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

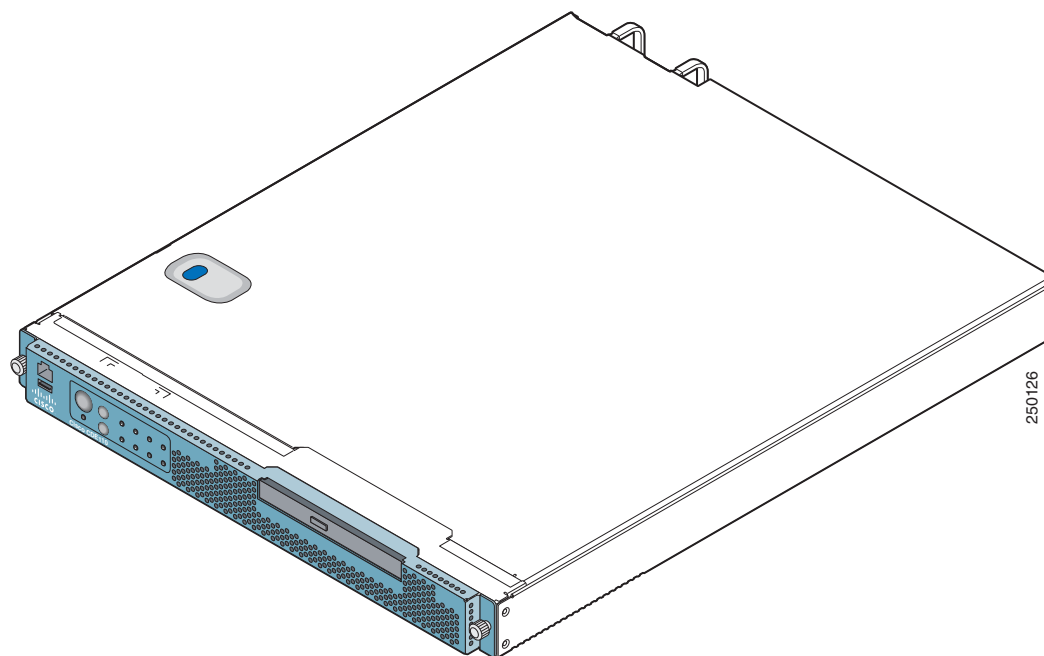
- Logging priority level for VCDS processes
- Debugging options for VCDS-related functions

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

# Content Delivery Engine 110

Each VQE-S runs on one Cisco Content Delivery Engine 110 (CDE110). If the VCPT and the VCDS are used, another Cisco CDE110 hosts these two facilities. The Cisco CDE110, shown in [Figure 1-14](#), comes with the Red Hat Enterprise Linux Release 5.1 operating system and either the VQE-S or the VCPT and the VCDS software preinstalled.

**Figure 1-14** 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 Layer 2 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 RCC streams to the VQE-Cs.

**Note**

The VQE-S supports Gigabit Ethernet (that is, 1000 Mb Ethernet) interfaces only.

The Cisco CDE110 has a 1-RU form factor and is available with redundant AC or DC hot-swappable power supplies. The Cisco CDE110 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 server (VQE-S)—CDE110 hosting VQE-S
- VQE Tools server—CDE110 hosting the VQE Channel Provisioning Tool (VCPT) and the VQE Client Configuration Delivery Server (VCDS)

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

For information on installing or upgrading VQE software, see *Release Notes for Cisco CDA Visual Quality Experience Application*.



### 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:

- [Web Browser, Screen Resolution, and Other Requirements, page 2-2](#)
- [System Port Numbers, page 2-3](#)
- [Configuring Terminal Emulation Software, page 2-3](#)
- [Security Restrictions for Logins and Root Privileges, page 2-4](#)
- [Prerequisites, page 2-4](#)
- [Setting Up SSL Certificates, page 2-5](#)
- [VQE-S: Routing and Interface Configuration Overview, page 2-14](#)
- [VQE Tools Server: Routing Configuration Overview, page 2-22](#)
- [Using the VQE Startup Configuration Utility, page 2-23](#)
- [On the VQE-S Host: Verifying the Status of the VQE and System Services, page 2-38](#)
- [On the VQE Tools Host: Verifying the Status of the VQE and System Services, page 2-40](#)

- [Configuring the VQE-S RTCP Exporter, page 2-42](#)
- [Configuring the Other Parameters for the VQE-S Host, page 2-43](#)
- [Configuring the Edge Router for VQE-S, page 2-44](#)

**Note**

The configuration instructions in this chapter are intended for new installations of Cisco VQE Software, Release 3.5, where the Cisco CDE110 has the Cisco VQE Software, Release 3.5 preinstalled.

For information on upgrading a Cisco CDE110, see *Release Notes for Cisco CDA Visual Quality Experience Application, Release 3.5*.

This chapter assumes that the Cisco CDE110 hardware has been installed as described in *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 AMT, the VCDS AMT, or the 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 the VQE-S AMT, the VCDS AMT, and the VCPT is 1024 x 768 pixels.

For the VQE-S AMT, Adobe Flash Player must be installed on the computer that hosts the browser accessing the VQE-S 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://get.adobe.com/flashplayer/>

# System Port Numbers

Table 2-1 presents the TCP ports used by the VQE-S, and displays the user of each port.

**Table 2-1 VQE-S System Ports**

Port Number	Menu Description
21	FTP
22	SSH <sup>1</sup>
161	SNMP <sup>2</sup>
162	SNMP traps
443	HTTPS <sup>3</sup>
444	HTTPS push
8005	Apache tomcat
8009	Apache tomcat
8050	VQE process monitor
8051	VQE-S CP <sup>4</sup> XML-RPC <sup>5</sup>
8052	MLB <sup>6</sup> RPC
8053	VCDS
8054	STUN Server RPC

1. SSH = Secure Shell.
2. SNMP = Simple Network Management Protocol.
3. HTTP = Hypertext Transfer Protocol Secure.
4. CP = control plane.
5. XML-RPC = XML remote procedure call.
6. MLB = multicast load balancer.

Ports 8005, 8009, 8050, 8051, 8052, 8053, and 8054 are not open for external use. All other ports listed in Table 2-1 are only accessible from a management interface. For information on management interfaces, see the “[Interface for a Management Network](#)” section on page 2-20.

## 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:

- SSH is used to log in to the CDE110 that hosts the VQE-S and VQE Tools server. However, a root user cannot use SSH to log in to a CDE110, VQE-S AMT, VCDS AMT, or VCPT. The `vqe` username should be used instead. The `vqe` username is a precreated Linux user ID, and has its password set during the 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 command syntax, `username` specifies the user who is 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 the 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 2-4](#).
- 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 2-5](#).

## Connecting Cables to the CDE110

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

- Depending on whether the host is for the VQE-S or the 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, use Category 5 UTP (Unshielded Twisted Pair) 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. Use Gigabit Ethernet (1000 Mb Ethernet) interfaces only. For optimal VQE-S performance, all Ethernet interfaces on the Cisco CDE110 should have a direct Layer 3 connection to the edge router. For OSPF routing on the VQE-S, 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 the VQE-S are on. It is recommended that you use Gigabit Ethernet interfaces. 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 *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 2-6](#).

## Setting Up SSL Certificates

SSL is used on the CDE110s hosting the VQE-S and the VQE Tools server to create secure communication channels using Triple Data Encryption Standard (3DES) between web browsers and the VQE-S Application Monitoring Tool (AMT), the VCDS AMT, and the VCPT. SSL is also used by the VCPT when providing channel information to the VQE-S and the VCDS.

The HTTP server on the VQE-S and the VQE Tools server is not usable until the SSL certificates and other required SSL files are created and deployed. The VQE-S AMT, the VCDS AMT, and the VCPT require SSL certificates from a certificate authority (CA) to be created and deployed. The CA can be you or someone in your company, or a commercial CA, such as VeriSign. The procedures to create and deploy certificates are explained in the following sections:

- [Using the Cisco VQE Startup Configuration Utility for SSL Certificates, page 2-6](#)
- [Creating Your Own Certificate Authority, page 2-9](#)
- [Generating and Deploying Your Own SSL Certificates, page 2-10](#)
- [Deploying Commercial SSL Certificates, page 2-13](#)

You perform the procedures for deploying CA certificates on the VQE-S hosts and the VQE Tools 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 the VQE Tools 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

The Cisco VQE Startup Configuration Utility provides you with various options to create and deploy SSL certificates:

- Option 1—Creating and deploying self-signed certificates using the Cisco VQE Startup Configuration Utility.

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

For an explanation of the tasks involved in Option 1, see the “[Step-by-Step Example: Creating and Deploying Self-Signed Certificates Using the Cisco VQE Startup Configuration Utility](#)” section on page 7.

- Option 2—Creating commercial or self-signed SSL certificates using the Cisco VQE Startup Configuration Utility to generate a Certificate-Signing Request and manually deploying certificates.

The Cisco VQE Startup Configuration Utility generates only a Certificate-Signing Request file (server.csr) in the /etc/opt/certs directory.

If you are signing the Certificate-Signing Request with a self-created certificate authority, see the “[Signing the Certificate-Signing Request](#)” section on page 11 for information on how to generate a self-signed SSL certificate. You must install the certificates, private key, and keystore as described in the “[Installing the Certificates, Private Key, and Keystore](#)” section on page 12.

If you are submitting the Certificate-Signing Request to a commercial CA, see the “[Deploying Commercial SSL Certificates](#)” section on page 13 for information on how to generate and deploy a commercial SSL certificate. You can, however, omit the first step in this section (generating a Certificate-Signing Request) because the VQE Startup Configuration Utility does this for you.

- Option 3—Manually creating and deploying commercial or self-signed SSL certificates.

To manually create and deploy SSL certificates without using the Cisco VQE Startup Configuration Utility, follow the directions provided in these sections:

- For overview information of the SSL tasks, see the “[Setting Up SSL Certificates](#)” section on page 5.
- For deploying your own SSL certificates, see the “[Creating Your Own Certificate Authority](#)” section on page 9 and the “[Generating and Deploying Your Own SSL Certificates](#)” section on page 10.
- For deploying commercial SSL certificates, see the “[Deploying Commercial SSL Certificates](#)” section on page 13.

## Step-by-Step Example: Creating and Deploying Self-Signed Certificates Using the Cisco VQE Startup Configuration Utility

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 the VQE-S, when the VQE Startup Configuration Utility runs and displays “Prepare SSL certificate for HTTPS service,” choose 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 the VQE-S before performing [Step 2](#).

**Step 2** On the CDE110 hosting VQE Tools, when the VQE Startup Configuration Utility runs and displays “Prepare SSL certificate for HTTPS service,” choose 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 is used on the VQE Tools 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 the VQE Tools before performing [Step 3](#).

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

**Step 4** On the CDE110 hosting the VQE Tools 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 its output, is used only on the VQE Tools host and must be located in the /etc/opt/certs directory.

**Step 5** On the VQE-S and VQE Tools hosts, restart the httpd daemon and the tomcat5 service by logging in as root and entering the following commands:

```
[root@system]# service httpd restart
[root@system]# service tomcat5 restart
```

**Step 6** After the VQE-S and VQE Tools hosts are configured and the 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 the VQE-S AMT, VCDS AMT, and VCPT.

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

```
https://ip_address_of_VQES_host
```

The VQE-S AMT login screen should be displayed.

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

```
https://ip_address_of_VQE_tools_host/vcds-amt
```

The VCDS AMT login screen should be displayed.

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

```
https://ip_address_of_VQE_tools_host
```

The VCPT login screen should be displayed.

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

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 the VQE-S and the VCPT. The CA that you create can be used to sign server certificates on all CDE110 servers hosting the VQE-S or the VQE Tools.

To create a CA certificate, perform the following steps:

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



### Note

When generating an encrypted RSA private key, a pass phrase requirement can be added by including the **-des3** option. The pass phrase is needed every time this CA signs a certificate request.

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

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

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 3650 -key ca.key -out ca.crt
```



### Note

The **-days** option specifies the number of days to certify the certificate for. Set this value so that it meets the requirements of your deployment. *The value 3650 (specified in the preceding command) may be too many or too few days for some deployments.*

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—Country where your company resides. Use the two-letter country code without punctuation for country (for example, US or FR).
- State or Province—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—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**—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**—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, perform the following steps:



#### Note

When generating a private key, a pass phrase requirement can be added by including the **-des3** option. However, adding a pass phrase requirement is not recommended as it requires human intervention. On every service or system restart someone must manually enter the pass phrase.

---

#### Step 1

To generate a server private key, enter the following command:

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

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 a Certificate-Signing Request, enter 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 9](#). 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 can be signed by commercial CA entities, such as VeriSign, or by your own CA, as described in the [“Creating Your Own Certificate Authority”](#) section on page 9.

**Note**

If you 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, enter the following command:

```
$ openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt
```

**Note**

The **-days** option specifies the number of days to make the certificate valid for. The start date is set to the current time and the end date is set to the value specified in the **-days** option. Set this value so that it meets the requirements of your deployment. *The value 3650 (specified in the preceding command) may be too many or too few days for some deployments.*

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-S-related or the VCPT-related software.

To install the server and CA certificates, the private key and the keystore, perform the following 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 following example shows the stackedChain.pem file:

```
-----BEGIN CERTIFICATE-----
MIIDvjCCAAyCAQEwDQYJKoZIhvcNAQEFBQAwZTElMAkGA1UEBhMCVVMxDTALBgNV
... Omitted contents ...
/kzgDk5wO1CbTwuxPIY1piy0Os1Q5EWk3VVAmv4tNMT9bANeKDUiVyYyOi1NIiHA
36w=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGDCCBACgAwIBAgIJAPtvlrCRokk4MA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
... Omitted contents ...
KV+sxNECGE40iWIVd1dXDA1034qhAwkVD6/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 a VCPT only, to create a trust-store file for the SSL Java client, enter 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 9.

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 the following steps:

1. Generate a Certificate-Signing Request. See the “[Generating a Certificate-Signing Request](#)” section on page 10.
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 on page 13 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 following example shows the `stackedChain.pem` file:

```
-----BEGIN CERTIFICATE-----
MIIDvjCCAaYCAQEwdQYJKoZIhvcNAQEFBQAwZTELMAkGA1UEBhMCVVMxDTALBgNV
... Omitted contents ...
/kzqDk5w01CbTwuxPIY1piy0Os1Q5EWk3VVAmv4tNMT9bANeKDUiVyYyOi1NIiHA
36w=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

```

MIIGDCCBACgAwIBAgIJAPtvlrCRokk4MA0GCSqGSIb3DQEEBBQUAMGUxCzAJBgNV
... Omitted contents ...
KV+sxNECGE40iWIVd1dXDA1034qhAwkVD6/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 the VCPT only, to create a trust-store file for the SSL Java client, enter 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: Routing and Interface Configuration Overview

For a VQE-S, the VQE Startup Configuration Utility supports configuring static routes and configuring both static and dynamic, Open Shortest Path First (OSPF) routing. This section provides overview information on how you can configure static routes and OSPF routing on a VQE-S. It introduces the concept of bond interfaces, which may be used for static and OSPF routing. It includes these topics:

- [Bond Interfaces on a VQE-S, page 2-15](#)
- [Types of Routes on a VQE-S, page 2-16](#)
- [Static Routes on a VQE-S, page 2-16](#)
- [OSPF Routing on a VQE-S, page 2-17](#)
- [Using Dedicated or Shared Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic, page 2-17](#)
- [Routing Configuration for Dedicated Interfaces and Shared Interfaces, page 2-18](#)
- [Interface for a Management Network, page 2-20](#)
- [Load Balancing and Redundancy with Multiple VQE-S, page 2-21](#)

At initial system startup, the VQE Startup Configuration Utility can be used to configure static routes and OSPF routing. After initial system startup, the VQE Configuration Tool can be used to modify the routing implementation.

## Bond Interfaces on a VQE-S

One or more bond interfaces may be configured on a CDE110 that hosts the VQE-S. Two or more physical, Ethernet interfaces, may be combined into a single, logical bond interface, which has the combined capacity of the underlying Ethernet interfaces. For example, a bond interface that combines three 1 Gbps Ethernet interfaces has a capacity of 3 Gbps. All Ethernet interfaces that are members of a bond interface are active. In Linux, a bond interface is referred to as a master interface. On Cisco routers, the terms EtherChannel and port-channel group are used to refer to a bond interface. A bond interface must be configured on both the VQE-S and on the attached Edge router.

The use of a bond interface has the following benefits:

- Complexity of interface and routing configuration is reduced. An IP address and prefix length is assigned to the bond interface only. None of the underlying physical, Ethernet interfaces have an IP address and prefix length assigned.
- Feedback Target (FTB) routes are advertised on the bond interface and not on each of the underlying, physical interfaces, thereby reducing the number of Equal Cost Multi-Path (ECMP) advertisements per VQE-S.

Bond interfaces may be used for the following interfaces:

- Bond interfaces may be used to support VQE-S traffic (ingest and services) in configurations where shared interfaces to the access and distribution networks are configured.
- Bond interfaces may be used to support VQE-S ingest traffic in configurations where dedicated interfaces to the distribution network are configured.
- Bond interfaces may be used to support VQE-S services traffic in configurations where dedicated interfaces to the access network are configured.
- Bond interfaces may be used to support management traffic on a VQE-S. Management traffic may use a designated interface or may share interfaces used by other traffic types, including VQE-S traffic (ingest and services), VQE-S ingest traffic, or VQE-S services traffic. On a VQE-S, a combination of bond interfaces and Ethernet interfaces can be used for management traffic.

All members of a bond interface must have the same capacity. Ethernet interfaces that are members of a bond interface should not be assigned an IP address and prefix length nor should they be specified as an interface for VQE-S traffic (ingest and services), VQE-S ingest traffic, VQE-S services traffic, or VQE-S management traffic. The IP address and prefix length, and the interface role are assigned to the parent bond interface. An Ethernet interface may be a member of a one bond interface only.

**Note**

For VQE-S traffic (ingest and services), VQE-S ingest traffic, VQE-S services traffic, multiple bond interfaces should not be used and a combination of bond interfaces and Ethernet interfaces can not be used because load balancing can not work effectively if there is no guarantee that each interface in the link has the same capacity.

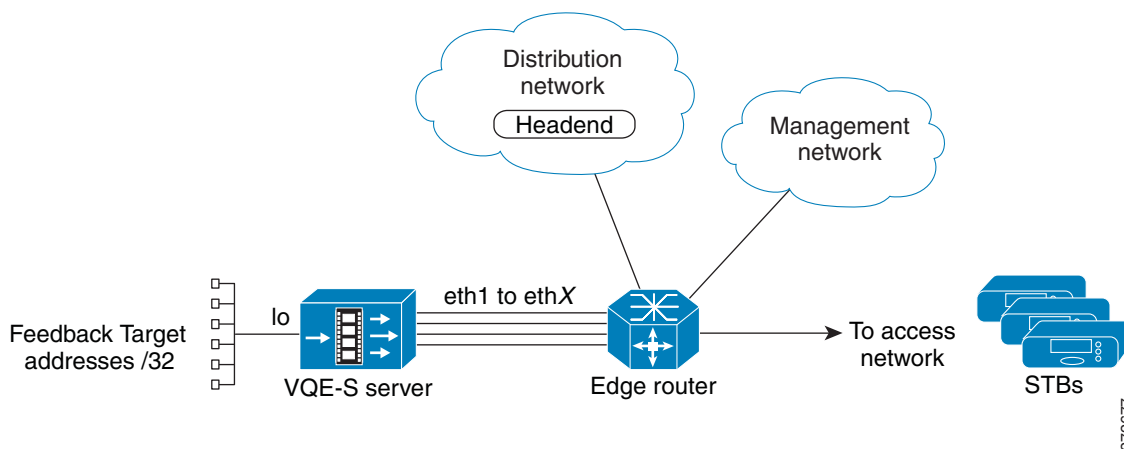
## Types of Routes on a VQE-S

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

- Management routes—Static route on the VQE-S through a directly attached edge router to the management network.
- Access routes—Routes on the VQE-S through a directly attached edge router to the access network, where the VQE Clients (VQE-Cs) on the set-top boxes (STBs) live.
- Feedback target routes—Routes on a directly attached edge router to the VQE-S that advertise reachability of the VQE-S feedback targets (FBTs) into the access network, where the STBs reside. Each FBT is associated with a channel. VQE-Cs on the STBs send requests for Unicast Retransmission and RCC services to the feedback target addresses. The VQE-S configures each channel FBT address as a host address on the VQE-S loopback interface.

The VQE-S also joins the multicast RTP streams from the distribution network. This interaction is between the VQE-S 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. This interaction is, in general, outside the scope of this discussion. [Figure 2-1](#) shows the types of routes used on a VQE-S.

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



## Static Routes on a VQE-S

In Cisco VQE Release 3.1, OSPF routing was introduced on the VQE-S. Before this, the access routes and feedback target routes on a VQE-S 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 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 configuring static-route parameters on a VQE-S, see the [“Static Route Configuration: IP Address, Prefix Length, and Gateway Address”](#) section on page 26.

For information on static route configuration on the edge router, see the [“For Static Routes: Guidance for Configuring the Feedback Targets on the Attached Router”](#) section on page 2-47.

## OSPF Routing on a VQE-S

Starting with Release 3.1, Cisco VQE supports a dynamic routing feature, which uses OSPF routing to the access network from the VQE-S. The use of OSPF routing eliminates the limitations of static routing, see the [“Static Routes on a VQE-S”](#) section on page 16. 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



### Note

If a bond interface is configured to support VQE-S traffic (ingest and services) or VQE-S services traffic and if OSPF routing is enabled, the corresponding edge router must support the configuration of EtherChannels (that is, bond interfaces). Otherwise, the bond interface between the VQE-S and the edge router does not operate.

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, 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. 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 configuring OSPF parameters for a VQE-S, see the [“OSPF Configuration \(VQE-S Host Only\)”](#) section on page 28.

For information on OSPF configuration on the edge router, see the [“For OSPF Routing: Guidance for Configuring the Attached Router”](#) section on page 45.

## Using Dedicated or Shared Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic

Some VQE deployments require that the CDE110 Ethernet interfaces or bond interfaces used for VQE-S ingest traffic (incoming multicast streams from the video sources) be separate from the interfaces used for VQE-S services traffic (Unicast Retransmission and RCC to the VQE-Cs on the STB). Dedicated Ethernet interfaces or dedicated bond interfaces allow the video distribution network to be separate from the access network.

The service provider can choose one of the following approaches when configuring the CDE110 Ethernet or bond interfaces:

- **Dedicated Interfaces**—If a VQE deployment requires that the interfaces used for VQE-S ingest traffic from upstream video sources be separate from the interfaces used for VQE-S services traffic to the downstream VQE-Cs on the STBs, the CDE110 Ethernet or bond interfaces must be configured as follows:
  - Either one or more Ethernet interfaces or one or more bond interfaces are configured as dedicated interfaces for VQE-S ingest traffic.
  - Either one or more Ethernet interfaces or one or more bond interfaces are configured as dedicated interfaces for VQE-S services traffic.

The Cisco VQE Startup Configuration Utility and the VQE Configuration Tool allow you to configure dedicated CDE110 Ethernet interfaces or bond interfaces for VQE-S ingest traffic and for VQE-S services traffic.

- **Shared Interfaces**—If a VQE deployment does not require that the Ethernet interfaces or bond interfaces used for VQE-S ingest traffic be separate from the interfaces used for VQE-S services traffic, a single set of CDE110 Ethernet interfaces are configured or one or more bond interfaces are configured as VQE-S traffic interfaces that handle both types of traffic. This combined traffic interface was the only configuration available before Cisco VQE Release 3.3.1. The Cisco VQE Startup Configuration Utility and the VQE Configuration Tool allow you to configure these shared VQE-S traffic interfaces.

**Note**

For VQE-S traffic (ingest and services), VQE-S ingest traffic, VQE-S services traffic, multiple bond interfaces should not be used because load balancing cannot work effectively if there is no guarantee that each interface in the link has the same capacity.

[Table 2-2](#) shows where to find information on the configuration parameters that are used for dedicated and shared interfaces.

**Table 2-2** Where To Find Information on Parameters for Dedicated and Shared Interfaces

Configuration Parameter For	Where To Find Information
<b>Dedicated Interfaces</b>	
Dedicated interfaces for VQE-S ingest traffic	<a href="#">“Interfaces for VQE-S Ingest Traffic (VQE-S Host Only)” section on page 2-29</a>
Dedicated interfaces for VQE-S services traffic	<a href="#">“Interfaces for VQE-S Services Traffic (VQE-S Host Only)” section on page 2-30</a>
<b>Shared Interfaces</b>	
VQE-S traffic interfaces that handle VQE-S ingest traffic and VQE-S services traffic	<a href="#">“Interfaces for VQE-S Traffic (Ingest and Services) (VQE-S Host Only)” section on page 2-30</a>

## Routing Configuration for Dedicated Interfaces and Shared Interfaces

When a VQE deployment uses shared VQE-S traffic interfaces that handle both VQE-S ingest traffic and VQE-S services traffic, configuration of the CDE110 interfaces is as follows:

- One or more interfaces for VQE-S traffic use a static default route, or OSPF routing, or both.
- One or more interfaces for VQE-S management traffic use static routing to the management network.

When a VQE deployment uses separate dedicated interfaces for VQE-S ingest traffic and for VQE-S services traffic, configuration of the CDE110 interfaces is as follows:

- One or more interfaces for VQE-S services traffic use either a static default route, or OSPF routing, or both.
- One or more interfaces for VQE-S ingest traffic use static routing to the distribution network where the video sources reside.
- One or more interfaces for VQE-S management traffic use static routing to the management network.

For information on the configuration parameters that are used for static routes, see the [“Static Route Configuration: IP Address, Prefix Length, and Gateway Address”](#) section on page 26.

For information on the configuration parameters that are used for OSPF routing, see the [“OSPF Configuration \(VQE-S Host Only\)”](#) section on page 28.

## Configuring Static Routes

When a VQE deployment uses dedicated interfaces for VQE-S ingest traffic, the ingest interfaces use static routing to the distribution network where the video sources reside. To configure one or more static routes to the video distribution network, use the VCDB parameter `network.route.static_route`. Using the VQE Startup Configuration Utility or VQE Configuration Tool and their VCDB parameters, you specify the following for each ingest interface:

- Subnet IP address and prefix length for the distribution network.
- Gateway (network hop) IP address of the router interface that is directly attached to a CDE110 Ethernet interface that is used for ingest traffic.
- Optionally, an outbound interface on the VQE-S or VQE Tools server for the static route. To specify an outbound interface, append the interface name to the Gateway IP address, and separate both with a colon.



### Caution

Configuring an outbound interface is not generally necessary nor is it recommended.

In following example from the VQE configuration Tool, two statics routes are configured. Ethernet interfaces `eth1` and `eth2` are configured as ingest interfaces. The IP address and prefix length of the distribution network is `192.0.0.0/8`. The gateway IP address for the router interface directly attached to `eth1` is `10.2.9.1`. The gateway IP address for the router interface directly attached to `eth2` is `10.2.10.1`.

VQE Configuration Tool <Static Routing Parameters> Menu:

```
1) Static Route(s):
P) Go to Parent Menu
R) Go to Root Menu
```

Enter your choice: **1**

Add new static routes by entering destination subnet IP/Prefix and gateway IP pairs when prompted.

To configure a default route, enter `0.0.0.0/0` as the destination subnet IP/Prefix.

To specify a specific gateway interface (optional), add it to the end of the gateway IP, separated by ":" (e.g. `"5.6.7.8:eth3"`).

To complete the configuration, press <Enter> at the prompt without entering data.

```
Enter the destination subnet in IP/Prefix format (e.g., 1.0.0.0/8): 192.0.0.0/8
```

```
Enter the gateway IP address: 10.2.9.1
```

```
Enter the destination subnet in IP/Prefix format (e.g., 1.0.0.0/8): 192.0.0.0/8
```

```
Enter the gateway IP address: 10.2.10.1
```

As the example shows, two static routes to the distribution network are configured; 192.0.0.0/8 via 10.2.9.1 (nexthop), and 192.0.0.0/8 via 10.2.10.1 (nexthop).

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)    192.0.0.0/8 via 10.2.9.1
   1.2)    192.0.0.0/8 via 10.2.10.1
P) Go to Parent Menu
R) Go to Root Menu

```

Enter your choice:

Each static route has its own submenu. This allows an additional static route to be added without having to delete and recreate existing static routes. It also means that a single static route can be deleted or edited without effecting the other static routes.

As the example below shows, static route 192.0.0.0/8 via 10.2.10.1 can be deleted without having to delete static route 192.0.0.0/8 via 10.2.9.1. To restore the default value of a specific route, enter the number of the sub-menu for that specific value followed by the letter “d” and press **Enter**. For example:

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)    192.0.0.0/8 via 10.2.9.1
   1.2)    192.0.0.0/8 via 10.2.10.1
P) Go to Parent Menu
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: **1.2d**

In this example, when the Static Route(s) menu is displayed, the menu shows that the static route 192.0.0.0/8 via 10.2.10.1 has been deleted.

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)    192.0.0.0/8 via 10.2.9.1
P) Go to Parent Menu
R) Go to Root Menu

```

## Interface for a Management Network

From Cisco VQE Release 3.4, management traffic is blocked from non-management interfaces. The service provider must designate at least one CDE110 Ethernet interface or one bond interface as a management interface. Bond interfaces are configurable on the VQE-S hosts only. Multiple Ethernet or bond interfaces may be designated as management interfaces. The default value is all Ethernet interfaces on the VQE-S or VQE Tools server, regardless of their operational status.



### Note

You must use the VQE Configuration Tool to limit the interfaces where management traffic is allowed or remove any Ethernet interfaces that are members of a bond interface and include the bond interface name.

Table 2-3 displays the list of protocol port numbers that are blocked on non-management interfaces on VQE-S and VQE Tools Server. It also displays the standard type of management traffic associated with each of the ports.

**Note**

If ports other than those listed in Table 2-3 are used for management traffic on non-management interfaces, management traffic on the non-standard protocol ports is not blocked.

**Table 2-3 Standard Management Protocol Ports Blocked on Non-Management Interfaces**

Port Number	Standard Management Traffic Type
22	SSH <sup>1</sup>
443	HTTPS <sup>2</sup>
444	HTTPS Push
161 and 162	SNMP <sup>3</sup>
21	FTP

1. SSH = Secure Shell.
2. HTTPS = Hypertext Transfer Protocol Secure.
3. SNMP = Simple Network Management Protocol.

VQE-S traffic (ingest and services), VQE-S ingest traffic or VQE-S services traffic may share the management interfaces. If your deployment requires that VQE-S traffic (ingest and services), VQE-S ingest traffic, or VQE-S services traffic be excluded from the CDE110 Ethernet interfaces or bond interfaces used for management traffic, do not include those CDE110 Ethernet interfaces or bond interfaces in the following VQE Startup Configuration Utility and Configuration Tool parameters:

- Interfaces for VQE-S Ingest Traffic
- Interfaces for VQE-S Services Traffic
- Interfaces for VQE-S Traffic (ingest and services)

To set up one or more static routes to the management network, use the Static Route(s) parameter in the VQE Startup Configuration Utility or Configuration Tool.

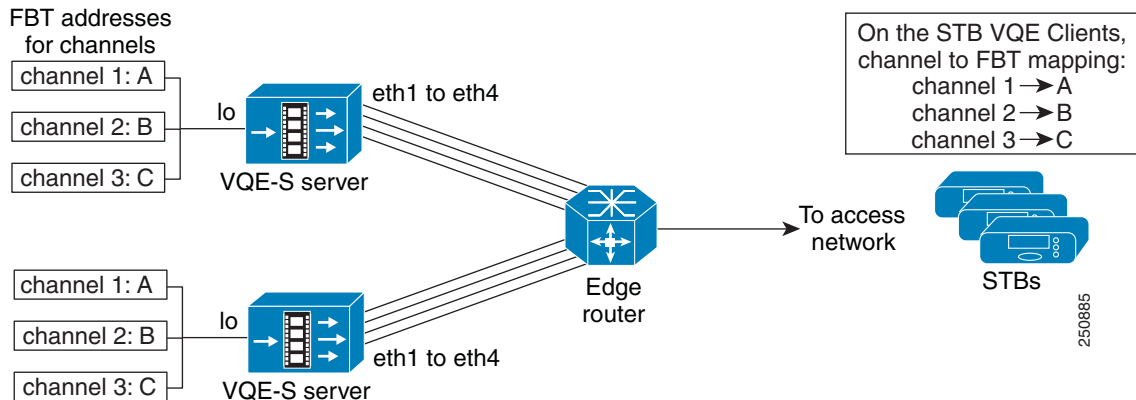
## Load Balancing and Redundancy with Multiple VQE-S

When more than one VQE-S provides Unicast Retransmission and RCC or both services for a set of channels, the VQE-Ss and edge router can load balance the requests from the VQE-Cs on the STBs and provide failover protection if a VQE-S fails.

In the VCPT channel definition, each channel is associated with a unique feedback target (FBT) IP address. The VQE-Cs on the STBs 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 the VQE-S 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 interface of the VQE-S that is identified by the address).

The use of anycast IP addresses and Equal Cost Multipath (ECMP) routing allows multiple VQE-Ss 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-Ss, each providing Unicast Retransmission and RCC services for the same set of three channels. On both VQE-Ss, 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-Ss for Service Failover and Load Balancing**



When OSPF routing is configured on the VQE-S, the FBT routes are advertised from the VQE-S to the edge router. In this example, both VQE-Ss 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 fails, the second VQE-S 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-Ss were configured for VQE-S traffic, the edge router would load balance STB 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—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 VCDS to send channel and configuration information to the VQE-Cs on the STBs 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 preinstalled. 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 the first time a CDE110 boots normally. Do *not* attempt to use the utility twice because this produces incorrect and unpredictable results.

Before using the VQE Startup Configuration Utility, do the following to 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: Routing and Interface Configuration Overview](#)” section on page 2-14.
- Read the “[VQE Tools Server: Routing Configuration Overview](#)” section on page 2-22.
- Read the “[Configuration Parameters](#)” section on page 2-24.
- Complete the “[Preconfiguration Worksheets](#)” section on page 2-33.
- Read the “[VQE Configuration Tool Root Menu](#)” section on page 2-36.

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 the Status of the VQE and System Services](#)” section on page 38
- “[On the VQE Tools Host: Verifying the Status of the VQE and System Services](#)” section on page 40

## 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 need to gather some information before booting the CDE110 for the first time and using the VQE Startup Configuration Utility. The worksheets in the “[Preconfiguration Worksheets](#)” section on page 33 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 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, VCDS 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 toward 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.

Creating Linux users and maintaining password settings is the responsibility of the Cisco CDE110 system administrator. The default password settings for root, vqe, and Linux users are located in the `/etc/pam.d/system-auth-ac` file on the VQE-S and the VQE Tools server. For information on changing passwords for Linux and vqe users, see the Linux *passwd* man page at <http://linux.die.net/man/1/passwd>. For information on resetting the root password, see the “[Resetting the Root Password on the VQE-S or VQE Tools Server](#)” section on page 6-31. For more information on configuring password settings such as length, complexity, and ageing, for root, vqe, and Linux users, see the *pam\_passwdqc* man page at [http://linux.die.net/man/8/pam\\_passwdqc](http://linux.die.net/man/8/pam_passwdqc).

### 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 are 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 external 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 are used for this CDE110. The VQE Startup Configuration Utility prompts for the needed information.

**Ethernet Interface Configuration: IP Address and Prefix Length**

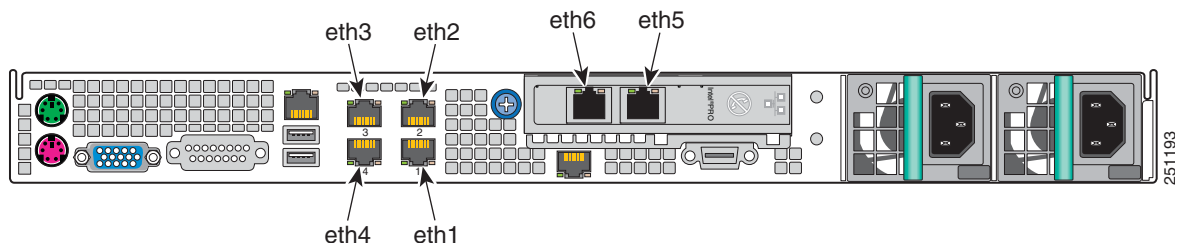
For one or more of the Ethernet ports on the Cisco CDE110, you specify an IP address and prefix length (for example, 1.2.3.4/32). The IP address and prefix length are not specified for any CDE110 Ethernet interface that is a member of a bond interface. The Ethernet ports are named eth1 to eth6 as shown 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 VCDS traffic.
- On the VQE-S host, at least one Ethernet or bond interface must be used for the management interface. On the VQE Tools host, at least one Ethernet interface must be used for the management interface. If an Ethernet interface is used, this 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**

**Bond Interface Configuration: IP Address and Prefix Length**

On the VQE-S, you specify an IP address and prefix length (for example, 1.2.3.4/32) for one or more bond interfaces using the `network.bondx.addr` parameter where, depending on CDE110 model, `bondx` is `bond1`, `bond2`, or `bond3`. For each bond interface, you assign Ethernet interfaces to the bond interface

using the network.*bondx*.member parameter where, depending on CDE110 model, *bondx* is bond1, bond2, or bond3. The Ethernet interfaces must not be members of an existing bond interface and do not have an IP address and prefix length assigned. On a VQE-S host, up to three bond interfaces may be configured and used for the Ethernet interfaces handling incoming multicast streams, outgoing VQE-S services, and management traffic.

In the following example from the VQE Configuration Tool, the IP address and prefix length of bond1 is 11.2.15.2/24 and the Ethernet interfaces assigned to bond1 are eth3 and eth4.

VQE Configuration Tool <Interface Parameters> Menu:

```

1) Eth1 Interface IP/Mask:          10.2.9.2/24
2) Eth2 Interface IP/Mask:          10.2.10.2/24
3) Eth3 Interface IP/Mask:          [bond1]
4) Eth4 Interface IP/Mask:          [bond1]
5) Eth5 Interface IP/Mask:          []
6) Eth6 Interface IP/Mask:          []
7) Bond1 IP/Mask and members:       [11.2.15.2/24 eth3,eth4]
8) Bond2 IP/Mask and members:       []
9) Bond3 IP/Mask and members:       []
10) Management Interface(s):        eth1,eth2
P) Go to Parent Menu
R) Go to Root Menu

```

Enter your choice:



#### Note

Bond interfaces are not supported on the VQE Tools server.

For more information on the restrictions that apply to the use of bond interfaces, see [“Bond Interfaces on a VQE-S” section on page 15](#).

#### Static Route Configuration: IP Address, Prefix Length, and Gateway Address

If your deployment makes use of static routes to the management, distribution, or access network, the VQE Startup Configuration Utility can configure static routes. Specify the following:

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

```
10.1.0.0/16
```



#### Note

On the VQE-S, when creating a default route, specify 0.0.0.0/0 as the subnet IP address and prefix length for the target network.

- Gateway (next hop) IP address of the interface on the router that is directly attached to the VQE-S CDE110 interface that is used for the target network. The interface on the VQE-S and the attached edge router may be an Ethernet interface or a bond interface. The interface on the VQE Tools server is always an Ethernet interface.
- Optionally, an outbound interface on the VQE-S or VQE Tools server for the static route. To specify an outbound interface, append the interface name to the Gateway IP address, and separate both with a colon.



#### Caution

Specifying an outbound interface is not generally needed, nor is it recommended.

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

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

**Note**

If you configure a static route for a management network, the Multicast Load Balancer (MLB) monitors the status of this route. If the MLB detects that the underlying interface is administratively down, the MLB attempts to recreate the route after the interface is brought back up.

On the VQE-S, multipath static routes can be configured for VQE-S traffic (ingest and services) or VQE-S services traffic. The VQE-S uses Equal Cost Multipath (ECMP) to load-balance its output traffic across CDE110 Ethernet interfaces or the physical Ethernet interfaces of a bond interface that are directly attached to the gateway router interfaces that are specified. If a default route (static route) 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 the CDE110 interfaces directly attached to the gateway router interfaces. Similarly, if a default route is configured for a bond interface, ECMP load balances output traffic across all the CDE110 physical interfaces assigned to the bond interface.

For more information on ECMP configuration, see the [“Configuring Static Routes for VQE-S Traffic or VQE-S Services Traffic \(VQE-S Host\)”](#) section on page D-8.

**SSL Certificate Options**

Secure Sockets Layer (SSL) certificates must be created and deployed for VQE-S AMT, VCDS 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 6.

**Trusted Provisioning Clients**

The use of this VCDB parameter, `system.iptables.trusted_provisioner`, varies depending on the VQE-S type:

- For a VQE-S host, if your IPTV deployment uses VCPT or another channel-provisioning server to send channel information to the VQE-S, 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 Clients. 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 or the `vcds_send_file` command sends a network configuration file to the VCDS, you specify, on the VQE Tools host, the IP address of the trusted VQE-C system configuration provisioning server or `vcds_send_file`. If `vcds_send_file` is used, *all Ethernet interfaces* (that have been assigned IP addresses) on the `vcds_send_file` host have to be specified as trusted provisioning clients. This requirement applies even when the VCDS is in the same VQE Tools server as the `vcds_send_file` command.

**Note**

If the needed IP addresses of the trusted provisioning servers are not configured on the VQE-S and VQE Tools servers, the servers reject attempts by the provisioning server or `vcdb_send_file` to send the channel or network configuration information.

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

**Remote Syslog Hosts**

On both the VQE-S and the VQE Tools server, VQE system messages are written to the file `/var/log/vqe/vqe.log` by default. In addition to logging system messages locally, you can send system messages by means of UDP to remote servers for centralized logging. This VCDB parameter, `system.syslog.remote_server`, is used to specify the IP addresses of the remote servers.

**SNMP Read-Only Community String, Location, Contact, and Trap-Listener IP Addresses or Hostnames**

If your deployment uses SNMP, 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 receives the SNMP messages.

For more information on SNMP for the CDE110, see [Appendix B, “SNMP MIBs.”](#)

**Sending SNMP Traps**

When SNMP is configured, the VQE-S and the VQE Tools server provide the capability to convert system messages to SNMP traps (syslog traps). To generate syslog traps, configure the following parameters:

- VCDB parameter `system.snmp.syslog_trap_enable` (Enable Syslog Traps menu)—Disabled by default.
- VCDB parameter `system.snmp.syslog_trap_priority` (Syslog Trap Priority menu)—When the generation of syslog traps is enabled, syslog messages with a severity level less than or equal to this value are sent as traps. The default value is 2 (critical). Valid values are 0 to 7. For a definition of each severity level, see [Table C-2 on page C-2](#).

The VQE-S provides the capability of sending a channel up trap when a channel becomes active and a channel down trap when a channel becomes inactive. Use the VCDB parameter `system.snmp.channel_trap_enable` (Enable Channel Up/Down traps menu) to enable or disable the generation of channel traps.

For information on configuring SNMP, see the [“SNMP Read-Only Community String, Location, Contact, and Trap-Listener IP Addresses or Hostnames”](#) section on page 28.

For more information on SNMP for the CDE110, see [Appendix B, “SNMP MIBs.”](#)

**OSPF Configuration (VQE-S Host Only)**

[Table 2-4](#) describes the parameters that can be configured if OSPF is enabled. For detailed information on the OSPF parameters, see the following Quagga documentation:

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

**Table 2-4 OSPF Parameters**

Parameter	Description
Enable OSPF	Specifies whether OSPF routing is enabled for VQE-S traffic (where shared interfaces to the access network are configured) or for VQE-S services traffic (where dedicated interfaces to the access network are configured).
Area Type	Type for the OSPF area that the VQE-S traffic interfaces and feedback target host addresses reside in. You can choose from 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 reside in. If no value is specified, the default value is 0. Allowed range is 0 to 4,294,967,295.
Router ID	IP address used as the router ID to uniquely identify the VQE-S 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 is added as an internal address to the loopback interface.
Enable MD5	Specifies whether MD5 <sup>1</sup> 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 is 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 is 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.
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 is 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 is 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.

1. MD5 = message digest 5.

For information about routing on the VQE-S host, see the [“VQE-S: Routing and Interface Configuration Overview”](#) section on page 14.

#### Interfaces for VQE-S Ingest Traffic (VQE-S Host Only)

If you choose to select dedicated interfaces for VQE-S ingest traffic, specify one or more CDE110 Ethernet interfaces or one or more bond interfaces that are used for ingest of multicast streams. Ethernet interfaces must not be members of an existing bond interface. Depending on CDE110 model, allowed choices of Ethernet interfaces are eth1 to eth6. Allowed bond interfaces are bond1 to bond3.

**Note**


---

For VQE-S ingest traffic, multiple bond interfaces should not be used because load balancing cannot work effectively if there is no guarantee that each interface in the link has the same capacity.

---

When you choose to select dedicated interfaces for VQE-S ingest traffic and separate dedicated interfaces for VQE-S services traffic (see the next parameter), the following rules apply:

- At least one interface must be specified in the Interfaces for VQE-S Ingest Traffic parameter (this parameter).
- At least one VQE-S services interface must be specified in the Interfaces for VQE-S Services Traffic parameter.
- Interfaces for VQE-S Ingest Traffic must not be specified in the Interfaces for VQE-S Services Traffic parameter.
- Interfaces for VQE-S Traffic (ingest and services) parameter (in VCDB, `vqe.vqes.vqe_interfaces`) must not be specified.
- If a dedicated interface is used for management traffic, it must not be specified in Interfaces for VQE-S Ingest Traffic parameter, in the Interfaces for VQE-S Services Traffic parameter, or in the Interfaces for VQE-S Traffic (ingest and services) parameter.

**Interfaces for VQE-S Services Traffic (VQE-S Host Only)**

If you choose to select a dedicated interface for VQE-S ingest traffic (the preceding parameter), you also must specify one or more CDE110 Ethernet interfaces or one or more bond interfaces that is used for VQE-S services—Unicast Retransmission and RCC traffic to downstream VQE-Cs on STBs. Ethernet interfaces must not be members of an existing bond interface. Depending on CDE110 model, allowed choices of Ethernet interfaces are eth1 to eth6. Allowed bond interfaces are bond1 to bond3.

**Note**


---

For VQE-S services traffic, multiple bond interfaces should not be used because load balancing cannot work effectively if there is no guarantee that each interface in the link has the same capacity.

---

For the rules that apply when you choose to select a dedicated interface for VQE-S ingest traffic and interfaces for VQE-S services traffic, see the preceding [“Interfaces for VQE-S Ingest Traffic \(VQE-S Host Only\)”](#) section on page 29.

**Interfaces for VQE-S Traffic (Ingest and Services) (VQE-S Host Only)**

If you choose *not to select* dedicated interfaces for VQE-S ingest and services traffic, you specify the CDE110 Ethernet interfaces or one or more bond interfaces that are available for all VQE-S Traffic (ingest and services). Ethernet interfaces must not be members of an existing bond interface. The shared interfaces are used for ingest of multicast streams from upstream video sources and for VQE-S services (Unicast Retransmission and RCC traffic to downstream VQE-Cs on STBs). Depending on CDE110 model, allowed choices of Ethernet interfaces are eth1 to eth6. Allowed bond interfaces are bond1 to bond3.

**Note**


---

For VQE-S Traffic (ingest and services), multiple bond interfaces should not be used because load balancing cannot work effectively if there is no guarantee that each interface in the link has the same capacity.

---

**Note**

If a dedicated interface is used for a management network, that interface must not be included as one of the interfaces that are available for VQE-S traffic (ingest and services).

**Interfaces for Management Traffic**

At least one CDE110 Ethernet interface or one bond interface must be specified as the management interface. Ethernet interface must not be members of an existing bond interface. VQE-S traffic (ingest and services), VQE-S ingest traffic or VQE-S services traffic may share the management interfaces. Management traffic is blocked from non-management interfaces.

For the rules that apply when you specify management interfaces, see the “[Interface for a Management Network](#)” section on page 2-20.

**VQE Configuration Tool Root Menu**

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:

For information on this menu, see the “[VQE Configuration Tool Root Menu](#)” section on page 2-36.

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 2-5](#) and [Table 2-6](#) are started.

**Table 2-5 VQE-S and System Services for CDE110 That Hosts VQE-S**

Service	Description
vqes	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) SNMP daemon.
snmpsa	(Optional) Intel SNMP subagent.
vqes_snmpsa	(Optional) VQE-S SNMP subagent
syslog_snmpsa	(Optional) Syslog SNMP subagent.
ntpd	(Optional) NTP daemon.
check_daemons	Script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a <b>cron</b> job owned by root.

**Table 2-5 VQE-S and System Services for CDE110 That Hosts VQE-S (continued)**

Service	Description
<b>If OSPF is selected as the routing type</b>	
watchquagga	Quagga watchdog process. If the ospfd or zebra daemon crashes or hangs, watchquagga restarts it automatically.
ospfd	OSPF daemon.
zebra	Zebra daemon.

**Table 2-6 VCDS and System Services for CDE110 That Hosts VQE Tools**

Service	Description
vcds	VCDS service.
sshd	Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	Apache Tomcat application server.
snmpd	(Optional) SNMP daemon.
snmpsa	(Optional) Intel SNMP subagent.
vcds_snmpsa	(Optional) VCDS SNMP subagent.
syslog_snmpsa	(Optional) Syslog SNMP subagent.
ntpd	(Optional) NTP daemon.
check_daemons	Script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a <b>cron</b> 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.

## Preconfiguration Worksheets

Before using the VQE Startup Configuration Utility, complete the preconfiguration worksheets in [Table 2-7](#) for a VQE-S host and [Table 2-8](#) 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 2-7](#) and [Table 2-8](#), see the “[Configuration Parameters](#)” section on page 24.

**Table 2-7 VQE-S CDE110: Preconfiguration Worksheet**

Configuration Item	Value for Your Deployment
Password for root	
Password for the vqe username (a predefined 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	
External NTP server IP addresses	
Ethernet interface configurations (IP address and prefix lengths)	eth1: eth2: eth3: eth4: eth5: eth6:
Bond interface configurations (IP address, subnet mask and members)	bond1: bond2: bond3:
For static routes, destination subnet IP address and prefix length, and gateway (next hop) IP address	Destination Subnet IP address and prefix length: Gateway (next hop) IP address:
SSL certificate option	
Trusted provisioning clients IP addresses	
Remote syslog hosts IP addresses	

**Table 2-7 VQE-S CDE110: Preconfiguration Worksheet (continued)**

Configuration Item	Value for Your Deployment
SNMP read-only community string	community string:
Location for SNMP	location:
Contact for SNMP	contact:
SNMP trap-listener IP addresses or hostnames	IP addresses or hostnames:
Are Syslog traps enabled?	Yes or No:
Syslog trap priority	
Are channel up/down traps enabled?	Yes or No:
If OSPF routing is enabled, 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 or bond interface name that is used for VQE-S ingest traffic	
Ethernet interface names or bond interface name that is used for VQE-S services traffic	
Ethernet interface names or bond interface name that is used for VQE-S traffic (ingest and services)	
One or more Ethernet interface names, or one or more bond interface names, or both that is used for management traffic	

**Table 2-8 VQE Tools CDE110: Preconfiguration Worksheet**

Configuration Item	Value for Your Deployment
Password for root	
Password for the vqe username (a predefined 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	

**Table 2-8 VQE Tools CDE110: Preconfiguration Worksheet (continued)**

<b>Configuration Item</b>	<b>Value for Your Deployment</b>
External NTP server IP addresses	
Ethernet interface configurations (IP address and mask)	eth1: eth2: eth3: eth4: eth5: eth6:
For static routes, destination subnet IP address and prefix length, and gateway (next hop) IP address	Destination Subnet IP address and prefix length: Gateway (next hop) IP address:
SSL certificate option	
Ethernet interface names that are used for management traffic	
Trusted provisioning clients IP addresses	
Remote syslog hosts IP addresses	
SNMP read-only community string	community string:
Location for SNMP	location:
Contact for SNMP	contact:
SNMP trap-listener IP addresses or hostnames	IP addresses or hostnames:
Are Syslog traps enabled?	Yes or No:
Syslog trap priority	

## VQE Configuration Tool 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 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 7-3](#). 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 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 or VQE Tools server.

Table 2-9 provides more information about the choices on the Root Menu. You enter the number or letter for your choice.

**Table 2-9 Root Menu Choices**

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) Trusted Provisioning Client(s) 7) Remote Syslog Host(s) 8) SNMP Parameters
1) System Parameters > SNMP Parameters	1) SNMP RO Community String 2) SNMP System Location 3) SNMP System Contact 4) SNMP Trap Listener(s) 5) Enable Syslog Traps 6) Syslog Trap Priority 7) Enable Channel Up/Down Traps
2) Network Parameters > Interface Parameters	Allows you to view the current interface parameter values that you have set, and to change or set the interface parameters values: 1) Eth1 Interface IP/Mask 2) Eth2 Interface IP/Mask 3) Eth3 Interface IP/Mask 4) Eth4 Interface IP/Mask 5) Eth5 Interface IP/Mask 6) Eth6 Interface IP/Mask 7) Bond1 IP/Mask and members 8) Bond2 IP/Mask and members 9) Bond3 IP/Mask and members 10) Management Interface(s)
2) Network Parameters > Routing Parameters > Static Routing Parameters	Allows you to view the current static routing parameter values that you have set, and change or set the static routing parameter value: 1) Static Route(s)
3) Configure VQE Password	Allows you to set the password for the vqe username. After 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 SSL <sup>1</sup> certificate for VQE-S AMT, VCDS AMT or VCPT, or to generate a Certificate-Signing Request file (server.csr).

Table 2-9 Root Menu Choices (continued)

Root Menu Choice	Menu Description
5) VQE-S Parameters	<p>Allows you to view the current VQE-S parameter values that you have set, and to change or set the VQE-S parameters values:</p> <ul style="list-style-type: none"> <li>1) Log Priority *</li> <li>2) Excess Bandwidth Fraction *</li> <li>3) Traffic (Ingest+Service) Interface(s)</li> <li>4) Ingest Interface(s)</li> <li>5) Service Interface(s)</li> </ul> <p>* 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 <code>vcdb.conf.sample</code> file and <a href="#">Appendix A, “VQE, System, and Network Parameters.”</a></p>
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 <code>/etc</code> , and reboots the CDE110 system.

1. SSL = Secure Sockets Layer

## On the VQE-S Host: Verifying the Status of the 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, enter 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, enter 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, enter 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, enter the following command:

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

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

- Step 6** If you configured SNMP, to verify that the Intel SNMP subagent service is running, enter the following command:

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

The SNMP subagent is running.

- Step 7** If you configured SNMP, to verify that the VQE-S subagent service is running, enter the following command:

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

vqes\_subagent (pid 28603) is running...

- Step 8** If you configured SNMP, to verify that the Syslog subagent service is running, enter the following command:

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

syslog\_subagent (pid 28472) is running...

- Step 9** If you enabled OSPF routing, to verify that the three OSPF-related services are running, enter 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 10** To verify that the VQE-S service is running, enter the following command:

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

process\_monitor (pid 21853) is running...

- Step 11** To check that the VQE-S processes are running, enter the following commands:

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

```
root      710      1  0 Mar24 pts/7    00:00:00 /opt/vqes/bin/process_monitor
vqes      723     710  0 Mar24 pts/7    00:00:00 stun_server --ss-uid 499 --ss-gid 499
--xmlrpc-port 8054 --log-level 6
root      782     710  99 Mar24 pts/7    29-21:09:08 vqes_dp --group vqes --max-channels 500
--max-outstanding-rpcs 500 --max-pkts 150000 --log-level 6 --rtp-inactivity-tmo 300
--max-core-bw 850000000 --reserved-core-rcv-bw 100000000 --reserved-core-er-bw 120000000
--max-rai-gap 15
vqes      855     710  0 Mar24 pts/7    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 --max-channels 500 --max-outstanding-rpcs 500 --max-queued-rpcs 1000
--max-reserved-rpcs 32000 --max-clients 32000 --er-pkt-tb-rate 50000 --er-pkt-tb-depth 100
--er-blp-tb-rate 10000 --er-blp-tb-depth 100 --client-er-policing
--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 --excess-bw-fraction-high-def 12
--high-def-min-bw 6000000 --buff-size-preroll-max 1500 --rcc-burst-delay-to-send 10
--rtp-dscp 0 --rtp-rcc-dscp -1 --rtcp-dscp 24 --overlap-loss 0 --intf-output-allocation 90
--max-rpr-stream-burst-msecs 30 --max-rpr-stream-burst-pkts 2 --unity-e-factor-interval 5
--min-client-excess-bw-fraction 0 --max-client-excess-bw-fraction 500
```

```
[root@system]# ps -ef | grep mlb
root      2989   2965   0 09:17 pts/0    00:00:03 mlb --interface eth2,eth3,eth4
--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 12** If you configured an IP address for an external NTP server, to verify that the NTP service is running, enter the following command:

```
[root@system]# service ntpd status
ntpd (pid 2790) is running...
```

**Step 13** To use the VQE-S AMT 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 AMT).

If you click **System** in the left pane, the VQE-S AMT displays information on the VQE-S processes and channels. [Figure 4-2](#) shows an example. Because at this point no channel information has been sent to the VQE-S, no channels are displayed.

**Step 14** 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 AMT.”](#)
- 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 the Status of the 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, perform the following steps:

**Step 1** If needed, log in as root.

- Step 2** To verify that the SSH service is running, enter 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, enter 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, enter 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, enter the following command:
- ```
[root@system]# service snmpd status
```
- snmpd (pid 2754) is running...
- Step 6** If you configured SNMP, to verify that the Intel SNMP subagent service is running, enter the following command:
- ```
[root@system]# service snmpsa status
```
- The SNMP subagent is running.
- Step 7** If you configured SNMP, to verify that the VCDS subagent service is running, enter the following command:
- ```
[root@system]# service vcds_snmpsa status
```
- vges\_subagent (pid 28603) is running...
- Step 8** If you configured SNMP, to verify that the Syslog subagent service is running, enter the following command:
- ```
[root@system]# service syslog_snmpsa status
```
- syslog\_subagent (pid 28472) is running...
- Step 9** If you configured an IP address for an external NTP server, to verify that the NTP service is running, enter the following command:
- ```
[root@system]# service ntpd status
```
- ntpd (pid 2790) is running...
- Step 10** To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE Tools:
- ```
https://ip_address_of_VQE_tools_host
```
- Log in with a Linux username and password.
- If you are able to log in successfully, VCPT is running correctly.
- Step 11** To use the VCDS AMT from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE Tools:
- ```
https://ip_address_of_VQE_tools_host/vcgs-amt
```

Log in using the VQE username and password. (Any valid Linux username and password can be used to log in to the VCDS AMT.)

If you click **System** in the left pane, the VCDS Status window displays information on the VCDS processes. [Figure 5-2](#) shows an example.

**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. You can get more information on VCPT host configuration in [Appendix D, “Manual Initial VQE System Configuration.”](#)

## Configuring the 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 AMT. This tool displays RTCP Exporter configuration details and status as well as counters of exported packets. The VQE-S AMT 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 the four key-value pairs for the RTCP Exporter parameters listed in [Table 2-10](#), to the file. 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 7-14](#). The parameters used for enabling the RTCP Exporter are not available in the VQE Configuration Tool.

**Step 3** Save the *vcdb.conf* file.

**Table 2-10** RTCP Exporter Parameters

Parameter	Value Required
<code>vqe.vqes.vqm_host="IP_addr_or_domain_name"</code>	IP address or fully qualified Internet domain name of the host on which the VQM application resides. There is no default value.
<code>vqe.vqes.vqm_port="vqm_port_no"</code>	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.

Table 2-10 RTCP Exporter Parameters (continued)

Parameter	Value Required
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.
vqe.vqes.exporter_filter_nack="true_or_false"	Either true or false. The value true excludes RTCP NACK compound packets from being exported to the VQM application, and false includes RTCP NACK compound packets in the RTCP data being exported.  This parameter is available in the VCDB starting with Cisco VQE Release 3.5.5.

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 the VQE-S, enter 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 7-18.

**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 the 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 RCC.

Read the following to get information on these additional parameters:

- [Chapter 7, “Configuring VQE Server and VQE Tools”](#) describes the tools and procedures 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.
- 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 is 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 Bond Interfaces: Guidance for Configuring Bond Interface on the Attached Router, page 2-44](#)
- [For OSPF Routing: Guidance for Configuring the Attached Router, page 2-45](#)
- [For Static Routes: Guidance for Configuring the Feedback Targets on the Attached Router, page 2-47](#)

### For Bond Interfaces: Guidance for Configuring Bond Interface on the Attached Router

This section provides guidance on manually configuring bond interfaces (EtherChannels) on the edge router that is directly attached to the VQE-S. This section assumes that the attached router is a Cisco 7600 running Cisco IOS software. A bond interface is referred to by the terms *EtherChannel* and *port-channel group* on a Cisco 7600 router. A port-channel is used to group up to four Ethernet interfaces. It aggregates the bandwidth of the underlying Ethernet interfaces. All Ethernet interfaces must have the same speed.

To configure a port-channel on the Cisco 7600 router, do the following:

---

**Step 1** Create a port-channel group.

```
interface port-channel channel-number
```

The *channel-number* is the number assigned to this port-channel interface. As each channel can consist of up to four Ethernet interfaces, the valid range is 1 to 4.

**Step 2** Assign an IP Address and subnet mask to the port-channel group.

```
ip address ip-address mask
```

**Step 3** Assign Ethernet interfaces to the port-channel group.

```
interface fastethernet number
```

**Step 4** Enable the EtherChannel by specifying the port-channel number and setting the mode to 'on'.

```
channel-group number mode ON
```

The EtherChannel has been statically configured without running dynamic protocols, such as Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP).

In the following example, the port-channel 1 is assigned an IP address and network mask. Next, the Ethernet port 1 and Ethernet port 2 on module 8 are assigned to port-channel 1. Finally, the EtherChannel is enabled.

```
7600# configure terminal
7600(config)# interface port-channel 1
7600(config-if)# ip address 1.1.1.10 255.255.255.0
7600(config-if)# exit
7600(config)# interface GigabitEthernet 8/1
7600(config-if)# channel-group 1 mode on
7600(config-if)# exit
7600(config)# interface GigabitEthernet 8/2
7600(config-if)# channel-group 1 mode on
```

```
7600(config-if)#
```

To display EtherChannel information, use the following command:

```
show etherchannel [channel-group] {port-channel | brief | detail | summary | port | load-balance | protocol}
```

The following example displays a summary of information for etherchannel 2.

```
7600# show etherchannel 2 brief

Group: 2
-----
Group state = L2
Ports: 4   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: - (Mode ON)

7600#
```

For more information on the commands used to configure EtherChannels on a Cisco 7600 router, see the [Cisco 7600 Series Router Cisco IOS Command Reference Guide](#).

## For OSPF Routing: Guidance for Configuring the Attached Router

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

- [VQE-S in a Separate OSPF Area, page 2-45](#)
- [VQE-S in Area 0, page 2-46](#)
- [General Guidelines, page 2-46](#)

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



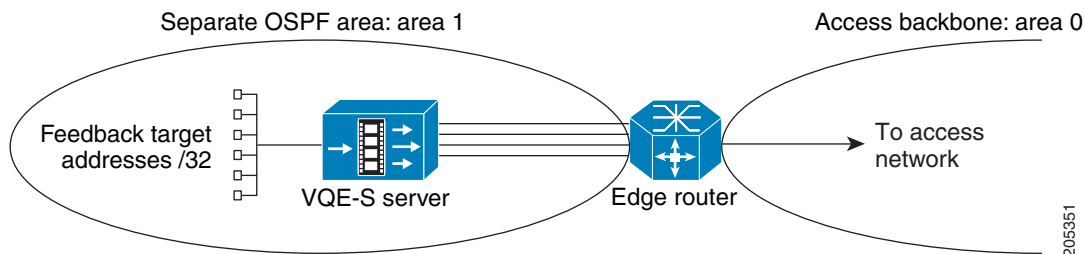
### Note

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 a Separate OSPF Area

The VQE-S 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 can be defined as a normal area or a Not So Stubby Area. [Figure 2-4](#) shows the VQE-S in a separate OSPF area: area 1.

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



When the VQE-S 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 in the same OSPF area as the VQE-S host.
- To keep the routing table on the VQE-S small in size, configure the separate area (in Figure 2-4, area 1) to be a Not So Stubby Area (NSSA). The VQE-S 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 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 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, see the “VQE-S in a Separate OSPF Area” section on page 45.

## General Guidelines

The following are general edge router configuration guidelines:

- Feedback target routes—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-Ss 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 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-Ss 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-Ss to work properly.
- **Forwarding table**—Size of the forwarding table on the edge router may be restricted, which limits the number of VQE-Ss 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-Ss and more traffic interfaces per VQE-S using the following commands:

```
router ospf process-id
maximum-paths maximum-paths
```

- **Directly connected VQE-S**—VQE-S must be directly connected to the edge router on all VQE-S traffic or VQE-S services 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 a Separate OSPF Area” section on page 45](#).

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

When channels are configured with a channel-provisioning tool such as VCPT, it is required that you specify a unique feedback target (FBT) address for each channel. If static routes are used for VQE-S traffic (ingest and services) or VQE-S services 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 10.2.9.2
ip route 8.86.1.0 255.255.255.0 10.2.10.2
ip route 8.86.1.0 255.255.255.0 10.2.11.2
ip route 8.86.1.0 255.255.255.0 10.2.12.2
```

For the preceding configuration example, the IP addresses 10.2.9.2, 10.2.10.2, 10.2.11.2, and 10.2.12.2 have been assigned to the Ethernet interfaces on the VQE-S host. See [Figure D-3](#). These Ethernet interfaces are used for VQE-S traffic, including Unicast Retransmission and RCC traffic.



# CHAPTER 3

## Using the VQE Channel Provisioning Tool

This chapter describes how to use Cisco VQE Channel Provisioning Tool (VCPT). [Table 3-1](#) lists the tasks you perform with the VCPT. 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	<a href="#">Logging into VCPT, page 3-2</a>
2. Create a new VCPT configuration file	<a href="#">Working with VCPT Configuration Files, page 3-3</a>
3. Provision VQE channels	<a href="#">Provisioning VQE Channels, page 3-7</a>
4. Create VQE Servers (VQE-S), VQE Client Configuration Delivery Servers (VCDSs), or Remote Servers	<a href="#">Defining VQE-Ss, VCDSs, or Remote Servers, page 3-14</a>
5. Specify channel associations for the VQE-Ss, VCDSs, or Remote Servers	<a href="#">Defining Channel Associations, page 3-18</a>
6. Send the channel information file to the VQE-Ss, VCDSs, or Remote Servers	<a href="#">Working with VCPT Configuration Files, page 3-3</a>

## Logging into VCPT

Before logging into the VCPT, you need a valid UNIX username and password on the Cisco CDE110 hosting the 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.

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

To log in to a VCPT, follow these steps:

- Step 1** Point your web browser to the Cisco CDE110 that hosts the 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.

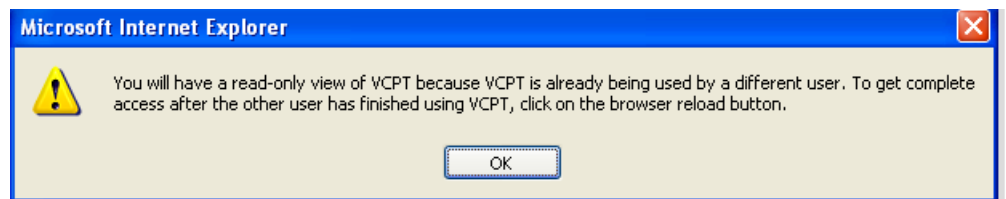
- Step 2** Enter a UNIX username and password.

- Step 3** Click **OK**.

If the username and password are valid, the VCPT main window is displayed.

If you log in to the VCPT when another person is using the same VCPT, the message shown in [Figure 3-1](#) is displayed and your access to the 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 the 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 the 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.

File management tasks for the VCPT are the responsibility of the VCPT user. The directories that the VCPT uses for its data files are as follows:

- VCPT configuration files are stored in the `/etc/opt/vcpt/data` directory.
- SDP-formatted files that the VCPT creates for each valid VCPT configuration are stored in the `/etc/opt/vcpt/data/sdp` directory.

If the `/etc/opt/vcpt/data` or `/etc/opt/vcpt/data/sdp` directory is deleted accidentally and does not exist at startup, VCPT fails to initialize. The missing directory must be recreated. For information on the remedy procedure, see the “[VCPT Fails to Initialize](#)” section on page 6-12.



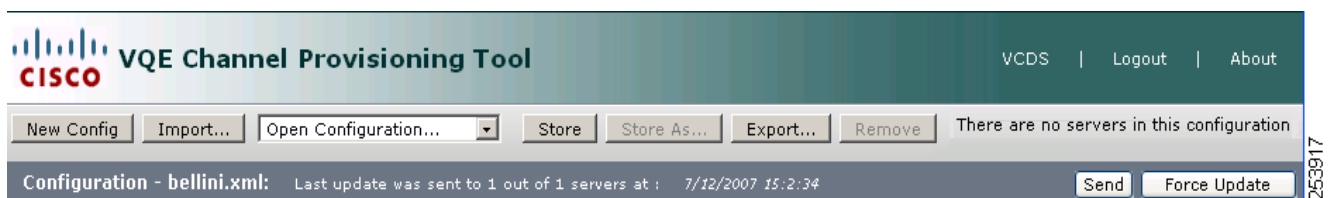
**Caution**

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, the VCPT sends the channel information in Session Description Protocol (SDP) format to the set of VQE-Ss and VCDSs. As an alternative to the VCDS, the channel information may be sent in SDP format to one or more user-specified remote servers using a password-less secure copy (SCP) mechanism.

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 Configuration-File Operations](#), page 3-4
- [Sending or Pushing Channel Information to Servers](#), page 3-5
- [Sending Channel Information to a Subset of Servers](#), page 3-7

## Performing 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**.
- **Import**—Clears the current configuration (if any), and imports a configuration from a file that you specify that is located on the VQE Tools server. The configuration file is in either XML (Extensible Markup Language) or CSV (text-based, comma-separated values) format.
- **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.
- **Export**—Exports the current configuration to a file in the format you specify. The format is either XML or CSV.
- **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.

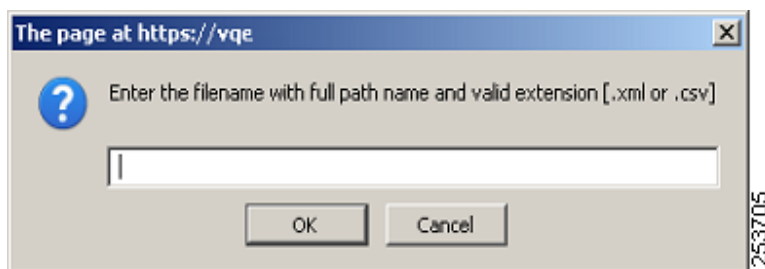
## Importing a Configuration

To create a VQE channel configuration in the VCPT without manually entering the data, you can import the required information from an external file. The file can be located in any directory on the VQE Tools server as long as the file has the correct permissions. However, the file must be in a valid format. For information on VCPT configuration file formats, see [Appendix I, “VCPT Configuration Files.”](#)

To import a configuration, do the following:

- 
- Step 1** Click **Import**.
- Step 2** The Import dialog box, shown in [Figure 3-3](#), is displayed.

**Figure 3-3** Import dialog



- Step 3** Enter the full path name and extension (xml or csv) of the configuration file, and click **OK**.

The VCPT clears the current configuration (if any) and displays the contents of the imported file. If the file is in XML format, the VCPT validates the file against the XML schema, *vcpt\_doc.xsd*, prior to importing.

## Exporting a Configuration

A VQE channel configuration can be exported to an external file you specify. The file can be in any directory on the VQE Tools server as long as the file has the correct permissions. Currently only two formats are supported by the VCPT; XML and CSV format. For information on the VCPT configuration file formats, see [Appendix I, “VCPT Configuration Files.”](#)

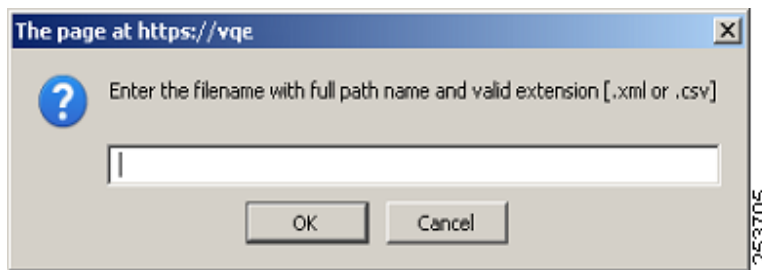
To export a VCPT configuration, do the following:

---

**Step 1** Click **Export**.

The Export dialog box, shown in [Figure 3-4](#), is displayed.

**Figure 3-4** Export dialog



**Step 2** Enter a full path, file name and file extension (xml or csv), and click **OK**.

The VCPT exports the VCPT configuration to this file.

## Sending or Pushing Channel Information to Servers

The VCPT buttons used to send or push channel information to VQE-Ss , VCDSs, or remote 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-Ss, VCDSs, or remote 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**

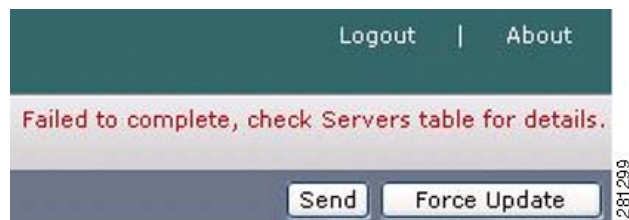
Using the Send button causes temporary disruption to Unicast Retransmission services for modified channels while the VQE-S cache used for packet retransmission on the modified channels is flushed.

The channel information to send is based on the channel associations that have been defined for the VQE-Ss, VCDSs, or remote 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, the VCPT displays the following:

- 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).
- Status message is displayed: either “Send Complete” or, if the send operation fails, the message text shown in [Figure 3-5](#).
- 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 17.

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 3-5** 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 (RCC) 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-Ss and VCDSs.

- Configuration file changes where you are reverting to an old version of the configuration file (older than 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-Ss, VCDSs, and remote 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-Ss, VCDSs, and remote servers.
- 

## Provisioning VQE Channels

In the Cisco VCPT, 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-S is determined by the ingest capacity of the CDE110 server. For VQE-S performance information, see [Appendix H, “VQE Server Performance and Scaling Limits”](#)

When you click the Channels tab, VCPT displays summary information on all channels that have been created. An incomplete channel is displayed in red. The Reduced Size RTCP Reports Enabled column show in [Figure 3-6](#) is available starting with Cisco VQE Release 3.5.5.

**Figure 3-6 Channels Summary**

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

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 that have been configured for the channel. [Table 3-2](#) shows the Error Repair Options column.

**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-S configures on its host Cisco CDE110 based on the channel information that is sent to it by the 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-S's CDE110 interface that is identified by the address). The use of anycast addresses to identify feedback targets is useful for VQE-S 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 the [“Enabling OSPF Routing for VQE-S Traffic or VQE-S Services Traffic”](#) section on page D-10.

To add a channel, follow these steps:

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

The New Channel dialog box, shown in [Figure 3-7](#), is displayed.

**Figure 3-7** New Channel Dialog Box

The screenshot shows the 'New Channel' dialog box with the following fields and options:

- Channel Details:** Channel Name: Channel 16; Feedback Target IP: 10.1.8.3
- Original Stream:** Multicast IP: 224.1.1.14; Source IP: 10.10.10.7; RTP Port: 1031; RTCP Port: 1032; Bit Rate: 4000 (Kbps)
- Unicast Retransmission Stream:** Source IP: 10.1.8.3; RTP Port: 50016; RTCP Port: 50017
- FEC 1 Stream:** Source IP: 10.10.10.7; Multicast IP: 224.1.1.14; RTP Port: 1033
- FEC 2 Stream:** Source IP: 10.10.10.7; Multicast IP: 224.1.1.14; RTP Port: 1035
- Channel Features:**
  - Enable RTCP
    - Enable Error Repair
    - Enable Rapid Channel Change
    - Enable Extended RTCP Reports
    - Enable Reduced Size RTCP
  - Enable FEC 1 Stream
  - Enable FEC 2 Stream

Buttons: Create, Cancel

**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	Unique anycast IP address on the VQE-Ss that provide services for this channel. Using the Feedback Target IP address that is sent to it by the VCPT in the channel information, the VQE-S automatically configures the specified address on one of its Cisco CDE110 interfaces.
<b>Channel Features</b>	
Enable RTCP	RTCP must be enabled to use Error Repair (Unicast Retransmission), RCC, 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 RCC, and Enable RTCP Extended Reports check boxes are grayed 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 RCC.
Enable Extended RTCP Reports	Check to enable RTCP Extended Reports.
Enable Reduced Size RTCP	Check to enable sending RTCP NACK compound packets to the VQE-S without Receiver Reports (RRs).  This option is available in Cisco VQE Release 3.5.5 and later releases.
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.
<b>Original Stream</b>	
Multicast IP	Multicast IP address for the original source stream of the channel. 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 original source stream of the channel.
RTCP Port	The RTCP port number of the original source stream of the channel. By default, RTCP Port is the (RTP/UDP) port number plus one.
Source IP	IP address of the original source stream of the channel.  <b>Note</b> A channel may be defined with a Source IP address of 0.0.0.0 for the Original Stream. When the channel Source IP address is 0.0.0.0 for the Original Stream, the SDP entry for this channel does not include the source-filter line in the original stream section that would be used to perform a Source Specific Multicast (SSM) join. In this case, the VQE-S and VQE-C does not perform a SSM join.

Table 3-3 VQE Channel Details (continued)

VCPT Field	Description
Bit Rate	Bit rate of the original source stream of the channel in kilobits per second. This parameter defines how many packets the VQE-S accepts and sends for this multicast stream.  <b>Note</b> The specified bit rate should be equal to the primary stream bandwidth but <i>should not</i> include bandwidth used for FEC.
<b>Unicast Retransmission Stream</b>	
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.
RTCP Port	RTCP port number of the unicast retransmission stream. By default, RTCP Port is a valid port number.
<b>FEC 1 Stream and FEC 2 Stream</b>	
Source IP	IP address of the source stream of the channel. By default, this is the IP address of the Source IP specified for the Original Stream.  <b>Note</b> A channel may be defined with a Source IP address of 0.0.0.0 for the FEC Stream. When the channel Source IP address is 0.0.0.0 for the FEC Stream, the SDP entry for this channel does not include the source-filter line in the FEC section that would be used to perform a SSM <sup>1</sup> join. In this case, the VQE-S and VQE-C does not perform a SSM join.
Multicast IP	IP address of the multicast stream of the channel. 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.

1. SSM = source specific multicast.

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

- 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.
- 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 is marked incomplete.

- Channel configuration file with an incomplete channel definition cannot be sent to VQE-Ss, remote servers, or VCDSs.

**Port Usage Recommendations.** When the STUN Server is enabled on a VQE-S (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 (STBs) 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, shown in [Figure 3-8](#), is displayed. The Reduced Size RTCP Reports Enabled column show in [Figure 3-8](#) is available starting with Cisco VQE Release 3.5.5.

**Figure 3-8 Details Dialog Box**

**Details**

**Channel Details**  
 Channel Name:  Feedback Target IP:

**Original Stream**  
 Multicast IP:  Source IP:   
 RTP Port:  Bit Rate:  (Kbps)  
 RTCP Port:

**Unicast Retransmission Stream**  
 Source IP:   
 RTP Port:   
 RTCP Port:

**FEC 1 Stream**  
 Source IP:   
 Multicast IP:   
 RTP Port:

**FEC 2 Stream**  
 Source IP:   
 Multicast IP:   
 RTP Port:

**Channel Features**  
 Enable RTCP  
 Enable Error Repair  
 Enable Rapid Channel Change  
 Enable Extended RTCP Reports  
 Enable Reduced Size RTCP  
 Enable FEC 1 Stream  
 Enable FEC 2 Stream

254375

- 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.
- 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-Ss, VCDSs, or Remote Servers

The Cisco VCPT requires that you provide information on each VQE-S, each VCDS, and each remote server that receives channel configuration information from the VCPT.

If you choose to send channel information to a remote server, you must install a SSH public key in .ssh directory of the authorized user on the remote server. For more information on generating the SSH public key, see the “[Setting-up a SSH Certificate on a Remote Server](#)” section on page 19.



### Note

The system integrator must ensure that the generated public key is stored in the authorized\_keys file in .ssh directory of the authorized user for channel configuration files to be transferred successfully to the remote server.

In the VCPT, 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, the VCPT displays summary information, shown in [Figure 3-9](#), on all servers that have been created.

**Figure 3-9 Servers Summary**

Name	Management IP Address	Role	Number of Channels Currently Associated	Status of Last Send	Last Successful Sent Time
jupiter	10.86.21.17	VQE-S	10	Success - Received 2 channels; 0 channels deleted; 0 channels restarted; and 0 new channels created	09/25/2008 14:25:01
server 1	3.4.6.6	VQE-S	0	Failed - The host did not accept the connection within timeout of 3000 ms	09/25/2008 14:16:15

Number of Servers: 3

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 row representing a server 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.

- **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.

- 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 is either 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-S 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-S or the current version of the VCPT server) 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 - <i>additional_information</i>	Send operation succeeded. The <i>additional_information</i> provides details on the send operation.
Failed - <i>additional_information</i>	Send operation failed. The <i>additional_information</i> provides details on the reasons for the failure.
Failed - Network Error	VCPT did not receive any error message back from the VQE-S, the VCDS, or the remote server.
Failed - Connection refused	See the “ <a href="#">Channel-Provisioning Server Cannot Send Channel Information to VQE-S: Trusted Provisioning Client Problem</a> ” section on page 6-13.
Failed - Unable to find valid certification path to requested target	See the “ <a href="#">Channel-Provisioning Server Cannot Send Channel Information to VQE-S: SSL Certificates Problems</a> ” section on page 6-13.
Failed - Unable to connect with Server	See the “ <a href="#">Unable to Connect Error When VCPT Tries to Send Channel Information</a> ” section on page 6-14.
Failed - Security Exception	Exception occurred while VCPT was authenticating the server SSL certificate.
Failed - Invalid EMS Address	Incorrect server URL format
Failed - VCPT Server Error	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	Channel configuration file could not be written to disk on the VQE-S, the VCDS or the remote server host.

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

Message	Explanation
Failed - File failed to open	VQE-S, the VCDS or the remote server could not open the channel configuration file.
Failed - Tomcat Service Unavailable	Tomcat application server has failed on the VCPT host.
Failed - Unable to store the SDP data on VCPT Server	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.

- 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:
  - Server is new and channel information has never been successfully sent to it
  - 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, shown in [Figure 3-10](#), is displayed.

**Figure 3-10** New Server Dialog Box

**New Server**

**Server Details**

Server Name:

Management IP:  .  .  .

Role:

Transfer Port:

Username:

Remote Path and Filename:

**Server Wide Channel Configuration**

RTCP Interval:  secs

Maximum Receivers:

Warning! Missing data in the fields - Management IP.

206591

- 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-S and VCDS Information**

VCPT Field	Description
<b>Server Details</b>	
Server Name	String having 1 to 40 alphanumeric characters.
Management IP	One of the following: <ul style="list-style-type: none"> <li>IP address of an Ethernet interface on the Cisco CDE110 server</li> <li>IP address of an Ethernet interface on the remote server.</li> </ul>
Role	One of the following: <ul style="list-style-type: none"> <li>VQE-S</li> <li>VCDS</li> <li>SCP (Secure Copy Protocol)—If chosen, VCPT pushes configuration data to a specified remote server using password-less SCP.</li> </ul>
Transfer Port	SCP port number on the remote server. If role type is not SCP, the Transfer Port field is grayed out.
Username	Username of the person who has the authority to access the path on the remote server specified in the Remote Path and Filename field. If role type is not SCP, the Username field is grayed out.
Remote Path and Filename	Absolute path to the channel configuration file on the remote server and its filename. If role type is not SCP, the Remote Path and Filename field is grayed out.
<b>Server Wide Channel Configuration</b>	
Maximum Receivers	Total number of VQE Clients (VQE-Cs) that are expected to tune in this channel. This value is used by the VQE-S to calculate how often the VQE-S sends an RTCP report to the video source for this channel.
RTCP Interval	Defines how often VQE-Cs send an RTCP report. By default, RTCP Interval is 5 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:

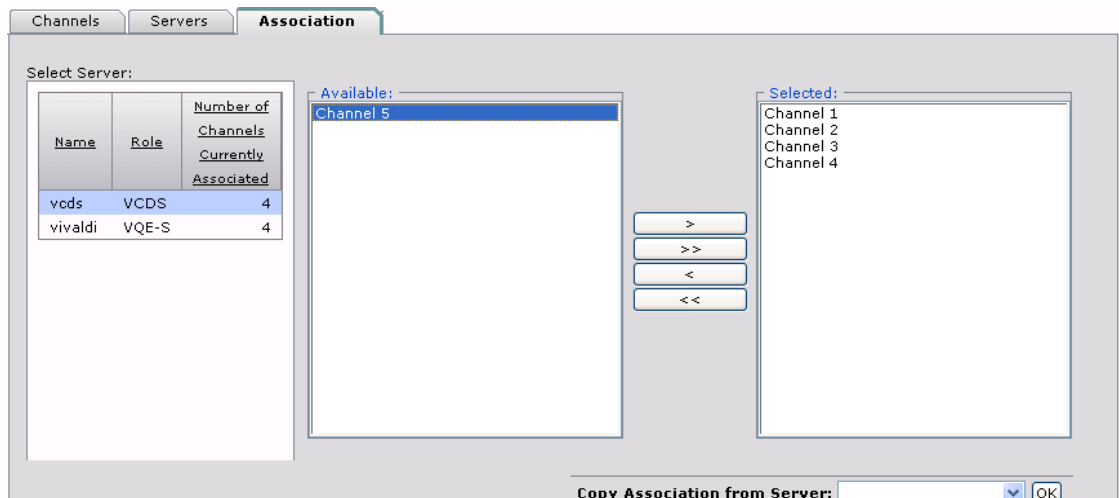
- Step 1** On the Servers tab, click the server you want to delete.
- Step 2** Click **Delete**.
- A dialog box asking if you want to delete the server is displayed.
- Step 3** Do one of the following:
- Click **Delete** to delete the server.
  - Click **Cancel** to close the server dialog box without 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-Ss, VCDSs, and Remote Servers have been defined, you associate a set of channels with the servers. When the channel information file is sent to the VQE-Ss, VCDSs or Remote Servers, only the channels associated with the server are included in the file.

In the VCPT, use the Association tab, shown in [Figure 3-11](#), to associate servers with channels or copy an existing channel association.

**Figure 3-11 Association Tab**



370171

The following sections explain how to associate channels with servers:

- [Defining Channel Associations for a Server, page 3-19](#)
- [Copying Channel Associations from Another Server, page 3-19](#)

## 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.
- The 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.
- The 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.
- 

## Setting-up a SSH Certificate on a Remote Server

If you choose to export channel configuration data to a remote provisioning server, a secure shell (SSH) certificate should be generated on the VQE Tools server and its public key deployed on the remote server to allow VCPT to securely send encrypted channel configuration files to the remote server. The **scpkey** command is available on the VQE Tools server to assist in generating the SSH public key file. The command also uses a secure copy mechanism to deliver the public key of SSH certificate to the remote server. The system integrator must supply a password for the authorized user when generating the certificates so that VCPT can later send data to the remote server without being prompted to supply a password.

On the VQE Tools server, the **scpkey** executable is located at `/opt/vqes/bin/scpkey`. To have the operating system find the **scpkey** executable, you must set the PATH environment variable to include the location of the `/opt/vqes/bin` directory, or use the full path to **scpkey** when executing the command.

**Note**


---

You must log in as root to execute the **scpkey** command.

---

To generate a SSH public key, follow these steps:

---

**Step 1** From the command prompt, issue the following command:

```
[root@system ~]# scpkey
```

```
Welcome to the SCP key generation and transfer utility.
```

```
Checking for existing SCP key data...
```

```
Generating new keys via Linux ssh-keygen tool...
spawn ssh-keygen -t dsa
Generating public/private dsa key pair
Enter file in which to save the key (/root/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
f9:2c:89:5a:bf:22:1c:20:b8:08:05:3c:fc:d1:a9:9f root@system
```

```
SCP key generation successfully completed.
```

The **scpkey** command creates a new SSH public key. The key file is named `id_dsa.pub` and is located in `/root/.ssh/`.

**Step 2** The **scpkey** command prompts you to automatically transfer the file to the remote server or to exit the command and manually copy the public key to the remote server at a later time. If you wish to automatically transfer the SSH public key file to the remote server, do the following:

- a. When prompted to transfer the file to the remote server using the secure copy protocol, enter 'y' at the prompt below.

```
Do you wish to SCP transfer the key file to a remote system (y/n)? y
```

```
Gathering info for SCP transfer...
```

- b. Enter the IP address of the remote server at the prompt below.

```
Enter IP address of remote system: 10.22.21.101
```

- c. Enter the username of the person who is authorized to access the channel configuration files on the remote server at the prompt below:

```
Enter remote system username: dmrp
```

- d. Enter a password for the authorized person at the prompt below:

```
Enter remote system username password:
```

- e. By default, the SSH public key file is copied to the `.ssh/authorized_keys` file relative to the authorized users home directory on the remote server. Press Enter to select the default path or enter the absolute path of the SSH key file on the remote server.

```
By default, key file will be copied to .ssh/authorized_keys file relative to
remote users home directory, however you may specify a different fully
qualified path/filename here if desired.
```

```
Enter optional remote path/file (<ENTER> for default file):
```

```
Transferring file, no further user input required...
```

```
spawn scp /root/.ssh/id_dsa.pub test@10.86.21.101:~/.ssh/authorized_keys
```

- Step 3** If you wish to manually transfer the SSH public key file to the remote server, copy the file named `id_dsa.pub` located in `/root/.ssh/` on the VQE Tools server to the `~/.ssh/authorized_keys` file relative to the authorized users home directory on the remote server.
-





# CHAPTER 4

## Using the VQE-S AMT

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

**Table 4-1** VQE-S AMT Tasks

VQE-S AMT Task	Section Where Described
Log in to the VQE-S AMT	<a href="#">Logging into and Navigating in the VQE-S AMT, page 4-2</a>
Monitor the health of the VQE-S processes	<a href="#">Monitoring the Health of the VQE-S Processes, page 4-4</a>
View channel configuration details, status, and statistics	<a href="#">Viewing Channel Configuration and Status, page 4-7</a>
Monitor statistics for Unicast Retransmission and RCC <sup>1</sup>	<a href="#">Monitoring Unicast Retransmission and RCC, page 4-16</a>
View configuration details, status, and statistics for CDE110 Ethernet interfaces	<a href="#">Monitoring Interfaces, page 4-26</a>
View configuration details, status, and statistics for the VQE-S RTCP <sup>2</sup> Exporter	<a href="#">Monitoring RTCP Exporter, page 4-28</a>
View STUN Server statistics	<a href="#">Monitoring the STUN Server, page 4-30</a>
Reset VQE-S counters	<a href="#">Resetting VQE-S Counters, page 4-31</a>
Restore VQE-S counters	<a href="#">Restoring VQE-S Counters, page 4-32</a>
Change VQE-S logging levels	<a href="#">Change VQE-S Logging, page 4-33</a>
Change VQE-S debugging levels	<a href="#">Change VQE-S Debugging, page 4-33</a>

1. RCC = rapid channel change.

2. RTCP = Real-Time Transport Control Protocol



**Note**

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

# Logging into and Navigating in the VQE-S AMT

Before logging into the VQE-S AMT, you need a valid Linux username and password on the Cisco CDE110 hosting the VQE-S 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.

The 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 the VQE-S AMT is 1024 x 768 pixels.

The 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 the VQE-S AMT. Adobe Flash Player is free and can be found at this URL:

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

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

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

`https://ip_address`

or

`https://fully_qualified_domain_name`

The VQE-S AMT login dialog box is displayed.

- Step 2** Enter a Linux username and password.

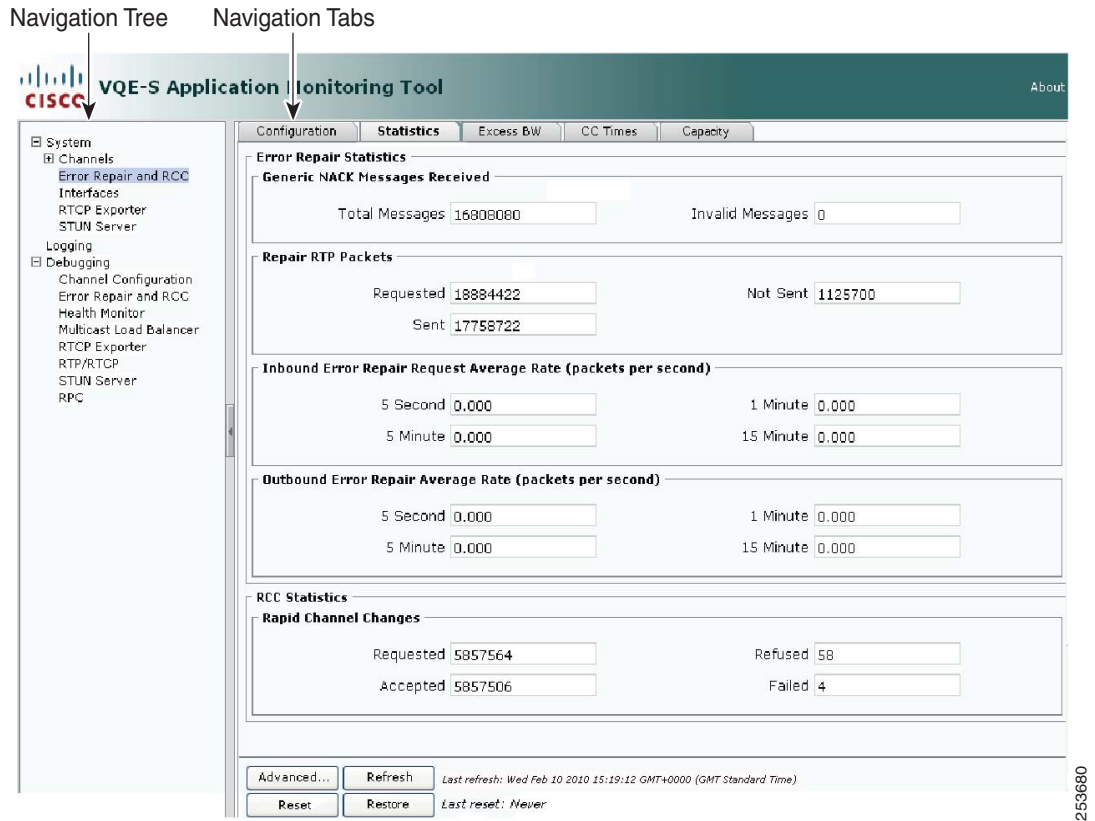
- Step 3** Click **OK**.

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**



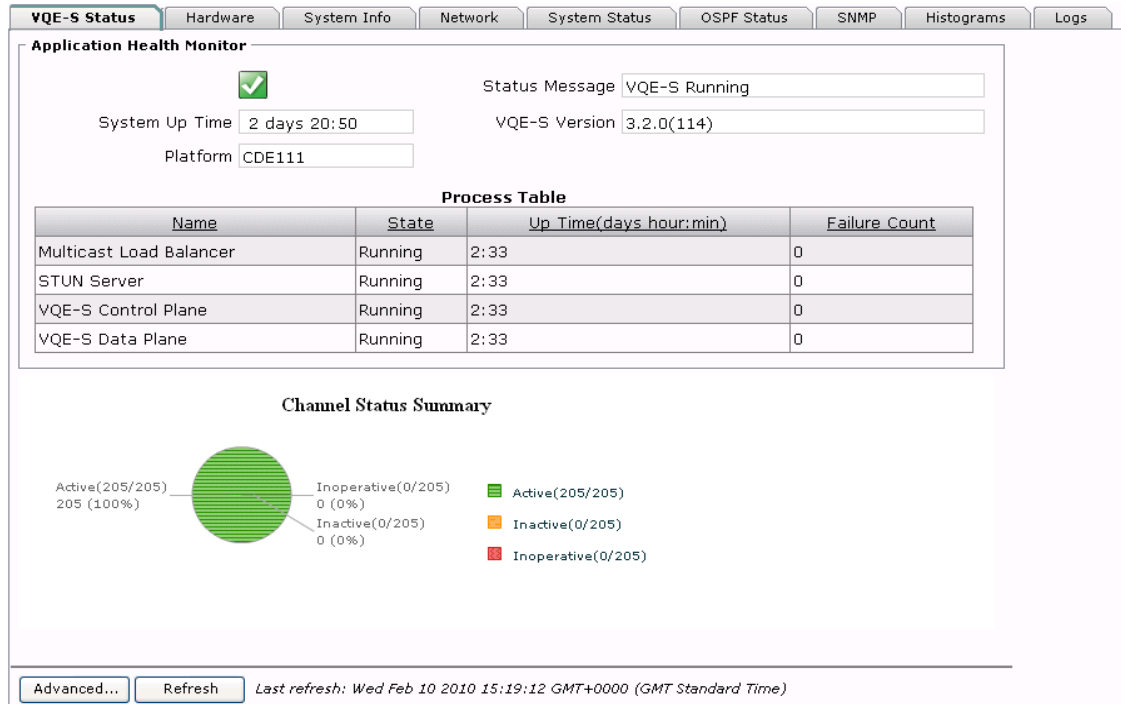
The VQE-S AMT (see [Figure 4-1](#)) provides these controls and buttons for navigating and displaying VQE data:

- **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.
  - Parent node in the tree (such as Channels) usually provides summary data.
  - 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. The VQE-S AMT statistical data are not automatically updated when the 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.
- **Reset**—Click to globally reset counter values displayed on the VQE-S AMT to zero. The results of this action are visible to all AMT users, even those in separate AMT browser sessions. Only a subset of counters can have their display value reset. Resetting the display of counter values is provided for debugging purposes. For example, resetting a counter after you have fixed an issue could allow you to easily see that an error counter no longer occurs. The last reset date-and-time information to the right of the **Reset** button indicates when the last manual reset of counters occurred, and displays *never* if a reset has not occurred.
- **Restore**—Click to globally restore counters to their true value since the last start of the VQE-S service.

## Monitoring the Health of the VQE-S Processes

When you click the **System** node in the navigation tree and the **VQE-S Status** tab, the VQE-S AMT displays the VQE-S Status window (see [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 check mark indicates that the VQE-S system is running and is 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 the 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 the VQE-S Process Monitor. The VQE-S 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 eight other tabs. Table 4-2 lists the information that is available from each tab accessible from the System node.

**Table 4-2 System Information**

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 the 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 <b>iptables</b> information (trusted channel-provisioning servers).
Network	Output from the <b>ifconfig</b> and <b>ip addr show lo</b> commands. <ul style="list-style-type: none"> <li>• Configuration information displayed by <b>ifconfig</b> is for the four CDE110 Ethernet interfaces and the CDE110 loopback addresses.</li> <li>• Loopback addresses displayed by <b>ip addr show lo</b> are the feedback target addresses for the configured channels.</li> </ul>
System Status	Detailed information on host uptime, currently running processes, and file system disk space.
OSPF Status	Output from several commands that show OSPF information, including status, neighbors, interfaces, database, and routes.
SNMP	SNMP <sup>1</sup> information on the VQE-S host taken from the <code>snmpd.conf</code> file.
Histograms	STB IGMP <sup>2</sup> latency data is displayed in graphs and tables.
Logs	Most recent 300 lines from the following VQE-related log files are displayed: <ul style="list-style-type: none"> <li>• VQE-S log (<code>/var/log/vqe/vqe.log</code>)</li> <li>• System messages log (<code>/var/log/messages</code>)</li> <li>• HTTPD error log (<code>/var/log/httpd/error_log</code>)</li> <li>• SSL error log (<code>/var/log/httpd/ssl_error_log</code>)</li> <li>• Tomcat log (<code>/usr/share/tomcat5/logs/catalina.out</code>)</li> </ul>

1. SNMP = simple network management protocol.

2. IGMP = internet group management protocol.

## Viewing Channel Configuration and Status

When you click the **Channels** node in the navigation tree, the VQE-S AMT displays the Channel Lineups window (see [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 a column heading to reorder the channels in the list. For example, clicking **Feedback Target** orders the entries by feedback target: the combination of an 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.
- Click the **Re-Activate** button to cause the 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 the 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](#).

- Status—Indicates channel status as follows:
  - Green with a checkmark—Channel is active. The VQE-S is receiving the multicast stream.
  - Yellow with exclamation mark (!)—Channel is inactive. The channel is successfully initialized, but the 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-Cs that are currently receiving this multicast stream.

## Viewing Channel Configuration

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

**Figure 4-4** Channel Configuration Window

The screenshot shows the Channel Configuration window with the following settings:

- Channel Configuration:**
  - Channel Name: Channel 229.1.1.1
  - Mode: Lookaside
  - Feedback Target Address: 11.112.1.1
  - Error Repair: true
  - Rapid Channel Change: true
  - Post Repair Loss RLE Enabled: true
- Original Source Stream:**
  - Multicast IP Address: 229.1.1.1
  - Port: 53170
  - Protocol: RTP
  - RTCP Port: 53171
  - IP Source Filter: 9.3.13.2
  - Bit Rate(Kbps): 4000
  - RTCP XR Enabled: true
  - Reduced size RTCP Enabled: true
- Unicast Retransmission Stream:**
  - Retransmission IP Address: 11.112.1.1
  - RTP Port: 10002
  - RTCP Port: 10003
  - RTCP XR Enabled: true

At the bottom, there is a Refresh button and a timestamp: Last refresh: Wed Feb 10 2010 15:19:12 GMT+0000 (GMT Standard Time).

[Table 4-3](#) lists the information presented in the Channel Configuration window.

**Table 4-3** Channel Configuration

Field	Description
<b>Channel Configuration</b>	
Channel Name	Name of the channel.
Feedback Target Address	Feedback Target IP address assigned on the VQE-S host.
RCC	<ul style="list-style-type: none"> <li>true—RCC is enabled for this channel.</li> <li>false—RCC is not enabled for this channel.</li> </ul>
Mode	Currently only Lookaside mode is supported.
Error Repair	<ul style="list-style-type: none"> <li>true—Unicast Retransmission is enabled for this channel.</li> <li>false—Unicast Retransmission is not enabled for this channel.</li> </ul>
Post Repair Loss RLE Enabled	<ul style="list-style-type: none"> <li>true—RTCP Extended Reports includes the Loss RLE (run-length encoded) report block type.</li> <li>false—RTCP Extended Reports does not include the Loss RLE report block type.</li> </ul>
<b>Original Source Stream</b>	

**Table 4-3 Channel Configuration (continued)**

Field	Description
Multicast IP Address	Multicast IP address for the channel's original source stream.
Protocol	Currently only RTP <sup>1</sup> is supported.
IP Source Filter	Source IP address of the channel's original source stream.
RTCP XR Enabled	<ul style="list-style-type: none"> <li>• true—RTCP Extended Reports are enabled.</li> <li>• false—RTCP Extended Reports are not enabled.</li> </ul>
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.
Reduced size RTCP Enabled	<ul style="list-style-type: none"> <li>• true—Sending reduced-size RTCP NACK compound packets is enabled.</li> <li>• false—Sending reduced-size RTCP NACK compound packets is not enabled.</li> </ul> <p>This field was introduced in Cisco VQE Release 3.5.5.</p>
<b>Unicast Retransmission Stream</b>	
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.

1. RTP = Real-Time Transport Protocol

## Viewing Channel Statistics

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

**Figure 4-5** Channel Statistics Window

The screenshot shows the 'Status/Statistics' tab of the Channel Statistics window. It contains several sections of data:

- Configuration:** Status: active
- Stream Performance:** Average Stream Rate (Mbps): 3.81, Received Packets: 2339128, Received Bytes: 3153144544, Lost RTP Packets: 634
- Error Repair Statistics:**
  - Generic NACK Messages Received:** Total Messages: 12544, Invalid Messages: 0
  - Repair Packets:** Requested: 13941, Sent: 13935, Not Sent: 6
  - Error Repair Average Rate (packets per second):** 5 Second: 4.600, 5 Minute: 3.457, 1 Minute: 3.425, 15 Minute: 3.460
- RCC Statistics:**
  - Rapid Channel Changes:** Requested: 1, Accepted: 1, Refused: 0, Failed: 0
- RTCP Packets:** Received: 13053, Sent Downstream: 286, Sent Upstream: 254, Reduced Size RTCP Received: 54

At the bottom, there are buttons for 'Advanced...' and 'Refresh', and a timestamp: 'Last refresh: Wed Feb 10 2010 15:19:12 GMT+0000 (GMT Standard Time)'. A vertical ID number '254373' is on the right side.

[Table 4-4](#) lists the information presented in the Channel Statistics window.

**Table 4-4** Channel Statistics

Field	Description
<b>Channel Input Stream</b>	
Status	<ul style="list-style-type: none"> <li>active—VQE-S is receiving the multicast stream.</li> <li>inactive—Channel is successfully initialized, but the VQE-S is not receiving the multicast stream.</li> <li>inoperative—Channel is not operational. For example, it is not configured correctly.</li> </ul>

**Table 4-4 Channel Statistics (continued)**

Field	Description
Received Packets	Number of RTP packets received by the VQE-S for this multicast stream. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
Lost RTP Packets	Number of RTP packets sent but not received by the 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. After the channel has been initialized (typically less than a 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. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
Average Stream Rate (Mbps)	Average megabits per second received by the VQE-S for this multicast stream.
Received Bytes	Number of bytes received by the VQE-S for this multicast stream. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
<b>Error Repair Statistics—Generic NACK Messages Received</b>	
Total Messages	Number of NACK messages received by the VQE-S from VQE-C for this multicast stream. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
Invalid Messages	Number of invalid messages received by the VQE-S from VQE-C for this multicast stream. Invalid messages are received messages that, for example, cannot be parsed. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
<b>Repair Packets</b>	
Requested	Number of RTP packets VQE-Cs have requested for ER <sup>1</sup> for this multicast stream. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
Sent	Number of RTP packets sent by the VQE-S that have succeeded in repairing an error for this multicast stream. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .

Table 4-4 Channel Statistics (continued)

Field	Description
Not Sent	<p>Number of failed RTP packets that were not repaired by the VQE-S for this multicast stream. The VQE-S may not be able to send an ER packet for the following reasons:</p> <ul style="list-style-type: none"> <li>• Most likely cause is that the ER requests were bursty and exceeded the ER rate-policer limit at one point.</li> <li>• Requested RTP packets were not found in the VQE-S memory cache.</li> <li>• VQE-S failed to send the RTP packets because of a socket sendto() failure.</li> </ul> <p>This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters”</a> section on page 31.</p>
<b>Error Repair Average Rate (packets per second)</b>	
5 second, 5 minute, 1 minute, 15 minute	<p>The average number of packets per second that the VQE-S has sent to VQE-Cs to repair errors for this multicast stream for each time interval. Averages are calculated for ER each time interval over a period of time that is greater than the interval. For example, the 5 second calculation might be an average of 12 five-second intervals over a 1 minute period.</p>
<b>RCC Statistics—RCCs</b>	
Requested	<p>Number of RCC requested for this channel. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters”</a> section on page 31.</p>
Accepted	<p>Number of RCCs requested for this channel where the VQE-S has accepted the request and sent IPTV packets and other channel data to a VQE-C on the STB. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters”</a> section on page 31.</p>
Refused	<p>Number of RCCs requested for this channel where the VQE-S refused the request. For example, the VQE-S may refuse an RCC request for the following reasons:</p> <ul style="list-style-type: none"> <li>• If the VQE-S did not find an I-frame that is a suitable starting point for the RCC burst.</li> <li>• If the VQE-S exceeded the output interface bandwidth limit or CPU load limit.</li> <li>• If the CPU load limit is exceeded, the Advanced Channel Debug Stats counter “Refused RCC - no core resources on DP” is displayed when the limit is exceeded.</li> </ul> <p>The Refused RCC counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters”</a> section on page 31.</p>
Failed	<p>Number of RCCs that have failed. A VQE-C has made an RCC request, and the VQE-S has accepted the request and sent IPTV packets and other channel data to a VQE-C. 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. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters”</a> section on page 31.</p>
<b>RTCP Packets</b>	

**Table 4-4 Channel Statistics (continued)**

Field	Description
Received	Number of RTCP packets received by the VQE-S for this multicast stream. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
Sent Downstream	Number of RTCP packets that the VQE-S sent downstream for this multicast stream. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
Sent Upstream	Number of RTCP packets that the VQE-S sent upstream for this multicast stream. This counter is resettable. For information on resetting counters, see the <a href="#">“Resetting VQE-S Counters” section on page 31</a> .
Reduced Size RTCP Received	Number of reduced-size RTCP NACK compound packets sent for this multicast stream.  This field was introduced in Cisco VQE Release 3.5.5.

1. ER = error repair

## Viewing Channel Histograms

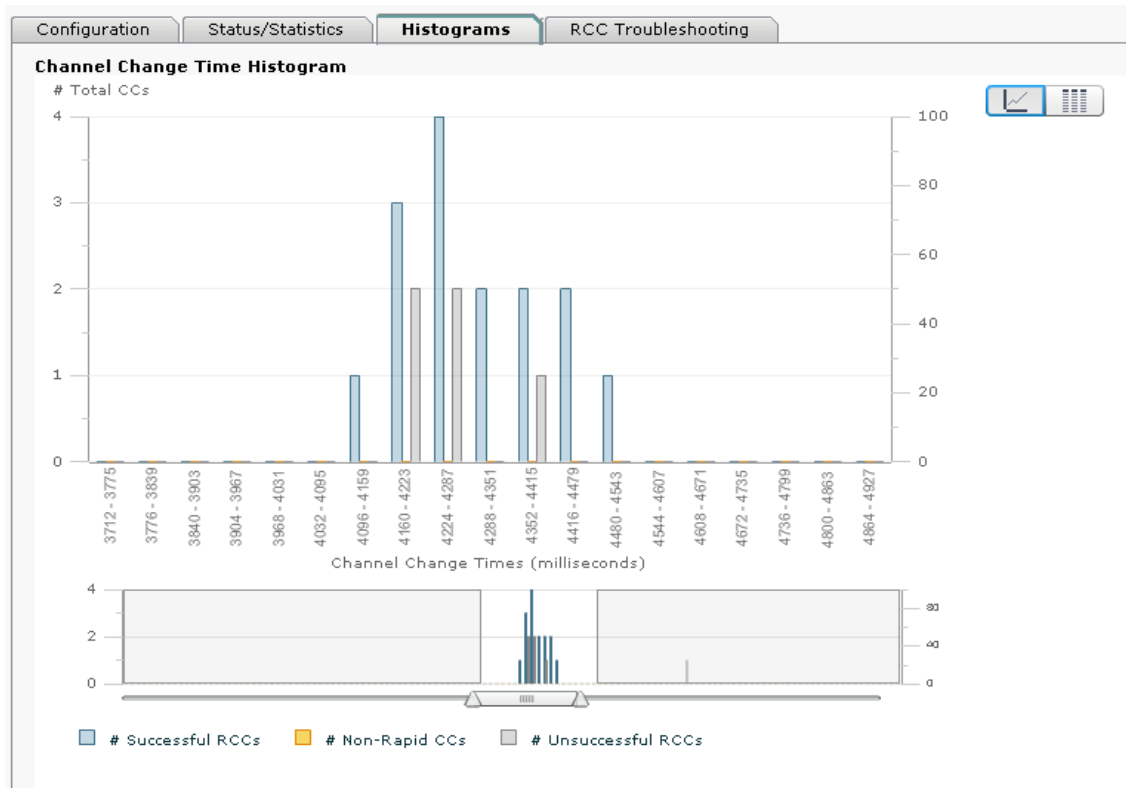
When you click a channel name in the navigation tree and then click the **Histograms** tab, the VQE-S AMT displays the Channel Histograms window (see [Figure 4-6](#)).



### Note

The VQE-S AMT Channel Channel Time histogram is only supported for VQE-C integrations that have implemented the RCC instrumentation as described in the VQE-C System Integration Guide.

**Figure 4-6** Channel Histograms Window



In the Channel Histogram window, the Channel Change Time histogram and table are displayed. The data displayed in the histogram and table include the following:

- Total number of channel changes (CCs) per time bucket.
- Number of successful RCCs for the selected time bucket.
- Number of unsuccessful RCCs for the selected time bucket.
- Number of non-rapid CCs (that is, channel changes where RCC was not requested) for the selected time bucket.

Each time bucket in this histogram represents a subset of channel change times from 0 to 7000 ms. Any channel change times that take longer than 7000 ms are collected in the uppermost bucket.

Move the slider below the histogram to change the way in which the histogram is displayed.

**Note**

The histogram is displayed and populated, regardless of whether RCC is enabled at the VQE-S. If no Multicast Acquisition (MA) XR report (a RTCP XR report block type) is received for a repair session, the histogram is unchanged.

## Viewing RCC Troubleshooting

When you click a channel name in the navigation tree and then click the **RCC Troubleshooting** tab, the VQE-S AMT displays the RCC Troubleshooting window (see [Figure 4-7](#)).

**Figure 4-7** *RCC Troubleshooting Window*

The screenshot shows the VQE-S Application Monitoring Tool interface. The 'RCC Troubleshooting' tab is selected. The main content area is titled 'Rapid Channel Change Status' and contains a table of 'Rapid Channel Change Errors'. The table has four columns: Client CNAME, Timestamp, Failure Reason, and Failure Detail. There are four rows of data, all showing 'No RCC: no RAP from stream' as the failure reason. A 'Refresh' button is located at the bottom left of the table area.

Client CNAME	Timestamp	Failure Reason	Failure Detail
00-14-f8-e2-d2-11	2009-07-21 11:17:25.957014	No RCC: no RAP from stream	There are no TSRAPs available for this stream.
00-14-f8-e2-d2-11	2009-07-21 11:14:09.599941	No RCC: no RAP from stream	There are no TSRAPs available for this stream.
00-14-f8-e2-d2-11	2009-07-21 11:10:49.403925	No RCC: no RAP from stream	There are no TSRAPs available for this stream.
00-14-f8-e2-d2-11	2009-07-21 11:07:25.486600	No RCC: no RAP from stream	There are no TSRAPs available for this stream.

The RCC Status window has the information listed in [Table 4-5](#).

**Table 4-5** *RCC Status*

Field	Description
Client CNAME	Identifier for the STB for which the RCC was requested but failed. Typically, the CNAME is the MAC address of the STB.
Timestamp	Time of the event. For example, 2009-07-21 08:42:03.05.
Failure Reason	Specific reason for the failure on either the VQE-S or the VQE-C.
Failure Detail	Additional information about the failure that may be used for debugging purposes.

The table presents the last 20 RCC failures on this channel. To reorder the list of RCC failures, click a column heading. For example, clicking **Timestamp** orders the RCC failures by date and time.

# Monitoring Unicast Retransmission and RCC


**Note**

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

Use the 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, the VQE-S AMT displays the Error Repair and RCC Configuration window (see [Figure 4-8](#)).

**Figure 4-8 Error Repair and RCC Configuration Window**

[Table 4-6](#) lists the information in the Error Repair and RCC Configuration window. Each of the parameters listed in the table can be configured with the VQE Configuration Management System. For information on configuring the VQE-S, see [Chapter 7, “Configuring VQE Server and VQE Tools.”](#)

**Table 4-6 Error Repair and RCC Configuration**

Field	Description
<b>Error Repair/RCC Configuration</b>	
RCC Mode	RCC mode can be aggressive or conservative. This value is configured with the <code>vqe.vqes.rcc_mode</code> parameter in VCDB. For information on this parameter, see <a href="#">Table A-3 on page A-6</a> .
IGMP Join Variability (msec)	Amount of variability (in milliseconds) between the fastest and slowest IGMP joins for RCC. This value is configured with the <code>vqe.vqes.igmp_join_variability</code> parameter. For information on this parameter, see <a href="#">Table A-3 on page A-6</a> .
Excess Bandwidth Fraction	Percent of channel bandwidth that is available on the access link for Unicast Retransmission and RCC. This value is configured with the <code>vqe.vqes.excess_bw_fraction</code> parameter. For information on this parameter, see <a href="#">Table A-4 on page A-9</a> .

**Table 4-6 Error Repair and RCC Configuration (continued)**

Field	Description
Maximum Interval between MPEG RAPs (msec)	Maximum time interval (in milliseconds) between MPEG RAPs <sup>1</sup> for the entire channel lineup. This value is configured with the <code>vqe.vqes.rap_interval</code> parameter in VCDB. For information on this parameter, see <a href="#">Table A-3 on page A-6</a> .
<b>Differentiated Services Code Point Configuration</b>	
RTCP Packets	DCSP value for RTCP packets that the VQE-S sends. This value is configured with the <code>vqe.vqes.rtcp_dscp</code> parameter in VCDB. For information on this parameter, see <a href="#">Table A-1 on page A-2</a> .
Retransmitted RTP Packets	DCSP value for RTP packets that the VQE-S sends. This value is configured with the <code>vqe.vqes.rtp_trans_dscp</code> parameter in VCDB. For information on this parameter, see <a href="#">Table A-1 on page A-2</a> .

1. RAP = random access point.

## Viewing Error Repair and RCC Statistics

When you click **Error Repair and RCC** in the navigation tree and click the **Statistics** tab, the VQE-S AMT displays the Error Repair and RCC Statistics tab (see [Figure 4-9](#)). The statistics are similar to the Error Repair and RCC statistics displayed for individual channels but are for all channels in the current channel lineup.

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

Figure 4-9 Error Repair and RCC Statistics Tab

Configuration	Statistics	Excess BW	CC Times	Capacity
<b>Error Repair Statistics</b>				
<b>Generic NACK Messages Received</b>				
Total Messages	464130	Invalid Messages	0	
<b>Repair RTP Packets</b>				
Requested	6310539	Not Sent	3530290	
Sent	2780249			
<b>Inbound Error Repair Request Average Rate (packets per second)</b>				
5 Second	0.000	1 Minute	0.000	
5 Minute	0.000	15 Minute	0.000	
<b>Outbound Error Repair Average Rate (packets per second)</b>				
5 Second	0.000	1 Minute	0.000	
5 Minute	0.000	15 Minute	0.000	
<b>RCC Statistics</b>				
<b>Rapid Channel Changes</b>				
Requested	1	Refused	0	
Accepted	1	Failed	0	
Advanced...	Refresh	Last refresh: Wed Feb 10 2010 15:19:12 GMT+0000 (GMT Standard Time)		
Reset	Restore	Last reset: Never		

253681

Table 4-7 lists the information in the Error Repair and RCC Statistics window.

Table 4-7 Error Repair and RCC Statistics

Field	Description
<b>Generic NACK Messages Received</b>	
Total Messages	Number of NACK messages received by this VQE-S from the VQE-Cs. This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.
Invalid Messages	Number of invalid messages received by this VQE-S from VQE-Cs. Invalid messages are received messages that, for example, cannot be parsed. This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.
<b>Repaired RTP Packets</b>	
Requested	Number of RTP packets VQE-Cs have requested for ER from this VQE-S. This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.

**Table 4-7 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. This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.
Not Sent	Number of failed RTP packets that were not repaired by the VQE-S. The VQE-S may not be able to send an ER packet for several reasons, among them: <ul style="list-style-type: none"> <li>• Most likely cause is that the ER requests were bursty and exceeded the ER rate-policer limit at one point.</li> <li>• Requested RTP packets were not found in the VQE-S memory cache.</li> <li>• VQE-S failed to send the RTP packets because of a socket sendto() failure.</li> </ul> The Repaired RTP Packets Not Sent counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.
<b>Inbound and Outbound Error Repair Average Rate (packets per second)</b>	
5 second, 5 minute, 1 minute, 15 minute	For each time period, the average number of packets per second that the VQE-S has received (inbound) or sent (outbound) to VQE-Cs to repair errors (Unicast Retransmission).
<b>RCC Statistics—Rapid Channel Changes</b>	
Requested	Number of RCCs requested for this channel. This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.
Accepted	Number of RCCs requested for this channel where the VQE-S has accepted the request and sent IPTV packets and other channel data to a VQE-C on the STB. This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.

Table 4-7 Error Repair and RCC Statistics (continued)

Field	Description
Refused	<p>Number of RCCs requested for this channel where the VQE-S has refused the request. For example, the VQE-S may refuse an RCC request for the following reasons:</p> <ul style="list-style-type: none"> <li>• VQE-S did not find an I-frame that is a suitable starting point for the RCC burst.</li> <li>• VQE-S exceeded the output interface bandwidth limit or CPU load limit.</li> <li>• CPU load limit is exceeded, the Advanced Channel Debug Stats counter “Refused RCC - no core resources on DP” shows when the limit is exceeded.</li> </ul> <p>This RCCs Refused counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.</p>
Failed	<p>Number of RCCs that have failed. A VQE-C has made an RCC request, and the VQE-S has accepted the request and sent IPTV packets and other channel data to a VQE-C 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.</p> <p>This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.</p>

## Viewing Excess Bandwidth

When you click **Error Repair and RCC** in the navigation tree and click the **Excess BW** tab, the VQE-S AMT displays the Excess BW window (see [Figure 4-10](#)).

**Figure 4-10** Excess BW Window



206594

If Error Repair or RCC is enabled and active, you can choose to display a client e-factor histogram or table by clicking the icons in the upper right corner of the window. Use the Select a client e-factor histogram drop-down menu to select Error Repair or RCC histograms.

An e-factor is an excess bandwidth fraction that determines the rate at which packets are sent during Error Repair and RCC. The data displayed in the histograms and tables include the following:

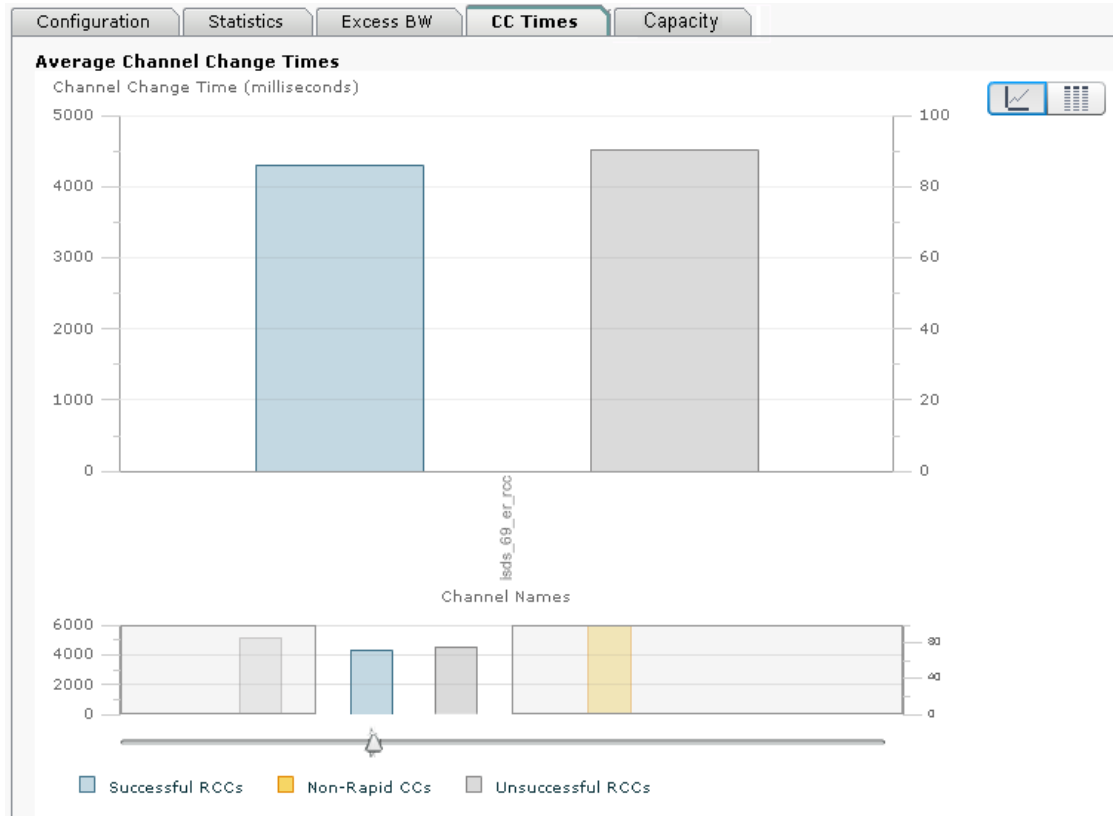
- E-factor count with the number of times a client e-factor has been calculated. This appears on the vertical axis in the histograms.
- E-factor distribution of the client e-factor percentages that have been used. This appears on the horizontal axis in the histograms. If the distribution is widely dispersed, there can be more than one grouping of percentages.

Move the slider below the histograms to change the way in which the histograms are displayed. The e-factor percentages cannot be negative values.

## Viewing Channel Change Times

When you click **Error Repair and RCC** in the navigation tree and click the **CC Times** tab, the VQE-S AMT displays the CC Times window (see [Figure 4-11](#)).

**Figure 4-11** Channel Change Times Window



In this window, the Average Channel Change Time histogram and table are displayed. The data displayed in the histogram and table includes the following:

- Average channel change time in milliseconds for each channel on the VQE-S for the following three categories:
  - Successful RCCs
  - Unsuccessful RCCs
  - Non-rapid CC (that is, channel changes where RCC was not requested).

The data displayed is based on the last 100 successful channel changes where RCC was enabled, the last 100 unsuccessful change changes where RCC was enabled, and the last 100 channel changes where RCC was disabled.

Move the slider below the histogram to change the way in which the histogram is displayed.

## Viewing Error Repair and RCC Capacity Statistics

When you click **Error Repair and RCC** in the navigation tree and click the **Capacity** tab, the VQE-S AMT displays the Error Repair and RCC Capacity tab (Figure 4-12). The VQE-S provides capacity statistics to indicate when Unicast Retransmission and RCC capacity limits have been exceeded.

The ER and RCC capacity counters and statistics are reset to 0 when the VQE-S service restarts or when the channel lineup changes.

**Figure 4-12** Error Repair and RCC Capacity Tab

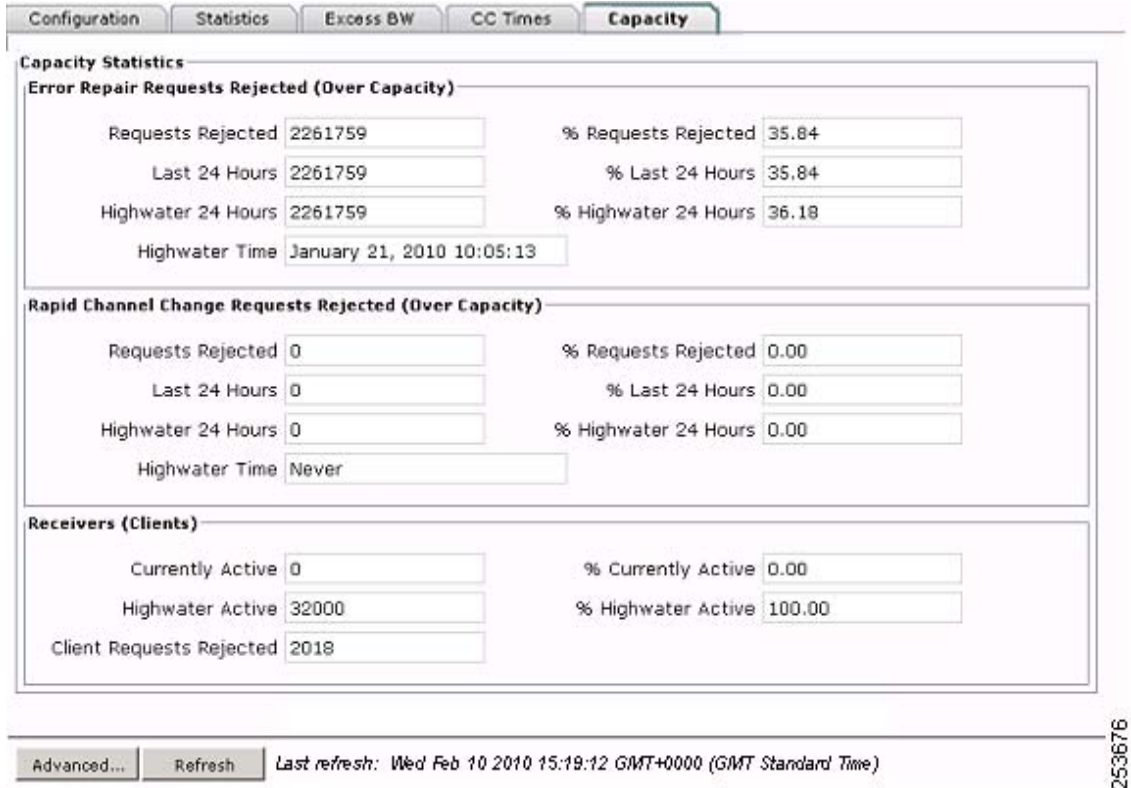


Table 4-8 lists the information presented in the Error Repair and RCC Capacity tab.

**Table 4-8** Error Repair and RCC Capacity Statistics

Field	Description
<b>Error Repair Requests Rejected (Over Capacity)</b>	
Requests Rejected	Number of ER requests rejected due to ER capacity limits being exceeded since the VQE-S service was last started. For information on the maximum number of ER requests and the maximum number of output ER packets, see <a href="#">Table H-3 on page H-2</a> . This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.

253676

**Table 4-8 Error Repair and RCC Capacity Statistics (continued)**

Field	Description
% Requests Rejected	Percentage of ER requests rejected due to ER capacity limits being exceeded out of the total number of ER requests received. For information on the maximum number of ER requests and the maximum number of output ER packets, see <a href="#">Table H-3 on page H-2</a> . This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.
Last 24 Hours	Number of ER requests rejected in the last 24 hours due to ER capacity limits being exceeded. For information on the maximum number of ER requests and the maximum number of output ER packets, see <a href="#">Table H-3 on page H-2</a> .
% Last 24 Hours	Percentage of ER requests rejected in the last 24 hours due to ER capacity limits being exceeded out of the total number of ER requests received during that same 24 hour period. For information on the maximum number of ER requests and the maximum number of output ER packets, see <a href="#">Table H-3 on page H-2</a> .
Highwater 24 Hours	Highest number of ER requests rejected during any 24 hour period due to ER capacity limits being exceeded. For information on the maximum number of ER requests and the maximum number of output ER packets, see <a href="#">Table H-3 on page H-2</a> .
% Highwater 24 Hours	Percentage of ER requests rejected during the highest 24 hour period due to ER capacity limits being exceeded out of the total number of ER requests received during that same 24 hour period. For information on the maximum number of ER requests and the maximum number of output ER packets, see <a href="#">Table H-3 on page H-2</a> .
Highwater Time	Date and time when the highwater mark was reached.
<b>RCC Requests Rejected (Over Capacity)</b>	
Requests Rejected	Number of RCC requests rejected due to RCC capacity limits being exceeded since the VQE-S service was last started. For information on the allocation of egress bandwidth to servicing RCC requests, see the <a href="#">“Scaling and Performance Summary”</a> section on page H-2. This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.
% Requests Rejected	Percentage of RCC requests rejected due to RCC capacity limits being exceeded out of the total number of RCC requests received. For information on the allocation of egress bandwidth to servicing RCC requests, see the <a href="#">“Scaling and Performance Summary”</a> section on page H-2. This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.
Last 24 Hours	Number of RCC requests rejected in the last 24 hours due to RCC capacity limits being exceeded. For information on the allocation of egress bandwidth to servicing RCC requests, see the <a href="#">“Scaling and Performance Summary”</a> section on page H-2.
% Last 24 Hours	Percentage of RCC requests rejected in the last 24 hours due to RCC capacity limits being exceeded out of the total number of RCC requests received during that same 24 hour period. For information on the allocation of egress bandwidth to servicing RCC requests, see the <a href="#">“Scaling and Performance Summary”</a> section on page H-2.

**Table 4-8 Error Repair and RCC Capacity Statistics (continued)**

Field	Description
Highwater 24 Hours	Highest number of RCC requests rejected during any 24 hour period due to RCC capacity limits being exceeded. For information on the allocation of egress bandwidth to servicing RCC requests, see the <a href="#">“Scaling and Performance Summary”</a> section on page H-2.
% Highwater 24 Hours	Percentage of RCC requests rejected during the highest 24 hour period due to RCC capacity limits being exceeded out of the total number of RCC requests received during that same 24 hour period. For information on the allocation of egress bandwidth to servicing RCC requests, see the <a href="#">“Scaling and Performance Summary”</a> section on page H-2.
Highwater Time	Date and time when the highwater mark was reached.
<b>Receivers (Clients)</b>	
Currently Active	Number of receivers currently active on the VQE-S.
% Currently Active	Percentage of receivers currently active on the VQE-S out of the total number of allowed receivers. For information on the maximum number of simultaneous receivers, see <a href="#">Table H-3 on page H-2</a> .
Highwater Active	Highest number of receivers simultaneously active on the VQE-S.
% Highwater Active	Percentage of receivers simultaneously active at the highwater mark out of the total number of allowed receivers. For information on the maximum number of simultaneous receivers, see <a href="#">Table H-3 on page H-2</a> .
Client Requests Rejected	Number of client requests rejected due to the maximum number of simultaneous receivers being exceeded. For information on the maximum number of simultaneous receivers, see <a href="#">Table H-3 on page H-2</a> . This counter is resettable. For information on resetting counters, see the <a href="#">Resetting VQE-S Counters</a> section.

# Monitoring Interfaces

When you click **Interfaces** in the navigation tree, the VQE-S AMT displays three tables associated with the CDE110 Ethernet and bond interfaces: the Interface Summary Table, the Input Bandwidth Table, and the Multicast Group Table. [Figure 4-13](#) shows these tables. (In [Figure 4-13](#), some channels in the Multicast Group Table have been omitted.)

**Figure 4-13** Interface-related Tables

The screenshot shows the VQE-S Application Monitoring Tool interface. It contains three tables:

Interface Summary Table				
I/F Name	IP Address	Status	Role	Max BW (Mbps)
bond1	18.17.1.2	up	Ingest, Management	2000
bond2	18.18.1.2	up	Service, Management	2000
eth1	18.86.61.26	up	Management	1000
eth2	(bond1)	up	(bond1)	1000
eth3	(bond1)	up	(bond1)	1000
eth4	(bond2)	up	(bond2)	1000
eth5	(bond2)	up	(bond2)	1000
eth6	13.3.20.2	up	Service	1000

Input Bandwidth Table				
I/F Name	Max Input BW (Mbps)	Reserved Input BW	Available Input BW (Mbps)	Multicast Group Count
bond1	2000	20%	508	202

Multicast Group Table				
Multicast Address	I/F Name	Source Filter	Used Input BW (Mbps)	
229.1.1.1	bond1	9.3.13.2	4.0	
229.1.1.2	bond1	9.3.13.2	4.0	
229.1.1.3	bond1	9.3.13.2	4.0	
229.1.1.4	bond1	9.3.13.2	4.0	
229.1.1.5	bond1	9.3.13.2	2.0	

[Table 4-9](#) lists the information presented in the Interface Summary Table (shown in [Figure 4-13](#)). The information is about the Ethernet and bond interfaces on the Cisco CDE110 that are currently configured for the VQE-S ingest and services traffic.

**Table 4-9** Interface Summary Table

Column	Description
I/F Name	Name that is assigned to the Ethernet interface or bond interface by Linux. For information on these names, see <a href="#">“Configuring the Linux Operating System for the VQE-S”</a> section on page D-3.
IP Address	IP address of one of the following interfaces: <ul style="list-style-type: none"> <li>If this interface is an Ethernet interface and it does not belong to a bond interface, the IP address assigned to the Ethernet interface is displayed.</li> <li>If this interface is an Ethernet interface and it belongs to a bond interface, the bond interface name is displayed.</li> <li>If this interface is a bond interface, the IP address assigned to the bond interface is displayed.</li> </ul>
Status	Interface is either up or down.

**Table 4-9** *Interface Summary Table (continued)*

Column	Description
Role	One or more of the following: <ul style="list-style-type: none"> <li>• Ingest—Used for traffic for multicast streams from the upstream video sources.</li> <li>• Service—Used for the VQE-S services traffic (Unicast Retransmission and RCC) to the downstream VQE-Cs on the STBs.</li> <li>• Management—Used for the VQE-S management traffic to the management network.</li> <li>• Bond interface name—Used for Ethernet interfaces that are members of a bond interface. Displays the bond interface name.</li> </ul>
Max BW (Mbps)	Maximum speed of the interface.

Table 4-10 lists information about the Input Bandwidth Table shown in Figure 4-13. The table provides information on the Ethernet interfaces or bond interfaces currently being used for VQE-S ingest traffic. The interfaces listed in this table are currently under the control of the VQE-S Multicast Load Balancer.

Multicast Load Balancer distributes traffic for incoming multicast streams over the Ethernet interfaces that are configured for ingest. If a bond interface is used for ingest traffic, the Multicast Load Balancer distributes traffic over the Ethernet interfaces that are members of the bond interface. The interfaces must be correctly configured and operational (up) to participate in this load balancing. The 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. It also monitors the status of these interfaces, moving the streams to other interfaces in case of interface failure.

**Table 4-10** *Input Bandwidth Table*

Column	Description
I/F Name	Name of the interface that is being used for receiving multicast streams.
Max Input BW (Mbps)	Maximum speed of the interface.
Reserved Input BW	Percentage of maximum input bandwidth that has been reserved for all non-ingest traffic and is not be used for receiving multicast streams. The VCDB parameter <code>vqe.vqes.unicast_reservation</code> specifies this percent. <ul style="list-style-type: none"> <li>• If the interface is used for both VQE-S ingest and VQE-S services, the reservation should include sufficient bandwidth for receiving Unicast Retransmission and RCC requests, RTCP reports from the STBs, and control traffic, such as IGMP and RTCP.</li> <li>• If the interface is used for ingest only, the reservation should include sufficient bandwidth for incoming control traffic, such as IGMP and RTCP.</li> </ul>

**Table 4-10** *Input Bandwidth Table (continued)*

Column	Description
Available Input BW (Mbps)	Interface bandwidth that is available for ingest of multicast streams but that is not currently being used. Initially, when no multicast streams are being received by this interface, this value is equal to Max Input BW minus Reserved Input BW.
Multicast Group Count	Number of multicast streams that are currently being received by the interface.

[Table 4-11](#) lists the information about the Multicast Group Table shown in [Figure 4-13](#). The table provides information about the multicast streams currently being received by this VQE-S.

**Table 4-11** *Multicast Group Table*

Column	Description
Multicast Address	Destination IP address for this multicast group.
I/F Name	Name of the interface that is being used for receiving this multicast stream.
Source Filter	Source IP address of the multicast group's sender.
Used Input Bandwidth (Mbps)	Receive bandwidth consumed on this interface by receiving this multicast steam. This bandwidth is specified in the channel definition (for example, in the Bit Rate field of the VCPT).

## Monitoring RTCP Exporter

When you click **RTCP Exporter** in the navigation tree and click the **Configuration** tab, the VQE-S AMT displays the VQE-S RTCP Exporter parameters. RTCP Exporter currently has no parameters that can be configured with the VQE-S AMT, and the parameters are for viewing only. For information on configuring RTCP Exporter, see the [“Configuring the VQE-S RTCP Exporter”](#) section on page 2-42.

When you click **RTCP Exporter** in the navigation tree and click the **Statistics** tab, the VQE-S AMT displays the RTCP Exporter Statistics window (see [Figure 4-14](#)).

**Figure 4-14** RTCP Exporter Statistics Window

[Table 4-12](#) lists the information presented in the RTCP Exporter Statistics window.

**Table 4-12** RTCP Exporter Statistics

Field	Description
<b>VQM Application Configuration</b>	
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.
Enabled	Either true (enabled) or false (not enabled).
Filtering NACKs	Either true (enabled) or false (not enabled). If enabled, RTCP NACK compound packets are not sent to the VQM application. This field was introduced in Cisco VQE Release 3.5.5.
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.
<b>RTCP Exporter Stats</b>	
Packets Exported	Number of RTCP compound packets that have been exported to a VQM host.

**Table 4-12** RTCP Exporter Statistics

Field	Description
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.
NACKs Filtered	Number of RTCP NACK compound packets omitted from the RTCP data sent to the VQM application.  This field was introduced in Cisco VQE Release 3.5.5.

For information on RTCP Exporter and the video-quality monitoring application, see the “[VQE-S RTCP Exporter for Video-Quality Monitoring](#)” section on page 1-23.

## Monitoring the STUN Server

When you click **STUN Server** in the navigation tree, the VQE-S AMT displays the STUN Server Statistics window (see [Figure 4-15](#)).

**Figure 4-15** STUN Server Statistics Window

The screenshot shows the 'STUN Server Statistics' window with the following data:

Total Requested	0	Response Failed	0
Successfully Sent	0	Sent Failed	0

Additional UI elements include a 'Refresh' button and a timestamp: 'Last refresh: Wed Feb 10 2010 15:19:12 GMT+0000 (GMT Standard Time)'. A vertical ID number '2536891' is visible on the right side.

[Table 4-13](#) lists information displayed in the STUN Server Statistics window.

**Table 4-13** 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 in which the STUN Server fails to generate a binding response because of an internal error.
Sent Failed	Number of instances in which 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).

## Resetting VQE-S Counters

The VQE-S maintains a set of counters for debugging purposes. A subset of counters can be manually reset from the VQE-S AMT GUI. The results of this action are visible to all AMT users, even those in separate AMT browser sessions. The **Reset** button is located on the **Statistics** tab of the **Error Repair and RCC** window, and resets all counters displayed in [Table 4-14](#) to zero.

**Table 4-14**      *Resettable VQE-S AMT counters*

Category	Counter
<b><i>Error Repair and RCC counters on Statistics tab</i></b>	
Generic NACK Messages Received	<ul style="list-style-type: none"> <li>• Total Messages</li> <li>• Invalid Messages</li> </ul>
Repaired RTP Packets	<ul style="list-style-type: none"> <li>• Requested</li> <li>• Sent</li> <li>• Not Sent</li> </ul>
RCC	<ul style="list-style-type: none"> <li>• Requested</li> <li>• Accepted</li> <li>• Refused</li> <li>• Failed</li> </ul>
<b><i>Capacity counters on Capacity tab</i></b>	
Capacity Statistics	<ul style="list-style-type: none"> <li>• Error Repair Requests Rejected (Over Capacity)—Requests Rejected</li> <li>• Error Repair Requests Rejected (Over Capacity)—% Requests Rejected</li> <li>• RCC Requests Rejected (Over Capacity)—Requests Rejected</li> <li>• RCC Requests Rejected (Over Capacity)—% Requests Rejected</li> <li>• Receivers (Clients)—Client Requests Rejected</li> </ul>
<b><i>Channel counters on Statistics/Status tab</i></b>	
Channel Input Stream	<ul style="list-style-type: none"> <li>• Received packets</li> <li>• Received bytes</li> <li>• Lost RTP Packets</li> </ul>
Error Repair—Generic NACK Messages Received	<ul style="list-style-type: none"> <li>• Total Messages</li> <li>• Invalid Messages</li> </ul>
Error Repair—Repaired RTP Packets	<ul style="list-style-type: none"> <li>• Requested</li> <li>• Sent</li> <li>• Not Sent</li> </ul>

**Table 4-14** *Resettable VQE-S AMT counters (continued)*

Category	Counter
RCC	<ul style="list-style-type: none"> <li>• Requested</li> <li>• Accepted</li> <li>• Refused</li> <li>• Failed</li> </ul>
RTCP Packets	<ul style="list-style-type: none"> <li>• Received</li> <li>• Sent Downstream</li> <li>• Sent Upstream</li> </ul>



**Note** When one user resets the subset of counters displayed in [Table 4-13](#), this change is reflected for all other users on performing a refresh of the VQE-S AMT GUI.

To reset counters, do the following:

- 
- Step 1** In the VQE-S AMT navigation tree, click the **Error Repair and RCC** node.  
The **Configuration** tab is displayed on the **Error Repair and RCC** window.
- Step 2** On the Error Repair and RCC window, click the Statistics tab.  
The **Reset** button is displayed on the Statistics tab.
- Step 3** Click **Reset**.  
The values of all counters listed in [Table 4-13](#) are reset to zero. The last reset timestamp is updated to display the current time.
- 

## Restoring VQE-S Counters

Following a reset of the subset of counters listed in [Table 4-14](#), you can restore counters from the VQE-S AMT GUI to display their cumulative value since the last start of the VQE-S service.



**Note** When one user restores the subset of counters displayed in [Table 4-14](#) to their cumulative value, this change is reflected for all users on performing a refresh of the VQE-S AMT GUI.

To reset counters, do the following:

- 
- Step 1** In the VQE-S AMT navigation tree, click the **Error Repair and RCC** node.  
The Configuration tab is displayed on the Error Repair and RCC window.
- Step 2** On the Error Repair and RCC window, click the **Statistics** tab.  
The Restore button is displayed on the Statistics tab.
- Step 3** Click **Restore**.

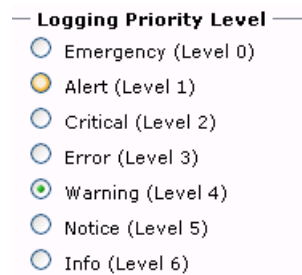
All counters that were reset now display their cumulative value. The last reset timestamp is updated to display the text *never*.

---

## Change VQE-S Logging

When you click **Logging** in the navigation tree, the VQE-S AMT displays the logging priority levels (Figure 4-16) for the 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`. In addition, you can send system messages to remote servers for centralized logging. For information on configuring remote syslog servers, see the “[Remote Syslog Hosts](#)” section on page 2-28.

**Figure 4-16** Logging Priority Levels



To change a VQE-S logging priority level, click the button next to the appropriate level 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 the VQE-S is stopped. When the 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](#).

## Change 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 4-17](#) 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 4-17 Debug Components**



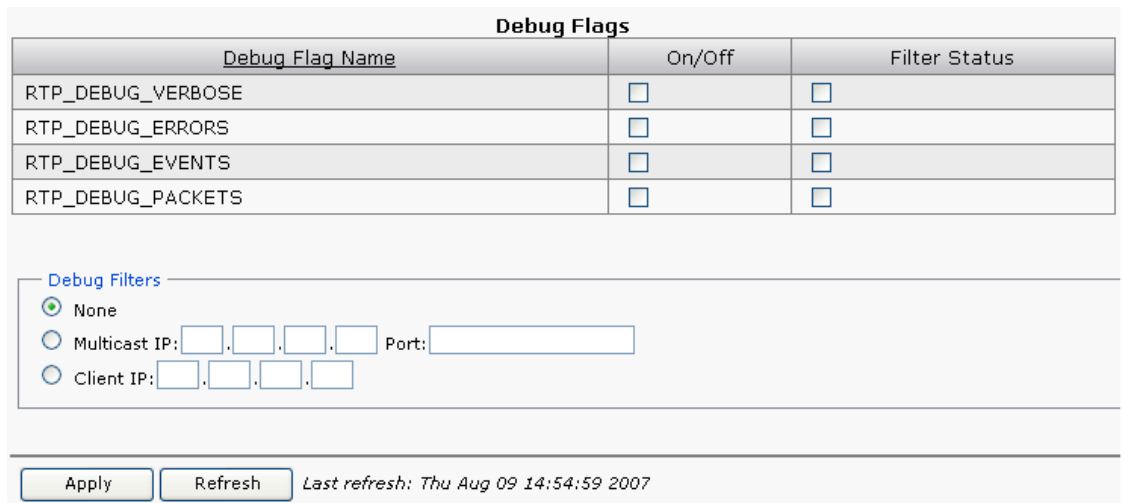
To change VQE-S debugging, follow these steps:

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

The debug flags and filters for that component are displayed.

For example, [Figure 4-18](#) shows the flags and filters for the RTP/RTCP category.

**Figure 4-18 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 provides debug messages for the specified client.

**Step 2** To enable a debugging flag, click the check box in the On/Off column. To disable an enabled flag, click the check box in the On/Off column 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** To filter debugging messages by a specific channel or VQE-C for an enabled debugging flag, 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 source stream IP address and (RTP/UDP) port number.
  - For Client IP, enter the VQE-C IP address.

**Step 4** Click **Apply**.

The selected debugging options are enabled.

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

---





# CHAPTER 5

## Using the VCDS AMT

This chapter describes how to use Cisco VQE Client Configuration Delivery Server (VCDS) Application Monitoring Tool (AMT). The VCDS is a software component installed on each VQE Tools server, the Cisco CDE110 that also hosts VCPT. The VCDS AMT is a web browser-based tool for displaying configuration, status, and statistics on the VCDS process and the VQE Tools server. The tasks that you can perform with the VCDS AMT are listed in [Table 5-1](#).

**Table 5-1** VCDS AMT Tasks

VCDS AMT Task	Section Where Described
Log in to VCDS AMT	<a href="#">Logging into and Navigating in VCDS AMT, page 5-2</a>
Monitor the health of the VCDS process and VQE Tools Server	<a href="#">Monitoring the Health of the VCDS Process and VQE Tools Server, page 5-3</a>
View configuration details and statistics for the VCDS	<a href="#">Viewing VCDS Configuration and Statistics, page 5-4</a>
Change VCDS logging levels	<a href="#">Change VCDS Logging, page 5-7</a>
Change VCDS debugging levels	<a href="#">Change VCDS Debugging, page 5-9</a>



**Note**

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

# Logging into and Navigating in VCDS AMT

Before logging into VCDS AMT, you need a valid Linux username and password on the Cisco CDE110 hosting the VCDS 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.

The VCDS 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 the VCDS AMT is 1024 x 768 pixels.

The VCDS AMT uses secure HTTPS. Access by multiple simultaneous browsers is supported.

To login to VCDS AMT, follow these steps:

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

```
https://ip_address/vcds-amt
```

or

```
https://fully_qualified_domain_name/vcds-amt
```

The VCDS AMT login dialog box is displayed.

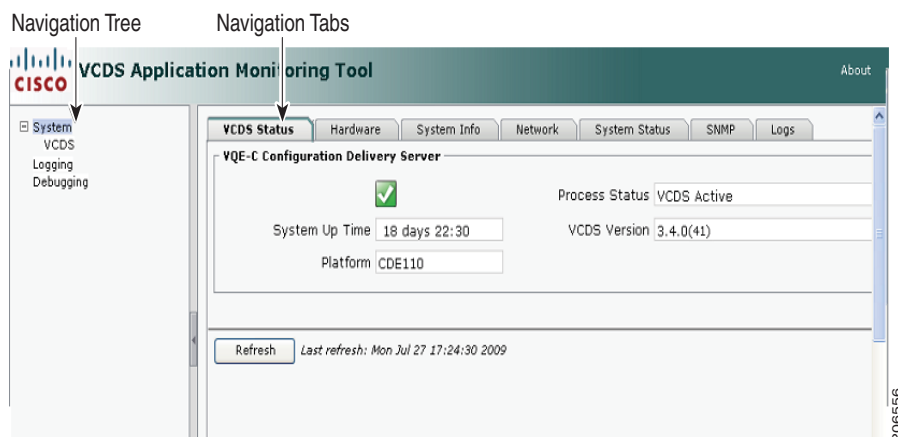
- Step 2** Enter a Linux username and password.

- Step 3** Click **OK**.

If the username and password are valid, the VCDS AMT Status window is displayed.

Figure 5-1 shows the VCDS AMT navigation controls and buttons.

**Figure 5-1** VCDS AMT Navigation



VCDS AMT (Figure 5-1) provides these controls and buttons for navigating and displaying VCDS data:

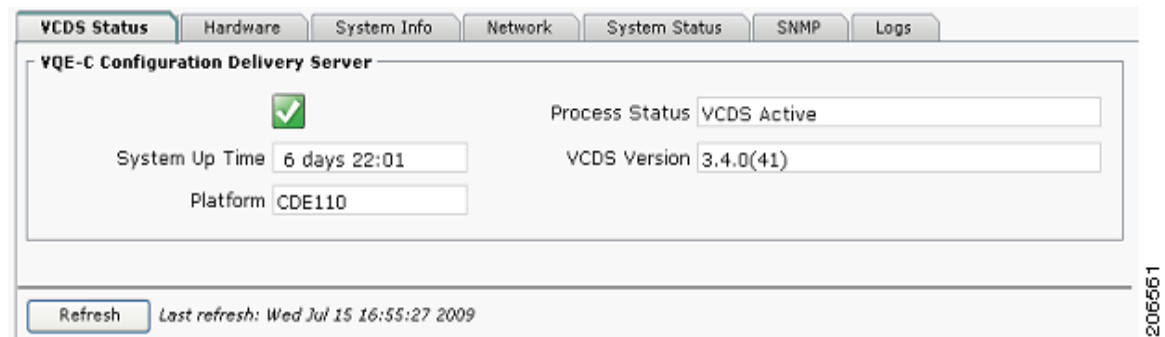
- **Navigation tree**—Use the collapsible and expandable tree to display the VCDS AMT items that can be viewed or configured. The navigation tree can be hidden by clicking the < arrow in its right border.
  - The parent node (**System**) in the tree provides summary data.

- Each child node in the tree (such as VCDS) provides data on the specific child node.
- **Navigation Tabs**—Click the tabs to display VCDS data for viewing. The VCDS node has two tabs: a Configuration tab and a Statistics tab.
- **Refresh** —Click to update the displayed data. The VCDS AMT statistical data are not automatically updated when the VCDS 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 VCDS Process and VQE Tools Server

When you click the **System** node in the navigation tree and the **VCDS Status** tab, the VCDS AMT displays VCDS and VQE Tools Server status information (Figure 5-2).

**Figure 5-2** VCDS Status Information



On the VCDS Status tab, a green icon with a checkmark indicates the VQE Tools server system is running and healthy. A red icon with an X indicates one or more problems with the VQE Tools server. A yellow icon with an exclamation mark (!) indicates that one or more of the following files are invalid:

- Channel configuration file
- Client database file
- Group attribute file

From the **VCDS Status** tab, you can view the following status information:

- **System Up Time**—Time that the Cisco CDE110 hosting VQE Tools has been running.
- **Platform**—Cisco CDE110 hardware platform that is hosting VQE Tools. 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 and CDE111-2-146TXD-K9)
  - UNKNOWN if the hardware platform cannot be determined
- **Process Status**—One of the following status messages:
  - VCDS Active—VCDS is running.
  - VCDS Stopped—VCDS is not running

- VCDS Inactive—A configuration file is not correct.
- VCDS Version—Current version of the VCDS software.

In addition to the VCDS Status tab, you can get information on the VCDS and the VQE Tools server on the five other tabs. [Table 5-2](#) lists the information that is available from each tab accessible from the System node.

**Table 5-2** System Node Tabs

System Node Tab	Information Provided
Hardware	Processor and memory on the Cisco CDE110 that hosts VQE Tools. 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 <b>iptables</b> information.
Network	Output from the <b>ifconfig</b> command. Configuration information displayed by <b>ifconfig</b> is for the four CDE110 Ethernet interfaces.
System Status	Detailed information on host uptime, currently running processes, and file system disk space.
SNMP	SNMP information on the VQE Tools server host taken from the <code>snmpd.conf</code> file.
Logs	Most recent 300 lines from the following VQE Tools Server log files are displayed: <ul style="list-style-type: none"> <li>• VCDS log (<code>/var/log/vqe/vqe.log</code>)</li> <li>• System messages log (<code>/var/log/messages</code>)</li> <li>• HTTPD error log (<code>/var/log/httpd/error_log</code>)</li> <li>• SSL error log (<code>/var/log/httpd/ssl_error_log</code>)</li> <li>• Tomcat log (<code>/usr/share/tomcat5/logs/catalina.out</code>)</li> <li>• VCDS AMT log (<code>/usr/share/tomcat5/logs/vcds.out</code>)</li> </ul>

## Viewing VCDS Configuration and Statistics

When you click the **VCDS** node in the navigation tree and click the **Configuration** tab, the VCDS AMT displays information relating to the VCDS configuration, to VQE Client (VQE-C) channel configuration, to the client database file, and to the group attribute file ([Figure 5-3](#)). For more information on the client database and the group attribute files, see “[VQE-C System Configuration Provisioning Server Role](#)” section on page 1-20.



### Note

In the VCDS AMT, the group attribute file is referred to as the VQE-C network configuration file and the client database file is referred to as the VQE-C group map file.

## Viewing VCDS Configuration

When you click the **Configuration** tab, VCDS AMT displays the VCDS Configuration window (Figure 5-3).

**Figure 5-3** VCDS Configuration Window

The screenshot shows the VCDS Configuration window with the following settings:




- VCDS Configuration:**
  - TCP Port: 8554
  - Max Connections Allowed: 2000
  - Inactive Connection Timeout (sec): 10
- VQE-C Channel Lineup:**
  - Validation Check: Pass
  - No. of Channels in Lineup: 1
  - Lineup Filename: /etc/opt/vqes/vqec\_channels.cfg
  - Last Modified: Thu, 9 Jul 2009 15:27:15 EDT
- VQE-C Group Map:**
  - Validation Check: Pass
  - No. of CNames in Map: 2
  - Map Filename: /etc/opt/vqes/vqec.group\_map
  - Last Modified: Mon, 13 Jul 2009 16:26:27 EDT
- VQE-C Network Configuration:**
  - Validation Check: Pass
  - No. of Groups in Network Configuration File: 2
  - Network Configuration Filename: /etc/opt/vqes/vqec\_attributes.cfg
  - Last Modified: Mon, 13 Jul 2009 17:20:30 EDT

The Configuration window has the information listed in Table 5-3.

**Table 5-3** VCDS Configuration

Field	Description
<b>VCDS Configuration</b>	
TCP Port	TCP port number on which the VCDS process listens.
Max Connections Allowed	Maximum number of clients allowed to connect to VCDS.
Inactive Connection Timeout (sec)	Number of seconds of inactivity that is allowed to elapse before a client is disconnected from the VCDS.
<b>VQE-C Channel Lineup</b>	

Table 5-3 VCDS Configuration (continued)

Field	Description
Validation Check	<ul style="list-style-type: none"> <li>Pass—Channel configuration file has passed a validation check performed by VCDS.</li> <li>Fail—Channel configuration file has failed a validation check performed by VCDS.</li> </ul>  <p><b>Note</b> On receiving the contents of the channel configuration file from the VQE Channel Provisioning Tool (VCPT), the VCDS validates its contents based on SDP syntax.</p>
No. of Channels in Lineup	Number of channels in the channel configuration file.
Lineup File name	Full pathname of the channel configuration file.
Last Modified	Date and time the channel configuration file was last modified.
<b>VQE-C Group Map</b>	
Validation Check	<ul style="list-style-type: none"> <li>Pass—Client database file has passed the validation check performed by VCDS.</li> <li>Fail—Client database file has failed the validation check performed by VCDS.</li> </ul>  <p><b>Note</b> On receiving the client database file from the VQE-C system configuration provisioning server, the VCDS validates its contents based on an XML schema defined by Cisco.</p>
No. of CNames in Map	Number of customer names (CNames) in the client database file. A CName is a unique identifier for a VQE-C.
Map Filename	Full pathname of the client database file.
Last Modified	Date and time the client database file was last modified.
<b>VQE-C Network Configuration</b>	
Validation Check	<ul style="list-style-type: none"> <li>Pass—Group attribute file has passed the validation check performed by the VCDS.</li> <li>Fail—Group attribute file has failed the validation check performed by the VCDS.</li> </ul>  <p><b>Note</b> On receiving the contents of the group attribute file from the VQE-C system configuration provisioning server, the VCDS validates its contents based on an XML schema defined by Cisco.</p>
No. of Groups in Network Configuration File	Number of attribute groups in the group attribute file. Each VQE-C is associated with at least one group of attributes. Each group of attributes can be associated with one or more VQE-Cs.
Network Configuration Filename	Full pathname of the group attribute file.
Last Modified	Date and time the group attribute file was last modified.

## Viewing VCDS Statistics

When you click the **Statistics** tab, the VCDS AMT displays the VCDS Statistics window (Figure 5-4).

**Figure 5-4** VCDS Statistics Window

The VCDS Statistics window has the information listed in Table 5-4.

**Table 5-4** VCDS Statistics

Field	Description
<b>VCDS Stats</b>	
Validation check	<ul style="list-style-type: none"> <li>Pass—Channel configuration, client database and group attribute files have all passed the validation check performed by VCDS.</li> <li>Fail—One or more channel configuration, client database, or group attribute files have failed the validation check performed by VCDS.</li> </ul>
Current Open Connections	Number of clients currently connected to VCDS.
Total Requests Received	Total number of Real Time Streaming Protocol (RTSP) requests received from STBs.
Total Responses Sent	Total number of RTSP responses sent to STBs.

## Change VCDS Logging

When you click **Logging** in the navigation tree, VCDS AMT displays the logging priority levels (Figure 5-5) for VCDS. The priority levels allow you to control the logging level for system messages for the VCDS process. All VCDS system messages are written to the file `/var/log/vqe/vqe.log`. In addition, you can send system messages to remote servers for centralized logging. For information on configuring remote syslog servers, see the “[Remote Syslog Hosts](#)” section on page 2-28.

Figure 5-5 Logging Priority Levels

**Logging Priority Level**

- Emergency (Level 0)
- Alert (Level 1)
- Critical (Level 2)
- Error (Level 3)
- Warning (Level 4)
- Notice (Level 5)
- Info (Level 6)

Apply Refresh Last refresh: Wed Jul 15 16:57:13 2009

206559

To change a VCDS logging priority level, click the button next to the level you want and click **Apply**.

In VCDS 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 the VCDS service is stopped. When VCDS restarts, the logging priority level goes back to the default (Warning).

# Change VCDS Debugging

When you click **Debugging** in the navigation tree, the debugging options for the VCDS are displayed. [Figure 5-6](#) shows the debug options. The options allow you to control the types of debugging messages that are written to the syslog file. Debug messages are written to the file `/var/log/vqe/vqe.log`.

**Figure 5-6** Debug Components

Debug Flags		
Debug Flag Name	On/Off	Filter Status
RTSP_DEBUG_CFG	<input type="checkbox"/>	<input type="checkbox"/>
RTSP_DEBUG_CONTENT	<input type="checkbox"/>	<input type="checkbox"/>
RTSP_DEBUG_MAIN	<input type="checkbox"/>	<input type="checkbox"/>
RTSP_DEBUG_RTSP	<input type="checkbox"/>	<input type="checkbox"/>
RTSP_DEBUG_XMLRPC	<input type="checkbox"/>	<input type="checkbox"/>

**Debug Filters**

None

Multicast IP:  .  .  .  Port:

Client IP:  .  .  .

Last refresh: Wed Jul 15 20:02:37 2009

To change VQE-S debugging, follow these steps:

- 
- Step 1** In the VCDS AMT navigation tree, click **Debugging**.  
The debug flags for VCDS are displayed.
- 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.
- Step 3** Click **Apply**.  
The selected debugging options are enabled.



**Note** The selected debugging options do not persist when the VCDS service is stopped. When the VCDS restarts, debugging goes back to the default—no options are enabled. Debug filters are always disabled.

---





# CHAPTER 6

## Troubleshooting VQE Software Components

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

- [Useful Linux Tools, page 6-1](#)
- [VQE Logging and Log Files, page 6-2](#)
- [VQE Files, Directories, and Permissions, page 6-3](#)
- [VQE-S and VQE Tools Server Troubleshooting, page 6-7](#)
- [RCC Troubleshooting, page 6-15](#)
- [Using the `vmreport` Command, page 6-29](#)
- [Gathering Information for a Service Request, page 6-30](#)
- [Stopping, Starting, and Restarting VQE-S, page 6-30](#)
- [Stopping, Starting, and Restarting VCDS, page 6-31](#)
- [Resetting the Root Password on the VQE-S or VQE Tools Server, page 6-31](#)

### Useful Linux Tools

[Table 6-1](#) provides information on some Linux commands that are particularly useful for troubleshooting VQE software components.

**Table 6-1** *Useful Linux Commands*

Command	Description	Notes
<code>arp</code>	Manipulates the ARP cache of the kernel	—
<code>ethtool</code>	Displays or changes Ethernet card settings	Detailed status on an Ethernet interface
<code>ifconfig</code>	Configures a network interface	Traditional interface configuration and status
<code>ip</code>	Shows or manipulates routing, devices, policy routing, and tunnels	Most useful interface to all Linux networking
<code>netstat</code>	Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships	Provides traditional network state information

Table 6-1 Useful Linux Commands (continued)

Command	Description	Notes
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, page 6-2](#)
- [VQE-S AMT, VCDS AMT, and VCPT Logging and Log Files, page 6-3](#)

### VQE Server and VQE Tools Logging and Log Files

The VQE Server (VQE-S) logging is based on the syslog-ng 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 the following five fields in this order:

- Timestamp (For example, Oct 22 08:42:03)
- Host name (For example, minnie)
- Name of process logging the message (For example, vqes\_mlb)
- Identity string—FACILITY-SEVERITY-MNEMONIC (For example, <<%VQES\_MLB-3-MLB\_NIC\_DOWN>>)
- Message text (For example, Network interface eth3 went down.)

For information on VQE system messages, see [Appendix C, “VQE System Messages.”](#)

By default, the 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 [“Change VQE-S Logging” section on page 4-33](#).

The 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 (for example, when backing up log files), be sure to stop the syslog-ng daemon before moving the `vqe.log` file. If syslog-ng is started with no `vqe.log` file in the `/var/log/vqe` directory, syslog-ng creates the `vqe.log` file.

In addition, you can send system messages to remote servers for centralized logging. For information on configuring remote syslog servers, see the [“Remote Syslog Hosts” section on page 2-28](#).

## VQE-S AMT, VCDS AMT, and VCPT Logging and Log Files

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

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

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

- For the VQE-S AMT and the VCDS 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 6-2 lists the most important default log4j configuration settings for VQE-S AMT, VCDS AMT, and VCPT logging.

**Table 6-2** Log4j Default Configuration for VQE-S AMT, VCDS 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 6-3 provides information for the CDE110 that hosts the VQE-S.
- Table 6-4 provides information for the CDE110 that hosts VCPT, VCDS AMT, and VCDS.

These sections provide additional information on resolving problems:

- [Changing Permissions, page 6-5](#)
- [Replacing a Lost or Corrupt VQE File, page 6-5](#)

**Table 6-3** 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
/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
/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	<b>vqe_cfgtool</b> command
/opt/vqes/bin/vqereport	-r-x----- root root	<b>vqereport</b> 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
/etc/syslog-ng/syslog-ng.conf	-rw-r--r-- 1 root root	VQE-S syslog configuration file
/opt/syslog-ng/sbin/syslog-ng	-rwxr-xr-x root root	VQE-S syslog-ng 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 6-4** 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	Link to the VCDB sample configuration file
/etc/opt/vqes/vcdb.conf.tools.sample	-r----- vqes vqes	VCDB sample 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.)

Table 6-4 VQE Tools Files, Directories, and Permissions (continued)

File or Directory	Required Permissions, Owner, and Group	Description
/etc/opt/vcpt/data/sdp (directory)	drwxr-xr-x root root	Directory for SDP-formatted files that VCPT creates for each valid VCPT configuration
SDP-formatted files in /etc/opt/vcpt/data/sdp	-rw-r--r-- root root	SDP-formatted files for each valid VCPT configuration
/opt/vqes (directory)	drwxr-xr-x vqes vqes	—
/opt/vqes/bin (directory)	drwxr-xr-x vqes vqes	—
/opt/vqes/bin/vcds_send_file	-r-x----- vqes vqes	Command to send a client database file and group attribute file to VCDS
/opt/vqes/bin/vqe_cfgtool	-r-x----- vqes vqes	<b>vqe_cfgtool</b> command
/opt/vqes/bin/vqereport	-r-x----- root root	<b>vqereport</b> command
/etc/syslog-ng/syslog-ng.conf	-rw-r--r-- 1 root root	VQE-S syslog configuration file
/opt/syslog-ng/sbin/syslog-ng	-rwxr-xr-x root root	VQE-S syslog-ng process
/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 is 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 is lost or corrupted, 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 3.5*.

If a configuration file located in the directories under /etc is lost or corrupted 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 corrupted 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 7-18.

# 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 6-5](#) lists the troubleshooting topics by the category of the problem.

**Table 6-5** *Troubleshooting Topics by Problem Category*

Problem Category	Troubleshooting Topics
Monitoring a VQE-S	<a href="#">Monitoring Received Multicast Streams, page 6-8</a>
VQE-S and VQE Tools servers	<a href="#">Repeated Message on CDE110 Hosting VQE-S or VQE Tools, page 6-9</a>
VQE-S	<a href="#">Repeated Message on CDE110 Hosting VQE-S or VQE Tools, page 6-9</a>
VQE-S AMT	<a href="#">VQE-S AMT, VCDS AMT, or VCPT Unavailable, page 6-10</a>
	<a href="#">Channels Are Not Displayed in VQE-S AMT, page 6-11</a>
	<a href="#">VQE-S AMT Channels Status Summary Has No Graphs, page 6-12</a>
VCDS AMT	<a href="#">VQE-S AMT, VCDS AMT, or VCPT Unavailable, page 6-10</a>
VCPT or other channel-provisioning servers*	<a href="#">VQE-S AMT, VCDS AMT, or VCPT Unavailable, page 6-10</a>
	<a href="#">VCPT Fails to Initialize, page 6-12</a>
	<a href="#">Channel-Provisioning Server Cannot Send Channel Information to VQE-S: Trusted Provisioning Client Problem, page 6-13</a>
	<a href="#">Channel-Provisioning Server Cannot Send Channel Information to VQE-S: SSL Certificates Problems, page 6-13</a>
	<a href="#">Unable to Connect Error When VCPT Tries to Send Channel Information, page 6-14</a>
	<a href="#">Internal Server Error When VCPT Tries to Send Channel Information to VQE-S, page 6-15</a>

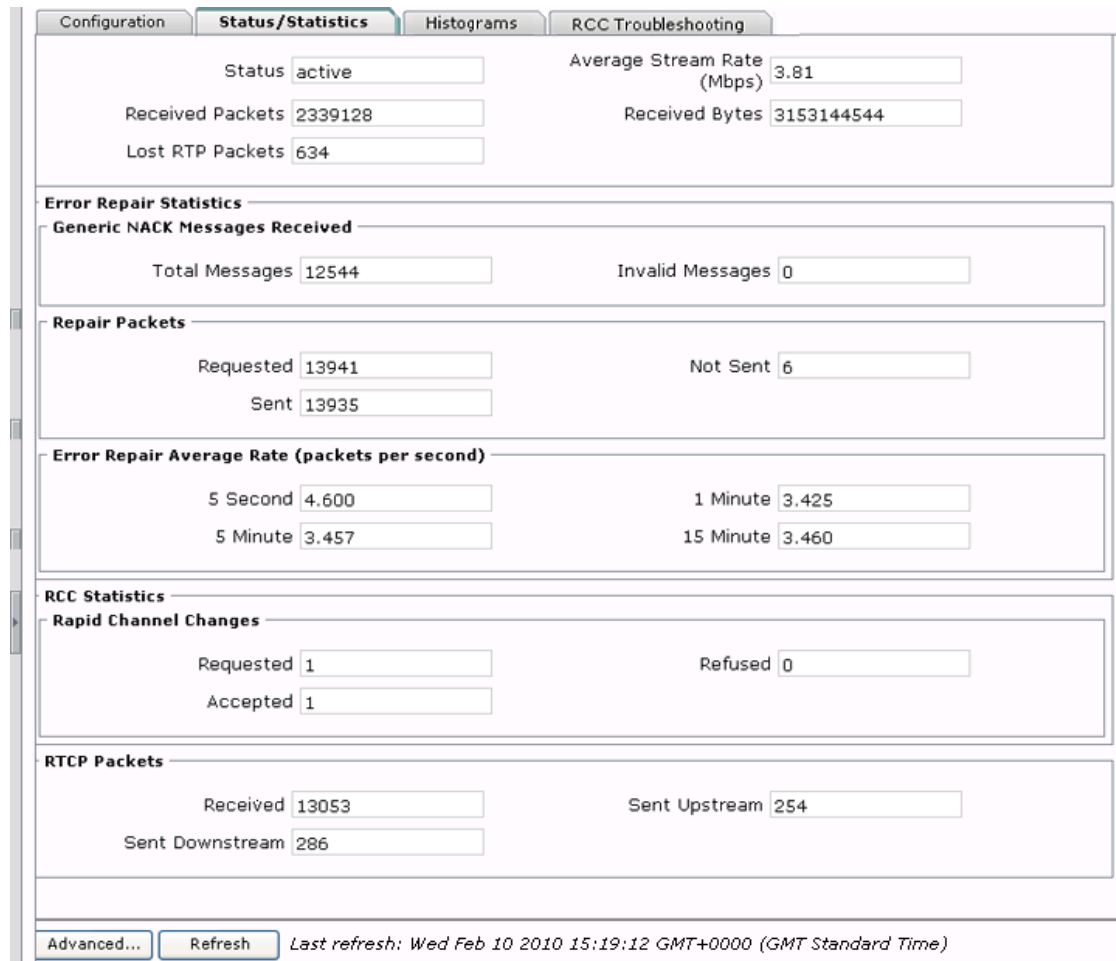
\* Some VCPT troubleshooting topics apply to other channel-provisioning servers, such as Cisco IPTV Services Delivery Server (ISDS).

## Monitoring Received Multicast Streams

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

We recommend that you use the VQE-S AMT to monitor received multicast streams. In the VQE-S AMT Channel Statistics window for each channel (see [Figure 6-1](#)), 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 original source stream of the channel but is not received by the VQE-S.

**Figure 6-1** Lost RTP Packets



## Repeated Message on CDE110 Hosting VQE-S or VQE Tools

**Symptom:** During initial system configuration, a new Cisco CDE110 hosting the 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 **ifconfig -a** command to verify that the addresses specified in the ifcfg-eth# files have been assigned to the interfaces.

Continue with the initial configuration tasks.

## 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 using the **-config** option. Use the System Parameters menu on the Configuration Tool 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 takes 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 by issuing the following command:

```
[root@system]# ntpq -p
```

**Step 10** Reboot the VQE-S by issuing the following command:

```
[root@system]# init 6
```

---

## Performing a Date and Time Change with the Linux date Command

When performing a time and 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 using the **-config** option. Use the System Parameters menu on the Configuration Tool 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 by issuing the following command:

```
[root@system]# init 6
```

---

## VQE-S AMT, VCDS AMT, or VCPT Unavailable

**Symptom:** The browser displays the message *Page Cannot Be Found* (status code 404) or *Service Temporarily Unavailable* (status code 503) even if the user enters a valid IP address or fully qualified domain name to browse the VQE-S AMT, VCDS AMT, or VCPT.

**Explanation:** The VQE-S AMT, VCDS 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 the VQE-S AMT, VCDS 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 the 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 the 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 section. If the httpd or tomcat5 processes continue to fail, check the log files for the services to determine the cause.

- httpd log file is `/etc/httpd/logs/error_log`.
- 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:** The VQE-S AMT does not display the channels after channels are defined in VCPT and channel information is pushed to the servers.

**Explanation:** The most likely reason why the VQE-S AMT does not display the channels is that the VQE-S was not associated with the channels in VCPT.

To determine whether the channels are associated with this VQE-S, 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-S 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 3-17.

---

If the channels are correctly associated with the VQE-S, it is possible that there were problems when the VQE-S attempted to process the channels. Check the VQE-S 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 2.

**Remedy:** If the channels have not been associated with the VQE-S in VCPT, associate the channels with the VCPT from the Association tab. For information on associating channels with servers, see the [“Defining Channel Associations for a Server”](#) section on page 3-19.

## VQE-S AMT Channels Status Summary Has No Graphs

**Symptom:** In the AMT VQE-S Status window (Figure 4-2), the Channels Status Summary does not have graphs for the channels.

**Explanation:** If one or more channels are successfully created in the VQE-S 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 the VQE-S AMT.

**Remedy:** Download and install Adobe Flash Player on the computer that hosts the browser used to access the VQE-S AMT. The software is free and can be found at this URL:

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

It is recommended that you close all other open browser windows before performing the installation.

## VCPT Fails to Initialize

**Symptom:** VCPT fails to initialize when the VQE Tools server starts. The following error message is displayed:

```
Initialization Failed. VCPT Data directory is missing, please refer to the Cisco CDA VQE
Application User Guide - Working with VCPT Configuration Files section."
```

**Explanation:** For VCPT to initialize successfully, the following directories must exist:

- /etc/opt/vcpt/data
- /etc/opt/vcpt/data/sdp

One or both of these directories are missing and may have been accidentally deleted.

**Remedy:** To recreate the directories and start VCPT, follow these steps:

- 
- Step 1** Login as root.
- Step 2** Determine which directory or directories are missing.
- Step 3** Create each missing directory using the permissions, owner, and group specified in Table 6-4 for that directory.
- Step 4** If up-to-date VCPT configuration files for the /etc/opt/vcpt/data directory are available in a set of backup files, the backup files can be copied to the /etc/opt/vcpt/data directory.



**Note**

There is no need to copy backup files for the set of SDP-formatted files in the /etc/opt/vcpt/data/sdp directory. The VCPT creates the SDP-formatted files when a request is made to send channel information to the VQE-S or VCDS servers.

---

- Step 5** Restart the Apache Tomcat application server:
- ```
[root@system]# service tomcat5 restart
```
- The VCPT is a web application and should initialize successfully.
- Step 6** To verify that the 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, the VCPT is running correctly.

---

## Channel-Provisioning Server Cannot Send Channel Information to VQE-S: Trusted Provisioning Client Problem

**Symptom:** The channel-provisioning server (for example, VCPT or Cisco IPTV Services Delivery Server [ISDS]) cannot send channel information to a VQE-S.

**Explanation:** When the channel-provisioning server attempts to send channel information to a VQE-S, the send operation fails. On the VQE-S, the VQE Configuration Tool parameter Trusted Provisioning Client 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 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 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 7-3](#).

**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, 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-S: SSL Certificates Problems

**Symptom:** The channel-provisioning server (for example, VCPT or ISDS) cannot send channel information to a VQE-S.

**Explanation:** When the channel-provisioning server attempts to send channel information to a VQE-S, the send operation fails. On the VQE-S 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 and on the channel-provisioning server. For information on setting up SSL certificates, see the [“Setting Up SSL Certificates” section on page 2-5](#).

After the certificate-related items have been copied to the correct locations on the VQE-S 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 the VCPT tries to send channel information to a VQE-S 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 the 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 the 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 section. If the httpd or tomcat5 processes continue to fail, check the log files for the services to determine the cause.

- httpd log file is `/etc/httpd/logs/error_log`.
- 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 the VQE-S, 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 the VCPT to send channel information to a VQE-S. The Status of Last Send column on the VCPT Servers tab shows the error.

From the CDE110 that hosts the VQE-S, you are able to successfully **ping** the machine running the web browser used for the 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 the 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`

## RCC Troubleshooting

**Symptom:** If a rapid channel change (RCC) fails or there is degradation in the performance of an RCC, video freeze or macroblocking may be observed. The following section describes how to troubleshoot RCC problems from the VQE-S.

## VQE-S RCC Troubleshooting

The section lists possible explanations for RCC problems and provides a remedy for each explanation:

- [Channel is not configured on the VQE-S, page 6-16](#)
- [Channel is not active on the VQE-S, page 6-16](#)
- [RCC is disabled on the channel, page 6-17](#)
- [No connectivity between the VQE-C and the FBT on the VQE-S, page 6-18](#)
- [No connectivity between the VQE-C and the VQE-S, page 6-18](#)
- [RCC refused by the VQE-S control or data planes, page 6-18](#)
- [RCC refused by the VQE-S—invalid e-factor, page 6-19](#)
- [RCC refused by the VQE-S—insufficient bandwidth, page 6-19](#)
- [MPEG Parser is unable to locate the burst start point, page 6-20](#)
- [VQE-S MPEG Parser is unable to locate the ECM PID, page 6-21](#)
- [Burst start point not found within the backfill range, page 6-21](#)
- [No burst start point found—stream is invalid, page 6-22](#)

To perform the troubleshooting activities described in this section you need to log in to the VQE-S AMT. For information on accessing the VQE-S AMT, see [“Logging into and Navigating in the VQE-S AMT” section on page 4-2](#).

To troubleshoot RCC problems, enable debugging of RCC messages on the VQE-S and analyze the debug logs. To enable debugging, see the [“Change VQE-S Debugging” section on page 4-33](#). The debug messages are written to the file `/var/log/vqe/vqe.log`. Alternatively, to view RCC failures, click the channel name in the navigation tree in the VQE-S AMT and click the **RCC Troubleshooting** tab. The RCC Troubleshooting tab displays the last twenty RCC failures on this channel.

### Channel is not configured on the VQE-S

**Explanation:** An RCC fails if the new channel is not configured on the VQE-S. To verify that a channel is configured on the VQE-S, click the **Channel** node in the navigation tree, and verify that the new channel is listed in the channel lineup.

**Remedy:** If the channel is not displayed in the channel lineup, add the channel to the channel configuration using the VCPT. For more information on adding channels, see the [“Adding a Channel” section on page 8](#). After the channel has been added to the channel configuration, send the updated configuration to the VQE-S and the VCDS. For information on deploying channel configurations, see the [“Sending or Pushing Channel Information to Servers” section on page 5](#).

### Channel is not active on the VQE-S

**Explanation:** An RCC fails if the new channel is not active on the VQE-S or if the channel is not receiving RTP packets. To verify that a channel is active on the VQE-S and receiving RTP packets, do the following:

- 
- Step 1** Click the **Channel** node in the navigation tree to expand the channel lineup.
  - Step 2** Click the channel in the lineup.
  - Step 3** Click the **Status/Statistics** tab.

- Step 4** Verify that the Status field is set to active.
- Step 5** Verify that the value of the Received Packets field is greater than zero.
- Step 6** Take note of the value of the Average Stream Rate(Mbps) field.
- Step 7** Click the **Configuration** tab.
- Step 8** Take note of the value of the Multicast IP Address field.
- Step 9** Take note of the value of the Bit Rate(Kbps) field for the original stream.
- Step 10** Verify that the Average Stream Rate(Mbps) for the original stream is within 10% of the configured Bit Rate (Kbps) for the original stream.

---

**Remedy:** If there is a mismatch between the expected bit rate and the actual bit rate, ensure that the configured bit rate represents the peak bit rate expected on the channel.

If the Status of the channel is inactive or if the number of received packets is zero, check that the interface on which the channel has joined is properly configured. To verify that the interface has been configured correctly, do the following:

- Step 1** Click the **Interfaces** node in the navigation tree.
- Step 2** In the Multicast Group table, locate the multicast address of the channel and identify the name of the interface associated with the channel.
- Step 3** Verify that the interface has been configured correctly.




---

**Note** 10 or 100 Mbps interfaces are not supported on the VQE-S.

---

If the interface is configured correctly, verify that the multicast stream is being received by the networking stack. To output a record of all TCP traffic to and from an Ethernet interface to the screen, use secure shell (SSH) to connect to the VQE-S and run the command `/sbin/tcpdump -i <ethx> host <multicast_address>` on the interface as user root.

## RCC is disabled on the channel

**Explanation:** An RCC fails if RCC is disabled on the new channel. To verify that RCC is enabled on a channel, do the following:

- Step 1** Click the **Channel** node in the navigation tree to expand the channel lineup.
- Step 2** Click the new channel in the lineup.
- Step 3** Click the **Configuration** tab.
- Step 4** Verify that the Rapid Channel Change field is set to true.

---

**Remedy:** If the Rapid Channel Change parameter is set to false for the channel, update the channel configuration in VCPT by clicking the Enable Rapid Channel Change check box. For information on updating channel information, see the [“Viewing or Updating Channel Information”](#) section on page 12.

After RCC has been enabled in the channel configuration, send the updated configuration to the VQE-S and the VCDS. For information on deploying channel configurations, see the [“Sending or Pushing Channel Information to Servers” section on page 5](#).

## No connectivity between the VQE-C and the FBT on the VQE-S

**Explanation:** An RCC fails if there is no connectivity between the VQE-C and the feedback target (FBT) of the new channel on the VQE-S.

To verify that the VQE-C can connect to the feedback target of the new channel, do the following:

- 
- Step 1** Click the **Channel** node in the navigation tree to expand the channel lineup.
  - Step 2** Click the new channel in the lineup.
  - Step 3** Click the **Configuration** tab.
  - Step 4** Take note of the IP address in the Feedback Target Address field.
  - Step 5** Ping the feedback target IP address from the VQE-C to verify that it is reachable.
- 

**Remedy:** If there is no connectivity between the VQE-C and the FBT on the VQE-S, check that the channel is active. A channel that is inactive does not have a FBT that is reachable. If the channel is active and a FBT for this channel does not exist, check the VQE system messages in the `/var/log/vqe/vqe.log` file for a FBT failure message.

## No connectivity between the VQE-C and the VQE-S

**Explanation:** An RCC fails if there is no connectivity between the VQE-C and the VQE-S.

To verify that the VQE-C can connect to the service interfaces of the VQE-S, do the following:

- 
- Step 1** Click the **Interfaces** node in the navigation tree.
  - Step 2** In the Interfaces Summary Table, take note of the IP address of each service interface.
  - Step 3** Ping the IP address of each service interface from the VQE-C to ensure it is reachable.
- 

**Remedy:** If there is no connectivity between the VQE-C and the VQE-S service interfaces, fix problems in the network relating to cabling, interface configurations, and routing tables.

## RCC refused by the VQE-S control or data planes

An RCC fails if the RCC is refused by the VQE-S control plane (CP) or data plane (DP). To verify that an RCC has not been refused for a channel by the VQE-S CP or DP, do the following:

- 
- Step 1** Click the **Channel** node in the navigation tree to expand the channel lineup.
  - Step 2** Click the new channel in the lineup.
  - Step 3** Click the **Advanced** button.

- Step 4** Under RCC Debug Counters, verify that the values of the Refused RCC—RCC disabled on DP and Refused RCC—RCC disabled on CP counters are zero.

---

**Explanation:** If the counter Refused RCC-RCC disabled on DP counter has been incremented, the RCC has been refused by the VQE-S DP.

**Remedy:** If an RCC has been refused by the VQE-S DP, verify that the following line is not included in the `/etc/opt/vqes/vcdb.conf` file:

```
vqe.vqes.rcc_disable="true"
```

If the line is present in the file, remove the line, and use the `vqe_cfgtool` command with the `-apply` option to apply the change to the VQE-S.



**Note**

The parameter `vqe.vqes.rcc_disable` is a hidden parameter and should only be used on the direction of the a Cisco technical support representative.

If the counter Refused RCC-RCC disabled on CP is incremented, the RCC has been refused by the VQE-S CP. If the Refused RCC - RCC disabled on CP counter has been incremented, contact your Cisco technical support representative.

## RCC refused by the VQE-S—invalid e-factor

**Explanation:** An RCC fails if the VQE-S refuses the RCC request because the e-factor is invalid. To verify that a valid e-factor has been configured on the VQE-S, check that the value of the VCDB parameter `vqe.vqes.excess_bw_fraction` is within the defined range of 3 to 500 in the `/etc/opt/vqes/vcdb.conf` file.

**Remedy:** If the e-factor value is outside of the permitted range, change the value of the parameter `vqes.excess_bw_fraction` in the `/etc/opt/vqes/vcdb.conf` file, and use the `vqe_cfgtool` command with the `-apply` option to apply the change to the VQE-S.

## RCC refused by the VQE-S—insufficient bandwidth

**Explanation:** An RCC fails if the VQE-S refuses an RCC because there is not enough bandwidth available on the access link to the VQE-C to perform the RCC.

To verify that there is sufficient bandwidth available to perform an RCC, do the following:

- 
- Step 1** Click the **Error Repair and RCC** node in the navigation tree to expand the channel lineup.
  - Step 2** Click the **Statistics** tab.
  - Step 3** Click the **Advanced** button.
  - Step 4** Verify that the total bandwidth available as displayed in the System available output b/w (Mbps) counter under the section CP Output Bandwidth Stats matches the expected total bandwidth of the service interfaces. For example, if two Gigabit Ethernet interfaces are configured and used for the access link, then the value of the System available output b/w (Mbps) counter should be 2000 Mbps.
  - Step 5** Verify that the value of the Committed RCC output b/w (Mbps) counter is less than the value of the RCC output b/w budget (Mbps) counter.
  - Step 6** Click the **Interfaces** node in the navigation tree.

- Step 7** Verify that all service interfaces have a role of *service* and have a status of *Up*. Verify that each service interface is a 1000 Mbps interface.
- 

**Remedy:** If a service interface is a 10 Mbps or a 100 Mbps interface, you need to upgrade to a 1000 Mbps interface. If the committed budget for RCC is close to the maximum budget for RCC, you are close to reaching the scalability limit of the VQE-S.

## MPEG Parser is unable to locate the burst start point

An RCC fails if the VQE-S MPEG parser is unable to locate the burst start point (that is, the Transport Stream Random Access Point [TSRAP]). To verify that the VQE-S is correctly identifying the burst start point, do the following:

---

- Step 1** Click the **Channel** node in the navigation tree to expand the channel lineup.
- Step 2** Click the new channel in the lineup.
- Step 3** Click the **Advanced** button.
- Step 4** Locate the MPEG Parser: Locating a Random Access Point section.
- Step 5** Verify that the value of the Num RAPs found by Adaptation Field RAI bit counter and Num RAPs found by locating I-frame or IDR counter is zero.
- 

**Explanation:** If the value of the Num RAPs found by Adaptation Field RAI counter and the Num RAPs found by locating I-frame or IDR counter has been incremented, it is likely that the VQE-S is unable to find a TSRAP. The VQE-S is optimized to skip the parsing of the Elementary Stream (ES) which contains the actual group of pictures (GOPs). Instead, the VQE-S uses the `random_access_indicator` (RAI) bit in the MPEG2-TS packet header. However, in some deployments, the RAI bit is not set. Without an RAI, random access points (RAPs) may be overlooked as valid RCC burst start points.

**Remedy:** To prevent the VQE-S from skipping the ES, add the following line to the `/etc/opt/vqes/vcdb.conf` file:

```
vqe.vqes.max_rai_gap="0"
```

Use the `vqe_cfgtool` command with the `-apply` option to apply the change to the VQE-S.

**Explanation:** If RCCs continue to fail, it may be that the VQE-S is still unable to find a TSRAP. The VQE-S is also optimized to skip to the beginning of the next MPEG Packetized Elementary Stream (PES) once it determines the picture type. In some deployments, more than one GOP is contained in the PES header. If multiple GOPs are skipped, some RAPs may be overlooked as valid RCC burst start points.

**Remedy:** To prevent the VQE-S from skipping multiple GOPs in a PES header, add the following line to the `/etc/opt/vqes/vcdb.conf` file:

```
vqe.vqes.mpeg_search_limit_disable="true"
```

Use the `vqe_cfgtool` command with the `-apply` option to apply the change to the VQE-S.

## VQE-S MPEG Parser is unable to locate the ECM PID

**Explanation:** When the new channel is scrambled, an RCC fails if the VQE-S MPEG parser is unable to locate the Entitlement Control Messages (ECM) Packet identifier (PID). To verify that the VQE-S is correctly locating the ECM PID, do the following:

- 
- Step 1** Click the **Channel** node in the navigation tree to expand the channel lineup.
  - Step 2** Click the new channel in the lineup.
  - Step 3** Click the **Advanced** button.
  - Step 4** Locate the MPEG Parser: PIDs section.
  - Step 5** Verify that the list of PIDs includes a PID Type (ES Video), with a Stream Type of H.262 or H.264.
  - Step 6** Verify that the list of PIDs includes a PID Type (ECM PID).
  - Step 7** Verify that none of the error counters associated with either the ES Video PID or the ECM PID have been incremented.
- 

**Remedy:** If either the ES Video PID or the ECM PID are not included under the list of PIDs, or if the error counters associated with either PID have been incremented, check the stream configuration and contact your Cisco technical support representative.

## Burst start point not found within the backfill range

**Explanation:** An RCC is rejected by the VQE-S if it is unable to find a burst start point (TSRAP) within the backfill range sent by the VQE-C. The VQE-C sends the parameters `min_rcc_backfill` and `max_rcc_backfill` in its RCC request. The VQE-S must find a TSRAP within the range provided by these two parameters. If none is found, the RCC is rejected.

The following is an example of a VQE-C PLI APP message (that is, a request for an RCC) taken from a VQE-S log file:

```
Feb 5 10:35:53 saturn-iptv vqes_cp: <{vqes-era}>Computed PLII APP
received=TRUE, min_rcc_backfill=200, max_rcc_backfill=2105; use
min_ref_a=1233848151597, max_age=1233848153492, idr=0
```

In this example, the VQE-C sends a `min_rcc_backfill` value of 200 ms and a `max_rcc_backfill` value of 2105 ms.

The following is an example of the message sent from the VQE-S in response to the RCC request:

```
Feb 5 10:35:53 saturn-iptv vqes_cp: <{vqes-era}>Candidate TSRAP #0
(96598729:1), ref_time=1233848153147(0.545301 secs ago), is_idr:1,
rai:0, pts:10970145, pts_pcr_offset:74430[90kHz ticks]
```

In this example, the VQE-S indicates that it is selecting a burst start point that is 545 ms old and therefore, within the defined range.

If several RCCs have been rejected, check the VQE-S logs to verify that the backfill range for each rejected RCC was sufficiently large enough for the VQE-S to find burst start point within the backfill range.

**Remedy:** It is usually not a viable option to change the size of a GOP stream. Instead, consider increasing the size of the packet pool. For more information on sizing the packet pool, see *VQE-C System Integration Guide*.

## No burst start point found—stream is invalid

**Explanation:** An RCC is rejected by the VQE-S if it is unable to locate a burst start point (TSRAP) in the stream sent by the stream source for one of the following reasons:

- Stream is of a type not supported by the VQE-S— VQE-S supports streams of type MPEG-2 part 2 (H.262) and MPEG-4 part 10 (H.264). The VQE-S does not support other stream types such as MPEG-4 part 2 (H.263) or DigiCipher II (DC II).
- Stream is empty or it is sent with null-padded packets.
- Stream is using a Conditional Access System (CAS) that is not ETSI ETR 289 compliant.
- Stream does not contain Program Map Tables (PMT) or Program Association Tables (PAT)—Priming information required by the VQE-S to perform the RCC is missing.
- Details of the PMT and PAT do not match the details of the stream—Priming information required by the VQE-S to perform the RCC is incorrect.

To verify that the VQE-S is correctly locating the burst start point, do the following:

- 
- Step 1** Click the **Channel** node in the navigation tree to expand the channel lineup.
  - Step 2** Click the new channel in the lineup.
  - Step 3** Click the **Advanced** button.
  - Step 4** Locate the RCC Debug Counters.
  - Step 5** Verify that the RCC Refused—No RAP for stream counter did not increment during the RCC.
- 

**Remedy:** If the RCC Refused—No RAP for stream counter has incremented, verify that the stream source is providing a valid stream for the channel and contact your Cisco technical support representative.

## VQE-C RCC Troubleshooting

As a starting point, use the **show counters** command on the VQE-C command line interface (CLI) to identify how many previous RCC requests have been attempted by the VQE-C and how many have failed. For those RCC requests that have aborted, the output of the **show counters** command provides RCC failure reasons and indicates the number of failures associated with each reason. The following is a sample output from the **show counters** command:

```
vqec# show counters
... Omitted contents ...
--- RCC status ---
-- Channel Change Counters --
requests:          8
rcc requests:      6
  rcc with loss:   0
  rcc aborts:      4
    server   stun   response  response  burst   burst
    rejects  timeout timeout   invalid  start   activity  other
    0         0     0         0         0     4         0
...
```

In this example, the RCC requests field presents the number of channel change requests made by the VQE-C. The RCC with loss field indicates the number of RCCs that did not abort but for which the post-repair loss rcc counter incremented. The number of RCCs aborted per failure reason is presented under the rcc aborts field. The following failure reason counters are presented:

- Server rejects—Number of times an RCC request was rejected by the VQE-S.
- Stun timeout—Number of times a STUN response was not received from the VQE-S.
- Response timeout—Number of times an APP packet (that is, priming information) was not received from the VQE-S.
- Response invalid—Number of times an APP packet received contained invalid contents.
- Burst start—Number of times the first repair packet was not received on time.
- Burst activity—Number of times a burst activity timed out prior to completion.

For further information on using the **show counters** command, see *VQE-C CLI Command Reference*.

The following sections describe how to troubleshoot RCC problems from the VQE-C:

- [RCC not enabled on the VQE-C, page 6-24](#)
- [Problem with priming information sent from the VQE-S, page 6-24](#)
- [First packets from repair burst not received within expected time period, page 6-25](#)
- [No multicast stream, page 6-25](#)
- [Output loss during RCC, page 6-25](#)
- [Output packets dropped, page 6-28](#)

Each section presents possible explanations for RCC problems and provides a remedy for the explanation.

## RCC not enabled on the VQE-C

**Explanation:** RCC must be enabled on the VQE-C for RCC to operate. Use the **show rcc** command on the VQE-C CLI to verify that RCC is enabled. The following is a sample output from the **show rcc** command:

```
vqec# show rcc
rcc: enabled
```

**Remedy:** If RCC is disabled, use the **rcc enable** command from the VQE-C CLI in configuration mode to enable RCC. For more information on enabling RCC, see *VQE-C System Integration Guide*. RCC must also be enabled on the new channel. To verify that RCC is enabled on a channel, either check the channel configuration in the channel lineup from VQE-S AMT or use the **show channel** command on the VQE-C CLI and verify that the RCC field is set to enabled. For more information on verifying the status of RCC from the VQE-S AMT, see the [“RCC is disabled on the channel”](#) section on page 17.

## Problem with priming information sent from the VQE-S

**Explanation:** An RCC may be unsuccessful on the VQE-C because of a problem with the APP packets (that is, priming information) sent by the VQE-S. Possible explanations are as follows:

- APP packet was not received within the `rcc_start_timeout` interval set at the VQE-C.
- APP packet was received by the VQE-C, but was empty.
- APP packet was received by the VQE-S, but was invalid.

To verify from the VQE-C that an RCC has succeeded, use the **show tuner <tuner name> rcc** command and verify that the RCC result field has a value of success. The following is a sample output from the **show tuner <tuner name> rcc** command:

```
vqec# show tuner name tuner1 rcc
Tuner name:                tuner1
... Omitted contents ...
--- RCC status ---
rcc enabled:                true
rcc result:                 success
cp failure reason:         NONE
dp failure reason:         NONE
...
```

If the `rcc result` field displays a value of failure, check the values of the `cp failure reason` field and the `dp failure reason` field.

**Remedy:** The `cp failure reason` field displays the reason why the RCC was aborted by the control plane (CP). If the field displays a value of `APP_Timeout`, the APP packet was not received within the RCC start timeout period set at the VQE-C. See the [“VQE-S RCC Troubleshooting”](#) section on page 16 for possible explanations why APP packets are not sent by the VQE-S within the timeout period.

The `dp failure reason` displays the reason why the RCC was aborted by the data plane (DP). If the field displays a value of `NULL_APP`, an empty APP packet was received. In this case, the VQE-S was unable to process the RCC. To identify why an RCC was refused by the VQE-S, view the Refused RCC counters on the Advanced window of the Error Repair and RCC tab of the VQE-S AMT. For more information on identifying reasons why the VQE-S rejects an RCC, see the [“VQE-S RCC Troubleshooting”](#) section on page 16. If the value of the `dp failure reason` is `INVALID_APP`, one or more of its fields in the APP packet was not set correctly by the VQE-S.

## First packets from repair burst not received within expected time period

**Explanation:** The VQE-C aborts an RCC if it does not receive the first repair packet (specified in the APP packet) from the VQE-S within the period of time specified by the VQE-C System Configuration parameter `rcc_start_timeout` and presents a `FIRST_REPAIR_TIMEOUT` error message on the CLI.

In a deployment that includes a NAT device between the STB and the VQE-S, the VQE-C must be configured to use NAT mode, as specified by the VQE-C System Configuration parameter `sig_mode`.

**Remedy:** Use Wireshark to determine that the unicast repair burst is being sent from the VQE-S and to determine that the repair burst is reaching the STB hosting the VQE-C. If the repair burst is reaching the VQE-C, the VQE-S is operating as intended, and the problem is occurring within the STB.

Furthermore, if the round-trip time on the network is large or inconsistent, it may help to increase the value of the VQE-C System Configuration parameter `rcc_start_timeout`, which increases the amount of time the VQE-C waits for a repair burst to start before failing with a `FIRST_REPAIR_TIMEOUT` error. For more information on configuring the `rcc_start_timeout` parameter, see *VQE Client System Configuration Guide*.

## No multicast stream

**Explanation:** When an RCC unicast burst is received but no multicast burst is received for the primary stream, the RCC appears to start and then stop. To verify that multicast bursts are received after the initial RCC unicast burst, use the `show tuner name <tuner_name> rcc` command on the VQE-C CLI to identify the time the primary packet was received. Verify that the value of the `PRIM` field under Actual Relative Times is a non-zero value. In addition, verify that the first primary sequence field under Output statistics contains a non-zero value. For further information on using the `show tuner name <tuner_name> rcc` command, see *VQE-C CLI Command Reference*. The following is a sample output from the command:

```
vqec> show tuner name 0 rcc
Tuner name: 0
... Omitted contents ...
---Actual relative times (ms)---
  CC      Pli      APP      Rep      Join      Prim      ER      Join-lat
  0        7       11       33      149       204      2422     30
... Omitted contents ...
--- Output statistics ---
first primary sequence: 13767
first repair sequence: 167261298
...
```

In the sample output, the `Prim` field under the Actual relative times (ms) section contains a non-zero value. The first primary sequence field under Output statistics also contains a non-zero value.

**Remedy:** If the multicast burst for the primary stream is not received, verify that IGMP is setup correctly in your network configuration.

## Output loss during RCC

**Explanation:** Video freeze or macroblocking may be observed during an RCC if output loss occurs at the VQE-C. To check for output losses on a tuner, use the `show tuner name <tuner_name> rcc` command. The following is a sample output from this command:

```
vqec> show tuner name 0 rcc
Tuner name: 0
... Omitted contents ...
--- Output statistics ---
  first primary sequence: 3125
```

```

rcc output loss packets: 0
rcc output loss holes: 0
rcc duplicate packets: 26
repairs in 1st nack: 0
first packet output time 34
last packet output time 2363
first packet decode time 183
...

```

Under Output Statistics, the rcc output loss packets field displays the number of missing packets on the output stream and the rcc output loss holes field displays the number of missing packet holes on the output stream. If no output loss has occurred, the value of both fields should be zero. If losses are observed in the network, check your network configuration.

The following are possible explanations why RCC output losses may occur:

- [IGMP join latency, page 6-26](#)
- [Packet pool is not size appropriately, page 6-27](#)
- [Excess bandwidth fraction is larger than the available bandwidth, page 6-27](#)
- [Previous stream is still flowing, page 6-28](#)

## IGMP join latency

**Explanation:** Video freeze or macroblocking may be observed during an RCC if the IGMP join latency is longer than expected. IGMP join latency is the time between a request to join a multicast group and the receipt of the first byte of data for a multicast group. The actual join latency should be less than the or equal to the value of the VCDB parameter `vqe.vqes.igmp_join_variability`. This parameter sets the amount of variability between the fastest and slowest IGMP joins for RCC.

To identify the actual IGMP Join Latency, use the `show tuner name <tuner_name> rcc` command on the VQE-C CLI. For information on using this command, see *VQE-C CLI Command Reference*. The following is a sample output from the `show tuner name <tuner_name> rcc` command:

```

vqec> show tuner name 0 rcc
Tuner name: 0
... Omitted contents ...
---Actual relative times (ms)---
CC      Pli      APP      Rep      Join      Prim      ER      Join-lat
0       7        11       33       149       204       2422    30
...

```

In the sample output, the Join-lat field is displayed under Actual relative times (ms).

**Remedy:** If Join-lat is greater than the value of the VCDB parameter `vqe.vqes.igmp_join_variability`, determine the maximum igmp join latency that will be experienced on your network, and set the VCDB parameter `vqe.vqes.igmp_join_variability` to this value in the `/etc/opt/vqes/vcdb.conf` file. Use the `vqe_cfgtool` command with the `-apply` option to apply the change to the VQE-S.



### Note

Increasing the value of the VCDB parameter `vqe.vqes.igmp_join_variability` increases the VQE-C memory requirements and may lead to RCCs being refused.

A historical view of the IGMP join latencies across STBs is provided by the STB IGMP Join Latency histogram on the VQE-S AMT. To view this histogram, do the following:

**Step 1** Click the **System** node in the navigation tree.

- Step 2** Click the **Histograms** tab.  
The Set-top Box IGMP Latency Histogram is displayed.
- Step 3** Move the slider below the histogram to change the way in which the histogram is displayed.
- 

### Packet pool is not size appropriately

**Explanation:** If the packet pool is not sized appropriately, video freeze or macroblocking may be observed during an RCC, and may continue after an RCC has been cancelled. The packet pool is a fixed size memory buffer pool for storing packet data. To verify that the packet pool buffer is sized appropriately, use the **show pak-pool** command from the VQE-C CLI. The following is a sample output from the **show pak-pool** command:

```
vqec# show pak-pool
global input pak pool stats:
  max entries:           1200
  used entries:          76
  high water entries:    1047
  fail pak alloc drops:  0
```

The high water entries field records a high number of packets allocated in the packet pool memory. The max entries field displays the maximum number of packets that can be allocated from the packet memory pool. If the high water mark value is close in value to the max entries value, the VQE-C has reached the currently configured limit of the packet pool.

**Remedy:** The system configuration parameter `pakpool_size` should be sized appropriately for streams and for associated network characteristics. For more information on sizing the packet pool, see *VQE-C System Integration Guide*.

### Excess bandwidth fraction is larger than the available bandwidth

**Explanation:** Video freeze or macroblocking may be observed during an RCC if there is not enough bandwidth available on the access link to perform an RCC. To verify that the excess bandwidth factor has not exceeded the available bandwidth, check the values of the VCDB parameter `vqe.vqes.excess_bandwidth_fraction` or, in the case of a high definition channel, the VCDB parameter `vqe.vqes.excess_bw_fraction_high_def`. Verify that the values of these parameters are appropriate for the capacity of the access link.



#### Note

The VQE-S does not take FEC into account when calculating available bandwidth. If your deployment uses FEC, consider the bandwidth used by FEC when determining the excess bandwidth fraction.

In your deployment, if the e-factor is determined on a per-client basis, verify that the e-factor calculated based on the VQE-C parameters `max_recieve_bandwidth_sd` and `max_receive_bandwidth_hd` is appropriate for the capacity of the access link.

**Remedy:** If a global e-factor value is used, modify the value of the VCDB parameter `vqe.vqes_excess_bandwidth_fraction` or the VCDB parameter `vqe.vqes.excess_bw_fraction_high_def`. If the e-factor is determined on the per-client basis, modify the value of the VQE-C parameters `max_receive_bandwidth_sd` or `max_receive_bandwidth_hd` to accurately reflect the maximum receive bandwidth.

## Previous stream is still flowing

**Explanation:** Video freeze or macroblocking may be observed during an RCC if the previous stream is still flowing into the VQE-C. If `igmp_immediate_leave` is not configured in the DSLAM, the combined bandwidth of the multicast stream of the previous channel and the bandwidth allocated for RCC on the new stream (the multicast bitrate of the new stream \* [1 + VQE e-factor used for the RCC]) exceeds the bandwidth of the access link. In this scenario, some of the bandwidth is still being consumed by the previous stream, and there is not enough bandwidth remaining on the access link for the unicast burst required to start the RCC for the new channel. The problem disappears as soon as the VQE-C joins the multicast stream for the new channel, usually several hundred milliseconds to several seconds after the start of the unicast burst.

If you want to verify that the previous stream has stopped flowing, connect to the access link using packet capture software such as Wireshark to identify which streams are flowing.

**Remedy:** If the previous stream is still flowing, configure `igmp immediate leave` processing in the DSLAM. Some DSLAMS may not stop the previous stream when an IGMP leave message is received. Instead, the DSLAM may wait until a new multicast stream has been joined before stopping the previous stream. In Cisco VQE Release 3.5.4, a new VQE-C configuration parameter, `rcc_extra_igmp_ip`, allows you to specify a multicast IP address that the VQE-C can join briefly on leaving an old channel and joining a new channel as part of an RCC to stop the flow of the multicast stream of the old channel. For more information on configuring the `rcc_extra_igmp_ip` VCDB parameter, see *VQE Client System Configuration Guide*.

## Output packets dropped

**Explanation:** Video freeze or macroblocking may be observed during an RCC if the capacity of the output packet queue is exceeded and output packets are dropped. To verify that output packets have not been dropped, use the `show tuner name <tuner_name> detail` command to view the value of the `qdrops` field under tuner status.

```
vqec# show tuner name 0 detail
Tuner name: 0
... Omitted contents ...
--- NAT status ---
... Omitted contents ...
qinputs: 92026859
qdrops: 82586551
qdepth: 300
qoutputs: 9440008
...
```

If the `qdrops` field has been incremented, the set-top box (STB) decoder is not serving the VQE-C buffer fast enough to display the stream.

**Remedy:** If output packets are being dropped, increase the value of the `output_pakq_limit` parameter on the VQE-C. For more information on configuring the `output_pakq_limit`, see the *VQE-C System Integration Guide*.

# Using the `vgereport` Command

The `vgereport` command can be useful for VQE troubleshooting. You can use the `vgereport` command to gather information on the software and hardware configuration of the VQE system. The information can be used by the VQE administrator or Cisco technical support representative to diagnose problems with VQE software or with the Cisco Content Delivery Engine 110 (CDE110) hardware.



## Caution

The `vgereport` 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 `vgereport` command is as follows:

```
vgereport [-h | -help]
```

## Syntax Description

<b>-h   -help</b>	Displays help information.
-------------------	----------------------------

## Usage Guidelines

The `vgereport` 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 representatives.



## Note

You must log in as root to execute the `vgereport` command.

The `vgereport` command can be executed on the CDE110 that hosts the VQE-S or on the CDE110 that hosts VCPT. The `vgereport` executable is located at `/opt/vqes/bin/vgereport`.

All information gathered is considered confidential, and Cisco uses this information for diagnostic purposes only.

## Examples

The following example shows the execution of the `vgereport` command and some abbreviated output:

```
[root@system ~]# /opt/vqes/bin/vgereport
```

```
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.

```

## Gathering Information for a Service Request

If you are experiencing a problem with Cisco VQE and need to submit a service request to Cisco, please gather and provide the following information to assist Cisco technical support representatives in diagnosing your issue:

- Report file that is generated from the **vqereport** command for issues involving the VQE-S or VQE Tools server.
- For an issue involving VQE-C, output from the following commands:
  - **show tuner all detail**
  - **show pak-pool**
  - **show counters**
  - **show channel**
  - **show system**

For information on the **vqereport** command, see the “Using the vqereport Command” section on page 29.

For information on submitting a service request, see the monthly *What’s New in Cisco Product Documentation* at:

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

## 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 the VQE-S, issue the following command:

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

- To start the VQE-S, issue the following command:

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

- To restart (stop and then start) the VQE-S, issue the following command:

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

---

# Stopping, Starting, and Restarting VCDS

The 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
```

---

# Resetting the Root Password on the VQE-S or VQE Tools Server

To reset the password on the VQE-S or the VQE Tools server, you need to boot into single-user mode from the GRUB loader and reset the password. To reset the password, do the following:

---

**Step 1** Connect to the serial console and reboot the VQE-S or the VQE Tools server by issuing the following command:

```
# reboot
```

The server reboots.

**Step 2** Press any key when the following message is displayed.

```
Press any key to continue.  
Press any key to continue.  
Press any Key to continue.
```

Red Hat Linux is selected as the operating system and the Grub Loader screen is displayed.

**Step 3** Select the entry "Red Hat Enterprise Linux Server (2.6.18-157.el5)" if not already selected, and press **e**.

**Step 4** Using the arrow keys, move the cursor to select the following line:

```
kernel /boot/vmlinuz-2.6.15-1-686 root=dev/sda1 ro
```

**Step 5** Press **e** to enter edit mode.

**Step 6** Using the arrow keys, move the cursor to the end of the line, press the **Spacebar** and enter **single**.

For example:

```
grub edit > kernel /boot/vmlinuz-2.6.15-1-686 root=dev/sda1 ro single
```

“single” is appended to the end of the line.

**Step 7** Press **Enter** to exit edit mode and return to the Grub Loader screen.

- Step 8** Press **b** to boot the Linux kernel into single user mode.  
The `sh-3.2#` prompt is displayed.
- Step 9** Enter **passwd** and specify the new password. For example:  
`sh-3.2# passwd new-password`
- Step 10** Issue the following command to reboot the VQE-S or the VQE Tools sever:  
`# reboot`  
The system reboots.
- Step 11** Login to the server using the new password.  
Your root password has been changed.
-



# CHAPTER 7

## Configuring VQE Server and VQE Tools

This chapter describes the following Cisco VQE Configuration Management System software components that reside on the VQE-S and the VQE Tools server: VQE Configuration Tool, Configuration Engine, and the VCDB Parser. The chapter also provides task-based information on the following topics:

- [Managing /etc Configuration Files Using the VQE CMS, page 7-2](#)
- [Using the VQE Configuration Tool, page 7-3](#)
- [VQE Configuration Engine, page 7-11](#)
- [VCDB Parser, page 7-13](#)
- [Manually Editing the VCDB File, page 7-14](#)
- [Using the VQE Configuration Tool Command-Line Options, page 7-18](#)

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 7-1](#) provides acronyms or terms and descriptions for the major components of the VQE Configuration Management System that you need to be familiar with.

**Table 7-1 VQE Configuration Management System Components**

Acronym or Term	Expansion and Description
VCDB	<i>VQE Configuration Database</i> stores key-value pairs with the parameters and values you have specified with Configuration Tool or by manually editing the <code>vcdb.conf</code> file (the VCDB file).
CT	<i>VQE Configuration Tool</i> 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 (VQE-S) or a VQE Tools system. See the <a href="#">“Using the VQE Configuration Tool”</a> section on page 7-3.
CE	<i>VQE Configuration Engine</i> is used to apply the configuration values in VCDB ( <code>vcdb.conf</code> ) to the running the 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 <a href="#">“VQE Configuration Engine”</a> section on page 7-11.

Table 7-1 VQE Configuration Management System Components (continued)

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 the VQE-S or the 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

Starting with Cisco VQE Release 3.0, the configuration files under the /etc directory can be managed by managing /etc configuration files with the VQE CMS (see section [Managing /etc Configuration Files with the VQE CMS, page 7-2](#))

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.

VQE is intended to be a closed system. As of Cisco VQE Release 3.0, all configuration should be done, whenever possible, using the VQE CMS.

There is no known deployment where manual editing is necessary. Furthermore, there is no support for any deployment where this is done without the permission of Cisco support. However, if you do manually edit /etc configuration files, these 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) are, in most cases, 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.

## 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-S 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 7-14.

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 7-18.

**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 7-2 describes the choices on the CT Root Menu. You enter the number or letter for your choice.

**Table 7-2 CT Root Menu Choices**

Choice	Description
1) System Parameters	Configures the system parameters
2) Network Parameters	Configures the network parameters. Contains sub-menus Interface Parameters and Routing 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 <i>are not applied</i> to the configuration files under /etc.
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 <i>are not saved</i> .

## Using the Configuration Tool Menus

The System Parameters, SNMP Parameters, Interface Parameters, Routing Parameters and the 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) Trusted Provisioning Client(s)           []
7) Remote Syslog Host(s)                    []
8) SNMP Parameters                          []
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 7-3](#) tells you where to find guidance on the system, network, and the 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 7-14](#).

**Table 7-3** *Where To Find Information on Configuration Tool Parameters*

Configuration Tool Parameter	Where To Find Information
<b>System Parameters</b>	
Hostname	<a href="#">Hostname for the CDE110, page 2-24</a>
DNS Server(s) DNS Search Domain	<a href="#">Domain Name System (DNS) IP Addresses and a Search Domain, page 2-24</a>
Timezone	<a href="#">System Timezone, page 2-25</a>
NTP Server(s)	<a href="#">NTP Server IP Addresses, page 2-25</a>
Trusted Provisioning Client(s)	<a href="#">Trusted Provisioning Clients, page 2-27</a>
Remote Syslog Host(s)	<a href="#">Remote Syslog Hosts, page 2-28</a>
<b>SNMP Parameters</b>	
SNMP RO Community String SNMP System Location SNMP System Contact SNMP Trap Listeners	<a href="#">SNMP Read-Only Community String, Location, Contact, and Trap-Listener IP Addresses or Hostnames, page 2-28</a>
Enable Syslog Traps	<a href="#">Sending SNMP Traps, page 2-28</a>
Syslog Trap Priority	<a href="#">Sending SNMP Traps, page 2-28</a>
Enable Channel Up/Down Traps	<a href="#">Sending SNMP Traps, page 2-28</a>
<b>Interface Parameters</b>	
Eth1 Interface IP/Mask Eth2 Interface IP/Mask Eth3 Interface IP/Mask Eth4 Interface IP/Mask Eth5 Interface IP/Mask Eth6 Interface IP/Mask	<a href="#">Ethernet Interface Configuration: IP Address and Prefix Length, page 2-25</a>  <b>Note</b> 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.
Bond1 IP/Mask and members Bond2 IP/Mask and members Bond3 IP/Mask and members	<a href="#">Bond Interfaces on a VQE-S, page 2-15</a>  <b>Note</b> Earlier models of the CDE110 have four Ethernet ports (eth1 to eth4) and support up to two bond interfaces (bond1 and bond2).
Management Interface(s)	<a href="#">Interface for a Management Network, page 2-20</a>
<b>Static Routing Parameters</b>	

**Table 7-3** Where To Find Information on Configuration Tool Parameters (continued)

Configuration Tool Parameter	Where To Find Information
Static Route(s)	<a href="#">Static Route Configuration: IP Address, Prefix Length, and Gateway Address, page 2-26</a> and <a href="#">Configuring Static Routes, page 2-19</a>
<b>OSPF Parameters</b>	
OSPF Parameters	<a href="#">OSPF Configuration (VQE-S Host Only), page 2-28</a>
<b>VQE-S Parameters (for VQE-S Host Only)</b>	
Log Priority	vqe.vqes.log_priority parameter in <a href="#">Table A-1</a>
Excess Bandwidth Fraction	vqe.vqes.excess_bw_fraction parameter in <a href="#">Table A-4</a>
Traffic (Ingest+Service) Interface(s)	<a href="#">Interfaces for VQE-S Traffic (Ingest and Services) (VQE-S Host Only), page 2-30</a>
Ingest Interface(s)	<a href="#">Interfaces for VQE-S Ingest Traffic (VQE-S Host Only), page 2-29</a>
Service Interface(s)	<a href="#">Interfaces for VQE-S Services Traffic (VQE-S Host Only), page 2-30</a>

## 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. 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) Trusted Provisioning Client(s):          []
7) Remote Syslog Host(s):                   []
8) SNMP Parameters:                         []

```

```
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.

Enter the Hostname of this server: **vqe\_server1**

For a parameter that allows only one definition, enter the needed data for the parameter. 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. 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) Trusted Provisioning Client(s)           []
7) Remote Syslog Host(s):                   []
8) SNMP Parameters:                         []
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** 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 a DNS server IP address: 5.6.7.8
Enter a DNS server IP address:

```

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:                       []
...

```

**Step 3** Repeat Step 1 and Step 2 to add further definitions for this parameter.

---

When configuring static routes, each static route is displayed as a sub-menu of the Static Route(s) menu. For example:

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)    0.0.0.0/0 via 10.86.21.1
   1.2)    0.0.0.0/0 via 10.86.21.2
P) Go to Parent Menu
R) Go to Root Menu

```

## Entering New Values for Parameters That Have a Currently Defined Value

For a parameter that has one or more currently defined values in VCDB, with the exception of the Static Route(s) parameter, 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. 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:
```

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 before 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
...

```

In the case of the Static Route(s) parameter, when you add a new static route, it is displayed as a sub-menu of the Static Route(s) menu. In the following example, static route 0.0.0.0/0 via 10.86.21.1 exists:

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)    0.0.0.0/0 via 10.86.21.1
P) Go to Parent Menu
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 [].

A new static route 192.0.0.0/8 via 10.2.9.1 is created:

Enter your choice: **1**

Add new static routes by entering destination subnet IP/Prefix and gateway IP pairs when prompted.

To configure a default route, enter 0.0.0.0/0 as the destination subnet IP/Prefix.

To specify a specific gateway interface (optional), add it to the end of the gateway IP, separated by ":" (e.g. "5.6.7.8:eth3").

To complete the configuration, press <Enter> at the prompt without entering data.

Enter the destination subnet in IP/Prefix format (e.g., 1.0.0.0/8): 192.0.0.0/8

Enter the gateway IP address: 10.2.9.1

Enter the destination subnet in IP/Prefix format (e.g., 1.0.0.0/8)

The new static route is added as a sub-menu of the Static Route(s) menu. For example:

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)    0.0.0.0/0 via 10.86.21.1
   1.2)    192.0.0.0/8 via 10.2.9.1
P) Go to Parent Menu
R) Go to Root Menu

```

## 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”. 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) Trusted Provisioning Client(s) []
7) Remote Syslog Host(s): []
8) SNMP Parameters:       []
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**

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
...

```

If the static route parameter has more than one value defined, and you want to restore the default value of a specific route, enter the number of the sub-menu for that specific route followed by the letter “d”. For example:

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)    0.0.0.0/0 via 10.86.21.1
   1.2)    0.0.0.0/0 via 10.86.21.2
P) Go to Parent Menu
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: **1.2d**

The existing value for that parameter definition in VCDB is deleted. In this example, when the Static Route(s) menu is displayed, the menu shows that the static route 0.0.0.0/0 via 1.86.21.2 has been deleted.

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)    0.0.0.0/0 via 10.86.21.1
P) Go to Parent Menu
R) Go to Root Menu

```

If you want to restore all static routes to their default value, enter the number for the static route(s) menu followed by the letter “d”. For example:

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s):
   1.1)      0.0.0.0/0 via 10.86.21.1
   1.2)      0.0.0.0/0 via 10.86.21.2
P) Go to Parent Menu
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**

Any existing values for the static route parameter that have been set in VCDB are deleted. The default value for the parameter is in effect. In this example, static routes 0.0.0.0/0 via 10.86.21.1 and 0.0.0.0/0 via 10.86.21.2 have been deleted.

VQE Configuration Tool <Static Routing Parameters> Menu:

```

1) Static Route(s): []
P) Go to Parent Menu
R) Go to Root Menu

```

## 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 7-18.

1. When CE is invoked, it does the following: 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 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.

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. Syslog-NG
  2. SNMP Master Agent
  3. Syslog SNMP Subagent
  4. network and routing
  5. iptables
  6. Network Time Protocol
  7. VQE-S Process Monitor (VQE-S only)
  8. VQE-S SNMP Subagent (VQE-S only)
  9. VCDS SNMP Subagent (VQE Tools 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 6-2](#).

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 7-18](#).

# 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 7-14](#)
- [Understanding the `vcdb.conf.sample` File, page 7-15](#)

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 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 7-18](#).



## 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 = "10.2.9.2/24"
```

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.
- Key and its value are separated by an equal sign (=).
- Value is enclosed by quotation marks ("value").
- Comment line starts with #. The VCDB Parser ignores these lines.
- 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 Cisco 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 `vcdb.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 7-4](#) lists the `vcdb.conf.sample` reference information that describes each VCDB parameter.

**Table 7-4** 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. <ul style="list-style-type: none"> <li>Integer—Whole number.</li> <li>Float—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.</li> <li>String—One or more characters. The set of characters allowed varies depending on the parameter.</li> <li>Boolean—Either true or false.</li> <li>IP—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.</li> <li>IP_PREFIX—IP address and prefix length in the form <i>ip-address/prefix-length</i> (for example, 10.0.0.0/8). The <i>ip_address</i> is the same as in IP. The <i>prefix-length</i> must be in the range 0 to 32.</li> <li>Route—Route in the format <i>ip-address/prefix-length via ip-address</i> (for example, 10.0.0.0/8 via 10.2.9.1). Each <i>ip_address</i> is the same as in IP. The <i>prefix-length</i> must be in the range 0 to 32.</li> <li>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.</li> </ul>
Default value	Specifies a default value. If there is no default value, this field is blank.
Required	Specifies one of the following: <ul style="list-style-type: none"> <li>Y—Parameter must be defined, and there is no default value.</li> <li>N—Parameter does not have to be defined.</li> </ul> <p>You can define a parameter by using the Configuration Tool or by manually editing the <code>vcdb.conf</code> file with a text editor.</p>
Service interruption	Indicates whether VQE services are interrupted when the parameter definition is applied to the relevant configuration file (for example, when you invoke the <code>vqe_cfgtool</code> command with the <code>-apply</code> option).

**Table 7-4** Parameter Information in the *vcdb.conf.sample* File (continued)

Field	Description
Allow multiple definition	Specifies one of the following: <ul style="list-style-type: none"> <li>• Y—Parameter can be specified more than once in the <i>vcdb.conf</i> file.</li> <li>• N—Parameter can be specified only once in the <i>vcdb.conf</i> file.</li> </ul>
Target /etc file	Specifies the configuration file under /etc that is written to when the parameter is applied. Also indicates the configuration items that are written to the /etc configuration file.  In the <code>system.global.hostname</code> parameter example preceding this table, “Target /etc file” indicates that a line <code>127.0.0.1 host_name</code> is written to the file <code>/etc/hosts</code> , and a line <code>HOSTNAME=host_name</code> is written to the <code>/etc/sysconfig/network</code> file. The <i>host_name</i> is the value specified for <code>system.global.hostname</code> . The exact syntax for the line that is 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_config | -help |
            -parse [full_pathname] | -restore full_pathname | -sanity_check | -version]
```

Syntax Description	
<b>-apply [prompt-off]</b>	Launches the Configuration Engine to apply the values in VCDB to the server <code>/etc</code> configuration files.  If you specify <b>prompt-off</b> , no interactive questions are displayed before changes are made to the running configuration.
<b>-backup</b>	Copies all files under <code>/etc</code> into a tar file and saves the tar file in <code>/vqe-etc/vqe-release-hostname-timestamp.tar.gz</code> .
<b>-config</b>	Launches the Configuration Tool so that you can modify the VQE configuration parameter values that are stored in VCDB.
<b>-fix_config</b>	Discards the current copy of each <code>/etc</code> configuration file where there is a checksum mismatch and replaces it with the original copy of the file that comes with the RPM package.
<b>-help</b>	Displays information on how to use the <b>vqe_cfgtool</b> command and its options. If no valid option is specified when <b>vqe_cfgtool</b> is invoked, <b>-help</b> is the default.
<b>-parse [full_pathname]</b>	Performs validation of the VCDB contents (parameters, values, syntax, and so on) for the current <code>vcdb.conf</code> file.  If <i>full_pathname</i> is specified, that file is parsed rather than the current <code>vcdb.conf</code> file.
<b>-restore full_pathname</b>	Extracts the contents of the tar file specified in <i>full_pathname</i> , and replaces all <code>/etc</code> configuration files with the tar file contents. The tar file is typically created with <b>vqe_cfgtool -backup</b> .
<b>-sanity_check</b>	Compares the parameter values in VCDB with the values in the <code>/etc</code> configuration files, and displays any differences on the command line.
<b>-version</b>	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) 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. For a detailed description of Configuration Engine processing, see the “[VQE Configuration Engine](#)” section on page 7-11.

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 7-3.

#### **-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 7-13.

#### **-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 a 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 7, “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 7-14](#)

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 (RCC) parameters
- [Table A-4](#)—VQE-S Unicast Retransmission and RCC parameters (parameters that affect the behavior of both Unicast Retransmission and RCC)
- [Table A-5](#)—VQE-S RTCP Exporter parameters
- [Table A-6](#)—System parameters
- [Table A-7](#)—Interface parameters
- [Table A-8](#)—Static Routing parameters
- [Table A-8](#)—OSPF 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 preceding information and 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"	<p>Logging level for all VQE-S processes. The range is from 0 to 6. Logging levels are as follows:</p> <ul style="list-style-type: none"> <li>• 0—Emergency (System is unusable)</li> <li>• 1—Alert (Action must be taken immediately)</li> <li>• 2—Critical (critical condition)</li> <li>• 3—Error (error condition)</li> <li>• 4—Warning (warning condition)</li> <li>• 5—Notice (normal but significant condition)</li> <li>• 6—Info (informational condition)</li> </ul> <p>Logging levels go from least verbose to most verbose. The Emergency level generates the smallest number of messages, and the Info level generates the most messages. By default, VQE-S logging messages are written to the file /var/log/vqe/vqe.log.</p> <p>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.</p> <p>For information on configuring VQE-S debugging messages, see the <a href="#">“Change VQE-S Debugging” section on page 4-33</a>.</p> <p>[CT: VQE-S Parameters &gt; Log Priority]</p>
vqe.vqes.max_pkts="1000000"	Maximum number of packet buffers in the VQE-S Cache Manager. Allowed range is 100,000 to 1,300,000.

Table A-1 VQE-S Global Parameters (continued)

Parameter and Default Value (if any)	Description
vqe.vqes.vqe_interfaces="eth1,eth2,eth3,eth4,eth5,eth6"	<p>Names of the interfaces to be used for ingest of multicast streams, Unicast Retransmission and RCC traffic, and other non-management VQE-S traffic. Multiple interface names should be separated by a comma without any space between names. If this parameter is used, the following rules apply:</p> <ul style="list-style-type: none"> <li>• If this parameter is specified, the vqe.vqes.vqe_ingest_interfaces and vqe.vqes.vqe_service_interfaces parameters must not be specified.</li> <li>• If a dedicated interface is used for management traffic, it should not be specified in this parameter.</li> <li>• Multiple Ethernet interfaces or multiple bond interfaces may be specified in this parameter.</li> <li>• Ethernet interface that is a member of a bond interface must not be specified in this parameter.</li> </ul> <p><b>Note</b> For load balancing to work effectively, each interface to the access or distribution network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot be specified in this parameter.</p> <p>Allowed values are eth1 to eth6 or bond1 to bond3. Interfaces eth5, eth6, and bond3 are available only on CDE110 servers that include the Intel PRO/1000 PT Dual Port Server Adapter.</p> <p>[CT: VQE-S Parameters &gt; Traffic (Ingest+Service) Interface(s)]</p>
vqe.vqes.vqe_ingest_interfaces=""	<p>Names of the interfaces to be used for ingest of multicast streams. Multiple interface names, separated by a comma without any space between names, should be specified in this parameter. If this parameter is used, the following rules apply:</p> <ul style="list-style-type: none"> <li>• At least one VQE-S services interface must be specified in the vqe.vqes.vqe_service_interfaces parameter.</li> <li>• Parameter vqe.vqes.vqe_interfaces must not be specified.</li> <li>• If a dedicated interface is used for management traffic, it must not be specified in this parameter.</li> <li>• Multiple Ethernet interfaces or multiple bond interfaces may be specified in this parameter.</li> <li>• Ethernet interface that is a member of a bond interface must not be specified in this parameter.</li> </ul> <p><b>Note</b> For load balancing to work effectively, each interface to the distribution network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot not be specified in this parameter.</p> <p>Allowed values are eth1 to eth6 or bond1 to bond3. Interfaces eth5, eth6 and bond3 are available only on CDE110 servers that include the Intel PRO/1000 PT Dual Port Server Adapter.</p> <p>[CT: VQE-S Parameters &gt; Ingest Interface(s)]</p>

Table A-1 VQE-S Global Parameters (continued)

Parameter and Default Value (if any)	Description
vqe.vqes.vqe_service_interfaces=""	<p>Names of the interfaces to be used for delivering VQE-S services—Unicast Retransmission, RCC traffic, and other non-management VQE-S traffic. Multiple interface names should be separated by a comma without any space between names. If this parameter is used, the following rules apply:</p> <ul style="list-style-type: none"> <li>At least one ingest interface for incoming multicast streams must be specified in the vqe.vqes.vqe_ingest_interfaces parameter.</li> <li>Parameter vqe.vqes.vqe_interfaces must not be specified.</li> <li>If a dedicated interface is used for management traffic, it must not be specified in this parameter.</li> <li>Multiple Ethernet interfaces or multiple bond interfaces may be specified in this parameter.</li> <li>Ethernet interface that is a member of a bond interface must not be specified in this parameter.</li> </ul> <p><b>Note</b> For load balancing to work effectively, each interface to the access network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot not be specified in this parameter.</p> <p>Allowed values are eth1 to eth6 or bond1 to bond3. Interfaces eth5, eth6, and bond3 are available only on CDE110 servers that include the Intel PRO/1000 PT Dual Port Server Adapter.</p> <p>[CT: VQE-S Parameters &gt; Service Interface(s)]</p>
vqe.vqes.rtcp_dscp="24"	DSCP <sup>1</sup> value for transmitted RTCP packets. The default value (24) is for the CS3 selector, which is used for broadcast video. The range is from 0 to 63.
vqe.vqes.rtp_inactivity_timeout="300"	Amount of time or the inactivity timeout on received RTP <sup>2</sup> streams, in ms. If no packets are received on an input channel for this amount of time, the channel is declared inactive until the next input packet is received for that stream. The range is from 10 to 900.
vqe.vqes.stun_enable="true"	<p>Specifies whether the STUN<sup>3</sup> Server is enabled. The value <i>true</i> enables the STUN Server, and <i>false</i> disables the STUN Server.</p> <p>Unless you are sure that no STBs<sup>4</sup> being serviced by the VQE-S are behind NAT devices, we recommend that the STUN Server be enabled.</p>
vqe.vqes.stun_dscp="-1"	<p>DSCP value for STUN Server binding responses.</p> <ul style="list-style-type: none"> <li>If the value -1 is specified, the DSCP value for the STUN binding response is set to the DSCP value in the STUN binding request.</li> <li>If a value other than -1 is specified, the DSCP value for the STUN binding response is set to the value given.</li> </ul> <p>The range is from -1 to 63.</p>
vqe.iptables.trusted_vcpt=""	Starting with Cisco VQE Release 3.2, this parameter is deprecated. Use the system.iptables.trusted_provisioner parameter.

1. DSCP = Differentiated Services Code Point.

2. RTP = Real-time Transport Protocol.

3. STUN = Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NATs)

4. STB = set-top box.

**Table A-2 VQE-S Unicast Retransmission (Error Repair) Parameters**

Parameter and Default Value (if any)	Description
vqe.vqes.client_er_policing="true"	<p>Specifies whether per-VQE-C<sup>1</sup> policing is enabled for Unicast Retransmission (error repair) packets. The value <i>true</i> enables per-VQE-C policing, and <i>false</i> disables per-VQE-C policing.</p> <p>The VQE-C policing mechanism is intended to limit the fraction of the VQE-S error-repair resources that can be consumed by a single VQE-C on the STB.</p> <p>When per-VQE-C policing is enabled, the policer is tuned by two parameters: vqe.vqes.client_er_tb_rate_ratio and vqe.vqes.client_er_tb_depth.</p>
vqe.vqes.client_er_tb_rate_ratio="5"	<p>Per-client policing token rate (percentage of stream rate) for each VQE-C for Unicast Retransmission. The range is from 1 to 100.</p> <p>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 is set the per-client policer token rate to 18 packets per second.</p> <p>Increasing this parameter increases the maximum load that a single STB can put on the VQE-S. By default, each VQE-C is permitted to request up to five percent of the overall stream bandwidth for whatever channel it is watching.</p> <p>In a situation with only a few VQE-Cs, some or all of which have very high error rates, it may be desirable to increase this parameter to allow each client to get more errors repaired. In a situation with a large number of VQE-Cs, it may be necessary to decrease this parameter to prevent a small proportion of misbehaving or very error-prone client connections from consuming a disproportionate fraction of the VQE-S error-repair resources.</p> <p>The VQE-S AMT channel statistics for each channel provide data that you can use to tune the VQE-C policing mechanism. In the Channel Statistics window, click <b>Advanced</b>. The Advanced Channel Debug Stats include the following parameters that indicate how many error-repair requests were refused because the VQE-S is overloaded and how many were refused because of per-client policing.</p> <ul style="list-style-type: none"> <li>• Dropped repair pkts by Packet Policers—If the server is overloaded with error repairs, this statistic may be an indication that the per-client policing should be lowered.</li> <li>• 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.</li> </ul>
vqe.vqes.reserved_er_bw="543200000"	<p>Total amount of bandwidth (in bits per second) dedicated to Unicast Retransmission. The bandwidth pools on a VQE-S include available non-management, output interface bandwidth. The range is from 0 to 543200000.</p> <p>The VQE-S separates the output interface bandwidth that is dedicated to Unicast Retransmission. The amount of bandwidth specified in this parameter is dedicated to Unicast Retransmission with the remainder used for RCC. This parameter allows the amount of output interface bandwidth dedicated to Unicast Retransmission to be reduced so that the bandwidth is available for RCC instead.</p>

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"	<p>Length of time (in milliseconds) needed to fill the per-VQE-C policer bucket for Unicast Retransmission (error repair). The range is from 1 to 60,000.</p> <p>The bucket <i>depth</i> 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 (<i>depth</i>) of the policer bucket is calculated as follows:</p> <p>maximum number of tokens =  <math>(\text{client\_er\_tb\_rate\_ratio} * \text{stream packet rate} * \text{client\_er\_tb\_depth})</math></p> <p>The bucket size should be set large enough to cover the maximum burst loss that may ordinarily occur on a client STB. In most cases, the default value for vqe.vqes.client_er_tb_depth should be adequate.</p>
vqe.vqes.er_cache_time="3000"	Maximum time interval (in milliseconds) to cache the original source stream packets for Unicast Retransmission (error repair). The range is from 100 to 5000.
vqe.vqes.rtp_retrans_dscp="0"	Starting with Cisco VQE Release 3.3, this parameter is deprecated. Use the vqe.vqes.rtp_er_dscp and vqe.vqes.rtp_rcc_dscp parameters.
vqe.vqes.rtp_er_dscp="0"	DSCP value for RTP packets for Unicast Retransmission. The vqe.vqes.rtp_rcc_dscp parameter can be used for DSCP marking of RTP packets for RCC. The range is from 0 to 63.

1. VQE-C = VQE client.

Table A-3 VQE-S RCC Parameters

Parameter and Default Value (if any)	Description
vqe.vqes.fastfill_enable="false"	Specifies whether FDBF <sup>1</sup> is enabled for RCC to reduce decoder buffering time. The value <i>true</i> enables FDBF, and <i>false</i> disables FDBF.
vqe.vqes.buff_size_preroll_max="1500"	If FDBF is enabled for RCC, specifies the maximum assumed delay (in milliseconds) for the PTS-PCR offset (Presentation Time Stamp-Program Clock Reference offset) for all streams going through the VQE-S. The parameter value is used only when sizing the VQE-S channel buffers. If FDBF is not enabled, this parameter is ignored. The range is from 0 to 10,000.
vqe.vqes.igmp_join_variability="100"	<p>Amount of variability (in milliseconds) between the fastest and slowest IGMP joins for RCC. The range is from 0 to 1000.</p> <p><b>Note</b> This parameter can have a large impact on the amount of bandwidth consumed by RCC. It needs to be carefully tuned for a deployment.</p>

Table A-3 VQE-S RCC Parameters (continued)


Parameter and Default Value (if any)	Description
vqe.vqes.max_idr_penalty="0"	<p>For MPEG-4 only, the maximum penalty (in milliseconds) that is permitted to begin an RCC burst with an instantaneous decoding refresh (IDR) frame rather than I-frame. The range is 0 to 10000.</p> <p>In cases in which there are several MPEG RAPs<sup>2</sup> 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 is 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.</p>
vqe.vqes.rap_max_interval="2000"	Maximum time interval (in milliseconds) between MPEG RAPs that the VQE-S supports for RCC operations. The range is 500 to 5000.
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 <i>fast leave</i> mechanism in the access node (for example, a DSLAM). The range is 0 to 100.
vqe.vqes.rcc_mode="conservative"	<p>RCC mode. Can be specified as either of these values:</p> <ul style="list-style-type: none"> <li>aggressive—Conserves bandwidth if all DSLAMs that may receive an RCC burst from the VQE-S are configured to give priority to the primary multicast video traffic over the unicast RCC burst traffic.</li> <li>conservative—Used when the DSLAM does not have the required QoS capability for aggressive mode.</li> </ul> <p>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 causes degraded video quality during RCC operations for customers attached to DSLAMs that are not properly configured for aggressive mode RCC.</p> <p> <b>Caution</b> 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 in which such congestion may have undesirable side effects, such as loss of data or voice traffic on the access link.</p>

Table A-3 VQE-S RCC Parameters (continued)

Parameter and Default Value (if any)	Description
vqe.vqes.rtp_hold_time="20"	<p>Amount of time (in milliseconds) to delay before making a packet in the Data Plane cache available for RCC to allow for reordering of received packets. The range is from 0 to 500.</p> <p>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.</p>
vqe.vqes.rtp_rcc_dscp="-1"	<p>DSCP value for transmitted RTP packets sent for RCC. If the value -1 is specified, the DSCP value is set to the value of vqe.vqes.rtp_er_dscp.</p> <p><b>Note</b> Use of the value -1 provides backward compatibility with earlier Cisco VQE releases that had only the vqe.vqes.rtp_er_dscp parameter, which was used for DCSP marking of RTP packets for both Unicast Retransmission and RCC.</p> <p>The range is from -1 to 63.</p>

1. FDBF = fast decoder buffer fill.
2. RAP = random access points.



**Note** Table A-4 lists parameters that affect the behavior of both Unicast Retransmission and RCC.

**Table A-4** VQE-S Unicast Retransmission and RCC Parameters

Parameter and Default Value (if any)	Description
vqe.vqes.unicast_reservation="20"	<p>For CDE110 Ethernet interfaces, percentage of total input bandwidth reserved for non-ingest traffic. This parameter specifies the amount of input bandwidth that is not to be allocated to receiving multicast streams. The range is from 0 to 100.</p> <ul style="list-style-type: none"> <li>If the interface is used for both VQE-S ingest and services, the reservation should include sufficient bandwidth for receiving Unicast Retransmission and RCC requests, RTCP reports from the STBs, and control traffic, such as IGMP and RTCP. Recommended value range is from 20 to 40.</li> <li>If the interface is used for VQE-S ingest only, the reservation should include sufficient bandwidth for incoming control traffic, such as IGMP and RTCP. Recommended value is 5.</li> </ul>
vqe.vqes.max_client_bw="0"	<p>Maximum access link bandwidth (in bits per second) available for each VQE-C for Unicast Retransmission and RCC. The range is from 0 to 58500000.</p> <p>If a non-zero value is specified, the vqe.vqes.excess_bw_fraction and the vqe.vqes.excess_bw_fraction_high_def are ignored. Instead, each time the STB tunes to a new channel, the implicit excess_bw_fraction for the client on the channel is calculated using vqe.vqes.max_client_bw.</p> <p><b>Note</b> If the VQE-C does not use the parameters max_receive_bandwidth_sd or max_receive_bandwidth_hd to send the MRB<sup>1</sup> to the VQE-S, the vqe.vqes.max_client_bw parameter is used to calculate the excess bandwidth fraction. If the vqe.vqes.max_client_bw is zero or not configured, either the vqe.vqes.excess_bw_fraction or the vqe.vqes.excess_bw_fraction_high_def is used depending on the channel bitrate and the value of the vqe.vqes.high_def_min_bw parameter.</p>

Table A-4 VQE-S Unicast Retransmission and RCC Parameters (continued)

Parameter and Default Value (if any)	Description
vqe.vqes.excess_bw_fraction="20"	<p>Specifies the rate <math>e</math> (<math>e = \text{excess\_bw\_fraction} / 100</math>) that determines the rate at which packets are sent during Unicast Retransmission and RCC. The range is from 3 to 500.</p> <ul style="list-style-type: none"> <li>For Unicast Retransmission, the VQE-S sends packets at rate (<math>e</math>).</li> <li>During RCC, the VQE-S initially sends packets at rate (<math>1+e</math>).</li> </ul> <p><b>Note</b> If the VQE-C does not use the parameters <code>max_receive_bandwidth_sd</code> or <code>max_receive_bandwidth_hd</code> to send the MRB to the VQE-S, the <code>vqe.vqes.max_client_bw</code> parameter is used to calculate the excess bandwidth fraction. If the <code>vqe.vqes.max_client_bw</code> is zero or not configured, either the <code>vqe.vqes.excess_bw_fraction</code> or the <code>vqe.vqes.excess_bw_fraction_high_def</code> is used depending on the channel bitrate and the value of the <code>vqe.vqes.high_def_min_bw</code> parameter.</p> <p>For information on defining an excess bandwidth fraction to use for HD channels, see the <code>vqe.vqes.excess_bw_fraction_high_def</code> parameter.</p> <p>[CT: VQE-S Parameters &gt; Excess Bandwidth Fraction]</p>
vqe.vqes.excess_bw_fraction_high_def=""	<p>For high definition channels, specifies the rate <math>e</math> (<math>e = \text{excess\_bw\_fraction\_high\_def} / 100</math>) that determines the rate at which packets are sent during Unicast Retransmission and RCC. The range is from 3 to 500.</p> <ul style="list-style-type: none"> <li>For Unicast Retransmission, the VQE-S sends packets at rate (<math>e</math>).</li> <li>During RCC, the VQE-S initially sends packets at rate (<math>1+e</math>).</li> </ul> <p>The VQE-S uses the value configured in the <code>vqe.vqes.high_def_min_bw</code> parameter to determine what constitutes a high-definition channel.</p> <p>If either <code>vqe.vqes.excess_bw_fraction_high_def</code> or <code>vqe.vqes.high_def_min_bw</code> is not explicitly configured, the VQE-S uses <code>vqe.vqes.excess_bw_fraction</code> for all channels.</p> <p><b>Note</b> If the VQE-C does not use the parameters <code>max_receive_bandwidth_sd</code> or <code>max_receive_bandwidth_hd</code> to send the MRB to the VQE-S, the <code>vqe.vqes.max_client_bw</code> parameter is used to calculate the excess bandwidth fraction. If the <code>vqe.vqes.max_client_bw</code> is zero or not configured, either the <code>vqe.vqes.excess_bw_fraction</code> or the <code>vqe.vqes.excess_bw_fraction_high_def</code> is used depending on the channel bitrate and the value of the <code>vqe.vqes.high_def_min_bw</code> parameter.</p>
vqe.vqes.high_def_min_bw=""	<p>Minimum bit rate (in bits per second) for a channel to be considered a high definition channel. The range is from 0 to 40,000,000.</p> <p>For high definition channels, the <code>vqe.vqes.high_def_min_bw</code> value determines whether the <code>vqe.vqes.excess_bw_fraction_high_def</code> value is used for the bandwidth that is available on the access link for Unicast Retransmission and RCC. For more information, see <code>vqe.vqes.excess_bw_fraction_high_def</code>.</p> <p>If either <code>vqe.vqes.excess_bw_fraction_high_def</code> or <code>vqe.vqes.high_def_min_bw</code> is not explicitly configured, the VQE-S uses <code>vqe.vqes.excess_bw_fraction</code> for all channels.</p>

Table A-4 VQE-S Unicast Retransmission and RCC Parameters (continued)

Parameter and Default Value (if any)	Description
vqe.vqes.max_client_excess_bw_fraction="500"	<p>If the VQE-C provides a MRB in a Unicast Retransmission error repair or RCC request to the VQE-S, this parameter specifies the maximum excess bandwidth fraction to use when that fraction is computed using a VQE-C-provided MRB. The range is from 3 to 500.</p> <p>If this parameter is not specified, the VQE-S caps incoming requests from the VQE-C to use an excess bandwidth fraction of 500%.</p> <p>The MRB is the maximum receive bandwidth available on each of the tuners for a specific VQE-C. The VQE-C configuration parameters <code>max_receive_bandwidth_sd</code> and <code>max_receive_bandwidth_hd</code> can be used to provide this information to the VQE-S.</p> <p>The <code>vqe.vqes.min_client_excess_bw_fraction</code> and <code>vqe.vqes.max_client_excess_bw_fraction</code> parameters allow the service provider to control the range of allowed excess bandwidth fractions. This capability can be used to limit the peak and aggregate bandwidth used by the VQE-S.</p>
vqe.vqes.min_client_excess_bw_fraction="0"	<p>If the VQE-C provides a MRB in a Unicast Retransmission error repair or RCC request to the VQE-S, this parameter specifies the minimum excess bandwidth fraction to use when that fraction is computed using a VQE-C-provided MRB. The range is from 0 and 3 to 500.</p> <p>If this parameter is not specified or is set to 0, a minimum value of 3% is assumed and requests for an excess bandwidth fraction of less than 3% are rejected.</p> <p>The MRB is the maximum receive bandwidth available on each of the tuners for a specific VQE-C. The VQE-C configuration parameters <code>max_receive_bandwidth_sd</code> and <code>max_receive_bandwidth_hd</code> can be used to provide this information to the VQE-S.</p> <p>The <code>vqe.vqes.min_client_excess_bw_fraction</code> and <code>vqe.vqes.max_client_excess_bw_fraction</code> parameters allow the service provider to control the range of allowed excess bandwidth fractions. This capability can be used to limit the peak and aggregate bandwidth used by the VQE-S.</p>

1. MRB = maximum receive bandwidth.

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 <i>true</i> enables RTCP exports, and <i>false</i> 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 the VQE-S RTCP Exporter, see the <a href="#">“Configuring the VQE-S RTCP Exporter” section on page 2-42</a> .
vqe.vqes.vqm_host=""	Specifies the IP address or fully qualified Internet domain name of the host on which the VQM <sup>1</sup> application resides.  For information on configuring RTCP Exporter, see the <a href="#">“Configuring the VQE-S RTCP Exporter” section on page 2-42</a> .
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 <a href="#">“Configuring the VQE-S RTCP Exporter” section on page 2-42</a> .
vqe.vqes.exporter_filter_nack="false"	Specifies whether RTCP NACK compound packets are excluded from the RTCP data exported to the VQM application. The value <i>true</i> excludes RTCP NACK compound packets from being exported, and <i>false</i> includes RTCP NACK compound packets in the data being exported.  For information on configuring the RTCP Exporter, see the <a href="#">“Configuring the VQE-S RTCP Exporter” section on page 2-42</a> .  This parameter was introduced in Cisco VQE Release 3.5.5.

1. VQM = video-quality monitoring.

Table A-6 System Parameters

Parameter and Default Value (if any)	Description
system.global.hostname="localhost"	FQDN <sup>1</sup> or hostname of the system. Hostname is used in multiple Linux configuration files. The range is from 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. The range for the search domain is from 3 to 200 characters.  [CT: System Parameters > DNS Server(s) and DNS Search Domain]
system.ntp.server=""	IP address of an external NTP <sup>2</sup> server.  [CT: System Parameters > NTP Server(s)]

Table A-6 System Parameters (continued)

Parameter and Default Value (if any)	Description
system.snmp.ro_community_string="" system.snmp.location="" system.snmp.contact="" system.snmp.trap_listener=""	<ul style="list-style-type: none"> <li>Read-only community string—Password for read-only access to the VQE-S or VQE Tools server. The range is from 3 to 200 characters.</li> <li>Location information—Physical location of the VQE-S or VQE Tools server. The range is from 3 to 200 characters.</li> <li>Contact information—User name of a contact person who has management information for the CDE110 server. The range is from 3 to 200 characters.</li> <li>Trap listener—IP address or fully qualified hostname of a management host that receives the SNMP messages.</li> </ul> <p>[CT: System Parameters &gt; SNMP RO Community String and SNMP System Location, SNMP System Contact, and SNMP Trap Listener(s)]</p>
system.snmp.syslog_trap_enable="false"	<p>Specifies whether system messages generate SNMP traps (syslog traps). Allowed values are <i>true</i> or <i>false</i>.</p> <p>If sending traps from system messages is enabled, use the parameter <code>system.snmp.syslog_trap_priority</code> to generate traps only if the severity level of a system message meets or is below a specified level. For more information on the configuration options for generating traps from system messages, see the <a href="#">“Sending SNMP Traps” section on page 28</a>.</p> <p>[CT: System Parameters &gt; SNMP Parameters &gt; Enable Syslog Traps]</p>
system.snmp.syslog_trap_priority="2"	<p>If sending traps on the generation of system messages is enabled, specifies that traps should only be generated for system messages that meet or are lower than the severity level defined by this parameter. The range is from 0 to 7. The default value is 2 (critical). For more information on the configuration options for generating traps from system messages, see the <a href="#">“Sending SNMP Traps” section on page 28</a>.</p> <p>[CT: System Parameters &gt; SNMP Parameters &gt; Syslog Trap Priority]</p>
system.snmp.channel_trap_enable="false"	<p>Specifies whether to generate SNMP traps when the state of a channel changes. Allowed values are <i>true</i> or <i>false</i>. If SNMP is configured and channel traps are enabled, channel up traps and channel down traps are sent to a NMS<sup>3</sup>.</p> <p>For more information on enabling channel traps, see the <a href="#">“Sending SNMP Traps” section on page 2-28</a>.</p> <p>[CT: System Parameters &gt; SNMP Parameters &gt; Enable Channel Up/Down Traps]</p>
system.clock.timezone="America/New York"	<p>time zone that is used for this CDE110 server.</p> <p>[CT: System Parameters &gt; Timezone]</p>

Table A-6 System Parameters (continued)

Parameter and Default Value (if any)	Description
system.iptables.trusted_provisioner=""	<p>Depending on the hardware platform, specifies the IP addresses of the following trusted provisioners:</p> <ul style="list-style-type: none"> <li>• On a VQE-S host, specifies IP addresses of one or more trusted channel-provisioning servers (such as VCPT). <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>• On a VQE Tools host where a VCDS receives channel information from VCPT, specifies the IP addresses of <i>all Ethernet interfaces</i> (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.</li> <li>• 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.</li> </ul> <p>Multiple system.iptables.trusted_provisioner parameters are used when there is more than one Ethernet port IP address that must be specified.</p> <p>This parameter is used for enhanced communications security beyond HTTPS. The VQE-S or VQE Tools server is configured so that only trusted HTTPS clients (as specified in system.iptables.trusted_provisioner) can send information to the VQE-S or VQE Tools server.</p> <p>[CT: System Parameters &gt; Trusted Provisioning Client(s)]</p>
system.syslog.remote_server=""	<p>Specifies the IP addresses of remote syslog servers. In addition to logging VQE system messages locally, you can send system messages by UDP to remote servers for centralized logging.</p> <p>On the VQE-S, specifying the priority levels for system messages using the VQE-S AMT<sup>4</sup> allows you to control the logging level for system messages for all VQE-S processes. For more information on configuring logging levels on the VQE-S, see the <a href="#">“Change VQE-S Logging” section on page 4-33</a>.</p> <p>On the VQE Tools server, specifying the priority levels for system messages using the VCDS AMT allows you to control the logging level for system messages for all VCDS processes. For more information on configuring logging levels on the VQE Tools server, see the <a href="#">“Change VCDS Logging” section on page 5-7</a>.</p> <p>[CT: System Parameters &gt; Remote Syslog Server(s)]</p>

1. FQDN = fully-qualified domain name.
2. NTP = Network Time Protocol.
3. NMS = Network Management System.
4. AMT = Application Monitoring Tool.

Table A-7 Interface 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=""	<p>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).</p> <ul style="list-style-type: none"> <li>On a VQE-S host, four Ethernet interfaces (eth1 to eth4) are typically configured and used for VQE-S traffic. On CDE110 servers that include the Intel PRO/1000 PT Dual Port Server Adapter, six Ethernet interfaces (eth1 to eth6) are typically configured and used for VQE-S traffic.</li> <li>On a VQE Tools host, at least one Ethernet interface is typically configured and used for VCPT and VCDS traffic.</li> <li>Ethernet interfaces that are members of a bond interface should not be assigned an IP address and prefix length.</li> </ul> <p><b>Note</b> If one Ethernet interface is used for a management network, that interface <i>should be included</i> in the set for which you provide IP addresses and prefix-lengths.</p> <p>[CT: Network Parameters &gt; Interface Parameters &gt; Eth1 Interface IP/Mask, Eth2 Interface IP/Mask, Eth3 Interface IP/Mask, Eth4 Interface IP/Mask, Eth5 Interface IP/Mask, and Eth6 Interface IP/Mask]</p>
network.bond1.addr="" network.bond2.addr="" network.bond3.addr=""	<p>For one or more bond interfaces on the Cisco CDE110, an IP address and prefix length (for example, 1.2.3.4/24).</p> <p><b>Note</b> Bond interfaces are not supported on the VQE Tools Server.</p> <p>A bond interface may be used as a management interface and as one of the following:</p> <ul style="list-style-type: none"> <li>VQE-S traffic interface</li> <li>VQE-S services interface</li> <li>VQE-S ingest interface</li> </ul> <p>For more information, see the <a href="#">“Bond Interfaces on a VQE-S” section on page 2-15</a>.</p> <p>The VCDB parameters for bond3 is used only on CDE110 servers that include the Intel PRO/1000 PT Dual Port Server Adapter.</p> <p>[CT: Network Parameters &gt; Interface Parameters &gt; Bond1 IP/Mask and members, Bond2 IP/Mask and members, Bond3 IP/Mask and members]</p>

Table A-7 Interface Parameters (continued)

Parameter and Default Value (if any)	Description
network.bond1.member="" network.bond2.member="" network.bond3.member=""	<p>For each bond member, names of Ethernet interfaces that are members of the bond interface.</p> <p><b>Note</b> Bond interfaces are not supported on the VQE Tools Server.</p> <p>All members of a bond interface must have the same capacity. All members must not be assigned an IP address and prefix length nor be assigned as a member of an existing bond interface.</p> <p>Bond interfaces are not supported on the VQE Tools Server.</p> <p>The VCDB parameters for bond3 is used only on CDE110 servers that include the Intel PRO/1000 PT Dual Port Server Adapter.</p> <p>For the rules on adding members to bond interfaces, see the <a href="#">“Bond Interfaces on a VQE-S”</a> section on page 2-15.</p>
network.network.interface.mgmt_interfaces="eth 1, eth2, eth3, eth4, eth5, eth6"	<p>Names of the Ethernet or bond interfaces or both to be used for management traffic. The default value is all Ethernet interfaces on the VQE-S or VQE Tools server, regardless of their operational status.</p> <p>Multiple interfaces (one or more Ethernet and one or more bond interfaces) may be used for management traffic.</p> <p>At least one Ethernet interface or one bond interface must be specified as a management interface. If you specify an Ethernet interface, it must not be a member of a bond interface.</p> <p>The management interfaces on the VQE-S may also be used for one of the following interface types:</p> <ul style="list-style-type: none"> <li>• VQE-S traffic interface</li> <li>• VQE-S ingest interface</li> <li>• VQE-S services interface.</li> </ul> <p>For more information on configuring management interfaces, see the <a href="#">“Interface for a Management Network”</a> section on page 2-20.</p> <p>[CT: Network Parameters &gt; Interface Parameters &gt; Management Interface(s)]</p>
network.route.mgmt_route=""	<p>Starting with Cisco VQE Release 3.5, this parameter is deprecated. Use the network.route.static_route parameter.</p>

Table A-8 Static Routing Parameters

Parameter and Default Value (if any)	Description
network.route.default_gateway=""	<p>Starting with Cisco VQE Release 3.5, this parameter is deprecated. Use the network.route.static_route parameter.</p>

Table A-8 Static Routing Parameters (continued)


Parameter and Default Value (if any)	Description
network.route.static_route=""	<p>If your deployment makes use of static routes to the management, distribution, or access network, specify the following:</p> <ul style="list-style-type: none"> <li>Subnet IP address and prefix length for the target network. The allowed format for the subnet IP address and prefix length is as follows: 10.1.0.0/16</li> </ul> <p> <b>Note</b> When creating a default route on the VQE-S, specify 0.0.0.0/0 as the subnet IP address and prefix length for the target network.</p> <ul style="list-style-type: none"> <li>Gateway (next hop) IP address of the interface on the router that is directly attached to the VQE-S CDE110 interface that is used for the target network. The interface on the VQE-S and the attached edge router may be an Ethernet interface or a bond interface. The interface on the VQE Tools server is always an Ethernet interface.</li> <li>(Optional) Outbound interface on the VQE-S or VQE Tools server for the static route. To specify an outbound interface, you append the interface name to the Gateway IP address, and separate both with a colon. Specifying an outbound interface is generally not required, nor is it recommended.</li> </ul> <p>For example: network.route.static_route="10.1.0.0/16 via 5.6.7.8"</p> <p>In this example,</p> <ul style="list-style-type: none"> <li>10.1.0.0/16 is the subnet IP address and prefix-length for the target network.</li> <li>5.6.7.8 is the IP address of the interface on the router directly attached to the CDE110 Ethernet interface of the VQE-S.</li> </ul> <p><b>Note</b> On the VQE Tools server, proper route configuration is needed for external access to the VQE Tools server. Use the static route created by this parameter to configure this access.</p> <p>On the VQE-S, multipath static routes can be configured for VQE-S traffic (ingest and services) or VQE-S services traffic. The VQE-S uses ECMP<sup>1</sup> to load-balance its output traffic across CDE110 Ethernet interfaces or the physical Ethernet interfaces of a bond interface that are directly attached to the gateway router interfaces that are specified. If a default route (static route) is configured for each Ethernet interface that is available to the VQE-S for Unicast Retransmissions, RCC, and other VQE-S traffic, ECMP load balances output traffic across all of the CDE110 interfaces directly attached to the gateway router interfaces. Similarly, if a default route is configured for a bond interface, ECMP load balances output traffic across all the CDE110 physical interfaces assigned to the bond interface.</p>

Table A-8 Static Routing Parameters (continued)

Parameter and Default Value (if any)	Description
	<p>If you subsequently configure another Ethernet interface or bond interface for VQE-S traffic, be sure to also configure an associated static route for that interface.</p> <p>For more information on configuring static routes, see the <a href="#">“Configuring Static Routes”</a> section on page 2-19.</p> <p>[CT: Network Parameters &gt; Routing Parameters &gt; Static Routing Parameters&gt; Static Route(s)]</p>

1. ECMP = equal cost multipath.

Table A-9 OSPF Parameters

Parameter and Default Value (if any)	Description
network.route.type="static"	<p>VQE-S host only—Specifies whether OSPF is enabled for VQE-S services (where dedicated interfaces to the access network are configured) or VQE-S traffic (where shared interfaces to the access network are configured). Allowed values are <i>static</i> and <i>ospf</i>.</p> <p>If OSPF routing is enabled, dynamic routing is used from the VQE-S to the access network. The following parameters can be configured:</p> <ul style="list-style-type: none"> <li>• network.ospf.router_id</li> <li>• network.ospf.area</li> <li>• network.ospf.area_type</li> <li>• network.ospf.md5_enable</li> <li>• network.ospf.md5_key</li> <li>• network.ospf.md5_keyid</li> <li>• network.ospf.hello_interval</li> <li>• network.ospf.dead_interval</li> </ul> <p>For descriptions of the preceding parameters, see <a href="#">Table A-8</a> (this table).</p> <p>If network.route.type="static", OSPF is disabled but static routing is still enabled. For static routing, the network.route.static_route parameter can be configured for one or more default gateway (next hop) router interfaces.</p> <p>[CT: Network Parameters &gt; Routing Parameters &gt; OSPF Parameters &gt; OSPF Enable]</p>
network.ospf.router_id=""	<p>VQE-S host only—If OSPF routing is enabled, specifies the IP address used as the router ID to uniquely identify the VQE-S 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 is added as an internal address to the loopback interface.</p> <p>[CT: Network Parameters &gt; Routing Parameters &gt; OSPF Parameters &gt; Router ID]</p>

Table A-9 OSPF 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 resides in. Allowed values are normal or nssa <sup>1</sup> .  [CT: Network Parameters > Routing 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 reside in. The range of integer values is from 0 to 4,294,967,295.  [CT: Network Parameters > Routing Parameters > OSPF Parameters > Area ID]
network.ospf.md5_enable="false"	VQE-S host only—If OSPF routing is enabled, specifies whether MD5 <sup>2</sup> 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 > Routing 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 is 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 > Routing 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 is used for all Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, an MD5 key and MD5 key ID are required. The range of integer values is from 1 to 255.  [CT: Network Parameters > Routing 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 is set for all VQE-S interfaces running OSPF. The range is from 1 to 65,535.  [CT: Network Parameters > Routing Parameters > OSPF Parameters > Hello Interval]

Table A-9 OSPF Parameters (continued)

Parameter and Default Value (if any)	Description
network.ospf.dead_interval="40"	<p>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 is set for all VQE-S interfaces running OSPF. The range is from 1 to 65,535.</p> <p>[CT: Network Parameters &gt; Routing Parameters &gt; OSPF Parameters &gt; Dead Interval]</p>

1. nssa = not so stubby area.
2. MD5 = Message Digest 5.



## APPENDIX **B**

# SNMP MIBs

---

This appendix provides an overview of the SNMP feature of the Cisco VQE Server (VQE-S) and VQE Tools server. This chapter contains the following topics:

- [SNMP Overview, page B-1](#)
- [VQE MIB Support, page B-2](#)

## SNMP Overview

The *Simple Network Management Protocol* (SNMP) is an application-layer protocol that provides a standardized framework and a common language for monitoring and managing devices in a network.

The SNMP framework has three parts:

- **SNMP manager**—System to control and monitor the activities of network hosts that use SNMP. The most common managing system is called a *Network Management System* (NMS). A variety of network management applications are available for use with SNMP (for example, Net-SNMP).
- **SNMP agent**—Software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and Management Information Base (MIB) reside on the network hosts rather than on the NMS.
- **MIB**—Database of the objects that can be managed on a device. The managed objects or MIB objects can be read or set to provide information on the network devices and interfaces, and are organized hierarchically. The MIB consists of collections of MIB objects identified by object identifiers.

## MIB Objects

MIB objects comprise of one or more object instances, which are essentially variables. The Cisco implementation of SNMP uses the definitions of MIB II variables described in RFC 1213.

MIBs can contain two types of MIB objects:

- **Scalar objects**—Define a single object instance (for example, `cvqsNumberOfChannels` in the `CISCO-VQES-MIB`).
- **Columnar objects**—Define multiple related objects such as zero, one, or more instances at any point in time that are grouped together in MIB tables (for example, `cvqsChannelTable` in the `CISCO-VQES-MIB` defines the status of each channel).

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—Function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—Function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS. SNMP SETs are not supported on the VQE-S or VQE Tools server.

## SNMP Notifications

An SNMP agent can notify the SNMP manager when important system events occur, such as when an interface card starts or stops running. SNMP notifications are sent as either one of the following:

- Traps—Unreliable messages, which do not require receipt acknowledgment from the SNMP manager.
- Informs—Reliable messages, which are stored in memory until the SNMP manager issues a response.

## Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices:

- Standard RFC MIB OIDs are assigned by the Internet Assigned Numbers Authority (IANA)
- Enterprise MIB OIDs are assigned by Cisco Assigned Numbers Authority (CANA).

Each number in the OID corresponds to a level of the MIB hierarchy. For example, the OID 1.3.6.1.4.1.9.9.xyz represents the .xyz with the location in the MIB hierarchy as follows:

1.3.6.1.4.1.9.9.942

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgt(9).nn-MIB

Note that the numbers in parentheses are included to help show correspondence to the MIB hierarchy. You can uniquely identify a MIB object, such as ifNumber in the IF-MIB, by its object name (iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber) or by its OID (1.3.6.1.2.1.2.1). In actual use, OIDs are represented as numerical values only.

For listings of OIDs assigned to MIB objects for all Cisco MIBs, see the link:

<ftp://ftp.cisco.com/pub/mibs/oid>

## VQE MIB Support

The VQE-S and the VQE Tools server provide a standard set of built-in MIBs for managing a Linux platform, as well as enterprise-specific MIBs for monitoring VQE services. The MIBs cover GETs and a limited number of TRAPS. Only SNMP version 2 (SNMPv2) is supported on both the VQE-S and the VQE Tools server.

**Note**

Configuration of the standard Linux MIBs, the Cisco System Messages (Syslog) MIB, or the VQE-specific Mibs using SNMP is disabled.

## Net-SNMP

The VQE-S and the VQE Tools server use Net-SNMP, a third-party product, for its tools and libraries that support SNMP. Net-SNMP offers an extensible agent, an SNMP library, tools to request or set information from SNMP agents, and tools to generate and handle SNMP traps.

**Note**

For information on configuring and using Net-SNMP, see the Net-SNMP website: <http://www.net-snmp.com/docs/>

In the VQE implementation, the SNMP agent consists of a master agent and three or more subagents. The master agent is implemented by means of Net-SNMP. An Intel subagent is used to support the Linux MIBs, while Cisco subagents support the VQE-specific MIBs and the syslog MIB. The master agent communicates directly with the NMS by means of SNMP, and directly with the subagents by means of the AgentX protocol. Each subagent has its own MIB file and OID.

**Figure B-1 Subagent Architecture**

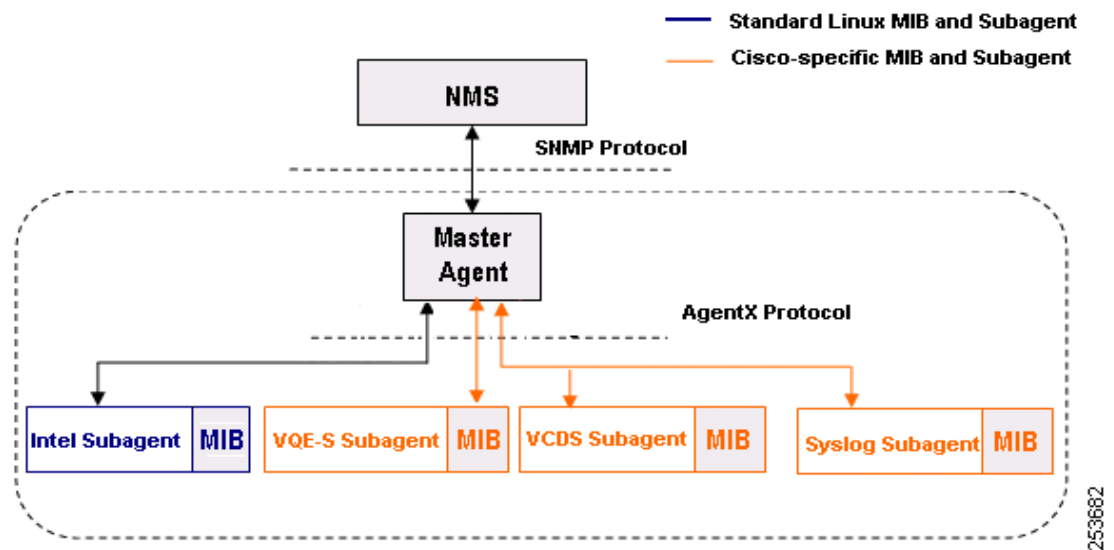


Figure B-1 shows the SNMP agent architecture. When a subagent initializes, it registers with the master agent, and informs the master agent of the range of OIDs for which it has responsibility. When a request for information is received from the NMS, the master agent sends a request to the subagent that is responsible for the OIDs defined in the request. The subagent processes the request and sends the information to the master agent, which forwards the information to the network manager.

On VQE-S and the VQE Tools server, the Intel subagent provides non-VQE system information, and the Syslog subagent provides information on system messages. On the VQE-S, the VQE-S subagent provides VQE-S-specific information. On the VQE Tools Server, the VQE Configuration Deployment Server (VCDS) subagent provides information specific to the VCDS.

**Note**

The Net-SNMP master agent service (snmpd) must be installed and be running for the subagent service to run.

## Standard Linux MIBs

Net-SNMP provides a set of standard built-in MIBs for Linux platforms. 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.

The sysDescr and sysObjectID objects in the SNMPv2-MIB identify a VQE system. The following values can be used to identify a CDE110 hosting a VQE-S or a 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

**Note**

Table B-1 lists the standard MIBs that are supported on the CDE110s that host a VQE-S and a VCPT. For information on the supported MIBs, see the MIB area of the Net-SNMP website: <http://www.net-snmp.com/docs/mibs/>

**Table B-1** MIBs for CDE110s That Host the VQE-S and the VCPT

MIB/Table	Description
SNMPv2-MIB/system	System contact, location, and so on.
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
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: <a href="http://people.redhat.com/peterm/IPMI/sw/basebrd5.mib">http://people.redhat.com/peterm/IPMI/sw/basebrd5.mib</a>

## Syslog MIB

The MIB CISCO-SYSLOG-MIB provides the means to gather system messages generated by the VQE-S or VQE Tools server. The VQE-S and the VQE Tools server can be configured so that these system messages are logged locally as well as being sent to a remote syslog server. With this MIB, system messages can also be received by means of SNMP. This MIB provides SNMP notifications only.

**Note**

An SNMP GET operation returns a zero value, and configuration of this MIB via an SNMP interface is disabled.

The MIB file is located in the /usr/share/snmp/mibs/ directory, and is available for download on Cisco.com from the following URL:

<ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SYSLOG-MIB.my>

The CISCO-SYSLOG-CAPABILITY MIB file describes the capabilities of the CISCO-SYSLOG-MIB for the VQE-S and VQE Tools platforms. The MIB file is located in the /usr/share/snmp/mibs/ directory, and is available for download on Cisco.com from the following URL:

<ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SYSLOG-CAPABILITY.my>

## VQE-Specific MIBs

A VQE-specific MIB, CISCO-VQES-MIB, is integrated with the VQE-S. This MIB reports the status of the channels, Rapid Channel Changes (RCC), Unicast Retransmissions, and VQE-S capacity. A VQE-specific MIB, CISCO-VQE-TOOLS-MIB, is integrated with the VQE Tools server. This MIB reports the status of the VCDS.

The MIB files are located in the /usr/share/snmp/mibs/ directory, and are available for download on Cisco.com from:

<ftp://ftp-sj.cisco.com/pub/mibs/v2/CISCO-VQES-MIB.my>

<ftp://ftp-sj.cisco.com/pub/mibs/v2/CISCO-VQE-TOOLS-MIB.my>

## CISCO-VQES-MIB

The MIB CISCO-VQES-MIB defines the managed objects that describe some of the VQE-S components. The MIB CISCO-VQES-MIB reports summary status information for several VQE-S components, including channel line ups, channels, Unicast Retransmission, and RCCs.

Table B-2 lists the types of summary information provided per component.

**Table B-2** Information Provided by CISCO-VQES-MIB by Component

Components	Summary Information
Channel line up	<ul style="list-style-type: none"> <li>Total number of channels in the lineup.</li> <li>Total number of active channels in the channel line up.</li> <li>Time and day when the channel line up was last updated.</li> </ul>
Channel	<ul style="list-style-type: none"> <li>Name of each channel in the channel line up.</li> <li>State of each channel in the channel line up—A channel may be active, inactive, or inoperative.</li> <li>Number of receivers on each channel in the line up.</li> <li>Multicast IP address and port number of each channel in the line up.</li> <li>Channel up trap.</li> <li>Channel down trap.</li> </ul>
Unicast Retransmission	<ul style="list-style-type: none"> <li>Total number of requests for error repair (generic NACK RTCP messages) received.</li> <li>Total number of Generic NACK RTCP messages received that were invalid.</li> <li>Total number of individual RTP packets requested for retransmission.</li> <li>Total number of individual RTP packets requested and sent for retransmission.</li> </ul>
RCC	<ul style="list-style-type: none"> <li>Total number of requests for RCC received.</li> <li>Total number of requests for RCC received and accepted.</li> <li>Total number of requests for RCC received but not accepted.</li> </ul>
VQE-S Capacity	<ul style="list-style-type: none"> <li>Number of currently active RTCP receivers.</li> <li>Number of received RTCP packets (ER requests, RCC requests or Receiver Reports) rejected by the VQE-S due to active RTCP receivers in the VQE-S reaching their limit of accepting RTCP requests.</li> <li>Number of received ER requests rejected by the VQE-S due to the VQE-S reaching its limit of accepting ER requests.</li> <li>Number of received RCC requests rejected by the VQE-S due to VQE-S reaching its limit of accepting RCC requests.</li> </ul>

The MIB CISCO-VQES-MIB contains fifteen scalar objects, one columnar object, and two traps. The tree structure of the CISCO-VQES-MIB is as follows:

```

+--ciscoVqeSMIB(942)
|
+--ciscoVqeSMIBNotifs(0)
|
|   +--cvqsChannelUp(1)
|   +--cvqsChannelDown(2)
|
+--ciscoVqeSMIBObjects(1)
|
|   +--cvqsControlInfo(1)
|   |
|   |   +-- -RW- EnumVal   cvqsNotificationsEnable(1)
|   |   |
|   |   |   Textual Convention: TruthValue
|   |   |   Values: true(1), false(2)
|   |
|   +--cvqsChannelInfo(2)
|   |
|   |   +-- -R-- Gauge     cvqsNumberOfChannels(1)
|   |   +-- -R-- Gauge     cvqsActiveChannels(2)
|   |   +-- -R-- String    cvqsLastUpdatedTime(3)
|   |   |
|   |   |   Textual Convention: DateAndTime
|   |   |   Size: 8 | 11
|   |
|   +--cvqsChannelTable(4)
|   |
|   |   +--cvqsChannelTableEntry(1)
|   |   |
|   |   |   Index: cvqsChannelIndex
|   |   |
|   |   |   +-- ---- Unsigned  cvqsChannelIndex(1)
|   |   |   |
|   |   |   |   Range: 1..2147483647
|   |   |   +-- -R-- EnumVal   cvqsChannelMulticastIPType(2)
|   |   |   |
|   |   |   |   Textual Convention: InetAddressType
|   |   |   |   Values: unknown(0), ipv4(1), ipv6(2), ipv4z(3), ipv6z(4), dns(16)
|   |   |   +-- -R-- String    cvqsChannelMulticastIPAddr(3)
|   |   |   |
|   |   |   |   Textual Convention: InetAddress
|   |   |   |   Size: 0..255
|   |   |   +-- -R-- Unsigned  cvqsChannelMulticastPort(4)
|   |   |   |
|   |   |   |   Textual Convention: InetPortNumber
|   |   |   |   Range: 0..65535
|   |   |   +-- -R-- EnumVal   cvqsChannelStatus(5)
|   |   |   |
|   |   |   |   Values: active(1), inactive(2), inoperative(3)
|   |   |   +-- -R-- Gauge     cvqsChannelMemberPopulation(6)
|   |
|   +--cvqsErrorRepair(3)
|   |
|   |   +-- -R-- Counter64  cvqsTotalReceivedERMsgs(1)
|   |   +-- -R-- Counter64  cvqsTotalReceivedInvalidERMsgs(2)
|   |   +-- -R-- Counter64  cvqsTotalReceivedERPkts(3)
|   |   +-- -R-- Counter64  cvqsTotalSentERPkts(4)
|   |
|   +--cvqsRCC(4)
|   |
|   |   +-- -R-- Counter64  cvqsTotalReceivedRCCs(1)
|   |   +-- -R-- Counter64  cvqsTotalAcceptedRCCs(2)
|   |   +-- -R-- Counter64  cvqsTotalRefusedRCCs(3)
|   |
|   +--cvqsCapacity(5)
|   |
|   |   +-- -R-- Gauge     cvqsTotalRTCPReceivers(1)
|   |   +-- -R-- Counter64  cvqsRejectedRTCPs(2)
|   |   +-- -R-- Counter64  cvqsRejectedERS(3)

```

```

|       +-- -R-- Counter64 cvqsRejectedRCCs(4)
|
+--ciscoVqeSMIBConform(2)
|
|   +--cvqsMIBCompliances(1)
|   |
|   |   +--cvqsMIBCompliance(1)
|   |
|   +--cvqsMIBGroups(2)
|   |
|   |   +--ciscoVqeSControlGroup(1)
|   |   +--ciscoVqeSChannelGroup(2)
|   |   +--ciscoVqeSERGroup(3)
|   |   +--ciscoVqeSRCCGroup(4)
|   |   +--ciscoVqeSCapacityGroup(5)
|   |
|   +--ciscoVqeSNotifGroup(6)

```

## CISCO-VQE-TOOLS-MIB

The CISCO-VQE-TOOLS-MIB is integrated with the VQE Tools server. It defines the managed objects and notifications that describe the VCDS component responsible for channel delivery. The data reported includes the following:

- Number of open connections
- Number of requests received
- Number of responses sent
- Number of requests per second.

The MIB CISCO-VQE-TOOLS-MIB contains four scalar objects. The tree structure of the CISCO-VQE-TOOLS-MIB is as follows:

```

+--ciscoVQETOOLSMIB(969)
|
|   +--ciscoVqeToolsMIBNotifs(0)
|
|   +--ciscoVQETOOLSMIBObjects(1)
|   |
|   |   +--vcdsInfo(1)
|   |   |
|   |   |   +-- -R-- Unsigned  numberOfSessions(1)
|   |   |   +-- -R-- Gauge    cvqtNumberOfSessions(1)
|   |   |   +-- -R-- Counter64 requestsReceivedTotal(2)
|   |   |   |   Textual Convention: Unsigned64
|   |   |   +-- -R-- Counter64 cvqtTotalReceivedRequests(2)
|   |   |   +-- -R-- Counter64 responsesSentTotal(3)
|   |   |   |   Textual Convention: Unsigned64
|   |   |   +-- -R-- Counter64 cvqtTotalSentResponses(3)
|   |   |   +-- -R-- Unsigned  requestsPerSecond(4)
|   |   |   +-- -R-- Gauge    cvqtRequestRate(4)
|   |
|   +--cvqtVcdsInfo(1)
|
+--ciscoVqeToolsMIBObjects(1)
|
+--ciscoVQETOOLSMIBConformance(2)
|
|   +--ciscoVQETOOLSMIBCompliances(1)
|   |
|   |   +--cvqtMIBReadOnlyCompliance(1)

```

```
| |
| |--cvqtMIBCompliances(1)
| |
| |--ciscoVQETOOLSMIBGroups(2)
| | |
| | |--ciscoVqeToolsVcdsGroup(1)
| | |
| |--cvqtMIBGroups(2)
|
|--ciscoVqeToolsMIBConform(2)
```

## Compiling VQE-Specific MIBs

If you plan to integrate the VQE-S or the VQE Tools server with an SNMP-based management application, then you must also compile the MIBs for that platform. For example, if you are running HP OpenView on a UNIX operating system, you must compile VQE-S or VQE Tools server MIBs with the HP OpenView Network Management System (NMS). For instructions, see the NMS documentation.





# 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 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 the VQE-S AMT and VCPT logging output, see the [“VQE-S AMT, VCDS AMT, and VCPT Logging and Log Files” section on page 6-3](#).

## 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 ( <code>vqe_cfgtool</code> 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 the RTCP <sup>1</sup> ).
VQE_RTSP	VQE Real Time Streaming Protocol (VCDS related)

1. RTCP = RTP Control Protocol.

- 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
[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.	<a href="#">Restarting the System and Verifying System and VQE-S Status, page D-28</a>
Restart the VQE-S application.	<a href="#">Stopping, Starting, and Restarting VQE-S, page 6-30</a>
Restart the VQE-S channels.	In VCPT, use the Force Update button to send the channel information to the VQE Server (VQE-S). See the <a href="#">“Force Update Button”</a> section on page 3-6.
Modify the channel configuration and resend it to the VQE-Ss or VCDS servers.	<a href="#">Chapter 3, “Using the VQE Channel Provisioning Tool”</a>

Table C-4 Recovery Procedures in Recommended Actions (continued)

Recovery Procedure in Recommended Action	Notes and Where to Find Information
Modify vcdb.conf and apply the configuration.	For VQE configuration (vcdb.conf) information, see <a href="#">Chapter 7, “Configuring VQE Server and VQE Tools.”</a>  For information on applying a VQE configuration with the <b>-apply</b> option to <b>vqe_cfgtool</b> , see the “Using the VQE Configuration Tool Command-Line Options” section on page 7-18.
Issue the <b>vgereport</b> command to gather data that may help identify the nature of the error.	“Using the vgereport Command” section on page 6-29

## VQE System Messages Reference Information

Starting with Cisco 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 from the [Error and Systems Messages page](#) on Cisco.com.



### Tip

The online system messages file with reference and recovery information is also available from the [VQE software download](#) area on Cisco.com. The files are located with the VQE software installation file. The system messages link is named System Messages and Recovery Procedures for X.X(X).

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

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: Routing and Interface Configuration Overview” section on page 2-14](#).



### 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 installing or upgrading VQE software, see *Release Notes for Cisco CDA Visual Quality Experience Application*.

The manual initial configuration procedures are explained in these sections:

- [Setting Up a Cisco CDE110 That Hosts VQE-S](#)
- [Setting Up a Cisco CDE110 That Hosts VQE Tools](#)

## Setting Up a Cisco CDE110 That Hosts VQE-S

This section explains how to perform the initial configuration tasks for a Cisco CDE110 hosting the 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 7-14](#).

Perform these initial configuration tasks in the order shown:

1. [Prerequisites for a Cisco CDE110 That Hosts the VQE-S, page D-3](#)
2. [Configuring the Linux Operating System for the VQE-S, page D-3](#)
3. [Configuring Bond Interfaces, page D-5](#)
4. [Configuring a Static Route for a Management Network \(VQE-S Host\), page D-6](#)
5. [Configuring Static Routes for VQE-S Traffic or VQE-S Services Traffic \(VQE-S Host\), page D-8](#)
6. [Enabling OSPF Routing for VQE-S Traffic or VQE-S Services Traffic, page D-10](#)
7. [Configuring Interfaces for VQE-S Traffic \(Ingest and Services\) and VQE-S Services Traffic, page D-15](#)
8. [Synchronizing the Time and Configuring Network Time Protocol, page D-19](#)
9. [VQE STUN Server Is Enabled By Default, page D-20](#)
10. [Configuring SNMP, page D-20](#)
11. [Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS, page D-21](#)
12. [Configuring Remote Syslog Servers, page D-22](#)
13. [Starting VQE-S System Services and Verifying Status, page D-22](#)
14. [Starting the VQE-S Processes and Verifying Status, page D-27](#)
15. [Restarting the System and Verifying System and VQE-S Status, page D-28](#)

**Note**

The configuration instructions in this section are intended for new installations of Cisco VQE Release 3.5 software, where the Cisco CDE110 has the Cisco VQE Release 3.5 software preinstalled.

For information on upgrading an already configured Cisco CDE110, see the Release Notes for Cisco CDA Visual Quality Experience, Release 3.5.

For information on configuring the VQE-S RTCP Exporter, see the [“Configuring the VQE-S RTCP Exporter” section on page 2-42](#).

## Prerequisites for a Cisco CDE110 That Hosts the VQE-S

This section explains tasks that should be performed before setting up a Cisco CDE110 that hosts the VQE-S.

### Connecting Cables for the VQE-S

For information on connecting cables on the VQE-S, see the “[Connecting Cables to the CDE110](#)” section on page 2-4.

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 the VQE-S

It is recommended that you deploy your own Secure Sockets Layer (SSL) certificates or commercial SSL certificates before beginning the tasks for setting up a Cisco CDE110 that hosts the VQE-S. For information on setting up the certificates, see the “[Setting Up SSL Certificates](#)” section on page 2-5.

## Configuring the Linux Operating System for the VQE-S

This section explains the initial Linux configuration tasks needed for a Cisco CDE110 appliance that runs the VQE-S software. The explanation assumes that the needed software for Linux and the VQE-S has been preinstalled on the Cisco CDE110 appliance. For Red Hat Enterprise Linux 5.1 documentation, go to the following website:

<http://www.redhat.com/docs/manuals/enterprise/>

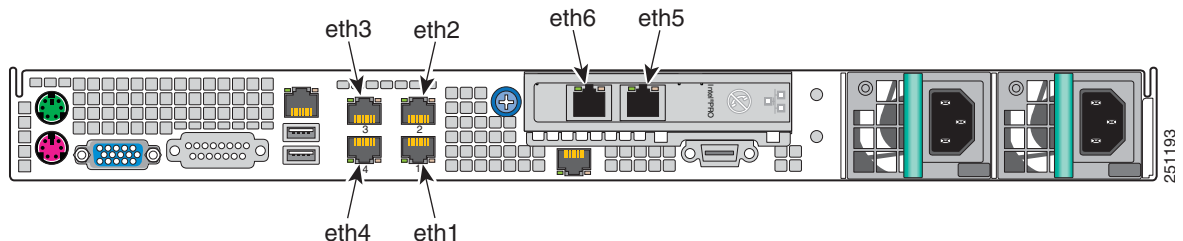
For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE110 back panel are specified as eth1 to eth6 as shown in [Figure D-1](#).



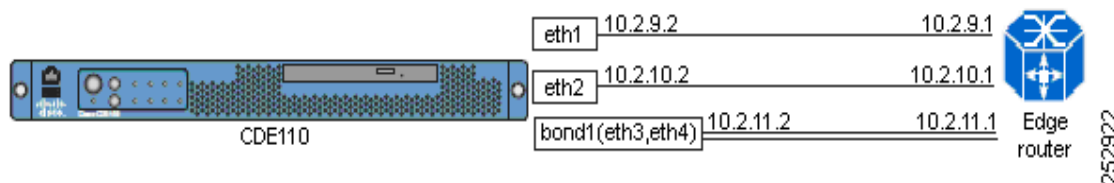
#### Note

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, bond1 (with eth3 and eth4 as its members), 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 the 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 AMT.

- 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.ethx.addr` parameters, where `ethx` is `eth1`, `eth2`, and so on. Specify an IP address and prefix length for each interface that is not a member of a bond interface. The following example shows two `vcdb.conf` lines for the two Ethernet interfaces:

```
network.eth1.addr="10.2.9.2/24"
network.eth2.addr="10.2.10.2/24"
```

- 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.

---

## Configuring Bond Interfaces

This section provides information on configuring bond interfaces on the CDE110 that hosts the VQE-S. Bond interfaces may be used for the VQE-S traffic (ingest and services), VQE-S ingest traffic, or VQE-S service traffic, depending on whether shared or dedicated interfaces are configured. Bond interfaces may also be used for VQE-S management traffic.



**Note** For guidance on using bond interfaces, see the [“Bond Interfaces on a VQE-S” section on page 2-15](#).

---

To configure a bond interface with one or more CDE110 Ethernet interfaces as members, 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 configure CDE110 bond interfaces `bond1` to `bond3`, edit the `/etc/opt/vqes/vcdb.conf` file by adding to the file one or more `network.bondx.addr` parameters, where `bondx` is `bond1`, `bond2`, or `bond3`. Specify an IP address and prefix length for each bond interface. The following example shows a line added to the `vcdb.conf` file for a single bond interface:

```
network.bond1.addr="10.2.11.2/24"
```

**Step 3** To add CDE110 Ethernet interfaces to a bond interface, edit the `/etc/opt/vqes/vcdb.conf` file by adding to the file one or more `network.bondx.member` parameters, where `bondx` is `bond1`, `bond2`, or `bond3`. Specify the CDE110 Ethernet interfaces to be added as members to each bond interface. The following example shows a line added to the `vcdb.conf` file to add two Ethernet interfaces to a bond interface:

```
network.bond1.member="eth3,eth4"
```



**Note** An Ethernet interface should not be assigned as a member of a bond interface if that Ethernet interface is either already assigned an IP address and prefix length, or if that Ethernet interface is already a member of another bond interface.

---

**Step 4** Save the `vcdb.conf` file.

---



**Note** VCDB configurations are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System and VQE-S Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options” section on page 7-18](#).

---

After the VQE-S host is rebooted or the configuration has been applied, you can verify that the Ethernet interfaces and bond interfaces are configured correctly and up and running by issuing the following commands:

- Use the **ifconfig interface** command to verify that each Ethernet interface or bond 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:C1:F4:0F
          inet addr:10.7.10.2  Bcast:10.7.10.255  Mask:255.255.255.0
          inet6 addr: fe90::20e:cff:fec7: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
```

The following example is for bond1:

```
[root@system]# ifconfig bond1

bond1     Link encap:Ethernet  HWaddr 00:0E:0C:C6:D4:2E
          inet addr:8.5.28.2  Bcast:8.5.28.255  Mask:255.255.255.0
          inet6 addr: fe90::20e:cff:fec5:d42e/64  Scope:Link
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:1198174 errors:0 dropped:0 overruns:0 frame:0
          TX packets:866284 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:124912504 (119.1 MiB)  TX bytes:105570108
```

- Use the **ip link show eth#** command (where # is the Ethernet or bond 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
```

The following is an example for bond1:

```
[root@system]# ip link show bond1

bond1: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue
link/ether 00:0e:0c:c6:d4:2e 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.static_route`. The configuration example in this section configures CDE110 Ethernet interface eth1 as the interface to the management network.

When the VQE-S uses dedicated interfaces for ingest traffic for multicast streams, the `network.route.static_route` parameter can be used to define a static route to the distribution network where video sources reside. For information, see the [“Routing Configuration for Dedicated Interfaces and Shared Interfaces”](#) section on page 2-18.

**Note**

If you configure a static route for a management network, the Multicast Load Balancer (MLB) monitors the status of this route. If the MLB detects that the underlying interface is administratively down, the MLB attempts to re-create the route once the interface is brought back up.

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.network.interface.mgmt_interfaces` parameter. Specify the name of the Ethernet interfaces and the bond interfaces designated for management traffic. One or more CDE110 Ethernet or bond interfaces may be specified. The Ethernet interface must not be a member of a bond interface.

For this example, assume CDE110 Ethernet interface `eth1` (10.2.9.2) on the VQE-S host is designated for management traffic.

The line in the `vcdb.conf` file is as follows:

```
network.network.mgmt_interfaces="eth1"
```

- Step 3** Add to the `/etc/opt/vqes/vcdb.conf` file a `network.route.static_route` parameter and specify the needed values using the following format:

```
network.route.static_route="target-network-subnet-addr/prefix-length via gateway-addr:outbound-interface"
```

The *target-network-subnet-addr/prefix-length* is the IP address and prefix length for the management network. The *gateway-addr* is the IP address of the router Ethernet interface or bond interface that is directly attached to the CDE110 Ethernet port or bond interface that is used for management network traffic. The *outbound-interface* is the interface used on the VQE-S for this static route.

For this example, assume the following:

- CDE110 Ethernet interface `eth1` (10.2.9.2) is used for the target management network on the VQE-S host.
- Management network is 192.0.0.0/8.

The line in the `vcdb.conf` file is as follows:

```
network.route.static_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` on the VQE-S host. [Figure D-2](#) shows the IP addresses used in this example for the `eth1` interface and the directly attached router.

- Step 4** Save the `vcdb.conf` file.

**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System and VQE-S Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

After the VQE-S host is rebooted or the configuration has been applied, 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 is 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 10.2.10.1 dev bond1 weight 1
```

## Configuring Static Routes for VQE-S Traffic or VQE-S Services Traffic (VQE-S Host)

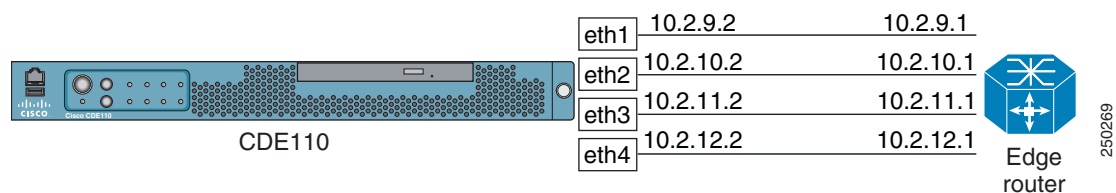
This section provides information on configuring static routes for VQE-S traffic to the access network on the CDE110 that hosts VQE-S. The configuration is similar regardless of whether dedicated interfaces or shared interfaces are used.

**Note**

For information on configuring static routes for feedback targets on the directly attached router, see the [“For Static Routes: Guidance for Configuring the Feedback Targets on the Attached Router”](#) section on page 2-47.

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 the VQE-S, multiple Ethernet interfaces or multiple bond interfaces can be used for the VQE-S traffic, including incoming multicast streams, outgoing Unicast Retransmissions and RCC unicast transmissions, and other VQE traffic. In addition, some VQE deployments may use one of the Ethernet or one of the bond interfaces as the interfaces to a management network.

If a default (next hop) route is configured for each CDE110 Ethernet interface or bond interface that is available for VQE-S traffic, Equal Cost Multipath (ECMP) is used to load-balance VQE-S output traffic across the CDE110 interfaces that are directly attached to the gateway router interfaces specified in the `network.route.static_route` parameter.

**Note**

A static route should be configured for each interface used for VQE-S traffic. Otherwise, output load is not balanced and some interfaces may be overloaded.

To configure a static route for one or more CDE110 Ethernet interfaces or one or more bond 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** If disabling OSPF routing for VQE-S traffic is needed, 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.static_route` parameters and specify the needed values using the following format:

```
network.route.static_route="target-network-subnet-addr/prefix-length via gateway-addr:outbound-interface"
```

For the `target-network-subnet-addr/prefix-length`, specify `0.0.0.0/0`.

The `gateway-addr` is the IP address of the router Ethernet interface or bond interface that is directly attached to the CDE110 Ethernet port or bond interface that is used for access network traffic. The `outbound-interface` is the interface used on the VQE-S for this static route and is optional.

**Note**

For load balancing to work effectively, each interface to the distribution network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot not be specified in this parameter.

The following example shows two `vcdb.conf` lines that add default gateways for the Ethernet interfaces displayed in [Figure D-3](#).

```
network.route.static_route="0.0.0.0/0 via 10.2.11.1"
network.route.static_route="0.0.0.0/0 via 10.2.12.1"
```

In the preceding example, `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 is designated 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 are applied to the CDE110 when it is rebooted in the [“Restarting the System and Verifying System and VQE-S Status”](#) section on page D-28. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

After the VQE-S host is rebooted or the configuration has been applied, 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 is similar to the following:

```
default
  nexthop via 10.2.11.1 dev bond1 weight 1
```

## Enabling OSPF Routing for VQE-S Traffic or VQE-S Services Traffic

This section provides information on enabling and configuring OSPF routing for VQE-S traffic (ingest and services) or VQE-S services traffic to the access network on the CDE110 that hosts the VQE-S. The configuration is similar regardless of whether dedicated interfaces or shared interfaces are used.

**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 2-45.

To configure OSPF routing for the CDE110 Ethernet interfaces or bond interfaces that are used for VQE-S traffic or VQE-S services 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 enable OSPF routing for VQE-S traffic to the access network, 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 or VQE-S services 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-8](#).

**Step 4** Save the vcdb.conf file.



**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the “[Restarting the System and Verifying System and VQE-S Status](#)” section on page D-28. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe\_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the “[Using the VQE Configuration Tool Command-Line Options](#)” section on page 7-18.

**On the VQE-S**

After the VQE-S host is rebooted or the configuration has been applied, 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.
- 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.
- 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 millise(c)s
Minimum hold time between consecutive SPF(s) 1000 millise(c)s
Maximum hold time between consecutive SPF(s) 10000 millise(c)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.
- 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 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 1. Checksum Sum 0x002F1B
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DChitless 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
10.0.0.0/24 is subnetted, 2 subnets
C      10.1.1.0 is directly connected, GigabitEthernet0/1
C      10.1.2.0 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 Interfaces for VQE-S Traffic (Ingest and Services) and VQE-S Services Traffic

The service provider can choose one of the following approaches when configuring the CDE110 interfaces:

- **Dedicated Interfaces**—If a VQE deployment requires that the Ethernet interfaces or bond interfaces used for VQE-S ingest traffic from upstream video sources be separate from the interfaces used for VQE-S services traffic to the downstream VQE Clients (VQE-Cs) on the set-top boxes (STBs), the CDE110 Ethernet interfaces or bond interfaces must be configured as follows:
  - One or more interfaces are configured as dedicated interfaces for VQE-S ingest traffic.
  - One or more interfaces are configured as dedicated interfaces for VQE-S services traffic.

See the [Configuring Dedicated Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic](#) section.

- **Shared Interfaces**—If a VQE deployment does not require that the Ethernet interfaces or bond interfaces used for VQE-S ingest traffic be separate from the interfaces used for VQE-S services traffic, a single set of CDE110 Ethernet interfaces or one or more bond interfaces are configured as VQE-S traffic interfaces that handle both types of traffic. See the [Configuring Shared Interfaces for All VQE-S Traffic](#) section.

## Configuring Dedicated Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic

On the VQE-S host, the `vqe.vqes.vqe_ingest_interfaces` and `vqe.vqes.vqe_services_interfaces` parameters in the `/etc/vqes/vcdb.conf` file allow you to specify the Ethernet interfaces or bond interfaces that are available, respectively, for VQE-S ingest traffic (incoming multicast streams) and for VQE-S services (Unicast Retransmission and RCC traffic). You manually edit the `vcdb.conf` file and specify the Ethernet interfaces or bond interfaces that are used.

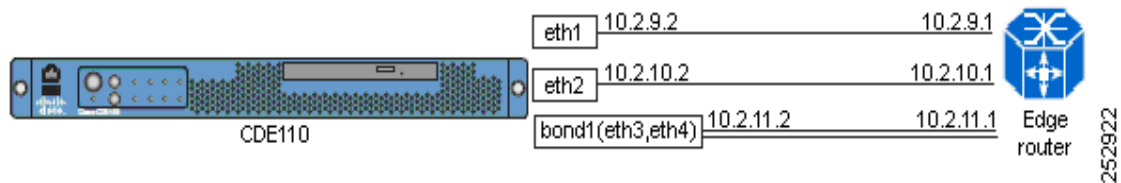


### Note

For information on the restrictions that apply to the `vqe.vqes.vqe_ingest_interfaces` and `vqe.vqes.vqe_services_interfaces` parameters, see the “[Interfaces for VQE-S Ingest Traffic \(VQE-S Host Only\)](#)” section on page 2-29.

For the configuration examples in this section, [Figure D-4](#) shows the IP addresses for interfaces `eth1`, `eth2`, `bond1` (with `eth3` and `eth4` as its members), and the corresponding interfaces on the edge router.

**Figure D-4** IP Addresses for VQE-S Configuration Examples



On the Cisco CDE110 that hosts VQE-S, to configure dedicated interfaces that are used for VQE-S ingest traffic and for VQE-S services traffic, follow these steps:

### Step 1

If needed, log in as root. You must have root privileges to modify the `vcdb.conf` file.



### Note

If your deployment uses one dedicated interface for a management network, be sure not to include that interface as one of the interfaces that are available for VQE-S ingest or services traffic.

For this example, assume that the implementation uses `eth1` for management network traffic only. Therefore, `eth1` is not included in the set of interfaces that are available for VQE-S ingest or services traffic.

- Step 2** Edit the `/etc/opt/vqes/vcdb.conf` file. Add the `vqe.vqes.vqe_ingest_interfaces` parameter to the file and specify the required values using the following format:

```
vqe.vqes.vqe_ingest_interfaces="ethernet-interface-name, ethernet-interface-name" or
```

```
vqe.vqes.vqe_ingest_interfaces="bond-interface-name, bond-interface-name"
```

For example:

```
vqe.vqes.vqe_ingest_interfaces="eth2"
```

**Note**

For load balancing to work effectively, each interface to the access or distribution network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot not be specified in this parameter.

For information on manually editing the `vcdb.conf` file, see the [“Manually Editing the VCDB File” section on page 7-14](#).

- Step 3** Add the `vqe.vqes.vqe_services_interfaces` parameter to the file and specify the required values using the following format:

```
vqe.vqes.vqe_ingest_interfaces="ethernet-interface-name, ethernet-interface-name" or
```

```
vqe.vqes.vqe_ingest_interfaces="bond-interface-name, bond-interface-name"
```

For example:

```
vqe.vqes.vqe_services_interfaces="bond1"
```

- Step 4** If `vqe.vqes.vqe_interfaces` parameter is present in the `vcdb.conf` file, delete the line containing that parameter.

- Step 5** Save the `vcdb.conf` file.

**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the [“Restarting the System and Verifying System and VQE-S Status” section on page D-28](#). Reboot once when all VCDB configuration tasks are completed.

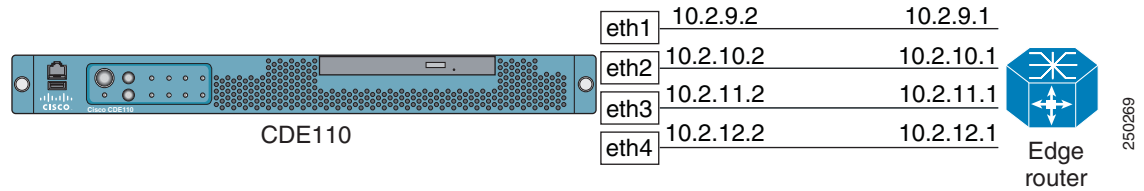
Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options” section on page 7-18](#).

## Configuring Shared Interfaces for All 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 or bond interfaces that are available for VQE-S traffic (ingest and services). You manually edit the `vcdb.conf` file and specify the Ethernet interfaces or bond interfaces that are used.

For the configuration examples in this section, [Figure D-5](#) shows the IP addresses for interfaces eth1, eth2, eth3, and eth4 and the corresponding interfaces on the edge router.

**Figure D-5** IP Addresses for VQE-S Configuration Examples



On the Cisco CDE110 that hosts VQE-S, to configure shared interfaces to handle both VQE-S ingest traffic and VQE-S services traffic, follow these steps:

---

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



**Note** If your deployment uses one dedicated interface for a management network, be sure *not to include* that interface as one of the interfaces that are available for VQE-S ingest and services traffic.

For this example, assume that the implementation uses eth1 for management network traffic. Therefore, eth1 is not included in the set of interfaces that are available for VQE-S ingest and services traffic.

---

**Step 2** Edit the `/etc/opt/vqes/vcdb.conf` file. Add the `vqe.vqes.vqe_interfaces` parameter to the file and specify the needed values using the following format:

```
vqe.vqes.vqe_ingest_interfaces="ethernet-interface-name, ethernet-interface-name" or
```

```
vqe.vqes.vqe_ingest_interfaces="bond-interface-name, bond-interface-name"
```

For example:

```
vqe.vqes.vqe_interfaces="eth2, eth3, eth4"
```



**Note** For load balancing to work effectively, each interface to the access or distribution network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot not be specified in this parameter.

---

For information on manually editing the `vcdb.conf` file, see the [“Manually Editing the VCDB File” section on page 7-14](#).

**Step 3** If `vqe.vqes.vqe_ingest_interfaces` or `vqe.vqes.vqe_services_interfaces` parameter is present in the `vcdb.conf` file, delete the lines containing those parameters.

**Step 4** Save the `vcdb.conf` file.

---

**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the [“Restarting the System and Verifying System and VQE-S Status”](#) section on page D-28. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

## 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 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 3** 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 external 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 external NTP server is 10.2.26.2.
- Step 4** Save the `vcdb.conf` file.
- 

**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the [“Restarting the System and Verifying System and VQE-S Status”](#) section on page D-28. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

For information on starting the NTP service (`ntpd` daemon), see the [“Starting VQE-S System Services and Verifying Status”](#) section on page D-22.

## 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 STBs behind NAT devices to be supported by VQE-S. Unless you are sure that no STBs being serviced by VQE-S are behind NAT devices, we recommend that you leave the STUN Server enabled.

## Configuring SNMP

The CDE110 that hosts the 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 VQE-S also provides a VQE-specific MIB and a system messages (Syslog) MIB. System messages that meet a specified severity level can be converted to SNMP traps and sent to a Network Management System (NMS). SNMP traps for indicating changes in a channel's state may also be generated. A channel up trap can be generated when a channel's state changes from inactive to active, and a channel down trap can be generated when a channel's state changes from active to inactive. Generating syslog and channel traps is optional. For more information on the SNMP MIBs on the VQE-S, see [Appendix B, "SNMP MIBs"](#).

To configure SNMP on the Cisco CDE110 that hosts the 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"`
  - `system.snmp.syslog_trap_enable="false"`
  - `system.snmp.syslog_trap_priority="2"`
  - `system.snmp.channel_trap_enable="false"`

For more information on these SNMP-related VCDB parameters, see [Table A-6 on page A-12](#).

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"
system.snmp.syslog_trap_enable="true"
system.snmp.syslog_trap_priority="4"
system.snmp.channel_trap_enable="true"
```

- Step 3** Save the `vcdb.conf` file.
-

**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System and VQE-S Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

## Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS

In your IPTV deployment, VCPT (VCPT) or another channel-provisioning server sends channel information to the VQE-Ss. You must configure each CDE110 that hosts the 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 [“VCPT and Channel Information”](#) section on page 1-15.

The `system.iptables.trusted_provisioner` parameter is for enhanced communications security beyond HTTPS. The VQE-S 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 are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System and VQE-S Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

## Configuring Remote Syslog Servers

VQE system messages can be sent by means of UDP to remote servers for centralized logging. The use of remote syslog servers is optional. For more information on configuring remote syslog servers, see the “Remote Syslog Hosts” section on page 2-28.

To configure remote syslog servers on the Cisco CDE110 that hosts the 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 parameter and specifying it’s value:
  - system.syslog.remote\_server="IP\_address"

For more information on the remote logging VCDB parameters, see Table A-6 on page A-12.

The following example shows the two vcdb.conf lines that specifies the remote logging parameter:

```
system.syslog.remote_server="192.0.7.25"
system.syslog.remote_server="192.0.7.26"
```

- Step 3** Save the vcdb.conf file.



**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System and VQE-S Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe\_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the “Using the VQE Configuration Tool Command-Line Options” section on page 7-18.

## Starting VQE-S System Services and Verifying Status

Table D-1 lists the system services that you configure and start for the CDE110 that hosts the VQE-S. 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 Intel SNMP subagent.                         |
| vqes_snmpsa   | (Optional) VQE-S SNMP subagent.                             |
| syslog_snmpsa | (Optional) Syslog SNMP subagent.                            |
| ntpd          | (Optional) The NTP daemon.                                  |

**Table D-1** System Services for CDE110 That Hosts VQE-S (continued)

| Service                                                                  | Description                                                                                                                                                    |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <b>cron</b> job owned by root. |
| <b>If OSPF Is Enabled for VQE-S traffic or VQE-S services interfaces</b> |                                                                                                                                                                |
| 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 the 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 subagents, 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 vqes_snmpsa
[root@system]# chkconfig vqes_snmpsa on
[root@system]# service vqes_snmpsa start
```

```
[root@system]# chkconfig --add syslog_snmpsa
[root@system]# chkconfig syslog_snmpsa on
[root@system]# service syslog_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 Intel 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 VQE-S SNMP subagent service, to verify the vqes\_snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep vqes_snmpsa

vqes_snmpsa   0:off  1:off  2:on   3:on   4:on   5:on   6:off

[root@system]# service vqes_snmpsa status

vqes_subagent (pid 28603) is running...

[root@system]# ps -ef | grep vqes_snmpsa

root      17878 17956  0 09:16 pts/3 00:00:00 grep vqes_snmpsa
```

- Step 13** If you have configured and started the Syslog SNMP subagent service, to verify the syslog\_snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep syslog_snmpsa

syslog_snmpsa 0:off  1:off  2:on   3:on   4:on   5:on   6:off

[root@system]# service syslog_snmpsa status

syslog_subagent (pid 9886) is running...

[root@system]# ps -ef | grep syslog_snmpsa

root      17984 17946  0 09:16 pts/2  00:00:00 grep syslog_snmpsa
```

- Step 14** 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 the 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 VCPT has not yet been sent to the 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      2965      1  0 09:17 pts/0    00:00:00 /opt/vqes/bin/process_monitor
vqes      2978  2965  0 09:17 pts/0    00:00:00 stun_server --ss-uid 499 --ss-gid 499
--xmlrpc-port 8054 --dscp -1 --log-level 6
root      3007  2965  99 09:17 pts/0    09:25:31 vqes_dp --group vqes --max-channels 500
--max-outstanding-rpcs 100 --max-pkts 1000000 --log-level 6 --rtp-inactivity-tmo 300
--max-core-bw 1100000000 --reserved-core-rcv-bw 3000000000 --reserved-core-er-bw 2000000000
--reserved-er-bw 543200000 --max-rai-gap 15
vqes      3061  2965  7 09:17 pts/0    00:13:56 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-outstanding-rpcs 100 --max-queued-rpcs 1000
--max-reserved-rpcs 32000 --max-clients 32000 --exporter-enable --vqm-host 10.86.21.4
--vqm-port 8192 --reserved-er-bw 543200000 --er-pkt-tb-rate 50000 --er-pkt-tb-depth 100
--er-blp-tb-rate 10000 --er-blp-tb-depth 100 --client-er-policing
```

```
--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 --buff-size-preroll-max 1500
--rcc-burst-delay-to-send 10 --rtp-dscp 0 --rtp-rcc-dscp -1 --rtcp-dscp 24 --overlap-loss
0 --intf-output-allocation 90 --max-rpr-stream-burst-msecs 30 --max-rpr-stream-burst-pkts
2 --unity-e-factor-interval 5 --min-client-excess-bw-fraction 0
--max-client-excess-bw-fraction
```

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

```
root      2989  2965  0 09:17 pts/0    00:00:03 mlb --interface eth2,eth3,eth4
--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 AMT from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts the 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 AMT.)

If you click **System** in the left pane, the VQE-S AMT displays information on the VQE-S processes. [Figure 4-2](#) shows an example.

## Restarting the System and Verifying System and VQE-S Status

To restart the Cisco CDE110 and verify system and the 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 the 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 VCPT has not yet been sent to the 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 Intel snmpsas service is running, issue the following command:

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

... Output omitted

**Step 15** If you configured SNMP, to verify that the VQE-S subagent service is running, issue the following command:

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

... Output omitted

**Step 16** If you configured SNMP, to verify that the Syslog subagent service is running, issue the following command:

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

... Output omitted

**Step 17** If you have configured an external NTP server, to verify that the ntpd service is running, issue the following command:

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

... Output omitted

**Step 18** 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.
- 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 (VCPT, VCDS, and VCDS AMT).

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 7-14](#).

Perform these initial configuration tasks in the order shown:

1. [Prerequisites for a Cisco CDE110 That Hosts VQE Tools, page D-32](#)
2. [Configuring the Linux Operating System for VQE Tools, page D-32](#)
3. [Configuring a Static Route for a Management Network \(VQE Tools Host\), page D-34](#)
4. [Synchronizing the Time and Configuring Network Time Protocol, page D-36](#)
5. [Configuring SNMP, page D-37](#)
6. [Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS, page D-38](#)
7. [Configuring Remote Syslog Servers, page D-39](#)
8. [Starting VQE Tools System Services and Verifying Status, page D-39](#)

9. [Starting the VCDS Service and Verifying VCDS, VCDS AMT and VCPT Status, page D-43](#)
10. [Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status, page D-44](#)

On the VQE Tools server, proper route configuration is needed for external access to the VQE Tools server. You can use the static route explained in the “[Configuring a Static Route for a Management Network \(VQE Tools Host\)](#)” section on page D-34 to configure this access.

**Note**

---

The configuration instructions in this section are intended for new installations of Cisco VQE Release 3.5 software, where the Cisco CDE110 has the Cisco VQE Release 3.5 software preinstalled.

For information on *upgrading an already configured* Cisco CDE110, see the [Release Notes for Cisco CDA Visual Quality Experience, Release 3.5](#).

---

## 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 2-4.

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 before 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 2-5.

## Configuring the Linux Operating System for VQE Tools

This section explains the initial Linux configuration tasks needed for a Cisco CDE110 appliance that runs the VQE Tools (VCPT and VCDS) software. The explanation assumes that the needed software for Linux, VCPT, and VCDS have been preinstalled on the Cisco CDE110 appliance. For Red Hat Linux 5.1 documentation, go to the following :

<http://www.redhat.com/docs/manuals/enterprise/>

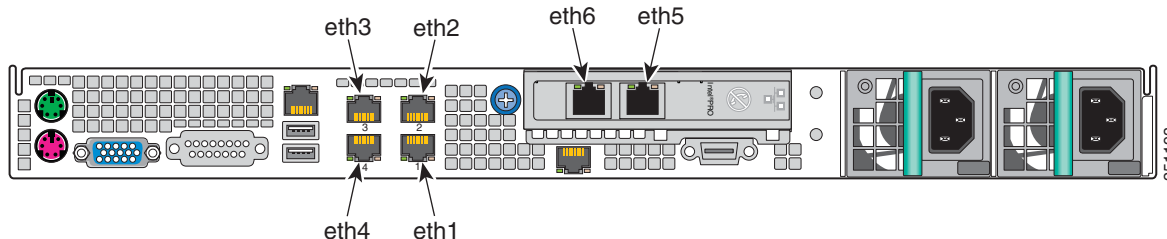
For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE110 back panel are specified as eth1 to eth6 as shown in Figure D-6.



**Note**

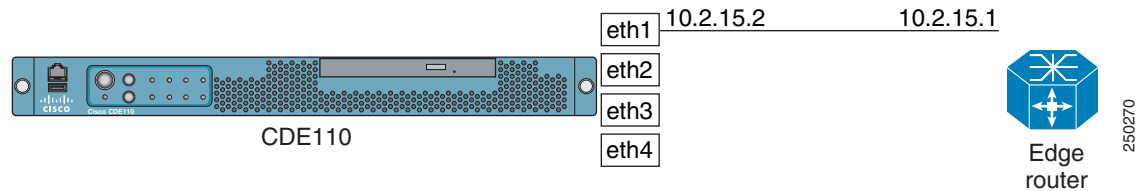
Earlier models of the CDE110 have four Ethernet ports (eth1 to eth4). These models did not have the Intel PRO/1000 PT Dual Port Server Adapter that provides the eth5 and eth6 ports.

**Figure D-6 NIC Port Numbering for Software Configuration**



For the configuration examples in this section, [Figure D-7](#) shows the IP addresses for interface eth1 and the corresponding interface on the edge router.

**Figure D-7** IP Addresses for VQE Tools Configuration Examples



**Note**

The configuration examples in this section assume that one CDE110 Ethernet interface (eth1) are used to connect to the VQE network.

To configure the Linux operating system and other software for the VQE Tools (VCPT and 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 VCPT.

**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.ethx.addr` parameters, where `ethx` 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 are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

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.static_route`. The configuration example in this section assumes that one CDE110 Ethernet interface (`eth1`) is 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 route parameter to configure this access.

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.network.interface.mgmt_interfaces` parameter and specifying the needed values using the following format:

```
network.network.interface.mgmt_interfaces="ethernet-interface-name, ethernet-interface-name"
```

The *ethernet-interface-name* arguments are names of the interfaces designated for management traffic. One or more CDE110 Ethernet interfaces may be designated for management traffic. For this example, assume CDE110 Ethernet interface `eth1(10.2.9.2)` on the VQE Tools host is designated for management traffic.

The line in the `vcdb.conf` file is as follows:

```
network.network.mgmt_interfaces="eth1"
```

- Step 3** Edit the `/etc/opt/vqes/vcdb.conf` file by adding to the file a `network.route.static_route` parameter and specifying the needed values using the following format:

```
network.route.static_route="target-network-subnet-addr/prefix-length via gateway-addr:outbound-interface"
```

The *target-network-subnet-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 is used for management network traffic. The *outbound-interface* is the interface used on the VQE Tools server for this static route

For this example, assume the following:

- CDE110 Ethernet interface `eth1 (10.2.15.2)` is used for the management network.
- Management network is `192.0.0.0/8`.

The line in the `vcdb.conf` file is as follows:

```
network.route.static_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-7](#) shows the IP addresses used in this example for the `eth1` interface and the directly attached router.

- Step 4** Save the `vcdb.conf` file.
- 

**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the [“Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status”](#) section on page D-44. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

---

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 is 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 external 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 external NTP server is 10.2.26.2.
- Step 5** Save the `vcdb.conf` file.
- 



### Note

VCDB configurations are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe\_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

---

For information on starting the NTP service (`ntpd` daemon), see the [Starting VQE Tools System Services and Verifying Status](#) section.

## Configuring SNMP

The CDE110 that hosts the VQE Tools sever 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 VQE Tools server also provides a VQE-specific MIB and a system messages (Syslog) MIB. System messages that meet a specified severity level can be sent as SNMP traps to a NMS. Sending syslog traps is optional. For more information on the SNMP MIBs, see [Appendix B, “SNMP MIBs”](#).

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"`
  - `system.snmp.syslog_trap_enable="false"`
  - `system.snmp.syslog_trap_priority="2"`

For more information on these SNMP-related VCDB parameters, see [Table A-6 on page A-12](#).

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"  
system.snmp.syslog_trap_enable="true"  
system.snmp.syslog_trap_priority="4"
```

- Step 3** Save the `vcdb.conf` file.
- 

**Note**

VCDB configurations are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status, page D-44](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

---

## 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 or the `vcds_send_file` command sends a network configuration file to the VCDS, you specify, on the VQE Tools host, the IP address of the trusted VQE-C system configuration provisioning server or `vcds_send_file`. If `vcds_send_file` is used, *all Ethernet interfaces* (that have been assigned IP addresses) on the `vcds_send_file` host have to be specified as trusted provisioning clients. This requirement applies even when the VCDS is in the same VQE Tools server as the `vcds_send_file` command.

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 are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System and VQE-S Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the [“Using the VQE Configuration Tool Command-Line Options”](#) section on page 7-18.

---

## Configuring Remote Syslog Servers

VQE system messages can be sent by means of UDP to remote servers for centralized logging. The use of remote syslog servers is optional. For more information on configuring remote syslog servers, see the “[Remote Syslog Hosts](#)” section on page 28.

To configure remote syslog servers 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 parameter and specifying its value:
- `system.syslog.remote_server="IP_address"`

For more information on the remote logging VCDB parameters, see [Table A-6 on page A-12](#).

The following example shows the two `vcdb.conf` lines that specifies the remote logging parameter:

```
system.syslog.remote_server="192.0.7.25"
system.syslog.remote_server="192.0.7.26"
```

- Step 3** Save the `vcdb.conf` file.
- 



### Note

VCDB configurations are applied to the CDE110 when it is rebooted in the [Restarting the System and Verifying System and VQE-S Status](#) section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the `vqe_cfgtool` command with the `-apply` option to restart only the required services. For more information on the `-apply` option, see the “[Using the VQE Configuration Tool Command-Line Options](#)” section on page 7-18.

---

## Starting VQE Tools System Services and Verifying Status

[Table D-2](#) lists the system services that you configure and start, for the CDE110 that hosts VQE Tools. 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.                                 |
| vcds_snmpsa   | VCDS SNMP subagent                                          |
| syslog_snmpsa | Syslog SNMP subagent.                                       |
| snmpsa        | (Optional) The SNMP subagent.                               |

**Table D-2** System Services for CDE110 That Hosts VQE Tools (continued)

| Service       | Description                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <b>cron</b> 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 vcds_snmpsa
[root@system]# chkconfig vcds_snmpsa on
[root@system]# service vcds_snmpsa start

[root@system]# chkconfig --add syslog_snmpsa
[root@system]# chkconfig syslog_snmpsa on
[root@system]# service syslog_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 Intel 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 VCDS SNMP subagent, to verify the vcds\_snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep vcds_snmpsa
```

```
vcds_snmpsa     0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

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

```
vcds_subagent (pid 10088) is running...
```

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

```
root      17273 17182  0 08:54 pts/2     00:00:00 grep vcds_snmpsa
```

- Step 10** If you have configured and started the Syslog SNMP subagent, to verify the syslog\_snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep syslog_snmpsa
```

```
syslog_snmpsa   0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

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

```
syslog_subagent (pid 9886) is running...
```

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

```
root      17984 17946  0 09:16 pts/2     00:00:00 grep syslog_snmpsa
```

- Step 11** 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, VCDS AMT and VCPT Status

This section explains how to start the VCDS service and verify that the process is running and that VCPT and the VCDS AMT are available.



### Note

VCPT and VCDS AMT are web applications and have no dedicated processes associated with them. The processes needed for the VCPT and VCDS AMT web applications to work (for example, the web server) are started automatically when the Cisco CDE110 is started.

To start the VCDS service and verify VCDS, VCDS AMT, 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

VCDServer (pid 29860) is running...
```

**Step 4** To check that the VCDS process (VCDServer) is running, issue the following command:

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

root          29860          1  0 Jul25 ?          00:00:00 /opt/vqes/bin/VCDServer
```

**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.

**Step 6** To use the VCDS AMT from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE Tools server

```
https://ip_address_of_VQE_Tools_host/vclds-amt
```

Log in using the vqe username and password. (Any valid Linux username and password can be used to log in to the VCDS AMT.)

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

## Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status

To restart the Cisco CDE110 and verify system, VCPT, VCDS (VCDS), and VCDS AMT 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 Intel snmpsa service is running, issue the following command:
- ```
[root@system]# service snmpsa status
```
- ... Output omitted
- Step 9** If you configured SNMP, to verify that the VCDS subagent service is running, issue the following command:
- ```
[root@system]# service vcds_snmpsa status
```
- ... Output omitted

**Step 10** If you configured SNMP, to verify that the Syslog subagent service is running, issue the following command:

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

... Output omitted

**Step 11** If you have configured an external NTP server, to verify that the ntpd service is running, issue the following command:

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

... Output omitted

**Step 12** To check that the vcds service is running, issue the following command:

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

... Output omitted

**Step 13** 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_VQE_Tools_host
```

Log in with a Linux username and password.

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

**Step 14** To that VCDS AMT from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE Tools server

```
https://ip_address_of_VQE_Tools_host/vcgs-amt
```

Log in using the vqe username and password. (Any valid Linux username and password can be used to log in to the VCDS AMT.)

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

**Step 15** Do one of the following:

- If the preceding checks indicate that all is well, you are ready to start using VCPT and VCDS AMT. For information on VCPT, see [Chapter 3, “Using the VQE Channel Provisioning Tool.”](#) For information on VCDS AMT, see [Chapter 5, “Using the VCDS AMT.”](#)
- 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 a channel configuration file and per-client network configuration file to the VQE Clients (VQE-Cs) in a VQE system. The VQE Client Configuration Delivery Server (VCDS) or a Real Time Streaming Protocol (RTSP) server sends the channel configuration file and network configuration file to the VQE-Cs on the set-top boxes (STBs).

This appendix provides information on configuring the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers so that they work correctly with the VCDS or with 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 a VQE-C to use the configuration delivery infrastructure. For information on the VQE-C system configuration parameters, see the *Cisco CDA Visual Quality Experience Client System Configuration Guide* listed in the “[Related Documentation](#)” section on page xi.

---

The components and interactions of the VQE CDI are shown in [Figure E-1](#). In this example, the VCDS sends the channel configuration file to the VQE-C. 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 hostname of one or more of the VCDS interfaces to VQE-C when the service lookup is for `_vqe_channel_cfg._tcp` (*exact string required*) with the VCDS domain name appended, as in `_vqe_channel_cfg._tcp.<VCDS_domain_name>`.

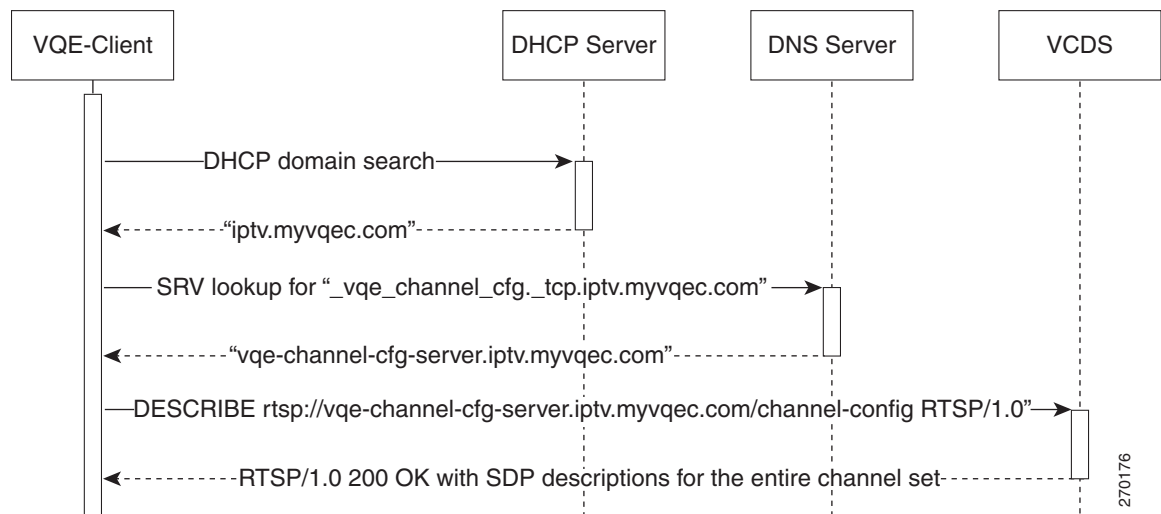


### Caution

The `_vqe_channel_cfg._tcp` part of the string is hardcoded in the 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.

---

Figure E-1 VQE Configuration Delivery Infrastructure



As shown in [Figure E-1](#), the interactions between the VQE-C and the other components of the configuration delivery infrastructure are as follows:

1. The VQE-C on the STB sends out a DHCP domain search request.
2. The DHCP server returns the domain (in this example, `iptv.myvqec.com`) to which the VCDS belongs. The domain is user-defined and configured in the DHCP server.
3. After receiving the domain name from the DHCP server, the VQE-C makes a DNS service request for the following string:  
`_vqe_channel_cfg._tcp.iptv.myvqec.com`
4. The DNS server responds with the hostname of each of the VCDS server interfaces defined in the SRV records in the DNS. In addition, the response may include the IP address of each VCDS server interfaces. If the IP addresses are not returned, the VQE-C initiates a separate request for them.
5. If the DNS query is successful, the VQE-C parses out the VCDS IP addresses from the DNS server response. If multiple interfaces are returned in the DNS response, the VQE-C randomizes the list of VCDS IP addresses returned by the DNS. The VQE-C sends out an RTSP DESCRIBE request for channel configuration data to the first VCDS interface on the list. The VQE-C waits 5 seconds for a response before it tries to connect to the next VCDS interface in the list. If the VQE-C tries all listed interfaces and no response is received, the RTSP DESCRIBE operation has failed.



**Note** The TCP implementation determines how many SYN packets are sent to the VCDS interface within the 5-second timeout interval.

6. If the RTSP DESCRIBE operation is successful, the VCDS sends back to the VQE-C the channel configuration data for the entire channel set in Session Description Protocol (SDP) format.

The VQE-C attempts to update the local `channel_lineup` file. During VQE-C initialization, if either 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. After the VQE-C has initialized, if either the DNS query or the RTSP DESCRIBE operation fails, the channel configuration is not updated.



## APPENDIX **F**

# Using the `vcds_send_file` Command

---

This appendix provides overview information on network-based per-client configuration of the VQE Client (VQE-C). It also explains how to use the `vcds_send_file` command to send the client database file and group attribute file to one or more VQE Client Configuration Delivery Servers (VCDSs).

## VQE CDI and VQE-C Network-based Per-Client Configuration

The VQE configuration delivery infrastructure (CDI) is used to deliver a channel configuration file and per-client network configuration file to the VQE-Cs on the set-top boxes (STBs). With the CDI, a VCDS or an RTSP server sends these two files to the VQE-Cs.

To create the network configuration files for the VQE-Cs, VCDS requires the following files:

- *Client database file*—In this file, each STB VQE-C has a unique identity (for example, MAC address) that is associated with a group identifier (group ID) for the specific network configuration that should be applied to the VQE-C system. Each VQE-C is associated with one group ID. The client database file can be a complete set of all STBs or a subset which adds to or modifies a previous set that exists on the VCDS.
- *Group attribute file*—In this file, different sets of per-client network configurations are defined. Each set of attributes is identified by a group ID.

The client database file and the group attribute file are XML-based and follow a schema specified by a specification defined by Cisco.

- Schema for the client database file is located at `/usr/share/tomcat5/webapps/vcds-amt/WEB-INF/db_schema.xsd`. The example file `/etc/opt/vqes/groupmap_sample.xml` contains an example of how to do group mapping.
- Schema for the group attribute file is located at `/usr/share/tomcat5/webapps/vcds-amt/WEB-INF/grp_cfg_schema.xsd`. The example file `/etc/opt/vqes/clientcfg_sample.xml` contains an example with all VQE-C attributes that are allowed.



### Note

The example client database and group attribute files are not preserved during an upgrade of the VQE-S. Any changes made to either file are lost.

---

A VQE-C system configuration provisioning server or the `vcds_send_file` command is used to send the client database file and the group attribute file to one or more VCDS servers. The `vcds_send_file` command is included with the VQE Tools software.

For more information on the roles VCDS and the VQE-C system configuration provisioning server, see the [“VCDS Delivery of the Per-Client Network Configuration File”](#) section on page 18.

# The `vcds_send_file` Command

The `vcds_send_file` command can be used to send the client database file and the group attribute file to a VCDS.

The syntax for the `vcds_send_file` command is as follows:

```
vcds_send_file type hostname filename
```

| Syntax Description |                 |                                                                                                                                                                                                                                                                     |
|--------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>type</i>     | Specifies the type of file that is sent to the VCDS. The following values are allowed: <ul style="list-style-type: none"> <li>VQE-GROUPMAP—Client database file</li> <li>VQE-GROUPATTR—Group attribute file</li> </ul>                                              |
|                    | <i>hostname</i> | Specifies the hostname or IP address of the VCDS to which the file is sent. If the VCDS to which the file is sent resides on the same VQE Tools server as the sending <code>vcds_send_file</code> command, <code>localhost</code> can be used for <i>hostname</i> . |
|                    | <i>filename</i> | Specifies the full pathname of the file that is sent to the VCDS. The file contents (a client database file or a group attribute file) must match the value given in the <i>type</i> argument.                                                                      |

## Usage Guidelines

The `vcds_send_file` command sends the client database file and the group attribute file to the VCDS using HTTPS. The VCDS to which the files are sent can be located on the same VQE Tools server where the `vcds_send_file` command is issued or can be located on a different VQE Tools server. On the VQE Tools server, the `vcds_send_file` executable is located at `/opt/vqes/bin/vcgs_send_file`.



### Note

You must log in as root to execute the `vcds_send_file` command.

To have the operating system find the `vcds_send_file` executable, you must set the `PATH` environment variable to include the location of the `/opt/vqes/bin` directory, or use the full path to `vcds_send_file` when executing the command.

## Examples

The following examples show how to use the `vcds_send_file` command to send a client database file and a group attribute file.

```
[root@system ~]# /opt/vqes/bin/vcgs_send_file VQE-GROUPMAP localhost
/etc/opt/vqes/groupmap_sample.xml
```

```
Status Code: 200
Status Message: Succeeded -- Received a new group map file for VQE-C
```

```
[root@system ~]# /opt/vqes/bin/vcgs_send_file VQE-GROUPATTR localhost
/etc/opt/vqes/clientcfg_sample.xml
```

```
Status Code: 200
Status Message: Succeeded -- Received a new attribute file for VQE-C
```

```
[root@system ~]#
```



## APPENDIX **G**

# 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 (VQE-S) 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 Cisco 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 Cisco VQE Release 3.0, changing the boot sequence should not be needed.

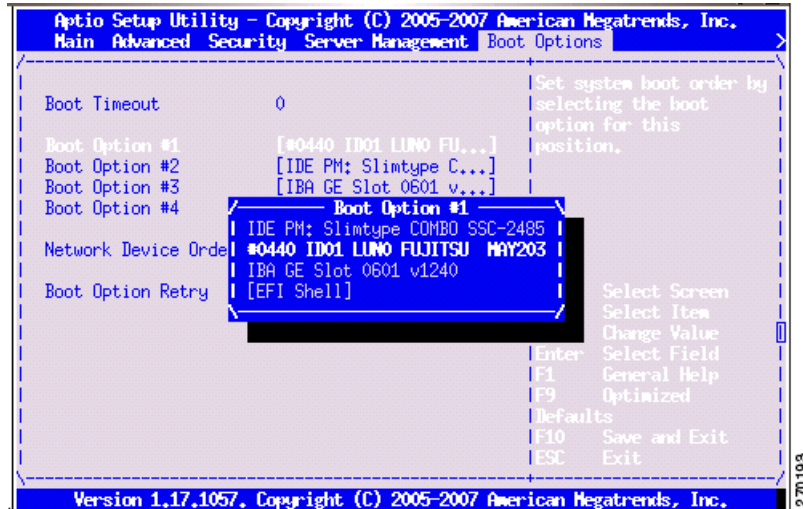
For information on installing VQE software, see the release notes for your version of the VQE software.

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 G-1).

**Figure G-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 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.



## VQE Server Performance and Scaling Limits

This appendix summarizes performance information of the Cisco CDE110 and CDE111 platforms hosting the Cisco VQE Server (VQE-S), and provides information on how to access VQE-S capacity statistics. The information is for general deployment estimates only and may vary according to network designs.

### Ingress and Egress Bandwidth Limits

[Table H-1](#) presents ingress and egress bandwidth limits for all Cisco VQE releases of the CDE110 platform hosting the VQE-S.

**Table H-1** *Ingress and Egress Bandwidth Limits of the CDE110 Platform hosting the VQE-S*

| Version               | Ingress Maximum Bandwidth (Gbps) | Egress Maximum Bandwidth (Gbps) | Combined Egress and Ingress Maximum Bandwidth (Gbps) |
|-----------------------|----------------------------------|---------------------------------|------------------------------------------------------|
| Cisco VQE Release 2.1 | 1.0                              | 1.0                             | 2.0                                                  |
| Cisco VQE Release 3.0 | 1.0                              | 1.5                             | 2.5                                                  |
| Cisco VQE Release 3.1 | 1.0                              | 2.0                             | 3.0                                                  |
| Cisco VQE Release 3.2 | 1.0                              | 2.0                             | 3.0                                                  |
| Cisco VQE Release 3.3 | 1.0                              | 2.0                             | 3.0                                                  |
| Cisco VQE Release 3.4 | 1.0                              | 2.0                             | 3.0                                                  |
| Cisco VQE Release 3.5 | 1.0                              | 2.0                             | 3.0                                                  |

[Table H-2](#) presents ingress and egress bandwidth limits for all VQE releases of the CDE111 platform hosting the VQE-S.

**Table H-2** *Ingress and Egress Bandwidth Limits of the CDE111 Platform hosting the VQE-S*

| Version               | Ingress Maximum Bandwidth (Gbps) | Egress Maximum Bandwidth (Gbps) | Combined Egress and Ingress Maximum Bandwidth (Gbps) |
|-----------------------|----------------------------------|---------------------------------|------------------------------------------------------|
| Cisco VQE Release 3.2 | 1.0                              | 3.0                             | 4.0                                                  |
| Cisco VQE Release 3.3 | 1.0                              | 3.0                             | 4.0                                                  |

**Table H-2** Ingress and Egress Bandwidth Limits of the CDE111 Platform hosting the VQE-S (continued)

|                       |     |     |     |
|-----------------------|-----|-----|-----|
| Cisco VQE Release 3.4 | 2.0 | 3.0 | 4.0 |
| Cisco VQE Release 3.5 | 2.0 | 3.0 | 4.0 |

As shown in [Table H-2](#), in Cisco VQE Release 3.4 and later releases, the maximum ingress bandwidth on the CDE111 platform hosting the VQE-S is up to 2 Gbps, and the maximum egress bandwidth is up to 3 Gbps. The combination of ingress and egress bandwidth cannot exceed 4 Gbps. For example, if 1 Gbps of ingress bandwidth is used, up to 3 Gbps of egress bandwidth may be used. Similarly, if 2 Gbps of ingress bandwidth are used, up to 2 Gbps of egress bandwidth may be used.

## Scaling and Performance Summary

[Table H-3](#) presents scaling and performance summary for all releases of the CDE110 and the CDE111 platforms hosting the VQE-S.

**Table H-3** Scaling and Performance Summary of the CDE110 and CDE111 Platforms hosting the VQE-S across all Releases

| Scale Factor                                                                                                                                                                                                                                    | Maximum Value across all Cisco VQE Releases                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Maximum number of Unicast Retransmission Repair Requests (NACKs) input per second.                                                                                                                                                              | 10,000 bitmaps resulting in a maximum of 50,000 RTP <sup>1</sup> packets                |
| Maximum Unicast Retransmission Rate—packets output per second.                                                                                                                                                                                  | 50,000                                                                                  |
| Maximum Number of Ingest Channels—This is subject to an additional constraint of platform ingest limits.                                                                                                                                        | 500 channels or the maximum ingest bandwidth in Gbps, whichever limit is reached first. |
| Maximum Number of Simultaneous Client Subscribers—Subscriber is defined as a consumer of video channel data. For a STB <sup>2</sup> with multiple tuners (such as a watch one, record one capable STB), the VQE-S counts this as 2 subscribers. | 32,000                                                                                  |

1. RTP = Real-time Transport Protocol.
2. STB = set-top box.

The VQE-S separates the bandwidth resources that are dedicated to Unicast Retransmission and Rapid Channel Change (RCC). A VQE-S configuration parameter (`vqe.vqes.reserved_er_bw`) controls the bandwidth resources that are dedicated to Unicast Retransmission. The parameter allows the amount of resources dedicated to Unicast Retransmission to be reduced so that the resources are available for RCC instead. For information on this parameter, see [Table A-2 on page A-5 of Appendix A, “VQE, System, and Network Parameters.”](#)

**Note**

VQE licenses for Unicast Retransmission and RCC are sold separately per STB. Software licenses for Unicast Retransmission and RCC are sold separately from the hardware.

**Note**

---

Each scaling limit is applied separately and all scaling limits must be met for proper service. Exceeding any of the scaling limits causes service to be denied.

---

## VQE-S Capacity Statistics

The VQE-S Application Monitoring Tool (AMT) displays several counters and statistics under **Capacity Statistics** on the **Statistics** tab of the **Error Repair and RCC Configuration** window which together indicate whether the Unicast Retransmission, RCC, or client subscriber capacity limits, presented in the [Scaling and Performance Summary](#) section, have been exceeded. For information on the capacity statistics, see the [“Viewing Error Repair and RCC Configuration”](#) section on page 4-16.

**Note**

---

The capacity statistics indicate when VQE services have been refused due to a capacity limit being reached. The capacity statistics provide no advanced warning of capacity limits being reached, nor do they provide an indication of when additional server capacity is required.

---





## VCPT Configuration Files

---

This appendix describes the VQE Channel Provisioning Tool (VCPT) import and export configuration file formats, and provides examples of both formats. This appendix contains the following sections:

- [Introduction, page I-1](#)
- [VCPT Configuration File Data Rules, page I-2](#)
- [VCPT Configuration in XML Format, page I-8](#)
- [VCPT Configuration in CSV Format, page I-21](#)

### Introduction

The VCPT is an optional channel-provisioning utility that assists with creating channel lineups required by both the VQE Server (VQE-S) and the VQE Client (VQE-C). A VCPT configuration contains a set of channel definitions, server definitions, and channel-server associations. The data can be entered directly using the VCPT GUI, or it can be imported from an external file. For more information on importing a configuration file, see the [“Importing a Configuration” section on page 3-4](#). The VCPT also provides an option to export a configuration to a file. For more information on exporting a configuration file, see the [“Exporting a Configuration” section on page 3-5](#).

The VCPT supports two configuration formats; extensible markup language (XML) and text-based, comma-separated values (CSV). A file in XML format must reference the XML schema file, `vcpt_doc.xsd`, which resides in the directory `/usr/share/tomcat5/webapps/vcpt/WEB-INF` on the VQE Tools server. The schema file constrains the set of elements that may be used in the configuration file and the order in which elements appear. It defines which attributes are applied to each elements, and describes parent/child relationships. When the VCPT loads a configuration file in XML format, it checks the configuration file against the file `vcpt_doc.xsd` for validity. A file in CSV format is made up of lines of ASCII text with values separated by commas. The benefit of using the CSV format is its simplicity. You can create a file in CSV format using any text editor.

The VCPT configuration file provides the following information for each channel in the channel lineup:

- Channel Identification
- Original Stream Configuration
- Unicast Retransmission Stream Configuration
- FEC 1 Stream Configuration
- FEC 2 Stream Configuration
- Enabling Channel Features Options

The VCPT configuration file provides the following information for each server in the channel lineup:

- Server name
- Unique identifier for the server
- Server role (such as VQE-S or VCDS)
- Server IP address
- Real-Time Transport Control Protocol (RTCP) Interval
- Maximum Receivers
- Channels assigned to the server

## VCPT Configuration File Data Rules

[Table I-1](#) below details the channel and server information included in both formats of the channel configuration file. The table presents the data type of each field and lists the rules associated with field.

Table I-1 Data Rules for Channel and Server Fields

| Data Field                 | In Format   | Data Type      | Rule                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|-------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Channel Information</b> |             |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Leading Label              | CSV only    | String         | <p>In Cisco VQE Release 3.5.4 and earlier releases the following data rules apply:</p> <ul style="list-style-type: none"> <li>• Each row representing a VQE-S or VCDS server must use SERVER as its label.</li> <li>• Each row representing a remote server must use SCP<sup>1</sup> as its label.</li> <li>• Each row representing a channel must use CHANNEL as its label.</li> </ul> <p>Starting with Cisco VQE Release 3.5.5 the following data rules apply:</p> <ul style="list-style-type: none"> <li>• Each row representing a VQE-S or VCDS server must use SERVER as its label.</li> <li>• Each row representing a remote server must use SCP as its label.</li> <li>• Each row representing a channel must use one of the following three labels: <ul style="list-style-type: none"> <li>– ER_CHANNEL—Channel data does not include FEC<sup>2</sup> services.</li> <li>– FEC_CHANNEL—Channel data includes FEC services.</li> <li>– CHANNEL—Provided for backward compatibility with Cisco VQE Release 3.5.4 and earlier releases.</li> </ul> </li> </ul> <p>The following data rule is common to all VQE 3.5 and later releases:</p> <ul style="list-style-type: none"> <li>• Only one label should be provided for each channel.</li> </ul> |
| Channel Identifier         | XML and CSV | String         | <p>The following data rules apply:</p> <ul style="list-style-type: none"> <li>• Unique identifier for the channel.</li> <li>• Range is from 1 to 20 alphanumeric characters.</li> <li>• Valid values include lowercase letters a to z, uppercase letters A to Z, and numeric characters from 0 to 9.</li> <li>• No duplicate channel entries are allowed in the configuration file.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Channel Data               | XML only    | attributeGroup | <p>The following data rules apply:</p> <ul style="list-style-type: none"> <li>• Set of attributes representing a channel.</li> <li>• Set of attributes includes id only.</li> <li>• Minimum number of channelData elements in an XML file is 0.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table I-1 Data Rules for Channel and Server Fields (continued)


| Data Field                                          | In Format   | Data Type  | Rule                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------|-------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Channel Name                                        | XML and CSV | String     | The following data rules apply: <ul style="list-style-type: none"> <li>Range is from 1 to 40 alphanumeric characters.</li> <li>Valid values include lowercase letters a to z, uppercase letters A to Z, and numeric characters 0 to 9.</li> <li>No spaces are allowed.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Original Source Stream Multicast IP address         | XML and CSV | IP address | The following data rules apply: <ul style="list-style-type: none"> <li>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.</li> <li>Range is from 224.0.0.0 to 239.255.255.255.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Original Source Stream RTP <sup>3</sup> Port Number | XML and CSV | Integer    | The following data rules apply: <ul style="list-style-type: none"> <li>RTP port number of the original source stream of the channel cannot be the same as the RTCP port number of the original source stream of the channel.</li> <li>Range is from 1024 to 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Original Source Stream RTCP Port Number             | XML and CSV | Integer    | The following data rules apply: <ul style="list-style-type: none"> <li>RTP port number of the original source stream of the channel cannot be the same as the RTCP port number of the original source stream of the channel.</li> <li>Range is from 1024 to 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Original Source Stream Source Filter IP Address     | XML and CSV | IP address | The following data rules apply: <ul style="list-style-type: none"> <li>Unicast IP address.</li> <li>Source filter IP address must not be equal to the Feedback Target IP address.</li> <li>Range is from 0.0.0.0 to 223.255.255.255.</li> </ul> <p> <b>Note</b> A channel may be defined with a source IP address of 0.0.0.0 for the Original Stream. When the channel Source IP address is 0.0.0.0 for the original stream, the SDP entry for this channel does not include the source-filter line in the original stream section that would be used to perform a SSM<sup>4</sup> join. In this case, the VQE-S and VQE-C does not perform an SSM join.</p> |

Table I-1 Data Rules for Channel and Server Fields (continued)

| Data Field                       | In Format   | Data Type  | Rule                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|-------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Original Source Stream Bit Rate  | XML and CSV | Integer    | The following data rules apply: <ul style="list-style-type: none"> <li>Bit rate of the original source stream of the channel in kilobits per second.</li> <li>Range is from 1000 to 30000.</li> <li>Specified bit rate should be equal to the primary stream bandwidth but should not include bandwidth used for FEC.</li> </ul>                                  |
| Enable Unicast Retransmission    | XML and CSV | Boolean    | Valid values are true and false.                                                                                                                                                                                                                                                                                                                                  |
| Enable Rapid Channel Change      | XML and CSV | Boolean    | Valid values are true and false.                                                                                                                                                                                                                                                                                                                                  |
| Enable RTCP Extended Reports     | XML and CSV | Boolean    | Valid values are true and false.                                                                                                                                                                                                                                                                                                                                  |
| Enable Reduced-size RTCP         | XML and CSV | Boolean    | Valid values are true and false. This field was introduced in Cisco VQE Release 3.5.5.                                                                                                                                                                                                                                                                            |
| Feedback Target Address          | XML and CSV | IP address | The following data rules apply: <ul style="list-style-type: none"> <li>Unique anycast IP address on the VQE-S that provide services for this channel.</li> <li>Feedback Target unicast IP address must be unique for each channel.</li> <li>Range is from 0.0.0.0 to 223.255.255.255.</li> </ul>                                                                  |
| Unicast Retransmission RTP Port  | XML and CSV | Integer    | The following data rules apply: <ul style="list-style-type: none"> <li>RTP port number of the Unicast Retransmission source stream of the channel cannot be the same as the RTCP port number of the Unicast Retransmission source stream of the channel.</li> <li>Range is from 1024 to 65535.</li> </ul>                                                         |
| Unicast Retransmission RTCP Port | XML and CSV | Integer    | The following data rules apply: <ul style="list-style-type: none"> <li>RTP port number of the Unicast Retransmission source stream of the channel cannot be the same as the RTCP port number of the Unicast Retransmission source stream of the channel.</li> <li>Range is from 1024 to 65535.</li> </ul>                                                         |
| FEC 1 Multicast Address          | XML and CSV | IP address | The following data rules apply: <ul style="list-style-type: none"> <li>Multicast IP address.</li> <li>Range is from 224.0.0.0 to 239.255.255.255.</li> <li>Configuring an FEC 1 Stream or an FEC 2 Stream provides 1-dimension FEC for the channel.</li> <li>Configuring an FEC 1 Stream and an FEC 2 Stream provides 2-dimension FEC for the channel.</li> </ul> |

**Table I-1 Data Rules for Channel and Server Fields (continued)**

| Data Field                     | In Format   | Data Type      | Rule                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|-------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FEC 1 RTP Port                 | XML and CSV | Integer        | The following data rules apply: <ul style="list-style-type: none"> <li>Range is from 1024 to 65535.</li> <li>RTP port number of the FEC 1 stream of the channel cannot be the same as the RTCP port number of the FEC 1 stream of the channel.</li> </ul>                                                                                                                                                 |
| FEC 1 Source Filter Address    | XML and CSV | IP address     | The following data rules apply: <ul style="list-style-type: none"> <li>Unicast IP address.</li> <li>Range is from 0.0.0.0 to 223.255.255.255.</li> </ul>                                                                                                                                                                                                                                                  |
| FEC 2 Multicast Address        | XML and CSV | IP address     | The following data rules apply: <ul style="list-style-type: none"> <li>Multicast IP address.</li> <li>Range is from 224.0.0.0 to 239.255.255.255.</li> <li>Configuring an FEC 1 Stream or an FEC 2 Stream provides 1-dimension FEC for the channel.</li> <li>Configuring an FEC 1 Stream and an FEC 2 Stream provides 2-dimension FEC for the channel.</li> </ul>                                         |
| FEC 2 RTP Port                 | XML and CSV | Integer        | The following data rules apply: <ul style="list-style-type: none"> <li>Port number specified for an FEC 2 stream cannot be the same as the port number used for the RTP or RTCP port for the Original Stream.</li> <li>RTP port number of the FEC 2 stream of the channel cannot be the same as the RTCP port number of the FEC 2 stream of the channel.</li> <li>Range is from 1024 to 65535.</li> </ul> |
| FEC 2 Source Filter IP address | XML and CSV | IP address     | The following data rules apply: <ul style="list-style-type: none"> <li>Unicast IP address.</li> <li>Range is from 0.0.0.0 to 223.255.255.255.</li> </ul>                                                                                                                                                                                                                                                  |
| <b>VQE-S Data</b>              |             |                |                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Name                    | XML and CSV | String         | The following data rules apply: <ul style="list-style-type: none"> <li>Range is from 1 to 40 characters.</li> <li>No spaces are allowed.</li> </ul>                                                                                                                                                                                                                                                       |
| Server Identifier              | XML and CSV | String         | The following data rules apply: <ul style="list-style-type: none"> <li>Unique identifier for the server.</li> <li>Range is from 1 to 20 alphanumeric characters.</li> </ul>                                                                                                                                                                                                                               |
| Server Data                    | XML only    | attributeGroup | The following data rules apply: <ul style="list-style-type: none"> <li>Set of attributes representing a server.</li> <li>Set of attributes includes id only.</li> </ul>                                                                                                                                                                                                                                   |

**Table I-1 Data Rules for Channel and Server Fields (continued)**

| Data Field                     | In Format   | Data Type   | Rule                                                                                                                                                                                                                                                  |
|--------------------------------|-------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Management IP Address   | XML and CSV | IP address. | The following data rules apply: <ul style="list-style-type: none"> <li>IP address of an Ethernet interface on the Cisco CDE110 server or Management IP address of an Ethernet interface on the remote server.</li> <li>Unicast IP address.</li> </ul> |
| Server Role                    | XML and CSV | Enumeration | The following data rules apply: <ul style="list-style-type: none"> <li>Role of the Cisco CDE110 server.</li> <li>Valid values are: <ul style="list-style-type: none"> <li>VQE-S</li> <li>VCDS</li> <li>SCP</li> </ul> </li> </ul>                     |
| Remote Server Port             | XML and CSV | Integer     | The following data rules apply: <ul style="list-style-type: none"> <li>SCP port number on the remote server.</li> <li>Range is from 1 to 65535.</li> </ul>                                                                                            |
| Remote Server Username         | XML and CSV | String      | The following data rules apply: <ul style="list-style-type: none"> <li>Username of the person authorized to access the path on the remote server.</li> <li>Range is from 1 to 40 characters.</li> </ul>                                               |
| Remote Server Location         | XML and CSV | String      | Remote path and filename for SCP operation.                                                                                                                                                                                                           |
| VQE-S and Channels Association | XML only    | Array       | Array of channels associated with the server.                                                                                                                                                                                                         |
| RTCP Interval                  | XML and CSV | Integer     | The following data rules apply: <ul style="list-style-type: none"> <li>Defines how often VQE-Cs send an RTCP report.</li> <li>Range is from 5 to 800.</li> </ul>                                                                                      |
| Maximum Receivers              | XML and CSV | Integer     | The following data rules apply: <ul style="list-style-type: none"> <li>Maximum number of receivers per server.</li> <li>Range is from 1 to 100,000.</li> </ul>                                                                                        |
| Channel Identifiers            | CSV only    | String      | Channel Identifiers for each channel associated with the server.                                                                                                                                                                                      |

1. SCP = Secure Copy Protocol.
2. FEC = Forward Error Correction.
3. RTP = Real-time Transport Protocol.
4. SSM = source specific multicast

When you import an external VCPT configuration file in either CSV or XML format, the only mandatory fields are Channel Identifier and Server Identifier. You can fill in all other fields using the VCPT GUI.

# VCPT Configuration in XML Format

A configuration file in XML format may be used to import configuration data into the VCPT or to export configuration data from the VCPT for modification or backup.

## XML Schema

On the VQE Tools server, the full path name of the XML schema file associated with the VCPT configuration file is `/usr/share/tomcat5/webapps/vcpt/WEB-INF/vcpt_doc.xsd`. The following is the XML schema defined in the file `vcpt_doc.xsd`:

```
<xs:schema xmlns:vqe="http://www.cisco.com/vqe/vcpt1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.cisco.com/vqe/vcpt1.0"
  version="1.0.0"
  elementFormDefault="qualified">
  <xs:element name="VcptFile" type="vqe:VcptFileType">
  </xs:element>
  <xs:complexType name="VcptFileType">
    <xs:sequence>
      <xs:element ref="vqe:channelData" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="vqe:serverData" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="version" type="xs:string" use="required"/>
  </xs:complexType>
  <!-- ***** -->
  <!-- VQE basic types -->
  <!-- ***** -->
  <xs:simpleType name="vqeStringType">
    <xs:restriction base="xs:string">
      <xs:minLength value="1"/>
      <xs:maxLength value="40"/>
      <xs:whiteSpace value="preserve"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="vqeIdType">
    <xs:restriction base="xs:string">
      <xs:minLength value="1"/>
      <xs:maxLength value="20"/>
      <xs:pattern value="[0-9a-zA-Z]+"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="vqePortType">
    <xs:restriction base="xs:positiveInteger">
      <xs:minInclusive value="1024"/>
      <xs:maxInclusive value="65535"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="vqeBooleanType">
    <xs:restriction base="xs:boolean"/>
  </xs:simpleType>
  <xs:simpleType name="vqeMulticastAddrType">
    <xs:restriction base="xs:string">
      <xs:pattern
value="(22[4-9]|23[0-9])\.((([1-9]?[0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.){2}([1-9]?[0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="vqeUnicastAddrType">
    <xs:restriction base="xs:string">
```

```

    <xs:pattern
value="([1-9]?[0-9]|1[0-9][0-9]|2[0-1][0-9]|22[0-3])\.\.([1-9]?[0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.\.){2}([1-9]?[0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])"/>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType name="vqeFBTAddrType">
    <xs:restriction base="xs:string">
        <xs:pattern
value="([1-9]|1[0-9][0-9]|1[0-9][0-9]|2[0-1][0-9]|22[0-3])\.\.([1-9]?[0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.\.){2}([1-9]?[0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])"/>
        </xs:restriction>
    </xs:simpleType>
<xs:simpleType name="vqeRoleType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="VQE-S"/>
        <xs:enumeration value="VCDS"/>
        <xs:enumeration value="SCP"/>
    </xs:restriction>
</xs:simpleType>
<xs:complexType name="extension_type">
    <xs:sequence>
        <xs:any processContents="lax" minOccurs="1"
maxOccurs="unbounded" namespace="##targetNamespace"/>
    </xs:sequence>
</xs:complexType>
<xs:element name="extension" type="vqe:extension_type"/>
<!-- ***** -->
<!-- VQE channel data -->
<!-- ***** -->
<xs:element name="channelData">
    <xs:complexType>
        <xs:all>
            <xs:element ref="vqe:channel-name"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:orig-multicast-addr"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:orig-RTP-port"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:orig-RTCP-port"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:src-filter-for-orig"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:bit-rate"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:error-repair"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:rapid-channel-change"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:RTCP-XR-report"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:RTCP-reduced-size"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:fbt-addr"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:rtx-RTP-port"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:rtx-RTCP-port"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:fec-col-multicast-addr"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:fec-col-RTP-port"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:src-filter-for-fec-col"
minOccurs="0" maxOccurs="1"/>
            <xs:element ref="vqe:fec-row-multicast-addr"
minOccurs="0" maxOccurs="1"/>
        </xs:all>
    </xs:complexType>
</xs:element>

```

```

        <xs:element ref="vqe:fec-row-RTP-port"
            minOccurs="0" maxOccurs="1"/>
        <xs:element ref="vqe:src-filter-for-fec-row"
            minOccurs="0" maxOccurs="1"/>
        <xs:element ref="vqe:extension"
            minOccurs="0" maxOccurs="1"/>
    </xs:all>
    <!-- Channel id attribute -->
    <xs:attribute name="id" use="required">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="20"/>
                <xs:pattern value="[0-9a-zA-Z]+"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
</xs:element>
<!-- channel-id -->
<xs:element name="channel-id">
    <xs:annotation>
        <xs:documentation>Unique channel id.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeIdType"/>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- channel-name -->
<xs:element name="channel-name">
    <xs:annotation>
        <xs:documentation>Channel name for viewing purpose only.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeStringType"/>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- orig-multicast-addr -->
<xs:element name="orig-multicast-addr">
    <xs:annotation>
        <xs:documentation>Multicast address for the original media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeMulticastAddrType"/>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- orig-RTP-port -->
<xs:element name="orig-RTP-port">
    <xs:annotation>
        <xs:documentation>RTP port for the original media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqePortType"/>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>

```

```

        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- orig-RTCP-port -->
<xs:element name="orig-RTCP-port">
    <xs:annotation>
        <xs:documentation>RTCP port for the original media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqePortType"/>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- src-filter-for-orig -->
<xs:element name="src-filter-for-orig">
    <xs:annotation>
        <xs:documentation>Source filter address for original media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeUnicastAddrType"/>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- bit-rate -->
<xs:element name="bit-rate">
    <xs:annotation>
        <xs:documentation>Bit rate for original stream.
        </xs:documentation>
    </xs:annotation>
    <xs:simpleType>
        <xs:restriction base="xs:nonNegativeInteger">
            <xs:minInclusive value="1000"/>
            <xs:maxInclusive value="30000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<!-- error-repair -->
<xs:element name="error-repair">
    <xs:annotation>
        <xs:documentation>Option for unicast error repair.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeBooleanType"/>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- rapid-channel-change -->
<xs:element name="rapid-channel-change">
    <xs:annotation>
        <xs:documentation>Option for rapid channel change.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeBooleanType"/>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>

```

```

<!-- RTCP-XR-report -->
<xs:element name="RTCP-XR-report">
  <xs:annotation>
    <xs:documentation>Option for RTCP XR report.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="vqe:vqeBooleanType"/>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<!-- RTCP-reduced-size -->
<xs:element name="RTCP-reduced-size">
  <xs:annotation>
    <xs:documentation>Option for reduced-size RTCP.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="vqe:vqeBooleanType"/>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<!-- fbt-addr -->
<xs:element name="fbt-addr">
  <xs:annotation>
    <xs:documentation>FBT address for the original media stream.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="vqe:vqeFBTAddrType"/>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<!-- rtx-RTP-port -->
<xs:element name="rtx-RTP-port">
  <xs:annotation>
    <xs:documentation>RTP port for retransmission media stream.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="vqe:vqePortType"/>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<!-- rtx-RTCP-port -->
<xs:element name="rtx-RTCP-port">
  <xs:annotation>
    <xs:documentation>RTCP port for retransmission media stream.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="vqe:vqePortType"/>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<!-- fec-col-multicast-addr -->
<xs:element name="fec-col-multicast-addr">
  <xs:annotation>
    <xs:documentation>Multicast address for FEC column media stream.
  </xs:annotation>

```

```

        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeMulticastAddrType" />
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- fec-col-RTP-port -->
<xs:element name="fec-col-RTP-port">
    <xs:annotation>
        <xs:documentation>RTP port for FEC column media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqePortType" />
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- src-filter-for-fec-col -->
<xs:element name="src-filter-for-fec-col">
    <xs:annotation>
        <xs:documentation>Source filter address for FEC column media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeUnicastAddrType" />
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- fec-row-multicast-addr -->
<xs:element name="fec-row-multicast-addr">
    <xs:annotation>
        <xs:documentation>Multicast address for FEC row media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeMulticastAddrType" />
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- fec-row-RTP-port -->
<xs:element name="fec-row-RTP-port">
    <xs:annotation>
        <xs:documentation>RTP port for FEC row media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqePortType" />
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- src-filter-for-fec-row -->
<xs:element name="src-filter-for-fec-row">
    <xs:annotation>
        <xs:documentation>Source filter address for FEC row media stream.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>

```

```

        <xs:extension base="vqe:vqeUnicastAddrType" />
    </xs:simpleContent>
</xs:complexType>
</xs:element>
<!-- ***** -->
<!-- VQE server data -->
<!-- ***** -->
<xs:element name="serverData">
    <xs:complexType>
        <xs:all>
            <xs:element ref="vqe:svr-name"
                minOccurs="0" maxOccurs="1" />
            <xs:element ref="vqe:svr-addr"
                minOccurs="0" maxOccurs="1" />
            <xs:element ref="vqe:svr-role"
                minOccurs="0" maxOccurs="1" />
            <xs:element ref="vqe:svr-port"
                minOccurs="0" maxOccurs="1" />
            <xs:element ref="vqe:svr-username"
                minOccurs="0" maxOccurs="1" />
            <xs:element ref="vqe:svr-remote-location"
                minOccurs="0" maxOccurs="1" />
            <xs:element ref="vqe:svr-channel-association"
                minOccurs="0" maxOccurs="1" />
            <xs:element ref="vqe:svr-rtcp-interval"
                minOccurs="0" maxOccurs="1" />
            <xs:element ref="vqe:svr-max-receivers"
                minOccurs="0" maxOccurs="1" />
        </xs:all>
        <!-- Server id attribute -->
        <xs:attribute name="id" use="required">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:minLength value="1" />
                    <xs:maxLength value="20" />
                    <xs:pattern value="[0-9a-zA-Z]+" />
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
    </xs:complexType>
</xs:element>
<!-- svr-name -->
<xs:element name="svr-name">
    <xs:annotation>
        <xs:documentation>VQE server name for viewing purpose only.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeStringType" />
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
<!-- svr-addr -->
<xs:element name="svr-addr">
    <xs:annotation>
        <xs:documentation>VQE server IP address.
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="vqe:vqeUnicastAddrType" />
        </xs:simpleContent>
    </xs:complexType>

```

```

</xs:element>
<!-- svr-role -->
<xs:element name="svr-role">
  <xs:annotation>
    <xs:documentation>VQE server role.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="vqe:vqeRoleType"/>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<!-- svr-port -->
<xs:element name="svr-port">
  <xs:annotation>
    <xs:documentation>Remote port for SCP operation.
    </xs:documentation>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:nonNegativeInteger">
      <xs:minInclusive value="1"/>
      <xs:maxInclusive value="65535"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<!-- svr-username -->
<xs:element name="svr-username">
  <xs:annotation>
    <xs:documentation>Remote user name for SCP operation.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="vqe:vqeStringType"/>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<!-- svr-remote-location -->
<xs:element name="svr-remote-location">
  <xs:annotation>
    <xs:documentation>Remote path and filename for SCP operation.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="vqe:vqeStringType"/>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
<!-- svr-channel-association -->
<xs:element name="svr-channel-association">
  <xs:annotation>
    <xs:documentation>VQE server and channels association.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="vqe:channel-id"
        minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<!-- svr-rtcp-interval -->

```

```

<xs:element name="svr-rtcp-interval">
  <xs:annotation>
    <xs:documentation>RTCP report interval.
    </xs:documentation>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:nonNegativeInteger">
      <xs:minInclusive value="5"/>
      <xs:maxInclusive value="800"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<!-- svr-max-receivers -->
<xs:element name="svr-max-receivers">
  <xs:annotation>
    <xs:documentation>Max receivers per server.
    </xs:documentation>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:nonNegativeInteger">
      <xs:minInclusive value="1"/>
      <xs:maxInclusive value="100000"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
</xs:schema>

```

**Note**

The data element RTCP-reduced-size was introduced in Cisco VQE Release 3.5.5.

## XML Data Elements and Attributes

Table I-1 presents the elements and attributes defined in `vcpt_doc.xsd`. This table maps each element and attribute to a data field. Table I-1 defines the data rules associated with each data field.

**Table I-2** Configuration File - XML Elements and Attributes

| Element/Attribute          | Data Field                                      |
|----------------------------|-------------------------------------------------|
| <b>Channel Information</b> |                                                 |
| channelData                | Channel Data                                    |
| id (attribute)             | Channel Identifier                              |
| channel-name               | Channel Name                                    |
| orig-multicast-addr        | Original Source Stream Multicast IP address     |
| orig-RTP-port              | Original Source Stream RTP Port Number          |
| orig-RTCP-port             | Original Source Stream RTCP Port Number         |
| src-filter-for-orig        | Original Source Stream Source Filter IP Address |
| bit-rate                   | Original Source Stream Bit Rate                 |
| error-repair               | Enable Unicast Retransmission                   |
| rapid-channel-change       | Enable Rapid Channel Change                     |
| RTCP-XR-Report             | Enable RTCP Extended Reports                    |

**Table I-2 Configuration File - XML Elements and Attributes**

| Element/Attribute       | Data Field                                                     |
|-------------------------|----------------------------------------------------------------|
| RTCP-reduced-size       | Enable reduced-size RTCP—Introduced in Cisco VQE Release 3.5.5 |
| fbt-addr                | Feedback Target Address                                        |
| rtx-RTP-port            | Unicast Retransmission RTP Port                                |
| rtx-RTCP-port           | Unicast Retransmission RTCP Port                               |
| fec-col-multicast-addr  | FEC 1 Multicast Address                                        |
| fec-col-RTP-port        | FEC 1 RTP Port                                                 |
| src-filter-for-fec-col  | FEC 1 Source Filter Address                                    |
| fec-row-multicast-addr  | FEC 2 Multicast Address                                        |
| fec-row-RTP-port        | FEC 2 RTP Port                                                 |
| src-filter-for-fec-row  | FEC 2 Source Filter IP Address                                 |
| <b>VQE-S Data</b>       |                                                                |
| serverData              | Server attributeGroup                                          |
| id (attribute)          | Server Identifier                                              |
| svr-name                | VQE-S Name                                                     |
| svr-addr                | Server Management IP Address                                   |
| svr-role                | Server Role                                                    |
| svr-port                | Remote Server Port                                             |
| svr-username            | Remote Server Username                                         |
| svr-remote-location     | Remote Server Location                                         |
| svr-channel-association | VQE-S and Channels Association                                 |
| svr-rtcp-interval       | RTCP Interval                                                  |
| svr-max-receivers       | Maximum Receivers                                              |
| channel-id              | Channel Identifier                                             |

## XML Example

The following section shows an example of the VQE Channel configuration file in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<VcptFile
  xmlns = "http://www.cisco.com/vqe/vcpt1.0"
  xmlns:xsi = "http://www.w3.org/2001/XMLSchema"
  version = "1.0.0">
  <channelData id = "1206996909">
    <channel-name>Channel 230.151.1.9</channel-name>
    <orig-multicast-addr>230.151.1.9</orig-multicast-addr>
    <orig-RTP-port>10032</orig-RTP-port>
    <orig-RTCP-port>10033</orig-RTCP-port>
    <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
    <bit-rate>20000</bit-rate>
    <error-repair>true</error-repair>
    <rapid-channel-change>true</rapid-channel-change>
  </channelData>
</VcptFile>
```

```

    <RTCP-XR-report>true</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.9</fbt-addr>
    <rtx-RTP-port>10034</rtx-RTP-port>
    <rtx-RTCP-port>10035</rtx-RTCP-port>
  </channelData>
  <channelData id = "1206996908">
    <channel-name>Channel 230.151.1.8</channel-name>
    <orig-multicast-addr>230.151.1.8</orig-multicast-addr>
    <orig-RTP-port>10028</orig-RTP-port>
    <orig-RTCP-port>10029</orig-RTCP-port>
    <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
    <bit-rate>15000</bit-rate>
    <error-repair>true</error-repair>
    <rapid-channel-change>true</rapid-channel-change>
    <RTCP-XR-report>true</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.8</fbt-addr>
    <rtx-RTP-port>10030</rtx-RTP-port>
    <rtx-RTCP-port>10031</rtx-RTCP-port>
  </channelData>
  <channelData id = "1206996907">
    <channel-name>Channel 230.151.1.7</channel-name>
    <orig-multicast-addr>230.151.1.7</orig-multicast-addr>
    <orig-RTP-port>10024</orig-RTP-port>
    <orig-RTCP-port>10025</orig-RTCP-port>
    <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
    <bit-rate>15000</bit-rate>
    <error-repair>true</error-repair>
    <rapid-channel-change>true</rapid-channel-change>
    <RTCP-XR-report>true</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.7</fbt-addr>
    <rtx-RTP-port>10026</rtx-RTP-port>
    <rtx-RTCP-port>10027</rtx-RTCP-port>
  </channelData>
  <channelData id = "1206996906">
    <channel-name>Channel 230.151.1.6</channel-name>
    <orig-multicast-addr>230.151.1.6</orig-multicast-addr>
    <orig-RTP-port>10020</orig-RTP-port>
    <orig-RTCP-port>10021</orig-RTCP-port>
    <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
    <bit-rate>2000</bit-rate>
    <error-repair>true</error-repair>
    <rapid-channel-change>true</rapid-channel-change>
    <RTCP-XR-report>true</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.6</fbt-addr>
    <rtx-RTP-port>10022</rtx-RTP-port>
    <rtx-RTCP-port>10023</rtx-RTCP-port>
  </channelData>
  <channelData id = "1206996905">
    <channel-name>Channel 230.151.1.5</channel-name>
    <orig-multicast-addr>230.151.1.5</orig-multicast-addr>
    <orig-RTP-port>10016</orig-RTP-port>
    <orig-RTCP-port>10017</orig-RTCP-port>
    <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
    <bit-rate>2000</bit-rate>
    <error-repair>true</error-repair>
    <rapid-channel-change>true</rapid-channel-change>
    <RTCP-XR-report>true</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.5</fbt-addr>
    <rtx-RTP-port>10018</rtx-RTP-port>
  </channelData>

```

```

    <rtx-RTCP-port>10019</rtx-RTCP-port>
  </channelData>
  <channelData id = "1206996904">
    <channel-name>Channel 230.151.1.4</channel-name>
    <orig-multicast-addr>230.151.1.4</orig-multicast-addr>
    <orig-RTP-port>10012</orig-RTP-port>
    <orig-RTCP-port>10013</orig-RTCP-port>
    <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
    <bit-rate>3750</bit-rate>
    <error-repair>true</error-repair>
    <rapid-channel-change>true</rapid-channel-change>
    <RTCP-XR-report>true</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.4</fbt-addr>
    <rtx-RTP-port>10014</rtx-RTP-port>
    <rtx-RTCP-port>10015</rtx-RTCP-port>
  </channelData>
  <channelData id = "1206996903">
    <channel-name>Channel 230.151.1.3</channel-name>
    <orig-multicast-addr>230.151.1.3</orig-multicast-addr>
    <orig-RTP-port>10008</orig-RTP-port>
    <orig-RTCP-port>10009</orig-RTCP-port>
    <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
    <bit-rate>3750</bit-rate>
    <error-repair>true</error-repair>
    <rapid-channel-change>true</rapid-channel-change>
    <RTCP-XR-report>true</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.3</fbt-addr>
    <rtx-RTP-port>10010</rtx-RTP-port>
    <rtx-RTCP-port>10011</rtx-RTCP-port>
  </channelData>
  <channelData id = "1206996902">
    <channel-name>Channel 230.151.1.2</channel-name>
    <orig-multicast-addr>230.151.1.2</orig-multicast-addr>
    <orig-RTP-port>10004</orig-RTP-port>
    <orig-RTCP-port>10005</orig-RTCP-port>
    <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
    <bit-rate>3750</bit-rate>
    <error-repair>true</error-repair>
    <rapid-channel-change>true</rapid-channel-change>
    <RTCP-XR-report>true</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.2</fbt-addr>
    <rtx-RTP-port>10006</rtx-RTP-port>
    <rtx-RTCP-port>10007</rtx-RTCP-port>
  </channelData>
  <channelData id = "1206996901">
    <channel-name>Channel 230.151.1.1</channel-name>
    <orig-multicast-addr>230.151.1.1</orig-multicast-addr>
    <orig-RTP-port>10000</orig-RTP-port>
    <orig-RTCP-port>10001</orig-RTCP-port>
    <src-filter-for-orig>0.0.0.0</src-filter-for-orig>
    <bit-rate>3750</bit-rate>
    <error-repair>false</error-repair>
    <rapid-channel-change>false</rapid-channel-change>
    <RTCP-XR-report>false</RTCP-XR-report>
    <RTCP-reduced-size>true</RTCP-reduced-size>
    <fbt-addr>8.61.1.1</fbt-addr>
    <rtx-RTP-port>10002</rtx-RTP-port>
    <rtx-RTCP-port>10003</rtx-RTCP-port>
    <fec-col-multicast-addr>230.151.1.1</fec-col-multicast-addr>
    <fec-col-RTP-port>20000</fec-col-RTP-port>
    <src-filter-for-fec-col>5.8.37.2</src-filter-for-fec-col>

```

```

    <fec-row-multicast-addr>230.151.1.1</fec-row-multicast-addr>
    <fec-row-RTP-port>20001</fec-row-RTP-port>
    <src-filter-for-fec-row>5.8.37.2</src-filter-for-fec-row>
</channelData>
<channelData id = "1206996910">
  <channel-name>Channel 230.151.1.10</channel-name>
  <orig-multicast-addr>230.151.1.10</orig-multicast-addr>
  <orig-RTP-port>10036</orig-RTP-port>
  <orig-RTCP-port>10037</orig-RTCP-port>
  <src-filter-for-orig>5.8.37.2</src-filter-for-orig>
  <bit-rate>12500</bit-rate>
  <error-repair>>true</error-repair>
  <rapid-channel-change>true</rapid-channel-change>
  <RTCP-XR-report>true</RTCP-XR-report>
  <RTCP-reduced-size>true</RTCP-reduced-size>
  <fbt-addr>8.61.1.10</fbt-addr>
  <rtx-RTP-port>10038</rtx-RTP-port>
  <rtx-RTCP-port>10039</rtx-RTCP-port>
  <fec-col-multicast-addr>230.151.1.10</fec-col-multicast-addr>
  <fec-col-RTP-port>20038</fec-col-RTP-port>
  <src-filter-for-fec-col>5.8.37.2</src-filter-for-fec-col>
  <fec-row-multicast-addr>230.151.1.10</fec-row-multicast-addr>
  <fec-row-RTP-port>20039</fec-row-RTP-port>
  <src-filter-for-fec-row>5.8.37.2</src-filter-for-fec-row>
</channelData>
<serverData id = "1246310633746">
  <svr-name>VCDS</svr-name>
  <svr-addr>10.86.21.70</svr-addr>
  <svr-role>VCDS</svr-role>
  <svr-channel-association>
    <channel-id>1206996901</channel-id>
    <channel-id>1206996910</channel-id>
    <channel-id>1206996902</channel-id>
    <channel-id>1206996903</channel-id>
    <channel-id>1206996904</channel-id>
    <channel-id>1206996905</channel-id>
    <channel-id>1206996906</channel-id>
    <channel-id>1206996907</channel-id>
    <channel-id>1206996908</channel-id>
    <channel-id>1206996909</channel-id>
  </svr-channel-association>
</serverData>
<serverData id = "1242662355264">
  <svr-name>VQE Server</svr-name>
  <svr-addr>10.86.21.70</svr-addr>
  <svr-role>VQE-S</svr-role>
  <svr-channel-association>
    <channel-id>1206996901</channel-id>
    <channel-id>1206996910</channel-id>
    <channel-id>1206996902</channel-id>
    <channel-id>1206996903</channel-id>
    <channel-id>1206996904</channel-id>
    <channel-id>1206996905</channel-id>
    <channel-id>1206996906</channel-id>
    <channel-id>1206996907</channel-id>
    <channel-id>1206996908</channel-id>
    <channel-id>1206996909</channel-id>
  </svr-channel-association>
</serverData>
<serverData id = "1259680856543">
  <svr-name>Carousel</svr-name>
  <svr-addr>10.86.21.76</svr-addr>
  <svr-role>SCP</svr-role>
  <svr-port>22</svr-port>

```

```

<svr-username>vqe</svr-username>
<svr-remote-location>/etc/opt/vqes</svr-remote-location>
<svr-channel-association>
  <channel-id>1206996901</channel-id>
  <channel-id>1206996910</channel-id>
  <channel-id>1206996902</channel-id>
  <channel-id>1206996903</channel-id>
  <channel-id>1206996904</channel-id>
  <channel-id>1206996905</channel-id>
  <channel-id>1206996906</channel-id>
  <channel-id>1206996907</channel-id>
  <channel-id>1206996908</channel-id>
  <channel-id>1206996909</channel-id>
</svr-channel-association>
</serverData>
</VcptFile>

```

In this example, 10 channels, a VCDS, a VQE-S, and a remote server are configured. Unicast retransmission and RCC are enabled on all channels, except for channel 230.151.1.1. FEC is configured on two channels: channel 230.151.1.1 and channel 230.151.1.10. Sending reduced-size RTCP packets is enabled on all channels. All 10 channels are associated with each server.

## VCPT Configuration in CSV Format

A configuration file in CSV format may be used to import configuration data into the VCPT or to export configuration data from the VCPT for modification or backup. Each line in the CSV configuration file represents a channel configuration, a server configuration, or a remote server configuration. [Table I-1](#) defines the data rules associated with each field of the configuration file.

Starting with Cisco VQE Release 3.5.5, the enable reduced-size RTCP option is added to the channel configuration. In this same release, the channel row in the CSV configuration file is separated into two rows: one for configuration of channels with no FEC services enabled, and one for configuration of channels with FEC services enabled.

The following list presents the data fields in Cisco VQE Release 3.5.5 and later releases for a channel configuration with no FEC services enabled in the CSV version of the configuration file. You must add fields in the order in which they are presented.

- Leading Label—ER\_CHANNEL
- Channel Identifier
- Channel Name
- Original Stream Multicast IP Address
- Original Source Stream RTP Port Number
- Original Source Stream RTCP Port Number
- Original Source Stream Source Filter IP Address
- Original Source Stream Bit Rate
- Feedback Target Address
- Unicast Retransmission RTP Port
- Unicast Retransmission RTCP Port
- Enable RTCP XR Reports
- Enable Unicast Retransmission

- Enable RCC
- Enable Reduced-Size RTCP

The following list presents the data fields in Cisco VQE Release 3.5.5 and later releases for a channel configuration with FEC services enabled in the CSV version of the configuration file. You must add fields in the order in which they are presented.

- Leading Label—FEC\_CHANNEL
- Channel Identifier
- Channel Name
- Original Stream Multicast IP Address
- Original Source Stream RTP Port Number
- Original Source Stream RTCP Port Number
- Original Source Stream Source Filter IP Address
- Original Source Stream Bit Rate
- Feedback Target Address
- Unicast Retransmission RTP Port
- Unicast Retransmission RTCP Port
- Enable RTCP XR Reports
- Enable Unicast Retransmission
- Enable RCC
- FEC 1 Multicast Address
- FEC 1 RTP Port
- FEC 1 Source Filter Address
- FEC 2 Multicast Address
- FEC 2 RTP Port
- FEC 2 Source Filter IP Address
- Enable Reduced-Size RTCP


**Note**

In Cisco VQE Release 3.5.5 and later releases, if more than one channel label is provided in the CSV file, the first label is accepted and all subsequent channel rows containing a different label are ignored.

The following list presents the data fields in Cisco VQE Release 3.5.4 and earlier releases for a channel configuration in the CSV version of the configuration file. You must add fields in the order in which they are presented.

- Leading Label—CHANNEL
- Channel Identifier
- Channel Name
- Original Stream Multicast IP Address
- Original Source Stream RTP Port Number
- Original Source Stream RTCP Port Number

- Original Source Stream Source Filter IP Address
- Original Source Stream Bit Rate
- Feedback Target Address
- Unicast Retransmission RTP Port
- Unicast Retransmission RTCP Port
- Enable RTCP XR Reports
- Enable Unicast Retransmission
- Enable RCC
- FEC 1 Multicast Address (Optional)
- FEC 1 RTP Port (Optional)
- FEC 1 Source Filter Address (Optional)
- FEC 2 Multicast Address (Optional)
- FEC 2 RTP Port (Optional)
- FEC 2 Source Filter IP Address (Optional)

The following list presents the data fields for a server (VCDS or VQE-S) configuration in the CSV version of the configuration file. You must add fields in the order in which they are presented.

- Leading Label
- Server Identifier
- Server Name
- Server Management IP Address
- Server Role
- Server RTCP Interval
- Server Maximum Receivers
- Channel Identifiers

The following list presents the data fields for an SCP (remote server) configuration in the CSV version of the configuration file. You must add fields in the order in which they are presented.

- Leading Label
- Server Identifier
- Server Name
- Server Management IP Address
- Server Role
- Server RTCP Interval
- Server Maximum Receivers
- Remote Server Port
- Remote Server Username
- Remote Server Location
- Channel Identifiers

## CSV Example

The following example shows a channel configuration file in CSV format prior to Cisco VQE Release 3.5.5:

```
#CHANNEL, id, name, multicast-addr, rtp-port, rtcp-port, src-ip, bit-rate, fbt-addr, rtx-rtp-port, r
tx-rtcp-port, xr-report-opt, err-opt, rcc-opt[, fec-col-addr, fec-col-port, fec-col-src-ip, fec-r
ow-addr, fec-row-port, fec-row-src-ip]
CHANNEL, 1206996909, Channel 230.151.1.9, 230.151.1.9, 10032, 10033, 5.8.37.2, 20000, 8.61.1.9, 100
34, 10035, true, true, true
CHANNEL, 1206996908, Channel 230.151.1.8, 230.151.1.8, 10028, 10029, 5.8.37.2, 15000, 8.61.1.8, 100
30, 10031, true, true, true
CHANNEL, 1206996907, Channel 230.151.1.7, 230.151.1.7, 10024, 10025, 5.8.37.2, 15000, 8.61.1.7, 100
26, 10027, true, true, true
CHANNEL, 1206996906, Channel 230.151.1.6, 230.151.1.6, 10020, 10021, 5.8.37.2, 2000, 8.61.1.6, 1002
2, 10023, true, true, true
CHANNEL, 1206996905, Channel 230.151.1.5, 230.151.1.5, 10016, 10017, 5.8.37.2, 2000, 8.61.1.5, 1001
8, 10019, true, true, true
CHANNEL, 1206996904, Channel 230.151.1.4, 230.151.1.4, 10012, 10013, 5.8.37.2, 3750, 8.61.1.4, 1001
4, 10015, true, true, true
CHANNEL, 1206996903, Channel 230.151.1.3, 230.151.1.3, 10008, 10009, 5.8.37.2, 3750, 8.61.1.3, 1001
0, 10011, true, true, true
CHANNEL, 1206996902, Channel 230.151.1.2, 230.151.1.2, 10004, 10005, 5.8.37.2, 3750, 8.61.1.2, 1000
6, 10007, true, true, true
CHANNEL, 1206996901, Channel 230.151.1.1, 230.151.1.1, 10000, 10001, 0.0.0.0, 3750, 8.61.1.1, 10002
, 10003, false, false, false, 230.151.1.1, 20000, 5.8.37.2, 230.151.1.1, 20001, 5.8.37.2
CHANNEL, 1206996910, Channel 230.151.1.10, 230.151.1.10, 10036, 10037, 5.8.37.2, 12500, 8.61.1.10,
10038, 10039, true, true, true, 230.151.1.10, 20038, 5.8.37.2, 230.151.1.10, 20039, 5.8.37.2
#SERVER, id, name, ip, role, rtcp-interval, max-receivers, channel-ids...
SERVER, 1246310633746, VCDS, 10.86.21.70, VCDS, , , 1206996901, 1206996910, 1206996902, 1206996903, 1
206996904, 1206996905, 1206996906, 1206996907, 1206996908, 1206996909
SERVER, 1242662355264, VQE Server, 10.86.21.70, VQE-S, , , 1206996901, 1206996910, 1206996902, 12069
96903, 1206996904, 1206996905, 1206996906, 1206996907, 1206996908, 1206996909
#SCP, id, name, ip, role, rtcp-interval, max-receivers, port, username, remote-location, channel-ids
...
SCP, 1259680856543, Carousel, 10.86.21.76, SCP, , , 22, vqe, /etc/opt/vqes, 1206996901, 1206996910, 12
06996902, 1206996903, 1206996904, 1206996905, 1206996906, 1206996907, 1206996908, 1206996909
```

In this example, 10 channels, a VCDS, a VQE-S, and a remote server are configured. Unicast retransmission and RCC are enabled on all channels, except for channel 230.151.1.1. FEC is configured on two channels: channel 230.151.1.1 and channel 230.151.1.10. All 10 channels are associated with each server.

The following example shows a channel configuration file in CSV format in Cisco VQE Release 3.5.5:

```
#ER_CHANNEL, id, name, multicast-addr, rtp-port, rtcp-port, src-ip, bit-rate, fbt-addr, rtx-rtp-por
t, rtx-rtcp-port, xr-report-opt, err-opt, rcc-opt, rtcp-rsize-opt
ER_CHANNEL, 1206996909, Channel 230.151.1.9, 230.151.1.9, 10032, 10033, 5.8.37.2, 20000, 8.61.1.9,
10034, 10035, true, true, true, false
ER_CHANNEL, 1206996908, Channel 230.151.1.8, 230.151.1.8, 10028, 10029, 5.8.37.2, 15000, 8.61.1.8,
10030, 10031, true, true, true, false
ER_CHANNEL, 1206996907, Channel 230.151.1.7, 230.151.1.7, 10024, 10025, 5.8.37.2, 15000, 8.61.1.7,
10026, 10027, true, true, true, false
ER_CHANNEL, 1206996906, Channel 230.151.1.6, 230.151.1.6, 10020, 10021, 5.8.37.2, 2000, 8.61.1.6, 1
0022, 10023, true, true, true, false
ER_CHANNEL, 1206996905, Channel 230.151.1.5, 230.151.1.5, 10016, 10017, 5.8.37.2, 2000, 8.61.1.5, 1
0018, 10019, true, true, true, false
ER_CHANNEL, 1206996904, Channel 230.151.1.4, 230.151.1.4, 10012, 10013, 5.8.37.2, 3750, 8.61.1.4, 1
0014, 10015, true, true, true, false
ER_CHANNEL, 1206996903, Channel 230.151.1.3, 230.151.1.3, 10008, 10009, 5.8.37.2, 3750, 8.61.1.3, 1
0010, 10011, true, true, true, false
ER_CHANNEL, 1206996902, Channel 230.151.1.2, 230.151.1.2, 10004, 10005, 5.8.37.2, 3750, 8.61.1.2, 1
0006, 10007, true, true, true, false
```

```
#SERVER, id, name, ip, role, rtcp-interval, max-receivers, channel-ids...
SERVER, 1246310633746, VCDS, 10.86.21.70, VCDS, , , 1206996902, 1206996903, 1206996904, 1206996905, 1206996906, 1206996907, 1206996908, 1206996909
SERVER, 1242662355264, VQE Server, 10.86.21.70, VQE-S, , , 1206996902, 1206996903, 1206996904, 1206996905, 1206996906, 1206996907, 1206996908, 1206996909
#SCP, id, name, ip, role, rtcp-interval, max-receivers, port, username, remote-location, channel-ids
...
SCP, 1259680856543, Carousel, 10.86.21.76, SCP, , , 22, vqe, /etc/opt/vqes, 1206996902, 1206996903, 1206996904, 1206996905, 1206996906, 1206996907, 1206996908, 1206996909
```

In this example, eight channels, a VCDS, a VQE-S, and a remote server are configured. Unicast retransmission and RCC are enabled on all channels. No FEC services are enabled. All eight channels are associated with each server. The field `rtcp_size-opt` was introduced in Cisco VQE Release 3.5.5. The option to send reduced-size RTCP packets is disabled for each channel.

## How to create the CSV format

You can create the CSV file by using lines of ASCII text with values separated by commas.

Use the following procedure to create a channel configuration file in CSV format.

- 
- Step 1** Open a text editor (such as Microsoft Notepad) or any application that allows you to export or create a CSV file.
- Step 2** Use a separate line to enter the values for a channel configuration or a server configuration. You must observe the following rules when you create the CSV data file.
- Always include comma separators, even if a field is blank.
  - You must enter channel, server, and remote server configurations on separate rows.
  - Label the first field of a row either CHANNEL, SERVER, or SCP to identify the type of data that the row represents.
  - If you insert a blank line an error will occur.
- Step 3** Upload the CSV file to the VQE Tools server on which the VCPT resides.
-





## INDEX

---

### Symbols

/etc configuration files

description [7-2](#)

managing with VQE CMS [7-2](#)

---

### A

access link bandwidth for each VQE-C [A-9](#)

access routes [2-16](#)

address and port-dependent mapping (with NAT) [1-10](#)

alarms [B-4](#)

anycast addresses [2-21, 3-8, 3-10](#)

Apache Tomcat application server [1-8, 2-31, 2-32, D-22, D-39](#)

Application Monitoring Tool (AMT)

*See* VQE-S Application Monitoring Tool (AMT)

-apply option to vqe\_cfgtool [7-18](#)

Area ID parameter [2-29](#)

Area Type parameter [2-29](#)

average stream rate [4-11](#)

---

### B

-backup option to vqe\_cfgtool [7-19](#)

bandwidth

conserving with RCC [A-6, A-7, A-8](#)

excess fraction [A-10](#)

maximum receive for a VQE-C [A-11](#)

on the access link for each VQE-C [A-9](#)

per VQE Client policing [A-5](#)

reserved for Unicast Retransmission [A-5](#)

reserving for incoming unicast traffic [A-9](#)

binding requests to STUN Server [1-10](#)

BIOS settings on CDE110 server [G-1](#)

Bit Rate field [3-11](#)

Bond interfaces

configuring [A-15, A-16, D-5](#)

description [2-15](#)

boot sequence on CDE110 server [G-1](#)

---

### C

cable connections [2-4, D-32](#)

cache time [A-6](#)

capacity statistics [4-23](#)

CD/DVD drive [G-1](#)

centralized logging [2-28, D-22, D-39](#)

certificate authority (CA) certificates

deploying commercial certificates [2-13](#)

generating [2-9](#)

installing [2-12](#)

Certificate Signing Request (CSR)

generating [2-10](#)

VQE Startup Configuration Utility [2-6](#)

Certificate-Signing Request (CSR)

signing [2-11](#)

channel change time [1-5](#)

Channel Lineups window [4-7](#)

channel-provisioning servers [2-27, D-21](#)

channels

associating with servers [1-15](#)

cloning with VCPT [3-13](#)

configuration database in VQE-S [1-9](#)

configuring [3-9](#)

copying associations with a server [3-19](#)

defining server associations [3-19](#)

- defining with VCPT [1-15, 3-11](#)
- deleting with VCPT [3-13](#)
- enabling Rapid Channel Change [3-10](#)
- error-repair options [3-11](#)
- lineups [1-7, 1-15, 1-22](#)
- Member Receiver Population [4-7](#)
- modifying configuration [C-3](#)
- multicast streams [3-10, 4-11](#)
- provisioning with VCPT [1-7, 1-16](#)
- rules for adding [3-11](#)
- viewing configuration with VQE-S AMT [4-8](#)
- viewing details with VCPT [3-12](#)
- viewing details with VQE-S AMT [1-21](#)
- viewing statistics with VQE-S AMT [4-10, 5-7](#)
- check\_daemons script [2-31, 2-32, D-23, D-40](#)
- Cisco CDA Visual Quality Experience Application
  - See* Cisco VQE
- Cisco CDE110 [1-4, 1-7, 1-9, 1-26](#)
  - configuring MIBs [D-20, D-22, D-37, D-39](#)
  - initial configuring for VQE-S [2-23, D-2](#)
  - initial configuring for VQE Tools [2-23, D-30](#)
  - restarting [D-28, D-44](#)
  - terminal emulation software [2-3](#)
  - viewing hardware information [4-6, 5-4](#)
- Cisco Digital Content Manager (DCM) [1-3, 1-7, 1-12](#)
- Cisco end-to-end IPTV solution model [1-14](#)
- Cisco set-top boxes [1-4, 1-12, 1-14](#)
- CISCO-SYSLOG-MIB
  - See* SNMP
- Cisco technical support [6-30](#)
- Cisco VQE
  - benefits [1-8](#)
  - deployment options [1-14](#)
  - deployment requirements [1-14](#)
  - Hybrid Error Repair [1-4](#)
  - major components [1-3](#)
  - overview [1-2](#)
  - reference architecture model [1-14](#)
  - software components [1-4](#)
  - software installation and upgrade [2-1](#)
- Cisco VQE Client (VQE-C)
  - See* VQE Client (VQE-C)
- Cisco VQE Server (VQE-S)
  - See* VQE Server (VQE-S)
- CISCO-VQES-MIB [B-5](#)
  - See* SNMP
- client database file [1-19, 1-20, F-1, F-2](#)
- cloning channels [3-13](#)
- commands
  - su and sudo [2-4](#)
  - vcds\_send\_file [F-1](#)
  - vqe\_cfgtool [7-18](#)
  - vqereport [6-29](#)
- config option to vqe\_cfgtool [7-19](#)
- configuration delivery infrastructure (CDI) [E-1, E-2, F-1](#)
- Configuration Engine (CE) [7-1](#)
- configuration files
  - managing with VQE CMS [7-2](#)
- Configuration Management System
  - See* VQE Configuration Management System (VQE CMS)
- configuration parameters (VCDB)
  - description [A-1](#)
  - network parameters [A-15](#)
  - OSPF parameters [A-18](#)
  - Rapid Channel Change parameters [A-6, A-9](#)
  - RTCP Exporter parameters [A-12](#)
  - system parameters [A-12](#)
  - Unicast Retransmission parameters [A-5, A-9](#)
  - VQE-S global parameters [A-2](#)
  - See also* VCDB parameters
- Configuration Tool (CT)
  - description [7-1, 7-3](#)
  - information on parameters [7-5](#)
  - parsing errors [7-3](#)
  - Root Menu [7-4](#)
  - using [7-4, 7-5](#)
  - vqe\_cfgtool command [7-18](#)

configuration utility for startup [2-23](#)  
 configuring VQE-S and VQE Tools servers  
   manually [D-1](#)  
   using VQE Startup Configuration Utility [2-1](#)  
 Control Plane process  
   monitoring by Process Monitor [1-10](#)  
   monitoring with Linux commands [2-40, D-28](#)  
   monitoring with VQE-S AMT [4-5](#)  
 CPE (customer premises equipment) [1-3, 1-4](#)  
   VQE-C integration [1-14](#)  
   VQE-C interface to VQE-S [1-11](#)

## D

Data Plane process  
   monitoring by Process Monitor [1-10](#)  
   monitoring with Linux commands [2-40, D-28](#)  
   monitoring with VQE-S AMT [4-5](#)  
 date and time  
   changing with Network Time Protocol [6-9, 6-31](#)  
   changing with the date command [6-10](#)  
 dead interval (OSPF) [A-20](#)  
 Dead Interval parameter [2-29](#)  
 debugging  
   configuring options [4-33](#)  
   messages written to vqe.log file [4-33, 5-9](#)  
   options in VQE-S AMT [1-22](#)  
 dedicated interfaces [2-18, D-15](#)  
 defining a channel [3-8](#)  
 defining channel associations with VCPT [3-19](#)  
 delay of IPTV packets [1-2, 1-13, 1-23](#)  
 Delete button in VCPT [3-4](#)  
 deleting channels [3-13](#)  
 Differentiated Services Code Point (DSCP)  
   configuring for RCC [A-8](#)  
   configuring for RTCP packets [A-4](#)  
   configuring for STUN Server binding requests [A-4](#)  
   configuring for Unicast Retransmission [A-6](#)  
   description [1-10](#)

  viewing configuration [4-17](#)  
 Digital Content Manager (DCM) [1-3, 1-5, 1-7, 1-14](#)  
 directories  
   for VCPT [6-4](#)  
   for VQE-S [6-4](#)  
 Domain Name System (DNS) servers [1-17, 2-24, A-12, E-1](#)  
 DSL  
   Cisco VQE for [1-2](#)  
   noise issues [1-8](#)  
 Dynamic Host Configuration Protocol (DHCP)  
 servers [E-1](#)  
 dynamic routing feature [2-17](#)

## E

Enable MD5 parameter [2-29](#)  
 Entitlement Control Messages (ECM) [1-6](#)  
 Equal Cost Multipath (ECMP) routes [2-22, 2-27, A-17, D-9](#)  
 error messages [C-4](#)  
 error repair  
   average rate [4-12, 4-19](#)  
   configuring [3-11](#)  
   options [3-8, 3-11](#)  
   *See also* FEC  
   *See also* Unicast Retransmission  
 Ethernet ports  
   CDE110 [1-26](#)  
   configuring [2-25, A-15](#)  
   Layer 3 connection [2-4](#)  
   MIB [B-4](#)  
   numbering [D-3, D-32](#)  
 excess bandwidth fraction [A-10](#)  
   configuring [A-10](#)  
   maximum [A-11](#)  
   minimum [A-11](#)  
   viewing configuration [4-16](#)  
   viewing distributions [4-21](#)  
 Export button in VCPT [3-4](#)  
 exporting RTP statistics [1-13, 1-23](#)

**F**

facility codes [C-1](#)

failover protection [2-21](#)

Fast Decoder Buffer Fill (FDBF) [1-7, A-6](#)

## FEC

configuring [3-11](#)

description [1-2, 1-12](#)

Hybrid Error Repair [1-4](#)

one and two dimensions [1-12](#)

stream generator [1-3](#)

VQE-C implementation [1-12](#)

feedback target addresses

anycast addresses [2-21, 3-8, 3-10](#)

static routes on attached router [2-47](#)

Feedback Target IP field [3-10, 3-11](#)

feedback target routes [2-16](#)

filenames

VCPT configuration files [3-4](#)

VQE-S and VCPT [6-3](#)

files

for VCPT [3-3, 6-4](#)

for VQE-S [6-4](#)

replacing a lost file [6-5](#)

-fix\_checksum -option to vqe\_cfgtool [7-19](#)

-fix\_config option to vqe\_cfgtool [7-19](#)

Force Update button [3-6](#)

forward error correction

*See* FEC

**G**

group attribute file [1-19, 1-20, F-1, F-2](#)

**H**

hello interval (OSPF) [A-19](#)

Hello Interval parameter [2-29](#)

hostname

configuring [2-24, D-4, D-33](#)

parameter [A-12](#)

HOST-RESOURCE-MIB [B-4](#)

httpd service

automatic start [2-31, 2-32](#)

error log [4-6, 5-4](#)

log files [6-11, 6-15](#)

restarting [6-11, 6-14](#)

verifying status [D-22, D-39](#)

HTTPS clients (trusted)

configuring on a VQE-S [2-27, D-21](#)

configuring on a VQE Tools server [D-38](#)

Hybrid Error Repair

Cisco VQE benefit [1-8](#)

configuring [3-11](#)

description [1-4](#)

*See also* error repair

HyperText Transfer Protocol daemon [2-31, 2-32, D-22, D-39](#)

**I**

If [A-3](#)

ifconfig command [D-6, D-34](#)

IF-MIB [B-4](#)

I-frames [1-6](#)

IGMP

channel change delay [1-2](#)

fast leave in access node [A-7](#)

join variability [A-6](#)

latency data [4-6](#)

VQE-S and multicast groups [1-9](#)

Import button in VCPT [3-4](#)

ingest of multicast streams [2-17, 2-29, 2-30, A-3, D-16](#)

initial configuration tasks

with manual configuration [D-1](#)

with VQE Startup Configuration Utility [2-1](#)

Input Bandwidth Table [4-27](#)

installing software [2-1](#)

INTEL-SERVER-BASEBOARD5 MIB [B-4](#)

## Interface parameters

reference information [A-15](#)

## interfaces

configuring [2-25, A-3, D-4, D-5, D-15, D-18, D-33](#)

configuring with Configuration Tool [7-6](#)

configuring with VCDB parameters [A-3, A-4](#)

dedicated [2-18, D-15](#)

for VQE-S ingest and services traffic [2-30, A-3, D-17](#)

for VQE-S ingest traffic [2-30, A-3, D-16, D-17](#)

for VQE-S services traffic [2-30, A-4, D-16, D-17](#)

shared [2-18, D-15](#)

Interface Summary Table [4-26](#)

ip link show command [D-6, D-34](#)

## IPTV

existing and new deployments [1-14](#)

packet loss [1-2, 1-23](#)

packets [1-7](#)

statistics [1-9](#)

subscribers [1-2](#)

video services [1-2](#)

## IPTV Packet Loss Monitoring

description [1-2](#)

with VQE-S RTCP Exporter [1-23](#)

## IPTV Services Delivery Server (ISDS)

cannot send channel information [6-13](#)

---

**J**

jitter [1-2, 1-13, 1-23](#)

---

**K**

keytool command [2-8](#)

---

**L**

Linux operating system [1-4, 1-8, 1-9, 1-26](#)

initial configuration [D-3, D-32](#)

MIBs [D-20, D-37](#)

## load balancing

of VQE-S services [1-9](#)

on VQE-Ss [2-21](#)

log files (VQE-related) [4-6, 5-4, 6-2](#)

## logging

configuring levels [4-33, 5-7, A-2](#)

levels [A-2](#)

messages written to vqe.log file [4-33, 5-7, A-2](#)

viewing log files [4-6, 5-4](#)

look-aside mode [1-8](#)

Loss RLE report block type [1-23, 4-8](#)

lost files [6-5](#)

---

**M**

## management networks

configuring for VQE-S hosts [2-16, D-6](#)

configuring for VQE Tools hosts [2-22, D-34](#)

configuring with VQE Startup Configuration Utility [2-26](#)

maximum receive bandwidth (MRB) [A-9, A-11](#)

MD5 authentication VCDB parameters [A-19](#)

MD5 Key ID parameter [2-29](#)

MD5 Key parameter [2-29](#)

Member Receiver Population [1-22, 4-7](#)

## messages

*See* system messages

Microsoft Internet Explorer [2-2](#)

Mozilla Firefox [2-2](#)

MPEG Parser [1-9](#)

Multicast Group Table [4-28](#)

multicast IP addresses [3-10](#)

Multicast IP field [3-10](#)

multicast IPTV [1-2](#)

multicast latency [1-6](#)

## Multicast Load Balancer process

description [4-27](#)

monitoring [4-5, 4-26](#)

Process Monitor role [1-10](#)  
 verifying it is running [2-40, D-28](#)  
 viewing statistics [1-21](#)

#### multicast streams

average rate [4-11](#)  
 for channels [1-9, 1-26, 3-10](#)  
 monitoring [6-8](#)

multiple definitions of VCDB parameters [7-15](#)

---

## N

### NACK messages

statistics [1-22, 4-11, 4-18](#)

### NAT

*See* Network Address Translation

Net-SNMP [B-3, D-20, D-37](#)

### Network Address Translation (NAT)

description [1-10](#)  
 STUN Server [A-4, D-20](#)

network configuration file [1-18](#)

network information [4-6, 5-4](#)

### network parameters

configuring [7-4](#)

### Network Time Protocol (NTP)

configuring [2-25, D-19, D-36](#)  
 daemon [2-31](#)  
 parameter [A-12](#)  
 with SSL certificates [2-11](#)

New Config button [3-4](#)

### ntpd service [2-31](#)

configuring and starting [D-22, D-40](#)  
 started automatically [2-32](#)  
 verifying it is running [2-40, 2-41](#)

---

## O

Open Configuration button [3-4](#)

open-source software [1-14](#)

OpenSSL Project [2-6](#)

original stream for a channel [3-10](#)

### OSPF

configuring for VQE-S traffic [D-10](#)  
 configuring system services [D-23](#)  
 initial configuration parameters [2-28](#)  
 on router attached to VQE-S host [2-45](#)  
 on VQE-S host [2-17](#)  
 routing type VCDB parameter [A-18](#)  
 status in VQE-S AMT [4-6](#)  
 VCDB parameters [A-18](#)  
 verifying edge router configuration [D-13](#)  
 verifying system services [D-25](#)  
 verifying VQE-S configuration [D-11](#)  
 VQE-S host in area 0 [2-46](#)  
 VQE-S host in separate area [2-45](#)  
 ospfd service [2-32, D-23](#)

---

## P

packet loss [1-2, 1-13, 1-23](#)

### packets

for IPTV [1-7](#)  
 lost [4-11](#)  
 received [4-11](#)  
 repair [4-11](#)  
 repair statistics [4-18](#)  
 RTCP [4-12](#)

### parameters

*See* VCDB parameters

### passwords

for root user [2-24](#)  
 for vqe user [2-4, 2-24](#)  
 requirements [2-24](#)

per-client network configuration [1-18](#)

### permissions for files and directories

changing [6-5](#)  
 for VCPT [6-4](#)  
 for VQE-S [6-4](#)

policing [A-5](#)  
 port usage on VQE-S [3-12](#)  
 Process Monitor process [1-10, 2-40, D-28](#)  
 Program Association Tables (PAT) [1-6](#)  
 Program Clock Reference (PCR) [1-6](#)  
 Program Map Tables (PMT) [1-6](#)

---

## Q

### Quagga

processes [2-32, D-23](#)  
 routing package [2-17](#)

---

## R

random access points (RAPs) [1-6, 4-17](#)  
 Rapid Channel Change (RCC) [1-2, 1-4](#)

- conserving bandwidth [A-6, A-8](#)
- e-factor histograms [4-14, 4-15, 4-21, 4-22](#)
- enabling with VCPT [3-10](#)
- monitoring statistics [1-22, 4-18, 4-23](#)
- parameters [A-6](#)
- viewing configuration [4-8, 4-16](#)
- viewing statistics [4-12](#)
- VQE-S role [1-9](#)

 Re-Activate button in VQE-S [4-7](#)  
 Real Time Streaming Protocol (RTSP) [1-17](#)  
 Real-Time Transport Protocol (RTP) [1-2, 1-3, 1-7, 1-14](#)

- repair packet statistics [4-18](#)

 rebooting
 

- VQE-S [C-3, D-28](#)
- VQE Tools server [D-44](#)

 recovery procedures [C-3](#)  
 Red Hat Enterprise Linux 5.1 operating system [1-26, D-3](#)  
 redundancy for VQE-S [1-10, 2-21, 3-8](#)  
 repair packets [4-11](#)  
 reset counters [4-31](#)  
 Resetting the root password [6-31](#)

resiliency of VQE-S [1-10](#)  
 restarting
 

- VCDS [6-31](#)
- VQE-S [6-30](#)
- VQE-S channels [C-3](#)

 restore counters [4-32](#)  
 -restore option to vqe\_cfgtool [7-19](#)  
 RMON MIB [B-4](#)  
 root user [2-4, 2-24, 2-33](#)  
 router attached to VQE-S host
 

- OSPF routing guidance [2-45](#)
- static routes for feedback targets [2-47, 3-8](#)

 Router ID parameter [2-29](#)  
 router ID VCDB parameter [A-18](#)  
 routing configuration
 

- for shared interfaces [2-18](#)
- overview [2-15](#)
- See also* OSPF

 routing types with VQE-S [2-28](#)  
 RTCP Exporter
 

- See* VQE-S RTCP Exporter

 RTCP Port field [3-10, 3-11](#)  
 RTCP Reports
 

- description [1-23](#)
- viewing configuration [4-8](#)

 RTP Control Protocol (RTCP)
 

- compound packets [1-23](#)
- description [1-7, 1-15](#)
- enabling and disabling [3-10](#)
- industry standards [1-2](#)
- packet statistics [4-12](#)
- sender and receiver reports [1-13](#)

 RTP inactivity timeout [A-4](#)  
 RTP Port field [3-10, 3-11](#)  
 RTSP DESCRIBE [E-2](#)

---

## S

-sanity\_check option to vqe\_cfgtool [7-20](#)

- Scientific-Atlanta IPTV Layer (SAIL) 1.x and 2.x [1-4](#)
- screen resolution requirements [2-2](#)
- SDP files created by VCPT [3-3](#)
- Secure Shell (SSH) [2-4](#)
- Secure Shell daemon [2-31, 2-32, D-22, D-39](#)
- Secure Sockets Layer (SSL) certificates
  - See* SSL certificates [D-3](#)
- security restrictions [2-4](#)
- selective retransmission
  - See* Unicast Retransmission
- Send button [3-5](#)
- sending channel information [3-5](#)
- serial ports [1-26](#)
- server.crt file [2-12, 2-13](#)
- server.key file [2-7, 2-12, 2-14](#)
- servers
  - adding [3-16](#)
  - defining with VCPT [3-14](#)
  - deleting with VCPT [3-18](#)
  - viewing server information [3-17](#)
- services
  - configuring and starting [D-23, D-43](#)
  - started automatically [2-31](#)
  - traffic for VQE-S [2-17](#)
  - VQE-S [1-10, 2-31, 6-30](#)
- Session Description Protocol (SDP) [1-7](#)
- set-top boxes [1-4, 1-7, 1-12, 1-14](#)
- severity levels [C-2](#)
- shared interfaces [2-18, D-15](#)
- SMPTE 2022 standard
  - stream orderings [1-13](#)
  - VQE-C extensions [1-13](#)
- SNMP
  - agent [B-2](#)
  - AgentX [B-3](#)
  - CISCO-SYSLOG-CAPABILITY [B-5](#)
  - CISCO-SYSLOG-MIB [B-5](#)
  - CISCO-VQES-MIB [B-5](#)
  - CISCO-VQE-TOOLS-MIB [B-5, B-8](#)
  - columnar objects [B-1](#)
  - community strings [2-28](#)
  - configuring [2-28, D-20, D-37](#)
  - events [1-27](#)
  - Intel subagent [B-3](#)
  - management hosts [2-28, A-13](#)
  - MIB [1-12, B-1](#)
  - object identifier [B-2](#)
  - parameters [A-13](#)
  - protocol-related counters [B-4](#)
  - scalar objects [B-1](#)
  - snmp manager [B-1](#)
  - SNMP subagent [B-3, D-22](#)
  - snmp subagent [B-1](#)
  - SNMPv2 [B-2](#)
  - trap [2-28, B-2](#)
  - viewing SNMP configuration [4-6, 5-4](#)
- snmpd service [2-31, 2-32, D-22, D-39](#)
- SNMP-NOTIFICATION-MIB [B-4](#)
- snmpsa service [2-31, 2-32, D-22, D-39](#)
- SNMP subagent [D-39](#)
- SNMP subagent daemon [2-31, 2-32](#)
- SNMPv2-MIB MIB [B-4](#)
- software components of Cisco VQE [1-4](#)
- software development kit (SDK) for VQE-C [1-13](#)
- software installation and upgrade [2-1](#)
- Source IP field [3-10, 3-11](#)
- SSH certificates [3-19](#)
- sshd service [2-31, 2-32, D-22, D-39](#)
- SSL certificates
  - deploying commercial [2-13](#)
  - deploying your own [2-10](#)
  - error log [4-6, 5-4](#)
  - setting up [2-5, D-3, D-32](#)
  - VQE Startup Configuration Utility [2-27](#)
- stackedChain.pem file [2-7, 2-8, 2-12, 2-13, 2-14](#)
- starting
  - VCDS [6-31, D-43](#)
  - VQE-S [6-30, D-27](#)

- startup configuration utility
    - See VQE Startup Configuration Utility
  - static routes
    - configuring for VQE-S traffic [D-8](#)
    - for a distribution network [D-7](#)
    - for a management network [D-6, D-34](#)
    - for feedback targets [2-45, 3-8](#)
    - limitations [2-16](#)
    - on VQE-S [2-16](#)
  - statistics
    - channels [4-10, 5-7](#)
    - Error Repair [4-16, 4-18, 4-23](#)
    - packet-loss monitoring [1-21](#)
    - RTCP Exporter [4-29](#)
  - Status of Last Send messages [3-15](#)
  - Status of Last Send Time [3-16](#)
  - status of VQE-S processes [1-7](#)
  - stopping
    - VCDS [6-31](#)
    - VQE-S [6-30](#)
  - Store As button [3-4](#)
  - Store button [3-4](#)
  - stream generators for FEC [1-3, 1-12](#)
  - STUN Client [1-10](#)
  - STUN Server [1-10](#)
    - configuration [1-11](#)
    - enabling [A-4, D-20](#)
    - monitoring [4-5](#)
  - su or sudo commands [2-4](#)
  - symmetric NAT [1-10](#)
  - syslog\_snmpsa service [2-31, 2-32, D-39](#)
  - syslog messages
    - See system messages [C-1](#)
  - syslog snmp service [D-22](#)
  - system.iptables.trusted\_provisioner parameter [A-14, D-38](#)
  - system console [2-5](#)
  - system information
    - system status [4-6, 5-4](#)
  - system messages
    - description [C-1](#)
    - no channel configuration [D-27](#)
    - online file with reference information [C-4](#)
    - setting logging level [4-33](#)
    - severity [C-2](#)
    - structure [C-1](#)
    - viewing system log [4-6, 5-4](#)
    - VQE-S logging [6-2](#)
    - written to vqe.log [4-33, 5-7, 6-2](#)
  - system parameters
    - configuring [7-4](#)
    - reference information [A-12](#)
    - See also VCDB parameters
  - system services
    - on VQE-S host [2-31, D-23](#)
    - on VQE Tools host [2-32, D-40](#)
  - system time
    - changing with Network Time protocol [6-9, 6-31](#)
    - changing with the date command [6-10](#)
- 
- ## T
- Telco Alarm Management [1-27](#)
  - terminal emulation software [2-3](#)
  - terminal servers [2-5](#)
  - time zones [2-25, A-13, D-19, D-36](#)
  - tomcat5 service
    - automatic start [2-31, 2-32](#)
    - log files [6-11, 6-15](#)
    - restarting [6-11, 6-14](#)
    - verifying status [D-22, D-39](#)
  - Tomcat log [4-6, 5-4](#)
  - TR-135 statistics [1-12](#)
  - TRAP listeners [B-4](#)
  - troubleshooting
    - channels not displayed in VQE-S AMT [6-11](#)
    - internal server error in VCPT [6-15](#)
    - multicast streams [6-8](#)
    - no graphs in VQE-S AMT [6-12](#)

repeated messages on Cisco CDE110 [6-9](#)  
 VCPT cannot send channel information [6-13, 6-15](#)  
 VCPT unavailable [6-10](#)  
 VQE-S, VQE-S AMT, and VCPT [6-7](#)  
 VQE-S AMT unavailable [6-10](#)  
 trustedca file [2-13, 2-14](#)  
 trusted provisioning clients [2-27, 6-13, A-14](#)  
 trusted provisioning servers [2-27, 6-13, A-14](#)

## U

unicast reservation [A-9](#)  
 Unicast Retransmission  
   bandwidth reserved [A-5](#)  
   configuring [3-11](#)  
   description [1-2](#)  
   Hybrid Error Repair [1-4](#)  
   monitoring statistics [1-21, 1-22, 4-16](#)  
   parameters [A-5](#)  
   per VQE Client policing [A-5](#)  
   viewing statistics [4-18, 4-23](#)  
   VQE-C role [1-11](#)  
   VQE-S AMT [1-7, 4-16](#)  
   VQE-S role [1-4, 1-9](#)  
 Unicast Retransmission Stream fields [3-11](#)  
 upgrading software [2-1](#)  
 usage statistics for channels [1-22](#)

## V

vcdb.conf.sample file [7-15](#)  
   description [7-15](#)  
   on VQE-S [6-4](#)  
   on VQE Tools server [6-4](#)  
   parameter information in [7-16](#)  
 vcdb.conf.tools.sample file [6-4](#)  
 VCDB file (vcdb.conf)  
   RTCP Exporter [2-43](#)

VCDB parameters  
   entering data [7-6](#)  
   multiple definitions allowed or not allowed [7-15](#)  
   order of [7-15](#)  
   reference information [A-1](#)  
   those not configurable with CT [7-5](#)

VCDB Parser  
   parsing errors [7-3](#)

### VCDS

*See* VQE Client Configuration Delivery Server (VCDS)

vcds\_send\_file command [F-1, F-2](#)

vcds\_snmpsa service [2-32](#)

### VCDS AMT

*See* VQE Client Configuration Delivery Server (VCDS)

VCDS Application Monitoring Tool (VCDS AMT) [5-1](#)

  configuring VCDS debugging [5-9](#)

  description [1-7](#)

  log files [5-7](#)

  logging in [5-2](#)

  navigating [5-2](#)

  VCDS Configuration Window [1-25](#)

  VCDS Status Information [1-24](#)

VCDServer process [D-43](#)

### vcds service

  configuring and starting [D-43](#)

  started automatically [2-32](#)

  verifying status [D-45](#)

vcds snmp service [D-39](#)

### VCPT

*See* VQE Channel Provisioning Tool (VCPT)

verifying host system

  for VCPT [D-44](#)

  for VQE-S [D-28](#)

verifying system services [2-38, 2-40, D-23, D-39, D-40](#)

video quality [1-2, 1-8, 1-23](#)

video-quality monitoring (VQM) application [1-23](#)

viewing channel details [3-12](#)

- VQE
  - See* Cisco VQE
  - vqe.cert file [2-7](#)
  - vqe.log file [4-33, 5-7, 5-9](#)
  - vqe\_cfgtool command [7-18](#)
    - config option [7-3](#)
  - VQE Channel Provisioning Tool
    - managing files [3-3](#)
  - VQE Channel Provisioning Tool (VCPT)
    - adding servers [3-16](#)
    - cloning channels [3-13](#)
    - configuration filenames [3-4](#)
    - configuration files [3-3](#)
    - copying channel associations [3-19](#)
    - csv [1-25](#)
    - csv format [1-21](#)
    - defining channel associations [3-18](#)
    - defining channels [2-21, 3-8, 3-9](#)
    - defining servers [3-14](#)
    - deleting channels [3-13](#)
    - deleting servers [3-18](#)
    - description [1-7, 1-15](#)
    - exporting [1-1](#)
    - export to remote server [1-17](#)
    - GUI [1-16](#)
    - importing [1-1](#)
    - initial configuring [2-1, D-1](#)
    - interactions with VQE Client Configuration Delivery Server [1-16](#)
    - interactions with VQE-S [1-16](#)
    - log files [6-3](#)
    - logging in [3-2](#)
    - provisioning channels [3-7](#)
    - sending channel information [3-7](#)
    - software [1-26](#)
    - SSL certificates [2-5](#)
    - Status of Last Send messages [3-15](#)
    - troubleshooting [6-7](#)
    - trusted HTTPS clients [D-21](#)
    - using [3-1](#)
    - verifying status [D-44](#)
    - viewing channel information [3-12](#)
    - viewing server information [3-17](#)
    - VQE deployment [1-15](#)
    - VQE reference architecture model [1-14](#)
    - xml schema [1-1, 1-8](#)
  - VQE Client (VQE-C)
    - Cisco end-to-end IPTV solution model [1-14](#)
    - description [1-4, 1-11](#)
    - DHCP and DNS servers [E-1](#)
    - Error Repair [1-11](#)
    - FEC [1-12](#)
    - IPTV Packet Loss Monitoring [1-11](#)
    - maximum receive bandwidth [A-11](#)
    - Network Address Translation (NAT) [1-10](#)
    - network configuration [1-20](#)
    - network connectivity [1-15](#)
    - number receiving a channel [1-22](#)
    - per-client policing [A-5](#)
    - policing [A-6](#)
    - policing for Unicast Retransmission [A-5](#)
    - Rapid Channel Change [1-7](#)
    - set-top box integration [1-14](#)
    - software development kit [1-13](#)
    - system configuration provisioning server [2-27, D-38](#)
    - VQE reference architecture model [1-14](#)
  - VQE Client Configuration Delivery Server (VCDS)
    - defining with VCPT [1-15](#)
    - description [1-7](#)
    - DHCP and DNS servers [E-1, F-1](#)
    - interactions with VQE Client [1-17](#)
    - log files [C-1](#)
    - role in VQE-C network configuration [1-20](#)
    - software [1-26](#)
    - starting [D-43](#)
    - starting and stopping [6-31](#)
    - system messages [C-1](#)
    - verifying status [D-43, D-45](#)

- VQE reference architecture [1-14](#)
- VQE Configuration Database (VCDB)
  - description [7-1](#)
  - parameters [A-1](#)
  - used for multiple CDE110 servers [7-3](#)
- VQE Configuration Management System (VQE CMS)
  - description [7-2](#)
  - vqe\_cfgtool command [7-18](#)
- VQE Configuration Tool
  - See* Configuration Tool
- VQE-C system configuration provisioning server [1-19](#), [1-20](#)
- VQE-GROUPATTR keyword [F-2](#)
- VQE-GROUPMAP keyword [F-2](#)
- vqereport command [6-29](#)
- vqes\_snmpsa service [2-31](#)
- VQE-S Application Monitoring Tool (AMT)
  - configuring logging [4-33](#), [5-7](#)
  - configuring VQE-S debugging [4-33](#), [5-9](#)
  - log files [6-3](#)
  - logging in [4-2](#), [5-2](#)
  - monitoring health of VQE-S processes [4-4](#), [5-3](#)
  - monitoring interfaces [4-26](#)
  - monitoring Multicast Load Balancer [4-26](#)
  - monitoring VQE-S RTCP Exporter [4-28](#)
  - navigating [4-4](#), [5-2](#)
  - troubleshooting [6-7](#)
  - using [4-1](#)
  - viewing channel configuration and status [4-7](#), [5-4](#)
  - viewing log files [4-6](#), [5-4](#)
  - web application [1-22](#)
- VQE-S Application Monitoring Tool (VQE-S AMT)
  - description [1-21](#)
- VQE Server (VQE-S)
  - bandwidth reserved for inbound requests [A-9](#)
  - cable connections [2-4](#)
  - configuring [2-1](#), [D-2](#)
  - configuring static routes [D-5](#), [D-8](#)
  - configuring VCDB parameters [7-4](#)
  - counters restarted [1-22](#)
  - current status [4-5](#)
  - debugging levels [1-21](#)
  - defining with VCPT [1-15](#)
  - description [1-4](#), [1-7](#), [1-9](#)
  - Equal Cost Multipath (ECMP) routes [2-27](#), [A-17](#), [D-8](#)
  - global parameters [A-2](#)
  - ingest and services traffic [A-3](#), [D-17](#)
  - ingest traffic [2-17](#), [2-29](#), [A-3](#), [D-17](#)
  - initial configuring [2-1](#), [D-1](#)
  - log files [6-2](#)
  - logging levels [1-21](#)
  - monitoring health of processes [1-21](#)
  - network connectivity [1-15](#)
  - per-client policing [A-5](#)
  - policers [1-9](#)
  - processes [1-10](#), [2-40](#), [4-5](#), [D-28](#)
  - Rapid Channel Change [1-9](#)
  - redundancy [1-10](#), [2-21](#)
  - resiliency [1-10](#)
  - routing overview [2-16](#), [2-17](#)
  - service (vqes) [1-10](#), [2-31](#), [6-30](#)
  - services traffic [2-17](#), [2-30](#), [A-4](#), [D-16](#)
  - software [1-26](#)
  - software version [4-5](#), [5-4](#)
  - starting [D-27](#)
  - starting and stopping [6-30](#)
  - static routes [D-10](#)
  - STUN Server [A-4](#), [D-20](#)
  - system messages [C-1](#)
  - system up time [4-5](#), [5-3](#)
  - trusted channel-provisioning servers [2-27](#), [D-21](#)
  - Unicast Retransmission [1-9](#)
  - verifying status [D-28](#)
  - viewing log file [4-6](#)
- VQE-S RTCP Exporter
  - configuring and enabling [2-42](#), [A-12](#)
  - description [1-23](#)
- IPTV Packet Loss Monitoring [1-2](#)

- monitoring with VQE-S AMT [4-28](#)
  - RTCP packet statistics [1-21, 4-29, 4-31](#)
- vqe-s snmpsa service [D-22](#)
- VQE Startup Configuration Utility
  - configuration items [2-24](#)
  - pre-configuration worksheets [2-33](#)
  - Root Menu choices [2-36, 2-37](#)
  - routing configuration [2-15](#)
  - using [2-23](#)
- VQE Tools server
  - configuring [2-1, D-30](#)
  - verifying status [2-40](#)
- vqe user ID [2-4, 2-24, 2-33, 2-34, 2-40, 2-42, D-4, D-33](#)
- vqm\_host parameter [A-12](#)
- vqm\_port parameter [A-12](#)
- VQM Host information [4-29](#)
- VQM TCP Port
  - information [4-29](#)

---

## W

- watchquagga process [2-32, D-23](#)
- web browser requirements [2-2](#)
- wheel group [2-4](#)

---

## X

- xDSL [1-2](#)
- XML schema and examples
  - for client database file [1-20, F-1](#)
  - for group attribute file [1-20, F-1](#)

---

## Z

- zebra service [2-32, D-23](#)

