Initial VQE Configuration

This chapter explains the initial configuration tasks needed to get the two categories of Cisco CDE servers running with the Cisco VQE software:

- VQE server (VQE-S)—CDE hosting VQE-S
- VQE Tools server—CDE 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 Release 3.11*.

Note We recommend that you use the **VQE Configuration Tool** rather than try to do the initial configuration manually because the tool 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 CDE configuration configuring a CDE:

Note The configuration instructions in this chapter are intended for new installations of Cisco VQE Software, Release 3.11, where the Cisco CDE has the Cisco VQE Software, Release 3.11 preinstalled.

For information on upgrading a Cisco CDE, see *Release Notes for Cisco CDA Visual Quality Experience Application, Release 3.11*.

This chapter assumes that the Cisco CDE hardware has been installed as described in *Cisco Content Delivery Engine 110 Hardware Installation Guide* and the *Cisco Content Delivery Engine 205/220/250/420 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[1]
161	SNMP[2]
162	SNMP traps
443	HTTPS[3]
444	HTTPS push
8005	Apache tomcat
8009	Apache tomcat
8050	VQE process monitor
8051	VQE-S CP[4] XML-RPC[5]
8052	MLB[6] 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 2-25.

Configuring Terminal Emulation Software

The RJ-45 serial ports on the Cisco CDE front and back panels can be used for administrative access to the CDE 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 CDE that hosts the VQE-S and VQE Tools server. However, a root user cannot use SSH to log in to a CDE, 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 CDE 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.

TACACS+ Authentication Support

Starting from the Cisco VQE Release 3.8.1, the VQE Tools Server and the VQE Server will also support TACACS+ Authentication mechanism for */etc/pam.d/sshd* service. Applications like SSH, SCP and SFTP makes use of */etc/pam.d/sshd* service. Starting from the Cisco VQE Release 3.10, TACACS+ authentication support is also extended to VQE Server and VQE Tools AMT GUI.

The VQE Server and VQE Tools server will act as TACACS+ Clients, and a non-VQE box in the Customer environment will act as TACACS+ Server.

The following are the methods that can be used for authentication of VQE Server and VQE Tools server:

- Local authentication mechanism
- TACACS+ authentication mechanism

  To enable the TACACS+ authentication mechanism, a TACACS+ Server must be provisioned in the network that is reachable to TACACS+ Client.

  There is no fall back supported.

Table 2-2 lists the TACACS+ Client parameters and the values.

Table 2-2 TACACS+Client Parameters

Parameter	Value Required
system.tacacsplus.tacacs_ssh_enable	Boolean: • True—Enables TACACS+ for SSH authentication. • False—Disables TACACS+ for SSH authentication. The default value is False.
system.tacacsplus.primary_server	The IP address or fully qualified name of the host on which the primary TACACS+ Server resides.
system.tacacsplus.primary_secret	The secret key word of primary TACACS+ Server. The range allowed is 1 to 64.

Table 2-2 TACACS+Client Parameters

Parameter	Value Required
system.tacacsplus.secondary_server	The IP address or fully qualified name of the host on which the secondary TACACS+ Server resides.
system.tacacsplus.secondary_secret	The secret key word of secondary TACACS+ Server. The range allowed is 1 to 64.
system.tacacsplus.tertiary_server	The IP address or fully qualified name of the host on which the tertiary TACACS+ Server resides
system.tacacsplus.tertiary_secret	The secret key word of tertiary TACACS+ Server. The range allowed is 1 to 64.
system.tacacsplus.time_to_wait	The time to wait for the response from TACACS+ Server. The range allowed is 1 to 20. The default value is 5 seconds.
system.tacacsplus.tacacs_gui_enable	Boolean: • True—Enables TACACS+ for GUI authentication. • False—Disables TACACS+ for GUI authentication. The default value is False.

Configuring the TACACS+ Authentication Support

You can configure TACACS+ authentication for VQE Server and VQE Tools server via the VQE Configuration Tool.

The following example shows how to configure TACACS+ Authentication mechanism:

```
[root@gambit-iptv ~]# vqe_cfgtool -config

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

Enter your choice: 1

VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          gambit-iptv
   2) DNS Server(s):
       2.1)                              9.1.40.2
       2.2)                              9.1.41.2
   3) DNS Search Domain:                 []
   4) Timezone:                          America/New_York
   5) NTP Server(s):
       5.1)                              9.1.40.2
       5.2)                              9.1.41.2
   6) Trusted Provisioner(s):
       6.1)                              10.86.61.31
       6.2)                              12.9.27.2
       6.3)                              12.9.28.2
       6.4)                              12.9.29.2
```

```
   7) Remote Syslog Host(s):
   8) SNMP Parameters
   9) TACACS+ Client Parameters
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d).  Default values are displayed inside
   square brackets [].

Enter your choice: 9

VQE Configuration Tool <TACACS+ Client Parameters> Menu:

    1) Enable TACACS+ for SSH:                          [false]
    2) Primary Server:                                   []
    3) Primary Security Word:                            []
    4) Secondary Server:                                 []
    5) Secondary Security Word:                          []
    6) Tertiary Server:                                  []
    7) Tertiary Security Word:                           []
    8) Time to wait:                                     [5]
    9) Enable TACACS+ for GUI:                          [false]
    P) Go to Parent Menu
    R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d).  Default values are displayed inside
   square brackets [].

Enter your choice: 9
Enable TACACS+ for GUI?: y/[n] y

VQE Configuration Tool <TACACS+ Client Parameters> Menu:

    1) Enable TACACS+ for SSH:                          false
    2) Primary Server:                                   []
    3) Primary Security Word:                            []
    4) Secondary Server:                                 []
    5) Secondary Security Word:                          []
    6) Tertiary Server:                                  []
    7) Tertiary Security Word:                           []
    8) Time to wait:                                     [5]
    9) Enable TACACS+ for GUI:                          true
    P) Go to Parent Menu
    R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d).  Default values are displayed inside
   square brackets [].

Enter your choice: 2
Enter the primary TACACS+ server IP/hostname(length 1-200): 138.98.78.67

VQE Configuration Tool <TACACS+ Client Parameters> Menu:

    1) Enable TACACS+ for SSH:                          false
    2) Primary Server:                                   138.98.78.67
    3) Primary Security Word:                            []
    4) Secondary Server:                                 []
    5) Secondary Security Word:                          []
    6) Tertiary Server:                                  []
    7) Tertiary Security Word:                           []
    8) Time to wait:                                     [5]
    9) Enable TACACS+ for GUI:                          true
```

```
   P) Go to Parent Menu
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d). Default values are displayed inside
   square brackets [].

Enter your choice: 3
Enter the primary TACACS+ server security word(length 1-64): secret_key

VQE Configuration Tool <TACACS+ Client Parameters> Menu:

    1) Enable TACACS+ for SSH:                          false
    2) Primary Server:                                  138.98.78.67
    3) Primary Security Word:                           secret_key
    4) Secondary Server:                                []
    5) Secondary Security Word:                         []
    6) Tertiary Server:                                 []
    7) Tertiary Security Word:                          []
    8) Time to wait:                                    [5]
    9) Enable TACACS+ for GUI:                          true
    P) Go to Parent Menu
    R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d). Default values are displayed inside
   square brackets [].

Enter your choice: 8
Enter the value for time to wait (seconds)(1-20): 6

VQE Configuration Tool <TACACS+ Client Parameters> Menu:

    1) Enable TACACS+ for SSH:                          false
    2) Primary Server:                                  138.98.78.67
    3) Primary Security Word:                           secret_key
    4) Secondary Server:                                []
    5) Secondary Security Word:                         []
    6) Tertiary Server:                                 []
    7) Tertiary Security Word:                          []
    8) Time to wait:                                    6
    9) Enable TACACS+ for GUI:                          true
    P) Go to Parent Menu
    R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d). Default values are displayed inside
   square brackets [].

Enter your choice: r

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

Enter your choice: a
vcdb.conf is successfully updated.
Configuration successfully applied.
[root@gambit-iptv ~]#
```

SSL Protocol Configuration

Starting from Release 3.11, VQE supports configuring a list of SSL protocols that the clients can use to connect to VQE server and VQE Tools Server via VQE Configuration tool. The default SSL protocol list is configured as *SSLProtocol -ALL +TLSv1.1 +TLSv1.2.* If an invalid protocol is configured in the list then an error is thrown during *service httpd restart.*

Table 2-3 SSL Protocol Configuration

Parameter	Value Required
system.global.ssl.protocol	String. The default value is *SSLProtocol -ALL +TLSv1.1 +TLSv1.2* **Note** The string should always begin with SSLProtocol

Configuring the SSL Protocol

You can configure a list of SSL Protocols for VQE Server and VQE Tools server via the VQE Configuration Tool.

The following example shows how to configure a SSL Protocol list:

```
[root@gambit-iptv ~]# vqe_cfgtool -config

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

Enter your choice: 1

VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          gandalf-iptv
   2) DNS Server(s):
   3) DNS Search Domain:                 []
   4) Timezone:                          [America/New_York]
   5) NTP Server(s):
       5.1)                              9.1.40.2
       5.2)                              9.1.41.2
   6) Trusted Provisioner(s):
       6.1)                              10.86.61.101
       6.2)                              10.86.61.111
   7) Remote Syslog Host(s):
   8) SNMP Parameters
   9) TACACS+ Client Parameters
   10) SSL Protocols:                     [SSLProtocol -ALL +TLSv1.1 +TLSv1.2]
   11) SSMAgent port change:
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
```

```
   followed by the letter 'd' (e.g. 3d).  Default values are displayed inside
   square brackets [].

Enter your choice: 10
Enter the required SSL protocols for this server.
   The string should always start with 'SSLProtocol' word.(length 1-200): SSLProtocol -ALL
+TLSv1.1

VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          gandalf-iptv
   2) DNS Server(s):
   3) DNS Search Domain:                 []
   4) Timezone:                          [America/New_York]
   5) NTP Server(s):
       5.1)                              9.1.40.2
       5.2)                              9.1.41.2
   6) Trusted Provisioner(s):
       6.1)                              10.86.61.101
       6.2)                              10.86.61.111
   7) Remote Syslog Host(s):
   8) SNMP Parameters
   9) TACACS+ Client Parameters
   10) SSL Protocols:                     SSLProtocol -ALL +TLSv1.1
   11) SSMAgent port change:
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d).  Default values are displayed inside
   square brackets [].

Enter your choice: r

VQE Configuration Tool Root Menu:

   1) System Parameters
   2) Network Parameters
   S) Save and Exit
   A) Save/Apply and Exit
   E) Exit without saving

Enter your choice: a
vcdb.conf is successfully updated.

Applying this configuration will cause the following service interruptions:
    Restart of HTTPD service for configuration change.

Do you want to proceed and apply these changes?: y/[n] y
Configuration successfully applied.
Service httpd restart...
```

SSMAgent Default Port Configuration

Starting from Cisco VQE 3.8.1 Release, Super Micro's SSMAgent with SNMP extension has been integrated in CDE250 device's bin and iso installation for Hardware Monitoring and reporting events like power supply failure via snmp traps.

The default SSMAgent uses TCP port numbers 5666 and 5999 to communicate with the SSM Server. SSMAgent is installed with the default settings in the VQE. Some customers run 3rd party applications, while Cisco does not officially support any 3rd party clients on the VQE, some customers do this on their own. The default ports chosen by SSM are known to conflict with certain 3rd party clients, and customers have requested the ability to alter the SSM default ports in light of this.

Table 2-4 lists the SSMAgent parameters and the values.

Table 2-4 SSMAgent Default Port Parameters

Parameter	Value Required
system.ssm.defaultssl_port	The default port is 5666. The range is from 1024 to 65535.
system.ssm.keypairssl_port	The default port is 5999. The range is from 1024 to 65535.

Configuring the SSMAgent Default Port Configuration

You can configure SSMAgent Default Port Configuration for VQE Server and VQE Tools server in CDE250 devices via the VQE Configuration Tool.

The following example shows how to configure SSMAgent Default Port Configuration:

```
[root@bootking-iptv ~]# vqe_cfgtool -config

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

Enter your choice: 1

VQE Configuration Tool <System Parameters> Menu:

   1) Hostname:                          bootking-iptv
   2) DNS Server(s):
       2.1)                              9.1.40.2
       2.2)                              9.1.41.2
   3) DNS Search Domain:                 []
   4) Timezone:                          America/New_York
   5) NTP Server(s):
       5.1)                              9.1.40.2
       5.2)                              9.1.41.2
   6) Trusted Provisioner(s):
       6.1)                              10.86.61.31
       6.2)                              12.9.27.2
       6.3)                              12.9.28.2
       6.4)                              12.9.29.2
   7) Remote Syslog Host(s):
   8) SNMP Parameters
   9) TACACS+ Client Parameters
   10) SSMAgent Parameters
   R) Go to Root Menu
```

```
   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d).  Default values are displayed inside
   square brackets [].

Enter your choice: 10

VQE Configuration Tool <SSMAgent Port Configuration Parameters> Menu:

   1) SSMAgent default ssl port                              [5666]
   2) SSMAgent keypair ssl port                              [5999]
   P) Go to Parent Menu
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d).  Default values are displayed inside
   square brackets [].

Enter your choice: 1
Enter SSMagent default ssl port(length 1024-65535): 5660

VQE Configuration Tool <SSMAgent Port Configuration Parameters> Menu:

   1) SSMAgent default ssl port                              5660
   2) SSMAgent keypair ssl port                              [5999]
   P) Go to Parent Menu
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d).  Default values are displayed inside
   square brackets [].

Enter your choice: r

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

Enter your choice: a

vcdb.conf is successfully updated.

Applying this configuration will cause the following service interruptions:
    Restart of SSMAgent service for configuration change.

Do you want to proceed and apply these changes?: y/[n]y
Configuration successfully applied.
[root@bootking-iptv ~]#
```

Prerequisites

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

- Connect cables to the CDE—See the "Connecting Cables to the CDE" section on page 2-12.

- 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" section on page 2-12.

Connecting Cables to the CDE

The following cable connections are used on the Cisco CDE that hosts the VQE-S and on the CDE 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 CDE have four Ethernet ports. The latest models of the CDE 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 CDE 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 CDE 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 CDE to the same network that the CDEs 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 CDE. Only one serial port can be used because it is one shared serial port.
- If a PC is directly connected to the CDE serial port, the cable from the PC is connected to an RJ-45 serial port on the front or back of the Cisco CDE. 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 CDE 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 CDE.

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

For the location of connectors on the Cisco CDE front and back panels, see *Cisco Content Delivery Engine 110 Hardware Installation Guide* and the *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*.

Setting Up SSL Certificates

SSL is used on the CDEs 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 Configuration Tool for SSL Certificates, page 2-13
- Creating Your Own Certificate Authority, page 2-13
- Generating and Deploying Your Own SSL Certificates, page 2-14
- Deploying Commercial SSL Certificates, page 2-17

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 Configuration Tool for SSL Certificates

To manually create and deploy SSL certificates, follow the directions provided in these sections:

- For overview information of the SSL tasks, see the "Setting Up SSL Certificates" section on page 12.
- For deploying your own SSL certificates, see the "Creating Your Own Certificate Authority" section on page 13 and the "Generating and Deploying Your Own SSL Certificates" section on page 14.
- For deploying commercial SSL certificates, see the "Deploying Commercial SSL Certificates" section on page 17.

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 CDE 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 CDE 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 CDE 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 13. 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 13.

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

We recommend that the system time of each CDE 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-----
MIIGGDCCBACgAwIBAgIJAPtvlrCRokk4MA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
```

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

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

Step 2 For 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 13.

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 15.
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 17 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 ...
/kzgDk5wO1CbTwuxPIY1piy0Os1Q5EWk3VVAmv4tNMT9bANeKDUiVyYyOi1NIiHA
36w=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGGDCCBACgAwIBAgIJAPtvlrCRokk4MA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
... Omitted contents ...
KV+sxNECGE40iWIvd1dXDA1O34qhAwkVD6/bxw==
-----END CERTIFICATE-----
```

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

Step 2 For 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 and VQE-Tools Server: Routing and Interface Configuration Overview

For a VQE-S, configuring static routes, both static and dynamic routes, and Open Shortest Path First (OSPF) routing is supported. 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:

At initial system startup, the VQE Configuration Tool 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 and VQE-Tools Server

Starting from the Cisco VQE Release 3.8, support for bond interfaces is extended to VQE-Tools Server.

One or more bond interfaces may be configured on a CDE that hosts the VQE-S and VQE-Tools Server. 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/VQE-Tools Server 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.

Note The user cannot assign roles to bonds for VQE-Tools

Types of Routes on a VQE-Tools Server

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 Configuration Tool can be used to configure one or more static routes.

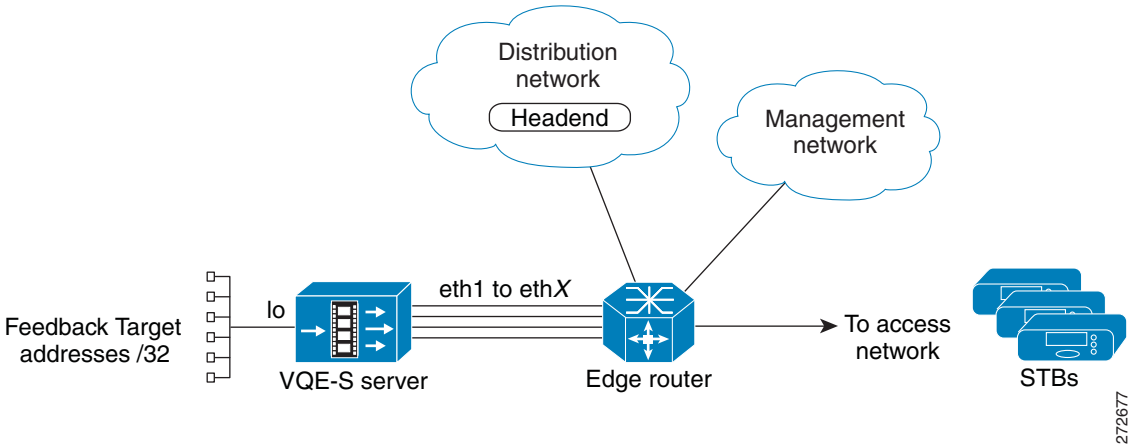
Types of Routes on a VQE-S

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 33.

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 2-59.

OSPF Routing on a VQE-S

Starting from 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 21. 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 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 36.

For information on OSPF configuration on the edge router, see the "For OSPF Routing: Guidance for Configuring the Attached Router" section on page 56.

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

Some VQE deployments require that the CDE 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 CDE 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 CDE 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 VQE Configuration Tool allow you to configure dedicated CDE 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 CDE 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 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 2-5 shows where to find information on the configuration parameters that are used for dedicated and shared interfaces.

Table 2-5 Where To Find Information on Parameters for Dedicated and Shared Interfaces

Configuration Parameter For	Where To Find Information
Dedicated Interfaces	
Dedicated interfaces for VQE-S ingest traffic	"Interfaces for VQE-S Ingest Traffic (VQE-S Host Only)" section on page 2-37
Dedicated interfaces for VQE-S services traffic	"Interfaces for VQE-S Services Traffic (VQE-S Host Only)" section on page 2-37
Shared Interfaces	
VQE-S traffic interfaces that handle VQE-S ingest traffic and VQE-S services traffic	"Interfaces for VQE-S Traffic (Ingest and Services) (VQE-S Host Only)" section on page 2-38

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 CDE 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 CDE 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 33.

For information on the configuration parameters that are used for OSPF routing, see the "OSPF Configuration (VQE-S Host Only)" section on page 36.

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 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 CDE 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

Management traffic is blocked from non-management interfaces. The service provider must designate at least one CDE 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 2-6 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 2-6 are used for management traffic on non-management interfaces, management traffic on the non-standard protocol ports is not blocked.

Table 2-6 Standard Management Protocol Ports Blocked on Non-Management Interfaces

Port Number	Standard Management Traffic Type
22	SSH[1]
443	HTTPS[2]
444	HTTPS Push
161 and 162	SNMP[3]
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 CDE Ethernet interfaces or bond interfaces used for management traffic, do not include those CDE Ethernet interfaces or bond interfaces in the following VQE 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 Configuration Tool.

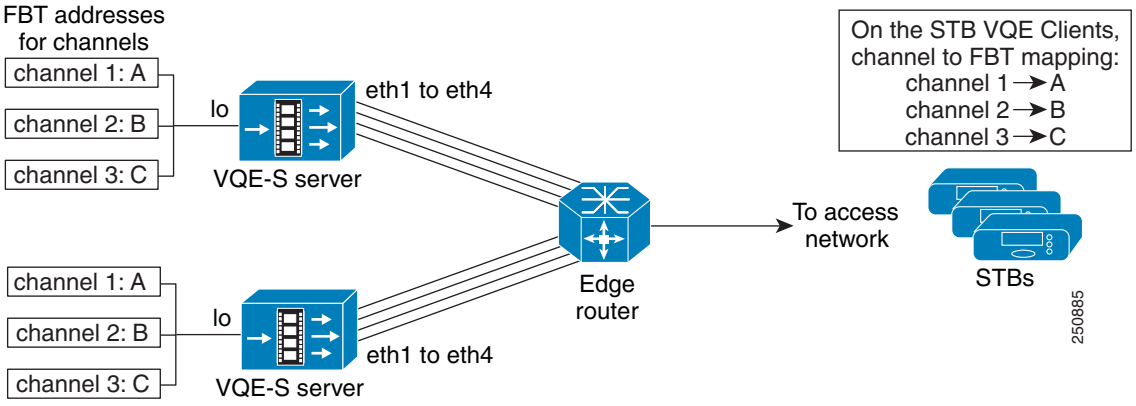
Load Balancing and Redundancy with Multiple VQE-S

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 CDE 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 CDE 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.

Configuring LACP Bonding on a VQE-S and VQE Tools Server

You can enable 803.ad LACP protocol for all bonds on the VQE-S and VQE-Tools Server. This is a global configuration for all bonds. To enable LACP bonding, use network.bond1 on the VQE-S and VQE-Tools Server:

The following two parameters support LACP bonding:

- network.bond.mode

  This can be set to either “lacp” or “balance-xor” (default).

- **network.bond.lacp_rate**

  This parameter can be either slow or fast. It is slow by default.

Restrictions

A service role (ingest, service, management) may only have a single VLAN assigned to it. For example, you may only assign one sub-interface of a given interface/bond to a given role.

LACP and LACP Rate are global configuration knobs. If LACP or LACP Rate are enabled, this applies to all bonds.

User Interface

The following example shows how to create a VLAN interface and enable LACP:

```
VQE Configuration Tool <Network Parameters> Menu:

1) Routing Parameters
   2) Interface Parameters
   3) Bond Parameters
   4) VLAN Parameters
   R) Go to Root Menu

Enter your choice: 3

VQE Configuration Tool <Bond Parameters> Menu:

   1) Bond1 IP/Mask and members:          []
   2) Bond2 IP/Mask and members:          []
   3) Bond3 IP/Mask and members:          []
   4) Bond4 IP/Mask and members:          []
   5) Bond5 IP/Mask and members:          []
   6) Enable 802.3ad LACP for Bonds:      [false]
   7) Enable fast LACP rate:              [false]
   P) Go to Parent Menu
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d). Default values are displayed inside
   square brackets [].

Enter your choice: 6

If you choose to enable LACP, all bonds will run in this mode instead of balance-xor.

Enable 802.3ad LACP: y/[n] y

VQE Configuration Tool <Bond Parameters> Menu:

   1) Bond1 IP/Mask and members:          []
   2) Bond2 IP/Mask and members:          []
   3) Bond3 IP/Mask and members:          []
   4) Bond4 IP/Mask and members:          []
   5) Bond5 IP/Mask and members:          []
   6) Enable 802.3ad LACP for Bonds:      true
   7) Enable fast LACP rate:              [false]
   P) Go to Parent Menu
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d). Default values are displayed inside
   square brackets [].

Enter your choice: 7
Enable fast rate for LACP: y/[n] y
VQE Configuration Tool <Bond Parameters> Menu:

   1) Bond1 IP/Mask and members:          []
   2) Bond2 IP/Mask and members:          []
   3) Bond3 IP/Mask and members:          []
```

```
   4) Bond4 IP/Mask and members:          []
   5) Bond5 IP/Mask and members:          []
   6) Enable 802.3ad LACP for Bonds:      true
   7) Enable fast LACP rate:              true
   P) Go to Parent Menu
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d). Default values are displayed inside
   square brackets [].

Enter your choice:
```

Configuring VLAN Support on a VQE-S and VQE-Tools Server

You can configure 802.1q VLAN sub-interfaces on all Ethernet and bond interfaces.

The following example shows how to configure VLAN support:

```
VQE Configuration Tool <Network Parameters> Menu:

   1) Routing Parameters
   2) Interface Parameters
   3) Bond Parameters
   4) VLAN Parameters
   R) Go to Root Menu

Enter your choice: 4

VQE Configuration Tool <802.1q Sub-Interface Parameters> Menu:

   1) Eth0 SubInterface VLAN tag IP/Mask:
   2) Eth1 SubInterface VLAN tag IP/Mask:
   3) Eth2 SubInterface VLAN tag IP/Mask:
   4) Eth3 SubInterface VLAN tag IP/Mask:
   5) Eth4 SubInterface VLAN tag IP/Mask:
   6) Eth5 SubInterface VLAN tag IP/Mask:
   7) Eth6 SubInterface VLAN tag IP/Mask:
   8) Eth7 SubInterface VLAN tag IP/Mask:
   9) Eth8 SubInterface VLAN tag IP/Mask:
   10) Eth9 SubInterface VLAN tag IP/Mask:
   11) Bond1 SubInterface VLAN tag IP/Mask:
   12) Bond2 SubInterface VLAN tag IP/Mask:
   13) Bond3 SubInterface VLAN tag IP/Mask:
   14) Bond4 SubInterface VLAN tag IP/Mask:
   15) Bond5 SubInterface VLAN tag IP/Mask:
   P) Go to Parent Menu
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d). Default values are displayed inside
   square brackets [].

Enter your choice: 1

Configure VLAN (802.1q) interfaces for eth0.
Enter subinterface VLAN tag: 100
Enter the IP/Prefix for eth0.100 (e.g. 1.2.3.4/8): 1.2.3.4/24
Enter subinterface VLAN tag: 200
Enter the IP/Prefix for eth0.200 (e.g. 1.2.3.4/8): 4.3.2.1/24
Enter subinterface VLAN tag:
```

```
VQE Configuration Tool <802.1q Sub-Interface Parameters> Menu:

   1) Eth0 SubInterface VLAN tag IP/Mask:
       1.1)                              100 1.2.3.4/24
       1.2)                              200 4.3.2.1/24
   2) Eth1 SubInterface VLAN tag IP/Mask:
   3) Eth2 SubInterface VLAN tag IP/Mask:
   4) Eth3 SubInterface VLAN tag IP/Mask:
   5) Eth4 SubInterface VLAN tag IP/Mask:
   6) Eth5 SubInterface VLAN tag IP/Mask:
   7) Eth6 SubInterface VLAN tag IP/Mask:
   8) Eth7 SubInterface VLAN tag IP/Mask:
   9) Eth8 SubInterface VLAN tag IP/Mask:
   10) Eth9 SubInterface VLAN tag IP/Mask:
   11) Bond1 SubInterface VLAN tag IP/Mask:
   12) Bond2 SubInterface VLAN tag IP/Mask:
   13) Bond3 SubInterface VLAN tag IP/Mask:
   14) Bond4 SubInterface VLAN tag IP/Mask:
   15) Bond5 SubInterface VLAN tag IP/Mask:
   P) Go to Parent Menu
   R) Go to Root Menu

   To reset a parameter to its factory default value, enter its number choice
   followed by the letter 'd' (e.g. 3d). Default values are displayed inside
   square brackets [].

Enter your choice:
V
```

Using the VQE Configuration Tool

The CDE server has the VQE software preinstalled. The tool is available on the CDE that hosts VQE-S and on the CDE that hosts VQE Tools. We recommend that you use the VQE Configuration Tool rather than try to do the initial configuration manually because the tool simplifies your work and is known to produce correct results.

Before using the VQE Configuration Tool, do the following to understand how the tool works and what information you need to collect before powering on the VQE-S or VCPT server:

- Read the "VQE-S and VQE-Tools Server: Routing and Interface Configuration Overview" section on page 2-19.
- Read the "V" section on page 2-30.
- Read the "Configuration Parameters" section on page 2-31.
- Complete the "Preconfiguration Worksheets" section on page 2-40.
- Read the "VQE Configuration Tool Root Menu" section on page 2-44.

When it is started, the VQE Configuration Tool 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 Configuration Tool prompts you for configuration values.

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

After you finish entering configuration values, the VQE Configuration Tool 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 Configuration Tool, 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 47
- "On the VQE Tools Host: Verifying the Status of the VQE and System Services" section on page 50

Configuration Parameters

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

Tip For many configuration parameters, you need to gather some information before booting the CDE for the first time and using the VQE Configuration Tool. The worksheets in the "Preconfiguration Worksheets" section on page 40 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 Configuration Tool prompt.

Passwords for root and vqe User IDs

The password for root is set when the CDE boots normally for the first time (when you log in as root) and before the VQE Configuration Tool 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 CDE 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 6-32. 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.

Hostname for the CDE

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 CDE. The VQE Configuration Tool 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 CDE 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 CDE. The VQE Configuration Tool prompts for the needed information.

Ethernet Interface Configuration: IP Address and Prefix Length

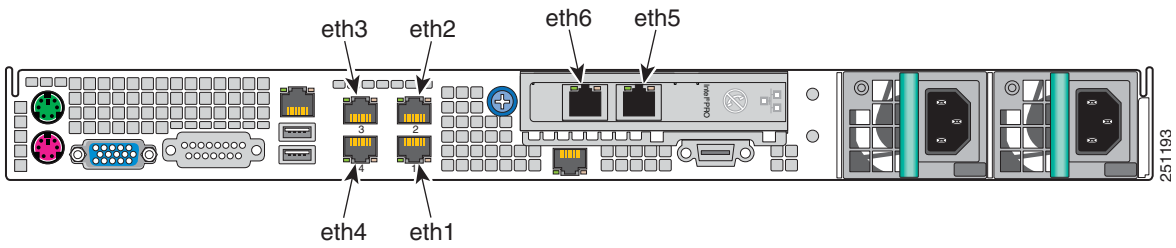
For one or more of the Ethernet ports on the Cisco CDE, you specify an IP address and prefix length (for example, 1.2.3.4/32). The IP address and prefix length are not specified for any CDE Ethernet interface that is a member of a bond interface. The Ethernet ports are named eth1 to eth6 as shown in Figure 2-3.

Note Earlier models of the CDE have four Ethernet ports (eth1 to e

th4). 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/VQE-Tool Server, 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 CDE 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 CDE 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. The number of bonds on a VQE-Tools Server is hardware dependent.

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 Starting from the Cisco VQE Release 3.8, bond interfaces are 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 and VQE-Tools Server" section on page 19.

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 Configuration Tool 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 CDE 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 CDE 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 CDE 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 CDE 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 Configuration Tool gives you three options for creating and deploying the certificates. For information on the three options and using the tool for creating and deploying SSL certificates, see the "Using the Cisco VQE Configuration Tool for SSL Certificates" section on page 13.

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 **vcds_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 CDE 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 CDE, 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 35.

For more information on SNMP for the CDE, see Appendix B, "SNMP MIBs."

For more information on TACACS+ Authentication Support, see TACACS+ Authentication Support.

For more information on SSMAgen Default Port Configuration, see SSL Protocol Configuration.

OSPF Configuration (VQE-S Host Only)

Table 2-7 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 2-7 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 CDE Ethernet interfaces because the router ID is added as an internal address to the loopback interface.
Enable MD5	Specifies whether MD5[1] 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.

Table 2-7 OSPF Parameters (continued)

Parameter	Description
Hello Interval	Interval (in seconds) at which OSPF Hello packets are sent. This value must be the same for all interfaces running OSPF in the network. The hello interval 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 and VQE-Tools Server: Routing and Interface Configuration Overview" section on page 19.

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 CDE 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 CDE 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 CDE 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 CDE 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 37.

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 CDE 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). Ethernet and bond interfaces are different depending on the CDE model, refer to Table 2-10 for allowed choices for each model.

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 CDE 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 2-25.

VQE Configuration Tool Root Menu

After you finish specifying values for the configuration items, the VQE Configuration Tool displays the following 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

Enter your choice:
```

For information on this menu, see the "VQE Configuration Tool Root Menu" section on page 2-44.

When you have completed the configuration items, you choose S) Save/Apply and reboot system. The VQE Configuration Tool saves your configuration in the VCDB file, applies the VCDB values to the configuration files under /etc, and reboots the CDE system. Each time the VQE-S or VQE Tools host reboots, the services listed in Table 2-8 and Table 2-9 are started.

Table 2-8 VQE-S and System Services for CDE 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).
tomcat7	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 **cron** job owned by root.
If OSPF is selected as the routing type	
watchquagga	Quagga watchdog process. If the ospfd or zebra daemon crashes or hangs, watchquagga restarts it automatically.
ospfd	OSPF daemon.
zebra	Zebra daemon.

Table 2-9 VCDS and System Services for CDE That Hosts VQE Tools

Service	Description
vcds	VCDS service.
sshd	Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat7	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 **cron** job owned by root.

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

Preconfiguration Worksheets

Before using the VQE Configuration Tool, complete the preconfiguration worksheets in Table 2-10 for a VQE-S host and Table 2-11 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 2-10 and Table 2-11, see the "Configuration Parameters" section on page 31.

Table 2-10 VQE-S CDE: Preconfiguration Worksheet

Configuration Item	Value for Your Deployment
Password for root	
Password for the vqe username (a predefined Linux user ID)	
Hostname of the CDE 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	
CDE110 Ethernet interface configurations (IP address and prefix lengths)	eth1: eth2: eth3: eth4: eth5: eth6:
CDE250 Ethernet interface configurations (IP address and prefix lengths)	eth0: eth1: eth2: eth3: eth4: eth5: eth6: eth7: eth8: eth9:

Table 2-10 VQE-S CDE: Preconfiguration Worksheet (continued)

Configuration Item	Value for Your Deployment
CDE110 Bond interface configurations (IP address, subnet mask and members	bond1: bond2: bond3:
CDE250 Bond interface configurations (IP address, subnet mask and members	bond1: bond2: bond3: bond4: bond5:
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	
SNMP read-only community string Location for SNMP Contact for SNMP SNMP trap-listener IP addresses or hostnames	community string: location: contact: IP addresses or hostnames:
Are Syslog traps enabled?	Yes or No:
Syslog trap priority	
Are channel up/down traps enabled?	Yes or No:
Is TACACS+ enabled?	Yes or No:
Primary TACACS+ Server	Mandatory if TACACS+ is enabled.
Primary Secret Key	
Secondary TACACS+ Server	
Secondary Secret Key	
Tertiary TACACS+ Server	
Tertiary Secret Key	
Time to wait	

Table 2-10 VQE-S CDE: Preconfiguration Worksheet (continued)

Configuration Item	Value for Your Deployment
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 2-11 VQE Tools CDE: Preconfiguration Worksheet

Configuration Item	Value for Your Deployment
Password for root	
Password for the vqe username (a predefined Linux user ID)	
Hostname of the CDE for VCPT	
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	
CDE110 Ethernet interface configurations (IP address and mask)	eth1: eth2: eth3: eth4: eth5: eth6:

Table 2-11 VQE Tools CDE: Preconfiguration Worksheet (continued)

Configuration Item	Value for Your Deployment
CDE250 Ethernet interface configurations (IP address and mask)	eth0: eth1: eth2: eth3: eth4: eth5: eth6: eth7: eth8: eth9:
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 Location for SNMP Contact for SNMP SNMP trap-listener IP addresses or hostnames	community string: location: contact: IP addresses or hostnames:
Are Syslog traps enabled?	Yes or No:
Syslog trap priority	
Is TACACS+ enabled?	Yes or No:
Primary TACACS+ Server	Mandatory if TACACS+ is enabled.
Primary Secret Key	
Secondary TACACS+ Server	
Secondary Secret Key	
Tertiary TACACS+ Server	
Tertiary Secret Key	
Time to wait	

VQE Configuration Tool Root Menu

After you have used the VQE Configuration Tool to specify values for the configuration items, the tool 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) VQE-S Parameters
     S) Save and Exit
     A) Save/Apply and Exit
     E) Exit without saving


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 Configuration Tool, and the Save/Apply choice in the VQE Configuration Tool 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 Configuration Tool.

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)
- Save the parameter values to the VQE Configuration Database (VCDB), and apply the values to the VQE-S or VQE Tools server (choice A)

To view and change parameter values, you can select choices 1, 2, and 3as 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 2-12 provides more information about the choices on the Root Menu. You enter the number or letter for your choice.

Table 2-12 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 9) TACACS+ Parameters 10) SSMAgent Parameters R) Go to Root Menu
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 P) Go to Parent Menu R) Go to Root Menu
2) System Parameters > TACACS+ Parameters	1) Enable TACACS+ for SSH 2) Primary Server 3) Primary Security Word 4) Secondary Server 5) Secondary Security Word 6) Tertiary Server 7) Tertiary Security Word 8) Time to wait 9) Enable TACACS+ for GUI P) Go to Parent Menu R) Go to Root Menu

Table 2-12 Root Menu Choices (continued)

Root Menu Choice	Menu Description
4) CDE110 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) P) Go to Parent Menu R) Go to Root Menu
4) CDE250 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) Eth0 Interface IP/Mask 2) Eth1 Interface IP/Mask 3) Eth2 Interface IP/Mask 4) Eth3 Interface IP/Mask 5) Eth4 Interface IP/Mask 6) Eth5 Interface IP/Mask 7) Eth6 Interface IP/Mask 8) Eth7 Interface IP/Mask 9) Eth8 Interface IP/Mask 10) Eth9 Interface IP/Mask 11) Bond1 IP/Mask and members 12) Bond2 IP/Mask and members 13) Bond3 IP/Mask and members 14) Bond4 IP/Mask and members 15) Bond5 IP/Mask and members 16) Management Interface(s)
4) 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)

Table 2-12 Root Menu Choices (continued)

Root Menu Choice	Menu Description
5) VQE-S Parameters	Allows you to view the current VQE-S parameter values that you have set, and to change or set the VQE-S parameters values: 1) Log Priority * 2) Excess Bandwidth Fraction * 3) Traffic (Ingest+Service) Interface(s) 4) Ingest Interface(s) 5) Service Interface(s) 6) RTCP Exporter Parameters) R) Go to Root Menu * The VQE Configuration Tool does not allow you to set the values of these parameters in the set of parameters that were previously displayed. You can supply values at this point if you want or accept the defaults. For more information on these values, see the vcdb.conf.sample file and Appendix A, "VQE, System and Network Parameters."
S) Save and Exit	Saves the changes you have made to the VCDB parameters and exits Configuration Tool. Any new parameter values *are not applied* 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 Configuration Tool..
E) Exit without saving	Exits Configuration Tool. Any changes you have made to the VCDB parameters *are not saved*.

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

After the VQE Configuration Tool finishes and the CDE 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 7 service is running, enter the following command:

```
[root@system]# service tomcat7 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.
```

Note This step does not apply to the CDE250.

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 2206 1 0 Jan28 ? 00:00:00 /opt/vqes/bin/process_monitor
vqes 2220 2206 0 Jan28 ? 00:00:00 stun_server --ss-uid 497 --ss-gid 497 --xmlrpc-port 8054
--dscp -1 --log-level 6
root 2813 2206 99 Jan28 ? 13-18:34:42 vqes_dp --group vqes --max-channels 500
--max-outstanding-rpcs 100 --max-pkts 1000000 --log-level 6 --rtp-inactivity-tmo 300
--max-core-bw 850000000 --reserved-core-rcv-bw 100000000 --reserved-core-er-bw 120000000
--reserved-er-bw 543200000
```

```
vqes 2934 2206 0 Jan28 ? 00:01:45 vqes_cp --cp-uid 497 --cp-gid 497 --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-port
10.86.21.144:3000,10.86.21.144:4000 --bwb-client-timeout 20 --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 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 CDE 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 Configuration Tool finishes and the CDE 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 7 service is running, enter the following command:

```
[root@system]# service tomcat7 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

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 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 CDE 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 CDE that hosts VQE Tools:

`https://ip_address_of_VQE_tools_host/vcds-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.

Starting from the Cisco VQE 3.8 Release, VQE-S supports exporting RTCP reports to one or at most two VQMs at a time.Also, in this release VQE-S RTCP Exporter can be configured either by vqe_cfgtool or by manually editing vcdb.conf file.

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.

Starting from the Cisco VQE 3.8 release, RTCP exporter can be configured/enabled via the following two methods:

- Manual editing of VCDB file
- Using VQE Configuration tool

Configuring VQE-S RTCP Exporter via manually editing the VCDB File

To configure and enable the RTCP Exporter on the Cisco CDE 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 Configuration Tool** by executing the following command:

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

Step 2 Edit the /etc/opt/vqes/vcdb.conf file, and specify values for the parameters listed in Table 2-13, to the file.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 7-15.

Step 3 Save the vcdb.conf file.

Table 2-13 RTCP Exporter Parameters

Parameter	Value Required
vqe.vqes.vqm_host="*IP_addr_or_domain_name*"	IP address or fully qualified Internet domain name of the host on which the VQM application resides. There is no default value. **Note** Though this parameter is still supported, Cisco recommends that the user use the new parameter **vqe.vqes.vqm_host_port** to configure the VQM host IP address and port.
vqe.vqes.vqm_port="*vqm_port_no*"	TCP port number on which the VQM application listens for video quality data from RTCP Exporter. Allowed range is 1024 to 65535. There is no default value. **Note** Though this parameter is still supported, Cisco recommends that the user use the new parameter **vqe.vqes.vqm_host_port** to configure the VQM host IP address and port.
vqe.vqes.vqm_host_port="*IP_addr_or_domain_name:vqm_port_no*"	The IP address or fully qualified Internet domain name of the host on which the VQM application resides and the TCP port number on which the VQM application listens for video quality data from RTCP Exporter are specified together as a single variable **Note** This parameter is available in the VCDB starting from the Cisco VQE Release 3.7.
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 from the Cisco VQE Release 3.5.5.

RTCP Exporter remains disabled unless both VQM Host IP Address and 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 7-19.

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 VQE-S RTCP Exporter via VQE Configuration Tool

You can also configure VQE-S RTCP Exporter via VQE Configuration Tool.

The following example shows how to configure VQE-S RTCP Exporter:

```
VQE Configuration Tool <VQE-S Parameters> Menu:

    1) Log Priority: 6
    2) Excess Bandwidth Fraction: [20]%
    3) Traffic (Ingest+Service) Interface(s): eth2,eth3,eth4,eth5,eth6
    4) Ingest Interface(s): []
    5) Service Interface(s): []
    6) RTCP Exporter Parameters:
    R) Go to Root Menu

To reset a parameter to its factory default value, enter its number choice
followed by the letter 'd' (e.g. 3d). Default values are displayed inside
square brackets [].

Enter your choice:6

VQE Configuration Tool <RTCP Exporter Parameters> Menu:

    1) Enable Exporter: [false]
    2) Enable NACK Filter: [false]
    3) VQM Parameters:
    P) Go to Parent Menu
    R) Go to Root Menu

To reset a parameter to its factory default value, enter its number choice
followed by the letter 'd' (e.g. 3d). Default values are displayed inside
square brackets [].

Enter your choice: 1
Enable Exporter?: y/[n] y

VQE Configuration Tool <RTCP Exporter Parameters> Menu:

    1) Enable Exporter: true
    2) Enable NACK Filter: [false]
    3) VQM Parameters:
    P) Go to Parent Menu
    R) Go to Root Menu

To reset a parameter to its factory default value, enter its number choice
followed by the letter 'd' (e.g. 3d). Default values are displayed inside
square brackets [].
```

```
Enter your choice: 2
Enable NACK Filter?: y/[n] y

VQE Configuration Tool <RTCP Exporter Parameters> Menu:

    1) Enable Exporter: true
    2) Enable NACK Filter: true
    3) VQM Parameters:
    P) Go to Parent Menu
    R) Go to Root Menu

To reset a parameter to its factory default value, enter its number choice
followed by the letter 'd' (e.g. 3d). Default values are displayed inside
square brackets [].

Enter your choice: 3

Configure the VQM host(s) for RTCP Exporter reports. VQM parameter must be
added as a colon separated field "host:port", where host is the IP address
or host name of the VQM, and "port" is the port number. For multiple VQMs,
enter one VQM parameter per line. Maximum number of VQMs supported is 2.
To complete the configuration, press <Enter> at the prompt without entering
data. Usage example: 127.0.0.1:3000

Enter VQM information as "host:port":123.0.0.98:4000
Enter VQM information as "host:port":134.98.78.67:6000

VQE Configuration Tool <RTCP Exporter Parameters> Menu:

    1) Enable Exporter: true
    2) Enable NACK Filter: true
    3) VQM Parameters:
        3.1) 123.0.0.98:4000
        3.2) 134.98.78.67:6000
    P) Go to Parent Menu
    R) Go to Root Menu

To reset a parameter to its factory default value, enter its number choice
followed by the letter 'd' (e.g. 3d). Default values are displayed inside
square brackets [].

Enter your choice: r

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

Enter your choice:A
vcdb.conf is successfully updated.

Applying this configuration will cause the following service interruptions:
Restart of VQE services (process_monitor) for configuration change.

Do you want to proceed and apply these changes?: y/[n] y
```

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 Configuration Tool. 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 2-55
- For OSPF Routing: Guidance for Configuring the Attached Router, page 2-56
- For Static Routes: Guidance for Configuring the Feedback Targets on the Attached Router, page 2-59

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 2-57
- VQE-S in Area 0, page 2-57
- General Guidelines, page 2-58

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

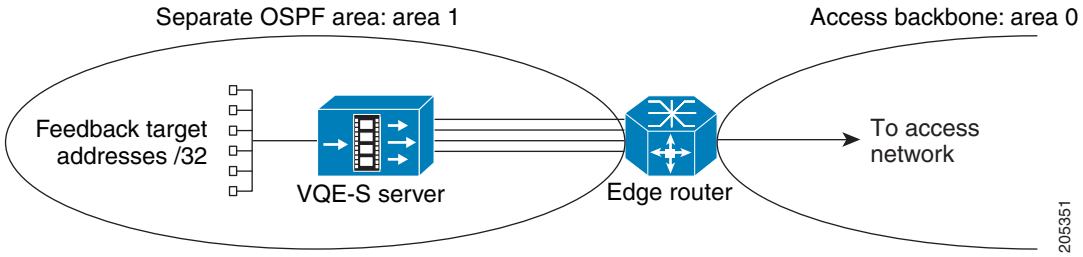
http://www.cisco.com/en/US/tech/tk365/tk480/tsd_technology_support_sub-protocol_home.html

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

VQE-S in 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 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 57.

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 57.

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.