CHAPTER 2

Getting Started with the VQE Startup Configuration Utility

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

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

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

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

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

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

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

- Web Browser, Screen Resolution, and Other Requirements, page 2-2
- System Port Numbers, page 2-2
- Configuring Terminal Emulation Software, page 2-3
- Security Restrictions for Logins and Root Privileges, page 2-3
- Prerequisites, page 2-4
- Setting Up SSL Certificates, page 2-5
- VQE-S Server: Routing and Interface Configuration Overview, page 2-14
- VQE Tools Server: Routing Configuration Overview, page 2-22
- Using the VQE Startup Configuration Utility, page 2-22
- On the VQE-S Host: Verifying Status of VQE and System Services, page 2-36
- On the VQE Tools Host: Verifying Status of VQE and System Services, page 2-38

- Configuring VQE-S RTCP Exporter, page 2-39
- Configuring Other Parameters for the VQE-S Host, page 2-41
- Configuring the Edge Router for VQE-S, page 2-41

Note The configuration instructions in this chapter are intended for new installations of Cisco VQE, Release 3.4, software, where the Cisco CDE110 has the Cisco VQE, Release 3.4, software preinstalled.

For information on upgrading a Cisco CDE110, see the *Release Notes for Cisco CDA Visual Quality Experience Application, Release 3.4*.

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

Web Browser, Screen Resolution, and Other Requirements

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

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

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

For VQE-S AMT, Adobe Flash Player must be installed on the computer that hosts the browser accessing 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://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash

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	Port User
21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
161	Simple Network Management Protocol (SNMP)
162	SNMP traps
443	Hypertext Transfer Protocol Secure (HTTPS)
444	HTTPS push
8005	Apache tomcat

Table 2-1 VQE-S System Ports

Port Number	Port User
8009	Apache tomcat
8050	VQE process monitor
8051	VQE-S Control Plane (CP) XML Remote Procedure Call (XML-RPC)
8052	Multicast Load Balancer (MIB) RPC
8053	VQE Client Configuration Delivery Server (VCDS)
8054	STUN Server RPC

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

Configuring Terminal Emulation Software

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

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

Security Restrictions for Logins and Root Privileges

For security reasons, the following restrictions apply to VQE:

- The root user cannot use Secure Shell (SSH) to log in to a CDE110 that hosts VQE-S or VQE Tools, or to log in to VQE-S AMT, VCDS AMT or VCPT. The vqe username should be used instead. The vqe username is a pre-created Linux user ID and has its password set during CDE110 initial system configuration.
- Only users in the wheel group can use the **su** or **sudo** commands. By default, the vqe username is in the wheel group.

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

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

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

Prerequisites

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

- Connect cables to the CDE110—See the "Connecting Cables to the CDE110" section on page 2-4.
- Determine how you will set up Secure Sockets Layer (SSL) certificates—For information on the alternatives available to you, see the "Setting Up SSL Certificates with the VQE Startup Configuration Utility" section on page 2-5.

Connecting Cables to the CDE110

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

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

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

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

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

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

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

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

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

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

Setting Up SSL Certificates with the VQE Startup Configuration Utility

Secure Sockets Layer (SSL) certificates must be deployed on the CDE110s for HTTPS to operate. You can let the Cisco VQE Startup Configuration Utility do most of the creation and deployment, or you can do the creation and deployment tasks yourself. For information on your options for SSL certificates with the startup utility, see the "Using the Cisco VQE Startup Configuration Utility for SSL Certificates" section on page 2-5.

Setting Up SSL Certificates

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

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

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

- Using the Cisco VQE Startup Configuration Utility for SSL Certificates, page 2-5
- Creating Your Own Certificate Authority, page 2-8
- Generating and Deploying Your Own SSL Certificates, page 2-9
- Deploying Commercial SSL Certificates, page 2-12

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 VQE Tools hosts. For more information on the Open Source toolkit and for documentation on toolkit commands, go to the following URL:

http://www.openssl.org

Using the Cisco VQE Startup Configuration Utility for SSL Certificates

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

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

  For an explanation of the tasks involved with using Option 1, see the "Step-by-Step Example: VQE Startup Configuration Utility's Option 1 for Preparing SSL Certificates" section on page 2-6.

- Option 2: The Cisco VQE Startup Configuration Utility generates only a Certificate Signing Request file (server.csr).
  - The VQE Startup Configuration Utility creates the Certificate Signing Request file in the /etc/opt/certs directory.

  - You sign the Certificate Signing Request as described one of the following sections:
  - If you are signing the Certificate Signing Request with a self-created certificate authority, see the "Signing the Certificate Signing Request" section on page 2-10.
  - If you are submitting the Certificate Signing Request to a commercial CA for signing, see the "Deploying Commercial SSL Certificates" section on page 2-12. You can omit the first step in this section (generating a Certificate Signing Request) as the VQE Startup Configuration Utility does this for you.
  - You install the certificates, private key, and keystore as described in the "Installing the Certificates, Private Key, and Keystore" section on page 2-11.
- Option 3: You manually deploy SSL certificates. Follow the directions in these sections for the needed information.
  - For overview information of the SSL tasks, see the "Setting Up SSL Certificates" section on page 2-5.
  - For deploying your own SSL certificates, see the "Creating Your Own Certificate Authority" section on page 2-8 and the "Generating and Deploying Your Own SSL Certificates" section on page 2-9.
  - For deploying commercial SSL certificates, see the "Deploying Commercial SSL Certificates" section on page 2-12.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   `https://ip_address_of_VQES_host`

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

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

   `https://ip_address_of_VQE_tools_host/vcds-amt`

   The VCDS Application Monitoring Tool login screen should be displayed.

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

   `https://ip_address_of_VQE_tools_host`

   The VQE Channel Provisioning Tool login screen should be displayed.

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

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

Creating Your Own Certificate Authority

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

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

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

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

Generating and Deploying Your Own SSL Certificates

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

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

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

Generating a Certificate Signing Request

To generate a Certificate Signing Request, follow these steps:

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, issue the following command:

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

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

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

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

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

The command prompts for the same X.509 attributes that were specified when you created your CA certificate in the "Creating Your Own Certificate Authority" section on page 2-8. It is recommended that you provide valid input for X.509 information. Use a period (.) to indicate blank input.

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

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

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

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

Signing the Certificate Signing Request

The Certificate Signing Request (CSR) can be signed by commercial CA entities, such as VeriSign, or by your own CA as created in the "Creating Your Own Certificate Authority" section on page 2-8.

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

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

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

```
$ openssl x509 -req -days 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 Server-related or the VCPT-related software.

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

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

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

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

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

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

The stackedChain.pem file looks something like the following:

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

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

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

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

The CA certificate (ca.crt) specified in the **-file** argument is the CA certificate that you created in the "Creating Your Own Certificate Authority" section on page 2-8.

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

Step 3 Do one of the following:

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

Deploying Commercial SSL Certificates

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

Deploying a commercial certificate involves these steps:

1. Generate a Certificate Signing Request. See the "Generating a Certificate Signing Request" section on page 2-9.
2. Submit the Certificate Signing Request to the commercial CA for signing.
3. Install the certificates, private key, and keystore. See the "Commercial CA: Installing the Certificates, Private Key, and Keystore" section that follows.

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

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

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

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

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

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

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

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

The stackedChain.pem file looks something like the following:

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

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

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

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

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

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

Step 3 Do one of the following:

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

VQE-S Server: Routing and Interface Configuration Overview

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

- Bond Interfaces on a VQE-S Server, page 2-14
- Types of Routes on a VQE-S Server, page 2-15
- Static Routes on a VQE-S Server, page 2-16
- OSPF Routing on a VQE-S Server, page 2-16
- Using Dedicated or Shared Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic, page 2-17
- Routing Configuration for Dedicated Interfaces and Shared Interfaces, page 2-18
- Interface for a Management Network, page 2-20
- Load Balancing and Redundancy with Multiple VQE-S Servers, page 2-21

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

Bond Interfaces on a VQE-S Server

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

The use of a bond interface has the following benefits:

- The 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 server, a combination of bond interfaces and Ethernet interfaces can be used for management traffic.

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

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

Types of Routes on a VQE-S Server

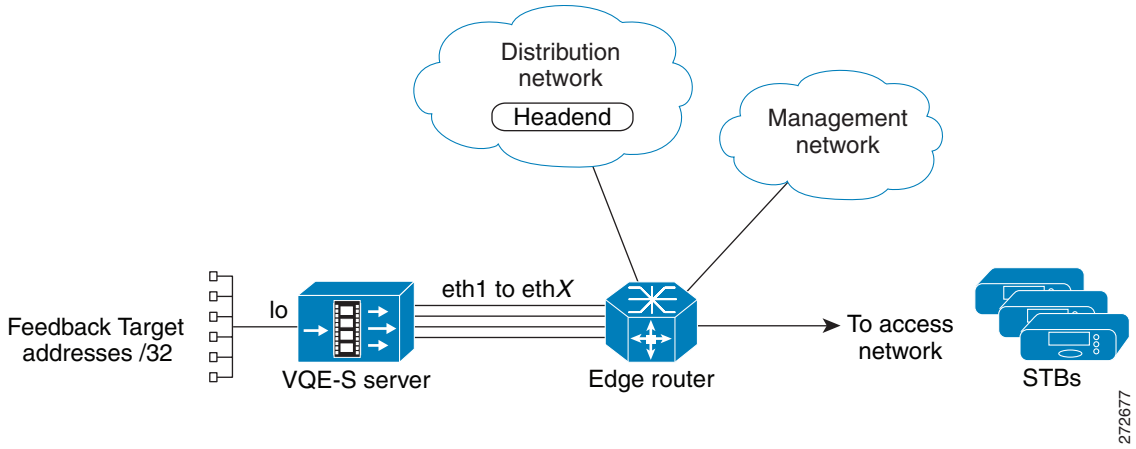
On the VQE-S server, three types of routes are used:

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

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

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

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



Static Routes on a VQE-S Server

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

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

For the feedback target routes, the use of static routes on the edge router means that repair services on the VQE-S for all feedback targets are assumed to always be available as long as the VQE-S interfaces are up. In some cases, although the interfaces are up, the VQE-S may not be able to handle requests for one or more feedback targets. The VQE-S itself can not add or withdraw the routes as services become available or unavailable for particular feedback targets. Another limitation of the use of static routes for feedback targets is that it requires the customer to take the extra step of configuring the edge router for feedback target addresses. In the worst case, this approach can require that each feedback target have a separate static route configured on the router if the feedback target addresses are not summarizable.

For information on configuring static-route parameters on a VQE-S server, see the "Gateway IP Addresses for Multipath Static Routes (VQE-S Host Only)" section on page 2-27.

For information on static route configuration on the edge router, see the "For Static Routes: Guidance for Configuring Feedback Targets on the Attached Router" section on page 2-44.

OSPF Routing on a VQE-S Server

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

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

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 will 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 server, the Quagga routing package provides the OSPF routing capability. The VQE Startup Configuration Utility and the VQE Configuration Tool simplify the OSPF configuration on the VQE-S server. After you enter values for OSPF configuration parameters, such as the OSPF area and router ID, these tools perform the configuration tasks for you. For information on configuring OSPF parameters for a VQE-S server, see the "OSPF Configuration (VQE-S Host Only)" section on page 2-27.

For information on OSPF configuration on the edge router, see the "For OSPF Routing: Guidance for Configuring the Attached Router" section on page 2-42.

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

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

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

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

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

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

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

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

Configuration Parameter For	Where To Find Information
Dedicated Interfaces	
Dedicated interfaces for VQE-S ingest traffic	"Interfaces for VQE-S Ingest Traffic (VQE-S Host Only)" section on page 2-28
Dedicated interfaces for VQE-S services traffic	"Interfaces for VQE-S Services Traffic (VQE-S Host Only)" section on page 2-29
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 2-29

Routing Configuration for Dedicated Interfaces and Shared Interfaces

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

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

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

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

For one or more interfaces for VQE-S ingest traffic, the best way to configure static routes to the distribution network is to use the configuration parameter that is (usually) used to define static routes to the management network. This parameter can also be used to define static routes to the distribution network. See "Configuring Static Routes to the Distribution Network" section on page 2-19.

For information on the configuration parameters that are used for static routes and OSPF routing, see the "Gateway IP Addresses for Multipath Static Routes (VQE-S Host Only)" section on page 2-27 and the "OSPF Configuration (VQE-S Host Only)" section on page 2-27.

For information on configuring static routes to the management network, see the "IP Address and Prefix Length and Gateway Address for a Static Route to a Management Network (Optional)" section on page 2-25.

Configuring Static Routes to the Distribution Network

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 network.route.mgmt_route parameter that is also used to configure a static route to a management network. Using the VQE Startup Configuration Utility or VQE Configuration Tool and their 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 this is directly attached to a CDE110 Ethernet interface that will be used for ingest traffic.

In the following example from the VQE Configuration Tool, Ethernet interfaces eth1 and eth2 are configured as ingest interfaces. The IP address and prefix length of the distribution network is 192.0.2.0/8. The gateway IP address for the router interface directly attached to eth1 is 11.2.9.1. The gateway IP address for the router interface directly attached to eth2 is 11.2.10.1.

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

   1) Eth1 Interface IP/Mask:                    11.2.9.2/24
   2) Eth2 Interface IP/Mask:                    11.2.10.2/24
   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 Route(s):                      []
   11) Management Interface(s):                  eth1,eth2
   P) Go to Parent Menu
   R) Go to Root Menu
Enter your choice: 10

Configure multiple static routes to the management network. Enter one IP/Prefix
each time. To complete the configuration, press <Enter> at the prompt without
entering data.

Enter the destination subnet in IP/Prefix format (e.g., 1.2.3.4/32): 192.0.2.0/8
Enter the gateway IP address: 11.2.9.1
Enter the destination subnet in IP/Prefix format (e.g., 1.2.3.4/32): 192.0.2.0/8
Enter the gateway IP address: 11.2.10.1
```

As the example below shows, two static routes to the distribution network are configured; 192.2.2.0/8 via 11.2.9.1 and 192.2.2.0/8 via 11.2.10.1.

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

   1) Eth1 Interface IP/Mask:                    11.2.9.2/24
   2) Eth2 Interface IP/Mask:                    11.2.10.2/24
   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 Route(s):                     192.2.2.0/8 via 11.2.9.1, 192.2.2.0/8
   via 11.2.10.1
   11) Management Interface(s):                   eth1,eth2
   P) Go to Parent Menu
   R) Go to Root Menu
```

```
Enter your choice:
```

Interface for a Management Network

From VQE Release 3.4, management traffic is blocked from non-management interfaces. The service provider must designate at least one CDE110 Ethernet interface or one bond interface as a management interface. Bond interfaces are configurable on VQE-S hosts only. The Ethernet interfaces must not be members of a bond interface. Multiple Ethernet or bond interfaces may be designated as management interfaces. The default value is all Ethernet interfaces on the VQE server or VQE Tools server, regardless of their operational status.

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

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

Note If ports other than those listed in Table 2-3 are used for management traffic on non-management interfaces, management traffic on the non-standard protocol ports will not be blocked. To block non-standard management protocol ports, you should manually update the rules in the **iptables.**

Manual changes to the **iptables** will not be preserved during an upgrade of the server. Also, to ensure manual changes are not overwritten, and to allow the VQE Configuration Tool to manage further configuration changes, use the **vqe_cfgtool** command with **-fix_checksum** option to have the checksum recomputed. For more information on the **-fix_checksum** option, see the "Managing /etc Configuration Files by Manually Editing the Files" section on page 7-3

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

Port Number	Standard Management Traffic Type
22	Secure Shell (SSH)
443	Hypertext Transfer Protocol Secure (HTTPS)
444	HTTPS Push
161 and 162	Simple Network Management Protocol (SNMP)
21	File Transfer Protocol (FTP)

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

- Interfaces for VQE-S Ingest Traffic
- Interfaces for VQE-S Services Traffic

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

To set up one or more static routes to the management network, use the Management Route(s) parameter in the VQE Startup Configuration Utility or Configuration Tool. This parameter requires that you specify the interface on the router that is directly attached to the CDE110 Ethernet interface or bond interface that will be used for the management network.

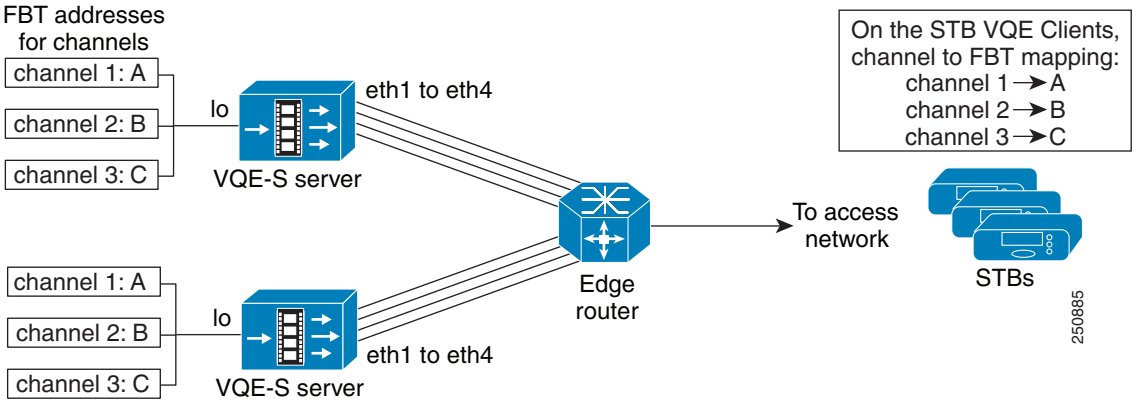
Load Balancing and Redundancy with Multiple VQE-S Servers

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

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

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

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



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

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

VQE Tools Server: Routing Configuration Overview

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

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

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

Using the VQE Startup Configuration Utility

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

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

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

- Read the "VQE-S Server: Routing and Interface Configuration Overview" section on page 2-14.
- Read the "VQE Tools Server: Routing Configuration Overview" section on page 2-22.
- Read the "Configuration Parameters" section on page 2-23.
- Complete the "Pre-Configuration Worksheets" section on page 2-31.
- Read the "VQE Configuration Tool Root Menu" section on page 2-34.

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

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

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

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

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

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

- On the VQE-S Host: Verifying Status of VQE and System Services, page 2-36
- On the VQE Tools Host: Verifying Status of VQE and System Services, page 2-38

Configuration Parameters

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

Tip For many configuration parameters, you will need to gather some information prior to booting the CDE110 for the first time and using the VQE Startup Configuration Utility. The worksheets in the "Pre-Configuration Worksheets" section on page 2-31 may be helpful in organizing the information.

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

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

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

Passwords for root and the vqe User IDs

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

The vqe username is a predefined Linux user ID that the system administrator can use to log in to VQE-S AMT, 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 towards the number of character classes used.

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

Hostname for the CDE110

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

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

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

System Timezone

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

NTP Server IP Addresses

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

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

Current System Time

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

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

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

- Read-only community string—Password for read-only access to the VQE-S or VQE Tools server
- Location information—Physical location of the VQE-S or VQE Tools server
- Contact information—Username of a contact person who has management information for the CDE110 server
- Trap listeners—IP addresses or fully qualified hostnames of the management hosts that will receive the SNMP messages

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

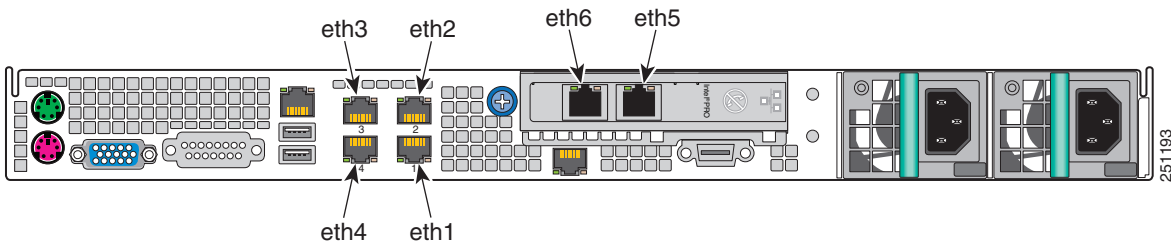
Ethernet Interface Configurations IP Addresses and Prefix Lengths

For one or more of the Ethernet ports on the Cisco CDE110, you specify an IP address and prefix length (for example, 1.2.3.4/32). The IP address and prefix length are not specified for any CDE110 Ethernet interface that is a member of a bond interface. The Ethernet ports are named eth1 to eth6 as shown in Figure 2-3.

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

- On a VQE-S host, up to six Ethernet interfaces are typically configured and used for incoming multicast streams, outgoing Unicast Retransmissions, and other VQE-S traffic.
- On a VQE Tools host, at least one Ethernet interface is typically configured and used for VCPT and VQE Client Configuration Delivery Server (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 Configurations IP Addresses and Prefix Lengths

On the VQE-S, you specify an IP address and prefix length (for example, 1.2.3.4/32) for one or more bond interfaces using the network.*bondx*.addr parameter where, depending on CDE110 model, *bondx* is bond1, bond2 or bond3. For each bond interface, you assign Ethernet interfaces to the bond interface using the network.*bondx*.member parameter where, depending on CDE110 model, *bondx* is bond1, bond2 or bond3. The Ethernet interfaces must not be members of an existing bond interface and do not have an IP address and prefix length assigned. On a VQE-S host, up to three bond interfaces may be configured and used for the Ethernet interfaces handling incoming multicast streams, outgoing VQE-S services, and management traffic.

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

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

   1) Eth1 Interface IP/Mask:                    11.2.9.2/24
   2) Eth2 Interface IP/Mask:                    11.2.10.2/24
   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 Route(s):                      []
   11) Management Interface(s):                  eth1,eth2
   P) Go to Parent Menu
   R) Go to Root Menu
Enter your choice:
```

Note Bond interfaces are not supported on the VQE Tools server.

For more information on the restrictions that apply to the use of bond interfaces, see "Bond Interfaces on a VQE-S Server" section on page 2-14.

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

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

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

  10.1.0.0/16

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

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

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 When the VQE-S server uses one or more dedicated interfaces for multicast stream ingest traffic, this parameter can be used to define a static route to the distribution network where video sources reside. For information on this use, see "Routing Configuration for Dedicated Interfaces and Shared Interfaces" section on page 2-18.

Note If you configure a static route for a management network, the Multicast Load Balancer (MLB) will monitor the status of this route. If the MLB detects that the underlying interface is administratively down, the MLB will attempt to re-create the route once the interface is brought back up.

SSL Certificates Options

Secure Sockets Layer (SSL) certificates must be created and deployed for VQE-S AMT, VCDS AMT, or VCPT to be accessed using HTTPS. The VQE Startup Configuration Utility gives you three options for creating and deploying the certificates. For information on the three options and using the utility for creating and deploying SSL certificates, see the "Using the Cisco VQE Startup Configuration Utility for SSL Certificates" section on page 2-5.

Trusted Provisioning Clients

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

- For a VQE Server host, if your IPTV deployment will use VCPT or another channel-provisioning server to send channel information to the VQE Servers, you specify the IP addresses of the trusted channel-provisioning servers. If VCPT is the channel-provisioning server, the IP addresses of all Ethernet interfaces (that have been assigned IP addresses) on the VCPT host must be configured as trusted HTTPS clients on the VQE-S host.
- For a VQE Tools host where a VCDS receives channel information from VCPT, *all Ethernet interfaces* (that have been assigned IP addresses) on the VCPT host sending the channel information must be specified as addresses in Trusted Provisioning Client(s). This requirement applies even when the VCDS is in the same VQE Tools server as the VCPT.
- For a VQE Tools host, if a VQE-C system configuration provisioning server 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 will 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 server or VQE Tools server is configured so that only trusted HTTPS clients (as specified in the Trusted Provisioning Client(s) parameter) can send information to, respectively, the VQE-S server or VQE Tools server using HTTPS.

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

If static routes are used for VQE-S traffic (ingest and services) or VQE-S services traffic, the VQE-S host is configured for one or more default gateway (next hop) router interfaces. To create a static route to the access network, you specify the IP addresses for the interfaces on the router that is directly attached to the VQE-S host. Specify as many gateway (next hop) router interfaces as are reachable through the CDE110 Ethernet interfaces or bond interfaces that have been configured with an IP address and prefix length.

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

VQE-S uses Equal Cost Multipath (ECMP) to load-balance its output traffic across CDE110 Ethernet interfaces or the physical Ethernet interfaces of a bond interface that are directly attached to the gateway router interfaces that are specified. If a default route (the gateway IP address) is configured for each Ethernet interface that is available to VQE-S for Unicast Retransmissions, RCC, and other VQE-S traffic, ECMP load balances output traffic across all of the CDE110 interfaces directly attached to the gateway router interfaces. Similarly, if a default route is configured for a bond interface, ECMP load balances output traffic across all of the CDE110 physical interfaces assigned to the bond interface.

For more information on ECMP configuration, see the "Configuring Static Routes for VQE-S Traffic or VQE-S Services Traffic" section on page D-8.

OSPF Configuration (VQE-S Host Only)

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

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

Table 2-4 OSPF Parameters

Parameter	Description
Enable OSPF	Specifies whether OSPF routing is enabled for VQE-S traffic (where shared interfaces to the access network are configured) or for VQE-S services traffic (where dedicated interfaces to the access network are configured).
Area Type	Type for the OSPF area that the VQE-S traffic interfaces and feedback target host addresses will reside in. You can choose either normal or nssa (Not So Stubby Area). If no value is specified, the default value is normal.
Area ID	Integer ID value for the OSPF area that the VQE-S Ethernet interfaces and feedback target addresses will reside in. If no value is specified, the default value is 0. Allowed range is 0 to 4,294,967,295.
Router ID	IP address used as the router ID to uniquely identify the VQE-S server in the OSPF network. The router ID must not be the same as the IP address of one of the CDE110 Ethernet interfaces because the router ID will be added as an internal address to the loopback interface.

Table 2-4 OSPF Parameters (continued)

Parameter	Description
Enable MD5	Specifies whether Message Digest 5 (MD5) authentication is enabled on the Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, specifying an MD5 key and MD5 key ID are required.
MD5 Key	If MD5 authentication is enabled, specifies a key (a string) that will be configured for all Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, an MD5 key and MD5 key ID are required. Allowed length for the string is 1 to 16 characters.
MD5 Key ID	If MD5 authentication is enabled, specifies an MD5 key ID (an integer) that will be used for all Ethernet interfaces used for VQE-S traffic. When MD5 authentication is enabled, an MD5 key and MD5 key ID are required. Allowed range of integer values is 1 to 255.
Hello Interval	Interval (in seconds) at which OSPF Hello packets are sent. This value must be the same for all interfaces running OSPF in the network. The hello interval will be set for all VQE-S interfaces running OSPF. If no value is specified, the default value is 10. Allowed range is 1 to 65,535.
Dead Interval	OSPF dead interval (in seconds). The dead interval is the maximum amount of time allowed to receive a Hello packet from a neighbor before that neighbor is declared down. This value must be the same for all interfaces running OSPF in the network. The dead interval will be set for all VQE-S interfaces running OSPF. If no value is specified, the default value is 40. Allowed range is 1 to 65,535.

For information about routing on the VQE-S host, see the Table 2-1“VQE-S Server: Routing and Interface Configuration Overview” section on page 2-14.

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

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

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

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

- At least one interface must be specified in the Interfaces for VQE-S Ingest Traffic (ingest and services) parameter (this parameter).
- At least one VQE-S services interface must be specified in the Interfaces for VQE-S Services Traffic parameter.
- The interfaces for VQE-S Ingest Traffic must not be specified in the Interfaces for VQE-S Services Traffic parameter.
- The interfaces for VQE-S Traffic (ingest and services) parameter (in VCDB, vqe.vqes.vqe_interfaces) must not be specified.

- If a dedicated interface is used for management traffic, it must not be specified in Interfaces for VQE-S Ingest Traffic parameter, in the Interfaces for VQE-S Services Traffic parameter, or in the Interfaces for VQE-S Traffic (ingest and services) parameter.

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

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

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

For the rules that apply when you choose to select a dedicated interface for VQE-S ingest traffic and interfaces for VQE-S services traffic, see the preceding section "Interfaces for VQE-S Ingest Traffic (VQE-S Host Only)".

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

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

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

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

Interfaces for Management Traffic

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

For the rules that apply when you specify management interfaces, see the "Interface for a Management Network" section on page 2-20.

VQE Configuration Tool Root Menu

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

```
VQE Configuration Tool Root Menu:
```

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

Enter your choice:
```

For information on this menu, see the "VQE Configuration Tool Root Menu" section on page 2-34.

When you have completed the configuration items, you choose `S) Save/Apply and reboot system`. The VQE Startup Configuration Utility saves your configuration in the VCDB file, applies the VCDB values to the configuration files under /etc, and reboots the CDE110 system. Each time the VQE-S or VQE Tools host reboots, the services listed in Table 2-5 and Table 2-6 will be started.

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

Service	Description
vqes	The VQE-S service (process_monitor process) starts and monitors the other VQE-S processes—Control Plane, Data Plane, Multicast Load Balancer, and STUN Server.
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.
snmpsa	(Optional) The SNMP subagent.
ntpd	(Optional) The NTP daemon.
check_daemons	A script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a **cron** job owned by root.
If OSPF is selected as the routing type	
watchquagga	The Quagga watchdog process. If the ospfd or zebra daemon crashes or hangs, watchquagga restarts it automatically.
ospfd	The OSPF daemon.
zebra	The zebra daemon.

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

Service	Description
vcds	VQE Client Configuration Delivery Server (VCDS) service
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.
snmpsa	(Optional) The SNMP subagent.

Table 2-6 VCDS and System Services for CDE110 That Hosts VQE Tools (continued)

Service	Description
ntpd	(Optional) The NTP daemon.
check_daemons	A script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a **cron** job owned by root.

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

Pre-Configuration Worksheets

Before using the VQE Startup Configuration Utility, complete the pre-configuration worksheets in Table 2-7 for a VQE-S host and Table 2-8 for a VQE Tools host before the first normal boot. The use of a VQE Tools server and VCPT is optional.

For information on the configuration items in Table 2-7 and Table 2-8, see the "Configuration Parameters" section on page 2-23.

Table 2-7 VQE-S CDE110: Pre-Configuration Worksheet

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

Table 2-7 VQE-S CDE110: Pre-Configuration Worksheet (continued)

Configuration Item	Value for Your Deployment
Ethernet interface configurations (IP address and prefix lengths)	eth1: eth2: eth3: eth4: eth5: eth6:
Bond interface configurations (IP address, subnet mask and members	bond1: bond2: bond3:
For static routes to a management network and for static routes to a distribution network—subnet IP address and prefix length, and gateway (next hop) IP address	IP address and prefix length: Gateway (next hop) IP address:
SSL certificate option	
Trusted provisioning clients IP addresses	
If static routes to the access network, default gateway (next hop) IP addresses for multipath static routes	IP addresses:
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 will be used for VQE-S ingest traffic Ethernet interface names or bond interface name that will be used for VQE-S services traffic	

Table 2-7 VQE-S CDE110: Pre-Configuration Worksheet (continued)

Configuration Item	Value for Your Deployment
Ethernet interface names or bond interface name that will be used for VQE-S traffic (ingest and services)	
One or more Ethernet interface names, or one or more bond interface names, or both that will be used for management traffic	

Table 2-8 VQE Tools CDE110: Pre-Configuration Worksheet

Configuration Item	Value for Your Deployment
Password for root	
Password for the vqe username (a pre-defined Linux user ID)	
Hostname of the CDE110 for VCPT	
Domain Name System (DNS) IP addresses and a search domain	DNS IP address: DNS IP address: Search domain:
System timezone	
External NTP server IP addresses	
SNMP read-only community string Location for SNMP: Contact for SNMP: SNMP trap-listener IP addresses or hostnames	community string: location: contact: IP addresses or hostnames:
Ethernet interface configurations (IP address and mask)	eth1: eth2: eth3: eth4: eth5: eth6:
For static routes to a management network or external access on the VQE Tools server—subnet IP address and prefix length, and gateway (next hop) IP address	IP address and prefix length: Gateway (next hop) IP address:

Table 2-8 VQE Tools CDE110: Pre-Configuration Worksheet (continued)

Configuration Item	Value for Your Deployment
SSL certificate option	
Ethernet interface names that will be used for management traffic	
Trusted provisioning clients IP addresses	

VQE Configuration Tool Root Menu

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

```
VQE Configuration Tool Root Menu:

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

Enter your choice:
```

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

Note For information on how to use the VQE Configuration Tool Root Menu and the other menu choices, see the "Using the VQE Configuration Tool" section on page 7-4. *The information in the "Using the VQE Configuration Tool" section is applicable to the Root Menu and other menu choices presented at the end of the VQE Startup Configuration Utility.*

The Root Menu choices allow you to do the following:

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

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

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

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

Table 2-9 Root Menu Choices (for a VQE -S Server)

Root Menu Choice	Menu Description
1) System Parameters	Allows you to view the current system parameter values that you have set, and to change or set the system parameters values: 1) Hostname 2) DNS Server(s) 3) DNS Search Domain 4) Timezone 5) NTP Server(s) 6) SNMP RO Community String 7) SNMP System Location 8) SNMP System Contact 9) SNMP Trap Listener(s) 10) Trusted Provisioning Client(s)
2) Network Parameters > 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 Route(s) 11) Management Interface(s)
2) Network Parameters > Routing Parameters > Static Routing Parameters	Allows you to view the current static routing parameter values that you have set, and to change or set the static routing parameter value: 1) Default Gateway(s)
3) Configure VQE Password	Allows you to set the password for the vqe username. Once you select this menu choice, you must enter the password value even if you choose to keep the current password.
4) Generate SSL Certificate	Allows you to create and deploy a Secure Sockets Layer (SSL) certificate for VQE-S AMT, VCDS AMT or VCPT, or to generate a Certificate Signing Request file (server.csr).

Table 2-9 Root Menu Choices (for a VQE -S Server) (continued)

Root Menu Choice	Menu Description
5) VQE-S Parameters	Allows you to view the current VQE-S parameter values that you have set, and to change or set the VQE-S parameters values: 1) Log Priority * 2) Excess Bandwidth Fraction * 3) Traffic (Ingest+Service) Interface(s) 4) Ingest Interface(s) 5) Service Interface(s) * The VQE Startup Configuration Utility does not allow you to set the values of these parameters in the set of parameters that were previously displayed. You can supply values at this point if you want or accept the defaults. For more information on these values, see the vcdb.conf.sample file and Appendix A, "VQE, System, and Network Parameters."
6) Save/Apply and reboot the system	Saves the changes you have made to the parameters in the VQE Configuration Database (VCDB), applies parameter values to the configuration files under /etc, and reboots the CDE110 system.

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

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

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

Step 1 If needed, log in as root.

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

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

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

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

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

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

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

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

Tomcat is running...
```

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

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

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

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

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

The SNMP subagent is running.
```

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

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

watchquagga (pid 2513) is running...

[root@system]# service ospfd status

ospfd (pid 7104) is running...

[root@system]# service zebra status

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

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

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

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

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

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

root       710     1  0 Mar24 pts/7    00:00:00 /opt/vqes/bin/process_monitor
vqes       723   710  0 Mar24 pts/7    00:00:00 stun_server --ss-uid 499 --ss-gid 499
--xmlrpc-port 8054 --log-level 6
root       782   710 99 Mar24 pts/7    29-21:09:08 vqes_dp --group vqes --max-channels
500 --max-outstanding-rpcs 500 --max-pkts 150000 --log-level 6 --rtp-inactivity-tmo
300 --max-core-bw 850000000 --reserved-core-rcv-bw 100000000 --reserved-core-er-bw
120000000 --max-rai-gap 15
vqes       855   710  0 Mar24 pts/7    00:00:00 vqes_cp --cp-uid 499 --cp-gid 499
--xmlrpc-port 8051 --cfg /etc/opt/vqes/vqe_channels.cfg --er-cache-time 3000
--rtp-hold-time 100 --max-channels 500 --max-outstanding-rpcs 500 --max-queued-rpcs
1000 --max-reserved-rpcs 32000 --max-clients 32000 --er-pkt-tb-rate 50000
--er-pkt-tb-depth 100 --er-blp-tb-rate 10000 --er-blp-tb-depth 100
--client-er-policing --client-er-tb-rate-ratio 5 --client-er-tb-depth 10000
--log-level 6 --rcc-mode conservative --igmp-join-variability 100 --max-client-bw 0
--max-idr-penalty 0 --rap-interval 2000 --excess-bw-fraction 20
--excess-bw-fraction-high-def 12 --high-def-min-bw 6000000 --buff-size-preroll-max
1500 --rcc-burst-delay-to-send 10 --rtp-dscp 0 --rtp-rcc-dscp -1 --rtcp-dscp 24
--overlap-loss 0 --intf-output-allocation 90 --max-rpr-stream-burst-msecs 30
--max-rpr-stream-burst-pkts 2 --unity-e-factor-interval 5
--min-client-excess-bw-fraction 0 --max-client-excess-bw-fraction 500

[root@system]# ps -ef | grep mlb

root      2989  2965  0 09:17 pts/0    00:00:03 mlb --interface eth2,eth3,eth4
--xmlrpc-port 8052 --unicast-reservation 20 --poll-interval 1 --ssm --log-level 6
```

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

- process_monitor—Process Monitor
- stun_server—STUN Server
- vqes_dp—Data Plane

- vqes_cp—Control Plane
- mlb—Multicast Load Balancer

Step 10 If you configured an IP address for an external NTP server, to verify that the NTP service is running, issue the following command:

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

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

Step 11 To use the VQE-S Application Monitoring Tool from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE-S:

```
https://ip_address_of_VQES_host
```

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

If you click **System** in the left pane, the VQE-S Application Monitoring Tool displays information on the VQE-S processes and channels. Figure 4-2 on page 4-3 shows an example. Because at this point no channel information has been sent to the VQE-S, no channels will be displayed.

Step 12 Do one of the following:

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

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

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

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

Step 1 If needed, log in as root.

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

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

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

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

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

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

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

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

Tomcat is running...
```

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

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

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

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

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

The SNMP subagent is running.
```

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

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

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

Step 8 To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts 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 9 To use the VCDS Application Monitoring Tool from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VQE Tools:

```
https://ip_address_of_VQE_tools_host/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 Application Monitoring Tool.)

If you click **System** in the left pane, the VCDS Status window displays information on the VCDS processes. Figure 5-2 on page 5-3 shows an example.

Step 10 Do one of the following:

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

Configuring VQE-S RTCP Exporter

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

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

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

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

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

Step 2 Edit the /etc/opt/vqes/vcdb.conf file and add to the file the three key-value pairs for the RTCP Exporter parameters listed in Table 2-10. Specify values for each of the parameters.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 7-13. The parameters used for enabling the RTCP Exporter are not available in the VQE Configuration Tool.

Step 3 Save the vcdb.conf file.

Table 2-10 RTCP Exporter Parameters

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

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

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

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

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

For more information on the **vqe_cfgtool** command and the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-17.

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

Configuring Other Parameters for the VQE-S Host

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

Read the following to get information on these additional parameters:

- Chapter 7, "Configuring VQE Server and VQE Tools" describes the tools and procedures to used to configure all parameters for a VQE-S or VQE Tools system.
- Appendix A, "VQE, System, and Network Parameters" describes the VQE-S, system, and network parameters.
- The file /etc/vqes/vcdb.conf.sample provides additional information on the VQE-S, system, and network parameters.

Configuring the Edge Router for VQE-S

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

- For Bond Interfaces: Guidance for Configuring Bond Interface on the Attached Router, page 2-41
- For OSPF Routing: Guidance for Configuring the Attached Router, page 2-42
- For Static Routes: Guidance for Configuring Feedback Targets on the Attached Router, page 2-44

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 1-4.

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 Separate OSPF Area, page 2-43
- VQE-S in Area 0, page 2-43
- General Guidelines, page 2-44

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

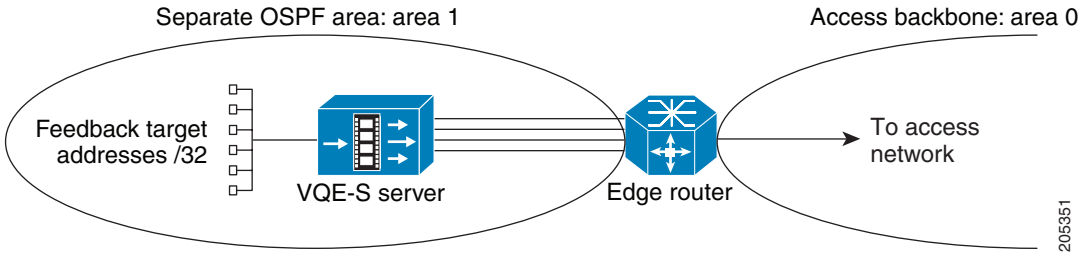
http://www.cisco.com/en/US/tech/tk365/tk480/tsd_technology_support_sub-protocol_home.html

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

VQE-S in Separate OSPF Area

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

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



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

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

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

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

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

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

VQE-S in Area 0

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

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

General Guidelines

The following are general edge router configuration guidelines:

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

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

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

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

- Directly connected VQE-S—The VQE-S server *must be directly connected* to the edge router on all VQE-S traffic 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 Separate OSPF Area" section on page 2-43.

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

When channels are configured with a channel-provisioning tool such as VQE Channel Provisioning Tool, it is required that you specify a unique feedback target (FBT) address for each channel. If static routes are used for VQE-S traffic (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 11.2.9.2
ip route 8.86.1.0 255.255.255.0 11.2.10.2
ip route 8.86.1.0 255.255.255.0 11.2.11.2
ip route 8.86.1.0 255.255.255.0 11.2.12.2
```

For the preceding configuration example, the IP addresses 11.2.9.2, 11.2.10.2, 11.2.11.2, and 11.2.12.2 have been assigned to the Ethernet interfaces on the VQE-S host. See Figure D-3 on page D-8. These Ethernet interfaces are used for VQE-S traffic, including Unicast Retransmission and Rapid Channel Change traffic.