Manual Initial VQE System Configuration

This appendix explains how to perform manual initial configuration on the two categories of CDE servers running the VQE software:

- VQE server (VQE-S)—CDE hosting the VQE-S
- VQE Tools server—CDE hosting VQE Channel Provisioning Tool (VCPT), VQE Client Configuration Delivery Server (VCDS) and VCDS AMT.

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

The alternative to manual configuration is to use the Cisco vqe_cfgtool. For information on using the utility, see the .

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

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

The manual initial configuration procedures are explained in these sections:

- Setting Up a Cisco CDE That Hosts VQE-S
- Setting Up a Cisco CDE That Hosts VQE Tools

Setting Up a Cisco CDE That Hosts VQE-S

This section explains how to perform the initial configuration tasks for a Cisco CDE hosting the VQE-S.

When performed manually, the initial configuration tasks involve editing the /etc/opt/vqes/vcdb.conf file to configure the essential VCDB parameters. The use of the vcdb.conf file simplifies the configuration tasks. Because the VQE Configuration Tool automatically applies the VCDB values to the /etc configuration files on system reboot, mistakes in configuration file syntax are unlikely.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 7-14.

Perform these initial configuration tasks in the order shown:

1. Prerequisites for a Cisco CDE That Hosts the VQE-S, page D-3

2. Configuring the Linux Operating System for the VQE-S, page D-3

3. Configuring Bond Interfaces, page D-5

4. Configuring a Static Route for a Management Network (VQE-S Host), page D-6

5. Configuring Static Routes for VQE-S Traffic or VQE-S Services Traffic (VQE-S Host), page D-8

6. Enabling OSPF Routing for VQE-S Traffic or VQE-S Services Traffic, page D-10

7. Configuring Interfaces for VQE-S Traffic (Ingest and Services) and VQE-S Services Traffic, page D-15

8. Synchronizing the Time and Configuring Network Time Protocol, page D-19

9. VQE STUN Server Is Enabled By Default, page D-20

10. Configuring SNMP, page D-20

11. Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS, page D-21

12. Configuring Remote Syslog Servers, page D-22

13. Starting VQE-S System Services and Verifying Status, page D-22

14. Starting the VQE-S Processes and Verifying Status, page D-27

15. Restarting the System and Verifying System and VQE-S Status, page D-28

✎

Note   The configuration instructions in this section are intended for new installations of Cisco VQE Release 3.6 software, where the Cisco CDE has the Cisco VQE Release 3.6 software preinstalled.

For information on upgrading an already configured Cisco CDE, see the Release Notes for Cisco CDA Visual Quality Experience, Release 3.6.

For information on configuring the VQE-S RTCP Exporter, see the "Configuring the VQE-S RTCP Exporter" section on page 2-41.

Prerequisites for a Cisco CDE That Hosts the VQE-S

This section explains tasks that should be performed before setting up a Cisco CDE that hosts the VQE-S.

Connecting Cables for the VQE-S

For information on connecting cables on the VQE-S, see the "Connecting Cables to the CDE" section on page 2-4.

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

Setting Up SSL Certificates for the VQE-S

It is recommended that you deploy your own Secure Sockets Layer (SSL) certificates or commercial SSL certificates before beginning the tasks for setting up a Cisco CDE that hosts the VQE-S. For information on setting up the certificates, see the "Setting Up SSL Certificates" section on page 2-5.

Configuring the Linux Operating System for the VQE-S

This section explains the initial Linux configuration tasks needed for a Cisco CDE appliance that runs the VQE-S software. The explanation assumes that the needed software for Linux and the VQE-S has been preinstalled on the Cisco CDE appliance. For Red Hat Enterprise Linux 5.1 documentation, go to the following website:

http://www.redhat.com/docs/manuals/enterprise/

For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE back panel are specified as eth1 to eth6 as shown in Figure D-1.

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

Figure D-1   NIC Port Numbering for Software Configuration
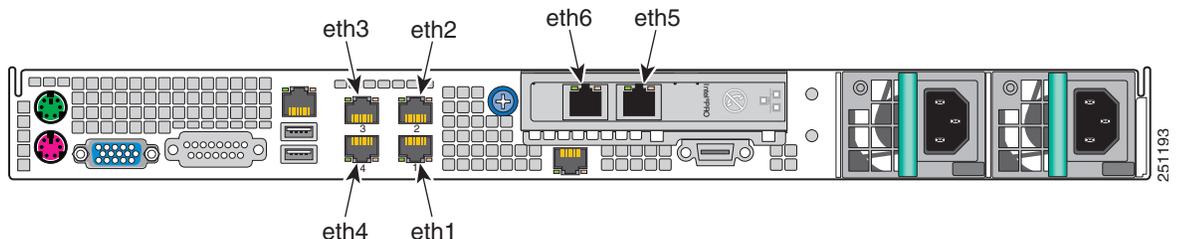
For the configuration examples in this section, Figure D-2 shows the IP addresses for interfaces eth1, eth2, bond1 (with eth3 and eth4 as its members), and the corresponding interfaces on the edge router.

Figure D-2   IP Addresses for VQE-S Configuration Examples
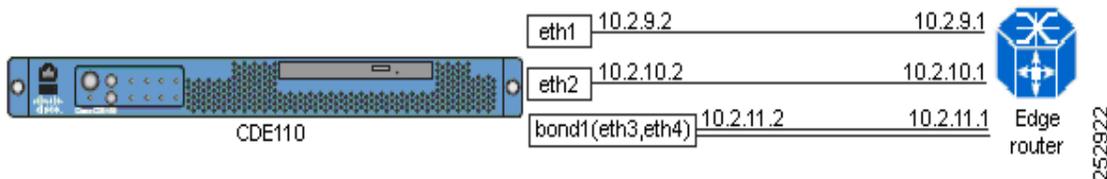
To configure the Linux operating system and other software for the VQE-S, follow these steps:

Step 1   If needed, login as root. You must have root privileges to modify the vcdb.conf file.

Step 2   To create the password for the vqe username (a pre-created Linux user ID), issue the following command:

```
[root@system]# passwd vqe
```

Enter a password that follows the password guidelines:

```
A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use an 8 character long
password with characters from at least 3 of these 4 classes, or
a 7 character long password containing characters from all the
classes.  An upper case letter that begins the password and a
digit that ends it do not count towards the number of character
classes used.

A passphrase should be of at least 3 words, 12 to 40 characters
long and contain enough different characters.
```

This username and password can be used to log in to Linux directly using SSH. The vqe username and password can also be used log in to the VQE-S AMT.

Step 3   To configure CDE Ethernet interfaces eth1 to eth6, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.*ethx*.addr parameters, where *ethx* is eth1, eth2, and so on. Specify an IP address and prefix length for each interface that is not a member of a bond interface. The following example shows two vcdb.conf lines for the two Ethernet interfaces:

```
network.eth1.addr="10.2.9.2/24"
network.eth2.addr="10.2.10.2/24"
```

Step 4   To configure the hostname for the CDE server, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the system.global.hostname parameter and specifying a hostname. The following example specifies the hostname as starfire-iptv:

```
system.global.hostname="starfire-iptv"
```

Step 5   To configure a DNS server, edit the /etc/opt/vqes/vcdb.conf file by adding the VCDB parameters for the IP address and optionally for the search domain of a DNS server and specifying the needed values:

- system.dns.server="*IP_address*"
- system.dns.search_domain="*search_domain*"

For example:

```
system.dns.server="192.0.20.53."
system.dns.search_domain="domain.com"
```

Step 6 Save the vcdb.conf file.

Configuring Bond Interfaces

This section provides information on configuring bond interfaces on the CDE that hosts the VQE-S. Bond interfaces may be used for the VQE-S traffic (ingest and services), VQE-S ingest traffic, or VQE-S service traffic, depending on whether shared or dedicated interfaces are configured. Bond interfaces may also be used for VQE-S management traffic.

Note For guidance on using bond interfaces, see the "Bond Interfaces on a VQE-S" section on page 2-12.

To configure a bond interface with one or more CDE Ethernet interfaces as members, follow these steps:

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

Step 2 To configure CDE bond interfaces bond1 to bond3, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.*bondx*.addr parameters, where *bondx* is bond1, bond2, or bond3. Specify an IP address and prefix length for each bond interface. The following example shows a line added to the vcdb.conf file for a single bond interface:

```
network.bond1.addr="10.2.11.2/24"
```

Step 3 To add CDE Ethernet interfaces to a bond interface, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.*bondx*.member parameters, where *bondx* is bond1, bond2, or bond3. Specify the CDE Ethernet interfaces to be added as members to each bond interface. The following example shows a line added to the vcdb.conf file to add two Ethernet interfaces to a bond interface:

```
network.bond1.member="eth3,eth4"
```

Note An Ethernet interface should not be assigned as a member of a bond interface if that Ethernet interface is either already assigned an IP address and prefix length, or if that Ethernet interface is already a member of another bond interface.

Step 4 Save the vcdb.conf file.

Note VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System and VQE-S Status section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

After the VQE-S host is rebooted or the configuration has been applied, you can verify that the Ethernet interfaces and bond interfaces are configured correctly and up and running by issuing the following commands:

- Use the **ifconfig** *interface* command to verify that each Ethernet interface or bond interface is up and running and the IP address and netmask for each are set correctly. The following example is for eth1:

```
[root@system]# ifconfig eth1

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:C1:F4:0F
          inet addr:10.7.10.2  Bcast:10.7.10.255  Mask:255.255.255.0
          inet6 addr: fe90::20e:cff:fec7:f30f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:192 (192.0 b)  TX bytes:2700 (2.6 KiB)
          Base address:0x3000 Memory:b8800000-b8820000
```

The following example is for bond1:

```
[root@system]# ifconfig bond1

bond1     Link encap:Ethernet  HWaddr 00:0E:0C:C6:D4:2E
          inet addr:8.5.28.2  Bcast:8.5.28.255  Mask:255.255.255.0
          inet6 addr: fe90::20e:cff:fec5:d42e/64 Scope:Link
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:1198174 errors:0 dropped:0 overruns:0 frame:0
          TX packets:866284 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:124912504 (119.1 MiB)  TX bytes:105570108
```

- Use the **ip link show eth**# command (where # is the Ethernet or bond interface number) to check that the link is up. The following example is for eth1:

```
[root@system]# ip link show eth1

eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0e:0c:c6:e4:fe brd ff:ff:ff:ff:ff:ff
```

The following is an example for bond1:

```
[root@system]# ip link show bond1

bond1: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue
link/ether 00:0e:0c:c6:d4:2e brd ff:ff:ff:ff:ff:ff
```

- Use the **ping** command to check that the Cisco CDE can reach the connected edge router. For example:

```
[root@system]# ping 10.2.9.1
```

Configuring a Static Route for a Management Network (VQE-S Host)

If your deployment makes use of a management network, a static route for the management network can be configured using the VCDB parameter network.route.static_route. The configuration example in this section configures CDE Ethernet interface eth1 as the interface to the management network.

When the VQE-S uses dedicated interfaces for ingest traffic for multicast streams, the network.route.static_route parameter can be used to define a static route to the distribution network where video sources reside. For information, see the "Routing Configuration for Dedicated Interfaces and Shared Interfaces" section on page 2-15.

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

To configure a static route for a management network, follow these steps:

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

Step 2 Edit the /etc/opt/vqes/vcdb.conf file by adding to the file a network.network.interface.mgmt_interfaces parameter. Specify the name of the Ethernet interfaces and the bond interfaces designated for management traffic. One or more CDE Ethernet or bond interfaces may be specified. The Ethernet interface must not be a member of a bond interface.

For this example, assume CDE Ethernet interface eth1(10.2.9.2) on the VQE-S host is designated for management traffic.

The line in the vcdb.conf file is as follows:

```
network.network.mgmt_interfaces="eth1"
```

Step 3 Add to the /etc/opt/vqes/vcdb.conf file a network.route.static_route parameter and specify the needed values using the following format:

network.route.static_route="*target-network-subnet-addr/prefix-length via gateway-addr:outbound-interface*"

The *target-network-subnet-addr/prefix-length* is the IP address and prefix length for the management network. The *gateway-addr* is the IP address of the router Ethernet interface or bond interface that is directly attached to the CDE Ethernet port or bond interface that is used for management network traffic. The *outbound-interface* is the interface used on the VQE-S for this static route.

For this example, assume the following:

- CDE Ethernet interface eth1 (10.2.9.2) is used for the target management network on the VQE-S host.
- Management network is 192.0.0.0/8.

The line in the vcdb.conf file is as follows:

```
network.route.static_route="192.0.0.0/8 via 10.2.9.1"
```

In the preceding example, 10.2.9.1 is the *gateway-addr*—the router interface that is directly attached to eth1 on the VQE-S host. Figure D-2 shows the IP addresses used in this example for the eth1 interface and the directly attached router.

Step 4 Save the vcdb.conf file.

> **Note** VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System and VQE-S Status section. Reboot once when all VCDB configuration tasks are completed.
>
> Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

After the VQE-S host is rebooted or the configuration has been applied, you can verify that the static route for the management network is present in the routing table by issuing the following command:

```
[root@system]# ip route show
```

The output is similar to the following:

```
192.0.0.0/8 via 10.2.9.1 dev eth1
default
    nexthop via 10.2.10.1 dev eth2 weight 1
    nexthop via 10.2.10.1 dev bond1 weight 1
```

Configuring Static Routes for VQE-S Traffic or VQE-S Services Traffic (VQE-S Host)

This section provides information on configuring static routes for VQE-S traffic to the access network on the CDE that hosts VQE-S. The configuration is similar regardless of whether dedicated interfaces or shared interfaces are used.

Note   For information on configuring static routes for feedback targets on the directly attached router, see the "For Static Routes: Guidance for Configuring the Feedback Targets on the Attached Router" section on page 2-47.

For the configuration examples in this section, Figure D-3 shows the IP addresses for interfaces eth1, eth2, eth3, and eth4 and the corresponding interfaces on the edge router.

Figure D-3   IP Addresses for VQE-S Configuration Examples
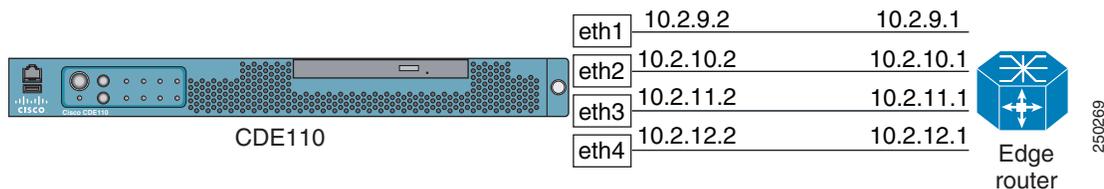
On the Cisco CDE that hosts the VQE-S, multiple Ethernet interfaces or multiple bond interfaces can be used for the VQE-S traffic, including incoming multicast streams, outgoing Unicast Retransmissions and RCC unicast transmissions, and other VQE-S traffic. In addition, some VQE deployments may use one of the Ethernet or one of the bond interfaces as the interfaces to a management network.

If a default (next hop) route is configured for each CDE Ethernet interface or bond interface that is available for VQE-S traffic, Equal Cost Multipath (ECMP) is used to load-balance VQE-S output traffic across the CDE interfaces that are directly attached to the gateway router interfaces specified in the network.route.static_route parameter.

Note   A static route should be configured for each interface used for VQE-S traffic. Otherwise, output load is not balanced and some interfaces may be overloaded.

To configure a static route for one or more CDE Ethernet interfaces or one or more bond interfaces, follow these steps:

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

Step 2   If disabling OSPF routing for VQE-S traffic is needed, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the network.route.type parameter and specifying the value static for the parameter:

```
network.route.type="static"
```

Step 3   To configure default gateways for each Ethernet interface that is available for VQE-S traffic, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.route.static_route parameters and specify the needed values using the following format:

```
network.route.static_route="target-network-subnet-addr/prefix-length via
gateway-addr:outbound-interface"
```

For the *target-network-subnet-addr/prefix-length,* specify 0.0.0.0/0.

The *gateway-addr* is the IP address of the router Ethernet interface or bond interface that is directly attached to the CDE Ethernet port or bond interface that is used for access network traffic. The *outbound-interface* is the interface used on the VQE-S for this static route and is optional.

> **Note**   For load balancing to work effectively, each interface to the distribution network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot not be specified in this parameter.

The following example shows two vcdb.conf lines that add default gateways for the Ethernet interfaces displayed in Figure D-3.

```
network.route.static_route="0.0.0.0/0 via 10.2.11.1"
network.route.static_route="0.0.0.0/0 via 10.2.12.1"
```

In the preceding example, 10.2.11.1 and 10.2.12.1 are the gateway (next hop) addresses on the router that is directly attached to the VQE-S host.

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

Step 4   Save the vcdb.conf file.

> **Note**   VCDB configurations are applied to the CDE when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-28. Reboot once when all VCDB configuration tasks are completed.
>
> Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

After the VQE-S host is rebooted or the configuration has been applied, you can verify that the default gateway routes are present in the routing table of the CDE by issuing the following command:

```
[root@system]# ip route show
```

The output is similar to the following:

```
default
    nexthop via 10.2.11.1 dev bond1 weight 1
```

Enabling OSPF Routing for VQE-S Traffic or VQE-S Services Traffic

This section provides information on enabling and configuring OSPF routing for VQE-S traffic (ingest and services) or VQE-S services traffic to the access network on the CDE that hosts the VQE-S. The configuration is similar regardless of whether dedicated interfaces or shared interfaces are used.

Note   For guidance on configuring the attached router for OSPF routing, see the "For OSPF Routing: Guidance for Configuring the Attached Router" section on page 2-44.

To configure OSPF routing for the CDE Ethernet interfaces or bond interfaces that are used for VQE-S traffic or VQE-S services traffic, follow these steps:

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

Step 2   To enable OSPF routing for VQE-S traffic to the access network, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the network.route.type parameter and specifying the value ospf for the parameter:

```
network.route.type="ospf"
```

Step 3   To configure OSPF routing for the VQE-S traffic or VQE-S services interface, edit the /etc/opt/vqes/vcdb.conf file by adding one or more of the following parameters to the file. The OSPF parameters that you choose to use depend on your network implementation.

Note   Some of the OSPF parameters have a default value if you do not add the parameter to and specify a value in the vcdb.conf file.

- network.ospf.router_id
- network.ospf.area
- network.ospf.area_type
- network.ospf.md5_enable
- network.ospf.md5_key
- network.ospf.md5_keyid
- network.ospf.hello_interval
- network.ospf.dead_interval

For information on each of the preceding parameters and default values, see Table A-8.

Step 4   Save the vcdb.conf file.

Note   VCDB configurations are applied to the CDE when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-28. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

On the VQE-S

After the VQE-S host is rebooted or the configuration has been applied, you can verify that the OSPF configuration is present on the CDE by issuing the following commands where:

- 8.31.200.1 is the OSPF router ID of the VQE-S.
- 8.31.1.1. is a feedback target address.
- 0.0.0.0/0 is the default route in the routing table on the VQE-S.
- VQE-S traffic interfaces are eth2 (10.1.1.2) and eth3 (10.1.2.2).

```
[root@system]# show ip ospf

vqe-s# show ip ospf
 OSPF Routing Process, Router ID: 8.31.200.1
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 OpaqueCapability flag is disabled
 Initial SPF scheduling delay 200 millisec(s)
 Minimum hold time between consecutive SPFs 1000 millisec(s)
 Maximum hold time between consecutive SPFs 10000 millisec(s)
 Hold time multiplier is currently 1
 SPF algorithm last executed 1m00s ago
 SPF timer is inactive
 Refresh timer 10 secs
 This router is an ASBR (injecting external routing information)
 Number of external LSA 1. Checksum Sum 0x0000efb2
 Number of opaque AS LSA 0. Checksum Sum 0x00000000
 Number of areas attached to this router: 1

 Area ID: 0.0.0.1 (NSSA)
   Shortcutting mode: Default, S-bit consensus: no
   Number of interfaces in this area: Total: 3, Active: 3
   It is an NSSA configuration.
   Elected NSSA/ABR performs type-7/type-5 LSA translation.
   It is not ABR, therefore not Translator.
   Number of fully adjacent neighbors in this area: 2
   Area has no authentication
   Number of full virtual adjacencies going through this area: 0
   SPF algorithm executed 4 times
   Number of LSA 6
   Number of router LSA 2. Checksum Sum 0x0000a03d
   Number of network LSA 2. Checksum Sum 0x00010556
   Number of summary LSA 1. Checksum Sum 0x0000519e
   Number of ASBR summary LSA 0. Checksum Sum 0x00000000
   Number of NSSA LSA 1. Checksum Sum 0x0000693e
   Number of opaque link LSA 0. Checksum Sum 0x00000000
   Number of opaque area LSA 0. Checksum Sum 0x00000000


[root@system]# show ip ospf database

        OSPF Router with ID (8.31.200.1)

             Router Link States (Area 0.0.0.1 [NSSA])

Link ID        ADV Router      Age  Seq#       CkSum  Link count
```

```
8.31.20.1       8.31.20.1       1120 0x80000012 0x1707 2
8.31.200.1      8.31.200.1      1120 0x8000001b 0x8936 3

                  Net Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#        CkSum
25.1.1.1        8.31.20.1       1125 0x80000001 0x08a6
25.1.2.1        8.31.20.1       1120 0x80000001 0xfcb0

                  Summary Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#        CkSum  Route
0.0.0.0         8.31.20.1        159 0x8000000c 0x4f9f 0.0.0.0/0

                  NSSA-external Link States (Area 0.0.0.1 [NSSA])

Link ID         ADV Router      Age  Seq#        CkSum  Route
8.31.1.1        8.31.200.1      1125 0x80000003 0x693e E2 8.31.1.1/32 [0x0]

                  AS External Link States

Link ID         ADV Router      Age  Seq#        CkSum  Route
8.31.1.1        8.31.200.1      1125 0x80000003 0xefb2 E2 8.31.1.1/32 [0x0]


[root@system]# show ip ospf route

=========== OSPF network routing table ============
N IA 0.0.0.0/0           [2] area: 0.0.0.1
                             via 25.1.1.1, eth2
                             via 25.1.2.1, eth3
N    8.31.200.1/32       [10] area: 0.0.0.1
                             directly attached to lo
N    25.1.1.0/24         [1] area: 0.0.0.1
                             directly attached to eth2
N    25.1.2.0/24         [1] area: 0.0.0.1
                             directly attached to eth3

=========== OSPF router routing table =============
R    8.31.20.1           [1] area: 0.0.0.1, ABR, ASBR
                             via 25.1.1.1, eth2
                             via 25.1.2.1, eth3

=========== OSPF external routing table ===========
```

```
[root@system]# show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>*   0.0.0.0/0 [110/2] via 25.1.1.1, eth2, 00:01:40
                        via 25.1.2.1, eth3, 00:01:40
C>* 8.31.1.1/32 is directly connected, lo
O   8.31.200.1/32 [110/10] is directly connected, lo, 00:01:49
C>* 8.31.200.1/32 is directly connected, lo
O   25.1.1.0/24 [110/1] is directly connected, eth2, 00:01:45
C>* 25.1.1.0/24 is directly connected, eth2
O   25.1.2.0/24 [110/1] is directly connected, eth3, 00:01:44
C>* 25.1.2.0/24 is directly connected, eth3
C>* 127.0.0.0/8 is directly connected, lo
K>* 224.0.0.0/4 is directly connected, eth1
```

On the Cisco 7600 Edge Router

After the VQE-S host is rebooted, you can verify that the OSPF configuration is present on the Cisco 7600 edge router by issuing the following commands where:

- 8.31.20.1 is the OSPF router ID on the edge router.

- In the **show ip route** command output, 8.31.1.1. is accessible from two interfaces, indicating the ECMP is configured correctly.

- Configuration on the edge router is as follows:

```
router ospf 100
 router-id 8.31.20.1
 log-adjacency-changes
 area 1 nssa no-summary
 traffic-share min across-interfaces
 network 25.1.1.0 0.0.0.255 area 1
 network 25.1.2.0 0.0.0.255 area 1
 network 26.1.1.0 0.0.0.255 area 0
 maximum-paths 8


c7600> show ip ospf
 Routing Process "ospf 100" with ID 8.31.20.1
 Start time: 00:00:04.540, Time elapsed: 06:07:33.660
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 It is an area border and autonomous system boundary router
 Redistributing External Routes from,
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x002F1B
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 2. 1 normal 0 stub 1 nssa
```

```
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm last executed 06:07:24.744 ago
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x012D0C
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 1
        Number of interfaces in this area is 2
        It is a NSSA area
        Perform type-7/type-5 LSA translation
        Area has no authentication
        SPF algorithm last executed 00:18:18.804 ago
        SPF algorithm executed 10 times
        Area ranges are
        Number of LSA 6. Checksum Sum 0x025E70
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 2
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

c7600> show ip ospf database

            OSPF Router with ID (8.31.20.1) (Process ID 100)

            Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#        Checksum Link count
8.31.20.1       8.31.20.1       288         0x8000000D 0x001B73 1

            Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#        Checksum
8.31.200.1      8.31.20.1       1239        0x80000001 0x009B69
25.1.1.0        8.31.20.1       1244        0x80000011 0x004292
25.1.2.0        8.31.20.1       1234        0x80000013 0x00339E

            Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#        Checksum Link count
8.31.20.1       8.31.20.1       1249        0x80000012 0x001707 2
8.31.200.1      8.31.200.1      1250        0x8000001B 0x008936 3

            Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#        Checksum
25.1.1.1        8.31.20.1       1254        0x80000001 0x0008A6
25.1.2.1        8.31.20.1       1250        0x80000001 0x00FCB0

            Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#        Checksum
0.0.0.0         8.31.20.1       289         0x8000000C 0x004F9F
```

```
                    Type-7 AS External Link States (Area 1)

        Link ID         ADV Router      Age         Seq#        Checksum Tag
        8.31.1.1        8.31.200.1      1256        0x80000003 0x00693E 0

                    Type-5 AS External Link States

        Link ID         ADV Router      Age         Seq#        Checksum Tag
        8.31.1.1        8.31.20.1       1240        0x80000001 0x002F1B 0

        c7600> show ip route

        Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
               D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
               N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
               E1 - OSPF external type 1, E2 - OSPF external type 2
               i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
               ia - IS-IS inter area, * - candidate default, U - per-user static route
               o - ODR, P - periodic downloaded static route

             8.0.0.0/32 is subnetted, 2 subnets
        O N2    8.31.1.1 [110/20] via 10.1.2.2, 00:20:45, GigabitEthernet0/2
                         [110/20] via 10.1.1.2, 00:20:45, GigabitEthernet0/1
        O       8.31.200.1 [110/11] via 10.1.2.2, 00:20:45, GigabitEthernet0/2
                           [110/11] via 10.1.1.2, 00:20:45, GigabitEthernet0/1
             10.0.0.0/24 is subnetted, 2 subnets
        C       10.1.1.0 is directly connected, GigabitEthernet0/1
        C       10.1.2.0 is directly connected, GigabitEthernet0/2
             26.0.0.0/24 is subnetted, 1 subnets
        C       26.1.1.0 is directly connected, GigabitEthernet0/3
```

Configuring Interfaces for VQE-S Traffic (Ingest and Services) and VQE-S Services Traffic

The service provider can choose one of the following approaches when configuring the CDE interfaces:

- **Dedicated Interfaces** —If a VQE deployment requires that the Ethernet interfaces or bond interfaces used for VQE-S ingest traffic from upstream video sources be separate from the interfaces used for VQE-S services traffic to the downstream VQE Clients (VQE-Cs) on the set-top boxes (STBs), the CDE Ethernet interfaces or bond interfaces must be configured as follows:

  - One or more interfaces are configured as dedicated interfaces for VQE-S ingest traffic.

  - One or more interfaces are configured as dedicated interfaces for VQE-S services traffic.

  See the Configuring Dedicated Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic section.

- **Shared Interfaces—**If a VQE deployment does not require that the Ethernet interfaces or bond interfaces used for VQE-S ingest traffic be separate from the interfaces used for VQE-S services traffic, a single set of CDE Ethernet interfaces or one or more bond interfaces are configured as VQE-S traffic interfaces that handle both types of traffic. See the Configuring Shared Interfaces for All VQE-S Traffic section.

Configuring Dedicated Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic

On the VQE-S host, the vqe.vqes.vqe_ingest_interfaces and vqe.vqes.vqe_services_interfaces parameters in the /etc/vqes/vcdb.conf file allow you to specify the Ethernet interfaces or bond interfaces that are available, respectively, for VQE-S ingest traffic (incoming multicast streams) and for VQE-S services (Unicast Retransmission and RCC traffic). You manually edit the vcdb.conf file and specify the Ethernet interfaces or bond interfaces that are used.

> **Note** For information on the restrictions that apply to the vqe.vqes.vqe_ingest_interfaces and vqe.vqes.vqe_services_interfaces parameters, see the "Interfaces for VQE-S Ingest Traffic (VQE-S Host Only)" section on page 2-29.

For the configuration examples in this section, Figure D-4 shows the IP addresses for interfaces eth1, eth2, bond1 (with eth3 and eth4 as its members), and the corresponding interfaces on the edge router.

Figure D-4   IP Addresses for VQE-S Configuration Examples
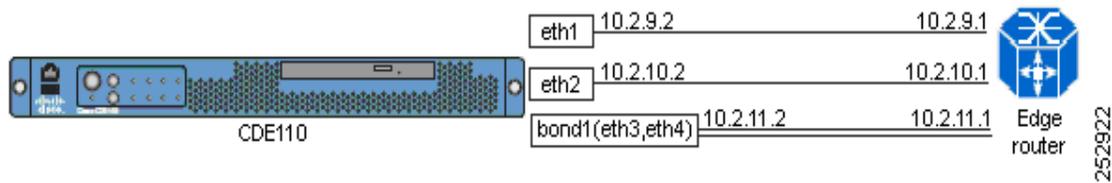
On the Cisco CDE that hosts VQE-S, to configure dedicated interfaces that are used for VQE-S ingest traffic and for VQE-S services traffic, follow these steps:

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

> **Note** If your deployment uses one dedicated interface for a management network, be sure not to include that interface as one of the interfaces that are available for VQE-S ingest or services traffic.

For this example, assume that the implementation uses eth1 for management network traffic only. Therefore, eth1 is not included in the set of interfaces that are available for VQE-S ingest or services traffic.

Step 2 Edit the /etc/opt/vqes/vcdb.conf file. Add the vqe.vqes.vqe_ingest_interfaces parameter to the file and specify the required values using the following format:

vqe.vqes.vqe_ingest_interfaces="*ethernet-interface-name, ethernet-interface-name"* or

vqe.vqes.vqe_ingest_interfaces="*bond-interface-name, bond-interface-name"*

For example:

```
vqe.vqes.vqe_ingest_interfaces="eth2"
```

✎
Note For load balancing to work effectively, each interface to the access or distribution network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot not be specified in this parameter.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 7-14.

Step 3 Add the vqe.vqes.vqe_services_interfaces parameter to the file and specify the required values using the following format:

vqe.vqes.vqe_ingest_interfaces="*ethernet-interface-name, ethernet-interface-name"* or

vqe.vqes.vqe_ingest_interfaces="*bond-interface-name, bond-interface-name"*

For example:

```
vqe.vqes.vqe_services_interfaces="bond1"
```

Step 4 If vqe.vqes.vqe_interfaces parameter is present in the vcdb.conf file, delete the line containing that parameter.

Step 5 Save the vcdb.conf file.

✎
Note VCDB configurations are applied to the CDE when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-28. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

Configuring Shared Interfaces for All VQE-S Traffic

On the VQE-S host, the vqe.vqes.vqe_interfaces parameter in the /etc/vqes/vcdb.conf file allows you to specify the Ethernet interfaces or bond interfaces that are available for VQE-S traffic (ingest and services). You manually edit the vcdb.conf file and specify the Ethernet interfaces or bond interfaces that are used.

For the configuration examples in this section, Figure D-5 shows the IP addresses for interfaces eth1, eth2, eth3, and eth4 and the corresponding interfaces on the edge router.

Figure D-5   IP Addresses for VQE-S Configuration Examples
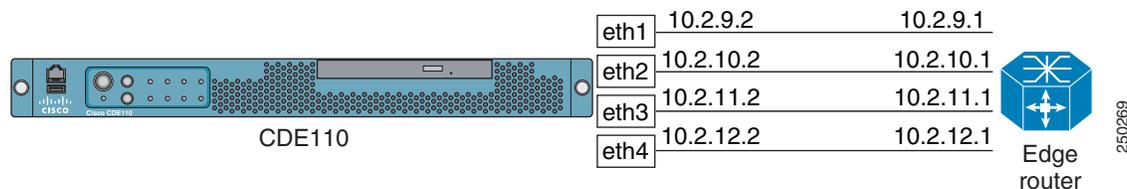
On the Cisco CDE that hosts VQE-S, to configure shared interfaces to handle both VQE-S ingest traffic and VQE-S services traffic, follow these steps:

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

> **Note**   If your deployment uses one dedicated interface for a management network, be sure *not to include* that interface as one of the interfaces that are available for VQE-S ingest and services traffic.
>
> For this example, assume that the implementation uses eth1 for management network traffic. Therefore, eth1 is not included in the set of interfaces that are available for VQE-S ingest and services traffic.

Step 2   Edit the /etc/opt/vqes/vcdb.conf file. Add the vqe.vqes.vqe_interfaces parameter to the file and specify the needed values using the following format:

vqe.vqes.vqe_ingest_interfaces="*ethernet-interface-name, ethernet-interface-name"* or

vqe.vqes.vqe_ingest_interfaces="*bond-interface-name, bond-interface-name"*

For example:

```
vqe.vqes.vqe_interfaces="eth2,eth3,eth4"
```

> **Note**   For load balancing to work effectively, each interface to the access or distribution network must have the same capacity. Multiple bond interfaces should not be specified and a combination of Ethernet and bond interfaces cannot not be specified in this parameter.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 7-14.

Step 3   If vqe.vqes.vqe_ingest_interfaces or vqe.vqes.vqe_services_interfaces parameter is present in the vcdb.conf file, delete the lines containing those parameters.

Step 4   Save the vcdb.conf file.

> **Note**   VCDB configurations are applied to the CDE when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-28. Reboot once when all VCDB configuration tasks are completed.
>
> Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

Synchronizing the Time and Configuring Network Time Protocol

To keep system time correct and synchronized, we recommend that you use Network Time Protocol (NTP) on the VQE-S host. To synchronize the time and configure NTP, follow these steps:

Step 1   If needed, log in as root.

Step 2   To set the time zone, issue the **tzselect** command and follow the prompts:

```
[root@system]# /usr/bin/tzselect To set the date and time, issue the date command as
follows:
    date -s "date_time_string"
```

For example:

```
[root@system]# date -s "16:55:30 July 7, 2008"
```

Step 3   Edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more system.ntp.server parameters and specifying the IP address of an external NTP server for each of the parameters. For example:

```
system.ntp.server="10.2.26.2"
```

In the preceding example, the IP address of the external NTP server is 10.2.26.2.

Step 4   Save the vcdb.conf file.

> **Note**   VCDB configurations are applied to the CDE when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-28. Reboot once when all VCDB configuration tasks are completed.
>
> Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

For information on starting the NTP service (ntpd daemon), see the "Starting VQE-S System Services and Verifying Status" section on page D-22.

VQE STUN Server Is Enabled By Default

Starting with Cisco VQE Release 3.0, the VQE STUN Server is enabled by default. The STUN Server allows STBs behind NAT devices to be supported by VQE-S. Unless you are sure that no STBs being serviced by VQE-S are behind NAT devices, we recommend that you leave the STUN Server enabled.

Configuring SNMP

The CDE that hosts the VQE-S uses Net-SNMP, a third-party product, for SNMP support for some basic, non-VQE system services. Net-SNMP offers a set of built-in MIBs for Linux platforms.

The VQE-S also provides a VQE-specific MIB and a system messages (Syslog) MIB. System messages that meet a specified severity level can be converted to SNMP traps and sent to a Network Management System (NMS). SNMP traps for indicating changes in a channel's state may also be generated. A channel up trap can be generated when a channel's state changes from inactive to active, and a channel down trap can be generated when a channel's state changes from active to to inactive. Generating syslog and channel traps is optional. For more information on the SNMP MIBs on the VQE-S, see Appendix B, "SNMP MIBs".

To configure SNMP on the Cisco CDE that hosts the VQE-S, follow these steps:

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

Step 2   Edit the /etc/opt/vqes/vcdb.conf file by adding the following VCDB parameters and specifying the needed values for each:

- system.snmp.ro_community_string="*community_string*"
- system.snmp.location="*server_location*"
- system.snmp.contact="*contact_person*"
- system_snmp_trap_listener="*listener_IP_or_host_name*"
- system.snmp.syslog_trap_enable="false"
- system.snmp.syslog_trap_priority="2"
- system.snmp.channel_trap_enable="false"

For more information on these SNMP-related VCDB parameters, see Table A-6 on page A-12.

The following example shows the four vcdb.conf lines that specify the SNMP parameters:

```
system.snmp.ro_community_string="XXYYZZ"
system.snmp.location="Building 6 San Francisco"
system.snmp.contact="Helen_Lee@company.com"
system_snmp_trap_listener="192.0.2.25"
system.snmp.syslog_trap_enable="true"
system.snmp.syslog_trap_priority="4"
system.snmp.channel_trap_enable="true"
```

Step 3   Save the vcdb.conf file.

Note   VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System and VQE-S Status section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS

In your IPTV deployment, VCPT (VCPT) or another channel-provisioning server sends channel information to the VQE-Ss. You must configure each CDE that hosts the VQE-S so that only trusted HTTPS clients (the channel-provisioning servers) can send the channel information to the CDE. If VCPT is the channel-provisioning server, the IP addresses of *all Ethernet interfaces* (that have been assigned IP addresses) on the VCPT host must be configured as trusted HTTPS clients on the VQE-S host. For more information on VCPT and how it sends channel information, see the "VCPT and Channel Information" section on page 1-15.

The system.iptables.trusted_provisioner parameter is for enhanced communications security beyond HTTPS. The VQE-S is configured so that only trusted HTTPS clients (as specified in system.iptables.trusted_provisioner) can send it information using HTTPS.

To allow only traffic from trusted HTTPS clients on the CDE port used for HTTPS, follow these steps:

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

Step 2   Edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more vqe.iptables.trusted_provisioner parameters and specifying the IP address of a trusted channel-provisioning server, such as VCPT. For example:

```
system.iptables.trusted_provisioner="10.86.17.200"
```

In the preceding example, `10.86.17.200` is the IP address of a trusted channel-provisioning server.

Step 3   Save the vcdb.conf file.

Note   VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System and VQE-S Status section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

Configuring Remote Syslog Servers

VQE system messages can be sent by means of UDP to remote servers for centralized logging. The use of remote syslog servers is optional. For more information on configuring remote syslog servers, see the "Remote Syslog Hosts" section on page 2-27.

To configure remote syslog servers on the Cisco CDE that hosts the VQE-S, follow these steps:

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

Step 2   Edit the /etc/opt/vqes/vcdb.conf file by adding the following VCDB parameter and specifying it's value:

- system.syslog.remote_server="*IP_address*"

For more information on the remote logging VCDB parameters, see Table A-6 on page A-12.

The following example shows the two vcdb.conf lines that specifies the remote logging parameter:

```
system.syslog.remote_server="192.0.7.25"
system.syslog.remote_server="192.0.7.26"
```

Step 3   Save the vcdb.conf file.

> ✎
> **Note**   VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System and VQE-S Status section. Reboot once when all VCDB configuration tasks are completed.
>
> Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

Starting VQE-S System Services and Verifying Status

Table D-1 lists the system services that you configure and start for the CDE that hosts the VQE-S. Use of the SNMP and NTP services are optional depending on your deployment requirements.

Table D-1   System Services for CDE That Hosts VQE-S

Service	Description
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.
snmpsa	(Optional) The Intel SNMP subagent.
vqes_snmpsa	(Optional) VQE-S SNMP subagent.
syslog_snmpsa	(Optional) Syslog SNMP subagent.
ntpd	(Optional) The NTP daemon.

Table D-1   System Services for CDE That Hosts VQE-S (continued)

Service	Description
check_daemons	A script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a **cron** job owned by root.
If OSPF Is Enabled for VQE-S traffic or VQE-S services interfaces	
watchquagga	The Quagga watchdog process. If a Quagga daemon crashes or hangs, watchquagga restarts it automatically.
ospfd	The OSPF daemon.
zebra	The zebra daemon.

To start the VQE-S system services and verify their status, follow these steps:

Note In the following procedure, abbreviated output is shown for some commands.

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

Step 2 To configure the system services to be managed by **chkconfig** and started automatically at run levels 2, 3, 4, and 5, and to start the services, issue the following commands:

```
[root@system]# chkconfig --add sshd
[root@system]# chkconfig sshd on
[root@system]# service sshd start

[root@system]# chkconfig --add httpd
[root@system]# chkconfig httpd on
[root@system]# service httpd start

[root@system]# chkconfig --add tomcat5
[root@system]# chkconfig tomcat5 on
[root@system]# service tomcat5 start
```

The following commands for the Quagga routing package and OSPF are optional depending on whether these services for Quagga and OSPF are used in your deployment:

```
[root@system]# chkconfig --add ospfd
[root@system]# chkconfig ospfd on
[root@system]# service ospfd start

[root@system]# chkconfig --add zebra
[root@system]# chkconfig zebra on
[root@system]# service zebra start

[root@system]# chkconfig --add watchquagga
[root@system]# chkconfig watchquagga on
[root@system]# service watchquagga start
```

The following commands for SNMP, SNMP subagents, and NTP are optional depending on whether these services are used in your deployment:

```
[root@system]# chkconfig --add snmpd
[root@system]# chkconfig snmpd on
[root@system]# service snmpd start

[root@system]# chkconfig --add snmpsa
```

```
[root@system]# chkconfig snmpsa on
[root@system]# service snmpsa start


[root@system]# chkconfig --add vqes_snmpsa
[root@system]# chkconfig vqes_snmpsa on
[root@system]# service vqes_snmpsa start

[root@system]# chkconfig --add syslog_snmpsa
[root@system]# chkconfig syslog_snmpsa on
[root@system]# service syslog_snmpsa start

[root@system]# chkconfig --add ntpd
[root@system]# chkconfig ntpd on
[root@system]# service ntpd start
```

Step 3   To configure the check_daemons script to run as a **cron** job under root, issue the following command:

```
[root@system]# /usr/bin/check_daemons >> /var/spool/cron/root
```

Step 4   To verify the sshd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep sshd

sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service sshd status

sshd (pid 2772) is running...

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

root      2772     1  0 Jul23 ?        00:00:00 /usr/sbin/sshd
```

Step 5   To verify the httpd run levels and that the services and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep httpd

httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service httpd status

httpd (2894) is running...

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

apache     447  2894  0 Jul23 ?        00:00:00 /usr/sbin/httpd
root      2894     1  0 Jul02 ?        00:00:00 /usr/sbin/httpd
apache   30078  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30079  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30080  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30082  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30083  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30084  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30085  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30087  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
```

Step 6   To verify the tomcat5 run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep tomcat5

tomcat5         0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

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

Tomcat is running...

[root@system]# ps -ef | grep tomcat5

root     19800     1  0 Jul23 ?        00:00:08 /usr/java/default/bin/java
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.util.logging.config.file=/usr/share/tomcat5/conf/logging.properties
-Djava.endorsed.dirs=/usr/share/tomcat5/common/endorsed -classpath
:/usr/share/tomcat5/bin/bootstrap.jar:/usr/share/tomcat5/bin/commons-logging-api.jar
-Dcatalina.base=/usr/share/tomcat5 -Dcatalina.home=/usr/share/tomcat5
-Djava.io.tmpdir=/usr/share/tomcat5/temp org.apache.catalina.startup.Bootstrap start
```

Step 7   If you have configured OSPF and started the ospfd service, to verify the ospfd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep ospfd

ospfd          0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service ospfd status

ospfd (pid 6173) is running...

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

quagga    6173     1  0 Sep22 ?        00:00:07 /usr/sbin/ospfd -d -A 127.0.0.1 -f
/etc/quagga/ospfd.conf
```

Step 8   If you have configured OSPF and started the zebra service, to verify the zebra run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep zebra

zebra          0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service zebra status

zebra (pid 6139) is running...

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

quagga    6139     1  0 Sep22 ?        00:00:00 /usr/sbin/zebra -d -A 127.0.0.1 -f
/etc/quagga/zebra.conf
```

Step 9   If you have configured OSPF and started the watchquagga service, to verify the watchquagga run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep watchquagga

watchquagga    0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service watchquagga status

watchquagga (pid 2513) is running...

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

root      2513     1  0 Sep15 ?        00:00:00 /usr/sbin/watchquagga -Az -d -b_
-r/sbin/service_%s_restart -s/sbin/service_%s_start -k/sbin/service_%s_stop zebra ospfd
```

Step 10 If you have configured and started the SNMP service, to verify the snmpd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep snmpd

snmpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service snmpd status

snmpd (pid 17654) is running...

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

root     17654    1  0 Jul25 ?        00:09:24 /usr/sbin/snmpd -Lsd -Lf /dev/null -p
/var/run/snmpd.pid -a
```

Step 11 If you have configured and started the SNMP Intel subagent service, to verify the snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep snmpsa

snmpsa          0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service snmpsa status

The SNMP subagent is running.

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

root     17678    1  0 Jul25 ttyS1    00:09:14 /usr/local/snmpsa/bin/smSubagent
```

Step 12 If you have configured and started the VQE-S SNMP subagent service, to verify the vqes_snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep vqes_snmpsa

vqes_snmpsa        0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service vqes_snmpsa status

vqes_subagent (pid 28603) is running...

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

root     17878 17956  0 09:16 pts/3 00:00:00 grep vqes_snmpsa
```

Step 13 If you have configured and started the Syslog SNMP subagent service, to verify the syslog_snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep syslog_snmpsa

syslog_snmpsa        0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service syslog_snmpsa status

syslog_subagent (pid 9886) is running...

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

root     17984 17946  0 09:16 pts/2    00:00:00 grep syslog_snmpsa
```

Step 14   If you have configured and started the NTP service, to verify that the ntpd service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep ntpd

ntpd            0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service ntpd status

ntpd (pid 17219) is running...

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

ntp      17219    1  0 Jul25 ?        00:00:06 ntpd -u ntp:ntp -p /var/run/ntpd.pid -g
```

Starting the VQE-S Processes and Verifying Status

To start the VQE-S service and processes and verify status, follow these steps:

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

Step 2   To configure the VQE-S service to be managed by **chkconfig** and started automatically at run levels 2, 3, 4, and 5, and to start the service, issue the following commands:

```
[root@system]# chkconfig --add vqes
[root@system]# chkconfig vqes on
[root@system]# service vqes start
```

> **Note**   System error messages are displayed indicating that the VQE-S processes are starting without a channel configuration file. This is normal behavior because a channel configuration file from the VCPT has not yet been sent to the VQE-S. Creating and sending the file is done when the Cisco CDE that hosts VCPT is configured, and VCPT is used to create and send the file.

Step 3   To verify that the VQE-S service is running, issue the following command:

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

process_monitor (pid 15189) is running...
```

Step 4   To check that the VQE-S processes are running, issue the following commands:

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

root      2965     1  0 09:17 pts/0    00:00:00 /opt/vqes/bin/process_monitor
vqes      2978  2965  0 09:17 pts/0    00:00:00 stun_server --ss-uid 499 --ss-gid 499
--xmlrpc-port 8054 --dscp -1 --log-level 6
root      3007  2965 99 09:17 pts/0    09:25:31 vqes_dp --group vqes --max-channels 500
--max-outstanding-rpcs 100 --max-pkts 1000000 --log-level 6 --rtp-inactivity-tmo 300
--max-core-bw 1100000000 --reserved-core-rcv-bw 300000000 --reserved-core-er-bw 200000000
--reserved-er-bw 543200000 --max-rai-gap 15
vqes      3061  2965  7 09:17 pts/0    00:13:56 vqes_cp --cp-uid 499 --cp-gid 499
--xmlrpc-port 8051 --cfg /etc/opt/vqes/vqe_channels.cfg --er-cache-time 3000
--rtp-hold-time 20 --max-channels 500 --max-outstanding-rpcs 100 --max-queued-rpcs 1000
--max-reserved-rpcs 32000 --max-clients 32000 --exporter-enable --vqm-host 10.86.21.4
--vqm-port 8192 --reserved-er-bw 543200000 --er-pkt-tb-rate 50000 --er-pkt-tb-depth 100
--er-blp-tb-rate 10000 --er-blp-tb-depth 100 --client-er-policing
```

```
--client-er-tb-rate-ratio 5 --client-er-tb-depth 10000 --log-level 6 --rcc-mode
conservative --igmp-join-variability 100 --max-client-bw 0 --max-idr-penalty 0
--rap-interval 2000 --excess-bw-fraction 20 --buff-size-preroll-max 1500
--rcc-burst-delay-to-send 10 --rtp-dscp 0 --rtp-rcc-dscp -1 --rtcp-dscp 24 --overlap-loss
0 --intf-output-allocation 90 --max-rpr-stream-burst-msecs 30 --max-rpr-stream-burst-pkts
2 --unity-e-factor-interval 5 --min-client-excess-bw-fraction 0
--max-client-excess-bw-fraction

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

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

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

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

Step 5   To use the VQE-S AMT from a web browser, enter as the URL the IP address of the Cisco CDE that hosts the VQE-S:

```
https://ip_address_of_VQES_host
```

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

If you click **System** in the left pane, the VQE-S AMT displays information on the VQE-S processes. Figure 4-2 shows an example.

Restarting the System and Verifying System and VQE-S Status

To restart the Cisco CDE and verify system and the VQE-S status, follow these steps:

✎
Note   The output for the commands issued in this section has been omitted. For example output, see the previous sections in this chapter where the same commands were issued.

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

Step 2   To restart the system, issue the following command:

```
[root@system]# reboot
```

The operating system boots.

✎
Note   Syslog error messages are displayed indicating that the VQE-S processes are starting without a channel configuration file. This is normal behavior because a channel configuration file from the VCPT has not yet been sent to the VQE-S. Creating and sending the file is done when the Cisco CDE that hosts VCPT is configured, and VCPT is used to create and send the file.

Step 3   Log in as root.

Step 4   To verify that interfaces eth1 to eth6 are up and running and the IP address and netmask for each are set correctly, issue the following command:

```
[root@system]# ifconfig -a

... Output omitted
```

Step 5   To check that the vqes service is running, issue the following command:

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

... Output omitted
```

Step 6   To check that the STUN Server process is running, issue the following command:

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

... Output omitted
```

Step 7   To verify that the sshd service is running, issue the following command:

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

... Output omitted
```

Step 8   To verify that the httpd service is running, issue the following command:

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

... Output omitted
```

Step 9   To verify that the tomcat5 service is running, issue the following command:

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

... Output omitted
```

Step 10   If you have configured OSPF, to verify the ospfd service is running, issue the following command:

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

... Output omitted
```

Step 11   If you have configured OSPF, to verify the zebra service is running, issue the following command:

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

... Output omitted
```

Step 12   If you have configured OSPF, to verify the watchquagga service is running, issue the following command:

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

... Output omitted
```

Step 13   If you have configured SNMP, to verify that the snmpd service is running, issue the following command:

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

... Output omitted
```

Step 14   If you have configured SNMP, to verify that the Intel snmpsa service is running, issue the following command:

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

... Output omitted
```

Step 15 If you configured SNMP, to verify that the VQE-S subagent service is running, issue the following command:

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

... Output omitted
```

Step 16 If you configured SNMP, to verify that the Syslog subagent service is running, issue the following command:

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

... Output omitted
```

Step 17 If you have configured an external NTP server, to verify that the ntpd service is running, issue the following command:

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

... Output omitted
```

Step 18 Do one of the following:

- If the preceding checks indicate that all is well, proceed to the Setting Up a Cisco CDE That Hosts VQE Tools section.

- If one of the preceding checks fails, inspect the configuration of the item that failed and make any needed adjustments.

Setting Up a Cisco CDE That Hosts VQE Tools

This section explains how to perform the initial configuration tasks for a Cisco CDE hosting VQE Tools (VCPT, VCDS, and VCDS AMT).

When performed manually, the initial configuration tasks involve editing the /etc/opt/vqes/vcdb.conf file to configure the essential VCDB parameters. The use of the vcdb.conf file simplifies the configuration tasks. Because the VQE Configuration Tool automatically applies the VCDB values to the /etc configuration files on system reboot, mistakes in configuration file syntax are unlikely.

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 7-14.

Perform these initial configuration tasks in the order shown:

1. Prerequisites for a Cisco CDE That Hosts VQE Tools, page D-31

2. Configuring the Linux Operating System for VQE Tools, page D-31

3. Configuring a Static Route for a Management Network (VQE Tools Host), page D-34

4. Synchronizing the Time and Configuring Network Time Protocol, page D-36

5. Configuring SNMP, page D-37

6. Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS, page D-38

7. Configuring Remote Syslog Servers, page D-39

8. Starting VQE Tools System Services and Verifying Status, page D-39

9. Starting the VCDS Service and Verifying VCDS, VCDS AMT and VCPT Status, page D-43

10. Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status, page D-44

On the VQE Tools server, proper route configuration is needed for external access to the VQE Tools server. You can use the static static route explained in the "Configuring a Static Route for a Management Network (VQE Tools Host)" section on page D-34 to configure this access.

Note   The configuration instructions in this section are intended for new installations of Cisco VQE Release 3.6 software, where the Cisco CDE has the Cisco VQE Release 3.6 software preinstalled.

For information on *upgrading an already configured* Cisco CDE, see the *Release Notes for Cisco CDA Visual Quality Experience, Release 3.6*.

Prerequisites for a Cisco CDE That Hosts VQE Tools

This section explains tasks that should be performed before setting up a Cisco CDE that hosts VQE Tools.

Connecting Cables

For information on connecting cables on the VQE Tools server, see the "Connecting Cables to the CDE" section on page 2-4.

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

Setting Up SSL Certificates for VCPT

It is recommended that you deploy your own or commercial Secure Sockets Layer (SSL) certificates before beginning the tasks for setting up a Cisco CDE that hosts VCPT. For information on setting up the certificates, see the "Setting Up SSL Certificates" section on page 2-5.

Configuring the Linux Operating System for VQE Tools

This section explains the initial Linux configuration tasks needed for a Cisco CDE appliance that runs the VQE Tools (VCPT and VCDS) software. The explanation assumes that the needed software for Linux, VCPT, and VCDS have been preinstalled on the Cisco CDE appliance. For Red Hat Linux 5.1 documentation, go to the following :

http://www.redhat.com/docs/manuals/enterprise/

For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE back panel are specified as eth1 to eth6 as shown in Figure D-6.

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

Figure D-6   NIC Port Numbering for Software Configuration

eth3   eth2   eth6   eth5

eth4   eth1
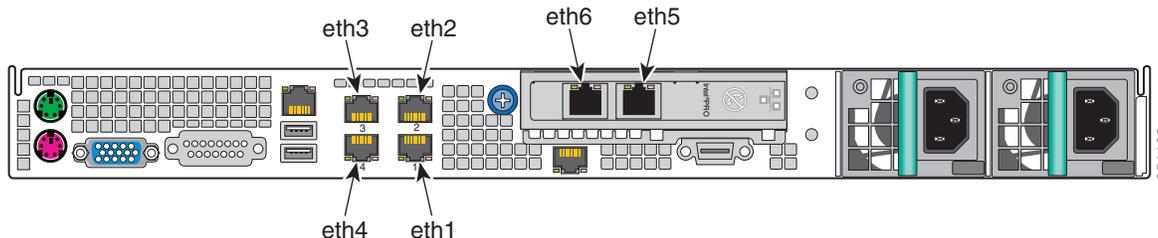
For the configuration examples in this section, Figure D-7 shows the IP addresses for interface eth1 and the corresponding interface on the edge router.

Figure D-7   IP Addresses for VQE Tools Configuration Examples

eth1 10.2.15.2   10.2.15.1

eth2

eth3

eth4

CDE110

Edge router
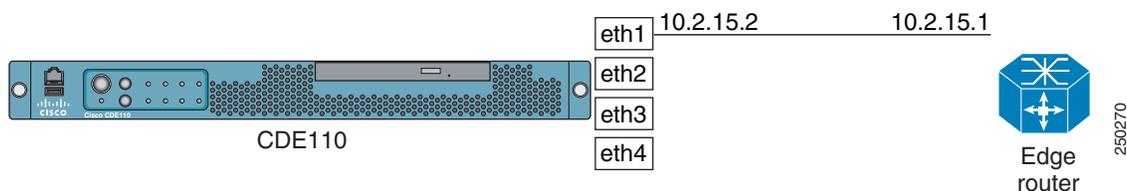
Note   The configuration examples in this section assume that one CDE Ethernet interface (eth1) are used to connect to the VQE network.

To configure the Linux operating system and other software for the VQE Tools (VCPT and VCDS), follow these steps:

Step 1   If needed, login as root. You must have root privileges to modify the vcdb.conf file.

Step 2   To create the password for the vqe username (a pre-created Linux user ID), issue the following command:

```
[root@system]# passwd vqe
```

Enter a password that follows the password guidelines:

```
A valid password should be a mix of upper and lower case letters,
digits, and other characters.  You can use an 8 character long
password with characters from at least 3 of these 4 classes, or
a 7 character long password containing characters from all the
classes.  An upper case letter that begins the password and a
digit that ends it do not count towards the number of character
classes used.

A passphrase should be of at least 3 words, 12 to 40 characters
long and contain enough different characters.
```

This username and password can be used to log in to Linux directly using SSH. The vqe username and password can also be used log in to the VCPT.

Step 3   To configure CDE Ethernet interfaces eth1 to eth6, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.*ethx*.addr parameters, where *ethx* is eth1, eth2, and so on. Specify an IP address and prefix length for each interface. The following example shows one vcdb.conf line for the eth1 Ethernet interface:

```
network.eth1.addr="10.2.15.2/24"
```

Step 4   To configure the hostname for the CDE server, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the system.global.hostname parameter and specifying a hostname. The following example specifies the hostname as starfire1-iptv:

```
system.global.hostname="starfire1-iptv"
```

Step 5   To configure a DNS server, edit the /etc/opt/vqes/vcdb.conf file by adding the VCDB parameters for the IP address and optionally for the search domain of a DNS server and specifying the needed values:

- system.dns.server="*IP_address*"

- system.dns.search_domain="*search_domain*"

For example:

```
system.dns.server="192.0.20.53."
system.dns.search_domain="domain.com"
```

Step 6   Save the vcdb.conf file.

✎
Note   VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

After the VQE Tools host is rebooted, you can verify that the eth1 interface is configured correctly and up and running.

- Use the **ifconfig** *interface* command to verify that the Ethernet interface is up and running and the IP address and netmask is set correctly. The following example is for eth1:

```
[root@system]# ifconfig eth1

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:C6:F3:0F
          inet addr:10.2.15.2  Bcast:10.2.15.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fec6:f30f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:192 (192.0 b)  TX bytes:2700 (2.6 KiB)
          Base address:0x3000 Memory:b8800000-b8820000
```

- Use the **ip link show eth#** command (where **#** is the Ethernet interface number) to check that the link is up. For example:

```
[root@system]# ip link show eth1

eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0e:0c:c6:e4:fe brd ff:ff:ff:ff:ff:ff
```

- Use the **ping** command to check that the Cisco CDE can reach the connected edge router. For example:

```
[root@system]# ping 10.2.15.1
```

Configuring a Static Route for a Management Network (VQE Tools Host)

If your deployment makes use of a management network, a static route for the management network can be configured using the VCDB parameter network.route.static_route. The configuration example in this section assumes that one CDE Ethernet interface (eth1) is used to connect to the VQE network.

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

To configure a static route for a management network, follow these steps:

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

Step 2   Edit the /etc/opt/vqes/vcdb.conf file by adding to the file a network.network.interface.mgmt_interfaces parameter and specifying the needed values using the following format:

network.network.interface.mgmt_interfaces="*ethernet-interface-name, ethernet-interface-name*"

The *ethernet-interface-name* arguments are names of the interfaces designated for management traffic. One or more CDE Ethernet interfaces may be designated for management traffic. For this example, assume CDE Ethernet interface eth1(10.2.9.2) on the VQE Tools host is designated for management traffic.

The line in the vcdb.conf file is as follows:

```
network.network.mgmt_interfaces="eth1"
```

Step 3   Edit the /etc/opt/vqes/vcdb.conf file by adding to the file a network.route.static_route parameter and specifying the needed values using the following format:

network.route.static_route="*target-network-subnet-addr/prefix-length via gateway-addr:outbound-interface*"

The *target-network-subnet-addr/prefix-length* is the IP address and prefix length for the management network. The *gateway-addr* is the IP address of the router interface that is directly attached to the CDE Ethernet port that is used for management network traffic. The *outbound-interface* is the interface used on the VQE Tools server for this static route

For this example, assume the following:

- CDE Ethernet interface eth1 (10.2.15.2) is used for the management network.

- Management network is 192.0.0.0/8.

The line in the vcdb.conf file is as follows:

```
network.route.static_route="192.0.0.0/8 via 10.2.15.1"
```

In the preceding example, 10.2.15.1 is the *gateway-addr*—the router interface that is directly attached to eth1. Figure D-7 shows the IP addresses used in this example for the eth1 interface and the directly attached router.

Step 4   Save the vcdb.conf file.

Note VCDB configurations are applied to the CDE when it is rebooted in the "Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status" section on page D-44. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

After the VQE Tools host is rebooted, you can verify that the static route for the management network is present in the routing table by issuing the following command:

```
[root@system]# ip route show
```

The output is similar to the following:

```
192.0.0.0/8 via 10.2.9.1 dev eth1
```

Synchronizing the Time and Configuring Network Time Protocol

To keep system time correct and synchronized, we recommend that you use Network Time Protocol (NTP) on the VQE Tools host. To synchronize the time and configure NTP, follow these steps:

Step 1   If needed, log in as root on the CDE that hosts VQE Tools.

Step 2   To set the time zone, issue the **tzselect** command and follow the prompts:

```
[root@system]# /usr/bin/tzselect
```

Step 3   To set the date and time, issue the **date** command as follows:

   date -s "*date_time_string*"

For example:

```
[root@system]# date -s "16:55:30 July 7, 2008"
```

Step 4   Edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more system.ntp.server parameters and specifying the IP address of an external NTP server for each of the parameters. For example:

```
system.ntp.server="10.2.26.2"
```

In the preceding example, the IP address of the external NTP server is 10.2.26.2.

Step 5   Save the vcdb.conf file.

✎
Note   VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

For information on starting the NTP service (ntpd daemon), see the Starting VQE Tools System Services and Verifying Status section.

Configuring SNMP

The CDE that hosts the VQE Tools sever uses Net-SNMP, a third-party product, for SNMP support for some basic, non-VQE system services. Net-SNMP offers a set of built-in MIBs for Linux platforms.

The VQE Tools server also provides a VQE-specific MIB and a system messages (Syslog) MIB. System messages that meet a specified severity level can be sent as SNMP traps to a NMS. Sending syslog traps is optional. For more information on the SNMP MIBs, see Appendix B, "SNMP MIBs".

To configure SNMP on the Cisco CDE that hosts VQE Tools, follow these steps:

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

Step 2   Edit the /etc/opt/vqes/vcdb.conf file by adding the following VCDB parameters and specifying the needed values for each:

- system.snmp.ro_community_string="*community_string*"
- system.snmp.location="*server_location*"
- system.snmp.contact="*contact_person*"
- system_snmp_trap_listener="*listener_IP_or_host_name*"
- system.snmp.syslog_trap_enable="false"
- system.snmp.syslog_trap_priority="2"

For more information on these SNMP-related VCDB parameters, see Table A-6 on page A-12.

The following example shows the four vcdb.conf lines that specify the SNMP parameters:

```
system.snmp.ro_community_string="XXYYZZ"
system.snmp.location="Building 6 San Francisco"
system.snmp.contact="Helen_Lee@company.com"
system_snmp_trap_listener="192.0.2.25"
system.snmp.syslog_trap_enable="true"
system.snmp.syslog_trap_priority="4"
```

Step 3   Save the vcdb.conf file.

Note   VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status, page D-44 section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS

The system.iptables.trusted_provisioner parameter must be configured for both of the following:

- For a VQE Tools host where a VCDS receives channel information from VCPT, *all Ethernet interfaces* (that have been assigned IP addresses) on the VCPT host sending the channel information must be specified as addresses using the system.iptables.trusted_provisioner parameter. This requirement applies even when the VCDS is in the same VQE Tools server as the VCPT.

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

The system.iptables.trusted_provisioner parameter is for HTTPS communications security. The VQE Tools server is configured so that only trusted HTTPS clients (as specified in system.iptables.trusted_provisioner) can send it information using HTTPS.

To allow only traffic from trusted HTTPS clients on the CDE port used for HTTPS, follow these steps:

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

Step 2 Edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more vqe.iptables.trusted_provisioner parameters and specifying the IP addresses as explained in the preceding discussion. For example, when VCPT send channel information to one of more VCDS's, you specify the IP addresses of *all Ethernet interfaces* that has been assigned an IP address on the VQE Tools host.

```
system.iptables.trusted_provisioner="10.2.15.2"
```

In the preceding example, `10.2.15.2` is the IP address of the only Ethernet interface that has been assigned an IP address on the VQE Tools host.

Step 3 Save the vcdb.conf file.

![Note icon]

Note VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System and VQE-S Status section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

Configuring Remote Syslog Servers

VQE system messages can be sent by means of UDP to remote servers for centralized logging. The use of remote syslog servers is optional. For more information on configuring remote syslog servers, see the"Remote Syslog Hosts" section on page 27.

To configure remote syslog servers on the Cisco CDE that hosts VQE Tools, follow these steps:

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

Step 2   Edit the /etc/opt/vqes/vcdb.conf file by adding the following VCDB parameter and specifying it's value:

- system.syslog.remote_server="*IP_address*"

For more information on the remote logging VCDB parameters, see Table A-6 on page A-12.

The following example shows the two vcdb.conf lines that specifies the remote logging parameter:

```
system.syslog.remote_server="192.0.7.25"
system.syslog.remote_server="192.0.7.26"
```

Step 3   Save the vcdb.conf file.

Note   VCDB configurations are applied to the CDE when it is rebooted in the Restarting the System and Verifying System and VQE-S Status section. Reboot once when all VCDB configuration tasks are completed.

Alternatively, to avoid a reboot of the system, you can use the **vqe_cfgtool** command with the **-apply** option to restart only the required services. For more information on the **-apply** option, see the "Using the VQE Configuration Tool Command-Line Options" section on page 7-18.

Starting VQE Tools System Services and Verifying Status

Table D-2 lists the system services that you configure and start, for the CDE that hosts VQE Tools. Use of the SNMP and NTP services are optional depending on your deployment's requirements.

Table D-2   System Services for CDE That Hosts VQE Tools

Service	Description
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.
vcds_snmpsa	VCDS SNMP subagent
syslog_snmpsa	Syslog SNMP subagent.
snmpsa	(Optional) The SNMP subagent.

Table D-2   System Services for CDE 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.

To start the VQE Tools system services and verify their status, follow these steps:

Note In the following procedure, abbreviated output is shown for some commands.

Step 1 If needed, log in as root on the CDE that hosts VQE Tools.

Step 2 To configure the system services to be managed by **chkconfig** and started automatically at run levels 2, 3, 4, and 5, and to start the services, issue the following commands:

```
[root@system]# chkconfig --add sshd
[root@system]# chkconfig sshd on
[root@system]# service sshd start

[root@system]# chkconfig --add httpd
[root@system]# chkconfig httpd on
[root@system]# service httpd start

[root@system]# chkconfig --add tomcat5
[root@system]# chkconfig tomcat5 on
[root@system]# service tomcat5 start
```

The following commands for SNMP and NTP are optional depending on whether these services are used in your deployment:

```
[root@system]# chkconfig --add snmpd
[root@system]# chkconfig snmpd on
[root@system]# service snmpd start

[root@system]# chkconfig --add snmpsa
[root@system]# chkconfig snmpsa on
[root@system]# service snmpsa start

[root@system]# chkconfig --add vcds_snmpsa
[root@system]# chkconfig vcds_snmpsa on
[root@system]# service vcds_snmpsa start

[root@system]# chkconfig --add syslog_snmpsa
[root@system]# chkconfig syslog_snmpsa on
[root@system]# service syslog_snmpsa start

[root@system]# chkconfig --add ntpd
[root@system]# chkconfig ntpd on
[root@system]# service ntpd start
```

Step 3 To configure the check_daemons script to run as a **cron** job under root, issue the following command:

```
[root@system]# /usr/bin/check_daemons >> /var/spool/cron/root
```

Step 4 To verify the sshd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep sshd
```

```
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service sshd status

sshd (pid 2772) is running...

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

root     2772     1  0 Jul23 ?        00:00:00 /usr/sbin/sshd
```

Step 5   To verify the httpd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep httpd

httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service httpd status

httpd (2894) is running...

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

apache     447  2894  0 Jul23 ?        00:00:00 /usr/sbin/httpd
root      2894     1  0 Jul02 ?        00:00:00 /usr/sbin/httpd
apache   30078  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30079  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30080  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30082  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30083  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30084  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30085  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
apache   30087  2894  0 Jul19 ?        00:00:00 /usr/sbin/httpd
```

Step 6   To verify the tomcat5 run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep tomcat5

tomcat5         0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service tomcat5 status

Tomcat is running...

[root@system]# ps -ef | grep tomcat5

root     19800     1  0 Jul23 ?        00:00:08 /usr/java/default/bin/java
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.util.logging.config.file=/usr/share/tomcat5/conf/logging.properties
-Djava.endorsed.dirs=/usr/share/tomcat5/common/endorsed -classpath
:/usr/share/tomcat5/bin/bootstrap.jar:/usr/share/tomcat5/bin/commons-logging-api.jar
-Dcatalina.base=/usr/share/tomcat5 -Dcatalina.home=/usr/share/tomcat5
-Djava.io.tmpdir=/usr/share/tomcat5/temp org.apache.catalina.startup.Bootstrap start
```

Step 7   If you have configured and started the SNMP daemon, to verify the snmpd run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep snmpd

snmpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off

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

```
snmpd (pid 17654) is running...

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

root     17654    1  0 Jul25 ?        00:09:24 /usr/sbin/snmpd -Lsd -Lf /dev/null -p
/var/run/snmpd.pid -a
```

Step 8   If you have configured and started the Intel SNMP subagent, to verify the snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep snmpsa

snmpsa          0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service snmpsa status

The SNMP subagent is running.

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

root     17678    1  0 Jul25 ttyS1   00:09:14 /usr/local/snmpsa/bin/smSubagent
```

Step 9   If you have configured and started the VCDS SNMP subagent, to verify the vcds_snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep vcds_snmpsa

vcds_snmpsa         0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service vcds_snmpsa status

vcds_subagent (pid 10088) is running...

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

root     17273 17182  0 08:54 pts/2   00:00:00 grep vcds_snmpsa
```

Step 10   If you have configured and started the Syslog SNMP subagent, to verify the syslog_snmpsa run levels and that the service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep syslog_snmpsa

syslog_snmpsa       0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service syslog_snmpsa status

syslog_subagent (pid 9886) is running...

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

root     17984 17946  0 09:16 pts/2   00:00:00 grep syslog_snmpsa
```

Step 11   If you have configured and started the NTP service, to verify run levels and that the ntpd service and process are running, issue the following commands:

```
[root@system]# chkconfig --list | grep ntpd

ntpd            0:off   1:off   2:on    3:on    4:on    5:on    6:off

[root@system]# service ntpd status

ntpd (pid 17219) is running...

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

```
ntp       17219    1  0 Jul25 ?        00:00:06 ntpd -u ntp:ntp -p /var/run/ntpd.pid -g
```

Starting the VCDS Service and Verifying VCDS, VCDS AMT and VCPT Status

This section explains how to start the VCDS service and verify that the process is running and that VCPT and the VCDS AMT are available.

> **Note**   VCPT and VCDS AMT are web applications and have no dedicated processes associated with them. The processes needed for the VCPT and VCDS AMT web applications to work (for example, the web server) are started automatically when the Cisco CDE is started.

To start the VCDS service and verify VCDS, VCDS AMT, and VCPT status, follow these steps:

Step 1   If needed, log in as root on the CDE that hosts VQE Tools.

Step 2   To configure the VCDS service to be managed by **chkconfig** and started automatically at run levels 2, 3, 4, and 5, and to start the service, issue the following commands:

```
[root@system]# chkconfig --add vcds
[root@system]# chkconfig vcds on
[root@system]# service vcds start
```

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

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

VCDServer (pid 29860) is running...
```

Step 4   To check that the VCDS process (VCDServer) is running, issue the following command:

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

root     29860    1  0 Jul25 ?        00:00:00 /opt/vqes/bin/VCDServer
```

Step 5   To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE that hosts VCPT:

```
https://ip_address_of_VCPT_host
```

Log in using the vqe username and password. (Any valid Linux username and password can be used to log in to VCPT.)

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

Step 6   To use the VCDS AMT from a web browser, enter as the URL the IP address of the Cisco CDE that hosts VQE Tools server

```
https://ip_address_of_VQE_Tools_host/vcds-amt
```

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

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

Restarting the System and Verifying System, VCPT, VCDS AMT, and VCDS Status

To restart the Cisco CDE and verify system, VCPT, VCDS (VCDS), and VCDS AMT status, follow these steps:

> ✎
>
> **Note**   The output for the commands issued in this section has been omitted. For example output, see the previous sections in this chapter where the same commands were issued.

Step 1   If needed, log in as root on the CDE that hosts VQE Tools.

Step 2   To restart the system, issue the following command:

```
[root@system]# reboot
```

The operating system boots.

Step 3   To verify that interface eth1 is up and running and the IP address and netmask is set correctly, issue the following command:

```
[root@system]# ifconfig -a

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

Step 6   To verify that the tomcat5 service is running, issue the following command:

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

... Output omitted
```

Step 7   If you have configured SNMP, to verify that the snmpd service is running, issue the following command:

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

... Output omitted
```

Step 8   If you have configured SNMP, to verify that the Intel snmpsa service is running, issue the following command:

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

... Output omitted
```

Step 9   If you configured SNMP, to verify that the VCDS subagent service is running, issue the following command:

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

... Output omitted
```

Step 10   If you configured SNMP, to verify that the Syslog subagent service is running, issue the following command:

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

... Output omitted
```

Step 11   If you have configured an external NTP server, to verify that the ntpd service is running, issue the following command:

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

... Output omitted
```

Step 12   To check that the vcds service is running, issue the following command:

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

... Output omitted
```

Step 13   To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE that hosts VCPT:

```
https://ip_address_of_VQE_Tools_host
```

Log in with a Linux username and password.

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

Step 14   To that VCDS AMT from a web browser, enter as the URL the IP address of the Cisco CDE that hosts VQE Tools server

```
https://ip_address_of_VQE_Tools_host/vcds-amt
```

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

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

Step 15   Do one of the following:

- If the preceding checks indicate that all is well, you are ready to start using VCPT and VCDS AMT. For information on VCPT, see Chapter 3, "Using the VQE Channel Provisioning Tool." For information on VCDS AMT, see Chapter 5, "Using the VCDS AMT."

- If one of the preceding checks fails, inspect the configuration of the item that failed and make any needed adjustments.