APPENDIX D

Manual Initial VQE System Configuration

This appendix explains how to perform manual initial configuration on the two categories of CDE110 servers running the VQE software:

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

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

The alternative to manual configuration is to use the Cisco VQE Startup Configuration Utility. For information on using the utility, see the "VQE-S Server: Routing and Interface Configuration Overview" section on page 2-13.

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

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

The manual initial configuration procedures are explained in these sections:

Setting Up a Cisco CDE110 That Hosts VQE-S

This section explains how to perform the initial configuration tasks for a Cisco CDE110 hosting VQE-S.

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

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-13.

Perform these initial configuration tasks in the order shown:

1. Prerequisites for a Cisco CDE110 That Hosts VQE-S, page D-2
2. Configuring the Linux Operating System for VQE-S, page D-3
3. Configuring a Static Route for a Management Network (VQE-S Host), page D-5
4. Configuring Static Routes for VQE-S Traffic, page D-6
5. Configuring OSPF Routing for VQE-S Traffic, page D-8
6. Configuring Ethernet Interfaces for VQE-S Traffic, page D-13
7. Synchronizing the Time and Configuring Network Time Protocol, page D-15
8. VQE STUN Server Is Enabled By Default, page D-16
9. Configuring SNMP (Optional), page D-16
10. Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS, page D-16
11. Starting VQE-S System Services and Verifying Status, page D-17
12. Starting the VQE-S Processes and Verifying Status, page D-21
13. Restarting the System and Verifying System and VQE-S Status, page D-22

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

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

For information on configuring VQE-S RTCP Exporter, see the "Configuring VQE-S RTCP Exporter" section on page 2-34.

Prerequisites for a Cisco CDE110 That Hosts VQE-S

This section explains tasks that should be performed before setting up a Cisco CDE110 that hosts VQE-S.

Connecting Cables for VQE-S

For information on connecting cables on the VQE-S server, see the "Connecting Cables to the CDE110" section on page 2-3.

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

Setting Up SSL Certificates for VQE-S

It is recommended that you deploy your own Secure Sockets Layer (SSL) certificates or commercial SSL certificates prior to beginning the tasks for setting up a Cisco CDE110 that hosts VQE-S. For information on setting up the certificates, see the "Setting Up SSL Certificates" section on page 2-4.

Configuring the Linux Operating System for VQE-S

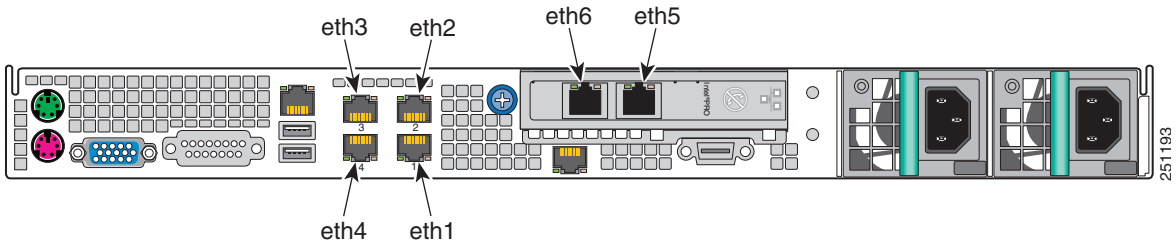
This section explains the initial Linux configuration tasks needed for a Cisco CDE110 appliance that will run VQE-S software. The explanation assumes that the needed software for Linux and VQE-S has been pre-installed on the Cisco CDE110 appliance. For Red Hat Enterprise Linux 5.1 documentation, go to the following web site:

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

For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE110 back panel are specified as eth1 to eth6 as shown in Figure D-1.

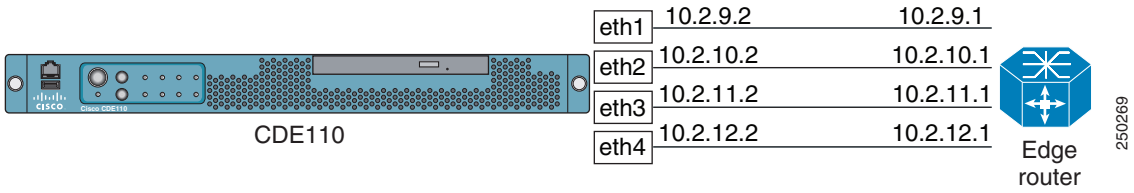
Note Earlier models of the CDE110 have four Ethernet ports (eth1 to eth4). These models did not have the Intel PRO/1000 PT Dual Port Server Adapter that provides the eth5 and eth6 ports.

Figure D-1 NIC Port Numbering for Software Configuration



For the configuration examples in this section, Figure D-2 shows the IP addresses for interfaces eth1, eth2, eth3, and eth4 and the corresponding interfaces on the edge router.

Figure D-2 IP Addresses for VQE-S Configuration Examples



To configure the Linux operating system and other software for VQE-S, follow these steps:

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

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

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

Enter a password that follows the password guidelines:

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

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

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

Step 3 To configure CDE110 Ethernet interfaces eth1 to eth6, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.eth*x*.addr parameters, where eth*x* is eth1, eth2, and so on. Specify an IP address and prefix length for each interface. The following example shows four vcdb.conf lines for the four Ethernet interfaces:

```
network.eth1.addr="10.2.9.2/24"
network.eth2.addr="10.2.10.2/24"
network.eth3.addr="10.2.11.2/24"
network.eth4.addr="10.2.12.2/24"
```

Step 4 To configure the hostname for the CDE110 server, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the system.global.hostname parameter and specifying a hostname. The following example specifies the hostname as starfire-iptv:

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

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

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

For example:

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

Step 6 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

After the VQE-S host is rebooted, you can verify that the eth1 to eth6 interfaces are configured correctly and up and running by issuing the following commands:

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

```
[root@system]# ifconfig eth1

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:C6:F3:0F
          inet addr:10.2.10.2  Bcast:10.2.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fec6:f30f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:192 (192.0 b)  TX bytes:2700 (2.6 KiB)
          Base address:0x3000 Memory:b8800000-b8820000
```

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

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

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

- Use the **ping** command to check that the Cisco CDE110 can reach the connected edge router. For example:

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

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

If your deployment makes use of a management network, a static route for the management network can be configured using the VCDB parameter network.route.mgmt_route. The configuration example in this section assumes that one CDE110 Ethernet interface will be used to connect to the VQE network.

When the VQE-S server uses a dedicated interface for ingest traffic for multicast streams, the network.route.mgmt_route parameter can be used to define a static route to the distribution network where video sources reside. For information on this use, see "Routing Configuration for Dedicated Interfaces and Shared Interfaces" section on page 2-16.

Note If you configure a static route for a management network as described in this section, see the "Static Route for a Management Network Is Missing on CDE110 Hosting VQE-S or VQE Tools" section on page 5-8 for some additional information.

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

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

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

network.route.mgmt_route="*management-network-addr/prefix-length* via *gateway-addr* "

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

For this example, assume the following:

- CDE110 Ethernet interface eth1 (10.2.9.2) will be used for the management network.
- The management network is 192.0.0.0/8.

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

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

In the preceding example, 10.2.9.1 is the *gateway-addr*—the router interface that is directly attached to eth1. Figure D-3 shows the IP addresses used in this example for the eth1 interface and the directly attached router.

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

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

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

The output will be similar to the following:

```
192.0.0.0/8 via 10.2.9.1 dev eth1
default
    nexthop via 10.2.10.1 dev eth2 weight 1
    nexthop via 10.2.11.1 dev eth3 weight 1
    nexthop via 10.2.12.1 dev eth4 weight 1
```

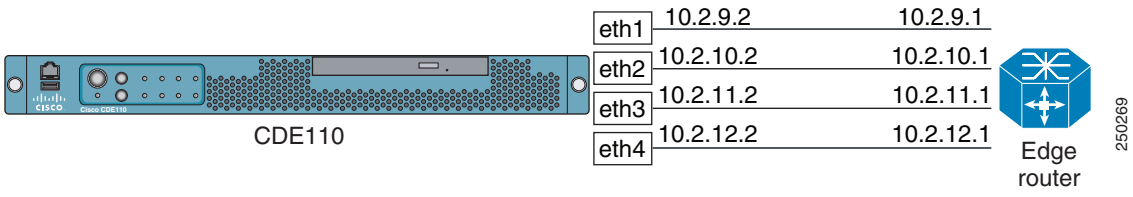
Configuring Static Routes for VQE-S Traffic

This section provides information on configuring static routes for VQE-S traffic on the CDE110 that hosts VQE-S.

Note For information on configuring static routes for feedback targets on the directly attached router, see the "For Static Routes: Guidance for Configuring Feedback Targets on the Attached Router" section on page 2-38.

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

Figure D-3 IP Addresses for VQE-S Configuration Examples



On the Cisco CDE110 that hosts VQE-S, multiple Ethernet interfaces are used for VQE-S traffic, including incoming multicast streams, outgoing Unicast Retransmissions and RCC unicast transmissions, and other VQE-S traffic. In addition, some VQE deployments may use one of the Ethernet ports as the interface to a management network.

If default gateway (next hop) route is configured for each CDE110 Ethernet interface that is available for VQE-S traffic, Equal Cost Multipath (ECMP) is used to load-balance VQE-S output traffic across the CDE110 interfaces that are directly attached to the gateway router interfaces specified in the network.route.default_gateway parameter.

Note A single default gateway should be configured for each interface used for VQE-S traffic. Otherwise, output load will not be balanced and some interfaces may be overloaded.

To configure a default gateway for one or more CDE110 Ethernet interfaces, follow these steps:

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

Step 2 To choose static routes for VQE-S traffic, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the network.route.type parameter and specifying the value static for the parameter:

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

Step 3 To configure default gateways for each Ethernet interface that is available for VQE-S traffic, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.route.default_gateway parameters and specifying values for each of the parameters. The following example shows four vcdb.conf lines that add default gateways for the four CDE110 Ethernet interfaces.

```
network.route.default_gateway=”10.2.9.1”
network.route.default_gateway=”10.2.10.1”
network.route.default_gateway=”10.2.11.1”
network.route.default_gateway=”10.2.12.1”
```

In the preceding example, 10.2.9.1, 10.2.10.1, 10.2.11.1 , and 10.2.12.1 are the gateway (next hop) addresses on the router that is directly attached to the VQE-S host.

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

Step 4 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the “Restarting the System and Verifying System and VQE-S Status” section on page D-22. You reboot once when all VCDB configuration tasks are completed.

After the VQE-S host is rebooted, you can verify that the default gateway routes are present in the routing table of the CDE110 by issuing the following command:

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

The output will be similar to the following:

```
default
    nexthop via 10.2.9.1 dev eth1 weight 1
```

```
nexthop via 10.2.10.1 dev eth2 weight 1
nexthop via 10.2.11.1 dev eth3 weight 1
nexthop via 10.2.12.1 dev eth4 weight 1
```

Configuring OSPF Routing for VQE-S Traffic

This section provides information on configuring OSPF routing for VQE-S traffic on the CDE110 that hosts VQE-S.

Note For guidance on configuring the attached router for OSPF routing, see the "For OSPF Routing: Guidance for Configuring the Attached Router" section on page 2-36.

To configure OSPF routing for the CDE110 Ethernet interfaces that will be used for VQE-S traffic, follow these steps:

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

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

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

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

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

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

For information on each of the preceding parameters and default values, see Table A-7 on page A-14.

Step 4 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

When the system is rebooted, the VQE Configuration Tool applies the OSPF configuration that you have specified to the VQE-S traffic interfaces.

On the VQE-S Server

After the VQE-S host is rebooted, you can verify that the OSPF configuration is present on the CDE110 by issuing the following commands where:

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

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

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

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


[root@system]# show ip ospf database

       OSPF Router with ID (8.31.200.1)

                Router Link States (Area 0.0.0.1 [NSSA])

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

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

                Net Link States (Area 0.0.0.1 [NSSA])

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

                Summary Link States (Area 0.0.0.1 [NSSA])

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

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

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

                AS External Link States

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


[root@system]# show ip ospf route

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

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

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


[root@system]# show ip route

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

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

On the Cisco 7600 Edge Router

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

- 8.31.20.1 is the OSPF router ID on the edge router.
- In the **show ip route** command output, 8.31.1.1. is accessible from two interfaces, indicating the ECMP is configured correctly.
- The configuration on the edge router is as follows:

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


c7600> show ip ospf
 Routing Process "ospf 100" with ID 8.31.20.1
 Start time: 00:00:04.540, Time elapsed: 06:07:33.560
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 It is an area border and autonomous system boundary router
 Redistributing External Routes from,
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x002F1B
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 2. 1 normal 0 stub 1 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm last executed 06:07:24.744 ago
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x012D0C
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 1
```

```
        Number of interfaces in this area is 2
        It is a NSSA area
        Perform type-7/type-5 LSA translation
        Area has no authentication
        SPF algorithm last executed 00:18:18.804 ago
        SPF algorithm executed 10 times
        Area ranges are
        Number of LSA 6. Checksum Sum 0x025E70
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 2
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

c7600> show ip ospf database

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

                Router Link States (Area 0)

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

                Summary Net Link States (Area 0)

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

                Router Link States (Area 1)

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

                Net Link States (Area 1)

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

                Summary Net Link States (Area 1)

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

                Type-7 AS External Link States (Area 1)

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

                Type-5 AS External Link States

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

c7600> show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

     8.0.0.0/32 is subnetted, 2 subnets
O N2    8.31.1.1 [110/20] via 10.1.2.2, 00:20:45, GigabitEthernet0/2
                 [110/20] via 10.1.1.2, 00:20:45, GigabitEthernet0/1
O       8.31.200.1 [110/11] via 10.1.2.2, 00:20:45, GigabitEthernet0/2
                   [110/11] via 10.1.1.2, 00:20:45, GigabitEthernet0/1
     25.0.0.0/24 is subnetted, 2 subnets
C       25.1.1.0 is directly connected, GigabitEthernet0/1
C       25.1.2.0 is directly connected, GigabitEthernet0/2
     26.0.0.0/24 is subnetted, 1 subnets
C       26.1.1.0 is directly connected, GigabitEthernet0/3
```

Configuring Ethernet Interfaces for VQE-S Traffic

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

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

  See the next section "Configuring Dedicated Interfaces for VQE-S Ingest Traffic and for VQE-S Services Traffic" section on page D-13.
- **Shared Interfaces—**If a VQE deployment does not require that the Ethernet interfaces used for VQE-S ingest traffic be separate from the interfaces used for VQE-S services traffic, a single set of CDE110 Ethernet interfaces is configured as VQE-S traffic interfaces that handle both types of traffic. See the "Configuring Shared Interfaces for All VQE-S Traffic" section on page D-14

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 that will be 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 that will be 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 "Interface for VQE-S Ingest Traffic (VQE-S Host Only)" section on page 2-24.

On the Cisco CDE110 that hosts VQE-S, to configure dedicated interfaces that will be 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 will be available for VQE-S ingest or 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 will be 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 one Ethernet interface that will be used for VQE-S ingest traffic. For example:

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

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-13.

Step 3 Add the vqe.vqes.vqe_services_interfaces parameter to the file and specify one or more Ethernet interfaces that will be used for VQE-S services traffic. For example:

```
vqe.vqes.vqe_services_interfaces="eth3,eth4"
```

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 will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

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 that will be available 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 that will be used.

On the Cisco CDE110 that hosts VQE-S, to configure shared interfaces that will 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 will be 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 will be 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 Ethernet interface names that will be used for VQE-S ingest and services traffic. For example:

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

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-13.

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 will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

Synchronizing the Time and Configuring Network Time Protocol

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

Step 1 If needed, log in as root.

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

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

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

date -s "*date_time_string*"

For example:

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

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

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

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

Step 5 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

For information on starting the NTP service (ntpd daemon), see the "Starting VQE-S System Services and Verifying Status" section on page D-17.

VQE STUN Server Is Enabled By Default

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

Configuring SNMP (Optional)

The CDE110 that hosts VQE-S uses Net-SNMP, a third-party product, for SNMP support for some basic, non-VQE system services. Net-SNMP offers a set of built-in MIBs for Linux platforms. The use of Net-SNMP is optional. For more information on Net-SNMP support, see Appendix B, "Using Net-SNMP."

To configure SNMP on the Cisco CDE110 that hosts VQE-S, follow these steps:

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

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

- system.snmp.ro_community_string="*community_string*"
- system.snmp.location="*server_location*"
- system.snmp.contact="*contact_person*"
- system_snmp_trap_listener="*listener_IP_or_host_name*"

For more information on the SNMP-related VCDB parameters, see Table A-6 on page A-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"
```

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS

In your IPTV deployment, VQE Channel Provisioning Tool (VCPT) or another channel-provisioning server sends channel information to the VQE Servers. You must configure each CDE110 that hosts VQE-S so that only trusted HTTPS clients (the channel-provisioning servers) can send the channel information to the CDE110. If VCPT is the channel-provisioning server, the IP addresses of *all Ethernet interfaces* (that have been assigned IP addresses) on the VCPT host must be configured as trusted HTTPS clients on the VQE-S host.

For more information on VCPT and how it sends channel information, see the "VQE Channel Provisioning Tool and Channel Information" section on page 1-14.

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

To allow only traffic from trusted HTTPS clients on the CDE110 port used for HTTPS, follow these steps:

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

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

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

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

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

Starting VQE-S System Services and Verifying Status

For the CDE110 that hosts VQE-S, Table D-1 lists the system services that you configure and start. Use of the SNMP and NTP services are optional depending on your deployment requirements.

Table D-1 System Services for CDE110 That Hosts VQE-S

Service	Description
sshd	The Secure Shell daemon.
httpd	HyperText Transfer Protocol daemon (the Apache web server).
tomcat5	The Apache Tomcat application server.
snmpd	(Optional) The SNMP daemon.
snmpsa	(Optional) The SNMP subagent.
ntpd	(Optional) The NTP daemon.
check_daemons	A script that monitors httpd and tomcat processes and attempts to restart them if they fail. The script runs once a minute as a **cron** job owned by root.
If OSPF Is Selected as the Routing Type	
watchquagga	The Quagga watchdog process. If a Quagga daemon crashes or hangs, watchquagga restarts it automatically.
ospfd	The OSPF daemon.
zebra	The zebra daemon.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

sshd (pid 2772) is running...

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

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

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

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

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

[root@system]# service httpd status

httpd (2894) is running...

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

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

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

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

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

[root@system]# service tomcat5 status

Tomcat is running...

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

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

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

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

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

[root@system]# service ospfd status

ospfd (pid 6173) is running...
```

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

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

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

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

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

[root@system]# service zebra status

zebra (pid 6139) is running...

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

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

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

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

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

[root@system]# service watchquagga status

watchquagga (pid 2513) is running...

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

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

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

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

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

[root@system]# service snmpd status

snmpd (pid 17654) is running...

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

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

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

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

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

[root@system]# service snmpsa status

The SNMP subagent is running.
```

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

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

Step 12 If you have configured and started the NTP service, to verify that the ntpd service and process are running, issue the following commands:

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

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

[root@system]# service ntpd status

ntpd (pid 17219) is running...

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

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

Starting the VQE-S Processes and Verifying Status

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

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

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

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

Note System error messages are displayed indicating that the VQE-S processes are starting without a channel configuration file. *This is normal behavior* because a channel configuration file from the VQE Channel Provisioning Tool (VCPT) has not yet been sent to VQE-S. Creating and sending the file is done when the Cisco CDE110 that hosts VCPT is configured, and VCPT is used to create and send the file.

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

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

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

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

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

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

```
https://ip_address_of_VQES_host
```

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

If you click **System** in the left pane, the VQE-S Application Monitoring Tool displays information on the VQE-S processes. Figure 4-2 on page 4-3 shows an example.

Restarting the System and Verifying System and VQE-S Status

To restart the Cisco CDE110 and verify system and VQE-S status, follow these steps:

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

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

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

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

The operating system boots.

Note Syslog error messages are displayed indicating that the VQE-S processes are starting without a channel configuration file. *This is normal behavior* because a channel configuration file from the VQE Channel Provisioning Tool (VCPT) has not yet been sent to VQE-S. Creating and sending the file is done when the Cisco CDE110 that hosts VCPT is configured, and VCPT is used to create and send the file.

Step 3 Log in as root.

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

```
... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

Step 15 If you have configured an NTP server, to verify that the ntpd service is running, issue the following command:

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

... Output omitted
```

Step 16 Do one of the following:

- If the preceding checks indicate that all is well, proceed to the "Setting Up a Cisco CDE110 That Hosts VQE Tools" section on page D-25.
- If one of the preceding checks fails, inspect the configuration of the item that failed and make any needed adjustments.

Setting Up a Cisco CDE110 That Hosts VQE Tools

This section explains how to perform the initial configuration tasks for a Cisco CDE110 hosting VQE Tools (VQE Channel Provisioning Tool [VCPT] and VQE Client Configuration Delivery Server).

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

For information on manually editing the vcdb.conf file, see the "Manually Editing the VCDB File" section on page 6-13.

Perform these initial configuration tasks in the order shown:

1. Prerequisites for a Cisco CDE110 That Hosts VQE Tools, page D-25
2. Configuring the Linux Operating System for VQE Tools, page D-26
3. Configuring a Static Route for a Management Network (VQE Tools Host), page D-28
4. Synchronizing the Time and Configuring Network Time Protocol, page D-29
5. Configuring SNMP (Optional), page D-30
6. Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS, page D-30
7. Starting VQE Tools System Services and Verifying Status, page D-31
8. Starting the VCDS Service and Verifying VCDS and VCPT Status, page D-34
9. Restarting the System and Verifying System, VCPT, and VCDS Status, page D-35

On the VQE Tools server, proper route configuration is needed for external access to the VQE Tools server. You can use the static management route explained in the "Configuring a Static Route for a Management Network (VQE Tools Host)" section on page D-28 to configure this access.

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

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

Prerequisites for a Cisco CDE110 That Hosts VQE Tools

This section explains tasks that should be performed before setting up a Cisco CDE110 that hosts VQE Tools.

Connecting Cables

For information on connecting cables on the VQE Tools server, see the "Connecting Cables to the CDE110" section on page 2-3.

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

Setting Up SSL Certificates for VCPT

It is recommended that you deploy your own or commercial Secure Sockets Layer (SSL) certificates prior to beginning the tasks for setting up a Cisco CDE110 that hosts VCPT. For information on setting up the certificates, see the "Setting Up SSL Certificates" section on page 2-4.

Configuring the Linux Operating System for VQE Tools

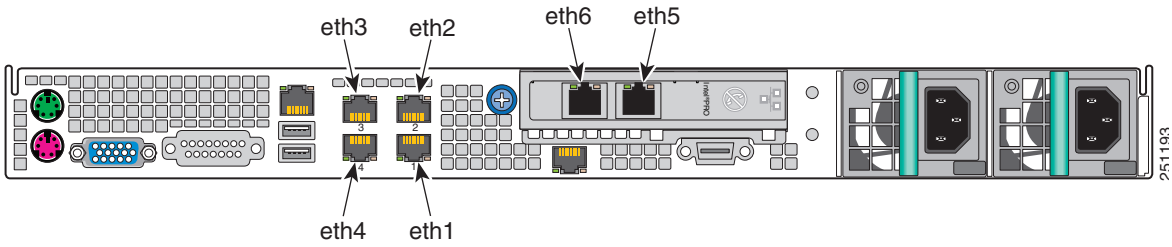
This section explains the initial Linux configuration tasks needed for a Cisco CDE110 appliance that will run the VQE Tools (VCPT and VQE Client Configuration Delivery Server) software. The explanation assumes that the needed software for Linux, VCPT, and VQE Client Configuration Delivery Server have been pre-installed on the Cisco CDE110 appliance. For Red Hat Linux 5.1 documentation, go to the following web site:

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

For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE110 back panel are specified as eth1 to eth6 as shown in Figure D-4.

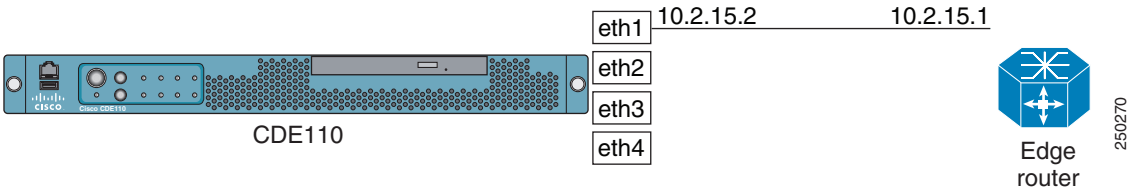
Note Earlier models of the CDE110 have four Ethernet ports (eth1 to eth4). These models did not have the Intel PRO/1000 PT Dual Port Server Adapter that provides the eth5 and eth6 ports.

Figure D-4 NIC Port Numbering for Software Configuration



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

Figure D-5 IP Addresses for VQE Tools Configuration Examples



Note The configuration examples in this section assume that one CDE110 Ethernet interface (eth1) will be used to connect to the VQE network.

To configure the Linux operating system and other software for the VQE Tools (VCPT and VQE Client Configuration Delivery Server [VCDS]), follow these steps:

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

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

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

Enter a password that follows the password guidelines:

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

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

This username and password can be used to log in to Linux directly using SSH. The vqe username and password can also be used log in to the VQE Channel Provisioning Tool.

Step 3 To configure CDE110 Ethernet interfaces eth1 to eth6, edit the /etc/opt/vqes/vcdb.conf file by adding to the file one or more network.eth*x*.addr parameters, where eth*x* is eth1, eth2, and so on. Specify an IP address and prefix length for each interface. The following example shows one vcdb.conf line for the eth1 Ethernet interface:

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

Step 4 To configure the hostname for the CDE110 server, edit the /etc/opt/vqes/vcdb.conf file by adding to the file the system.global.hostname parameter and specifying a hostname. The following example specifies the hostname as starfire1-iptv:

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

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

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

For example:

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

Step 6 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System, VCPT, and VCDS Status" section on page D-35. You reboot once when all VCDB configuration tasks are completed.

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

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

```
[root@system]# ifconfig eth1

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

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

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

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

- Use the **ping** command to check that the Cisco CDE110 can reach the connected edge router. For example:

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

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

If your deployment makes use of a management network, a static route for the management network can be configured using the VCDB parameter network.route.mgmt_route. The configuration example in this section assumes that one CDE110 Ethernet interface (eth1) will be used to connect to the VQE network.

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

Note If you configure static route for a management network as described in this section, see "Static Route for a Management Network Is Missing on CDE110 Hosting VQE-S or VQE Tools" section on page 5-8 for some additional information.

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

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

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

network.route.mgmt_route="*management-network-addr/prefix-length* via *gateway-addr* "

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

For this example, assume the following:

- CDE110 Ethernet interface eth1 (10.2.15.2) will be used for the management network.
- The management network is 192.0.0.0/8.

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

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

In the preceding example, 10.2.15.1 is the *gateway-addr*—the router interface that is directly attached to eth1. Figure D-5 shows the IP addresses used in this example for the eth1 interface and the directly attached router.

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System, VCPT, and VCDS Status" section on page D-35. You reboot once when all VCDB configuration tasks are completed.

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

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

The output will be similar to the following:

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

Synchronizing the Time and Configuring Network Time Protocol

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

Step 1 If needed, log in as root on the CDE110 that hosts VQE Tools.

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

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

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

date -s "*date_time_string*"

For example:

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

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

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

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

Step 5 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System, VCPT, and VCDS Status" section on page D-35. You reboot once when all VCDB configuration tasks are completed.

For information on starting the NTP service (ntpd daemon), see the "Starting VQE Tools System Services and Verifying Status" section on page D-31.

Configuring SNMP (Optional)

The CDE110 that hosts VQE Tools uses Net-SNMP, a third-party product, for SNMP support for some basic, non-VQE system services. Net-SNMP offers a set of built-in MIBs for Linux platforms. The use of Net-SNMP is optional. For more information on Net-SNMP support, see Appendix B, "Using Net-SNMP."

To configure SNMP on the Cisco CDE110 that hosts VQE Tools, follow these steps:

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

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

- system.snmp.ro_community_string="*community_string*"
- system.snmp.location="*server_location*"
- system.snmp.contact="*contact_person*"
- system_snmp_trap_listener="*listener_IP_or_host_name*"

For more information on the SNMP-related VCDB parameters, see Table A-6 on page A-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"
```

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System, VCPT, and VCDS Status" section on page D-35. You reboot once when all VCDB configuration tasks are completed.

Ensuring That Only Trusted HTTPS Clients Can Communicate Using HTTPS

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

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

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

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

To allow only traffic from trusted HTTPS clients on the CDE110 port used for HTTPS, follow these steps:

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

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

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

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

Step 3 Save the vcdb.conf file.

Note VCDB configurations will be applied to the CDE110 when it is rebooted in the "Restarting the System and Verifying System and VQE-S Status" section on page D-22. You reboot once when all VCDB configuration tasks are completed.

Starting VQE Tools System Services and Verifying Status

For the CDE110 that hosts VQE Tools, Table D-2 lists the system services that you configure and start. Use of the SNMP and NTP services are optional depending on your deployment's requirements.

Table D-2 System Services for CDE110 That Hosts VQE Tools

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

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

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

Step 1 If needed, log in as root on the CDE110 that hosts VQE Tools.

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

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

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

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

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

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

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

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

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

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

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

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

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

[root@system]# service sshd status

sshd (pid 2772) is running...

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

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

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

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

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

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

```
httpd (2894) is running...

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

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

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

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

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

[root@system]# service tomcat5 status

Tomcat is running...

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

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

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

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

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

[root@system]# service snmpd status

snmpd (pid 17654) is running...

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

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

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

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

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

[root@system]# service snmpsa status

The SNMP subagent is running.
```

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

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

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

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

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

[root@system]# service ntpd status

ntpd (pid 17219) is running...

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

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

Starting the VCDS Service and Verifying VCDS and VCPT Status

This section explains how to start the VQE Client Configuration Delivery Server (VCDS) service and verify that the process is running and that VCPT is available.

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

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

Step 1 If needed, log in as root on the CDE110 that hosts VQE Tools.

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

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

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

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

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

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

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

root     29860     1  0 Jul25 ?        00:00:00 /opt/vqes/bin/VQECCfgDeliveryServer -d
-f /etc/opt/vqes/VCDServer.cfg
```

Step 5 To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VCPT:

```
https://ip_address_of_VCPT_host
```

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

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

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

To restart the Cisco CDE110 and verify system, VCPT, and VQE Client Configuration Delivery Server (VCDS) status, follow these steps:

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

Step 1 If needed, log in as root on the CDE110 that hosts VQE Tools.

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

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

The operating system boots.

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

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

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

... Output omitted
```

Step 9 If you have configured an NTP server, to verify that the ntpd service is running, issue the following command:

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

... Output omitted
```

Step 10 To check that the vcds service is running, issue the following command:

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

... Output omitted
```

Step 11 To verify that VCPT is accessible from a web browser, enter as the URL the IP address of the Cisco CDE110 that hosts VCPT:

```
https://ip_address_of_VCPT_host
```

Log in with a Linux username and password.

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

Step 12 Do one of the following:

- If the preceding checks indicate that all is well, you are ready to start using VCPT. For information, see Chapter 3, "Using the VQE Channel Provisioning Tool."
- If one of the preceding checks fails, inspect the configuration of the item that failed and make any needed adjustments.