C H A P T E R 16

Configuring High Availability (HA)

This chapter describes how to set up a pair of Clean Access Manager machines for high-availability. By deploying Clean Access Managers in high-availability mode, you can ensure that important monitoring, authentication, and reporting tasks continue in the event of an unexpected shutdown. Topics include:

Note You must use identical appliances (e.g. NAC-3350 and NAC-3350) in order to configure High Availability (HA) pairs of Clean Access Managers (CAMs) or Clean Access Servers (CASs).

Overview

The following key points provide a high-level summary of HA-CAM operation:

- The Clean Access Manager high-availability mode is an Active/Passive two-server configuration in which a standby CAM machine acts as a backup to an active CAM machine.
- The active Clean Access Manager performs all tasks for the system. The standby CAM monitors the active CAM and keeps its database synchronized with the active CAM's database.

Note CAM Authorization settings are not automatically passed from one CAM to the other in an HA-pair. If you use the Authorization feature in a CAM HA-pair, follow the guidelines in Backing Up and Restoring CAM/CAS Authorization Settings, page 15-57 to ensure you are able to *exactly* duplicate your Authorization settings from one CAM to its high availability counterpart.

- Both CAMs share a virtual Service IP for the eth0 trusted interface. The Service IP must be used for the SSL certificate.

- The Service IP address is used for all messages and requests sent to the CAM, including communication from the CAS and the administration web console.

- The CAM uses its individual (eth0) IP address for all communications sent to the CAS and proxy authentication messages.

- The primary and secondary CAM machines exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.

- In order to ensure an active CAM is always available, its trusted interface (eth0) must be up. To avoid a situation where a CAM is active but is not accessible via its trusted interface (that is, the standby CAM receives heartbeat packets from the active CAM, but the active CAM's eth0 interface fails), the link-detect mechanism allows the standby CAM to be aware of when the active CAM's eth0 interface becomes unavailable.

- Both the Clean Access Manager and Clean Access Server are designed to automatically reboot in the event of a hard-drive failure, thus automatically initiating failover to the standby CAM/CAS.

- You can choose to "automatically configure" the eth1 interface in the **Administration > CCA Manager > Failover** page, but you must manually configure other (eth2 or eth3) HA interfaces with an IP address, netmask, etc. prior to configuring HA on the CAM.

- The eth0, eth1 and eth2/eth3 interfaces can be used for heartbeat packets and database synchronization. In addition, any available serial (COM) interface can also be used for heartbeat packets. If using more than one of these interfaces, then all the heartbeat interfaces need to fail for failover to occur.

Note If you are configuring your CAM for HA, you must use eth1 for heartbeat and database synchronization. All other Ethernet interfaces (eth0 and eth2/eth3) are optional for this purpose.

Note When deploying the CAM/CAS across a WAN, you must prioritize all CAM/CAS traffic and SNMP traffic, and include the eth0/eth1 IP addresses of the CAM and CAS in addition to the Service IP address for HA pairs.

Caution The connection between HA pairs must be extremely reliable, with communication between HA pairs unimpeded. The best practice is to use a dedicated Ethernet cable. Breaking communication between HA pairs will result in two active nodes, which can have serious negative operational consequences. A key aspect of the link between HA pairs is the ability to restore that link should it go down; restoration may be fundamental to network stability, depending on your design.

Figure 16-1 illustrates a sample configuration.

Figure 16-1 **Clean Access Manager Example High-Availability Configuration**
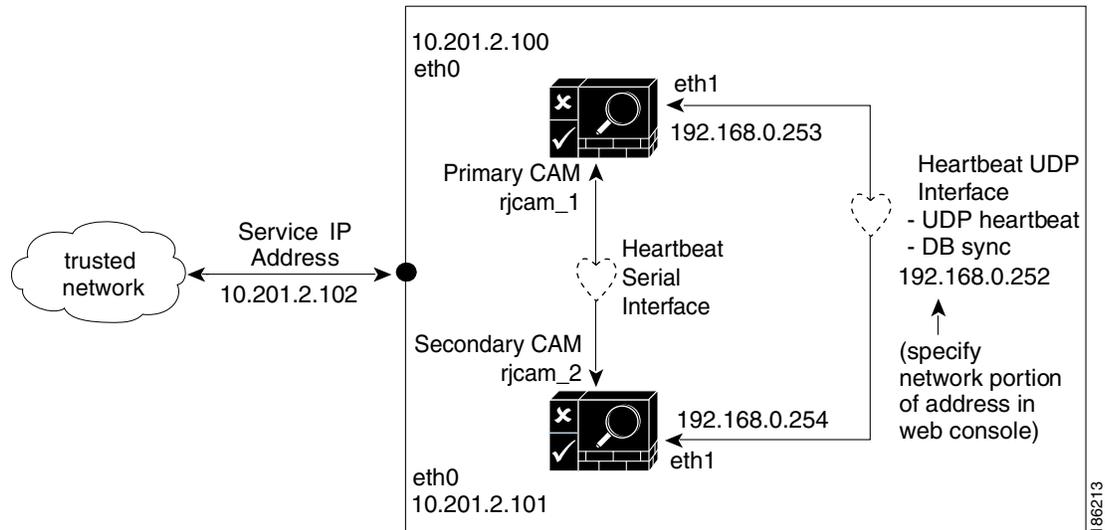
The Clean Access Manager high-availability mode is an Active/Passive two-server configuration in which a standby Clean Access Manager machine acts as a backup to an active Clean Access Manager machine. While the active CAM carries most of the workload under normal conditions, the standby monitors the active CAM and keeps its data store synchronized with the active CAM's data.

If a failover event occurs, such as the active CAM shuts down or stops responding to the peer's "heartbeat" signal, the standby assumes the role of the active CAM.

When first configuring the HA peers, you must specify an HA-Primary CAM and HA-Secondary CAM. Initially, the HA-Primary is the active CAM, and the HA-Secondary is the standby (passive) CAM, but the active/passive roles are not permanently assigned. If the primary CAM goes down, the secondary (standby) becomes the active CAM. When the original primary CAM restarts, it assumes the backup role.

Note   If *both* the HA-Primary and HA-Secondary CAMs in your HA deployment lose their configuration, you can restore the system using the guidelines in Restoring Configuration From CAM Snapshot—HA-CAM or HA-CAS, page 15-60.

When the Clean Access Manager starts up, it checks to see if its peer is active. If not, the starting CAM assumes the active role. If the peer is active, on the other hand, the starting CAM becomes the standby.

You can configure two Clean Access Managers as an HA pair at the same time, or you can add a new Clean Access Manager to an existing standalone CAM to create a high-availability pair. In order for the pair to appear to the network as one entity, you must specify a **Service IP Address** to be used as the trusted interface (eth0) address for the HA pair. This Service IP address is also used to generate the SSL certificate.

To create the Heartbeat UDP Interface link over which HA information is exchanged, you connect the eth1 ports of both CAMs and specify a private network address not currently routed in your organization (the default Heartbeat UDP interface IP address is 192.168.0.252). The Clean Access Manager then creates a private, secure two-node network for the eth1 ports of each CAM to exchange UDP heartbeat traffic and synchronize databases.

> **Note** The CAM always uses eth1 as the UDP heartbeat interface.

For heartbeat redundancy, you can also connect the serial ports of each Clean Access Manager for heartbeat exchange. In this case, both the UDP heartbeat and serial heartbeat interfaces must fail for the standby system to take over.

> **Note** When the primary eth1 link has been disconnected and only the serial link remains, the CAM returns a database error indicating that it cannot sync with its HA counterpart, and the administrator sees the following error in the CAM web console: "WARNING! Closed connections to peer [standby IP] database! Please restart peer node to bring databases in sync!!"

> **Warning** **When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.**

> **Note** For serial cable connection for HA (either HA-CAM or HA-CAS), the serial cable must be a "null modem" cable. For details, refer to http://www.nullmodem.com/NullModem.htm.

The following sections describe the steps for setting up high availability.

> **Note** The instructions in this section assume that you are adding a Clean Access Manager to a standalone CAM in order to configure the HA pair for a test network.

Before Starting

⚠️

Warning   To prevent any possible data loss during database synchronization, always make sure the standby (secondary) Clean Access Manager is up and running before failing over the active (primary) Clean Access Manager.

Before configuring high availability, ensure that:

- You have obtained a high-availability (failover) license.

✎

Note   When installing a CAM Failover (HA) license, install the Failover license to the Primary CAM first, then load all the other licenses.

- Both CAMs are installed and configured (see Perform the Initial Configuration, page 2-9.)
- The two CAMs in the HA pair must remain Layer 2 adjacent to support heartbeat and sync functions.
- For heartbeat, each CAM needs to have a unique hostname (or node name). For HA CAM pairs, this host name will be provided to the peer, and must be resolved via DNS or added to the peer's /etc/hosts file.
- You have a CA-signed certificate for the Service IP of the HA CAM pair. (For testing, you can use the CA-signed certificate of the HA-Primary CAM, but this requires additional steps to configure the HA-Primary CAM's IP as the Service IP).
- The HA-Primary CAM is fully configured for runtime operation. This means that connections to authentication sources, policies, user roles, access points, and so on, are all specified. This configuration is automatically duplicated in the HA-Secondary (standby) CAM.
- If you use the Authorization feature in a CAM HA-pair, follow the guidelines in Backing Up and Restoring CAM/CAS Authorization Settings, page 15-57 to ensure you are able to *exactly* duplicate your Authorization settings from one CAM to its high availability counterpart. (CAM Authorization settings are not automatically passed from one CAM to the other in an HA-pair.)
- Both Clean Access Managers are accessible on the network (try pinging them to test the connection).
- The machines on which the CAM software is installed have at least one free Ethernet port (eth1) and at least one free serial port. Use the specification manuals for the server hardware to identify the serial port (ttyS0 or ttyS1) on each machine.
- In Out-of-Band deployments, Port Security is not enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.

The following procedures require you to reboot the Clean Access Manager. At that time, its services will be briefly unavailable. You may want to configure an online CAM when downtime has the least impact on your users.

✎

Note   Cisco NAC Appliance web admin consoles support the Internet Explorer 6.0 or above browser.

Connect the Clean Access Manager Machines

There are two types of connections between HA-CAM peers: one for exchanging runtime data relating to the Clean Access Manager activities and one for the heartbeat signal. In High Availability, the Clean Access Manager **always** uses the eth1 interface for both data exchange and heartbeat UDP exchange. When the UDP heartbeat signal fails to be transmitted and received within a certain time period, the standby system takes over. In order to provide an extra measure of heartbeat redundancy, Cisco recommends you use more Ethernet interfaces in addition to eth1 (mandatory) interface and/or use one of the available serial interfaces for heartbeat exchange. In order for a failover to occur, all configured heartbeat interfaces must report heartbeat exchange failure. (The eth0 and eth2/eth3 can be used for additional heartbeat interfaces.) Note, however, that the eth1 connection between the CAM peers is mandatory.

Physically connect the peer Clean Access Managers as follows:

- Use a crossover cable to connect the eth1 Ethernet ports of the Clean Access Manager machines. This connection is used for the heartbeat UDP interface and data exchange (database mirroring) between the failover peers.

- Use null modem serial cable to connect the serial ports (highly recommended). This connection is used as an additional heartbeat serial exchange (keep-alive) between the failover peers.

- Optionally connect eth2 and/or eth3 interfaces on the CAM to counterpart interfaces on the HA peer using either crossover cables or via an in-line switch. (Remember: you must configure these interfaces manually before configuring your CAM for HA).

> **Note**   For serial cable connection for HA, the serial cable must be a "null modem" cable. For details, refer to http://www.nullmodem.com/NullModem.htm.

Serial Connection

If the machine running the Clean Access Manager software has two serial ports, you can use the additional port for the serial heartbeat connection. By default, the first serial port detected on the CAM server is configured for console input/output (to facilitate installation and other types of administrative access).

If the machine has only one serial port (COM1 or ttyS0), you can reconfigure the port to serve as the high-availability heartbeat connection. This is because, after the CAM software is installed, SSH or KVM console can always be used to access the command line interface of the CAM.

> **Note**   When the primary eth1 link has been disconnected and only the serial link remains, the CAM returns a database error indicating that it cannot sync with its HA counterpart, and the administrator sees the following error in the CAM web console: "WARNING! Closed connections to peer [standby IP] database! Please restart peer node to bring databases in sync!!"

> **Warning**   **When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.**

Configure the HA-Primary CAM

Once you have verified the prerequisites, perform the following steps to configure the Clean Access Manager as the HA-Primary for the high availability pair. See Figure 16-1 for an example high-availability configuration.

Step 1   Open the web admin console for the Clean Access Manager to be designated as the HA-Primary, and go to **Administration** > **CCA Manager > SSL > X509 Certificate** to configure the SSL certificate for the primary CAM.

> ✎
> **Note**   The HA configuration steps in this chapter assume that a temporary certificate will be exported from the HA-Primary CAM to the HA-Secondary CAM.

If using a temporary certificate for the HA pair:

  a.   Click **Generate Temporary Certificate**, enter information for all of the fields in the form, and click **Generate**. The certificate must be associated with the Service IP addresses of the HA pair.

  b.   When finished generating the temporary certificate, click the checkboxes for the certificate and Private Key to highlight them in the table.

  c.   Click **Export** to save the certificate and Private Key to your local machine. You must import the certificate and Private Key later when configuring the HA-Secondary CAM.

If using a CA-signed certificate for the HA pair:

> ✎
> **Note**   This process assumes you have already generated a Certificate Signing Request and accompanying Private Key, submitted the request to your Certificate Authority, and have received your CA-signed certificate. If you have not yet obtained a CA-signed certificate for the CAS, be sure to follow the instructions in Manage CAM SSL Certificates, page 15-6 for details.

  a.   Click **Browse** and navigate to the directory on your local machine containing the CA-signed certificate and Private Key.

  b.   Click **Import**. Note that you will need to import the same certificate later to the HA-Secondary CAS.

Step 2   Go to **Administration** > **CCA Manager** and click the **Failover** tab. Choose the **HA-Primary** option from the **Clear Access Manager Mode** dropdown menu. The high availability settings appear:

Figure 16-2   HA-Primary Clean Access Manager Failover Settings

Step 3   Copy the value from the **IP Address** field under **Administration > CCA Manager > Network** and enter it in **Service IP Address** field. The Network Settings IP Address is the existing IP address of the primary Clean Access Manager. The idea here is to turn this IP address, which the Clean Access Servers already recognize, into the virtual Service IP address Clean Access Servers use for the Clean Access Manager pair.

Step 4   Change the **IP address** under **Administration > CCA Manager > Network** to an available address (for example *x.x.x*.121).

Step 5   (Recommended) Specify parameters to enable failover based on eth0 link failure detection for the HA-Primary CAM:

a.   Enter IP addresses for the interfaces the HA pair uses to failover from the primary to the secondary CAM in the **Link-detect IP Address for eth0** field. When IP addresses are entered in this field, the HA-Secondary CAM attempts to ping the specified HA-Primary CAM IP address to verify connectivity. Typically, the same IP address is entered on both the HA-Primary and HA-Secondary CAM, but you *can* specify different addresses for each CAM if your network topology allows.

b.   Specify the duration (in seconds) the CAM continues to ping the Link-detect IP address before determining that the eth0 interface may have gone down, thus initiating a failover to the secondary CAM, in the **Link-detect Timeout** field. The minimum value for this setting is 10 seconds, but Cisco recommends at least a 25-second timeout interval.

> ✎
>
> **Note**   Link-detect settings on the CAM (Release 4.1(3) and later) are needed to allow the active CAM to failover to the standby CAM in case of a switch port failure or a link failure on the switch port connected to eth0 of the active CAM. In the event a failover must take place, the Link detect setting allows the standby CAM to ensure that the secondary CAM eth0 interface is up and able to take on the active role.

Step 6   Each Clean Access Manager must have a unique host name (such as `rjcam_1` and `rjcam_2`). Type the host name of the HA-Primary CAM in the **Host Name** field under **Administration > CCA Manager > Network**, and type the host name of the HA-Secondary CAM in the **Peer Host Name** field under **Administration > CCA Manager > Failover**.

> ✎
>
> **Note**   • A **Host Name** value is mandatory when setting up high availability, while the **Host Domain** name is optional.
>
> • The **Host Name** and **Peer Host Name** fields are case-sensitive. Make sure to match what is typed here with what is typed for the HA-Secondary CAM later.

Step 7   If you are using the default setting for the mandatory eth1 UDP heartbeat interface, leave the **Auto eth1 Setup** checkbox enabled (checked). If you want to specify a different **[Secondary] Heartbeat eth1 Address**, uncheck the **Auto eth1 Setup** checkbox and enter the new IP address in the **(peer IP on heartbeat udp interface on eth1)** field.

> ✎
>
> **Note**   The **Auto eth1 Setup** option automatically assigns 192.168.0.254 as the primary CAM's eth1 (heartbeat) interface and assumes the IP address for the peer (secondary) eth1 interface is 192.168.0.253.

> ⚠
>
> **Warning**   **To specify redundant failover links as described in Step 9, you must first configure the appropriate Ethernet interfaces on the CAM before you try to set up HA. If you attempt to configure these interfaces and the NICs on which the Ethernet interfaces reside are not configured correctly, the CAM will enter maintenance mode (will not boot properly) when you reboot.**

Step 8   (Optional) If you want to enable the CAM's **Heartbeat UDP Interface 2** function that sets up a redundant failover heartbeat via the CAM eth0 interface, enable the **eth0** checkbox and specify an associated peer IP address in the **[Secondary] Heartbeat IP Address on eth0** field. Otherwise, leave this N/A if not using the additional UDP heartbeat interface.

Step 9   (Optional) If you want to enable the CAM's **Heartbeat UDP Interface 3** function, select **eth2** or **eth3** from the dropdown menu and specify an associated peer IP address in the **[Secondary] Heartbeat IP Address on interface 3** field. Otherwise, leave this N/A if not using the additional UDP heartbeat interface.

Step 10   From the **Heartbeat Serial Interface** dropdown menu, choose the serial port to which you connected the serial cable of the HA-Primary CAM, or leave this N/A if not using serial connection. The options in this dropdown list are the serial interfaces that are both enabled and available on the CAM for heartbeat interface connection. (See Serial Connection, page 16-6 for further details.)

Step 11   Specify the **Heartbeat Timeout** value for the HA primary CAM to set the duration the CAM should wait before declaring that it has lost communication with its HA peer, thus assuming the role of the active CAM in the HA pair. The default **Heartbeat Timeout** value is 30 seconds.

✎

Note   Starting from Cisco NAC Appliance Release 4.6(1), the **Heartbeat Timeout** default value has been increased to 30 seconds to help accommodate CAM HA peers located in relatively distant locations on the network, where latency issues might cause a standby HA CAM to assume the active role when it has not received heartbeat packets from its HA peer within the specified **Heartbeat Timeout** period. In the resulting network scenario, you could potentially end up with two "active" CAMs performing Cisco NAC Appliance functions, requiring you to reboot both CAMs to re-establish the correct primary/secondary HA peer relationship.

Step 12   Click **Update** and then **Reboot** to restart the Clean Access Manager.

After the Clean Access Manager restarts, make sure that the CAM machine is working properly. Check to see if the Clean Access Servers are connected and new users are being authenticated.

Configure the HA-Secondary CAM

Step 1   Open the web admin console for the Clean Access Manager to be designated as the HA-Secondary, and go to **Administration > CCA Manager > SSL > X509 Certificate**.

Step 2   Before starting:

- Back up the secondary CAM's private key.
- Make sure the private key and SSL certificate files associated with the Service IP/HA-Primary CAM are available (previously exported as described in Configure the HA-Primary CAM, page 16-7).

Step 3   Import the HA-Primary CAM's private key file and certificate as described below:

If using a temporary certificate for the HA pair:

a.   Click **Browse** and navigate to the location on your local machine where you have saved the temporary certificate and Private Key you previously exported from the HA-Primary CAS.

b.   Select the certificate file and click **Import**.

c.   Repeat the process to import the Private Key.

If using a CA-signed certificate for the HA pair:

a.   Click **Browse** and navigate to the location on your local machine where you have saved the CA-signed certificate you received from your Certificate Authority and the associated Private Key you exported from the HA-Primary CAS and saved to your local machine.

b.   Select the CA-signed certificate file and click **Import**.

c.   Repeat the process to import the Private Key.

For more information, see Manage CAM SSL Certificates, page 15-6.

Step 4   Go to the **Administration > CCA Manager > Network** and change the **IP Address** of the secondary CAM to an address that is different from the HA-Primary CAM IP address and the Service IP address (such as $x.x.x.122$).

Figure 16-3   HA-Secondary Clean Access Manager Failover Settings

Step 5   Set the **Host Name** value to the same value set for the **Peer Host Name** in the HA-Primary CAM configuration. See Figure 16-1 on page 16-3.

> **Note**   The **Host Name** and **Peer Host Name** fields are case-sensitive. Make sure to match what is typed here with what was typed for the HA-Primary CAM.

Step 6   Choose **HA-Secondary** in the **Clean Access Manager Mode** dropdown menu. The high availability settings appear.

Step 7   Set the **Service IP Address** value to the same value set for the **Service IP Address** in the HA-Primary CAM configuration.

Step 8   (Recommended) Specify parameters to enable failover based on eth0 link failure detection for the HA-Secondary CAM:

a.   Enter IP addresses for the interfaces the HA pair uses to failover from the primary to the secondary CAM in the **Link-detect IP Address for eth0** field.

b.   Specify the duration (in seconds) the CAM continues to ping the Link-detect IP address before determining that the eth0 interface may have gone down, thus initiating a failover to the secondary CAM, in the **Link-detect Timeout** field. The minimum value for this setting is 10 seconds, but Cisco recommends at least a 25-second timeout interval.

> ✎
> **Note**   Link-detect settings on the CAM (Release 4.1(3) and later) are needed to allow the active
> CAM to failover to the standby CAM in case of a switch port failure or a link failure on the
> switch port connected to eth0 of the active CAM. In the event a failover must take place, the
> Link detect setting allows the standby CAM to ensure that the secondary CAM eth0 interface
> is up and able to take on the active role.

Step 9   Set the **[Primary] Peer Host Name** value to the HA-Primary CAM's host name.

Step 10   If you are using the default setting for the mandatory eth1 UDP heartbeat interface, leave the **Auto eth1 Setup** checkbox enabled (checked). If you want to specify a different **[Primary] Heartbeat eth1 Address**, uncheck the **Auto eth1 Setup** checkbox and enter the new IP address in the **(peer IP on heartbeat udp interface on eth1)** field.

> ✎
> **Note**   The **Auto eth1 Setup** option automatically assigns 192.168.0.254 as the primary CAM's eth1
> (heartbeat) interface and assumes the IP address for the peer (secondary) eth1 interface is
> 192.168.0.253.

> ⚠
> **Warning**   **To specify redundant failover links as described in Step 12, you must first configure the appropriate Ethernet interfaces on the CAM before you try to set up HA. If you attempt to configure these interfaces, however, and the NICs on which the Ethernet interfaces reside are not configured correctly, the CAM will enter maintenance mode (will not boot properly) when you reboot.**

Step 11   (Optional) If you enabled the HA-Primary CAM's **Heartbeat UDP Interface 2** function that sets up a redundant failover heartbeat via the CAM eth0 interface on the HA-Primary CAM, enable the **eth0** checkbox and specify the same peer IP address in the **[Primary] Heartbeat IP Address on eth0** field as on the HA-Primary CAM.

Step 12   (Optional) If you enabled the HA-Primary CAM's **Heartbeat UDP Interface 3** function on the HA-Primary CAM, select **eth2** or **eth3** from the dropdown menu and the same associated peer IP address in the **[Primary] Heartbeat IP Address on interface 3** field as on the HA-Primary CAM.

Step 13   From the **Heartbeat Serial Interface** dropdown menu, choose the serial port to which you connected the serial cable of the HA-Primary CAM, or leave this N/A if not using serial connection. The options in this dropdown list are the serial interfaces that are both enabled and available on the CAM for heartbeat interface connection. (See Serial Connection, page 16-6 for further details.)

Step 14   Specify the **Heartbeat Timeout** value for the HA secondary CAM to set the duration the CAM should wait before declaring that it has lost communication with its HA peer, thus assuming the role of the active CAM in the HA pair. The default **Heartbeat Timeout** value is 30 seconds.

> ✎
> **Note**   Starting from Cisco NAC Appliance Release 4.6(1), the **Heartbeat Timeout** default value has
> been increased to 30 seconds to help accommodate CAM HA peers located in relatively distant
> locations on the network, where latency issues might cause a standby HA CAM to assume the
> active role when it has not received heartbeat packets from its HA peer within the specified
> **Heartbeat Timeout** period. In the resulting network scenario, you could potentially end up with
> two "active" CAMs performing Cisco NAC Appliance functions, requiring you to reboot both
> CAMs to re-establish the correct primary/secondary HA peer relationship.

⚠ **Warning   When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.**

Step 15   Click **Update** and then **Reboot**.

When the standby CAM starts up, it automatically synchronizes its database with the active CAM.

Step 16   Finally, open the admin console for the standby again and complete the configuration as follows. Notice that the admin console for the standby CAm displays limited management modules (Figure 16-4 and Figure 16-5).

Figure 16-4   Standby Web Admin Console Example—Summary Page
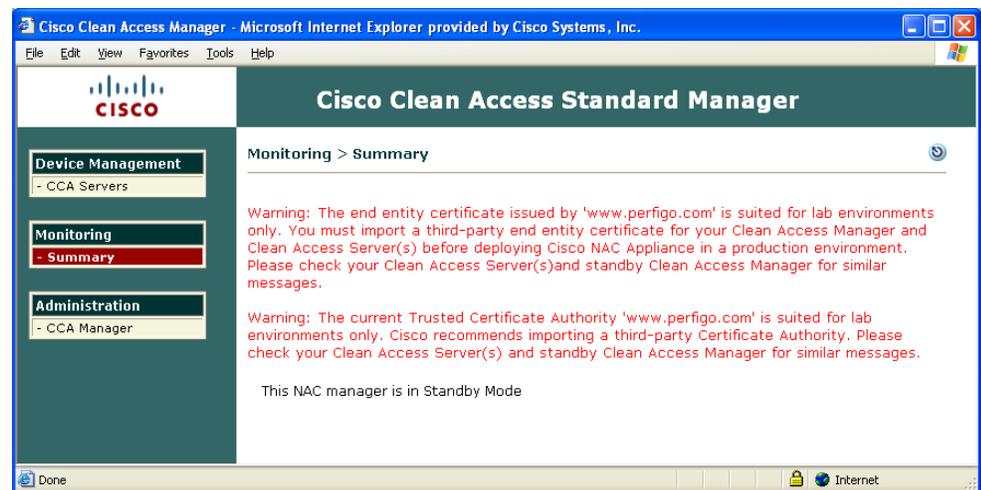
Figure 16-5   Standby Web Admin Console Example—CCA Manager > Network Page

Complete the Configuration

Verify settings in the **Failover** pages for both the active and standby CAMs. The high availability configuration is now complete.

Upgrading an Existing Failover Pair

For instructions on how to upgrade an existing failover pair to a new Cisco NAC Appliance release, see "Upgrading High Availability Pairs" in the *Release Notes for Cisco NAC Appliance, Version 4.6(1)*.

Failing Over an HA-CAM Pair

Warning   **To prevent any possible data loss during database synchronization, always make sure the standby CAM is up and running before failing over the active CAM.**

To failover an HA-CAM pair, SSH to the active machine in the pair and perform one of the following commands:

- **shutdown**, or
- **reboot**, or
- **service perfigo stop**

This stops all services on the active machine. When heartbeat fails, the standby machine will assume the active role. Perform **service perfigo start** to restart services on the stopped machine. This should cause the stopped machine to assume the standby role.

Note   **service perfigo restart** should not be used to test high availability (failover). Instead, Cisco recommends "shutdown" or "reboot" on the machine to test failover, or, the CLI commands **service perfigo stop** and **service perfigo start**. See CAM CLI Commands, page 2-19.

Useful CLI Commands for HA

The following are useful files to know about for HA on the CAM:

- /etc/ha.d/perfigo.conf
- /etc/ha.d/ha.cf

The following example shows the location of the HA debug/log files, as well as the name of each CAM (node) in the HA pair:

```
[root@rjcam_1 ha.d]# more ha.cf
# Generated by make-hacf.pl
udpport          694
bcast            eth1
auto_failback    off
apiauth          default uid=root
log_badpack      false
debug            0
```

```
debugfile      /var/log/ha-debug
logfile        /var/log/ha-log
#logfacility   local0
watchdog       /dev/watchdog
keepalive      2
warntime       10
deadtime       15
node           rjcam_1
node           rjcam_2
```

Verifying Active/Standby Runtime Status on the HA CAM

The following example shows how to use the CLI to determine the runtime status (active or standby) of each CAM in the HA pair. You can run the **fostate.sh** command from the **/perfigo/common/bin/** directory on new and upgraded CAMs.

1. Run the fostate.sh script on the first CAM:

```
[root@rjcam_1 ~]# ./fostate.sh
My node is active, peer node is standby
[root@rjcam_1 ~]#
```

This CAM is the active CAM in the HA-pair.

2. Run the fostate.sh script on the second CAM:

```
[root@rjcam_2 ~]# ./fostate.sh
My node is standby, peer node is active
[root@rjcam_2 ~]#
```

This CAM is the standby CAM in the HA-pair.

Accessing High Availability Pair Web Consoles

Determining Active and Standby CAM

Access the web console for each CAM in the HA pair by typing the IP address of each individual CAM (not the Service IP) in the URL/Address field of a web browser. You should have two browsers open. The web console for the Standby (inactive) CAM only displays a subset of the module menus and respective submenus available on the Active CAM.

Note   The CAM configured as HA-Primary may not be the currently Active CAM.

Determining Primary and Secondary CAM

In each CAM web console, go to **Administration > CCA Manager > Failover**.

- The Primary CAM is the CAM you configured as the **HA-Primary** when you initially set up HA.
- The Secondary CAM is the CAM you configured as the **HA-Secondary** when you initially set up HA.

✎
Note   For releases prior to 4.0(0), the Secondary CAM is labeled as **HA-Standby** (CAM) for the initial HA configuration.

Adding High Availability Cisco NAC Appliance To Your Network

The following diagrams illustrate how HA-CAMs and HA-CASs can be added to an example core-distribution-access network (with Catalyst 6500s in the distribution and access layers).

Figure 16-6 shows a network topology without Cisco NAC Appliance, where the core and distribution layers are running HSRP (Hot Standby Router Protocol), and the access switches are dual-homed to the distribution switches.

Figure 16-6   Example Core-Distribution-Access Network Before Cisco NAC Appliance
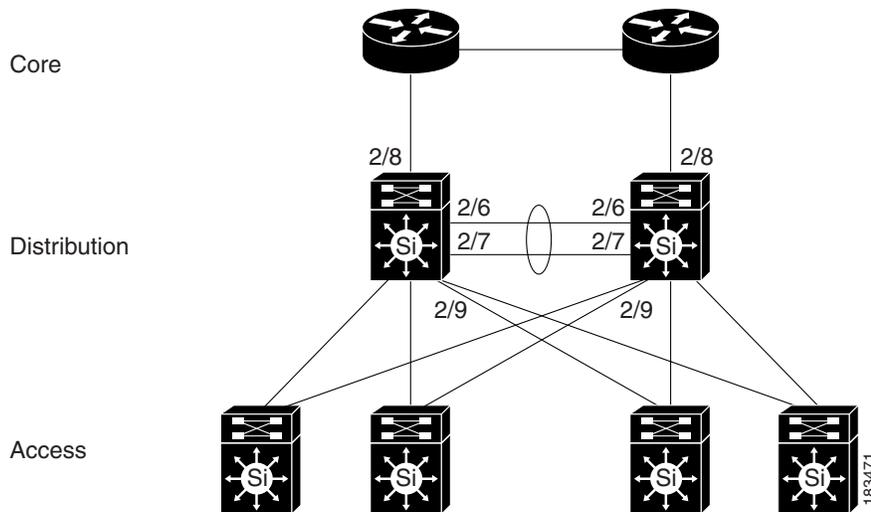

Figure 16-7 shows how HA-CAMs can be added to the core-distribution-access network. In this example, the HA heartbeat connection is configured over both serial and eth1 interfaces.
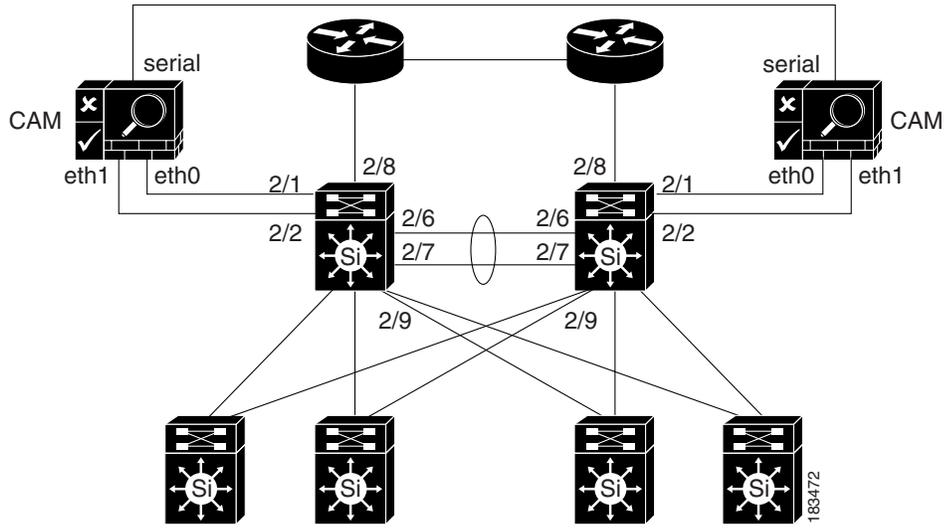
Figure 16-7   Adding HA CAMs to Network

Figure 16-8 shows how HA-CASs can be added to the core-distribution-access network. In this example, the CAS is configured as an L2 OOB Virtual Gateway in Central Deployment. The HA heartbeat connection is configured over both a serial interface and a dedicated eth2 interface. Link-failure based failover connection can also be configured over the eth0 and/or eth1 interfaces.

Note   Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

Figure 16-8   Adding HA CAS to Network