



CHAPTER 15

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:

- [Overview, page 15-1](#)
- [Before Starting, page 15-3](#)
- [Connect the Clean Access Manager Machines, page 15-4](#)
- [Configure the HA-Primary CAM, page 15-5](#)
- [Configure the HA-Secondary CAM, page 15-9](#)
- [Upgrading an Existing Failover Pair, page 15-11](#)
- [Failing Over an HA-CAM Pair, page 15-11](#)
- [Useful CLI Commands for HA, page 15-12](#)
- [Adding High Availability Cisco NAC Appliance To Your Network, page 15-13](#)

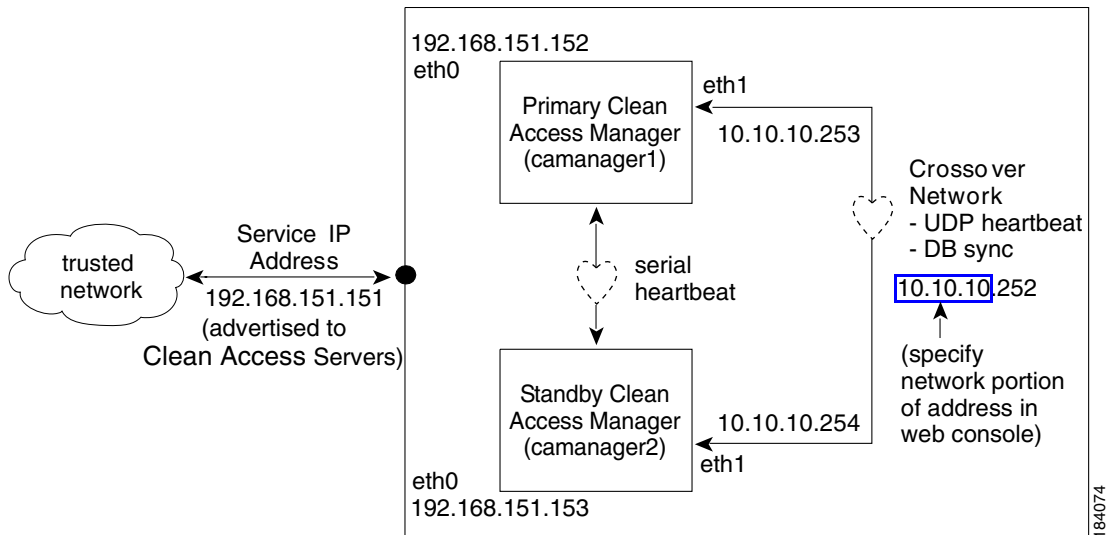
Overview

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 active CAM's database.
- Both CAMs share a virtual Service IP for the eth0 trusted interface. The Service IP should be used for the SSL certificate.
- The primary and secondary CAM machines exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.
- The eth1 interface and/or serial interface on the CAMs can be used for heartbeat packets and database synchronization. If both eth1 and serial interfaces are configured for heartbeat, both interfaces need to fail for failover to occur.

[Figure 15-1](#) illustrates a sample configuration.

Figure 15-1 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 In HA Deployment](#), page 14-35.

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 and to the Clean Access Servers 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 crossover network on which high-availability 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 HA crossover network 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 that the CAM always uses eth1 as the UDP heartbeat interface.

For extra security, 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.

**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 2-7.](#))
- 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.
- 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 a 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 security, it is highly recommended to add a serial heartbeat connection between the Clean Access Manager peers. The serial connection provides an additional dedicated heartbeat exchange method that must fail before the standby system can take over. However, note that the eth1 connection between the CAM peers is mandatory.

Physically connect the peer Clean Access Managers as follows:

- Use 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.

**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.

**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.

You can enable/disable the serial port using the **Disable Serial Login** checkbox on the HA CAM settings (under **Administration > Clean Access Manager > Network & Failover | Failover Settings | Disable Serial Login**). When there is only one serial port on the CAM machine, this checkbox allows administrators to disable serial login on COM1 so that it can be used as the Heartbeat Serial Interface for a pair of HA-Clean Access Managers.

**Note**

Serial login is **enabled** by default on the CAM. If you are using COM1 for the Heartbeat Serial Interface of the CAM, you must click the **Disable Serial Login** checkbox to disable serial login on COM1.

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 15-1](#) for a sample configuration example.

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 Certificate** to configure the SSL certificate for the primary CAM. The **Generate Temporary Certificate** form appears.

**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. Complete the **Generate Temporary Certificate** form and click **Generate**. The certificate must be generated for the Service IP address of the HA pair.
- b. When finished generating the temporary certificate, choose **Export CSR/Private Key/Certificate** from the **Choose an action** menu.
- c. Click the **Export** button for **Currently Installed Private Key** to export the SSL private key. Save the key file to disk. You will have to import this key into the HA-Secondary CAM later.
- d. Click the **Export** button for **Currently Installed Certificate** to export the current SSL certificate. Save the certificate file to disk. You will have to import this certificate file into the HA-Secondary CAM later.

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

**Note**

The CA-signed certificate must either be based on the Service IP or a hostname/domain name resolvable to the Service IP through DNS. See [Manage CAM SSL Certificates, page 14-5](#) for details.

- a. Select **Import Certificate** from the **Choose an action:** menu.
- b. Use the **Browse** button next to the **Certificate File** field and navigate to the CA-signed cert.
- c. Choose **CA-signed PEM-encoded X.509 Cert** from the **File Type** dropdown menu:
- d. Click **Upload** to import the certificate. Note that you will need to import this same certificate into the HA-Secondary CAM later.
- e. Click **Verify and Install Uploaded Certificates**.

- f. Select **Export CSR/Private Key/Certificate** from the **Choose an action** dropdown list.
 - g. Click the **Export** button for the **Currently Installed Private Key** to export the SSL private key associated with the CA-signed certificate. Save the key file to disk. You will need to import this file into the HA-Secondary CAM later.
2. Go to **Administration > CCA Manager** and click the **Network & Failover** tab. Choose the **HA-Primary** option from the **High-Availability Mode** dropdown menu. The high availability settings appear:

Figure 15-2 Network & Failover Settings for the CAM

The screenshot shows the 'Administration > Clean Access Manager' interface. The 'Network & Failover' tab is selected. The 'Network Settings' section includes fields for IP Address (192.168.151.151), Subnet Mask (255.255.255.0), Default Gateway (192.168.151.1), Host Name (camanager1), Host Domain (cisco.com), and DNS Servers (63.93.96.20). The 'Failover Settings' section is highlighted with a red box and labeled 'HA settings'. It includes a dropdown for High-Availability Mode set to 'HA-Primary', a note '(for high availability, set up the primary server before the secondary server)', fields for Service IP Address and Peer Host Name, a dropdown for Heartbeat UDP Interface set to 'eth1', a dropdown for Heartbeat Serial Interface set to 'N/A', a checked checkbox for 'Disable Serial Login', and a note '(Serial Login disabled by default when HA mode selected)'. Below this is the 'Crossover Network Interface Setting' section with fields for Crossover Network (empty) and Crossover Netmask (255.255.255.252). 'Update' and 'Reboot' buttons are at the bottom.

3. Copy the value from the **IP Address** field under **Network Settings** and enter it in **Service IP Address** field. The Network Settings IP Address is the existing IP address of the current 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 for the Clean Access Manager pair.

183486

Figure 15-3 Configuring the Service IP

Administration > Clean Access Manager

Network & Failover | System Time | SSL Certificate | System Upgrade

Network Settings

IP Address: 192.168.151.151

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.151.1

Host Name: camanager1

Host Domain: perfigo.com

DNS Servers: 63.93.96.20
(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode: HA-Primary
(For high availability, set up the primary server before the standby)

Service IP Address: 192.168.151.151

Peer Host Name:

Heartbeat UDP Interface: eth1

Heartbeat Serial Interface: N/A
(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

Crossover Network Interface Setting

Crossover Network: .252

Crossover Netmask: 255.255.255.252

Update Reboot

183483

4. Change the **IP address** under **Network Settings** to an available address (for example *n.152*)

Figure 15-4 Configuring New IP Address

Administration > Clean Access Manager

Network & Failover | System Time

Network Settings

IP Address: 192.168.151.152 — New IP address

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.151.1

183484

5. Each Clean Access Manager must have a unique host name (such as `camanager1` and `camanager2`). Type the host name of the HA-Primary CAM in the **Host Name** field under **Network Settings**, and type the host name of the HA-Secondary CAM in the **Peer Host Name** field under **Failover Settings**.

Figure 15-5 Example Primary Clean Access Manager Failover Settings

Administration > Clean Access Manager

Network & Failover | System Time | SSL Certificate | System Upgrade | Licensing | Support Logs

Network Settings

IP Address: 192.168.151.152
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.151.1
 Host Name: **camanager1**
 Host Domain: cisco.com
 DNS Servers: 63.93.96.20
(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode: HA-Primary
(for high availability, set up the primary server before the secondary server)
 Service IP Address: 192.168.151.151
 Peer Host Name: **camanager2**
 Heartbeat UDP Interface: eth1
 Heartbeat Serial Interface: COM1 [port:3F8,irq:4]
(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)
 Disable Serial Login:
(Serial Login disabled by default when HA mode selected)

Crossover Network Interface Setting

Crossover Network: 10.10.10.252
 Crossover Netmask: 255.255.255.252

Update Reboot

Primary CAM host name
 Secondary CAM host name

183485

**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.

6. 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.
7. If your machine only has one serial port and you are using COM1 as the Heartbeat Serial Interface, you must check the **Disable Serial Login** checkbox to ensure serial login is disabled on COM1. See [Serial Connection](#), page 15-4 for further details.
8. To maintain synchronization, the Clean Access Manager peers exchange data by a crossover network. You must specify a private network address space not currently routed in your organization in the **Crossover Network** field (such as 10.10.10). The default crossover network provided is 192.168.0.252. If this address conflicts with your network, make sure to specify a different private address space. For example, if your organization uses the private network 192.168.151.0, use 10.1.1.x as the crossover network. The subnet mask and last octet of the IP address are fixed, so only enter the network portion of the IP address in the **Crossover Network** field.
9. 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

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 Certificate**.
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 15-5](#)).
3. Import the HA-Primary CAM's private key file and certificate as described below:
 - a. In the **SSL Certificate** tab, choose **Import Certificate** from the **Choose an action:** menu
 - b. Click **Browse** next to the **Certificate File** field, and browse to your backup copy of the private key file generated with the certificate that will be used for the HA pair.
 - c. Choose **Private Key** as the File Type.
 - d. Click **Upload** to upload the private key.
 - e. With **Import Certificate** selected from the **Choose an action:** menu, browse to the certificate (temporary or CA-signed) associated with the private key.
 - f. Choose **CA-signed PEM-encoded X.509 Cert** as the File Type.
 - g. Click **Upload** to upload the temporary certificate or CA-signed certificate.
 - h. Click **Verify and Install Uploaded Certificates**.

See [Manage CAM SSL Certificates, page 14-5](#) for details.
4. Go to the **Administration > CCA Manager > Network & Failover | Network Settings** 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 *n.153*).

Figure 15-6 Example HA-Secondary Clean Access Manager Failover Settings

The screenshot shows the 'Administration > Clean Access Manager' configuration page. The 'Network & Failover' tab is selected. The page is divided into three main sections: Network Settings, Failover Settings, and Crossover Network Interface Setting.

Network Settings:

- IP Address: 192.168.151.153
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.151.1
- Host Name: camanager2
- Host Domain: cisco.com
- DNS Servers: 63.93.96.20 (separate multiple addresses with a comma)

Failover Settings:

- High-Availability Mode: HA-Secondary (for high availability, set up the primary server before the secondary server)
- Service IP Address: 192.168.151.151
- Peer Host Name: camanager1
- Heartbeat UDP Interface: eth1
- Heartbeat Serial Interface: COM1 [port:3F8,irq:4] (HA on eth1 interface is enabled by default. A serial port can additionally be configured.)
- Disable Serial Login: (Serial Login disabled by default when HA mode selected)

Crossover Network Interface Setting:

- Crossover Network: 10.10.10.252
- Crossover Netmask: 255.255.255.252

Buttons for 'Update' and 'Reboot' are located at the bottom right of the configuration area.

- Set the **Host Name** value under **Network Settings** to the same value set for the **Peer Host Name** in the HA-Primary CAM configuration. See [Figure 15-5 on page 15-8](#).

**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.

- Choose **HA-Secondary** in the **High-Availability Mode** dropdown menu. The high availability settings appear.
- Set the **Service IP Address** value under **Failover Settings** to the same value set for the **Service IP Address** in the HA-Primary CAM configuration.
- Set the **Peer Host Name** value under **Failover Settings** to the HA-Primary CAM's host name.
- 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.

**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.

- If your machine only has one serial port and you are using COM1 as the Heartbeat Serial Interface, you must check the **Disable Serial Login** checkbox to ensure serial login is disabled on COM1. See [Serial Connection, page 15-4](#) for further details.
- Type the same **Crossover Network Interface Settings** as you entered for the HA-Primary CAM.
- Click **Update** and then **Reboot**.

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

Finally, open the admin console for the standby again and complete the configuration as follows. Notice that the admin console for the standby now has only one management module.

Figure 15-7 Standby Web Admin Console



Complete the Configuration

1. Verify settings in the **Network & Failover** page for the standby CAM.

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 CCA release, see “Upgrading High Availability Pairs” in the appropriate [Release Notes](#).

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 [Using the Command Line Interface \(CLI\)](#), page 2-10.

Useful CLI Commands for HA

The following are useful directories 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@cam1 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       cam1
node       cam2
```

How to Verify 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 generally find the `fostate.sh` command from the `/store` directory of your last upgrade, for example, `/store/cca_upgrade-4.x.x`.

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

```
[root@cam1 cca_upgrade-4.x.x]# ./fostate.sh
My node is active, peer node is standby
[root@cam1 cca_upgrade-4.x.x]#
```

This CAM is the active CAM in the HA-pair

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

```
[root@cam2 cca_upgrade-4.x.x]# ./fostate.sh
My node is standby, peer node is active
[root@cam2 cca_upgrade-4.x.x]#
```

This CAM is the standby CAM in the HA-pair

How to Verify Primary/Secondary Configuration Status on the HA CAM

The following example shows how to use the CLI to determine the HA mode (Primary/Secondary) for which each CAM was initially configured in the HA pair.

1. Find the name of the CAMs (nodes) with `/etc/ha.d/ha.cf`.
2. Then check status on each CAM, for example:


```
[root@cam1 ~]# /perfigo/control/bin/check-ha cam1
active
[root@cam1 ~]# /perfigo/control/bin/check-ha cam2
active
```
3. Go to `/perfigo/control/tomcat` and perform `ls -la`:
 - If `webapps` is pointing to `normal-webapps`, it is the primary CAM
 - If `webapps` is pointing to `admin-webapps`, it is the secondary CAM

For example, this CAM is the primary CAM:

```
[root@cam1 tomcat]# cd /perfigo/control/tomcat
[root@cam1 tomcat]# ls -la
total 216
drwxr-xr-x 12 root root 4096 Sep 14 23:28 .
drwxr-xr-x  8 root root 4096 Aug 28 22:12 ..
drwxr-xr-x  4 root root 4096 Aug 28 22:12 admin-webapps
<output cut...>
drwxr-xr-x  2 root root 4096 Aug 28 22:12 temp
lrwxrwxrwx  1 root root   38 Sep 14 23:28 webapps ->
/perfigo/control/tomcat/normal-webapps
drwxr-xr-x  3 root root 4096 Aug 28 15:15 work
```

This CAM is the secondary CAM:

```
[root@cam2 tomcat]# ls -la
total 216
drwxr-xr-x 12 root root 4096 Sep 14 23:33 .
drwxr-xr-x  8 root root 4096 Sep 15 2006 ..
drwxr-xr-x  4 root root 4096 Sep 15 2006 admin-webapps
<output cut ...>
drwxr-xr-x  2 root root 4096 Sep 15 2006 temp
lrwxrwxrwx  1 root root   37 Sep 14 23:33 webapps ->
/perfigo/control/tomcat/admin-webapps
drwxr-xr-x  3 root root 4096 Sep 14 23:25 work
```

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 15-8 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 15-8 Example Core-Distribution-Access Network Before Cisco NAC Appliance

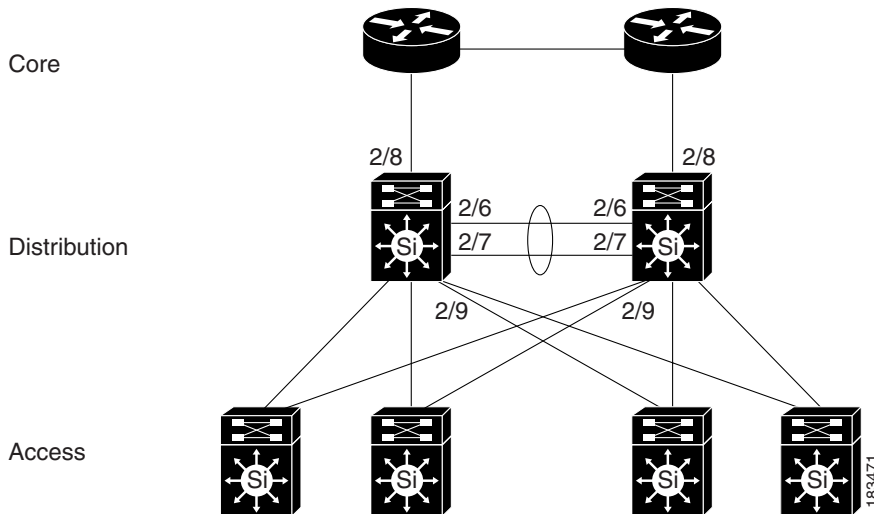


Figure 15-9 shows how HA-CAMs can be added to the core-distribution-access network. In this example, the HA heartbeat connection is configured over both serial and eth1 interfaces.

Figure 15-9 Adding HA CAMs to Network

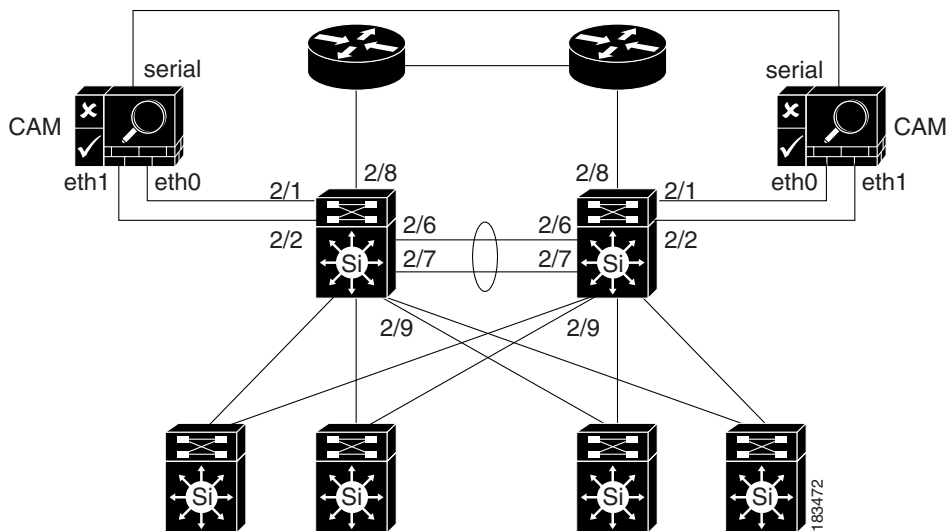


Figure 15-10 shows how HA-CASs can be added to the core-distribution-access network. In this example, the CAS is configured as an L2 OOB Virtual Gateway in Central Deployment. The HA heartbeat connection is configured over both a serial interface and a dedicated eth2 interface. Link-failure based failover connection can also be configured over the eth0 and/or eth1 interfaces.

Figure 15-10 Adding HA CAS to Network

