CHAPTER 4

Configuring High Availability (HA)

This chapter covers the following topics:

- Adding High Availability Cisco NAC Appliance To Your Network, page 4-1
- Installing a Clean Access Manager High Availability Pair, page 4-3
- Installing a Clean Access Server High Availability Pair, page 4-16
- Useful CLI Commands for HA, page 4-39

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 4-1 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 4-1 Example Core-Distribution-Access Network Before Cisco NAC Appliance

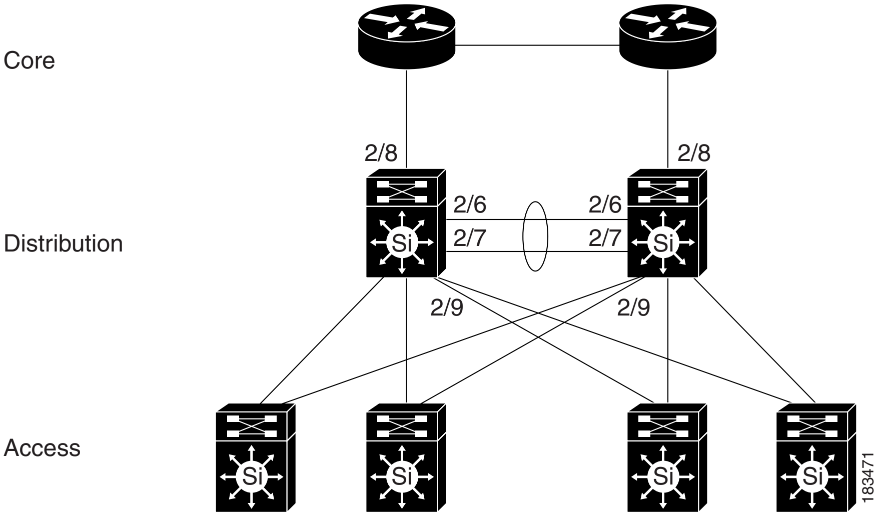


Figure 4-2 shows how HA-CAMs can be added to the core-distribution-access network. In this example, the HA heartbeat connection is configured over both serial and eth1 interfaces.

Figure 4-2 Adding HA CAMs to Network

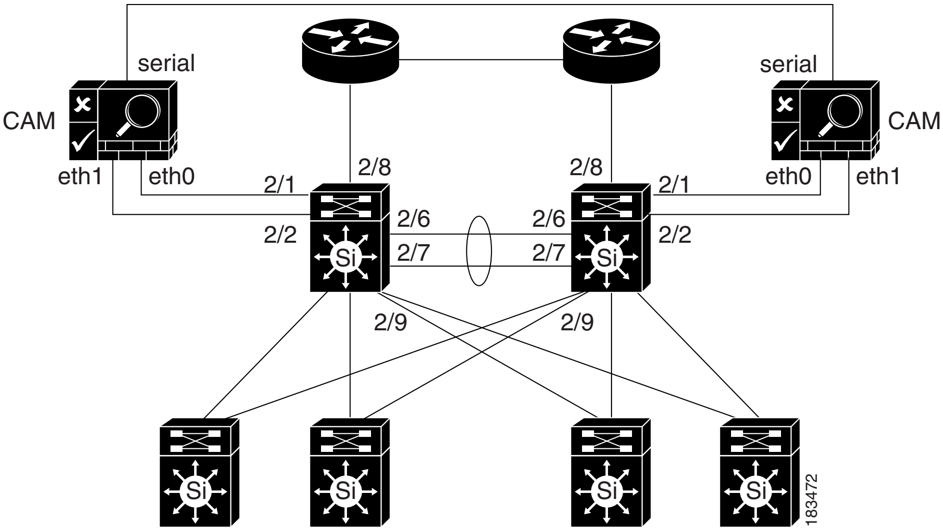
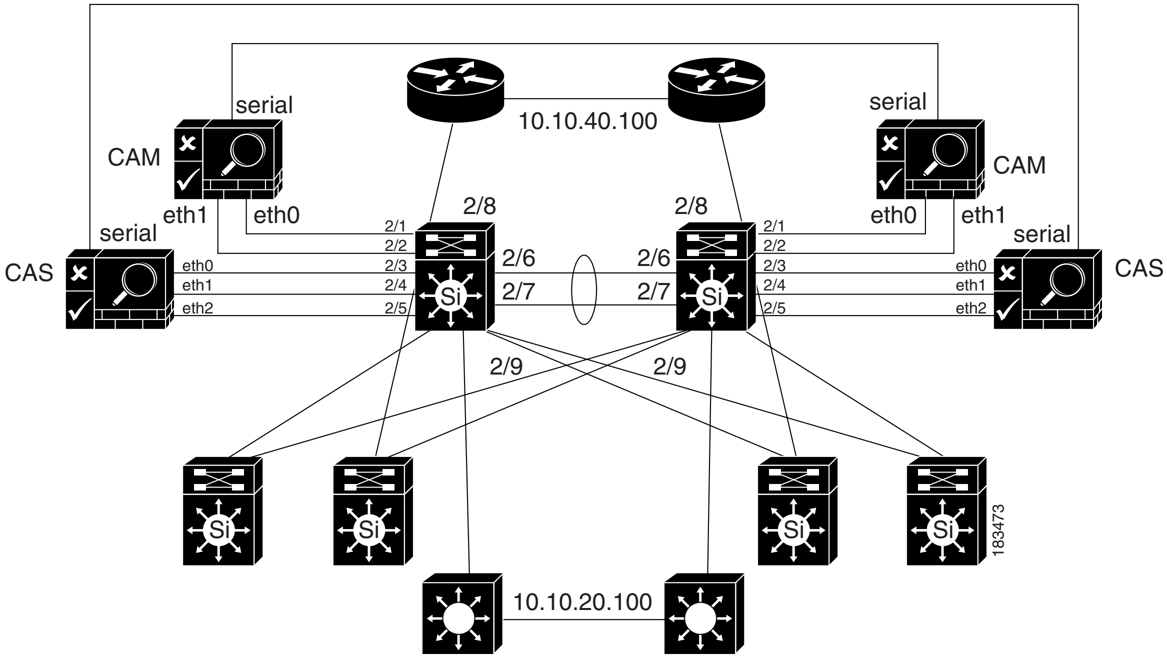


Figure 4-3 shows how HA-CASs can be added to the core-distribution-access network. In this example, the CAS is configured as an L2 OOB Virtual Gateway in Central Deployment. The HA heartbeat connection is configured over both a serial interface and a dedicated eth2 interface. Link-failure based failover 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 4-3 Adding HA CAS to Network



Installing a Clean Access Manager High Availability Pair

This section 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 the "Backing Up and Restoring CAM/CAS Authorization Settings" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)* to ensure you are able to *exactly* duplicate your Authorization settings from one CAM to its high availability counterpart.

- Clean Access Managers and Clean Access Servers use a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to fail over to the HA peer CAM/CAS in HA deployments. (HA-Secondary CAMs/CASs are not able to assume the "active" role following a failover event when the master secret passwords are different.)
- 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.
- To support FIPS 140-2 compliance, HA CAMs/CASs automatically establish an IPSec tunnel to ensure all communications between the HA Pair appliances remains secure across the network.
- 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.
- Newer Cisco NAC-3310 CAMs/CASs feature a 160GB hard drive, while older NAC-3310s originally shipped with 80GB hard drives. Both of these hard drive sizes support High Availability (HA) deployments, and you can safely deploy a 160GB model in an HA pair with an 80GB model.
- 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.

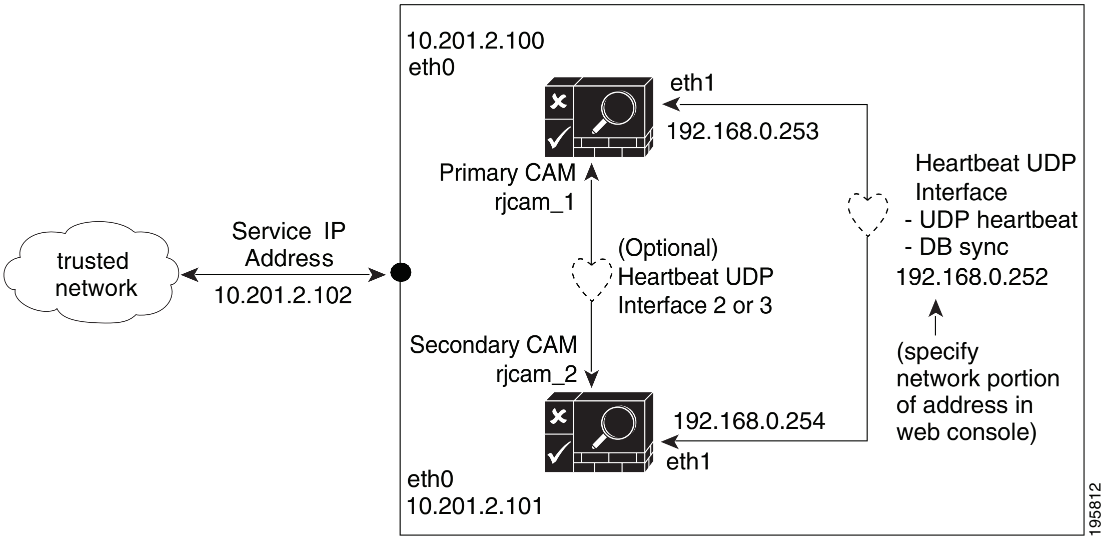
Note If you are configuring your CAM for HA, you must use eth1 for heartbeat and database synchronization. All other Ethernet interfaces (eth0 and eth2/eth3) are optional for this purpose.

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 4-4 illustrates a sample configuration.

Figure 4-4 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 the "Restoring Configuration from CAM Snapshot—HA-CAM or HA-CAS" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)*.

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.

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 Cisco NAC Appliance CAMs/CASs 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 CAM Configuration, page 3-6).
- 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” section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)* 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 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).
- 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

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 Cisco NAC Appliance CAMs/CASs 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 4-4 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:

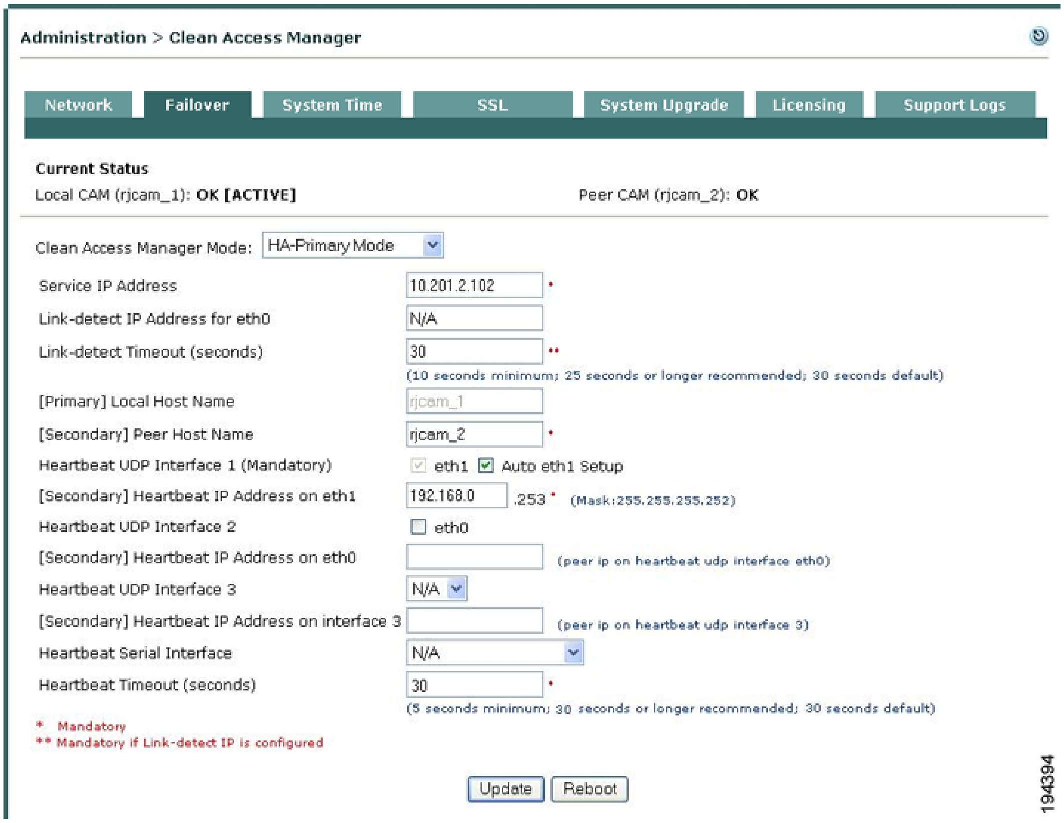
Note This process assumes you have already generated a Certificate Signing Request and accompanying Private Key, submitted the request to your Certificate Authority, and have received your CA-signed certificate. If you have not yet obtained a CA-signed certificate for the CAS, be sure to follow the instructions in the "Manage CAM SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)* 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 4-5 HA-Primary Clean Access Manager Failover Settings



Current Status
Local CAM (rjcam_1): **OK [ACTIVE]**
Peer CAM (rjcam_2): **OK**

Clean Access Manager Mode: HA-Primary Mode

Service IP Address	10.201.2.102 *
Link-detect IP Address for eth0	N/A
Link-detect Timeout (seconds)	30 ** (10 seconds minimum; 25 seconds or longer recommended; 30 seconds default)
[Primary] Local Host Name	rjcam_1
[Secondary] Peer Host Name	rjcam_2 *
Heartbeat UDP Interface 1 (Mandatory)	☑ eth1 ☑ Auto eth1 Setup
[Secondary] Heartbeat IP Address on eth1	192.168.0 .253 * (Mask:255.255.255.252)
Heartbeat UDP Interface 2	□ eth0
[Secondary] Heartbeat IP Address on eth0	(peer ip on heartbeat udp interface eth0)
Heartbeat UDP Interface 3	N/A
[Secondary] Heartbeat IP Address on interface 3	(peer ip on heartbeat udp interface 3)
Heartbeat Serial Interface	N/A
Heartbeat Timeout (seconds)	30 * (5 seconds minimum; 30 seconds or longer recommended; 30 seconds default)

* Mandatory
** Mandatory if Link-detect IP is configured

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.

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

Step 10 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 11 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 4-8).

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.

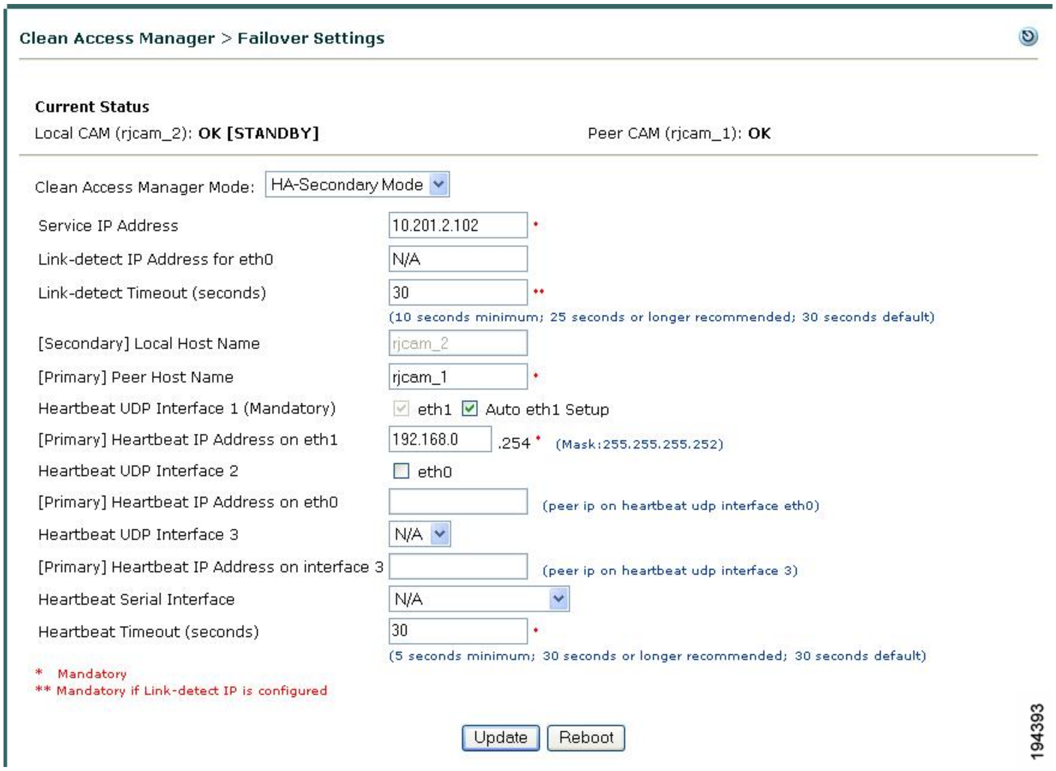
b. Select the CA-signed certificate file and click **Import**.

c. Repeat the process to import the Private Key.

For more information, see the "Manage CAM SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)*.

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 4-6 HA-Secondary Clean Access Manager Failover Settings



Clean Access Manager > Failover Settings

Current Status

Local CAM (rjcam_2): **OK [STANDBY]** Peer CAM (rjcam_1): **OK**

Clean Access Manager Mode:	HA-Secondary Mode
Service IP Address	10.201.2.102 *
Link-detect IP Address for eth0	N/A
Link-detect Timeout (seconds)	30 ** (10 seconds minimum; 25 seconds or longer recommended; 30 seconds default)
[Secondary] Local Host Name	rjcam_2
[Primary] Peer Host Name	rjcam_1 *
Heartbeat UDP Interface 1 (Mandatory)	☑ eth1 ☑ Auto eth1 Setup
[Primary] Heartbeat IP Address on eth1	192.168.0 .254 * (Mask:255.255.255.252)
Heartbeat UDP Interface 2	☐ eth0
[Primary] Heartbeat IP Address on eth0	(peer ip on heartbeat udp interface eth0)
Heartbeat UDP Interface 3	N/A
[Primary] Heartbeat IP Address on interface 3	(peer ip on heartbeat udp interface 3)
Heartbeat Serial Interface	N/A
Heartbeat Timeout (seconds)	30 * (5 seconds minimum; 30 seconds or longer recommended; 30 seconds default)

* Mandatory
** Mandatory if Link-detect IP is configured

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 4-4 on page 4-5.

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.

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

Step 13 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.

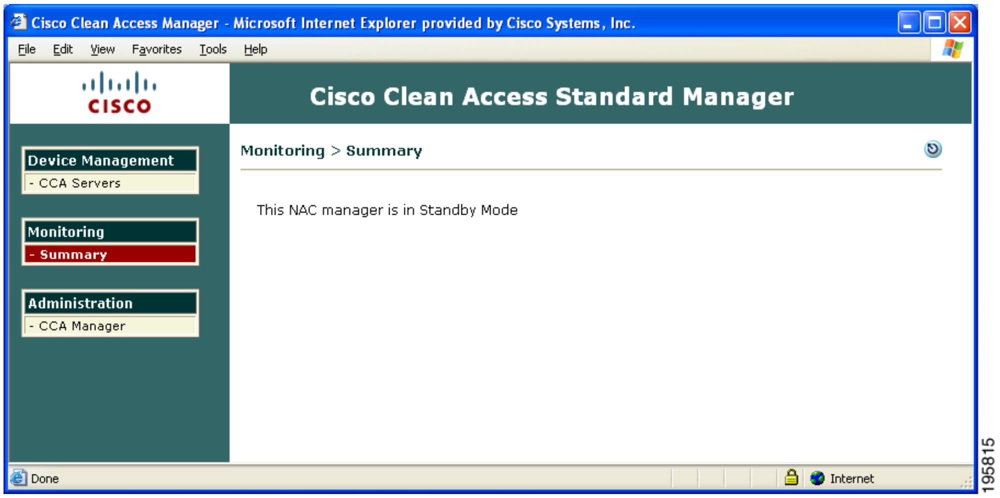
Warning **When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for Cisco NAC Appliance CAMs/CASs and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System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

Step 14 Click **Update** and then **Reboot**.

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

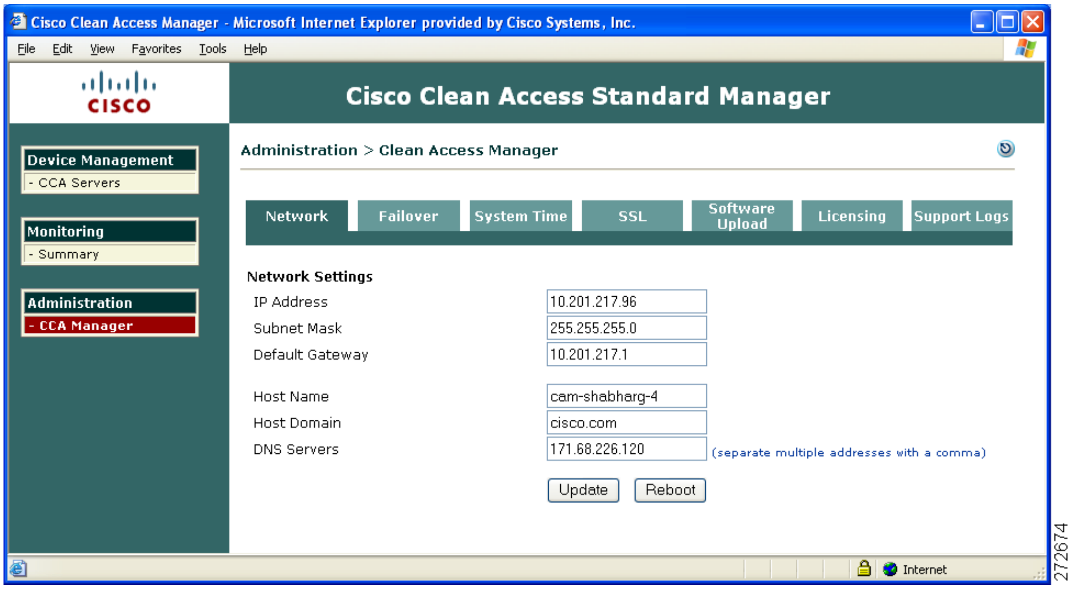
Step 15 Finally, open the admin console for the standby again and complete the configuration as follows. Notice that the admin console for the standby CAm displays limited management modules (Figure 4-7 and Figure 4-8).

Figure 4-7 Standby Web Admin Console Example—Summary Page


Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
CISCO
Cisco Clean Access Standard Manager
Device Management
- CCA Servers
Monitoring
- Summary
Administration
- CCA Manager
Monitoring > Summary
Done
Internet
195815

This NAC manager is in Standby Mode

Figure 4-8 Standby Web Admin Console Example—CCA Manager > Network Page


Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
CISCO
Cisco Clean Access Standard Manager
Device Management
- CCA Servers
Monitoring
- Summary
Administration
- CCA Manager
Administration > Clean Access Manager
Network
Failover
System Time
SSL
Software Upload
Licensing
Support Logs
Update
Reboot
Internet
272674

Network Settings

IP Address	10.201.217.96
Subnet Mask	255.255.255.0
Default Gateway	10.201.217.1
Host Name	cam-shabharg-4
Host Domain	cisco.com
DNS Servers	171.68.226.120 (separate multiple addresses with a comma)

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 4.7(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 Useful CLI Commands for HA, page 4-39.

Accessing High Availability Pair CAM 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.

Installing a Clean Access Server High Availability Pair

This chapter describes how to set up two Clean Access Servers in high availability (HA) mode.By deploying Clean Access Servers in high-availability mode, you can ensure that important user authentication and connection 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

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

The following key points provide a high-level overview of HA-CAS operation:

- The Clean Access Server high-availability mode is an Active/Passive two-server configuration in which a standby CAS machine acts as a backup to an active CAS machine.
- The active CAS performs all tasks for the system. Since most of the CAS configuration is stored on the CAM, when CAS failover occurs, the CAM pushes the configuration to the newly-active CAS.

  Note If you use the Authorization feature in a CAS HA-pair, follow the guidelines in “Backing Up and Restoring CAM/CAS Authorization Settings” in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1)* to ensure you are able to exactly duplicate your Authorization settings from one CAS to its high availability counterpart.

- Clean Access Managers and Clean Access Servers use a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to fail over to the HA peer CAM/CAS in HA deployments. (HA-Secondary CAMs/CASs are not able to assume the “active” role following a failover event when the master secret passwords are different.)
- The standby CAS does not forward any packets between its interfaces.
- The standby CAS monitors the health of the active CAS via heartbeat interface (serial and one or more UDP interfaces). Heartbeat packets can be sent on the dedicated eth2 interface, dedicated eth3 interface, or eth0/eth1 interface (if no eth2 or eth3 interface is available).
- The primary and secondary CAS machines exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.
- In addition to heartbeat-based failover, the CAS also provides link-based failover based on eth0 or eth1 link failure. The CAS sends ICMP ping packets to an external IP address via the eth0 and/or eth1 interface. Failover will occur if only one CAS can ping the external addresses.

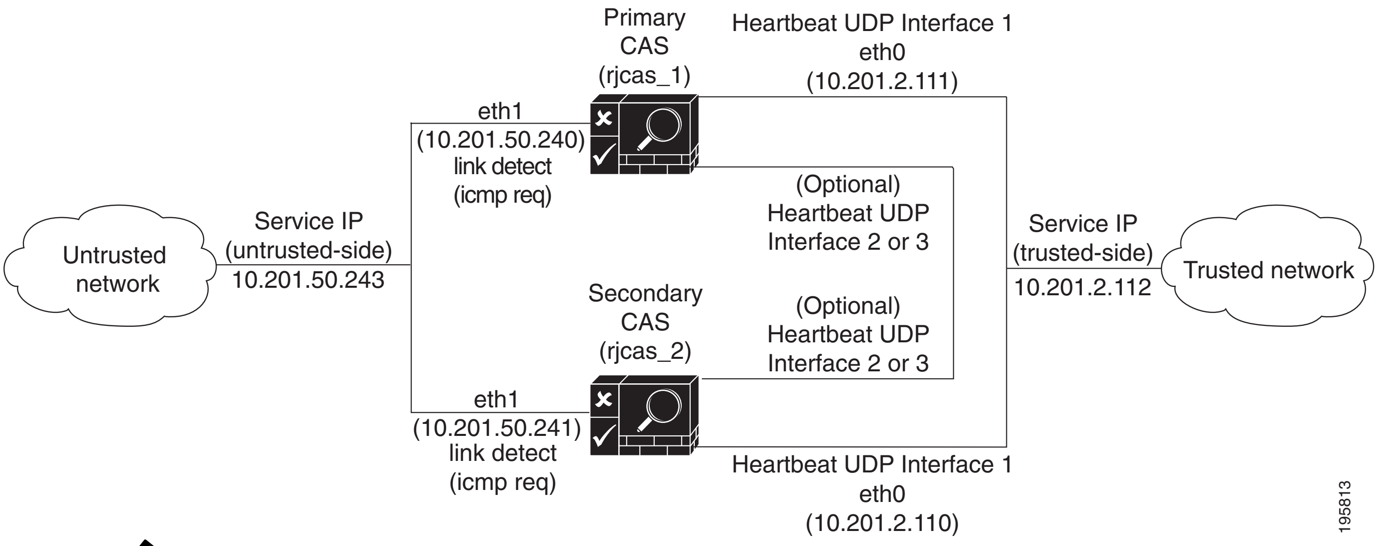
  Note The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

- Both Clean Access Servers share a virtual Service IP for the eth0 trusted interface and eth1 untrusted interface. The Service IP should be used for SSL certificates.
- Newer Cisco NAC-3310 CAMs/CASs feature a 160GB hard drive, while older NAC-3310s originally shipped with 80GB hard drives. Both of these hard drive sizes support High Availability (HA) deployments, and you can safely deploy a 160GB model in an HA pair with an 80GB model.
- To support FIPS 140-2 compliance, HA CAMs/CASs automatically establish an IPSec tunnel to ensure all communications between the HA Pair appliances remains secure across the network.
- Starting from release 4.5(1), when a standby CAS assumes the role of an active CAS that is performing DHCP address management and has gone into Fallback state, the new active CAS also assumes DHCP functions in addition to user login.

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 4-9 illustrates the basic connections in an example HA-CAS configuration.

Figure 4-9 Clean Access Server Example High-Availability Configuration


Primary CAS (rjcas_1)
Heartbeat UDP Interface 1 eth0 (10.201.2.111)
eth1 (10.201.50.240) link detect (icmp req)
(Optional) Heartbeat UDP Interface 2 or 3
Untrusted network
Service IP (untrusted-side) 10.201.50.243
Service IP (trusted-side) 10.201.2.112
Trusted network
Secondary CAS (rjcas_2)
(Optional) Heartbeat UDP Interface 2 or 3
eth1 (10.201.50.241) link detect (icmp req)
Heartbeat UDP Interface 1 eth0 (10.201.2.110)
195813

Note "Primary/Secondary" denotes the server mode when it is configured for HA. "Active/Standby" denotes the runtime status of the server.

When first configuring the HA peers, you must specify an HA-Primary CAS and HA-Secondary CAS. Initially, the HA-Primary is the active CAS, and the HA-Secondary is the standby (passive) CAS. If a failover event occurs, such as the active CAS shuts down or stops responding to the peer's heartbeat signal, the standby assumes the role of the active CAS.

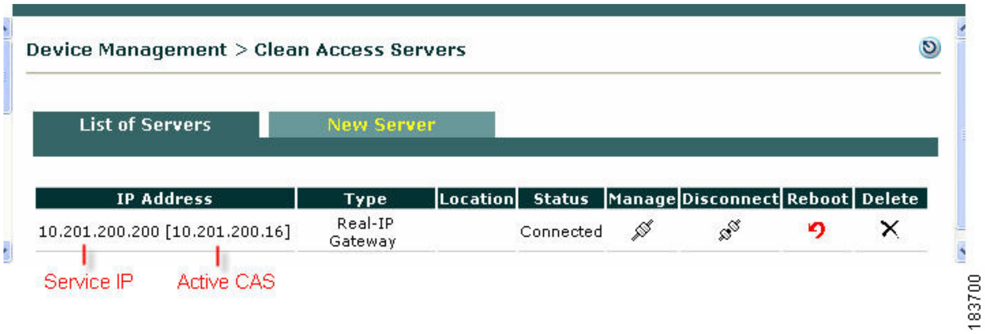
Note If *both* the HA-Primary and HA-Secondary CASs in your HA deployment lose their configuration, you can restore the system using the guidelines in the “Restoring Configuration from CAM Snapshot In HA Deployment” section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(1).*

When the CAS starts up again, it checks to see if its peer is active. If the peer is active, the starting CAS becomes the standby. If the peer is not active, then the starting CAS assumes the active role.

Typically, Clean Access Servers are configured as an HA pair at the same time, but you can add a new Clean Access Server to an existing standalone CAS to create a high-availability pair. In order for the pair to appear to the network and to the Clean Access Manager as one entity, you must specify a **Service IP Address** for the trusted interface (eth0) and a Service IP address for untrusted interface (eth1) of the pair.

Use the Service IP of the CASs to add the CAS to the CAM. Figure 4-10 shows how the active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair in the **List of Servers** in the CAM web console. In addition, either the trusted or untrusted interface Service IP address should be used to generate the SSL certificate.

Figure 4-10 Active CAS in an HA-Pair



IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.200.200 [10.201.200.16]	Real-IP Gateway		Connected				✕

Note If a CAS was previously configured and added to the CAM as a standalone CAS, it must be deleted prior to configuring it for HA. After HA configuration is complete on both CASs, the Service IP is then entered in the **New Server** form to add the HA-CAS pair to the CAM.

Note To ensure heartbeat redundancy, Cisco recommends configuring optional Heartbeat UDP Interface 2 or 3 between the HA CASs in your deployment.

Failover Events

- If multiple heartbeat UDP interfaces are configured, then they must all fail for the standby system to take over. See Physical Connection, page 4-21 for additional details.
- If the CAS is unable to communicate with the CAM:
  - Users that are already connected will not be affected.
  - New users will not be able to log in.

- You can configure link-based failover. Two IP addresses that are external to the CAS are configured for Link-detect: one on the trusted network, the other on the untrusted network.
  - The active and standby CAS will send ICMP ping packets via eth0 to the IP address on the trusted network.
  - The active and standby CAS will send ICMP ping packets via eth1 to the IP address on the untrusted network.

Note If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the **/etc/ha.d/linkdetect.conf** file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See Link-Detect Interfaces, page 4-41 for more details.

The status of these ping packets is communicated between the CASs via the heartbeat signal:

  - If the active and standby CAS can ping both external IPs, no failover occurs
  - If the active and standby CAS cannot ping either of the external IPs, no failover occurs
  - If the active CAS cannot ping either of the external IPs, but the standby CAS can ping them, failover occurs

- 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.

Choosing External IPs for Link-Based Failover

- Keep in mind that when the CAS initiates traffic, it will always send packets out of its untrusted (eth1) interface except for packets destined to its default gateway. Therefore, when choosing an external IP on trusted network for CAS to ping via the eth0 interface, choose any IP belonging to a subnet other than the CAS subnet.
- When choosing an external IP on the untrusted network for CAS to ping via the eth1 interface:
  - This IP has to exist on the CAS management subnet
  - It cannot be the default gateway of the CAS
  - The CAS will send these ping packets out of the eth1 interface
  - Verify whether **Set Management VLAN ID** is enabled for the eth1 interface. If this option is not enabled, CAS will send traffic out untagged on the eth1 interface. The switch will determine whether these packets should be received on its native VLAN. Therefore, on the untrusted interface, ensure that the native VLAN is being forwarded.
  - The external IP address will be in the CAS management subnet, but on the untrusted side, the traffic will be going out from the CAS in the native VLAN; hence ensure the native VLAN is being forwarded towards the external IP device.

Refer to c. Configure HA-Primary Mode and Update, page 4-26 and c. Configure HA-Secondary Mode and Update, page 4-32 for additional configuration details.

CAS High Availability Requirements

This section describes addition planning considerations when implementing high availability.

Note In a CAS HA deployment using NAT on the trusted (eth0) side, you must ensure that the -Dperfigo.nat.serviceip=<*NAT'ed service IP or CAS service hostname*> property is set for the **starttomcat** and **restartweb** files on both the Primary and Secondary CAS.

For example, `-Dperfigo.nat.serviceip=172.10.20.100`.

Physical Connection

Cisco recommends using a **dedicated** connection for failover heartbeat on Clean Access Server high-availability pairs. You can use:

- A dedicated Ethernet NIC card, configured as the eth2 or eth3 interface of the CAS

Note If a dedicated Ethernet interface (e.g. eth2 or eth3) is not available on the server machine, eth0 and eth1 are supported for the Heartbeat UDP interface. (This function does not apply, however, if you have deployed your CASs in Virtual Gateway mode *and* the eth0 and eth1 interfaces have the *same* IP address.) See Selecting and Configuring the Heartbeat UDP Interface, page 4-23.

If additional network interfaces (e.g. eth2 or eth3) are available, you can use them for UDP heartbeat instead of eth0. In this case, the eth2 or eth3 interfaces on the two machines are connected using a crossover cable. If installing an additional Ethernet interface, configure the IP address for the interface. For instructions, see Configuring Additional NIC Cards, page 3-38.

Switch Interfaces for OOB Deployment

For Out-of-Band deployments, ensure that 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.

Service IP Addresses

In addition to the IP addresses for the trusted and untrusted interfaces for each individual CAS, you will need to provide two Service IP addresses for the trusted and untrusted interfaces of the CAS pair (see Figure 4-9 on page 4-18 for an example configuration). A **Service IP address** is the common IP address that the external network uses to address the pair.

In addition, either the trusted or untrusted interface Service IP address should be used to generate the SSL certificate. If a CAS was previously configured and added to the CAM as a standalone CAS, it must be deleted prior to configuring it for HA.

After HA configuration is complete on both CASs, use the Service IP in the **New Server** form to add the HA-CAS pair to the CAM. Note that the HA-CAS pair is automatically added as the same Server Type (for example, Out-of-Band Virtual Gateway).

Host Names

For heartbeat, each CAS needs to have a unique hostname (or node name). For HA CAS 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.

DHCP Synchronization

When you configure two CASs that also perform DHCP functions for your deployment as an HA pair, Cisco NAC Appliance automatically synchronizes and exchanges the required keys between the HA-Primary and HA-Secondary CASs to ensure DHCP continues to work properly following a failover event.

SSL Certificates

As in standalone mode, in HA mode the Clean Access Servers can use either a temporary, self-signed certificate or a CA (Certificate Authority)-signed certificate. A temporary certificate is useful for testing or development. A production deployment should have a CA-signed certificate. Considerations in either case are:

1. Both the temporary or CA-signed certificates can use either the Service IP address (for either the trusted interface or untrusted interface) or a domain name as the certificate domain name.
2. If creating a certificate using a domain name, then the domain name must map to the Service IP in DNS. If you are not using a domain name in the certificate, then the DNS mapping is not necessary.
3. For a temporary certificate, generate the temporary certificate on one of the Clean Access Servers, and transfer it from that CAS to the other CAS.
4. For a CA-signed certificate, you will need to import the CA-signed certificate into each of the Clean Access Servers in the pair.

Note The CA-signed certificate must be either based on the Service IP or a hostname/domain name resolvable to the Service IP through DNS.

Note The Clean Access Server retrieves session information from the CAM during failover. For example, if user A is logged into the system in role B, when failover occurs, user A will still be logged in and have access specified by role B.

If the CAS is the DHCP server and failover occurs, user A also retains his/her assigned IP address because to HA CASs *do* directly exchange DHCP failover information.

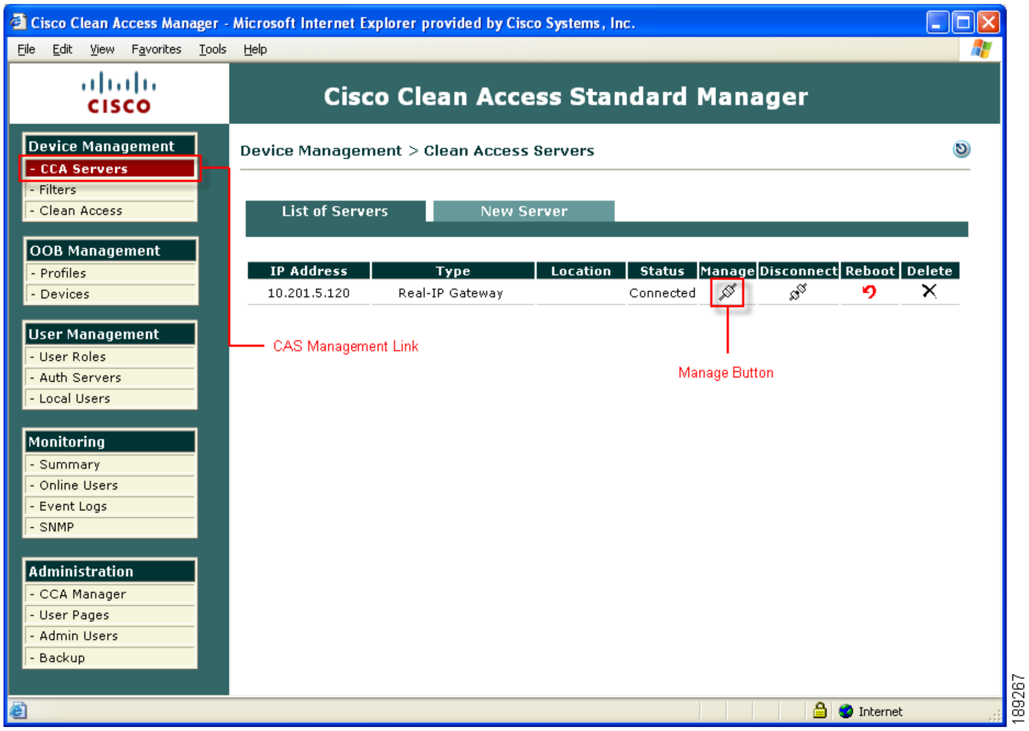
Note For HA CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the HA-Secondary CAS unit through its direct access web console. These settings include updating the SSL certificate, system time, time zone, DNS, or Service IP. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(1)* and Modifying CAS High Availability Settings, page 4-38 for details.

Before Starting

1. Before starting, make sure that both Clean Access Servers are installed and accessible over the network. See Perform the Initial CAS Configuration, page 3-25.
2. The two Clean Access Servers in the HA pair must remain Layer 2 adjacent to support heartbeat and sync functions.

3. If the Clean Access Servers have already been added to the management domain of a CAM, they should be removed. Use the **Delete** button in the **List of Servers** tab to remove the CASs.

Figure 4-11 List of Servers



IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.5.120	Real-IP Gateway		Connected				✕

Note Cisco NAC Appliance web consoles support Internet Explorer 6.0 and 7.0 browsers.

Selecting and Configuring the Heartbeat UDP Interface

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

The Heartbeat UDP interface, if specified, is used to send UDP heartbeat traffic related to high availability. The interface used depends on the interfaces available on the server machine and the load level expected. This interface can use either a dedicated Ethernet interface (such as eth2 or eth3) or the trusted interface eth0, if a dedicated interface is not available.

When using an additional Ethernet interface, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see Configuring Additional NIC Cards, page 3-38. When a dedicated interface is used, the dedicated interfaces on both machines should be connected using a crossover cable.

Servers running a CAS typically use both available interfaces (eth0 and eth1), with eth0 configured as the trusted network interface. Cisco recommends using the eth2 and eth3 interfaces for heartbeat redundancy, thus freeing up the eth0 and eth1 interfaces to handle Cisco NAC Appliance traffic.

Note If using eth0 as the UDP heartbeat interface, make sure that the management interfaces on the CAS are in their own VLAN, not on a VLAN with other user traffic. This is a general best practice that allows you to segment and protect management traffic when running the failover heartbeat over the same physical interface.

Serial Port High-Availability Connection

If each machine running the CAS software has two serial ports, use one of the ports for the serial cable connection.

By default, the first serial connector detected on the server is configured for console input/output (to facilitate installation and other types of administrative access).

Warning **When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for Cisco NAC Appliance CAMs/CASs 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.**

When high-availability mode is selected, the serial console login (ttyS0) is automatically disabled to free the serial port for HA mode. To re-enable ttyS0 as the console login, deselect the **Disable Serial Login** checkbox on the **Failover > General** tab after clicking **Update** and before clicking **Reboot**. For details, see steps c. Configure HA-Primary Mode and Update, page 4-26 and c. Configure HA-Secondary Mode and Update, page 4-32.

Configure High Availability

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

The following sections describe how to set up high availability in four general procedures:

- Step 1: Configure the HA-Primary Clean Access Server, page 4-24
- Step 2: Configure the HA-Secondary Clean Access Server, page 4-32
- Step 3: Connect the Clean Access Servers and Complete the Configuration, page 4-36
- Step 4: Failing Over an HA-CAS Pair, page 4-37

Note “Primary/Secondary” denotes the server mode when it is configured for HA.
“Active/Standby” denotes the runtime status of the server.

Configure the HA-Primary Clean Access Server

The general sequence to configure the HA-Primary CAS is as follows:

a. Access the HA-Primary CAS Directly, page 4-25

b. Configure the Host Information for the HA-Primary CAS, page 4-25

c. Configure HA-Primary Mode and Update, page 4-26

d. Configure the SSL Certificate, page 4-30

e. Reboot the HA-Primary CAS, page 4-31

f. Add the CAS to the CAM Using the Service IP, page 4-31

When done, continue to Configure the HA-Secondary Clean Access Server, page 4-32.

a. Access the HA-Primary CAS Directly

Each Clean Access Server has its own web admin console that allows configuration of certain limited Administration settings directly on the CAS. The CAS direct access web console must be used to configure CAS pairs for HA.

To access the HA-Primary Clean Access Server's direct access web admin console:

1. Open a web browser and type the IP address of the trusted (eth0) interface of the CAS in the URL/address field, as follows: **https://<primary_CAS_eth0_IP_address>/admin** (for example, `https://172.16.1.2/admin`).
2. Accept the temporary certificate and log in as user `admin` with the web console password specified during initial configuration.

Note

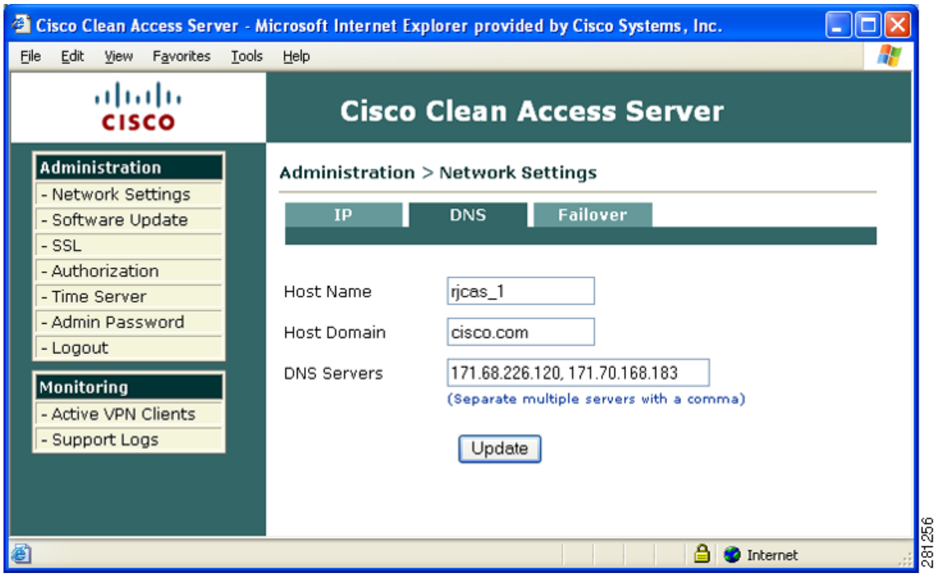
- In order to copy and paste values to/from configuration forms, Cisco recommends keeping both web consoles open for each CAS (primary and secondary). See also a. Access the HA-Secondary CAS Directly, page 4-32.
- To ensure security, Cisco recommends changing the default password of the CAS.

b. Configure the Host Information for the HA-Primary CAS

3. Click the **Network Settings** link, then the **DNS** tab.
4. In the **Host Name** field, type the host name for the HA-Primary CAS. Make sure there is a domain in the **Host Domain** field, such as cisco.com. If necessary, add one and click **Update**.

Note When configuring HA, it is mandatory to specify a Host Name for each machine in the HA-pair. The Host Name is case-sensitive and cannot be an IP address. Host Names are needed later for the **Local Host Name** and **Peer Host Name** fields of the HA Primary and HA Secondary configuration. The **Local Host Name** and **Peer Host Name** do not need to be resolvable via DNS; however, they are case-sensitive and need to match the Host Names you have specified for the machines.

Figure 4-12 DNS Tab



Host Name: rjcas_1

Host Domain: cisco.com

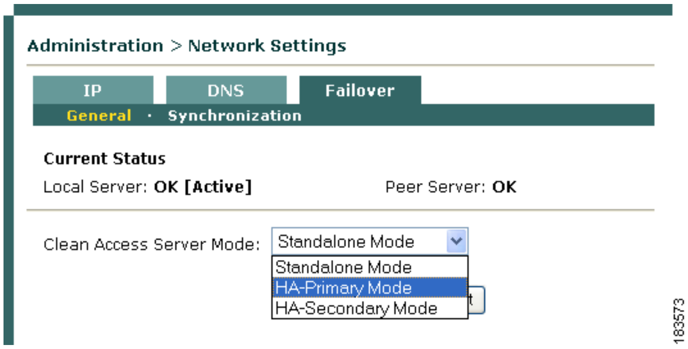
DNS Servers: 171.68.226.120, 171.70.168.183

(Separate multiple servers with a comma)

c. Configure HA-Primary Mode and Update

5. Click the **Failover > General** tab and choose **HA-Primary Mode** from the **Clean Access Server Mode** dropdown menu.

Figure 4-13 Failover —Choose Mode



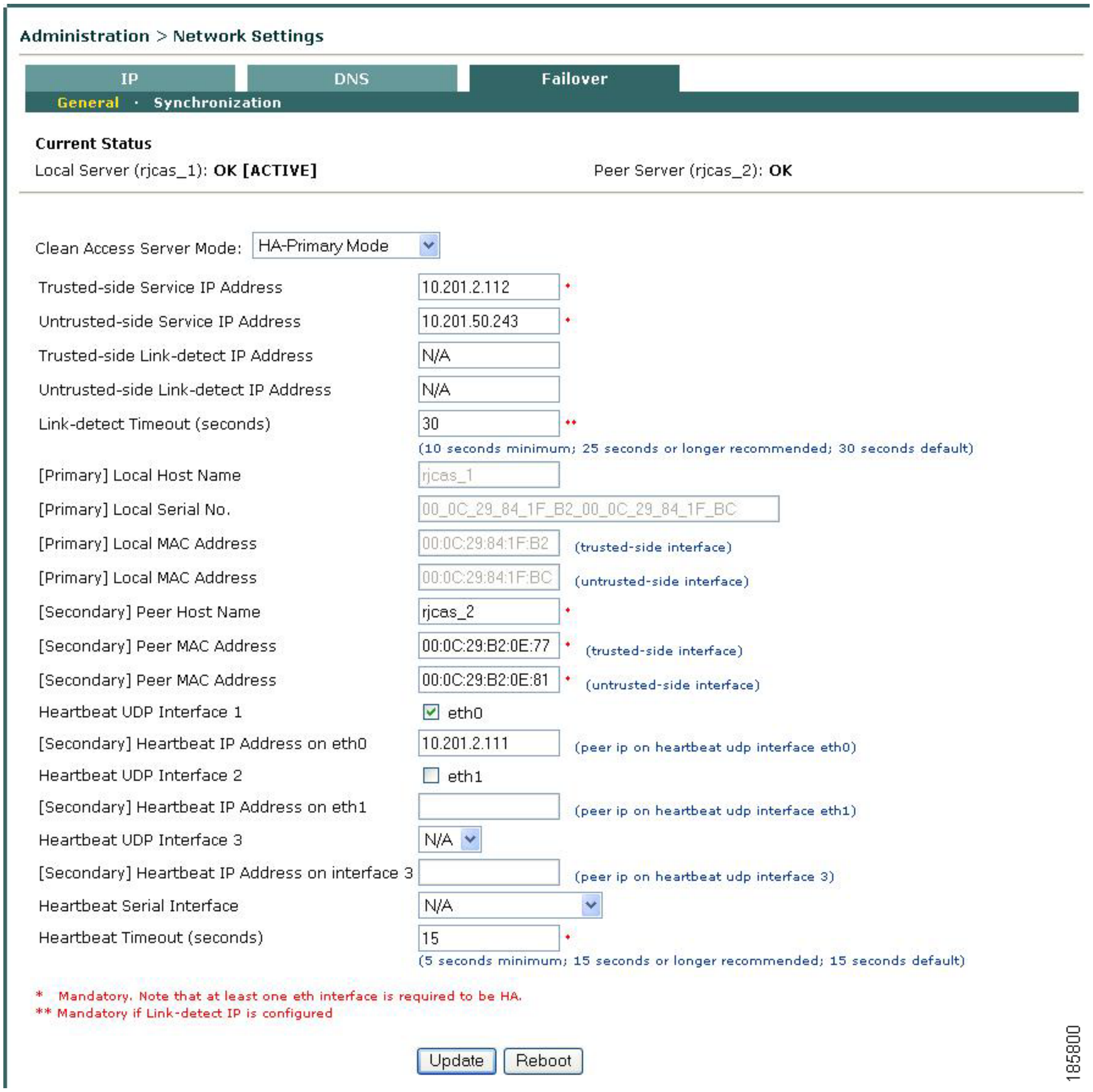
Current Status

Local Server: OK [Active] Peer Server: OK

Clean Access Server Mode: Standalone Mode

6. In the **HA-Primary Mode** form that opens, type values for the following fields.

Figure 4-14 Failover —HA-Primary Mode



Current Status

Local Server (rjcas_1): **OK [ACTIVE]**   Peer Server (rjcas_2): **OK**

Clean Access Server Mode:	HA-Primary Mode	
Trusted-side Service IP Address	10.201.2.112	*
Untrusted-side Service IP Address	10.201.50.243	*
Trusted-side Link-detect IP Address	N/A	
Untrusted-side Link-detect IP Address	N/A	
Link-detect Timeout (seconds)	30	** (10 seconds minimum; 25 seconds or longer recommended; 30 seconds default)
[Primary] Local Host Name	rjcas_1	
[Primary] Local Serial No.	00_0C_29_84_1F_B2_00_0C_29_84_1F_BC	
[Primary] Local MAC Address	00:0C:29:84:1F:B2	(trusted-side interface)
[Primary] Local MAC Address	00:0C:29:84:1F:BC	(untrusted-side interface)
[Secondary] Peer Host Name	rjcas_2	*
[Secondary] Peer MAC Address	00:0C:29:B2:0E:77	* (trusted-side interface)
[Secondary] Peer MAC Address	00:0C:29:B2:0E:81	* (untrusted-side interface)
Heartbeat UDP Interface 1	☑ eth0	
[Secondary] Heartbeat IP Address on eth0	10.201.2.111	(peer ip on heartbeat udp interface eth0)
Heartbeat UDP Interface 2	☐ eth1	
[Secondary] Heartbeat IP Address on eth1		(peer ip on heartbeat udp interface eth1)
Heartbeat UDP Interface 3	N/A	
[Secondary] Heartbeat IP Address on interface 3		(peer ip on heartbeat udp interface 3)
Heartbeat Serial Interface	N/A	
Heartbeat Timeout (seconds)	15	* (5 seconds minimum; 15 seconds or longer recommended; 15 seconds default)

* Mandatory. Note that at least one eth interface is required to be HA.
** Mandatory if Link-detect IP is configured

  - **Trusted-side Service IP Address**: The common IP address by which the pair is addressed from the trusted network (10.201.2.112 in the example in Figure 4-9 on page 4-18).
  - **Untrusted-side Service IP Address**: The common address for the pair on the untrusted (managed) network (10.201.50.243 in the sample).

- **Trusted-side Link-detect IP Address**: When an IP address (e.g. for an upstream router) is optionally entered in this field, the CAS attempts to ping this external address. Typically, the same trusted-side link-detect address is entered on both the HA-Primary and HA-Secondary CAS, but you can specify different addresses for each CAS if your network topology is different.
- **Untrusted-side Link-detect IP Address**: When an IP address (e.g. for a downstream switch) is optionally entered in this field, the CAS will attempt to ping this external address. You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.

Note If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the **/etc/ha.d/linkdetect.conf** file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See Link-Detect Interfaces, page 4-41 for more details.

- **Link-detect Timeout (seconds)**: This configures the length of time the CAS attempts to ping the Trusted-side and/or Untrusted-side Link-detect IP address(es). Cisco recommends entering a time of at least 26 seconds. If the CAS cannot ping the node for the period of time specified, the node is not pingable.

Note In addition to UDP Interface configuration, you can optionally configure the CAS to respond to link failures on the trusted and/or untrusted sides as failover events. The CAS attempts to ping the trusted and/or untrusted link-detect addresses specified, then counts the number of nodes it can reach:

0-for no addresses

1-for either trusted/untrusted

2-for both trusted/untrusted

If the Standby CAS can reach more nodes than the Active CAS, the Standby CAS will take over and become the Active CAS. If both CASs can ping the same number of addresses (all addresses or only one address), no failover event occurs, since neither CAS has the advantage. To enable link-detect, enter at least one link-detect IP address on each CAS and a link-detect timeout. See also Choosing External IPs for Link-Based Failover, page 4-20 for further details.

Note The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

The CAS performs Heartbeat connection and (optionally) Link-detect according to the same interval, approximately every 1-2 seconds.

- **[Primary] Local Host Name**: This is filled in by default for the HA-Primary CAS, as configured under **Administration > Network Settings > DNS | Host Name** (“rjcas_1” in Figure 4-12).
- **[Primary] Local Serial No**: Filled in by default for the HA-Primary CAS. The local serial number identifies this CAS to the Clean Access Manager (and is composed of eth0/eth1 MAC addresses). In an HA-CAS pair, the serial number of the Primary CAS is the key used to associate all the configuration information specific to this CAS in the CAM database.
- **[Primary] Local MAC Address (trusted-side interface)**: Filled in by default; the MAC address of the eth0 interface for the HA-Primary CAS.

- **[Primary] Local MAC Address (untrusted-side interface)**: Filled in by default; the MAC address of the eth1 interface for the HA-Primary CAS.

Note

- You may want to copy and paste the **[Primary] Local Host Name**, **[Primary] Local Serial No**, and **[Primary] Local MAC Address (trusted/untrusted)** values into a text file. These values are necessary later when configuring the HA-Secondary CAS.
- To enter the HA-Secondary CAS information into the form for the HA-Primary CAS, copy and paste the corresponding fields from the HA-Secondary CAS web console.

- **[Secondary] Peer Host Name**: Type the host name for the HA-Secondary CAS peer ("rjcas_2" in this example). The Secondary Peer Host Name is case-sensitive and must exactly match the **Host Name** specified in the peer machine **DNS** tab (under **Administration > Network Settings > DNS | Host Name**).
- **[Secondary] Peer MAC Address (trusted-side interface)**: This is the peer MAC address from the trusted (eth0) side of the HA-Secondary CAS.
- **[Secondary] Peer MAC Address (untrusted-side interface)**: This is the peer MAC address from the untrusted (eth1) side of the HA-Secondary CAS.
- **Heartbeat UDP Interface 1**: This setting specifies eth0 as a failover IP interface on the CAS. If a dedicated Ethernet connection is not available,
- **[Secondary] Heartbeat IP Address on eth0**: The IP address of the trusted interface (eth0) of the HA-Secondary CAS.
- **Heartbeat UDP Interface 2**: This setting specifies eth1 as a failover IP interface on the CAS. If you configure your CAS HA system to use eth0 as the primary failover heartbeat connection, you can also use the eth1 interface as a redundant heartbeat monitor.
- **[Secondary] Heartbeat IP Address on eth1**: The IP address of the untrusted interface (eth1) of the HA-Secondary CAS.
- **Heartbeat UDP Interface 3**: Options are N/A, eth2, or eth3. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 or another Ethernet interface for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.

Note Before you can specify either the eth2 or eth3 interfaces to be **Heartbeat UDP Interface 3**, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see Configuring Additional NIC Cards, page 3-38.

- **[Secondary] Heartbeat IP Address on Interface 3**: The IP address of the tertiary failover heartbeat link configured on the HA-Secondary CAS.

Note You must configure at least one of the additional Ethernet interfaces on the HA-Primary CAS to connect to a peer interface on the Secondary CAS in order to support HA behavior. In an HA scenario, The Ethernet interface you configure serves as the medium for data sync between the Primary and Secondary CAS.

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

- **Heartbeat Timeout (seconds)**: Choose a value greater than 15 seconds.

  Note To avoid a potentially serious network issue where two CASs deployed as an HA pair reboot at the same time (in the event power returning after an outage, for example) and *both* come up as the active CAS in the HA pair, Cisco recommends setting the **Heartbeat Timeout** to a value greater than 30 seconds. The possible network implication in this scenario is that the to "active" CASs can introduce a Layer 2 broadcast loop that almost immediately brings down the network.

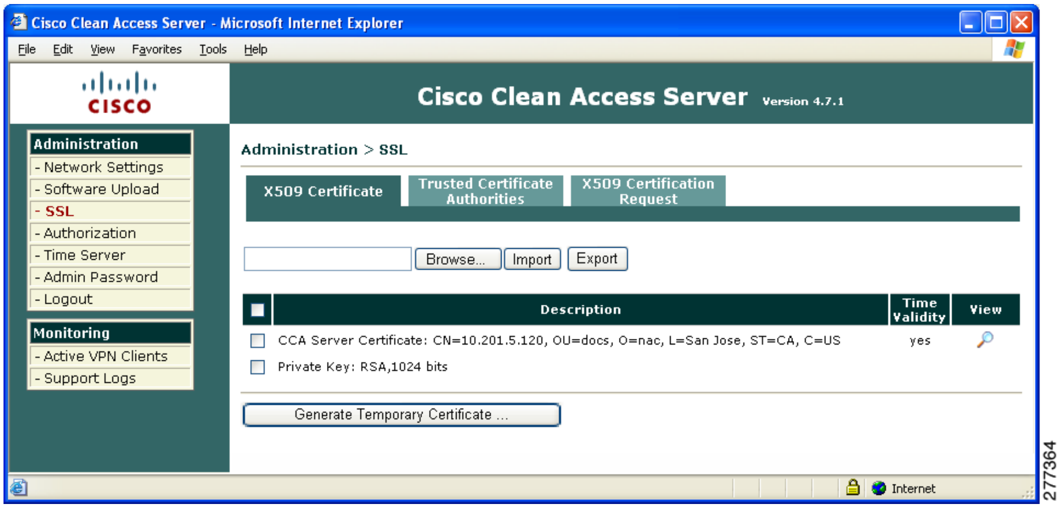
  Another method you can use to avoid this scenario is to ensure you use an additional Ethernet interface link (eth2, eth3) for heartbeat monitoring between your CAS Ha pair nodes. See **Heartbeat UDP Interface 2** and **Heartbeat UDP interface 3**, above and Configuring Additional NIC Cards, page 3-38, for more information.

- **Update**: Click to update the HA configuration information for the CAS without rebooting it.
- **Reboot**: This is used to reboot the CAS at the end of HA-Primary CAS configuration. (Do **not** click Reboot at this point.)

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Primary CAS. Navigate to **Administration > SSL > X509 Certificate**.

Figure 4-15 Administration > SSL > X509 Certificate



□	Description	Time Validity	View
□	CCA Server Certificate: CN=10.201.5.120, OU=docs, O=nac, L=San Jose, ST=CA, C=US	yes	🔍
□	Private Key: RSA,1024 bits		

8. Perform one of the following procedures, depending on whether you intend to use a temporary, self-signed certificate or a CA-signed certificate:

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 CAS.

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 the "Manage CAS SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(1)*.

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.

Note The CA-signed certificate must either be based on the Service IP or a host name/domain name resolvable to the Service IP through DNS.

e. Reboot the HA-Primary CAS

9. **Reboot** the Clean Access Server from either the CAS direct access interface (**Network Settings > Failover > General > Reboot** button) or from the CAM web console (**Administration > CCA Manager > Network > Reboot** button).

f. Add the CAS to the CAM Using the Service IP

10. In the CAM web console, go to **Device Management > CCA Servers > New Server**, and add the CAS to the CAM using the Service IP for the pair (10.201.2.112) as the **Server IP** address.

11. Configure any other settings desired, such as DHCP settings, to control the runtime behavior of the CAS.

12. Test the configuration by trying to log into the untrusted (managed) network from a computer connected to the untrusted interface of the Clean Access Server. Proceed to the next step only if you can successfully access the network.

Configure the HA-Secondary Clean Access Server

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

The general sequence to configure the HA-Secondary CAS is as follows:

a. Access the HA-Secondary CAS Directly

b. Configure the Host Information for the HA-Secondary CAS

c. Configure HA-Secondary Mode and Update

d. Configure the SSL Certificate

e. Reboot the HA-Secondary CAS

a. Access the HA-Secondary CAS Directly

1. Access the web console for the HA-Secondary CAS by opening a web browser and typing the IP address of the trusted (eth0) interface of the HA-Secondary CAS in the URL/address field, as follows: **https://<standby_CAS_eth0_IP_address>/admin** (for example, `https://172.16.1.3/admin`)
2. Log in as user `admin` and provide the correct password.

Note
- In order to copy and paste values to/from configuration forms, Cisco recommends keeping both web consoles open for each CAS (primary and secondary). See also a. Access the HA-Primary CAS Directly, page 4-25.
- To ensure security, Cisco recommends changing the default password of the CAS.

b. Configure the Host Information for the HA-Secondary CAS

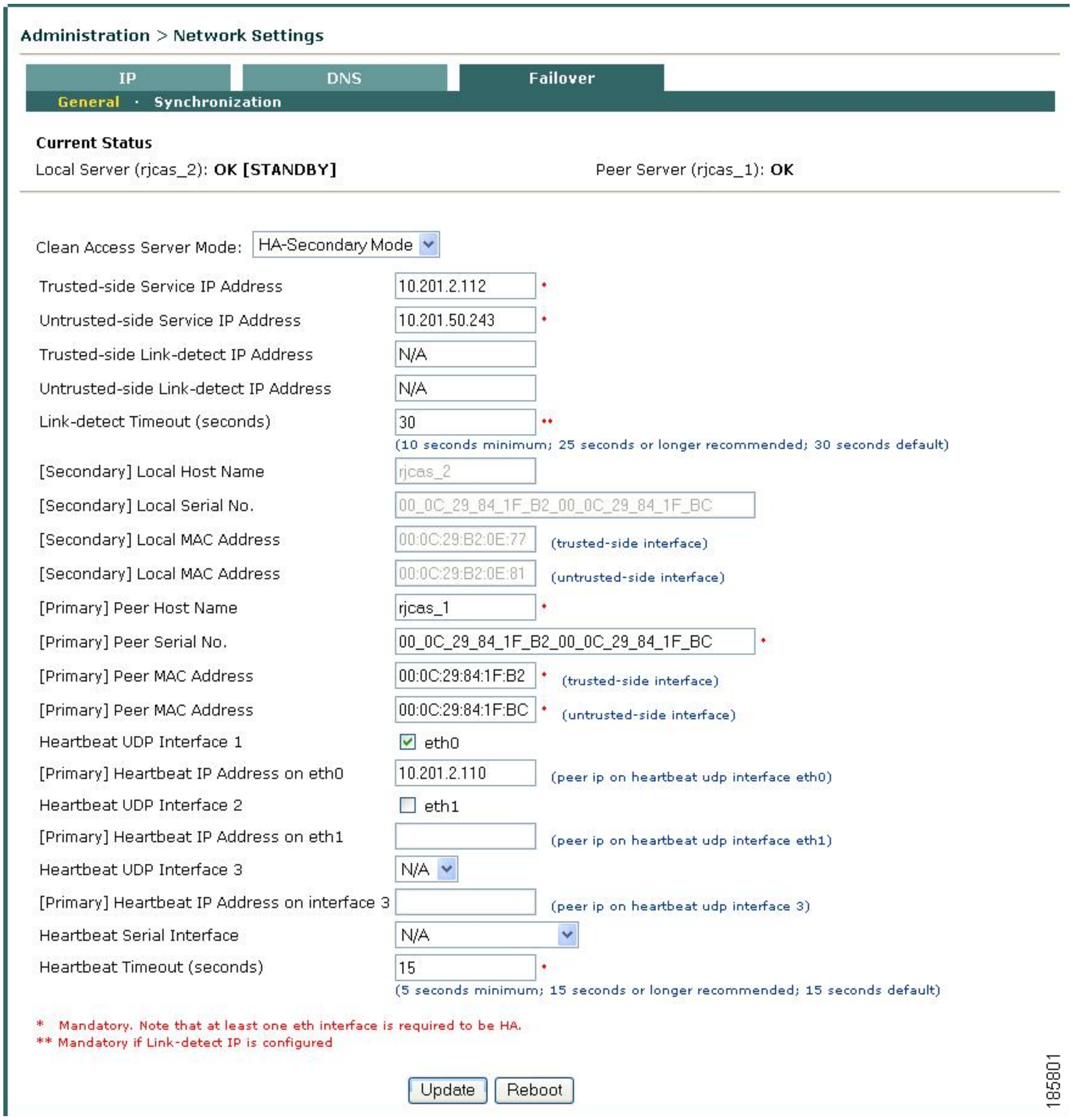
3. In the **Network Settings** page, open the **DNS** tab.
4. Make sure the host name is a unique host name for the HA-Secondary CAS, such as "rjcas_2." You must have the same domain name specified in this tab as you did for the HA-Primary CAS (see b. Configure the Host Information for the HA-Primary CAS, page 4-25).

Note When configuring HA, it is mandatory to specify a Host Name for each machine in the HA-pair. The Host Name is case-sensitive and cannot be an IP address. Host Names are needed later for the **Local Host Name** and **Peer Host Name** fields of the HA Primary and HA Secondary configuration. The **Local Host Name** and **Peer Host Name** do not need to be resolvable via DNS; however, they are case-sensitive and need to match the Host Names you have specified for the machines.

c. Configure HA-Secondary Mode and Update

5. Click the **Failover > General** tab and select **HA-Secondary Mode** from the **Clean Access Server Mode** dropdown menu.

Figure 4-16 Failover —HA-Secondary Mode



Current Status
Local Server (rjcas_2): **OK [STANDBY]** Peer Server (rjcas_1): **OK**

Clean Access Server Mode:	HA-Secondary Mode	
Trusted-side Service IP Address	10.201.2.112	*
Untrusted-side Service IP Address	10.201.50.243	*
Trusted-side Link-detect IP Address	N/A	
Untrusted-side Link-detect IP Address	N/A	
Link-detect Timeout (seconds)	30	** (10 seconds minimum; 25 seconds or longer recommended; 30 seconds default)
[Secondary] Local Host Name	rjcas_2	
[Secondary] Local Serial No.	00_0C_29_84_1F_B2_00_0C_29_84_1F_BC	
[Secondary] Local MAC Address	00:0C:29:B2:0E:77	(trusted-side interface)
[Secondary] Local MAC Address	00:0C:29:B2:0E:81	(untrusted-side interface)
[Primary] Peer Host Name	rjcas_1	*
[Primary] Peer Serial No.	00_0C_29_84_1F_B2_00_0C_29_84_1F_BC	*
[Primary] Peer MAC Address	00:0C:29:84:1F:B2	* (trusted-side interface)
[Primary] Peer MAC Address	00:0C:29:84:1F:BC	* (untrusted-side interface)
Heartbeat UDP Interface 1	☑ eth0	
[Primary] Heartbeat IP Address on eth0	10.201.2.110	(peer ip on heartbeat udp interface eth0)
Heartbeat UDP Interface 2	□ eth1	
[Primary] Heartbeat IP Address on eth1		(peer ip on heartbeat udp interface eth1)
Heartbeat UDP Interface 3	N/A	
[Primary] Heartbeat IP Address on interface 3		(peer ip on heartbeat udp interface 3)
Heartbeat Serial Interface	N/A	
Heartbeat Timeout (seconds)	15	* (5 seconds minimum; 15 seconds or longer recommended; 15 seconds default)

* Mandatory. Note that at least one eth interface is required to be HA.
** Mandatory if Link-detect IP is configured

6. In the HA-Secondary form, complete the following fields:

- **Trusted-side Service IP Address**: The IP address by which the pair is addressed from the *trusted* network. Use the same value as for the primary CAS (10.201.2.112 in the example in Figure 4-9 on page 4-18).
- **Untrusted-side Service IP Address**: The IP address by which the pair is addressed from the *untrusted* (managed) network. Use the same value as for the primary CAS (10.201.50.243 in the example).

- **Trusted-side Link-detect IP Address (Optional)**: When an IP address (e.g. for an upstream router) is optionally entered in this field, the CAS will attempt to ping this address. Typically, the same trusted-side link-detect address is entered on both the HA-Primary and HA-Secondary CAS, but you can specify different addresses for each CAS if your network topology is different.

- **Untrusted-side Link-detect IP Address (Optional)**: When an IP address (e.g. for a downstream switch) is optionally entered in this field, the CAS will attempt to ping this address. You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.

Note If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the **/etc/ha.d/linkdetect.conf** file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See Link-Detect Interfaces, page 4-41 for more details.

- **Link-detect Timeout (seconds) (Optional)**: This configures the length of time the CAS will attempt to ping the Trusted-side and/or Untrusted-side Link-detect IP address(es). Enter a time of at least 26 seconds. If the CAS cannot ping the node for the period of time specified, the node is not pingable.

Note The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

See Choosing External IPs for Link-Based Failover, page 4-20 for additional details.

- **[Secondary] Local Host Name**: This is filled in by default for the HA-Secondary CAS, as configured under **Administration > Network Settings > DNS | Host Name** (“rjcas_2” in this example).
- **[Secondary] Local Serial No**: Filled in by default for the HA-Secondary CAS.
- **[Secondary] Local MAC Address (trusted-side interface)**: Filled in by default; the MAC address of the eth0 interface for the HA-Secondary CAS.
- **[Secondary] Local MAC Address (untrusted-side interface)**: Filled in by default; the MAC address of the eth1 interface for the HA-Secondary CAS.

Note

- You may want to copy and paste the **[Secondary] Local Host Name**, **[Secondary] Local Serial No**. and **[Secondary] Local MAC Address (trusted/untrusted)** values into a text file. These values are needed to configure the HA-Primary CAS.
- To enter the HA-Primary CAS information into the form for the HA-Secondary CAS, copy and paste the corresponding fields from the web console of the HA-Primary CAS.

- **[Primary] Peer Host Name**: Type the host name of the HA-Primary CAS (“rjcas_1” in Figure 4-12). The **[Primary] Peer Host Name** is case-sensitive and must exactly match the Host Name specified in the peer machine **DNS** tab (under **Administration > Network Settings > DNS | Host Name**).
- **[Primary] Peer Serial No**: The serial number of the HA-Primary CAS. When the HA-Secondary CAS becomes Active, it must use the serial number of the HA-Primary CAS to identify itself to the CAM in order to access the CAS configuration information.

- **[Primary] Peer MAC Address (trusted-side interface)**: The peer MAC address from the trusted side (eth0) of the HA-Primary CAS.
- **[Primary] Peer MAC Address (untrusted-side interface)**: The peer MAC address from the untrusted side (eth1) of the HA-Primary CAS.
- **Heartbeat UDP Interface 1**: This setting specifies eth0 as a failover IP interface on the CAS. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.
- **[Primary] Heartbeat IP Address on eth0**: The IP address of the trusted interface (eth0) of the HA-Primary CAS.
- **Heartbeat UDP Interface 2**: This setting specifies eth1 as a failover IP interface on the CAS. If you configure your CAS HA system to use eth0 as the primary failover heartbeat connection, you can also use the eth1 interface as a redundant heartbeat monitor.
- **[Primary] Heartbeat IP Address on eth1**: The IP address of the untrusted interface (eth1) of the HA-Primary CAS.
- **Heartbeat UDP Interface 3**: Options are N/A, eth2, or eth3. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 or another Ethernet interface for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.

Note Before you can specify either the eth2 or eth3 interfaces to be **Heartbeat UDP Interface 3**, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see Configuring Additional NIC Cards, page 3-38.

- **[Primary] Heartbeat IP Address on Interface 3**: The IP address of the tertiary failover heartbeat link configured on the HA-Primary CAS.

Note You must configure at least one of the additional Ethernet interfaces on the HA-Primary CAS to connect to a peer interface on the Secondary CAS in order to support HA behavior. In an HA scenario, The Ethernet interface you configure serves as the medium for data sync between the Primary and Secondary CAS.

Note Cisco strongly recommends you do not use the serial interface on the NAC-3315/3355/3395 for the HA heartbeat function. Although this element still appears in the CAM web console, the **Heartbeat Serial Interface** feature is being deprecated in a future Cisco NAC Appliance release. (The associated **Heartbeat Timeout** value remains a valid configuration point, however, for deployments using optional Heartbeat UDP interfaces 2 and 3.)

- **Heartbeat Timeout (seconds)**: Choose a value greater than 15 seconds.

Note To avoid a potentially serious network issue where two CASs deployed as an HA pair reboot at the same time (in the event power returning after an outage, for example) and *both* come up as the active CAS in the HA pair, Cisco recommends setting the **Heartbeat Timeout** to a value greater than 30 seconds. The possible network implication in this scenario is that the to "active" CASs can introduce a Layer 2 broadcast loop that almost immediately brings down the network.

Another method you can use to avoid this scenario is to ensure you use an additional Ethernet interface link (eth2, eth3) for heartbeat monitoring between your CAS Ha pair nodes. See **Heartbeat UDP Interface 2** and **Heartbeat UDP interface 3**, above and Configuring Additional NIC Cards, page 3-38, for more information.

- **Update**: Click to update the HA configuration information for the CAS without rebooting it.
- **Reboot**: This is used to reboot the CAS at the end of HA-Primary CAS configuration. (Do **not** click Reboot at this point.)

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Secondary CAS. Navigate to **Administration > SSL > X509 Certificate** and perform one of the following procedures:

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 the "Manage CAS SSL Certificates" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(1)*.

e. Reboot the HA-Secondary CAS

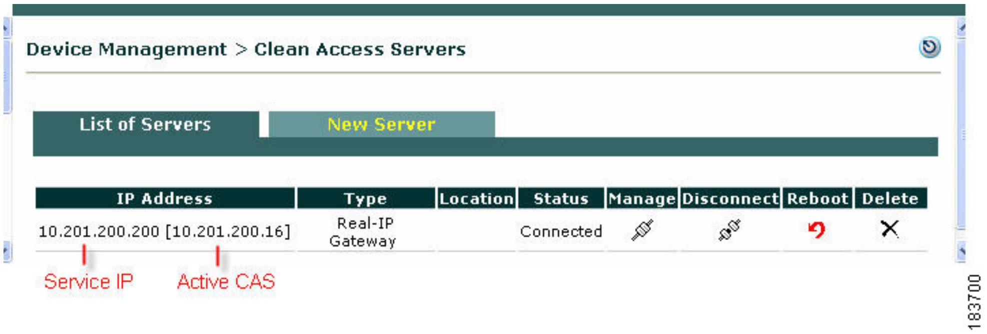
8. From the CAS direct access interface (**Network Settings > Failover > General**), click the **Reboot** button to reboot the Clean Access Server.

Connect the Clean Access Servers and Complete the Configuration

1. Shut down the HA-Primary CAS machine and connect the `rjcas_1` and `rjcas_2` machines using a serial null modem cable (connecting available serial ports) and/or a crossover cable (connecting Ethernet ports if using a pair of Ethernet interfaces such as eth2 or eth3 for failover).

2. Open the Clean Access Manager administration console.
3. Go to **Device Management > CCA Servers > List of Servers**. The Active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in Figure 4-17. Since the HA-Primary CAS is turned off, the IP address of the HA-Secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.

Figure 4-17 Active CAS in an HA-Pair



IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.200.200 [10.201.200.16]	Real-IP Gateway		Connected			↺	✕

4. Click the **Manage** button for the pair. The management pages of the HA-Secondary CAS (now the Active CAS) should appear.
5. From a client computer connected to the Clean Access Server's untrusted interface, test the configuration by trying to log on to the untrusted (managed) network as an authorized user. If successful, remain logged on and proceed to the next step.

Failing Over an HA-CAS Pair

To test your HA system, use the following steps:

1. Turn on the HA-Primary CAS machine. Make sure that the CAS is fully started and functioning before proceeding.
2. From the client computer, log off the user's session and try to log onto the untrusted (managed) network again as the user.
3. The HA-Secondary CAS should still be active and providing services for the user.
4. Shut down the HA-Secondary CAS machine.

Note Cisco recommends "shutdown" or "reboot" on the machine to test failover, or, if a CLI command is preferred, **`service perfigo stop`** and **`service perfigo start`**. For a Virtual Gateway CAS, use **`service perfigo maintenance`** instead to bring the CAS to maintenance mode and allow network connectivity to the management VLAN. See Useful CLI Commands for HA, page 4-39 for details.

5. After about 15 seconds, you should be able to continue browsing, with the HA-Primary CAS becoming the Active server and providing the service.
6. Turn on the HA-Secondary CAS machine (the standby server).
7. Check the event log on the Clean Access Manager. It should correctly indicate the status of the Clean Access Servers (e.g., "`rjcas_1 is dead. rjcas_2 is up`").
8. Testing of the high availability configuration is now complete.

Modifying CAS High Availability Settings

The following instructions describe how to change settings for an existing high-availability Clean Access Server pair. Changing the Service IP, the subnet mask, or the default gateway for a high-availability pair requires updating the Clean Access Manager and rebooting the Clean Access Server.

Additionally, if the Service IP address is changed and the SSL certificate for the Clean Access Server is based on the Service IP, a new certificate must be generated and imported to each Clean Access Server in the high-availability pair. If the SSL certificate is based on the host name of the Clean Access Server, generating a new certificate is not necessary. However, make sure to change the IP address for that host name in your DNS server.

The general sequence of steps is as follows:

1. Update the Clean Access Server settings in the Clean Access Manager first (but do not reboot).
2. Update the HA settings in the direct access web console for the primary CAS and reboot the primary CAS.
3. While the primary CAS reboots, wait for the secondary CAS to become active in the CAM's List of Servers.
4. Repeat steps 1-3 for the secondary CAS and reboot the secondary CAS.
5. While the secondary CAS reboots, the primary CAS becomes active in the Clean Access Manager and displays the new settings.

To Change IP Settings for an HA-CAS

1. From the CAM web admin console, go to **Device Management > CCA Servers**.
2. Click the **Manage** button for the Clean Access Server.
3. Click the **Network** tab.
4. Change the **IP Address**, **Subnet Mask**, or **Default Gateway** settings for the trusted/untrusted interfaces as desired.
5. Click the **Update** button only.

Caution Do not click the **Reboot** button at this stage.

6. If the SSL certificate for the CAS was based on the previous IP address, you will need to generate a new SSL certificate based on the new IP address configured. This can be done under **Administration > SSL > X509 Certificate**. See the "Manage CAS SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(1)* for details.
7. If the SSL certificate was based on the host name of your Clean Access Server, you do not need to generate a new certificate. However, make sure to change the IP address for that host name in your DNS server.
8. Next, open the direct access web admin console for the **primary** Clean Access Server as follows:

```
https://<primary_CAS_eth0_IP_address>/admin
```

9. The IP form for the primary CAS will reflect the changes you made in the CAM web console under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.
10. In Clean Access Server direct access console, click the **Network > Failover> General** tab.

11. Change the following as needed:
    - Trusted-side Service IP Address
    - Untrusted-side Service IP Address
    - [Secondary] Peer Host Name
    - [Secondary] Peer MAC Address (trusted-side interface)
    - [Secondary] Peer MAC Address (untrusted-side interface)
    - [Secondary] Heartbeat IP Address
12. Click the **Update** button, then the **Reboot** button.
13. From the Clean Access Manager administrator web console, go to **Device Management > CCA Servers** and wait for the secondary Clean Access Server to become active. (Note that this can take a few minutes.) The active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in Figure 4-9 on page 4-18. The IP address of the secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.
14. Once the IP address of the secondary CAS appears in brackets in the **List of Servers**, and the CAS has a status of Connected, repeat steps 1-11 for the secondary CAS.
15. Once changes are made and the secondary CAS is rebooted, the primary CAS will appear as the active server on the List of Servers and displays all the new IP information.

Upgrading an Existing Failover Pair

For instructions on upgrading 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 4.7(1)*.

Useful CLI Commands for HA

Clean Access Manager

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.

Clean Access Server

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

- HA CAS Configuration Status (**/etc/ha.d/perfigo.conf**)
- Heartbeat/Link-Based Connections (**/etc/ha.d/ha.cf**)
- Link-Detect Interfaces (**/etc/ha.d/linkdetect.conf**)
- Active/Standby Status (**/perfigo/common/bin/fostate.sh**)

HA CAS Configuration Status

The **/etc/ha.d/perfigo.conf** file shows a variety of configuration information for an HA-CAS, including hostname (rjcas_1), peer hostname (rjcas_2), HA mode (Primary), heartbeat interface (UDP/serial), and Link-detect interface information:

```
[root@rjcas_1 ha.d]# more perfigo.conf
#linux-ha
#Mon Aug 28 18:50:15 PDT 2006
WIRELESS_SERVICEIP=10.10.20.4
PING_DEAD=25
HOSTNAME=rjcas_1
HA_DEAD=15
PEERGUSSK=
PEERMAC=00\:16\:35\:BF\:FE\:67
PEERHOSTNAME=rjcas_2
TRUSTED_PINGNODE=10.10.40.100
UNTRUSTED_PINGNODE=10.10.20.100
HAMODE=PRIMARY
PEERMAC0=00\:16\:35\:BF\:FE\:66
PEERHOSTIP=10.10.50.2
HA_FAILBACK=off
```

```
HA_UDP=eth2
WIRED_SERVICEIP=10.10.20.4
HA_SERIAL=ttyS0
```

Heartbeat/Link-Based Connections

The **/etc/ha.d/ha.cf** file shows additional information about the heartbeat and link-based connections:

```
[root@rjcas_1 ha.d]# more ha.cf
# Generated by make-hacf-ss.pl
udpport         694
ucast           eth2 10.10.50.2
baud            19200
serial          /dev/ttyS0
keepalive       2
deadtime        15
deadping        25
auto_failback   off
apiauth         default uid=root
respawn         hacluster /usr/lib64/heartbeat/ipfail
ping            10.10.20.100
ping            10.10.40.100

log_badpack     false
warntime        10
debug           0
debugfile       /var/log/ha-debug
logfile         /var/log/ha-log
watchdog        /dev/watchdog
node            rjcas_1
node            rjcas_2
```

Link-Detect Interfaces

The **/etc/ha.d/linkdetect.conf** file is useful if your network topology restricts configuring external (pingable) interfaces for Link-detect functionality between your CAS HA pair appliances. This file specifies the CAS network interfaces (eth0, eth1, or both) to monitor for Link-detect functionality. If a monitored interface loses connectivity with its associated external interface, the active CAS fails over and the standby CAS assumes the active role.

To create and/or update the **linkdetect.conf** file in the CAS:

Step 1 Log in to the CAS direct console CLI and direct console as the root user.

Step 2 Navigate to the **/etc/ha.d/** directory on the CAS.

Step 3 Using a standard text editor (like vi), edit the linkdetect.conf file so that it contains the interface names you want to monitor, or (if the linkdetect.conf file does not currently exist on the CAS) add the linkdetect.conf file to this directory.

Step 4 Verify the contents of the file:

```
[root@rjcas_1 ha.d]# more linkdetect.conf

# The following network interfaces will be monitored for link healthiness
# The active CAS will change to standby mode when any link failure is detected
#
eth0
eth1
```

Step 5 Enable the new function by stopping and restarting CAS services with the **service perfigo stop** and **service perfigo start** commands.

In the above **linkdetect.conf** file example, both the eth0 and eth1 interfaces on the CAS are monitored for network connectivity.

Note Any other CAS interfaces specified in the **linkdetect.conf** file (like eth2 or eth3, for example) are ignored for purposes of Link-detect behavior.

Active/Standby Status

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

1. Cd to `/perfigo/common/bin/`, and run the fostate.sh script on the first CAS:

```
[root@rjcas_1 bin]# ./fostate.sh
My node is active, peer node is standby
[root@rjcas_1 bin]#
```

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

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

```
[root@rjcas_2 bin]# ./fostate.sh
My node is standby, peer node is active
[root@rjcas_2 bin]#
```

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

Accessing High Availability Pair CAS Web Consoles

Determining Active and Standby CAS

From the CAM web console, go to **Device Management > CCA Servers > List of Servers** to view your HA-CAS pairs. The List of Servers page displays the **Service IP** of the CAS pair first, followed by the IP address of the Active CAS in brackets. When a secondary CAS takes over, its IP address will be listed in the brackets as the Active server.

Note The CAS configured in HA-Primary Mode may not be the currently Active CAS.

Determining Primary and Secondary CAS

Open the direct access console for each CAS in the pair by typing the following in the URL/Address field of a web browser (you should have two browsers open):

- For the Primary CAS, type: **https://<*primary_CAS_eth0_IP_address*>/admin**. For example, `https://172.16.1.2/admin`.

- For the Secondary CAS, type: **https://<*secondary_CAS_eth0_IP_address*>/admin**. For example, `https://172.16.1.3/admin`.

In each CAS web console, go to **Administration > Network Settings > Failover > General**.

- The Primary CAS is the CAS you configured in **HA-Primary Mode** when you initially set up HA**.**
- The Secondary CAS is the CAS you configured in **HA-Secondary Mode** when you initially set up HA.

For releases prior to 4.0(0), the Secondary CAS is labelled as **HA-Standby Mode** (CAS) for the initial HA configuration.