



CHAPTER 14

Configuring High Availability (HA)

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:

- [Overview, page 14-1](#)
- [CAS High Availability Requirements, page 14-4](#)
- [Before Starting, page 14-6](#)
- [Configure High Availability, page 14-7](#)
- [Failing Over an HA-CAS Pair, page 14-18](#)
- [Configure DHCP Failover, page 14-19](#)
- [Modifying High Availability Settings, page 14-22](#)
- [Upgrading an Existing Failover Pair, page 14-24](#)
- [Useful CLI Commands for HA, page 14-24](#)
- [Adding High Availability Cisco NAC Appliance To Your Network, page 14-25](#)

Overview

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.
- 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/or UDP). Heartbeat packets can be sent on the serial interface, dedicated eth2 interface, or eth0 interface (if an eth2 interface is not 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.

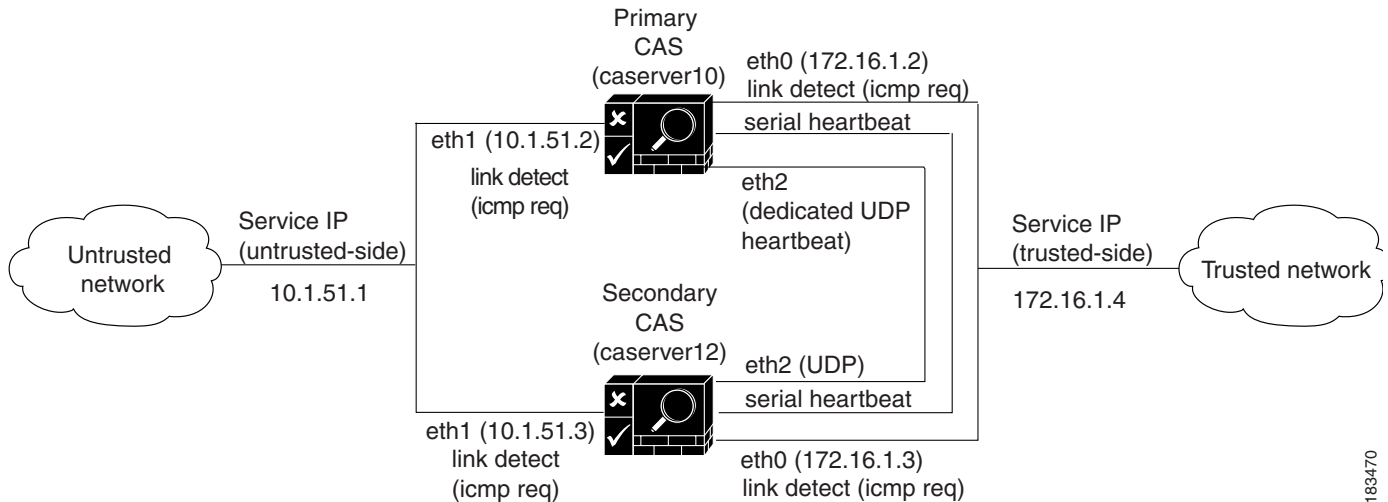


Note The status of these ping packets is communicated between the CASes via the heartbeat interface. Therefore, heartbeat connection is still required if using link-based failover.

- 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.

Figure 14-1 illustrates the basic connections in an example HA-CAS configuration.

Figure 14-1 Clean Access Server Example High-Availability Configuration



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 CASes 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 Installation and Configuration Guide, Release 4.1(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 CASes to add the CAS to the CAM. Figure 14-2 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 14-2 Active CAS in an HA-Pair

**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 CASes, the Service IP is then entered in the **New Server** form to add the HA-CAS pair to the CAM.

**Note**

For extra security, Cisco recommends connecting the serial ports of each Clean Access Server (using “null modem cable”) for heartbeat exchange.

Failover Events

- If both UDP heartbeat and serial heartbeat interfaces are configured, then both must fail for the standby system to take over. See [Physical Connection, page 14-4](#) for additional details.
- If the CAS is unable to communicate with the CAM via heartbeat:
 - 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.

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

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 14-9](#) and [c. Configure HA-Secondary Mode and Update, page 14-14](#) for additional configuration details.

CAS High Availability Requirements

This section describes additional planning considerations when implementing high availability:

Physical Connection

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

- A serial null-modem cable, or
- A dedicated Ethernet NIC card, configured as the eth2 interface of the CAS, or
- UDP heartbeat over eth0 **and** a serial null-modem cable.

Cisco recommends configuring a third NIC card as the eth2 interface of CAS. If your server only has two network interfaces, you can purchase one of the following NIC cards for this purpose:

- PWLA8492MT = Intel PRO/1000 MT Dual Port Server Adapter (copper)
- PWLA8492MF = Intel PRO/1000 MF (dual SX fiber LC connectors)



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>.

If a third network interface (e.g. eth2) is available, it can be used for UDP heartbeat instead of eth0. In this case, the eth2 interfaces on the two machines are connected using a crossover cable. If installing an additional Ethernet interface, configure the IP address for the interface (see [Configuring Additional NIC Cards, page 4-19](#) for details).

If a dedicated Ethernet interface (e.g. eth2) is not available on the server machine, eth0 is supported for the Heartbeat UDP interface, in conjunction with serial heartbeat. See [Selecting and Configuring the Heartbeat UDP Interface, page 14-7](#).

Serial heartbeat connection generally requires the server machine to have at least two serial ports: one port (ttyS0) is used for the serial heartbeat connection and the other is used to access to the server for configuration tasks. For details, see [Serial Port High-Availability Connection, page 14-7](#).

**Note**

Do not connect the serial cable before starting HA (failover) configuration. The serial cable must be connected after the configuration is complete. See [Connect the Clean Access Servers and Complete the Configuration, page 14-17](#).

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 14-1 on page 14-2](#) 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 CASes, 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

If the Clean Access Servers operate as DHCP Servers (not in DHCP Relay or DHCP Passthrough mode) additional configuration steps must be taken to enable the Clean Access Servers to keep their DHCP-related information synchronized. DHCP information, such as information regarding active leases and lease times, is exchanged by SSH tunnel, which you configure as described in [Configure DHCP Failover, page 14-19](#).

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 maintains session information 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 a user has a particular IP address prior to failover, DHCP failover on the CAS will ensure that the user is given the same IP address when the IP address is renewed. See [Configure DHCP Failover, page 14-19](#).



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 [Clean Access Server Direct Access Web Console, page 13-2](#) and [Modifying High Availability Settings, page 14-22](#) 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 Configuration, page 4-9](#).
2. 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 CASes.

Figure 14-3 List of Servers

The screenshot shows the Cisco Clean Access Standard Manager interface. The left sidebar contains navigation menus for Device Management, Switch Management, and User Management. The main content area is titled 'Cisco Clean Access Standard Manager' and shows the 'List of Servers' tab. A table lists the following servers:

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.240.10	Out-of-Band NAT Gateway	Dell350	Connected				
10.201.240.12	NAT Gateway	DellPowerEdge750	Connected				

The Delete button for the second server (10.201.240.12) is highlighted with a red box and labeled 'Delete button'.



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

Selecting and Configuring the Heartbeat UDP Interface

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 interface such as eth2 or the trusted interface eth0, if a dedicated interface is not available.

On some servers, an additional NIC card can be installed to provide an interface dedicated to UDP heartbeat (e.g. eth2). In this case, configure the IP address for the new interface as described in [Configuring Additional NIC Cards, page 4-19](#). 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. The eth0 trusted network interface can be shared in most deployments. When eth0 is used as the heartbeat interface, Cisco recommends additionally configuring serial heartbeat connection.

**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).

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 14-9](#) and [c. Configure HA-Secondary Mode and Update, page 14-14](#).

**Note**

The serial console login and HA serial heartbeat cannot be located on the same serial port.

Configure High Availability

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

- Step 1: [Configure the Primary Clean Access Server, page 14-8](#)
- Step 2: [Configure the HA-Secondary Clean Access Server, page 14-14](#)
- Step 3: [Connect the Clean Access Servers and Complete the Configuration, page 14-17](#)
- Step 4: [Failing Over an HA-CAS Pair, page 14-18](#)
- Step 5: [Configure DHCP Failover, page 14-19](#)

If configuring high availability for Clean Access Servers that operate as DHCP servers (not in DHCP relay or passthrough mode), you also need to configure the SSH tunnel between them.

**Note**

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

Configure the Primary Clean Access Server

The general sequence to configure the primary CAS is as follows:

- a. [Access the Primary CAS Directly, page 14-8](#)
- b. [Configure the Host Information for the Primary, page 14-8](#)
- c. [Configure HA-Primary Mode and Update, page 14-9](#)
- d. [Configure the SSL Certificate, page 14-12](#)
- e. [Reboot the Primary Server, page 14-13](#)
- f. [Add the CAS to the CAM Using the Service IP, page 14-13](#)

When done, continue to [Configure the HA-Secondary Clean Access Server, page 14-14](#).

a. Access the 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 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://<PrimaryCAS_eth0_IP>/admin** (for example, **https://172.16.1.2/admin**)
2. Accept the temporary certificate and log in as user **admin** (default password is **cisco123**).

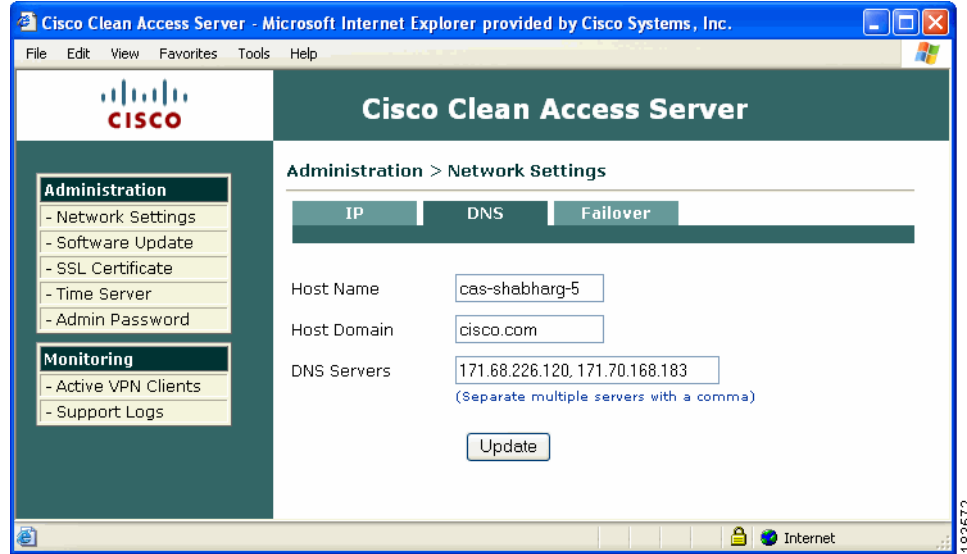
**Note**

- 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 14-14](#).
- To ensure security, Cisco recommends changing the default password of the CAS.

b. Configure the Host Information for the Primary

3. Click the **Network Settings** link, then the **DNS** tab.
4. In the **Host Name** field, type the host name for the primary CAS (for example, caserver10). Make sure there is a domain in the **Host Domain** field, such as cisco.com. If necessary, add one and click **Update**.

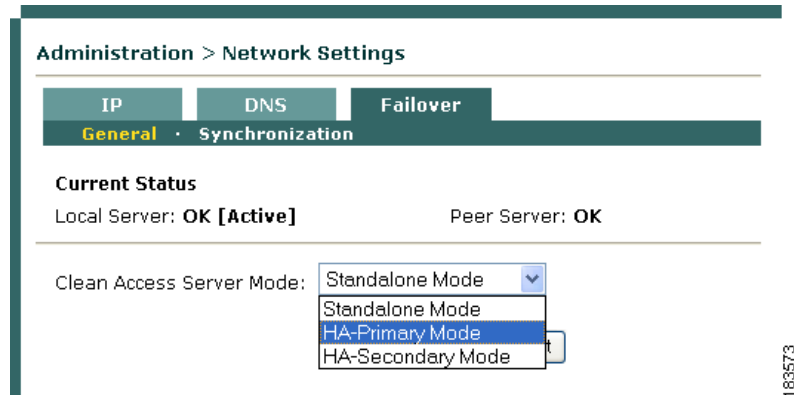
Figure 14-4 DNS Tab



c. Configure HA-Primary Mode and Update

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

Figure 14-5 Failover – Choose Mode



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

Figure 14-6 Failover – HA-Primary Mode

The screenshot shows the 'Administration > Network Settings' page with the 'Failover' tab selected. The 'Current Status' shows 'Local Server: OK [Active]' and 'Peer Server: OK'. The 'Clean Access Server Mode' is set to 'HA-Primary Mode'. The configuration includes fields for Trusted-side and Untrusted-side Service IP Addresses (both 10.201.217.193), Link-detect IP Addresses (both N/A), and Link-detect Timeout (60 seconds). It also lists Primary and Secondary Local/Peer Host Names, MAC Addresses, and Heartbeat IP Addresses. The Heartbeat UDP Interface is set to 'eth0' and the Heartbeat Timeout is 30 seconds. There are 'Update' and 'Reboot' buttons at the bottom.

183575

- **Trusted-side Service IP Address:** The common IP address by which the pair is addressed from the trusted network (172.16.1.4 in the example in [Figure 14-1](#) on [page 14-2](#)).
- **Untrusted-side Service IP Address:** The common address for the pair on the untrusted (managed) network (10.1.51.1 in the sample).
- **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 on its trusted interface (eth0). 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 on its untrusted interface (eth1). You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.
- **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**

In addition to Heartbeat Serial/UDP configuration, you can optionally configure the CAS to respond to link failures on the trusted and/or untrusted sides as failover events. The CAS will attempt to ping the trusted and/or untrusted link-detect addresses specified, then count 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 CASes 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 14-3](#) for further details.

**Note**

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

- **[Primary] Local Host Name:** Filled in by default for the HA-Primary CAS, as configured under **Administration > Network Settings > DNS | Host Name** (caserver10 in the sample).
- **[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:** The host name for the HA-Secondary CAS peer (caserver12 in the sample). You will need to specify this value again as the **Host Name** value in the peer machine's **DNS** tab.
- **[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:** Options are N/A, eth0, eth2, eth3, eth4. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 for the Heartbeat UDP interface in conjunction with serial heartbeat when configuring a Clean Access Server in HA mode.
- **[Secondary] Heartbeat IP Address:** The IP address of the trusted interface (eth0) of the HA-Secondary CAS (in the sample, 172.16.1.3).
- **Heartbeat Serial Interface:** Select the COM port for the serial connection. Cisco recommends using both serial and UDP connections for the Heartbeat interface.



Note Do not connect the serial cable before starting HA (failover) configuration. The serial cable must be connected after the configuration is complete.

- **Heartbeat Timeout (seconds):** Choose a value greater than 15 seconds.
- **Disable Serial Login:** Serial login is disabled by default when HA mode is selected. To re-enable the serial console (ttyS0), deselect the **Disable Serial Login** checkbox at this stage (after **Update** and before **Reboot**).
- **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. Click the **SSL Certificate** link from the **Administration** menu. The **Generate Temporary Certificate** form appears.

Figure 14-7 Generate Temporary Certificate

The screenshot shows the Cisco Clean Access Server Administration interface in a Microsoft Internet Explorer browser. The page title is "Cisco Clean Access Server" and the breadcrumb is "Administration > SSL Certificate". On the left, there is a navigation menu with "Administration" and "Monitoring" sections. The "Administration" section includes links for Network Settings, Software Update, SSL Certificate, Time Server, and Admin Password. The "Monitoring" section includes Active VPN Clients and Support Logs. The main content area displays the "Generate Temporary Certificate" form. The form has a dropdown menu for "Choose an action:" with the following options: "Generate Temporary Certificate" (selected), "Export CSR/Private Key/Certificate", and "Import Certificate". Below this are input fields for "Full Domain Name", "Organization Unit Name", "Organization Name", "City Name", "State Name", and "2-letter Country Code". A "Generate" button is located at the bottom of the form. At the bottom of the page, it states "Current SSL Certificate Domain: 10.201.217.193 (This is the domain name for which you have the SSL certificate of the web login page.)".

8. In the **SSL Certificate** page, 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. Complete the **Generate Temporary Certificate** 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, select **Export CSR/Private Key/Certificate** from the **Choose an action** dropdown menu.
- c. Click the **Export** button for **Currently Installed Private Key** to export the SSL private key. Save the key file to disk. You must import this key file later when configuring the HA-Secondary CAS.
- d. Click the **Export** button for **Currently Installed Certificate** to export the current temporary certificate. Save the certificate file to disk. You will have to import this file into the HA-Secondary CAS later.

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

- a. Choose **Import Certificate** from the **Choose an action** menu
- b. Use the **Browse** button next to the **Certificate File** field and navigate to the certificate file.
- c. Choose **CA-signed PEM-encoded X.509 Cert** from the **File Type** dropdown menu:
- d. Click **Upload** to import the certificate. Note that you will need to import the same certificate later to the HA-Secondary CAS.
- e. Click **Verify and Install Uploaded Certificates**.
- f. Choose **Export CSR/Private Key/Certificate** from the **Choose an action** list.
- g. Click the **Export Private Key** button. You must import this key later when configuring the HA-Secondary CAS.

See [Manage CAS SSL Certificates, page 13-3](#) for additional details.

**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 Primary Server

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 & Failover > 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 (172.16.1.4) 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

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](#)
- c. [Configure HA-Secondary Mode and Update](#)
- d. [Configure the SSL Certificate](#)
- e. [Reboot the HA-Secondary Server](#)

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://<StandbyCAS_eth0_IP>/admin** (for example, **https://172.16.1.3/admin**)
2. Log in as user **admin** (default password is **cisco123**). (Cisco recommends changing the default password for the CAS to ensure the security of your network environment.)



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 Primary CAS Directly, page 14-8](#).
- To ensure security, Cisco recommends changing the default password of the CAS.

b. Configure the Host Information for the HA-Secondary

3. In the **Network Settings** page, open the **DNS** tab.
4. Change the host name to the unique host name for the secondary CAS, such as **caserver12**. You must have the same domain name specified in this tab as you did for the primary Clean Access Server (see [b. Configure the Host Information for the Primary, page 14-8](#)).

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 14-8 Failover – HA-Secondary Mode

Administration > Network Settings

IP DNS Failover

General · Synchronization

Current Status
Local Server: OK [Active] Peer Server: OK

Clean Access Server Mode: HA-Primary Mode

Trusted-side Service IP Address: 10.201.217.193

Untrusted-side Service IP Address: 10.201.217.193

Trusted-side Link-detect IP Address: N/A (optional)

Untrusted-side Link-detect IP Address: N/A (optional)

Link-detect Timeout (seconds): 60
(make longer than 25 seconds)

[Primary] Local Host Name: cas-shabhang-5

[Primary] Local Serial No.: 00_17_08_52_F9_C0_00_17_08_52_F9_C2

[Primary] Local MAC Address: 00:17:08:52:F9:C0 (trusted-side interface)

[Primary] Local MAC Address: 00:17:08:52:F9:C2 (untrusted-side interface)

[Secondary] Peer Host Name: cas-shabhang-6

[Secondary] Peer MAC Address: 00:18:71:E6:C7:92 (trusted-side interface)

[Secondary] Peer MAC Address: 00:18:71:E6:C7:90 (untrusted-side interface)

Heartbeat UDP Interface: eth0

[Secondary] Heartbeat IP Address: 10.201.217.195 (peer ip on heartbeat udp interface)

Heartbeat Serial Interface: N/A

Heartbeat Timeout (seconds): 30
(make longer than 15 seconds)

Disable Serial Login: (Serial Login disabled by default when HA mode selected)

Update Reboot

183576

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 (172.16.1.4 in the example in Figure 14-1 on page 14-2).
- **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 (10.1.51.1 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 on its trusted interface (eth0). 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 on its untrusted interface (eth1). You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.

- **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 See [Choosing External IPs for Link-Based Failover, page 14-3](#) for additional details.

- **[Secondary] Local Host Name:** Filled in by default for the HA-Secondary CAS (caserver12 in the sample).
- **[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:** The host name of the HA-Primary CAS, as specified in the **Host Name** field in the primary's **DNS** tab (caserver10 in the sample).
- **[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:** Options are N/A, eth0, eth2, eth3, eth4. 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:** The IP address of the trusted-side interface (eth0) of the HA-Primary CAS (in the sample, 172.16.1.2)
- **Heartbeat Serial Interface:** Select the COM port for the serial connection. Cisco recommends using both serial and UDP connections for the Heartbeat interface.
- **Heartbeat Timeout (seconds):** Choose a value greater than 15 seconds.
- **Disable Serial Login:** Serial login is disabled by default when HA mode is selected. To re-enable the serial console (ttyS0), deselect the **Disable Serial Login** checkbox at this stage (after **Update** and before **Reboot**).
- **Update:** Click to update the HA configuration information for the CAS without rebooting it.

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Secondary CAS. Click the **SSL Certificate** link. In the **SSL Certificate** page, perform one of the following procedures:

If using a temporary certificate for the HA pair:

- a. Select **Import Certificate** from the **Choose an action** menu.
- b. Use the **Browse** button next to the **Certificate File** field to find the private key associated with temporary certificate file that you previously exported from the primary CAS.
- c. Choose **Private Key** as the File Type.
- d. Click **Upload** to upload the private key.
- e. With **Import Certificate** selected from the **Choose an action:** menu, browse to the temporary certificate associated with the private key.
- f. Choose **CA-signed PEM-encoded X.509 Cert** as the File Type.
- g. Click **Upload** to upload the temporary certificate.
- h. Click **Verify and Install Uploaded Certificates**.

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

- a. Select **Import Certificate** from the **Choose an action** menu.
- b. Use the **Browse** button next to the **Certificate File** field to select the private key file you exported from the primary CAS.
- c. Choose **Private Key** as the File Type.
- d. Click **Upload** to upload the private key.
- e. With **Import Certificate** selected from the **Choose an action:** menu, browse to the same CA-signed certificate file you imported into the primary Clean Access Server.
- f. Choose **CA-signed PEM-encoded X.509 Cert** as the File Type.
- g. Click **Upload** to upload the CA-signed certificate.
- h. Click **Verify and Install Uploaded Certificates**.

**Note**

In some cases, you will be required to import a CA-Root certificate and/or an Intermediate Root certificate. If so, choose the **Root/Intermediate Certificate** file type when importing the file(s). See [Manage CAS SSL Certificates, page 13-3](#) for additional details.

e. Reboot the HA-Secondary Server

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 `caserver10` and `caserver12` machines using a serial null modem cable (connecting available serial ports) and/or a crossover cable (connecting Ethernet ports if using a third Ethernet interface such as eth2 for failover).

- Open the Clean Access Manager administration console.
- 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 14-9](#). 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 14-9 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				

- Click the **Manage** button for the pair. The management pages of the HA-Secondary CAS (now the Active CAS) should appear.
- Configure the DHCP Server settings so that they match the DHCP settings of the HA-Primary CAS. If the HA-CAS pair operates as a DHCP server, follow the steps in [Configure DHCP Failover, page 14-19](#) to allow the peer Clean Access Servers to keep DHCP information in synchronization.
- 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



Note

For a DHCP Server HA-CAS pair, perform the steps in [Configure DHCP Failover, page 14-19](#) first.

To test your HA system, use the following steps:

- Turn on the HA-Primary CAS machine. Make sure that the CAS is fully started and functioning before proceeding.
- From the client computer, log off the user's session and try to log onto the untrusted (managed) network again as the user.
- The HA-Secondary CAS should still be active and providing services for the user.
- 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 [Using the Command Line Interface \(CLI\), page 4-17](#) 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. "caserver10 is dead. caserver12 is up").
8. Testing of the high availability configuration is now complete.

Configure DHCP Failover

High-availability peer Clean Access Servers (CASes) that operate in DHCP server mode exchange information regarding their DHCP activities, such as active leases and lease times, by secure SSH connection (tunnel). If configuring high availability for Clean Access Servers that will operate as DHCP servers (not in DHCP relay or passthrough mode), you need to configure DHCP failover. Keys for the server and for the account accessing the server are required for both the HA-Primary and HA-Secondary Clean Access Servers. As a result, a total of four keys must be exchanged. The interface described below is provided to facilitate the generation and exchange of the security keys necessary to transfer DHCP failover information between the primary and secondary Clean Access Servers.

**Note**

After the DHCP server and CAS failover have been configured, both primary and secondary Clean Access Servers must be failed over in order to create the `/var/state/dhcp` directory on each server. The `/var/state/dhcp` directory must exist on both servers for DHCP failover to function correctly. See [Connect the Clean Access Servers and Complete the Configuration, page 14-17](#) and [Failing Over an HA-CAS Pair, page 14-18](#).

To Configure DHCP Failover

To start, open the admin console of the primary CAS and the secondary CAS (`https://<Server IP Address>/admin`). You will have two browsers open during this process.

- Step 1** Go to the admin console of the primary CAS and click the **Network Settings > Failover > Synchronization** tab.
- Step 2** Click the **Enable** button to enable DHCP failover on the primary CAS (notice that this button toggles to **Disable** afterwards).

Figure 14-10 Enable DHCP Failover—Primary CAS

Administration > Network Settings

IP DNS Failover

General Synchronization

Configure SSH here to synchronize files (DHCP config, DHCP leases, Subnet and VLAN settings) between the CAS failover pair.

File Synchronization is enabled

SSH Client Key:

```
AAAAAB3NzaC1yc2EAAAABIAAAAEAsbbsIdawmakT46H8AbOEzL156EavQZf
SVBt1Y6dHuKza2ic2jmw8E1JUsGg7zOgHQ8r8Iws6Uw2eSnnHwdNH653kq
/2p1YHUNGb1JBZeBf1T5aeKncQHcV6ksH80cpgZimUZcx7yKQwa6f4ciWZ
ZpZw8704YJWMTCViKZ0sa0=
```

Current peer SSH Client key:

Enter peer SSH Client key here:

SSH Server Key:

```
AAAAAB3NzaC1yc2EAAAABIAAAAEAspTsXx+XTGf36P8+35k9Vd4Au3USyh
XY1v+fCsCIB9OqpJZ6X+b0ICOhf63bCdF3dr9Nw9MQED/bEnMx779C1Px2f
DxYH4gtmkeT8onI5QjUoB7iR6pgvSXevHnx9Zwh/CCJZ7hG073Q6oihJFbx
ftQL7TpgVC+87eQuZuKMMM=
```

Current peer SSH Server key:

Enter peer SSH Server key here:

Write peer SSH keys:

183821

- Step 3** Copy the value from the **SSH Client Key** field from the primary CAS.
- Step 4** Go to the admin console of the secondary CAS and click the **Network Settings > Failover > Synchronization** tab. (See [Figure 14-11](#).)

Figure 14-11 Enable DHCP Failover—Secondary CAS

Administration > Network Settings

IP DNS Failover

General Synchronization

Configure SSH here to synchronize files (DHCP config, DHCP leases, Subnet and VLAN settings) between the CAS failover pair.

File Synchronization is enabled

SSH Client Key:

```

AAAAAB3NzaC1yc2EAAAABIAAAAEIAA2AaBrcCUCdgs2vGX714LdEmISvalxysp
TeZBPm4a6vUHB YnEnIkBw1Vrc7nasebr u3PzSHhI971GLB2HwqajqEvc0z6v
uF1d09fUAWK/V65IEsxj2Gu7C81cGmn9PP8QZCFYmUto5cPhhhPOJhByZfK
J1sbwL2c1B0ve/vBNSK1IU=

```

Current peer SSH Client key:

```

AAAAAB3NzaC1yc2EAAAABIAAAAEIAshhSIDAwmaKt46H8AbOExL156EavQXf
SVBt1X6dMuKzA2ic2jmWh8ELJUsGg7zOgNQ6r8Ivs6UvZeSnnHwNH65SKg
/2piYHUNGb1JBZeBK1T5AeKncQhtqV6ksH80cpgXimUZtx7yKQwa6f4tiWZ
ZpXw6704YJMNTCViKZ0sAO=

```

Enter peer SSH Client key here:

SSH Server Key:

```

AAAAAB3NzaC1yc2EAAAABIAAAAEIAktV5E0eIRKodcRMSZsObgCepIHUFyk2
h/SXj7ZvttZLC2pmIpQqikHmEvLXjYewk+/EztxFiaUDJnlYhhVyEgCz/3
Koag8cRG9hg10jFVNeJkgFDOLFfgASFhntciNz/J+pD21gHDU23n6IBLCUe
hH0e4eQfzpd80Es5sICqV8=

```

Current peer SSH Server key:

Enter peer SSH Server key here:

Write peer SSH keys:

- Step 5** Click the **Enable** button to enable DHCP failover on the secondary CAS (notice that this button toggles to **Disable** afterwards).
- Step 6** Paste the SSH Client Key you copied from the primary CAS into the **Enter peer SSH Client key here:** field.
- Step 7** While still in the admin console of the secondary CAS, copy the value from the **SSH Client Key** field.
- Step 8** Now go back to the admin console of the primary CAS and paste the SSH Client Key of the secondary CAS into the **Enter peer SSH Client key here:** field. (See [Figure 14-10](#).)
- Step 9** While still in the admin console of the primary CAS, copy the value from the **SSH Server Key** field.
- Step 10** Now go to the admin console of the secondary CAS and paste the SSH Server Key of the primary CAS into the **Enter peer SSH Server key here:** field.
- Step 11** While in the admin console of the secondary CAS, copy the value from the **SSH Server key** field.
- Step 12** Click the **Update** button to write the peer SSH keys to the secondary CAS.
- Step 13** Go to the admin console of the primary CAS and paste the SSH Server Key from the secondary CAS into the **Enter peer SSH Server key here:** field.
- Step 14** Click the **Update** button to write the peer SSH keys to the primary CAS. DHCP failover configuration is now complete.

Figure 14-12 DHCP Failover – Configuration Complete

Administration > Network Settings

IP DNS Failover

General · Synchronization

Configure SSH here to synchronize files (DHCP config, DHCP leases, Subnet and VLAN settings) between the CAS failover pair.

File Synchronization is enabled

SSH Client Key:

```
AAAAAB3NzaC1yc2EAAAABIwAAAIEA5spTsXx+XTGf36P8+35k9Vd4Au3USyh
XY1v+fCsCIB90qpJZ6X+b0ICOhf63bCdF3dr9N09MQED/bEnMx779C1Fx2f
DxYH4gtmkeT8onI5QjUoB7iR6pgvSXevHnx9Zwh/CCJZ7hGO73Q6oihFbx
ftQL7TpgVC+87eQuZuKMMM=
```

Current peer SSH Client key:

```
AAAAAB3NzaC1yc2EAAAABIwAAAIEA2AzBzCUtdgz2vGXY14LdEmI5valxysp
TeXBpm4a6vUMBvYnEnIkBw1Vrt7nseDru3Kz5MhI971GLB2NWqajqEvt0z6u
uFd09fUAWK/V65IEsXj2Gu7C8lcGmn9RP8OZCFYmUto5rRhhbPOJhByZKh
J1sDwL2riBOve/vBN5K1IU=
```

Enter peer SSH Client key here:

SSH Server Key:

```
AAAAAB3NzaC1yc2EAAAABIwAAAIEA5spTsXx+XTGf36P8+35k9Vd4Au3USyh
XY1v+fCsCIB90qpJZ6X+b0ICOhf63bCdF3dr9N09MQED/bEnMx779C1Fx2f
DxYH4gtmkeT8onI5QjUoB7iR6pgvSXevHnx9Zwh/CCJZ7hGO73Q6oihFbx
ftQL7TpgVC+87eQuZuKMMM=
```

Current peer SSH Server key:

```
AAAAAB3NzaC1yc2EAAAABIwAAAIEA5spTsXx+XTGf36P8+35k9Vd4Au3USyh
XY1v+fCsCIB90qpJZ6X+b0ICOhf63bCdF3dr9N09MQED/bEnMx779C1Fx2f
DxYH4gtmkeT8onI5QjUoB7iR6pgvSXevHnx9Zwh/CCJZ7hGO73Q6oihFbx
ftQL7TpgVC+87eQuZuKMMM=
```

Enter peer SSH Server key here:

Write peer SSH keys:

1433/200

Modifying 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 **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**. See [Manage CAS SSL Certificates, page 13-3](#) 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_IPaddress>/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 14-1 on page 14-2](#). 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 CCA release, see “Upgrading High Availability Pairs” in the [Release Notes for Cisco NAC Appliance \(Cisco Clean Access\), Version 4.1\(1\)](#).

Useful CLI Commands for HA

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

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

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

The /etc/ha.d/perfigo.conf file shows a variety of configuration information for an HA-CAS, including hostname (cas1), peer hostname (cas2), HA mode (Primary), heartbeat interface (UDP/serial), and link-detect interface information:

```
[root@cas1 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=cas1
HA_DEAD=15
PEERGUSSK=
PEERMAC=00\ :16\ :35\ :BF\ :FE\ :67
PEERHOSTNAME=cas2
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
```

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

```
[root@cas1 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         cas1
node         cas2

```

How to Verify Active/Standby Runtime Status on the HA CAS

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

1. Cd to `/store/cca_upgrade-4.x.x`, and run the `fostate.sh` script on the first CAS:

```

[root@cas1 cca_upgrade-4.x.x]# ./fostate.sh
My node is active, peer node is standby
[root@cas1 cca_upgrade-4.x.x]#

```

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

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

```

[root@cas2 cca_upgrade-4.x.x]# ./fostate.sh
My node is standby, peer node is active
[root@cas2 cca_upgrade-4.x.x]#

```

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

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 14-13](#) 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.

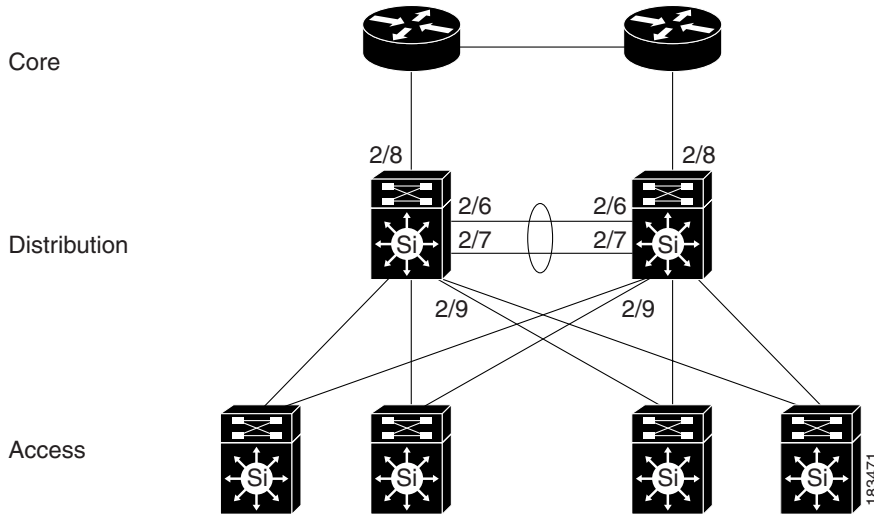
Figure 14-13 Example Core-Distribution-Access Network Before Cisco NAC Appliance

Figure 14-14 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.

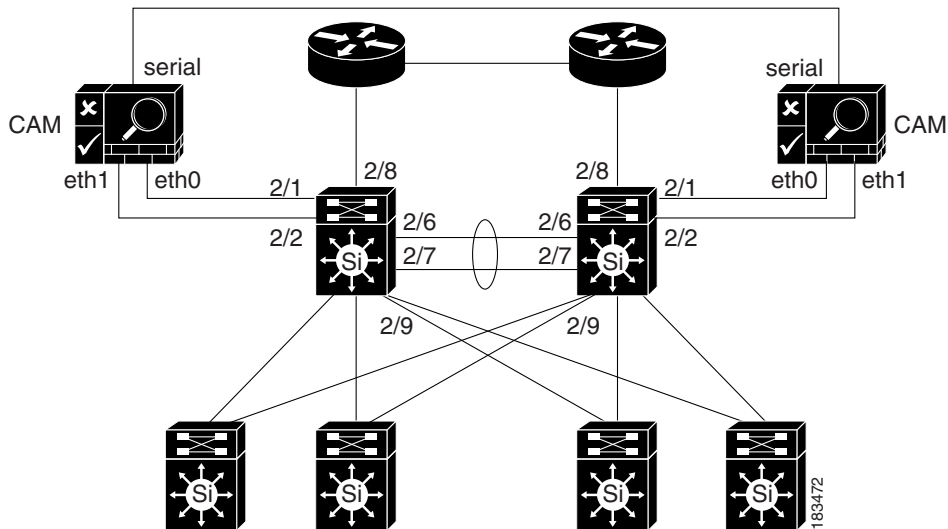
Figure 14-14 Adding HA CAMs to Network

Figure 14-15 shows how HA-CASs can be added to the core-distribution-access network. In this example, the CAS is configured as an L2 OOB Virtual Gateway in Central Deployment. The HA heartbeat connection is configured over both a serial interface and a dedicated eth2 interface. Link-failure based failover connection can also be configured over the eth0 and/or eth1 interfaces.

Figure 14-15 Adding HA CAS to Network

