



## CHAPTER 4

# Installation and Initial Configuration

---

This chapter contains the following sections:

- [Cisco NAC Profiler Collector/Server Hardware Overview](#)
- [Installing the Cisco NAC Profiler Server](#)
- [Configure a Standalone Cisco NAC Profiler Server](#)
- [Configure a Cisco NAC Profiler Server HA Pair](#)
- [Configuring the Collector on the Clean Access Server](#)
- [Collector Configuration on HA-CAS Pairs for Cisco NAC Profiler](#)

## Cisco NAC Profiler Collector/Server Hardware Overview

This section describes installation details for the two primary components of Cisco NAC Profiler:

- [Cisco NAC Profiler Collector, page 4-1](#)
- [Cisco NAC Profiler Server, page 4-2](#)

You can obtain additional information from the following documents:

- For ordering details, refer to the [Cisco NAC Profiler Ordering Guide](#).
- For licensing details, refer to [Cisco NAC Appliance Service Contract / Licensing Support](#).
- For details on Cisco NAC Appliance hardware platforms, refer to the [Cisco NAC Appliance Hardware Installation Quick Start Guide, Release 4.1](#).
- For details on software compatibility between the CAS, Collector and Profiler Server, refer to the [Release Notes for Cisco NAC Profiler](#) for the software version you are running.

## Cisco NAC Profiler Collector

The Cisco NAC Profiler Collector is a distributed component that resides on the Cisco NAC Appliance SERVER (Clean Access Server) and communicates with the Cisco NAC Profiler Server. A default version of the Collector is shipped with each CAS, and there is one Collector per CAS.

The Collector gathers information about endpoints using SNMP, NetFlow, DHCP, and active profiling, using the 4th NIC of the CAS to collect data from a SPAN port, or SNMP, or NetFlow. The Collector aggregates the relevant data, then consolidates and forwards it to the Profiler Server. The Profiler Server performs the profiling and categorization function, and then updates the NAC Manager automatically.

The Collector requires the following to function:

- A Collector license must be obtained and installed on the Cisco NAC Profiler Server. Refer to [Cisco NAC Appliance Service Contract/Licensing Support](#) for details on how to obtain and install product licenses for Cisco NAC Profiler.
- The Collector must be initially configured and enabled via the CAS CLI as described in [Configuring the Collector on the Clean Access Server](#), page 4-39.
- The version of the Collector on the CAS must be compatible with the Cisco NAC Profiler software version running on the Profiler Server. You can upgrade the Collector version independently of the Cisco NAC Appliance software on the CAS appliance. For version 2.1.8 instructions, refer to the “[Upgrading Collector Service on the CAS](#)” section of the [Release Notes for Cisco NAC Profiler](#).

Table 4-1 summarizes the number of endpoints supported when the Collector is enabled on the CAS for each Cisco NAC Appliance SERVER hardware platform.

**Table 4-1 Cisco NAC Appliance Server Hardware Summary and Collector Support**

Clean Access Server Platform	Number of Hosts Supported <sup>1</sup>	
	Users/Endpoints	Endpoints Only
NAC-3310 SERVER	100/100	200
	250/250	500
	500/500	1000
NAC-3350 SERVER	1500/1500	3000
	2500/2500	5000
	3500/3500	7000

1. Cisco NAC Profiler Collector licensing has a 1:1 or 2:1 relationship to Clean Access Server user limits in a Cisco NAC Appliance deployment, depending on whether posture assessment is used. For example, a 2500-user CAS can support 2500 users and 2500 Collector endpoints, or up to 5000 Collector endpoints-only if there is no posture assessment.

## Cisco NAC Profiler Server

The Cisco NAC Profiler Server is an appliance that aggregates and classifies data from Collectors and manages a database of endpoint information. The Cisco NAC Profiler Server updates the Cisco NAC Appliance MANAGER (Clean Access Manager) device filter list to place endpoints into appropriate access roles.

The Cisco NAC Profiler Server can communicate with multiple Collectors on multiple Clean Access Servers. The Profiler Server has a 1:1 relationship to the Clean Access Manager (CAM). There is one Profiler Server for each CAM in a Cisco NAC Appliance deployment.

There are two platforms available for Cisco NAC Profiler Server standalone or failover appliances:

- Profiler Server hardware platform (maximum 7,000 endpoints supported), based on the Cisco NAC-3350 hardware platform.
- “Profiler Lite” platform (maximum 5,000 endpoints supported), based on the Cisco NAC-3310 hardware platform.



**Note** The Profiler Lite platform is supported as a new installation only and requires its own ISO file (upgrade does not apply). Only the **nac\_profilerlite\_2.1.8-37-K9.iso** file can be installed on the Profiler Lite platform.

There are standalone and failover licences for each hardware platform, as well as Collector licenses associated to the CAS size and Profiler platform size. For details, refer to the [Cisco NAC Profiler Ordering Guide](#).

## Cisco NAC Profiler Server Hardware Summary

Table 4-2 summarizes the hardware specifications for the Cisco NAC Profiler Server platforms.

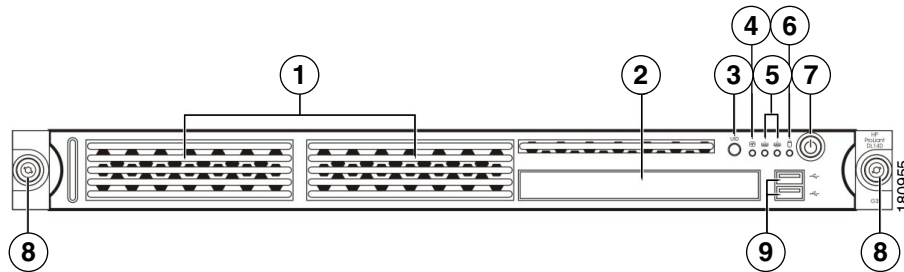
**Table 4-2 Cisco NAC Profiler Server Hardware Summary**

Cisco NAC Profiler Server Platform	Hardware Specifications	Diagrams
<b>“Profiler Lite”</b> <sup>1</sup> (based on NAC-3310 <sup>2,3</sup> )	<ul style="list-style-type: none"> <li>Single processor: Xeon 2.33 GHz dual core</li> <li>1 GB RAM</li> <li>160 GB NHP SATA HDD</li> </ul> <p><b>Note</b> Newer Cisco NAC-3310 based platforms feature a 160GB hard drive, while older NAC-3310 platforms 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.</p> <ul style="list-style-type: none"> <li>4 10/100/1000 LAN ports [2 Broadcom 5721 integrated NICs; 2 Intel e1000 PCI-X NICs (HP #NC360T)]</li> <li>CD/DVD-ROM Drive</li> <li>4 USB Ports (2 front, 2 rear)</li> </ul> <p><b>Note</b> NAC-3310 is based on <a href="#">HP ProLiant DL140 G3</a>.</p>	<ul style="list-style-type: none"> <li>“Profiler Lite Front Panel” on page 4</li> <li>“Profiler Lite Front Panel LEDs/Buttons” on page 4</li> <li>“Profiler Lite Rear Panel” on page 5</li> <li>“Profiler Lite Rear Panel LEDs” on page 6</li> </ul>
<b>“Profiler Server”</b> (based on NAC-3350 <sup>4</sup> )	<ul style="list-style-type: none"> <li>Single processor: Xeon 3.0 GHz dual core</li> <li>Dual power supply</li> <li>2 GB RAM</li> <li>2 x 72 GB SFF SAS RAID HDD</li> <li>Smart Array E200i Controller</li> <li>4 10/100/1000 LAN ports [2 Broadcom 5708 integrated NICs; 2 Intel e1000 PCI-X NICs (HP #NC360T)]</li> <li>CD/DVD-ROM Drive</li> <li>4 USB Ports (1 front, 1 internal, 2 rear)</li> </ul> <p><b>Note</b> NAC-3350 is based on <a href="#">HP ProLiant DL360 G5</a>.</p>	<ul style="list-style-type: none"> <li>“Profiler Server Front Panel” on page 6</li> <li>“Profiler Server Front Panel LEDs/Buttons” on page 7</li> <li>“Profiler Server Rear Panel” on page 8</li> <li>“Profiler Server Rear Panel LEDs” on page 8</li> </ul>

1. The Profiler Lite platform is supported as a new installation only and requires its own ISO file (upgrade does not apply). Only the `nac_profilerlite_2.1.8-37-K9.iso` file can be installed on the Profiler Lite platform.
2. NAC-3310 may require firmware/BIOS upgrades for the HP ProLiant DL140 G3. See the “[DL140 G3 Required BIOS/Firmware Upgrades](#)” section of the *Supported Hardware and System Requirements for Cisco NAC Appliance (Clean Access)* for details.
3. NAC-3310 supports iLO ([Lights Out 100i Remote Management](#)). The default iLO “Administrator” account has default username/password: admin/admin. Defaults can be changed through the BIOS setup.
4. NAC-3350 supports iLO2 ([Integrated Lights Out, version 2](#)). See panel tags for admin account details.

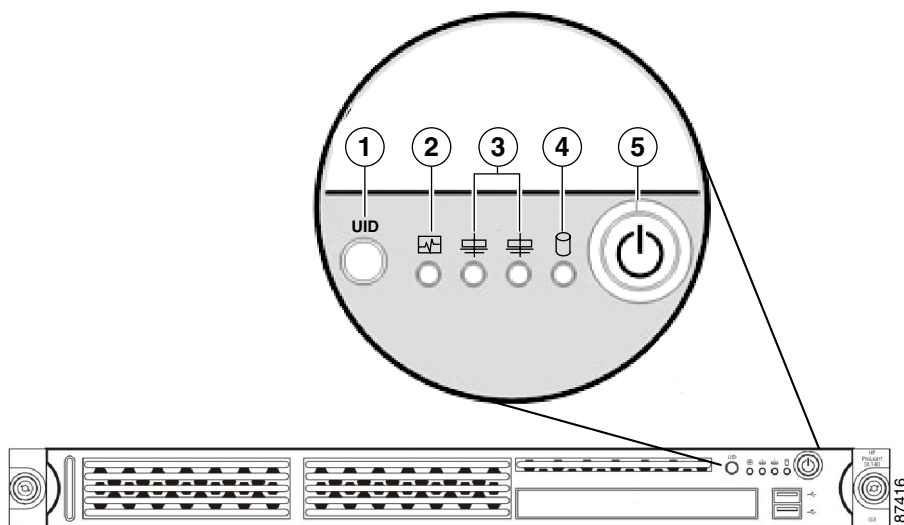
## “Profiler Lite” Front/Rear Panels (based on NAC-3310)

Figure 1 Profiler Lite Front Panel



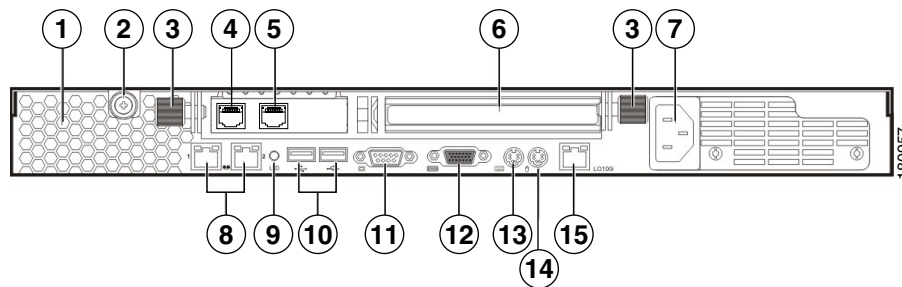
1	Hard disk drive (HDD) bay	6	HDD activity LED indicator (green)
2	CD-ROM/DVD drive	7	Power button with LED indicator (bicolor: green/amber)
3	UID (Unit identification) button with recessed LED indicator (blue)	8	Thumbscrews for the front bezel
4	System health LED indicator (amber)	9	Front USB ports
5	Activity/link status LED indicators for NIC 1 (eth0) and NIC2 (eth1) (green)		

Figure 2 Profiler Lite Front Panel LEDs/Buttons



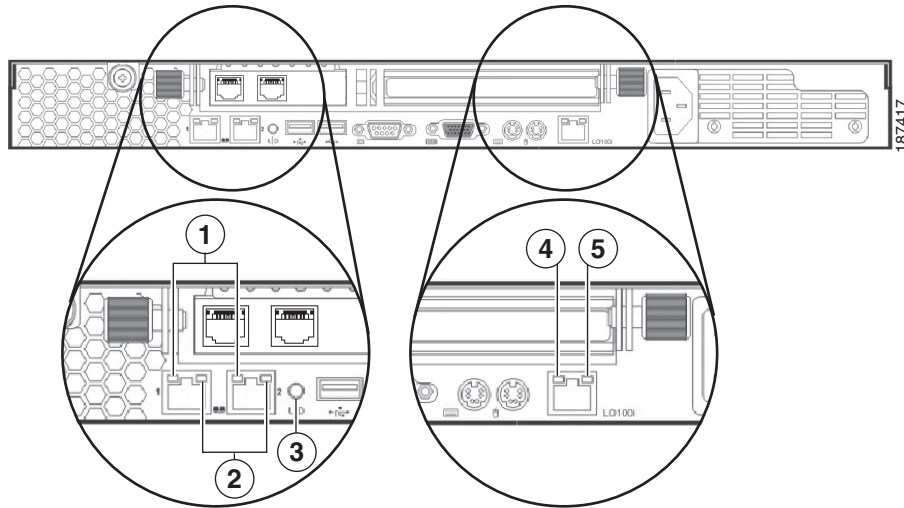
1	UID LED (recessed)	Blue = A UID button has been pressed.
2	System health LED	Off = System health is normal. Amber = A pre-failure system threshold has been breached. This can be any of the following: <ul style="list-style-type: none"> <li>At least one fan failure (system or processor fan).</li> <li>At least one of the temperature sensors reached critical level (system or processor thermal sensors).</li> <li>At least one memory module failure.</li> <li>A power supply unit error has occurred.</li> </ul>
3	Activity/link status LED for NIC 1 (eth0) and NIC 2 (eth1)	Solid green = An active network link exists. Flashing green = An ongoing network data activity exists. Off = The server is off-line.
4	HDD activity LEDs	Flashing green = Ongoing drive activity. Off = No drive activity.
5	Power status LED (recessed)	Green = The server has AC power and is powered up. Amber = The server has AC power and is in standby mode. Off = The server is powered off (AC power disconnected).

Figure 3 Profiler Lite Rear Panel



1	Ventilation holes	9	UID button with recessed LED indicator (blue)
2	Thumbscrew for the top cover	10	Rear USB ports (black)
3	Thumbscrews for the PCI riser board assembly	11	Video port (blue)
4	NIC 3 (eth2) and NIC 4 (eth3) PCI Express GbE LAN (RJ-45) ports (Intel)	12	Serial port
5		13	PS/2 keyboard port (purple)
6	Standard height/full-length PCI Express x16/PCI-X riser board slot cover	14	PS/2 mouse port (green)
7	Power supply cable socket	15	10/100 Mbps iLO LAN port for IPMI management (RJ-45)
8	NIC 1 (eth0) and NIC 2 (eth1) integrated GbE LAN (RJ-45) ports (Broadcom)		

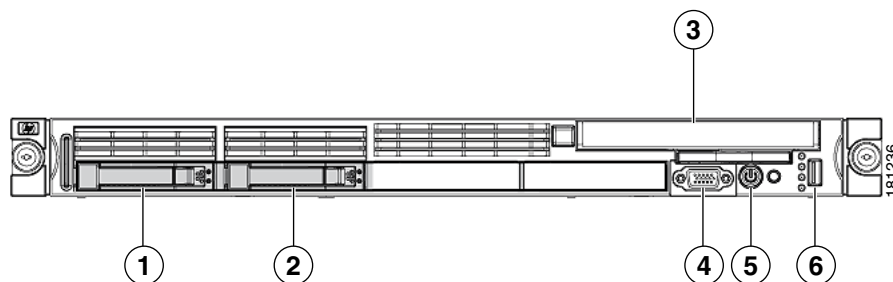
Figure 4 Profiler Lite Rear Panel LEDs



1	NIC activity/link status LEDs for NIC 1 (eth0) and NIC 2 (eth1)	Solid green = An active network link exists. Flashing green = An ongoing network data activity exists. Off = The server is off-line.
2	NIC network speed LEDs	Steady amber = The LAN connection is using a GbE link. Steady green = The LAN connection is using a 100 Mbps link. Off = The LAN connection is using a 10 Mbps link.
3	UID LED (recessed)	Blue = A UID button has been pressed.
4	Link status LED for the 10/100 Mbps LAN port	Green = A network link exists. Off = No network link exists.
5	Activity status LED for the 10/100 Mbps LAN port	Flashing green = Network activity exists. Off = No network activity exists.

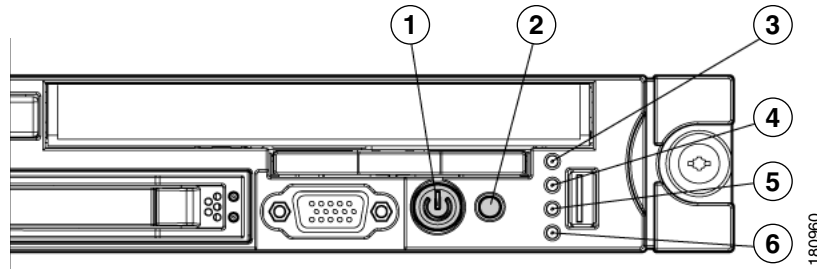
## Profiler Server Front/Rear Panels (based on NAC-3350)

Figure 4-5 Profiler Server Front Panel



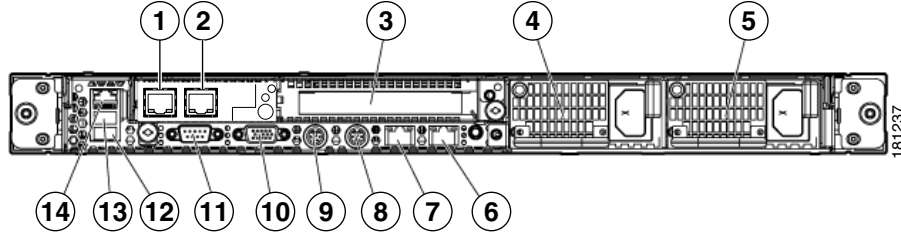
1	Hard drive bay 1	4	Video connector
2	Hard drive bay 2	5	HP Systems Insight Display
3	CD-ROM/DVD drive	6	USB connector

Figure 4-6 Profiler Server Front Panel LEDs/Buttons



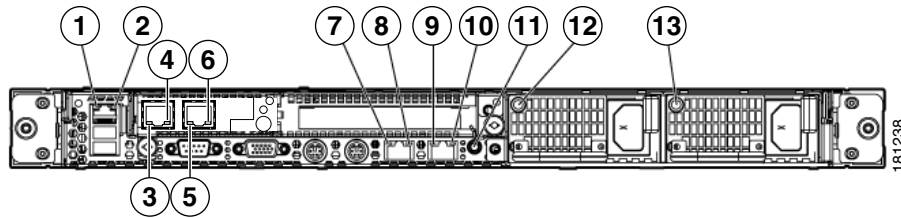
1	Power On/Standby button and system power LED	Green = System is on. Amber = System is shut down, but power is still applied. Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed; facility power is not available, or disconnected power button cable.
2	UID button/LED	Blue = Identification is activated Flashing blue = System is being managed remotely Off = Identification is deactivated
3	Internal health LED	Green = System health is normal. Amber = System health is degraded. (To identify the component in a degraded state, refer to “HP Systems Insight Display and LEDs.”) Red = System health is critical. (To identify the component in a critical state, refer to “HP Systems Insight Display and LEDs.”) Off = System health is normal when in standby mode.
4	External health LED (power supply)	Green = Power supply health is normal. Amber = Power redundancy failure occurred. Off = Power supply health is normal when in standby mode.
5	NIC 1 (eth0) link/activity LED	Green = Network link exists Flashing green = Network link and activity exist. Off = No link to network exists. If power is off, the front panel LED is not active. For status, view the rear panel LED for the RJ-45 connector ( <a href="#">Figure 4-8 on page 4-8</a> )
6	NIC 2 (eth1) link/activity LED	Green = Network link exists Flashing green = Network link and activity exist. Off = No link to network exists. If power is off, the front panel LED is not active. For status, view the rear panel LED for the RJ-45 connector ( <a href="#">Figure 4-8 on page 4-8</a> )

Figure 4-7 Profiler Server Rear Panel



1	NIC 3 (eth2) PCI-X port (Intel)	8	Keyboard connector (purple)
2	NIC 4 (eth3) PCI-X port (Intel)	9	Mouse connector (green)
3	PCI Express expansion slot 2	10	Video connector (blue)
4	Power supply bay 1	11	Serial connector
5	Power supply bay 2	12	USB connector
6	Integrated NIC 2 (eth1) port (Broadcom)	13	USB connector
7	Integrated NIC 1 (eth0) port (Broadcom)	14	iLO 2 NIC connector (RJ-45)

Figure 4-8 Profiler Server Rear Panel LEDs



1	iLO 2 NIC activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
2	iLO 2 NIC link LED	Green = Link exists Off = No link exists
3	10/100/1000 NIC 3 (Intel) Activity LED	Steady green = High activity Flashing green = Activity exists Off = No activity (if link LED is off, link is dead)
4	10/100/1000 NIC 3 (Intel) Link LED	Orange = 1000 Mbps Green = 100 Mbps Off = 10 Mbps (if activity LED is off, link is dead)
5	10/100/1000 NIC 4 (Intel) Activity LED	Steady green = High activity Flashing green = Activity exists Off = No activity (if link LED is off, link is dead)
6	10/100/1000 NIC 4 (Intel) Link LED	Orange = 1000 Mbps Green = 100 Mbps Off = 10 Mbps (if activity LED is off, link is dead)

7	10/100/1000 NIC 1 (Broadcom) Activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
8	10/100/1000 NIC 1 (Broadcom) Link LED	Green = Link exists Off = No link exists
9	10/100/1000 NIC 2 (Broadcom) Activity LED	Green = Activity exists Flashing green = Activity exists Off = No activity exists
10	10/100/1000 NIC 2 (Broadcom) Link LED	Green = Link exists Off = No link exists
11	UID button/LED	Blue = Identification is activated Flashing blue = System is being managed remotely Off = Identification is deactivated
12	Power supply 1 LED	Green = Normal Off = System is off or power supply has failed.
13	Power supply 2 LED	Green = Normal Off = System is off or power supply has failed.

**Note**

See the in-box documentation that shipped with your Cisco NAC Profiler Server for information on using the controls and interpreting the status LEDs on the front panel of the unit.

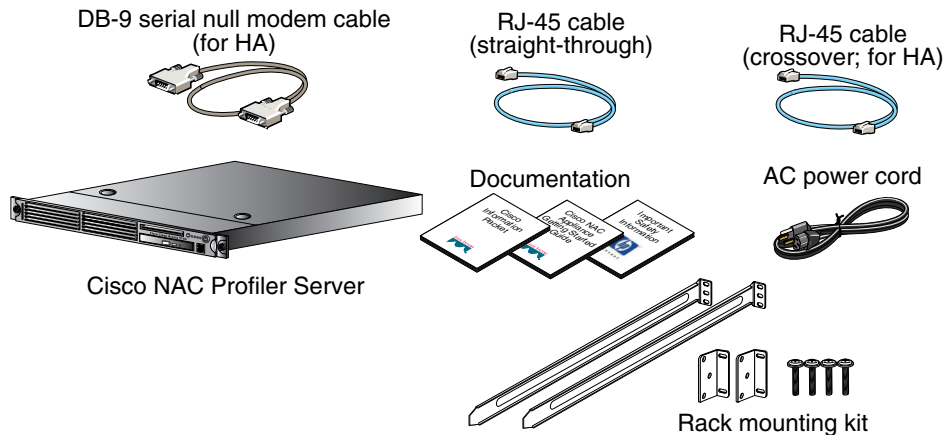
## Installing the Cisco NAC Profiler Server

**Caution**

Before performing the following procedure, see the safety instructions and important regulatory information in the *Important Safety Information* documentation packet.

Use the following steps to power-up the Cisco NAC Profiler Server and establish a network connection with the Management interface of the appliance:

- Step 1** Carefully open the shipping carton and remove the appliance. Remove any packing material from the appliance.
- Step 2** Confirm that the box contains the items shown in [Figure 4-9](#).

**Figure 4-9 Shipping Box Contents****Note**

Retain the carton and the shipping materials in the event that the unit needs to be shipped in the future.

**Step 3** Check the unit for obvious damage. If the appliance appears to be damaged, **DO NOT INSTALL** the unit. Contact customer support for instructions on how to obtain a replacement unit. Refer to [Cisco NAC Appliance Service Contract /Licensing Support](#) for details.

**Step 4** The appliance may be operated as a free-standing unit or mounted in a standard 19-inch equipment rack or cabinet.

**Note**

A rack-mounting kit is included in the shipment. For rack-mounting information and instructions, refer to the *IU Rack Hardware Installation Instructions for HP Products* document also included in the shipment.

**Step 5** After mounting the unit in the desired location, connect the power cable to the device's AC power receptacle located on the rear of the appliance and plug the other end of the power cable into a grounded AC outlet.

**Step 6** Connect a monitor, keyboard, and mouse to the Cisco NAC Profiler Server either directly or via a KVM switch by making the appropriate connections using the keyboard, mouse and video connectors provided on the rear of the Cisco NAC Profiler Server as shown in [Figure 4-7](#). Alternatively, a laptop or desktop computer running HyperTerminal or similar terminal emulation program can be used to access the Cisco NAC Profiler Server command line interface. Connect the RJ-45 connector of console cable to serial port B on the Cisco NAC Profiler Server, and the DB9F connector to the serial port of the laptop/desktop. Use the following parameters for the serial connection: 9600 Baud, 1 stop bit, 8 data bits, no parity.

**Note**

These peripherals are necessary only for the initial IP configuration of the management interface of the Cisco NAC Profiler Server that establishes a valid IP configuration and network connectivity for access to the web-based user interface later.

**Step 7** To connect the management interface of the Cisco NAC Profiler Server to the network, attach an appropriate Ethernet cable (equipped with an RJ-45 connector) to the copper Ethernet port labeled NIC 1 (eth0) located on the rear of the appliance. (See [Figure 4-7](#).)

**Step 8** Power on the Cisco NAC Profiler Server by pressing the power button on the front of the appliance. The diagnostic LEDs will flash a few times as part of the power-on self-test (POST). Status messages are displayed on the console as the appliance boots up.

- Step 9** Confirm the network connectivity to the Cisco NAC Profiler Server by observing the Ethernet port's status LEDs. The LEDs on the NIC cards of the Cisco NAC Profiler Server are interpreted as described in the table under [Figure 4-8](#).

**Tip**

If the NIC port LEDs do not indicate properly after connecting the cable from the appliance to the network port, check to make sure that the correct type of cable has been used to connect the Cisco NAC Profiler Server to the network and that the switch port is enabled and properly configured.

- Step 10** Connect the monitoring interface or interfaces to the desired network ports. The second on-board copper port (NIC 2 in [Figure 4-7](#) above) as well as the copper and or fiber ports added to the appliance expansion slots can be utilized as additional monitor ports for the Cisco NAC Profiler Server. The Cisco NAC Profiler Server uses the monitor ports to passively collect network packets of interest for use in Endpoint Profiling and Behavior Monitoring. See [Chapter 3, "Preparing for Deployment"](#) for further information.

**Tip**

In order for the monitoring ports to collect network traffic useful for Endpoint Profiling and Behavior Monitoring, traffic of interest needs to be redirected to the network infrastructure port connected to the Cisco NAC Profiler Server monitoring port using SPAN, RSPAN or other traffic mirroring capability provided by the installed network infrastructure. See [Chapter 7, "Configuring Collector Modules"](#) for detailed information on the use of monitoring ports.

The Cisco NAC Profiler Server may be operated as a single, non-redundant system or it can be configured as high-availability pair of servers:

- If implementing the system as a single Profiler Server, follow the instructions outlined in [Configure a Standalone Cisco NAC Profiler Server, page 4-11](#).
- If implementing the system as a HA pair of Profiler Servers, you will receive two physical appliances, which you will need to connect together and configure via web console to create a High-Availability pair. Refer to [Configure a Cisco NAC Profiler Server HA Pair, page 4-20](#) for details.

## Configure a Standalone Cisco NAC Profiler Server

The Cisco NAC Profiler Server ships with the Cisco NAC Profiler software pre-installed on the hard drive. When the system is started for the first time, a series of startup scripts guide the installer through several tasks necessary to configure the Cisco NAC Profiler Server and establish IP connectivity so that the web-based NAC Profiler user interface can be accessed via standard web browser from any point on the network. At the successful completion of these steps, continue to [Chapter 5, "Configuring Cisco NAC Profiler for the Target Environment"](#). Detailed configuration of the Cisco NAC Profiler system (Profiler Server and one or more Collectors) is performed as described in [Chapter 6, "Cisco NAC Profiler Server Configuration"](#).

## Collect Necessary Configuration Data

Prior to beginning the setup of a Cisco NAC Profiler Server in a Standalone configuration, collect and record the data in [Table 4-3](#) to ease the setup process.

**Table 4-3 Standalone Cisco NAC Profiler Server—Configuration Data**

Parameter	Value
Password for LINUX root user	
Password for LINUX beacon user	
Hostname	
Management Interface IP address	
Management Interface Net Mask	
Default Gateway	
Name Server IP address	
Profiler Database Password (default: <b>profiler</b> )	
Web Admin User Password (default: <b>profiler</b> )	

The following Cisco NAC Profiler Server startup tasks are completed via the command line using the keyboard and monitor connected to the appliance peripheral ports or through a laptop/desktop computer running terminal emulation as described [Installing the Cisco NAC Profiler Server, page 4-9](#). The scripts guide the user through input of basic configuration information to enable the Cisco NAC Profiler Server component of the Cisco NAC Profiler system.

## Initial System Startup—Set Passwords

Upon the Cisco NAC Profiler Server booting for the first time, a standard login prompt is presented either on the monitor connected to the appliance or displayed through terminal emulation on a connected laptop/desktop as shown in [Table 4-3](#)

**Figure 4-10 Cisco NAC Profiler System Login Prompt**

```

Fedora Core release 6 (Zod)
Kernel 2.6.20-1.2925.fc6 on an i686

profiler login: _

```

Two LINUX user accounts are used on the Cisco NAC Profiler Server: **root** and **beacon**. As the system is started for the first time, passwords for both accounts need to be established.

**Note**

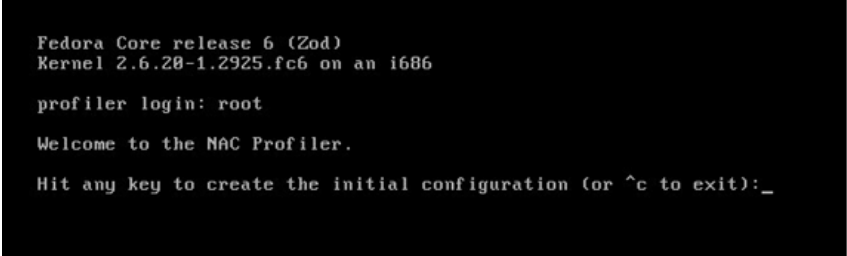
Make sure to note the passwords assigned to these accounts as they need to be accessed later.

- Step 1** In order to complete the initial Cisco NAC Profiler configuration, log into the system as the root LINUX user.
- Step 2** On the first boot of the system, there are no passwords for the root or beacon users.

**Step 3** Enter 'root' at the login prompt, and press Enter.

**Step 4** The system display the following message indicating that the system startup scripts are executing:

**Figure 4-11** Welcome to the Cisco NAC Profiler



```

Fedora Core release 6 (Zod)
Kernel 2.6.28-1.2925.fc6 on an i686

profiler login: root

Welcome to the NAC Profiler.

Hit any key to create the initial configuration (or ^c to exit):_

```



**Warning**

**Selecting Control-C or selecting Cancel on one of the user input screens while running the startup scripts will result in bypass of the configuration scripts, taking the user to the operating system command prompt without completing the initial configuration.**

**Step 5** Press the Enter key and create a password for the root user at the prompt.

If the password is too short or is derived from a dictionary word, the system gives a warning suggesting selection of an alternate, stronger password. Select a stronger password **or override** the warning by typing the same password again. An identical password string has to be entered twice in succession in order for the password to be accepted.

**Step 6** The system then prompts for a password for the **beacon user**. Choose a password for the beacon user.

**Step 7** After successfully setting the LINUX account passwords, the initial configuration scripts step the installer through several screens to set a number of environment-specific IP configuration parameters for the Cisco NAC Profiler Server including hostname, management interface IP address and mask, default gateway and name server (DNS server) for the newly installed Cisco NAC Profiler Server appliance. Referring to [Table 4-3](#) can greatly expedite this process.

These parameters enable the system to communicate across the network allowing the detailed configuration of the system to be accomplished via the web-based graphical user interface.

The following sections outline the steps and illustrate the interfaces for setting the IP configuration parameters for a new Cisco NAC Profiler Server.

## Configure Hostname

- Step 1** The first step in the IP configuration of the Cisco NAC Profiler Server is the assignment of its hostname (Figure 4-12).

**Figure 4-12** Configure Hostname

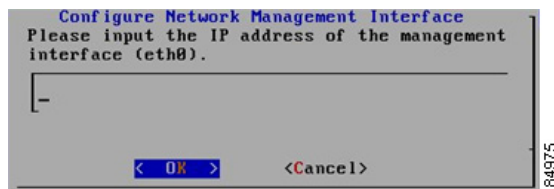


- Step 2** Enter the desired hostname for this Cisco NAC Profiler Server. Select OK and press Enter to go on to the next step of the configuration script.

## Configure Network Management Interface: IP Address, Net Mask and Default Gateway and Name Server

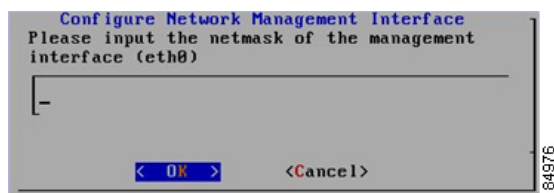
The network management interface is the primary communications interface for the Cisco NAC Profiler Server. It must be assigned IP configuration parameters that are appropriate for its operating environment. The device requires a valid host IP address, network mask and default gateway in order to be able to communicate via TCP/IP. The Cisco NAC Profiler Server is also provided with the address of the appropriate DNS server to be used for name resolution.

**Figure 4-13** Configure Network Management Interface: IP Address



- Step 1** After entering the desired IP address for the Cisco NAC Profiler Server management interface in dotted decimal notation (e.g., 10.10.10.1), press Enter to go to the next step and enter the network mask of the management interface.

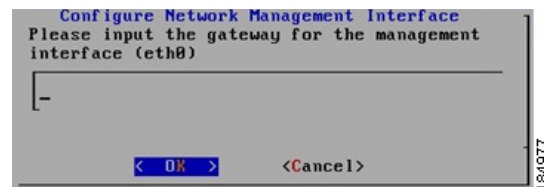
**Figure 4-14** Configure Network Management Interface Network Mask



- Step 2** Enter the network mask to be utilized by the management interface in dotted decimal notation (e.g., 255.255.0.0), select OK using the arrow keys and press Enter to go to the next configuration page which enables the setting of the default gateway IP address.

The default gateway is the IP address of the router interface servicing the network segment to which the Cisco NAC Profiler Server is physically connected. This parameter specifies the router the Cisco NAC Profiler Server will utilize to reach other subnets and networks beyond its own.

**Figure 4-15** Configure Network Management Interface: Gateway



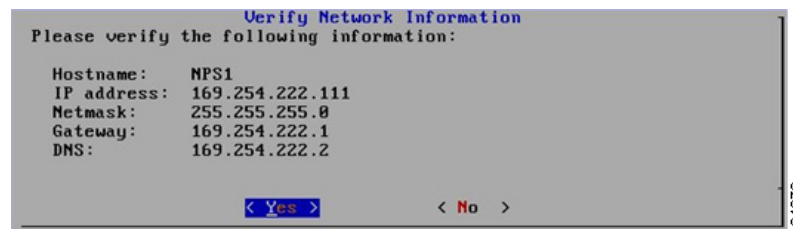
- Step 3** Enter the IP address of the desired default gateway for the Cisco NAC Profiler Server in dotted decimal notation (e.g., 10.10.10.254). OK using the arrow keys and press Enter to move onto the next step, name server (DNS) configuration.

**Figure 4-16** Configure Network Management Interface: Name Server



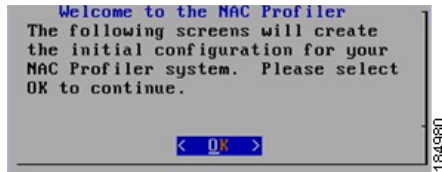
Upon entering the name server IP address, selecting OK and pressing enter, a summary of the IP Information configured thus far will be provided as illustrated in [Figure 4-17](#).

**Figure 4-17** Verify Network Information



Verify that the information entered thus far is correct. If changes are required, use the arrow keys to select No and press enter. This will cause the scripts to restart from the beginning of the assignment of the IP parameters. All data entered for these parameters will be lost and the data entry steps beginning with the assignment of the management interface IP address will restart.

If the information is correct, make certain that Yes is selected and press Enter. The configuration scripts will restart all the network interfaces on the Cisco NAC Profiler Server to make the configuration changes active on the management interface. After the interfaces restart successfully, the Welcome screen appears. (See [Figure 4-18](#).)

**Figure 4-18** Welcome to the Cisco NAC Profiler

At this time, the validity of the completed IP configuration can be verified by issuing a Ping to the IP address of the Cisco NAC Profiler Server. Successfully pinging the appliance indicates a valid IP configuration which is necessary for management of the system via the web-based user interface.

## Configure the Operational Parameters of Cisco NAC Profiler Server

Once the Cisco NAC Profiler Server has been configured for IP connectivity in the environment, the configuration scripts progress to setting up several parameters specific to the Cisco NAC Profiler Server such as installing and initializing the database and configuring the Cisco NAC Profiler for single-server or HA pair operation.

The first step is the selection of the password for the Cisco NAC Profiler Database and the administrative user account for the web-based NAC Profiler User Interface.



### Note

The admin web user account has full administrative access to the system configuration, including the creation and deletion of user accounts via the web interface. The database password is necessary for direct access to the database for operations such as backup and restore.

Figure 4-19 illustrates the screen that is used for setting the database password after progressing past the Welcome screen.

**Figure 4-19** Set Database Password

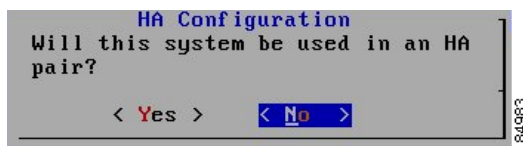
- Step 1** If the default Database password 'profiler' is acceptable, select OK using the arrow keys and press Enter to move onto the next step, or edit the password as desired selecting OK and pressing enter when finished.

The system will now setup and initialize the Cisco NAC Profiler database, and when complete prompt the administrator to provide the password for the web interface administrative user, username 'admin.'

The next screen sets the web-based user interface password for the admin user, which again defaults to 'profiler' as illustrated in Figure 4-20.

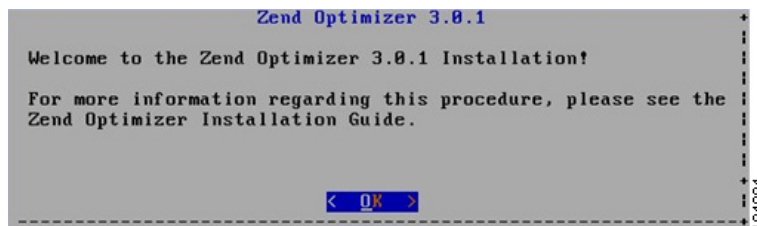
**Figure 4-20 Set Admin Web UI Password**

- Step 2** If the default password is acceptable, select OK using the arrow keys and press Enter to move onto the next step, or edit the password as desired. Press OK to proceed with the next step of the configuration, designating whether this Cisco NAC Profiler Server will operate as a single server, or in a High Availability (HA) pair.

**Figure 4-21 HA Configuration**

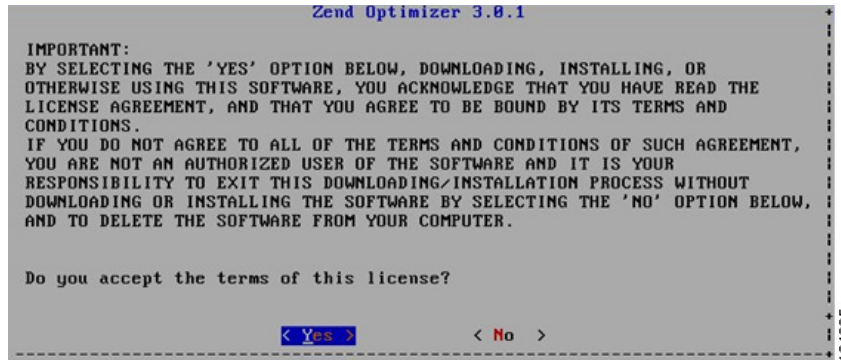
- Step 3** Select No and press enter to configure this Cisco NAC Profiler for standalone operation. The installation script will now install the Zend Optimizer. The Zend Optimizer is used to accelerate PHP performance within the Cisco NAC Profiler user interface.

- 
- Step 1** The following screen appears, select OK and press Enter to proceed with Zend Optimizer installation.

**Figure 4-22 Zend Optimizer Installation**

The next screen displays the end-user license for Zend Optimizer. Review the license for the Zend Optimizer, using the arrow keys to scroll up and down.

- Step 2** When you have completed reading the license agreement, select Exit and press Enter. The following screen appears that enables the installer to accept the agreement.

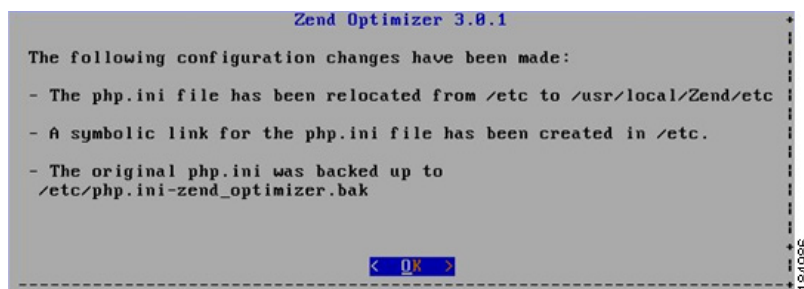
**Figure 4-23** Accept Zend Optimizer License

- Step 3** Select Yes to continue with installation. Selecting No will terminate the Cisco NAC Profiler configuration scripts.

Complete the following steps accomplished through a series of screens to finish the install of the Zend Optimizer:

- Step 1** Accept the default installation location (/usr/local/Zend) for the Zend Optimizer, select OK and press enter.
- Step 2** Confirm the location (/etc) of the PHP.ini file by accepting the default. Select OK and press enter.
- Step 3** Confirm that Apache (web server component used for serving NAC Profiler web-based UI) is in use, select Yes and press Enter.
- Step 4** Confirm the full path to the Apache Control Utility by accepting the default (/usr/sbin/apachectl) select OK and press Enter.

The Zend Optimizer installation begins, and successful Completion of the Zend Optimizer installation is indicated by receiving the following messages on the terminal:

**Figure 4-24** Zend Optimizer Configuration Change Notification

- Step 5** Select OK and press Enter to confirm the configuration changes. A “successful installation” screen like [Figure 4-25](#) appears.

**Figure 4-25** *Zend Optimizer Installation Successful*

```

Zend Optimizer 3.0.1
The installation has completed successfully.
Zend Optimizer is now ready for use.
You must restart your Web server for the modifications to take effect.

< OK >

```

- Step 6** Select OK and press enter, and the next screen prompts to confirm restart of the web server on the Cisco NAC Profiler.

**Figure 4-26** *Confirm Restart of Web Server*

```

Zend Optimizer 3.0.1
Restart the Web server now?

< Yes > < No >

```

- Step 7** Select OK and press Enter to complete the installation by restarting the web server. Upon successful restart of the web server, the following screen is displayed on the console.

**Figure 4-27** *Web Server Restart Complete*

```

Zend Optimizer 3.0.1
Apache has restarted successfully.

< OK >

```

- Step 8** Select OK to complete the installation of the Cisco NAC Profiler. Successful completion of the initial configuration is indicated by the following message displayed at the console.

**Figure 4-28** *Standalone Cisco NAC Profiler Installation Complete*

```

Installation complete.

Starting Profiler
o Starting Server

[root@profiler ~]# _

```

## Transition to Web Management

At this juncture, the Cisco NAC Profiler Server is ready for configuration via the web-based user interface. Using a standard browser on another network-attached PC or laptop, enter the following URL to confirm that the UI being served by the Cisco NAC Profiler Server is accessible over the network:

```
https://[IP address of management interface]/profiler
```

Enter **admin** as the username and the password selected above for the web interface. [Figure 4-29](#) web page should display in the browser:

**Figure 4-29** NAC Profiler Web UI Home Page



The session created for the initial configuration of the Cisco NAC Profiler Server appliance is still logged in as the root user at the appliance console. Issue the command “logout” at the prompt to logout of the system and lock the console.

This completes the initial configuration of your Cisco NAC Profiler Server appliance. Refer to [Configuring the Collector on the Clean Access Server, page 4-39](#) next, then continue to [Chapter 5, “Configuring Cisco NAC Profiler for the Target Environment”](#) for further configuration instructions of the Profiler system.

## Configure a Cisco NAC Profiler Server HA Pair

The Cisco NAC Profiler Server can be configured to run as a High Availability (HA) pair. In this configuration two Cisco NAC Profiler Server appliances are deployed, a Primary and Secondary. Profiler Server high-availability mode is an Active/Passive two-appliance configuration in which a standby Profiler Server appliance acts as a backup to an active Profiler Server appliance. While the active Profiler Server carries most of the workload under normal conditions, the standby monitors the active Profiler Server and keeps its data store synchronized with the active Profiler Server’s data. The data store includes system configuration information as well as the endpoint database.

If a failover event occurs, such as the active Profiler Server is shut down or stops responding to the peer’s “heartbeat” signal, the standby assumes the role of the active Profiler Server.

When configuring an HA pair, the steps outlined in this section should be followed carefully to ensure successful start-up of the system in HA mode. It is highly recommended that this section be read in its entirety prior to beginning configuration.

Before powering either appliance on and beginning any configuration activities, the following steps should be completed.

1. Both Cisco NAC Profiler Server appliances in the pair should be installed with power available, but not powered on.
2. The eth0 (management) interfaces should be connected to the network on ports that are configured appropriately to allow IP connectivity between the appliances when they are powered-up and configured.
3. The eth1 (heartbeat) interfaces should be interconnected in such a way as to provide a private LAN (e.g., via a crossover cable or standalone switch) for maintenance of the heartbeat signal between the appliances.
4. Determination of the host address of a third device, preferably on the same subnet with ICMP enabled (required) which both Cisco NAC Profiler Server appliances can ping to determine that they are still able to communicate with the network. This mechanism adds to the failover capability by detecting/reacting to the failure of a network interface or other network connectivity issue.
5. Gather and record the required configuration parameters for each individual appliance and the HA pair as outlined in the next section.

## Collect Necessary Configuration Data

Prior to beginning the setup of a Cisco NAC Profiler HA Pair, the data in the following tables should be collected and recorded to ease the setup process. Data that is specific to the Primary and Secondary appliances, as well as data that is shared by the pair needs to be collected and should be available for reference during the configuration steps outlined in the remaining sections of this chapter.

**Table 4-4 Secondary Cisco NAC Profiler Server Appliance**

Parameter	Value
Password for LINUX root user <sup>1</sup>	
Password for LINUX beacon user <sup>1</sup>	
Hostname	
Management Interface IP address	
Management Interface Net Mask	
Default Gateway	
Name Server IP address	
Profiler Database Password <sup>1</sup>	
Web Admin User Password <sup>1</sup>	

1. LINUX user passwords for the root and beacon users, the Cisco NAC Profiler database and admin web UI password should be identical for both appliances in the HA pair.

**Table 4-5 Primary Cisco NAC Profiler Server Appliance**

Parameter	Value
Password for LINUX root user <sup>1</sup>	
Password for LINUX beacon user <sup>1</sup>	

**Table 4-5 Primary Cisco NAC Profiler Server Appliance**

Hostname	
Management Interface IP address	
Management Interface Net Mask	
Default Gateway	
Name Server IP address	
Profiler Database Password <sup>1</sup>	
Web Admin User Password <sup>1</sup>	

1. LINUX user passwords for the root and beacon users, the Cisco NAC Profiler database and admin web UI password should be identical for both appliances in the HA pair.

In addition to the standard parameters that are specific to the Primary and Secondary Cisco NAC Profiler Servers in the HA pair; there are also several parameters that are required for the configuration of the virtualization and will be requested during the setup scripts:

- **Virtual HA IP Address**—The IP host address of the virtual management interface of the HA pair. This is the IP address that will be used to communicate with the Cisco NAC Profiler HA pair, and used by the HA pair when communicating with other network entities, regardless of which physical appliance is the Master. It is specified as a host address in dotted-decimal notation with the number of mask bits specified in CIDR format (e.g., 10.1.1.200/24)
- **Local HA Network**—Specify the first three octets of a private **network IP** address (e.g., 192.168.1) to be used for the heartbeat network between the 2 appliances (eth1 interfaces).
- **HA Authentication Key**—Specify a text-string to be utilized by the appliances to authenticate. **The HA Shared Key must be entered identically (case sensitive) on both appliances in order for the relationship to be established.**
- **HA External Ping Host**—This is the host IP address of another network device, preferably on the same subnet as the HA pair **that will respond to ICMP echo requests** from the Cisco NAC Profiler Server appliances. The Profiler Server appliances will ping this device regularly to ensure that they still have network connectivity as a measure to detect the failure of their network interface.

**Table 4-6 Cisco NAC Profiler Server HA Pair Parameters**

Parameter	Value
Virtual HA IP address	
Local HA Network	
HA Authentication Key	
HA External Ping Host	

Once this information is collected, the configuration of the HA pair can be initiated.

The sequence of events for the configuration of a Cisco NAC Profiler HA pair is as follows:

1. Configure the Cisco NAC Profiler Server that will be the **Secondary** appliance up until the point that the “Subscribe” process is ready to be run.
2. Configure the Cisco NAC Profiler Server that will be the Primary appliance through to completion.

- Return to the Secondary appliance and run the Subscribe process which will initiate the communication between the two appliances, enabling the HA pair for completion of the system configuration as described in [Chapter 5, “Configuring Cisco NAC Profiler for the Target Environment”](#).

These steps will be outlined in detail in the remainder of this chapter.

## Configure the Secondary Cisco NAC Profiler Server of the HA Pair

Power-on the Cisco NAC Profiler Server designated as the Secondary appliance of the pair with the data collection sheet completed in the last section readily available.

Upon the Cisco NAC Profiler booting for the first time, a standard login prompt is presented either on the monitor connected to the appliance or displayed through terminal emulation on a connected laptop/desktop as shown in [Figure 4-30](#):

**Figure 4-30** Cisco NAC Profiler system login prompt

```
Fedora Core release 6 (Zod)
Kernel 2.6.28-1.2925.fc6 on an i686

profiler login: root

Welcome to the NAC Profiler.

Hit any key to create the initial configuration (or ^c to exit):_
```

184992

There are two LINUX user accounts on the Cisco NAC Profiler that are utilized: root and ‘beacon.’ As the system is started for the first time, passwords for both accounts need to be established.



### Note

Be sure to note the passwords assigned to these accounts as they may need to be accessed later.

- Step 1** In order to complete the initial Cisco NAC Profiler configuration, log into the system as the root LINUX user.

On the first boot of the system, there will be no passwords for the root or beacon users.

- Step 2** Enter ‘root’ at the login prompt, and press Enter.

The system will display the following message indicating that the system startup scripts are executing:

**Figure 4-31** Welcome to the Cisco NAC Profiler

```
Fedora Core release 6 (Zod)
Kernel 2.6.28-1.2925.fc6 on an i686

profiler login: root

Welcome to the NAC Profiler.

Hit any key to create the initial configuration (or ^c to exit):_
```

184993

**Warning**

**Selecting Control-C or selecting Cancel on one of the user input screens while running the startup scripts will result in bypass of the configuration scripts, taking the user to the operating system command prompt without completing the initial configuration.**

- Step 3** Press the enter key and you will be prompted to create a password for the root user.
- If the password is too short or is derived from a dictionary word, the system will give a warning suggesting selection of an alternate, stronger password. Select a stronger password **or override** the warning by typing the same password again.
- An identical password string has to be entered twice in succession in order for the password to be accepted. The system will then prompt for a password for the beacon user.
- Step 4** Choose a password for the beacon user referring to the notes above regarding root password selection.
- At the successful completion of setting the LINUX account passwords, The initial configuration scripts will then step the installer through several screens to set a number of environment-specific IP configuration parameters for the Cisco NAC Profiler Server including hostname, management interface IP address and mask, default gateway and name server (DNS server) for the newly installed Cisco NAC Profiler Server appliance. Referring to the information in [Collect Necessary Configuration Data, page 4-21](#) can greatly expedite this process.
- These parameters enable the system to communicate across the network allowing the detailed configuration of the system to be accomplished via the web-based graphical user interface as outlined in [Chapter 5, “Configuring Cisco NAC Profiler for the Target Environment”](#).

The following sections outline the steps and illustrate the interfaces for setting the IP configuration parameters for the newly installed Cisco NAC Profiler Server.

## Configure Hostname

The first step in the IP configuration of the Cisco NAC Profiler Server is the assignment of its hostname, which is accomplished through the screen illustrated in [Figure 4-32](#).

**Figure 4-32** *Configure Hostname*

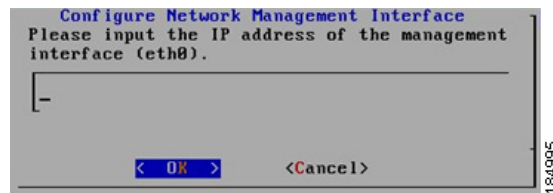


Enter the desired hostname for this Cisco NAC Profiler Server. Select OK and press Enter to go on to the next step of the configuration script.

## Configure Network Management Interface: IP Address, Net Mask, Default Gateway, Name Server

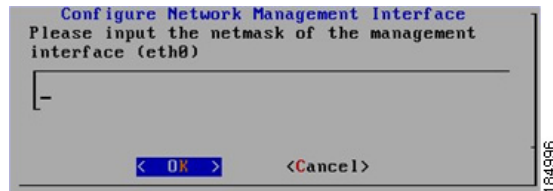
The network management interface is the primary communications interface for the Cisco NAC Profiler Server. It must be assigned IP configuration parameters that are appropriate for its operating environment such that IP communications are enabled in the environment the appliance will be installed in. The device requires a valid host IP address, network mask and default gateway in order to be able to communicate via the TCP/IP. The Cisco NAC Profiler Server is also provided with the address of the appropriate DNS server to be used for name resolution.

**Figure 4-33** Configure Network Management Interface—IP Address



- Step 1** After entering the desired IP address for the Cisco NAC Profiler Server management interface in dotted decimal notation (e.g., 10.10.10.1), press Enter to go to the next step and enter the network mask of the management interface.

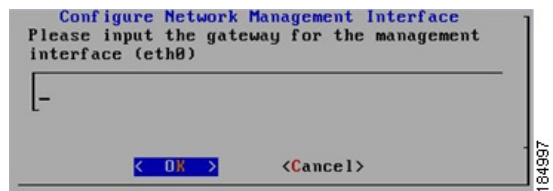
**Figure 4-34** Configure Network Management Interface—Network Mask



- Step 2** Enter the network mask to be utilized by the management interface in dotted decimal notation (e.g., 255.255.0.0), select OK using the arrow keys and press Enter to go to the next configuration page which enables the setting of the default gateway IP address.

The default gateway is the IP address of the router interface servicing the network segment to which the Cisco NAC Profiler Server is physically connected. This parameter specifies the router the Cisco NAC Profiler Server will utilize to reach other subnets and networks beyond its own.

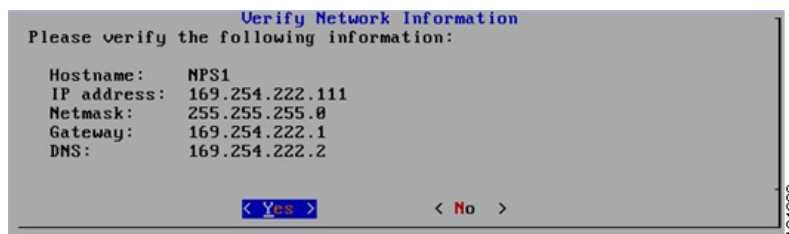
**Figure 4-35** Configure Network Management Interface—Gateway



- Step 3** Enter the IP address of the desired default gateway for the Cisco NAC Profiler Server in dotted decimal notation (e.g., 10.10.10.254). OK using the arrow keys and press Enter to move onto the next step, name server (DNS) configuration.

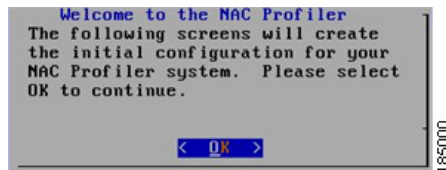
**Figure 4-36** Configure Network Management Interface: Name Server

Upon entering the name server IP address, selecting OK and pressing enter, a summary of the IP Information configured thus far will be provided as illustrated in [Figure 4-37](#).

**Figure 4-37** Verify Network Information

Verify that the information entered thus far is correct. If changes are required, use the arrow keys to select No and press enter. This will cause the scripts to restart from the beginning of the assignment of the IP parameters. All data entered for these parameters will be lost and the data entry steps beginning with the assignment of the management interface IP address will restart.

If the information is correct, make certain that Yes is selected and press Enter. The configuration scripts will restart all the network interfaces on the Cisco NAC Profiler Server to make the configuration changes active on the management interface. After the interfaces restart successfully, a Welcome screen appears. (See [Figure 4-38](#).)

**Figure 4-38** Welcome to the Cisco NAC Profiler

At this time, the validity of the completed IP configuration can be verified by issuing a Ping to the IP address of the Cisco NAC Profiler Server. Successfully pinging the appliance indicates a valid IP configuration which is necessary for management of the system via the web-based user interface.

## Configure the Operational Parameters of the Cisco NAC Profiler Server

Once the Cisco NAC Profiler Server has been configured for IP connectivity in the environment, the configuration scripts progress to setting up several parameters specific to the Cisco NAC Profiler Server such as installing and initializing the database and configuring the Cisco NAC Profiler for single-server or HA pair operation.

The first step is the selection of the password for the Cisco NAC Profiler Database and the administrative user account for the web-based NAC Profiler User Interface.

**Note**

The admin web user account has full administrative access to the system configuration, including the creation and deletion of user accounts via the web interface. The database password is necessary for direct access to the database for operations such as backup and restore.

Figure 4-39 illustrates the screen that is used for setting the database password after progressing past the Welcome screen.

**Figure 4-39 Set Database Password**



- Step 1** If the default Database password 'profiler' is acceptable, select OK using the arrow keys and press Enter to move onto the next step, or edit the password as desired selecting OK and pressing enter when finished.

The system will now setup and initialize the Cisco NAC Profiler database, and when complete prompt the administrator to provide the password for the web interface administrative user, username 'admin.'

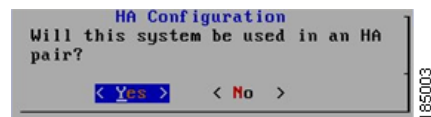
The next screen sets the web-based user interface password for the admin user, which again defaults to 'profiler' as illustrated in Figure 4-40.

**Figure 4-40 Set Admin Web UI Password**



- Step 2** If the default password is acceptable, select OK using the arrow keys and press Enter to move onto the next step, or edit the password as desired. Press OK to proceed with the next step of the configuration, designating whether this Cisco NAC Profiler Server will operate as a single server, or in a High Availability (HA) pair.

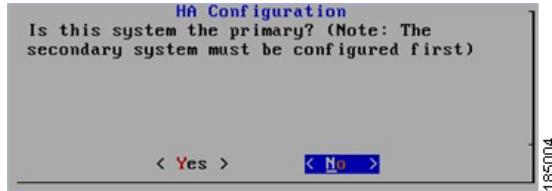
**Figure 4-41 Configure HA Pair**



- Step 3** Select Yes using the arrow keys and press enter to configure this Cisco NAC Profiler HA operation.

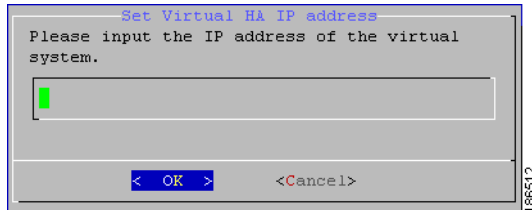
Selecting Yes progresses the script to asking the installer if this Cisco NAC Profiler Server will be the Primary or Secondary.

**Figure 4-42 HA Configuration – Secondary Appliance**



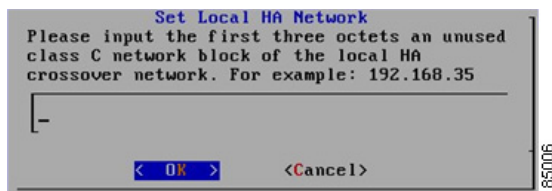
- Step 4** Use the arrow keys to select **No**, and press enter to set up the Secondary Cisco NAC Profiler Server. Refer to [Collect Necessary Configuration Data, page 4-21](#) in the first section of this chapter. The next several screens allow for the entry of the HA pair attributes, beginning with the Virtual HA IP address, as shown in [Figure 4-43](#).

**Figure 4-43 Set Virtual IP Address of Secondary**



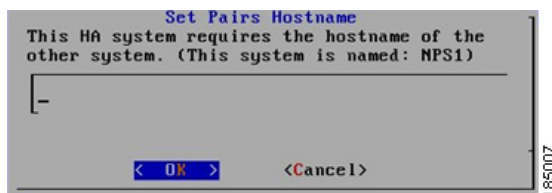
- Step 5** Input the host address chosen for the virtual IP address of the HA pair. When the desired virtual HA IP address has been entered, select OK. Next, the script will prompt for the local HA network address, as shown in [Figure 4-44](#).

**Figure 4-44 Set Local HA Network for Secondary**



- Step 6** Specify the **first three octets** of the class C network selected for the private LAN between the appliances used for the maintenance of heartbeat. Select OK and Enter to enter the next parameter, the hostname of the Primary appliance in the next screen shown in [Figure 4-45](#).

**Figure 4-45 Set Pairs Hostname for Secondary**



- Step 7** Enter the hostname of the Primary HA Cisco NAC Profiler Server, refer to the data sheets collected at the beginning of the installation process to ensure that the hostname entered here matches the hostname of the other appliance in the HA pair exactly.
- Step 8** Select OK and Enter to enter the next parameter, the HA Authentication Key in the next screen.

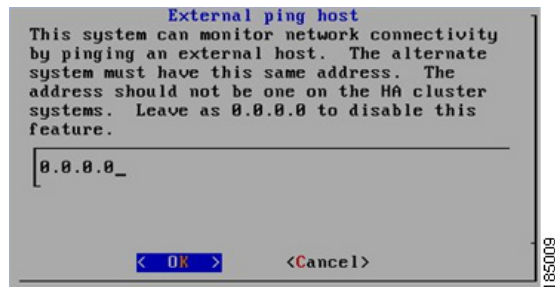
**Figure 4-46 Set HA Authentication Key for Secondary**



The HA authentication key is a secret shared between the two appliances. The HA authentication key between the two members of an HA pair must match exactly in order for the HA relationship to be established. Ensure that the HA authentication key entered in this step for the Secondary appliance is entered identically for the Primary appliance in the next step of the configuration process.

- Step 9** Once the desired HA authentication key is entered, select OK and press enter to move to the next parameter, the External Ping Host which is entered as shown in [Figure 4-47](#).

**Figure 4-47 External Ping Host for Secondary**



The External Ping Host should be a device external to the HA pair that is enabled to respond to ICMP Echo Requests. This is an optional parameter in the HA configuration but it is highly recommended that it be used as it is utilized to guard against network interface failure. The external ping host should be identical for both appliances in the HA pair. If this additional failover protection is not desired, leave the default IP address of 0.0.0.0.

- Step 10** Select OK and Enter.

After the external ping host is entered, the startup scripts will display a summary of all the HA parameters entered for the Primary appliance as illustrated in [Figure 4-48](#).

**Figure 4-48** Verify HA Information for Secondary

```

Verify HA Information
Please verify the following information:

Primary Host:          no
Virtual IP address:   169.254.222.225/24
Local Hostname:       NPS1
Remote Hostname:      NPS2
HA interface prefix:  192.168.1
Primary IP:           192.168.1.100
Secondary IP:         192.168.1.101
Auth String:          GBSbeacon
Ping host:            169.254.222.1

< Yes >           < No >

```

This screen allows for the checking of all the HA parameters entered for the Secondary Cisco NAC Profiler Server in the HA pair being configured.

- Step 11** If all the parameters are correct, select Yes and Enter to complete the HA Configuration of the Secondary appliance.

If a correction or change needs to be made, selecting no will restart the process—all previously entered parameters will be lost.

Upon selecting yes, the Secondary Cisco NAC Profiler Server will initialize the HA configuration.

At the completion of that process, the startup scripts will resume with the setup of the remaining parameters for the secondary Cisco NAC Profiler Server.

- Step 12** The installation script will now install the Zend Optimizer. The Zend Optimizer is used to accelerate PHP performance within the Cisco NAC Profiler user interface. The following screen appears, select OK and press Enter to proceed with Zend Optimizer installation.

**Figure 4-49** Zend Optimizer Installation

```

Zend Optimizer 3.0.1
Welcome to the Zend Optimizer 3.0.1 Installation!

For more information regarding this procedure, please see the
Zend Optimizer Installation Guide.

< OK >

```

The next screen displays the end-user license for Zend Optimizer. Review the license for the Zend Optimizer, using the arrow keys to scroll up and down.

- Step 13** When you have completed reading the license agreement, select Exit and press Enter. The following screen appears that enables the installer to accept the agreement.

**Figure 4-50** Accept Zend Optimizer License

```

Zend Optimizer 3.8.1

IMPORTANT:
BY SELECTING THE 'YES' OPTION BELOW, DOWNLOADING, INSTALLING, OR
OTHERWISE USING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THE
LICENSE AGREEMENT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS AND
CONDITIONS.
IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF SUCH AGREEMENT,
YOU ARE NOT AN AUTHORIZED USER OF THE SOFTWARE AND IT IS YOUR
RESPONSIBILITY TO EXIT THIS DOWNLOADING/INSTALLATION PROCESS WITHOUT
DOWNLOADING OR INSTALLING THE SOFTWARE BY SELECTING THE 'NO' OPTION BELOW,
AND TO DELETE THE SOFTWARE FROM YOUR COMPUTER.

Do you accept the terms of this license?

< Yes >          < No  >

```

- Step 14** Select Yes to continue with installation. Selecting No will terminate the Cisco NAC Profiler configuration scripts.

Complete the following steps accomplished through a series of screens to finish the install of the Zend Optimizer:

- Step 1** Accept the default installation location (/usr/local/Zend) for the Zend Optimizer, select OK and press enter.
- Step 2** Confirm the location (/etc) of the PHP.ini file by accepting the default. Select OK and press enter.
- Step 3** Confirm that Apache (web server component used for serving NAC Profiler web-based UI) is in use, select Yes and press Enter.
- Step 4** Confirm the full path to the Apache Control Utility by accepting the default (/usr/sbin/apachectl) select OK and press Enter.

The Zend Optimizer installation begins, and successful Completion of the Zend Optimizer installation is indicated by receiving the following messages on the terminal:

**Figure 4-51** Zend Optimizer Configuration Change Notification

```

Zend Optimizer 3.8.1

The following configuration changes have been made:

- The php.ini file has been relocated from /etc to /usr/local/Zend/etc
- A symbolic link for the php.ini file has been created in /etc.
- The original php.ini was backed up to
  /etc/php.ini-zend_optimizer.bak

< OK >

```

- Step 5** Select OK and press Enter to confirm the configuration changes. A “successful installation” screen like [Figure 4-52](#) appears.

**Figure 4-52 Zend Optimizer Installation Successful**

```

Zend Optimizer 3.0.1
The installation has completed successfully.
Zend Optimizer is now ready for use.
You must restart your Web server for the modifications to take effect.

< OK >
185014

```

- Step 6** Select OK and press enter, and the next screen prompts to confirm restart of the web server on the Cisco NAC Profiler.

**Figure 4-53 Confirm Restart of Web Server**

```

Zend Optimizer 3.0.1
Restart the Web server now?

< Yes > < No >
185015

```

- Step 7** Select OK and press Enter to complete the installation by restarting the web server. Upon successful restart of the web server, the following screen is displayed on the console.

**Figure 4-54 Web Server Restart Complete**

```

Zend Optimizer 3.0.1
Apache has restarted successfully.

< OK >
185016

```

- Step 8** Select OK to complete the installation of the Secondary Cisco NAC Profiler Server of the HA pair. The following message at the console indicates successful completion of a Secondary appliance of an HA pair:

**Figure 4-55 Installation of Secondary Complete**

```

Installation complete.

Continue with the installation and configuration of the primary NAC Profiler
system. Once completed, return to this system user and run (as root):
/usr/ beacon/sql/subscribe.sh

[root@profiler ~]# _
185017

```

As outlined previously and stated in the message above, the Secondary Cisco NAC Profiler Server will need to be revisited after the completion of the configuration of the Primary appliance. Proceed with the configuration of the Primary as outlined in [Configure the Primary Cisco NAC Profiler Server of the HA Pair, page 4-33](#), and [Run the Subscribe Script on the Secondary Appliance, page 4-37](#) details the process for running Subscribe to initialize the Cisco NAC Profiler HA pair.

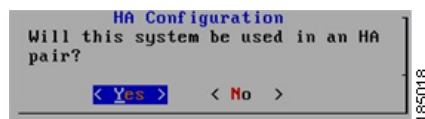
## Configure the Primary Cisco NAC Profiler Server of the HA Pair

Power-on the Cisco NAC Profiler Server designated as the Primary appliance of the pair with the data collection sheet completed in the last section readily available.

The initial startup of the appliance: assignment of network parameters and initial configuration of the Cisco NAC Profiler Server follows the exact same sequence as that outlined for the Secondary Server in the previous section. Using the data sheet parameters collected in the first section of this chapter for the **Primary Cisco NAC Profiler**, repeat the steps from the top of page 22 through the middle of page 30.

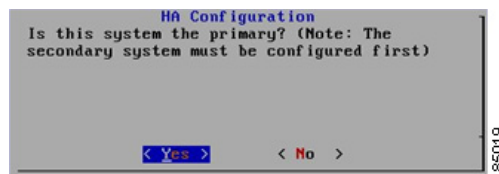
When the screen prompts for whether this system will be used in an HA pair (as illustrated in [Figure 4-56](#)), resume the Primary appliance setup procedure below.

**Figure 4-56** *Configure HA Pair*



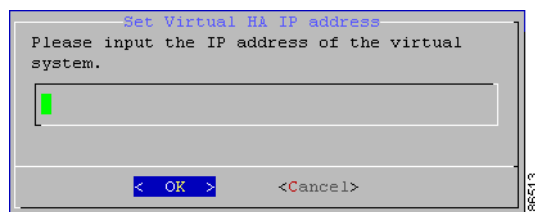
- Step 1** Select Yes using the arrow keys and press enter to configure this Cisco NAC Profiler HA operation. Selecting Yes progresses the script to asking the installer if this Cisco NAC Profiler Server will be the Primary or Secondary.

**Figure 4-57** *HA Configuration—Primary Appliance*

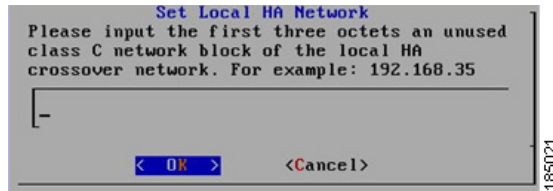


- Step 2** Use the arrow keys to select Yes, and press enter to set up the Primary Cisco NAC Profiler Server. Refer to [Collect Necessary Configuration Data](#), page 4-21 in the first section of this chapter. The next several screens allow for the entry of the HA pair attributes for the Primary, beginning with the Virtual HA IP address, as shown in [Figure 4-58](#).

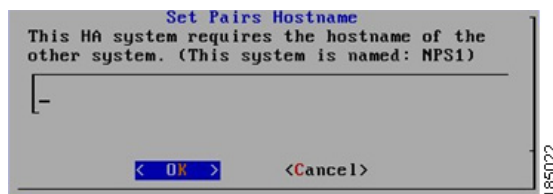
**Figure 4-58** *Set Virtual IP Address of Primary*



- Step 3** Input the host address chosen for the virtual IP address of the HA pair. Next, the script will prompt for the local HA network address, as shown in [Figure 4-59](#).

**Figure 4-59 Set Local HA Network for Primary**

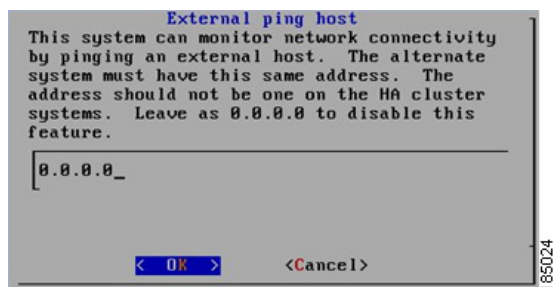
- Step 4** Specify the **first three octets** of the class C network selected for the private LAN between the appliances used for the maintenance of heartbeat between the Primary and Secondary appliances. Select OK and Enter to enter the next parameter, the hostname of the other appliance in the next screen shown in [Figure 4-60](#).

**Figure 4-60 Set Pairs Hostname for Primary**

- Step 5** Enter the **hostname of the Secondary HA Cisco NAC Profiler Server**; refer to the data sheets collected at the beginning of the installation process to ensure that the hostname entered here matches the hostname of the Secondary exactly.
- Step 6** Select OK and Enter to enter the next parameter, the HA Authentication Key in the next screen.

**Figure 4-61 Set HA Authentication Key for Primary**

- Step 7** Ensure that the HA authentication key entered in this step for the Primary appliance is entered identically to that specified for the Secondary appliance in the previous step of the configuration process. Once the desired HA authentication key is entered, select OK and press enter to move to the next parameter, the External Ping Host which is entered as shown in [Figure 4-62](#).

**Figure 4-62 External Ping Host for Primary**

The External Ping Host specified for the Primary should be the same device specified for the Secondary. After the external ping host is entered, the startup scripts display a summary of all the HA parameters entered for the Primary appliance as illustrated in Figure 4-63.

**Figure 4-63** Verify HA Information for Primary

```

Verify HA Information
Please verify the following information:

Primary Host:          yes
Virtual IP address:   169.254.222.225/24
Local Hostname:       NPS1
Remote Hostname:      NPS2
HA interface prefix:  192.168.1
Primary IP:           192.168.1.100
Secondary IP:         192.168.1.101
Auth String:          GBSbeacon
Ping host:            169.254.222.1

< Yes >      < No >
  
```

This screen allows for the checking of all the HA parameters entered for the Primary Cisco NAC Profiler Server in the HA pair being configured.



**Note**

Before selecting Yes and proceeding with the setup of HA on the Primary appliance, ensure that the HA parameters on the Primary are consistent with those configured on the Secondary in the previous step. In particular, ensure that the appliance hostnames, HA interface prefix and the HA auth string are consistent with that entered on the Secondary appliance. Doing so will ensure that the HA pair will come up successfully on the first attempt. It is also good to verify again that the crossover cable for the heartbeat between the appliances is connected to the eth1 interface on both appliances, with link indicated on both sides prior to proceeding.

**Step 8** If all the parameters are correct, select Yes and Enter to complete the HA Configuration of the Primary appliance.

If a correction or change needs to be made, selecting no will restart the process—all previously entered HA parameters for the Primary will be lost and will have to be entered again.

Upon selecting yes, the Primary Cisco NAC Profiler Server will initialize the HA configuration.

Upon completion of the HA initialization, the following message will display at the console:

**Figure 4-64** Completion of HA Initialization on Primary

```

*** You will be prompted for the beacon password on the secondary system.
*** Hit <enter> to continue.

Warning: Permanently added '172.16.1.101' (RSA) to the list of known hosts.
beacon@172.16.1.101's password:
pub                               100% 402      0.4KB/s   00:00
Warning: Permanently added '172.16.1.101' (RSA) to the list of known hosts.
Stopping High-Availability services:
[ OK ]
Waiting to allow resource takeover to complete:
[ OK ]
Starting High-Availability services:
2007/07/30_16:12:28 INFO: Resource is stopped
[ OK ]
Please, wait ...
  
```

As part of the HA setup, an SSH session is initiated between the two appliances for the purpose of creating a permanent SSH channel that will be used for HA database updates over the heartbeat connection (eth1).

In completing this step, the Primary appliance will require the LINUX “beacon” user password for the Secondary appliance. Hit enter to continue and then enter the password for the beacon user on the Secondary appliance when prompted as shown in [Figure 4-64](#).

You will see “Warning” messages on the screen as the SSH session is established. Note that the IP address that displays on this screen is the “Secondary IP” address that was automatically determined based on the “Set Local HA Network” parameter that was configured earlier (see [Figure 4-44 on page 4-28](#)).

After High-Availability services are stopped and restarted as part of the installation process, the startup scripts will resume with the setup of the remaining parameters for the Primary Cisco NAC Profiler Server.

The installation script will now install the Zend Optimizer on the Primary appliance. The Zend installation process for the Primary is identical to that of the Secondary. If necessary, refer to that procedure in the last section beginning on page 34. Step through the process to complete Zend installation. At the successful completion of that installation, the installer will be prompted to restart the web server as shown in [Figure 4-65](#).

**Figure 4-65 Confirm Restart of Web Server**

```

Zend Optimizer 3.0.1
Restart the Web server now?
< Yes > < No >
185027

```

- Step 1** Select OK and press Enter to complete the installation by restarting the web server on the Primary Cisco NAC Profiler Server. Upon successful restart of the web server, the following screen is displayed on the console.

**Figure 4-66 Web Server Restart Complete**

```

Zend Optimizer 3.0.1
Apache has restarted successfully.
< OK >
185028

```

- Step 2** Select OK to complete the installation of the Primary Cisco NAC Profiler Server of the HA pair. The following message at the console indicates successful completion of a Primary appliance of an HA pair:

**Figure 4-67** Successful Installation on Primary appliance of HA pair

```

Installation complete.
[root@profiler ~]#

```

## Run the Subscribe Script on the Secondary Appliance

After the successful completion of the previous step which included complete configuration of the Primary appliance, and the successful establishment of an SSH session between the two appliances in the HA pair, the Secondary appliance must be revisited in order to run the “subscribe.sh” script.

If the Secondary appliance is not already logged in as root, SSH to the Secondary appliance IP as user “beacon”.

**su** – to elevate to the root user by providing the root password

Run the “subscribe script” by typing `/usr/beacon/sql/subscribe.sh` as shown in [Figure 4-68](#).

**Figure 4-68** Run `subscribe.sh` on Secondary

```

Installation complete.

Continue with the installation and configuration of the primary NAC Profiler
system. Once completed, return to this system user and run (as root):
/usr/beacon/sql/subscribe.sh

[root@profiler]# /usr/beacon/sql/subscribe.sh
Warning: Permanently added '172.16.1.100' (RSA) to the list of known hosts.
Starting High-Availability services:
2007/07/30_01:23:59 INFO: Resource is stopped
[ OK ]
is slave
[root@profiler]#

```

After the SSH channel is established between the two appliances in the HA pair, High-Availability services will initialize and this secondary appliance will become the “slave” of the HA pair.

This completes the installation scripts for a pair of Profiler Server appliances in HA mode. At this time, the remaining configuration of the Cisco NAC Profiler system can be completed using the web UI, managing the system via the Virtual IP address assigned in the configuration of the Cisco NAC Profiler Servers.

## Verify HA Operation

To verify proper operation of the HA process at this stage of the configuration, verify that both members of the pair are running the heartbeat and SLON processes which are required for normal HA operation. Complete the following steps to ensure these processes are running on both members of the HA pair after starting up the pair as described in this document:

1. Initiate an SSH session with both the Primary and Secondary appliances to their respective interface eth0 IP address and elevate to root access.
2. Issue the following command on both appliances to determine the status of the heartbeat service:

```
service heartbeat status
```

The command should return a result such as the following on both the current Primary and Secondary members of an HA pair:

```
heartbeat OK [pid 20960 et al] is running on beaconha1 [beaconha1]...
```

3. Verify that both the Primary and Secondary have the required two slon processes running by issuing the following command:

```
ps aux | grep slon
```

This command should show a similar result on both members of an HA pair if the slon processes are running normally:

```
[root@BeaconHA1 ~]# ps aux | grep slon
root      4646  0.0  0.0  3880  676 pts/1    S+   12:43   0:00 grep slon
beacon    20686  0.0  0.0  67468  932 ?        Sl   07:47   0:00 /usr/bin/slon -d
0 -p /usr/beamon/working/slon.pid -s 1000 beacon_cluster dbname=beacon user=beacon
password=beacon
beacon    21089  0.0  0.0   4840   904 ?        S    Dec26   0:00 /usr/bin/slon -d
0 -p /usr/beamon/working/slon.pid -s 1000 beacon_cluster dbname=beacon user=beacon
password=beacon
[root@BeaconHA1 ~]#
```

## Transition to Web Management

At this juncture, the Cisco NAC Profiler HA pair is ready for configuration via the web-based user interface. Using a standard browser on another network-attached PC or laptop, enter the following URL to confirm that the UI being served by the Cisco NAC Profiler HA pair is accessible over the network:

```
https://[Virtual HA IP Address]/profiler
```

Enter 'admin' as the username and the password selected above for the web interface. The following web page should display in the browser:

**Figure 4-69** NAC Profiler Web UI Home Page



The session created for the initial configuration of the Cisco NAC Profiler Server is still logged in as the root user at the appliance console. Issue the command “logout” at the prompt to logout of the system and lock the console.

This completes the initial configuration of your Cisco NAC Profiler Server HA pair. Refer to [Configuring the Collector on the Clean Access Server, page 4-39](#) next, then continue to [Chapter 5, “Configuring Cisco NAC Profiler for the Target Environment”](#) for further configuration instructions of the Profiler system.

## Configuring the Collector on the Clean Access Server

The Cisco NAC Profiler Collector module co-resides on the Cisco NAC Appliance Clean Access Server and must be enabled on the Clean Access Server as described in this section.

See [CLI Commands for Cisco NAC Profiler, page 4-45](#) for additional details.

### Enable the Remote Collector Service on the CAS

Remote Collection service can be configured to connect back to the NAC Profiler for the system in one of two ways via the Connection Type: to actively connect to a Server maintaining the centralized NAC Profiler database (act as a Client), or alternatively to wait for the Server to initiate contact with the Remote Collector (act as a Server). This subtle difference is important to understand, and the option chosen is determined by the environment in which the Remote Collector service will be deployed.

Selecting the **Client** option will result in the Forwarder on the Remote Collection Service to initiate communications with the Server system module running on the NAC Profiler maintaining the endpoint database and providing system management. This is the most common configuration for Remote Collection appliances and simplifies the system configuration of the Server module.

In environments where a firewall is in place between the Remote Collector Service and the NAC Profiler maintaining the endpoint database and providing system management, the Remote Collector service will likely be unable to initiate a TCP communication through the firewall back to the Server. In this case, the Remote Collector service should be configured with the **Server** Connection Type option selected to ensure that the Forwarder module on the Remote Collection service waits for the NAC Profiler to initiate TCP communications through the firewall, opening the port and enabling firewall traversal. Use this option if necessary, remembering that the NAC Profiler for the system will have to have a Network Connection added to the configuration for each Remote Collection service configured as a Server. Connection Type is **Client**. See [Chapter 6, “Cisco NAC Profiler Server Configuration”](#) for instructions on adding Network Connection to the Profiler Server Module.

**Note**

Be sure to note the Connection Type chosen for each Remote Collection service so that the correct Server Side configuration can be completed when the Remote Collection service(s) are added to the system configuration as described in [Chapter 6, “Cisco NAC Profiler Server Configuration”](#).

## Connection Type is Client

- 
- Step 1** Connect to the Clean Access Server and access its command line by direct console, serial connection, or SSH.
- Step 2** Login as user **root** with the root password (default is **cisco123**)
- Step 3** At the command line, type **service collector config**.
- ```
[root@CAS_OOB /]# service collector config
```
- This starts the short configuration script for the Collector. Either type a value or press the Enter key to accept the default value (shown in brackets [ ]) for each of the following prompts.
- Step 4** Type **y** or press Enter to enable the Collector service on the CAS:
- ```
Enable the NAC Collector (y/n) [y]: y
```
- Step 5** Type **y** or press Enter to enter configure network settings for the Collector so that it can connect to the Cisco NAC Profiler Server:
- ```
Configure NAC Collector (y/n) [y]: y
```
- Enter the name for this remote collector. Please note that if this collector exists on a HA pair that this name must match its pair's name for proper operation. (24 char max) [GBS-CAS]:
- Step 6** Type this Remote Collector's name and press Enter.
- ```
Network configuration to connect to a NAC Profiler Server
```
- Step 7** Press Enter to configure the Collector as a client (default) or type **server** to configure it otherwise (not common):
- ```
Connection type (server/client) [client]:
```
- Step 8** Type the IP address of the Cisco NAC Profiler Server that the Collector will communicate with:
- ```
Connect to IP [127.0.0.1]: 10.30.30.5
```
- Step 9** Press Enter to accept the default port number (31416), or type another port number for communication with the Cisco NAC Profiler Server:
- ```
Port number [31416]:
```
- Step 10** Type **none** if no encryption is desired, or select **AES** (default) or type **blowfish** to configure encryption:

- Encryption type (AES, blowfish, none) [AES]: none
- Step 11** Type the shared secret for the Profiler Server. See [Shared Secret, page 6-10](#) for additional details.
- ```
Shared secret []: cisco123
```
- Step 12** The NAC Collector configuration utility will next show status for each of the modules (Forwarder, NetMap, NetTrap, NetWatch, NetInquiry, NetRelay) in the Collector followed by a final confirmation:
- ```
-- Configured CAS_OOB-fw
-- Configured CAS_OOB-nm
-- Configured CAS_OOB-nt
-- Configured CAS_OOB-nw
-- Configured CAS_OOB-ni
-- Configured CAS_OOB-nr

NAC Collector has been configured
[root@CAS_OOB /]#
```
- Step 13** Collector configuration on the Clean Access Server for a connection type of Client is complete.
- 

Refer to [Chapter 7, “Configuring Collector Modules”](#) for details on how to further configure Collector modules through the Cisco NAC Profiler Server web interface.

## Connection Type is Server

- Step 1** Connect to the Clean Access Server and access its command line by direct console, serial connection, or SSH.
- Step 2** Login as user `root` with the root password (default is `cisco123`)
- Step 3** At the command line, type `service collector config`.
- ```
[root@CAS_OOB /]# service collector config
```
- This starts the short configuration script for the Collector. Either type a value or press the Enter key to accept the default value (shown in brackets [ ]) for each of the following prompts.
- Step 4** Type `y` or press Enter to enable the Collector service on the CAS:
- ```
Enable the NAC Collector (y/n) [y]: y
```
- Step 5** Type `y` or press Enter to enter configure network settings for the Collector so that it can connect to the Cisco NAC Profiler Server:
- ```
Configure NAC Collector (y/n) [y]: y
```
- Step 6** Type this Remote Collector’s name and press Enter.
- ```
Enter the name for this remote collector. Please note that if
this collector exists on a HA pair that this name must match
its pair's name for proper operation. (24 char max) [GBS-CAS]:
```
- Step 7** Press Enter to configure the Collector as a client (default) or type `server` to configure it otherwise (not common):
- ```
Network configuration to connect to a NAC Profiler Server
Connection type (server/client) [server]:
```
- Step 8** Type the IP address of this Remote Collector Service
- ```
Listen on IP [10.40.1.10]:
```
- Step 9** Type the IP address of the Cisco NAC Profiler Server that the Collector will communicate with:
- ```
You will be asked to enter the IP address(es) of the NPS. This
is necessary to configure the access control list used by this
collector. If the NPS is part of an HA pair then you must include
the real IP address of each independant NPS and the virtual IP to
ensure proper connectivity in the case of failover.
```

```
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [127.0.0.1]:
```

- Step 10** Press Enter to accept the default port number (31416), or type another port number for communication with the Cisco NAC Profiler Server:

```
Port number [31416]:
```

- Step 11** Type **none** if no encryption is desired, or select **AES** (default) or type **blowfish** to configure encryption:

```
Encryption type (AES, blowfish, none) [AES]: none
```

- Step 12** Type the shared secret for the Profiler Server. See [Shared Secret, page 6-10](#) for additional details.

```
Shared secret []: cisco123
```

- Step 13** The NAC Collector configuration utility will next show status for each of the modules (Forwarder, NetMap, NetTrap, NetWatch, NetInquiry, NetRelay) in the Collector followed by a final confirmation:

```
-- Configured CAS_OOB-fw
-- Configured CAS_OOB-nm
-- Configured CAS_OOB-nt
-- Configured CAS_OOB-nw
-- Configured CAS_OOB-ni
-- Configured CAS_OOB-nr
```

```
NAC Collector has been configured
[root@CAS_OOB /]#
```

- Step 14** Collector configuration on the Clean Access Server is complete.

## Collector Configuration on HA-CAS Pairs for Cisco NAC Profiler

Cisco NAC Profiler (release 2.1.8 and later) includes changes to the procedure for the configuration of CAS/Collector HA pairs deployed with standalone and HA Profiler Server pairs. Use the following procedure when deploying CAS/Collector HA pairs in a Cisco NAC Profiler system:

- 
- Step 1** Configure CASs for HA mode operation and verify that the HA protocol is operational. This step is critical to complete first to ensure that the HA protocol between the CASs is operating normally and the VIP is available for the Collector service configuration on both appliances in the CAS pair.
- Step 2** Determine a name for the Collector service to run on the CAS pair. The name must be no greater than 24 characters, and must be identical on both members of the CAS Pairs. A name that associates the Collector service on both members the CAS pair is recommended such as “Building-26-CAS” for example. This name will be used in the Profiler Server configuration to identify the Collector service on the HA CAS Pair so that it can be managed via the GUI as a single Collector.

### Configure Collector Service on Primary CAS

- Step 3** Login as user **root** with the root password (default is **cisco123**)

- Step 4** At the command line, type **service collector config**.

```
[root@CAS_OOB /]# service collector config
```

This starts the short configuration script for the Collector. Either type a value or press the Enter key to accept the default value (shown in brackets [ ]) for each of the following prompts.

- Step 5** Type **y** or press Enter to enable the Collector service on the CAS:

```
Enable the NAC Collector (y/n) [y]: y
```

- Step 6** Type `y` or press `Enter` to enter configure network settings for the Collector so that it can connect to the Cisco NAC Profiler Server:

```
Configure NAC Collector (y/n) [y]: y
```

- Step 7** Type this Remote Collector's name and press `Enter`.

```
Enter the name for this remote collector. Please note that if
this collector exists on a HA pair that this name must match
its pair's name for proper operation. (24 char max) [GBS-CAS]:
```



**Note**

An identical name for the Collector service must be used in the configuration on both CASs in the HA pair. Normally, the hostname of the CAS appliance is chosen by default when configuring a Collector. In release 2.1.8 and later, there is an option to specify a name for the Collector when using the 'service collector config' command. When configuring CAS/Collector HA pairs, a name for the Collector service must be chosen and used on both appliances in the pair identically (e.g., case sensitive, spaces, etc.).

- Step 8** The Connection type for the Collector configuration **must be set to 'Server'**. For CAS/Collector HA Pairs, the Profiler Server will have to initiate the connection to the Collector service running on the pair. This is accomplished by selecting the Server connection type for the CAS/Collector.

```
Network configuration to connect to a NAC Profiler Server
Connection type (server/client) [client]:server
```

- Step 9** Listen on IP - the Collector should be configured to listen on the **VIP/Service IP** address assigned to the CAS HA pair during CAS HA configuration.

```
Listen on IP [10.40.1.10]:
```

- Step 10** The eth0 interface IP addresses of both members of the Profiler Server HA pair need to be entered in this step along with the VIP/Service IP of the HA Profiler Server pair. Enter the IP address of the eth0 interface of the first Profiler Server appliance, press `enter`; enter the IP address of the eth0 interface of the other Profiler Server appliance in the HA pair, press `enter`, enter the VIP/Service IP address of the HA Profiler Server pair, then enter 'done' to progress the script to the next step.

```
You will be asked to enter the IP address(es) of the NPS. This
is necessary to configure the access control list used by this
collector. If the NPS is part of an HA pair then you must include
the real IP address of each independant NPS and the virtual IP to
ensure proper connectivity in the case of failover.
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [127.0.0.1]: 10.10.0.211
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [10.10.0.211]: 10.10.0.212
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [10.10.0.210]: 10.10.0.210
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [10.10.0.212]: done
```

- Step 11** Press `Enter` to accept the default port number (31416), or type another port number for communication with the Cisco NAC Profiler Server:

```
Port number [31416]:
```

- Step 12** Type **none** if no encryption is desired, or select **AES** (default) or type **blowfish** to configure encryption:

```
Encryption type (AES, blowfish, none) [AES]: none
```

- Step 13** Type the shared secret for the Profiler Server. See [Shared Secret, page 6-10](#) for additional details.

```
Shared secret []: cisco123
```

- Step 14** The NAC Collector configuration utility will next show status for each of the modules (Forwarder, NetMap, NetTrap, NetWatch, NetInquiry, NetRelay) in the Collector followed by a final confirmation:

```
-- Configured CAS_OOB-fw
-- Configured CAS_OOB-nm
-- Configured CAS_OOB-nt
```

```
-- Configured CAS_OOB-nw
-- Configured CAS_OOB-ni
-- Configured CAS_OOB-nr

      NAC Collector has been configured
[root@CAS_OOB /]#
```

## Configure Collector Service on Secondary CAS

**Step 15** Login as user **root** with the root password (default is **cisco123**)

**Step 16** At the command line, type **service collector config**.

```
[root@CAS_OOB /]# service collector config
```

This starts the short configuration script for the Collector. Either type a value or press the Enter key to accept the default value (shown in brackets [ ]) for each of the following prompts.

**Step 17** Type **y** or press Enter to enable the Collector service on the CAS:

```
      Enable the NAC Collector (y/n) [y]: y
```

**Step 18** Type **y** or press Enter to enter configure network settings for the Collector so that it can connect to the Cisco NAC Profiler Server:

```
Configure NAC Collector (y/n) [y]: y
```

**Step 19** Type this Remote Collector's name and press Enter.

```
Enter the name for this remote collector. Please note that if
this collector exists on a HA pair that this name must match
its pair's name for proper operation. (24 char max) [GBS-CAS]:
```



### Note

An identical name for the Collector service must be used in the configuration on both CASs in the HA pair. Normally, the hostname of the CAS appliance is chosen by default when configuring a Collector. In release 2.1.8 and later, there is an option to specify a name for the Collector when using the 'service collector config' command. When configuring CAS/Collector HA pairs, a name for the Collector service must be chosen and used on both appliances in the pair identically (e.g., case sensitive, spaces, etc.).

**Step 20** The Connection type for the Collector configuration **must be set to 'Server'**. For CAS/Collector HA Pairs, the Profiler Server will have to initiate the connection to the Collector service running on the pair. This is accomplished by selecting the Server connection type for the CAS/Collector.

```
Network configuration to connect to a NAC Profiler Server
      Connection type (server/client) [client]:server
```

**Step 21** Listen on IP - the Collector should be configured to listen on the VIP/Service IP address assigned to the CAS HA pair during CAS HA configuration.

```
Listen on IP [10.40.1.10]:
```

**Step 22** The eth0 interface IP addresses of both members of the Profiler Server HA pair need to be entered in this step along with the VIP/Service IP of the HA Profiler Server pair. Enter the IP address of the eth0 interface of the first Profiler Server appliance, press enter; enter the IP address of the eth0 interface of the other Profiler Server appliance in the HA pair, press enter, enter the VIP/Service IP address of the HA Profiler Server pair, then enter 'done' to progress the script to the next step.

```
You will be asked to enter the IP address(es) of the NPS. This
is necessary to configure the access control list used by this
collector. If the NPS is part of an HA pair then you must include
the real IP address of each independant NPS and the virtual IP to
ensure proper connectivity in the case of failover.
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [127.0.0.1]: 10.10.0.211
Enter the IP address(es) of the NAC Profiler.
```

```
(Finish by typing 'done') [10.10.0.211]: 10.10.0.212
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [10.10.0.210]: 10.10.0.210
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [10.10.0.212]: done
```

**Step 23** Press Enter to accept the default port number (31416), or type another port number for communication with the Cisco NAC Profiler Server:

```
Port number [31416]:
```

**Step 24** Type **none** if no encryption is desired, or select **AES** (default) or type **blowfish** to configure encryption:

```
Encryption type (AES, blowfish, none) [AES]: none
```

**Step 25** Type the shared secret for the Profiler Server. See [Shared Secret, page 6-10](#) for additional details.

```
Shared secret []: cisco123
```

**Step 26** The NAC Collector configuration utility will next show status for each of the modules (Forwarder, NetMap, NetTrap, NetWatch, NetInquiry, NetRelay) in the Collector followed by a final confirmation:

```
-- Configured CAS_OOB-fw
-- Configured CAS_OOB-nm
-- Configured CAS_OOB-nt
-- Configured CAS_OOB-nw
-- Configured CAS_OOB-ni
-- Configured CAS_OOB-nr
```

```
NAC Collector has been configured
```

```
[root@CAS_OOB /]#
```

**Step 27** This completes the Configuration of Collectors on HA CAS pairs for NAC Profiler

See [Chapter 6, “Cisco NAC Profiler Server Configuration”](#) for instructions on adding Network Connection to the Profiler Server Module.

## CLI Commands for Cisco NAC Profiler

[Table 4-7](#) lists CLI commands issued on the CAS for the Cisco NAC Profiler Collector service. Refer to the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide](#) for complete details on the CAS CLI.



### Note

To display the version of the Collector on the CAS, SSH to the CAS machine running the Collector service and type **rpm -q Collector**.

**Table 4-7** Cisco NAC Profiler Collector CLI Commands for CAS

Command	Description
<b>service collector start</b>	Starts the Collector service on the CAS.
<b>service collector stop</b>	Shuts down the Collector service on the CAS.

Table 4-7 Cisco NAC Profiler Collector CLI Commands for CAS

Command	Description
<code>service collector verify</code>	<p>Displays the configured Collector Services running on the CAS</p> <pre>Collector Network Configuration Collector Name      = bcas1-fw Connection Type    = server Listen on IP       = 10.40.1.10 Network IP ACL 127.0.0.1 10.10.0.211 10.10.0.210 10.10.0.212 Port Number        = 31416 Encryption type    = AES Shared secret      = profiler</pre>
<code>service collector status</code>	<p>Displays the running status of the individual Collector modules on the CAS, for example:</p> <pre>Profiler Status o Server           Not Installed o Forwarder        Running o NetMap           Running o NetTrap          Running o NetWatch         Running o NetInquiry       Running o NetRelay         Running</pre>
<code>service collector restart</code>	<p>Stops and then restarts the Collector service on the CAS. This is used when the service is already running and you want to restart it.</p>
<code>service collector config</code>	<p>Starts the configuration of the Collector component so that it can communicate with the Cisco NAC Profiler Server. For example a client connection:</p> <pre>[root@caserver12 /]# service collector config Enable the NAC Collector (y/n) [y]: Configure NAC Collector (y/n) [y]: Enter the name for this remote collector. Please note that if this collector exists on a HA pair that this name must match its pair's name for proper operation. (24 char max) [GBS-CAS]: Network configuration to connect to a NAC Profiler Server   Connection type (server/client) [client]: client   Connect to IP [127.0.0.1]: 192.168.96.20   Port number [31416]:   Encryption type (AES, blowfish, none) [AES]: none   Shared secret []: cisco123 -- Configured caserver12-fw -- Configured caserver12-nm -- Configured caserver12-nt -- Configured caserver12-nw -- Configured caserver12-ni -- Configured caserver12-nr  NAC Collector has been configured</pre>