NAC Profiler and NAC SERVER Collectors in a Layer 3 Out−of−Band Configuration Guide

Document ID: 108318

Contents

Introduction

This document describes how to implement NAC Profiler and NAC SERVER Collectors in a Layer 3 Out−of−Band deployment. If you deploy the NAC Server in High−availability (HA), then only one Collector is active and the other is on standby. If you do not do HA, you can add each Collector in the Profiler separately and have both NAC Servers run as Collectors. This guide reflects on the HA Server deployment.

Prerequisites

Requirements

The requirements of this guide are that you have configured your NAC Manager, NAC Server, NAC Profiler, and Network infrastructure according to the installation and configuration guides for each product.

Components Used

The information in this document is based on these software and hardware versions:

- NAC Manager
- NAC Server
- NAC Profiler
- 3750 Distribution Switch
- 3750 Remote Site Access Switch

- 2800 Remote Site Router
- 3800 Distribution Router

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

NAC Profiler Overview

Cisco NAC Profiler enables network administrators to efficiently deploy and manage Network Admission Control (NAC) in enterprise networks of varying scale and complexity with the identification, location and determination of the capabilities of all attached network endpoints, regardless of device type, in order to ensure and maintain appropriate network access. Cisco NAC Profiler is an agentless system that discovers, catalogs, and profiles all endpoints connected to a network.

NAC Overview

The Cisco Network Admission Control (NAC) Appliance, which is also known as Cisco Clean Access, is a powerful, easy−to−use admission control and compliance enforcement solution. With comprehensive security features, in−band or out−of−band deployment options, user authentication tools, and bandwidth and traffic filtering controls, Cisco NAC Appliance is a complete solution to control and secure networks. As the central access management point for your network, Cisco NAC Appliance lets you implement security, access, and compliance policies in one place instead of the need to propagate the policies throughout the network on many devices.

Deployment Guide Overview

In Figure 1, there is a simple remote site deployment with central HA NAC Servers that acts as the enforcement point for Layer 3 Out−of−Band devices. The NAC Profiler and NAC Manager sit on the same management network and send and receive information from the Servers and Collectors. There is also a stand−alone Collector that grabs essential DHCP information about the devices through SPAN in the data center or core layer. There are several ways to discover remote endpoints and this guide can help you in your deployment. It is not intended to be a mandatory guide but shows you how each module on the collectors can be used and how endpoint data is seen by the Profiler to make the Profiling decisions for you.

A list of the mandatory and optional tools that the NAC Server Collectors use is provided.

Mandatory Collector Modules

NetTrap This module listens for SNMP traps sent by switches for new−mac notification or Link Up/Down notifications. This module sends all new MAC addresses to Profiler for profiling. This feature is defined per switch on the SNMP−Server configuration command line on Cisco IOS®.

NetMap This module sits on the Collector and is responsible for doing SNMP polling of devices in the remote branch at timed intervals. In the diagram of Figure 1, the CAS1a Collector SNMP polls the remote switch and router for specific MIB information with read access to the switch. This polling provides things like mac−address to port information, interfaces, link status, dot1x information, system information and so forth.

NetWatch (SPAN) NetWatch module can listen on a SPAN port of a switch and send the ingested traffic information back to the Profiler. A NAC Server requires an additional interface on each NAC SERVER to collect data. This is essential because Profiler is based primarily on DHCP information passed by devices and some other application traffic matching.

Optional Collector Modules

You can use SPAN or Netflow. It is up to the deployment and customer requirements but one is only recommended on a NAC Server due to the amount of traffic that is sent to the Collector Modules and the other NAC functionalities that the NAC Server has to perform. You also lose more vital informational pieces about devices with Netflow like DHCP vendor information, URL destinations, Web client info, Web server info and so forth.

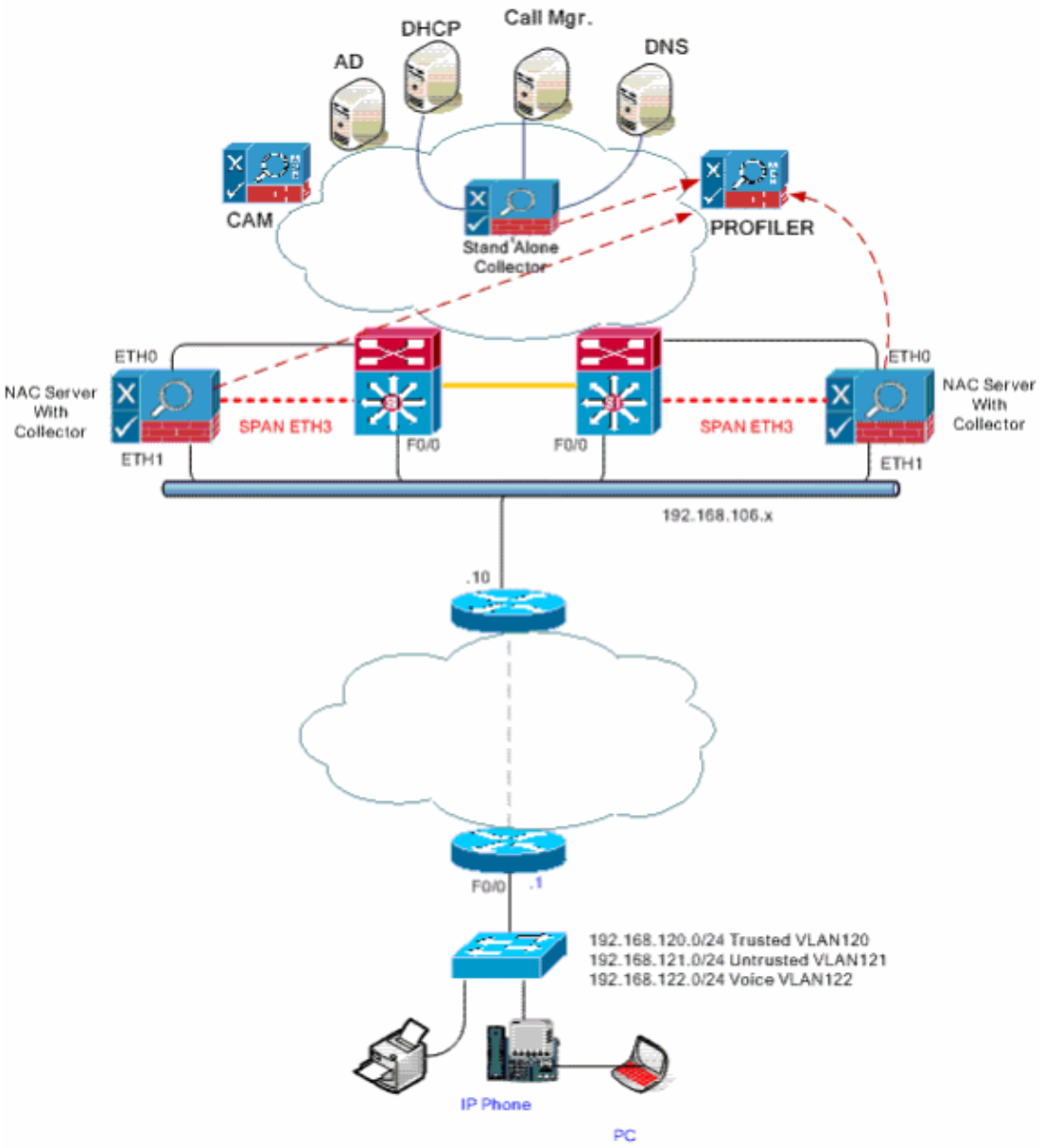
NetRelay (Netflow) is configured on each router on a per interface basis and the destination is the management IP address of the NAC SERVER. A Netflow agent sits on the NAC SERVER and parses the Netflow information based on your traffic rules and networks configured on the Profiler.

NetInquiry This is a passive and active mechanism based on your things like TCP Open ports. For example the NAC SERVER does a SYN/ACK and then drops the connection in order to poll a particular subnet range or ranges for open TCP ports. If there is a response, it sends the information to the Profiler with the IP address and TCP port polled.

Note: For NetInquiry, only add specific subnets or hosts that can not be reached or seen with Netflow or NetWatch. NetInquiry can overload your NAC Server with extra processing and hardware resources like memory and CPU utilization if not configured properly. Use this feature as a last resort.

Note: If you have a stand−alone Collector you can enable both Netflow and SPAN on the same device but make sure not to oversubscribe the Collector.

Figure 1



Configuration

Configure the NAC Profiler in the Layer 3 OOB Topology

- NAC Servers need to be configured through the normal NAC HA setup.
- NAC Collector utilizes the Virtual IP address of the NAC server to communicate with the Profiler.
- NAC Collector HA pair is added as a single entry in the Profiler and communicates to the virtual IP address of the CAS.

Figure 2

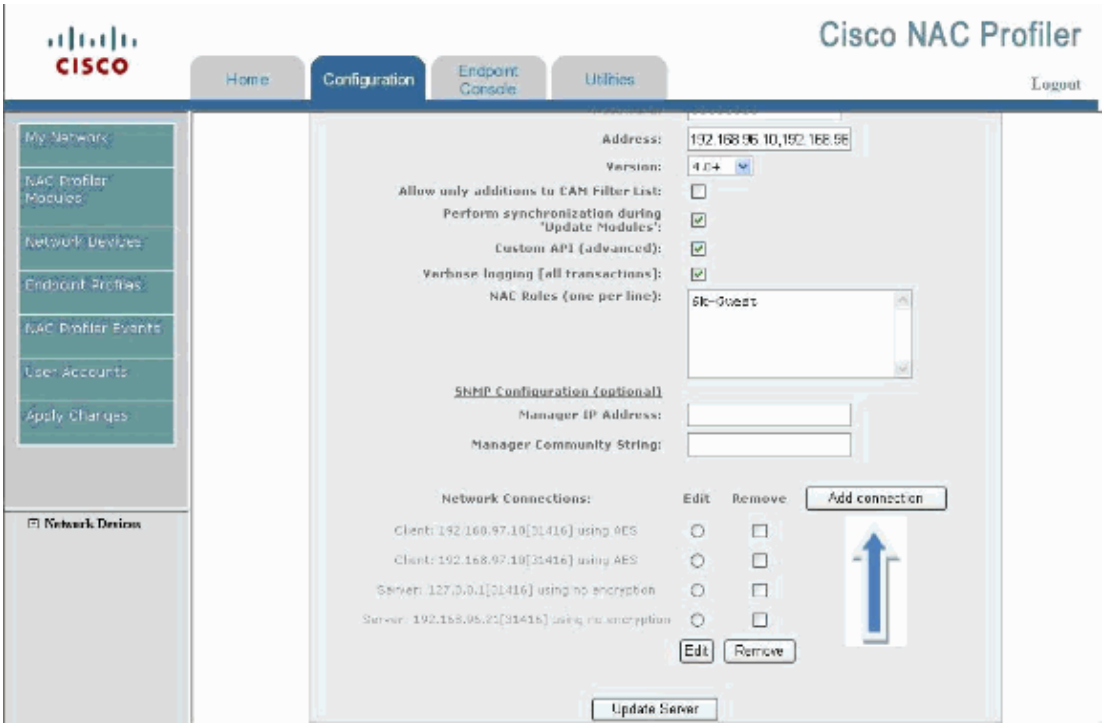
Configuration Setup

Complete these steps:

1. Profiler needs a *Client* connection for the new NAC Collectors.
2. Profiler needs a *Server* connection for the stand−alone device that sits close to the distribution|data center|services layer in the network diagram.
3. Choose **Configuration > NAC Profiler Modules List NAC Profiler Modules** and then click the **Server** tab.

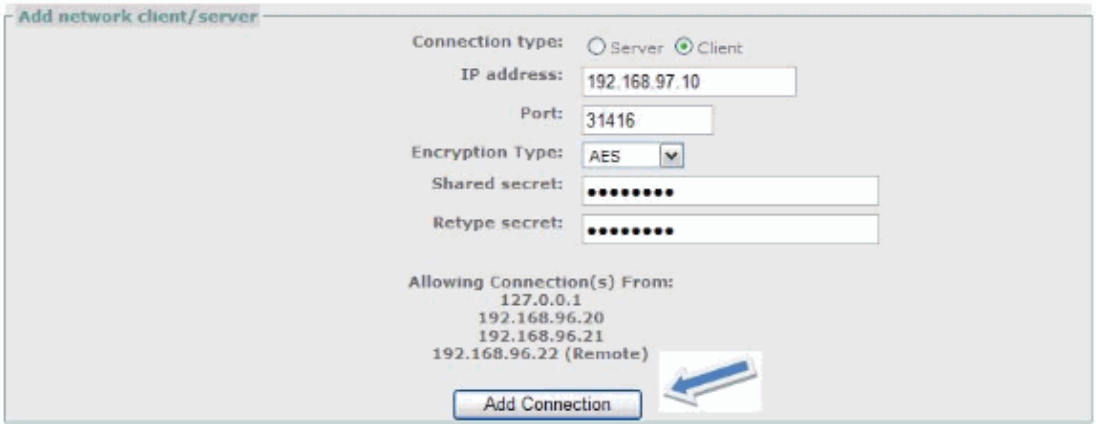
   Scroll to the bottom of the page and click **Add Connection**.

   Figure 3



4. Enter the service IP address and secret key information of the HA Collector and click **Add Connection**.

Figure 4



5. Click **Add connection** again.

Figure 5

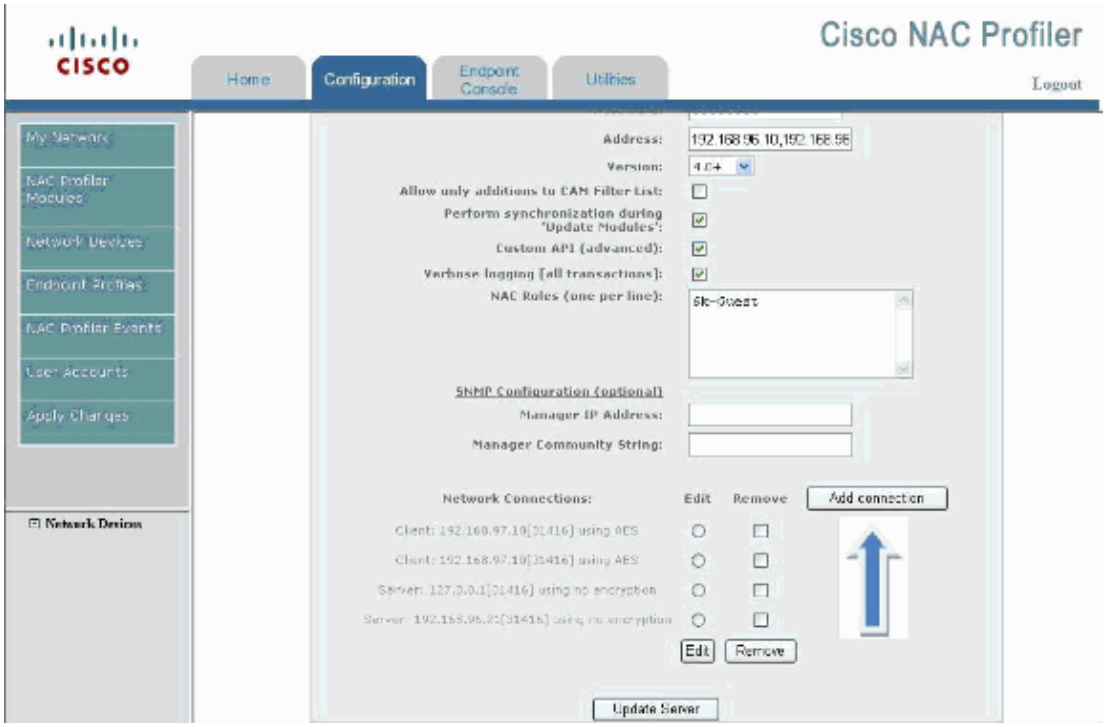
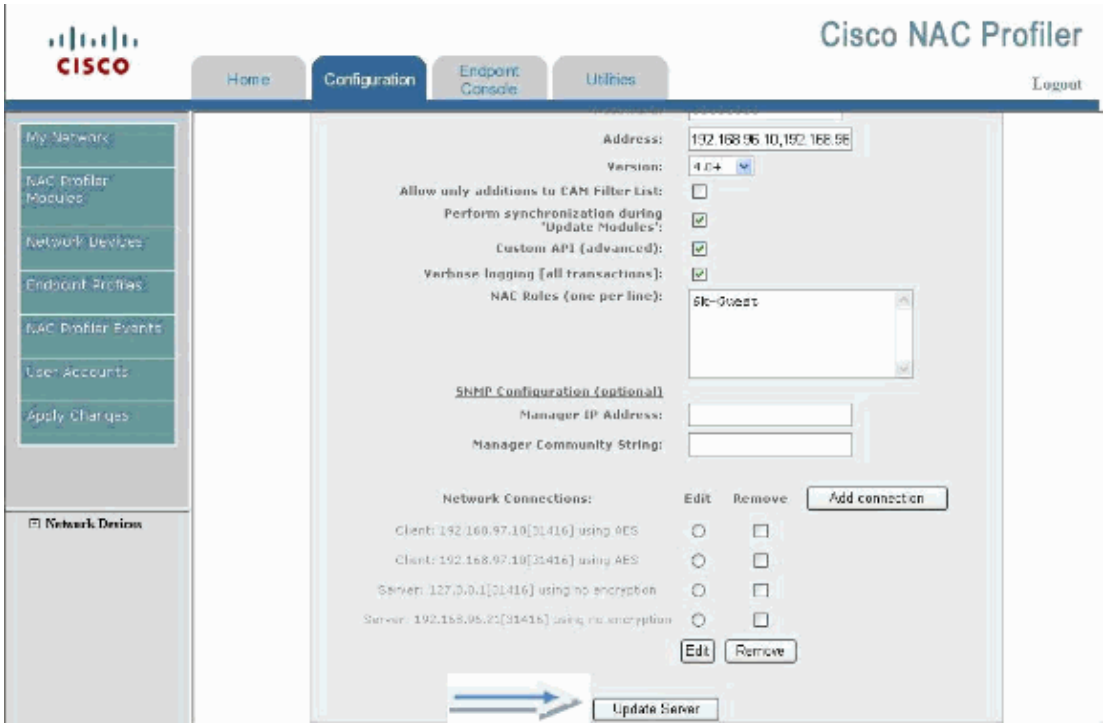


Figure 6

6. Enter the **IP address** in order to configure a *Server* Connection to which the Standalone Collector connects.
7. Click **Edit Connection** when you are done in order to get back to the Server configuration page.
8. Click **Update Server** on the Server configuration page.

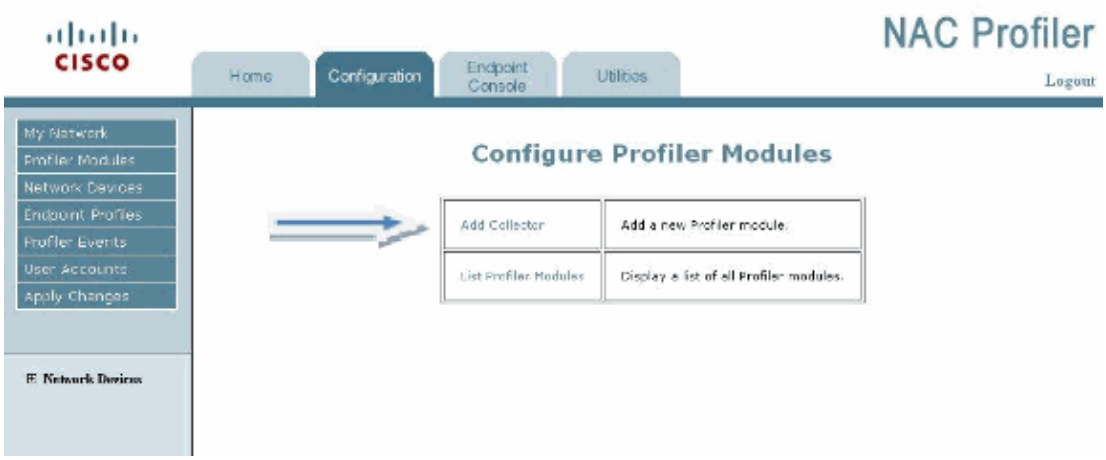
Figure 7



Add two new Collectors to the Profiler. Complete these steps:

1. Choose **Configuration > NAC Profiler Modules > Add Collector**.

   Figure 8



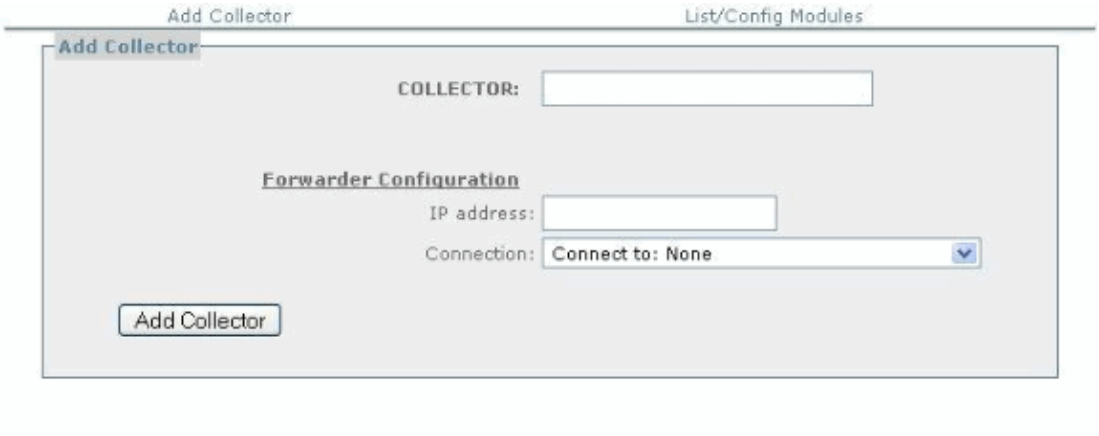
2. Add a new Collector name for the NAC Server HA Pair. This can be anything you want but must match on the Collector Configuration.

   Collector name CAS−OOB−Pair1

   IP address¡92.168.97.10 (Virtual address of the NAC Server)

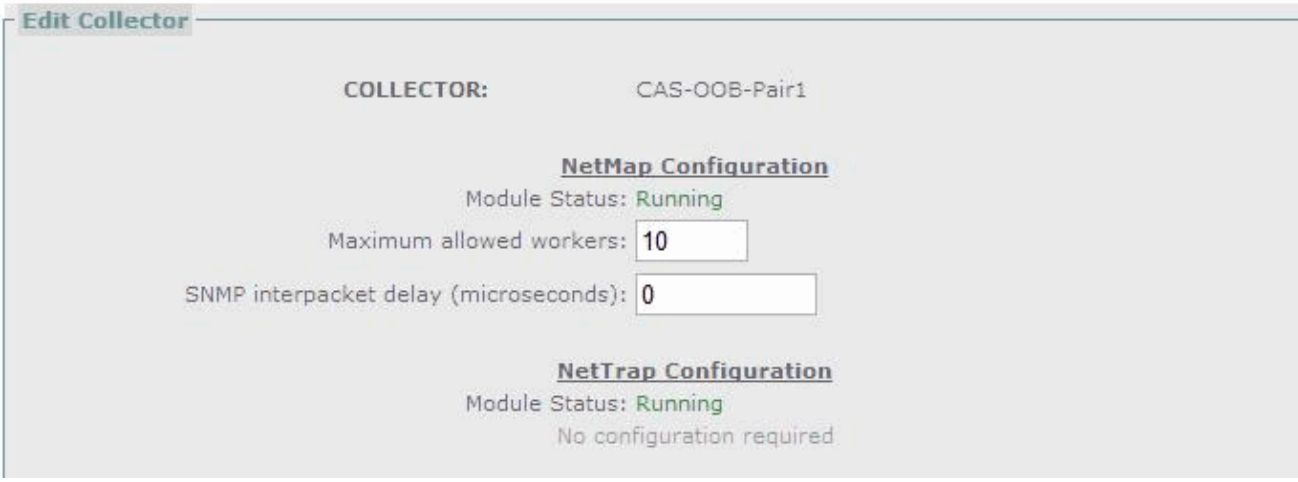
   Connection Leave it as **NONE** for now. You can change this at a later time to a Server connection that is in listen mode.
3. Click **Add Collector Button**.

   Figure 9



4. Configure your Collector Service Modules. Leave NetMap and NetTrap alone.

Figure 10

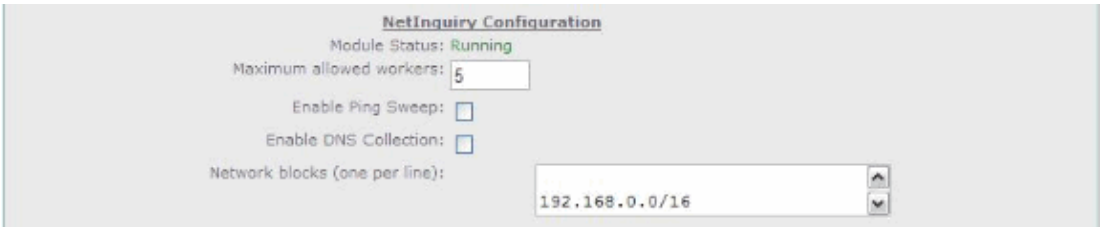


5. Add a NetWatch interface (eth3), which is connected to a SPAN port on the distribution switch.

Figure 11

6. Add a subnet Block for the NetInquiry module in order to listen for interesting traffic that comes from the access networks. Be specific on the networks as to not tax the NAC server unnecessarily. In this lab setup, it can be the whole 192.168.0.0 private space.

Figure 12

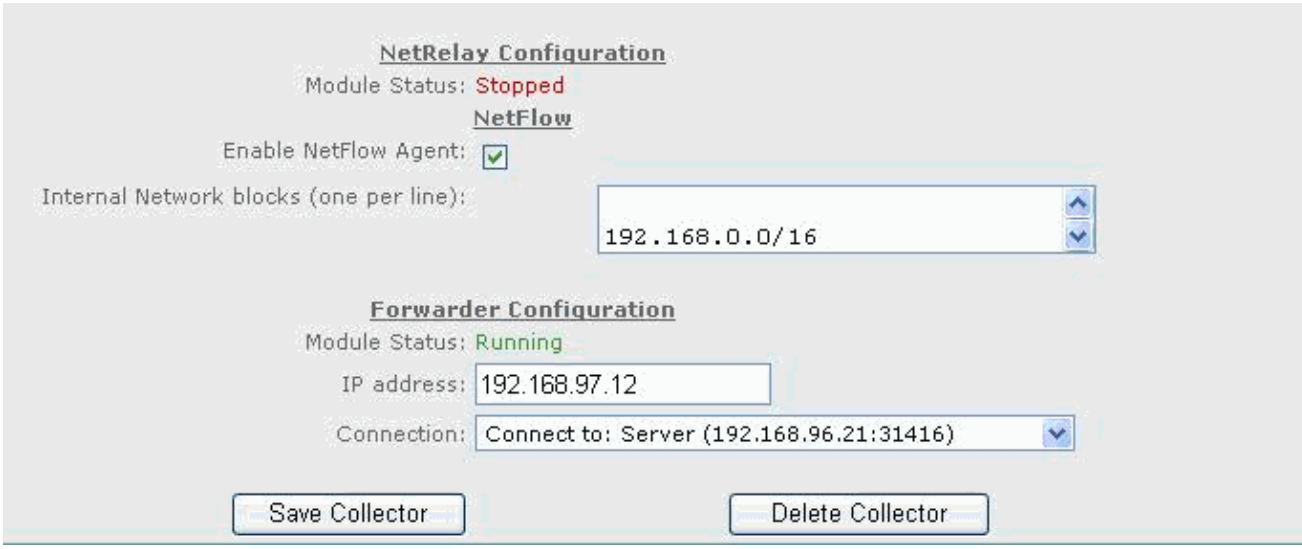


Note: Leave Ping Sweep and DNS collection disabled. Use this as a last resort. Ping sweep and DNS Collection triggers pings and nslookups on the range of IP subnets you put in the Network Blocks section. This is not recommended and rarely used.

7. Configure the Forwarder to listen on IP address 192.168.97.10 (VIP) and TCP port 31416. This allows the Collector to act as a server and listen for a connection from Profiler to the specific TCP port. This reflects on first few steps for the Server configuration.
8. Enable Netflow for the Collector Pair. (Optional)

   You can do this here since Netflow is passed from the remote router due to no remote collector.
9. Enter the IP address blocks for the remote site as depicted. In this example, the whole 192.168.0.0 private space is used.

Figure 13



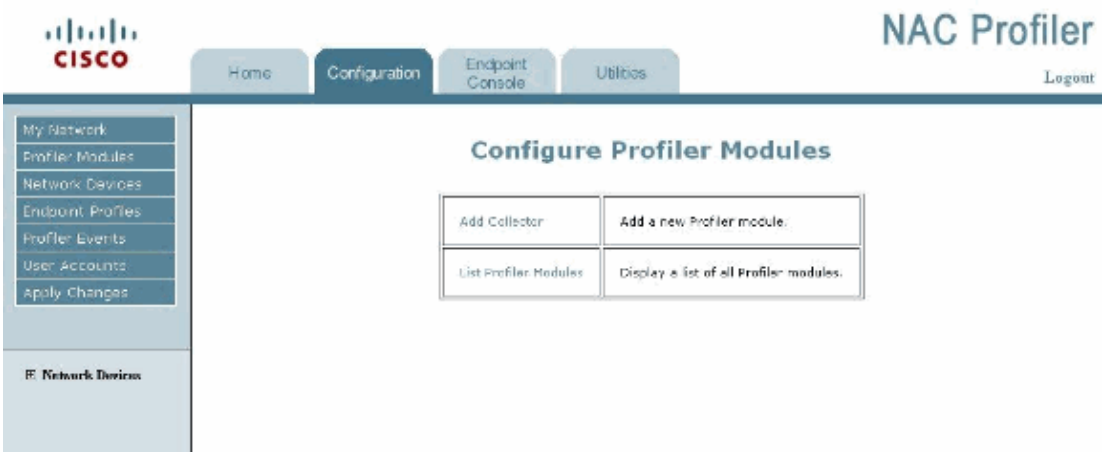
10. Click **Save Collector** in order to save your configuration.

Add the Additional Stand−alone Collector to Profiler

Complete these steps:

1. Click **Add Collector**.

Figure 14



2. Collector name can be anything you want. In this example, it is CAS2.
3. The Forwarder IP address is itself. The IP address of eth0 is for management.

In this example, it is 192.168.97.12.

The Connection should be the IP address of the Profiler. In this case, it is 192.168.96.21.

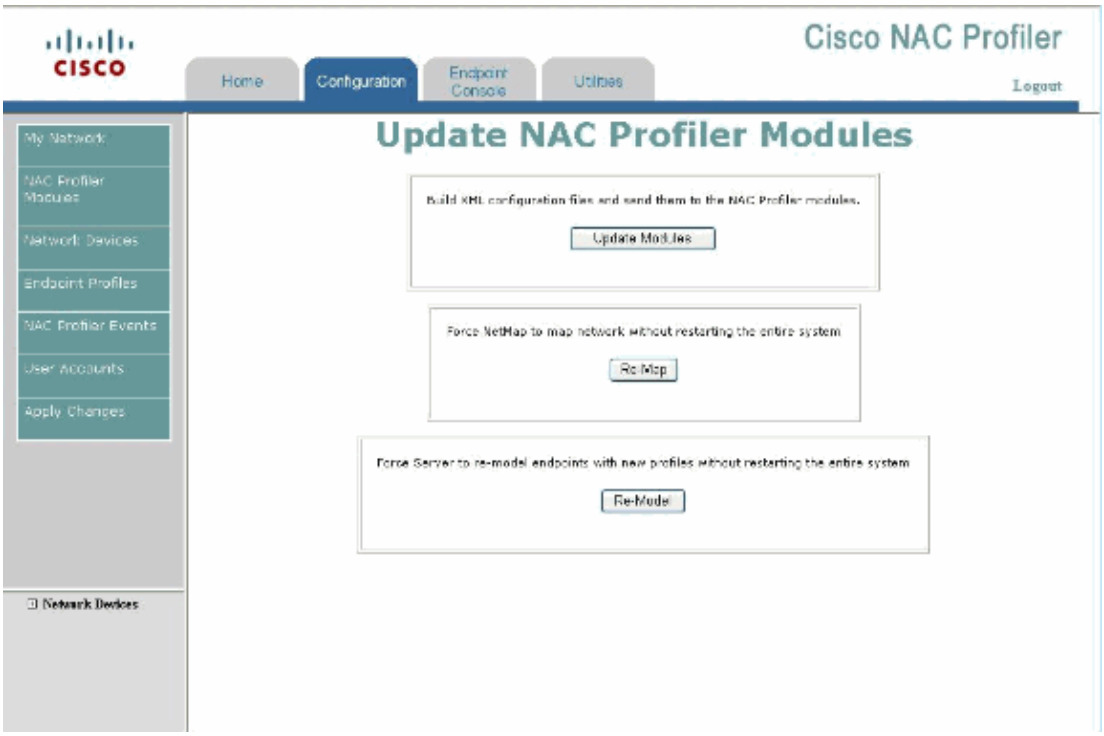
4. Click **Add Collector**.

Figure 15

5. After this, you are brought to the Collector configuration page. Complete steps 5 9 in the previous section. This allows you to modify and add the unique IP addresses and configuration settings of the standalone Collector.
6. One unique setting for the Stand−Alone Collector is the ability to add multiple interfaces to the NetWatch configuration. Here you can add several interfaces so you can see traffic for DHCP, DNS, and IP Telephony from the remote endpoints.
7. Configure the NetWatch interfaces for your setup. In this example, three interfaces were added to SPAN traffic on the stand−alone Collector.

Figure 16

8. **Note:** Choose the **Configuration > Apply Changes > Update Modules** in order to save your settings.



Configure the NAC Collector Modules on the NAC Server

Note: This configuration needs to be run on all of the Collectors.

This configuration allows the Profiler and Collectors to communicate and establish secure connections for information about devices to start flowing. Complete these steps:

1. SSH or console to the Collector and login as **root** from the console or **beacon** from the SSH session.
2. Enter the **service collector config** command.
3. Run through the configuration script in order to setup the NAC Collector portion.

HA Collector Example

The Collector is setup as a *Server* connection type :

```
[root@cas1 ~]#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) [cas1]: CAS-OOB-Pair1
Network configuration to connect to a NAC Profiler Server
Connection type (server/client) [server]:
Listen on IP [192.168.97.10]:
```

You are 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 independent 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]: 192.168.96.20  (Real IP address of  NAC Serve
Enter the IP address(es) of the NAC Profiler.
(Finish by typing  done ) [192.168.96.20]: 192.168.96.21 (Virtual IP of NAC Server)
Enter the IP address(es) of the NAC Profiler.
```

```
(Finish by typing  done ) [done]: 192.168.96.22 (Real IP of NAC Server2)
Enter the IP address(es) of the NAC Profiler.
(Finish by typing  done ) [done]: done
Port number [31416]:
Encryption type (AES, blowfish, none) [none]: AES
Shared secret []: cisco123
"       Configured CAS-OOB-Pair1-fw
"       Configured CAS-OOB-Pair1-nm
"       Configured CAS-OOB-Pair1-nt
"       Configured CAS-OOB-Pair1-nw
"       Configured CAS-OOB-Pair1-ni
"       Configured CAS-OOB-Pair1-nr

NAC Collector has been configured.
```

4. Start the Collector Services.

```
[root@cas1 ~]#service collector start
```

Stand Alone Collector example

```
[root@cas2 ~]#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) [cas2]:
Network configuration to connect to a NAC Profiler Server
  Connection type (server/client) [client]:
  Connect to IP [192.168.96.21]:
  Port number [31416]:
  Encryption type (AES, blowfish, none) [none]:
  Shared secret []:
-- Configured cas2-fw
-- Configured cas2-nm
-- Configured cas2-nt
-- Configured cas2-nw
-- Configured cas2-ni
-- Configured cas2-nr


        NAC Collector has been configured.

[root@cas2 ~]#service collector start
```

Configure the Remote Access Switch to send SNMP Traps to the NAC Collector

This configuration allows Profiler to dynamically receive all new devices connecting to a switchport through the mac−notification traps. This is especially important since in the topology there is an IP Phone and PC connected to the same port.

Console or telnet into the switch (nac−3750−access#).

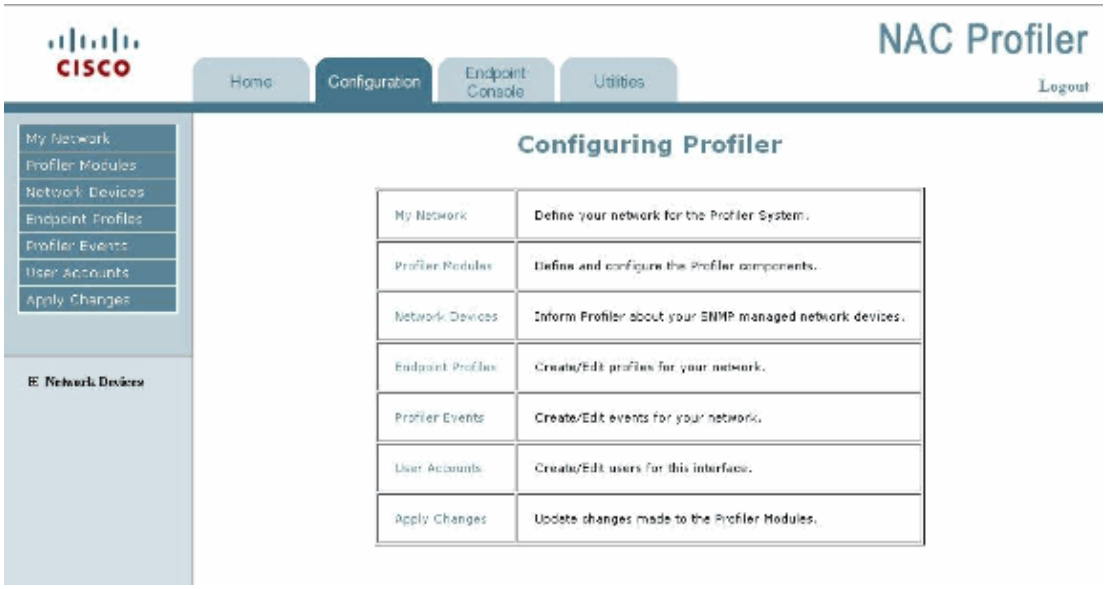
```
snmp-server community cleanaccess RW
snmp-server community profiler RO
snmp-server enable traps mac-notification
snmp-server host 192.168.96.10 version 2c cleanaccess
snmp-server host 192.168.97.10 version 1 profiler
```

Configure the Remote Access Switch on the Profiler for SNMP Information Gathering

Complete these steps:

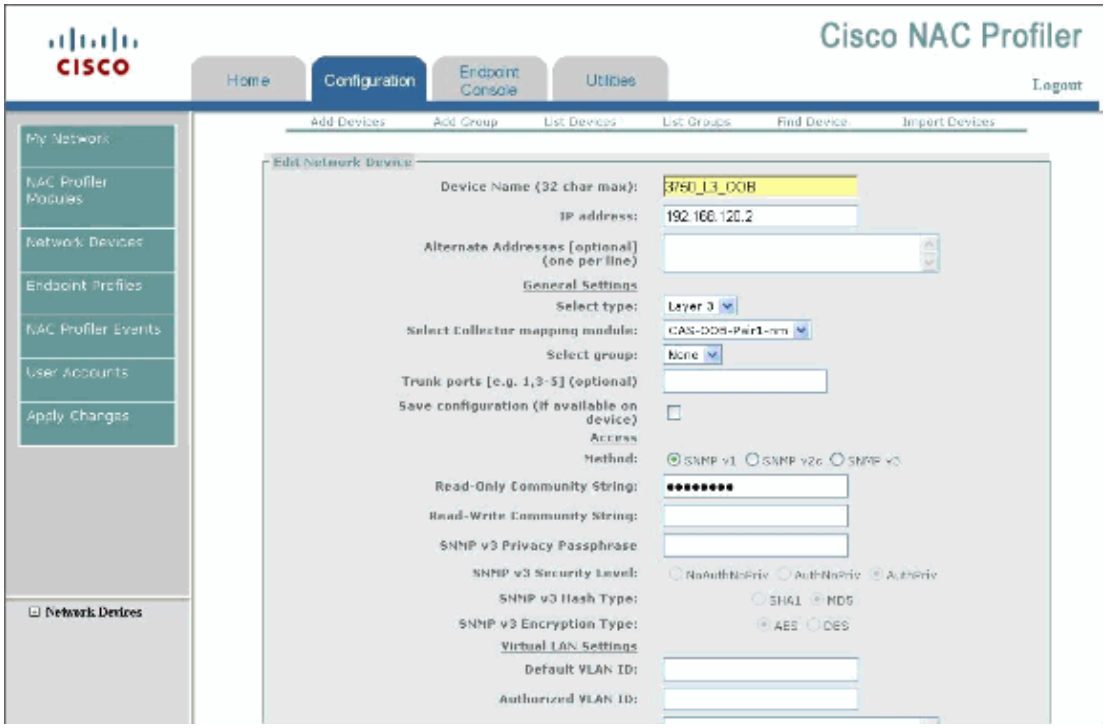
1. Choose **Profiler GUI > Configuration > Network devices > Add Device**.

   Figure 18



2. Add the host name and management IP address of the switch.
3. Also enter the read−only snmp strings configured on the switch. Make sure to choose the NAC Collector mapping module so the Collector is chosen to SNMP poll the access switch every hour and forward the information to Profiler.
4. Click **Add Device** and **Apply Changes** in order to update Modules from the left−hand pane of the GUI.

   Figure 19

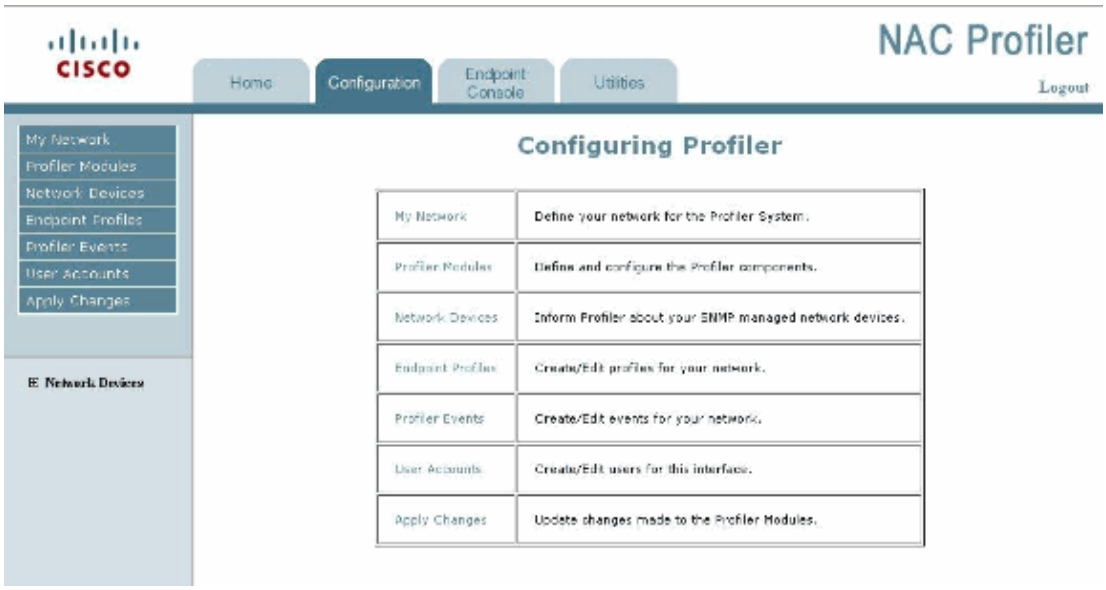


Configure the Remote Access Router on the Profiler for SNMP Information Gathering

This allows Layer 3 IP address to MAC binding in the Profiler database.

1. Choose the **Profiler GUI > Configuration > Network devices > Add Device**.

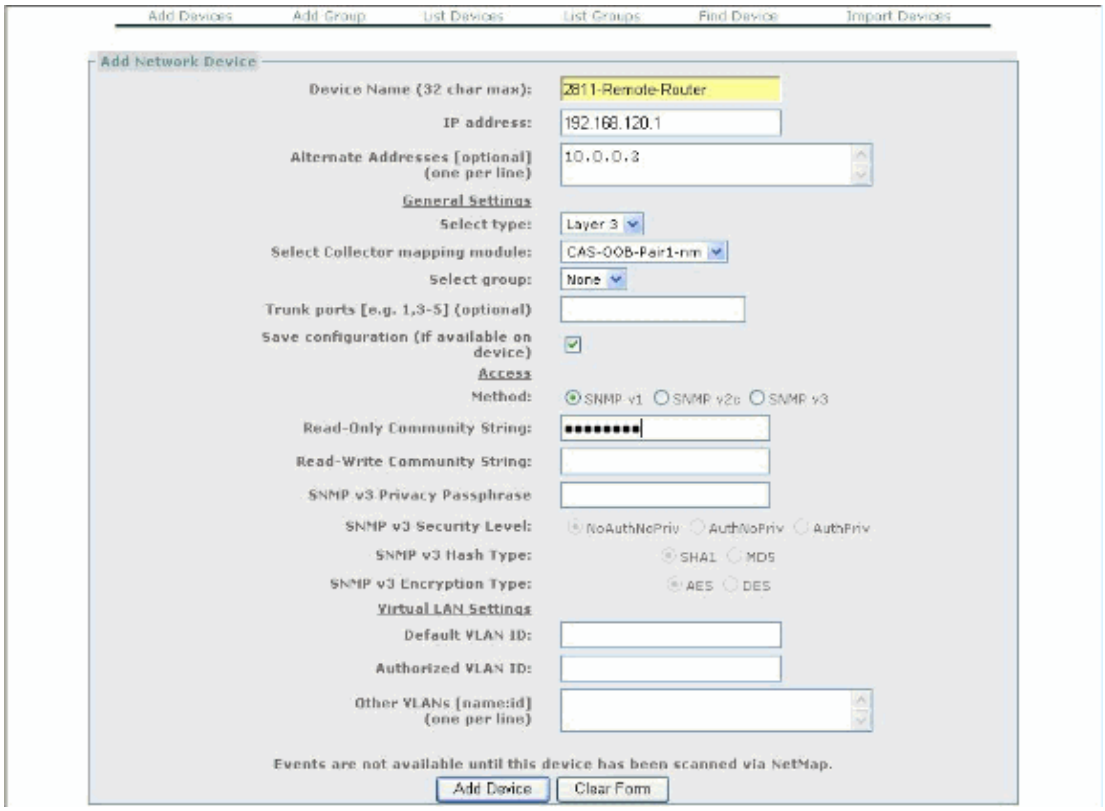
   Figure 20



   See the Figure 21.
2. Add the host name and management IP address of the Router.
3. Also enter the read−only snmp strings configured on the Router. Make sure to choose the NAC Collector mapping module so the Collector is chosen to SNMP poll the access switch every hour and forward the information to Profiler.

4. Click **Add Device** and **Apply Changes** in order to update Modules from the left−hand pane of the GUI.

Figure 21



Configure the NAC Collectors to Receive SPAN Traffic on their Local Switches

Note: This allows the NetWatch Module to start to listen for traffic on the network and forward information to the Profiler. Make sure you do not oversubscribe the interface of the NAC Collector. It has a limitation of 1 GB/sec. You can source the interfaces or vlans of the switch, and that depends on your switch model and version of code.

Note: Minimally you want to see the DHCP requests and offers from the endpoints on your access switches. If this is not possible, try to add a NAC Collector on or near the DHCP servers on your network. This is done in this configuration guide.

Complete these steps:

1. Configure a monitor session on the distribution switch #1 for remote site incoming and outgoing traffic:

```
monitor session 1 source interface F0/0
monitor session 1 destination interface Gi1/0/44
```

2. Configure a duplicate monitor session on the distribution switch #2 for remote site incoming and outgoing traffic:

```
monitor session 1 source interface F0/0
monitor session 1 destination interface Gi1/0/44
```

3. Configure another monitor session for the Stand−alone Collector. This example monitors several

interfaces connected to a core switch that are of importance. These are the DHCP, DNS, and Cisco CallManager Servers for this lab setup.

```
monitor session 1 source interface G1/0/7-9
monitor session 1 destination interface G1/0/48
```

Configure the Remote Access Router to Send NetFlow Data to the Collector in the Main Site

Complete these steps:

1. Telnet to the remote Router.
2. Enable Netflow globally.

   ```
   ip flow-export version 5
   ip flow-export destination 192.168.97.12 2055
   ```

   Note: Collectors listen on UDP port 2055 for Netflow. The IP address to send Netflow is always the Collectors management IP address.
3. Enable Netflow on the interfaces.

   ```
   interface FastEthernet0/1
    ip address 192.168.121.1 255.255.255.0
    ip flow ingress
    ip route-cache flow
   ```

Verify

See the Troubleshooting Procedure section in order to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

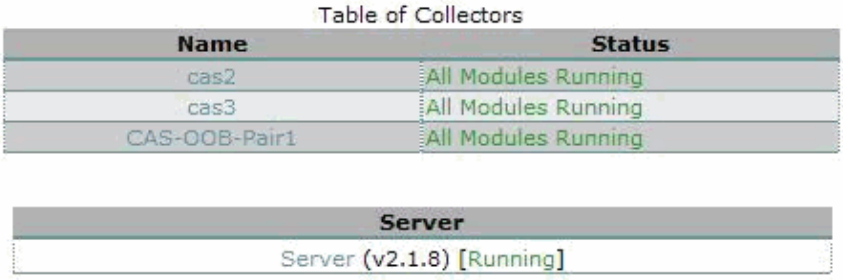
Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Troubleshooting Procedure

Complete these steps in order to troubleshoot your configuration.

1. Make sure Profiler and Collector are communicating and running. If they are not, then you do not see any information about devices in your network. If there are issues, do not proceed until all Collector Modules and the Server are `Running`.

   On the Profiler, choose **Configuration > NAC Profiler Modules > List NAC Profiler Modules**.



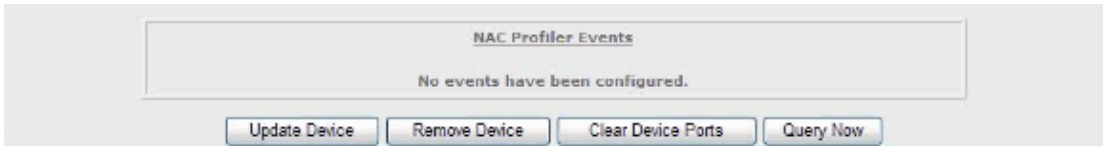
2. Verify the access switch sends new−mac notification traps to the Collector. Be careful when you enable debug and you should know its dangers.

```
nac−3750−access#debug snmp packet
nac−3750−access#debug snmp header
```

3. Verify the Collector has SNMP polled the switch:

   Look at the Last Scan column.

4. Debug SNMP again on the switch.
5. From the Profiler, choose **Configuration > Network Devices**. Choose to list **Network Devices** and then choose the **Device**.
6. Click **Query**.



7. Watch the debug output on the Switch for the Collector to SNMP poll the switch :

```
*Mar 30 23:09:24: SNMP: Packet received via UDP from 192.168.97.11 on Vlan100
*Mar 30 23:09:24: SNMP: Get−next request, reqid 1347517983, errstat 0, erridx 0
ifType = NULL TYPE/VALUE
*Mar 30 23:09:24: SNMP: Response, reqid 1347517983, errstat 0, erridx 0
ifType.1 = 53
*Mar 30 23:09:24: SNMP: Packet sent via UDP to 192.168.97.11
```

8. Plug in your IP phone on the switch or issue the **shut then no shut** command on the interface :

```
15w4d: %LINK−3−UPDOWN: Interface GigabitEthernet1/0/4, changed state to down
15w4d: %ILPOWER−5−POWER_GRANTED: Interface Gi1/0/4: Power granted
15w4d: %LINK−3−UPDOWN: Interface GigabitEthernet1/0/4, changed state to up
15w4d: %LINEPROTO−5−UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed
15w4d: SNMP: Queuing packet to 192.168.97.12
15w4d: Outgoing SNMP packet
15w4d: v2c packet
15w4d: community string: profiler
15w4d: SNMP: V2 Trap, reqid 14430, errstat 0, erridx 0
 sysUpTime.0 = 949829672
 snmpTrapOID.0 = cmnMacChangedNotification
 cmnHistMacChangedMsg.0 =
01 00  79 00   07 50  C6 82    27 00  04 00
```

9. Verify the Collector sends a new trap request for the MAC address received:

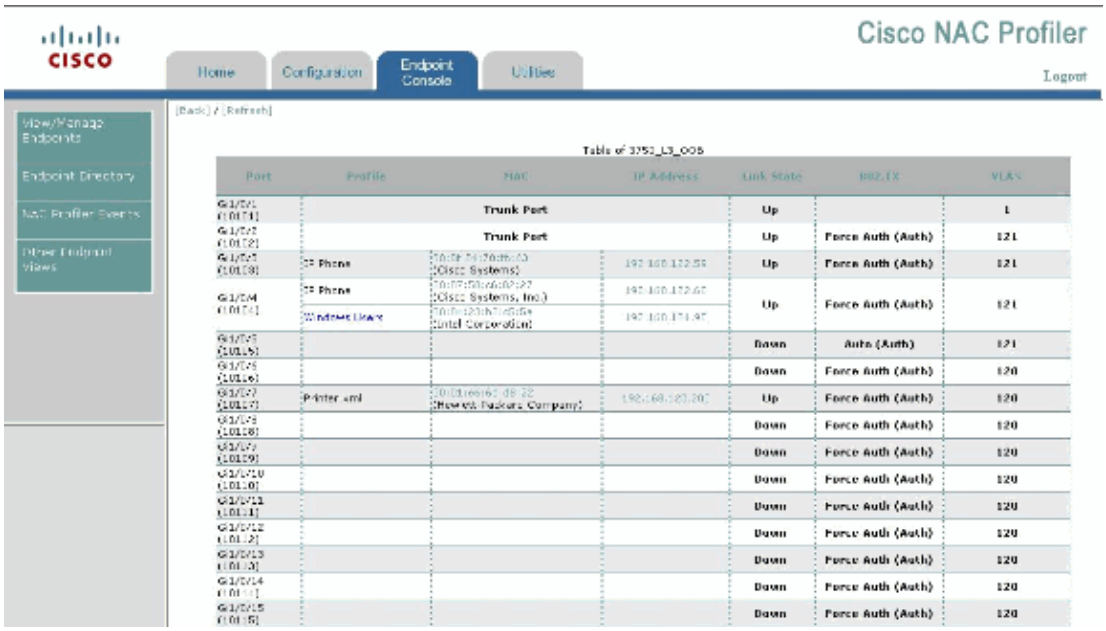
```
15w4d: SNMP: Packet received via UDP from 192.168.97.11 on Vlan120
```

```
15w4d: SNMP: Get request, reqid 1576567642, errstat 0, erridx 0
 system.1.0 = NULL TYPE/VALUE
 ifIndex.10104 = NULL TYPE/VALUE
 ifDescr.10104 = NULL TYPE/VALUE
 ifType.10104 = NULL TYPE/VALUE
 ifSpeed.10104 = NULL TYPE/VALUE
 ifPhysAddress.10104 = NULL TYPE/VALUE
 ifAdminStatus.10104 = NULL TYPE/VALUE
 ifOperStatus.10104 = NULL TYPE/VALUE
 ifName.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortStatus.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortControl.10104 = NULL TYPE/VALUE
paeMIBObjects.2.4.1.9.10104 = NULL TYPE/VALUE

-------snip ----------
ifIndex.10104 = 10104
 ifDescr.10104 = GigabitEthernet1/0/4
 ifType.10104 = 6
 ifSpeed.10104 = 100000000
 ifPhysAddress.10104 = 00 14 A8 2E A5 04
 ifAdminStatus.10104 = 1
 ifOperStatus.10104 = 1
 ifName.10104 = Gi1/0/4
 dot1xAuthAuthControlledPortStatus.10104 = 1
 dot1xAuthAuthControlledPortControl.10104 = 3
15w4d: SNMP: Packet sent via UDP to 192.168.97.11
```

10. Verify the Profiler received the new MAC address of the IP Phone from the Collector:

    Choose **Endpoint Console > View/Manage Endpoints > Display Endpoints by device ports > ungrouped > Table of Devices** and then choose your switch.



11. Verify SPAN works on the switch and the Collector is receiving traffic.

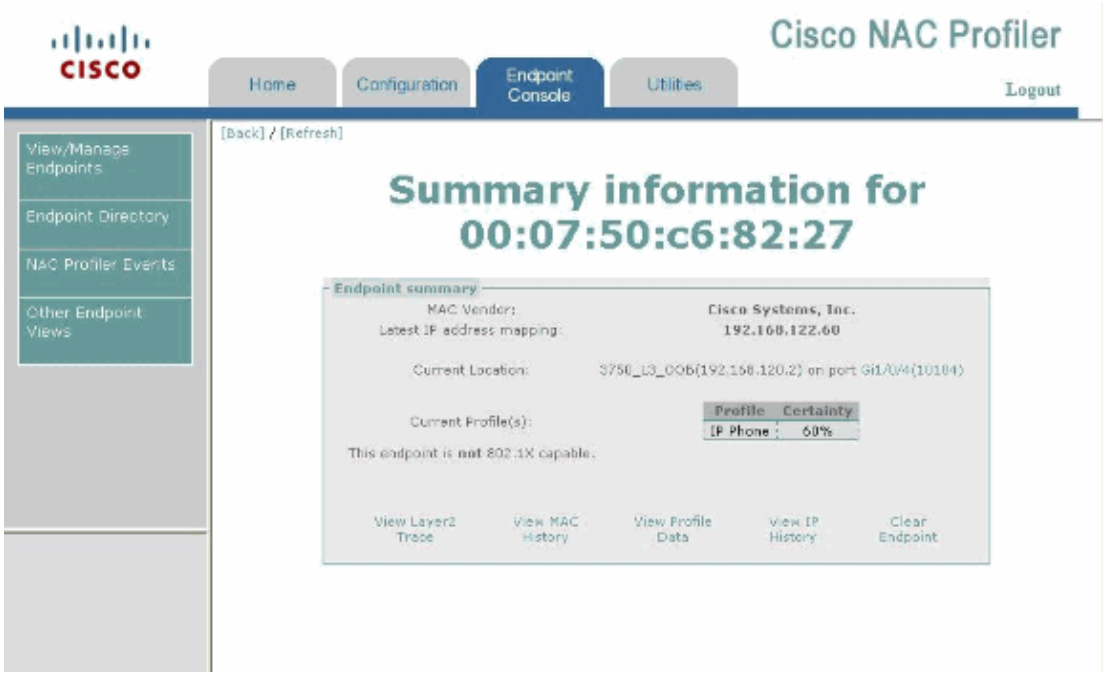
```
SSH to the NAC Profiler :
Type : tcpdump  i eth3

16:54:36.432218 IP cas2.nacelab2.cisco.com.9308 > elab2-dns-
dhcp.nacelab2.cisco.com.domain:  48871+ PTR? 68.39.168.192.in-addr.arpa. (44)
```

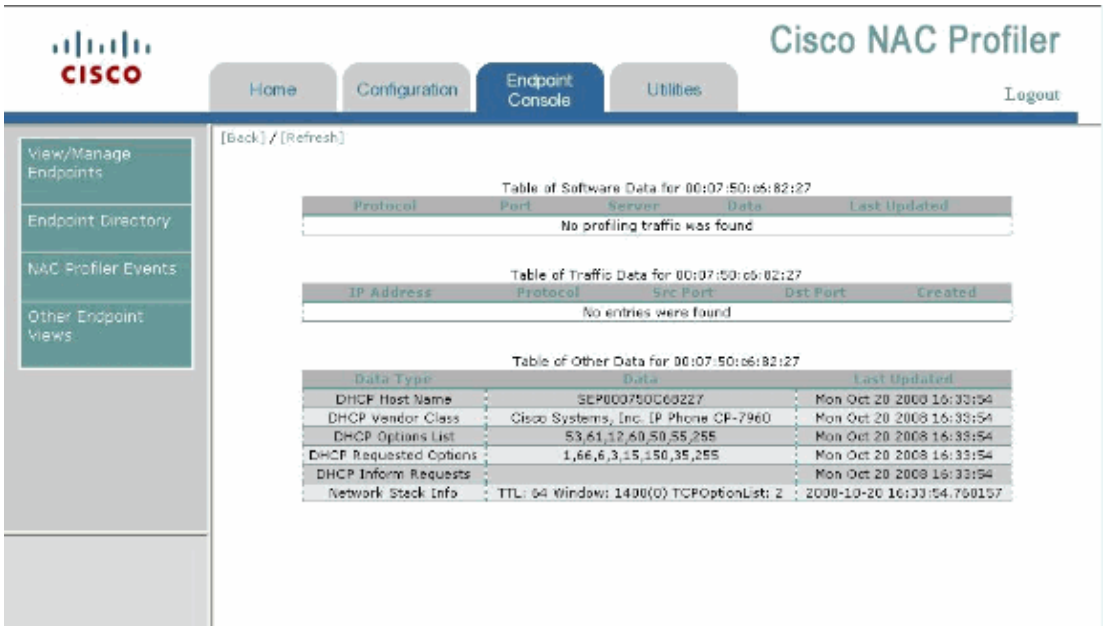
    Watch the output on the screen. If you are concerned about the amount of output, you can pipe the output to a file on the NAC Collector. See the man pages in Linux on how to perform this.

12. Check to see if DHCP traffic about the IP Phone endpoint has been seen through the SPAN port and sent up to the Profiler.

    a. Choose **Endpoint Console > View/Manage Endpoints > Display Endpoints by device ports > ungrouped > Table of Devices** and then choose your switch.
    b. Then choose the **MAC address** of your devices.
    c. Click **View Profile Data**.



You should see DHCP Vendor Class information from the devices captured from NetWatch/SPAN traffic on the Collector. This information can come from the DHCP Server or the DHCP Offer on the SPAN port back to the client, which depends on your routing and environment.



13. Verify Netflow is being passed from the remote router to the management interface of the Collector.

```
NAC-2800-Remote#show ip flow export
```

```
Flow export v5 is enabled for main cache
  Exporting flows to 192.168.97.12 (2055)
  Exporting using source IP address 10.0.0.2
  Version 5 flow records
  2602429 flows exported in 554968 udp datagrams
  0 flows failed due to lack of export packet

NAC-2800-Remote#show ip flow top 10 aggregate source-address
```

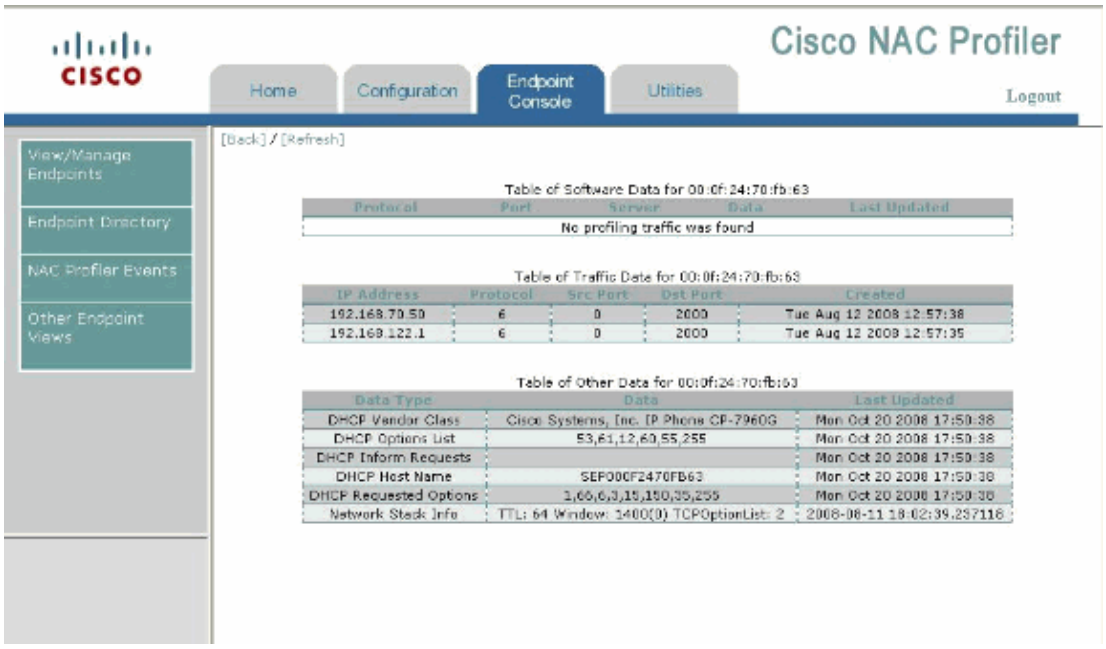
There are four top talkers:

```
IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
192.168.122.60           44           1           1
192.168.122.59           88           2           2
192.168.121.90          367           3           3
10.0.0.1              19320         322           1
```

14. Verify that the Profiler from the Collectors receives Netflow. Choose your remote MAC or Endpoint IP and look at the Profiled Data:

    a. Choose **Endpoint Console > View/Manage Endpoints > Display Endpoints by device ports > ungrouped > Table of Devices** and then choose your switch.
    b. Then choose the MAC address of your devices.
    c. Click **View Profile Data**.

    In the output, you see destination traffic to IP 192.168.70.50 and destination port 2000. This is the IP address of the Cisco CallManager and the destination port 2000 is used for SCCP control traffic.



Related Information

- **Technical Support & Documentation − Cisco Systems**