

# Colectores del Profiler del NAC y del SERVIDOR del NAC en una guía de configuración fuera de banda de la capa 3

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Descripción del Profiler del NAC](#)

[Descripción del NAC](#)

[Descripción del Guía de despliegue](#)

[Configuración](#)

[Configure el Profiler del NAC en la topología de la capa 3 OOB](#)

[Configure los módulos del colector del NAC en el servidor del NAC](#)

[Configure el Switch de Acceso Remoto para enviar el SNMP traps al colector del NAC](#)

[Configure el Switch de Acceso Remoto en el Profiler para la reunión de la información de SNMP](#)

[Configure al router del Acceso Remoto en el Profiler para la reunión de la información de SNMP](#)

[Configure los colectores del NAC para recibir el tráfico del SPAN en sus switches locales](#)

[Configure al router del Acceso Remoto para enviar los datos de NetFlow al colector en el sitio principal](#)

[Verificación](#)

[Troubleshooting](#)

[Procedimiento de Troubleshooting](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento describe cómo implementar los colectores del Profiler del NAC y del SERVIDOR del NAC en un despliegue fuera de banda de la capa 3. Si usted despliega el servidor del NAC en la alta disponibilidad (HA), después solamente un colector es activo y el otro está en el recurso seguro. Si usted no hace el HA, usted puede agregar cada colector en el Profiler por separado y tener ambos servidores del NAC funcionados con como colectores. Esta guía refleja en la instrumentación del servidor HA.

## [prerrequisitos](#)

### [Requisitos](#)

Los requisitos de esta guía son que usted ha configurado su administrador del NAC, servidor del NAC, Profiler del NAC, y infraestructura de red según las guías de instalación y configuración para cada producto.

## [Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Administrador del NAC
- Servidor del NAC
- Profiler del NAC
- Switch de distribución 3750
- Switch de acceso de 3750 sitios remotos
- Router de sitio remoto 2800
- Router de distribución 3800

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## [Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## [Descripción del Profiler del NAC](#)

Administradores de la red de los permisos del Cisco NAC Profiler para desplegar y para manejar eficientemente el Network Admission Control (NAC) en las redes para empresas de la escala diversa y de la complejidad con la identificación, la ubicación y la determinación de las capacidades de todos los puntos finales de red conectada, sin importar el tipo de dispositivo, para asegurar y mantener el acceso a la red apropiado. El Cisco NAC Profiler es un sistema agentless que descubre, catálogos, y perfila todos los puntos finales conectados con una red.

## [Descripción del NAC](#)

El dispositivo del Cisco Network Admission Control (NAC), que también se conoce como acceso limpio de Cisco, es solución un control de admisión y de una aplicación potentes, fáciles de usar de la conformidad. Con las funciones de seguridad completas, en-banda o las Opciones de instrumentación fuera de banda, las herramientas de la autenticación de usuario, y los controles del ancho de banda y del filtrado de tráfico, el dispositivo NAC de Cisco es una solución completa para controlar y para asegurar las redes. Como la punta central de la Administración de acceso para su red, el dispositivo NAC de Cisco le deja implementar la Seguridad, el acceso, y las directivas de la conformidad en un lugar en vez de la necesidad de propagar las directivas en la red en muchos dispositivos.

## [Descripción del Guía de despliegue](#)

En el cuadro 1, hay un despliegue simple del sitio remoto con los servidores centrales del NAC HA que actúa como la punta de la aplicación para los dispositivos fuera de banda de la capa 3. El Profiler del NAC y el administrador del NAC se sientan en la misma red de administración y envían y reciben la información de los servidores y de los colectores. Hay también un colector independiente que ase la información de DHCP esencial sobre los dispositivos con el SPAN en el centro de datos o la capa del núcleo. Hay varias maneras de descubrir que los puntos finales remotos y esta guía pueden ayudarle en su despliegue. No se piensa para ser una guía obligatoria sino le muestra cómo cada módulo en los colectores puede ser utilizado y cómo los datos del punto final son considerados por el Profiler para tomar las decisiones de perfilado para usted.

Una lista de las herramientas obligatorias y opcionales que los colectores del servidor del NAC utilizan se proporciona.

### **Módulos obligatorios del colector**

**NetTrap** — Este módulo está atento el SNMP traps enviado por el Switches para la notificación del nuevo-mac o las notificaciones arriba/abajas del link. Este módulo envía todas las nuevas direcciones MAC al Profiler para perfilar. Esta característica se define por el Switch en la línea de comando configuration del Servidor SNMP en el <sup>®</sup> del Cisco IOS.

**NetMap** — Este módulo se sienta en el colector y es responsable de hacer la Consulta SNMP de los dispositivos en la sucursal remota en los intervalos temporizados. En el diagrama del cuadro 1, el colector SNMP CAS1a sondea el switch remoto y al router para la información MIB específica con el acceso de lectura al Switch. Esta interrogación proporciona las cosas como el MAC address a la información de puerto, las interfaces, estado de link, información del dot1x, información del sistema y así sucesivamente.

(SPAN) de **NetWatch** — El módulo de NetWatch puede escuchar en un puerto SPAN de un Switch y enviar la información del tráfico ingerida de nuevo al Profiler. Un servidor del NAC requiere una interfaz adicional en cada SERVIDOR del NAC recoger los datos. Esto es esencial porque el Profiler se basa sobre todo en la información de DHCP pasajera por los dispositivos y cierto otro corresponder con del tráfico de aplicación.

### **Módulos opcionales del colector**

Usted puede utilizar el SPAN o el Netflow. Está hasta el despliegue y los requisitos del cliente pero uno se recomienda solamente en un servidor debido del NAC a la cantidad de tráfico que se envía a los módulos del colector y a las otras funciones del NAC que el servidor del NAC tiene que realizar. Usted también pierde pedazos informativos más vitales sobre los dispositivos con el Netflow como la información del vendedor del DHCP, los destinos URL, información del cliente de Web, información del servidor Web y así sucesivamente.

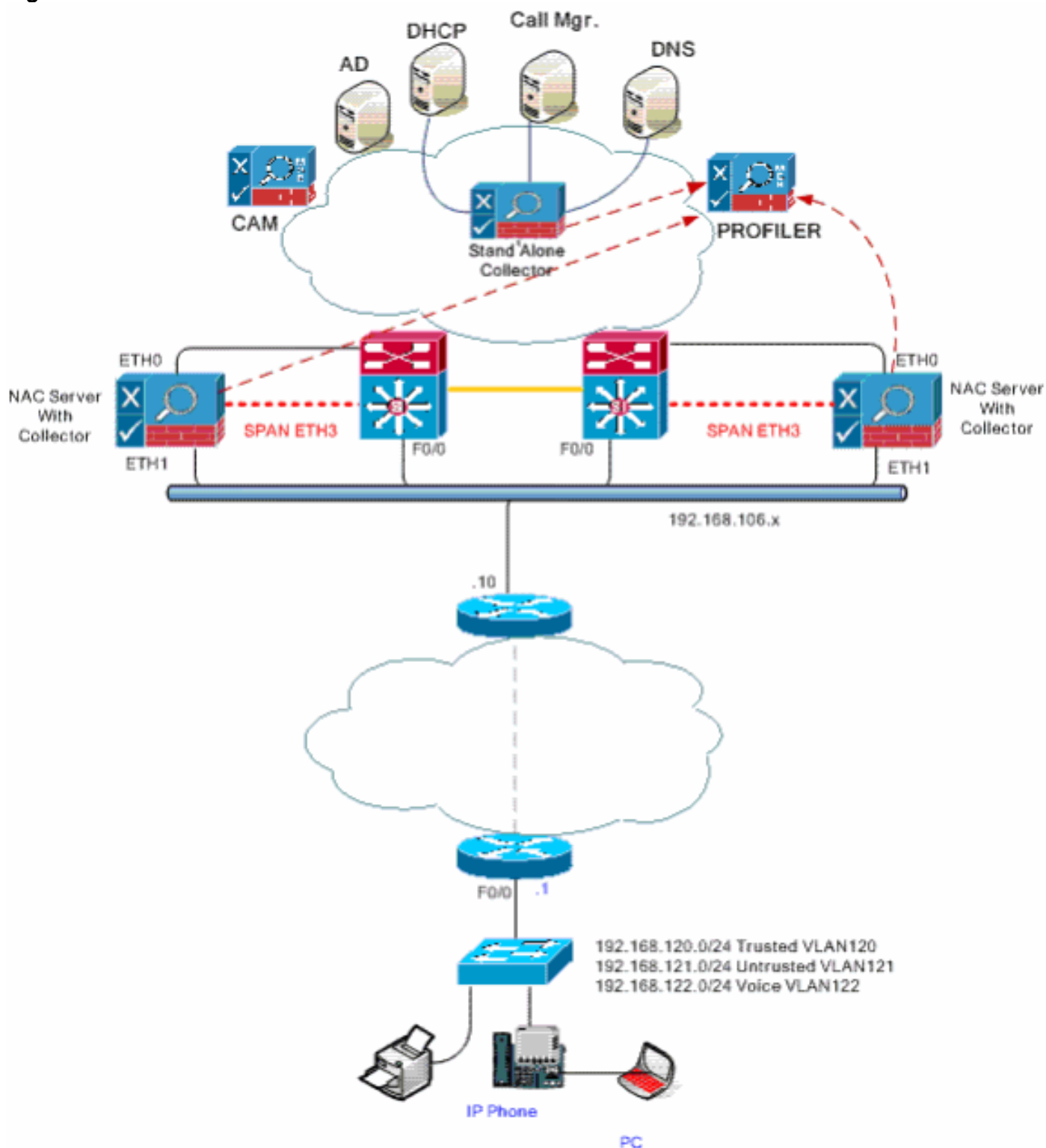
**NetRelay** — (Netflow) se configura en cada router en a por la base de la interfaz y el destino es el IP Address de administración del SERVIDOR del NAC. Un agente del Netflow se sienta en el SERVIDOR del NAC y analiza la información de NetFlow basada en sus reglas y redes de tráfico configuradas en el Profiler.

**NetInquiry** — Esto es un mecanismo pasivo y activo basado en sus cosas como los puertos abiertos TCP. Por ejemplo el SERVIDOR del NAC hace un SYN/ACK y después cae la conexión para sondear un rango o los rangos de la subred determinada para los puertos TCP abiertos. Si hay una respuesta, envía la información al Profiler con la dirección IP y el puerto TCP sondeados.

**Note:** Para NetInquiry, agregue solamente las subredes o los host específicos que no se pueden alcanzar o considerar con el Netflow o NetWatch. NetInquiry puede sobrecargar su servidor del NAC con el procesamiento extra y a los Recursos de hardware como la memoria y la utilización de la CPU si no configuradas correctamente. Utilice esta característica como último recurso.

**Note:** Si usted tiene un colector independiente usted puede habilitar el Netflow y el SPAN en el mismo dispositivo sino asegúrese no al oversubscribe el colector.

Figura 1



## Configuración

## Configure el Profiler del NAC en la topología de la capa 3 OOB

- Los servidores del NAC necesitan ser configurados con la configuración normal del NAC HA.
- El colector del NAC utiliza a la dirección IP virtual del servidor del NAC para comunicarse con el Profiler.
- El par del colector HA del NAC se agrega como sola entrada en el Profiler y comunica a la dirección IP virtual de CAS.

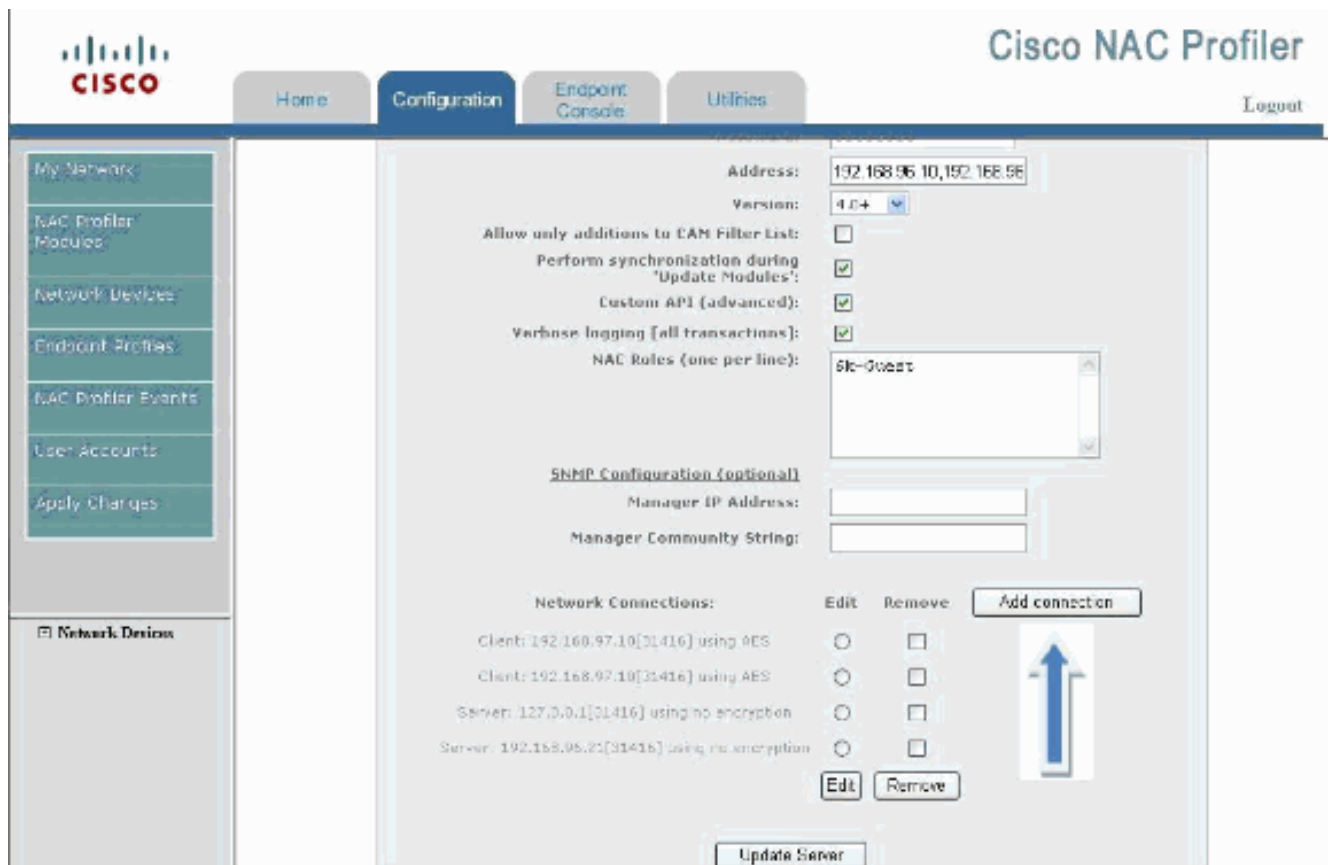
Figura 2



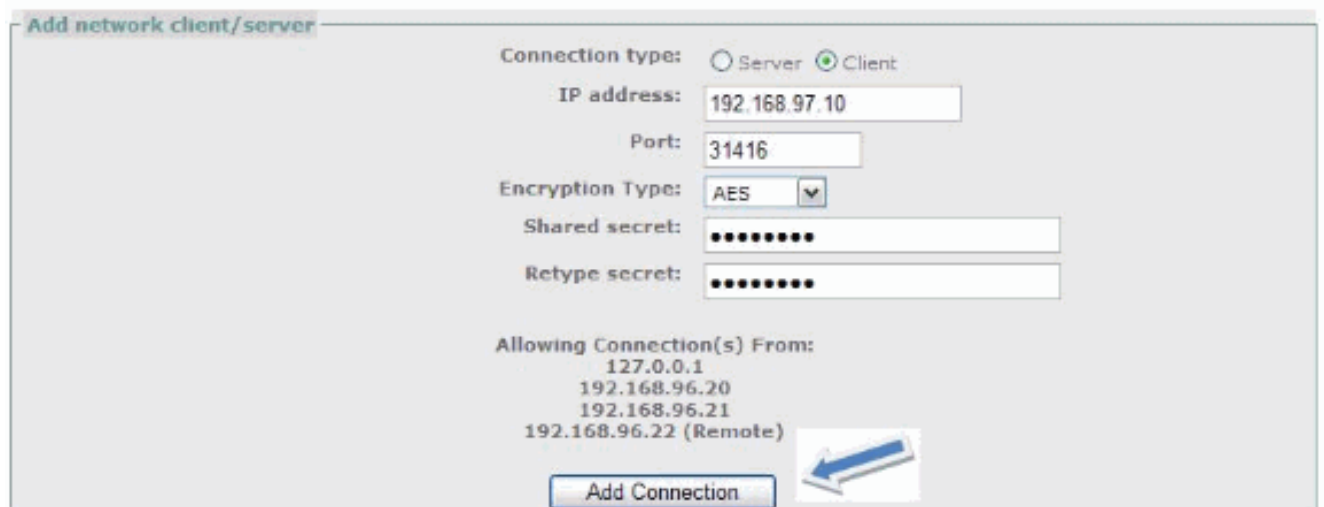
### Configuración de la configuración

Complete estos pasos:

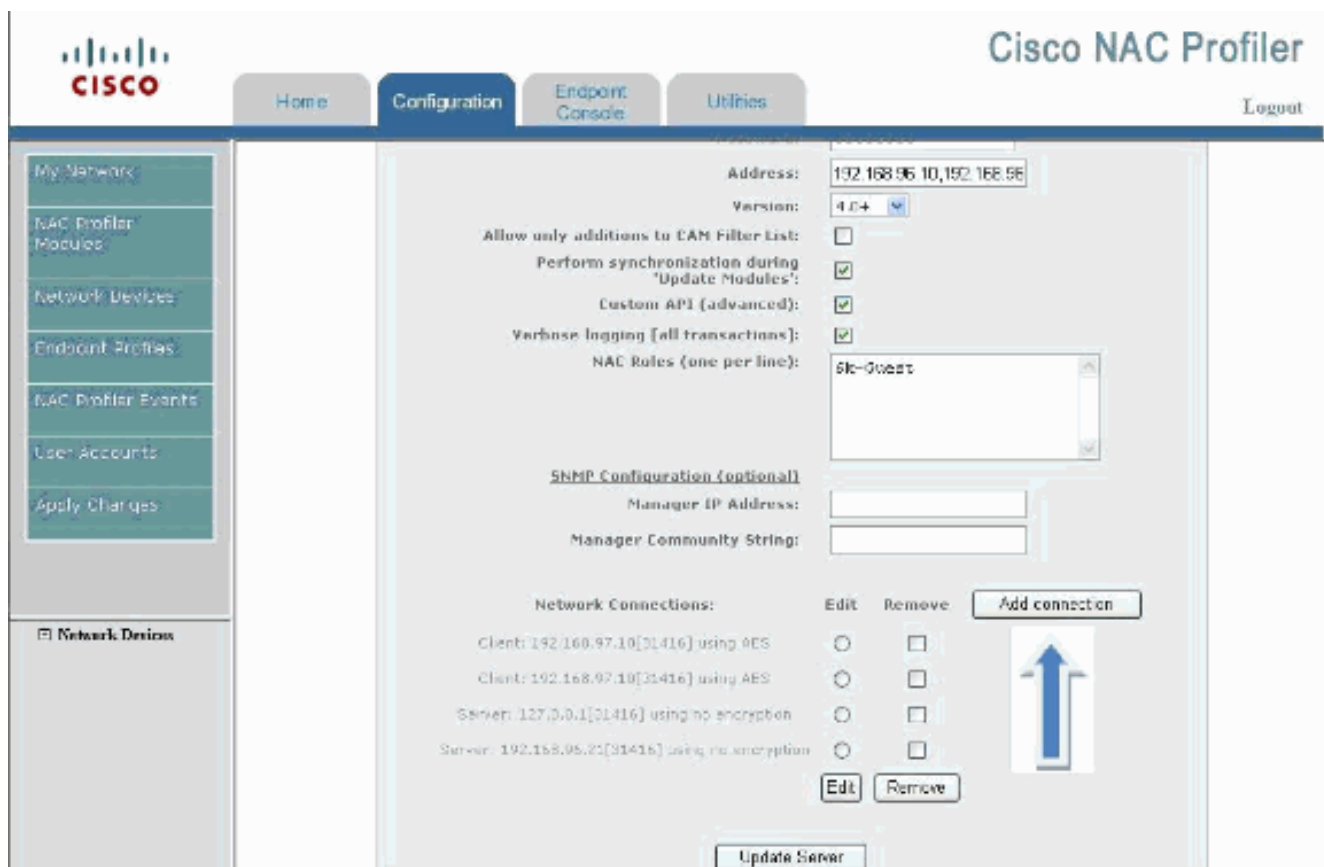
1. El Profiler necesita una *conexión cliente* para los nuevos colectores del NAC.
2. El Profiler necesita una *conexión del servidor* para el dispositivo independiente que se sienta cerca de la distribución|centro de datos|capa de los servicios en el diagrama de la red.
3. Elija los **módulos de la configuración > del Profiler del NAC – Enumere los módulos del Profiler del NAC** y después haga clic la lengüeta del **servidor**. Navegue a la parte inferior de la página y el tecleo **agrega la conexión**. Figura 3



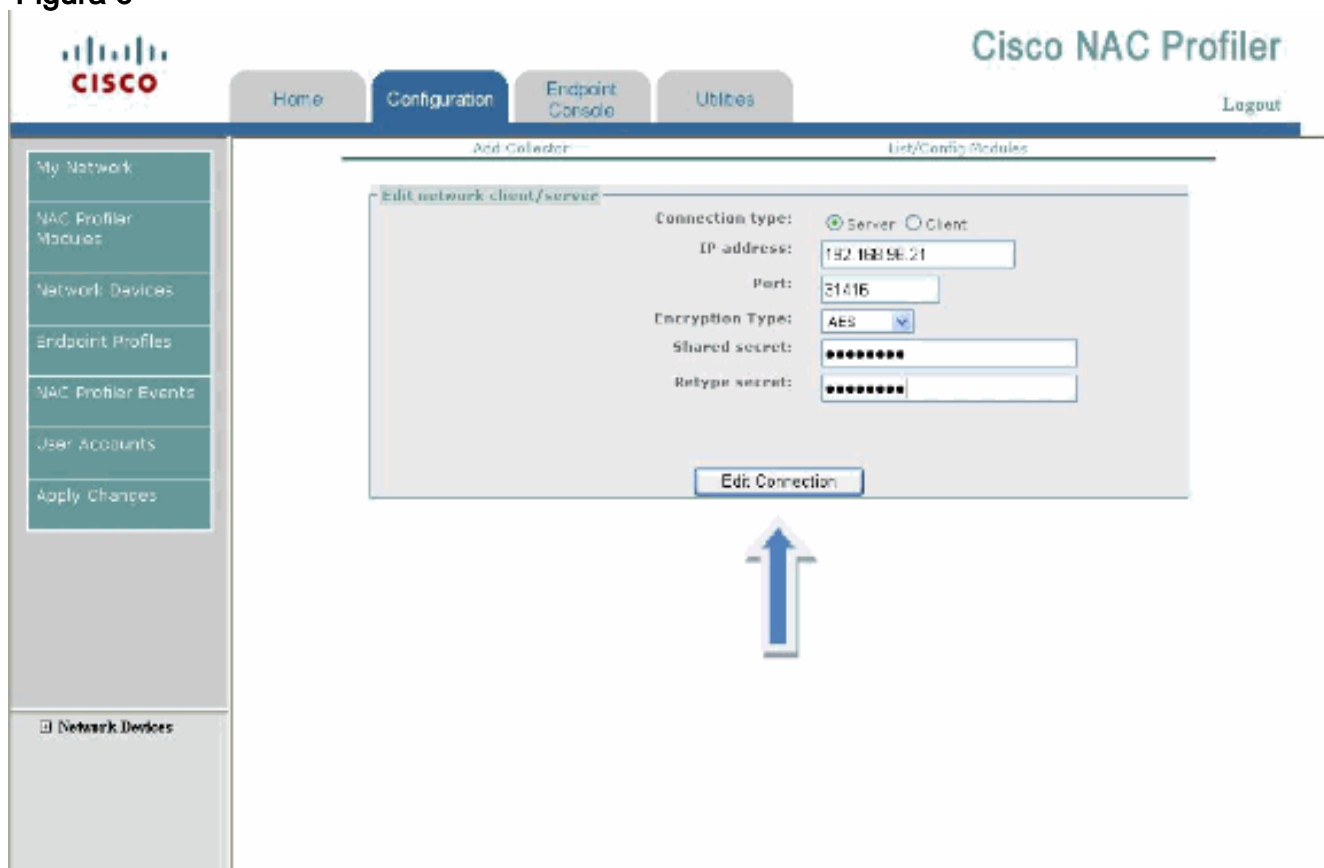
4. Ingrese el IP Address del servicio y la información de clave secreta del colector y del teclado HA agrega la conexión. 'Figura 4'



5. El teclado agrega la conexión otra vez. Figura 5

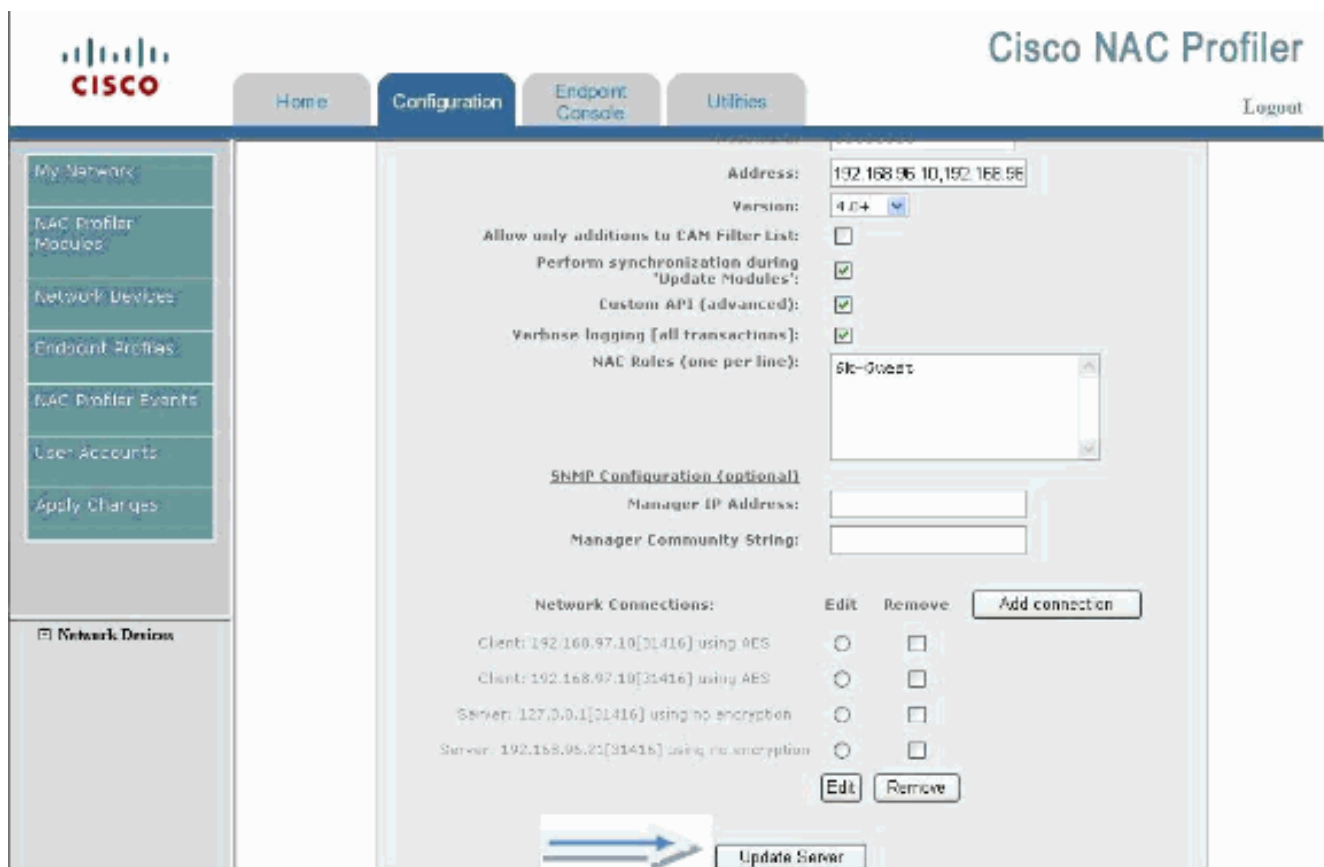


'Figura 6'



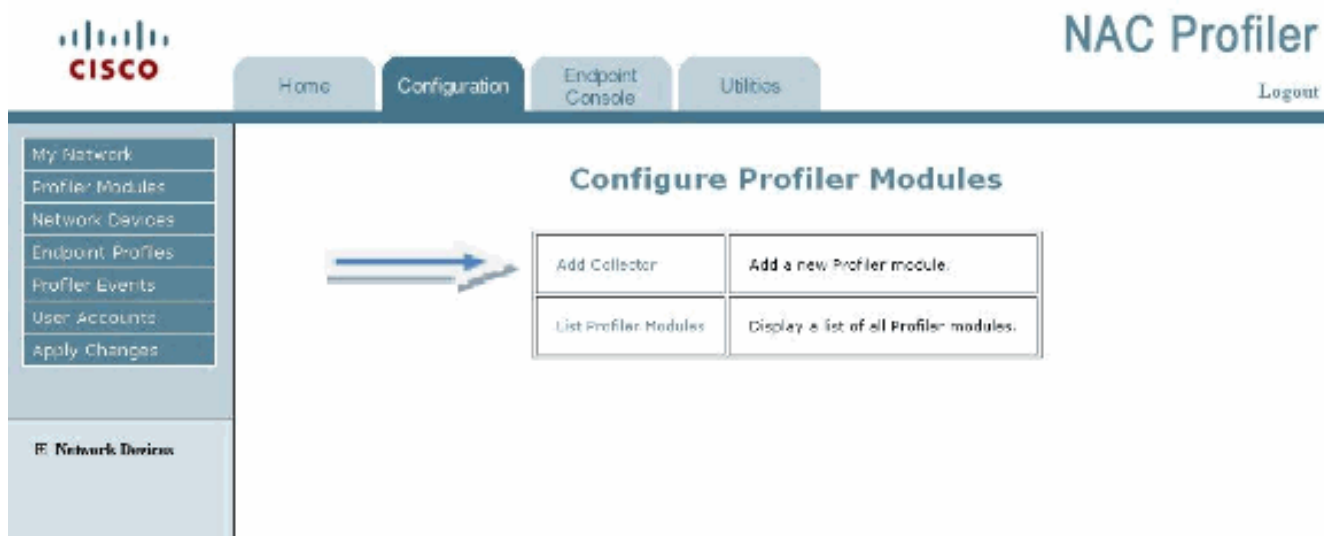
6. Ingrese el **IP Address** para configurar una *conexión del servidor* con la cual el colector autónomo conecte.
7. El tecleo **edita la conexión** cuando le hacen para volver a la página de la Configuración del servidor.
8. **Servidor de actualización del tecleo** en la página de la Configuración del servidor. **Figura 7**





Agregue dos nuevos colectores al Profiler. Complete estos pasos:

1. Elija el colector de los módulos de la configuración > del Profiler del NAC > Add.Figura 8



2. Agregue un nuevo nombre del colector para los pares del servidor HA del NAC. Éste puede ser cualquier cosa que usted quiere pero que debe hacer juego en la configuración del colector.Nombre del colector — CAS-OOB-Pair1Dirección IP 192.168.97.10 (dirección virtual del servidor del NAC)Conexión — Déjela como **NINGUNOS** por ahora. Usted puede cambiar esto en otro momento a una conexión del servidor que sea adentro escuche modo.
3. El tecleo **agrega** el botón del colector.Figura 9



Add Collector List/Config Modules

---

**Add Collector**

**COLLECTOR:**

**Forwarder Configuration**

IP address:

Connection:  ▼

4. Configure sus módulos de servicio del colector. Deje NetMap y NetTrap solos. **Figura 10**

**Edit Collector**

**COLLECTOR:** CAS-OOB-Pair1

**NetMap Configuration**

Module Status: Running

Maximum allowed workers:

SNMP interpacket delay (microseconds):

**NetTrap Configuration**

Module Status: Running

No configuration required

5. Agregue una interfaz de NetWatch (eth3), que está conectada con un puerto SPAN en el switch de distribución. **Figura 11**

**NetWatch Configuration**

Module Status: Running

**Interfaces:**

eth3:

6. Agregue un bloque de la subred para el módulo de NetInquiry para estar atento el tráfico interesante que viene de las redes de acceso. Sea específico en las redes en cuanto a no el impuesto el servidor del NAC innecesariamente. En esta configuración de laboratorio, puede ser el espacio entero del soldado de 192.168.0.0. **Figura 12**

**NetInquiry Configuration**

Module Status: Running

Maximum allowed workers:

Enable Ping Sweep:

Enable DNS Collection:

Network blocks (one per line):  ▲▼

**Note:** Deje el ping sweep y la colección DNS inhabilitados. Utilice esto como último recurso. El ping sweep y la colección DNS acciona los ping y los nslookups en el rango de las subredes IP que usted pone en la sección de los bloques de la red. Esto no se recomienda y se utiliza raramente.

7. Configure el promotor para escuchar en la dirección IP 192.168.97.10 (VIP) y el puerto TCP 31416. Esto permite que el colector actúe como servidor y esté atenta una conexión del Profiler al puerto TCP específico. Esto refleja en los primeros pasos para la Configuración

del servidor.

8. Netflow del permiso para los pares del colector. (Opcional)Usted puede hacer esto aquí puesto que el Netflow se pasa del router remoto debido a ningún colector remoto.
9. Ingrese los bloques del IP Address para el sitio remoto según lo representado. En este ejemplo, se utiliza el espacio privado entero de 192.168.0.0.**Figura 13**

The screenshot shows the 'NetRelay Configuration' page. Under the 'NetFlow' section, the 'Module Status' is 'Stopped', and the 'Enable NetFlow Agent' checkbox is checked. The 'Internal Network blocks (one per line):' field contains '192.168.0.0/16'. Under the 'Forwarder Configuration' section, the 'Module Status' is 'Running', the 'IP address' is '192.168.97.12', and the 'Connection' dropdown is set to 'Connect to: Server (192.168.96.21:31416)'. At the bottom, there are 'Save Collector' and 'Delete Collector' buttons.

10. El tecleo **salva el colector** para salvar su configuración.

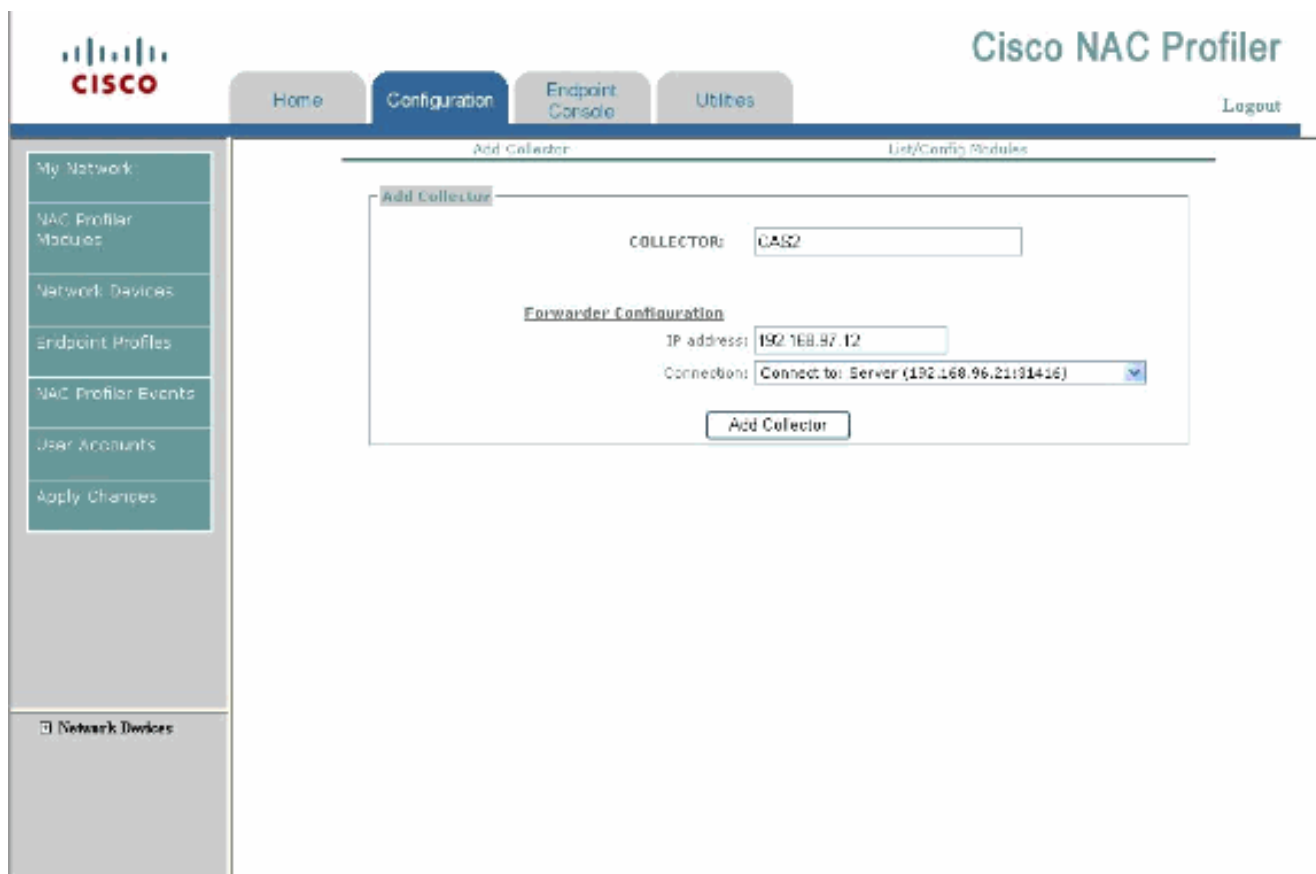
### Agregue el colector independiente adicional al Profiler

Complete estos pasos:

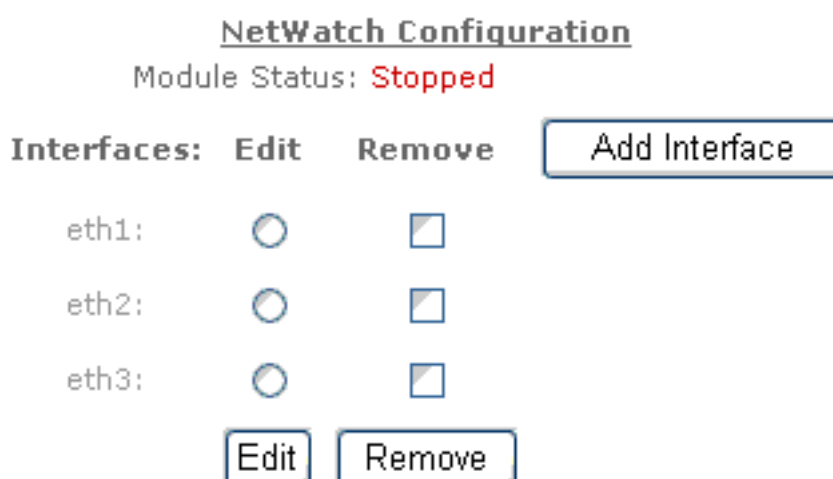
1. El tecleo **agrega el colector**.**Figura 14**

The screenshot shows the 'NAC Profiler' interface. The top navigation bar includes 'Home', 'Configuration', 'Endpoint Console', and 'Utilities'. The 'Configuration' tab is active. The main content area is titled 'Configure Profiler Modules' and contains four buttons: 'Add Collector', 'Add a new Profiler module.', 'List Profiler Modules', and 'Display a list of all Profiler modules.'. A sidebar on the left contains a menu with items like 'My Network', 'Profiler Modules', 'Network Devices', 'Endpoint Profiles', 'Profiler Events', 'User Accounts', and 'Apply Changes'. The Cisco logo is visible in the top left corner.

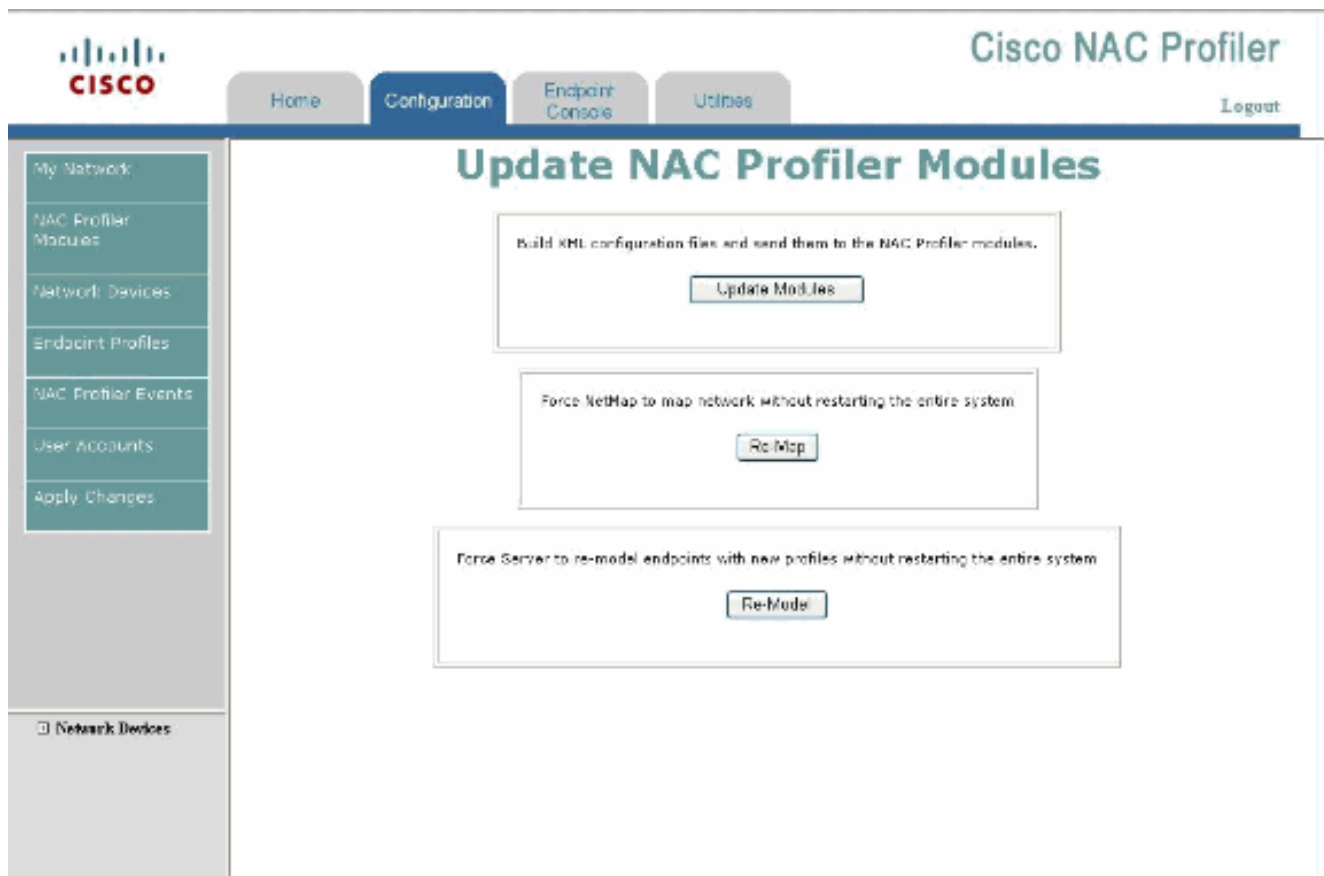
2. El nombre del colector puede ser cualquier cosa que usted quiere. En este ejemplo, es CAS2.
3. La dirección IP es sí mismo del promotor. La dirección IP del eth0 está para la Administración.En este ejemplo, es 192.168.97.12.La conexión debe ser la dirección IP del Profiler. En este caso, es 192.168.96.21.
4. El tecleo **agrega el colector**.**Figura 15**



5. Después de esto, le traen a la página de configuración del colector. Pasos completos 5 – 9 en la sección anterior. Esto permite que usted modifique y que agregue los IP Address únicos y los ajustes de la configuración del colector autónomo.
6. Una configuración única para el colector independiente es la capacidad de agregar las interfaces múltiples a la configuración de NetWatch. Aquí usted puede agregar varias interfaces así que usted puede ver el tráfico para el DHCP, el DNS, y la Telefonía IP de los puntos finales remotos.
7. Configure las interfaces de NetWatch para su configuración. En este ejemplo, tres interfaces fueron agregadas PARA ATRAVESAR el tráfico en el colector independiente. **Figura 16**



8. **Note:** Elija la configuración > aplican los cambios > los módulos de la actualización para salvar sus configuraciones.



## [Configure los módulos del colector del NAC en el servidor del NAC](#)

**Note:** Esta configuración necesita ser funcionada con en todos los colectores.

Esta configuración permite que el Profiler y los colectores comuniquen y establezcan las conexiones seguras para la información sobre los dispositivos para comenzar a fluir. Complete estos pasos:

1. SSH o consola al colector y login como **raíz de la consola** o del **faro de la sesión SSH**.
2. Ingrese el **comando config del colector del servicio**.
3. Ejecútese a través de la secuencia de comandos de configuración para poner la porción del colector del NAC. **Ejemplo del colector HAEI** el colector se pone como tipo de *conexión del servidor*.

```
[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]:
```

Le piden ingresar el IP Address de los NP. Esto es necesario configurar el Access Control List usado por este colector. Si los NP son parte de a los pares HA, después usted debe incluir el IP Address real de cada independiente NP y IP virtual para asegurar la conectividad apropiada en el caso de la Conmutación por falla. Ingrese el IP Address del Profiler del NAC.

```
[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]:
```

#### 4. Comience los servicios del colector.

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

#### Coloque el ejemplo solo del colector

```
[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 el Switch de Acceso Remoto para enviar el SNMP traps al colector del NAC](#)

Esta configuración permite que el Profiler reciba dinámicamente todos los nuevos dispositivos que conectan con un switchport a través de los desvíos de la mac-notificación. Esto es especialmente importante puesto que en la topología hay un teléfono del IP y un PC conectados con el mismo puerto.

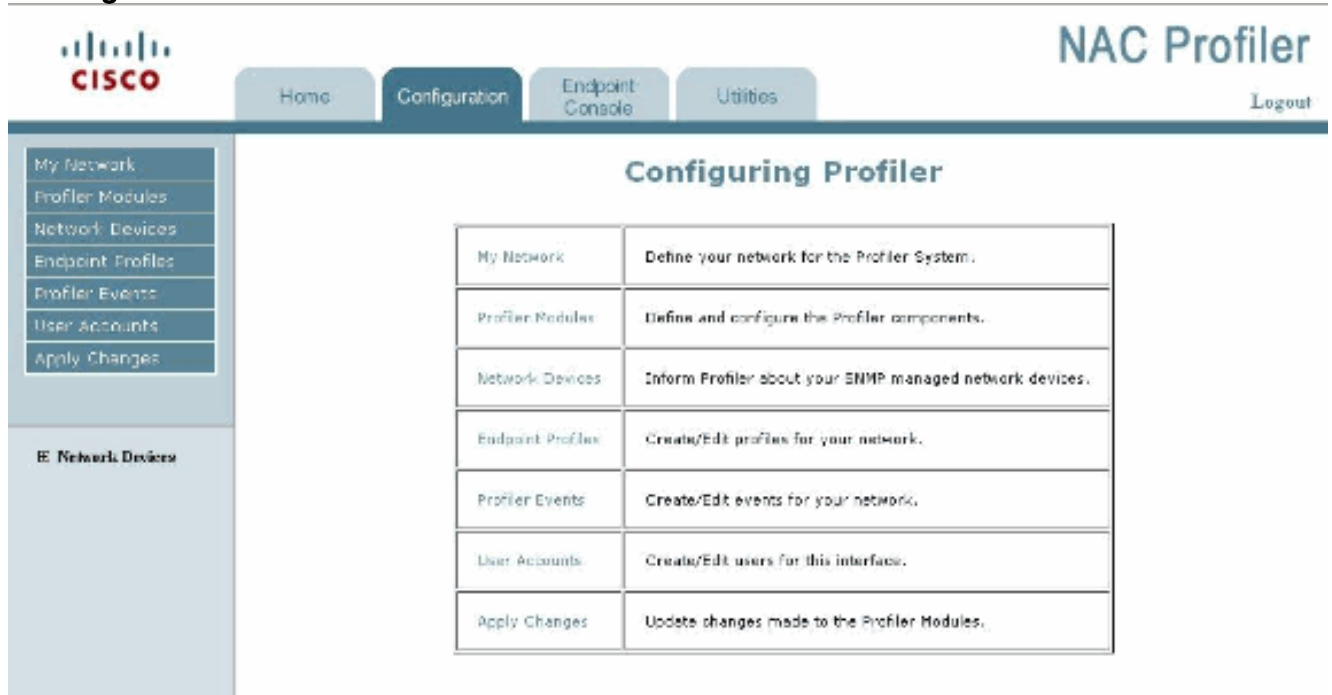
Consola o telnet en el Switch (`nac-3750-access#`).

```
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
```

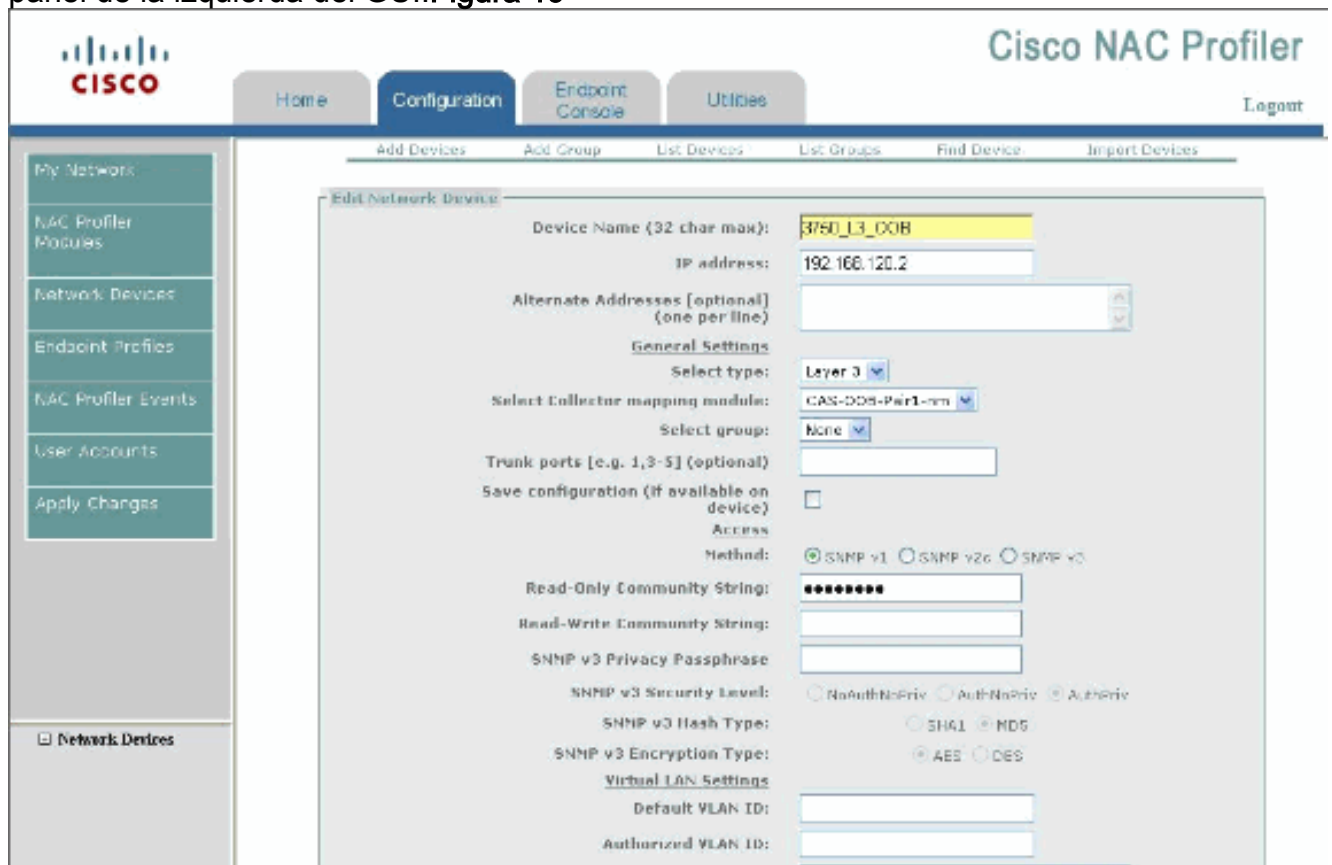
## [Configure el Switch de Acceso Remoto en el Profiler para la reunión de la información de SNMP](#)

Complete estos pasos:

1. Elija el Profiler GUI > dispositivo de la configuración > de los dispositivos de red > Add.Figura 18



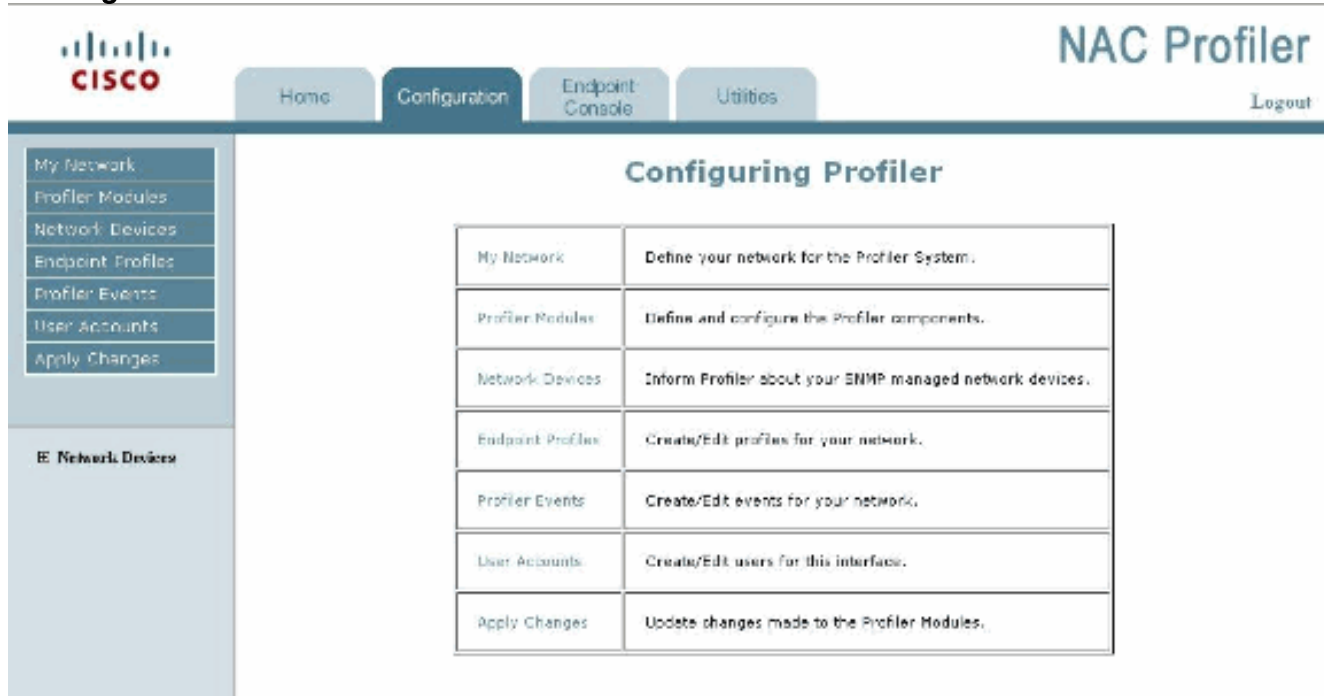
2. Agregue el nombre del host y el IP Address de administración del Switch.
3. También ingrese las cadenas solo lecturas SNMP configuradas en el Switch. Asegúrese elegir el módulo de la asignación del colector del NAC así que el colector se elige a la encuesta SNMP el switch de acceso cada hora y delantero la información al Profiler.
4. Haga clic **agregan el dispositivo** y **aplican los cambios** para poner al día los módulos del panel de la izquierda del GUI.Figura 19



## [Configure al router del Acceso Remoto en el Profiler para la reunión de la información de SNMP](#)

Esto permite la dirección IP de la capa 3 al MAC que ata en la base de datos del Profiler.

1. Elija el Profiler GUI > dispositivo de la configuración > de los dispositivos de red > Add.Figura 20



Véase el cuadro 21.

2. Agregue el nombre del host y el IP Address de administración del router.
3. También ingrese las cadenas solo lecturas SNMP configuradas en el router. Asegúrese elegir el módulo de la asignación del colector del NAC así que el colector se elige a la encuesta SNMP el switch de acceso cada hora y delantero la información al Profiler.
4. Haga clic **agregan el dispositivo** y **aplican los cambios** para poner al día los módulos del panel de la izquierda del GUI.Figura 21



[Add Devices](#)   [Add Group](#)   [List Devices](#)   [List Groups](#)   [Find Device](#)   [Import Devices](#)

---

**Add Network Device**

Device Name (32 char max):

IP address:

Alternate Addresses [optional] (one per line):

**General Settings**

Select type:

Select Collector mapping module:

Select group:

Trunk ports [e.g. 1,3-5] (optional):

Save configuration (if available on device):

**Access**

Method:  SNMP v1    SNMP v2c    SNMP v3

Read-Only Community String:

Read-Write Community String:

SNMP v3 Privacy Passphrase:

SNMP v3 Security Level:  NoAuthNoPriv    AuthNoPriv    AuthPriv

SNMP v3 Hash Type:  SHA1    MD5

SNMP v3 Encryption Type:  AES    DES

**Virtual LAN Settings**

Default VLAN ID:

Authorized VLAN ID:

Other VLANs [name:id] (one per line):

Events are not available until this device has been scanned via NetMap.

## [Configure los colectores del NAC para recibir el tráfico del SPAN en sus switches locales](#)

**Note:** Esto permite que el módulo de NetWatch comience a estar atenta el tráfico en la red y la información delantera al Profiler. Asegurese le no hacen oversubscribe la interfaz del colector del NAC. Tiene una limitación de 1 GB/sec. Usted puede fuente las interfaces o vlans del Switch, y ése depende de su modelo de switches y versión del código.

**Note:** Usted quiere como mínimo ver los pedidos de DHCP y las ofertas de los puntos finales en sus switches de acceso. Si esto no es posible, intente agregar un colector del NAC en o cerca de los servidores DHCP en su red. Esto se hace en esta guía de configuración.

Complete estos pasos:

1. Configure a una sesión de monitoreo en el switch de distribución #1 para el sitio remoto entrante y el tráfico saliente:

```
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
```

2. Configure a una sesión de monitoreo duplicado en el switch de distribución #2 para el sitio remoto entrante y el tráfico saliente:

```
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
```

3. Configure a otra sesión de monitoreo para el colector independiente. Este ejemplo monitorea varias interfaces conectadas con un switch del núcleo que sean de importancia. Éstos son el DHCP, el DNS, y el Cisco Callmanager servers para esta configuración de laboratorio.

```
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 al router del Acceso Remoto para enviar los datos de NetFlow al colector en el sitio principal](#)

Complete estos pasos:

1. Telnet al router remoto.
2. Netflow del permiso global.

```
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
```

**Note:** Los colectores escuchan en el puerto 2055 UDP el Netflow. La dirección IP para enviar el Netflow es siempre los colectores IP Address de administración.

3. Netflow del permiso en las interfaces.

```
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
```

## [Verificación](#)

Vea la sección del [procedimiento de Troubleshooting](#) para confirmar que su configuración trabaja correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

## [Troubleshooting](#)

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

**Note:** Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

## Procedimiento de Troubleshooting

Complete estos pasos para resolver problemas su configuración.

1. Asegurese el Profiler y el colector está comunicando y se está ejecutando. Si no son, después usted no ve ninguna información sobre los dispositivos en su red. Si hay problemas, no proceda hasta que todos los módulos del colector y el servidor se estén ejecutando. En el Profiler, elija de la **lista de la configuración > del Profiler del NAC los módulos del Profiler del NAC de los módulos >**.

Table of Collectors

Name	Status
cas2	All Modules Running
cas3	All Modules Running
CAS-OOB-Pair1	All Modules Running

Server
Server (v2.1.8) [Running]

2. Verifique el switch de acceso envía los desvíos de la notificación del nuevo-mac al colector. Tenga cuidado cuando usted habilita el debug y usted debe conocer sus peligros.

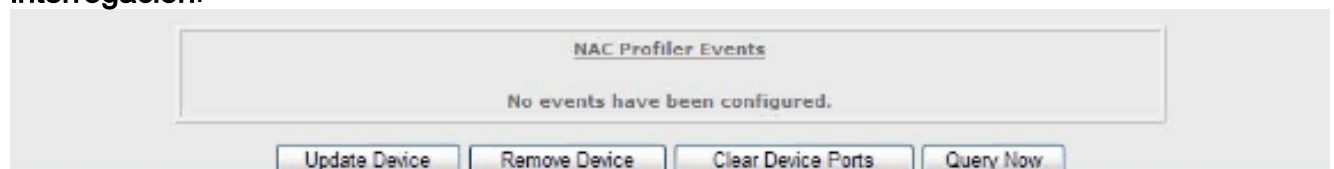
```
nac-3750-access#debug snmp packet  
nac-3750-access#debug snmp header
```

3. Verifique el colector tiene SNMP sondeado el Switch: Mire la columna más reciente de la exploración.

Table of Network Devices

Name	IP Address	System Description	Location	Contact	Type	Group	Last Scan
3560-access-switch	192.168.100.25	Cisco IOS Software, C3560 Software (C3560-ADVENTER/UCESK9 M), Version 12.2(25)S2E3, RELEASE SOFTWARE...			Router	Ungrouped	Fri Aug 1 2008 16:25:03

4. Haga el debug del SNMP otra vez en el Switch.
5. Del Profiler, elija la **configuración > los dispositivos de red**. Elija enumerar los **dispositivos de red** y después elegir el **dispositivo**.
6. Haga clic la **interrogación**.



7. Mire la salida de los debugs en el Switch para el colector al SNMP sondear el 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. Enchufe su teléfono del IP en el Switch o publique **entonces cerrado el comando no shut** en la interfaz:

```

15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down
15w4d: %ILPOWER-5-POWER_GRANTED: Interface Gil/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 state to up
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. Verifique el colector envía un nuevo pedido del desvío la dirección MAC recibida:

```

15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down
15w4d: %ILPOWER-5-POWER_GRANTED: Interface Gil/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 state to up
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

```

10. Verifique el Profiler recibió la nueva dirección MAC del teléfono del IP del colector: Elija la consola > la opinión del punto final/maneje los puntos finales > los puntos finales de la visualización por los puertos del dispositivo > ungrouped > tabla de dispositivos y después elija su Switch.

The screenshot shows the Cisco NAC Profiler interface. The top navigation bar includes 'Home', 'Configuration', 'Endpoint Console', and 'Utilities'. The 'Endpoint Console' tab is active. On the left, there is a sidebar with 'View/Manage Endpoints', 'Endpoint Directory', 'NAC Profiler Events', and 'Device Endpoint Views'. The main area displays a table titled 'Table of 3751\_L3\_005'. The table has columns for Port, Profile, MAC, IP Address, Link State, PORT, and VLAN. The table lists various endpoints, including Trunk Ports, Phones, Windows Laptops, and Printers, with their respective MAC and IP addresses, link states, and VLAN assignments.

Port	Profile	MAC	IP Address	Link State	PORT	VLAN
G1/0/1 (101-11)				Up		1
G1/0/2 (101-12)				Up	Force Auth (Auth)	121
G1/0/3 (101-13)	Phone	000F.74.06.06.00 (Cisco Systems)	192.168.172.58	Up	Force Auth (Auth)	121
G1/0/4 (101-14)	Phone	0007.50.66.09.07 (Cisco Systems, Inc.)	192.168.172.60	Up	Force Auth (Auth)	121
G1/0/5 (101-15)	Windows Laptop	000C.12.03.00.05 (Intel Corporation)	192.168.171.97	Down	Auth (Auth)	121
G1/0/6 (101-16)				Down	Force Auth (Auth)	120
G1/0/7 (101-17)	Printer xml	000D.0000.00.00.00 (Shenzhen Huaqun Company)	192.168.127.201	Up	Force Auth (Auth)	120
G1/0/8 (101-18)				Down	Force Auth (Auth)	120
G1/0/9 (101-19)				Down	Force Auth (Auth)	120
G1/0/10 (101-20)				Down	Force Auth (Auth)	120
G1/0/11 (101-21)				Down	Force Auth (Auth)	120
G1/0/12 (101-22)				Down	Force Auth (Auth)	120
G1/0/13 (101-23)				Down	Force Auth (Auth)	120
G1/0/14 (101-24)				Down	Force Auth (Auth)	120
G1/0/15 (101-25)				Down	Force Auth (Auth)	120

11. Verifique los trabajos del SPAN sobre el Switch y el colector está recibiendo el tráfico.

```

15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down
15w4d: %ILPOWER-5-POWER_GRANTED: Interface Gil/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 state
to up
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

```

Mire la salida en la pantalla. Si usted se refiere sobre la cantidad de salida, usted puede transmitir la salida a un archivo en el colector del NAC. Vea los página de man en Linux en cómo realizar esto.

12. Marque para ver si el tráfico del DHCP sobre el punto final del teléfono del IP se ha considerado a través del puerto SPAN y envió hasta el Profiler. Elija la **consola > la opinión del punto final/maneje los puntos finales > los puntos finales de la visualización por los puertos del dispositivo > ungrouped > tabla de dispositivos** y después elija su Switch. Entonces elija la **dirección MAC** de sus dispositivos. Haga clic los **datos de perfiles de la visión**.

The screenshot shows the Cisco NAC Profiler web interface. The top navigation bar includes 'Home', 'Configuration', 'Endpoint Console', 'Utilities', and 'Logout'. The main content area displays 'Summary information for 00:07:50:c6:82:27'. Below this, an 'Endpoint summary' box provides details:

- MAC Vendor: Cisco Systems, Inc.
- Latest IP address mapping: 192.168.122.60
- Current Location: 3750\_L3\_006(192.158.120.2) on port Gi1A/4(10184)
- Current Profile(s): IP Phone (60% certainty)
- Note: This endpoint is not 802.1X capable.

At the bottom of the summary box, there are five buttons: 'View Layer2 Trace', 'View MAC History', 'View Profile Data', 'View IP History', and 'Clear Endpoint'.

Usted debe ver la información de la clase del vendedor del DHCP de los dispositivos capturados del tráfico NetWatch/SPAN en el colector. Esta información puede venir del servidor DHCP o de la oferta de DHCP en el puerto SPAN de nuevo al cliente, que depende de su encaminamiento y entorno.

Table of Software Data for 00:07:50:c6:82:27

Protocol	Port	Server	Data	Last Updated
No profiling traffic was found				

Table of Traffic Data for 00:07:50:c6:82:27

IP Address	Protocol	Src Port	Dst Port	Created
No entries were found				

Table of Other Data for 00:07:50:c6:82:27

Data Type	Data	Last Updated
DHCP Host Name	SEP00750C68227	Mon Oct 20 2008 16:33:54
DHCP vendor Class	Cisco Systems, Inc. IP Phone CP-7960	Mon Oct 20 2008 16:33:54
DHCP Options List	53,61,12,60,50,55,255	Mon Oct 20 2008 16:33:54
DHCP Requested Options	1,66,6,3,15,150,35,255	Mon Oct 20 2008 16:33:54
DHCP Inform Requests		Mon Oct 20 2008 16:33:54
Network Stack Info	TTL: 64 Window: 1490(0) TCPOptionList: 2	2008-10-20 16:33:54.760157

13. Verifique el Netflow se está pasando del router remoto a la interfaz de administración del colector.

```
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
```

Hay cuatro transmisores superiores:

```
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
```

14. Verifique que el Profiler de los colectores reciba el Netflow. Elija su IP del MAC remoto o del punto final y mire los datos perfilados: Elija la consola > la opinión del punto final/maneje los puntos finales > los puntos finales de la visualización por los puertos del dispositivo > ungrouped > tabla de dispositivos y después elija su Switch. Entonces elija la dirección MAC de sus dispositivos. Haga clic los datos de perfiles de la visión. En la salida, usted ve el tráfico del destino a IP 192.168.70.50 y puerto destino 2000. Ésta es la dirección IP del Cisco CallManager y el puerto destino 2000 se utiliza para el tráfico de control del SCCP.



[View/Manage Endpoints](#)[Endpoint Directory](#)[NAC Profiler Events](#)[Other Endpoint Views](#)[\[Back\]](#) / [\[Refresh\]](#)

Table of Software Data for 00:0f:24:70:fb:63

Protocol	Port	Server	Data	Last Updated
No profiling traffic was found				

Table of Traffic Data for 00:0f:24:70:fb:63

IP Address	Protocol	Src Port	Dst Port	Created
192.168.70.50	6	0	2000	Tue Aug 12 2008 12:57:38
192.169.122.1	6	0	2000	Tue Aug 12 2008 12:57:35

Table of Other Data for 00:0f:24:70:fb:63

Data Type	Data	Last Updated
DHCP Vendor Class	Cisco Systems, Inc. IP Phone CP-7960G	Mon Oct 20 2008 17:50:38
DHCP Options List	53,61,12,60,55,255	Mon Oct 20 2008 17:50:38
DHCP Inform Requests		Mon Oct 20 2008 17:50:38
DHCP Host Name	SEP00F2470FB63	Mon Oct 20 2008 17:50:38
DHCP Requested Options	1,66,6,3,15,150,35,255	Mon Oct 20 2008 17:50:38
Network Stack Info	TTL: 64 Window: 1400(0) TCPOptionList: 2	2008-08-11 18:02:39.237118

## [Información Relacionada](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)