

Deploy NAC Profiler in an Existing Out-of-Band NAC

Document ID: 107703

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

- NAC Profiler Overview
- NAC Overview

Configure

- Configuration Guide Overview
- Network Diagram
- Configurations
 - Configure the NAC Profiler for the OOB Topology
 - Configure the NAC Collector
 - Configure the Access Switch to Send SNMP Traps to the NAC Collector
 - Configure the Access Switch on the Profiler to Gather SNMP Information
 - Configure the ETH3 Switchport of the NAC Collector on the Distribution Switches for

SPAN

Verify

[NetPro Discussion Forums – Featured Conversations](#)

Related Information

Introduction

This deployment guide describes how to implement the Cisco NAC Profiler Server and Cisco NAC Profiler Collectors (located on the Cisco NAC Appliance Clean Access Server) in a Out-of-Band (OOB) Campus deployment. This document describes how to best deploy the Cisco NAC Profiler in an existing OOB High Availability NAC deployment. It is intended to help you understand the basic features and topology of a Cisco NAC Profiler solution integrated with the Cisco NAC Appliance. It also helps you understand how endpoint information about all NAC-less devices is sent from the Collectors to the Profiler Server. The goal of the solution is to profile the endpoints and add them to the Device Filter list of the Cisco NAC Appliance Clean Access Manager (CAM) in order to apply the appropriate policy.

Prerequisites

Requirements

You must first configure your Cisco NAC Manager, Cisco NAC Server, and Cisco NAC Profiler in accordance with 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 (192.168.96.10 HA Service IP)

- NAC Server (192.168.97.10 HA Service IP)
- NAC Profiler (192.168.96.21)
- 3560 Access Switch (192.168.100.35)
- 3750 Distribution Switch (192.168.97.1)

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.

Background Information

NAC Profiler Overview

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

NAC Overview

The Cisco Network Admission Control (NAC) Appliance (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, the Cisco NAC Appliance is a complete solution to control and secure networks. As the central access management point for your network, the Cisco NAC Appliance lets you implement security, access, and compliance policies in one place instead of having to propagate the policies throughout the network on many devices.

Configure

Configuration Guide Overview

In this section, you are presented with the information to configure the features described in this document.

The diagram in Figure 1 shows a basic Layer 2 Campus deployment with High Availability (HA) NAC Servers across distribution switches. The Profiler Server and NAC Manager can sit on the same management network and send and receive information from the NAC Servers and Collectors. There are several ways that the Cisco NAC Profiler can discover non-NAC remote endpoints, and this guide describes the most common and recommended methods. This configuration guide describes how to accomplish these:

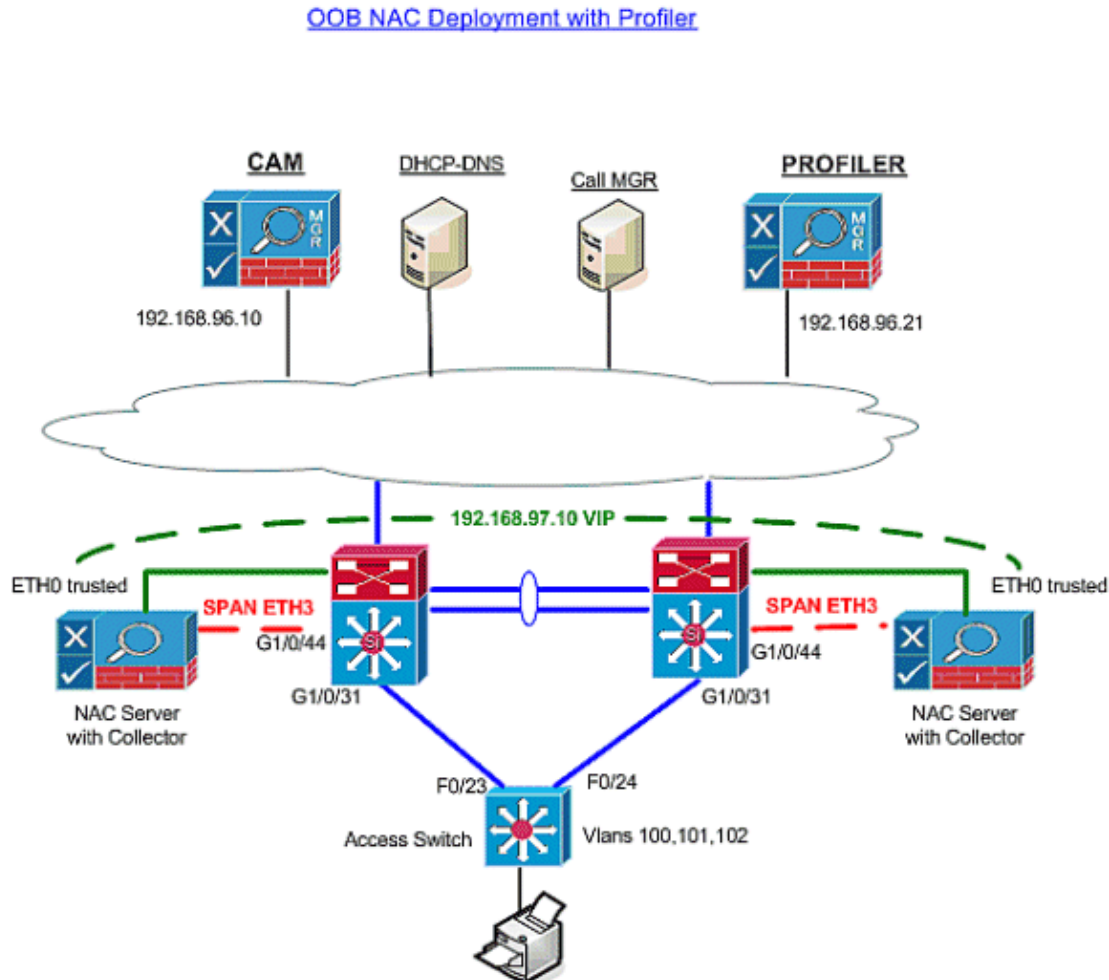
- Add SNMP communication to and from the access switch to the NAC Collectors.
- Configure a SPAN port on the distribution switches to capture all traffic from the access layer devices, specifically DHCP traffic from the endpoints, since we are most interested in the DHCP vendor class information attribute about endpoints.
- Configure the Cisco NAC Profiler Server and Collector communication accordingly to receive all the information gathered by the Collectors.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

Figure 1: OOB Cisco NAC Appliance Deployment with Cisco NAC Profiler



Configurations

This document uses these configurations to configure the NAC Profiler and Collectors in an Out-of-Band solution:

- Configure the NAC Profiler for the OOB Topology
- Configure the NAC Collector
- Configure the Access Switch to Send SNMP Traps to the NAC Collector
- Configure the Access Switch on the Profiler to Gather SNMP Information
- Configure the ETH3 Switchport of the NAC Collector on the Distribution Switches for SPAN

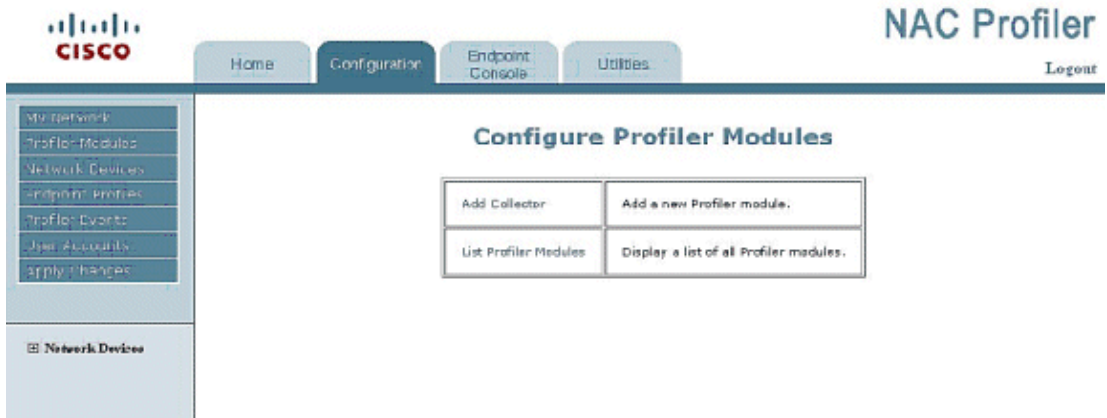
Configure the NAC Profiler for the OOB Topology

- NAC Servers need to be configured through the normal NAC HA setup.
- The Collector utilizes the virtual IP address of the NAC Server to communicate with the Profiler.

- The NAC Collector HA pair are added as a single entry in the Profiler and communicate to the virtual IP address of the NAC SERVER.

1. Add a new Collector to the Profiler.

Go to **Configuration > NAC Profiler Modules > Add Collector**.

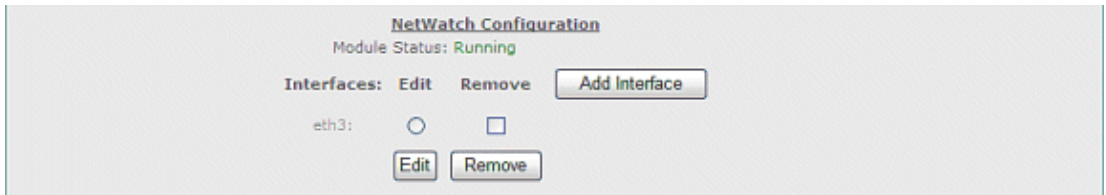


2. Add a new Collector name for the NAC Server HA Pair. This can be anything you want but must match the Collector configuration.

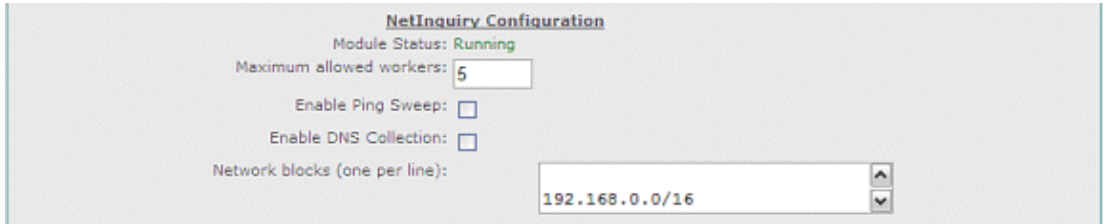
- ◆ Collector name: **CAS-OOB-Pair1**
- ◆ IP address: **192.168.97.10** (virtual address of the NAC Server)
- ◆ Connection: Leave it as **NONE** for now

3. Configure your Collector Service Modules. Leave **NetMap** and **NetTrap** alone (configuration by default is not necessary).

4. Add a **NetWatch interface (ETH3)** that is connected to a SPAN port on the distribution switch.

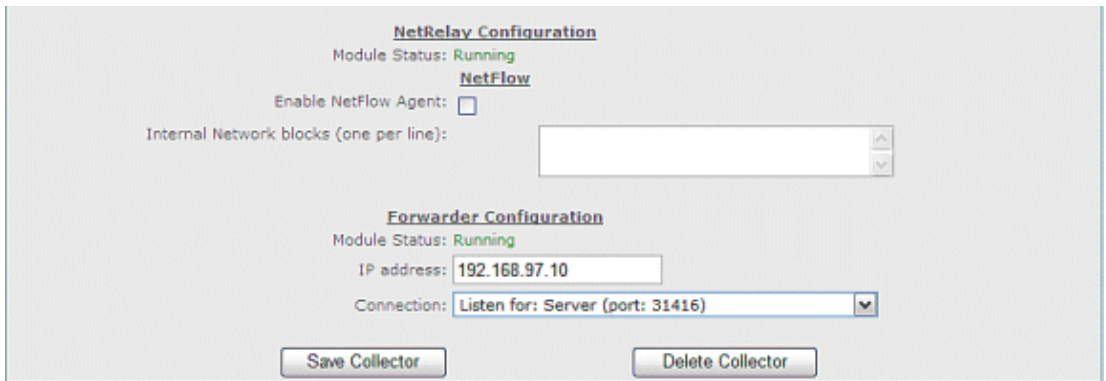


5. Add a **subnet Block** for the NetInquiry module to listen for interesting traffic that comes from the access networks. Be specific on the networks and do not tax the NAC server unnecessarily. In this lab setup, it can be the entire 192.168.0.0 private space.



Leave **Ping Sweep** and **DNS Collection** disabled.

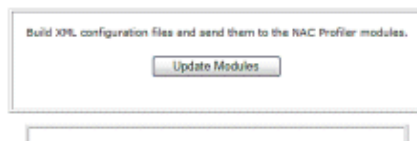
6. Configure the Forwarder as listen on IP address 192.168.97.10 (VIP) and TCP port 31416. This allows the Collector to act as a server and listen for a connection from the Profiler to the specific port.
7. Leave **NetFlow** disabled in the NetWatch SPAN session. Make sure you click the **Save Collector** button to save the configuration.



8. Go to **Configuration tab > Apply Changes > Update Modules.**



Update NAC Profiler Modules



Configure the NAC Collector

This configuration needs to be run exactly as is on both devices.

1. SSH to the Collector and login as **root**.
2. Type **service collector config** and run through the configuration script to setup the NAC Collector portion.

```
[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) [NAC Server1]: NAC SERVER-OOB-Pa
Network configuration to connect to a NAC Profiler Server
Connection type (server/client) [server]:
Listen on IP [192.168.97.10]:
```

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 independent NPS and the virtual IP to ensure proper connectivity in the NAC Server 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 Pr
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 Profi
Enter the IP address(es) of the NAC Profiler.
(Finish by typing 'done') [done]: 192.168.96.22 (Real IP of NAC Profiler2)
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 NAC SERVER-OOB-Pair1-fw
-- Configured NAC SERVER-OOB-Pair1-nm
-- Configured NAC SERVER-OOB-Pair1-nt
-- Configured NAC SERVER-OOB-Pair1-nw
-- Configured NAC SERVER-OOB-Pair1-ni
-- Configured NAC SERVER-OOB-Pair1-nr
```

The NAC Collector is configured.

3. Start the Collector Services.

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

Configure the Access Switch to Send SNMP Traps to the NAC Collector

This configuration allows the Profiler to dynamically receive all new devices that connect to a switchport throughout the network.

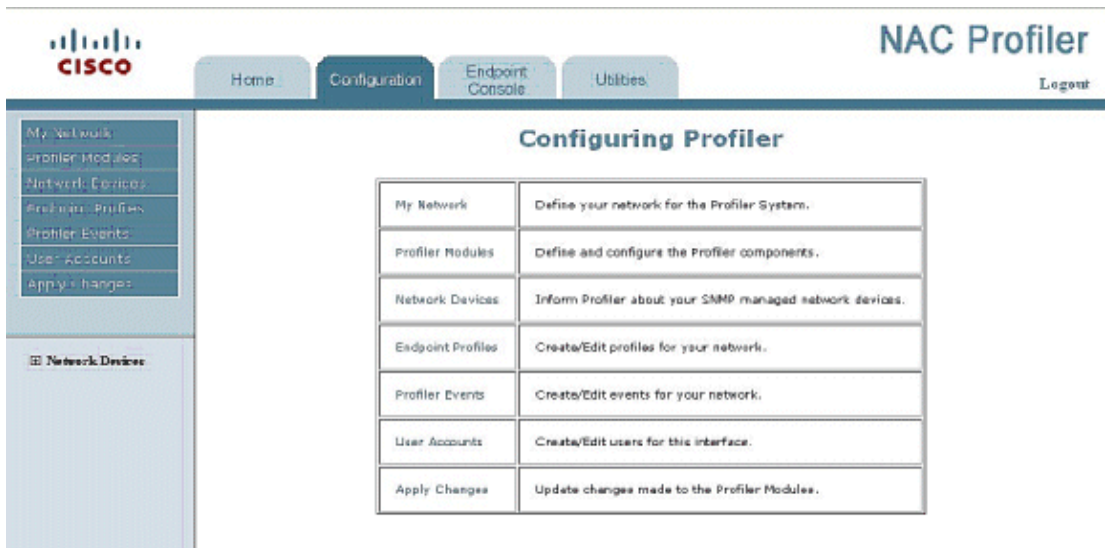
Console/Telnet into the switch (nac-3560-access#).

```
snmp-server community cleanaccess RW
## Allows read-write access from the NAC Manager
snmp-server community profiler RO
## Allows read only access from Collectors
snmp-server enable traps mac-notification
## Enables new-mac notification traps
snmp-server host 192.168.96.10 version 2c cleanaccess
## Traps sent to NAC Manager IP address
snmp-server host 192.168.97.10 version 1 profiler
## Allow traps to the NAC Collectors Management IP addresss
```

Configure the Access Switch on the Profiler to Gather SNMP Information

Follow these instructions to configure the access switch on the Profiler to gather SNMP information.

1. Go to the Profiler GUI: **Configuration > Network Devices > Add Device.**



2. Add the host name and management IP address of the switch.
3. 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 the Profiler.
4. Click **Add Device** and **Apply Changes**. Update the modules from the left-hand pane of the GUI.

Configure the ETH3 Switchport of the NAC Collector on the Distribution Switches for SPAN

Note: This allows the NetWatch Module 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 1GB/sec. Source the interfaces or VLANs of the switch depending 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, add a NAC Collector on or near the DHCP servers on your network.

Configure a monitor session on the distribution switch.

```
monitor session 1 source interface Gi1/0/1 - 43 , Gi1/0/46 - 48
monitor session 1 source interface Po10
monitor session 1 destination interface Gi1/0/44
```

Verify

Use this section to confirm that your configuration works properly.

- Make sure that the Profiler and Collector communicate and are running. If they are not, you do not see any information about the devices in your network. If there are issues, do not proceed until all the Collector Modules and the Server are running.

On the Profiler, go to **Configuration > NAC Profiler Modules > List NAC Profiler Modules**.

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

Server
Server (v2.1.8) [Running]

- Verify that the access switch can send new-MAC notification traps to the Collector.

Note: Be careful when you enable debug, and know its dangers.

```
nac-3560-access# debug snmp packet
nac-3560-access# debug snmp header
```

```
SNMP packet debugging is on
SNMP packet debugging is on
*Mar 30 22:45:12: SNMP: Queuing packet to 192.168.97.10
*Mar 30 22:45:12:
Outgoing SNMP packet
*Mar 30 22:45:12: v1 packet
*Mar 30 22:45:12: community string: profiler
*Mar 30 22:45:12: SNMP: V1 Trap, ent cmnMIBNotificationPrefix,
      addr 192.168.100.35, gentrap 6, spectrap 1
cmnHistMacChangedMsg.0 =
01 00 65 00 04 23 B3 82 60 00 04 00
cmnHistTimestamp.0 = 258751290
```

- Verify that the Profiler received the new MAC address from the Collector.

Go to **Endpoint Console > View/Manage Endpoints > Display Endpoints by Device Ports > Ungrouped > Table of Devices > (Choose the switch)**.

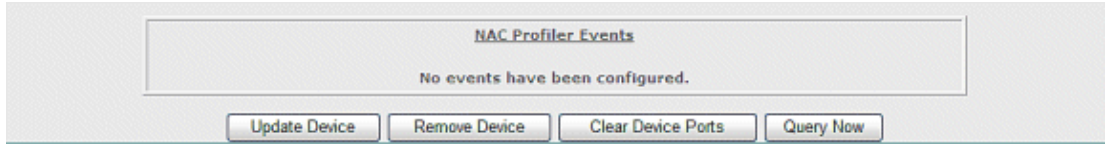
Port	Profile	MAC	IP Address	Link State	802.1X	VLAN
Fo0/1 (10001)				Down		100
Fo0/2 (10002)	Windows Users	00:04:23:b3:82:60 (Intel Corporation)	192.168.100.23	Up		101
Fo0/3 (10003)				Down		101
Fo0/4 (10004)				Down		101

- Verify that the Collector has SNMP-pollled the switch.

1. Look at the **Last Scan** column. This verifies that the Collector scanned the switch every 60 minutes by default.

Name	IP Address	System Description	Location	Contact	Type	Group	Last Scan
3560-access-switch	192.168.100.35	Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(25)SEE3, RELEASE SOFTWARE...			Router	Ungrouped	Fri Aug 1 2008 16:21:08

2. **Debug SNMP** again on the switch CLI.
3. From the Profiler GUI, go to **Configuration > Network Devices > List Network Devices > (Choose the device)**.
4. Click **Query Now**.



5. 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
```

6. Verify that SPAN works on the switch and the Collector can receive traffic.

- a. SSH to the NAC Profiler.
- b. 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)
16:54:36.432223 IP cas2.nacelab2.cisco.com.9308 >
elab2-dns-dhcp.nacelab2.cisco.com.domain:
48871+ PTR? 68.39.168.192.in-addr.arpa. (44)
16:54:36.432468 IP cas2.nacelab2.cisco.com.9308 >
elab2-dns-dhcp.nacelab2.cisco.com.domain:
58368+ PTR? 69.39.168.192.in-addr.arpa. (44)
16:54:36.432472 IP cas2.nacelab2.cisco.com.9308 >
elab2-dns-dhcp.nacelab2.cisco.com.domain:
58368+ PTR? 69.39.168.192.in-addr.arpa. (44)
16:54:36.432842 IP cas2.nacelab2.cisco.com.9308 >
elab2-dns-dhcp.nacelab2.cisco.com.domain:
1650+ PTR? 70.39.168.192.in-addr.arpa. (44)
16:54:36.432846 IP cas2.nacelab2.cisco.com.9308 >
elab2-dns-dhcp.nacelab2.cisco.com.domain:
1650+ PTR? 70.39.168.192.in-addr.arpa. (44)
```

- c. 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. Refer to the main pages in Linux.

7. Check whether you can see DHCP traffic about the endpoints on your switch.

Go to **Profiler GUI > Endpoint Console > View/Manage Endpoints**. Click a profile; click a device, and click the endpoint data.

You see DHCP Vendor Class information of the device captured from the NetWatch/SPAN traffic on the Collector:

Data Type	Data	Last Updated
DHCP Host Name	cca-xp2	Fri Aug 1 2008 16:54:40
DHCP Vendor Class	MSFT 5.0	Fri Aug 1 2008 16:54:40
DHCP Options List	53,61,12,81,60,55,255	Fri Aug 1 2008 16:54:40
DHCP Inform Requests		Fri Aug 1 2008 16:54:40
DHCP Requested Options	1,15,3,6,44,46,47,31,33,249,43,255	Fri Aug 1 2008 16:54:40
Network Stack Info	TTL: 128 Window: 65535(0) TCPOptionList: 2,1,1,4	2008-08-01 16:58:17.252152

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Technical Support & Documentation – Cisco Systems](#)
- [Cisco NAC Appliance \(Clean Access\)](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 02, 2008

Document ID: 107703
