CHAPTER 7

Configuring Collector Modules

This chapter includes the following topics:

Overview

The Cisco NAC Profiler Collector modules, deployed on NAC Server NAC Appliances in Cisco NAC Profiler deployment are essentially the “eyes and ears” of the system.

Note The Collector service must be enabled & configured as described in prior to adding the Collector to the system configuration and completing configuration of the component modules via the Cisco NAC Profiler UI.

The five component modules running on the Collector(s): NetInquiry, NetWatch, NetMap, NetTrap and NetRelay collect endpoint information for the system that is processed into the database and analyzed and presented by the Cisco NAC Profiler Server. The Profiler Server also updates the Cisco NAC Appliance CAM with information about non-NAC endpoints based on the database it maintains using information from the Collectors deployed throughout the system and compiled by the component modules. The component modules each utilize different technologies and techniques for endpoint data collection and analysis, providing a full complement of Endpoint Profiling and Behavior Monitoring capabilities for the system.

Table 7-1 lists the purpose and functionality of each of the five Collector component modules which can be utilized by each Cisco NAC Profiler Collector as required by the implementation:

Table 7-1 Collector Modules Description

Module	Description	Endpoint Data Collection Methodology
NetMap	Collector component module that queries network devices via SNMP for: • System information • Interface information • Bridge information • 802.1X information (PAE MIB) • Routing/IP information • CDP MIB Information This information is used to Build and maintain a model of the network topology and endpoint discovery.	SNMP communications with Network Devices (switches and routers) LDAP Query of Active Directory Servers
NetTrap	Collector component module that receives selected traps from network devices to assist NetMap in maintaining the model of the network topology. Traps are used to detect endpoints joining or leaving the network and trigger a NetMap poll of the device sending the trap to determine what changed.	SNMP Traps from edge switches
NetWatch	The passive network analyzer collector component module. Collects information about endpoints using network traffic received at one or more of the interfaces on the appliance the NetWatch module instance is running on.	Traffic analysis via redirection (SPAN, mirror port) to Collector monitor port

Module	Description	Endpoint Data Collection Methodology
NetInquiry	Active profiling Collector component module that can be used to collect information about endpoints using active techniques: TCP Open ports, web & SMTP banners, and DNS name information.	Network communication initiated/analyzed by Collector
NetRelay	Receives exported data from other systems such as NetFlow and RADIUS preparing it for use in Endpoint Profiling and Identity Monitoring. In the case of NetFlow, NetRelay can be configured to process NetFlow XDRs for matches to Traffic Rules in enabled profiles. NetRelay can be configured to receive RADIUS accounting data from RADIUS clients (switches running 802.1X/MAB) to gather information about authenticated endpoints.	Analysis of NetFlow XDRs forwarded by NetFlow Collectors/Aggregators (e.g., routers). Analysis of RADIUS accounting records forwarded by RADIUS clients.

Determining the Required Collector Components per Collector

The component modules utilized on the Collector(s) employed in each NAC Profiler system is implementation-dependent as well as environment-dependent. Based on the characteristics of the environment such as number of endpoint devices, whether or not the network is on a single campus or dispersed across multiple campuses, and how the Endpoint Profiling and Identity Monitoring functions will be implemented determines how the Collector(s) deployed in the system will be implemented. For example, not all of the component modules in Figure 7-2 on page 7-8 will be utilized on a given Collector, or used at all for that matter in every deployment. For example, in environments that do not have NetFlow collectors running in the network, the NetRelay module would not be utilized on the NAC Profiler Collectors for the processing of NetFlow data.

The decision on what Collector component modules are configured/enabled on each Collector is driven primarily by the rule types used in the endpoint profiles in the system configuration and the endpoint data that is accessible by a given Collector. For example, is the Collector placed in the network in a location where traffic between the endpoints and a service on the network is aggregated so that the traffic can easily be redirected to a monitor port on the Collector for NetWatch analysis? Such a Collector would then likely have NetWatch enabled on a monitor port the aggregated network traffic could be redirected to. The following table, introduced in Chapter 1, “Introduction to Cisco NAC Profiler”, is presented again for the purposes of reviewing the attributes used by the NAC Profiler system for profiling endpoints, along with the Collector component module (or modules for some attributes) that can collect

that endpoint data. Using the two tables in this section to review the function of each collector component, what data sources it uses along with the attributes used for endpoint profiling can facilitate planning of what Collector components will be used on each Collector to be deployed in the system.

Table 7-2 Endpoint Identity Attributes Used by Cisco NAC Profiler

Endpoint Attribute	Description	Collector Component(s)
MAC Address/MAC Vendor	The entire MAC address of an endpoint, or the manufacturer that registered the OUI.	NetMap (SNMP) NetWatch (ARP/DHCP)
IP Address	Full host address (or subnet) being used by the endpoint.	NetMap (SNMP) NetWatch (ARP/DHCP)
Open TCP port	Indication that an endpoint is accepting TCP connections on a specified TCP port via analysis traffic	NetWatch NetInquiry
Network Traffic	Communicated with other host(s) on specified UDP/TCP port number	NetWatch NetRelay
Web User Agent	Displayed a specific web user agent	NetWatch
Web URL	Visited a specified URL via HTTP	NetWatch
Server Banner	Displayed a specified Web or SMTP server banner	NetWatch NetInquiry
Stack Information	Displayed specified network stack parameters: TTL, window size, TCP options list	NetWatch
DHCP Vendor Class	Displayed a specific DHCP Vendor Class Identifier in DHCP request	NetWatch
DHCP Host Name	Displayed a specific host name in DHCP request	NetWatch
DHCP Requested Options	Requested specified options in DHCP request (option 55)	NetWatch
DHCP Options	Full list of DHCP options supported by the DHCP client as specified in the DHCP request	NetWatch
DNS Name	The name the endpoint's IP address resolves to in DNS	NetInquiry
RADIUS Accounting Information	The RADIUS username of an endpoint that has successfully completed RADIUS authentication.	NetRelay

Table 7-2 Endpoint Identity Attributes Used by Cisco NAC Profiler

Endpoint Attribute	Description	Collector Component(s)
Active Directory Attributes	Information about the endpoint maintained in Active Directory: • Domain membership • Active Directory Computer (Common) Name • Active Directory Computer Information – Computer OS – OS Version – OS Service Pack	NetMap
CDP Information	Information in the CDP message that identifies the device to its upstream neighbor.	NetMap
SNMP System Description	Text string contained within SNMP system description for devices polled by NetMap.	

Note As described in Chapter 7, "Configuring Collector Modules", Cisco NAC Profiler systems require that the Server module for the system be configured with the necessary Network Connections to enable inter-module communications. If you have not configured the Server module Network Connections, refer to Chapter 6, "Cisco NAC Profiler Server Configuration" before proceeding.

As discussed in Chapter 5, "Configuring the Cisco NAC Profiler for the Target Environment," whenever changes are made to module configuration parameters, an Apply Changes and system restart must be performed to commit the changes to Cisco NAC Profiler running configuration. Upon completion of editing or adding a Collector module (or modules) to the system configuration, perform an Apply Changes to update the system configuration.

Changes made to Cisco NAC Profiler system configuration are saved to the running configuration by clicking the Update Modules button on the Apply Changes page. The Apply Changes page is accessed by selecting the Apply Changes from the global navigation pane in the left hand margin on all pages of the Configuration Tab, or by selecting Apply Changes from the table on the main Configuration page.

Adding a Collector to the System Configuration

Each of the Profiler Collectors to be deployed in the NAC Profiler system must be added manually to the system configuration using the procedure outlined in this section, and the required component modules configured according to the instructions outlined in the latter sections of this chapter. Adding a new Collector is a two-step process:

1. Adding the new Collector to the configuration according to the steps in this section,
2. Configuring the Forwarder and the desired component modules on the newly added Collector as required.The Collector component modules configured on a given Collector is dependent upon which endpoint data collection methods will be employed by that Collector. See Configuration of Collector Component Modules, page 7-11.

Tip Recall that Profiler Collector HA pairs deployed on NAC Server HA pairs are treated as a single Collector instance using the Collector name assigned to the Collector service running on both nodes of the NAC Server pair. The procedure for adding a Collector to the system configuration is the same then for standalone Collectors and HA Collector pairs.

Follow the steps below to add a Collector to the Cisco NAC Profiler system configuration:

Step 1 Navigate to the Configuration Tab and select the Modules link from the secondary menu. This displays the Table of NAC Profiler System. Select the Add Collector link in the upper right hand corner to add a new Collector to the NAC Profiler system configuration via the Add Collector form shown in Figure 7-1.

Figure 7-1 Add Collector Form

The Add Collector form is used to create a new Collector instance in the system configuration. Both the fields in the form are required, and are described in detail below. Enter this information to add the new Collector to the Profiler system configuration.

Step 2 Enter Collector name for this Collector.

Each NAC Profiler Collector in the system was configured with a name during the startup and initial configuration performed in accordance with the procedures outlined in Chapter 4, "Installation and Initial Configuration". By default, standalone NAC Profiler servers use the NAC Server appliance hostname, or an alternate name assigned at startup.

For Collector HA Pairs, the Collector name must be configured to be the same on both nodes.

Tip Each Collector name must be unique, trying to add a Collector to the system configuration using a Collector name already saved to the system configuration will result in an error.

Tip The Collector name entered in this field when adding a Collector **must** match the Collector name configured at startup **exactly** (e.g., is case sensitive) in order for the Profiler Server module to establish communications with the Forwarder on the Collector and process the collected endpoint data into the database. An exact match (e.g., case sensitive) is necessary for reporting status of the component modules running on the Collector. If the Collector name is not known, it can be verified from the NAC Server command line using the `service collector verify` command which will show the current Collector configuration.

Note As outlined in Chapter 4, "Installation and Initial Configuration", the Collector name must be no greater than 24 characters in length.

Step 3 Enter the Collector IP Address.

For standalone (non-HA) Collectors, enter the host IP address of the management interface (eth0) of the NAC Server appliance hosting the Collector.

For Collector HA pairs, the VIP of the NAC Server pair should be entered.

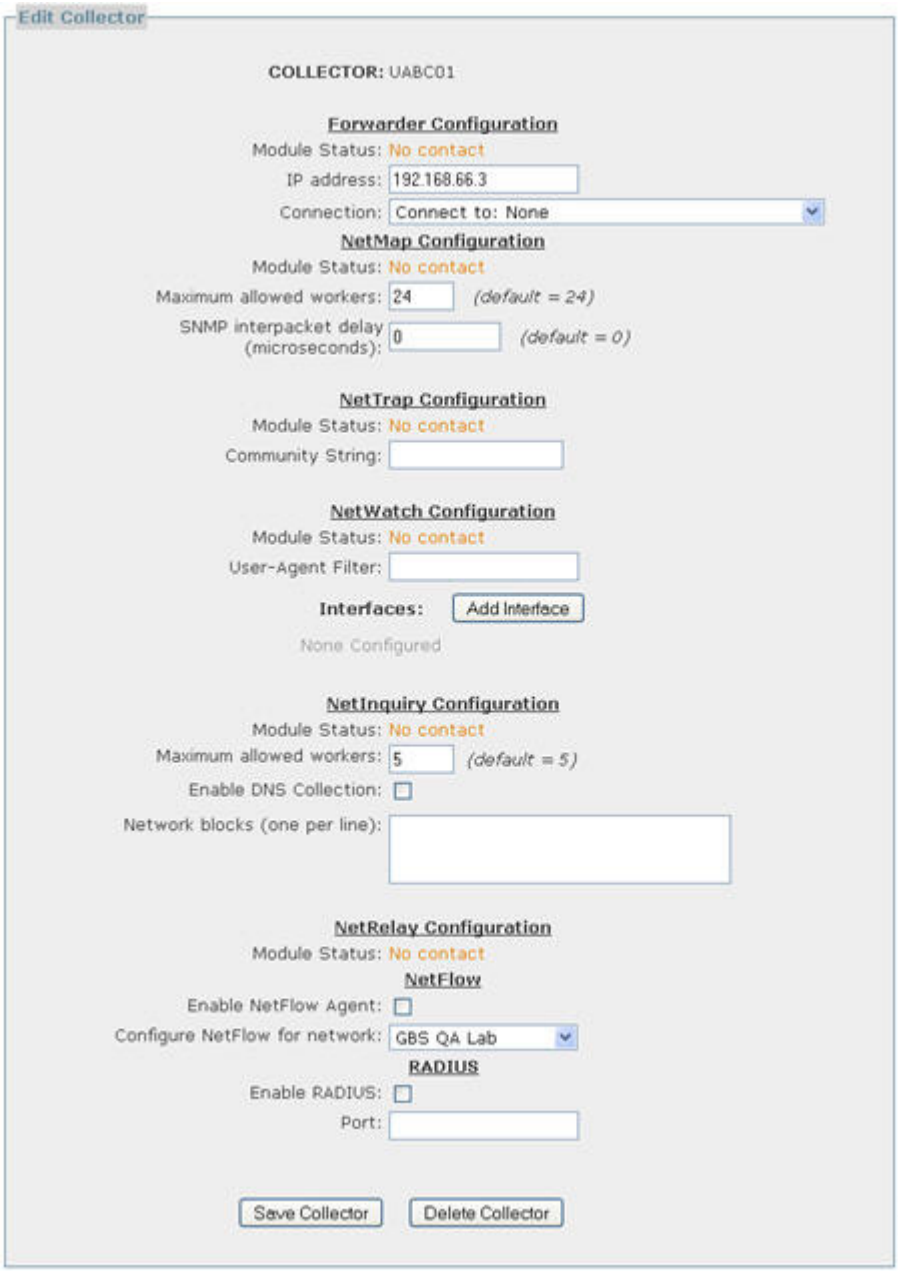
Step 4 Select the Add Collector button at the bottom of the form to add the Collector to the system configuration.

This action adds the Collector and displays the Edit Collector form shown in the next figure (Figure 7-2 on page 7-8) that enables the configuration of the Forwarder and desired Collector component modules on this NAC Profiler Collector.

Configuration of Profiler Collectors

The Edit Collector form illustrated in Figure 7-2 is displayed automatically upon successfully adding a Collector instance to the system configuration as described in the previous section, or when a Collector name link is selected from the Profiler Modules table on the Configuration Tab.

Figure 7-2 Edit Collector Form



Configuration of the Collector Component Modules is outlined in the next section.

Verify the Forwarder Configuration of the Collector

Immediately upon adding any Collector service to the system configuration, the configuration of the Forwarder module should be verified for consistency with the startup configuration of the Collector service completed upon NAC Profiler system startup completed as outlined in Chapter 4, "Installation and Initial Configuration". As each Collector service is started up, several parameters determining how that Collector communicates with the Profiler Server running the Server module for the system are configured. Prior to proceeding with the configuration of the other Collector component modules, it is important to verify that the Forwarder configuration for the Collector is correct.

Upon the next Apply Changes -> Update Modules, the Server module creates new Forwarder configuration file(s) based upon what is set in the GUI for the remote Collector(s) in the system. The configuration file(s) are sent down to the remote Collector(s) and the Collector(s) restart based on the new configuration sent down by the Server.

Figure 7-3 shows the Forwarder configuration for a Collector which is the first section of Edit Collector form.

Figure 7-3 Forwarder Configuration

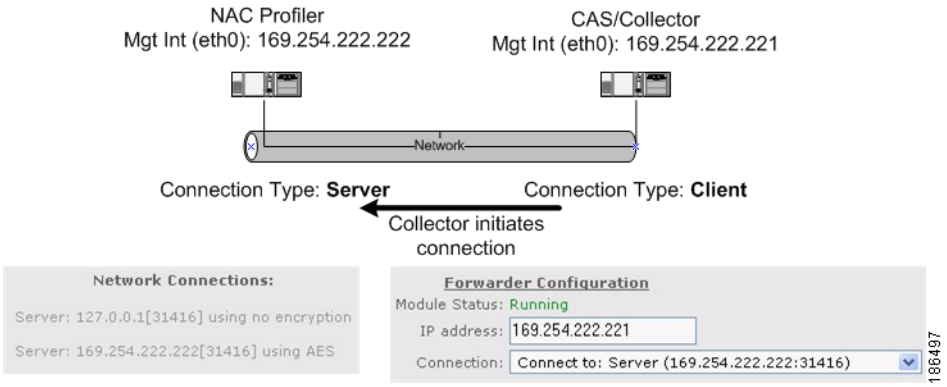
The Forwarder on each Collector is configured to communicate with the Server module on the NAC Profiler Server in one of two ways as outlined several times previously:

- As a Client —initiating connection back to the Server module
- As a Server—listening for connection initiated by the Server module

Note Collectors implemented as a HA pair on a NAC Server HA pair must use the Server Connection Type, and the Profiler Server configuration must have had a Network Connection of Type Client added to the Server configuration so that it initiates the connection to the Collector pair VIP. The configuration of the NAC Profiler Server to include this Network Connection should be performed prior to adding Collector HA pairs to the configuration

The following figures depict these two options for Collector configuration. They include excerpts from the Network Connections section of the Server module configuration (Configure Server form - see Chapter 6, "Cisco NAC Profiler Server Configuration"), as well as the Forwarder configuration section of the Edit Collector form (required to support the two network connection options for communications between the NAC Profiler Server and a Collector.

Figure 7-4 Collector Configured as Client - Standalone NAC Server



As shown in Figure 7-4 above, standalone Collectors (only) configured with Network Connections of type Client, the Forwarder configuration for the Collector should specify the IP address of the management interface (eth0) of the Collector service (169.254.222.221 in the example). The Connection parameter in the Forwarder configuration should specify that this Forwarder is to initiate the connection to the Server (169.254.222.222 in the example). In the Network Connections of the Server module of this system, it can be seen that a Server connection has been configured on the eth0 interface of the NAC Profiler Server. This configures the Server to listen for connections on the specified port (31416) for Forwarders on standalone Collectors connecting back to the Server.

Figure 7-5 Collector Configured as Server - Collectors on HA NAC Server Pairs

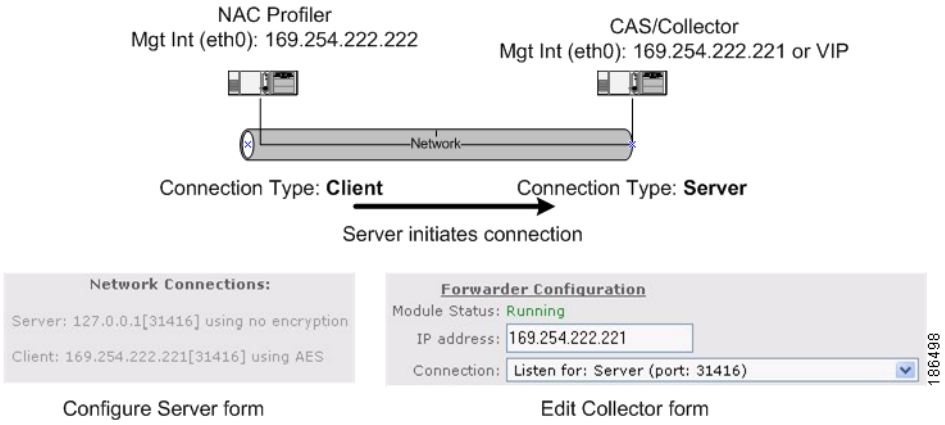


Figure 7-5 illustrates the other possible Forwarder configuration. In this case the Forwarder is configured to listen for a connection initiated by the Server module, the configuration which must be used for Collector HA pairs running on NAC Server HA pairs, and may be used in rare cases for standalone Collectors that maybe deployed beyond a firewall.

In this case, The IP address in the Forwarder Configuration is the management interface (eth0) IP of the standalone NAC Server appliance or NAC Server HA pair VIP (e.g. HA NAC Server/Collector pair 169.254.222.221 in Figure 7-5). The primary difference in the configuration of Collectors as Servers is the Connection specified in the Forwarder Configuration. Note that the **"Listen for: Server"** option has been selected from the Connection drop-down menu in the Forwarder configuration. In addition, the Network Connections section of the Server module configuration includes a Client connection that specifies that the Server should connect to the Forwarder running on this Remote Collection appliance.

Note Absence of the "Listen for: Server" choice from the Connection drop-down list of the Forwarder Configuration indicates the Network Connection of type Client was not configured in the Profiler Server configuration required to connect to a Collector via this method. Review the section in Chapter 6, "Cisco NAC Profiler Server Configuration" regarding configuring Network Connections for Servers to support communications with Collectors configured as Servers, add the Client Network Connection to the Server configuration, then edit the Collector configuration.

Once the Forwarder configuration is verified, each of the component modules that are needed on the Collector being added to the system configuration should be configured with the desired operating parameters. Again, not all the collector modules listed in Figure 7-2 will be configured/used on every Cisco NAC Profiler Collector. The form presented in the interface after the new Collector is added enables the configuration of the desired component modules that will be utilized on the new Collector.

For each of the component modules required on the Collector, complete the procedures outlined below to configure/enable it.

Changes made to Cisco NAC Profiler configuration are saved to the running configuration by clicking the Update Modules button on the Apply Changes page. The Apply Changes page is accessed by navigating to the Configuration Tab, and selecting Apply Changes from the secondary menu.

Configuration of Collector Component Modules

Once the Forwarder configuration is verified, each of the component modules that are needed on the Collector being added to the system configuration should be configured with the desired operating parameters. Again, not all the collector modules listed in Table 7-1 on page 7-2, will be configured/used on every Collector.

The Edit Collector form enables the viewing and editing of the configuration of the desired component modules that will be utilized on a Collector, and allows edits to be made to the configuration of a running Collector at any time.

The remainder of this chapter contains an overview of the functionality of each of the Collector component modules which collect endpoint data, along with detailed instructions for configuration/enablement. For each Collector, determine which component modules will be enabled and refer to the applicable sections below to configure accordingly:

- Configure NetMap Collector Module, page 7-12
- Configure NetTrap Collector Module, page 7-14
- Configure NetWatch Collector Module, page 7-16
- Configure NetInquiry Collector Module, page 7-21
- Configure NetRelay Collector Module, page 7-24

Configure NetMap Collector Module

NetMap Collector Module Overview

NetMap is the Collector component module that provides the network topology collection function. NetMap communicates with the network devices added to the system configuration at regular intervals as specified in the Server module configuration (Chapter 6, "Cisco NAC Profiler Server Configuration") using SNMP. The NetMap component module collects information about the network topology and endpoint landscape to construct a model of the network used in the Endpoint Profiling process by the NAC Profiler System.

As of version 3.1, NetMap will as an option make LDAP queries to designated Microsoft Active Directory Servers to gather information about endpoints that are members of the Domain. As described in Chapter 8, "Network Devices", Active Directory servers within an enterprise can be added to the NAC Profiler system configuration. Each AD Server added to the configuration will be assigned a NetMap module that will be responsible for querying it via LDAP to collect the endpoint data. This query is performed every 10 minutes by default.

The NetMap component module is enabled by default on all Collectors and in the majority of cases requires no additional configuration. Upon adding network devices (switches, routers and AD Servers) to the NAC Profiler configuration, NetMap modules designated to poll/query will begin regular polling/queries of the network devices assigned to immediately after an Apply Changes is executed.

Note Each network device in the NAC Profiler configuration has a NetMap module in the system designated to poll it. This designation is made either in the individual device configuration, or by the device group configuration via the 'Select Collector Mapping Module' parameter. This parameter will default as a device or group is added to a value of "default" which means the first NetMap module in the drop-down list will be selected as the polling (mapping) module for devices/groups with the value of this parameter left at default. If the NetMap module for a given Collector is not assigned any network devices to poll, it will be effectively disabled on that Collector.

NetMap uses SNMP Get, GetNext and GetBulk (when available) requests to query the SNMP agents running on the network infrastructure devices to gather specific Management Information Base (MIB) objects about their status based on device type (Layer 2 or Layer 3). By default, NetMap queries Layer 2 devices every 60 minutes and Layer 3 devices every 30 minutes. The polling intervals are configurable and set system-wide in the Server module configuration. (Chapter 6, "Cisco NAC Profiler Server Configuration")

In addition to polling each network device for all MIB data at a regular interval, NetMap may also be commanded to poll port-specific information when the NAC Profiler system is notified that an endpoint has joined or left the network via SNMP traps sent by devices at the network edge, switches typically. The NetTrap component module described in the next section, processes SNMP traps from edge devices in the NAC Profiler configuration to track the movement of endpoints in near real time.

Upon receipt and verification of a link state (link up, link down) or MAC notification trap, NetTrap will notify the NAC Profiler Server that a change has occurred on the network edge (endpoint joined or left a network port). If the trapping device is in the NAC Profiler configuration, the NetMap component module assigned to poll the device that sent the trap will be commanded by the Server module to initiate a poll of the device's port information to determine the change to the endpoint topology that resulted in the trap being sent by the network device. The information gathered by NetMap is processed by the Server accordingly to update the network topology, noting the endpoint joining or leaving a port. Note

that NetMap SNMP polling of network devices resulting from a trap is localized to the port specified in the trap. This is unlike the regular polling that occurs at the frequency specified for each device type (L2 and L3) which gathers all SNMP information from the device used by the NAC Profiler system.

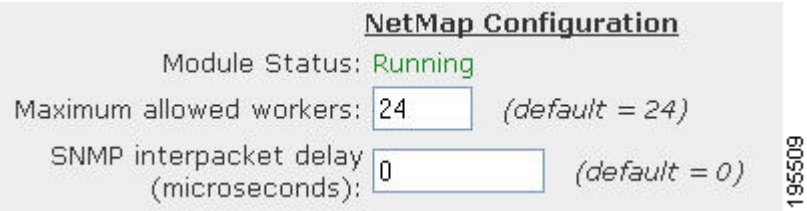
Edit NetMap Collector Module

As a Collector is added to the system configuration as described above use the following procedure to change any of the configurable parameters of the NetMap component module running on that Collector.

Tip In most cases the default values of these parameters are sufficient, and no additional configuration is required.

The NetMap section of the Edit Collector form (figure) appears as illustrated below.

Figure 7-6 Edit Collector: NetMap Module Configuration



Each of the configurable parameters of NetMap is described below.

Maximum allowed workers

The NetMap component module on a Collector can fork multiple NetMap workers to poll network devices in parallel. This number sets the maximum number, therefore limiting the amount of SNMP traffic generated by NetMap. This value may be configured to allow up to 128 workers to be spawned at once, with the default value being 24.

SNMP inter-packet delay

This value represents the microseconds delay between SNMP packets issued by NetMap and should not be altered unless the system is experiencing SNMP packet loss or as directed by Great Bay Software Technical Support. The default value is 0, meaning that no delay will be introduced between SNMP requests issued by the Collector.

This parameter may be used in some environments to throttle the rate of SNMP polling by the NAC Profiler system.

Tip In cases where older, heavily loaded network devices (switches, routers) are experiencing high rates of CPU utilization when being polled by NetMap, increasing this value to something other than 0 (25000 microseconds, or .025 seconds) will significantly lower the impact of NetMap polling.

After completing the NetMap module configuration, configure the other component modules (if required) as outlined below. If no other component modules require configuration, skip to the section entitled Saving Edits to a Collector Configuration, page 7-27.

Configure NetTrap Collector Module

NetTrap Collector Module Overview

NetTrap is the component module running on each Collector responsible for receiving and processing SNMP traps from the edge network devices. The NAC Profiler system utilizes SNMP traps from the edge infrastructure when available in conjunction with NetMap to maintain an accurate model of the network as endpoints join and leave the network edge. As described in Chapter 3, "Preparing for Deployment", whenever possible the edge infrastructure equipment should be configured to send Link State and MAC Notification Traps (if available) to the eth0 (management interface) of one or more Collectors running the NetTrap module.

As described in Chapter 8, "Network Devices", each network device added to the system configuration is assigned to be polled by one of the NetMap components running on one of the Collectors to distribute SNMP polling. This polling occurs at the interval specified in the Server module, depending on device type (L2 or L3). Each edge network device connecting endpoints to the network being polled by NetMap should also be configured to send either v1 or v2c link state and MAC notification traps (if available) to a Collector in the NAC Profiler system. This requires a configuration change to the edge devices, switches typically, to include the IP address of the designated Collector as a trap receiver, preferably for only the Link State and MAC notification traps when available.

Tip It is recommended that the NetTrap Community String checking functionality be enabled to ensure that NetTrap processes only traps received from network devices with the community string specified in the NetTrap configuration. This requires that network devices also be properly configured to send the community string specified in the NetTrap configuration in the SNMP traps they send to the Profiler system so they are processed by the system.

NetTrap and NetMap are decoupled in the NAC Profiler system: when a NetTrap module in the system receives a link state or MAC notification trap from a network device, the Server module is notified. If a community string is configured for the NetMap module, only traps with the specified community string will be processed by NetTrap and result in the Server being signaled of a change on a network device. The Server schedules a polling task with the NetMap module that has been assigned to poll the network device that initiated the trap assuming that the network device is known to the system (e.g., in the NAC Profiler network device list). NAC Profiler will only respond to traps from network devices in the system configuration. It is not necessary to configure network devices to forward traps to the same Collector that is hosting the NetMap module designated to poll the device. Any Collector running NetTrap in the system will process incoming traps and the Server will schedule polling with the correct NetMap module accordingly, using the SNMP configuration of the device in the NAC Profiler Network Devices configuration.

Note Device polling based on receipt of a trap by NetTrap is localized to the port on the device that traps. That is, the resulting poll by NetMap will be only for the port-specific parameters as opposed to the entire device poll that occurs during the regular polling cycle specified by the L2/L3 Polling Interval parameters specified in the Server module configuration. This significantly increases the efficiency of the network device polling resulting from traps as only a subset of device information is polled by the Profiler. Note that because MAC notification traps contain additional information in the trap such as the VLAN the connecting endpoint is on, the device poll can be made more efficient.

The SNMP poll of port information based on link change/MAC notification is not instantaneous. A slight delay is implemented to ensure that the MIB is fully populated based on a change to one of the ports, and the best information is available. On a link up trap, the Profiler will wait 60 seconds before initiating the SNMP poll for port information. If a MAC notification trap for the port is received immediately following the link up, the system will wait only 5 seconds to begin the poll. On link down trap, the Profiler will delay only 5 seconds before polling the network device to verify the port status (up/down) for positive verification that the endpoint has left the port so that current location information for the endpoint can be cleared. This is the only automated mechanism available to Profiler to detect endpoints disconnecting from the network: link down trap verified by the poll that follows that the port is in a down state.

Tip While most SNMP-capable devices can be configured to send link state traps, MAC address change notification traps are vendor-specific therefore may not be supported on all devices. MAC notification traps should be forwarded to NAC Profiler Collector(s) whenever available to reduce the time required to discover new devices connecting to the network and make the polling of port information as efficient as possible.

Tip If the edge infrastructure devices are not configured to send SNMP Traps to the NAC Profiler system, there will be a delay in notification that a new end node has joined the network and potentially no notification that an endpoint has disconnected from ports. In the absence of traps, new endpoints joining or leaving the network will not be discovered until the NetMap module polls the network device providing connectivity at the next scheduled poll. Similarly, if an endpoint is "sleeping" (connected to network, but not active) on the network and a link down trap is not processed by NetTrap its departure from that location will not be processed by the NAC Profiler system necessitating the use of the Port Timeout (see Chapter 6, “Cisco NAC Profiler Server Configuration”).

Edit NetTrap Collector Module

As the Edit Collector form indicates (see below), there is only one configurable parameter for the NetTrap collector module. As a Collector is added to the system configuration, the NetTrap module is added and enabled automatically. As a highly recommended option, community string checking of traps received by NetTrap is enabled by specifying the community string in the field labeled Community String as shown in the figure below. As stated previously, if this field is populated, NetTrap on this Collector will verify the community string on all traps received, discarding those with community strings that do not match what is specified.

Figure 7-7 Edit Collector: NetTrap Configuration

If no other component modules require configuration on this Collector, skip to the section entitled Saving Edits to a Collector Configuration, page 7-27.

Configure NetWatch Collector Module

NetWatch Collector Module Overview

NetWatch is the network packet analysis component module on a Collector. A NetWatch module running on a Collector can monitor one or more of the specified physical network interfaces on the host appliance for endpoint traffic useful for Endpoint Profiling and Identity Monitoring. Typically, these physical interfaces are connected to network ports configured as SPAN/RSPAN ports providing visibility to endpoint traffic of interest redirected to the NetWatch component for the purposes of Endpoint Profiling and Identity Monitoring. NetWatch may also have eth0 added to the configuration to enable processing of packets destined for the management interface of the Collector, such as when IP Helper is being used to forward endpoint DHCP broadcasts beyond their local subnet to a Collector.

Refer to Table 7-2 at the beginning of this chapter. NetWatch is capable of collecting endpoint data from network traffic for essentially every attribute of endpoint identity currently used by the NAC Profiler system. As such, it can in many deployments be the workhorse for the NAC Profiler system in terms of endpoint data collection. For this reason the placement of Collectors using NetWatch and the configuration of this module and supporting systems (e.g., SPAN/mirror ports or network taps) to enable NetWatch configuration is critical.

Tip The NetWatch module must be configured to monitor traffic on one or more of the appliance network interfaces in order to enable the passive traffic analysis features of the Collector. Utilize the Edit NetWatch Module process outlined below to add one or more monitoring interfaces to the NetWatch module configuration to enable the NetWatch module

Edit the NetWatch Module on a Cisco NAC Profiler Collector

Use the following procedure to change any of the configurable parameters of the NetWatch module running on a Collector.

The NetWatch section of the Edit Collector form (figure) appears as illustrated below.

Figure 7-8 Edit Collector: NetWatch Configuration

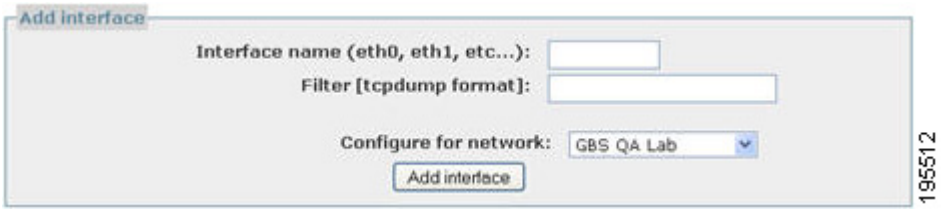
Tip As outlined in the last section, Collectors added to the configuration will not have any physical interfaces on the appliance designated for passive monitoring by default. In order to enable the NetWatch module on this Collector, one or more physical interfaces must be added to the NetWatch configuration for each Collector.

Follow the following procedures for adding, editing or deleting an interface to-from the NetWatch configuration on a Collector:

Adding Monitoring interfaces to a NetWatch module configuration

Step 1 Select the Add Interface button in the NetWatch Configuration section of the Edit Collector to launch the NetWatch Add Interface form shown below:

Figure 7-9 Add NetWatch Interface Form



Step 2 Specify an Ethernet interface name using the standard interface name (e.g., eth0, eth1, etc.) on the appliance that the NetWatch module is running on to be added as a monitoring interface so that traffic received on the interface is processed by NetWatch.

Tip Note that in order for NetWatch to process directed traffic sent to the Collector IP such as DHCP traffic redirected via IP Helper, that the interface assigned with the IP enabling network communication (typically the management interface, eth0) must be added to the NetWatch configuration.

Monitoring interfaces that are connected to network ports configured for span or mirroring, or network tap devices require no address. These interfaces will be configured for promiscuous mode, and all packets received on the interface will be processed subject to filters (if any) on interface.

Tip Ensure that when entering the interface name that the name is exactly as the interface is called out on the Cisco NAC Profiler Appliance. (e.g., eth0, eth1, eth2, eth3, eth4). Entering the command **`ifconfig -a`** at the command line will list the interfaces with the current status.

Tip Eth2 on NAC Server HA-pairs is not available for use as a monitoring interface and should not be added to the NetWatch configuration. This interface is used for the private heartbeat/database synch network connection between the members of the pair and will yield no useful endpoint data.

Step 3 Configure NetWatch Monitor Interface Filter - **Optional**

The NetWatch monitor interface filter is an advanced option used only when it is recommended by Cisco TAC to filter unwanted traffic from the NetWatch collection on the interface on very high-traffic segments.

If filters are specified on a NetWatch monitor interface, those filters will be applied to network traffic received on the interface first--packets dropped by the filter will not be forwarded/processed by NetWatch. As described below, NetWatch monitor interfaces are also configured to collect traffic only for a single Organization Name configured within My Network. This bounds data collection by NetWatch as well, programming the NetWatch module to collect data only for endpoints with the host addresses specified for the Organization Name.

When the amount of traffic of interest (from hosts within the address space specified by the Organization Name) on a monitoring interface is still very high, filters can be used to discard traffic not useful for Endpoint Profiling and or Identity Monitoring to avoid using system resources on the appliance unnecessarily.

The format of a filter added to a NetWatch interface must be entered as a tcpdump/libcap style expression that selects which packets will (or will not) be forwarded to NetWatch. If nothing is entered in the filter name field, all packets received on the interface will be forwarded to/processed by the NetWatch module. If an expression is entered, only packets for which the entered expression is true will be forwarded to/processed by NetWatch.

Expressions entered in the Filter field of a NetWatch monitor interface consist of one or more primitives. Primitives usually consist of an id (name or number) preceded by one or more qualifiers. There are three different types of qualifiers:

- ***type*** qualifiers say what kind of thing the id name or number refers to. Possible types are host, net and port. E.g., 'host foo','net 128.3', 'port 20'. If there is no type qualifier, host is assumed.
- ***dir*** qualifiers specify a particular transfer direction to and/or from id. Possible directions are src, dst, src or dst and src and dst. E.g., 'src foo', 'dst net 128.3', 'src or dst port ftp-data'. If there is no dir qualifier, src or dst is assumed.
- ***proto*** qualifiers restrict the match to a particular protocol. Possible protos are: ether, ip, ip6, arp, rarp, decnet, tcp and udp. E.g., 'ether src foo', 'arp net 128.3', 'tcp port 21'. If there is no proto qualifier, all protocols consistent with the type are assumed. E.g., 'src foo' means `(ip or arp or rarp) src foo' (except the latter is not legal syntax), 'net bar' means '(ip or arp or rarp) net bar' and 'port 53' means '(tcp or udp) port 53'.

Primitives may be combined using: A parenthesized group of primitives and operators (parentheses are special to the Shell and must be escaped).

```
Negation (`!' or `not').
Concatenation (`&&' or `and').
Alternation (`||' or `or').
```

Negation has highest precedence. Alternation and concatenation have equal precedence and associate left to right. Note that explicit and tokens, not juxtaposition, are now required for concatenation. If an identifier is given without a keyword, the most recent keyword is assumed. For example,

```
not host vs and ace
```

is short for

```
not host vs and host ace
```

which should not be confused with

```
not (host vs or ace)
```

For complete documentation of the allowable primitives and expressions for the Filter option, see the manual page for TCPdump. Enter the following command at the command line of a NAC Profiler system:

```
man tcpdump
```

Step 4 Configure for network

This parameter allows the specification of the network (by My Network Organization Name - see Chapter 5, "Configuring the Cisco NAC Profiler for the Target Environment") this monitoring interface will gather endpoint data for. The drop-down list is populated with the Organization Names saved in the My Network portion of the system configuration that specify a group of endpoints by IP host address.

Recall that each Organization Name consists of Internal Network Blocks, that specify a range of host addresses that are used by the endpoints to be Profiled. Optionally, each Organization Name may also specify Exclude Address Blocks that call out a subset of the larger Internal Network Blocks which enables filtering of a subset of host addresses from NetWatch collection. If there are multiple Organization Names saved to the configuration, select the Organization Name from the drop-down menu this interface being added to NetWatch should collect endpoint data for.

Step 5 Select the Add interface button to save the configured interface and return to the Edit Collector form. Adding additional interfaces to the NetWatch module configuration can be accomplished by repeating the process outlined above.

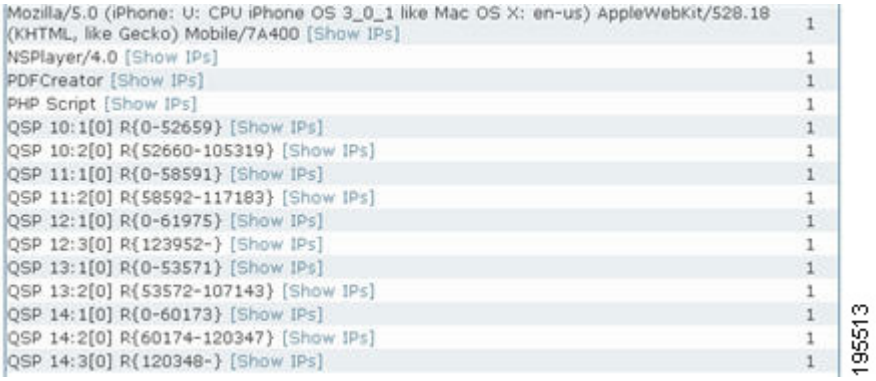
Using the NetWatch User-Agent Filter Option

NetWatch will promiscuously collect Web User Agent data for endpoints with a source IP address within the bounds of the Internal Network Blocks specified for the Organization Name selected for the monitor interface. Normally Web User Agents are static, but recently some media players have come onto the market that use dynamic Web User Agents, typically incrementing a number within the agent string so that in a single session, hundreds of unique Web User Agents could be collected for a single endpoint.

The User-Agent Filter is used to configure a NetWatch module to not forward collected Web User Agents that contain the specified string to the Server so they are not stored in the database. This field will support a Regular Expression so that multiple strings can be specified for filtering.

For example, viewing streaming video on the Fox On Demand site utilizes a media browser that uses a dynamic web user agent mechanism. Without a filter in place, each time an endpoint is used to watch a video on this site and that traffic is analyzed by NetWatch, those user agents are collected and stored in the database as profiling data for the endpoint. Viewing the web user agents on a system that had collected these agents might appear as shown in Figure 7-10.

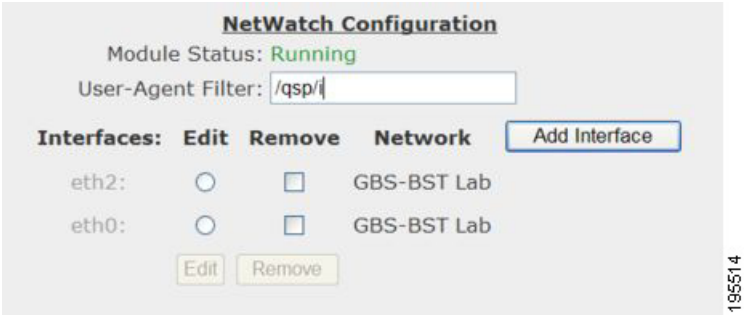
Figure 7-10 Example Dynamic Web User Agents



If a large number of endpoints were regularly watching streaming video content on the web utilizing this media player, the collected data could become large and impact performance of the NAC Profiler system. To prevent NetWatch from collecting this or any similar web agent, specify a User Agent filter in the NetWatch module configuration.

For example, to prevent NetWatch from collecting a Web User Agent containing the string 'QSP', configure the NetWatch module as shown in Figure 7-11.

Figure 7-11 Configuration of a NetWatch User-Agent Filter



Note Configuring a NetWatch User-Agent Filter stops the system from Collecting web user agents that contain the specified string, but does not clear existing data from the database. To clear collected web user agent data from the system, use the Cleanup Database button located on the System Summary page accessed from the Utilities tab. Use of Cleanup Database is described in Chapter 16, "The Cisco NAC Profiler Utilities Tab".

Editing/Removing interfaces from a NetWatch module configuration

If monitoring interfaces have been added to the NetWatch component module configuration previously, the interface (or interfaces) will be listed, with an Edit radio button, and Remove checkbox to the right of each interface, as in Figure 7-11.

To remove an interface (or interfaces) from a NetWatch configuration:

Step 1 Select the Remove checkbox adjacent to the interface(s) to be removed and select the Remove button (which becomes active when one or more of the Remove check boxes are checked).

Step 2 A dialog box will be presented to confirm the deletion of the selected interface(s), select 'Ok' to remove the checked interface(s), or 'Cancel' to cancel the remove.

To edit an interface in a NetWatch configuration:

Step 1 Select the Edit radio-button adjacent to the interface name, then select the Edit button below the interface radio button(s). This brings up the Edit interface form which reflects the current saved parameters for the interface as shown in Figure 7-12.

Figure 7-12 Edit NetWatch Interface

All NetWatch monitor interface parameters can be edited. Refer to Adding Monitoring interfaces to a NetWatch module configuration, page 7-17 earlier in the chapter for a complete description of each configuration parameter of a NetWatch Monitor interface.

After completing the NetWatch module configuration, configure the other component modules (if required) as outlined below. If no other component modules require configuration, skip to the section entitled Saving Edits to a Collector Configuration, page 7-27.

Configure NetInquiry Collector Module

NetInquiry Collector Module Overview

The NetInquiry module provides an active means of Profiling endpoints that are difficult to Profile passively. This may be desirable in environments where a NAC Profiler Collector is not able to directly observe traffic from endpoints of interest that can be used for Endpoint Profiling, or in the case of endpoints that do not regularly generate traffic on the network.

Unlike active scanners used primarily for endpoint vulnerability assessment, the NetInquiry module will attempt to initiate communications with endpoints according to narrowly defined criteria (e.g., on a single TCP port), not broadly defined scans which can potentially harm some endpoints.

In the current version of NAC Profiler, the NetInquiry collector module operates in conjunction with a limited number of the rule types that maybe used in Endpoint Profiles. Those rule types include TCP Open Port rules and the following Application Rule Types:

- Web Server Type

- SMTP Server Banner

These rule types contain the option at time of rule creation to be made "Active" as rules of these types are added to one or more profiles.

In addition, the NetInquiry module is also able to gather DNS Name information from the enterprise name service for use with the DNS Name Application rule type. Configuration of these rules is explained in detail in Chapter 8, "Network Devices" of this document.

An additional configuration parameter required for the enablement of NetInquiry functionality for Active Profiling is implemented within the Cisco NAC Profiler which limits the scanning only to a specified number of devices. As outlined later in this section, the NetInquiry functionality on a given Collector is constrained to only the network blocks specified in the configuration of the NetInquiry module for that Collector.

Zone Transfer (AXFR) capability for DNS Name collection by NetInquiry was added in Cisco NAC Profiler version 3.1. When this option is used for DNS Name collection, NetInquiry will query the name server specified for the appliance hosting the Collector to gather the master record for the specified domain as described later in this section.

In the case of TCP Open Port, Web Server Type and SMTP Server Banner rules used in "active" mode, the NetInquiry module initiates an attempt to actively probe the devices only within the specified Network Blocks of configured NetInquiry module(s) across the system via the management interface of the Collector appliance on which it is running.

In this approach to active profiling, the NetInquiry module results in the appliance actively generating traffic that is extremely useful for the Endpoint Profiling process via sending traffic on the management interface of the appliance. The responses to that traffic is then available for processing by NetInquiry, and it is generated efficiently and with minimum impact on the endpoints or the network.

Recall that the Server module configuration also contains a parameter that is used to regulate Active Profiling at the system level. The Server parameter named 'Frequency' in the Active Profiling Configuration section specifies the frequency of active profiling for the entire NAC Profiler system. On all Collectors that have a configured NetInquiry module running, active profiling tasks will be generated on those collectors according to the frequency specified in the Server module.

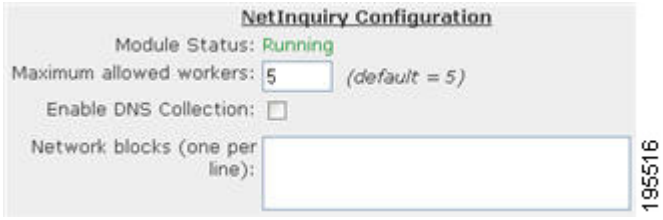
Edit NetInquiry Collector Module

Use the following procedure to change any of the configurable parameters of the NetInquiry module running on a given Collector.

Tip The NetInquiry module on a NAC Profiler Collector should be configured/enabled only when Active profiling will be used. Until such time that there are active rules present in enabled Profiles, the parameters of the NetInquiry modules should be left at the default which effectively disables NetInquiry on the Collector.

The NetInquiry section of the Edit Collector form Figure 7-13 appears as illustrated below prior to the configuration of the module.

Figure 7-13 Edit NetInquiry Collector Module



Each of the configurable parameters of a NetInquiry Collector component module is described below. Complete the following steps to configure NetInquiry as desired.

Step 1 Set Maximum allowed workers

The NetInquiry process can create multiple NetInquiry workers to act in parallel. This number sets the maximum number, thereby limiting the amount of network traffic generated and the system resources used by NetInquiry. This value may be configured to allow up to 16 workers to be spawned at once, with the default value being 5.

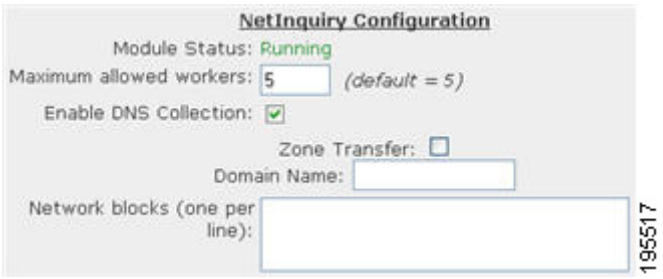
Tip Default value is recommended unless directed otherwise by Cisco TAC.

Step 2 Enable DNS Collection - As desired

This optional feature of the NetInquiry Collector modules enables the NAC Profiler system to perform name lookups on the addresses specified in the Network blocks field, or as an option using Zone Transfer to request the master record for the domain. The actively discovered name can then be used by the system to match DNS Name Application rules used in endpoint Profiles.

When this option is enabled, the NetInquiry module configuration parameters change as shown in Figure 7-14 to allow for the enablement of the Zone Transfer option discussed earlier.

Figure 7-14 NetInquiry Module Configuration with DNS Collection Enabled



Tip This feature should only be used when DNS Name Application Rules are being used in enabled Endpoint Profiles. In NAC Profiler implementations where the Zone Transfer option cannot be used and DNS Collection is enabled, the NetInquiry module(s) employed in the system that have this option enabled will query the DNS for each host address (reverse lookup) on the subnet(s) specified in the Network Blocks parameter of their configuration. This may place a high load on the DNS Server and should be avoided.

To enable the Zone Transfer option for DNS name collection, check the Zone Transfer checkbox, and enter the domain name of the endpoints of interest. Note that NetInquiry will query the DNS Server specified for the All-in-one/Remote Collection appliance it is running on and the zone transfer will fail if that name server does not maintain the name service for the specified domain.

Step 3 Configure Network Blocks as required

This field is used to specify the subnet or subnets which contain the endpoints that are desired to be actively probed by this NetInquiry Collector module. The format is X.X.X.X/CIDR, for example 10.10.0.0/16 means any IP Address in which the first two octets are 10.

Add the subnet(s) that contain the hosts to be probed by NetInquiry when one or more Active rules are present in enabled profiles. Enter one address/mask per line.

Note that the Network Blocks are always used when active TCP Open Port, Web Server type and or SMTP Server Banner rules are present in enabled profiles to determine which endpoints will be probed by this NetInquiry module. If Zone Transfer is enabled, this parameter is not used in the collection of DNS Name data. If the Zone Transfer option is not used, with DNS Name Collection enabled, a reverse DNS lookup to the DNS Server specified for the All-in-one/Remote Collection appliance for every host address within the Network Block.

Tip Caution is required when using active profiling on large host address ranges. Particularly in the case of using /8 masks on Class A networks, or /16 masks for class A and B networks it is important to understand that each active rule in enabled profiles will result in attempted data collection (e.g, DNS Name Resolution (if Zone Transfer is not enabled), banner request, or TCP Open Port attempt) for over 16 million host addresses in the case of the Class A with /8, or 65K host addresses in the case of a /16 on Class A or B networks, either of which may result in unintended impacts on the Profiler and or the network and is **not recommended** as a general practice.

After completing the NetInquiry module configuration, configure the other component modules (if required) as outlined below. If no other component modules require configuration, skip to the section entitled Saving Edits to a Collector Configuration, page 7-27.

Configure NetRelay Collector Module

NetRelay Collector Module Overview

The NetRelay collector module is an optional module that enables the NAC Profiler system to ingest captured data from other endpoint data collection systems that may already be in service in some enterprise networks.As of version 3.1, NetRelay is able to collect endpoint data from NetFlow collection (e.g., routers) and NetFlow aggregation systems. The version 3.1 release added RADIUS accounting.

In the case of NetFlow, NetRelay can be especially useful for performing Endpoint Profiling and Identity Monitoring on remote segments of the network (e.g., remote offices, etc.) that the NAC Profiler System cannot directly monitor traffic to/from via NetWatch. In order to utilize the NetFlow ingestion feature, on a NetRelay module in a NAC Profiler system, NetFlow collectors such as routers must already be in place on the network and collecting NetFlow data on the endpoints of interest. The NetRelay collector module enables the NAC Profiler system to re-use this data for the purposes of Endpoint Profiling and Identity Monitoring.

NetFlow data is used by the NAC Profiler system in conjunction with Traffic Rules which are described in Chapter 10, "Endpoint Profile Configuration: Part II". NetFlow data can be used in lieu of raw network traffic to enable the NAC Profiler system to examine traffic flows between endpoints for attributes specified in Traffic Rules contained in endpoint profiles.

This functionality is dependent upon the presence of NetFlow collector devices (e.g., routers, switches or other devices that have a NetFlow collector capability) on the network segments of interest, with NetFlow collection enabled and configured to forward their data to the NAC Profiler system. By default, a Collector with NetRelay collection configured/enabled will listen on its management interface for XDRs sent to the management interface IP on port 2055. The NetFlow Collectors (routers, etc.) must be configured to send NetFlow XDRs to the IP of the management interface on that port number.

Like NetWatch, NetRelay is configured to constrain the collection of data from NetFlow XDRs forwarded to it to a specific host address range. When NetRelay is enabled/configured on a Collector, the NetRelay module is assigned an Organization Name from the MyNetwork configuration that programs the range of host addresses that NetRelay module will collect data from.

In environments where RADIUS clients (generally access switches) are performing endpoint authentication (e.g., 802.1X or MAC Authentication) and are configured to send RADIUS accounting records to a NAC Profiler Collector running NetRelay configured for this data collection option, the NetRelay module will collect this information about endpoints authenticating (or attempting authentication) to those network devices. Like in the case of NetFlow Collectors, RADIUS Clients need to be configured to forward accounting records to the NetRelay module designated in the NAC Profiler configuration to receive and process this data. The NetRelay module must have RADIUS collection enabled, and the RADIUS Client must be known to the NAC Profiler system. RADIUS clients and shared secrets are configured per network device or network device group as described in Chapter 8, "Network Devices".

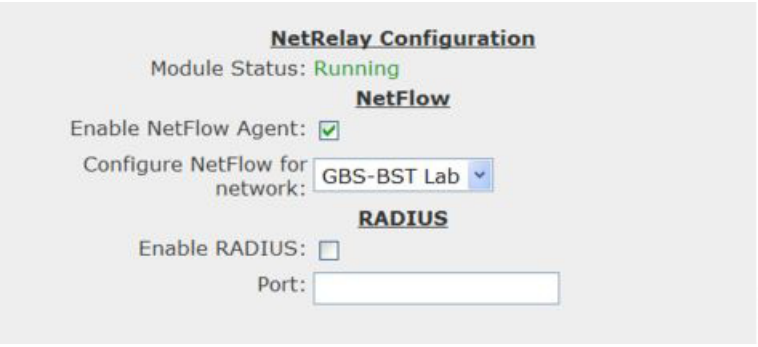
Edit NetRelay Collector Module

Use the following procedure to change any of the configurable parameters of the NetRelay module running on a Collector.

Each NetRelay module in the system that is enabled must be configured for desired modes of data collection: NetFlow and or RADIUS accounting.

The NetRelay section of the Edit Collector form appears as illustrated in Figure 7-15.

Figure 7-15 Edit Collector: NetRelay Configuration



To enable a NetRelay module for NetFlow Collection, complete the following steps:

Step 1 Check the 'Enable NetFlow Agent' checkbox

This checkbox must be checked in order for the NetRelay Collector component module to accept NetFlow traffic from NetFlow collectors on the network configured to forward their data to the NAC Profiler system.

Tip By default, enabling the NetFlow Agent on a NetRelay module initiates listening for XDRs sent to the Collector management interface (eth0) by routers and other NetFlow collectors on port 2055.

Step 2 Select the Network Name (My Network Organization Name) that this NetRelay module should collect data for.

The drop-down control allows the selection of the Organization Name from those saved to the MyNetwork configuration (see Chapter 5, "Configuring the Cisco NAC Profiler for the Target Environment") to specify the host address range which this NetRelay module will perform endpoint data collection from received NetFlow XDRs.

Tip As discussed earlier in the Guide, in large systems with multiple Collectors, consideration may be given to distributing processing of NetFlow across multiple NetRelay modules. This requires the dividing the host address space into two or more network (Organization Names) in the MyNetwork configuration and then assigning them amongst the NetRelay modules using this parameter of the NetRelay configuration.

Step 3 Verify that the NetFlow collectors/harvesters in the network are properly configured to export their flow data to the eth0 interface IP address of the Collector running the NetRelay module, on the designated port number.

Tip The listening port number for inbound NetFlow export data for a NetRelay module can be modified, but not through the UI. Contact Great Bay Software Technical support for instructions on modifying the NetFlow listening port.

To enable a NetRelay module for RADIUS Accounting data collection, perform the following steps:

Step 1 Check the 'Enable RADIUS' checkbox.

Step 2 Specify the port number that the RADIUS clients are configured to export their accounting data on.

Typically, port 1813 is used by RADIUS clients for exportation of accounting data. Verify the configuration of the RADIUS clients configured to send their accounting data to NAC Profiler, and set this parameter accordingly.

Step 3 Verify that the RADIUS clients that will be sending accounting data to the NetRelay module have been configured with RADIUS accounting enabled, the correct shared secret and are assigned to the NetRelay module as described in Chapter 8, "Network Devices".

Saving Edits to a Collector Configuration

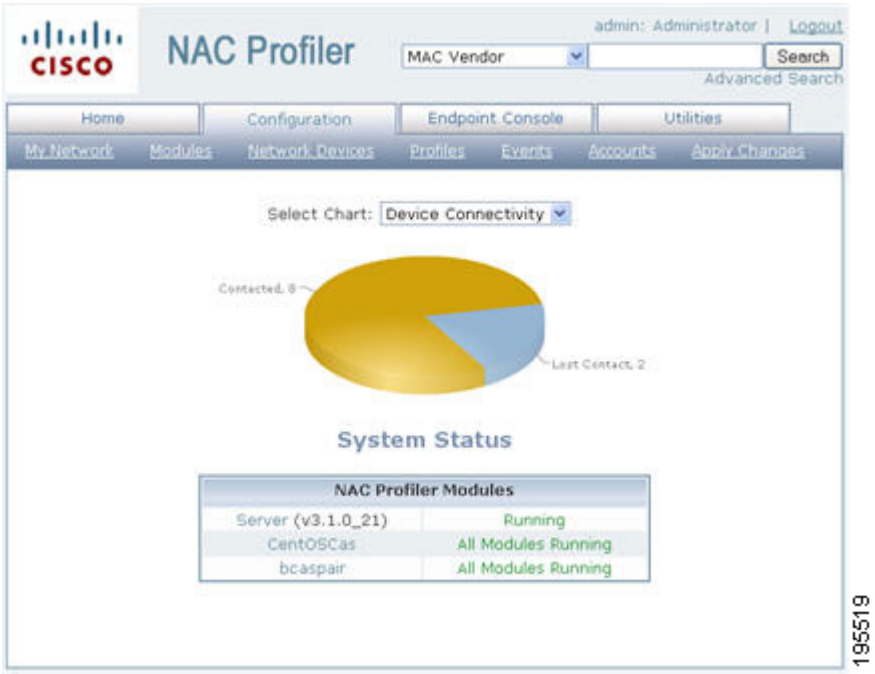
When all desired changes have been made to a NAC Profiler Collector configuration, select the Save Collector button to save all changes to the Collector.

Tip Changes made to Collectors are saved to the running NAC Profiler system configuration by clicking the Update Modules button on the Apply Changes page. The Apply Changes page is accessed by selecting the Apply Changes link from the Configuration tab secondary menu.

Determining Status of Cisco NAC Profiler Collectors

After saving the edits to a Collector, the status of all Collectors in the NAC Profiler system as well as the Server module can be ascertained by navigating to the Configuration tab. The Configuration tab will display as shown in Figure 7-16.

Figure 7-16 Configuration Tab Showing Cisco NAC Profiler Modules Status



Note the NAC Profiler Modules table, which displays the Server module and each of the Collectors added to the system configuration in separate rows, along with their status. The Status column of the NAC Profiler Modules table indicates the condition of the component modules of each Collector in the NAC Profiler system configuration. There are seven possible Collector statuses that reflect the condition of the component modules which is reported for each Collector in the configuration.

The Collector statuses and their interpretations are provided in the figure below:

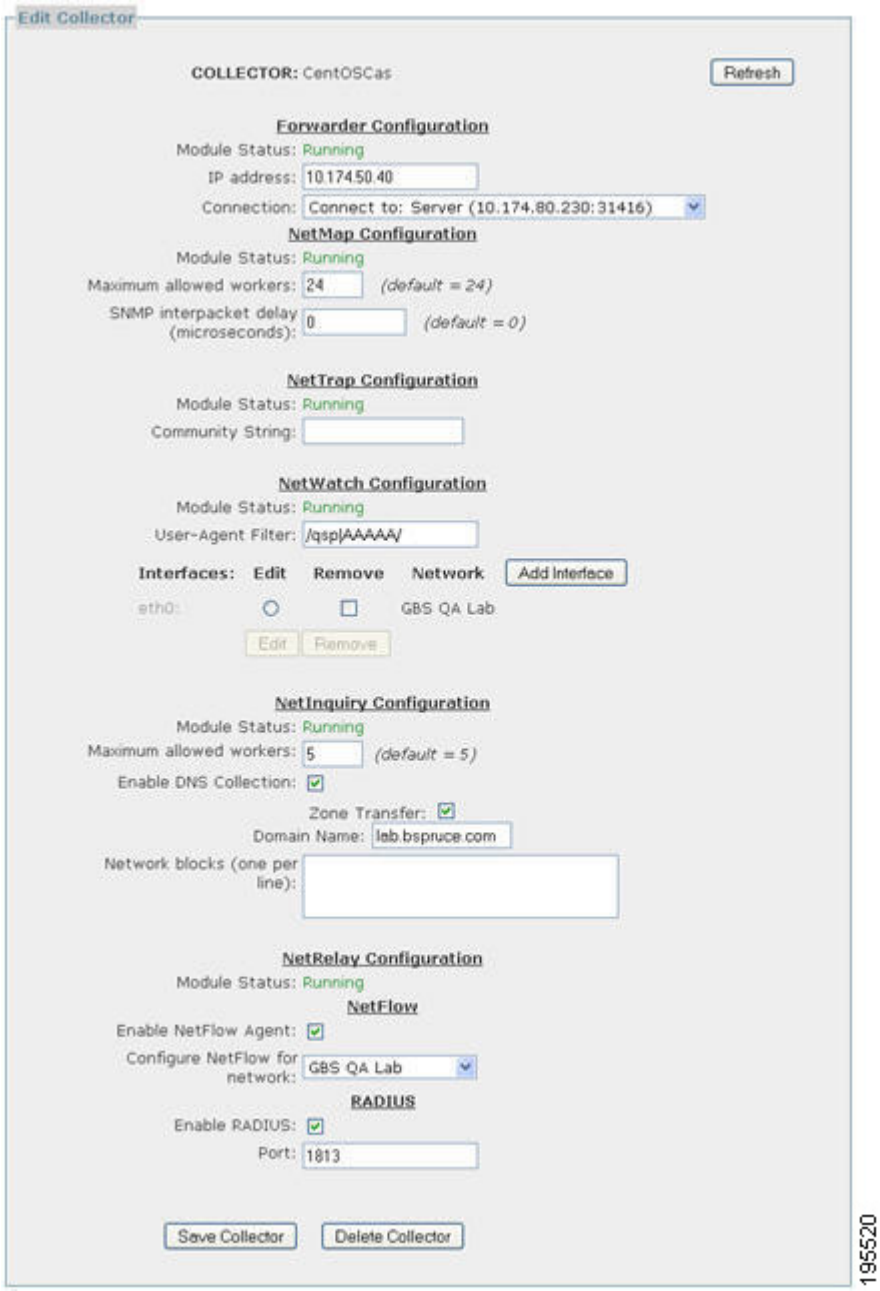
Table 7-3 Collector Status Messages

Status	Interpretation
All Modules Running	All modules of the Collector have been contacted by the Server and are running. The Collector is online and operating normally.
All Modules Stopped	All modules of the Collector have been contacted by the Server, but they are in a stopped condition. This is typically a transitory condition resulting from the system restart following an Apply Changes.
One or More Modules Stopped	All modules of the Collector have been contacted by the Server, but one or more are in a stopped condition. Again, this may be a transitory state as some modules may take longer to come back online after a system restart. If the condition does not clear, follow the procedures outlined in the section below to determine what module(s) are in the stopped condition and troubleshoot accordingly.
Not Contacted	The Server has been unable to establish communications with the Forwarder module running on the Collector. Status of the Collector and its component modules cannot be determined by the Server. See troubleshooting steps outlined in next section.
Licensing Issue	The number of Collectors added to the configuration exceeds the number of valid Collector licenses uploaded to the NAC Profiler Server.
One or more Modules Restarting	One or more component modules on the Collector are in the process of restarting. This is a very short transitory state between stopped and running that will not normally be observed. It occurs when a Collector initially establishes contact with the Server when a new system is brought online.
One or more Modules reporting an error	One or more component modules on the Collector have posted an error message. This is typically indicative of an error in the configuration of one or more component modules.

Troubleshooting Component Modules on a Collector

The Table of Collectors provides a top-level view of each Collector in the NAC Profiler system. If the status of a Collector is other than "All Modules Running," status of the underlying modules of a given Collector can be determined by selecting the name of the Collector in the table of Collectors to open the Edit Collector form. An example of this form from a configured/running system is shown inFigure 7-17.

Figure 7-17 Edit Collector Form Displaying Modules Status



As shown in the figure, each of the component modules running on a Collector (e.g., NetMap, NetTrap, NetWatch, NetInquiry, NetRelay and Forwarder) has a Module Status indicated at the top of each section of the form pertaining to each component module. The status of a component module can be one of the following:

- **Running** – the component module is running and reporting normal status.
- **Stalled** – When component modules on a Collector report a status of stalled this is indicative that contact with the Collector was established but subsequently lost, typically due to the loss of network communications between the Server and Collector.

- **Stopped** – the component module is not currently running. As a Collector is restarted, the component modules will temporarily transition through this state.
- **No contact** – The Server has not made contact with the Collector or the component modules running on it and therefore cannot ascertain status. If the Collector status is indicating 'Not contacted' as described above, the component modules indicate 'no contact' individually.
- **Invalid configuration file (missing Internal Address)** – NetWatch–specific error condition that indicates that a monitoring interface was never specified for the NetWatch component module.
- **No Traffic to Monitor** – NetWatch–specific error condition that indicates that a monitoring interface was specified for the NetWatch component module, but no traffic is being received for processing.
- **Ignored** - indicated by all component modules on a Collector added to the system in excess of the Collector licenses validated by the NAC Profiler Server. Endpoint data is not being collected by the component module, it is effectively disabled. This is accompanied by the Collector status reporting "Licensing Issue" as described in Table 7-3 on page 7-28.

A Module Status of 'running' indicates that the module is running and requires no attention.

A Module Status of 'stopped' indicates that the Server is in communications with the Forwarder on Collector, but the respective component module was not running. After a system restart (following an Apply Changes -> Update Modules for example) some amount of time may be required for the underlying modules to restart using the new configuration sent down to the module by the Server (if applicable). Wait several minutes and check the status again by refreshing the page. If a module continues to indicate a status of stopped, further troubleshooting is required. The troubleshooting should begin with checking the existing configuration of the affected module to ensure it is configured according to the instructions in this chapter. After verifying the configuration an Apply Changes -> Update Modules should be performed to attempt restart of the module to return it to a running status. Regardless of whether or not configuration of the module is modified, an Apply Changes -> Update Modules is recommended as the first step in attempting to restart a stopped component module on a Collector.

When the status of a module indicates 'no contact', this is indicative of the Server and Forwarder being unable to establish communication. On All-in-one appliances, this communication should occur over the internal loop-back interface. In the case of Remote Collection appliances, this communication occurs over the network.

The parameters for the communication such as Collector name (must match host name of the Remote Collection appliance, connection type (e.g., client or server), IP address, network connection defined on the Server, connection on the Forwarder, encryption type and shared secrets on both must be consistent in order for the communication between Server and Forwarder to be established. Revisit these parameters in the respective Collector module setup, as well as the Server and Forwarder configuration to ensure that the configurations are consistent. In addition, verify that there are no other measures deployed (e.g., ACLs, firewalls, etc.) that would prevent TCP communications between the Server and the remote Collector paying particular attention in the case of a firewall deployed between the devices that traversal is possible on the selected port number. When these troubleshooting steps have been completed, perform the Apply Changes -> Update Modules procedure to restart all modules which will result in a reattempt to establish the network connection between the Server and Collector.

Component modules reporting a "stalled" status is likely due to the Collector going offline completely or a condition in the network that has interrupted the TCP connection between the Collector and the Server. If the Collector is determined to be up and running from the Collector command line (via **`service profiler status`** command), troubleshooting should begin with determining if the connection between the devices is established beginning with a 'ping' between devices to determine the status of network communications between the appliances.

In the case of component modules reporting an error, in general this is due to an error in the configuration, or in the case of the NetWatch module specifically, not having a monitoring interface specified in the component module configuration or no traffic being delivered to a monitoring interface. Verify the configuration of the component module to ensure at least one of the interfaces on the Collector appliance is specified as a monitoring interface, and the monitoring interfaces are receiving traffic for NetWatch analysis.

Editing a Cisco NAC Profiler Collector Configuration

Once a Collector has been added to the system configuration, changes can be made to the configuration parameters of the Forwarder and Collector component modules running on the Collector using the UI. For example, if previously not configured/disabled endpoint data collection techniques are to be enabled on a given Collector, those changes can be effected via the UI, and committed to the running configuration by executing an Apply Changes -> Update modules to create the new configuration, push it to the Collector, and restart the Collector to make the changes effective.

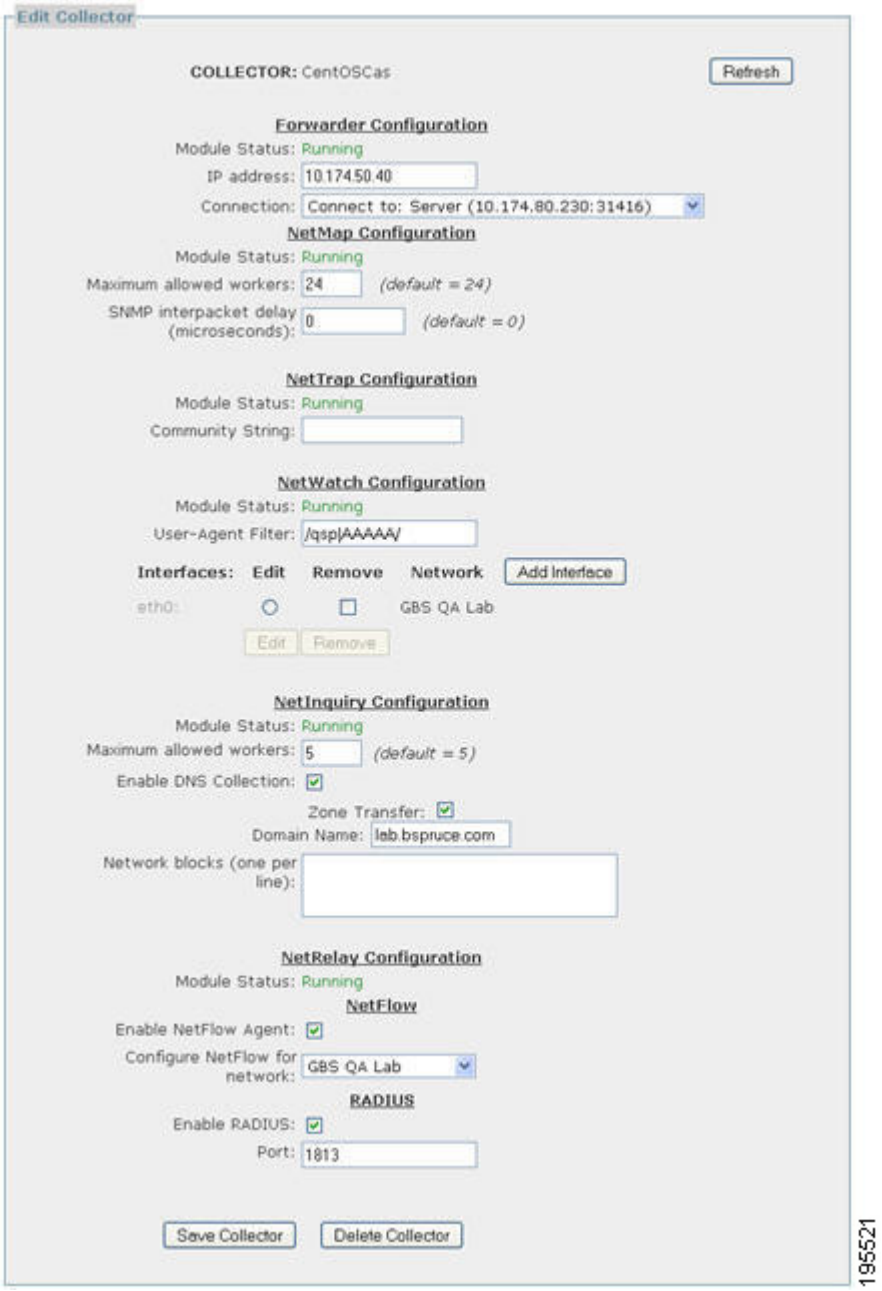
To edit a Collector previously saved to the Cisco NAC Profiler system configuration, perform the following steps:

Note Collector Names cannot be edited. If a Collector name was entered in error and needs to be edited, the Collector must be deleted first and then added back with the correct name.

Step 1 Navigate to the Configuration tab and select the link for the Collector Name to be edited from the NAC Profiler Modules Table.

This opens the Edit Collector form for the Collector already saved to the configuration. An example of the Edit Collector form for a running Collector module that has been contacted by the Server is shown in the Figure 7-18.

Figure 7-18 Edit Collector Form



Step 2 Refer to the earlier sections in this chapter which cover the configuration of each module of a Collector to make desired changes.

Step 3 When all desired changes have been made to components of the Collector, select the Save Collector button at the bottom of the form to save configuration changes.

Tip Changes made to NAC Profiler Modules are saved to the running NAC Profiler system configuration by clicking the Update Modules button on the Apply Changes page. The Apply Changes page is accessed by selecting the Apply Changes link from the secondary menu under the Configuration Tab selection.

Delete a Collector from the System Configuration

To delete a Collector from the system configuration:

Step 1 Navigate to the Table of Collectors, and select the name of the Collector to be deleted. The Edit Collector form is displayed.

Step 2 Scroll down to the bottom of the form to the Delete Collector button. Selecting this button will delete the Collector configuration from the system configuration, and return the interface to the Table of Collector/Table of Servers page, displaying a message that the modules on the deleted Collector have been deleted from the database.

Step 3 The deleted Collector is removed from the table of Collectors. If desired, the Collector can be re-added to the system configuration using the procedure outlined earlier in this chapter.

Step 4 Insure that a Apply Changes -> Update Modules is executed after deleting the Collector.