Application Note

Cisco Router and Security Device Manager
Network Admission Control

Introduction

This document explains how to configure a Cisco IOS® router as a network access device using the Cisco® Router and Security Device Manager (SDM). This document contains these sections:

- Overview
- How Network Admission Control Works
- Deploying Network Admission Control on a Cisco IOS Router
- Verification

Overview

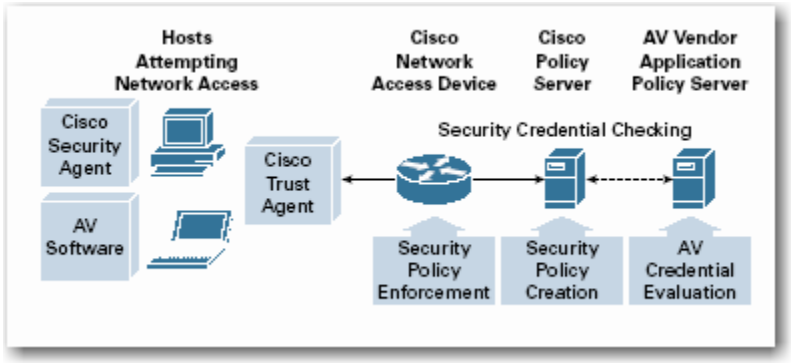
Network Admission Control (NAC) is an industry initiative sponsored by Cisco Systems® that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network resources, thereby limiting damage from viruses and worms.

Using NAC, organizations can provide network access to endpoint devices such as PCs, PDAs, and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined state, or give them restricted access to computing resources.

NAC is comprised of several essential components (Figure 1):

1. Communications agent—Cisco Trust Agent is a software tool that collects security state information from security software solutions on the endpoint, such as antivirus, OS, and Cisco Security Agent, and communicates this to the network access device.
2. Network access devices—Every device seeking network access initially contacts a network access device, such as router, switch, VPN concentrator, or firewall. These devices can demand endpoint security "credentials" from the endpoint through Cisco Trust Agent and relay this information to the policy servers for an admission decision.
3. NAC policy servers—Cisco Secure Access Control Server (ACS) and third-party vendor policy servers evaluate endpoint security credentials relayed from the network access device and determine the appropriate access policy to be applied (*permit, deny, quarantine, restrict*).

Figure 1. NAC Components



How Network Admission Works

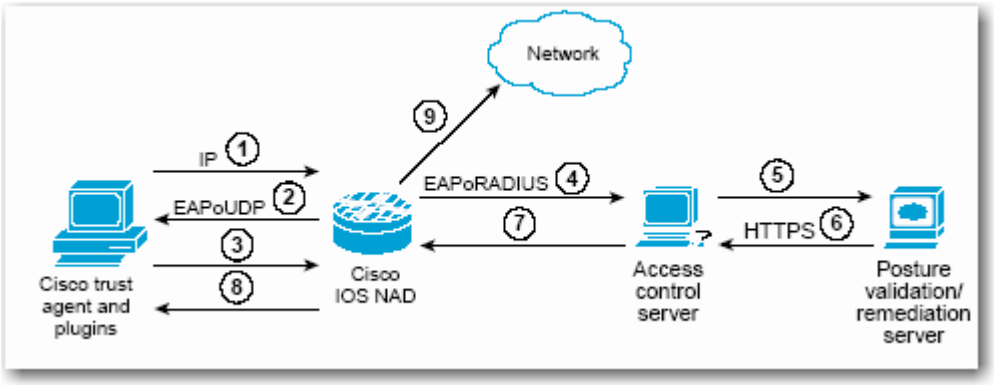
NAC implementation combines a number of existing protocols and Cisco products, including:

- Cisco Trust Agent
- Network access device (the router in our lab)
- Extensible Authentication Protocol (EAP)
- NAC policy server: Cisco Secure ACS/RADIUS
- Posture validation/remediation server

Figure 2 shows the way that the different components of the NAC solution interact. For more information, please refer to "Implementing Network Admission Control – Phase One Configuration and Deployment," available at:

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

Figure 2. NAC Operation



Deploying NAC on a Cisco IOS Router

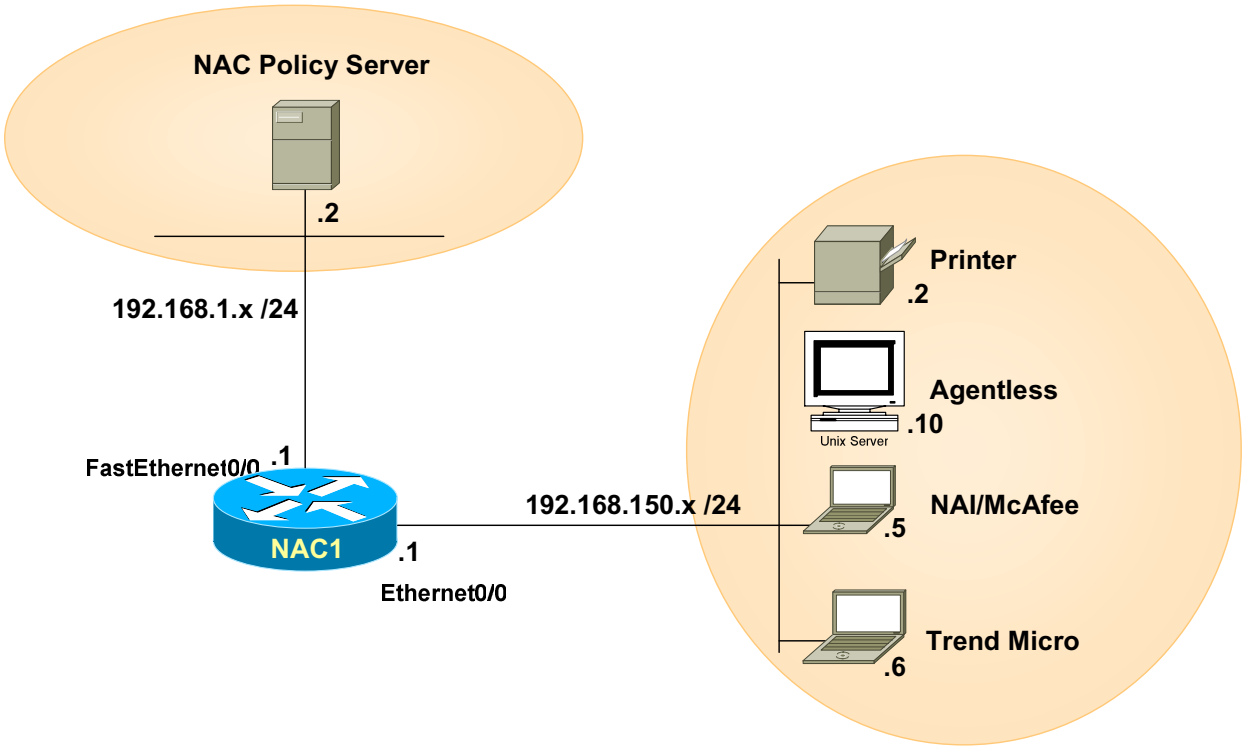
Prerequisite

Before configuring a network access device, collect the following information:

- RADIUS parameters for the NAC policy server (or Cisco ACS)
- IP or MAC addresses for the exception list, which allows hosts such as printers and IP phones to bypass the NAC policy server validation process
- The information for the agentless host policy, which allows hosts without Cisco Trust Agent installed, such as a UNIX server that Cisco Trust Agent does not support, to bypass the NAC policy server validation process

This document demonstrates how to configure a Cisco IOS router as a network access device that is connected to subnet 192.168.1.x containing a NAC policy server for security policy, and connected to subnet 192.168.150.x where endpoint devices are located. Figure 3 shows the network topology. The printer should be in the exception list. The agentless UNIX server is allowed to bypass the validation process, as are the two laptops installed with Cisco Trust Agent that employees are taking home. Cisco Trust Agent installation and configuration and NAC policy server installation and configuration are not covered in this document.

Figure 3. Network Topology



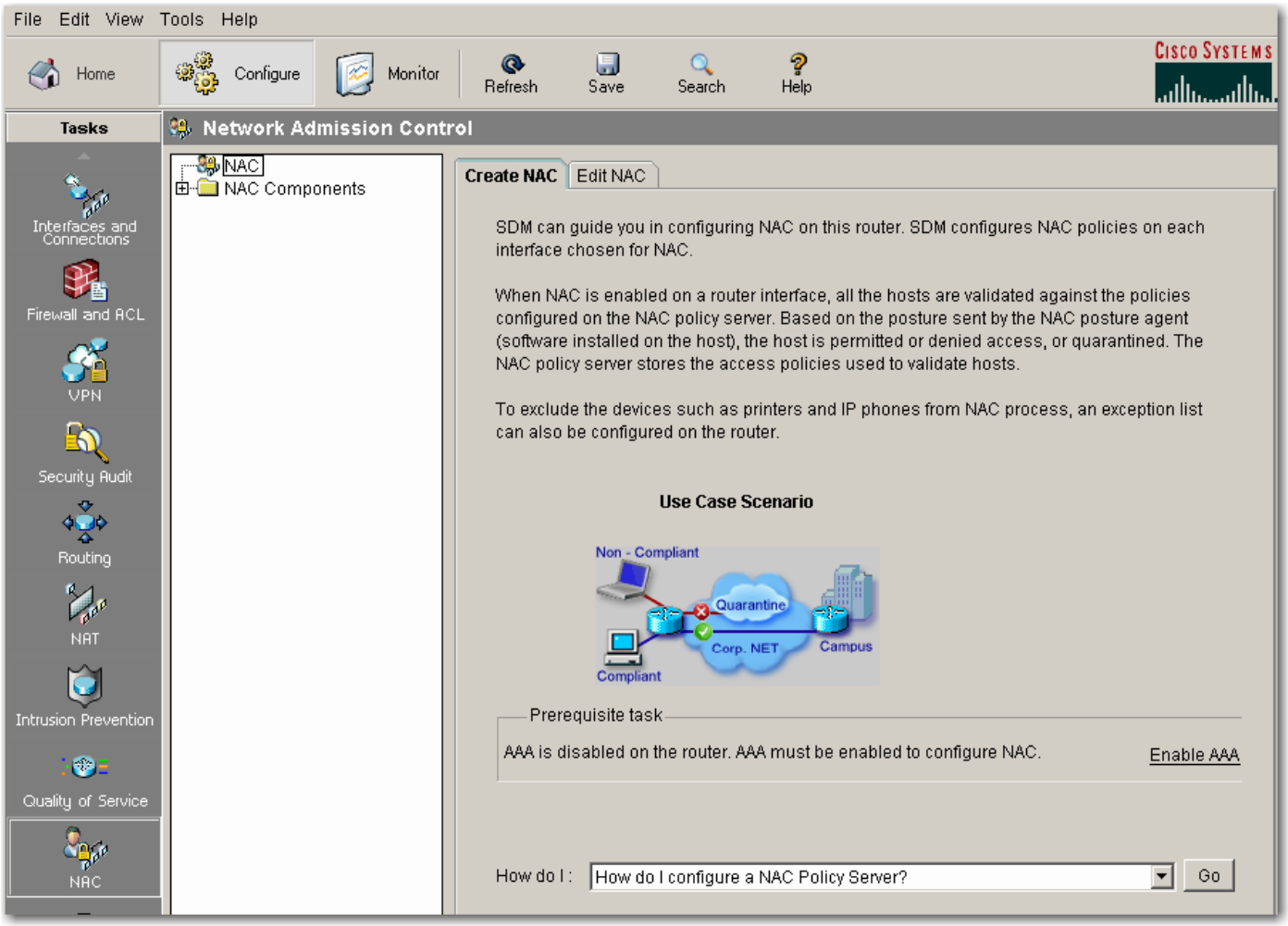
Configuring a Network Admission Device

It is highly recommended to use the NAC wizard if NAC has not been configured. The NAC wizard enables you to:

- Select the interface on which NAC is to be enabled—Hosts attempting access to the network through this interface must undergo the NAC validation process.
- Configure the NAC policy server—Admission control policies are configured on these servers, and the router contacts them when a network host attempts access to the network. NAC policy servers use the RADIUS protocol.
- Configure a NAC exception list—Hosts such as printers, IP phones, and hosts without Cisco Trust Agent installed may need to bypass the NAC process. Hosts with static IP addresses and other devices can be identified in an exception list, and be handled using an associated exception policy.
- Configure an agentless host policy—To use a policy residing on a NAC policy server to handle hosts without a Cisco Trust Agent.
- Configure NAC for remote access—Hosts using Cisco SDM to manage the router must be allowed to access the router. The wizard lets you specify IP addresses for remote management so that Cisco SDM will modify the NAC access control list (ACL) to allow the hosts with those addresses access to the router.

Click **Configure**, select **NAC**, and then click the **Create NAC** tab. In our example, AAA is not enabled (Figure 4). To enable AAA, click **Enable AAA**; the **Launch NAC Wizard** button will be available once the AAA is enabled.

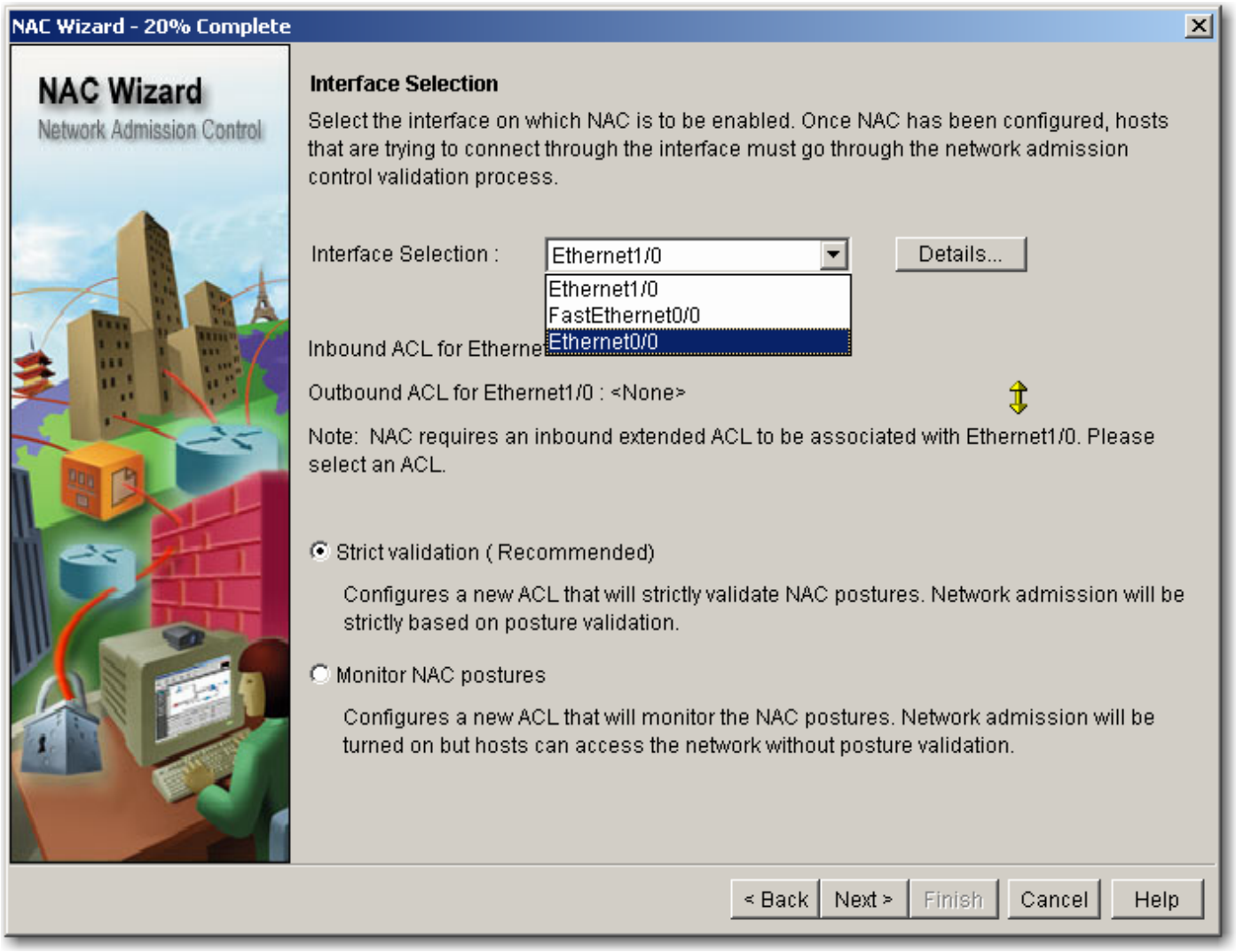
Figure 4. Create NAC



To configure the router as a network access device, follow these steps:

1. Launch the NAC Wizard by clicking the **Launch NAC Wizard** button. Click **Next** after reading the welcome information.
2. Choose the interface on which NAC is to be enabled (Figure 5).
    - Interface Selection: **Ethernet0/0**
    - Select **Strict validation**[1]
    - Click **Next**

Figure 5. Interface Selection



[1] Strict Validation: By default, all traffic is denied, and access is allowed only if the traffic is found to be valid based on the policy configured on the NAC policy server.

3. For NAC policy servers, in our example, the NAC policy server (or the RADIUS server) is located in the 192.168.1.0 network. Select the FastEtherent0/0 interface.

   - Choose the RADIUS Client source[2]: Select **FastEthernet0/0** from the pull-down menu (Figure 6). You will be prompted by an SDM Warning message after selecting the interface.
   - Read the warning information, and click **Yes** to close the SDM Warning message (Figure 7).

Figure 6. Choose the RADIUS Client Source

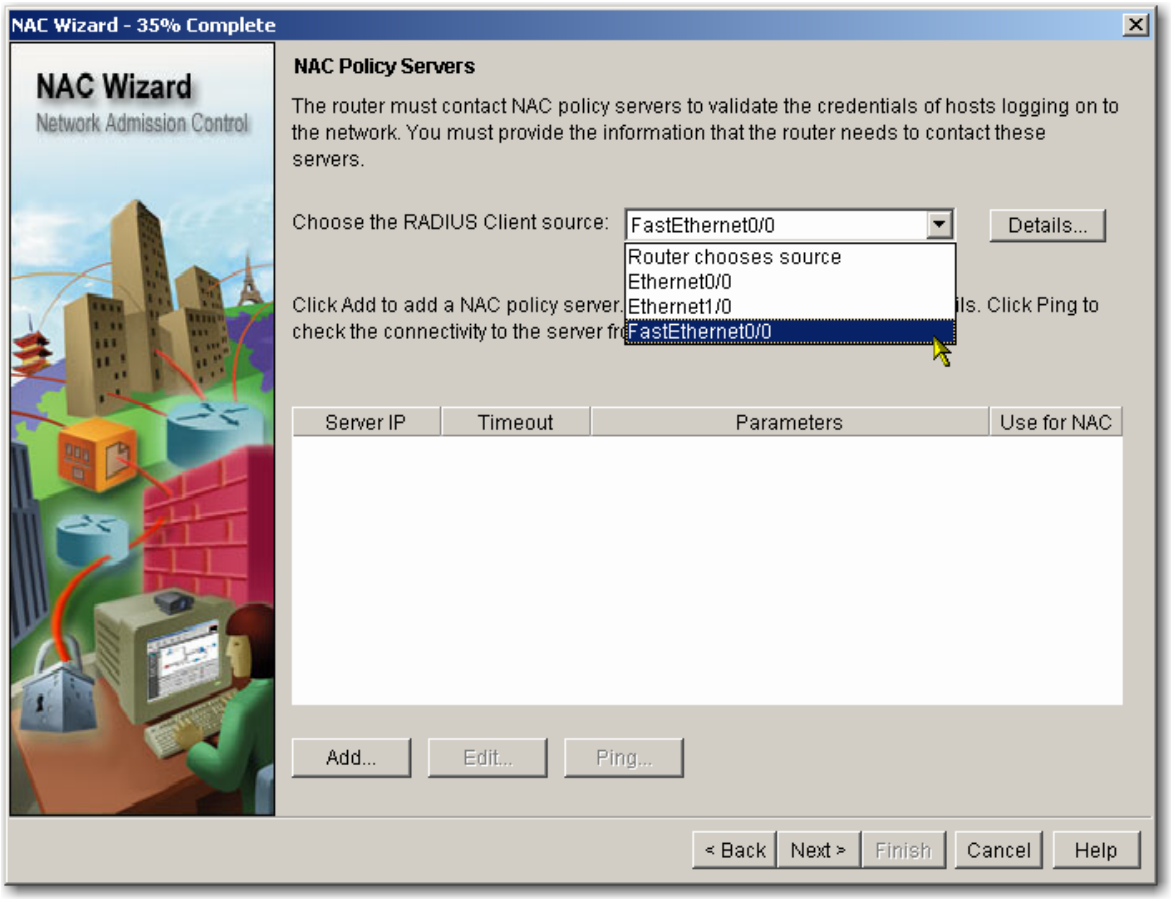
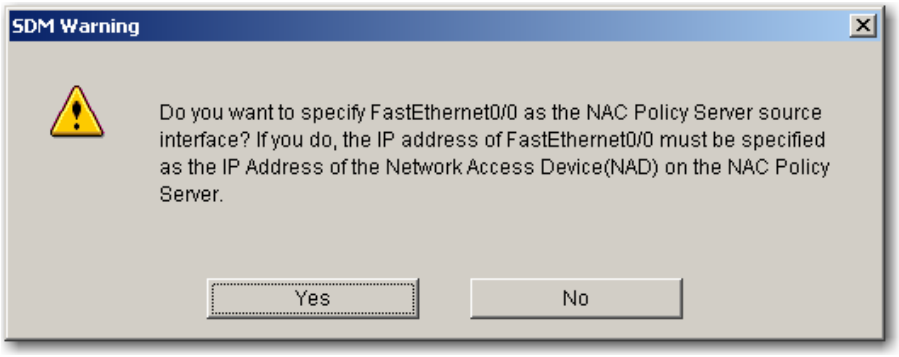


Figure 7. SDM Warning

[2] If you choose **Router chooses source**, the source IP address in the RADIUS packets will be the address of the interface through which the RADIUS packets exit the router. Make sure your NAC policy server permits the packets with this source IP address.



- Click the **Add…** button in the lower part of the NAC Wizard window to add a NAC policy server. The **Add NAC Policy Server**[3] dialog appears (Figure 8). In our sample, the IP address of the NAC policy server is 192.168.1.2 with a key **radiuskey**. We use the default values for Authorization Port and Accounting Port, and we leave the Timeout blank—the NAC Wizard will use the system default value (five seconds).

  Server Type: **RADIUS**

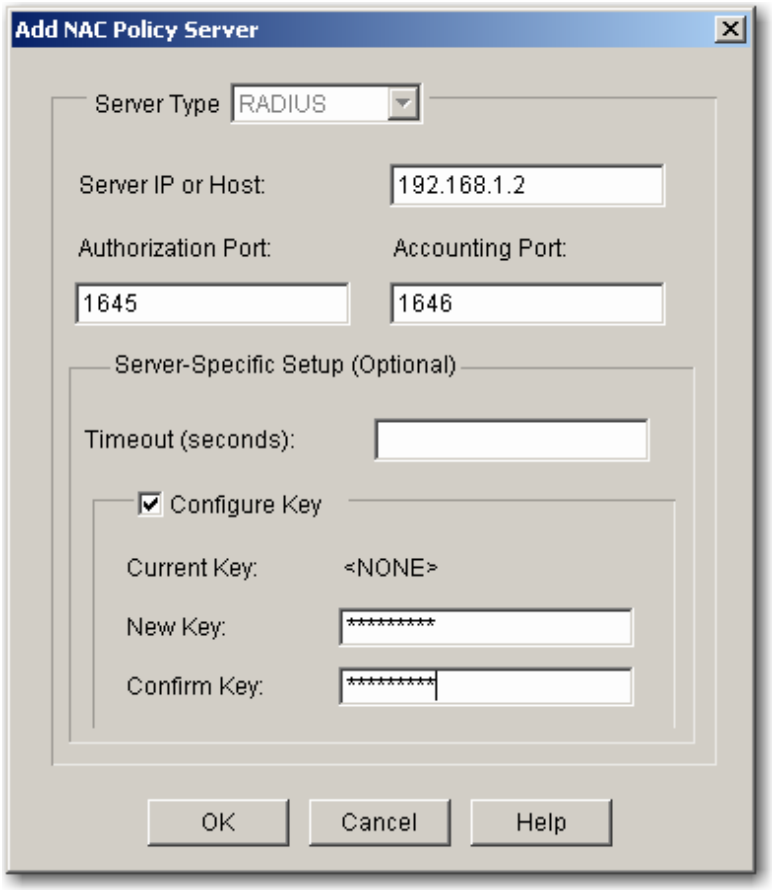
  Server IP or Host: **192.168.1.2**

  Key: **radiuskey**

- Click **OK** to return to the NAC policy servers screen.
- Click **Next**.

Figure 8. Add NAC Policy Server

[3] Provide the information the router uses to contact the NAC policy server (or RADIUS server). Each NAC policy server that you specify must have Cisco Secure ACS Software version 3.3 installed and configured.



4. For the NAC Exception List in this example, add the printer 192.168.150.2 to the list, so the printer is exempt from the NAC validation process.

   - Click the **Add…** button. The **Add to the Exception List** dialog displays:

     Type: **IP address**

     Address: **192.168.150.2**

   - Policy: click the **…** button and select **Create and apply a new policy**.

   - The **Add Exception Policy** dialog displays:

     - Name: **NAC-EL**
     - Access Rule: click the **…** button and select **Create a new rule(ACL) and select**.
     - The **Add a Rule** dialog is displayed:
       - Name: **NAC-acl**
       - Type: **Extended Rule**

- Description: **ACL for NAC exception list**
- Click **Add…**; the **Add an Extended Rule Entry** dialog appears. Deny any traffic if the traffic is not found valid in NAC policy server.

  Action: **Permit**

  Description: **ACL for NAC exception list**

  Source Host/Network Type: **Any IP Address**

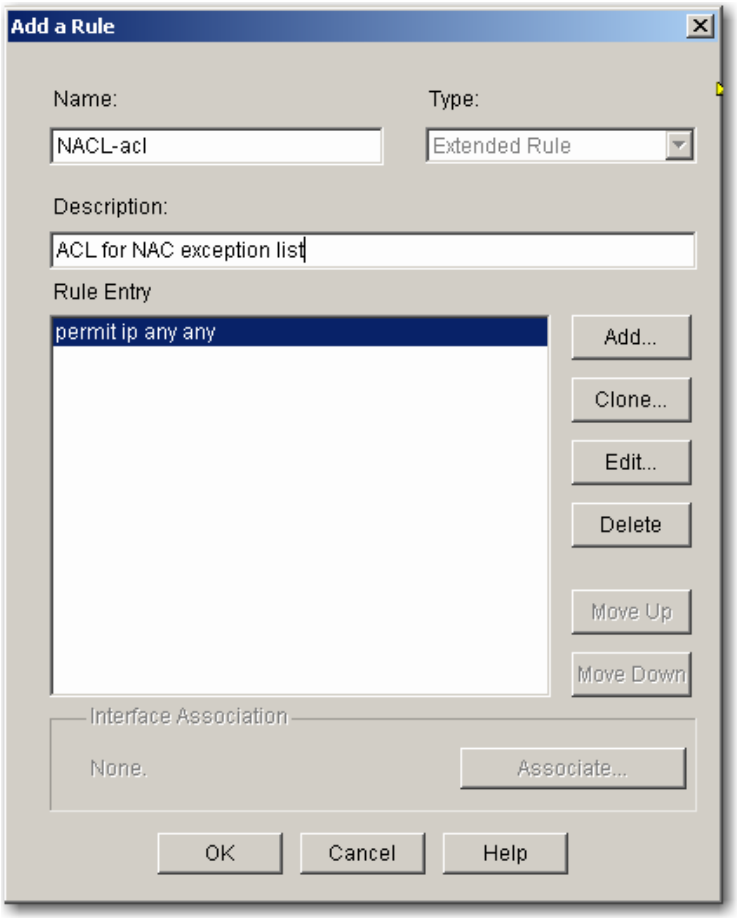
  Destination Host/Network Type: **Any IP Address**

  Protocol and Service: **IP/any**

  Click **OK** to build the rule.

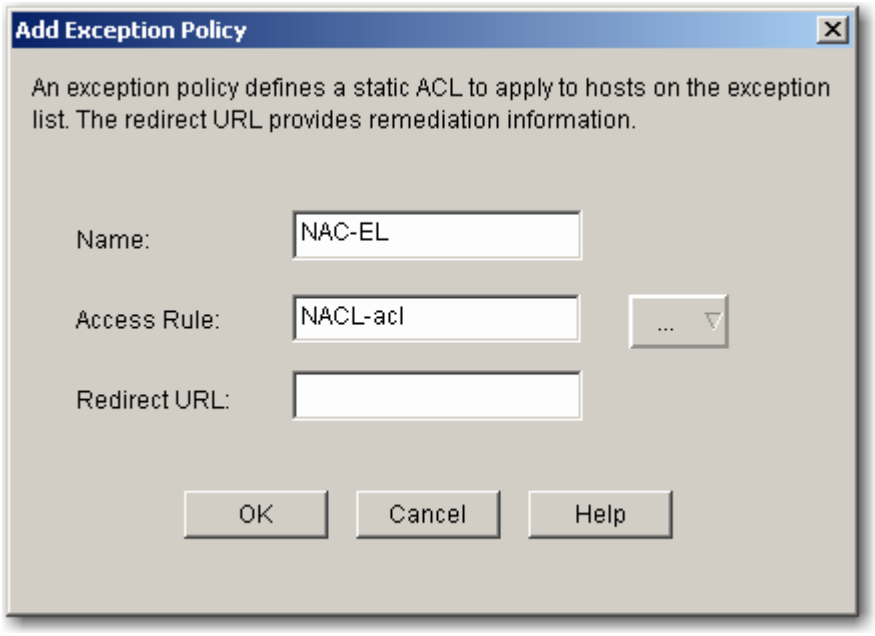
§ You will be directed back to the **Add a Rule** dialog (Figure 9). Click **OK** to build the rule.

Figure 9. Add a Rule



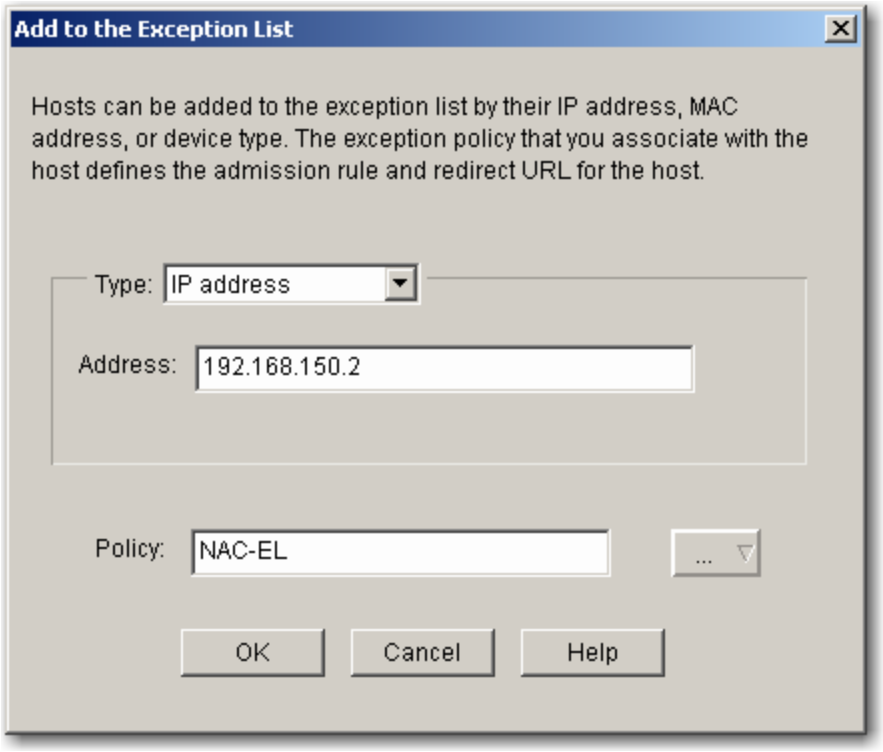
- You will be directed back to the **Add Exception Policy** dialog (Figure 10). In this example**,** leave **Redirect URL** blank. Click **OK** to build the exception policy.

Figure 10. Add Exception Policy



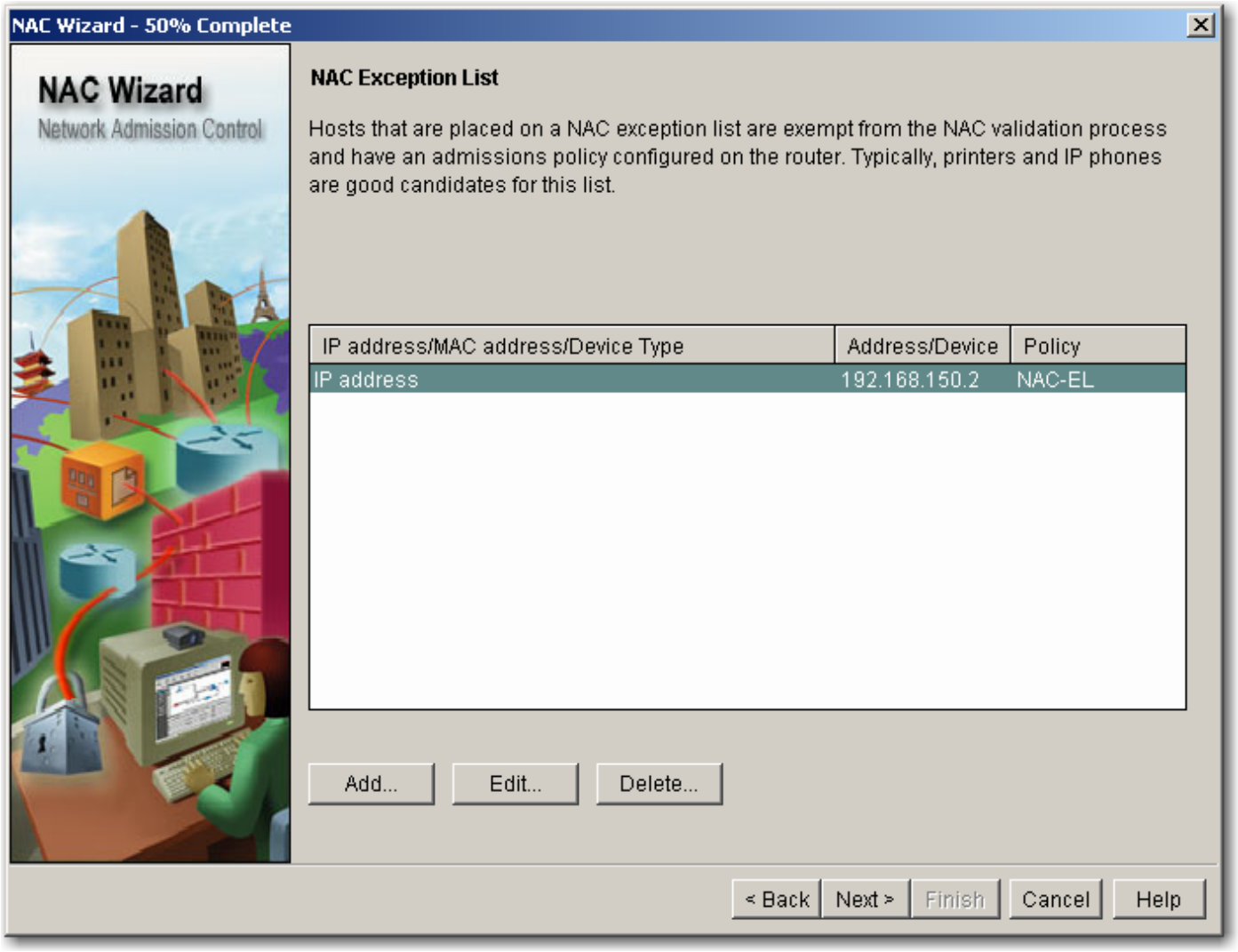
- You will be directed back to the **Add to the Exception List** dialog (Figure 11). Click **OK** to build the exception list.

Figure 11. Add to the Exception List



You are directed back to the **NAC Exception List**[4] dialog (Figure 12). Click **Next**.

Figure 12. NAC Exception List

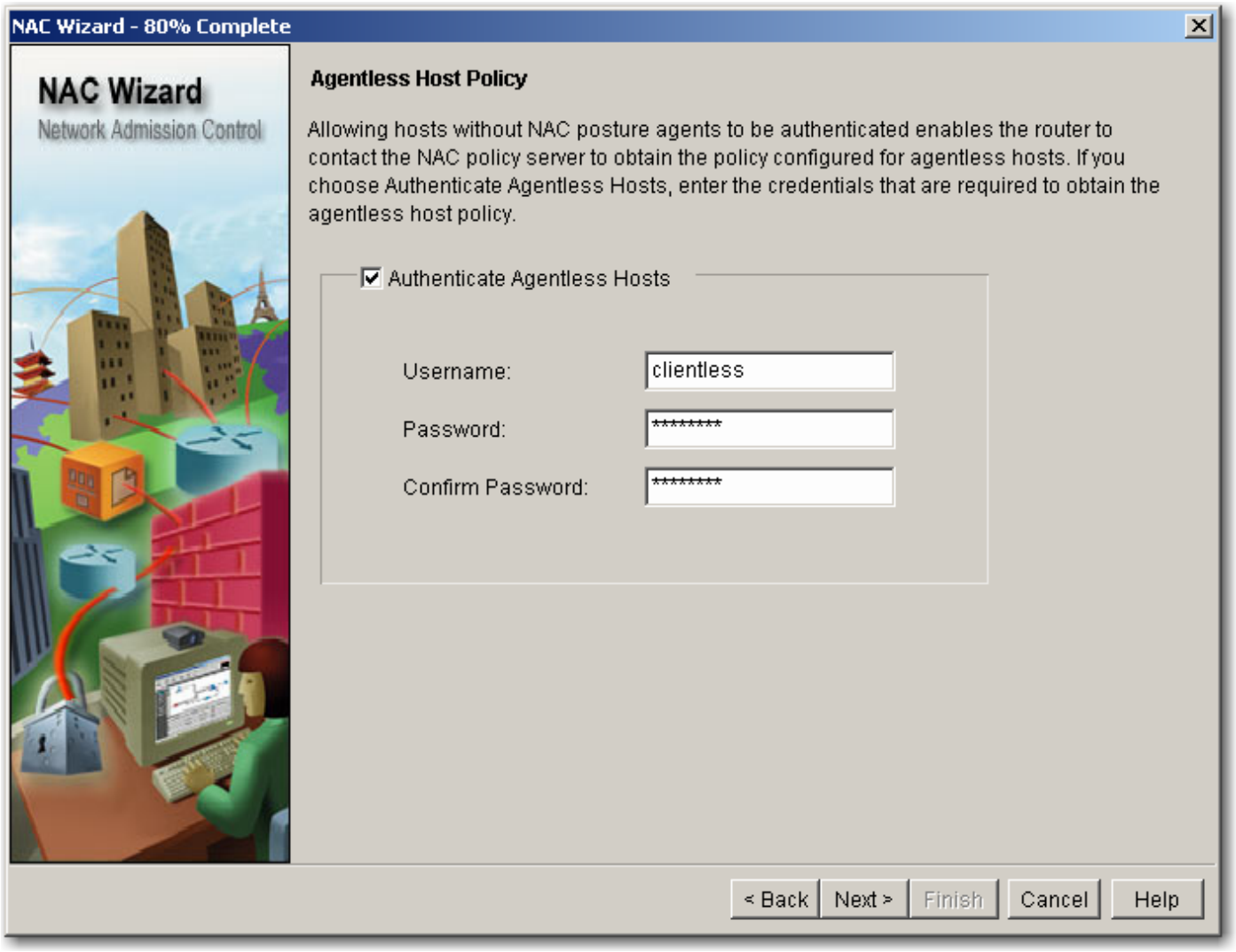


5. For Agentless Host Policy, enter the credential of the agentless hosts[5] (Figure 13), then click **Next**.
   - Check **Authenticate Agentless Hosts**
   - User name: **clientless**
   - Password: Enter **clientless** for this lab

[4] If the host's IP address is dynamic, use its MAC address. The NAC exception policy may not work properly if host IP addresses change. Usually the known incompliant hosts, such as printers and IP phones, are added in the Exception List.

[5] Enter the credentials of the agentless hosts defined in the NAC policy server (collect the information from your system administrator). Usually, the hosts without Cisco Trust Agent are added to the Agentless Host Policy. When a device is configured on both the Exception List and the Agentless Host Policy, the Exception List takes precedence.

Figure 13. **Agentless Host Policy**

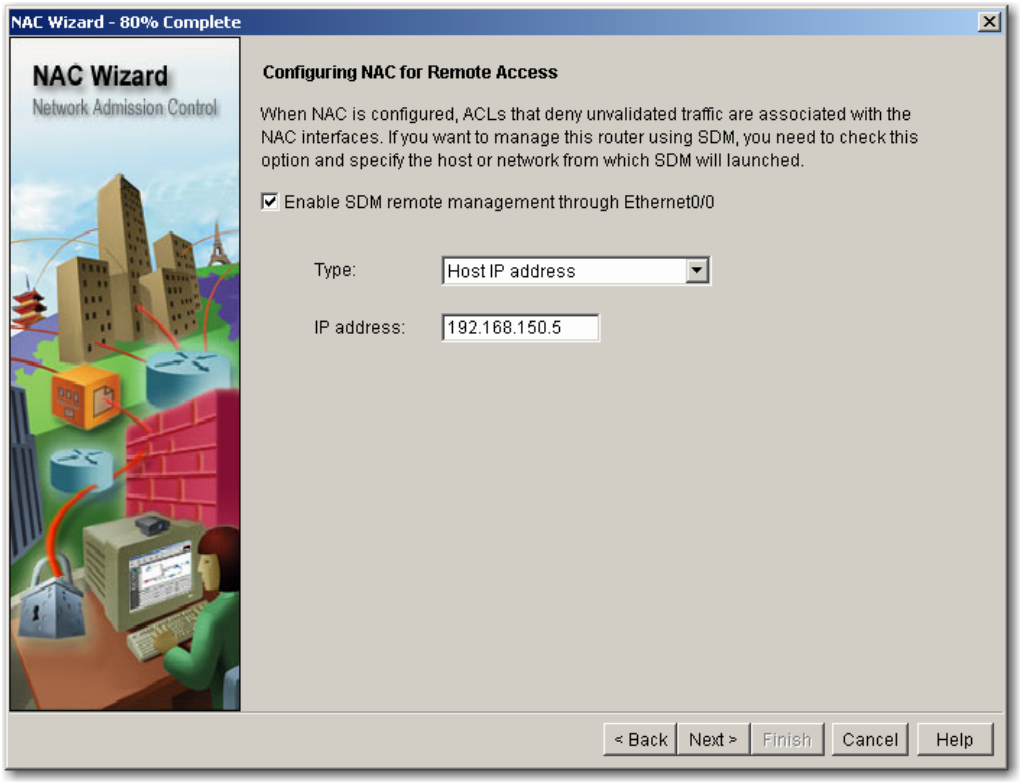


6. Configuring NAC for Remote Access (Figure 14) allows you to modify the ACLs that NAC configuration creates so that Cisco SDM traffic will be permitted. Specify the hosts that must be able to use Cisco SDM to access the router. In this example, we allow Cisco SDM traffic from 192.168.150.5 (Note: Remote access is not part of NAC configuration. Consult your system administrator for information).

   Click **Next** to finish the NAC configuration. Cisco SDM checks the existing ACLs applied to the NAC interfaces to determine if they block any traffic used by the NAC validation process. You will be prompted by **Modify Interface ACL** dialog. You can use Cisco SDM to modify the ACL to allow the traffic listed.

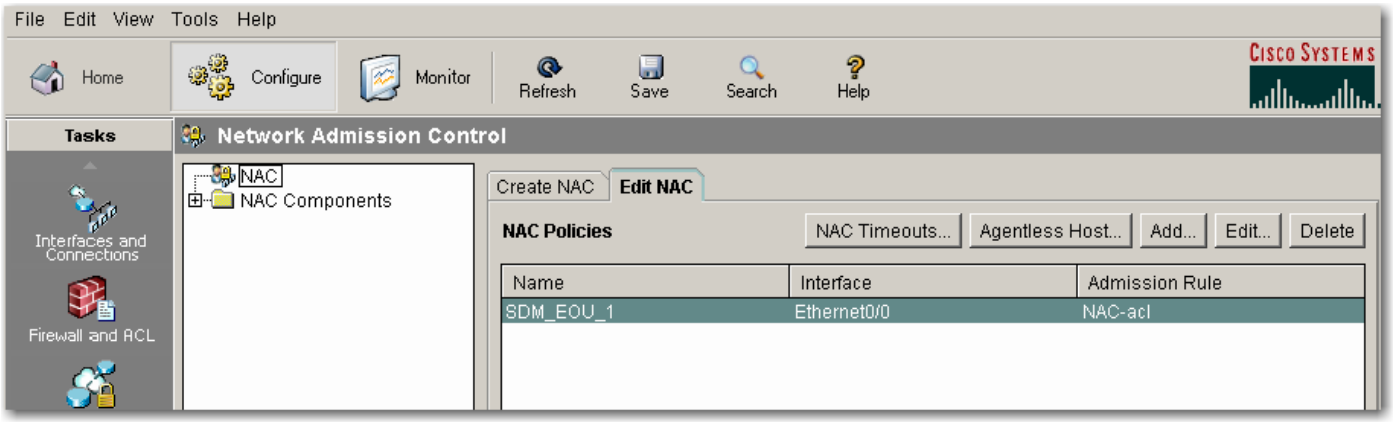
   Click **Finish** on the summary of the configuration dialog if you are satisfied with the configuration.

Figure 14. **Configuring NAC for Remote Access**



7. You will be redirected to the **Edit NAC** page (Figure 15) when the configuration is delivered to the router.

Figure 15. Network Admission Control/Edit NAC



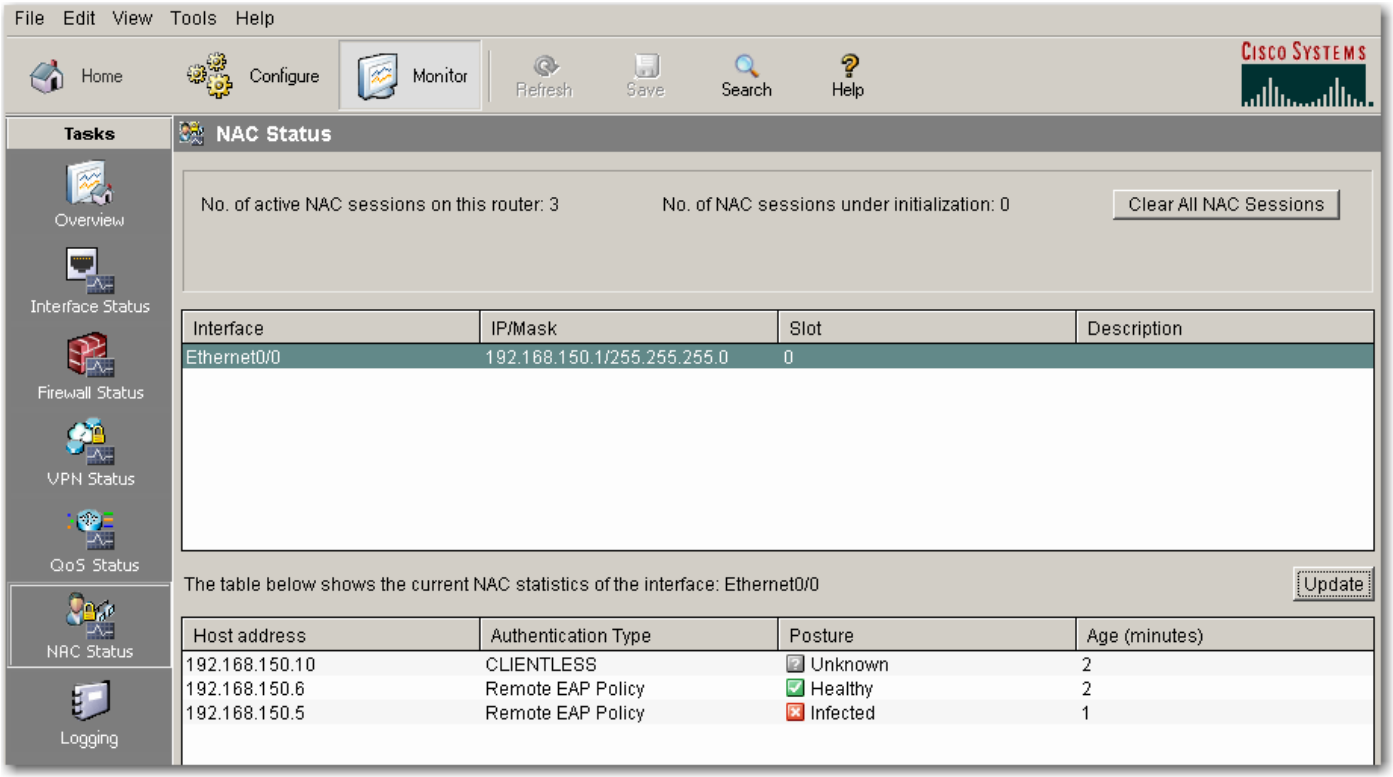
The NAC policy created by Cisco SDM is named SDM_EOU_1 and is applied to interface Ethernet0/0 with the admission rule named NAC-acl. You can check and modify the NAC timeout values the router is to use for EAPoUDP[6] communication with network hosts by clicking **NAC Timeouts…**

[6] EAPoUDP: EAP over User Datagram Protocol; sometimes shortened to EoU. The protocol used by the client and a network access device to perform posture validation.

Monitoring

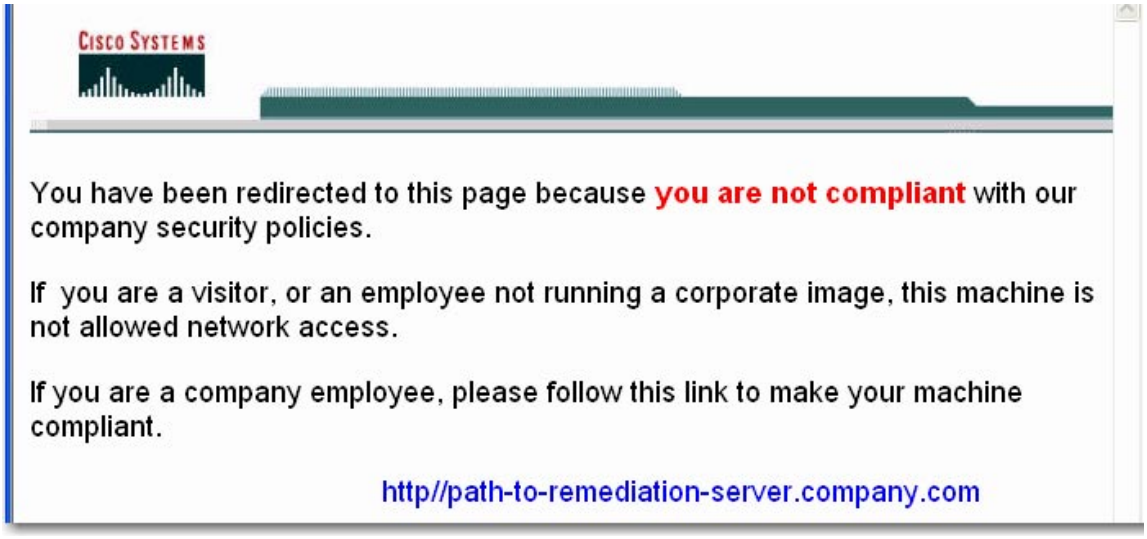
Click **Monitor** and select **NAC Status** to view the posture status. Select the NAC-enabled interface from the upper panel. The NAC statistics will be shown in the lower panel. In this example, click on **Ethernet0/0** on the upper panel. The lower panel (Figure 16) is displayed (Note: click **Update** to reflect the current NAC statistics).

Figure 16. NAC Status



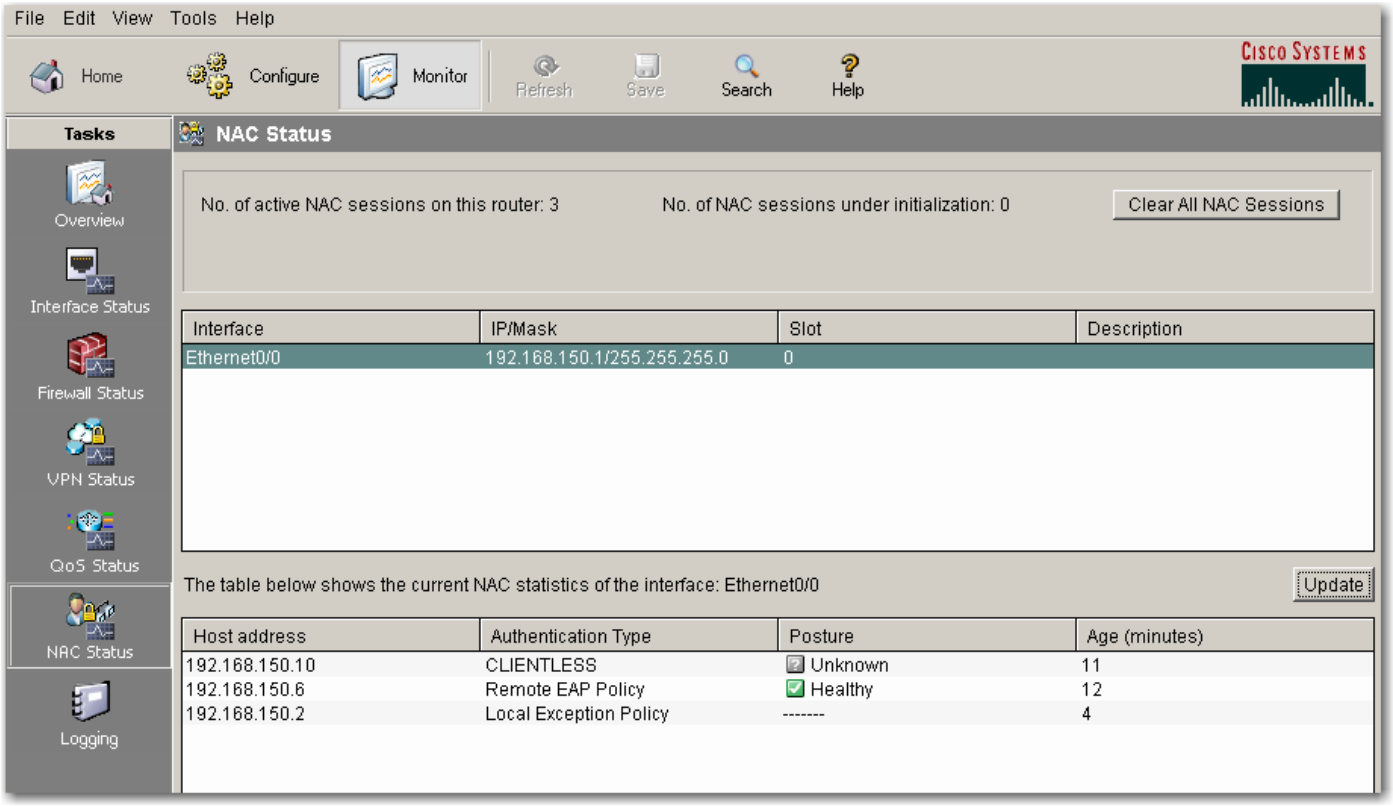
- Host 192.168.150.6 is authenticated by Remote EAP Policy. The host is company security policy-compliant, and the posture token returned from the NAC policy server is Healthy. Host 192.168.150.6 is allowed to access the network.
- Host 192.268.150.5 is authenticated by Remote EAP Policy, but the host is not company security policy-compliant, and the posture token returned from the NAC policy server is Infected. Host 192.168.150.5 is denied to access the network.
- Host 192.168.150.10 is detected with no Cisco Trust Agent installed by the network access device, and the posture token returned from the NAC policy server is Unknown (Note: Check the security profile defined for **posture token = Unknown** in the NAC policy server for the action. In this example, the action defined in the NAC policy server is to redirect HTTP traffic to a warning page [Figure 17]).

Figure 17. **URL Redirect**



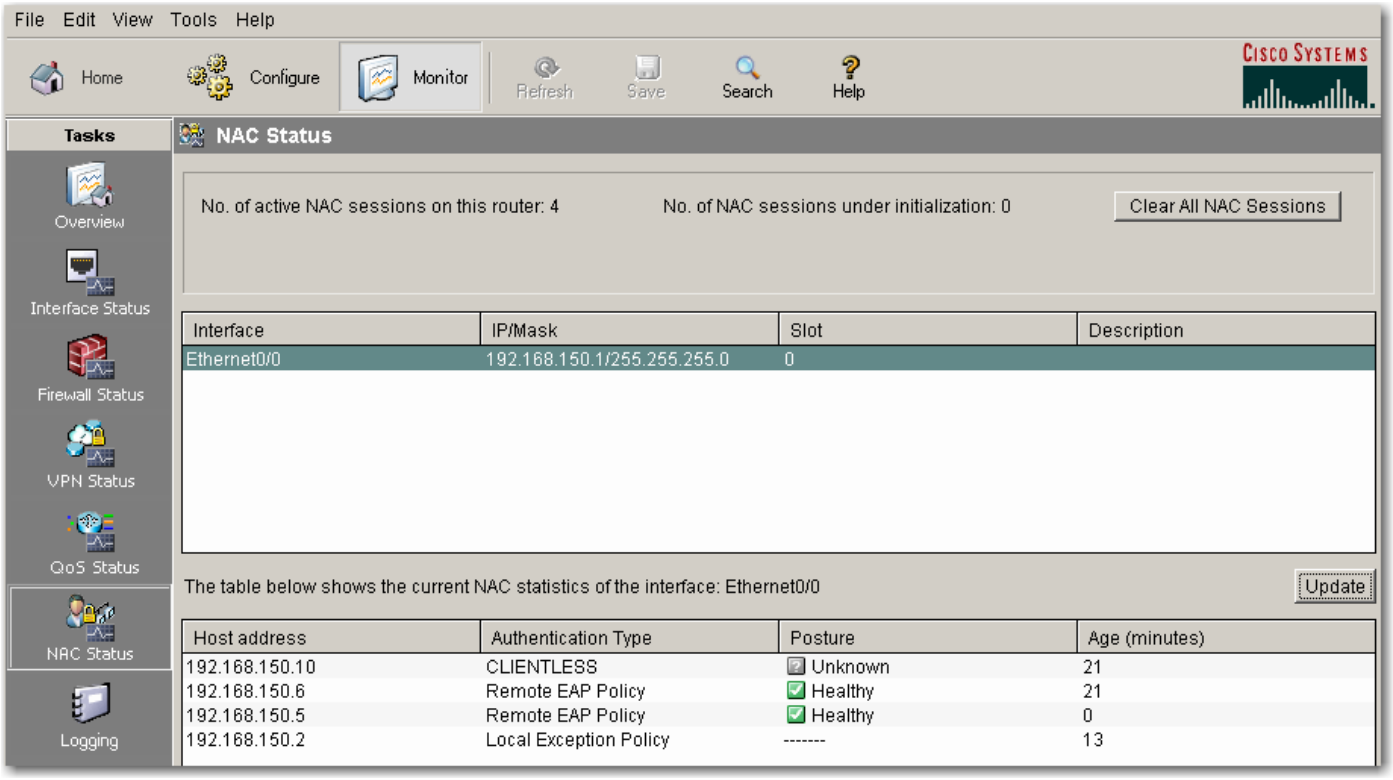
Click the **Update** button to update the NAC statistics. In this example, the updated status (Figure 18) shows that the infected host 192.168.150.5 is removed from the network and that the printer 192.168.150.2 is online and exempt from NAC posture validation.

Figure 18. **Updated NAC Status**



You can restart a revalidation manually by clicking **Clear All NAC Sessions**. Figure 19 shows that host 192.168.150.5 is EAP-authenticated and compliant after the host installed required software.

Figure 19. Updated NAC Status



In summary, by using the Cisco SDM, users can quickly deploy a network access device to support a NAC solution.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico• The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA