CANAC

Implementing Cisco NAC Appliance

Version 2.1

Lab Guide

Editorial, Production, and Web Services: 02.26.07

Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Lab Guide

Overview

This guide presents the instructions and other information concerning the lab activities for this course.

Note This lab assumes that the Cisco NAS and the Cisco NAM software have been installed and that the Cisco NAC Appliance database has been repopulated with the required data. Therefore, the Cisco NAS and Cisco NAM can now be configured using the student lab. The instructor or remote lab support personnel carried out these activities prior to the start of this lab.

Outline

This guide includes these activities:

- Lab 1-1: Preparing the Cisco NAM to Support Web-Based Administration Console Configuration
- Lab 2-1: Configuring User Roles
- Lab 3-1: Adding an In-Band Virtual Gateway Cisco NAS to the Cisco NAM
- Lab 3-2: Configuring the Microsoft Windows Active Directory SSO Feature on the Cisco NAC Appliance
- Lab 3-3: Configuring the Cisco VPN SSO Feature on the Cisco NAC Appliance
- Lab 4-1: Configuring the Cisco NAA
- Lab 4-2: Configuring an HA In-Band VPN Cisco NAC Appliance Solution
- **Lab 3-4: Adding an Out-of-Band Virtual Gateway Cisco NAS to an HA Cisco NAC Appliance Deployment
- **Lab 3-5: Configuring SNMP, Switch, and Port Profiles for an Out-of-Band Cisco NAC Appliance Deployment

Note **Check with your instructor for the sequence of labs for your course. The sequence above is the suggested sequence if all of the labs are to be done. The first number of the lab refers to the lesson in which the instruction for the lab activity can be found.

Lab 1-1: Preparing the Cisco NAM to Support Web-Based Administration Console Configuration

Complete this lab activity to practice what you learned in the related module. Your instructor will provide the login and password for your pod. Refer to Appendix A for cabling and IP addressing details.

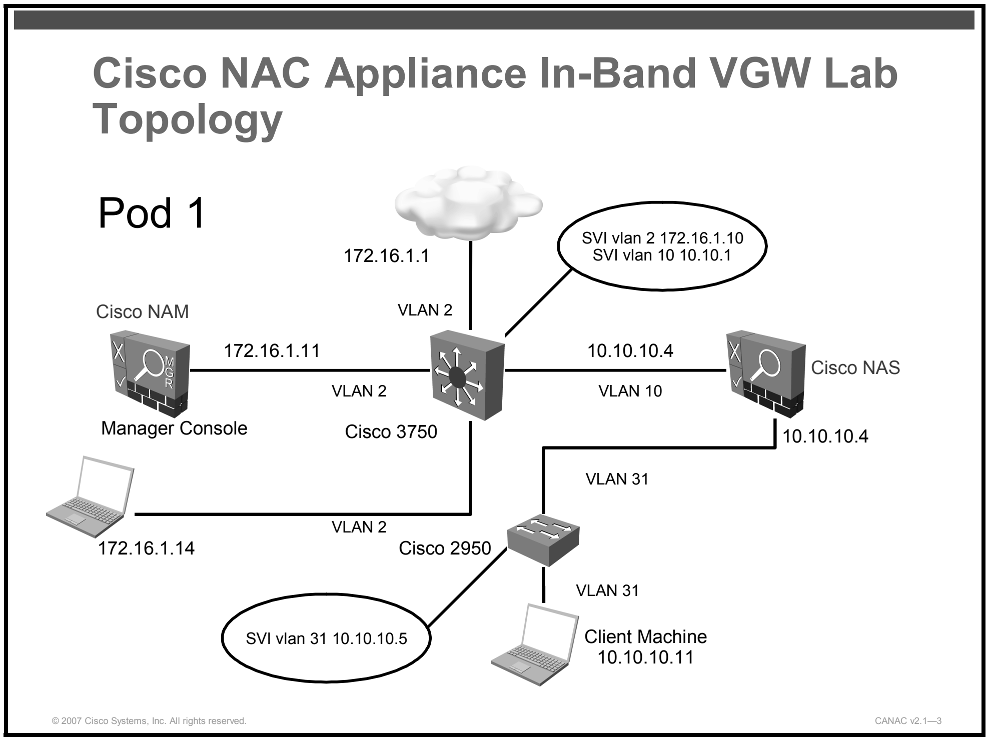
Activity Objective

In this activity, you will access the Cisco NAM web-based administration console. After completing this activity, you will be able to meet these objectives:

- Confirm the time on the lab components
- Navigate to the Cisco NAM web-based administration console
- Log onto the Cisco NAM web-based administration console

Visual Objective

The figure shows the topology of the CANACv2.1 in-band VGW Cisco NAC Appliance lab.



Cisco NAC Appliance In-Band VGW Lab Topology

CANAC v2.1—3

Required Resources

These are the resources and equipment that are required to complete this activity:

- Internet connection
- Correctly configured CANACv2.1 remote student lab
- Cisco NAM HA licenses

Command List

There are no CLI commands used in this activity. All tasks are performed from the Cisco NAM console menus.

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Confirm the Time on the Lab Components

In this task, you will log onto the CANACv2.1 remote student lab and confirm the time on the lab components. If the dates on the components differ, the instructor will provide the commands to enter the correct date.

Note Because your lab may be different than the CANACv2.1 remote student lab topology, found in Appendix A, the instructor may use this lab to familiarize you with how to connect to and navigate around the lab used in your class.

Activity Procedure

Complete these steps:

Note The Cisco NAC Appliance uses SSL to communicate; consequently, it is important that all components in the lab have the same date and time.

Step 1 There are two Cisco NAM servers in the CANACv2.1 remote student lab. Log onto the console of each Cisco NAM and confirm the time. Type **root** for the username and **cisco123** for the password.

Note Your instructor will provide the login and password for your pod.

Step 2 Type **Date** and make a note of the date and time.

Step 3 Log onto the console of the Cisco NAS.

Step 4 Type **root** for the username and **cisco123** for the password.

Step 5 Type **Date** and make a note of the date and time.

Activity Verification

You have completed this task when you attain this result:

- The date and time on Cisco NAM and Cisco NAS are the same.

Task 2: Navigate to the NAM Web-Based Administration Console

In this task, you will open the Cisco NAM web-based administration console. Recall that to log onto the Cisco NAM PC or the client machine, you will use the username “administrator” and the password “cisco”.

Activity Procedure

Complete these steps:

Step 1 Open a browser and navigate to the Cisco NAM web-based administration console, **`https://172.16.1.11/admin`**

Note If you are using the CANACv2.1 remote student lab topology, you must start a VPN connection to the manager machine. Once you have made this connection, you can either use the Microsoft Remote Desktop application to access the manager machine's browser or use the browser on your own machine.

Step 2 Click the **Yes** button on all Security Alert dialog boxes.

Note The Cisco NAM web-based administration console should open.

Step 3 In the PAK section of the screen, click the **Browse** button and navigate to where your instructor has put the license keys for your pod.

Step 4 Enter the license keys for your pod in the Enter Product License field. Reenter the license key for your pod in the first license key field and click **Enter**. There are two license keys, one for the Cisco NAC Appliance failover or high-availability features and one for the Cisco NAC Appliance out-of-band server features.

Tip Your instructor will provide you with the license keys.

Activity Verification

You have completed this task when you attain these results:

- The Cisco NAM web-based administration console opens with the login form displayed.
- If the license keys are correct, the Cisco NAM administration console displays the Monitoring > Summary page.

Task 3: Log onto the Cisco NAM Web-Based Administration Console

In this task, you will log onto the Cisco NAM web-based administration console.

Activity Procedure

Complete this step:

Step 1 Enter **admin** as the administrator login and **cisco123** as the administrator password in the Cisco NAM web-based administration console.

Step 2 Log out of the Cisco NAM and now log onto the Cisco NAS using the URL https://10.10.10.4/admin

Step 3 Enter **admin** as the username login and **cisco123** as the administrator password in the Cisco NAM web-based administration console.

Activity Verification

You have completed this task when you attain this result:

- The Monitoring > Summary page of the Cisco NAM web-based administration console appears.
- The Cisco NAS web-based console opens. Notice how similar the Cisco NAS web-based GUI is to the Cisco NAM.

Prepare for the next lab:

- Log out of the Cisco NAS.

Lab 2-1: Configuring User Roles

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will create user roles, apply traffic control policies to user roles, create new local users, and assign user roles to these users. After completing this activity, you will be able to meet these objectives:

- Configure a default user page
- Create user roles on the Cisco NAM
- Create an IP-based traffic control policy for each user role
- Configure new users

Visual Objective

There is no visual objective for this lab.

Required Resources

These are the resources and equipment required to complete this activity:

- Internet connection
- Correctly configured CANACv2.1 remote student lab

Command List

There are no CLI commands used in this activity. All tasks are performed from the Cisco NAM console menus.

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Configure Default User Page

In this task, you will configure the default user page to allow all web login users or Cisco NAA users to authenticate. For the purposes of this lab, a simple user login page is required.

Activity Procedure

Complete these steps:

Step 1 Choose **Administration > User Pages > Login Page**.

Step 2 Click the **Add** tab link. The Add Login Page form appears.

Step 3 Click **Add** to accept the default settings ("*").

Step 4 Explore the user page you have configured. Use the Edit and View features found at the **Administration > User Pages > Login Page** location.

Activity Verification

You have completed this task when you attain this result:

- On the Administration > User Pages > Login Page > List, you see these results:

```
"VLAN ID = *″ , ‶Subnet = *″ and ‶OS = ALL"
```

Note You can modify the configuration of the page later by clicking **Edit** on the General, Content, and Style pages.

Task 2: Create New User Roles on the Cisco NAM

In this task, you will create new user roles on the Cisco NAM. You will create the new user roles ("Employee" and "Consultant") using the User Management menu of the Cisco NAM.

Activity Procedure

Complete these steps to create the new roles:

Step 1 Choose **User Management > User Roles > New Role**. The New Role form appears.

Step 2 Enter **Employee** in the Role Name field.

Step 3 Enter **Employee Role** in the Role Description field.

Step 4 Click **Create Role** to accept all existing default settings.

Step 5 Choose **User Management > User Roles > New Role**. The New Role form appears.

Step 6 Enter **Consultant** in the Role Name field for the second role type.

Step 7 Enter **Consultant Role** in the Role Description field for the second role type.

Step 8 Click **Create Role** to accept all existing default settings.

Activity Verification

You have completed this task when you attain these results:

- The new roles appear in the User Management > User Roles > List of Roles tab.
- On the List of Roles tab, the properties displayed for the new roles are correct.

Task 3: Create an IP-Based Traffic Control Policy for a User Role

In this task, you will create an IP-based traffic control policy for the new user role.

Activity Procedure

Complete these steps:

Step 1 Choose **User Management > User Roles > List of Roles**.

Step 2 Click the **Policies** button for the Employee role. The User Management > User Roles > Traffic Control > IP form for the Employee role appears.

Step 3 Click the **Add Policy** link to accept the Untrusted > Trusted direction. The Add Policy form for the role appears.

Step 4 Ensure that **Allow** is checked as the Action.

Step 5 Choose **ALL TRAFFIC** from the Category drop-down menu.

Step 6 Click **Add Policy**.

Step 7 Choose **User Management > User Roles > List of Roles**.

Step 8 Click the **Policies** button for the Consultant role. The User Management > User Roles > Traffic Control > IP form for the Consultant role appears.

Step 9 Click the **Add Policy** link to accept the Untrusted > Trusted direction. The Add Policy form for the role appears.

Step 10 Choose **ALL TRAFFIC** from the Category drop-down menu.

Step 11 Click **Add Policy**.

Activity Verification

You have completed this task when you attain these results:

- The new traffic control policy appears in the User Management > User Roles > Traffic Control IP tab link.
- The properties displayed for the new traffic control policy are correct.
- The Employee role is now configured to allow all traffic from in-band users in the role once they are authenticated and certified.
- The Consultant role is configured to allow all traffic from in-band users in the role once they are authenticated and certified.

Note Cisco NAC Appliance traffic policies only apply for in-band traffic to and from client machines.

Task 4: Configure New Users

In this task, you will configure new users. The new users are employees who access the network locally and consultants who access the network from remote sites.

Note The Cisco NAC Appliance Network Scanning feature scans consultant systems.

Activity Procedure

Complete these steps:

Step 1 Choose **User Management > Local Users > New Local User**.

Step 2 Enter **cisco** in the User Name field.

Step 3 Enter **cisco123** in the Password field.

Step 4 Enter **cisco123** again in the Confirm Password field.

Step 5 Enter **Cisco Employee** in the optional Description field.

Step 6 Choose the **Employee** user role from the Role drop-down menu.

Step 7 Click **Create User**.

Step 8 Choose **User Management > Local Users > New Local User** to add a second user.

Step 9 Enter **consultant** in the User Name field.

Step 10 Enter **con123** in the Password field.

Step 11 Enter **con123** in the Confirm Password field.

Step 12 Enter **Outside consultant** in the optional Description field.

Step 13 Choose the **Consultant** user role from the Role drop-down menu.

Step 14 Click **Create User**.

Activity Verification

You have completed this task when you attain this result:

- The Cisco and consultant new users appear under User Management > Local Users > List of Local Users.

Lab 3-1: Adding an In-Band Virtual Gateway Cisco NAS to the Cisco NAM

Complete this lab activity to practice what you learned in the related module.

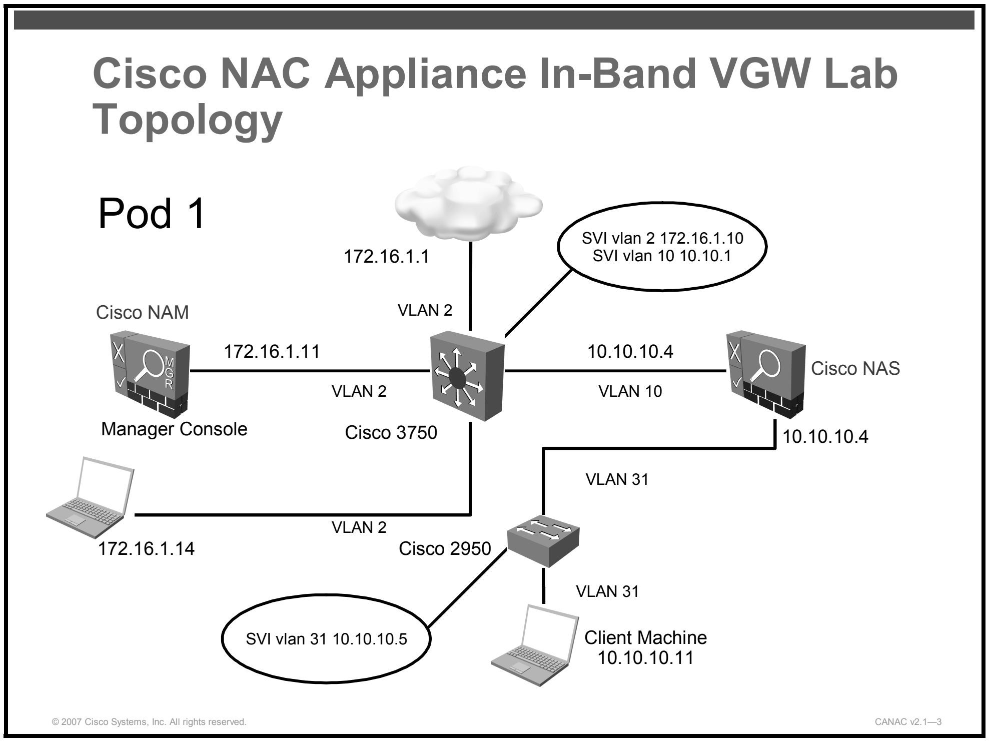
Activity Objective

In this activity, you will configure an in-band virtual gateway Cisco NAC Appliance deployment. After completing this activity, you will be able to meet these objectives:

- Add an in-band virtual gateway Cisco NAS to the Cisco NAM domain
- Configure in-band virtual gateway Cisco NAS settings
- Configure VLAN mapping for the in-band virtual gateway Cisco NAS

Visual Objective

The figure shows the topology of the in-band VGW VPN Cisco NAC Appliance lab.



Cisco NAC Appliance In-Band VGW Lab Topology

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3

Required Resources

These are the resources and equipment required to complete this activity:

- Internet connection
- Correctly configured CANACv2.1 remote student lab

Command List

There are no CLI commands used in this activity. All tasks are performed from the Cisco NAM console menus.

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Add an In-Band Virtual Gateway Cisco NAS to the Cisco NAM Domain

In this task, you will add an in-band virtual gateway Cisco NAS to the Cisco NAM domain.

Activity Procedure

Complete these steps:

Step 1 On the Cisco NAS server console interface, log on using **root** as the username and **cisco123** as the password.

Step 2 Enter **ifconfig eth1 down** to shut down the untrusted interface. This step helps to prevent a loop from being created while the Cisco NAS is configured.

Step 3 On the manager machine, using the Cisco NAM web-based administration console, click the **Device Management > CCA Servers** link from the left menu in the Cisco NAM web-based administration console.

Step 4 Click the **New Server** tab.

Step 5 In the Server IP Address field, enter the IP address of the Cisco NAS trusted interface: **10.10.10.4**.

Step 6 Enter **Cisco Student Lab** as the optional description of the Cisco NAS in the Server Location field.

Step 7 Choose **Virtual Gateway** from the Server Type drop-down menu.

Note If you forgot to add the Cisco NAM license key, the Out-of-Band Virtual Gateway option will not be available from the Server Type drop-down menu.

Step 8 Click the **Add the Cisco NAC Appliance Server** button.

Activity Verification

You have completed this task when you attain these results:

- The new server appears in the Device Management > CCA Servers > List of Servers page with a status of Connected.
- When your web browser is refreshed, the Cisco NAM correctly displays the connected in-band virtual gateway Cisco NAS.
- The IP address is 10.10.10.4.

Task 2: Configure the In-Band Virtual Gateway Cisco NAS Settings

In this task, you will configure the in-band virtual gateway Cisco NAS settings.

Activity Procedure

Complete these steps:

Step 1 Go to **Device Management** > **CCA Servers** > **List of Servers.**

Step 2 Click the **Manage** button for the Cisco NAS that you added. The management pages for the Cisco NAS appear.

Step 3 Click the **Network** tab. The Clean Access Server Type drop-down menu displays the virtual gateway type.

Step 4 Select the **Enable L3 Support** check box.

Step 5 Verify the settings in the Trusted Interface and Untrusted Interface fields with your instructor. These settings are entered during the initial software configuration process.

Step 6 Click the **Update** button to store the changes in the Cisco NAM database. You will reboot the server after you have mapped the VLANs.

Activity Verification

You have completed this task when you attain these results:

- The in-band virtual gateway Cisco NAS reboots successfully.
- The in-band virtual gateway Cisco NAS is listed in the Device Management > CCA Servers > List of Servers list.

Task 3: Configure VLAN Mapping for the In-Band Virtual Gateway Cisco NAS

In this task, you will configure VLAN mapping for the in-band virtual gateway Cisco NAS.

Activity Procedure

Complete these steps:

Step 1 On the Device Management > CCA Servers page, click the **Manage** button for the Cisco NAS that you added. The management pages for the Cisco NAS appear.

Step 2 Click the **Advanced** tab.

Step 3 Click the **VLAN Mapping** link.

Step 4 Check the check box for **Enable VLAN Mapping**.

Step 5 Click the **Update** button to store the changes in the Cisco NAM database**.**

Step 6 Enter the Auth VLAN ID of **31** in the Untrusted network VLAN ID field.

Step 7 Enter the Access VLAN ID of **10** in the Trusted Network VLAN ID field.

Step 8 Enter **Users on Edge Switch** as the optional description in the Description field.

Step 9 Click **Add Mapping**.

Step 7 Go to **Device Management > CCA Servers > List of Servers.**

Step 8 Click the **Reboot** icon to enable the changes.

Step 10 Once the Cisco NAS has rebooted, go to the Cisco NAS server console interface and log on, entering **root** as the username and **cisco123** as the password.

Step 11 Enter **ifconfig eth1 up** to enable the untrusted interface.

Prepare the Cisco NAS for the next lab:

Step 1 Go to the **Device > Management > Clean Access > General Setup** form.

Step 2 Click the **Agent Login** link.

Step 3 Choose **Employee** in the User Role drop-down menu.

Step 4 Check the **Require Use of Clean Access Agent** check box.

Step 5 Check the **Logoff Clean Access Agent Users from Network on Their Machine Logoff or Shutdown (for In-Band only)** check box

Step 6 Click the **Update** button.

Step 7 Log off the web-based Cisco NAM administration console, close the Microsoft remote desktop session, and disconnect your VPN connection with the manager machine.

Step 8 On the client machine, log on using the **cisco** username and **cisco123** password with the domain **Client_Machine (this computer).**

Step 9 Open a browser window and wait for the Cisco NAC Appliance web login page to appear.

Step 10 Choose **Run** from the download dialogue box.

Step 11 Accept all warnings and security alerts and log on using **cisco** for a username and **cisco123** for the password.

Step 12 Download and install the Cisco NAA when you are asked to. The Cisco NAA is needed for the next lab.

Step 13 Log onto the network using the Cisco NAA login dialogue box.

Step 14 Browse to a web page to verify that you have network connectivity to the trusted side.

Step 15 Close the browser window.

Step 16 Right-click the Cisco NAA icon in the Windows tray area.

Step 17 Choose **Logout** in the pop-up menu.

Step 18 Log off the client machine.

Activity Verification

You have completed this task when you attain these results:

- In the Device Management > CCA Servers > List of Servers > Manage > Advanced > VLAN Mapping subtab, the mapping of VLAN 31 -> 10 is listed at the bottom of the page.
- The employee role requires the use of the Cisco NAA.
- The client machine was able to log onto the network using the Cisco NAA.

Lab 3-2: Configuring the Microsoft Windows Active Directory SSO Feature on the Cisco NAC Appliance

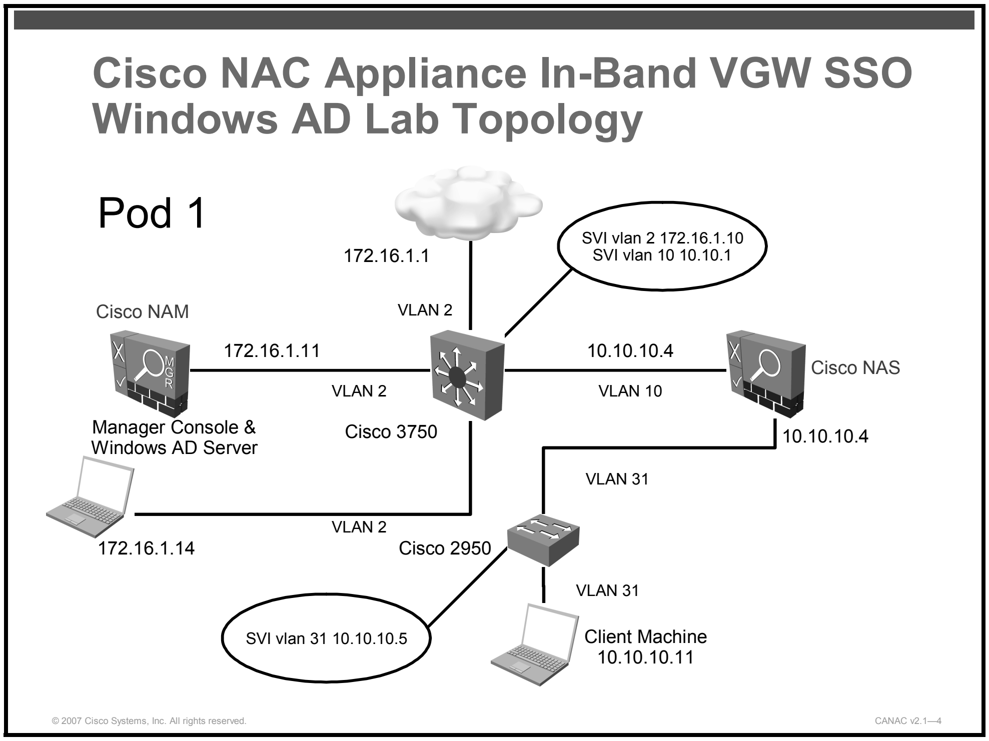
Activity Objective

In this activity, you will be able to use the Cisco NAC Appliance web-based administration console to configure the Microsoft Windows SSO feature on the Cisco NAC Appliance. After completing this activity, you will be able to meet these objectives:

- Confirm readiness to configure Windows Active Directory SSO
- Add Windows Active Directory SSO authentication server
- Configure traffic policies for the unauthenticated role
- Configure Windows Active Directory SSO on the Cisco NAS
- Confirm the Windows Active Directory server configuration
- Enable agent-based Windows SSO with Active Directory (Kerberos)
- Test Windows Active Directory SSO configuration using Cisco NAA

Visual Objective

The figure shows the topology of the in-band VGW Microsoft SSO Windows Active Directory Server lab.



Cisco NAC Appliance In-Band VGW SSO Windows AD Lab Topology

Required Resources

These are the resources and equipment required to complete this activity:

- Internet connection

- Correctly configured CANACv2.1 remote student lab

Command List

There are no CLI commands used in this activity. All tasks are performed from the Cisco NAM console menus.

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Confirm Readiness to Configure Windows Active Directory SSO

In this task, you will confirm that you are ready to configure Windows Active Directory SSO on the Windows Active Directory server and on the Cisco NAS.

Activity Procedure

Complete these steps:

Step 1 Reconnect to the manager machine and log on as the administrator using **cisco123** as the password.

Step 2 Confirm that the ktpass.exe file is present in the C:\Program Files\Support Tools folder. You will not be running the ktpass.exe program in this lab, but you need to know where the ktpass.exe program is located.

Step 3 Write down the IP address of the Windows Active Directory server (manager machine).

Step 4 Write down the FQDN of the Windows Active Directory server.

Step 5 Ensure time synchronization between the Windows Active Directory server and the Cisco NAS. If the times are not synchronized, synchronize them by changing the time on the manager machine; do not change the time on the Cisco NAM or Cisco NAS because that change would invalidate their SSL certificates.

Activity Verification

You have completed this task when you attain these results:

- The ktpass.exe file is present.
- The IP address and the name of the FQDN of the windows Active Directory server in the exact letter case as it was displayed is recorded.
- The time on the Windows Active Directory server is synchronized to the time on the Cisco NAS.

Task 2: Add Windows Active Directory SSO Authentication Server

In this task, you will add the Windows Active Directory SSO authentication server to the Cisco NAS.

Activity Procedure

Complete these steps:

Step 1 In a browser on the manager machine, open the Cisco NAM web-based administration console.

Step 2 Go to **User Management > Auth Servers > New**.

Step 3 Choose **Active Directory SSO** from the Authentication Type drop-down menu.

Step 4 Choose **Unauthenticated Role** from the Default Role drop-down menu.

Step 5 Type **WindowsADServer** in the Provider Name field to identify the Active Directory SSO authentication server on the list of authentication providers.

Step 6 Leave the LDAP Lookup Server drop-down menu at the default NONE setting.

Step 7 Type **Windows Active Directory Server for SSO** in the Description field.

Step 8 Click the **Add Server** button.

Activity Verification

You have completed this task when you attain this result:

- In User Management > Authentication servers > List, the new Windows Active Directory SSO authentication server has been added to the list.

Task 3: Configure Traffic Policies for the Unauthenticated Role

In this task, you will configure traffic policies for the traffic traveling between the Cisco NAS and the Active Directory server.

Activity Procedure

Complete these steps:

Step 1 Go to **User Management > Traffic Control.**

Step 2 Choose **Unauthenticated Role** from the Roles drop-down menu**.**

Step 3 Choose **Untrusted ->Trusted** from the Direction drop-down menu and click the **Select** button.

Step 4 Click the **Add Policy** link. The Add Policy form appears.

Step 5 Leave these fields at their defaults:

— **Action**: Allow

— **State**: Enabled

— **Category**: IP

— **Protocol**: TCP 6

— **Untrusted (IP/Mask:Port)**:* / * / *

Step 6 Enter this information in the Trusted (IP/Mask:Port) fields:

— The IP address of the Active Directory server: **172.16.1.14**

— The subnet mask for the Active Directory server: **255.255.255.255**.

— The UDP ports to open: **88,135,389,1025,1026**

Note The UDP ports are described here: TCP 88 (Kerberos), TCP 135 [remote-procedure call], TCP 389 (LDAP) or TCP 636 [LDAP with SSL], TCP 1025 (RPC)–non-standard, TCP 1026 (RPC)–non-standard

Step 7 Type **Open default Kerberos ports** in the Description field.

Step 8 Click **Add Policy**.

Activity Verification

You have completed this task when you attain this result:

- The new traffic policy appears in the list at the bottom of the User Management > Traffic Control form.

Task 4: Configure Windows Active Directory SSO on the Cisco NAS

In this task, you will configure the Cisco NAS with the Windows Active Directory domain information.

Activity Procedure

Complete these steps:

Step 1 Go to **Device Management > Clean Access Servers**.

Step 2 Click the **Manage** icon for the server with the IP address 10.10.10.4.

Step 3 Go to **Authentication > Windows Auth > Active Directory SSO**.

Step 4 Uncheck the check box for Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos).

Step 5 Enter the FQDN of the Windows Active Directory server in the Active Directory Server (FQDN) field.

Note The FQDN must be in the same case as the domain. If the domain name has mixed cases, enter mixed cases in the FQDN field.

Step 6 In the Active Directory Port field, leave the default of 88 for Kerberos.

Step 7 In the Active Directory Domain field, use uppercase letters to enter the domain name for the Key Distribution Center on the Windows Active Directory server.

Note The “Active Directory Domain” is equivalent to “Kerberos Realm” and must be in upper case.

Step 8 In the Account Name for CAS field, enter **nas1_primary** as the one-word name of the Cisco NAS user that you will create on the Windows server. Write this name down so that you can use it to configure the Windows Active Directory server using the correct username for the Cisco NAS.

Step 9 Enter **cisco123** as the password for the Cisco NAS in the Account Password for CAS field. Write this password down so that you can use it to configure the Windows AS server using the correct password for the Cisco NAS.

Step 10 From the Active Directory SSO Authentication server drop-down menu, choose the Windows SSO server that you configured on the Cisco NAM.

Note Leave the Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos) check box unchecked.

Step 11 Click the **Update** button.

Activity Verification

You have completed this task when you attain this result:

- The task completes without any error messages.

Task 5: Confirm the Windows Active Directory Server Configuration

In this task, you will navigate to the Windows Active Directory server to confirm that there is a Cisco NAS user and you will ensure that the Kerberos versions used by Cisco NAC Appliance and Windows Active Directory server will work together.

Activity Procedure

Complete these steps:

Step 1 Log on as the administrator on the Windows Active Directory server machine.

Step 2 Go to **Programs > Administration Tools > Active Directory Users and Computers**. Look on the manager desktop for a shortcut icon to the Active Directory Users and Computers management console.

Step 3 Open the Active Directory Management console.

Step 4 From the left pane of the Active Directory Users and Computers window, navigate to the Windows Active Directory server domain.

Step 5 Right-click the **Users** folder. In the menu that appears, select **New > User.** The New Object – User window opens.

Step 6 Look for the **nas1_primary** username.

Step 7 Right-click the **nas1 primary** username and select **Properties**.

Step 8 Click the **Account** tab and observe that the account name for the nas1_primary user is: **nas1_primary/2000_server.w2ksp4.adserver.com@W2KSP4.ADSERVER.**

Note The nas1_primary/2000_server.w2ksp4.adserver.com@W2KSP4.ADSERVER is the user for the CANAC v2.1 student lab. Your Cisco NAS username and server may be different.

Activity Verification

You have completed this task when you attain this result:

- The Cisco NAS user is a user in the Active Directory domain in the User folder in the Active Directory Users and Computers window.
- The Cisco NAS account name is: **nas1_primary/2000_server.w2ksp4.adserver.com@W2KSP4.ADSERVER**

Task 6: Enable Agent-Based Windows SSO with Active Directory (Kerberos)

In this task, you will enable Windows SSO with Active Directory (Kerberos) on the Cisco NAS.

Activity Procedure

Complete these steps:

Step 1 Open the Cisco NAM web-based administration console on the manager machine.

Step 2 Go to **Device Management > Clean Access Servers**.

Step 3 Click the **Manage** icon for the server with the IP address 10.10.10.4.

Step 4 Go to **Authentication > Windows Auth > Active Directory SSO**.

Step 5 Click the check box for **Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)**.

Step 6 Click **Update**.

Activity Verification

You have completed this task when you attain this result:

- The task completes without any error messages.
- In Device Management > Clean Access Servers > Manage, you see that the Windows Active Directory SSO service is started.

Task 7: Test Windows Active Directory SSO Configuration Using Cisco NAA

In this task, you will use the Cisco NAA on the client machine to log onto the Cisco NAS using the SSO feature of the Cisco NAC Appliance.

Activity Procedure

Complete these steps:

Step 1 Log onto the client machine using the **cisco** username and **cisco123** password with the domain **w2ksp4**.

Note If you see the Cisco NAA login screen, it is likely that the difference in time on the client machine and the time on the manager machine is greater than 5 minutes. Configure the time on the client machine to match the time on the manager machine.

Step 2 You will see the Cisco NAC Appliance Windows SSO dialogue box and you will be logged in to the network using your Windows credentials.

Step 3 Double-click on the **Shortcut to Kerbtray** short cut. Explore the Microsoft Kerberos ticket utility. Look for the Kerberos nas1_primary service ticket.

Activity Verification

You have completed this task when you attain this result:

- The Cisco NAA reports that you have successfully logged in to the network.

Prepare the Cisco NAS for the next lab:

- On the Cisco NAM, go to **Clean Access > Certified Devices > Certified List** and remove the **cisco** user from the certified list.

Prepare the client machine for the next lab:

- Change the client machine’s IP address and the Gateway address to the addresses needed for the VPN lab. Ask your instructor for the addresses used in your lab.
- Log out the cisco.w2ksp4.adserver.com user.

Lab 3-3: Configuring the Cisco VPN SS0 Feature on the Cisco NAC Appliance

Complete this lab activity to practice what you learned in the related module.

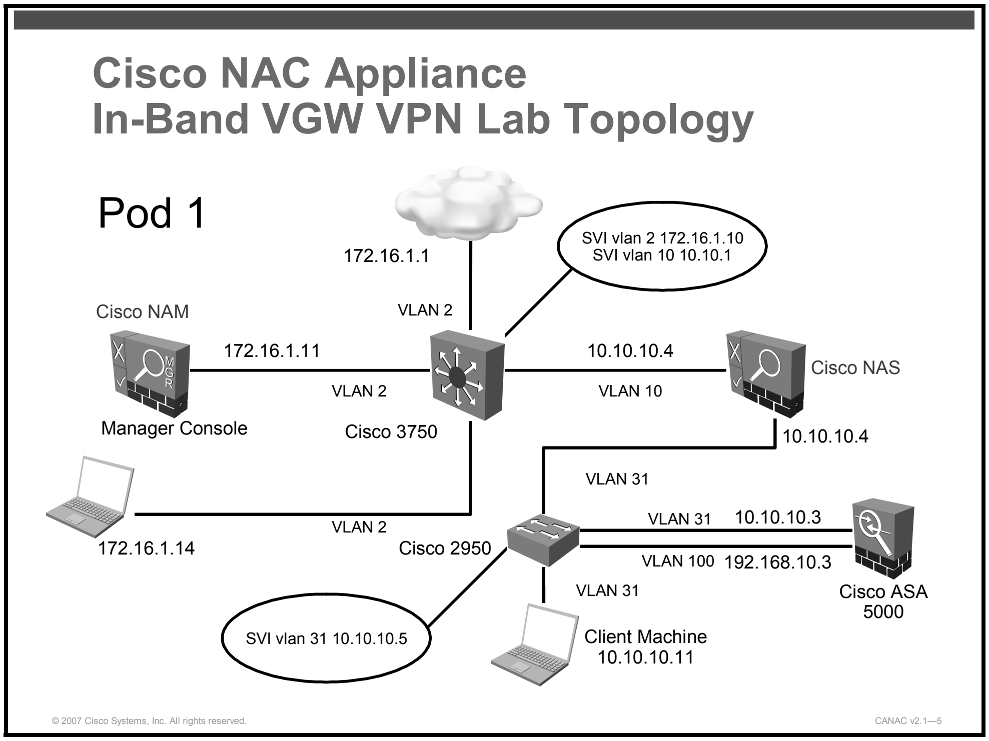
Activity Objective

In this activity, you will use the Cisco NAC Appliance web-based administration console to configure the Cisco NAS to use the Cisco VPN 3000 Series Concentrator. After completing this activity, you will be able to meet these objectives:

- Configure the filter for the Cisco ASA
- Add Cisco ASA 5520 as a floating device in the Cisco NAM
- Add Cisco VPN Auth Server to the Cisco NAM
- Map VPN users to roles in the Cisco NAM
- Enable SSO in the Cisco NAS
- Add Cisco ASA 5520 to the Cisco NAS
- Add an accounting server to the Cisco NAS
- Map the Cisco ASA 5520 to the accounting server
- Test the auto login as Cisco NAA

Visual Objective

The figure shows the topology of the in-band VGW VPN Cisco NAC Appliance lab.



Cisco NAC Appliance
In-Band VGW VPN Lab Topology

CANAC v2.1—5

Required Resources

These are the resources and equipment required to complete this activity:

- Internet connection
- Correctly configured CANACv2.1 remote student lab

Command List

There are no CLI commands used in this activity. All tasks are performed from the Cisco NAM console menus.

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Configure the Filter for the Cisco ASA

In this task, you will configure a filter to allow the Cisco ASA to be the authentication server on the trusted network. Cisco NAC Appliance for VPN requires this configuration in order for the server to communicate with the Cisco ASA 5520 on the untrusted network.

Activity Procedure

Complete these steps:

Step 1 Ensure that the client machine has the correct IP address and gateway for this lab as provided by your instructor.

Step 2 Go to **Device Management > Filters > Subnets**.

Step 3 Enter **10.10.10.3 / 32** for the Subnet Address/Netmask fields. This is the private IP address of the Cisco ASA.

Step 4 Enter **Access_Cisco_ASA_Management** in the Description field.

Step 5 Leave **allow** as the Access Type.

Step 6 Click **Add**.

Activity Verification

You have completed this task when you attain this result:

- The subnet filter with the Cisco ASA configuration details appears at the bottom of the Device Management > Filters > Subnets form.

Task 2: Add ASA 5520 as a Floating Device in the Cisco NAM

In this task, you will add the Cisco ASA 5520 as a floating device in the Cisco NAM.

Activity Procedure

Complete these steps:

Step 1 Log out of the manager machine and log onto the Cisco ASA 5520 using the console port and obtain the MAC address of the private interface FA 0/0.

Step 2 On the manager machine, go to **Device Management > Clean Access > Certified Devices > Add Floating Device**.

Step 3 Enter the private `<MAC> <type> <description>` for the Cisco ASA 5520 gateway in the Floating Device MAC Address field. For example:

```
00:12:D9:48:FB:0D 1 ASAVPN
```

Note Use the console interface on the Cisco ASA 5520 to determine the MAC address of the private interface of the Cisco ASA.

Recall these facts about the components of the Floating Device MAC Address field:

`<MAC>`

This is the MAC address from the private interface of the ASA 5520 for your pod.

`<type>`

Enter **1** for the device to never be considered certified.

`<description>`

Enter an optional description of the device.

Include spaces between each element and use line breaks to separate multiple entries.

Step 4 Click the **Add Device** button.

Activity Verification

You have completed this task when you attain this result:

- The Cisco ASA 5520 MAC address, type, and description appear at the bottom of the form.

Task 3: Add a Cisco VPN Auth Server to Cisco NAM

In this task, you will add a Cisco VPN Server authentication source to the Cisco NAM. This task supports VPN SSO when configuring Cisco NAC Appliance ASA 5520 integration.

Activity Procedure

Complete these steps:

Step 1 Go to **Device Management** > **CCA Server** > **Manage** > **Authentication** > **Windows Auth** > **Active Directory SSO.**

Step 2 Uncheck the **Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)** check box.

Step 3 Click the **Update** button to stop the Active Directory SSO module.

Step 4 Go to **User Management** > **Auth Servers.**

Step 5 Click the **Delete** icon for the WindowsADServer entry. You are now configuring the Cisco NAS to perform VPN SSO; the Windows Active Directory SSO is no longer used.

Step 6 Go to **User Management** > **Auth Servers** > **New**.

Step 7 Select **Cisco VPN SSO** from the Authentication Type drop-down menu.

Step 8 The Provider Name is Cisco VPN Server by default.

Step 9 Select **Unauthenticated Role** from the Default Role drop-down menu.

Note The Default Role is used if RADIUS mapping is not defined or set correctly or if RADIUS attributes are not defined or set correctly on the RADIUS server.

Step 10 Enter **For VPN SSO** in the Description field.

Step 11 Click **Add Server**.

Activity Verification

You have completed this task when you attain this result:

- The Cisco VPN server appears under User Management > Auth Servers > List.

Task 4: Map VPN Users to Roles in the Cisco NAM

In this task, you will map VPN users to specific roles in the Cisco NAM. You can use Auth Server Mapping Rules to map users to Cisco NAC Appliance roles based on attributes passed from the authentication server. Because RADIUS accounting packets pass user attributes, the Cisco NAM and Cisco NAS can use the RADIUS information passed from the Cisco VPN Server type to map client machines using the VPN services of the ASA 5520 to map users to roles.

Activity Procedure

Complete these steps:

Step 1 Go to **User Management > Auth Servers > Mapping Rules** and click the **Add Mapping Rule** link for the Cisco VPN server.
OR
Go to **User Management > Auth Servers > List of Servers**, click the **Mapping** button for the Cisco VPN Server and then click the **Add Mapping Rule** link for the Cisco VPN server.

Step 2 Select **Attribute** from the Condition Type drop-down menu.

Step 3 Leave the default of **Standard** in the Vendor drop-down menu.

Step 4 Leave the default of **Class** in the Attribute Name drop-down menu.

Step 5 Select **contains** from the Operator drop-down menu.

Step 6 Enter **Employee** in the Attribute Value field.

Note Be sure to use the same capitalization as you did for the role name.

Step 7 Click **Add Condition**. The condition appears at the bottom of the form.

Step 8 Select **Employee** from the Role Name drop-down menu.

Step 9 Leave **1** in the Priority drop-down menu.

Step 10 Enter **Employee mapping rule** in the Description field.

Step 11 Click **Add Mapping** to add this mapping to the server for the role. The new employee mapping appears under the Mapping Rules tab for the Cisco VPN server.

Step 12 Click the **Add Mapping Rule** link again while on this User Management > Auth Servers > Mapping Rules page (filtered for the Cisco VPN server).

Step 13 Select **Attribute** from the Condition Type drop-down menu.

Step 14 Leave the default of **Standard** in the Vendor drop-down menu.

Step 15 Leave the default of **Class** in the Attribute Name drop-down menu.

Step 16 Select **contains** from the Operator drop-down menu.

Step 17 Enter **Consultant** in the Attribute Value field.

Note Be sure to use the same capitalization as you did for the role name.

Step 18 Click **Add Condition**. The condition appears at the bottom of the form.

Step 19 Select **Consultants** from the Role Name drop-down menu.

Step 20 Leave **2** in the Priority drop-down menu.

Step 21 Enter **Consultant mapping rule** for the Description field.

Step 22 Click **Add Mapping** to add this mapping to the server for the role.

Activity Verification

You have completed this task when you attain this result:

- The employee and the consultant roles appear in the Mapping Rules form for the Cisco VPN server.

Task 5: Enable VPN SSO

In this task, you will enable VPN SSO on the Cisco NAS using the Cisco NAM web administration console.

Activity Procedure

Complete these steps:

Step 1 Go to **Device Management > CCA Servers**.

Step 2 Click the **Manage** button for the Cisco NAS server.

Step 3 Select **Authentication > VPN Auth > General** on the subtab menu.

Step 4 Check the **Single Sign-On** check box. This sets the Cisco NAS to process the user login via RADIUS accounting packets.

Step 5 Check the **Auto Logout** check box. This configures the Cisco NAM to remove the user from the Cisco NAM Online Users List when the RADIUS stop record is received (the record is sent when the user disconnects from the VPN).

Step 6 Leave the default port of **1813** for the RADIUS Accounting Port.

Step 7 Click the **Update** button to store the VPN SSO changes in the Cisco NAM database.

Note For the Cisco ASA and the Cisco NAC Appliance Release 4.0.0, the supported UDP port used for RADIUS accounting is 1813.

Activity Verification

You have completed this task when you attain this result:

- The acceptance of the last task is the activity verification.

Task 6: Add the Cisco ASA 5520 to the Cisco NAS

In this task, you will add the Cisco ASA 5520 to the Cisco NAS using the Cisco NAM web administration console.

Activity Procedure

Complete these steps:

Step 1 Go to **Device Management > CCA Servers**.

Step 2 Click the **VPN Concentrators** subtab menu option.

Step 3 Enter **Cisco ASA VPN SSO** as the name for the VPN concentrator in the Name field.

Step 4 Enter **10.10.10.3** in the IP Address field. This is the private IP address of the Cisco ASA.

Step 5 Enter **cisco123** in the Shared Secret field for the VPN concentrator.

Step 6 Reenter **cisco123** in the Confirm Shared Secret field.

Step 7 Enter **Cisco ASA VPN SSO** in the Description field.

Step 8 Click **Add VPN Concentrator**.

Activity Verification

You have completed this task when you attain this result:

- The Cisco ASA 5520 appears at the bottom of the VPN Concentrators form.

Task 7: Add an Accounting Server to the Cisco NAS

In this optional task, you will add an accounting server to the Cisco NAS using the Cisco NAM web administration console.

Note Tasks 7 and 8 are optional. Complete these tasks if your lab has a Cisco ACS accounting server configured on the manager machine.

Activity Procedure

Complete these steps:

Step 1 Click the **Accounting Services** subtab menu link.

Step 2 Enter **ACS Accounting** in the Name field.

Step 3 Enter **172.16.1.14** in the IP Address field.

Step 4 Enter **1813** in the Port field.

Note For the Cisco ASA and the Cisco NAC Appliance Release 4.0.0, the supported UDP port used for RADIUS accounting is 1813.

Step 5 Enter **2** in the Retry field.

Step 6 Enter **3** in the Timeout field.

Step 7 Enter **cisco123** in the Shared Secret field. Enter **cisco123** in the Confirm Shared Secret field.

Step 8 Enter **Cisco ACS on manager machine** in the Description field.

Step 9 Click the **Add Accounting Server** button.

Activity Verification

You have completed this task when you attain this result:

- The Cisco VPN accounting server appears at the bottom of the Accounting Services form.

Task 8: Map the Cisco ASA 5520 to the Accounting Server

In this optional task, you will map the Cisco ASA 5520 to the Cisco ACS accounting server using the Cisco NAM web administration console.

Activity Procedure

Complete these steps:

Step 1 Click the **Accounting Mapping** subtab menu link.

Step 2 Confirm the settings in the Accounting Mapping form.

Note The Cisco NAM will populate the fields in this form with the ASA 5520 information and the accounting server that you have configured.

Step 3 Click the **Add Entry** button.

Activity Verification

You have completed this task when you attain this result:

- The new mapping appears at the bottom of the Accounting Mapping form.

Task 9: Test the Auto Login Using the Cisco NAA

In this task, you will test the Cisco NAC Appliance VPN configuration by logging in as a user with the VPN client.

Activity Procedure

Complete these steps:

Step 4 Log onto the client machine using the **cisco** username and **cisco123** password with the domain **CLIENT_MACHINE (this computer)**.

Step 5 Change the IP addresses for the LAN and the gateway to the addresses for the VPN lab. Your instructor will tell you what these addresses are.

Step 6 Open the VPN client using the VPN client desktop icon, or right-click the taskbar icon and select **VPN Client** from the menu.

Step 7 Select **Employee** as the Connection Entry server and click **Connect**.

Step 8 Log on with username **cisco** and password **cisco123** and click **OK**. These credentials associate you in the Cisco NAC Appliance system with the Employee user role.

Step 9 You will see the Cisco NAA dialogue boxes appear and you will be logged in to the network.

Step 10 Open a browser and navigate to https://172.16.1.11/admin, which is the IP address of the Cisco NAM.

Activity Verification

You have completed this task when you attain these results:

- In the Cisco NAM web-based administration console, go to **Monitoring > Online Users**. The Online Users form shows that the Cisco user is logged in in the Employee role with the provider identified as the Cisco VPN.

Note With Auto Logout enabled, when the user disconnects from the VPN, the user is automatically removed from the Online Users list.

- Go to **Device Management > Clean Access > Certified Devices > Certified List**. Observe that the Certified Device List does not contain addresses for Cisco NAC Appliance Remote VPN/L3 Users. Recall that the Certified Device List includes users authenticated and certified based on a known Layer 2 MAC address. Refer to the Online In-band Users List for a list of authenticated users.

Prepare for the next lab:

- Remove the VPN SSO authentication server and the configuration.

Lab 4-1: Configuring the Cisco NAA

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will configure the Cisco NAA to scan for specific network threats. After completing this activity, you will be able to meet these objectives:

- Configure the General Setup tab to require the use of the Cisco NAA for the Employee user role
- Configure host policies for Cisco NAA
- Create checks and rules
- Create a requirement
- Associate requirements to rules and user roles
- Use the Role-Requirements form to associate requirements to a selected user role
- Verify Cisco NAA configuration

Visual Objective

There is no visual objective for this lab.

Required Resources

These are the resources and equipment required to complete this activity:

- Internet connection
- Correctly configured CANACv2.1 remote student lab

Command List

There are no CLI commands used in this activity. All tasks are performed from the Cisco NAM console menus.

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Configure General Setup

In this task, you will configure the General Setup tab to require the use of the Cisco NAA for the Employee user role.

Activity Procedure

Complete these steps:

Step 1 Choose **Device Management** > **Clean Access** > **General Setup** > **Agent Login.**

Step 2 Choose **Employee** from the User Role drop-down menu and leave the default setting ALL in the Operating System field.

Step 3 Check the **Require Use of Clean Access Agent** box.

Step 4 Leave all other options unchecked.

Step 5 Click the **Update** button to store the changes in the Cisco NAM database.

Activity Verification

You have completed this task when you attain this result:

- The updates are accepted.

Task 2: Configure Host Policies for Clean Access Agent

In this task, you will configure host policies for the Cisco NAA.

Activity Procedure

Complete these steps:

Step 1 Choose **User Management** > **User Roles** > **Traffic Control** > **Host.**

Step 2 In the Host-Based Policy page, choose **Temporary Role** from the drop-down menu and click **Select**.

Step 3 Click the **Add** button under the Trusted DNS Server section that has "*" already filled in the Trusted DNS Server field and "Any DNS Server" entered in the Description field.

Note By leaving the default setting (*) in its field and clicking the **Add** button, you have added a trusted DNS server.

Step 4 Scroll down to the Allow Host Name field and enter **www.cisco.com.** Leave the drop-down menu as equals and type **Cisco.com** in the description field.

Step 5 Click the **Add** button and then check the **Enable** check box.

Activity Verification

You have completed this task when you attain this result:

- An IP-based traffic policy allowing UDP traffic to the trusted network for the selected role appears under User Management > User Roles > Traffic Control > IP.

Task 3: Create Checks and Rules

In this task, you create checks and rules.

Activity Procedure

Complete these steps:

Step 1 Choose **Device Management > Clean Access > Clean Access Agent > Rules > New Check**.

Step 2 Ensure that the entry in the Check Category drop-down menu is Registry Check and that the entry in the Check Type drop-down menu is Registry Key.

Note In this case, the check will look for a registry key created by the update HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP2\KB835732\

Step 3 Enter a meaningful Check Name, such as **Windows_Security_Update_for_KB835732**.

Step 4 From the root key list, choose **HKLM** (HKEY_LOCAL_MACHINE) for the Registry Key.

Step 5 In the Registry Key field to the right of the HKLM drop-down menu, enter **SOFTWARE\Microsoft\Updates\Windows XP\SP2\KB835732.**

Tip As a shortcut, you can navigate to the tested key in the Microsoft Registry Editor (search for KB835732), select the key reference, and choose **Copy Key Name** from the Edit menu. After copying the key name, paste the key name into the registry key field. Remove any trailing spaces.

Step 6 Choose **Exists** from the Operator drop-down menu.

Step 7 Check the **Windows XP (All)** check box to set the operating system that the rule will check.

Note This step directs the Cisco NAC Appliance to perform the check only on computers running Windows XP.

Step 8 Choose the **Automatically Create Rule Based on this Check** check box.

Step 9 Click **Add Check**.

Activity Verification

You have completed this task when you attain these results:

- In the Device Management > Clean Access > Clean Access Agent > Rules > Rule list, the new check appears at the bottom of the Check List.
- A rule appears at the bottom of the list with suffix “-rule” under Device Management > Clean Access > Clean Access Agent > Rules > Rule List.

- When you click the **Edit** button for the new rule to bring up the Edit Rule configuration page, the new check is listed.

Task 4: Create a Requirement

In this task, you will create a requirement.

Activity Procedure

Complete these steps:

Step 1 Choose **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**.

Note The New/Edit Requirement form configures the name and type of the requirement, the operating system version that the requirement applies to, and the instructions, files, or links to be passed to the user.

Step 2 Choose **Link Distribution** from the Requirement Type list.

Note For the requirements that you create, this version number can be any value that helps you keep track of subsequent versions of the requirement.

Step 3 In the File Link URL field, enter **http://www.cisco.com**.

Step 4 Enter **Windows Security Update** in the Requirement Name field.

Step 5 Enter these statements in the Description field:
"Your system does not meet requirements. Click the Go To Link button and scan your computer for updates in the Windows Update page"

Step 6 Choose **Windows XP (All)** from the Operating System check boxes.

Step 7 Click **Add Requirement**.

Activity Verification

You have completed this task when you attain this result:

- The requirement appears in the Requirement List under Device Management > Clean Access > Clean Access Agent > Requirement.

Task 5: Associate Requirements to Rules and User Roles

In this task, you will associate requirements to rules and user roles.

Activity Procedure

Complete these steps:

Step 1 Choose **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**.

Step 2 From the Requirement Name drop-down menu, choose the **Windows Security Update** requirement.

Step 3 From the Operating System drop-down menu, choose **Windows XP**.

Step 4 Choose the **All Selected Rules Succeed** option in the Requirement Met If option list.

Step 5 Under Rules for Selected Operating System, check the check box for the **WindowsSecurityUpdate-KB835732-Rule** rule that was automatically created for your check.

Step 6 Click the **Update** button to store the changes in the Cisco NAM database.

Activity Verification

You have completed this task when you attain this result:

- The update is accepted.

Task 6: Associate the Requirement to a Selected Role

In this task, you will use the Role Requirements form to associate requirements to a selected user role.

Activity Procedure

Complete these steps:

Step 1 Choose **Device Management > Clean Access > Clean Access Agent > Role Requirements**.

Step 2 Choose the **Normal Login Role.**

Step 3 Choose **Employee** in the Role Type list as the user role that you will apply the requirement to.

Step 4 Choose the **Windows Security Update** requirement from the Select Requirements to Associate with the Role list.

Step 5 Click the **Update** button to store the changes in the Cisco NAM database.

Activity Verification

You have completed this task when you attain this result:

- The update is accepted.

Task 7: Verify Cisco NAA Configuration

In this task, you will log on using the Cisco NAA and then verify the configuration.

Activity Procedure

Complete these steps:

Step 1 On the client machine, click the **Add kb835732** shortcut on the client machine desktop to apply the patch and to ensure that the next step removes this patch.

Step 2 On the client machine, click the **Remove kb835732** shortcut on the client machine desktop and click **Remove** to remove current patches.

Step 3 Establish a VPN connection with the network. The Cisco NAA dialog box appears.

Step 4 Click the **Continue** button in the Temporary Access dialog box. The Requirement Not Met dialog box appears on the client machine.

Step 5 Click the **Next** button in the Required Software dialog box.

Note You cannot continue until you have downloaded and installed the required software.

Step 6 Click the **Go to Link** button and see that you have access to the http://www.cisco.com website. Try to navigate to another website; you will not be able to.

Step 7 Close the browser.

Step 8 Leave the Temporary Access dialog box open and click the **Add kb835732** shortcut on the client machine desktop to apply the patch. Wait 15 seconds.

Step 9 Click the **Next** button in the Required Software dialog box.

Note You are notified that you have successfully logged in to the network.

Activity Verification

You have completed this task when you attain these results:

- You are notified that you have successfully logged in to the network.
- On the Cisco NAM PC, when you choose **Device Management** > **Clean Access** > **Clean Access Agent** > **Reports** and click the **View** button, you see the individual report for a user.

Lab 4-2: Configuring an HA In-Band VPN Cisco NAC Appliance Solution

Complete this lab activity to practice what you learned in the related module. Your instructor will need to reconfigure the switches to support this lab.

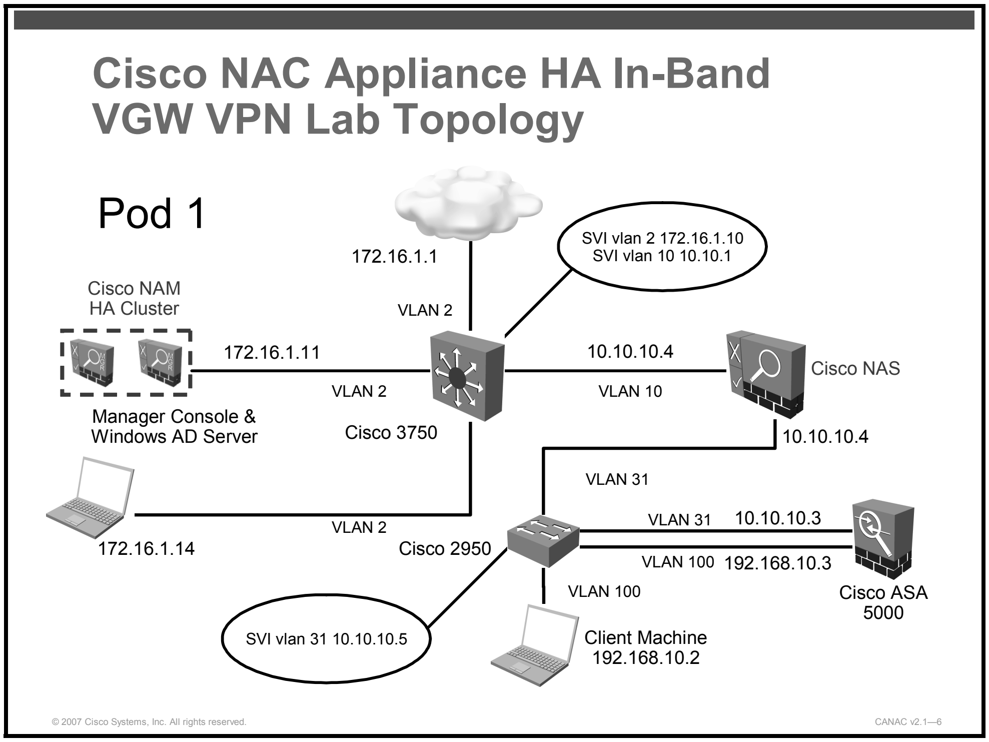
Activity Objective

In this activity, you will configure a highly available in-band VPN Cisco NAC Appliance solution. After completing this activity, you will be able to meet these objectives:

- Confirm connectivity between primary and secondary Cisco NAM
- Export an SSL private key and an SSL temporary certificate
- Configure primary Cisco NAM network and failover settings
- Import an SSL private key and an SSL temporary certificate into the secondary Cisco NAM
- Configure secondary Cisco NAM network and failover settings
- Test the HA Cisco NAM cluster

Visual Objective

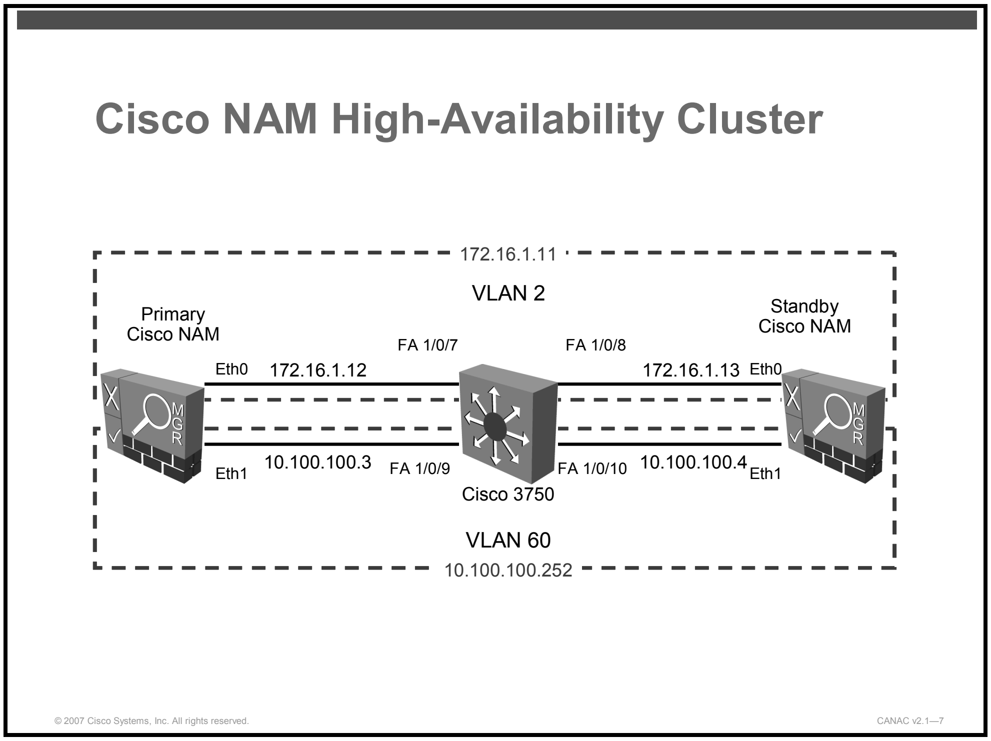
The figure shows the topology of the highly available in-band VGW VPN Cisco NAC Appliance lab.



Cisco NAC Appliance HA In-Band VGW VPN Lab Topology

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—6

The figure shows the topology for the Cisco NAM HA cluster, a part of the highly available in-band VGW VPN Cisco NAC Appliance lab.



Cisco NAM High-Availability Cluster

CANAC v2.1—7

Required Resources

These are the resources and equipment required to complete this activity:

- Internet connection
- Correctly configured CANACv2.1 remote student lab

Command List

This lab does not use the command line interface. All tasks are performed from the Cisco NAM web-based administration console menus.

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Confirm Connectivity Between Primary and Secondary Cisco NAM

In this task, you will confirm connectivity between the primary and secondary Cisco NAMs and ensure that the primary and secondary interfaces are in the same VLAN and are operational.

Activity Procedure

Complete these steps:

Step 1 Examine the HA topology diagrams for the Cisco NAM and Cisco NAS and prepare some observations to share with the class. The instructor will lead a discussion with the class.

Step 2 Log onto the primary Cisco NAM console and ping the Ethernet 0 interface on the secondary Cisco NAM: 172.16.1.13.

Note For more configuration information, see the Cisco NAC Appliance Cabling table located in Appendix A of this document.

Activity Verification

You have completed this task when you attain this result:

- The output confirms that the line is operational, that the correct protocol has been used, and that this line is in the same VLAN as the Ethernet 0 interface on the primary Cisco NAM.

Task 2: Export an SSL Private Key and an SSL Temporary Certificate

In this task, you will export an SSL private key and an SSL temporary certificate for the secondary Cisco NAM to use.

Activity Procedure

Complete these steps:

Step 1 Open the Cisco NAM administration console for the primary Cisco NAM.

Step 2 Choose **Administration > CCA Manager > SSL Certificate**.

Step 3 Choose **Export CSR/Private Key/Certificate** from the Choose an Action drop-down menu.

Step 4 Click the **Export** button next to the Currently Installed Private Key field to export the SSL private key.

Step 5 Save the key file to the desktop on the manager machine.

Step 6 Click the **Export** button next to the Currently Installed Certificate field to export the SSL temporary certificate key.

Step 7 Save the certificate file to the desktop on the manager machine.

Activity Verification

You have completed this task when you attain this result:

- The task completes with no warnings.

Task 3: Configure the Primary Cisco NAM Network and Failover Settings

In this task, you will configure the primary network and failover settings of the primary Cisco NAM.

Activity Procedure

Complete these steps:

Step 1 Go to the **Administration > CCA Manager** > **Network & Failover** tab.

Step 2 Select the **HA-Primary** option from the High-Availability Mode drop-down menu.

Step 3 Copy the value in the IP Address field that is under Network Settings and paste it into the Service IP Address field found in the Failover Settings column.

Step 4 Change the IP address under the Network Settings column to the IP address assigned to the Primary Cisco NAM of your pod. For example:

```
172.16.1.12
```

Step 5 Enter the hostname of the primary Cisco NAM in the Host Name field under Network Settings.

Step 6 Enter the hostname of the secondary Cisco NAM in the Peer Host Name field in the Failover Settings column.

Caution The Host Name and Peer Host Name fields are case-sensitive. You will need to enter the exact primary Cisco NAM hostname when you configure the secondary Cisco NAM.

Step 7 Enter **10.100.100** for the crossover network field.

Step 8 Click the **Update** button to update the database on the primary Cisco NAM.

Step 9 Click the **Reboot** button to enable the changes on the primary Cisco NAM.

Activity Verification

You have completed this task when you attain this result:

- The task completes with no warnings.

Task 4: Import an SSL Private Key and an SSL Temporary Certificate into the Secondary Cisco NAM

In this task, you will import an SSL private key and an SSL temporary certificate into the secondary Cisco NAM.

Activity Procedure

Complete these steps:

Step 1 Open the Cisco NAM administrator console for the secondary Cisco NAM.

Step 2 Click the **Yes** button on all Security Alert dialog boxes. This includes accepting the Cisco NAM temporary certificate. The Cisco NAM license key web page should open.

Step 3 In the PAK section of the window, click the **Browse** button and navigate to where your instructor has put the license keys for your pod

Step 4 Enter the high-availability (failover) license key for your pod in the Enter Product License field.

Tip Your instructor will provide you with the license keys.

Step 5 Click the **Yes** button on all Security Alert dialog boxes that appear. This includes accepting the Cisco NAM temporary certificate. The Cisco NAM web-based administration console should open.

Step 6 In the SSL Certificate tab, choose **Import Certificate** from the Choose an Action drop-down menu.

Step 7 Choose **Private Key** from the File Type drop-down menu. Click the **Browse** button next to the Certificate File field. Browse to the desktop of the manager machine and select the private key file that you saved there. The private key file will have the word “key” in its file name.

Step 8 Click the **Upload** button. The word "Success" will appear at the top of the SSL Certificate form.

Step 9 Ensure that **Import Certificate** is selected in the Choose an Action drop-down menu.

Note You will notice that the secondary Cisco NAM generates warnings displayed at the top of the SSL certificate form.

Step 10 Choose **CA-Signed PEM-Encoded X.509 Cert** from the File Type drop-down menu. Click the **Browse** button next to the Certificate File field. Browse to the desktop of the manager machine and select the certificate file. The certificate file will have "crt" in its file name.

Step 11 Click the **Upload** button. The word "Success" appears at the top of the SSL Certificate form.

Step 12 Click the **Verify and Install Uploaded Certificates** button. The phrase "Successfully Installed" appears at the top of the SSL Certificate form.

Activity Verification

You have completed this task when you attain this result:

- The task completes with no warnings.

Task 5: Configure Secondary Cisco NAM Network and Failover Settings

In this task, you will configure secondary network and failover settings of the Cisco NAC Appliance HA feature.

Activity Procedure

Complete these steps:

Step 1 Go to the **Administration > CCA Manager > Network & Failover** tab.

Step 2 Select the **HA-Secondary** option from the High-Availability Mode drop-down menu.

Step 3 Change the IP address under the Network Settings column to the IP address assigned to the Secondary Cisco NAM of your pod. For example:

```
172.16.1.13
```

Step 4 Enter the hostname of the primary Cisco NAM in the Peer Host Name field in the Failover Settings column.

Step 5 Enter **172.16.1.11** in the Service IP Address field in the Failover Settings column.

Step 6 Under Network Settings, enter the Host Name of the secondary Cisco NAS.

Step 7 Confirm that "N/A" is entered in the Heartbeat Serial Interface field.

Step 8 Enter **10.100.100** in the Crossover Network Interface Settings field.

Step 9 Click the **Update** button to update the database on the secondary Cisco NAM.

Step 10 Click the **Reboot** button to enable the changes on the secondary Cisco NAM.

Activity Verification

You have completed this task when you attain this result:

- The task completes with no warnings.

Task 6: Test the HA Cisco NAM Cluster

In this task, you will test the HA Cisco NAM cluster.

Activity Procedure

Complete these steps:

Step 1 On the manager machine, open a console window to the primary and secondary Cisco NAM; for example:

```
172.16.1.13 and 172.16.1.12
```

Step 2 In the console window for the secondary Cisco NAM, type **tail -f /var/log/ha-log.** This command displays the log file for the secondary Cisco NAM.

Step 3 In the console window for the primary Cisco NAM, enter **Service Perfigo Restart** at the system prompt.

Step 4 In the console window for the secondary Cisco NAM, observe the entries in the ha-log file indicating that the primary Cisco NAS has failed and the secondary Cisco NAM has become active.

Step 5 Open a browser on the manager machine and go to the service IP address for the Cisco NAM HA cluster.

Step 6 Go to **Monitoring > Event Logs** and observe log entries confirming that the database has been restored and the database connection pool has been created.

Activity Verification

You have completed this task when you attain these results:

- The HA log on the secondary Cisco NAM, displayed in an SSH terminal window, indicates that the primary Cisco NAM stopped and then started operating again.
- The event logs displayed in the Cisco NAM cluster web-based administration console (use the service IP address) observe log entries that confirm that the database has been restored and the database connection pool has been created.

Lab 3-4: Adding an Out-of-Band Virtual Gateway Cisco NAS to an HA Cisco NAC Appliance Deployment

Complete this lab activity to practice what you learned in the related module. Your instructor will need to reconfigure the switches to support this lab.

Note This lab is placed here to enable a smooth transition between the labs.

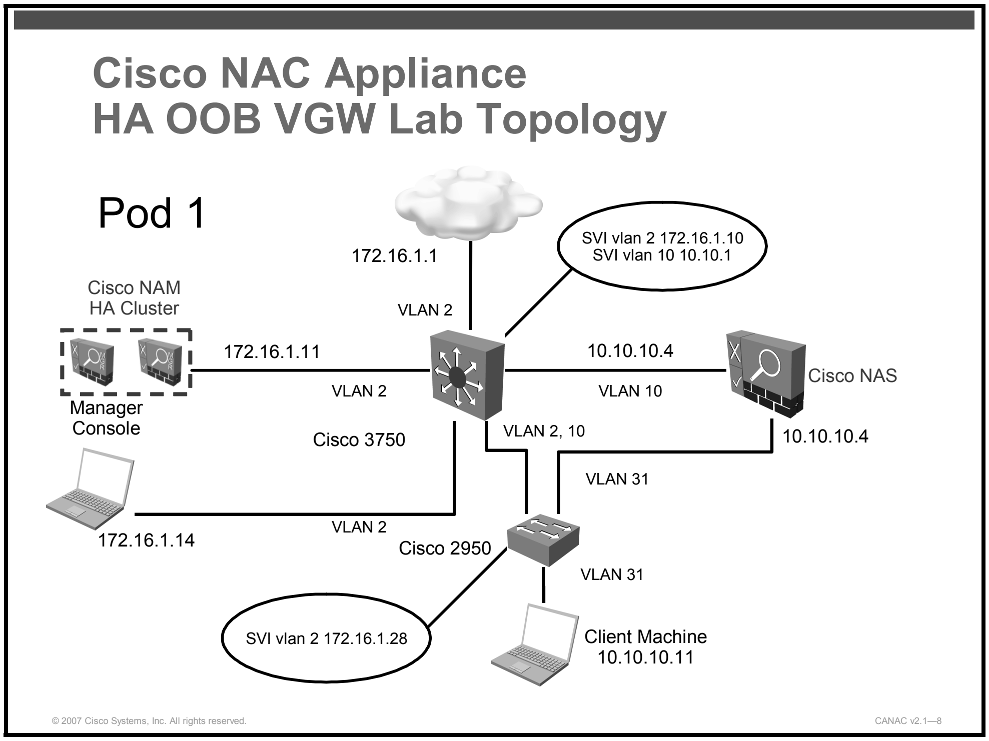
Activity Objective

In this activity, you will add an out-of-band virtual gateway Cisco NAS to an HA Cisco NAC Appliance deployment. After completing this activity, you will be able to meet these objectives:

- Reconfigure the client machine
- Add an out-of-band virtual gateway Cisco NAS to the Cisco NAM domain
- Configure VLAN mapping for the out-of-band virtual gateway Cisco NAS

Visual Objective

The figure shows the topology for the HA out-of-band VGW Cisco NAC Appliance lab.



Cisco NAC Appliance
HA OOB VGW Lab Topology

Required Resources

These are the resources and equipment required to complete this activity:

- Internet connection
- Correctly configured CANACv2.1 remote student lab

Command List

There are no CLI commands used in this activity. All tasks are performed from the Cisco NAM web-based administration console menus.

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Reconfigure the Client Machine

In this task, you reconfigure the client machine with a new IP address and default gateway.

Activity Procedure

Complete these steps:

Step 1 Reconfigure the client machine IP address to 10.10.10.11.

Step 2 Reconfigure the client machine default gateway to 10.10.10.1.

Activity Verification

You have completed this task when you attain these results:

- You can ping 10.10.10.1.

Task 2: Add an Out-of-Band Virtual Gateway Cisco NAS to the Cisco NAM Domain

In this task, you will add an out-of-band virtual gateway Cisco NAS to the Cisco NAM domain.

Activity Procedure

Complete these steps:

Step 1 On the primary Cisco NAM, click the **Device Management > CCA Servers** link from the left menu in the Cisco NAM web-based administration console.

Step 2 Click the **Manage** button for the existing virtual gateway server listed.

Step 3 Go to the **Network** tab.

Step 4 Uncheck the Enable L3 check box.

Step 5 Choose **Out-of-Band Virtual Gateway** from the Server Type drop-down menu.

Step 6 Click the **Update** button to update the Cisco NAM database.

Step 7 Click the **Reboot** button to enable the changes on the primary and secondary Cisco NAS.

Activity Verification

You have completed this task when you attain these results:

- The new server appears in the Device Management > CCA Servers > List of Servers page with a status of Connected.
- When you refresh your web browser, the Cisco NAM displays that the Cisco NAS is connected.
- The IP address for the client machine is 10.10.10.4.

Task 3: Configure VLAN Mapping for the Out-of-Band Virtual Gateway Cisco NAS

In this task, you will configure VLAN mapping for the out-of-band virtual gateway Cisco NAS.

Activity Procedure

Complete these steps:

Step 1 Go to **Device Management > CCA Servers** and click the **Manage** button for the Cisco NAS that you added. The management pages for the Cisco NAS appear.

Step 2 Click the **Advanced** tab.

Step 3 Click the **VLAN Mapping** link.

Step 4 Check the check box for **Enable VLAN Mapping**.

Step 5 Click the **Update** button to store the changes in the Cisco NAM database**.**

Step 6 Enter the Auth VLAN ID of **31** for the Untrusted Network VLAN ID field.

Step 7 Enter the Access VLAN ID of **10** for the Trusted Network VLAN ID field.

Step 8 Enter **Users on Edge Switch** as the optional description in the Description field.

Step 9 Click **Add Mapping**.

Note If you closed the Cisco NAS console window, you will need to log on with a username "root" and password "cisco123".

Activity Verification

You have completed this task when you attain these results:

- Choose **Device Management > CCA Servers > List of Servers**, then click **Manage,** and then the **Advanced** tab. Click the **VLAN Mapping** subtab link. The mapping of VLAN 31 -> 10 is listed at the bottom of the page.

Lab 3-5: Configuring SNMP, Switch, and Port Profiles for an Out-of-Band Cisco NAC Appliance Deployment

Complete this lab activity to practice what you learned in the related module.

Note This lab is placed here to enable a smooth transition between the labs.

Activity Objective

In this activity, you will complete the configuration of the switch to support an out-of-band Cisco NAC Appliance deployment. After completing this activity, you will be able to meet these objectives:

- Verify switch SNMP notification
- Configure group and switch profiles
- Configure port profiles
- Configure the SNMP receiver
- Add a switch to the Cisco NAM
- Configure ports on the switch
- Verify your configuration

Visual Objective

There is no visual objective for this lab.

Required Resources

These are the resources and equipment required to complete this activity:

- Internet connection
- Correctly configured CANACv2.1 remote student lab

Command List

There no CLI commands used in this activity, but the following commands are verified in this lab.

Command	Description
`snmp-server contact <admin_contact_info>`	Sets the system contact (sysContact) string
`snmp-server enable traps mac-notification`	Enables only the MAC-notification SNMP trap type
`snmp-server enable traps snmp linkdown`	Enables only the linkdown SNMP trap type
`snmp-server location <location_string>`	Sets up information on where the SNMP device is located
`snmp-server community <community name> view <view> [RO/RW]`	Configures SNMP community strings
`snmp-server enable traps tty`	Enables only the TTY SNMP trap type
`snmp-server view <view> <view> included`	Configures SNMP object identifier
`access-list 20 permit 172.16.0.0 0.0.255.255`	Creates an access list
`snmp-server host 172.16.1.11 traps version 1 public mac-notification snmp.`	Specifies the recipient of an SNMP notification operation

Job Aids

Job aids are not required to help you complete the lab activity.

Task 1: Verify Switch SNMP Notification

In this task, you will verify SNMP notification on the switch. With switch SNMP notification configured, the Cisco NAM is able to obtain VLAN and port information from the switch and to set VLANs for managed switch ports.

Note The example IP address is based on Pod 1.

Activity Procedure

Complete these steps:

Step 1 Ask the instructor how to gain console access to the Layer 2 switch.

Step 2 Enter the **enable** command at the switch prompt and enter the enable password **cisco123**.

Step 3 Enter **show run** at the switch prompt.

Activity Verification

You have completed this task when you attain this result:

- These SNMP configuration items appear:

```
access-list 20 permit 172.16.0.0 0.0.255.255
snmp-server engineID local 800000090300000B46F62701
snmp-server community c2950_read RO 20
snmp-server community public RW 20
snmp-server location San_Jose
snmp-server contact Lab_Staff
snmp-server enable traps snmp linkdown
snmp-server enable traps MAC-Notification
snmp-server host 172.16.1.11 public  MAC-Notification snmp
```

Task 2: Configure Group and Switch Profiles

Add group and switch profiles in order to apply the same SNMP settings to the pod switch.

Activity Procedure

Complete these steps:

Step 1 Choose **Switch Management** > **Profiles** > **Group** > **New**.

Step 2 Enter **2950s** in the Group Name field.

Step 3 Enter **2950s** in the Group Description field.

Step 4 Click **Add**.

Step 5 Choose **Switch Management** > **Profiles** > **Switch** > **New**.

Step 6 Enter **2950v1** in the Profile Name field.

Step 7 Choose **Cisco Catalyst 2950 Series** from the Switch Model drop-down menu.

Note The above selection is based on the equipment in the remote lab at the time of development. Please select the correct switch type based on the current remote lab topology.

Step 8 Leave **161** as the default SNMP Port.

Step 9 Choose **SNMP_V1** from the SNMP Version drop-down menu in the SNMP Read Settings and enter **c2950_read** for the read Community String**.**

Step 10 Choose **SNMP_V1** from the SNMP Version drop-down menu in the SNMP Write Settings and enter **public** for the write Community String.

Step 11 Click **Add**.

Activity Verification

You have completed this task when you attain these results:

- The new Group profile appears under Switch Management > Profiles > Group > List.
- The new Switch profile appears under Switch Management > Profiles > Switch > List.

Task 3: Configure Port Profiles

In this task, you will configure port profiles. There are three port profile types for switch ports: uncontrolled, controlled, and controlled using role settings. Regular switch ports should use the uncontrolled port profile and client machine-connected switch ports should use controlled port profiles.

Note When a client machine connects to a controlled port, the port is set to the authentication VLAN. After the client machine is authenticated and certified, the port is set to the access VLAN specified in the port profile or the role settings. For out-of-band virtual gateways, the client machine uses the same IP address after successful authentication and certification.

Activity Procedure

Complete these steps:

Step 1 Choose **Switch Management** > **Profiles** > **Port** > **New**.

Step 2 Enter **Control31** in the Profile Name field.

Step 3 Enter **Users to 10** in the Description field.

Step 4 Check the **Manage This Port** option.

Step 5 Enter **31** for the Auth VLAN field and enter **10** for the Default Access VLAN field.

Step 6 Choose **Default Access VLAN** from the Access VLAN drop-down menu.

Step 7 Check **Remove Out-of-Band Online User When SNMP Linkdown Trap Is Received**.

Step 8 Check **Remove Out-of-Band Online User Without Bouncing the Port**.

Note Leave other settings unchecked.

Step 9 Click **Add**.

Activity Verification

You have completed this task when you attain this result:

- When you choose **Switch Management** > **Profiles** > **Port** > **List**, you see the controlled port profile that you configured (Control31).

Task 4: Configure the SNMP Receiver

In this task, you will configure the SNMP receiver running on the Cisco NAM to receive the MAC notification and linkdown SNMP trap notifications from the controlled switches and to set the VLAN on the corresponding switch ports.

Activity Procedure

Complete these steps:

Step 1 Choose **Switch Management** > **Profiles** > **SNMP Receiver** > **SNMP Trap**.

Note Leave **162** as the default for Trap Port on the Cisco NAM.

Step 2 Enter **public** in the Community String field in the SNMP V1 section.

Step 3 Click the **Update** button to store the changes in the Cisco NAM database.

Activity Verification

You have completed this task when you attain this result:

- The updates are accepted.

Task 5: Add a Switch to the Cisco NAM

In this task, you will add a switch to the Cisco NAM using the Search page and view the ports of an added switch.

Activity Procedure

Complete these steps:

Step 1 Go to **Switch Management** > **Devices** > **Switches** > **Search**.

Step 2 Choose **2950v1** from the Switch Profile drop-down menu.

Note The read community string of this switch profile is used to find switches with matching read settings.

Step 3 Enter **172.16.1.15 - 172.16.1.30** in the Switch IP Range text fields.

Step 4 Click **Search**. The Cisco NAM finds and lists switches in this IP range and with matching SNMP read settings at the bottom of the page.

Note By default, the **Don't List Switches Already in the Database** box is already checked. If you uncheck this box, the resulting search includes switches that the Cisco NAM is already managing, but the Commit boxes to the left of each entry will be disabled for these switches.

Step 5 Choose **2950s** in the Switch Group drop-down menu. This choice will apply to the switches that you will add.

Step 6 Choose **uncontrolled** in the Default Port Profile drop-down menu. This choice will be the default port profile of switches added to the Cisco NAM.

Step 7 Check the box at the top of the column to add *all* uncontrolled switches found from the search.

Step 8 Click the **Commit** button to add the new switch to the Cisco NAM. These switches are now listed under Switch Management > Devices > Switches > List.

Note While all switches matching the read community string of the switch profile that is used for the search are listed, only those switches matching the write SNMP version and community string can be added using the Commit button. A switch cannot be controlled unless its write SNMP settings match the settings that are configured for the switch profile in the Cisco NAM.

Activity Verification

You have completed this task when you attain this result:

- When you choose **Switch Management > Devices > Switches > List,** the list displays the IP address, MAC address, and switch profile for the switch that you added.

Note When you click the **Manage Ports** button to bring up the Port tab for the switch, the Port and Configure buttons and tabs only appear for a switch after the switch is added.

Task 6: Configure Ports on the Switch

In this task, you will configure ports on the switch.

Activity Procedure

Complete these steps:

Step 1 Click the **Ports** icon for switch 172.16.1.28 to bring up the Port tab for the switch. The default values displayed in the VLAN column indicate which ports are currently on the Access VLAN and which ports are on the Auth VLAN.

Step 2 Click the **OK** button in the two dialog boxes that appear.

Step 3 Choose **Control31** in the drop-down menu for Port 5.

Step 4 Click the **Update** button to store the changes in the Cisco NAM database.

Step 5 Click the **OK** button in the two dialog boxes that appear.

Step 6 Click **Save** to initialize the switch ports and update the running configuration of the switch.

Note If the running configuration of the switch has not been saved, a dialog box appears that prompts you to save the configuration.

Step 7 Click the bounce port icon to bounce Port 5. The bounce port icon is located under the Bounce column heading next to the Status indicator icon.

Step 8 After 15 seconds, click the **Update** button and confirm that the Port 5 status indicator is green.

Note Configuring ports on the switch is done to initialize port configuration in the Cisco NAC Appliance remote lab. For specific procedures on actual Cisco NAC Appliance implementation, please refer to the *Cisco NAC Appliance Manager Installation and Administration Guide* and the *Cisco NAC Appliance Server Installation and Administration Guide*.

Activity Verification

You have completed this task when you attain this result:

- The update is accepted.

Task 7: Verify Your Configuration

In this task, you will verify your configuration by connecting your client machine to a controlled switch port and successfully logging in as a user on the Auth VLAN.

Activity Procedure

Complete these steps:

Step 1 Log onto the client machine.

Note Once your client machine computer is detected on the network, the Cisco NAA login dialog box should appear automatically (the Popup Login Window option is selected). If the login dialog box does not pop up, click the Cisco NAA icon on the task bar and choose **Login**.

Step 2 Enter **cisco** in the User Name field and enter **cisco123** in the Password field in the Cisco NAA login dialog box.

Note **LocalDB** should be the default authentication provider.

Step 3 Click **Login** to log on and then click **OK** to complete the login procedure.

Step 4 Click **Yes** to both dialog boxes that appear.

Note You may need to disconnect and reconnect the client machine if the Cisco NAA dialog box does not appear.

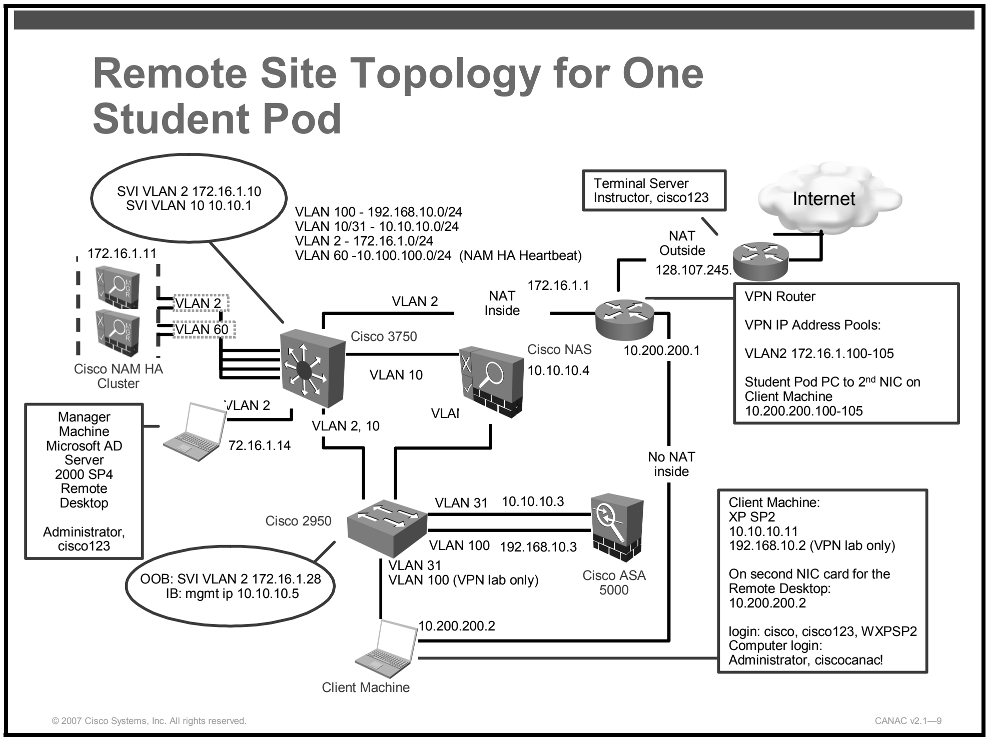
Activity Verification

You have completed this task when you attain these results:

- You have access to the default URL configured for the browser.
- Online user status is confirmed when you go to **Monitoring** > **Online Users** > **View Online Users** > **Out-of-Band** and you are listed as an authenticated Access VLAN user in the out-of-band users list.
- When you choose **Switch Management** > **Devices** > **Switches** > **List** and click the **Manage Ports** button for switch 172.16.1.28, the Port tab for the switch appears.
- The Current VLAN column displays the Access VLAN ID for the port that the client machine is attached to, as configured in the port profile.

Appendix A

This appendix provides the Cisco NAM and Cisco NAS configuration information that you use in this lab.

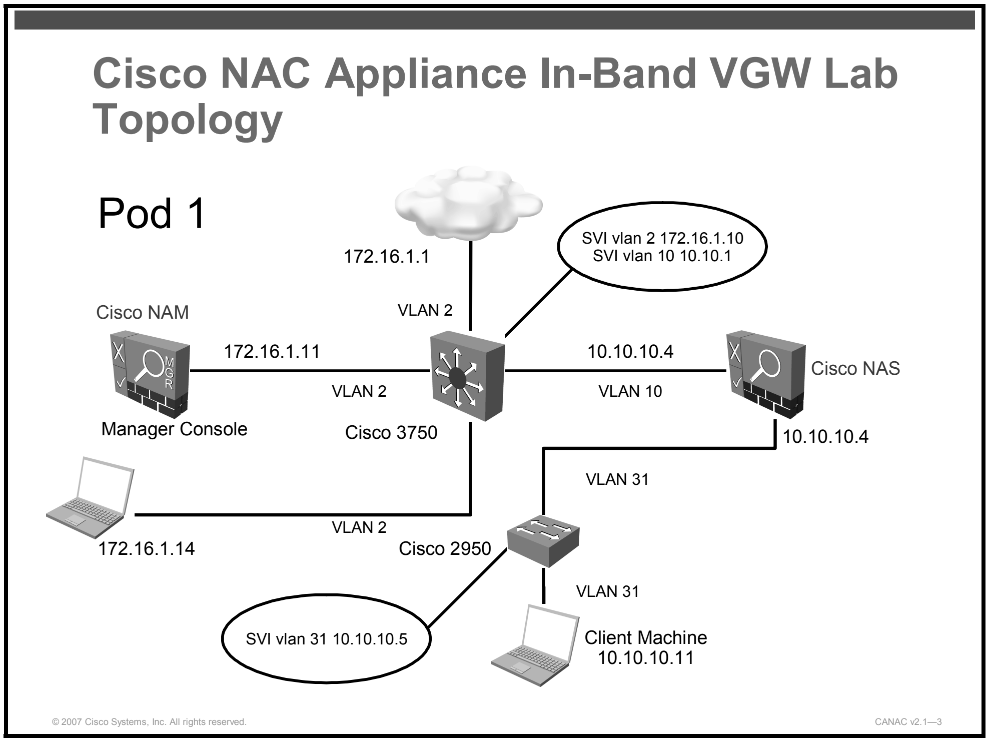


Remote Site Topology for One Student Pod

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—9

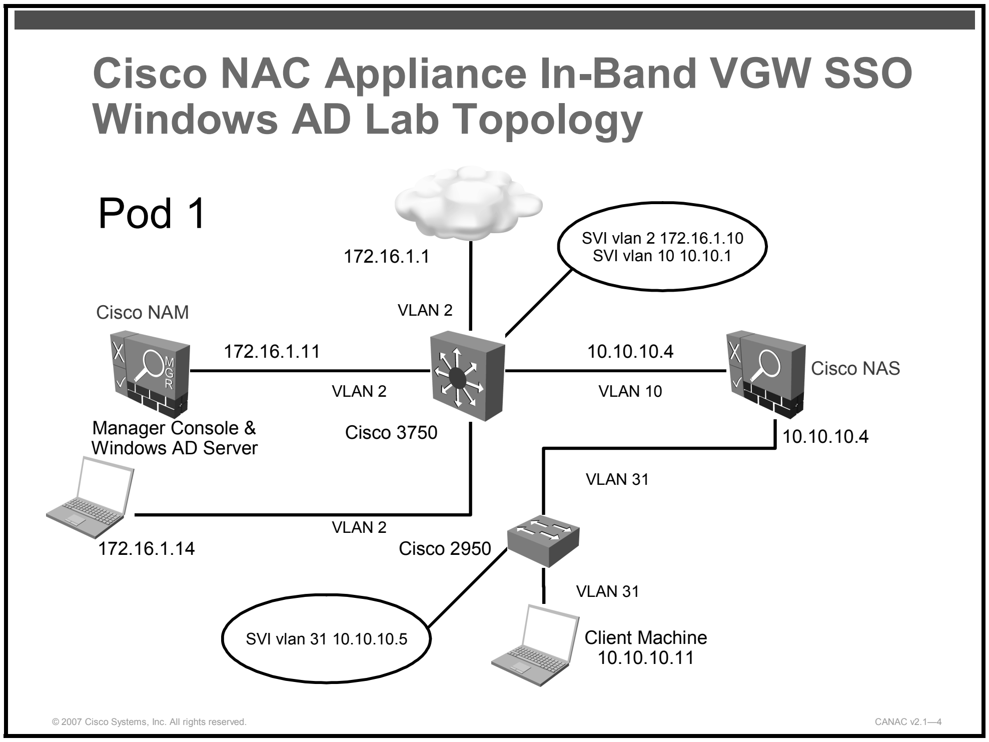
The figure shows the topology of one student pod. Your remote lab topology may differ. The method that is used here to provide remote access allows the same IP addressing scheme to be used for each student pod. Remote desktop access is provided by using VPN accounts to the manager console and the client machine. Students will connect using a VPN tunnel to the manager console or the client machine as required. A second network interface card is used in the client machine to provide remote desktop access. This setup is required because the various labs reconfigure the IP address of the client machine. The terminal server provides console access to the Cisco NAM cluster, the Cisco NAS, the Cisco 3750, the Cisco 2950, and the Cisco ASA 5000.



Cisco NAC Appliance In-Band VGW Lab Topology

CANAC v2.1—3

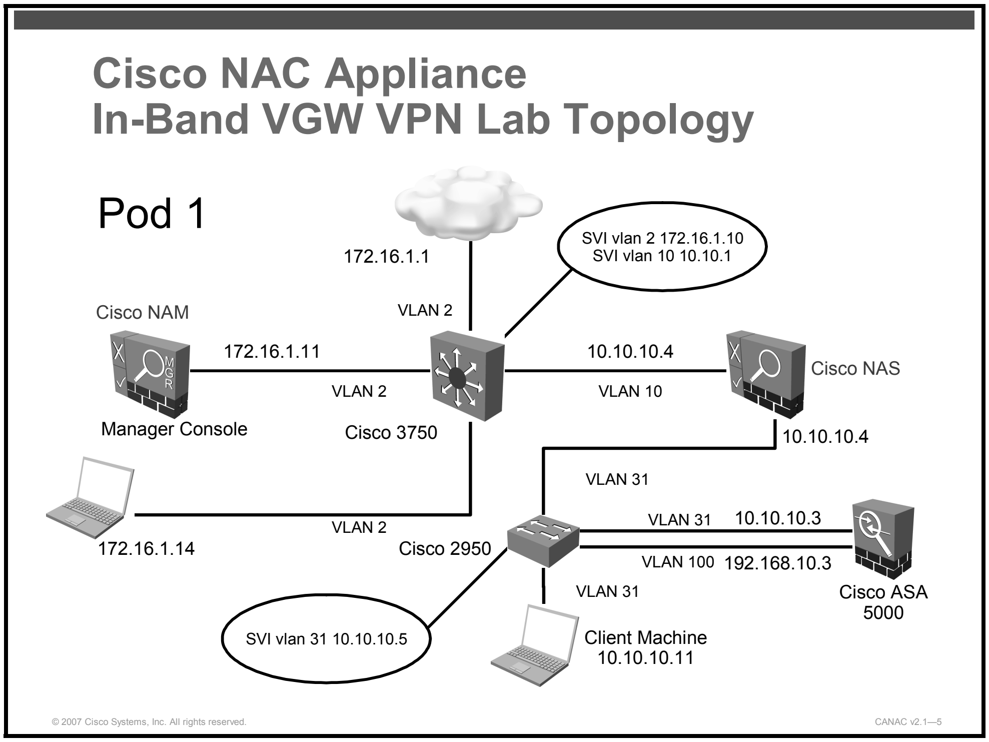
The figure shows the topology of the in-band VGW Cisco NAC Appliance lab.



Cisco NAC Appliance In-Band VGW SSO Windows AD Lab Topology

CANAC v2.1—4

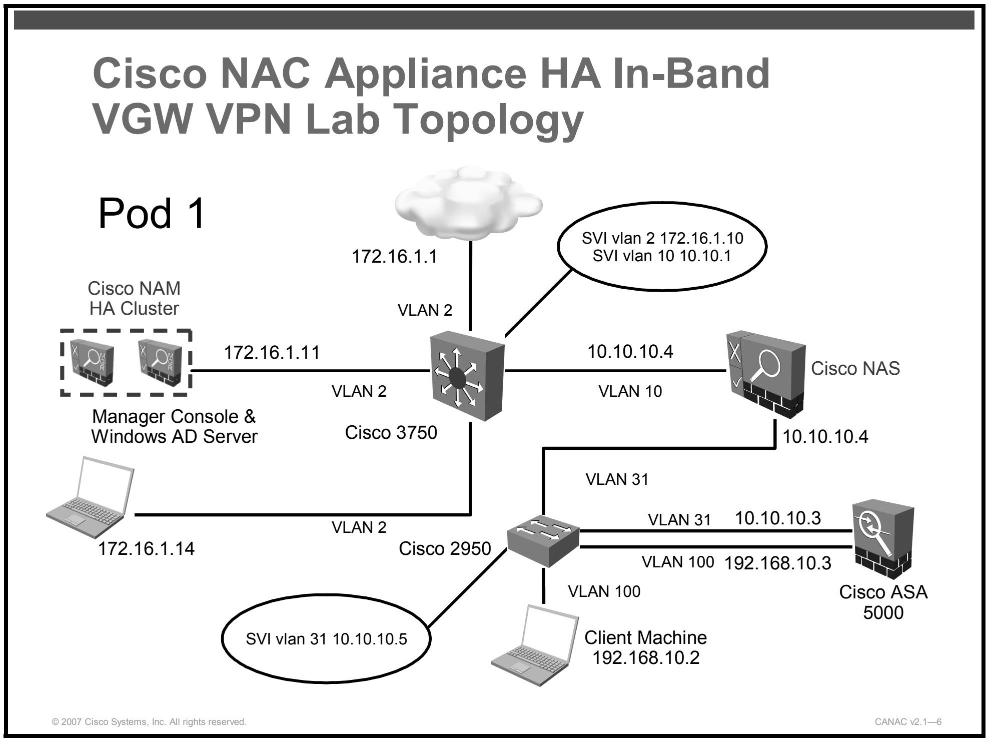
The figure shows the topology of the in-band VGW SSO Windows Active Directory Cisco NAC Appliance lab.



Cisco NAC Appliance In-Band VGW VPN Lab Topology

CANAC v2.1—5

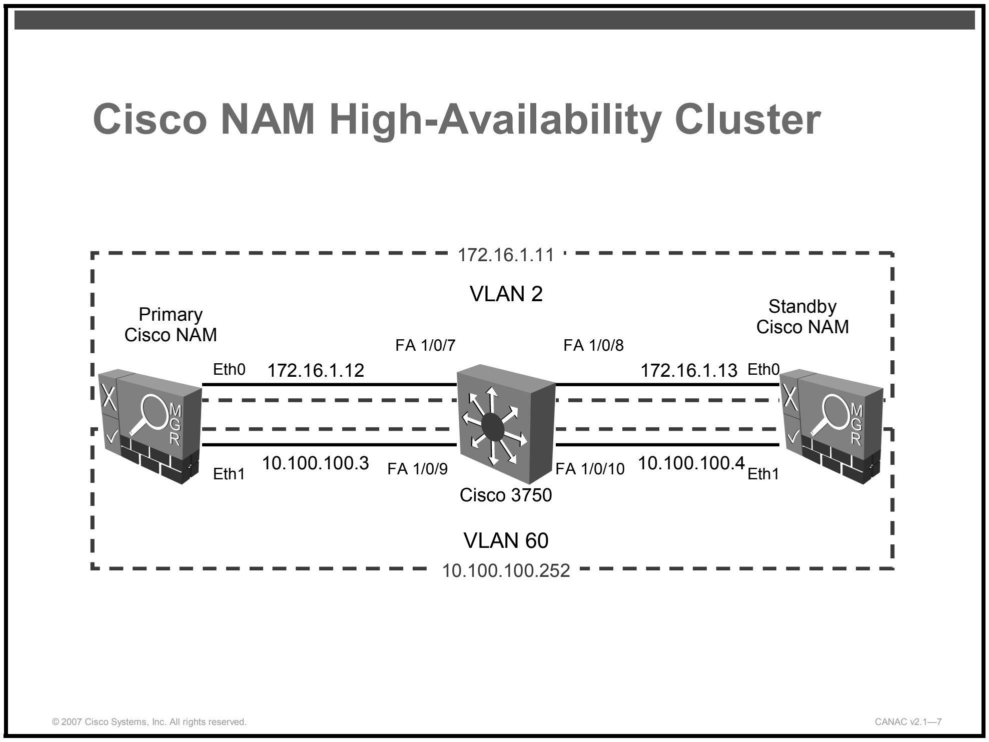
The figure shows the topology of the in-band VGW VPN Cisco NAC Appliance lab.



Cisco NAC Appliance HA In-Band VGW VPN Lab Topology

CANAC v2.1—6

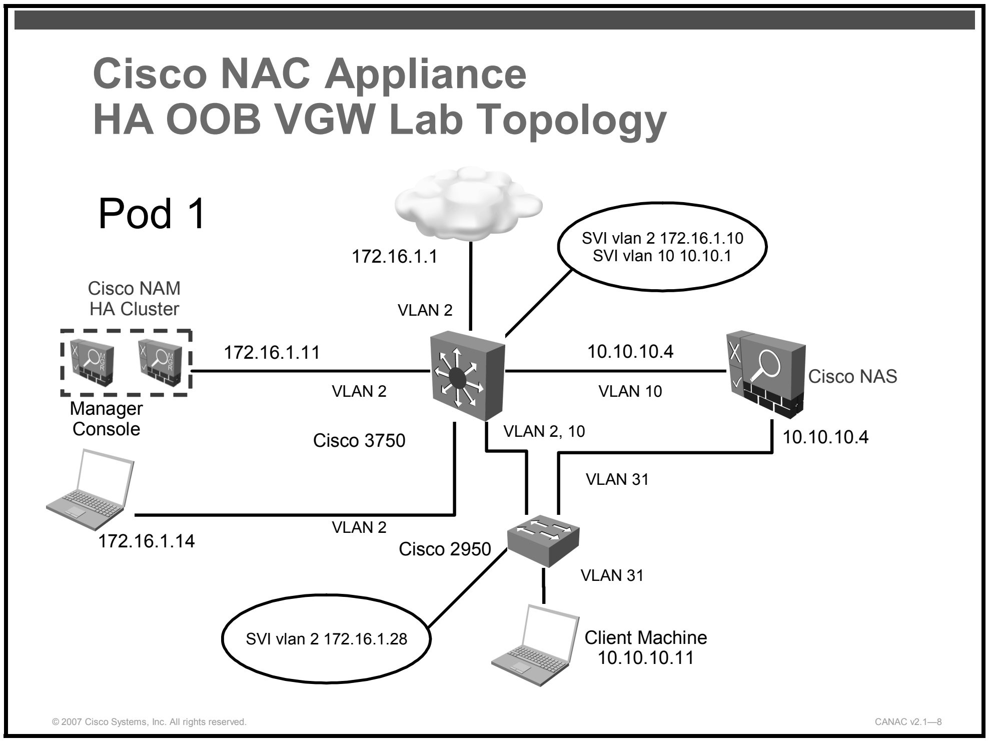
The figure shows the topology for the HA in-band VGW VPN Cisco NAC Appliance lab.



Cisco NAM High-Availability Cluster

CANAC v2.1—7

The figure shows the topology for the Cisco NAM HA cluster, a part of the HA out-of-band VGW Cisco NAC Appliance lab.



Cisco NAC Appliance HA OOB VGW Lab Topology

CANAC v2.1—8

The figure shows the topology for the HA out-of-band VGW Cisco NAC Appliance lab.

License Key

Ask your instructor for the license key.

Cisco NAC Appliance Cabling

The following table shows the cabling and VLANs used for the entire lab.

Switch	Interface	Cable Type	Mode	VLAN	Device
Cisco 3750					
	FA 1/0/2	Crossover	Trunk	2,10	Trunk to 2950 for vlans 2 and 10
Implementation specific and therefore not shown on lab topology	FA 1/0/4	Straight	Access	2	Internet_Router e0/1 Inside
	FA 1/0/5	Straight	Access	10	Eth0 NAS Trusted
	FA 1/0/7	Straight	Access	2	Eth0 NAM Primary
	FA 1/0/8	Straight	Access	2	Eth0 NAM Secondary
	FA 1/0/9	Straight	Access	60	Eth1 NAM Primary
	FA 1/0/10	Straight	Access	60	Eth1 NAM Secondary
	FA 1/0/11	Straight	Access	2	manager machine
Cisco 2950					
	FA 0/1	Straight	Access	31	Eth1 NAS Untrusted
	FA 0/3	Straight	Access	31	ASA 5520 Private Interface
	FA 0/4	Straight	Access	100	ASA 5520 Public Interface
	FA 0/5	Straight	Access	31,100	Client machine Public Interface
	FA 0/6	Crossover	Trunk	2,10	Trunk to 3750 for OOB for vlans 2 and 10
Cisco ASA 5520					
	FA 0/0	Straight	Access	100	Cisco 2950 FA 0/4
	FA 0/1	Straight	Access	31	Cisco 2950 FA 0/3

Cisco NAC Appliance IP Addressing

The following table shows the IP addresses used for the entire lab.

Device	Interface	VLAN	IP Address	Gateway
Internet	Eth0		172.16.1.1	
Cisco 3750		2	172.16.1.10	172.16.1.1
		10	10.10.10.1	
		60		
Cisco 2950		31	10.10.10.5	
Cisco 2950 OOB		2	172.16.1.28	
Cisco NAM HA	virtual Eth0		172.16.1.11	
	virtual Eth1		10.100.100.252	
Cisco NAM Primary	Eth0		172.16.1.12	172.16.1.10
	Eth1	60	10.100.100.3	
Cisco NAM Secondary	Eth0		172.16.1.13	172.16.1.10
	Eth1	60	10.100.100.4	
Cisco NAS	Eth0		10.10.10.4	10.10.10.1
	Eth1		10.10.10.4	
Cisco ASA 5520	Public		192.168.10.3	
	Private		10.10.10.3	10.10.10.1
Manager machine	Ethernet Port		172.16.1.14	172.16.1.10
Client machine In-band VGW, AD SSO, OOB labs	Ethernet Port	31	10.10.10.11	10.10.10.1
Client machine VPN	Ethernet Port	100	192.168.10.2	192.168.10.3