Cisco NAC Layer 3 OOB with ACLs

Document ID: 112168

Contents

Introduction

Cisco Network Admission Control (NAC) enforces an organization's network security policies on all devices seeking network access. Cisco NAC allows only compliant and trusted endpoint devices, such as PCs, servers, and PDAs, onto the network. Access is restricted for non−compliant devices, which limits the potential damage from emerging security threats and risks. Cisco NAC gives organizations a powerful, roles−based method to preventing unauthorized access and improve network resiliency.

The Cisco NAC solution provides the following business benefits:

- **Security policy compliance**: Ensures that endpoints conform to security policy; protects infrastructure and employee productivity; secures managed and unmanaged assets; supports internal environments and guest access; tailors policies to your risk level.
- **Protects existing investments**: Is compatible with third−party management applications; flexible deployment options minimize the need for infrastructure upgrades.
- **Mitigates risks from viruses, worms, and unauthorized access**: Controls and reduces large−scale infrastructure disruptions; reduces operating expenses by making moves, adds, and changes dynamic and automated, which enables higher IT efficiency; integrates with other Cisco Self−Defending Network components to deliver comprehensive security protection.

Solution Overview

This section briefly introduces Layer 3 out−of−band (OOB) using access control list (ACL) methods to implement a Cisco Network Admission Control (NAC) architecture.

Solution Description

Cisco NAC is used in the network infrastructure to enforce security policy compliance on all devices that seek access to network resources. Cisco NAC allows network administrators to authenticate and authorize users and to evaluate and remediate their associated machines before they are granted network access. There are several configuration methods you can use to accomplish this task, but Layer 3 out−of−band (OOB) has rapidly become one of the most popular deployment methodologies for NAC. This shift in popularity is based on several dynamics, including better utilization of hardware resources.

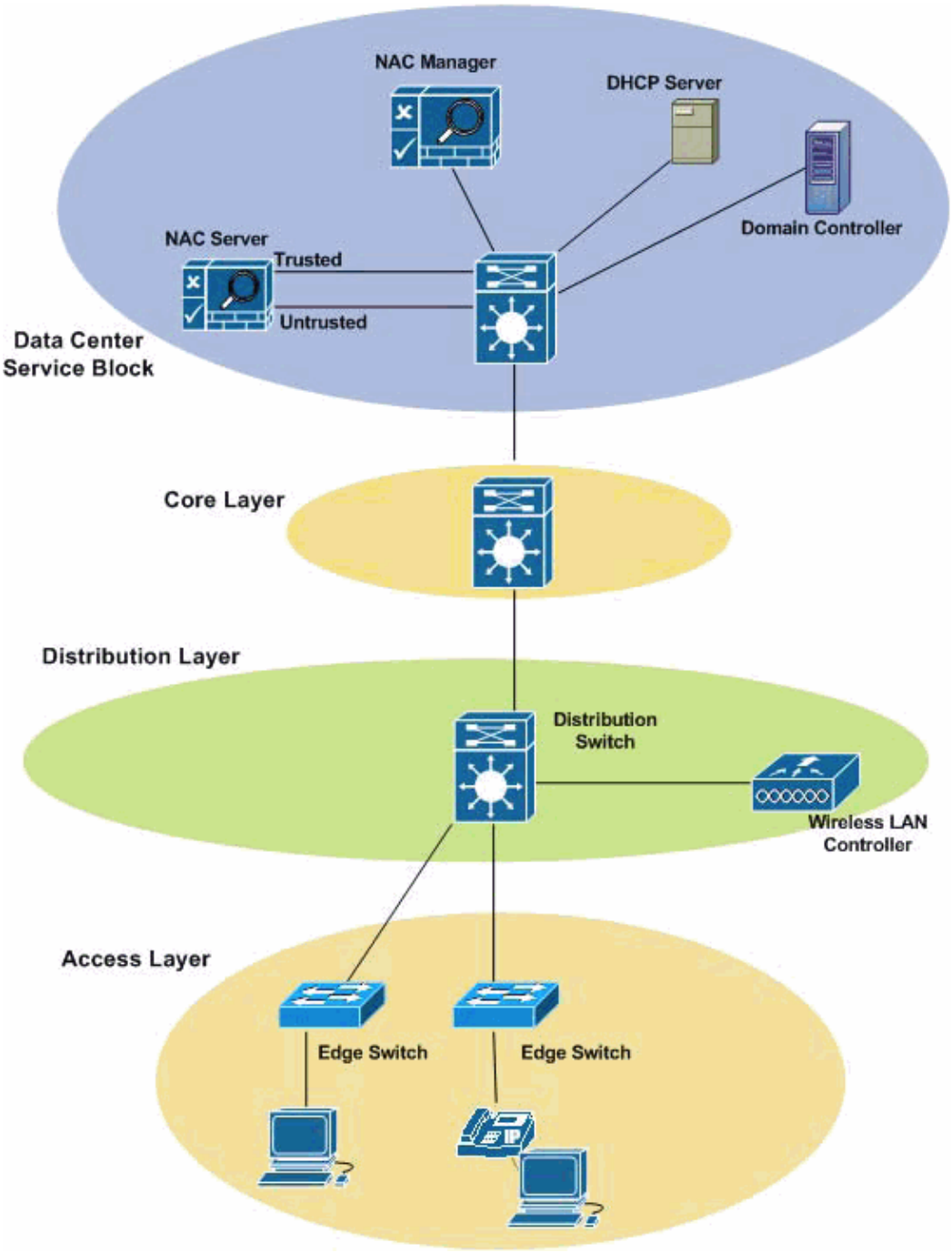
By deploying Cisco NAC in a Layer 3 OOB methodology, a single Cisco NAC Appliance (Cisco NAC Manager or Cisco NAC Server) can scale to accommodate more users. It also allows NAC Appliances to be centrally located rather than distributed across the campus or organization. Thus, Layer 3 OOB deployments are much more cost−effective both from a capital and operational expense standpoint.

This guide describes an ACL−based implementation of Cisco NAC in a Layer 3 OOB deployment.

Solution Architecture

The solution architecture (see Figure 1) identifies the key solution components and integration points.

Figure 1: Cisco NAC Appliance Placement in a Typical Campus Environment



The following sections describe the access layer, distribution layer, core layer, and data center services integration points that make up a typical campus architecture.

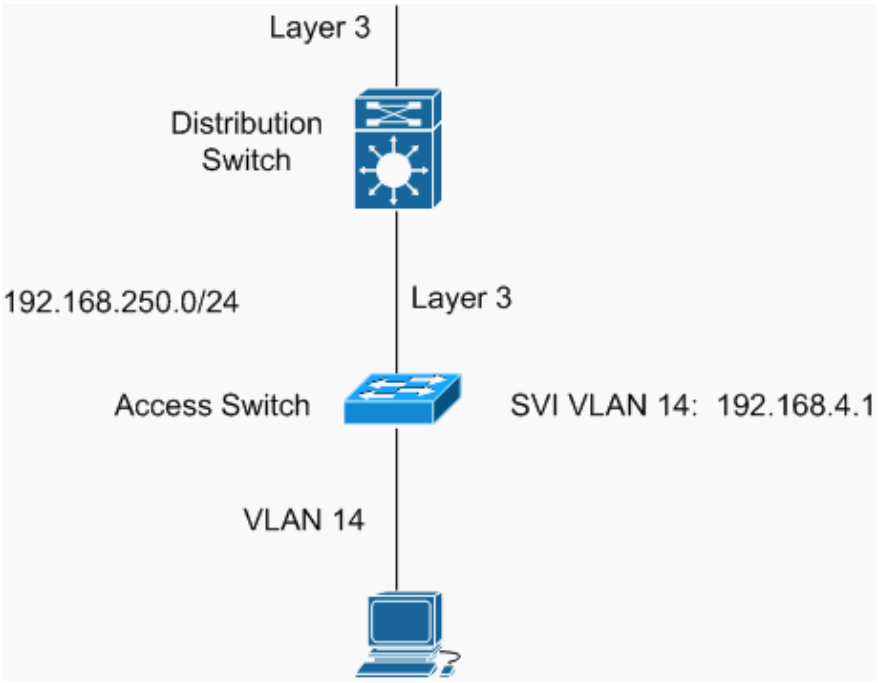
Access Layer

The Cisco Layer 3 OOB NAC solution is applicable to a routed access campus design. In routed access mode, Layer 3 switched virtual interfaces (SVIs) are configured on the access switch, and there is a Layer 3 link between access and distribution switches.

Note: The term access switch and edge switch are used interchangeably in this document.

As seen in Figure 2, the Layer 3 access VLAN (for example, VLAN 14) is configured on the edge switch, Layer 3 routing is supported from the switch to the upstream distribution switch or router, and the Cisco NAC Manager manages the ports on the access switch.

Figure 2: Access Switches with Layer 3 to the Edge



Distribution Layer

The distribution layer is responsible for Layer 3 routing. Unlike a Layer 2 solution, the Cisco NAC server does not need to be located at the distribution layer. Instead, it is placed centrally at the data center service block.

Core Layer

The core layer uses Cisco IOS−based routers. The core layer is reserved for high−speed routing, without any services. Services can be placed on a service switch in the data center.

Data Center Services Layer

The data center services layer uses Cisco IOS−based routers and switches. The Cisco NAC Manager and Cisco NAC Server are centrally located at the data center service block.

Solution Components

This section describes the components of the Cisco NAC Appliance solution.

Cisco NAC Manager

The Cisco NAC Manager is the administration server and database that centralizes configuration and monitoring of all Cisco NAC Servers, users, and policies in a Cisco NAC Appliance deployment. For an OOB NAC deployment, the Manager provides the OOB management to add and control switches in the domain of the Manager and to configure switch ports.

Cisco NAC Server

The Cisco NAC Server is the enforcement point between the untrusted (managed) network and the trusted (internal) network. The Server enforces polices defined in the Cisco NAC Manager, and endpoints communicate with the Server during authentication. In this design, the Server is not placed logically or physically inline to separate the untrusted and trusted network. This concept is addressed in more detail later in the Out−of−Band (OOB) Mode section.

Cisco NAC Agent

The Cisco NAC Agent is an optional component of the Cisco NAC solution. When the Agent is enabled for your Cisco NAC deployment, the Agent ensures that computers that access your network meet the system posture requirements you specify. The Cisco NAC Agent is a read−only, easy−to−use, small−footprint program that resides on user machines. When a user attempts to access the network, the Agent checks the client system for the software you require, and helps users acquire any missing updates or software.

Out−of−Band (OOB) Mode

In the Cisco NAC Appliance OOB deployment, the Cisco NAC Server communicates with the end host only during the authentication process, posture assessment, and remediation. After it is certified, the end host does not communicate with the Server. In OOB mode, the Cisco NAC Manager uses simple network management protocol (SNMP) to control switches and set VLAN assignments for ports. When the Cisco NAC Manager and Server are set up for OOB, the Manager can control the switch ports of supported switches. For a list of supported switches, go to:

http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html#wp40017.

The next few diagrams show how the Cisco NAC Manager uses OOB to control how a user gets access to the network. The sequence is as follows:

1. A PC is physically connected to a switch on the network (see Figure 3).
2. The switch sends the MAC address using SNMP to the Cisco NAC Manager (see Figure 3).
3. The Cisco NAC Manager verifies whether or not the PC is Certified.

    a. If the PC is not certified, the Cisco NAC Manager instructs the switch to assign the PC s switch port to an authentication VLAN (see Figure 4). Continue with step 4 through step 6.
    b. If the PC is certified, go to Step 5.
4. The PC communicates with the Cisco NAC Server and goes through authentication, posture assessment, and remediation (see Figure 4).
5. The Cisco NAC Server informs the Cisco NAC Manager that the PC is certified (see Figure 5).
6. The PC is connected to the network as a trusted device.

Figure 3: OOB SNMP Communication (1 of 3)

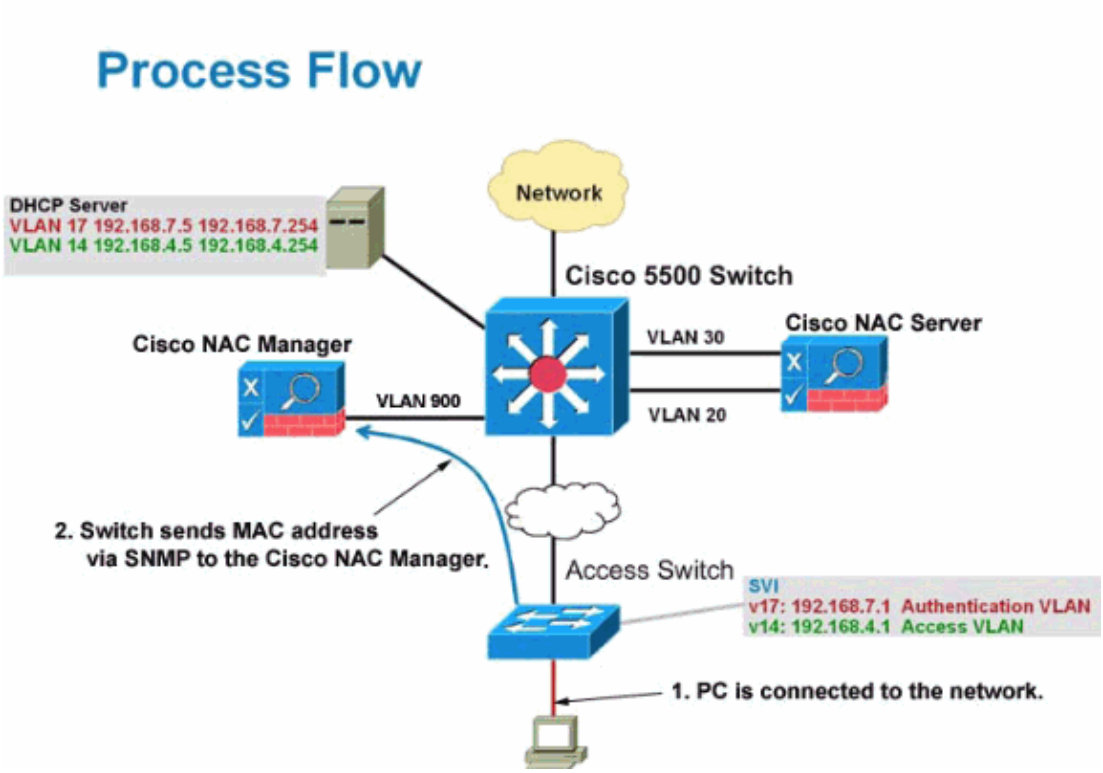


Figure 4: OOB SNMP Communication (2 of 3)

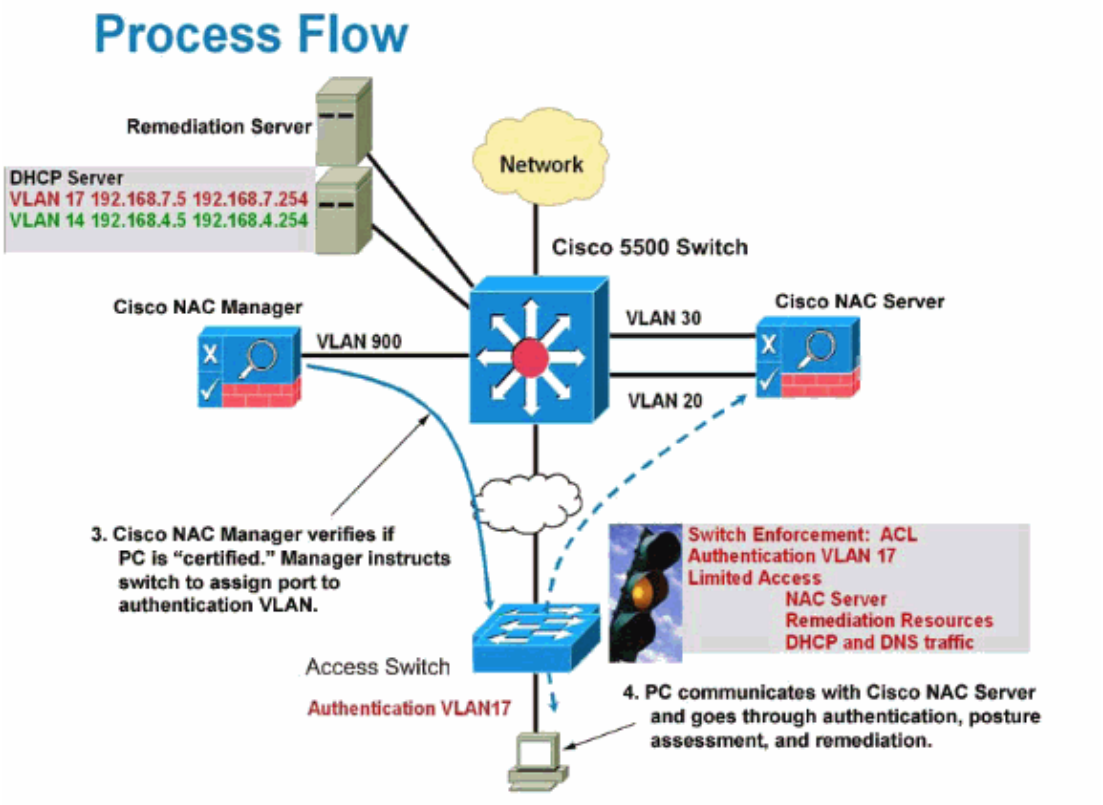
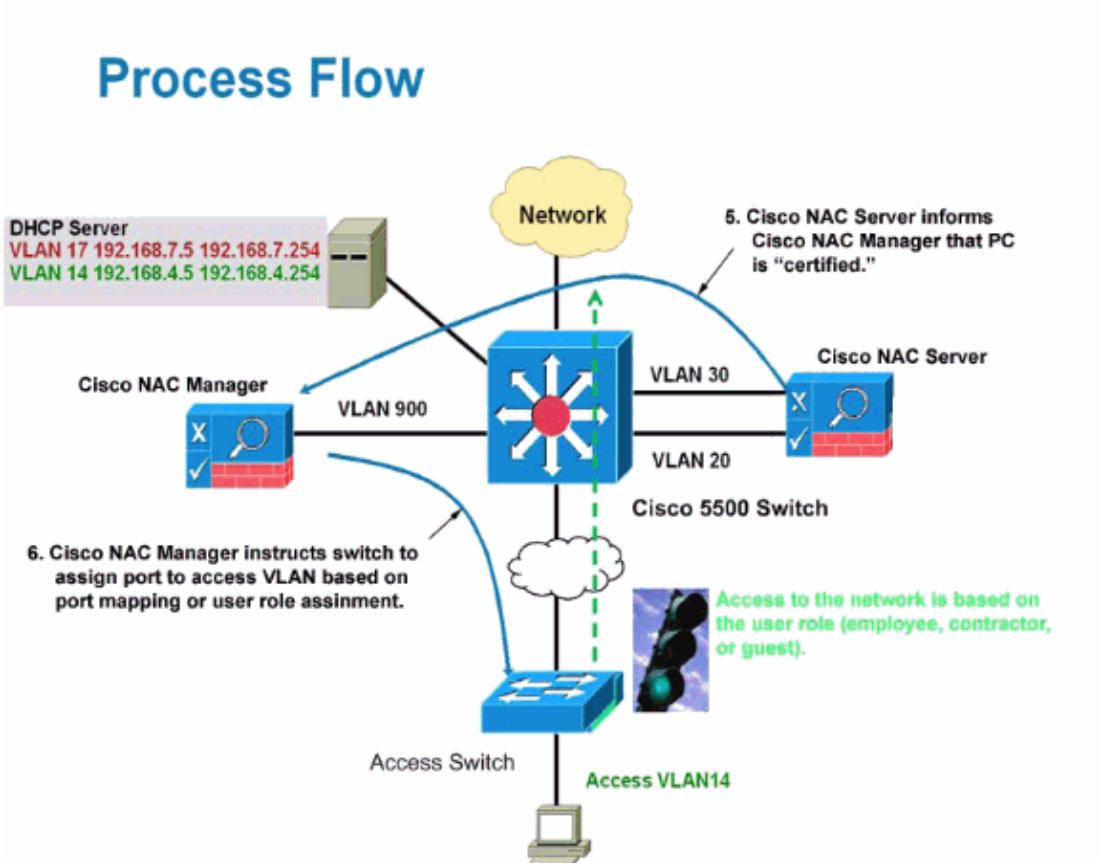


Figure 5: OOB SNMP Communication (3 of 3)



Design Considerations

When you consider a Layer 3 OOB NAC deployment, you should review several design considerations. These considerations are listed discussed in the following subsections, and a brief discussion of their importance is included.

End−point Classification

Several factors contribute to endpoint classification, including device types and user roles. Both device type and user role impact the endpoint role.

Possible device types

- Corporate devices
- Non−corporate devices
- Non−PC devices

Possible user roles

- Employee
- Contractor
- Guests

Initially, all endpoints are assigned to the unauthenticated VLAN. Access to the other roles is permitted after the identity and posture process is complete.

Endpoint Roles

The role of each type of endpoint must be initially determined. A typical campus deployment includes several roles, such as employees, guests, and contractors, and other endpoints, such as printers, wireless access points, and IP cameras. Roles are mapped to the edge switch VLANs.

Note: The Unauthenticated role initially maps all users to an unauthenticated VLAN for first−time authentication.

Role Isolation

It is vital to isolate the endpoint roles when you implement the Cisco NAC solution. Select an appropriate enforcement mechanism to provide traffic and path isolation for all traffic originating from unauthenticated and unauthorized host machines. In a Layer 3 OOB environment, the Layer 3 edge switch (using ACLs) acts as the enforcement point that ensures segregation between the clean and unauthenticated networks.

Traffic Flow

The NAC process begins when an endpoint connects to a NAC−managed switch. Traffic classified as unauthenticated is restricted by the ACLs applied on the unauthenticated VLAN. The endpoint is allowed to communicate to the Untrusted interface of the Cisco NAC Server to continue through the posture assessment and remediation process (there are several methods to perform posture assessment and remediation that are discussed later in the Update policies from Cisco.com on the Cisco NAC Manager. section). After authentication, the endpoint is moved to the trusted VLAN.

Cisco NAC Server Mode

A Cisco NAC Server can be deployed in either the virtual gateway (bridge) mode or the real−IP gateway (routed) mode.

Virtual Gateway (Bridge) Mode

The virtual gateway (bridge) mode is typically used when the Cisco NAC Server is Layer 2 adjacent to the endpoints. In this mode, the Server acts as a bridge and is not involved in the routing decision of the network traffic.

Note: The virtual gateway (bridge) mode is NOT applicable for the Layer 3 OOB ACL design.

Real−IP Gateway (Routed) mode

The real−IP gateway (routed) mode is applicable when the Cisco NAC Server is multiple hops away from the endpoint. When you use the Server as a real−IP gateway, specify the IP addresses of its two interfaces: one IP address for the trusted side (to provide for management from the Cisco NAC Manager) and one IP address for the untrusted side. The two addresses should be on different subnets. The untrusted interface IP address is used for communicating with the endpoint on the untrusted subnet. A Layer 3 OOB deployment using ACLs requires the endpoint to communicate with the untrusted interface for authentication and authorization purposes. Because real−IP mode uses a valid IP address for the untrusted interface, the Cisco NAC Server must be configured to function in real−IP gateway mode.

Scalability

A standard Cisco NAC Server can manage up to 5000 concurrent end users. The Layer 3 OOB ACL design is suited for a site serving no more than 5000 users. If you have multiple sites, you can have additional Servers

per site. If you have a single site that needs to serve more than 5000 users, you can use external load balancing techniques (for example, Application Control Engine (ACE) Load Balancer) to scale more than 5000 users for the single site.

Note: The ACE load balancer discussion is beyond the scope of this document.

Discovery Host

The Discovery Host is the fully qualified domain name (FQDN) or untrusted interface IP address used by the Cisco NAC Agent to discover the Cisco NAC Server located multiple hops away on the network. The Agent initiates the discovery process by sending UDP packets to the known Discovery Host address. Discovery packets must reach the NAC Server untrusted interface to receive a response. In the case of a Layer 3 OOB deployment, the Server is not in the path of data traffic on the authentication VLAN. Therefore, the Discovery Host setting must be configured to be the IP address of the untrusted interface of the Cisco NAC Server so that the agent can send the discovery packets directly to the Server.

User Experience (with Cisco NAC Agent)

Typically, corporate network administrators install the Cisco NAC Agent on client machines before issuing those machines to users. The Discovery Host IP address or resolvable name in the Cisco NAC Agent triggers discovery packets to be sent to the Untrusted Interface of the NAC Server, which automatically guides the client machine through the NAC process.

User Experience (without Cisco NAC Agent)

Endpoints without a Cisco NAC Agent (most likely guests, contractors, and non−corporate assets) may not automatically continue through the NAC process. Manual and guided methods exist to assist the endpoints that do not have the Agent. For more detail, see Endpoint to Cisco NAC Server Communication section.

Note: For the best end−user experience possible, use certificates that are trusted by the end−user's browser. Using self−generated certificates on the Cisco NAC Server is not recommended for a production environment.

Cisco NAC Process Flows

This section explains the basic process flow for a NAC OOB solution. Scenarios are described both with and without a Cisco NAC Agent installed on the client machine. This section shows how the Cisco NAC Manager controls the switch ports using SNMP as the control medium. These process flows are macro−analytical in nature and contain only functional decision steps. The process flows do not include every option or step that occurs and do not include authorization decisions that are based on endpoint assessment criteria.

Refer to the process flow diagram shown in Figure 7 for the circled steps shown in Figure 6.

Figure 6: NAC Process Flow for Layer 3 Out−Of−Band NAC Solution

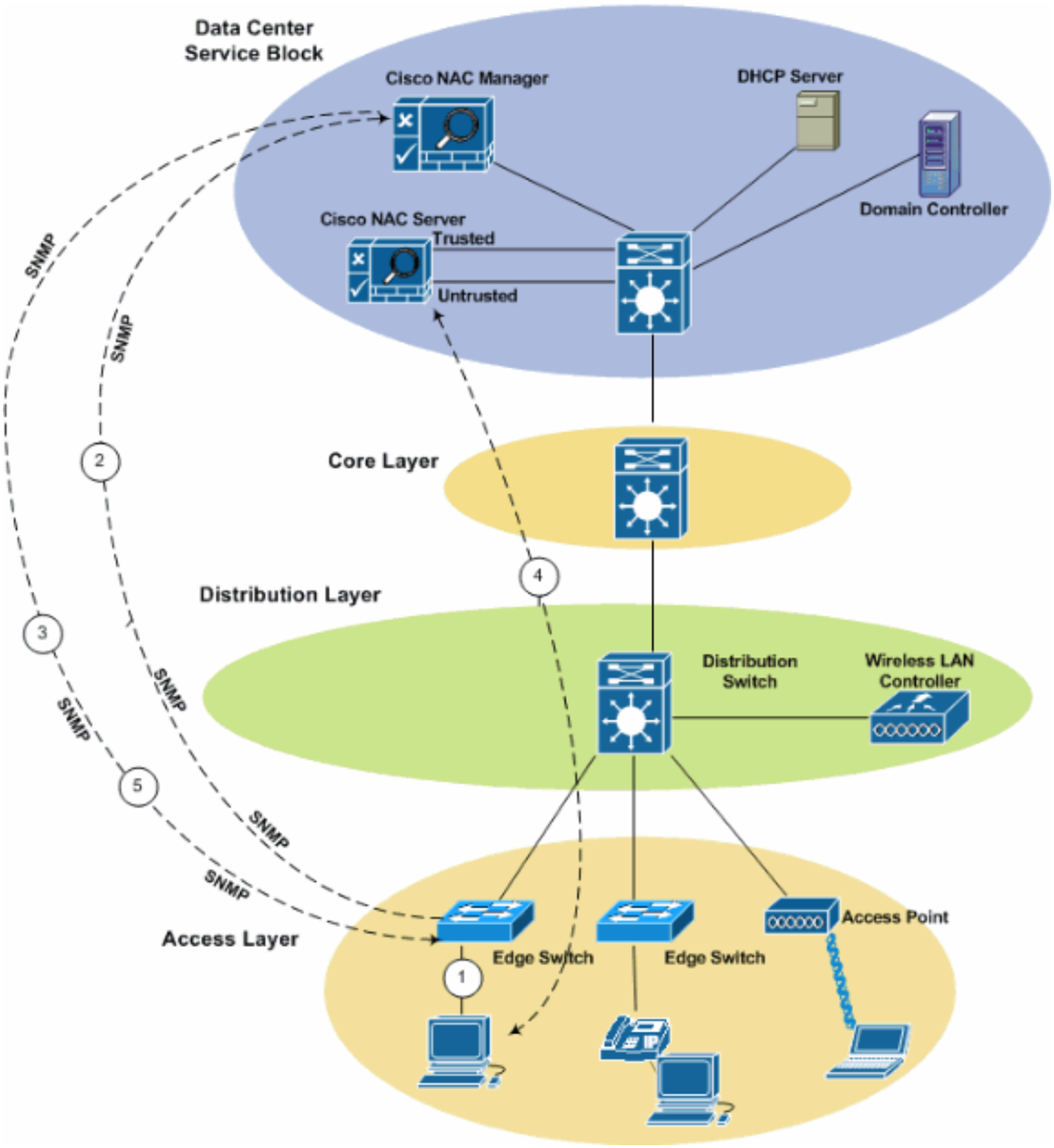
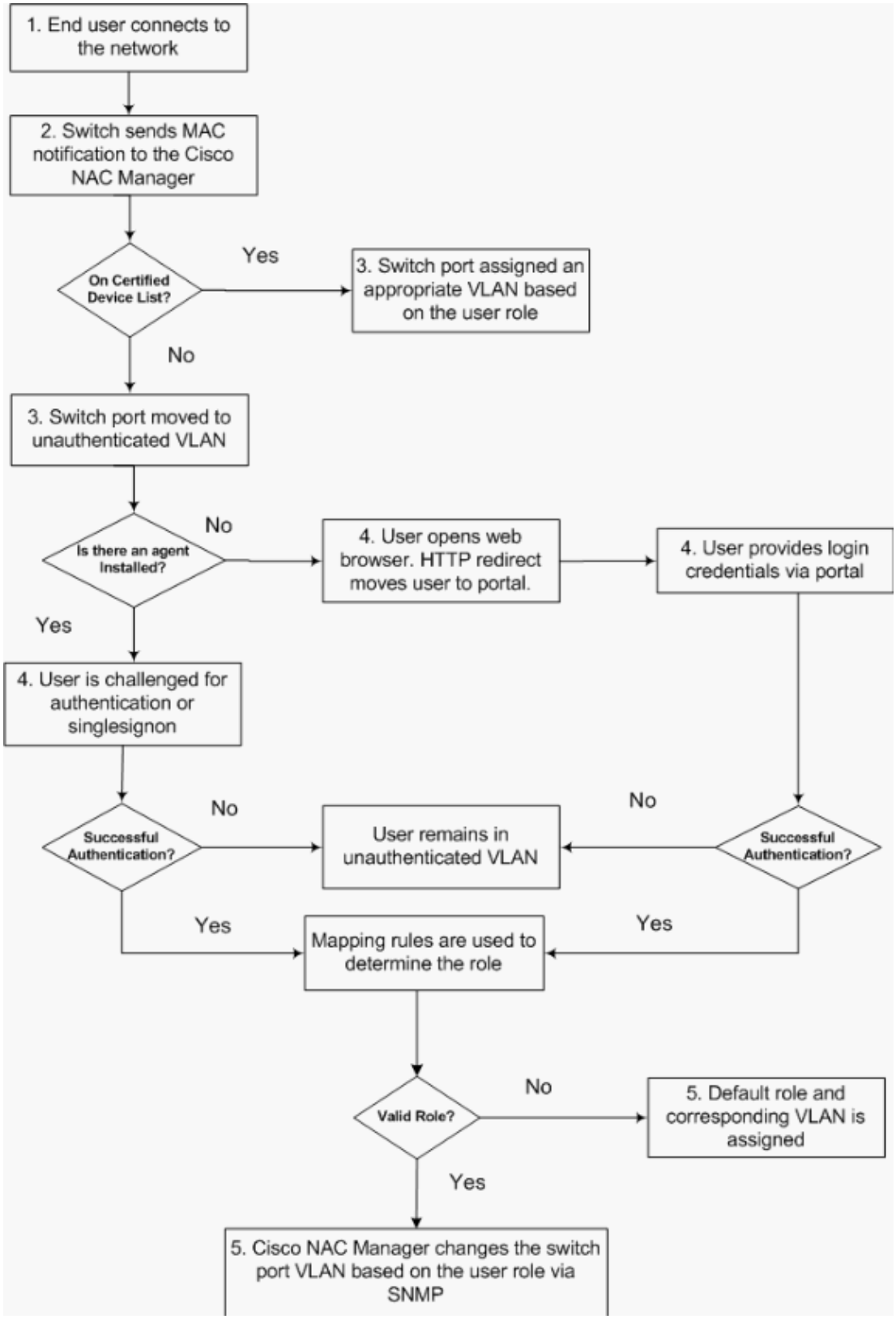


Figure 7: Process Flow Diagram



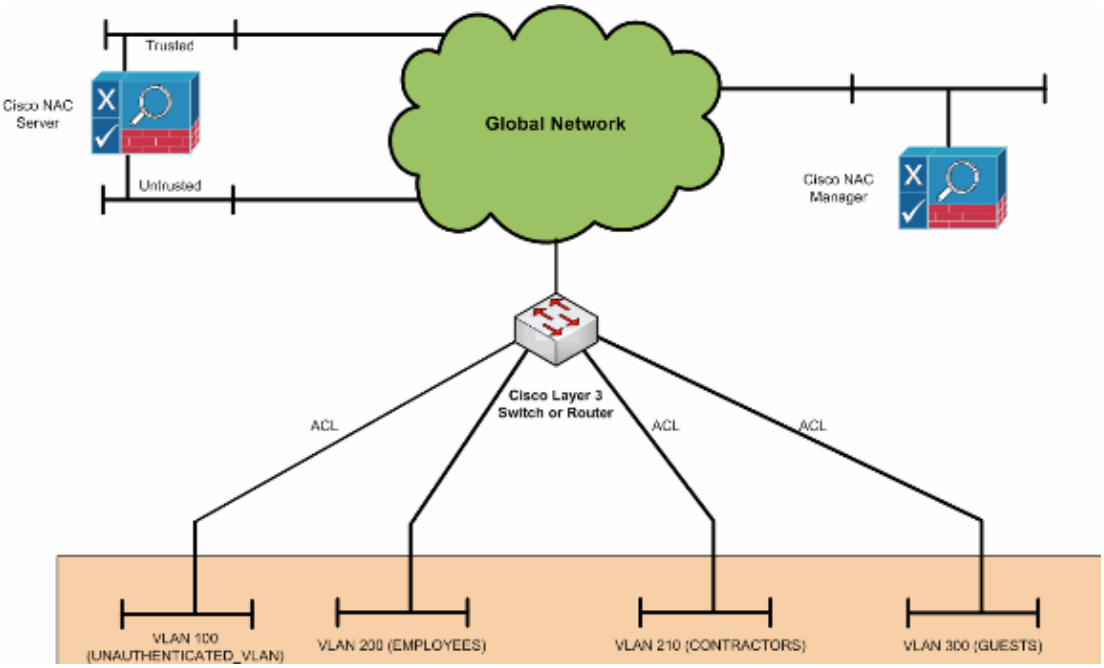
Cisco NAC Solution Implementation

In a Layer 3 OOB NAC design that uses ACLs, the Cisco NAC Server guides authentication functions, but the Server is not the policy enforcement point in the network. The edge switch acts as an enforcement point during the authentication, quarantine, and access stages. Based on this shift, some additional changes are required on the edge switch.

Role Isolation

For a successful NAC deployment, isolation of the endpoints is critical. After the endpoint classification design is determined, the permissions between classes should be determined. A recommended approach follows, based on Figure 8.

Figure 8: Role Isolation Approach in the Cisco NAC OOB Solution



Note: The Cisco NAC Manager interface and the Cisco NAC Server's trusted interface are illustrated above on different VLANs. However, these two interfaces can be on the same VLAN if the Server is deployed in the real−IP gateway mode.

The unauthenticated VLAN requires access to these resources:

- Infrastructure services such as DHCP and DNS
- Authentication servers, typically the domain controller for Windows domain login prior to NAC validation
- NAC Server's untrusted Interface
- Remediation servers (optional)

The employee VLAN typically has unrestricted access to all resources, the contractor VLAN typically has limited access to a subset of resources, and the guest VLAN typically only has access to the Internet.

Access List Technique

An access list (ACL) is used to specify network traffic. After you specify traffic with an ACL, you can do a variety of things with the traffic. For example, you can allow it, deny it, limit it, or use it to restrict routing updates.

In the ACL technique, a set of ACLs is applied to each new VLAN interface you create based on your requirements. The CLI commands given in the following subsections shows the commands required to configure trusted and untrusted network path isolation using VLAN ACLs. Follow the procedure below to implement ACLs.

Note: Addition of VLANs for role isolation and configuring ACLs on those VLANs must be performed on every edge switch. This work should be part of NAC deployment readiness.

1. Before implementing NAC, examine the existing VLAN configuration.

   The CLI commands shown in the following text show how the employees VLAN is typically configured before NAC is implemented.

   ```
   !
   int vlan
   200description EMPLOYEES_Vlan
   ip address 10.100.1.1 255.255.255.0
   !
   ```

2. Configure additional VLANs.

   The pre−deployment NAC planning requires configuring the additional VLANs and relevant ACLs applied to the VLAN interfaces. As an example, the following CLI text shows how to add a new Layer 3 VLAN for each of the unauthenticated, employees, contractors, and guest roles.

   ```
   !
   int vlan
   100description UNAUTHENTICATED_Vlan
   ip address 172.16.1.1 255.255.255.0
   !
   int vlan
   200description EMPLOYEES_Vlan
   ip address 10.100.1.1 255.255.255.0
   !
   int VLAN
   210description CONTRACTORS_Vlan
   ip address 10.120.1.1 255.255.255.0
   !
   int vlan
   300description GUESTS_Vlan
   ip address 192.168.1.1 255.255.255.0
   !
   ```

3. Implement restrictions on the unauthenticated role.

   Unauthenticated devices in the unauthenticated role typically require access to resources on the clean network, such as DNS, DHCP, Active Directory, and remediation servers. They also require access to the untrusted interface of the Cisco NAC Server, In the sample configuration below, the unauthenticated role has access to resources on the 10.10.10.0 / 24 networks and the Cisco NAC Server's untrusted interface.

   ```
   !
   ! this access−list permits traffic destined to devices on 10.10.10.x
   ! this should be a consistent ACL that can be applied across all L3
   switches
   !
   ip host NAC_SERVER_UNTRUSTED_INTERFACE <IP_Address>
   access−list 100 permit ip any host NAC_SERVER_UNTRUSTED_INTERFACE
   access−list 100 permit ip any 10.10.10.0 255.255.255.0
   !
   !
   ! then apply this access−list to the UNAUTHENTICATED_Vlan
   !
   int vlan100
   description UNAUTHENTICATED_Vlan
   ip address 172.16.1.1 255.255.255.0
   ip access−group 100 in
   !
   ```

```
int vlan200
description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
int vlan300
description GUESTS_Vlan
ip address 192.168.1.1 255.255.255.0
!
```

4. Implement restrictions on the guests VLAN.

   Typically, the guest role has access to the Internet only. All access to unneeded resources, such as all internal networks, should be explicitly denied. The only exception may be an internal DNS server.

```
!
! ACL 100 permits traffic destined to devices on 10.10.10.0 / 24
! this should be a consistent ACL that can be applied across all L3
switches
!
access-list 100 permit ip any 10.10.10.0 255.255.255.0
!
!
! ACL 101 for Guests should deny access to all internal networks
! while DNS is permitted
!
access-list 101 permit udp any host GUEST_DNS_SERVER eq 53
access-list 101 deny ip any 10.0.0.0 255.0.0.0
access-list 101 deny ip any 192.168.0.0 255.255.0.0
access-list 101 deny ip any 172.16.0.0 255.240.0.0
access-list 101 permit ip any any
!
int VLAN100
description UNAUTHENTICATED_VLAN
ip address 172.16.1.1 255.255.255.0
ip access-group 100 in
!
int VLAN200
description EMPLOYEES_VLAN
ip address 10.100.1.1 255.255.255.0
!
!
int VLAN300
description GUESTS_VLAN
ip address 192.168.1.1 255.255.255.0
ip access-group 101 in
!
```

Endpoint to Cisco NAC Server Communication

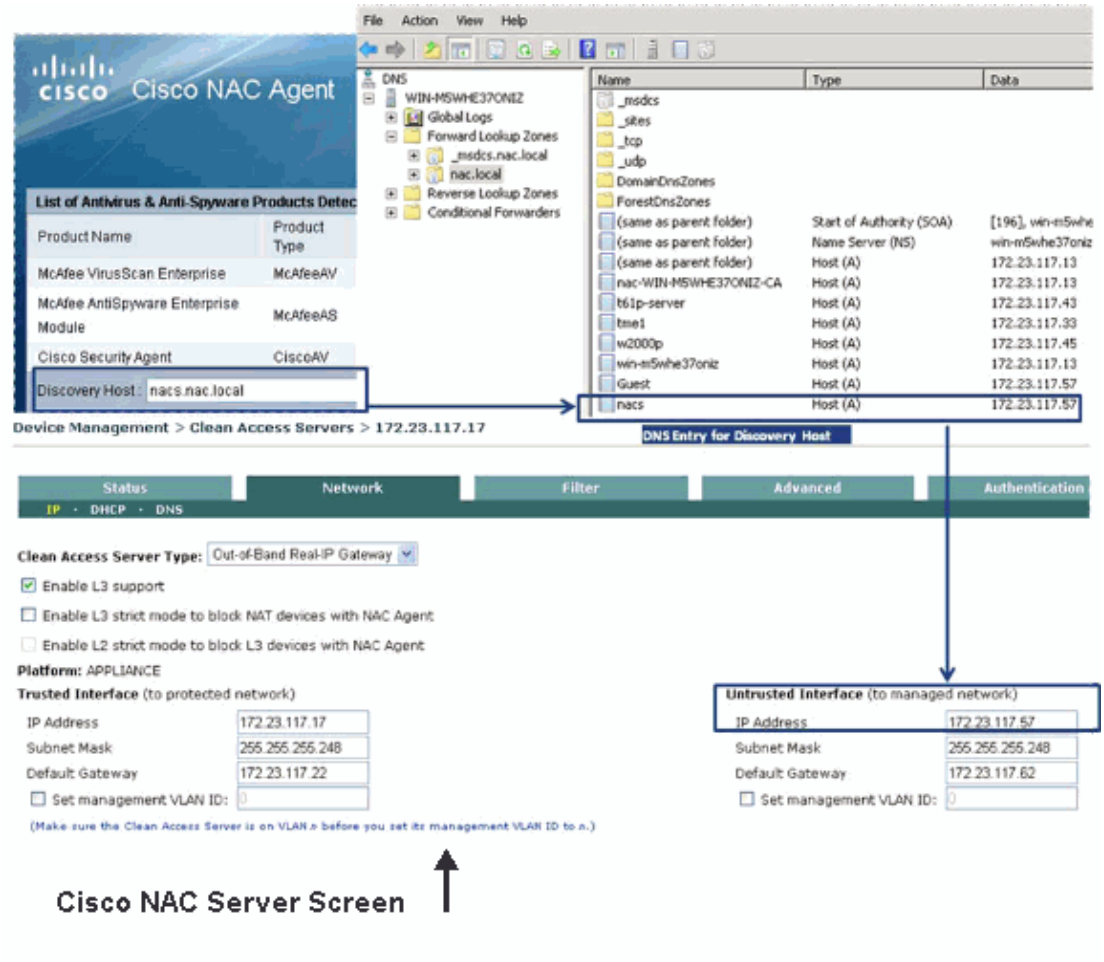
The Cisco NAC Server gets MAC information from either the Cisco NAC Agent or a web login page enabled for ActiveX or Java Applet to determine the device MAC address and report it back to the Cisco NAC Manager.

Cisco NAC Agent

The Cisco NAC Agent needs to communicate with the NAC Server untrusted interface to initiate the login process. The Agent tries to discover the Server based on the known Discovery Host value. As shown in Figure 9, the Discovery Host value in the Cisco Agent (nacs.nac.local) points to the untrusted interface (172.23.117.57) on the NAC Server. Figure 9 shows a combination of three screens.

See the Agent login. section for more details on logging in through the Cisco NAC Agent.

Figure 9: Discovery Host Pointing to Untrusted Interface of the NAC Server



Note: The Cisco NAC Agent does not appear if the Agent is NOT able to receive any response back from the Cisco NAC Server.

Web Login

Web login is typically required for guest login sessions. When the ACL isolation technique is used, the NAC Server untrusted interface is not directly in the path of the data traffic. Therefore, the user is not automatically redirected to the login page when the browser is first opened. Two options can enable the end host to get the login page.

Option 1

- Create a guest login URL known to the users (for example, guest.cisco.com).
- The guest must then open a browser and enter that URL, which causes a re−direct to the login page.

Option 2

- Create a dummy DNS server for the unauthenticated user subnet.
- This dummy DNS server resolves every URL to the untrusted interface of the Cisco NAC Server.
- When the guest opens a browser, regardless of which URL he is trying to reach, he is redirected to the login page.
- When the user is then moved to the appropriate VLAN for his role, he gets a new DNS address assignment when performing IP release or renew on a successful login.

In a Layer 3 OOB design, users who log in using a web page download and execute either an ActiveX control (for Internet Explorer browsers) or a Java applet (for non−IE browsers). The ActiveX control (or Java) must be running to perform the following:

- Collect the MAC address of the host, which is reported to the Cisco NAC Server and the Cisco NAC Manager to provide the IP address and MAC address mapping.
- Perform IP release and renew of the endpoint client.

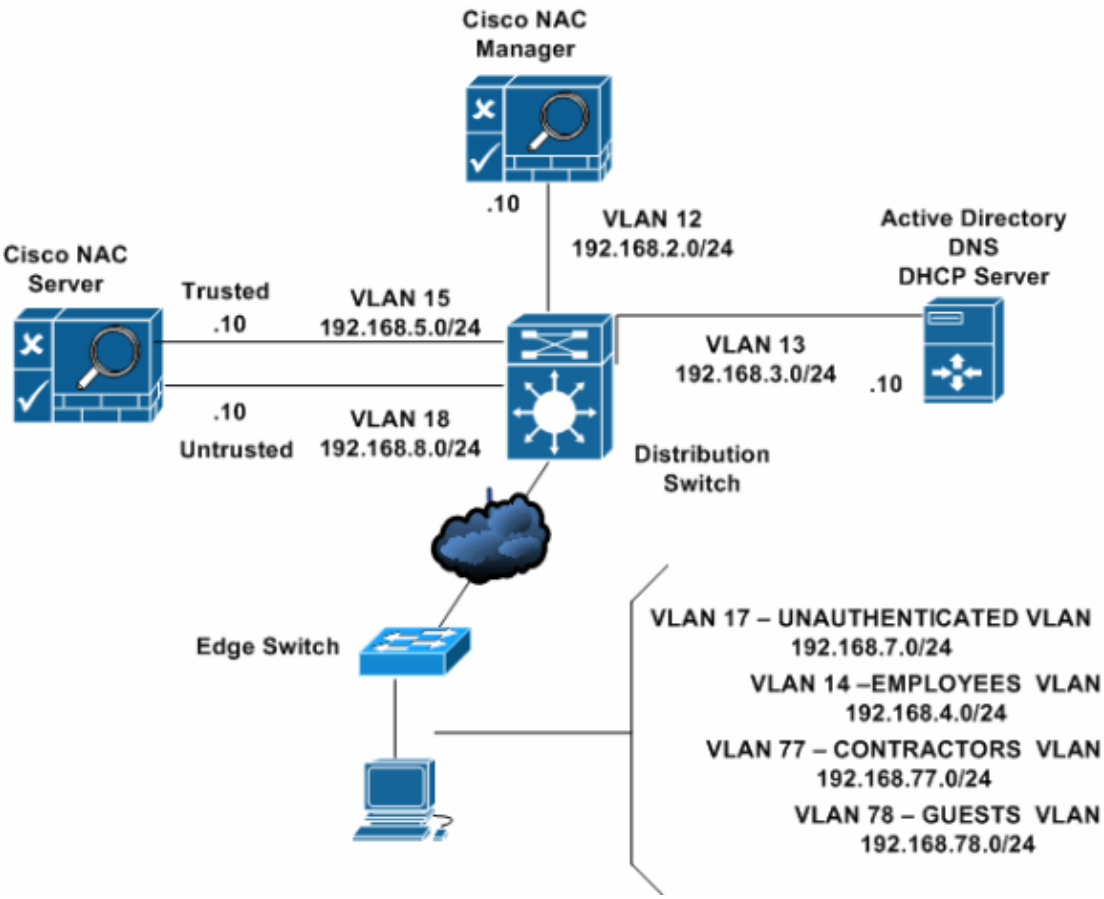
Note: The decision to allow guests to use internal or external DNS is a policy decision each organization must make. Using a publicly−based DNS service poses the least potential risk in this approach.

See Web login, for more details on logging in through a web page.

NAC Layer 3 OOB ACL Configuration Example

To successfully deploy a NAC OOB solution, the NAC components need to be configured to match the desired architecture. Figure 10 shows a Layer 3 NAC OOB logical network diagram that is used in this section to illustrate the relevant configuration of Cisco NAC Manager, Cisco NAC Server, and an edge switch for NAC Layer 3 OOB deployment using ACLs.

Figure 10: NAC Layer 3 OOB Logical Topology Diagram



To configure a Layer 3 real−IP OOB NAC deployment, follow these steps:

1. Configure the edge switch for enforcement.

a. First, create three additional VLANs (UNAUTHENTICATED, CONTRACTORS, and GUESTS) on the edge switch. The existing production VLAN will be used for the employees.
b. Configure and apply ACLs on each VLAN to restrict access to the network based on the assigned role.

◊ Unauthenticated role: VLAN 17 and ACL name: UNAUTH_ACL

```
! Create SVI for Un-auth VLAN

Edge Switch(config)#interface vlan 17
Edge Switch (config)#ip address 192.168.7.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10
! 192.168.3.10 is the dhcp server (see Figure 10)

! Configure ACL for Un-auth Role
Edge Switch(conf)#ip access-list extended UNAUTH_ACL
   remark Allow Discovery packets from Agent to NAC Server
   permit udp any host 192.168.8.10 eq 8906
   remark Allow Discovery packets from Agent to NAC Server for ADSSO
   permit udp any host 192.168.8.10 eq 8910
   remark Allow Web traffic from PC to NAC Server
   permit tcp any host 192.168.8.10 eq www
   remark Allow SSL traffic from PC to NAC Server
   permit tcp any host 192.168.8.10 eq 443
   remark Allow DHCP permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark Allow Web traffic to the Remediation Server
   permit tcp any host 192.168.3.10 eq www

! Apply ACL for Un-auth VLAN Interface

Edge Switch(config)#interface vlan 17
Edge Switch(config)# ip access-group UNAUTH_ACL in
```

◊ Contractor role: VLAN 77 and ACL name: CONTRACTOR_ACL

```
! Create SVI for Contractor VLAN

Edge Switch(config)#interface vlan 77
Edge Switch (config)#ip address 192.168.77.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL for Contractor Role

Edge Switch(conf)#ip access-list extended CONTRACTOR_ACL
   remark Allow DHCP permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark Allow traffic to DMZ Subnet
   permit ip any 192.168.3.0 0.0.0.255
   remark deny rest of the internal resources
   deny ip any 10.0.0.0 255.0.0.0
   deny ip any 192.168.0.0 255.255.0.0
   deny ip any 172.16.0.0 255.240.0.0
   remark permit internet
   permit ip any any

! Apply ACL for Contractor VLAN Interface

Edge Switch(config)#interface vlan 77
Edge Switch(config)# ip access-group CONTRACTOR_ACL in
```

◊ Guest role: VLAN 78 and ACL name: GUEST_ACL

```
! Create SVI for GUEST VLAN

Edge Switch(config)#interface vlan 78
Edge Switch (config)#ip address 192.168.78.1 255.255.255.0
Edge Switch (config)#ip helper−address 192.168.3.10

! Configure ACL for Guest Role

Edge Switch(conf)#ip access−list extended GUEST_ACL
   remark Allow DHCP
   permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark deny access to the internal resources
   deny ip any 10.0.0.0 255.0.0.0
   deny ip any 192.168.0.0 255.255.0.0
   deny ip any 172.16.0.0 255.240.0.0
   remark permit internet
   permit ip any any

! Apply ACL for GUEST VLAN Interface

Edge Switch(config)#interface vlan 78
Edge Switch(config)# ip access−group GUEST_ACL in
```

◊ Employee role: VLAN 14 and ACL: Production_ACL

The existing production VLAN can be used to move the employee from the unauthenticated VLAN to the employee VLAN. After the end client is moved to this VLAN, the Cisco NAC Agent still attempts to discover the Cisco NAC Server. The Agent is designed to behave this way. If the Agent is able to reach the Server, the Agent pops up and attempts to perform the login process again, even though the machine has already granted access. Obviously, this is an unwanted behavior and administrators must ensure that UDP 8906 discovery packets originating from the Agent are dropped. Employee_ACL is configured to drop these discovery packets.

```
! Use Existing Production Layer 3 VLAN for Employees

Edge Switch(config)#interface vlan 14
Edge Switch (config)#ip helper−address 192.168.3.10

! Configure ACL to prevent discovery packets from reaching the
untrusted interface on the NAC Server

Edge Switch(conf)#ip access−list extended Employee_ACL
   remark Deny Discovery packets from Agent to NAC Server
   deny udp any host 192.168.8.10 eq 8906
   permit ip any any

! Apply ACL for Employee VLAN Interface

Edge Switch(config)#interface vlan 14
Edge Switch(config)# ip access−group Employee_ACL in
```

2. Perform initial setup of Cisco NAC Manager and Server.

   Cisco NAC Manager and Server installation is performed through console access. The install utility guides you through the initial configuration for both Manager and Server. To perform initial setup, go to:

   http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html
3. Apply license to the Cisco NAC Manager.

After you perform the initial setup through the console, access the Cisco NAC Manager GUI to continue configuring the Cisco NAC Manager and Server. First upload the Manager and Server licenses that came with the appliances. For more detail on uploading the licenses, go to:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html#wp11

Note: All the Cisco NAC Manager and Server licenses are based on the eth0 MAC address of the Manager. In a failover setup, the licenses are based on the eth0 MAC address of both primary and secondary Cisco NAC Managers.

4. Update policies from Cisco.com on the Cisco NAC Manager.

   Cisco NAC Manager must be configured to retrieve periodic updates from the central update server located at Cisco. The Cisco NAC Appliance Supported AV/AS Product List is a versioned XML file distributed from a centralized update server that provides the most current matrix of supported antivirus and antispyware vendors and product versions used to configure antivirus or antispyware rules and antivirus or antispyware definition update requirements for posture assessment and remediation. This list is updated regularly for the antivirus and antispyware products and versions supported in each Cisco NAC Agent release and includes new products for new Agent versions. Note that the list provides version information only. When the Cisco NAC Manager downloads the supported antivirus and antispyware product list, it is downloading the information about what the latest versions are for antivirus and antispyware products; it is not downloading actual patch files or virus definition files. Based on this information, the Agent can then trigger the native antivirus or antispyware application to perform updates. For more information about how updates are retrieved, go to:

   http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html#wp13518

5. Install certificates from a third−party certificate authority (CA).

   During installation, the configuration utility script for both the Cisco NAC Manager and Cisco NAC Server requires you to generate a temporary SSL certificate. For the lab environment, you may continue to use the self−signed certificates; however, they are not recommended for a production network.

   For more information on installing certificates on the Cisco NAC Manager from a third−party CA, go to:

   http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_admin.html#wp1078

   For more information on installing certificates on the Cisco NAC server from a third−party CA, go to:

   http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_admin.html#wp10401

   Note: If you are using the self−sign certificates in the lab environment, the Cisco NAC Manager and Cisco NAC Server each need to trust the certificate of the other, which requires you to upload the certificates for both as a Trusted Certificate Authority under SSL > Trusted Certificate Authorities.

6. Add the Cisco NAC Server to the Cisco NAC Manager.

   To add the NAC Server to the NAC Manager, follow these steps:

   a. Click **CCA Servers** under the Device Management pane (see Figure 11).
   b. Click the **New Server** tab.
   c. Use the *Server IP Address* box to add the IP address of the NAC Server's Trusted interface.
   d. In the *Server Location* box, enter **OOB NAC Server** as the server location.
   e. Choose **Out−of−Band Real−IP−Gateway** from the *Server Type* dropdown list.

f. Click **Add Clean Access Server**.

Figure 11: Adding Cisco NAC Server to Cisco NAC Manager

After you add the Cisco NAC Server, it appears in the list under the List of Servers tab (see Figure 12).

Note: The Cisco NAC Manager and Cisco NAC Server have to trust each other's certificate authority (CA) for the Manager to successfully add the Server.

7. Configure the Cisco NAC Server.

a. As shown in Figure 12, click the **List of Servers** tab.
b. Click the **Manage** icon (circled) for the Cisco NAC Server to continue the configuration.

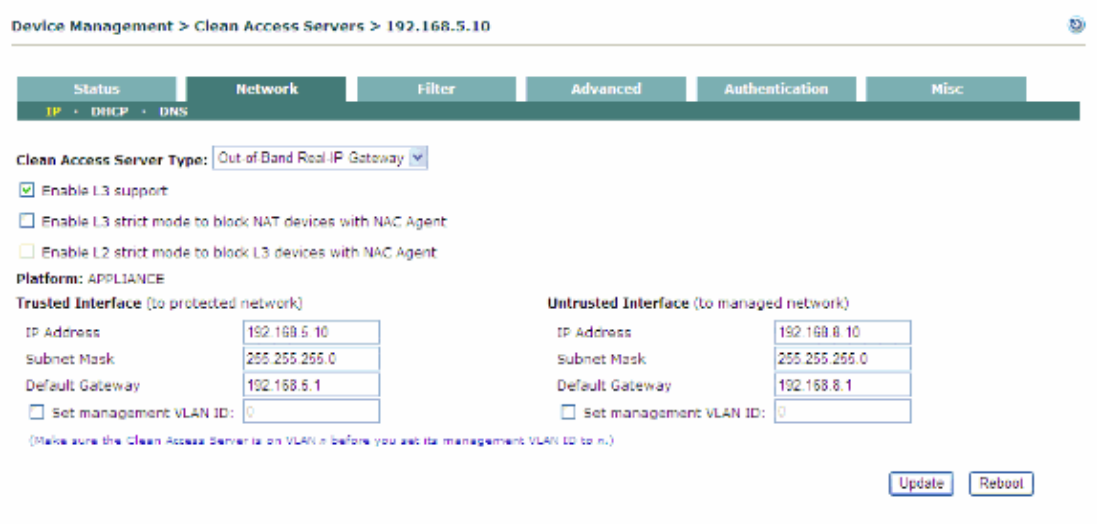
Figure 12: Cisco NAC Server Managed by Cisco NAC Manager

After you click the Manage icon, the screen shown in Figure 13 appears.

8. Enable Layer 3 support.

a. Click the **Network** tab (Figure 13).
b. Check the **Enable L3 Support** checkbox.
c. Check the **Enable L3 strict mode to block NAT devices with Clean Access Agent** checkbox.
d. Click **Update**.
e. Reboot the Cisco NAC Server as instructed.

Figure 13: Cisco NAC Server Network Details



Note: Always generate the certificate for the Cisco NAC Server with the IP address of its UNTRUSTED interface. For name−based certificate, the name should resolve to the untrusted interface IP address. When the endpoint communicates with the untrusted interface of the Server to begin the NAC process, the Server will redirect the user to the certificate hostname or IP. If the certificate points to the trusted interface, the login process will not function correctly.

In Figure 13 above, you see that the two default gateways are present. Only the default gateway configured on the trusted interface is applicable. The value on the untrusted interface is not used for forwarding the traffic. The traffic that is forwarded from the untrusted interface is dependent on the static route covered in the next step.

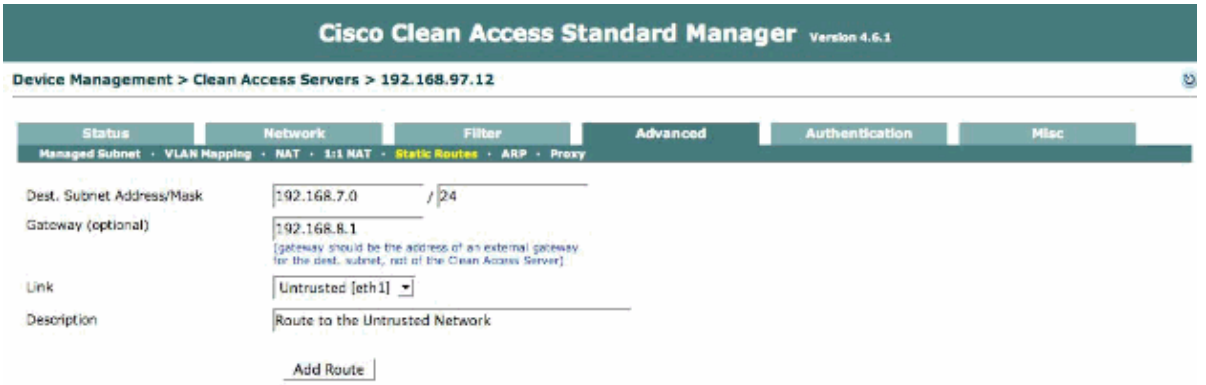
9. Configure static routes.

    a. After the Cisco NAC Server reboots, return to the Server and continue with the configuration.

    The Server must use the untrusted interface to communicate with endpoints on the unauthenticated VLAN.

    b. Go to **Advanced > Static Routes** (see Figure 14) to add routes to the unauthenticated VLAN.
    c. Fill in the appropriate subnets for the unauthenticated VLANs.
    d. Click **Add Route**.
    e. Select **Untrusted interface [eth1]** for these routes.

Figure 14: Adding Static Route to Reach the Unauthenticated User Subnet



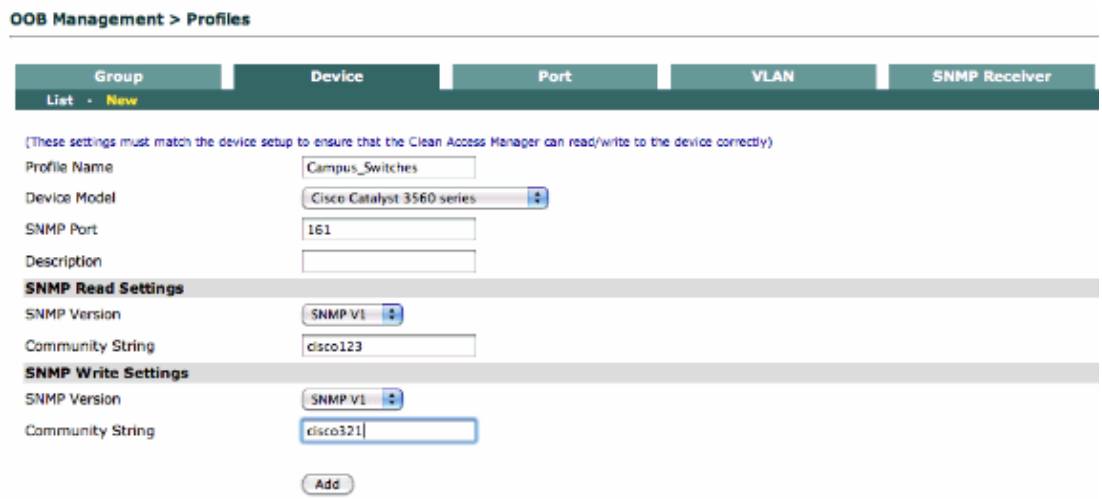
10. Set up profiles for switches in the Cisco NAC Manager.

    a. Select **OOB Management > Profiles > Device > Edit** (see Figure 15).

b. Fill in the Device Profile information, using the example as a guide.

Each switch will be associated with a profile. Add a profile for each type of edge switch the Cisco NAC Manager will manage. The Manager supports SNMPv1, SNMPv2c, and SNMPv3. This example covers SNMPv1 only. You may want to configure SNMPv2 or SNMPv3c for more secure SNMP communication between the Manager and the switch.

Figure 15: SNMP Profile Used to Manage the Switch



c. Set up the switch configuration for SNMP.

The edge switch should be configured for the same SNMP read/write community strings as those configured on the Cisco NAC Manager. See the CLI commands below.

```
3560-remote(config)#snmp-server community cisco123 RO
3560-remote(config)#snmp-server community cisco321 RW
```

d. Select **OOB Management** > **Profiles** > **Port** > **New** (see Figure 16).

For individual port control, configure a port profile under **OOB Management** > **Profiles** > **Port** that includes the default unauthenticated VLAN and default access VLAN. In the access VLAN section, specify the User Role VLAN using the **Access VLAN** dropdown. The Cisco NAC Manager changes the unauthenticated VLAN to the access VLAN based on the VLAN defined in the role where the user belongs.

Define the port profile to control the port's VLAN based upon the user roles and VLANs implemented.

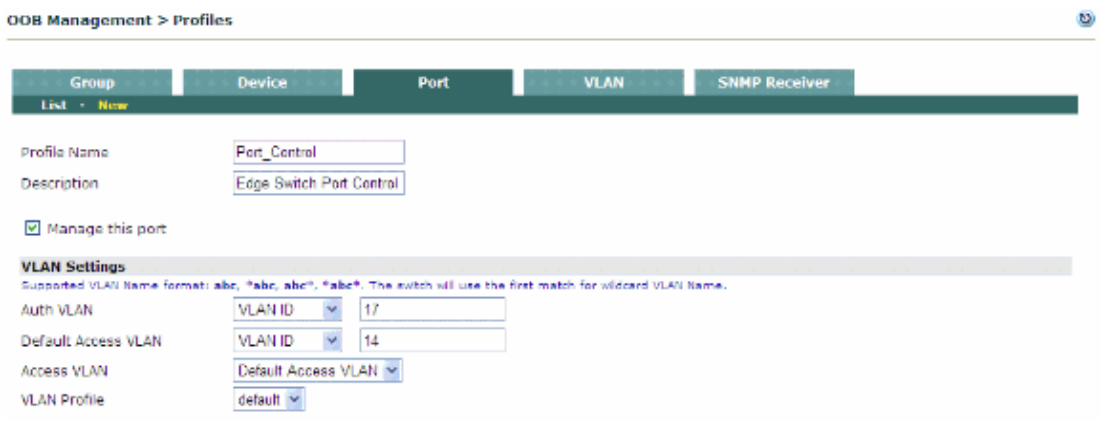
The Auth VLAN is the UNAUTHENTICATED VLAN (VLAN 17) to which unauthenticated devices are initially assigned.

The Default Access VLAN is the EMPLOYEES VLAN (VLAN 14). This VLAN is used if the authenticated user does not have a role−based VLAN defined.

The Access VLAN can override the default VLAN to a user role VLAN, which is defined under the user role (for more information about setting up user roles, see the Configure user roles. section). LDAP mappings can be used to map user roles in NAC to LDAP groups. For more information, go to:

http://www.cisco.com/en/US/products/ps6128/products_tech_note09186a0080846d7a.shtml

Figure 16: Port Profile to Manage the Switch Port



Note: You can also define VLAN names instead of IDs. If you define VLAN names, you can have different VLAN IDs on different switches across the campus, but the same VLAN name attached to a particular role.

Additional options are available under the port profile for IP release and renew options. Scroll down the page shown in Figure 16 to see these options.

If the user is behind an IP phone, uncheck the Bounce the port after VLAN is changed checkbox (see Figure 17), which, if checked, might reboot the IP phone when the port is bounced.

Figure 17: Various Options Available under Port Profile

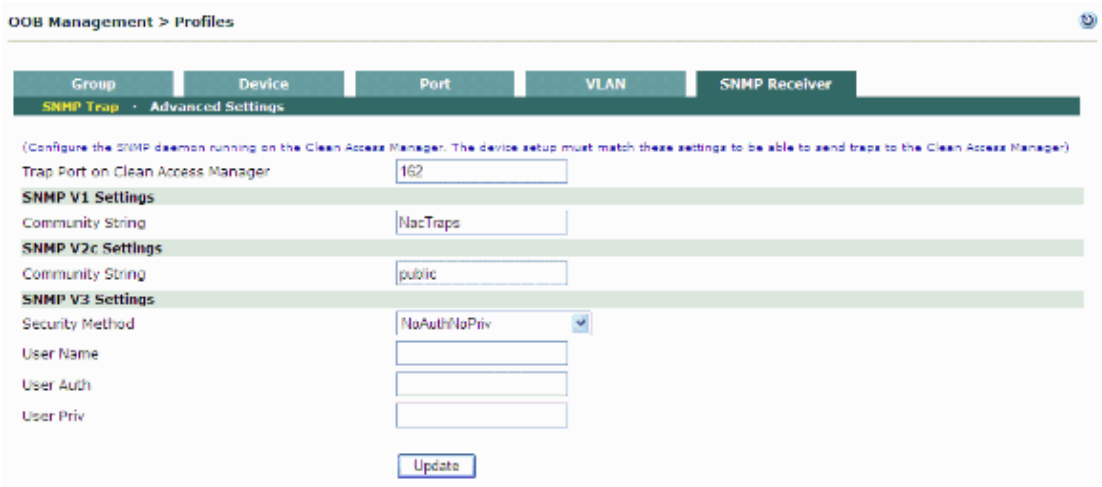
11. Configure SNMP receiver settings.

    In addition to setting up the SNMP community string for read or write, you must also configure the Cisco NAC Manager to receive SNMP traps from the switch. These traps are sent when the user connects and disconnects from the port. When the Cisco NAC Server sends the MAC/IP address information of a particular endpoint to the Manager, the Manager builds a mapping table internally for MAC/IP and switch port.

Note: You must configure all switches to send traps or informs to the Cisco NAC Manager using the community strings defined in Figure 18.

a. Select **OOB Management > Profiles > SNMP Receiver** (see Figure 18).
b. Configure the SNMP trap settings using the screen in Figure 18 as a guide.

Figure 18: NAC Manager SNMP Receiver Setting to Collect SNMP Traps and Informs



c. To configure the switch settings for SNMP traps, increase the default switch Clean Access Manager (CAM) flush timer to 1 hour (3600 in the CLI box below) per Cisco best practice recommendations for NAC OOB. The CLI sample shows the mac−address−table aging−time parameter set to 3600.

Setting the timer to 1 hour reduces the frequency of MAC notifications sent out of already connected devices to the Cisco NAC Manager. Use the source trap command to specify the source address that is used to send out the traps.

```
snmp−server enable traps mac−notification
snmp−server host 192.168.2.33 informs NacTraps
snmp−server trap−source Vlan 2
mac−address−table aging−time 3600
```

Optionally, configure linkup and linkdown traps to send to the Cisco NAC Manager (not shown in the CLI sample). These traps are used only in a deployment scenario where the end hosts are NOT connected behind an IP phone.

Note: SNMP informs are recommended because they are more reliable than the SNMP traps. Also, consider QoS for SNMP in a high−traffic network environment.

12. Add switches as devices in the Cisco NAC Manager.

a. Select **OOB Management > Devices > Devices > New** (see Figure 19).

The switch profile created in Step 10 will be used to add the switch.
b. Under the Device Profile, use the profile you created, but do not change the Default Port Profile value when you add the switch.

Note: For the Default Port Profile, always select uncontrolled, because you never manage all the ports of the access switch. A minimum of one uplink port must be uncontrolled. Therefore, you must add the switch with an uncontrolled port profile and then select the ports that needs to be managed.

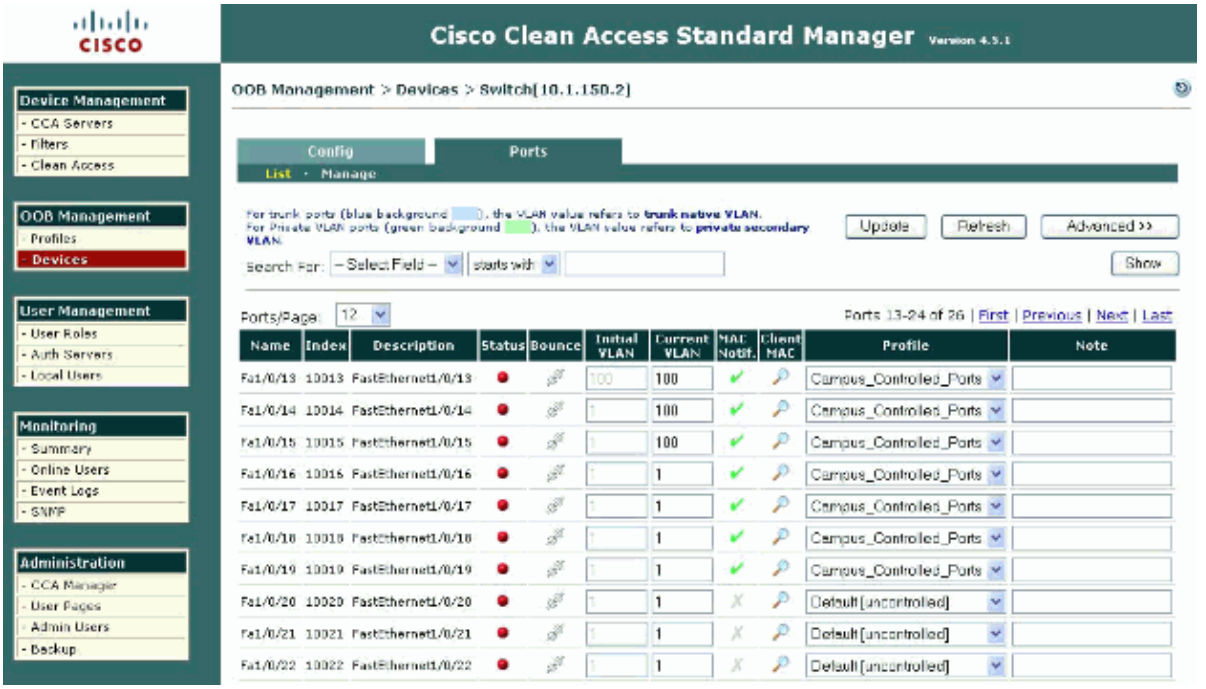
Figure 19: Adding an Edge Switch in the Cisco NAC Manager to Control Using SNMP

c. After the switch is added to the Cisco NAC Manager, select the ports that you want to manage.

13. Configure switch ports for the devices to be managed by NAC.

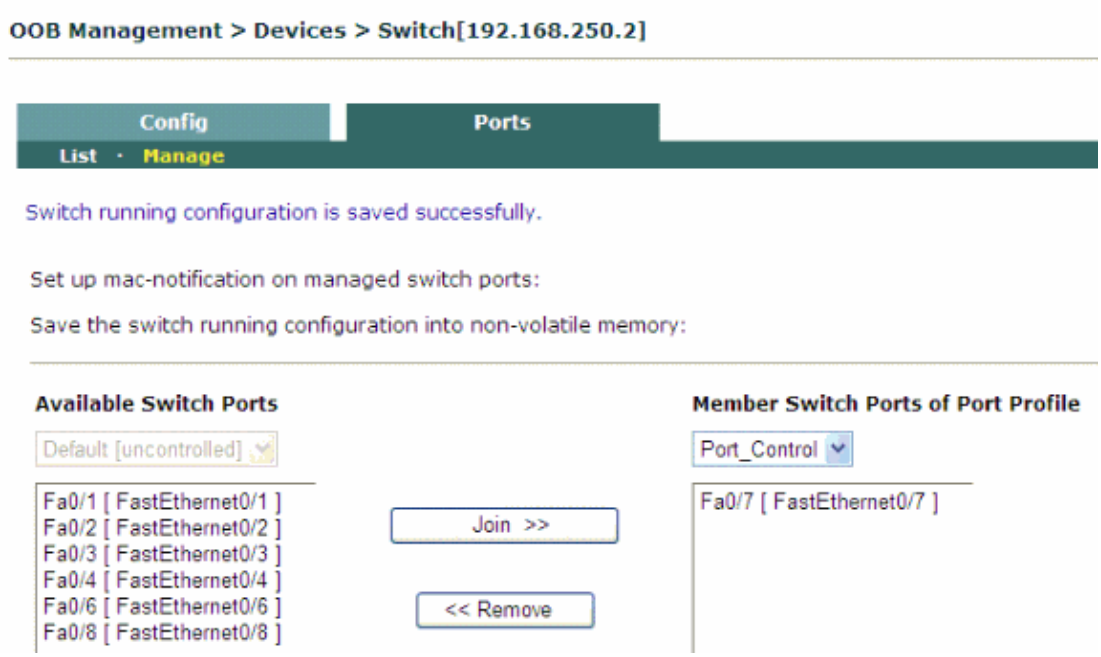
a. Select **OOB Management > Devices Switch[IP address] > Ports > List** to see the available switch ports you can manage (see Figure 20).

Figure 20: Port Control Selection Available for a Managed Switch



b. Select **OOB Management > Devices Switch[IP address] > Ports > Manage** to manage several ports at once (see Figure 21).

Figure 21: Managing Multiple Ports with Join Option

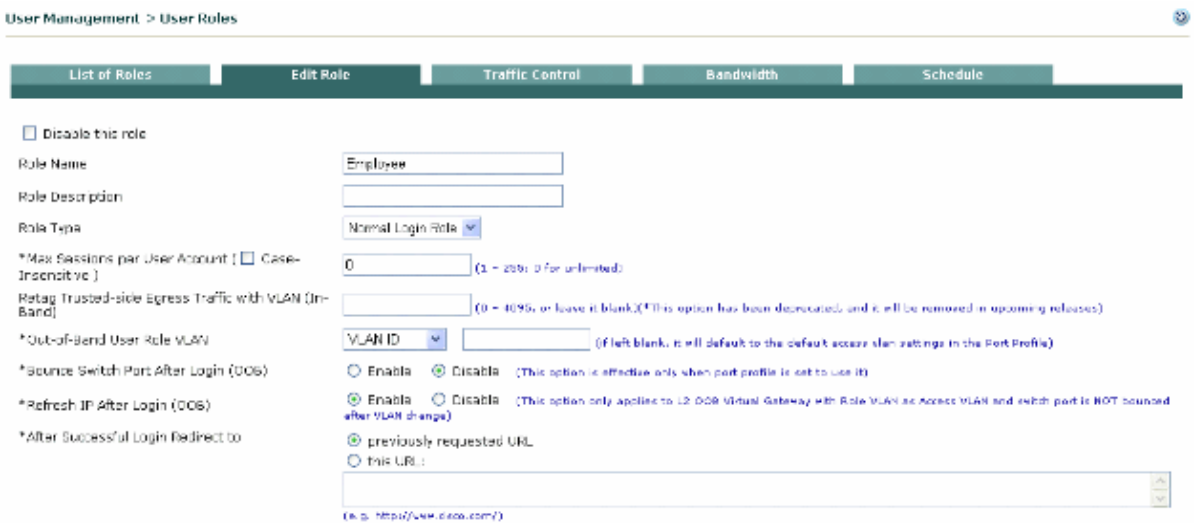


14. Configure user roles.

    In this example, three additional roles are created. The VLANs already created in the edge which each correspond to a role.

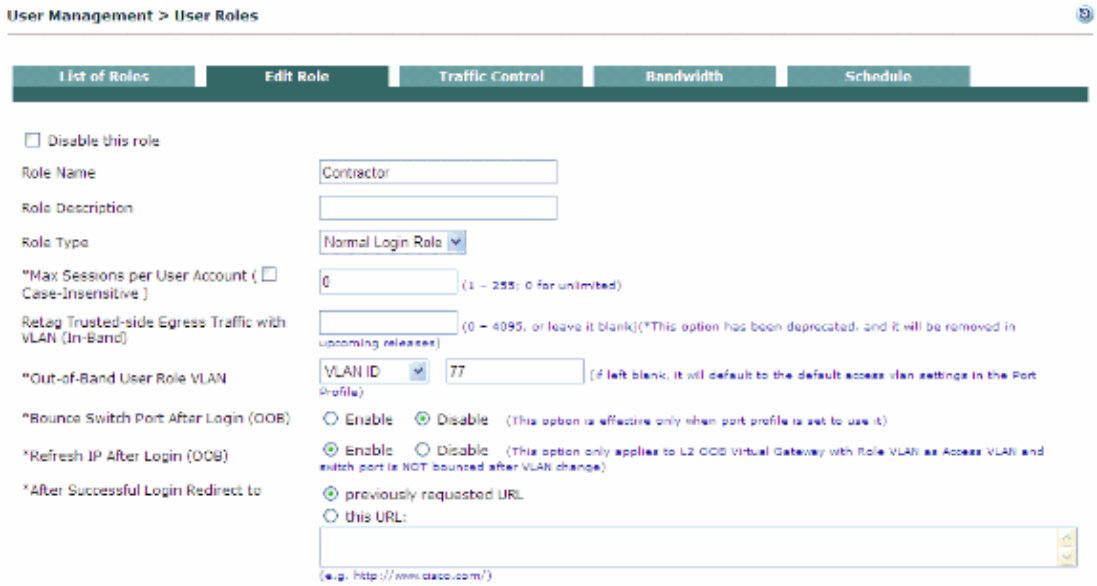
    a. Select **User Management > User Roles > Edit Role** and create an employee role using Figure 22 as a guide.

    Figure 22: Creating Employee Role and Mapping to the production VLAN 14



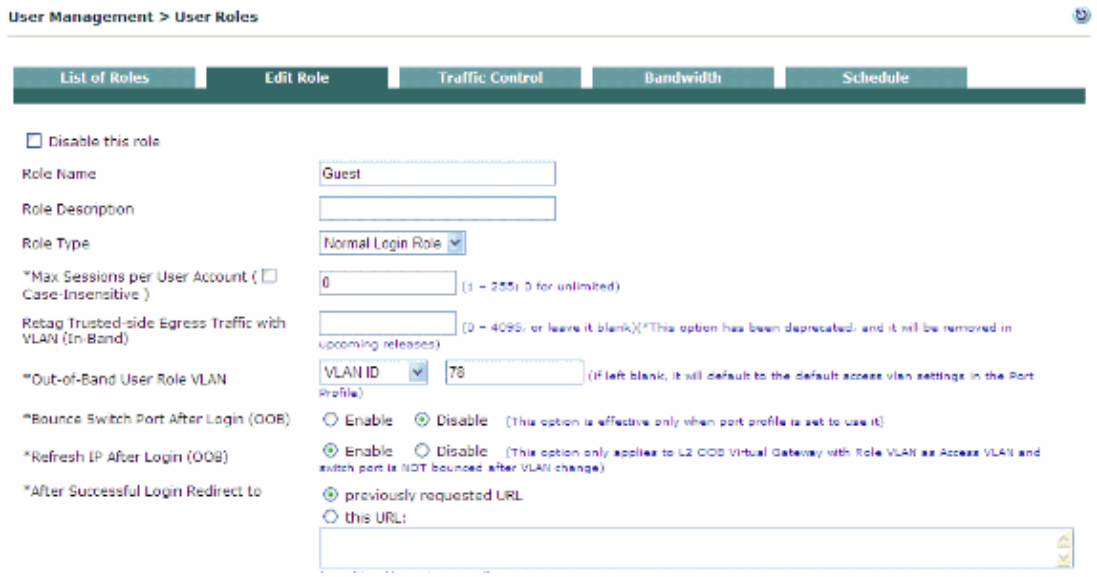
    b. Select **User Management > User Roles > Edit Role** and create a contractor role using Figure 23 as a guide.

    Figure 23: Creating Contractor Role and Mapping it to the Limited Access VLAN 77



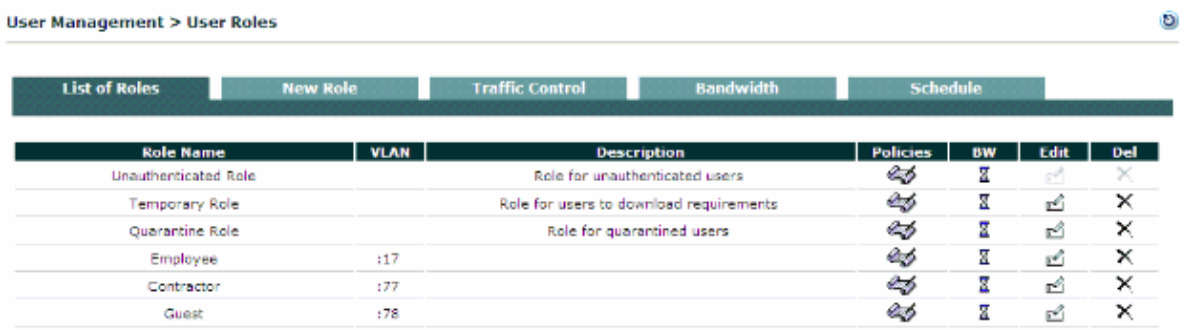
c. Select **User Management > User Roles > Edit Role** and create a guest role using Figure 24 as a guide.

Figure 24: Creating Guest Role and Mapping it to the Internet Only VLAN



In total, you should see six roles created in this section (three default roles and three new roles), as shown in Figure 25.

Figure 25: Adding Roles in the NAC Manager



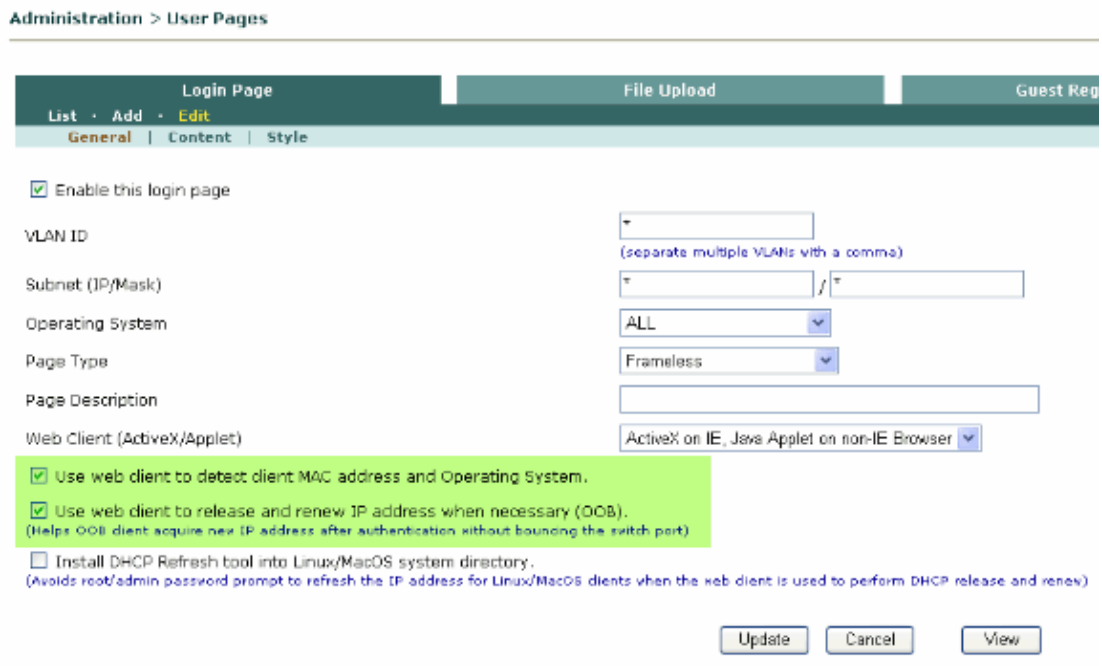
15. Add users and assign to appropriate user role.

    In a campus environment, you will integrate with an external authentication server and map the user to a particular role by means of the LDAP attribute. This example uses a local user and associates that local user with a role.
16. Customize user login page for web login.

    A default login page is already created in Cisco NAC Manager. You can optionally customize the login page to change the appearance of the web portal. For a NAC Layer 3 OOB solution, the ActiveX or Java component must be downloaded to the end client to perform the following tasks:

    a. Fetch the MAC address of the client machine.
    b. Perform IP address release and renew.
    c. Select **Administration > User Pages** (see Figure 26).
    d. Edit the page to make enable the options shown in Figure 26.

    Figure 26: User Page Settings for Web Login

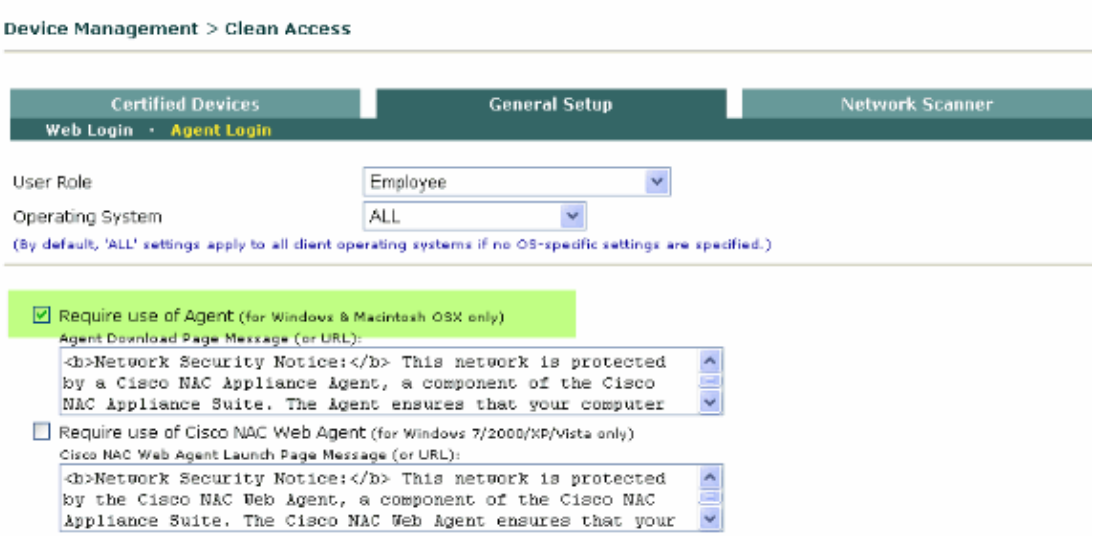


17. Customize the Cisco NAC Agent for the user roles.

    a. Select **Device Management > Clean Access > General Setup > Agent Login** (see Figure 27).

       The Cisco NAC Manager can be configured to make the Agent mandatory for any user role. In this example, the Agent is mandatory for the employee role. The contractor and guest roles must use web login.
    b. Check the **Require use of Agent** checkbox.

    Figure 27: Agent Login Required for Employee Role

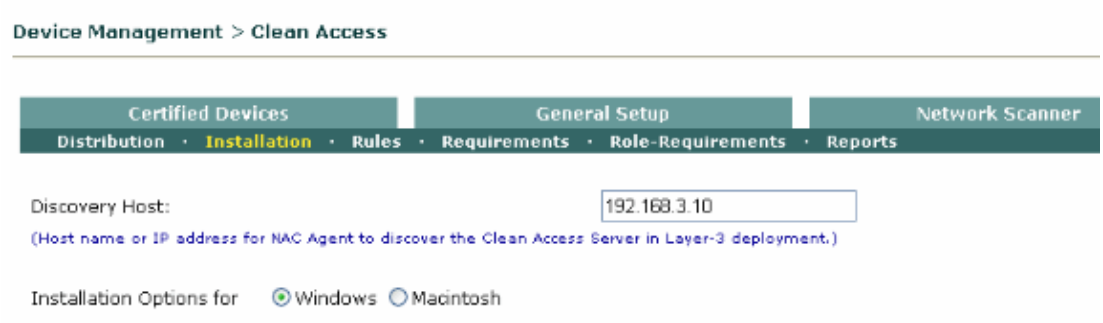


18. Distribute Discovery Host for Cisco NAC Agent.

    The Cisco NAC Agent software distribution, installation, and configuration are covered in the Appendix in the Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment section. This example configures the discovery host on the Cisco NAC Manager.

    Select **Device Management > Clean Access > Clean Access Agent > Installation** (see Figure 28).

    Figure 28: Discovery Host for Cisco NAC Agent



    The Discovery Host field is pre−populated as shown in Figure 28 if the Cisco NAC Agent is downloaded from the Cisco NAC Server.

19. Web login.

    a. Connect the client machine using one of the edge ports controlled by the Cisco NAC Manager.

       The client machine is placed in the unauthenticated VLAN. The machine should get an IP address from the unauthenticated VLAN subnet.

    b. Open the browser to perform login.

       The assumption is that this client machine does not have a Cisco NAC Agent already installed. If all of the DNS entries are being redirected to the untrusted interface of the Cisco NAC Server, the browser should be redirected to a login page automatically. Otherwise, go to a specific URL (for example, guest.nac.local) to perform login (Figure 29).

       Figure 29: Web Login Page

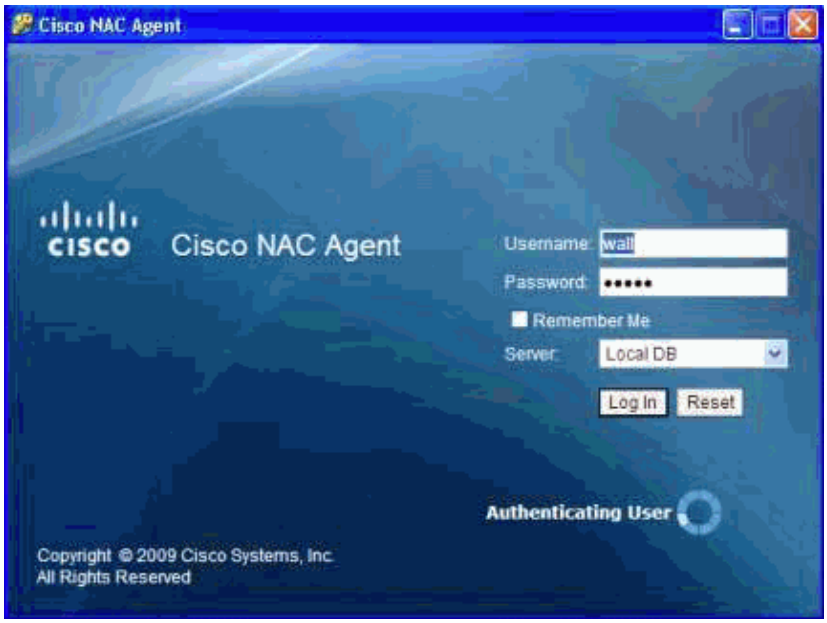
20. Agent login.

    The Cisco NAC Agent can be distributed just like any other software application to end users or it can be forced using the Cisco NAC Server.

    Note: More detailed information on Agent distribution and installation is available in the *Cisco NAC Appliance − Clean Access Manager Configuration Guide*.

    When the agent is activated, the screen shown in Figure 30 appears.

    Figure 30: Agent Login



    a. Select the server from the **Server** dropdown list.
    b. Enter the **Username**.
    c. Enter the **Password**.
    d. Click **Log In**.

    The screen in Figure 31 appears, followed shortly by Figure 32.

    Figure 31: Cisco NAC Agent Performing IP Release and Renew

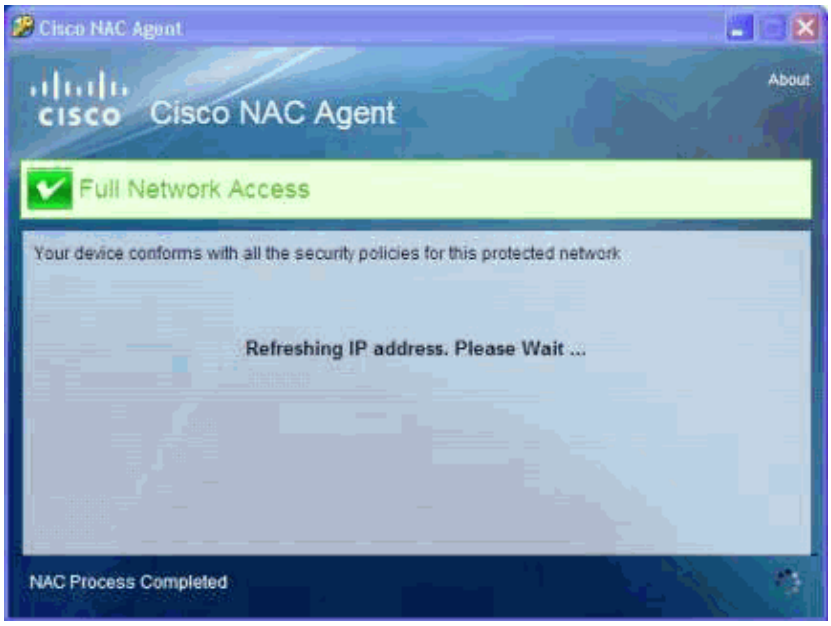
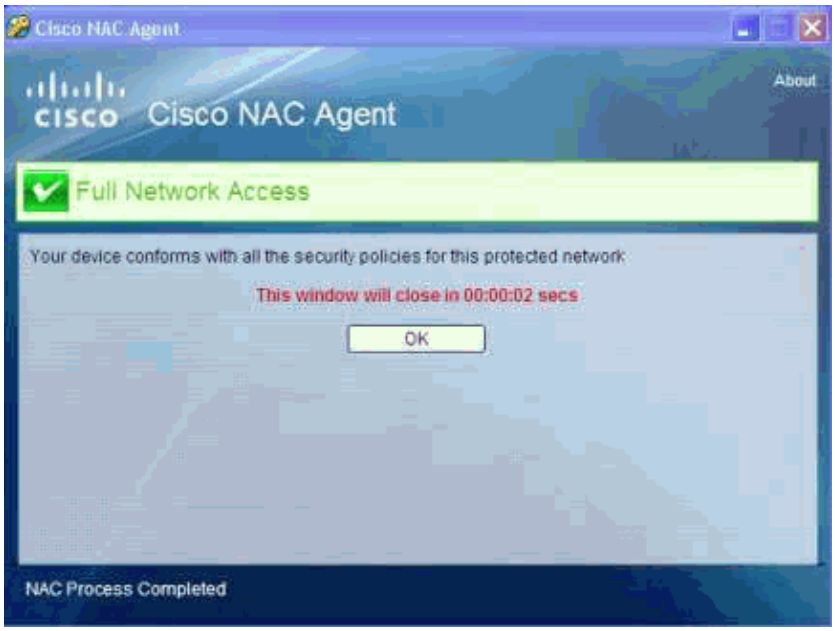


Figure 32: Cisco NAC Agent Indicating Full Network Access After IP Refresh



e. Click **OK**.

Verify VLAN Assignment

The managed port for this example is 0/7. After you successfully complete the login process, the VLAN is changed from the unauthenticated VLAN 14 to employee VLAN 17. You can confirm which port is running the configuration by issuing the following command:

```
3560-remote#show run interface fast 0/7
Building configuration&

Current configuration : 153 bytes
!
interface FastEthernet0/7
 switchport access VLAN 14
 switchport mode access
 snmp trap mac-notification change added
```

```
 spanning-tree portfast
end
```

NAC Layer 3 OOB ACL Solution for Wireless

The existing NAC OOB wireless solution currently is limited to a Layer 2 OOB solution with Cisco NAC Server in virtual gateway mode. The limitation of that solution is that the wireless LAN controller (WLC) must be Layer 2 adjacent with the Cisco NAC Server. For more information about Layer 2 OOB wireless deployment, go to:

http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml

Note: Currently, Cisco is working on a NAC Layer 3 OOB ACL solution for wireless deployments.

Appendix

High Availability

Each of the individual Cisco NAC Managers and Cisco NAC Servers in the solution can be configured in high availability mode, meaning that there are two appliances that act in an active−standby configuration.

NAC Manager

Cisco NAC Manager can be configured in high availability mode where there are two NAC Managers that act in an active−standby configuration. The entire configuration on a Manager is stored in a database. The standby Manager synchronizes its database with the database on the active Manager. Any configuration changes made to the active Manager are immediately pushed to the standby Manager. The following key points provide a high−level summary of high availability Manager operation:

- The Cisco NAC Manager high availability mode is an active or passive two−server configuration in which a standby Manager acts as a backup to an active Manager.
- The active Cisco NAC Manager performs all tasks for the system. The standby Manager monitors the active Manager and keeps its database synchronized with the active Manager s database.
- Both Cisco NAC Managers share a virtual service IP for the Eth0 trusted interface. The service IP should be used for the SSL certificate.
- The primary and secondary Cisco NAC Managers exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.
- To ensure an active Cisco NAC Manager is always available, its trusted interface (Eth0) must be up. The situation must be avoided where a Manager is active but is not accessible through its trusted interface. This condition occurs if the standby Manager receives heartbeat packets from the active Manager, but the active Manager s Eth0 interface fails). The link−detect mechanism allows the standby Manager to know when the active Manager s Eth0 interface becomes unavailable.
- You can choose to automatically configure the Eth1 interface in the Administration > CCA Manager > Failover page. However, you must manually configure other (Eth2 or Eth3) high availability interfaces with an IP address and netmask before you configure high availability on the Cisco NAC Manager.
- The Eth0, Eth1, and Eth2/Eth3 interfaces can be used for heartbeat packets and database synchronization. In addition, any available serial (COM) interface can also be used for heartbeat packets. If you are using more than one of these interfaces, failover occurs only if all the heartbeat interfaces fail.

Note: The Cisco NAC Manager high availability pair cannot be separated by a Layer 3 link.

For more details, refer to the Cisco NAC Manager documentation at:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_ha.html

Cisco NAC Server

To provide protection against a single point of failure, the Cisco NAC Server can be configured in high availability mode. The high availability mode for the Cisco NAC Server is similar to that of the Cisco NAC Manager and also uses an active−standby configuration. The Cisco NAC Servers still share a virtual IP address (called a Service IP), but they do not share virtual MAC addresses.

The following key points provide a high−level overview of high availability Cisco NAC Server operation:

- The Cisco NAC Server high availability mode is an active−passive two−server configuration in which a standby Cisco NAC Server machine acts as a backup to an active Cisco NAC Server.
- The active Cisco NAC Server performs all tasks for the system. Because most of the Server configuration is stored on the Cisco NAC Manager, when Server failover occurs, the Manager pushes the configuration to the newly−active Server.
- The standby Cisco NAC Server does not forward any packets between its interfaces.
- The standby Cisco NAC Server monitors the health of the active Server through a heartbeat interface (serial and one or more UDP interfaces). Heartbeat packets can be sent on the serial interface, dedicated Eth2 interface, dedicated Eth3 interface, or Eth0/Eth1 interface (if no Eth2 or Eth3 interface is available).
- The primary and secondary Cisco NAC Servers exchange UDP heartbeat packets every two seconds. If the heartbeat timer expires, stateful failover occurs.
- In addition to heartbeat−based failover, the Cisco NAC Server also provides link−based failover based on Eth0 or Eth1 link failure. The Server sends ICMP ping packets to an external IP address through the Eth0 and/or Eth1 interface. Failover occurs only if one Cisco NAC Server can ping the external addresses.

For more details, refer to the Cisco NAC Server documentation at:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_ha.html

Active Directory SingleSignOn (Active Directory SSO)

Windows active directory SSO is the ability for a Cisco NAC appliance to automatically log in users already authenticated to a backend Kerberos Domain Controller (Active Directory server). This ability eliminates the need to log into the Cisco NAC Server after you are already logged into the domain. For more details about configuring the active directory SSO on a Cisco NAC Appliance, go to:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_adsso.html

Windows Domain Environment Considerations

In preparation for a NAC deployment, changes to the login script policy may be required. Windows login scripts can be classified as startup or shutdown and logon or logoff scripts. Windows runs startup and shutdown scripts in a machine context. Running the scripts only functions if the Cisco NAC appliance opens the appropriate network resources required by the script for the particular role when these scripts are executed at PC boot up or shutdown, which is typically the unauthenticated role. Logon and logoff scripts are executed in a user context, which means the logon script executes after the user has logged in through Windows GINA. The logon script can fail to execute if the authentication or client machine posture assessment does not complete and network access is not granted in time. These scripts can also be interrupted

by IP address refresh initiated by the Cisco NAC Agent after an OOB logon event. For more information regarding necessary changes to the login scripts, go to:

http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a70c18.shtml

Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment

The Cisco NAC Agent and Cisco NAC Web Agent provide local posture assessment and remediation for client machines. Users download and install the Cisco NAC Agent or Cisco NAC Web Agent (read−only client software), which can check the host registry, processes, applications, and services. For more details about the agent and posture assessment and remediation, go to:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Nov 11, 2010 Document ID: 112168