CANAC

Implementing Cisco NAC Appliance

Volume 1

Version 2.1

Student 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.

Students, this letter describes important course evaluation access information!

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco Systems is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions; therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. We would appreciate a few minutes of your time to complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL directing you to a short post-course evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,

Cisco Systems Learning

Table of Contents

Volume 1

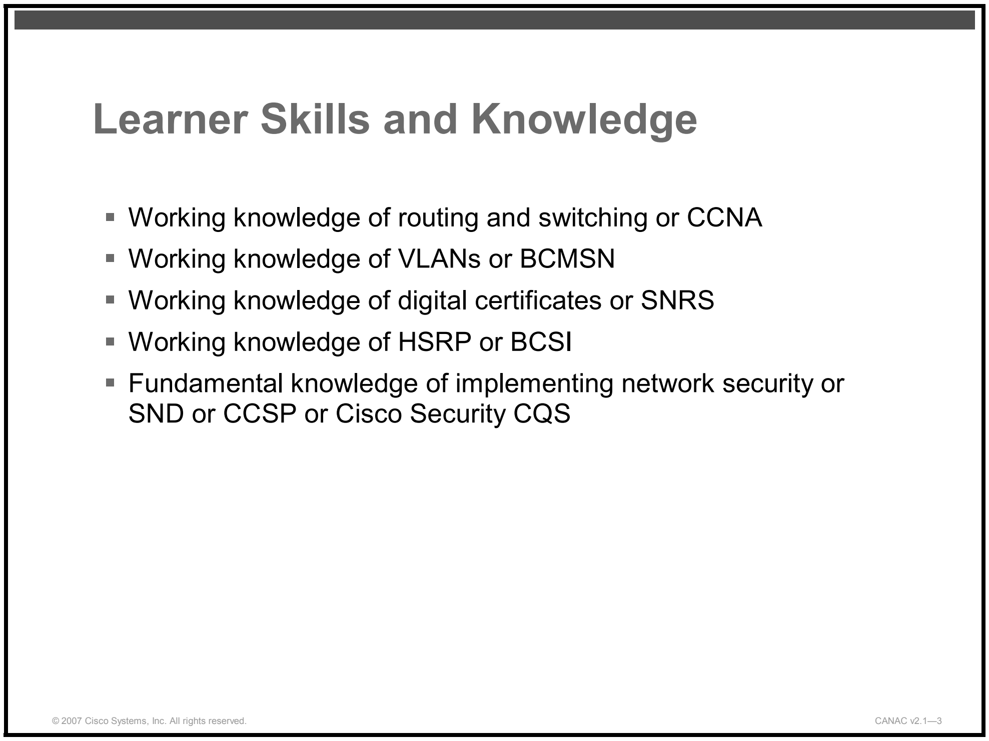
Course Introduction

Overview

The Cisco Self-Defending Network (SDN) strategy addresses the need for Network Admission Control (NAC). The Cisco NAC Appliance is an easily deployed software NAC solution that can automatically detect, isolate, and clean infected or vulnerable devices that attempt to access your network. The *Implementing Cisco NAC Appliance (CANAC) v2.1* course will provide learners with the skills and knowledge to be able to implement the Cisco NAC Appliance solution as a part of a Cisco SDN security strategy.

Learner Skills and Knowledge

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.



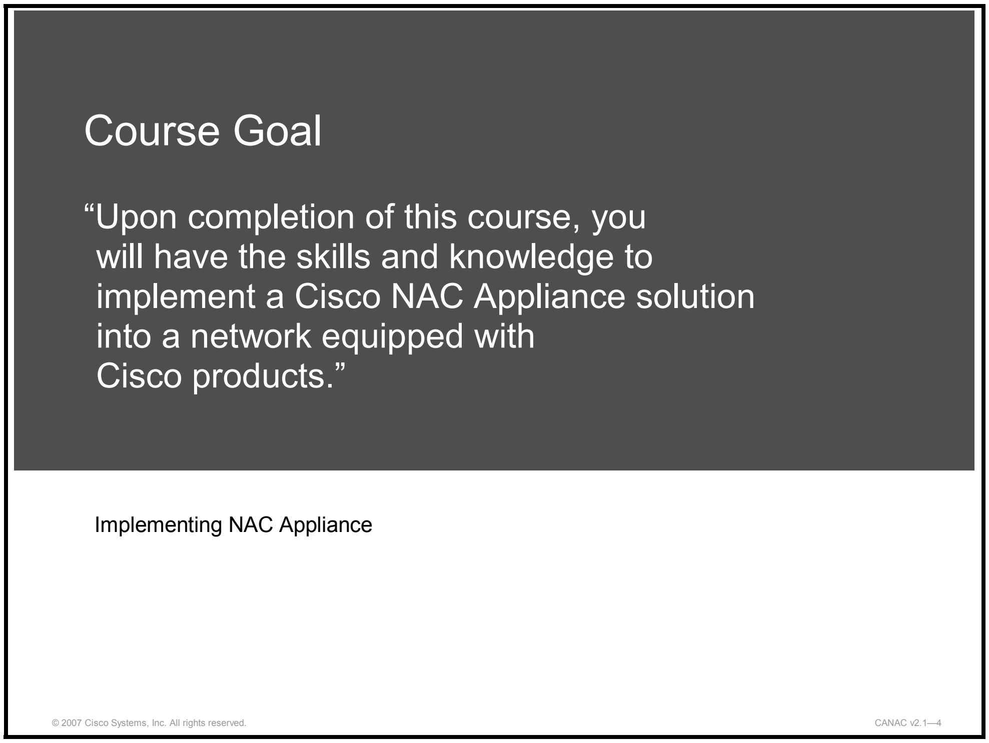
Learner Skills and Knowledge

- Working knowledge of routing and switching or CCNA
- Working knowledge of VLANs or BCMSN
- Working knowledge of digital certificates or SNRS
- Working knowledge of HSRP or BCSI
- Fundamental knowledge of implementing network security or SND or CCSP or Cisco Security CQS

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

Course Goal and Objectives

This topic describes the course goal and objectives.



Course Goal

"Upon completion of this course, you will have the skills and knowledge to implement a Cisco NAC Appliance solution into a network equipped with Cisco products."

Implementing NAC Appliance

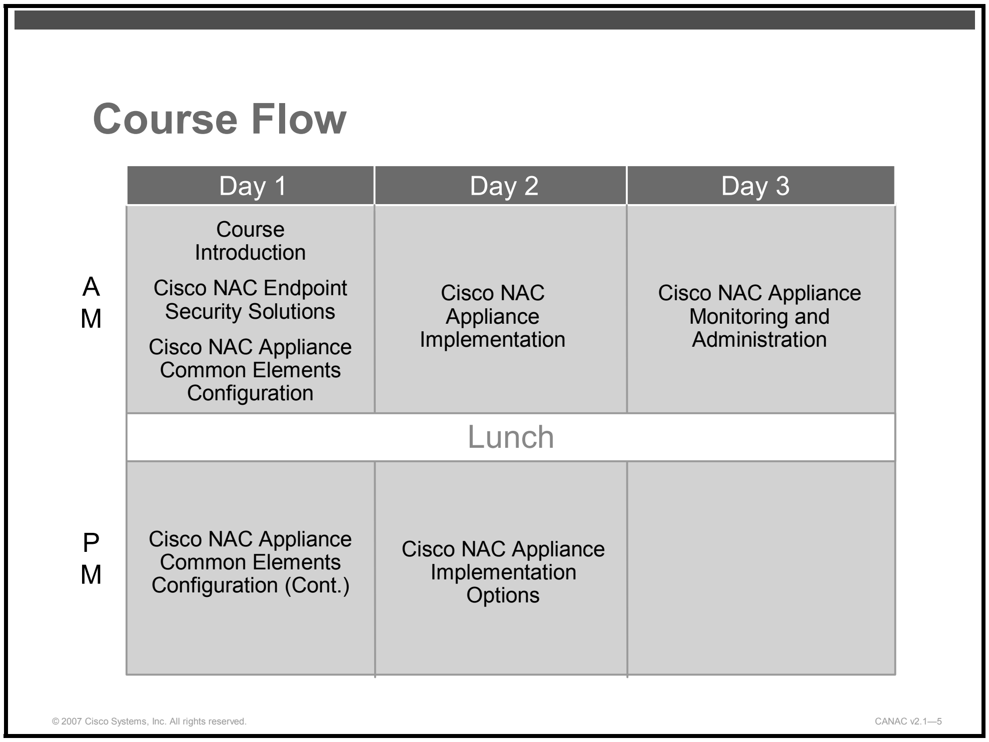
CANAC v2.1—4

Upon completing this course, you will be able to meet these objectives:

- Given network security requirements, select the appropriate NAC endpoint security deployment scenario that will meet or exceed network security requirements
- Configure the elements of a NAC Appliance solution
- Configure the NAC Appliance in-band and out-of-band implementation options
- Implement a highly available NAC Appliance solution to mitigate network threats and facilitate network access for those users that meet corporate security requirements
- Maintain a highly available NAC Appliance deployment in medium-sized and enterprise-sized network environments

Course Flow

This topic presents the suggested flow of the course materials.



Course Flow

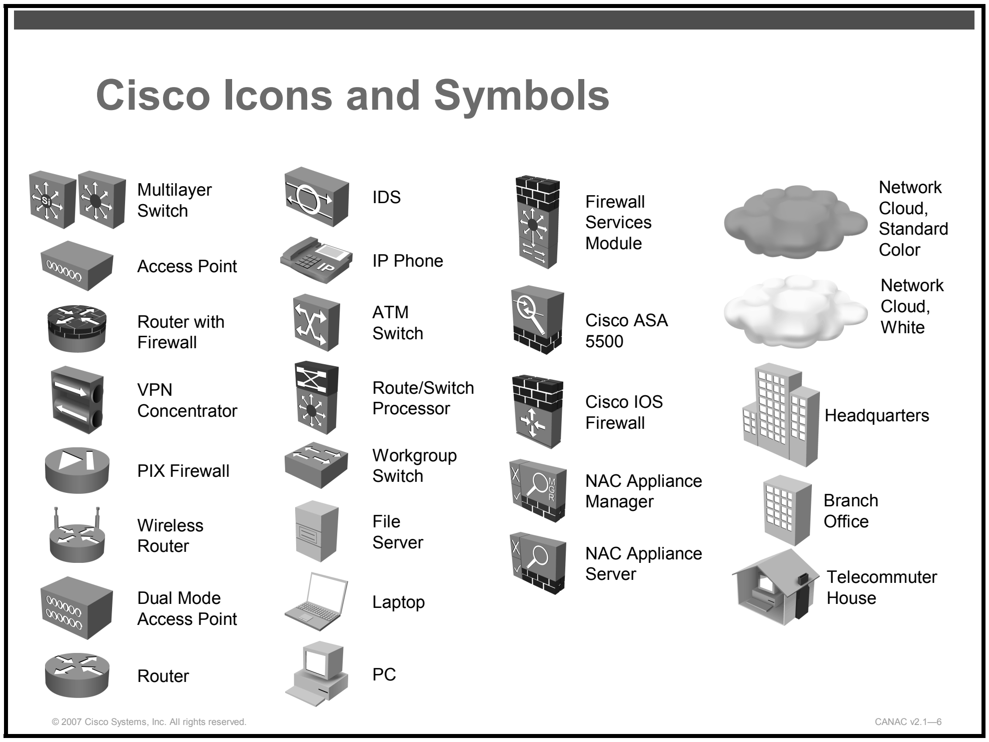
	Day 1	Day 2	Day 3
AM	Course Introduction Cisco NAC Endpoint Security Solutions Cisco NAC Appliance Common Elements Configuration	Cisco NAC Appliance Implementation	Cisco NAC Appliance Monitoring and Administration
	Lunch		
PM	Cisco NAC Appliance Common Elements Configuration (Cont.)	Cisco NAC Appliance Implementation Options	

CANAC v2.1—5

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Additional References

This topic presents the Cisco icons and symbols that are used in this course, as well as information on where to find additional technical references.



Cisco Icons and Symbols

Multilayer Switch

Access Point

Router with Firewall

VPN Concentrator

PIX Firewall

Wireless Router

Dual Mode Access Point

Router

IDS

IP Phone

ATM Switch

Route/Switch Processor

Workgroup Switch

File Server

Laptop

PC

Firewall Services Module

Cisco ASA 5500

Cisco IOS Firewall

NAC Appliance Manager

NAC Appliance Server

Network Cloud, Standard Color

Network Cloud, White

Headquarters

Branch Office

Telecommuter House

CANAC v2.1—6

Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm.

Module 1

Cisco NAC Endpoint Security Solutions

Overview

Cisco developed the Network Admission Control (NAC) Appliance solution as a NAC appliance to be an integral part of the standards-based NAC framework. Using NAC, organizations can identify noncompliant devices and then deny them access, place them in a quarantined area, or give them restricted access to computing resources. This module provides the knowledge and skills that are required to deploy a Cisco NAC Appliance solution to enforce security policy compliance on all devices that are seeking to access network resources. This module focuses on Cisco NAC Appliance features and the deployment options that are available to protect your network from specified threats.

Module Objectives

Upon completing this module, you will be able to select the appropriate Cisco NAC endpoint security deployment scenario that will meet or exceed network security requirements. This ability includes being able to meet these objectives:

- Describe how the Cisco Self-Defending Network strategy can meet network security requirements
- Describe the Cisco NAC Appliance solution
- Describe how Cisco NAC Appliance can be deployed to protect against specified threats

Lesson 1

Introducing Cisco Self-Defending Networks

Overview

Preserving the integrity, confidentiality, and longevity of corporate information is critical to successful companies, especially in the current era of regulatory activity. The information technology infrastructure of a company must consist of systems that can detect and protect against unauthorized access while providing timely access to legitimate users. This lesson describes the approaches that Cisco Systems has adopted to deliver these capabilities based on the rationale and foundation of the Cisco Self-Defending Network (SDN). The Cisco Network Admission Control (NAC) framework and the Cisco NAC Appliance solution are described in relation to the Cisco SDN.

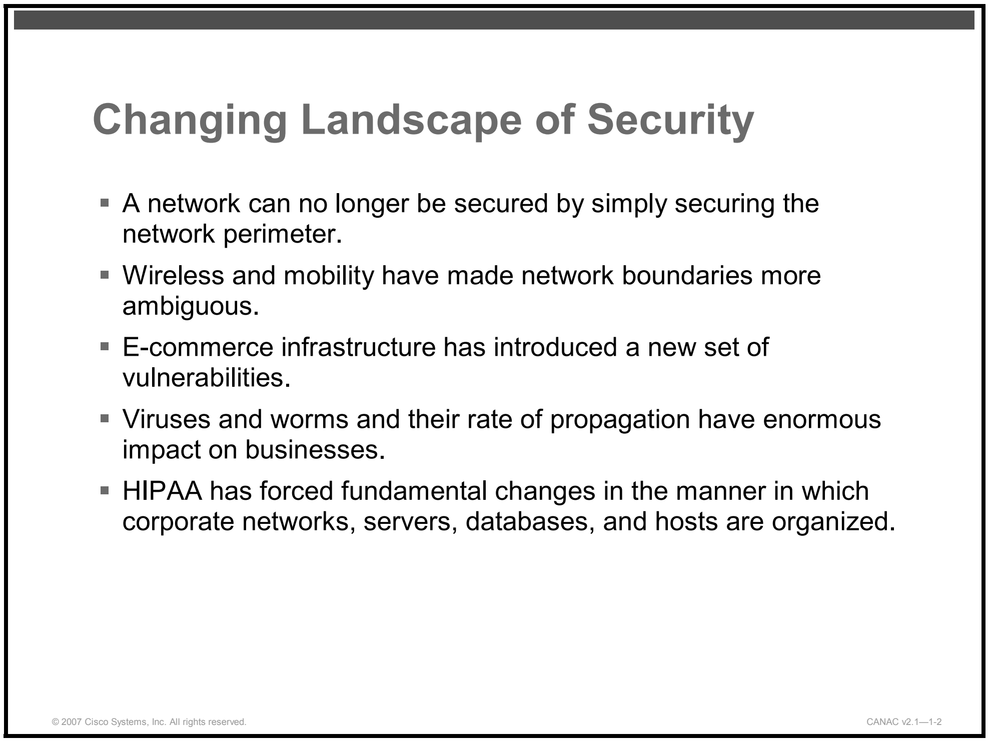
Objectives

Upon completing this lesson, you will be able to describe how the Cisco SDN strategy can meet network security requirements. This ability includes being able to meet these objectives:

- Describe the key factors that are causing changes to network security
- Describe the role of each of the three components of the Cisco host-protection strategy
- Describe the Cisco SDN strategy
- Describe Cisco NAC products

Changing Landscape of Security

This topic describes the key factors that are causing changes to network security.



Changing Landscape of Security

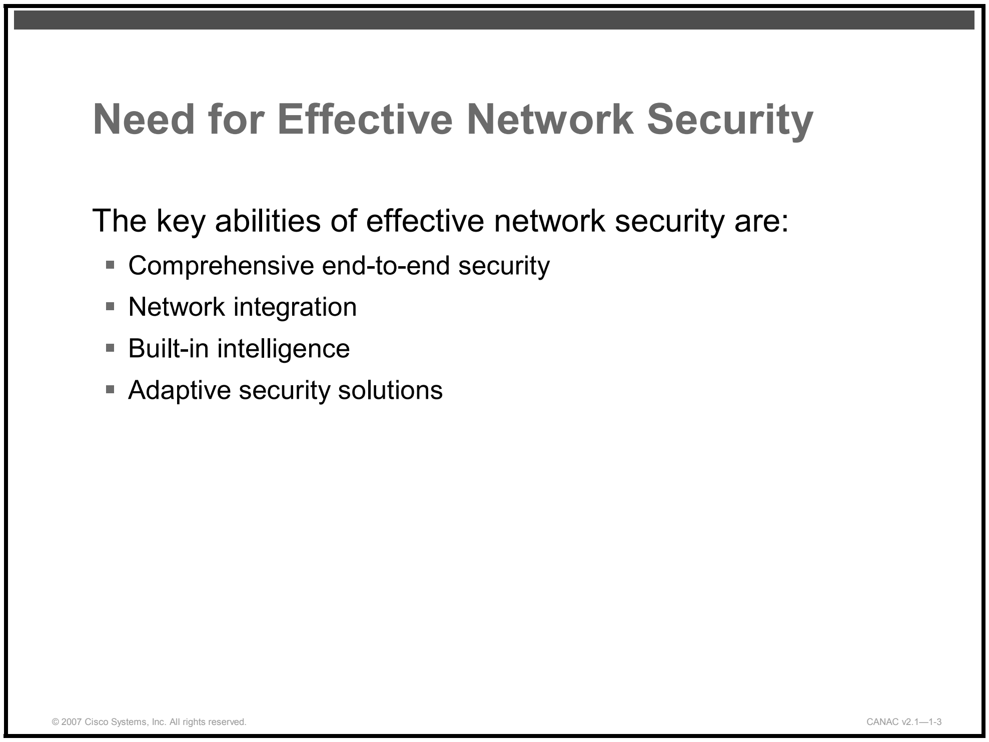
- A network can no longer be secured by simply securing the network perimeter.
- Wireless and mobility have made network boundaries more ambiguous.
- E-commerce infrastructure has introduced a new set of vulnerabilities.
- Viruses and worms and their rate of propagation have enormous impact on businesses.
- HIPAA has forced fundamental changes in the manner in which corporate networks, servers, databases, and hosts are organized.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—1-2

Security technology is changing at an increasing rate. The extent of the changes and the rate of change have made it difficult for IT departments to stay current with security technology developments. This changing landscape is the result of these key factors in network security:

- **The secure network perimeter:** A network can no longer be secured by simply securing the network perimeter. As corporations have embraced the Internet, the network environment is now typically open to partners through business-to-business extranets, retail outlet connections, and home-based employees. Extending the corporate network in this way extends the trust boundary across untrusted intermediate networks and into uncontrolled environments. Devices that connect to the corporate network through these pathways frequently do not comply with corporate policies. Devices that are compliant with corporate policies are frequently used to access other uncontrolled networks prior to connecting to the corporate network. As a result of such use, devices on these external networks can become conduits for attacks and related misuse.
- **Wireless and mobile networks:** The wireless and mobile networks within enterprises now support laptop PCs, personal digital assistants, and mobile phones that have more than one network connection. These multihomed hosts are capable of establishing informal wireless networks to enable peer-to-peer communication. Information packets can effectively be forwarded across devices at the application level. As a result, the network boundary becomes less clearly defined. Corporations must be able to extend a control point to these mobile devices in order to manage a secure system and maintain network availability.

- **E-commerce, extranets, and web-based business:** The emergence of common application interfaces based on messaging protocols (such as Extensible Markup Language [XML] and Simple Object Access Protocol [SOAP]) has been good for e-commerce and corporate productivity. However, these new messaging protocols have introduced a new set of vulnerabilities and attack vectors that corporations must now cope with. Data that was once spread across multiple network protocols and that could be filtered through firewall policies is now combined within a few, if not a single, transport protocol, such as HTTP on TCP port 80. As a result, much of the data that previously resided in packet headers now resides in the packet payload. These circumstances create significant processing challenges that make it easier for an attacker to evade traditional network defenses. To meet corporate data confidentiality and integrity requirements, an increased amount of application-level traffic is now encrypted through the Secure Sockets Layer (SSL), Transport Layer Security (TLS), and secure HTTP (HTTPS) protocols. It is now more difficult for IT departments to enforce corporate access policies at the network edge because security software cannot inspect the packet payloads of encrypted flows.
- **Viruses and worms and the rate of propagation:** An increasing number and types of viruses and worms have appeared in recent years. Two factors that impact businesses and their operational efficiency are the reduction in the time between when a vulnerability is detected and the time that an exploit appears, and the rate at which these attacks spread across a business network. These factors have led to unacceptable levels of business network failures and expensive remediation projects that consume staff, time, and extra funds.
- **Regulatory compliance:** Well-publicized breaches of security and internally generated corporate misconduct have forced regulatory bodies in many industries to create rules for corporate information risk management. In the United States, regulations such as the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act (HIPAA) have forced fundamental changes in the organization of corporate networks, servers, databases, and hosts.



Need for Effective Network Security

The key abilities of effective network security are:

- Comprehensive end-to-end security
- Network integration
- Built-in intelligence
- Adaptive security solutions

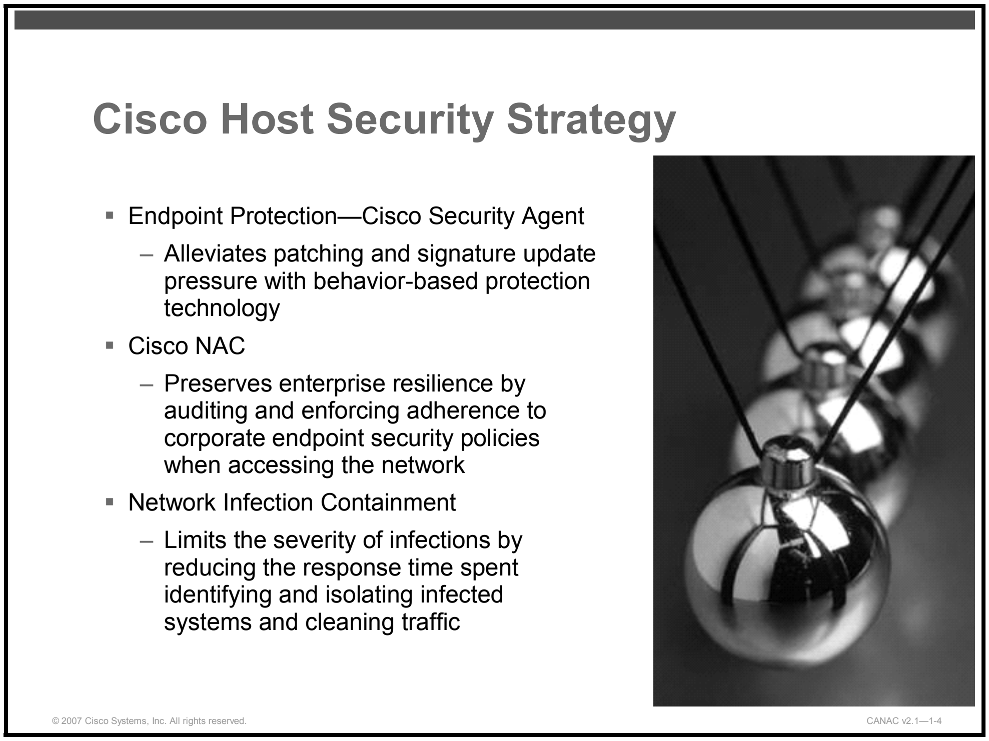
CANAC v2.1—1-3

Corporate network attacks are so complex that you cannot rely on a single mechanism to maintain security. Until recently, the concept of defending networks was based on proactive defense. Cisco believes in building adaptive solutions in addition to using a proactive defense. Network systems should include these qualities:

- **Comprehensive end-to-end security:** Network security must span the entire network end-to-end, regardless of device, location, or application.
- **Network integration:** A successful business requires a truly integrated and embedded network. As traffic passes through a networking device, the traffic must be scanned and analyzed, then either to be allowed to continue, to be partitioned, or to be rejected. Network integration requires that integrated security devices possess intelligence, performance, and scalability, and that the devices are embedded in the network at key locations in the network infrastructure. Key locations include the end-user workstation, remote branches, the campus, and the data center.
- **Built-in intelligence:** The network must be intelligent enough to be able to correlate the context and content of network traffic.
- **Adaptive security solutions:** Because security threats are always evolving, the solution itself must be adaptable to changes in security threats and requirements.

Cisco Host-Protection Strategy

This topic describes the role of each of the three components of the Cisco host-protection strategy.



Cisco Host Security Strategy

- Endpoint Protection—Cisco Security Agent
  - Alleviates patching and signature update pressure with behavior-based protection technology
- Cisco NAC
  - Preserves enterprise resilience by auditing and enforcing adherence to corporate endpoint security policies when accessing the network
- Network Infection Containment
  - Limits the severity of infections by reducing the response time spent identifying and isolating infected systems and cleaning traffic

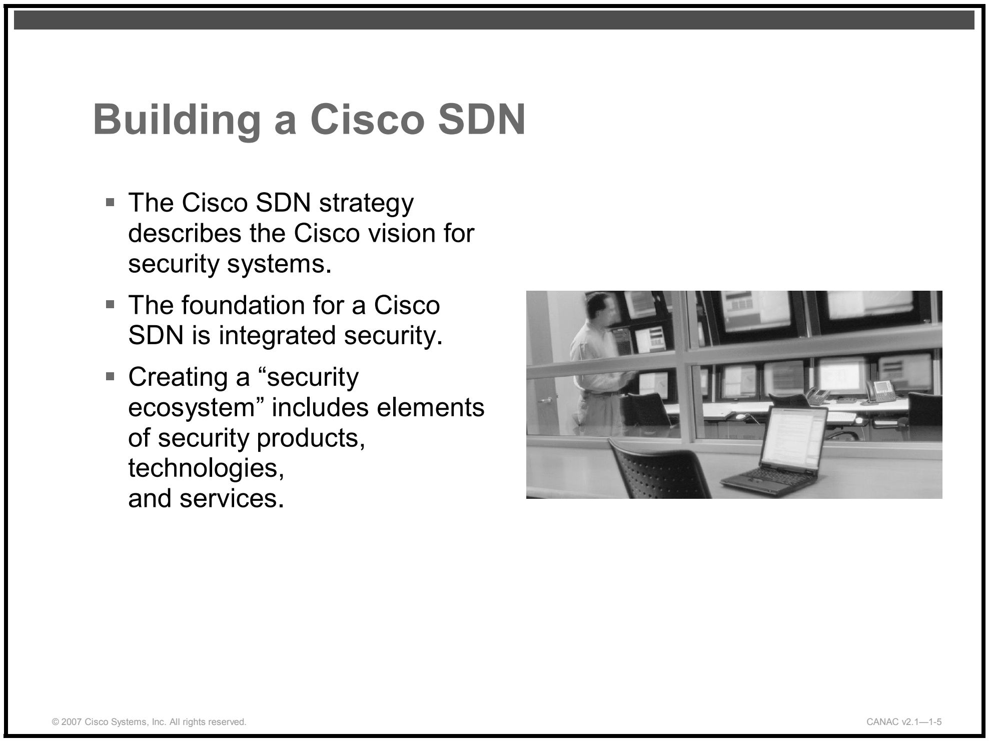
© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—1-4

The Cisco strategy for addressing host security, and therefore network and enterprise security, is based on three broad elements:

- **Endpoint protection:** New behavior-based technology is available with Cisco Security Agent. This technology protects hosts against the changing threats posed by viruses and worms.
- **Cisco NAC:** The Cisco NAC framework ensures that every endpoint complies with network security policies before being granted access. Cisco NAC provides network access to endpoint devices that fully comply with established security policy while ensuring that noncompliant devices are denied access, placed in quarantine for remediation, or given restricted access to resources.
- **Network infection containment:** To address the newest attack method that may penetrate your environment, network infection containment focuses on automating key elements of the infection response process.

The Cisco SDN Initiative

This topic describes the Cisco SDN strategy.



Building a Cisco SDN

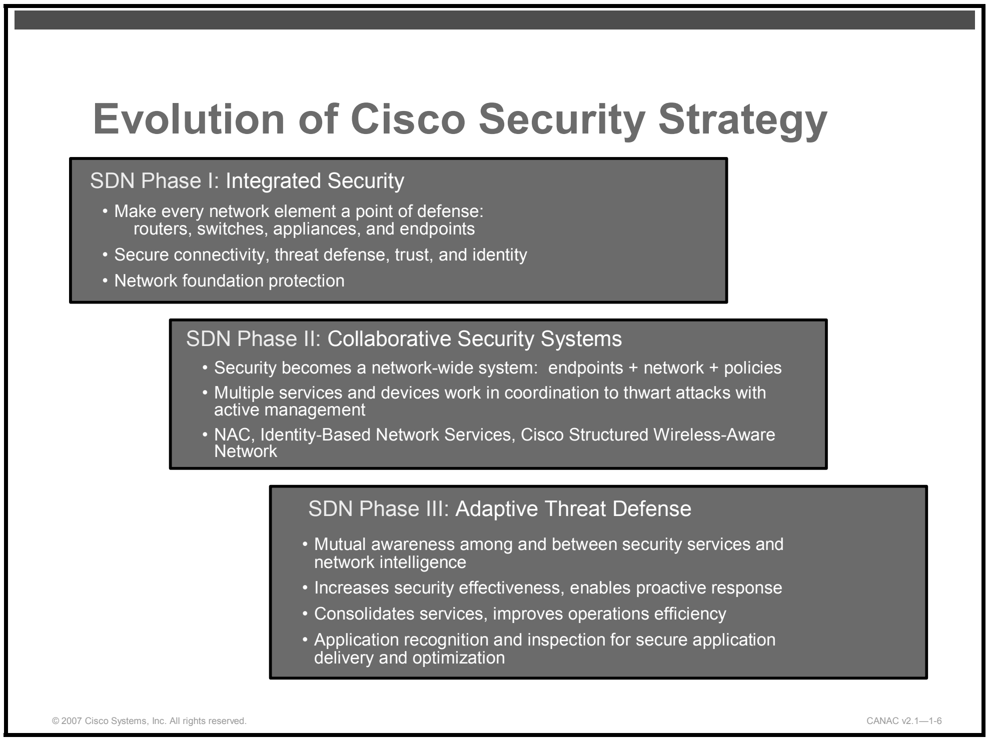
- The Cisco SDN strategy describes the Cisco vision for security systems.
- The foundation for a Cisco SDN is integrated security.
- Creating a "security ecosystem" includes elements of security products, technologies, and services.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—1-5

Networks have evolved from closed systems to open, sophisticated systems. As a result, security threats have grown exponentially, both at the network perimeter and from within the network. Cisco has responded with a strategy to integrate security services into the network infrastructure. The Cisco strategy provides a flexible, cost-effective, and comprehensive approach to securing an extended network. Building an SDN is part of this process and is characterized by three concepts:

- **Cisco vision for security systems:** The SDN strategy describes the Cisco vision for security systems. In the past, threats from both internal and external sources were slow-moving and easy to defend against. Now, Internet worms spread across the world in a matter of minutes; security systems and the network must react instantly.
- **Integrated security solutions:** The foundation for an SDN is integrated security. Security must be incorporated into all aspects of an organization. Every device in the network (desktops, the LAN, and the WAN) plays a part in securing the network environment through a globally distributed defense. The continued evolution of the Cisco integrated security vision involves incorporating capabilities from other security vendors. This form of SDN identifies threats, reacts appropriately to the severity level, isolates infected servers and desktops, and reconfigures network resources in response to an attack.
- **Cisco "security ecosystem":** The security products, technologies, and services in the Cisco portfolio are fundamental elements of a successful network security solution. A comprehensive approach to network security creates a "security ecosystem" that takes full advantage of the benefits delivered by the Cisco product line. This ecosystem includes several important elements, such as compatibility of third-party products, implementation services, customer support, and compatible service offerings. The Cisco Architecture for Voice, Video and Integrated Data (AVVID) Partner Program is a testing and comarketing program that validates the compatibility of complementary, third-party security solutions

with Cisco products. The program develops independent products into effective security solutions and offers a trusted and tested security implementation for Cisco customers.



Evolution of Cisco Security Strategy

SDN Phase I: Integrated Security

- Make every network element a point of defense: routers, switches, appliances, and endpoints
- Secure connectivity, threat defense, trust, and identity
- Network foundation protection

SDN Phase II: Collaborative Security Systems

- Security becomes a network-wide system: endpoints + network + policies
- Multiple services and devices work in coordination to thwart attacks with active management
- NAC, Identity-Based Network Services, Cisco Structured Wireless-Aware Network

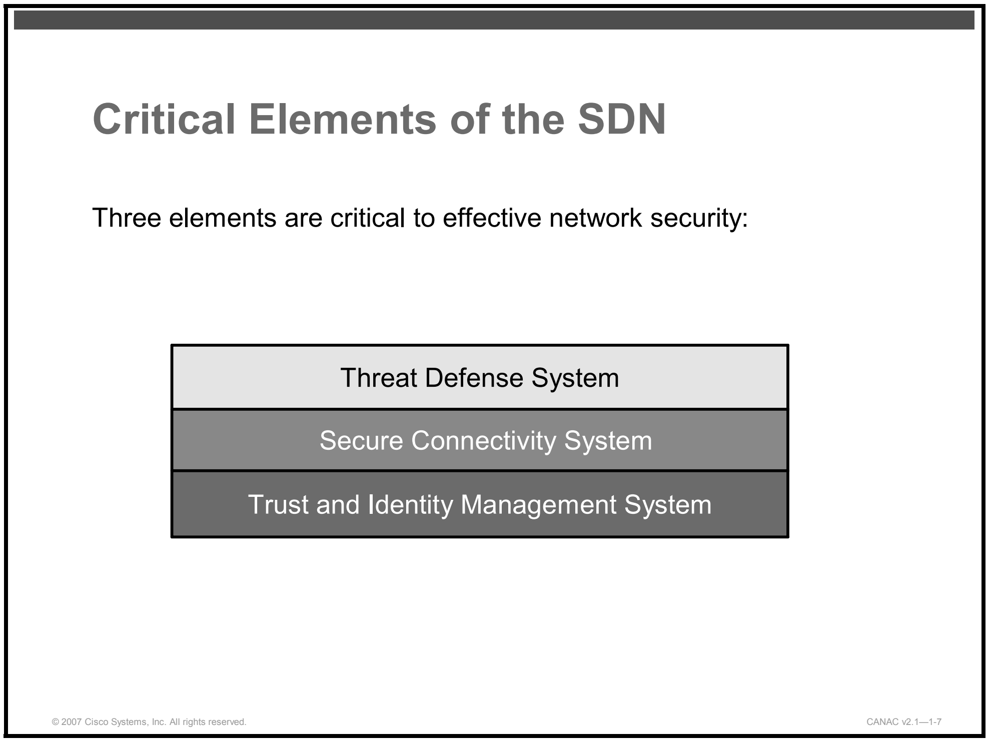
SDN Phase III: Adaptive Threat Defense

- Mutual awareness among and between security services and network intelligence
- Increases security effectiveness, enables proactive response
- Consolidates services, improves operations efficiency
- Application recognition and inspection for secure application delivery and optimization

CANAC v2.1—1-6

The Cisco SDN initiative continues to improve its ability to respond to new threats. The SDN has evolved in three phases:

- **Phase I—Integrated security:** Cisco SDN incorporates security in individual network elements such as switches and routers. Cisco initiated an integrated security model with the introduction of SDNs. The SDN integrates several protective layers of security such as virtual private networks (VPNs), firewalls, intrusion prevention, and anomaly mitigation that span the Internet class of the network.
- **Phase II—Collaborative security:** Cisco SDN builds links between multiple network security elements and extends the network presence to endpoints that connect to a network.
- **Phase III—Adaptive Threat Defense (ATD):** ATD capabilities enhance the ability of a network to respond to threats based on a new set of anti-X technologies. The Cisco ATD was designed with a very ambitious goal in mind: to provide protection for every packet and every flow that crosses the network. The model intelligently incorporates and integrates three crucial security components: application security, anti-X defenses, and network-wide containment and control.



Critical Elements of the SDN

Three elements are critical to effective network security:

Threat Defense System

Secure Connectivity System

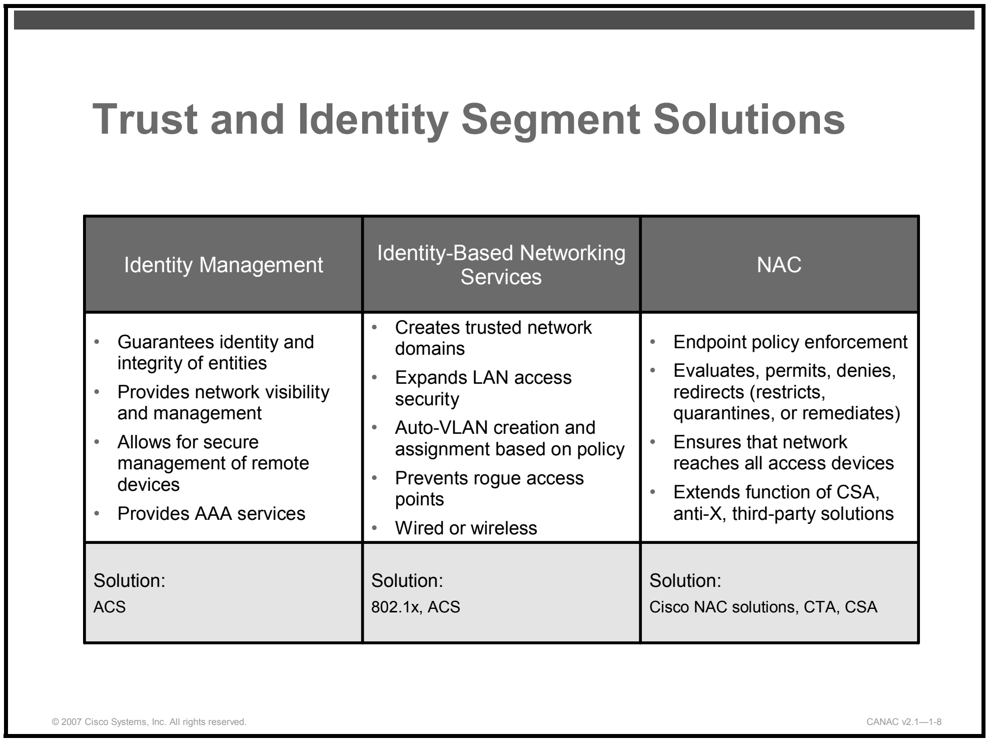
Trust and Identity Management System

CANAC v2.1—1-7

Cisco SDN solutions incorporate three elements that are critical to effective network security:

- **Cisco Threat Defense System (TDS):** Both known and unknown threats are increasingly more destructive and frequent than in the past. Internal and external threats have the ability to significantly affect business profitability. The Cisco TDS provides a strong defense against both known and unknown attacks. Appropriate security technologies and advanced networking intelligence are required to defend against attacks. To provide the highest effectiveness, defense system technologies must be implemented throughout the entire network rather than just in products or technologies, because an attack can start anywhere and instantly spread across all network resources. The Cisco TDS enhances security in the existing network infrastructure, adds comprehensive security to the endpoints, and adds dedicated security technologies to networking devices and appliances. This approach thereby proactively defends the business, applications, users, and network. The Cisco TDS includes these solutions:
  - Integrated firewall
  - Network intrusion protection
  - Endpoint security
  - Content security
  - Intelligent network and security services (embedded in routers and switches)
  - Management and monitoring

- **Cisco Secure Connectivity System:** When network connectivity increases, exposure also increases. Preserving the confidentiality and integrity of data and applications that cross the wired or wireless LAN is an important part of business transactions. The Cisco Secure Connectivity System uses encryption and authentication capabilities to provide secure transport across untrusted networks. To protect data, voice, and video applications over wired and wireless media and to ensure the privacy of all IP communications, Cisco offers IP Security (IPsec), Secure Sockets Layer (SSL), Secure Shell Protocol (SSH), and Multiprotocol Label Switching (MPLS) VPN technologies, in addition to extensive security capabilities that are incorporated into Cisco wireless and IP telephony solutions. Some of the solutions included in the Cisco Secure Connectivity System include the following:
  - Site-to-site VPNs
  - Remote access VPNs
  - Voice security
  - Wireless security
  - Solution management and monitoring
- **Cisco Trust and Identity Management Solutions:** The Cisco Trust and Identity Management System is critical for e-business and supports the creation of a secure network or system. The management system involves providing or denying access to business applications and network resources based on the specific privileges and rights of a user. The Cisco Trust and Identity Management System focuses on network-based admission control. After validating the identity of a user or device and compliance with corporate security policy, user access to certain resources or portions of the network is enabled. The network is responsible for identification, authorization, and security enforcement. The Cisco Trust and Identity Management System includes the Cisco Secure Access Control Server (ACS), authentication protocols such as 802.1x, and authentication, authorization, and accounting (AAA) capabilities in Cisco switches and routers. The Cisco Trust and Identity Management System is capable of providing a high level of detail about access rights, creating quarantine zones for noncompliant endpoints, and blocking unauthorized access entirely.



Trust and Identity Segment Solutions

Identity Management	Identity-Based Networking Services	NAC
• Guarantees identity and integrity of entities • Provides network visibility and management • Allows for secure management of remote devices • Provides AAA services	• Creates trusted network domains • Expands LAN access security • Auto-VLAN creation and assignment based on policy • Prevents rogue access points • Wired or wireless	• Endpoint policy enforcement • Evaluates, permits, denies, redirects (restricts, quarantines, or remediates) • Ensures that network reaches all access devices • Extends function of CSA, anti-X, third-party solutions
Solution: ACS	Solution: 802.1x, ACS	Solution: Cisco NAC solutions, CTA, CSA

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—1-8

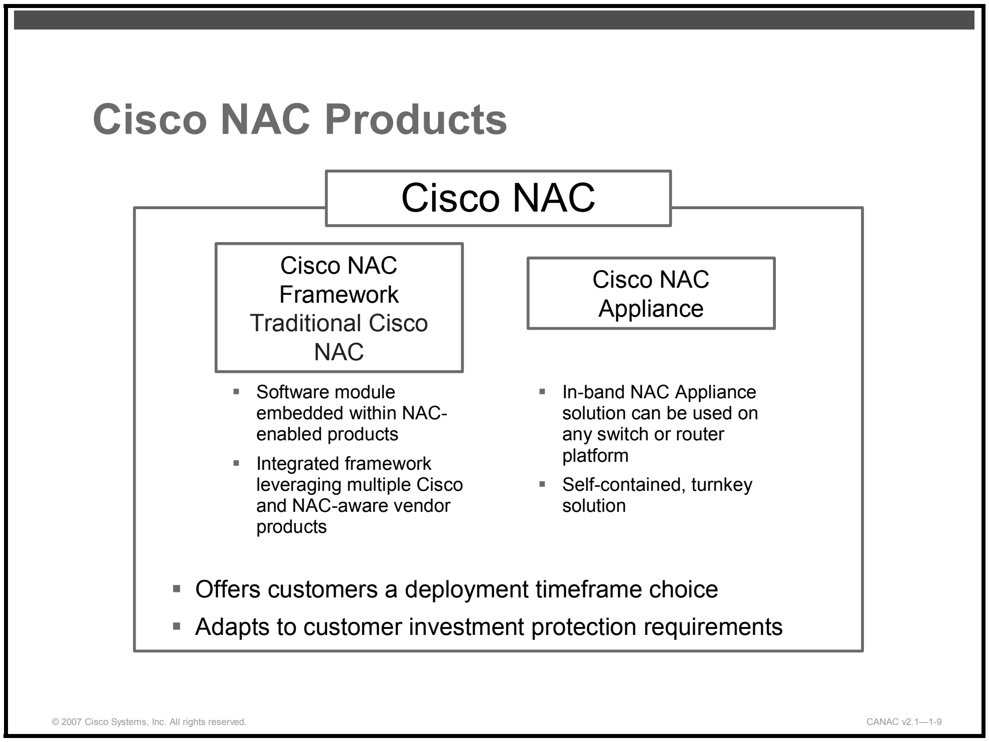
The Cisco Trust and Identity Management System technology consists of these three solution categories:

- **Identity management:** Cisco Secure ACS provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. The Cisco Secure ACS extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework to allow greater flexibility and mobility, increased security, and user productivity gains. With Cisco Secure ACS, you can manage and administer user access for Cisco IOS routers, VPNs, firewalls, dialup and DSL connections, cable access solutions, storage, content, VoIP, Cisco wireless solutions, and Cisco Catalyst switches using IEEE 802.1x access control. These are the Cisco Secure ACS features:
  - Guarantees identity and integrity of each unit in the network
  - Provides network visibility and management
  - Allows for secure management of remote devices
  - Provides AAA services
- **Cisco Identity-Based Networking Services (IBNS):** Cisco IBNS is an integrated solution that combines several Cisco products to offer authentication, access control, and user policies to secure network connectivity and resources. The Cisco IBNS solution enables greater security while offering cost-effective management of changes throughout the organization. Cisco IBNS includes these features:
  - Creates trusted network domains
  - Expands LAN access security
  - Creates and assigns auto-VLAN based on policy
  - Prevents rogue access points
  - Supports wired or wireless networks

- **NAC:** Cisco NAC is a Cisco-sponsored industry initiative that uses network infrastructure to enforce security policy compliance on all devices that are trying to access network computing resources. NAC thereby limits damage from viruses and worms. These are the NAC features:
  - Enforces endpoint policy using the Cisco Trust Agent
  - Evaluates, permits, denies, or redirects (restricts, quarantines, or remediates) network traffic flow
  - Ensures that the network reaches all access devices
  - Extends effective functioning of Cisco Security Agent (CSA), anti-X (antivirus, antispyware, and antispam), and third-party solutions

Cisco NAC Products

This topic describes Cisco NAC products.



Cisco NAC Products

Cisco NAC

Cisco NAC Framework Traditional Cisco NAC

- Software module embedded within NAC-enabled products
- Integrated framework leveraging multiple Cisco and NAC-aware vendor products

Cisco NAC Appliance

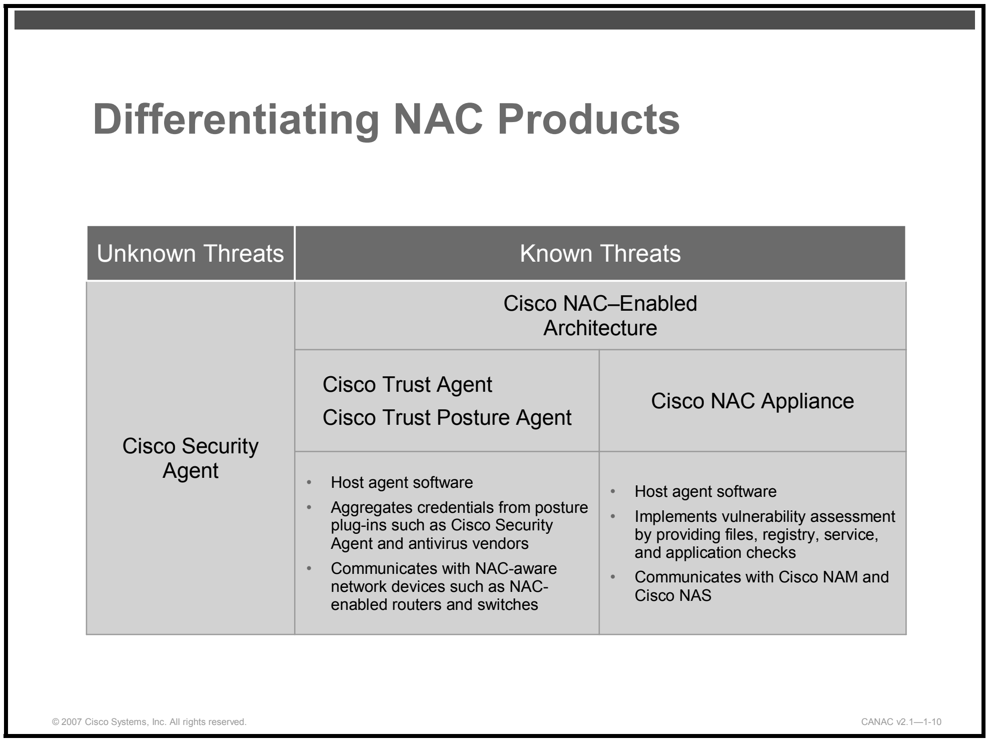
- In-band NAC Appliance solution can be used on any switch or router platform
- Self-contained, turnkey solution

- Offers customers a deployment timeframe choice
- Adapts to customer investment protection requirements

CANAC v2.1—1-9

Cisco NAC products come in two general categories:

- **NAC framework:** The NAC framework uses the network infrastructure and third-party software to enforce security policy compliance on all endpoints. The NAC framework is a system suited for high-performance network environments with diverse endpoints. These environments require a consistent LAN, WAN, wireless, extranet, and remote-access solution that integrates into existing security and patch software, tools, and processes.
- **Cisco NAC Appliance:** The Cisco NAC Appliance solution condenses NAC capabilities into appliance form and provides a turnkey solution to control network access. This solution is a natural fit for medium-scaled networks that require a self-contained, turnkey solution. Cisco NAC Appliance is especially ideal for organizations with few resources to design, deploy, and manage a solution, as well as those organizations that need simplified and integrated tracking of operating system, antivirus, and antispyware patches and vulnerability updates.



Differentiating NAC Products

Unknown Threats	Known Threats	
Cisco Security Agent	Cisco NAC–Enabled Architecture	
	Cisco Trust Agent Cisco Trust Posture Agent	Cisco NAC Appliance
	• Host agent software • Aggregates credentials from posture plug-ins such as Cisco Security Agent and antivirus vendors • Communicates with NAC-aware network devices such as NAC-enabled routers and switches	• Host agent software • Implements vulnerability assessment by providing files, registry, service, and application checks • Communicates with Cisco NAM and Cisco NAS

CANAC v2.1—1-10

Cisco NAC products can be grouped by either known or unknown security threats, and whether there are specific protocol requirements within the company network to deal with the threats. The figure shows that the Cisco Security Agent is designed to fight unknown security threats. The products that need to be configured for known security threats are NAC-enabled routers and switches: Cisco Trust Agent and Cisco NAC Appliance. The Cisco Trust Agent relies on the 802.1x authentication protocol, and the Cisco NAC Appliance product does not require any specific protocol to operate. Each Cisco NAC product has distinct key features:

- **Cisco Security Agent:** Cisco Security Agent provides threat protection for server and desktop computing systems, or endpoints, by analyzing behavior rather than relying on signature matching. Cisco Security Agent does not need updating to stop an attack that has not previously been encountered. It reduces operational costs by identifying, preventing, and eliminating both known and unknown security threats. The Cisco Security Agent consolidates endpoint security functions in a single agent and provides these benefits:
  - Host intrusion prevention
  - Spyware and adware protection
  - Protection against buffer overflow attacks
  - Distributed firewall capabilities
  - Malicious mobile code protection
  - Operating system integrity assurance
  - Application inventory
  - Audit log consolidation

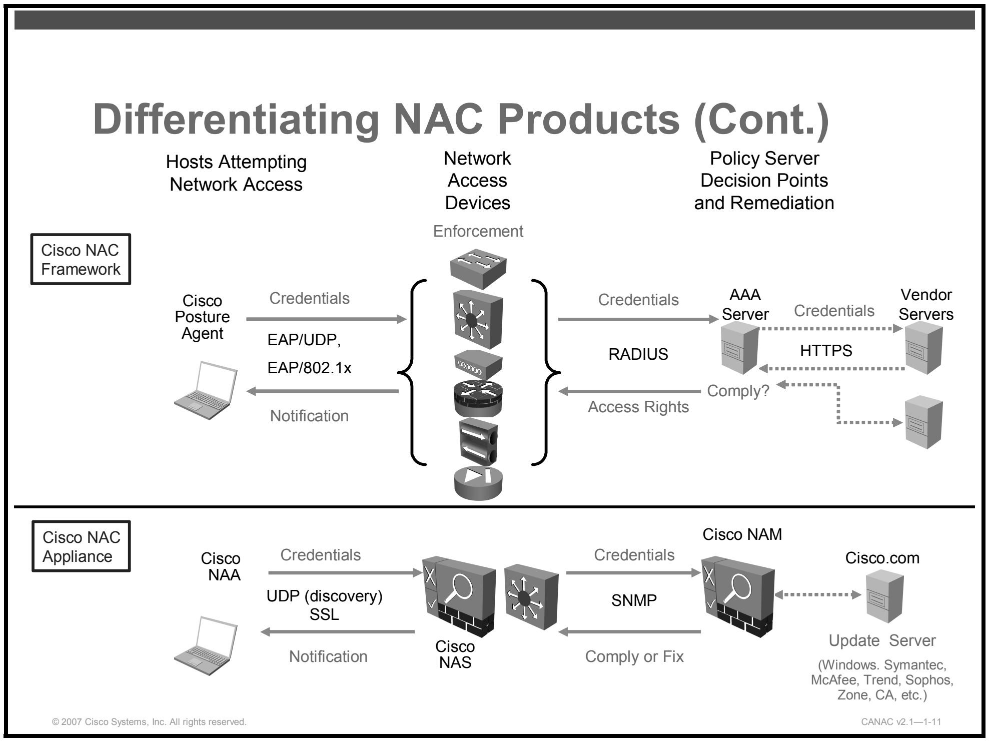
- **Cisco NAC-enabled architecture:** Phase 1 of NAC enables Cisco routers that communicate with the Cisco Trust Agent to gather endpoint security credentials and to enforce admission control policies. Router access control lists (ACLs) restrict communication between noncompliant hosts and other systems in the network. For example, the router ACL may only allow communication to an antivirus server in order to download a new pattern file. NAC currently supports endpoints running Microsoft Windows NT, XP, and 2000 operating systems. In Phase 2 of NAC, Cisco switches will be able to assign noncompliant hosts to quarantine VLAN segments on which only remediation servers reside. NAC also supports IPsec remote-access platforms such as the Cisco VPN 3000 Concentrator and expands support for additional endpoint operating systems. Cisco expands support beyond the initial NAC co-sponsors in order to support a broader range of access policy assessment and enforcement through the implementation of a broad application programming interface (API).

  — **Cisco Trust Agent:** Cisco Trust Agent is a core component of the NAC solution. Cisco Trust Agent must be installed on hosts if the host policy state is required to be validated before permitting network access. The Cisco Trust Agent interfaces with other posture plug-in software on the host using a published API and responds to posture queries from the Cisco network access device (NAD). A posture plug-in is a client built by a third-party vendor that has partnered with Cisco, and gathers vendor posture credentials. Cisco NAC uses vendor posture credentials to evaluate the posture of the Cisco NAC client.

  — **Cisco Trust Posture Agent:** A posture agent serves as the single point of contact on the endpoint device for aggregating credentials from all posture plug-ins and communicating with the network. The posture agent also provides a trusted relationship with the network for the purposes of exchanging posture credentials, and it maintains a record of registered posture plug-ins by both application type and vendor. The posture agent multiplexes and demultiplexes posture requests and posture notifications between the posture plug-ins and the network. The posture agent does not interpret credentials and notifications communicated between the network and a posture plug-in or vice versa. The only processing that the posture agent does is the necessary multiplexing and demultiplexing of requests and responses to and from the plug-ins and the network. In Cisco NAC, the posture agent is known as the Cisco Trust Agent. The Cisco Trust Agent interfaces with other software on the Cisco NAC client using a published API and responds to posture queries from the Cisco NAD.

  — **Cisco NAC Appliance:** Cisco NAC Appliance automatically detects, isolates, and cleans infected or vulnerable devices that attempt to access your network. Cisco NAC Appliance ensures that Cisco Security Agent exists on the endpoint device. Cisco NAC Appliance agent-based scans check the user system registry, file system, and system memory for specific services and applications. Networks with Cisco NAC Appliance can provide benefits such as these:

    - Minimized network outages
    - Enforced security policies
    - Automated device repairs and updates that provide significant cost savings



Differentiating NAC Products (Cont.)

Hosts Attempting Network Access

Network Access Devices

Policy Server Decision Points and Remediation

Cisco NAC Framework

Enforcement

Cisco Posture Agent

Credentials

EAP/UDP,

EAP/802.1x

Notification

Credentials

RADIUS

Access Rights

AAA Server

Credentials

HTTPS

Comply?

Vendor Servers

Cisco NAC Appliance

Cisco NAA

Credentials

UDP (discovery)
SSL

Notification

Cisco NAS

Credentials

SNMP

Comply or Fix

Cisco NAM

Cisco.com

Update Server

(Windows. Symantec, McAfee, Trend, Sophos, Zone, CA, etc.)

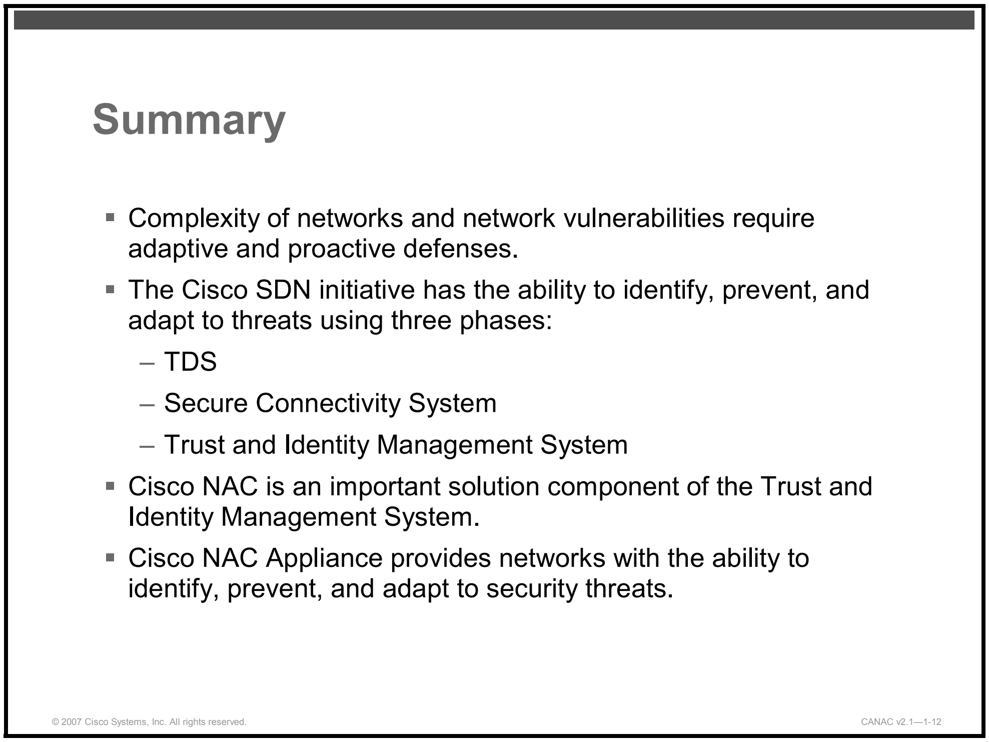
CANAC v2.1—1-11

The top of the figure shows the components of a Cisco NAC framework that provide compliance-based access control. NAC functions, including AAA, scanning, and remediation, are performed by other Cisco products (for example, the Cisco ACS provides AAA) or partner products (for example, TrendMicro provides antivirus updates).

Cisco NAC Appliance components, shown in the bottom of the figure, can authenticate, scan, and remediate without requiring other products. Cisco NAC Appliance also includes preconfigured checks for Windows updates and most major antivirus and antispyware software packages.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- Complexity of networks and network vulnerabilities require adaptive and proactive defenses.
- The Cisco SDN initiative has the ability to identify, prevent, and adapt to threats using three phases:
  - TDS
  - Secure Connectivity System
  - Trust and Identity Management System
- Cisco NAC is an important solution component of the Trust and Identity Management System.
- Cisco NAC Appliance provides networks with the ability to identify, prevent, and adapt to security threats.

Lesson 2

Introducing Cisco NAC Appliance

Overview

To have a secure network, companies need a way to recognize users, their devices, and their roles in the network. Beyond recognition, companies must evaluate whether machines are compliant with security policies, and then enforce security policies by blocking, isolating, and repairing noncompliant machines. A Cisco Network Admission Control (NAC) Appliance solution offers these capabilities.

This lesson provides an overview of the features, benefits, and key components of a Cisco NAC Appliance solution. The lesson describes the purpose of and certified platform for each component of Cisco NAC Appliance. In addition, the lesson lists steps needed to configure a Cisco NAC Appliance solution and describes the navigational features of the Cisco NAC Appliance web-based GUI.

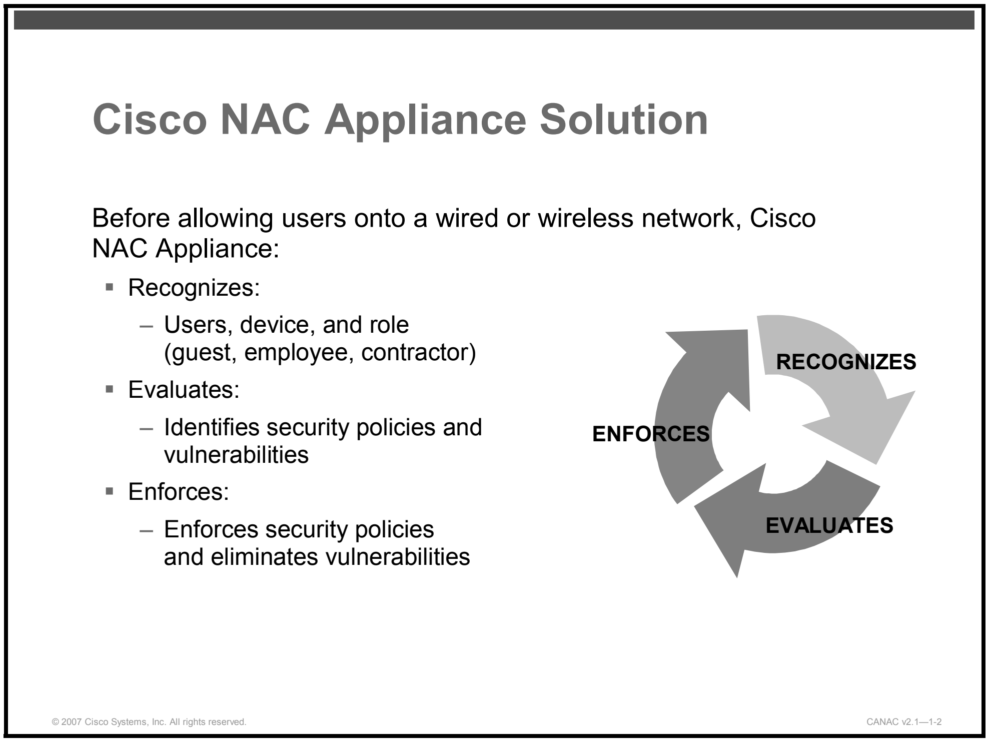
Objectives

Upon completing this lesson, you will be able to describe the Cisco NAC Appliance solution. This ability includes being able to meet these objectives:

- Summarize how the Cisco NAC Appliance solution controls and secures networks
- Describe the components of a Cisco NAC Appliance solution
- Describe the supported platforms for a Cisco NAC Appliance solution
- Explain how Cisco NAC Appliance enforces compliance for remote and local users
- Summarize how to configure a Cisco NAC Appliance solution
- Navigate through the Cisco NAC Appliance web-based GUI

Cisco NAC Appliance Solution

This topic describes how the Cisco NAC Appliance solution controls and secures networks.



Cisco NAC Appliance Solution

Before allowing users onto a wired or wireless network, Cisco NAC Appliance:

- Recognizes:
  - Users, device, and role (guest, employee, contractor)
- Evaluates:
  - Identifies security policies and vulnerabilities
- Enforces:
  - Enforces security policies and eliminates vulnerabilities

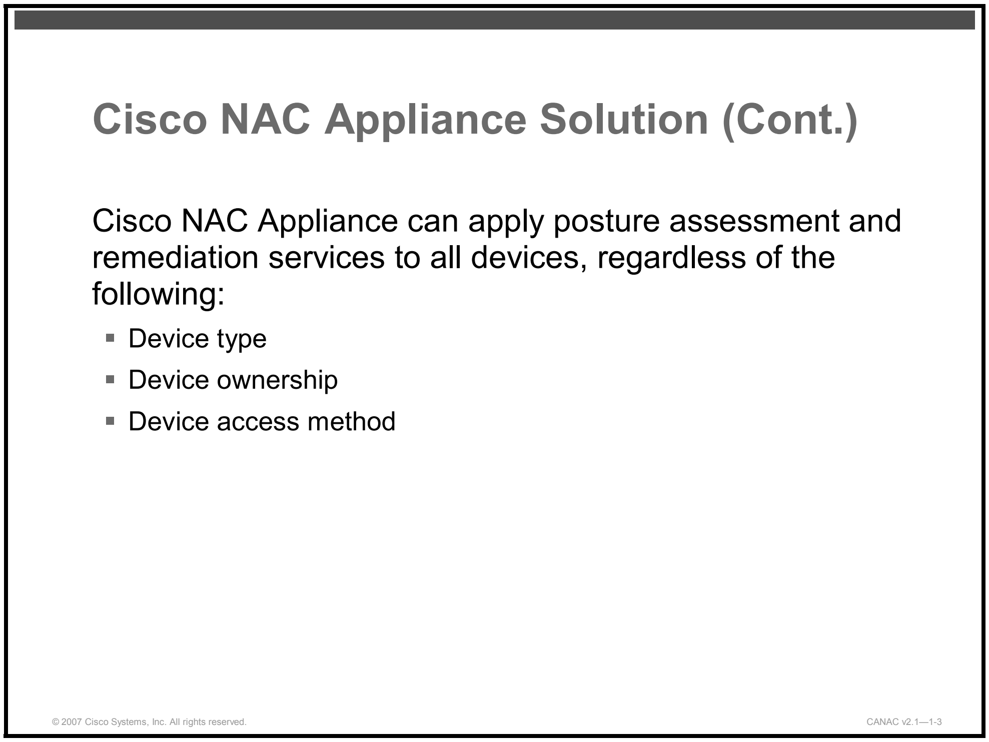
RECOGNIZES
EVALUATES
ENFORCES

CANAC v2.1—1-2

Cisco NAC Appliance is part of the Cisco Self-Defending Network initiative to improve the ability of networks to identify, prevent, and adapt to security threats. As the central management point for your network, Cisco NAC Appliance allows you to implement security and access policies in one place instead of propagating the policies throughout the network on many different devices.

There are three essential protective functions of Cisco NAC Appliance:

- **Recognize:** Recognize users, their devices, and their role in the network. This first step occurs at the point of authentication, before malicious code can cause damage.
- **Evaluate:** Evaluate whether machines are compliant with security policies. Security policies can vary by user type, device type, or operating system.
- **Enforce:** Enforce security policies by blocking, isolating, and repairing noncompliant machines. Cisco NAC Appliance redirects noncompliant machines to a quarantine area. Remediation then occurs at the discretion of the administrator.



Cisco NAC Appliance Solution (Cont.)

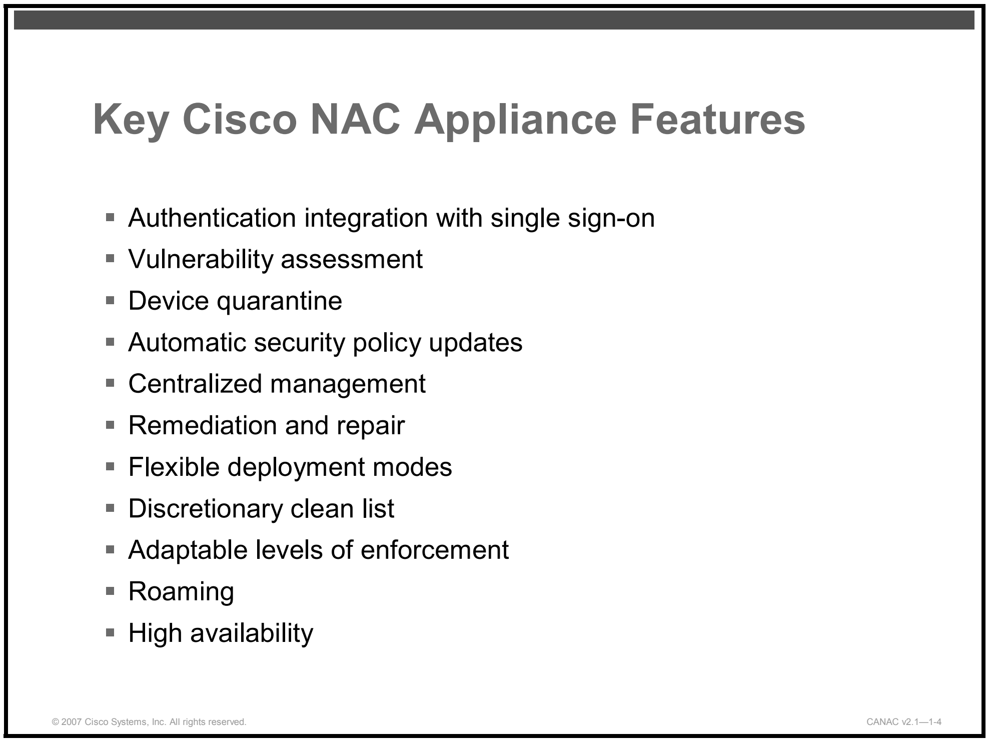
Cisco NAC Appliance can apply posture assessment and remediation services to all devices, regardless of the following:

- Device type
- Device ownership
- Device access method

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

Cisco NAC Appliance can apply posture assessment and remediation services to all devices, regardless of three things:

- **Device type:** Cisco NAC Appliance can enforce security policies on all networked devices, including Windows, Mac, or Linux machines, laptops, desktops, personal digital assistants (PDAs), and corporate assets such as printers and IP phones.
- **Device ownership:** Cisco NAC Appliance can apply security policies to systems owned by the corporation, employees, contractors, and guests.
- **Device access method:** Cisco NAC Appliance applies network admission control to devices connecting through the LAN, WLAN, WAN, or through virtual private networks (VPNs).



Key Cisco NAC Appliance Features

- Authentication integration with single sign-on
- Vulnerability assessment
- Device quarantine
- Automatic security policy updates
- Centralized management
- Remediation and repair
- Flexible deployment modes
- Discretionary clean list
- Adaptable levels of enforcement
- Roaming
- High availability

CANAC v2.1—1-4

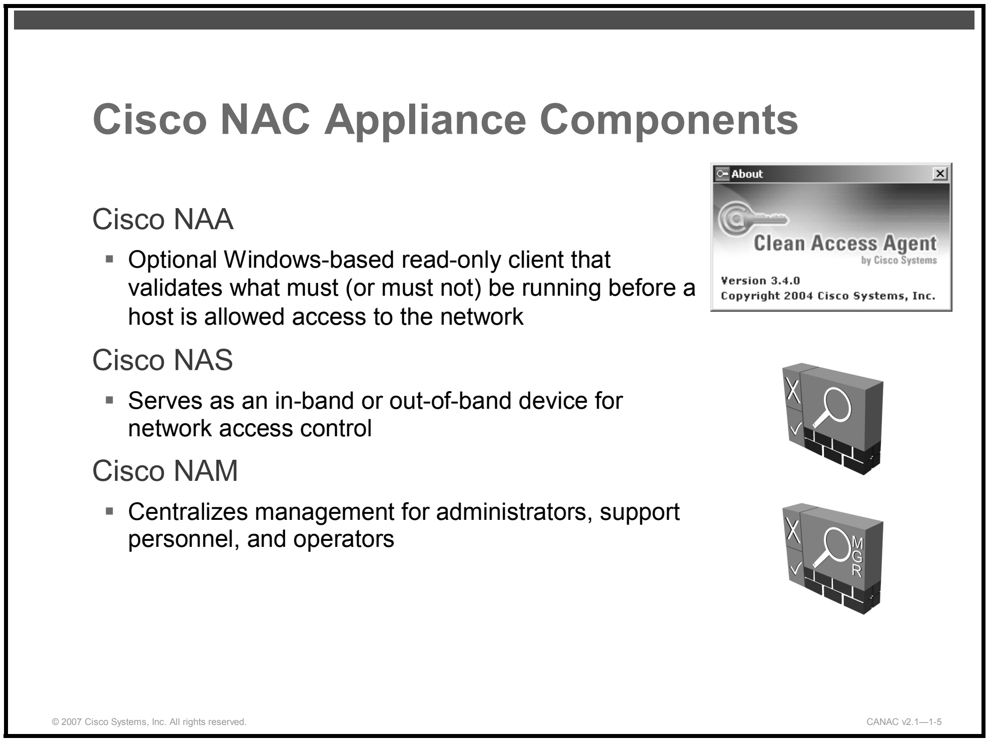
Cisco NAC Appliance includes these features:

- **Authentication integration with single sign-on:** Cisco NAC Appliance serves as an authentication proxy for most forms of authentication. Cisco NAC Appliance authentication is integrated with Kerberos, Lightweight Directory Access Protocol (LDAP), RADIUS, Active Directory, S/Ident, and others. To minimize the inconvenience to end users, Cisco NAC Appliance supports single sign-on for VPN clients, wireless clients, and Windows Active Directory domains. Administrators can maintain multiple user profiles with different permission levels through the use of roles-based access control.
- **Vulnerability assessment:** The Cisco NAC Appliance supports scanning of all network-based operating systems, Apple Macintosh operating systems, Linux machines, and non-PC networked devices including Xbox, PlayStation 2, and PDAs. Cisco NAC Appliance conducts network-based scans. You can base these scans on the scans provided by the open-source Nessus organization or you can custom-build scans. In a domain-controlled environment, Cisco NAC Appliance can also conduct scans of Windows registries without client software.
- **Device quarantine:** Cisco NAC Appliance can place noncompliant machines into quarantine, which prevents the spread of infection while enabling the machines to maintain access to remediation resources. Quarantine can be accomplished by using subnets as small as /30 or by using a quarantine VLAN.
- **Automatic security policy updates:** Automatic security policy updates provided by Cisco Systems as part of the standard software maintenance package provide predefined policies for the most common network access criteria. Updates include policies that check for critical operating system updates, common antivirus software virus definition updates, and common antispyware definition updates. Automatic updating eases the management cost on network administrators, who can rely on the Cisco NAC Appliance to constantly maintain updated policies.
- **Centralized management:** The web-based management console allows you to define the types of scans that are required for each role and the related remediation packages necessary for recovery. One management console can manage several servers.

- **Remediation and repair:** Quarantining provides devices with access to remediation servers that can provide operating system patches and updates, virus definition files, or endpoint security solutions such as Cisco Security Agent. You can automatically install these fixes using the Cisco NAC Appliance enforcement agent.
- **Flexible deployment modes:** Cisco NAC Appliance offers the broadest available array of deployment modes to fit into any customer network. Customers can deploy the product as a virtual or real IP gateway, at the edge or centrally, with Layer 2 or Layer 3 client access, and in-band or out-of-band with network traffic.
- **Discretionary clean list:** The clean list feature allows you to simplify access for devices known to be clean through processes other than the processes of Cisco NAC Appliance. If the clean list option is disabled, all machines are subject to scanning each time they enter the network. You can clear the clean list with one click during times of high virus and worm activity.
- **Adaptable levels of enforcement:** You can adapt to the fluctuations of malicious code incidents by adjusting which scans are required, the roles subject to these scans, the use of the clean list, and the types of remediation required. You can also limit available bandwidth and protocols based on user roles.
- **Roaming:** Network connections roam seamlessly across Cisco NAC Appliance server-connected subnets.
- **High availability:** Highly available servers ensure that services continue in the event of unexpected shutdowns.

Cisco NAC Appliance Components

This topic describes the components of a Cisco NAC Appliance solution.



Cisco NAC Appliance Components

Cisco NAA

- Optional Windows-based read-only client that validates what must (or must not) be running before a host is allowed access to the network

Cisco NAS

- Serves as an in-band or out-of-band device for network access control

Cisco NAM

- Centralizes management for administrators, support personnel, and operators

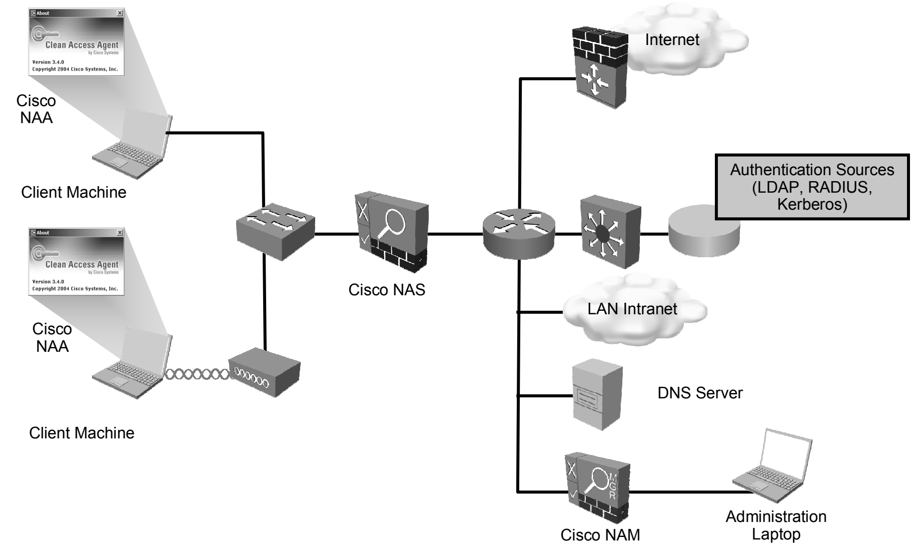
About
Clean Access Agent
by Cisco Systems
Version 3.4.0
Copyright 2004 Cisco Systems, Inc.
MGR

CANAC v2.1—1-5

The Cisco NAC Appliance solution consists of these three components, one of which is optional:

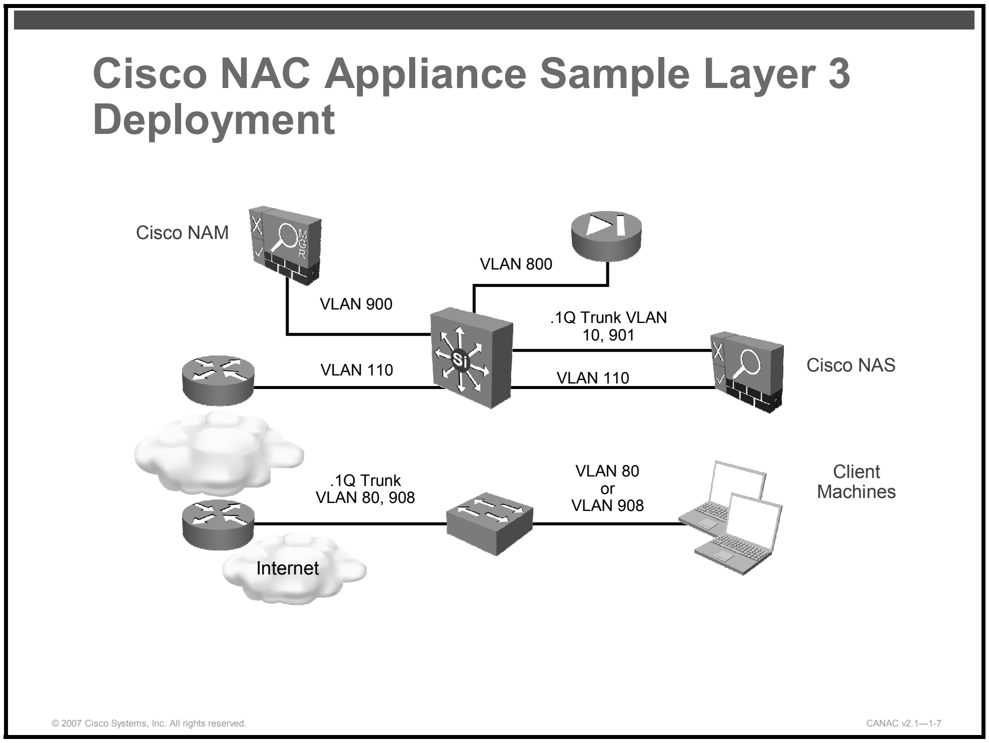
- **Cisco NAC Appliance Server:** The Cisco NAC Appliance Server (Cisco NAS) is the gateway server and enforcement engine between the untrusted (managed) network and the trusted network. It can be deployed in-band so that all traffic is managed by the Cisco NAS. The Cisco NAS can also be deployed out-of-band so that it manages client traffic during authentication; after the client has been given network access, client traffic is routed around the Cisco NAS. The Cisco NAS enforces the policies that you defined in the Cisco NAC Appliance Manager (Cisco NAM) administration console, including network access privileges, authentication requirements, bandwidth restrictions, and Cisco NAC Appliance system requirements.
- **Cisco NAM:** The Cisco NAM is the administration server for Cisco NAC Appliance deployment. The Cisco NAM can manage up to 20 Cisco NASs remotely, globally, or individually. The Cisco NAM acts as the authentication proxy to the authentication servers that reside on the back end of the network. Both the Cisco NAS and the Cisco NAM are available in failover mode. There is no single point of failure on these devices, which guarantees 100 percent operating time. The Cisco NAS and the Cisco NAM work together to ensure that the client computer meets your specified network and software requirements prior to gaining access to the network.
- **Cisco NAC Appliance Agent (Cisco NAA):** The Cisco NAA is an optional remediation agent of Cisco NAC Appliance that resides on Windows client computers. The Cisco NAA does not alter the client machine. It checks applications, files, services, or registry keys and prepares a report to send to the other Cisco NAC Appliance components. For web-based users, the Cisco NAC Appliance solution also includes web-based applets.

Cisco NAC Appliance Sample Layer 2 Deployment



There are many ways to implement Cisco NAC Appliance. This figure shows an in-band Layer 2 deployment of the components of Cisco NAC Appliance.

When a device attempts to log onto the network using a wired or wireless connection, Cisco NAC Appliance consults a certified devices list that contains the MAC and IP addresses of compliant machines. Cisco NAC Appliance scans any machine that is absent from the list. If Cisco NAC Appliance finds vulnerabilities in a machine, it redirects the machine to a quarantine area where the user can perform the necessary downloads to update the machine. The machine is then rescanned and, if compliant, is granted access to the network. Cisco NAC Appliance blocks client machines by either logical or physical means. The Cisco NAM controls admission of noncompliant wireless or wired users by restricting them to a particular subnet. It also generates a nonbroadcast, multi-access topology for virtual segmentation.

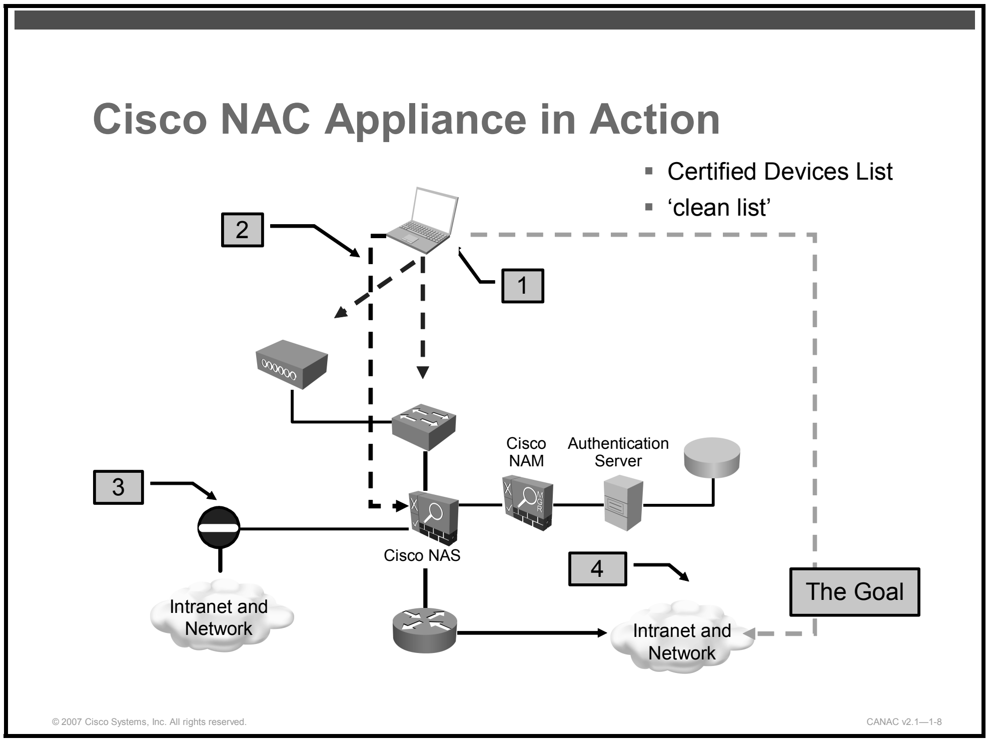


Cisco NAC Appliance Sample Layer 3 Deployment

CANAC v2.1—1-7

This figure shows an out-of-band Layer 3 deployment of the components of Cisco NAC Appliance. You can deploy Cisco NAC Appliance behind other Layer 3 network access devices, including VPN concentrators, dialup servers, and other routers. When the Cisco NAS notices a new IP address, it starts the authentication-assessment-remediation process.

When deployed out-of-band, Cisco NAC Appliance blocks noncompliant users at a port layer and prevents them from accessing the network until they pass inspection.



Cisco NAC Appliance in Action

- Certified Devices List
- ‘clean list’

CANAC v2.1—1-8

This figure shows how each component works when a user attempts to access a network.

When an end user attempts to access a web page on the network, Cisco NAC Appliance goes through these four steps to block access until the wired or wireless user provides login information:

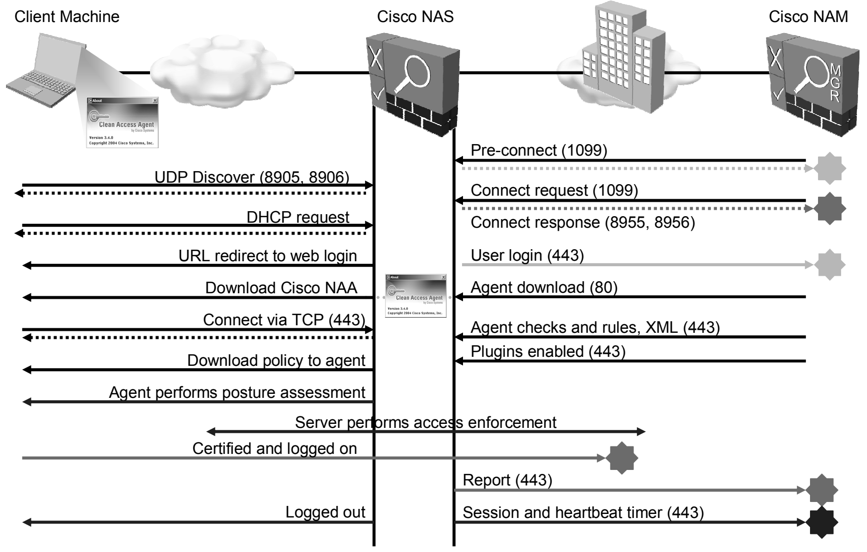
Step 1 Cisco NAC Appliance checks only hosts that are not on a certified devices list. You can clear the certified devices list manually or automatically at specified intervals. You can use the Certified Devices Timer form to clear the global certified devices list at a specified initial time and at regular intervals after that. Clearing the certified devices list forces client devices to repeat the Cisco NAC Appliance requirements at the next login. You can use the Certified Devices Timer to set how often the list is cleared for network scanning based on emerging vulnerabilities.

Step 2 If the user device is not on the certified devices list (as in the figure), Cisco NAC Appliance redirects the user to a login page provided by the Cisco NAS. The Cisco NAS validates the username and password and performs device and network scans to assess vulnerabilities on the device.

Step 3 If the Cisco NAS finds that the device is noncompliant or the login is incorrect, it denies the user access and assigns a quarantine role to the device. The quarantine role provides access to online remediation resources.

Step 4 If the Cisco NAS finds that the device is clean, or free of vulnerabilities, it places it on a “clean list” and grants the user access to the corporate intranet and network.

Cisco NAC Appliance in Action (Cont.)



Client Machine

Cisco NAS

Cisco NAM

Pre-connect (1099)

UDP Discover (8905, 8906)

Connect request (1099)

DHCP request

Connect response (8955, 8956)

URL redirect to web login

User login (443)

Download Cisco NAA

Agent download (80)

Connect via TCP (443)

Agent checks and rules, XML (443)

Plugins enabled (443)

Download policy to agent

Agent performs posture assessment

Server performs access enforcement

Certified and logged on

Report (443)

Logged out

Session and heartbeat timer (443)

This figure shows a ladder diagram of the protocols used at each step of the interaction between the client machine, the Cisco NAS, and the Cisco NAM. The communication process that the Cisco NAC Appliance components use reveals how difficult it is to undermine the security provided by a Cisco NAC Appliance implementation.

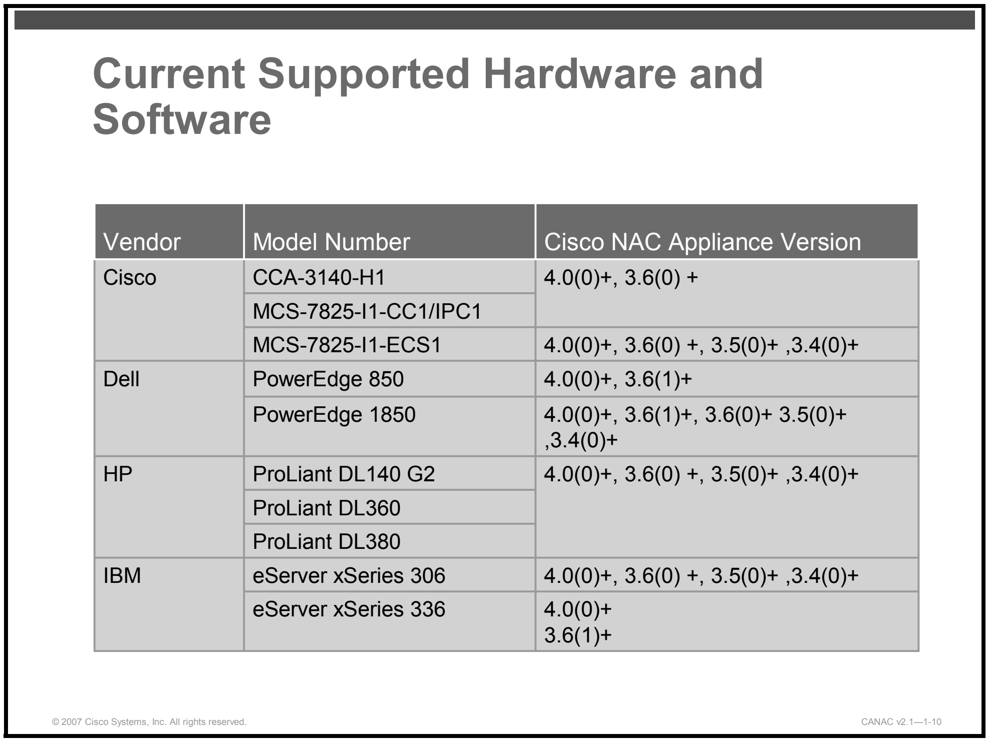
Starting at the top left of the ladder diagram and after the client machine attaches to the network, the Cisco NAM and the Cisco NAS engage in a Remote Method Invocation (RMI) registry communication process. The client machine and the Cisco NAS then begin a User Datagram Protocol (UDP) discovery process.

Note If the client logs onto the client machine and then opens a browser, the client machine will send HTTP packets to the Cisco NAS, and the Cisco NAS will then send the web login page to the client machine.

After the Cisco NAS has determined the presence of the client machine, the Cisco NAS requests and receives a connection to the network. The client machine then requests a DHCP, and, if this is a new user and does not yet have a Cisco NAA, the Cisco NAS redirects the client to a web login page and the client machine downloads the Cisco NAA. Once the Cisco NAA is downloaded, the process continues through posture assessment, access enforcement, and certification. The client is logged onto the network and the Cisco NAS sends a login report to the Cisco NAM. In the final step of the process, the client logs out and the session ends.

Cisco NAC Appliance Platforms

This topic describes the supported platforms for a Cisco NAC Appliance solution.



Current Supported Hardware and Software

Vendor	Model Number	Cisco NAC Appliance Version
Cisco	CCA-3140-H1	4.0(0)+, 3.6(0) +
	MCS-7825-I1-CC1/IPC1	
	MCS-7825-I1-ECS1	4.0(0)+, 3.6(0) +, 3.5(0)+ ,3.4(0)+
Dell	PowerEdge 850	4.0(0)+, 3.6(1)+
	PowerEdge 1850	4.0(0)+, 3.6(1)+, 3.6(0)+ 3.5(0)+ ,3.4(0)+
HP	ProLiant DL140 G2	4.0(0)+, 3.6(0) +, 3.5(0)+ ,3.4(0)+
	ProLiant DL360	
	ProLiant DL380	
IBM	eServer xSeries 306	4.0(0)+, 3.6(0) +, 3.5(0)+ ,3.4(0)+
	eServer xSeries 336	4.0(0)+ 3.6(1)+

CANAC v2.1—1-10

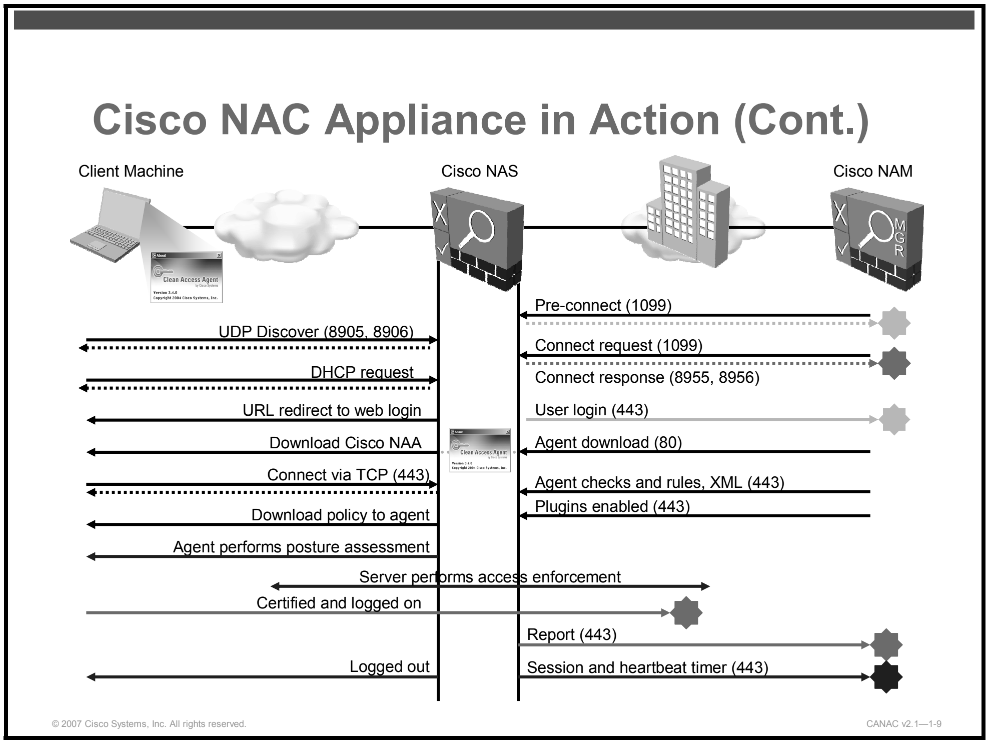
Both the Cisco NAS and Cisco NAM are delivered as a disc image that must be loaded onto a standard server. Both Cisco components are built on a hardened Linux kernel. The figure shows the currently supported hardware and software that is used to support a Cisco NAC Appliance solution.

The server models shown are considered certified because the hardware has been tested with the Cisco NAC Appliance software and is a fully supported platform.

The table has been simplified from the table found in the reference documentation. For detailed and current information on how to perform a custom installation and how to ensure that you have the most current hardware and software options available for the Cisco NAC Appliance solution, refer to the Supported Hardware and System Requirements for Cisco NAC Appliance section found on the Cisco NAC Appliance page at http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a00807600e1.html

Cisco NAC Appliance Local and Remote Compliance Scenarios

This topic describes how the Cisco NAC Appliance enforces compliance for local and remote users.



Cisco NAC Appliance in Action (Cont.)

Client Machine

Cisco NAS

Cisco NAM

Pre-connect (1099)

UDP Discover (8905, 8906)

Connect request (1099)

DHCP request

Connect response (8955, 8956)

URL redirect to web login

User login (443)

Download Cisco NAA

Agent download (80)

Connect via TCP (443)

Agent checks and rules, XML (443)

Plugins enabled (443)

Download policy to agent

Agent performs posture assessment

Server performs access enforcement

Certified and logged on

Report (443)

Logged out

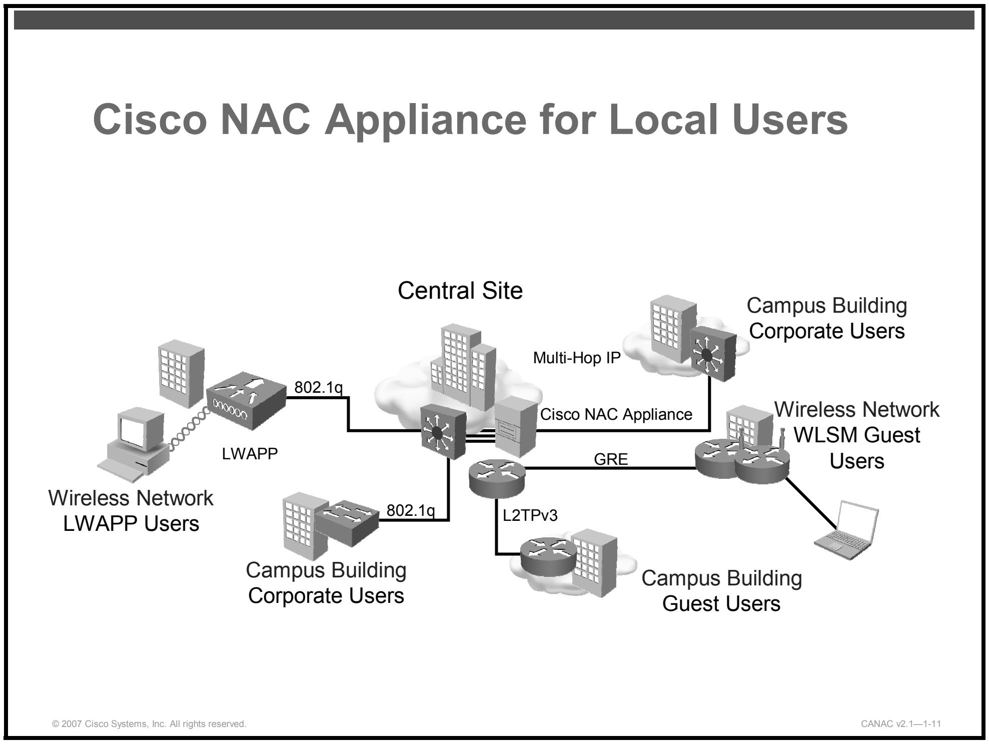
Session and heartbeat timer (443)

CANAC v2.1—1-9

The figure shows the different Cisco NAC Appliance deployments available for local users. In this example, Cisco NAC Appliance is deployed centrally. The Cisco NAC Appliance Deployment for Local Users table summarizes the features and benefits of a central deployment of Cisco NAC Appliance.

Cisco NAC Appliance Deployment for Local Users

Feature	Benefit
Supports 802.1q trunking	Enables central deployment mode
Supports Layer 3 multihop	End user devices can be several hops away
Supports Layer 2 Tunneling Protocol (L2TP) version 3 and generic routing encapsulation (GRE) tunneling	Extends enforcement to small remote buildings
Supports thin or thick wireless access points	Extends enforcement to any wireless networks



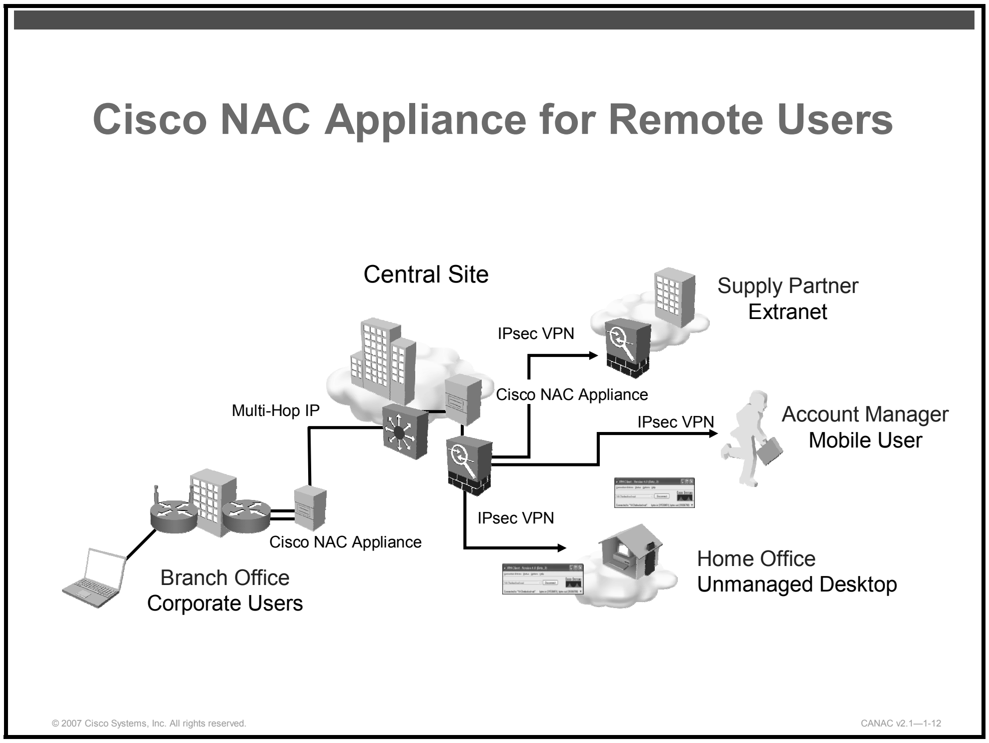
Cisco NAC Appliance for Local Users

CANAC v2.1—1-11

The figure shows a Cisco NAC Appliance deployment for remote users. The central site deploys the Cisco NAC Appliance solution behind the IPsec VPN and a switch. The IPsec VPN services support external users such as supply partners and the unmanaged desktops found in home offices. The branch office deploys their own Cisco NAC Appliance solution and uses a multihop IP connection with their central site. The Cisco NAC Appliance Deployment for Remote Users table summarizes the features and benefits of a Cisco NAC Appliance deployment for remote users.

Cisco NAC Appliance Deployment for Remote Users

Feature	Benefit
Supports remote access IPsec VPNs	Extends policy enforcement and compliance to remote access and VPN users
Supports site-to-site VPNs	Extends enforcement to site-to-site VPN partners
Supports VPN user sign-on	Leverages VPN sign-on for single-sign-on



Cisco NAC Appliance for Remote Users

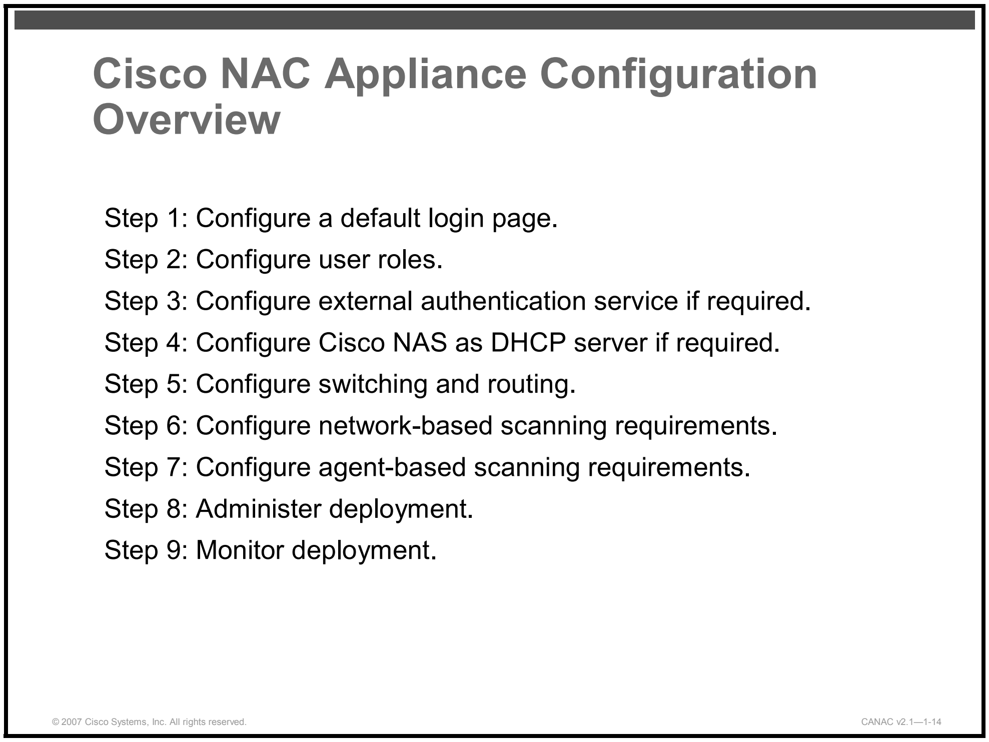
CANAC v2.1—1-12

The figure shows some of the many possible applications for Cisco NAC Appliance:

- **Endpoint compliance:** This deployment scenario prevents hosts in nonproduction segments such as labs from connecting to the production environment unless they have the latest required security patches installed.
- **Wireless compliance:** This deployment scenario prevents noncompliant devices from joining the network over wireless links.
- **Guest compliance:** This deployment scenario allows guests working within the company environment to access the Internet without accessing intranet resources.
- **VPN user compliance:** Ensures that only compliant remote-access users can access the intranet.
- **Internet compliance:** In this deployment scenario, compliance is checked when managed hosts attempt to communicate to unmanaged and high-risk areas such as sites on the Internet.

Cisco NAC Appliance Configuration Overview

This topic describes the steps required to configure a Cisco NAC Appliance solution.



Cisco NAC Appliance Configuration Overview

Step 1: Configure a default login page.

Step 2: Configure user roles.

Step 3: Configure external authentication service if required.

Step 4: Configure Cisco NAS as DHCP server if required.

Step 5: Configure switching and routing.

Step 6: Configure network-based scanning requirements.

Step 7: Configure agent-based scanning requirements.

Step 8: Administer deployment.

Step 9: Monitor deployment.

CANAC v2.1—1-14

You have been introduced to the Cisco NAC Appliance solution and you now have an understanding of how a Cisco NAC Appliance solution performs posture assessment, access enforcement, and certification. After you have physically deployed the components of a Cisco NAC Appliance solution, you must configure them. Follow these nine high-level steps to configure a Cisco NAC Appliance solution:

Step 1 Configure a default login page, which is required in order for both web login and Cisco NAA users to authenticate.

Step 2 Configure all user roles such as “employee,” “guest,” “wireless,” and so on.

Step 3 If you are using an external authentication service such as LDAP, RADIUS, Kerberos, or Active Directory, you will need to configure that service appropriately.

Step 4 If you are using the Cisco NAS as a DHCP server, you will have to configure the DHCP server separately.

Step 5 If you have chosen an out-of-band deployment, you must configure switches and routers appropriately.

Step 6 Configure these network-based scanning requirements:

— Check for worms such as Sasser, Bagle, Netsky, and others that you want to block.

— Check for vulnerabilities, such as the remote procedure call (RPC) buffer.

— Check for messenger buffer overflow, Blaster, and so on.

Step 7 Configure these agent-based scanning requirements:

— Define policy requirements for each user role.

— Define what software must be installed on the client.

- — Define what software must be running.
- — Define which version of the software must be present.

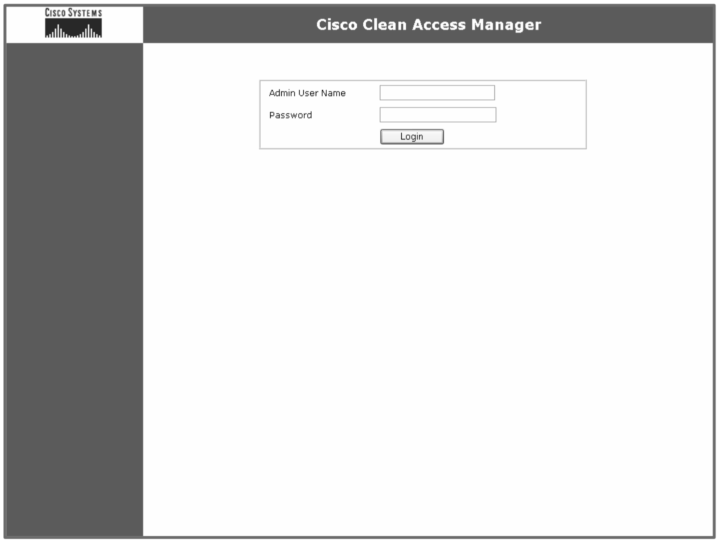
Step 8 Administer Cisco NAC Appliance deployment to manage users, modify network settings, and upgrade software.

Step 9 Monitor Cisco NAC Appliance deployment by interpreting event logs.

Cisco NAC Appliance User Interface

This topic describes how to navigate through the Cisco NAC Appliance web-based GUI.

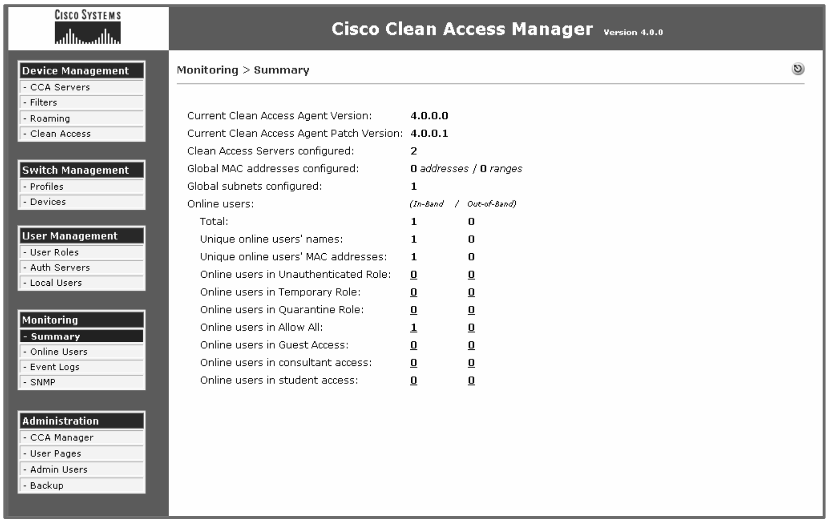
The Administration Console



CANAC v2.1—1-15

The Cisco NAM and the Cisco NAS have similar user interfaces that differ only in the type of features available. The figure shows the Cisco NAM login page. On either the Cisco NAM or the Cisco NAS, the first page that you need to navigate is the login page. Authorized users enter their login name and password. By default, Cisco NAM initially uses a username “admin” with a password “cisco123”. You will typically spend most of your time using the Cisco NAM to configure a Cisco NAC Appliance solution. The exception to this is when you configure a Cisco NAS high-availability solution. This topic will use the Cisco NAM web-based administration console to present user interfaces typical of the Cisco NAC Appliance GUI.

Cisco NAC Appliance Summary Page

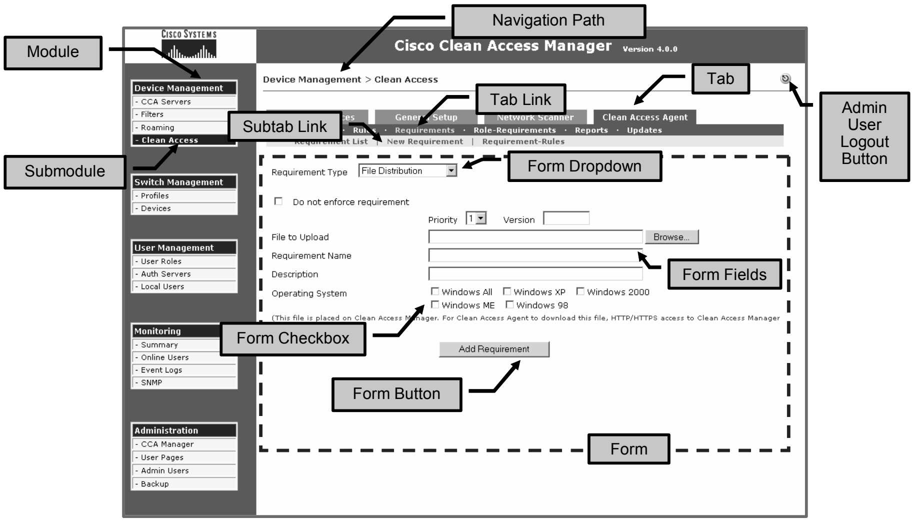


Monitoring > Summary

Current Clean Access Agent Version:	4.0.0.0	
Current Clean Access Agent Patch Version:	4.0.0.1	
Clean Access Servers configured:	2	
Global MAC addresses configured:	0 *addresses* / 0 *ranges*	
Global subnets configured:	1	
Online users:	*(In-Band*	*/ Out-of-Band)*
Total:	1	0
Unique online users' names:	1	0
Unique online users' MAC addresses:	1	0
Online users in Unauthenticated Role:	0	0
Online users in Temporary Role:	0	0
Online users in Quarantine Role:	0	0
Online users in Allow All:	1	0
Online users in Guest Access:	0	0
Online users in consultant access:	0	0
Online users in student access:	0	0

After a successful login to the Cisco NAM, the Monitoring > Summary page appears, which displays the main modules and module menus on the left panel. Choose any menu option.

Administration Console Page Elements



Device Management > Clean Access

Requirement Type: File Distribution

□ Do not enforce requirement

Priority 1 Version

File to Upload

Requirement Name

Description

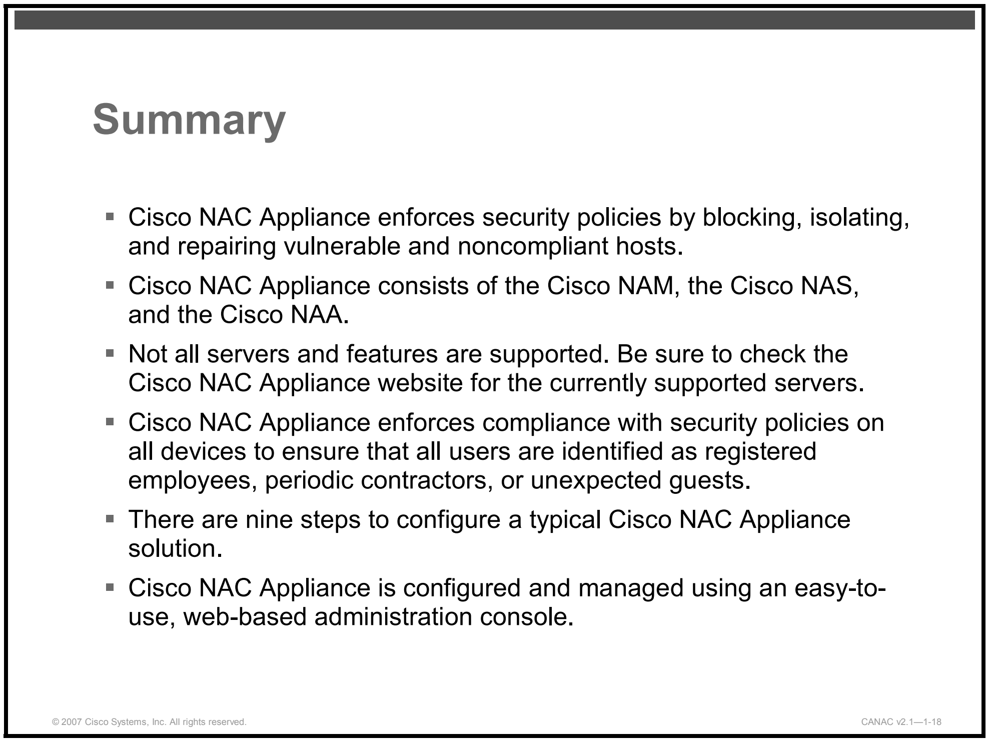
Operating System □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

(This file is placed on Clean Access Manager. For Clean Access Agent to download this file, HTTP/HTTPS access to Clean Access Manager

The administration console page is shown in the figure, which identifies components of the Cisco NAC Appliance GUI that are found in the Cisco NAM and the Cisco NAS web-based administration consoles.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- Cisco NAC Appliance enforces security policies by blocking, isolating, and repairing vulnerable and noncompliant hosts.
- Cisco NAC Appliance consists of the Cisco NAM, the Cisco NAS, and the Cisco NAA.
- Not all servers and features are supported. Be sure to check the Cisco NAC Appliance website for the currently supported servers.
- Cisco NAC Appliance enforces compliance with security policies on all devices to ensure that all users are identified as registered employees, periodic contractors, or unexpected guests.
- There are nine steps to configure a typical Cisco NAC Appliance solution.
- Cisco NAC Appliance is configured and managed using an easy-to-use, web-based administration console.

CANAC v2.1—1-18

Lesson 3

Introducing In-Band and Out-of-Band Deployment Options

Overview

A key advantage of a Cisco Network Admission Control (NAC) Appliance solution is the number of ways that it can be deployed. A disadvantage is that it can be a challenge to select the correct deployment option for your network environment. This lesson describes the deployment options that are available, the key differences between out-of-band and in-band deployment options, and the Cisco NAC Appliance Server (Cisco NAS) modes of operation.

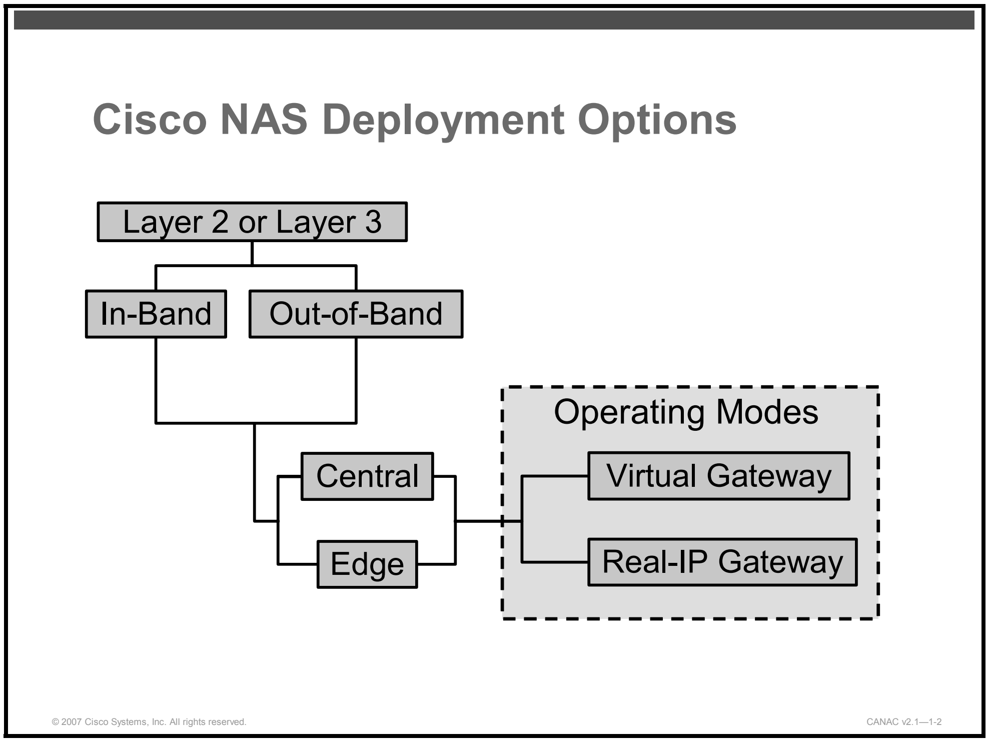
Objectives

Upon completing this lesson, you will be able to describe how you can deploy Cisco NAC Appliance to protect against specified threats. This ability includes being able to meet these objectives:

- Describe the Cisco NAS deployment options
- Describe the in-band and out-of-band deployment options
- Describe the key features of a Cisco NAC Appliance out-of-band deployment
- Describe the key features of a Cisco NAC Appliance in-band deployment
- Describe the Cisco NAS operating modes for an in-band and out-of-band deployment

Cisco NAS Deployment Options

This topic describes the Cisco NAS deployment options.

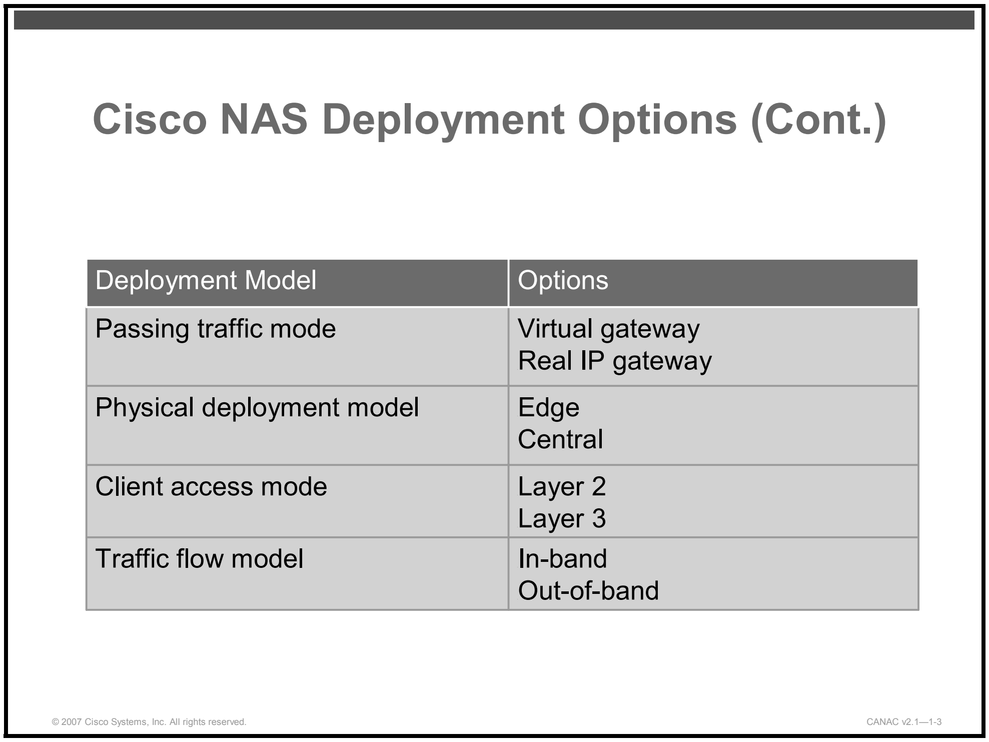


The figure shows how you can deploy the Cisco NAS. After an in-band or an out-of-band deployment option is selected, all other deployment options are the same for either choice. Here is a summary of each deployment option shown in the flow chart:

- **Layer 2 or Layer 3:** The first decision to make in determining the deployment you want to use is to determine whether or not your solution will be implemented as a Layer 2 or a Layer 3 solution.
- **In-band deployment:** In an in-band Cisco NAC Appliance deployment, all network traffic to or from each client goes through the Cisco NAS.
- **Out-of-band deployment:** In an out-of-band deployment, client machines pass through the Cisco NAC Appliance network only when they are authenticated and certified before being connected directly to the trusted network. This is the ideal deployment for high throughput or highly routed environments.
- **Central deployment:** A centrally deployed Cisco NAS reduces the number of Cisco NASs that you need to deploy, which facilitates management and scalability. In a central deployment, you can configure the Cisco NAS to perform either routing or bridging for the untrusted network.
- **Edge deployment:** When you deploy the Cisco NAS at the edge of your network, the Cisco NAS is placed between each managed subnet and router in the network. This deployment allows the Cisco NAS to continue to capture MAC addresses for the devices that are being managed. In edge deployment, the Cisco NAS can act as either a virtual bridge or a real-IP gateway.
- **Real-IP gateway:** In real-IP gateway mode, the Cisco NAS operates as a router and is the default gateway for the untrusted network. In this mode, the Cisco NAS can act as the DHCP server for client machines.

- **Virtual gateway:** In virtual gateway mode, the Cisco NAS operates as a Layer 2 transparent bridge.

Caution You can deploy the Cisco NAS as a Network Address Translation (NAT) gateway operating as an IP gateway and providing NAT services for the untrusted network. However, a Cisco NAS NAT deployment is only recommended for student labs and demonstrations.



Cisco NAS Deployment Options (Cont.)

Deployment Model	Options
Passing traffic mode	Virtual gateway Real IP gateway
Physical deployment model	Edge Central
Client access mode	Layer 2 Layer 3
Traffic flow model	In-band Out-of-band

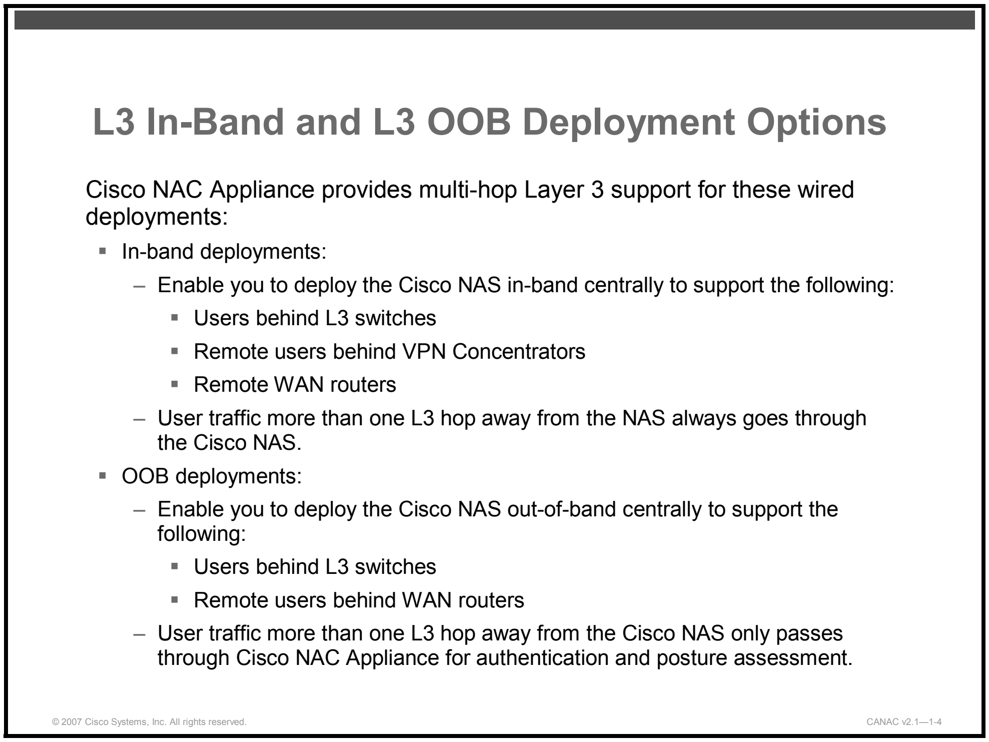
CANAC v2.1—1-3

Another way to consider how a Cisco NAS can be deployed is to look at different deployment models. The Cisco NAS Deployment Options table matches types of deployment models with the Cisco NAS deployment options that you should use to accommodate customer network requirements.

Cisco NAS Deployment Options

Deployment Model	Options
Passing traffic mode	■ Virtual gateway (bridged mode) ■ Real IP gateway (routed mode)
Physical deployment model	■ Edge ■ Central
Client access mode	■ **Layer 2:** When the client is adjacent to the Cisco NAS ■ **Layer 3:** When the client is multiple hops away from the Cisco NAS
Traffic flow model	■ **In-band:** When the Cisco NAS is always in line with user traffic ■ **Out-of-band:** When the Cisco NAS is in line only during authentication, posture assessment, and remediation

Cisco NAC Appliance can be purchased as either a software-only product or an appliance that includes compatible, rack-mountable hardware from Cisco Systems. Customers choosing to purchase the software-only version should consult with the certified hardware list located at http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a00807600e1.html



L3 In-Band and L3 OOB Deployment Options

Cisco NAC Appliance provides multi-hop Layer 3 support for these wired deployments:

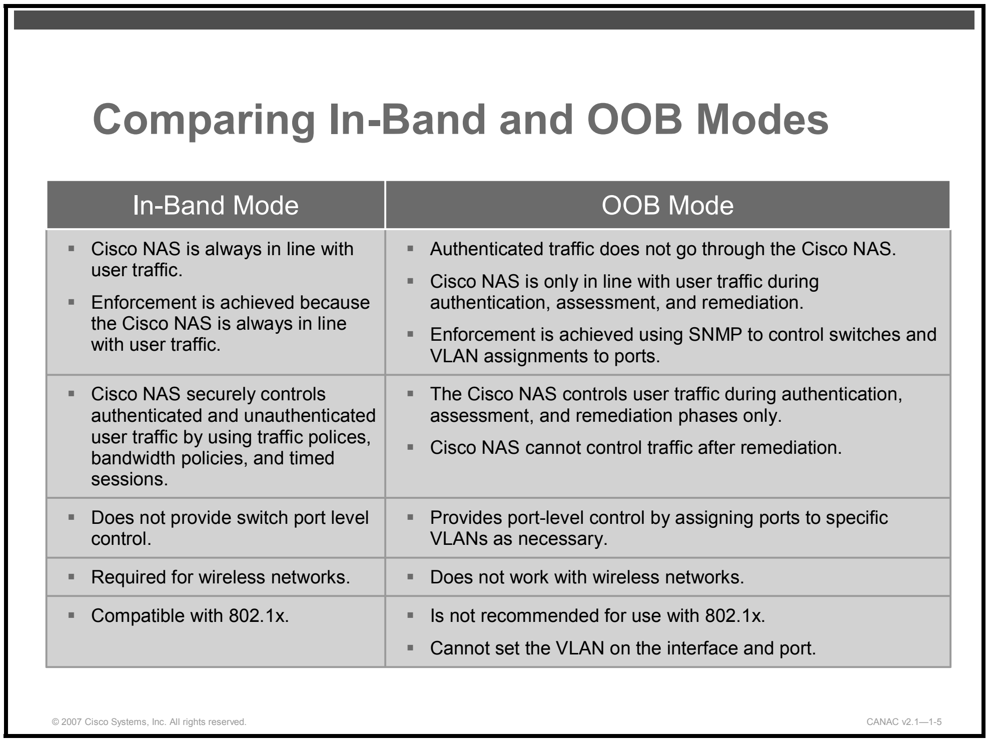
- In-band deployments:
  - Enable you to deploy the Cisco NAS in-band centrally to support the following:
    - Users behind L3 switches
    - Remote users behind VPN Concentrators
    - Remote WAN routers
  - User traffic more than one L3 hop away from the NAS always goes through the Cisco NAS.
- OOB deployments:
  - Enable you to deploy the Cisco NAS out-of-band centrally to support the following:
    - Users behind L3 switches
    - Remote users behind WAN routers
  - User traffic more than one L3 hop away from the Cisco NAS only passes through Cisco NAC Appliance for authentication and posture assessment.

The Cisco NAC Appliance solution now supports Layer 3 in-band and out-of-band deployments. Cisco NAC Appliance Release 3.5(3) introduced multi-hop Layer 3 support for in-band (wired) deployments, enabling administrators to deploy the Cisco NAS in-band centrally (in the core or distribution layer) to support users behind Layer 3 switches (for example, routed access) and remote users behind virtual private network (VPN) Concentrators or remote WAN routers. With Layer 3 in-band deployment, users more than one Layer 3 hop away from the Cisco NAS are supported and their traffic always goes through the Cisco NAS.

Cisco NAC Appliance Release 4.0 introduces multi-hop Layer 3 support for out-of-band (wired) deployments, enabling administrators to deploy the Cisco NAS out-of-band centrally (in the core or distribution layer) to support users behind Layer 3 switches (for example, routed access) and remote users behind WAN routers in some instances. Using Layer 3 out-of-band deployment, users more than one Layer 3 hop away from the Cisco NAS are supported and their traffic goes through the Cisco NAS for authentication and posture assessment only.

In-Band and Out-of-Band Deployment Options

This topic describes the in-band and out-of-band deployment options.

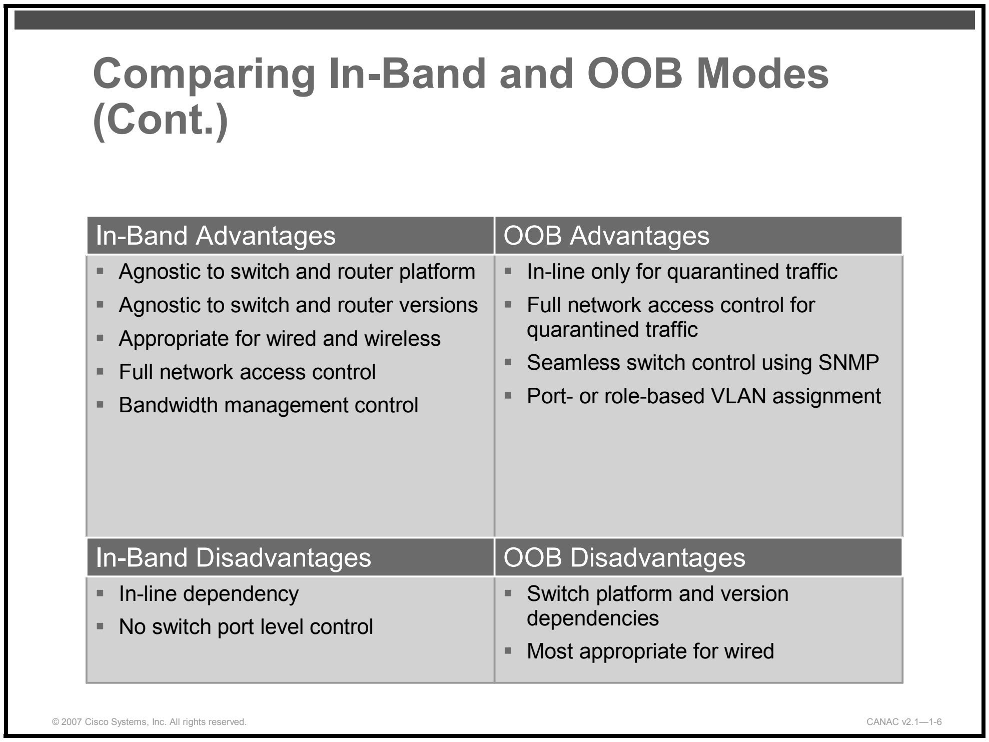


Comparing In-Band and OOB Modes

In-Band Mode	OOB Mode
- Cisco NAS is always in line with user traffic. - Enforcement is achieved because the Cisco NAS is always in line with user traffic.	- Authenticated traffic does not go through the Cisco NAS. - Cisco NAS is only in line with user traffic during authentication, assessment, and remediation. - Enforcement is achieved using SNMP to control switches and VLAN assignments to ports.
- Cisco NAS securely controls authenticated and unauthenticated user traffic by using traffic polices, bandwidth policies, and timed sessions.	- The Cisco NAS controls user traffic during authentication, assessment, and remediation phases only. - Cisco NAS cannot control traffic after remediation.
- Does not provide switch port level control.	- Provides port-level control by assigning ports to specific VLANs as necessary.
- Required for wireless networks.	- Does not work with wireless networks.
- Compatible with 802.1x.	- Is not recommended for use with 802.1x. - Cannot set the VLAN on the interface and port.

CANAC v2.1—1-5

The table compares the in-band and out-of-band deployment modes. Cisco NAC Appliance solution offers the flexibility to connect users with either in-band or out-of-band deployment, depending on specific requirements. The specifics of a customer network can require in-band deployment, out-of-band deployment, or a combination of both.



Comparing In-Band and OOB Modes (Cont.)

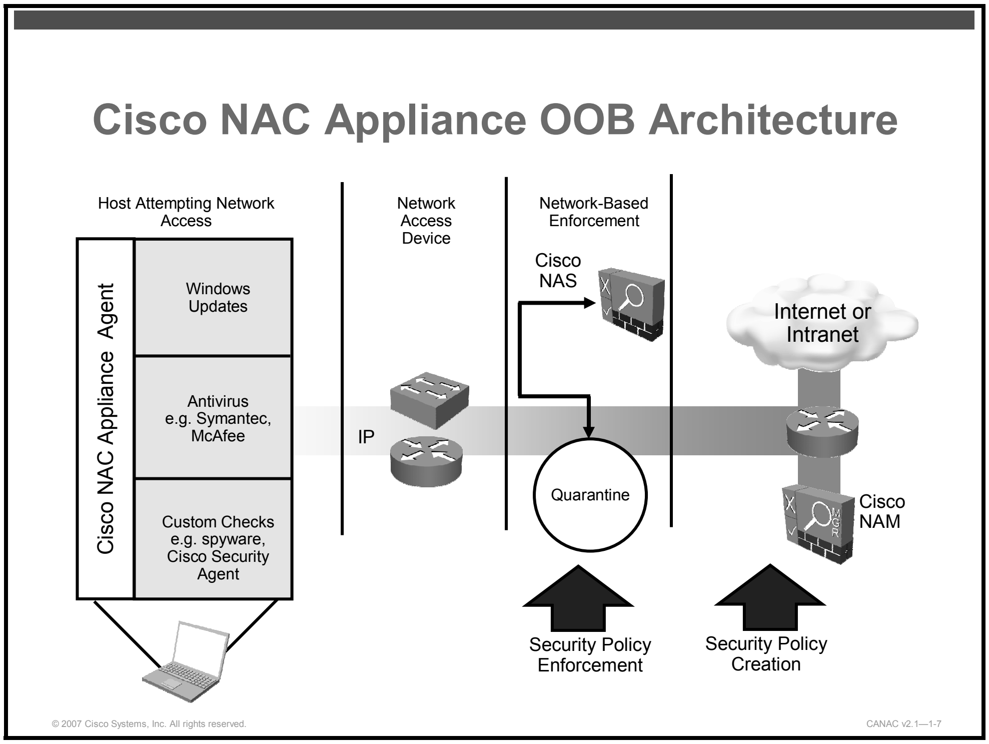
In-Band Advantages	OOB Advantages
▪ Agnostic to switch and router platform ▪ Agnostic to switch and router versions ▪ Appropriate for wired and wireless ▪ Full network access control ▪ Bandwidth management control	▪ In-line only for quarantined traffic ▪ Full network access control for quarantined traffic ▪ Seamless switch control using SNMP ▪ Port- or role-based VLAN assignment
In-Band Disadvantages	**OOB Disadvantages**
▪ In-line dependency ▪ No switch port level control	▪ Switch platform and version dependencies ▪ Most appropriate for wired

CANAC v2.1—1-6

The figure shows the advantages and disadvantages of in-band and out-of-band deployments.

Cisco NAC Appliance Out-of-Band Deployment

This topic describes the key features of a Cisco NAC Appliance out-of-band deployment.



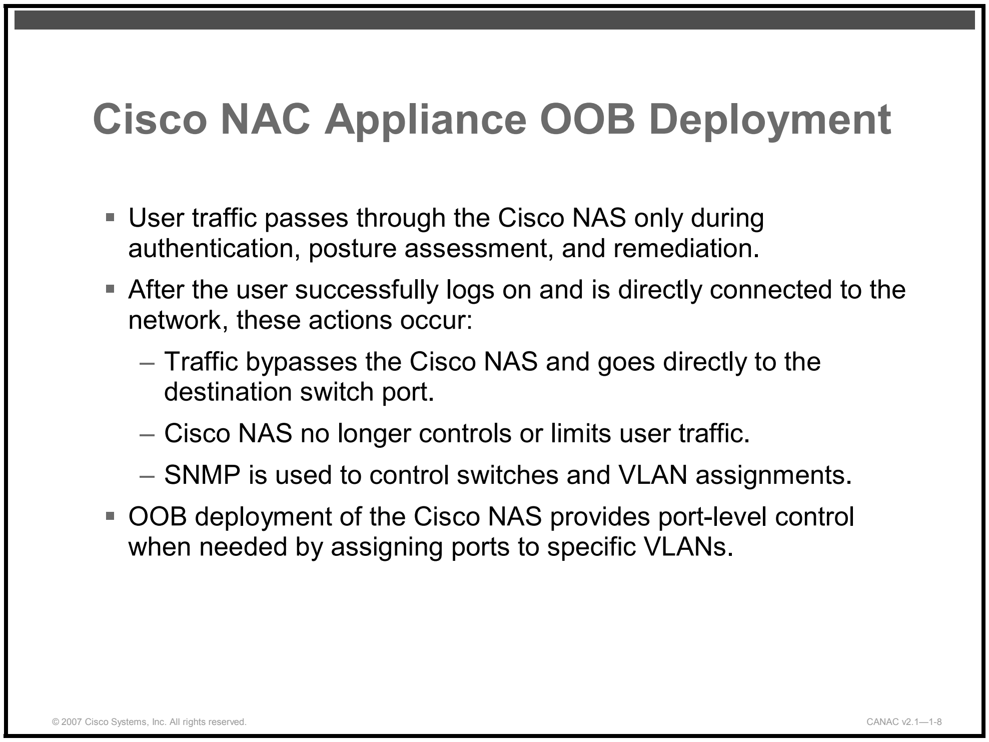
Cisco NAC Appliance OOB Architecture

Host Attempting Network Access
Cisco NAC Appliance Agent
Windows Updates
Antivirus e.g. Symantec, McAfee
Custom Checks e.g. spyware, Cisco Security Agent
IP
Network Access Device
Network-Based Enforcement
Cisco NAS
Quarantine
Internet or Intranet
Cisco NAM
Security Policy Enforcement
Security Policy Creation

CANAC v2.1—1-7

The figure shows a logical diagram of Cisco NAC Appliance in out-of-band deployment mode. In out-of-band mode, the Cisco NAS is located in the authentication VLAN, which is where all devices that are not found on the certified devices list are redirected upon entry. Users are blocked at the port layer and restricted from access to the trusted network until they successfully pass inspection.

To incorporate out-of-band architecture, you must add an authentication VLAN to your network and trunk all authentication VLANs to the untrusted interface of the Cisco NAS.



Cisco NAC Appliance OOB Deployment

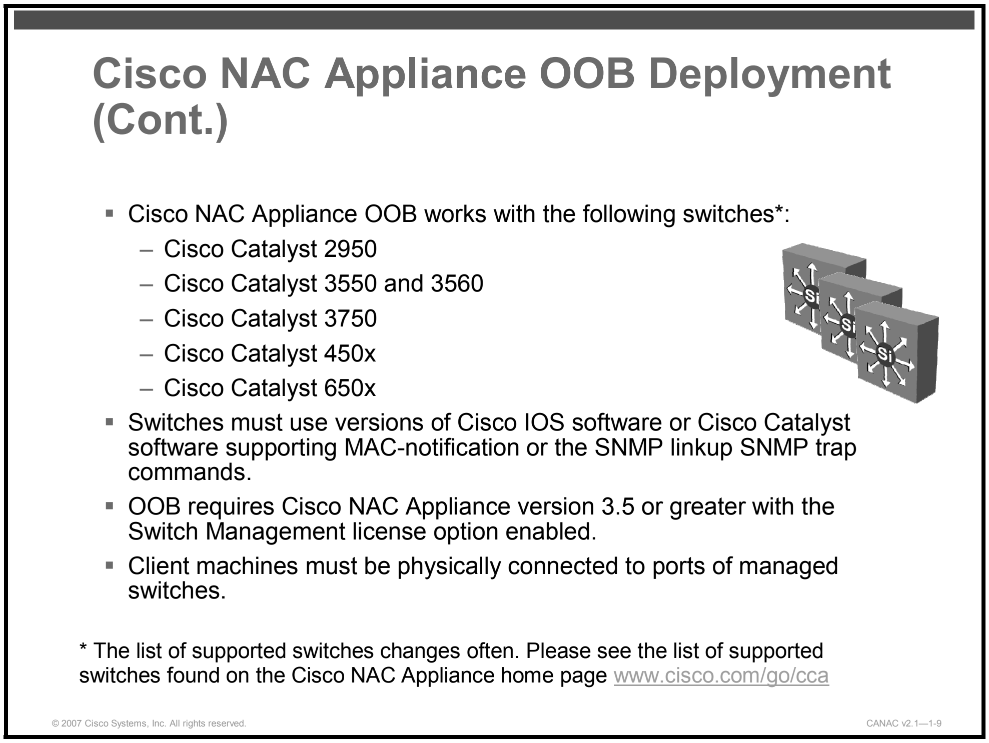
- User traffic passes through the Cisco NAS only during authentication, posture assessment, and remediation.
- After the user successfully logs on and is directly connected to the network, these actions occur:
  - Traffic bypasses the Cisco NAS and goes directly to the destination switch port.
  - Cisco NAS no longer controls or limits user traffic.
  - SNMP is used to control switches and VLAN assignments.
- OOB deployment of the Cisco NAS provides port-level control when needed by assigning ports to specific VLANs.

CANAC v2.1—1-8

For high throughput or highly routed environments, a Cisco NAS out-of-band deployment allows client machines to pass through the Cisco NAC Appliance network only to be authenticated and certified before being connected directly to the trusted network.

With out-of-band deployment, the Cisco NAS is in line with user traffic only during the process of authentication, assessment, and remediation. Once this process is complete, user traffic does not come to the Cisco NAS. Enforcement of network security policies is achieved through the use of Simple Network Management Protocol (SNMP) to control switches and VLAN assignments to ports.

The Cisco NAM provides port-level or role-level control by assigning ports to specific VLANs, by assigning users to specific roles that map to specific VLANs, and by providing a time-based session timeout per role. Shared or unmanaged access devices (for example, hubs and access points) are not supported by out-of-band deployment.



Cisco NAC Appliance OOB Deployment (Cont.)

- Cisco NAC Appliance OOB works with the following switches*:
  - Cisco Catalyst 2950
  - Cisco Catalyst 3550 and 3560
  - Cisco Catalyst 3750
  - Cisco Catalyst 450x
  - Cisco Catalyst 650x
- Switches must use versions of Cisco IOS software or Cisco Catalyst software supporting MAC-notification or the SNMP linkup SNMP trap commands.
- OOB requires Cisco NAC Appliance version 3.5 or greater with the Switch Management license option enabled.
- Client machines must be physically connected to ports of managed switches.

* The list of supported switches changes often. Please see the list of supported switches found on the Cisco NAC Appliance home page www.cisco.com/go/cca

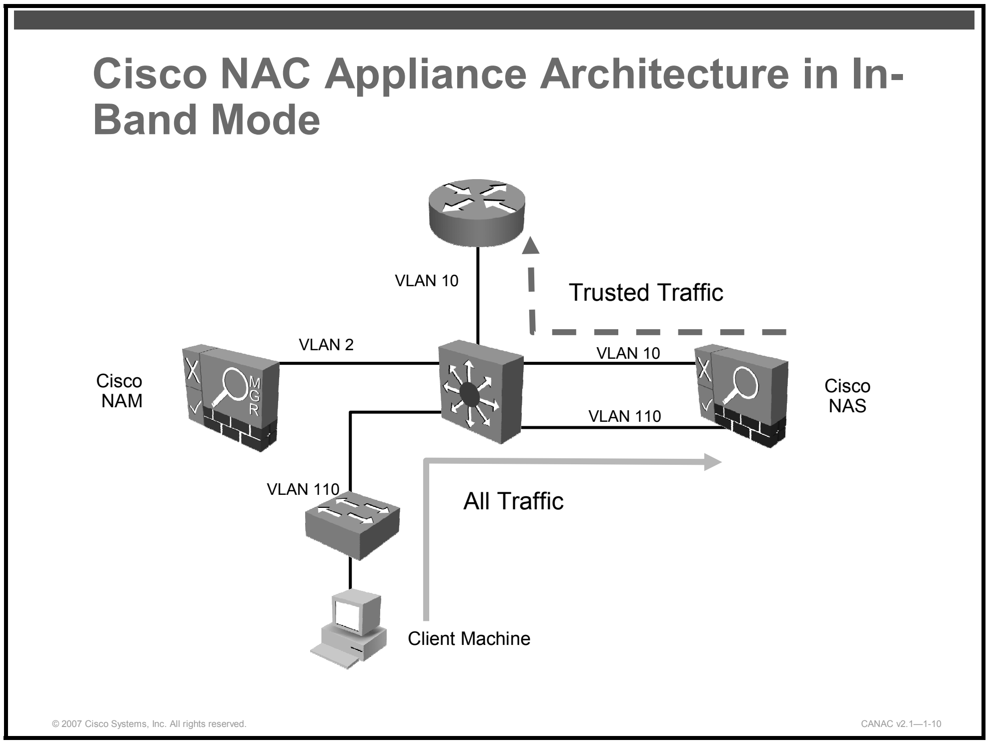
CANAC v2.1—1-9

An out-of-band implementation of Cisco NAC Appliance has these requirements:

- The Cisco switches that your network uses must be supported by the Cisco NAC Appliance. Here is a list of some of the supported models:
  - Cisco Catalyst 2950 Switch
  - Cisco Catalyst 3550 Switch or Cisco Catalyst 3560 Switch
  - Cisco Catalyst 3750 Switch
  - Cisco Catalyst 4500 Series Switch
  - Cisco Catalyst 6500 Series Switch
- Controlled switches must use the latest versions of Cisco IOS software or Cisco Catalyst software that supports the **mac-notification** or the **snmp linkup** SNMP trap commands.
- Your Cisco NAC Appliance license must enable switch management, and your Cisco NASs and Cisco NAM must be version 3.5 or greater.
- Clients must be physically connected to the ports of managed switches.

Cisco NAC Appliance In-Band Deployment

This topic describes the key features of a Cisco NAC Appliance in-band deployment.

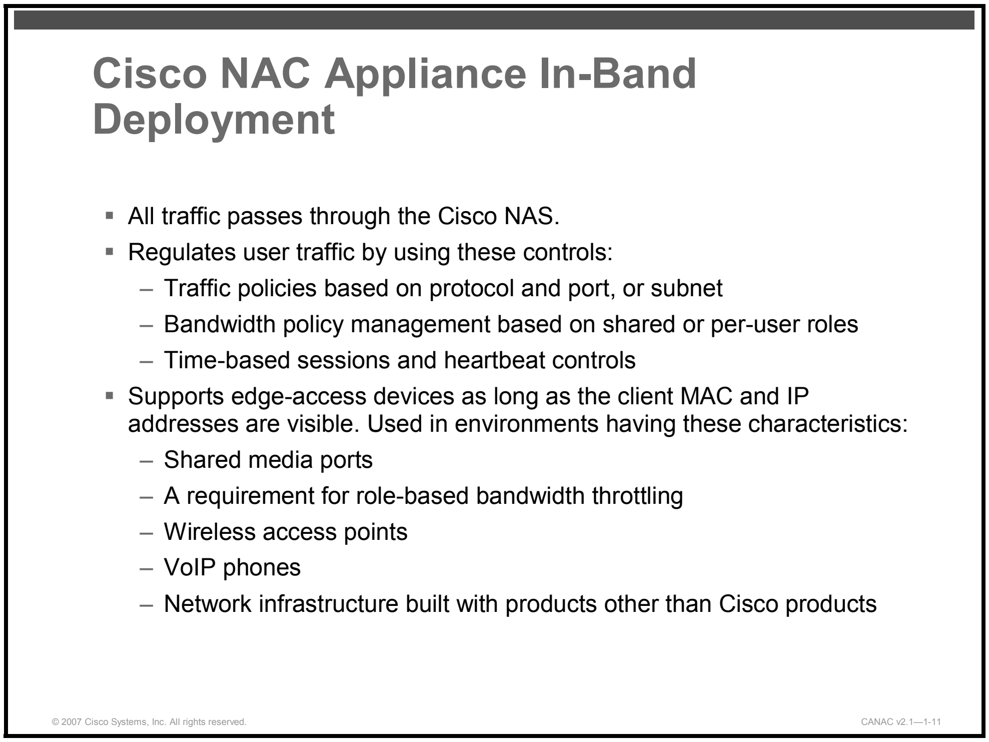


Cisco NAC Appliance Architecture in In-Band Mode

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—1-10

The figure shows a logical diagram of Cisco NAC Appliance in an in-band deployment mode. In the in-band mode, the Cisco NAS sits in line with all traffic. In this configuration, the Cisco NAS can also work with any 802.11 wireless access point, including Cisco Aironet Series access points.



Cisco NAC Appliance In-Band Deployment

- All traffic passes through the Cisco NAS.
- Regulates user traffic by using these controls:
  - Traffic policies based on protocol and port, or subnet
  - Bandwidth policy management based on shared or per-user roles
  - Time-based sessions and heartbeat controls
- Supports edge-access devices as long as the client MAC and IP addresses are visible. Used in environments having these characteristics:
  - Shared media ports
  - A requirement for role-based bandwidth throttling
  - Wireless access points
  - VoIP phones
  - Network infrastructure built with products other than Cisco products

CANAC v2.1—1-11

In this scenario, the Cisco NAS is in-band with user traffic before and following authentication, posture assessment, and remediation. The Cisco NAS must be in-band with traffic for security enforcement. The Cisco NAS securely controls authenticated and unauthenticated user traffic by using traffic policies based on port, protocol, subnet, and bandwidth policies.

The in-band Cisco NAS securely controls all authenticated and unauthenticated user traffic using these methods:

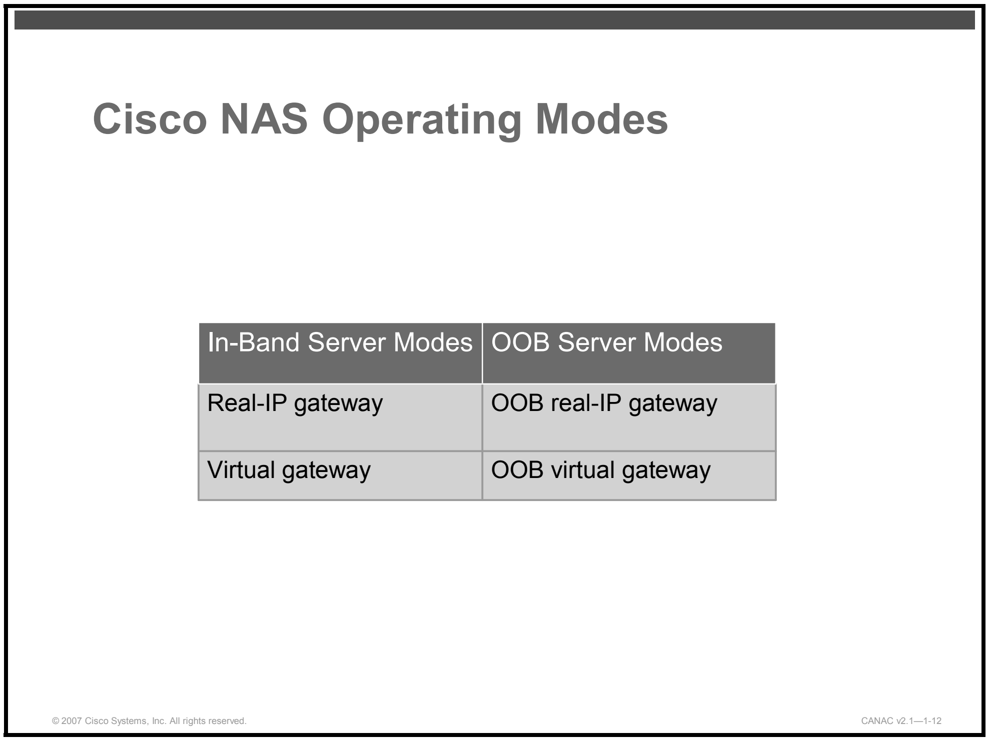
- Managing traffic policies based on protocol and port or subnet
- Providing bandwidth policy management based on shared or per-user roles
- Using time-based sessions and heartbeat controls

In-band deployment supports any edge access device as long as the MAC address and IP address of the client machine are visible to the Cisco NAS. Because the server is in-band with traffic, the in-band deployment mode is ideal for environments with these characteristics:

- Shared media ports
- A requirement for role-based bandwidth throttling
- Wireless access points
- VoIP phones
- Network infrastructure built with products other than Cisco products

Cisco NAS Operating Modes

This topic describes the Cisco NAS operating modes for an in-band and out-of-band deployment.



Cisco NAS Operating Modes

In-Band Server Modes	OOB Server Modes
Real-IP gateway	OOB real-IP gateway
Virtual gateway	OOB virtual gateway

CANAC v2.1—1-12

There are two in-band operating modes:

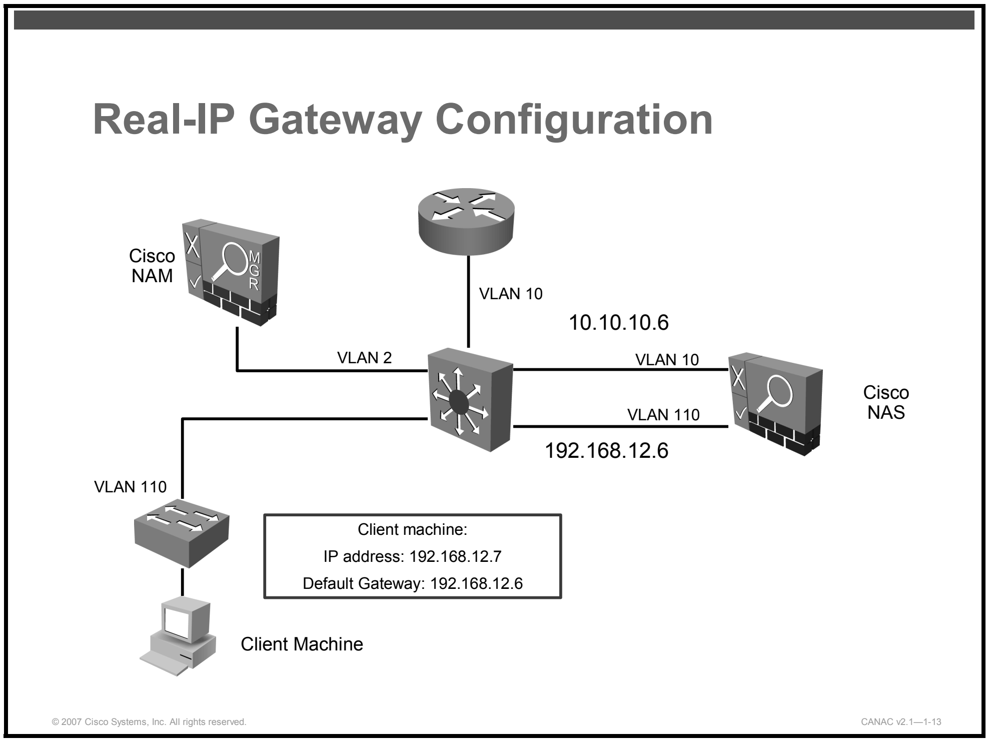
- **Real-IP gateway:** Operates as the default gateway for the untrusted network
- **Virtual gateway:** Operates as a Layer 2 transparent bridge

The out-of-band server types appear in the drop-down menu when you apply an out-of-band-enabled (switch management) license to a Cisco NAC Appliance deployment.

There are two out-of-band operating modes:

- **Out-of-band real-IP gateway:** Operates as a real-IP gateway while traffic is in-band for authentication and certification
- **Out-of-band virtual gateway:** Operates as a virtual gateway while traffic is in-band for authentication and certification

Caution The Cisco NAS can be deployed as a NAT gateway operating as an IP gateway and providing NAT services for the untrusted network. However, a Cisco NAS NAT deployment is only recommended for student labs and demonstrations.



Real-IP Gateway Configuration

Client machine:
IP address: 192.168.12.7
Default Gateway: 192.168.12.6

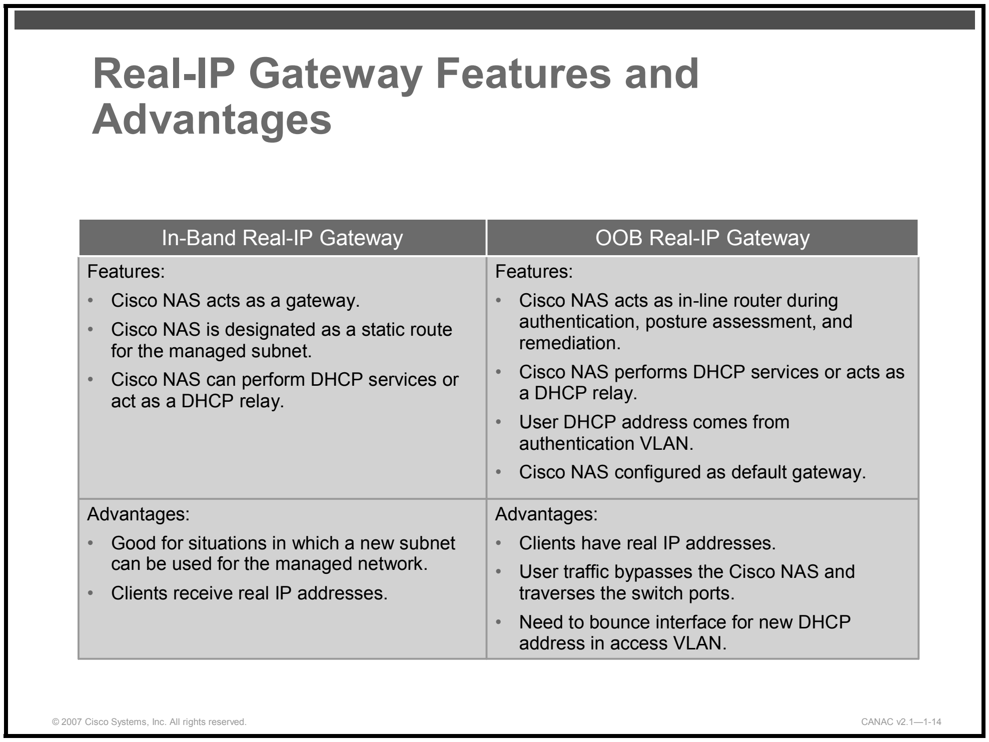
CANAC v2.1—1-13

In the real-IP gateway configuration, the Cisco NAS operates as the default gateway for untrusted (managed) network clients. All traffic between the untrusted and trusted networks is routed through the Cisco NAS. The Cisco NAS applies the IP filtering rules, access policies, and any other traffic-handling mechanisms that you configure.

When using the Cisco NAS as a real-IP gateway, you must specify the IP addresses of the two Cisco NAS interfaces: one for the trusted side of the network and one for the untrusted side of the network. The two addresses should be on different subnets. The Cisco NAS can manage one or more subnets when the untrusted interface acts as a gateway for the managed subnets.

The Cisco NAS does not advertise routes. Instead, static routes must be added to the next-hop router to indicate that traffic to the managed subnets must be relayed to the Cisco NAS trusted interface.

Additionally, when the Cisco NAS is in real-IP gateway mode, it can act as a DHCP server or relay. With DHCP functionality enabled, the Cisco NAS provides the appropriate gateway information (that is, the Cisco NAS untrusted interface IP address) to the clients. If the Cisco NAS is working as a DHCP relay, then the DHCP server must be configured to provide the managed clients with the appropriate gateway information (that is, the Cisco NAS untrusted interface IP address).

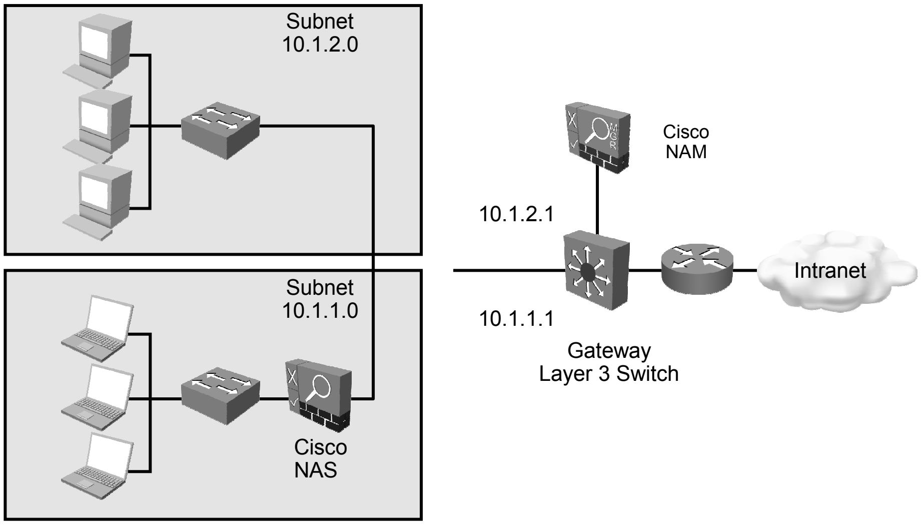


Real-IP Gateway Features and Advantages

In-Band Real-IP Gateway	OOB Real-IP Gateway
Features: • Cisco NAS acts as a gateway. • Cisco NAS is designated as a static route for the managed subnet. • Cisco NAS can perform DHCP services or act as a DHCP relay.	Features: • Cisco NAS acts as in-line router during authentication, posture assessment, and remediation. • Cisco NAS performs DHCP services or acts as a DHCP relay. • User DHCP address comes from authentication VLAN. • Cisco NAS configured as default gateway.
Advantages: • Good for situations in which a new subnet can be used for the managed network. • Clients receive real IP addresses.	Advantages: • Clients have real IP addresses. • User traffic bypasses the Cisco NAS and traverses the switch ports. • Need to bounce interface for new DHCP address in access VLAN.

The figure shows the features and advantages of deploying the Cisco NAS as an in-band real-IP gateway and as an out-of-band real-IP gateway.

Virtual Gateway Configuration



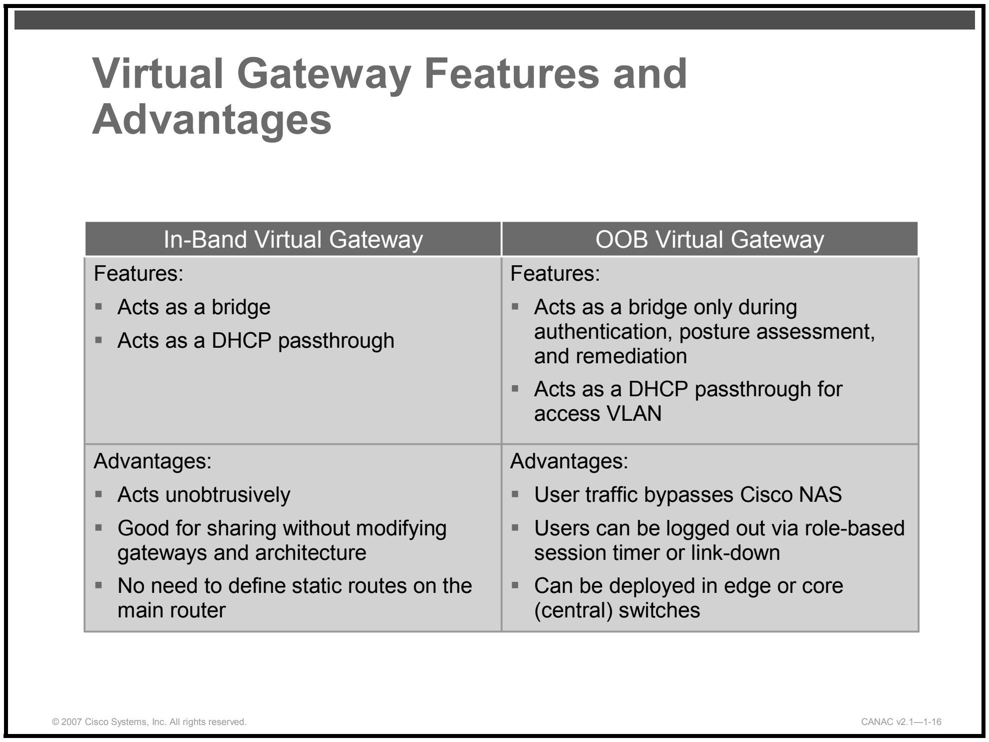
CANAC v2.1—1-15

In the virtual gateway configuration, the Cisco NAS operates as a standard Ethernet bridge.

For example, suppose that a network has two subnets, 10.1.1.0 and 10.1.2.0. Only 10.1.1.0 is a managed subnet. The other subnet is a trusted network. Because this is a virtual gateway configuration, the gateway of 10.1.1.1 cannot be replaced, as it can when the Cisco NAS is deployed in the real-IP gateway configuration. The figure shows the Cisco NAS deployed as a virtual gateway only in the 10.1.1.0 network.

Note these points regarding virtual gateway configuration:

- The Cisco NAS should be configured for DHCP forwarding.
- The Cisco NAS and the Cisco NAM must be on different subnets.
- eth0 and eth1 of the Cisco NAS can have the same IP address.
- All end devices in the bridged subnet in virtual gateway mode must be on the untrusted side of the Cisco NAS.
- If you are trunking subnets across the virtual gateway, the Cisco NAM must not be on the trunked subnet on the trusted network.



Virtual Gateway Features and Advantages

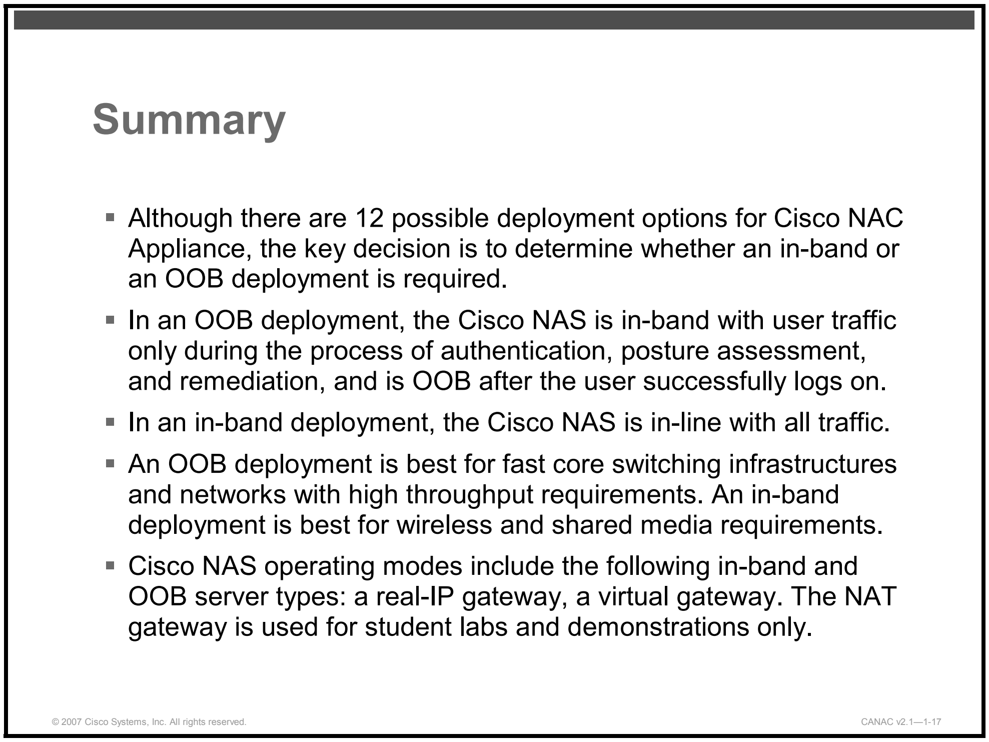
In-Band Virtual Gateway	OOB Virtual Gateway
Features: ▪ Acts as a bridge ▪ Acts as a DHCP passthrough	Features: ▪ Acts as a bridge only during authentication, posture assessment, and remediation ▪ Acts as a DHCP passthrough for access VLAN
Advantages: ▪ Acts unobtrusively ▪ Good for sharing without modifying gateways and architecture ▪ No need to define static routes on the main router	Advantages: ▪ User traffic bypasses Cisco NAS ▪ Users can be logged out via role-based session timer or link-down ▪ Can be deployed in edge or core (central) switches

CANAC v2.1—1-16

The figure shows the features and advantages of deploying the Cisco NAS as an in-band virtual gateway and as an out-of-band virtual gateway.

Summary

This topic summarizes the key points that were discussed in this lesson.

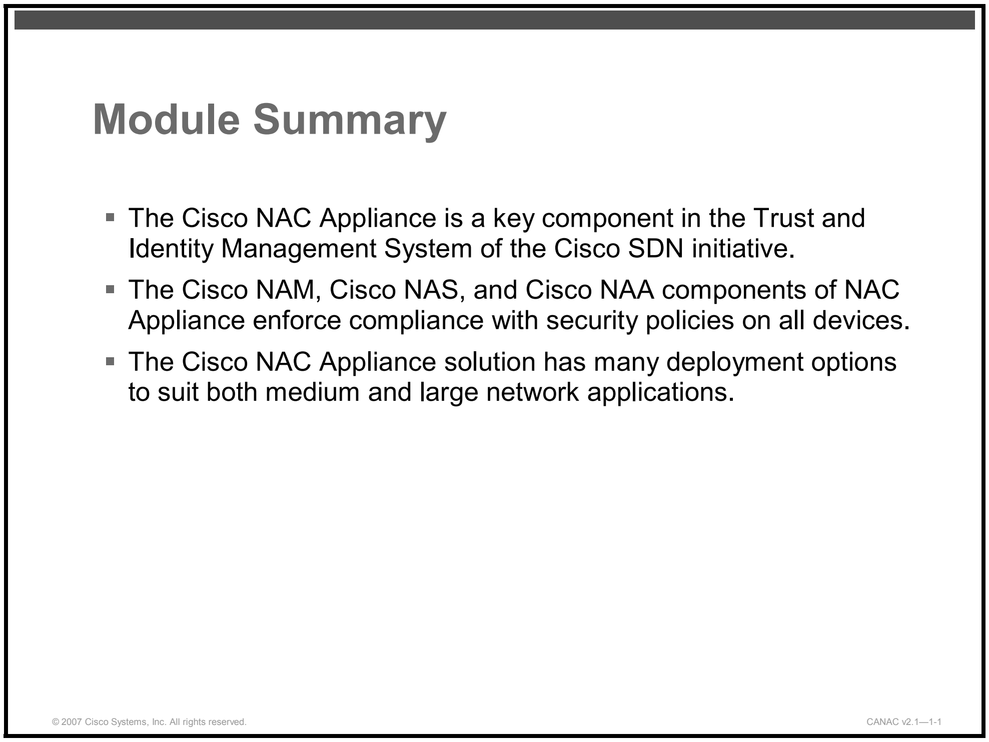


Summary

- Although there are 12 possible deployment options for Cisco NAC Appliance, the key decision is to determine whether an in-band or an OOB deployment is required.
- In an OOB deployment, the Cisco NAS is in-band with user traffic only during the process of authentication, posture assessment, and remediation, and is OOB after the user successfully logs on.
- In an in-band deployment, the Cisco NAS is in-line with all traffic.
- An OOB deployment is best for fast core switching infrastructures and networks with high throughput requirements. An in-band deployment is best for wireless and shared media requirements.
- Cisco NAS operating modes include the following in-band and OOB server types: a real-IP gateway, a virtual gateway. The NAT gateway is used for student labs and demonstrations only.

Module Summary

This topic summarizes the key points that were discussed in this module.



Module Summary

- The Cisco NAC Appliance is a key component in the Trust and Identity Management System of the Cisco SDN initiative.
- The Cisco NAM, Cisco NAS, and Cisco NAA components of NAC Appliance enforce compliance with security policies on all devices.
- The Cisco NAC Appliance solution has many deployment options to suit both medium and large network applications.

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

This module describes the Network Admission Control (NAC) Appliance solution as an integral part of the NAC framework, which provides a comprehensive defense against viruses, worms, and denial-of-service attacks. The module describes the Cisco Self-Defending Network (SDN) initiative and describes where the NAC Appliance solution fits into the SDN. In addition, the module describes the components of a NAC Appliance solution and how these components work together to support corporate security policies. The module explains how deployment modes (in-band, out-of-band, central, and edge deployment) combine with the three Cisco NAS operating modes to provide the breadth of options that allow you to protect your network against specified threats. The GUI web-based administration console, which makes it easy to configure the options that you need to implement a NAC Appliance solution, is also described.

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *Cisco NAC Appliance (Cisco Clean Assess) Introduction*. http://www.cisco.com/en/US/products/ps6128/index.html.
- Cisco Systems, Inc. *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*. http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.
- Cisco Systems, Inc. *Cisco NAC Appliance—Clean Access Server Installation and Administration Guide*. http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) What is the new concept for defending corporate networks? (Source: Introducing Cisco Self-Defending Networks)

A) proactive defense
B) reactive defense
C) adaptive defense

Q2) What does the Cisco security ecosystem consist of? (Source: Introducing Cisco Self-Defending Networks)

A) security products, technologies, and services
B) solutions, systems, and networks
C) self-defending networks, infection isolation, and worm mitigation

Q3) What is Phase II of the SDN initiative? (Source: Introducing Cisco Self-Defending Networks)

A) integrated security
B) collaborative security
C) Adaptive Threat Defense

Q4) What are two essential functions of the NAC Appliance solution? (Choose two.) (Source: Introducing Cisco Self-Defending Networks)

A) recognizing users
B) evaluating users
C) evaluating computers
D) enforcing security collaboration
E) promoting ATD

Q5) What is the fourth step to configure a NAC Appliance solution? (Source: Introducing Cisco NAC Appliance)

A) Configure an authentication service.
B) Configure user roles.
C) Configure network-based scanning requirements.
D) Configure agent-based scanning requirements.

Q6) Which environment is an in-band implementation of the NAC Appliance solution suitable for? (Source: Introducing Cisco NAC Appliance)

A) VLAN-based quarantine
B) wireless
C) multigigabit networks

Q7) How does endpoint protection work? (Source: Introducing Cisco NAC Appliance)

A) by using the new behavior-based technology available with CSA
B) by providing network access only to endpoint devices that fully comply with established security policies
C) by focusing on automating key elements of the infection response process

Q8) Which three components are required for a NAC appliance? (Choose three.) (Source: Introducing Cisco NAC Appliance)

A) NAC-enabled Cisco routers and switches
B) Cisco NAS
C) Cisco NAM
D) Cisco switches
E) Cisco VPN 3000 Concentrators
F) Cisco Integrated Service Router
G) Cisco Secure ACS

Q9) What is a key difference between the NAC framework and NAC Appliance? (Source: Introducing Cisco NAC Appliance)

A) The NAC Appliance is an industry-wide initiative led by Cisco, and the NAC framework is a natural fit for medium-scaled networks that require a self-contained, turnkey solution.
B) The NAC framework is an industry-wide initiative led by Cisco, and the NAC Appliance is a natural fit for medium-scaled networks that require a self-contained, turnkey solution.
C) The NAC framework is designed for service providers that need simplified and integrated tracking of operating system and antivirus patches, and the NAC Appliance is designed for vulnerability protection in high-performance network environments with diverse endpoints.

Q10) What is the role of the Cisco NAM in the Cisco NAC Appliance solution? (Source: Introducing Cisco NAC Appliance)

A) The Cisco NAM acts as an administration server for Cisco NAC Appliance deployment managing Cisco NASs remotely, globally, or individually.
B) The Cisco NAM acts as a gateway server and enforcement engine between the untrusted (managed) network and the trusted network.
C) The Cisco NAM acts as a required remediation agent of Cisco NAC Appliance that checks applications, files, services, or registry keys on client machines.

Q11) Which two types of features does Cisco NAC Appliance offer for local users? (Choose two.) (Source: Introducing Cisco NAC Appliance)

A) IPsec VPNs
B) site-to-site VPNs
C) 802.1q trunking
D) Layer 4 Transport Protocol version 2
E) Layer 3 multihop

Q12) What is one difference between an in-band and an out-of-band Cisco NAC Appliance deployment? (Source: Introducing In-Band and Out-of-Band Deployment Options)

A) An in-band deployment is designed to support wireless and shared media and an out-of-band deployment is designed to support fast core-switching infrastructures.
B) An in-band deployment uses a Cisco NAS with a quarantine VLAN for NAC enforcement and an out-of-band deployment uses only a Cisco NAS for NAC enforcement.
C) An in-band deployment uses VLANs for quarantine and an out-of-band deployment uses ACLs for quarantine.

Q13) What is a key operational feature of a Cisco NAS when it is deployed in-band as a real-IP gateway? (Source: Introducing In-Band and Out-of-Band Deployment Options)

A) The Cisco NAS operates as the default gateway for the trusted network.
B) The Cisco NAS operates as the default gateway for the untrusted network.
C) The Cisco NAS operates as the default gateway, but only for in-band traffic during authentication and certification.

Q14) Which page is displayed when a user successfully logs into the Cisco NAM? (Source: Introducing Cisco NAC Appliance)

A) Monitoring > Summary page
B) Monitoring > User page
C) Administration > Summary page

Q15) When the Cisco NAS is configured to operate as an in-band real-IP gateway, which three of these statements apply? (Choose three.) (Source: Introducing In-Band and Out-of-Band Deployment Options)

A) The Cisco NAS untrusted interface acts as a gateway for the managed subnets.
B) The Cisco NAS operates as a standard Ethernet bridge, but with the added functionality provided by the IP filter and IPsec module.
C) The Cisco NAS performs the translation between the private and public addresses as traffic is routed between the untrusted (managed) and external network.
D) This configuration is typically used when the untrusted network already has a gateway and you do not want to alter the existing configuration.
E) The IP addresses of the Cisco NAS trusted and untrusted interfaces should be on different subnets.
F) Static routes must be added to the next-hop router to relay traffic destined for the managed subnets to the Cisco NAS trusted interface.
G) The Cisco NAS should be configured for DHCP forwarding.

Q16) Which Cisco NAC Appliance deployment should be used when all network traffic to or from each client must go through the Cisco NAS? (Source: Introducing In-Band and Out-of-Band Deployment Options)

A) edge deployment
B) in-band deployment
C) central deployment
D) out-of-band deployment

Q17) Which Cisco NAC Appliance deployment should be used if a client wants to reduce the number of Cisco NASs to deploy and wants to facilitate management and scalability? (Source: Introducing In-Band and Out-of-Band Deployment Options)

A) bridged deployment
B) edge deployment
C) core deployment
D) central deployment

Q18) How are unsecured client devices kept from logging onto the network in an out-of-band deployment? (Source: Introducing In-Band and Out-of-Band Deployment Options)

A) The Cisco NAS securely controls authenticated and unauthenticated client devices by using traffic policies based on port, protocol, subnet, and bandwidth policies.
B) The Cisco NAM blocks device access at the port layer and places these devices in a quarantine zone until they successfully pass inspection.
C) The Cisco NAS blocks device access at the port layer and places these devices in a quarantine zone until they successfully pass inspection.

Q19) Which type of gateway is in effect when the Cisco NAS operates as the default gateway for the untrusted network? (Source: Introducing In-Band and Out-of-Band Deployment Options)

A) real-IP gateway
B) virtual gateway
C) NAT gateway

Module Self-Check Answer Key

Q1)	C
Q2)	A
Q3)	B
Q4)	A, C
Q5)	C
Q6)	B
Q7)	A
Q8)	B, C, D
Q9)	B
Q10)	A
Q11)	C, E
Q12)	A
Q13)	B
Q14)	A
Q15)	A,E,F
Q16)	B
Q17)	D
Q18)	C
Q19)	A

Module 2

Cisco NAC Appliance Common Elements Configuration

Overview

You can deploy Cisco NAC Appliance on a variety of network topologies, and it is often difficult, therefore, to determine which elements of a configuration to complete. This module describes how to configure the common elements in a Cisco NAC Appliance solution. Common elements include the procedures for configuring user management, configuring external authentication with different authentication providers, and configuring the Cisco NAC Appliance Server (Cisco NAS) for a DHCP-enabled network.

Module Objectives

Upon completing this module, you will be able to configure the common elements of a Cisco NAC Appliance solution. This ability includes being able to meet these objectives:

- Configure user roles for a customer network scenario using the Cisco NAM
- Describe how to configure external authentication for users in a network using the Cisco NAM
- Describe how to configure the Cisco NAS for a DHCP-enabled network

Lesson 1

Configuring User Roles

Overview

In any security system, managing user roles is a key skill. This lesson describes the user roles that exist in a Cisco Network Admission Control (NAC) Appliance solution and details how to create, modify, and delete user roles. This lesson also describes how to configure traffic control policies for user roles and discusses local users and how to set up a local user account for testing purposes.

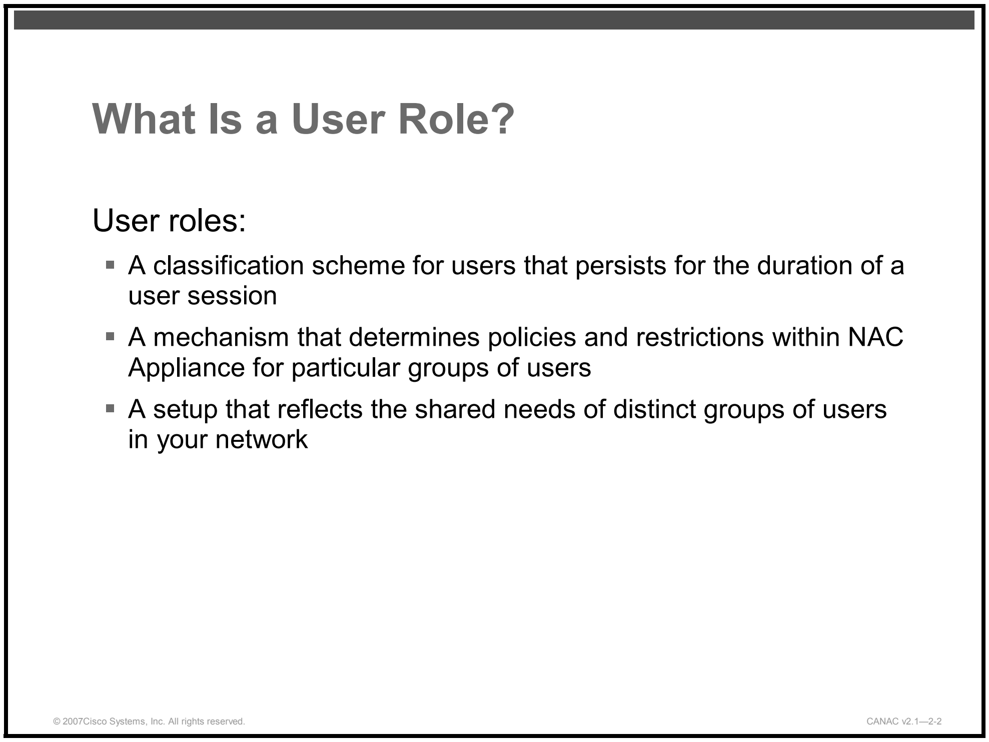
Objectives

Upon completing this lesson, you will be able to configure user roles in a NAC Appliance solution for a customer network scenario using the Cisco NAC Appliance Manager (Cisco NAM). This ability includes being able to meet these objectives:

- Describe user roles in Cisco NAC Appliance
- Describe how to manage user roles
- Explain traffic control policies for user roles
- Describe how to configure traffic control policies for a user role
- Describe how to create a local user account
- Describe how to configure user session timeouts for user roles
- Describe how to configure guest access for visitors or temporary users in a Cisco NAC Appliance network

What Is a User Role?

This topic describes user roles in a Cisco NAC Appliance solution.



What Is a User Role?

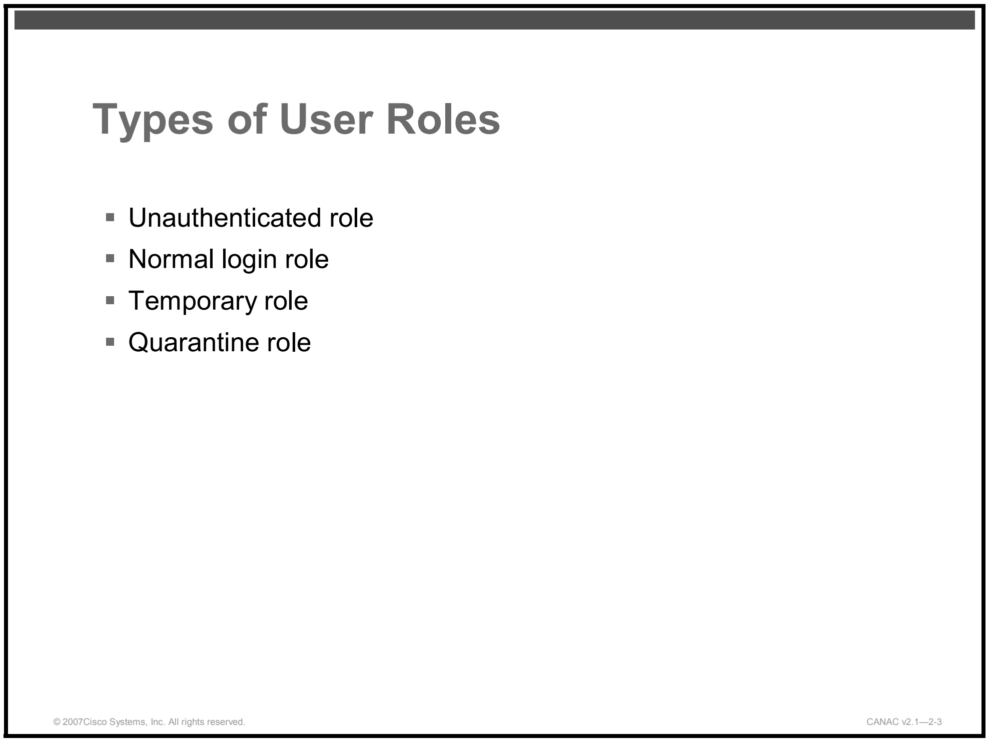
User roles:

- A classification scheme for users that persists for the duration of a user session
- A mechanism that determines policies and restrictions within NAC Appliance for particular groups of users
- A setup that reflects the shared needs of distinct groups of users in your network

User roles are integral to how Cisco NAC Appliance functions and can be described as follows:

- A classification scheme for users that persists for the duration of a user session
- A mechanism that determines traffic policies, bandwidth restrictions, session duration, vulnerability assessment, and other policies within Cisco NAC Appliance for particular groups of users

In general, you should set user roles to reflect the shared needs of distinct groups of users in your network. Before creating roles, consider how you want to allocate privileges in your network, apply traffic control policies, or group types of client devices. Roles can be based on existing groups within your organization, such as students, faculty, and staff.



Types of User Roles

- Unauthenticated role
- Normal login role
- Temporary role
- Quarantine role

The system places a user in a role when the user attempts to log in. These are the four types of user roles in the Cisco NAC Appliance solution:

- **Unauthenticated role:** There is only one unauthenticated role and it is the system default role. If a configured normal login role is deleted, users in that role are reassigned to the unauthenticated role. You can configure traffic and other policies for the unauthenticated role, but the role itself cannot be edited or removed from the system. Users on the untrusted (managed) side of the Cisco NAC Appliance Server (NAS) are in the unauthenticated role prior to the initial web login or Cisco NAC Appliance Agent (NAA) login. When using web login or network scanning only, users remain in the unauthenticated role until clients pass scanning and are transferred to a normal login role or fail scanning and are either blocked or transferred to the quarantine role.
- **Normal login role**: There can be multiple normal login roles in the system. The default unauthenticated role is a normal login role. If a normal login role is deleted, users in that role are reassigned to the unauthenticated role. A user is put into a normal login role after a successful login. You can configure normal login roles in order to associate users with these characteristics:
  - — **Network access traffic control policy:** Controls which parts of the network and which application ports that users can access
  - — **Virtual private network (VPN), IP security (IPsec) key, and roaming policy:** Dictates how to group and manage remote or wireless users
  - — **VLAN ID:** Used for in-band users so that traffic destined to the trusted network is retagged to differentiate priority to the upstream router; used for out-of-band users using role-based configuration where the access VLAN ID is set for a given role
  - — **NAC Appliance network scanning plug-ins:** Determine which port scanning to perform
  - — **Cisco NAA requirements:** Dictate what software that users with particular operating systems must have

— **End-user HTML page or pages displayed after a successful or unsuccessful login:** Indicates which pages and what information to show users in various subnets, VLANs, or user roles

You can create different login roles in a deployment; for example, for students, faculty, and staff, or for engineering, human resources, and sales. You can create and assign normal login roles for users based on several factors such as these:

— **Client device:** The MAC address or subnet of a client device.

— **Local user attributes:** A local user is one that is authenticated by Cisco NAC Appliance rather than by an external authentication mechanism.

— **External authentication provider attributes:** For users validated by an external authentication source, the role assigned can be based on the untrusted network VLAN of the user. For Lightweight Directory Access Protocol (LDAP) and RADIUS authentication servers, the role assigned can also be based on user attributes provided by the authentication source. You can use external authentication provider attributes to map users to multiple roles within Cisco NAC Appliance. If no mapping rules are specified, users are assigned to the default role designated for their particular authentication server after login.

Note The default unauthenticated role is a normal login role. If a normal login role is deleted, users in that role are reassigned to the unauthenticated role.

These two roles are associated with the use of the Cisco NAA:

- **Temporary role:** The temporary login role is assigned by the Cisco NAA to allow a user to download and install required packages. The user is denied access to the network until Cisco NAA requirements are met.

  There is only one Cisco NAA temporary role in the system. This role is in effect only when the user is required to use Cisco NAA to log in and pass Cisco NAC Appliance requirements. The Cisco NAA temporary role is assigned to users for these time periods:

  — From the time of the initial login attempt until successful network access. When the client system meets Cisco NAA requirements and no vulnerabilities are found after a network scan, the user transfers from the Cisco NAA temporary role into the normal login role.

  — From the time of the initial login attempt until Cisco NAA requirements are met. The user has the amount of time configured in the session timer for the role to download and install required packages. If the user cancels or times out, the user is removed from the Cisco NAA temporary role and must restart the login process. If the user downloads requirements within the time allotted, the user stays in the Cisco NAA temporary role and repeats network scanning.

  — From the time of the initial login attempt until network scanning finds vulnerabilities on the user system. If the client system meets Cisco NAA requirements but is found to have vulnerabilities during network scanning, the user is transferred from the Cisco NAA temporary role into the quarantine role.

- **Quarantine role:** With network scanning enabled, the purpose of the Cisco NAC Appliance quarantine role is to allow the user limited network access to resources needed to fix vulnerabilities that exist on the user system. The user is prevented from normal login role access to the network until all vulnerabilities are fixed. There can be one or multiple quarantine roles in the system. A user is put in a quarantine role if either of these two situations exists:
  - The user attempts to log in using the web login page but Cisco NAC Appliance network scanning finds a vulnerability on the user system.
  - The user logs in using Cisco NAA and meets Cisco NAA requirements, but the Cisco NAC Appliance network scanning finds a vulnerability on the user system.

The user has the amount of time configured in the session timer for the role to access resources and fix vulnerabilities. If the user cancels or times out, the user is logged out of the quarantine role and must restart the login process. At the next login attempt, the client again goes through Cisco NAC Appliance network scanning.

When the user fixes vulnerabilities within the time allotted, and if Cisco NAA is used to log in, the user can go through network scanning again during the same session. If web login is used, the user must log out or time out and then log in again for the second network scanning to occur.

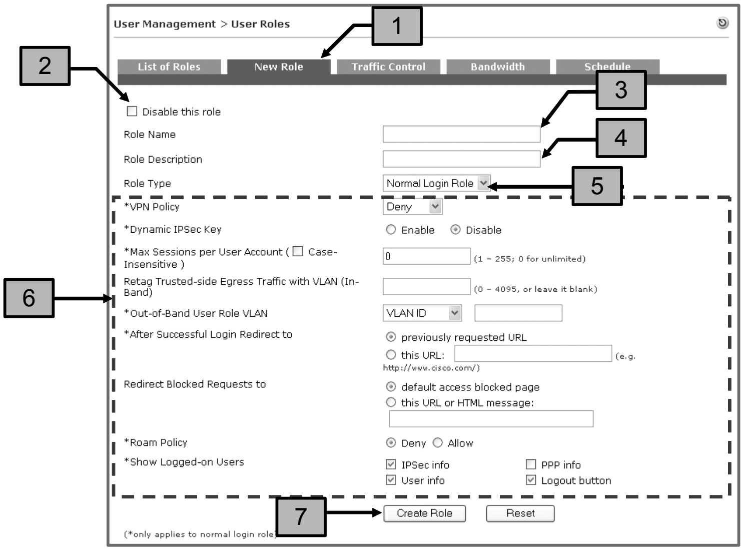
Only when the user has met requirements and fixed vulnerabilities is the user granted network access in the corresponding normal login role. You can map all normal login roles to a single quarantine role, or you can create and customize different quarantine roles. For example, multiple quarantine roles can be used if different resources are required to fix vulnerabilities for particular operating systems. In both cases, a normal login role can be mapped to only one quarantine role.

Note When using a web login page, the user should be careful not to close the logout page. If the user cannot log out but attempts to log in again before the session times out, the user is still considered to be in the original quarantine role and is not redirected to the login page.

Managing User Roles

This topic describes how to manage user roles.

Creating a New User Role



User Management > User Roles

☐ Disable this role

Role Name

Role Description

Role Type: Normal Login Role

*VPN Policy: Deny

*Dynamic IPSec Key: ○ Enable ● Disable

*Max Sessions per User Account (☐ Case-Insensitive): 0 (1 – 255; 0 for unlimited)

Retag Trusted-side Egress Traffic with VLAN (In-Band): (0 – 4095, or leave it blank)

*Out-of-Band User Role VLAN: VLAN ID

*After Successful Login Redirect to: ● previously requested URL ○ this URL: (e.g. http://www.cisco.com/)

Redirect Blocked Requests to: ● default access blocked page ○ this URL or HTML message:

*Roam Policy: ● Deny ○ Allow

*Show Logged-on Users: ☑ IPSec info ☐ PPP info ☑ User info ☑ Logout button

Create Role   Reset

(*only applies to normal login role)

CANAC v2.1—2-4

The temporary role and one quarantine role already exist in the system and only need to be configured. However, normal login roles and any additional quarantine roles must be created. When you create a new role, you can associate it with traffic policies and other properties that you customize in the web administration console for your environment.

Note	For new roles, you must add traffic policies to allow traffic from the untrusted network to flow to the trusted network.

To add a new role, complete these steps:

Step 1 Choose **User Management > User Roles** and click the **New Role** tab. The New Role form appears.

Step 2 If you want the role to be active immediately, leave the Disable this role check box cleared.

Step 3 Enter a unique name for the role in the Role Name field.

Step 4 Enter an optional Role Description.

Step 5 From the Role Type drop-down menu, choose either **Normal Login Role** or **Quarantine Role.**

Note A system quarantine role already exists and can be configured. However, the New Role form allows you to add quarantine roles if needed.

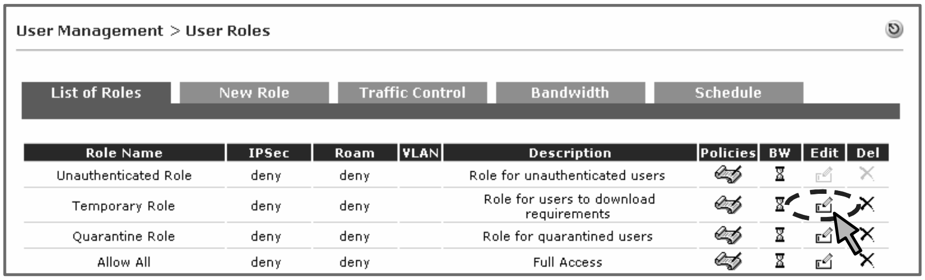
Step 6 Configure any other settings desired for the role. For example, you can configure VPN and VLAN settings and roaming policies.

Step 7 When finished, click **Create Role**. The new role appears in the List of Roles tab. To restore default properties on the form, click **Reset**.

Note For a complete description of all the settings in the New Role form, refer to the Role Properties section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

If you are creating a role for testing purposes, the next step is to create a local user to associate to the role.

Modifying a User Role



Role Name	IPSec	Roam	VLAN	Description	Policies	BW	Edit	Del
Unauthenticated Role	deny	deny		Role for unauthenticated users		⌛	✎	✕
Temporary Role	deny	deny		Role for users to download requirements		⌛	✎	✕
Quarantine Role	deny	deny		Role for quarantined users		⌛	✎	✕
Allow All	deny	deny		Full Access		⌛	✎	✕

CANAC v2.1—2-5

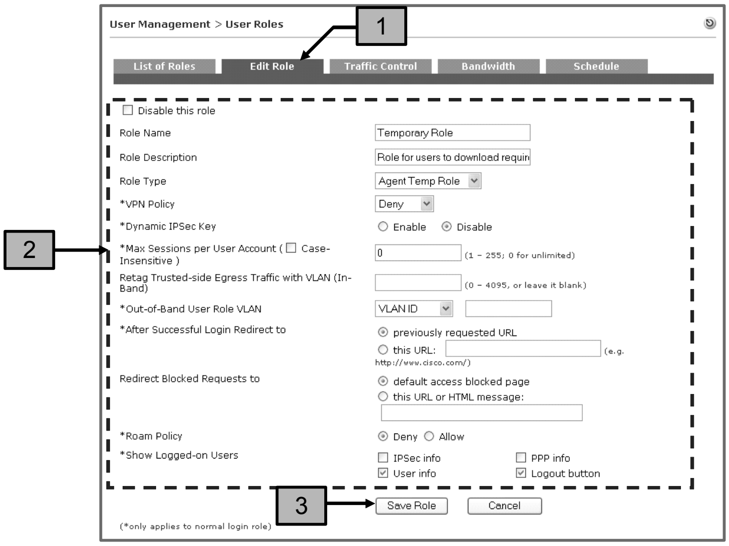
From the User Management > User Roles > List of Roles tab, you can edit any normal login role that you have created or you can configure system default roles, such as the unauthenticated role and the temporary and quarantine roles.

You can perform these operations from the List of Roles tab:

- Set traffic filter policies for the role by clicking the **Policies** button.
- Set upstream and downstream bandwidth restrictions by role by clicking the **BW** (bandwidth) button.
- Modify role properties by clicking the **Edit** button.
- Delete the role from the system by clicking the **Delete** button.
- Specify a network access schedule for the role by selecting the role and clicking the **Schedule** tab.

Note Traffic and bandwidth policies can be configured for the unauthenticated role, but this system default role cannot be edited or deleted.

Editing Role Properties



□ Disable this role

Role Name	Temporary Role
Role Description	Role for users to download requir
Role Type	Agent Temp Role
*VPN Policy	Deny
*Dynamic IPSec Key	○ Enable ● Disable
*Max Sessions per User Account (□ Case-Insensitive)	0 (1 – 255; 0 for unlimited)
Retag Trusted-side Egress Traffic with VLAN (In-Band)	(0 – 4095, or leave it blank)
*Out-of-Band User Role VLAN	VLAN ID
*After Successful Login Redirect to	● previously requested URL ○ this URL: (e.g. http://www.cisco.com/)
Redirect Blocked Requests to	● default access blocked page ○ this URL or HTML message:
*Roam Policy	● Deny ○ Allow
*Show Logged-on Users	□ IPSec info □ PPP info ☑ User info ☑ Logout button

(*only applies to normal login role)

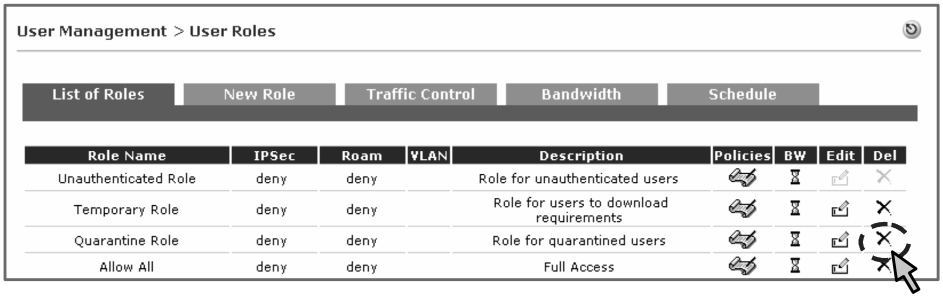
To edit a role, complete these steps:

Step 1 Choose **User Management > User Roles > List of Roles**. Click the **Edit** button next to the role you want to edit to access the Edit Role form.

Step 2 Modify role settings as desired. The example shows the default settings for the Cisco NAA temporary role.

Step 3 Click the **Save Role** button.

Deleting a Role



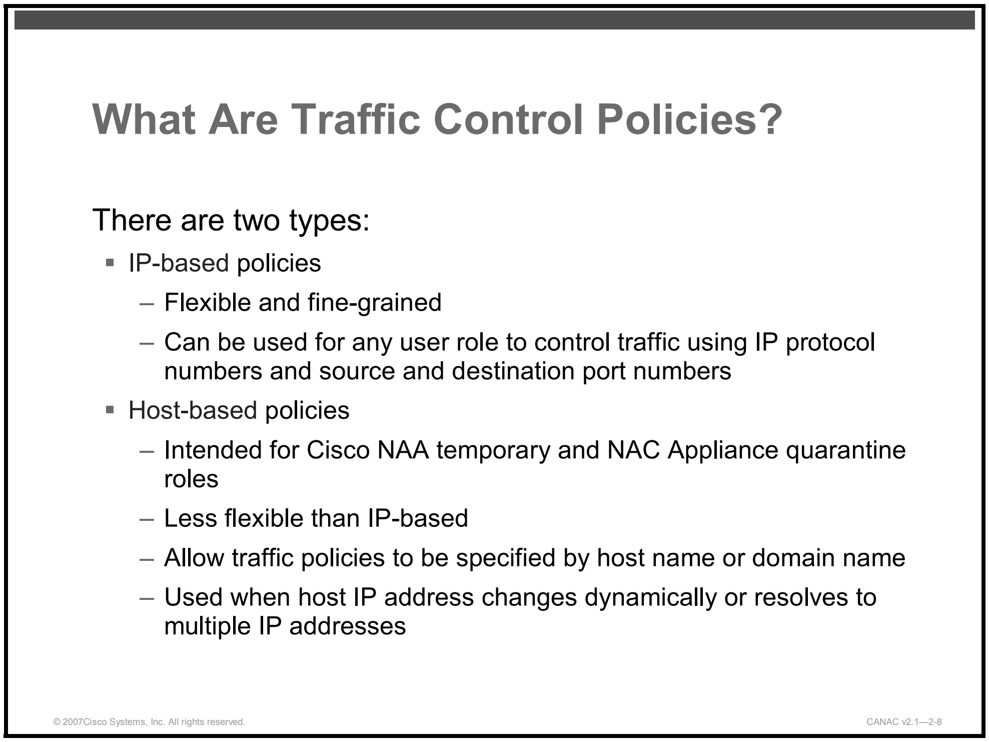
Role Name	IPSec	Roam	VLAN	Description	Policies	BW	Edit	Del
Unauthenticated Role	deny	deny		Role for unauthenticated users		⌛	✎	✕
Temporary Role	deny	deny		Role for users to download requirements		⌛	✎	✕
Quarantine Role	deny	deny		Role for quarantined users		⌛	✎	✕
Allow All	deny	deny		Full Access		⌛	✎	✕

To delete a role, choose **User Management > User Roles** and click the **List of Roles** tab. Click the **Delete** button next to the role that you want to delete.

Users actively connected to the network in the deleted role will be unable to use the network. However, their connection will remain active. Such users should be logged off the network manually by clicking the **Kick User** button next to the user in the Monitoring > Online Users > View Online Users page. The users are indicated in the online user page by a value of "Invalid**"** in the Role column. These users will be reassigned to the unauthenticated role as long as they retain their current client machine configuration.

Defining Traffic Policies for User Roles

This topic describes traffic control policies for user roles.



What Are Traffic Control Policies?

There are two types:

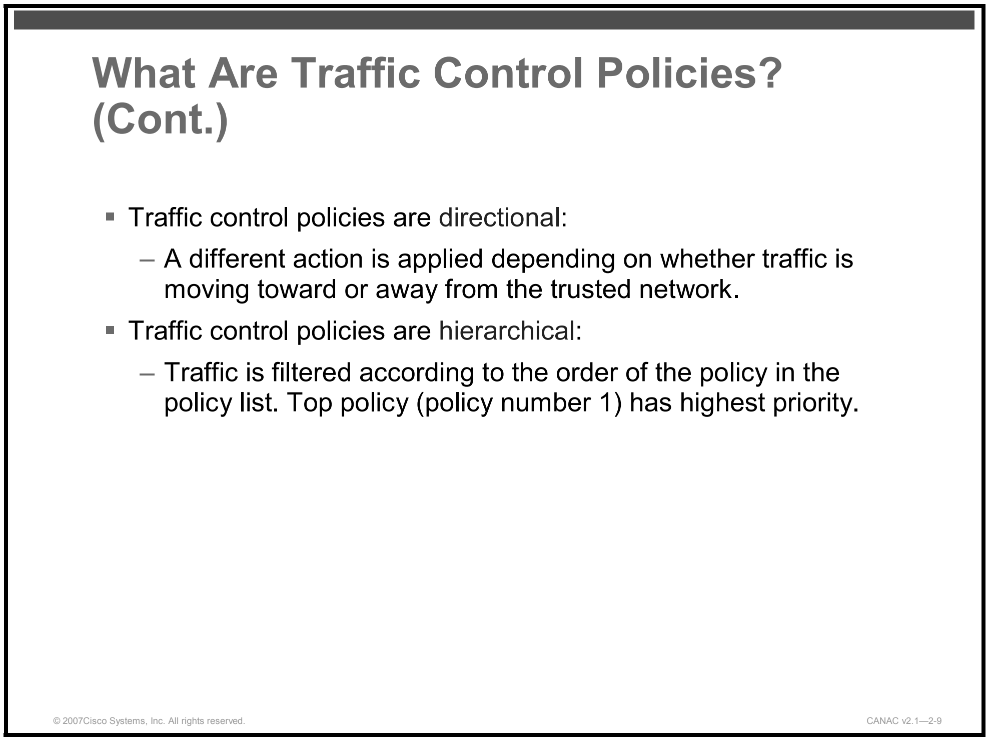
- IP-based policies
  - Flexible and fine-grained
  - Can be used for any user role to control traffic using IP protocol numbers and source and destination port numbers
- Host-based policies
  - Intended for Cisco NAA temporary and NAC Appliance quarantine roles
  - Less flexible than IP-based
  - Allow traffic policies to be specified by host name or domain name
  - Used when host IP address changes dynamically or resolves to multiple IP addresses

© 2007Cisco Systems, Inc. All rights reserved. CANAC v2.1—2-8

Traffic control policies let you control which network resources can be accessed and which users can access each resource. Traffic control policies are configured by user role and must be configured for the Cisco NAA temporary role and NAC Appliance quarantine roles.

Cisco NAC Appliance offers these two types of traffic policies:

- **IP-based policies:** These policies are fine-grained and flexible and can stop traffic in several ways. IP-based policies are intended for any role and allow you to specify IP protocol numbers as well as source and destination port numbers. For example, you can create an IP-based policy to pass IPsec traffic to a particular host while denying all other traffic.
- **Host-based policies:** These policies are less flexible than IP-based policies but have the advantage of allowing traffic policies to be specified by host name or domain name when a host has multiple or dynamic IP addresses. Host-based policies allow wildcards to be specified as part of a host name (for example, *.windowsupdate.microsoft.com). This feature is intended to ease the specification of traffic policies for the Cisco NAA temporary role and the Cisco NAC Appliance quarantine roles after NAC Appliance scans clients for requirements or vulnerabilities. Configuring Domain Name System (DNS) addresses for each Cisco NAC Appliance role facilitates client access to Windows or antivirus update sites that enable clients to fix their systems when requirements are not met or vulnerabilities are found.



What Are Traffic Control Policies? (Cont.)

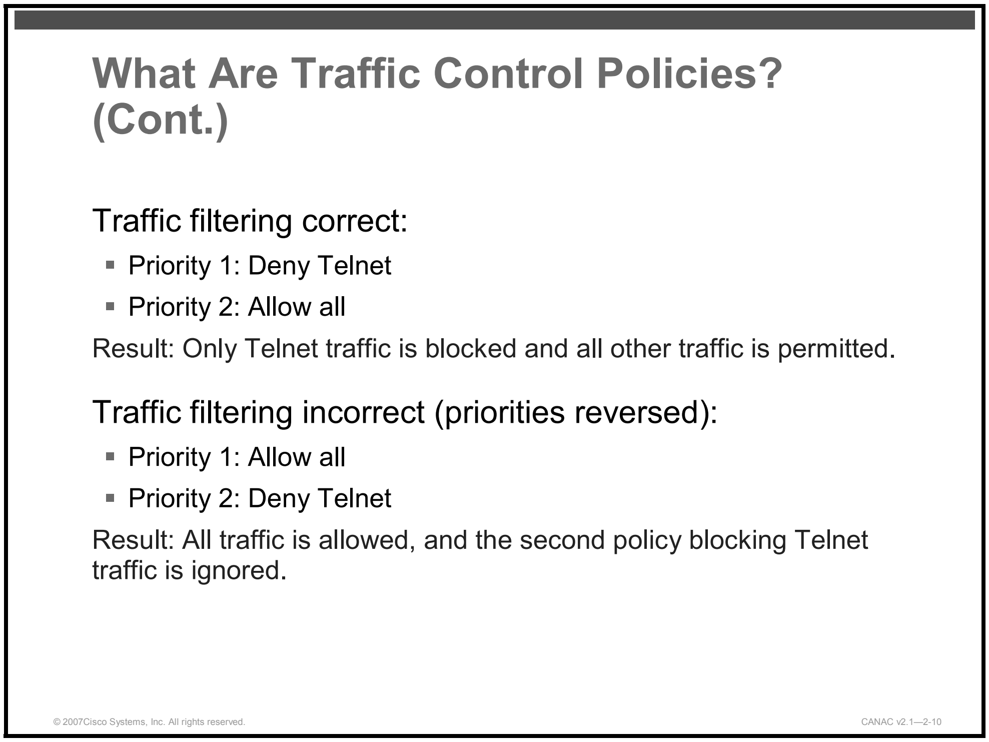
- Traffic control policies are directional:
  - A different action is applied depending on whether traffic is moving toward or away from the trusted network.
- Traffic control policies are hierarchical:
  - Traffic is filtered according to the order of the policy in the policy list. Top policy (policy number 1) has highest priority.

CANAC v2.1—2-9

Traffic control policies are directional. IP-based policies can allow or block traffic moving from the untrusted (managed) network to the trusted network or from the trusted network to the untrusted network. Host-based policies allow traffic from the untrusted network to the specified host and specified trusted DNS server. Alternatively, a traffic control policy can block traffic to a particular machine or limit users to particular activities, such as e-mail use or web browsing. Examples of traffic policies are as follows:

- Deny access to the computer at 191.168.11.1.
- Allow web communication from computers on subnet 191.111.50/24.

Traffic control policies are hierarchical and the order of the policies in the policy list affects how traffic is filtered. The policy at the top of the list has the highest priority.



What Are Traffic Control Policies? (Cont.)

Traffic filtering correct:

- Priority 1: Deny Telnet
- Priority 2: Allow all

Result: Only Telnet traffic is blocked and all other traffic is permitted.

Traffic filtering incorrect (priorities reversed):

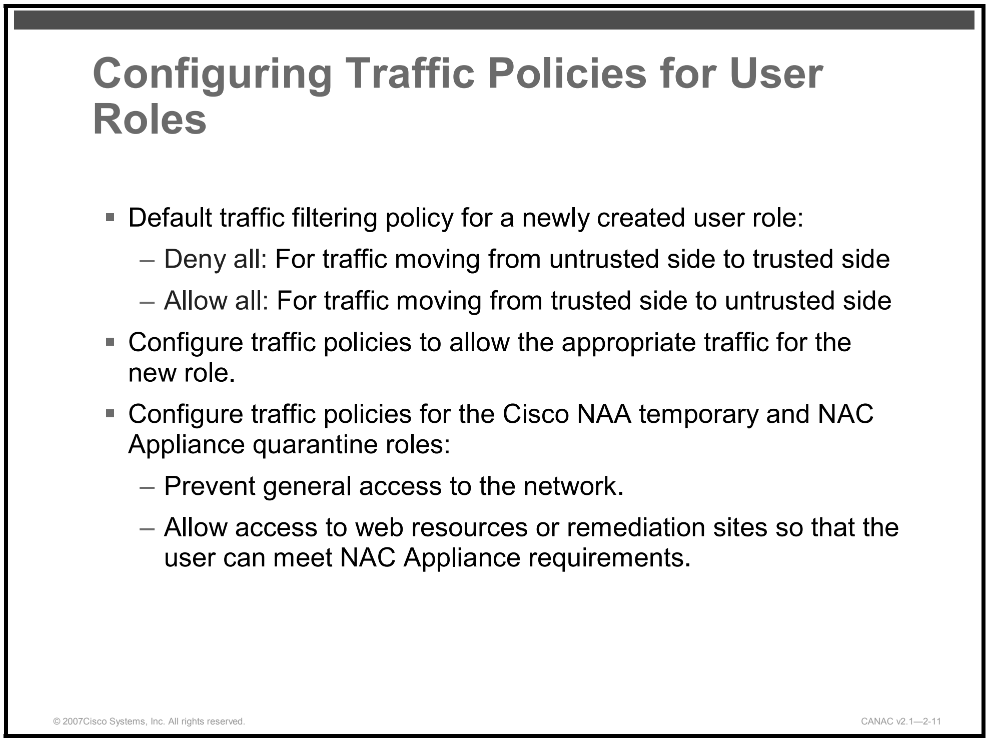
- Priority 1: Allow all
- Priority 2: Deny Telnet

Result: All traffic is allowed, and the second policy blocking Telnet traffic is ignored.

The traffic filtering examples in the figure show how priorities work for traffic policies that control traffic moving from the untrusted side to the trusted side of the network.

Configuring Traffic Policies for User Roles

This topic describes how to configure traffic control policies for a user role.



Configuring Traffic Policies for User Roles

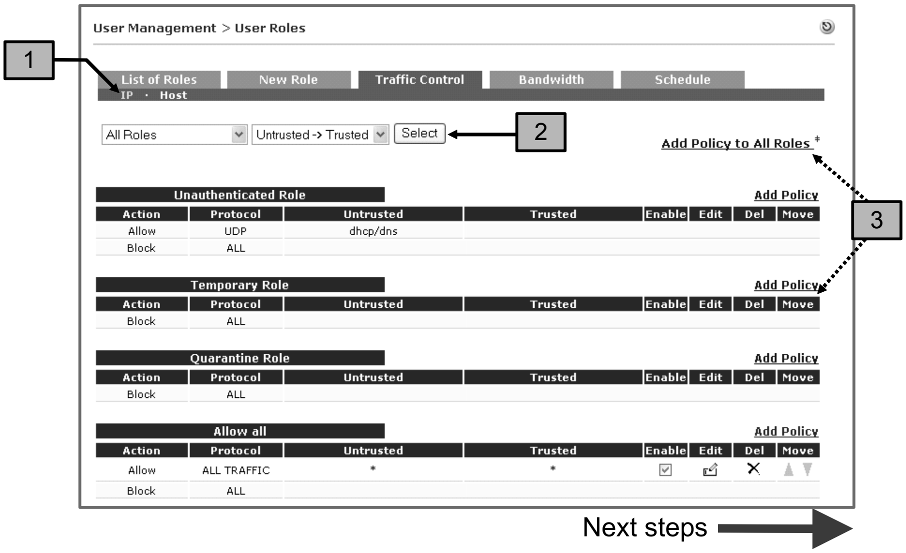
- Default traffic filtering policy for a newly created user role:
  - Deny all: For traffic moving from untrusted side to trusted side
  - Allow all: For traffic moving from trusted side to untrusted side
- Configure traffic policies to allow the appropriate traffic for the new role.
- Configure traffic policies for the Cisco NAA temporary and NAC Appliance quarantine roles:
  - Prevent general access to the network.
  - Allow access to web resources or remediation sites so that the user can meet NAC Appliance requirements.

CANAC v2.1—2-11

When you first create a role, it has a default traffic-filtering policy of “deny all” for traffic moving from the untrusted side to the trusted side of the network and “allow all” for traffic from the trusted side to the untrusted side of the network. Therefore, after creating a new role, you must create policies to permit the appropriate traffic for that role.

In addition, traffic policies must be configured for the Cisco NAA temporary role and Cisco NAC Appliance quarantine roles to prevent general access to the network but allow access to web resources or remediation sites required to meet requirements or fix vulnerabilities.

Creating an IP-Based Traffic Control Policy



Unauthenticated Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	UDP	dhcp/dns					
Block	ALL						

Temporary Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Block	ALL						

Quarantine Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Block	ALL						

Allow all

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	ALL TRAFFIC	*	*	☑	✎	✕	▲ ▼
Block	ALL						

Next steps →

Traffic control policies are created for each user role. Before creating a traffic control policy, ensure that the role that you will assign the policy to already exists. You can reach the Traffic Control tab from the List of Roles tab by clicking the traffic control icon associated with a user role.

To create or modify an IP-based traffic control policy, complete these steps:

Step 1 Choose **User Management > User Roles**. Click the **Traffic Control** tab and click the **IP** link.

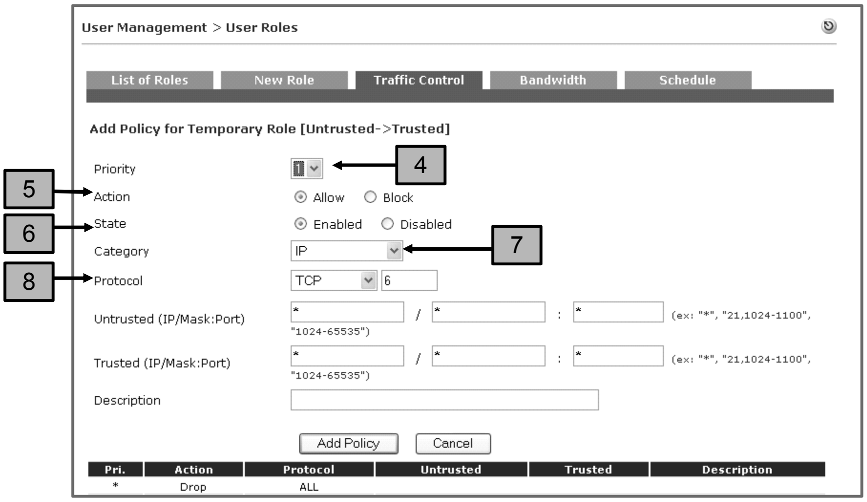
Step 2 Select the source-to-destination direction for which you want the policy to apply. Choose either **Trusted -> Untrusted** or **Untrusted -> Trusted** and click **Select**.

Step 3 Click the **Add Policy** link next to the role that you want to create a new policy for, or click **Add Policy to All Roles** to add the new policy to all the roles at once. To modify an existing policy, click the **Edit** button next to the policy you want to modify.

The Add Policy form for the role appears. Clicking **Edit** for an existing policy brings up the similar Edit Policy form for the role.

Note After creating a policy for all roles, you can remove or modify one policy at a time.

Creating an IP-Based Traffic Control Policy (Cont.)



Add Policy for Temporary Role [Untrusted->Trusted]

Priority	1
Action	● Allow ○ Block
State	● Enabled ○ Disabled
Category	IP
Protocol	TCP 6
Untrusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Description	

Pri.	Action	Protocol	Untrusted	Trusted	Description
*	Drop	ALL			

Next steps

Step 4 For a new policy, set the priority of the policy from the Priority drop-down menu. By default, the form displays a lower priority than all existing priorities when a new policy is created. For example, if you are creating the very first policy for the role, a priority of "1" appears. When you create a second policy, a priority of "2" is displayed, and so on. The number of priorities in the list will reflect the number of policies created for the role. The built-in Block All policy has the lowest priority of all policies by default.

Note For an edited policy, the Priority field is fixed on the Edit form. However, you can change the priority for the policy later in the IP form by clicking the up or down arrows for the policy in the Move column.

Step 5 Set the Action of the traffic policy as follows:

- **Allow** (default)**:** Permit the traffic.
- **Block:** Drop the traffic.

Step 6 Set the State of the traffic policy.

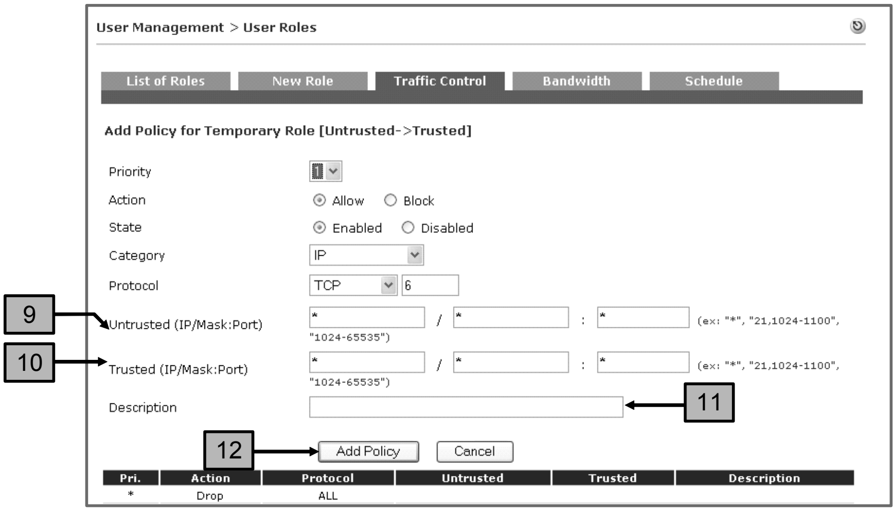
Step 7 Set the Category of the traffic as follows:

- **ALL TRAFFIC** (default): The policy applies to all protocols and to all trusted and untrusted source and destination addresses.
- **IP:** If selected, the Protocol field appears as described in Step 8.
- **IP FRAGMENT:** By default, the Cisco NAM blocks IP fragment packets because they can be used in denial of service (DoS) attacks. To define a policy that permits fragmented packets, choose **IP FRAGMENT** and set the action of the traffic policy to **Allow**.

Step 8 The Protocol field appears if the IP Category is chosen. There are six options in this field:

- **CUSTOM:** Used to specify a different protocol number than the protocols listed in the drop-down menu
- **TCP (6):** Used for TCP applications including HTTP, secure HTTP (HTTPS), and Telnet
- **UDP (17):** Used for User Datagram Protocol (UDP), which is generally used for broadcast messages
- **ICMP (1):** Used for Internet Control Message Protocol (ICMP)
- **ESP (50):** Used for Encapsulating Security Payload (ESP), which is an IPsec subprotocol used to encrypt the IP packet data that is typically used to create VPN tunnels
- **AH (51):** Used for an Authentication Header (AH), which is an IPsec subprotocol used to compute a cryptographic checksum to guarantee the authenticity of the IP header and packet

Creating an IP-Based Traffic Control Policy (Cont.)



User Management > User Roles

Add Policy for Temporary Role [Untrusted->Trusted]

Priority	1
Action	● Allow ○ Block
State	● Enabled ○ Disabled
Category	IP
Protocol	TCP 6
Untrusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Description	

Pri.	Action	Protocol	Untrusted	Trusted	Description
*	Drop	ALL			

CANAC v2.1—2-14

Step 9 In the Untrusted (IP/Mask:Port) field, specify the IP address and subnet mask of the untrusted network that the policy applies to. An asterisk in the Untrusted (IP/Mask**:** Port) field or the Trusted (IP/Mask: Port) field means that the policy applies for any address or application. If you choose TCP or UDP in the Protocol field, also choose the TCP/UDP application from the Port (CUSTOM) drop-down menu. The protocol port number is automatically populated by default.

Step 10 In the Trusted (IP/Mask:Port) field, specify the IP address and subnet mask of the trusted network that the policy applies to. An asterisk in the IP or Mask fields means that the policy applies for any address or application. If you choose TCP or UDP in the Protocol field, also choose the TCP/UDP application from the Port (CUSTOM) drop-down menu.

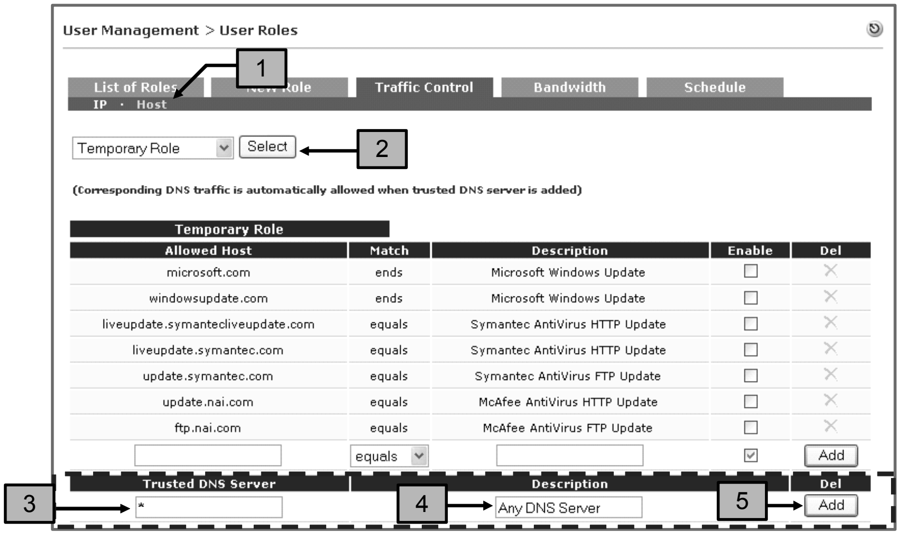
The traffic direction that you choose for viewing the list of policies (Untrusted -> Trusted or Trusted -> Untrusted) sets the source and destination IP addresses when you open the Add Policy form. These IP/Mask:Port entries appear:

- The first IP/Mask:Port entry listed is the source.
- The second IP/Mask:Port entry listed is the destination.

Step 11 Optionally, enter a description of the policy in the Description field.

Step 12 Click **Add Policy** when finished. If modifying a policy, click the **Update Policy** button.

Adding a Trusted DNS Server



User Management > User Roles

Temporary Role [Select]

(Corresponding DNS traffic is automatically allowed when trusted DNS server is added)

Temporary Role

Allowed Host	Match	Description	Enable	Del
microsoft.com	ends	Microsoft Windows Update	□	✕
windowsupdate.com	ends	Microsoft Windows Update	□	✕
liveupdate.symantecliveupdate.com	equals	Symantec AntiVirus HTTP Update	□	✕
liveupdate.symantec.com	equals	Symantec AntiVirus HTTP Update	□	✕
update.symantec.com	equals	Symantec AntiVirus FTP Update	□	✕
update.nai.com	equals	McAfee AntiVirus HTTP Update	□	✕
ftp.nai.com	equals	McAfee AntiVirus FTP Update	□	✕
	equals		☑	Add

Trusted DNS Server	Description	Del
*	Any DNS Server	Add

© 2007Cisco Systems, Inc. All rights reserved. CANAC v2.1—2-15

To add a trusted DNS server, complete these steps:

Step 1 Choose **User Management > User Roles**. Click the **Traffic Control** tab and then click the **Host** link.

Step 2 Choose the role that you want to add a trusted DNS server for and click the **Select** button.

Step 3 Enter an IP address in the Trusted DNS Server field or enter an asterisk, "*", to add any DNS server.

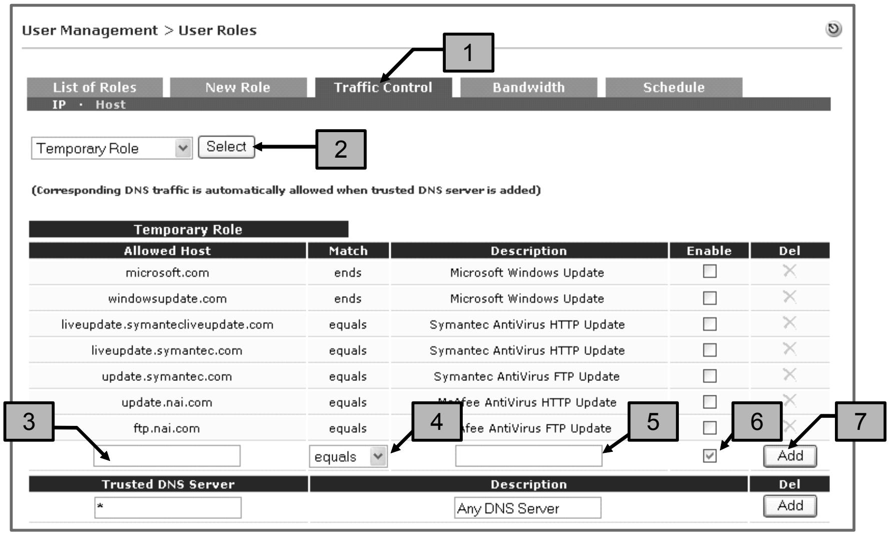
Note When you add a specific DNS server and then use this form later to add any DNS server by entering an asterisk, the previously added server becomes a subset of the overall policy that allows all DNS servers and is not displayed. If you later delete the any ("*") DNS server policy, the specific trusted DNS server previously allowed is again displayed.

Step 4 (Optional) Enter a description for the DNS server in the Description field (for example, "Microsoft Windows Update").

Step 5 Click **Add**. The new policy appears in the Trusted DNS Server column, above the Add field.

Note When a trusted DNS server is added, an IP-based traffic policy allowing that server is automatically added for the role.

Adding an Allowed Host



Temporary Role

(Corresponding DNS traffic is automatically allowed when trusted DNS server is added)

Temporary Role

Allowed Host	Match	Description	Enable	Del
microsoft.com	ends	Microsoft Windows Update	□	×
windowsupdate.com	ends	Microsoft Windows Update	□	×
liveupdate.symantecliveupdate.com	equals	Symantec AntiVirus HTTP Update	□	×
liveupdate.symantec.com	equals	Symantec AntiVirus HTTP Update	□	×
update.symantec.com	equals	Symantec AntiVirus FTP Update	□	×
update.nai.com	equals	McAfee AntiVirus HTTP Update	□	×
ftp.nai.com	equals	McAfee AntiVirus FTP Update	□	×
	equals		☑	Add

Trusted DNS Server	Description	Del
*	Any DNS Server	Add

You can configure DNS host-based policies for a role by host name or domain name when a host has multiple or dynamic IP addresses.

To add an allowed host name to a role, complete these steps:

Step 1 Choose **User Management > User Roles**. Click the **Traffic Control** tab and then click the **Host** link.

Step 2 Choose the role that you want to add a DNS host for and click **Select**.

Step 3 Enter the hostname in the Allowed Host field (for example, "*.windowsupdate.microsoft.com").

Step 4 In the Match drop-down menu, choose an operator to match the host name. Operators include "equals," "ends," "begins," and "contains."

Step 5 Enter a description for the host in the Description field (for example, "Microsoft Windows Update").

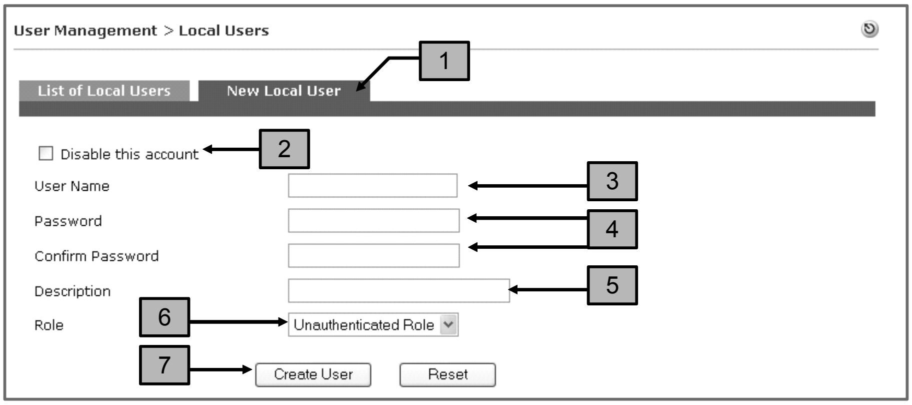
Step 6 Check the **Enable** check box if it is not already checked.

Step 7 Click **Add**. The new policy appears above the Add field in the host list part of the form.

Creating Local User Accounts

This topic describes how to create a local user account.

Creating Local User Accounts



Role: Unauthenticated Role

CANAC v2.1—2-17

A local user is one who is validated by the Cisco NAM, not by an external authentication server. Local user accounts are not intended for general use because the users cannot change their password outside the web administration console. Local user accounts are primarily intended for testing or for guest user accounts.

For testing purposes, a user should be created immediately after you have created a user role.

To create a local user account, complete these steps:

Step 1 Choose **User Management > Local Users** and click the **New Local User** tab. The New Local User form appears.

Step 2 Clear the **Disable this account** check box if you want the user account to be active immediately.

Step 3 Enter a unique username for the user in the User Name field. This username is the login name that identifies the user in the system.

Step 4 Enter a password in the Password field and reenter the password in the Confirm Password field. The password value is case-sensitive.

Step 5 (Optional) Enter a description for the user in the Description field.

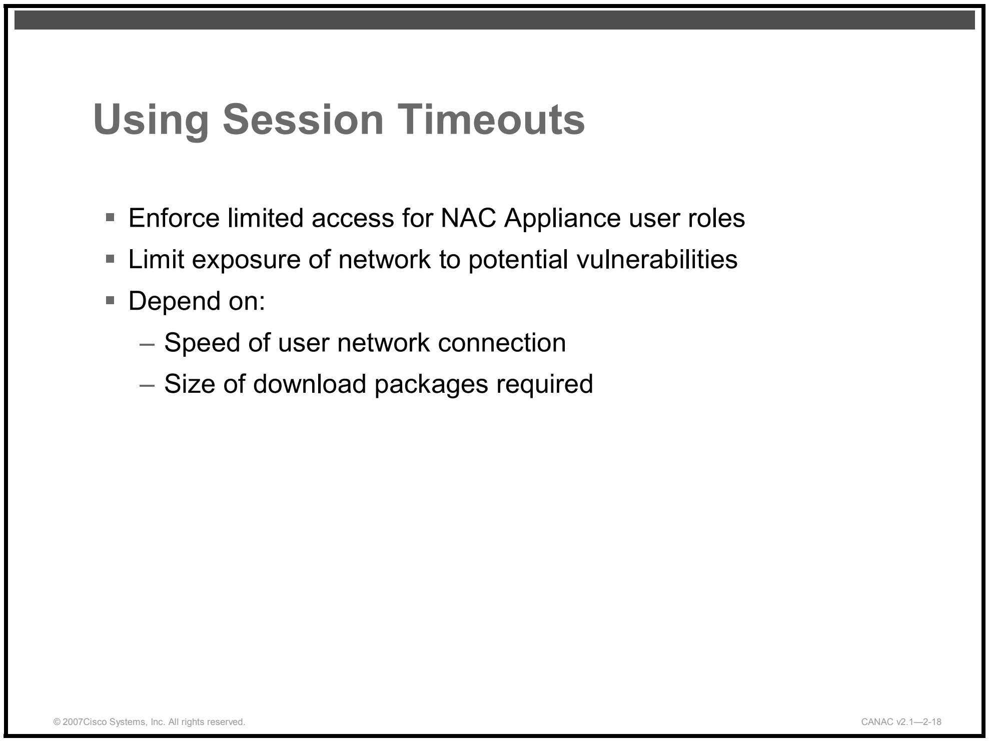
Step 6 Choose the default role for the user from the Role drop-down menu. All configured roles appear in the list. If the role you want to assign the user does not exist yet, create the role in the User Roles page and modify the user profile with the new role.

Step 7 Click **Create User** to finish.

The user now appears in the List of Local Users tab. From this tab, you can view user information, edit user settings such as the name, password, and role, or you can remove the user.

Configuring User Session Timeouts

This topic describes how to configure user session timeouts for user roles.



Using Session Timeouts

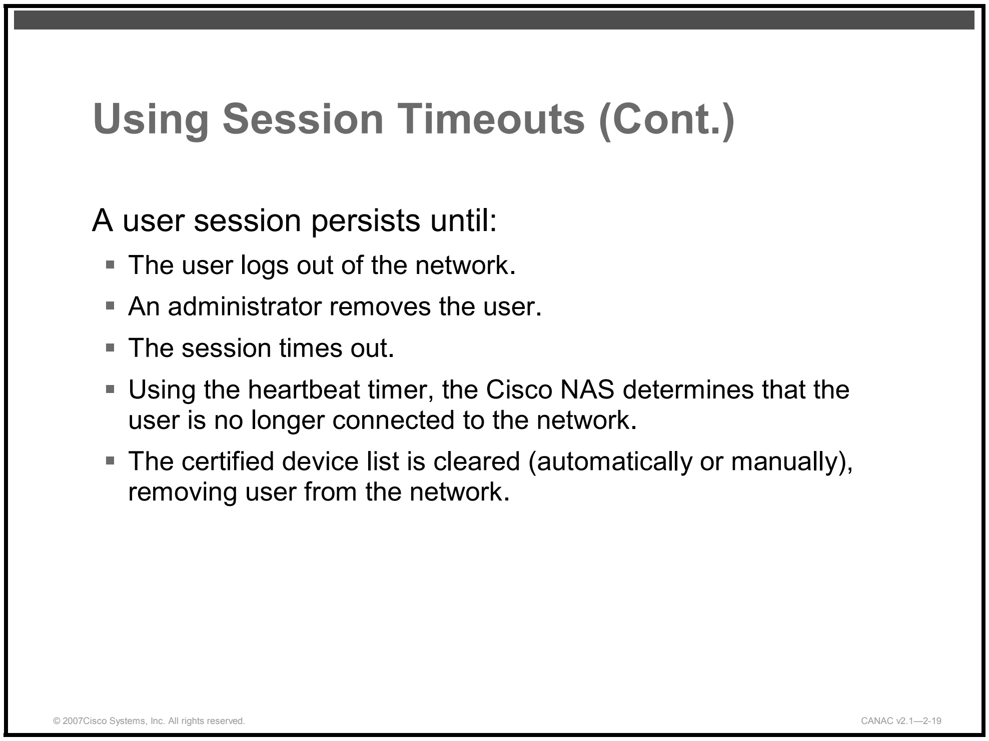
- Enforce limited access for NAC Appliance user roles
- Limit exposure of network to potential vulnerabilities
- Depend on:
  - Speed of user network connection
  - Size of download packages required

CANAC v2.1—2-18

To enforce limited access for the Cisco NAS temporary role and the NAC Application quarantine role, configure both roles to have brief session timeout periods and few traffic policy privileges. Use special care in determining the exact timeout period suitable for your environment. The session timeout period should afford users the opportunity to complete the check and acquire needed software. The timeout period should not allow much more than the minimum amount of time to perform these two tasks. A minimal timeout period for these Cisco NAC Appliance-related roles limits exposure of vulnerable users to the network.

Factors that determine the timeout period that is appropriate for your environment include the typical speed of the network connection that is available to your users and the size of the download packages that you will require.

You can also configure a heartbeat timer that sets the number of minutes after which any user is logged off the network if they are unreachable by a connection attempt from the Cisco NAS.



Using Session Timeouts (Cont.)

A user session persists until:

- The user logs out of the network.
- An administrator removes the user.
- The session times out.
- Using the heartbeat timer, the Cisco NAS determines that the user is no longer connected to the network.
- The certified device list is cleared (automatically or manually), removing user from the network.

CANAC v2.1—2-19

A user session persists until one of the following occurs:

- The user logs out of the network through the browser logout page or the Cisco NAS logout icon located in the top right of the Cisco NAC Appliance GUI.
- An administrator manually removes the user from the network.
- The session times out as configured in the session timer for the user role.
- Using the heartbeat timer, the Cisco NAS determines that the user is no longer connected to the network and the Cisco NAM terminates the session.
- The certified device list is cleared (automatically or manually) and the user is removed from the network.

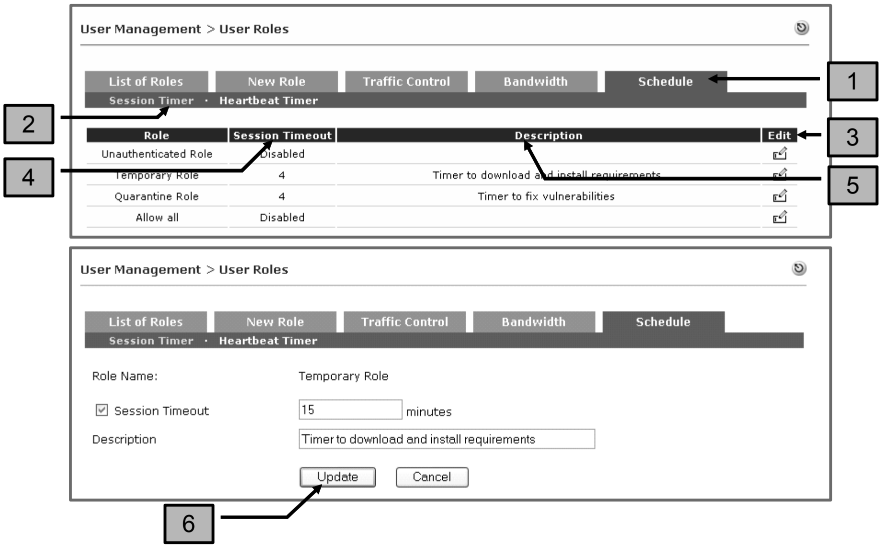
Timeout properties enhance the security of your network by ensuring that sessions are terminated after a configured period of time. Timeout settings apply to all users, whether they are locally or externally authenticated. The following points apply to session timeouts where the user is either permitted to stay or is removed from the network regardless of connection status or activity:

- If the session timer is zero and the heartbeat timer is not set, the user remains on the online users list and is not required to log in again.
- If the session timer is zero and the heartbeat timer is set, the heartbeat timer takes effect.
- If the session timer is not zero and the heartbeat timer is not set, the session timer takes effect.
- If both timers are set, the first timeout to be reached is activated.
- If the user logs out and shuts down the machine, the user is removed from the online users list and is required to log in again.

- If the DHCP lease is longer than the session timeout, the DHCP leases are not being reused efficiently.

Note Determining when a user session is dropped when the session timer and the heartbeat timer are used can be confusing. For details on the interaction between the session timer and the heartbeat timer, refer to Session Timer/Heartbeat Timer Interaction in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Configuring a Session Timer for a User Role



Role	Session Timeout	Description	Edit
Unauthenticated Role	Disabled		✎
Temporary Role	4	Timer to download and install requirements	✎
Quarantine Role	4	Timer to fix vulnerabilities	✎
Allow all	Disabled		✎

Role Name: Temporary Role

☑ Session Timeout 15 minutes

Description Timer to download and install requirements

CANAC v2.1—2-20

To configure a session timer for a user role, complete these steps:

Step 1 Choose **User Management > User Roles** and click the **Schedule** tab.

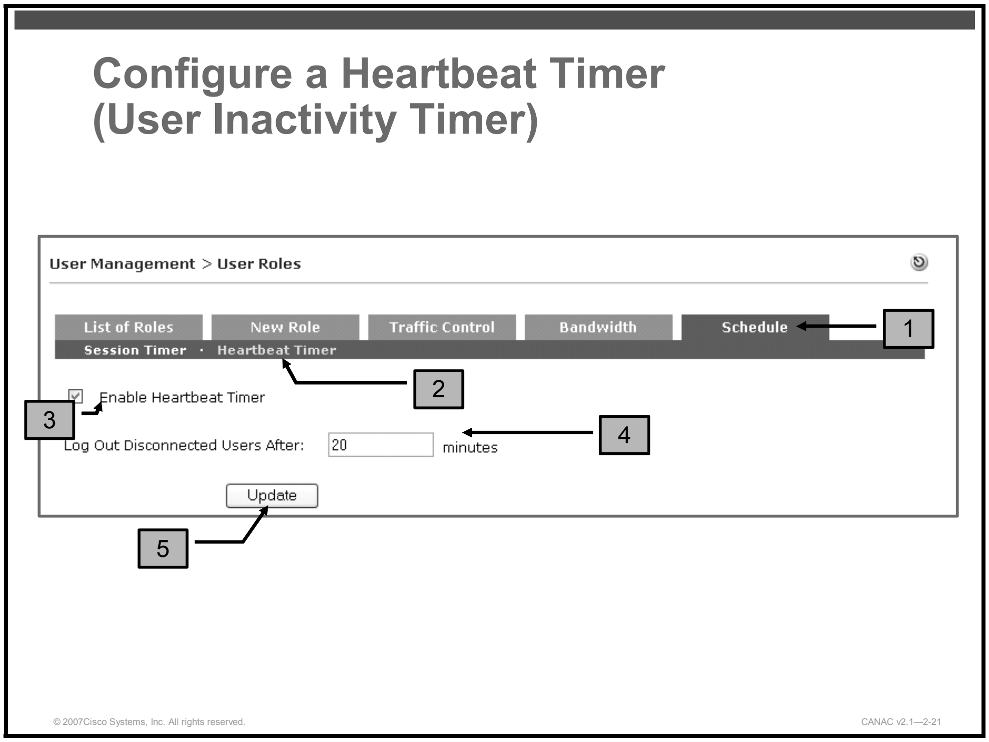
Step 2 Click the **Session Timer** submenu.

Step 3 Click the **Edit** button next to the role you want to configure for timeout settings.

Step 4 Check the **Session Timeout** check box and enter the number of minutes after which the user session times out. The timeout clock starts when the user logs in and is not affected by user activity. After the session expires, the user must log in again to continue using the network.

Step 5 (Optional) Enter a description of the session length limitation in the Description field.

Step 6 Click **Update** when you are finished.



Configure a Heartbeat Timer (User Inactivity Timer)

User Management > User Roles

List of Roles | New Role | Traffic Control | Bandwidth | Schedule

Session Timer · Heartbeat Timer

☑ Enable Heartbeat Timer

Log Out Disconnected Users After: 20 minutes

© 2007Cisco Systems, Inc. All rights reserved. CANAC v2.1—2-21

The heartbeat timer sets the number of minutes after which a user will be logged off the network if the user is unreachable through a connection attempt from the Cisco NAS. This feature enables the Cisco NAS to detect and disconnect users who have restarted their computers without logging out of the network.

To configure a heartbeat timer for a user role, complete these steps:

Step 1 Choose **User Management > User Roles** and click the **Schedule** tab.

Step 2 Click the **Heartbeat Timer** link. The Heartbeat Timer page appears.

Step 3 Check the **Enable Heartbeat Timer** check box.

Step 4 In the Log Out Disconnected Users After field, enter the number of minutes after which a user will be logged off the network when that user is unreachable by a connection attempt.

Step 5 Click **Update** to save your settings.

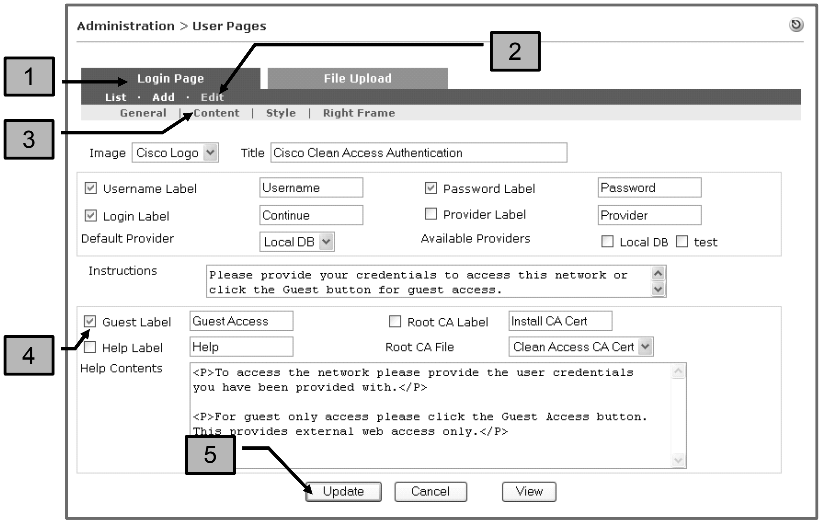
Note The actual connection check is performed with an Address Resolution Protocol (ARP) message rather than using a ping function. This allows the heartbeat check to function even if ICMP traffic is blocked.

Logging a user off the network does not remove the user from the certified list. However, removing a user from the certified list does log the user off the network. You can drop users from the network individually or terminate sessions for all users at once.

Configuring Guest Access

This topic describes how to configure guest access for visitors or temporary users in a Cisco NAC Appliance network.

Setting Up Guest Access Using the Built-In Guest Account



Administration > User Pages
Login Page
File Upload
List · Add · Edit
General | Content | Style | Right Frame
1
2
3
4
5
Update
Cancel
View

Image: Cisco Logo   Title: Cisco Clean Access Authentication

☑ Username Label: Username   ☑ Password Label: Password

☑ Login Label: Continue   □ Provider Label: Provider

Default Provider: Local DB   Available Providers: □ Local DB □ test

Instructions:

```
Please provide your credentials to access this network or
click the Guest button for guest access.
```

☑ Guest Label: Guest Access   □ Root CA Label: Install CA Cert

□ Help Label: Help   Root CA File: Clean Access CA Cert

Help Contents:

```
<P>To access the network please provide the user credentials
you have been provided with.</P>

<P>For guest only access please click the Guest Access button.
This provides external web access only.</P>
```

Guest access enables you to provide limited access to your network for visitors or temporary users. Cisco NAC Appliance includes a built-in guest user account. By default, the account belongs to the unauthenticated role and is validated by the (local) NAC Appliance provider. You should specify appropriate traffic control policies and timeout properties for the guest user role on your network.

Note Local authentication must be enabled to use the built-in guest access account.

To implement guest access, you must enable the guest access button that appears in the login page. When a visitor clicks the guest access button, the login credentials ("guest" for the user name and "guest" for the password) are sent to the Cisco NAM for authentication. To enable the guest access button, complete these steps:

Step 1 Choose **Administration > User Pages** and click the **Login Page** tab.

Step 2 Click the **Edit** submenu to edit the login page for which you want to provide guest access.

Step 3 Click the **Content** link. The Content form appears.

Step 4 Check the **Guest Label** check box. The label for the Guest Access button defaults to "Guest Access." If you want to use a different label than the default, enter the label text in the Guest Label text box.

Step 5 Click **Update**.

Setting Up Differentiated Guest Access

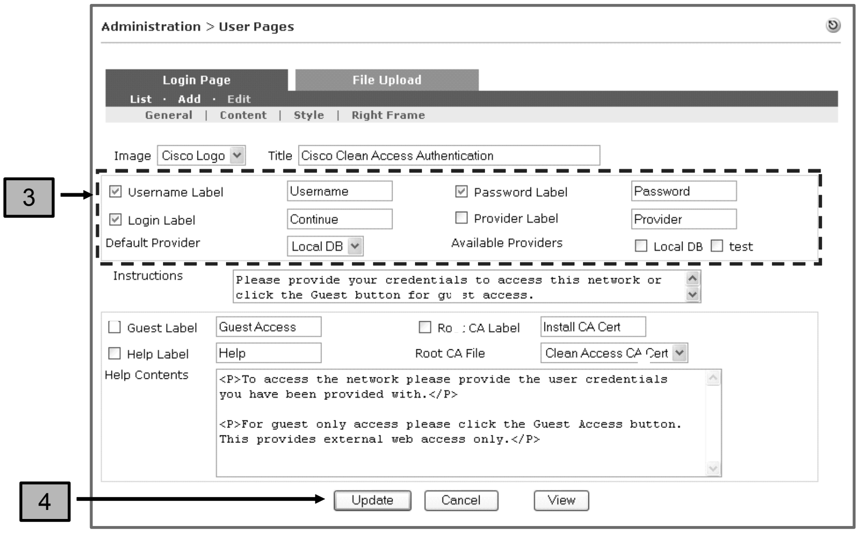

Administration > User Pages
Login Page
File Upload
List · Add · Edit
General | Content | Style | Right Frame
3
4

Image: Cisco Logo
Title: Cisco Clean Access Authentication

☑ Username Label: Username
☑ Password Label: Password
☑ Login Label: Continue
□ Provider Label: Provider
Default Provider: Local DB
Available Providers: □ Local DB □ test

Instructions:

```
Please provide your credentials to access this network or
click the Guest button for gu st access.
```

□ Guest Label: Guest Access
□ Ro : CA Label: Install CA Cert
□ Help Label: Help
Root CA File: Clean Access CA Cert

Help Contents:

```
<P>To access the network please provide the user credentials
you have been provided with.</P>

<P>For guest only access please click the Guest Access button.
This provides external web access only.</P>
```

When you use a guest account for guest access, guest users share the network with authenticated users. Multiple guests are not differentiated in the Cisco NAM user logs. An alternative for setting up guest access involves setting up networks solely for guest users. In this case, you can use e-mail addresses (or any other user property) as identifiers for the individual guests. An example application of this type of access is a library in which you want users to be differentiated, in guestbook fashion, but not closely authenticated.

To set up differentiated guest access, complete these steps:

Step 1 (Not shown) Create an authentication provider server of type "Allow All." See the "Configuring External Authentication" lesson for instructions.

Step 2 (Not shown) Add another (new) global login page for guest access and configure these settings:

- For VLAN ID, enter "*****" (this indicates any VLAN ID).
- For subnet, enter "*****" (this indicates any subnet).
- For Operating System, choose **ALL**.

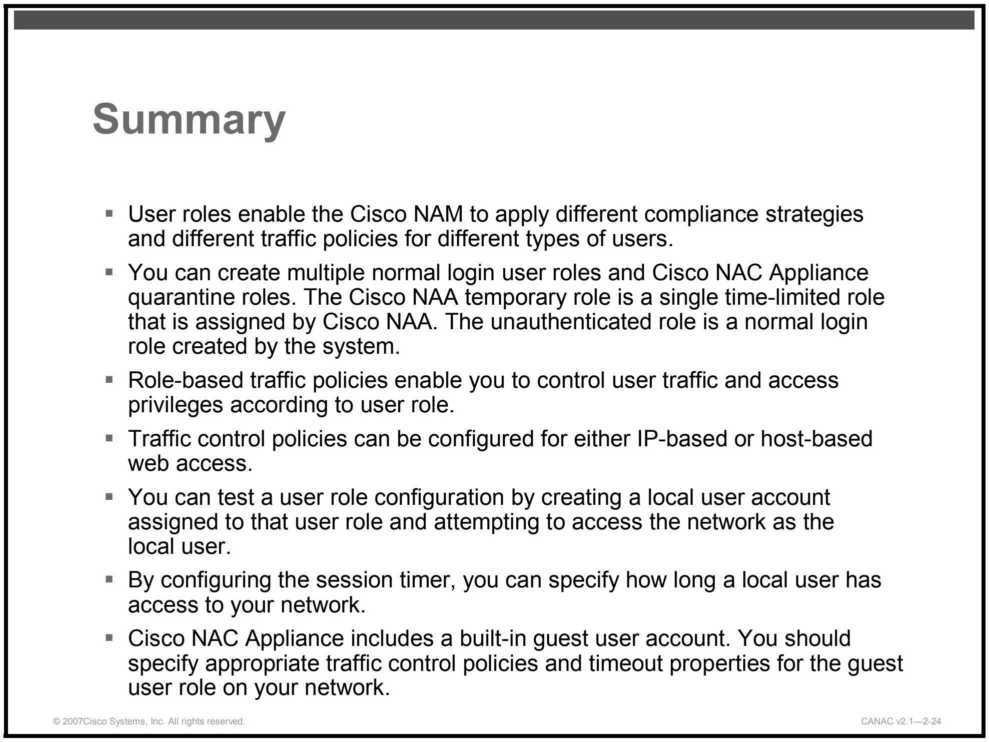
Step 3 From the Content form accessed in the previous procedure, edit the Login Page content as follows:

- Rename the Username Label to E-mail Address, or hide the username label if you do not want users to provide an identifier. The default username and password for the Allow All authentication provider are "guest" and "guest", respectively.
- Uncheck the **Password Label**, **Provider Label**, **Available Providers,** and **Guest Label** check boxes to hide these login page elements.
- In the Default Provider field drop-down menu, choose the authentication provider that you set up in the first step of this procedure.

Step 4 Click **Update**. Guests can now access the network without login credentials. If the user submits an identifier in the login page, such as an e-mail address, the identifier appears in the Online Users page while the user is logged in.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- User roles enable the Cisco NAM to apply different compliance strategies and different traffic policies for different types of users.
- You can create multiple normal login user roles and Cisco NAC Appliance quarantine roles. The Cisco NAA temporary role is a single time-limited role that is assigned by Cisco NAA. The unauthenticated role is a normal login role created by the system.
- Role-based traffic policies enable you to control user traffic and access privileges according to user role.
- Traffic control policies can be configured for either IP-based or host-based web access.
- You can test a user role configuration by creating a local user account assigned to that user role and attempting to access the network as the local user.
- By configuring the session timer, you can specify how long a local user has access to your network.
- Cisco NAC Appliance includes a built-in guest user account. You should specify appropriate traffic control policies and timeout properties for the guest user role on your network.

Lesson 2

Configuring External Authentication

Overview

Companies often use an external authentication source to provide secure access to their network-based applications. Network administrators need to know how to configure a Network Admission Control (NAC) Appliance solution to support external authentication. This lesson describes the steps for setting up external authentication for a Cisco NAC Appliance solution. The steps include configuring external authentication providers, mapping users to user roles, testing user authentication, and configuring RADIUS accounting.

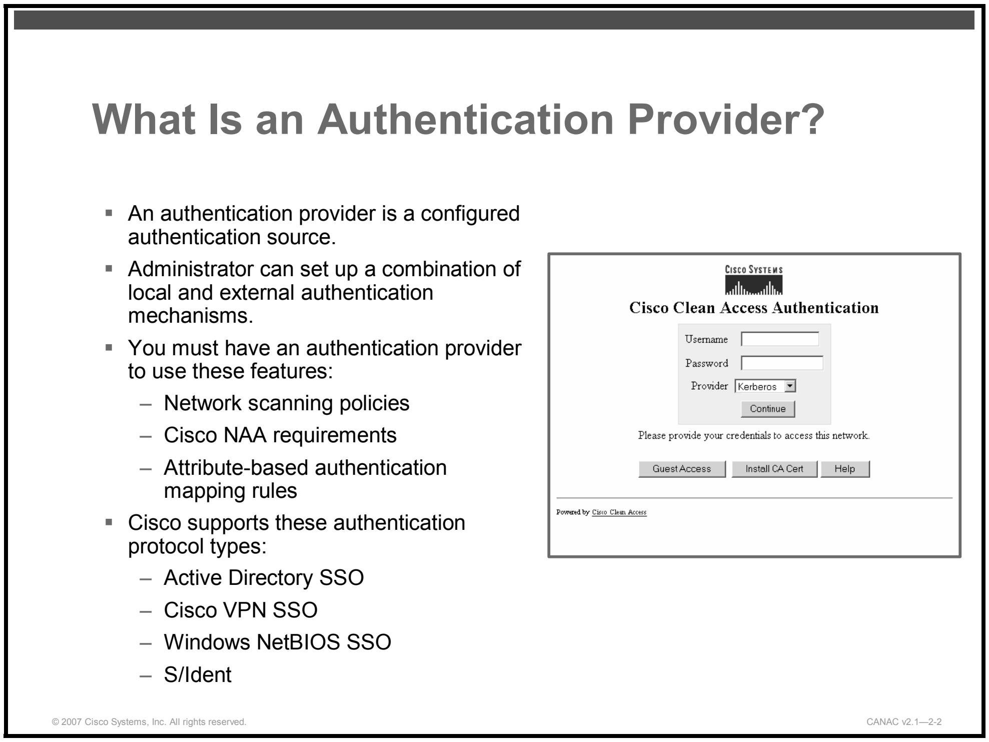
Objectives

Upon completing this lesson, you will be able to describe how to configure external authentication for users in a network using the Cisco NAC Appliance Manager (Cisco NAM). This ability includes being able to meet these objectives:

- Describe how to configure the Cisco NAM to use external authentication providers
- Describe how to map users to user roles when configuring external authentication
- Describe how to test user authentication for configured external authentication providers
- Describe how to configure RADIUS accounting for users in a Cisco NAC Appliance network

Configuring External Authentication Providers

This topic describes how to configure the Cisco NAM to use external authentication providers.



What Is an Authentication Provider?

- An authentication provider is a configured authentication source.
- Administrator can set up a combination of local and external authentication mechanisms.
- You must have an authentication provider to use these features:
  - Network scanning policies
  - Cisco NAA requirements
  - Attribute-based authentication mapping rules
- Cisco supports these authentication protocol types:
  - Active Directory SSO
  - Cisco VPN SSO
  - Windows NetBIOS SSO
  - S/Ident

Cisco Systems
Cisco Clean Access Authentication
Username
Password
Provider Kerberos
Continue
Please provide your credentials to access this network.
Guest Access
Install CA Cert
Help
Powered by Cisco Clean Access

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—2-2

An authentication provider is a configured authentication source. By connecting the Cisco NAM to external authentication mechanisms, you can use existing user data to authenticate users in the untrusted network. As shown in the figure, users can access a secure network from the web by selecting an authentication provider from the Provider drop-down menu on the web login page.

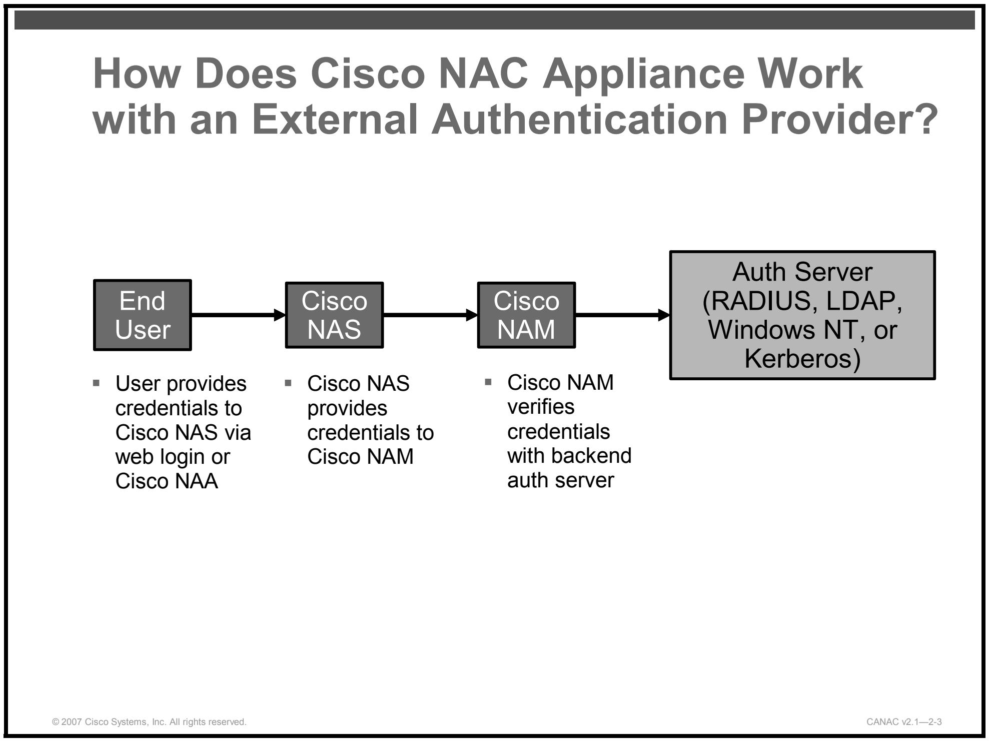
You can set up any combination of local and external authentication mechanisms. Typically, external authentication sources are used for general users and local authentication is for guests, test users, or other types of users with limited network access.

Currently, you are required to use a local database, RADIUS, Lightweight Directory Access Protocol (LDAP), Windows NT, or Kerberos authentication server type if you want to enable Cisco NAC Appliance system features such as network scanning policies, Cisco Clean Access Agent requirements, and attribute-based authentication mapping rules.

When you want to employ single sign-on (SSO) or transparent authentication servers, remember that Cisco supports these authentication protocol types:

- Windows Active Directory SSO
- Cisco VPN SSO
- Windows NetBIOS SSO (formerly known as "Transparent Windows")
- S/Ident

Note Cisco VPN SSO and Microsoft Windows Active Directory SSO are presented in separate lessons in the Cisco NAC Appliance Implementation module.



How Does Cisco NAC Appliance Work with an External Authentication Provider?

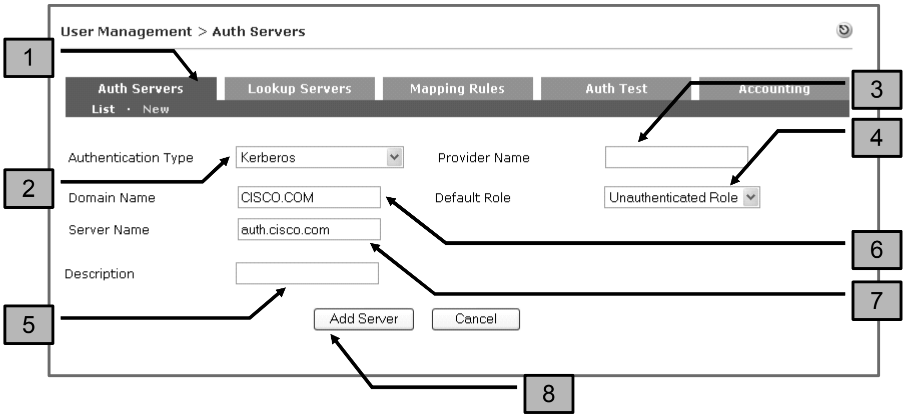
End User → Cisco NAS → Cisco NAM → Auth Server (RADIUS, LDAP, Windows NT, or Kerberos)

- User provides credentials to Cisco NAS via web login or Cisco NAA
- Cisco NAS provides credentials to Cisco NAM
- Cisco NAM verifies credentials with backend auth server

CANAC v2.1—2-3

The schematic shows an end user logging in to a network protected by Cisco NAC Appliance. Whether the end user has the Cisco NAA installed on their computer or is using an Internet kiosk to log in determines how the end user credentials are provided to Cisco NAC Appliance. As the schematic shows, the Cisco NAC Appliance components work seamlessly with external or backend authentication providers.

Example: Configuring a Kerberos Authentication Provider



User Management > Auth Servers

Authentication Type: Kerberos

Provider Name:

Domain Name: CISCO.COM

Default Role: Unauthenticated Role

Server Name: auth.cisco.com

Description:

You must configure the server that you want Cisco NAC Appliance to use as an authentication provider. The authentication type that you choose brings up the form appropriate to that type.

To configure a Kerberos provider for Cisco NAC Appliance users, complete these steps:

Step 1 Choose **User Management > Auth Servers > New**.

Step 2 From the Authentication Type drop-down menu, choose **Kerberos**.

Step 3 In the Provider Name field**,** enter a name that is unique for authentication providers. If you intend to offer your users the ability to select providers from the login page, be sure to use a name that is meaningful or recognizable for your users.

Step 4 From the Default Role field drop-down menu, choose the role to assign to users that are authenticated by this provider. The role you choose is used if it is not overridden by a role assignment based on MAC address or IP address. All the configured roles will appear in the drop-down menu.

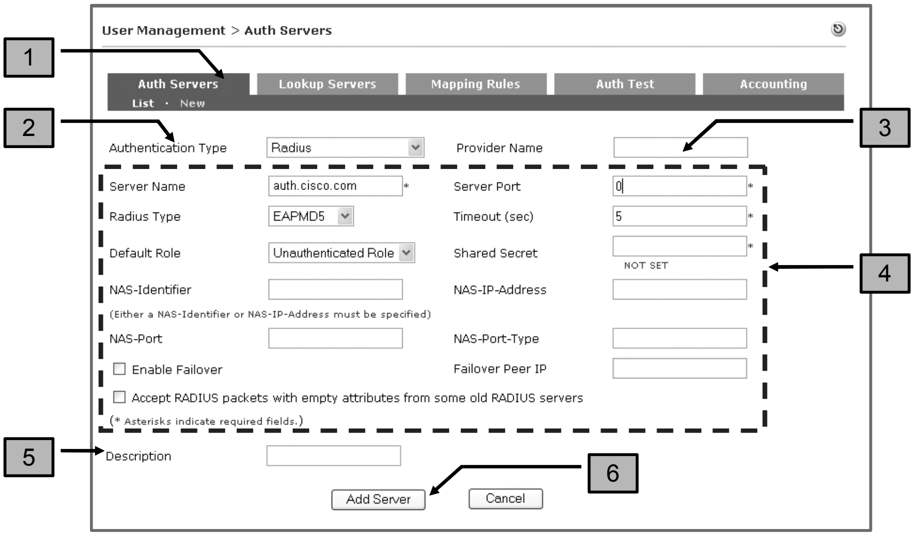
Step 5 (Optional) Enter a description for the authentication server in the Description field.

Step 6 In the Domain Name field, enter the domain name for your Kerberos authentication type (for example, cisco.com).

Step 7 In the Server Name field, enter the fully qualified hostname or IP address of the Kerberos authentication server.

Step 8 When finished, click **Add Server**. The authentication source is now configured and appears in the list of servers. From the list of servers, you can modify the settings by clicking the **Edit** button next to the source.

Example: Configuring a RADIUS Authentication Provider



User Management > Auth Servers

Authentication Type	Radius	Provider Name	
Server Name	auth.cisco.com *	Server Port	0 *
Radius Type	EAPMD5	Timeout (sec)	5 *
Default Role	Unauthenticated Role	Shared Secret	* NOT SET
NAS-Identifier		NAS-IP-Address	
NAS-Port		NAS-Port-Type	
☐ Enable Failover		Failover Peer IP	

(Either a NAS-Identifier or NAS-IP-Address must be specified)

☐ Accept RADIUS packets with empty attributes from some old RADIUS servers

(* Asterisks indicate required fields.)

Description

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—2-5

The RADIUS authentication client in the Cisco NAM supports failover between two RADIUS servers. This setup allows the Cisco NAM to attempt authentication of a pair of RADIUS servers. The primary server is authenticated first; if authentication fails, the secondary server is authenticated. The Enable Failover and Failover Peer IP field descriptions provide details on authentication.

To configure a RADIUS authentication client, perform these steps:

Step 1 Choose **User Management** > **Auth Servers > New**.

Step 2 From the Authentication Type drop-down menu, choose **RADIUS**. The RADIUS form appears.

Step 3 In the Provider Name field, enter a name that is unique for the authentication provider. If you want to provide your users with the ability to select providers from the login page, use a name that is meaningful or recognizable.

Step 4 Complete the remaining fields as follows:

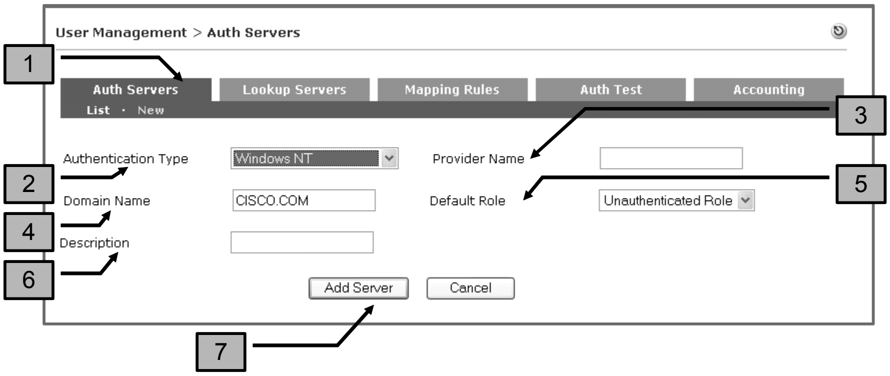
- In the Server Name field, enter the fully qualified hostname (for example, auth.cisco.com) or the IP address of the RADIUS authentication server.
- In the Server Port field, enter the port number on which the RADIUS server is listening.
- From the Radius Type drop-down menu, choose the RADIUS authentication method you want to use. Supported methods include Extensible Authentication Protocol Message Digest 5 (EAPMD5), Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and MS-CHAP2.
- In the Timeout (sec) field, enter the timeout value in seconds for the authentication request session.

- From the Default Role drop-down menu, choose the role to assign to users who are authenticated by this provider. The role you choose is used if it is not overridden by a role assignment based on MAC address or IP address.
- In the Shared Secret field, enter the RADIUS shared secret password bound to the specified client IP address.
- In the NAS-Identifier field, enter the Cisco NAC Appliance Server (Cisco NAS)-Identifier value to be sent with all RADIUS authentication packets. Either a NAS-Identifier or a NAS-IP-Address must be specified to send the packets.
- In the NAS-IP-Address field, enter the Cisco NAS-IP-Address value to be sent with all RADIUS authentication packets. Either a NAS-IP-Address or a NAS-Identifier must be specified to send the packets.
- In the NAS-Port field, enter the Cisco NAS-Port value to send with all RADIUS authentication packets.
- In the NAS-Port-Type field, enter the Cisco NAS-Port-Type value to send with all RADIUS authentication packets.
- Check the **Enable Failover** check box to enable sending a second authentication packet to a RADIUS failover peer IP if the primary RADIUS authentication server response times out.
- In the Failover Peer IP field, enter the IP address of the failover RADIUS authentication server, if appropriate.

Step 5 (Optional) Enter a description for the authentication server in the Description field.

Step 6 When finished, click the **Add Server** button. The authentication source is now configured and appears in the list of servers. From the list of servers, you can modify the settings by clicking the **Edit** button next to the source.

Example: Configuring a Windows NT Authentication Provider


User Management > Auth Servers

Authentication Type: Windows NT

Provider Name:

Domain Name: CISCO.COM

Default Role: Unauthenticated Role

Description:

CANAC v2.1—2-6

To configure a Windows NT provider for Cisco NAC Appliance users, complete these steps:

Step 1 Choose **User Management > Auth Servers > New**.

Step 2 From the Authentication Type drop-down menu, choose **Windows NT**. The Windows NT form appears.

Step 3 In the Provider Name field, enter a name that is unique for the authentication provider. If you intend to provide your users with the ability to select providers from the login page, be sure to use a name that is meaningful or recognizable.

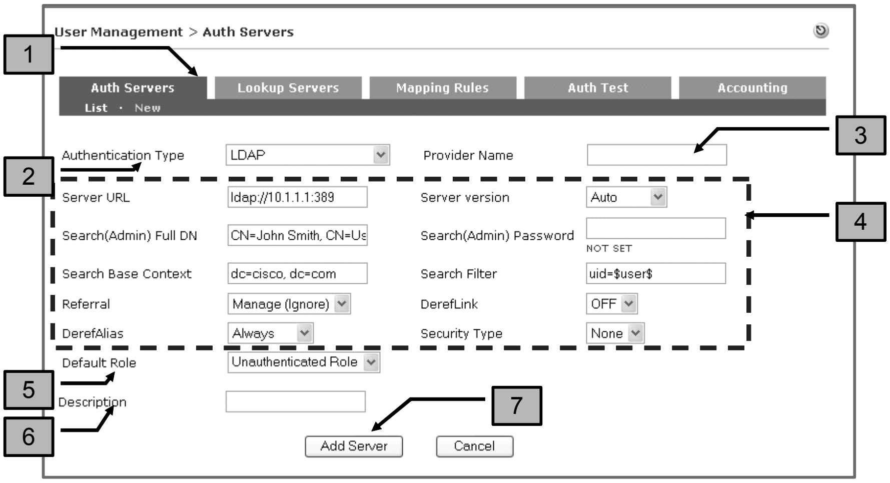
Step 4 In the Domain Name field, enter the domain name of the Windows NT environment.

Step 5 From the Default Role drop-down menu, choose the role to assign to users who are authenticated by this provider. The role you choose is used if it is not overridden by a role assignment based on a MAC address or IP address.

Step 6 (Optional) Enter a description for the authentication server in the Description field.

Step 7 When you are finished, click the **Add Server** button. The authentication source is now configured and appears in the list of servers. From the list of servers, you can modify the settings by clicking the **Edit** button next to the source.

Example: Configuring an LDAP Authentication Provider



Authentication Type	LDAP	Provider Name	
Server URL	ldap://10.1.1.1:389	Server version	Auto
Search(Admin) Full DN	CN=John Smith, CN=Us	Search(Admin) Password	NOT SET
Search Base Context	dc=cisco, dc=com	Search Filter	uid=$user$
Referral	Manage (Ignore)	DerefLink	OFF
DerefAlias	Always	Security Type	None
Default Role	Unauthenticated Role		
Description			

To configure an LDAP provider for Cisco NAC Appliance users, complete these steps:

Step 1 Choose **User Management > Auth Servers > New**.

Step 2 From the Authentication Type drop-down menu, choose **LDAP**. The LDAP form appears.

Step 3 In the Provider Name field**,** enter a name that is unique for the authentication provider. If you intend to provide your users with the ability to select providers from the login page, be sure to use a name that is meaningful or recognizable.

Step 4 Complete the remaining fields as follows:

- In the Server URL field, enter the URL of the LDAP server in the following form:
  ldap://<*directory_server_name*>:<*port_number*>
  If no port number is specified, 389 is assumed.
- From the Server version drop-down menu, choose the LDAP version. Supported types include Version 2 and Version 3. Choose **Auto** to have the server version automatically detected.
- In the Search (Admin) Full DN (distinguished name) field, if access to the directory is controlled, enter the LDAP administrator ID that is used to connect to the server.
- In the Search (Admin) Password field, enter the password for the LDAP administrator.
- In the Search Base Context field, enter the root of the LDAP tree where the search for users is performed.
- In the Search Filter field, enter the attribute that is to be authenticated (for example, uid=$user$).

- From the Referral drop-down menu, choose whether referral entries are managed (the LDAP server returns referral entries as ordinary entries) or returned as handles.
- From the DerefLink drop-down menu, choose the object alias referencing option. If you chose **ON**, object aliases that are returned as search results are de-referenced. That is, the actual object that the alias refers to is returned as the search result rather than the alias itself.
- From the DerefAlias drop-down menu, choose one of the following options: **Always**, **Never**, **Finding**, **Searching**.
- From the Security Type drop-down menu, choose whether or not the connection to the LDAP server uses Secure Sockets Layer (SSL).

Note If the LDAP server uses SSL, be sure to import the certificate from the SSL Certificate tab of the User Management > Clean Access Manager page.

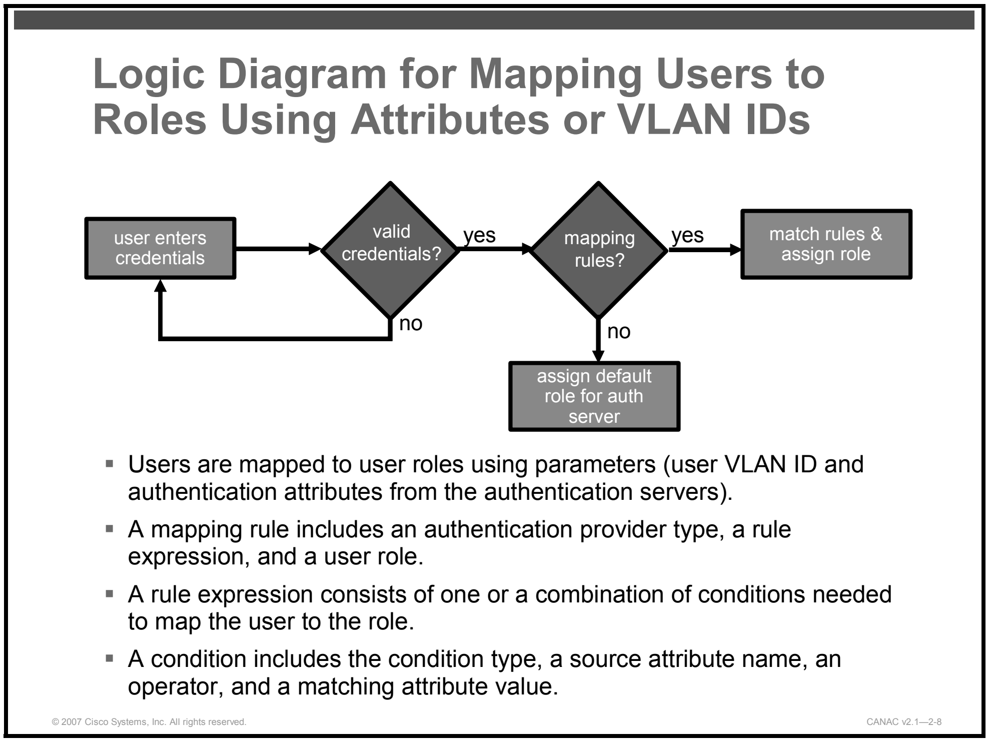
Step 5 From the Default Role drop-down menu, choose the role to assign to users who are authenticated by this provider. The role you choose is used if it is not overridden by a role assignment based on a MAC address or IP address.

Step 6 (Optional) In the Description field, enter a description for the authentication server.

Step 7 When you are finished, click the **Add Server** button. The authentication source is now configured and appears in the list of servers. From the list of servers, you can modify the settings for an authentication source by clicking the **Edit** button next to the source.

Mapping Users to User Roles

This topic describes how to map users to user roles when configuring external authentication.



Logic Diagram for Mapping Users to Roles Using Attributes or VLAN IDs

- Users are mapped to user roles using parameters (user VLAN ID and authentication attributes from the authentication servers).
- A mapping rule includes an authentication provider type, a rule expression, and a user role.
- A rule expression consists of one or a combination of conditions needed to map the user to the role.
- A condition includes the condition type, a source attribute name, an operator, and a matching attribute value.

CANAC v2.1—2-8

The Mapping Rules form can be used to map users into a user role based on these parameters:

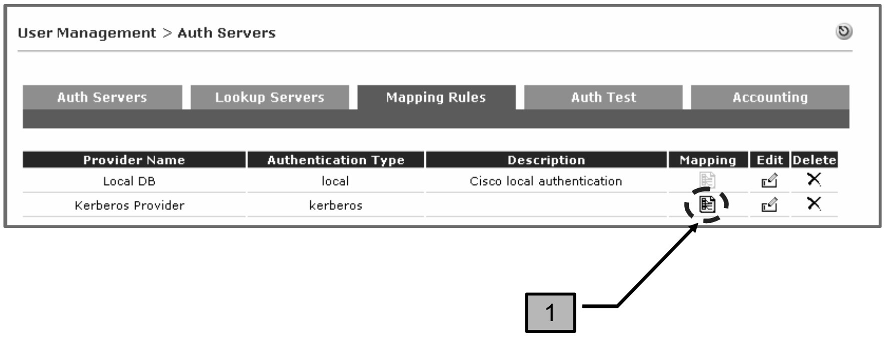
- The VLAN ID of user traffic originating from the untrusted side of the Cisco NAS (or any authentication server)
- Authentication attributes passed from LDAP and RADIUS authentication servers (and RADIUS attributes passed from Cisco VPN Concentrators)

The figure shows the mapping sequence that Cisco NAC Appliance performs to associate users with a role based on a VLAN ID value or another user-specific attribute passed by LDAP and RADIUS authentication sources.

The Cisco NAC Appliance allows you to specify complex Boolean operators when defining mapping rules for Kerberos, LDAP, and RADIUS authentication servers. Mapping rules are broken down into conditions. You can use Boolean operators to combine multiple user attributes and multiple VLAN IDs to map users into user roles. You can create mapping rules for a range of VLAN IDs, and you can make attribute matches case-insensitive to allow multiple conditions to be flexibly configured for a mapping rule.

A mapping rule consists of an authentication provider type, a rule expression, and the user role to map the user into. The rule expression consists of one condition or a combination of conditions that the user parameters must match to be mapped into the specified user role. A condition consists of a condition type, a source attribute name, an operator, and the attribute value against which the particular attribute is matched.

Configuring a Mapping Rule



Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication			✕
Kerberos Provider	kerberos				✕

Next steps →

To create a mapping rule, you first add and save conditions to configure a rule expression. After a rule expression is created, you can add the mapping rule to the authentication server.

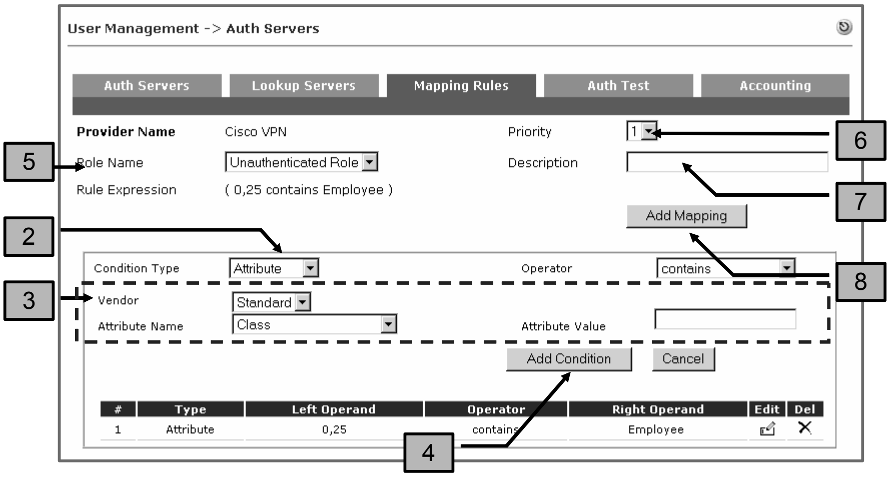
Mapping rules can be cascading. If a source has more than one mapping rule, the rules are evaluated in the order in which they appear in the mapping rules list. The role for the first mapping rule that is found positive is used. After a rule is met, other rules are not tested. If no rule is met, the default role for that authentication source is used.

To configure a mapping rule:

Step 1 Go to **User Management > Auth Servers > List of Servers** and click the **Mapping** button next to the authentication server that you want to configure. You can alternatively go to **User Management > Auth Servers > Mapping Rules** (as shown in the figure) and then select the authentication provider from the View drop-down menu.

The provider name that you selected in the Provider Name field sets the fields of the Mapping Rules form for that authentication server type. For example, the form only allows VLAN ID mapping rule configurations if you choose Kerberos, Windows NT, Windows NetBIOS SSO, or S/Ident as the authentication server types. The form allows VLAN ID or Attribute mapping rule configurations if you choose RADIUS, LDAP, or Cisco VPN SSO as the authentication server type.

Configuring a Mapping Rule (Cont.)



User Management -> Auth Servers

Provider Name: Cisco VPN

Priority: 1

Role Name: Unauthenticated Role

Description:

Rule Expression: (0,25 contains Employee)

Condition Type: Attribute

Operator: contains

Vendor: Standard

Attribute Name: Class

Attribute Value:

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,25	contains	Employee		✕

CANAC v2.1—2-10

Step 2 From the Condition Type drop-down menu, choose one of the following options to set the fields of the Condition form:

- **Attribute:** For LDAP, RADIUS, and Cisco VPN Server authentication providers only.
- **VLAN ID:** For all authentication server types.
- **Compound:** This condition type only appears after you have at least one condition statement added to the mapping rule. This condition type allows you to combine individual conditions using Boolean operators. You can combine VLAN ID conditions with the operators “equals”, “not equals”, and “belongs to”. You can combine attribute conditions alone, or mix VLAN ID and attribute conditions with the operators “AND”, “OR”, or “NOT”. For compound conditions, instead of associating attribute types to attribute values, you choose two existing conditions to associate together. These conditions become the Left and Right Operands for the compound statement.

Step 3 Configure the rest of the condition fields according to the type of authentication provider that you have.

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

Note If you want to add another condition, repeat Steps 2 through 4.

Step 5 From the Role Name drop-down menu, choose the user role that users are mapped to when they meet the conditions of the mapping rule.

Step 6 From the Priority drop-down menu, choose the numeric priority of the rule. The priority determines the order in which the rules are tested. The first rule that evaluates to true is used to assign the user a role.

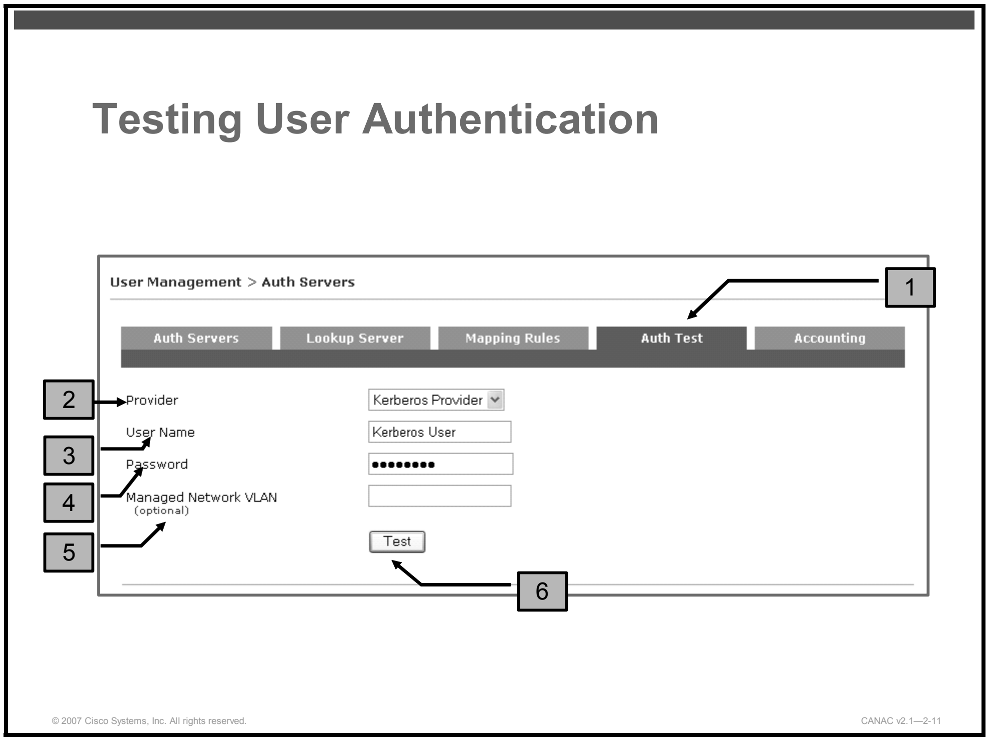
Step 7 (Optional) In the Description field, enter a description of the rule.

Step 8 Click the **Add Mapping** button to save your mapping rule configuration.

Note If you are creating a compound mapping rule, click the **Save Mapping** button to save a compound mapping rule. You have to either add or save the mapping or your configuration and conditions will not be saved.

Testing User Authentication

This topic describes how to test user authentication for configured external authentication providers.



Testing User Authentication

User Management > Auth Servers

Auth Servers | Lookup Server | Mapping Rules | Auth Test | Accounting

Provider	Kerberos Provider
User Name	Kerberos User
Password	•••••••••
Managed Network VLAN (optional)	

Test

CANAC v2.1—2-11

The Auth Test tab lets you test the authentication sources you configured against actual user credentials. This tab also shows the role assigned to the user.

To test authentication, complete these steps:

Step 1 Choose **User Management > Auth Servers** and choose the **Auth Test** tab.

Step 2 From the Provider field drop-down menu, choose the provider against which you want to test the user credentials.

Note If the provider does not appear in the list, make sure it is correctly configured on the List of Servers tab.

Step 3 In the User Name field, enter the username for the user you are testing.

Step 4 In the Password field, enter the user password.

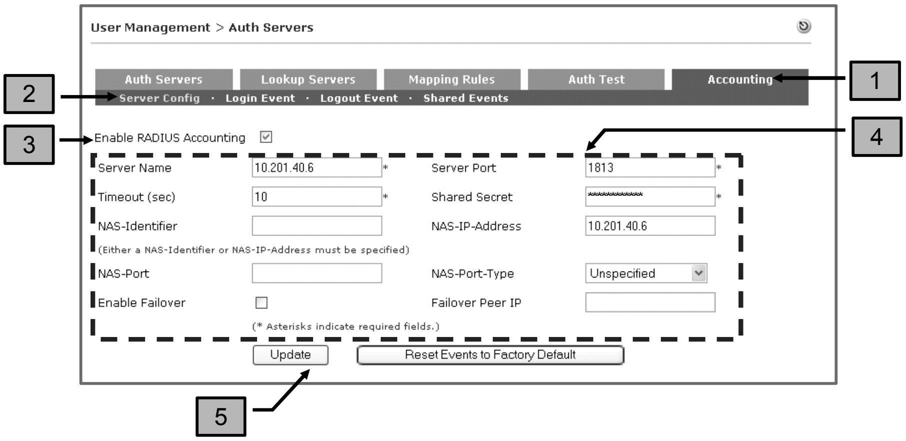
Step 5 (Optional) In the Managed Network VLAN field, enter the user VLAN ID value, if needed.

Step 6 Click the **Test** button. The test results (not shown) appear at the bottom of the form.

Configuring RADIUS Accounting for Users

This topic describes how to configure RADIUS accounting for users in a Cisco NAC Appliance network.

Enabling RADIUS Accounting for Users



User Management > Auth Servers

Enable RADIUS Accounting	☑		
Server Name	10.201.40.6 *	Server Port	1813 *
Timeout (sec)	10 *	Shared Secret	************ *
NAS-Identifier		NAS-IP-Address	10.201.40.6
(Either a NAS-Identifier or NAS-IP-Address must be specified)			
NAS-Port		NAS-Port-Type	Unspecified
Enable Failover	☐	Failover Peer IP	

(* Asterisks indicate required fields.)

Auth Servers
Lookup Servers
Mapping Rules
Auth Test
Accounting
Server Config · Login Event · Logout Event · Shared Events
Update
Reset Events to Factory Default
1
2
3
4
5

CANAC v2.1—2-12

You can configure the Cisco NAM to send accounting messages to a RADIUS accounting server. The Cisco NAM sends a "Start" accounting message when a user logs in to the network and sends a "Stop" accounting message when the user logs out of the system (or is logged out or timed out). This feature allows you to account for user time and other attributes on the network.

Cisco NAC Appliance Release 3.5 added additional control over which data is sent in accounting packets. You can customize the data to be sent for login events, logout events, or shared events (login and logout events).

To enable RADIUS accounting for users in a network, complete these steps:

Step 1 Choose **User Management > Auth Servers** and click the **Accounting** tab.

Step 2 Click the **Server Config** submenu link. The RADIUS accounting form appears.

Step 3 Check the **Enable RADIUS Accounting** check box to enable the Cisco NAM to send accounting information to the Cisco RADIUS accounting server.

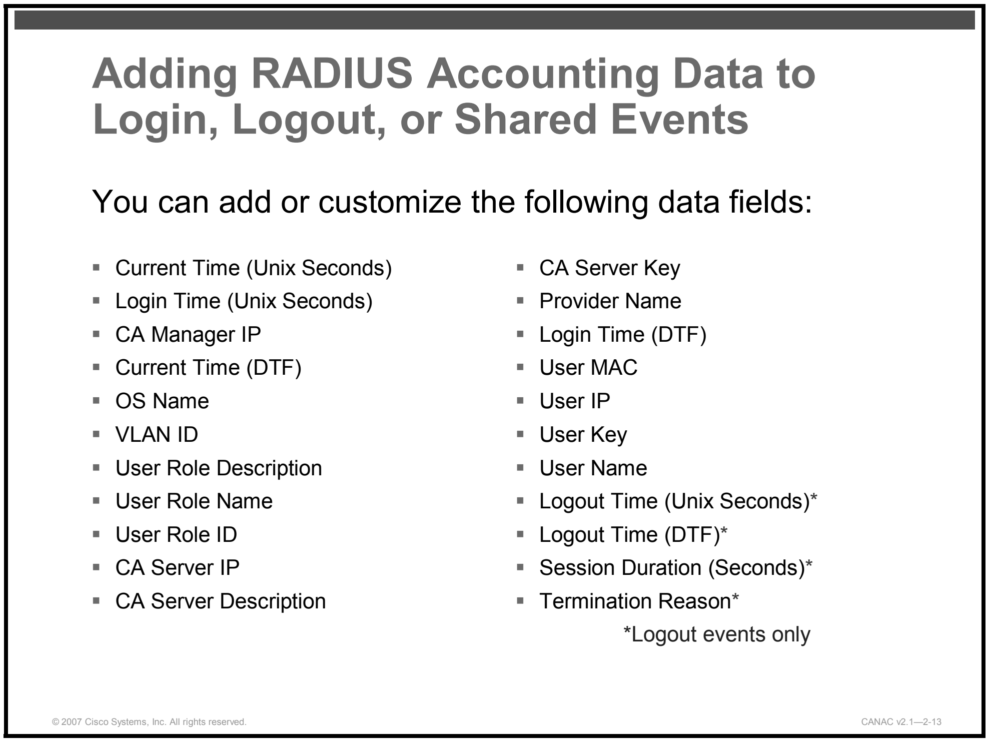
Step 4 Enter values for the fields in the RADIUS accounting form:

- **Server Name:** The fully qualified host name (for example, auth.cisco.com) or IP address of the RADIUS accounting server.
- **Server Port:** The port number on which the RADIUS server is listening. The Server Name and Server Port are used to direct accounting traffic to the accounting server.

- **Timeout (sec):** Specifies how long to attempt to retransmit a failed packet.
- **Shared Secret:** The shared secret used to authenticate the Cisco NAM accounting client with the specified RADIUS accounting server.
- **NAS-Identifier:** The NAS-Identifier value to be sent with all RADIUS accounting packets. Either a NAS-Identifier or a NAS-IP-Address must be specified to send the packets.
- **NAS-IP-Address:** The NAS-IP-Address value to be sent with all RADIUS accounting packets. Either a NAS-IP-Address or a NAS-Identifier must be specified to send the packets.
- **NAS-Port:** The NAS-Port value to be sent with all RADIUS accounting packets.
- **NAS-Port-Type:** The NAS-Port-Type value to be sent with all RADIUS accounting packets.
- **Enable Failover:** Checking this check box enables you to send a second accounting packet to a RADIUS failover peer IP if the primary RADIUS accounting server response times out.
- **Failover Peer IP:** The IP address of the failover RADIUS accounting server.

Step 5 Click the **Update** button to update the server configuration.

Tip To restore the Cisco NAM to the factory default accounting configuration, click the **Reset Events to Factory Default** button and then click **OK** in the confirmation dialog box that appears. It is important to back up your database before restoring any default settings.



Adding RADIUS Accounting Data to Login, Logout, or Shared Events

You can add or customize the following data fields:

- Current Time (Unix Seconds)
- Login Time (Unix Seconds)
- CA Manager IP
- Current Time (DTF)
- OS Name
- VLAN ID
- User Role Description
- User Role Name
- User Role ID
- CA Server IP
- CA Server Description
- CA Server Key
- Provider Name
- Login Time (DTF)
- User MAC
- User IP
- User Key
- User Name
- Logout Time (Unix Seconds)*
- Logout Time (DTF)*
- Session Duration (Seconds)*
- Termination Reason*

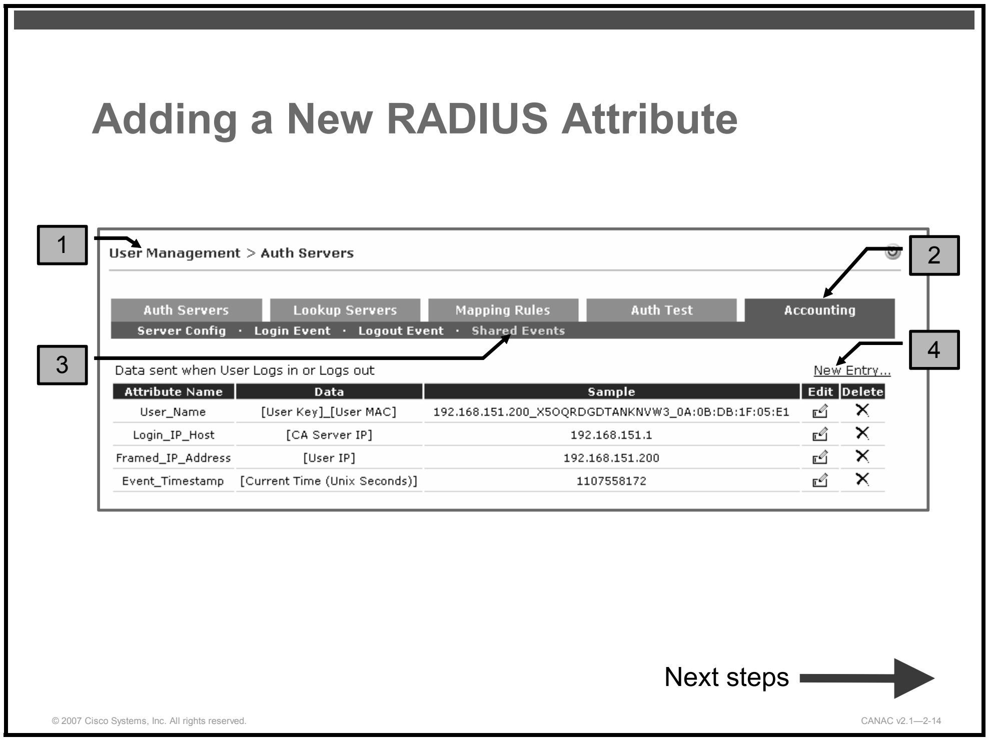
*Logout events only

For greater control over the data that is sent in accounting packets, you can add or customize the RADIUS accounting data that is sent for login events, logout events, or shared events (data sent for both login and logout events). The following data fields and explanations apply to all events (login, logout, or shared):

- **Current Time (Unix Seconds):** The time when the event occurred
- **Login Time (Unix Seconds):** The time when the user logged in
- **CA Manager IP:** IP address of the Cisco NAM
- **Current Time (DTF):** Current time in date-time format (DTF)
- **OS Name:** Operating system (OS) of the user
- **Vlan ID:** VLAN ID that the user session was created with
- **User Role Description:** Description of the user role for the user
- **User Role Name:** Name of the user role for the user
- **User Role ID:** Role ID that uniquely identifies the user role
- **CA Server IP:** IP of the Cisco NAS that the user logged in to
- **CA Server Description:** Description of the Cisco NAS that the user logged in to
- **CA Server Key:** Key of the Cisco NAS
- **Provider Name:** Authentication provider for the user
- **Login Time (DTF):** Login time of the user in DTF
- **User MAC:** MAC address for the user
- **User IP:** IP address for the user
- **User Key:** Key that the user logged in with
- **User Name:** User account name

Four data fields apply to logout events only and are not sent for login or shared events:

- **Logout Time (Unix Seconds):** Logout time of the user in Unix seconds
- **Logout Time (DTF):** Logout time of the user in DTF
- **Session Duration (Seconds):** Duration of the session in seconds
- **Termination Reason:** Output of the Acct_Terminate_Cause RADIUS attribute



Adding a New RADIUS Attribute

User Management > Auth Servers

Data sent when User Logs in or Logs out

Attribute Name	Data	Sample	Edit	Delete
User_Name	[User Key]_[User MAC]	192.168.151.200_X5OQRDGDTANKNVW3_0A:0B:DB:1F:05:E1		✕
Login_IP_Host	[CA Server IP]	192.168.151.1		✕
Framed_IP_Address	[User IP]	192.168.151.200		✕
Event_Timestamp	[Current Time (Unix Seconds)]	1107558172		✕

CANAC v2.1—2-14

The process used to configure a RADIUS attribute with customized data for a shared event is the same as the process used to customize data for login and logout events. Only the submenu link that you choose changes.

To add new data to a RADIUS attribute for a shared event, complete these steps:

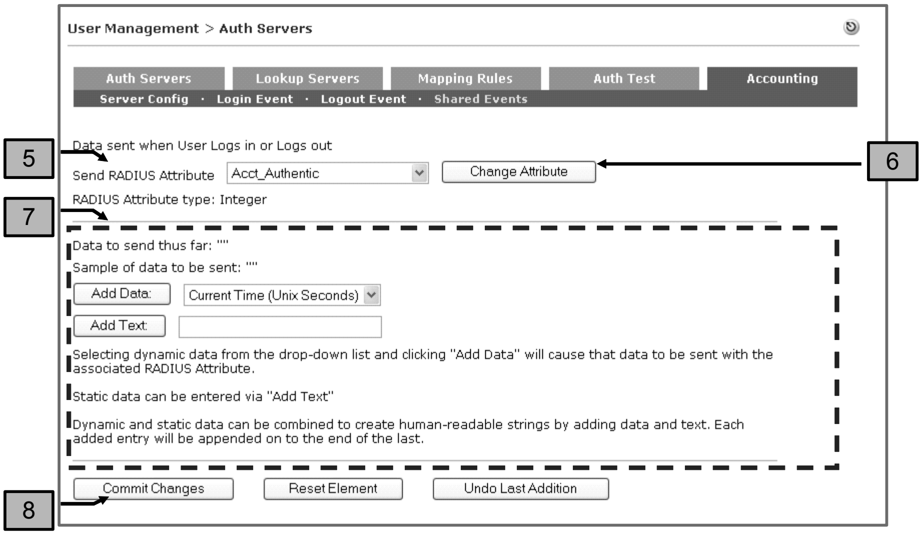
Step 1 Choose **User Management > Auth Servers.**

Step 2 Click the **Accounting** tab.

Step 3 Click the **Shared Events** (or **Login Event** or **Logout Event**) submenu link to bring up the appropriate page.

Step 4 Click the **New Entry** link at the right side of the page. The Add form appears.

Adding a New RADIUS Attribute (Cont.)



User Management > Auth Servers

Data sent when User Logs in or Logs out

Send RADIUS Attribute: Acct_Authentic

RADIUS Attribute type: Integer

Data to send thus far: ""

Sample of data to be sent: ""

Add Data: Current Time (Unix Seconds)

Selecting dynamic data from the drop-down list and clicking "Add Data" will cause that data to be sent with the associated RADIUS Attribute.

Static data can be entered via "Add Text"

Dynamic and static data can be combined to create human-readable strings by adding data and text. Each added entry will be appended on to the end of the last.

CANAC v2.1—2-15

Step 5 From the **Send RADIUS Attribute** drop-down menu, choose a RADIUS attribute (there are 253 choices).

Step 6 Click the **Change Attribute** button to update the RADIUS attribute type. The type, such as “String” or “Integer,” appears in the RADIUS Attribute Type field.

Step 7 Configure the type of data to send with the attribute. There are three options:

- **Send static data:** In this case, enter the text to be added in the Add Text field and click the **Add Text** button. Every time a user logs in and logs out, the RADIUS attribute that is selected is sent with the static data that you have entered.
- **Send dynamic data:** In this case, select one of the 14 dynamic data variables (or one of the 18 variables for logout events) from the drop-down menu and click the **Add Data** button. Every time a user logs in and logs out, the dynamic data that is selected is replaced with the appropriate value when sent.
- **Send static and dynamic data:** In this case, a combination of static and dynamic data is sent. An example of data sent in this case is: User: [User Name] logged in at: [Login Time DTF] from certificate authority (CA) server [CA Server Description]

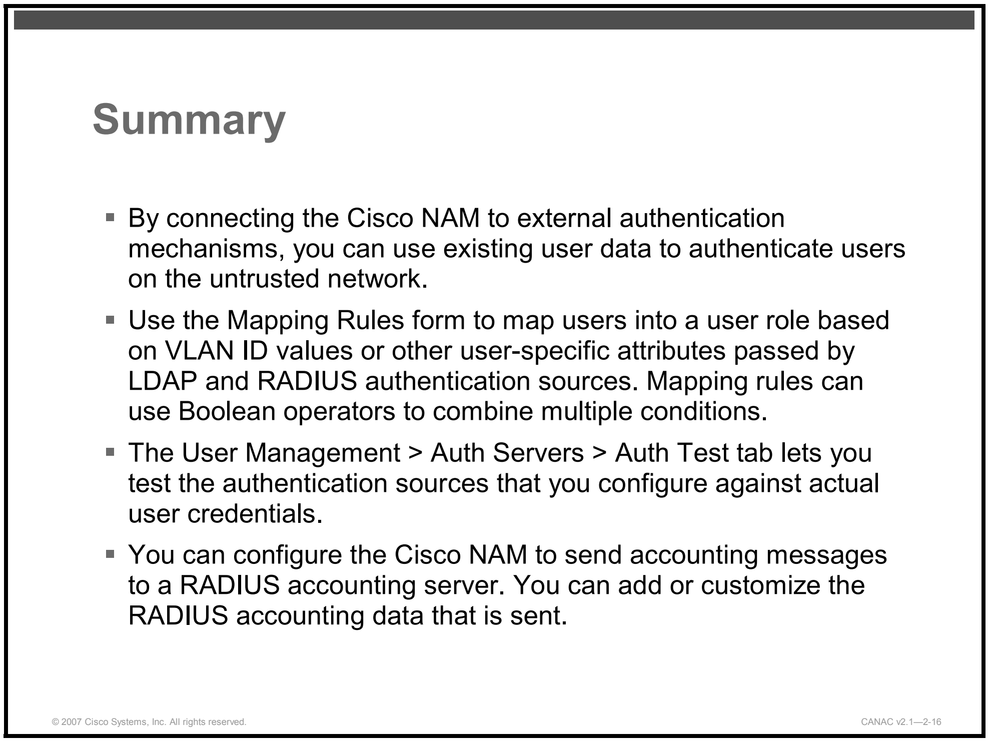
  As data is added, the Data to send thus far field displays all the data types that have been selected to send with the attribute. The Sample of data to be sent field illustrates how the data will appear.

Step 8 Click the **Commit Changes** button to save your changes.

Note To reset the form, click **Reset Element**. To remove the last entry added to the Data to send thus far field, click **Undo Last Addition**.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- By connecting the Cisco NAM to external authentication mechanisms, you can use existing user data to authenticate users on the untrusted network.
- Use the Mapping Rules form to map users into a user role based on VLAN ID values or other user-specific attributes passed by LDAP and RADIUS authentication sources. Mapping rules can use Boolean operators to combine multiple conditions.
- The User Management > Auth Servers > Auth Test tab lets you test the authentication sources that you configure against actual user credentials.
- You can configure the Cisco NAM to send accounting messages to a RADIUS accounting server. You can add or customize the RADIUS accounting data that is sent.

Lesson 3

Configuring DHCP on the Cisco NAS

Overview

DHCP is a broadcast protocol for dynamically allocating IP addresses to computers on a network. When a client computer attempts to join a DHCP-enabled network, the client broadcasts an address request message. A DHCP server on the network responds to the request, and after several exchanges, an IP address is negotiated and delivered to the client. This lesson describes how to set up the Cisco NAC Appliance Server (NAS) for a DHCP-enabled network.

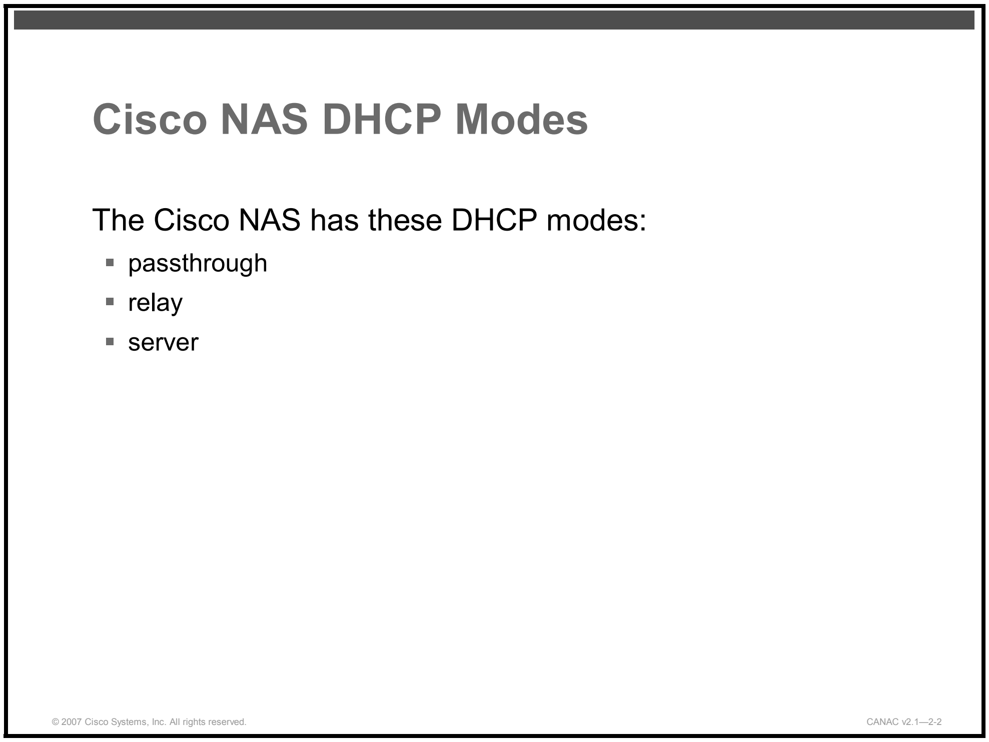
Objectives

Upon completing this lesson, you will be able to describe how to configure the Cisco NAS for a DHCP-enabled network. This ability includes being able to meet these objectives:

- Describe Cisco NAS modes of operation for a DHCP-enabled network
- Describe how to enable the Cisco NAS DHCP module
- Describe how to configure the Cisco NAS to provide DHCP services
- Describe how to manage generated subnets on the Cisco NAS
- Describe how to configure the Cisco NAS to provide reserved IP addresses
- Describe how to configure user-specified DHCP options on the Cisco NAS

Cisco NAS DHCP Modes

This topic describes the Cisco NAS modes of operation for a DHCP-enabled network.



Cisco NAS DHCP Modes

The Cisco NAS has these DHCP modes:

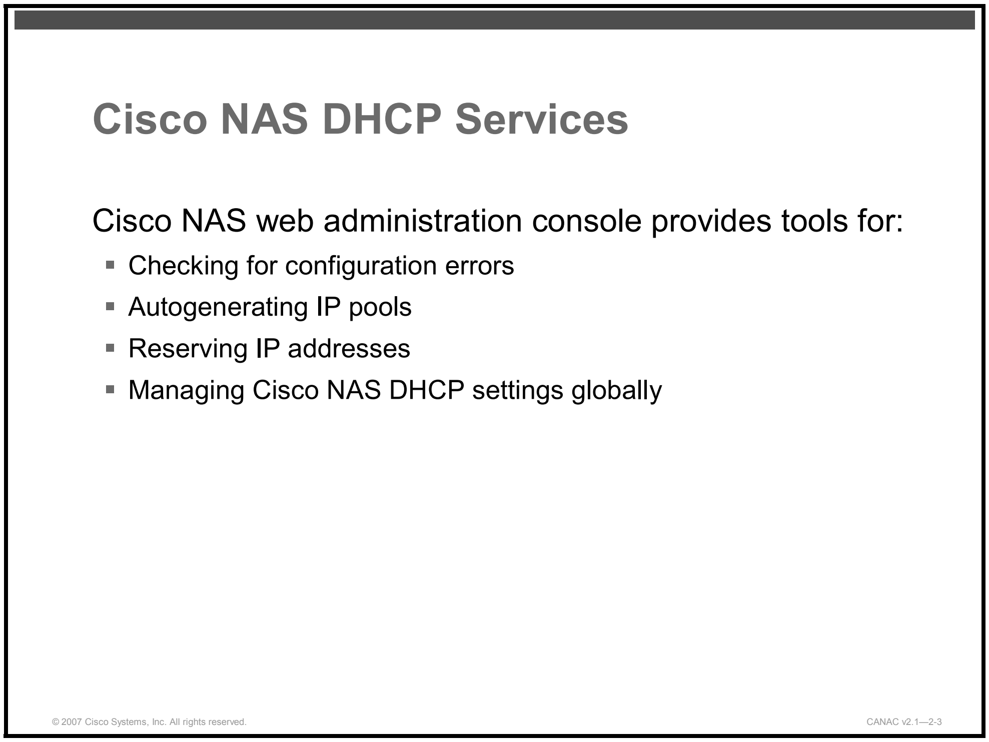
- passthrough
- relay
- server

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—2-2

The Cisco NAS provides the services of a full-featured DHCP server when in real-IP gateway mode. The Cisco NAS can allocate addresses from a single IP pool or from multiple pools across many subnets, and can assign static IP addresses to particular client devices. The Cisco NAS can operate in one of three DHCP modes:

- **Passthrough:** DHCP passthrough is the only mode that can be used when the Cisco NAS is configured as a virtual gateway. In DHCP passthrough mode, a virtual gateway Cisco NAS propagates the DHCP broadcast messages across its interfaces without modification.
- **Relay:** In DHCP relay mode, a real-IP gateway Cisco NAS forwards messages from clients to another DHCP server.
- **Server:** In server mode, a real-IP gateway Cisco NAS acts as the DHCP server and allocates client IP addresses for the managed (untrusted) network performing DHCP services for managed clients.

Note Cisco NAC Appliance references a Network Address Translation (NAT) deployment of a Cisco NAS. The NAT gateway deployment option is only for student labs and other nonproduction lab environments.



Cisco NAS DHCP Services

Cisco NAS web administration console provides tools for:

- Checking for configuration errors
- Autogenerating IP pools
- Reserving IP addresses
- Managing Cisco NAS DHCP settings globally

CANAC v2.1—2-3

Extensive configuration checking in the web administration console helps to ensure that you detect configuration errors during configuration rather than during deployment. The administration console includes tools for autogenerating IP address pools, making it easier to create many pools at once.

Autogenerating IP pools as a response to heightened virus activity can help to protect your network. By segmenting your network into many small subnets, you can isolate clients from each other. Because clients cannot communicate directly across subnets, all traffic between them is routed through the Cisco NAS, limiting the ability of worms to propagate over peer-to-peer connections.

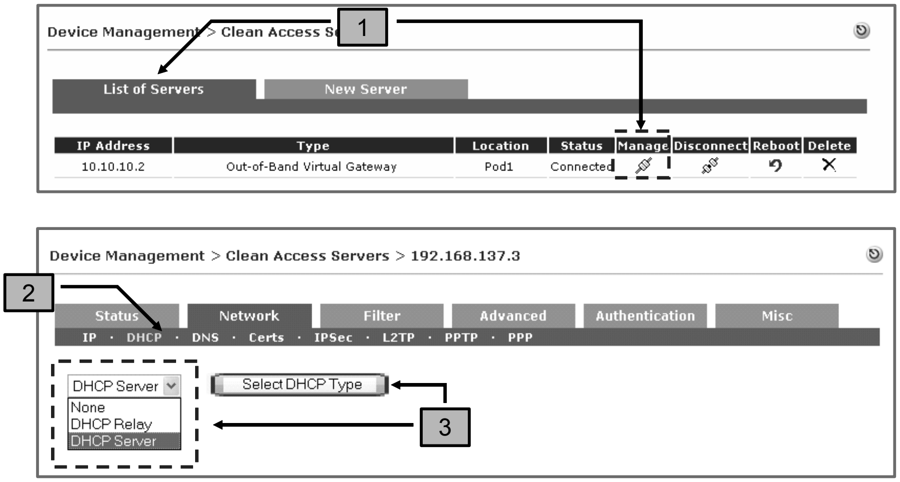
When you generate subnetted IP address pools, the Cisco NAS is automatically configured as the router for the subnet. An Address Resolution Protocol (ARP) entry for the subnet is also automatically generated. For static addresses, you can reserve a particular IP address for a particular device by using the MAC address of the device.

You can manage Cisco NAS DHCP settings globally. The Global Action form allows you to change fields on all DHCP elements of a particular Cisco NAS. For example, if you have 300 managed subnets and IP pools, you can change the Domain Name System (DNS) server in all of them at once.

Enabling the DHCP Module

This topic describes how to enable the Cisco NAS DHCP module.

Enabling the DHCP Module



Device Management > Clean Access Se...

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.10.10.2	Out-of-Band Virtual Gateway	Pod1	Connected				

Device Management > Clean Access Servers > 192.168.137.3

CANAC v2.1—2-4

To enable the DHCP operation mode on a per-Cisco NAS basis, complete these steps:

Step 1 From Device Management > Clean Access Servers > List of Servers, click the **Manage** button next to the Cisco NAS that you want to enable for DHCP operation.

Step 2 In the Network tab, click the **DHCP** link to open the DHCP form.

Step 3 From the DHCP Type drop-down menu, choose an option and click the **Select DHCP Type** button.

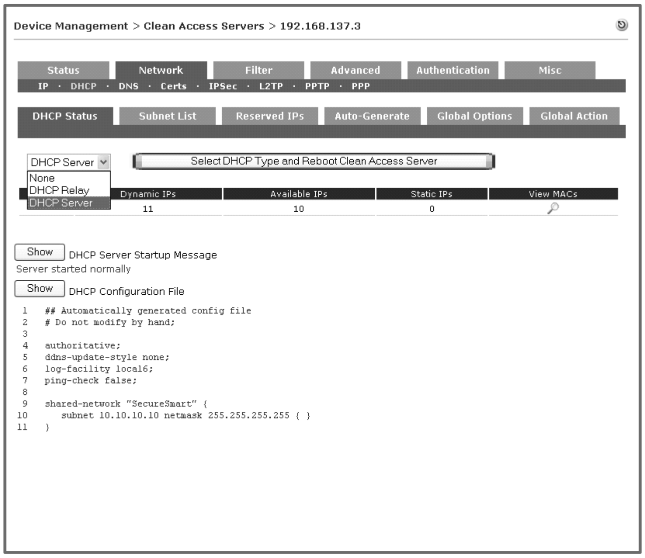
— The None selection appears by default. When the None DHCP type is selected, the Cisco NAS propagates DHCP broadcast messages across its interfaces without change. If a DHCP server already exists on the trusted network, keep the Cisco NAS configured with the None DHCP type mode.

— Selecting **DHCP Relay** or **DHCP Server** from the drop-down menu displays a different form on which the **Select DHCP Type** and the **Reboot Cisco NAS** buttons appear.

— When you choose DHCP Server type for the Cisco NAS, the DHCP Status, Subnet List, Reserved IPs, Auto-Generate, and Global Options subtabs appear.

Note If you choose the DHCP server option, you must reboot the Cisco NAS to switch to a different DHCP type for the Cisco NAS.

Viewing DHCP Server Startup Messages



Dynamic IPs	Available IPs	Static IPs	View MACs
11	10	0	🔍

DHCP Server Startup Message

Server started normally

DHCP Configuration File

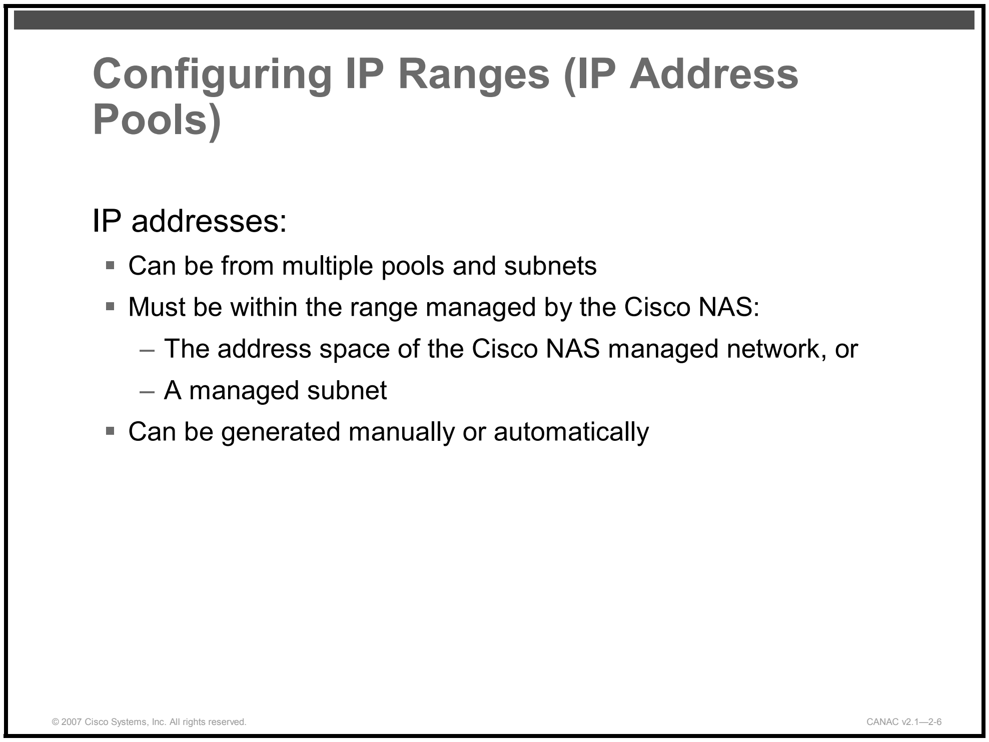
```
## Automatically generated config file
# Do not modify by hand;

authoritative;
ddns-update-style none;
log-facility local6;
ping-check false;

shared-network "SecureSmart" {
   subnet 10.10.10.10 netmask 255.255.255.255 { }
}
```

The DHCP Status tab includes these enable buttons:

- [**Show**] or [**Hide**] **DHCP Server Startup Message:** When this button is clicked, the last DHCP server startup message appears. If the server does not start, an error message appears.
- [**Show**] **or** [**Hide**] **DHCP Configuration File:** When this button is clicked, the DHCP configuration file appears. In some cases, the startup message shows an error for a particular line of the configuration. Clicking this button allows you to view the configuration file line-by-line for error-checking.

Configuring IP Ranges

This topic describes how to configure the Cisco NAS to provide DHCP services.



Configuring IP Ranges (IP Address Pools)

IP addresses:

- Can be from multiple pools and subnets
- Must be within the range managed by the Cisco NAS:
  - The address space of the Cisco NAS managed network, or
  - A managed subnet
- Can be generated manually or automatically

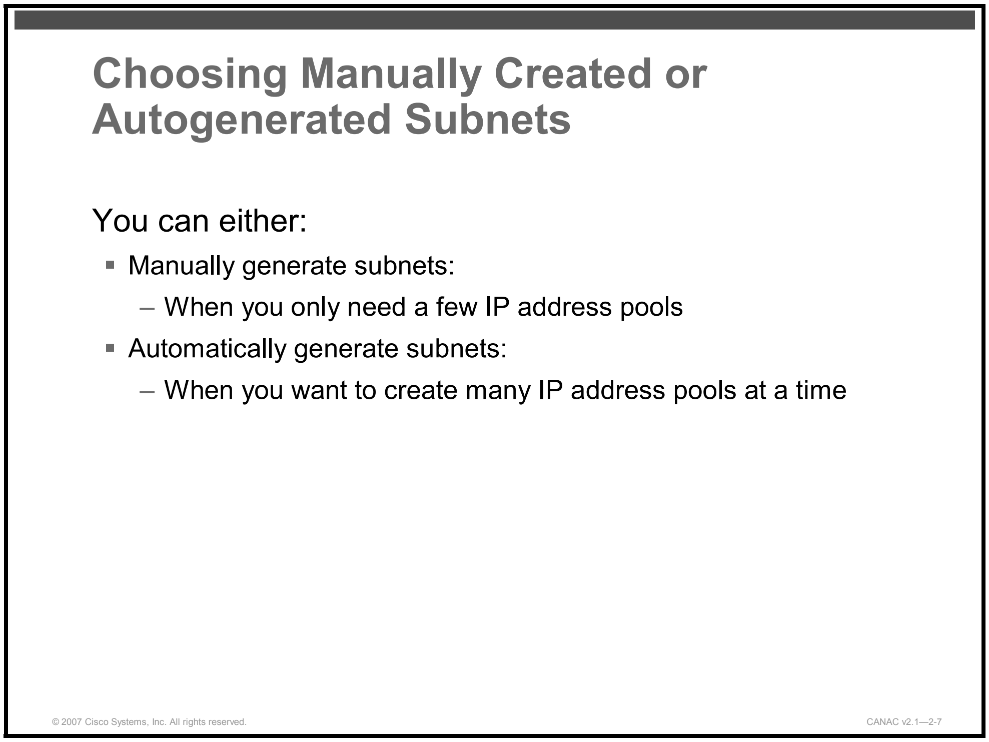
CANAC v2.1—2-6

To set up the Cisco NAS to provide DHCP services, you must first configure the range of IP addresses to be allocated to clients (the IP address pool). In addition, you can specify the types of network information, such as DNS addresses, that is sent to client machines with each IP address.

The Cisco NAS can allocate addresses from multiple pools and subnets. However, allocated addresses must be from within one of these ranges managed by the Cisco NAS:

- The address space of the managed network for the Cisco NAS (as set in the IP form of the Network tab)
- A managed subnet specified in the Managed Subnet form of the Advanced tab

You can generate IP addresses manually or automatically. However, if you try to create an address pool from a subnet that is not managed, an error message notifying you of the condition appears in the administration console and the pool is not created.



Choosing Manually Created or Autogenerated Subnets

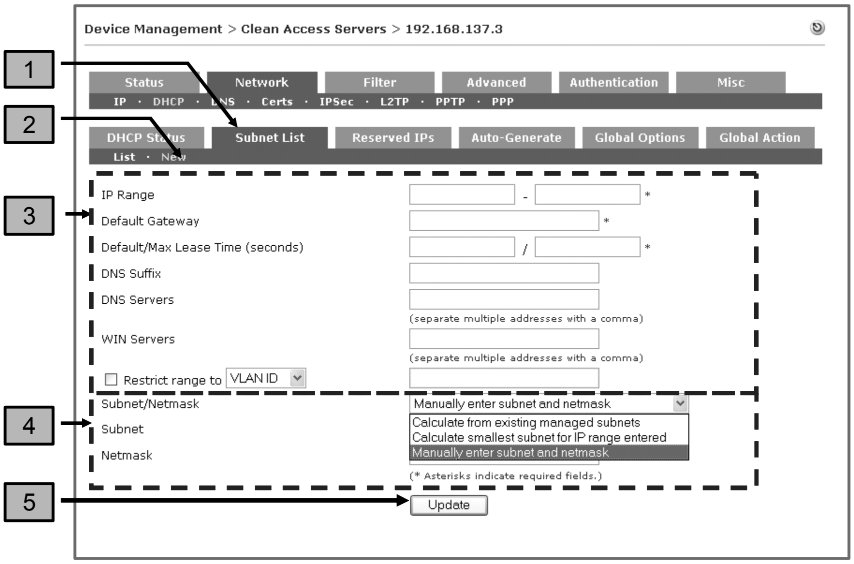
You can either:

- Manually generate subnets:
  - When you only need a few IP address pools
- Automatically generate subnets:
  - When you want to create many IP address pools at a time

If you only need a few IP address pools, you can create subnets manually.

You can automatically generate subnets to create many IP address pools at one time. Creating a large number of IP pools of a small size, from which only a few addresses can be assigned, will help protect your network. By isolating clients into small subnets, you limit the ability of peers to communicate directly with one another, and thereby prevent security threats such as worms from proliferating across peer connections.

Creating IP Pools Manually



Device Management > Clean Access Servers > 192.168.137.3

IP Range - *

Default Gateway *

Default/Max Lease Time (seconds) / *

DNS Suffix

DNS Servers (separate multiple addresses with a comma)

WIN Servers (separate multiple addresses with a comma)

□ Restrict range to VLAN ID

Subnet/Netmask: Manually enter subnet and netmask

- Calculate from existing managed subnets
- Calculate smallest subnet for IP range entered
- Manually enter subnet and netmask

Subnet

Netmask

(* Asterisks indicate required fields.)

CANAC v2.1—2-8

To create an IP pool manually, you must also define the subnet in which the pool resides. There are these three ways to configure the subnet address and netmask values for a manually generated pool:

- Enter the subnet address directly, as an IP address and netmask.
- Have the administration console generate the smallest possible subnet based on the IP range that you enter.
- Have the administration console calculate the values from the list of subnets currently managed by the Cisco NAS.

These steps create an IP pool range:

Step 1 In the DHCP form, click the **Subnet List** tab.

Step 2 Click the **New** link. The new IP pool form appears.

Step 3 Enter values for these fields:

- **IP Range:** Enter the IP address pool to assign to clients. Provide a range of addresses that are not currently assigned in your environment.
- **Default Gateway:** Enter the IP address of the default gateway that is passed to clients. This should be the untrusted interface address of the Cisco NAS.
- **Default/Max Lease Time (seconds):** Enter the amount of time that the IP address is assigned to the client (if the client does not request a particular lease time) and the maximum amount of time for which a lease can be granted. If the client requests a lease for a time that is greater than the defined maximum time, the maximum lease time is used.
- **DNS Suffix:** Enter the DNS suffix information to pass to clients along with the IP address.

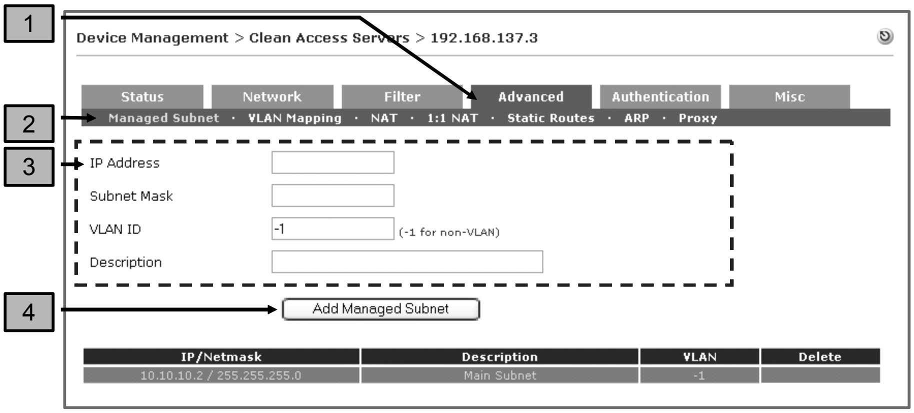
- **DNS Servers:** Enter the address of one or more DNS servers in the client environment. Multiple addresses should be separated by commas.
- **WIN Servers:** Enter the address of one or more WIN servers in the client environment. Multiple addresses should be separated by commas.
- **Restrict Range to VLAN ID:** If selected, specify the VLAN identifier in the field. Clients not associated with the specified VLAN cannot receive addresses from this IP pool. A VLAN ID can be any number between 0 and 4095.

Step 4 From the Subnet/Netmask list, choose how you want the subnet address to be specified. These are the choices:

- **Calculate from Existing Managed Subnets:** When this choice is selected, the administration console determines what to use for the subnet and netmask values based on the configuration in the Managed Subnet form (in the Advanced tab). The administration console calculates the network address by applying the netmask to the gateway address for each managed subnet.
- **Calculate Smallest Subnet for IP Range Entered:** When this choice is selected, the administration console determines the subnet and netmask values based on the IP address range that you entered.
- **Manually Enter Subnet and Netmask:** You can specify the desired network address and netmask manually. If this choice is selected, the Subnet and Netmask fields appear at the bottom of the form.
- **Inherit Scoped Global Options:** This field is only visible if DHCP options are enabled (the field is then turned on by default). If this field is disabled, the scoped global options configured in the Global Options tab are not inherited.

Step 5 Click **Update** when you are finished. If there are errors in the configuration, warning messages appear. Follow the instructions to correct the settings.

Auto-Generating IP Pools in a Managed Subnet


1
2
3
4
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Add Managed Subnet

Device Management > Clean Access Servers > 192.168.137.3

IP Address

Subnet Mask

VLAN ID -1 (-1 for non-VLAN)

Description

IP/Netmask	Description	VLAN	Delete
10.10.10.2 / 255.255.255.0	Main Subnet	-1	

You must ensure that the IP pools are in the range of a managed subnet.

CANAC v2.1—2-9

Before you can autogenerate IP addresses, you must ensure that the IP pools that you want to add are in the range of a managed subnet. These steps add the managed subnet:

Step 1 From the Device Management > Clean Access Server > [IP address] menu, click the **Advanced** tab.

Step 2 Click the **Managed Subnet** link. The Managed Subnet form appears.

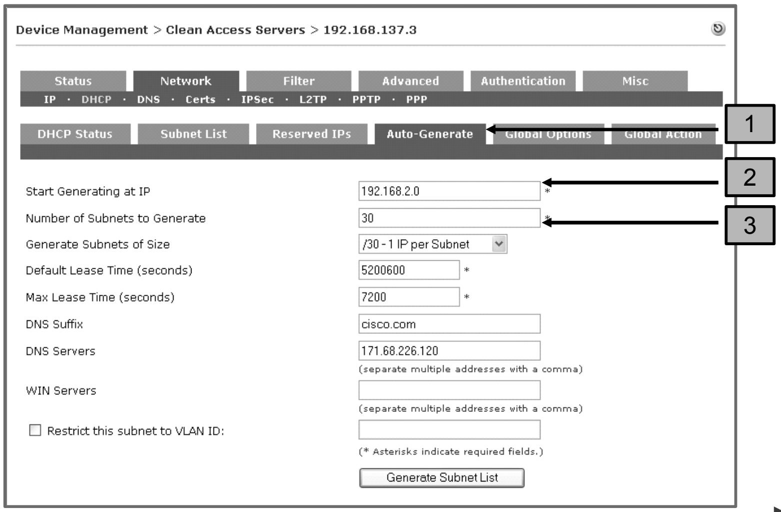
Step 3 Enter values for these fields:

- **IP Address**: The gateway address for the subnet (the address used by the Cisco NAS to route the subnet)
- **Subnet Mask:** The subnet mask for the gateway address
- **VLAN ID:** The VLAN identifier value to be assigned to this subnet
- **Description:** (Optional) A description for the managed subnet

Note When adding a managed subnet, the IP address field that you configure should be the gateway address for the subnet and *not* the network address. The Cisco NAC Appliance Manager (NAM) calculates the network address by applying the subnet mask to the gateway address.

Step 4 When you are finished, click the **Add Managed Subnet** button. The new subnet appears in the list of subnets at the bottom of the form.

Auto-Generating IP Pools and Subnets



Start Generating at IP: 192.168.2.0 *

Number of Subnets to Generate: 30 *

Generate Subnets of Size: /30 - 1 IP per Subnet

Default Lease Time (seconds): 5200600 *

Max Lease Time (seconds): 7200 *

DNS Suffix: cisco.com

DNS Servers: 171.68.226.120
(separate multiple addresses with a comma)

WIN Servers:
(separate multiple addresses with a comma)

☐ Restrict this subnet to VLAN ID:

(* Asterisks indicate required fields.)

Next steps

By automatically generating subnets, you can quickly divide your network into small segments. Segmenting your network into small subnets can be an effective security measure in response to a worm attack, because a network consisting of many small subnets (with one host per subnet possible) limits the ability of clients to engage in peer-to-peer interaction.

Caution The recommended maximum number of subnets per Cisco NAS is 1000. If the Cisco NAS has sufficient memory (more than 1GB), up to 2500 subnets can be configured. Do not exceed the recommended limit if this would place an excessive burden on system resources, particularly server memory.

To create an autogenerated subnet, complete these steps:

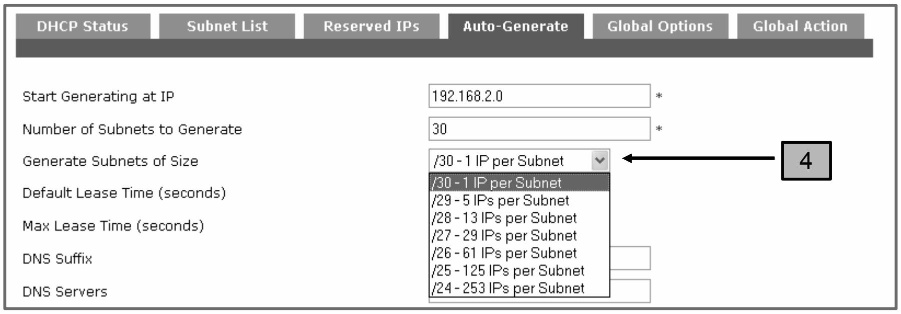
Step 1 Choose **Network > DHCP > Auto-Generate**. The Auto-Generate form appears.

Step 2 In the Start Generating at IP field, enter the first IP address of the range to be generated.

Note As previously mentioned, the number you enter is used as the network address for the first subnet, and the next number is used as the router address. The third number is the first address that is able to be leased to clients.

Step 3 In the Number of Subnets to Generate field, type the number of subnets that you want to generate. The maximum recommended number is 1000. Exceeding this number can impose a burden on the system resources of the server.

Auto-Generating IP Pools and Subnets (Cont.)



Start Generating at IP: 192.168.2.0 *

Number of Subnets to Generate: 30 *

Generate Subnets of Size: /30 - 1 IP per Subnet

Default Lease Time (seconds)

Max Lease Time (seconds)

DNS Suffix

DNS Servers

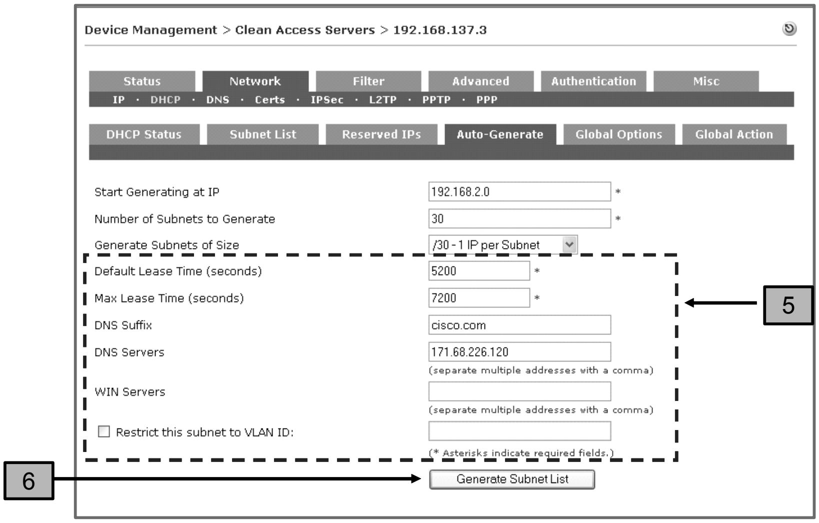
Next steps

Step 4 From the Generate Subnets of Size drop-down menu, choose the size of each subnet. Subnet sizes are presented in classless interdomain routing (CIDR) format (such as /30). The drop-down menu also lists the corresponding number of available host addresses per subnet for each CIDR prefix. For each range, three addresses are automatically reserved and cannot be allocated to clients. These are the three addresses:

- The network address of the subnet
- The router address (for the Cisco NAS)
- The broadcast address

Note A /30 size subnet has four addresses, but only one IP is available for hosts.

Auto-Generating IP Pools and Subnets (Cont.)



Device Management > Clean Access Servers > 192.168.137.3

Start Generating at IP	192.168.2.0 *
Number of Subnets to Generate	30 *
Generate Subnets of Size	/30 - 1 IP per Subnet
Default Lease Time (seconds)	5200 *
Max Lease Time (seconds)	7200 *
DNS Suffix	cisco.com
DNS Servers	171.68.226.120 (separate multiple addresses with a comma)
WIN Servers	 (separate multiple addresses with a comma)
□ Restrict this subnet to VLAN ID:	 (* Asterisks indicate required fields.)

Next steps

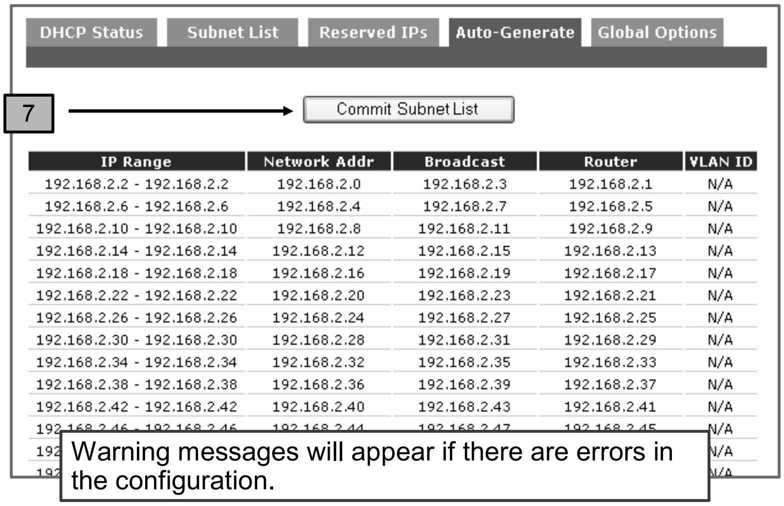
CANAC v2.1—2-12

Step 5 Provide values for these remaining fields:

- **Default Lease Time (seconds):** Enter the amount of time that the IP address is assigned to the client if the client does not request a particular lease time.
- **Max Lease Time (seconds):** Enter the maximum amount of time that a lease can be reserved. If the client requests a lease for a time that is greater than the maximum lease time you enter, this maximum lease time is used.
- **DNS Suffix:** Enter the DNS suffix information to pass to clients with the address lease.
- **DNS Servers:** Enter the address of one or more DNS servers in the client environment. Multiple addresses should be separated by commas.
- **WIN Servers:** Enter the address of one or more Windows servers in the client environment. Multiple addresses should be separated by commas.
- **Restrict this Subnet to VLAN ID:** Clients not associated with the specified VLAN cannot receive addresses from this IP pool. A VLAN ID can be any number between 0 and 4095.
- **Inherit Scoped Global Options:** If DHCP options are enabled, this field appears and is enabled by default. If DHCP options are enabled and this field is disabled, the scoped global options configured in the Global Options tab are not inherited.

Step 6 When you are finished, generate a preliminary list of subnets by clicking **Generate Subnet List**. If there are errors in the values provided, error messages appear. If the subnet based on your address is not properly aligned, the interface suggests the closest legal starting IP address for your range.

Auto-Generating IP Pools and Subnets (Cont.)



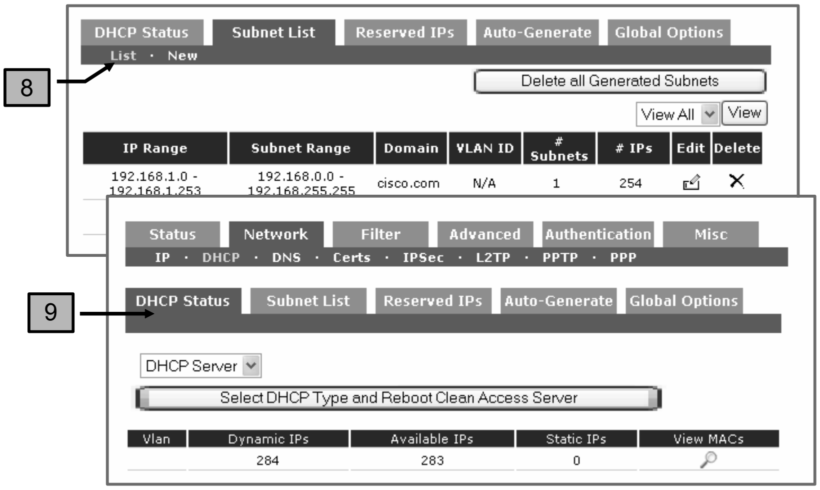
IP Range	Network Addr	Broadcast	Router	VLAN ID
192.168.2.2 - 192.168.2.2	192.168.2.0	192.168.2.3	192.168.2.1	N/A
192.168.2.6 - 192.168.2.6	192.168.2.4	192.168.2.7	192.168.2.5	N/A
192.168.2.10 - 192.168.2.10	192.168.2.8	192.168.2.11	192.168.2.9	N/A
192.168.2.14 - 192.168.2.14	192.168.2.12	192.168.2.15	192.168.2.13	N/A
192.168.2.18 - 192.168.2.18	192.168.2.16	192.168.2.19	192.168.2.17	N/A
192.168.2.22 - 192.168.2.22	192.168.2.20	192.168.2.23	192.168.2.21	N/A
192.168.2.26 - 192.168.2.26	192.168.2.24	192.168.2.27	192.168.2.25	N/A
192.168.2.30 - 192.168.2.30	192.168.2.28	192.168.2.31	192.168.2.29	N/A
192.168.2.34 - 192.168.2.34	192.168.2.32	192.168.2.35	192.168.2.33	N/A
192.168.2.38 - 192.168.2.38	192.168.2.36	192.168.2.39	192.168.2.37	N/A
192.168.2.42 - 192.168.2.42	192.168.2.40	192.168.2.43	192.168.2.41	N/A
192.168.2.46 - 192.168.2.46	192.168.2.44	192.168.2.47	192.168.2.45	N/A
192				N/A
192				N/A

Warning messages will appear if there are errors in the configuration.

Next steps

Step 7 The warning messages that appear provide instructions to correct errors in the settings. When you correct all errors, a preliminary list of IP ranges appears, allowing you to review the results. Click **Commit Subnet List** to save the IP ranges.

Auto-Generating IP Pools and Subnets (Cont.)



IP Range	Subnet Range	Domain	VLAN ID	# Subnets	# IPs	Edit	Delete
192.168.1.0 - 192.168.1.253	192.168.0.0 - 192.168.255.255	cisco.com	N/A	1	254		✕

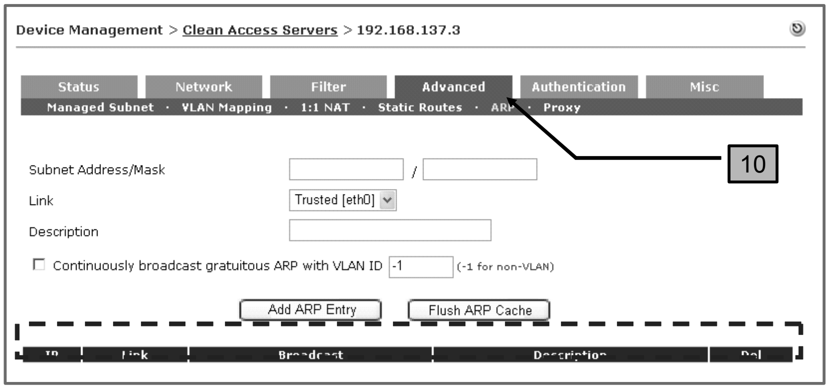
Vlan	Dynamic IPs	Available IPs	Static IPs	View MACs
	284	283	0	

Next steps →

Step 8 The autogenerated subnets appear as a single subnet range under Subnet List > List. The # Subnets and # IPs columns allow you to view how large the autogenerated range is in terms of how many subnets have been created and the number of IP addresses for the range.

Step 9 The newly generated list also appears in summary form under the DHCP Status tab, listing VLAN ID and the number of dynamic, available, and static IP addresses.

Auto-Generating IP Pools and Subnets (Cont.) ARP Entries Generated for DHCP



Device Management > Clean Access Servers > 192.168.137.3

Subnet Address/Mask /

Link: Trusted [eth0]

Description

□ Continuously broadcast gratuitous ARP with VLAN ID -1 (-1 for non-VLAN)

ARP entries are automatically created.

CANAC v2.1—2-15

Step 10 ARP entries are automatically created in the Cisco NAS configuration for the generated subnets (under Device Management > Clean Access Servers > [IP address] > Advanced > ARP). Selecting generated subnets removes the corresponding ARP entries.

Example Addresses for Auto-Generated Subnets

IP Range Entries	1st Subnet	2nd Subnet	3rd Subnet	4th Subnet
Network address	192.168.2.12	192.168.2.16	192.168.2.20	192.168.2.24
Router address	192.168.2.13	192.168.2.17	192.168.2.21	192.168.2.25
Client address range	192.168.2.14 - 192.168.2.14	192.168.2.18 - 192.168.2.18	192.168.2.22 - 192.168.2.22	192.168.2.26 - 192.168.2.26
Broadcast address	192.168.2.15	192.168.2.19	192.168.2.23	192.168.2.27

Automatically Generated IP Range of Four /30 Subnets

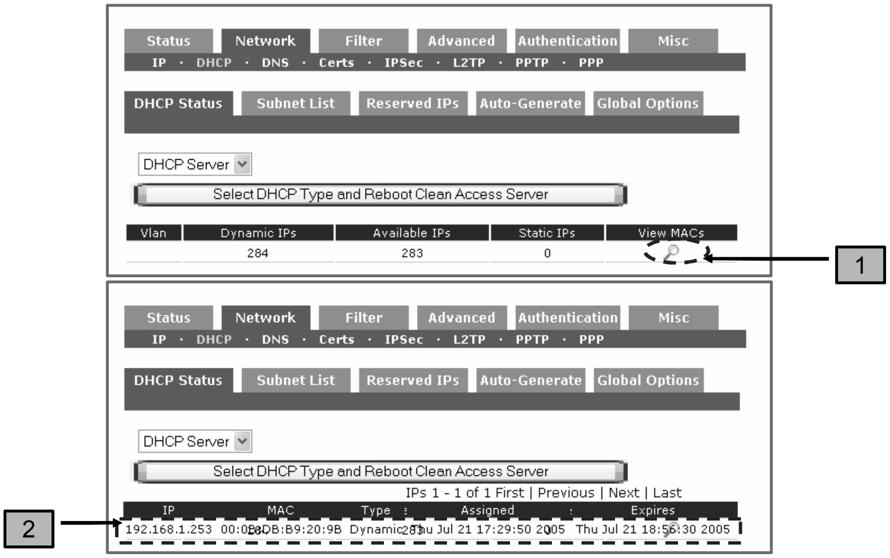
CANAC v2.1—2-16

The figure shows the addressing for an automatically-generated IP range of four /30 subnets starting at address 192.168.2.12.

Working with Subnets

This topic describes how to manage generated subnets on the Cisco NAS.

Working with Subnets—Viewing Users by MAC Address or VLAN


Status
Network
Filter
Advanced
Authentication
Misc
IP · DHCP · DNS · Certs · IPSec · L2TP · PPTP · PPP
DHCP Status
Subnet List
Reserved IPs
Auto-Generate
Global Options
DHCP Server
Select DHCP Type and Reboot Clean Access Server
1
2
IPs 1 - 1 of 1 First | Previous | Next | Last

Vlan	Dynamic IPs	Available IPs	Static IPs	View MACs
	284	283	0	🔍

IP	MAC	Type	Assigned	Expires
192.168.1.253	00:0B:DB:B9:20:9B	Dynamic	Thu Jul 21 17:29:50 2005	Thu Jul 21 18:56:30 2005

CANAC v2.1—2-17

After creating an autogenerated list, the Network > DHCP > DHCP Status page appears and lists the newly generated subnet. If the autogenerated subnet is restricted to a VLAN ID, the subnet is listed by that VLAN ID; otherwise, the VLAN column is blank if no VLAN is specified.

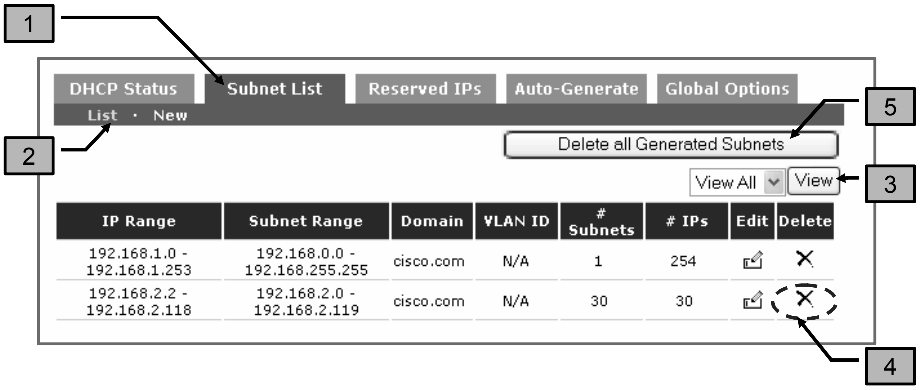
To view users by MAC address, complete these steps:

Step 1 Click the **View MACs** icon for the subnet that you want to view.

Step 2 The MAC address, IP, and type of client appear in the list at the bottom of the DHCP Status page. The Type column will contain one of these two entries:

- For DHCP clients, the Type column lists "Dynamic" and shows the lease assignment and expiration times.
- For reserved IP clients, the Type column lists "Static" and the lease time columns display "N/A."

Viewing or Deleting Subnets from the Subnet List



IP Range	Subnet Range	Domain	VLAN ID	# Subnets	# IPs	Edit	Delete
192.168.1.0 - 192.168.1.253	192.168.0.0 - 192.168.255.255	cisco.com	N/A	1	254	✎	✕
192.168.2.2 - 192.168.2.118	192.168.2.0 - 192.168.2.119	cisco.com	N/A	30	30	✎	✕

CANAC v2.1—2-18

To view the list of subnets created or to delete individual subnets, complete these steps:

Step 1 Choose **Network > DHCP**, and click the **Subnet List** tab.

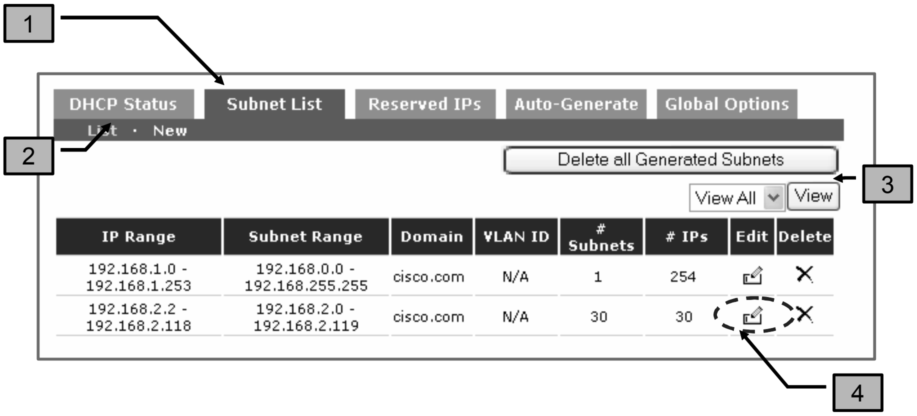
Step 2 Click the **List** link. The list of generated subnets appears.

Step 3 To view the subnets for a particular VLAN only, choose the **VLAN** option from the drop-down menu and click the **View** button.

Step 4 To remove an individual subnet, click the **Delete** icon next to that subnet.

Step 5 To remove all autogenerated subnets, click the **Delete all Generated Subnets** button. This action deletes only autogenerated subnets; all manually entered subnets are retained.

Editing a Subnet



IP Range	Subnet Range	Domain	VLAN ID	# Subnets	# IPs	Edit	Delete
192.168.1.0 - 192.168.1.253	192.168.0.0 - 192.168.255.255	cisco.com	N/A	1	254	✎	✕
192.168.2.2 - 192.168.2.118	192.168.2.0 - 192.168.2.119	cisco.com	N/A	30	30	✎	✕

Next steps →

To modify individual subnets, complete these steps:

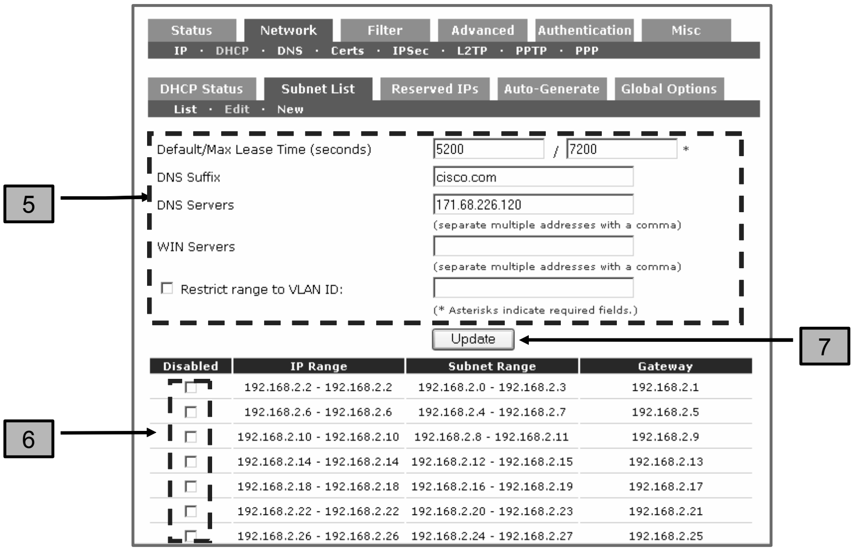
Step 1 Choose **Network > DHCP** and click the **Subnet List** tab.

Step 2 Click the **List** link. The list of generated subnets appears.

Step 3 To view the subnets for a particular VLAN only, choose the **VLAN** option from the drop-down menu and click the **View** button.

Step 4 In the Subnet List, click the **Edit** button next to the subnet that you want to modify. The Edit Subnet List form appears.

Editing a Subnet (Cont.)



Default/Max Lease Time (seconds)	5200 / 7200	*
DNS Suffix	cisco.com	
DNS Servers	171.68.226.120 (separate multiple addresses with a comma)	
WIN Servers	(separate multiple addresses with a comma)	
□ Restrict range to VLAN ID:	(* Asterisks indicate required fields.)	

Disabled	IP Range	Subnet Range	Gateway
□	192.168.2.2 - 192.168.2.2	192.168.2.0 - 192.168.2.3	192.168.2.1
□	192.168.2.6 - 192.168.2.6	192.168.2.4 - 192.168.2.7	192.168.2.5
□	192.168.2.10 - 192.168.2.10	192.168.2.8 - 192.168.2.11	192.168.2.9
□	192.168.2.14 - 192.168.2.14	192.168.2.12 - 192.168.2.15	192.168.2.13
□	192.168.2.18 - 192.168.2.18	192.168.2.16 - 192.168.2.19	192.168.2.17
□	192.168.2.22 - 192.168.2.22	192.168.2.20 - 192.168.2.23	192.168.2.21
□	192.168.2.26 - 192.168.2.26	192.168.2.24 - 192.168.2.27	192.168.2.25

CANAC v2.1—2-20

Step 5 To modify the lease time, DNS or WINS server information, and VLAN ID restriction of the subnet list, enter the new values in the corresponding fields.

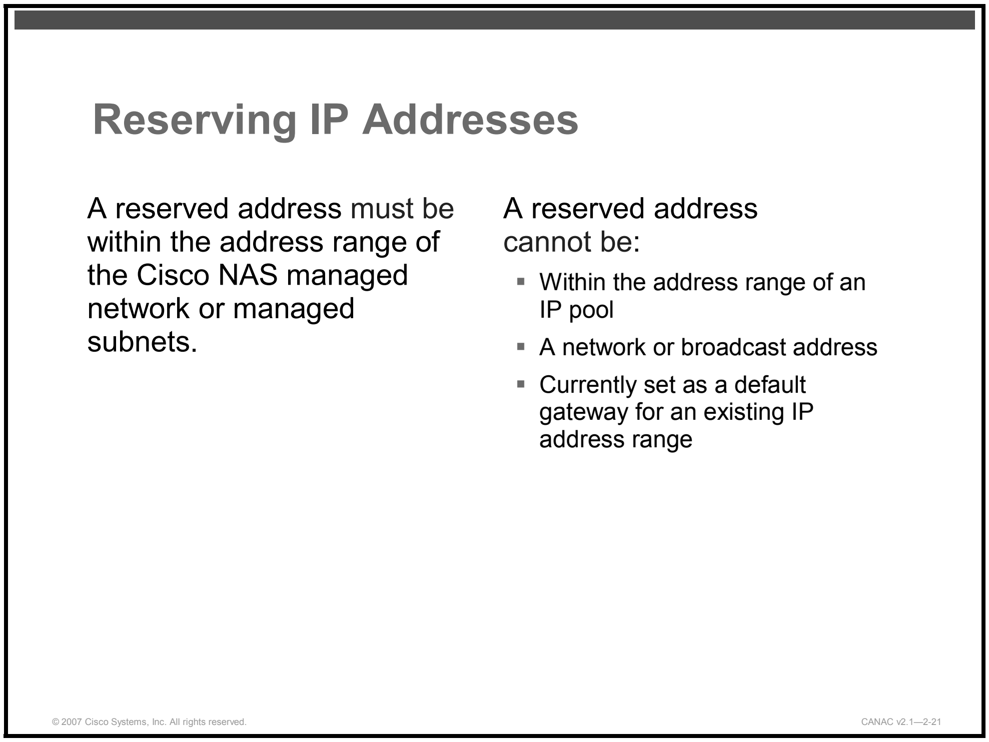
Step 6 For autogenerated subnets, you can disable a particular subnet by clicking the **Disabled** check box next to it. This step allows you to disable the IP range associated with a particular generated subnet so that the IP addresses in the range are not leased. This feature can be particular useful if you have one or two servers in the middle of a subnet range.

Step 7 Click **Update** to save the changes.

Note To change the IP range, default gateway, or subnet mask, the subnet must be deleted from the Subnet List > List form and added again with the modified parameters.

Reserving IP Addresses

This topic describes how to configure the Cisco NAS to provide reserved IP addresses.



Reserving IP Addresses

A reserved address must be within the address range of the Cisco NAS managed network or managed subnets.

A reserved address cannot be:

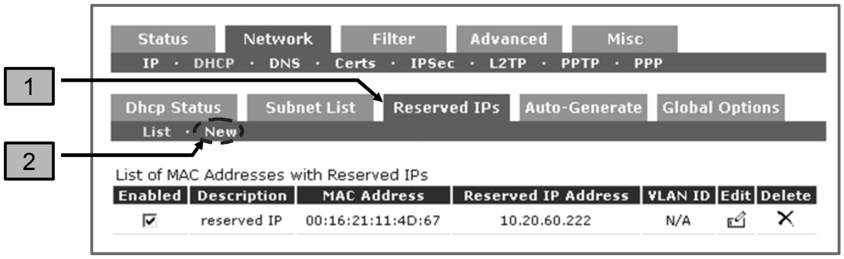
- Within the address range of an IP pool
- A network or broadcast address
- Currently set as a default gateway for an existing IP address range

CANAC v2.1—2-21

By reserving an IP address, you can keep a permanent association between a particular IP address and device. A reserved device is identified by the MAC address of the device. Therefore, before starting, you need to know the MAC address of the device that will reserve an IP address.

The configuration for a reserved IP address does not include a maximum or default lease time. The address is always available for the device and, therefore, has an unlimited lease time. The figure lists several rules that apply to reserved IP addresses.

Adding a Reserved IP Address



List of MAC Addresses with Reserved IPs

Enabled	Description	MAC Address	Reserved IP Address	VLAN ID	Edit	Delete
☑	reserved IP	00:16:21:11:4D:67	10.20.60.222	N/A	✎	✕

Next steps →

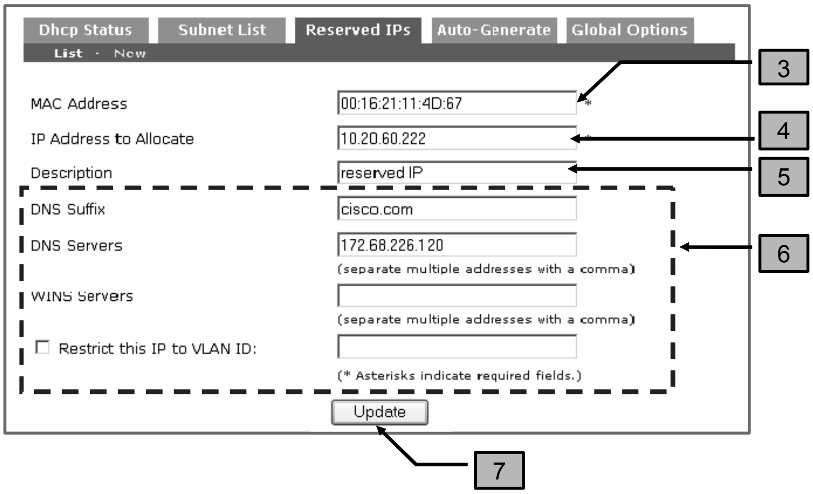
CANAC v2.1—2-22

To add a reserved IP address, complete these steps:

Step 1 Choose **Network > DHCP** and click the **Reserved IPs** tab.

Step 2 Click the **New** link. The New Reserved IP Address form appears.

Adding a Reserved IP Address (Cont.)



MAC Address: 00:16:21:11:4D:67 *

IP Address to Allocate: 10.20.60.222 *

Description: reserved IP

DNS Suffix: cisco.com

DNS Servers: 172.68.226.120
(separate multiple addresses with a comma)

WINS Servers:
(separate multiple addresses with a comma)

□ Restrict this IP to VLAN ID:

(* Asterisks indicate required fields.)

CANAC v2.1—2-23

Step 3 In the MAC Address field, enter the MAC address in hexadecimal MAC address format (for example, 00:16:21:11:4D:67) for the device that will have a reserved IP address.

Step 4 In the IP Address to Allocate field, enter the IP address that you want to reserve.

Step 5 (Optional) Enter a description for the IP address in the Description field.

Step 6 Enter values for these remaining fields:

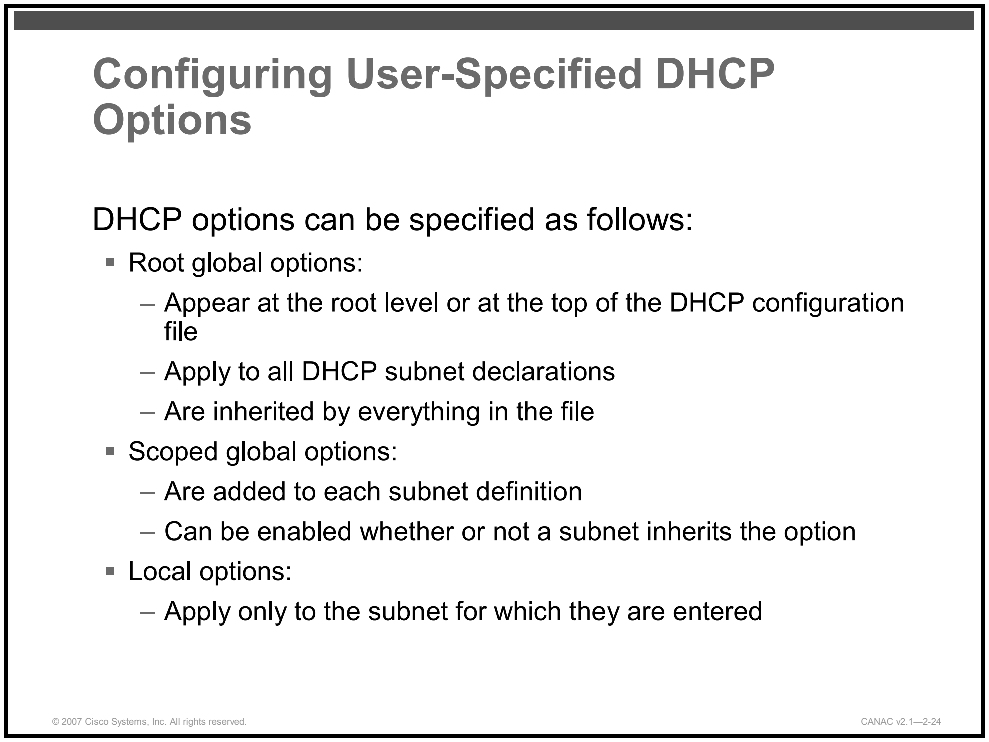
- **DNS Suffix:** Enter the DNS suffix information to pass to clients with the address lease.
- **DNS Servers:** Enter the address of one or more DNS servers in the client network. Separate multiple addresses with commas.
- **WINS Servers:** Enter the address of one or more WINS servers in the client network. Separate multiple addresses with commas.
- **Restrict this IP to VLAN ID:** If you want to associate the client with a particular VLAN, check this check box and specify the VLAN identifier in the VLAN ID field. Otherwise, leave the check box unchecked.

Step 7 Click the **Update** button.

The reserved IP address now appears under Subnet List > List. You can modify the reserved IP address by clicking the **Edit** button, or you can remove the reserved IP address by clicking the **Delete** button.

Configuring User-Specified DHCP Options

This topic describes how to configure user-specified DHCP options on the Cisco NAS.



Configuring User-Specified DHCP Options

DHCP options can be specified as follows:

- Root global options:
  - Appear at the root level or at the top of the DHCP configuration file
  - Apply to all DHCP subnet declarations
  - Are inherited by everything in the file
- Scoped global options:
  - Are added to each subnet definition
  - Can be enabled whether or not a subnet inherits the option
- Local options:
  - Apply only to the subnet for which they are entered

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—2-24

The Global Options tab allows advanced users to modify the DHCP configuration directly.

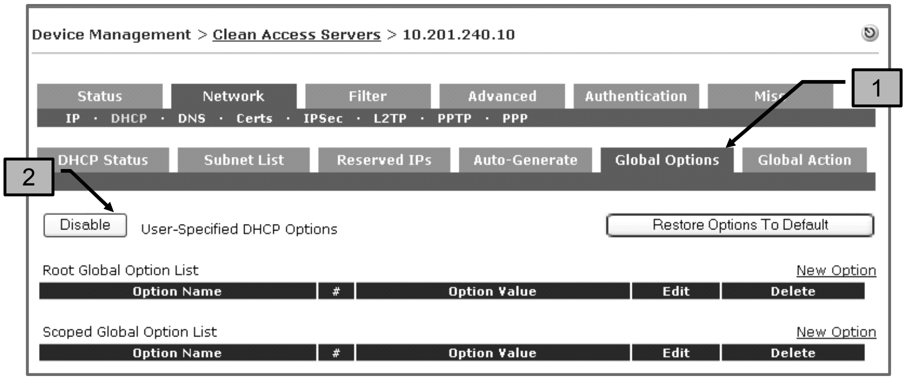
DHCP options can be specified as follows:

- **Root global options:** Root global options appear at the root level or at the top of the DHCP configuration file and apply to all DHCP subnet declarations. Root global options are inherited by everything in the file.
- **Scoped global options:** Scoped global options are added to each subnet definition. However, you can enable whether or not a subnet inherits each option. When DHCP options are enabled, an Inherit Scoped Global Option check box appears on the forms used to add or edit manually-created or autogenerated subnets. Note that the Inherit Scoped Global Option check box appears only while customized DHCP options are enabled and only for subnets created after the options are enabled.
- **Local options:** Local options apply only to the subnet for which they are entered.

In Release 4.0 and later of Cisco NAC Appliance, you can create DHCP option rules based on class restrictions to restrict access to DHCP subnets. You can also create rules for all clients on a specific VLAN and for clients coming from a specific relay IP.

Caution The DHCP configuration file should not be modified under most circumstances.

Enabling User-Specified DHCP Options



Device Management > Clean Access Servers > 10.201.240.10

Disable User-Specified DHCP Options

Root Global Option List

Option Name	#	Option Value	Edit	Delete

Scoped Global Option List

Option Name	#	Option Value	Edit	Delete

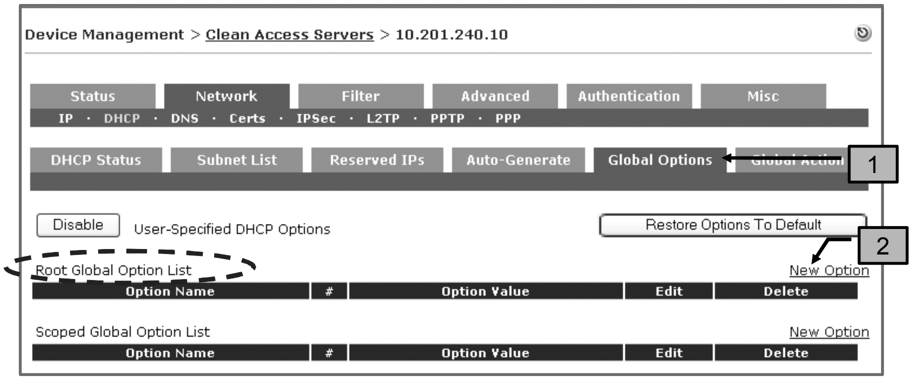
CANAC v2.1—2-25

To enable user-specified DHCP options, complete these steps:

Step 1 Choose **Network > DHCP** and click the **Global Options** tab.

Step 2 Click the **Enable** button. This button toggles between Enable and Disable. After clicking the **Enable** button, you can add user-specified DHCP options.

Adding the Root Global DHCP Option



Device Management > Clean Access Servers > 10.201.240.10

User-Specified DHCP Options

Root Global Option List

Option Name	#	Option Value	Edit	Delete

Scoped Global Option List

Option Name	#	Option Value	Edit	Delete

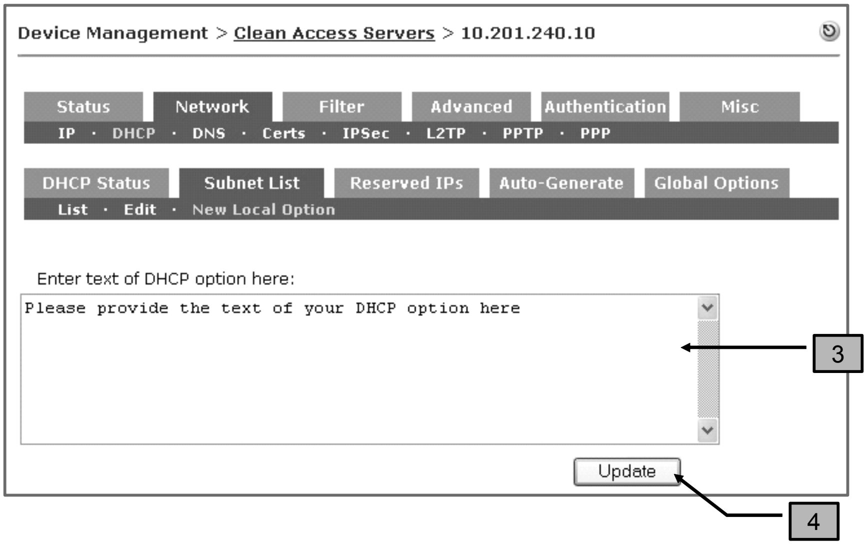
Next steps →

To add a root global DHCP option, complete these steps:

Step 1 Choose **Network > DHCP** and click the **Global Options** tab. The Root Global Options form provides access to the Root Global, Scoped Global, and Class Option global DHCP options.

Step 2 In this example, you are adding a Root Global DHCP option, so click the Root Global **New Option** link to add a new option. Once an option is added, it is listed on this main page under the corresponding type.

Adding the Root Global DHCP Option (Cont.)



Device Management > Clean Access Servers > 10.201.240.10

Enter text of DHCP option here:

```
Please provide the text of your DHCP option here
```

CANAC v2.1—2-27

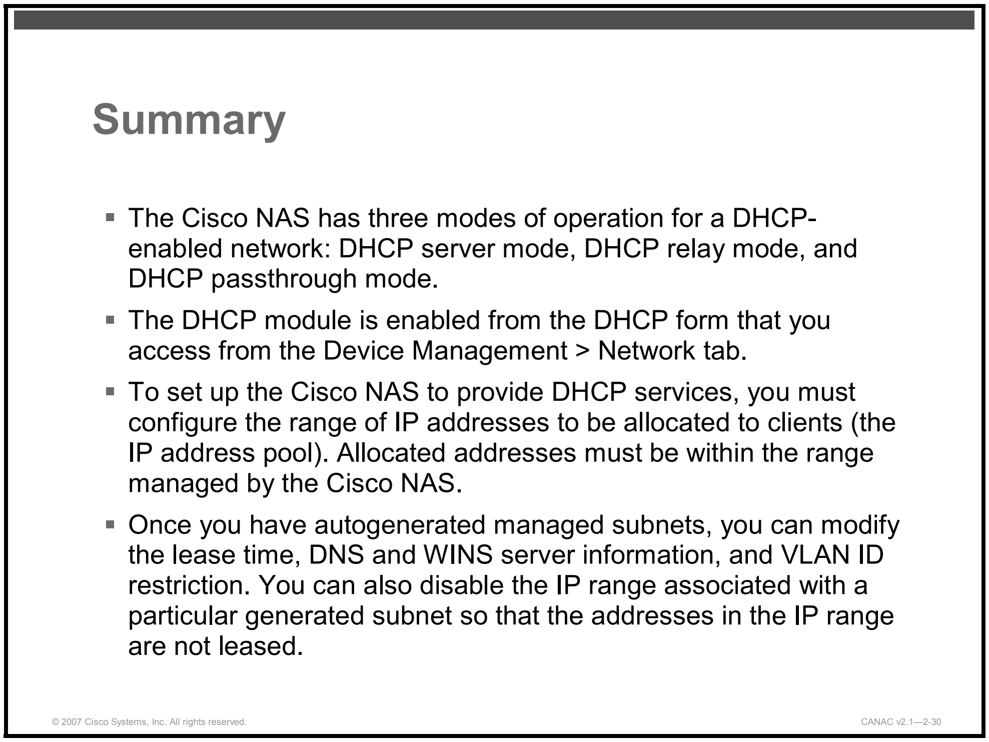
Step 3 In the Root Global Options form, enter the text of the new root global DHCP option in the text field.

Step 4 Click **Update** to save your configuration when you are finished.

Note For details on adding a scoped global option or class options, refer to User-Specified DHCP Options in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide.*

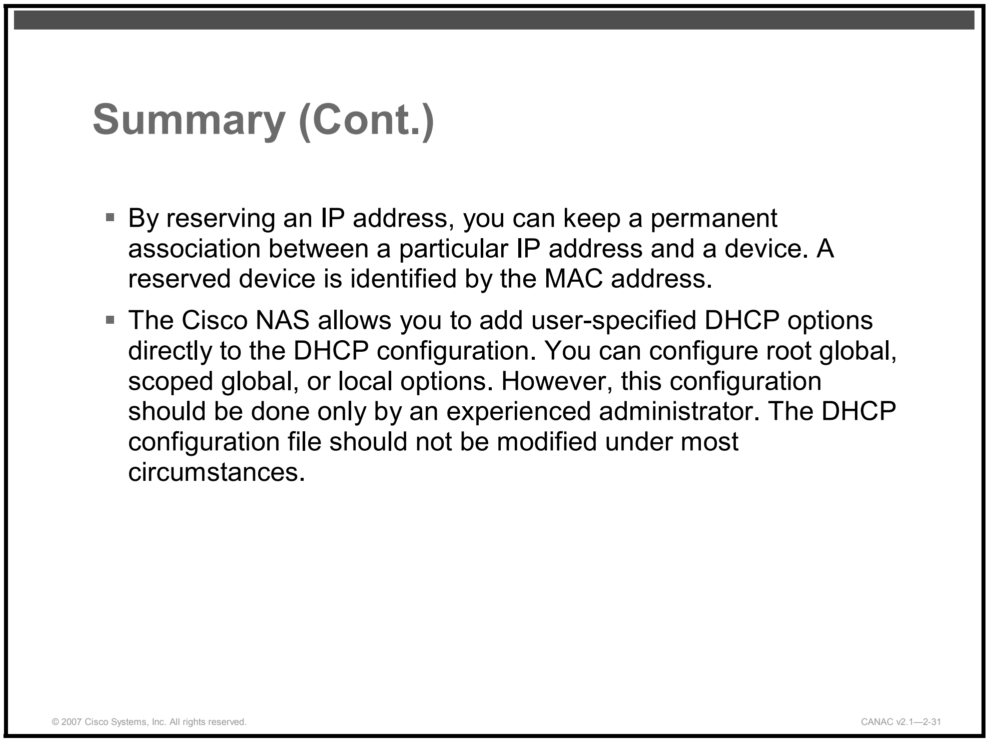
Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- The Cisco NAS has three modes of operation for a DHCP-enabled network: DHCP server mode, DHCP relay mode, and DHCP passthrough mode.
- The DHCP module is enabled from the DHCP form that you access from the Device Management > Network tab.
- To set up the Cisco NAS to provide DHCP services, you must configure the range of IP addresses to be allocated to clients (the IP address pool). Allocated addresses must be within the range managed by the Cisco NAS.
- Once you have autogenerated managed subnets, you can modify the lease time, DNS and WINS server information, and VLAN ID restriction. You can also disable the IP range associated with a particular generated subnet so that the addresses in the IP range are not leased.

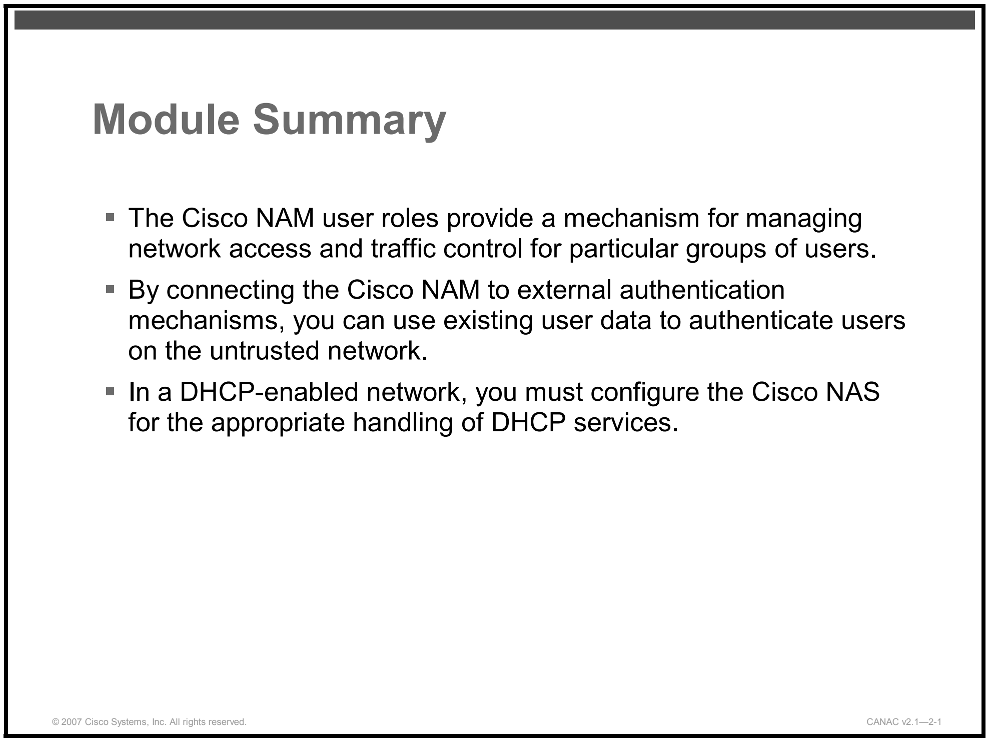


Summary (Cont.)

- By reserving an IP address, you can keep a permanent association between a particular IP address and a device. A reserved device is identified by the MAC address.
- The Cisco NAS allows you to add user-specified DHCP options directly to the DHCP configuration. You can configure root global, scoped global, or local options. However, this configuration should be done only by an experienced administrator. The DHCP configuration file should not be modified under most circumstances.

Module Summary

This topic summarizes the key points that were discussed in this module.



Module Summary

- The Cisco NAM user roles provide a mechanism for managing network access and traffic control for particular groups of users.
- By connecting the Cisco NAM to external authentication mechanisms, you can use existing user data to authenticate users on the untrusted network.
- In a DHCP-enabled network, you must configure the Cisco NAS for the appropriate handling of DHCP services.

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—2-1

This module describes how to configure the common elements of a Cisco Network Admission Control (NAC) Appliance solution to either an in-band or out-of-band deployment. User roles are integral to the functioning of Cisco NAC Appliance and provide a mechanism to manage which sites users can visit, how much bandwidth they are provided, and how long they can remain logged in to the network. Many clients require that an authentication provider be used as an authentication source. By connecting the Cisco NAC Appliance Manager (Cisco NAM) to external authentication mechanisms, you can set up any combination of local and external authentication mechanisms. The Cisco NAC Appliance solution allows you to configure the Cisco NAS to handle DHCP services as a DHCP server, a DHCP relay, or to perform DHCP passthrough.

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *Cisco NAC Appliance (Clean Access) Introduction*. http://www.cisco.com/en/US/products/ps6128/index.html.
- Cisco Systems, Inc. *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*. http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.
- Cisco Systems, Inc. *Cisco NAC Appliance—Clean Access Server Installation and Administration Guide*. http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers are found in the Module Self-Check Answer Key.

Q1) What are the three types of user roles for Cisco NAC Appliance? (Source: Configuring User Roles)

A) normal login role, Cisco NAC Appliance quarantine role, and Cisco NAA temporary role
B) temporary login role, Cisco NAC Appliance quarantine role, and Cisco NAS temporary role
C) normal login role, Cisco NAC Appliance quarantine role, and Cisco NAS temporary role
D) standby login role, Cisco NAC Appliance quarantine role, and primary login role

Q2) Which web administration console form is used to delete a role? (Source: Configuring User Roles)

A) User Management > User Roles > Existing Roles
B) User Management > User Roles
C) User Management > User Roles > Delete Role
D) User Management > User Roles > List of Roles

Q3) Which types of users would use local authentication? (Source: Configuring External Authentication)

A) general users
B) VPN-based users
C) test users

Q4) What is the recommended authentication method when the Cisco NAM communicates with a Microsoft Active Directory? (Source: Configuring External Authentication)

A) RADIUS
B) Windows NT
C) S/Ident
D) LDAP
E) Transparent 801.1q

Q5) What do Cisco NAC Appliance VLAN mapping rules map? (Source: Configuring External Authentication)

A) VLAN ID of authentication traffic from the trusted interface of the Cisco NAS into a user role
B) VLAN ID of user traffic from the untrusted interface of the Cisco NAS into a user role
C) VLAN ID of user traffic from the untrusted interface of the Cisco NAS into the temporary role
D) VLAN ID of user traffic from the trusted interface of the Cisco NAS into a temporary role

Q6) Which web-based administration console page do you use to test user authentication configured with an external authentication provider? (Source: Configuring External Authentication)

A) User Management > Auth Servers > Auth Test
B) User Management > User Roles > Auth Test
C) User Management > Users > Auth Test

Q7) In a DHCP-enabled network, how does the Cisco NAS handle DHCP messages when operating in DHCP relay mode? (Source: Configuring DHCP on the Cisco NAS)

A) The Cisco NAS allocates client IP addresses for the managed (untrusted) network.
B) The Cisco NAS forwards messages from clients to another DHCP server.
C) The Cisco NAS propagates the DHCP broadcast messages across its interfaces without modification.

Q8) When first enabling DHCP services on the Cisco NAS from the Device Management > Clean Access Servers menu, which tab provides access to the DHCP form? (Source: Configuring DHCP on the Cisco NAS)

A) Status
B) DHCP Status
C) Network
D) Advanced
E) Misc

Q9) Which page must you be on to delete all autogenerated subnets? (Source: Configuring DHCP on the Cisco NAS)

A) Network > DHCP > DHCP Status
B) Network > DHCP > Subnet List
C) Network > DHCP > Reserved IPs
D) Network > DHCP > Auto-Generate
E) Network > DHCP > Global Options

Q10) What must a reserved IP address be? (Source: Configuring DHCP on the Cisco NAS)

A) within the address range of the Cisco NAS managed network or managed subnets
B) within the address range of an IP pool
C) currently set as a default gateway for an existing IP address range
D) a network or broadcast address

Q11) If you want to modify the DHCP configuration to add an option that will only be enabled for autogenerated subnets, which type of DHCP option should you configure? (Source: Configuring DHCP on the Cisco NAS)

A) root global option
B) scoped global option
C) local option

Module Self-Check Answer Key

Q1)	A
Q2)	D
Q3)	C
Q4)	D
Q5)	B
Q6)	A
Q7)	B
Q8)	C
Q9)	B
Q10)	A
Q11)	B

Module 3

Cisco NAC Appliance Implementation

Overview

Clients need a network security solution that fits their specific requirements. With the Cisco Network Admission Control (NAC) Appliance solution, clients can select an in-band implementation to minimize infrastructure costs or select an out-of band implementation to ensure that maximum bandwidth is provided while maintaining corporate network security policies. This module describes the procedures for implementing Cisco NAC Appliance for network admission control for in-band and out-of-band deployment scenarios.

Module Objectives

Upon completing this module, you will be able to configure the Cisco NAC Appliance in-band and out-of-band implementation options. This ability includes being able to meet these objectives:

- Deploy the Cisco NAC Appliance in-band solution for Layer 2 and Layer 3 network environments
- Describe how to configure Microsoft Windows Active Directory Server SSO support on the Cisco NAS
- Configure the Cisco NAS to support Cisco VPN SSO
- Deploy Cisco NAC Appliance out-of-band solution for VLAN-based quarantine
- Configure the Cisco NAM to manage switches in a network

Lesson 1

Implementing Cisco NAC Appliance In-Band Deployment

Overview

In-band deployment is one of two implementation options for the Cisco Network Admission Control (NAC) Appliance. The in-band deployment option offers clients a cost-effective way to use all the benefits of Cisco NAC Appliance network security. This lesson describes the procedure for implementing the Cisco NAC Appliance in-band deployment in Layer 2 and Layer 3 network environments.

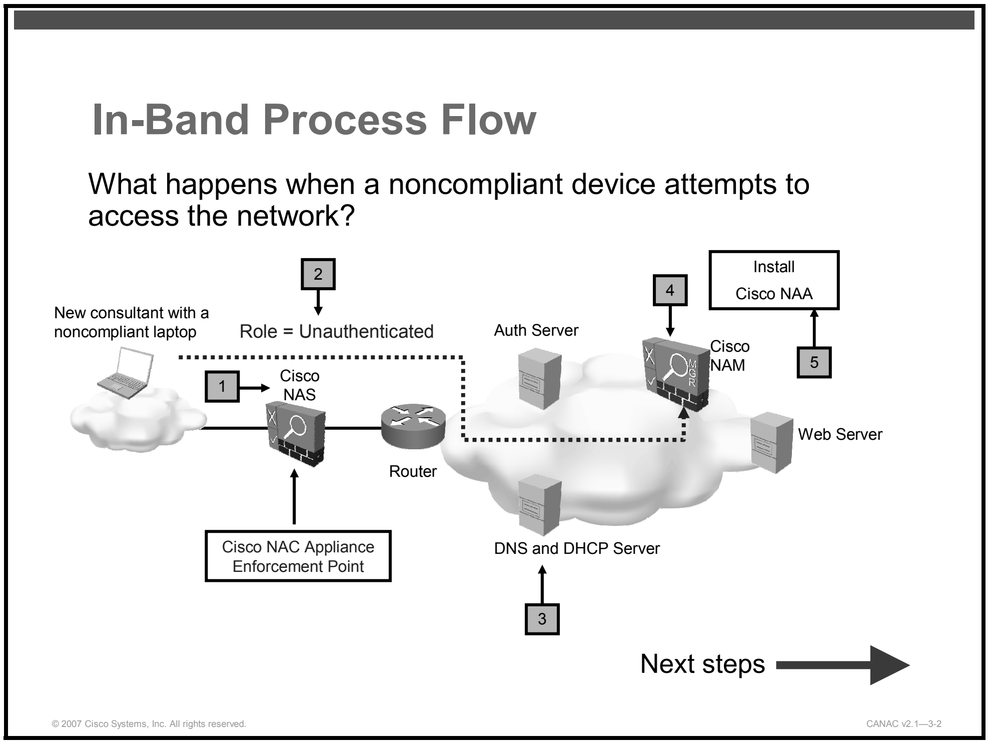
Objectives

Upon completing this lesson, you will be able to deploy the Cisco NAC Appliance in-band solution for Layer 2 and Layer 3 network environments. This ability includes being able to meet these objectives:

- Describe the Cisco NAC Appliance in-band process flow
- Describe central and edge in-band deployment configurations for Cisco NAC Appliance
- Describe how to configure the Cisco NAS for in-band deployment
- Describe how to add the Cisco NAS to the Cisco NAM managed domain for in-band deployment
- Describe how to use the Cisco NAM to configure the trusted and untrusted interfaces of the Cisco NAS
- Describe how to add managed subnets on the Cisco NAS
- Describe how to configure Cisco NAS VLAN settings

In-Band Process Flow

This topic describes the Cisco NAC Appliance in-band process flow.



In-Band Process Flow

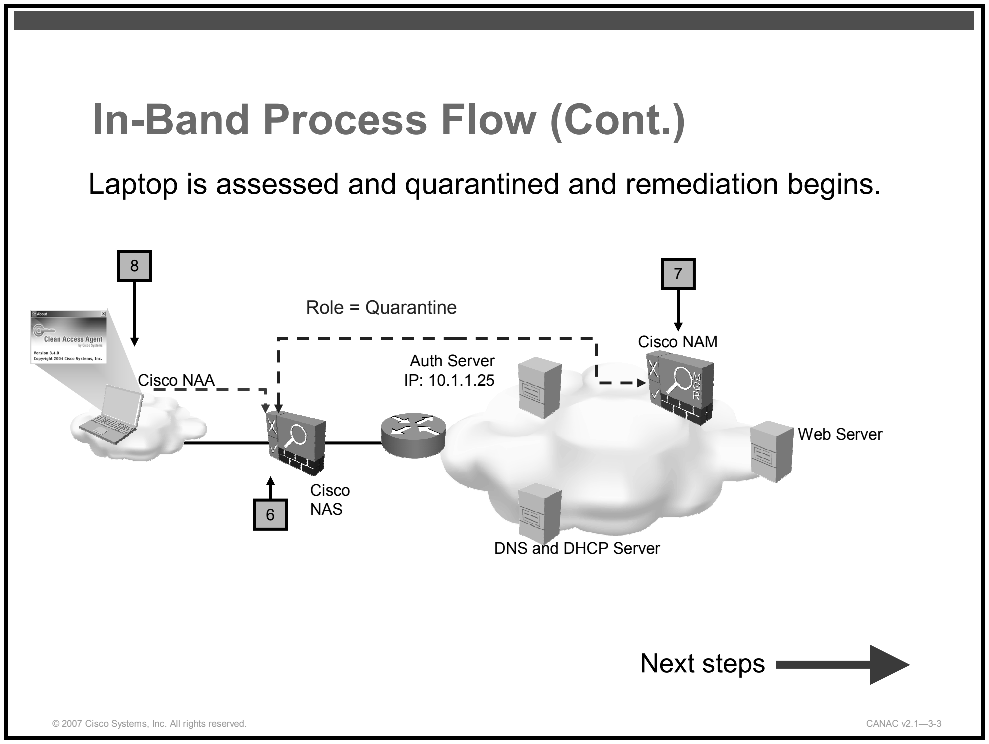
What happens when a noncompliant device attempts to access the network?

Next steps

CANAC v2.1—3-2

The scenario in the figure shows what happens when a new consultant using a noncompliant laptop accesses the network for the first time. The network security policy of the company accounts for the probability that any new consultant will have a noncompliant laptop, and the company wants to ensure that all updates are current. The web server that the consultant is trying to access is protected by the Cisco NAC Appliance in-band solution, and the following actions occur when a user logs into the corporate network with a laptop that is noncompliant with security policies:

1. When the user first accesses the network, the Cisco NAC Appliance Server (Cisco NAS) checks to see if the laptop MAC address is on the list of certified devices.
2. When the Cisco NAS determines that the laptop is not on the certified list, the laptop is placed in an unauthenticated role.
3. The unauthenticated laptop obtains an IP address from the DHCP server but cannot pass the Cisco NAS, which is acting as an IP filter. While in the unauthenticated role, only User Datagram Protocol (UDP) Port 53, Domain Name System (DNS), and DHCP traffic (via DHCP and VLAN passthrough) are allowed.
4. The Cisco NAC Appliance Manager (NAM) instructs the user to open a web browser.
5. When the user opens a browser, the user is redirected to a Secure Sockets Layer (SSL)-based login page. After entering the user credentials, the user is mapped into the consultant role. Now in the consultant role, the user is asked to download the Cisco NAC Appliance Agent (Cisco NAA).



In-Band Process Flow (Cont.)

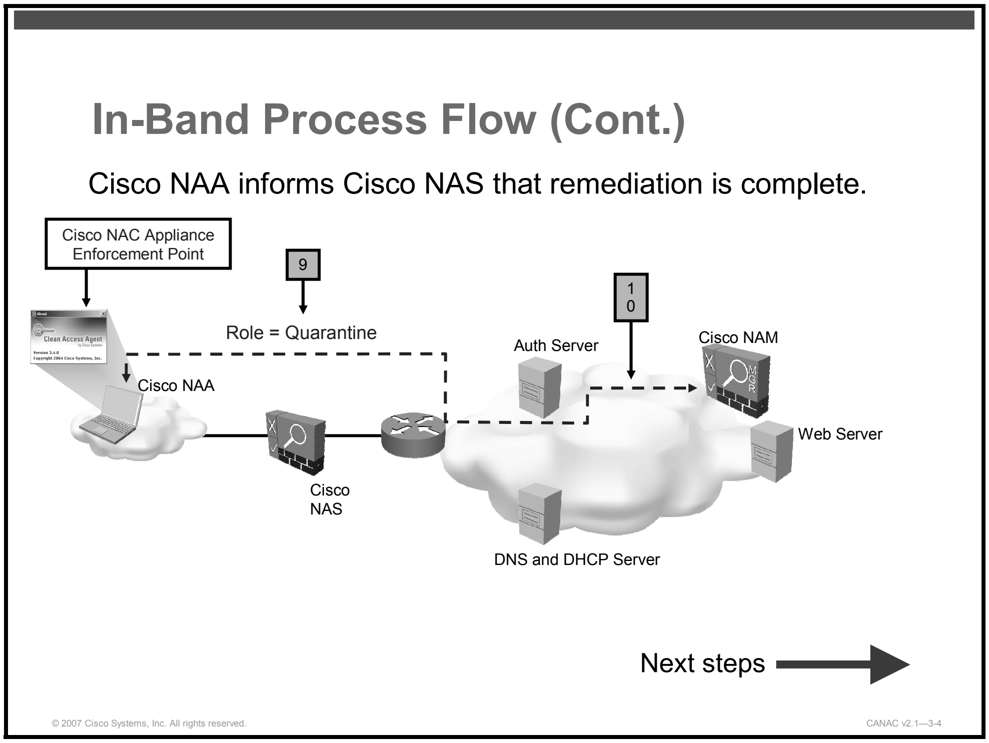
Laptop is assessed and quarantined and remediation begins.

Next steps

6. The Cisco NAA that is running on the user laptop performs a posture assessment. That is, the Cisco NAA collects data about the laptop operating system, software, and hardware vulnerabilities. The Cisco NAA then sends a posture report to the Cisco NAS to make a network admission decision about the user device.

7. The Cisco NAS forwards the posture report to the Cisco NAM for further analysis. If the Cisco NAM determines that the laptop is not in compliance with security and vulnerability standards, it instructs the Cisco NAS to put the laptop into the temporary role. The temporary role can be as small as a /30 subnet.

8. The Cisco NAM sends the necessary remediation steps to the Cisco NAA that is running on the user laptop and starts the session timer for the user session.



In-Band Process Flow (Cont.)

Cisco NAA informs Cisco NAS that remediation is complete.

Next steps →

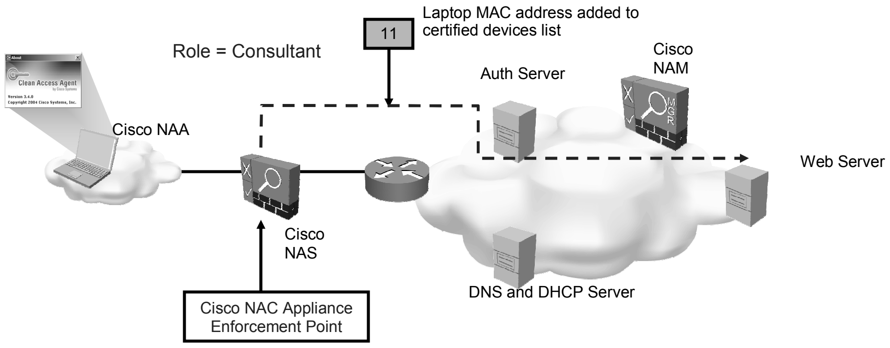
CANAC v2.1—3-4

9. A clock displays the time that is remaining in the quarantine role for the laptop user while the Cisco NAA guides the user, step by step, through remediation. Patches can be downloaded from an internal or external update site (such as http://windowsupdate.microsoft.com) or from the Cisco NAM.

10. When remediation is finished, the Cisco NAA informs the Cisco NAM that the laptop is now compliant.

In-Band Process Flow (Cont.)

User and laptop are now authorized to access the web server.

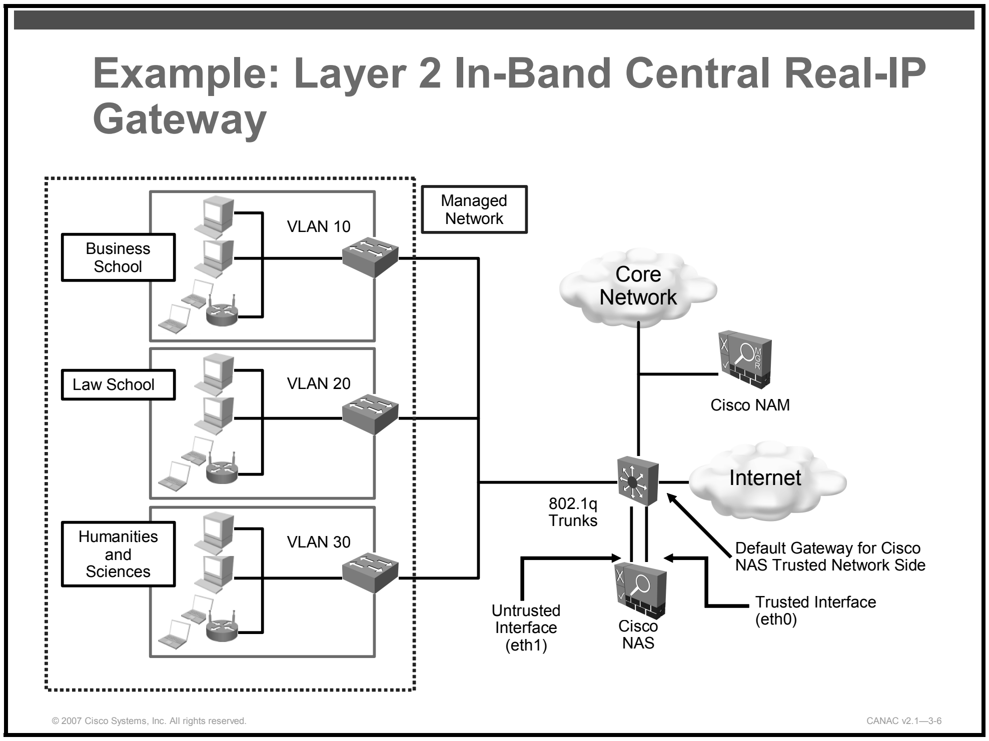


CANAC v2.1—3-5

11. The Cisco NAS then adds the MAC address of the user laptop to the list of certified devices and assigns the laptop to the consultant user role. The user is now able to access the internal web server.

In-Band Deployment Configurations

This topic describes central and edge in-band deployment configurations for Cisco NAC Appliance.

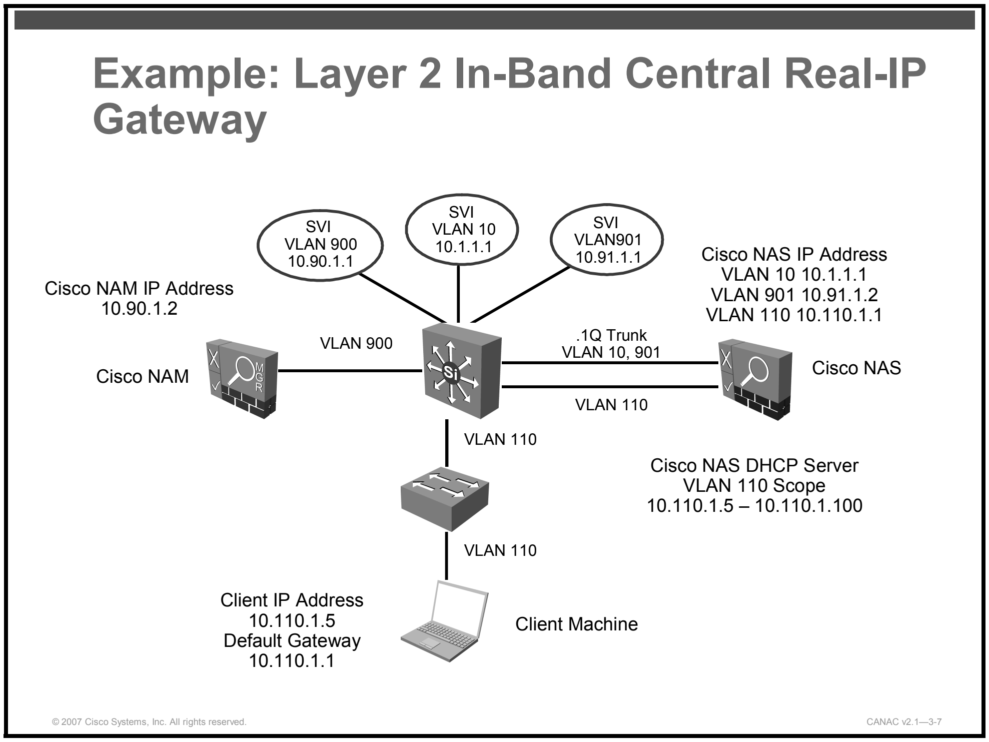


Example: Layer 2 In-Band Central Real-IP Gateway

CANAC v2.1—3-6

In a routed central deployment, the Cisco NAS is configured to act as the real-IP gateway for each of the subnets that you want to manage.

In a VLAN-enabled environment, you can trunk multiple VLANs through a single Cisco NAS. Aggregating multiple VLANs that are organized by location, wiring, or shared needs of users through a single Cisco NAS (by VLAN trunking) can help simplify your deployment.

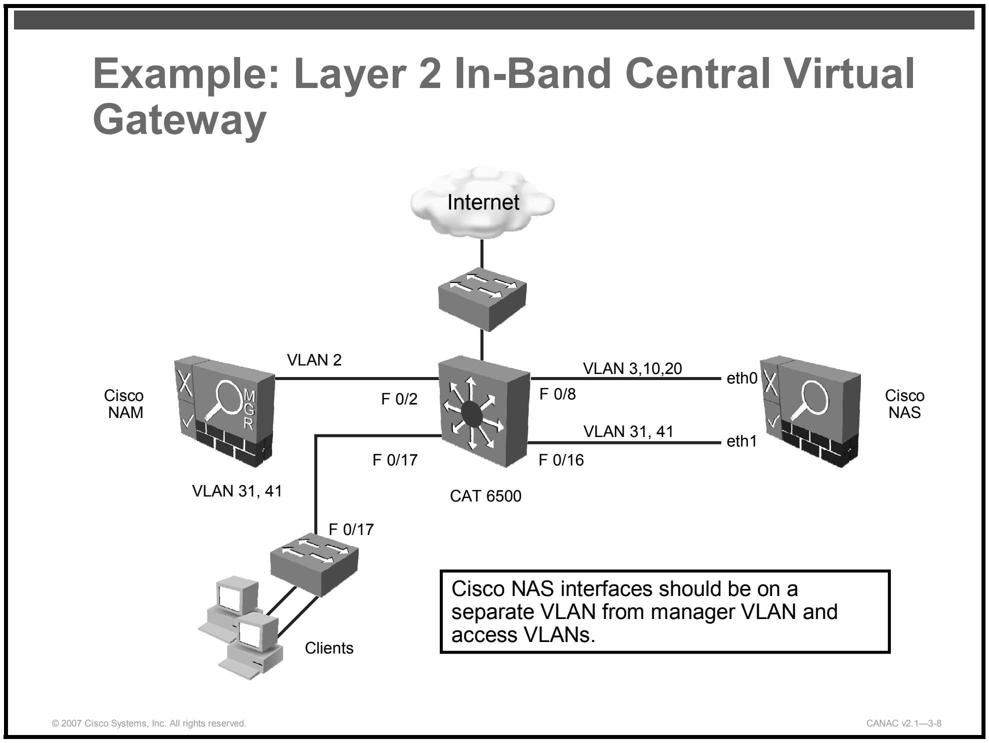


Example: Layer 2 In-Band Central Real-IP Gateway

CANAC v2.1—3-7

The figure shows a Layer 2 in-band central real-IP gateway sample topology. The topology shows how each of the components of the solution are on separate VLANs. For example, the untrusted side of the network is on VLAN 110, the Cisco NAM is on VLAN 900, and there are two VLANS accessing the Cisco NAS from the trusted side of the network, VLAN 10 for client access and VLAN 901 for management.

Note In central deployment configurations, a Cisco NAS virtual gateway uses managed subnets to help devices on different untrusted VLANs to arrive at the respective default gateways on the trusted side of the network.



Example: Layer 2 In-Band Central Virtual Gateway

Cisco NAS interfaces should be on a separate VLAN from manager VLAN and access VLANs.

CANAC v2.1—3-8

The figure shows an example Layer 2 in-band central virtual gateway Cisco NAS deployment. Consider these aspects of this configuration example:

- **VLAN for the Cisco NAM:** In the figure, the management VLAN for the Cisco NAM is VLAN 2.
- **VLAN for the Cisco NAS:** The VLAN for the Cisco NAS must be different from the VLAN for the Cisco NAM. In the figure, the management VLAN for the Cisco NAS is VLAN 3.
- **VLAN IDs for Access (User):** In the figure, the access VLANs are VLANs 10 and 20.
- **VLAN IDs for Mapped Access (User):** In the figure, the mapped access VLANs are VLAMs 31 and 41.
- On the switch interface connecting to eth0 of the Cisco NAS, the trunk settings are configured for the trusted traffic. This is a possible configuration for the trusted traffic:

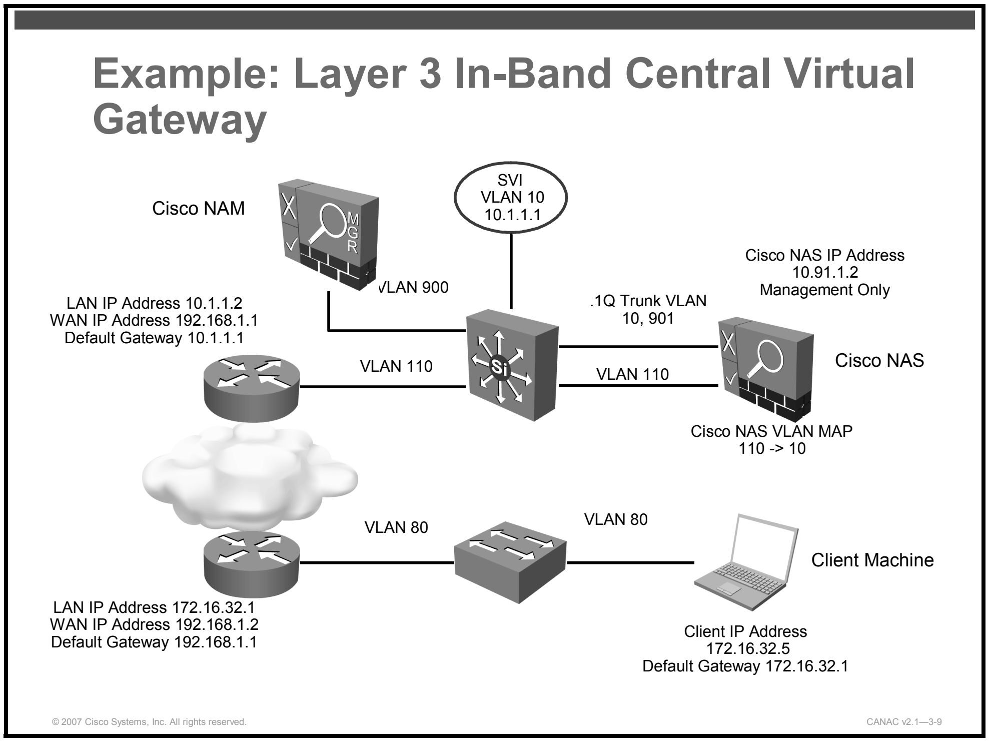
```
# switchport trunk encapsulation dot1q
# switchport trunk native vlan 999
# switchport trunk allowed vlan 3,10,20
```

- On the switch interface connecting to eth1 of the Cisco NAS, the trunk settings are configured for the untrusted traffic. The following is an example configuration of trunk settings for the untrusted traffic:

```
# switchport trunk encapsulation dot1q
# switchport trunk native vlan 999
# switchport trunk allowed vlan 31,41
```

- The same IP address has been configured for both eth0 and eth1 of the Cisco NAS using the command-line interface (CLI).
- The management VLAN has been configured for eth0 of the Cisco NAS using the CLI.

Note When the Cisco NAS operates in virtual gateway mode, it passes network traffic from its eth0 interface to eth1 and from eth1 to eth0 without changing the VLAN tag. For in-band configurations, you do not want to pass traffic from both interfaces through the same Layer 2 switch, which would create a loop. To avoid this situation, use VLAN mapping; tag incoming traffic to the Cisco NAS on a VLAN that is different from the VLAN used for outgoing traffic of the Cisco NAS.



Example: Layer 3 In-Band Central Virtual Gateway

Cisco NAM

SVI
VLAN 10
10.1.1.1

Cisco NAS IP Address
10.91.1.2
Management Only

VLAN 900

.1Q Trunk VLAN
10, 901

LAN IP Address 10.1.1.2
WAN IP Address 192.168.1.1
Default Gateway 10.1.1.1

VLAN 110

VLAN 110

Cisco NAS

Cisco NAS VLAN MAP
110 -> 10

VLAN 80

VLAN 80

Client Machine

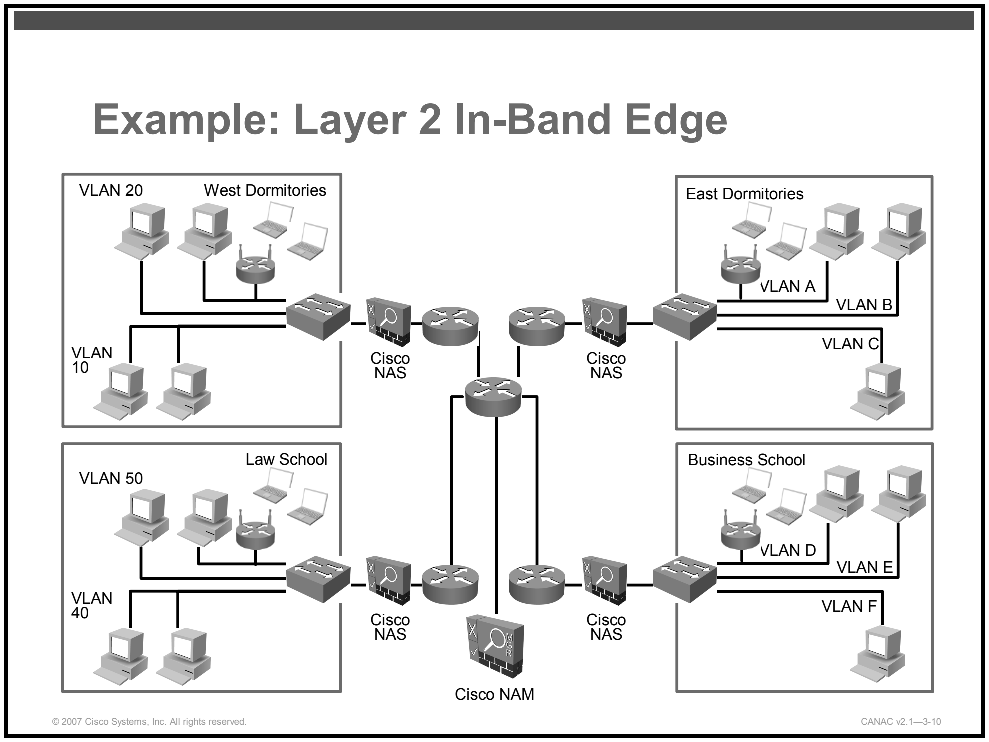
LAN IP Address 172.16.32.1
WAN IP Address 192.168.1.2
Default Gateway 192.168.1.1

Client IP Address
172.16.32.5
Default Gateway 172.16.32.1

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—3-9

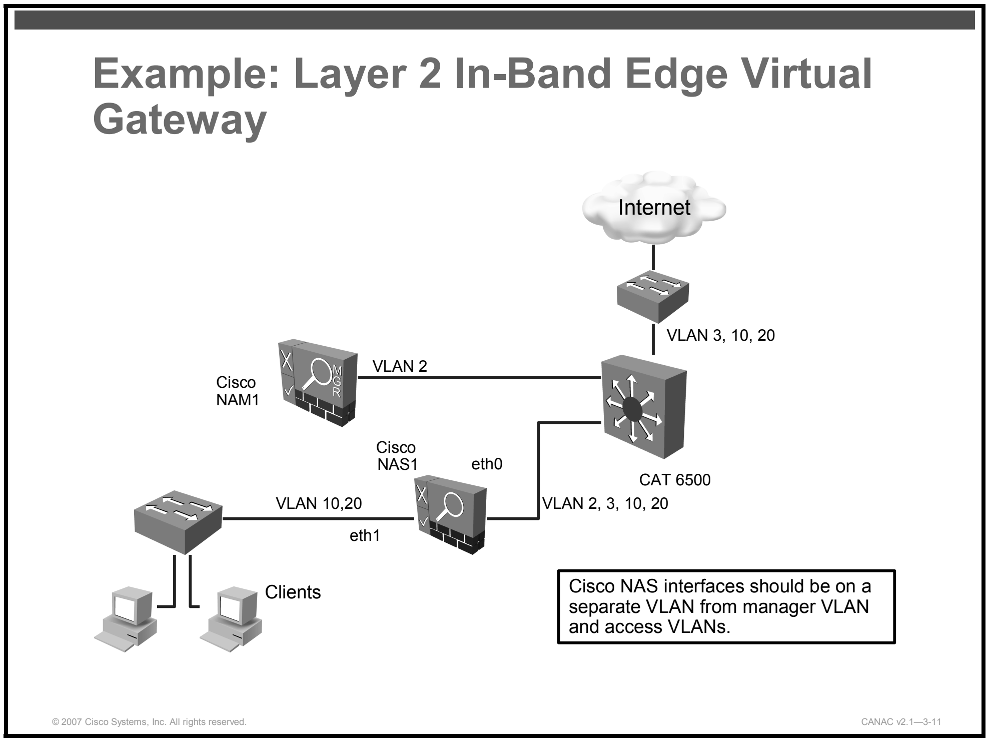
The figure shows an example of a Layer 3 in-band central virtual gateway. In this deployment, the client is separated from the Cisco NAS by multiple hops. Recall that in the in-band topology, client-generated network traffic is always routed through the Cisco NAS before and after posture assessment. The Cisco NAS securely manages traffic filters, bandwidth, VLAN retagging for each user role, and user time-outs. This topology is used when the MAC addresses of the clients are not unique.



Example: Layer 2 In-Band Edge

CANAC v2.1—3-10

In Layer 2 in-band edge deployment, the Cisco NAS is placed between each managed subnet and router in the network and can act as either a virtual bridge or a real-IP gateway.



Example: Layer 2 In-Band Edge Virtual Gateway

Cisco NAS interfaces should be on a separate VLAN from manager VLAN and access VLANs.

CANAC v2.1—3-11

The topology shows a Layer 2 in-band edge virtual gateway Cisco NAS deployment. Consider these aspects of this configuration example:

- **VLAN for the Cisco NAM:** In the figure, the management VLAN for the Cisco NAM is VLAN 2.
- **VLAN for the Cisco NAS:** This VLAN must be different from the VLAN for the Cisco NAM. In the figure, the management VLAN for the Cisco NAS is VLAN 3.
- **VLAN IDs for Access (User):** In the figure, the access VLANs are VLANs 10 and 20.
- On the switch interface that connects to eth0 of the Cisco NAS, the trunk settings have been configured for the trusted traffic. The following configuration shows an example of this setup:

```
# switchport trunk encapsulation dot1q
# switchport trunk native vlan 999
# switchport trunk allowed vlan 2,3,10,20
```

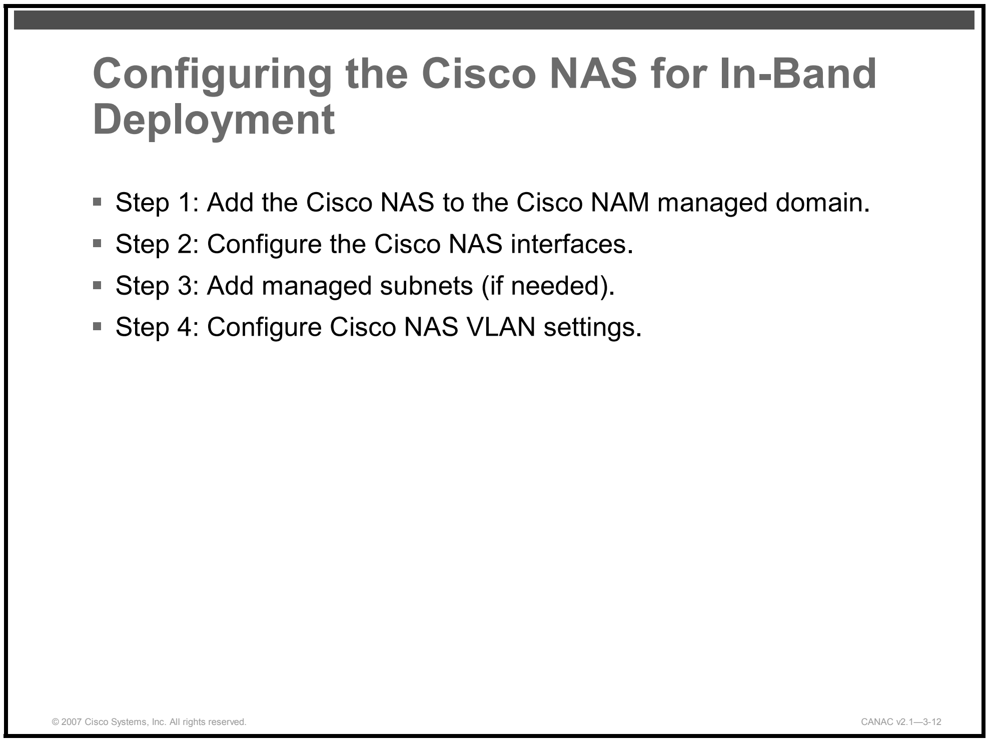
- On the edge switch interface that connects to eth1 of the Cisco NAS, the trunk settings have been configured for the untrusted traffic. The following configuration shows an example of this setup:

```
# switchport trunk encapsulation dot1q
# switchport trunk native vlan 999
# switchport trunk allowed vlan 2,3,10,20
```

Note In edge deployment, a Cisco NAS virtual gateway uses managed subnets to help devices on different untrusted VLANs arrive at the respective default gateways on the trusted side of the network.

Configuring the Cisco NAS for In-Band Deployment

This topic describes how to configure the Cisco NAS for in-band deployment.



Configuring the Cisco NAS for In-Band Deployment

- Step 1: Add the Cisco NAS to the Cisco NAM managed domain.
- Step 2: Configure the Cisco NAS interfaces.
- Step 3: Add managed subnets (if needed).
- Step 4: Configure Cisco NAS VLAN settings.

CANAC v2.1—3-12

To configure the Cisco NAS for in-band deployment, follow these steps, which are described in detail in the subsequent topics:

Step 1 **Add the Cisco NAS to the Cisco NAM managed domain:** The Cisco NAS receives its runtime parameters from the Cisco NAM and cannot operate until it is added to the Cisco NAM domain. After the Cisco NAS is installed and added to the Cisco NAM, you can configure local parameters in the Cisco NAS and monitor the Cisco NAS through the web administration console. For in-band deployment, you must choose one of the in-band server operating modes.

Step 2 **Configure the Cisco NAS interfaces:** When you use the Cisco NAS as a real-IP gateway, you must specify the IP addresses of its two interfaces: one address for the trusted side of the network and one address for the untrusted side of the network. The two addresses should be on different subnets.

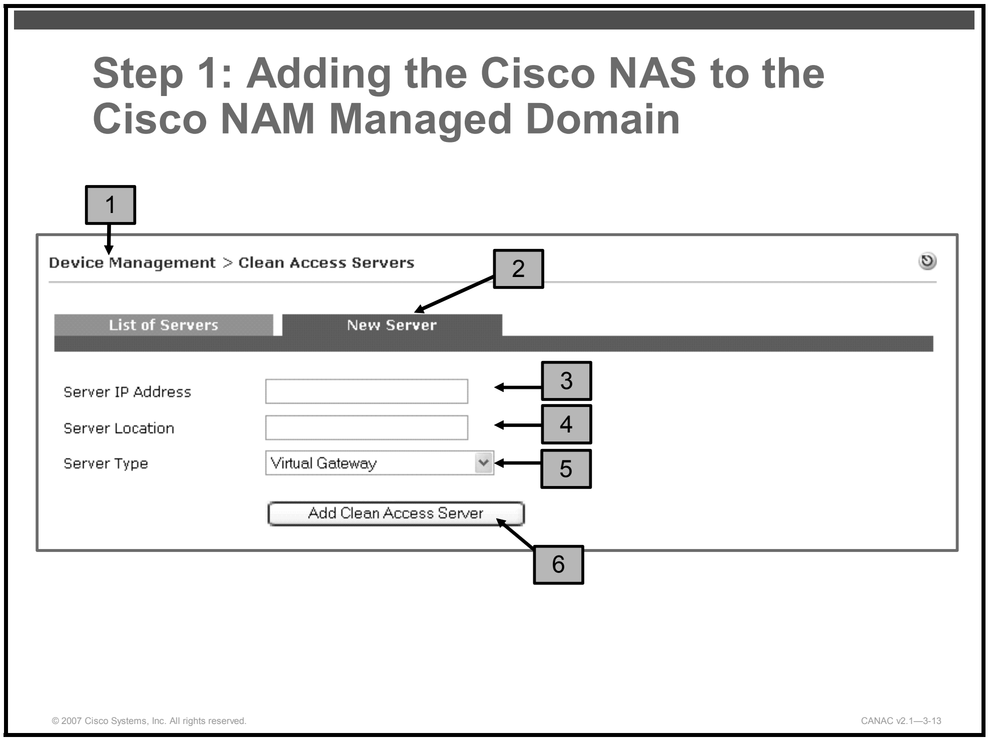
Step 3 **Add managed subnets (if needed):** When the Cisco NAS is first added to the Cisco NAM, the untrusted IP address that is provided for the Cisco NAS is automatically assigned a VLAN ID of -1 to denote that it is a main subnet. By default, the network that the Cisco NAS initially manages is the main subnet. You can configure the Cisco NAS to manage additional subnets. When the Cisco NAS manages additional subnets, the Cisco NAS untrusted interface acts as the default virtual gateway for the managed subnets.

Step 4 **Configure the Cisco NAS VLAN settings:** You can configure the Cisco NAS to act as a VLAN termination point or to perform VLAN passthrough. You can also add management VLAN IDs to tag the outbound traffic for the entire managed network, a managed subnet, or a particular user role. When the Cisco NAS operates as a virtual gateway, you must configure VLAN mapping to ensure that the incoming traffic and the outgoing traffic of the Cisco NAS are on different VLANs.

Caution To prevent loops from occurring in a central deployment, disable the untrusted interface on the Cisco NAS. After you have completed VLAN mapping, enable the untrusted interface on the Cisco NAS.

Adding the Cisco NAS to the Managed Domain

This topic describes how to add the Cisco NAS to the Cisco NAM managed domain for in-band deployment.



Step 1: Adding the Cisco NAS to the Cisco NAM Managed Domain

Device Management > Clean Access Servers

List of Servers | New Server

Server IP Address

Server Location

Server Type: Virtual Gateway

Add Clean Access Server

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—3-13

Note	The Cisco NAS must be running to be added to the Cisco NAM.

The first step in configuring the Cisco NAS for in-band deployment is to add an in-band Cisco NAS to the Cisco NAM managed domain. Complete these steps:

Step 1 From the navigation bar, choose **Device Management > Clean Access Servers.** The Cisco NAS page appears showing the list of servers that have already been configured.

Step 2 Click the **New Server** tab. The Add form appears.

Step 3 In the Server IP Address field, enter the IP address of the Cisco NAS trusted interface (eth0: the IP address connected to the trusted network).

Step 4 (Optional) In the Server Location field, enter a description of the Cisco NAS location or other identifying information.

Step 5 From the Server Type drop-down menu, choose the in-band Cisco NAS operating mode that you want to use. These are the choices for a production environment:

- **Virtual Gateway:** In this mode, the Cisco NAS operates as an IP bridge, while providing IP Security (IPsec), filtering, virus protection, and other services.
- **Real-IP Gateway:** In this mode, the Cisco NAS acts as the default gateway for the untrusted network.

Note The Network Address Translation (NAT) gateway mode option is not recommended for production environments.

Step 6 Click **Add Clean Access Server**. The Cisco NAM looks for the Cisco NAS on the network and adds it to its list of managed servers.

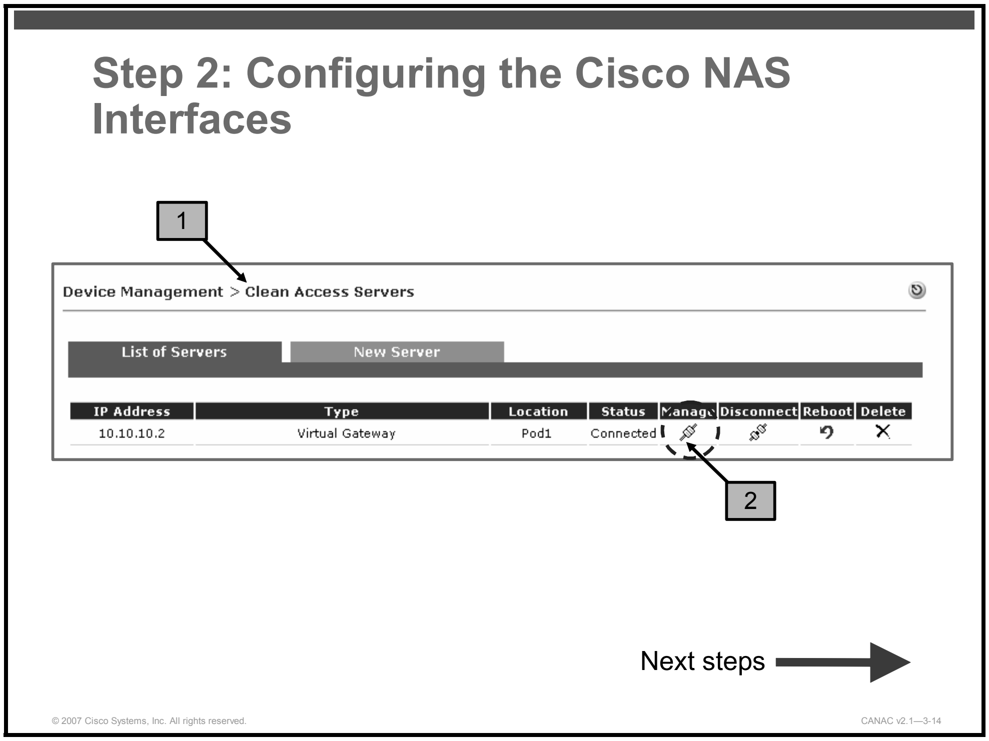
The Cisco NAS is now in the Cisco NAM administrative domain.

If the Cisco NAS cannot be added to Cisco NAM, check these conditions:

- The shared secret password is the same on the Cisco NAS and Cisco NAM.
- The SSL certificates for the Cisco NAM and Cisco NAS are correct.
- There is connectivity between the Cisco NAS and Cisco NAM and there are no firewall rules blocking Remote Method Invocation (RMI) ports.

Configuring the Cisco NAS Interfaces

This topic describes how to use the Cisco NAM to configure the trusted and untrusted interfaces of the Cisco NAS.



Step 2: Configuring the Cisco NAS Interfaces

Device Management > Clean Access Servers

List of Servers | New Server

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.10.10.2	Virtual Gateway	Pod1	Connected				✕

Next steps

© 2007 Cisco Systems, Inc. All rights reserved.

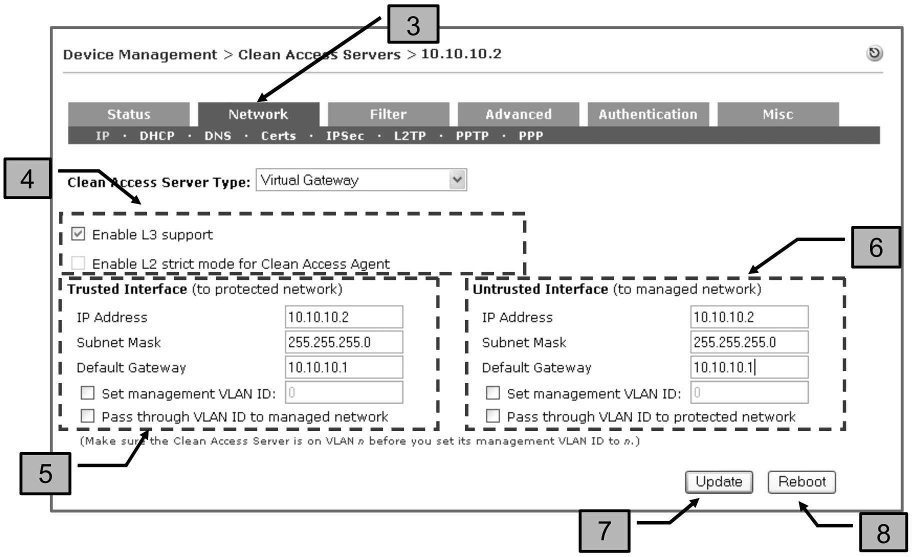
CANAC v2.1—3-14

To configure the Cisco NAS interface network settings, complete these steps:

Step 1 From the Device Management menu, choose **Clean Access Servers**.

Step 2 On the list of Clean Access servers, click the **Manage** button next to the server that you want to configure.

Step 2: Configuring the Cisco NAS Interfaces (Cont.)



Device Management > Clean Access Servers > 10.10.10.2

Clean Access Server Type: Virtual Gateway

☑ Enable L3 support

□ Enable L2 strict mode for Clean Access Agent

Trusted Interface (to protected network)

IP Address	10.10.10.2
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.1
□ Set management VLAN ID:	0

□ Pass through VLAN ID to managed network

Untrusted Interface (to managed network)

IP Address	10.10.10.2
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.1
□ Set management VLAN ID:	0

□ Pass through VLAN ID to protected network

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

CANAC v2.1—3-15

Step 3 Click the **Network** tab. The IP form appears showing the network settings for the Cisco NAS interfaces.

Step 4 Check the **Enable L3 support** check box. With this option selected, the Cisco NAS allows access to all users from any number of hops away. When the Enable L2 strict mode for Clean Access Agent option is selected, the Cisco NAS does not allow network access to client machines configured with the Cisco NAA who are more than one hop away from the Cisco NAS. The user with a Cisco NAA configured on their machine will have to be Layer 2-connected to the Cisco NAS before gaining access to the network.

Step 5 In the Trusted Interface area, enter the appropriate network settings for the trusted (eth0) interface in the corresponding fields. The trusted interface IP address should be on a different subnet from the subnet of the untrusted interface.

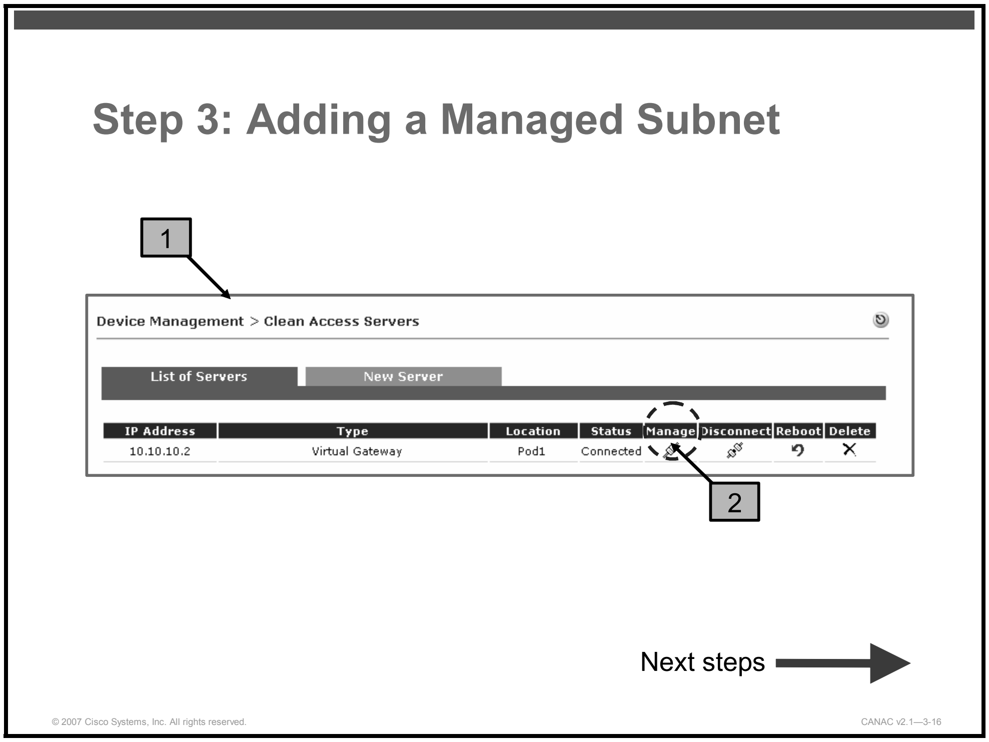
Step 6 In the Untrusted Interface area, enter the appropriate network settings for the untrusted (eth1) interface in the corresponding fields. The untrusted interface IP address should be on a different subnet from the subnet of the trusted interface.

Step 7 Click the **Update** button.

Step 8 Click **Reboot**. The Cisco NAS will show a status of Not Connected while it reboots. Wait until the Cisco NAS shows a Connected status.

Adding Managed Subnets

This topic describes how to add managed subnets on the Cisco NAS.



Step 3: Adding a Managed Subnet

Device Management > Clean Access Servers

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.10.10.2	Virtual Gateway	Pod1	Connected			↺	✕

Next steps

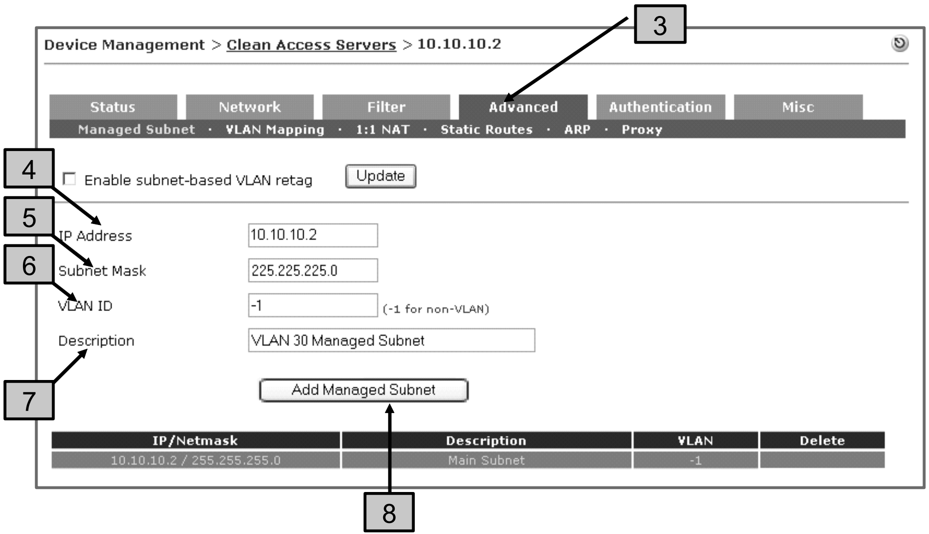
CANAC v2.1—3-16

To add a managed subnet to the NAS, complete these steps:

Step 1 From the Device Management menu, choose **Clean Access Servers**.

Step 2 On the list of servers, click the **Manage** button next to the server that you want to configure.

Step 3: Adding a Managed Subnet (Cont.)



Device Management > Clean Access Servers > 10.10.10.2

□ Enable subnet-based VLAN retag

IP Address: 10.10.10.2

Subnet Mask: 225.225.225.0

VLAN ID: -1 (-1 for non-VLAN)

Description: VLAN 30 Managed Subnet

IP/Netmask	Description	VLAN	Delete
10.10.10.2 / 255.255.255.0	Main Subnet	-1	

CANAC v2.1—3-17

Step 3 Click the **Advanced** tab. The Managed Subnet page appears by default.

Step 4 In the IP Address field, enter the IP address of the gateway for the subnet you want to add. This IP address should be the address that is assigned to the Cisco NAS to route the subnet, not the network address that is calculated by applying the subnet mask to the gateway address.

Step 5 Enter the mask for the network address in the Subnet Mask field. The Cisco NAM calculates the network address by applying the subnet mask to the gateway address in the IP Address field.

Step 6 If a VLAN ID is associated with this subnet, enter this VLAN ID in the VLAN ID field. Use -1 if the subnet is not on a VLAN.

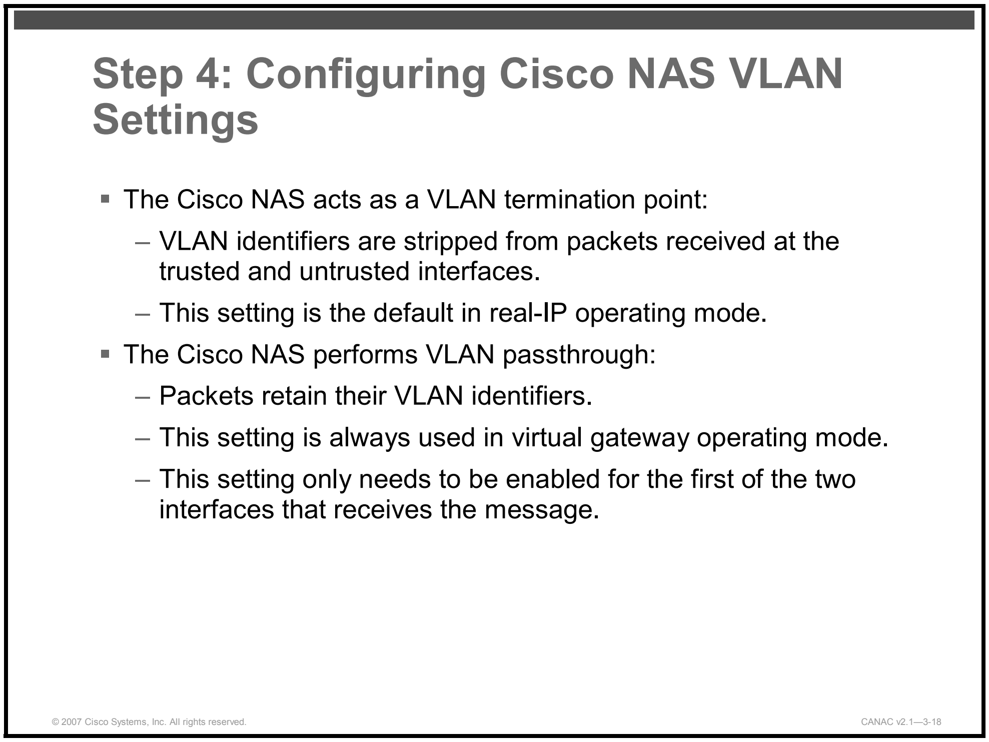
Step 7 (Optional) Add a description for the managed subnet in the Description field.

Step 8 Click the **Add Managed Subnet** button to add the subnet to the list of managed subnets.

The new managed subnet appears in the list of subnets in the bottom half of the screen.

Configuring Cisco NAS VLAN Settings

This topic describes how to configure Cisco NAS VLAN settings.



Step 4: Configuring Cisco NAS VLAN Settings

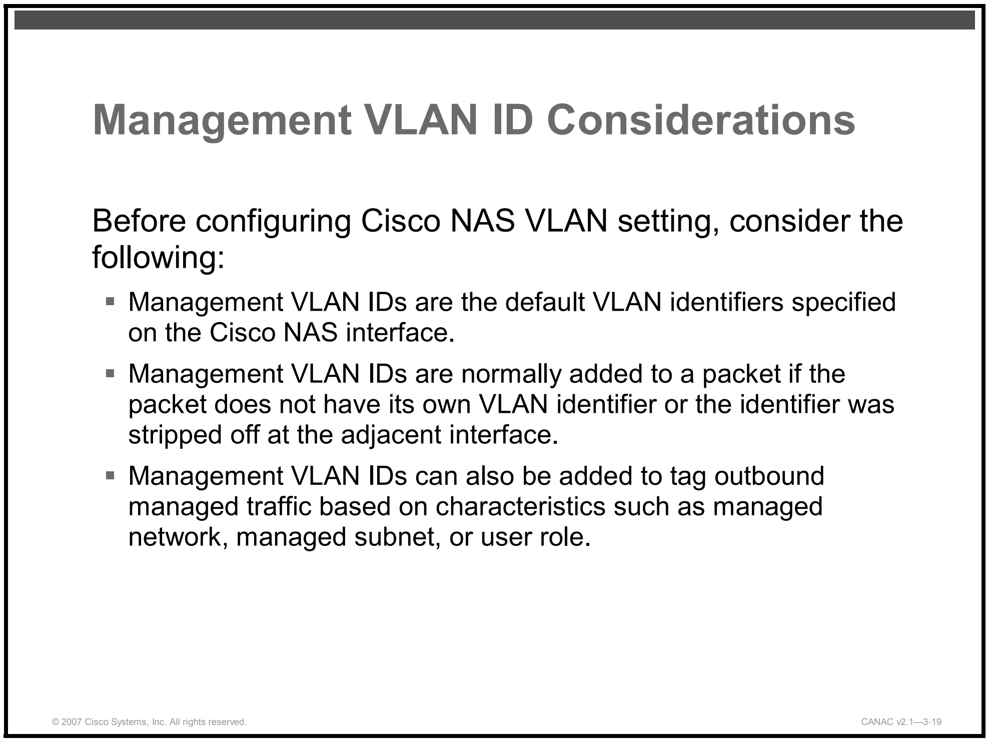
- The Cisco NAS acts as a VLAN termination point:
  - VLAN identifiers are stripped from packets received at the trusted and untrusted interfaces.
  - This setting is the default in real-IP operating mode.
- The Cisco NAS performs VLAN passthrough:
  - Packets retain their VLAN identifiers.
  - This setting is always used in virtual gateway operating mode.
  - This setting only needs to be enabled for the first of the two interfaces that receives the message.

CANAC v2.1—3-18

You can configure the Cisco NAS to handle VLAN identifiers in one of two ways:

- **Act as a VLAN termination point:** In a real-IP gateway configuration, if VLAN support is enabled for the Cisco NAS, by default the VLAN identifiers are terminated at the Cisco NAS (that is, identifiers are stripped from packets received at the trusted and untrusted interfaces).
- **Perform VLAN passthrough:** If you enable VLAN ID passthrough, packets retain their VLAN identifiers. For the VLAN identifier to be retained, passthrough needs to be enabled only for the first of the two interfaces that receive the message. In a virtual gateway configuration, VLAN IDs are always passed through the Cisco NAS.

Note In most cases, VLAN passthrough does not need to be used. If you are unsure of which mode to use, you should use the default behavior of the Cisco NAS.



Management VLAN ID Considerations

Before configuring Cisco NAS VLAN setting, consider the following:

- Management VLAN IDs are the default VLAN identifiers specified on the Cisco NAS interface.
- Management VLAN IDs are normally added to a packet if the packet does not have its own VLAN identifier or the identifier was stripped off at the adjacent interface.
- Management VLAN IDs can also be added to tag outbound managed traffic based on characteristics such as managed network, managed subnet, or user role.

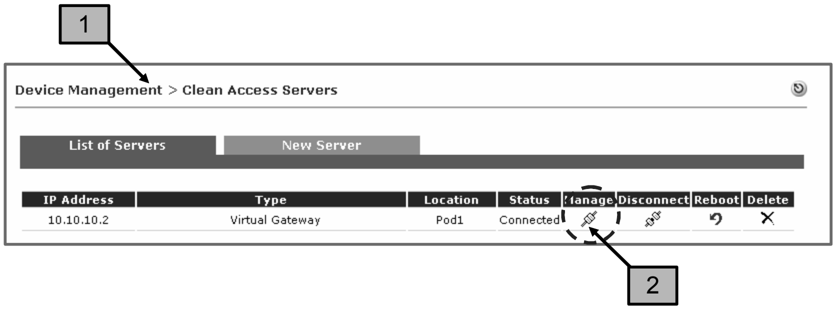
CANAC v2.1—3-19

A management VLAN identifier is a default VLAN identifier. If a packet does not have its own VLAN identifier, or if the identifier was stripped by the adjacent interface, a management VLAN identifier specified at the interface is added to the packets. By setting the management VLAN ID value for the managed network, you can add VLAN ID tags to the outbound traffic of the entire managed network. You can also set VLAN IDs based on other characteristics. Specifically, the Cisco NAS can tag outbound traffic by managed network, managed subnet, or user role.

You can apply roles to users that are authenticated by an external authentication source based on the VLAN ID. Refer to the New Role section in the *Cisco Clean Access Manager Installation and Administration Guide* for further details on VLAN retagging.

Caution Use care when configuring VLAN settings. Incorrect VLAN settings can cause the Cisco NAS to be inaccessible from the Cisco NAM administration console. If you cannot access the Cisco NAS from the Cisco NAM after modifying the VLAN settings, you will need to access the Cisco NAS directly through a serial connection to correct its configuration.

Step 4: Configuring Cisco NAS VLAN Settings (Cont.)



Device Management > Clean Access Servers

List of Servers | New Server

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.10.10.2	Virtual Gateway	Pod1	Connected			↺	✕

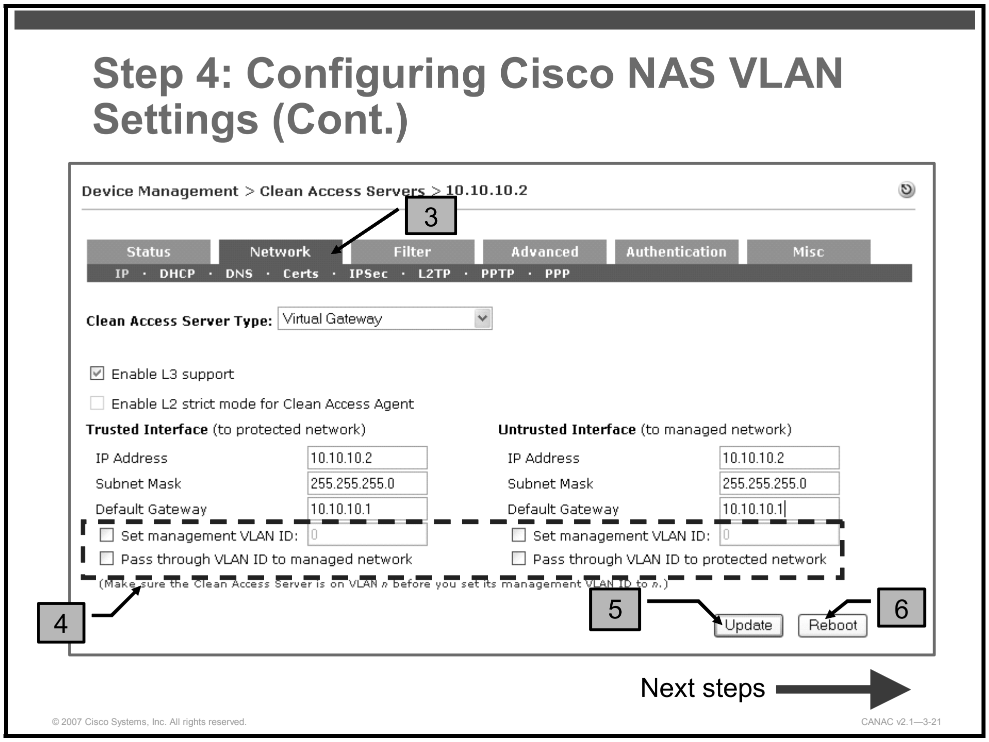
Next steps →

CANAC v2.1—3-20

To configure VLAN settings for the Cisco NAS, complete these steps:

Step 1 From the Device Management menu, choose **Clean Access Servers**.

Step 2 On the list of servers, click the **Manage** button next to the server that you want to configure.



Step 4: Configuring Cisco NAS VLAN Settings (Cont.)

Device Management > Clean Access Servers > 10.10.10.2

Clean Access Server Type: Virtual Gateway

☑ Enable L3 support

□ Enable L2 strict mode for Clean Access Agent

Trusted Interface (to protected network)		**Untrusted Interface** (to managed network)	
IP Address	10.10.10.2	IP Address	10.10.10.2
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.10.10.1	Default Gateway	10.10.10.1
□ Set management VLAN ID:	0	□ Set management VLAN ID:	0
□ Pass through VLAN ID to managed network		□ Pass through VLAN ID to protected network	

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—3-21

Step 3 Click the **Network** tab. The IP form appears showing the network settings for the Cisco NAS interfaces.

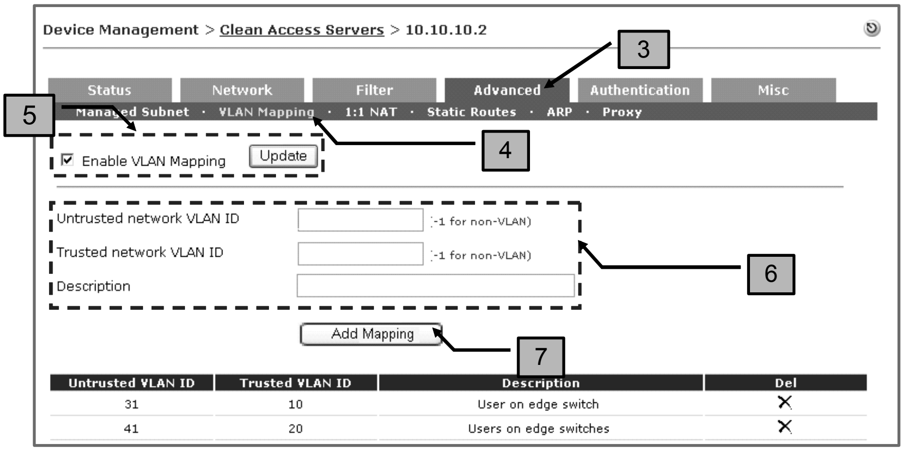
Step 4 Enter the appropriate management VLAN settings for the trusted and untrusted interfaces in the corresponding fields of these settings.

- **Set Management VLAN ID:** Check this check box and enter a default VLAN ID value to have the specified default VLAN identifier value added to packets that do not have an identifier. If this option is set at the untrusted interface, the default VLAN ID is added to packets directed to managed clients. If this option is set at the trusted interface, the default VLAN ID is added to packets destined for the trusted (protected) network.
- **Pass Through VLAN ID to Managed Network** and **Pass Through VLAN ID to Protected Network:** If one of these check boxes is checked, VLAN identifiers in the packets pass through the interface unmodified.

Step 5 Click the **Update** button.

Step 6 Click **Reboot**. The Cisco NAS will show a status of Not Connected while it reboots. Wait for the Cisco NAS to show a Connected status.

Step 4: Configuring VLAN Mapping in Virtual Gateway Mode


Device Management > Clean Access Servers > 10.10.10.2
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · 1:1 NAT · Static Routes · ARP · Proxy
Update
Add Mapping
3
4
5
6
7

☑ Enable VLAN Mapping

Untrusted network VLAN ID		(-1 for non-VLAN)
Trusted network VLAN ID		(-1 for non-VLAN)
Description		

Untrusted VLAN ID	Trusted VLAN ID	Description	Del
31	10	User on edge switch	✕
41	20	Users on edge switches	✕

Cisco NAS uses VLAN mapping to retag allowed traffic from the untrusted VLAN to the trusted VLAN.

CANAC v2.1—3-22

When the Cisco NAS operates in virtual gateway mode, the Cisco NAS passes network traffic from its eth0 interface to eth1 and from eth1 to eth0 without changing the VLAN tag. For in-band configurations, in order to pass traffic from both interfaces through the same Layer 2 switch without creating a loop, you must place incoming traffic to the Cisco NAS on a different VLAN from the VLAN for the outgoing traffic of the Cisco NAS.

For virtual gateway mode only, the VLAN mapping form appears under Device Management > Clean Access Servers > [IP address] > Advanced > VLAN Mapping. This form allows you to map an untrusted interface VLAN ID to a trusted network VLAN ID. Traffic going through the Cisco NAS will be VLAN-retagged according to this VLAN mapping setting.

To configure VLAN mapping in virtual gateway mode, complete these steps:

Step 1 From the Device Management menu, choose **Clean Access Servers** (not shown).

Step 2 On the list of servers, click the **Manage** button next to the server that you want to configure (not shown).

Step 3 Click the **Advanced** tab.

Step 4 Click the **VLAN Mapping** submenu link.

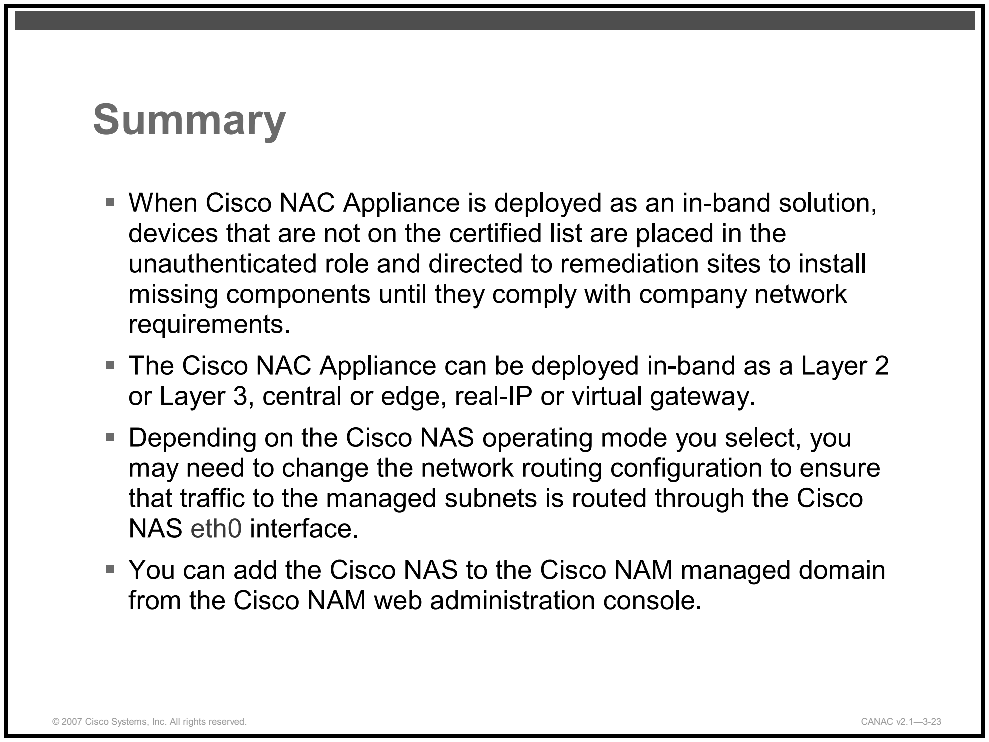
Step 5 Check the **Enable VLAN Mapping** check box and then click the **Update** button.

Step 6 Enter the VLAN ID values for the untrusted and trusted networks and an optional description in the Description field, if a description is needed.

Step 7 Click the **Add Mapping** button. Traffic going through the Cisco NAS will now be VLAN-retagged according to the settings that you configured.

Summary

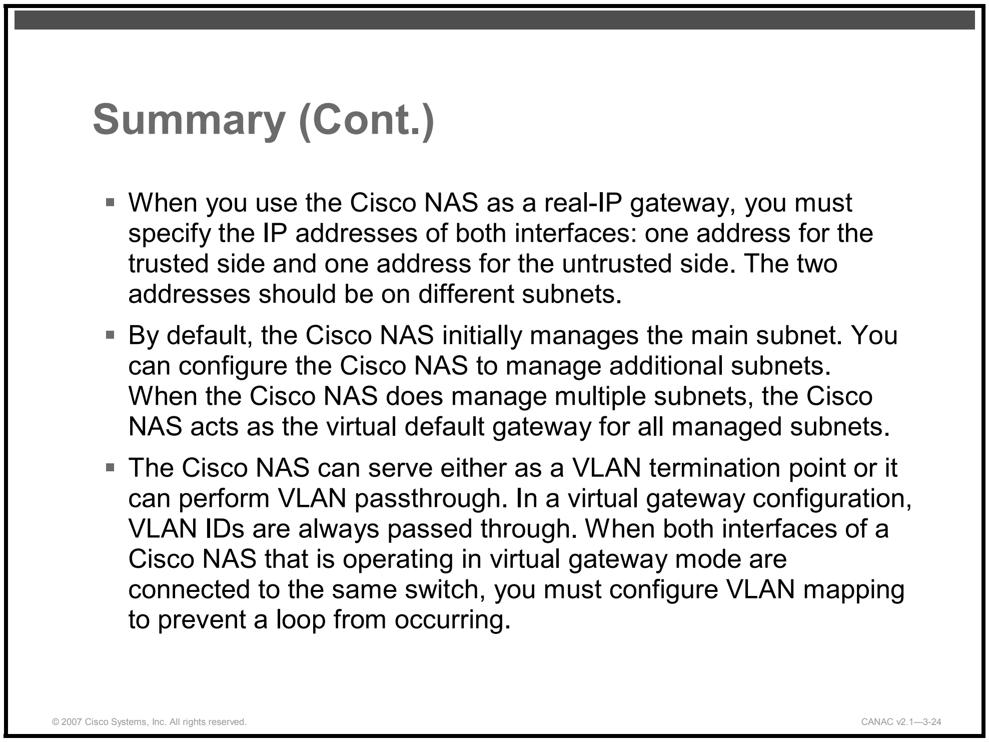
This topic summarizes the key points that were discussed in this lesson.



Summary

- When Cisco NAC Appliance is deployed as an in-band solution, devices that are not on the certified list are placed in the unauthenticated role and directed to remediation sites to install missing components until they comply with company network requirements.
- The Cisco NAC Appliance can be deployed in-band as a Layer 2 or Layer 3, central or edge, real-IP or virtual gateway.
- Depending on the Cisco NAS operating mode you select, you may need to change the network routing configuration to ensure that traffic to the managed subnets is routed through the Cisco NAS eth0 interface.
- You can add the Cisco NAS to the Cisco NAM managed domain from the Cisco NAM web administration console.

CANAC v2.1—3-23



Summary (Cont.)

- When you use the Cisco NAS as a real-IP gateway, you must specify the IP addresses of both interfaces: one address for the trusted side and one address for the untrusted side. The two addresses should be on different subnets.
- By default, the Cisco NAS initially manages the main subnet. You can configure the Cisco NAS to manage additional subnets. When the Cisco NAS does manage multiple subnets, the Cisco NAS acts as the virtual default gateway for all managed subnets.
- The Cisco NAS can serve either as a VLAN termination point or it can perform VLAN passthrough. In a virtual gateway configuration, VLAN IDs are always passed through. When both interfaces of a Cisco NAS that is operating in virtual gateway mode are connected to the same switch, you must configure VLAN mapping to prevent a loop from occurring.

CANAC v2.1—3-24

Lesson 2

Implementing the Microsoft Windows SSO Feature on the Cisco NAC Appliance

Overview

This lesson describes how to implement the Cisco Network Admission Control (NAC) Appliance single sign-on feature using the Microsoft Windows single sign-on (SSO) with Active Directory.

Because the Active Directory feature of Microsoft Windows Server is a widely used feature, a Cisco NAC Appliance solution typically includes the configuration of the Windows SSO feature. Being able to configure the Cisco NAC Appliance Microsoft Windows SSO feature for client and server machines is a key skill for an NAC endpoint security specialist.

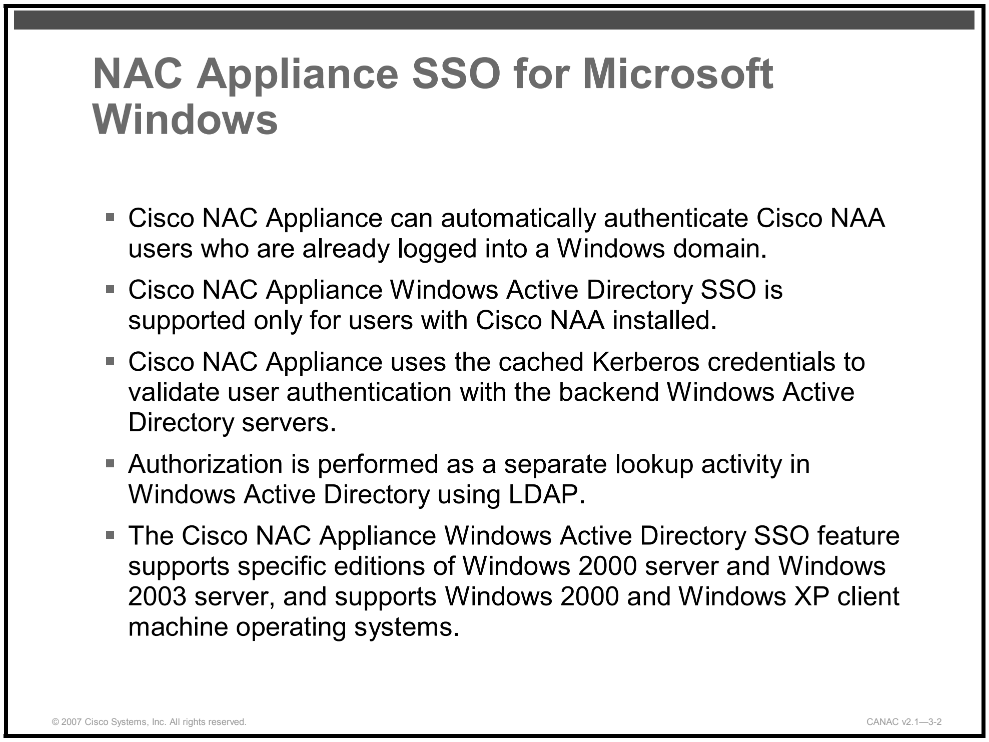
Objectives

Upon completing this lesson, you will be able to configure the Cisco NAC Appliance Server (Cisco NAS) to support the Cisco NAC Appliance Microsoft Windows SSO with Active Directory feature for client and server machines to meet customer remote access requirements. This ability includes being able to meet these objectives:

- Describe how Cisco NAC Appliance uses Windows SSO to ensure increased security
- Summarize the process used by Microsoft Windows to exchange Kerberos tickets with the Cisco NAS
- Describe how a Cisco NAS communicates with a Microsoft Windows Active Directory server
- Describe the steps that are used to configure Active Directory SSO for the Cisco NAM, Cisco NAS, and Microsoft Windows Active Directory Server

Cisco NAC Appliance SSO for Microsoft Windows

This topic describes how Cisco NAC Appliance uses Windows SSO to ensure increased security.



NAC Appliance SSO for Microsoft Windows

- Cisco NAC Appliance can automatically authenticate Cisco NAA users who are already logged into a Windows domain.
- Cisco NAC Appliance Windows Active Directory SSO is supported only for users with Cisco NAA installed.
- Cisco NAC Appliance uses the cached Kerberos credentials to validate user authentication with the backend Windows Active Directory servers.
- Authorization is performed as a separate lookup activity in Windows Active Directory using LDAP.
- The Cisco NAC Appliance Windows Active Directory SSO feature supports specific editions of Windows 2000 server and Windows 2003 server, and supports Windows 2000 and Windows XP client machine operating systems.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-2

Cisco NAC Appliance can automatically authenticate the Cisco NAC Appliance Agent (Cisco NAA) users who are already logged in to a Windows domain. This feature allows users logging in to their systems using Ctrl-Alt-Del to automatically go through posture assessment and Cisco NAC Appliance certification without having to log in through the Cisco NAA.

Note Active Directory SSO is supported only for users who have Cisco NAA installed.

Cisco NAC Appliance uses the cached credentials and a Kerberos ticket from the client machine Windows login. The cached credentials and Kerberos ticket are used to validate the user authentication with the backend Windows 2000 and Windows 2003 Active Directory server. After the user authentication is validated, authorization occurs in the form of role-mapping as a separate lookup activity on the Windows Active Directory server using Lightweight Directory Access Protocol (LDAP).

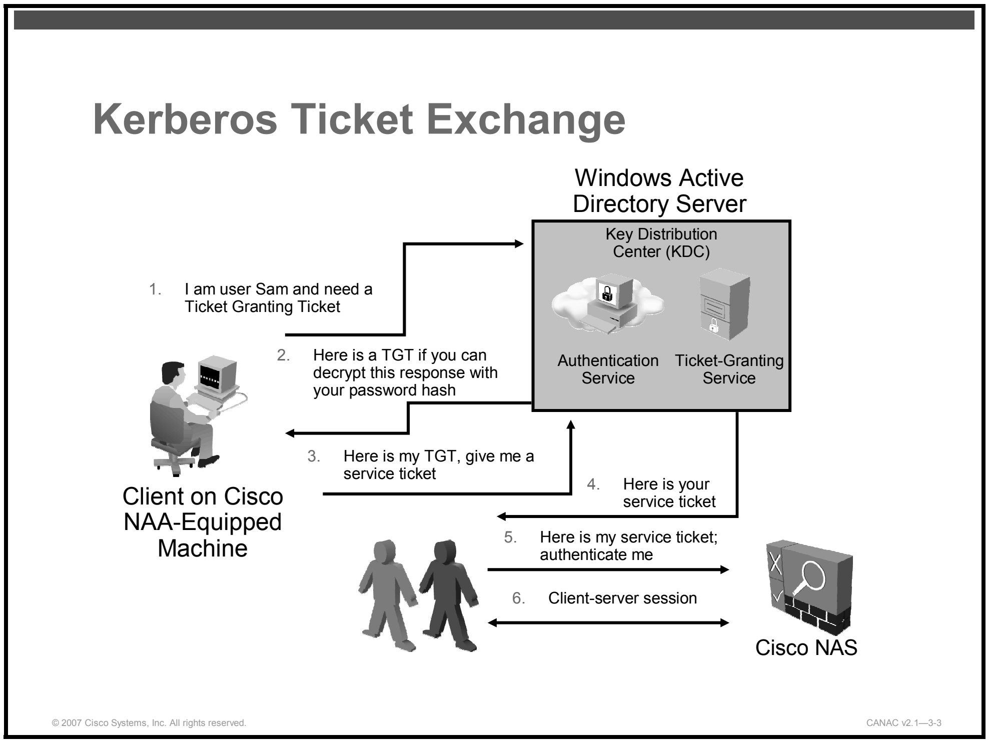
The Windows Active Directory SSO Support table shows which client machines the Cisco NAC Appliance supports, and on which servers that the Cisco NAC Appliance currently supports the Windows SSO feature.

Windows Active Directory SSO Support

Active Directory Servers	Client Machine
■ Windows 2000 Server service pack 4 ■ Windows 2003 Enterprise service pack 1 ■ Windows 2003 Enterprise R2 ■ Windows 2003 Standard service pack 1	■ Windows 2000 service pack 4 ■ Windows XP (Home and Professional) service pack 1 and 2 and later

Kerberos Ticket Exchange

This topic summarizes the process used by Microsoft Windows to exchange Kerberos tickets with the Cisco NAS.



Kerberos Ticket Exchange

Windows Active Directory Server

Key Distribution Center (KDC)

Authentication Service

Ticket-Granting Service

1. I am user Sam and need a Ticket Granting Ticket

2. Here is a TGT if you can decrypt this response with your password hash

3. Here is my TGT, give me a service ticket

4. Here is your service ticket

5. Here is my service ticket; authenticate me

6. Client-server session

Client on Cisco NAA-Equipped Machine

Cisco NAS

CANAC v2.1—3-3

The figure shows the process that the client machine goes through when Windows Active Directory SSO is in effect. In this scenario, the client using a Cisco NAA-equipped machine and the Cisco NAS both have an account on the Windows Active Directory server. The process for authentication has six steps:

Step 1 The client logs in to the Windows Active Directory server (or uses cached credentials) and requests a ticket-granting ticket (TGT) from the Windows Active Directory server.

Step 2 Using the client machine credentials, the Active Directory server authenticates the client machine and sends back a TGT to the client machine.

Step 3 The Cisco NAA asks the client machine to request a Kerberos service ticket from the Active Directory server with the Cisco NAS username so that the Cisco NAA can communicate directly with the Cisco NAS.

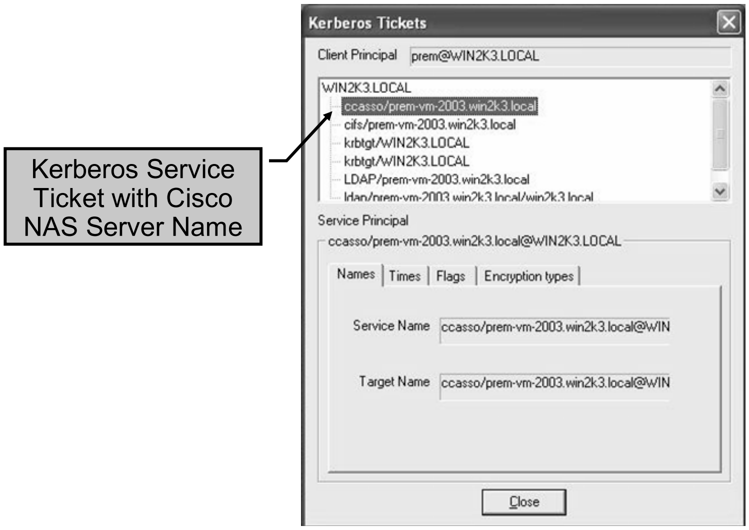
Step 4 The Windows Active Directory server sends the Kerberos service ticket to the client machine, and the client machine then gives the Kerberos service ticket to the Cisco NAA. Now the Cisco NAA can communicate with the Cisco NAS directly.

Step 5 The Cisco NAA sends the Kerberos service ticket and the client authentication information to the Cisco NAS and requests access to the network. In the figure, the two men are a symbol for the Kerberos ticket exchange between the Cisco NAA and the Cisco NAS.

Step 6 The client machine is signed on using only the Windows Active Directory server credentials of the machine.

Note For additional user role-mapping (for Cisco NAC Appliance certification and posture assessment), you can configure an LDAP lookup server with attribute mapping, as described later in this lesson.

Confirming Cisco NAS Kerberos Ticket



Kerberos Tickets

Client Principal: prem@WIN2K3.LOCAL

```
WIN2K3.LOCAL
  ccasso/prem-vm-2003.win2k3.local
  cifs/prem-vm-2003.win2k3.local
  krbtgt/WIN2K3.LOCAL
  krbtgt/WIN2K3.LOCAL
  LDAP/prem-vm-2003.win2k3.local
  ldap/prem-vm-2003.win2k3.local/win2k3.local
```

Service Principal: ccasso/prem-vm-2003.win2k3.local@WIN2K3.LOCAL

Service Name: ccasso/prem-vm-2003.win2k3.local@WIN

Target Name: ccasso/prem-vm-2003.win2k3.local@WIN

Kerberos Service Ticket with Cisco NAS Server Name

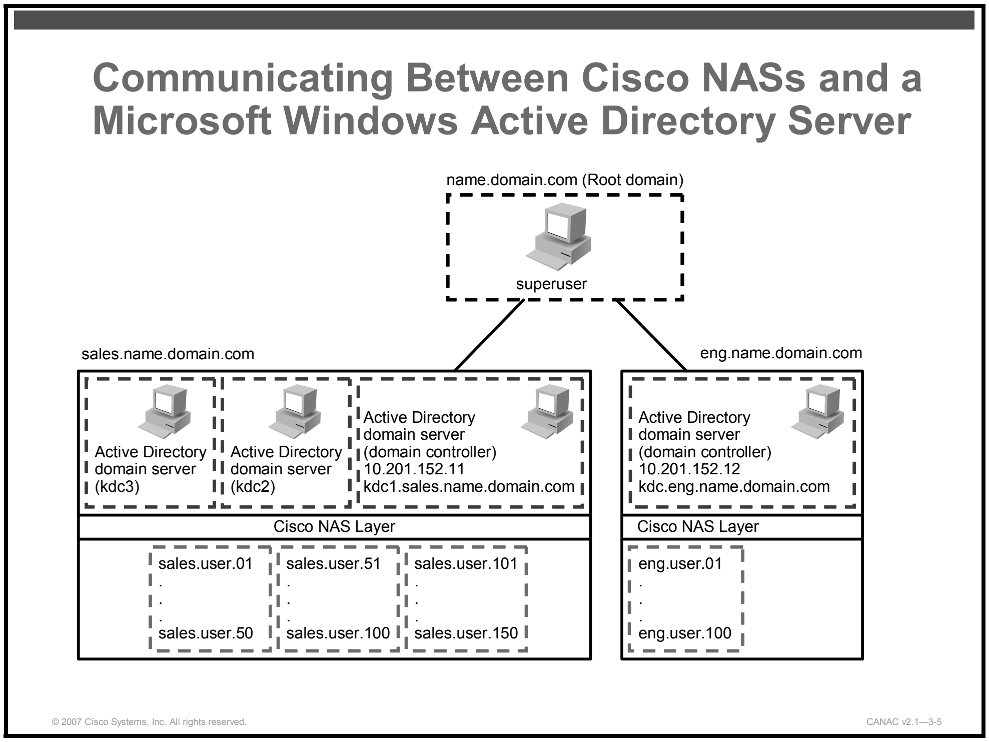
CANAC v2.1—3-4

The figure shows a dialog box of the Microsoft utility called Kerbtray running on a client machine. The dialog box shows a Kerberos service ticket with the username of the Cisco NAS, “ccasso”. Recall that the Cisco NAA asks the client machine to request a Kerberos service ticket from the Active Directory server with the Cisco NAS username. The Cisco NAA uses the Kerberos service ticket to communicate directly with the Cisco NAS. Kerbtray is a useful tool to help you confirm that a client machine receives the correct Kerberos tickets.

Note The Kerbtray utility displays ticket information for a given computer running the Kerberos protocol. The Kerbtray utility is freely available from Microsoft.com.

Communicating Between Cisco NAS and a Microsoft Windows Active Directory Server

This topic describes how a Cisco NAS communicates with a Microsoft Windows Active Directory server.



Communicating Between Cisco NASs and a Microsoft Windows Active Directory Server

name.domain.com (Root domain)

superuser

sales.name.domain.com

Active Directory domain server (kdc3)

Active Directory domain server (kdc2)

Active Directory domain server (domain controller) 10.201.152.11 kdc1.sales.name.domain.com

Cisco NAS Layer

sales.user.01 . . . sales.user.50

sales.user.51 . . . sales.user.100

sales.user.101 . . . sales.user.150

eng.name.domain.com

Active Directory domain server (domain controller) 10.201.152.12 kdc.eng.name.domain.com

Cisco NAS Layer

eng.user.01 . . . eng.user.100

CANAC v2.1—3-5

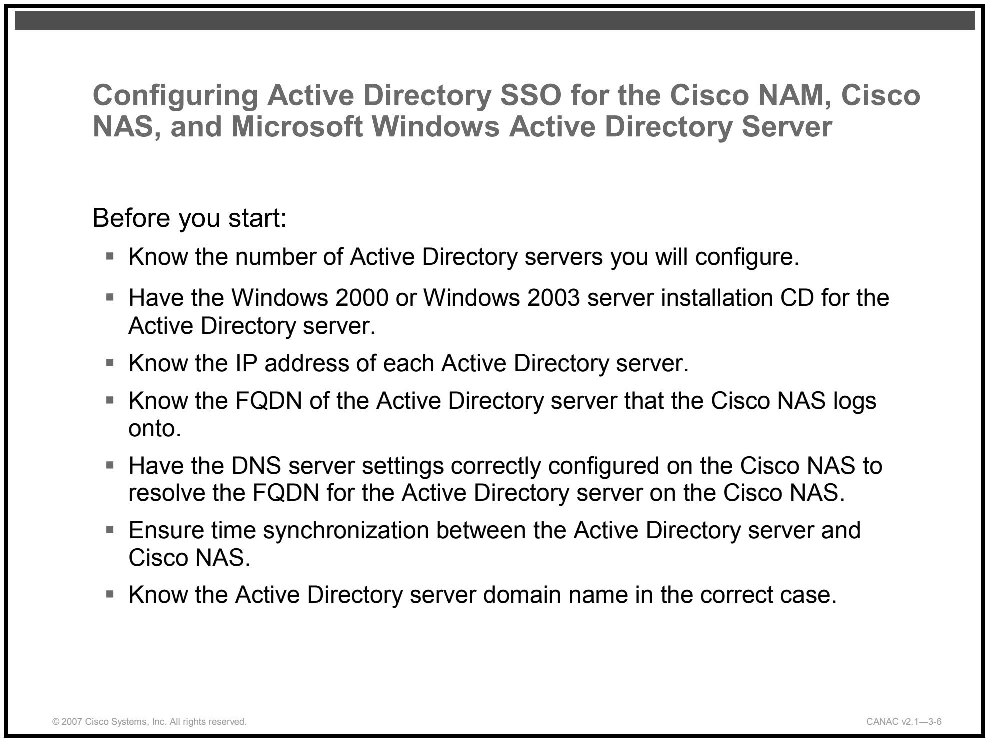
The slide shows the logical diagram for Cisco NAS communication with the Active Directory server for Microsoft Windows SSO. The Cisco NAS has a user account on the Windows Active Directory server. When you enable the service on the Cisco NAS, the Cisco NAS authenticates itself with the local domain Active Directory server. The local domain server then propagates the Cisco NAS user credentials to the root domain.

The Cisco NAS sends user login traffic only to the Active Directory servers under the root domain. In the example, the sales domain (sales.name.domain.com) and the engineering domain (eng.name.domain.com) are configured under different Cisco NASs.

Because the Cisco NAS has its credentials propagated to the root domain, the sales Cisco NAS users, as an example, need only to be created and configured on the kdc1.sales.name.domain.com Windows Active Directory server for the users in the sales.name.domain.com to be able to log in to the engineering domain or any domain controlled by the root domain server.

Configuring Active Directory SSO for the Cisco NAM, Cisco NAS, and Microsoft Windows Active Directory Server

This topic describes the steps that are used to configure Active Directory SSO for the Cisco NAM, Cisco NAS, and Microsoft Windows Active Directory Server.



Configuring Active Directory SSO for the Cisco NAM, Cisco NAS, and Microsoft Windows Active Directory Server

Before you start:

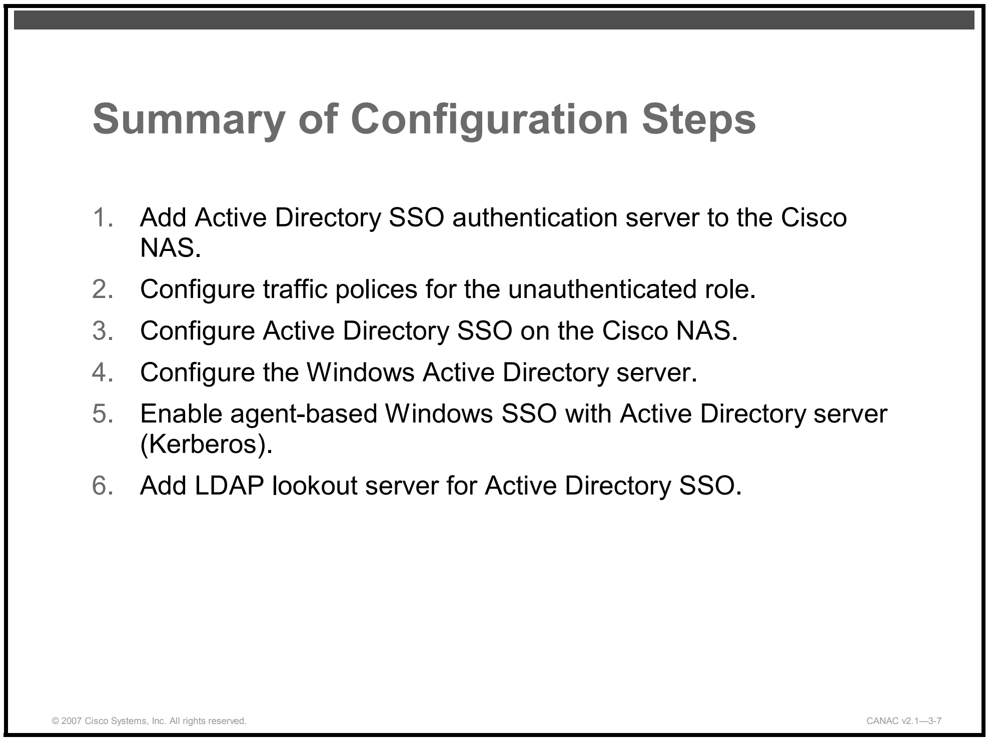
- Know the number of Active Directory servers you will configure.
- Have the Windows 2000 or Windows 2003 server installation CD for the Active Directory server.
- Know the IP address of each Active Directory server.
- Know the FQDN of the Active Directory server that the Cisco NAS logs onto.
- Have the DNS server settings correctly configured on the Cisco NAS to resolve the FQDN for the Active Directory server on the Cisco NAS.
- Ensure time synchronization between the Active Directory server and Cisco NAS.
- Know the Active Directory server domain name in the correct case.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-6

You must know the following before you begin to configure Active Directory SSO.

- **Know the number of Active Directory servers that you will configure:** Typically, the Cisco NAS corresponds to one Active Directory server.
- **Have the Windows 2000 or Windows 2003 server installation CD for the Active Directory server:** You will need the CD to install support tools for the **ktpass.exe** command. Running the **ktpass.exe** command is a requirement only on the Active Directory server (acting as the domain controller) that the Cisco NAS is logging in to.
- **Know the IP address of each Active Directory server:** This information is used to configure unauthenticated role traffic policies. You will need to allow traffic to the Cisco NAS for every Active Directory server that is in charge of that domain (this server is the domain controller). For example, if users can log onto multiple domain controllers in the domain, you should allow traffic to all the multiple domain controllers for the unauthenticated role.
- **Know the fully qualified domain name (FQDN) of the Active Directory server that the Cisco NAS logs in to:** You will use the FQDN for Cisco NAS configuration.
- **Have the Domain Name System (DNS) server settings correctly configured on the Cisco NAS:** All DNS settings are configured under Device Management > CCA Servers > Manage [CAS_IP] > Network > DNS. You will use these settings to resolve the FQDN for the Active Directory server on the Cisco NAS.

- **Ensure time synchronization between the Active Directory and Cisco NAS:** Time synchronization is required because Kerberos needs to have the clock settings on the components that take part in the authentication procedure with a time difference of less than five minutes (300 seconds).
- **Enter and know the Active Directory domain name in Kerberos format:** This naming convention applies to Windows 2000 and above. The correctly formatted name (correct case) is needed for both Cisco NAS configuration and command-line interface (CLI) configuration of the Active Directory server.



Summary of Configuration Steps

1. Add Active Directory SSO authentication server to the Cisco NAS.
2. Configure traffic polices for the unauthenticated role.
3. Configure Active Directory SSO on the Cisco NAS.
4. Configure the Windows Active Directory server.
5. Enable agent-based Windows SSO with Active Directory server (Kerberos).
6. Add LDAP lookout server for Active Directory SSO.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-7

The slide summarizes the steps that are used to configure Active Directory SSO:

Step 1 **Add Active Directory SSO authentication server:** On the Cisco NAM, add a new authentication server of type Active Directory SSO and specify a default role for users.

Step 2 **Configure traffic policies for the unauthenticated role:** Open ports on the Cisco NAS to allow client authentication traffic to pass through the Cisco NAS to and from the Active Directory server.

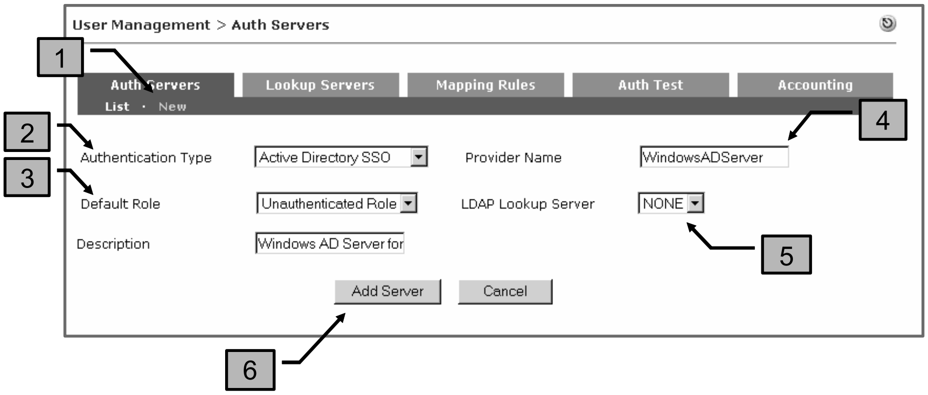
Step 3 **Configure Active Directory SSO on the Cisco NAS:** From the Cisco NAS management pages, configure the Active Directory server settings, Cisco NAS user account settings, and authentication server settings for the Cisco NAS corresponding to the domain of the users.

Step 4 **Configure the Active Directory server:** Add a Cisco NAS account on the Windows 2000 or 2003 Active Directory server that the Cisco NAS will communicate with, and configure encryption parameters to support the Linux operating system of the Cisco NAS.

Step 5 **Enable Agent-Based Windows SSO with Active Directory (Kerberos).**

Step 6 **Add LDAP Lookup Server for Active Directory SSO:** Optionally, configure LDAP lookup servers to map users to multiple roles after user authentication.

Step 1: Add Active Directory SSO Authentication Server



Authentication Type: Active Directory SSO

Provider Name: WindowsADServer

Default Role: Unauthenticated Role

LDAP Lookup Server: NONE

Description: Windows AD Server for

CANAC v2.1—3-8

The first part of configuring Active Directory SSO is to add the Active Directory SSO auth server. There are six steps to this procedure:

Step 1 Go to **User Management > Auth Servers > New**.

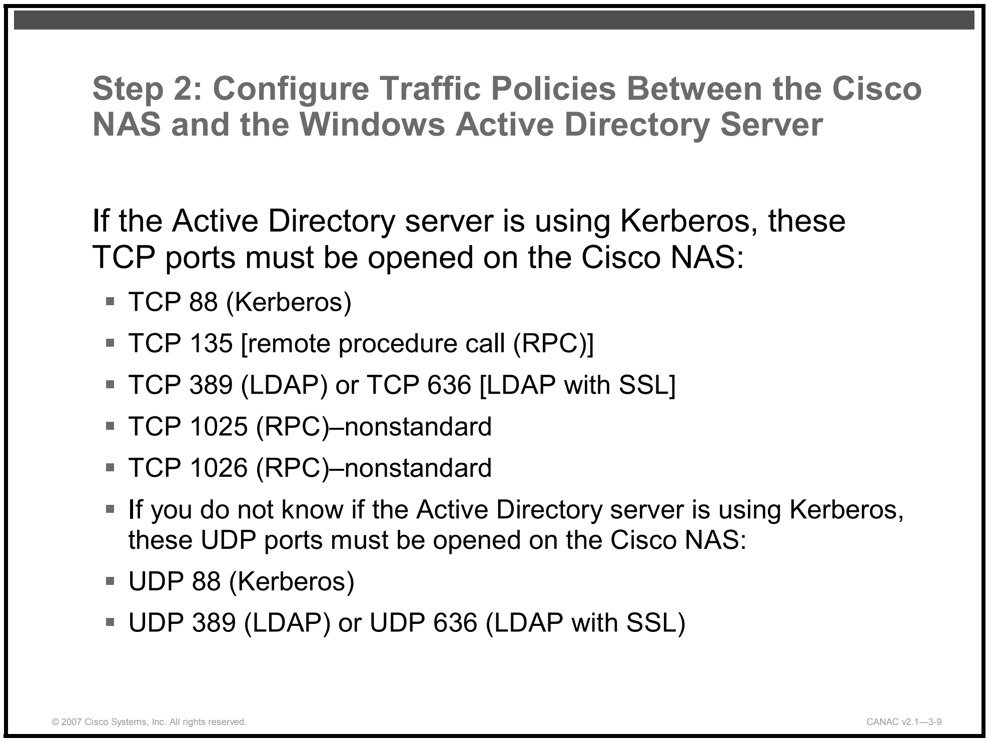
Step 2 From the Authentication Type drop-down menu, choose **Active Directory SSO**.

Step 3 Choose a role from the Default Role drop-down menu. If no additional lookup is required to map users to roles, all users performing authentication via Active Directory SSO will be assigned to the default role. Posture assessment and Cisco NAC Appliance certification should be configured for this role.

Step 4 Type a name in the Provider Name field that will identify the Active Directory SSO auth server on the list of authentication providers. Do not use spaces or special characters in the name.

Step 5 You can leave the LDAP Lookup Server drop-down menu at the default NONE setting if you plan to assign your users to one default role and no additional lookup is required. If you plan to map Windows domain SSO users to multiple roles, the Cisco NAM will need to perform a second-level lookup using the LDAP lookup server that you configure later in this lesson. If you are using multiple roles, select the LDAP lookup server that you have already configured from the LDAP Lookup Server drop-down menu.

Step 6 Click **Add Server**.



Step 2: Configure Traffic Policies Between the Cisco NAS and the Windows Active Directory Server

If the Active Directory server is using Kerberos, these TCP ports must be opened on the Cisco NAS:

- TCP 88 (Kerberos)
- TCP 135 [remote procedure call (RPC)]
- TCP 389 (LDAP) or TCP 636 [LDAP with SSL]
- TCP 1025 (RPC)–nonstandard
- TCP 1026 (RPC)–nonstandard
- If you do not know if the Active Directory server is using Kerberos, these UDP ports must be opened on the Cisco NAS:
- UDP 88 (Kerberos)
- UDP 389 (LDAP) or UDP 636 (LDAP with SSL)

CANAC v2.1—3-9

The second step in configuring SSO for Windows Active Directory is to configure traffic policies for the traffic traveling between the Cisco NAS and the Active Directory server. The Cisco NAS is configured to read the login credentials of user machines as they authenticate to the Active Directory server. Ports must be opened on the Cisco NAS to allow the authentication traffic to pass through the Cisco NAS to and from the Active Directory server. The administrator can open either TCP or User Datagram Protocol (UDP) ports, depending on what the Active Directory server uses. Configure traffic policies for the unauthenticated role to allow these ports on the trusted-side IP address of the Active Directory server.

Note This configuration allows the client to authenticate to the Active Directory and allows for group policy objects and scripts to run. Cisco recommends that you install Cisco Security Agent on the Active Directory and Demilitarized Zone Active Directory.

Before beginning, you must have specific ports open. If the Active Directory server is using Kerberos, these five TCP ports must be open on the Cisco NAS:

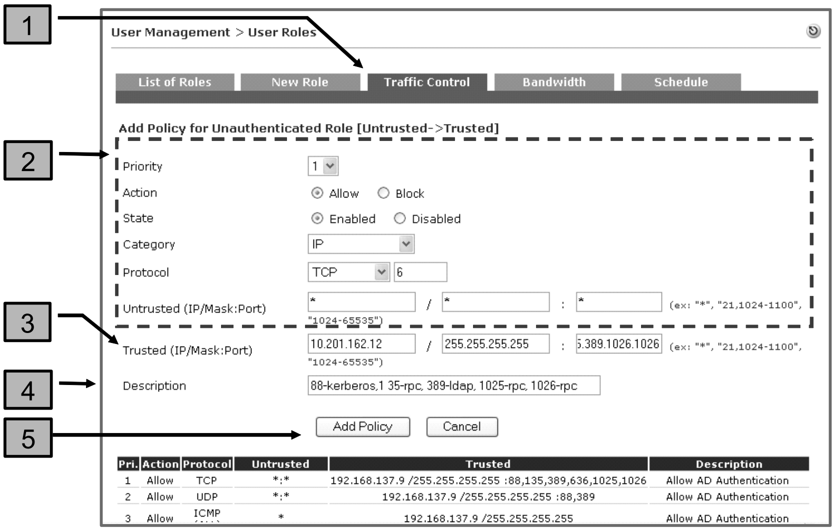
- TCP 88 (Kerberos)
- TCP 135 (remote procedure call [RPC])
- TCP 389 (LDAP) or TCP 636 [LDAP with Secure Sockets Layer (SSL)]
- TCP 1025 (RPC)–nonstandard
- TCP 1026 (RPC)–nonstandard

If you do not know if the Active Directory server is using Kerberos, you must open these two UDP ports instead:

- UDP 88 (Kerberos)
- UDP 389 (LDAP) or UDP 636 (LDAP with SSL)

Note Typically, LDAP uses plain text when sending traffic on TCP or UDP port 389. If encryption is required for LDAP communications, use TCP or UDP port 636 (LDAP with SSL encryption) instead.

Step 2: Configure Traffic Policies Between the Cisco NAS and the Windows Active Directory Server (Cont.)



User Management > User Roles

Add Policy for Unauthenticated Role [Untrusted->Trusted]

Priority	1
Action	● Allow ○ Block
State	● Enabled ○ Disabled
Category	IP
Protocol	TCP 6
Untrusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port)	10.201.162.12 / 255.255.255.255 : 5.389.1026.1026 (ex: "*", "21,1024-1100", "1024-65535")
Description	88-kerberos,1 35-rpc, 389-ldap, 1025-rpc, 1026-rpc

Pri.	Action	Protocol	Untrusted	Trusted	Description
1	Allow	TCP	*:*	192.168.137.9 /255.255.255.255 :88,135,389,636,1025,1026	Allow AD Authentication
2	Allow	UDP	*:*	192.168.137.9 /255.255.255.255 :88,389	Allow AD Authentication
3	Allow	ICMP	*	192.168.137.9 /255.255.255.255	Allow AD Authentication

CANAC v2.1—3-10

Now that you have the open ports that you need, configure the traffic policy by following these steps:

Step 1 Go to **User Management > User Roles > List of Roles > Traffic Control > Unauthenticated Role** to open the IP traffic policy form for the unauthenticated role. Choose **Untrusted ->Trusted** from the Direction drop-down menu and click the **Add Policy** link (not shown). The Add Policy form appears.

Step 2 Leave these fields at their defaults:

— **Priority:** 1

— **Action**: Allow

— **State**: Enabled

— **Category**: IP

— **Protocol**: TCP 6

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

Step 3 Enter information in the Trusted (IP/Mask:Port) fields:

— The first field is for the IP address of the Active Directory server.

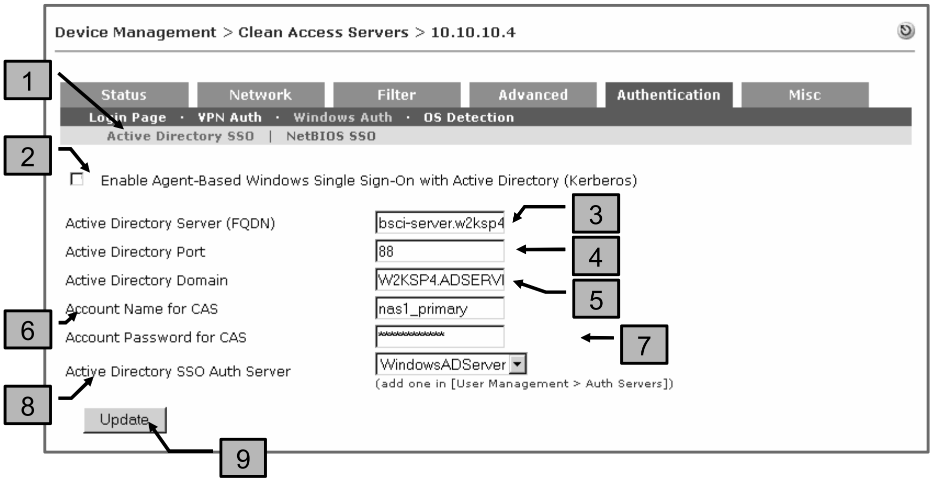
— The second field is for the subnet mask for the Active Directory server. Enter **255.255.255.255**.

— The last field is for ports that you have open for this configuration (use commas to separate port numbers).

Step 4 Type an optional description in the **Description** field.

Step 5 Click **Add Policy**.

Step 3: Configure Active Directory SSO on the Cisco NAS



Device Management > Clean Access Servers > 10.10.10.4

Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
Active Directory SSO | NetBIOS SSO
1
2
3
4
5
6
7
8
9
Update

□ Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Active Directory Server (FQDN)	bsci-server.w2ksp4
Active Directory Port	88
Active Directory Domain	W2KSP4.ADSERVI
Account Name for CAS	nas1_primary
Account Password for CAS	************
Active Directory SSO Auth Server	WindowsADServer (add one in [User Management > Auth Servers])

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-11

Follow these steps to configure the Cisco NAS to correspond to the domain of the users:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO.**

Step 2 Ensure that the check box for Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos) is not checked.

Note The Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos) service should only be enabled after you configure the Active Directory server. Until you perform the configuration on the Active Directory server, the following error message appears:

Error: Could not start the SSO service. Please check the configuration.

Step 3 In the Active Directory Server (FQDN) field, enter the FQDN of the Active Directory server for the domain (case-sensitive, including the domain name). Note that if there are multiple Active Directory servers (domain controllers) for the domain, you only need to choose one Active Directory server. Make sure to type the FQDN of the Active Directory server (not the IP address); for example, `bsci-server.w2ksp4.adserver.com`.

Caution This setting assumes that you have a DNS server correctly configured on the Cisco NAS. The DNS server must be able to resolve the FQDN for the Active Directory server on the Cisco NAS.

Step 4 In the Active Directory Port field, leave the default of 88 for Kerberos.

Step 5 In the Active Directory Domain field, use uppercase letters to enter the name of the domain for the Key Distribution Center on the Active Directory server. The "Active Directory Domain" is equivalent to "Kerberos realm." For example, `W2KSP4.ADSERVER.COM`

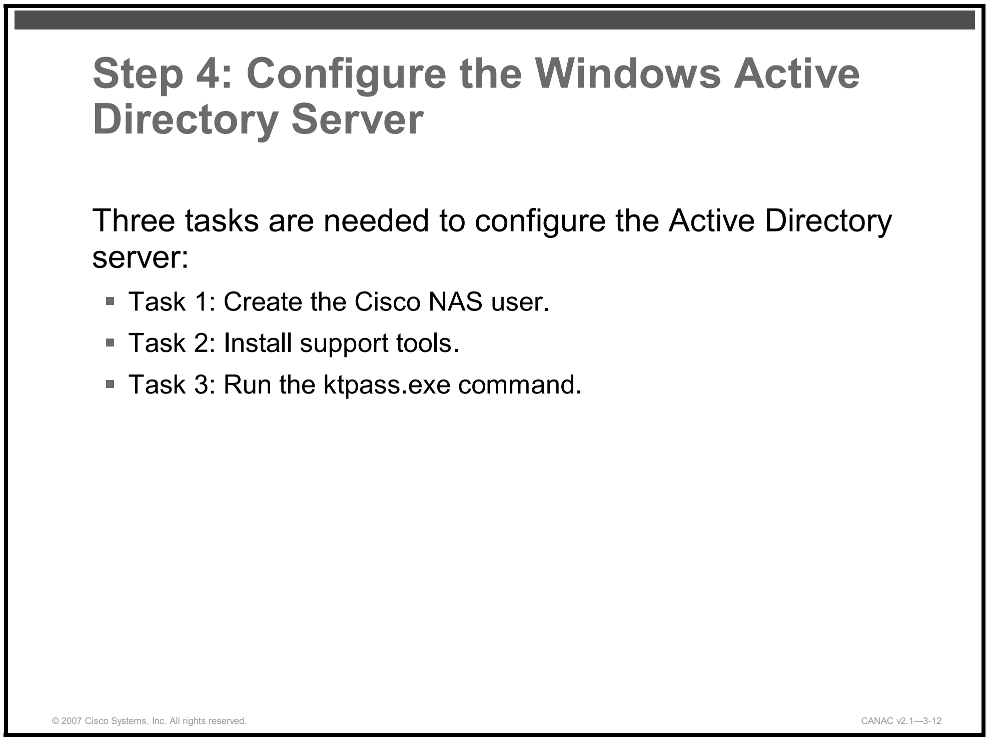
Step 6 In the Account Name for CAS field, enter the name of the Cisco NAS user that you have created on the Active Directory server (for example, nas1_primary). The Cisco NAS user account allows the Cisco NAS to log onto the Active Directory server.

Step 7 Enter a password for the Cisco NAS user on the Active Directory server in the Account Password for CAS field.

Step 8 From the Active Directory SSO Auth Server drop-down menu, choose the Active Directory SSO server that you configured on the Cisco NAM. This field maps the authentication provider that was created on the Cisco NAM to the Cisco NAS (along with the default role and secondary LDAP lookup server if these were also configured).

Step 9 Click **Update**.

Tip If the Active Directory server cannot be reached from the Cisco NAS at the time of Cisco NAS startup, Active Directory SSO service is not started. As a workaround, go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO** and click the **Update** button to restart the Active Directory SSO service.



Step 4: Configure the Windows Active Directory Server

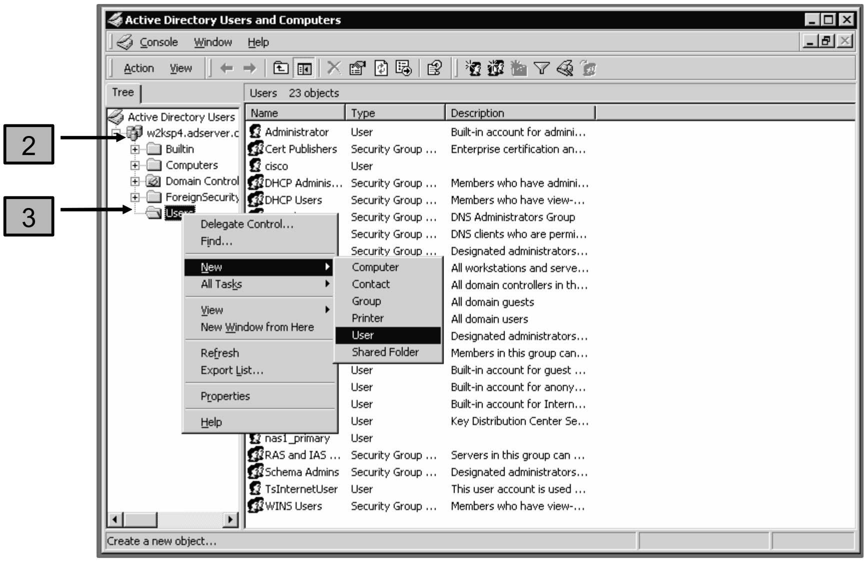
Three tasks are needed to configure the Active Directory server:

- Task 1: Create the Cisco NAS user.
- Task 2: Install support tools.
- Task 3: Run the ktpass.exe command.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-12

The figure shows the three tasks that are involved in configuring the Active Directory server.

Task 1: Create the Cisco NAS User



Users 23 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Enterprise certification an...
cisco	User	
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
	Security Group ...	DNS Administrators Group
	Security Group ...	DNS clients who are permi...
	Security Group ...	Designated administrators...
		All workstations and serve...
		All domain controllers in th...
		All domain guests
		All domain users
		Designated administrators...
		Members in this group can...
	User	Built-in account for guest ...
	User	Built-in account for anony...
	User	Built-in account for Intern...
	User	Key Distribution Center Se...
nas1_primary	User	
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
TsInternetUser	User	This user account is used ...
WINS Users	Security Group ...	Members who have view-...

Create a new object...

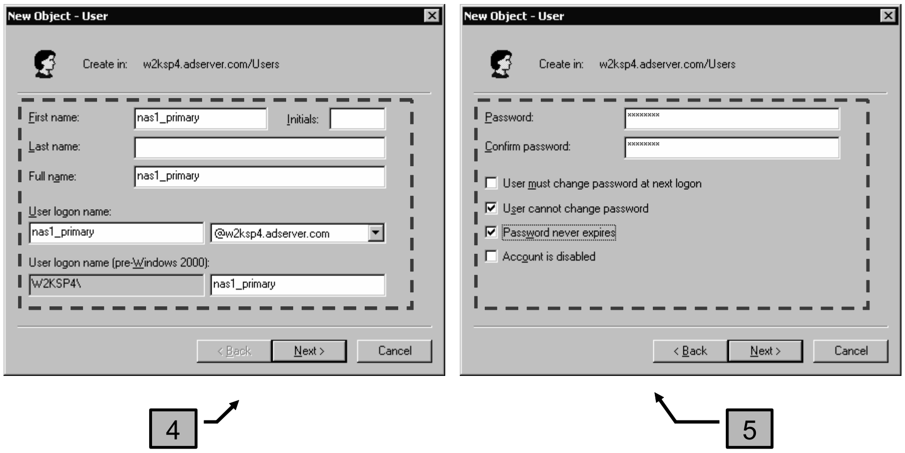
Begin configuring the Active Directory server by creating the Cisco NAS user, as follows:

Step 1 (Not shown) Log in as the administrator on the Active Directory server machine and open the Active Directory Management console from **All Programs > Admin Tools > Active Directory Users and Computers.**

Step 2 From the left pane of the Active Directory Users and Computers window, navigate to the domain that you want to configure the Cisco NAS for (for example, w2ksp4.adserver.com).

Step 3 Right-click the **Users** folder. In the menu that appears, select **New > User.**

Task 1: Create the Cisco NAS User (Cont.)



New Object - User

Create in: w2ksp4.adserver.com/Users

First name: nas1_primary
Initials:
Last name:
Full name: nas1_primary
User logon name: nas1_primary @w2ksp4.adserver.com
User logon name (pre-Windows 2000): W2KSP4\ nas1_primary

New Object - User

Create in: w2ksp4.adserver.com/Users

Password: ********
Confirm password: ********

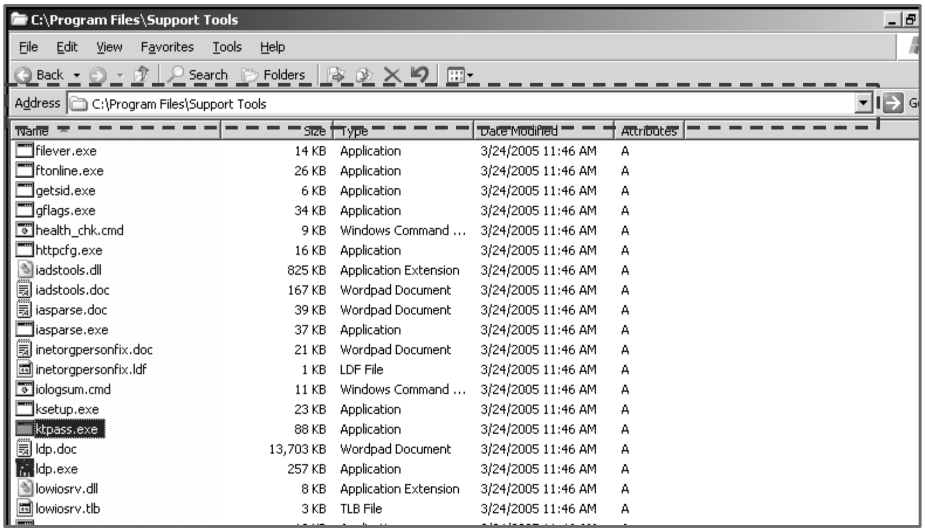
□ User must change password at next logon
☑ User cannot change password
☑ Password never expires
□ Account is disabled

Step 4 In the first New Object – User window, configure the fields for the Cisco NAS user. Type the name that you want the Cisco NAS to use in the First Name field (for example, nas1_primary). This automatically populates the Full Name and User Logon Name fields. The user logon name must be one word. Make sure that the entry in the First Name field is the same as in the Full Name field, and both entries are the same as the name in the User Name field for the user account. Click **Next**.

Step 5 In the second New Object – User window, enter and reenter a password for the Cisco NAS user in the Password and Confirm Password fields. Check the **Password never expires** and the **User cannot change password** check boxes**.** Be sure to leave the User Must Change Password at Next Logon check box unchecked. Click **Next** to bring up the confirmation New Object – User window.

The properties for the Cisco NAS user appear in the confirmation window (not shown). Ensure that all properties are correct and click **Finish** to conclude, or click **Back** if you need to make corrections. The Cisco NAS user is successfully added to the Active Directory domain in the User folder in the Active Directory Users and Computers window.

Task 2: Install Support Tools


C:\Program Files\Support Tools
File Edit View Favorites Tools Help
Back Search Folders

Address C:\Program Files\Support Tools

Name	Size	Type	Date Modified	Attributes
filever.exe	14 KB	Application	3/24/2005 11:46 AM	A
ftonline.exe	26 KB	Application	3/24/2005 11:46 AM	A
getsid.exe	6 KB	Application	3/24/2005 11:46 AM	A
gflags.exe	34 KB	Application	3/24/2005 11:46 AM	A
health_chk.cmd	9 KB	Windows Command ...	3/24/2005 11:46 AM	A
httpcfg.exe	16 KB	Application	3/24/2005 11:46 AM	A
iadstools.dll	825 KB	Application Extension	3/24/2005 11:46 AM	A
iadstools.doc	167 KB	Wordpad Document	3/24/2005 11:46 AM	A
iasparse.doc	39 KB	Wordpad Document	3/24/2005 11:46 AM	A
iasparse.exe	37 KB	Application	3/24/2005 11:46 AM	A
inetorgpersonfix.doc	21 KB	Wordpad Document	3/24/2005 11:46 AM	A
inetorgpersonfix.ldf	1 KB	LDF File	3/24/2005 11:46 AM	A
iologsum.cmd	11 KB	Windows Command ...	3/24/2005 11:46 AM	A
ksetup.exe	23 KB	Application	3/24/2005 11:46 AM	A
ktpass.exe	88 KB	Application	3/24/2005 11:46 AM	A
ldp.doc	13,703 KB	Wordpad Document	3/24/2005 11:46 AM	A
ldp.exe	257 KB	Application	3/24/2005 11:46 AM	A
lowiosrv.dll	8 KB	Application Extension	3/24/2005 11:46 AM	A
lowiosrv.tlb	3 KB	TLB File	3/24/2005 11:46 AM	A

CANAC v2.1—3-15

The figure shows the support tools that are installed on the Active Directory server. Task 2 to configure the Active Directory server involves installing support tools for Windows servers. The **ktpass.exe** command is a Windows server support tool that is not installed by default and must be retrieved from the installation CD. These three steps are used to install the support tools on the Active Directory server:

Step 1 Insert the Windows Server installation CD into the CD drive of the Active Directory server machine.

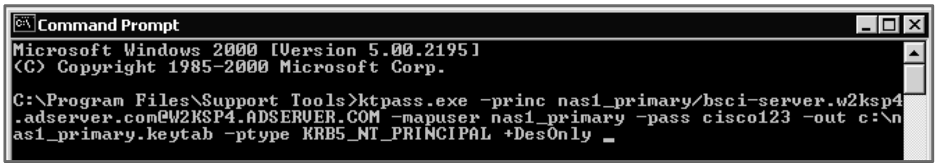
Step 2 Browse to the \SUPPORT\TOOLS folder on the CD.

Note For Windows 2000, the support tools are at (CD)/SUPPORT/TOOLS/Setup.exe. For Windows 2003, the support tools are at (CD)/SUPPORT/TOOLS/Suptools.msi.

Step 3 Double-click and install the executable or MSI file for the support tools. By default, this installs the support tools to C:\Program Files\Support Tools.

Note Do not double-click the **ktpass.exe** command; it must be run from a command tool.

Task 3: Run the ktpass.exe Command



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Program Files\Support Tools>ktpass.exe -princ nas1_primary/bsci-server.w2ksp4
.adserver.com@W2KSP4.ADSERVER.COM -mapuser nas1_primary -pass cisco123 -out c:\n
as1_primary.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly _
```

CANAC v2.1—3-16

In Task 3 of configuring the Active Directory server, you will run the **ktpass.exe** command. Every domain controller configured in the Cisco NAS that a client will need to log onto needs to run the **ktpass.exe** command, even multiple domain controllers used by multiple Cisco NASs under a single domain. The Cisco NAS user account is replicated, but the map user functionality is not. Therefore, the command must be run on all domain controllers that the Cisco NASs log onto.

Linux supports Data Encryption Standard (DES) but does not support the default encryption of Active Directory (RC4) which is specific to Microsoft. Because the Cisco NAS is a Linux machine, the **ktpass.exe** command must be run to ensure that the Cisco NAS user uses DES instead of the default encryption for compatibility when logging onto Active Directory.

Running the **ktpass.exe** command involves these four steps:

Step 1 Open a command prompt and change directories to **C:\Program Files\Support Tools**\. The **ktpass.exe** command should be in the folder.

Step 2 Execute the following command:

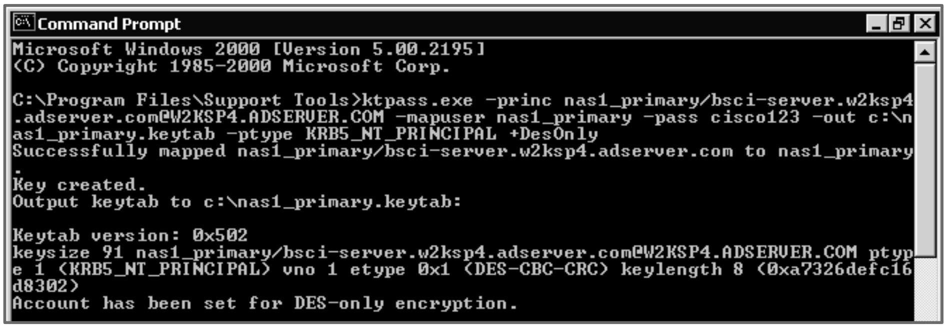
```
ktpass.exe -princ <NAS_username>/<Active Directory Domain
Server>@<Active Directory Domain> -mapuser <NAS_username> -
pass <NAS_password> -out c:\<CAS_username>.keytab -ptype
KRB5_NT_PRINCIPAL +DesOnly
```

For example:

```
ktpass.exe -princ nas1_primary/bsci-
server.w2ksp4.adserver.com@W2KSP4.ADSERVER.COM -mapuser
nas1_primary -pass cisco123 -out c:\nas1_primary.keytab -ptype
KRB5_NT_PRINCIPAL +DesOnly
```

Note When issuing the **ktpass.exe** command, it is crucial that no warnings appear after the command is executed and that executing the command displays the following output: Account has been set for DES-only encryption.

Task 3: Run the ktpass.exe Command (Cont.)



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Program Files\Support Tools>ktpass.exe -princ nas1_primary/bsci-server.w2ksp4
.adserver.com@W2KSP4.ADSERVER.COM -mapuser nas1_primary -pass cisco123 -out c:\n
as1_primary.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
Successfully mapped nas1_primary/bsci-server.w2ksp4.adserver.com to nas1_primary
.
Key created.
Output keytab to c:\nas1_primary.keytab:

Keytab version: 0x502
keysize 91 nas1_primary/bsci-server.w2ksp4.adserver.com@W2KSP4.ADSERVER.COM ptyp
e 1 (KRB5_NT_PRINCIPAL) vno 1 etype 0x1 (DES-CBC-CRC) keylength 8 (0xa7326defc16
d8302)
Account has been set for DES-only encryption.
```

CANAC v2.1—3-17

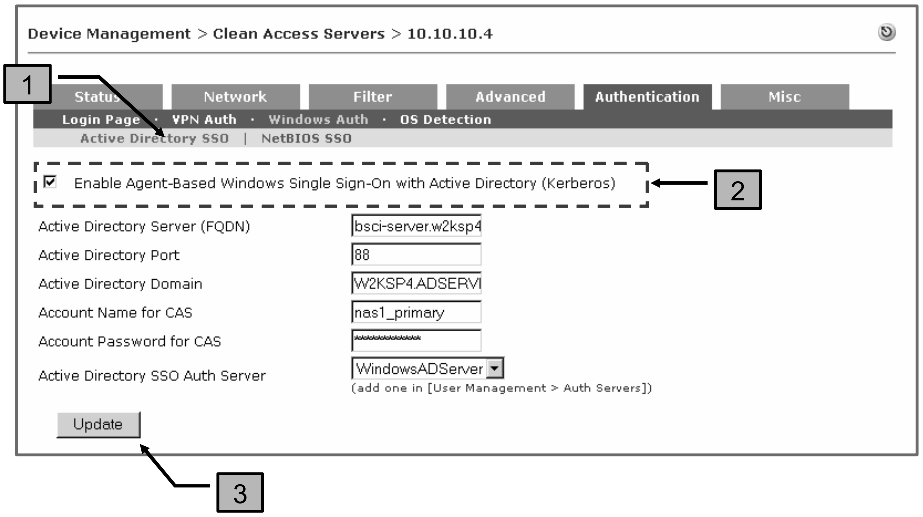
Step 3 The output of the command should look like the screen on the slide:

```
Targeting domain controller: bsci-server.w2ksp4.adserver.com
Successfully mapped nas1_primary/bsci-
server.w2ksp4.adserver.com to nas1_primary.
Key created.
Output keytab to c:\nas1_primary.keytab
Keytab version: 0x502
keysize 97 nas1_primary/bsci-
server.w2ksp4.adserver.com@W2KSP4.ADSERVER.COM  ptype 1
(KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8
(0xbc5120bcfeda01f8)
Account nas1_primary has been set for DES-only encryption.
```

Step 4 Save the exact command you executed and the output to a text file (you do not need to save the Cisco NAS user password). For troubleshooting purposes, this will facilitate Technical Assistance Center support.

Note For details on the parameters used by **Ktpass.exe**, refer to Configure the Active Directory Server in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Step 5: Enable Agent-Based Windows SSO with Active Directory (Kerberos)


Device Management > Clean Access Servers > 10.10.10.4
1
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
Active Directory SSO | NetBIOS SSO
2
Update
3

☑ Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Active Directory Server (FQDN)	bsci-server.w2ksp4
Active Directory Port	88
Active Directory Domain	W2KSP4.ADSERVI
Account Name for CAS	nas1_primary
Account Password for CAS	************
Active Directory SSO Auth Server	WindowsADServer (add one in [User Management > Auth Servers])

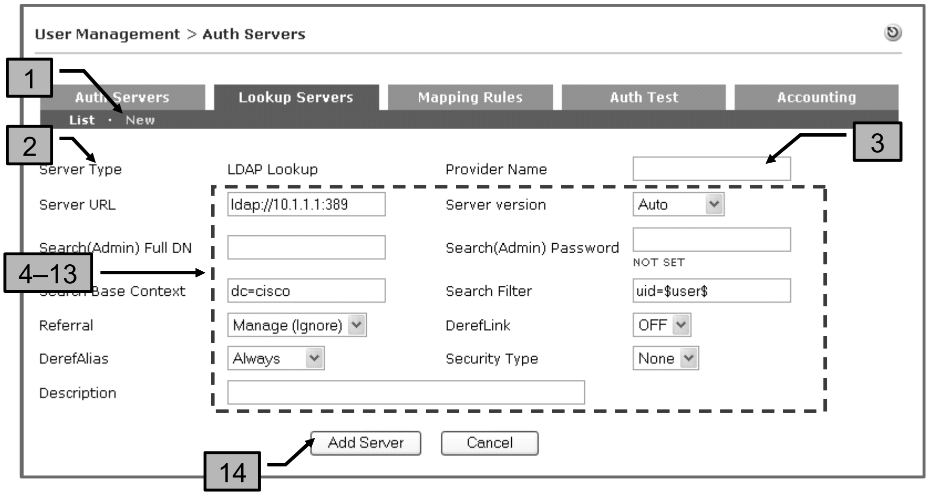
Now that the Active Directory server is configured, you must enable Windows SSO with Active Directory (Kerberos) using these three steps:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO**.

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

Step 3 Click **Update**.

Step 6: Configure the LDAP Lookup Server for Active Directory SSO



User Management > Auth Servers

Server Type	LDAP Lookup	Provider Name	
Server URL	ldap://10.1.1.1:389	Server version	Auto
Search(Admin) Full DN		Search(Admin) Password	NOT SET
Search Base Context	dc=cisco	Search Filter	uid=$user$
Referral	Manage (Ignore)	DerefLink	OFF
DerefAlias	Always	Security Type	None
Description			

© 2007 Cisco Systems, Inc. All rights reserved.　　CANAC v2.1—3-19

If you plan to map Windows domain SSO users to multiple user roles, you will need to configure a secondary LDAP lookup server so that the Cisco NAM can perform the mapping. You must then specify a secondary LDAP lookup server for the Active Directory SSO authentication provider, as previously described in the Add Active Directory SSO authentication server step.

To configure an LDAP lookup server, follow these steps:

Step 1 Go to **User Management > Auth servers > Lookup Servers > New**.

Step 2 Note that the Server Type is set to LDAP Lookup.

Note There is no Default Role drop-down menu on the LDAP lookup server form because the role is already assigned to the Active Directory SSO authentication server. If the LDAP lookup fails, users are mapped to the default role of the Active Directory authentication server.

Step 3 In the Provider Name field, type a unique name with no spaces for this lookup server.

Step 4 In the Server URL field, enter the URL of the LDAP lookup server in the form ldap://<directory_server_IP address>:<port_number>. If no port number is specified, 389 is assumed.

Step 5 The Server Version field lists the LDAP version. Leave the entry as Auto (default) to have the server version automatically detected. LDAP versions 2 and 3 are supported.

Step 6 The Search(Admin) Full DN field is a required field where you enter the full domain name (DN) of the administrator user of the LDAP server. For example, for a domain of ENG.CCA.CISCO.COM, the Search DN is `CN=<username>, CN=Users, DC=ENG, DC=CCA, DC=CISCO, DC=COM`.

Step 7 The Search(Admin) Password is another required field where you enter the password for the administrator user of the LDAP server.

Step 8 In the Search Base Context field, enter the base context (root of the LDAP tree) of searches for users; for example, `CN=Users, DC=ENG, DC=CCA, DC=CISCO, DC=COM`.

Step 9 Enter the attribute that you want to be authenticated in the Search Filter field. This entry is the search attribute that will be matched with any user in the base of the LDAP tree. For example: `CN=$user$`, or `uid=$user$`, or `sAMAccountName=$user$`.

Step 10 The default entry in the Referral field is Manage(Ignore). This entry sets whether referral entries are managed (in which the LDAP server returns referral entries as ordinary entries) or returned as handles (Handle[Follow]).

Step 11 The default setting in the DerefLink field is OFF. If you change this to ON, object aliases that are returned as search results are de-referenced; that is, the actual object that the alias refers to is returned as the search result, not the alias itself.

Note The available settings in the DerefAlias field are Always (default), Never, Finding, Searching.

Step 12 Set the entry in the Security Type field to determine whether or not the connection to the LDAP server uses SSL. The default in this field is None.

Note If the LDAP server uses SSL, be sure to import the certificate to the Cisco NAM from Administration > CCA Manager > SSL Certificate | Import Certificate.

Step 13 (Optional) Enter a description of the LDAP lookup server in the Description field.

Step 14 Click **Add Server**.

Step 15 (Not shown) Once the lookup server is added, make sure to configure the Active Directory SSO authentication server accordingly:

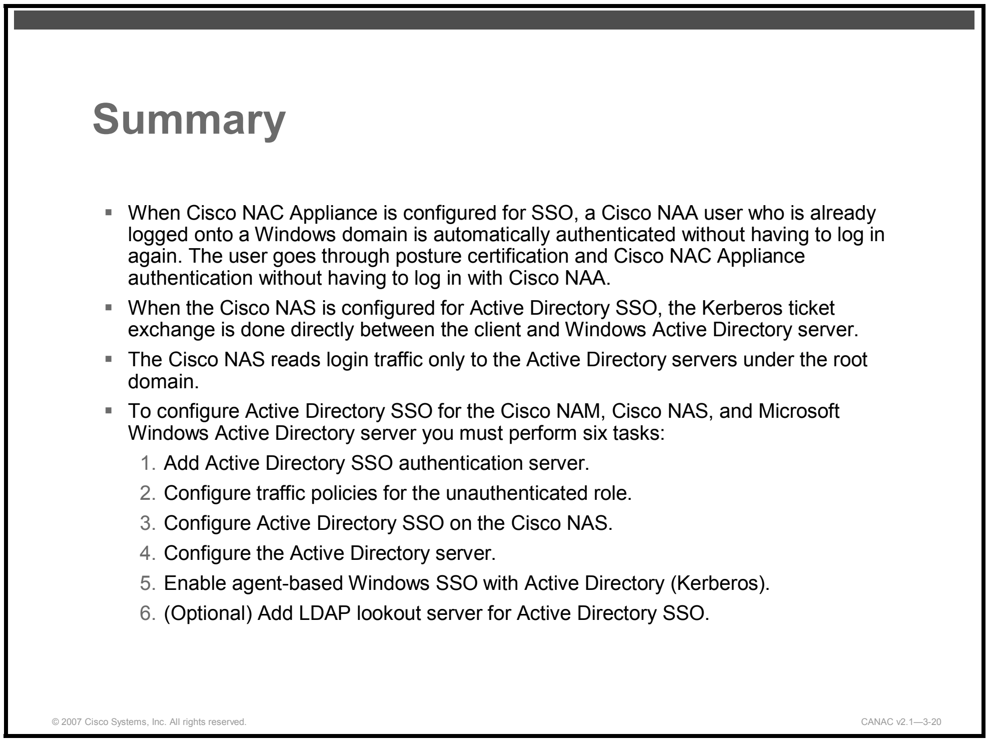
— Go to **User Management > Auth Servers > List**.

— Click the **Edit** button for the Active Directory SSO authentication server that you configured.

— In the Edit form, choose the lookup server from the LDAP Lookup Server drop-down menu.

— Click **Update Server**.

Summary



Summary

- When Cisco NAC Appliance is configured for SSO, a Cisco NAA user who is already logged onto a Windows domain is automatically authenticated without having to log in again. The user goes through posture certification and Cisco NAC Appliance authentication without having to log in with Cisco NAA.
- When the Cisco NAS is configured for Active Directory SSO, the Kerberos ticket exchange is done directly between the client and Windows Active Directory server.
- The Cisco NAS reads login traffic only to the Active Directory servers under the root domain.
- To configure Active Directory SSO for the Cisco NAM, Cisco NAS, and Microsoft Windows Active Directory server you must perform six tasks:
  1. Add Active Directory SSO authentication server.
  2. Configure traffic policies for the unauthenticated role.
  3. Configure Active Directory SSO on the Cisco NAS.
  4. Configure the Active Directory server.
  5. Enable agent-based Windows SSO with Active Directory (Kerberos).
  6. (Optional) Add LDAP lookout server for Active Directory SSO.

CANAC v2.1—3-20

Lesson 3

Implementing the Cisco VPN SSO Feature on the Cisco NAC Appliance

Overview

This lesson describes how to implement the Network Admission Control (NAC) Appliance with Cisco virtual private network (VPN) concentrators. VPN services allow remote workers to access their corporate network over a secure connection. When VPN services are used in combination with Cisco NAC Appliance, network administrators can ensure compliance with corporate software requirements while protecting the corporate network from vulnerabilities.

Cisco VPN Single Sign-On (SSO) allows the user to log in only once via the VPN client before being directed through the Cisco NAC Appliance process. The VPN SSO feature provides users not using a Microsoft Windows Active Directory server access to the SSO feature of the Cisco NAC Appliance solution. To perform SSO, Cisco NAC Appliance takes the RADIUS accounting information from the Cisco VPN SSO device, a Cisco VPN concentrator or Cisco Adaptive Security Appliances (ASAs), for the user authentication and uses it to map the user into a user role. This allows the user to go through the Cisco NAC Appliance process directly without having to also log in to the Cisco NAC Appliance Server (Cisco NAS).

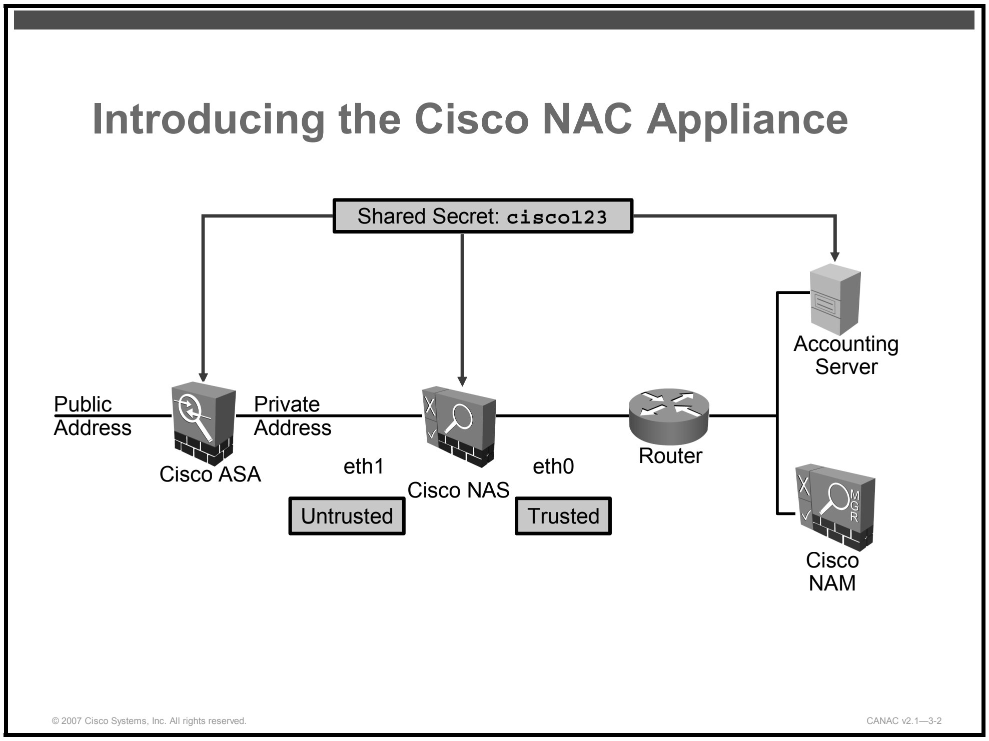
Objectives

Upon completing this lesson, you will be able to use the Cisco NAC Appliance web-based administration console to configure the Cisco NAS to support Cisco VPN SSO devices. This ability includes being able to meet these objectives:

- Describe the Cisco NAC Appliance VPN SSO support for Cisco VPN concentrators and Cisco Adaptive Security Appliances
- Explain how the SSO improves the use of VPN services with the Cisco NAC Appliance solution
- Describe how to configure the Cisco NAC Appliance for Cisco VPN SSO device integration

Introducing Cisco NAC Appliance VPN SSO

This topic describes the Cisco NAC Appliance VPN SSO support for Cisco VPN concentrators and Cisco ASAs.

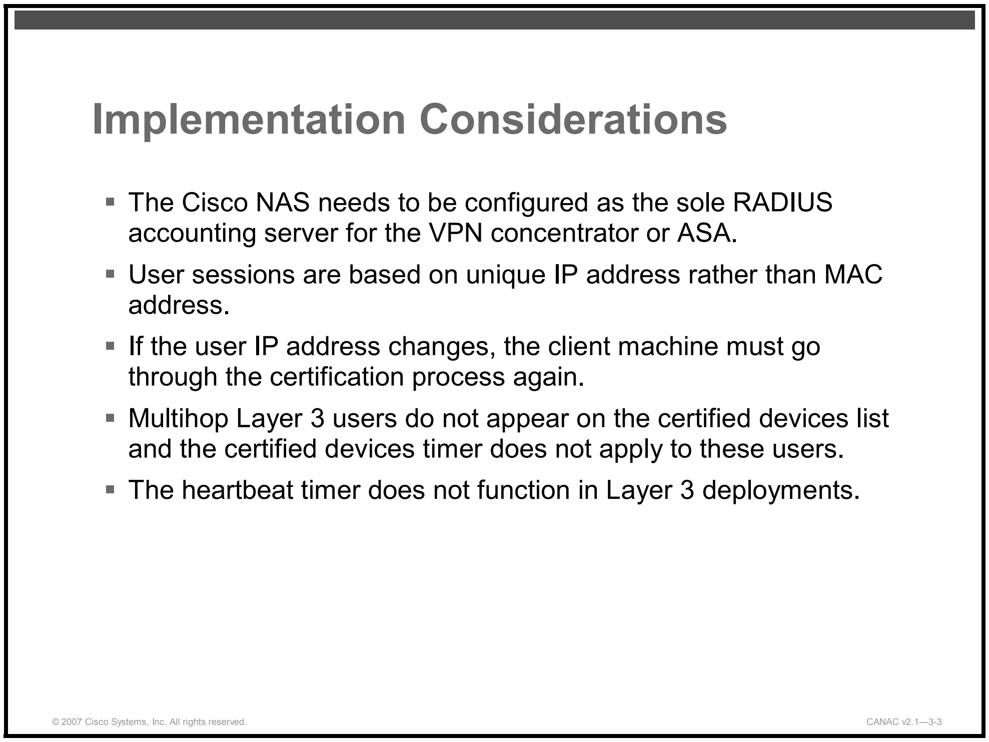


Introducing the Cisco NAC Appliance

CANAC v2.1—3-2

The figure shows a topology of the Cisco NAC Appliance solution supporting the deployment of the Cisco NAC Appliance Server (Cisco NAS) in-band behind a VPN concentrator or ASA. The Cisco NAC Appliance has the capability of multihop Layer 3 in-band deployment by allowing the Cisco NAC Appliance Manager (Cisco NAM) and Cisco NAS to track user sessions by unique IP address. Cisco NAC Appliance can track user sessions when users are separated from the Cisco NAS by one or more routers. The VPN concentrator or ASA, the Cisco NAS, and the accounting server recognize each other using a password called a “shared secret.” The Cisco NAS and the VPN concentrator or ASA must be configured with the same shared secret.

Note You can have a Cisco NAS supporting both Layer 2 and Layer 3 users. With Layer 2-connected users, the Cisco NAM and Cisco NAS manage user sessions based on the user MAC addresses.



Implementation Considerations

- The Cisco NAS needs to be configured as the sole RADIUS accounting server for the VPN concentrator or ASA.
- User sessions are based on unique IP address rather than MAC address.
- If the user IP address changes, the client machine must go through the certification process again.
- Multihop Layer 3 users do not appear on the certified devices list and the certified devices timer does not apply to these users.
- The heartbeat timer does not function in Layer 3 deployments.

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

When you deploy a Cisco NAS in-band behind a VPN concentrator or ASA, where users are one or more Layer 3 hops away from the Cisco NAS, you must consider the following:

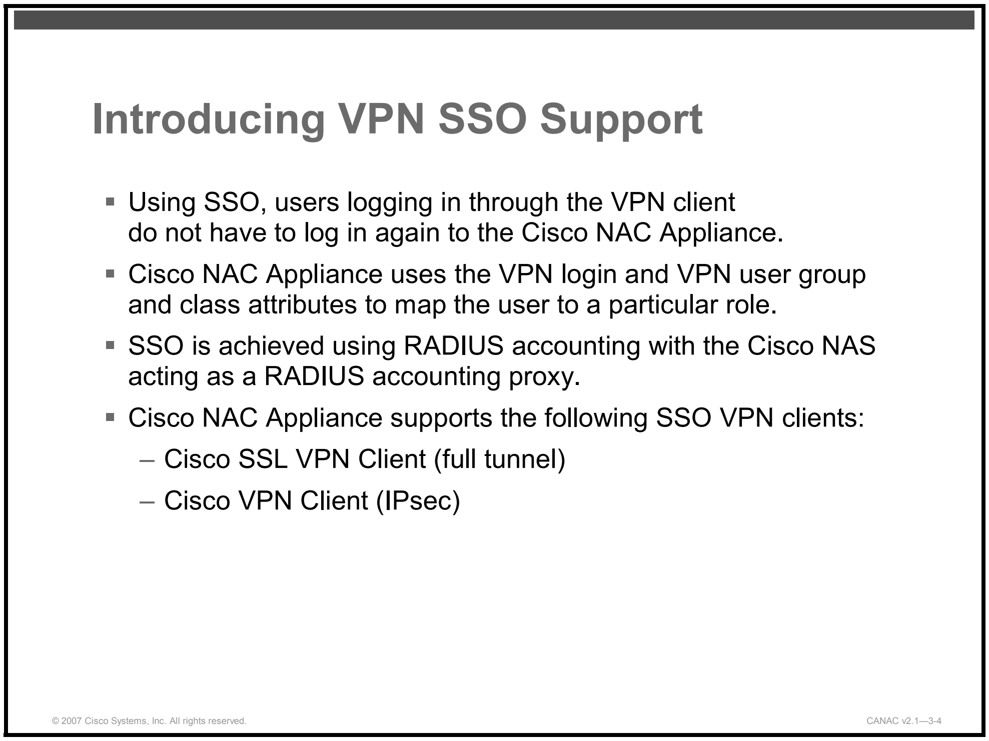
- The Cisco NAS needs to be configured as the sole RADIUS accounting server for the VPN concentrator or ASA. If the VPN concentrator or ASA is already configured for one or more RADIUS accounting servers, the configuration for these servers needs to be transferred from the concentrator or ASA to the Cisco NAS.
- User sessions are based on unique IP address rather than MAC address.
- If the user IP address changes (for example, the user loses VPN connectivity), the client machines must go through the Cisco NAC Appliance certification process again.
- Because the Cisco NAM certified devices list tracks Layer 2 users by MAC address, multihop Layer 3 users do not appear on the certified devices list and the certified devices timer does not apply to these users. The Layer 3 users will only be on the online user list (in-band).

Note If you use the Cisco NAC Appliance Agent (NAA), the MAC address of the client appears on the online users list. If you do not use the Cisco NAA, the MAC address of the VPN concentrator appears on the online users list.

- The heartbeat timer will not function in Layer 3 deployments and does not apply to out-of-band deployments. The heartbeat timer will work if the Cisco NAS is the first hop behind the VPN concentrator because the VPN concentrator responds to Address Resolution Protocol (ARP) queries for the IP addresses of its current tunnel clients.

Introducing VPN SSO Support

This topic describes how the SSO feature improves the use of VPN services with the Cisco NAC Appliance solution.



Introducing VPN SSO Support

- Using SSO, users logging in through the VPN client do not have to log in again to the Cisco NAC Appliance.
- Cisco NAC Appliance uses the VPN login and VPN user group and class attributes to map the user to a particular role.
- SSO is achieved using RADIUS accounting with the Cisco NAS acting as a RADIUS accounting proxy.
- Cisco NAC Appliance supports the following SSO VPN clients:
  - Cisco SSL VPN Client (full tunnel)
  - Cisco VPN Client (IPsec)

CANAC v2.1—3-4

Using SSO and VPN services, users logging in through the VPN client do not have to log in again to the Cisco NAC Appliance. The Cisco NAC Appliance uses the VPN login and VPN user group and class attributes to map the user to a particular role.

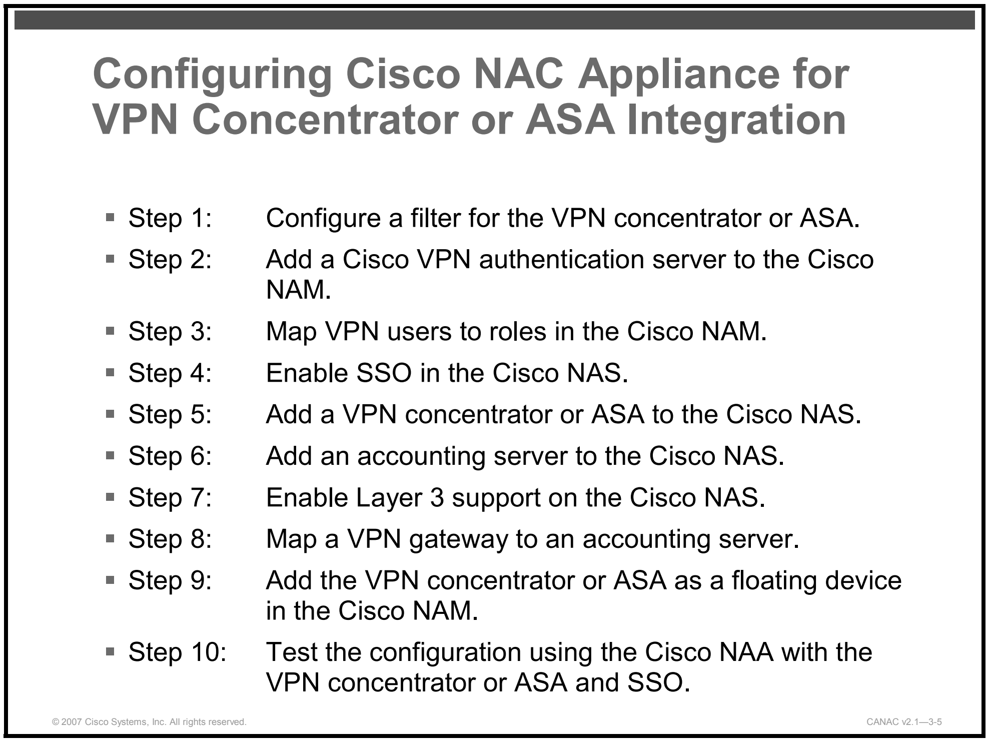
This level of integration is achieved using RADIUS accounting with the Cisco NAS acting as a RADIUS accounting proxy. The Cisco NAC Appliance supports these VPN clients for the purposes of SSO:

- Cisco Secure Sockets Layer (SSL) VPN Client (full tunnel)
- Cisco VPN Client (IPsec)

Note When the SSO feature is configured for a multihop Layer 3 VPN concentrator or ASA integration, if the user session on the Cisco NAS times out but the user is still logged in on the VPN concentrator or ASA, the user session will be restored without the user having to provide a username and password.

Configuring Cisco NAC Appliance for VPN Concentrator or ASA Integration

This topic describes how to configure the Cisco NAC Appliance for Cisco VPN SSO device integration.



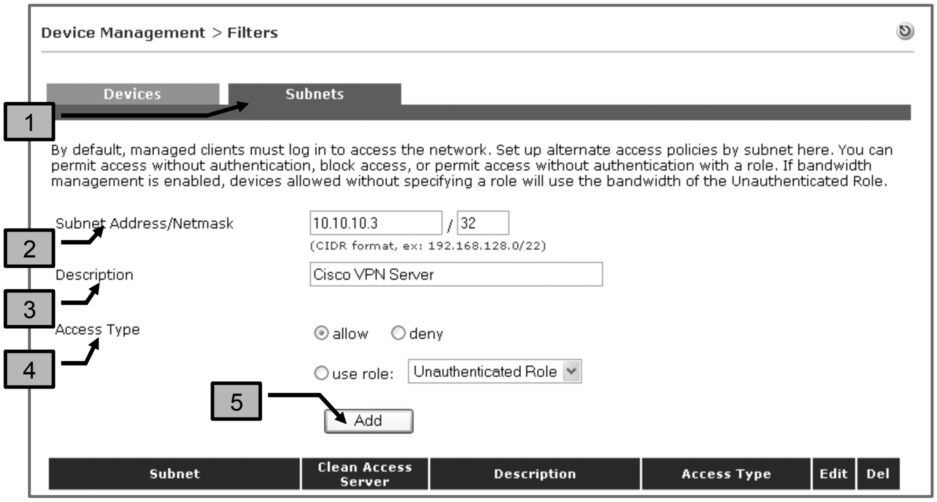
Configuring Cisco NAC Appliance for VPN Concentrator or ASA Integration

- Step 1: Configure a filter for the VPN concentrator or ASA.
- Step 2: Add a Cisco VPN authentication server to the Cisco NAM.
- Step 3: Map VPN users to roles in the Cisco NAM.
- Step 4: Enable SSO in the Cisco NAS.
- Step 5: Add a VPN concentrator or ASA to the Cisco NAS.
- Step 6: Add an accounting server to the Cisco NAS.
- Step 7: Enable Layer 3 support on the Cisco NAS.
- Step 8: Map a VPN gateway to an accounting server.
- Step 9: Add the VPN concentrator or ASA as a floating device in the Cisco NAM.
- Step 10: Test the configuration using the Cisco NAA with the VPN concentrator or ASA and SSO.

CANAC v2.1—3-5

The figure shows the steps used to configure the Cisco NAC Appliance to work with a VPN concentrator.

Configure a Filter for the VPN Concentrator or ASA



Device Management > Filters

By default, managed clients must log in to access the network. Set up alternate access policies by subnet here. You can permit access without authentication, block access, or permit access without authentication with a role. If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role.

Subnet Address/Netmask: 10.10.10.3 / 32
(CIDR format, ex: 192.168.128.0/22)

Description: Cisco VPN Server

Access Type: ● allow ○ deny

○ use role: Unauthenticated Role

Subnet	Clean Access Server	Description	Access Type	Edit	Del

For the Cisco NAC Appliance to allow the VPN concentrator or ASA onto the trusted side of the network, you need to configure a subnet filter. The subnet filter allows the authentication server on the trusted network to communicate with the VPN concentrator or ASA on the untrusted network. To configure a subnet filter for the VPN concentrator or ASA, follow these steps:

Step 1 Using the Cisco NAM administration console, go to **Device Management > Filters > Subnets**.

Step 2 Enter the subnet IP address and netmask for the VPN concentrator or ASA in the Subnet Address/Netmask fields.

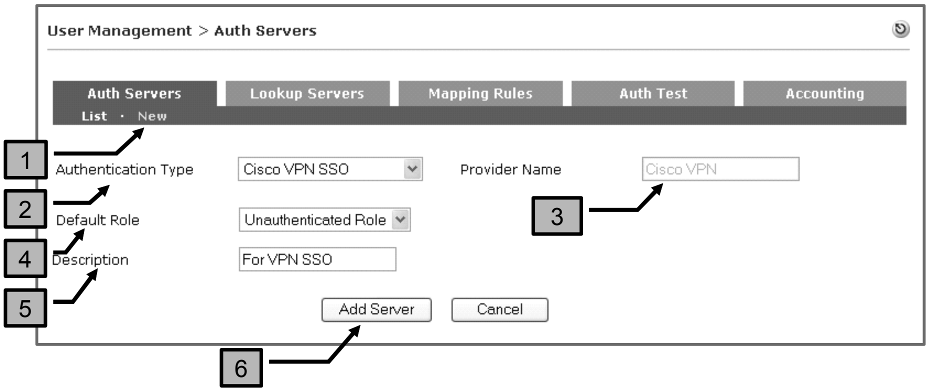
Step 3 Enter a suitable description for the VPN concentrator or ASA in the Description field.

Step 4 Select the Access Type option for your configuration.

Step 5 Click the **Add** button. The new subnet filter appears at the bottom of the list of configured subnet filters under Device Management > Filters > Subnets.

Note Refer to the Global Device and Subnet Filtering section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for further details on how filters are used in the Cisco NAC Appliance.

Add a Cisco VPN Authentication Server to the Cisco NAM



Authentication Type: Cisco VPN SSO

Provider Name: Cisco VPN

Default Role: Unauthenticated Role

Description: For VPN SSO

The second step of configuring Cisco NAC Appliance to support VPN concentrator or ASA integration using SSO is to add a VPN authentication server to the Cisco NAM. To add a VPN authentication server to the Cisco NAM, follow these steps:

Step 1 Using the Cisco NAM administration console, go to **User Management > Auth Servers > New**.

Step 2 Select **Cisco VPN SSO** server from the Authentication Type drop-down menu.

Step 3 Enter a provider name in the Provider Name field.

Note "Cisco VPN" is entered in the Provider Name field by default.

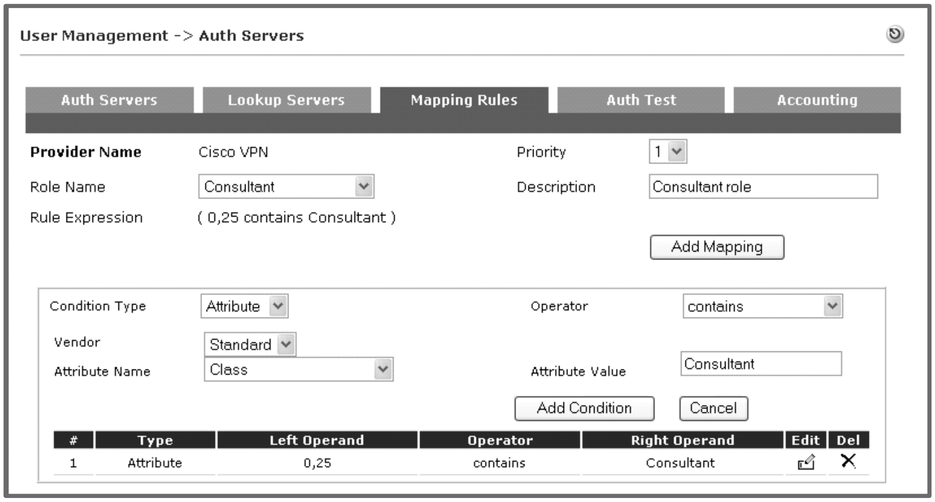
Step 4 Select a user role from the Default Role drop-down menu.

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. Typically, the default role will be the unauthenticated role.

Step 5 Enter a suitable description in the Description field.

Step 6 Click the **Add Server** button. The new server appears in the User Management > Auth Servers > List of Servers form.

Map VPN Users to Roles in the Cisco NAM



User Management -> Auth Servers

Provider Name	Cisco VPN	Priority	1
Role Name	Consultant	Description	Consultant role
Rule Expression	(0,25 contains Consultant)		

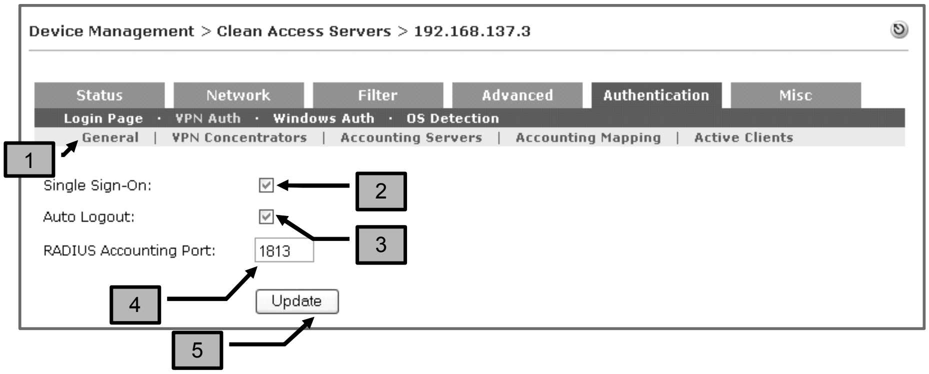
Condition Type	Attribute	Operator	contains
Vendor	Standard		
Attribute Name	Class	Attribute Value	Consultant

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,25	contains	Consultant	✎	✕

At this stage in the implementation of a VPN concentrator or ASA with Cisco NAC Appliance, you need to map VPN users to user roles in the Cisco NAM. Because RADIUS accounting packets pass user attributes, the Cisco NAM and the Cisco NAS can use the RADIUS information that is passed from the VPN server type to map VPN concentrator or ASA users to roles. In the Cisco NAM web-based administration console, use the User Management > Auth Servers > Mapping Rules form. Use this form to map users to Cisco NAC Appliance roles based on attributes passed from the external authentication server. These actions will help ensure that you correctly map the VPN users to Cisco NAC Appliance user roles:

- Make sure that the correct VPN server appears in the Provider Name field.
- Make sure you enter “contains” in the Operator drop-down menu. Though undocumented, the “contains” operator provides the most consistent way to ensure that the Cisco NAS finds the attribute value.
- Make sure that the attribute value entered in the Attribute Value field has the same capitalization as the role name you created in the Users Role form.
- Make sure that the Cisco ASA or VPN concentrator has been configured with RADIUS group attributes that have the same capitalization as you configured in the Users Role form.

Enable VPN SSO in the Cisco NAS


Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
1
2
3
4
5
Update

Device Management > Clean Access Servers > 192.168.137.3

Single Sign-On: ☑

Auto Logout: ☑

RADIUS Accounting Port: 1813

CANAC v2.1—3-9

To enable VPN SSO in the Cisco NAS, follow these steps:

Step 1 Using the Cisco NAM administration console, go to **Device Management > Clean Access Servers >** [**IPaddress**] **> Authentication > VPN Auth > General**.

Step 2 Check the **Single Sign-On** check box to set the Cisco NAS to process the user login via RADIUS accounting packets.

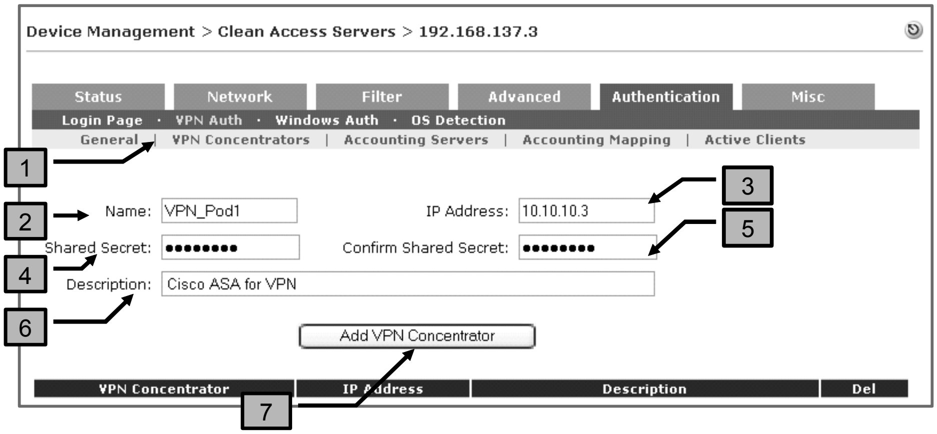
Step 3 Check the **Auto Logout** check box to set the user to be removed from the content-addressable memory (CAM) online users list when the RADIUS stop record is received. The RADIUS stop record is sent when a user disconnects from the VPN concentrator.

Step 4 Enter a port number in the RADIUS Accounting Port field. Typically, UDP Port 1813 or UDP Port 1646 is used.

Step 5 Click the **Update** button.

Note SSO is enabled on the Cisco NAM by adding the Cisco VPN server type as an authentication source.

Add a VPN Concentrator or ASA to the Cisco NAS


Device Management > Clean Access Servers > 192.168.137.3
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
1
2
3
4
5
6
7
Add VPN Concentrator
VPN Concentrator
IP Address
Description
Del

Name: VPN_Pod1

IP Address: 10.10.10.3

Shared Secret: ●●●●●●●●

Confirm Shared Secret: ●●●●●●●●

Description: Cisco ASA for VPN

CANAC v2.1—3-10

To add a VPN Concentrator or ASA to the Cisco NAS, follow these steps:

Step 1 Using the Cisco NAM administration console, go to **Device Management** > **Clean Access Servers** > [**IP address**] > **Authentication** > **VPN Auth** > **VPN Concentrators**.

Step 2 Enter a name for the concentrator in the Name field.

Step 3 Enter the private IP address of the VPN concentrator or ASA in the IP Address field.

Step 4 Enter a shared secret password in the Shared Secret field.

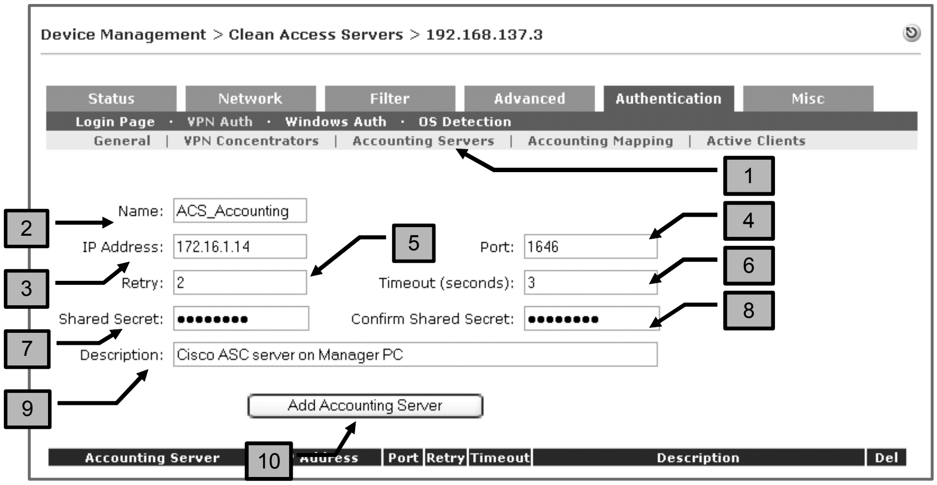
Note This shared secret password will be used by the Cisco NAS and the VPN concentrator or ASA. The shared secret password must be separately configured on the VPN concentrator or ASA using the same password that you use here.

Step 5 Reenter the password in the Confirm Shared Secret field.

Step 6 Enter an optional description in the Description field.

Step 7 Click the **Add VPN Concentrator** button.

Add an Accounting Server to the Cisco NAS



Device Management > Clean Access Servers > 192.168.137.3
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
1
2
3
4
5
6
7
8
9
10
Add Accounting Server
Accounting Server
Address
Port
Retry
Timeout
Description
Del

Name: ACS_Accounting

IP Address: 172.16.1.14

Port: 1646

Retry: 2

Timeout (seconds): 3

Shared Secret: ●●●●●●●●

Confirm Shared Secret: ●●●●●●●●

Description: Cisco ASC server on Manager PC

When the VPN concentrator is configured to work with an accounting server, the information for the accounting servers, the associations between users and RADIUS attributes, needs to also be transferred to the Cisco NAS using the Cisco NAM. If this transfer does not occur, the Cisco NAS maintains the associations between users and RADIUS attributes. To add an accounting server to the Cisco NAS, follow these steps:

Step 1 Using the Cisco NAM administration console, go to **Device Management > Clean Access Servers >** [**IP address**] **>Authentication > VPN Auth > Accounting Servers**.

Step 2 Enter an appropriate name for the accounting server in the Name field.

Step 3 Enter the IP address of the accounting server in the IP Address field.

Step 4 Enter the port number for the accounting server in the Port field.

Step 5 Enter the number of times to retry a request attempt in the Retry field.

Step 6 Enter the number of seconds the Cisco NAS should wait before retrying a request in the Timeout (seconds) field.

Note If the value in the Retry field is 2, and the value in the Timeout field is 3 (seconds), it will take 6 seconds for the Cisco NAS to send the request to the next accounting server on the list.

Step 7 Enter the shared secret password in the Shared Secret field.

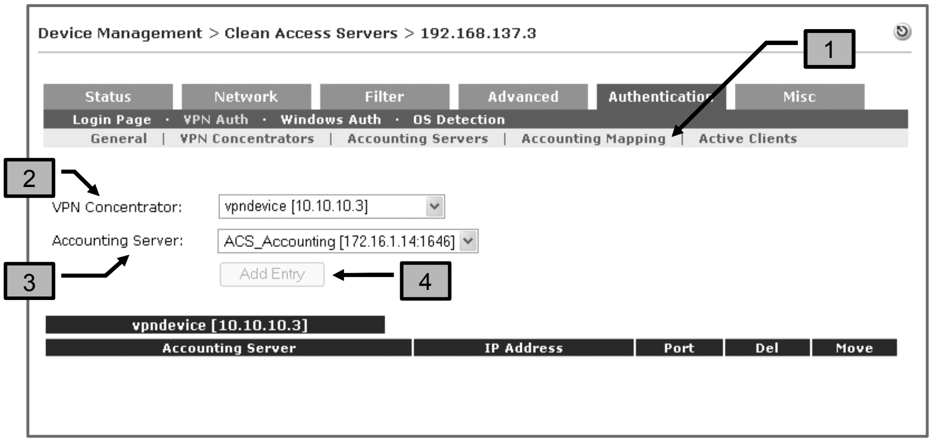
Note This shared secret password is the password that is passed between the Cisco NAS and the accounting server. The same password must be configured on the accounting server.

Step 8 Reenter the shared secret password in the Confirm Shared Secret field.

Step 9 Enter an appropriate description of the accounting server in the Description field.

Step 10 Click the **Add Accounting Server** button. The new accounting server appears at the bottom of the accounting server list.

Map a VPN Gateway to an Accounting Server



Device Management > Clean Access Servers > 192.168.137.3

Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Add Entry
1
2
3
4

VPN Concentrator: vpndevice [10.10.10.3]

Accounting Server: ACS_Accounting [172.16.1.14:1646]

vpndevice [10.10.10.3]

Accounting Server	IP Address	Port	Del	Move

If you are managing multiple VPN concentrators and multiple accounting servers, you can create mappings to associate the VPN concentrators with sets of accounting servers. Associating VPN concentrators with sets of accounting servers allows the Cisco NAS to go to the next server on the list when an accounting server becomes unreachable. To map a VPN gateway to an accounting server, follow these steps:

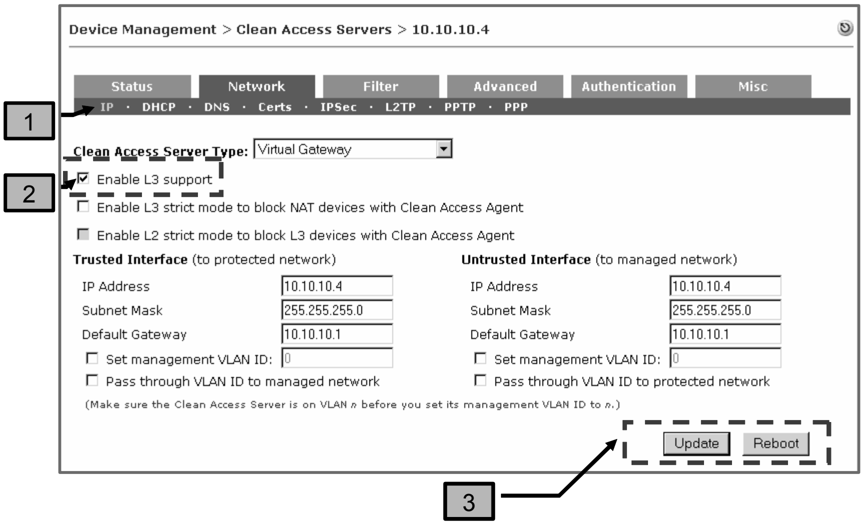
Step 1 Using the Cisco NAM administration console, go to **Device Management > Clean Access Servers >** [**IP address**] **> Authentication > VPN Auth > Accounting Mapping**.

Step 2 Choose the appropriate VPN concentrator from the VPN Concentrator drop-down menu. The VPN Concentrator drop-down menu displays all the VPN concentrators added to the Cisco NAS.

Step 3 Choose the appropriate accounting server from the Accounting Server drop-down menu. The Accounting Server drop-down menu displays all the accounting servers that have been configured for the Cisco NAS.

Step 4 Click the **Add Entry** button to add the mapping from the VPN gateway to the accounting server. The new mapping appears at the bottom of the Accounting Mapping list.

Enable Layer 3 Support on the Cisco NAS



Device Management > Clean Access Servers > 10.10.10.4

Clean Access Server Type: Virtual Gateway

☑ Enable L3 support

☐ Enable L3 strict mode to block NAT devices with Clean Access Agent

☐ Enable L2 strict mode to block L3 devices with Clean Access Agent

Trusted Interface (to protected network)		**Untrusted Interface** (to managed network)	
IP Address	10.10.10.4	IP Address	10.10.10.4
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.10.10.1	Default Gateway	10.10.10.1
☐ Set management VLAN ID:	0	☐ Set management VLAN ID:	0
☐ Pass through VLAN ID to managed network		☐ Pass through VLAN ID to protected network	

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

CANAC v2.1—3-13

The Enable L3 support option must be checked on the Cisco NAS for the Cisco NAA to work in VPN tunnel mode. Layer 3 and Layer 2 strict options are mutually exclusive. Enabling one option disables the other option. Enable Layer 3 support on the Cisco NAS as follows:

Note The Clean Access Server Type, Trusted Interface, and Untrusted Interface settings should already be correctly configured from when the Cisco NAS was added.

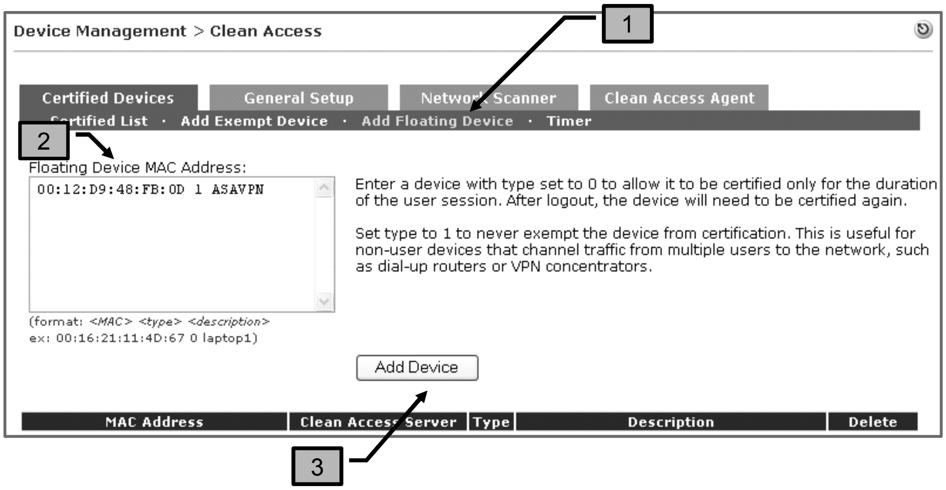
Step 1 Go to **Device Management > Clean Access Servers > [IP Address] > Network > IP**.

Step 2 Click the check box for **Enable L3 support**.

Step 3 Click the **Update** button and then click the **Reboot** button.

Note The enable and disable Layer 3 feature is disabled by default. Any change in this setting *always* requires an update and reboot of the Cisco NAS to take effect. Clicking **Update** here causes the web console to retain the changed setting until the next reboot. Clicking **Reboot** here causes the process to start in the Cisco NAS.

Add a VPN Concentrator or ASA as a Floating Device in the Cisco NAM



Floating Device MAC Address:

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

(format: *<MAC> <type> <description>*
ex: 00:16:21:11:4D:67 0 laptop1)

Enter a device with type set to 0 to allow it to be certified only for the duration of the user session. After logout, the device will need to be certified again.

Set type to 1 to never exempt the device from certification. This is useful for non-user devices that channel traffic from multiple users to the network, such as dial-up routers or VPN concentrators.

In general, if the Cisco NAS is not on the same subnet as client machines, the Cisco NAS will not obtain client MAC information for IP addresses when clients log onto the system. If there is a VPN concentrator or ASA between users and the Cisco NAS (all server types), the Cisco NAS will see the MAC address of the VPN device with each new client IP address. This information is visible because the VPN device performs proxy ARP for the client IP addresses. Unless the VPN device is configured as a floating device, only the first user logging onto Cisco NAC Appliance must meet Cisco NAC Appliance requirements. You must add the MAC address of the VPN device to the Floating Device list using the administration console. Refer to the Add Floating Devices section in the *Cisco NAC Appliance* (*Clean Access) - Manager Installation and Administration Guide* for details on adding floating devices.

To add a VPN concentrator as a floating device in the Cisco NAM, follow these steps:

Step 1 Using the Cisco NAM administration console, go to **Device Management > Clean Access > Certified Devices > Add Floating Device**.

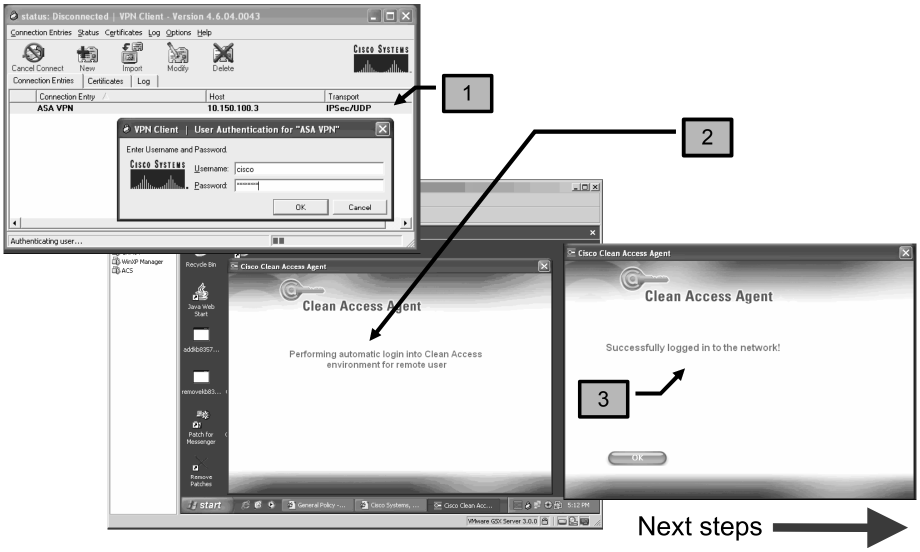
Step 2 Enter the MAC address, the type of device, and an appropriate description in the Floating Device MAC Address field. Include spaces between each element and use line breaks to separate multiple entries; for example:

```
00:90:A4:08:0A:B8 1 ASA5520
```

Note Typically, set the device type to 1. If the device type is set to 1, the VPN concentrator is never considered certified. Type 0 is used for session-scope device certification.

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

Test the Configuration Using the Cisco NAA with the VPN Concentrator or ASA and SSO



status: Disconnected | VPN Client - Version 4.6.04.0043

Connection Entry	Host	Transport
ASA VPN	10.150.100.3	IPSec/UDP

VPN Client | User Authentication for "ASA VPN"

Enter Username and Password.

Username: cisco

Password: ********

Authenticating user…

Cisco Clean Access Agent

Performing automatic login into Clean Access environment for remote user

Cisco Clean Access Agent

Successfully logged in to the network!

Next steps →

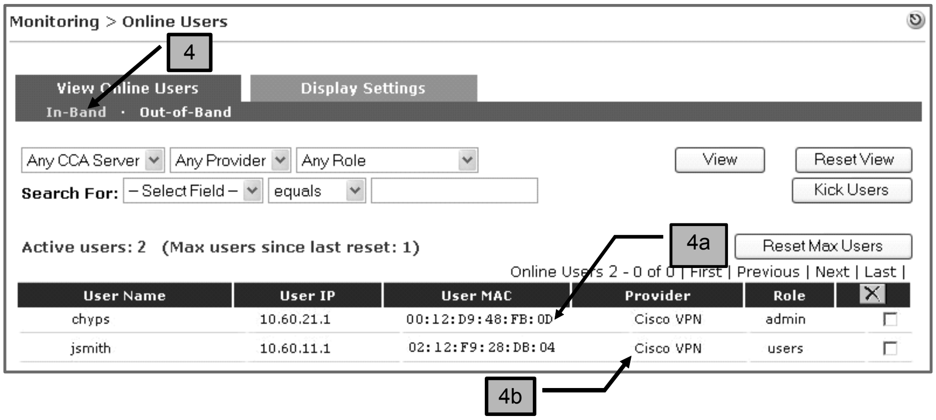
The figure shows three screen captures associated with testing the configuration using the Cisco NAA with the VPN concentrator and SSO. To test the configuration, follow these steps:

Step 1 Log in to the VPN client on a client machine.

Step 2 Observe the Cisco NAA automatic login screen.

Step 3 Observe the Cisco NAA successful login screen.

Test the Configuration Using the Cisco NAA with the VPN Concentrator or ASA and SSO (Cont.)



Monitoring > Online Users

Any CCA Server | Any Provider | Any Role

Search For: – Select Field – | equals

Active users: 2 (Max users since last reset: 1)

Online Users 2 - 0 of 0 | First | Previous | Next | Last |

User Name	User IP	User MAC	Provider	Role	☒
chyps	10.60.21.1	00:12:D9:48:FB:0D	Cisco VPN	admin	□
jsmith	10.60.11.1	02:12:F9:28:DB:04	Cisco VPN	users	□

Next steps →

CANAC v2.1—3-16

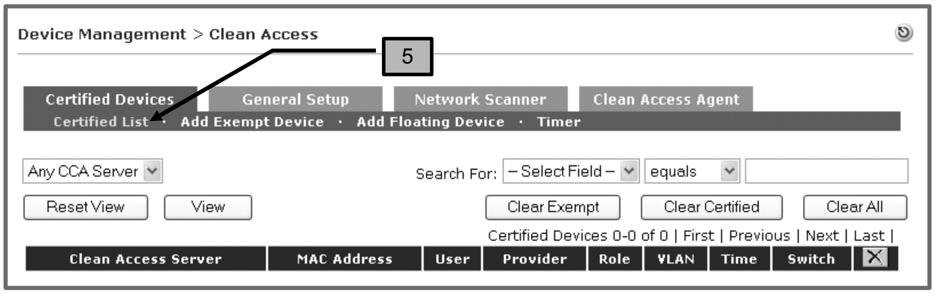
Step 4 Use the Cisco NAM administration console and go to **Monitoring > Online Users > View Online Users > In-Band** to verify online user status. Check the following:

— **Step 4a:** The MAC address in the User MAC column contains zeros.

— **Step 4b:** The provider is the correct VPN provider (Cisco VPN) showing that the user was automatically logged in via RADIUS accounting records.

Note If you use the Cisco NAA to log in, the MAC address of the client appears on the online users list. If you do not use the Cisco NAA to log in, the MAC address of the VPN concentrator appears on the online users list.

Test the Configuration Using the Cisco NAA with the VPN Concentrator or ASA and SSO (Cont.)



Device Management > Clean Access

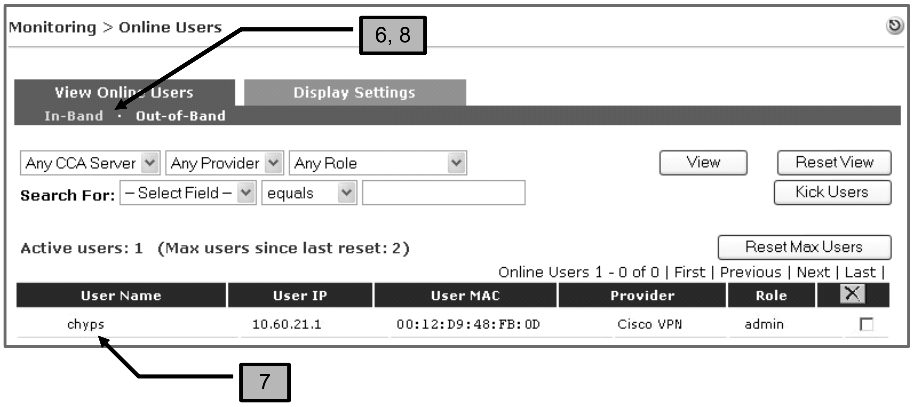
Certified Devices 0-0 of 0 | First | Previous | Next | Last |

Next steps →

Step 5 Use the Cisco NAM administration console and go to **Device Management > Clean Access > Certified Devices > Certified List**. Observe the following:

- The Certified Devices list does not contain addresses for Cisco NAC Appliance remote VPN and Layer 3 users.
- The Certified Devices list includes users that are authenticated and certified based on known Layer 2 MAC addresses.

Test the Configuration Using the Cisco NAA with the VPN Concentrator or ASA and SSO (Cont.)



Active users: 1 (Max users since last reset: 2)

User Name	User IP	User MAC	Provider	Role	☒
chyps	10.60.21.1	00:12:D9:48:FB:0D	Cisco VPN	admin	□

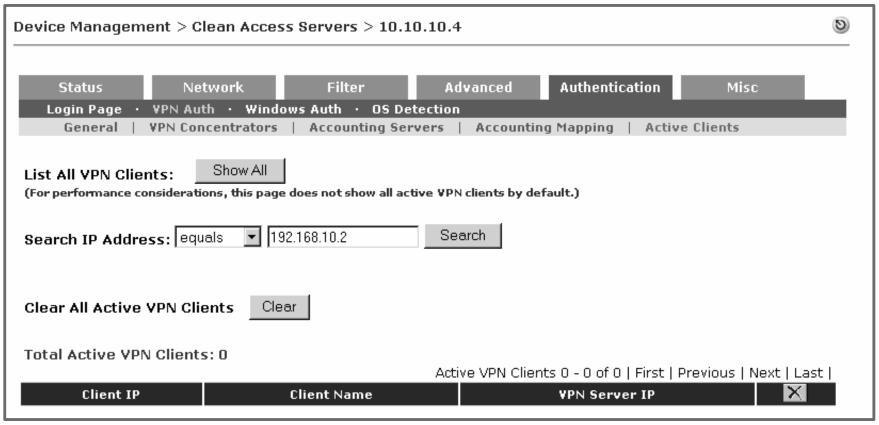
Step 6 Using the Cisco NAM administration console, go to **Monitoring** > **Online Users** > **View Online Users** > **In-Band**. Observe the current online users. Keep the Cisco NAM administration console open.

Step 7 Log out the user from the network and the VPN concentrator on the client machine.

Step 8 Using the Cisco NAM administration console, go to **Monitoring** > **Online Users** > **View Online Users** > **In-Band** and confirm that the user has been logged out.

Note In the example, the user jsmith, who was listed in Step 4, is no longer logged in.

Test the Configuration Using the Cisco NAA with the VPN Concentrator or ASA and SSO (Cont.)


Device Management > Clean Access Servers > 10.10.10.4
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Show All
Search
Clear
Active VPN Clients 0 - 0 of 0 | First | Previous | Next | Last |

List All VPN Clients:
(For performance considerations, this page does not show all active VPN clients by default.)

Search IP Address: equals 192.168.10.2

Clear All Active VPN Clients

Total Active VPN Clients: 0

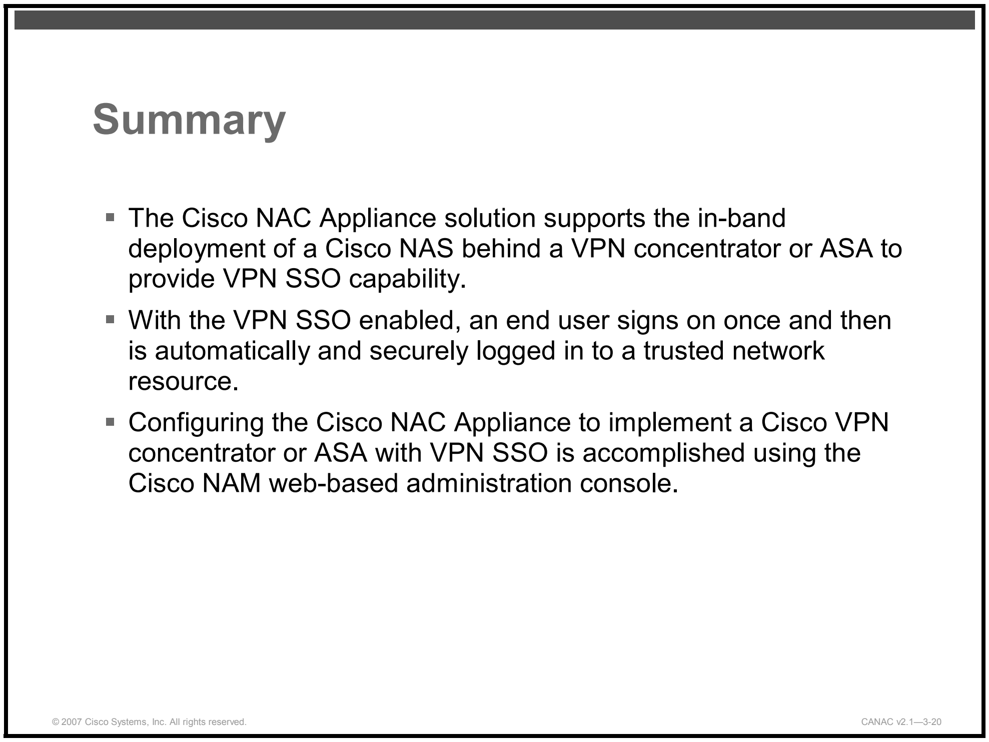
Client IP	Client Name	VPN Server IP	☒

CANAC v2.1—3-19

An Active VPN Clients page is available in the Cisco NAS management pages and Cisco NAS direct access console, which lists IP addresses known to the Cisco NAS through VPN SSO. This page is intended to facilitate troubleshooting for VPN SSO.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- The Cisco NAC Appliance solution supports the in-band deployment of a Cisco NAS behind a VPN concentrator or ASA to provide VPN SSO capability.
- With the VPN SSO enabled, an end user signs on once and then is automatically and securely logged in to a trusted network resource.
- Configuring the Cisco NAC Appliance to implement a Cisco VPN concentrator or ASA with VPN SSO is accomplished using the Cisco NAM web-based administration console.

CANAC v2.1—3-20

Lesson 4

Implementing Cisco NAC Appliance Out-of-Band Deployment

Overview

Out-of-band deployment is one of two implementation options for Cisco Network Admission Control (NAC) Appliance. The out-of-band deployment option offers clients all the benefits of the Cisco NAC Appliance network security with increased network performance. This lesson describes the procedure for implementing the Cisco NAC Appliance out-of-band deployment for VLAN-based quarantine.

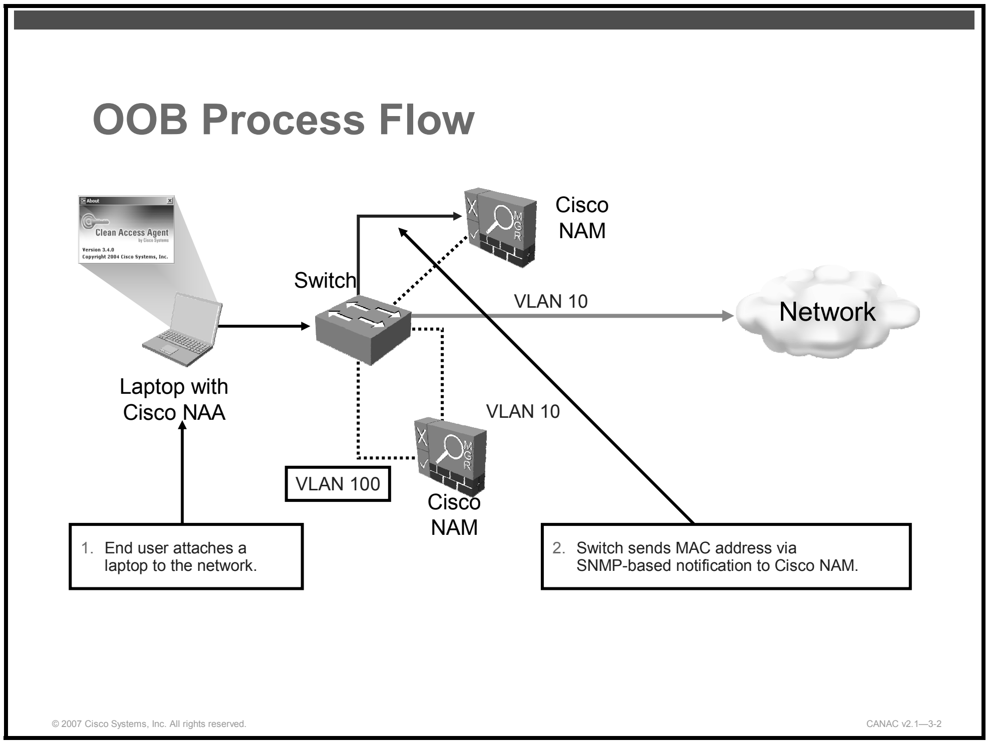
Objectives

Upon completing this lesson, you will be able to deploy Cisco NAC Appliance out-of-band solution for VLAN-based quarantine. This ability includes being able to meet these objectives:

- Describe the Cisco NAC Appliance out-of-band process flow
- Describe the considerations for implementing Cisco NAC Appliance out-of-band for central- and edge-deployment scenarios
- Describe how to add an out-of-band Cisco NAS to the Cisco NAM
- Describe how to implement the Cisco NAC Appliance out-of-band deployment for the different Cisco NAS operating modes

Out-of-Band Process Flow

This topic describes the Cisco NAC Appliance out-of-band process flow.



OOB Process Flow

1. End user attaches a laptop to the network.

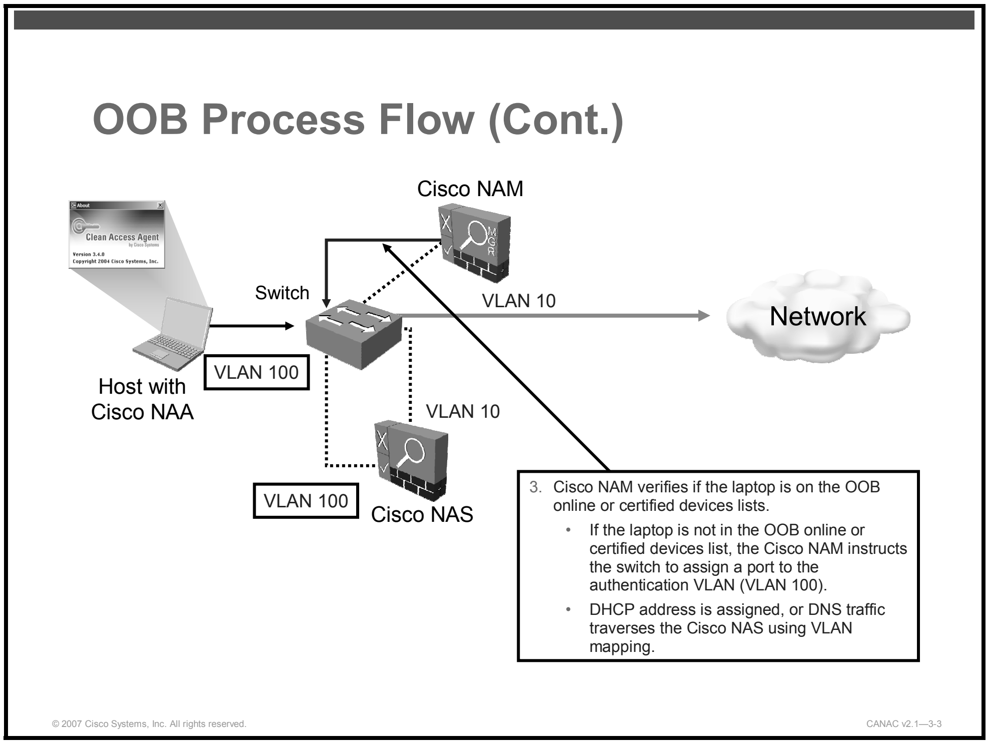
2. Switch sends MAC address via SNMP-based notification to Cisco NAM.

CANAC v2.1—3-2

The following process occurs when a user attempts to access a network web server that is protected by the Cisco NAC Appliance out-of-band solution:

Step 1 A user attaches a laptop to the network.

Step 2 When the laptop first accesses the network, the switch sends the MAC address of the laptop via a Simple Network Management Protocol (SNMP)-based notification to the Cisco NAC Appliance Manager (Cisco NAM).

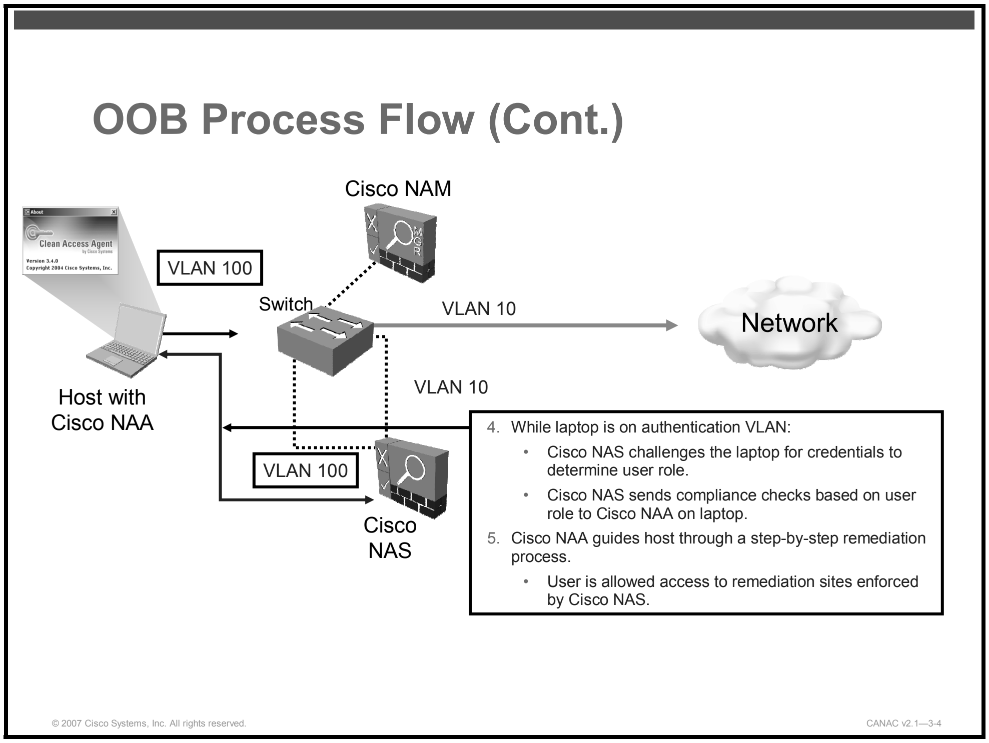


OOB Process Flow (Cont.)

3. Cisco NAM verifies if the laptop is on the OOB online or certified devices lists.
   - If the laptop is not in the OOB online or certified devices list, the Cisco NAM instructs the switch to assign a port to the authentication VLAN (VLAN 100).
   - DHCP address is assigned, or DNS traffic traverses the Cisco NAS using VLAN mapping.

Step 3 The Cisco NAM verifies whether the laptop (device) is on the out-of-band online list or certified devices list. If the device is on one of the two lists, the laptop is logged onto the network. If the device does not appear on either list, these processes take place:

- The Cisco NAM instructs the switch to assign the port that the device is on to either the authentication or quarantine VLAN (authentication VLAN 100 in the figure).
- Using VLAN mapping, a DHCP address is assigned and Domain Name System (DNS) traffic traverses the Cisco NAC Appliance Server (Cisco NAS).



OOB Process Flow (Cont.)

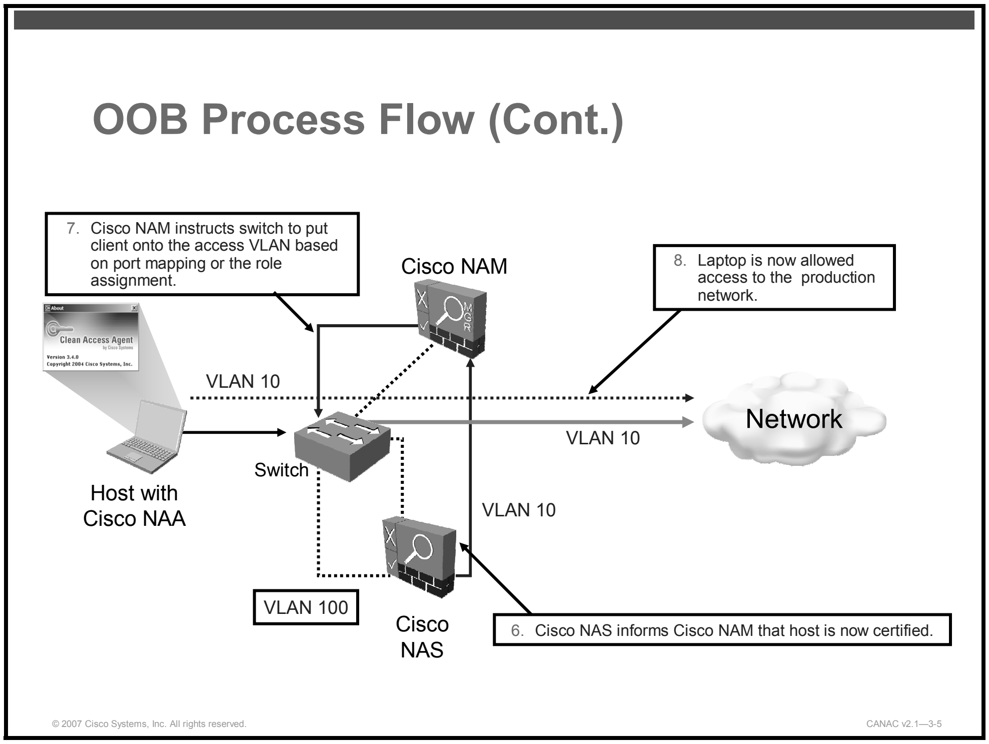
4. While laptop is on authentication VLAN:
   - Cisco NAS challenges the laptop for credentials to determine user role.
   - Cisco NAS sends compliance checks based on user role to Cisco NAA on laptop.
5. Cisco NAA guides host through a step-by-step remediation process.
   - User is allowed access to remediation sites enforced by Cisco NAS.

CANAC v2.1—3-4

Step 4 The Cisco NAS is on the same authentication VLAN (VLAN 100) that the device is now on. While the device is on the authentication VLAN, these processes occur:

- The Cisco NAS challenges the device for user credentials to determine the role of the device user.
- If the use of the Cisco NAC Appliance Agent (Cisco NAA) is enforced, the Cisco NAS sends compliance checks to the Cisco NAA based on the requirements of that role.

Step 5 The Cisco NAA guides the user through a step-by-step remediation process. During this process, the user is allowed access to remediation sites that are provided by the Cisco NAS.



OOB Process Flow (Cont.)

7. Cisco NAM instructs switch to put client onto the access VLAN based on port mapping or the role assignment.

8. Laptop is now allowed access to the production network.

6. Cisco NAS informs Cisco NAM that host is now certified.

CANAC v2.1—3-5

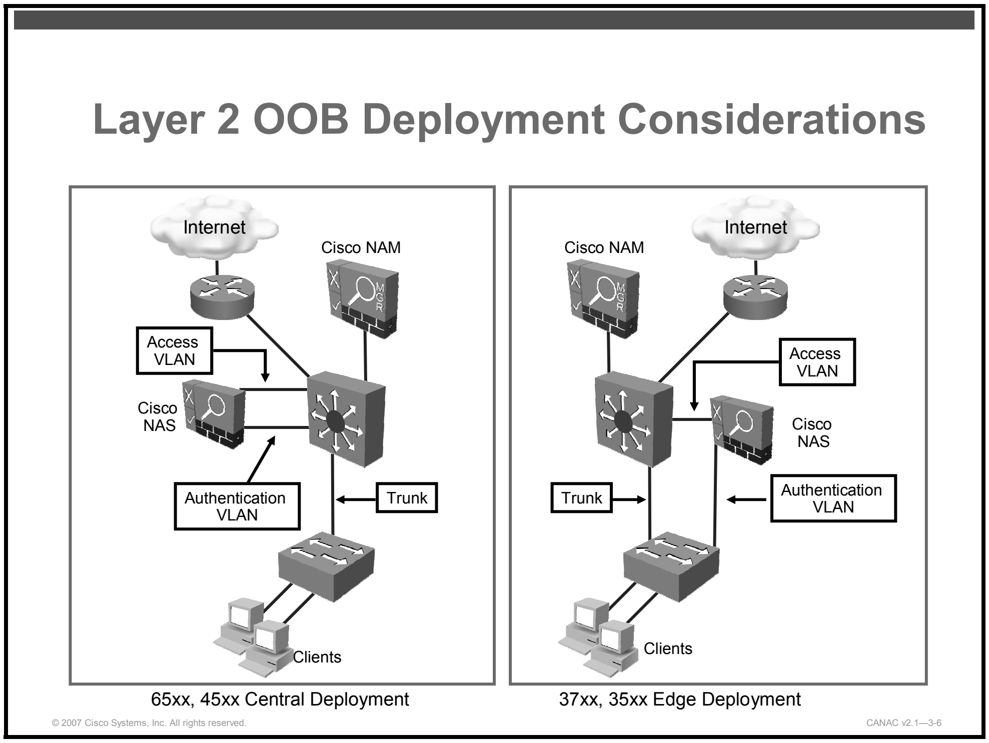
Step 6 When remediation is complete, the Cisco NAS informs the Cisco NAM that the device is now certified.

Step 7 The Cisco NAM instructs the switch to put the device port onto the access VLAN (VLAN 10 in the diagram) based on either port mapping or role assignment.

Step 8 The device can now access the network.

Out-of-Band Deployment Considerations

This topic describes the considerations for implementing the Cisco NAC Appliance out-of-band for central and edge deployment scenarios.



Layer 2 OOB Deployment Considerations

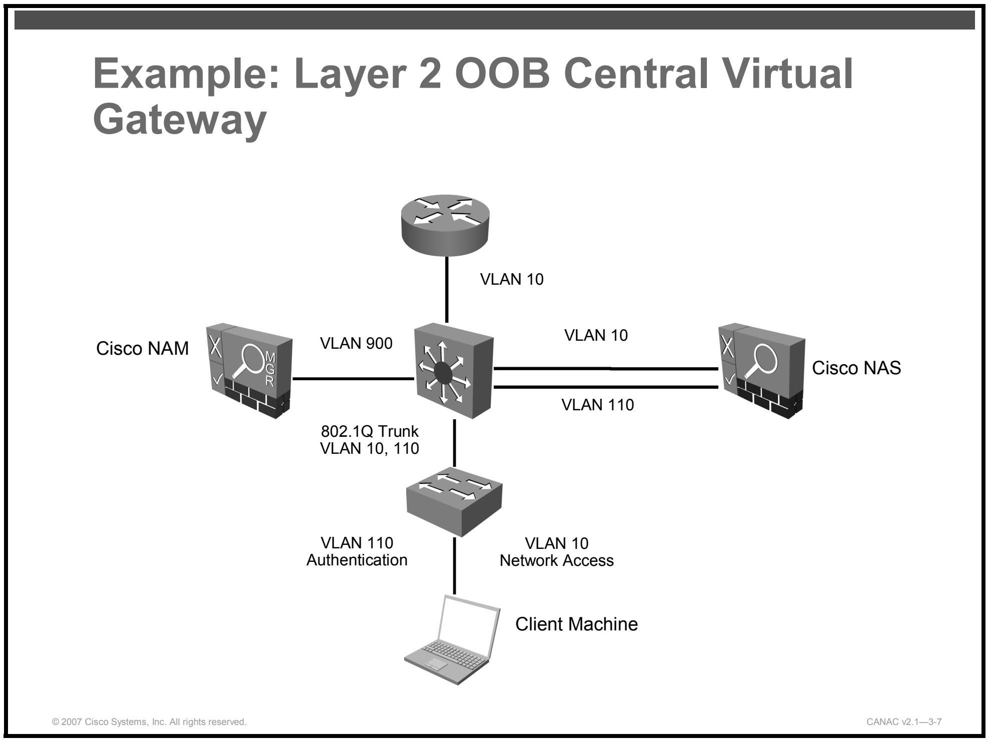
65xx, 45xx Central Deployment

37xx, 35xx Edge Deployment

CANAC v2.1—3-6

The in-band implementation considerations for central versus edge deployments generally apply to out-of-band implementation. However, to incorporate Cisco NAC Appliance out-of-band in your network, you must add an authentication VLAN to your network and trunk all authentication VLANs to the untrusted interface of the Cisco NAS for all gateway modes.

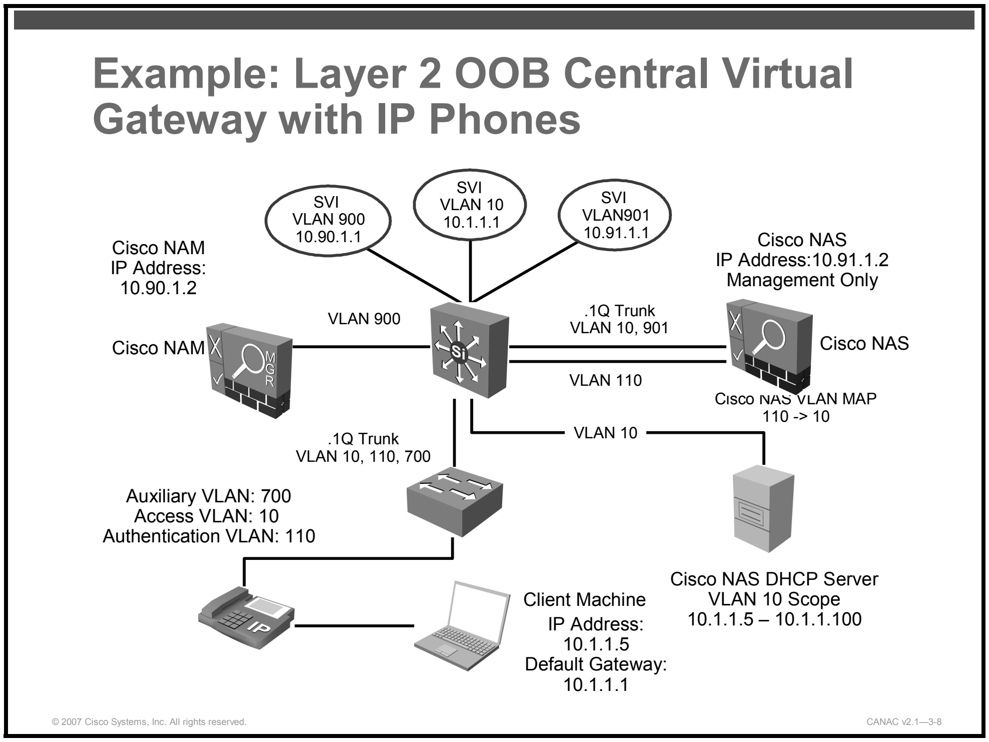
Note For out-of-band implementations, central deployment for the Cisco NAS virtual gateway operating mode is normally implemented for Cisco Catalyst 6500 Series switches and the Cisco 4500 Layer 3 switches. Edge deployment for the Cisco NAS virtual gateway is normally implemented for Cisco 3750 and Cisco 3550 Layer 3 switches.



Example: Layer 2 OOB Central Virtual Gateway

CANAC v2.1—3-7

The figure shows an example Cisco NAC Appliance Layer 2 out-of-band topology. The posture assessment is completed in-band with the Cisco NAS on the authentication VLAN 110. After the client has been successfully assessed, the client can access the network on VLAN 10.



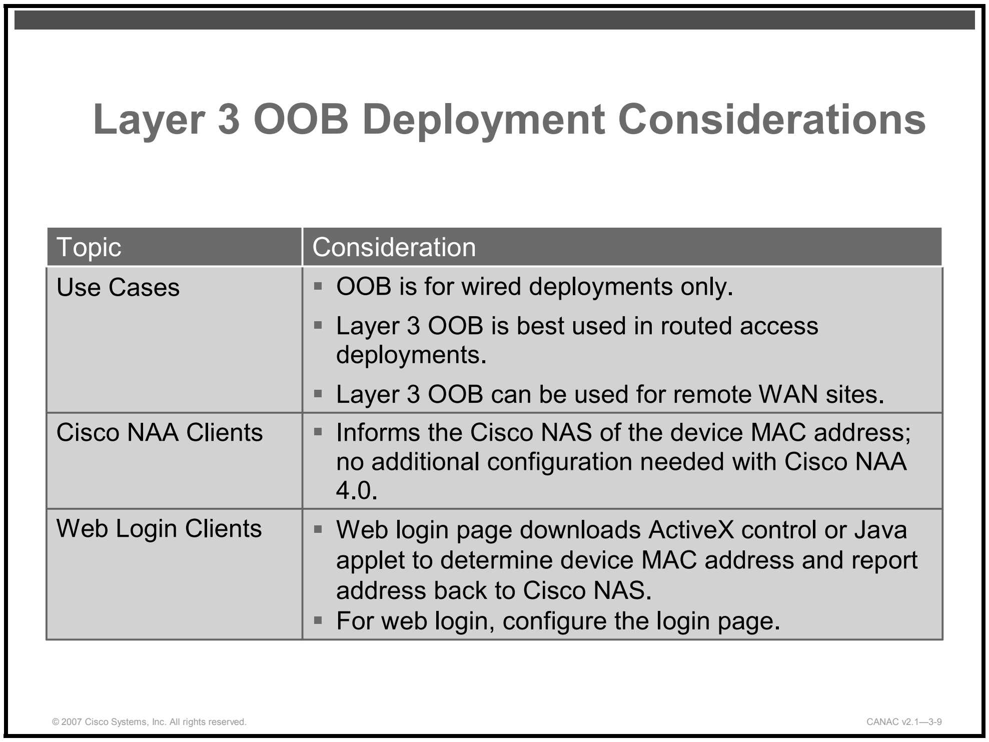
Example: Layer 2 OOB Central Virtual Gateway with IP Phones

CANAC v2.1—3-8

The Cisco NAC Appliance Layer 2 out-of-band central virtual gateway solution works well with VoIP solutions. In the figure, the authorization VLAN is 110 and the access VLAN is 10. The auxiliary VLAN 700 is used by the Cisco IP phone.

There are some Cisco NAC Appliance deployment scenarios that require that a client machine obtains a new IP address when it is moved from the authentication VLAN to the access VLAN. Currently, the only way to trigger the client machine to perform a DHCP release and renew procedure is to bounce the switchport. However, if the client machine is connected behind an IP phone, bouncing the port disrupts IP-based phone service. Port bouncing is required in these three modes:

- Layer 2 out-of-band virtual gateway with role-based VLAN assignment
- Layer 2 out-of-band real-IP gateway
- Layer 3 out-of-band



Layer 3 OOB Deployment Considerations

Topic	Consideration
Use Cases	▪ OOB is for wired deployments only. ▪ Layer 3 OOB is best used in routed access deployments. ▪ Layer 3 OOB can be used for remote WAN sites.
Cisco NAA Clients	▪ Informs the Cisco NAS of the device MAC address; no additional configuration needed with Cisco NAA 4.0.
Web Login Clients	▪ Web login page downloads ActiveX control or Java applet to determine device MAC address and report address back to Cisco NAS. ▪ For web login, configure the login page.

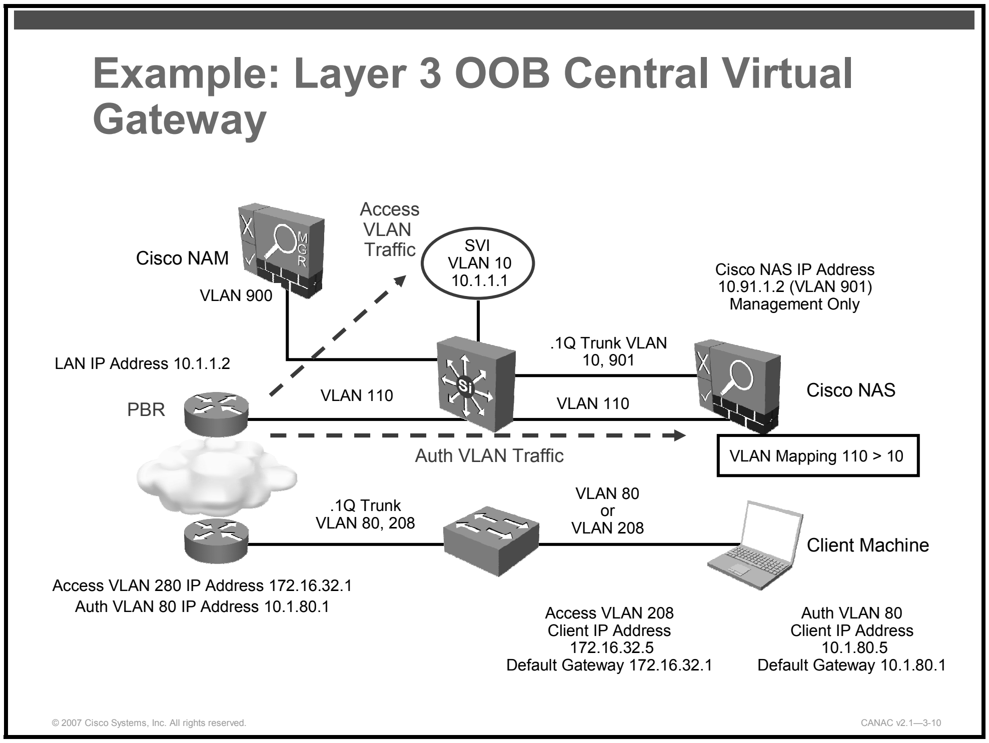
When deploying Cisco NAC Appliance as Layer 3 out-of-band, there are considerations for the use of the deployment and for Cisco NAA and web login clients.

The Cisco NAC Appliance Release 4.0 supports multihop Layer 3 support for out-of-band deployments, enabling administrators to deploy the Cisco NAS out-of-band centrally in the core or in the distribution layer. Using the Cisco NAC Appliance Layer 3 out-of-band feature, users who are more than one Layer 3 hop away from the Cisco NAS are supported and their traffic only has to go through Cisco NAC Appliance for authentication and posture assessment. Layer 3 out-of-band can be used for remote WAN sites. However, consider alternatives to this scenario, including having a remote Cisco NAS at the WAN sites and having a Layer 3 in-band Cisco NAS in the central site to support the remote WAN sites.

Note Layer 3 out-of-band requires changing the end-user IP address using port bouncing. The Cisco NAC Appliance Release 4.0.0 does not support the end user behind IP telephony for Layer 3 out-of-band. Support will be enabled for end users behind IP telephony for Layer 3 out-of-band in an upcoming maintenance release.

In any type of deployment, the Cisco NAM and Cisco NAS need to obtain the client MAC address to be able to perform IP address-to-MAC address mapping. In Layer 3 out-of-band deployment, it is the job of the Cisco NAA Release 4.0, or in the case of web-based clients, an ActiveX control or a Java applet, to acquire the client MAC address. After the MAC address has been acquired, the login process continues with the Cisco NAA or the ActiveX control or Java applet sending the MAC address to the Cisco NAS and the Cisco NAM.

For clients with Cisco NAA Release 4.0, the MAC address detection mechanism of the Release 4.0.0.0 and above Cisco NAA will automatically acquire the client MAC address in Layer 3 out-of-band deployments. Cisco NAA Release 4.0 and above will inform the Cisco NAS of MAC addresses. For clients using Cisco NAA, no additional configuration is needed. For clients using web login, you must configure the login page on the Cisco NAM found at Administration > User Pages > Login Page > Add or Edit. Alternatively, you can configure the login page on the Cisco NAS by navigating to Device Management > CCA Servers > Manage [Cisco NAS_IP] > Authentication > Login Page | [Override Global Settings].



Example: Layer 3 OOB Central Virtual Gateway

Cisco NAM
VLAN 900
Access VLAN Traffic
SVI VLAN 10 10.1.1.1
Cisco NAS IP Address 10.91.1.2 (VLAN 901) Management Only
.1Q Trunk VLAN 10, 901
LAN IP Address 10.1.1.2
PBR
VLAN 110
VLAN 110
Cisco NAS
Auth VLAN Traffic
VLAN Mapping 110 > 10
.1Q Trunk VLAN 80, 208
VLAN 80 or VLAN 208
Client Machine
Access VLAN 280 IP Address 172.16.32.1
Auth VLAN 80 IP Address 10.1.80.1
Access VLAN 208 Client IP Address 172.16.32.5 Default Gateway 172.16.32.1
Auth VLAN 80 Client IP Address 10.1.80.5 Default Gateway 10.1.80.1

CANAC v2.1—3-10

The figure shows a typical Layer 3 central out-of-band virtual gateway configuration. The client is multiple hops away from the Cisco NAS. Traffic generated by the client machine before and during posture assessment is sent only to the Cisco NAS. After the client machine is successfully logged in, the client machine is switched from VLAN 80 to VLAN 208, and the machine bypasses the Cisco NAS. In this sample topology, the Cisco NAS securely manages traffic only during assessment.

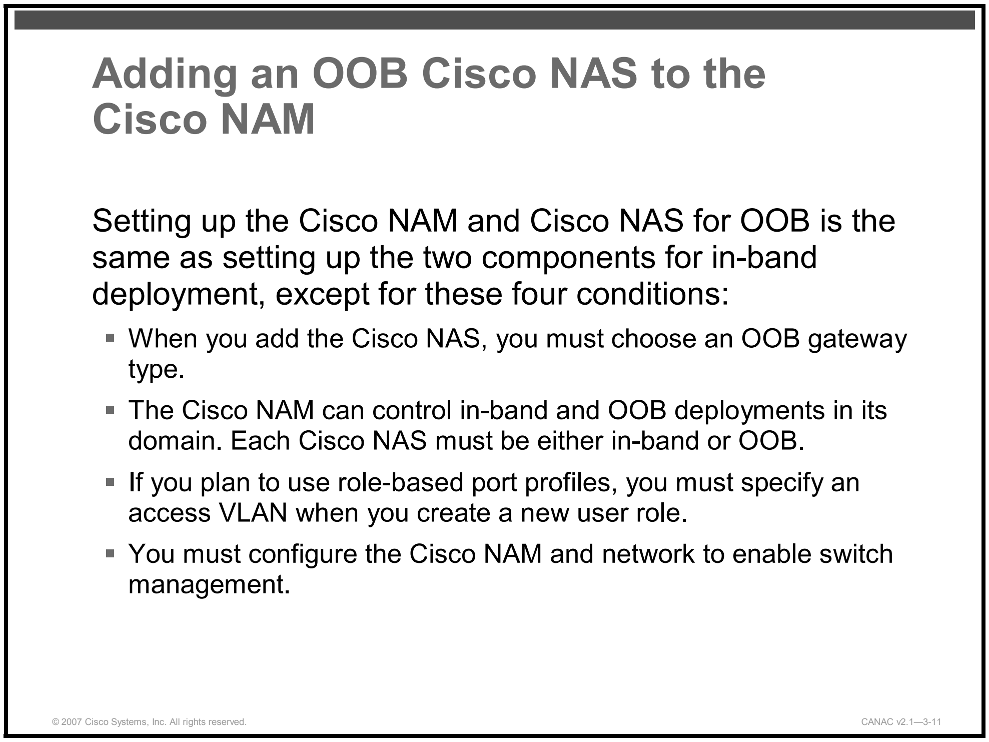
You can use policy-based routing (PBR) or VPN routing and forwarding (VRF) to route the authenticated VLAN traffic to the Cisco NAS and to route the access VLAN traffic to bypass the Cisco NAS.

The Cisco NAM and Cisco NAS use SNMP for traps and switch configuration. In a Layer 3 out-of-band topology, you can use only the supported Cisco switches. For a Cisco NAC Appliance Layer 3 out-of-band deployment to work, client machines have to pass their MAC address to the Cisco NAM. To pass the MAC address, client machines must either have Cisco NAA Release 4.0 installed or use ActiveX or a Java applet.

The Cisco NAA Release 4.0 always sends the MAC and IP address pair of the client at login request regardless of the Cisco NAS configuration.

Adding an Out-of-Band Cisco NAS to the Cisco NAM

This topic describes how to add an out-of-band Cisco NAS to the Cisco NAM.



Adding an OOB Cisco NAS to the Cisco NAM

Setting up the Cisco NAM and Cisco NAS for OOB is the same as setting up the two components for in-band deployment, except for these four conditions:

- When you add the Cisco NAS, you must choose an OOB gateway type.
- The Cisco NAM can control in-band and OOB deployments in its domain. Each Cisco NAS must be either in-band or OOB.
- If you plan to use role-based port profiles, you must specify an access VLAN when you create a new user role.
- You must configure the Cisco NAM and network to enable switch management.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-11

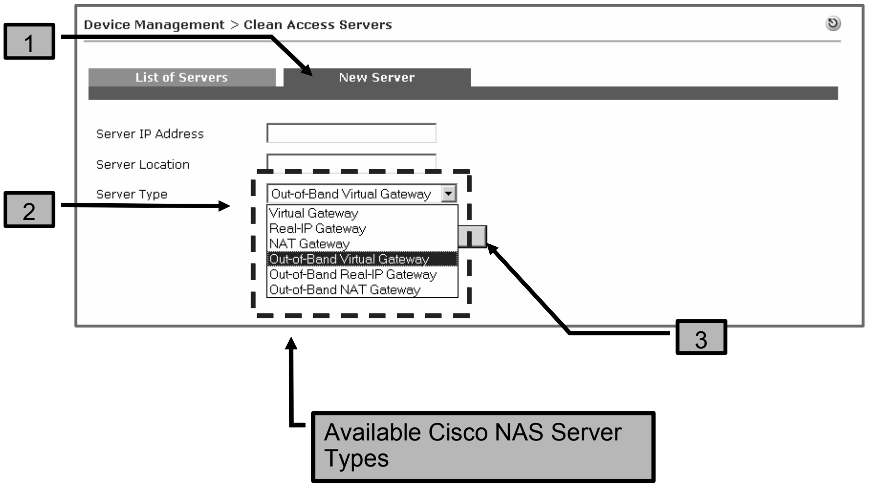
The Cisco NAC Appliance out-of-band setup differs from a traditional Cisco NAC Appliance in-band setup in these ways:

- When you add the Cisco NAS, you must choose from these out-of-band gateway types:
  - Out-of-band virtual gateway
  - Out-of-band real-IP gateway
  - Out-of-band Network Address Translation (NAT) gateway

Note The out-of-band NAT gateway server choice is only used in labs and is not considered a production server type.

- The Cisco NAM can control both in-band and out-of-band Cisco NAS deployments in its domain. However, a single Cisco NAS must be either in-band or out-of-band.
- If you plan to use role-based port profiles, you must specify an access VLAN when you create a new user role.
- You must configure the network and the Cisco NAM for switch management to enable the proper functioning of the authentication and certification processes. Switch management configuration for out-of-band deployment is done directly in the Switch Management module of the Cisco NAM web administration console and is described in the Managing Switches lesson of this module.

Adding an OOB Cisco NAS to the Cisco NAM (Cont.)



Available Cisco NAS Server Types

CANAC v2.1—3-12

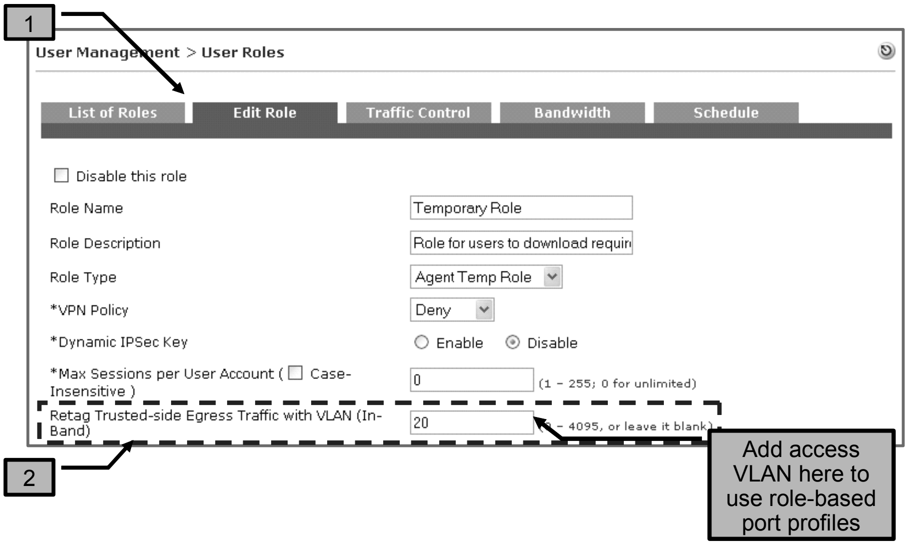
To add an out-of-band Cisco NAS to a Cisco NAM, complete these steps:

Step 1 Go to **Device Management > Clean Access Servers** and click the **New Server** tab.

Step 2 Select the server type that you want from the Server Type drop-down menu.

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

Configuring User Roles to Specify Access VLANs for Role-Based Port Profiles



☐ Disable this role

Role Name: Temporary Role

Role Description: Role for users to download requir

Role Type: Agent Temp Role

*VPN Policy: Deny

*Dynamic IPSec Key: ○ Enable ● Disable

*Max Sessions per User Account (☐ Case-Insensitive): 0 (1 – 255; 0 for unlimited)

Retag Trusted-side Egress Traffic with VLAN (In-Band): 20 (0 – 4095, or leave it blank)

Add access VLAN here to use role-based port profiles

CANAC v2.1—3-13

To configure user roles to specify access VLANs for role-based port profiles, follow these steps:

Step 1 Go to User Management > User Roles > Edit Role.

Step 2 In the Retag Trusted-Side Egress Traffic with VLAN (In-Band) field, enter the access VLAN that is used for role-based port profiles.

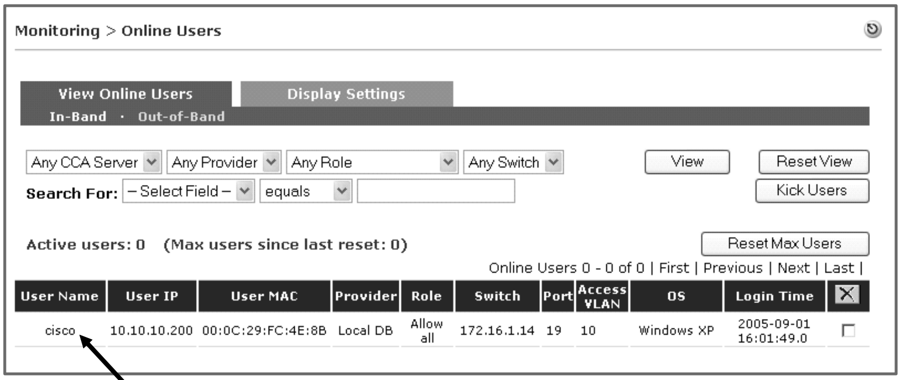
After you have finished posture assessment and any necessary remediation, and the client device is deemed certified, you can assign the switch port to which the client is connected to a different access VLAN. The new access VLAN that the machine is assigned to is the Out-of-Band User Role VLAN value specified by user role. With this configuration, users connecting to the same port at different times can be assigned to different access VLANs based on this setting in their user role.

For out-of-band deployment, if you are configuring role-based VLAN switching for a controlled port, you must specify an access VLAN ID when you create the user role. When an out-of-band user logs in from a managed switch port, the Cisco NAM does three things:

- Determines the role of the user based on the user login credentials
- Checks if role-based VLAN switching is specified for the port in the Port Profile
- Switches the user to the access VLAN, after the client is certified, according to the value specified in the Out-of-Band User Role VLAN field for the user role

Client-connected switch ports use managed port profiles. When a client connects to a managed port, the port is set to the authentication VLAN. After the client is authenticated and certified, the port is set to the access VLAN that you specified in the Port profile (default access VLAN, user role VLAN, or initial port VLAN).

Display OOB Users



Monitoring > Online Users

Search For: – Select Field – equals

Active users: 0 (Max users since last reset: 0)

Online Users 0 - 0 of 0 | First | Previous | Next | Last |

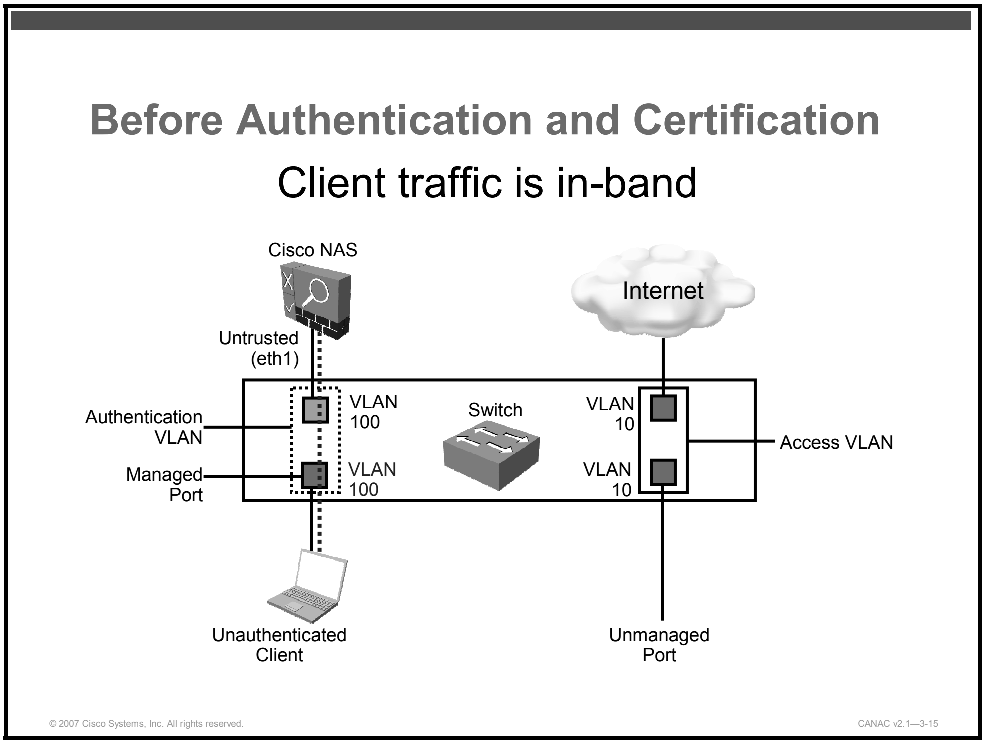
User Name	User IP	User MAC	Provider	Role	Switch	Port	Access VLAN	OS	Login Time	☒
cisco	10.10.10.200	00:0C:29:FC:4E:8B	Local DB	Allow all	172.16.1.14	19	10	Windows XP	2005-09-01 16:01:49.0	□

Current OOB Online User List

To display current out-of-band users, go to **Monitoring > Online Users > Out-of-Band**. The information that appears on this form allows you to filter for specific types of online users. You can also see the same information for the list of in-band users by clicking the In-Band sublink.

Implementing Cisco NAS Out-of-Band Operating Modes

This topic describes how to implement the Cisco NAC Appliance out-of-band deployment for the different Cisco NAS operating modes.



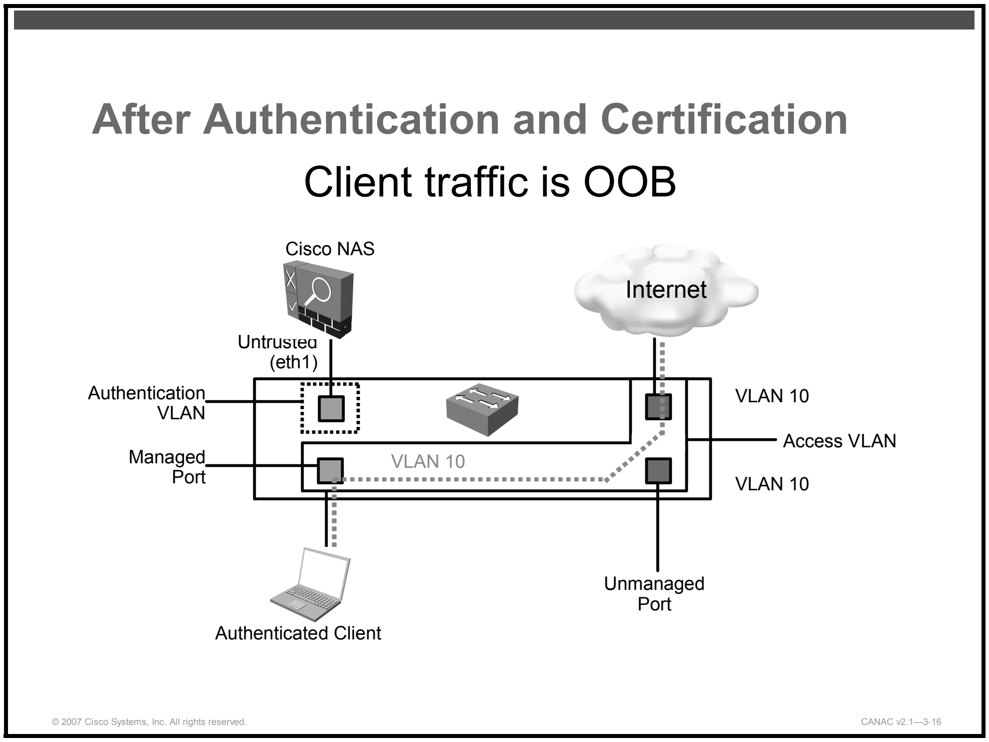
Before Authentication and Certification

Client traffic is in-band

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—3-15

The figure shows the basic VLAN traffic flow for an unauthenticated client attached to an out-of-band deployment. When an unauthenticated client first connects to a managed port on a managed switch, the switch assigns the client the authentication VLAN that is specified in the port profile that you configured for this managed port. The switch then sends all traffic from the authentication VLAN client to the untrusted interface of the Cisco NAS. The client authenticates through the Cisco NAS, and if the Cisco NAC Appliance is enabled, the client goes through the Cisco NAC Appliance certification process. Because the client is on the authentication VLAN, all client traffic must go through the Cisco NAS and the client is considered to be in-band.

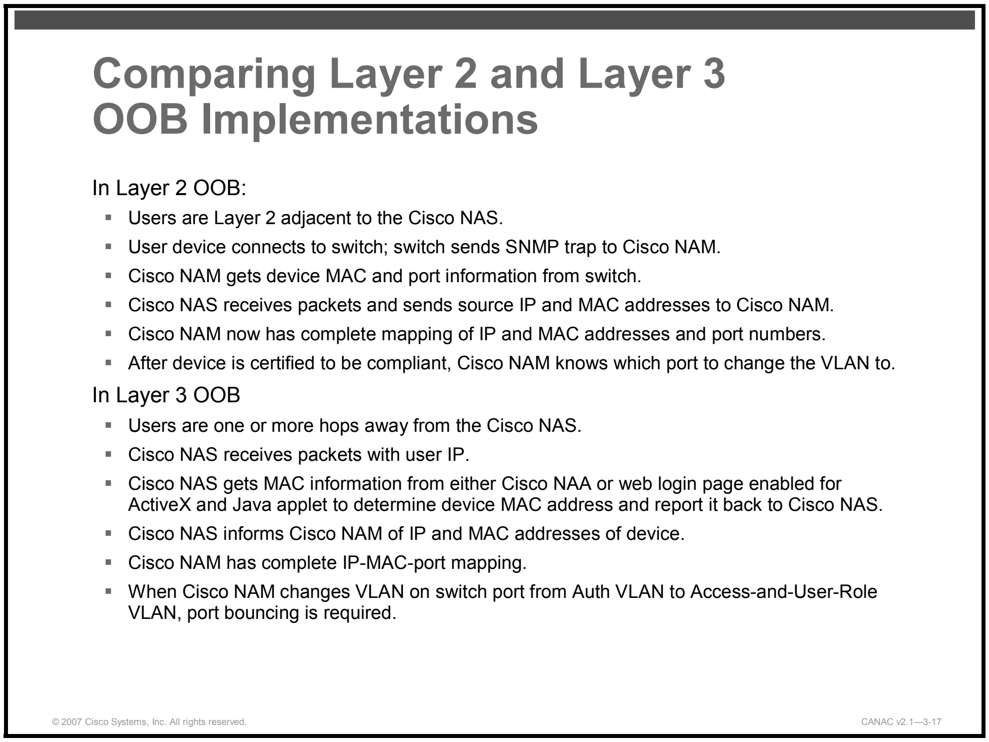


After Authentication and Certification

Client traffic is OOB

CANAC v2.1—3-16

After the client is authenticated and certified (that is, appears on the certified devices list), the Cisco NAM switches the VLAN of the client port to the access VLAN that is specified in the port profile that you configured for the port (VLAN 10 in the figure). After the client is on the access VLAN, the switch no longer directs the client traffic to the untrusted interface of the Cisco NAS. At this point, the client is on the trusted network and is considered to be out-of-band.



Comparing Layer 2 and Layer 3 OOB Implementations

In Layer 2 OOB:

- Users are Layer 2 adjacent to the Cisco NAS.
- User device connects to switch; switch sends SNMP trap to Cisco NAM.
- Cisco NAM gets device MAC and port information from switch.
- Cisco NAS receives packets and sends source IP and MAC addresses to Cisco NAM.
- Cisco NAM now has complete mapping of IP and MAC addresses and port numbers.
- After device is certified to be compliant, Cisco NAM knows which port to change the VLAN to.

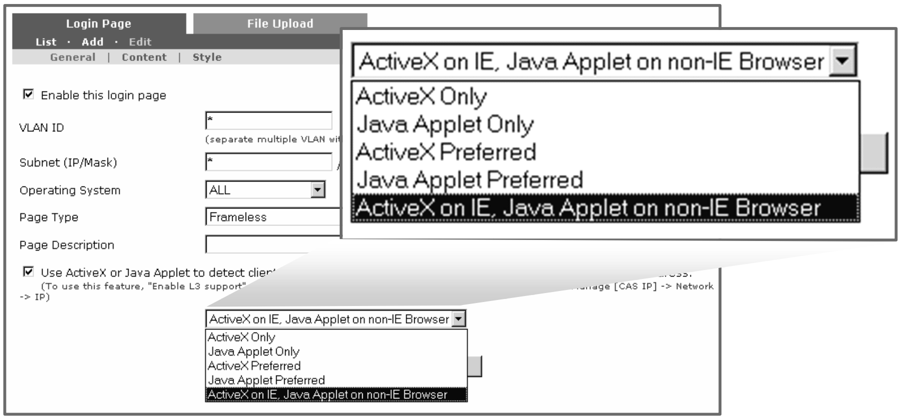
In Layer 3 OOB

- Users are one or more hops away from the Cisco NAS.
- Cisco NAS receives packets with user IP.
- Cisco NAS gets MAC information from either Cisco NAA or web login page enabled for ActiveX and Java applet to determine device MAC address and report it back to Cisco NAS.
- Cisco NAS informs Cisco NAM of IP and MAC addresses of device.
- Cisco NAM has complete IP-MAC-port mapping.
- When Cisco NAM changes VLAN on switch port from Auth VLAN to Access-and-User-Role VLAN, port bouncing is required.

The figure describes the differences between Layer 2 and Layer 3 Cisco NAC Appliance out-of-band deployments.

Comparing Layer 2 and Layer 3 OOB Implementations (Cont.)

In a Layer 3 implementation, when a client machine will not be using the Cisco NAA, configure the Cisco NAS to download ActiveX or Java applets to the client machine.



☑ Enable this login page

VLAN ID: *
(separate multiple VLAN wi

Subnet (IP/Mask): *

Operating System: ALL

Page Type: Frameless

Page Description:

☑ Use ActiveX or Java Applet to detect clien
(To use this feature, "Enable L3 support" ...anage [CAS IP] -> Network -> IP)

ActiveX on IE, Java Applet on non-IE Browser

- ActiveX Only
- Java Applet Only
- ActiveX Preferred
- Java Applet Preferred
- ActiveX on IE, Java Applet on non-IE Browser

The figure shows the form for setting up the Login Page, where there is a new check box and drop-down menu called “Use ActiveX or Java Applet to detect client MAC address when Cisco NAS cannot detect the MAC address.” To use this feature, the Enable L3 Support check box must be enabled under Device Management > CCA Servers > Manage [CAS_IP] > Network > IP. For Layer 3 out-of-band configuration details, refer to Configuring Layer 3 Out-of-Band in the *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide.*

The Use ActiveX or Java Applet to detect client MAC address when the Cisco NAS cannot detect the MAC address drop-down menu has these five options:

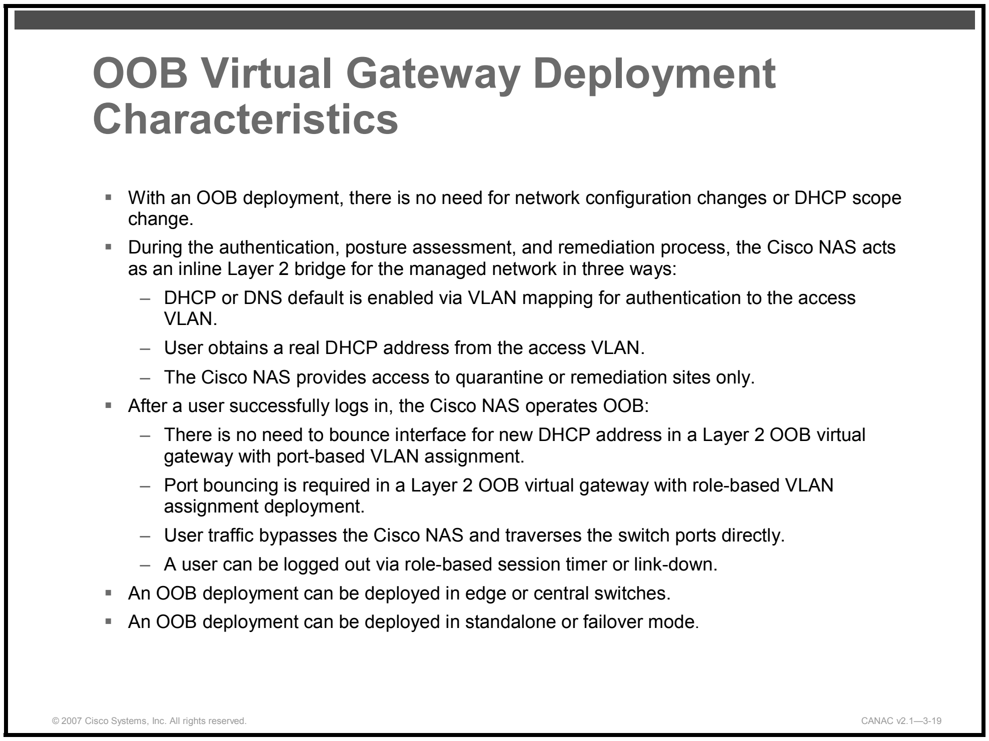
- **ActiveX Only:** Only runs ActiveX. If ActiveX fails, the client machine does not attempt to run the Java applet.
- **Java Applet Only:** Only runs a Java applet. If the Java applet fails, the client machine does not attempt to run ActiveX.
- **ActiveX Preferred:** Runs ActiveX first. If ActiveX fails, the client machine attempts to run a Java applet.
- **Java Applet Preferred:** Runs a Java applet first. If the Java applet fails, the client machine attempts to run ActiveX.
- **ActiveX on IE, Java Applet on Non-IE Browser** (Default): The client machine runs ActiveX if Internet Explorer is detected and runs a Java applet if another (non-IE) browser is detected. If ActiveX fails on IE, the Cisco NAS attempts to run a Java applet. For non-IE browsers, only the Java applet is run.

Here are some useful facts to know about ActiveX and Java applets as they relate to Cisco NAC Appliance:

- ActiveX is fastest with IE.
- ActiveX is preferred and faster than a Java applet.
- ActiveX is supported on IE 6.0 on Windows XP and Windows 2000.

- A Java applet is supported on most browsers.

Note A managed subnet is used for Layer 2 out-of-band only.



OOB Virtual Gateway Deployment Characteristics

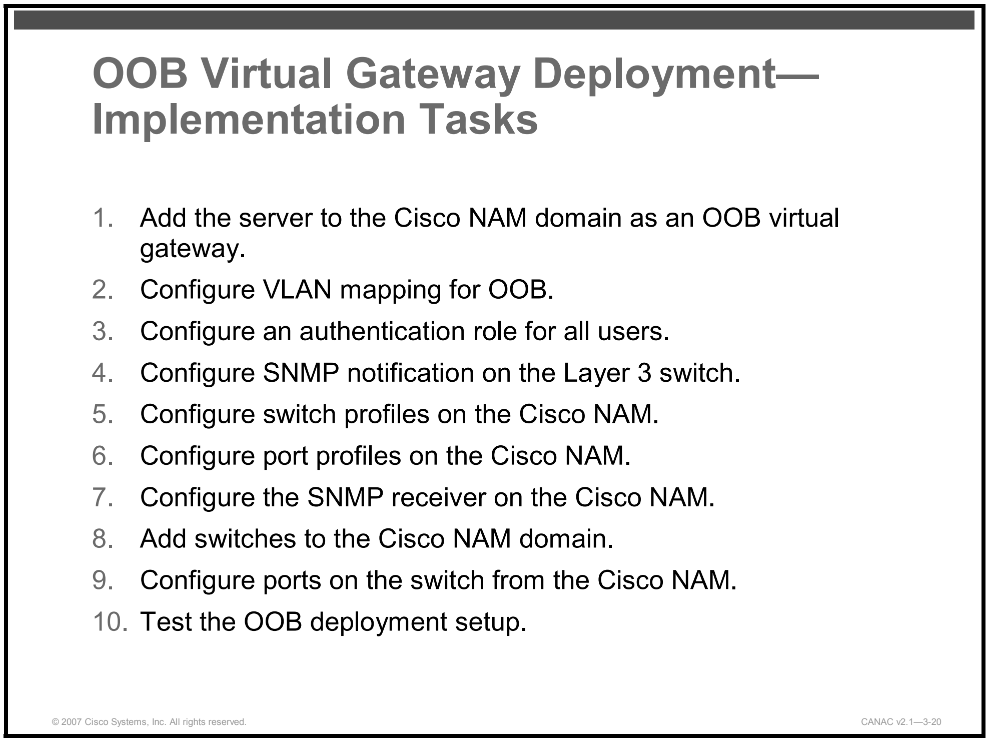
- With an OOB deployment, there is no need for network configuration changes or DHCP scope change.
- During the authentication, posture assessment, and remediation process, the Cisco NAS acts as an inline Layer 2 bridge for the managed network in three ways:
  - DHCP or DNS default is enabled via VLAN mapping for authentication to the access VLAN.
  - User obtains a real DHCP address from the access VLAN.
  - The Cisco NAS provides access to quarantine or remediation sites only.
- After a user successfully logs in, the Cisco NAS operates OOB:
  - There is no need to bounce interface for new DHCP address in a Layer 2 OOB virtual gateway with port-based VLAN assignment.
  - Port bouncing is required in a Layer 2 OOB virtual gateway with role-based VLAN assignment deployment.
  - User traffic bypasses the Cisco NAS and traverses the switch ports directly.
  - A user can be logged out via role-based session timer or link-down.
- An OOB deployment can be deployed in edge or central switches.
- An OOB deployment can be deployed in standalone or failover mode.

CANAC v2.1—3-19

The Cisco NAS can operate in either out-of-band virtual gateway mode or out-of-band real-IP gateway mode. The figure describes out-of-band virtual gateway deployment characteristics. The key advantage of out-of-band virtual gateway deployment is that the client does not change IP addresses from the time that an IP address is acquired to the time that the client gains actual network access on the access VLAN.

In a Layer 2 out-of-band virtual gateway with port-based VLAN assignment, the Cisco NAS uses VLAN mapping to retag the unauthenticated client-allowed traffic (such as DNS or DHCP requests) from the authentication VLAN to the access VLAN and vice versa. In this way, a new client IP address is not needed when the client is eventually switched to the access VLAN, because the DHCP-acquired IP address is already paired with the access VLAN ID.

In a Layer 2 out-of-band virtual gateway with role-based VLAN assignment deployment, the client machine will have one IP address in the authentication VLAN and a different IP address when it is moved to an access VLAN. The change of address is accomplished using port bouncing.



OOB Virtual Gateway Deployment—Implementation Tasks

1. Add the server to the Cisco NAM domain as an OOB virtual gateway.
2. Configure VLAN mapping for OOB.
3. Configure an authentication role for all users.
4. Configure SNMP notification on the Layer 3 switch.
5. Configure switch profiles on the Cisco NAM.
6. Configure port profiles on the Cisco NAM.
7. Configure the SNMP receiver on the Cisco NAM.
8. Add switches to the Cisco NAM domain.
9. Configure ports on the switch from the Cisco NAM.
10. Test the OOB deployment setup.

CANAC v2.1—3-20

To deploy the Cisco NAS as an out-of-band virtual gateway, complete these tasks:

Step 1 Add the Cisco NAS to the Cisco NAM domain as an out-of-band virtual gateway. A Cisco NAS must first be added to the Cisco NAM domain before you can manage it from the web administration console. Ensure that the Cisco NAM and Cisco NAS are on different subnets.

Step 2 Configure VLAN mapping for out-of-band. In virtual gateway mode, the out-of-band Cisco NAS uses VLAN mapping to retag the unauthenticated allowed traffic of a DHCP- or DNS-based client from the authentication VLAN to the access VLAN and vice versa.

Step 3 Configure an authentication role for all users. Add the default login page to allow all users (web login or Cisco NAA users) to authenticate. Create a user role and a local user for out-of-band. Configure an Allow All Traffic policy for authentication.

Step 4 Configure SNMP notification on the Layer 3 switch. Configure SNMP settings and enable SNMP traps for the switch. Cisco NAC Appliance uses MAC notification and linkdown traps, or SNMP linkup and linkdown traps (if MAC notification is not supported).

Step 5 Configure switch profiles on the Cisco NAM. Add a group profile. Then add and configure switch profiles so that the same SNMP settings apply to the same types of switches.

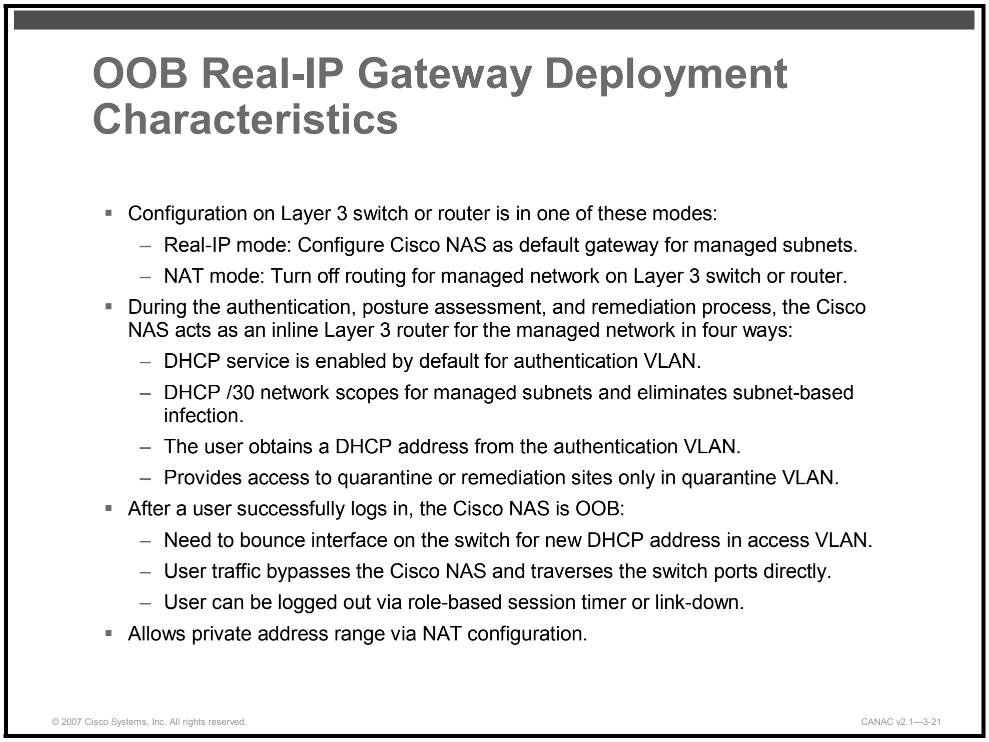
Step 6 Configure port profiles on the Cisco NAM. There are three port profile types for switch ports: uncontrolled, controlled, and controlled using role settings. Regular switch ports should use the uncontrolled port profile. Client-connected switch ports should use controlled port profiles. When a client connects to a controlled port, the port is set to the authentication VLAN. After the client is authenticated and certified, the port is set to the access VLAN that is specified in the port profile or the role settings. For out-of-band real-IP gateways, enable port bouncing to ensure that the client receives a new IP address after each successful authentication and certification. For out-of-band virtual gateways, port bouncing is not necessary because the client uses the same IP address after successful authentication and certification.

Step 7 Configure the SNMP receiver on the Cisco NAM. The SNMP receiver setup provides configuration settings for the SNMP receiver that is running on the Cisco NAM. The SNMP receiver receives the MAC notification or linkdown SNMP trap notifications from the controlled switches and sets the VLAN on the corresponding switch ports.

Step 8 Add switches to the Cisco NAM domain. You can add a switch individually using the Cisco NAC Appliance web-based administration console.

Step 9 Configure ports on the switch. Use the Cisco NAM to apply the appropriate port profile settings to switch ports so that the ports are on the correct access or authentication VLAN specified in the profiles.

Step 10 Test the out-of-band deployment setup. After configuration is complete, connect your client machine to a controlled switch port and test your setup by logging in on the authentication VLAN as a user.

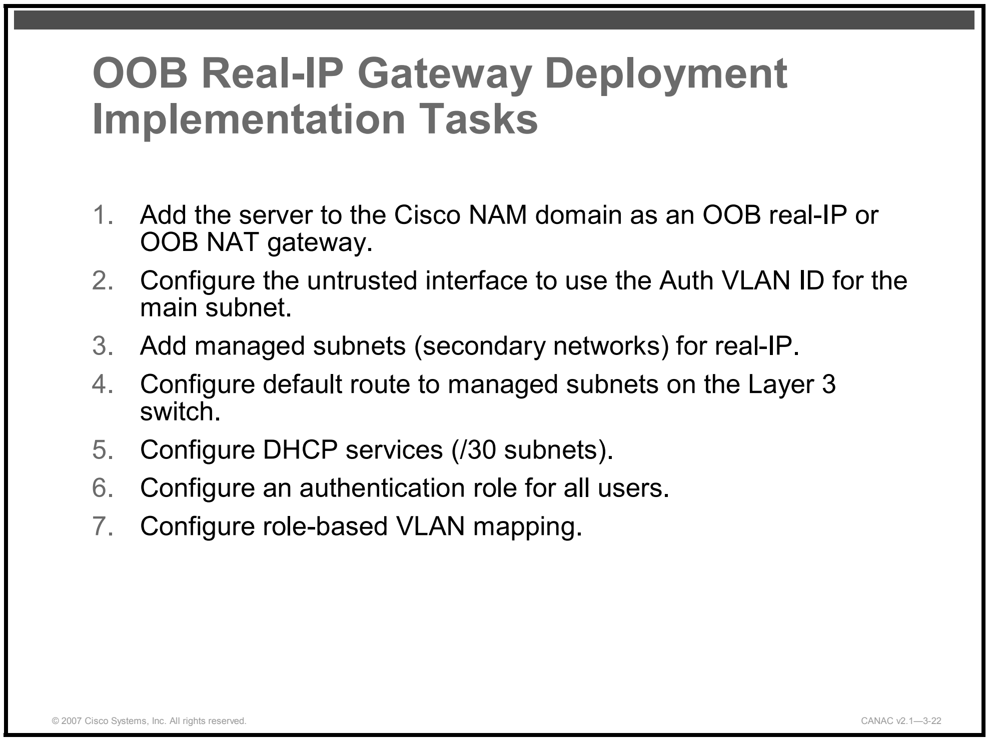


OOB Real-IP Gateway Deployment Characteristics

- Configuration on Layer 3 switch or router is in one of these modes:
  - Real-IP mode: Configure Cisco NAS as default gateway for managed subnets.
  - NAT mode: Turn off routing for managed network on Layer 3 switch or router.
- During the authentication, posture assessment, and remediation process, the Cisco NAS acts as an inline Layer 3 router for the managed network in four ways:
  - DHCP service is enabled by default for authentication VLAN.
  - DHCP /30 network scopes for managed subnets and eliminates subnet-based infection.
  - The user obtains a DHCP address from the authentication VLAN.
  - Provides access to quarantine or remediation sites only in quarantine VLAN.
- After a user successfully logs in, the Cisco NAS is OOB:
  - Need to bounce interface on the switch for new DHCP address in access VLAN.
  - User traffic bypasses the Cisco NAS and traverses the switch ports directly.
  - User can be logged out via role-based session timer or link-down.
- Allows private address range via NAT configuration.

CANAC v2.1—3-21

The figure outlines the characteristics of the Cisco NAS in out-of-band real-IP gateway mode. In this deployment, the client IP address must change when the port is changed from the authentication VLAN to the access VLAN. In an out-of-band real-IP gateway deployment, the switch port has to be bounced so that when the client machine is finally placed on the access VLAN, the client machine will be able to recognize that its authentication VLAN IP address is invalid and then signal the Cisco NAS to receive a new IP address.



OOB Real-IP Gateway Deployment Implementation Tasks

1. Add the server to the Cisco NAM domain as an OOB real-IP or OOB NAT gateway.
2. Configure the untrusted interface to use the Auth VLAN ID for the main subnet.
3. Add managed subnets (secondary networks) for real-IP.
4. Configure default route to managed subnets on the Layer 3 switch.
5. Configure DHCP services (/30 subnets).
6. Configure an authentication role for all users.
7. Configure role-based VLAN mapping.

CANAC v2.1—3-22

To deploy the Cisco NAS as an out-of-band real-IP gateway deployment, complete these tasks:

Step 1 Add the server to the Cisco NAM domain as an out-of-band real-IP or out-of-band NAT gateway. You must first add a Cisco NAS to the Cisco NAM domain before you can manage the Cisco NAS from the web administration console.

Step 2 Configure the untrusted interface to use the authentication VLAN ID for the main subnet. When the Cisco NAS is first added, the untrusted IP address that is provided for the Cisco NAS is automatically assigned a VLAN ID of -1 to denote a main subnet. For out-of-band deployment, you must edit the main subnet so that it uses the authentication VLAN ID value.

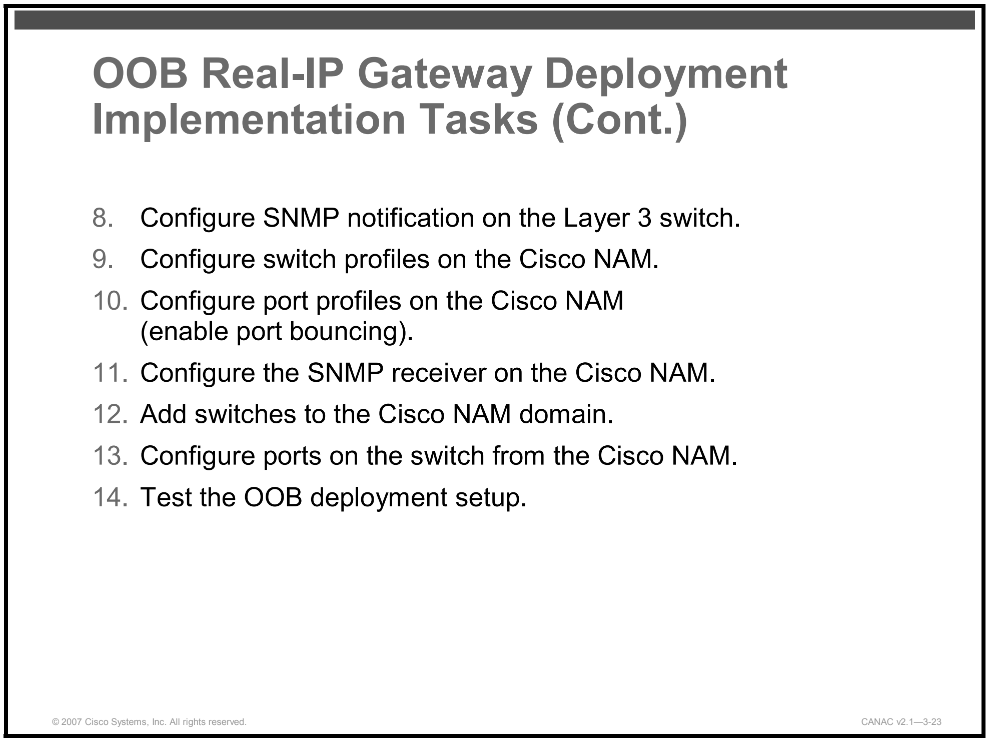
Step 3 Add managed subnets (secondary networks) if you have configured a real-IP gateway. If you have more than one authentication VLAN, you must add additional managed subnets for each authentication VLAN prior to setting up the DHCP configuration.

Step 4 Configure a default route to managed subnets on the Layer 3 switch. When you are using a real-IP gateway, you must configure the switch or router to use the Cisco NAS as the default gateway for the managed subnets. When you are using a NAT gateway, you must turn off routing for the managed network at the Layer 3 switch or router.

Step 5 Configure DHCP services. Enable the Cisco NAS DHCP server mode and configure /30 subnets. The DHCP /30 network searches for managed subnets to eliminate subnet-based infection.

Step 6 Configure an authentication role for all users. Add the default login page to allow all users (web login or Cisco NAA users) to authenticate. Create a user role and a local user for out-of-band. Configure an Allow All Traffic policy for authentication.

Step 7 Configure role-based VLAN mapping. If you plan to use role-based port profiles, you must first specify an access VLAN when you create a new user role and then modify port profiles to use a role-based authentication VLAN-to-access VLAN mapping.



OOB Real-IP Gateway Deployment Implementation Tasks (Cont.)

8. Configure SNMP notification on the Layer 3 switch.
9. Configure switch profiles on the Cisco NAM.
10. Configure port profiles on the Cisco NAM (enable port bouncing).
11. Configure the SNMP receiver on the Cisco NAM.
12. Add switches to the Cisco NAM domain.
13. Configure ports on the switch from the Cisco NAM.
14. Test the OOB deployment setup.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-23

Step 8 Configure SNMP notification on the Layer 3 switch. Configure SNMP settings and enable SNMP traps for the switch. Cisco NAC Appliance uses MAC notification and linkdown traps, or SNMP linkup and linkdown traps if MAC notification is not supported.

Step 9 Configure switch profiles on the Cisco NAM. Add a group profile. Then add and configure switch profiles so that the same SNMP settings apply to the same types of switches.

Step 10 Configure port profiles on the Cisco NAM. Regular switch ports should use the uncontrolled port profile. Client-connected switch ports should use controlled port profiles. For out-of-band real-IP gateways, you must enable port bouncing to ensure that the client receives a new IP address after successful authentication and certification. If you plan to use role-based port profiles, you must also configure the port profiles for role-based authentication VLAN-to-access VLAN mapping.

Step 11 Configure the SNMP receiver on the Cisco NAM. The SNMP receiver setup provides configuration settings for the SNMP receiver that is running on the Cisco NAM. The SNMP receiver receives the MAC notification or linkdown SNMP trap notifications from the controlled switches and sets the VLAN on the corresponding switch ports.

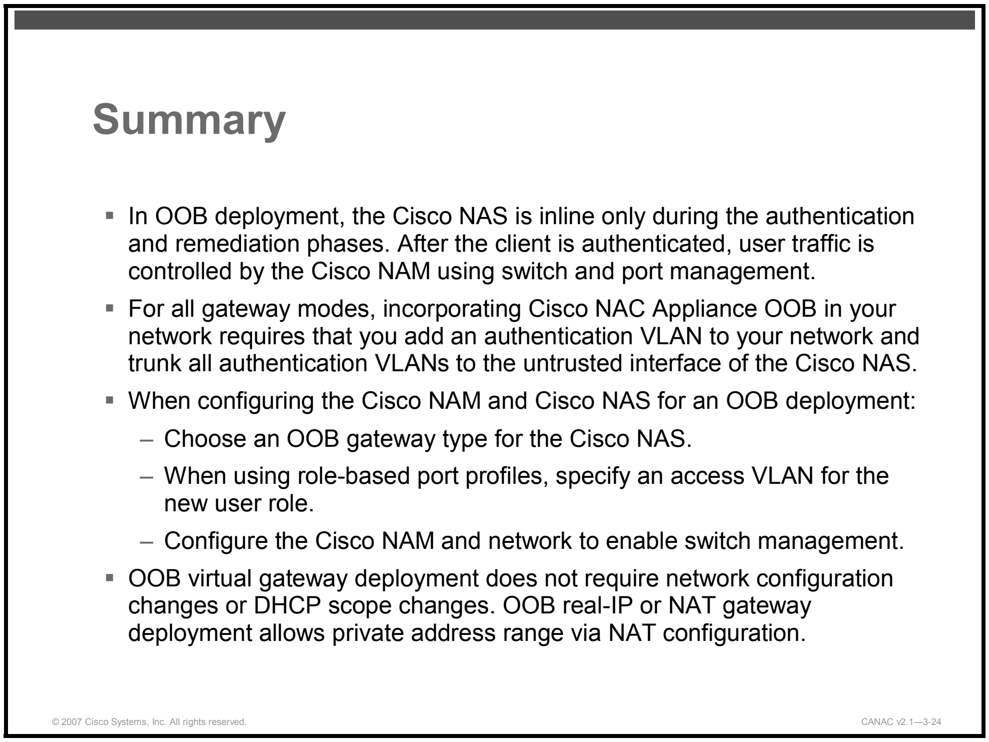
Step 12 Add switches to the Cisco NAM domain. You can add a switch individually using the Cisco NAC Appliance web-based administration console.

Step 13 Configure ports on the switch. Use the Cisco NAM to apply the appropriate port profile settings to switch ports so that the ports are on the correct access VLAN or authentication VLAN that you specified in the port profiles.

Step 14 Test the out-of-band deployment setup. After configuration is complete, connect your client machine to a controlled switch port and test your setup by logging in as a user on the authentication VLAN.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- In OOB deployment, the Cisco NAS is inline only during the authentication and remediation phases. After the client is authenticated, user traffic is controlled by the Cisco NAM using switch and port management.
- For all gateway modes, incorporating Cisco NAC Appliance OOB in your network requires that you add an authentication VLAN to your network and trunk all authentication VLANs to the untrusted interface of the Cisco NAS.
- When configuring the Cisco NAM and Cisco NAS for an OOB deployment:
  - Choose an OOB gateway type for the Cisco NAS.
  - When using role-based port profiles, specify an access VLAN for the new user role.
  - Configure the Cisco NAM and network to enable switch management.
- OOB virtual gateway deployment does not require network configuration changes or DHCP scope changes. OOB real-IP or NAT gateway deployment allows private address range via NAT configuration.

CANAC v2.1—3-24

Lesson 5

Managing Switches

Overview

Most clients will implement a Cisco Network Access Control (NAC) Appliance solution into their existing networks. Therefore, you need to know how to configure and manage existing switches using the Cisco NAC Appliance web-based administration console. This lesson describes how to configure the Cisco NAC Appliance Manager (Cisco NAM) to manage switches and routers for out-of-band deployment scenarios.

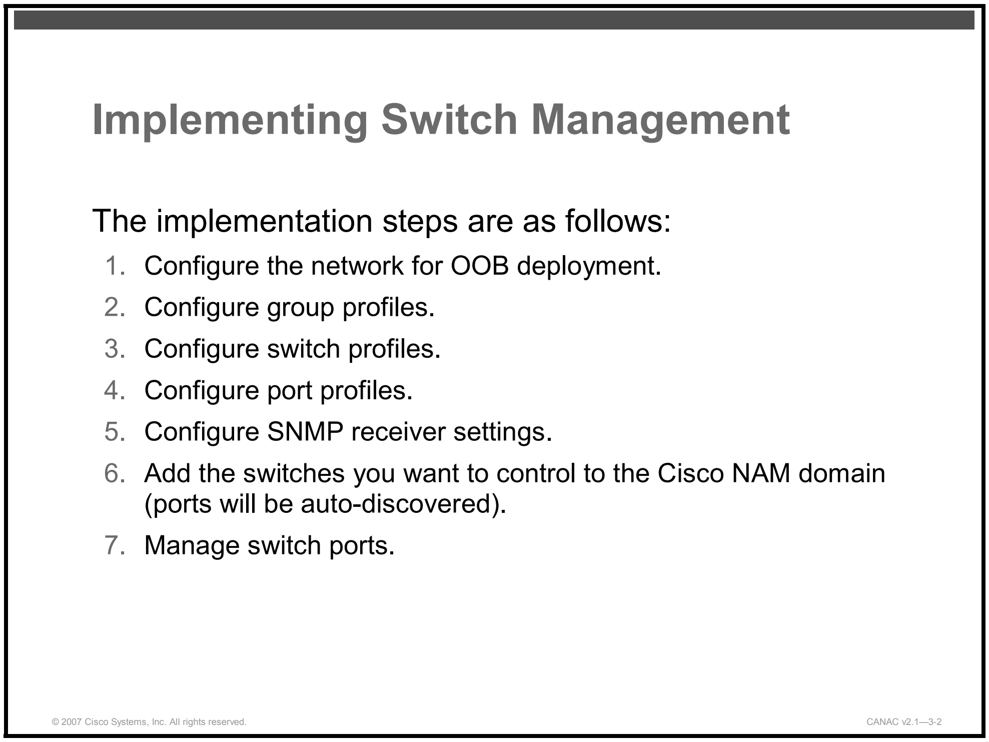
Objectives

Upon completing this lesson, you will be able to configure the Cisco NAM to manage switches for out-of-band deployment scenarios. This ability includes being able to complete these objectives:

- Describe how to implement switch management for Cisco NAC Appliance out-of-band deployment
- Describe how to set up switches so that they can be used with Cisco NAC Appliance out-of-band deployment
- Describe how to configure group profiles on the Cisco NAM for out-of-band deployment
- Describe how to configure switch profiles on the Cisco NAM for out-of-band deployment
- Describe how to configure port profiles on the Cisco NAM for out-of-band deployment
- Describe how to configure the SNMP receiver on the Cisco NAM for out-of-band deployment
- Describe how to add switches to the Cisco NAM managed domain for out-of-band deployment
- Describe how to configure switch ports to use the Cisco NAM port profiles for out-of-band deployment
- Describe how to manage the switch configuration settings for out-of-band deployment

Implementing Switch Management

This topic describes how to implement switch management for out-of-band deployment.



Implementing Switch Management

The implementation steps are as follows:

1. Configure the network for OOB deployment.
2. Configure group profiles.
3. Configure switch profiles.
4. Configure port profiles.
5. Configure SNMP receiver settings.
6. Add the switches you want to control to the Cisco NAM domain (ports will be auto-discovered).
7. Manage switch ports.

CANAC v2.1—3-2

When implementing switch management in the Cisco NAM for out-of-band deployment, you must first configure the switches and routers in your network to communicate with the Cisco NAM and to use the appropriate Simple Network Management Protocol (SNMP) settings. Next, you must configure group, switch, and port profiles on the Cisco NAM, and the Cisco NAM SNMP receiver settings.

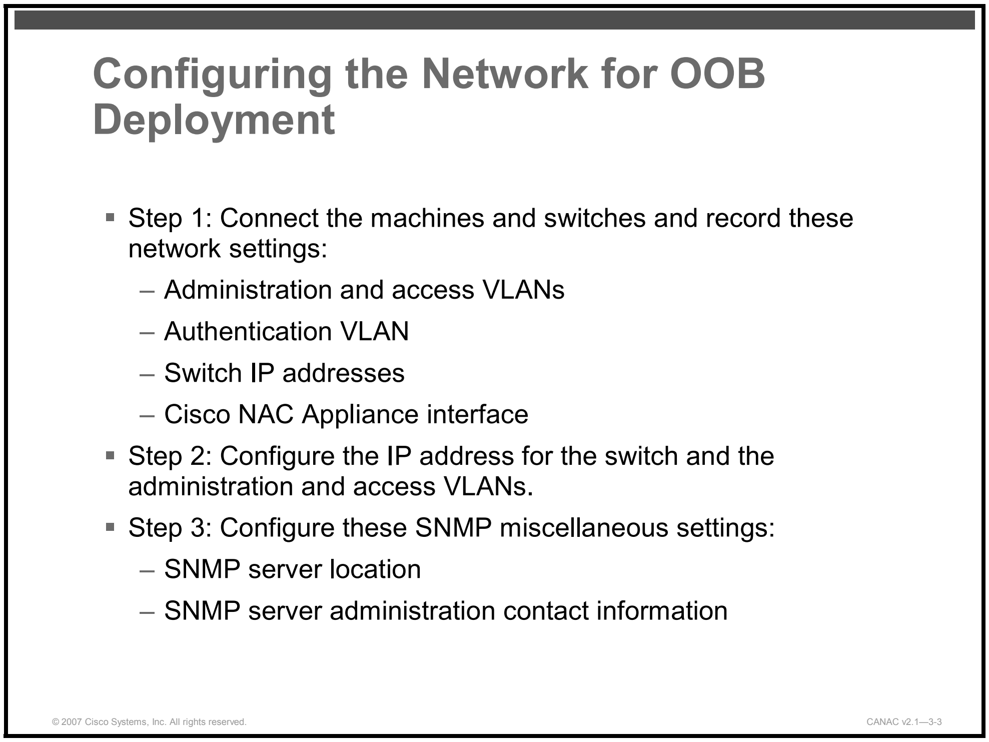
Note The profile concept and the interface that you use for these tasks are similar to those used for the creation and application of user roles or administration groups.

After you configure profiles, add the switches that you want to control to the Cisco NAM domain. Apply the appropriate profiles to each switch.

When switches are added and the ports on the switch are discovered, you can configure the relevant switch ports to use the relevant port profiles. These profiles set up the ports so that they use the appropriate access and authentication VLANs to enable client traffic to be routed temporarily through the Cisco NAC Appliance Server (Cisco NAS) for authentication and certification before allowing this traffic on the trusted network.

Configuring the Network for Out-of-Band Deployment

This topic describes how to set up the switches so that they can be used with a Cisco NAC Appliance out-of-band deployment.



Configuring the Network for OOB Deployment

- Step 1: Connect the machines and switches and record these network settings:
  - Administration and access VLANs
  - Authentication VLAN
  - Switch IP addresses
  - Cisco NAC Appliance interface
- Step 2: Configure the IP address for the switch and the administration and access VLANs.
- Step 3: Configure these SNMP miscellaneous settings:
  - SNMP server location
  - SNMP server administration contact information

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

For the out-of-band authentication sequence to work, you must configure your switches and routers so that they can be managed by the Cisco NAM.

Note Refer to your switch documentation for details on configuring your specific switch model.

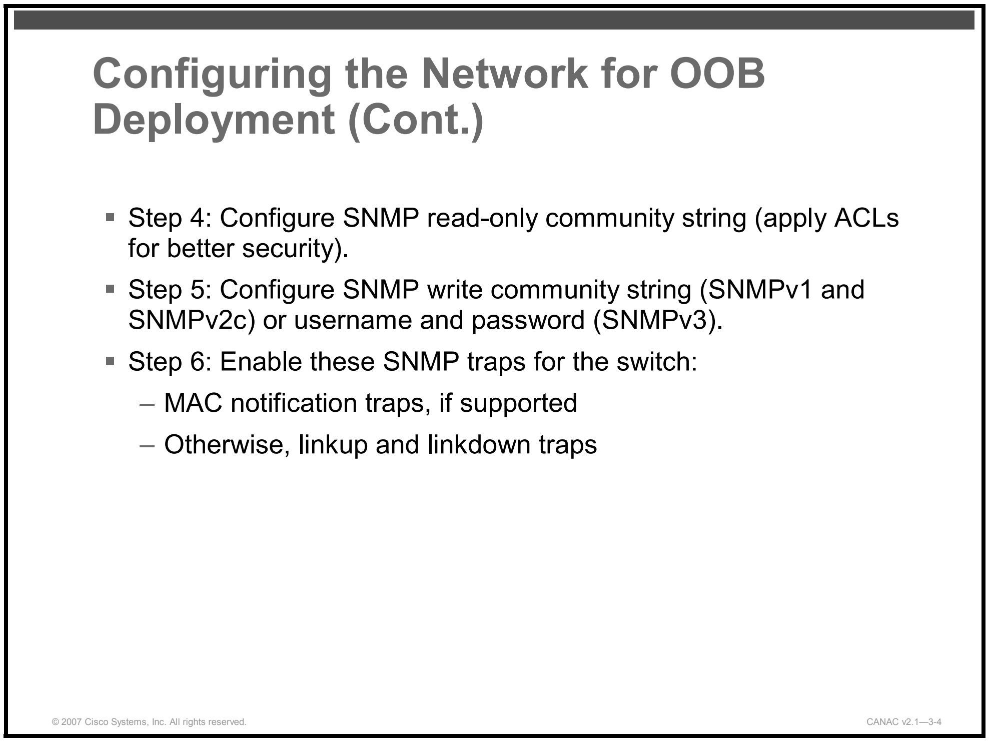
To configure the network for Cisco NAC Appliance out-of-band deployment, complete these steps:

Step 1 Connect the machines and switches. Write down the administration and access VLANs, authentication VLAN, switch IP addresses, and Cisco NAC Appliance interface.

Step 2 Configure the IP address for the switch and the administration and access VLANs.

Step 3 Configure SNMP miscellaneous settings such as the following:

```
# snmp-server location <location_string>
# snmp-server contact <admin_contact_info>
```



Configuring the Network for OOB Deployment (Cont.)

- Step 4: Configure SNMP read-only community string (apply ACLs for better security).
- Step 5: Configure SNMP write community string (SNMPv1 and SNMPv2c) or username and password (SNMPv3).
- Step 6: Enable these SNMP traps for the switch:
  - MAC notification traps, if supported
  - Otherwise, linkup and linkdown traps

Step 4 Configure the SNMP read-only community string. Apply access control lists (ACLs) for increased security. Here is an example configuration:

```
# access-list 20 permit 10.201.0.0 0.0.255.255
# snmp-server community c2950_read ro 20
```

Step 5 Configure the SNMP write community string, either SNMPv1 or SNMPv2c, or username and password (SNMPv3). You can apply ACLs here for increased security. Here is an example configuration:

```
# access-list 21 permit host 10.201.2.15
```

- **SNMPv1 and SNMPv2c settings:** Consider an example in which the SNMP read-write community string is “c2950_write”. The following command string would be used:

  ```
  # snmp-server community c2950_write rw 21
  ```

- **SNMPv3 settings:** Consider an example in which the SNMP username is “c2950_user” and the password is “c2950_auth”. The following command strings would be used:

  ```
  # snmp-server group c2950_group V3 auth read v1default
  write v1default
  # snmp-server user c2950_user c2950_group V3 auth md5
  c2950_auth access 21
  ```

Step 6 Enable SNMP traps for the switch. Cisco NAC Appliance uses the MAC notification trap by default. If the switch does not support the MAC-notification trap, the Cisco NAM uses the SNMP linkup or linkdown trap. To enable MAC-notification traps, use this command:

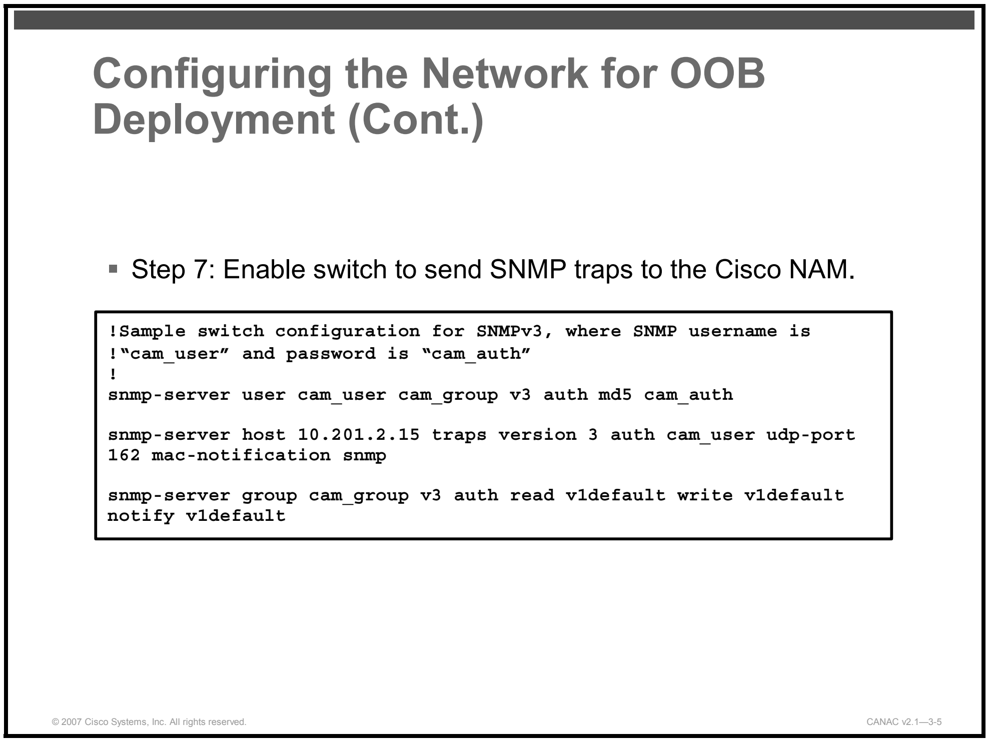
```
# snmp-server enable traps mac-notification
```

If MAC notification is not supported, enable linkup and linkdown traps using this command:

```
# snmp-server enable traps snmp linkup linkdown
```

Alternatively, you can simply enable all traps using this command:

```
# snmp-server enable traps
```



Configuring the Network for OOB Deployment (Cont.)

- Step 7: Enable switch to send SNMP traps to the Cisco NAM.

```
!Sample switch configuration for SNMPv3, where SNMP username is
!"cam_user" and password is "cam_auth"
!
snmp-server user cam_user cam_group v3 auth md5 cam_auth

snmp-server host 10.201.2.15 traps version 3 auth cam_user udp-port
162 mac-notification snmp

snmp-server group cam_group v3 auth read v1default write v1default
notify v1default
```

CANAC v2.1—3-5

Step 7 Enable the switch to send SNMP MAC notification and linkup traps to the Cisco NAM. The switch commands in the following examples depend on the SNMP version that is used in the SNMP trap settings in the Cisco NAM configuration:

- This example uses SNMPv1 with an SNMP community string "nam_v1":

```
# snmp-server host 10.201.2.15 traps version 1 nam_v1 udp-
port 162 mac-notification snmp
```

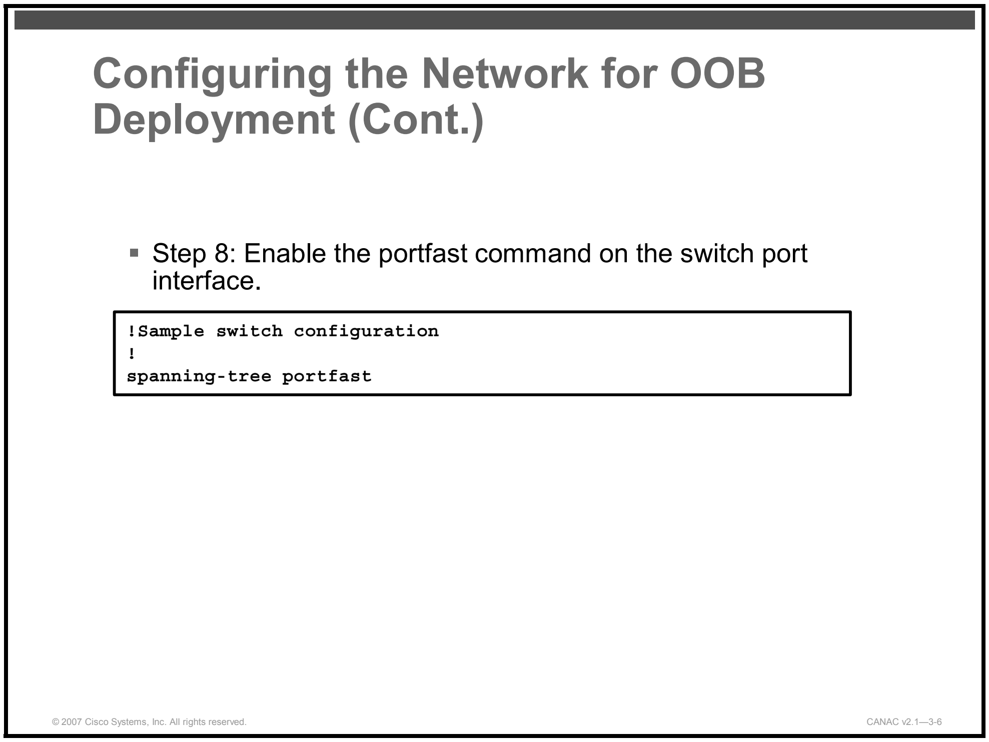
- This example uses SNMPv2c with an SNMP community string "nam_v2":

```
# snmp-server host 10.201.2.15 traps version 2c nam_v2 udp-
port 162 mac-notification snmp
```

- The following example uses SNMPv3 with an SNMP username and password "nam_user" and "nam_auth". The group command should be run after the user and host commands.

```
# snmp-server user nam_user nam_group V3 auth md5 nam_auth

# snmp-server host 10.201.2.15 traps version 3 auth
cam_user udp-port 162 mac-notification snmp

# snmp-server group nam_group V3 auth read v1default write
v1default notify v1default
```

Note For better security, you should use SNMPv3 and define ACLs to limit SNMP write access to the switch.



Configuring the Network for OOB Deployment (Cont.)

- Step 8: Enable the portfast command on the switch port interface.

```
!Sample switch configuration
!
spanning-tree portfast
```

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-6

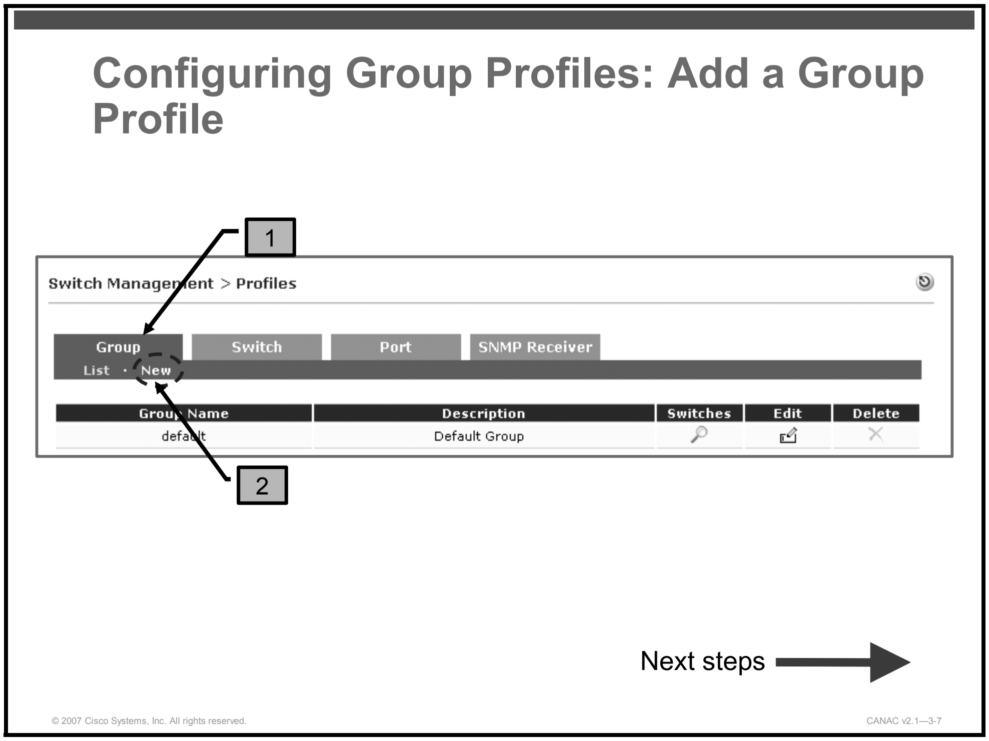
Step 8 Enter interface configuration mode and enable the **portfast** command to bring a port more quickly to a Spanning Tree Protocol (STP) forwarding state. Use this command:

```
# spanning-tree portfast
```

Note Enabling the STP feature on a port that is connected to a switch or hub could prevent STP from detecting and disabling loops in your network. Refer to your switch documentation for details.

Configuring Group Profiles

This topic describes how to configure group profiles on the Cisco NAM for out-of-band deployment.



Configuring Group Profiles: Add a Group Profile

Switch Management > Profiles

Group · Switch · Port · SNMP Receiver

List · New

Group Name	Description	Switches	Edit	Delete
default	Default Group	🔍	✎	✕

Next steps →

CANAC v2.1—3-7

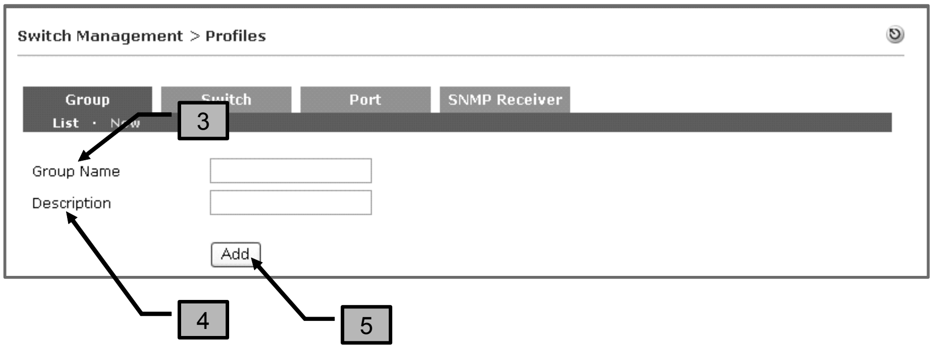
When you first add a switch to the Cisco NAM domain, a group profile is applied to the new switch. The figure shows a predefined group profile called “default.” All switches are automatically put in the default group when you add them. You can leave this default group profile setting, or you can create additional group profiles as needed. If you are adding and managing a large number of switches, creating multiple group profiles allows you to filter which sets of devices you want to display from the list of available switches.

To add a group profile, complete these steps:

Step 1 Choose **Switch Management > Profiles** and click the **Group** tab. The list of group profiles appears.

Step 2 Click the **New** link. The group profile Add form appears.

Configuring Group Profiles: Add a Group Profile (Cont.)



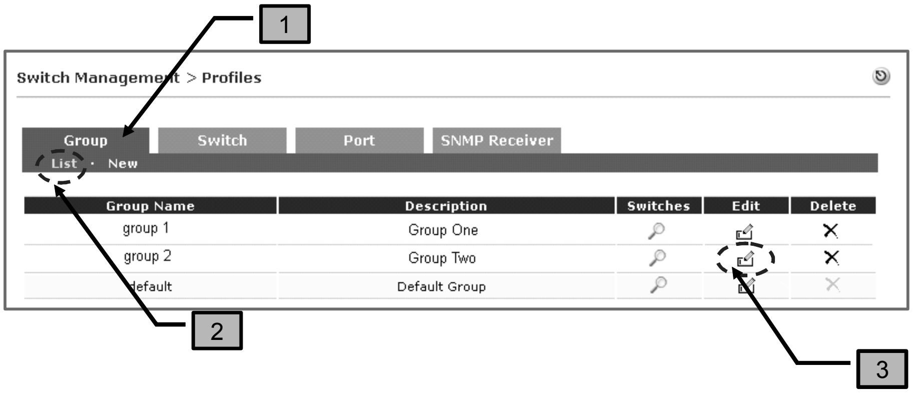
CANAC v2.1—3-8

Step 3 In the group profile Add form, enter a single word in the Group Name field. You can use digits and underscores, but no spaces.

Step 4 Enter an optional description in the Description field.

Step 5 Click **Add**. The new group profile appears under Switch Management > Profiles > Group > List. From the list, you can edit or delete the group profile.

Configuring Group Profiles: Edit a Group Profile



Switch Management > Profiles

Group | Switch | Port | SNMP Receiver

List · New

Group Name	Description	Switches	Edit	Delete
group 1	Group One	🔍	✎	✕
group 2	Group Two	🔍	✎	✕
default	Default Group	🔍	✎	✕

Next steps →

CANAC v2.1—3-9

After the switches are added, you can edit the group profile to change which switches are assigned to the group profile.

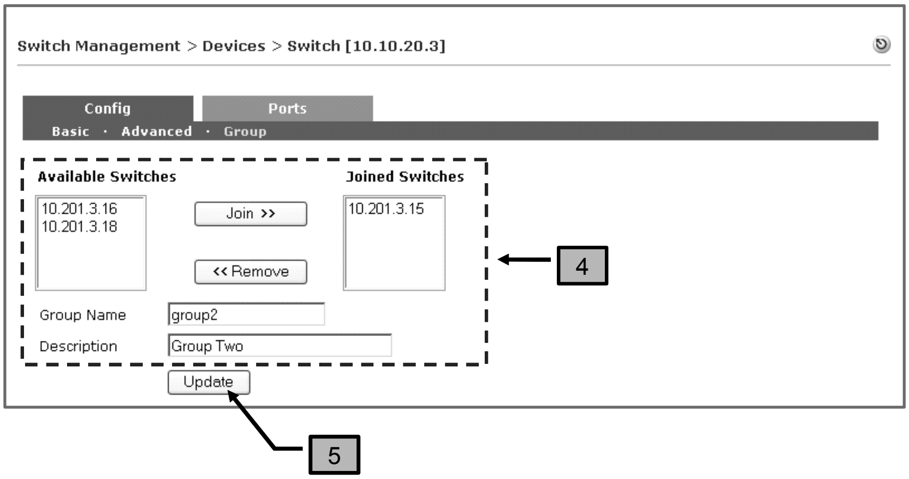
To edit a group profile after actual switches are added, complete these steps:

Step 1 Choose **Switch Management > Profiles** and click the **Group** tab.

Step 2 Click the **List** link. The page listing the defined group profiles appears.

Step 3 Click the **Edit** button next to the group profile that you want to edit. The Edit page appears.

Configuring Group Profiles: Edit a Group Profile (Cont.)



Switch Management > Devices > Switch [10.10.20.3]

Available Switches: 10.201.3.16, 10.201.3.18

Joined Switches: 10.201.3.15

Group Name: group2

Description: Group Two

CANAC v2.1—3-10

Step 4 You can toggle the switches that belong in the group profile by choosing the IP address of the switch from the Joined Switches or Available Switches columns and clicking the Join or Remove buttons as applicable. You can also edit the Group Name or Description.

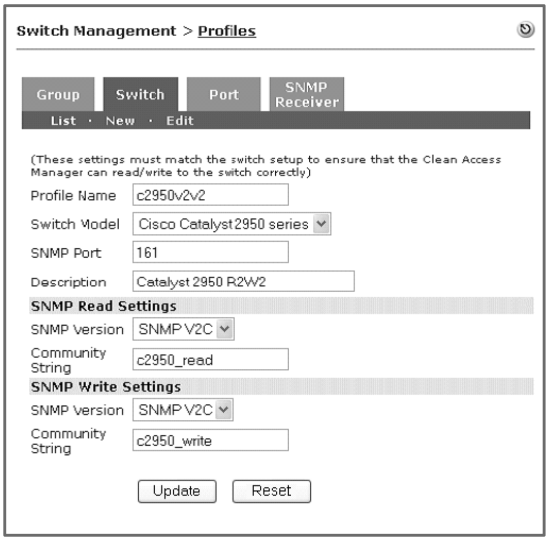
Step 5 Click the **Update** button to save your changes.

Note To delete a group profile, you must first remove the joined switches from the profile.

Configuring Switch Profiles

This topic describes how to configure switch profiles on the Cisco NAM for out-of-band deployment.

Configuring Switch Profiles: Example Switch Profile



(These settings must match the switch setup to ensure that the Clean Access Manager can read/write to the switch correctly)

Profile Name: c2950v2v2

Switch Model: Cisco Catalyst 2950 series

SNMP Port: 161

Description: Catalyst 2950 R2W2

SNMP Read Settings

SNMP Version: SNMP V2C

Community String: c2950_read

SNMP Write Settings

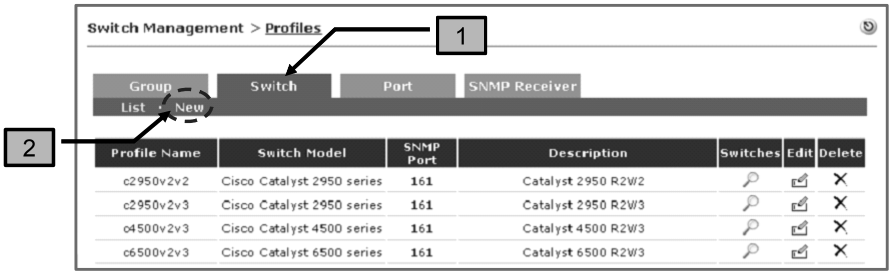
SNMP Version: SNMP V2C

Community String: c2950_write

CANAC v2.1—3-11

You must first create and apply a switch profile when you add a new switch. A switch profile classifies switches of the same model and with the same SNMP settings. The figure illustrates a switch profile defining Cisco Catalyst 2950 switches with the same SNMP settings: SNMPv2c with read community string “c2950_read” and write community string “c2950_write”.

Configuring Switch Profiles: Add a Switch Profile



Switch Management > Profiles

Group | Switch | Port | SNMP Receiver

List · New

Profile Name	Switch Model	SNMP Port	Description	Switches	Edit	Delete
c2950v2v2	Cisco Catalyst 2950 series	161	Catalyst 2950 R2W2	🔍	✎	✕
c2950v2v3	Cisco Catalyst 2950 series	161	Catalyst 2950 R2W3	🔍	✎	✕
c4500v2v3	Cisco Catalyst 4500 series	161	Catalyst 4500 R2W3	🔍	✎	✕
c6500v2v3	Cisco Catalyst 6500 series	161	Catalyst 6500 R2W3	🔍	✎	✕

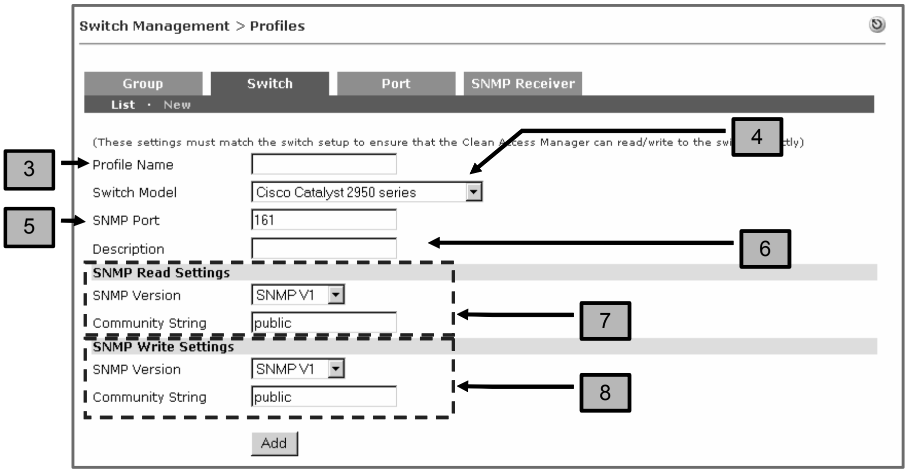
Next steps →

To add a switch profile, complete these steps:

Step 1 Choose **Switch Management > Profiles** and click the **Switch** tab. The list of defined switch profiles appears.

Step 2 Click the **New** link. The switch profile Add form appears.

Configuring Switch Profiles: Add a Switch Profile (Cont.)



Switch Management > Profiles

(These settings must match the switch setup to ensure that the Clean Access Manager can read/write to the sw tly)

Profile Name

Switch Model: Cisco Catalyst 2950 series

SNMP Port: 161

Description

SNMP Read Settings

SNMP Version: SNMP V1

Community String: public

SNMP Write Settings

SNMP Version: SNMP V1

Community String: public

CANAC v2.1—3-13

Step 3 In the Profile Name field, enter a single word profile name. You can use digits and underscores, but no spaces.

Tip You should enter a switch profile name that identifies the switch model and SNMP read and write versions; for example, “2950v2v3.”

Step 4 Choose the switch model for the profile from the Switch Model drop-down menu.

Step 5 In the SNMP Port field, enter the SNMP port number that is configured on the switch to send and receive traps. The default port is 161.

Step 6 Enter an optional description in the Description field.

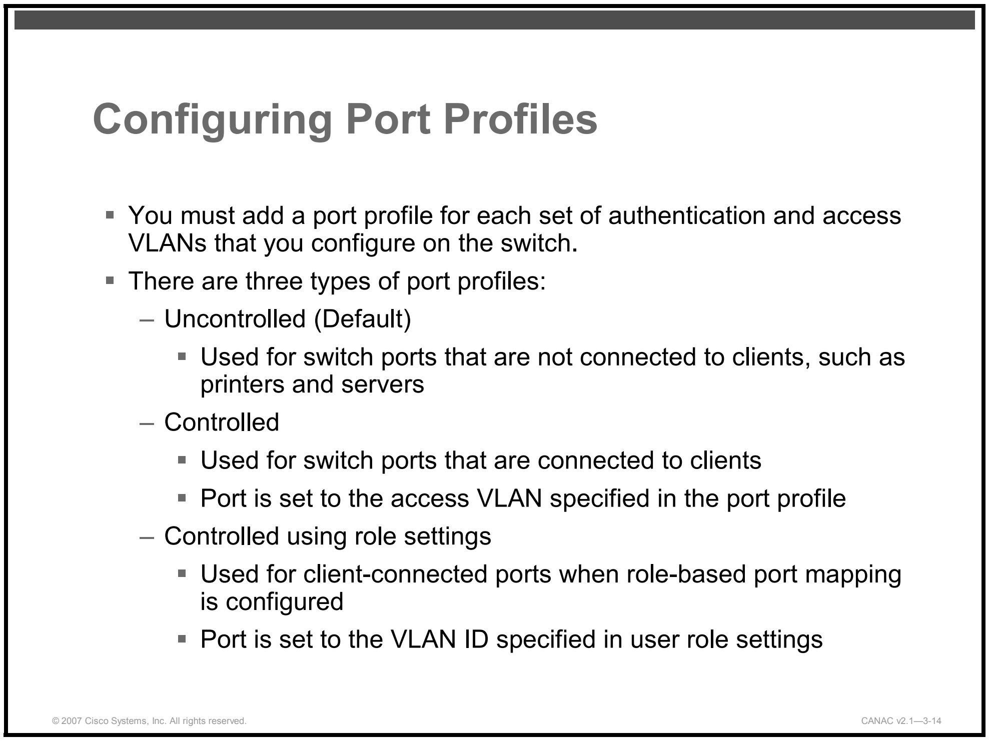
Step 7 Configure the SNMP Read Settings to match the settings on the switch.

Step 8 Configure the SNMP Write Settings to match the settings on the switch.

Step 9 Click the **Add** button to add the switch profile to the switch profiles list on the List page. From Switch Management > Profiles > Switch > List, you can view, modify, or delete the profile.

Configuring Port Profiles

This topic describes how to configure port profiles on the Cisco NAM for out-of-band deployment.



Configuring Port Profiles

- You must add a port profile for each set of authentication and access VLANs that you configure on the switch.
- There are three types of port profiles:
  - Uncontrolled (Default)
    - Used for switch ports that are not connected to clients, such as printers and servers
  - Controlled
    - Used for switch ports that are connected to clients
    - Port is set to the access VLAN specified in the port profile
  - Controlled using role settings
    - Used for client-connected ports when role-based port mapping is configured
    - Port is set to the VLAN ID specified in user role settings

CANAC v2.1—3-14

The port profile determines whether a port is managed or unmanaged and which authentication and access VLANs to use when switching the client port. You need to add a port profile for each set of authentication and access VLANs that you configure on the switch.

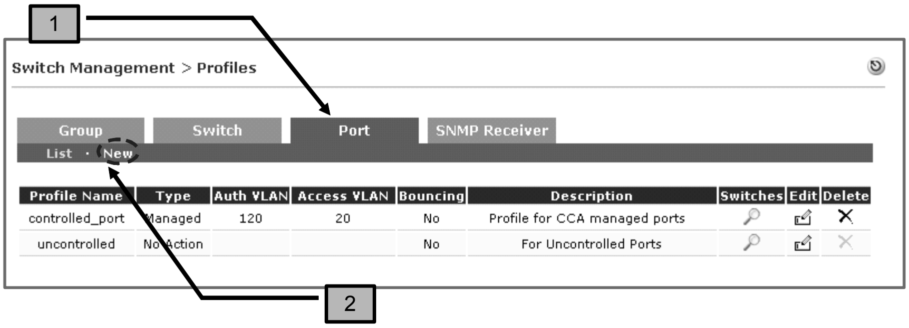
These are three types of port profiles for switch ports:

- **Uncontrolled:** Uncontrolled port profiles are used for switch ports that are not connected to clients (such as printers, servers, switches, and so on). The uncontrolled port profile is typically the default port profile.
- **Controlled:** Controlled port profiles are used for switch ports that are connected to clients.
- **Controlled using role settings:** A controlled port profile using role settings is used for switch ports that are connected to clients and to apply the VLAN ID from an existing user role.

Regular switch ports that are not connected to clients use the uncontrolled port profile. Client-connected switch ports use controlled profiles. When a client connects to a controlled port, the port is set to the authentication VLAN. After the client is authenticated and certified, the port is set to either the access VLAN specified in the port profile, the user role settings, or the initial VLAN.

In out-of-band real-IP gateway and out-of-band NAT gateway modes, the Cisco NAM enables port bouncing to help clients acquire a new IP address after successful authentication and certification. In out-of-band virtual gateway mode, port bouncing is not necessary because the client uses the same IP address after successful authentication and certification.

Configuring Port Profiles: Add a Port Profile



Profile Name	Type	Auth VLAN	Access VLAN	Bouncing	Description	Switches	Edit	Delete
controlled_port	Managed	120	20	No	Profile for CCA managed ports			✕
uncontrolled	No Action			No	For Uncontrolled Ports			✕

Next steps →

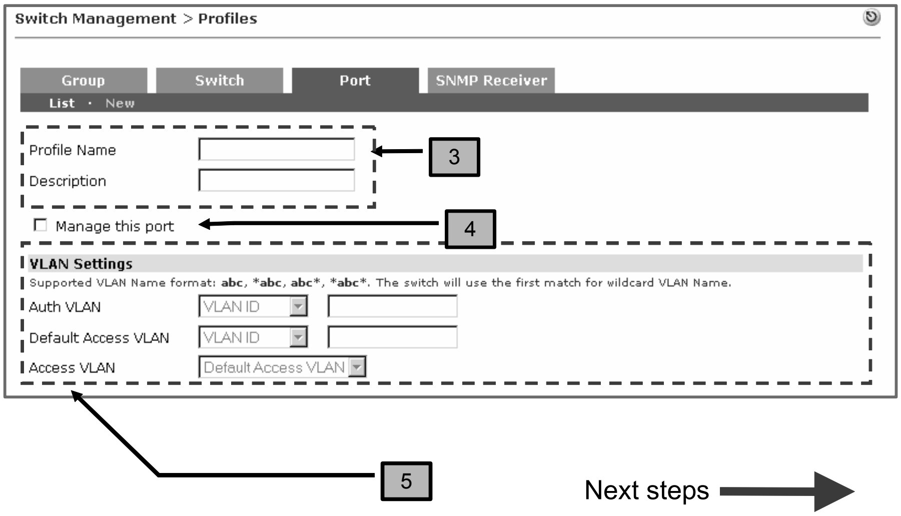
CANAC v2.1—3-15

To add a port profile, complete these steps:

Step 1 Choose **Switch Management > Profiles** and click the **Port** tab.

Step 2 Click the **New** link.

Configuring Port Profiles: Add a Port Profile (Cont.)



Switch Management > Profiles

Group | Switch | Port | SNMP Receiver

List · New

Profile Name

Description

□ Manage this port

VLAN Settings

Supported VLAN Name format: **abc**, ***abc**, **abc***, ***abc***. The switch will use the first match for wildcard VLAN Name.

Auth VLAN: VLAN ID

Default Access VLAN: VLAN ID

Access VLAN: Default Access VLAN

Next steps

CANAC v2.1—3-16

Step 3 Type a single word for the Profile Name. You can use digits and underscores, but no spaces. The name should reflect whether the Port profile is controlled or uncontrolled.

Type an optional Description for the Port profile.

Step 4 Click the check box for Manage this port to enable the configuration of this Port Profile.

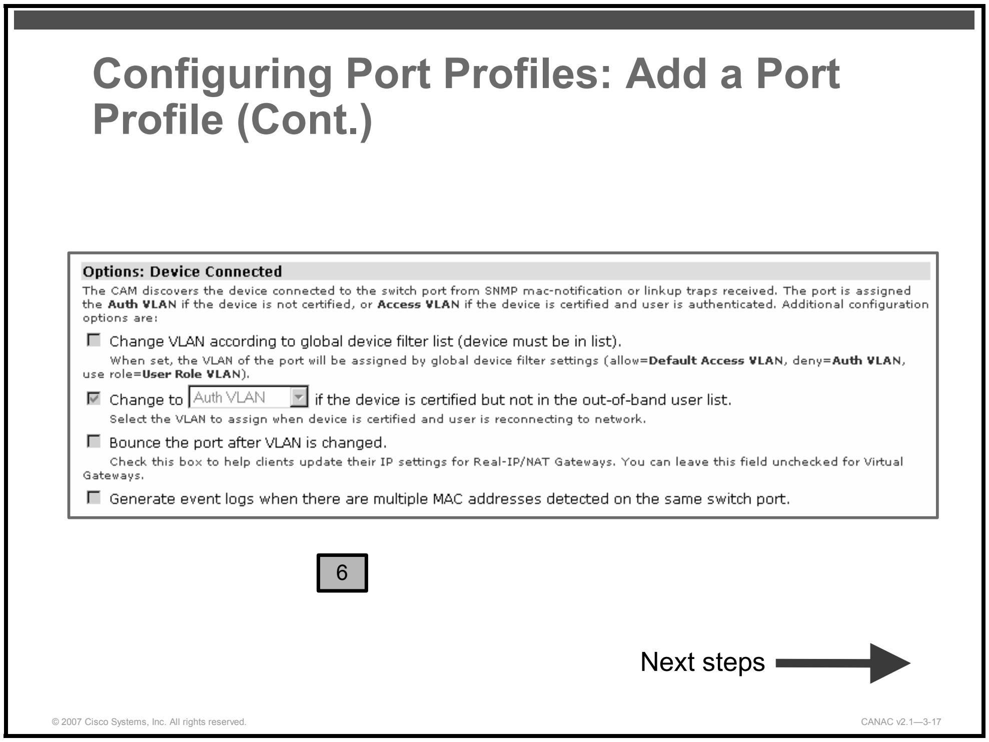
Step 5 Choose either VLAN ID (default) or VLAN Name from the Auth VLAN drop-down menu and type the authorization VLAN that you want to use for this port profile.

Choose either VLAN ID (default) or VLAN Name from the Default Access VLAN drop-down menu and type the default access VLAN that you want to use for this port profile.

From the Access VLAN drop-down menu, choose one of the following options:

- **Default Access VLAN:** The Cisco NAM will put authenticated users with certified devices on the default access VLAN that you specified in the Port Profile.
- **User Role VLAN:** The Cisco NAM will put authenticated users with certified devices on the access VLAN that you specified when you configured the unauthenticated user role.

- **Initial Port VLAN:** The Cisco NAM will put authenticated users with certified devices on the initial VLAN that you specified for the port in the Switch Management > Devices > Switch [IP address] > Ports page. The initial VLAN is the value that is saved by the Cisco NAM for the port when the switch is added. Instead of using a specified access VLAN, the client is switched from the initial port VLAN to an auth VLAN for authentication and certification and then switched back to the initial port VLAN when the client is certified.



Configuring Port Profiles: Add a Port Profile (Cont.)

Options: Device Connected

The CAM discovers the device connected to the switch port from SNMP mac-notification or linkup traps received. The port is assigned the **Auth VLAN** if the device is not certified, or **Access VLAN** if the device is certified and user is authenticated. Additional configuration options are:

☐ Change VLAN according to global device filter list (device must be in list).

When set, the VLAN of the port will be assigned by global device filter settings (allow=**Default Access VLAN**, deny=**Auth VLAN**, use role=**User Role VLAN**).

☑ Change to [Auth VLAN ▾] if the device is certified but not in the out-of-band user list.

Select the VLAN to assign when device is certified and user is reconnecting to network.

☐ Bounce the port after VLAN is changed.

Check this box to help clients update their IP settings for Real-IP/NAT Gateways. You can leave this field unchecked for Virtual Gateways.

☐ Generate event logs when there are multiple MAC addresses detected on the same switch port.

CANAC v2.1—3-17

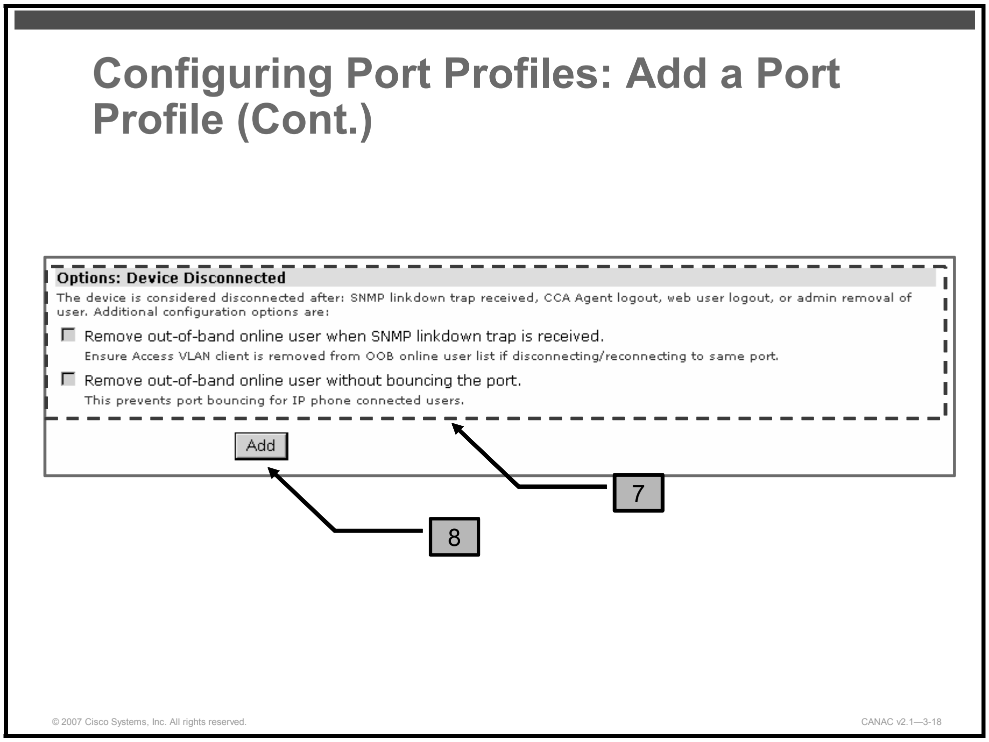
Step 6 The figure shows the middle part of the Port form. The Cisco NAM discovers the device connected to the switch port from SNMP MAC-notification or linkup traps received. The port is assigned the Auth VLAN if the device is not certified or Access VLAN if the device is certified, and the user is authenticated. The bottom part of the port profile form lets you configure the options on the port when devices are connected to the port. You can configure the following options:

- **Change VLAN according to global device filter list (device must be in list):** Check this check box if you want to use the Cisco NAM global Device Filter rules to set the VLAN of the port. You must have device filters added under Device Management > Filters > Devices for this feature to work.

Note Rules that are configured for MAC addresses on the global Device Filter list have the highest priority for user and device processing in both out-of-band and in-band deployments.

- **Change to [Auth VLAN | Access VLAN] if the device is certified, but not in the out-of-band user list:** This check box is automatically enabled when a port is managed.
- **Bounce the port after VLAN is changed:** Check this check box so the client machine will obtain a new IP address after the client machine is switched to the Access VLAN. For virtual gateways, leave this box unchecked.

- **Generate event logs when there are multiple MAC addresses detected on the same switch port:** Check this check box to generate event logs when multiple MAC addresses are found on the same switch port.



Configuring Port Profiles: Add a Port Profile (Cont.)

Options: Device Disconnected

The device is considered disconnected after: SNMP linkdown trap received, CCA Agent logout, web user logout, or admin removal of user. Additional configuration options are:

□ Remove out-of-band online user when SNMP linkdown trap is received.
Ensure Access VLAN client is removed from OOB online user list if disconnecting/reconnecting to same port.

□ Remove out-of-band online user without bouncing the port.
This prevents port bouncing for IP phone connected users.

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—3-18

Step 7 The figure shows the bottom part of the Port form, which provides port profile options for a device that is disconnected from a port. A device is considered disconnected after one of these events:

- SNMP linkdown trap received
- User logs out using Cisco NAA
- User performs a web logout
- Administrator removes user

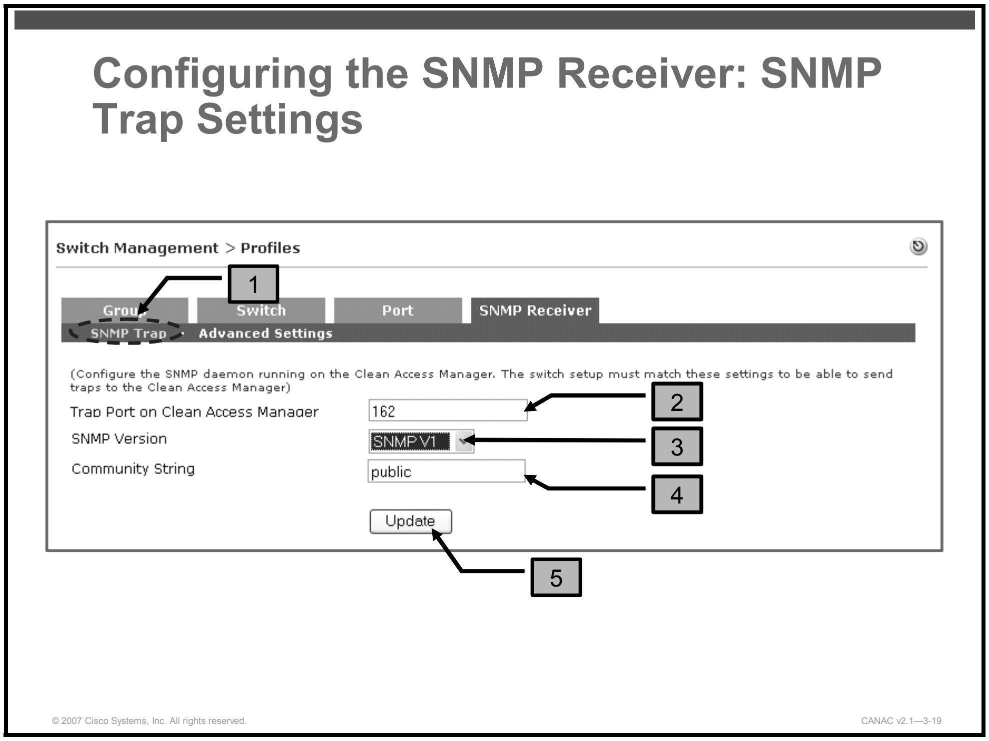
You can configure these options:

- **Remove out-of-band online user when SNMP linkdown trap is received:** Check this check box to ensure that a client on the access VLAN is removed from the out-of-band online user list when disconnecting or reconnecting to the same port.
- **Remove out-of-band online user without bouncing the port:** Check this check box if you need to prevent bouncing of a switch port when a client machine is connected to the switch port through a VoIP phone. Use this feature when you need the Cisco NAC Appliance to provide NAC for a client machine without affecting the operation of a VoIP phone connected to the switch port. When this option is checked for out-of-band virtual gateways, the client port is not bounced when users are removed from the Out-of-Band Online Users List or when devices are removed from the Certified Devices list. Instead, the port access VLAN is changed to the authenticated VLAN.

Step 8 Click **Add** to add the port profile. The new profile appears on the Switch Management > Profiles > Port > List page. From this page, you can view, modify, or delete the profile.

Configuring the SNMP Receiver

This topic describes how to configure the SNMP receiver on the Cisco NAM for out-of-band deployment.



Configuring the SNMP Receiver: SNMP Trap Settings

Switch Management > Profiles

(Configure the SNMP daemon running on the Clean Access Manager. The switch setup must match these settings to be able to send traps to the Clean Access Manager)

Trap Port on Clean Access Manager: 162

SNMP Version: SNMP V1

Community String: public

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-19

Settings in the SNMP Receiver tab configure the SNMP receiver that is running on the Cisco NAM. The SNMP receiver receives MAC notification or linkup SNMP trap notifications from the controlled switches and sets the VLAN on the corresponding switch ports. The configuration on the switch must match the SNMP receiver settings to be able to send traps to the Cisco NAM.

To configure the SNMP receiver module on the Cisco NAM, complete these steps:

Step 1 Choose the **Switch Management** > **Profiles** > **SNMP Receiver** tab and click the **SNMP Trap** link.

Step 2 In the Trap Port on Clean Access Manager field, enter the port number that you want to use as the trap port on the Cisco NAM. The default port number is 162.

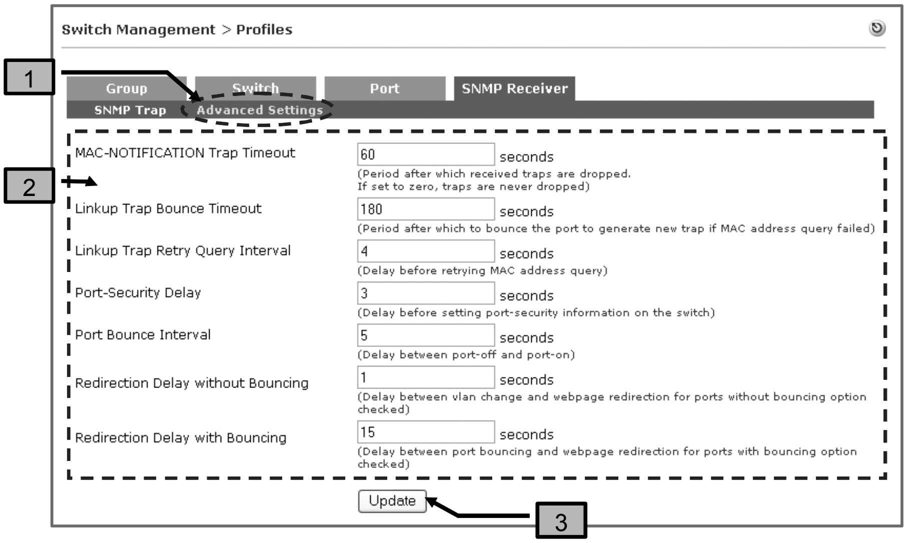
Step 3 From the SNMP Version drop-down menu, choose the appropriate SNMP version: SNMP V1, SNMP V2, or SNMP V3.

Step 4 Depending on which SNMP version you choose, the remaining settings appear. If you choose SNMP V1 or SNMP V2c, enter the community string of the SNMP receiver in the Community String field. If you choose SNMP V3, you have three fields to populate:

- From the Security Method drop-down menu, choose one of the available methods: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES-CBC), or AuthPriv(SHA+DES-CBC).
- In the User Name field, enter the SNMP user name.
- In the User Auth field and in the User Priv field, enter the authentication and encryption algorithm available for each user to use.

Step 5 Click **Update** to save your settings.

Configuring the SNMP Receiver: Advanced Settings



MAC-NOTIFICATION Trap Timeout: 60 seconds
(Period after which received traps are dropped. If set to zero, traps are never dropped)

Linkup Trap Bounce Timeout: 180 seconds
(Period after which to bounce the port to generate new trap if MAC address query failed)

Linkup Trap Retry Query Interval: 4 seconds
(Delay before retrying MAC address query)

Port-Security Delay: 3 seconds
(Delay before setting port-security information on the switch)

Port Bounce Interval: 5 seconds
(Delay between port-off and port-on)

Redirection Delay without Bouncing: 1 seconds
(Delay between vlan change and webpage redirection for ports without bouncing option checked)

Redirection Delay with Bouncing: 15 seconds
(Delay between port bouncing and webpage redirection for ports with bouncing option checked)

CANAC v2.1—3-20

The SNMP Receiver > Advance Settings page configures advanced timeout and delay settings for the SNMP traps that are received and sent by the Cisco NAM.

To change the default settings, complete these steps:

Step 1 Choose the **Switch Management > Profiles > SNMP Receiver** tab and click the **Advanced Settings** link.

Step 2 Configure the advanced settings that you want to change:

- In the MAC-Notification Trap Timeout field, enter a timeout value in seconds (default is 60 seconds). If the time difference between the timestamp of a MAC-notification trap and the current time is greater than the setting in this field, the trap is dropped.
- In the Linkup Trap Bounce Timeout field, enter a timeout value in seconds (default is 180 seconds). When the Cisco NAM receives a linkup trap, the Cisco NAM tries to resolve the MAC address that is connected to the port. If the Cisco NAM cannot obtain the MAC address within the time interval specified in this field, the Cisco NAM bounces the port to force the switch to generate a new linkup trap.
- In the Linkup Trap Retry Query Interval field, enter a timeout value in seconds (default is 4 seconds). When the Cisco NAM receives a linkup trap, it queries the switch for the MAC address that is connected to the port. If the MAC address is not yet available, the Cisco NAM first waits the number of seconds specified in this field and then tries again.
- In the Port-Security Delay field, enter a timeout value in seconds (default is 3 seconds). If port security is enabled on the switch, after the VLAN is switched, the Cisco NAM must wait the number of seconds specified in this field before setting the port security information on the switch.

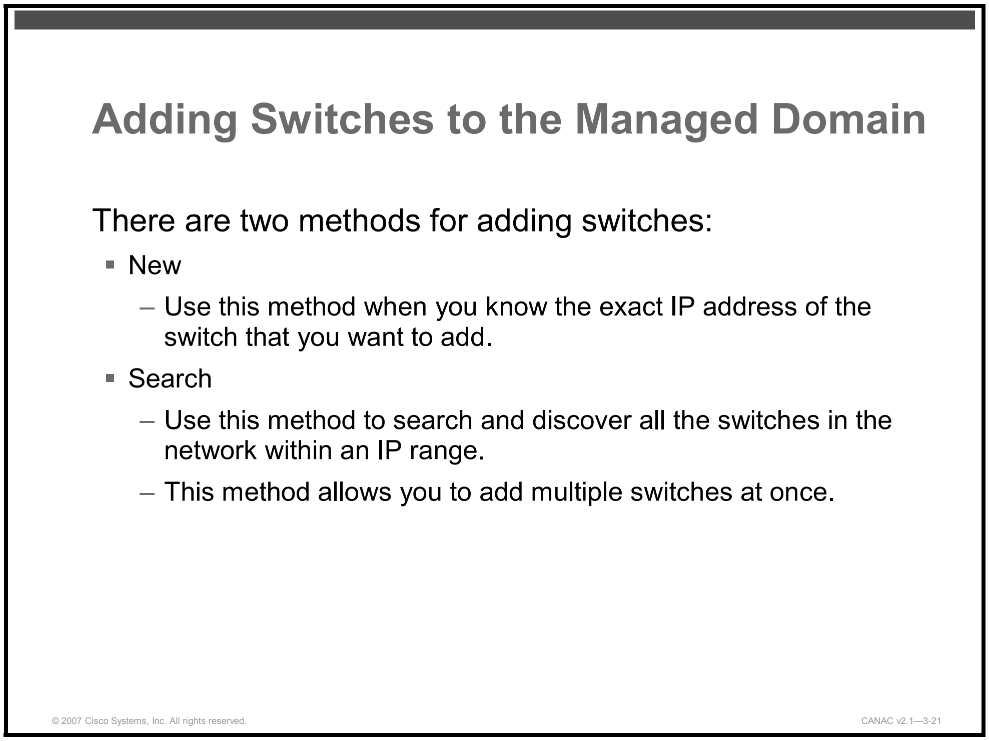
- In the Port Bounce Interval field, enter a timeout value in seconds (default is 5 seconds). The port bounce interval is the time delay between turning off and turning on the port. This delay is inserted to help client machines issue DHCP requests.

Step 3 Click **Update** to save settings.

Note For more detailed information on the SNMP receiver settings, see the Advanced Setting section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Adding Switches to the Managed Domain

This topic describes how to add switches to the Cisco NAM managed domain for out-of-band deployment.



Adding Switches to the Managed Domain

There are two methods for adding switches:

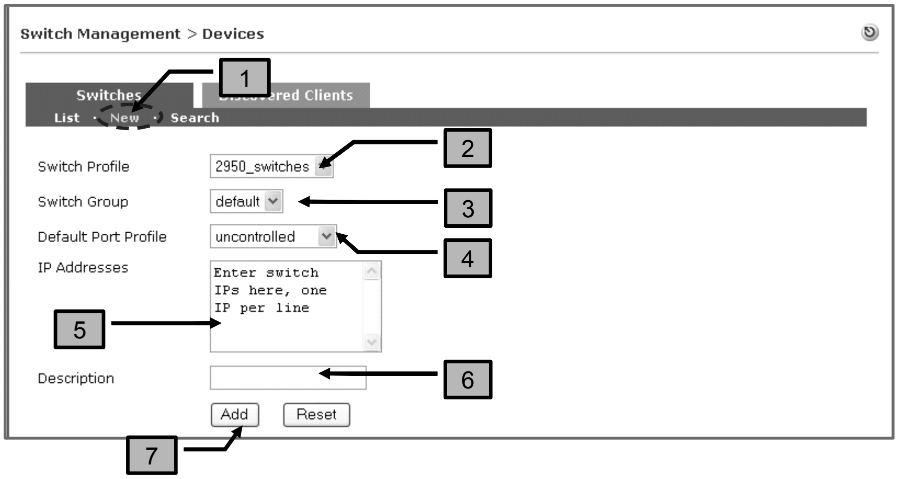
- New
  - Use this method when you know the exact IP address of the switch that you want to add.
- Search
  - Use this method to search and discover all the switches in the network within an IP range.
  - This method allows you to add multiple switches at once.

CANAC v2.1—3-21

The pages under the Switch Management > Devices > Switches tab are used to discover and add new controlled switches within an IP range, to add new controlled switches by exact IP address, and to manage the list of controlled switches. There are two methods to add new controlled switches:

- Use the New form to add a switch by specifying the switch IP address.
- Use the Search form to allow the Cisco NAM to discover the switches in the network.

Adding Switches to the Managed Domain: Add a Controlled Switch



Switch Management > Devices

CANAC v2.1—3-22

The New page allows you to add switches when exact IP addresses are already known. To add a controlled switch using the New page, complete these steps:

Step 1 Choose **Switch Management > Devices > Switches** and click the **New** link.

Step 2 From the Switch Profile drop-down menu, choose the switch profile that you want to apply to the switches that will be added.

Step 3 From the Switch Group drop-down menu, choose the group profile to apply to the switches that will be added.

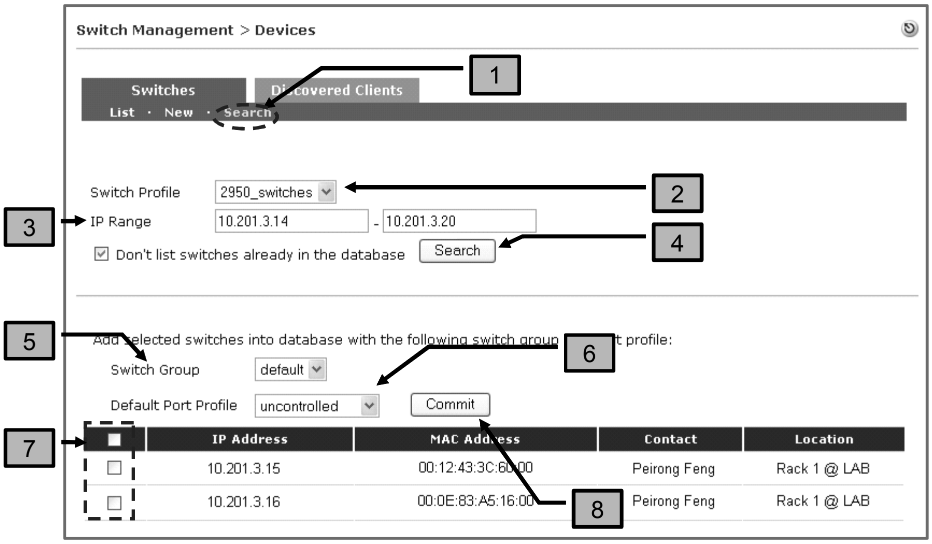
Step 4 From the Default Port Profile drop-down menu, choose the default port profile to apply to the ports of the switches that will be added. Typically, the default port profile should be uncontrolled.

Step 5 In the IP Addresses field, enter the IP addresses of the switches that you want to add. Enter each IP address on a separate line.

Step 6 In the Description field, enter an optional description for the new switch.

Step 7 Click the **Add** button to add the switch.

Adding Switches to the Managed Domain: Search and Add an Uncontrolled Switch



Switch Management > Devices

Switch Profile: 2950_switches
IP Range: 10.201.3.14 - 10.201.3.20
☑ Don't list switches already in the database [Search]

Add selected switches into database with the following switch group and port profile:
Switch Group: default
Default Port Profile: uncontrolled [Commit]

□	IP Address	MAC Address	Contact	Location
□	10.201.3.15	00:12:43:3C:60:00	Peirong Feng	Rack 1 @ LAB
□	10.201.3.16	00:0E:83:A5:16:00	Peirong Feng	Rack 1 @ LAB

CANAC v2.1—3-23

The Search page allows you to discover uncontrolled switches within an IP range and add them to the managed domain so that they will become controlled switches. To add switches from the Search page, complete these steps:

Step 1 Choose the **Switch Management** > **Devices** > **Switches** tab and click the **Search** link.

Step 2 Select a profile from the Switch Profile drop-down menu. The read community string of the selected switch profile is used to find switches with matching read settings.

Step 3 Enter an IP range in the IP Range text boxes. The maximum IP search range is 256 IP addresses.

Step 4 Click the **Search** button to begin the search.

Note By default, the Don’t list switches already in the database check box is checked. If you uncheck this box, the resulting search will include switches that you have already added. However, the check boxes to the left of each entry will be disabled for switches that are already managed.

The Cisco NAM searches for uncontrolled switches in the network and lists them at the bottom of the page.

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

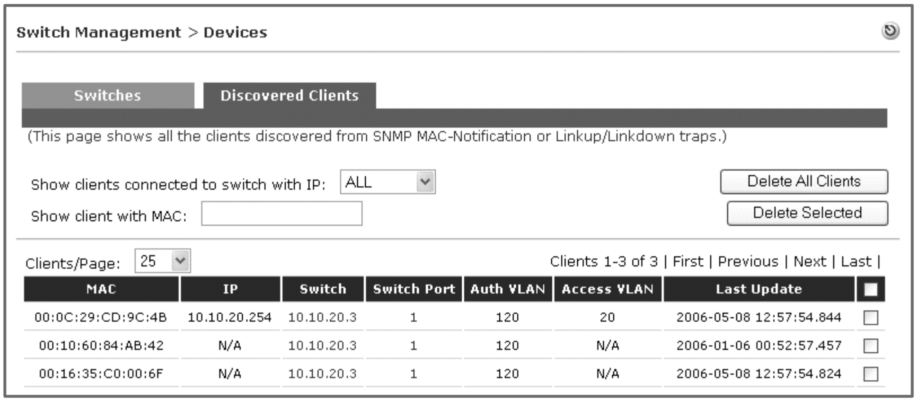
Step 5 From the Switch Group drop-down menu, choose the group profile that you want to apply to the uncontrolled switches that were found in the search.

Step 6 From the Default Port Profile drop-down menu, choose the default port profile that you want to apply to the uncontrolled switches that were found in the search.

Step 7 Check the check box to the left of each uncontrolled switch that you want to manage through the Cisco NAM. Alternatively, you can check the check box at the top of the column to add all uncontrolled switches that were found in the search.

Step 8 Click the **Commit** button to add the new switches to the managed domain. The new switches appear on the list of switches on the Switch Management > Devices > Switches > List page.

View Discovered Clients



Switch Management > Devices

(This page shows all the clients discovered from SNMP MAC-Notification or Linkup/Linkdown traps.)

Show clients connected to switch with IP: ALL

Show client with MAC:

Clients/Page: 25

Clients 1-3 of 3 | First | Previous | Next | Last |

MAC	IP	Switch	Switch Port	Auth VLAN	Access VLAN	Last Update	□
00:0C:29:CD:9C:4B	10.10.20.254	10.10.20.3	1	120	20	2006-05-08 12:57:54.844	□
00:10:60:84:AB:42	N/A	10.10.20.3	1	120	N/A	2006-01-06 00:52:57.457	□
00:16:35:C0:00:6F	N/A	10.10.20.3	1	120	N/A	2006-05-08 12:57:54.824	□

The figure shows the Switch Management > Devices > Discovered Clients page. This page lists all clients discovered by the Cisco NAM via SNMP MAC notification and linkup or linkdown traps. The page records the activities of out-of-band clients (regardless of VLAN) based on the SNMP trap information that the Cisco NAM receives.

When a client connects to a port on the authentication VLAN, a trap is sent and the Cisco NAM creates an entry on the Discovered Clients page. The Cisco NAM adds a client MAC address, originating switch IP address, and switch port number to the out-of-band discovered clients list after receiving SNMP trap information for the client from the switch. Subsequently, the Cisco NAM updates the entry as it receives new SNMP trap information for the client.

Removing an entry from the discovered clients list clears the status information for the out-of-band client from the Cisco NAM.

Note An entry must exist in the discovered clients list for the Cisco NAM to determine which switch port VLAN will be changed. If the user is logging in at the same time that an entry in the discovered clients list is deleted, the Cisco NAM will not be able to detect the switch port.

The Switch Management > Devices > Discovered Clients page provides several viewing options:

- In the Show Clients Connected to Switch with IP field, leave the default ALL displayed, or choose a specific switch from the drop-down menu. The menu will be populated with all the controlled switches that are in the system.
- In the Show Client with MAC field, enter a specific MAC address and press **Enter** to display a particular client.
- In the Clients/Page drop-down menu, leave the default of 25 entries displayed per page, or choose from the drop-down menu to display 50, 100, 200, or ALL entries on the page.

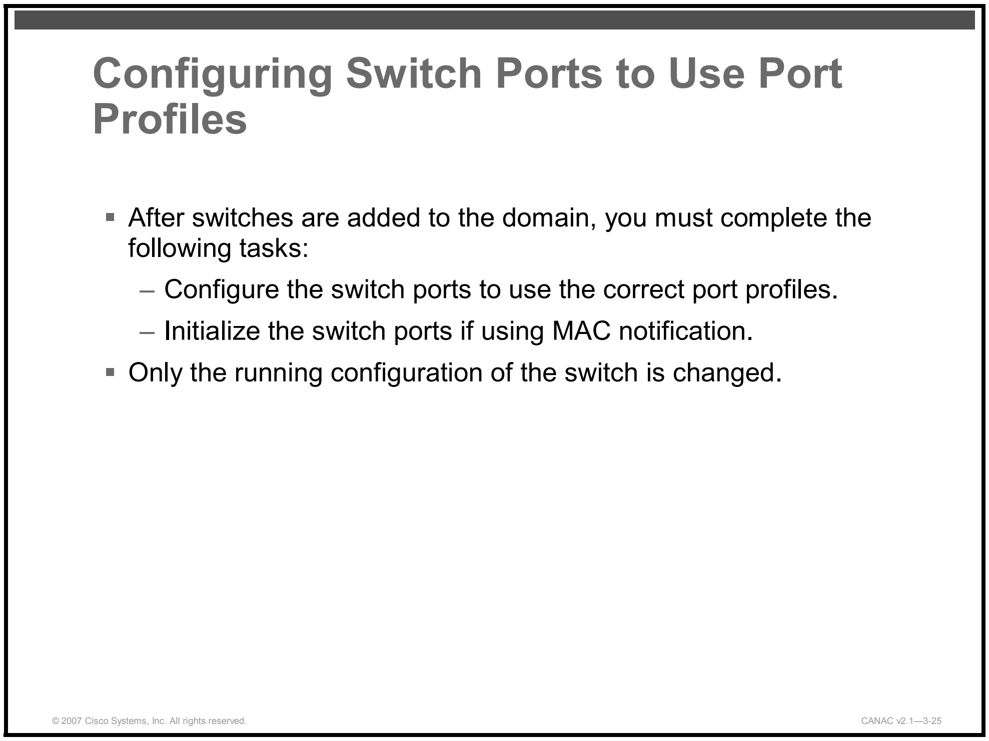
- The Delete All Clients button removes all clients from the list.
- The Delete Selected button removes only the clients that you select in the check column on the right-hand side of the page.

You can click any of the following column headings to sort results by that column:

- **MAC:** Sorts by the MAC address of a discovered client.
- **IP:** Sorts by the IP address of the client.
- **Switch:** Sorts by the IP of the originating controlled switch. Clicking the IP address brings up the Switch Management > Devices > Switch [IP Address] > Config > Basic page for the switch.
- **Switch Port:** Sorts by the switch port of the client. Clicking the port number brings up the Switch Management > Devices > Switch [IP address] > Ports configuration page for the switch.
- **Auth VLAN:** Sorts by the authentication (quarantine) VLAN of the client.
- **Access VLAN:** Sorts by the access VLAN of the client.
- **Last Update:** Sorts by the last time the Cisco NAM updated the information of the entry, beginning with the most recently updated entry at the top of the list.

Configuring Switch Ports to Use Port Profiles

This topic describes how to configure switch ports to use the Cisco NAM port profiles for out-of-band deployment.



Configuring Switch Ports to Use Port Profiles

- After switches are added to the domain, you must complete the following tasks:
  - Configure the switch ports to use the correct port profiles.
  - Initialize the switch ports if using MAC notification.
- Only the running configuration of the switch is changed.

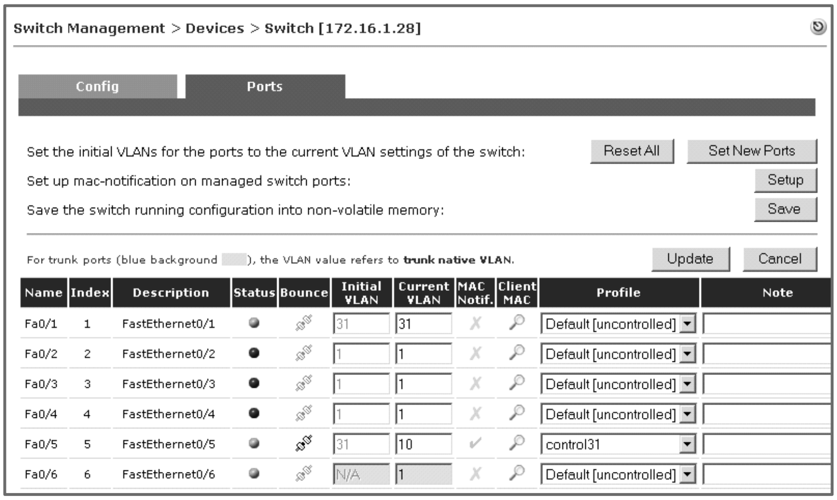
© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—3-25

Switch ports typically use the uncontrolled port profile if they are not connected to clients. Switch ports that are connected to clients use controlled port profiles. After configuring the switch ports, save the settings by clicking the **Update** button on the Switch Management > Devices > Switch [IP address] > Ports page. You must initialize the switch ports by clicking the **Update Switch Running Configuration** button on the Switch Management > Devices > Switch [IP address] > Ports page, but only when the switch supports MAC notification.

Note Only the running configuration of the switch, not the stored configuration, is changed by clicking the **Update Switch Running Configuration** button.

Caution Do not save the running configuration of the switch while the Cisco NAS is active. If the Cisco NAS fails and you need to provide client access to the Internet, the switch will not be able to revert to its baseline configuration.

Configuring Switch Ports to Use Port Profiles: View Switch Ports



Switch Management > Devices > Switch [172.16.1.28]

Set the initial VLANs for the ports to the current VLAN settings of the switch: Reset All | Set New Ports

Set up mac-notification on managed switch ports: Setup

Save the switch running configuration into non-volatile memory: Save

For trunk ports (blue background), the VLAN value refers to **trunk native VLAN**.

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	MAC Notif.	Client MAC	Profile	Note
Fa0/1	1	FastEthernet0/1	●		31	31	✗		Default [uncontrolled]	
Fa0/2	2	FastEthernet0/2	●		1	1	✗		Default [uncontrolled]	
Fa0/3	3	FastEthernet0/3	●		1	1	✗		Default [uncontrolled]	
Fa0/4	4	FastEthernet0/4	●		1	1	✗		Default [uncontrolled]	
Fa0/5	5	FastEthernet0/5	●		31	10	✓		control31	
Fa0/6	6	FastEthernet0/6	●		N/A	1	✗		Default [uncontrolled]	

CANAC v2.1—3-26

The Ports and Config tabs appear only after a switch is added to the Switch Management > Devices > Switch [IP address] list. When the Ports tab first appears, one entry per Ethernet port appears, and corresponding fields for the Ethernet port entry are populated according to the information that the Cisco NAM receives from direct SNMP queries. For example, if a switch that is added to the Cisco NAM has 24 Fast Ethernet ports and 2 Gigabit Ethernet uplinks, the Ports tab will display 26 rows to accommodate one entry per port.

Additionally, if the switch does not support MAC-notification traps, the MAC Notification column and Update Switch Running Configuration button do not appear on the page. When a switch does not support MAC notification, linkup or linkdown traps must be supported and configured on the switch and configured on the Cisco NAM.

At the top of the form, you can reset all the ports or just the new ports from the initial VLANs for the ports to the current VLAN setting of the switch. You can also set up MAC notification on the managed switch and save the configuration running on the switch to the nonvolatile (flash) memory.

Note For more detailed information about the switch ports, refer to the Ports Tab section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide.*

The Ports page displays these columns:

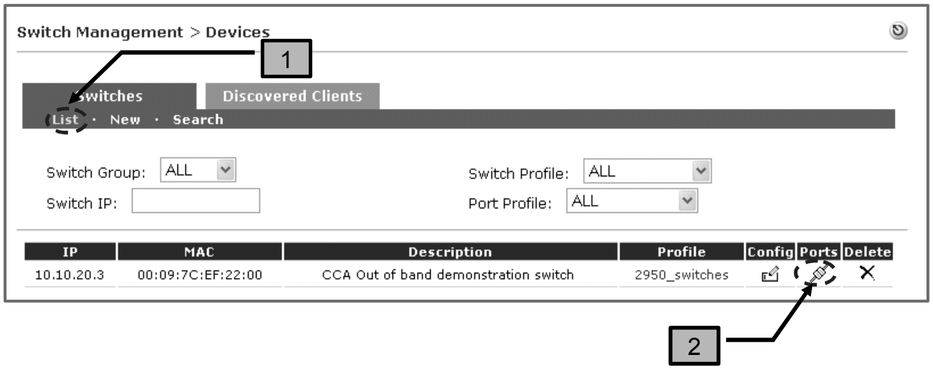
- **Name:** This column lists the port name for Cisco switches; for example, Fa0/1, Fa0/24, Gi0/1, and Gi0/21.
- **Index:** This column lists the port number on the switch; for example, 1, 24, 25, and 26.
- **Description:** This column lists the type of port; for example, FastEthernet0/1, FastEthernet0/24, GigabitEthernet0/1, and GigabitEthernet0/2.

- **Status:** This column lists the connection status of the port:
  - A green button indicates that a device is connected to the port.
  - A red button means that no device is connected to the port.
- **Bounce:** Clicking the Bounce icon in this column bounces an initialized, controlled port. You will see a confirmation dialog box before the port is bounced.

Note The Bounce button is only available for controlled ports. A port that is connected but not controlled cannot be bounced. By default, this feature is disabled for trunk ports.

- **Initial VLAN:** This column lists the initial VLAN value for the port that was saved by the Cisco NAM.
- **Current VLAN:** This column lists the current VLAN value for the port.
- **MAC Notification:** This column indicates MAC notification capability. The presence of this column indicates that the switch supports the proprietary SNMP MAC-notification trap. The following icons appear in the column:
  - A green check in the MAC Notification column means that the corresponding port on the switch is enabled for this trap.
  - A grey “x” means that either the port has not been enabled for this trap or that the port is not controlled.
  - A red exclamation point (!) means that an inconsistency exists between the port configuration on the switch and the port configuration in the Cisco NAM.
- **Client MAC:** This column provides a button that you can click to bring up a dialog box that displays the MAC address of the client that is attached to this port, the IP address of the switch, and the name of the port that the client is connected to.
- **Profile:** This column provides a drop-down menu for each switch port and is used to assign the appropriate port profile to the port.
- **Note:** This field allows you enter an optional description for the ports that you configure.

Configuring Switch Ports to Use Port Profiles to Configure a Port



Switch Group: ALL

Switch IP:

Switch Profile: ALL

Port Profile: ALL

IP	MAC	Description	Profile	Config	Ports	Delete
10.10.20.3	00:09:7C:EF:22:00	CCA Out of band demonstration switch	2950_switches			×

Next steps →

© 2007 Cisco Systems, Inc. All rights reserved.

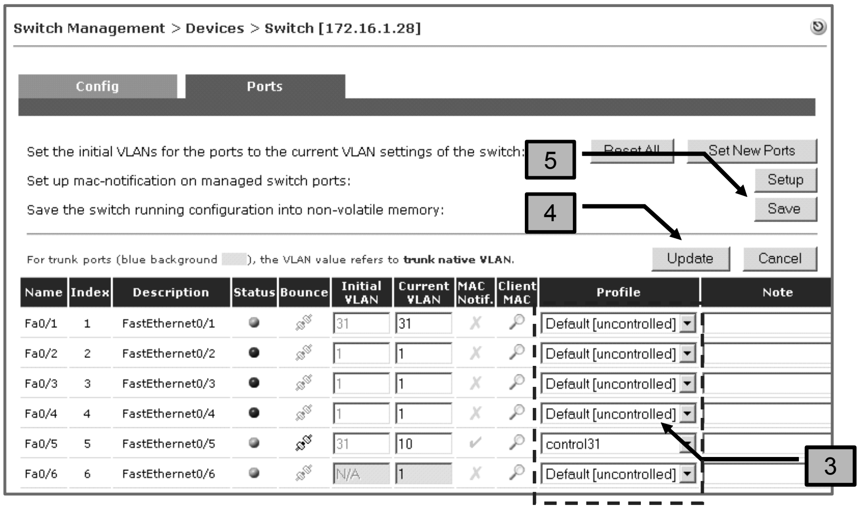
CANAC v2.1—3-27

To configure the ports on the switch, complete these steps:

Step 1 Choose **Switch Management** > **Devices** > **Switches** and then click the **List** link. The list of switches appears.

Step 2 From the list, click the **Ports** button for the switch that you want to configure. The port configuration form appears.

Configuring Switch Ports to Use Port Profiles to Configure a Port (Cont.)



Switch Management > Devices > Switch [172.16.1.28]

Config | Ports

Set the initial VLANs for the ports to the current VLAN settings of the switch: Reset All | Set New Ports

Set up mac-notification on managed switch ports: Setup

Save the switch running configuration into non-volatile memory: Save

For trunk ports (blue background), the VLAN value refers to **trunk native VLAN**. Update | Cancel

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	MAC Notif.	Client MAC	Profile	Note
Fa0/1	1	FastEthernet0/1	●		31	31	✗	🔍	Default [uncontrolled]	
Fa0/2	2	FastEthernet0/2	●		1	1	✗	🔍	Default [uncontrolled]	
Fa0/3	3	FastEthernet0/3	●		1	1	✗	🔍	Default [uncontrolled]	
Fa0/4	4	FastEthernet0/4	●		1	1	✗	🔍	Default [uncontrolled]	
Fa0/5	5	FastEthernet0/5	●		31	10	✓	🔍	control31	
Fa0/6	6	FastEthernet0/6	●		N/A	1	✗	🔍	Default [uncontrolled]	

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—3-28

Step 3 For each port that you want to configure, choose the port profile that you want to assign to this port from the Profile drop-down menu.

Note Each Profile drop-down menu contains all the port profiles that are configured in the system, the system default uncontrolled port profile, and the designated default profile. The Default[port profile name] designation specifies which port profile to apply by default to all unconfigured (uninitialized) ports. Typically, the default profile is Default[uncontrolled] and should be applied to all ports on the switch that do not have clients attached. In general, apply controlled port profiles to ports that clients are attached to in order to access and set the SNMP traps from those ports. All other ports should be uncontrolled.

Step 4 After you configure controlled ports by choosing the applicable port profile, click the **Update** button to save these settings on the Cisco NAM.

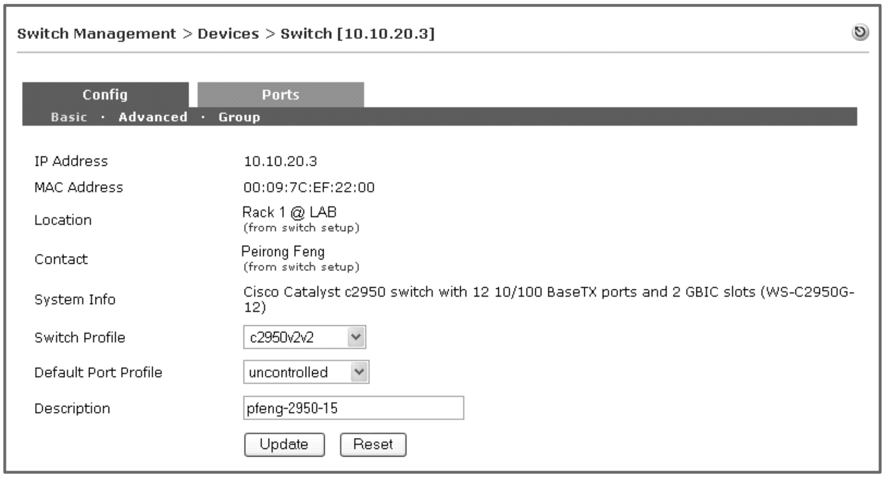
Step 5 Click the **Update Switch Running Configuration** button to set these configuration values on the switch.

Note Clicking the Update Switch Running Configuration button saves the running configuration of the switch. To save the stored configuration of the switch, you must connect directly to the switch by console, by Telnet, or by another method and perform a **save** command. You will see a confirmation dialog box before the ports are initialized.

Managing Switch Configuration Settings

This topic describes how to manage the switch configuration settings for out-of-band deployment.

Managing Switch Configuration Settings: Basic



Switch Management > Devices > Switch [10.10.20.3]

IP Address	10.10.20.3
MAC Address	00:09:7C:EF:22:00
Location	Rack 1 @ LAB (from switch setup)
Contact	Peirong Feng (from switch setup)
System Info	Cisco Catalyst c2950 switch with 12 10/100 BaseTX ports and 2 GBIC slots (WS-C2950G-12)
Switch Profile	c2950v2v2
Default Port Profile	uncontrolled
Description	pfeng-2950-15

Under the Switch Management > Devices > Switch [IP address] > Config tab, you can modify basic, advanced, and group profile settings for a particular switch.

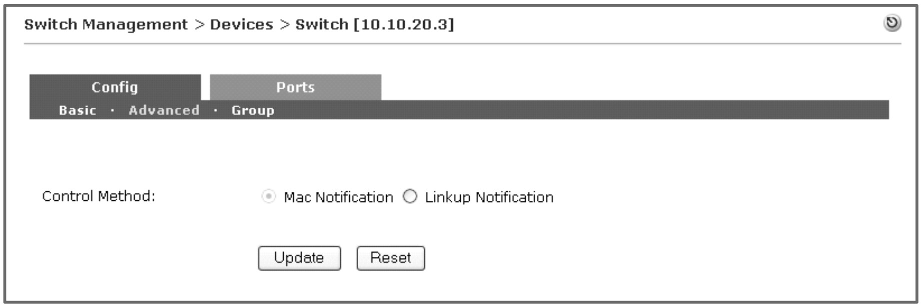
Note You can access the Config tab by clicking the Config button beside a switch listed on the Switch Management > Devices > Switch [IP address] page. The top banner of the GUI stays, and the central part of the screen becomes the Config tab shown in the figure.

The Config > Basic page shows the following values that have been configured for the switch:

- The first five values are obtained from the initial configuration that you performed on the switch itself:
  - — IP Address
  - — MAC Address
  - — Location
  - — Contact
  - — System Info (translated from the MIB for the switch)

- **Switch Profile:** This drop-down menu shows the switch profile that you are using for the switch that was configured under Switch Management > Profiles > Switch. The switch profile sets the model type, the SNMP port to send SNMP traps on, SNMP version for read and write, and corresponding community strings or authentication parameters (SNMPv3 write).
- **Default Port Profile:** This drop-down menu shows the default port profile that you chose to apply to unconfigured ports on the switch on the Ports tab. The uncontrolled port profile is the initial default profile for all ports, unless you change the setting here.
- **Description:** This field shows the optional description of the switch that you entered.

Managing Switch Configuration Settings: Advanced



Switch Management > Devices > Switch [10.10.20.3]

Control Method: ● Mac Notification ○ Linkup Notification

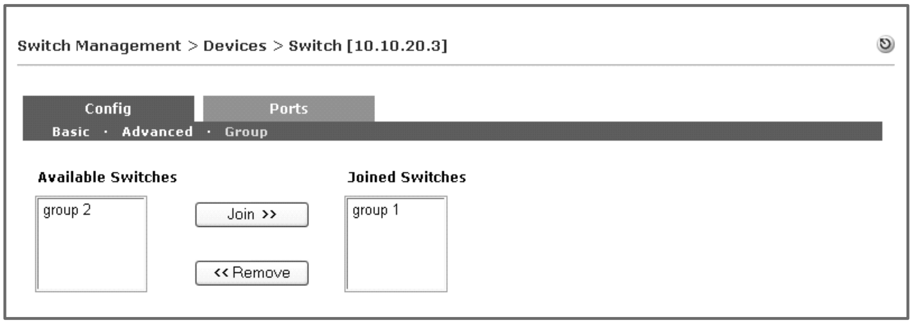
CANAC v2.1—3-30

The Config > Advanced page shows which SNMP trap method is being used for the switch. These SNMP trap method options are available:

- If a switch supports MAC notification, the Cisco NAM automatically enables the Mac Notification option as the control method and no further action is necessary.
- If a switch does not support MAC notification, the Cisco NAM enables the Linkup Notification option as the control method. With the linkup notification control method, the Cisco NAM must poll each port to determine the number of MAC addresses on the port.
- If the switch additionally supports port security, the Port Security option also appears on the Config > Advanced Page. With this feature, even if the port is connected to a hub, only the first MAC address that is authenticated is allowed to send traffic. Availability of the Port Security feature depends on the switch model and operating system that you are using.

Note For more detailed information on the Config > Advanced page, refer to the Config Tab section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Managing Switch Configuration Settings: Group



Switch Management > Devices > Switch [10.10.20.3]

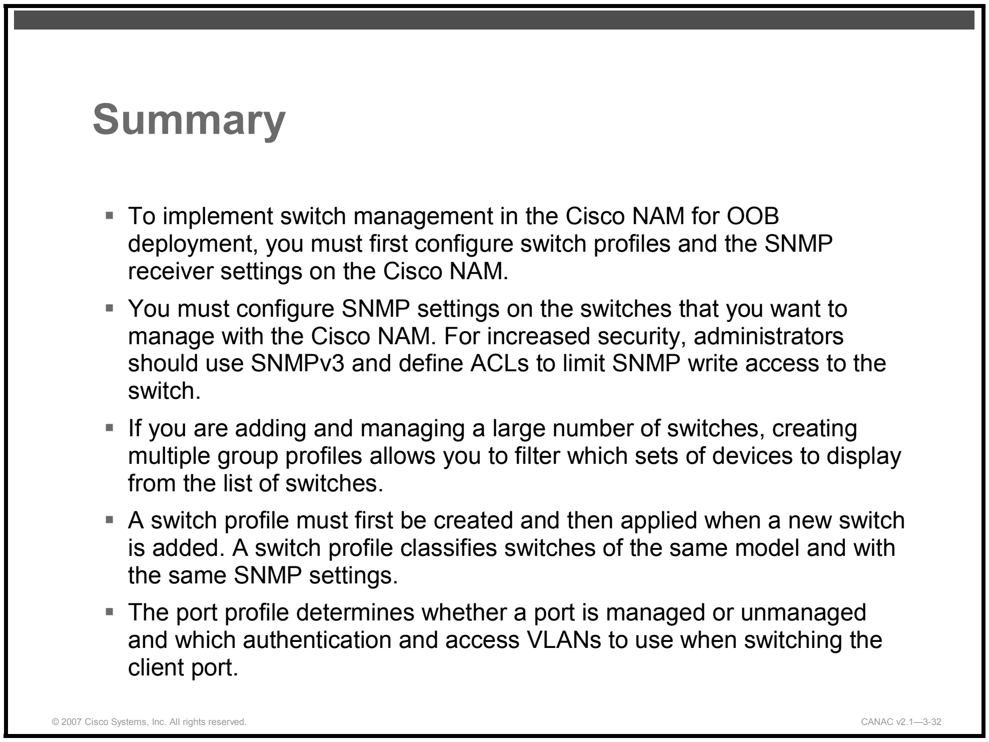
Available Switches: group 2

Joined Switches: group 1

The Config > Group page displays all the group profiles that are configured in the Cisco NAM and shows the present group profiles of the switch. From this page, you can join the switch to other groups or you can remove the switch from a joined group. To change the group membership for all switches, go to **Switch Management > Profiles > Group**.

Summary

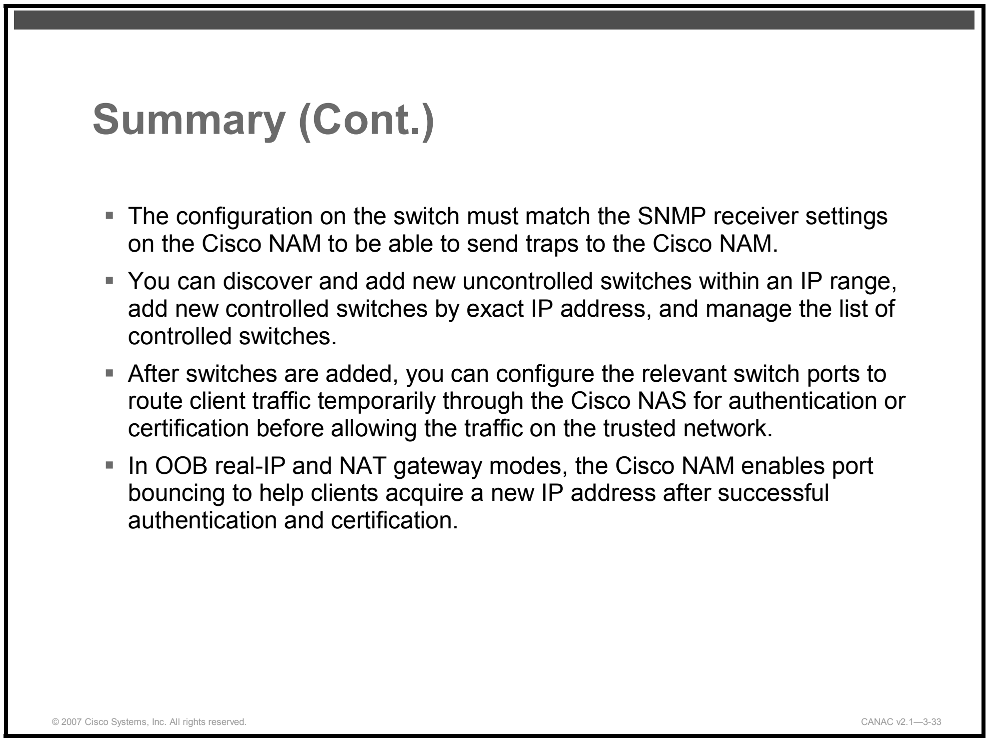
This topic summarizes the key points that were discussed in this lesson



Summary

- To implement switch management in the Cisco NAM for OOB deployment, you must first configure switch profiles and the SNMP receiver settings on the Cisco NAM.
- You must configure SNMP settings on the switches that you want to manage with the Cisco NAM. For increased security, administrators should use SNMPv3 and define ACLs to limit SNMP write access to the switch.
- If you are adding and managing a large number of switches, creating multiple group profiles allows you to filter which sets of devices to display from the list of switches.
- A switch profile must first be created and then applied when a new switch is added. A switch profile classifies switches of the same model and with the same SNMP settings.
- The port profile determines whether a port is managed or unmanaged and which authentication and access VLANs to use when switching the client port.

CANAC v2.1—3-32



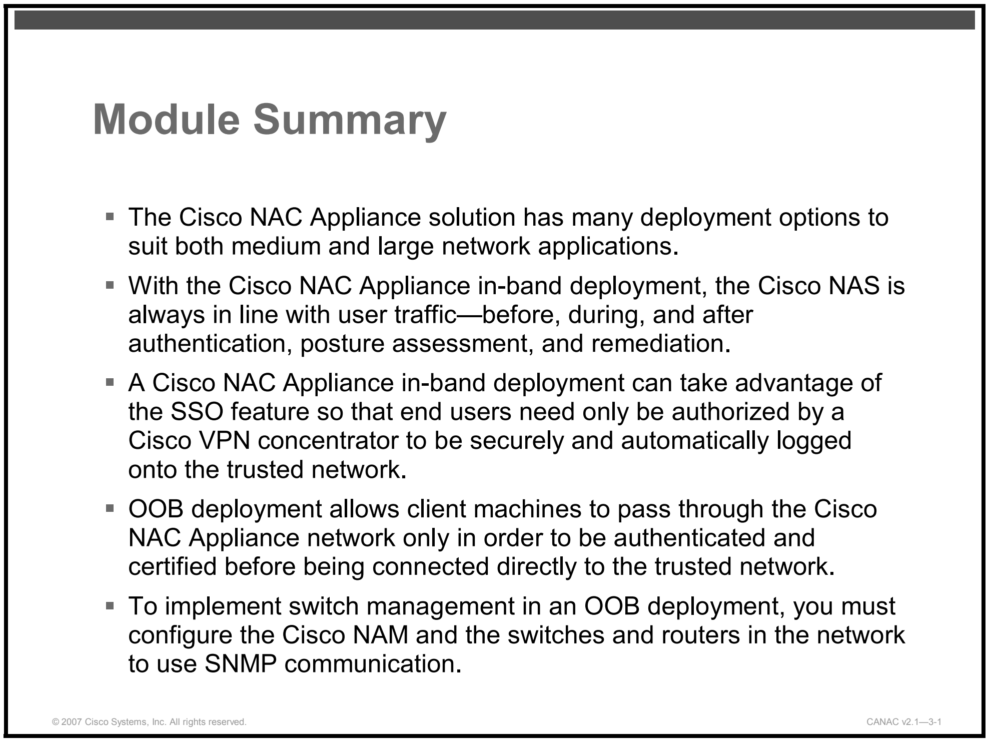
Summary (Cont.)

- The configuration on the switch must match the SNMP receiver settings on the Cisco NAM to be able to send traps to the Cisco NAM.
- You can discover and add new uncontrolled switches within an IP range, add new controlled switches by exact IP address, and manage the list of controlled switches.
- After switches are added, you can configure the relevant switch ports to route client traffic temporarily through the Cisco NAS for authentication or certification before allowing the traffic on the trusted network.
- In OOB real-IP and NAT gateway modes, the Cisco NAM enables port bouncing to help clients acquire a new IP address after successful authentication and certification.

CANAC v2.1—3-33

Module Summary

This topic summarizes the key points that were discussed in this module.



Module Summary

- The Cisco NAC Appliance solution has many deployment options to suit both medium and large network applications.
- With the Cisco NAC Appliance in-band deployment, the Cisco NAS is always in line with user traffic—before, during, and after authentication, posture assessment, and remediation.
- A Cisco NAC Appliance in-band deployment can take advantage of the SSO feature so that end users need only be authorized by a Cisco VPN concentrator to be securely and automatically logged onto the trusted network.
- OOB deployment allows client machines to pass through the Cisco NAC Appliance network only in order to be authenticated and certified before being connected directly to the trusted network.
- To implement switch management in an OOB deployment, you must configure the Cisco NAM and the switches and routers in the network to use SNMP communication.

CANAC v2.1—3-1

This module describes the many deployment options of a Cisco Network Admission Control (NAC) Appliance that are available to administrators of networks of all sizes. The implementation of a Cisco NAC Appliance in-band deployment is described as a procedure that involves only minor changes to the switch or router configuration, or no changes at all, depending on the Cisco NAC Appliance Server (Cisco NAS) operating mode that you choose. When in-band deployment is used, the Cisco NAS is always in line with user traffic, while using out-of-band (OOB) deployment means that the client machine only has to pass through the Cisco NAC Appliance network once to be authenticated and certified. The implementation of NAC Appliance for out-of-band deployment is more complex than for in-band deployment. Out-of-band deployment requires that you configure the network for out-of-band operation as well as configure the Cisco NAM to manage switches and ports for VLAN quarantine operation.

Using the skills and knowledge that you learn in this module, you are able to deploy a Cisco NAC Appliance in-band solution centrally or at the edge of your network. You are also able to deploy Cisco NAC Appliance for out-of-band operation, including configuring the network and the Cisco NAM to enable switch management from the Cisco NAM web console.

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *Cisco NAC Appliance (Clean Assess) Introduction* http://www.cisco.com/en/US/products/ps6128/index.html
- Cisco Systems, Inc. *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html
- Cisco Systems, Inc. *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*. http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

Q1) During one stage of the Cisco NAC Appliance in-band process flow, the Cisco NAA guides the user to download updates or patches from an antivirus vendor update website. Which user role applies to the user during this stage? (Source: Implementing Cisco NAC Appliance In-Band Deployment)

A) temporary role
B) normal login role "employee"
C) unauthenticated role
D) quarantine role

Q2) When the Cisco NAS is configured to operate as an in-band real-IP gateway, which three of the following statements apply? (Choose three.) (Source: Implementing Cisco NAC Appliance In-Band Deployment)

A) The Cisco NAS untrusted interface acts as a gateway for the managed subnets.
B) The Cisco NAS operates as a standard Ethernet bridge but with the added functionality that is provided by the IP filter and IPsec module.
C) The Cisco NAS performs the translation between the private and public addresses while traffic is routed between the untrusted (managed) and the external network.
D) This configuration is typically used when the untrusted network already has a gateway and you do not want to alter the existing configuration.
E) The IP addresses of the Cisco NAS trusted and untrusted interfaces should be on different subnets.
F) Static routes must be added to the next-hop router to relay traffic destined for the managed subnets to the Cisco NAS trusted interface.
G) The Cisco NAS should be configured for DHCP forwarding.

Q3) When you are unable to add a Cisco NAS to the Cisco NAM domain, which three of the following steps should you take to troubleshoot the problem? (Choose three.) (Source: Implementing Cisco NAC Appliance In-Band Deployment)

A) Check that the type of server that you selected is correct.
B) For the server IP address, ensure that you entered the address of the Cisco NAS untrusted interface (eth1).
C) Test the connectivity between the Cisco NAS and Cisco NAM.
D) Run the Cisco NAM install script again.
E) Ensure that the shared secret is the same on the Cisco NAS and Cisco NAM.
F) Configure the firewall rules to block the RMI ports.
G) Check that the certificates on the Cisco NAM and Cisco NAS are correct.

Q4) Place the following statements describing the out-of-band process flow into the correct sequence, using the letters A, B, C, and so on. (Source: Implementing Cisco NAC Appliance Out-of-Band Deployment)

_____ 1. The Cisco NAM instructs the switch to put the device port onto the access VLAN (10) based on port mapping or the role assignment.

_____ 2. The Cisco NAS challenges the device for user credentials to determine the role of the device user.

_____ 3. The Cisco NAS informs the Cisco NAM that the device is now certified.

_____ 4. The Cisco NAM instructs the switch to assign the port the device is on to the authentication or quarantine VLAN.

_____ 5. A user attaches a laptop to the network.

_____ 6. The Cisco NAA guides the user through a step-by-step remediation process.

_____ 7. The Cisco NAM verifies whether the device is on the out-of-band online list or certified devices list.

_____ 8. The switch sends the MAC address of the device via SNMP-based notification to the Cisco NAM.

_____ 9. The device is allowed access to the network.

_____ 10. The Cisco NAS sends compliance checks to the Cisco NAA.

Q5) When implementing switch management for out-of-band deployment, what is the last step in the implementation sequence? (Source: Managing Switches)

A) Configure the SNMP receiver module on the Cisco NAM.
B) Add the out-of-band Cisco NAS and configure the environment.
C) Add switches to the Cisco NAM managed domain.
D) Initialize the switch ports to use the correct port profiles.
E) Configure group profiles on the Cisco NAM.

Q6) When configuring the switch settings for an out-of-band Cisco NAC Appliance operation, which two measures can you take for improved security? (Choose two.) (Source: Managing Switches)

A) Set the MAC address aging-time parameter to zero.
B) Define ACLs to limit SNMP write access to the switch.
C) Enable the **portfast** command.
D) Use SNMPv3.
E) Enable MAC notification traps.

Q7) What should you do when you are deploying the Cisco NAS as an out-of-band gateway? (Source: Managing Switches)

A) Connect the untrusted interface of the Cisco NAS to the switch port on the administrative or access VLAN.
B) Configure VLAN mapping after connecting the untrusted interface to the switch.
C) Specify an access VLAN when you create a new user role for role-based port profiles.

Q8) Which statement correctly describes a switch profile? (Source: Managing Switches)

A) A switch profile determines which authentication and access VLANs to use when switching the client port.
B) A switch profile classifies switches of the same model and with the same SNMP settings.
C) A switch profile allows you to filter which sets of devices to display from the list of switches.

Q9) Which one of the following statements about port profiles is true? (Source: Managing Switches)

A) You must add a port profile for each set of authentication or access VLANs that you configure on the switch.
B) Regular switch ports that are not connected to clients use the controlled port profile.
C) Client-connected switch ports use uncontrolled profiles.
D) For virtual gateway deployments, you must enable the port bouncing option on the port profile.

Q10) Match the following SNMP receiver settings with the correct application. (Source: Managing Switches)

A) MAC-notification Trap Timeout field
B) Port Bounce Interval field
C) Linkup Trap Bounce Timeout field
D) Port Security Delay field

_____ 1. After the VLAN is switched, the Cisco NAM must wait the number of seconds specified in this field before setting the related information on the switch.

_____ 2. If the time difference between the timestamp and the current time is greater than the setting in this field, the trap is dropped.

_____ 3. This delay is inserted to help client machines issue DHCP requests.

_____ 4. In order to keep the port controlled and to limit the number of times that the Cisco NAM tries to resolve the MAC address, the Cisco NAM bounces the port after the time interval specified in this field.

Q11) When is a heartbeat timer used? (Source: Implementing the Cisco VPN SSO Feature on the Cisco NAC Appliance)

A) The heartbeat timer is used in Layer 3 deployments.
B) The heartbeat timer is used in out-of-band Layer 2 and Layer 3 deployments.
C) The heartbeat timer is used when Cisco NAS is the first hop behind the VPN concentrator.
D) The heartbeat timer is used when Cisco NAS is two or more hops behind the VPN concentrator.

Q12) What does an end user need to do when SSO is implemented in a Cisco NAC Appliance using a Cisco VPN concentrator? (Source: Implementing the Cisco VPN SSO Feature on the Cisco NAC Appliance)

A) Using SSO, users logging in through the VPN client do not have to log in again to the Cisco NAC Appliance.
B) In out-of-band Cisco NAS deployments, the user logs in using SSO and does not have to log in again to the Cisco NAC Appliance.
C) In a wireless in-band deployment, users need only log in twice, once to access their device and once to enable VPN tunneling.

Q13) When you are configuring the Cisco NAS user in the New Object > User window, when do you enter the full name of the user? (Source: Implementing the Microsoft Windows SSO Feature on the Cisco NAC Appliance)

A) never; the Full Name field is populated automatically
B) after entering a name in the User Logon Name field
C) before entering either a first name or user logon name
D) after entering a name in the First Name field

Q14) When you are configuring the FQDN field in the Active Directory Server form, which letter case must be used? (Source: Implementing the Microsoft Windows SSO Feature on the Cisco NAC Appliance)

A) never uppercase
B) sentence case
C) exact case
D) lowercase

Module Self-Check Answer Key

Q1)	D
Q2)	A, E, F
Q3)	C, E, G
Q4)	A-5, B-8, C-7, D-4, E-2, F-10, G-6, H-3, I-1, J-9
Q5)	D
Q6)	B,D
Q7)	C
Q8)	B
Q9)	A
Q10)	1-D, 2-A, 3-B, 4-C
Q11)	C
Q12)	A
Q13)	A
Q14)	C

Module 4

Cisco NAC Appliance Implementation Options

Overview

A Cisco Network Admission Control (NAC) Appliance solution ensures that users gain access to the network only after the correct application software is on their machines and they are certified clean of all currently known vulnerabilities. A network security administrator needs to implement the correct options so that their Cisco NAC Appliance solution will provide users with the appropriate combination of security and ease of use. This module describes how to implement network scanning to identify which end-user systems are vulnerable, and how to provide web page feedback to help those users mitigate identified vulnerabilities. This module includes the steps that are required to configure the Cisco NAC Appliance Manager (Cisco NAM) to implement the NAC Appliance Agent (Cisco NAA) on user devices. This configuration ensures a seamless implementation of your corporate security policies. This module also describes how to configure the Cisco NAM and the Cisco NAC Appliance Servers (Cisco NASs) in high-availability mode to ensure continuous, secure network resources to your clients.

Module Objectives

Upon completing this module, you will be able to implement a highly available Cisco NAC Appliance solution to mitigate network threats and facilitate network access for users that meet corporate security requirements. This ability includes being able to meet these objectives:

- Explain which Cisco NAC Appliance features you must implement to protect a network
- Configure the Cisco NAC Appliance network scanner to use Nessus plugins for checking security vulnerabilities
- Explain how to configure the Cisco NAM to implement the Cisco NAA on client machines in a network
- Configure a high-availability pair of Cisco NAMs
- Configure a high-availability pair of Cisco NASs

Lesson 1

Implementing Cisco NAC Appliance on a Network

Overview

This lesson describes how you can implement Cisco Network Admission Control (NAC) Appliance to protect a network. You must implement Cisco NAC Appliance correctly in order to minimize network attacks, ensure that users are able to gain access to the network only after installing the latest application software, and certify that user machines are clean of all currently known vulnerabilities.

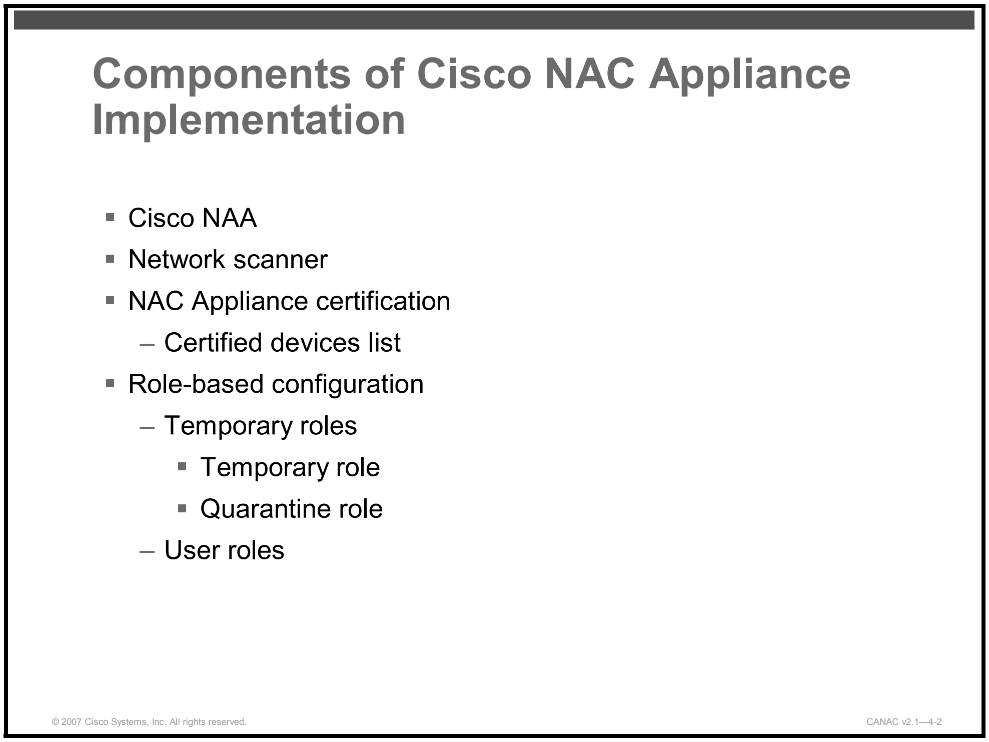
Objectives

Upon completing this lesson, you will be able to explain which Cisco NAC Appliance features you need to implement in order to protect a network. This ability includes being able to meet these objectives:

- Describe how to implement Cisco NAC Appliance to protect a network
- Describe how to use the Device Management menu options to configure the general setup options
- Explain how user pages are configured in Cisco NAC Appliance
- Describe how to use the Cisco NAM to manage certified devices in the network

Implementing Cisco NAC Appliance

This topic describes how to implement Cisco NAC Appliance to protect a network.



Components of Cisco NAC Appliance Implementation

- Cisco NAA
- Network scanner
- NAC Appliance certification
  - Certified devices list
- Role-based configuration
  - Temporary roles
    - Temporary role
    - Quarantine role
  - User roles

CANAC v2.1—4-2

Before you implement Cisco NAC Appliance on a network, it is worthwhile to review the components that are used in the implementation procedure, as follows:

- **Cisco NAC Appliance Agent (Cisco NAA):** The Cisco NAA software resides on Microsoft Windows systems and can verify if an application or service is running and if a registry key exists or if the value of a registry key is known. The Cisco NAA is referred to as a read-only agent; the Cisco NAA does not alter client system information, but reads the information and reports this information to the Cisco NAC Appliance Manager (Cisco NAM). The Cisco NAA ensures that, for example, a corporate laptop has an up-to-date configuration of the standard corporate software before the laptop is allowed to access the corporate network. The Cisco NAA can ensure that users install the resources necessary to keep their machines from becoming vulnerable or infected.

  The Cisco NAA is included as part of the Cisco NAM software. When the Cisco NAM is installed, the Cisco NAA setup executable file is already present and is automatically published from the Cisco NAM to the Cisco NAC Appliance Servers (Cisco NASs). To distribute the Cisco NAA to clients, set up the Cisco NAA in the web administration console for the desired user role and operating system.

- **Network scanner:** Network scans are implemented with Nessus plug-ins. Nessus is an open-source vulnerability scanner. Nessus plug-ins test client systems for security vulnerabilities over the network. If a system is scanned and found to be vulnerable or infected, Cisco NAC Appliance takes immediate action by alerting vulnerable users. Cisco NAC Appliance either blocks vulnerable users from the network or assigns users to a quarantine role in which they can fix their systems. When new Nessus plug-ins are released, they can be loaded into the Cisco NAM repository. The Cisco NAM distributes new plug-ins to the Cisco NASs. The Cisco NASs then perform client scanning using the latest vulnerability protection code.

- **Cisco NAC Appliance certification:** Client devices that meet the configured Cisco NAC Appliance requirements are considered certified devices and are added to the certified devices list. A certified device remains on the certified devices list until one of these events takes place:

  - The administrator manually removes the client from the list.
  - The administrator manually clears the entire list.
  - The list is automatically cleared using the certified devices timer.

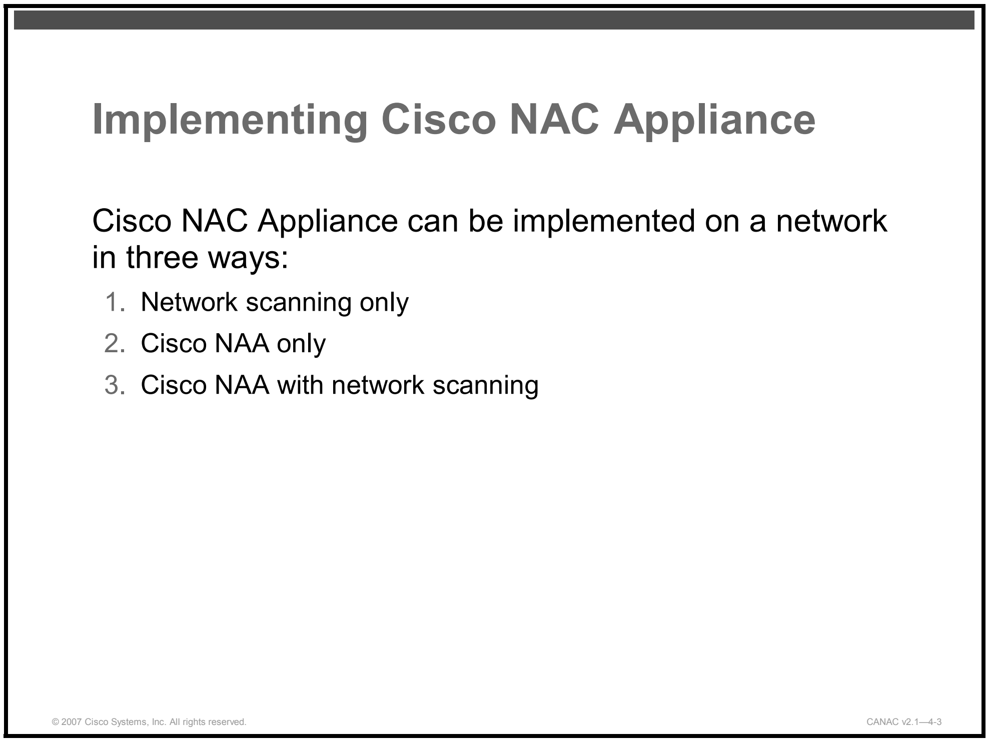
  When the client is taken off the certified devices list, the client must go through the Cisco NAC Appliance authentication process again to be readmitted to the network. You can add floating devices to the certified devices list that are certified only for the duration of a user session. Alternatively, you can exempt devices from the Cisco NAC Appliance certification process altogether by manually adding them to the certified list.

- **Role-based configuration:** Cisco NAC Appliance network protection features are configured for users by role and by operating system. There are two types of roles specifically used by Cisco NAC Appliance. These roles are intended as temporary roles that offer users limited network access in order to fix their systems:

  - **Quarantine role:** A user is put in the quarantine role after failing a network scan such as a Nessus plug-in check.
  - **Cisco NAA temporary role:** A user is put in the temporary role when the machine is running the Cisco NAA and fails a required check (for example, a registry check).

  When a user authenticates, either through the web login page or through the Cisco NAA, Cisco NAC Appliance determines the role of the user. After the user role is determined, Cisco NAC Appliance verifies that the requirements are met and performs the network scanning that is configured for that role and operating system.

  The user role is determined immediately after the initial login to determine the scans or system requirements associated with that user. The user is not put into a normal login role until all requirements are met, scanning has occurred, and no vulnerabilities are found. If the client has not met requirements, the user stays in the Cisco NAA temporary role until requirements are met or the session times out. If the user has met requirements but is found with network scanning vulnerabilities, the user can be either assigned to a quarantine role or blocked, depending on the configuration for that role and operating system.



Implementing Cisco NAC Appliance

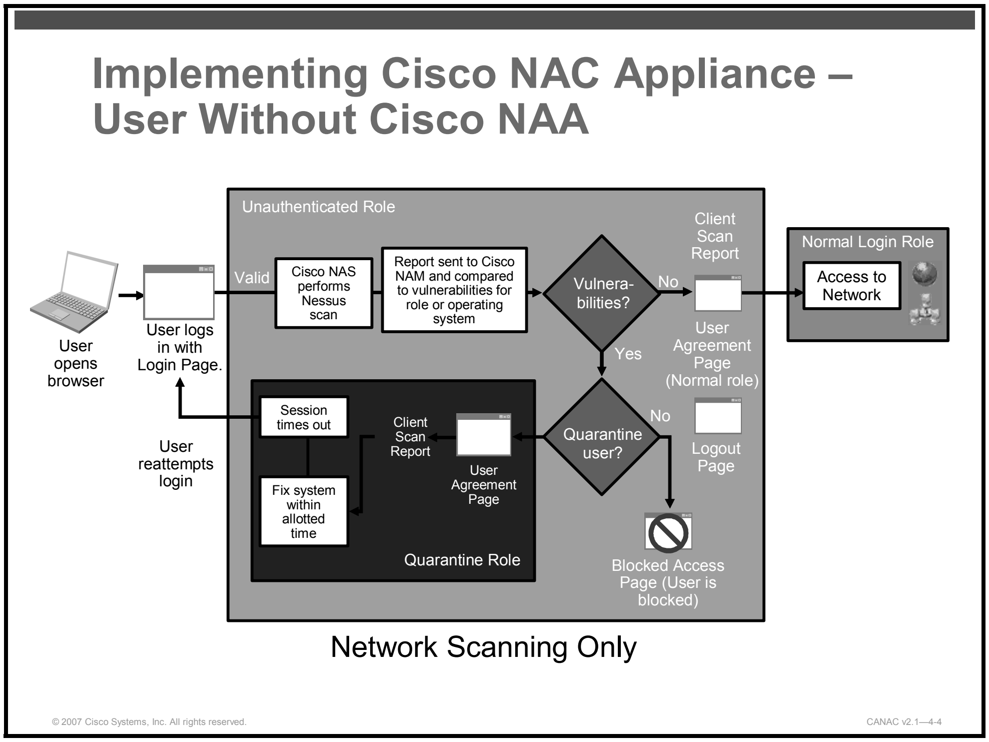
Cisco NAC Appliance can be implemented on a network in three ways:

1. Network scanning only
2. Cisco NAA only
3. Cisco NAA with network scanning

CANAC v2.1—4-3

You can implement Cisco NAC Appliance on a network in these three ways:

- **Network scanning only:** This method provides network-based vulnerability assessment and web-based remediation. The network scanner in the local Cisco NAS performs the actual network scanning and checks for well-known port vulnerabilities that a particular host may be prone to. If vulnerabilities are found, web pages that are configured in the Cisco NAM are available to distribute links to websites to the user or to provide information on how users can fix vulnerabilities in their systems.
- **Cisco NAA only:** This method provides local machine agent-based vulnerability assessment and remediation. Users must download and install the Cisco NAA. The Cisco NAA allows for visibility into the host registry, process checking, application checking, and service checking. The Cisco NAA can be used to distribute links to websites or upload files to the Cisco NAM that users can access to fix vulnerabilities in their systems.
- **Cisco NAA with network scanning:** This method combines the benefits of the Cisco NAA, Cisco NAS, and Cisco NAM. The Cisco NAA provides visibility into the host registry, process checking, application checking, and service checking. The Cisco NAS provides network scanning and port vulnerability checks. The Cisco NAM provides web-based remediation on how users can fix vulnerabilities in their systems.



Implementing Cisco NAC Appliance – User Without Cisco NAA

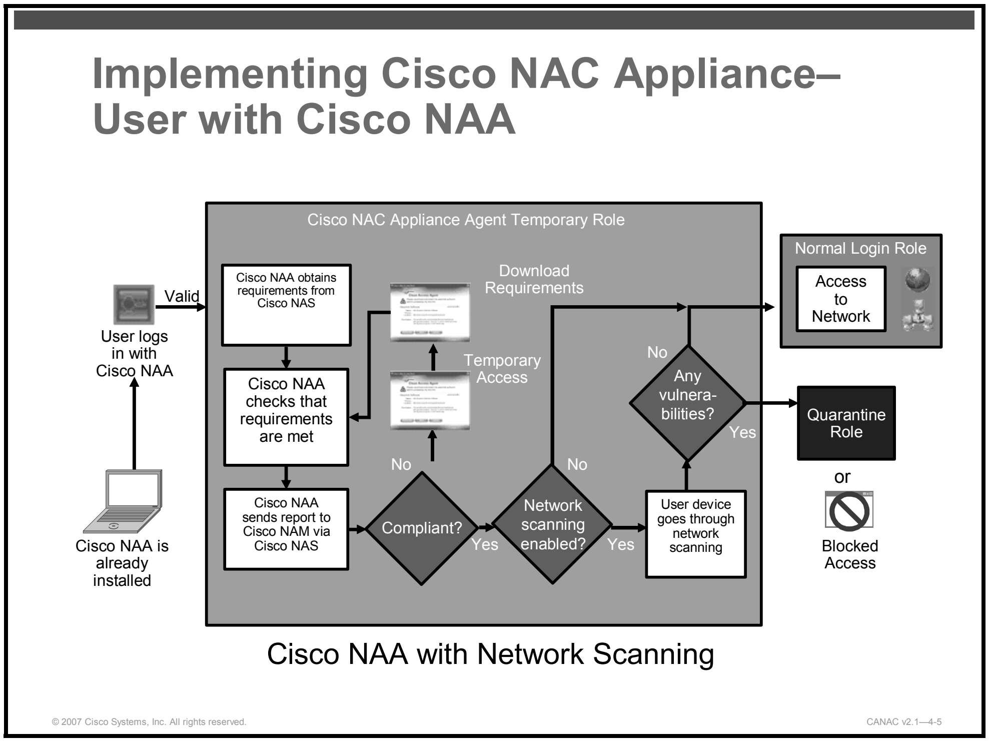
Unauthenticated Role
User opens browser
User logs in with Login Page.
Valid
Cisco NAS performs Nessus scan
Report sent to Cisco NAM and compared to vulnerabilities for role or operating system
Vulnera-bilities?
No
Client Scan Report
User Agreement Page (Normal role)
Normal Login Role
Access to Network
Yes
Quarantine user?
No
Logout Page
Blocked Access Page (User is blocked)
User Agreement Page
Client Scan Report
Session times out
Fix system within allotted time
Quarantine Role
User reattempts login

Network Scanning Only

CANAC v2.1—4-4

The figure shows that an end user without Cisco NAA must go through a comprehensive authentication procedure. If the user has valid login credentials and the Nessus scan does not reveal any role or operating system vulnerabilities, the user is presented with a user agreement form. When the agreement is accepted, the user receives role-based access to the network. If vulnerabilities are found in the user system, the user must go through a process requiring that the end-user system be repaired within a specific time frame.

Note If a client machine fails a Nessus scan, the user is placed in the quarantine role. The Cisco NAA places users, when they are attempting to authenticate into the normal user role, into the temporary role until they pass requirements associated with the normal login role.



Implementing Cisco NAC Appliance– User with Cisco NAA

Cisco NAC Appliance Agent Temporary Role

Cisco NAA is already installed

User logs in with Cisco NAA

Valid

Cisco NAA obtains requirements from Cisco NAS

Cisco NAA checks that requirements are met

Cisco NAA sends report to Cisco NAM via Cisco NAS

Compliant?

No

Temporary Access

Download Requirements

Yes

Network scanning enabled?

No

Yes

User device goes through network scanning

Any vulnera-bilities?

No

Yes

Normal Login Role

Access to Network

Quarantine Role

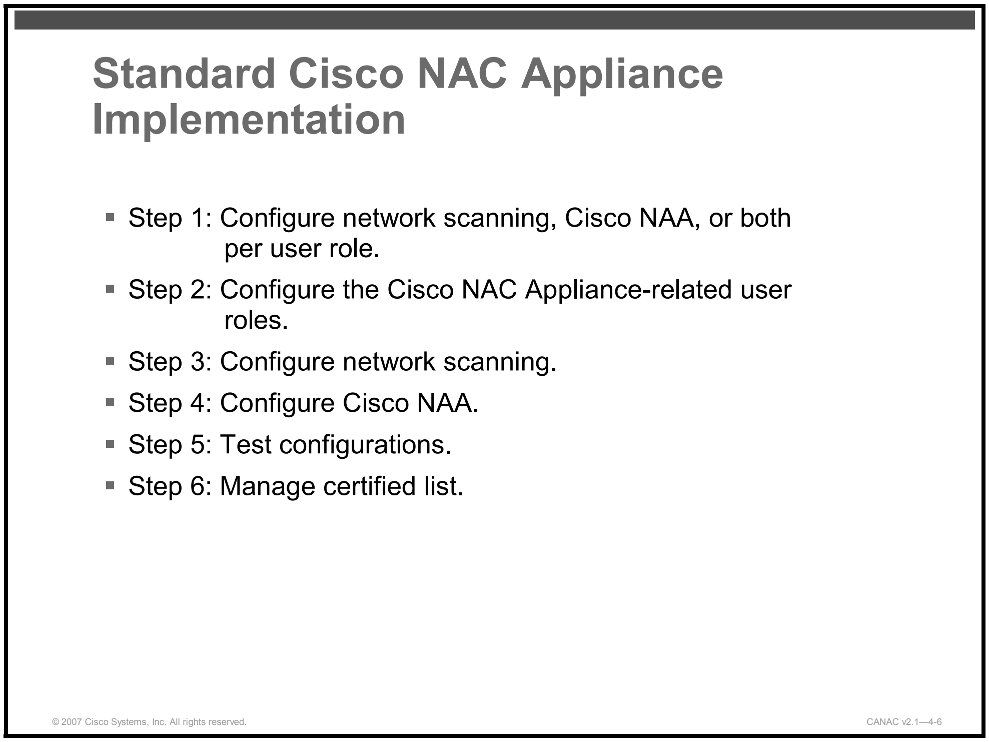
or

Blocked Access

Cisco NAA with Network Scanning

CANAC v2.1—4-5

The figure shows how an end user with Cisco NAA, Cisco NAS, and Cisco NAM installed goes through a less complicated, but equally comprehensive, authentication procedure. When the user logs in, Cisco NAA provides a valid certification that allows the Cisco NAA to obtain information from the Cisco NAS regarding the requirements for the current role and operating system of the user. Cisco NAA checks that the system requirements for the current end user are met and then sends the requirements report to the Cisco NAM. If these requirements are met and the network scan does not reveal any vulnerabilities, the user is granted access to the network. If the user device fails to meet the requirements or fails the network scan, remediation takes place based on where the user is in the login process. Remediation at the requirements phase involves downloading the required software upgrades, and is done in the temporary role. Remediation at the network scanning phase is done in the quarantine role.



Standard Cisco NAC Appliance Implementation

- Step 1: Configure network scanning, Cisco NAA, or both per user role.
- Step 2: Configure the Cisco NAC Appliance-related user roles.
- Step 3: Configure network scanning.
- Step 4: Configure Cisco NAA.
- Step 5: Test configurations.
- Step 6: Manage certified list.

CANAC v2.1—4-6

These six steps outline the typical procedure that is used to implement Cisco NAC Appliance:

Step 1 **Configure network scanning, Cisco NAA, or both per user role in the General Setup tab.** The General Setup tab allows you to require the use of the Cisco NAA during login, to block or quarantine users in a role, and to enable other general settings per user role and client operating system.

Step 2 **Configure the Cisco NAC Appliance-related user roles with session timeout and traffic policies (in-band).** Traffic policies for the quarantine role allow access to the User Agreement page and provide web resources for quarantined users who fail network scanning. Traffic policies for the Cisco NAA temporary role allow access to the resources from which the user can download required software packages.

Step 3 **Configure network scanning.** Load Nessus plug-ins to the Cisco NAM repository. To enable network scanning, choose the Nessus plug-ins that you want to have participate in scanning and then configure scan result vulnerabilities for the user roles and operating systems. You must also customize the User Agreement page.

Step 4 **Configure Cisco NAA.** Require the use of the Cisco NAA for a user role in the General Setup tab. Perform an update to download the latest Cisco checks, rules, and antivirus product support. Plan and define your requirements for each user role. Configure antivirus rules or create custom rules from checks. Map antivirus rules to an antivirus requirement and map custom rules to a custom requirement, if necessary. Map requirements to a user role.

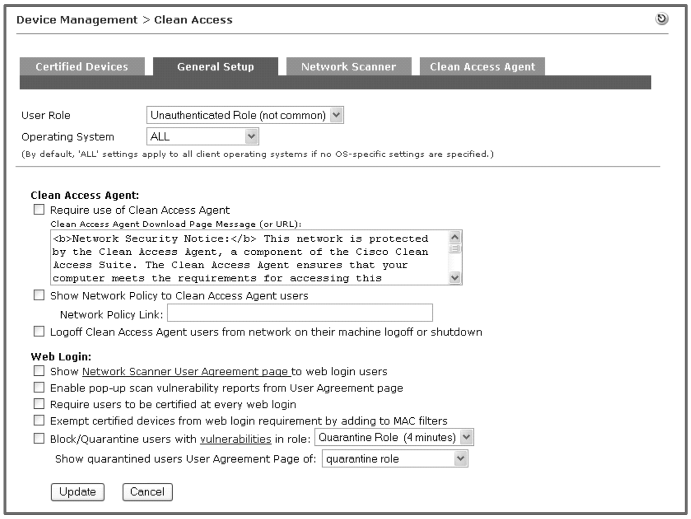
Step 5 **Test your configurations.** Confirm configurations for each user role and operating system by connecting as a client to the newly configured network. Monitor the certified list, Online Users page, and event logs during testing. Test network scanning by performing a web login and then checking the network scanning process, the logout page, and the associated client and administrator reports. Test the Cisco NAA configuration by performing the initial web login, Cisco NAA download, Cisco NAA login, requirement checks, and scanning and then view the associated client and administrator reports.

Step 6 **Manage the certified list.** If required, manage the certified list by configuring other devices, such as floating or exempt devices. Floating devices must be certified at the start of every user session. Exempt devices are excluded from Cisco NAC Appliance requirements.

Introducing the General Setup Tab

This topic describes how to use the Device Management menu options to configure the general setup options.

General Setup Tab



Device Management > Clean Access

User Role: Unauthenticated Role (not common)
Operating System: ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Clean Access Agent:

□ Require use of Clean Access Agent

Clean Access Agent Download Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
by the Clean Access Agent, a component of the Cisco Clean
Access Suite. The Clean Access Agent ensures that your
computer meets the requirements for accessing this
```

□ Show Network Policy to Clean Access Agent users
Network Policy Link:
□ Logoff Clean Access Agent users from network on their machine logoff or shutdown

Web Login:

□ Show Network Scanner User Agreement page to web login users
□ Enable pop-up scan vulnerability reports from User Agreement page
□ Require users to be certified at every web login
□ Exempt certified devices from web login requirement by adding to MAC filters
□ Block/Quarantine users with vulnerabilities in role: Quarantine Role (4 minutes)
Show quarantined users User Agreement Page of: quarantine role

Update Cancel

The General Setup tab organizes the Cisco NAA and web login setup features.

Note This course uses the GUI found in Cisco NAC Appliance Release 4.0.0. Expect minor differences in the GUI in other versions of the Cisco NAC Appliance.

Web pages that appear to Cisco NAC Appliance users must first be enabled in the administrator console. The General Setup tab on the Device Management > Clean Access page enables several page controls for Cisco NAC Appliance. Some of these controls pertain to pages that are shown to the user during network scanning. Other controls enable Cisco NAA-related dialog boxes or web pages. In addition to page content, you can also specify whether pages appear when the user logs in with a specific user role and operating system.

Note Cisco NAC Appliance pages are always configured according to both user role and client operating system.

After installation, Cisco NAA users should log in through the Cisco NAA dialog box. This dialog box is configured to automatically pop up when the pop-up login window is checked in the General Setup tab in the Cisco NAM administration console. Alternatively, Cisco NAA users can bring up the login window by right-clicking the Cisco NAA icon on the taskbar. Typically, Cisco NAA users will not see quarantine role pages or pop-up scan vulnerability reports because the Cisco NAA dialog box communicates this information.

If users are allowed to access the network based on user system configurations, web login users can see the login and logout pages, quarantine role or blocked access pages, and Nessus scan vulnerability reports.

These Cisco NAA configurable options are found on the General Setup tab:

- **User Role:** This field refers to the user role that will be configured with Cisco NAC Appliance controls. The drop-down menu shows all available roles in the system.

Note To modify existing roles or to add a new role, refer to the Add New Role section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

- **Operating System:** This field refers to the operating system for the specified user role. By default, ALL applies to all client operating systems if no operating system-specific settings are selected.
- **Require use of Clean Access Agent:** If this box is checked, client devices for the defined user role and operating system are required to use the Cisco NAA to access the network. If checked, the Cisco NAA download page message (or URL) appears after the initial web login to prompt users to download, install, and use the Cisco NAA to log onto the network. To modify the default message, type HTML text or enter a URL to instruct users to download the Cisco NAA.

Note Cisco NAA configuration must also be completed. This configuration requirement is described in the Clean Access Agent section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

- **Show Network Policy to Clean Access Agent users:** Click this check box if you want to display a link for Cisco NAA users in the Clean Access Agent to a Network Policy (Acceptable Use Policy) web page. You can use this option to provide a policies or information page that users must accept before they access the network. This page can be hosted on an external web server or on the Cisco NAM itself.

Note The Network Policy page is shown only to the first user that logs in with the device. This feature helps to identify the authenticating user who accepted the Network Policy page. Clearing the device from the Certified Devices list forces the user to accept the network policy again at the next login.

- **Logoff Clean Access Agent users from network on their machine logoff or shutdown:** This option allows you to ensure that users are logged off from the Cisco NAC Appliance network when they log off the Windows domain or shut down a Windows workstation. If this option is not checked, users remain logged onto Cisco NAC Appliance after their machine is logged off or shut down and restarted. Enabling this feature ensures that the Auto-Upgrade function checks for updates on the Cisco NAA at machine restart. If this feature is not enabled, the client will be checked for updates only at the next user login.

These web-based configurable login options are found on the General Setup tab:

- **Show network scanner User Agreement page to web login users:** Check this check box to present the User Agreement page after web login and network scanning. The page displays the content you configure in the User Agreement configuration form. Users must click the **Accept** button to access the network. Clearing an end-user device from the Certified Devices list forces the user to accept the User Agreement page again at the next login.

- **Enable pop-up scan vulnerability reports from User Agreement page:** If this box is checked, the results of the scan appear in a pop-up browser window for users who are authenticated by web login. If pop-up windows are blocked on the client computer, the user can view the report by clicking the Scan Report link on the logout page. An example of the scan report can be found in the General Setup Tab Summary section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide.*
- **Require users to be certified at every web login:** If this box is checked, users must be certified by Cisco NAC Appliance every time that they access the network. If this box is not checked (the default setting), users need to be certified only during the first time that they access the network, or until their MAC address is cleared from the certified list.
- **Exempt certified devices from web login requirement by adding to MAC filters:** Check this check box to place the MAC address of devices that are on the Cisco Clean Access certified list into the authentication passthrough list. This allows devices to bypass authentication and the Cisco NAC Appliance process altogether the next time that they access the network.
- **Block/quarantine users with vulnerabilities in role:** Enabling this option and choosing a quarantine role from the drop-down menu will put the user in the quarantine role if vulnerabilities are found after network scanning. If quarantined, the user must correct the problem with the system. Network scanning is performed again until no vulnerabilities are found, and only then is access to the network granted.

  Choosing Block Access from the drop-down menu instead of the Quarantine option blocks the user from accessing the network if vulnerabilities are found after network scanning. If a user is blocked, the Blocked Access page is shown with the content (or URL) that you have entered in the message for the Blocked Access page field.

Note The role-based session expiration time appears in parentheses next to the quarantine role name. This session time also appears on the User Agreement page if a display of the page is enabled for a quarantined user.

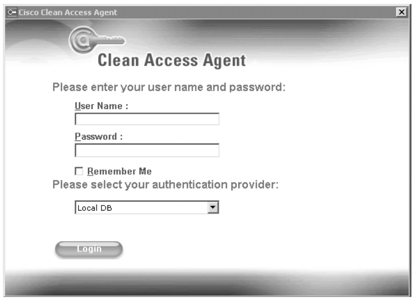
- **Show quarantined users User Agreement Page of:** The Quarantine Role option appears in the drop-down box by default. This option allows you to present a User Agreement page specific to the quarantine role chosen for users who fail scanning. Alternatively, Cisco NAC Appliance can present the page that is associated with the normal login role for a user.

Note If you choose Block Access from the Show quarantined users User Agreement page drop-down menu, the message (or URL) for the Blocked Access page option appears (not shown in the figure). To modify the default message, enter HTML text or enter a URL for the message that you want to appear when a user is blocked from the network after failing Cisco NAC Appliance certification.

Introducing User Pages

This topic describes how to configure user pages in Cisco NAC Appliance.

User Pages

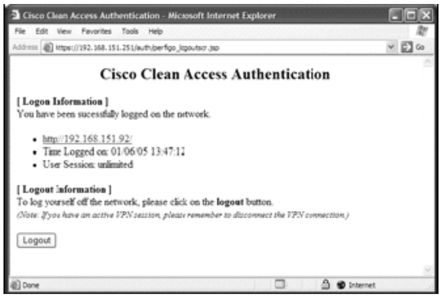


Please enter your user name and password:

Please select your authentication provider:

Local DB

Cisco NAA Login Page


Cisco Clean Access Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Logout
Done
Internet

https://192.168.151.251/auth/perfigo_logoutscr.jsp

Cisco Clean Access Authentication

[Logon Information]
You have been sucessfully logged on the network.

- http://192.168.151.92/
- Time Logged on: 01/06/05 13:47:12
- User Session: unlimited

[Logout Information]
To log yourself off the network, please click on the **logout** button.
(Note: If you have an active VPN session, please remember to disconnect the VPN connection.)

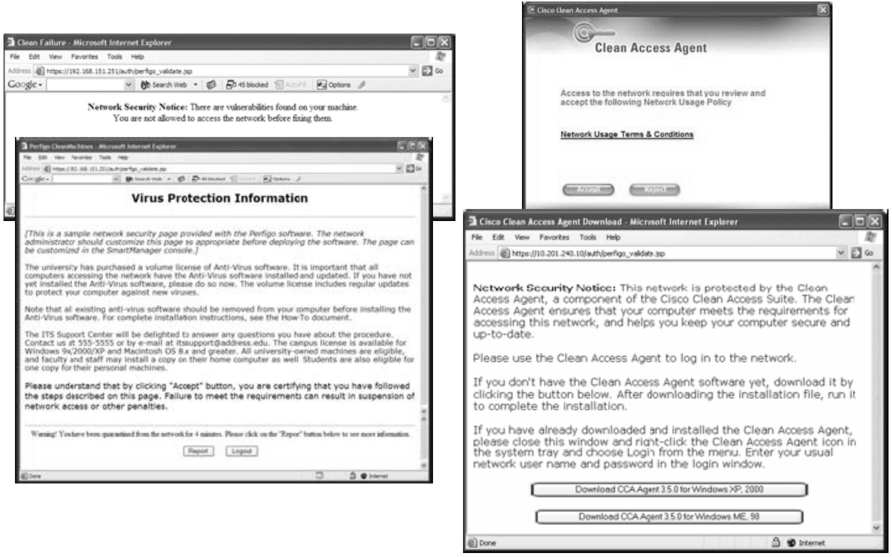
Web Logout Page

The pages shown in the figure are called “user pages.” These pages appear during web login and during the Cisco NAC Appliance certification process. User pages can be configured to suit the security requirements of a company. Different user pages are configured in different places within the Cisco NAM web administration console. Knowing where to find each of these pages makes your configuration proceed smoothly. The figure shows these user pages:

- **Login page:** There are two types of login pages. The figure shows the Cisco NAA login page. A web login page, not shown, is configured separately from Cisco NAC Appliance user pages. A web login page is the network authentication interface only when you are using network scanning. You can configure login pages per VLAN, subnet, or client operating system. Users authenticate by entering their credentials, and the Cisco NAM determines the user role assignment based on local user and user role configurations. For more information, refer to the User Login Page section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

- **Logout page:** The logout page appears only for users who use web login (not Cisco NAA login). After the user successfully logs in, the logout page appears in its own browser and displays the user status based on the combination of options that the user chooses.

Sample Cisco NAC Appliance User Pages


Clean Failure - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.151.251/auth/perfigo_validate.jsp
Go
Google
Search Web
45 blocked
AutoFill
Options

Network Security Notice: There are vulnerabilities found on your machine. You are not allowed to access the network before fixing them.

Perfigo CleanMachines - Microsoft Internet Explorer

Virus Protection Information

[This is a sample network security page provided with the Perfigo software. The network administrator should customize this page as appropriate before deploying the software. The page can be customized in the SmartManager console.]

The university has purchased a volume license of Anti-Virus software. It is important that all computers accessing the network have the Anti-Virus software installed and updated. If you have not yet installed the Anti-Virus software, please do so now. The volume license includes regular updates to protect your computer against new viruses.

Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact us at 555-5555 or by e-mail at itssupport@address.edu. The campus license is available for Windows 9x/2000/XP and Macintosh OS 8.x and greater. All university-owned machines are eligible, and faculty and staff may install a copy on their home computer as well. Students are also eligible for one copy for their personal machines.

Please understand that by clicking "Accept" button, you are certifying that you have followed the steps described on this page. Failure to meet the requirements can result in suspension of network access or other penalties.

Warning! You have been quarantined from the network for 4 minutes. Please click on the "Report" button below to see more information.

Access to the network requires that you review and accept the following Network Usage Policy

Network Usage Terms & Conditions

Accept
Reject
Cisco Clean Access Agent Download - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.201.240.10/auth/perfigo_validate.jsp
Go

Network Security Notice: This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.

Please use the Clean Access Agent to log in to the network.

If you don't have the Clean Access Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.

If you have already downloaded and installed the Clean Access Agent, please close this window and right-click the Clean Access Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window.

Download CCA Agent 3.5.0 for Windows XP, 2000
Download CCA Agent 3.5.0 for Windows ME, 98
Done
Internet

CANAC v2.1—4-9

In addition to the login and logout user pages, there are these four Cisco NAC Appliance user pages:

- **Cisco NAA download page:** When you use the Cisco NAA, this page appears after the initial one-time web login. This page prompts the user to download and install the Cisco NAA. After the Cisco NAA is installed, the user should log onto Cisco NAA rather than opening a browser.
- **Cisco NAC Appliance network policy page:** You can choose to enable the network policy page for Cisco NAA users. Unlike the User Agreement page, which web login users can bypass to access the network, Cisco NAA users must accept the network policy page before accessing the network.
- **Network scanning user agreement page:** If enabled, this page appears after a user logs onto the network and passes network scanning. The user must click the **Accept** button to proceed to the originally requested page.

Note You can configure the network scanning user agreement page in the Network Scan > Scan Setup menu, and you can enable it in the General Setup tab. For more information about the user agreement page, refer to the Customize the User Agreement Page section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

- **Block access page:** If vulnerabilities are found on the client system after network scanning, the blocked user sees the block access page, if enabled. For more information, refer to the Customize the User Agreement Page section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

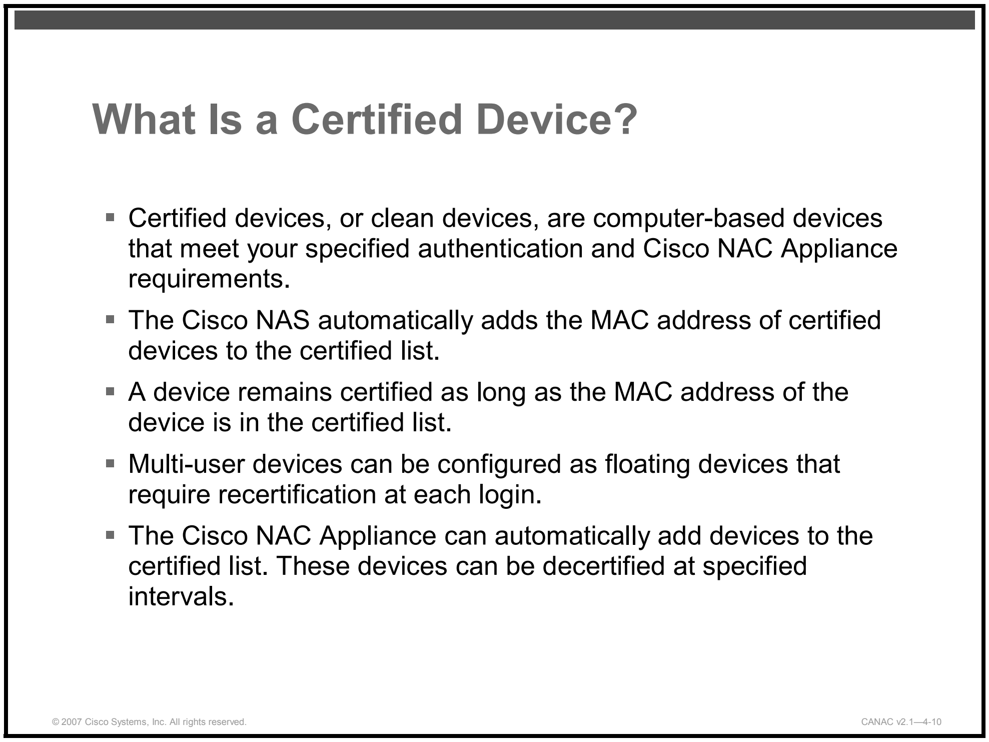
Cisco NAC Appliance also provides these two user agreement pages that you can enable:

- **Quarantined User, Original Role:** This page, if enabled, appears to a user if the user is quarantined when network scanning discovers vulnerabilities on the user system. This page has the same information page content (virus protection information) or URL as the user agreement page for the normal login role.
- **Quarantined User, Quarantine Role:** This page, if enabled, appears to a user if the user is quarantined when network scanning reveals vulnerabilities on the user system. This page allows you to specify a user agreement page for the quarantine role. The agreement page for a quarantine user in the quarantine role provides more options to configure than does the quarantine version of the user agreement page for the normal login role.

Note For both user agreement pages, the acknowledgment instructions are hard-coded to include the session timeout for both the original role and the quarantine role. The button labels are also hard-coded as Report and Logout.

Managing Certified Devices

This topic describes how to use the Cisco NAM to manage certified devices in the network.

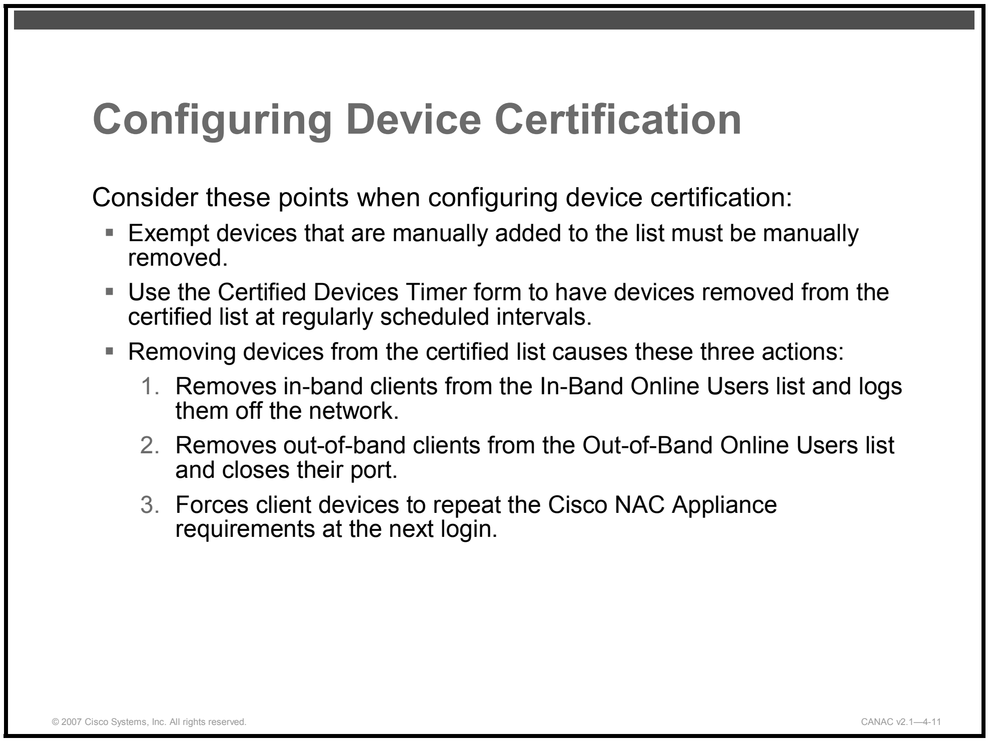


What Is a Certified Device?

- Certified devices, or clean devices, are computer-based devices that meet your specified authentication and Cisco NAC Appliance requirements.
- The Cisco NAS automatically adds the MAC address of certified devices to the certified list.
- A device remains certified as long as the MAC address of the device is in the certified list.
- Multi-user devices can be configured as floating devices that require recertification at each login.
- The Cisco NAC Appliance can automatically add devices to the certified list. These devices can be decertified at specified intervals.

CANAC v2.1—4-10

A user device must be certified to gain access to the network. Certified devices are devices that have successfully met your specified authentication and Cisco NAC Appliance requirements and are considered “clean” by your configured standards. When the device has met this criteria, the Cisco NAS automatically adds the MAC address of the device to the certified list and the device is considered clean until that device is removed from the list. Device recertification is not required as long as the MAC address of the device is on the certified list. For example, device recertification is not required if the user of the device logs out and accesses the network again as another user. Multiuser devices can be configured as floating devices that require recertification at each login. Devices that are automatically added to the certified list by Cisco NAC Appliance can be cleared manually or cleared automatically at specified intervals.



Configuring Device Certification

Consider these points when configuring device certification:

- Exempt devices that are manually added to the list must be manually removed.
- Use the Certified Devices Timer form to have devices removed from the certified list at regularly scheduled intervals.
- Removing devices from the certified list causes these three actions:
  1. Removes in-band clients from the In-Band Online Users list and logs them off the network.
  2. Removes out-of-band clients from the Out-of-Band Online Users list and closes their port.
  3. Forces client devices to repeat the Cisco NAC Appliance requirements at the next login.

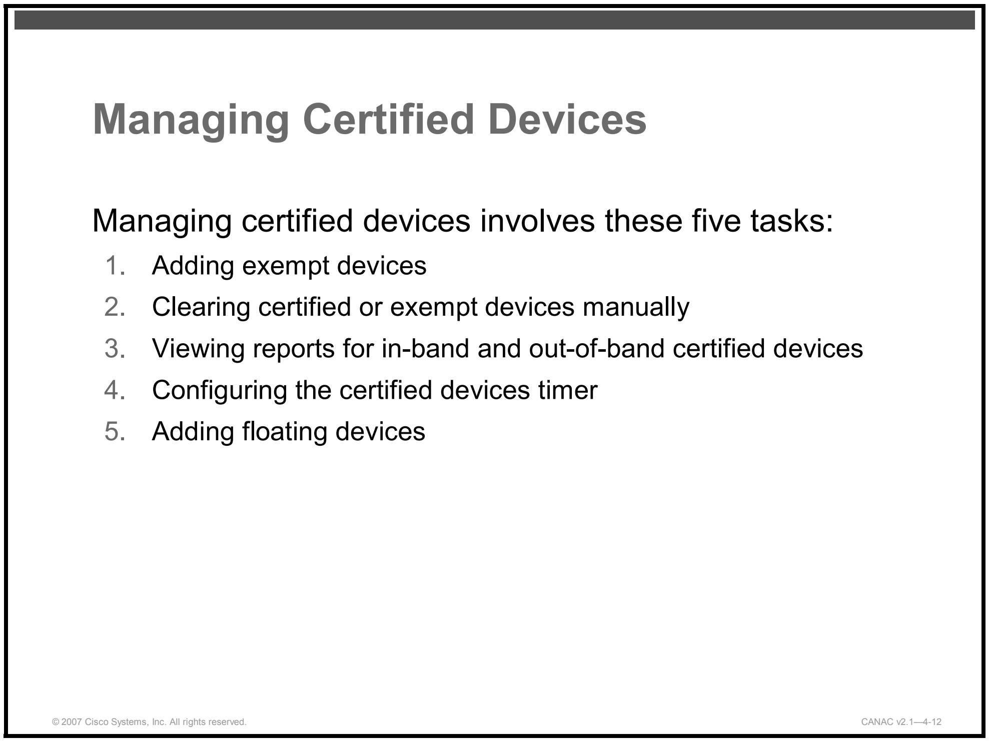
CANAC v2.1—4-11

There are several ways to control certification and decertification of devices using the Cisco NAC Appliance management console. When using the certified list, remember these points:

- Exempt devices that are manually added to the list must be manually removed.
- Use the global Certified Devices Timer form to clear the certified list at regularly scheduled intervals.

Note Exempt devices on the certified list are protected from being automatically removed when the global Certified Devices Timer form clears the certified list.

- Clearing devices from the certified list causes these three actions to occur:
  - — Removes in-band clients from the In-Band Online Users list and logs them off the network
  - — Removes out-of-band clients from the Out-of-Band Online Users list and closes their port
  - — Forces client devices to repeat the Cisco NAC Appliance requirements at the next login



Managing Certified Devices

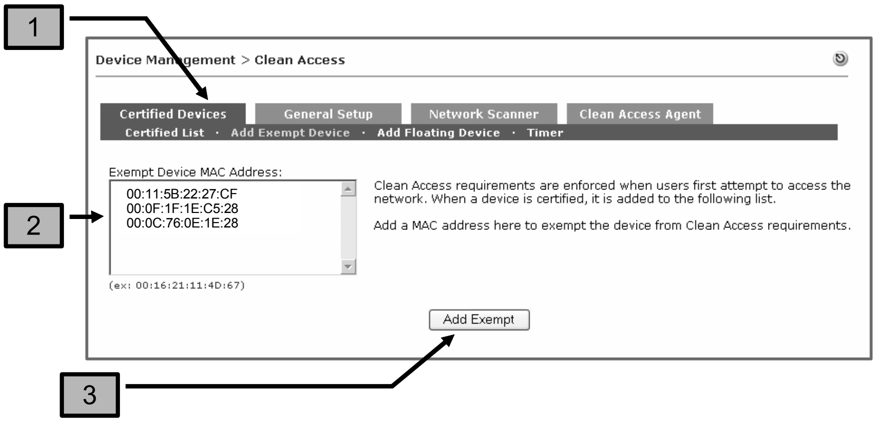
Managing certified devices involves these five tasks:

1. Adding exempt devices
2. Clearing certified or exempt devices manually
3. Viewing reports for in-band and out-of-band certified devices
4. Configuring the certified devices timer
5. Adding floating devices

CANAC v2.1—4-12

The figure summarizes the five tasks that you perform to manage certified devices. The remainder of this lesson provides details on how to manage certified devices using these five tasks.

Task 1: Adding Exempt Devices


1
2
3
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Certified List · Add Exempt Device · Add Floating Device · Timer
Add Exempt

Exempt Device MAC Address:

00:11:5B:22:27:CF
00:0F:1F:1E:C5:28
00:0C:76:0E:1E:28

(ex: 00:16:21:11:4D:67)

Clean Access requirements are enforced when users first attempt to access the network. When a device is certified, it is added to the following list.

Add a MAC address here to exempt the device from Clean Access requirements.

Next steps →

CANAC v2.1—4-13

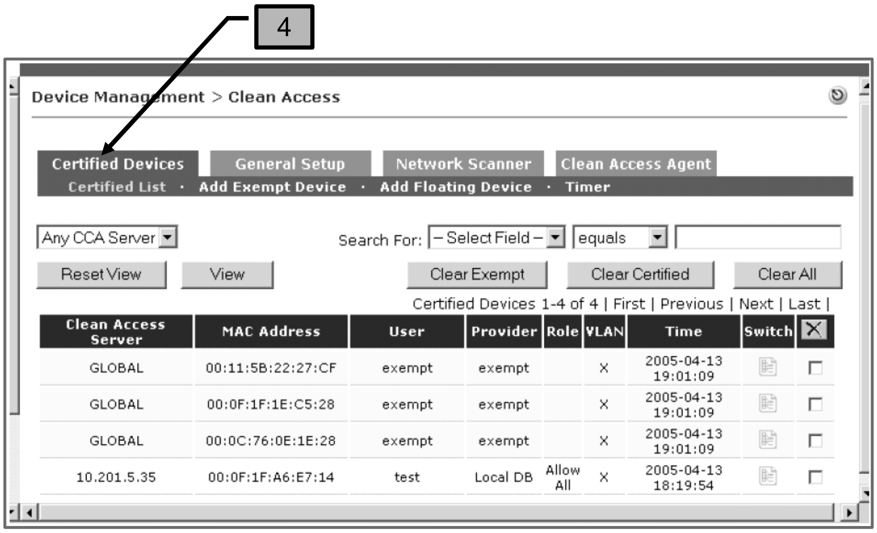
To begin managing certified devices, add exempt devices. Exempt devices are network appliances such as printers or phones. These three steps manually add exempt devices to the certified list:

Step 1 Choose **Device Management > Clean Access > Certified Devices > Add Exempt Device**.

Step 2 Enter the MAC address in the Exempt Device MAC Address field.

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

Task 1: Adding Exempt Devices (Cont.)



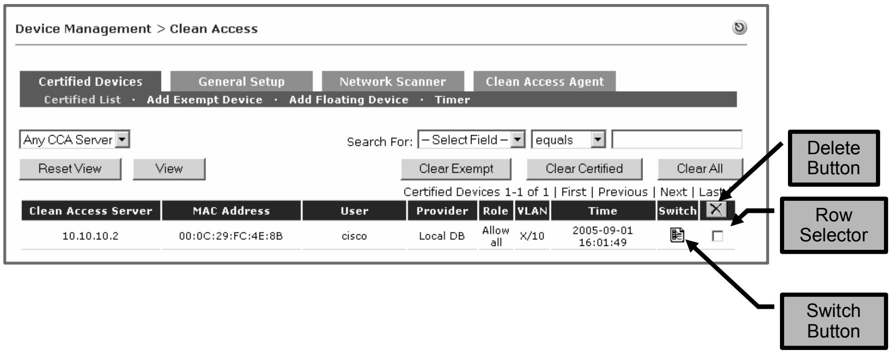
Device Management > Clean Access

Certified Devices 1-4 of 4 | First | Previous | Next | Last |

Clean Access Server	MAC Address	User	Provider	Role	VLAN	Time	Switch	☒
GLOBAL	00:11:5B:22:27:CF	exempt	exempt		X	2005-04-13 19:01:09		□
GLOBAL	00:0F:1F:1E:C5:28	exempt	exempt		X	2005-04-13 19:01:09		□
GLOBAL	00:0C:76:0E:1E:28	exempt	exempt		X	2005-04-13 19:01:09		□
10.201.5.35	00:0F:1F:A6:E7:14	test	Local DB	Allow All	X	2005-04-13 18:19:54		□

Step 4 The Certified List page appears listing the exempt devices.

Task 2: Clearing Certified or Exempt Devices Manually



Device Management > Clean Access

Certified Devices 1-1 of 1 | First | Previous | Next | Last

Clean Access Server	MAC Address	User	Provider	Role	VLAN	Time	Switch	☒
10.10.10.2	00:0C:29:FC:4E:8B	cisco	Local DB	Allow all	X/10	2005-09-01 16:01:49	🗎	□

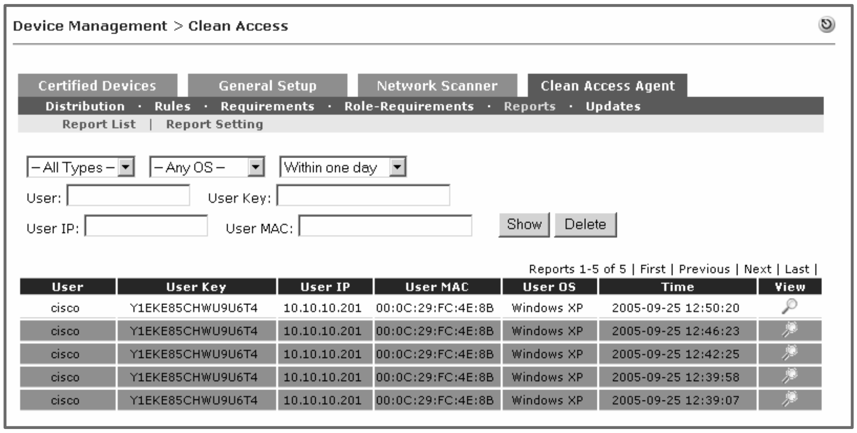
You can manually clear certified or exempt devices using the Certified List dialog box. The Certified List dialog box is found by choosing Device Management > Clean Access > Certified Devices > Certified List.

These four tasks are associated with clearing certified or exempt devices manually, and each task is specific to a different situation:

- To clear all MAC addresses that were added manually with the Add Exempt button, click the **Clear Exempt** button.
- To clear all MAC addresses that were added automatically by Cisco NAC Appliance, click the **Clear Certified** button.
- To clear MAC addresses of both exempt and certified devices, click the **Clear All** button.
- To clear individual addresses, select each address separately. Click the row selector found at the end of each MAC address row. To delete the selected addresses, click the **Delete** button.

Note The Switch column in the screen capture is not highlighted. The Switch column is made available for out-of-band users so that they can view switch information for out-of-band certified devices. Clicking the **Switch** button that is associated with a MAC address brings up a dialog box with the switch IP, port ID, and last update time of that MAC address. Refer to the View Switch Information for Out-of-Band Certified Devices section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Task 3: Viewing Reports for Certified Devices



Device Management > Clean Access

Reports 1-5 of 5 | First | Previous | Next | Last |

User	User Key	User IP	User MAC	User OS	Time	View
cisco	Y1EKE85CHWU9U6T4	10.10.10.201	00:0C:29:FC:4E:8B	Windows XP	2005-09-25 12:50:20	🔍
cisco	Y1EKE85CHWU9U6T4	10.10.10.201	00:0C:29:FC:4E:8B	Windows XP	2005-09-25 12:46:23	🔍
cisco	Y1EKE85CHWU9U6T4	10.10.10.201	00:0C:29:FC:4E:8B	Windows XP	2005-09-25 12:42:25	🔍
cisco	Y1EKE85CHWU9U6T4	10.10.10.201	00:0C:29:FC:4E:8B	Windows XP	2005-09-25 12:39:58	🔍
cisco	Y1EKE85CHWU9U6T4	10.10.10.201	00:0C:29:FC:4E:8B	Windows XP	2005-09-25 12:39:07	🔍

Orange backgrounds indicate clients who have failed system checking.

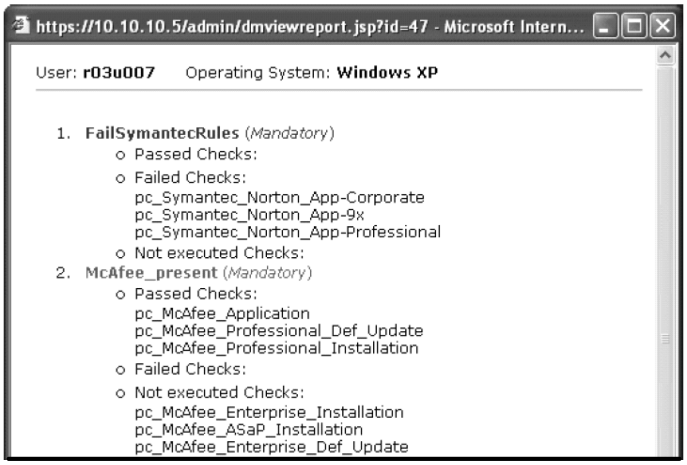
You can view a report of the results of previous Cisco NAA scans for certified devices. This report shows which requirements, rules, and checks succeeded or failed for an individual client. You can also generate a report of the results of previous network scans for certified devices. All out-of-band Cisco NAC Appliance users are provided with a list of the certified devices and can access a dialog box that lists the switch IP, port ID, and last update time of the client.

Note You can access the out-of-band report from the certified list. The in-band and out-of-band reports are found in different locations.

To learn more about Cisco NAA reporting options, refer to the Clean Access Agent Reports section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*. To learn more about the network scan reporting options, refer to the View Scan Reports section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

To view the results of previous Cisco NAA scans for certified devices, choose **Device Management > Clean Access > Clean Access Agent > Reports.** Click the **View** button to see which requirements, rules, and checks succeeded and which failed for an individual client.

Task 3: Viewing Reports for Certified Devices (Cont.)


https://10.10.10.5/admin/dmviewreport.jsp?id=47 - Microsoft Intern...

User: **r03u007** Operating System: **Windows XP**

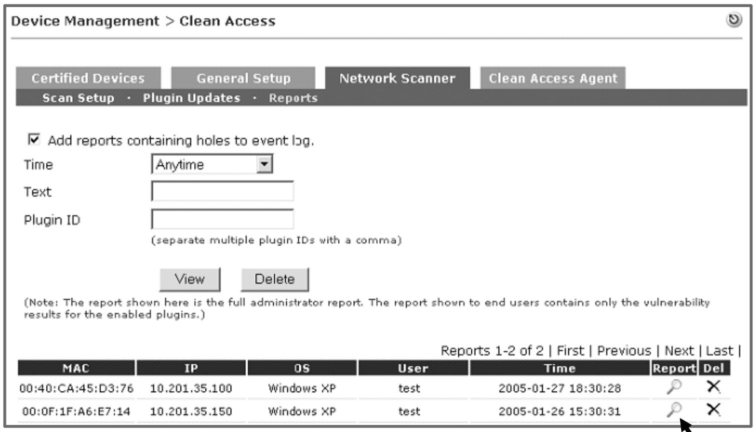
1. **FailSymantecRules** (*Mandatory*)
   - o Passed Checks:
   - o Failed Checks:
     pc_Symantec_Norton_App-Corporate
     pc_Symantec_Norton_App-9x
     pc_Symantec_Norton_App-Professional
   - o Not executed Checks:
2. **McAfee_present** (*Mandatory*)
   - o Passed Checks:
     pc_McAfee_Application
     pc_McAfee_Professional_Def_Update
     pc_McAfee_Professional_Installation
   - o Failed Checks:
   - o Not executed Checks:
     pc_McAfee_Enterprise_Installation
     pc_McAfee_ASaP_Installation
     pc_McAfee_Enterprise_Def_Update

Cisco NAA User Report

CANAC v2.1—4-17

The figure shows the Cisco NAA user report for a specific user, listing the status of each of the system checks that the Cisco NAA performs.

Task 3: Viewing Reports for Certified Devices (Cont.)



☑ Add reports containing holes to event lɔg.

Time: Anytime

Text:

Plugin ID:

(separate multiple plugin IDs with a comma)

(Note: The report shown here is the full administrator report. The report shown to end users contains only the vulnerability results for the enabled plugins.)

Reports 1-2 of 2 | First | Previous | Next | Last |

MAC	IP	OS	User	Time	Report	Del
00:40:CA:45:D3:76	10.201.35.100	Windows XP	test	2005-01-27 18:30:28	🔍	✕
00:0F:1F:A6:E7:14	10.201.35.150	Windows XP	test	2005-01-26 15:30:31	🔍	✕

Network Scanner Reports

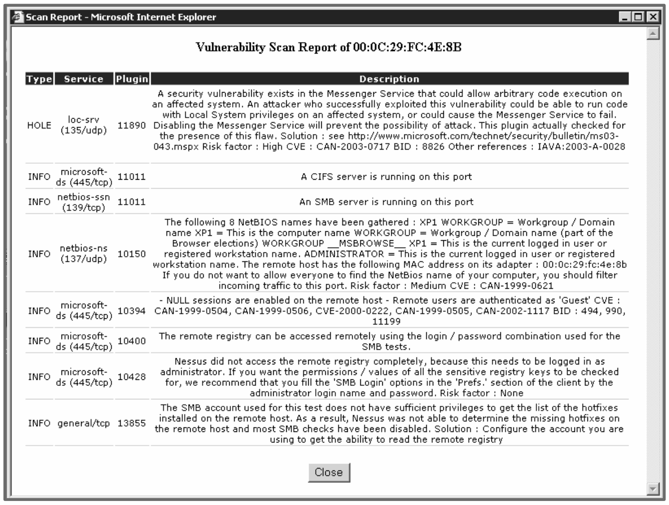
Report Buttons

CANAC v2.1—4-18

To view the results of previous network scans for certified devices, choose **Device Management > Clean Access > Network Scanner > Reports.** Click the **Report** button to see an individual scan report.

For details on the network scanner administrator report, refer to the View Scan Reports section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Task 3: Viewing Reports for Certified Devices (Cont.)



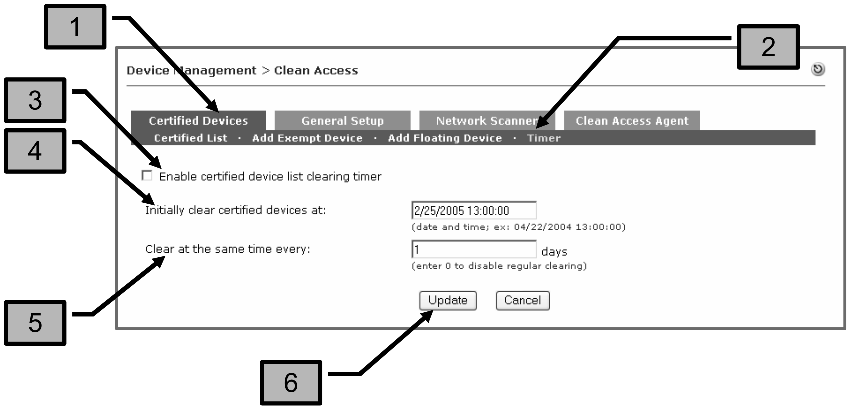
Vulnerability Scan Report of 00:0C:29:FC:4E:8B

Type	Service	Plugin	Description
HOLE	loc-srv (135/udp)	11890	A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack. This plugin actually checked for the presence of this flaw. Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-043.mspx Risk factor : High CVE : CAN-2003-0717 BID : 8826 Other references : IAVA:2003-A-0028
INFO	microsoft-ds (445/tcp)	11011	A CIFS server is running on this port
INFO	netbios-ssn (139/tcp)	11011	An SMB server is running on this port
INFO	netbios-ns (137/udp)	10150	The following 8 NetBIOS names have been gathered : XP1 WORKGROUP = Workgroup / Domain name XP1 = This is the computer name WORKGROUP = Workgroup / Domain name (part of the Browser elections) WORKGROUP __MSBROWSE__ XP1 = This is the current logged in user or registered workstation name. ADMINISTRATOR = This is the current logged in user or registered workstation name. The remote host has the following MAC address on its adapter : 00:0c:29:fc:4e:8b If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621
INFO	microsoft-ds (445/tcp)	10394	- NULL sessions are enabled on the remote host - Remote users are authenticated as 'Guest' CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117 BID : 494, 990, 11199
INFO	microsoft-ds (445/tcp)	10400	The remote registry can be accessed remotely using the login / password combination used for the SMB tests.
INFO	microsoft-ds (445/tcp)	10428	Nessus did not access the remote registry completely, because this needs to be logged in as administrator. If you want the permissions / values of all the sensitive registry keys to be checked for, we recommend that you fill the 'SMB Login' options in the 'Prefs.' section of the client by the administrator login name and password. Risk factor : None
INFO	general/tcp	13855	The SMB account used for this test does not have sufficient privileges to get the list of the hotfixes installed on the remote host. As a result, Nessus was not able to determine the missing hotfixes on the remote host and most SMB checks have been disabled. Solution : Configure the account you are using to get the ability to read the remote registry

Network Scanner Administrator Report

The figure shows a network scanner administrator report detailing the type, service, plug-in, and a description of the vulnerabilities that were found on a client.

Task 4: Configuring the Certified Devices Timer


1
2
3
4
5
6
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Certified List · Add Exempt Device · Add Floating Device · Timer
Update
Cancel

□ Enable certified device list clearing timer

Initially clear certified devices at: 2/25/2005 13:00:00
(date and time; ex: 04/22/2004 13:00:00)

Clear at the same time every: 1 days
(enter 0 to disable regular clearing)

The Certified Devices Timer form is where you set the parameters for clearing the global certified device list. The timer is configured with a specified startup time for the first cleansing of the global certified device list. You can configure the timer to clear the global certified device list at regular intervals.

Note The procedure enabled by the Certified Devices Timer form is an automatic process that clears only those devices added to the certified list by Cisco NAC Appliance. This form does not clear exempt devices, which are manually added to the certified list.

Clearing the certified device list on a timed basis requires these six steps:

Step 1 Choose **Device Management > Clean Access > Certified Devices**.

Step 2 Click the **Timer** submenu link.

Step 3 Check the **Enable Certified Device List Clearing Timer** check box.

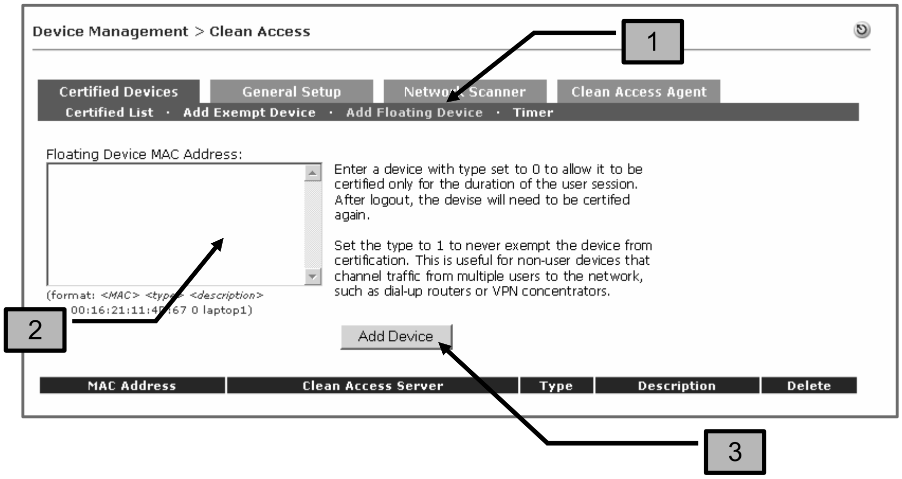
Step 4 In the Initially Clear Certified Devices At field, specify the time at which the devices should initially be cleared. Use the format mm/dd/yyyy hour:min:sec.

Step 5 To have the list cleared regularly after the initial clearing, enter an interval in number of days in the Clear at the Same Time Every field.

Step 6 Click the **Update** button.

Note The next scheduled clearing time appears at the bottom of the page.

Task 5: Adding Floating Devices


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Certified List · Add Exempt Device · Add Floating Device · Timer
Floating Device MAC Address:
(format: <MAC> <type> <description>
00:16:21:11:4[illegible]:67 0 laptop1)
Add Device
MAC Address
Clean Access Server
Type
Description
Delete
1
2
3

Enter a device with type set to 0 to allow it to be certified only for the duration of the user session. After logout, the devise will need to be certifed again.

Set the type to 1 to never exempt the device from certification. This is useful for non-user devices that channel traffic from multiple users to the network, such as dial-up routers or VPN concentrators.

A floating device is certified only for the duration of a user session. When the user logs out, the next user of the device needs to be certified. Floating devices are useful for managing shared equipment, such as kiosk computers or wireless cards that are loaned by a library.

In addition to session-length certification, you can configure devices that are never certified. For example, you can configure a dial-up router that channels multiuser traffic from the side of the network that is not trusted as a floating device that is never certified. For virus protection purposes, each user accessing the network through the device is treated individually.

Caution In this example, if the router is certified and performs Network Address Translation (NAT) services, the users are indistinguishable to the Cisco NAM. Consequently, only the first user is certified, leaving additional users exempt from certification. The Cisco NAA is not designed to be installed behind routers or dial-up routers and does not work if it is installed in this way.

Note Some tasks that are associated with managing certified devices can also be performed at the local level for an individual Cisco NAS. For more information on these tasks, refer to the Implementing Clean Access section in the *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*.

To configure a floating device, complete these steps:

Step 1 Choose **Device Management** > **Clean Access** > **Certified Devices** > **Add Floating Device.**

Step 2 In the Floating Device MAC Address field, enter the MAC address of the device that you are adding. Use line breaks to separate multiple addresses. Type the address in the following form:

- <MAC> <type> <description>
  Where <MAC> is the MAC address of the device, <type> is either 0 for session-scope certification or 1 if the device should never be considered certified, and <description> is an optional description of the device.

Tip Include spaces between each element and use line breaks to separate multiple entries. For example:

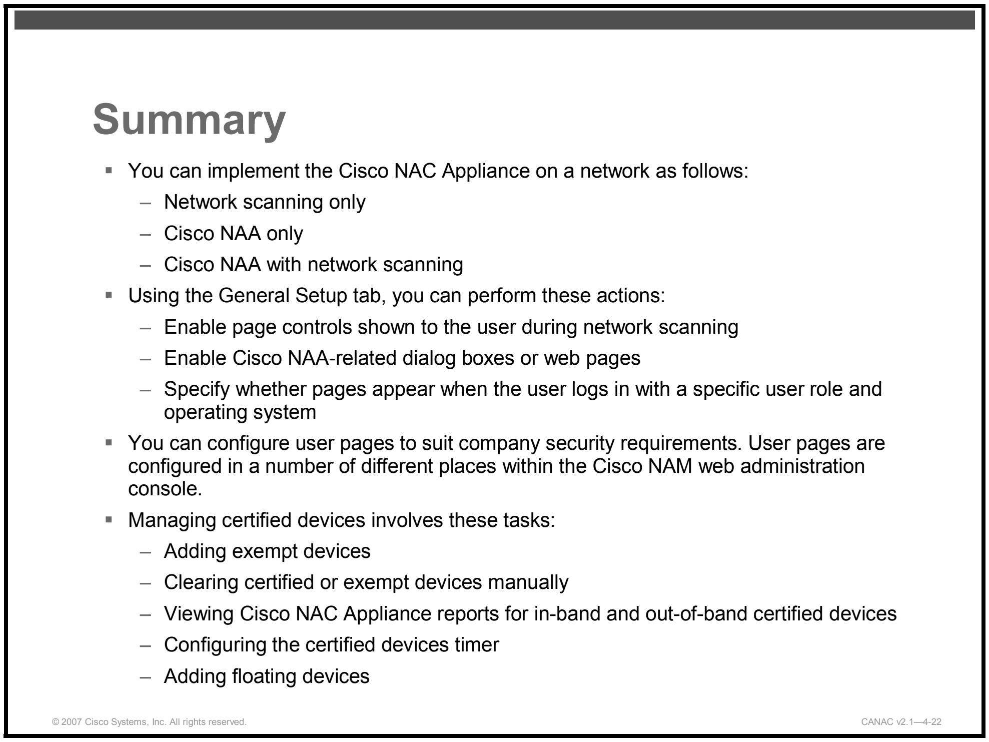
```
00:16:21:23:4D:67 0 LibCard1
00:16:34:21:4C:68 0 LibCard2
00:16:11:12:4A:71 1 Router1
```

Step 3 Click the **Add Device** button to save the setting.

Note To remove a floating device, click the **Delete** icon at the bottom of the form for the MAC address of the device.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- You can implement the Cisco NAC Appliance on a network as follows:
  - Network scanning only
  - Cisco NAA only
  - Cisco NAA with network scanning
- Using the General Setup tab, you can perform these actions:
  - Enable page controls shown to the user during network scanning
  - Enable Cisco NAA-related dialog boxes or web pages
  - Specify whether pages appear when the user logs in with a specific user role and operating system
- You can configure user pages to suit company security requirements. User pages are configured in a number of different places within the Cisco NAM web administration console.
- Managing certified devices involves these tasks:
  - Adding exempt devices
  - Clearing certified or exempt devices manually
  - Viewing Cisco NAC Appliance reports for in-band and out-of-band certified devices
  - Configuring the certified devices timer
  - Adding floating devices

Lesson 2

Implementing Network Scanning

Overview

Companies must identify vulnerabilities in the end-user network system and provide web-based feedback to users with vulnerable systems so that the users are made aware of the threat that they pose. In a Cisco Network Admission Control (NAC) Appliance implementation, the network scanning feature allows companies to identify vulnerabilities and provide feedback. This lesson describes how to implement network scanning in the Cisco NAC Appliance Manager (Cisco NAM).

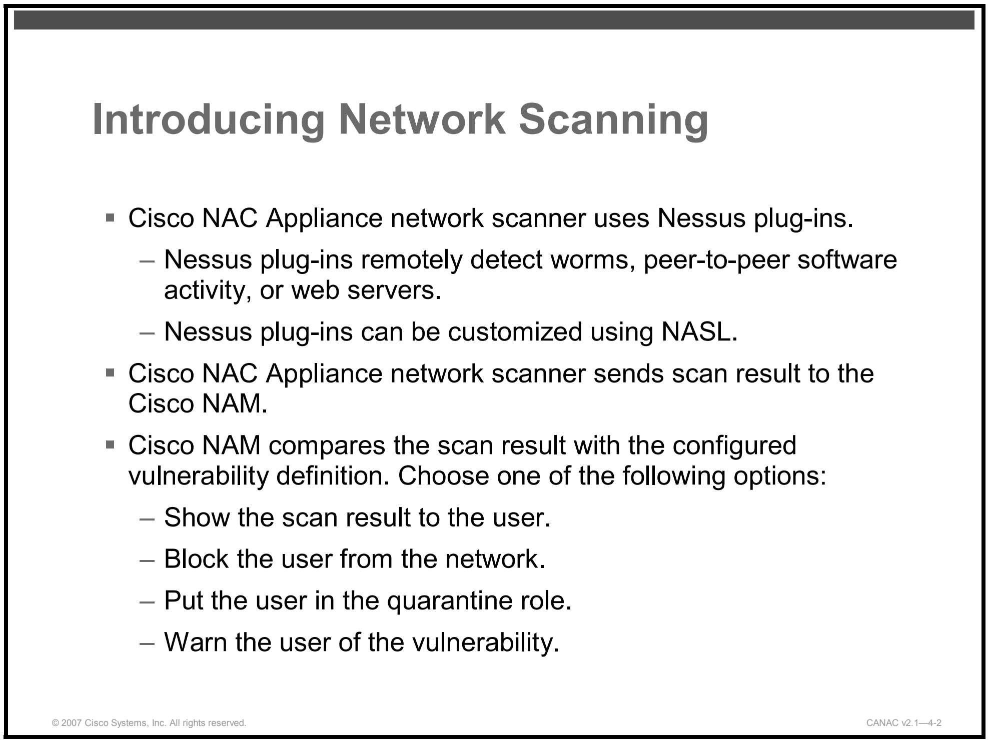
Objectives

Upon completing this lesson, you will be able to configure the Cisco NAC Appliance network scanner to use Nessus plug-ins to check for security vulnerabilities. This ability includes being able to meet these objectives:

- Describe the steps that are needed to configure the Cisco NAC Appliance network scanner to use Nessus plug-ins
- Describe how to configure the quarantine role
- Describe how to implement Nessus plug-ins into the Cisco NAM repository
- Describe how to test a network scanning configuration
- Describe how to customize the User Agreement page
- Describe how to view scan reports

Introducing Network Scanning

This topic describes the steps that are needed to configure the Cisco NAC Appliance network scanner to use Nessus plug-ins and to implement Cisco NAC Appliance network scanning.



Introducing Network Scanning

- Cisco NAC Appliance network scanner uses Nessus plug-ins.
  - Nessus plug-ins remotely detect worms, peer-to-peer software activity, or web servers.
  - Nessus plug-ins can be customized using NASL.
- Cisco NAC Appliance network scanner sends scan result to the Cisco NAM.
- Cisco NAM compares the scan result with the configured vulnerability definition. Choose one of the following options:
  - Show the scan result to the user.
  - Block the user from the network.
  - Put the user in the quarantine role.
  - Warn the user of the vulnerability.

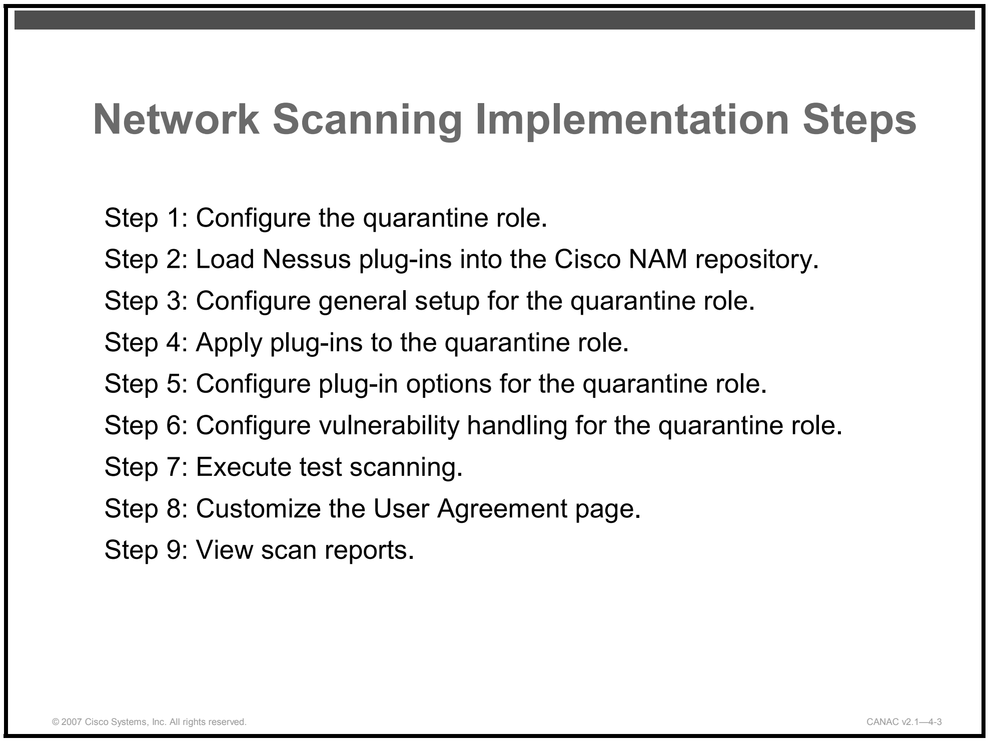
© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-2

The Cisco NAC Appliance network scanner uses Nessus plug-ins to check for security vulnerabilities. There are currently more than 8000 different Nessus plug-ins that check for both local and remote system flaws. In addition to plug-ins that detect the presence of particular worms, plug-ins monitor peer-to-peer software activity and web servers. You can use any standard Nessus plug-in with Cisco NAC Appliance. You can also customize plug-ins or create your own plug-ins using the Nessus Attack Scripting Language (NASL). Using Nessus plug-ins with Cisco NAC Appliance allows you to define and implement automatic, immediate responses to scan results.

The Cisco NAC Appliance network scanner analyzes the client system using the Nessus plug-ins that you select. The Nessus plug-ins produce a standard report containing the results of the scan, and the report is sent to the Cisco NAM. This scanning report indicates if the scan resulted in finding a security hole, issuing a warning or listing system information. The Cisco NAM then interprets the report by comparing the report results to the vulnerability definition that you configured for the Cisco NAM. If the report result matches the result that you classified as a vulnerability, the event is logged and these options are available:

- Show the result of the scan to the user.
- Block the user from the network.
- Put the user in the quarantine role for limited access until the client system no longer displays vulnerabilities.
- Warn the user of the vulnerability by displaying the User Agreement page.

Note Tenable Network Security is the owner, sole developer, and licensor for the Nessus Open-Source Scanner source code. The Nessus Open-Source Scanner source code is managed by Nessus and is an open-source project for network security-related software.



Network Scanning Implementation Steps

Step 1: Configure the quarantine role.

Step 2: Load Nessus plug-ins into the Cisco NAM repository.

Step 3: Configure general setup for the quarantine role.

Step 4: Apply plug-ins to the quarantine role.

Step 5: Configure plug-in options for the quarantine role.

Step 6: Configure vulnerability handling for the quarantine role.

Step 7: Execute test scanning.

Step 8: Customize the User Agreement page.

Step 9: View scan reports.

CANAC v2.1—4-3

Follow these steps to implement network scanning:

Step 1 Configure the quarantine role as follows:

- Create additional quarantine roles.
- Set session timeout.
- Configure traffic control policies.

Step 2 Load Nessus plug-ins into the Cisco NAM repository.

Step 3 Configure general setup for the quarantine role.

Step 4 Apply plug-ins to the quarantine role.

Step 5 Configure plug-in options for the quarantine role.

Step 6 Configure vulnerability handling for the quarantine role.

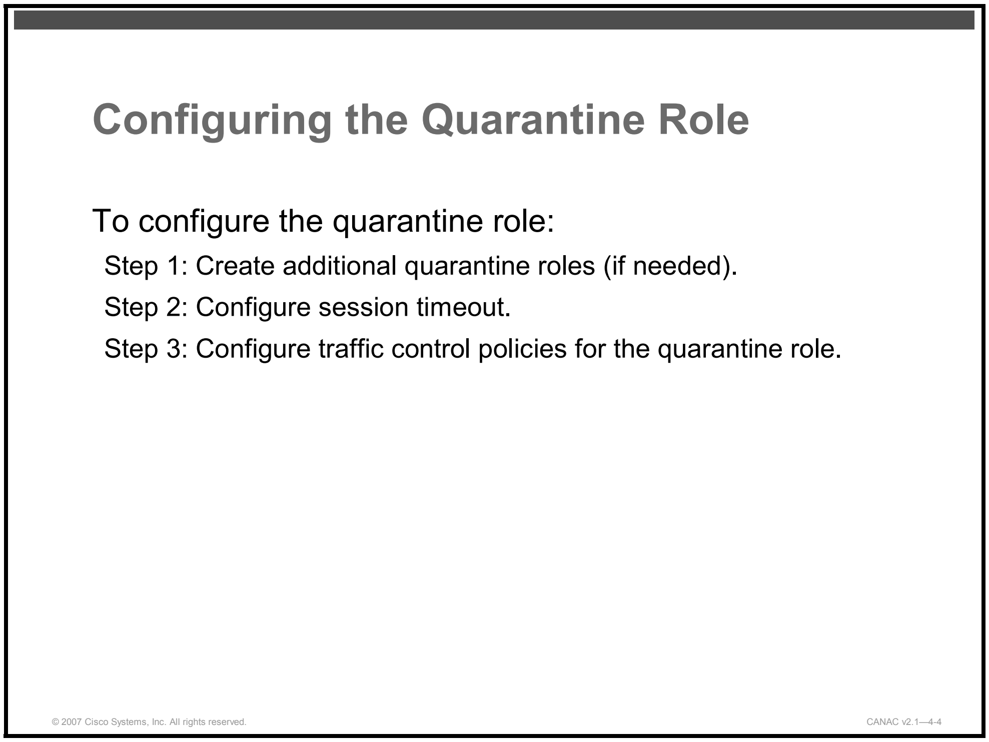
Step 7 Execute test scanning.

Step 8 Customize the User Agreement page.

Step 9 View the scan reports.

Configuring the Quarantine Role

This topic describes how to configure the quarantine role.



Configuring the Quarantine Role

To configure the quarantine role:

Step 1: Create additional quarantine roles (if needed).

Step 2: Configure session timeout.

Step 3: Configure traffic control policies for the quarantine role.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-4

Cisco NAC Appliance can assign a user to a quarantine role if a vulnerability is discovered in the client system. Quarantining a vulnerable user is an option. Alternatives to quarantine include blocking the user or providing the user with a warning. The quarantine role is a mechanism that gives the user temporary network access while the user workstation is being correctly configured. Follow these three steps to configure the quarantine role:

Step 1 **Create additional quarantine roles if needed.** The system provides one default quarantine role that needs to be configured with traffic policies. If additional quarantine roles are needed, you can define them at the User Management > User Roles > New Role menu.

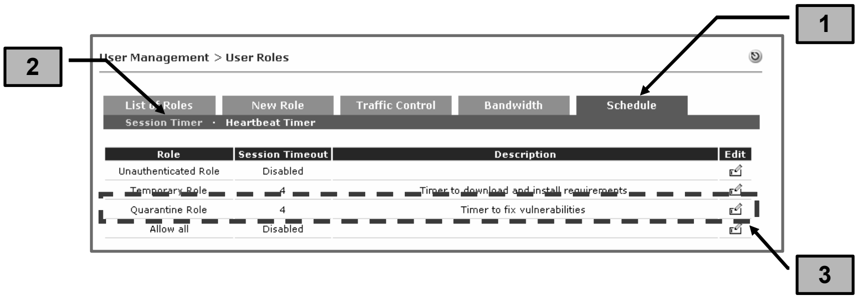
Step 2 **Set session timeout.** The system default quarantine role has a session timeout of 4 minutes. You can set the session timeout for a role by accessing the User Management > User Roles > Schedule > Session Timer menu. Set the session timeout parameters to a small value. A small session timeout value helps the Cisco NAC Appliance Server (Cisco NAS) detect and disconnect users who have restarted their computers without logging out of the network. This initial session timeout value is typically refined later as you determine how much time that you need to perform test scans and to download the required software.

Step 3 **Configure traffic control policies.** You can configure the traffic control policies for the new quarantine role from the User Management > User Roles > List of Roles menu, or from the Traffic Control tab by choosing the quarantine role from the drop-down menu. You must add a new IP-based policy and reconfigure trusted policies to conform to this new role. The trusted policies that you need depend on whether you are providing required software installation files or whether you want users to correct their systems using external sources, such as the Windows Update page. You can also add a local, host-based policy.

Note	A local, host-based traffic control policy for a Cisco NAS takes precedence over a global policy for all Cisco NASs if the local policy is given higher priority.

After you configure the quarantine role, apply the role to users by selecting this role as their quarantine role in the Block/Quarantine Users with Vulnerabilities in Role option of the General Setup tab. After configuring this role, you can load the scan plug-ins into the Cisco NAM repository, as described in the next topic.

Configuring the Quarantine Role–Configure Session Timeout



Role	Session Timeout	Description	Edit
Unauthenticated Role	Disabled		✎
Temporary Role	4	Timer to download and install requirements	✎
Quarantine Role	4	Timer to fix vulnerabilities	✎
Allow all	Disabled		✎

Next steps →

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-5

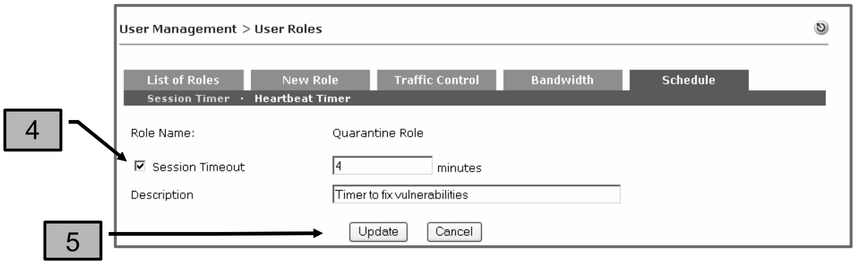
These five steps are used to configure the session timeout for a given quarantine role:

Step 1 Choose **User Management > User Roles** and click the **Schedule** tab.

Step 2 Click the **Session Timer** option to view a list of roles.

Step 3 Choose the role that you want by clicking **Edit** at the end of the line next to the desired quarantine role. This opens the Session Timer form.

Configuring the Quarantine Role– Configure Session Timeout (Cont.)



Role Name: Quarantine Role

☑ Session Timeout 4 minutes

Description Timer to fix vulnerabilities

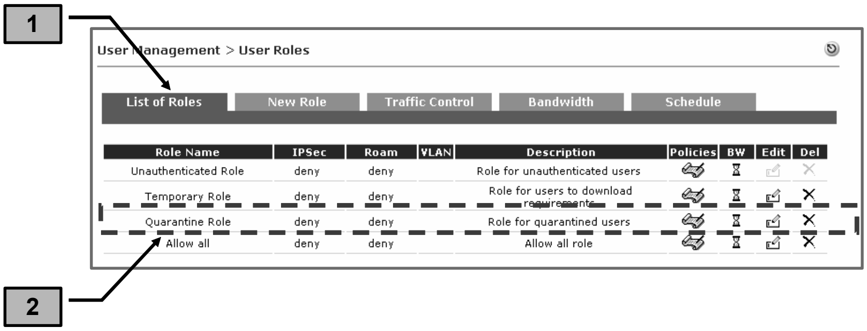
CANAC v2.1—4-6

Step 4 In the Session Timer form, complete these tasks:

- Check the **Session Timeout** check box.
- Enter the number of minutes that you want the user session to last. Choose an amount that allows the user enough time to download the files that are needed to correct problems in the system.
- Optionally, enter a description for the session timeout requirement. An example of a description that you can use is "heartbeat timer."

Step 5 Click the **Update** button. The timeout value that you have entered appears in the session timeout column next to the role in the List of Roles tab.

Configuring the Quarantine Role–Configure Traffic Control Policies for the Quarantine Role



User Management > User Roles

Role Name	IPSec	Roam	VLAN	Description	Policies	BW	Edit	Del
Unauthenticated Role	deny	deny		Role for unauthenticated users				×
Temporary Role	deny	deny		Role for users to download requirements				×
Quarantine Role	deny	deny		Role for quarantined users				×
Allow all	deny	deny		Allow all role				×

Next steps →

CANAC v2.1—4-7

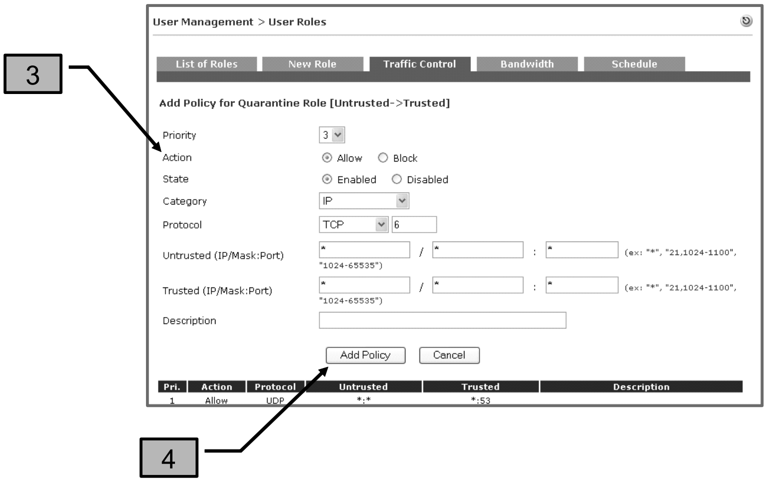
Follow these four steps to configure traffic control policies for a given quarantine role:

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

Step 2 Click the **Policies** icon next to the desired role. The Traffic Control > IP form appears (not shown in the figure). Click the **Add Policy** link next to the new role. A new IP-based policy for the selected role is now ready to be configured.

Note Alternately, you can click the **Traffic Control** tab, choose the appropriate quarantine role from the drop-down menu, and click **Select**.

Configuring the Quarantine Role–Configure Traffic Control Policies for the Quarantine Role (Cont.)



User Management > User Roles

List of Roles | New Role | Traffic Control | Bandwidth | Schedule

Add Policy for Quarantine Role [Untrusted->Trusted]

Priority: 3
Action: ● Allow ○ Block
State: ● Enabled ○ Disabled
Category: IP
Protocol: TCP 6
Untrusted (IP/Mask:Port): * / * : * (ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port): * / * : * (ex: "*", "21,1024-1100", "1024-65535")
Description:

Add Policy | Cancel

Pri.	Action	Protocol	Untrusted	Trusted	Description
1	Allow	UDP	*:*	*:53	

CANAC v2.1—4-8

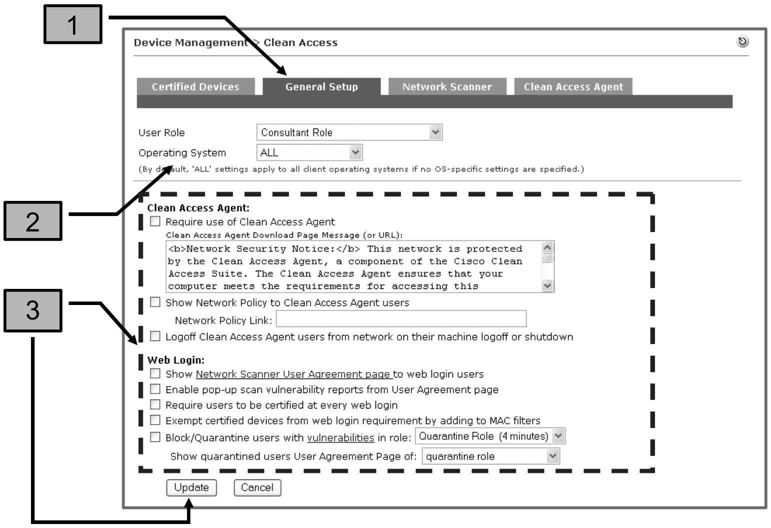
Step 3 Now that a new policy is added, the policy must be configured. Configure both untrusted and trusted policies as follows:

- If you are providing required software installation files for the Cisco NAM to reference, set up a policy that allows the role access to port 80 of the Cisco NAM. Include the IP address and subnet mask of the Cisco NAM in the policy. If you are providing required software installation files from the Cisco NAM (for example, via the network scanning Vulnerabilities page), set up an Untrusted-Trusted IP-based traffic policy that allows the quarantine role access to port 80 (HTTP), port 443 (secure HTTP [HTTPS]), or both ports of the Cisco NAM (for example, 10.201.240.11/255.255.255.255:80).

- If you want users to correct the user system using external sources, such as the Windows Update page, set up permissions for accessing web resources.

Step 4 Click **Add Policy**.

Configuring General Setup



Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent

User Role: Consultant Role

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Clean Access Agent:

☐ Require use of Clean Access Agent

Clean Access Agent Download Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
by the Clean Access Agent, a component of the Cisco Clean
Access Suite. The Clean Access Agent ensures that your
computer meets the requirements for accessing this
```

☐ Show Network Policy to Clean Access Agent users

Network Policy Link:

☐ Logoff Clean Access Agent users from network on their machine logoff or shutdown

Web Login:

☐ Show Network Scanner User Agreement page to web login users

☐ Enable pop-up scan vulnerability reports from User Agreement page

☐ Require users to be certified at every web login

☐ Exempt certified devices from web login requirement by adding to MAC filters

☐ Block/Quarantine users with vulnerabilities in role: Quarantine Role (4 minutes)

Show quarantined users User Agreement Page of: quarantine role

Update Cancel

The General Setup tab allows you to enable the various warning pages that pop up as the client system proceeds through Cisco NAC Appliance certification.

Follow these three steps to configure network scanning user page options on the General Setup tab:

Step 1 Choose **Device Management > Clean Access** and click the **General Setup** tab. Scanning must be configured for both the user role and the operating system of a user. Choose the desired role from the User Role drop-down box.

Step 2 From the Operating System drop-down box, choose the operating system that the configuration applies to.

Note The ALL setting applies to a client system if a configuration for the specific version of that user operating system does not exist. To provide specialized settings, choose the operating system and clear the check box for the ALL setting..

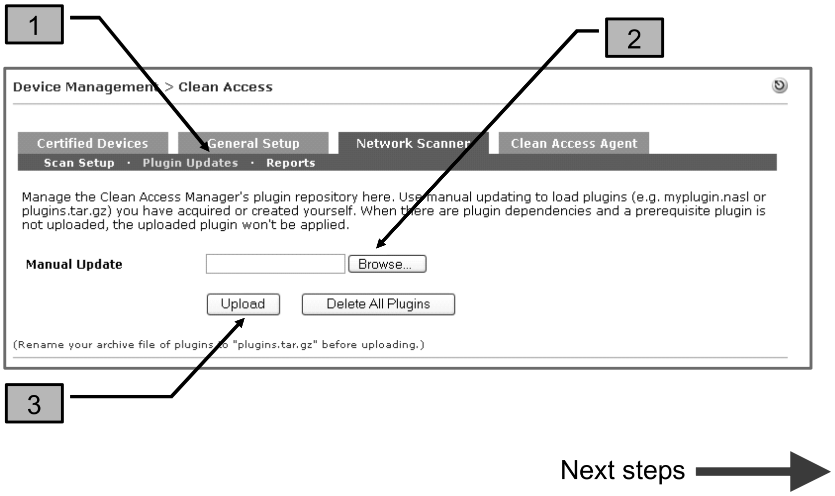
Step 3 Configure the General Setup tab options as desired. When you are finished, click **Update** to save your changes. Some of the options available, and those typically enabled for network scanning, are as follows:

- Show Network Scanner User Agreement Page to Web Login Users.
- Enable Pop-Up Scan Vulnerability Reports from User Agreement Page.
- Block/Quarantine Users with Vulnerabilities in Role (role to be specified). You can choose Block Access from the drop-down box to block the user from the network and to modify the contents (if desired) of the blocked access page that appears.

Implementing Nessus Plug-Ins

This topic describes how to implement Nessus plug-ins into the Cisco NAM repository.

Loading Nessus Plug-Ins Manually



Manage the Clean Access Manager's plugin repository here. Use manual updating to load plugins (e.g. myplugin.nasl or plugins.tar.gz) you have acquired or created yourself. When there are plugin dependencies and a prerequisite plugin is not uploaded, the uploaded plugin won't be applied.

(Rename your archive file of plugins to "plugins.tar.gz" before uploading.)

CANAC v2.1—4-10

When the Cisco NAM is first installed, its Nessus scan plug-in repository is empty. You must manually load plug-ins that you have created or downloaded from the Nessus website to the Nessus scan plug-in repository in the Cisco NAM. After Nessus plug-ins are loaded, the plug-ins are automatically published from the Cisco NAM repository to the Cisco NASs. The Cisco NASs then perform the scan on user machines. If the Cisco NAM determines that the Cisco NAS version of the plug-in set is different from the Cisco NAM version of the plug-in, the Cisco NAM will distribute this plug-in set to the Cisco NASs when the Cisco NASs start up.

Tip When you add a new plug-in, be sure to check for dependencies that the plug-in may have. Ensure that you load all other plug-ins that your new plug-in depends on. The Cisco NAS will automatically use the dependent plug-ins when the new plug-in is used.

Follow these four steps to manually load Nessus plug-ins:

Step 1 Choose **Device Management** > **Clean Access** > **Network Scanner** > **Plugin Updates**.

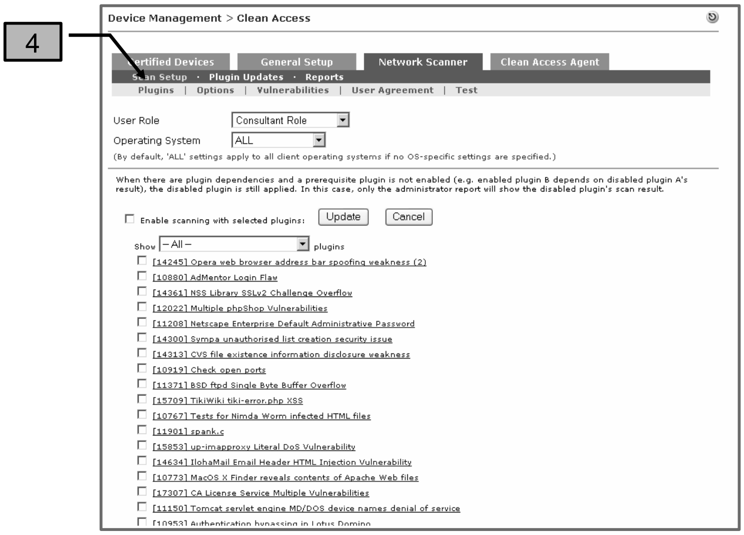
Step 2 Click the **Browse** button next to the Manual Update field and navigate to the plug-in file that you want to add. In order to do this, the plug-in file must be in a location that is accessible to the computer that is loading the plug-in file.

Note Nessus plug-in files have extensions such as myplug-in.nasl or plug-ins.tar.gz.

Step 3 Click the **Upload** button.

Note When you need to delete plug-ins, do so from the dialog box found at Device Management > Clean Access > Network Scanner > Plugin Updates. Click the **Delete All Plugins** button to remove all plug-ins from the Nessus scan plug-in repository.

Loading Nessus Plug-Ins Manually (Cont.)


4
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: Consultant Role

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

When there are plugin dependencies and a prerequisite plugin is not enabled (e.g. enabled plugin B depends on disabled plugin A's result), the disabled plugin is still applied. In this case, only the administrator report will show the disabled plugin's scan result.

□ Enable scanning with selected plugins: Update Cancel

Show – All – plugins

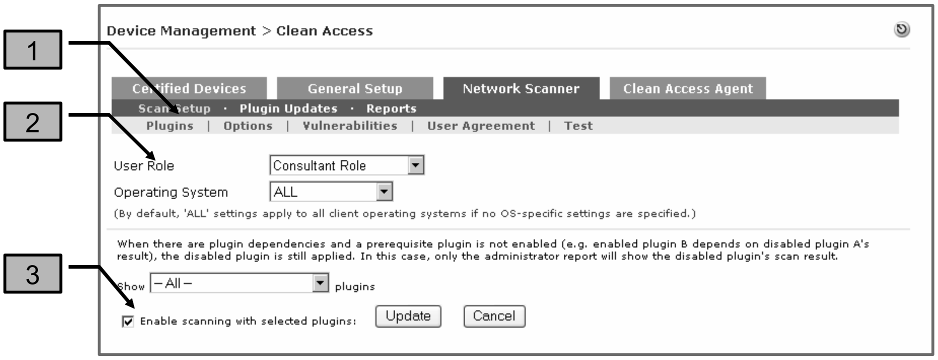
- □ [14245] Opera web browser address bar spoofing weakness (2)
- □ [10880] AdMentor Login Flaw
- □ [14361] NSS Library SSLv2 Challenge Overflow
- □ [12022] Multiple phpShop Vulnerabilities
- □ [11208] Netscape Enterprise Default Administrative Password
- □ [14300] Sympa unauthorised list creation security issue
- □ [14313] CVS file existence information disclosure weakness
- □ [10919] Check open ports
- □ [11371] BSD ftpd Single Byte Buffer Overflow
- □ [15709] TikiWiki tiki-error.php XSS
- □ [10767] Tests for Nimda Worm infected HTML files
- □ [11901] spank.c
- □ [15853] up-imapproxy Literal DoS Vulnerability
- □ [14634] IlohaMail Email Header HTML Injection Vulnerability
- □ [10773] MacOS X Finder reveals contents of Apache Web files
- □ [17307] CA License Service Multiple Vulnerabilities
- □ [11150] Tomcat servlet engine MD/DOS device names denial of service
- □ [10953] Authentication bypassing in Lotus Domino

CANAC v2.1—4-11

Step 4 Click **Scan Setup** in the Network Scanner tab. The list of plug-ins that were loaded to the repository appears here.

Note Use this dialog box to verify that all plug-ins have been deleted after clicking the **Delete All Plugins** button.

Applying Plug-Ins


1
2
3
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
Update
Cancel

User Role: Consultant Role

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

When there are plugin dependencies and a prerequisite plugin is not enabled (e.g. enabled plugin B depends on disabled plugin A's result), the disabled plugin is still applied. In this case, only the administrator report will show the disabled plugin's scan result.

Show – All – plugins

☑ Enable scanning with selected plugins:

Next steps →

CANAC v2.1—4-12

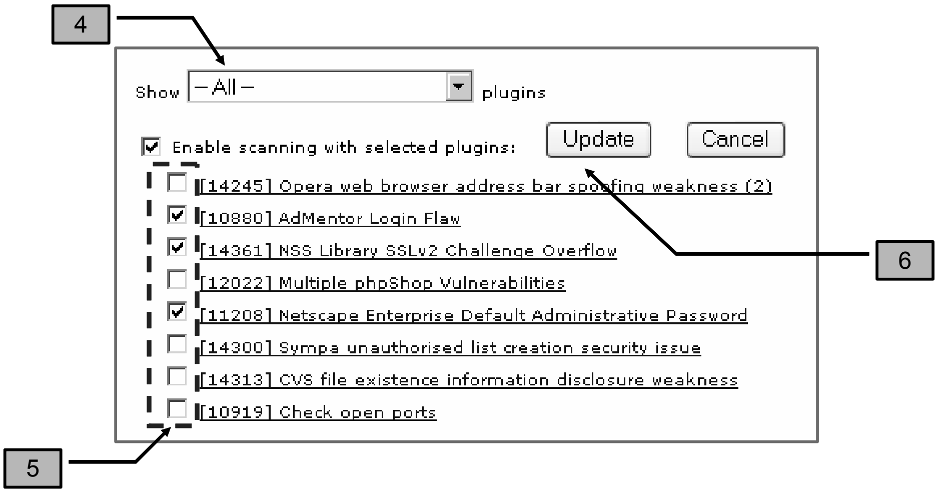
Follow these six steps to apply plug-ins that are used to scan a specified user role and operating system:

Step 1 Choose the **Network Scanner > Scan Setup > Plugins** form.

Step 2 Choose a **User Role** and **Operating System** that the plug-in applies to.

Step 3 Check the **Enable Scanning with Selected Plugins** check box.

Applying Plug-Ins (Cont.)



Show – All – plugins

☑ Enable scanning with selected plugins:

☐ [14245] Opera web browser address bar spoofing weakness (2)
☑ [10880] AdMentor Login Flaw
☑ [14361] NSS Library SSLv2 Challenge Overflow
☐ [12022] Multiple phpShop Vulnerabilities
☑ [11208] Netscape Enterprise Default Administrative Password
☐ [14300] Sympa unauthorised list creation security issue
☐ [14313] CVS file existence information disclosure weakness
☐ [10919] Check open ports

Step 4 Choose **All** in the Show drop-down menu to display all available plug-ins in the Nessus scan plug-in repository.

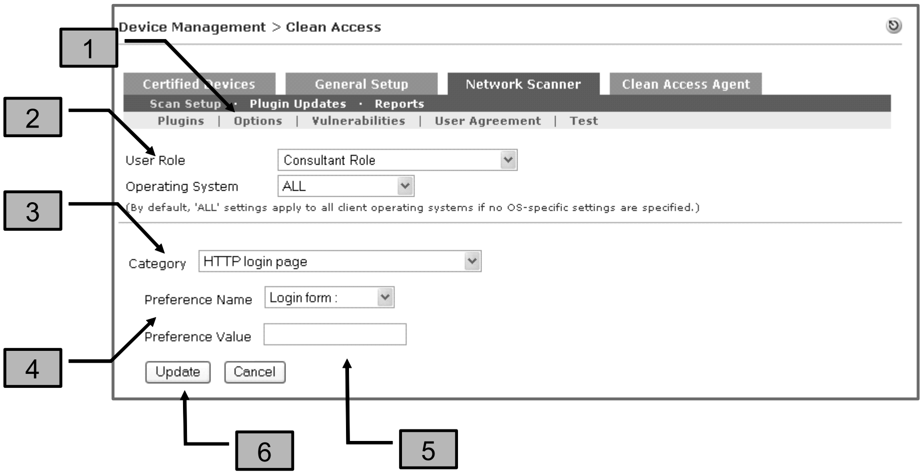
Note If you have many plug-ins in the repository, you can filter which options appear by choosing a plug-in family from the plug-ins list. For example, choosing Selected in the Show Drop-down Menu displays only the plug-ins that you have selected and enabled for the specified role.

Step 5 Check the check box for each plug-in that you want to incorporate into the scan for the selected role.

Note To review the details of a plug-in, click the individual plug-in name. If the plug-in is dependent on other plug-ins in the repository, the other plug-ins are enabled automatically.

Step 6 When all the needed plug-ins are selected, click **Update**. This action transfers the selected plug-ins to the Vulnerabilities page. You can now configure how vulnerabilities are handled when vulnerabilities are discovered on a client system.

Configuring Plug-In Options



Device Management > Clean Access

User Role: Consultant Role

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Category: HTTP login page

Preference Name: Login form :

Preference Value:

Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
Update
Cancel
1
2
3
4
5
6

CANAC v2.1—4-14

Some plug-ins support input parameters. After you enable such a plug-in, you can configure the input parameters in the Options form.

Follow these six steps to configure plug-in parameter options**:**

Step 1 In the Network Scanner tab, click **Scan Setup > Options** to display the Options form.

Step 2 Choose the desired user role and operating system from the User Role drop-down menu and the Operating System drop-down menu.

Step 3 Choose the plug-in that you want to configure from the Category drop-down menu. All plug-ins enabled for the selected user role appear in the list.

Step 4 Choose the option that you want to configure for the plug-in from the Preference Name drop-down menu.

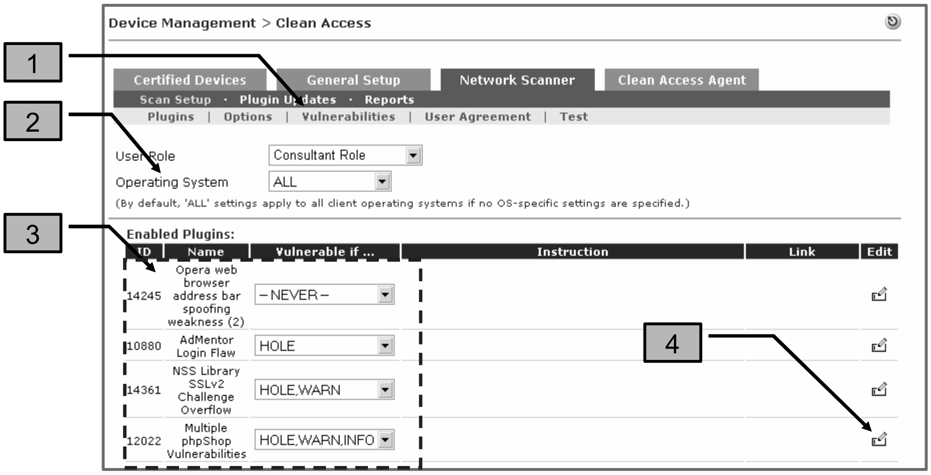
Step 5 A parameter text box appears to the right of the option that you select. Enter either **enable** or the parameter value in the text box.

Note Parameters that cannot be configured are assigned a Not Supported message.

Step 6 Click **Update** to complete the plug-in configuration.

Note You must click **Update** for each parameter that you configure.

Configuring Vulnerability Handling



Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent

Scan Setup · Plugin Updates · Reports

Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: Consultant Role

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Enabled Plugins:

ID	Name	Vulnerable if ...	Instruction	Link	Edit
14245	Opera web browser address bar spoofing weakness (2)	– NEVER –			
10880	AdMentor Login Flaw	HOLE			
14361	NSS Library SSLv2 Challenge Overflow	HOLE,WARN			
12022	Multiple phpShop Vulnerabilities	HOLE,WARN,INFO			

Next steps →

CANAC v2.1—4-15

If scanning detects a vulnerability on the user system, the user can be blocked from the network, quarantined, or warned about the vulnerability. When client scan reports are enabled, a client scan report appears in a pop-up window to notify users when vulnerabilities are found. This client report is a subset of the scan report and lists vulnerability results along with instruction steps or a URL link that guides the user through remediation for the vulnerability.

Note If browser pop-up windows are blocked on the user system, the user can click the Scan Report link on the logout page to view the report.

Follow these eight steps to configure how vulnerabilities are handled:

Step 1 Choose **Network Scanner > Scan Setup > Vulnerabilities** to open the Vulnerabilities form.

Step 2 Choose the desired user role and operating system from the User Role drop-down menu and the Operating System drop-down menu.

Note Plug-ins that are selected apply to the current choice of user role and operating system pair. The same set of plug-ins appears for all operating systems in the role. However, you can customize which plug-ins are considered vulnerabilities for each operating system.

Step 3 Configure the properties of the plug-ins that have been enabled through the plug-ins menu:

- **ID:** The number of the plug-in that will be listed on the scan report.
- **Name:** The name of the plug-in.
- **Vulnerable If:** The options in this drop-down menu determine how the Cisco NAM interprets the scan result for each plug-in. You can determine the kind of result that indicates a vulnerability and assigns the user to the quarantine role. Results fall into these four classifications:

— **NEVER:** Ignore the report for the plug-in. Even if a security hole (HOLE), warning (WARN), or system information (INFO) result appears on the report, this plug-in is never treated as a vulnerability and will never cause the user to be put in the quarantine role.

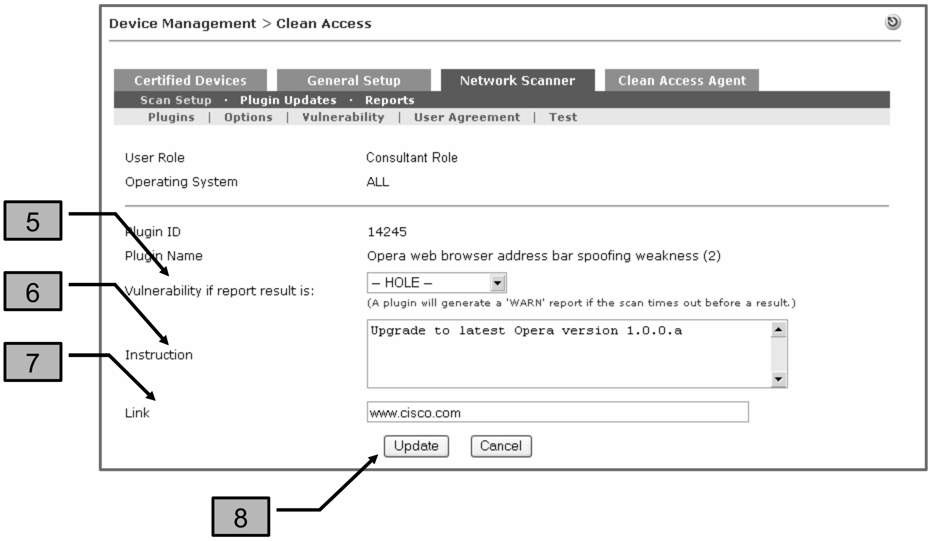
— **HOLE:** If a security HOLE is the result for this plug-in, the client is put in the quarantine role. A result of WARN or INFO on the report is not considered a vulnerability for this plug-in, and no action is taken.

— **HOLE, WARN (Timeout):** A security HOLE result for this plug-in is considered a vulnerability, and the client is put in the quarantine role. If a WARN result occurs, the client is also put in the quarantine role. A WARN result means that the scan timed out (due to personal firewalls or other software) and could not be performed on the machine. Choosing WARN as a vulnerability puts the client in the quarantine role as a precaution, even though the results of the scan are not known. An INFO result on the report is not considered a vulnerability for this plug-in.

— **HOLE, WARN, INFO:** A security HOLE, WARN, or INFO result for this plug-in means that the client has this vulnerability and will be put in the quarantine role. An INFO result indicates status information available through the scan. This information can include which services may be running on a port or NetBIOS information for the workstation that is scanned.

Step 4 Click the **Edit** button to edit the vulnerability features of a plug-in. The Edit Vulnerability form appears.

Configuring Vulnerability Handling (Cont.)


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerability | User Agreement | Test
Update
Cancel
5
6
7
8

User Role: Consultant Role

Operating System: ALL

Plugin ID: 14245

Plugin Name: Opera web browser address bar spoofing weakness (2)

Vulnerability if report result is: – HOLE –

(A plugin will generate a 'WARN' report if the scan times out before a result.)

Instruction: Upgrade to latest Opera version 1.0.0.a

Link: www.cisco.com

CANAC v2.1—4-16

Step 5 Choose the level of vulnerability required to assign the user to the quarantine role from the Vulnerability if Report Result Is drop-down menu.

Step 6 In the Instruction text field, enter the message that appears in the pop-up window if the plug-in discovers a vulnerability.

Step 7 In the Link field, enter the URL where the user can find the necessary steps to fix the system and remove vulnerabilities. The URL appears as a link in the scan report.

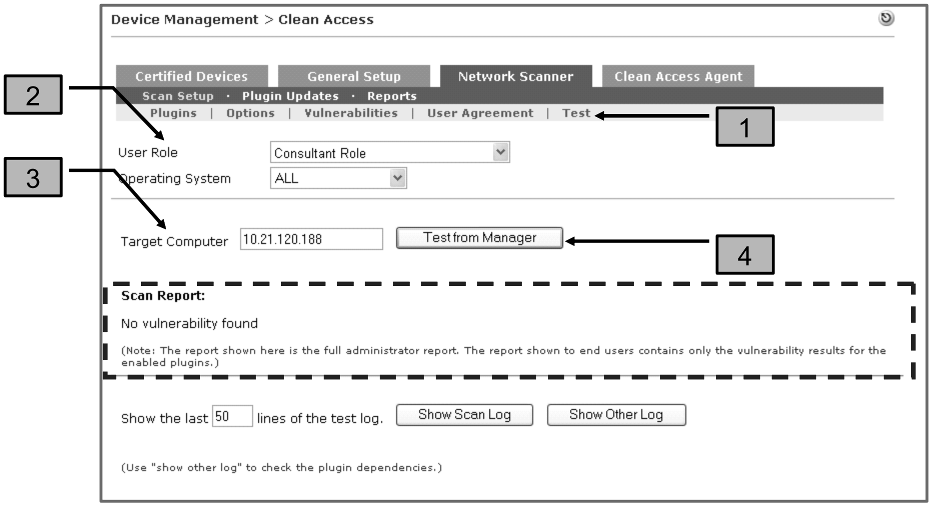
Step 8 Click the **Update** button.

Note Follow Steps 4 to 8 to edit the vulnerability features for each plug-in that is used.

Testing a Scanning Configuration

This topic describes how to test a network scanning configuration.

Test Scanning


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
Test from Manager
Show Scan Log
Show Other Log
1
2
3
4

User Role: Consultant Role

Operating System: ALL

Target Computer: 10.21.120.188

Scan Report:

No vulnerability found

(Note: The report shown here is the full administrator report. The report shown to end users contains only the vulnerability results for the enabled plugins.)

Show the last 50 lines of the test log.

(Use "show other log" to check the plugin dependencies.)

The Test form lets you test your scanning configuration. You can target any machine for the scan and specify the user role that is assumed by the target client for the purpose of the test. For this type of testing, the test is performed against copies of the scan plug-ins that are kept in the Cisco NAM. In a production environment, the Cisco NASs have copies of scan plug-ins from the Cisco NAM, and each Cisco NAS performs the scanning.

Follow these four steps to perform a test scan:

Step 1 Choose **Device Management** > **Clean Access** > **Network Scanner** > **Scan Setup** > **Test**.

Step 2 Choose the user role and operating system that you want to test for the chosen user from the User Role drop-down menu and the Operating System drop-down menu.

Step 3 Enter the IP address of the machine that you want to scan in the Target Computer field. The address of the current machine appears by default.

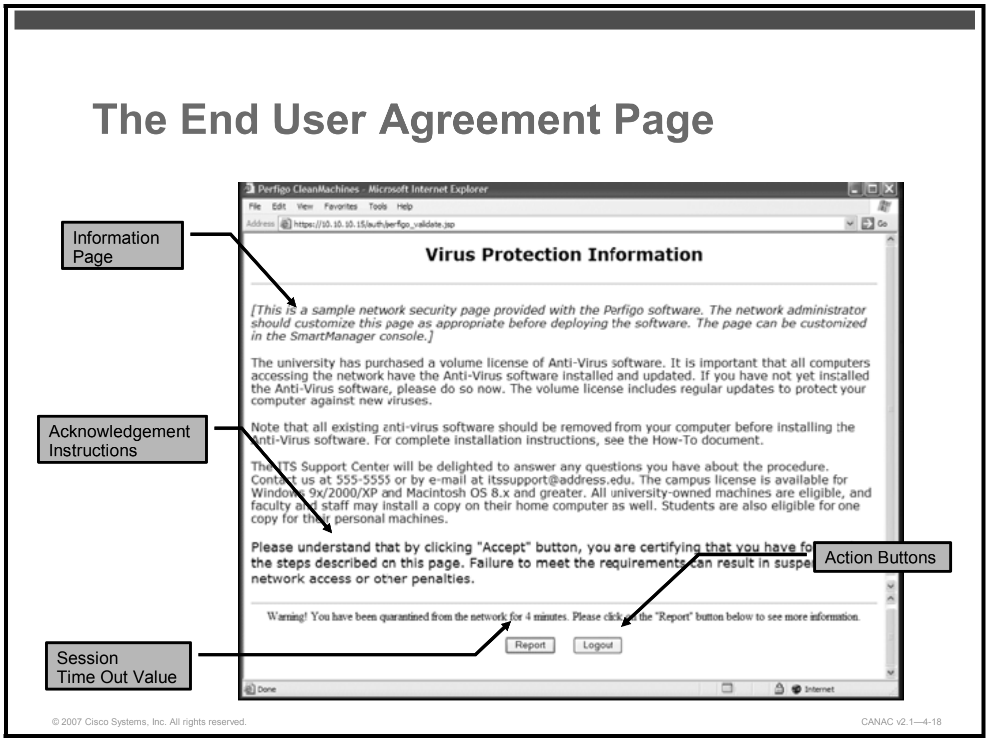
Step 4 Click **Test from Manager**. The scan result appears at the bottom of the page. The figure shows the scan result enclosed in the dashed box

---

Note Click the **Show Scan Log** button to show the debug log for the target computer that has been tested. This log can be found on the computer where the Cisco NAM is installed and is located at /var/nessus/logs/nessusd.messages. The log shows which plug-ins were executed, the results of the execution, which plug-ins were skipped, and why certain plug-ins were skipped (dependency, timeout, and so on). You can check this log to debug a scan result.

Customizing the User Agreement Page

This topic describes how to customize the User Agreement page.



The End User Agreement Page

Perfigo CleanMachines - Microsoft Internet Explorer

Address: https://10.10.10.15/auth/perfigo_validate.jsp

Virus Protection Information

[This is a sample network security page provided with the Perfigo software. The network administrator should customize this page as appropriate before deploying the software. The page can be customized in the SmartManager console.]

The university has purchased a volume license of Anti-Virus software. It is important that all computers accessing the network have the Anti-Virus software installed and updated. If you have not yet installed the Anti-Virus software, please do so now. The volume license includes regular updates to protect your computer against new viruses.

Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact us at 555-5555 or by e-mail at itssupport@address.edu. The campus license is available for Windows 9x/2000/XP and Macintosh OS 8.x and greater. All university-owned machines are eligible, and faculty and staff may install a copy on their home computer as well. Students are also eligible for one copy for their personal machines.

Please understand that by clicking "Accept" button, you are certifying that you have fo the steps described on this page. Failure to meet the requirements can result in suspe network access or other penalties.

Warning! You have been quarantined from the network for 4 minutes. Please click on the "Report" button below to see more information.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-18

The figure shows what the generated User Agreement page looks like for the quarantine role.

Note For quarantine role pages, the text cannot be changed and contains the session timeout configured for the role. The Report and Logout buttons also cannot be changed.

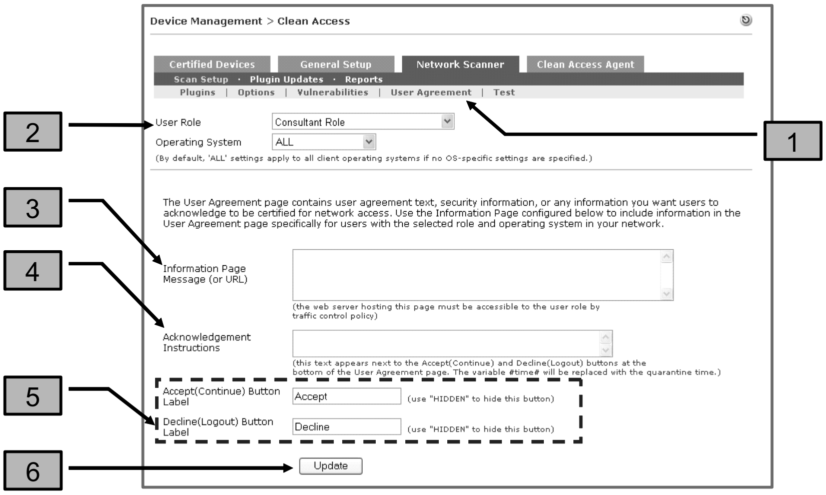
The User Agreement page (also called the Virus Protection page) allows you to provide users with security information, virus warnings, and links to software patches or updates after the network has been scanned. The User Agreement page is an HTML frame-based page made up of these components:

- The information page message (or URL) component. This component contains the text or URL that you specify.
- The acknowledgement instructions component that you specify.
- The session timeout value configured for the role.
- The action buttons that support the role that is associated with this User Agreement page. These buttons vary according to the content of the User Agreement page. For example, for normal login role pages, the buttons could be configured as I Accept and I Do Not Accept. For quarantine role pages, the buttons are hard-coded as Report and Logout. The figure shows a User Agreement page for the quarantine role.

Note The User Agreement page text is hard-coded for the quarantine role.

Cisco NAC Appliance lets you present a specific information page to users with a particular role or operating system. Therefore, before configuring the User Agreement page, create the HTML page that you will use for the information page message (or URL) component for each role or operating system available. Each customized page should be on a web server accessible to Cisco NAC Appliance elements.

Customizing the User Agreement Page


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
Update
1
2
3
4
5
6

User Role: Consultant Role

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

The User Agreement page contains user agreement text, security information, or any information you want users to acknowledge to be certified for network access. Use the Information Page configured below to include information in the User Agreement page specifically for users with the selected role and operating system in your network.

Information Page Message (or URL)

(the web server hosting this page must be accessible to the user role by traffic control policy)

Acknowledgement Instructions

(this text appears next to the Accept(Continue) and Decline(Logout) buttons at the bottom of the User Agreement page. The variable #time# will be replaced with the quarantine time.)

Accept(Continue) Button Label: Accept (use "HIDDEN" to hide this button)

Decline(Logout) Button Label: Decline (use "HIDDEN" to hide this button)

Complete these six steps to customize the User Agreement page:

Step 1 Choose **Device Management > Clean Access > Network Scanner > Scan Setup > User Agreement**. The configuration form for the User Agreement page appears.

Step 2 Choose the user role and operating system from the User Role and Operating System drop-down menus. The Cisco NAM determines the operating system of the user system at login time and serves the page that you have specified for that operating system.

Note If you select a quarantine role, the Acknowledgement Instructions and Button fields are disabled.

Step 3 Enter HTML content or the URL of the page that you want to appear in the Information Page Message (or URL) field. If you are using a file that you uploaded to the Cisco NAM or Cisco NAS, reference the file as follows:

- **Enter HTML:** To add a combination of resource files, such as logos and HTML links, enter HTML content directly into the text field. To reference an uploaded resource file as part of the HTML content, use these formats:
  - — To reference a link to an uploaded HTML file, use <a href=“file_name.html”> file_name.html </a>.
  - — To reference an image file, such as a .jpg file, enter: <img src=“file_name.jpg”>.

- **Enter URLs:** (for a single webpage to appear)
  - — For an external URL, use the format http://www.webpage.com.
  - — For a URL on the Cisco NAM, use the format https://<Manager>/admin/file_name.htm, where <Manager> is the domain name or IP that is listed on the certificate.

Note If you enter an external URL or Cisco NAM URL, ensure that you have created a traffic policy for the unauthenticated role that allows the user HTTP access to the external site or to the Cisco NAM.

Step 4 If desired, enter the text that you want to appear above the Accept and Decline buttons in the Acknowledgement Instructions field.

Step 5 Enter the labels that should appear on the action buttons in their respective fields (for example, Accept and Decline).

Step 6 Click the **Update** button to save the changes that you have made.

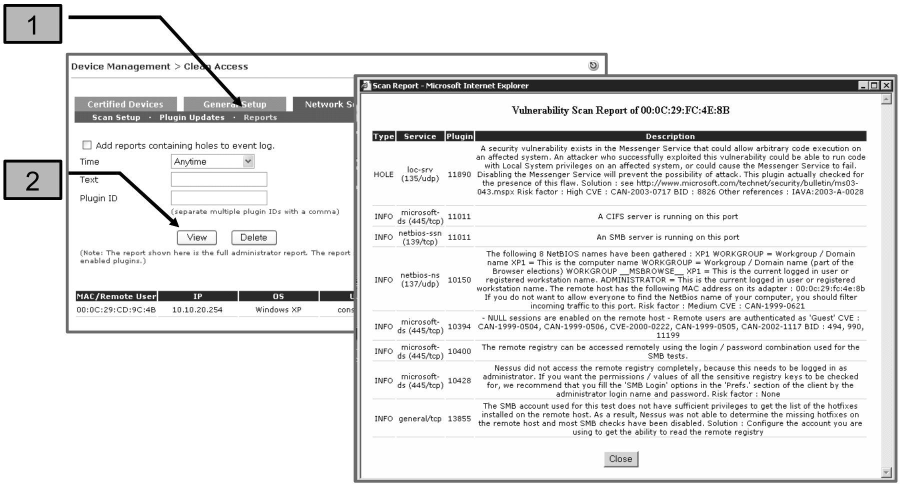
The customized User Agreement page is now generated for users when they attempt to log onto the network.

Note After configuring the User Agreement page, you must create a traffic control policy for the user role to enable users to have access to the web resources of the page. This role must grant access to port 80 of the Cisco NAM.

Viewing Scan Reports

This topic describes how to view scan reports.

Viewing Scan Reports


1
2
Device Management > Clean Access
Certified Devices
General Setup
Network Sc
Scan Setup · Plugin Updates · Reports
View
Delete
Scan Report - Microsoft Internet Explorer
Close

□ Add reports containing holes to event log.

Time: Anytime

Text:

Plugin ID:

(separate multiple plugin IDs with a comma)

(Note: The report shown here is the full administrator report. The report
enabled plugins.)

MAC/Remote User	IP	OS	U
00:0C:29:CD:9C:4B	10.10.20.254	Windows XP	cons

Vulnerability Scan Report of 00:0C:29:FC:4E:8B

Type	Service	Plugin	Description
HOLE	loc-srv (135/udp)	11890	A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack. This plugin actually checked for the presence of this flaw. Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-043.mspx Risk factor : High CVE : CAN-2003-0717 BID : 8826 Other references : IAVA:2003-A-0028
INFO	microsoft-ds (445/tcp)	11011	A CIFS server is running on this port
INFO	netbios-ssn (139/tcp)	11011	An SMB server is running on this port
INFO	netbios-ns (137/udp)	10150	The following 8 NetBIOS names have been gathered : XP1 WORKGROUP = Workgroup / Domain name XP1 = This is the computer name WORKGROUP = Workgroup / Domain name (part of the Browser elections) WORKGROUP __MSBROWSE__ XP1 = This is the current logged in user or registered workstation name. ADMINISTRATOR = This is the current logged in user or registered workstation name. The remote host has the following MAC address on its adapter : 00:0c:29:fc:4e:8b If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621
INFO	microsoft-ds (445/tcp)	10394	- NULL sessions are enabled on the remote host - Remote users are authenticated as 'Guest' CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117 BID : 494, 990, 11199
INFO	microsoft-ds (445/tcp)	10400	The remote registry can be accessed remotely using the login / password combination used for the SMB tests.
INFO	microsoft-ds (445/tcp)	10428	Nessus did not access the remote registry completely, because this needs to be logged in as administrator. If you want the permissions / values of all the sensitive registry keys to be checked for, we recommend that you fill the 'SMB Login' options in the 'Prefs.' section of the client by the administrator login name and password. Risk factor : None
INFO	general/tcp	13855	The SMB account used for this test does not have sufficient privileges to get the list of the hotfixes installed on the remote host. As a result, Nessus was not able to determine the missing hotfixes on the remote host and most SMB checks have been disabled. Solution : Configure the account you are using to get the ability to read the remote registry

Full Administrator Report

Follow these steps to view scan reports:

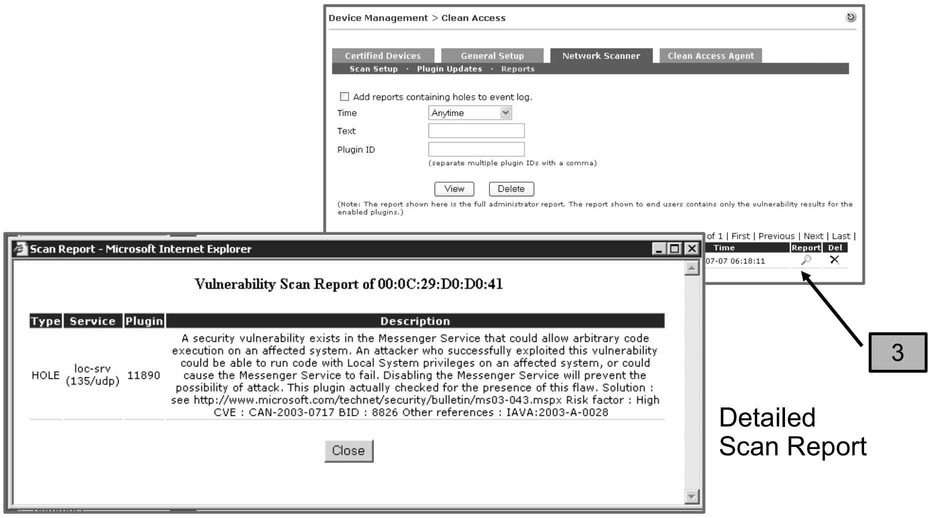
Step 1 Choose **Device Management > Clean Access > Network Scanner > Reports**.

Step 2 Click **View** to see the full administrator report. The report appears in a separate window.

Tip To view only selected reports, choose a time from the drop-down menu or enter search text or plug-in ID, according to the report that you want to view, and click **View**. To delete reports displayed according to the selected criteria, click **Delete**.

Note Sometimes there are dependencies between plug-ins. For example, plug-in B is enabled and the scan result of plug-in A is the prerequisite of a scan by plug-in B. When this is the case, the network scanner automatically applies plug-in A, whether or not plug-in A is enabled. However, because plug-in A is not explicitly enabled, the scan result reported from plug-in A is shown only in the full administrator report.

Viewing Scan Reports (Cont.)



Device Management > Clean Access

□ Add reports containing holes to event log.

Time: Anytime

Text:

Plugin ID:

(separate multiple plugin IDs with a comma)

(Note: The report shown here is the full administrator report. The report shown to end users contains only the vulnerability results for the enabled plugins.)

of 1 | First | Previous | Next | Last |

Time	Report	Del
07-07 06:18:11	🔍	✕

Scan Report - Microsoft Internet Explorer

Vulnerability Scan Report of 00:0C:29:D0:D0:41

Type	Service	Plugin	Description
HOLE	loc-srv (135/udp)	11890	A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack. This plugin actually checked for the presence of this flaw. Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-043.mspx Risk factor : High CVE : CAN-2003-0717 BID : 8826 Other references : IAVA:2003-A-0028

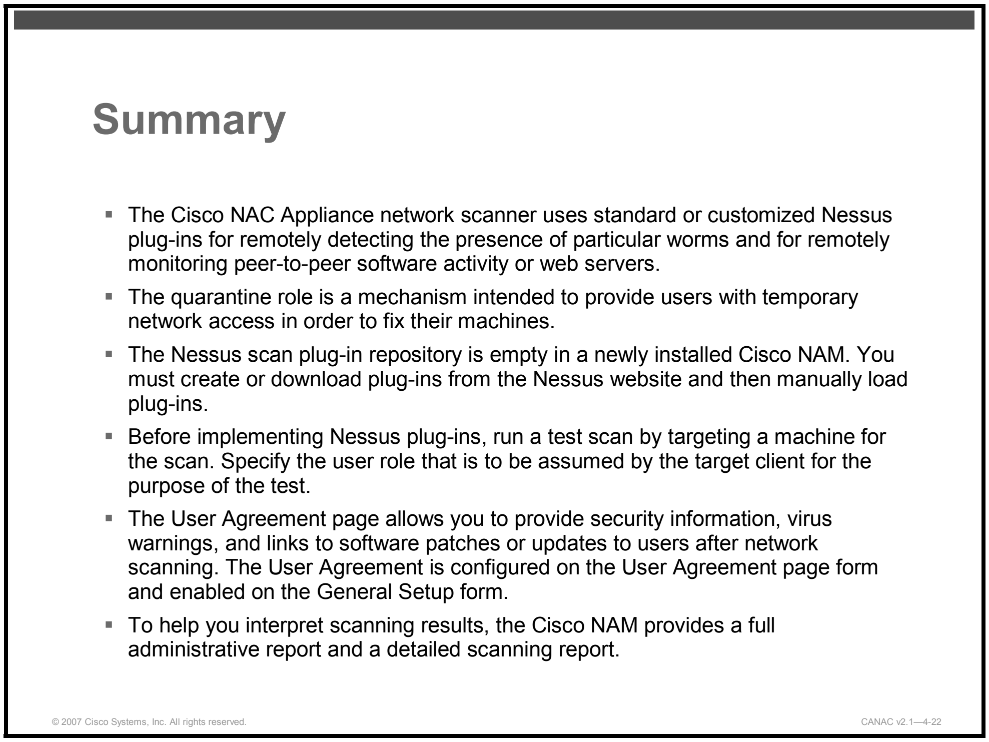
Detailed Scan Report

Step 3 Alternatively, to view a detailed scan report for a given MAC address, click the **Report** icon beside the MAC address. The detailed report appears in a separate window.

Note You can delete reports by using the Delete button on this form.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- The Cisco NAC Appliance network scanner uses standard or customized Nessus plug-ins for remotely detecting the presence of particular worms and for remotely monitoring peer-to-peer software activity or web servers.
- The quarantine role is a mechanism intended to provide users with temporary network access in order to fix their machines.
- The Nessus scan plug-in repository is empty in a newly installed Cisco NAM. You must create or download plug-ins from the Nessus website and then manually load plug-ins.
- Before implementing Nessus plug-ins, run a test scan by targeting a machine for the scan. Specify the user role that is to be assumed by the target client for the purpose of the test.
- The User Agreement page allows you to provide security information, virus warnings, and links to software patches or updates to users after network scanning. The User Agreement is configured on the User Agreement page form and enabled on the General Setup form.
- To help you interpret scanning results, the Cisco NAM provides a full administrative report and a detailed scanning report.

Lesson 3

Configuring the Cisco NAM to Implement the Cisco NAA on User Devices

Overview

Companies must ensure that client machines have all the software that is required in order to access the company network. The Cisco Network Admission Control (NAC) Appliance Agent (Cisco NAA) allows companies to add an extra level of risk mitigation to their network. This lesson describes how to configure the Cisco NAC Appliance Manager (Cisco NAM) to implement the Cisco NAA on user devices (also referred to as client machines).

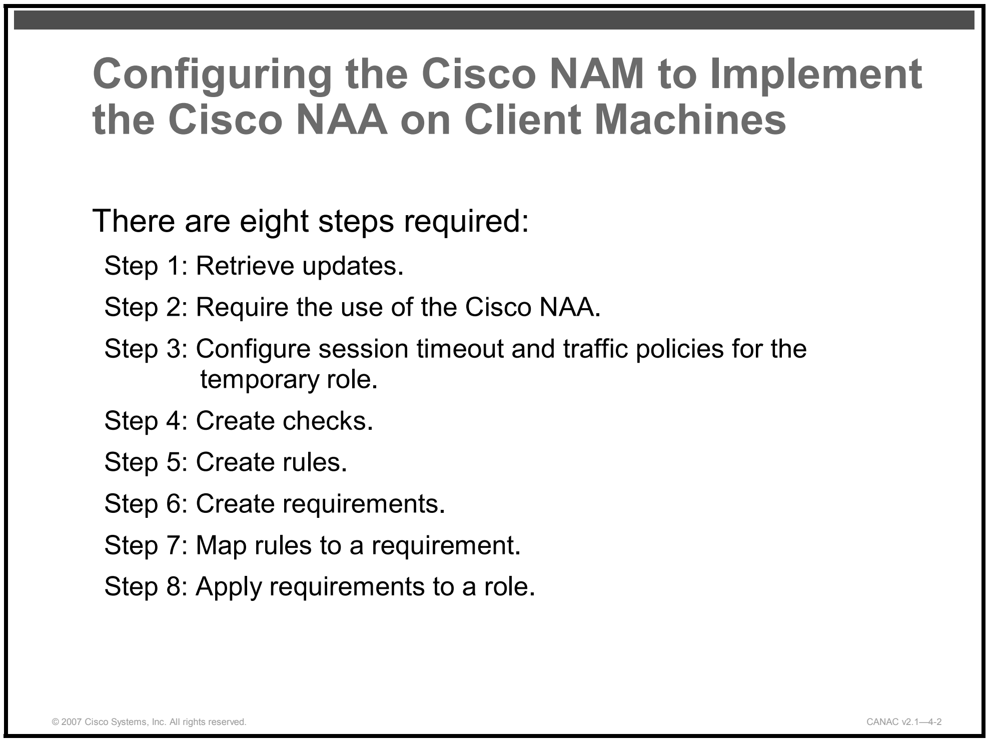
Objectives

Upon completing this lesson, you will be able to explain how to configure the Cisco NAM to implement Cisco NAA on client machines in a network. This ability includes being able to meet these objectives:

- Describe the steps that are used to configure the Cisco NAM to implement the Cisco NAA on client machines
- Describe how to retrieve updates from the Cisco NAC Appliance update server
- Describe how to ensure that the Cisco NAA is installed on user devices
- Describe how to configure the Cisco NAA temporary role on the Cisco NAM
- Explain Cisco NAA system requirements
- Describe how to create a check
- Describe how to create an antivirus rule and a normal rule
- Describe how to create an antivirus requirement and a custom requirement
- Describe how to map requirements to rules and roles

Configuring the Cisco NAM to Implement the Cisco NAA

This topic describes the steps that are used to configure the Cisco NAM in order to implement the Cisco NAA on client machines.



Configuring the Cisco NAM to Implement the Cisco NAA on Client Machines

There are eight steps required:

Step 1: Retrieve updates.

Step 2: Require the use of the Cisco NAA.

Step 3: Configure session timeout and traffic policies for the temporary role.

Step 4: Create checks.

Step 5: Create rules.

Step 6: Create requirements.

Step 7: Map rules to a requirement.

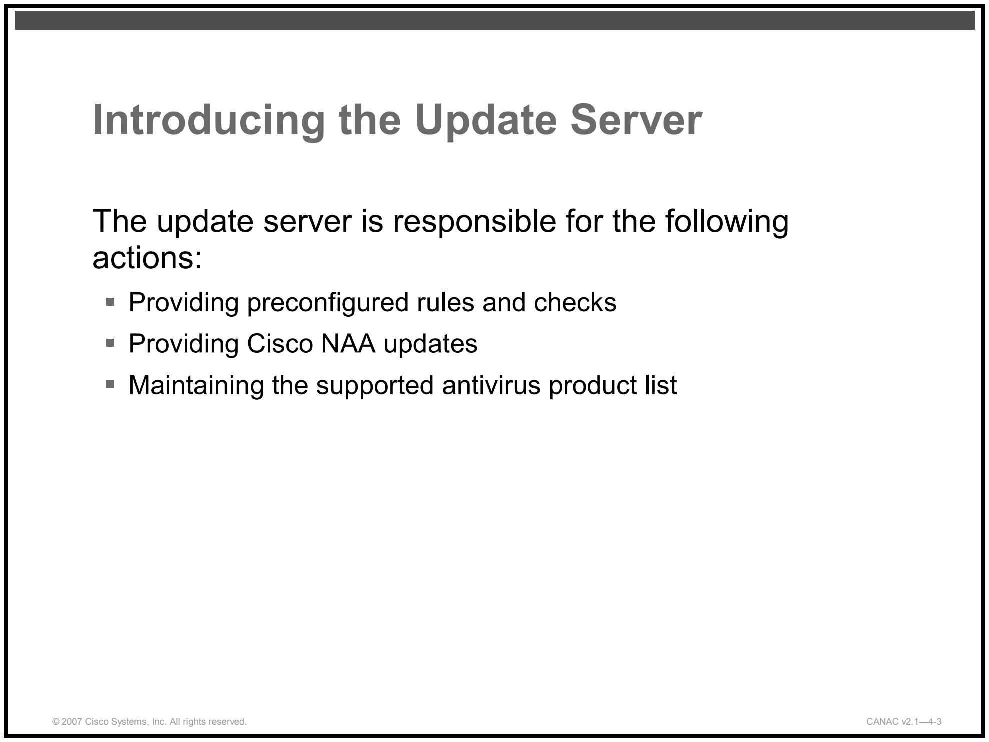
Step 8: Apply requirements to a role.

CANAC v2.1—4-2

The Cisco NAM manages the installation and upgrade of the Cisco NAA on Cisco NAC Appliance Servers (Cisco NASs) and client machines. The eight steps that are used to configure the Cisco NAM to implement the Cisco NAA on client machines are listed in the figure.

Retrieving Updates

This topic describes how to retrieve updates from the Cisco NAC Appliance update server.



Introducing the Update Server

The update server is responsible for the following actions:

- Providing preconfigured rules and checks
- Providing Cisco NAA updates
- Maintaining the supported antivirus product list

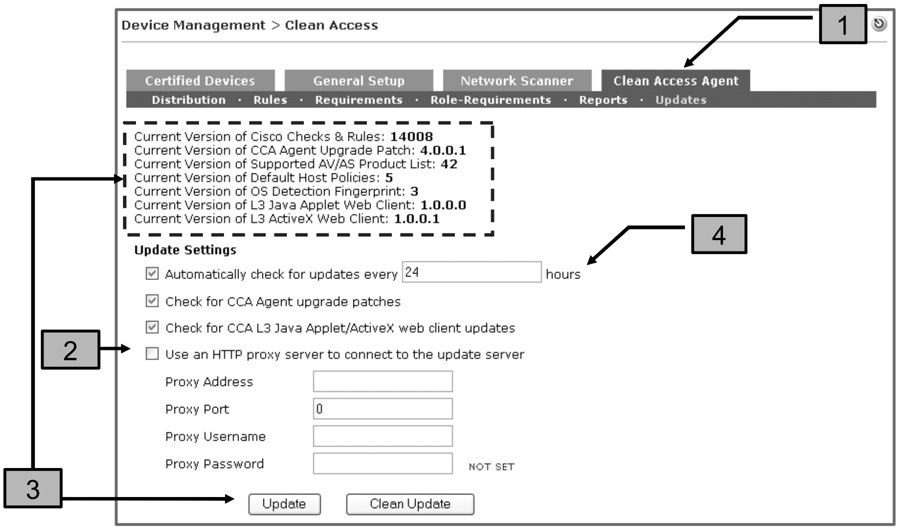
CANAC v2.1—4-3

The Cisco NAC Appliance update server is a separate server, which is configured to provide the Cisco NAM with the most recent version of approved software that is used by client machines. The update server may keep the most current versions of software such as MS Windows, Symantec, McAfee, Trend, Sophos, Zone Labs, and Computer Associates to download to a client at the request of the Cisco NAM. The following are available from the Cisco NAC Appliance update server:

- Preconfigured rule files (files that are prefaced with “pr_”) and preconfigured check files (files that are prefaced with “pc_”). These files are responsible for many applications, such as applications that scan for hot fixes or that ensure that the auto-update is operating.
- Cisco NAA updates.
- The supported antivirus product list. This list provides the most current matrix of supported antivirus vendors and products that are used to configure antivirus definition update requirements and antivirus rules. The supported antivirus product list is updated periodically as new supported products are added.

Tip	The preconfigured rules and checks that Cisco provides are a convenient starting point for customizing specified rules and checks.

Retrieving Updates



Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
1
2
3
4
Update
Clean Update

Current Version of Cisco Checks & Rules: **14008**
Current Version of CCA Agent Upgrade Patch: **4.0.0.1**
Current Version of Supported AV/AS Product List: **42**
Current Version of Default Host Policies: **5**
Current Version of OS Detection Fingerprint: **3**
Current Version of L3 Java Applet Web Client: **1.0.0.0**
Current Version of L3 ActiveX Web Client: **1.0.0.1**

Update Settings

☑ Automatically check for updates every 24 hours

☑ Check for CCA Agent upgrade patches

☑ Check for CCA L3 Java Applet/ActiveX web client updates

☐ Use an HTTP proxy server to connect to the update server

Proxy Address

Proxy Port 0

Proxy Username

Proxy Password NOT SET

Follow these four steps to retrieve updates from the update server:

Step 1 Choose **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates**.

Step 2 If required, check the **Use an HTTP Proxy Server to Connect to the Update Server** check box and fill in the required information.

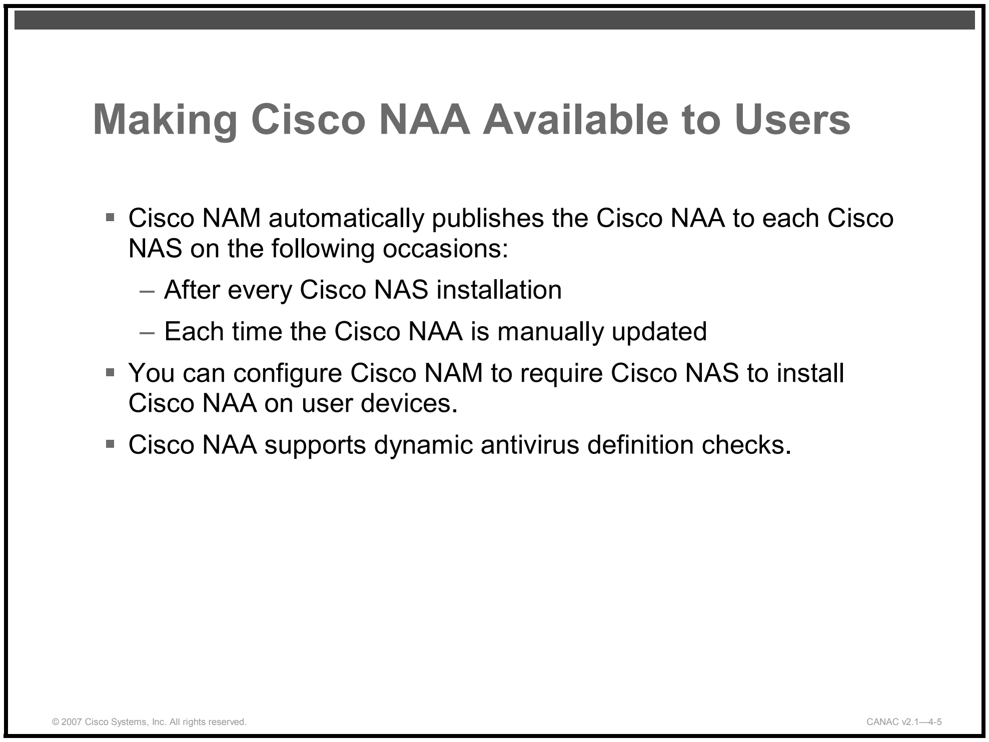
Step 3 Click **Update** to update your existing database with the latest rules, checks, and most recent supported antivirus product list. The dashed box in the figure shows the versions and the quantities of updated Cisco NAC Appliance components.

Step 4 Check the **Automatically Check for Updates Every [ ] Hours** check box and enter an hour value. This value determines the interval at which the client machine will automatically check for updates.

Note When you click the **Update** button, the Cisco NAC Appliance performs an incremental update. When you click the **Clean Update** button, the Cisco NAC Appliance retrieves the most recent version of the product, and all previous updates from the database, including all checks, rules, and the supported anti-X product list, are removed. A complete update (clean update) is typically done when the Cisco NAC Appliance is first installed.

Requiring the Use of the Cisco NAA

This topic describes how to ensure that the Cisco NAA is installed on user devices.



Making Cisco NAA Available to Users

- Cisco NAM automatically publishes the Cisco NAA to each Cisco NAS on the following occasions:
  - After every Cisco NAS installation
  - Each time the Cisco NAA is manually updated
- You can configure Cisco NAM to require Cisco NAS to install Cisco NAA on user devices.
- Cisco NAA supports dynamic antivirus definition checks.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-5

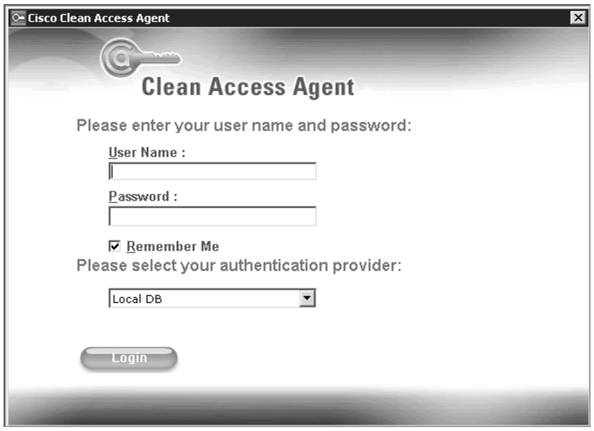
The Cisco NAA is included as part of the Cisco NAC Appliance software. To ensure that the Cisco NAS always has the most recent version of the Cisco NAA, the Cisco NAM automatically publishes the Cisco NAA to each Cisco NAS after every Cisco NAS installation and each time the Cisco NAA is manually updated. If it becomes necessary to manually upload the Cisco NAA, check for release compatibility information between the Cisco NAA version that you install and the Cisco NAS and Cisco NAM software versions that you are using. Refer to the release notes for the applicable release version, which is available from http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/index.htm.

You can configure the Cisco NAM to require the Cisco NAS to install the Cisco NAA on user devices. The optional requirement of using the Cisco NAA is configured for each user role and operating system. When the Cisco NAA is required for a user role, users in that role are forwarded to the Cisco NAA download page after initially authenticating via the web login page. The user is then prompted to download and run the Cisco NAA installation file. When this installation is complete, the user is prompted to log onto the network using the Cisco NAA.

Cisco NAC Appliance flexibly allows multiple versions of the Cisco NAA to be used on the network. Each new version of the Cisco NAA adds support for the latest antivirus products as these products are released. With Cisco NAC Appliance Release 4.0, the system picks the best method to execute antivirus definition checks based on the antivirus product support at the time of execution.

This dynamic antivirus definition checking means that the Cisco NAM now decides at runtime (based on the supported antivirus product list) whether to use the virus definition date or version to execute antivirus rule checks. You do not need to reconfigure antivirus rules when the check method changes because of updates to the antivirus support chart.

The Cisco NAA Login Dialog Box



Cisco Clean Access Agent

Clean Access Agent

Please enter your user name and password:

User Name :

Password :

☑ Remember Me

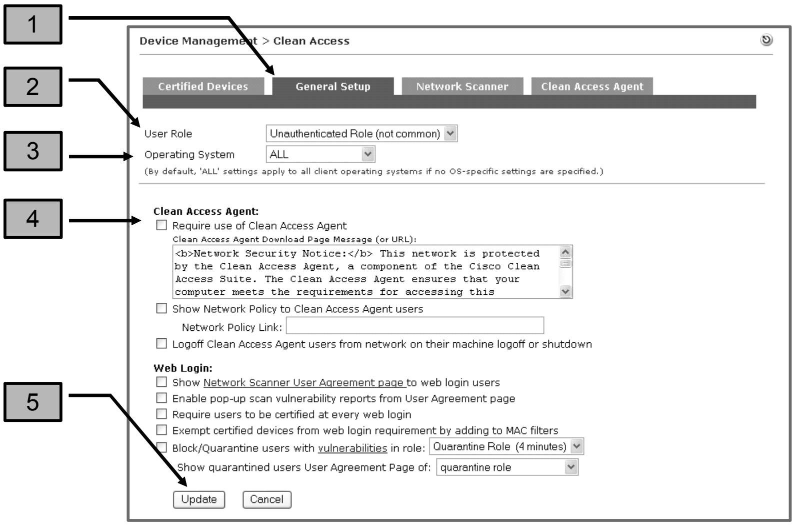
Please select your authentication provider:

Local DB

CANAC v2.1—4-6

After you install the Cisco NAA on a client machine, the Cisco NAA login dialog box appears. The Cisco NAA login dialog box is configured to appear as soon as the user has logged onto their machine. The user would then use the Cisco NAA rather than a web-based login screen to log onto the network.

Requiring the Use of the Cisco NAA



Device Management > Clean Access

User Role: Unauthenticated Role (not common)

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Clean Access Agent:

□ Require use of Clean Access Agent

Clean Access Agent Download Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
by the Clean Access Agent, a component of the Cisco Clean
Access Suite. The Clean Access Agent ensures that your
computer meets the requirements for accessing this
```

□ Show Network Policy to Clean Access Agent users

Network Policy Link:

□ Logoff Clean Access Agent users from network on their machine logoff or shutdown

Web Login:

□ Show Network Scanner User Agreement page to web login users

□ Enable pop-up scan vulnerability reports from User Agreement page

□ Require users to be certified at every web login

□ Exempt certified devices from web login requirement by adding to MAC filters

□ Block/Quarantine users with vulnerabilities in role: Quarantine Role (4 minutes)

Show quarantined users User Agreement Page of: quarantine role

CANAC v2.1—4-7

Follow these five steps to add the Cisco NAA use requirement to the Cisco NAM:

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

Step 2 Choose the user role from the User Role drop-down menu. This will be the user role that requires the use of the Cisco NAA.

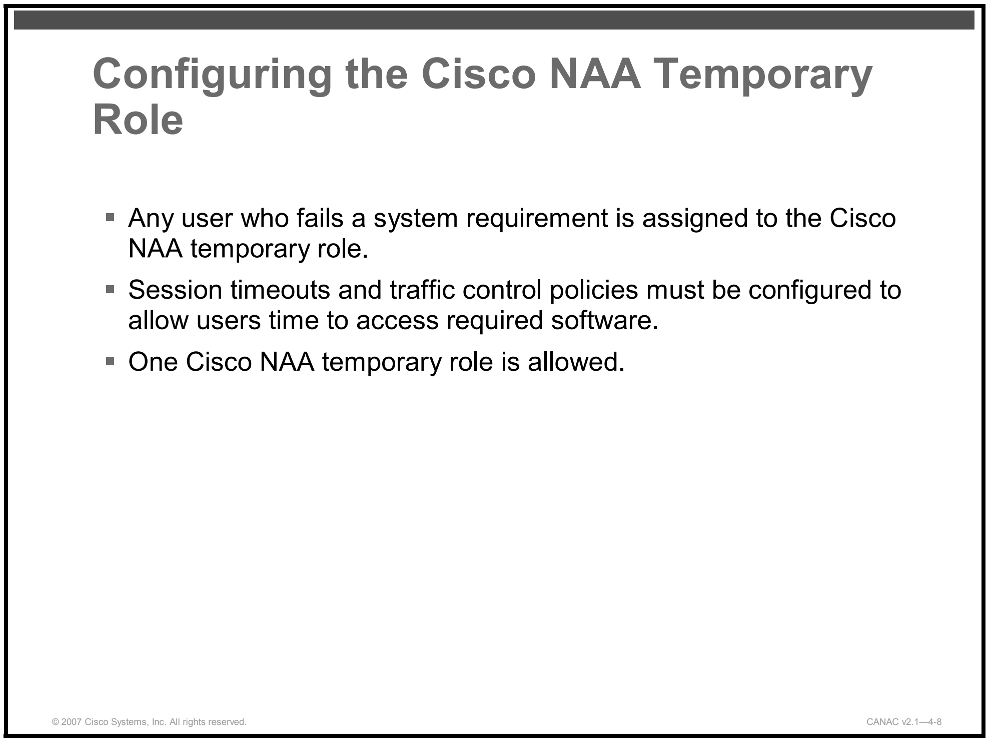
Step 3 Choose an operating system from the Operating System drop-down menu. Users with this operating system will be required to use the Cisco NAA. ALL is included as one of the options in the drop-down menu.

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

Step 5 Click the **Update** button.

Configuring the Cisco NAA Temporary Role

This topic describes how to configure the Cisco NAA temporary role on the Cisco NAM.



Configuring the Cisco NAA Temporary Role

- Any user who fails a system requirement is assigned to the Cisco NAA temporary role.
- Session timeouts and traffic control policies must be configured to allow users time to access required software.
- One Cisco NAA temporary role is allowed.

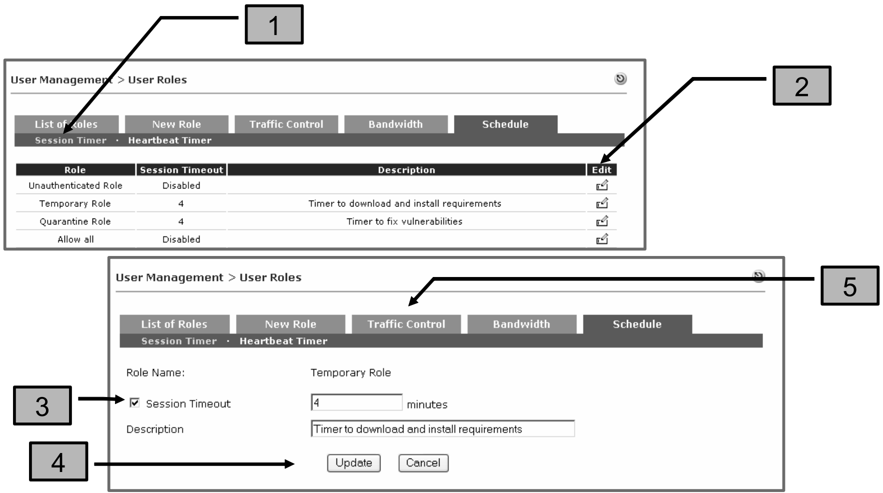
© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-8

Users who fail a system check are assigned to the Cisco NAA temporary role, which provides users limited network access to find and retrieve the resources that are needed to comply with Cisco NAA requirements. The temporary role can be fully edited. It acts as one location where all traffic control policies that allow users to access required installation files are aggregated. The Cisco NAA temporary and quarantine roles have default traffic control policies of Block All Traffic from the untrusted side of the network to the trusted side. The temporary role has a default session timeout of 4 minutes. This default timeout may not provide enough time for the user to access the software that is needed to pass the network scan and gain entry.

Configure session timeout and traffic policies for the temporary role by associating requirements (required packages) to the normal login roles that users attempt to log onto. Client machines must meet these requirements while still in the temporary role. Traffic control policies must be added to the temporary role to allow client machines access to any required software installation files from the download site or sites.

Note	Unlike quarantine roles, you cannot have more than one Cisco NAA temporary role in the system at any time. Cisco NAC Appliance allows only one Cisco NAA temporary role in the system.

Configuring the Cisco NAA Temporary Role (Cont.)



Role	Session Timeout	Description	Edit
Unauthenticated Role	Disabled		✎
Temporary Role	4	Timer to download and install requirements	✎
Quarantine Role	4	Timer to fix vulnerabilities	✎
Allow all	Disabled		✎

Role Name: Temporary Role

☑ Session Timeout 4 minutes

Description Timer to download and install requirements

Next steps

To configure the session timeout and traffic policies for the Cisco NAA temporary role, you must first adjust the session timer value and then configure traffic policies. Follow these steps:

Step 1 Choose **User Management > User Roles > Schedule > Session Timer**. The Session Timer list appears.

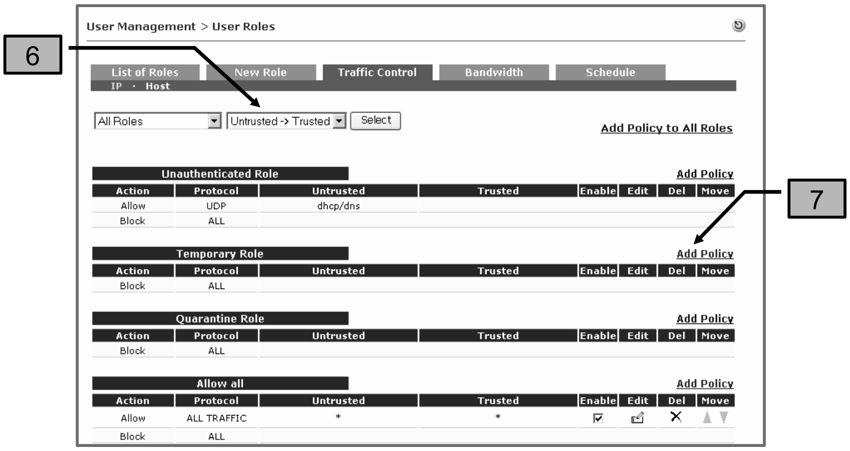
Step 2 Click the **Edit** button for the Temporary Role. The Session Timer form appears.

Step 3 Check the **Session Timeout** check box and enter the number of minutes for the user session to live (default is 4 minutes). Choose a value that provides users with enough time to download required files in order to patch or configure their systems. Optionally, you can enter a description for the session timeout requirement in the Description field.

Step 4 Click **Update**. The temporary role will display the new time in the Session Timer list.

Step 5 Click the **Traffic Control** tab.

Configuring the Cisco NAA Temporary Role (Cont.)



Unauthenticated Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	UDP	dhcp/dns					
Block	ALL						

Temporary Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Block	ALL						

Quarantine Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Block	ALL						

Allow all

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	ALL TRAFFIC	*	*	☑	✎	✕	▲ ▼
Block	ALL						

CANAC v2.1—4-10

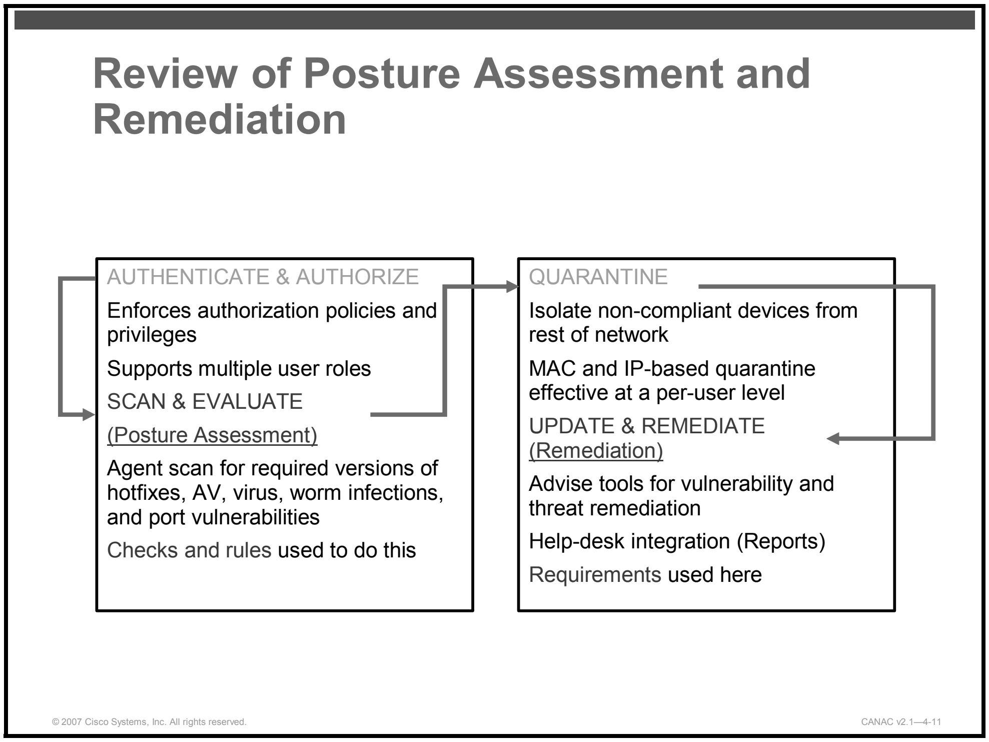
Step 6 Choose **Untrusted -> Trusted** from the drop-down menu. This page is where you create policies that enable the user to access the servers that host the installation files.

If you are providing any required software installation files, set up a policy that allows users in this role to access port 80 of the Cisco NAM. If you want users to be able to correct their systems using external sources such as the Windows Update page, set up permissions for the role to access web resources.

Step 7 Click the **Add Policy** link next to the new role.

Introducing Cisco NAA Checks, Rules, and Requirements

This topic explains Cisco NAA system requirements



Review of Posture Assessment and Remediation

AUTHENTICATE & AUTHORIZE

Enforces authorization policies and privileges

Supports multiple user roles

SCAN & EVALUATE

(Posture Assessment)

Agent scan for required versions of hotfixes, AV, virus, worm infections, and port vulnerabilities

Checks and rules used to do this

QUARANTINE

Isolate non-compliant devices from rest of network

MAC and IP-based quarantine effective at a per-user level

UPDATE & REMEDIATE (Remediation)

Advise tools for vulnerability and threat remediation

Help-desk integration (Reports)

Requirements used here

© 2007 Cisco Systems, Inc. All rights reserved.

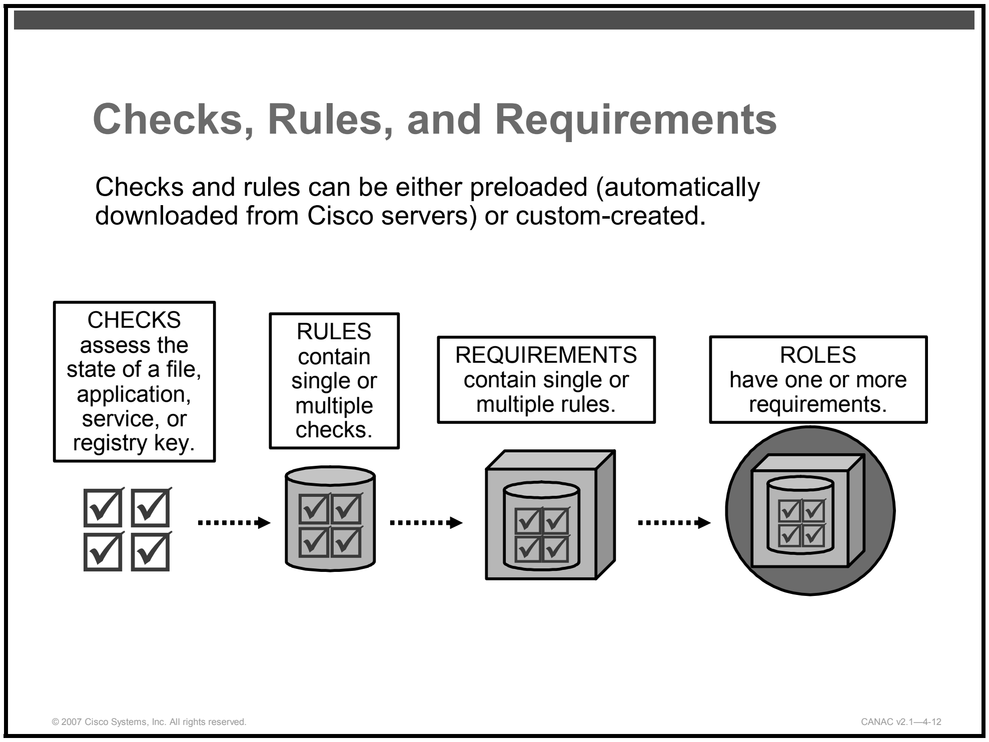
CANAC v2.1—4-11

The Cisco NAC Appliance posture assessment and remediation process starts with authentication and authorization, during which the Cisco NAC Appliance enforces authorization policies and privileges. Cisco NAC Appliance authentication and authorization can support multiple user roles.

During posture assessment, the Cisco NAC Appliance uses the Cisco NAA to scan a client machine for the required versions of hotfixes, antivirus software, and other software. The Cisco NAC Appliance solution supports client machines that do not have a Cisco NAA by using a network scanning feature. The network scan scans for virus and worm infections and port vulnerabilities. Using the Cisco NAC Appliance, multiple user roles can be configured for Cisco NAA and network scanning. Posture assessment is achieved using a Cisco NAC Appliance feature called “checks and rules.” Client machines that fail posture assessment are quarantined and advised for remediation.

If vulnerabilities are found, the Cisco NAC Appliance places the client machine into a quarantine role, in which it is isolated from the rest of network. Client machines can be identified by their MAC and IP addresses, which make this process effective at a per-user level.

While in the quarantine role, remediation takes place by providing web pages to the user that provide guidance on how to update and remediate the machine. Web pages can include links and contact information to help desk support services. Remediation determines the action or set of actions that must take place based on the posture assessment results. For example, if the Cisco NAC Appliance detects that a particular upgrade is not present, an update program can be launched. Remediation is achieved using another Cisco NAC Appliance feature called Requirements.



Checks, Rules, and Requirements

Checks and rules can be either preloaded (automatically downloaded from Cisco servers) or custom-created.

CHECKS assess the state of a file, application, service, or registry key.

RULES contain single or multiple checks.

REQUIREMENTS contain single or multiple rules.

ROLES have one or more requirements.

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—4-12

When Cisco NAC Appliance scans a client machine, it uses requirements made up of checks and rules to help determine the degree of compliance of the client machine. The checks, rules, and requirements are defined as follows:

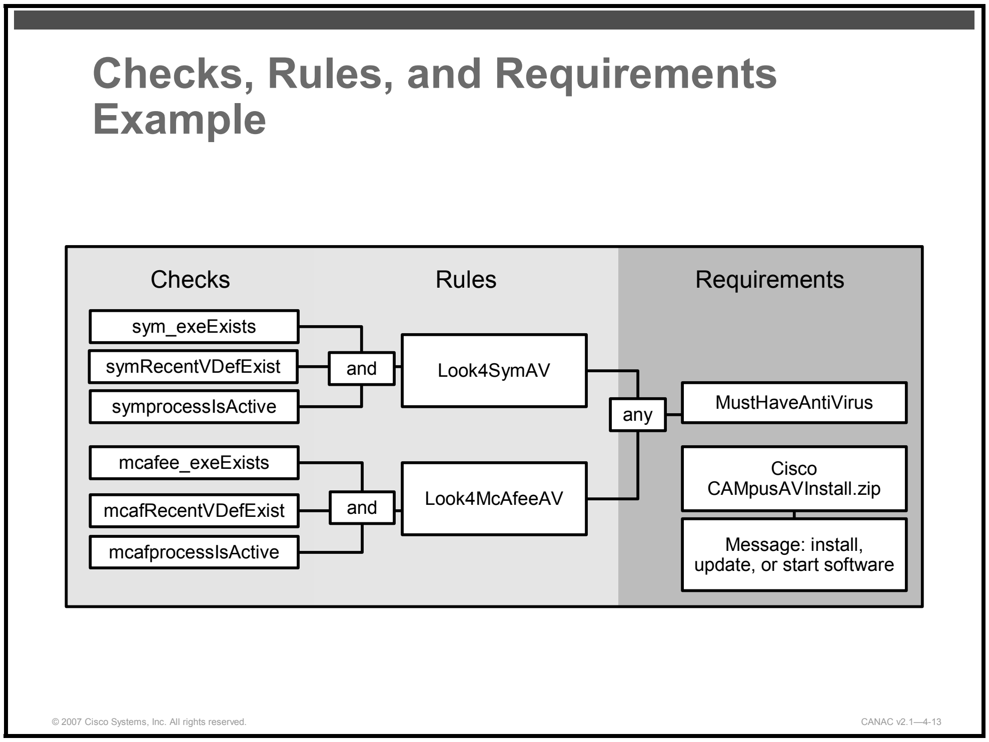
- **Checks:** A check is a condition statement that is used to examine the client system. In the simplest Cisco NASs, a requirement with a single rule consists of a single check (without the "not" operator). If the condition statement yields a true result, the system in question is considered to be in compliance with the Cisco NAA requirement and no remediation is required. Cisco preconfigured checks have a prefix of "pc_" in their names; for example, pc_Hotfix828035. You can configure these four check categories:
  - **Registry check:** Determines whether or not a registry key exists and what a registry key value is
  - **File check:** Determines whether or not a file exists, its modification or creation date, and its file version
  - **Service check:** Determines whether or not a service is running
  - **Application check:** Determines whether or not an application is running
- **Rules:** A rule is an expression consisting of checks and operators. A rule is used by the Cisco NAA to assess whether a vulnerability exists on a particular operating system. If the result of the rule expression statement is true, the system is considered in compliance with the Cisco NAA requirement. Cisco preconfigured rules have a prefix of "pr_" in their names; for example, pr_AutoUpdateCheck_Rule. There are several rule categories:
  - **Antivirus rules:** There are two basic types of antivirus rules:
    - **Installation rules:** Installation antivirus rules check whether the selected antivirus software is installed for the client operating system.
    - **Virus definition rules:** Virus definition antivirus rules check whether the virus definition files are up-to-date on the client. Virus definition antivirus rules checks can be mapped into antivirus definition update requirements so that a

user that fails the requirement can automatically obtain updated software using the Cisco NAA.

  - **Antispyware rules:** There are two basic types of antispyware rules:
    - **Installation antispyware rules:** Installation antispyware rules check whether the selected antispyware software is installed for the client operating system.
    - **Spyware definition antispyware rules**: Spyware definition antispyware rules check whether the spyware definition files are up-to-date on the client. Spyware definition antispyware rules can be mapped into antispyware definition update requirements so that a user that fails the requirement can automatically obtain updated software using the Cisco NAA.

Note Antivirus rules are typically associated with antivirus definition update requirements, and antispyware rules are typically associated with antispyware definition update requirements.

- **Requirements:** To log onto a network that is guarded by Cisco NAC Appliance, a client machine must meet specific requirements. Cisco NAC Appliance requirements implement business-level decisions about the software that client machines must or must not have running on their systems. A Cisco NAC Appliance requirement consists of a rule or set of rules made up of checks that client machines in each user role must meet, and the remediation action that a user must take if the client machine fails to meet the requirement rules. These are the different requirement types:
  - **File distribution:** The file distribution requirement type distributes the required software directly to the user by making the installation package available for user download using the Cisco NAA. In this case, the file that is to be downloaded by the user is placed on the Cisco NAM. For the Cisco NAA to download this file, create a traffic policy for the Cisco NAA temporary role allowing both HTTP and Secure HTTP (HTTPS) access to the Cisco NAM.
  - **Link distribution:** The link distribution requirement type refers users to a separate web page, such as Microsoft Windows Update, where required software is available.
  - **Local check:** The local check requirement type is used when creating checks that are not associated with installable software. Examples of this type of requirement are checking if Windows Update Service (Automatic updates) is enabled and looking for software that should not be on the system.
  - **Antivirus and antispyware update requirements:** The antivirus and antispyware requirements update the definition files for virus and spyware products on a client machine. If the client fails to meet the antivirus and antispyware requirements, the Cisco NAA communicates directly with the installed antivirus or antispyware software on the client and automatically updates the definition files.
  - **Microsoft Windows update requirement:** Cisco NAC Appliance Release 4.0 adds a new Cisco NAA "Windows Update" requirement type configuration page to allow administrators to check and modify Windows Update settings and launch Windows Updater on NAA-enabled user machines. When this requirement is configured, the administrator can turn on Automatic Updates on Windows 2000 or XP clients that have this option disabled on the machine. For more information on this feature, refer to the Configure Windows Update Requirement section in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.



Checks, Rules, and Requirements Example

Checks

Rules

Requirements

sym_exeExists

symRecentVDefExist

symprocessIsActive

and

Look4SymAV

any

MustHaveAntiVirus

mcafee_exeExists

mcafRecentVDefExist

mcafprocessIsActive

and

Look4McAfeeAV

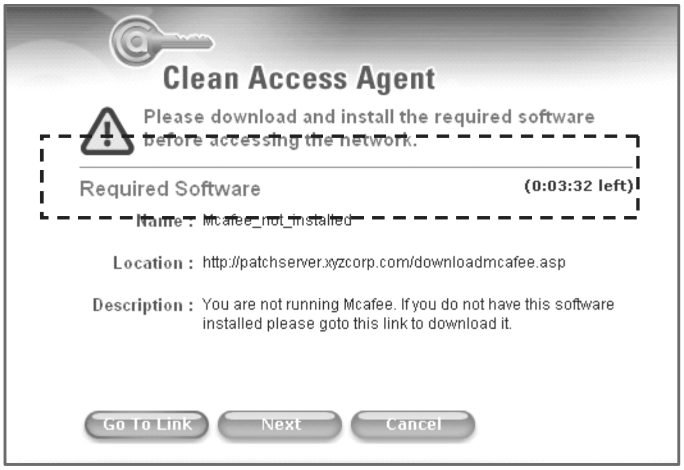
Cisco CAMpusAVInstall.zip

Message: install, update, or start software

The figure shows an example of a requirement that combines several checks and rules with the Boolean operators “and” and “any”. This requirement ensures that client machines have the correct and current antivirus software installed. In the example, the names given to the checks, rules, and requirements were created to explain what each step is responsible for and to provide a single combination of checks and rules that is used to arrive at the requirement.

Note You can create custom requirements to map rules that allow users to meet the rule condition for the mechanism. The mechanism can be an installation file, a link to an external resource, or simply instructions. If a rule check is not satisfied (for example, required software is not found on the client system), users can be warned or required to fix their systems, depending on what you have configured.

Enforcing Rules and Requirements



Clean Access Agent

Please download and install the required software before accessing the network.

Required Software (0:03:32 left)

Name : Mcafee_not_installed

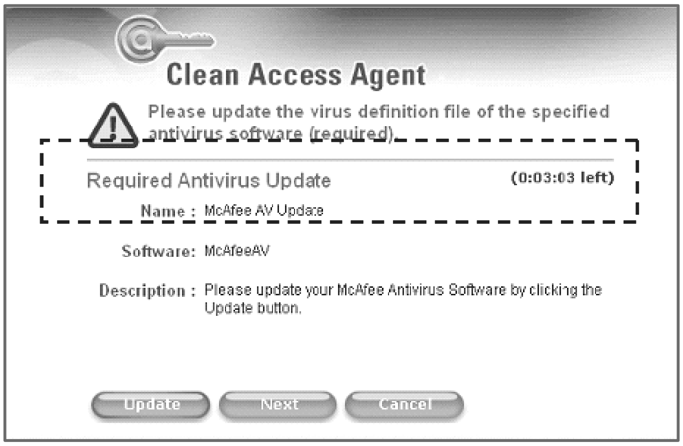
Location : http://patchserver.xyzcorp.com/downloadmcafee.asp

Description : You are not running Mcafee. If you do not have this software installed please goto this link to download it.

CANAC v2.1—4-14

The Cisco NAC Appliance uses the Cisco NAA to inform the client that their machine is not in compliance with configured requirements. The figure shows the Cisco NAA dialog box that appears when a client machine does not have antivirus software installed. Notice how the client is given a time limit to remediate this issue. There is also a command button that takes the user to the location described in the dialog box. The next series of slides show examples of Cisco NAA dialog boxes that appear when a requirement that you have configured is not met.

Enforcing Rules and Requirements (Cont.)



Clean Access Agent

Please update the virus definition file of the specified antivirus software (required).

Required Antivirus Update (0:03:03 left)

Name : McAfee AV Update

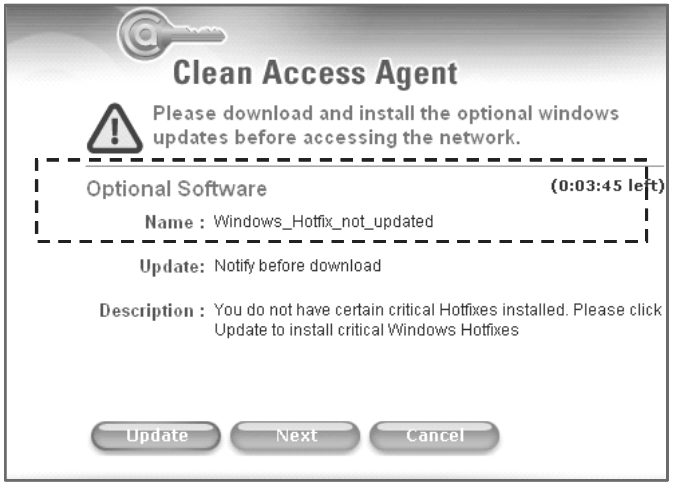
Software: McAfeeAV

Description : Please update your McAfee Antivirus Software by clicking the Update button.

The figure shows a dialog box that appears to the user when the Cisco NAC Appliance determines that an antivirus update is missing. Again, a time limit is included to let the user know how much time there is to perform the update. In this dialog box, an Update button appears. Cisco NAC Appliance can be configured to take the client to a remediation site to download the required software update.

Caution Not all product versions of a selected vendor support automatic updates via the Cisco NAA. When a product does not support automatic updates via the Cisco NAA, client machines may be instructed to update their antivirus or antispyware software or both from the user interface menu of their installed antivirus product. For details, see the Cisco NAC Appliance product web page at http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html. From the Cisco NAC Appliance product web page, find the release notes for the latest version of the software and search for the supported antivirus and antispyware product list.

Enforcing Rules and Requirements (Cont.)



Clean Access Agent

Please download and install the optional windows updates before accessing the network.

Optional Software (0:03:45 left)

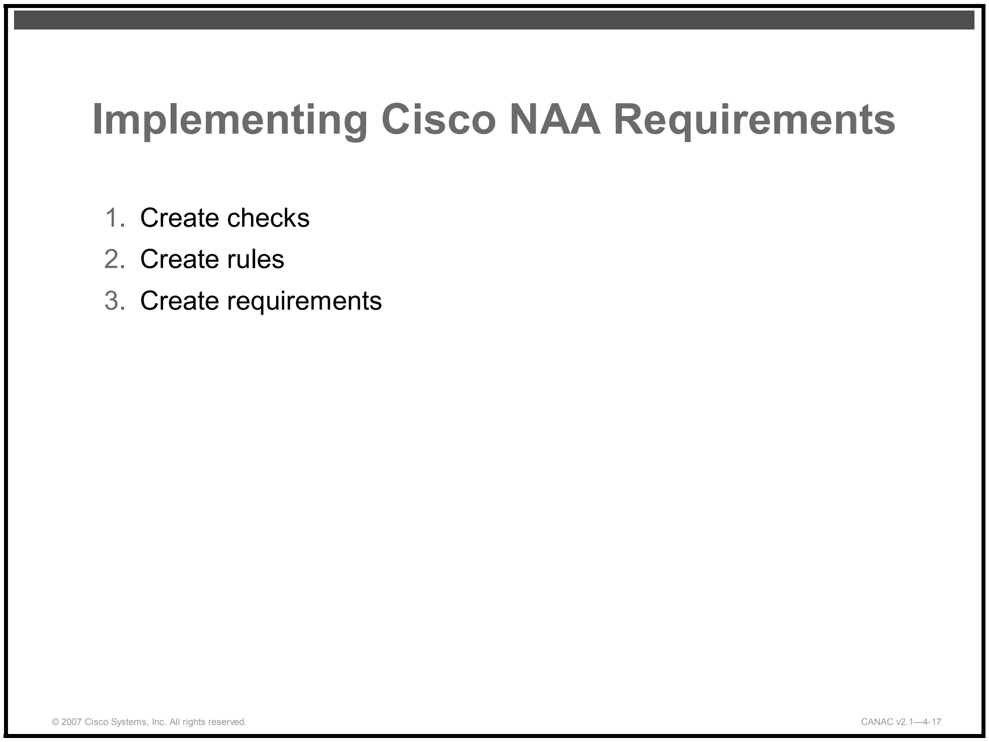
Name : Windows_Hotfix_not_updated

Update: Notify before download

Description : You do not have certain critical Hotfixes installed. Please click Update to install critical Windows Hotfixes

CANAC v2.1—4-16

In this example, the figure shows a dialog box that appears when the Cisco NAC Appliance finds that optional software has not been installed. Again, there is a time limit to perform this update and an Update button to guide the client to the update site.



Implementing Cisco NAA Requirements

1. Create checks
2. Create rules
3. Create requirements

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—4-17

To implement Cisco NAA system requirements, you must create three system requirement elements: checks, rules, and requirements.

- **Checks:** You must configure checks to find a required feature in the user device. The check categories: Registry check, File check, Service check, and Application check, are selected to match the feature category that the requirement demands. To configure a check, identify a defining feature of the requirement. The feature (such as a registry key or process name) should indicate whether or not the client meets the requirement. The best way to find such an indicator is to examine a system that you know has the requirement. To determine which feature to use, refer to the documentation that is provided with the software for that system.
- **Rules:** A rule is an expression made up of checks and operators. A rule is the unit that is used by the Cisco NAA to assess whether or not a vulnerability exists on a particular operating system. If the result of the rule expression statement is true, the system is considered in compliance with the Cisco NAA requirement. A rule can either consist of a single check or have multiple checks combined with Boolean operators. The order of precedence of the available Boolean operators is:

  1. parenthesis “()”
  2. not “!”
  3. and “&”
  4. or “|”

  After a rule is created, it is automatically validated.

Note There is no need to create checks with the antivirus or antispyware rule types.

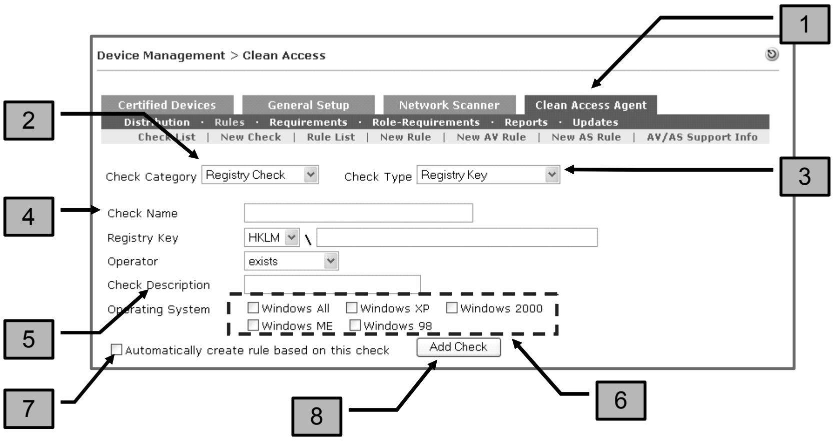
Tip	Errors can arise when you create checks and rules for a particular operating system and later change the operating system property of one check that is used in a rule. Because rules can use a variety of checks, confirm that each rule that is using the modified check remains valid.

- **Requirements:** Requirements point to installation files or links where downloadable software can be found. For local checks that are not associated with a specific installation file, the requirement can map the rule to an informational message that instructs the user to remove specific software or to run a virus check. A new requirement can be created at any time during the configuration process. The requirement must be associated with a rule for both an operating system and a user role before the requirement can take effect. The Cisco NAM automatically validates requirements as they are created.

Creating a Check

This topic describes how to create a check.

Creating a Check



Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Add Check
1
2
3
4
5
6
7
8

Check Category: Registry Check

Check Type: Registry Key

Check Name

Registry Key: HKLM \

Operator: exists

Check Description

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

□ Automatically create rule based on this check

Follow these eight steps to create a check:

Step 1 In the Clean Access Agent tab, click the **Rules** submenu and then click the **New Check** option.

Step 2 Choose a check category from the Check Category drop-down menu. The choices are Registry Check, File Check, Service Check, and Application Check.

Step 3 Choose a check type from the Check Type drop-down menu and fill in the form fields for parameters, operator, and (if the check type is a value comparison) the value and data type for the statement.

Step 4 Enter a descriptive name in the Check Name field. The rules that are created from this check reference the check by this name. Therefore, give the check a unique, self-descriptive name. The name is case-sensitive, must be less than 255 characters, and should not include spaces or special characters.

Step 5 Enter an optional description in the Check Description field.

Step 6 Choose at least one operating system for the check. Options include Windows All, Windows XP, Windows 2000, Windows ME, and Windows 98.

Step 7 If desired, check the **Automatically Create Rule Based on This Check** check box.

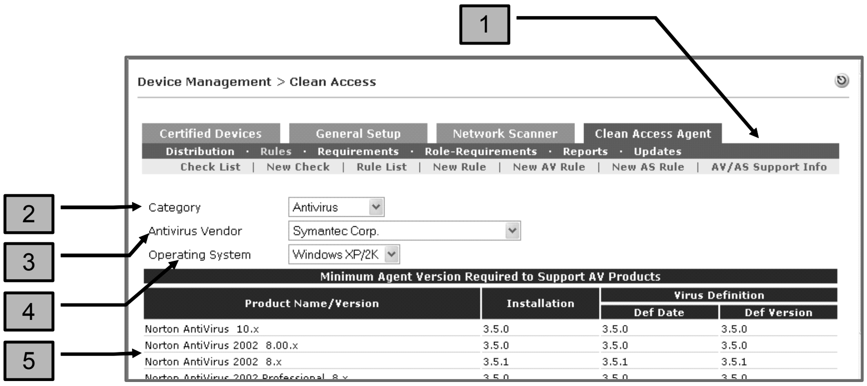
Note When a rule is automatically created based on the check, the rule is named “given check name-rule” (not shown in the figure).

Step 8 Click **Add Check** to create the evaluation statement. If the condition statement evaluates to false, the required software is considered missing.

Creating Rules

This topic describes how to create an antivirus rule and a normal rule. Creating an antivirus rule and creating an antispyware rule follow very similar procedures and have very similar user interfaces. The procedure that is detailed here can be used, with minor modification, to create an antispyware rule.

Checking Antivirus Product Support Information


1
2
3
4
5
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info

Category: Antivirus
Antivirus Vendor: Symantec Corp.
Operating System: Windows XP/2K

Minimum Agent Version Required to Support AV Products

Product Name/Version	Installation	Virus Definition	
		Def Date	Def Version
Norton AntiVirus 10.x	3.5.0	3.5.0	3.5.0
Norton AntiVirus 2002 8.00.x	3.5.0	3.5.0	3.5.0
Norton AntiVirus 2002 8.x	3.5.1	3.5.1	3.5.1
Norton AntiVirus 2002 Professional 8.x	3.5.0	3.5.0	3.5.0

CANAC v2.1—4-19

The first task in creating either an antivirus rule or an antispyware rule is to check for the most recent and supported version of the product.

Cisco NAC Appliance allows multiple versions of the Cisco NAA to be used on the network. New updates to the Cisco NAA will add support for the latest antivirus or antispyware products as they are released. Cisco NAC Appliance picks the best method to execute antivirus rule or antispyware definition checks based on the antivirus rule or antispyware products that are available and the version of the Cisco NAA. When you are running multiple versions of the Cisco NAA on your network, use the AV/AS Support Info (antivirus and antispyware support information) page to determine Cisco NAA compatibility with the latest supported antivirus rule or antispyware product list downloaded to the Cisco NAM.

Note The Cisco NAA sends its version information to the Cisco NAM, and the Cisco NAM always attempts to first use the virus definition version for antivirus checks. If the version is not available, the Cisco NAM uses the virus definition date instead.

Follow these five steps to check for the most recent and supported version of an antivirus product:

Step 1 Choose **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**.

Step 2 Choose **Antivirus** from the Category drop-down menu.

Step 3 Choose a corresponding vendor from the Antivirus Vendor drop-down menu.

Step 4 Choose **Windows XP/2K** or **Windows 9x/ME** from the Operating System drop-down menu to view the support information for those two Windows client systems.

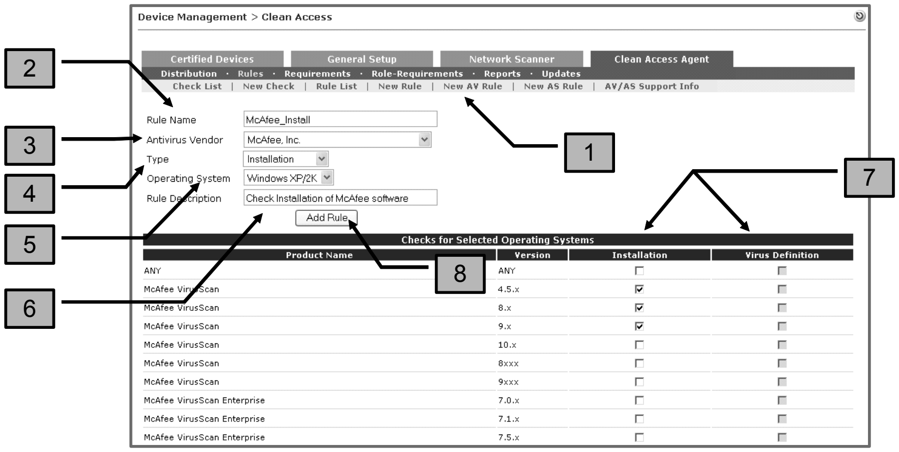
Note Step 4 populates the following tables in the AV/AS Support Info form:

– **Minimum Agent Version Required to Support AV Products:** This table shows the minimum Cisco NAA version that is required to support each antivirus product. For example, a 4.0.0.0 Cisco NAA can log onto a role that requires AOL Safety and Security Center Virus Protection 1.x, but for a 3.6.0.0 or below Cisco NAA, this check will fail. If a version of the Cisco NAA supports both Def Date and Def Version checks, the Def Version check will be used.

– **Latest Virus Definition Version/Date for Selected Vendor:** This table displays the latest version and date information for the antivirus product. The antivirus software for an up-to-date client should display the same values. This table is not displayed in the figure.

Step 5 Review the information in the AV/AS Support Info form to determine the minimum Cisco NAA version that is required to support a given antivirus product.

Creating an Antivirus Rule


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Add Rule
1
2
3
4
5
6
7
8

Rule Name: McAfee_Install
Antivirus Vendor: McAfee, Inc.
Type: Installation
Operating System: Windows XP/2K
Rule Description: Check Installation of McAfee software

Checks for Selected Operating Systems

Product Name	Version	Installation	Virus Definition
ANY	ANY	□	□
McAfee VirusScan	4.5.x	☑	□
McAfee VirusScan	8.x	☑	□
McAfee VirusScan	9.x	☑	□
McAfee VirusScan	10.x	□	□
McAfee VirusScan	8xxx	□	□
McAfee VirusScan	9xxx	□	□
McAfee VirusScan Enterprise	7.0.x	□	□
McAfee VirusScan Enterprise	7.1.x	□	□
McAfee VirusScan Enterprise	7.5.x	□	□

Now that you have confirmed that you have the latest supported antivirus product version, follow these eight steps to create an antivirus rule:

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

Step 2 Enter a rule name in the Rule Name field. You can use digits and underscores in the name, but do not include spaces.

Step 3 Choose an antivirus vendor from the Antivirus Vendor drop-down menu. This choice populates the Checks for Selected Operating Systems table at the bottom of the page with the supported products and product versions from this vendor. The checks that are listed here apply to the specific operating system that is chosen.

Step 4 Choose either **Installation** or **Virus Definition** from the Type drop-down menu. This choice enables the check boxes for either the Installation or Virus Definition column in the Checks for Selected Operating Systems table.

Step 5 Choose an operating system from the Operating System drop-down menu. The operating system that you choose identifies which operating system the product versions listed in the Checks for Selected Operating Systems table will support.

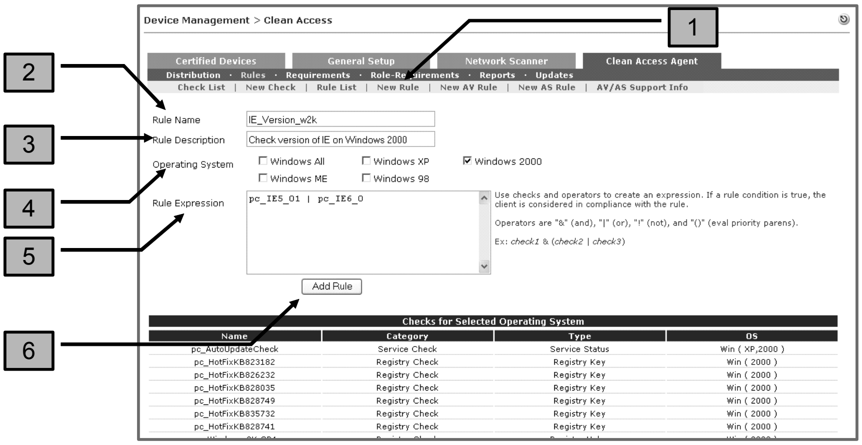
Step 6 Enter an optional rule description in the Rule Description field.

Step 7 In the Checks for Selected Operating Systems table, check the check box or check boxes in either the Installation or the Virus Definition column to choose the product versions that you want to check for on the client machine. The Latest Virus Definition Version/Date for Selected Vendor section displays the type of value (either the virus definition version or the virus definition date) that is used by the antivirus rule to check for the virus definition file on the client. Typically, the virus definition version is used for the check. If the version is not available, the virus definition date is used.

Step 8 Click the **Add Rule** button. The new antivirus rule, with the name you provided, is added at the bottom of the Rule List.

Note For information on how to add an antispyware rule, refer to Configure AV/AS Definition Update Requirements in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Creating a Rule


1
2
3
4
5
6
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Add Rule

Rule Name: IE_Version_w2k

Rule Description: Check version of IE on Windows 2000

Operating System: □ Windows All □ Windows XP ☑ Windows 2000 □ Windows ME □ Windows 98

Rule Expression:

```
pc_IE5_01 | pc_IE6_0
```

Use checks and operators to create an expression. If a rule condition is true, the client is considered in compliance with the rule.

Operators are "&" (and), "|" (or), "!" (not), and "()" (eval priority parens).

Ex: *check1* & (*check2* | *check3*)

Checks for Selected Operating System

Name	Category	Type	OS
pc_AutoUpdateCheck	Service Check	Service Status	Win (XP,2000)
pc_HotFixKB823182	Registry Check	Registry Key	Win (2000)
pc_HotFixKB826232	Registry Check	Registry Key	Win (2000)
pc_HotFixKB828035	Registry Check	Registry Key	Win (2000)
pc_HotFixKB828749	Registry Check	Registry Key	Win (2000)
pc_HotFixKB835732	Registry Check	Registry Key	Win (2000)
pc_HotFixKB828741	Registry Check	Registry Key	Win (2000)

Follow these six steps to create a rule other than an antivirus or an antispyware rule:

Step 1 In the Device Management > Clean Access > Clean Access Agent tab, choose **Rules > New Rule**.

Step 2 Enter a unique rule name in the Rule Name field. Do not include spaces in the name.

Step 3 Enter a rule description in the Rule Description field.

Step 4 Check the check box for the operating system that you want the rule to apply to. If updates have been downloaded, the preconfigured checks for that operating system appear automatically in the Checks for Selected Operating System list at the bottom of the page.

Step 5 Construct the rule expression by combining checks and operators. Use the Checks for Selected Operating System list to select the names of checks, then copy and paste them to the Rule Expression field. Use the following operators with the checks: () (evaluation priority), ! (not), & (and), and | (or); for example, adawareLogRecent & (NorAVProcessIsActive | SymAVProcessIsActive).

For a simple rule that tests a single check, simply type the name of the check (for example, SymAVProcessIsActive).

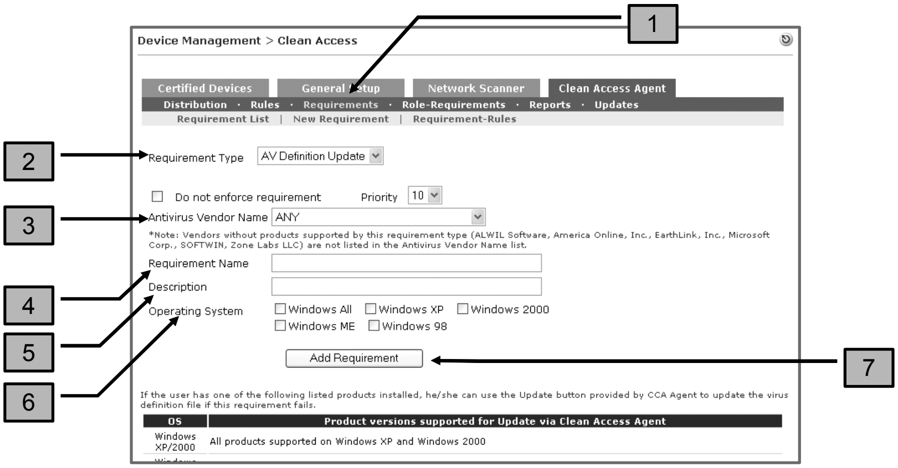
Step 6 Click the **Add Rule** button.

Note The console validates the rule, and if the rule is formed correctly, the rule appears in the Rule List. For details on correcting invalid rules, refer to Validate Rules in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Creating Requirements

This topic describes how to create an antivirus update requirement and a custom requirement. Creating an antivirus requirement and creating an antispyware update requirement follow very similar procedures and have very similar user interfaces. The procedure that is detailed here can be used, with minor modification, to create an antispyware update requirement.

Creating an Antivirus Update Requirement


1
2
3
4
5
6
7
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules
Add Requirement

Device Management > Clean Access

Requirement Type: AV Definition Update

□ Do not enforce requirement   Priority: 10

Antivirus Vendor Name: ANY

*Note: Vendors without products supported by this requirement type (ALWIL Software, America Online, Inc., EarthLink, Inc., Microsoft Corp., SOFTWIN, Zone Labs LLC) are not listed in the Antivirus Vendor Name list.

Requirement Name:

Description:

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

If the user has one of the following listed products installed, he/she can use the Update button provided by CCA Agent to update the virus definition file if this requirement fails.

OS	Product versions supported for Update via Clean Access Agent
Windows XP/2000	All products supported on Windows XP and Windows 2000

CANAC v2.1—4-22

Follow these seven steps to create an antivirus update requirement:

Step 1 In the Device Management > Clean Access > Clean Access Agent tab, choose **Requirements > New Requirement**.

Step 2 Choose **AV Definition Update** in the Requirement Type drop-down menu**.**

Step 3 Choose an antivirus vendor name from the Antivirus Product Name drop-down menu. The Products table lists all the virus definition product versions supported per client operating system.

Step 4 Enter a unique name in the Requirement Name field to identify this antivirus virus definition file requirement in the Cisco NAA. This name will be visible to users on the Cisco NAA dialog boxes.

Step 5 Enter a description of the requirement and instructions for users who fail to meet the requirement in the Description field. For an antivirus definition update requirement, include instructions for users to click the **Update** button to update their systems.

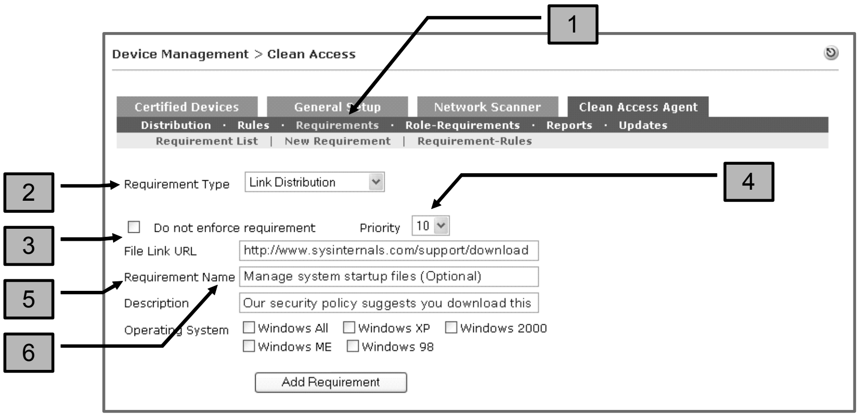
Step 6 Check an **Operating System** check box (at least one operating system must be chosen).

Step 7 Click **Add Requirement** to add the selected requirement to the Requirement List.

Note For information on how to add a Windows update requirement, refer to Configure Windows Update Requirement in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

For information on how to add an antispyware update requirement, refer to Configure AV/AS Definition Update Requirements in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide.*

Creating a Custom Requirement


1
2
3
4
5
6
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules
Add Requirement

Device Management > Clean Access

Requirement Type: Link Distribution

□ Do not enforce requirement   Priority: 10

File Link URL: http://www.sysinternals.com/support/download

Requirement Name: Manage system startup files (Optional)

Description: Our security policy suggests you download this

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

Next steps →

CANAC v2.1—4-23

Follow these nine steps to create a custom requirement:

Step 1 In the Device Management > Clean Access > Clean Access Agent tab, choose **Requirements > New Requirement**.

Step 2 Choose a requirement type from the Requirement Type drop-down menu.

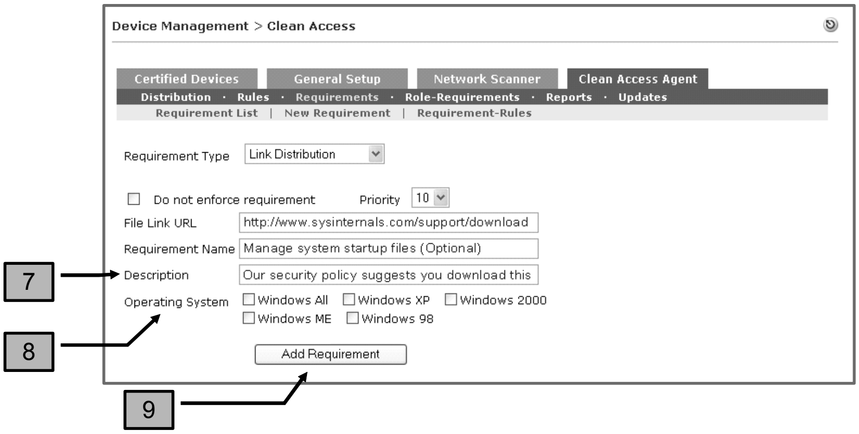
Step 3 You have the option to check the Do Not Enforce Requirement check box. If this option is enabled, the requirement check of the client system is called “soft.” To perform a soft check, the Cisco NAA applies the rules of the requirement, and if the client does not meet the rules, the client is advised only of the check result. The client is neither blocked from the network nor quarantined.

Step 4 Choose the priority of the requirement from the Priority drop-down menu. Requirements with the lowest number (“1”) have the highest priority and are performed first. If a requirement fails, the remediation instructions that are configured for the requirement are shown to the user without additional requirements being tested. You can thereby minimize processing time by putting the requirements that are most likely to fail at a high priority.

Step 5 If you chose Link Distribution as the Requirement Type, you must fill in the File Link URL field. This field is where you enter the URL of the web page where users can find the install file or patch update that is needed.

Step 6 Enter a unique name in the Requirement Name field to identify the system requirement. The name will be visible to users on the Cisco NAA dialog box.

Creating a Custom Requirement (Cont.)


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules
Add Requirement
7
8
9

Requirement Type: Link Distribution

□ Do not enforce requirement Priority: 10

File Link URL: http://www.sysinternals.com/support/download

Requirement Name: Manage system startup files (Optional)

Description: Our security policy suggests you download this

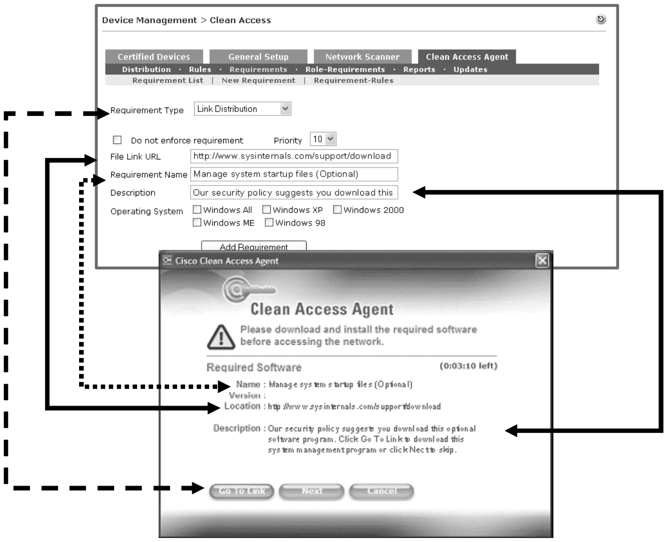
Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

Step 7 In the Description field, enter a description of the requirement and instructions that will be helpful to your users.

Step 8 Check a check box for an Operating System for the requirement that you are creating (at least one must be chosen).

Step 9 Click the **Add Requirement** button to save the settings for the download requirement. The requirement now appears in the Requirement List.

Relating the Requirements Form to the Cisco NAA Dialog Box



Device Management > Clean Access

Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules

Requirement Type: Link Distribution

□ Do not enforce requirement Priority: 10

File Link URL: http://www.sysinternals.com/support/download

Requirement Name: Manage system startup files (Optional)

Description: Our security policy suggests you download this

Operating System: □ Windows All □ Windows XP □ Windows 2000 □ Windows ME □ Windows 98

Add Requirement
Cisco Clean Access Agent
Clean Access Agent

Please download and install the required software before accessing the network.

Required Software (0:03:10 left)

Name : Manage system startup files (Optional)

Version :

Location : http://www.sysinternals.com/support/download

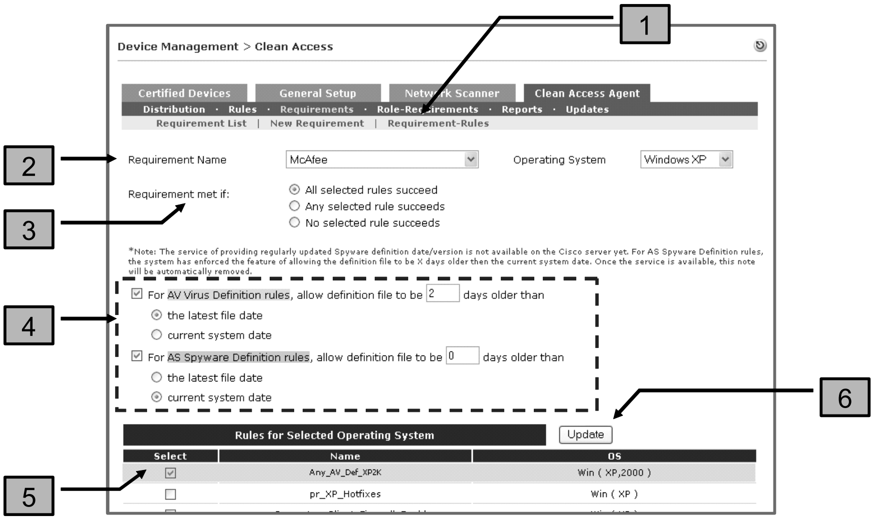
Description : Our security policy suggests you download this optional software program. Click Go To Link to download this system management program or click Next to skip.

The figure shows how the fields on the Requirements form relate to information that is found in the Cisco NAA dialog box.

Mapping Requirements to Rules and Roles

This topic describes how to map requirements to rules and roles.

Mapping Requirements to Rules


1
2
3
4
5
6
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Requirement List | New Requirement | Requirement-Rules
Update

Device Management > Clean Access

Requirement Name: McAfee — Operating System: Windows XP

Requirement met if:
● All selected rules succeed
○ Any selected rule succeeds
○ No selected rule succeeds

*Note: The service of providing regularly updated Spyware definition date/version is not available on the Cisco server yet. For AS Spyware Definition rules, the system has enforced the feature of allowing the definition file to be X days older then the current system date. Once the service is available, this note will be automatically removed.

☑ For AV Virus Definition rules, allow definition file to be 2 days older than
● the latest file date
○ current system date

☑ For AS Spyware Definition rules, allow definition file to be 0 days older than
○ the latest file date
● current system date

Rules for Selected Operating System

Select	Name	OS
☑	Any_AV_Def_XP2K	Win (XP,2000)
□	pr_XP_Hotfixes	Win (XP)

After the requirement is created and the remediation links and instructions are specified, you can map the requirement to a rule or to a set of rules. A rule-to-requirement mapping associates the rule set that checks whether the client system meets the requirement to the instructions and links that permit the user to make the client system comply.

Follow these six steps to map rules to a requirement:

Step 1 In the Device Management > Clean Access > Clean Access Agent tab, choose **Requirements > Requirement-Rules**.

Step 2 From the Requirement Name menu, choose the requirement that you want to map. The operating system for the requirement appears in the Operating System drop-down menu, and the Rules for Selected Operating System list is populated with all rules available for the chosen operating system.

Step 3 In the Requirements Met If area, choose one of these options:

- **All Selected Rules Succeed:** Choose this option if all the rules must be satisfied for the client to be considered in compliance with the requirement.
- **Any Selected Rule Succeeds:** Choose this option if at least one selected rule must be satisfied for the client to be considered in compliance with the requirement.
- **No Selected Rule Succeeds:** Choose this option if the selected rules must all fail for the client to be considered in compliance with the requirement.

Note If client machines are not in compliance with the requirement, clients must install the software that is associated with the requirement or take the steps that are instructed before being permitted access to the network.

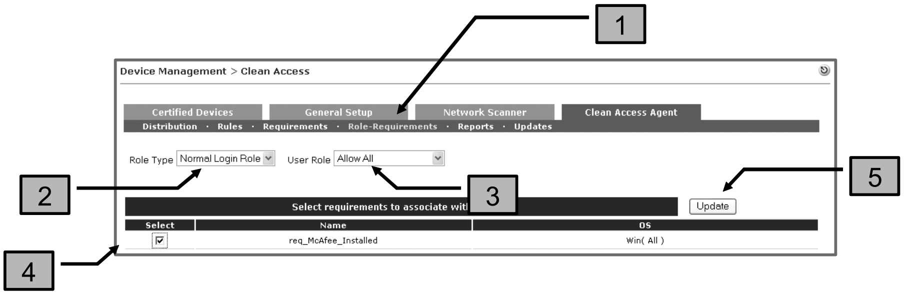
Step 4 Check the **AV Virus Definition Rules** check box and type a number of days in the text box to indicate the maximum age of the definition file. The default is "0," indicating that the definition date cannot be older than the file or system date.

Note Step 4 is an optional step that is used to configure the Cisco NAM to allow definition files on the client to be a number of days older than what the Cisco NAM has available from the Cisco NAC Appliance update server. This allows you to configure a flexible requirement so that when no new virus or spyware definition files are released from a product vendor, your clients can still pass the requirement and log onto the network.

Step 5 Click the **Select** box next to each rule that you want to associate with this requirement.

Step 6 Click the **Update** button.

Applying Requirements to a Role


1
2
3
4
5
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Update

Device Management > Clean Access

Role Type: Normal Login Role   User Role: Allow All

Select requirements to associate wit

Select	Name	OS
☑	req_McAfee_Installed	Win(All)

Now that the rule-to-requirement mapping is complete, you can apply the requirements to the user groups in the system.

Follow these five steps to apply requirements to a role:

Step 1 In the Device Management > Clean Access > Clean Access Agent tab, click the **Role-Requirements** link.

Step 2 From the Role Type drop-down menu, choose the type of role that you are configuring. In most Cisco cases, this role is the Normal Login Role.

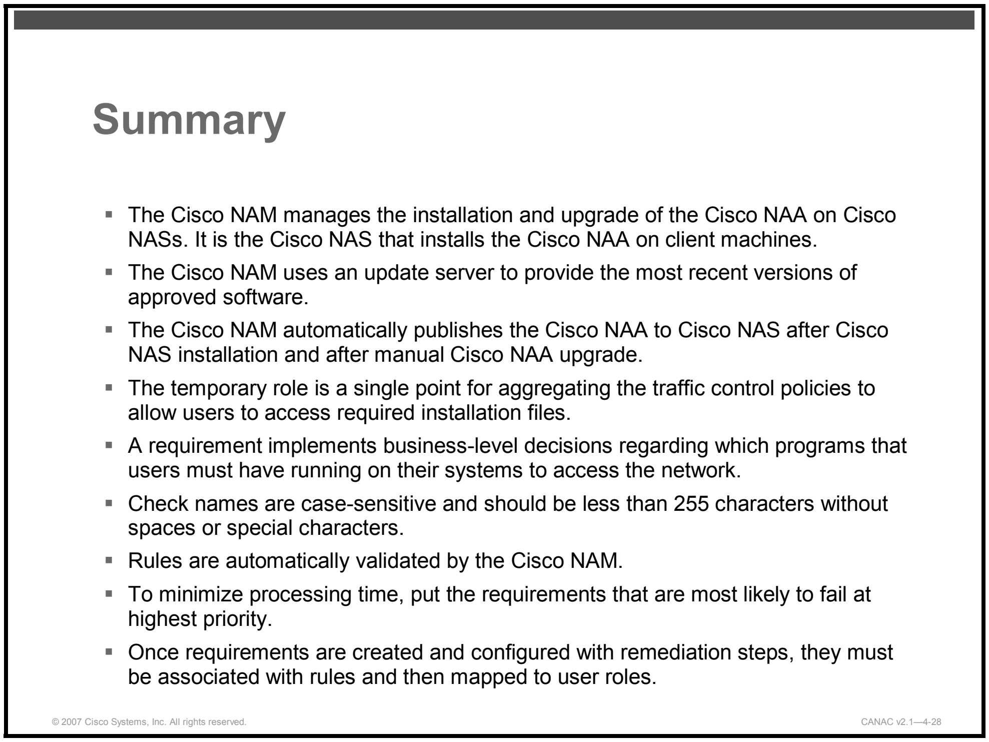
Step 3 Choose the name of the role from the User Role drop-down menu.

Step 4 Check the **Select** check box for each requirement that you want to apply to users in the selected role.

Step 5 Click the **Update** button.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- The Cisco NAM manages the installation and upgrade of the Cisco NAA on Cisco NASs. It is the Cisco NAS that installs the Cisco NAA on client machines.
- The Cisco NAM uses an update server to provide the most recent versions of approved software.
- The Cisco NAM automatically publishes the Cisco NAA to Cisco NAS after Cisco NAS installation and after manual Cisco NAA upgrade.
- The temporary role is a single point for aggregating the traffic control policies to allow users to access required installation files.
- A requirement implements business-level decisions regarding which programs that users must have running on their systems to access the network.
- Check names are case-sensitive and should be less than 255 characters without spaces or special characters.
- Rules are automatically validated by the Cisco NAM.
- To minimize processing time, put the requirements that are most likely to fail at highest priority.
- Once requirements are created and configured with remediation steps, they must be associated with rules and then mapped to user roles.

Lesson 4

Configuring Cisco NAM High Availability

Overview

Corporate networks must operate all the time, and therefore so must the security systems that protect them. By deploying Cisco Network Admission Control (NAC) Appliance Managers (Cisco NAMs) in high-availability mode, you can ensure that important monitoring, authentication, and reporting tasks continue in the event of an unexpected shutdown. This lesson describes how to configure Cisco NAMs for high availability.

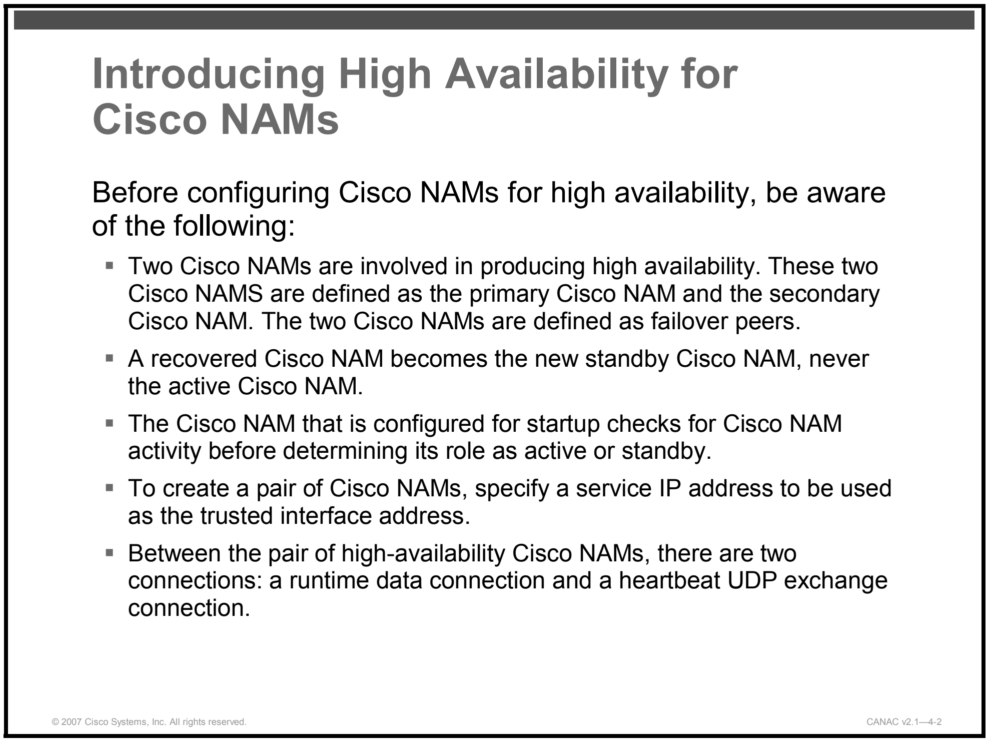
Objectives

Upon completing this lesson, you will be able to configure a high-availability pair of Cisco NAMs. This ability includes being able to meet these objectives:

- Describe how to configure high availability between two Cisco NAMs
- Describe how to establish a serial connection between two Cisco NAMs
- Describe how to configure a primary Cisco NAM for high availability
- Describe how to configure a secondary Cisco NAM for high availability

Introducing High Availability for Cisco NAMs

This topic describes how to configure high availability between two Cisco NAMs.



Introducing High Availability for Cisco NAMs

Before configuring Cisco NAMs for high availability, be aware of the following:

- Two Cisco NAMs are involved in producing high availability. These two Cisco NAMS are defined as the primary Cisco NAM and the secondary Cisco NAM. The two Cisco NAMs are defined as failover peers.
- A recovered Cisco NAM becomes the new standby Cisco NAM, never the active Cisco NAM.
- The Cisco NAM that is configured for startup checks for Cisco NAM activity before determining its role as active or standby.
- To create a pair of Cisco NAMs, specify a service IP address to be used as the trusted interface address.
- Between the pair of high-availability Cisco NAMs, there are two connections: a runtime data connection and a heartbeat UDP exchange connection.

CANAC v2.1—4-2

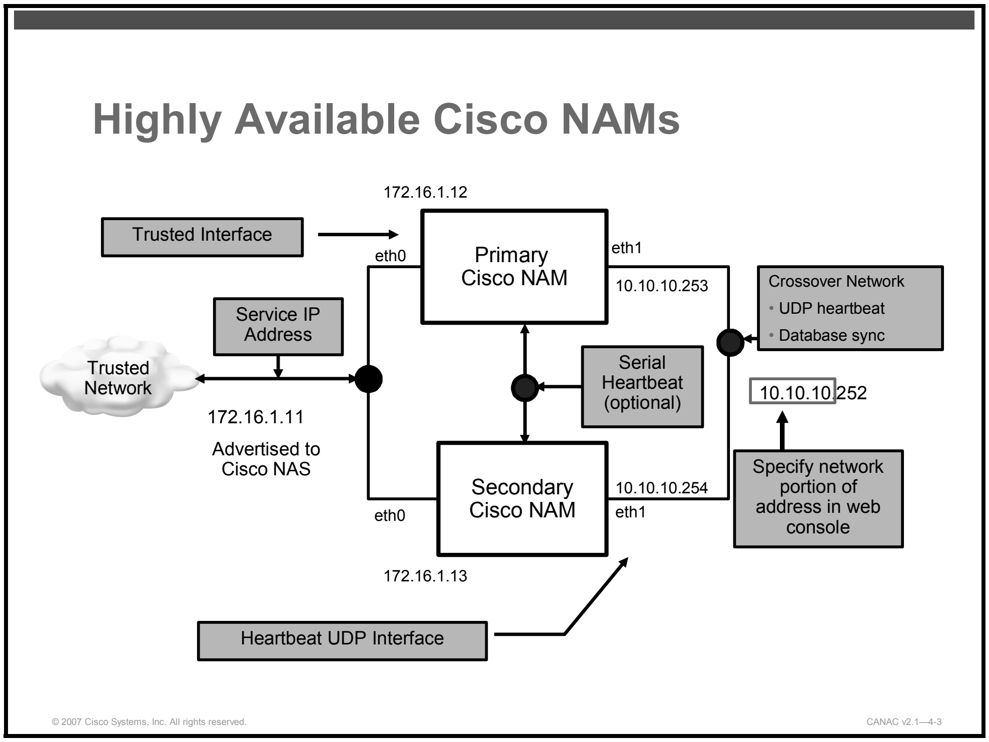
Implementing high availability ensures that Cisco NAM activities continue in the event of an unexpected Cisco NAM shutdown. The Cisco NAM high-availability mode is a two-server configuration in which a secondary Cisco NAM machine acts as a backup to a primary Cisco NAM machine. A highly available Cisco NAM pair requires that if the primary (active) Cisco NAM shuts down or stops responding to the peer Cisco NAM heartbeat signal, the secondary Cisco NAM assumes the role of the active Cisco NAM. Although you specify a primary and a secondary Cisco NAM at the time of configuration, these Cisco NAM roles are not permanent. If the primary (active) Cisco NAM shuts down, two things happen. First, the secondary Cisco NAM becomes the active Cisco NAM. Second, when the primary Cisco NAM restarts, this Cisco NAM assumes the standby role.

When the primary Cisco NAM starts up, it checks to see if the secondary Cisco NAM is active. If the secondary Cisco NAM is not active, then the primary Cisco NAM assumes the active role. If the secondary Cisco NAM is active, then the primary Cisco NAM assumes the role of the standby Cisco NAM.

Typically, a second Cisco NAM is added to an existing Cisco NAM to create a high-availability pair. For the pair to appear to the network and to the Cisco NAC Appliance Servers (Cisco NASs) as one entity, you must specify a service IP address to be used as the trusted virtual address (eth0) for the two Cisco NAMs. This service IP address is also used to generate the Secure Sockets Layer (SSL) certificate.

There are two types of connections between the Cisco NAM peers: one type of connection exchanges runtime data relating to the Cisco NAM activities, and the other type of connection exchanges the heartbeat signal. In high-availability mode, the Cisco NAM always uses the eth1 interface for both data exchange and heartbeat User Datagram Protocol (UDP) exchange. When the UDP heartbeat signal is not transmitted and received within a certain time period, the standby system becomes active. To provide an extra measure of security, you should take the optional step of adding a serial heartbeat connection between the Cisco NAM failover peers. This serial connection provides an additional method of heartbeat exchange that must fail before the standby system takes over.

Note Only the eth1 connection between the peers is mandatory.



Highly Available Cisco NAMs

172.16.1.12

Trusted Interface

eth0

Primary Cisco NAM

eth1

10.10.10.253

Crossover Network
- UDP heartbeat
- Database sync

Service IP Address

Trusted Network

Serial Heartbeat (optional)

10.10.10.252

172.16.1.11

Advertised to Cisco NAS

Secondary Cisco NAM

10.10.10.254

eth1

eth0

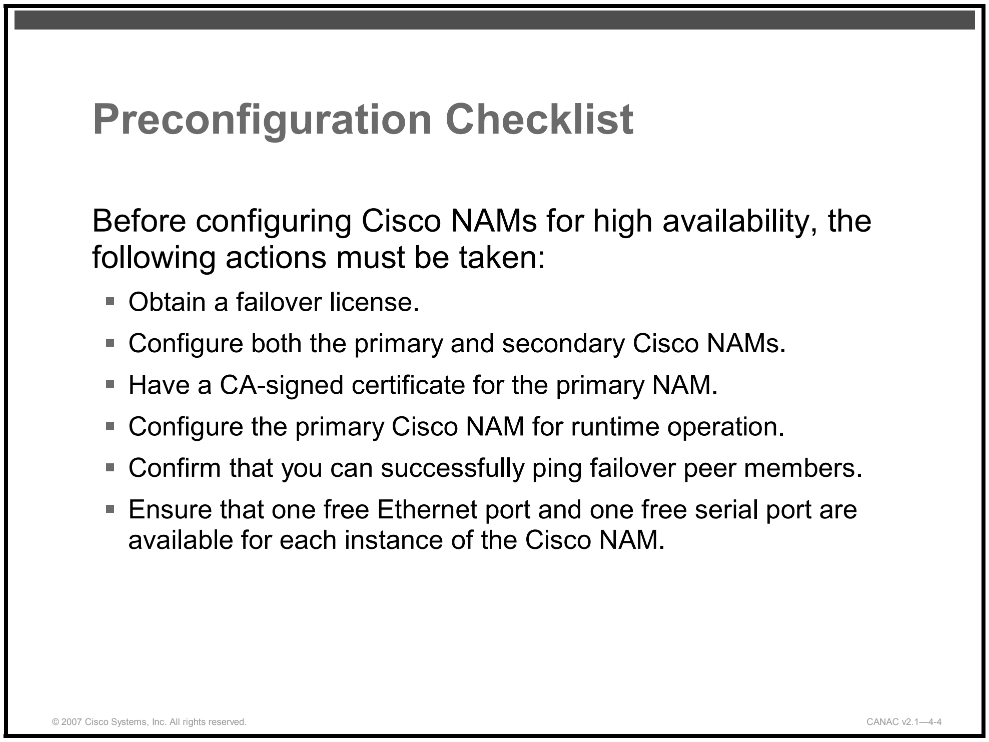
Specify network portion of address in web console

172.16.1.13

Heartbeat UDP Interface

To create the crossover network on which high-availability information is exchanged, you must connect the eth1 ports of the primary and secondary Cisco NAMs to each other and specify a private network address that is not currently routed in your organization (the default high-availability crossover network is 192.168.0.252). The primary Cisco NAM then creates a private, secure, two-node network using the eth1 ports of each Cisco NAM. This network exchanges UDP heartbeat traffic and synchronizes the Cisco NAM databases. Use the eth0 interface as the trusted interface address for each Cisco NAM.

For extra security, you can also connect the serial ports of each Cisco NAM to facilitate heartbeat exchange. In this case, both the UDP heartbeat and serial heartbeat interfaces must fail before the secondary system takes over. The Cisco NAM always uses eth1 as the heartbeat UDP interface.



Preconfiguration Checklist

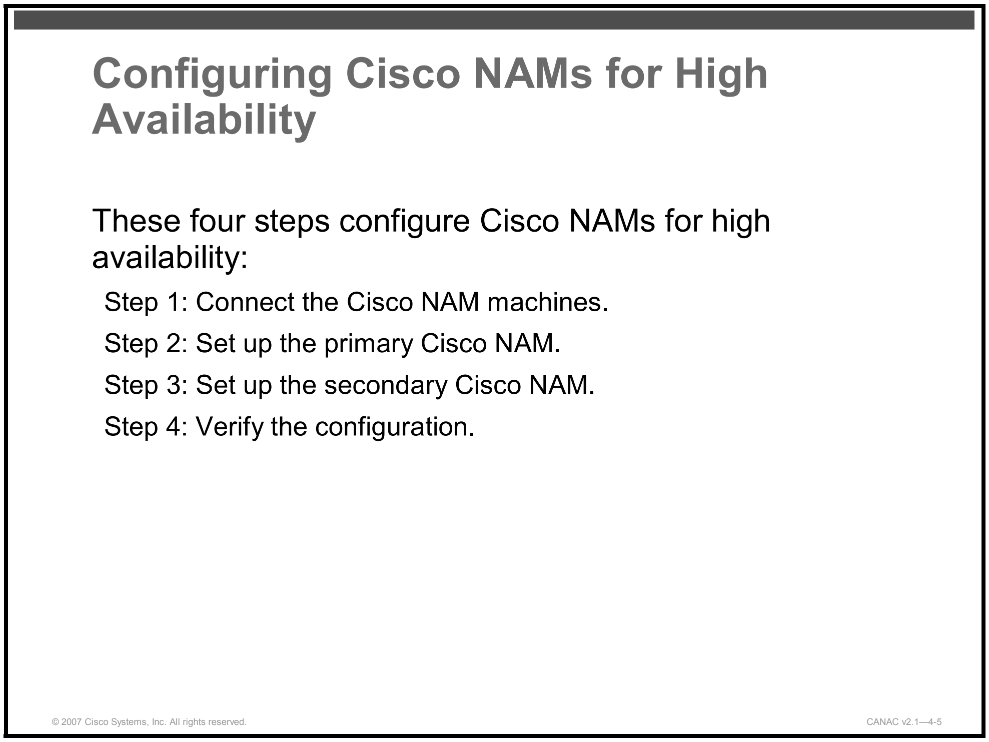
Before configuring Cisco NAMs for high availability, the following actions must be taken:

- Obtain a failover license.
- Configure both the primary and secondary Cisco NAMs.
- Have a CA-signed certificate for the primary NAM.
- Configure the primary Cisco NAM for runtime operation.
- Confirm that you can successfully ping failover peer members.
- Ensure that one free Ethernet port and one free serial port are available for each instance of the Cisco NAM.

CANAC v2.1—4-4

Before configuring Cisco NAMs for high availability, ensure that the following conditions are true:

- You have a high-availability (failover) license.
- Both Cisco NAMs that you want to use are installed and configured as provided for by the installation script.
- You have a certificate authority (CA)-signed certificate for the primary Cisco NAM.
- The primary Cisco NAM is fully configured for runtime operation. This configuration means that connections to authentication sources, policies, user roles, access points, and so on are all specified. The configuration in the primary Cisco NAM is automatically duplicated in the secondary Cisco NAM when the two machines are configured to be primary and secondary Cisco NAMs (as failover peers).
- Both Cisco NAMs are accessible on your network. You can demonstrate connectivity to members of the pair using the **ping** command.
- The server machines on which the Cisco NAM software is installed have a free Ethernet port (eth1) and one free serial port. Use the specification manuals for the server hardware to identify the serial port (ttyS0 or ttyS1) on each failover peer.



Configuring Cisco NAMs for High Availability

These four steps configure Cisco NAMs for high availability:

Step 1: Connect the Cisco NAM machines.

Step 2: Set up the primary Cisco NAM.

Step 3: Set up the secondary Cisco NAM.

Step 4: Verify the configuration.

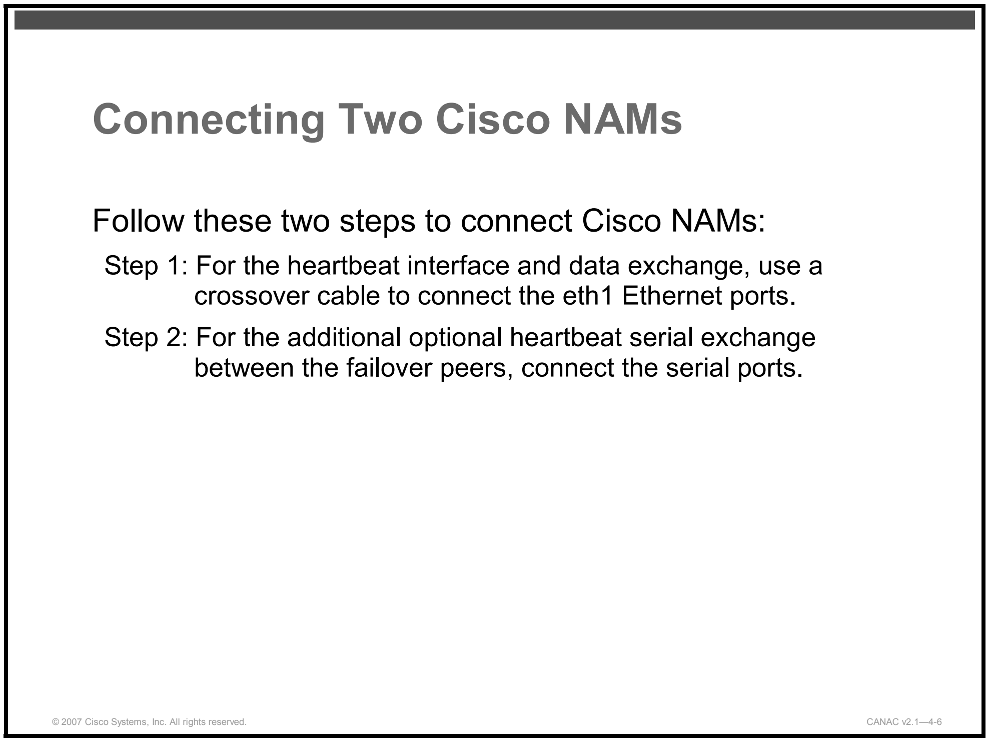
CANAC v2.1—4-5

The figure lists the steps (explained in detail in the subsequent topics of this lesson) that are used to configure a pair of Cisco NAMs for high availability.

Note For instructions on how to upgrade an existing pair of Cisco NAMs, refer to the Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.0(2), available at http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html.

Establishing a Serial Connection Between Cisco NAMs

This topic describes how to establish a serial connection between two Cisco NAMs.



Connecting Two Cisco NAMs

Follow these two steps to connect Cisco NAMs:

Step 1: For the heartbeat interface and data exchange, use a crossover cable to connect the eth1 Ethernet ports.

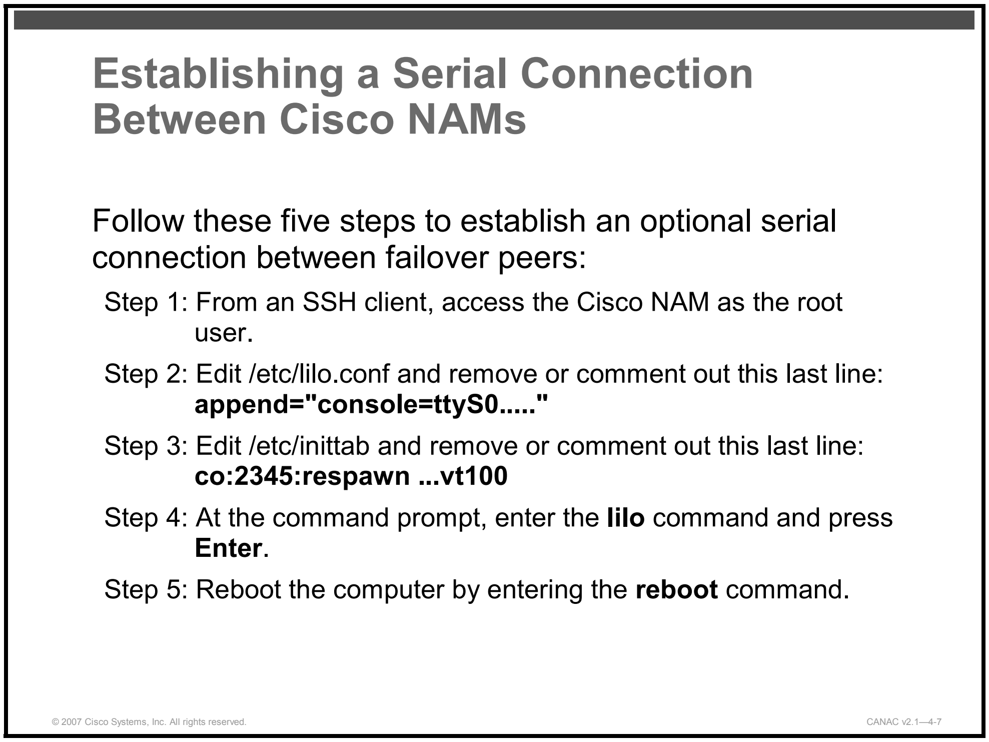
Step 2: For the additional optional heartbeat serial exchange between the failover peers, connect the serial ports.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-6

Follow these two steps to physically connect two Cisco NAMs:

Step 1 Use a crossover cable to connect the eth1 Ethernet ports of the Cisco NAM machines. This connection is used for the heartbeat UDP interface and data exchange (database mirroring) between the failover peers.

Step 2 If you decide to add an optional serial connection, use a serial cable to connect the two serial ports. This connection is used for the additional and optional heartbeat serial exchange (keepalive message) between the failover peers.



Establishing a Serial Connection Between Cisco NAMs

Follow these five steps to establish an optional serial connection between failover peers:

Step 1: From an SSH client, access the Cisco NAM as the root user.

Step 2: Edit /etc/lilo.conf and remove or comment out this last line: **append="console=ttyS0....."**

Step 3: Edit /etc/inittab and remove or comment out this last line: **co:2345:respawn ...vt100**

Step 4: At the command prompt, enter the **lilo** command and press **Enter**.

Step 5: Reboot the computer by entering the **reboot** command.

CANAC v2.1—4-7

If the computer that is running the Cisco NAM software has two serial ports, you can use the additional port for the serial heartbeat connection. By default, the first serial port that is detected on the Cisco NAM server is configured for console input and output. This configuration facilitates program installation and other types of administrative access.

Note If the computer has only one serial port (ttyS0), you can reconfigure the port to serve as the high-availability heartbeat connection. This connection is possible because Secure Shell (SSH) Protocol can access the command-line interface (CLI) of the Cisco NAM after the Cisco NAM is installed.

Follow these five steps to reconfigure ttyS0 as the heartbeat connection on both the primary and standby Cisco NAMs:

Step 1 From an SSH client, access the Cisco NAM as a root user.

Step 2 Edit the /etc/lilo.conf file and remove or comment out this last line:

```
append="console=ttyS0....."
```

Note This last line causes console output to be redirected to the serial port.

Tip To comment out a line, add the "#" character to the start of the line. Lines beginning with this character are ignored by the Cisco NAM.

Step 3 Edit the /etc/inittab file and remove or comment out this last line:

```
co:2345:respawn ...vt100
```

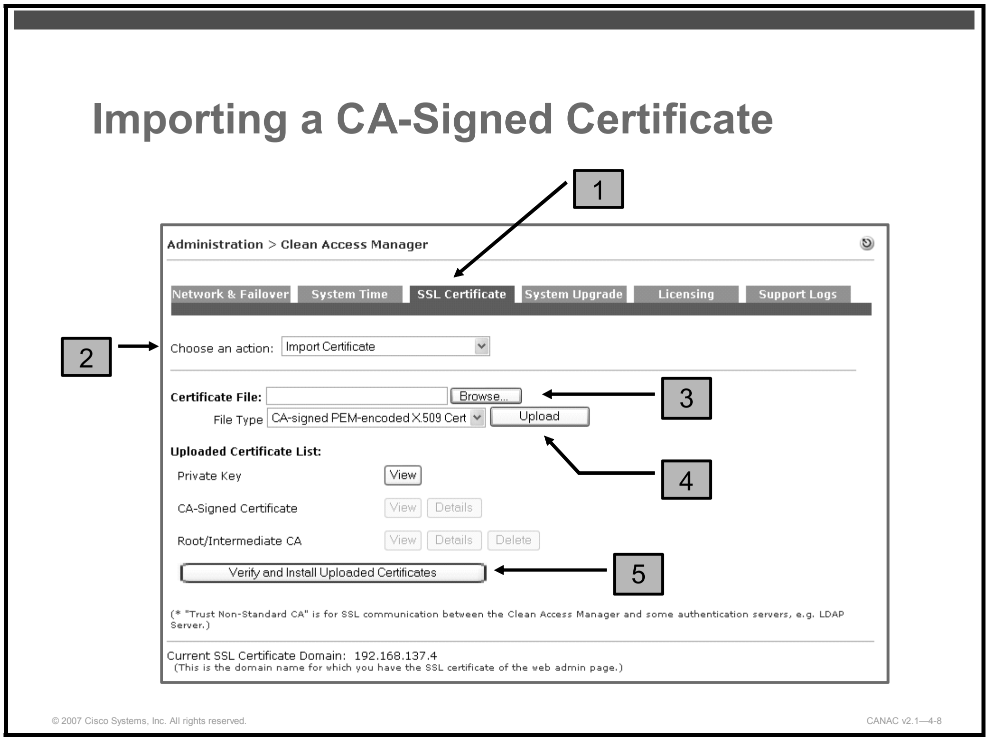
Note This last line causes a login terminal to be started on the serial port.

Step 4 At the command prompt, enter the **lilo** command and press **Enter**. This starts Lilo, which is the Linux bootloader.

Step 5 Reboot the computer by entering the **reboot** command.

Configuring the Primary Cisco NAM

This topic describes how to configure a primary Cisco NAM for high availability. There are two multistep tasks that you must follow to configure the primary Cisco NAM for high availability. First, you must import the CA-signed certificate and export an SSL private key for the secondary Cisco NAM to use. Second, you must configure the primary Cisco NAM network and failover settings.



Importing a CA-Signed Certificate

Administration > Clean Access Manager

Choose an action: Import Certificate

Certificate File:

File Type CA-signed PEM-encoded X.509 Cert

Uploaded Certificate List:

Private Key

CA-Signed Certificate

Root/Intermediate CA

(* "Trust Non-Standard CA" is for SSL communication between the Clean Access Manager and some authentication servers, e.g. LDAP Server.)

Current SSL Certificate Domain: 192.168.137.4
(This is the domain name for which you have the SSL certificate of the web admin page.)

© 2007 Cisco Systems, Inc. All rights reserved.

CANAC v2.1—4-8

You must have a CA-signed certificate or self-signed certificate for the primary Cisco NAM before you can begin this procedure. On the Cisco NAM administrator console for the primary Cisco NAM, follow these five steps when using a CA-signed certificate:

Step 1 From the administrator console of the primary Cisco NAM, choose **Administration > Clean Access Manager** and click the **SSL Certificate** tab.

Step 2 Choose **Import Certificate** from the Choose an Action drop-down menu.

Note Unneeded buttons are disabled.

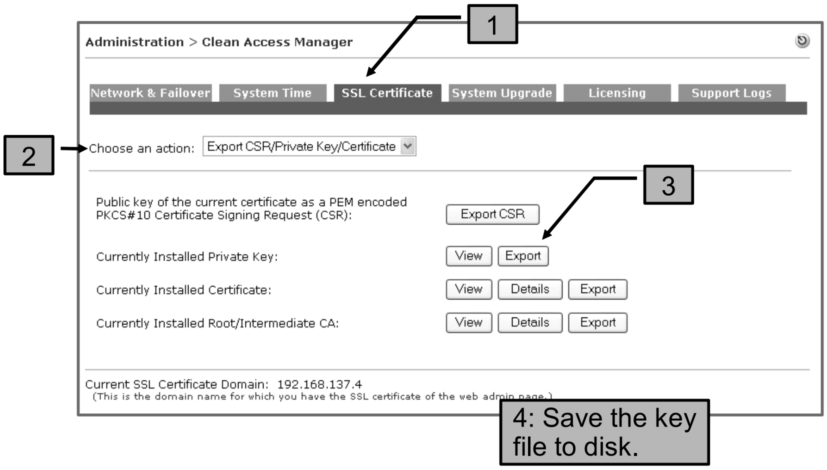
Step 3 Click **Browse** next to the Certificate File field and navigate to the certificate file that you want to import.

Step 4 Click **Upload** to import the certificate.

Step 5 Click **Verify and Install Uploaded Certificates** to verify the entire certificate chain and private key in the temporary store and install the verified certificate files to the correct locations in the Cisco NAM.

Note If any files are missing, errors appear that indicate which files need to be uploaded. For example, if an intermediate CA certificate is required for the CA that you are using, upload it to the Cisco NAM temporary store in order for the certificate chain to be verified and installed on the Cisco NAM.

Exporting an SSL Private Key



Administration > Clean Access Manager

Choose an action: Export CSR/Private Key/Certificate

Public key of the current certificate as a PEM encoded PKCS#10 Certificate Signing Request (CSR): Export CSR

Currently Installed Private Key: View Export

Currently Installed Certificate: View Details Export

Currently Installed Root/Intermediate CA: View Details Export

Current SSL Certificate Domain: 192.168.137.4
(This is the domain name for which you have the SSL certificate of the web admin page.)

4: Save the key file to disk.

CANAC v2.1—4-9

Follow these four steps to export an SSL private key to a file so that you can use this key to configure the secondary Cisco NAM:

Note	The instructions in this section assume that you will export the certificate from the primary Cisco NAM.

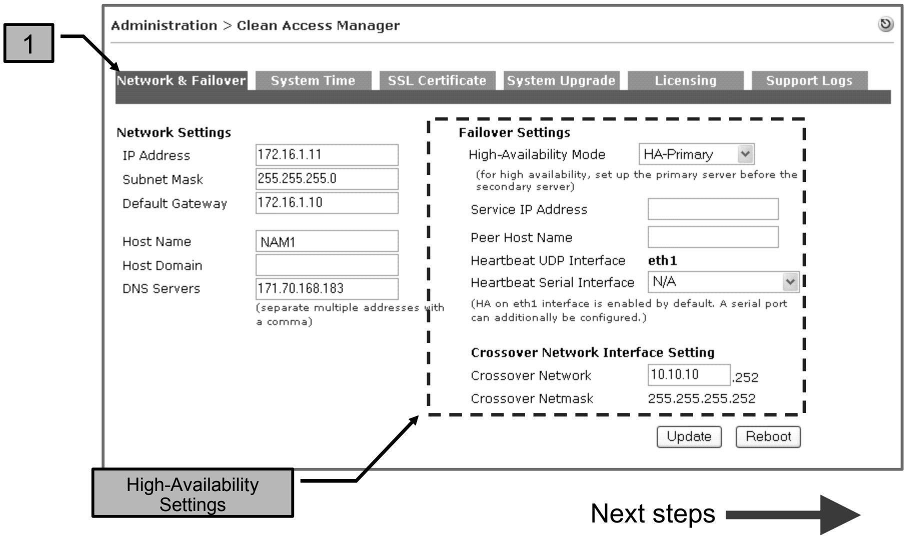
Step 1 Open the administrator console for the primary Cisco NAM and choose **Administration > Clean Access Manager > SSL Certificate**.

Step 2 Choose **Export CSR/Private Key/Certificate** from the Choose an Action drop-down menu.

Step 3 Click **Export** next to Currently Installed Private Key to export the SSL private key.

Step 4 Save the key file to disk. You will import this file into the secondary Cisco NAM later.

Configuring Primary Network and Failover Settings



Administration > Clean Access Manager

Network & Failover | System Time | SSL Certificate | System Upgrade | Licensing | Support Logs

Network Settings

IP Address	172.16.1.11
Subnet Mask	255.255.255.0
Default Gateway	172.16.1.10
Host Name	NAM1
Host Domain	
DNS Servers	171.70.168.183

(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode	HA-Primary

(for high availability, set up the primary server before the secondary server)

Service IP Address	
Peer Host Name	
Heartbeat UDP Interface	**eth1**
Heartbeat Serial Interface	N/A

(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

Crossover Network Interface Setting

Crossover Network	10.10.10 .252
Crossover Netmask	255.255.255.252

Update | Reboot

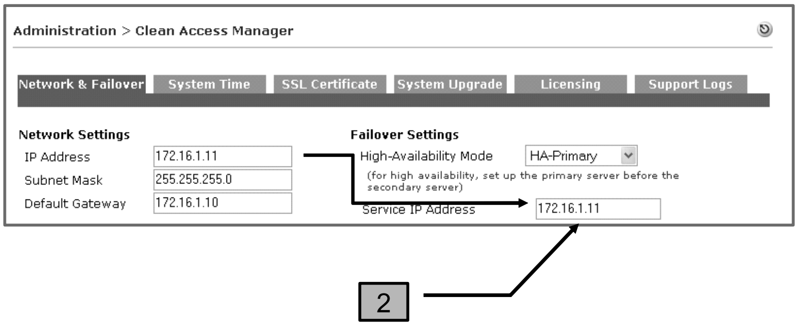
Next steps

CANAC v2.1—4-10

Follow these seven steps to configure primary network and failover settings:

Step 1 Choose **Administration** > **Clean Access Manager** and click the **Network & Failover** tab. The figure shows a dashed box around the failover setting you will configure. Choose the **HA-Primary** option from the High-Availability Mode drop-down menu. The high-availability settings appear inside the dashed box in the figure.

Configuring Primary Network and Failover Settings (Cont.)



Administration > Clean Access Manager

Network & Failover | System Time | SSL Certificate | System Upgrade | Licensing | Support Logs

Network Settings

IP Address	172.16.1.11
Subnet Mask	255.255.255.0
Default Gateway	172.16.1.10

Failover Settings

High-Availability Mode	HA-Primary

(for high availability, set up the primary server before the secondary server)

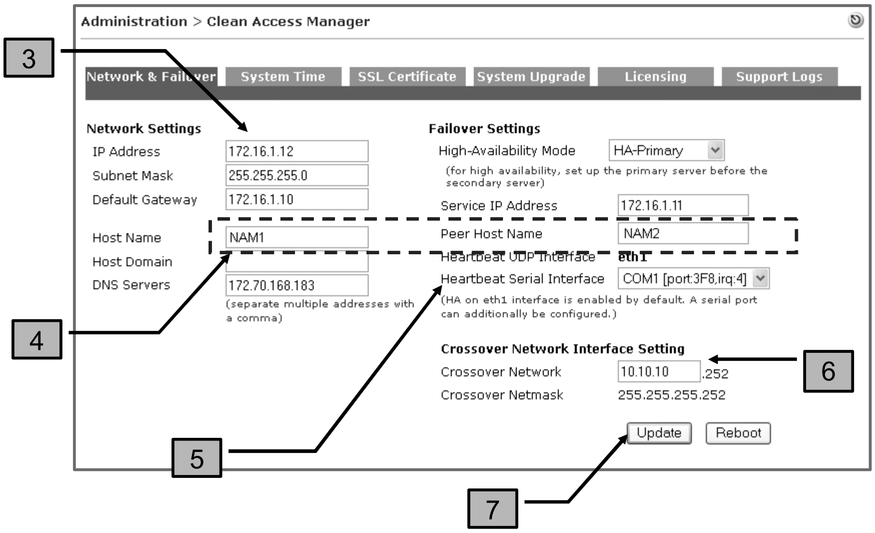
Service IP Address	172.16.1.11

Next steps

CANAC v2.1—4-11

Step 2 Copy the value from the IP Address field under Network Settings and enter it in the Service IP Address field.

Configuring Primary Network and Failover Settings (Cont.)



Administration > Clean Access Manager

Network Settings

IP Address: 172.16.1.12
Subnet Mask: 255.255.255.0
Default Gateway: 172.16.1.10
Host Name: NAM1
Host Domain:
DNS Servers: 172.70.168.183
(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode: HA-Primary
(for high availability, set up the primary server before the secondary server)
Service IP Address: 172.16.1.11
Peer Host Name: NAM2
Heartbeat UDP Interface: **eth1**
Heartbeat Serial Interface: COM1 [port:3F8,irq:4]
(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

Crossover Network Interface Setting

Crossover Network: 10.10.10 .252
Crossover Netmask: 255.255.255.252

CANAC v2.1—4-12

Step 3 Change the IP address under Network Settings to an available address, for example: `172.16.1.12.` This is the new physical IP address of the primary Cisco NAM (eth0 interface).

Step 4 Each Cisco NAM must have a unique host name (such as NAM1 and NAM2). Enter the host name of the primary Cisco NAM in the Host Name field under Network Settings. Enter the host name of the secondary Cisco NAM in the Peer Host Name field under Failover Settings. The dashed box in the figure shows the location of the Host Name and the Peer Host Name fields.

Note A host name field value is mandatory when setting up high availability. The host domain field value is optional. The Host Name and Peer Host Name fields are case-sensitive. Ensure that you later match what is entered here with what is entered for the secondary Cisco NAM.

Step 5 From the Heartbeat Serial Interface drop-down menu, choose the serial port to which you connected the serial cable of the primary Cisco NAM. Enter N/A for this field if you are not using a serial connection.

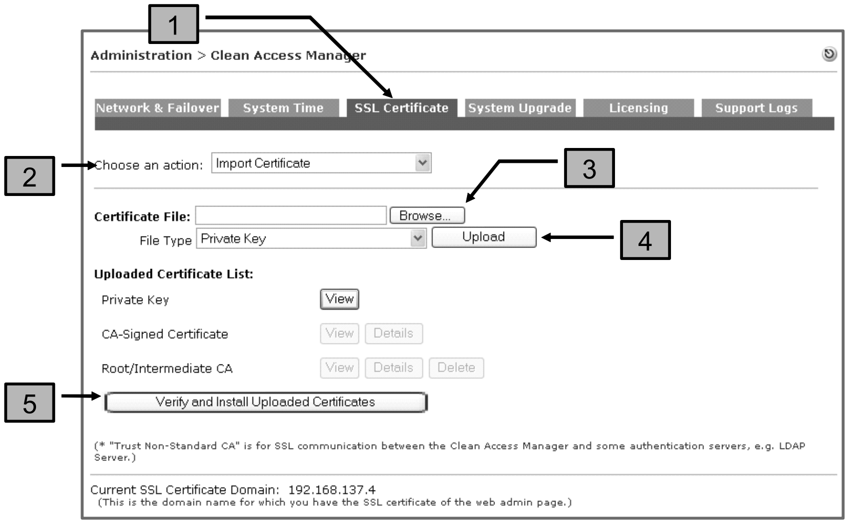
Step 6 To maintain synchronization, the failover peers exchange data via a crossover network. You must specify the first three octets of a private network address space such as 10.10.10 in the Crossover Network field.

Step 7 Click the **Update** button. Click **Reboot** to restart the Cisco NAM.

Configuring the Secondary Cisco NAM

This topic describes how to configure a secondary Cisco NAM for high availability.

Importing the SSL Private Key and the CA-Signed Certificate



Administration > Clean Access Manager

Choose an action: Import Certificate

Certificate File:

File Type Private Key

Uploaded Certificate List:

Private Key

CA-Signed Certificate

Root/Intermediate CA

(* "Trust Non-Standard CA" is for SSL communication between the Clean Access Manager and some authentication servers, e.g. LDAP Server.)

Current SSL Certificate Domain: 192.168.137.4
(This is the domain name for which you have the SSL certificate of the web admin page.)

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-13

Before you begin configuring the secondary Cisco NAM, ensure that the private key and SSL certificate files that are associated with the primary Cisco NAM are available. You should create a backup of the current private key of the secondary Cisco NAM before making these changes.

Follow these five steps to import the private key file and the CA-signed certificate from the primary Cisco NAM to the secondary Cisco NAM:

Step 1 Open the Cisco NAM administrator console for the secondary Cisco NAM. Choose **Administration > Clean Access Manager > SSL Certificate.**

Step 2 In the SSL Certificate tab, choose **Import Certificate** from the Choose an Action drop-down menu.

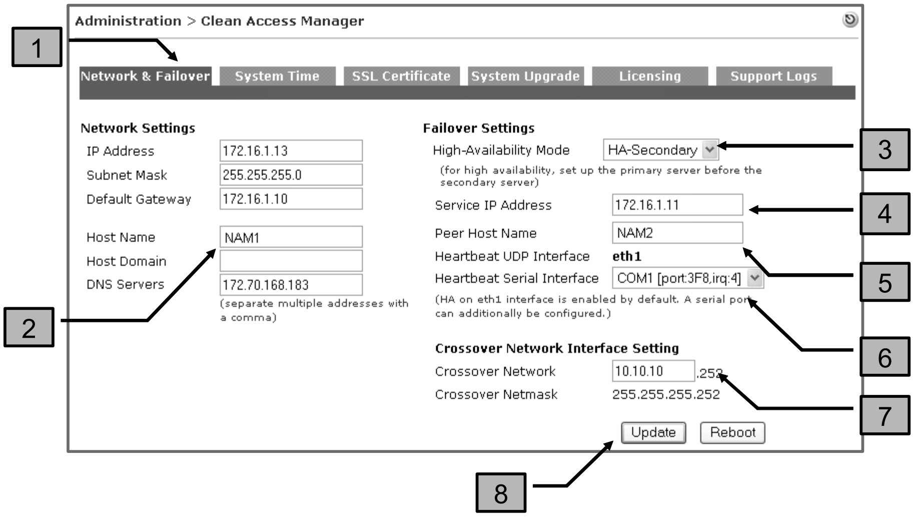
Step 3 Click **Browse** next to the Certificate File field. Browse to the private key file that you want to import.

Step 4 Choose **Private Key** from the File Type drop-down menu. Click **Upload.**

Step 5 Click **Verify and Install Uploaded Certificates** to verify the entire certificate chain and private key in the temporary store and install the verified certificate files to the correct locations in the Cisco NAM.

Note If any files are missing, errors appear that indicate which files need to be uploaded. For example, if an intermediate CA certificate is required for the CA that you are using, upload it to the Cisco NAM temporary store in order for the certificate chain to be verified and installed on the Cisco NAM.

Configuring Secondary Network and Failover Settings



Administration > Clean Access Manager

Network Settings

IP Address: 172.16.1.13
Subnet Mask: 255.255.255.0
Default Gateway: 172.16.1.10

Host Name: NAM1
Host Domain:
DNS Servers: 172.70.168.183
(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode: HA-Secondary
(for high availability, set up the primary server before the secondary server)
Service IP Address: 172.16.1.11
Peer Host Name: NAM2
Heartbeat UDP Interface: eth1
Heartbeat Serial Interface: COM1 [port:3F8,irq:4]
(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

Crossover Network Interface Setting

Crossover Network: 10.10.10 .252
Crossover Netmask: 255.255.255.252

CANAC v2.1—4-14

Follow these eight steps to configure the secondary Cisco NAM network and failover settings:

Step 1 Choose **Administration > Clean Access Manager** > **Network & Failover**. Change the IP address in the IP Address field under Network Settings to an address that is different from the primary Cisco NAM IP address and the Service IP address.

Step 2 Enter the same host name value in the Host Name field under Network Settings that was set for the peer host name in the primary Cisco NAM configuration.

Note The Host Name and Peer Host Name fields are case-sensitive. Ensure that you match what is entered here with what was entered for the primary Cisco NAM.

Step 3 Choose the **HA-Secondary** option from the High-Availability Mode drop-down menu under Failover Settings. The high-availability settings appear.

Step 4 Enter the same value in the Service IP Address field under Failover Settings that was set for the Service IP in the primary Cisco NAM.

Step 5 Enter the same peer host name in the Peer Host Name field under Failover Settings that was entered for the primary Cisco NAM host name.

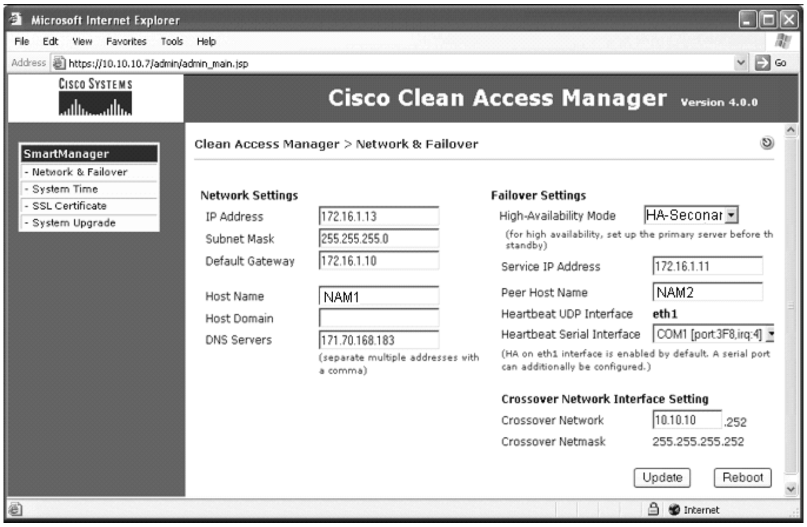
Step 6 From the Heartbeat Serial Interface drop-down menu, choose the serial port to which you connected the serial cable of the primary Cisco NAM. Enter N/A for the port if you are not using a serial connection.

Step 7 Enter the same values for the Crossover Network Interface Settings fields that were set for the primary Cisco NAM.

Step 8 Click the **Update** button. Click **Reboot** to restart the secondary Cisco NAM.

Note When the secondary Cisco NAM starts up, it automatically synchronizes its database with the database of the primary Cisco NAM.

Verifying Secondary Cisco NAM Configuration


Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.10.10.7/admin/admin_main.jsp
Go
Cisco Systems
Cisco Clean Access Manager Version 4.0.0
SmartManager
- Network & Failover
- System Time
- SSL Certificate
- System Upgrade
Update
Reboot
Internet

Clean Access Manager > Network & Failover

Network Settings

IP Address: 172.16.1.13
Subnet Mask: 255.255.255.0
Default Gateway: 172.16.1.10

Host Name: NAM1
Host Domain:
DNS Servers: 171.70.168.183
(separate multiple addresses with a comma)

Failover Settings

High-Availability Mode: HA-Seconar
(for high availability, set up the primary server before th standby)
Service IP Address: 172.16.1.11
Peer Host Name: NAM2
Heartbeat UDP Interface: eth1
Heartbeat Serial Interface: COM1 [port:3F8,irq:4]
(HA on eth1 interface is enabled by default. A serial port can additionally be configured.)

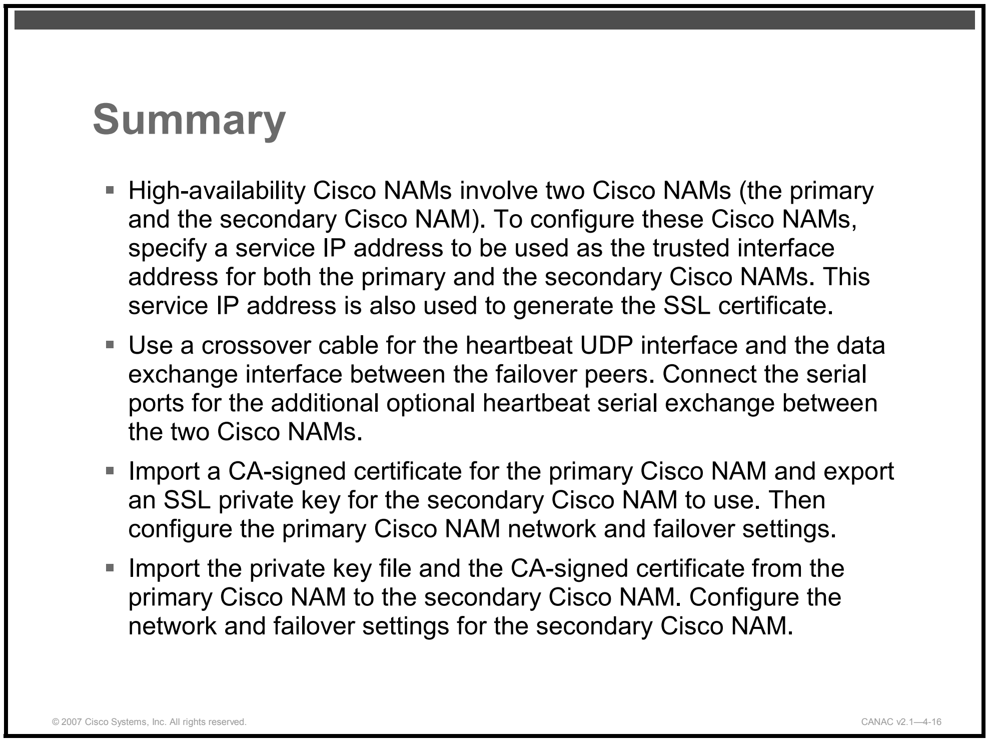
Crossover Network Interface Setting

Crossover Network: 10.10.10 .252
Crossover Netmask: 255.255.255.252

To verify the correct configuration of the secondary Cisco NAM, open the administrator console for this Cisco NAM. Confirm that the administrator console for the secondary Cisco NAM now has only one management module.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- High-availability Cisco NAMs involve two Cisco NAMs (the primary and the secondary Cisco NAM). To configure these Cisco NAMs, specify a service IP address to be used as the trusted interface address for both the primary and the secondary Cisco NAMs. This service IP address is also used to generate the SSL certificate.
- Use a crossover cable for the heartbeat UDP interface and the data exchange interface between the failover peers. Connect the serial ports for the additional optional heartbeat serial exchange between the two Cisco NAMs.
- Import a CA-signed certificate for the primary Cisco NAM and export an SSL private key for the secondary Cisco NAM to use. Then configure the primary Cisco NAM network and failover settings.
- Import the private key file and the CA-signed certificate from the primary Cisco NAM to the secondary Cisco NAM. Configure the network and failover settings for the secondary Cisco NAM.

CANAC v2.1—4-16

Lesson 5

Configuring Cisco NAS High Availability

Overview

It is important that more than one part of a company security system is highly available. To provide a comprehensive failover strategy for a Cisco Network Admission Control (NAC) Appliance solution, you must ensure that Cisco NAC Appliance Managers (Cisco NAMs) and Cisco NAC Appliance Servers (Cisco NASs) are highly available. Deploying Cisco NASs in high-availability mode ensures that important monitoring, authentication, and reporting tasks continue in the event of an unexpected shutdown. This lesson describes how to configure Cisco NASs for high availability.

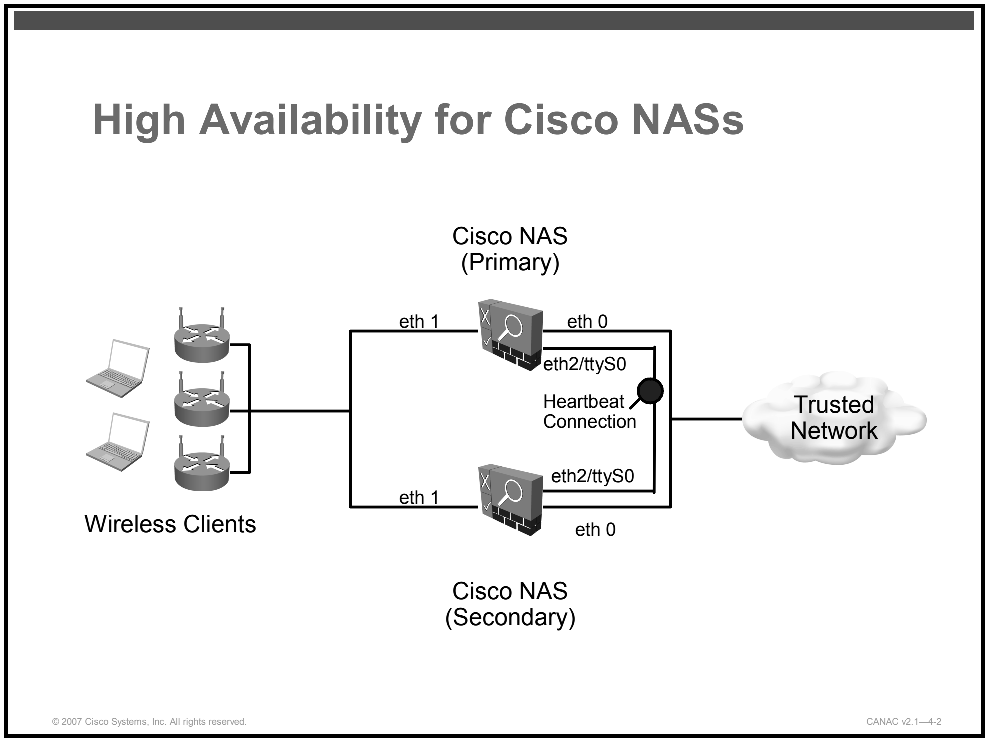
Objectives

Upon completing this lesson, you will be able to configure a high-availability pair of Cisco NASs. This ability includes being able to meet these objectives:

- Describe how to configure high availability between two Cisco NASs
- Describe how to configure the primary Cisco NAS for high availability
- Describe how to configure the secondary Cisco NAS for high availability
- Describe how to test the Cisco NAS high-availability configuration
- Describe how to configure DHCP failover

Introducing High Availability for Cisco NASs

This topic describes how to configure high availability between two Cisco NASs.



High Availability for Cisco NASs

CANAC v2.1—4-2

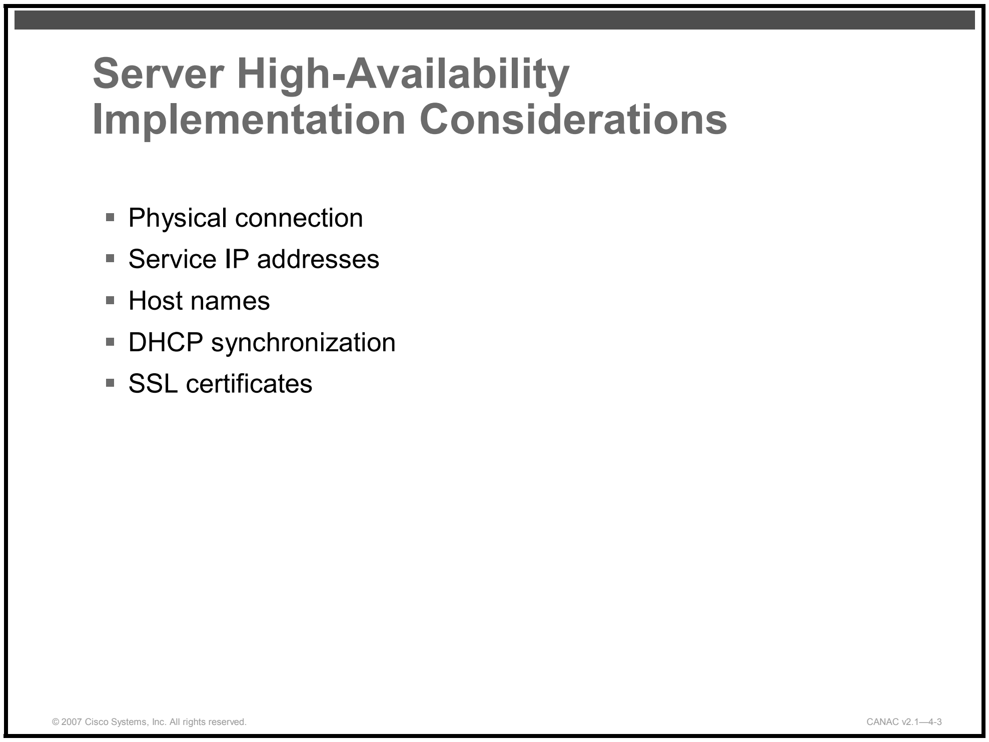
The figure shows how Cisco NAC Appliance supports two-node Cisco NAS clusters in which a secondary Cisco NAS backs up a primary Cisco NAS.

The secondary Cisco NAS monitors the health of the primary Cisco NAS via a heartbeat signal exchanged on a dedicated Ethernet or serial connection. If the secondary Cisco NAS cannot detect a heartbeat signal from the primary Cisco NAS, the secondary Cisco NAS becomes the active Cisco NAS.

Note Cisco NAS high-availability failover works the same way that Cisco NAM high-availability failover works.

Specifying a primary and secondary Cisco NAS at configuration time does not make these roles permanent. If the primary Cisco NAS stops working, the secondary Cisco NAS becomes the active Cisco NAS. When the primary Cisco NAS restarts, this Cisco NAS assumes the standby role. When the primary Cisco NAS restarts, it checks to see if the secondary Cisco NAS is active. If the secondary Cisco NAS is not active, the primary Cisco NAS becomes active. If the secondary Cisco NAS is active, the primary Cisco NAS becomes the standby Cisco NAS.

Note Starting with Cisco NAC Appliance Release 4.0.3.1, the primary Cisco NAS can also fail over if the eth1 or eth0 fails. You can configure the eth1 and eth0 interfaces on the primary and secondary Cisco NAS to ping two different IP addresses of your choice. If the primary Cisco NAS cannot ping its eth1 or its eth0 external IP address, but the secondary Cisco NAS can, the primary Cisco NAS will fail and the secondary Cisco NAS will become active. If the secondary failover peer cannot ping an external IP address either, failover does not happen.



Server High-Availability Implementation Considerations

- Physical connection
- Service IP addresses
- Host names
- DHCP synchronization
- SSL certificates

CANAC v2.1—4-3

Before implementing a high-availability Cisco NAS, be aware of these implementation considerations:

- **Physical connection:** For the heartbeat signals, you can use eth0 for User Datagram Protocol (UDP) heartbeat and the serial port (ttyS0) for the serial heartbeat.

  When the UDP heartbeat interface is specified, it sends UDP heartbeat traffic that is related to high availability. Servers that are set up as Cisco NASs typically use both available interfaces (eth0 and eth1), with eth0 configured as the trusted network interface. In some cases, you can install an additional network interface card (NIC) to provide an additional interface (eth2) that is dedicated to the UDP heartbeat. If you are installing an additional NIC, configure the IP address for the eth2 interface.

  A serial heartbeat connection (ttyS0) generally requires that the server machine that will function as a Cisco NAS has at least two serial ports. One port is used for the serial heartbeat connection and the other is used to access the Cisco NAS for configuration tasks.

Caution Do not connect the serial cable before starting high-availability (failover) configuration. The serial cable must be connected after the configuration is complete.

- **Service IP addresses:** In addition to the IP addresses for the trusted and untrusted interfaces for each individual Cisco NAS, you must provide two service IP addresses for the trusted and untrusted interfaces of the Cisco NAS failover peers. A service IP address is the common IP address that the external network uses to address the failover peers.
- **Host names:** Each Cisco NAS must have a unique host name.
- **DHCP synchronization:** If the Cisco NASs operate as DHCP servers (not in DHCP relay or pass-through mode), additional configuration steps must be taken to enable the Cisco NASs to keep their DHCP-related information synchronized. DHCP information, such as information regarding active leases and lease times, is exchanged by a Secure Shell (SSH) protocol tunnel, which you configure.

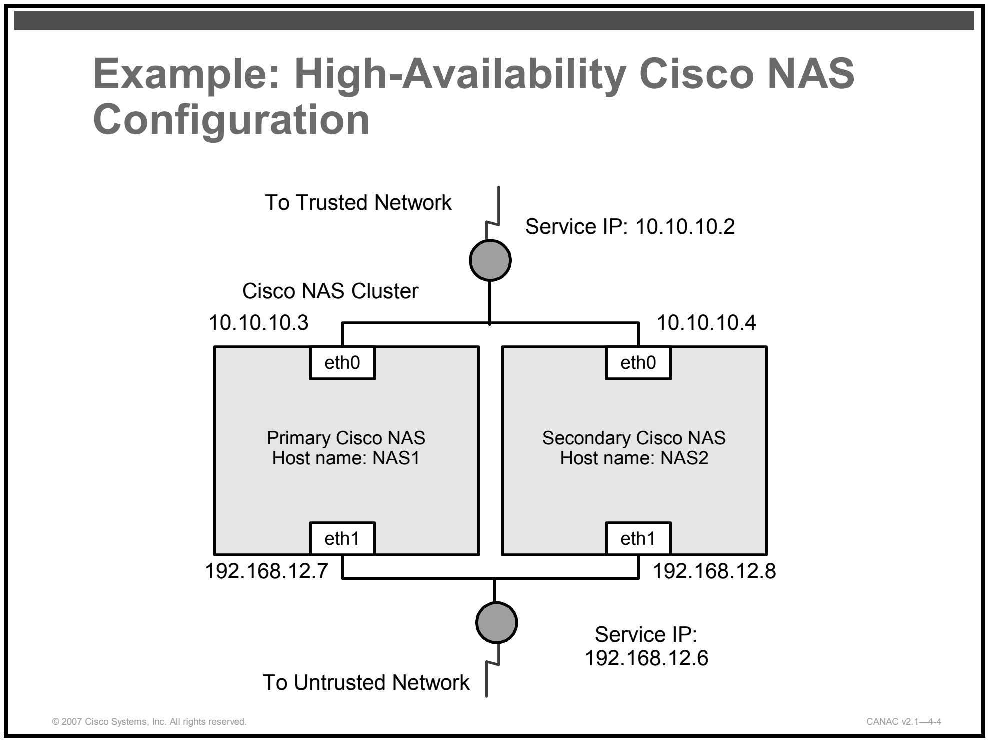
- **Secure Sockets Layer (SSL) certificates:** In high-availability mode, similar to standalone mode, the failover peers can use either a temporary, self-signed certificate or a certificate authority (CA)-signed certificate. A temporary certificate is useful for testing and development. A production deployment should have a CA-signed certificate. Consider these points in either case:

  — You can use the service IP address (for either the trusted interface or untrusted interface) or a domain name as the certificate domain name for both the temporary and the CA-signed certificates.

  — If you are creating a certificate using a domain name, the domain name must map to the service IP address in the Domain Name System (DNS). If you are not using a domain name in the certificate, DNS mapping is not necessary.

  — You can generate a temporary certificate on one of the failover peers and then transfer it from that Cisco NAS to the other Cisco NAS.

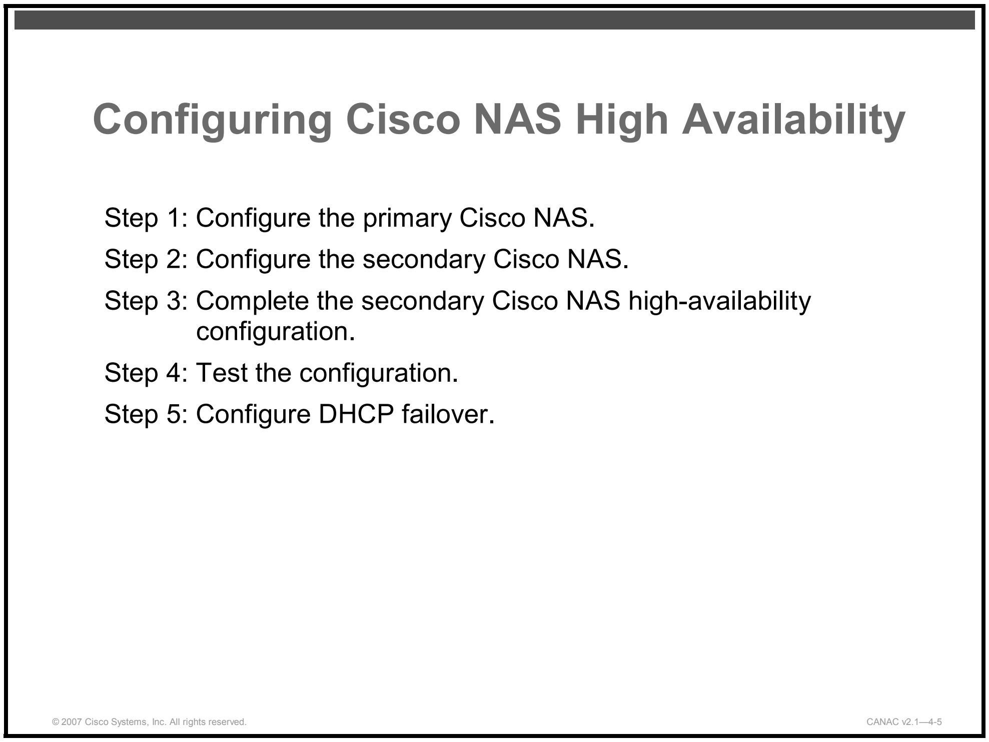
  — For a CA-signed certificate, you must import the CA-signed certificate into each Cisco NAS in the cluster.



Example: High-Availability Cisco NAS Configuration

CANAC v2.1—4-4

The figure shows a Cisco NAS cluster with sample values for the configuration.



Configuring Cisco NAS High Availability

Step 1: Configure the primary Cisco NAS.

Step 2: Configure the secondary Cisco NAS.

Step 3: Complete the secondary Cisco NAS high-availability configuration.

Step 4: Test the configuration.

Step 5: Configure DHCP failover.

CANAC v2.1—4-5

These steps are used to configure Cisco NAS high availability:

Step 1 Configure the primary Cisco NAS.

Step 2 Configure the secondary Cisco NAS.

Step 3 Complete the secondary Cisco NAS high-availability configuration.

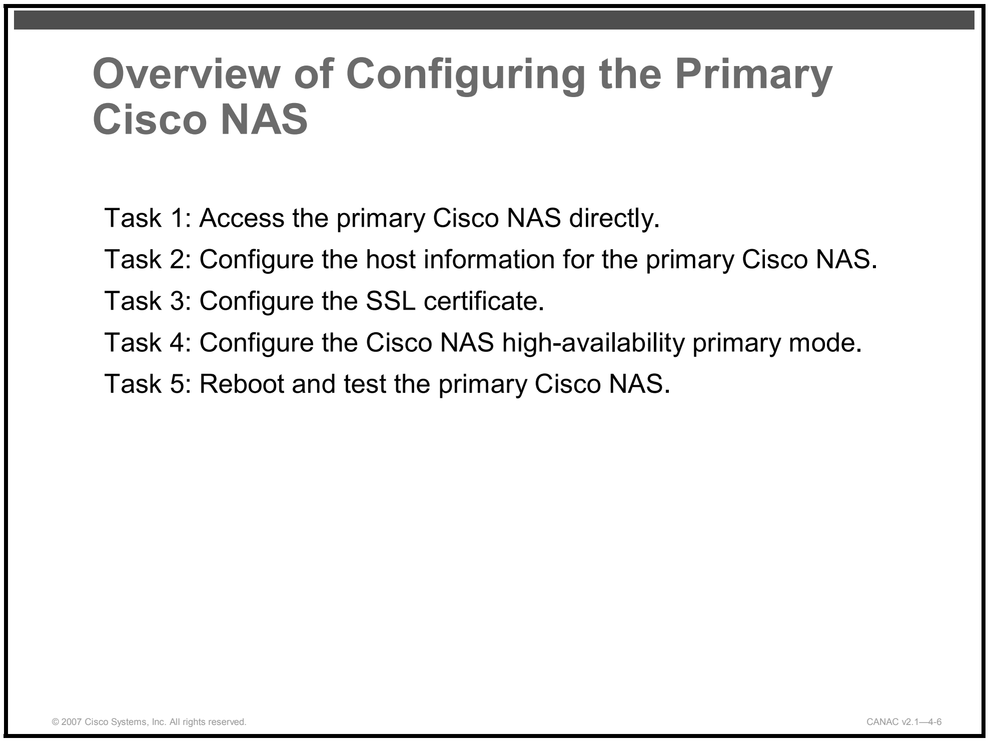
Step 4 Test the configuration.

Step 5 Configure DHCP failover.

Note If you are configuring high availability for Cisco NASs that operate as DHCP servers (not in DHCP relay or pass-through mode), you must also configure the SSH tunnel between them.

Configuring the Primary Cisco NAS

This topic describes how to configure the primary Cisco NAS for high availability.



Overview of Configuring the Primary Cisco NAS

Task 1: Access the primary Cisco NAS directly.

Task 2: Configure the host information for the primary Cisco NAS.

Task 3: Configure the SSL certificate.

Task 4: Configure the Cisco NAS high-availability primary mode.

Task 5: Reboot and test the primary Cisco NAS.

Follow these tasks to configure the primary Cisco NAS:

Task 1 Access the primary Cisco NAS directly.

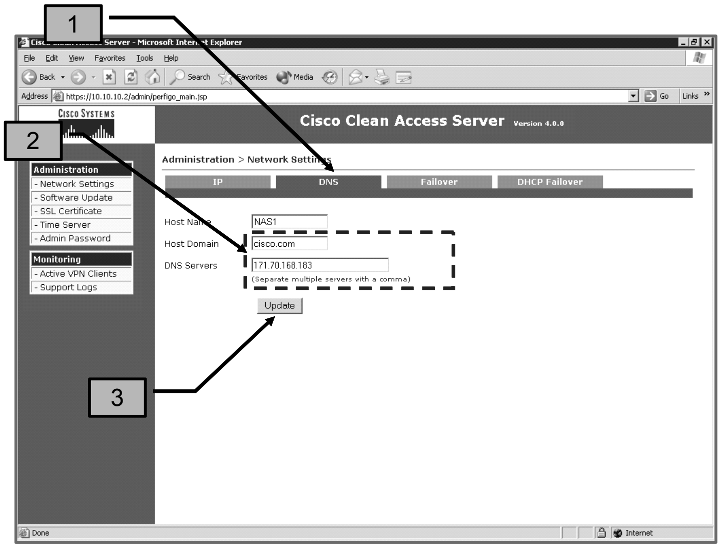
Task 2 Configure the host information for the primary Cisco NAS.

Task 3 Configure the SSL certificate.

Task 4 Configure the Cisco NAS high-availability primary mode.

Task 5 Reboot and test the primary Cisco NAS.

Task 2: Configuring the Host Information for the Primary Cisco NAS


1
2
3
Cisco Clean Access Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.10.10.2/admin/perfigo_main.jsp
Go Links
Cisco Systems
Cisco Clean Access Server Version 4.0.0
Administration
- Network Settings
- Software Update
- SSL Certificate
- Time Server
- Admin Password
Monitoring
- Active VPN Clients
- Support Logs
Administration > Network Settings
IP
DNS
Failover
DHCP Failover
Update
Done
Internet

Host Name: NAS1

Host Domain: cisco.com

DNS Servers: 171.70.168.183 (Separate multiple servers with a comma)

CANAC v2.1—4-7

The first task (not shown) is to bypass the Cisco NAM web administrator console and access the Cisco NAS configuration directly by opening the Cisco NAS web administration page of the primary Cisco NAS. This is a two-step process:

Step 1 Access the Cisco NAS web administration page using this address:

```
https://<ServerIP>/admin
<ServerIP> is the IP address of the trusted Cisco NAS
interface (eth0). For example:
https://172.16.1.2/admin
```

Note The Cisco NAS web administration pages allow direct access to specific administration settings in the Cisco NAS. These settings cannot be accessed from the Cisco NAM web administrator console.

Step 2 Accept the temporary certificate and log in as "admin" user. Recall that the default password for the admin user is "cisco123".

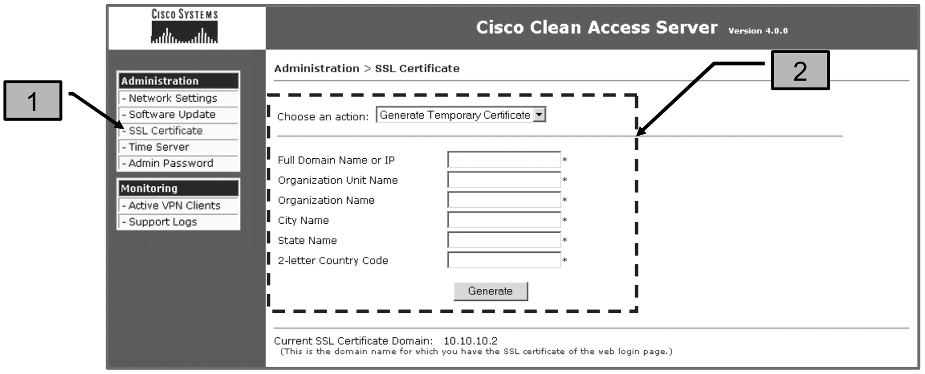
Now that you are at the Cisco NAS web-based administration console, follow these steps to complete Task 2, configuring the host information for the primary Cisco NAS:

Step 1 Click the **Network Settings** link (if the Network Settings page is not already open) and then click the **DNS** tab.

Step 2 In the Host Name field, enter the host name for the primary server (for example, CAS1). Ensure that there is a domain such as cisco.com in the Host Domain field. If no domain is listed, add a domain.

Step 3 Click the **Update** button.

Task 3: Configuring the SSL Certificate



Administration > SSL Certificate

Choose an action: Generate Temporary Certificate

Full Domain Name or IP *
Organization Unit Name *
Organization Name *
City Name *
State Name *
2-letter Country Code *

Current SSL Certificate Domain: 10.10.10.2
(This is the domain name for which you have the SSL certificate of the web login page.)

CANAC v2.1—4-8

Follow these steps to configure the SSL certificate for the primary Cisco NAS:

Step 1 From the Administration menu, click the **SSL Certificate** link. The Generate Temporary Certificate form appears.

Step 2 In the SSL Certificate page, perform one of these procedures:

- To use a temporary certificate for the high-availability pair, complete these steps:

  1. Complete the Generate Temporary Certificate form and click **Generate**. The certificate must be associated with the service IP addresses of the high-availability pair.

  2. When you finish generating the temporary certificate, choose **Export Certificate Request** from the Choose an Action drop-down menu.

  3. Click the **Export Private Key** button. You will import this key database later when you configure the standby Cisco NAS.

- To use a CA-signed certificate for the failover pair, follow this procedure:

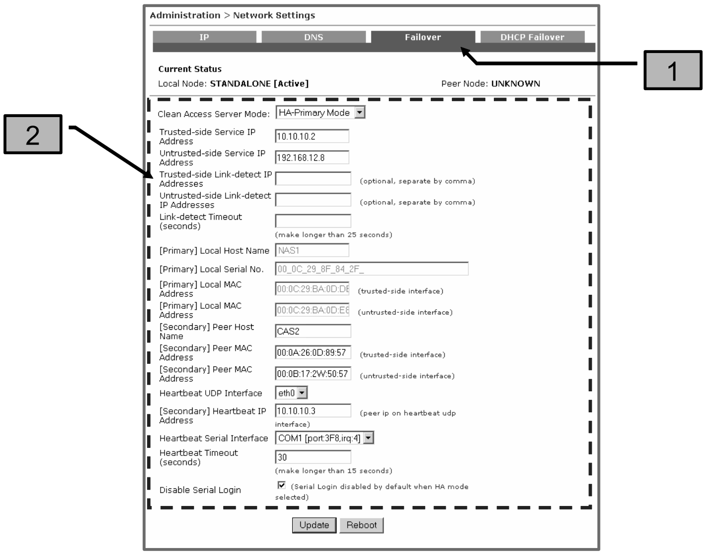
  1. Choose **Import Certificate** from the Choose an Action drop-down menu.

  2. Click the **Browse** button next to the Certificate File field and navigate to the certificate file.

  3. Click **Import CA-Signed Certificate** to import the certificate. You will import the same certificate later into the standby Cisco NAS.

Note The CA-signed certificate must be based on the service IP address or on a host name and domain name resolvable to the service IP address through DNS.

Task 4: Configuring the Cisco NAS High-Availability Primary Mode



Administration > Network Settings

Current Status

Local Node: **STANDALONE [Active]** Peer Node: **UNKNOWN**

Clean Access Server Mode:	HA-Primary Mode	
Trusted-side Service IP Address	10.10.10.2	
Untrusted-side Service IP Address	192.168.12.8	
Trusted-side Link-detect IP Addresses		(optional, separate by comma)
Untrusted-side Link-detect IP Addresses		(optional, separate by comma)
Link-detect Timeout (seconds)	(make longer than 25 seconds)	
[Primary] Local Host Name	NAS1	
[Primary] Local Serial No.	00_0C_29_8F_84_2F_	
[Primary] Local MAC Address	00:0C:29:BA:0D:DE	(trusted-side interface)
[Primary] Local MAC Address	00:0C:29:BA:0D:E8	(untrusted-side interface)
[Secondary] Peer Host Name	CAS2	
[Secondary] Peer MAC Address	00:0A:26:0D:89:57	(trusted-side interface)
[Secondary] Peer MAC Address	00:0B:17:2W:50:57	(untrusted-side interface)
Heartbeat UDP Interface	eth0	
[Secondary] Heartbeat IP Address	10.10.10.3	(peer ip on heartbeat udp interface)
Heartbeat Serial Interface	COM1 [port:3F8,irq:4]	
Heartbeat Timeout (seconds)	30 (make longer than 15 seconds)	
Disable Serial Login	☑ (Serial Login disabled by default when HA mode selected)	

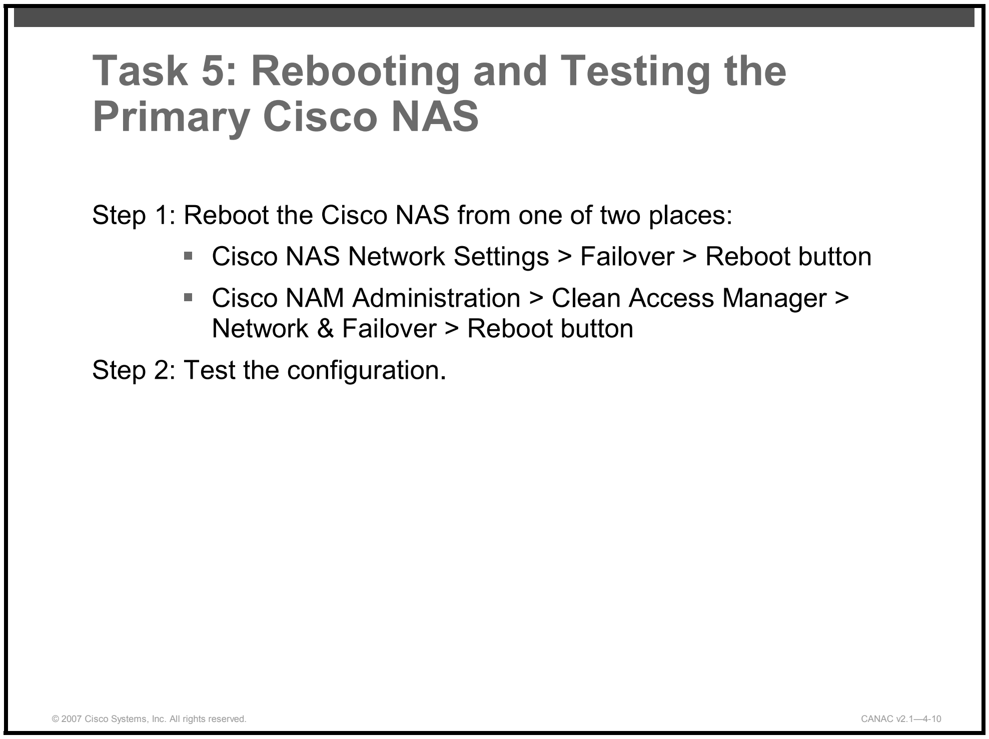
Follow these two steps to configure the Cisco NAS high-availability primary mode:

Step 1 From the Network Settings link, click the **Failover** tab and choose **HA-Primary Mode** from the Clean Access Server Mode drop-down menu.

Step 2 Enter the field values that are required for the High-Availability Primary Mode fields.

Tip Copy and paste the values from these fields into a text file: [Primary] Local Serial No., Trusted-side Service IP Address, Untrusted-side Service IP Address, [Primary] Local MAC Address (trusted-side interface), and the [Primary] Local MAC Address (untrusted-side interface). Use these values to help configure the standby Cisco NAS.

Note The screen capture shows the new Cisco NAC Appliance failover for link failure feature. Check the latest Cisco NAC Appliance documentation for details on this feature.



Task 5: Rebooting and Testing the Primary Cisco NAS

Step 1: Reboot the Cisco NAS from one of two places:

- Cisco NAS Network Settings > Failover > Reboot button
- Cisco NAM Administration > Clean Access Manager > Network & Failover > Reboot button

Step 2: Test the configuration.

Follow these steps to reboot and test the primary Cisco NAS:

Step 1 Reboot the Cisco NAS from one of these places:

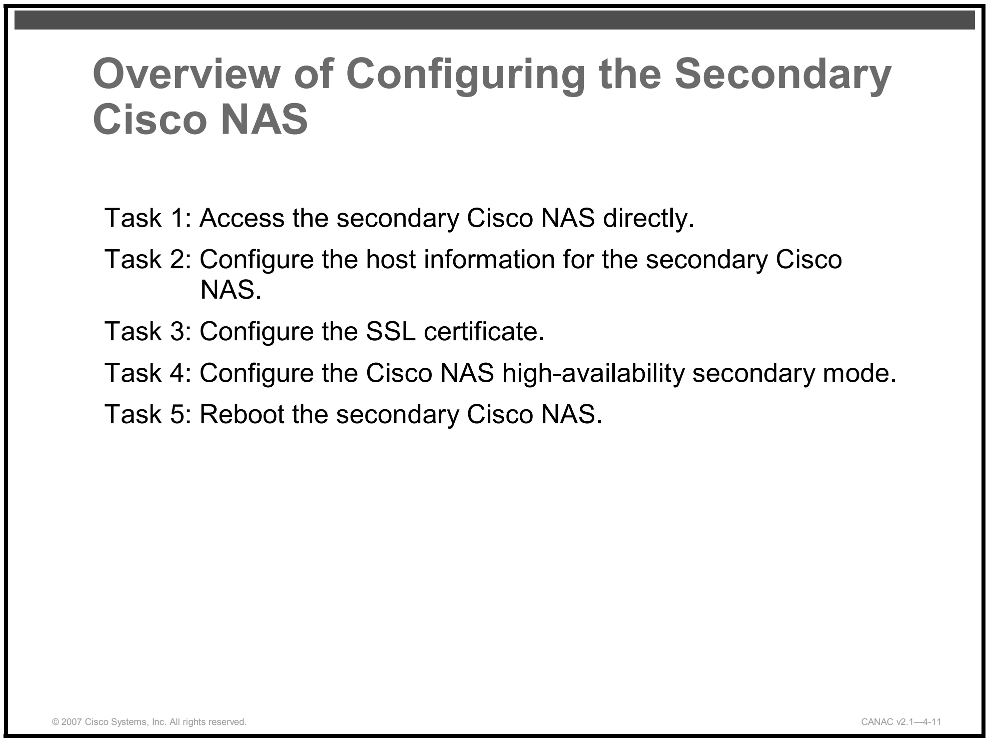
— Go to the Cisco NAS Administration interface, choose **Network Settings** > **Failover,** and then click the **Reboot** button.

— Go to the Cisco NAM administrator console, choose **Administration** > **CCA Manager** > **Network & Failover**, and then click the **Reboot** button.

Step 2 Test the configuration by logging onto the untrusted (managed) network from a computer that is connected to the untrusted interface of the Cisco NAS.

Configuring the Secondary Cisco NAS

This topic describes how to configure the secondary Cisco NAS for high availability.



Overview of Configuring the Secondary Cisco NAS

Task 1: Access the secondary Cisco NAS directly.

Task 2: Configure the host information for the secondary Cisco NAS.

Task 3: Configure the SSL certificate.

Task 4: Configure the Cisco NAS high-availability secondary mode.

Task 5: Reboot the secondary Cisco NAS.

CANAC v2.1—4-11

The tasks to configure the standby Cisco NAS, listed in the figure, closely parallel the tasks that are used to configure the primary Cisco NAS; therefore, the first task steps that follow are presented in an abbreviated form. Follow these multistep tasks to configure the secondary Cisco NAS:

Task 1: Access the secondary Cisco NAS directly.

Step 1 Access the administration interface for the secondary Cisco NAS by opening a browser and entering the following address:

https://<ServerIP>/admin

Where <ServerIP> is the IP address of the standby Cisco NAS trusted interface. For example, https://172.16.1.3/admin.

Step 2 Log in as user “admin” with password “cisco123”.

Tip	You should change the default password for the Cisco NAS to a unique password to ensure the security of your network environment.

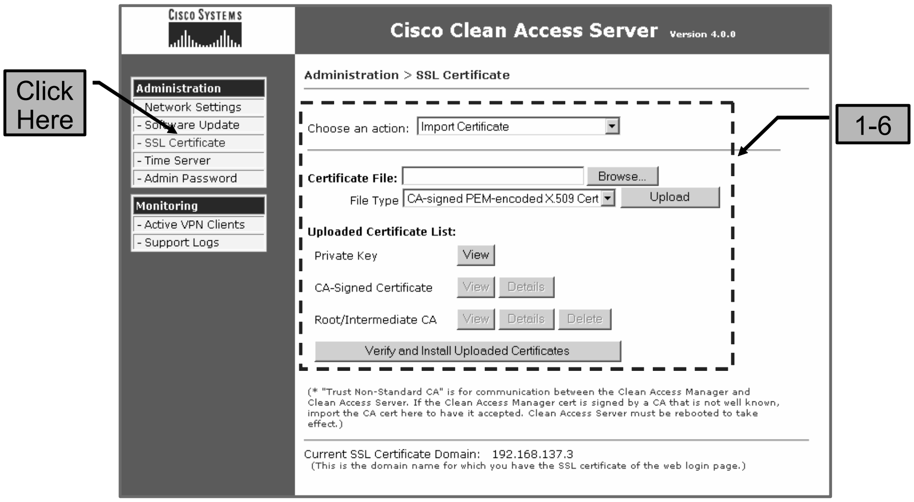
Task 2: Configure the host information for the secondary Cisco NAS.

Step 1 In the Network Settings page, click the **DNS** tab.

Step 2 Change the host name to a unique host name for the secondary Cisco NAS.

Caution	The domain name that is specified in this tab must be the same name that you entered for the primary Cisco NAS domain name.

Task 3: Configuring the SSL Certificate



Administration > SSL Certificate

Choose an action: Import Certificate

Certificate File:

File Type CA-signed PEM-encoded X.509 Cert

Uploaded Certificate List:

Private Key

CA-Signed Certificate

Root/Intermediate CA

(* "Trust Non-Standard CA" is for communication between the Clean Access Manager and Clean Access Server. If the Clean Access Manager cert is signed by a CA that is not well known, import the CA cert here to have it accepted. Clean Access Server must be rebooted to take effect.)

Current SSL Certificate Domain: 192.168.137.3
(This is the domain name for which you have the SSL certificate of the web login page.)

CANAC v2.1—4-12

Task 3: To configure the SSL certificate for the standby Cisco NAS, click the **Administration > SSL Certificate** link. On the SSL Certificate page, complete one of the following procedures:

- To use a temporary certificate for the failover pair, complete these steps:

Step 1 Click **Import Certificate** from the Choose an Action drop-down menu.

Step 2 Click the **Browse** button next to the Certificate File field to choose the temporary certificate file that you previously exported from the primary Cisco NAS.

Step 3 Click **Import CA-Signed Certificate** to import the certificate file.

Step 4 Choose **Import Certificate** from the Choose an Action drop-down menu.

Step 5 Click the **Browse** button next to the Certificate File field to choose the private key that you exported from the primary Cisco NAS.

Step 6 Click **Import Private Key from Backup** to import the private key.

- To use a CA-signed certificate for the failover pair, complete these steps:

Step 1 Choose **Import Certificate** from the Choose an Action drop-down menu.

Step 2 Click the **Browse** button next to the Certificate File field to choose the same certificate file that you used for the primary Cisco NAS.

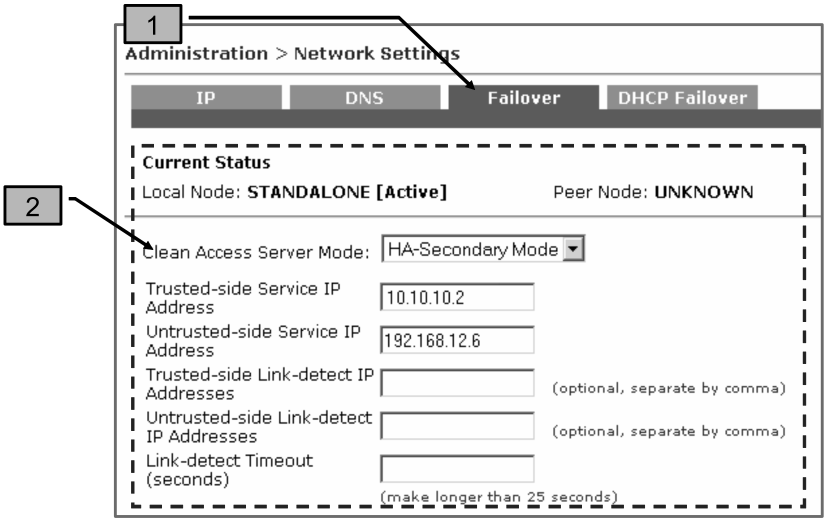
Step 3 Click **Import CA-Signed Certificate** to import the certificate file.

Step 4 Choose **Import Certificate** from the Choose an Action drop-down menu.

Step 5 Click the **Browse** button next to the Certificate File field to choose the private key file that you exported from the primary Cisco NAS.

Step 6 Click **Import Private Key from Backup** to import the private key.

Task 4: Configuring the Cisco NAS High-Availability Secondary Mode



Administration > Network Settings

Current Status

Local Node: **STANDALONE [Active]** Peer Node: **UNKNOWN**

Clean Access Server Mode: HA-Secondary Mode

Trusted-side Service IP Address: 10.10.10.2

Untrusted-side Service IP Address: 192.168.12.6

Trusted-side Link-detect IP Addresses: (optional, separate by comma)

Untrusted-side Link-detect IP Addresses: (optional, separate by comma)

Link-detect Timeout (seconds): (make longer than 25 seconds)

CANAC v2.1—4-13

The figure shows the first half of the fields that are used to configure the secondary Cisco NAS. The rest of the fields are found in the subsequent figure.

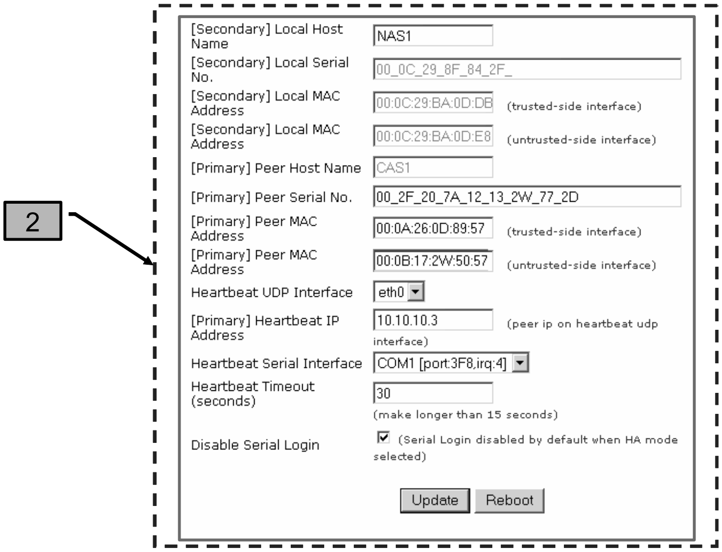
Task 4: Follow these steps to configure the Cisco NAS high-availability secondary mode:

Step 1 In **Administration > Network Settings**, click the **Failover** tab and choose **HA-Secondary Mode** from the Clean Access Server Mode drop-down menu.

Step 2 Enter values for the fields that are provided in the High-Availability Secondary Mode table.

Caution Read the descriptions for each field carefully; they are only slightly different from the values you used to configure the primary Cisco NAS.

Task 4: Configuring the Cisco NAS High-Availability Secondary Mode (Cont.)



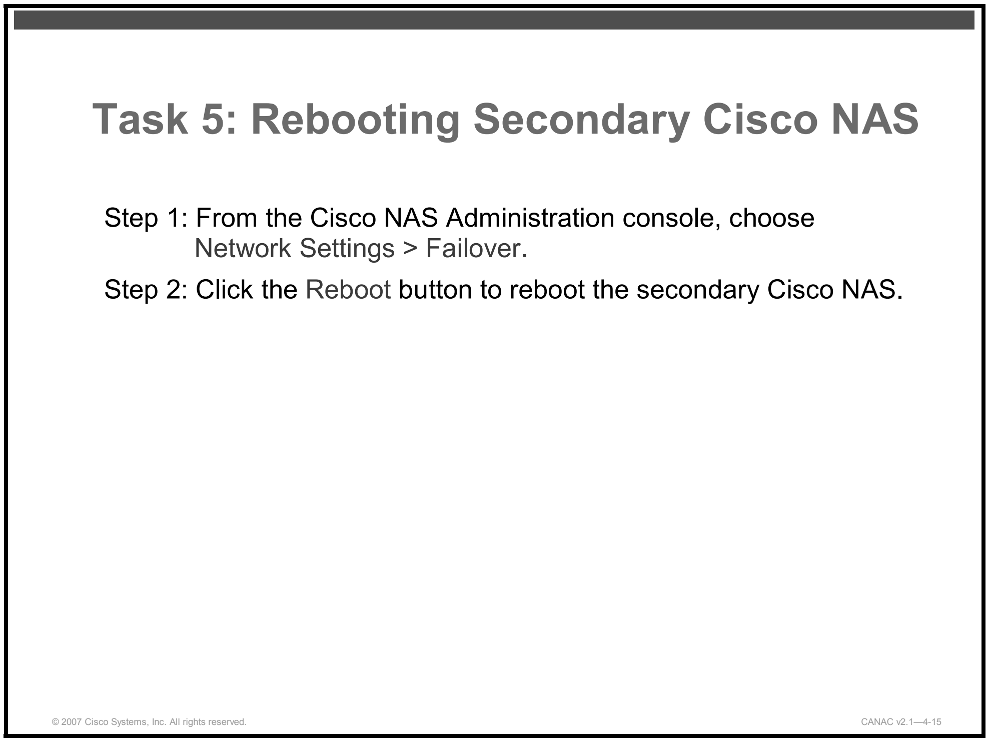
[Secondary] Local Host Name	NAS1	
[Secondary] Local Serial No.	00_0C_29_8F_84_2F_	
[Secondary] Local MAC Address	00:0C:29:BA:0D:DB	(trusted-side interface)
[Secondary] Local MAC Address	00:0C:29:BA:0D:E8	(untrusted-side interface)
[Primary] Peer Host Name	CAS1	
[Primary] Peer Serial No.	00_2F_20_7A_12_13_2W_77_2D	
[Primary] Peer MAC Address	00:0A:26:0D:89:57	(trusted-side interface)
[Primary] Peer MAC Address	00:0B:17:2W:50:57	(untrusted-side interface)
Heartbeat UDP Interface	eth0 ▾	
[Primary] Heartbeat IP Address	10.10.10.3	(peer ip on heartbeat udp interface)
Heartbeat Serial Interface	COM1 [port:3F8,irq:4] ▾	
Heartbeat Timeout (seconds)	30	(make longer than 15 seconds)
Disable Serial Login	☑	(Serial Login disabled by default when HA mode selected)

The figure shows the second half of the fields used to configure the secondary Cisco NAS. The first half of the fields are found in the previous figure. Continue to enter values for the fields that are described in the High-Availability Secondary Mode table.

The High Availability Secondary Mode table lists the fields that are required to configure a Cisco NAS in high-availability secondary mode.

High-Availability Secondary Mode

Field Name	Description
Trusted-Side Service IP Address	The IP address of the *trusted* network. Use the same value that was used for the primary Cisco NAS.
Untrusted-Side Service IP Address	The IP address of the *untrusted* (managed) network. Use the same value that was used for the primary Cisco NAS.
[Primary] Peer Host Name	The host name of the primary Cisco NAS, as specified in the Host Name field in the primary DNS tab.
[Primary] Peer Serial No.	The serial number of the primary Cisco NAS. This is the value you noted when configuring the primary server.
[Primary] Peer MAC Address	The MAC address of the primary server.
Heartbeat UDP Interface	Options are N/A, eth0, eth2, eth3, and eth4. If a dedicated Ethernet connection is not available, use eth0 for the heartbeat UDP interface when configuring a Cisco NAS in high-availability mode.
[Primary] Heartbeat IP Address	The IP address of the UDP based heartbeat.
Heartbeat Serial Interface	Select the COM port for the serial connection. Use both serial and UDP connections for the heartbeat interface.
Heartbeat Timeout (seconds)	Choose a value greater than 10 seconds for the time the standby Cisco NAS will wait before becoming the active Cisco NAS
Enable Serial Login	Serial login is disabled by default when high-availability mode is selected. To reenable the serial console (ttyS0), click the **Enable** button (after you click the **Update** button and before you click the **Reboot** button).

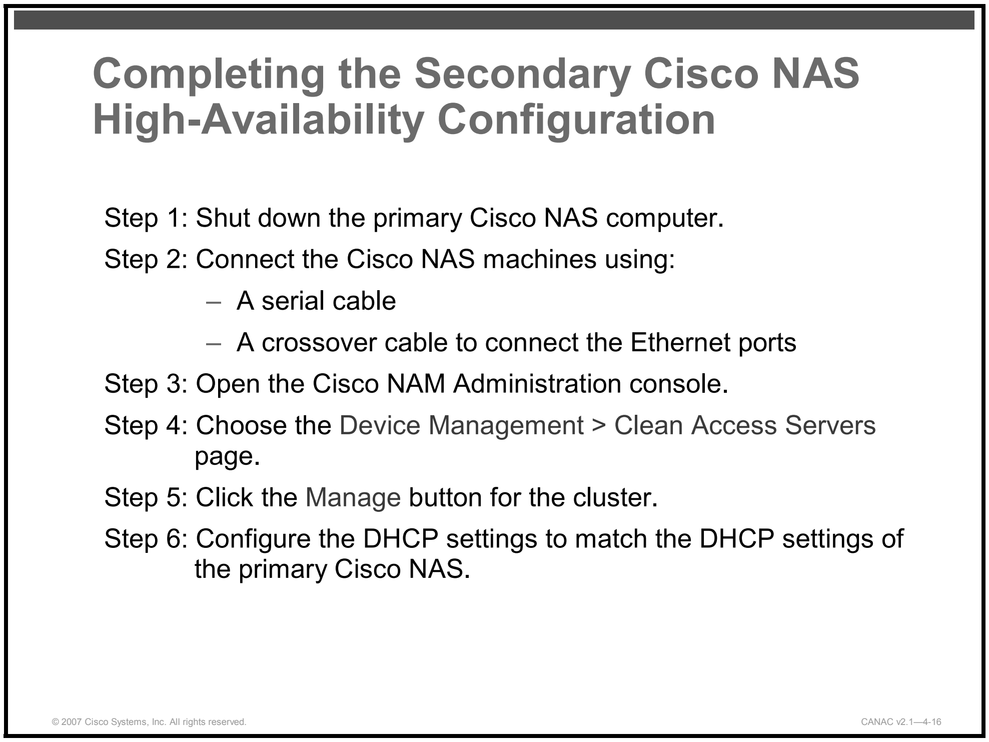


Task 5: Rebooting Secondary Cisco NAS

Step 1: From the Cisco NAS Administration console, choose Network Settings > Failover.

Step 2: Click the Reboot button to reboot the secondary Cisco NAS.

The figure shows the two steps that are used to reboot the secondary Cisco NAS.



Completing the Secondary Cisco NAS High-Availability Configuration

Step 1: Shut down the primary Cisco NAS computer.

Step 2: Connect the Cisco NAS machines using:

- A serial cable
- A crossover cable to connect the Ethernet ports

Step 3: Open the Cisco NAM Administration console.

Step 4: Choose the Device Management > Clean Access Servers page.

Step 5: Click the Manage button for the cluster.

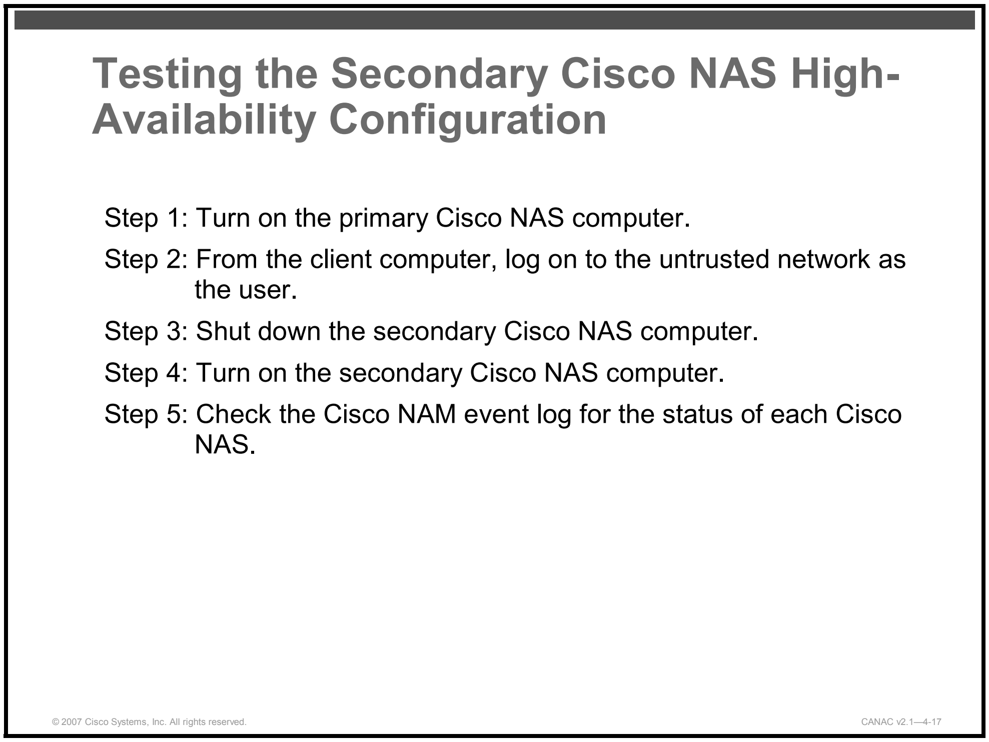
Step 6: Configure the DHCP settings to match the DHCP settings of the primary Cisco NAS.

The figure shows the six steps that are used to complete the high-availability configuration of the secondary Cisco NAS.

Note Connect the Ethernet ports if you are using a third Ethernet interface, such as eth2, for failover.

Testing the Cisco NAS High-Availability Configuration

This topic describes how to test the secondary Cisco NAS high-availability configuration.



Testing the Secondary Cisco NAS High-Availability Configuration

Step 1: Turn on the primary Cisco NAS computer.

Step 2: From the client computer, log on to the untrusted network as the user.

Step 3: Shut down the secondary Cisco NAS computer.

Step 4: Turn on the secondary Cisco NAS computer.

Step 5: Check the Cisco NAM event log for the status of each Cisco NAS.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-17

Follow these five steps to test your high-availability Cisco NAS configuration:

Step 1 Turn on the primary Cisco NAS computer. Ensure that the server is fully started and functioning before proceeding.

Step 2 From the client computer, log out of the user session. Try to log onto the untrusted (managed) network again as the user. The secondary Cisco NAS should still be providing services for the user.

Step 3 Shut down the secondary Cisco NAS computer. After about 15 seconds, you should be able to continue browsing, with the primary server providing the service.

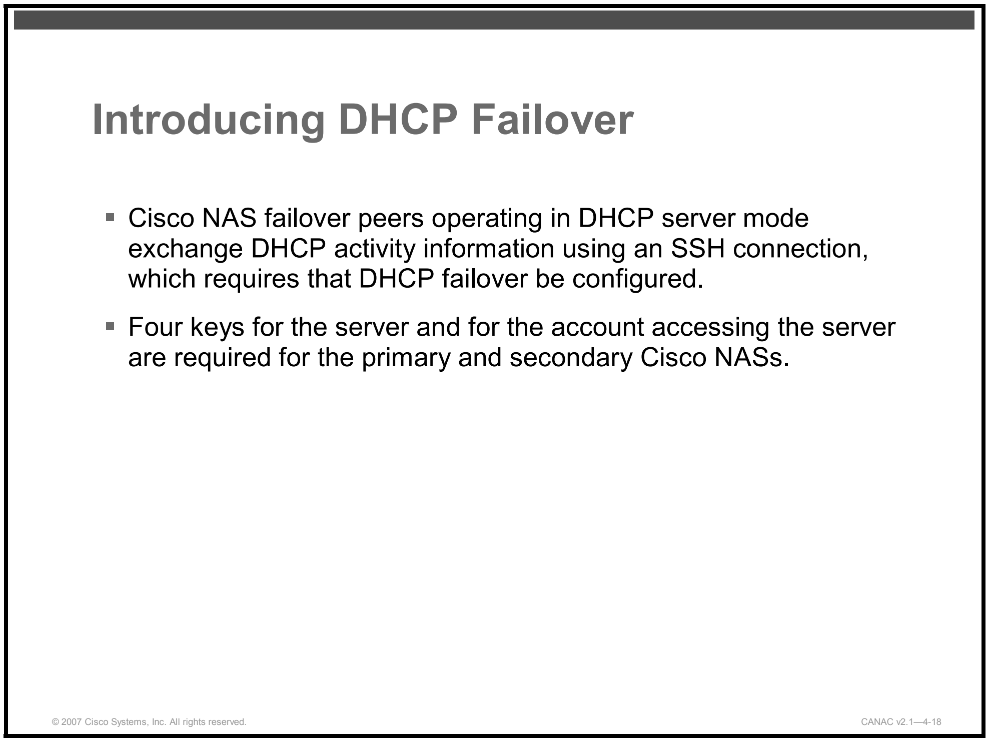
Step 4 Turn on the secondary Cisco NAS computer.

Step 5 Check the event log on the Cisco NAM. It should correctly indicate the status of each Cisco NAS ("naserver1 is dead. naserver2 is up").

Note To manage an existing high-availability Cisco NAS cluster, refer to the Modifying High Availability Settings sections in the *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*.

Configuring DHCP Failover

This topic describes how to configure DHCP failover.



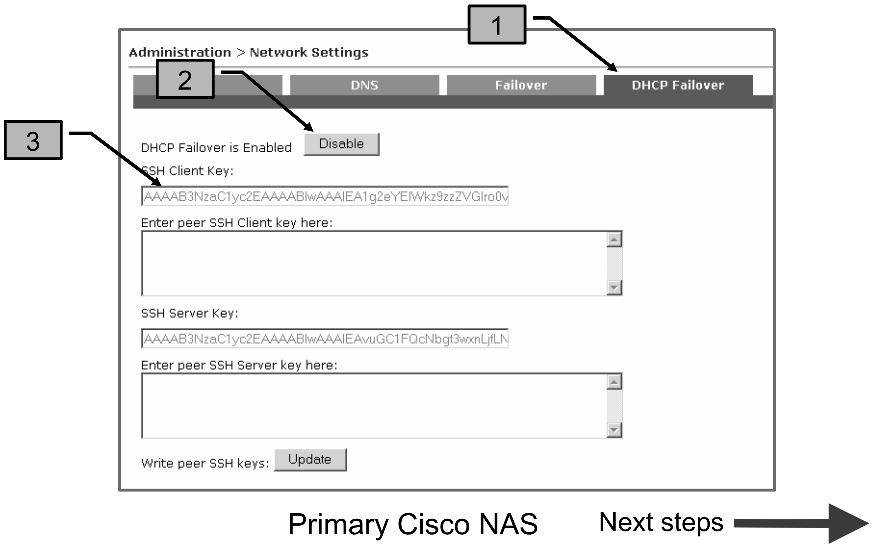
Introducing DHCP Failover

- Cisco NAS failover peers operating in DHCP server mode exchange DHCP activity information using an SSH connection, which requires that DHCP failover be configured.
- Four keys for the server and for the account accessing the server are required for the primary and secondary Cisco NASs.

© 2007 Cisco Systems, Inc. All rights reserved. CANAC v2.1—4-18

Cisco NAS failover peers that operate in DHCP server mode exchange DHCP activity information, such as active leases and lease times, by SSH connection (tunnel). When configuring high availability for Cisco NASs that will operate as DHCP servers (not in DHCP relay or pass-through mode), you must configure DHCP failover. Keys for the server and for the account accessing the server are required for both the primary and the secondary Cisco NAS. As a result, a total of four keys must be exchanged. The Cisco NAS provides a browser interface to facilitate the generation and exchange of the security keys that are necessary to transfer DHCP failover information between the primary and secondary Cisco NASs.

Configuring DHCP Failover



Administration > Network Settings

DHCP Failover is Enabled

SSH Client Key:

AAAAB3NzaC1yc2EAAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0v

Enter peer SSH Client key here:

SSH Server Key:

AAAAB3NzaC1yc2EAAAABIwAAAIEAvuGC1FQcNbgt3wxnLjfLN

Enter peer SSH Server key here:

Write peer SSH keys:

Primary Cisco NAS

Next steps

CANAC v2.1—4-19

Follow these 14 steps to configure DHCP failover for a high-availability Cisco NAS cluster:

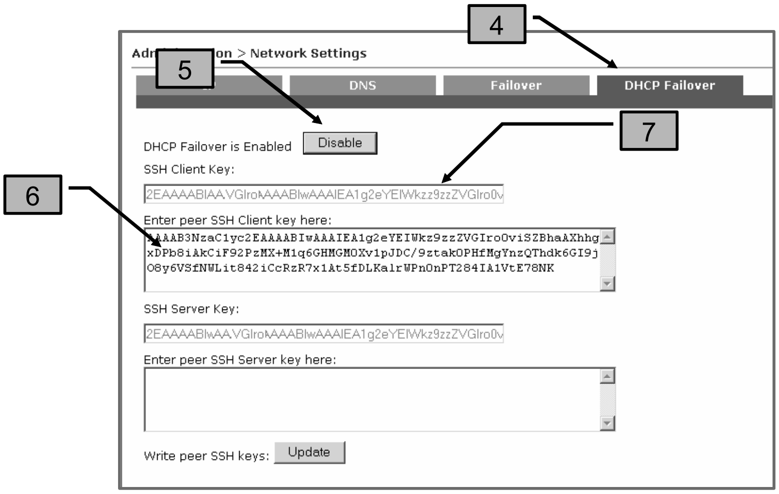
Note Access the administrator console of the primary Cisco NAS and the secondary Cisco NAS (https://<ServerIP>/admin). You will have two browsers open during this process.

Step 1 In the administrator console of the primary Cisco NAS, click the **DHCP Failover** tab.

Step 2 Click the **Enable** button to enable DHCP failover on the primary Cisco NAS. Notice that this button toggles to Disable.

Step 3 Copy the value from the SSH Client Key field from the primary Cisco NAS. You will use this value in Step 6.

Configuring DHCP Failover (Cont.)



Adm on > Network Settings

DHCP Failover is Enabled

SSH Client Key:

```
2EAAAABIAA.VGIroMAAABIwAAAIEA1g2eYEIWkzz9zzZVGIro0v
```

Enter peer SSH Client key here:

```
AAAAB3NzaC1yc2EAAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0viSZBhaAXhhg
xDPb8iAkCiF92PzMX+M1q6GHMGMOXv1pJDC/9ztakOPHfMgYnzQThdk6GI9j
O8y6VSfNWLit842iCcRzR7x1At5fDLKalrWPnOnPT284IA1VtE78NK
```

SSH Server Key:

```
2EAAAABIwAA.VGIroMAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0v
```

Enter peer SSH Server key here:

Write peer SSH keys:

Secondary Cisco NAS

Next steps →

CANAC v2.1—4-20

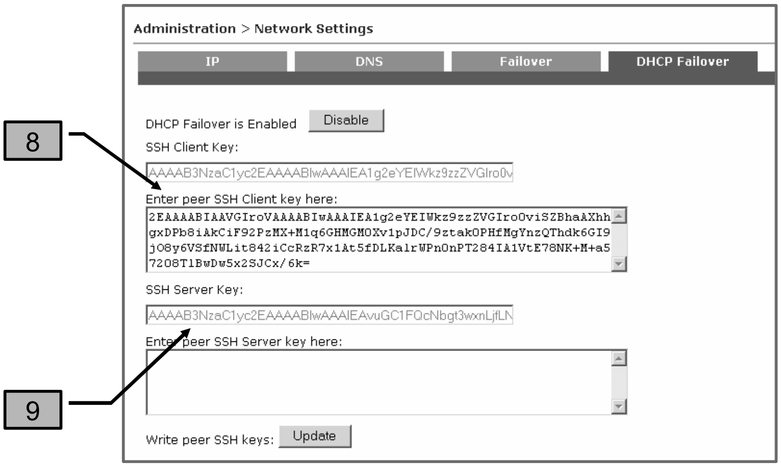
Step 4 In the administrator console of the secondary Cisco NAS, click the **DHCP Failover** tab.

Step 5 Click the **Enable** button to enable DHCP failover on the secondary Cisco NAS (the button now reads Disable).

Step 6 Paste the SSH client key that you copied from the primary server into the Enter Peer SSH Client Key Here field.

Step 7 While still in the administrator console of the secondary Cisco NAS, copy the value from the SSH Client Key field.

Configuring DHCP Failover (Cont.)



DHCP Failover is Enabled

SSH Client Key:

```
AAAAB3NzaC1yc2EAAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0v
```

Enter peer SSH Client key here:

```
2EAAAABIAAVGIroVAAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0viSZBhaAXhh
gxDPb8iAkCiF92PzMX+M1q6GHMGMOXv1pJDC/9ztakOPHfMgYnzQThdk6GI9
jO8y6VSfNWLit842iCcRzR7x1At5fDLKalrWPnOnPT284IA1VtE78NK+M+a5
72O8TlBwDw5x2SJCx/6k=
```

SSH Server Key:

```
AAAAB3NzaC1yc2EAAAABIwAAAIEAvuGC1FQcNbgt3wxnLjfLN
```

Enter peer SSH Server key here:

Write peer SSH keys:

Primary Cisco NAS

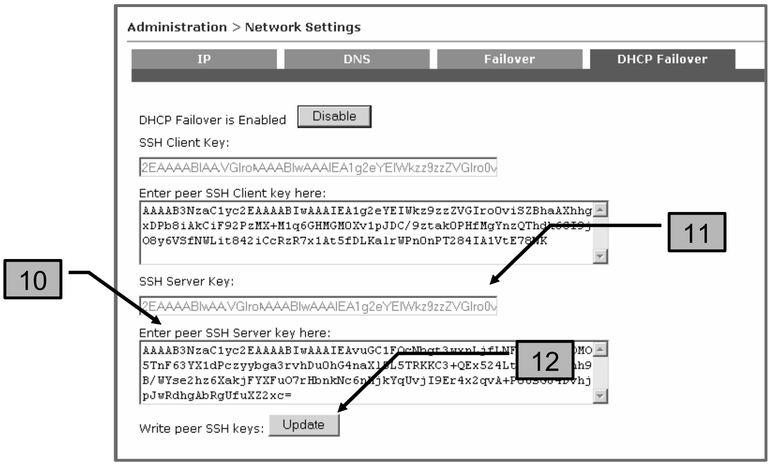
Next steps →

CANAC v2.1—4-21

Step 8 In the administrator console of the primary Cisco NAS, paste the SSH client key of the secondary Cisco NAS into the Enter Peer SSH Client Key Here field.

Step 9 While still in the administrator console of the primary Cisco NAS, copy the value from the SSH Server Key field.

Configuring DHCP Failover (Cont.)



Administration > Network Settings

DHCP Failover is Enabled

SSH Client Key:

2EAAAABIAAVGIroMAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0v

Enter peer SSH Client key here:

```
AAAAB3NzaC1yc2EAAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0viSZBhaAXhhg
xDPb8iAkCiF92PzMX+M1q6GHMGMOXv1pJDC/9ztakOPHfMgYnzQThd[illegible]j
O8y6VSfNWLit842iCcRzR7x1At5fDLKalrWPnOnPT284IA1VtE78NK
```

SSH Server Key:

2EAAAABIwAAVGIroMAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0v

Enter peer SSH Server key here:

```
AAAAB3NzaC1yc2EAAAABIwAAAIEAvuGC1FOcNbgt3wxnLjfLNF[illegible]OMO
5TnF63YX1dPczyybga3rvhDu0hG4naX1BL5TRKKC3+QEx524Lt[illegible]ah9
B/WYse2hz6XakjFYXFuO7rHbnkNc6nHjkYqUvjI9Er4x2qvA+P[illegible]vhj
pJwRdhgAbRgUfuXZ2xc=
```

Write peer SSH keys:

Secondary Cisco NAS

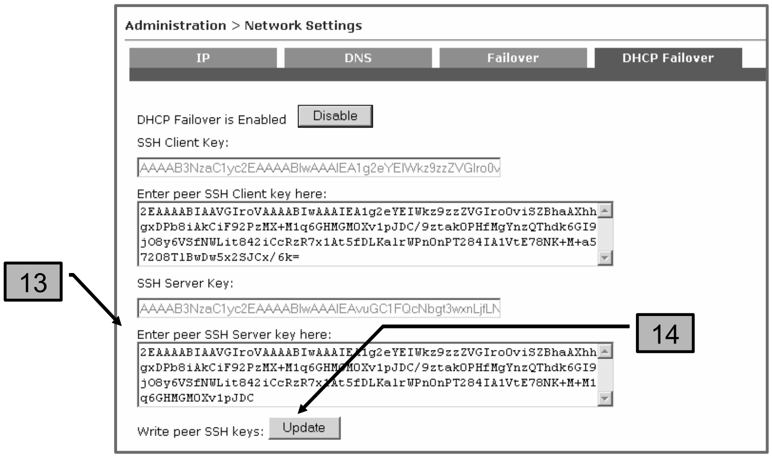
Next steps →

Step 10 In the administrator console of the secondary server, paste the SSH server key of the primary Cisco NAS into the Enter Peer SSH Server Key Here field.

Step 11 While in the administrator console of the secondary Cisco NAS, copy the value from the SSH Server Key field.

Step 12 Click the **Update** button to write the peer SSH keys to the secondary Cisco NAS.

Configuring DHCP Failover (Cont.)



Administration > Network Settings

IP | DNS | Failover | DHCP Failover

DHCP Failover is Enabled [Disable]

SSH Client Key:

```
AAAAB3NzaC1yc2EAAAABIwAAAIEA1g2eYEIWkz9zzZVGIro0v
```

Enter peer SSH Client key here:

```
2EAAAABIAAVGIroVAAAABIwAAAIEA1g2eYEIWkz9zzZVGIroOviSZBhaAXhh
gxDPb8iAkCiF92PzMX+M1q6GHMGMOXv1pJDC/9ztakOPHfMgYnzQThdk6GI9
jO8y6VSfNWLit842iCcRzR7x1At5fDLKalrWPnOnPT284IA1VtE78NK+M+a5
72O8TlBwDw5x2SJCx/6k=
```

SSH Server Key:

```
AAAAB3NzaC1yc2EAAAABIwAAAIEAvuGC1FQcNbgt3wxnLjfLN
```

Enter peer SSH Server key here:

```
2EAAAABIAAVGIroVAAAABIwAAAIEA1g2eYEIWkz9zzZVGIroOviSZBhaAXhh
gxDPb8iAkCiF92PzMX+M1q6GHMGMOXv1pJDC/9ztakOPHfMgYnzQThdk6GI9
jO8y6VSfNWLit842iCcRzR7x1At5fDLKalrWPnOnPT284IA1VtE78NK+M+M1
q6GHMGMOXv1pJDC
```

Write peer SSH keys: [Update]

Primary Cisco NAS

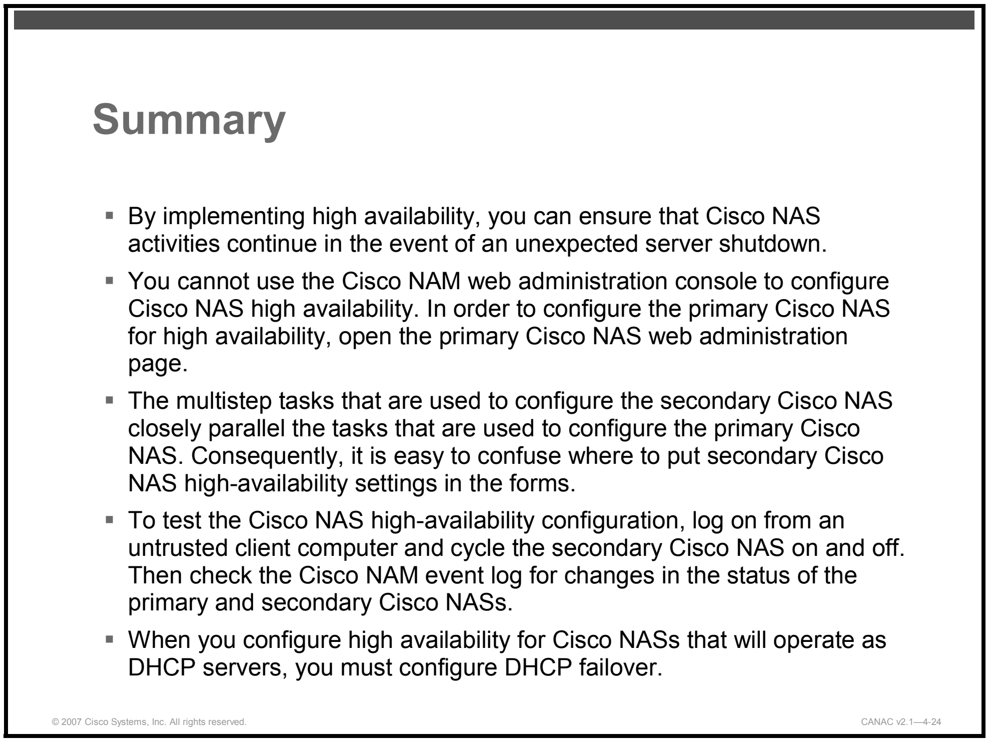
CANAC v2.1—4-23

Step 13 In the administrator console of the primary Cisco NAS, paste the SSH server key from the secondary Cisco NAS into the Enter Peer SSH Server Key Here field.

Step 14 Click the **Update** button to write the peer SSH keys to the primary Cisco NAS.

Summary

This topic summarizes the key points that were discussed in this lesson.



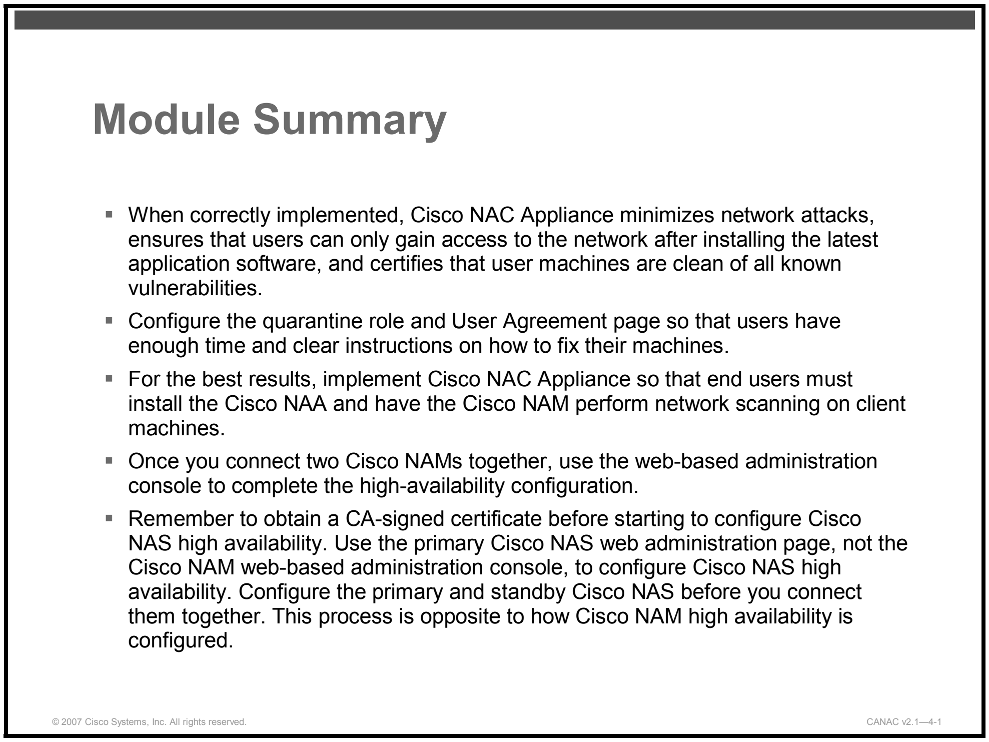
Summary

- By implementing high availability, you can ensure that Cisco NAS activities continue in the event of an unexpected server shutdown.
- You cannot use the Cisco NAM web administration console to configure Cisco NAS high availability. In order to configure the primary Cisco NAS for high availability, open the primary Cisco NAS web administration page.
- The multistep tasks that are used to configure the secondary Cisco NAS closely parallel the tasks that are used to configure the primary Cisco NAS. Consequently, it is easy to confuse where to put secondary Cisco NAS high-availability settings in the forms.
- To test the Cisco NAS high-availability configuration, log on from an untrusted client computer and cycle the secondary Cisco NAS on and off. Then check the Cisco NAM event log for changes in the status of the primary and secondary Cisco NASs.
- When you configure high availability for Cisco NASs that will operate as DHCP servers, you must configure DHCP failover.

CANAC v2.1—4-24

Module Summary

This topic summarizes the key points that were discussed in this module.



Module Summary

- When correctly implemented, Cisco NAC Appliance minimizes network attacks, ensures that users can only gain access to the network after installing the latest application software, and certifies that user machines are clean of all known vulnerabilities.
- Configure the quarantine role and User Agreement page so that users have enough time and clear instructions on how to fix their machines.
- For the best results, implement Cisco NAC Appliance so that end users must install the Cisco NAA and have the Cisco NAM perform network scanning on client machines.
- Once you connect two Cisco NAMs together, use the web-based administration console to complete the high-availability configuration.
- Remember to obtain a CA-signed certificate before starting to configure Cisco NAS high availability. Use the primary Cisco NAS web administration page, not the Cisco NAM web-based administration console, to configure Cisco NAS high availability. Configure the primary and standby Cisco NAS before you connect them together. This process is opposite to how Cisco NAM high availability is configured.

CANAC v2.1—4-1

This module describes how to implement a Cisco Network Admission Control (NAC) Appliance solution to ensure that network users gain access only after they have been certified as having the required software and being clean of vulnerabilities. When implementing Cisco NAC Appliance, you must configure the quarantine role to provide users with the time and instructions they need to meet your security requirements. The module also describes how to implement network scanning to help users implement their security policies while they remain in a quarantined area of the network. The steps for configuring the Cisco NAC Appliance Manager (Cisco NAM) to ensure that Cisco NAC Appliance Agent (Cisco NAA) is automatically downloaded to user devices, in order to provide an additional layer of control for remote users, were described. You should now be able to describe how to configure the Cisco NAM and the Cisco NAC Appliance Server (Cisco NAS) so that they can provide a highly available Cisco NAC Appliance solution to your users.

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide.* http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.
- Cisco Systems, Inc. *Cisco NAC Appliance—Clean Access Server Installation and Administration Guide.* http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html.
- Cisco Systems, Inc. *Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.1(0).* http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html.

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers are found in the Module Self-Check Answer Key.

Q1) In what two ways can Cisco NAA be implemented on a network? (Choose two.) (Source: Implementing Cisco NAC Appliance on a Network)

A) Cisco NAS only
B) Cisco NAM only
C) Cisco NAA only
D) network scanning only
E) Cisco NAM with network scanning

Q2) In a standard Cisco NAC Appliance implementation, which step comes after you configure network scanning? (Source: Implementing Cisco NAC Appliance on a Network)

A) configuring Cisco NAA
B) configuring the Cisco NAC Appliance-related user roles
C) configuring Cisco NAA per user role
D) testing the configurations

Q3) Which menu option accesses the General Setup tab? (Source: Implementing Cisco NAC Appliance on a Network)

A) Device Management > Clean Access
B) Device Management > General Setup
C) User Management > General Setup
D) Management > Setup

Q4) Which of the following pages appear as Cisco Clean Access user pages? (Source: Implementing Cisco NAC Appliance on a Network)

A) Login page and End User Agreement page
B) Login page and Logout page
C) Block Access page and Network Scanning User Agreement page

Q5) Where do you enable the user agreement pages? (Source: Implementing Cisco NAC Appliance on a Network)

A) General Setup tab
B) User Pages tab
C) Network Scanner tab
D) User Agreement tab

Q6) What is an exempt device? (Source: Implementing Cisco NAC Appliance on a Network)

A) a single user device that is not required to be recertified as long as its MAC address is in the certified list
B) a single or multiuser device that is recertified only when another user of the device logs out and accesses the network
C) a multiuser device that is configured as a floating device, so recertification is not required at each login

Q7) In the fields where MAC addresses are added, how do you add multiple MAC addresses? (Source: Implementing Cisco NAC Appliance on a Network)

A) Press the **Tab** key to separate MAC addresses.
B) Press the **Shift + Enter** key combination to separate MAC addresses.
C) Press the **Enter** key to separate MAC addresses.

Q8) How does the Cisco NAM determine the presence of a vulnerability when a user is attempting to access the network? (Source: Implementing Network Scanning)

A) The plug-in scan report matches the result of the configured vulnerability definition.
B) The end-user quarantine role scan results match the plug-in scan results.
C) The peer-to-peer software activity plug-in scan matches the configured vulnerability definition.

Q9) When implementing network scanning, what is the next step after you configure Nessus plug-in options? (Source: Implementing Network Scanning)

A) Configure General Setup.
B) Apply plug-ins.
C) Configure vulnerability handling.
D) Test scanning.

Q10) Do you have to create a quarantine role before you configure traffic control policies? (Source: Implementing Network Scanning)

A) Yes, you have to create at least one quarantine role before you configure traffic policies.
B) No, you do not; there is a default quarantine role that you can use to configure traffic control policies.
C) No, you select from preconfigured quarantine roles when you configure traffic control policies.

Q11) After you run a network scan and view the report, you notice that the plug-in did not access any of its dependent plug-ins. What did you forget to do? (Source: Implementing Network Scanning)

A) enable the Dependent Plug-In check box on the General Setup Tab form
B) check the Enable Dependent Plug-In check box associated with the failed plug-in
C) load the dependent plug-ins for that plug-in in the Plug-In Updates form

Q12) What does the Network Scanning Test form allow you to do? (Source: Implementing Network Scanning)

A) try out your scanning configuration
B) test your quarantine role settings
C) try out your Cisco NAS and Cisco NAA communication configuration

Q13) Where do you go to view a full administrator report in the Cisco NAM web console? (Source: Implementing Network Scanning)

A) Choose **Device Management** > **Clean Access** > **Network Scanner** > **Reports** and click the **Report** icon.
B) Choose **Device Management** > **Clean Access** > **General Setup** > **Reports** and click the **Report** icon.
C) Choose **Device Management** > **Clean Access** > **Network** S**canne**r and click the **View** icon.
D) Choose **Device Management** > **Clean Access** > **Network Scanner** > **Reports** and click the **View** icon.

Q14) Where do you enable the use of the User Agreement page? (Source: Implementing Network Scanning)

A) on the User Agreement Page form
B) on the Users Page form
C) on the User Pages Setup form
D) on the General Setup form

Q15) In the Updates form, how do you show the current version of Cisco checks and rules that have been downloaded? (Source: Configuring the Cisco NAM to Implement the Cisco NAA on User Devices)

A) click **Update**
B) click **Show Current Version**
C) click **Cisco Checks & Rules**

Q16) What is a “check” in a Cisco NAC Appliance system requirement? (Source: Configuring the Cisco NAM to Implement the Cisco NAA on User Devices)

A) a pointer to installation files or links from which software can be downloaded
B) a condition statement that examines a feature of the client system
C) a condition statement with logical operators that form a Boolean statement

Q17) Which of the following statements is an example of a Cisco NAC Appliance system requirement? (Source: Configuring the Cisco NAM to Implement the Cisco NAA on User Devices)

A) a requirement that ensures that there is a registry entry for a specific antivirus software
B) a requirement to have the temporary role session timeout configured for a 4-minute session timeout
C) a requirement to have the latest version of Microsoft Windows downloaded to a client

Q18) What happens when the **Automatically Create Rule Based on This Check** option is chosen? (Source: Configuring the Cisco NAM to Implement the Cisco NAA on User Devices)

A) The rule is given the name of the new check and the rules form is opened.
B) A new rule is added to the rules form and this new rule is also mapped to the default requirement.
C) The rule is named “checkname-rule” and populated with the new check.

Q19) Which menu path accesses the form that is used to create a new antivirus rule? (Source: Configuring the Cisco NAM to Implement the Cisco NAA on User Devices)

A) **Clean Access Agent > Rules > New AV Rule**
B) **Clean Access Agent > Rules > New Rule**, then choose the antivirus rule type
C) **Clean Access Agent > AV Rules > New AV Rule**

Q20) Based on the Boolean order of precedence, how would Cisco NAC Appliance evaluate the following rule: “spamawareLogRecent & (NorAVProcessIsActive | SymAVProcessIsActive)”? (Source: Configuring the Cisco NAM to Implement the Cisco NAA on User Devices)

A) Either the Norton Antivirus or the Symantec antivirus process is active and there is a recent Spam Aware log entry.
B) There is a recent Spam Aware log entry and the Norton Antivirus is active or the Symantec antivirus process is active.
C) There is a recent Spam Aware log entry, the Norton Antivirus is active, and the Symantec antivirus process is active.

Q21) What happens when a client does not meet the rules of a “soft” requirement? (Source: Configuring the Cisco NAM to Implement the Cisco NAA on User Devices)

A) The client is advised of the check result, blocked from the network, and quarantined.
B) The client is advised of the check result, assigned the temporary role, and allowed to download the required software.
C) The client is advised of the check result but is not quarantined or blocked from the network.

Q22) What are the two heartbeat interfaces called in a Cisco NAM high-availability configuration? (Source: Configuring Cisco NAM High Availability)

A) primary and standby
B) TCP and UDP
C) UDP and serial

Q23) Which port does the Cisco NAM use as the trusted interface? (Source: Configuring Cisco NAM High Availability)

A) eth1
B) eth10
C) eth0
D) eth20

Q24) Which type of cable is used to connect the eth1 Ethernet ports of the two Cisco NAMs of a high-availability cluster? (Source: Configuring Cisco NAM High Availability)

A) a crossover cable
B) a serial cable
C) a Cat5e cable

Q25) How can a computer with only one serial port running the Cisco NAM support a serial heartbeat connection? (Source: Configuring Cisco NAM High Availability)

A) A computer with only one serial port cannot be used to support a serial heartbeat connection.
B) The first serial port that is detected on the Cisco NAM server is configured for console input and output and you need a second Cisco NAM server to support the redundant serial heartbeat connection.
C) After the Cisco NAM is installed, you can reconfigure the serial port to serve as the high-availability heartbeat connection.
D) Use SSH to access the command-line interface of the router and install the Cisco NAM, leaving the one serial port as the high-availability heartbeat connection.

Q26) What IP address must the CA-signed certificate be based on? (Source: Configuring Cisco NAM High Availability)

A) the service IP
B) the default gateway
C) the DNS server
D) the crossover network

Q27) In the second step of configuring the primary Cisco NAM, why do you copy the existing network settings IP address to the Service IP Address field? (Source: Configuring Cisco NAM High Availability)

A) to have an IP address that the Cisco NAAs already recognize
B) to have an IP address that the standby Cisco NAM recognizes
C) to have an IP address that the Cisco NASs already recognize

Q28) When you configure the standby Cisco NAM, what do you do with the SSL key and the CA-signed certificate? (Source: Configuring Cisco NAM High Availability)

A) The private SSL key file and the CA-signed certificate are imported into the standby Cisco NAM.
B) The public SSL key file and the CA-signed certificate are exported to be used by the primary Cisco NAM.
C) The public SSL token file and the CA-signed certificate are exported to be used by the primary Cisco NAM.

Q29) Which port does a highly available Cisco NAS pair use as the heartbeat? (Source: Configuring Cisco NAS High Availability)

A) eth1
B) eth10
C) eth0
D) eth20

Q30) What additional configuration must be done if you are configuring high availability for Cisco NAS pairs that operate as DHCP servers? (Source: Configuring Cisco NAS High Availability)

A) Enable serial login on each Cisco NAS.
B) Configure an SSH tunnel between the Cisco NAS pairs.
C) Configure an SSL tunnel between the Cisco NAS pairs.
D) Enable DHCP passthrough on the standby Cisco NAS.

Q31) You are implementing a high-availability configuration for your Cisco NAC Appliance. You have configured your standby Cisco NAS with a 10.10.10.3 address. The current IP address of the Cisco NAS is 10.10.10.2. What should the service IP address of the primary Cisco NAS be? (Source: Configuring Cisco NAS High Availability)

A) 10.10.10.2
B) 10.10.10.3
C) 10.10.10.4

Module Self-Check Answer Key

Q1)	C, D
Q2)	A
Q3)	A
Q4)	B
Q5)	A
Q6)	A
Q7)	C
Q8)	A
Q9)	C
Q10)	B
Q11)	C
Q12)	A
Q13)	A
Q14)	D
Q15)	A
Q16)	B
Q17)	C
Q18)	C
Q19)	A
Q20)	A
Q21)	C
Q22)	B
Q23)	C
Q24)	A
Q25)	B
Q26)	A
Q27)	C
Q28)	A
Q29)	C
Q30)	B
Q31)	A