Network Infrastructure Identity-Based Network Access Control and Policy Enforcement

Implementation Guide
April, 2003

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

Customer Order Number: 956650

CONTENTS

About this Document vii

Intended Audience vii

Document Organization vii

Document Conventions viii

Obtaining Documentation viii

World Wide Web viii

Documentation CD-ROM ix

Ordering Documentation ix

Documentation Feedback ix

Obtaining Technical Assistance ix

Cisco.com x

Technical Assistance Center x

Cisco TAC Web Site x

Cisco TAC Escalation Center xi

CHAPTER 1 **Overview** 1-1

How It Works 1-1

Enhanced Policy Enforcement with Cisco End-to-End 1-2

Extending Identity and Policy Management to Devices 1-3

Summary 1-4

CHAPTER 2 **Deploying EAP-TLS Network Access Control** 2-1

Client Configuration 2-1

Verify Client-Side Operating System Support for 802.1x 2-1

Install an X.509 v3 PKI Certificate on the Client 2-2

Obtain the Certificate 2-2

Install the Certificate 2-7

Verify the Installation of the Certificate 2-8

Enable 802.1x Authentication in the Operating System 2-12

Specify the EAP-TLS Authentication Facility for 802.1x 2-13

CiscoSecure ACS Configuration 2-14

Install CiscoSecure ACS V3.0 on a Microsoft Windows 2000 Server 2-14

Configure RADIUS Communications to the Switch 2-15

Install a Server-Side PKI Certificate on the ACS 2-17

Configure the Relevant PKI CA as Trusted **2-19**
Configure EAP-TLS as the Global Authentication Mechanism **2-21**
Create Necessary Accounts in Applicable User Databases **2-22**
Using the Built-In CiscoSecure ACS User Database **2-23**
Integrating With Microsoft Active Directory **2-24**
Switch Configuration **2-25**
Enable RADIUS Support on the Switch **2-26**
Enable 802.1x Support on the Switch **2-26**
Configure Port-Level 802.1x Settings **2-26**
Configure the 802.1x Timers (Optional) **2-27**

CHAPTER 3 **Deploying EAP-MD5 Network Access Control 3-1**
Client Configuration **3-1**
Verify Client-Side Operating System Support for 802.1x **3-1**
Enable 802.1x Authentication in the Operating System **3-2**
Select EAP-MD5 Authentication Facility for 802.1x **3-3**
CiscoSecure ACS Configuration **3-4**
Install CiscoSecure ACS V3.0 on a Microsoft Windows 2000 Server **3-4**
Configure RADIUS Communications to the Switch **3-4**
Create a Client Account in the ACS User Database **3-7**
Switch Configuration **3-7**
Enable RADIUS Support on the Switch **3-7**
Enable 802.1x Support on the Switch **3-8**
Configure Port-Level 802.1x Settings **3-8**
Configure the 802.1x Timers (Optional) **3-9**

CHAPTER 4 **Configuring Identity-Based 802.1x Dynamically Assigned VLANs for Catalyst Switches 4-1**
Prerequisites **4-1**
Operational Overview **4-2**
RADIUS Server Configuration **4-3**
Configuring Group & User VLAN Policies **4-7**
Group VLAN Policies **4-8**
User-Specific Policies **4-9**
Enforcing Group Policies Using VLANs **4-10**
VLAN-Based Group Access Control Configuration **4-11**
Common Configuration **4-12**
Configuration Example using ACLs and VLANs **4-12**
Configuration Example using Firewalls **4-15**

Example Using the 802.1x Guest VLAN Feature **4-16**
Enabling Guest VLANs **4-18**
ACLs and Addressing **4-19**
DHCP and Retries **4-19**

CHAPTER 5 **Moving to an Identity-Based Networking Environment** **5-1**
Components of Identity Networking **5-1**
Impact of Client Side Supplicant Code **5-2**
Impact of Authenticator Network Access Devices **5-3**
Impact of the RADIUS Server and the User Database **5-3**
Moving to an Identity-Based Networking Environment **5-3**
Migrating Non-Authenticator Capable Hardware **5-6**
Upgrading Authenticator Capable Devices **5-7**
Upgrading the Clients and Enabling Supplicant Capabilities **5-7**
Disabling the Guest VLAN Feature **5-8**
Migrating in an Environment of Non-guest Capable Authenticators **5-8**

About this Document

This document is designed to present an example-based overview of how to implement the identity-based network access control and policy enforcement features available in a Cisco end-to-end solution.

Intended Audience

This document is intended for the Enterprise Systems Engineer (SE) or customer who has recently become involved with the security aspects of a Cisco AVVID network and who may be unfamiliar with the deployment choices available to an Enterprise customer.

Document Organization

This document contains the following chapters:

Chapter or Appendix	Description
Chapter 1, “Overview”	Provides an overview of the Network Access Control and Policy Enforcement solution from Cisco.
Chapter 2, “Deploying EAP-TLS Network Access Control”	Provides information and tips on deploying x.509 public key infrastructure (PKI) certificate authenticated 802.1x port-based access control using CiscoSecure ACS v3.0 in a wired environment of Cisco Catalyst switches.
Chapter 3, “Deploying EAP-MD5 Network Access Control”	Provides information and tips on deploying username and password authenticated 802.1x port-based access control using CiscoSecure ACS v3.0
Chapter 4, “Configuring Identity-Based 802.1x Dynamically Assigned VLANs for Catalyst Switches”	Provides information about using dynamically assigned identity-based VLANs to implement administrative policy.
Chapter 5, “Moving to an Identity-Based Networking Environment”	Provides a recommendations for migrating to an 802.1x identity-based network.

Document Conventions

This guide uses the following conventions to convey instructions and information:

Table 1 Document Conventions

Convention	Description
boldface font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{x | y | z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information you must enter.
< >	Nonprinting characters, for example passwords, appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the "Leave Feedback" at the bottom of the Cisco Documentation home page.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

Overview

The need for enterprise-wide security has never been greater or as well understood as in today's climate. Various threats abound with the goal of stealing, manipulating, or impeding information. Numerous solutions have been developed that address perimeter defenses, but the fact remains that the greatest level of risk, or threat, with regard to information theft or unauthorized access remains within the internal network boundaries.

One point of concern is the relative ease of physical and logical access to an enterprise network. Both physical and logical access have been broadened to enable a level of mobility, providing several benefits to business operations and overall productivity. However, simultaneously, this enabling of mobility, combined with a very narrow field of available solutions to address the security thereof, has also increased the overall risk of network exposure.

This document outlines a framework and solution based on technology standards that allow the network administrator to implement true identity-based network access control and policy enforcement, down to the user and individual access-port level. The solution provides user or device identification using strong authentication technologies known to be secure and reliable. It ties the identified entity with policies that are created and administered by management, thereby providing unparalleled granularity of control. Ultimately, the network infrastructure described in this solution is designed to enforce those policies, up to the edge of the network.

How It Works

The Network Access Control and Policy Enforcement solution from Cisco provides the network with the following services and abilities:

- User and/or device authentication
- The ability to tie the identity of a network entity to a defined set of policies configured by management
- Granting or denying network access, at an individual port level, based on configured authorization policy
- Enforcing of additional applicable policies, such as resource access and quality of service, on any access granted

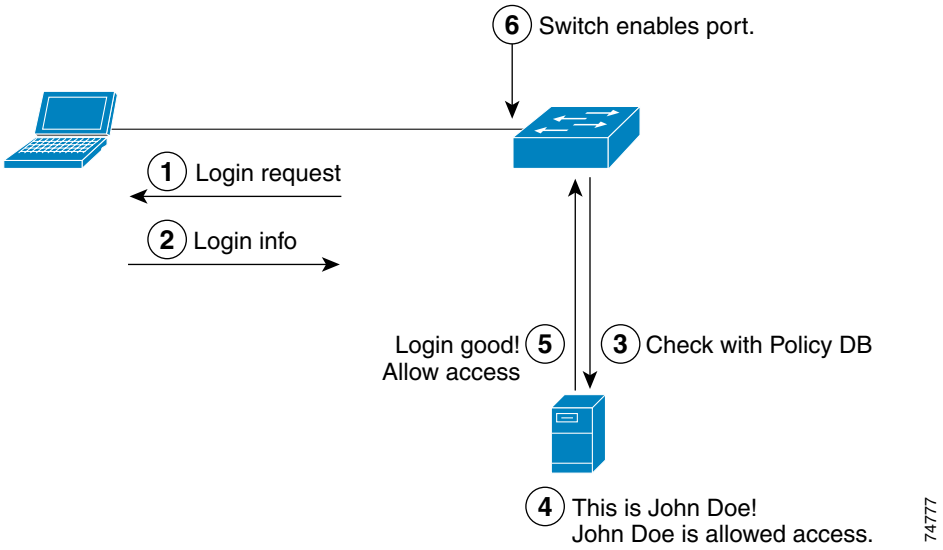
These abilities are introduced when a Cisco end-to-end solution is implemented with the following features and technologies:

- Cisco Catalyst 4000 or 6000 family switches
- Cisco Catalyst 2950 or 3550 switches

- CiscoSecure Access Control Server (ACS) for Windows v3.1
- An 802.1x compliant client operating system, such as Microsoft Windows XP or Windows 2000
- Optionally, for strong authentication, an X.509 Public Key Infrastructure (PKI) certificate architecture

In compliance with the IEEE 802.1x standard, Cisco Catalyst switches can perform basic port-based network access control. By configuring 802.1x compliant client software with a PKI certificate, or username and password, the Cisco Catalyst switches running 802.1x features will authenticate the requesting user or system in conjunction with a back-end CiscoSecure ACS server. Figure 1-1 illustrates these concepts.

Figure 1-1 Port-based Network Access Control



User or device credentials and reference information are processed by the CiscoSecure ACS server. The CiscoSecure ACS is able to reference user or device policy profile information either internally, using the integrated user database, or externally, using database sources such as Microsoft Active Directory, LDAP, Novell NDS, or Oracle databases. This allows for integration of the solution into exiting user management structures and schemes, thereby simplifying overall management.

Enhanced Policy Enforcement with Cisco End-to-End

Although simple authentication with all basic 802.1x compliant devices stands as remarkably improved over current access control solutions, an even more advantageous solution can be realized when an end-to-end Cisco solution is deployed. Completely standards-based and interoperable with third party 802.1x and RADIUS compliant devices, Cisco's Network Access Control and Policy Enforcement Solution provides enhanced features when deployed as a Cisco end-to-end solution. Building on the basic authentication concept, an end-to-end Cisco solution allows clear integration of network-wide, identity-based policies and the enforcement of those policies by the network. A Cisco end-to-end solution also provides better overall integration for VoIP installations. This is possible by leveraging the additional ability of the CiscoSecure ACS server to communicate policy information and parameters back to the network devices. This allows the ACS back-end databases to become the central point for

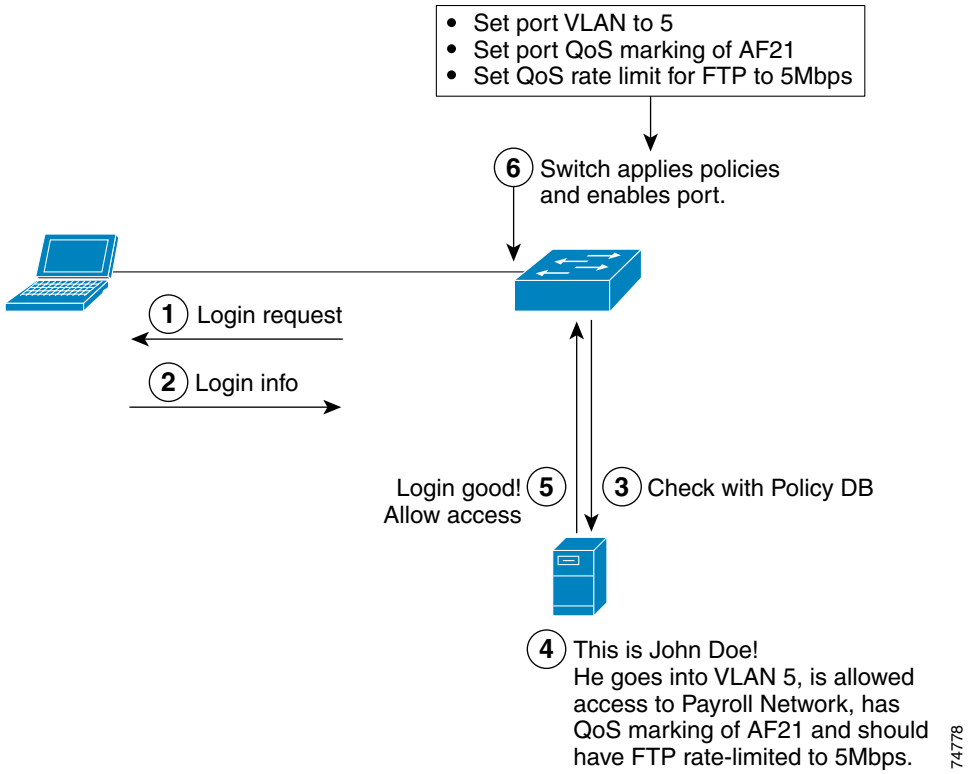
policy configuration and reference, while the network becomes the enforcement point for those policies. Some of the parameters that can be dynamically configured and assigned to a port based on identity include:

- VLAN
- QoS Trust State
- QoS Marking and Queuing
- QoS Rate Limiting
- Access Control Lists
- Per port features, such as port description and CDP operation state

Note Currently, only the VLAN parameters can be assigned using identity. Support for the other parameters is expected in the second half of 2003.

Figure 1-2 illustrates the enhanced policy enforcement capabilities of a Cisco end-to-end solution.

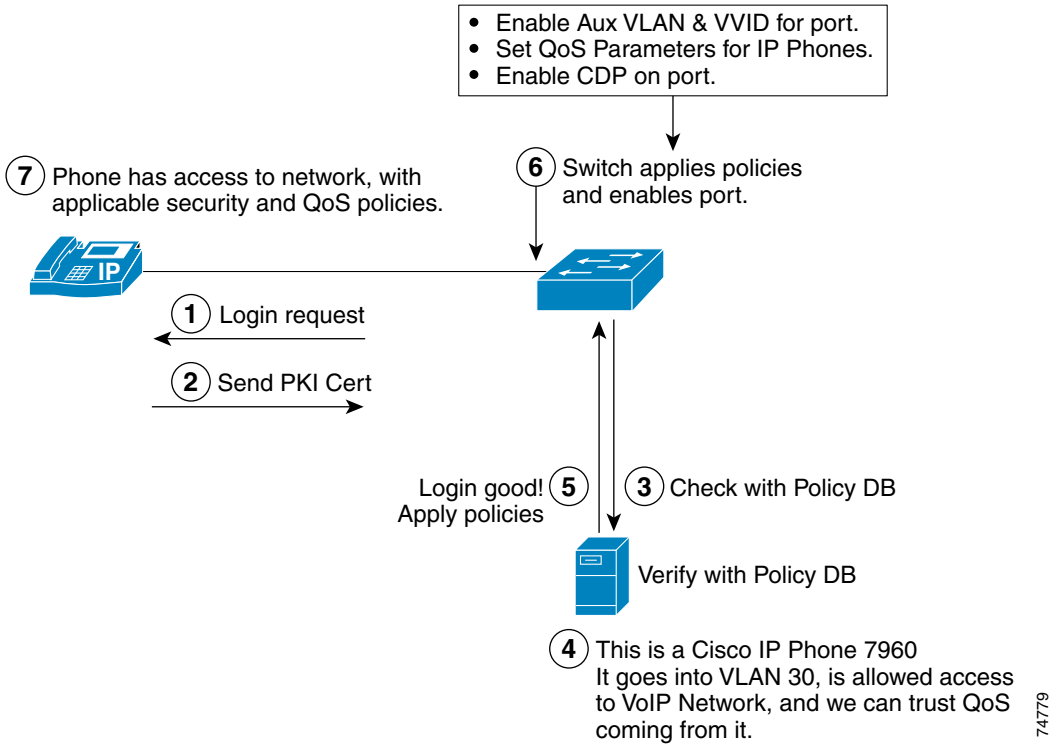
Figure 1-2 Enhanced Policy Enforcement with Cisco End-to-End



Extending Identity and Policy Management to Devices

The identity, authentication, and policy enforcement paradigm can also be extended to include the authentication of network devices, which are 802.1x compliant and allow secured access to the network for authorized standalone devices. Figure 1-3 illustrates this scenario.

Figure 1-3 Extending Identity and Policy Management



Extending the paradigm of identity to include all network connected entities allows the possibility to tie policies to standalone network devices, such as IP phones, manufacturing robots, and IP-based video equipment. This, in turn, provides the network manager with enhanced control over access, authorization, and security policies for those devices.

Summary

The advent of new protocols, such as 802.1x, in combination with the ability for network devices and components to communicate using existing protocols, now provides network managers with new possibilities and unseen flexibility in managing network access control and policies. The association of the identity of a network connected entity to a corresponding set of control policies has never before been as secure and as flexible as today. Proper design and deployment offer the network manager increased security and control of access to network segments and resources, while practically being transparency to the end-user.

The IEEE 802.1x standard allows the implementation of port-based, network access control to a network device. This relies on the 802.1x link-layer protocol to transport EAP-MD5 messages to the authenticator device. In this document, the authenticator device is a Cisco Catalyst switch, which relays the EAP information to a CiscoSecure ACS using the RADIUS protocol.

Two methods of providing identity-based access are discussed in the following chapters: Extensible Authentication Protocol Transport Layer Security (EAP-TLS), which uses x.509 public key infrastructure (PKI) certificate-authenticated 802.1x port-based access control, and EAP Message Digest 5 (EAP-MD5).

CHAPTER 2

Deploying EAP-TLS Network Access Control

This chapter provides examples and tips on deploying x.509 PKI certificate-authenticated 802.1x port-based access control using EAP-TLS and the CiscoSecure ACS v3.0 in a wired environment of Cisco Catalyst switches.

Note This chapter uses Microsoft Windows XP as the supporting client operating system for example and illustration purposes. However, the concepts described should apply equally to any operating system that supports 802.1x.

Client Configuration

The client configuration required to support a network access control solution is fairly straight-forward. To configure the client side of the network access control, do the following:

Step 1 Verify Client-Side Operating System Support for 802.1x

Step 2 Install an X.509 v3 PKI Certificate on the Client

Step 3 Enable 802.1x Authentication in the Operating System

Step 4 Specify the EAP-TLS Authentication Facility for 802.1x

Note The operating system used in the examples in this chapter is Microsoft Windows XP Professional. Application notes for the configuration of other client side operating systems will be available soon.

Verify Client-Side Operating System Support for 802.1x

For the client (supplicant) and the switch (authenticator) to be able to communicate using 802.1x, the client-side operating system must support the IEEE 802.1x standard. The following popular operating systems are known to have either integrated or add-on support for the 802.1x protocol:

- Microsoft Windows XP Professional (integrated)
- Microsoft Windows 2000 & 2000 Server (Microsoft add-on)
- Microsoft Windows NT 4.0 (Microsoft add-on)

- Microsoft Windows 98 & 98 SE (Microsoft add-on)
- Microsoft Windows 95 (3rd party add-on)
- Linux (Open Source add-on)
- Sun Solaris (Open Source add-on)

Support may be available for additional operating systems. If your system is not listed above, please contact your operating system vendor for support information.

Install an X.509 v3 PKI Certificate on the Client

For the 802.1x client to authenticate using the EAP-TLS method, a client side X.509 PKI certificate must be installed on that client. The process by which a user obtains a certificate to validate their identity is called *enrollment*. This section describes how to:

- Obtain the Certificate
- Install the Certificate
- Verify the Installation of the Certificate

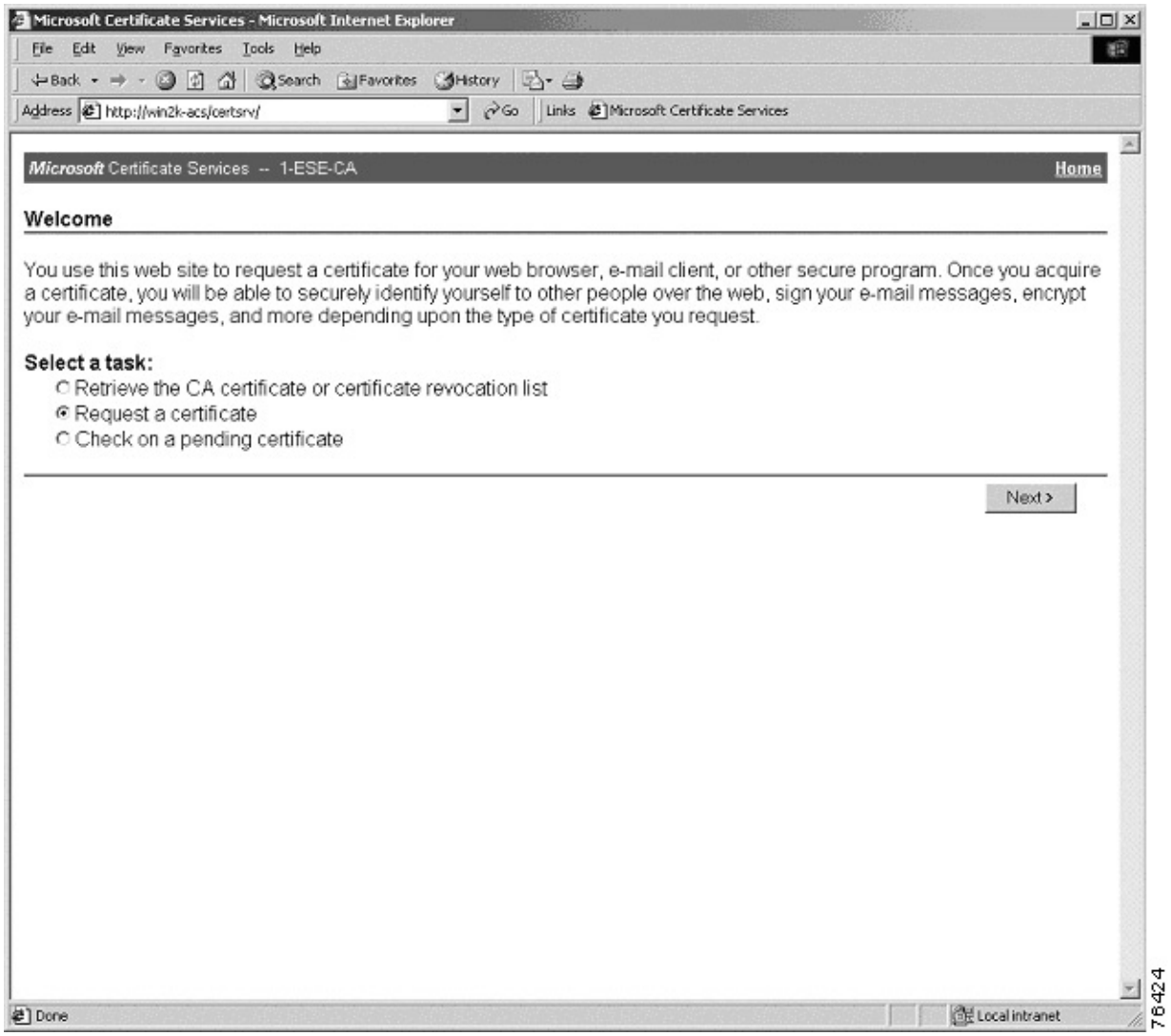
Note Cisco's Network Access control solution is compatible with any X.509 standard PKI solution. However, for the purposes of illustration, the following examples use Microsoft Certificate Services.

Obtain the Certificate

To obtain a PKI certificate suitable for authentication purposes, do the following:

Step 1 Access the Certificate Authority (CA) and select the option to request a certificate (as shown in Figure 2-1). The CA can be found at http://*hostname*/certsrv/.

Figure 2-1 Microsoft Certificate Services—Welcome Page

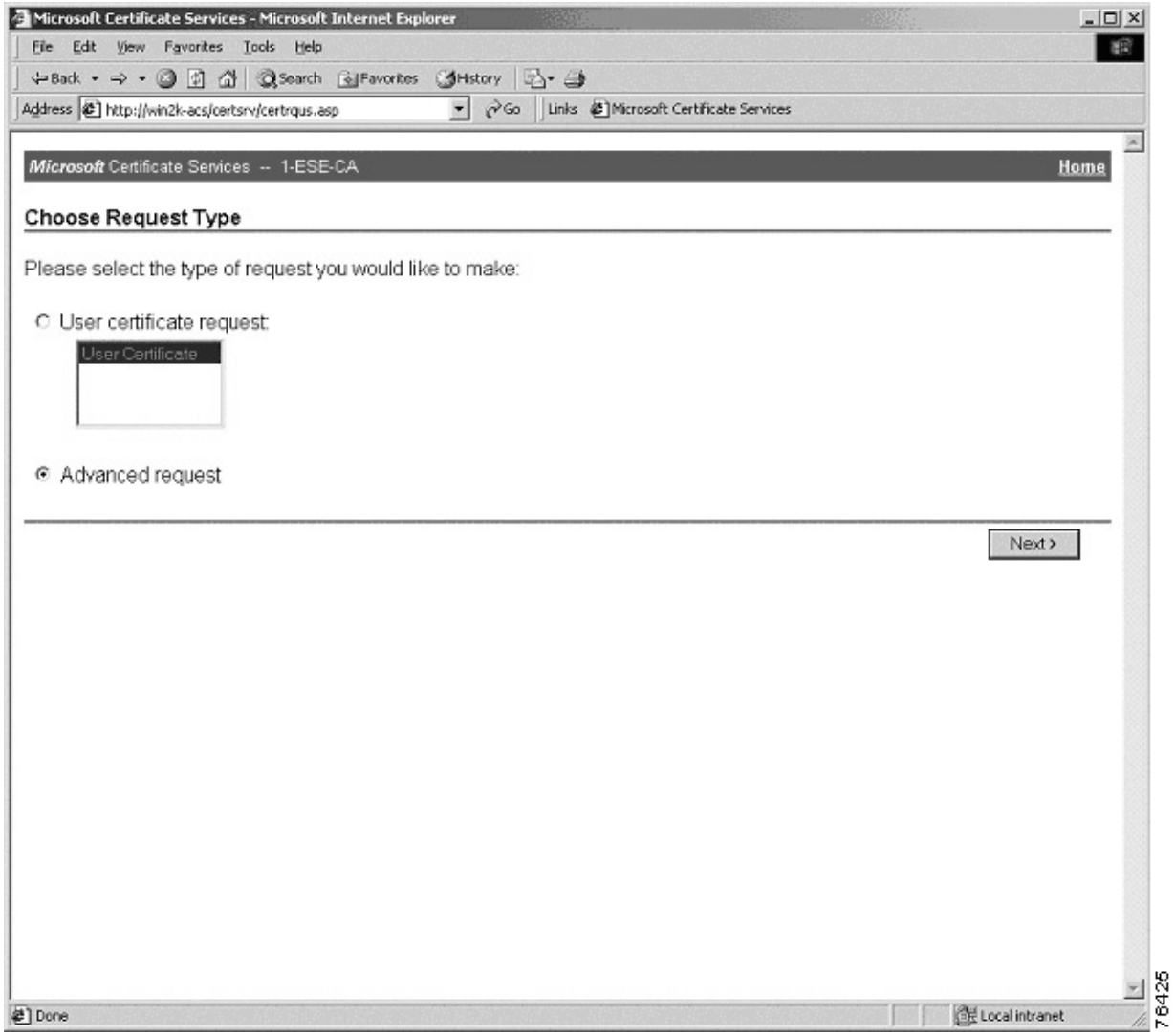


Note Certificates for various purposes (i.e. E-mail encryption, File/Disk encryption, etc.) may be obtained from the CA. However, for 802.1x-based authentication to work, a client authenticating certificate must be obtained.

Step 2 Click on **Next**.

Step 3 Select either a certificate from the list of user certificates or **Advanced request** (as shown in Figure 2-2). In this example, Advanced request was selected. The Advanced request option allows you to specify details, such as key length and other additional fields.

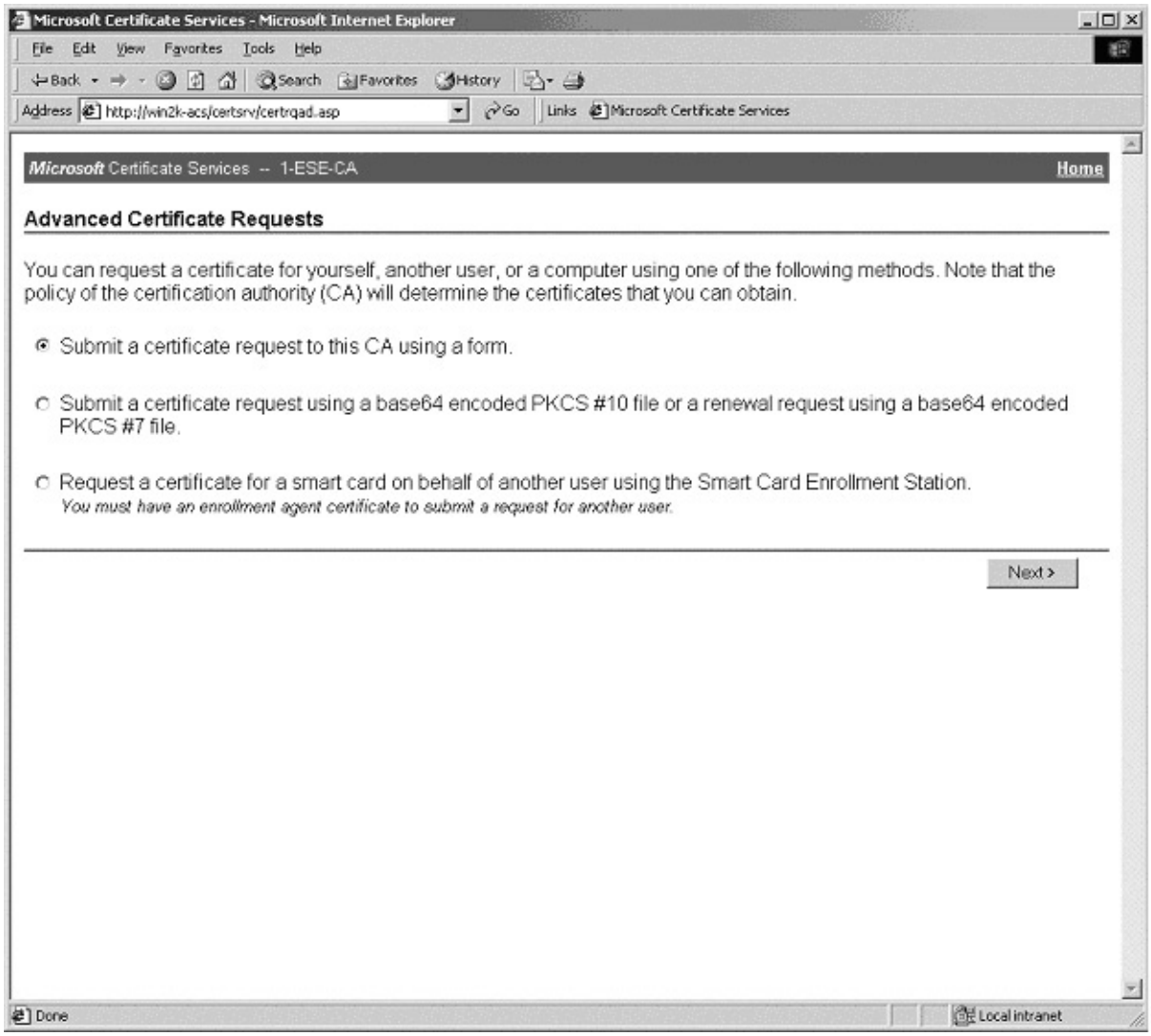
Figure 2-2 Microsoft Certificate Services—Choose Request Type Page



Step 4 Click on **Next**.

Step 5 On the first page of the Advanced Certificate Request (Figure 2-3) specify whether the request is to be sent using a form template, a pre-created PKCS#10 formatted file, or a smart-card enrollment station. For the purposes of manual enrollment in this example, the form-based request is selected.

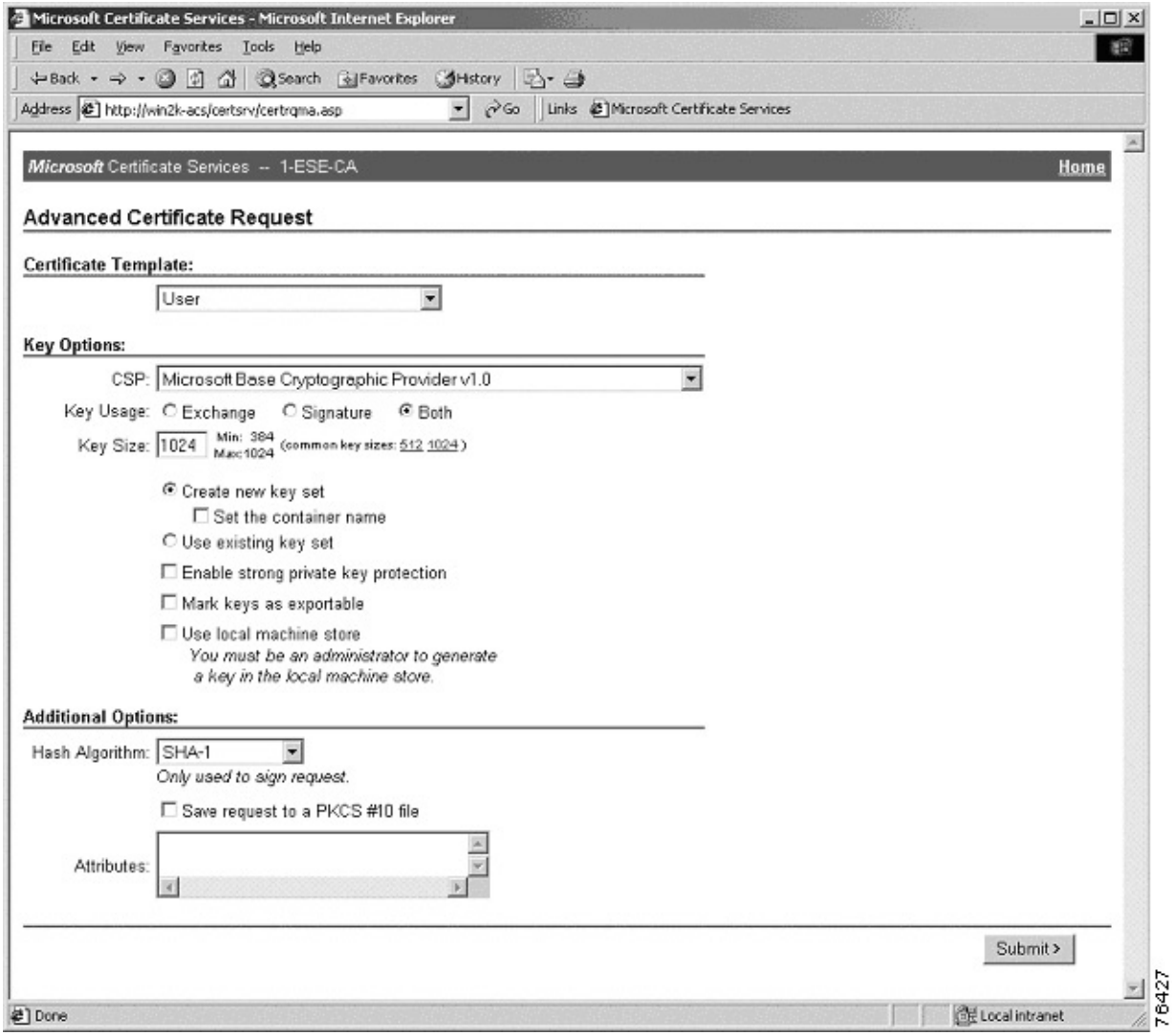
Figure 2-3 Microsoft Certificate Services—Advanced Certificate Requests Page 1



Step 6 Click on **Next**.

Step 7 On the second page of the Advanced Certificate Request (Figure 2-4) specify the public key/private key pair length. The default is 512 bits. For most applications, a minimum key size of 1024 bits is recommended. Enter **1024** in the Key Size field. Make sure that the certificate template chosen is "User".

Figure 2-4 Microsoft Certificate Services—Advanced Certificate Request Page 2



Step 8 Click on **Submit**.

Once the request has been submitted it is processed by the CA according to the policies set by the CA administrator.

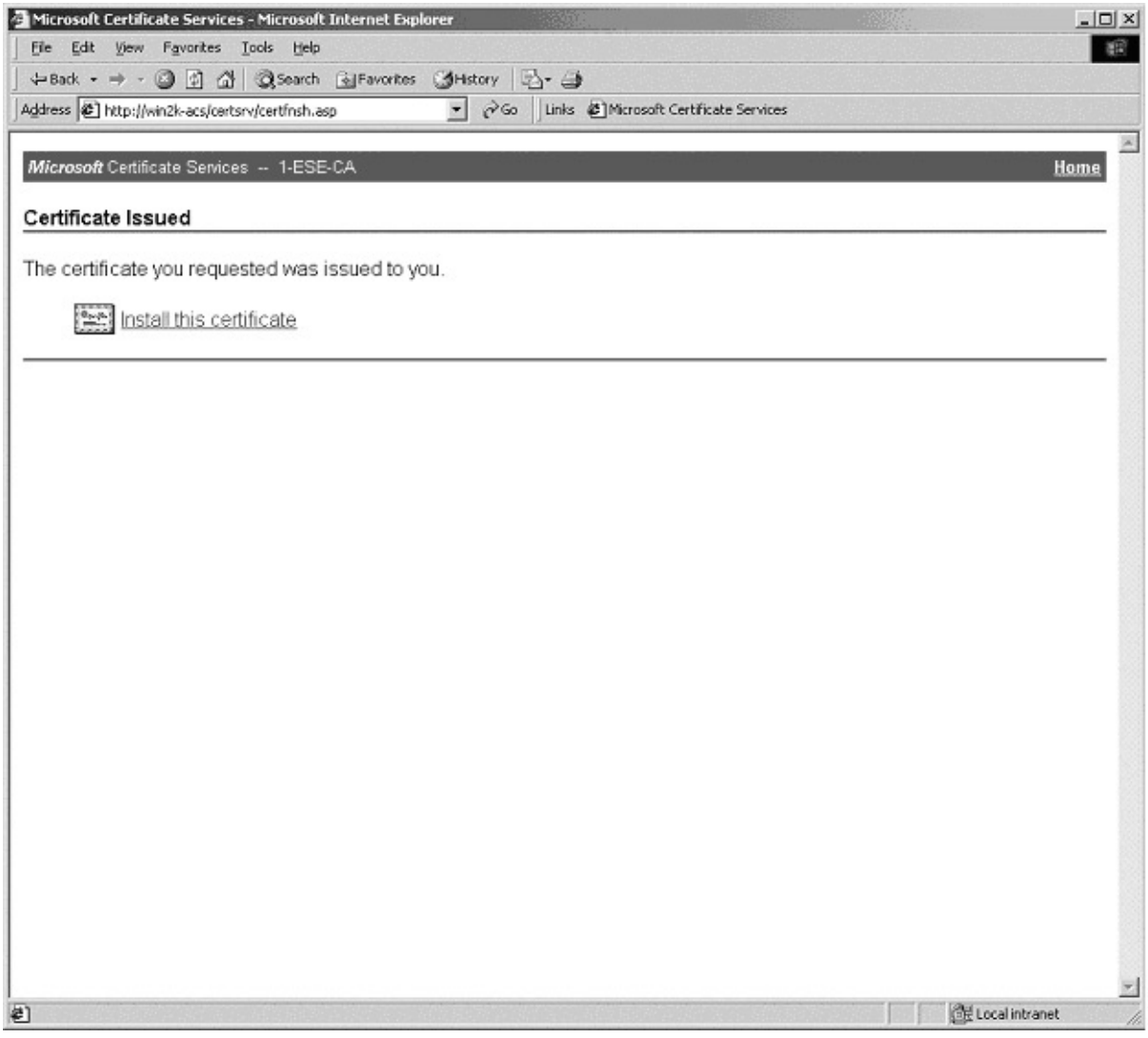
- If the identity of the requester must be verified prior to issuing the certificate, the CA indicates that the pending request must be processed and approved manually. At that point, the user may be asked to check back with the CA at a later date to see if the request has been approved. Once the certificate has been approved, it is ready to be installed.
- If the CA issuing policy has been configured to automatically issue the certificate to domain authenticated users, then the requested PKI certificate is immediately ready for installation by the client.

Note For a request to be processed automatically, the requesting user must be authenticated into the Windows domain or Active Directory. If the user has logged into the domain prior to accessing the enrollment web interface, the process will be transparent. If the user has not logged into the domain, they will be prompted to log into the web enrollment interface at the time of access.

Install the Certificate

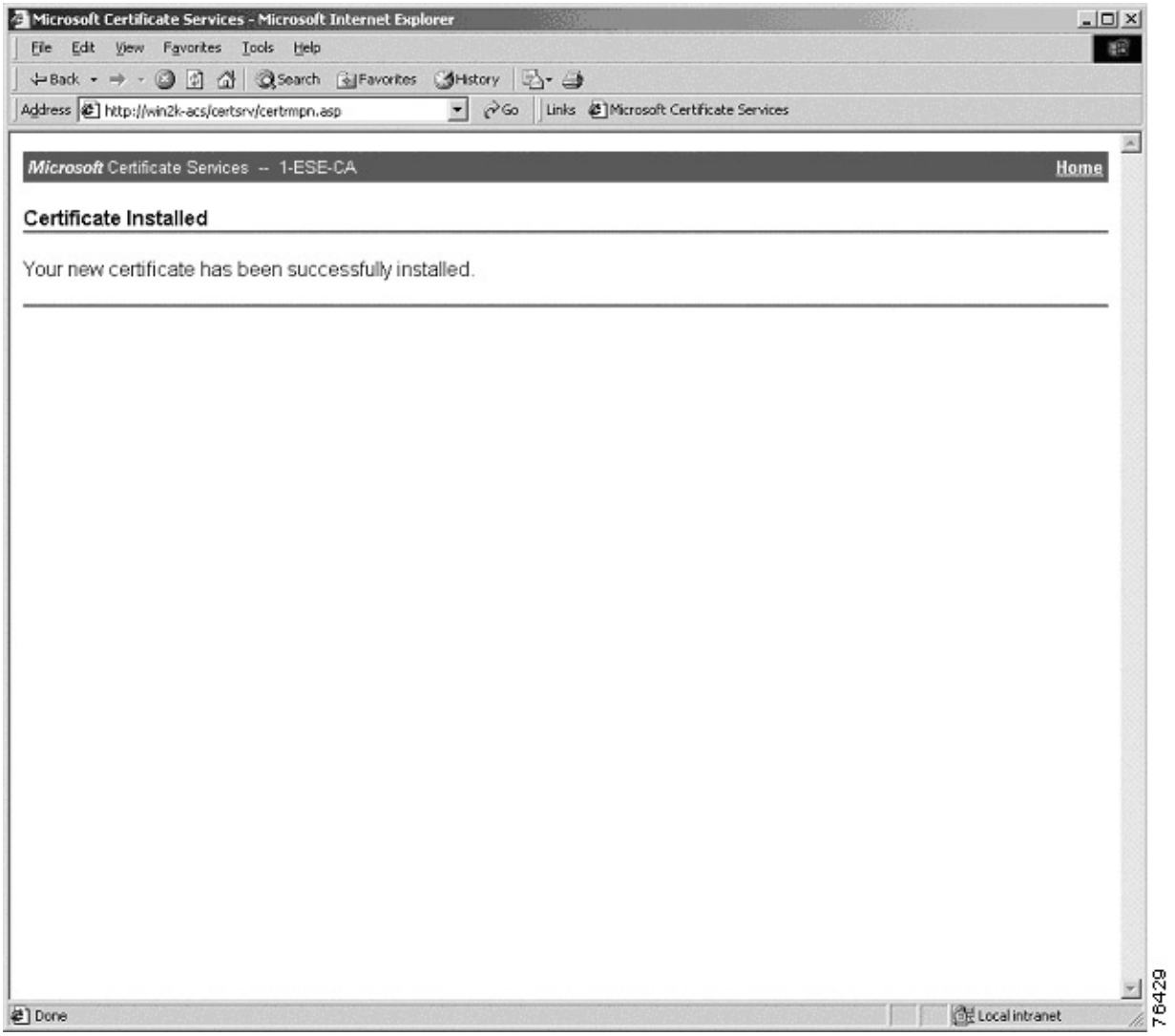
Once the request has been approved, the certificate is ready for installation (as shown in Figure 2-5).

Figure 2-5 Microsoft Certificate Services—Certificate Issued Page



To install the certificate, click on **Install this certificate**. The certificate and the associated private key are automatically installed into the local client machine's secure store associated with that user. When the installation is complete, a confirmation page is displayed (as shown in Figure 2-6).

Figure 2-6 Microsoft Certificate Services—Certificate Installed Page

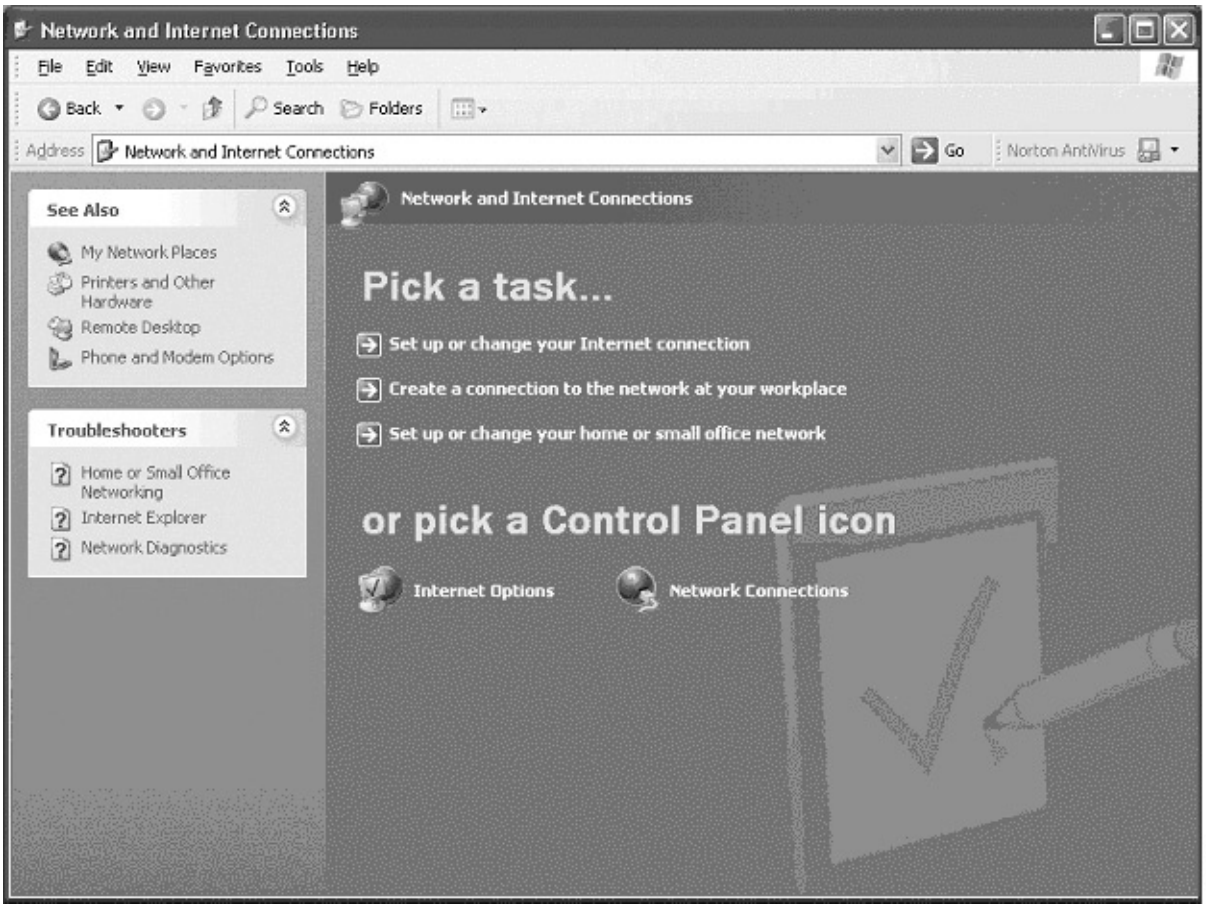


Verify the Installation of the Certificate

To verify the installation of the client-side certificate, do the following:

Step 1 Select **Internet Options** in the Network and Internet Connections page of the Windows XP control panel (as shown inFigure 2-7).

Figure 2-7 Network and Internet Connections Page



The Internet Properties window is displayed.

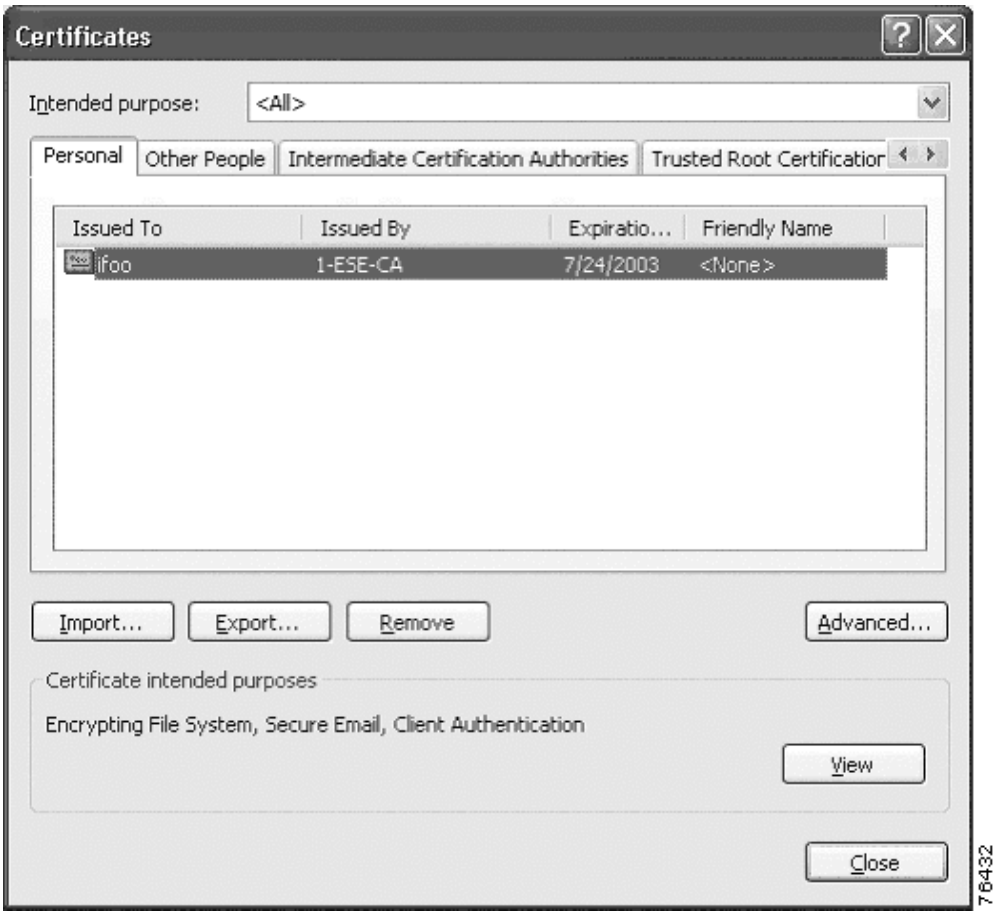
Step 2 To access the certificate stored for the user that is currently logged in, select the "Content" tab, then click on **Certificates** under the "Certificates" section (as shown in Figure 2-8).

Figure 2-8 Internet Properties Window—Content Page

The Certificates window, which shows all the relevant PKI certificate information, is displayed.

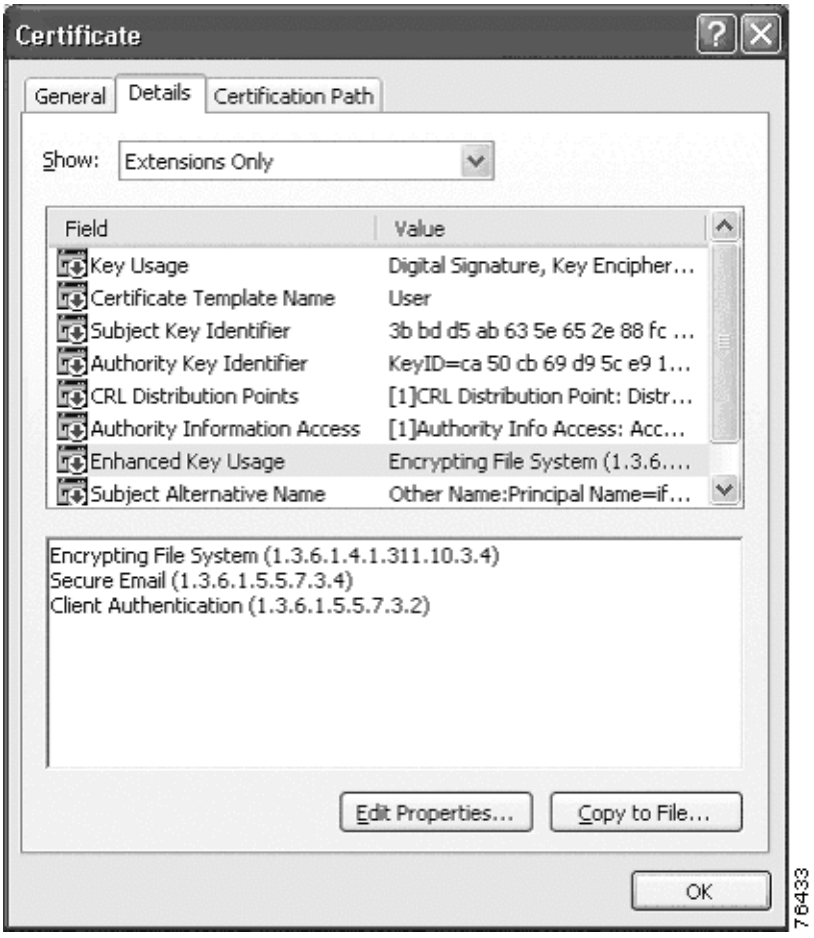
Step 3 Select the "Personal" tab. The user certificate that was issued is listed along with the issuing CA and the expiration date (as shown in Figure 2-9).

Figure 2-9 Certificates Window—Personal Page



Step 4 To display additional details, select the installed certificate and click on **View**. The Certificate window is displayed. To display the various fields in the X.509 certificate, select the "Details" tab (as shown in Figure 2-10).

Figure 2-10 Certificate Window—Details Page



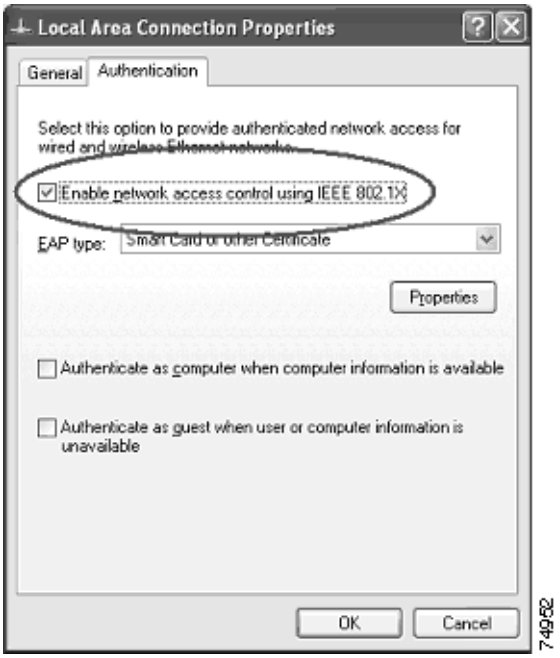
Step 5 Verify the contents of the following fields:

- The "Subject" field should contain the username to which the certificate was issued.
- The "Enhanced Key Usage" field must contain the option for "Client Authentication" (OID 1.3.6.1.5.5.7.3.2). If the certificate lacks the Client Authentication enhanced usage key, the certificate cannot be used for EAP-TLS 802.1x authentication. To correct this situation, the certificate must be deleted and a new certificate must be requested and issued.

Enable 802.1x Authentication in the Operating System

The client-side operating system may, by default, have 802.1x support disabled. Ensure that 802.1x capabilities have been enabled. In Microsoft Windows XP Professional, for example, 802.1x is enabled by selecting the checkbox found in the Authentication section of the Properties page (as shown in Figure 2-11).

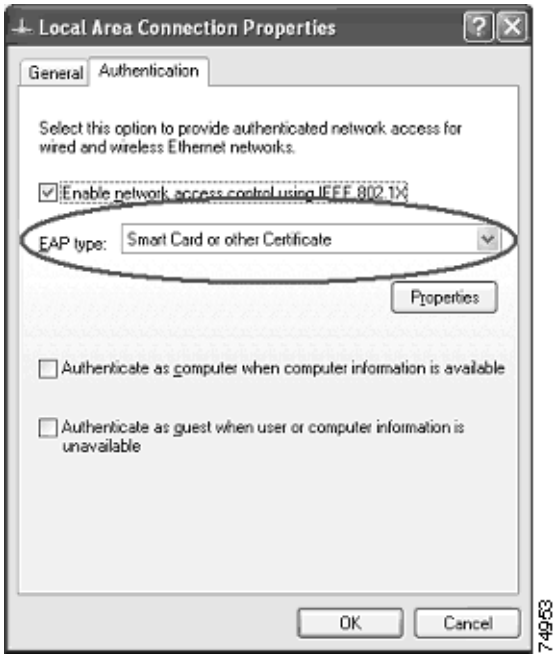
Figure 2-11 Enabling 802.1x in Microsoft Windows XP Professional



Specify the EAP-TLS Authentication Facility for 802.1x

The 802.1x portion of the operating system's configuration may support more than one EAP authentication method. If this is the case, the EAP-TLS certificate-based compatibility mode must be selected from the options. In Microsoft Windows XP Professional, for example, the authentication mode is selected using the pull-down in the Authentication section of the Properties page (as shown in Figure 2-12).

Figure 2-12 Selecting the Authentication Mode in Microsoft Windows XP Professional



Note To increase security with Windows XP, we recommend that you disable the "Authenticate as guest" and "Authenticate as computer" options.

CiscoSecure ACS Configuration

To configure the CiscoSecure ACS, do the following:

Step 1 Install CiscoSecure ACS V3.0 on a Microsoft Windows 2000 Server

Step 2 Configure RADIUS Communications to the Switch

Step 3 Install a Server-Side PKI Certificate on the ACS

Step 4 Configure the Relevant PKI CA as Trusted

Step 5 Configure EAP-TLS as the Global Authentication Mechanism

Step 6 Create Necessary Accounts in Applicable User Databases

Install CiscoSecure ACS V3.0 on a Microsoft Windows 2000 Server

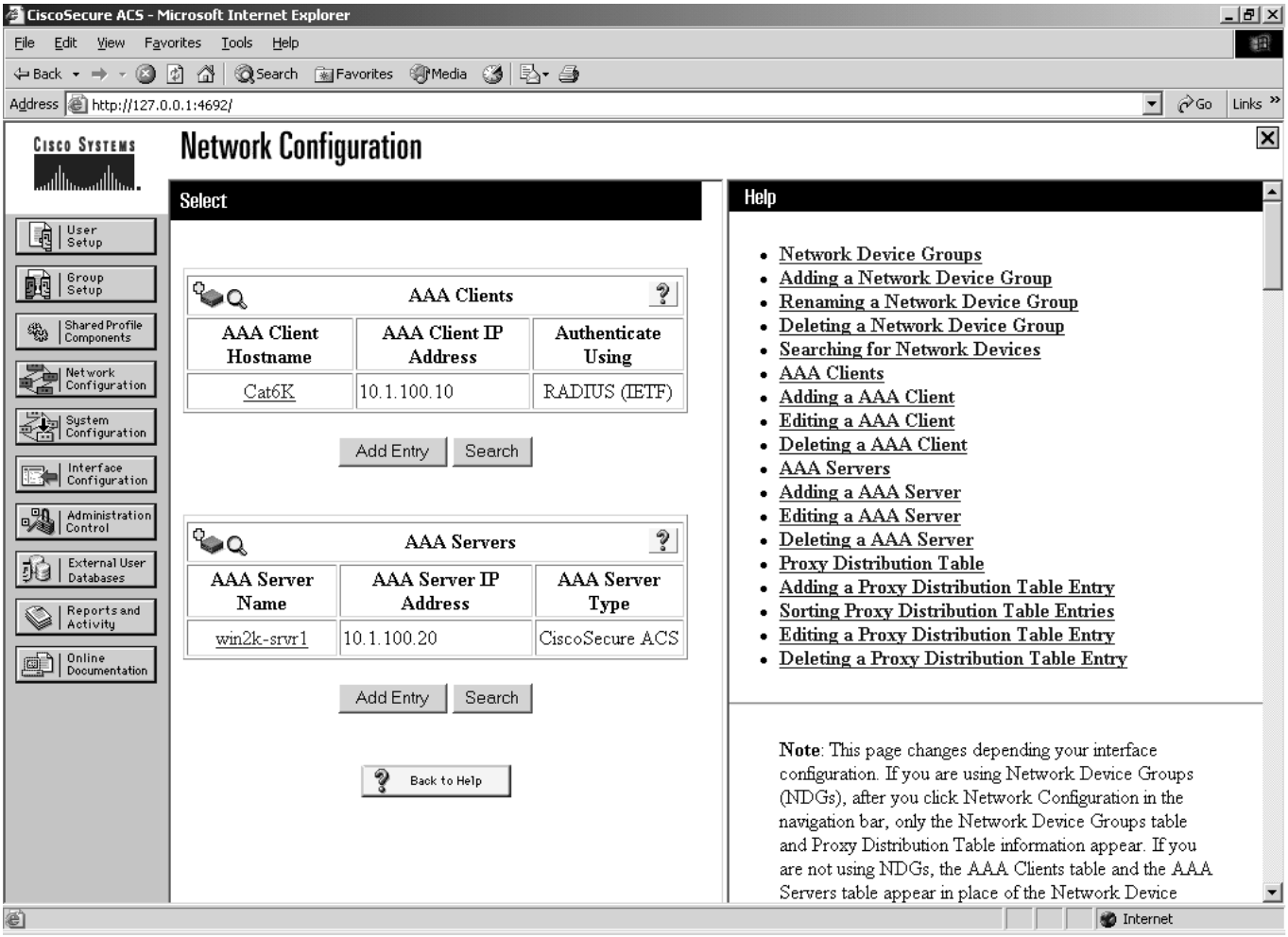
IEEE 802.1x EAP methods are supported in CiscoSecure ACS v3.0 and higher. This version of ACS is designed to be installed on a Microsoft Windows 2000 server. Please refer to the *Installation Guide* that accompanied your CiscoSecure ACS for detailed information on installation and basic configuration.

Configure RADIUS Communications to the Switch

For the CiscoSecure ACS to communicate with the switch (authenticator), RADIUS must be configured between the two. To configure RADIUS communications to the switch, do the following:

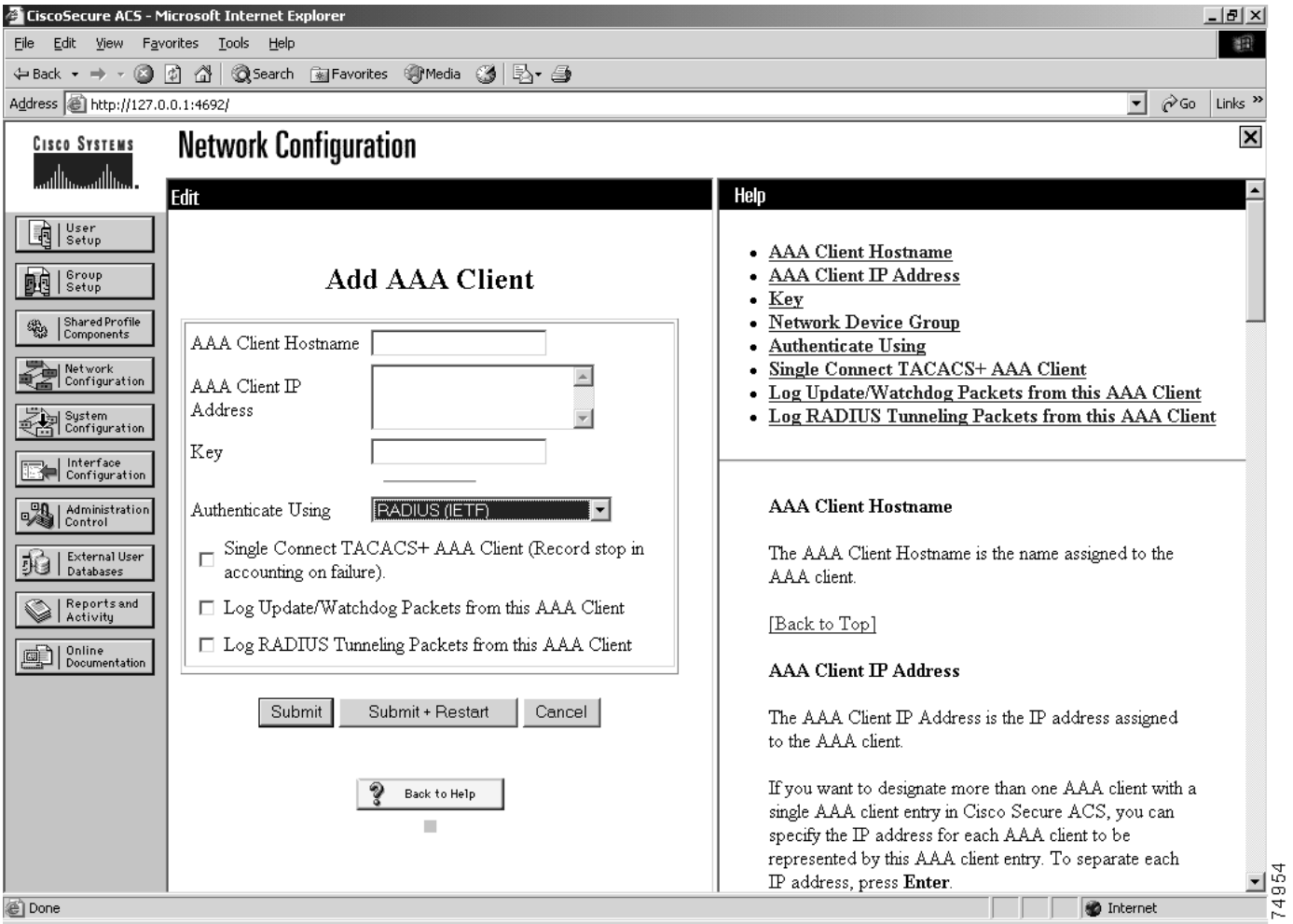
Step 1 On the Network Configuration page (Figure 2-13), click on **Add Entry** under the "AAA Servers" field.

Figure 2-13 NAS Entry Page of Network Configuration Page



Step 2 On the Add AAA Client page (Figure 2-14), specify the IP address, hostname, authentication type, and key.

Figure 2-14 Add AAA Client Page of Network Configuration Page



The fields of this page are explained in Table 2-1.

Table 2-1 CiscoSecure ACS Network Configuration Fields

Field	Description
AAA Client Hostname	The common name used to describe this particular AAA client.
AAA Client IP Address	The IP of the switch's administrative interface.
Key	The shared secret key used to encrypt communications between the AAA Client and the ACS server.
Authenticate Using	The choice of authentication protocol to use. Different versions of TACACS and RADIUS can be selected. The choice of RADIUS type will affect the formatting of the RADIUS packets. The suggested choice is “RADIUS (IETF)”.

Step 3 Click on **Submit**.

Once RADIUS communication has been configured on both the switch and the CiscoSecure ACS, it can be tested by enabling AAA login on the switch. The same username and password combination should be able to login to the CLI interface using AAA and the RADIUS parameters configured.

Install a Server-Side PKI Certificate on the ACS

The EAP-TLS mechanism allows for mutual authentication of the server to the client in addition to the standard client authentication. This feature allows clients to verify the authenticating server for added security. For this mechanism to work, a server-side PKI certificate must be installed on the CiscoSecure ACS. The key usage fields for the certificate issued should allow for "web-server" or "server authentication" uses. Certificates may be installed using various methods, including:

- Import a certificate that is pre-created and formatted in Public-Key Cryptography Standard (PKCS) #12 coding. The CiscoSecure ACS server is capable of generating a PKCS #12 coded certificate request in order to generate a new PKI certificate.
- Import a certificate from a file.
- Use an existing certificate in the local machine store (as shown in Figure 2-16).

Figure 2-15 Using a Pre-existing Certificate from the Local Machine

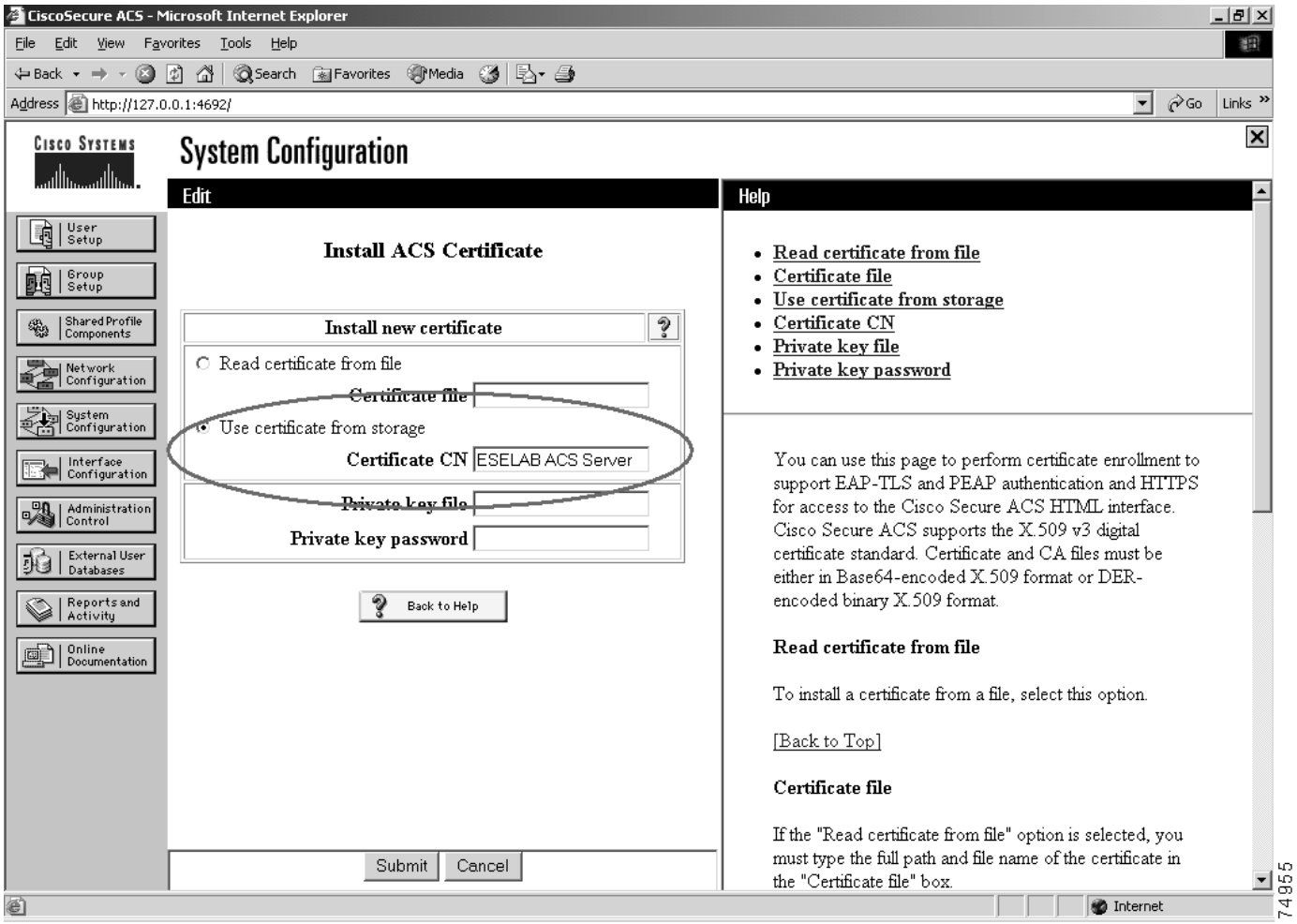
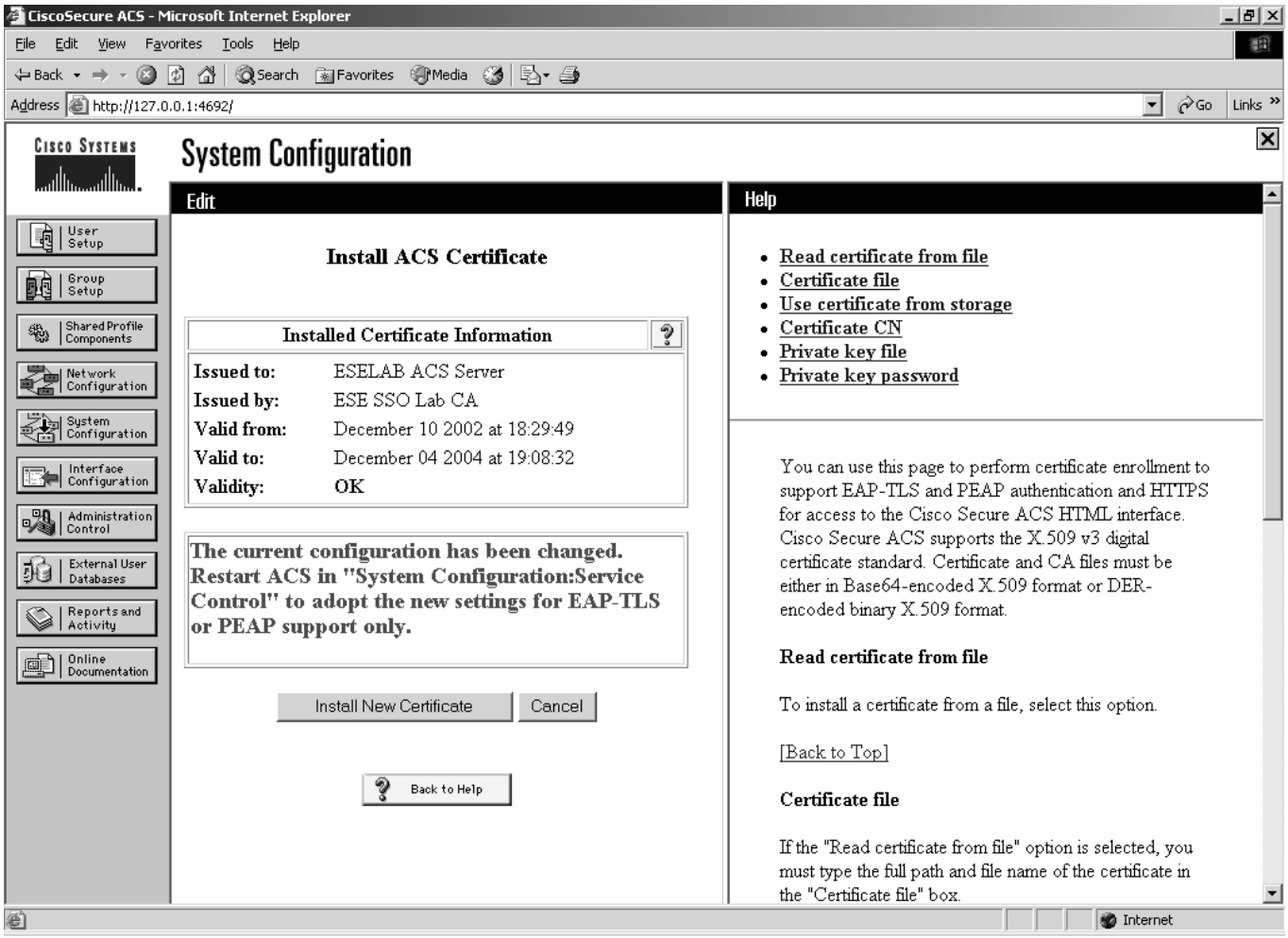


Figure 2-16 illustrates a properly installed server-side PKI certificate.

Figure 2-16 Server-side PKI Certificate Page



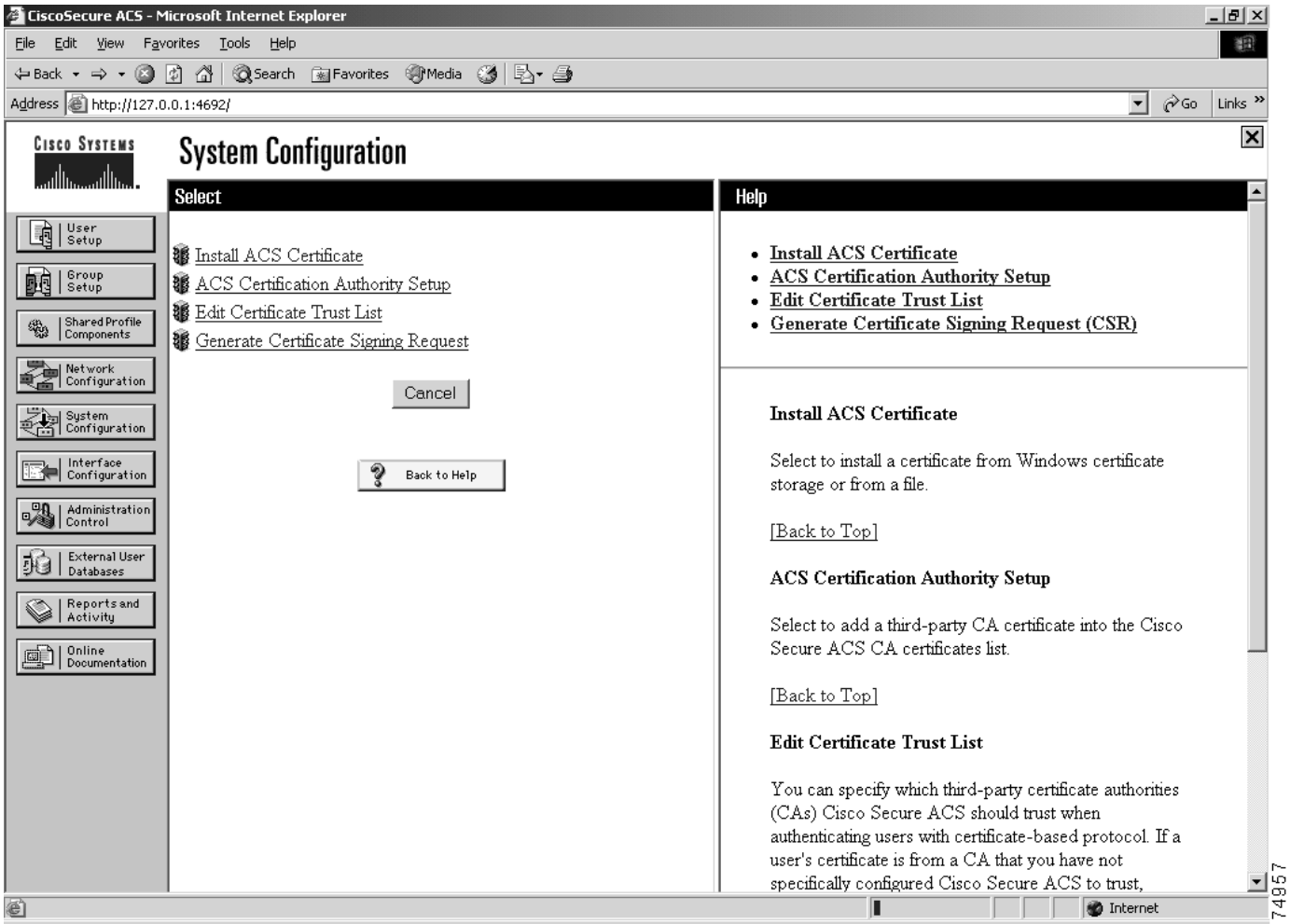
Configure the Relevant PKI CA as Trusted

The PKI certificate issued to the server and the clients must be considered valid and signed by a trusted root CA. If the root CA signing the certificates is a private enterprise root CA, then that CA must be added to the trust list on the server (for the certificates presented to be considered valid).

To add the CA to the trust list, do the following:

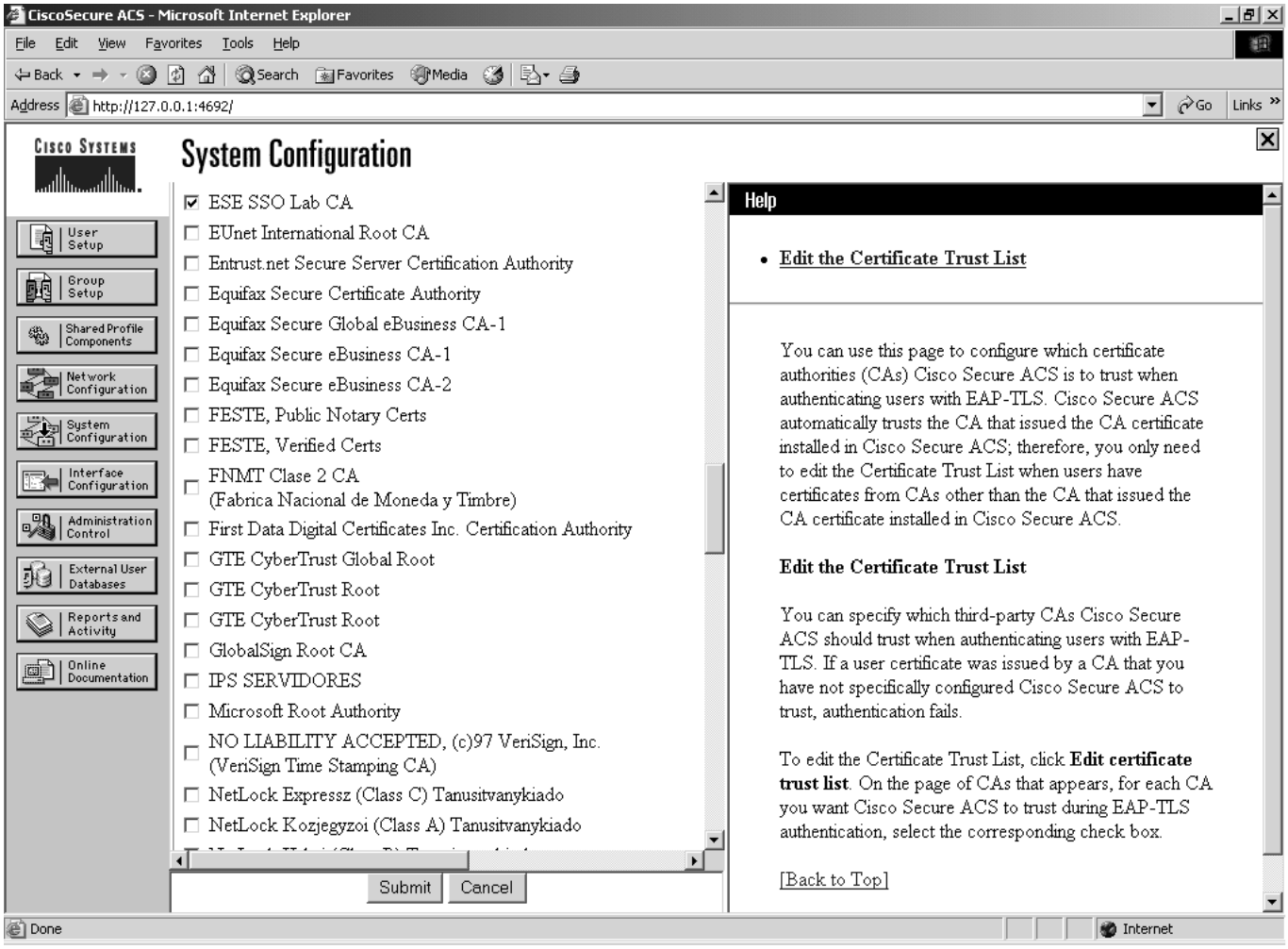
Step 1 Select **Edit certificate list** on the Certification Authorities Setup page of the System Configuration section (as shown in Figure 2-17). A list of installed root server CA certificates is displayed.

Figure 2-17 Certification Authorities Setup Page



Step 2 Check the selection box corresponding to the installed CA entry on the ACS Certificate Setup page (as shown in Figure 2-18).

Figure 2-18 ACS Certificate Setup Page



Step 3 Click on **Submit**.

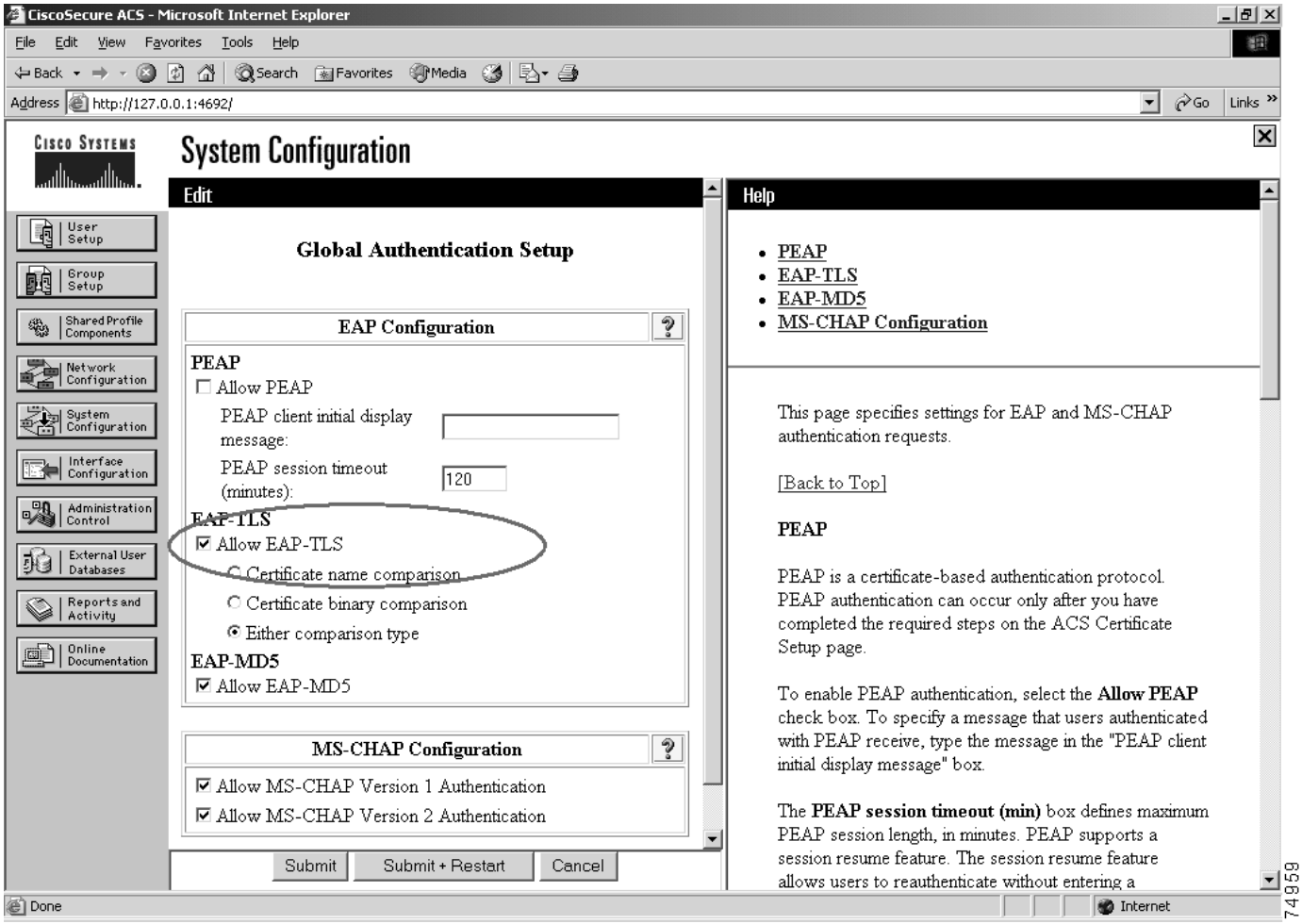
Configure EAP-TLS as the Global Authentication Mechanism

By default, the EAP mechanism used with 802.1x clients is EAP-MD5 challenge/response. To support EAP-TLS, the EAP-TLS mechanism must be configured.

To configure the EAP mechanism, do the following:

Step 1 Select **Allow EAP-TLS** in the Global Authentication Setup page of the System Configuration section (as shown in Figure 2-19).

Figure 2-19 Global Authentication Setup Page



Once the correct EAP type has been selected, the change must be committed and the ACS server restarted for the change to take effect.

Step 2 Click on **Submit + Restart**.

Note As of version 3.0, these two mechanisms are mutually exclusive—only one EAP mechanism can be used by a single CiscoSecure ACS server. If you require both EAP-MD5 and EAP-TLS concurrently (because of various client authentication types), we recommend that you use multiple CiscoSecure ACS servers to service each EAP type.

Create Necessary Accounts in Applicable User Databases

CiscoSecure ACS can support multiple sources for user account authentication validation. Table 2-2 lists the various database sources and authentication methods that can be supported.

Table 2-2 Authentication Protocol and User Database Compatibility

Database	ASCII	PAP	CHAP	ARAP	MS-CHAP v.1	MS-CHAP v.2	LEAP	EAP-MD5	EAP-TLS	PEAP
Cisco Secure ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Windows SAM	Yes	Yes	No	No	Yes	Yes	Yes	No	No	Yes
Windows AD	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	Yes
Novell NDS	Yes	Yes	No	No	No	No	No	No	No	Yes
LDAP	Yes	Yes	No	No	No	No	No	No	Yes	Yes
ODBC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
LEAP Proxy RADIUS Server	Yes	Yes	No	No	Yes	Yes	Yes	No	No	No
ActivCard	Yes	Yes	No	No	No	No	No	No	No	Yes
CRYPTOCard	Yes	Yes	No	No	No	No	No	No	No	Yes
RADIUS Token Server	Yes	Yes	No	No	No	No	No	No	No	Yes
Vasco	Yes	Yes	No	No	No	No	No	No	No	Yes
PassGo	Yes	Yes	No	No	No	No	No	No	No	Yes
RSA	Yes	Yes	No	No	No	No	No	No	No	Yes
Safeword	Yes	Yes	No	No	No	No	No	No	No	Yes

For authentication to occur correctly, the user account for the client must be configured in the appropriate database. The EAP-TLS authentication method supports authentication that references the integrated CiscoSecure User Database (CSDB), Microsoft Active Directory (AD), Novell NDS, or a generic LDAP standard directory.

The following sections describe the process of using the built-in CiscoSecure ACS user database and optional integration into Microsoft Active Directory. For information on using other external database types, please consult the CiscoSecure ACS documentation.

Using the Built-In CiscoSecure ACS User Database

The integrated user database of the CiscoSecure ACS can be used as a source of user information. To use the built-in account database, the administrator must create an account corresponding to the user's certificate subject name.

Note The account created in the CiscoSecure ACS database must match exactly the format and text of the subject in the issued certificate. In a Windows environment that uses Active Directory and the Microsoft Certificate Server, the user name in the subject field of the certificate may be in the format of "user@domain".

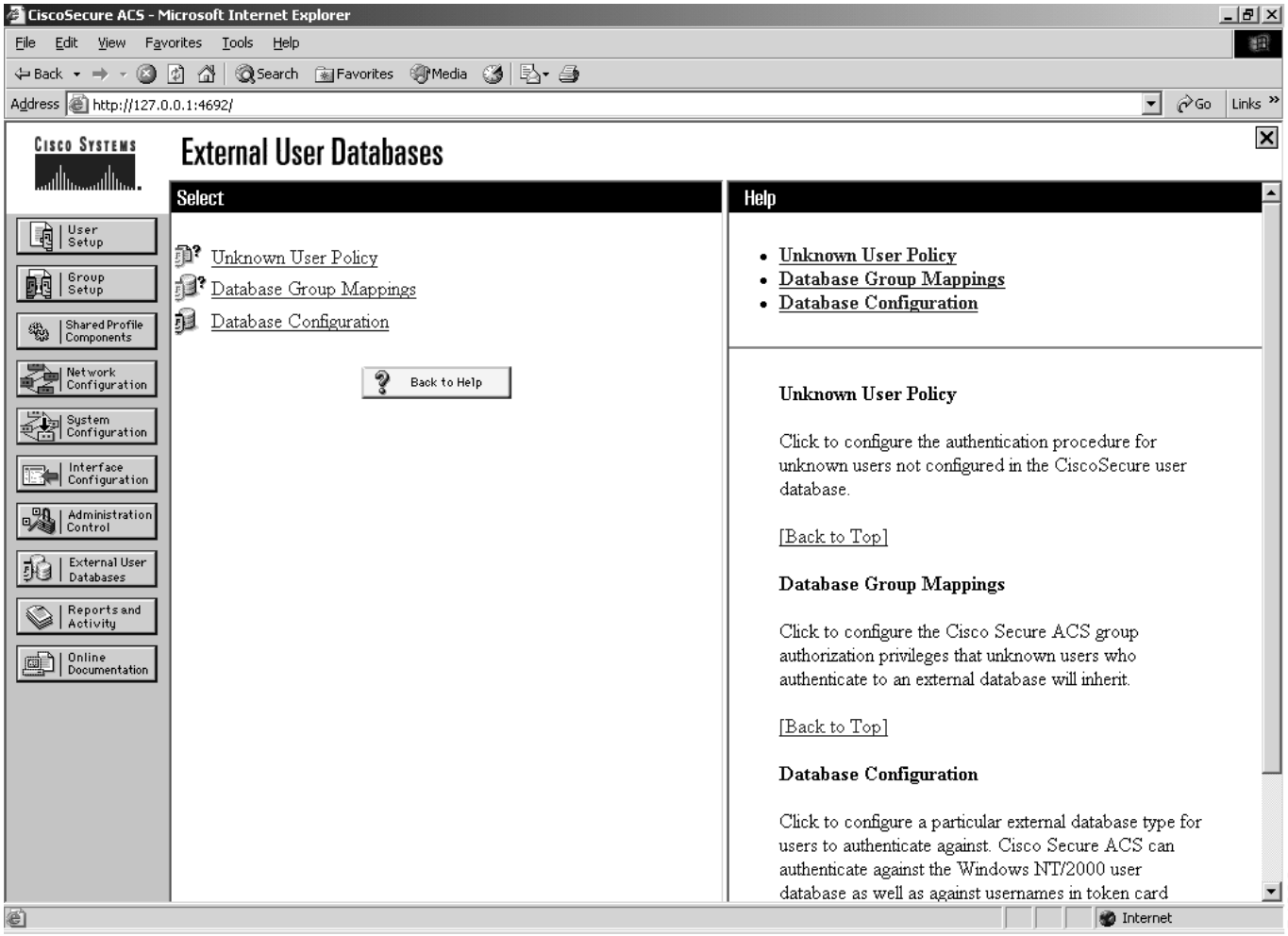
Integrating With Microsoft Active Directory

Integration with Microsoft Active Directory is simple. The CiscoSecure ACS server can be configured to reference outside user information stores if a corresponding value is not found in the internal, integrated user database. To enable Active Directory Integration, the Windows domain service must be selected as a fallback for unknown users.

To configure the external database, do the following:

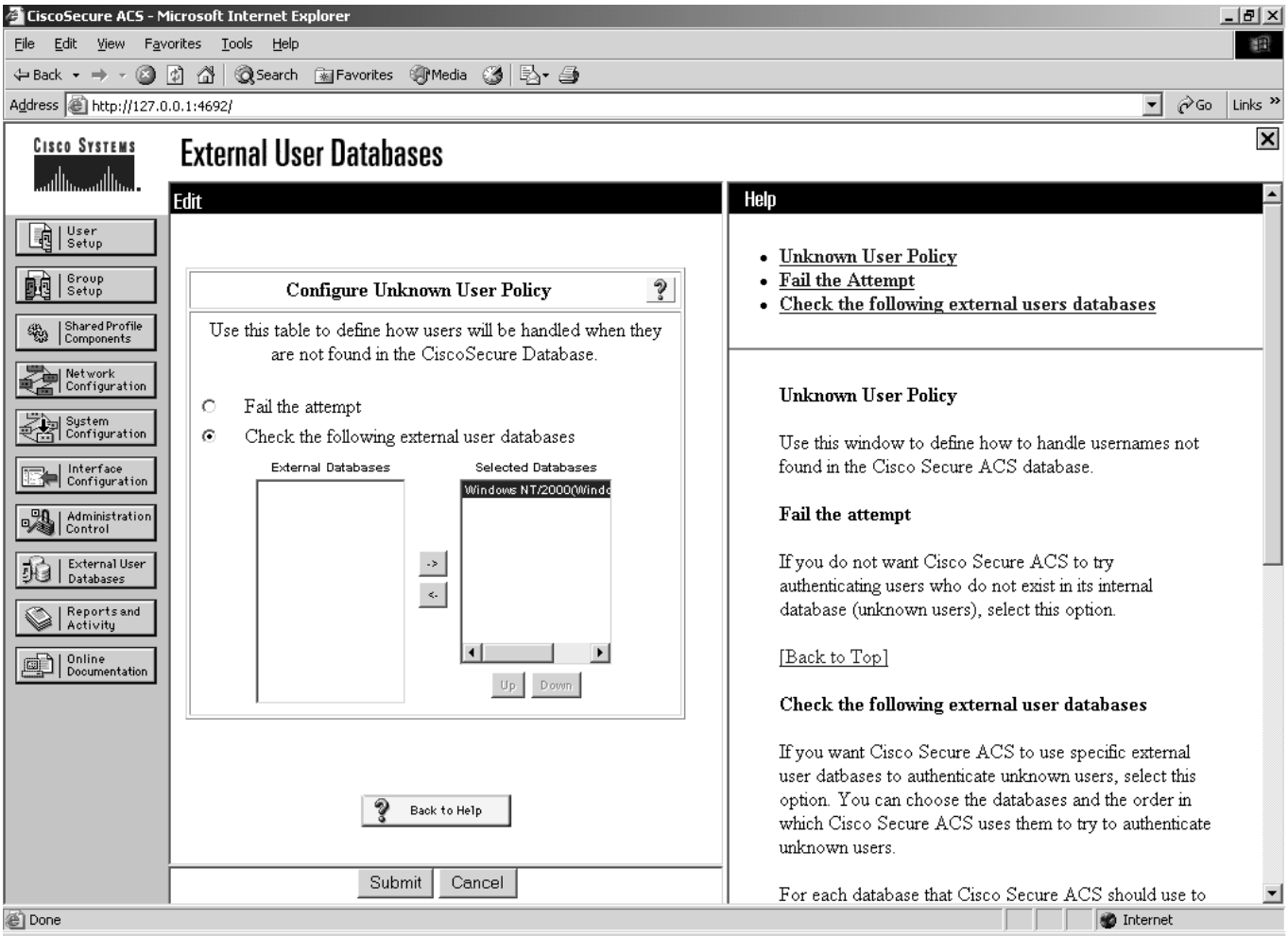
Step 1 Select **Unknown User Policies** in the External User Databases section (as shown in Figure 2-20).

Figure 2-20 External User Databases



Step 2 Select **Check the following external user databases** and double-click on the Windows NT/2000 database (as shown in Figure 2-21).

Figure 2-21 External User Databases (Unknown User Policy)



Step 3 Click on **Submit**.

Switch Configuration

Little configuration is needed on the switch to enable 802.1x port-based access control. The tasks that need to be completed can be summarized as follows:

Step 1 Enable RADIUS Support on the Switch

Step 2 Enable 802.1x Support on the Switch

Step 3 Configure Port-Level 802.1x Settings

Step 4 Configure the 802.1x Timers (Optional)

Enable RADIUS Support on the Switch

The 802.1x port-based authentication scheme relies on RADIUS for back-end communication between the authenticator (in this case, the switch) and the authentication server (the ACS). In addition to configuring the ACS for RADIUS communications to the switch (described in "Configure RADIUS Communications to the Switch"), the switch must also be configured for RADIUS.

To configure RADIUS communications on a Catalyst switch using the Catalyst OS, use the following commands:

set radius server *ACS_ IP_ address* **auth-port 1812** [**primary**]	Specifies the IP address of the RADIUS server. Multiple entries may be entered to provide redundant failover between RADIUS servers. The optional **primary** keyword indicates the preferred RADIUS server under normal conditions.
set radius key *RADIUS_key*	Sets the pre-shared secret RADIUS key used to hash and encrypt communications between the RADIUS server and the switch.

Enable 802.1x Support on the Switch

By default, 802.1x is disabled on Catalyst switches. To enable 802.1x support, use the following command:

set dot1x system-auth-control enable	Enables the 802.1x authentication control feature globally.

Configure Port-Level 802.1x Settings

Catalyst switches also allow the configuration of various 802.1x options on a per-port basis. These options include the ability to enable or disable port authentication, enable or disable periodic re-authentication, and enable or disable 802.1x multiple host mode.

Port authentication states and participation can be configured individually on a per port basis using the following commands:

set port dot1x 3/2 port-control auto	Sets port-control to auto. This requires an 802.1x login for that port.
set port dot1x *ports* **port-control force-authorized**	Sets the port-control state to force-authorized, which disables login requirements.
set port dot1x *ports* **multiple-host enable**	Allows for multiple hosts. By default only one host is allowed per port.
set port dot1x *ports* **re-authentication enable**	Enables periodic re-authentication. By default re-authentication is disabled.

Configure the 802.1x Timers (Optional)

802.1x-associated timers can be configured to modify the behavior characteristics and interactions between the client, the switch, and the ACS. Examples of timers that can be set are as follows:

set dot1x quiet-period *value*	Sets the wait period between initial link detection and issuing a login request.
set dot1x tx-period *value*	Regulates the wait time between TX retries.
set dot1x supp-timeout *value*	Sets the timeout period in waiting for client communications.
set dot1x server-timeout *value*	Sets the timeout period on communications with the ACS server.
set dot1x max-req *value*	Sets the number of retries issued of login requests to the client before the client if automatically failed.
set dot1x re-authperiod *value*	Sets the interval period between re-authentication for ports with re-authentication configured.

CHAPTER 3

Deploying EAP-MD5 Network Access Control

This chapter provides information and tips on deploying username- and password-authenticated 802.1x port-based access control using EAP-MD5 and the CiscoSecure ACS v3.0 in a wired environment of Cisco Catalyst switches.

Note This chapter uses Microsoft Windows XP as the supporting client operating system for example and illustration purposes. However, the concepts described should apply equally to any operating system that supports 802.1x.

Client Configuration

The client-side configuration required to support a network access control solution is fairly straight-forward. To configure the client side of the network access control, do the following:

Step 1 Verify Client-Side Operating System Support for 802.1x

Step 2 Enable 802.1x Authentication in the Operating System

Step 3 Select EAP-MD5 Authentication Facility for 802.1x

Note The operating system used in the examples in this chapter is Microsoft Windows XP Professional.

Verify Client-Side Operating System Support for 802.1x

For the client (supplicant) and the switch (authenticator) to communicate using 802.1x, the client-side operating system must support the IEEE 802.1x standard. The following popular operating systems are known to either have integrated or add-on support for the 802.1x protocol:

- Microsoft Windows XP Professional (Integrated)
- Microsoft Windows 2000 & 2000 Server (Microsoft add-on)
- Microsoft Windows NT 4.0 (Microsoft add-on)
- Microsoft Windows 98 & 98 SE (Microsoft add-on)

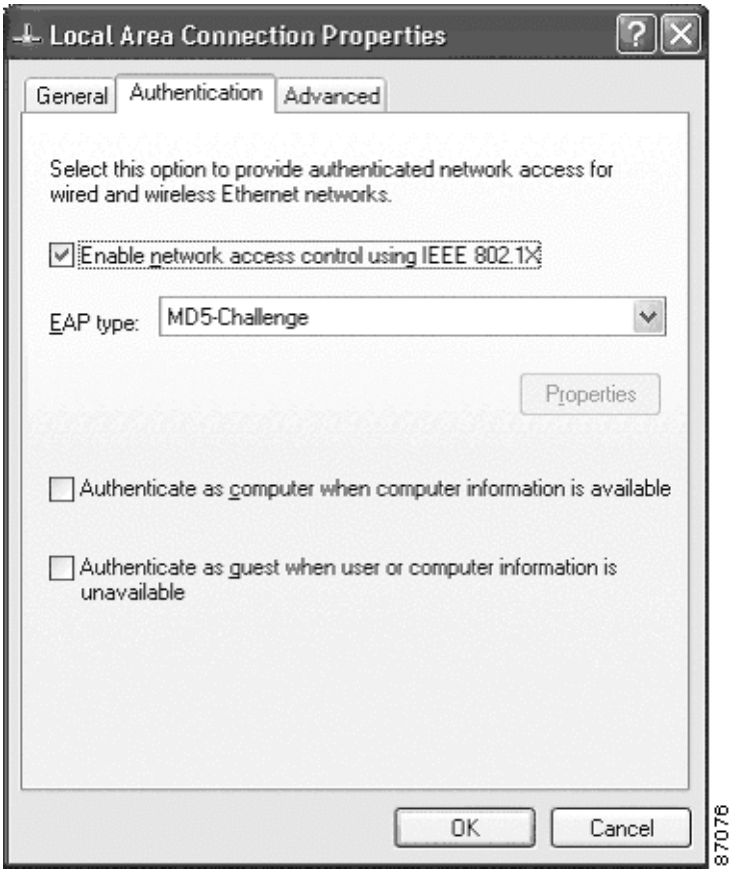
- Microsoft Windows 95 (3rd party add-on)
- Linux (Open Source add-on)
- Sun Solaris (Open Source add-on)

Support may be available for additional operating systems. If your system is not listed above, please contact your operating system vendor for support information.

Enable 802.1x Authentication in the Operating System

The client-side operating system may, by default, have 802.1x support disabled. Ensure that 802.1x capabilities have been enabled. In Microsoft Windows XP Professional, for example, 802.1x is enabled by selecting the checkbox found in the Authentication section of the Properties page (as shown in Figure 3-1).

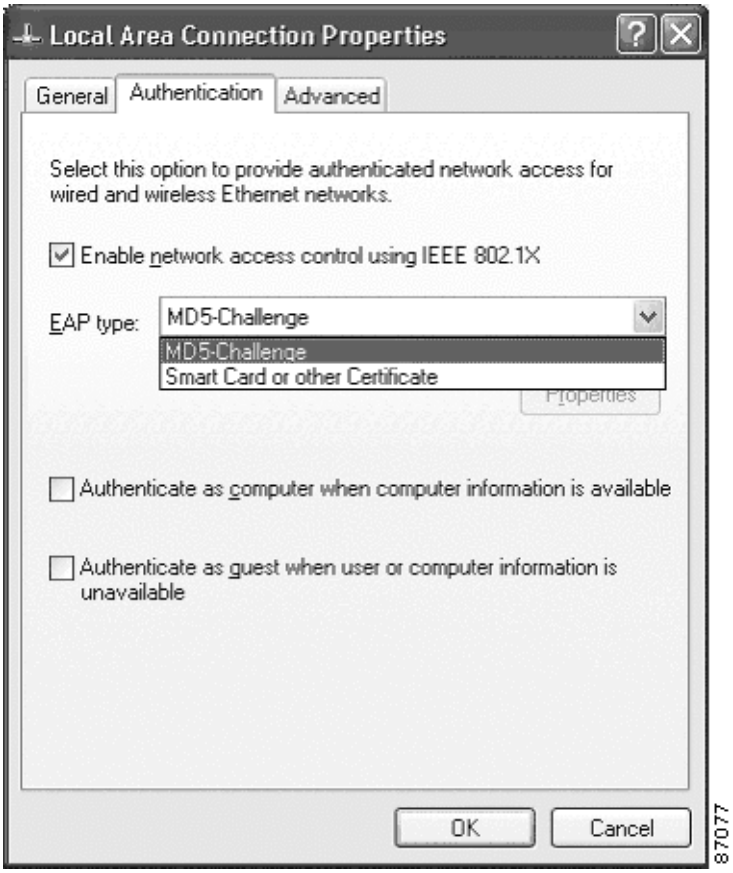
Figure 3-1 Enabling 802.1x in Microsoft Windows XP Professional



Select EAP-MD5 Authentication Facility for 802.1x

The 802.1x portion of the operating system's configuration may support more than one EAP authentication method. If this is the case, the EAP-MD5 Challenge compatibility mode must be selected from the options. In Microsoft Windows XP Professional, for example, the authentication mode is selected using the pull-down in the Authentication section of the Properties page (as shown in Figure 3-2).

Figure 3-2 Selecting the Authentication Mode in Microsoft Windows XP Professional



Note For the user to be prompted for their username and password when using EAP-MD5, the checkbox beside "Show icon in notification box when connected." located in the General section of the Properties page must be selected. If this option is not selected, the user will not be prompted for their credentials.

CiscoSecure ACS Configuration

To configure the CiscoSecure ACS, do the following:

Step 1 Install CiscoSecure v3.0 on a Microsoft Windows 2000 server.

Step 2 Configure RADIUS communications to the relevant switch.

Step 3 Create an account for the client-side user in the applicable user database.

Note Username and password deployments of network access control using the EAP-MD5 challenge/response method of authentication are not compatible with the use of external database sources within CiscoSecure ACS. The user must be created and exist in the internal CiscoSecure ACS database for this authentication method to work correctly.

Install CiscoSecure ACS V3.0 on a Microsoft Windows 2000 Server

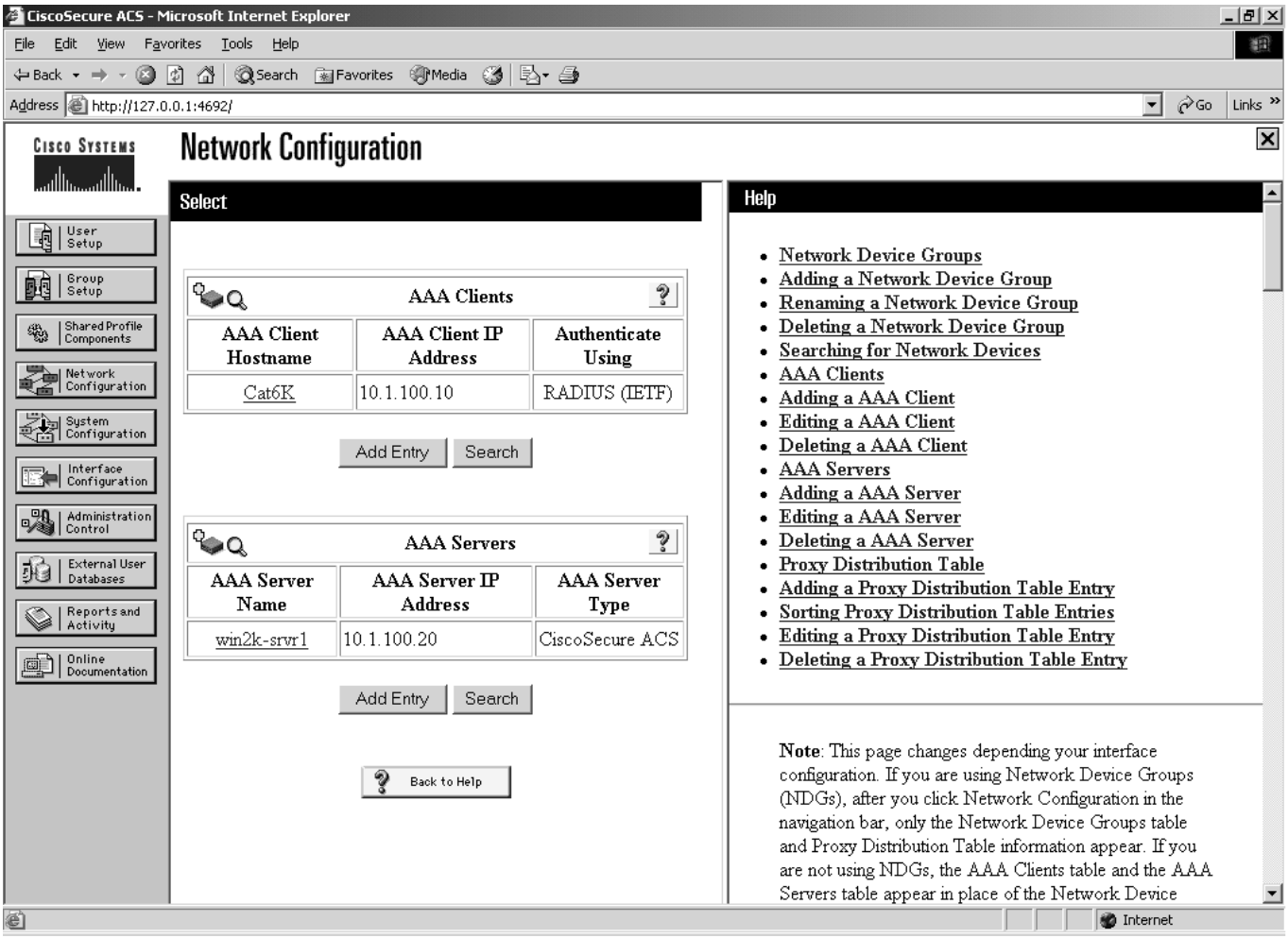
IEEE 802.1x EAP methods are supported in CiscoSecure ACS v3.0 and higher. This version of ACS is designed to be installed on a Microsoft Windows 2000 server. Please refer to the *Installation Guide* that accompanied your CiscoSecure ACS for detailed information on installation and basic configuration.

Configure RADIUS Communications to the Switch

For the CiscoSecure ACS to communicate with the switch (authenticator), RADIUS must be configured between the two. To configure RADIUS communications to the switch, do the following:

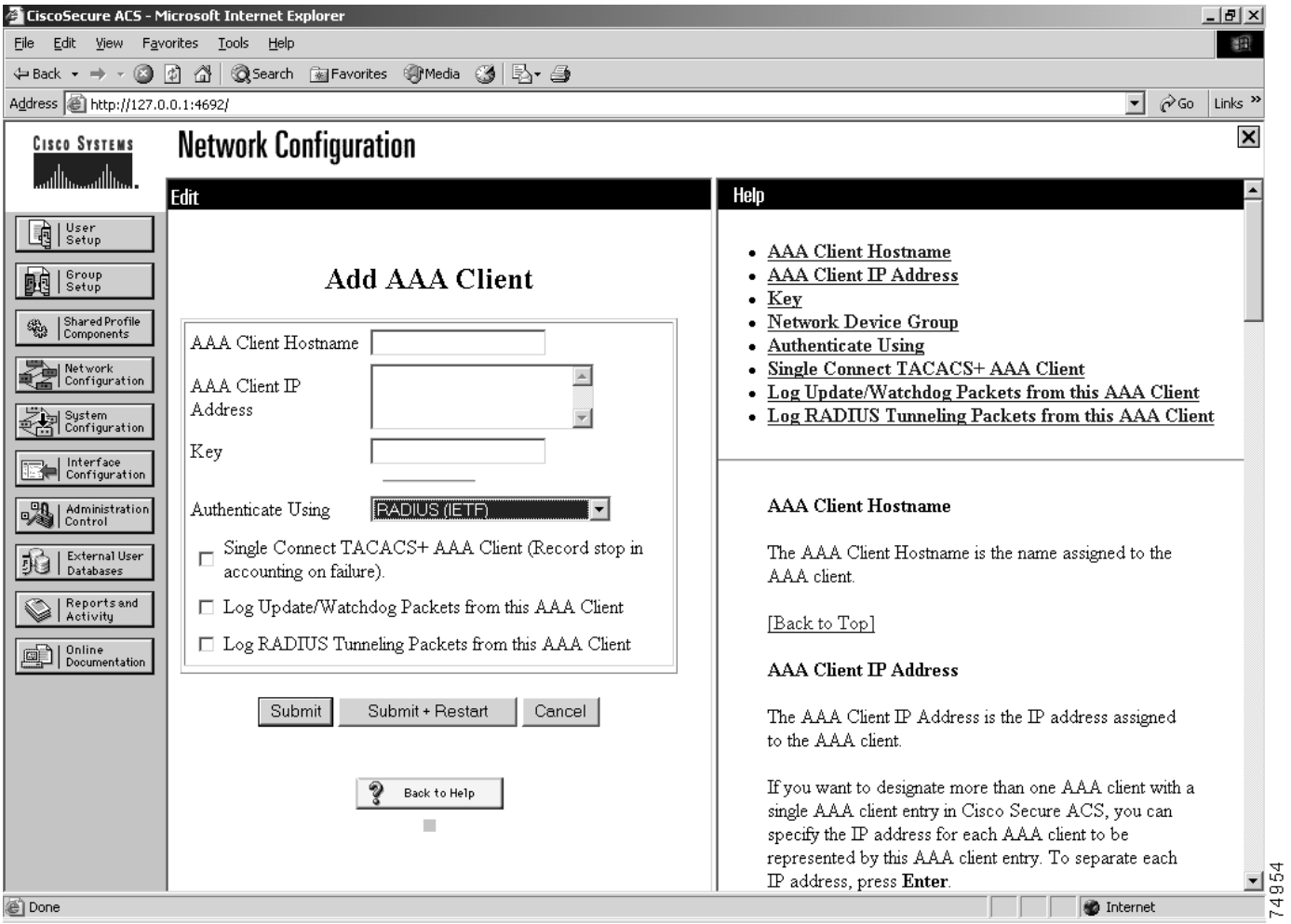
Step 1 On the Network Configuration page (Figure 3-3), click on **Add Entry** under the “AAA Servers” field.

Figure 3-3 Create NAS Entry Page of Network Configuration Page



Step 2 On the Add AAA Client page (Figure 3-4), specify the IP address, hostname, authentication type, and key.

Figure 3-4 Add AAA Client Page of Network Configuration Page



The fields of this page are explained in Table 3-1.

Table 3-1 CiscoSecure ACS Network Configuration Fields

Field	Description
AAA Client Hostname	The common name used to describe this particular AAA client.
AAA Client IP Address	The IP of the switch's administrative interface.
Key	The shared secret key used to encrypt communications between the AAA Client and the ACS server.
Authenticate Using	The choice of authentication protocol to use. Different versions of TACACS and RADIUS can be selected. The choice of RADIUS type will affect the formatting of the RADIUS packets. The suggested choice is “RADIUS (IETF)”.

Step 3 Click on **Submit**.

Once RADIUS communication has been configured on both the switch and the CiscoSecure ACS, it can be tested by enabling AAA login on the switch. The same username and password combination should be able to login to the CLI interface using AAA and the RADIUS parameters configured.

Create a Client Account in the ACS User Database

For the client to be able to authenticate using EAP-MD5 and 802.1x, an account must exist for that user in the internal ACS user database. The network administrator must create an account in the user database and maintain it within ACS.

Note There is currently no integration of EAP-MD5 with external user databases. Because of the current state of implementation of MD5 authentication in the Windows operating systems, it is not possible to perform EAP-MD5 authentication using CiscoSecure ACS against a Microsoft Windows Domain or Active Directory user store. Microsoft has currently chosen to maintain a closed API to the MD5 system calls, which does not allow for ACS to Domain/Active Directory authentication. Those wishing to use a Microsoft user store for authentication must use the Microsoft Internet Authentication Server (IAS) service. If you use the MS-IAS service, be aware that Cisco extensions to 802.1x, namely the dynamic policy enforcement features, are unsupported outside of CiscoSecure ACS as the authentication server.

Switch Configuration

Little configuration is needed on the switch to enable 802.1x port-based access control. The tasks that need to be completed can be summarized as follows:

Step 1 Enable RADIUS Support on the Switch

Step 2 Enable 802.1x Support on the Switch

Step 3 Configure Port-Level 802.1x Settings

Step 4 Configure the 802.1x Timers (Optional)

Enable RADIUS Support on the Switch

The 802.1x port-based authentication scheme relies on RADIUS for back-end communication between the authenticator (in this case, the switch) and the authentication server (the ACS). In addition to configuring the ACS for RADIUS communications to the switch (described in "Configure RADIUS Communications to the Switch") the switch must also be configured for RADIUS.

To configure RADIUS communications on a Catalyst switch using the Catalyst OS, use the following commands:

set radius server *ACS_ IP_ address* **auth-port 1812** [**primary**]	Specifies the IP address of the RADIUS server. Multiple entries may be entered to provide redundant failover between RADIUS servers. The optional **primary** keyword indicates the preferred RADIUS server under normal conditions.
set radius key *RADIUS_key*	Sets the pre-shared secret RADIUS key used to hash and encrypt communications between the RADIUS server and the switch.

Enable 802.1x Support on the Switch

By default, 802.1x is disabled on Catalyst switches. To enable 802.1x support, use the following command:

set dot1x system-auth-control enable	Enables the 802.1x authentication control feature globally.

Configure Port-Level 802.1x Settings

Catalyst switches also allow the configuration of various 802.1x options on a per-port basis. These options include the ability to enable or disable port authentication, enable or disable periodic re-authentication, and enable or disable 802.1x multiple host mode.

Port authentication states and participation can be configured individually on a per port basis using the following commands:

set port dot1x 3/2 port-control auto	Sets port-control to auto. This requires an 802.1x login for that port.
set port dot1x *ports* **port-control force-authorized**	Sets the port-control state to force-authorized, which disables login requirements.
set port dot1x *ports* **multiple-host enable**	Allows for multiple hosts. By default only one host is allowed per port.
set port dot1x *ports* **re-authentication enable**	Enables periodic re-authentication. By default re-authentication is disabled.

Configure the 802.1x Timers (Optional)

802.1x-associated timers can be configured to modify the behavior characteristics and interactions between the client, the switch, and the ACS. Examples of timers that can be set are as follows:

set dot1x quiet-period *value*	Sets the wait period between initial link detection and issuing a login request.
set dot1x tx-period *value*	Regulates the wait time between TX retries.
set dot1x supp-timeout *value*	Sets the timeout period in waiting for client communications.
set dot1x server-timeout *value*	Sets the timeout period on communications with the ACS server.
set dot1x max-req *value*	Sets the number of retries issued of login requests to the client before the client if automatically failed.
set dot1x re-authperiod *value*	Sets the interval period between re-authentication for ports with re-authentication configured.

Configuring Identity-Based 802.1x Dynamically Assigned VLANs for Catalyst Switches

Part of Cisco's Network Access Control and Policy Enforcement solution strategy is to provide the network administrator the flexibility of enforcing policies or access profiles at the network based on a network client's authenticated identity. The first phase of this to use a Cisco end-to-end, identity-configured network that dynamically assigns a VLAN to a connecting client.

By dynamically assigning port-based VLAN values to connecting clients based on the clients' authenticated identity, the network can group users by administrative policy. This allows group policy profiles to be carried down to the networking level. For example, different groups can be assigned different security access permissions based on duties, roles, and security risk level. For example, "Group A" could be allowed unrestricted access, while the users in "Group B" are limited to accessing only public resources and servers that maintain non-confidential information. The ability to limit access by risk criteria or levels allows a network administrator to minimize overall security exposure and risk.

Using VLANS to group users makes it possible to control access by identity and group policies. The same holds true for group-specific quality of service (QoS). For example, users in "Group 1" could have unrestricted access to bandwidth, while users in "Group 2" are rate limited via QoS to an FTP maximum of 8 Mbps. This allows network administrators to perform resource allocation and control on a group-by-group basis.

Note This ability is based on the IEEE 802.1x recommendations for the use of RADIUS attributes with 802.1x.

This chapter provides the basic technical configuration guidance needed to enable identity-based, dynamically-assigned VLANs on Catalyst switches that support this feature.

Prerequisites

To be able to apply the design outlined in this chapter, the following are required:

- A Catalyst 6000, 6500, 4000, or 4500 platform switch must be used.
- Catalyst OS 7.2(2) or greater must be running on the switch.

Note Only Catalyst OS 7.2(2) or greater running on a Catalyst 6000, 6500, 4000, or 4500 platform supports dynamic identity-based VLAN assignment. Prior versions and other platforms are not currently supported at this time.

- Basic 802.1x port-level authentication must be properly configured, tested, and working. Only then should identity based policy enforcement features, such as dynamic VLAN assignment, be configured.

Note The information in this chapter is in addition to any base identity 802.1x configuration performed to enable basic port-level authentication to a Catalyst switch. Identity-based dynamic VLAN assignment will work with all configurable authentication types (EAP-TLS, EAP-MD5, PEAP/EAP-GTC, PEAP/MS-CHAPv2, etc.) used for 802.1x authentication.

The ability to dynamically assign a VLAN to a network client based on its identity requires the proper authentication of that client. For information on the configuration and deployment of basic 802.1x authentication, please refer to:

- Chapter 2, "Deploying EAP-TLS Network Access Control" for information on configuring and deploying 802.1x based port-level authentication using EAP-TLS for PKI x.509 v3 certificate based login.
- Chapter 3, "Deploying EAP-MD5 Network Access Control" for information on configuring and deploying 802.1x based port-level authentication using EAP-MD5 for username/password based login.

Operational Overview

The dynamic policy features, including dynamic identity-based VLAN assignment, leverage RADIUS attributes to convey identity-specific policy information from the authentication (RADIUS) server to the authenticator (Catalyst switch, wireless AP, etc.). RADIUS standard attributes (RFC 2868) or Vendor Specific Attributes (VSAs) are used to indicate the policy points. The first of these policy points to be implemented by Cisco is the fact that the VLAN is associated with a particular identity. This is transmitted from the authentication server to the authenticator using the RADIUS attributes as outlined in IEEE 802.1x specification recommendations. Table 4-1 lists the RADIUS attributes used for dynamic identity-based assignment.

Table 4-1 RADIUS Attributes for Dynamic, Identity-based Assignments

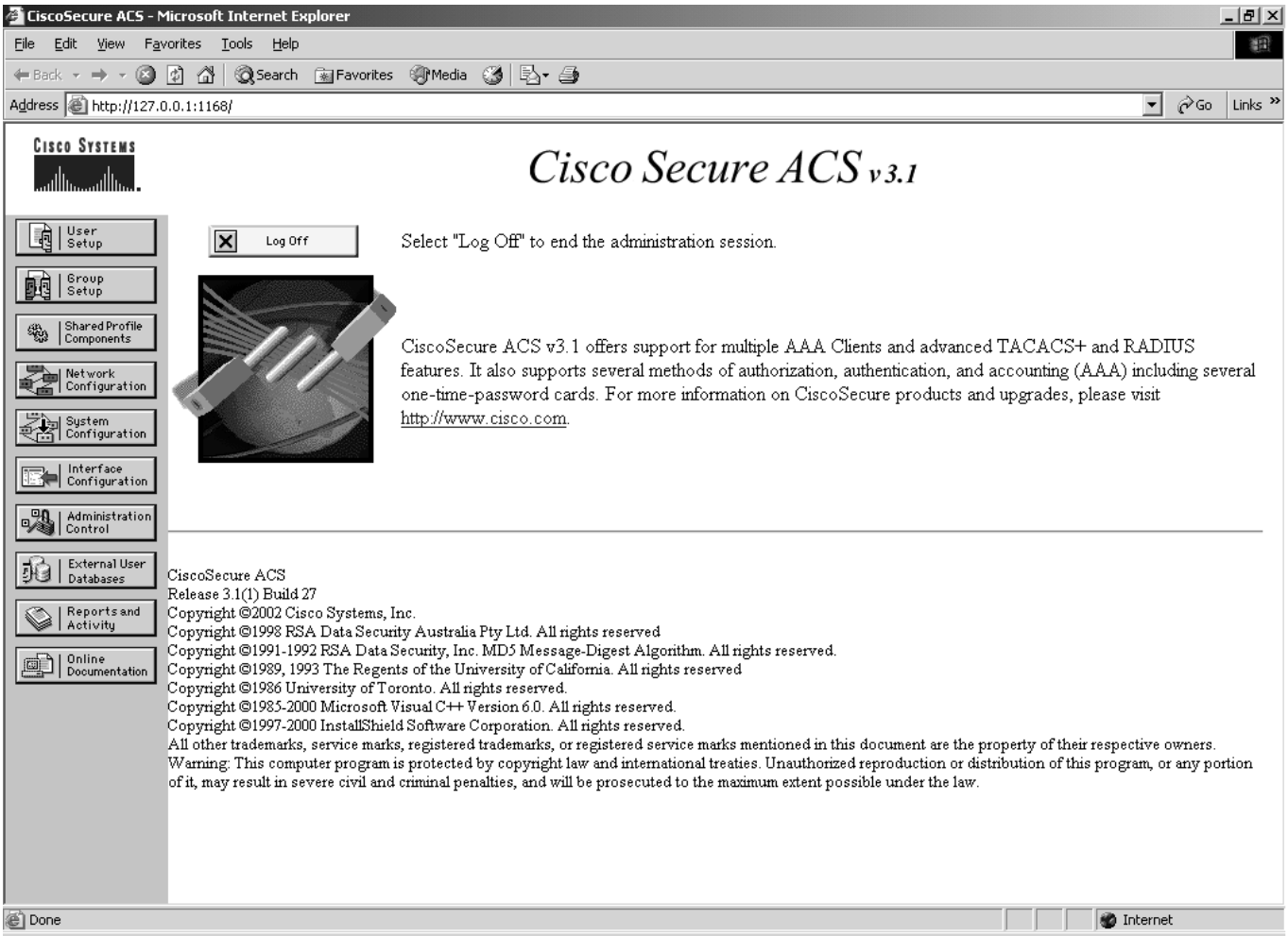
Attribute ID No.	Attribute Name	Attribute Values	Description
[064]	Tunnel-Type	Integer: VLAN (13)	Indicates the tunneling type parameter to be set by this RADIUS attribute. In this case, the value is "VLAN" (13).
[065]	Tunnel-Medium-Type	Integer: 802	Indicates the link-layer topology to which the Tunnel-Type is being applied. For LAN technologies (Ethernet, Token Ring, Wireless 802.11b, etc.), the value should be "802."
[081]	Tunnel-Private-Group-ID	Text String	The string used to indicate the specific tunnel (in this case VLAN) to be associated with the authenticated client. This field is a free-form text string which will be matched against the names of configured VLANs on the Catalyst switch.

RADIUS Server Configuration

Once all the prerequisites are met, the only configuration necessary to enable the dynamic assignment of VLANs to an authenticated identity is that of the RADIUS server. With CiscoSecure ACS, the necessary RADIUS attributes are not displayed in the configuration user interface. They must be selected and added to the group and user profile configurations. To complete the configuration of the RADIUS server, do the following:

Step 1 On the CiscoSecure ACS main window (Figure 4-1), select **Interface Configuration**.

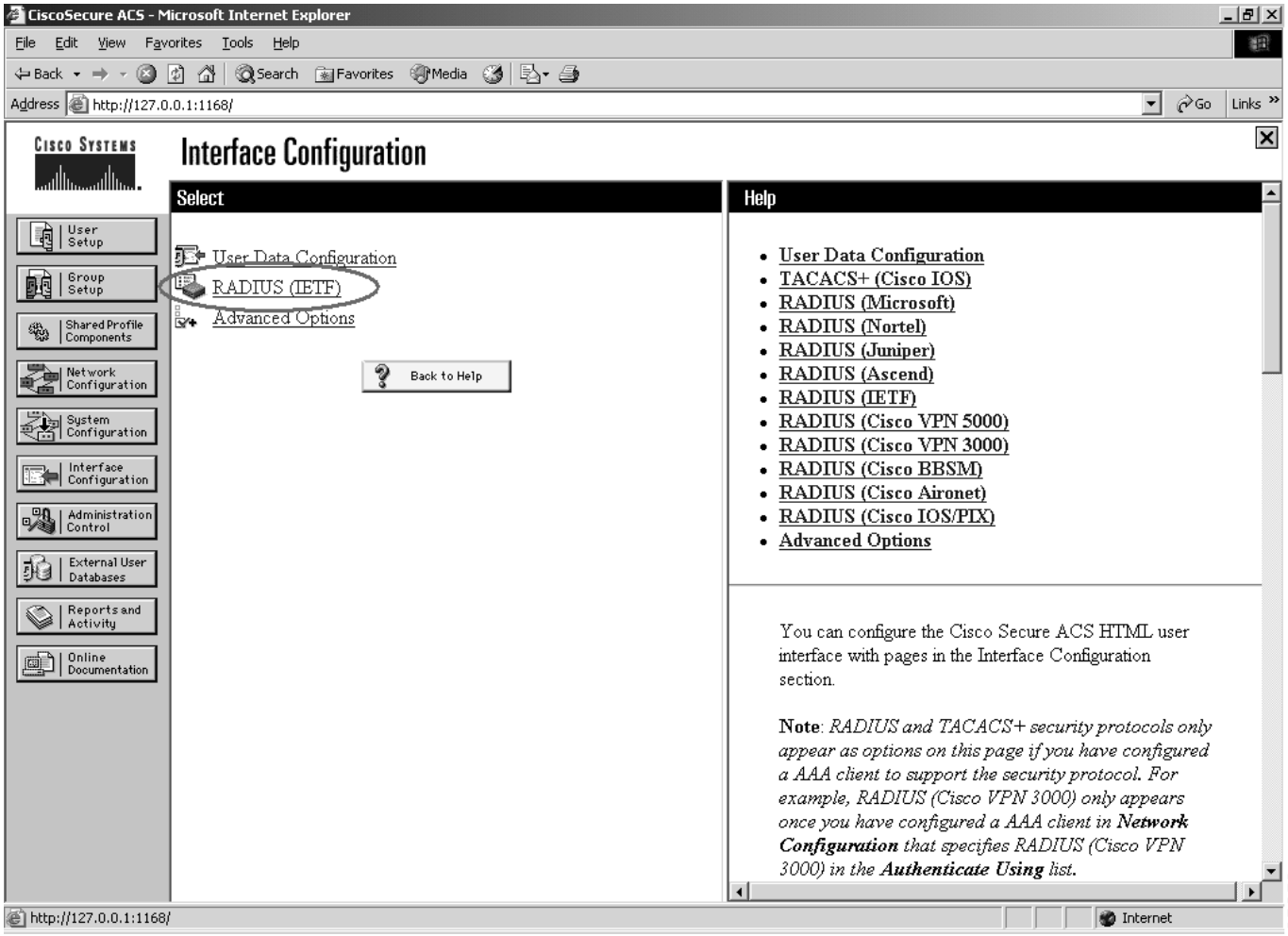
Figure 4-1 ACS Main Menu Interface Configuration Option



The Interface Configuration window (shown in Figure 4-2) is displayed. This window allows the administrator to enable specific RADIUS attributes to be visible and configurable at a group level, user level, or both.

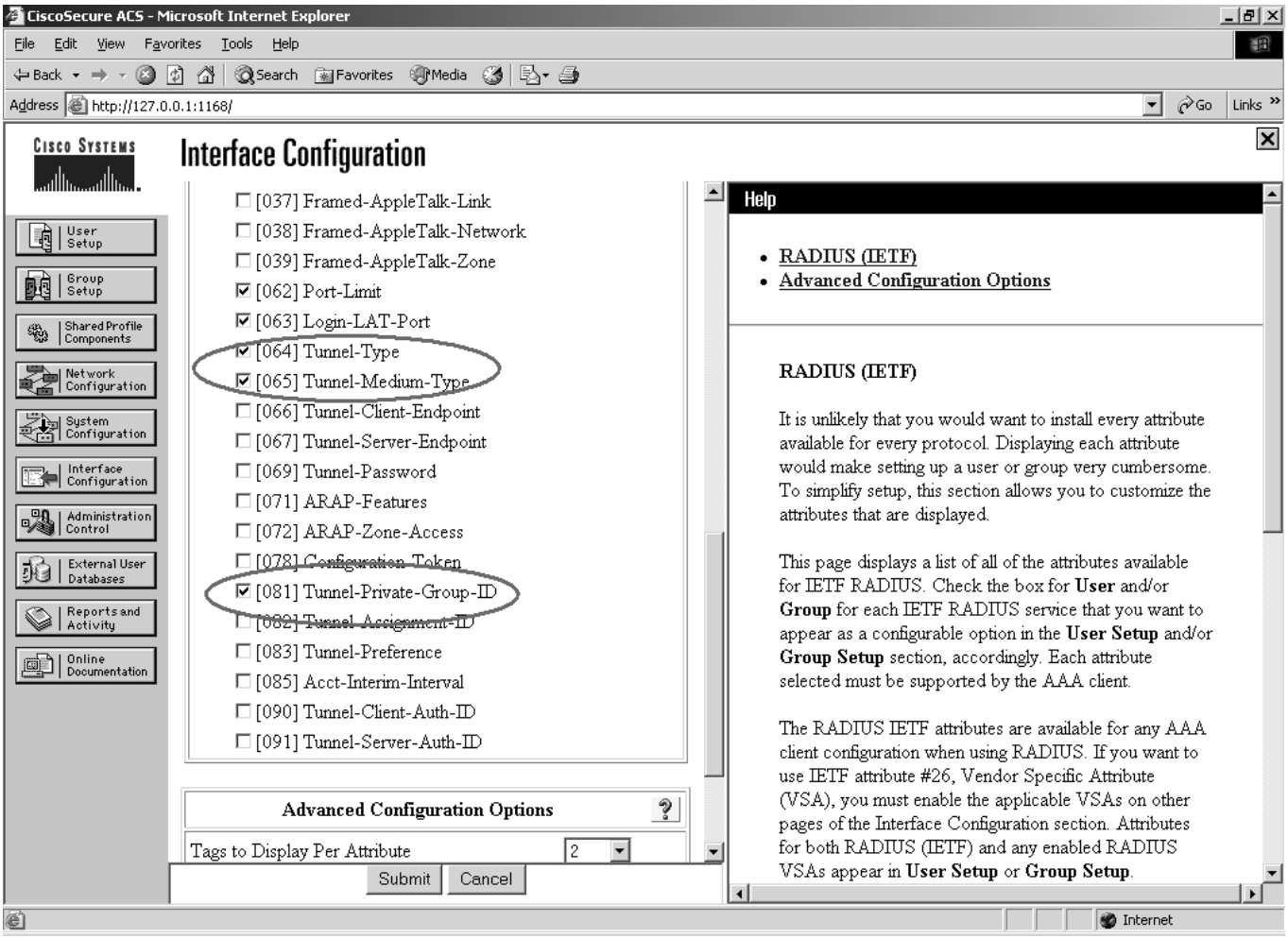
Step 2 Select **Radius (IETF)**. Because the attributes used for dynamic identity-based VLAN assignment are RFC standard attributes, they are listed under the IETF RADIUS attribute configuration option.

Figure 4-2 RADIUS (IETF) Attribute Configuration Option



Step 3 Select the appropriate RADIUS attributes. By default, most of the RADIUS attributes shown in Figure 4-3 are selected automatically upon installation of the ACS. However, the attributes for dynamic identity-based VLAN assignment are not among those selected and must be added. These attributes are the same as those previously listed in Table 4-1 and are shown in Figure 4-3.

Figure 4-3 Selecting RADIUS Attributes for Group Profile Configuration



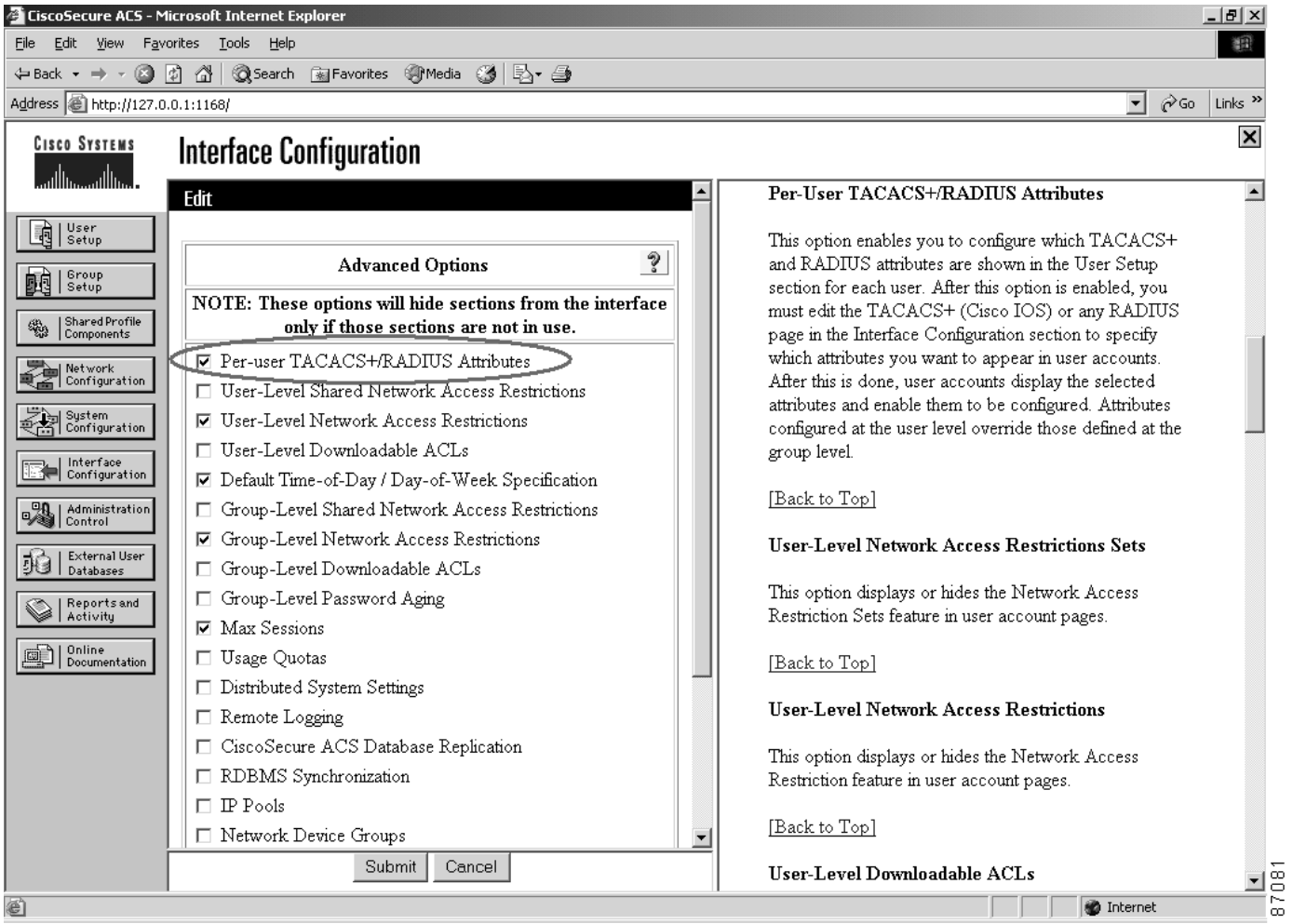
Once the appropriate RADIUS attributes have been selected in the RADIUS (IETF) user interface configuration section, those attributes will become available for configuration under group profiles.

Optionally, user-specific RADIUS attributes can be configured, which will override group-assigned values. To assign user-specific RADIUS attributes, do the following:

Step 1 On the Interface Configuration window, select **Advanced Options**.

The Advanced Options page is displayed (as shown in Figure 4-4). This page allows the administrator to enable per user attributes.

Figure 4-4 Per User Attributes Advanced Option



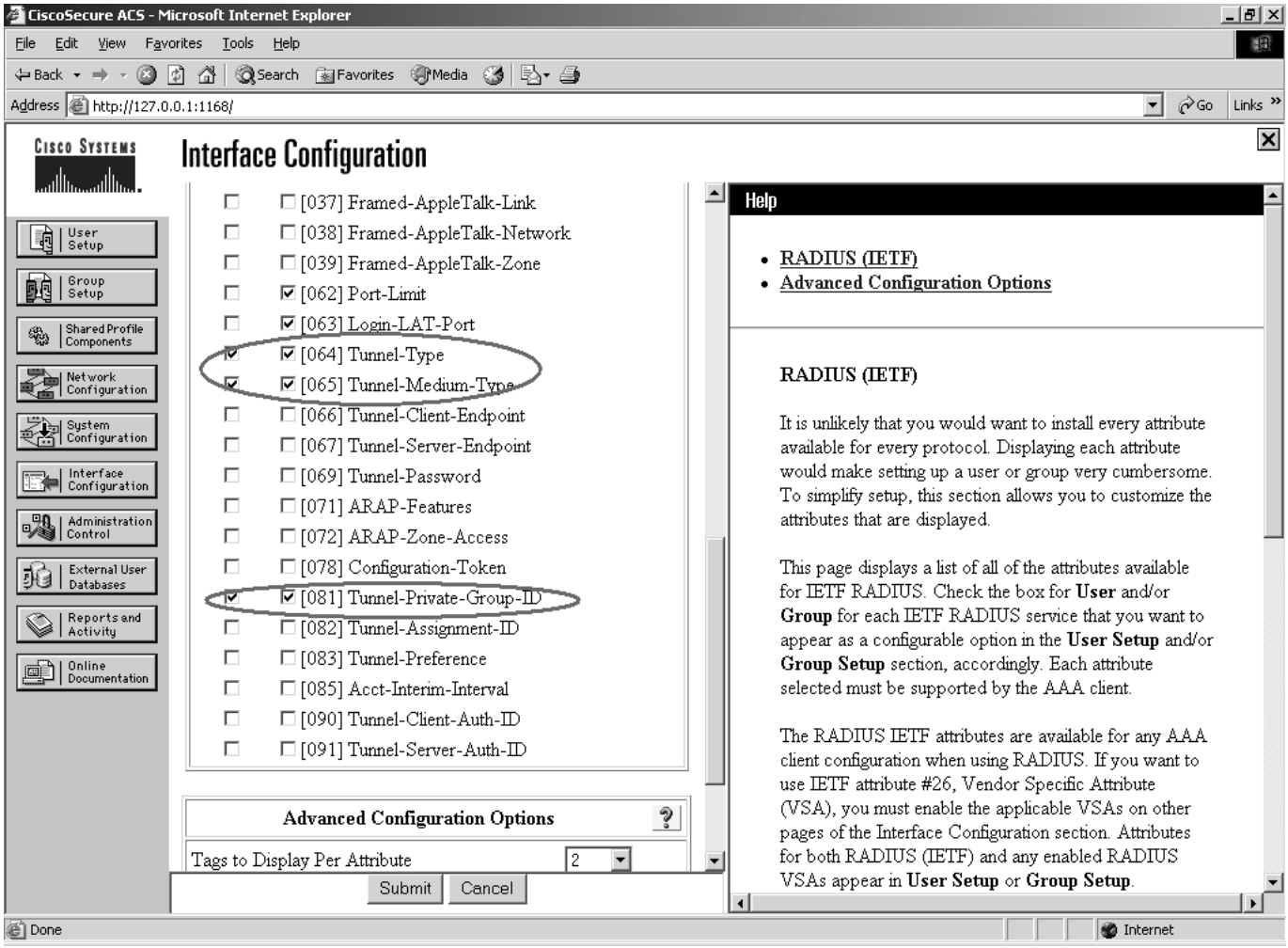
Step 2 Select the desired option and click on **Submit**.

Once per user attribute capabilities have been enabled, the RADIUS (IETF) portion of the Interface Configuration will change to reflect the ability to select the RADIUS attributes that can be applied to individual user profiles or accounts.

Note Per-user settings automatically override any values configured for the group profile to which a given user may belong.

Figure 4-5 illustrates the new column of selectable RADIUS attributes for per user application.

Figure 4-5 Per User RADIUS Attributes Now Selectable



Once the proper RADIUS attributes have been made available for configuration, the corresponding parameters for groups or individual users must be set.

Configuring Group & User VLAN Policies

VLAN assignment policies can be configured on a per group basis, a per user basis, or both. If both are applied to a particular user, the user-specific policies will override any policies imposed as the result of a group membership. For example, if user A is a member of Group 1 and does not have any user-specific attributes or policies set, then user A will assume any configured policies of Group 1. If user A is a member of Group 1 but has specific policies assigned to their particular account by the network administrator, then those specific policies will be assumed. The values for any policies that are not specifically assigned to that user will be derived from Group 1.

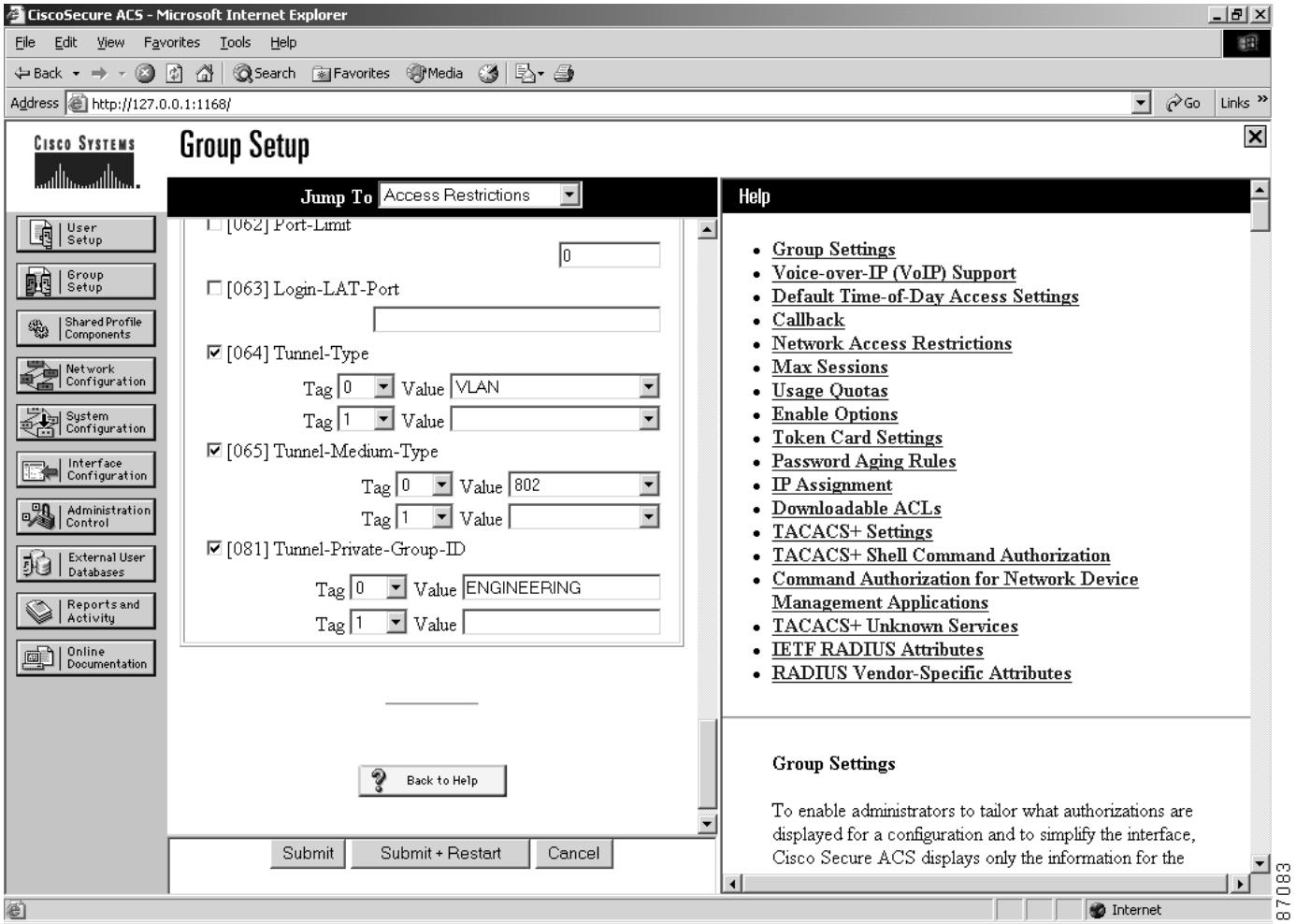
Group VLAN Policies

To configure VLAN assignment policies for a group of users, an administrator must enter the values in the group configuration portion of ACS as follows:

Step 1 On the CiscoSecure ACS main window, select **Group Setup**. The Group Setup page is displayed.

Step 2 Scroll down to the lower part of the page where the configurable "IETF RADIUS Attributes" are displayed (as shown in Figure 4-6) and set the values.

Figure 4-6 Group Setup—RADIUS Attribute Configuration for VLAN Assignment



The following values should be set for dynamic identity-based VLAN assignment.

- *Tunnel-Type* (64) is set to "VLAN."
- *Tunnel-Medium-Type* (65) is set to "802."
- *Tunnel-Private-Group-ID* (81) is set to the name of the VLAN to be assigned to this user group.

The VLAN name used should match the name of a VLAN configured on the access-layer switches to which this user group will have access. If the configuration of the VLAN name is consistent across multiple access switches, then the user will have the ability to maintain mobility between those switches while having their profile for VLAN assignment follow them. If the VLAN to which the user is assigned is not available on the switch, the authentication process will fail and connectivity will be denied.

Note *Tag* is for grouping attributes together in cases in which multiple attributes of the same class are sent back to the authenticator. This feature is not currently used, but will be employed in the future. For now, all the tags for selected attributes much match. In this example, all attribute tags are set to "1." The number of attribute tag sets displayed for configuration is also configurable. This parameter is set in the RADIUS(IETF) portion of the Interface Configuration. (See Figure 4-3.)

Note In the examples in this document, VLAN identification has been by the VLAN logical configured name and not the VLAN ID number. Using the VLAN name instead of the VLAN ID number allows for flexibility in VLAN topological configurations. By implementing dynamic VLANs with name-based identifiers, the administrator can think in terms of logical client group membership and policy assignment rather than having to focus on the Layer 2 or VLAN topology.

For example, by assigning a dynamic VLAN to a client using the network group name, a Layer 2 topology of distributed, diverse, Layer 2 domains separated by Layer 3 can easily be accommodated. In such a case, a given VLAN (such as VLAN 100) does not need to span across the campus network. The VLAN name assigned could remain consistent, yet the VLAN ID mapping to that name would only be locally relevant within a Layer 2 domain. In a topology such as this, it is entirely possible and workable to have a VLAN name "Group A" available as VLAN ID 100 in one of the Layer 2 domains, while "Group A" is represented in a different Layer 2 domain by either the same (VLAN 100) or different (such as VLAN 300) ID.

Using the VLAN name as the identifying factor for assignment also allows support for traditional large Layer 2 domains in which VLANs may span across a campus network.

Step 3 Click on **Submit**.

User-Specific Policies

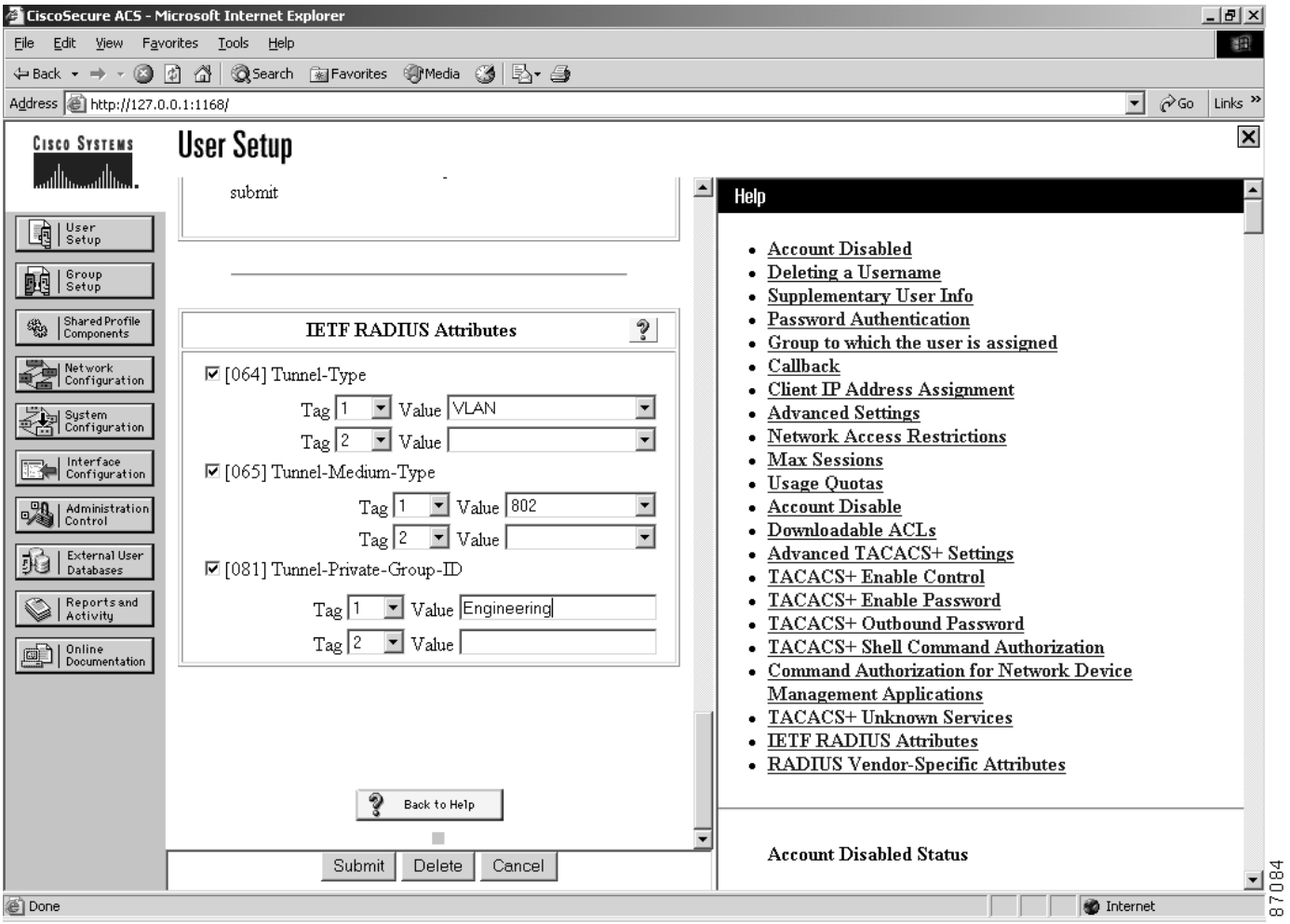
If a user is part of a group, but the administrator would like to override portions of their particular VLAN assignment policy, specific VLAN policy attribute values can be assigned to that user's profile and account.

To do assign user-specific policies, do the following:

Step 1 On the CiscoSecure ACS main window, select **User Setup**. The User Setup page is displayed.

Step 2 Scroll down to the lower part of the page where the configurable "IETF RADIUS Attributes" are displayed (as shown in Figure 4-7) and set the values.

Figure 4-7 User-Specific VLAN Assignment Policy Attributes



As with the group Policies, the following values should be set for dynamic identity-based VLAN assignment.

- *Tunnel-Type* (64) is set to "VLAN."
- *Tunnel-Medium-Type* (65) is set to "802."
- *Tunnel-Private-Group-ID* (81) is set to the name of the VLAN to be assigned to this user group.

Step 3 Click on **Submit**.

Enforcing Group Policies Using VLANs

The main benefit to dynamically assigning VLANs based on authenticated identity is the ability to apply group security and access policies. Currently, two types of access and resource control are recommended for configuration.

- Access security control using address assignment by subnet, traditional ACLs, and firewalls.
- Resource usage in the form of QoS configuration on a per VLAN basis.

VLAN-Based Group Access Control Configuration

Once network clients have authenticated and have been assigned to a VLAN based on their authenticated identity, the challenge becomes maintaining a separation of the traffic between client groups. This can be accomplished using ACLs and firewalls.

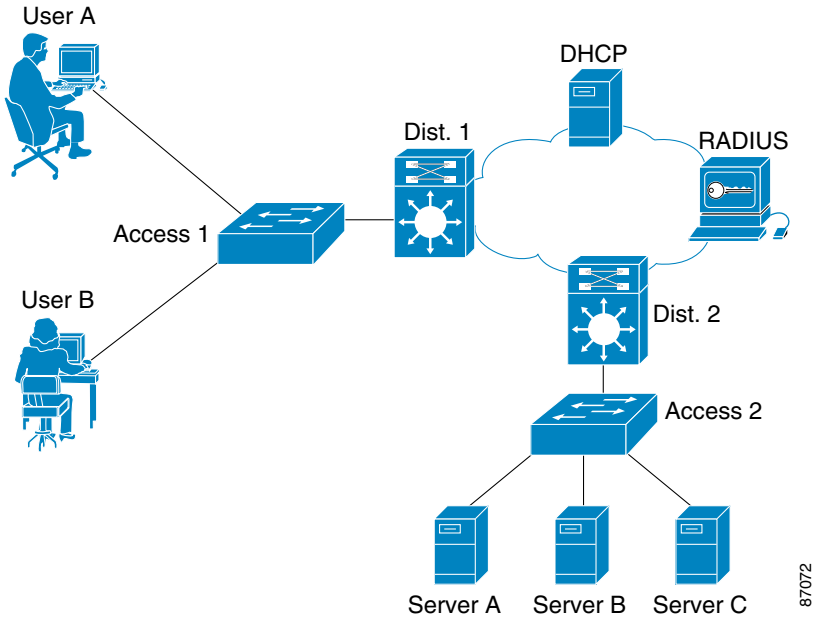
Note For the sake of simplifying the network compartmentalization configuration, redundancy for high-availability (HA) in the network has been omitted in the examples in this section. However, all of the examples can be deployed in high-availability configurations that conform to the Cisco recommended HA network designs. When deploying network compartmentalization and dynamic VLAN assignments in an HA environment, it is critical to ensure the consistency of rules and configurations across redundant points in the network.

Figure 4-8 depicts an example network in which two users are each dynamically assigned working VLANs based on their authenticated identities. In this example, the users' directly connecting access switch is a Cisco Catalyst 6500 series switch with a Supervisor II and PFC II. No MSFC is installed. The users' distribution switch is a Catalyst 6500 series switch with a Supervisor II and MSFC II installed. Similarly, the data center aggregation and front-end switches that provide access to application servers A, B, and C are also Catalyst 6500 series switches, with and without MSFCs, respectively.

In this example, the configuration enforces the following administrative network policies:

- User A should be able to access Server A and Server C.
- User B should be able to access Server B and Server C.
- All systems should be able to contact the DHCP server.
- All servers should be able to access each of the other servers.
- No other direct communications patterns should be allowed by the network.

Figure 4-8 VLAN-Based Group Access Control Example



Conforming to the network design requirements can be accomplished in a number of ways using ACLs or firewalls. The first example uses ACLs and VLANs only. This example can apply equally to other Cisco router and switch platforms that support VLANs and ACLs. The second example uses a combination of ACLs and firewalls to supplement the minimal protection afforded by ACLs alone. To be effective, the firewall must be inserted in the traffic path.

Common Configuration

In both examples, the following is true:

- Both users must authenticate to the network using 802.1x. The authentication method may be either EAP-TLS or EAP-MD5. Upon successful authentication, VLANs associated with each user will be assigned to the client's connected access port. For User A, this will be VLAN 100. For User B, the assigned VLAN will be VLAN 200.
- The distribution switch is configured to perform as a DHCP relay to forward DHCP packets between the clients and the DHCP server in the enterprise network. The VLAN assignment of each respective client will automatically dictate the DHCP address scope each is assigned. This is determined using the “gipaddr” (gateway IP address) field tagged onto DHCP packets from the default gateway's VLAN interfaces.
- Using DHCP and the DHCP relay process in the default gateway for each client, the following IP addressing will be assigned:
  - User A in VLAN 100 will obtain an address from the 10.1.100.0/24 subnet.
  - User B in VLAN 200 will obtain an address from the 10.1.200.0/24 subnet.
- Application server “Server A” resides in VLAN 301. Application server “Server B” resides in VLAN 302. And application server “Server C” resides in VLAN 303. The servers use static IP address assignments out of the 10.1.301.0/24, 10.1.302.0/24, and 10.1.303.0/24 subnets, respectively.
- The VLANs do not need to span the enterprise network. In these examples, they are separated by a Layer 3, routed IP core. The VLANs used have relevance only to their respective Layer 2 domain, or distribution level area.

Configuration Example using ACLs and VLANs

In this configuration example, ACLs and the configured VLANs are used to provide logical separation between user groups (compartmentalization). The process is as follows:

Step 1 User A (and other users with similar administrative policies associated with their accounts) will be dynamically configured into VLAN 100.

Step 2 Once User A has authenticated and has been assigned to VLAN 100, the client will proceed with the standard dynamic configuration procedure of requesting a DHCP address.

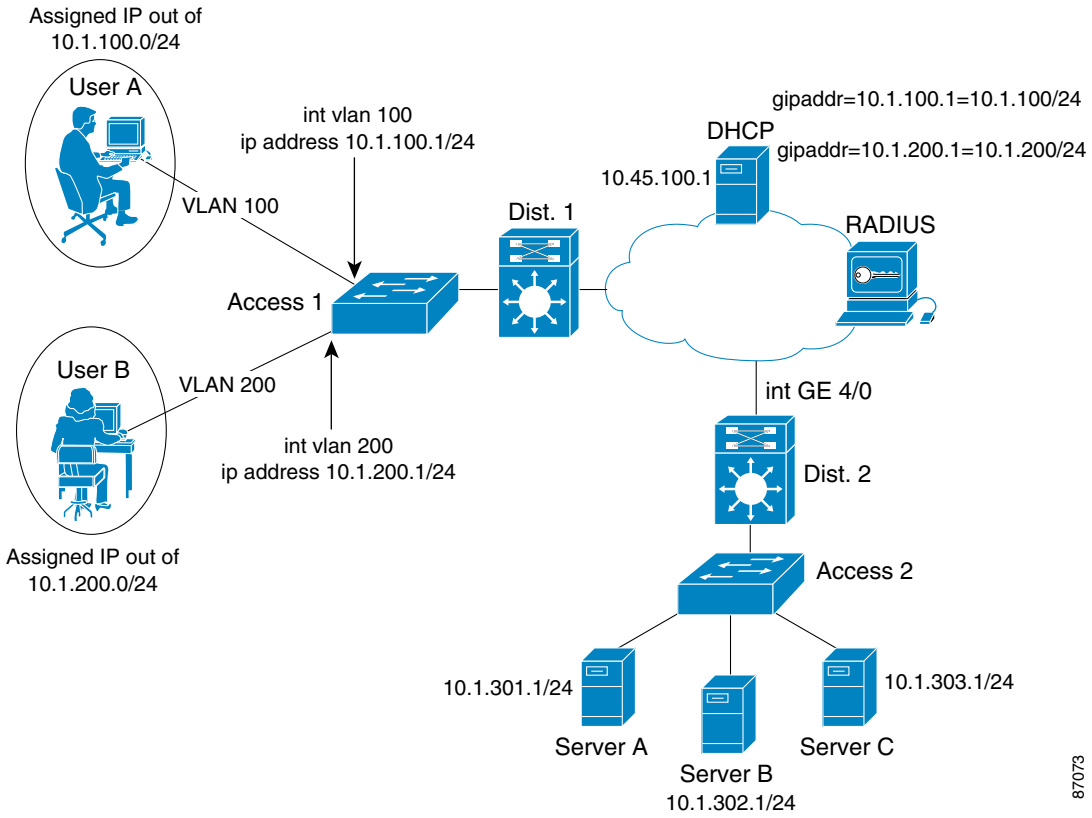
Step 3 The DHCP process will be relayed to the DHCP server via the Layer 2 domain's default gateway (in this case, the Distribution 1 multilayer switch).

Step 4 Upon relaying the DHCP packets, Distribution 1 will also insert the “gipaddr” field in those packets within the stream. This information includes the IP address sourced from the interface that received the client DHCP requests to be relayed, In this example, the interface is VLAN 100 in Distribution 1.

Step 5 Based on the "gipaddr" field, the DHCP server can make an intelligent decision as to which scope to apply to the relayed client request. In this example, Distribution 1 has interface VLAN 100 configured with the IP address of 10.1.100.1/24. Therefore, the DHCP server will allocate an address to the requesting client out of the configured scope for that "gipaddr" range, thereby sending back an address from the 10.1.100.0/24 range. Using the same mechanism across interface VLAN 200 of Distribution 1, User B will automatically be assigned an address out of the 10.1.200.0/24 range. This allows the initial Layer 2 separation to carry the compartmentalization of the network into the Layer 3 domain.

Now begin traffic patterns and groupings can be manipulated using Layer 3 features.

Figure 4-9 Configuration Example using ACLs and VLANs



To enforce the separation of the traffic, ACLs must be installed at the Layer 2-to-Layer 3 borders. In this example, ACLs must be installed on Distribution 1 and Distribution 2. The logic of the ACLs needed can be broken down by examining each rule carefully in the context of the IP subnets configured and available.

The best practice for managing ACLs in a secure manner is to permit only what is specifically allowed and deny all other traffic by default. To simplify the example, the level of granularity used with permit or deny statements is at the IP packet level. There will be no differentiation of protocols or ports.In practice, if a policy mandates more r granularity, ACLs with protocol and port specific information can be used in place of the simple, IP-only ACLs.

With this default deny policy in mind, the initial ACLs for the distribution switches are as follows:

Switch Name	Interface	ACL Logic
Distribution 1	int vlan 100	deny ip any any
	int vlan 200	deny ip any any
Distribution 2	int vlan 301	deny ip any any

The first rule that needs to be enforced is that all systems are allowed to access the DHCP server. This will be necessary for DHCP auto-configuration to work for attaching authenticated clients. The rules can be updated to reflect this as follows:

Switch	Interface	ACL Logic
Distribution 1	int vlan 100	permit udp any host 10.45.100.1 eq bootp deny ip any any
	int vlan 200	permit udp any host 10.45.100.1 eq bootp deny ip any any
Distribution 2	int vlan 301	deny ip any any

From the rules outlined earlier, it is clear that Server C is a common resource to both user groups. By assigning the VLAN and IP subnet to commonly available resources as a whole, future expansion of this class of resource is possible and simplified. In this example, Server C resides in the 10.1.303.0/24 subnet. Therefore, that subnet must be designated as the common resource subnet.

With that in mind, the ACL logic on both switches can be updated to reflect this as follows:

Switch Name	Interface	ACL Logic
Distribution 1	int vlan 100	permit ip 10.1.100.0 0.0.0.255 10.1.303.0 0.0.0.255 permit udp any host 10.45.100.1 eq bootp deny ip any any
	int vlan 200	permit ip 10.1.200.0 0.0.0.255 10.1.303.0 0.0.0.255 permit udp any host 10.45.100.1 eq bootp deny ip any any
Distribution 2	int GigEther4/0	permit ip 10.1.100.0 0.0.0.255 10.1.303.0 0.0.0.255 permit ip 10.1.200.0 0.0.0.255 10.1.303.0 0.0.0.255 deny ip any any

Next, the respective ACLs can be updated to reflect the rules of User A contacting Server A and User B contacting Server B as follows:

Switch Name	Interface	ACL Logic
Distribution 1	int vlan 100	permit ip 10.1.100.0 0.0.0.255 10.1.301.0 0.0.0.255 permit ip 10.1.100.0 0.0.0.255 10.1.303.0 0.0.0.255 deny ip any any
	int vlan 200	permit ip 10.1.200.0 0.0.0.255 10.1.302.0 0.0.0.255 permit ip 10.1.200.0 0.0.0.255 10.1.303.0 0.0.0.255 deny ip any any
Distribution 2	int GigEther4/0	permit ip 10.1.100.0 0.0.0.255 10.1.301.0 0.0.0.255 permit ip 10.1.200.0 0.0.0.255 10.1.302.0 0.0.0.255 permit ip 10.1.100.0 0.0.0.255 10.1.303.0 0.0.0.255 permit ip 10.1.200.0 0.0.0.255 10.1.303.0 0.0.0.255 deny ip any any

Finally, the last rule that needs to be enforced is that all the servers should be allowed to communicate with each other. This is inherently allowed via Distribution 2 because the enforcing ACLs are not applied to any of the interfaces involved in direct communications between the servers.

Configuring and managing ACLs such as these in a large environment can become unwieldy. The easiest method to use to minimize this is to use an addressing plan that allows summarized ACLs to be applied to client groups. For example, an addressing plan such as the following can be used:

- Assign the accounting group of users to the address range of 10.3.0.0-10.3.127.0/24. This allows the accounting group to be represented across up to 128 distribution switches.
- Assign the engineering group of users to the address range of 10.4.0.0-10.4.63.0/24. This allows the engineering group to be represented across up to 64 distribution switches.

By creating groups in address spaces that can be summarized, it is now possible to represent the ranges with the following single lines in any applicable ACLs, despite the various individual subnets sourced from multiple distribution layers:

- Accounting: permit ip 10.3.0.0 0.0.127.255 *destination_IP destination_mask*
- Engineering: permit ip 10.4.0.0 0.0.63.255 *destination_IP destination_mask*

Note Future identity-based features being developed by Cisco should allow for more manageable deployment of compartmentalization of traffic with significantly less per-hop configuration necessary.

Configuration Example using Firewalls

To increase overall security and the protection of clients and network attached resources, another alternative is to use firewalls instead of ACLs to provide stateful inspection filtering. This can be accomplished by adding the firewalls inline on inbound interfaces of the distribution switch that connects the network-attached resources. This approach provides greater protection for the

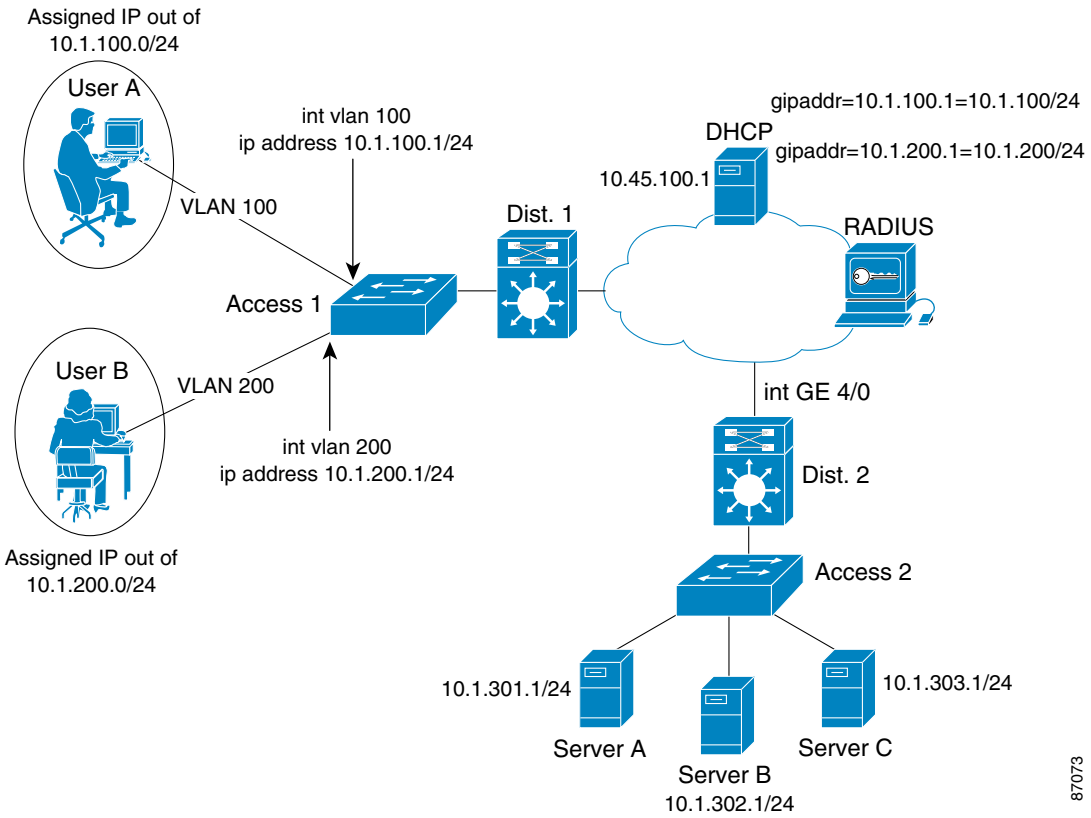
network-attached resources from more complex attacks or probes. The ACL logic previously discussed can be ported to the firewall context commands and implemented in a similar fashion inbound towards the resource.

In this example, the following can be used:

- PIX 535 firewall inline on interface Gigabit Ethernet 4/0 of Distribution 2
- Cisco Firewall Services Module in Distribution 2, because the example uses a Catalyst 6000 series switch.

The same logic as used for the ACLs can be applied in the form of conduits for the firewall, both in the generalized form used in these examples and in a more detailed form that integrates specific protocols and ports.

Figure 4-10 Configuration Example using Firewalls



Example Using the 802.1x Guest VLAN Feature

Catalyst OS version 7.5.0 and higher support a feature called “802.1x guest VLAN.” This feature allows administrators to configure strategic switches to allow *limited guest access* for network clients without 802.1x supplicant capabilities.

The guest VLAN feature, which is available on the Catalyst 6000/6500 platforms (and soon on the Catalyst 2950/3550 platforms), allows the assignment of a pre-determined VLAN to users that fail to authenticate using the 802.1x protocol. By configuring a designated VLAN as the 802.1x guest VLAN,

clients that do not have 802.1x supplicants or have disabled 802.1x supplicant abilities can connect to the network using only that specified VLAN. With proper planning and design, that VLAN can provide controlled or quarantined access to selected resources.

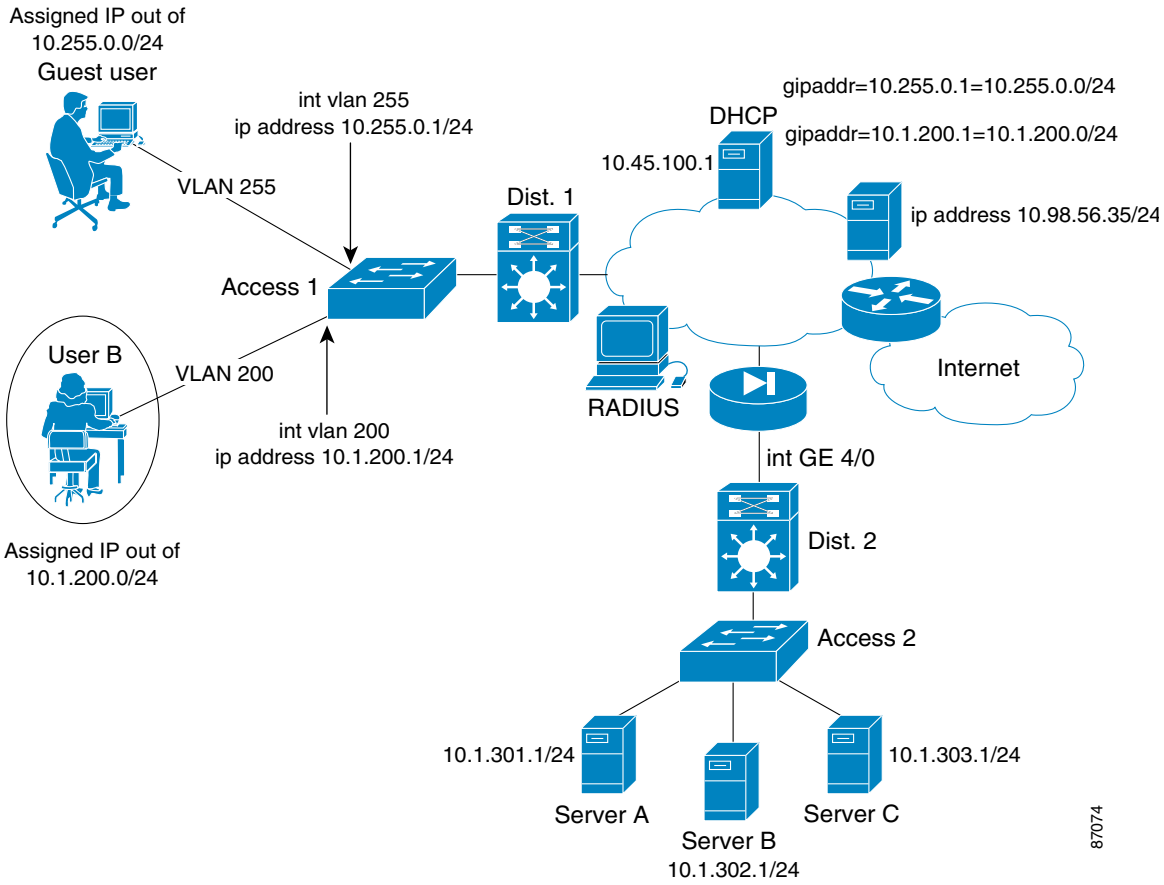
The 802.1x guest VLAN feature may be suitable for deployment in public areas, where connectivity services are provided to clients that are not necessarily part of the host enterprise's IT organization. For example, this feature can be used to provide access to visitors in conference rooms or lobby areas. In this situation, it might be desirable to provide limited network connectivity to only the Internet and not internal resources. This feature can also be useful during the migration from a non-802.1x networking environment to an 802.1x secured environment. In this scenario, it is likely that supplicant capabilities will be phased in, thereby presenting various parts of the network with some clients that are 802.1x capable while others are not. By leveraging the 802.1x guest VLAN feature, a more subtle migration plan can be realized for users.

Note A *guest* user is defined as a user without supplicant capabilities. This is determined by the connecting switch by observing the timeout of wait periods and retries in attempting to authenticate the client. This differs greatly from a client that authenticates, but fails authentication. A failed authentication will never be treated as a guest access situation. Instead all failed authentication attempts are blocked from network access. Therefore, if a visiting guest user is configured for 802.1x functionality within another enterprise context outside of the network that they require guest access on, it is essential that they disable their supplicant functionality.

In this example, limited network access is provided to allow Internet access by visiting clients that are not 802.1x capable.

Figure 4-11 includes two network connected clients. One is an enterprise user with access to enterprise resources. The other is a guest user visiting the enterprise and accessing the network from a public area. User A requires the same access as was described in the previous examples. User A’s VLAN and access privileges are dictated by that specific user's assigned policies, which are applied upon authentication. The guest user in this case requires only direct Internet access in order to VPN back to their respective headquarters. Because the focus is on supplying *limited* connectivity to the guest user, only the configuration required to do so is covered in this example.

Figure 4-11 Configuration Example Using Guest VLANs



The rules for access from the guest VLAN in this case are simple:

- The guest user should be able to access the Internet, unrestricted, outbound, via their default gateway router at 10.255.0.1/24.
- The guest user should not have access to any Enterprise resources other than DNS services from the guest DNS server at 10.98.56.35.
- All parameters for the auto-configuration of guest users should be supplied by the DHCP server at 10.45.100.1.

Guest VLANs are global on a per access switch basis, but may vary from switch to switch, even within a distribution layer. In this example, the guest users are placed into VLAN 255.

Enabling Guest VLANs

By default, Catalyst switches do not allow guest connectivity. Guest VLAN capabilities must be enabled on the access switches that are chosen to provide guest access. To enable guest VLAN capabilities, issue the following command:

set dot1x guest-vlan *VLAN_ID*

Where *VLAN_ID* is the numeric identifier for the VLAN designated as the guest VLAN.

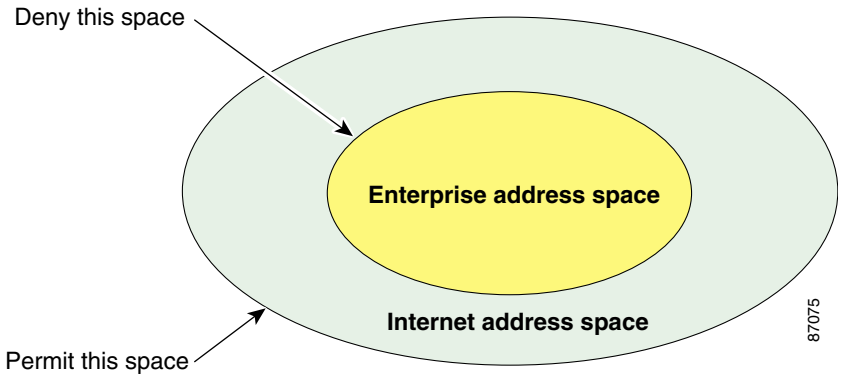
ACLs and Addressing

To control access to meet the rules previously listed, every distribution switch that connects guest-capable ports must be configured with an ACL on the inbound VLAN interface that corresponds to the guest VLANs.

Using ACLs to limit resource access is simplified if addressing is properly planned and contiguous. If the addressing space in which enterprise resources reside can be effectively identified in a simplified manner, then restriction ACLs can be summarized to reduce complexity of configuration.

The goal of the ACLs is to isolate all subnets and segments that contain resources that should be restricted by explicitly denying those address ranges. The default outside of that address space should encompass the Internet address space to which access is allowed. Figure 4-12 illustrates this concept.

Figure 4-12 Guest VLAN Goal



Given the addressing scheme in the example (in which the enterprise space is drawn from the RFC 1918 reserved private address space), the access policy can be effectively summarize with the following ACL:

```
access-list 100 deny ip any 10.0.0.0 0.255.255.255
access-list 100 permit ip any any
```

Traffic can be controlled by applying this ACL to each distribution router at each Layer 2 to Layer 3 boundary for all areas providing guest access.

Some basic services are also required for guest access. These include DNS and must be added to the ACL for connectivity to function correctly. The updated ACLs now appears as:

```
access-list 100 permit udp any host 10.98.56.35 eq 53
access-list 100 deny ip any 10.0.0.0 0.255.255.255
access-list 100 permit ip any any
```

The resulting example ACL provides limited access according to the predefined rules.

DHCP and Retries

The total time required to determine that a client is not 802.1x capable and, therefore, a guest user, is a product of the configured number of maximum retries multiplied by the supplicant timeout period.

max(time to guest access) = max_retries * max_client_wait

This aspect is important to configuration as most DHCP clients will timeout DHCP configuration attempts after 64 seconds. For most client operating systems (particularly Microsoft Windows variants), the DHCP process is not necessarily serialized to the 802.1x authentication process. This means that

improperly configured timers on the switch could affect the DHCP process of the connecting client. Therefore, it is important that the timers and retries not be configured such that they result in a total DHCP process delay greater than 60 seconds.

For example, the following configuration will cause problems:

```
max_retries = 3  max_client_timeout=30
3 * 30 = 90 > 64
```

In this case, the client's DHCP process will likely timeout before guest access is granted. This will result in a scenario in which the user has obtained guest access with working Layer 2 connectivity. However, they will not receive a valid configuration via DHCP and, therefore, do not have working Layer 3 connectivity.

The following is a better configuration:

```
max_retries = 5  max_client_timeout=3
5 * 3 = 15 < 64
```

By reducing the time it takes to establish non-supplicant guest status, DHCP processing can occur within the necessary window of time and connectivity will be accomplished at both Layer 2 and Layer 3.

CHAPTER 5

Moving to an Identity-Based Networking Environment

The IEEE 802.1x protocol in combination with Cisco's identity-based networking features provides the network administrator with the ability to control access and enforce policies on network clients based on authenticated identity. This unparalleled control in network access contributes to the overall enterprise security architecture by reducing exposure to intrusion and unauthorized use of the network or network-attached resources.

A comprehensive migration strategy from existing environments to one that integrates the features of an identity networking solution is crucial to an effective security implementation. In migrating to (or implementing) 802.1x and Cisco's identity networking solutions, various components that do not currently exist in the typical enterprise environment must be introduced. This must be done in an orchestrated manner so as:

- Not to impact current network clients in their current configurations.
- Not to inadvertently reduce the security benefits of network segments that are migrated into an identity-based network environment.

A planned, phased approach that systematically moves sections of the network and groups of network clients to the identity-based environment is the most logical approach to this challenge.

This chapter briefly reviews the components of an identity-based network and discusses the impact of introducing each into a campus network. It also describes the recommended steps for migrating from a non-identity network to an identity-based network.

Components of Identity Networking

Identity-based networking introduces some new entities into the network and leverages some existing ones. The first step in planning a migration to incorporate identity features into a network is to identify the components of an identity-based solution and understand their impact on the network and it's clients. By understanding the components and their respective potential impact, it becomes easier to create a migration strategy to minimize their effects.

The basic components of Cisco's identity networking solution are:

- Client-side supplicant code—IEEE 802.1x supplicant code supplied by either the OS developer or 3rd-party client developers.
- Authenticator Network Access Point—The entry point into the network infrastructure to which a client directly connects in order to request and gain network access.

- Back-end RADIUS-based Authentication Server—The reference decision and policy engine that communicates with the network access point in order to provide the authentication and authorization logic of the identity process.
- The client information database—The information storage base that maintains all of the generalized account and policy information needed by the authentication server to process and render decisions regarding a client based on its identity.

Impact of Client Side Supplicant Code

Typically, most production networks do not include code for client-side supplicant ability. In most cases, add-in code or operating system updates are available to add the ability. When integrating client-side code and the necessary processes to incorporate IEEE 802.1x-based authentication, the goal should be to minimize the following impacting characteristics:

- The downtime required to update the client-side system to add IEEE 802.1x supplicant abilities.
- Change in the operational parameters or processes required by users to make use of the new abilities of the system.

Both of these impacting characteristics have the potential to directly affect end-user productivity. To minimize these effects, the migration should:

- Allow the end-user to apply updates or add-ins in a comprehensively automated manner, accompanied by any required instructions for applying the updates. The requirement for this update must be independent of the actual overall network migration state. Therefore, during the migration period, the network should accept and handle both authenticating and non-authenticating clients.
- Not significantly change the method by which the client end-user interacts with the system to gain access to the network and provide authentication information. This means that the once the supplicant abilities have been integrated into the client system, usage parameters and previously formed user habits should not be changed significantly.

  To minimize change in the user interaction with the system, the method chosen for authentication in 802.1x should allow the user to continue using credentials with which they are already familiar. For most enterprise environments, this is the standard username and password combination. By maintaining these as the criteria for authentication, very little change is required in most cases. In the example deployment environment discussed in previous chapters, the client-side operating system and server environment consist of Windows 2000 operating systems. On the client side, the choice of EAP-TLS or PEAP with EAP-MSCHAPv2 allows the user to continue using their familiar username and password credentials.

In addition to this, it is important to consider the actual availability of supplicant support for the various client platforms.

- For operating systems, supplicant support is typically made available by the OS vendor. In some cases, third party or open source supplicant code may be available.
- For hardware client devices, embedded supplicant support is typically made available in firmware upgrades, issued by the appropriate hardware vendor. For example, HP JetDirect wireless print server adapter cards have integrated 802.1x supplicants.

Note Currently, Cisco WLAN APs and IP Phones have planned support for 802.1x supplicant capabilities in future firmware releases.

Impact of Authenticator Network Access Devices

The Authenticator Network Access Point in this environment refers to any network device that provides connectivity for end-clients into the network infrastructure. This may consist of a switch or a wireless access point. In either case, the common factor is the ability of that network device to communicate via IEEE 802.1x with the client and via RADIUS with the back-end authentication server.

The potential impact of integrating authenticator functionality is that of reduced productivity due to a client's inability to connect to the network. This may happen if plans are not made to accommodate both supplicant and non-supplicant clients simultaneously on any given network access device.

The migration strategy presented in this chapter assumed that the network contains a device that has been upgraded to provide IEEE 802.1x authenticator functionality. For cases in which the network access hardware is not upgradable the general rules for a complete hardware upgrade would apply.

In the case of a software upgrade, such as with an installed base of Catalyst 6500 switches, the codebase of the hardware can be updated even if the IEEE 802.1x features are not going to be enabled immediately. This ability, in conjunction with the guest VLAN feature, allows a gradual transition that can provide connectivity for both supplicant and non-supplicant capable clients.

Impact of the RADIUS Server and the User Database

The impact of the RADIUS subsystem and the user database is relatively low compared with that of the other components in an identity solution. In most cases, a user database already exists. The process of integrating identity features into the network should not change the structure, data, or operation of any existing databases. Instead, it will only rely on the database as a current store from which to draw client-related information for the process of authentication and client-associated policies.

The RADIUS server provides the role of integration and interface between the network access device (acting as an authenticator) and the information within the user database. Typically, the RADIUS server is given read-only access to the user database. Policy information can be stored in the RADIUS server engine, but it can also be drawn from the user database (using methods similar to how it accesses specific client identity information). In some cases, one or more RADIUS servers may already be integrated into the network environment to support other AAA functions.

Moving to an Identity-Based Networking Environment

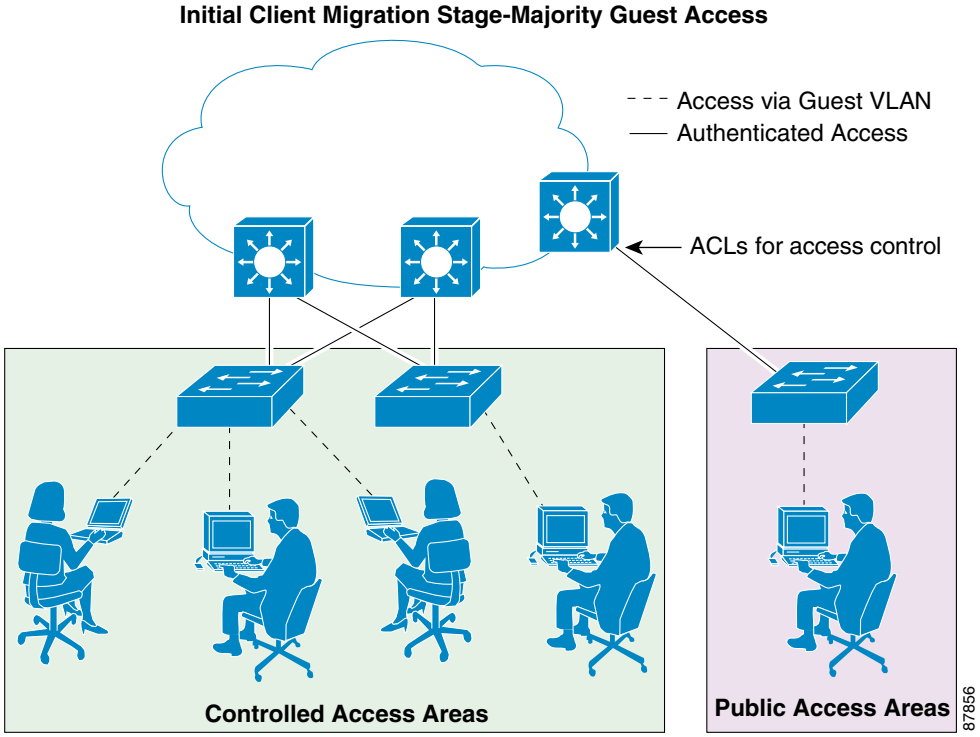
Taking into account the potential impact and effects examined earlier, the suggested sequence of events in migrating to an identity-based network environment are as follows:

Step 1 Perform the hardware migration of any network access devices that are not inherently IEEE 802.1x authenticator capable.

Step 2 Perform a sequential, phased software migration of hardware platforms that are IEEE 802.1x authenticator capable once updated. **Do not** enable authenticator features until later. Verify that the codebase that incorporates the authenticator functionalities is stable and able to provide all other functionality previously available.

Step 3 Enable IEEE 802.1x authenticator functionality on the network access devices that have been software upgraded. The configuration of the devices should provide support for simultaneous access by supplicant and non-supplicant capable clients. This can be performed by leveraging the guest VLAN feature of Catalyst OS (as shown in Figure 5-1).

Figure 5-1 Initial Client Migration Stage – Majority Guest Access

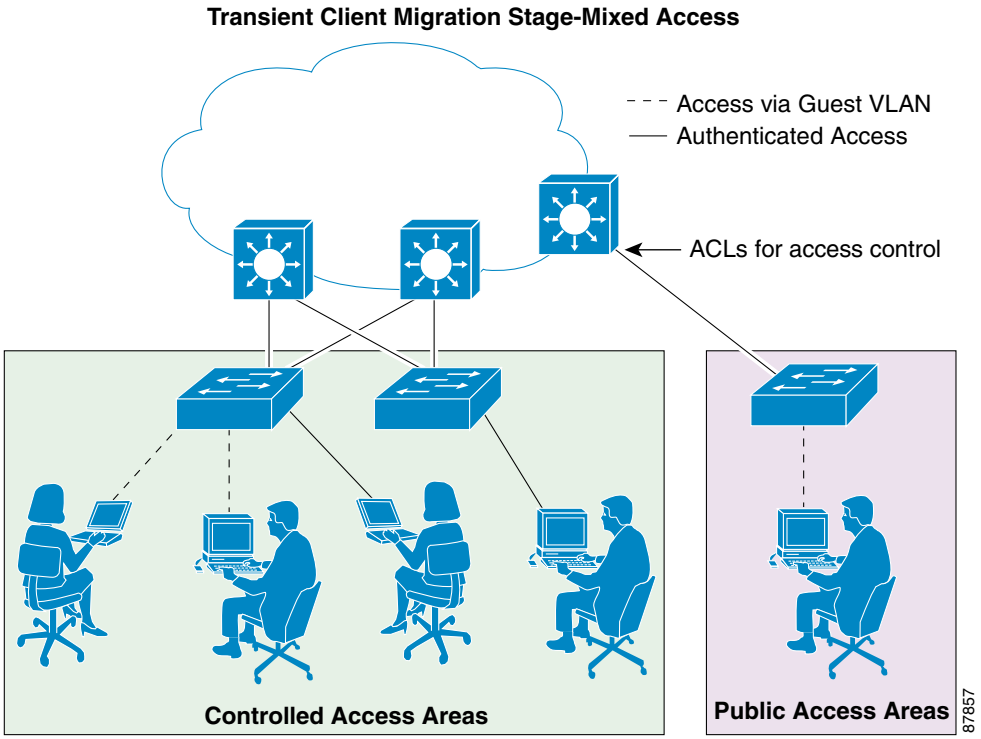


For more information about Guest VLANs, see "Enabling Guest VLANs" section on page 4-18.

Step 4 Distribute and install supplicant capabilities on the network clients to be migrated.

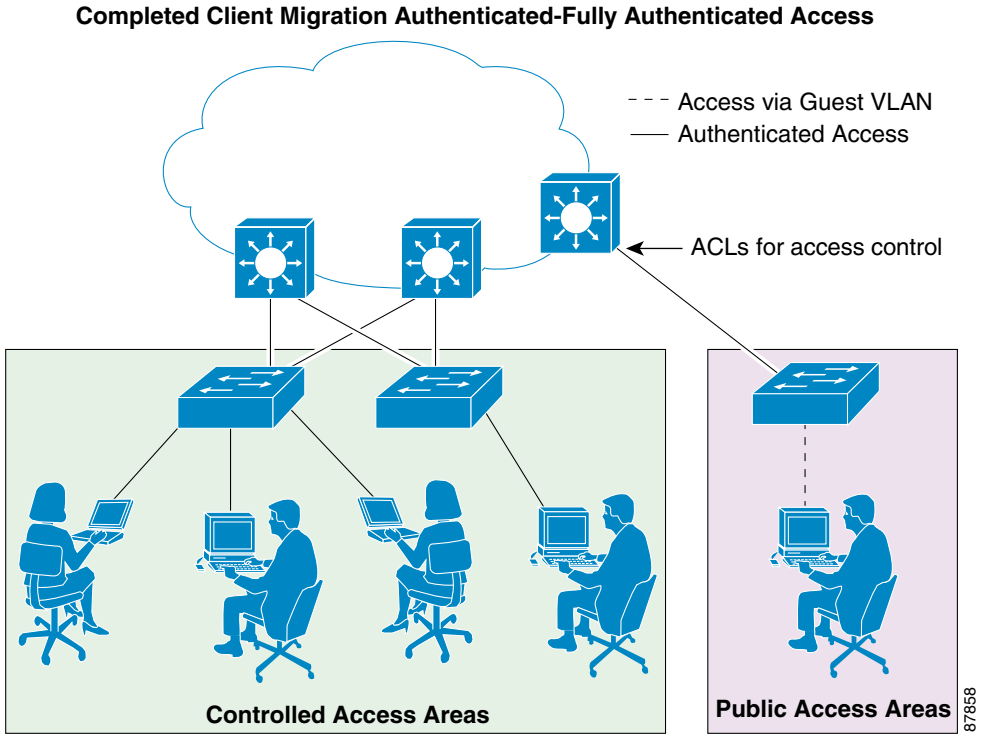
Step 5 Sequentially enable client-side configurations to make use of the newly installed supplicant capabilities, reducing the number of Guest VLAN users (as shown inFigure 5-2).

Figure 5-2 Transient Client Migration Stage – Mixed Access



Step 6 Once all of the clients connecting to a particular network authenticating network access device are capable of authenticating and accessing the network within the configured policy parameters, disable the guest VLAN feature on that network access device for the controlled access areas. (as shown in Figure 5-3).

Figure 5-3 Completed Client Migration Authenticated – Fully Authenticated Access



This sequence of events minimizes the potential impact of the identity components being introduced, modularizes the migration, and allows easy reversal in the event of a complication.

Migrating Non-Authenticator Capable Hardware

Certain hardware platforms may not be capable of supporting authenticator capabilities. These platforms should be migrated to newer hardware that is capable of performing the required functionality to avoid the possibility of holes in the identity architecture through which clients might potentially access the network without authentication.

Some implementation plans may choose to either omit this step or defer it to a later stage in the migration. However, careful consideration and additional planning is required to do so in a secure manner. The inherent danger in omitting, or deferring, this step is the potential for authenticated segments of the network to interconnect inadvertently with the non-authenticating segments.

If this step must be skipped or deferred to a later phase, it is imperative that the authenticating and non-authenticating segments be separated and the interconnection between authenticating and non-authenticating segments be carefully controlled. This can be provided via the use of access control lists, firewalls, and actual physical separation. It is important to note, however, that these facilities require per-point configuration for every interconnection point between authenticating and non-authenticating segments. It is therefore in the best interest of reducing complexity and the probability of error, to reduce the number of interconnecting points between the two security environments.

Upgrading Authenticator Capable Devices

The true first stage in migration is to begin adding authenticator capabilities to the network access devices. These new authenticating network access device must be able to provide the same functionality at the same level of stability as the previous device. To confirm this, do the following:

1. Upgrade the software to an adequate version with the required features and allow that version to run as a direct replacement of the previous software version *without* the authenticator features enabled.
2. Once the device as been running for a period of time that is sufficient to assess its stability and overall replacement functionality, the authenticator functionality can be enable.

For some period of time, the network access devices must be able to support both supplicant and non-supplicant capable clients. This can be accomplished by enabling the authenticator functionality in conjunction with the guest VLAN feature. The guest VLAN feature enables the access switch to detect the lack of an authenticating supplicant via the timeout of authentication requests originated by the authenticator. Upon expiration of the administrator-configured timeouts and retries, the guest VLAN feature can provide default connectivity to a designated VLAN for clients that exhibit the lack of a functioning supplicant. Simultaneously, clients that respond to the authenticator-initiated requests will be authenticated using the IEEE 802.1x model and granted network access accordingly, based on administrator-configured parameters. This enables networks to simultaneous support of both supplicant and non-supplicant capable clients and allows a phased, sequential migration of clients themselves.

Note For more information about configuring guest VLANs, see "Enabling Guest VLANs" section on page 4-18.

The following is a list of the current software upgradeable Cisco authenticator platforms.

- Catalyst 5500 Family
- Catalyst 6500 Family
- Catalyst 6000 Family
- Catalyst 4000 Family
- Catalyst 4500 Family
- Catalyst 2950
- Catalyst 3550
- Cisco Aironet 340/350/1200/1100 APs

Upgrading the Clients and Enabling Supplicant Capabilities

The next stage of the migration process involves distributing and enabling the client-side supplicant software. Existing or traditional methods of distribution can be used to provide the necessary software to the client end-systems. The topic of software distribution is outside the scope of this document. However, the migration process should be integrated with the distribution schema already in use.

Once the necessary client-side supplicant code (or updates) is installed on the end-systems, the supplicant capabilities can be enabled and the enrollment credentials can be distributed in a flexible window of time. This is due to the migratory state of the authenticator, which is able to simultaneously support supplicant and non-supplicant capable clients.

If the current environment permits unauthenticated access to a specific guest VLAN for users of a particular access switch, then that guest VLAN can be used for non-supplicant capable clients.

If the dynamic VLAN assignment feature is being deployed, the VLANs assigned should follow the same schema developed for dynamic VLAN usage. If the dynamic VLAN feature is not being used, then all clients will automatically assume the statically-configured VLAN that is associated with the particular port to which they are connecting. The statically defined VLANs will dictate the IP subnet obtained in the DHCP process.

For more information on enabling supplicant capabilities, see:

- Chapter 2, "Deploying EAP-TLS Network Access Control"
- Chapter 3, "Deploying EAP-MD5 Network Access Control"

Disabling the Guest VLAN Feature

Once all the required clients for a given device have been migrated and 802.1x-based authentication is operational, the guest VLAN feature can be disabled in order to provide an authenticated-only access device and a more secure environment.

Migrating in an Environment of Non-guest Capable Authenticators

Migration into an 802.1x environment becomes much more challenging and less smooth in environments in which the authenticator devices do not support a guest mode of access. Without a guest mode capability, there is no way to implement an interim state in which both supplicant and non-supplicant clients may access a given switch port simultaneously. Generally, the only method of migration applicable in this scenario is to hot-cut a given port from a non-authenticating port to an authenticating port. To do this, all preparations necessary to perform authentication, including preparation of the client, must be performed first.

Note An IEEE 802.1x client configured to authenticate is still capable of accessing the network via a non-authenticating switch. The default behavior of the IEEE 802.1x model is for a supplicant that is not prompted to authenticate to assume that connectivity is automatically granted and authorized. This model allows simplified backward compatibility for connectivity to non-802.1x compliant switches. In the case of a network migration, this fact places the client migration at a point of easier conversion prior to migration or reconfiguration of the authenticator.

Once all preparations have been made (authenticator upgrade, client upgrade, and so forth) the task of switching over to an authenticated environment must be done incrementally on a port-by-port basis with each port and client pair migrated and tested for successful authentication. Obviously, this deployment scenario tends to be more tedious. However, the gradual verification is necessary to minimize the complexity of a reversal, if necessary.