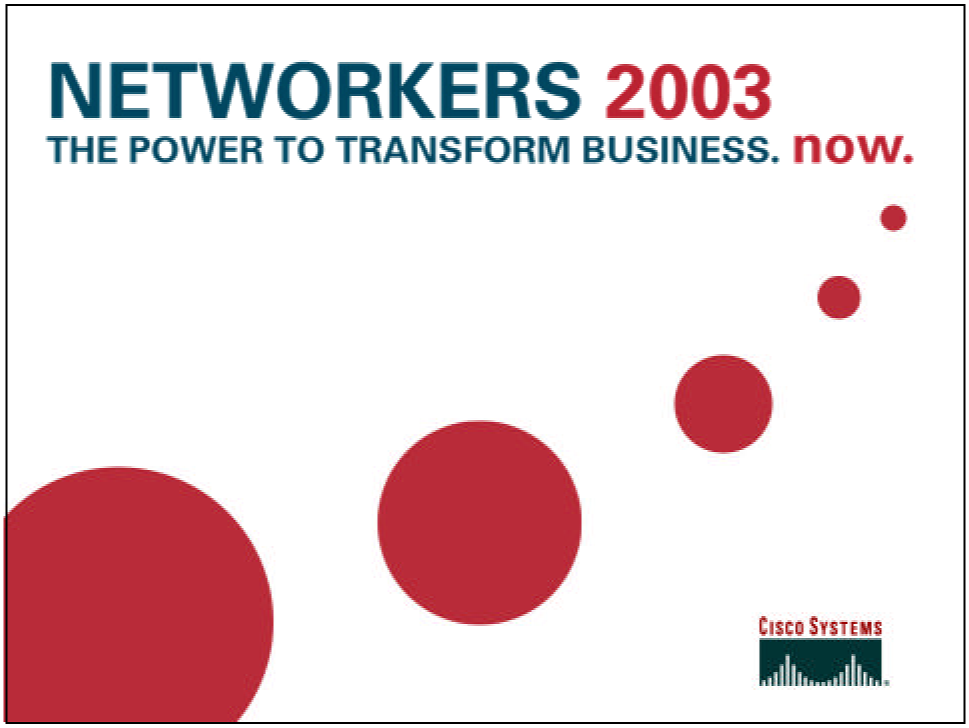
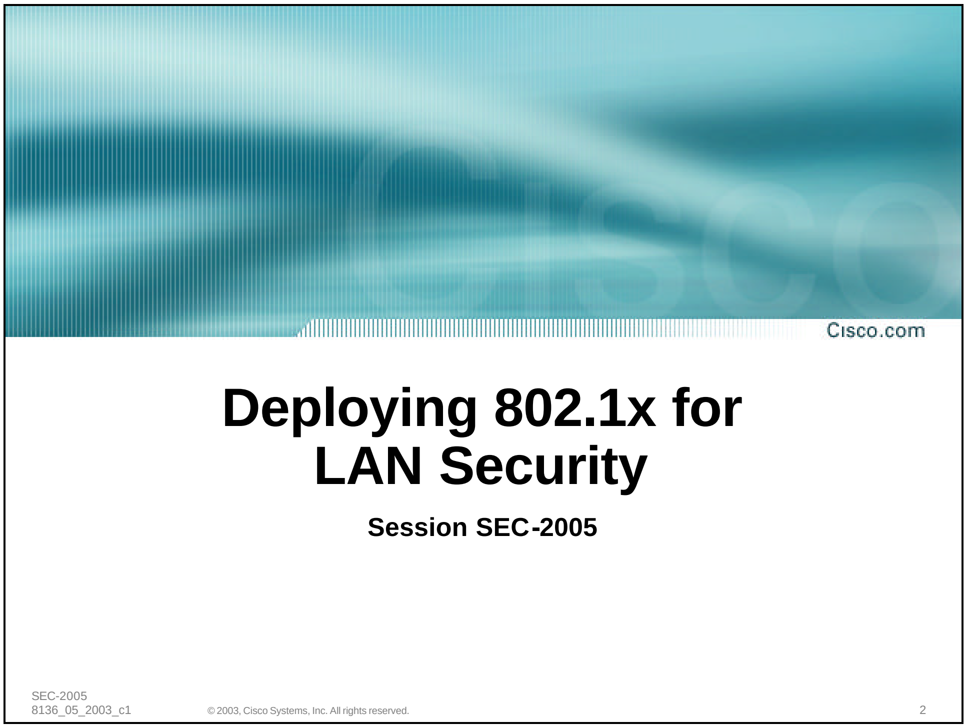


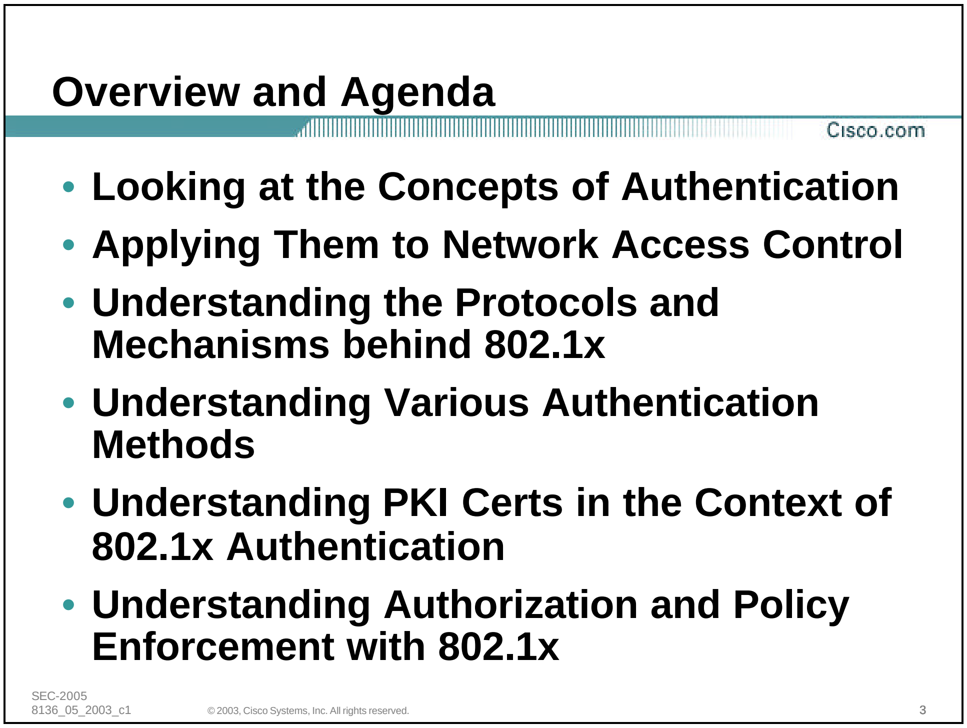
NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.



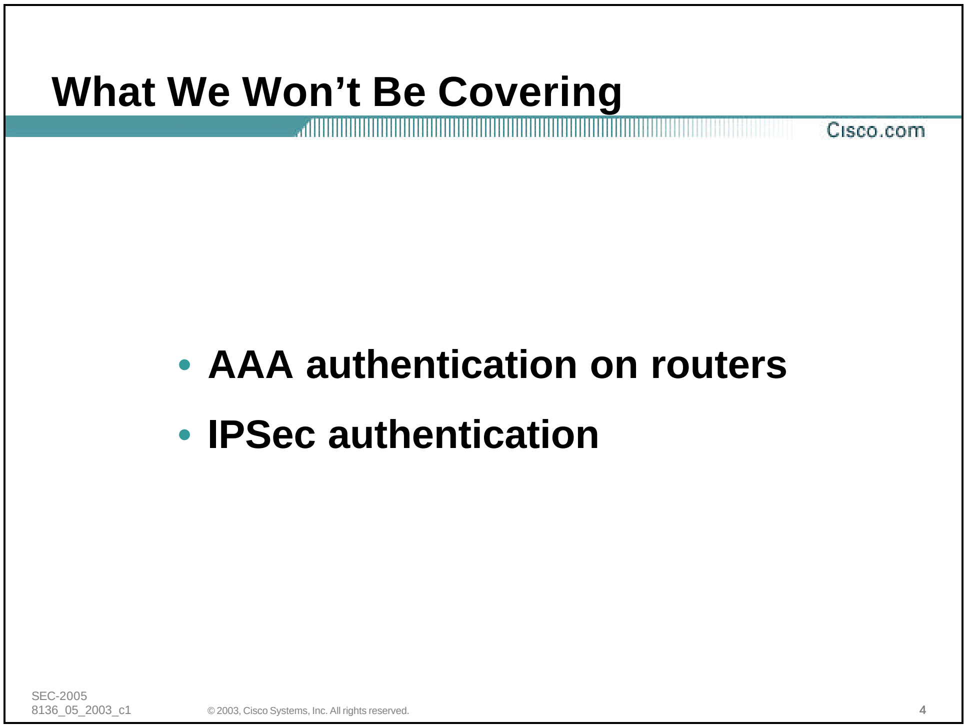
Deploying 802.1x for LAN Security

Session SEC-2005



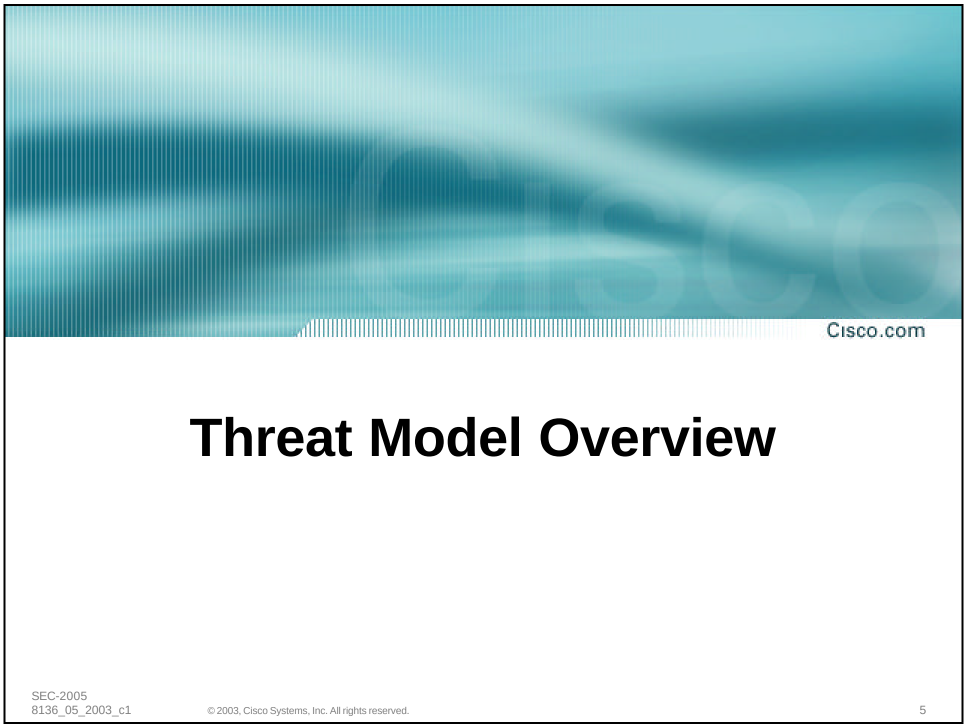
Overview and Agenda

- Looking at the Concepts of Authentication
- Applying Them to Network Access Control
- Understanding the Protocols and Mechanisms behind 802.1x
- Understanding Various Authentication Methods
- Understanding PKI Certs in the Context of 802.1x Authentication
- Understanding Authorization and Policy Enforcement with 802.1x



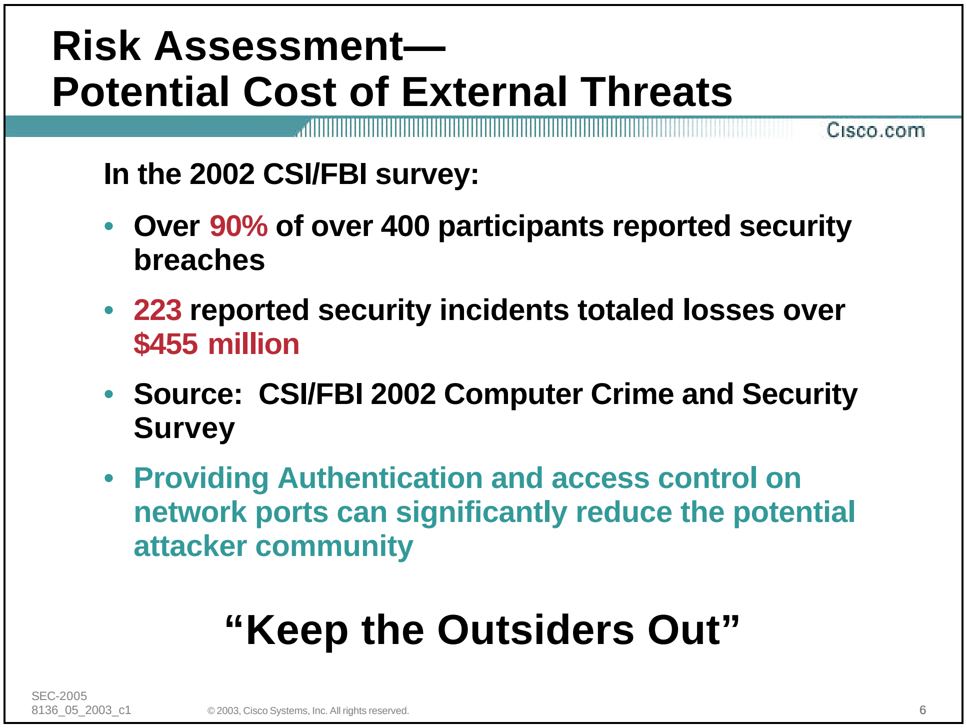
What We Won’t Be Covering

- AAA authentication on routers
- IPSec authentication



Cisco.com

Threat Model Overview



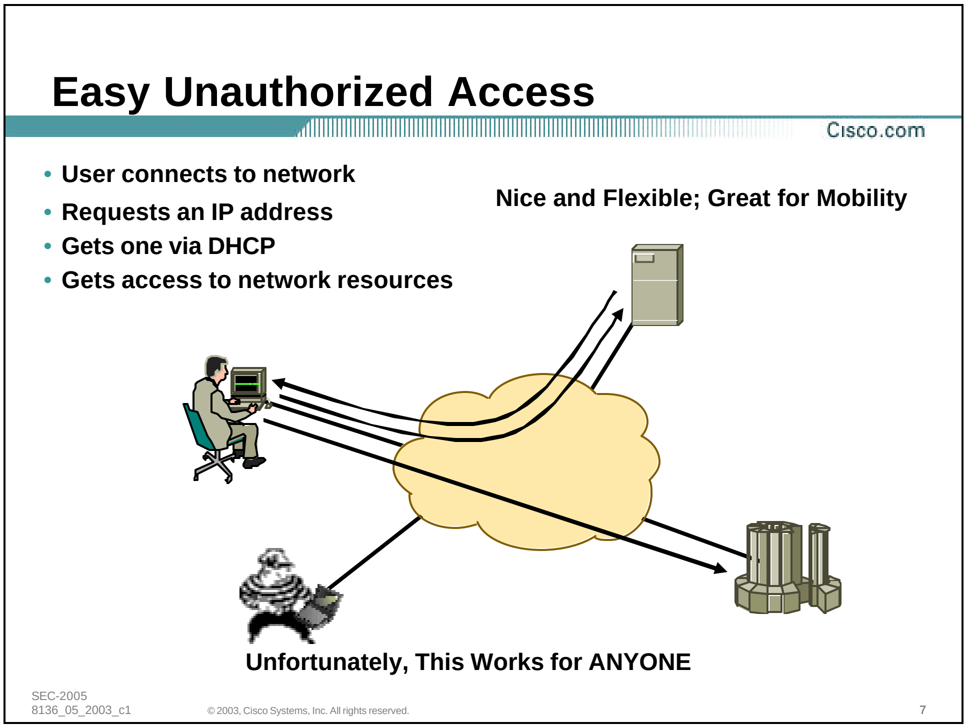
Risk Assessment—
Potential Cost of External Threats

Cisco.com

In the 2002 CSI/FBI survey:

- Over 90% of over 400 participants reported security breaches
- 223 reported security incidents totaled losses over $455 million
- Source: CSI/FBI 2002 Computer Crime and Security Survey
- Providing Authentication and access control on network ports can significantly reduce the potential attacker community

“Keep the Outsiders Out”

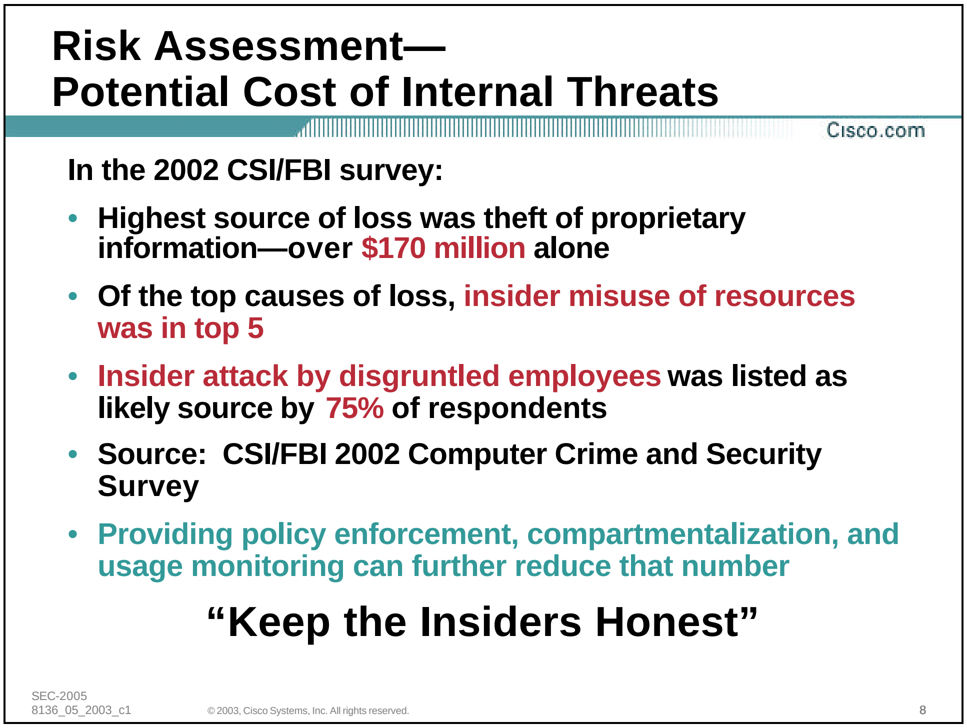


Easy Unauthorized Access

- User connects to network
- Requests an IP address
- Gets one via DHCP
- Gets access to network resources

Nice and Flexible; Great for Mobility

Unfortunately, This Works for ANYONE



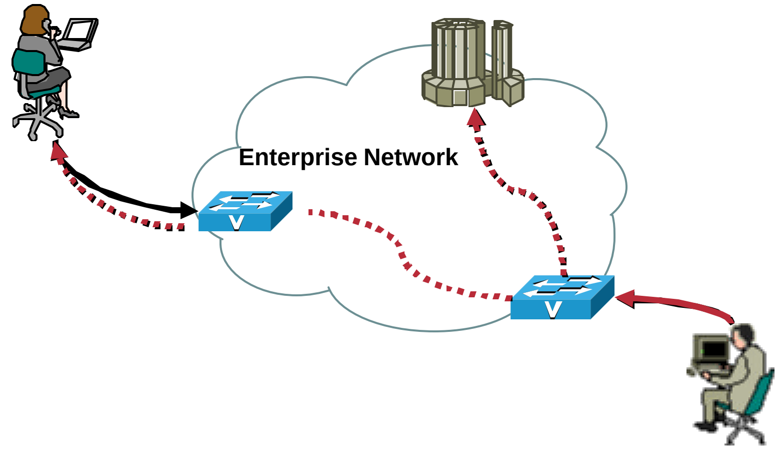
Risk Assessment— Potential Cost of Internal Threats

In the 2002 CSI/FBI survey:

- Highest source of loss was theft of proprietary information—over $170 million alone
- Of the top causes of loss, insider misuse of resources was in top 5
- Insider attack by disgruntled employees was listed as likely source by 75% of respondents
- Source: CSI/FBI 2002 Computer Crime and Security Survey
- Providing policy enforcement, compartmentalization, and usage monitoring can further reduce that number

“Keep the Insiders Honest”

Unauthorized Use of the Network

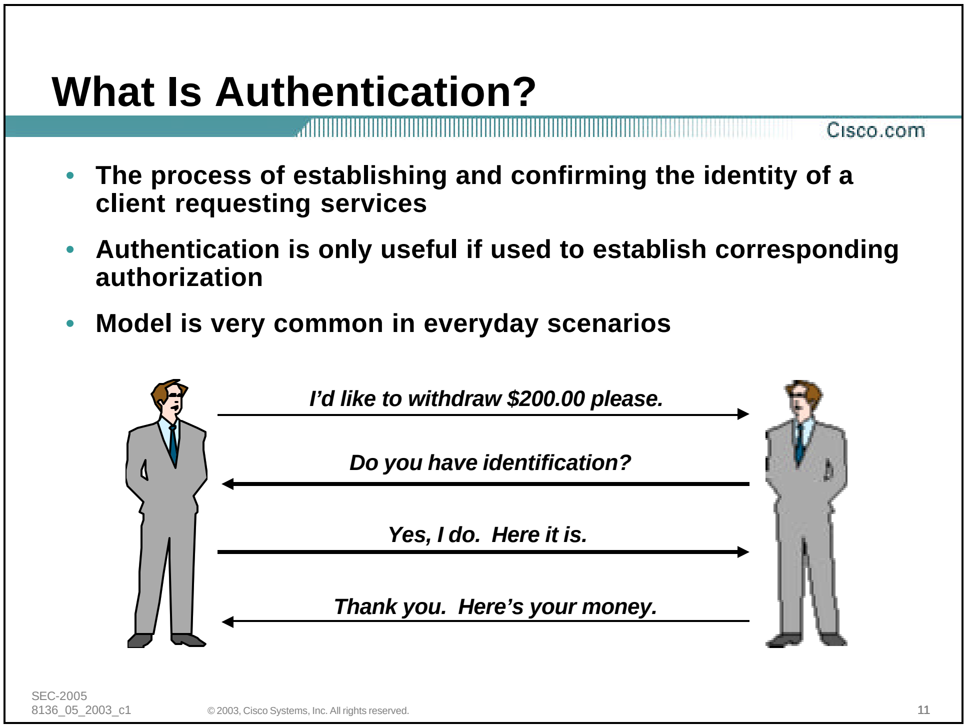


Authorized User/Employee

Enterprise Network

Authorized User/Employee

Understanding Authentication



What Is Authentication?

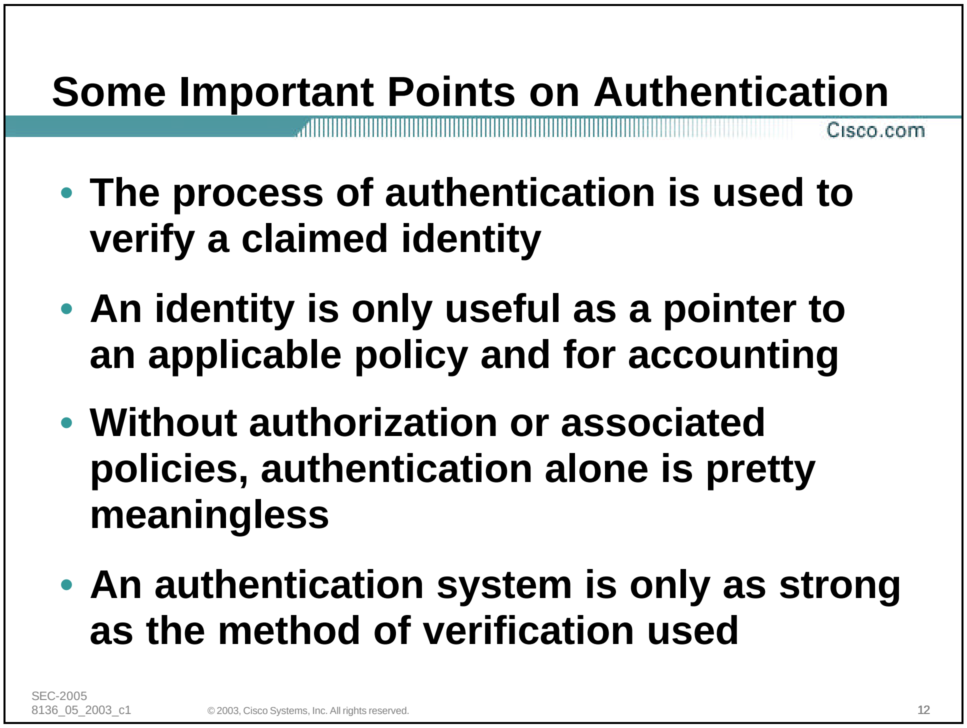
- The process of establishing and confirming the identity of a client requesting services
- Authentication is only useful if used to establish corresponding authorization
- Model is very common in everyday scenarios

I'd like to withdraw $200.00 please.

Do you have identification?

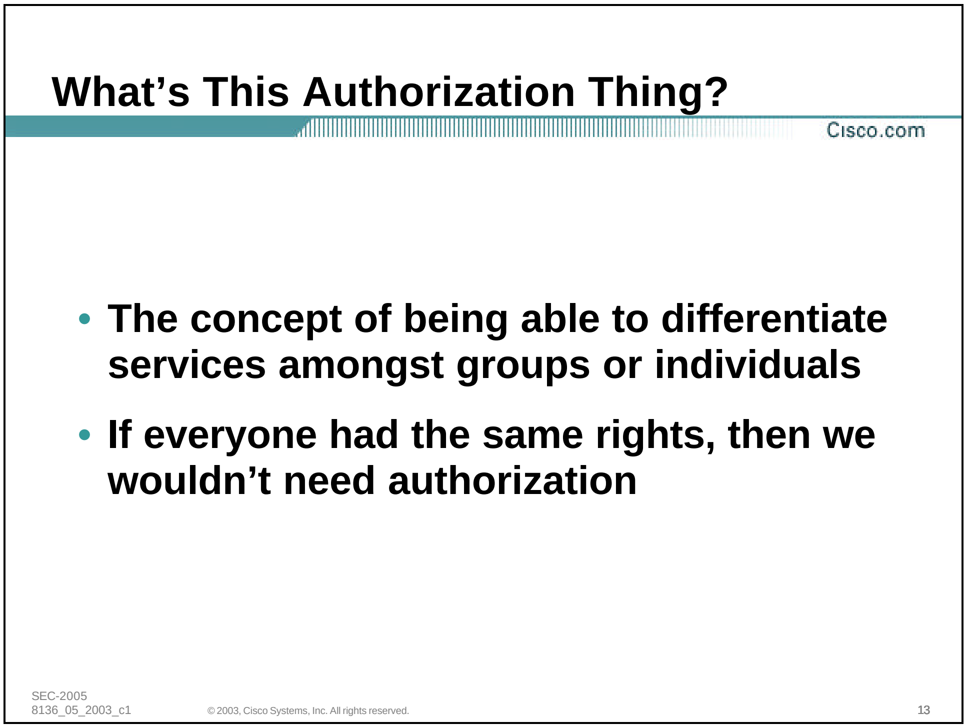
Yes, I do. Here it is.

Thank you. Here's your money.



Some Important Points on Authentication

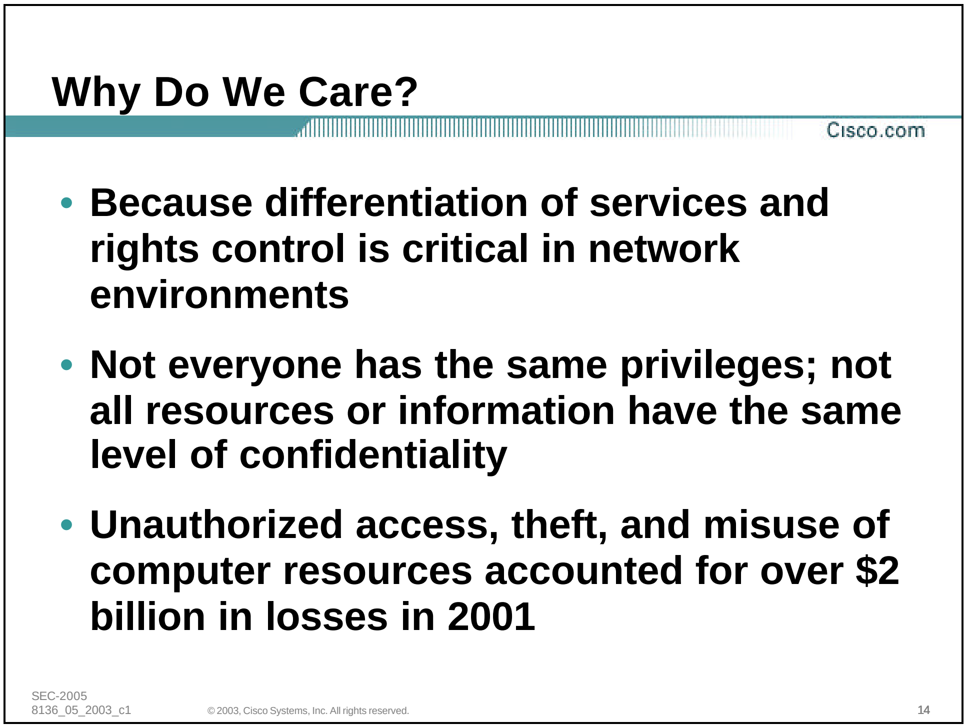
- The process of authentication is used to verify a claimed identity
- An identity is only useful as a pointer to an applicable policy and for accounting
- Without authorization or associated policies, authentication alone is pretty meaningless
- An authentication system is only as strong as the method of verification used



What’s This Authorization Thing?

Cisco.com

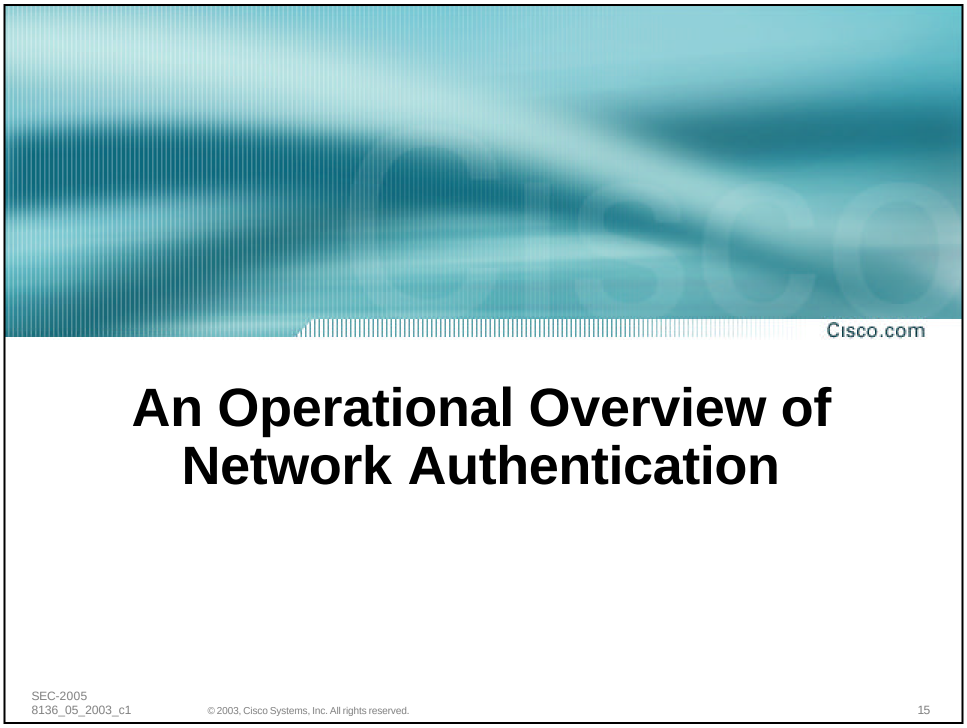
- The concept of being able to differentiate services amongst groups or individuals
- If everyone had the same rights, then we wouldn’t need authorization



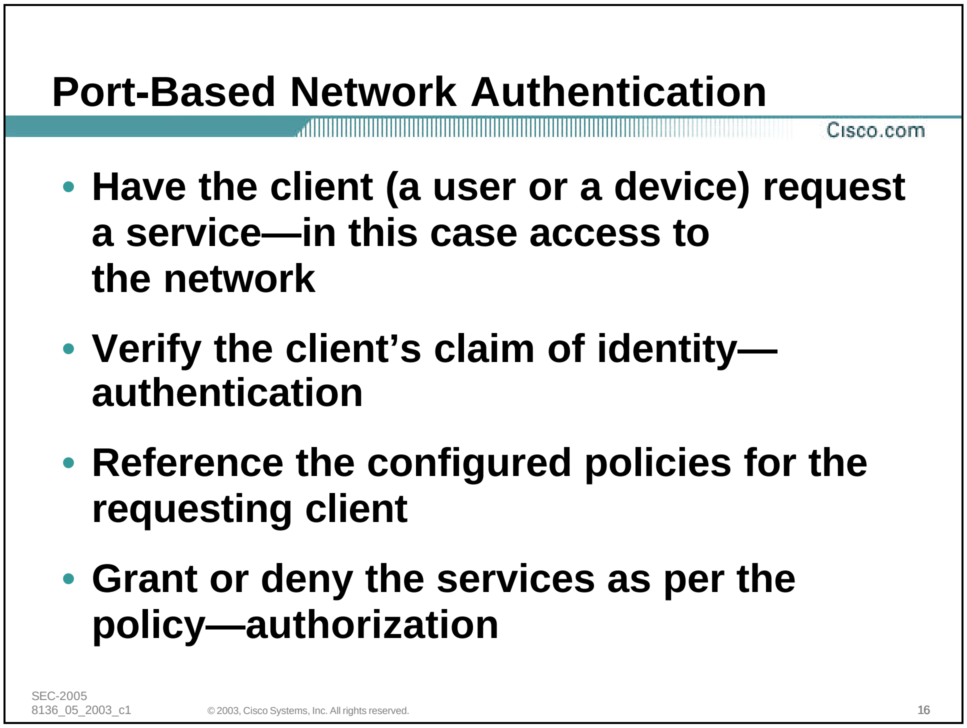
Why Do We Care?

Cisco.com

- Because differentiation of services and rights control is critical in network environments
- Not everyone has the same privileges; not all resources or information have the same level of confidentiality
- Unauthorized access, theft, and misuse of computer resources accounted for over $2 billion in losses in 2001

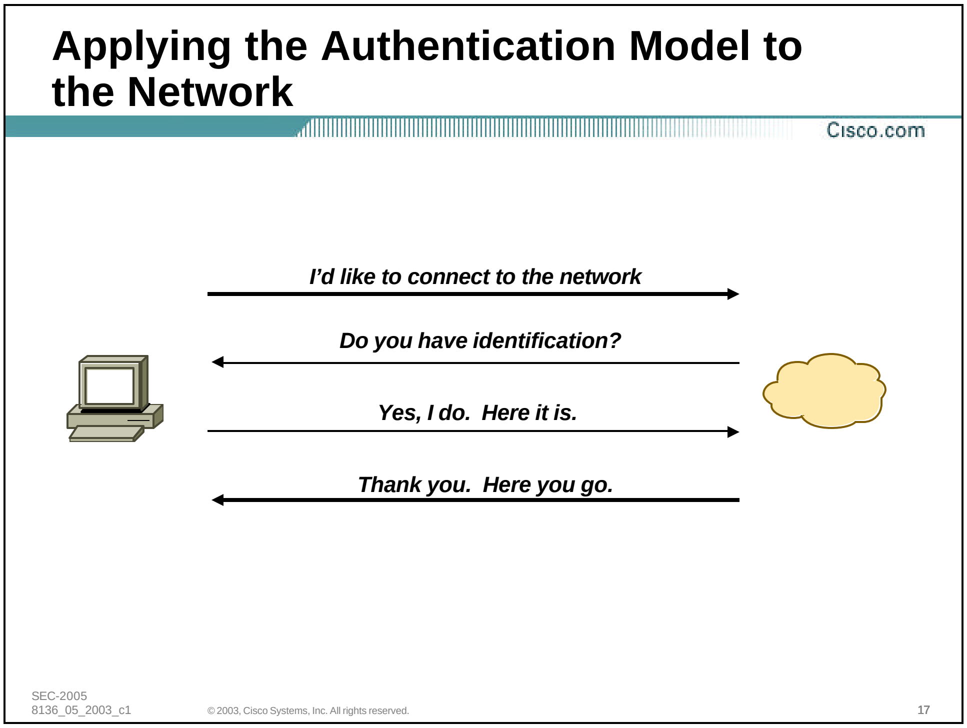


An Operational Overview of Network Authentication



Port-Based Network Authentication

- Have the client (a user or a device) request a service—in this case access to the network
- Verify the client’s claim of identity—authentication
- Reference the configured policies for the requesting client
- Grant or deny the services as per the policy—authorization



Applying the Authentication Model to the Network

Cisco.com

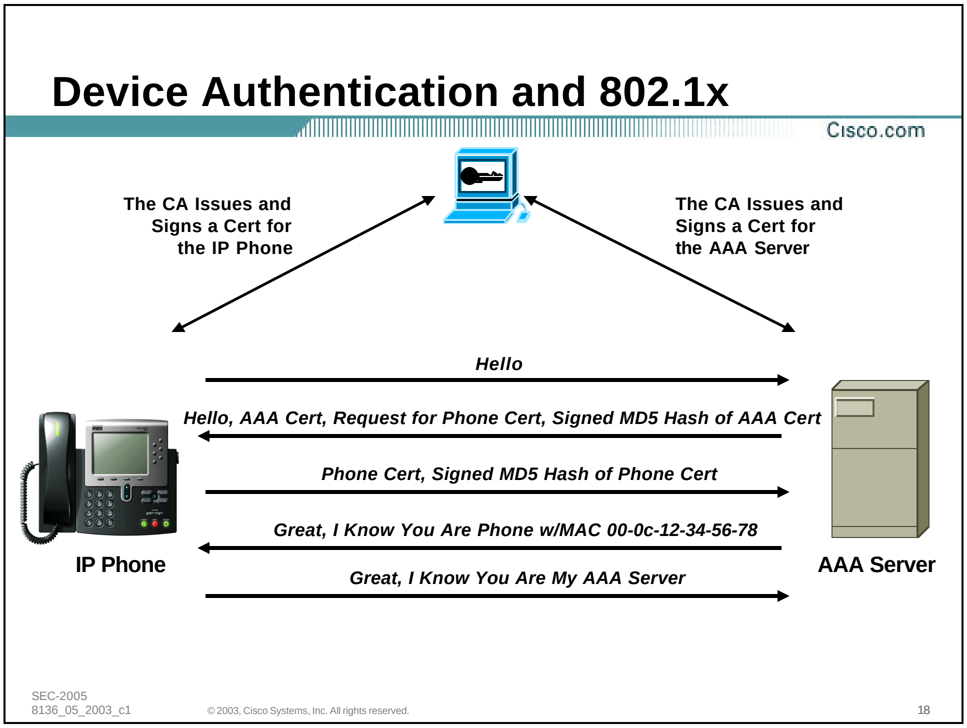
I'd like to connect to the network

Do you have identification?

Yes, I do. Here it is.

Thank you. Here you go.

SEC-2005
8136_05_2003_c1



Device Authentication and 802.1x

Cisco.com

The CA Issues and
Signs a Cert for
the IP Phone

The CA Issues and
Signs a Cert for
the AAA Server

Hello

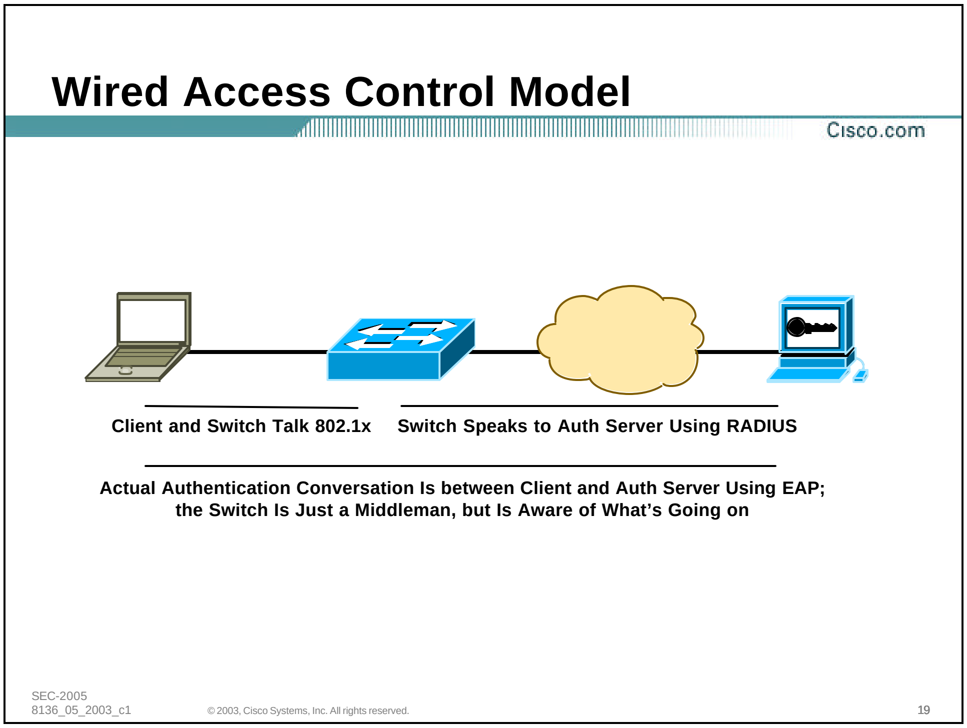
Hello, AAA Cert, Request for Phone Cert, Signed MD5 Hash of AAA Cert

Phone Cert, Signed MD5 Hash of Phone Cert

Great, I Know You Are Phone w/MAC 00-0c-12-34-56-78

Great, I Know You Are My AAA Server

SEC-2005
8136_05_2003_c1



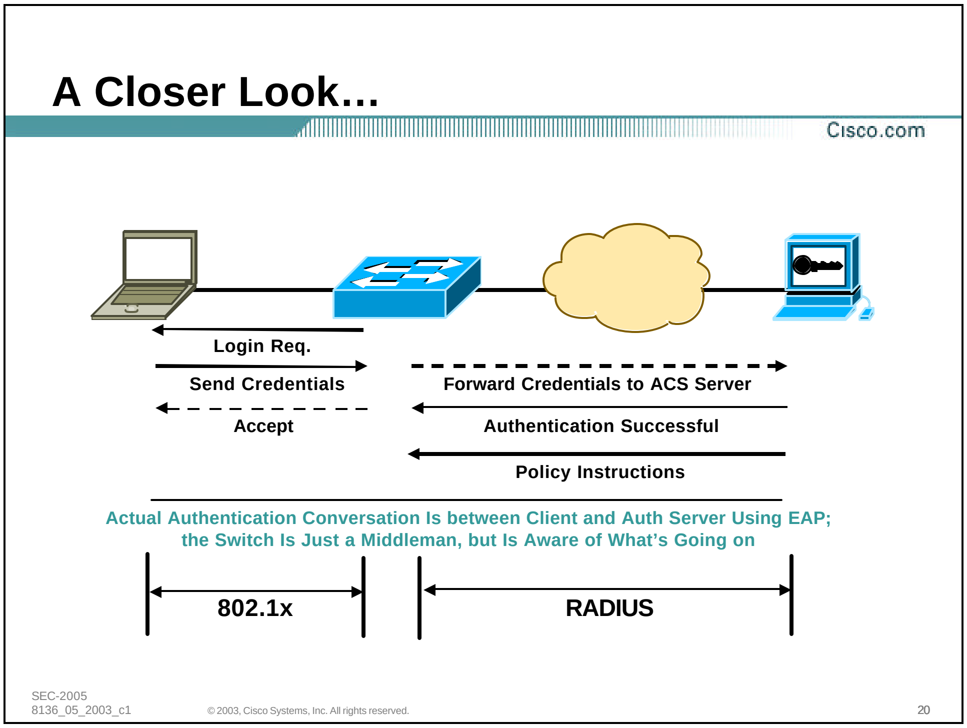
Wired Access Control Model

Client and Switch Talk 802.1x

Switch Speaks to Auth Server Using RADIUS

Actual Authentication Conversation Is between Client and Auth Server Using EAP; the Switch Is Just a Middleman, but Is Aware of What's Going on

SEC-2005
8136_05_2003_c1



A Closer Look…

Login Req.

Send Credentials

Accept

Forward Credentials to ACS Server

Authentication Successful

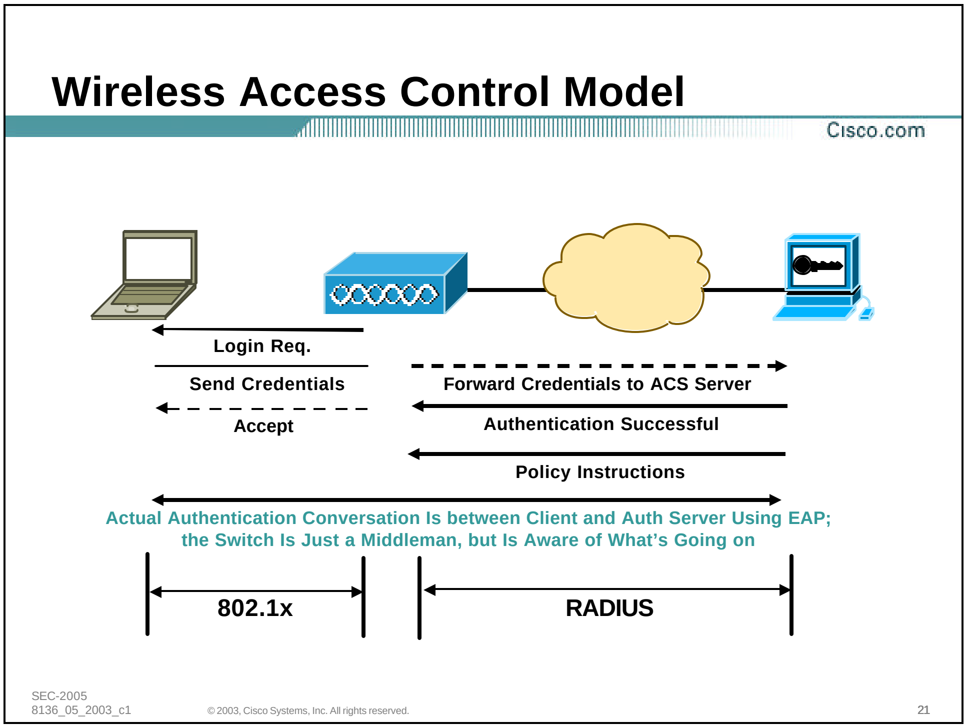
Policy Instructions

Actual Authentication Conversation Is between Client and Auth Server Using EAP; the Switch Is Just a Middleman, but Is Aware of What's Going on

802.1x

RADIUS

SEC-2005
8136_05_2003_c1



Wireless Access Control Model

Cisco.com

Login Req.

Send Credentials

Accept

Forward Credentials to ACS Server

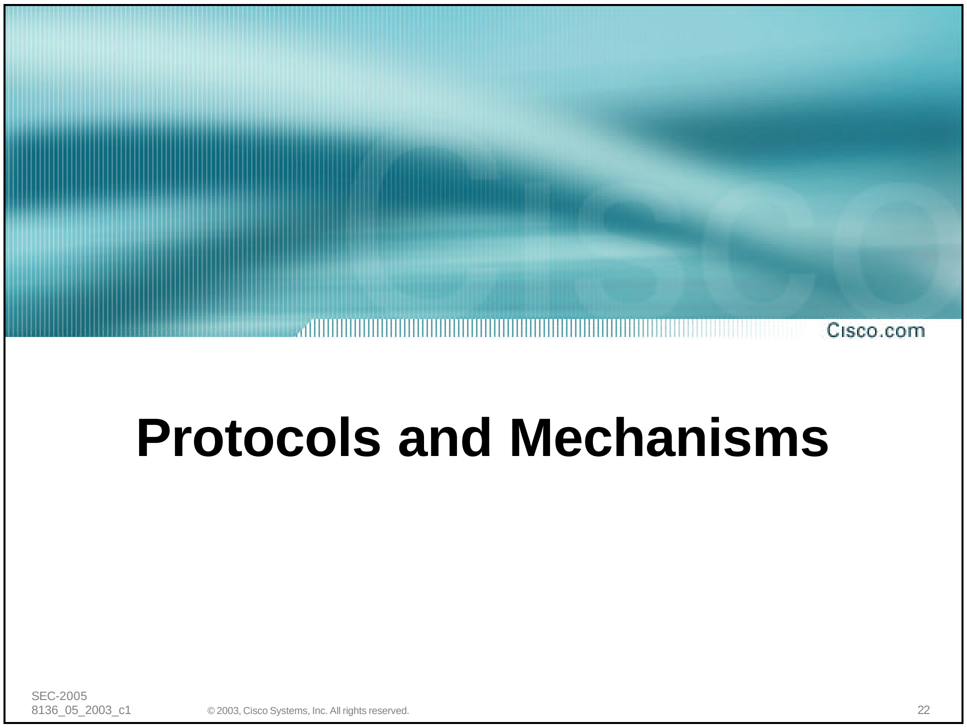
Authentication Successful

Policy Instructions

Actual Authentication Conversation Is between Client and Auth Server Using EAP; the Switch Is Just a Middleman, but Is Aware of What’s Going on

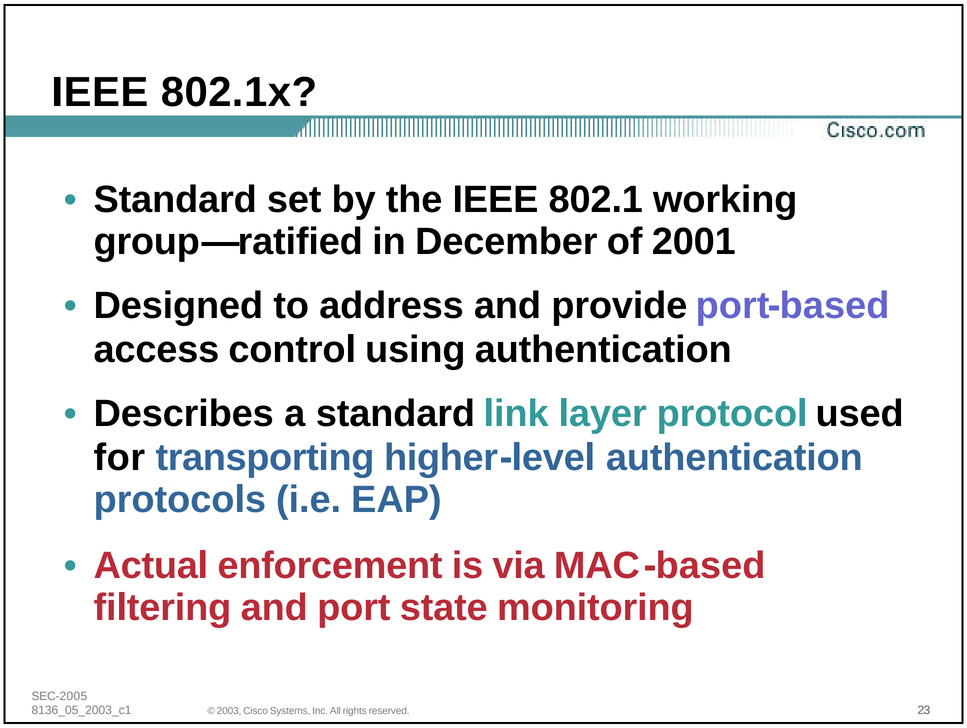
802.1x

RADIUS



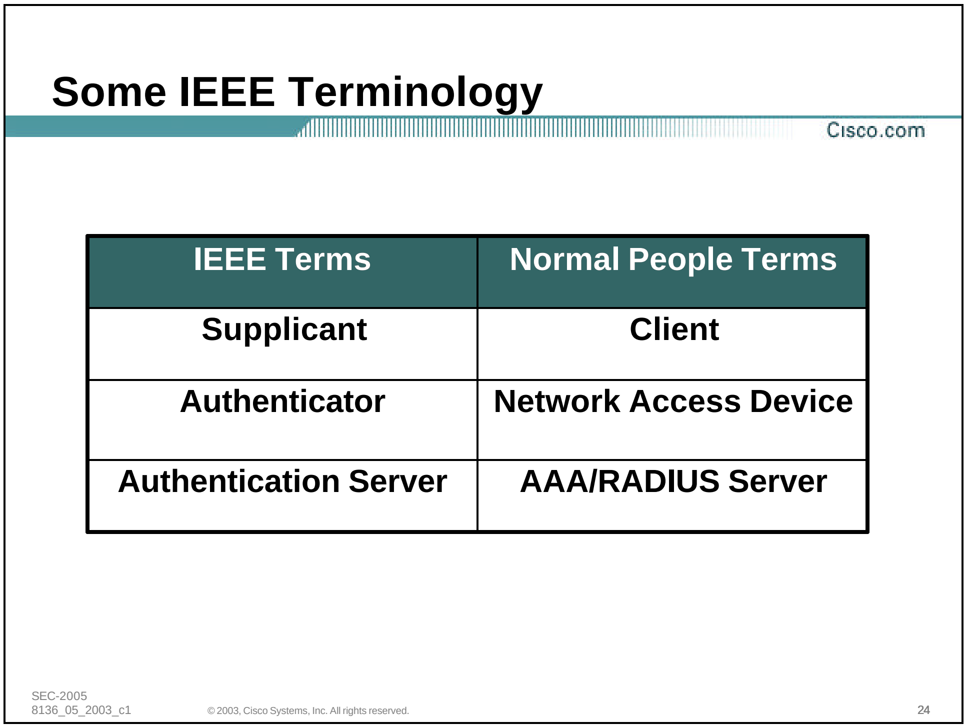
Cisco.com

Protocols and Mechanisms



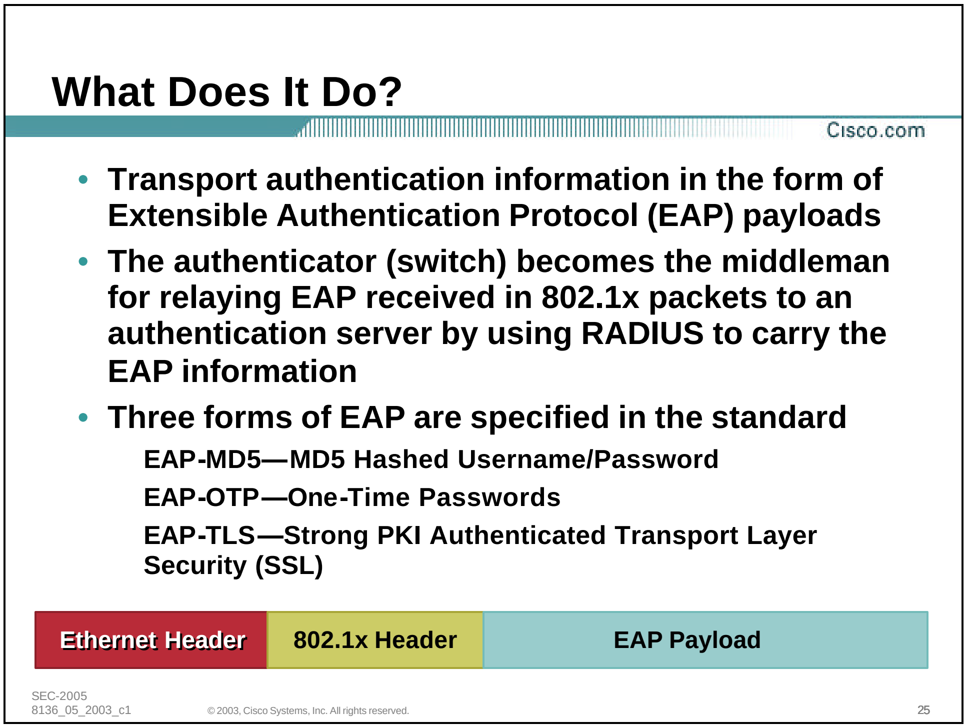
IEEE 802.1x?

- Standard set by the IEEE 802.1 working group—ratified in December of 2001
- Designed to address and provide port-based access control using authentication
- Describes a standard link layer protocol used for transporting higher-level authentication protocols (i.e. EAP)
- Actual enforcement is via MAC-based filtering and port state monitoring



Some IEEE Terminology

IEEE Terms	Normal People Terms
Supplicant	Client
Authenticator	Network Access Device
Authentication Server	AAA/RADIUS Server



What Does It Do?

Cisco.com

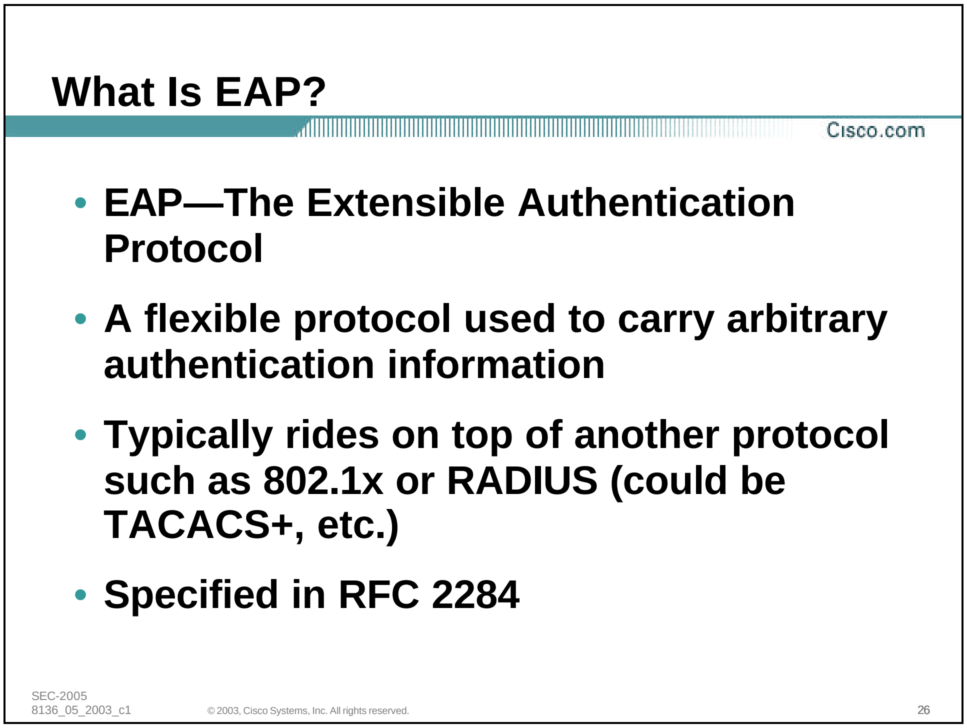
- Transport authentication information in the form of Extensible Authentication Protocol (EAP) payloads
- The authenticator (switch) becomes the middleman for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information
- Three forms of EAP are specified in the standard

  EAP-MD5—MD5 Hashed Username/Password

  EAP-OTP—One-Time Passwords

  EAP-TLS—Strong PKI Authenticated Transport Layer Security (SSL)

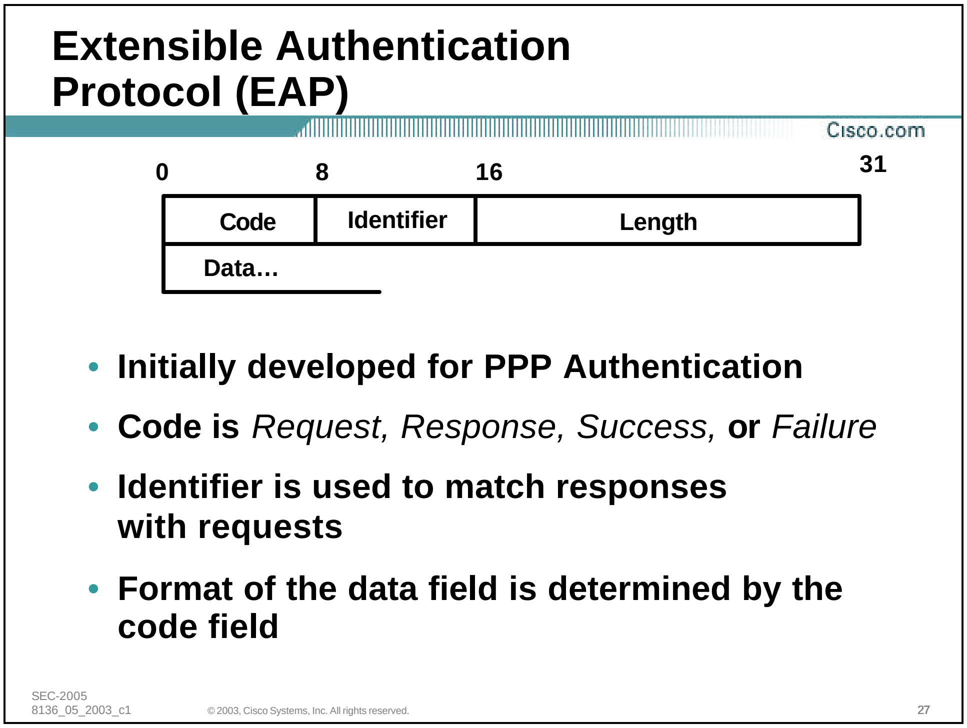
Ethernet Header	802.1x Header	EAP Payload



What Is EAP?

Cisco.com

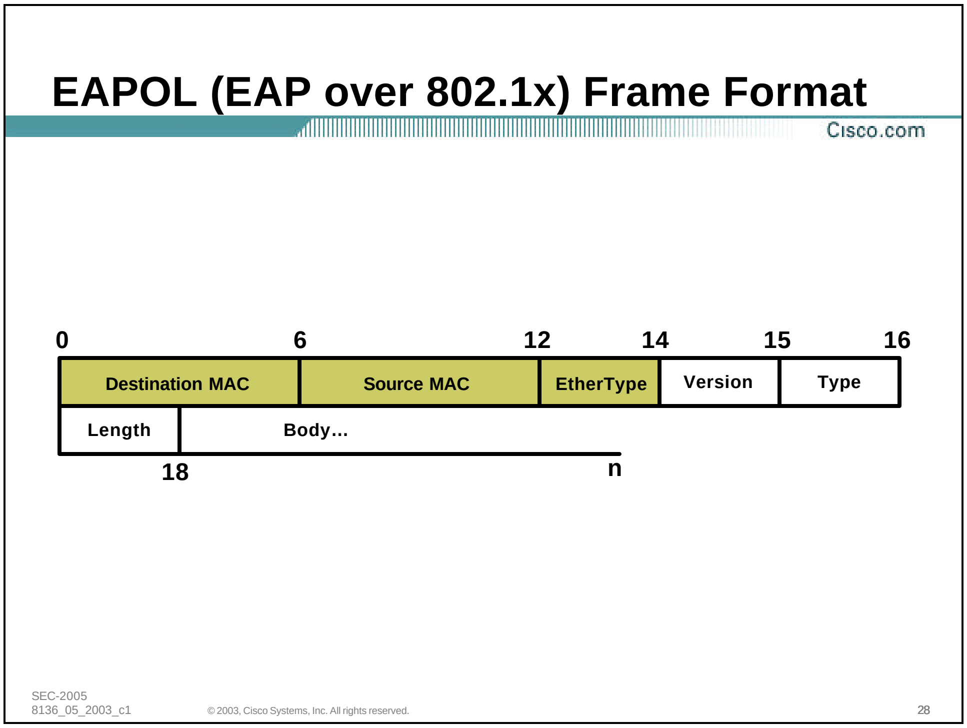
- EAP—The Extensible Authentication Protocol
- A flexible protocol used to carry arbitrary authentication information
- Typically rides on top of another protocol such as 802.1x or RADIUS (could be TACACS+, etc.)
- Specified in RFC 2284



Extensible Authentication Protocol (EAP)

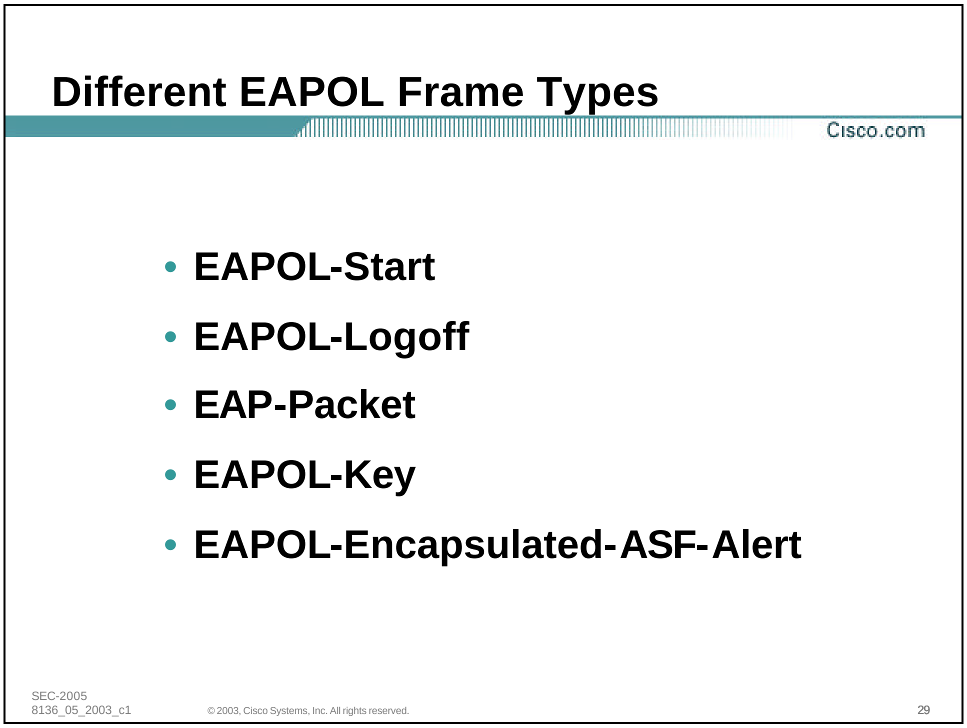
0	8	16	31
Code	Identifier	Length	
Data…			

- Initially developed for PPP Authentication
- Code is *Request, Response, Success,* or *Failure*
- Identifier is used to match responses with requests
- Format of the data field is determined by the code field



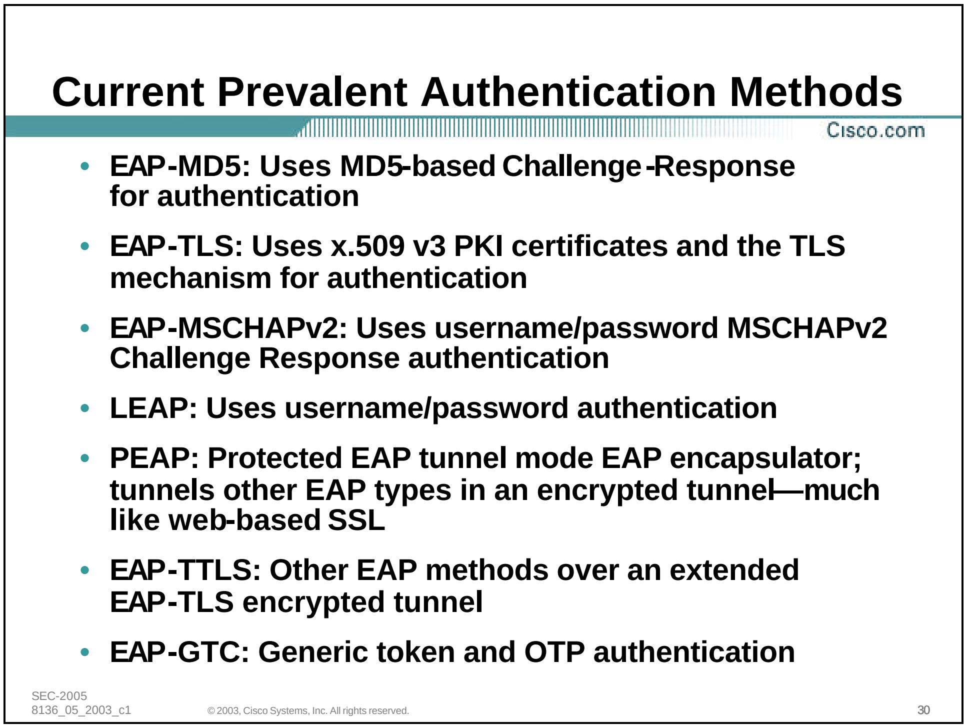
EAPOL (EAP over 802.1x) Frame Format

0	6	12	14	15	16
Destination MAC	Source MAC	EtherType	Version	Type	
Length	Body…				
18	n				



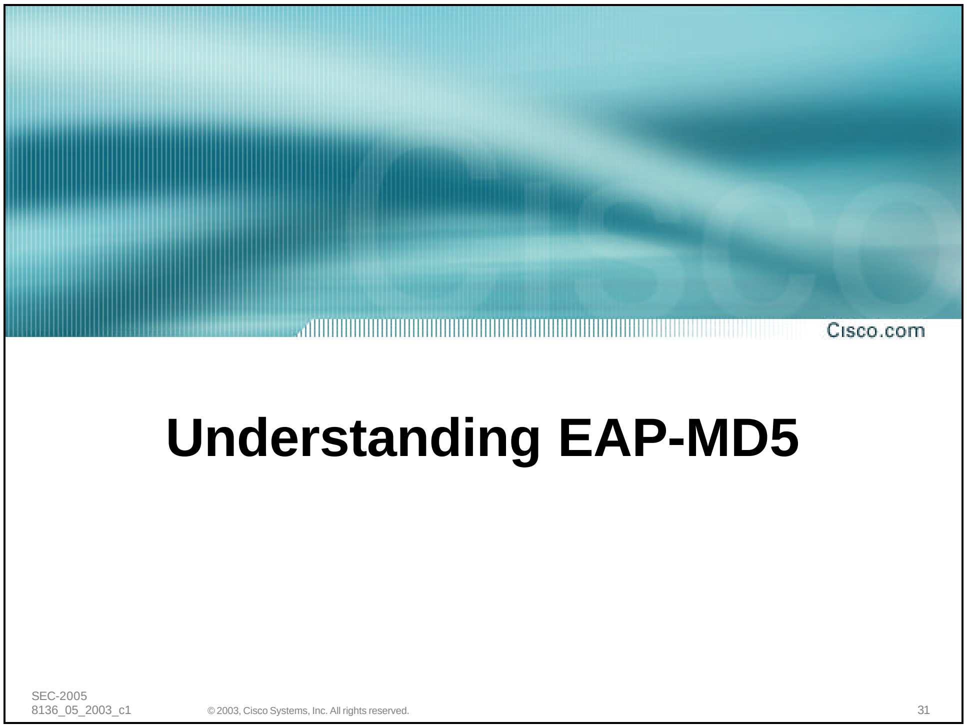
Different EAPOL Frame Types

- EAPOL-Start
- EAPOL-Logoff
- EAP-Packet
- EAPOL-Key
- EAPOL-Encapsulated-ASF-Alert

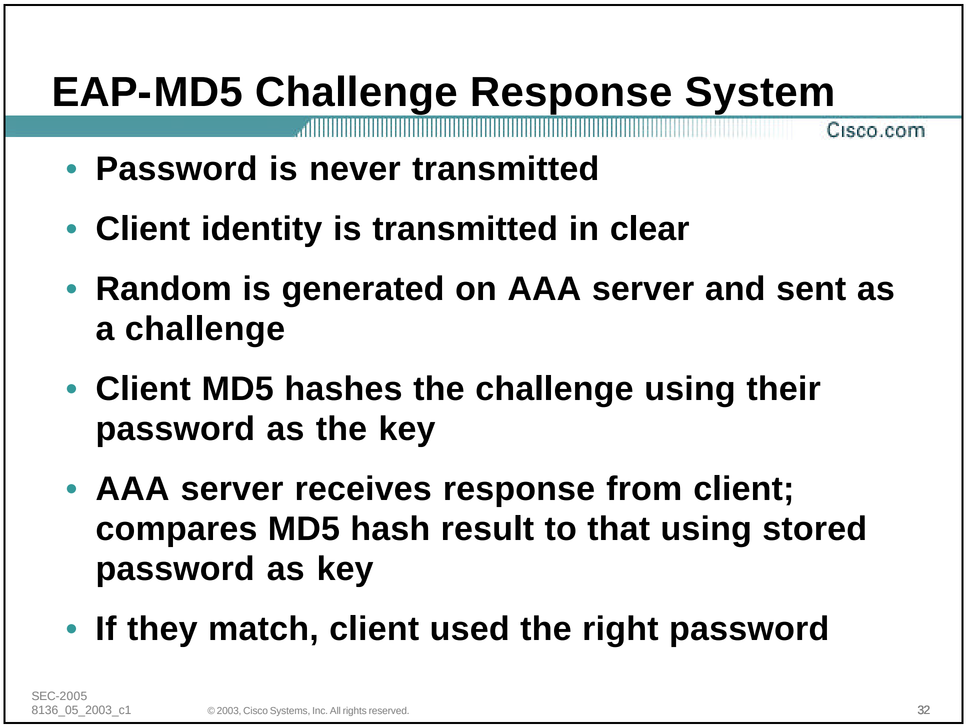


Current Prevalent Authentication Methods

- EAP-MD5: Uses MD5-based Challenge-Response for authentication
- EAP-TLS: Uses x.509 v3 PKI certificates and the TLS mechanism for authentication
- EAP-MSCHAPv2: Uses username/password MSCHAPv2 Challenge Response authentication
- LEAP: Uses username/password authentication
- PEAP: Protected EAP tunnel mode EAP encapsulator; tunnels other EAP types in an encrypted tunnel—much like web-based SSL
- EAP-TTLS: Other EAP methods over an extended EAP-TLS encrypted tunnel
- EAP-GTC: Generic token and OTP authentication



Understanding EAP-MD5

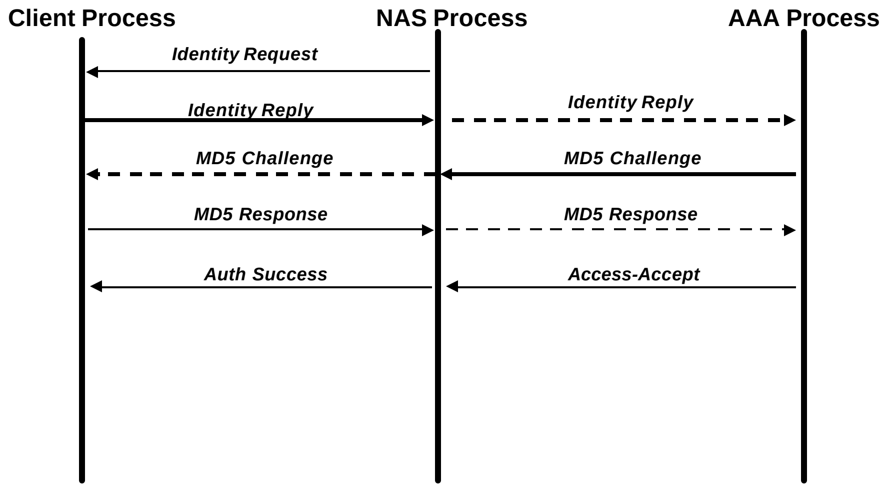


EAP-MD5 Challenge Response System

- Password is never transmitted
- Client identity is transmitted in clear
- Random is generated on AAA server and sent as a challenge
- Client MD5 hashes the challenge using their password as the key
- AAA server receives response from client; compares MD5 hash result to that using stored password as key
- If they match, client used the right password

EAP-MD5

Cisco.com



EAP-MD5 Pros and Cons

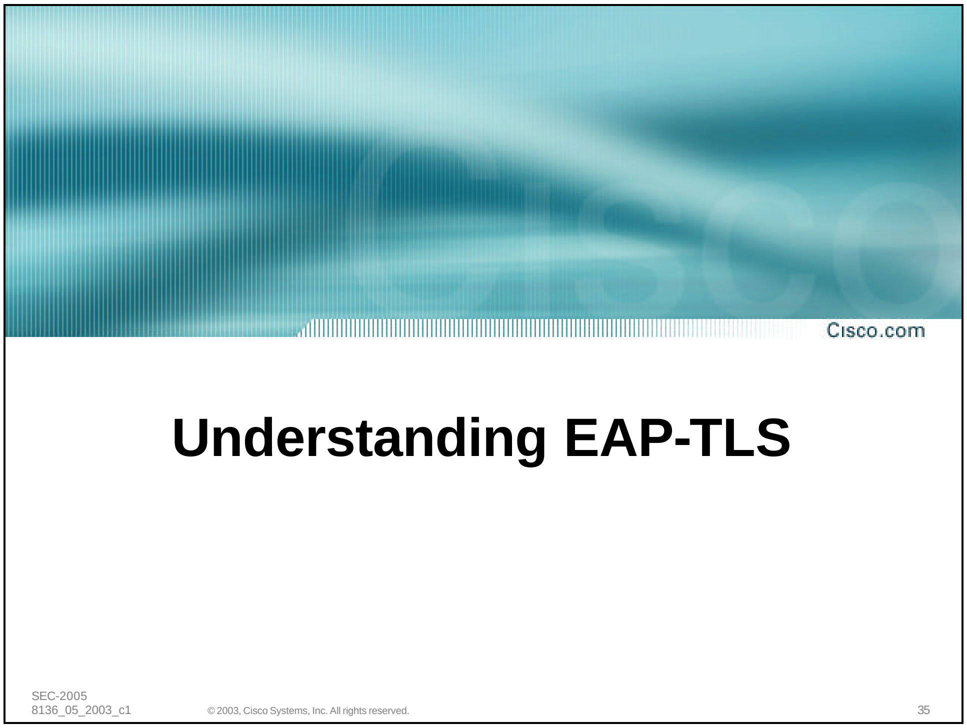
Cisco.com

Pros

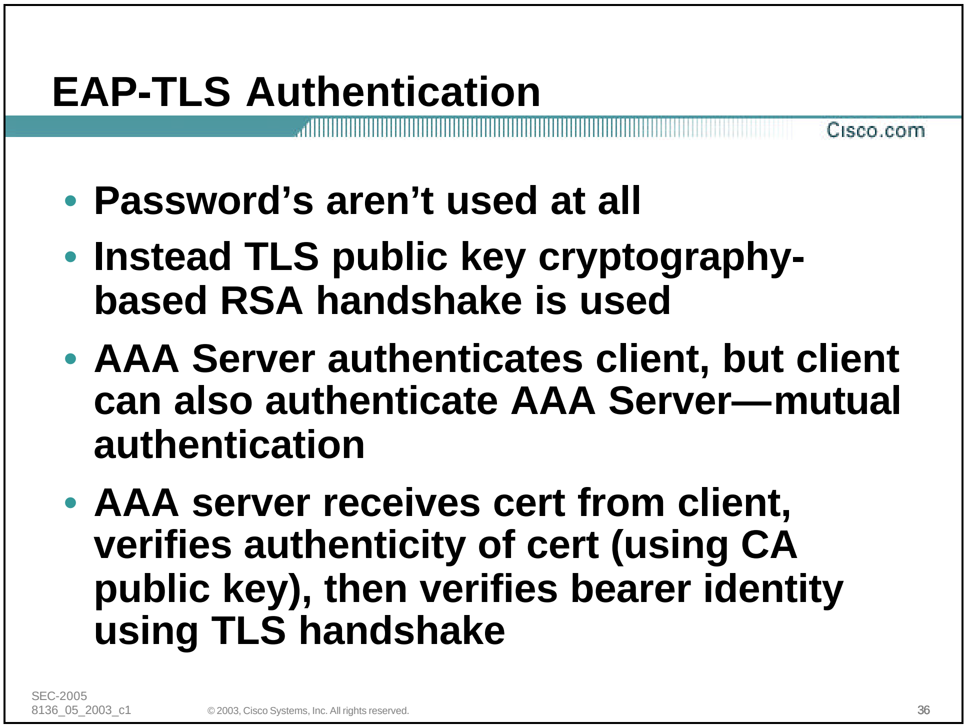
- Well supported—mandatory in all EAP implementations
- Simple username/ password scheme
- Lightweight on processing

Cons

- In theory, security weaknesses— requires the storage of plaintext or reversible passwords on the AAA server
- Single factor auth only
- Being phased out by MSFT

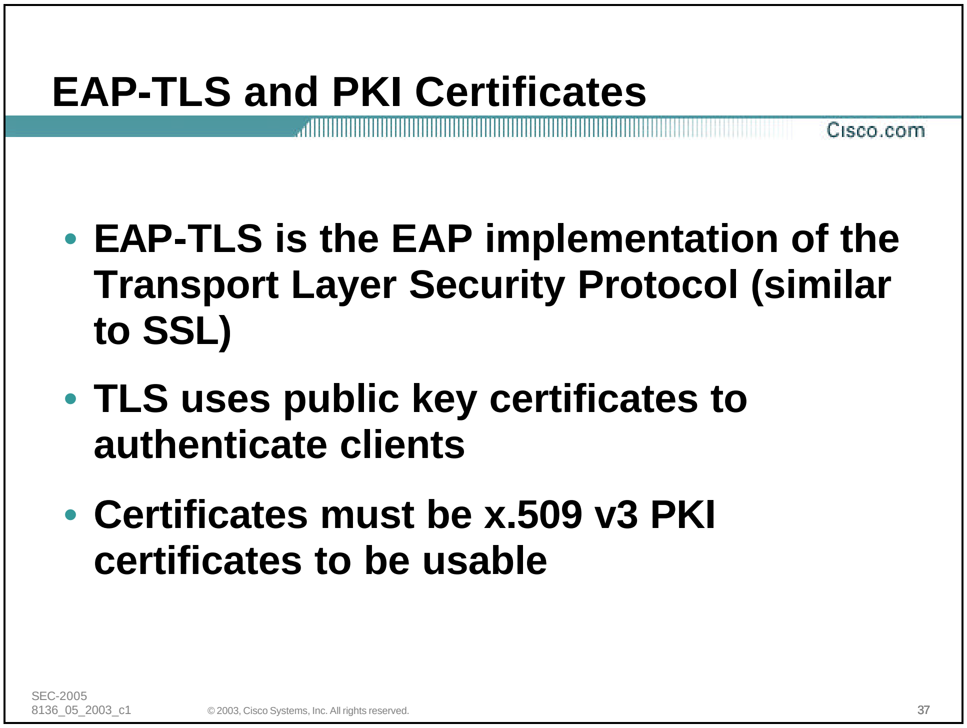


Understanding EAP-TLS



EAP-TLS Authentication

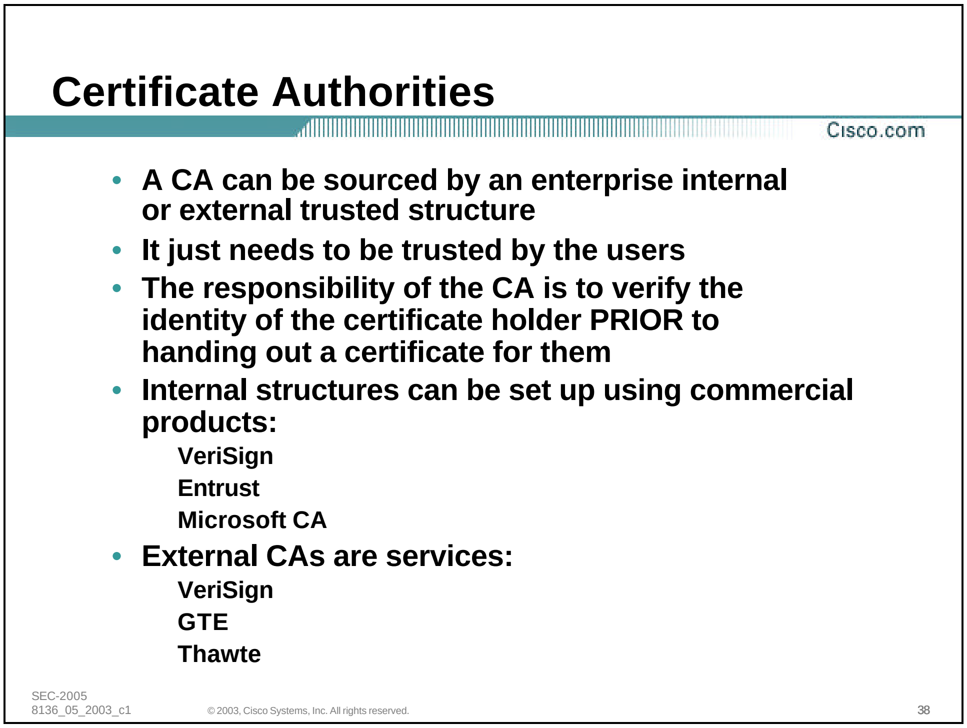
- Password's aren't used at all
- Instead TLS public key cryptography-based RSA handshake is used
- AAA Server authenticates client, but client can also authenticate AAA Server—mutual authentication
- AAA server receives cert from client, verifies authenticity of cert (using CA public key), then verifies bearer identity using TLS handshake



EAP-TLS and PKI Certificates

Cisco.com

- EAP-TLS is the EAP implementation of the Transport Layer Security Protocol (similar to SSL)
- TLS uses public key certificates to authenticate clients
- Certificates must be x.509 v3 PKI certificates to be usable



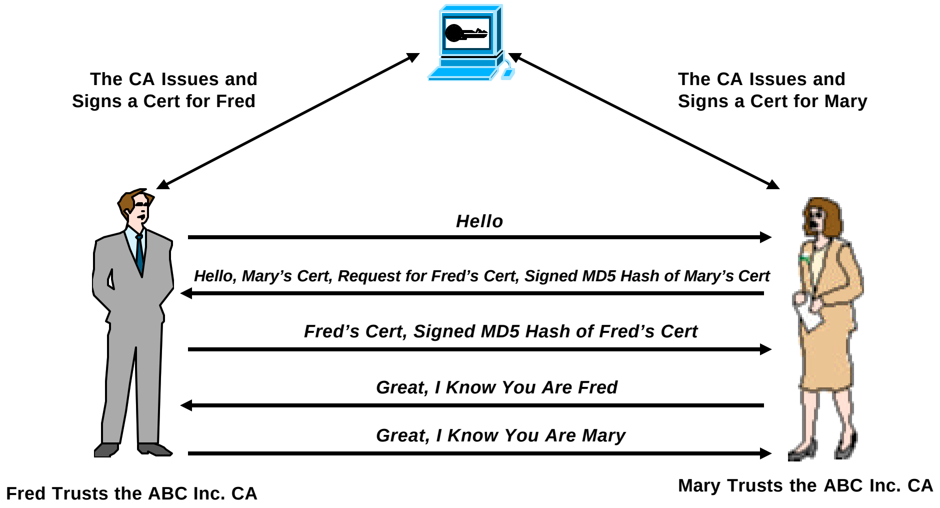
Certificate Authorities

Cisco.com

- A CA can be sourced by an enterprise internal or external trusted structure
- It just needs to be trusted by the users
- The responsibility of the CA is to verify the identity of the certificate holder PRIOR to handing out a certificate for them
- Internal structures can be set up using commercial products:
  VeriSign
  Entrust
  Microsoft CA
- External CAs are services:
  VeriSign
  GTE
  Thawte

The TLS Authentication Model (RSA-Based)

Cisco.com



The CA Issues and Signs a Cert for Fred

The CA Issues and Signs a Cert for Mary

Hello

Hello, Mary's Cert, Request for Fred's Cert, Signed MD5 Hash of Mary's Cert

Fred's Cert, Signed MD5 Hash of Fred's Cert

Great, I Know You Are Fred

Great, I Know You Are Mary

Fred Trusts the ABC Inc. CA

Mary Trusts the ABC Inc. CA

How Fred Authenticates Mary

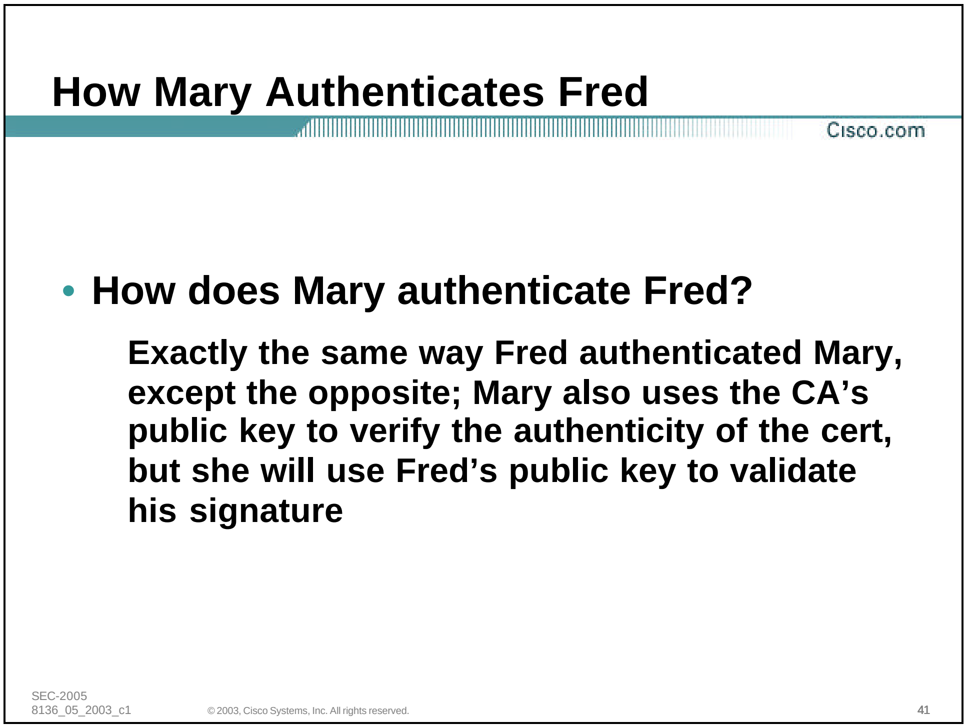
Cisco.com

- How does Fred Authenticate Mary?

  Mary's cert is signed by the ABC Inc. CA's private key. Fred should already have a copy of ABC Inc. CA's public key. He can use that to verify the validity of the cert by performing a digital signature check with the CA's public key.

- But how does Fred know that the entity that presented the cert is really Mary, and not someone with a copy of Mary's cert?

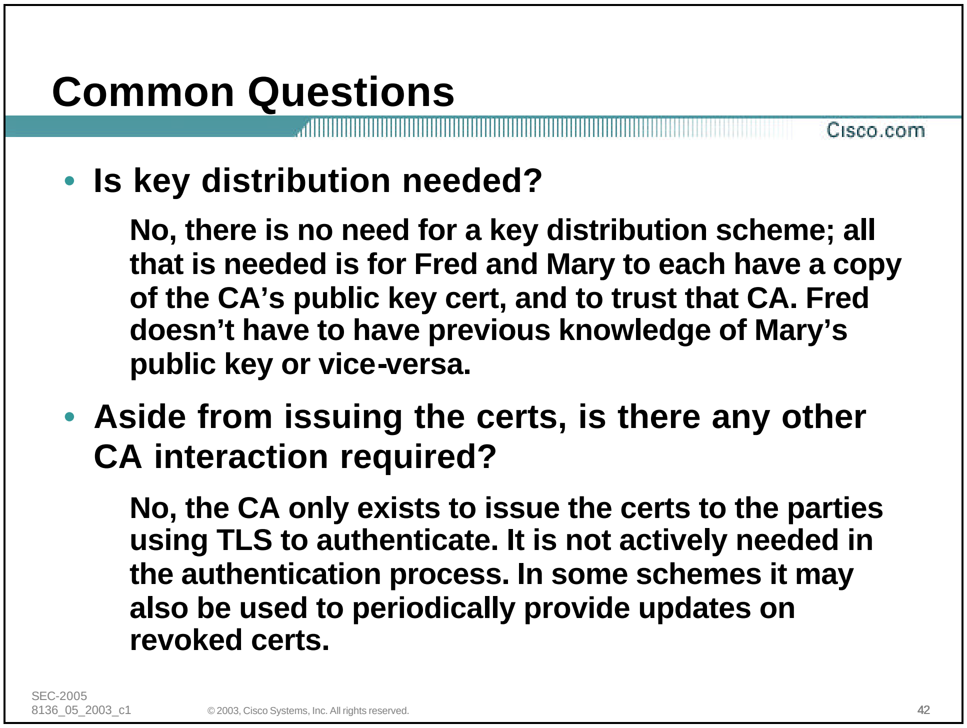
  At the end of Mary's reply, Mary includes an MD5 hash of her cert and some other information unique to this communication session, that is signed with her private key. Fred uses the public key contained in the cert to verify the signature by the private key. If this works, he can now believe that the presenter of the cert with whom he is speaking to is also the bearer of the correct private key, meaning, by inference that the other person is indeed Mary.



How Mary Authenticates Fred

- How does Mary authenticate Fred?

  Exactly the same way Fred authenticated Mary, except the opposite; Mary also uses the CA’s public key to verify the authenticity of the cert, but she will use Fred’s public key to validate his signature



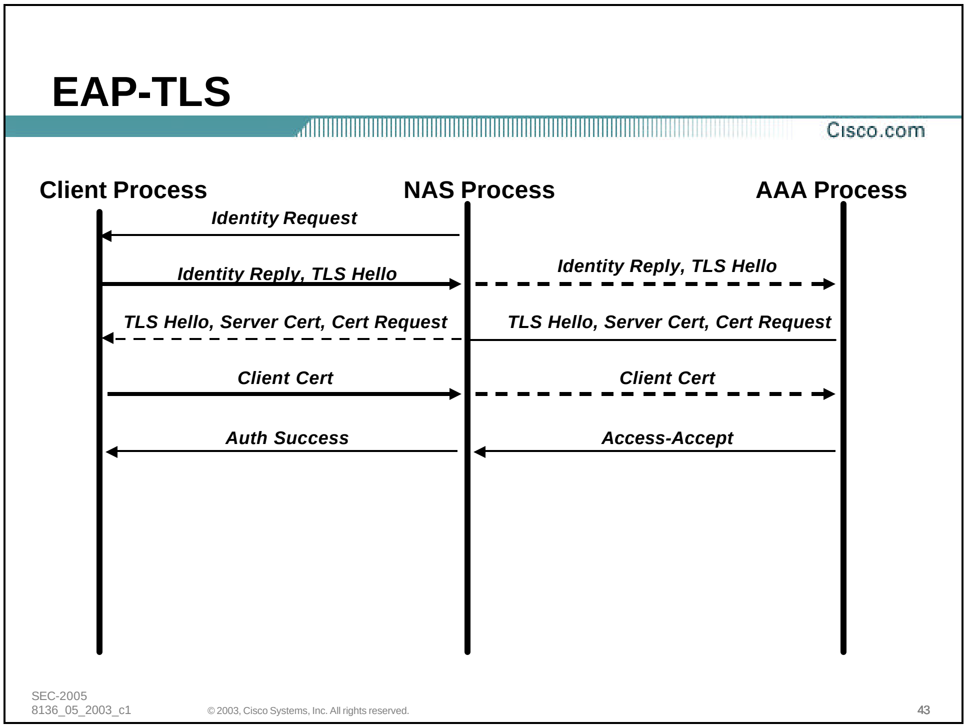
Common Questions

- Is key distribution needed?

  No, there is no need for a key distribution scheme; all that is needed is for Fred and Mary to each have a copy of the CA’s public key cert, and to trust that CA. Fred doesn’t have to have previous knowledge of Mary’s public key or vice-versa.

- Aside from issuing the certs, is there any other CA interaction required?

  No, the CA only exists to issue the certs to the parties using TLS to authenticate. It is not actively needed in the authentication process. In some schemes it may also be used to periodically provide updates on revoked certs.



EAP-TLS

Client Process

NAS Process

AAA Process

Identity Request

Identity Reply, TLS Hello

Identity Reply, TLS Hello

TLS Hello, Server Cert, Cert Request

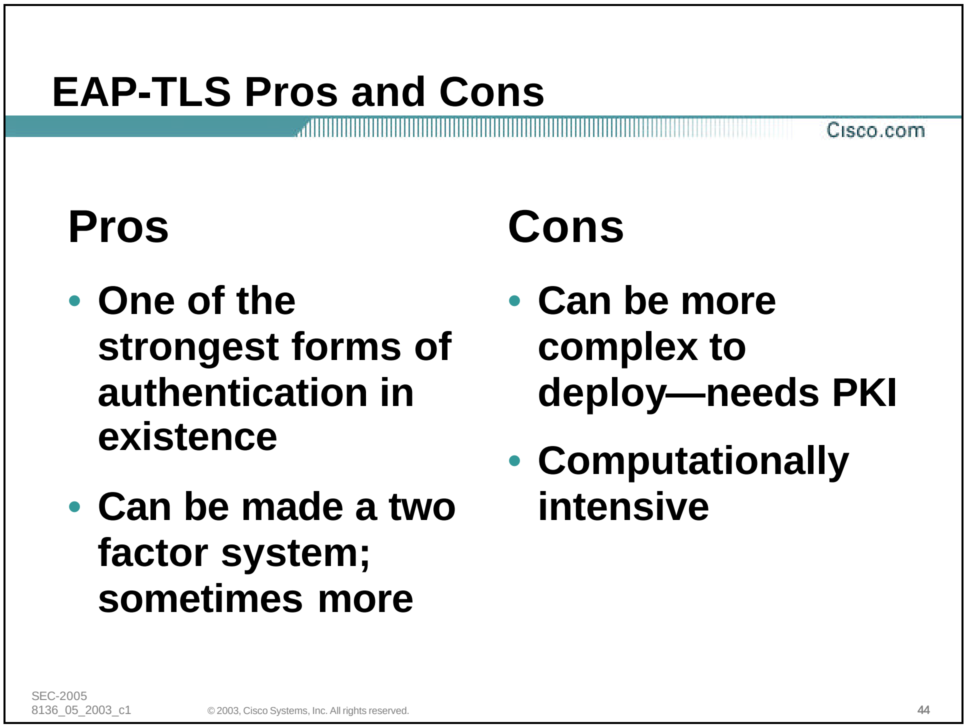
TLS Hello, Server Cert, Cert Request

Client Cert

Client Cert

Auth Success

Access-Accept



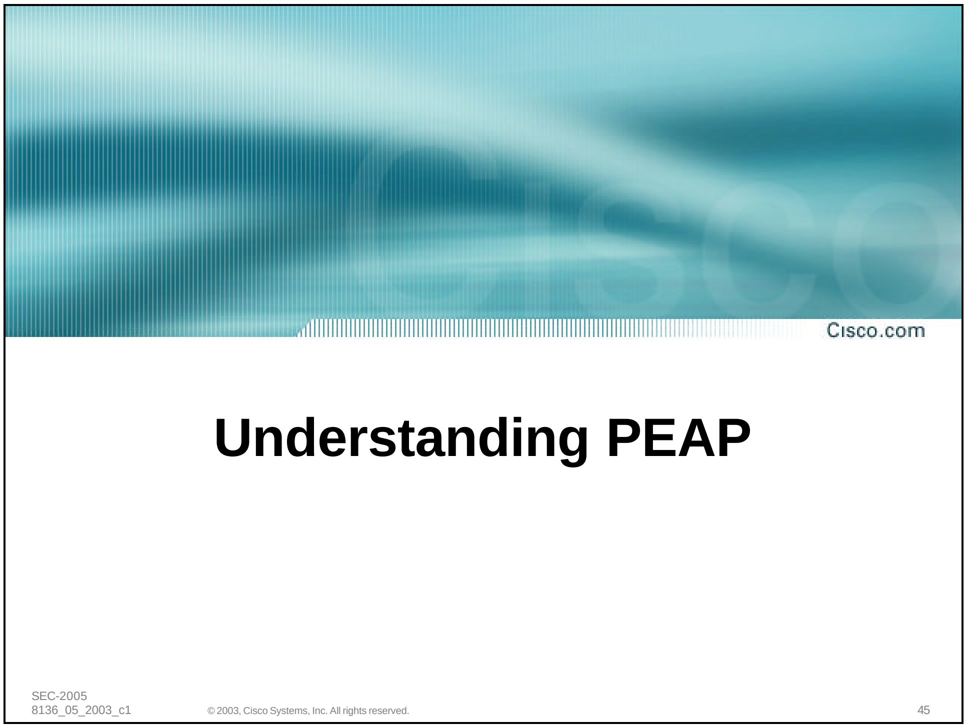
EAP-TLS Pros and Cons

Pros

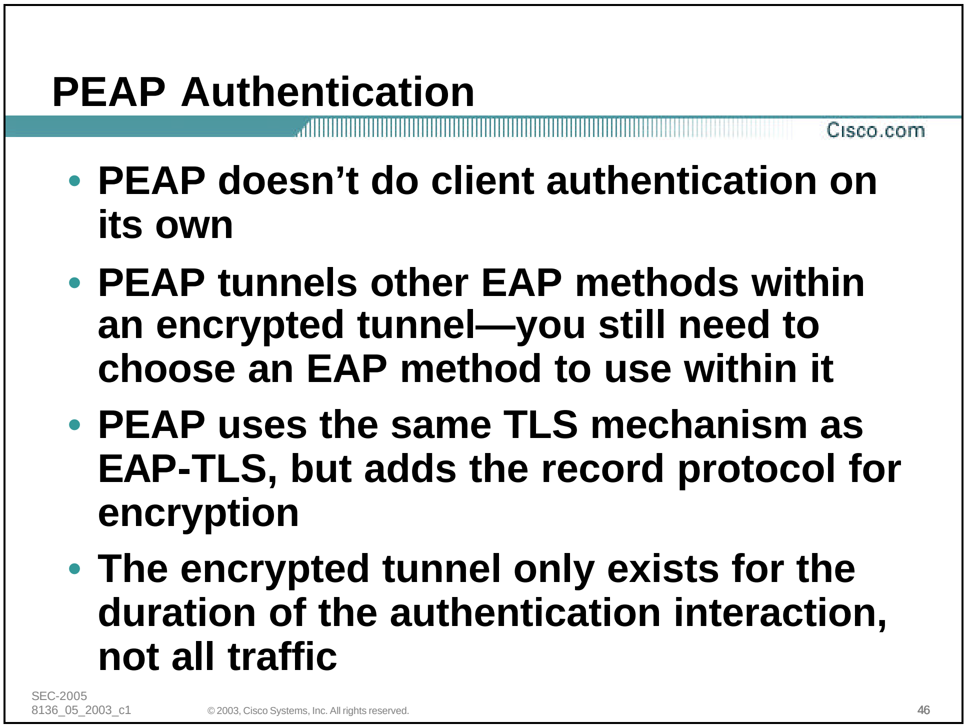
- One of the strongest forms of authentication in existence
- Can be made a two factor system; sometimes more

Cons

- Can be more complex to deploy—needs PKI
- Computationally intensive

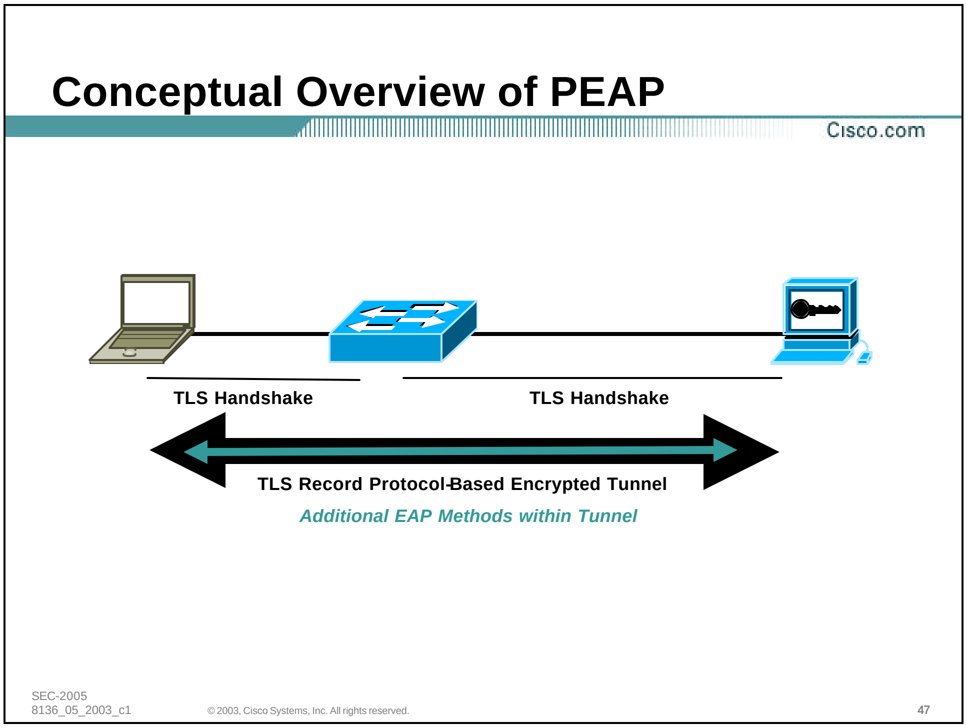


Understanding PEAP



PEAP Authentication

- PEAP doesn’t do client authentication on its own
- PEAP tunnels other EAP methods within an encrypted tunnel—you still need to choose an EAP method to use within it
- PEAP uses the same TLS mechanism as EAP-TLS, but adds the record protocol for encryption
- The encrypted tunnel only exists for the duration of the authentication interaction, not all traffic



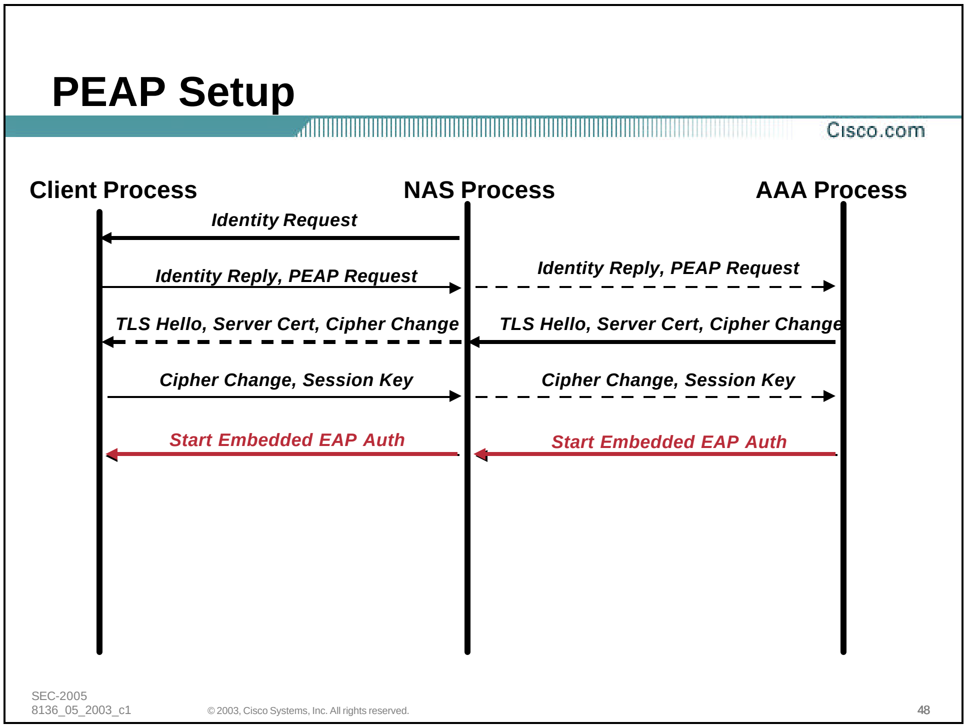
Conceptual Overview of PEAP

TLS Handshake

TLS Handshake

TLS Record Protocol-Based Encrypted Tunnel

Additional EAP Methods within Tunnel



PEAP Setup

Client Process

NAS Process

AAA Process

Identity Request

Identity Reply, PEAP Request

Identity Reply, PEAP Request

TLS Hello, Server Cert, Cipher Change

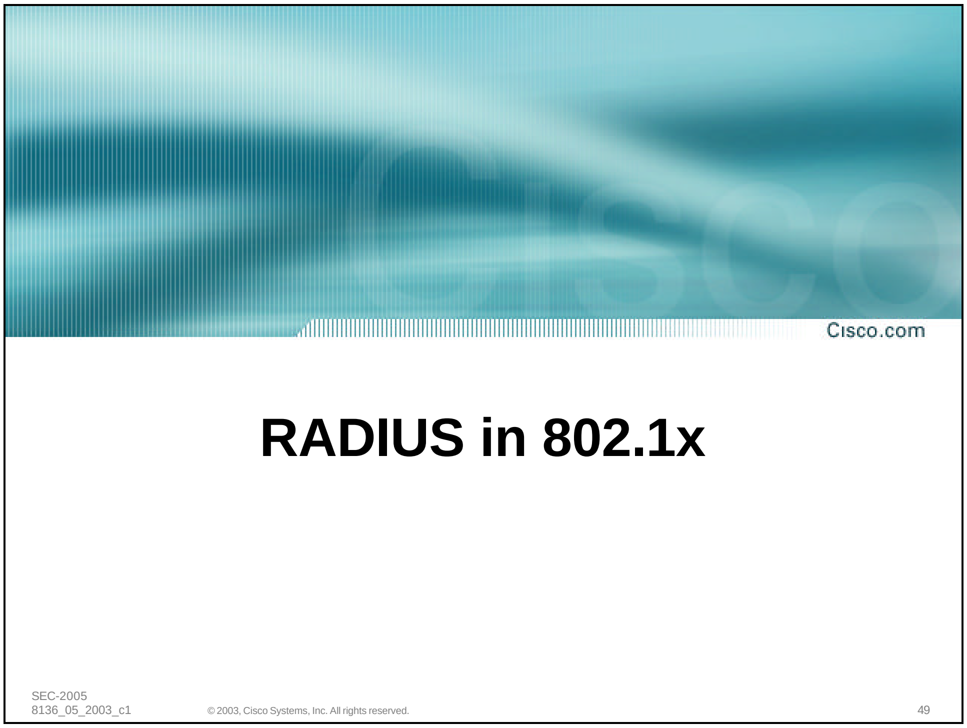
TLS Hello, Server Cert, Cipher Change

Cipher Change, Session Key

Cipher Change, Session Key

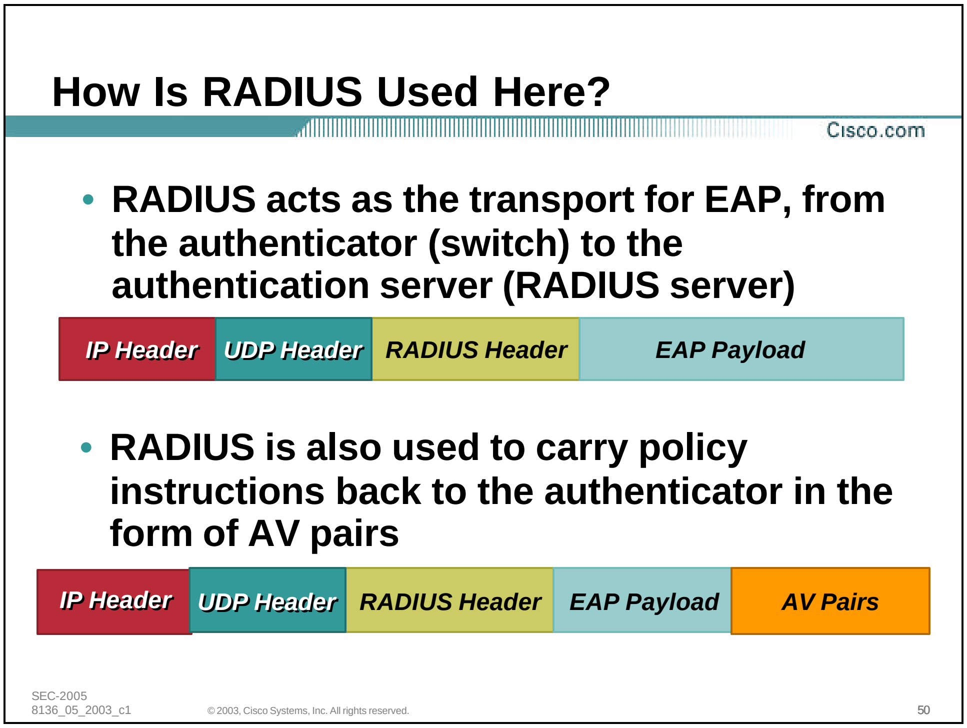
Start Embedded EAP Auth

Start Embedded EAP Auth



Cisco.com

RADIUS in 802.1x



How Is RADIUS Used Here?

Cisco.com

- RADIUS acts as the transport for EAP, from the authenticator (switch) to the authentication server (RADIUS server)

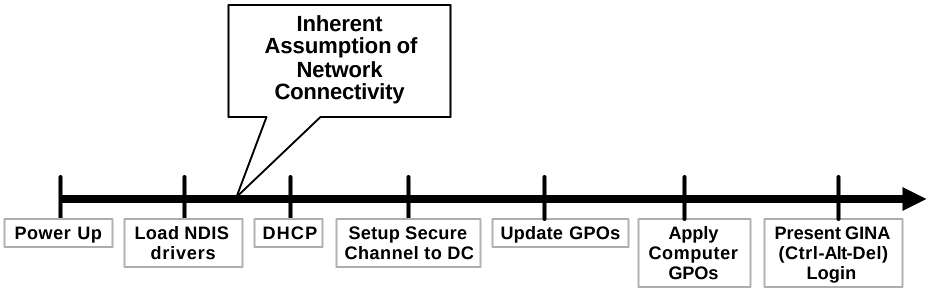
IP Header	*UDP Header*	*RADIUS Header*	*EAP Payload*

- RADIUS is also used to carry policy instructions back to the authenticator in the form of AV pairs

IP Header	*UDP Header*	*RADIUS Header*	*EAP Payload*	*AV Pairs*

Understanding Microsoft Environments

Windows Boot Cycle Overview


Inherent Assumption of Network Connectivity
Power Up
Load NDIS drivers
DHCP
Setup Secure Channel to DC
Update GPOs
Apply Computer GPOs
Present GINA (Ctrl-Alt-Del) Login

Microsoft and Machine Authentication

Cisco.com

- What is Machine Authentication?

  The ability of a Windows workstation to authenticate under it’s own identity, independent of the requirement for an interactive user session

- What is it used for?

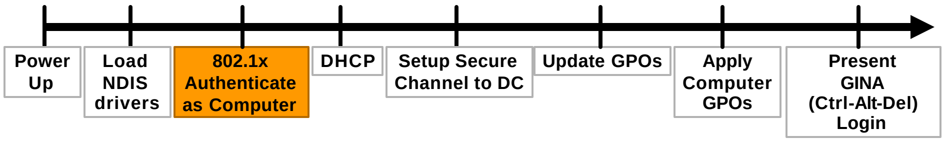
  Machine authentication is used at boot time by Windows OSes to authenticate and communicate with Windows Domain Controllers in order to pull down machine group policies

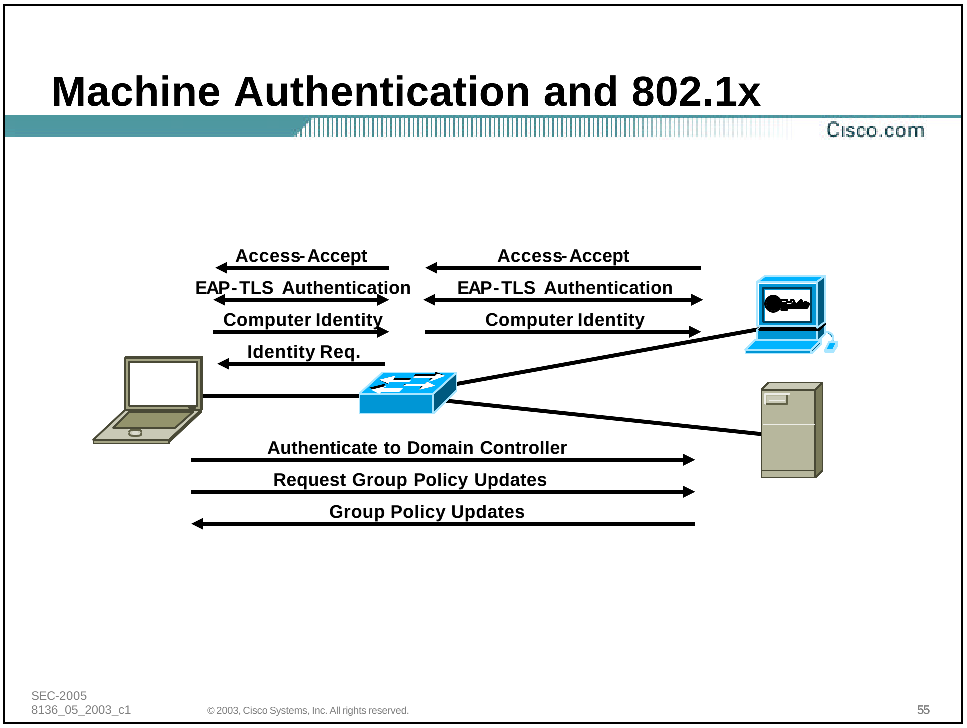
- Why do we care?

  Pre-802.1x this worked under the assumption that network connectivity was a given; post-802.1x the blocking of network access prior to 802.1x authentication breaks the machine-based group policy model—UNLESS the machine can authenticate using its own identity in 802.1x

Windows Machine Authentication

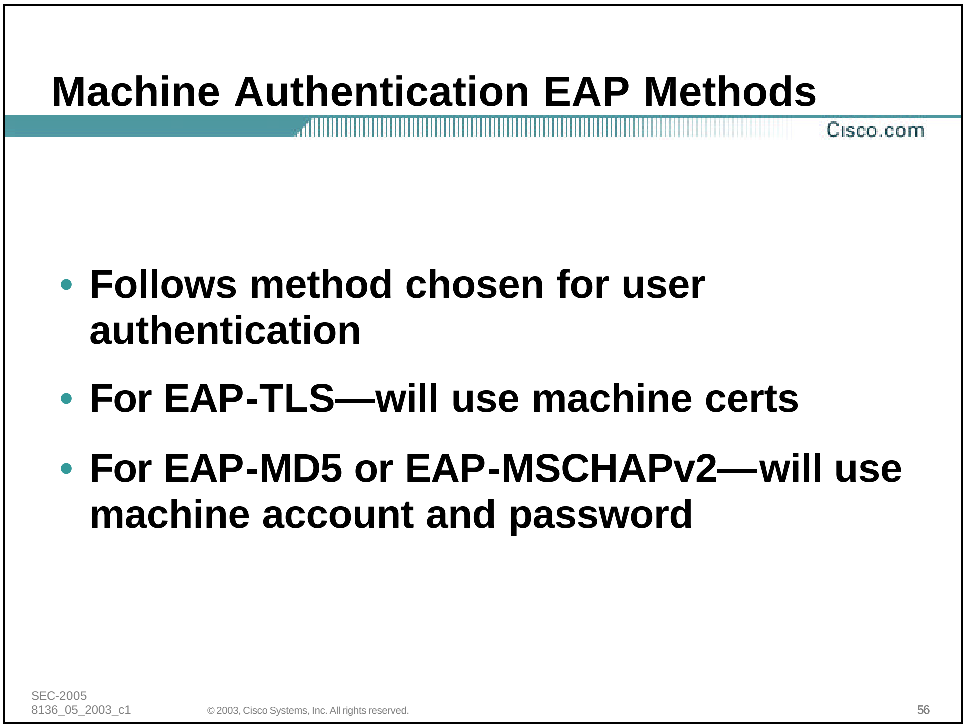
Cisco.com


Power Up
Load NDIS drivers
802.1x Authenticate as Computer
DHCP
Setup Secure Channel to DC
Update GPOs
Apply Computer GPOs
Present GINA (Ctrl-Alt-Del) Login



Machine Authentication and 802.1x

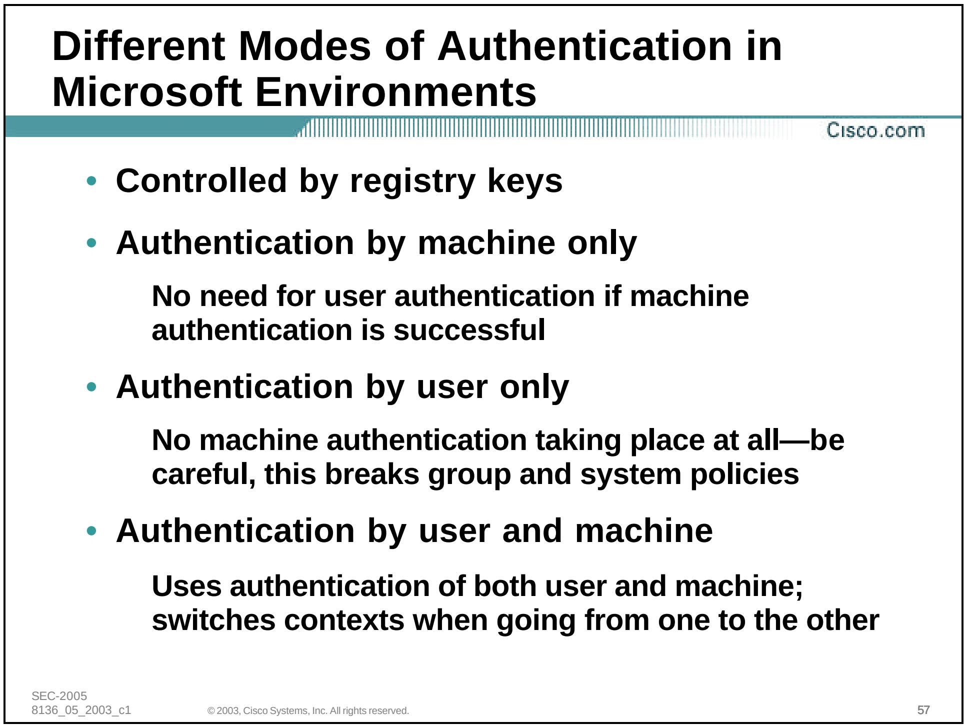
Cisco.com



Machine Authentication EAP Methods

Cisco.com

- Follows method chosen for user authentication
- For EAP-TLS—will use machine certs
- For EAP-MD5 or EAP-MSCHAPv2—will use machine account and password



Different Modes of Authentication in Microsoft Environments

- Controlled by registry keys
- Authentication by machine only

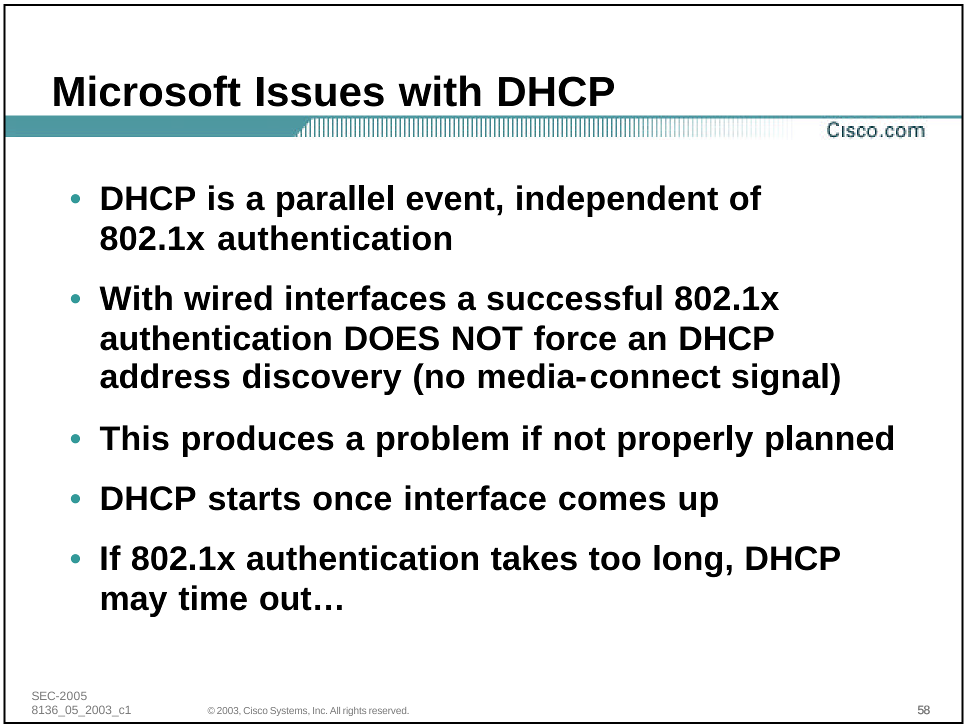
  No need for user authentication if machine authentication is successful

- Authentication by user only

  No machine authentication taking place at all—be careful, this breaks group and system policies

- Authentication by user and machine

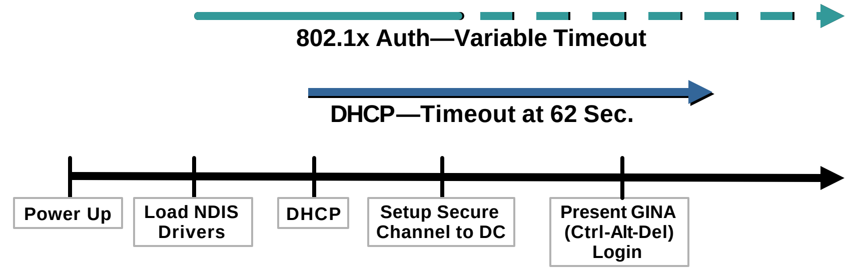
  Uses authentication of both user and machine; switches contexts when going from one to the other



Microsoft Issues with DHCP

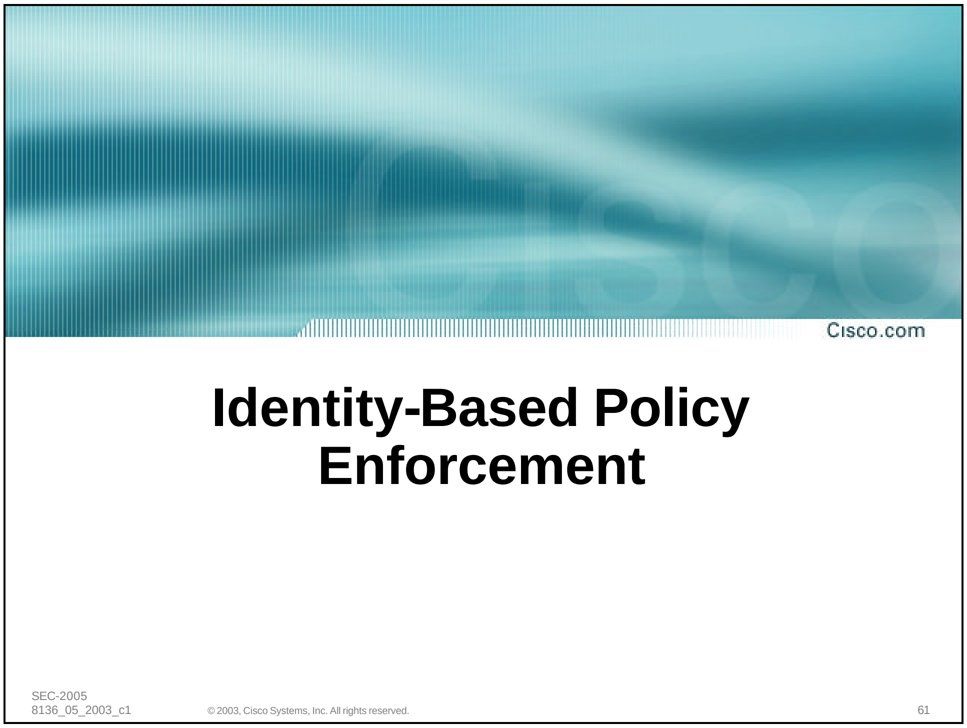
- DHCP is a parallel event, independent of 802.1x authentication
- With wired interfaces a successful 802.1x authentication DOES NOT force an DHCP address discovery (no media-connect signal)
- This produces a problem if not properly planned
- DHCP starts once interface comes up
- If 802.1x authentication takes too long, DHCP may time out…

DHCP Timeout Problem

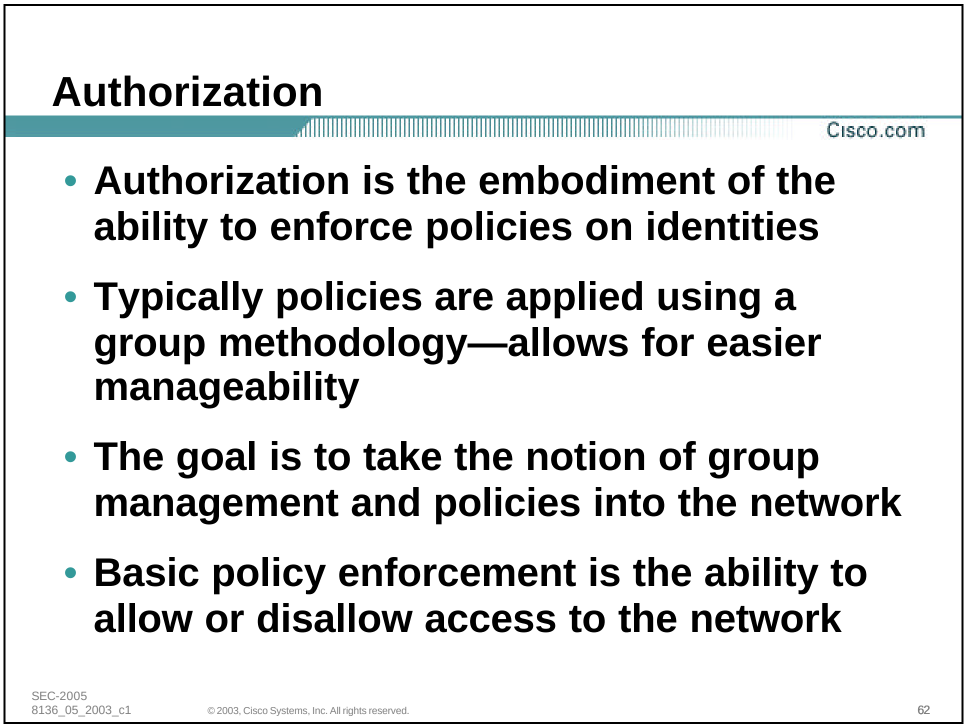

802.1x Auth—Variable Timeout
DHCP—Timeout at 62 Sec.
Power Up
Load NDIS Drivers
DHCP
Setup Secure Channel to DC
Present GINA (Ctrl-Alt-Del) Login

How to Address DHCP Timeout with 802.1x?

- Use machine authentication—this allows the initial machine authentication to obtain an IP address
- Force an IP address renewal—using a script, using a service, disconnect/ reconnect interface
- Don’t plug in Ethernet interface until you are ready to log in

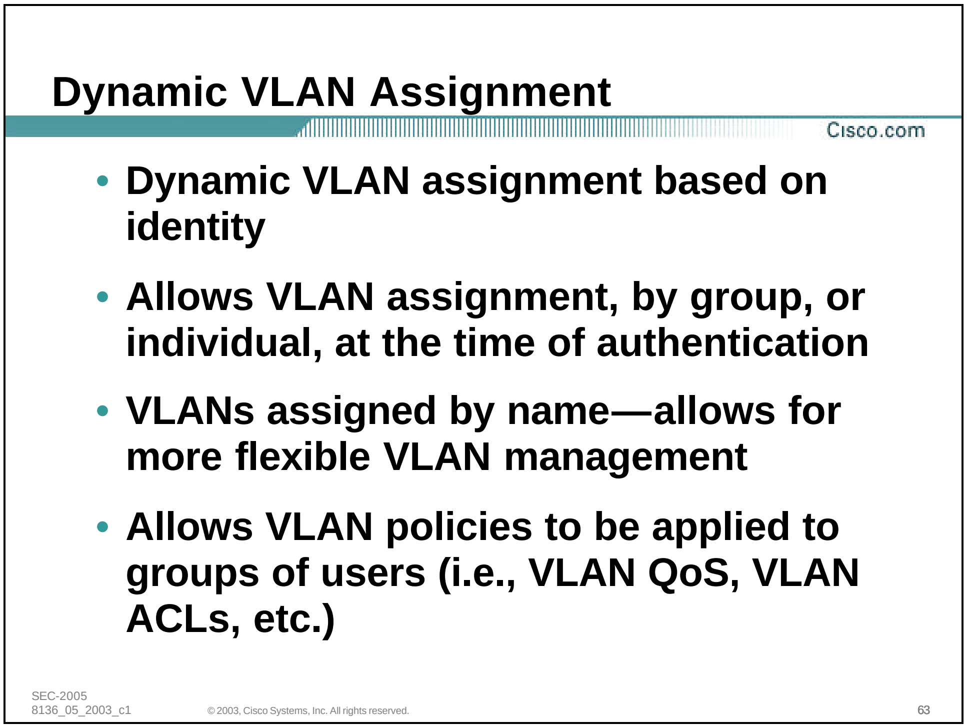


Identity-Based Policy Enforcement



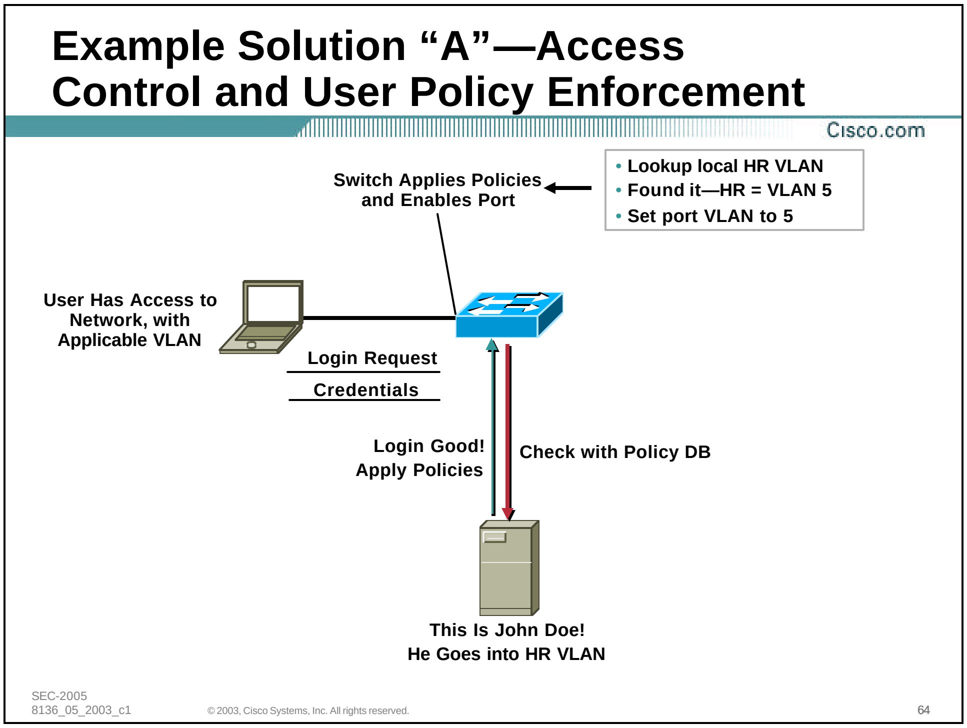
Authorization

- Authorization is the embodiment of the ability to enforce policies on identities
- Typically policies are applied using a group methodology—allows for easier manageability
- The goal is to take the notion of group management and policies into the network
- Basic policy enforcement is the ability to allow or disallow access to the network



Dynamic VLAN Assignment

- Dynamic VLAN assignment based on identity
- Allows VLAN assignment, by group, or individual, at the time of authentication
- VLANs assigned by name—allows for more flexible VLAN management
- Allows VLAN policies to be applied to groups of users (i.e., VLAN QoS, VLAN ACLs, etc.)



Example Solution "A"—Access Control and User Policy Enforcement

Switch Applies Policies and Enables Port

- Lookup local HR VLAN
- Found it—HR = VLAN 5
- Set port VLAN to 5

User Has Access to Network, with Applicable VLAN

Login Request

Credentials

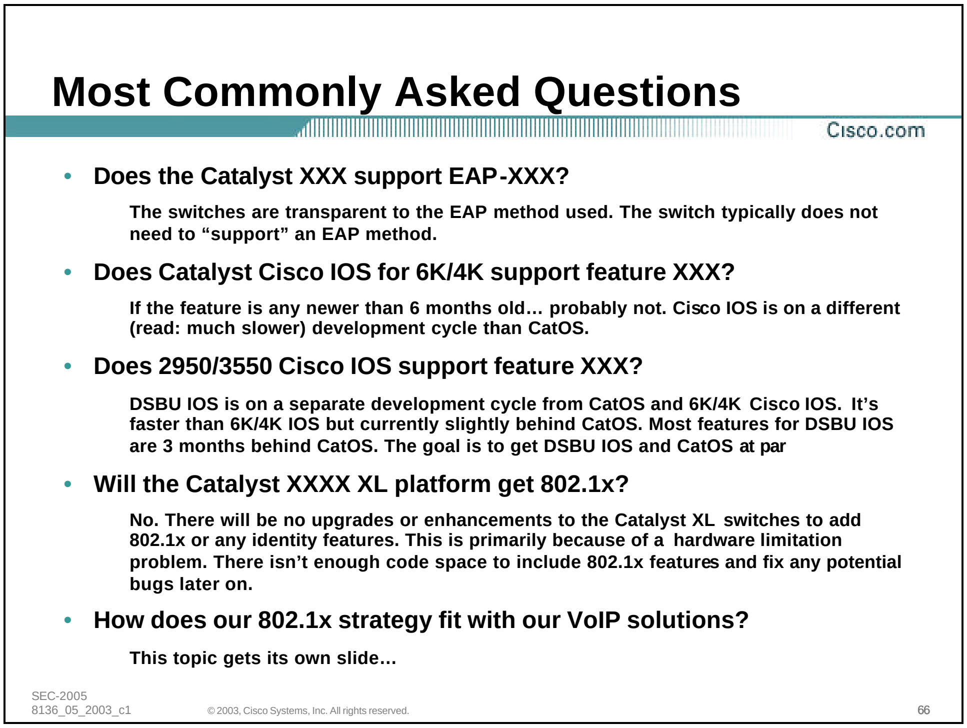
Login Good! Apply Policies

Check with Policy DB

This Is John Doe! He Goes into HR VLAN

Cisco.com

Commonly Asked Questions



Most Commonly Asked Questions

Cisco.com

- Does the Catalyst XXX support EAP-XXX?

  The switches are transparent to the EAP method used. The switch typically does not need to “support” an EAP method.

- Does Catalyst Cisco IOS for 6K/4K support feature XXX?

  If the feature is any newer than 6 months old… probably not. Cisco IOS is on a different (read: much slower) development cycle than CatOS.

- Does 2950/3550 Cisco IOS support feature XXX?

  DSBU IOS is on a separate development cycle from CatOS and 6K/4K Cisco IOS. It’s faster than 6K/4K IOS but currently slightly behind CatOS. Most features for DSBU IOS are 3 months behind CatOS. The goal is to get DSBU IOS and CatOS at par

- Will the Catalyst XXXX XL platform get 802.1x?

  No. There will be no upgrades or enhancements to the Catalyst XL switches to add 802.1x or any identity features. This is primarily because of a hardware limitation problem. There isn’t enough code space to include 802.1x features and fix any potential bugs later on.

- How does our 802.1x strategy fit with our VoIP solutions?

  This topic gets its own slide…

802.1x and VoIP

Cisco.com

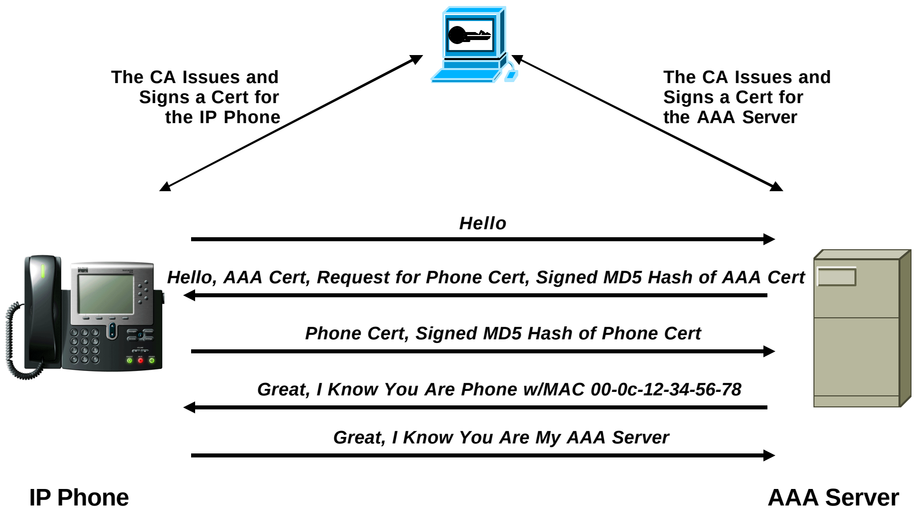
- Two phases of VoIP and 802.1x support

  802.1x with VVID—Unauthenticated Voice VLAN (VVID) access, Authenticated Data VLAN (PVID) access; this leaves voice no better than it is today, but allows 802.1x and VoIP to co-exist at the same time

  802.1x supplicants in IP phones—Committed for next gen phones (7965) work in progress for existing phones (7960)—not yet committed; phones will act as passthrough for PVID authentication

In the Context of IP Phones and 802.1x

Cisco.com



The CA Issues and Signs a Cert for the IP Phone

The CA Issues and Signs a Cert for the AAA Server

Hello

Hello, AAA Cert, Request for Phone Cert, Signed MD5 Hash of AAA Cert

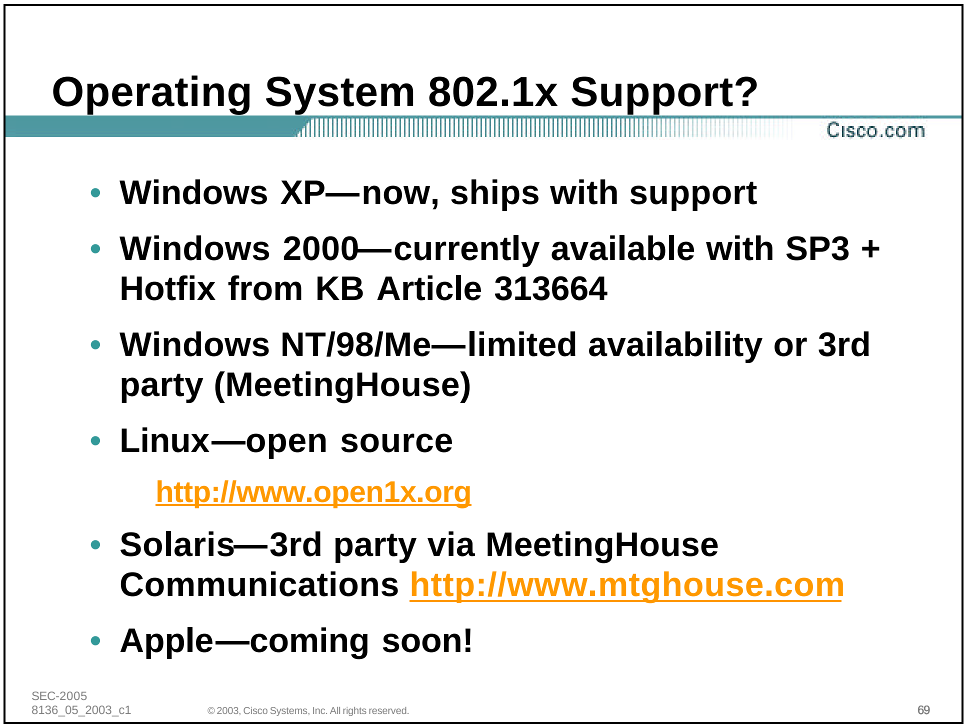
Phone Cert, Signed MD5 Hash of Phone Cert

Great, I Know You Are Phone w/MAC 00-0c-12-34-56-78

Great, I Know You Are My AAA Server

IP Phone

AAA Server

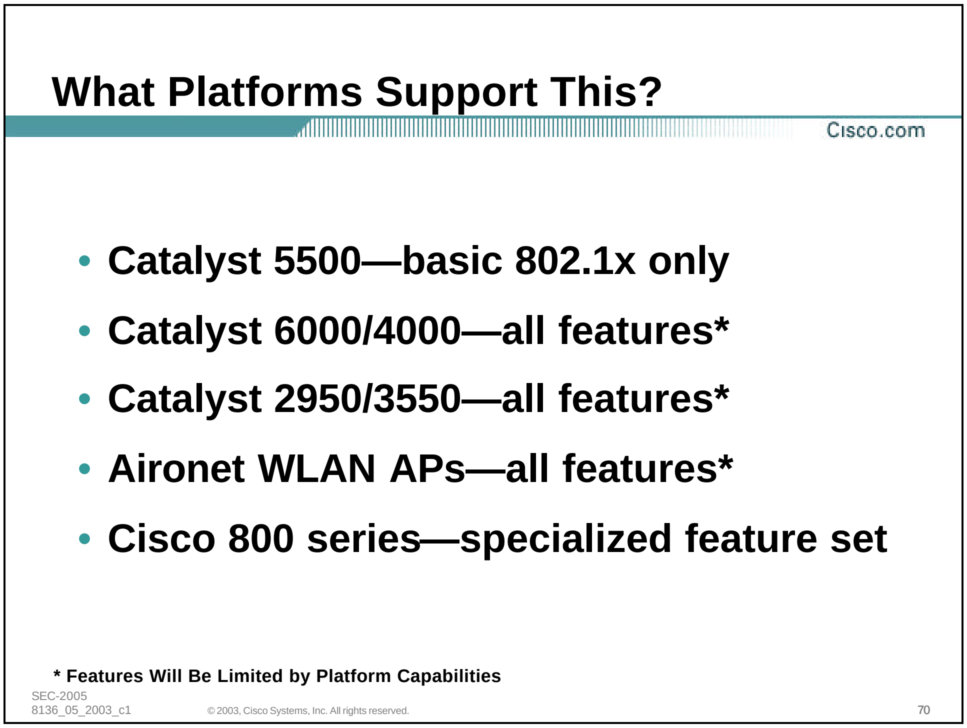


Operating System 802.1x Support?

Cisco.com

- Windows XP—now, ships with support
- Windows 2000—currently available with SP3 + Hotfix from KB Article 313664
- Windows NT/98/Me—limited availability or 3rd party (MeetingHouse)
- Linux—open source

  http://www.open1x.org
- Solaris—3rd party via MeetingHouse Communications http://www.mtghouse.com
- Apple—coming soon!



What Platforms Support This?

Cisco.com

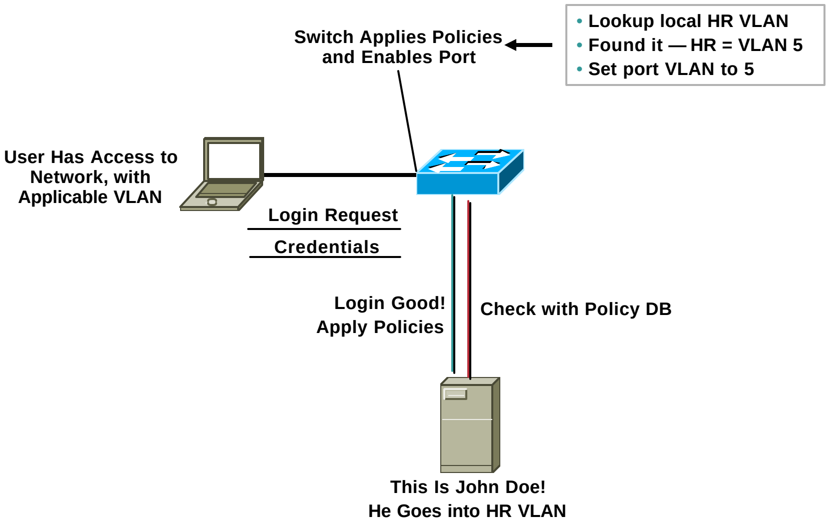
- Catalyst 5500—basic 802.1x only
- Catalyst 6000/4000—all features*
- Catalyst 2950/3550—all features*
- Aironet WLAN APs—all features*
- Cisco 800 series—specialized feature set

* Features Will Be Limited by Platform Capabilities

Deployment Example

Creating Value out of All the Pieces

Example Solution "A"—Access Control and User Policy Enforcement



- Lookup local HR VLAN
- Found it — HR = VLAN 5
- Set port VLAN to 5

Switch Applies Policies and Enables Port

User Has Access to Network, with Applicable VLAN

Login Request

Credentials

Login Good! Apply Policies

Check with Policy DB

This Is John Doe! He Goes into HR VLAN

Deployment Example Overview

Cisco.com

- Windows XP clients
- CiscoSecure ACS 3.2
- Authenticating to Active Directory
- Controlling access via switches
- Dynamically assigning VLANs based on group membership in AD
- Using username and password to authenticate via PEAP/EAP-MSCHAPv2

Scenario Dependencies

Cisco.com

- WinXP clients: require Service Pack 1 installed
- Windows 2000 server for ACS 3.2: requires all current service packs and patches
- CatOS switches: CatOS 7.5.1+
- Cisco IOS switches: Cisco IOS 12.1(EA1)13+
- Enterprise PKI (i.e. MS CA) or trusted 3rd party (i.e. Verisign) certificate for ACS

Cisco.com

Authentication Server Configuration

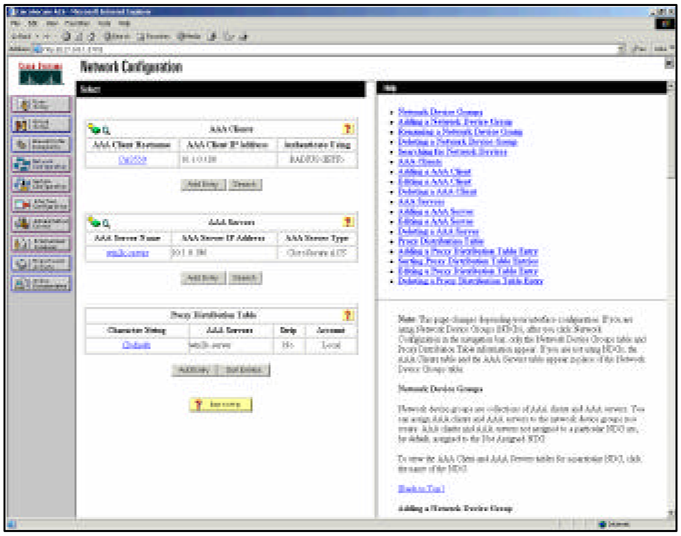
CiscoSecure ACS for Windows

CiscoSecure ACS Appliance

ACS Configuration

Adding the Network Access Device

Cisco.com



Network Configuration

Select

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
Cat3550	[illegible]	RADIUS (IETF)

AAA Servers		
AAA Server Name	AAA Server IP Address	AAA Server Type
smith-server	[illegible]	CiscoSecure ACS

Proxy Distribution Table			
Character String	AAA Servers	Strip	Account
(Default)	smith-server	No	Local

Help

- Network Device Groups
- Adding a Network Device Group
- Renaming a Network Device Group
- Deleting a Network Device Group
- Searching for Network Devices
- AAA Clients
- Adding a AAA Client
- Editing a AAA Client
- Deleting a AAA Client
- AAA Servers
- Adding a AAA Server
- Editing a AAA Server
- Deleting a AAA Server
- Proxy Distribution Table
- Adding a Proxy Distribution Table Entry
- Sorting Proxy Distribution Table Entries
- Editing a Proxy Distribution Table Entry
- Deleting a Proxy Distribution Table Entry

Note: This page changes depending on your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.

Network Device Groups

Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and AAA servers not assigned to a particular NDG are, by default, assigned to the (Not Assigned) NDG.

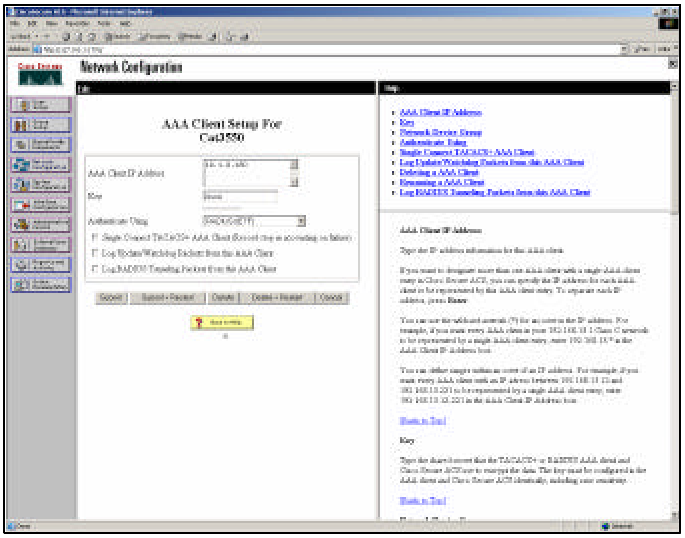
To view the AAA Client and AAA Server tables for a particular NDG, click the name of the NDG.

Back to Top

Adding a Network Device Group

ACS Configuration

Adding the Network Access Device



Network Configuration

AAA Client Setup For Cat3550

AAA Client IP Address

Key

Authenticate Using: RADIUS (IETF)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Deleting a AAA Client
- Renaming a AAA Client
- Log RADIUS Tunneling Packets from this AAA Client

AAA Client IP Address

Type the IP address information for this AAA client.

If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.

Back to Top

Key

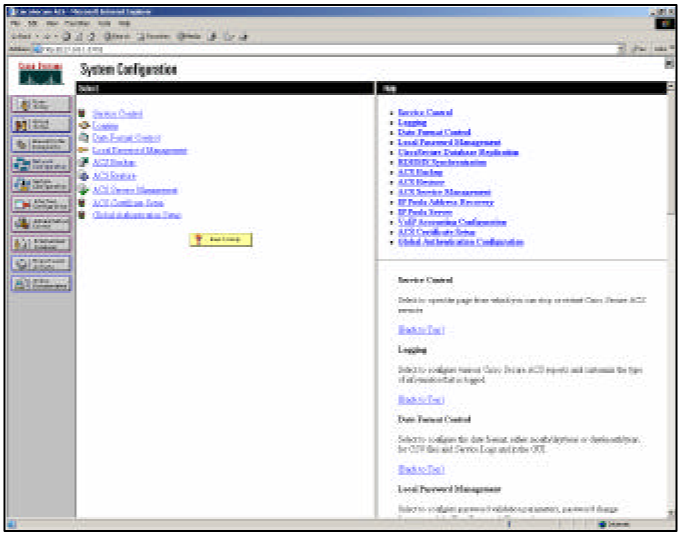
Type the shared secret that the TACACS+ or RADIUS AAA client and Cisco Secure ACS use to encrypt the data. The key must be configured in the AAA client and Cisco Secure ACS identically, including case sensitivity.

Back to Top

Network Device Group

ACS Configuration

Server Certificate Setup



System Configuration

- Service Control
- Logging
- Date Format Control
- Local Password Management
- ACS Backup
- ACS Restore
- ACS Service Management
- ACS Certificate Setup
- Global Authentication Setup

- Service Control
- Logging
- Date Format Control
- Local Password Management
- CiscoSecure Database Replication
- RDBMS Synchronization
- ACS Backup
- ACS Restore
- ACS Service Management
- IP Pools Address Recovery
- IP Pools Server
- VoIP Accounting Configuration
- ACS Certificate Setup
- Global Authentication Configuration

Service Control

Select to open the page from which you can stop or restart Cisco Secure ACS services.

Back to Top

Logging

Select to configure various Cisco Secure ACS reports and customize the type of information that is logged.

Back to Top

Date Format Control

Select to configure the date format, either month/day/year or day/month/year, for CSV files and Service Logs and in the GUI.

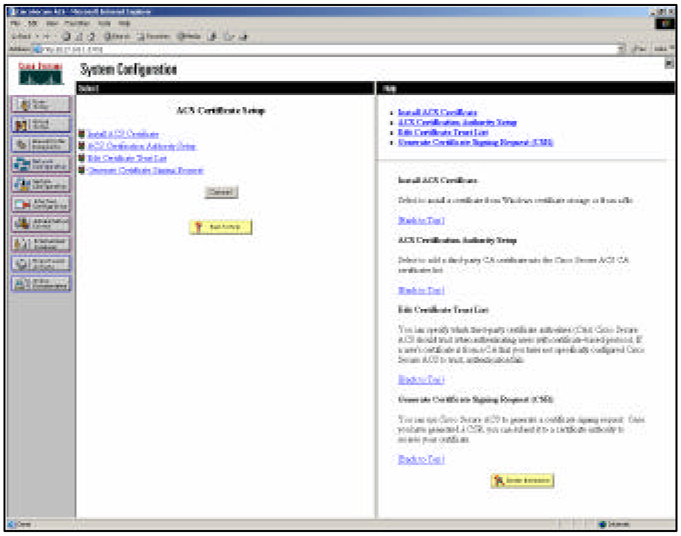
Back to Top

Local Password Management

Select to configure password validation parameters, password change

ACS Configuration
Server Certificate Setup

Cisco.com



System Configuration

ACS Certificate Setup

- Install ACS Certificate
- ACS Certification Authority Setup
- Edit Certificate Trust List
- Generate Certificate Signing Request

Cancel

- Install ACS Certificate
- ACS Certification Authority Setup
- Edit Certificate Trust List
- Generate Certificate Signing Request (CSR)

Install ACS Certificate

Select to install a certificate from Windows certificate storage or from a file.

Back to Top

ACS Certification Authority Setup

Select to add a third-party CA certificate into the Cisco Secure ACS CA certificate list.

Back to Top

Edit Certificate Trust List

You can specify which third-party certificate authorities (CAs) Cisco Secure ACS should trust when authenticating users with certificate-based protocols. If a user's certificate is from a CA that you have not specifically configured Cisco Secure ACS to trust, authentication fails.

Back to Top

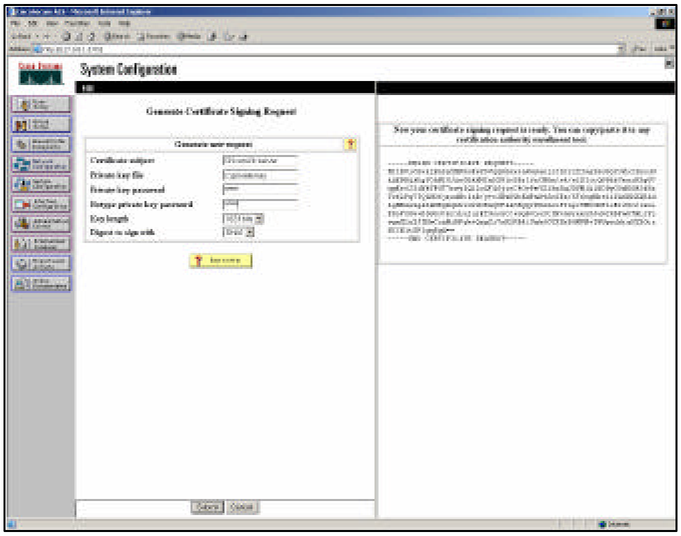
Generate Certificate Signing Request (CSR)

You can use Cisco Secure ACS to generate a certificate signing request. Once you have generated a CSR, you can submit it to a certificate authority to receive your certificate.

Back to Top

ACS Configuration
Server Certificate Setup—PKCS #7 Certificate Request

Cisco.com



System Configuration

Generate Certificate Signing Request

Generate new request	
Certificate subject	[illegible]
Private key file	[illegible]
Private key password	[illegible]
Retype private key password	[illegible]
Key length	[illegible]
Digest to sign with	[illegible]

Now your certificate signing request is ready. You can copy/paste it to any certification authority enrollment tool.

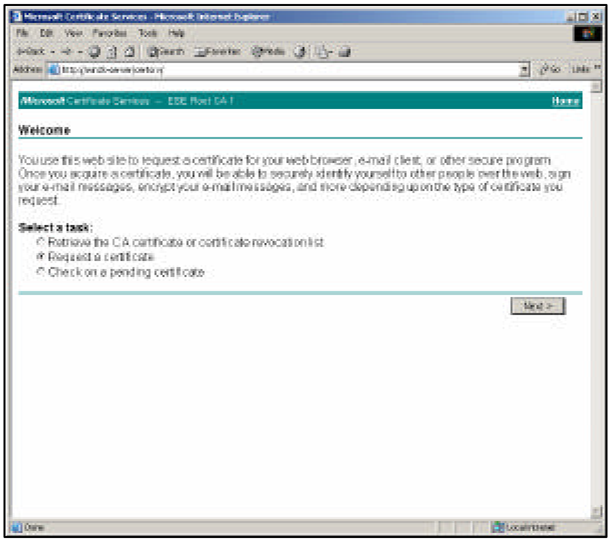
```
-----BEGIN CERTIFICATE REQUEST-----
[illegible]
-----END CERTIFICATE REQUEST-----
```

Submit Cancel

ACS Configuration

Server Certificate Request (MS Certificate Services)

Cisco.com


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Done
Local intranet

Microsoft Certificate Services -- ESE Root CA 1 Home

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

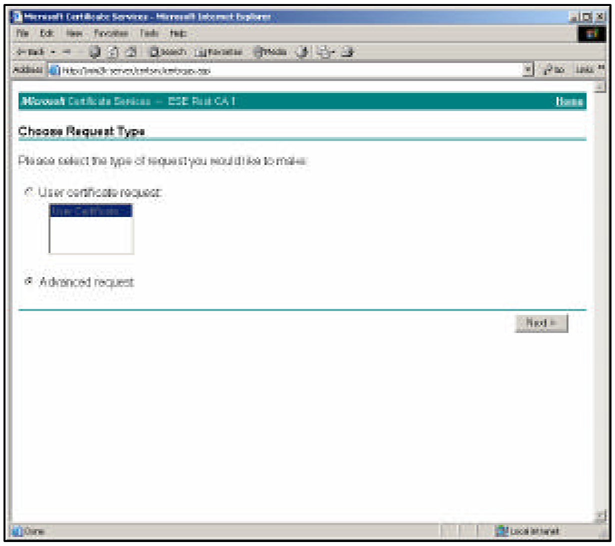
○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

Next >

ACS Configuration

Server Certificate Request (MS Certificate Services)

Cisco.com


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Done
Local intranet

Microsoft Certificate Services -- ESE Root CA 1 Home

Choose Request Type

Please select the type of request you would like to make:

○ User certificate request:

User Certificate

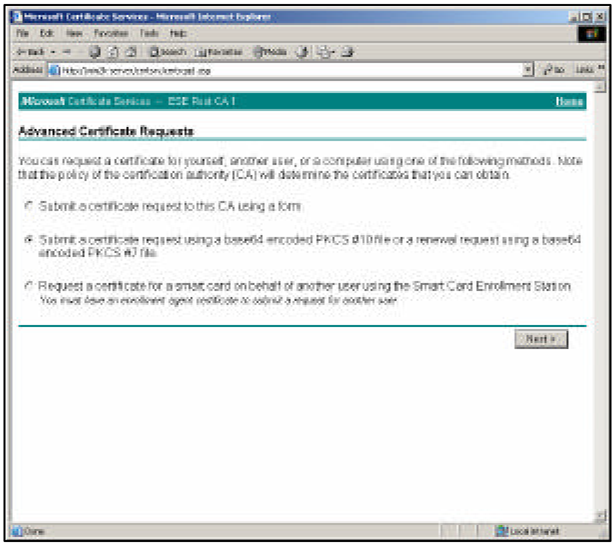
● Advanced request

Next >

ACS Configuration

Server Certificate Request (MS Certificate Services)

Cisco.com



Microsoft Certificate Services - Microsoft Internet Explorer

Microsoft Certificate Services -- ESE Root CA 1 | Home

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

○ Submit a certificate request to this CA using a form.

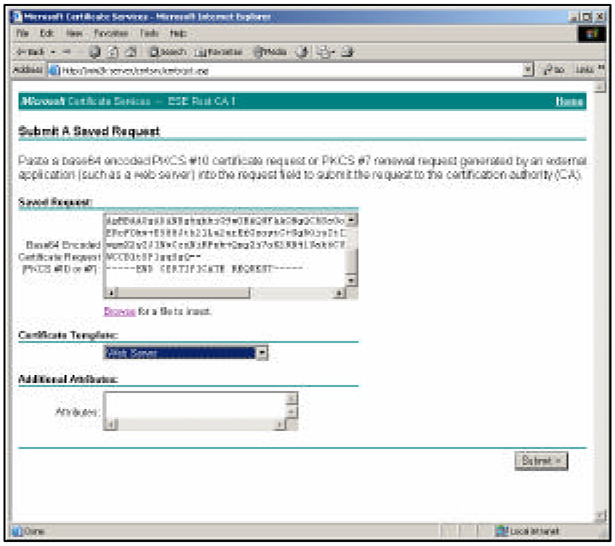
● Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

ACS Configuration

Server Certificate Request (MS Certificate Services)

Cisco.com



Microsoft Certificate Services - Microsoft Internet Explorer

Microsoft Certificate Services -- ESE Root CA 1 | Home

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
[illegible]
[illegible]
[illegible]
[illegible]
-----END CERTIFICATE REQUEST-----
```

Browse for a file to insert.

Certificate Template:

Web Server

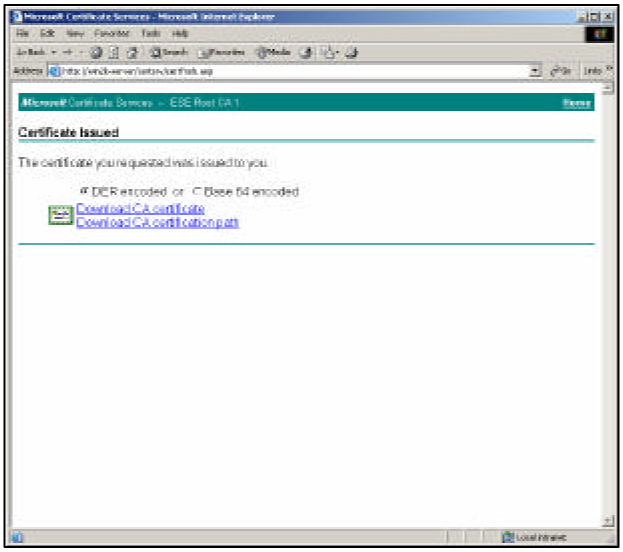
Additional Attributes:

Attributes:

ACS Configuration

Server Certificate Request (MS Certificate Services)

Cisco.com


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://win2k-server/certsrv/certfnsh.asp
Go Links

Microsoft Certificate Services -- ESE Root CA 1 Home

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

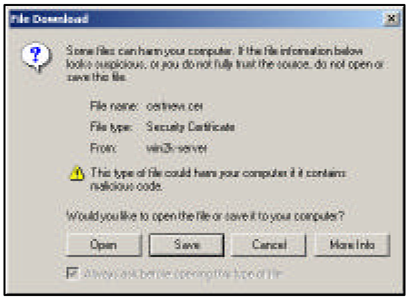
Download CA certificate

Download CA certification path

ACS Configuration

Server Certificate Request (MS Certificate Services)

Cisco.com



Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: certnew.cer

File type: Security Certificate

From: win2k-server

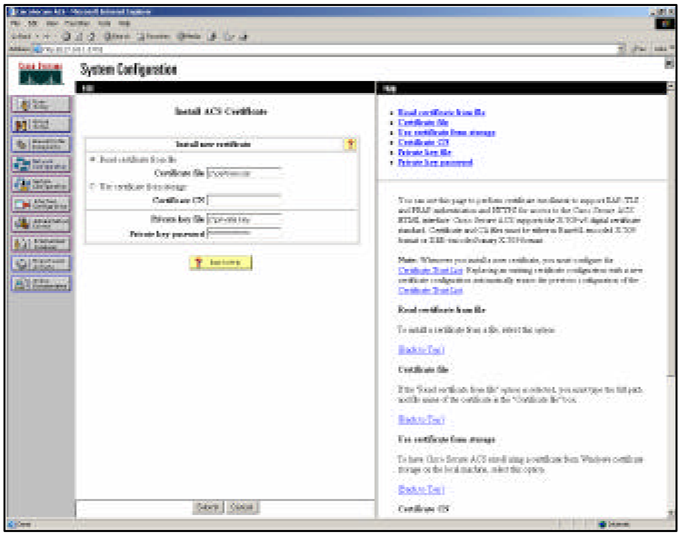
This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

ACS Configuration

Server Certificate Installation



System Configuration

Install ACS Certificate

Install new certificate

● Read certificate from file

Certificate file [illegible]

○ Use certificate from storage

Certificate CN

Private key file [illegible]

Private key password ••••••••••

- Read certificate from file
- Certificate file
- Use certificate from storage
- Certificate CN
- Private key file
- Private key password

You can use this page to perform certificate enrollment to support EAP-TLS and PEAP authentication and HTTPS for access to the Cisco Secure ACS HTML interface. Cisco Secure ACS supports the X.509 v3 digital certificate standard. Certificate and CA files must be either in Base64-encoded X.509 format or DER-encoded binary X.509 format.

Note: Whenever you install a new certificate, you must configure the Certificate Trust List. Replacing an existing certificate configuration with a new certificate configuration automatically erases the previous configuration of the Certificate Trust List.

Read certificate from file

To install a certificate from a file, select this option.

Back to Top

Certificate file

If the "Read certificate from file" option is selected, you must type the full path and file name of the certificate in the "Certificate file" box.

Back to Top

Use certificate from storage

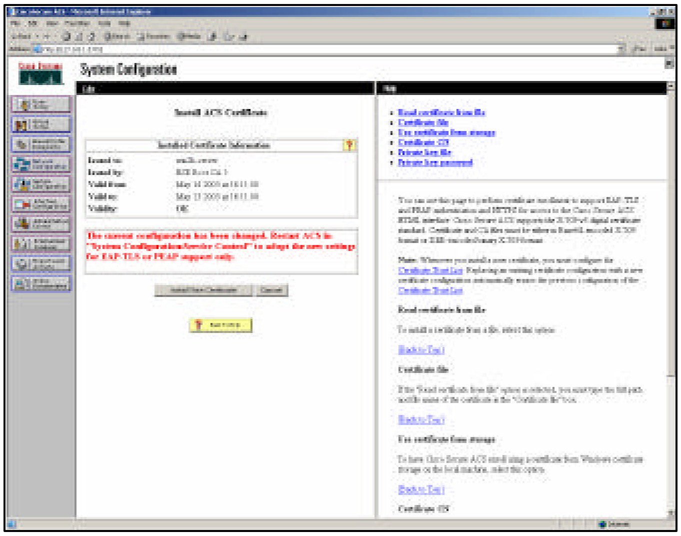
To have Cisco Secure ACS enroll using a certificate from Windows certificate storage on the local machine, select this option.

Back to Top

Certificate CN

ACS Configuration

Server Certificate Installation



System Configuration

Install ACS Certificate

Installed Certificate Information

Issued to:	[illegible]
Issued by:	[illegible] Root CA 1
Valid from:	May 14 2003 at 18:11:30
Valid to:	May 13 2005 at 18:11:30
Validity:	OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

- Read certificate from file
- Certificate file
- Use certificate from storage
- Certificate CN
- Private key file
- Private key password

You can use this page to perform certificate enrollment to support EAP-TLS and PEAP authentication and HTTPS for access to the Cisco Secure ACS HTML interface. Cisco Secure ACS supports the X.509 v3 digital certificate standard. Certificate and CA files must be either in Base64-encoded X.509 format or DER-encoded binary X.509 format.

Note: Whenever you install a new certificate, you must configure the Certificate Trust List. Replacing an existing certificate configuration with a new certificate configuration automatically erases the previous configuration of the Certificate Trust List.

Read certificate from file

To install a certificate from a file, select this option.

Back to Top

Certificate file

If the "Read certificate from file" option is selected, you must type the full path and file name of the certificate in the "Certificate file" box.

Back to Top

Use certificate from storage

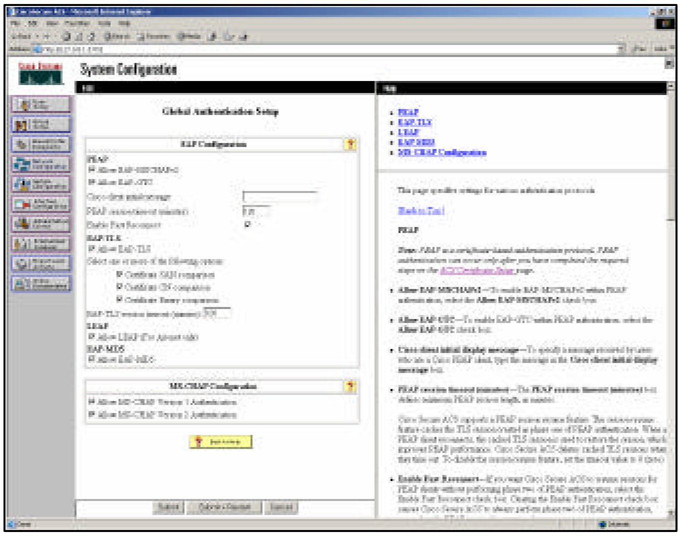
To have Cisco Secure ACS enroll using a certificate from Windows certificate storage on the local machine, select this option.

Back to Top

Certificate CN

ACS Configuration

Global Authentication Setup—EAP Method Selection



System Configuration

Global Authentication Setup

EAP Configuration

PEAP

☑ Allow EAP-MSCHAPv2

☑ Allow EAP-GTC

Cisco client initial message

PEAP session timeout (minutes) 120

Enable Fast Reconnect ☑

EAP-TLS

☑ Allow EAP-TLS

Select one or more of the following options:

☑ Certificate SAN comparison

☑ Certificate CN comparison

☑ Certificate Binary comparison

EAP-TLS session timeout (minutes) 120

LEAP

☑ Allow LEAP (For Aironet only)

EAP-MD5

☑ Allow EAP-MD5

MS-CHAP Configuration

☑ Allow MS-CHAP Version 1 Authentication

☑ Allow MS-CHAP Version 2 Authentication

- PEAP
- EAP-TLS
- LEAP
- EAP-MD5
- MS-CHAP Configuration

This page specifies settings for various authentication protocols.

Back to Top

PEAP

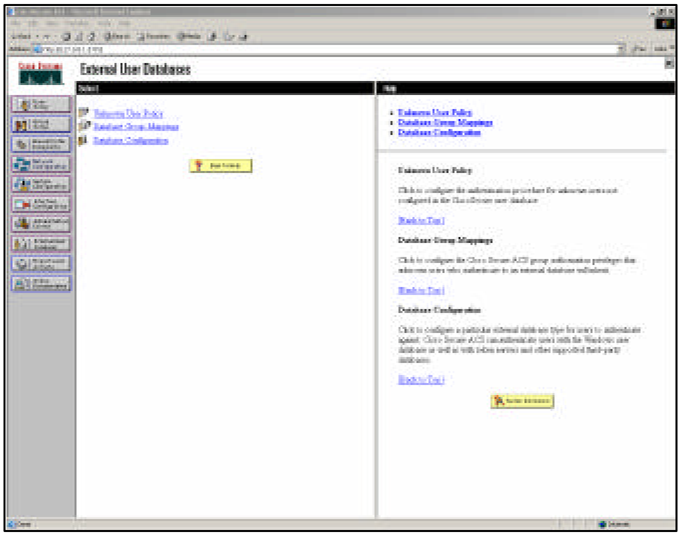
Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.

- **Allow EAP-MSCHAPv2**—To enable EAP-MSCHAPv2 within PEAP authentication, select the **Allow EAP-MSCHAPv2** check box.
- **Allow EAP-GTC**—To enable EAP-GTC within PEAP authentication, select the **Allow EAP-GTC** check box.
- **Cisco client initial display message**—To specify a message sent to users who log in with a Cisco PEAP client, type the message in the **Cisco client initial display message** box.
- **PEAP session timeout (minutes)**—The **PEAP session timeout (minutes)** box defines maximum PEAP session length, in minutes.

  Cisco Secure ACS supports a PEAP session resume feature. This session resume feature caches the TLS session created in phase one of PEAP authentication. When a PEAP client reconnects, the cached TLS session is used to restore the session, which improves PEAP performance. Cisco Secure ACS deletes cached TLS sessions when they time out. To disable the session resume feature, set the timeout value to 0 (zero).
- **Enable Fast Reconnect**—If you want Cisco Secure ACS to resume sessions for PEAP clients without performing phase two of PEAP authentication, select the Enable Fast Reconnect check box. Clearing the Enable Fast Reconnect check box causes Cisco Secure ACS to always perform phase two of PEAP authentication,

ACS Configuration

External User Database Configuration



External User Databases

Unknown User Policy

Database Group Mappings

Database Configuration

- Unknown User Policy
- Database Group Mappings
- Database Configuration

Unknown User Policy

Click to configure the authentication procedure for unknown users not configured in the Cisco Secure user database.

Back to Top

Database Group Mappings

Click to configure the Cisco Secure ACS group authorization privileges that unknown users who authenticate to an external database will inherit.

Back to Top

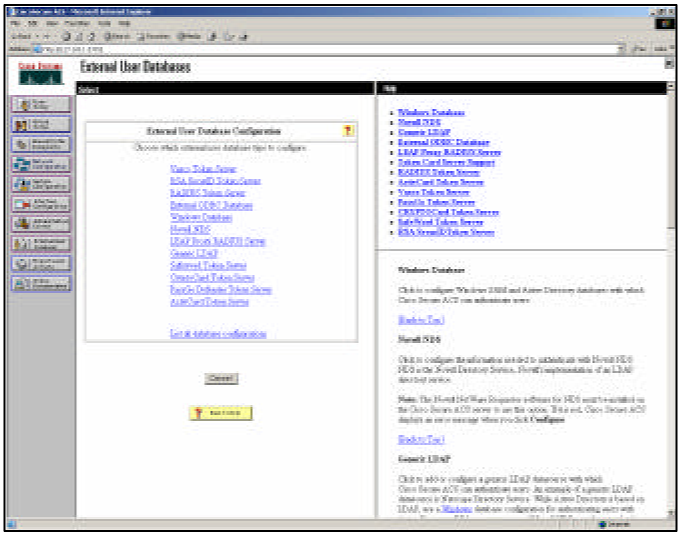
Database Configuration

Click to configure a particular external database type for users to authenticate against. Cisco Secure ACS can authenticate users with the Windows user database as well as with token servers and other supported third-party databases.

Back to Top

ACS Configuration
External User Database Configuration

Cisco.com



External User Database Configuration

Choose which external user database type to configure.

- Vasco Token Server
- RSA SecurID Token Server
- RADIUS Token Server
- External ODBC Database
- Windows Database
- Novell NDS
- LEAP Proxy RADIUS Server
- Generic LDAP
- Safeword Token Server
- CryptoCard Token Server
- PassGo Defender Token Server
- ActivCard Token Server

List all database configurations

- Windows Database
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- ActivCard Token Server
- Vasco Token Server
- PassGo Token Server
- CRYPTOCard Token Server
- SafeWord Token Server
- RSA SecurID Token Server

Windows Database

Click to configure Windows 2000 and Active Directory databases with which Cisco Secure ACS can authenticate users.

[Back to Top]

Novell NDS

Click to configure the information needed to authenticate with Novell NDS. NDS is the Novell Directory Service, Novell's implementation of an LDAP directory service.

Note: The Novell NetWare Requestor software for NDS must be installed on the Cisco Secure ACS server to use this option. If it is not, Cisco Secure ACS displays an error message when you click **Configure**.

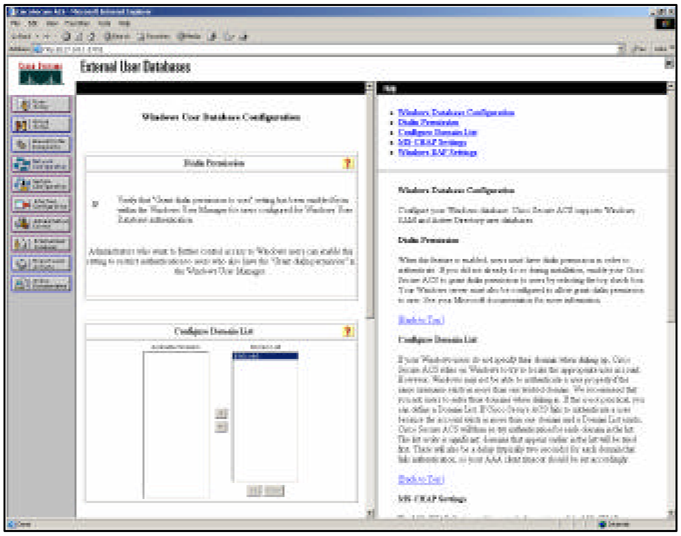
[Back to Top]

Generic LDAP

Click to add or configure a generic LDAP datasource with which Cisco Secure ACS can authenticate users. An example of a generic LDAP datasource is Netscape Directory Server. While Active Directory is based on LDAP, use a Windows database configuration for authenticating users with

ACS Configuration
External User Database Configuration

Cisco.com



Windows User Database Configuration

Dialin Permission

☑ Verify that "Grant dialin permission to user" setting has been enabled from within the Windows User Manager for users configured for Windows User Database authentication.

Administrators who want to further control access to Windows users can enable this setting to restrict authentication to users who also have the "Grant dialin permission" in the Windows User Manager.

Configure Domain List

- Windows Database Configuration
- Dialin Permission
- Configure Domain List
- MS-CHAP Settings
- Windows EAP Settings

Windows Database Configuration

Configure your Windows database. Cisco Secure ACS supports Windows SAM and Active Directory user databases.

Dialin Permission

When this feature is enabled, users must have dialin permission in order to authenticate. If you did not already do so during installation, enable your Cisco Secure ACS to grant dialin permission to users by selecting the top check box. Your Windows server must also be configured to allow grant dialin permission to user. See your Microsoft documentation for more information.

[Back to Top]

Configure Domain List

If your Windows users do not specify their domain when dialing up, Cisco Secure ACS relies on Windows to try to locate the appropriate user account. However, Windows may not be able to authenticate a user properly if the same username exists in more than one trusted domain. We recommend that you ask users to enter their domains when dialing in. If that is not practical, you can define a Domain List. If Cisco Secure ACS fails to authenticate a user because the account exists in more than one domain and a Domain List exists, Cisco Secure ACS will then try to authenticate the user in each domain in the list. The list order is significant; domains that appear earlier in the list will be tried first. There will also be a delay (typically two seconds) for each domain that fails authentication, so your AAA client timeout should be set accordingly.

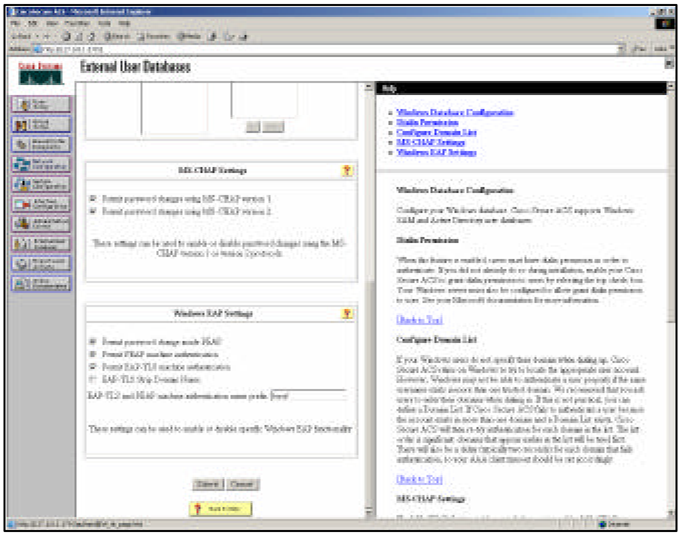
[Back to Top]

MS-CHAP Settings

ACS Configuration

External User Database Configuration

Cisco.com



External User Databases

MS-CHAP Settings

☑ Permit password changes using MS-CHAP version 1

☑ Permit password changes using MS-CHAP version 2

These settings can be used to enable or disable password changes using the MS-CHAP version 1 or version 2 protocols.

Windows EAP Settings

☑ Permit password change inside PEAP

☑ Permit PEAP machine authentication

☑ Permit EAP-TLS machine authentication

☐ EAP-TLS Strip Domain Name

EAP-TLS and PEAP machine authentication name prefix: host/

These settings can be used to enable or disable specific Windows EAP functionality

Help

- Windows Database Configuration
- Dialin Permission
- Configure Domain List
- MS-CHAP Settings
- Windows EAP Settings

Windows Database Configuration

Configure your Windows database. Cisco Secure ACS supports Windows SAM and Active Directory user databases.

Dialin Permission

[illegible]

[Back to Top]

Configure Domain List

[illegible]

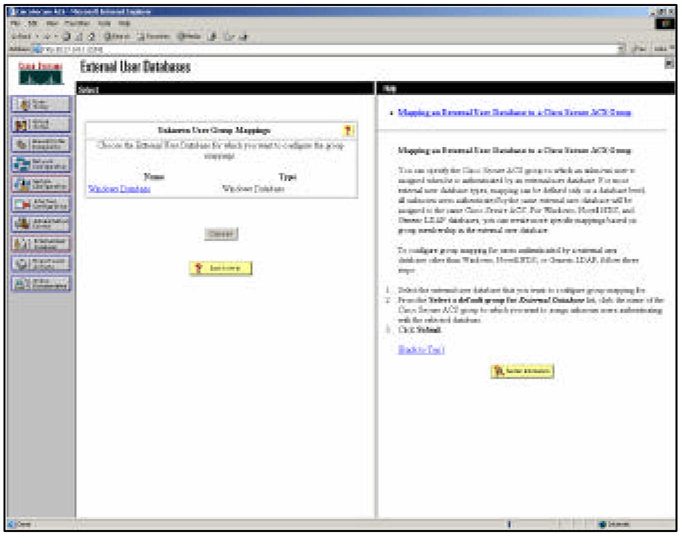
[Back to Top]

MS-CHAP Settings

ACS Configuration

External User Database Group Mapping

Cisco.com



External User Databases

Select

Unknown User Group Mappings

Choose the External User Database for which you want to configure the group mapping.

Name	Type
Windows Database	Windows Database

Help

- Mapping an External User Database to a Cisco Secure ACS Group

Mapping an External User Database to a Cisco Secure ACS Group

You can specify the Cisco Secure ACS group to which an unknown user is assigned when he is authenticated by an external user database. For most external user database types, mapping can be defined only on a database level; all unknown users authenticated by the same external user database will be assigned to the same Cisco Secure ACS. For Windows, Novell NDS, and Generic LDAP databases, you can create more specific mappings based on group membership in the external user database.

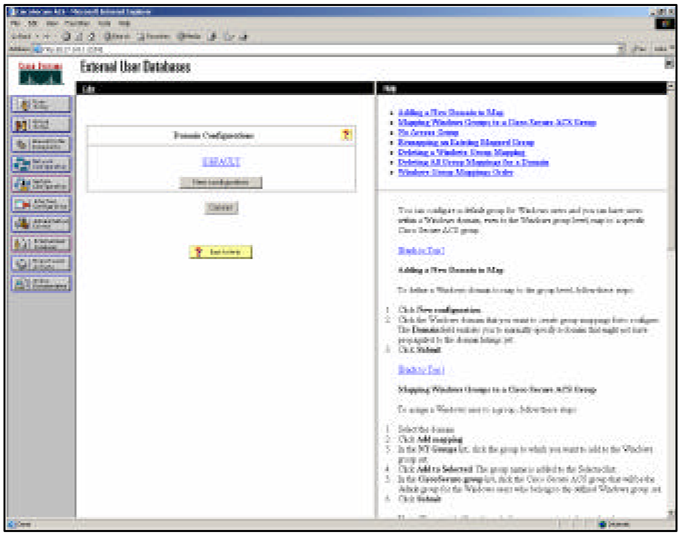
To configure group mapping for users authenticated by external user databases other than Windows, Novell NDS, or Generic LDAP, follow these steps:

1. Select the external user database that you want to configure group mapping for.
2. From the **Select a default group for External Database** list, click the name of the Cisco Secure ACS group to which you want to assign unknown users authenticating with the selected database.
3. Click **Submit**.

[Back to Top]

ACS Configuration

External User Database Group Mapping



External User Databases

Edit

Domain Configurations

DEFAULT

New configuration

Cancel

Back to Help

Help

- Adding a New Domain to Map
- Mapping Windows Groups to a Cisco Secure ACS Group
- No Access Group
- Remapping an Existing Mapped Group
- Deleting a Windows Group Mapping
- Deleting All Group Mappings for a Domain
- Windows Group Mappings Order

[illegible]

Back to Top

Adding a New Domain to Map

[illegible]

1. Click **New configuration**.
2. [illegible]
3. Click **Submit**.

Back to Top

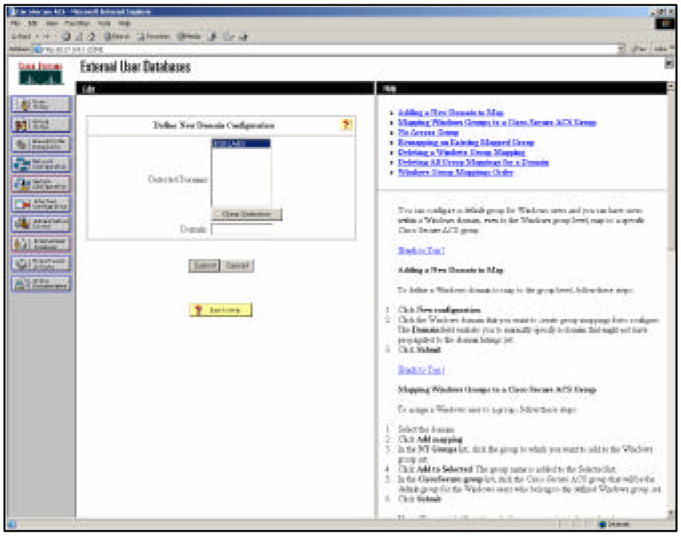
Mapping Windows Groups to a Cisco Secure ACS Group

[illegible]

1. Select the domain.
2. Click **Add mapping**.
3. In the **NT Groups** list, [illegible]
4. Click **Add to Selected**. [illegible]
5. In the **CiscoSecure group** list, [illegible]
6. Click **Submit**.

ACS Configuration

External User Database Group Mapping



External User Databases

Edit

Define New Domain Configuration

Detected Domains: DEFAULT

Clear Selection

Domain:

Submit Cancel

Back to Help

Help

- Adding a New Domain to Map
- Mapping Windows Groups to a Cisco Secure ACS Group
- No Access Group
- Remapping an Existing Mapped Group
- Deleting a Windows Group Mapping
- Deleting All Group Mappings for a Domain
- Windows Group Mappings Order

[illegible]

Back to Top

Adding a New Domain to Map

[illegible]

1. Click **New configuration**.
2. [illegible]
3. Click **Submit**.

Back to Top

Mapping Windows Groups to a Cisco Secure ACS Group

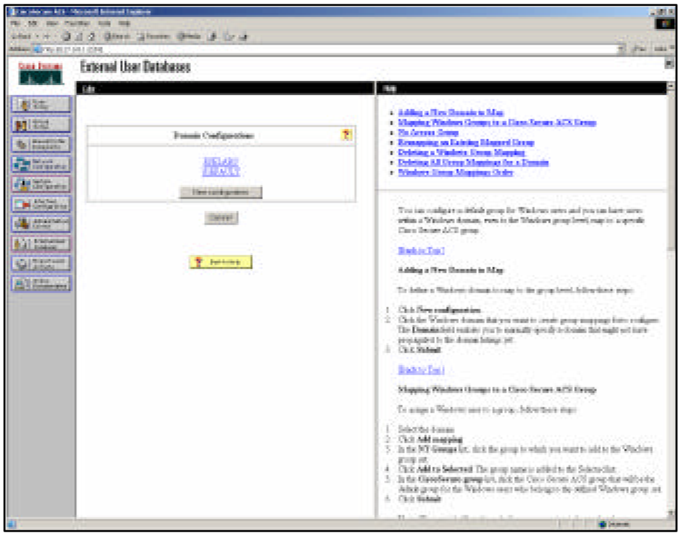
[illegible]

1. Select the domain.
2. Click **Add mapping**.
3. In the **NT Groups** list, [illegible]
4. Click **Add to Selected**. [illegible]
5. In the **CiscoSecure group** list, [illegible]
6. Click **Submit**.

ACS Configuration

External User Database Group Mapping

Cisco.com



External User Databases

Edit

Domain Configurations

ESELAB

[illegible]

New configuration

Cancel

Back to Help

Help

- Adding a New Domain to Map
- Mapping Windows Groups to a Cisco Secure ACS Group
- No Access Group
- Remapping an Existing Mapped Group
- Deleting a Windows Group Mapping
- Deleting All Group Mappings for a Domain
- Windows Group Mappings Order

You can configure a default group for Windows users and you can have users within a Windows domain, even to the Windows group level, map to a specific Cisco Secure ACS group.

[Back to Top]

Adding a New Domain to Map

To define a Windows domain to map to the group level, follow these steps:

1. Click **New configuration**.
2. Click the Windows domain that you want to create group mappings for to configure. The **Domain** field enables you to manually specify a domain that might not have propagated to the domain being set.
3. Click **Submit**.

[Back to Top]

Mapping Windows Groups to a Cisco Secure ACS Group

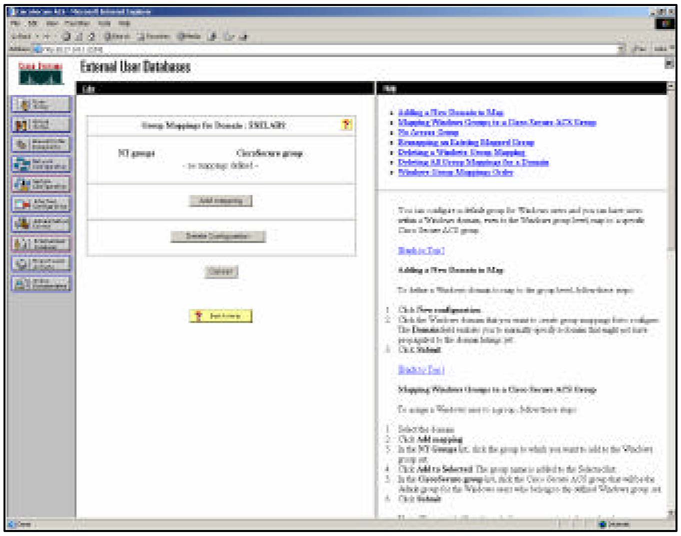
To assign a Windows user to a group, follow these steps:

1. Select the domain.
2. Click **Add mapping**.
3. In the **NT Groups** list, click the group to which you want to add to the Windows group set.
4. Click **Add to Selected**. The group name is added to the Selected list.
5. In the **CiscoSecure group** list, click the Cisco Secure ACS group that will be the default group for the Windows users who belong to the defined Windows group set.
6. Click **Submit**.

ACS Configuration

External User Database Group Mapping

Cisco.com



External User Databases

Edit

Group Mappings for Domain : ESELAB

NT groups CiscoSecure group

- no mappings defined -

Add mapping

Delete Configuration

Cancel

Back to Help

Help

- Adding a New Domain to Map
- Mapping Windows Groups to a Cisco Secure ACS Group
- No Access Group
- Remapping an Existing Mapped Group
- Deleting a Windows Group Mapping
- Deleting All Group Mappings for a Domain
- Windows Group Mappings Order

You can configure a default group for Windows users and you can have users within a Windows domain, even to the Windows group level, map to a specific Cisco Secure ACS group.

[Back to Top]

Adding a New Domain to Map

To define a Windows domain to map to the group level, follow these steps:

1. Click **New configuration**.
2. Click the Windows domain that you want to create group mappings for to configure. The **Domain** field enables you to manually specify a domain that might not have propagated to the domain being set.
3. Click **Submit**.

[Back to Top]

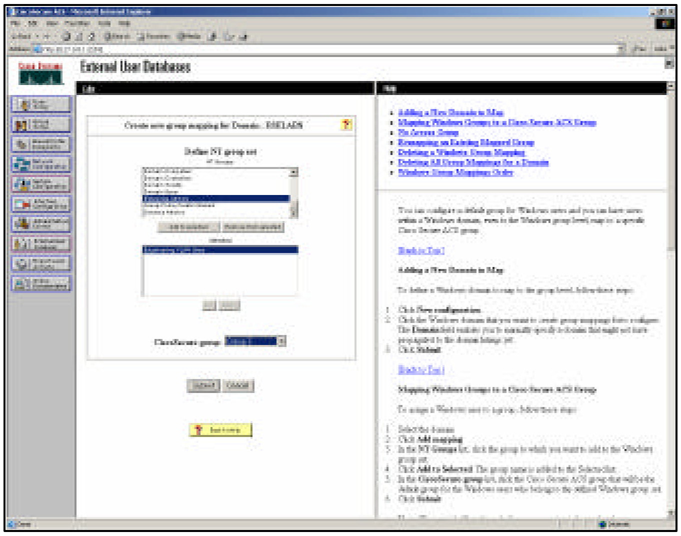
Mapping Windows Groups to a Cisco Secure ACS Group

To assign a Windows user to a group, follow these steps:

1. Select the domain.
2. Click **Add mapping**.
3. In the **NT Groups** list, click the group to which you want to add to the Windows group set.
4. Click **Add to Selected**. The group name is added to the Selected list.
5. In the **CiscoSecure group** list, click the Cisco Secure ACS group that will be the default group for the Windows users who belong to the defined Windows group set.
6. Click **Submit**.

ACS Configuration
External User Database Group Mapping

Cisco.com



External User Databases

Edit

Create new group mapping for Domain : ESELABS

Define NT group set

CiscoSecure group: Group 1

Help

- Adding a New Domain to Map
- Mapping Windows Groups to a Cisco Secure ACS Group
- No Access Group
- Remapping an Existing Mapped Group
- Deleting a Windows Group Mapping
- Deleting All Group Mappings for a Domain
- Windows Group Mappings Order

You can configure a default group for Windows users and you can have users within a Windows domain, even in the Windows group level, map to a specific Cisco Secure ACS group.

[Back to Top]

Adding a New Domain to Map

To define a Windows domain to map to the group level, follow these steps:

1. Click **New configuration**.
2. Click the Windows domain that you want to create group mappings for to configure. The **Domain** field enables you to manually specify a domain that might not have propagated to the domain listings yet.
3. Click **Submit**.

[Back to Top]

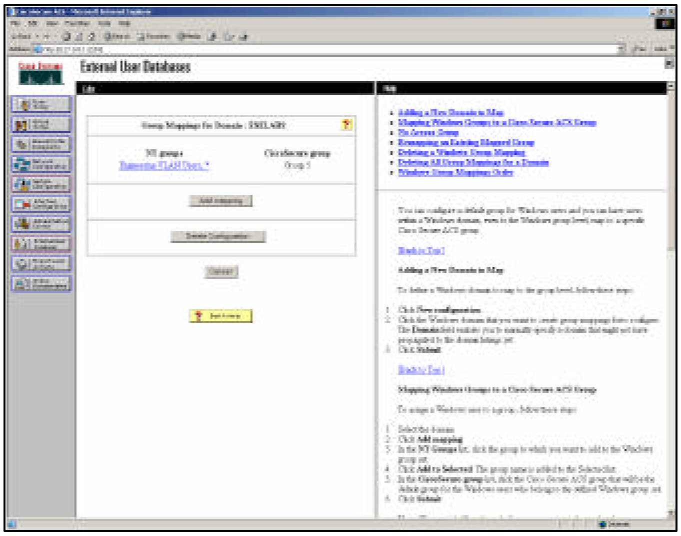
Mapping Windows Groups to a Cisco Secure ACS Group

To assign a Windows user to a group, follow these steps:

1. Select the domain.
2. Click **Add mapping**.
3. In the **NT Groups** list, click the group to which you want to add to the Windows group set.
4. Click **Add to Selected**. The group name is added to the Selected list.
5. In the **CiscoSecure group** list, click the Cisco Secure ACS group that will be the default group for the Windows users who belong to the defined Windows group set.
6. Click **Submit**.

ACS Configuration
External User Database Group Mapping

Cisco.com



External User Databases

Edit

Group Mappings for Domain : ESELABS

NT groups	CiscoSecure group
Engineering VLAN Users, *	Group 5

Help

- Adding a New Domain to Map
- Mapping Windows Groups to a Cisco Secure ACS Group
- No Access Group
- Remapping an Existing Mapped Group
- Deleting a Windows Group Mapping
- Deleting All Group Mappings for a Domain
- Windows Group Mappings Order

You can configure a default group for Windows users and you can have users within a Windows domain, even in the Windows group level, map to a specific Cisco Secure ACS group.

[Back to Top]

Adding a New Domain to Map

To define a Windows domain to map to the group level, follow these steps:

1. Click **New configuration**.
2. Click the Windows domain that you want to create group mappings for to configure. The **Domain** field enables you to manually specify a domain that might not have propagated to the domain listings yet.
3. Click **Submit**.

[Back to Top]

Mapping Windows Groups to a Cisco Secure ACS Group

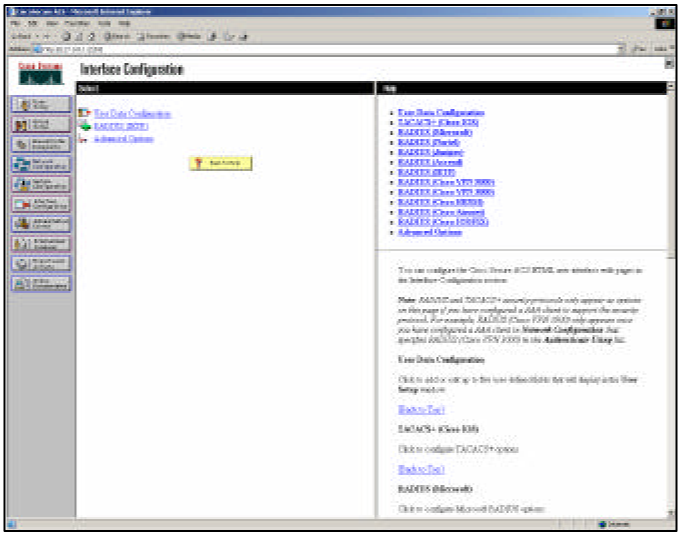
To assign a Windows user to a group, follow these steps:

1. Select the domain.
2. Click **Add mapping**.
3. In the **NT Groups** list, click the group to which you want to add to the Windows group set.
4. Click **Add to Selected**. The group name is added to the Selected list.
5. In the **CiscoSecure group** list, click the Cisco Secure ACS group that will be the default group for the Windows users who belong to the defined Windows group set.
6. Click **Submit**.

ACS Configuration

User Interface Option Configuration

Cisco.com



Interface Configuration

Select

- User Data Configuration
- RADIUS (IETF)
- Advanced Options

Help

- User Data Configuration
- TACACS+ (Cisco IOS)
- RADIUS (Microsoft)
- RADIUS (Nortel)
- RADIUS (Juniper)
- RADIUS (Ascend)
- RADIUS (IETF)
- RADIUS (Cisco VPN 3000)
- RADIUS (Cisco VPN 5000)
- RADIUS (Cisco BBSM)
- RADIUS (Cisco Aironet)
- RADIUS (Cisco IOS/PIX)
- Advanced Options

You can configure the Cisco Secure ACS HTML user interface with pages in the Interface Configuration section.

Note: *RADIUS and TACACS+ security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000) only appears once you have configured a AAA client in* **Network Configuration** *that specifies RADIUS (Cisco VPN 3000) in the* **Authenticate Using** *list.*

User Data Configuration

Click to add or edit up to five user-defined fields that will display in the **User Setup** section.

Back to Top

TACACS+ (Cisco IOS)

Click to configure TACACS+ options.

Back to Top

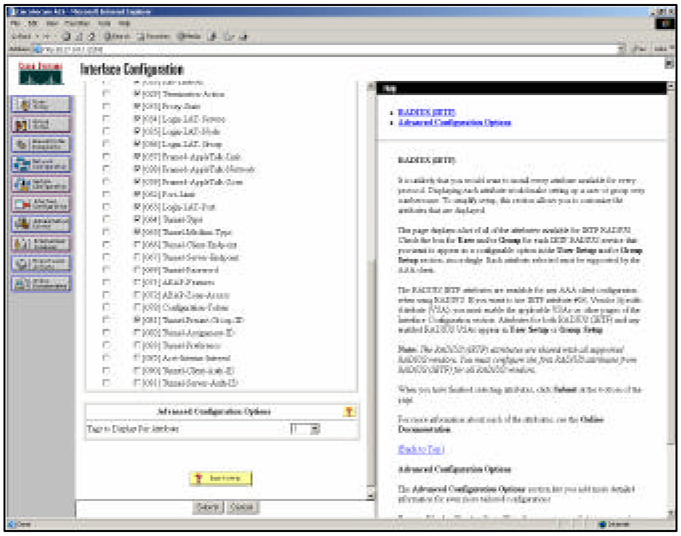
RADIUS (Microsoft)

Click to configure Microsoft RADIUS options.

ACS Configuration

User Interface Options—RADIUS AV Pair Configuration

Cisco.com



Interface Configuration

☐ ☑ [029] Termination-Action
☐ ☑ [033] Proxy-State
☐ ☑ [034] Login-LAT-Service
☐ ☑ [035] Login-LAT-Node
☐ ☑ [036] Login-LAT-Group
☐ ☑ [037] Framed-AppleTalk-Link
☐ ☑ [038] Framed-AppleTalk-Network
☐ ☑ [039] Framed-AppleTalk-Zone
☐ ☑ [062] Port-Limit
☐ ☑ [063] Login-LAT-Port
☐ ☑ [064] Tunnel-Type
☐ ☑ [065] Tunnel-Medium-Type
☐ ☐ [066] Tunnel-Client-Endpoint
☐ ☐ [067] Tunnel-Server-Endpoint
☐ ☐ [069] Tunnel-Password
☐ ☐ [071] ARAP-Features
☐ ☐ [072] ARAP-Zone-Access
☐ ☐ [078] Configuration-Token
☐ ☑ [081] Tunnel-Private-Group-ID
☐ ☐ [082] Tunnel-Assignment-ID
☐ ☐ [083] Tunnel-Preference
☐ ☐ [085] Acct-Interim-Interval
☐ ☐ [090] Tunnel-Client-Auth-ID
☐ ☐ [091] Tunnel-Server-Auth-ID

Advanced Configuration Options

Tags to Display Per Attribute: 1

Help

- RADIUS (IETF)
- Advanced Configuration Options

RADIUS (IETF)

It is unlikely that you would want to install every attribute available for every protocol. Displaying each attribute would make setting up a user or group very cumbersome. To simplify setup, this section allows you to customize the attributes that are displayed.

This page displays a list of all of the attributes available for IETF RADIUS. Check the box for **User** and/or **Group** for each IETF RADIUS service that you want to appear as a configurable option in the **User Setup** and/or **Group Setup** section, accordingly. Each attribute selected must be supported by the AAA client.

The RADIUS IETF attributes are available for any AAA client configuration when using RADIUS. If you want to use IETF attribute #26, Vendor-Specific Attribute (VSA), you must enable the applicable VSAs on other pages of the Interface Configuration section. Attributes for both RADIUS (IETF) and any enabled RADIUS VSAs appear in **User Setup** or **Group Setup**.

Note: *The RADIUS (IETF) attributes are shared with all supported RADIUS vendors. You must configure the first RADIUS attributes from RADIUS (IETF) for all RADIUS vendors.*

When you have finished selecting attributes, click **Submit** at the bottom of the page.

For more information about each of the attributes, see the **Online Documentation**.

Back to Top

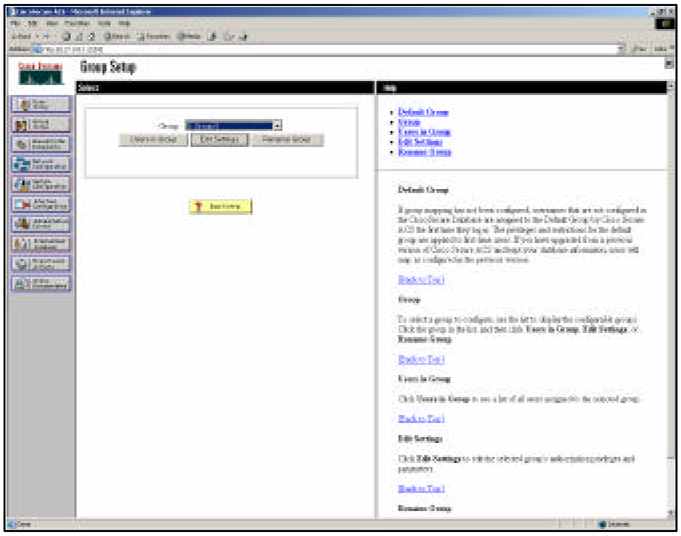
Advanced Configuration Options

The **Advanced Configuration Options** section lets you add more detailed information for even more tailored configurations.

ACS Configuration

Group Policy Configuration

Cisco.com



Group Setup

Select

Group: 0: Default

Help

- Default Group
- Group
- Users in Group
- Edit Settings
- Rename Group

Default Group

If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version.

Back to Top

Group

To select a group to configure, use the list to display the configurable groups. Click the group in the list, and then click **Users in Group**, **Edit Settings**, or **Rename Group**.

Back to Top

Users in Group

Click **Users in Group** to see a list of all users assigned to the selected group.

Back to Top

Edit Settings

Click **Edit Settings** to edit the selected group's authorization privileges and parameters.

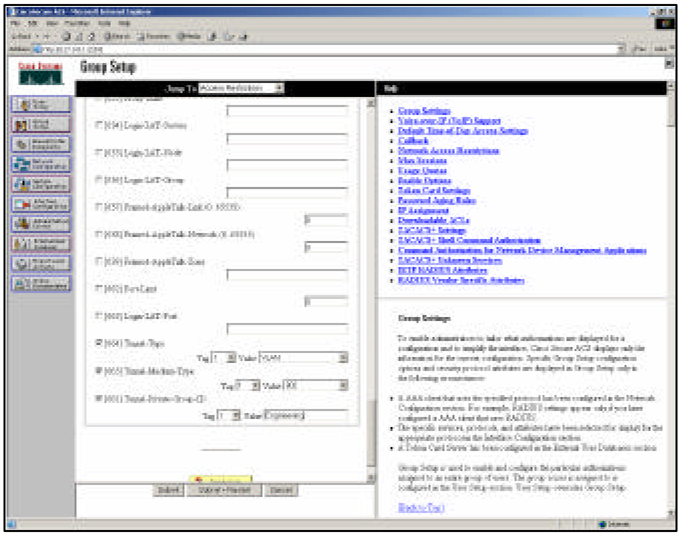
Back to Top

Rename Group

ACS Configuration

Group Policy Configuration—VLAN Assignment

Cisco.com



Group Setup

Jump To: Access Restrictions

- ☐ [054] Login-LAT-Service
- ☐ [055] Login-LAT-Node
- ☐ [056] Login-LAT-Group
- ☐ [037] Framed-AppleTalk-Link (0 - 65535): 0
- ☐ [038] Framed-AppleTalk-Network (0 - 65535): 0
- ☐ [039] Framed-AppleTalk-Zone
- ☐ [062] Port-Limit: 0
- ☐ [063] Login-LAT-Port
- ☑ [064] Tunnel-Type — Tag: 1, Value: VLAN
- ☑ [065] Tunnel-Medium-Type — Tag: 1, Value: 802
- ☑ [081] Tunnel-Private-Group-ID — Tag: 1, Value: Engineering

Help

- Group Settings
- Voice-over-IP (VoIP) Support
- Default Time-of-Day Access Settings
- Callback
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Enable Options
- Token Card Settings
- Password Aging Rules
- IP Assignment
- Downloadable ACLs
- TACACS+ Settings
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

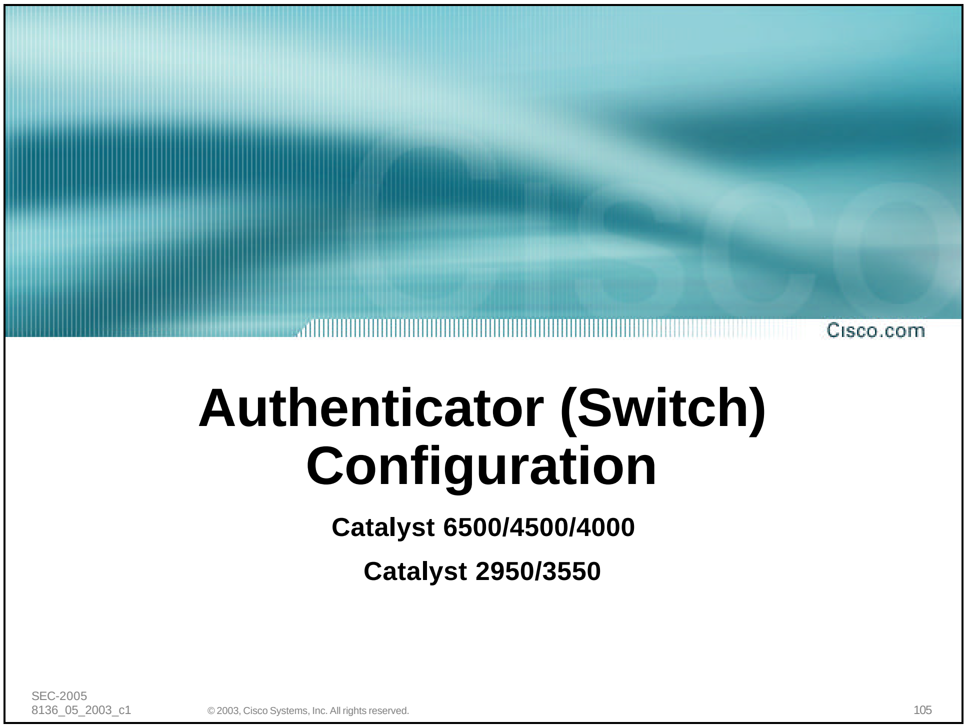
Group Settings

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances:

- A AAA client that uses the specified protocol has been configured in the Network Configuration section. For example, RADIUS settings appear only if you have configured a AAA client that uses RADIUS.
- The specific services, protocols, and attributes have been selected for display for the appropriate protocols in the Interface Configuration section.
- A Token Card Server has been configured in the External User Databases section.

Group Setup is used to enable and configure the particular authorizations assigned to an entire group of users. The group is used to assign to a [illegible] configured in the User Setup section. User Setup overrides Group Setup.

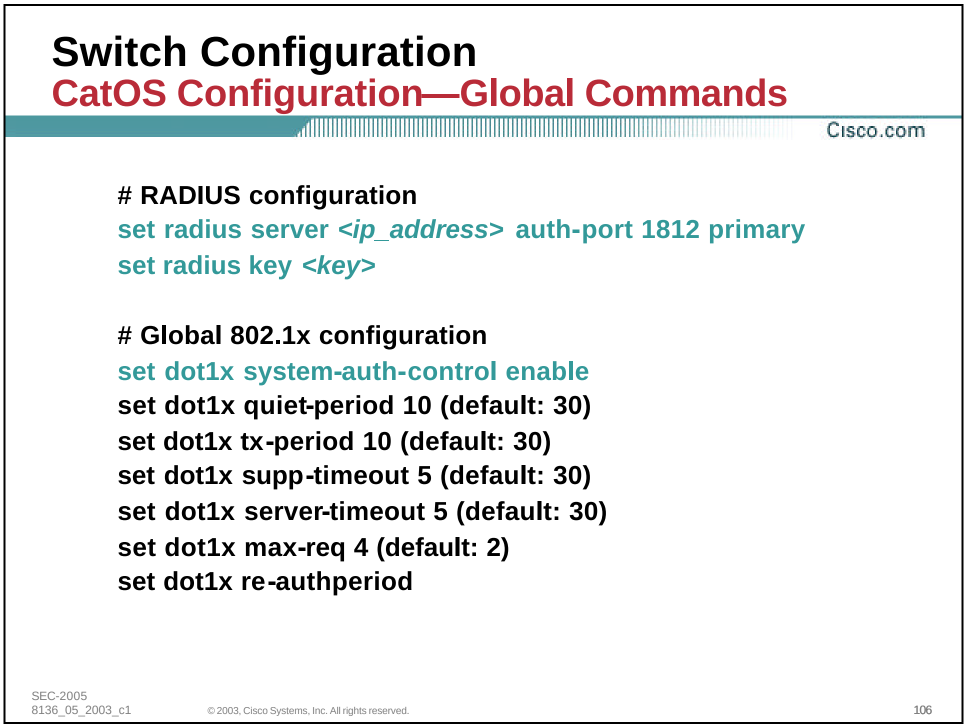
Back to Top



Authenticator (Switch) Configuration

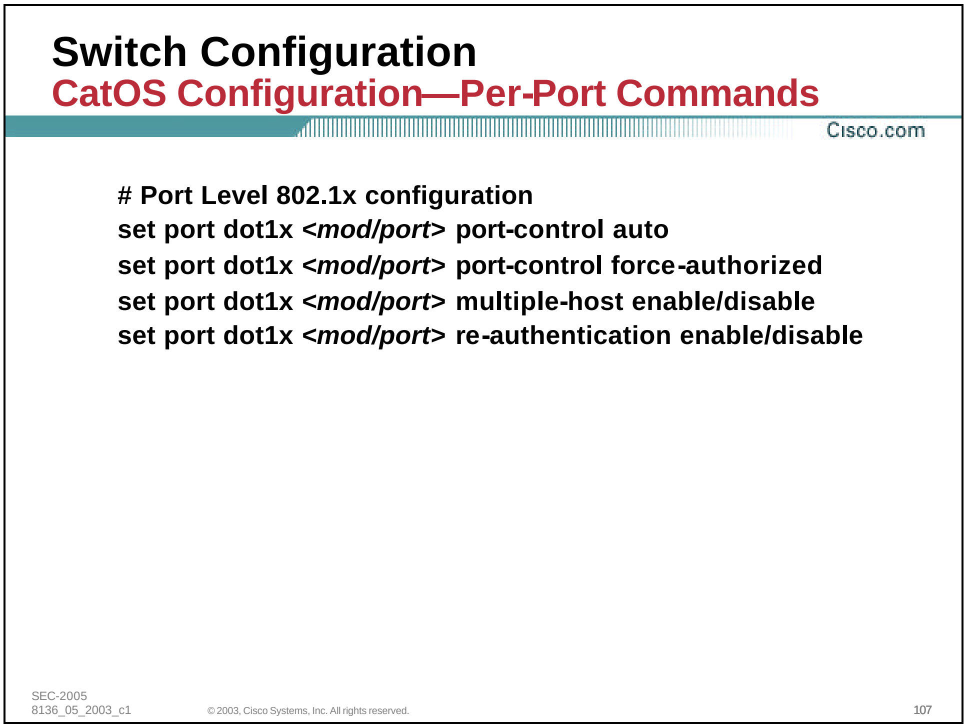
Catalyst 6500/4500/4000

Catalyst 2950/3550



Switch Configuration
CatOS Configuration—Global Commands

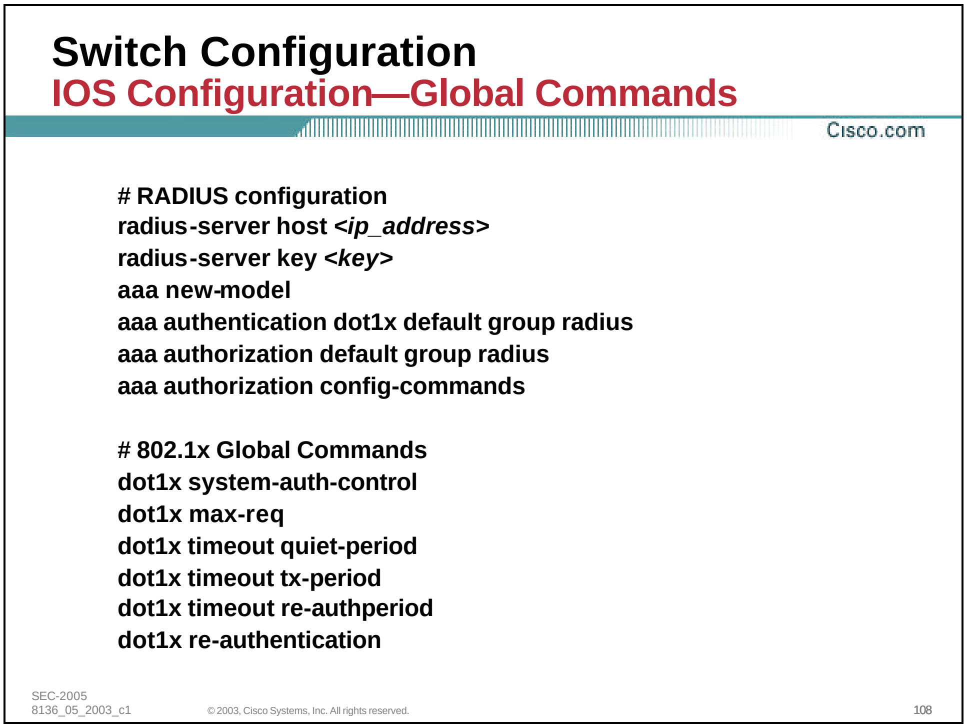
```
# RADIUS configuration
set radius server <ip_address> auth-port 1812 primary
set radius key <key>

# Global 802.1x configuration
set dot1x system-auth-control enable
set dot1x quiet-period 10 (default: 30)
set dot1x tx-period 10 (default: 30)
set dot1x supp-timeout 5 (default: 30)
set dot1x server-timeout 5 (default: 30)
set dot1x max-req 4 (default: 2)
set dot1x re-authperiod
```



Switch Configuration

CatOS Configuration—Per-Port Commands

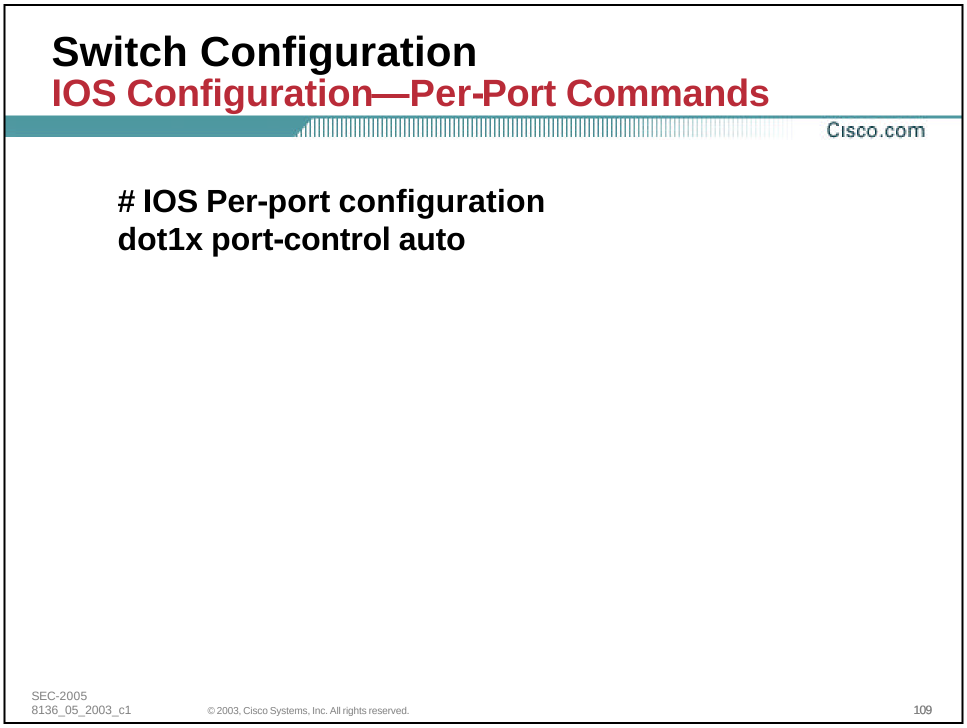
```
# Port Level 802.1x configuration
set port dot1x <mod/port> port-control auto
set port dot1x <mod/port> port-control force-authorized
set port dot1x <mod/port> multiple-host enable/disable
set port dot1x <mod/port> re-authentication enable/disable
```



Switch Configuration

IOS Configuration—Global Commands

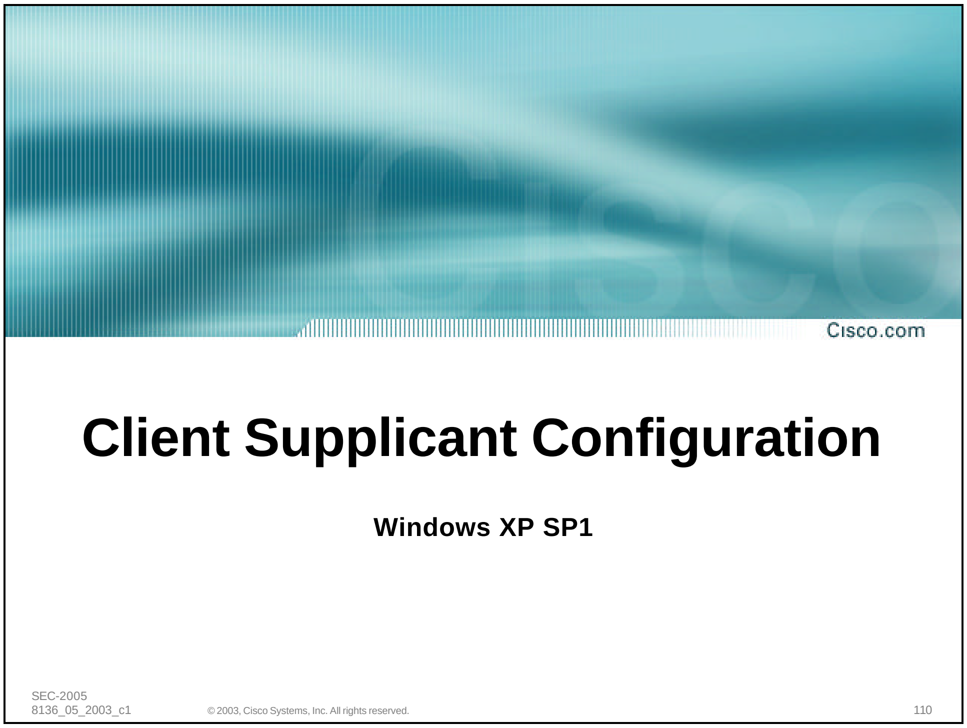
```
# RADIUS configuration
radius-server host <ip_address>
radius-server key <key>
aaa new-model
aaa authentication dot1x default group radius
aaa authorization default group radius
aaa authorization config-commands

# 802.1x Global Commands
dot1x system-auth-control
dot1x max-req
dot1x timeout quiet-period
dot1x timeout tx-period
dot1x timeout re-authperiod
dot1x re-authentication
```



Switch Configuration
IOS Configuration—Per-Port Commands

Cisco.com

```
# IOS Per-port configuration
dot1x port-control auto
```



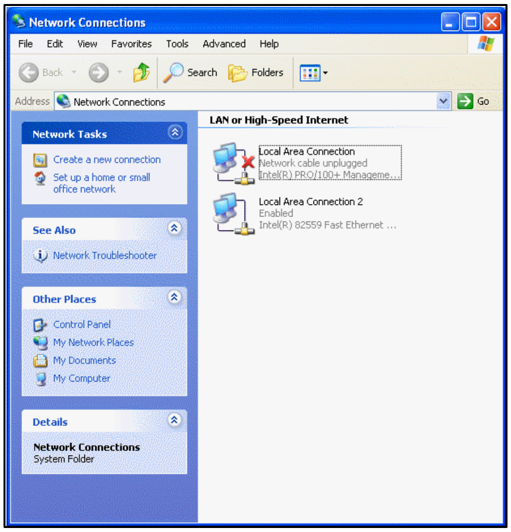
Cisco.com

Client Supplicant Configuration

Windows XP SP1

Supplicant Configuration
Network Connection Properties

Cisco.com


Network Connections

File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go

Network Tasks
- Create a new connection
- Set up a home or small office network

See Also
- Network Troubleshooter

Other Places
- Control Panel
- My Network Places
- My Documents
- My Computer

Details

Network Connections
System Folder

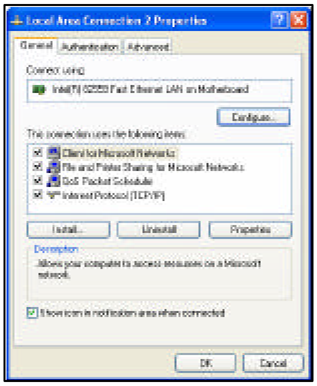
LAN or High-Speed Internet

Local Area Connection
Network cable unplugged
Intel(R) PRO/100+ Manageme...

Local Area Connection 2
Enabled
Intel(R) 82559 Fast Ethernet ...

Supplicant Configuration
Network Interface Authentication Properties

Cisco.com


Local Area Connection 2 Properties

General Authentication Advanced

Connect using:

Intel(R) 82559 Fast Ethernet LAN on Motherboard

This connection uses the following items:

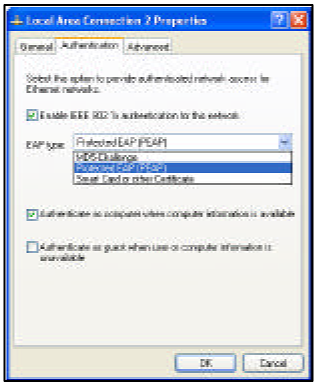
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Install... Uninstall Properties

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected


Local Area Connection 2 Properties

Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

- MD5-Challenge
- Protected EAP (PEAP)
- Smart Card or other Certificate

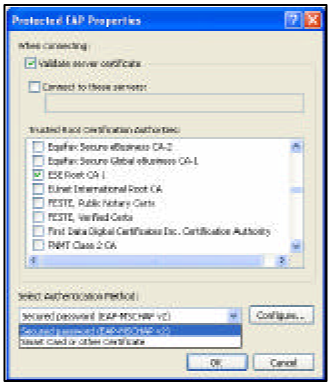
☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

Supplicant Configuration

Authentication Method—PEAP Configuration

Cisco.com



Protected EAP Properties

When connecting:

☑ Validate server certificate

☐ Connect to these servers:

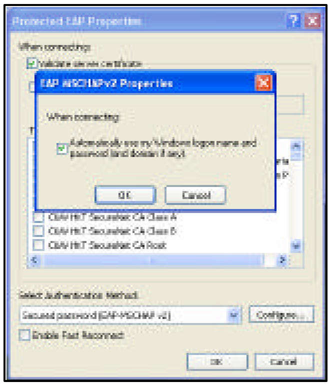
Trusted Root Certification Authorities:

☐ Equifax Secure eBusiness CA-2
☐ Equifax Secure Global eBusiness CA-1
☑ ESE Root CA 1
☐ EUnet International Root CA
☐ FESTE, Public Notary Certs
☐ FESTE, Verified Certs
☐ First Data Digital Certificates Inc. Certification Authority
☐ FNMT Clase 2 CA

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Secured password (EAP-MSCHAP v2)
Smart Card or other Certificate



Protected EAP Properties

When connecting:

☑ Validate server certificate

EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

☐ GTE CyberTrust Global Root...
☐ CBAW HKT SecureNet CA Class A
☐ CBAW HKT SecureNet CA Class B
☐ CBAW HKT SecureNet CA Root

Select Authentication Method:

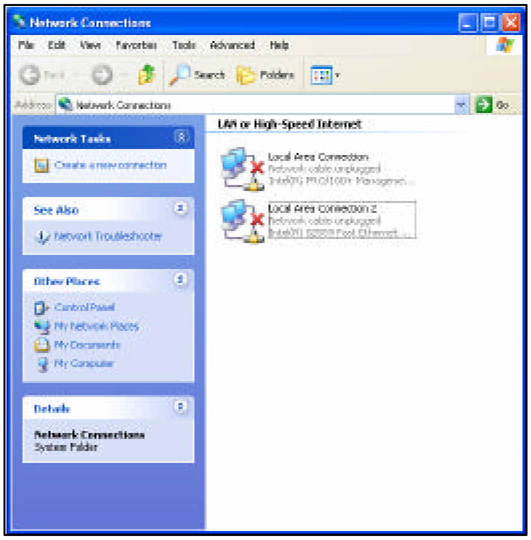
Secured password (EAP-MSCHAP v2)

☐ Enable Fast Reconnect

Supplicant Configuration

Interface Status—Disconnected State

Cisco.com



Network Connections
System Folder

LAN or High-Speed Internet

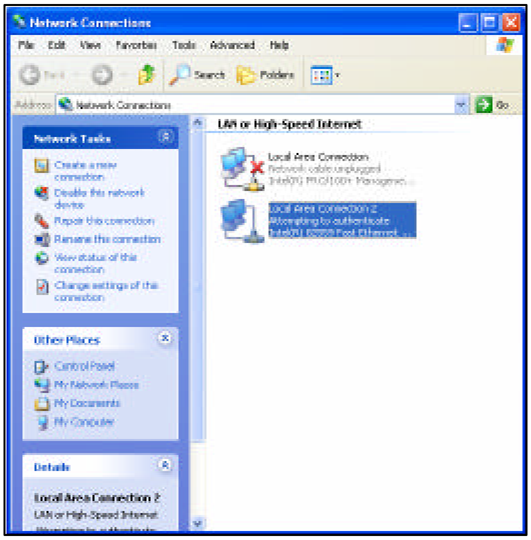
Local Area Connection
Network cable unplugged
Intel(R) PRO/100+ Manageme...

Local Area Connection 2
Network cable unplugged
Intel(R) 82559 Fast Ethernet ...

Supplicant Configuration

Interface Status—Connected/Authenticating State

Cisco.com



LAN or High-Speed Internet

Local Area Connection
Network cable unplugged
Intel(R) PRO/100+ Manageme...

Local Area Connection 2
Attempting to authenticate
Intel(R) 82559 Fast Ethernet ...

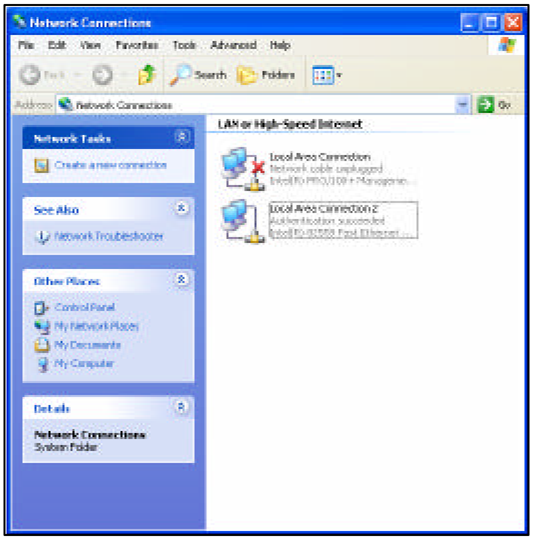
Details

Local Area Connection 2
LAN or High-Speed Internet

Supplicant Configuration

Interface Status—Auth Successful/Connected State

Cisco.com



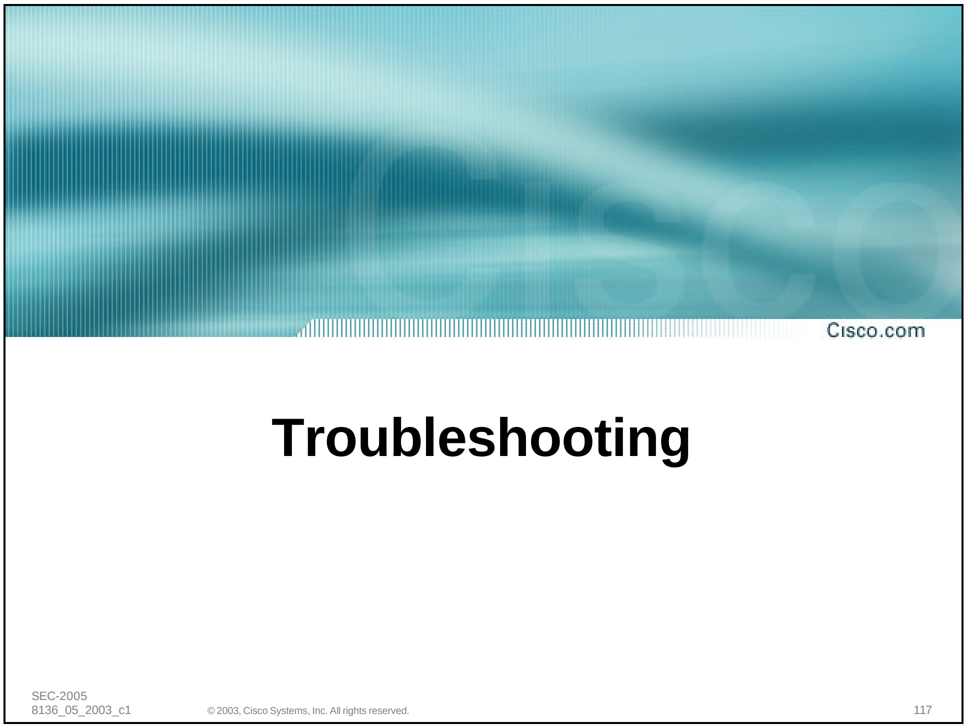
LAN or High-Speed Internet

Local Area Connection
Network cable unplugged
Intel(R) PRO/100+ Manageme...

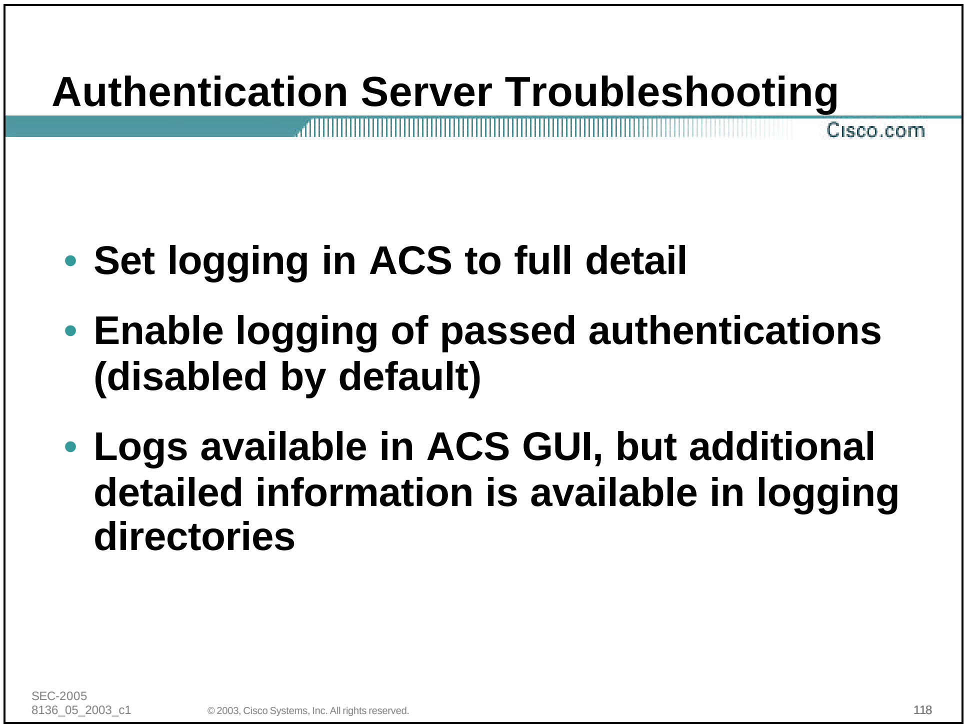
Local Area Connection 2
Authentication succeeded
Intel(R) 82559 Fast Ethernet ...

Details

Network Connections
System Folder



Troubleshooting



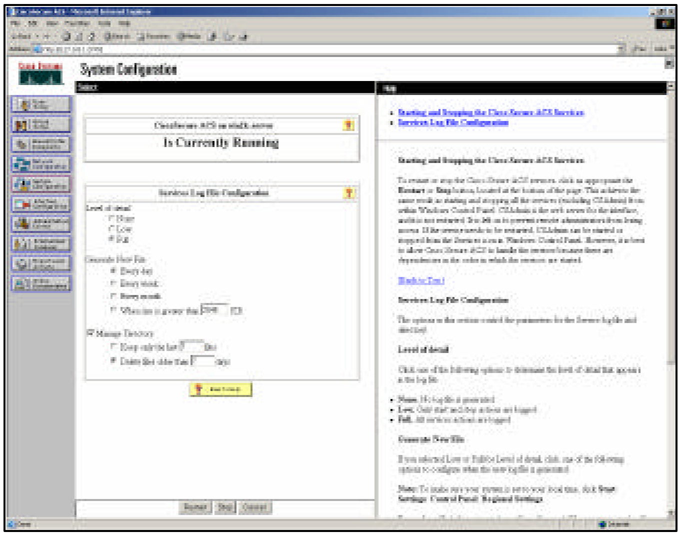
Authentication Server Troubleshooting

- Set logging in ACS to full detail
- Enable logging of passed authentications (disabled by default)
- Logs available in ACS GUI, but additional detailed information is available in logging directories

Authentication Server Troubleshooting

Logging Detail Level Configuration

Cisco.com



System Configuration

CiscoSecure ACS on [illegible]

Is Currently Running

Services Log File Configuration

Level of detail
○ None
○ Low
● Full

Generate New File
● Every day
○ Every week
○ Every month
○ When size is greater than [2048] KB

☑ Manage Directory
○ Keep only the last [7] files
● Delete files older than [ ] days

- Starting and Stopping the Cisco Secure ACS Services
- Services Log File Configuration

Starting and Stopping the Cisco Secure ACS Services

To restart or stop the Cisco Secure ACS services, click as appropriate the **Restart** or **Stop** button, located at the bottom of the page. This achieves the same result as starting and stopping all the services (excluding CSAdmin) from within Windows Control Panel. CSAdmin is the web server for the interface, and it is not restarted. It is left on to prevent remote administrators from losing access. If the service needs to be restarted, CSAdmin can be started or stopped from the Services icon in Windows Control Panel. However, it is best to allow Cisco Secure ACS to handle the services because there are dependencies in the order in which the services are started.

Back to Top

Services Log File Configuration

The options in this section control the parameters for the Service logfile and directory.

Level of detail

Click one of the following options to determine the level of detail that appears in the log file:

- **None.** No logfile is generated.
- **Low.** Only start and stop actions are logged.
- **Full.** All services actions are logged.

Generate New File

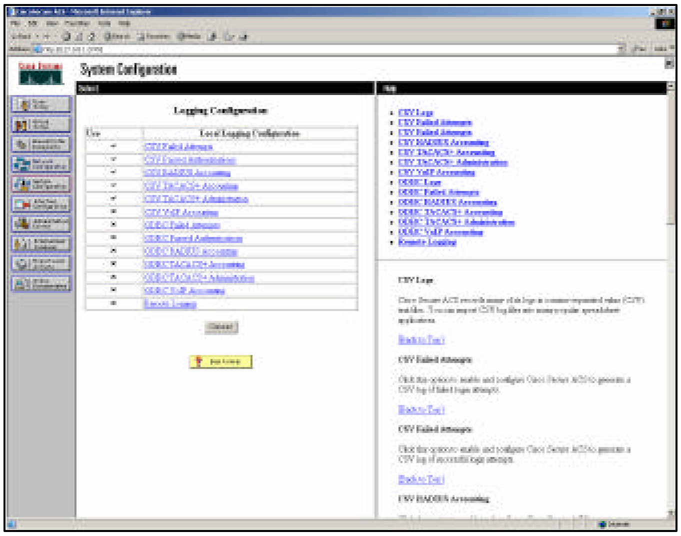
If you selected Low or Full for Level of detail, click one of the following options to configure when the new logfile is generated:

Note: To make sure your system is set to your local time, click **Start> Settings> Control Panel> Regional Settings**.

Authentication Server Troubleshooting

General Logging Configuration

Cisco.com



System Configuration

Logging Configuration

Use	Local Logging Configuration
✓	CSV Failed Attempts
✓	CSV Passed Authentications
✓	CSV RADIUS Accounting
✓	CSV TACACS+ Accounting
✓	CSV TACACS+ Administration
☒	CSV VoIP Accounting
☒	ODBC Failed Attempts
☒	ODBC Passed Authentications
☒	ODBC RADIUS Accounting
☒	ODBC TACACS+ Accounting
☒	ODBC TACACS+ Administration
☒	ODBC VoIP Accounting
☒	Remote Logging

- CSV Logs
- CSV Failed Attempts
- CSV Failed Attempts
- CSV RADIUS Accounting
- CSV TACACS+ Accounting
- CSV TACACS+ Administration
- CSV VoIP Accounting
- ODBC Logs
- ODBC Failed Attempts
- ODBC RADIUS Accounting
- ODBC TACACS+ Accounting
- ODBC TACACS+ Administration
- ODBC VoIP Accounting
- Remote Logging

CSV Logs

Cisco Secure ACS records many of its logs in comma-separated value (CSV) text files. You can import CSV log files into many popular spreadsheet applications.

Back to Top

CSV Failed Attempts

Click this option to enable and configure Cisco Secure ACS to generate a CSV log of failed login attempts.

Back to Top

CSV Failed Attempts

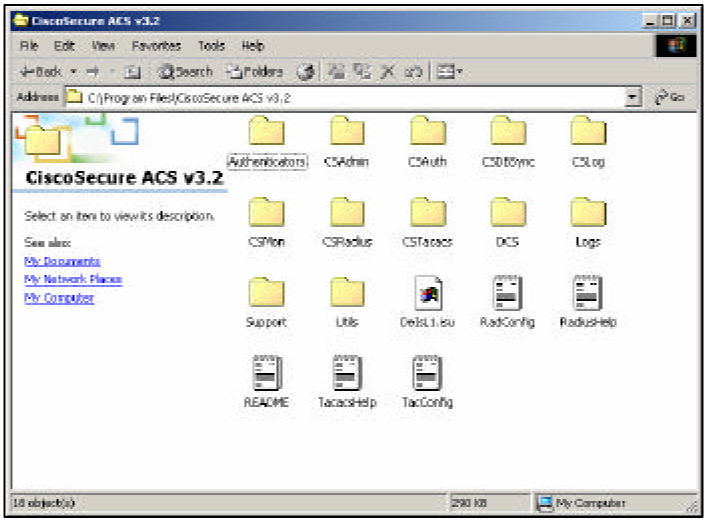
Click this option to enable and configure Cisco Secure ACS to generate a CSV log of successful login attempts.

Back to Top

CSV RADIUS Accounting

Authentication Server Troubleshooting

Additional Logging File Directories



CatOS Authenticator Troubleshooting

- **Enable 802.1x tracing on CatOS platforms**

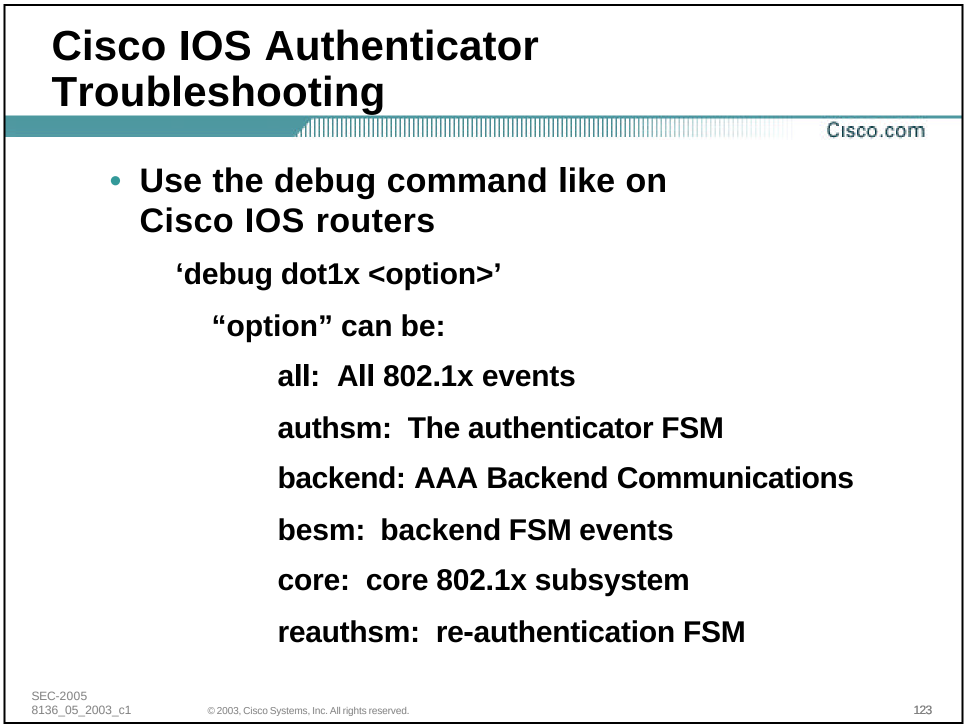
  ‘set trace dot1x <*level*>’

  “*level*” is a detail level value between 0–15

  15 will do a full packet dump!

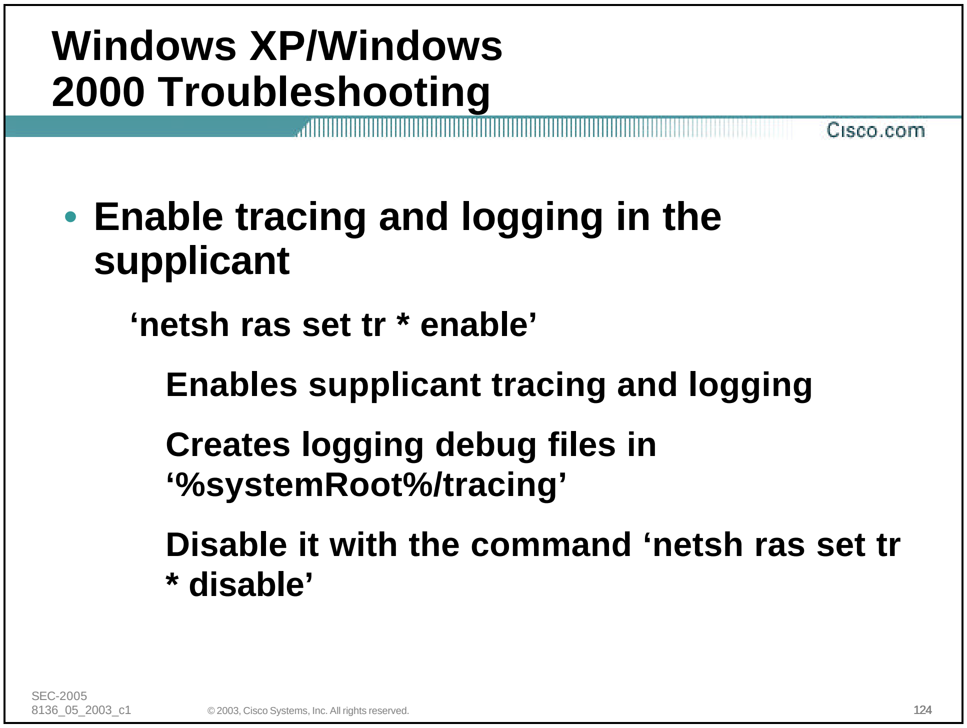
  10 is usually good enough for most troubleshooting

  Don’t forget to disable tracing once you are done!
  ‘set trace all 0’



Cisco IOS Authenticator Troubleshooting

- Use the debug command like on Cisco IOS routers
  - ‘debug dot1x <option>’
    - “option” can be:
      - all: All 802.1x events
      - authsm: The authenticator FSM
      - backend: AAA Backend Communications
      - besm: backend FSM events
      - core: core 802.1x subsystem
      - reauthsm: re-authentication FSM

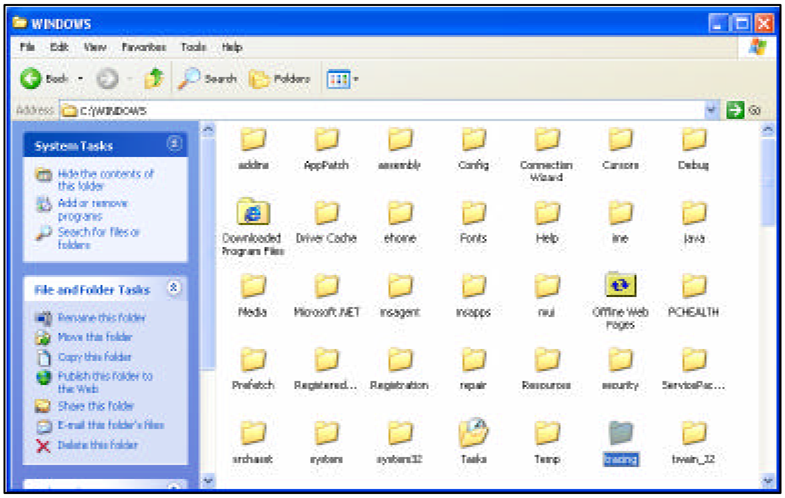


Windows XP/Windows 2000 Troubleshooting

- Enable tracing and logging in the supplicant
  - ‘netsh ras set tr * enable’
    - Enables supplicant tracing and logging
    - Creates logging debug files in ‘%systemRoot%/tracing’
    - Disable it with the command ‘netsh ras set tr * disable’

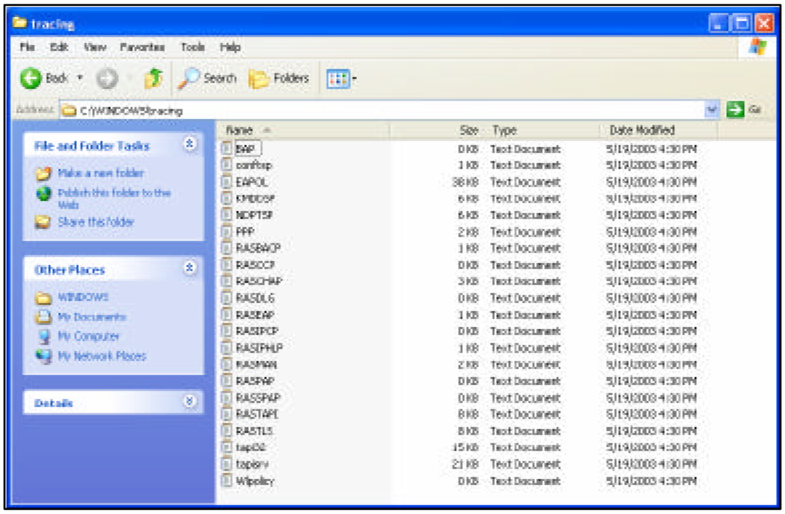
Windows Troubleshooting—Tracing Directory

Cisco.com

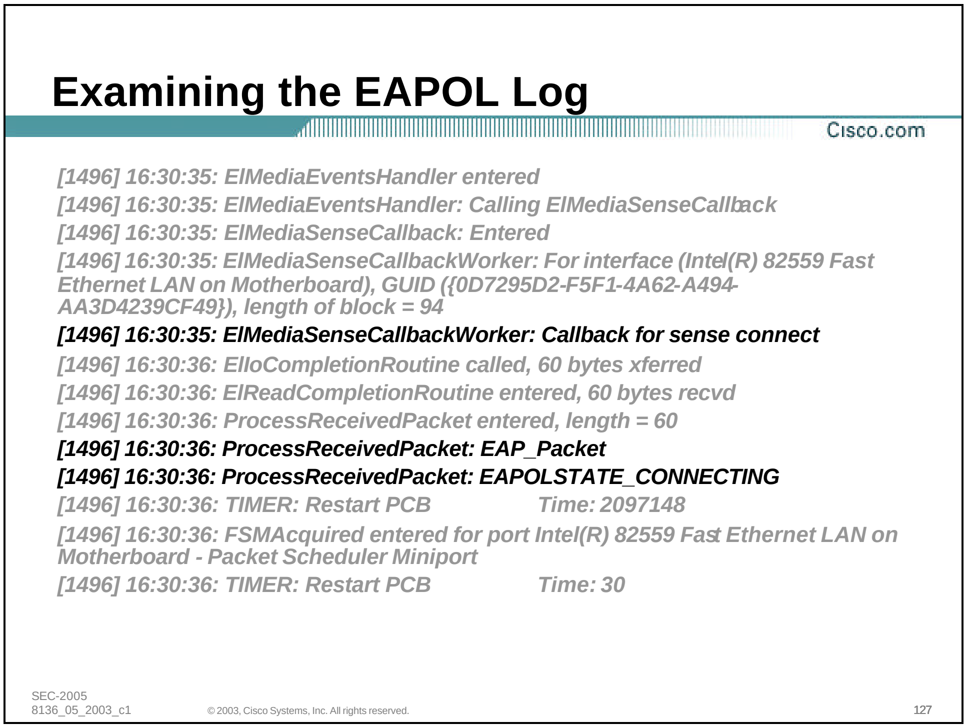


Windows Troubleshooting—Tracing Files

Cisco.com

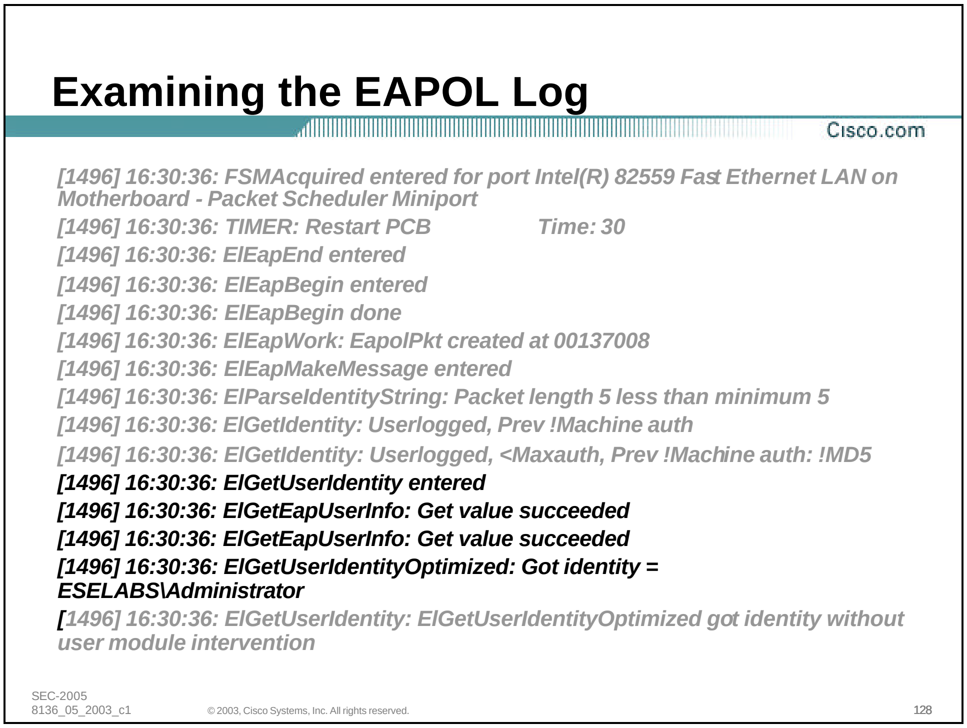


Name	Size	Type	Date Modified
EAP	0 KB	Text Document	5/19/2003 4:30 PM
confbsp	1 KB	Text Document	5/19/2003 4:30 PM
EAPOL	38 KB	Text Document	5/19/2003 4:30 PM
KMDDSP	6 KB	Text Document	5/19/2003 4:30 PM
NDPTSP	6 KB	Text Document	5/19/2003 4:30 PM
PPP	2 KB	Text Document	5/19/2003 4:30 PM
RASBACP	1 KB	Text Document	5/19/2003 4:30 PM
RASCCP	0 KB	Text Document	5/19/2003 4:30 PM
RASCHAP	3 KB	Text Document	5/19/2003 4:30 PM
RASDLG	0 KB	Text Document	5/19/2003 4:30 PM
RASEAP	1 KB	Text Document	5/19/2003 4:30 PM
RASIPCP	0 KB	Text Document	5/19/2003 4:30 PM
RASIPHLP	1 KB	Text Document	5/19/2003 4:30 PM
RASMAN	2 KB	Text Document	5/19/2003 4:30 PM
RASPAP	0 KB	Text Document	5/19/2003 4:30 PM
RASSPAP	0 KB	Text Document	5/19/2003 4:30 PM
RASTAPI	8 KB	Text Document	5/19/2003 4:30 PM
RASTLS	8 KB	Text Document	5/19/2003 4:30 PM
tapi32	15 KB	Text Document	5/19/2003 4:30 PM
tapisrv	21 KB	Text Document	5/19/2003 4:30 PM
Wlpolicy	0 KB	Text Document	5/19/2003 4:30 PM



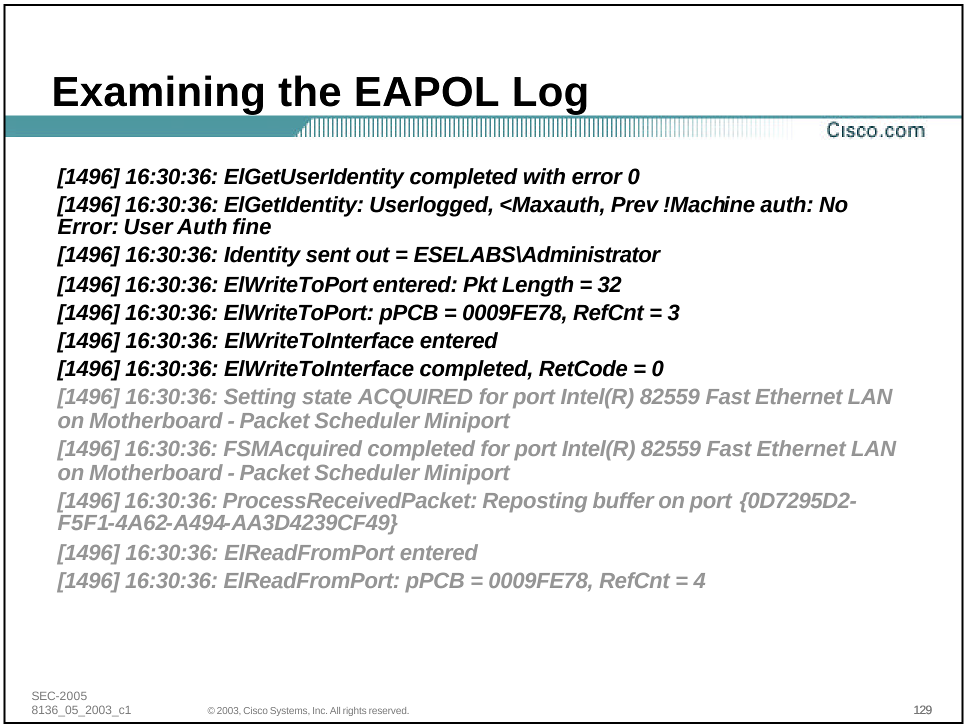
Examining the EAPOL Log

```
[1496] 16:30:35: ElMediaEventsHandler entered
[1496] 16:30:35: ElMediaEventsHandler: Calling ElMediaSenseCallback
[1496] 16:30:35: ElMediaSenseCallback: Entered
[1496] 16:30:35: ElMediaSenseCallbackWorker: For interface (Intel(R) 82559 Fast
Ethernet LAN on Motherboard), GUID ({0D7295D2-F5F1-4A62-A494-
AA3D4239CF49}), length of block = 94
[1496] 16:30:35: ElMediaSenseCallbackWorker: Callback for sense connect
[1496] 16:30:36: ElIoCompletionRoutine called, 60 bytes xferred
[1496] 16:30:36: ElReadCompletionRoutine entered, 60 bytes recvd
[1496] 16:30:36: ProcessReceivedPacket entered, length = 60
[1496] 16:30:36: ProcessReceivedPacket: EAP_Packet
[1496] 16:30:36: ProcessReceivedPacket: EAPOLSTATE_CONNECTING
[1496] 16:30:36: TIMER: Restart PCB              Time: 2097148
[1496] 16:30:36: FSMAcquired entered for port Intel(R) 82559 Fast Ethernet LAN on
Motherboard - Packet Scheduler Miniport
[1496] 16:30:36: TIMER: Restart PCB              Time: 30
```



Examining the EAPOL Log

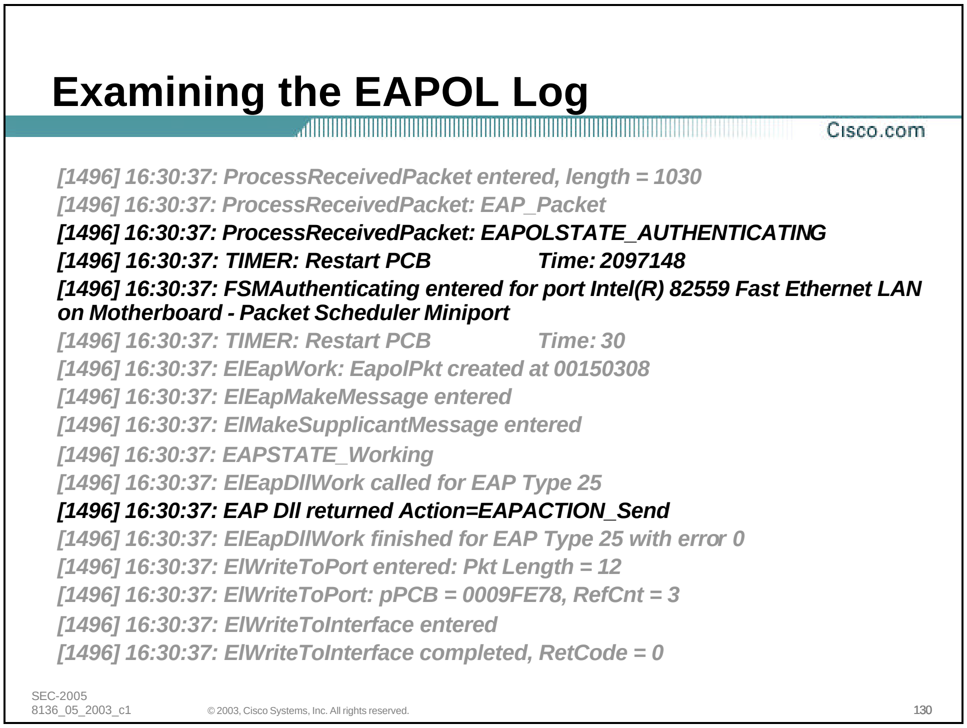
```
[1496] 16:30:36: FSMAcquired entered for port Intel(R) 82559 Fast Ethernet LAN on
Motherboard - Packet Scheduler Miniport
[1496] 16:30:36: TIMER: Restart PCB              Time: 30
[1496] 16:30:36: ElEapEnd entered
[1496] 16:30:36: ElEapBegin entered
[1496] 16:30:36: ElEapBegin done
[1496] 16:30:36: ElEapWork: EapolPkt created at 00137008
[1496] 16:30:36: ElEapMakeMessage entered
[1496] 16:30:36: ElParseIdentityString: Packet length 5 less than minimum 5
[1496] 16:30:36: ElGetIdentity: Userlogged, Prev !Machine auth
[1496] 16:30:36: ElGetIdentity: Userlogged, <Maxauth, Prev !Machine auth: !MD5
[1496] 16:30:36: ElGetUserIdentity entered
[1496] 16:30:36: ElGetEapUserInfo: Get value succeeded
[1496] 16:30:36: ElGetEapUserInfo: Get value succeeded
[1496] 16:30:36: ElGetUserIdentityOptimized: Got identity =
ESELABS\Administrator
[1496] 16:30:36: ElGetUserIdentity: ElGetUserIdentityOptimized got identity without
user module intervention
```



Examining the EAPOL Log

Cisco.com

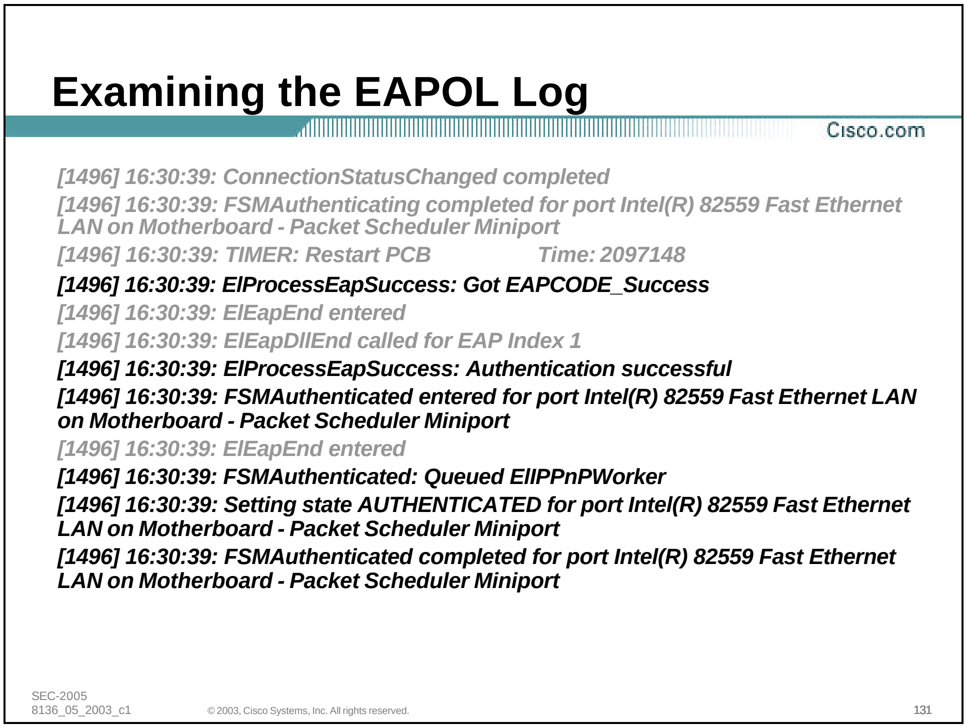
```
[1496] 16:30:36: ElGetUserIdentity completed with error 0
[1496] 16:30:36: ElGetIdentity: Userlogged, <Maxauth, Prev !Machine auth: No
Error: User Auth fine
[1496] 16:30:36: Identity sent out = ESELABS\Administrator
[1496] 16:30:36: ElWriteToPort entered: Pkt Length = 32
[1496] 16:30:36: ElWriteToPort: pPCB = 0009FE78, RefCnt = 3
[1496] 16:30:36: ElWriteToInterface entered
[1496] 16:30:36: ElWriteToInterface completed, RetCode = 0
[1496] 16:30:36: Setting state ACQUIRED for port Intel(R) 82559 Fast Ethernet LAN
on Motherboard - Packet Scheduler Miniport
[1496] 16:30:36: FSMAcquired completed for port Intel(R) 82559 Fast Ethernet LAN
on Motherboard - Packet Scheduler Miniport
[1496] 16:30:36: ProcessReceivedPacket: Reposting buffer on port {0D7295D2-
F5F1-4A62-A494-AA3D4239CF49}
[1496] 16:30:36: ElReadFromPort entered
[1496] 16:30:36: ElReadFromPort: pPCB = 0009FE78, RefCnt = 4
```



Examining the EAPOL Log

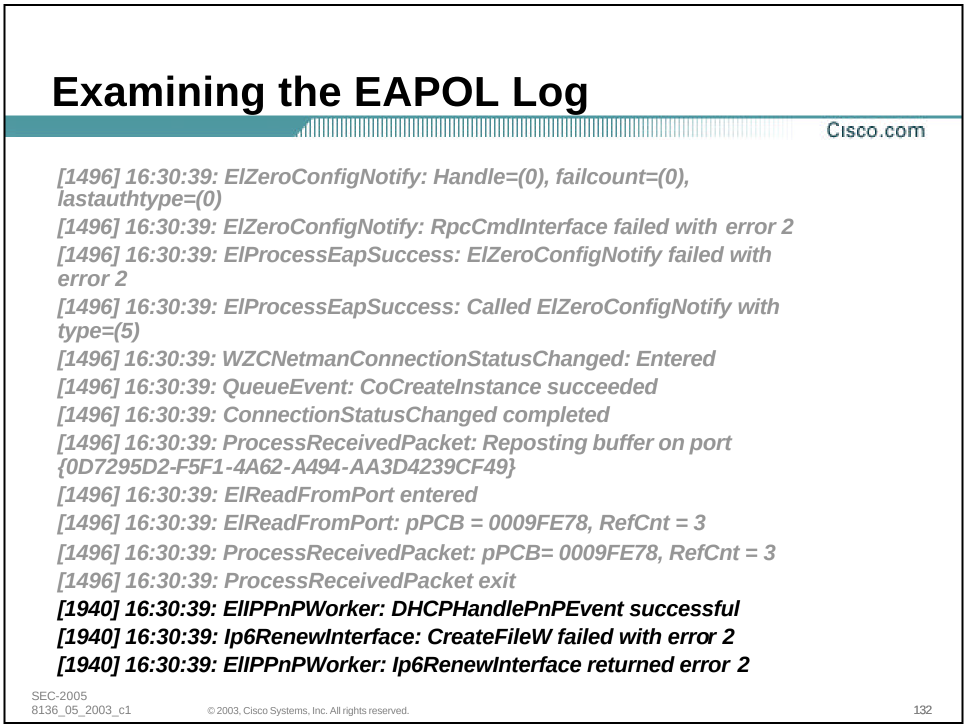
Cisco.com

```
[1496] 16:30:37: ProcessReceivedPacket entered, length = 1030
[1496] 16:30:37: ProcessReceivedPacket: EAP_Packet
[1496] 16:30:37: ProcessReceivedPacket: EAPOLSTATE_AUTHENTICATING
[1496] 16:30:37: TIMER: Restart PCB              Time: 2097148
[1496] 16:30:37: FSMAuthenticating entered for port Intel(R) 82559 Fast Ethernet LAN
on Motherboard - Packet Scheduler Miniport
[1496] 16:30:37: TIMER: Restart PCB              Time: 30
[1496] 16:30:37: ElEapWork: EapolPkt created at 00150308
[1496] 16:30:37: ElEapMakeMessage entered
[1496] 16:30:37: ElMakeSupplicantMessage entered
[1496] 16:30:37: EAPSTATE_Working
[1496] 16:30:37: ElEapDllWork called for EAP Type 25
[1496] 16:30:37: EAP Dll returned Action=EAPACTION_Send
[1496] 16:30:37: ElEapDllWork finished for EAP Type 25 with error 0
[1496] 16:30:37: ElWriteToPort entered: Pkt Length = 12
[1496] 16:30:37: ElWriteToPort: pPCB = 0009FE78, RefCnt = 3
[1496] 16:30:37: ElWriteToInterface entered
[1496] 16:30:37: ElWriteToInterface completed, RetCode = 0
```



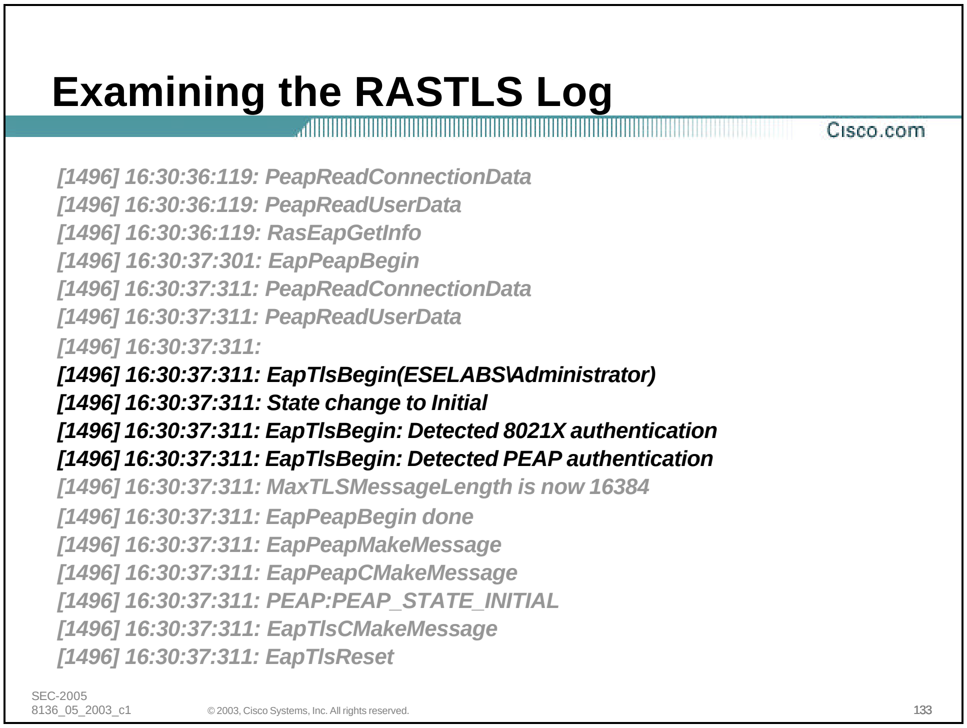
Examining the EAPOL Log

```
[1496] 16:30:39: ConnectionStatusChanged completed
[1496] 16:30:39: FSMAuthenticating completed for port Intel(R) 82559 Fast Ethernet
LAN on Motherboard - Packet Scheduler Miniport
[1496] 16:30:39: TIMER: Restart PCB              Time: 2097148
[1496] 16:30:39: ElProcessEapSuccess: Got EAPCODE_Success
[1496] 16:30:39: ElEapEnd entered
[1496] 16:30:39: ElEapDllEnd called for EAP Index 1
[1496] 16:30:39: ElProcessEapSuccess: Authentication successful
[1496] 16:30:39: FSMAuthenticated entered for port Intel(R) 82559 Fast Ethernet LAN
on Motherboard - Packet Scheduler Miniport
[1496] 16:30:39: ElEapEnd entered
[1496] 16:30:39: FSMAuthenticated: Queued ElIPPnPWorker
[1496] 16:30:39: Setting state AUTHENTICATED for port Intel(R) 82559 Fast Ethernet
LAN on Motherboard - Packet Scheduler Miniport
[1496] 16:30:39: FSMAuthenticated completed for port Intel(R) 82559 Fast Ethernet
LAN on Motherboard - Packet Scheduler Miniport
```



Examining the EAPOL Log

```
[1496] 16:30:39: ElZeroConfigNotify: Handle=(0), failcount=(0),
lastauthtype=(0)
[1496] 16:30:39: ElZeroConfigNotify: RpcCmdInterface failed with error 2
[1496] 16:30:39: ElProcessEapSuccess: ElZeroConfigNotify failed with
error 2
[1496] 16:30:39: ElProcessEapSuccess: Called ElZeroConfigNotify with
type=(5)
[1496] 16:30:39: WZCNetmanConnectionStatusChanged: Entered
[1496] 16:30:39: QueueEvent: CoCreateInstance succeeded
[1496] 16:30:39: ConnectionStatusChanged completed
[1496] 16:30:39: ProcessReceivedPacket: Reposting buffer on port
{0D7295D2-F5F1-4A62-A494-AA3D4239CF49}
[1496] 16:30:39: ElReadFromPort entered
[1496] 16:30:39: ElReadFromPort: pPCB = 0009FE78, RefCnt = 3
[1496] 16:30:39: ProcessReceivedPacket: pPCB= 0009FE78, RefCnt = 3
[1496] 16:30:39: ProcessReceivedPacket exit
[1940] 16:30:39: ElIPPnPWorker: DHCPHandlePnPEvent successful
[1940] 16:30:39: Ip6RenewInterface: CreateFileW failed with error 2
[1940] 16:30:39: ElIPPnPWorker: Ip6RenewInterface returned error 2
```

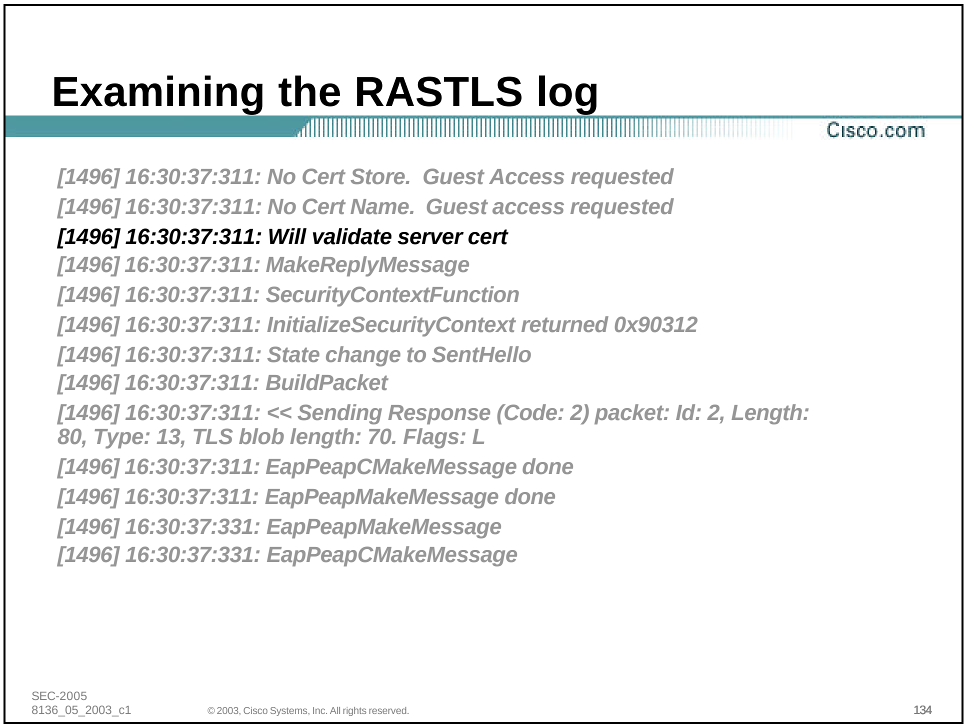


Examining the RASTLS Log

Cisco.com

```
[1496] 16:30:36:119: PeapReadConnectionData
[1496] 16:30:36:119: PeapReadUserData
[1496] 16:30:36:119: RasEapGetInfo
[1496] 16:30:37:301: EapPeapBegin
[1496] 16:30:37:311: PeapReadConnectionData
[1496] 16:30:37:311: PeapReadUserData
[1496] 16:30:37:311:
[1496] 16:30:37:311: EapTlsBegin(ESELABS\Administrator)
[1496] 16:30:37:311: State change to Initial
[1496] 16:30:37:311: EapTlsBegin: Detected 8021X authentication
[1496] 16:30:37:311: EapTlsBegin: Detected PEAP authentication
[1496] 16:30:37:311: MaxTLSMessageLength is now 16384
[1496] 16:30:37:311: EapPeapBegin done
[1496] 16:30:37:311: EapPeapMakeMessage
[1496] 16:30:37:311: EapPeapCMakeMessage
[1496] 16:30:37:311: PEAP:PEAP_STATE_INITIAL
[1496] 16:30:37:311: EapTlsCMakeMessage
[1496] 16:30:37:311: EapTlsReset
```

SEC-2005
8136_05_2003_c1 © 2003, Cisco Systems, Inc. All rights reserved. 133

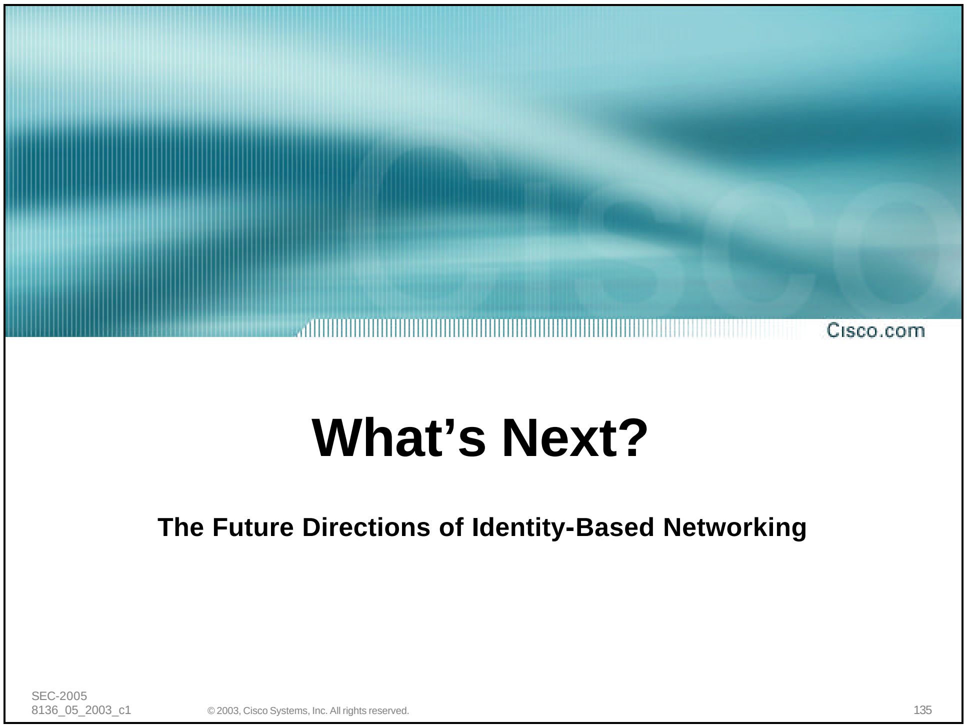


Examining the RASTLS log

Cisco.com

```
[1496] 16:30:37:311: No Cert Store.  Guest Access requested
[1496] 16:30:37:311: No Cert Name.  Guest access requested
[1496] 16:30:37:311: Will validate server cert
[1496] 16:30:37:311: MakeReplyMessage
[1496] 16:30:37:311: SecurityContextFunction
[1496] 16:30:37:311: InitializeSecurityContext returned 0x90312
[1496] 16:30:37:311: State change to SentHello
[1496] 16:30:37:311: BuildPacket
[1496] 16:30:37:311: << Sending Response (Code: 2) packet: Id: 2, Length:
80, Type: 13, TLS blob length: 70. Flags: L
[1496] 16:30:37:311: EapPeapCMakeMessage done
[1496] 16:30:37:311: EapPeapMakeMessage done
[1496] 16:30:37:331: EapPeapMakeMessage
[1496] 16:30:37:331: EapPeapCMakeMessage
```

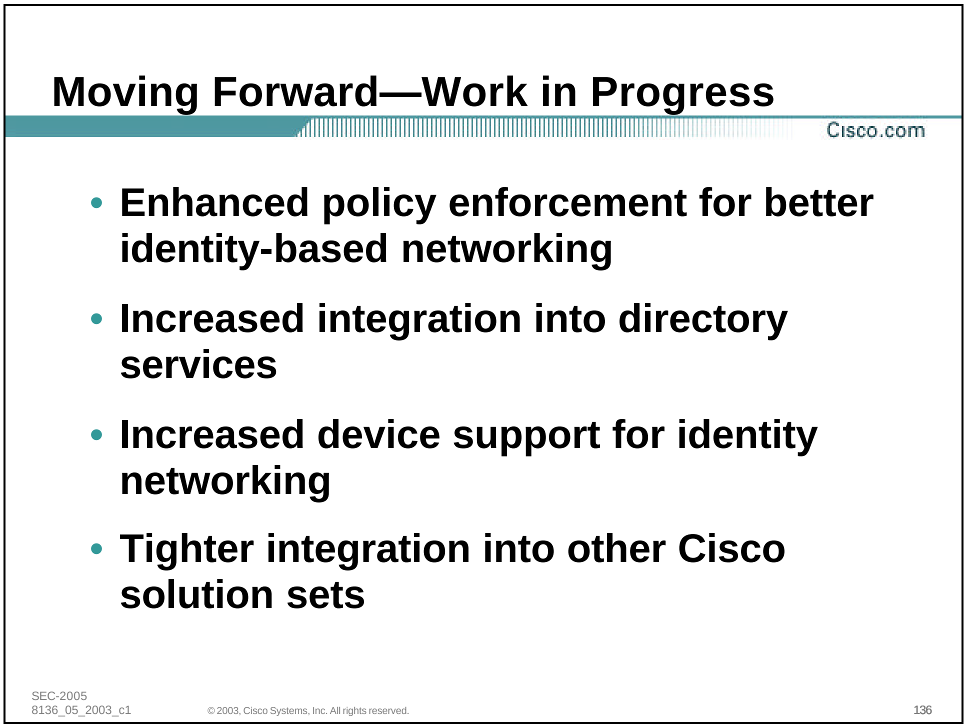
SEC-2005
8136_05_2003_c1 © 2003, Cisco Systems, Inc. All rights reserved. 134



Cisco.com

What’s Next?

The Future Directions of Identity-Based Networking



Moving Forward—Work in Progress

Cisco.com

- Enhanced policy enforcement for better identity-based networking
- Increased integration into directory services
- Increased device support for identity networking
- Tighter integration into other Cisco solution sets

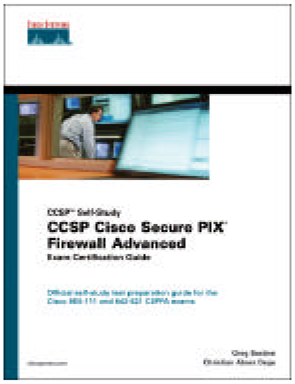
Recommended Reading

Cisco.com

Network Security Principles and Practices
ISBN: 1587050250

CCIE Security Exam Certification Guide
ISBN: 1587200651

CCIE Practical Studies: Security
ISBN: 1587051109



Available on-site at the Cisco Company Store

Recommended Reading

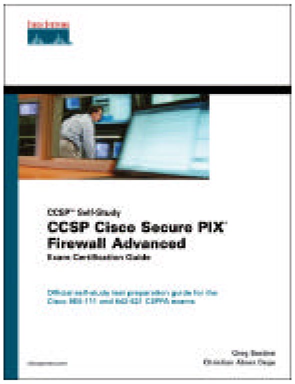
Cisco.com

Managing Cisco Network Security
ISBN: 1578701031

Cisco Secure Internet Security Solutions
ISBN: 1587050161

Designing Network Security, Second Ed.
ISBN: 1587051176
Available in Oct 2003

Available on-site at the Cisco Company Store



NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.

Please Complete Your Evaluation Form

Session SEC-2005

CISCO SYSTEMS

CISCO SYSTEMS