



# Cisco Identity Based Networking Services

# Overview and Agenda

- **Looking at the concepts of authentication.**
- **Applying them to network access control.**
- **Understanding the protocols & mechanisms behind 802.1x.**
- **Understanding various authentication (EAP) methods.**
- **Understanding PKI Certs in the context of 802.1x authentication.**
- **Understanding authorization & policy enforcement with 802.1x.**



# Threat Model Overview

# Risk Assessment – Potential cost of External Threats

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 & Security Survey

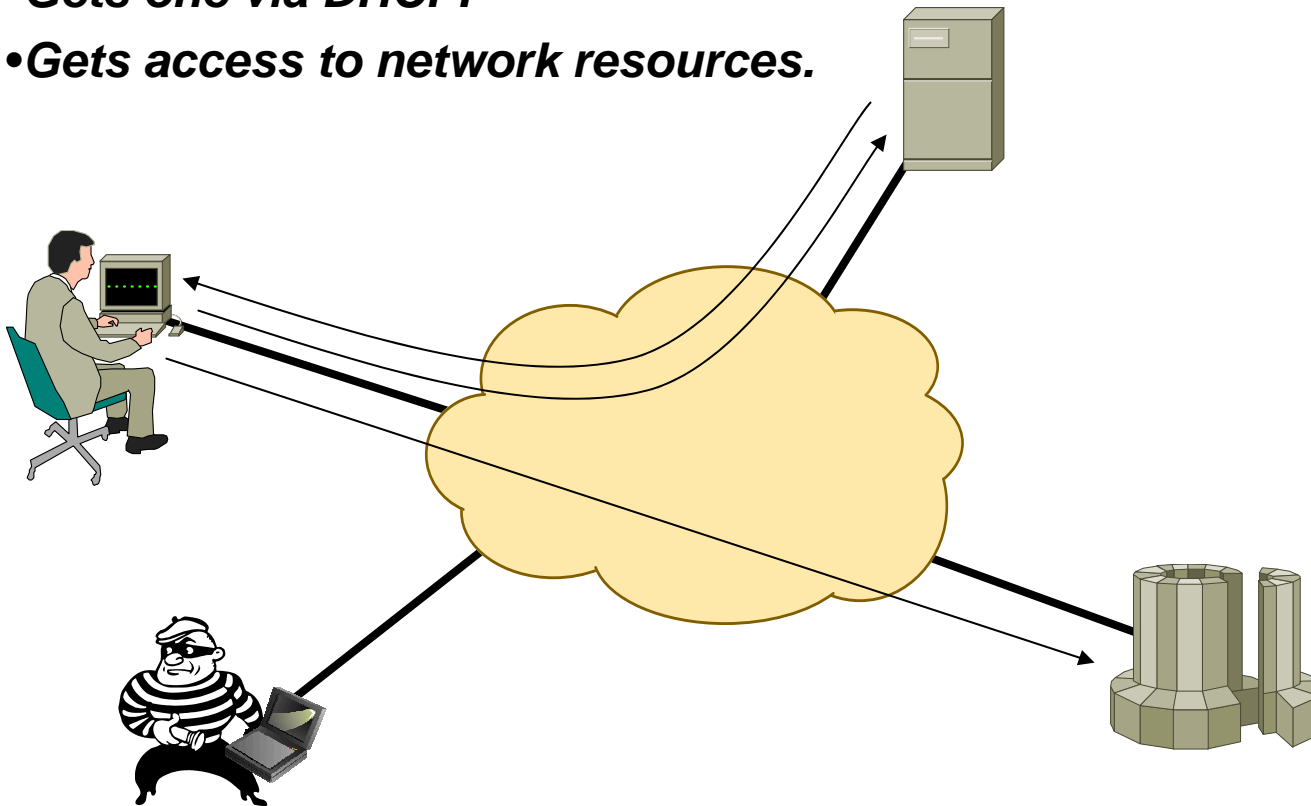
**Providing Authentication and access control on network ports can significantly reduce the potential attacker community.**

**“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

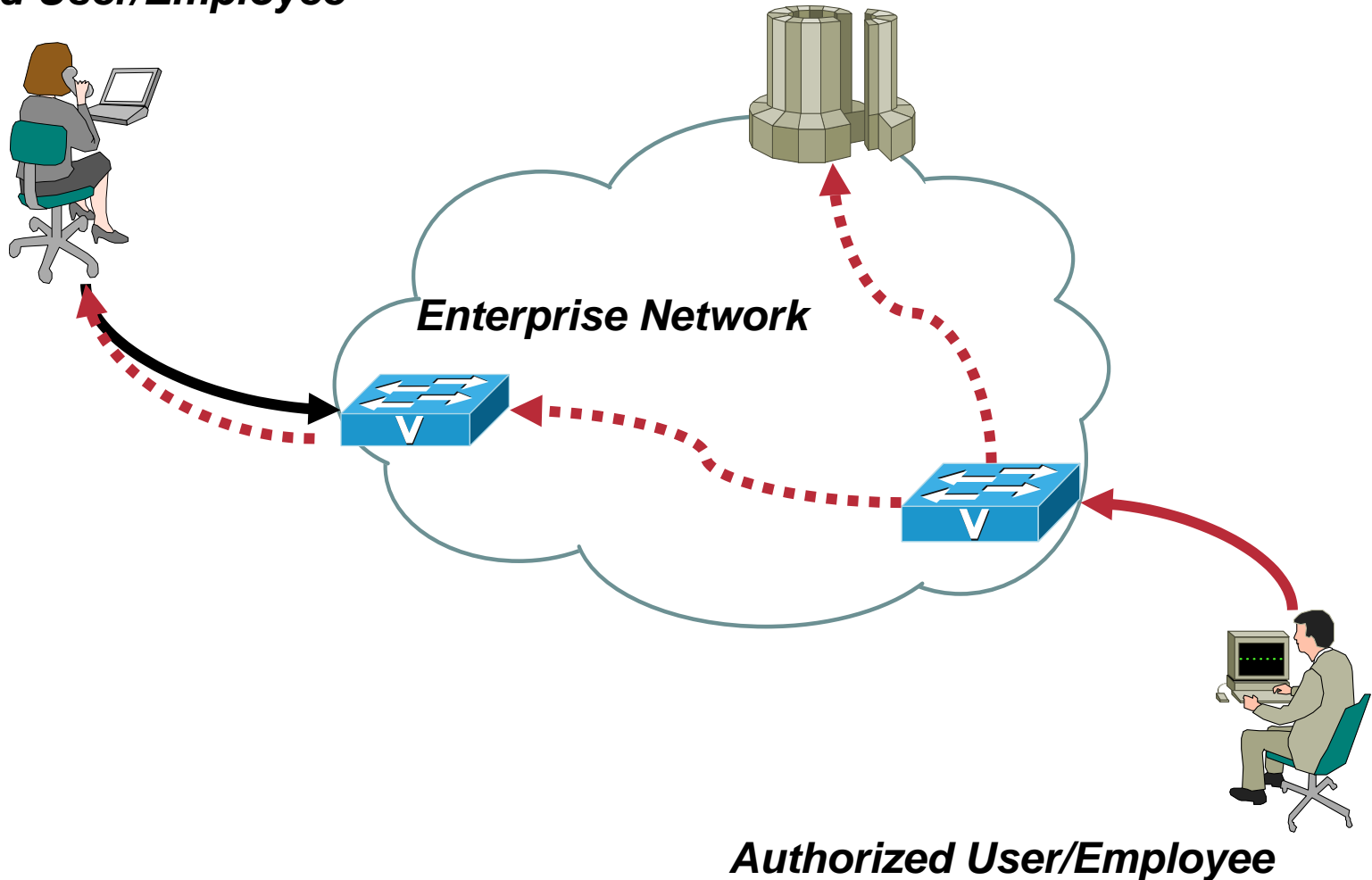
- Source: CSI/FBI 2002 Computer Crime & Security Survey

**Providing policy enforcement, compartmentalization, and usage monitoring can further reduce the risk.**

**“Keep the insiders honest”**

# Unauthorized Use of the Network

*Authorized User/Employee*

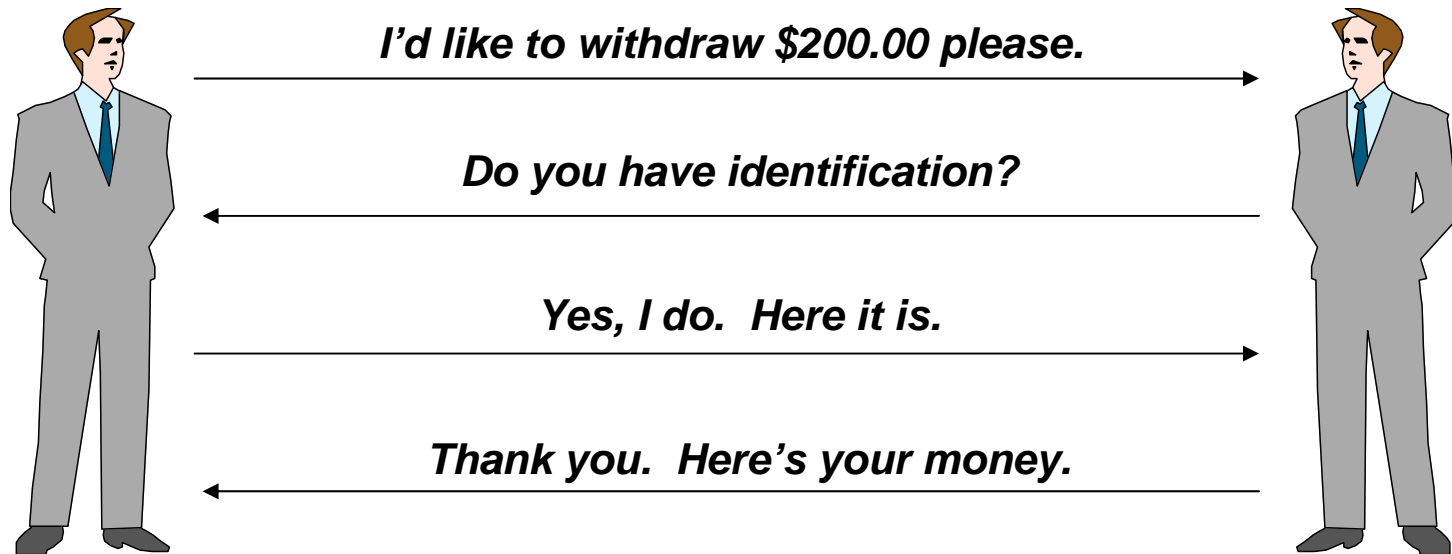




# Understanding Authentication

# 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.
- Authentication is only as strong as method of verification.



# 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?

- **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?

- **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.**

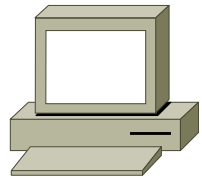


# An Operational Overview of Network Authentication

# 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

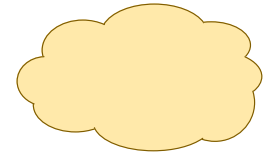


*I'd like to connect to the network*

*Do you have identification?*

*Yes, I do. Here it is.*

*Thank you. Here you go.*



# Applying the Authentication Model to the Network

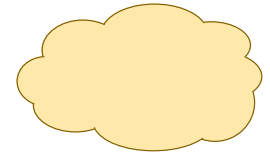


*I'd like to connect to the network*

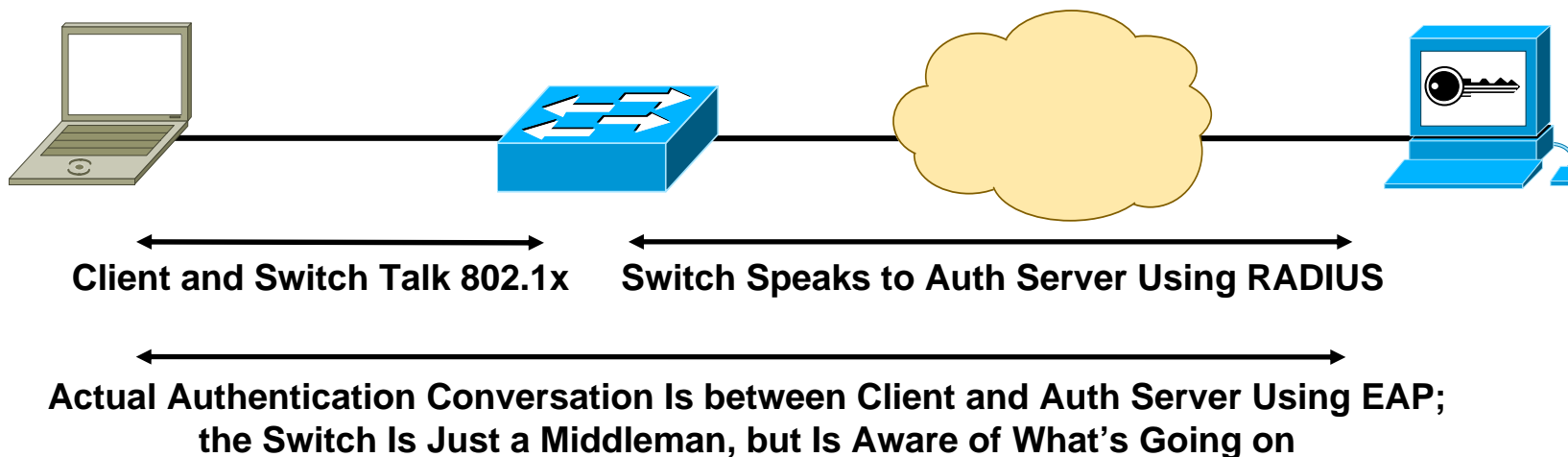
*Do you have identification?*

*Yes, I do. Here it is.*

*Thank you. Here you go.*



# Wired Access Control Model





# Protocols & Mechanisms

# IEEE 802.1x?

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

# Some IEEE Terminology

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

# What Does It Do?

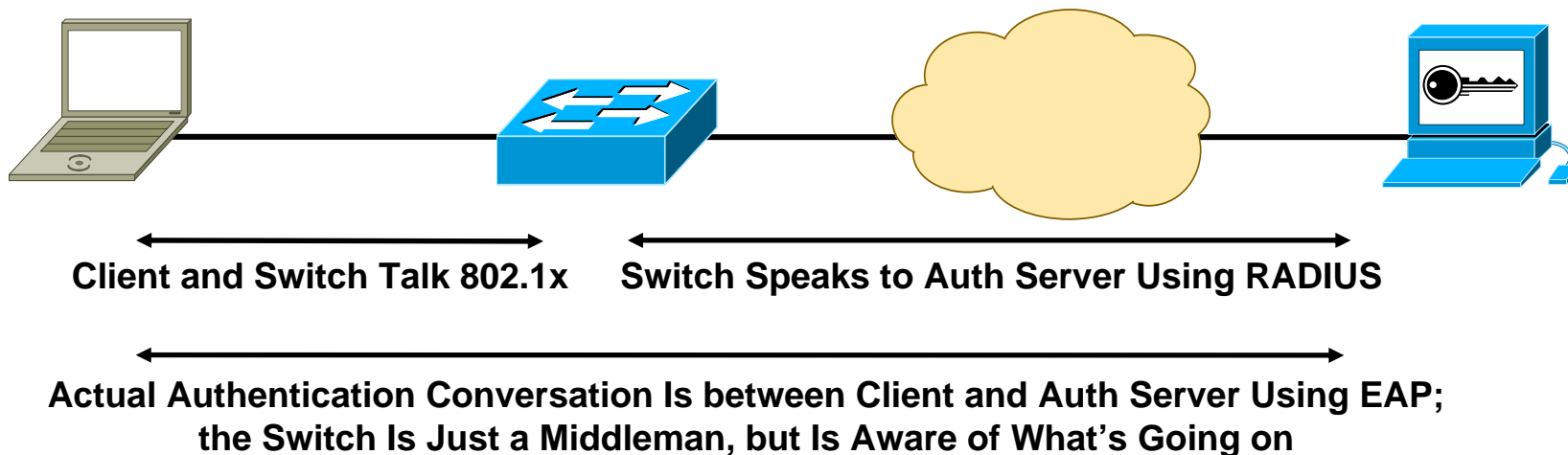
- Transport authentication information in the form of Extensible Authentication Protocol (EAP) payloads
- The authenticator (switch) becomes the middleman for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information
- Three forms of EAP are specified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

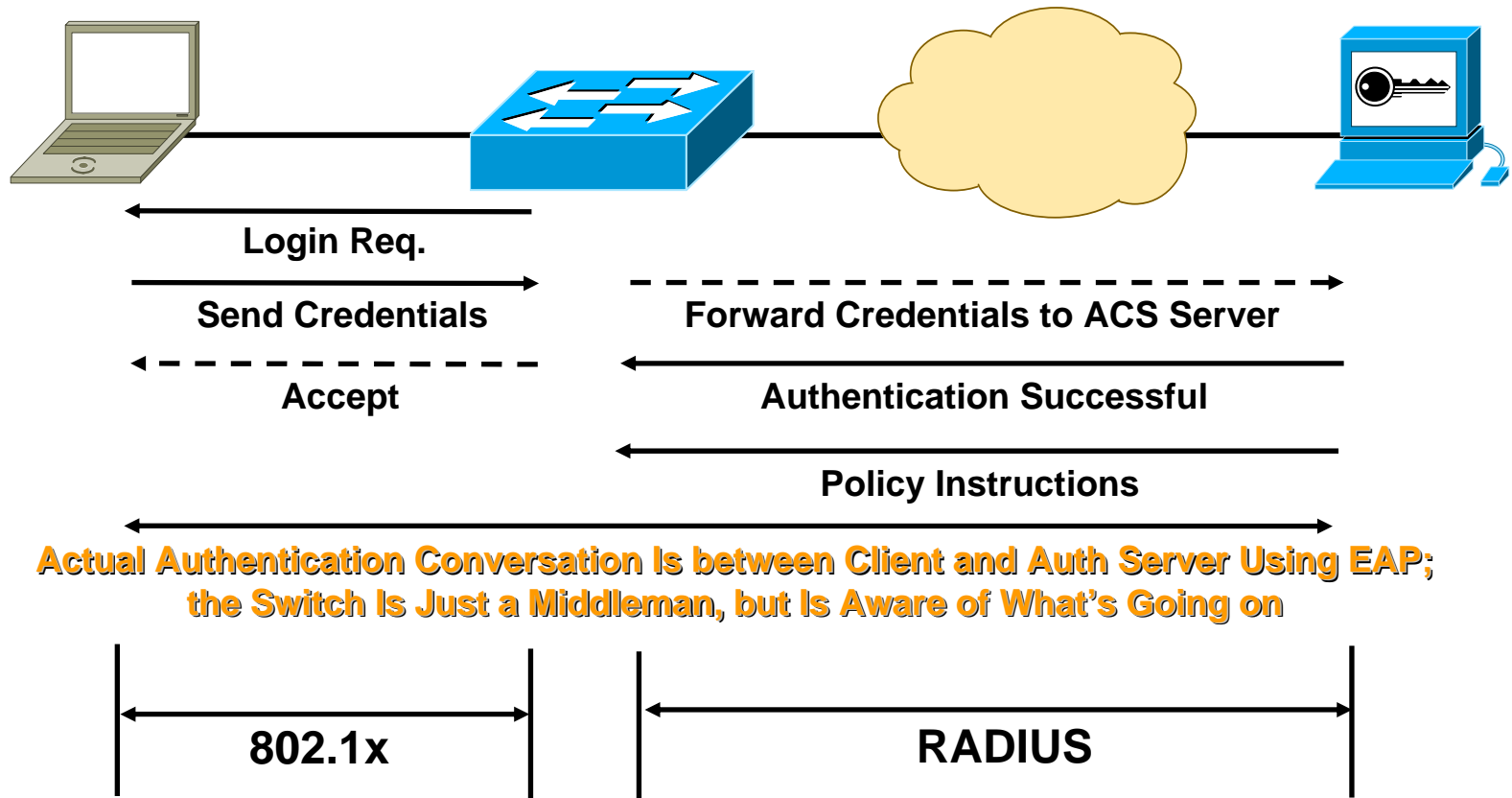
*802.1x Header*

*EAP Payload*

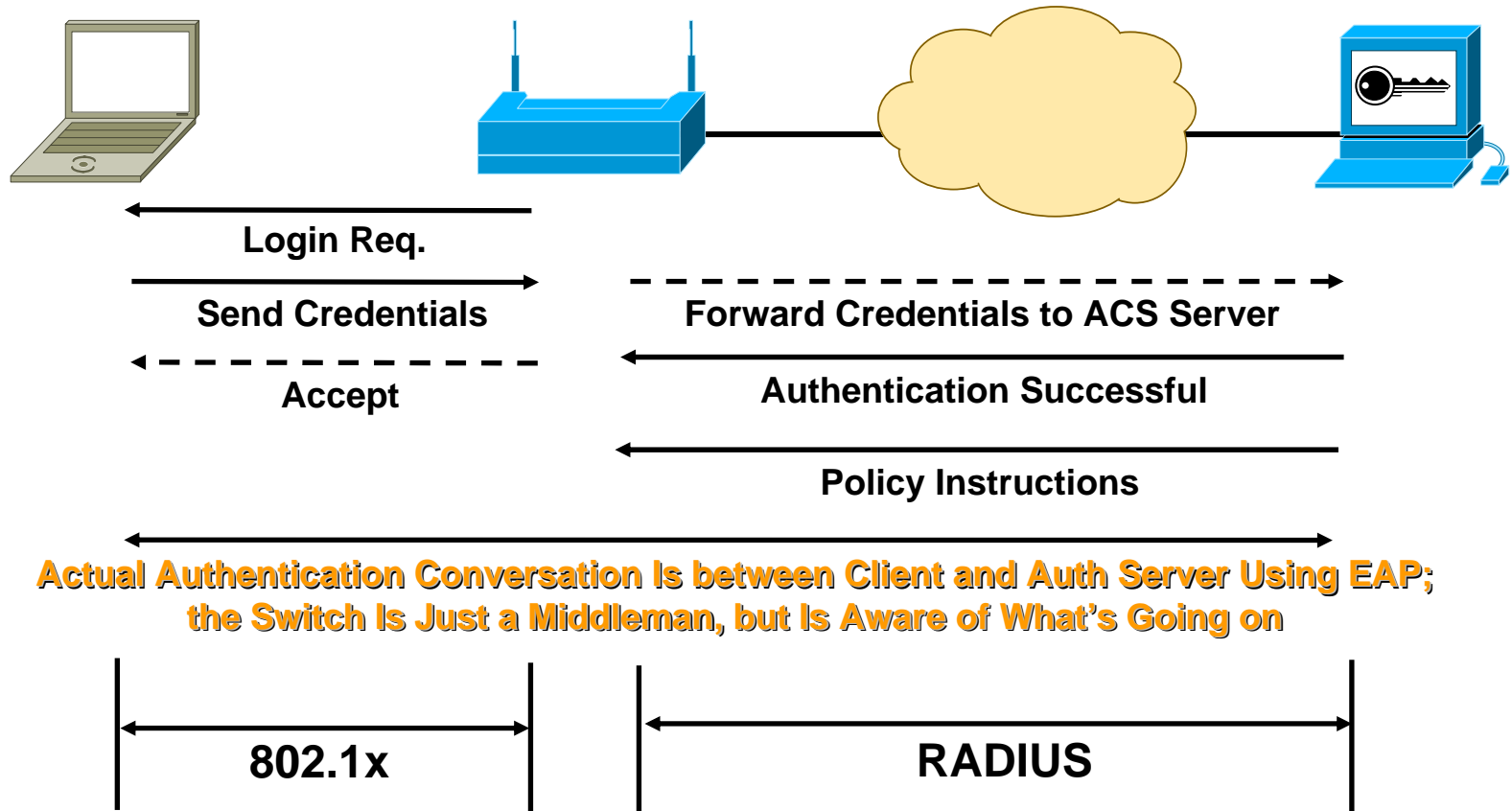
# Wired Access Control Model



# A Closer Look...



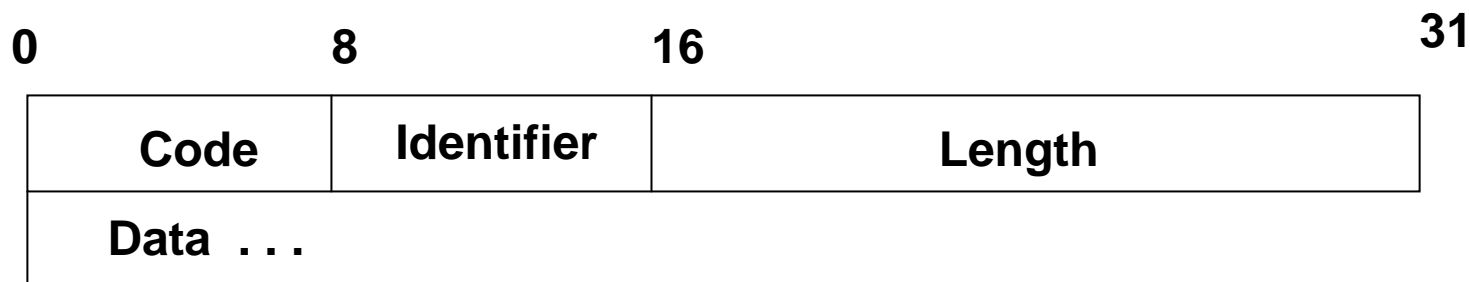
# Wireless Access Control Model



# What Is EAP?

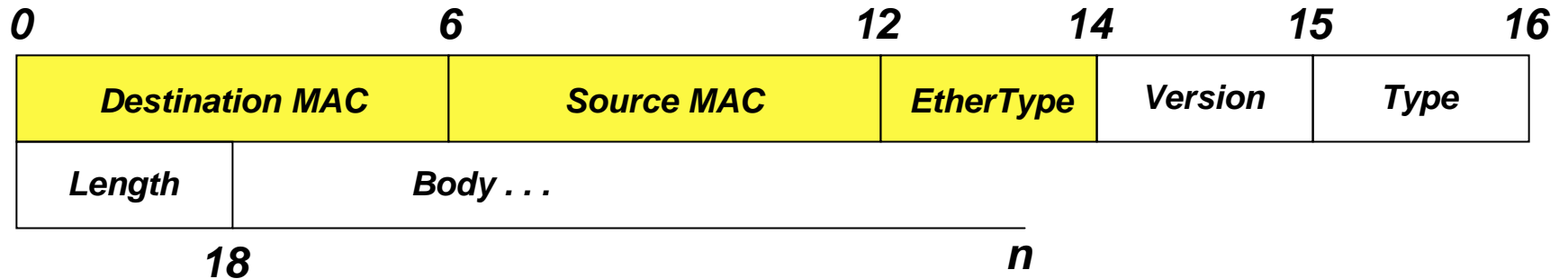
- **EAP—The Extensible Authentication Protocol**
- **Defined in RFC 2284**
- **A flexible protocol used to carry arbitrary authentication information**
- **Typically rides on top of another protocol such as 802.1x or RADIUS (could be TACACS+, etc.)**

# Extensible Authentication Protocol (EAP)



- **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



## Authenticator to Supplicant

**Destination MAC: 01-80-C2-00-00-03 until learned then unicast**

**Source MAC: Unicast Authenticator MAC**

## Supplicant to Authenticator

**Destination MAC: 01-80-C2-00-00-03**

**Source MAC: Unicast Supplicant MAC**





























# 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.
- ✓ **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.
- ✓ **LEAP:** Uses username/password authentication
- ✓ **EAP-GTC:** Generic token & OTP authentication

# EAP Method Comparison

	Username/Password Credentials	Challenge-Response	Encrypted/Crypto Protected	Single Sign On
<b>EAP-MD5</b>				
<b>EAP-TLS</b>				
<b>EAP-MSCHAPv2</b>				
<b>LEAP</b>				
<b>PEAP</b>				
<b>EAP-GTC</b>				
<b>EAP-TTLS</b>				

# How Is RADIUS in 802.1x?

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



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



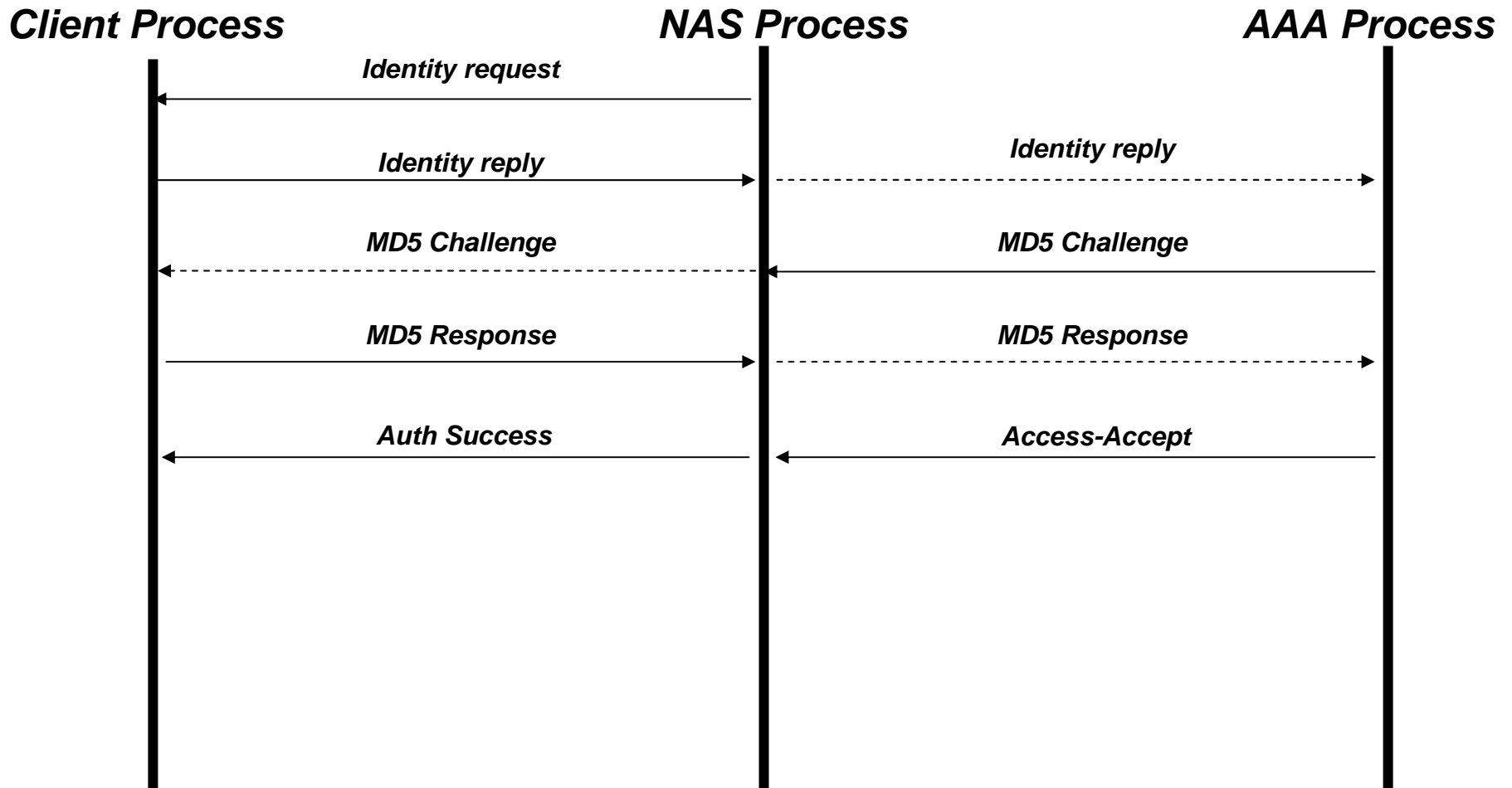


# Understanding EAP-MD5

# 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



# EAP-MD5 Pros & Cons

## 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.**

# LEAP

- **Very much like EAP-MD5 except uses another (undisclosed) hashing algorithm.**
- **Also makes accommodations for WEP key rotation.**
- **Used extensively in wireless, not in wired 802.1x.**
- **Lightweight – hence the name Lightweight EAP.**
- **Can be programmed into the DSP of the wireless NIC for very fast, hardware based, authentication.**



# Understanding Public-Key Cryptography and Certificates

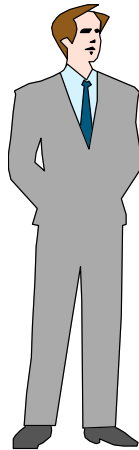
# What Is a PKI Cert?

- It is a statement of identity signed by a trusted third party
- Like a passport
- Passport is signed by the passport office, stating your verified identity
- A PKI cert is signed by a certificate authority stating your verified identity
- Unlike passports, PKI certs can't easily be forged
- When implemented **properly**, PKI certs provide “strong” authentication

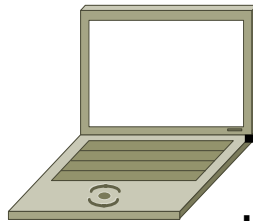
# How Does a PKI Cert Work?

- **Uses Public-Key Cryptography to establish identities**
- **Does this by using Public-Key verification of digital signatures**
- **For the rest of this presentation we just need to understand that a PKI cert can guarantee an identity**

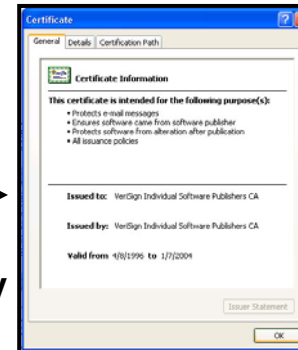
# Using a PKI Certificate



**Hello Mr. Customs Agent; I Have  
This to Validate My Identity**



**Hello Authentication Server; I  
Have This to Validate My Identity**



- **A Public-Key Infrastructure Certificate contains:**
  - Information on the Identity of the holder**
  - The holder's public key**
  - The signing authority**
  - A whole lot of other miscellaneous information.**
- **The signing authority needs to be a trusted third party. This is typically known as the Certificate Authority or CA.**

# Certificate Authorities

- **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**

# Important Fields in x.509 v3 Certs

- The following fields in a PKI cert are **CRITICAL** for it to work properly:
- **Subject Name (also known as CN name)** – should match exactly the identity that will be transmitted as the identity to authenticate. **le. Server cert must match the server name, user cert must match the user name AS IT IS TRANSMITTED**
- **Valid From/Expiration Date** – Cert must be within these two dates as perceived from the receiver or the side doing the cert checking. **Make sure times/dates are set properly.**
- **Enhanced Key Usage** – The EKU should be formatted accordingly for the type of use allowed or that the cert is to be used for. This is indicated by an OID.

Client authentication:

Server Authentication:

**When using MS CA this can be simplified by choosing the correct template type from an enterprise root CA.**

Client authentication: User template

Server Authentication: Web Server template



# Understanding EAP-TLS

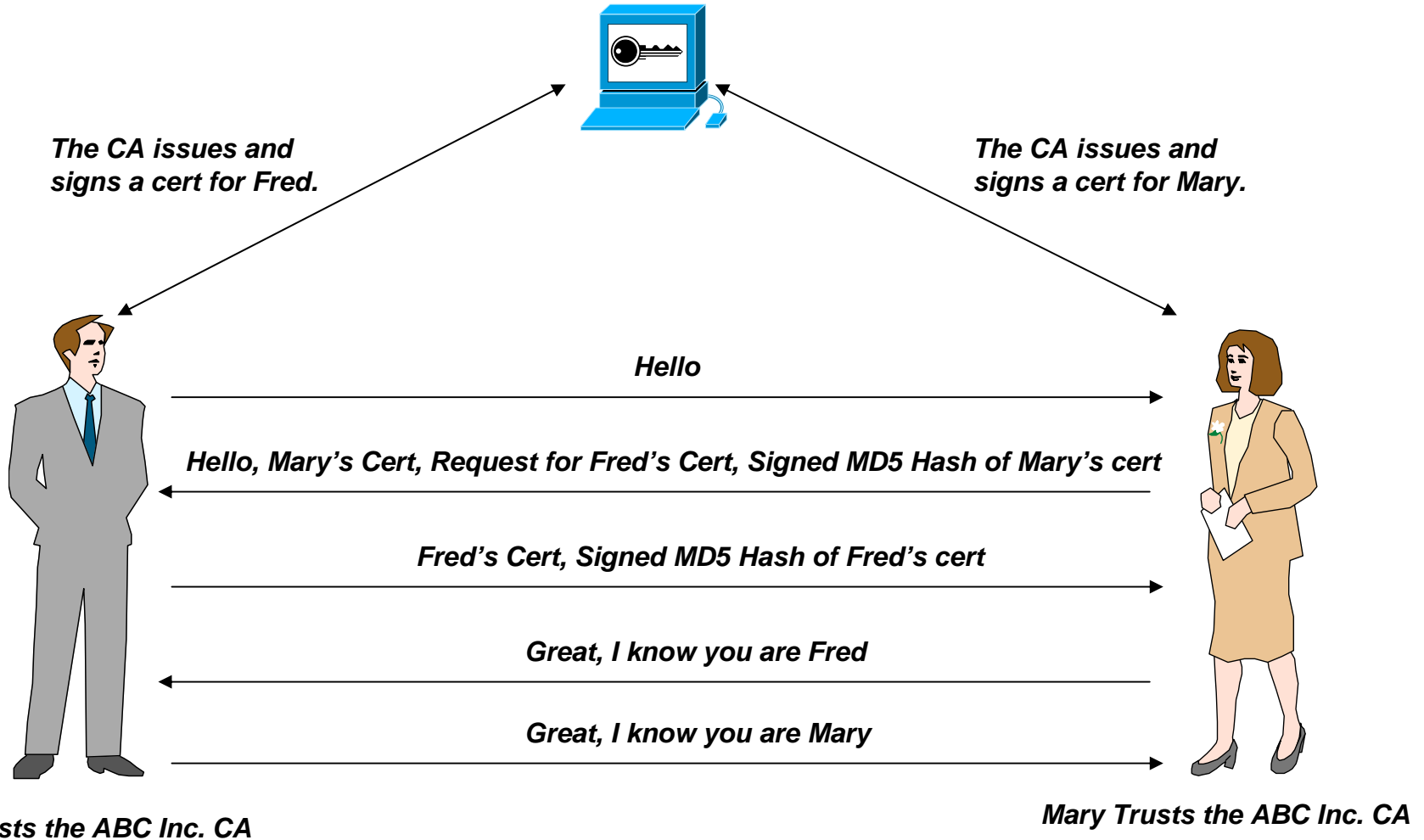
# EAP-TLS Authentication

- **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 & PKI Certificates

- **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.**

# The TLS Authentication Model (RSA Based)



# How Fred Authenticates Mary

- **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

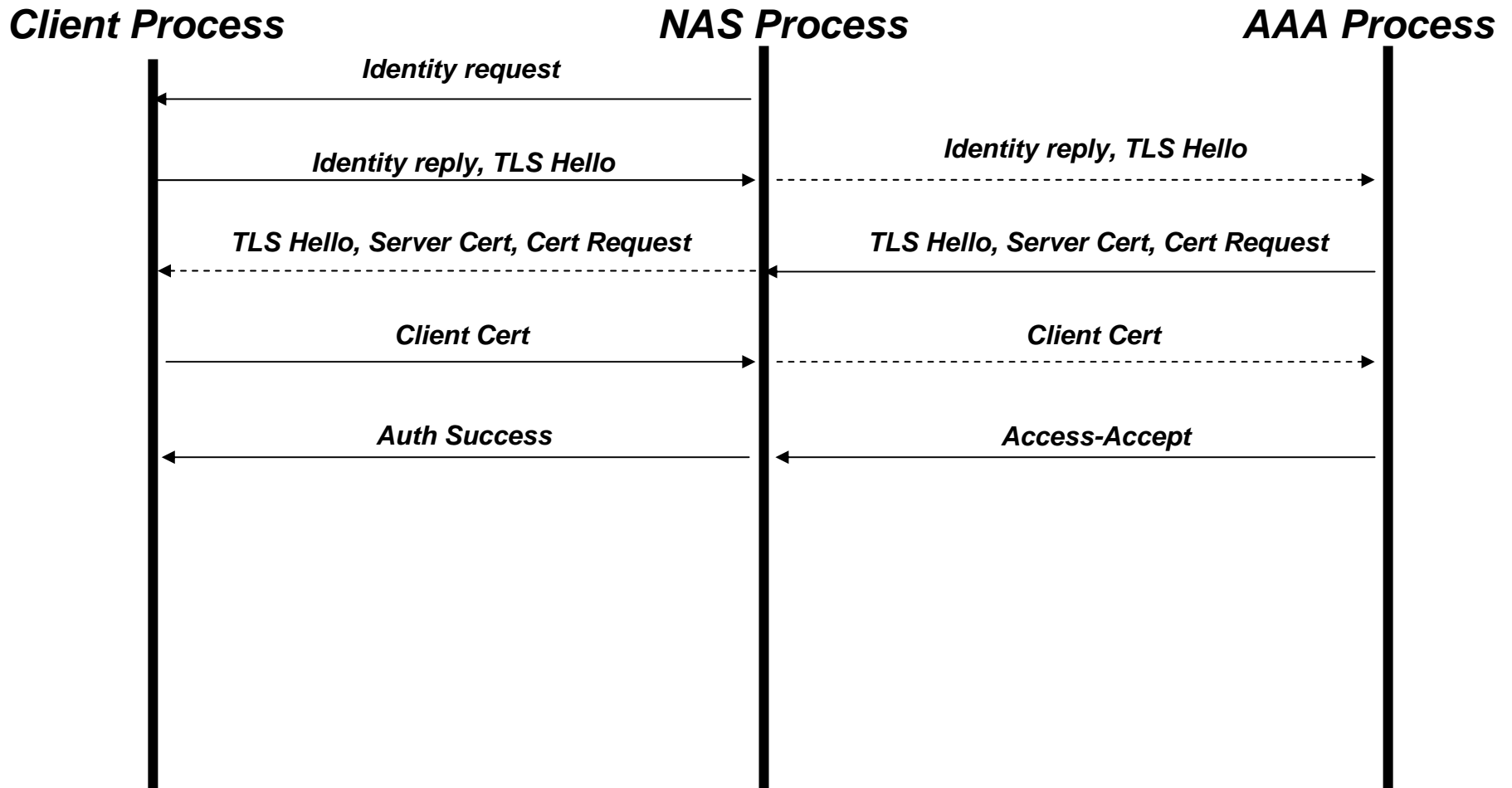
- **Is key distribution needed?**

**No, there is no need for a key distribution scheme. All that is needed is for Fred & 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



# EAP-TLS Pros & 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.

**CISCO SYSTEMS**

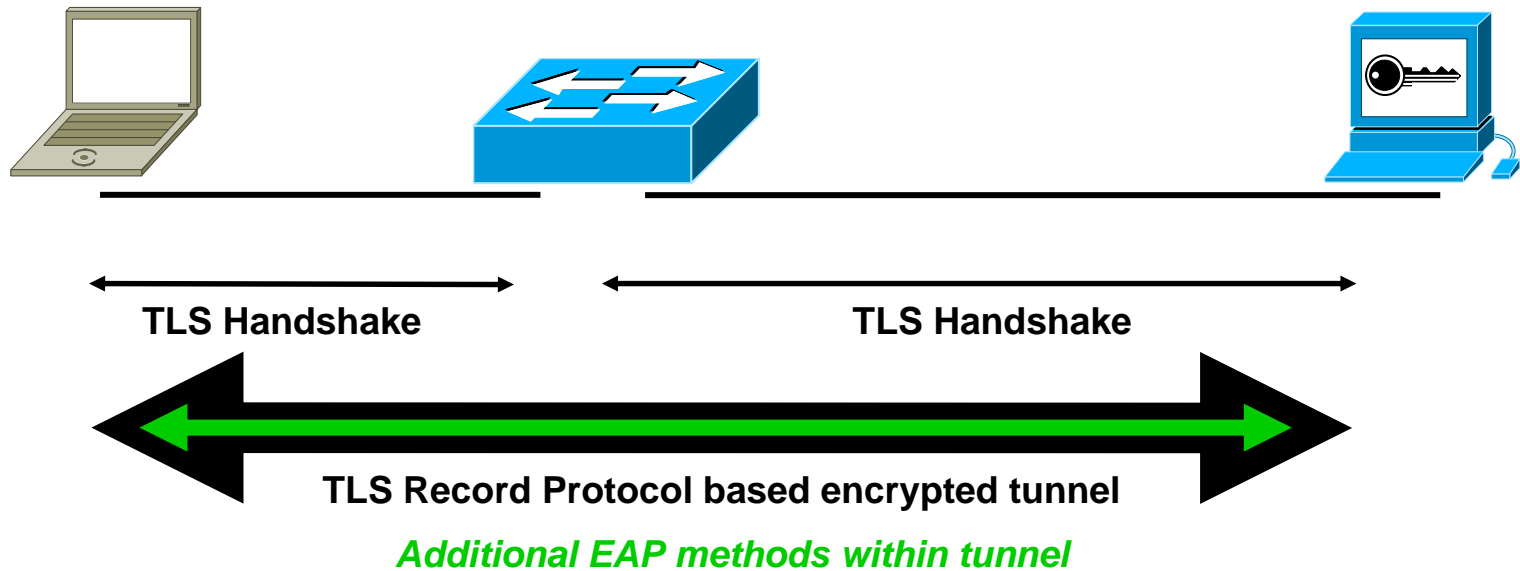


# Understanding PEAP

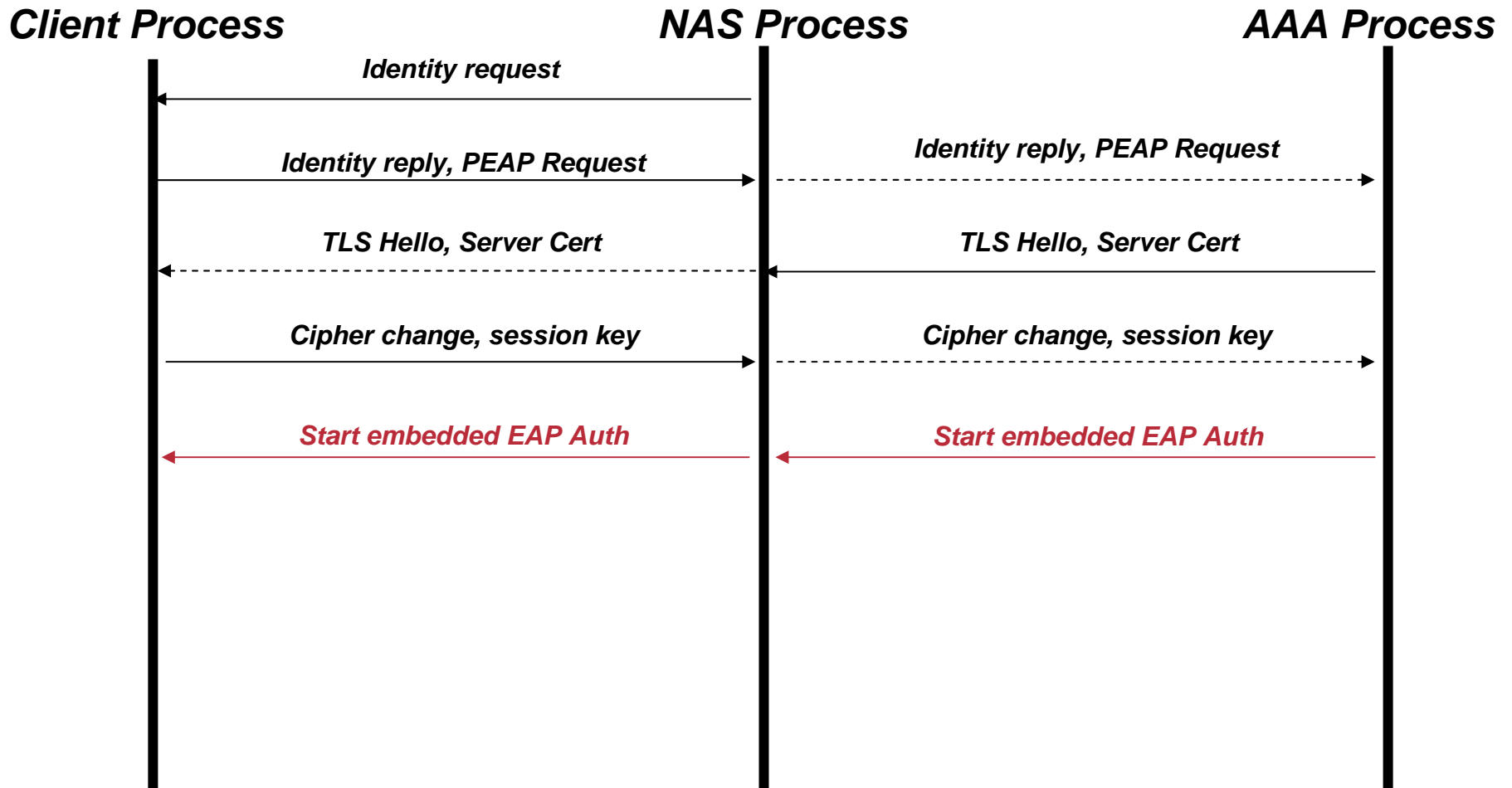
# PEAP Authentication

- **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



# PEAP Setup



# PEAP Pros & Cons

## Pros

- **Highly protected authentication using encrypted tunnel.**
- **Flexible credential options with multiple EAP sub-types.**
- **Doesn't require client certs.**

## Cons

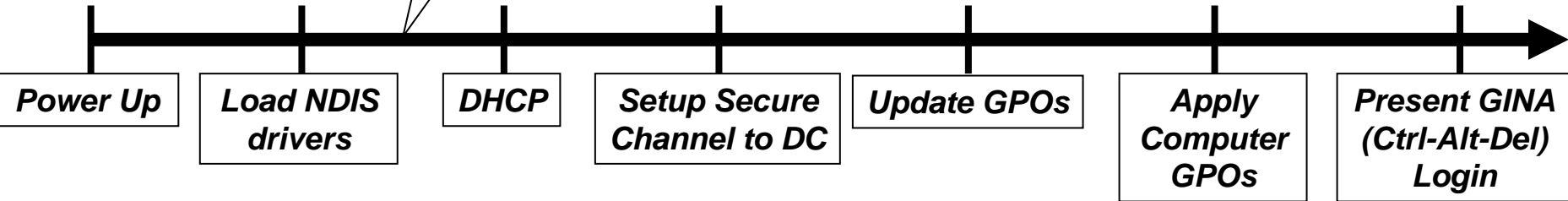
- **Still requires server side certs.**
- **Not as widely supported as other option.**



# Understanding Microsoft Environments

# Windows Boot Cycle Overview

*Inherent assumption of network connectivity.*



# Microsoft & Machine Authentication

- **What is Machine Authentication?**

**The ability of a Windows workstation to authenticate under its own identity, independent of the requirement for an interactive user session.**

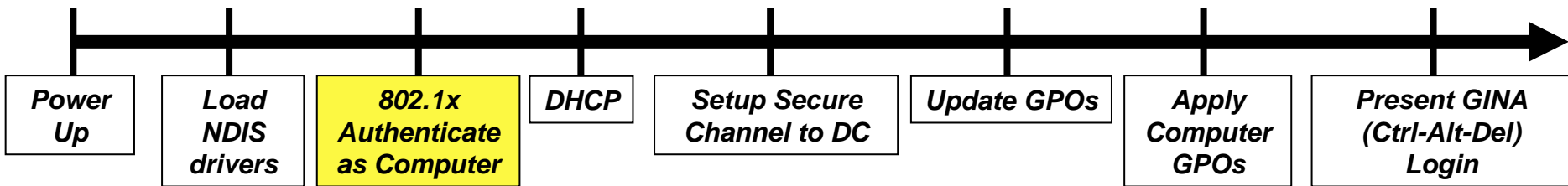
- **What is it used for?**

**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.**

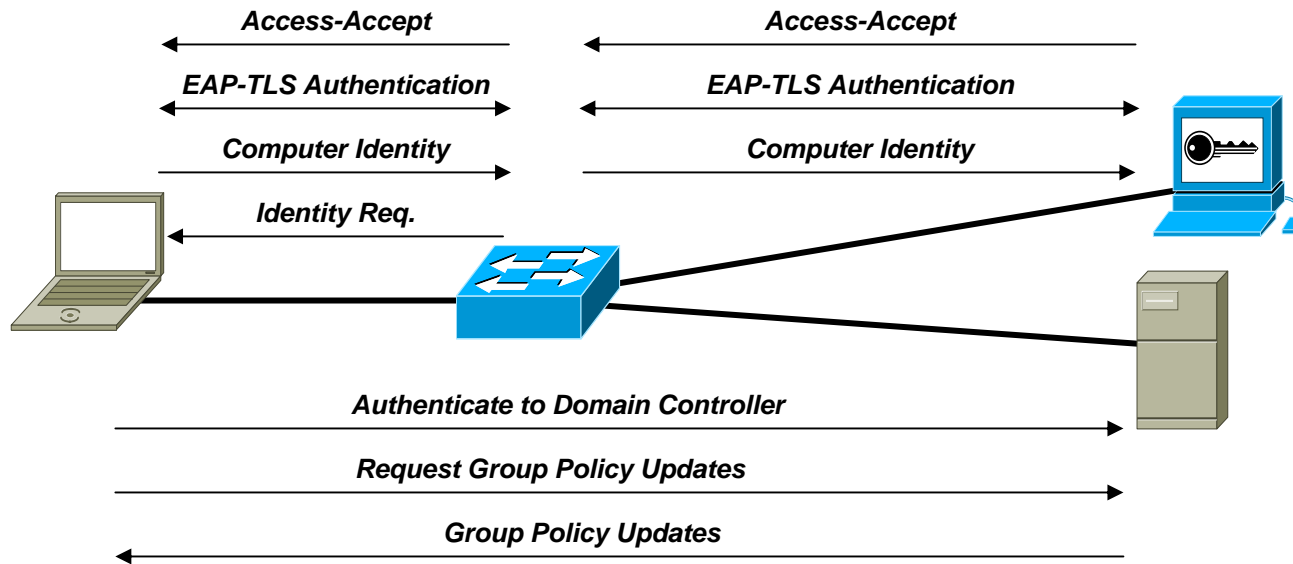
- **Why do we care?**

**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



# Machine Authentication & 802.1x



# Machine Authentication EAP Methods

- **Follows method chosen for user authentication.**
- **For EAP-TLS – will use machine certs.**  
**Computer certs can be enrolled either manually (yeah, right), or automatically via GPOs.**
- **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 & system policies.**
- **Authentication by user and machine.**
  - Uses authentication of both user & machine. Switches contexts when going from one to the other.**
- **See PDF on Registry Settings at <http://identity.cisco.com>**

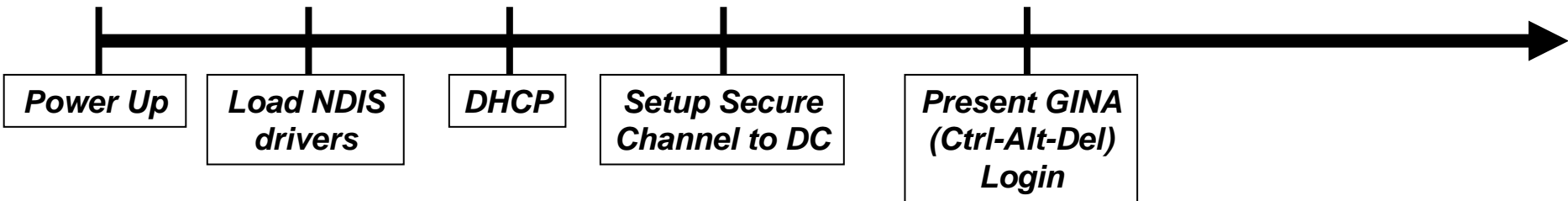
# Microsoft Issues With DHCP

- **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.**



# 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.**

# Microsoft Supplicant News

- **Microsoft has issued Cisco a beta patch due in SP2 to fix the 80.21x/DHCP issue.**
- **Initial testing is looking good.**
- **Issue: Windows did not initiate a proper DHCP renewal after a successful 802.1x authentication – Breaks subnet changes ie. Dynamic VLAN assignment. They were issuing a unicast DHCP request.**
- **Fix: Immediately following an 802.1x authentication DHCP is triggered. The DHCP client pings for the current default gateway (<500ms timeout). If no response is received a broadcast request is made.**
- **Ping shows if you have changed subnets. MSFT does this for WLAN roaming**
- **SP2 due in December but may be pushed back to a later date (Jan/Feb?)**

# More Microsoft Supplicant News

- **802.1x/DHCP fix will also be made for Win2K in SP4 – no confirmed ETA for that yet.**
- **Windows Server 2003 provides a management tool for configuring and pushing out 802.1x supplicant configuration using Domain Group Policies.**
- **Only available in Windows Server 2003**

# How do you enable Machine auth?

- **Make sure the computer is a member of the domain.**
- **If using TLS, make sure the computer gets a cert – either through auto-enrollment or manually.**
- **If using PEAP or TLS make sure that the CA cert is in the local machine store. Typically added if CA is up when machine is added to the domain. If not, you can force via auto-enrollment too.**
- **Click the check box for the “Authenticate as Computer” option.**

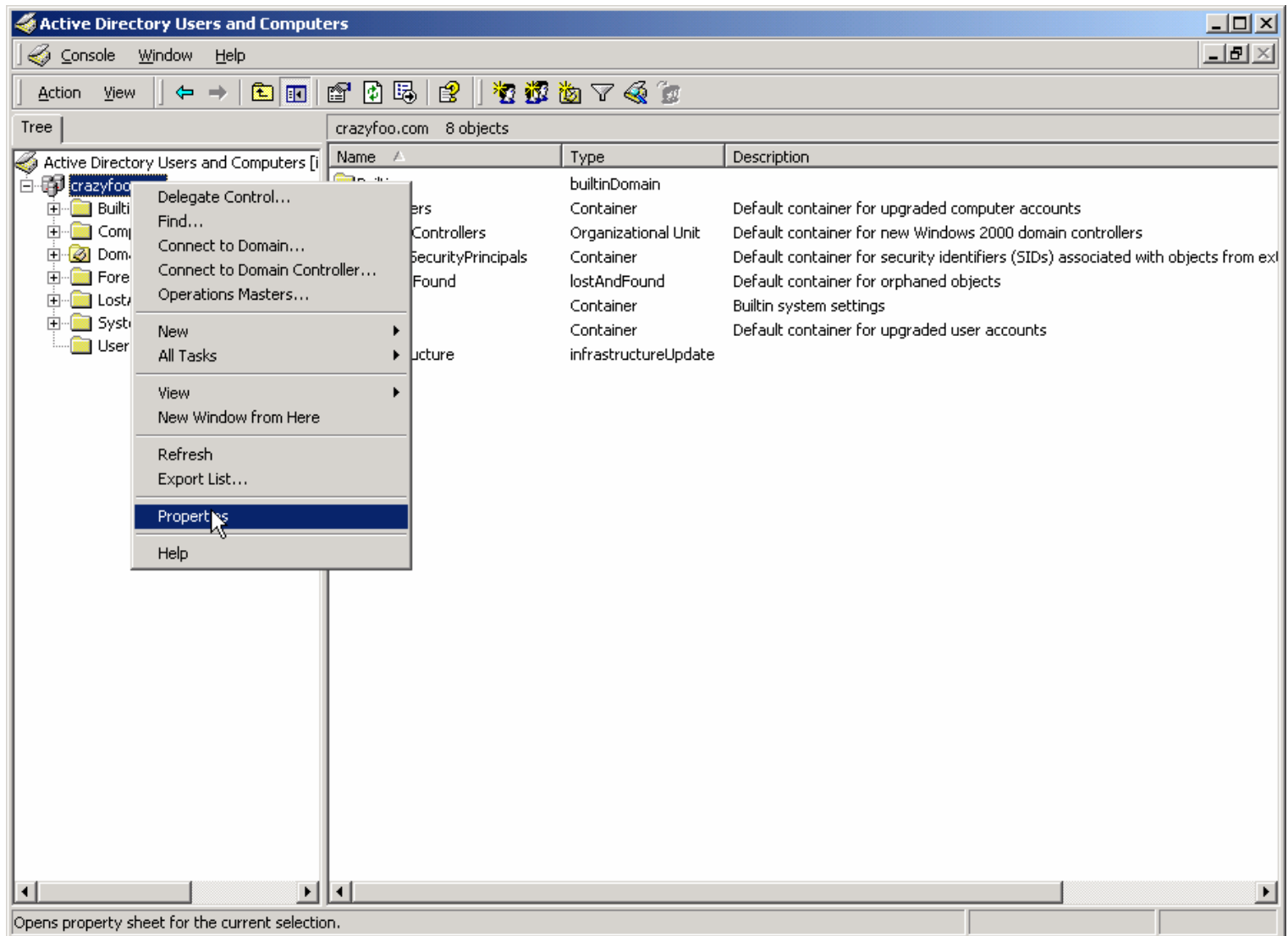
# Machine Auth Using PEAP

- **Uses account information for the computer created at the time the machine is added to the domain.**
- **Computer MUST be a member of the domain.**
- **If doing mutual authentication, the computer MUST trust the signing CA of the RADIUS server's cert.**

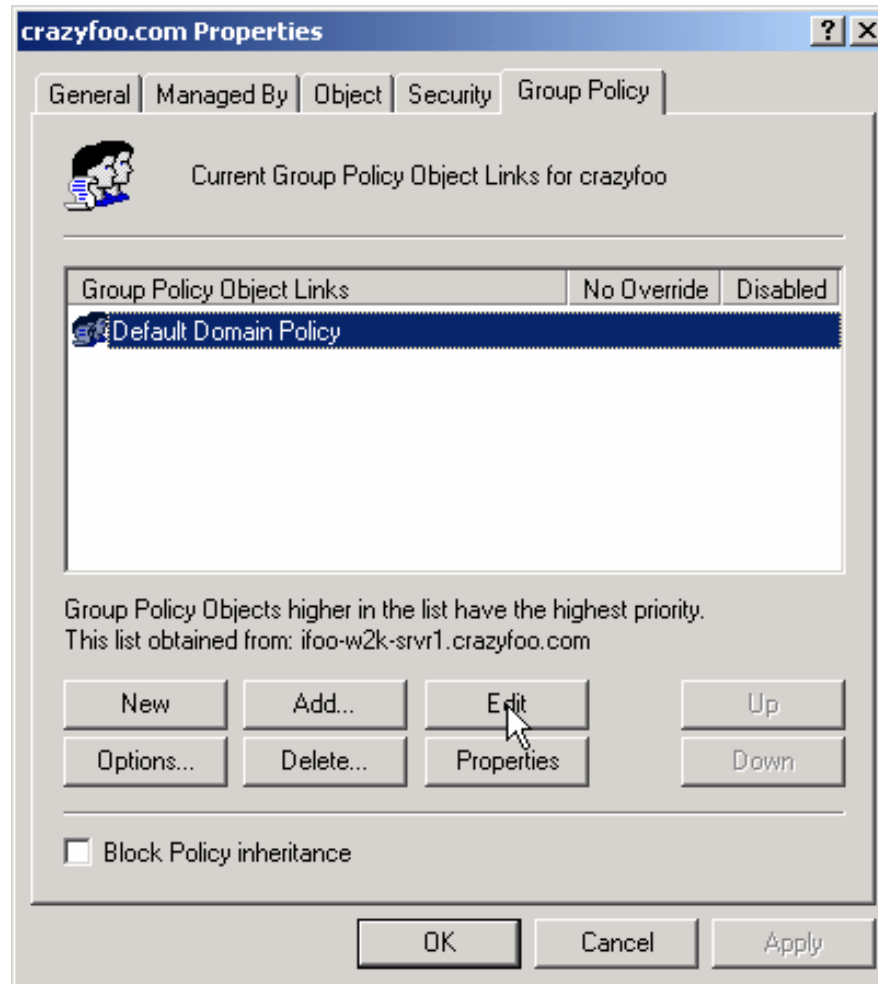
# Machine Auth Using EAP-TLS

- **Authenticates the computer using certs.**
- **The computer MUST have a valid cert.**
- **If doing mutual authentication, the computer MUST trust the signing CA of the RADIUS server's cert.**

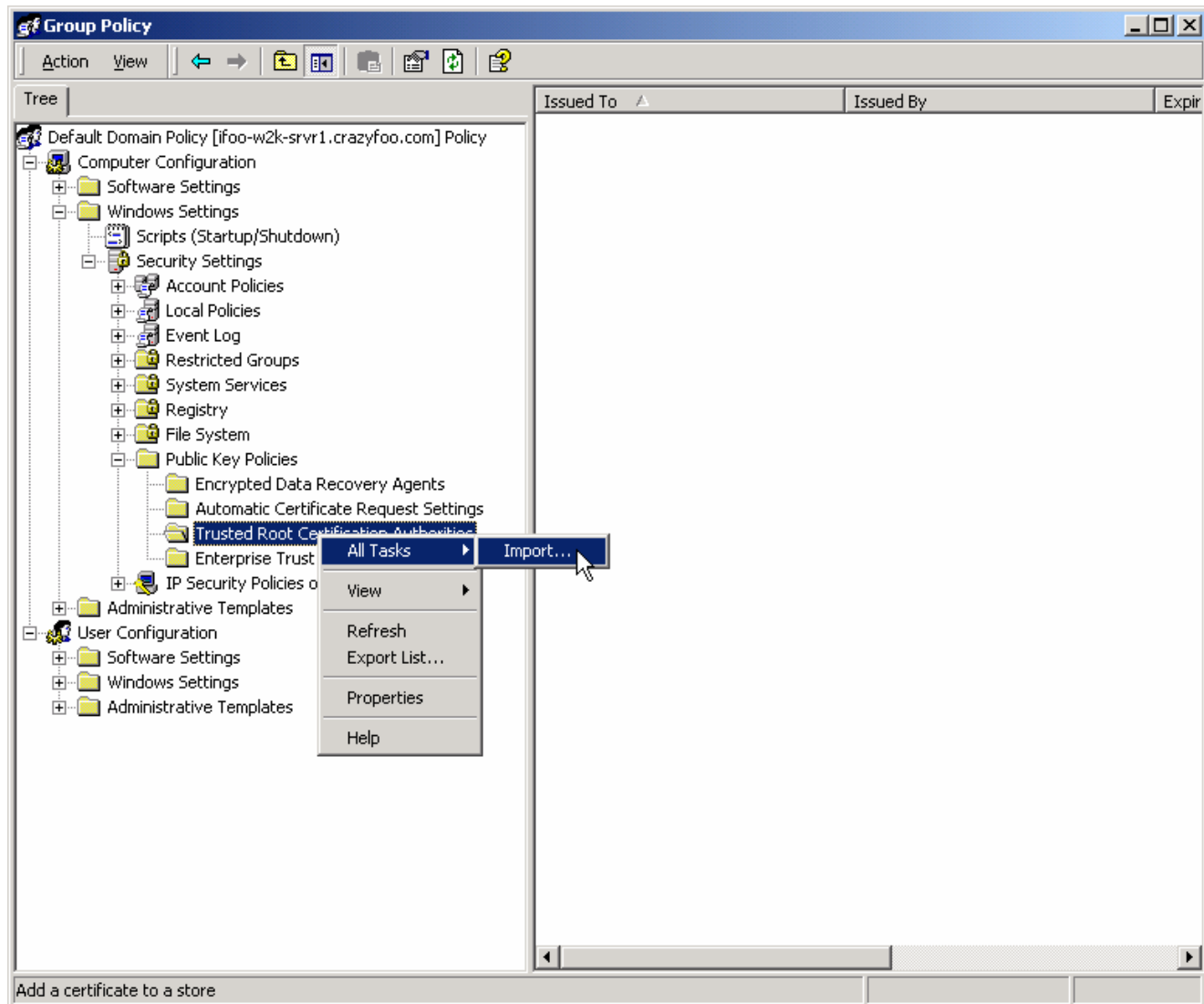
# Using GPOs To Control Computer Certs



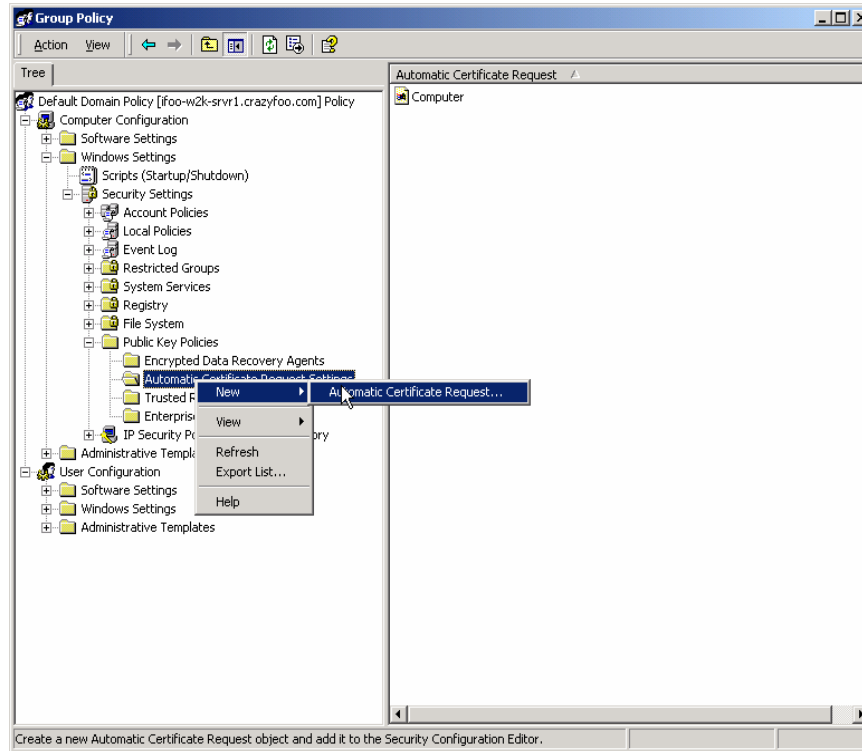
# Using GPOs To Control Computer Certs



# Using GPOs To Control Computer Certs



# Using GPOs To Control Computer Certs



# Machine Auth with “Dial-in Permission” Checking

Cisco.com

- If using the “Check Dial-In permissions” option in ACS you may run into a problem with machine auth.
- There is no “Dial-In permission” tab for a computer by default in Win2K.
- You need to add it.
- Requires SP3.
- Type the command:  

```
Idifde -i -f %systemRoot%\system32\mac8021x.Idf -c DC=DN DC=domain,DC=com
```
- See **Microsoft KnowledgeBase Article #306260** for more details.



# Identity Based Policy Enforcement

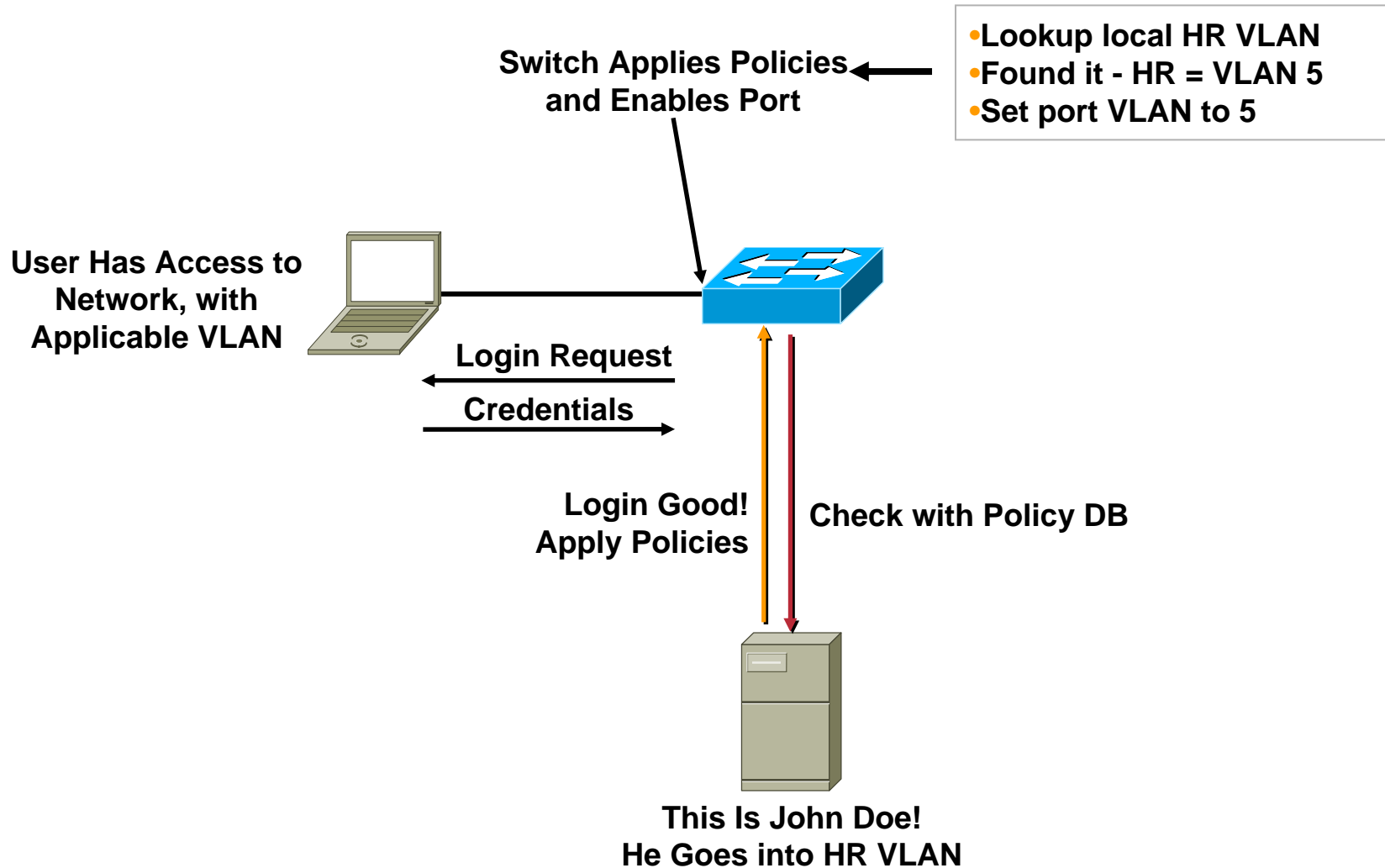
# Authorization

- **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 (ie. VLAN QoS, VLAN ACLs, etc.)**

# Example Solution “A”—Access Control and User Policy Enforcement



# Dynamic VLAN Mechanism

- **RADIUS AV-Pairs used to send back VLAN configuration information to authenticator.**
- **AV-Pair usage for VLANs is IEEE specified in the 802.1x standard.**
- **AV-Pairs used – all are IETF standard:**
  - [64] Tunnel-Type – “VLAN” (13)**
  - [65] Tunnel-Medium-Type – “802” (6)**
  - [81] Tunnel-Private-Group-ID - <VLAN name>**

# ACS Configuration

## Group Policy Configuration – VLAN Assignment

**CiscoSecure ACS - Microsoft Internet Explorer**  
Address: http://127.0.0.1:2253/

### Group Setup

Jump To: Access Restrictions

- [053] Proxy-State
- [034] Login-LAT-Service
- [035] Login-LAT-Node
- [036] Login-LAT-Group
- [037] Framed-AppleTalk-Link (0..65535) Value: 0
- [038] Framed-AppleTalk-Network (0..65535) Value: 0
- [039] Framed-AppleTalk-Zone
- [062] Port-Limit Value: 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

Buttons: Submit, Submit + Restart, Cancel

#### 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 protocol in the Interface Configuration section.
- A Token Card Server has been configured in the External User Databases section.

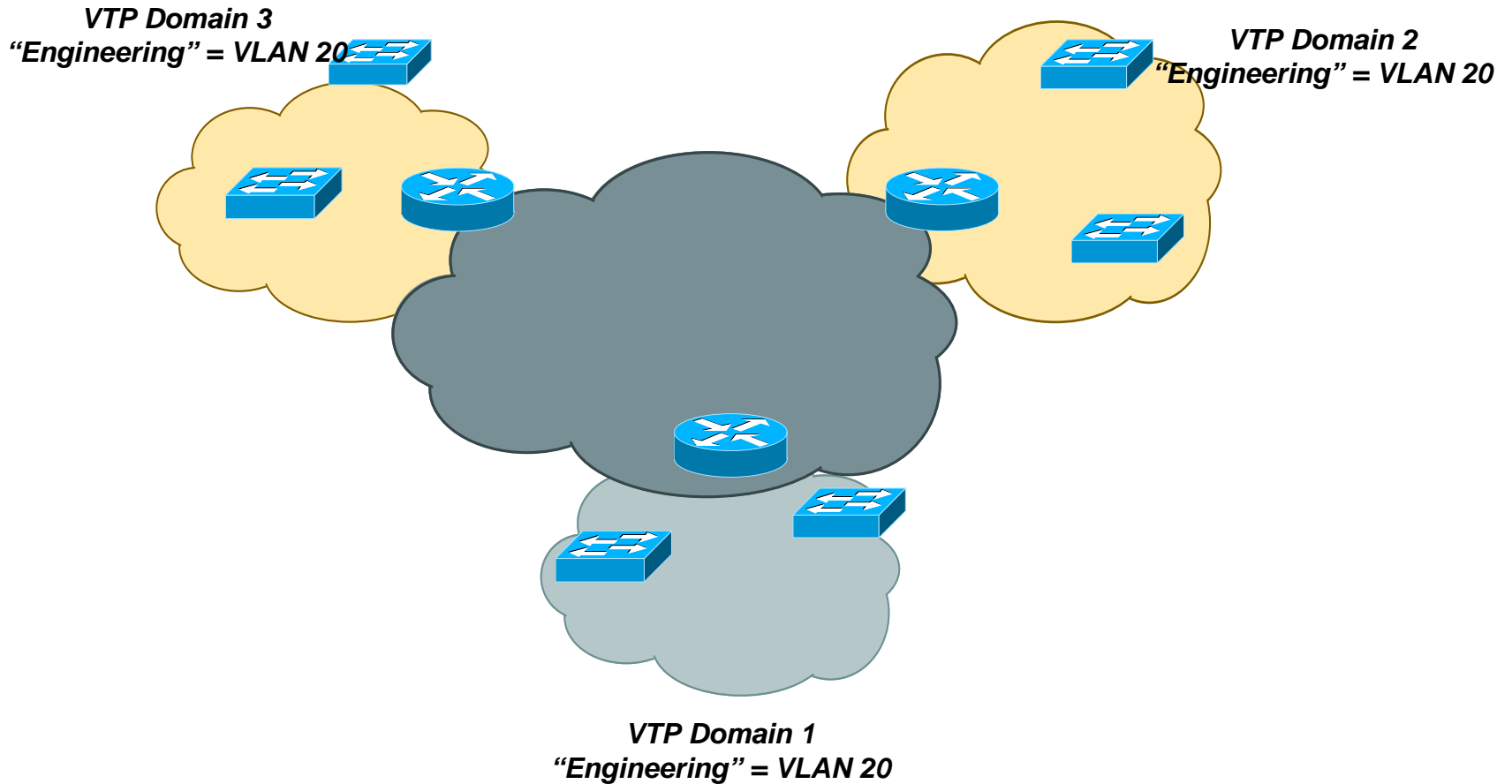
Group Setup is used to enable and configure the particular authorizations assigned to an entire group of users. The group a user is assigned to is configured in the User Setup section. User Setup overrides Group Setup.

[\[Back to Top\]](#)

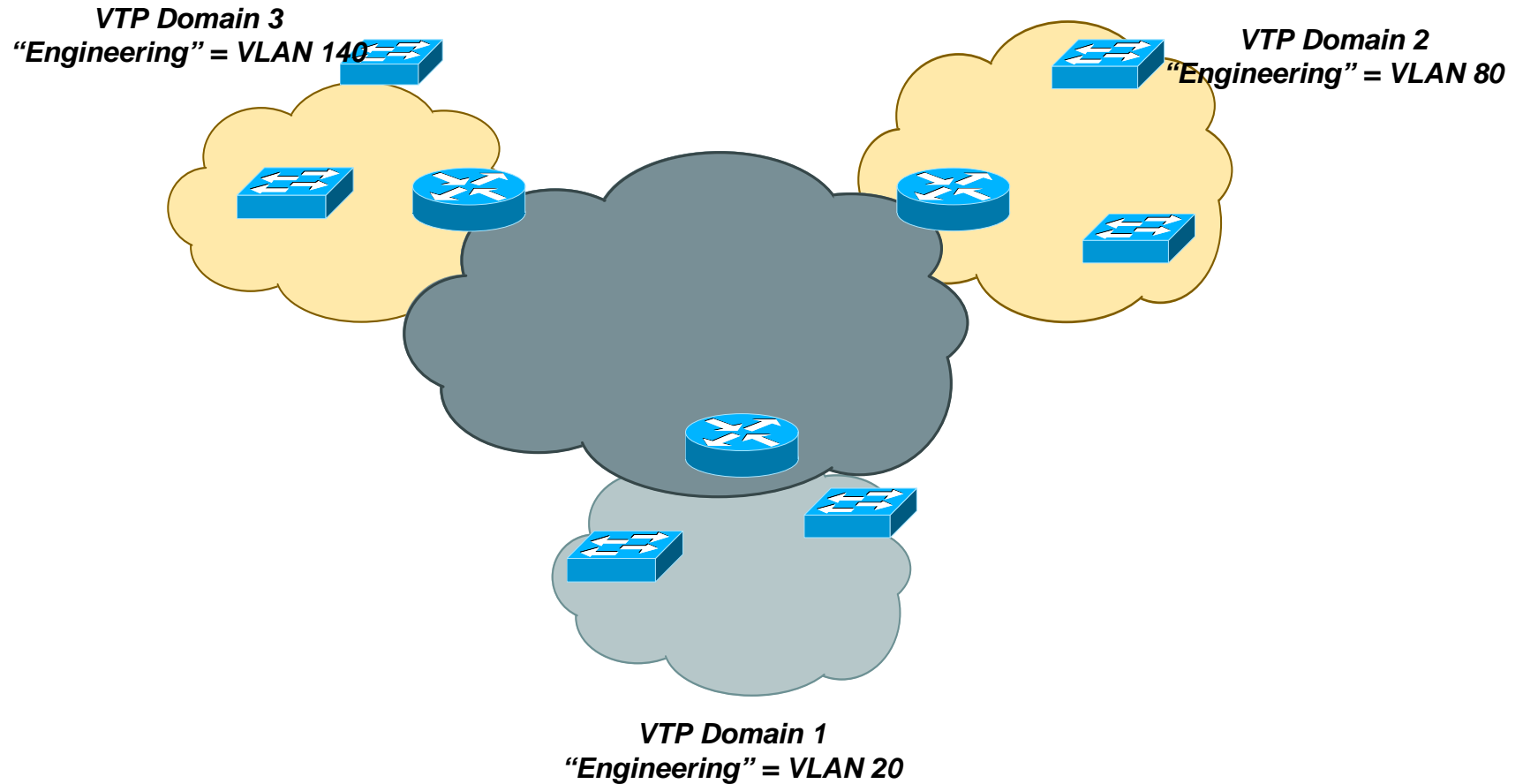
# Dynamic VLAN Deployment Recommendations

- **Use VLAN names to assign VLANs. This allows independence between separate L2 or VTP domains.**

# Dynamic VLANs – VLAN ID Re-Use



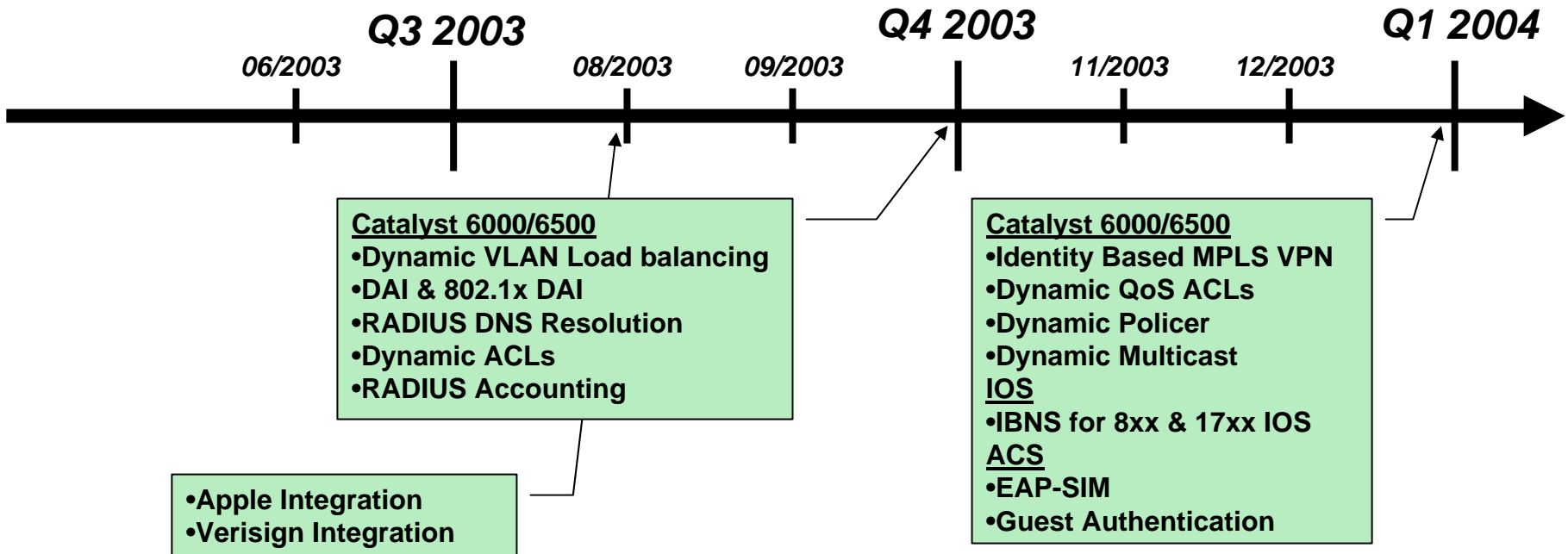
# Dynamic VLAN – Unique VLAN IDs



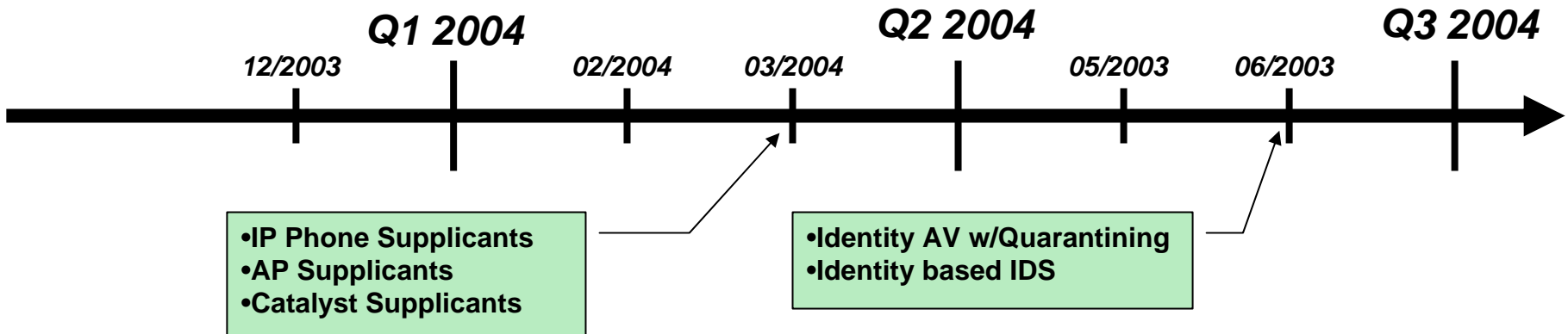
# Future Policies via RADIUS

- **QoS**
- **Port Description**
- **Per-port ACLs**
- **Multicast Join/Block**

# IBNS Roadmap – 6 month window



# IBNS Roadmap – 12 month window

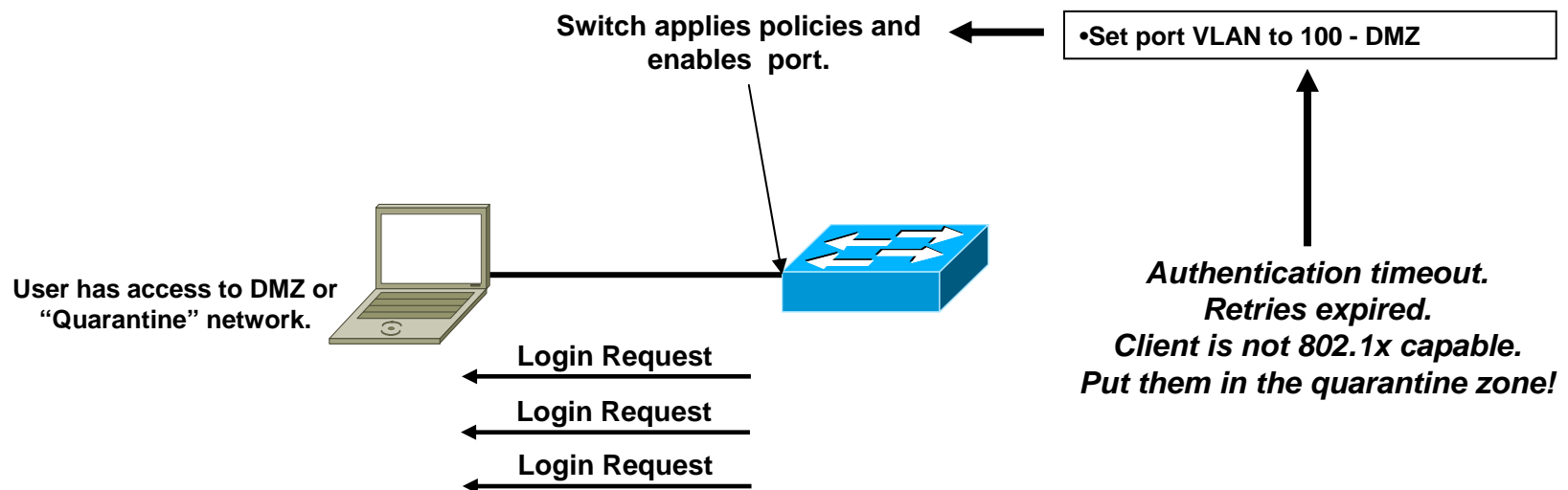




# Providing Guest Access

# Guest Access Scenario 1

- Guest clients do NOT have an 802.1x supplicant.
- This type of guest access is provided by the switch.
- If client does not respond to 802.1x auth requests before timeout, guest access will be applied.
- Default timeout is 30 seconds with 3 retries. Total timeout period is 90 secs by default.



# Current Guest VLAN Issue

- There is a window in which the client authenticating is active on the guest VLAN until they are authenticated.
- Microsoft clients run DHCP independently of 802.1x
- The client gets an address out of the guest VLAN and does not get a new address after auth.

	Does Guest VLAN Work ?	Expected FIX or work-around ?
XP	X	
W2K	X	
Linux	?	

# Guest Access Scenario 2

- **Guest client PC uses 802.1x but does not have a valid account in the current domain.**

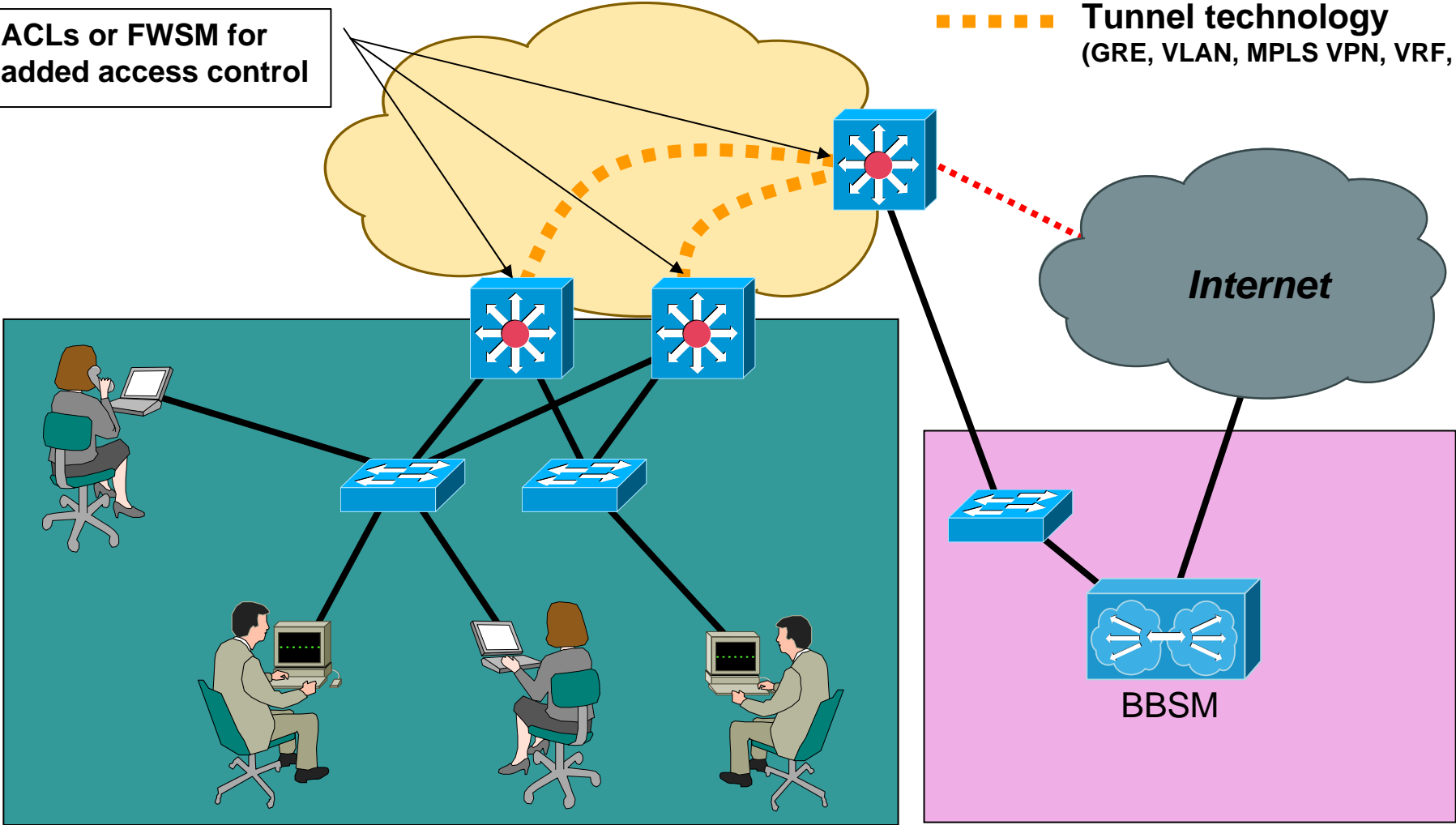
**Client responds to authentication request, but fails authentication.**

- **This is not a currently supported scenario. Targeted for support in ACS 3.3.**

# Example Guest Access Architecture

ACLs or FWSM for added access control

Tunnel technology (GRE, VLAN, MPLS VPN, VRF, etc.)



Diverse Guest User Access

Guest Access Control Point

**CISCO SYSTEMS**



# Migrating to 802.1x

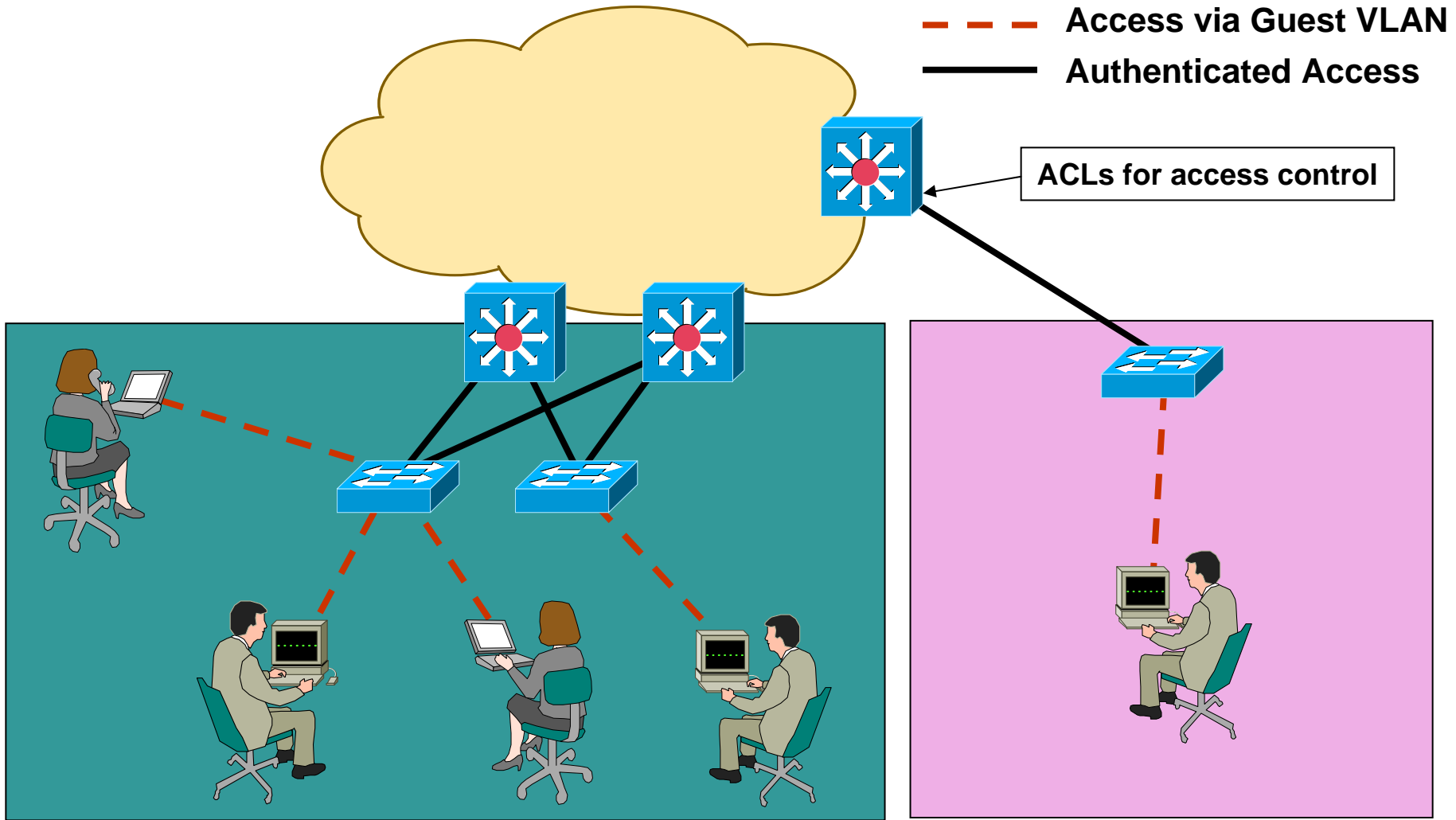
# Migration Strategies – 1<sup>st</sup> Method

- **Requirements: All clients are 802.1x capable.**
  - 1. Fully patch & migrate clients first.**
  - 2. If supporting Dynamic VLANs, build out VLAN support structure.**
  - 3. Enable authentication in sections of the network in modular windows.**

# Migration Strategies – 2<sup>nd</sup> Method

- **Challenge: Not all clients are 802.1x capable.**
- 1. Enable guest vlan access to support non-compliant clients.**
- 2. If supporting Dynamic VLANs, build out VLAN support structure.**
- 3. Fully patch & migrate 802.1x capable clients.**
- 4. Enable authentication in sections of the network in modular windows.**
- 5. Migrate non-compliant clients to compliant OSes.**
- 6. Disable guest access in restricted areas.**

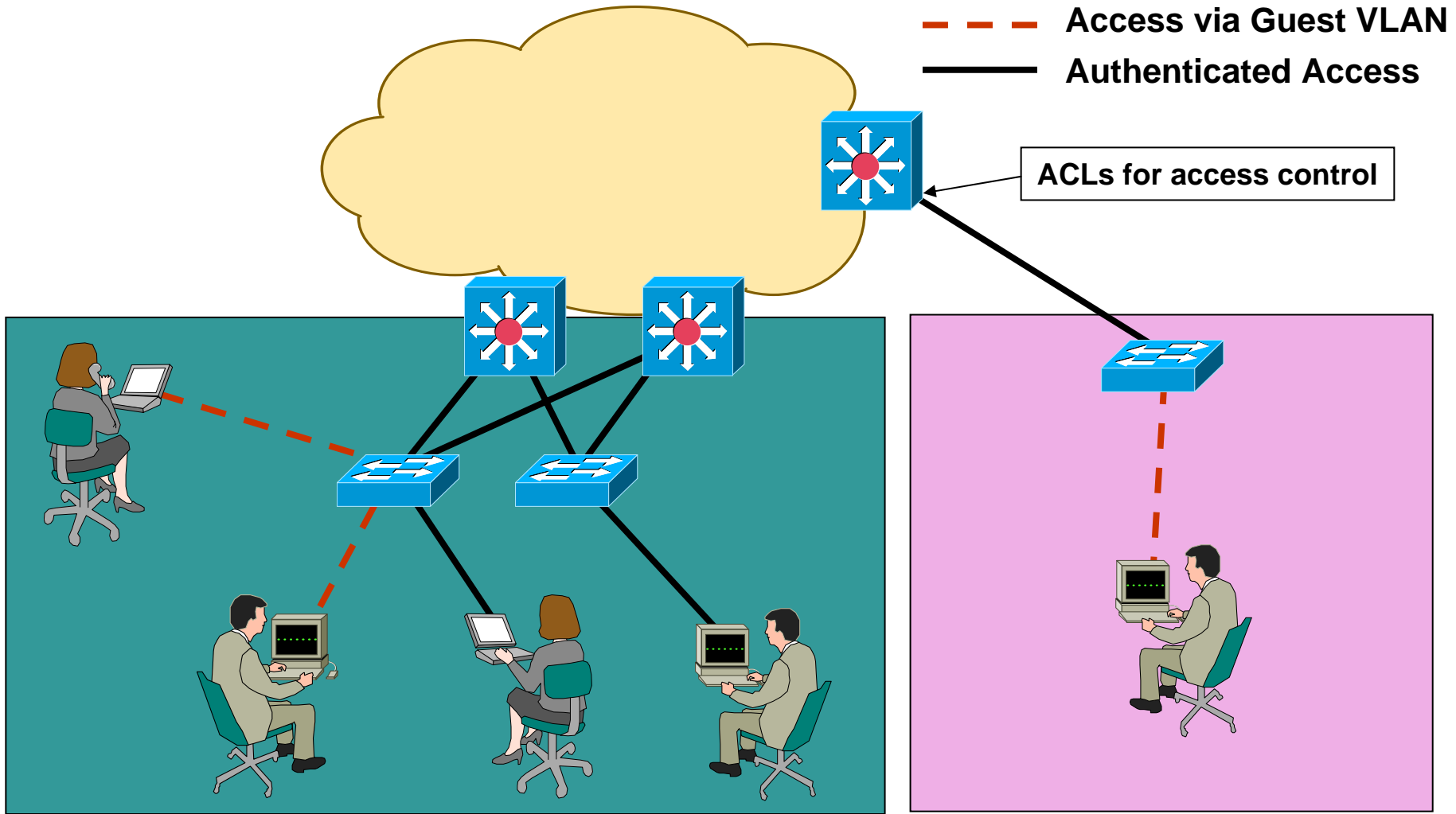
# Initial Client Migration Stage – Majority Guest Access



Controlled Access Areas

Public Access Areas

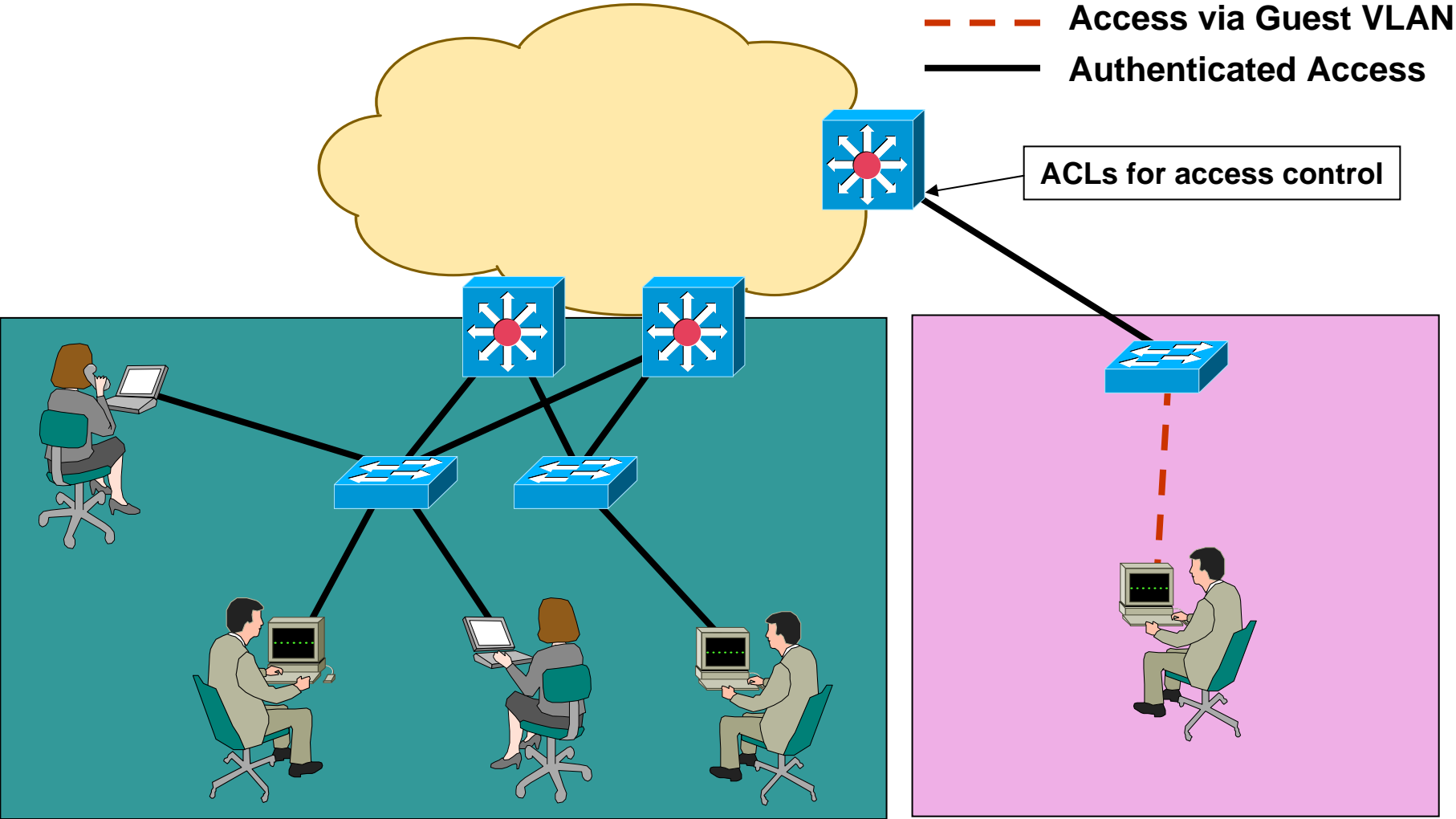
# Transient Client Migration Stage – Mixed Access



Controlled Access Areas

Public Access Areas

# Completed Migration – Fully Authenticated Access



Controlled Access Areas

Public Access Areas



# Commonly Asked Questions

# Most Commonly Asked Questions

- **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.**

- **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

- **Two phases of VoIP and 802.1x support.**

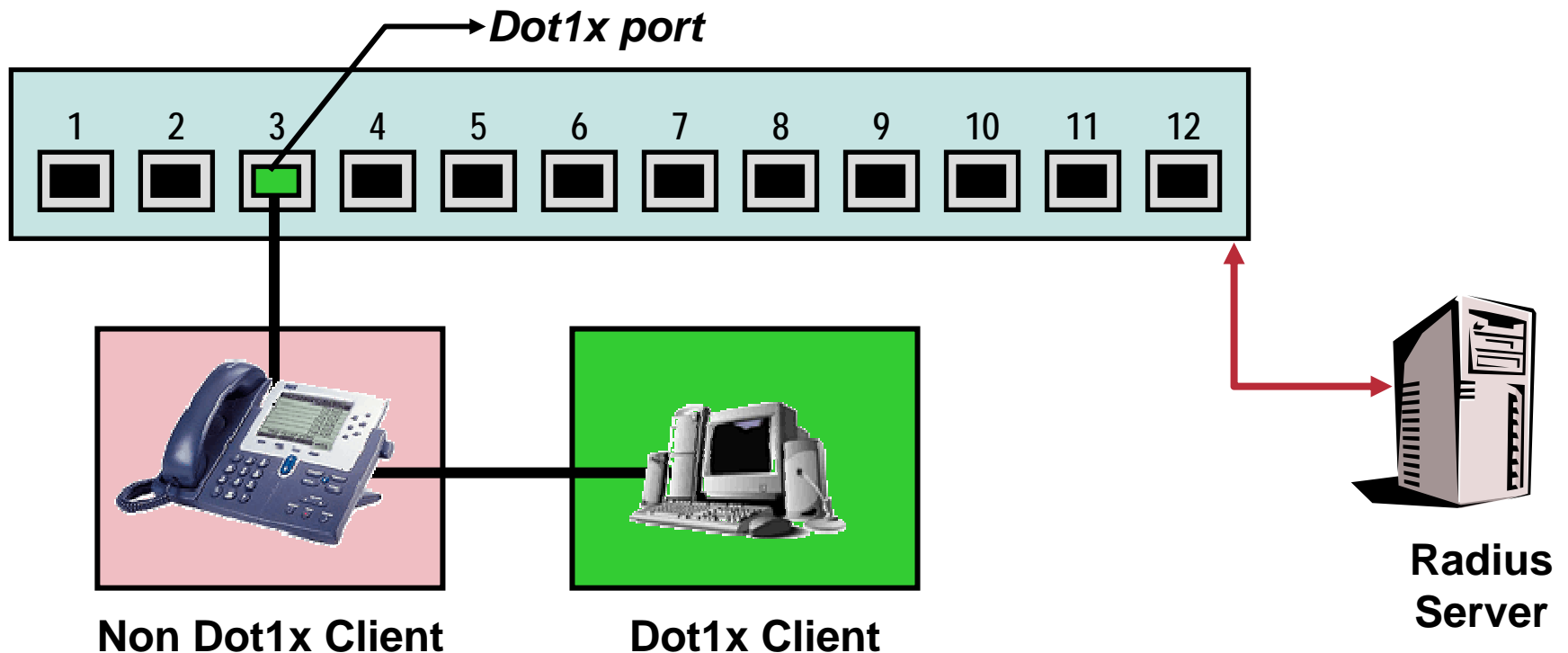
**802.1x with VVID – Unauthenticated Voice VLAN (VVID) access, Authenticated Data VLAN (PVID) access. This leaves voice no better than it is today, but allows 802.1x and VoIP to co-exist at the same time.**

**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.**

# IEEE 802.1x with Voice VLAN

**Problem – How to connect a PC (dot1x client) through an IP Phone (non-dot1x client) to a dot1x enabled switch port?**

**Answer – Switch identifies IP Phone (as a Cisco phone) and bypasses dot1x authentication – BUT – still forces authentication for downstream device**



# IP Phone Supplicants

*The CA issues and signs a cert for the IP phone.*



*The CA issues and signs a cert for the AAA server.*

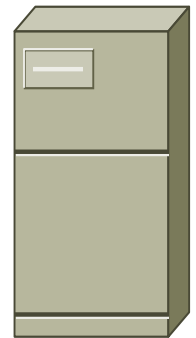
*Hello*

*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?

- **Windows XP – Now, Ships with support (requires SP 1a for PEAP)**
- **Windows 2000 - Currently available with SP3 + Hotfix from KB Article 313664**
- **Windows NT/98/Me - Limited Availability or 3<sup>rd</sup> Party (MeetingHouse)**
- **Linux - Open Source or 3<sup>rd</sup> Party (MeetingHouse)**  
<http://www.open1x.org>
- **Solaris – Open Source or 3<sup>rd</sup> Party via MeetingHouse Communications <http://www.mtghouse.com>**

# Apple Supplicant News

- **Apple has an integrated working 802.1x supplicant in Jaguar (OS X 1.3) – no current ETA on FCS (possibly late Q4CY2003).**
- **ESE is currently testing and troubleshooting for Apple. (Yes, we have Macs 😊)**
- **Currently supported EAP methods are pretty much everything!**

**EAP-TLS**

**LEAP**

**EAP-TTLS**

**PEAP with any sub-type**

**EAP-GTC**

**MS-CHAPv2**

# MeetingHouse Supplicant News

- **MeetingHouse supplicant has been extensively tested with IBNS – a few minor bugs being addressed.**
- **Current focus is to develop a “machine authentication” capability.**
- **Generally a good supplicant supporting:**
  - LEAP**
  - EAP-TLS**
  - EAP-TTLS**
  - PEAP/MS-CHAPv2**
- **Cisco maintains a strong relationship with MeetingHouse.**

Vendor	OSes Supported	EAP-TLS	EAP-TTLS	EAP-MD5	EAP-MSCHAPv2
Cisco	Windows (all) Apple OS 9 Apple OS X Linux	✗	✗	✗	✗
Microsoft	Windows XP Windows 2000	✓ (SSO)	✗	✓	✓
Apple	OS X	✓ (SSO)	✓ (SSO)	✓	✓
MeetingHouse	Windows (all) Apple OS X Linux Sun Solaris	✓	✓	✓	✓
Funk	Windows (all) Linux Sun Solaris	✓	✓	✓	✓

Vendor	OSes Supported	LEAP	EAP-GTC	PEAP (Cisco)	PEAP (MSFT)
Cisco	Windows (all) Apple OS 9 Apple OS X Linux	✓ (SSO)	✓ (SSO)	✓ (SSO)	✗
Microsoft	Windows XP Windows 2000	✗	✗	✗	✓ (SSO)
Apple	OS X	✓ (SSO)	✓ (SSO)	✓ (SSO)	✓
MeetingHouse	Windows (all) Apple OS X Linux Sun Solaris	✓	✓	✓	✓
Funk	Windows (all) Linux Sun Solaris	✓	✓	✓	✓



# IBNS Product Support

# Which Cisco Platforms Support IBNS?

- **Catalyst 5500 – Basic 802.1x only**
- **Catalyst 6000/4000 - IBNS**
- **Catalyst 2950/3550 – IBNS**
- **Aironet WLAN APs – Some IBNS**
- **Cisco 800 series – IBNS Subset**

**Features will be limited by platform capabilities.**

# IBNS Features

- **Centralized Management with AAA server**
- **Wireless Mobility with 802.1X and EAP Authentication Types**
- **Catalyst Switch Portfolio**
  - **Basic 802.1X Support**
  - **802.1X with VLANs**
  - **802.1X with Port Security**
  - **802.1X with VVID**
  - **802.1X Guest VLANs**
  - **802.1X with ACLs**
- **Enhanced Port Based Access Control**
- **Greater flexibility and mobility for a stratified user community**
- **Enhanced User Productivity**
- **Added support for converged VoIP networks**

# Identity Based Networking Services

## Component Availability

Cisco.com

Catalyst 6500



Catalyst 4000/4500



Catalyst 3550/2950/3750



Cisco ACS Server



Cisco Aironet



	CAT6500/ CatOS	CAT6500/ IOS	CAT4k/4500/ CatOS	CAT4k/4500/ IOS	CAT2950/ 2955	CAT3550	CAT3750
802.1x w/ VLAN Assignment	7.5.1	12.1(13)E	7.5.1	12.1(19)EW	12.1(12c)ea1	12.1(12c)ea1	Aug03
802.1x w/ VVID	7.5.1	1HCY04	8.1 Q4CY03	roadmapped	12.1(12c)ea1	12.1(12c)ea1	Aug03
802.1x w/ Guest VLAN	7.5.1	1HCY04	8.1 Q4CY03	12.1(19)EW	12.1(14 )ea1	12.1(14 )ea1	Aug03
802.1x w/ Port Security	7.5.1	1HCY04	8.1 Q4CY03	roadmapped	12.1(12c)ea1	12.1(12c)ea1	na
802.1x w/ DHCP	7.6.1	na	na	na	na	na	Aug03
802.1x w/ Guest VLAN/Port	7.7.1 (Target)	na	na	na	na	na	na
802.1x w/ ACL/QoS	7.8/8.1 (Target)	1HCY04	na	roadmapped	na	na	Aug03
Accounting	na	na	na	roadmapped	na	na	na

# Identity Based Networking Service

Cisco.com

Catalyst 6500



Catalyst 4000/4500



Catalyst 3550/2950/3750



Cisco ACS Server



Cisco Aironet



- **CatOS**

7.5.1

802.1x w/ VLAN Assignment

802.1x w/ VVID

802.1x w/ Guest VLAN

802.1x w/ Port Security

7.6.1

802.1x w/ DHCP

7.7.1 (Target)

802.1x w/ Guest VLAN/port

7.8/8.1 (Target) – Q4CY03

802.1x with ACL/QoS

- **IOS**

12.1(13)E

802.1x w/ VLAN Assignment

1HCY04:

802.1x w/VVID

802.1x Guest VLAN

802.1x w/Port Security

802.1x with ACL/QoS

**Identity Based Network Services (IBNS)  
End-to-End Architecture**

# Identity Based Networking Service

Cisco.com

Catalyst 6500



Catalyst 4000/4500



Catalyst 3550/2950/3750



Cisco ACS Server



Cisco Aironet



- **CatOS**

7.5.1

802.1x w/ VLAN Assignment

8.1 – Q4CY03

802.1x w/ VVID

802.1x w/ Guest VLAN

802.1x w/ Port Security

- **IOS**

12.1(19)EW – June '03

802.1x w/ VLAN Assignment

802.1x Guest VLAN

Roadmapped

802.1x w/VVID

802.1x w/Port Security

802.1x with ACL/QoS

802.1x Accounting

**Identity Based Network Services (IBNS)  
End-to-End Architecture**

# Identity Based Networking Service

Cisco.com

Catalyst 6500



Catalyst 4000/4500



Catalyst 3550/2950/3750



Cisco ACS Server



Cisco Aironet



- **2950/2955**
  - 12.1(12c)EA1
  - 802.1x w/ VLAN Assignment
  - 802.1x w/VVID
  - 802.1x w/ Port Sec
- 12.1(14)EA1
  - 802.1x Guest VLAN

- **3550 (EMI/SMI)**
  - 12.1(12c)EA1
    - 802.1x w/ VLAN Assignment
    - 802.1x w/VVID
    - 802.1x w/ Port Sec
  - 12.1(14)EA1
    - 802.1x Guest VLAN

- **3750 – Aug '03**
  - 802.1x w/ VLAN Assignment
  - 802.1x w/VVID
  - 802.1x Guest VLAN
  - 802.1x w/ DHCP
  - 802.1x w/ ACL/QoS

**Identity Based Network Services (IBNS)  
End-to-End Architecture**

# Identity Based Networking Service

Cisco.com

Catalyst 6500



Catalyst 4000/4500



Catalyst 3550/2950/3750



Cisco ACS Server



Cisco Aironet



- Commercial RADIUS & TACACS+
- Scalable to 100K users/8K devices)

- 3.2 Avail Now  
Appliance  
Microsoft Peap  
PEAP Proxy  
Machine Auth  
EAP Type Negotiation  
LDAP Multithreading  
EAP Performance  
Windows password

- 3.3 Avail Q2 '04  
802.1X/IBNS complementary features with Catalyst/Wireless  
802.1X Catalyst /IBNS enhancements (guest VLAN, accounting, CRL)  
EAP enhancements (LEAP, PEAP v2)  
User Quarantine

**Identity Based Network Services (IBNS)  
End-to-End Architecture**

# Identity Based Networking Service

Cisco.com

Catalyst 6500



Catalyst 4000/4500



Catalyst 3550/2950/3750



Cisco ACS Server



Cisco Aironet



- AP 350

802.1x for AP LAN Access Not Committed

- AP 1100

802.1x for AP LAN Access Q1CY04

- AP 1200

802.1x for AP LAN Access Q1CY04

- **For Wireless Clients Across These Products:**
- Multiple VLANs for employees, guests and application specific devices
- Expanded 802.1X Authentication Support for: Cisco LEAP, EAP-TLS, EAP-TTLS, PEAP, EAP-SIM
- Expanded Encryption Support for 802.11i TKIP

**Identity Based Network Services (IBNS)  
End-to-End Architecture**

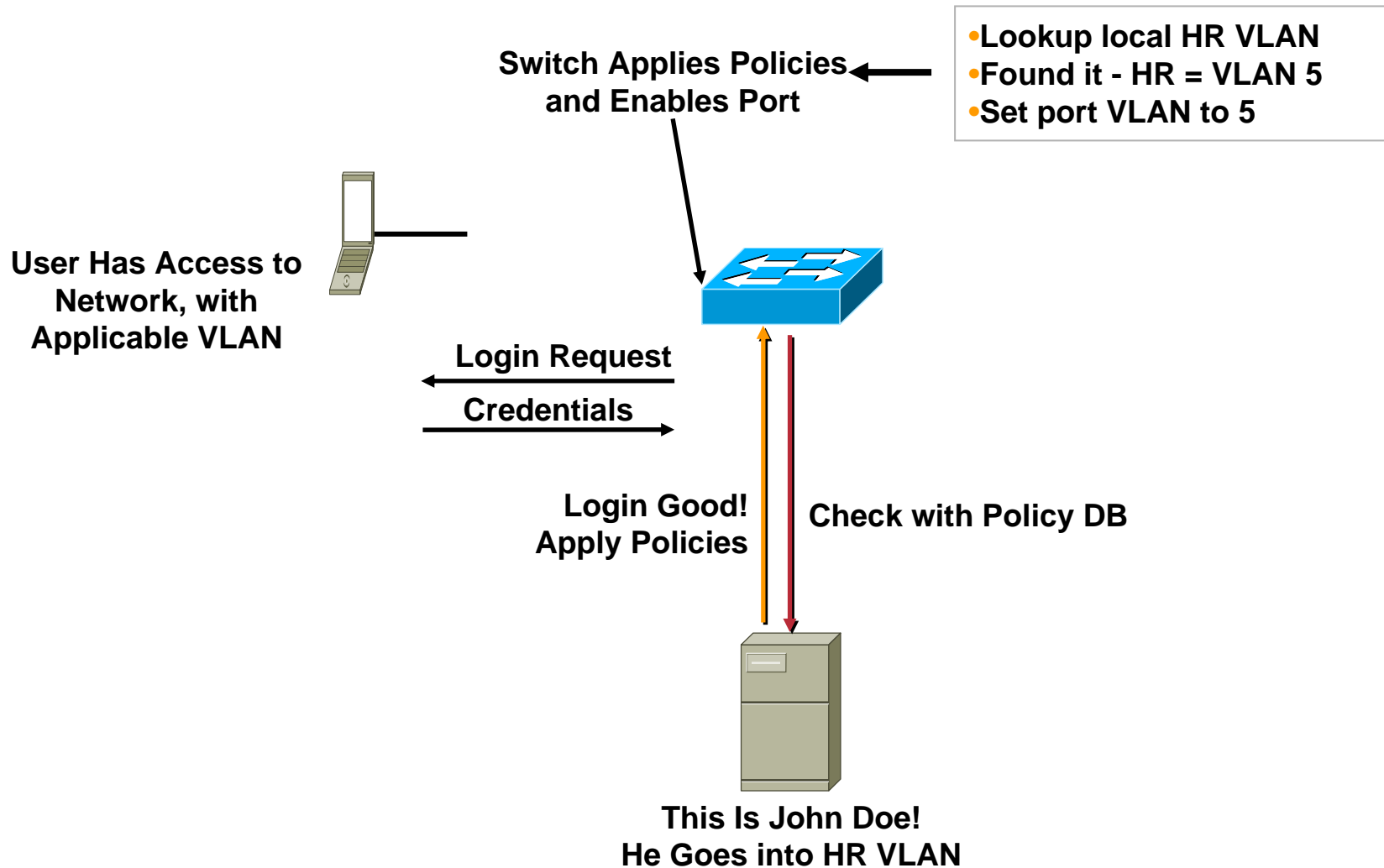
Products	Basic 802.1x	VVID Support	Dynamic VLAN Assignment	Guest VLAN and/or DHCP Assignment	Per-User QoS/Security Policies
<b>2950</b>	IOS 12.1(6)EA2	VeCal5a Release (Nov '02)	Dynamic VLAN via 802.1x: VeCal5a Release: Nov'02	Guest VLAN: No Support 802.1x w/DHCP: No Support	Not Supported
<b>3550</b>	IOS 12.1(8)EA1	VeCal5a Release (Nov '02)	Dynamic VLAN via 802.1x: VeCal5a Release: Nov'02	Guest VLAN: Feb'03 802.1x w/DHCP: No Support	User-based ACLs VeCal5a Release: Nov.'02 User-based QoS: No Support
<b>4000/4500</b>	CatOS 7.2.1+	Clearwater Release (Q3'02)	CatOS 7.2.2+	Clearwater Release (Q3'02)	???
<b>6500</b>	CatOS 7.2.1+ IOS (Achilles)	Clearwater Release (Q3'02)	CatOS 7.2.2+	Clearwater Release (Q3'02)	QoS – Q4CY2003 ACL – Not Supported
<b>Aironet AP (Authenticator)</b>	11.06	N/A	Twin Peaks (Q4 '02)		
<b>Cisco 83x</b>	CC in late Sept. '02			CC in late Sept. '02	
<b>CiscoSecure ACS</b>	V3.0 – Wireless PKI support for 802.1x	V3.1 – Catalyst support V3.1 – 802.1x and EAP	V3.0	N/A	
<b>IP Phones</b>	Supplicant – Q4CY03				



# Deployment Example

**Creating Value out of All the Pieces**

# Example Solution “A”—Access Control and User Policy Enforcement



# Deployment Example Overview

- **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 & Password to authenticate via PEAP/EAP-MSCHAPv2.**

# Scenario Dependencies

- **WinXP Clients: Require Service Pack 1 installed**
- **Windows 2000 Server for ACS 3.2: Requires all current Service Packs & Patches**
- **CatOS Switches: CatOS 7.5.1+**
- **IOS Switches: IOS 12.1(EA1)13+**
- **Enterprise PKI (ie. MS CA) or trusted 3<sup>rd</sup> party (ie. Verisign) Certificate for ACS**

# Basic Steps to Configuring 802.1x

- 1. Configure the Authentication (RADIUS) Server**
  - Add the relevant NAD.
  - Configure the required EAP Method.
  - Configure external DB access.
  - Configure policies and group mappings.
  - Create accounts.
- 2. Configure the Authenticator**
  - Add the Authentication (RADIUS) Server.
  - Configure global timers.
  - Enable authentication on relevant ports.
- 3. Configure the Supplicant**
  - Choose the EAP method.



# Authentication Server Configuration

**CiscoSecure ACS for Windows**

**CiscoSecure ACS Appliance**

# ACS Configuration

## Adding The Network Access Device

**Network Configuration**

**Select**

**AAA Clients**

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">Cat3550</a>	10.1.0.180	RADIUS (IETF)

Add Entry Search

**AAA Servers**

AAA Server Name	AAA Server IP Address	AAA Server Type
<a href="#">win2k-server</a>	10.1.0.190	CiscoSecure ACS

Add Entry Search

**Proxy Distribution Table**

Character String	AAA Servers	Strip	Account
<a href="#">(Default)</a>	win2k-server	No	Local

Add Entry Sort Entries

[Back to Help](#)

**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 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 Servers 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

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser address bar shows `http://127.0.0.1:1791/`. The main content area is titled "Network Configuration" and "AAA Client Setup For Cat3550". The configuration form includes the following fields and options:

- AAA Client IP Address: `10.1.0.180`
- Key: `cisco`
- Authenticate Using: `RADIUS (IETF)`
- Options:
  - 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

Buttons at the bottom of the form include: Submit, Submit + Restart, Delete, Delete + Restart, Cancel, and a "Back to Help" button.

The Help sidebar on the right contains the following content:

- [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.

[\[Back to Top\]](#)

# ACS Configuration

## Server Certificate Setup

**System Configuration**

**Select**

- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [ACS Certificate Setup](#)
- [Global Authentication Setup](#)

[Back to Help](#)

**Help**

- [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

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser window title is "CiscoSecure ACS - Microsoft Internet Explorer" and the address bar shows "http://127.0.0.1:1791/". The main content area is titled "System Configuration" and is divided into "Select" and "Help" sections.

**Select**

**ACS Certificate Setup**

- [Install ACS Certificate](#)
- [ACS Certification Authority Setup](#)
- [Edit Certificate Trust List](#)
- [Generate Certificate Signing Request](#)

Buttons: Cancel, Back to Help

**Help**

- [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 certificates 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 protocol. 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.

[\[Back to Top\]](#)

Buttons: Section Information

# ACS Configuration

## Server Certificate Setup – PKCS #7 Certificate Request

The screenshot shows the Cisco ACS System Configuration web interface in Microsoft Internet Explorer. The browser address bar shows `http://127.0.0.1:1791/`. The page title is "System Configuration" and the current view is "Edit".

The main content area is titled "Generate Certificate Signing Request". It contains a form for generating a new request with the following fields:

- Certificate subject:
- Private key file:
- Private key password:
- Retype private key password:
- Key length:
- Digest to sign with:

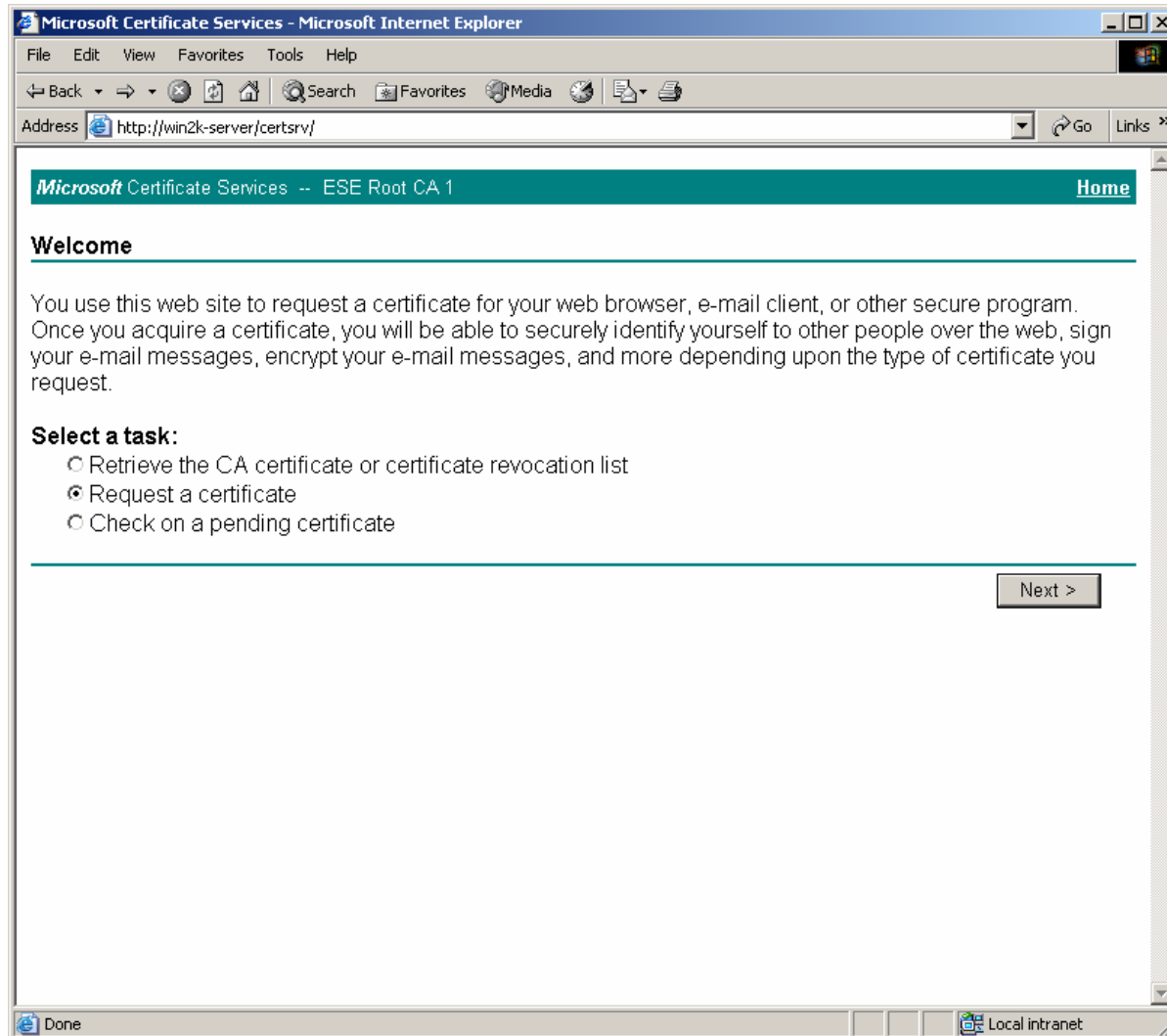
Below the form is a "Back to Help" button. At the bottom of the form area are "Submit" and "Cancel" buttons.

On the right side of the page, a message box states: "Now your certificate signing request is ready. You can copy/paste it to any certification authority enrollment tool." Below this message is a text area containing the following PKCS#7 certificate request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBVjCBwAIBADANRUwEwYDVQQDEw3aW4yay1zZXJ2ZXIwZzZ8wDQYJKoZIhvcN
AQEBBQADgYOAHIg3AoGBAKNInDX1r8Bj16xCHOm/ #4/ s2S1itQ8WfzYejK5gW7
qgEr 6ZZ1nkTPGT7rsyIQ2 1oXFQ5j 1cC40+PeYX15nSgJUVN1Q18DwYGoD809JfSx
TvE2Pg7TQ1No6jrxdBtLzB/ y+tzEwDwCkdpnS4JrUEz/ ST6vgKb+21YA6BDXXR1d
AgMBAAGgADANBgkqhkiG9w0BAQUFAA0BgQCRSsGoxF2nps5MOObEt+ErJ9c21aG+
ERoFOkw+E588Jth21Lu2urEfGzoytC+SgROju2t INvaSreeyXJuRJRDFa8THLzYL
wgaX2yZJ INwCznJrPyk+QngZj 7oK2RB41Uak6CUXXeD4NVM+IWWpeddia0XXotz
WCCB1t5P1gg5gQ==
-----END CERTIFICATE REQUEST-----
```

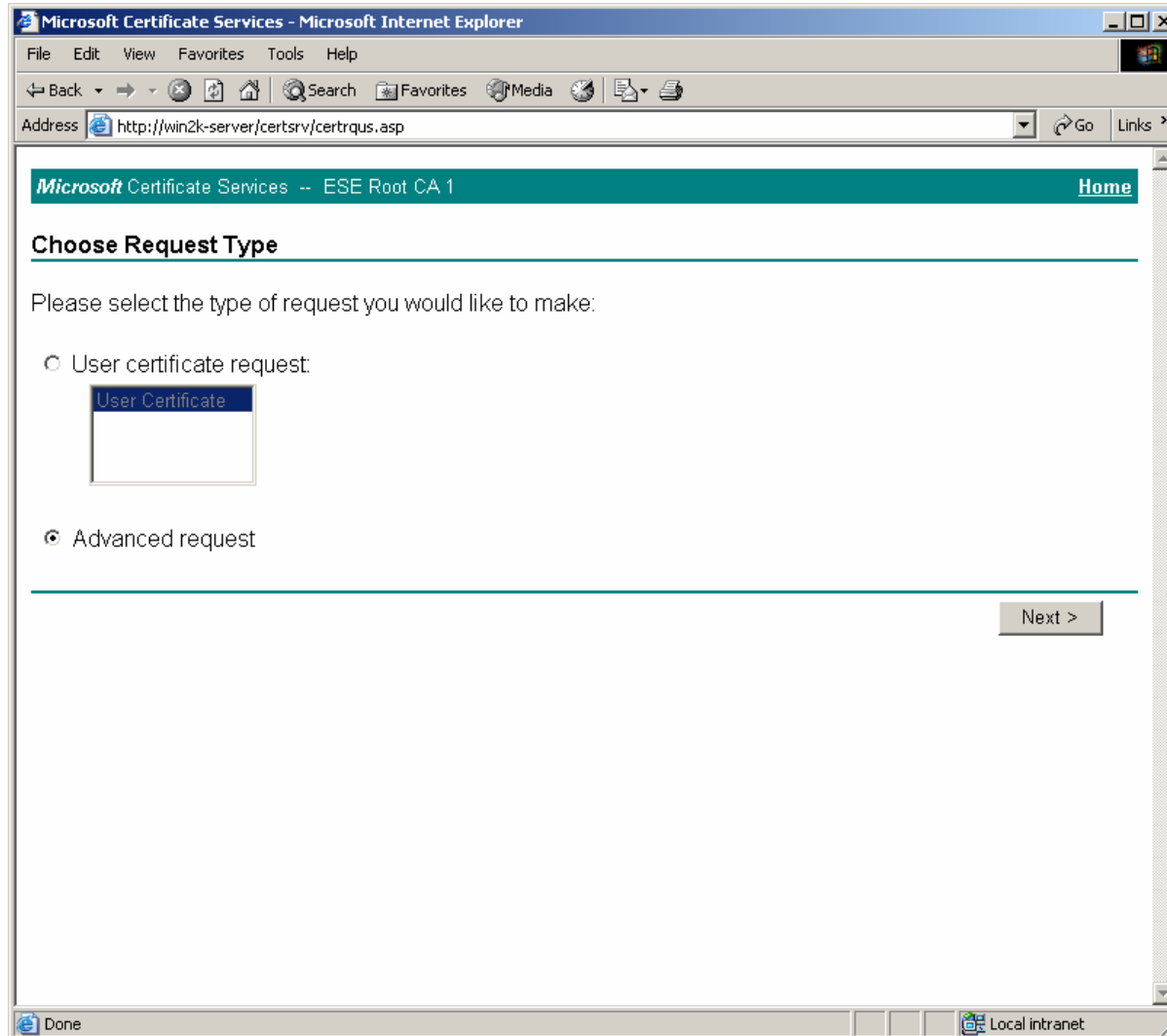
# ACS Configuration

## Server Certificate Request (MS Certificate Services)



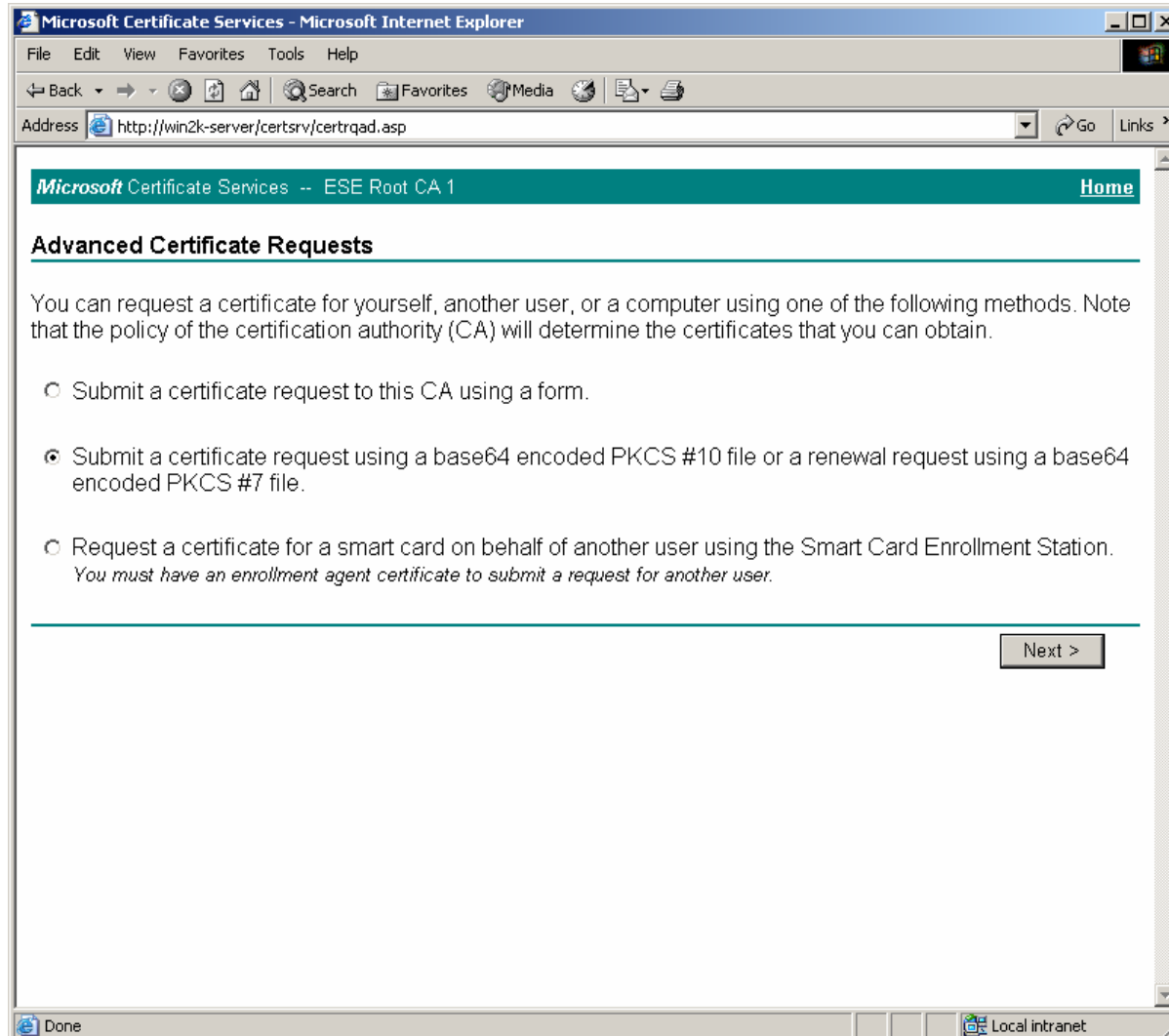
# ACS Configuration

## Server Certificate Request (MS Certificate Services)



# ACS Configuration

## Server Certificate Request (MS Certificate Services)



# ACS Configuration

## Server Certificate Request (MS Certificate Services)

The screenshot shows a Microsoft Internet Explorer browser window titled "Microsoft Certificate Services - Microsoft Internet Explorer". The address bar shows the URL "http://win2k-server/certsrv/certrqxt.asp". The page content includes a navigation bar with "Home" and a section titled "Submit A Saved Request". Below this, there is a text instruction: "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).". A text area labeled "Saved Request:" contains a base64 encoded certificate request. Below the text area is a "Browse" link. A "Certificate Template:" dropdown menu is set to "Web Server". An "Additional Attributes:" section has an empty text area. A "Submit >" button is located at the bottom right of the form.

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):

```
AgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQCRSsGo  
ERoF0kw+E588Jth21Lu2urEfGzoytC+SgROjuZtI  
wgaX2yZJINwCznNjRPyk+QngZj7oK2RB41Uak6CU  
WCCB1t5P1gq5gQ==  
-----END CERTIFICATE REQUEST-----
```

[Browse](#) for a file to insert.

**Certificate Template:**

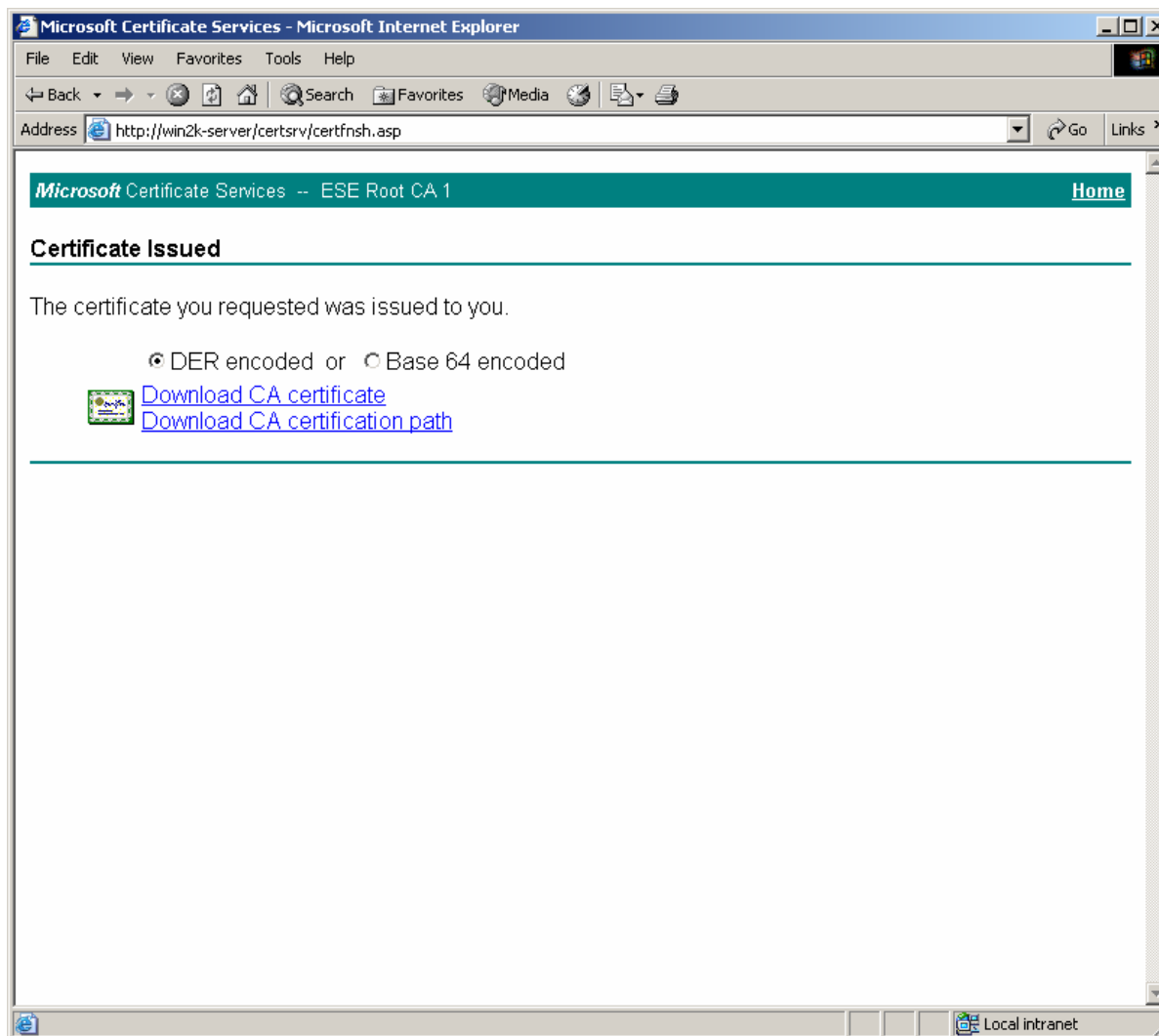
Web Server

**Additional Attributes:**

Attributes:

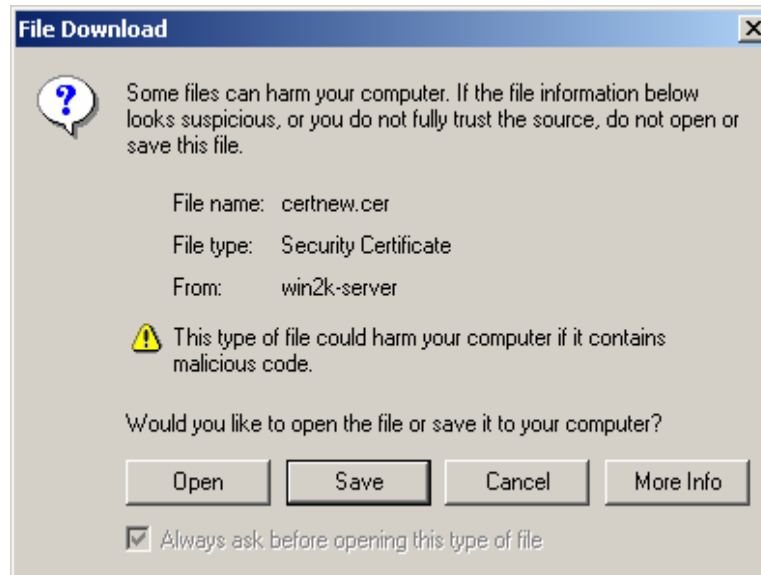
# ACS Configuration

## Server Certificate Request (MS Certificate Services)



# ACS Configuration

## Server Certificate Request (MS Certificate Services)



# ACS Configuration

## Server Certificate Installation

The screenshot shows the Cisco Secure ACS System Configuration web interface in a Microsoft Internet Explorer browser window. The browser's address bar shows the URL `http://127.0.0.1:1791/`. The main content area is titled "System Configuration" and is divided into two panes: "Edit" and "Help".

**Edit Pane:**

- Install ACS Certificate**
- Install new certificate** (with a help icon)
- Read certificate from file
  - Certificate file:
- Use certificate from storage
  - Certificate CN:
- Private key file:
- Private key password:
- [Back to Help](#)
- Buttons:

**Help Pane:**

- [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:	win2k-server
Issued by:	ESE Root CA 1
Valid from:	May 14 2003 at 16:11:00
Valid to:	May 13 2005 at 16:11:00
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.**

Install New Certificate    Cancel

[Back to Help](#)

**Help**

- [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

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser address bar shows `http://127.0.0.1:1791/`. The page title is "System Configuration" and the current view is "Edit".

**Global Authentication Setup**

**EAP Configuration**

**PEAP**

- Allow EAP-MSCHAPv2
- Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

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):

**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

[Back to Help](#)

Buttons:

**Help**

- [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 received by users who use 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. The 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

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser address bar shows <http://127.0.0.1:1791/>. The page title is "External User Databases". On the left is a navigation menu with items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases (selected), Reports and Activity, and Online Documentation. The main content area is split into two columns: "Select" and "Help".

**Select**

- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)

[Back to Help](#)

**Help**

- [Unknown User Policy](#)
- [Database Group Mappings](#)
- [Database Configuration](#)

**Unknown User Policy**

Click to configure the authentication procedure for unknown users not configured in the CiscoSecure 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](#)

[Section Information](#)

# ACS Configuration

## External User Database Configuration

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser window title is "CiscoSecure ACS - Microsoft Internet Explorer" and the address bar shows "http://127.0.0.1:1791/". The main content area is titled "External User Databases" and is divided into two panes: "Select" and "Help".

**Select Pane:**

**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](#)

**Help Pane:**

- [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 SecurIDToken Server](#)

**Windows Database**

Click to configure Windows SAM 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 Service. While Active Directory is based on LDAP, use a [Windows](#) database configuration for authenticating users with Active Directory.

# ACS Configuration

## External User Database Configuration

**External User Databases**

**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**

Available Domains: [Empty Box]

Domain List: ESELABS

Buttons: [->], [-<], [Up], [Down]

**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**

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 this 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 re-try authentication for 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

The screenshot shows the Cisco Secure ACS web interface in Microsoft Internet Explorer. The browser title is "CiscoSecure ACS - Microsoft Internet Explorer" and the address bar shows "http://127.0.0.1:1791/". The main content area is titled "External User Databases" and contains several configuration sections:

- MS-CHAP Settings:** Includes two checked options: "Permit password changes using MS-CHAP version 1." and "Permit password changes using MS-CHAP version 2." Below these is a note: "These settings can be used to enable or disable password changes using the MS-CHAP version 1 or version 2 protocols."
- Windows EAP Settings:** Includes three checked options: "Permit password change inside PEAP.", "Permit PEAP machine authentication.", and "Permit EAP-TLS machine authentication." There is an unchecked option "EAP-TLS Strip Domain Name." and a text input field for "EAP-TLS and PEAP machine authentication name prefix" containing the text "host/". Below this is a note: "These settings can be used to enable or disable specific Windows EAP functionality."

At the bottom of the configuration area are "Submit" and "Cancel" buttons, and a "Back to Help" button with a question mark icon. The right sidebar contains a "Help" section with a list of links: "Windows Database Configuration", "Dialin Permission", "Configure Domain List", "MS-CHAP Settings", and "Windows EAP Settings". Below the links are three sections of help text: "Windows Database Configuration", "Dialin Permission", and "Configure Domain List", each with a "[Back to Top]" link. The "MS-CHAP Settings" section is partially visible at the bottom of the sidebar.

# ACS Configuration

## External User Database Group Mapping

**External User Databases**

**Select**

**Unknown User Group Mappings**

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

Name	Type
<a href="#">Windows Database</a>	Windows Database

[Cancel](#)

[Back to Help](#)

**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 an external user database 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](#)

[Section Information](#)

# 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](#)

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 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

**External User Databases**

**Edit**

**Define New Domain Configuration**

Detected Domains:

- ESELABS

Domain:

Clear Selection

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](#)

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 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

**External User Databases**

**Edit**

Domain Configurations
<a href="#">ESELABS\DEFAULT</a>

**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 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

**External User Databases**

**Edit**

Group Mappings for Domain : ESELABS

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 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

**External User Databases**

**Edit**

Create new group mapping for Domain : ESELABS

**Define NT group set**

NT Groups

- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins**
- Group Policy Creator Owners
- Schema Admins

Add to selected Remove from selected

Selected

- Engineering VLAN Users**

Up Down

CiscoSecure group: Group 5

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](#)

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 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**.

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://127.0.0.1:2253/

## External User Databases

**CISCO SYSTEMS**

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

**Edit**

Group Mappings for Domain : ESELABS

NT groups	CiscoSecure group
<a href="#">Engineering VLAN Users, *</a>	Group 5

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 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**.

Presentation\_ID

© 2003 Cisco Systems, Inc. All rights reserved.

151

# ACS Configuration

## User Interface Option Configuration

The screenshot shows a web browser window titled "CiscoSecure ACS - Microsoft Internet Explorer" with the address bar showing "http://127.0.0.1:2253/". The main content area is titled "Interface Configuration" and is divided into two columns: "Select" and "Help".

**Select Column:**

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

**Help Column:**

- [User Data Configuration](#)
- [RADIUS \(IETF\)](#)
- [Advanced Options](#)

A "Back to Help" button is visible in the Select column.

**Help Content:**

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 window.

[\[Back to Top\]](#)

**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

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser address bar shows `http://127.0.0.1:2253/`. The main content area is titled "Interface Configuration" and contains a list of configuration options for RADIUS AV pairs. A sidebar on the left contains navigation links for various configuration sections. A "Help" window is open on the right, displaying information about RADIUS (IETF) attributes.

**Interface Configuration**

- [020] Termination-Action
- [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:

[Back to Help](#)

**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

**CiscoSecure ACS - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Address <http://127.0.0.1:2253/>

### CISCO SYSTEMS Group Setup

**Select**

Group: 5. Group 5

Users in Group Edit Settings Rename Group

Back to Help

**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

The screenshot displays the CiscoSecure ACS Group Setup configuration page. The browser window title is "CiscoSecure ACS - Microsoft Internet Explorer" and the address bar shows "http://127.0.0.1:2253/". The page features a left-hand navigation menu with icons for User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Group Setup" and includes a "Jump To" dropdown menu set to "Access Restrictions". Below this, there is a list of configuration options, each with a checkbox and a corresponding input field:

- [034] Login-LAT-Service
- [035] Login-LAT-Node
- [036] Login-LAT-Group
- [037] Framed-AppleTalk-Link (0..65535)
- [038] Framed-AppleTalk-Network (0..65535)
- [039] Framed-AppleTalk-Zone
- [062] Port-Limit
- [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

At the bottom of the configuration area are buttons for "Submit", "Submit + Restart", and "Cancel". On the right side, there is a "Help" section with a list of links:

- [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](#)

Below the links, there is a section titled "Group Settings" with explanatory text and a list of conditions:

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 protocol 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 a user is assigned to is 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*

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

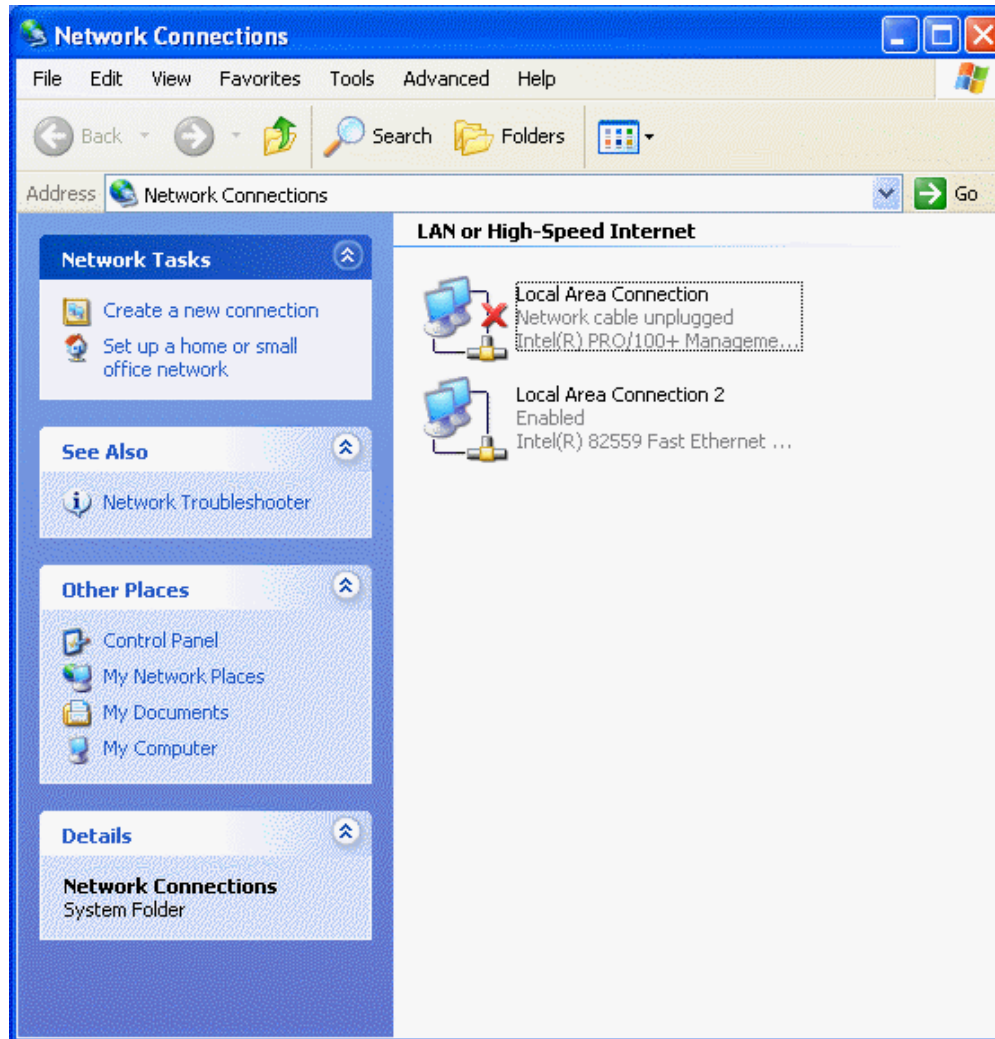


# Client Supplicant Configuration

## Windows XP SP1

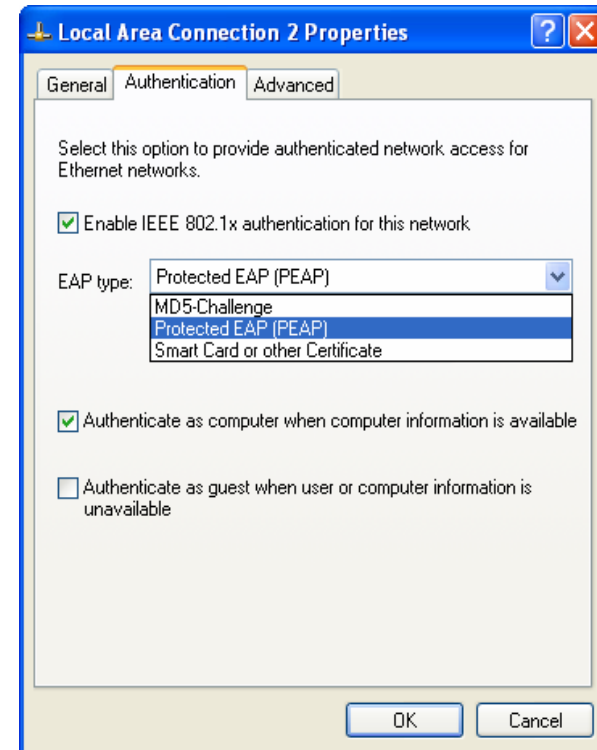
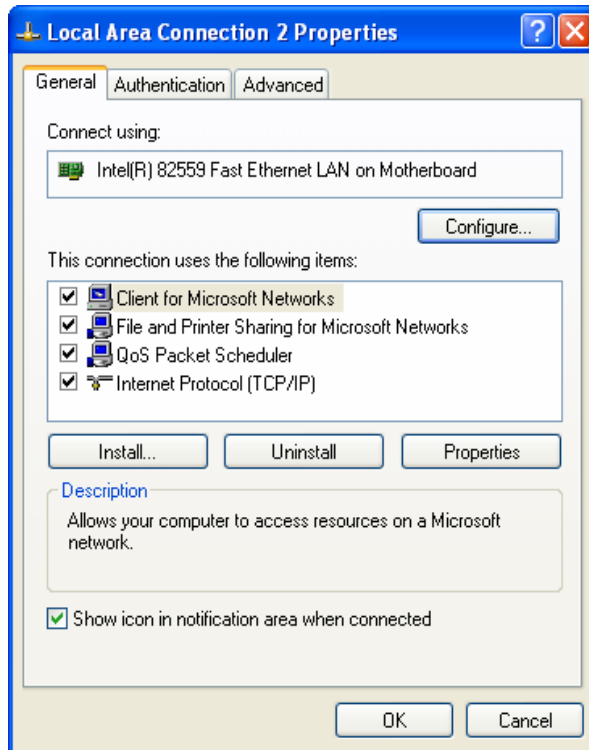
# Supplicant Configuration

## *Network Connection Properties*

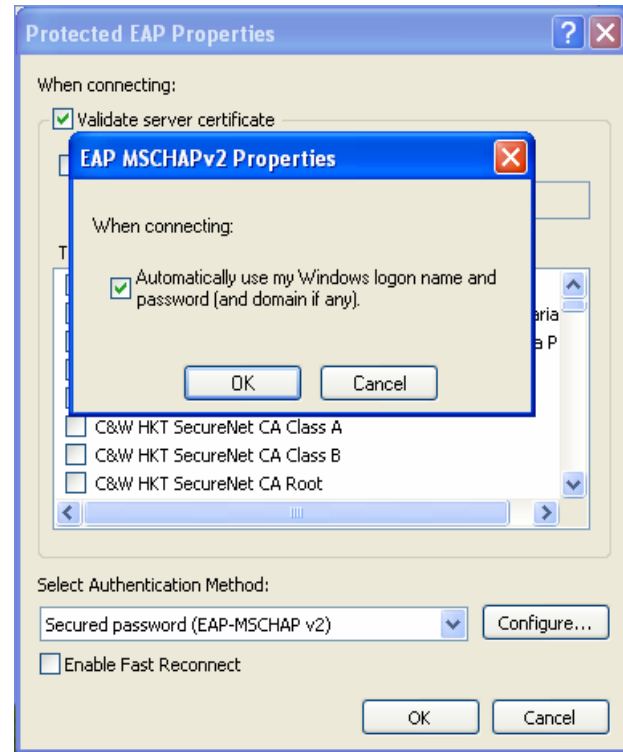
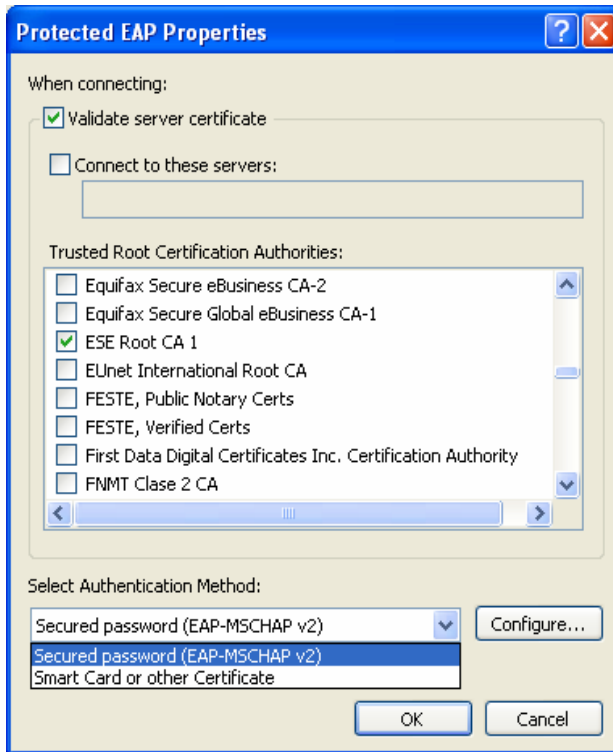


# Supplicant Configuration

## Network Interface Authentication Properties

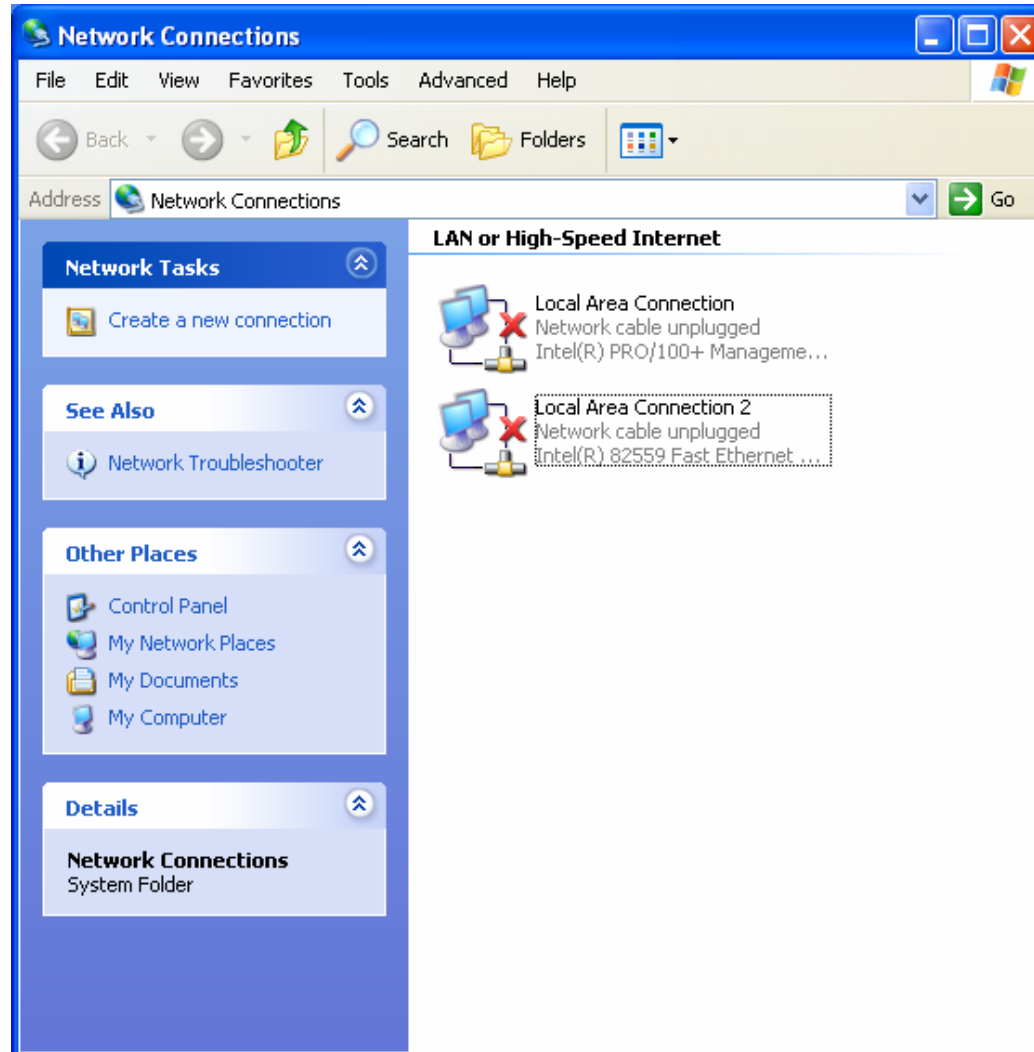


# Supplicant Configuration Authentication Method - *PEAP* Configuration



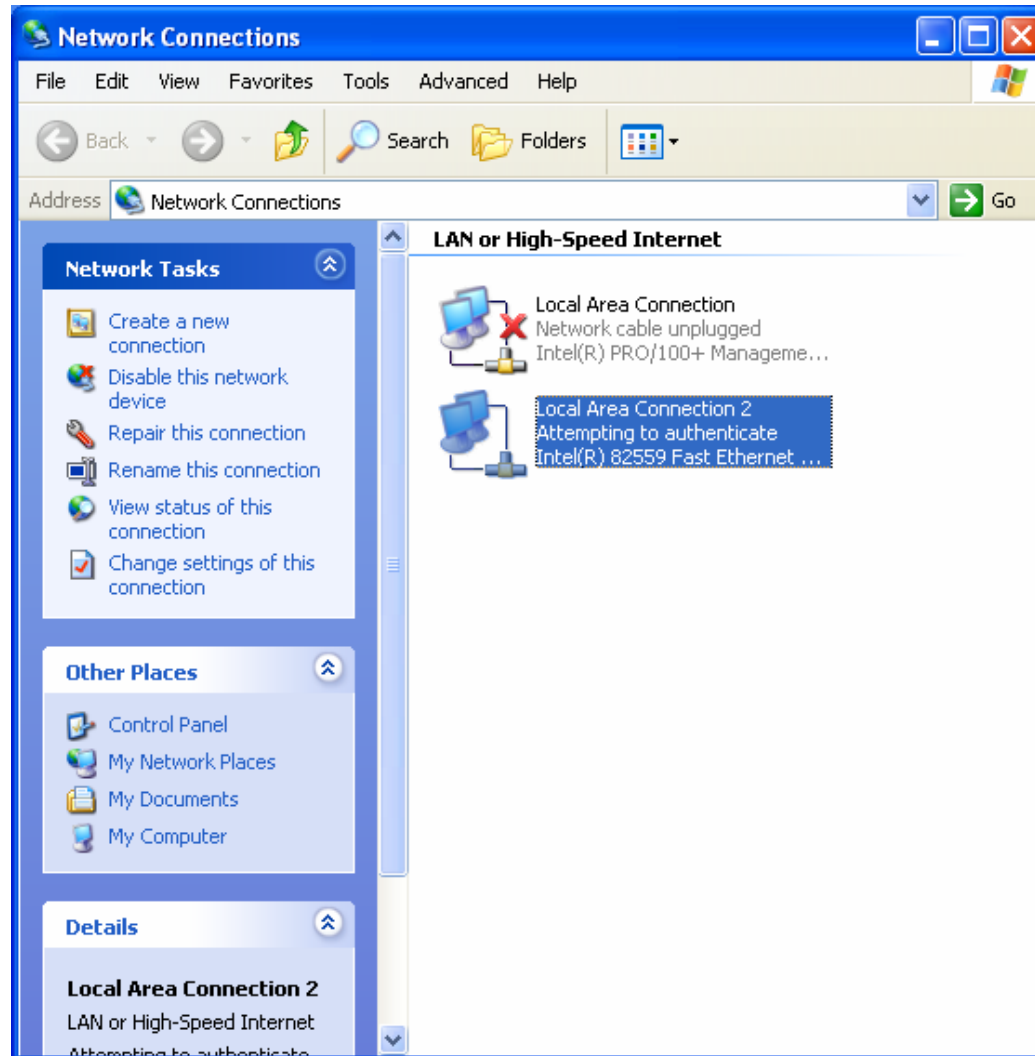
# Supplicant Configuration

## Interface Status – *Disconnected State*



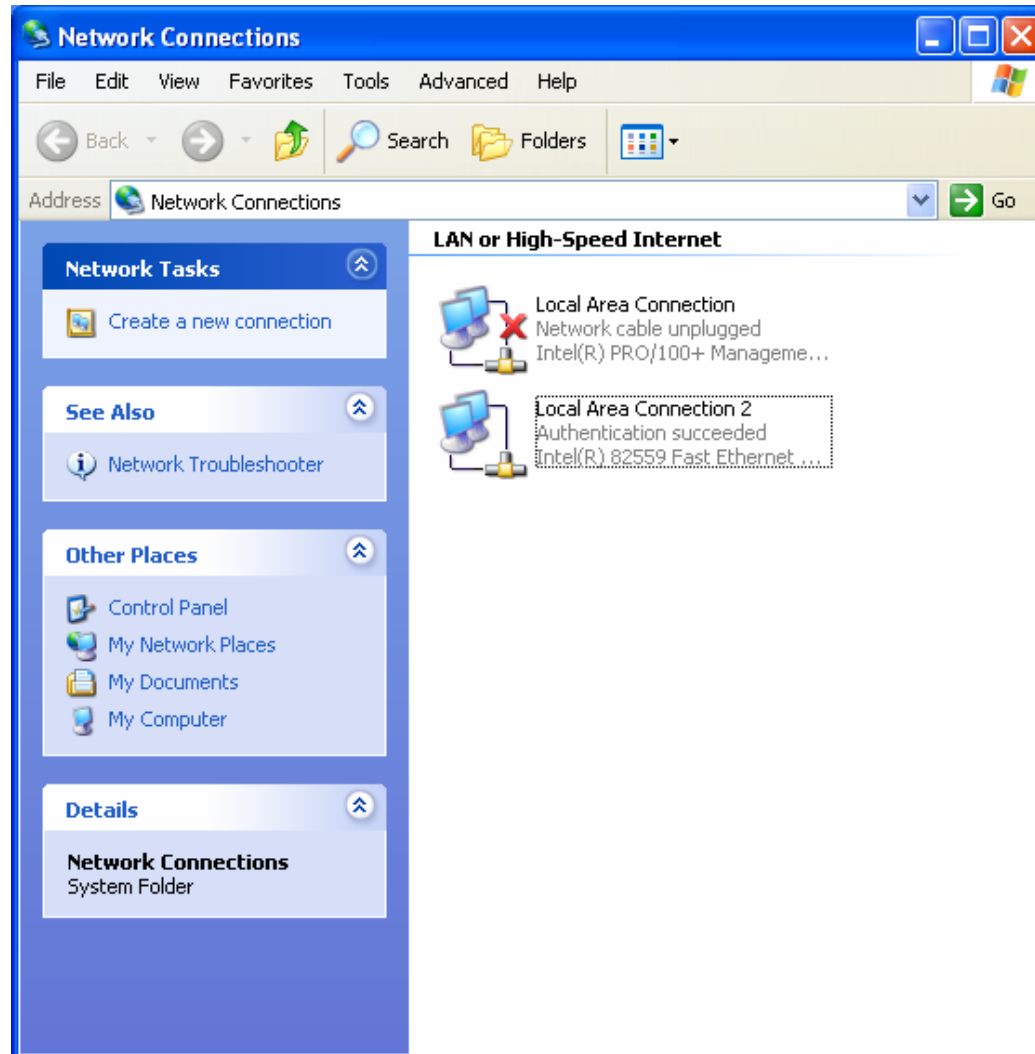
# Supplicant Configuration

## Interface Status – Connected/Authenticating State



# Supplicant Configuration

## Interface Status – Auth Successful/Connected State



**CISCO SYSTEMS**



# 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

**CiscoSecure ACS on win2k-server**  
**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  KB

Manage Directory  
 Keep only the last  files  
 Delete files older than  days

[Back to Help](#)

Restart Stop Cancel

**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 CSAAdmin) from within Windows Control Panel. CSAAdmin 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, CSAAdmin 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 log file 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 log file 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 log file 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

**System Configuration**

**Logging Configuration**

Use	Local Logging Configuration
<input checked="" type="checkbox"/>	<a href="#">CSV Failed Attempts</a>
<input checked="" type="checkbox"/>	<a href="#">CSV Passed Authentications</a>
<input checked="" type="checkbox"/>	<a href="#">CSV RADIUS Accounting</a>
<input checked="" type="checkbox"/>	<a href="#">CSV TACACS+ Accounting</a>
<input checked="" type="checkbox"/>	<a href="#">CSV TACACS+ Administration</a>
<input type="checkbox"/>	<a href="#">CSV VoIP Accounting</a>
<input type="checkbox"/>	<a href="#">ODBC Failed Attempts</a>
<input type="checkbox"/>	<a href="#">ODBC Passed Authentications</a>
<input type="checkbox"/>	<a href="#">ODBC RADIUS Accounting</a>
<input type="checkbox"/>	<a href="#">ODBC TACACS+ Accounting</a>
<input type="checkbox"/>	<a href="#">ODBC TACACS+ Administration</a>
<input type="checkbox"/>	<a href="#">ODBC VoIP Accounting</a>
<input type="checkbox"/>	<a href="#">Remote Logging</a>

[Cancel](#)

[Back to Help](#)

**Help**

- [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**

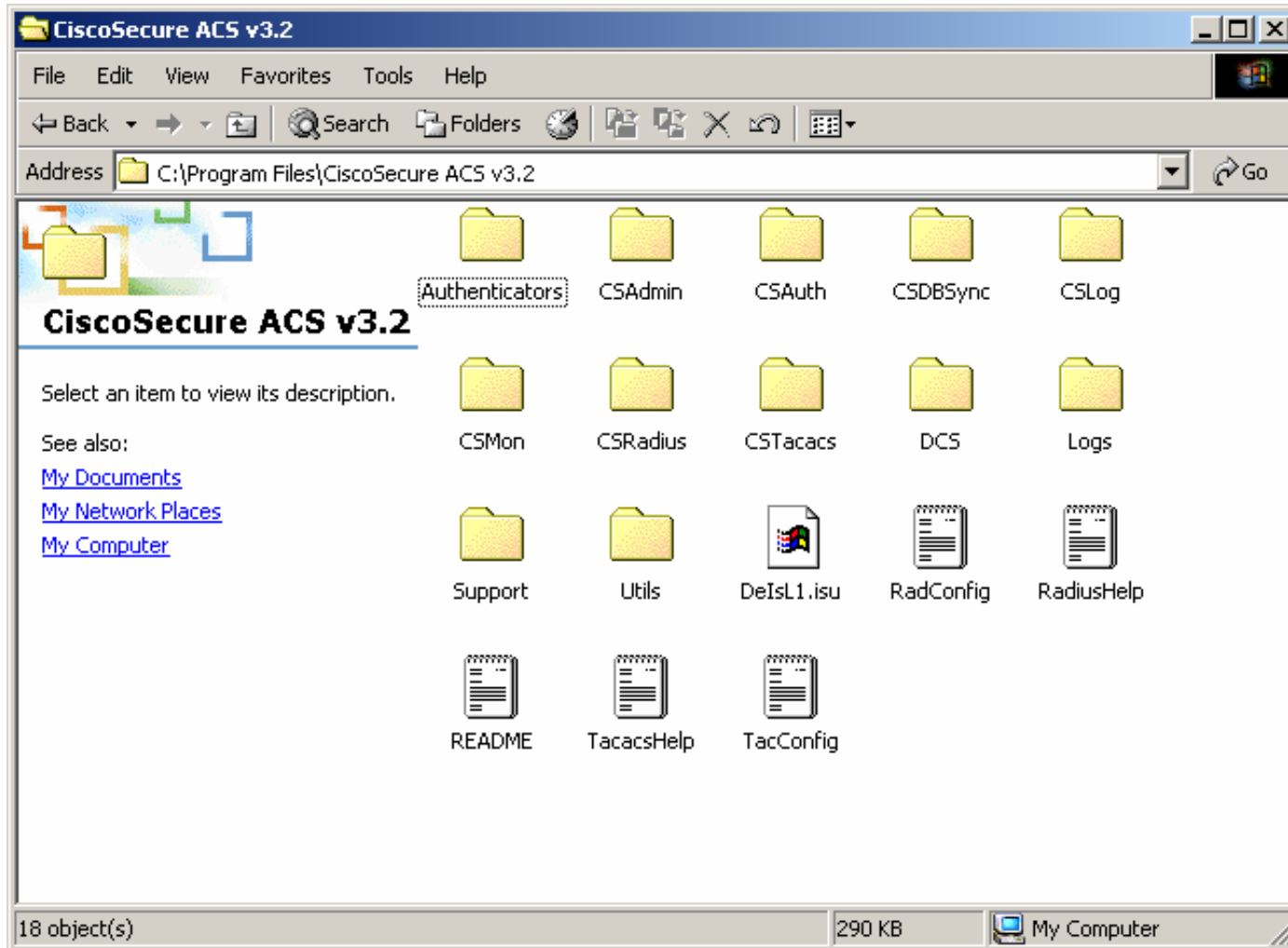
Click this option to enable and configure Cisco Secure ACS to generate a CSV log of successful login attempts.

[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'**

# IOS Authenticator Troubleshooting

- Use the debug command like on 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**

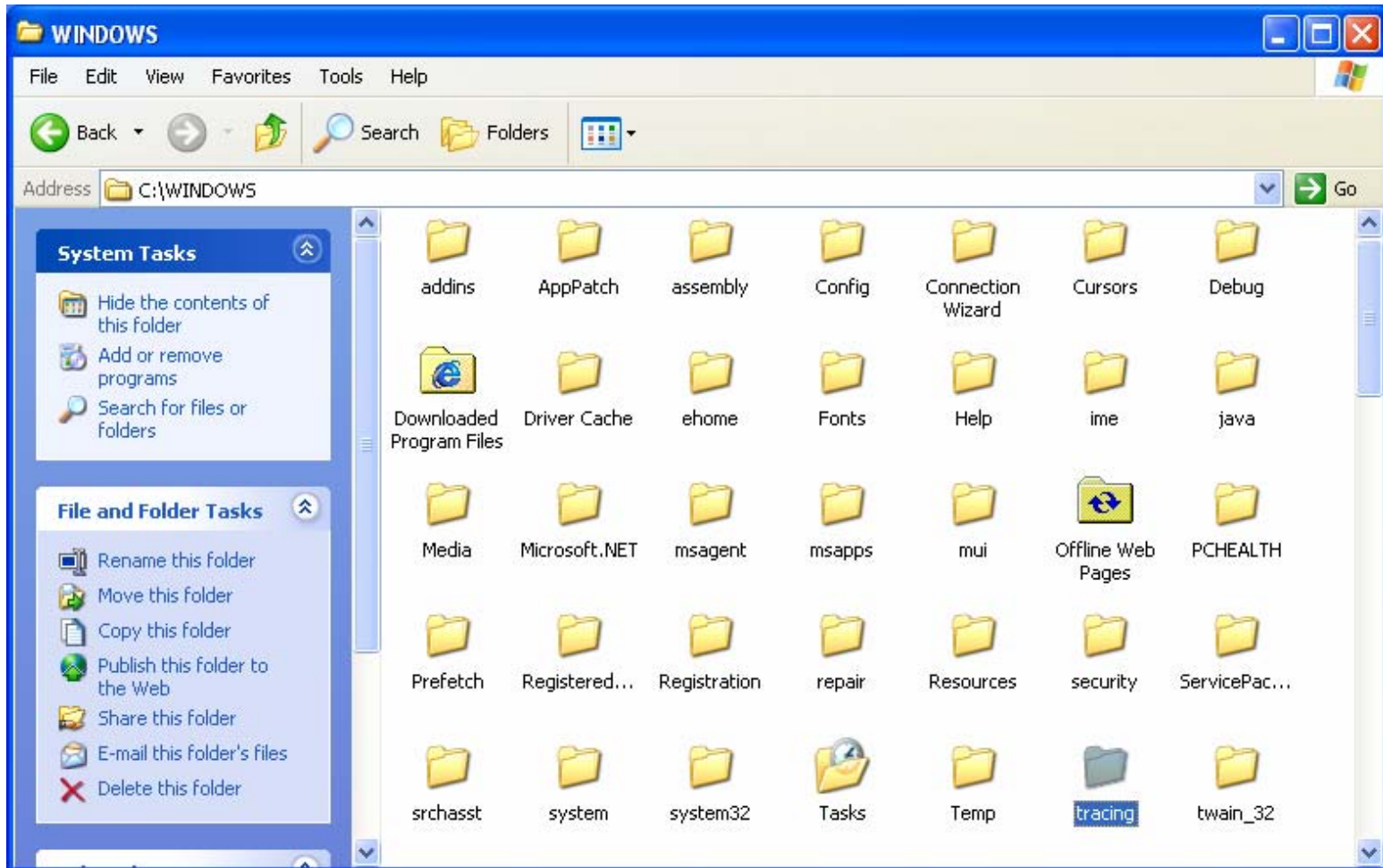
**'netsh ras set tr \* enable'**

**Enables supplicant tracing and logging.**

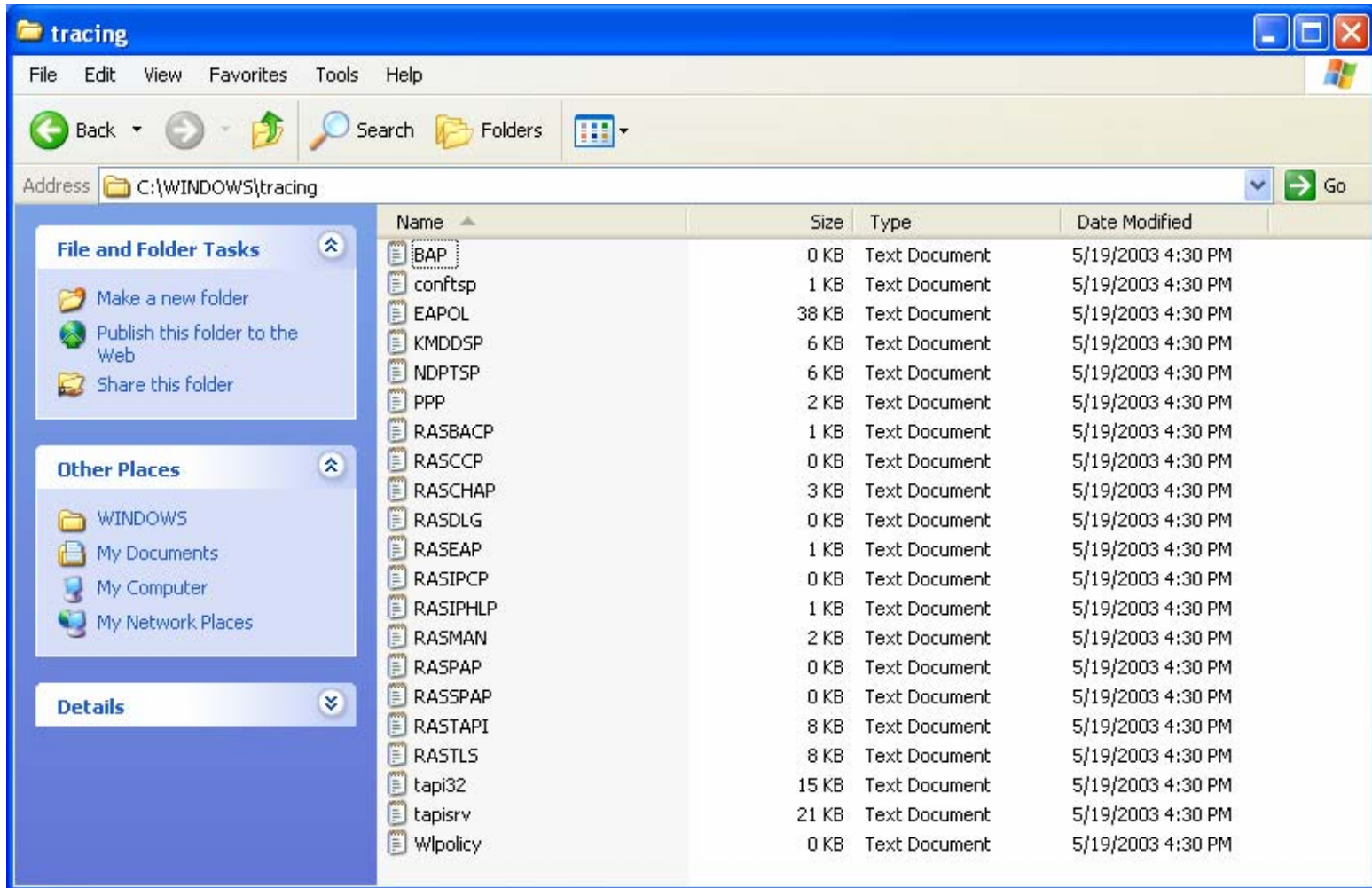
**Creates logging debug files in '%systemRoot%/tracing'**

**Disable it with the command 'netsh ras set tr \* disable'**

# Windows Troubleshooting – Tracing Directory



# Windows Troubleshooting – Tracing Files



# Examining the EAPOL log

[1496] 16:30:35: *EIMediaEventsHandler entered*  
[1496] 16:30:35: *EIMediaEventsHandler: Calling EIMediaSenseCallback*  
[1496] 16:30:35: *EIMediaSenseCallback: Entered*  
[1496] 16:30:35: *EIMediaSenseCallbackWorker: For interface (Intel(R) 82559 Fast Ethernet LAN on Motherboard), GUID ({0D7295D2-F5F1-4A62-A494-AA3D4239CF49}), length of block = 94*  
**[1496] 16:30:35: EIMediaSenseCallbackWorker: Callback for sense connect**  
[1496] 16:30:36: *ElloCompletionRoutine called, 60 bytes xferred*  
[1496] 16:30:36: *EIReadCompletionRoutine 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: EIEapEnd entered*

*[1496] 16:30:36: EIEapBegin entered*

*[1496] 16:30:36: EIEapBegin done*

*[1496] 16:30:36: EIEapWork: EapIPkt created at 00137008*

*[1496] 16:30:36: EIEapMakeMessage entered*

*[1496] 16:30:36: EIParseIdentityString: Packet length 5 less than minimum 5*

*[1496] 16:30:36: EIGetIdentity: Userlogged, Prev !Machine auth*

*[1496] 16:30:36: EIGetIdentity: Userlogged, <Maxauth, Prev !Machine auth: !MD5*

*[1496] 16:30:36: EIGetUserIdentity entered*

*[1496] 16:30:36: EIGetEapUserInfo: Get value succeeded*

*[1496] 16:30:36: EIGetEapUserInfo: Get value succeeded*

*[1496] 16:30:36: EIGetUserIdentityOptimized: Got identity = ESELABS\Administrator*

*[1496] 16:30:36: EIGetUserIdentity: EIGetUserIdentityOptimized got identity without user module intervention*

# Examining the EAPOL log

*[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

```
[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: ElEapDIIWork called for EAP Type 25
[1496] 16:30:37: EAP DII returned Action=EAPACTION_Send
[1496] 16:30:37: ElEapDIIWork 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: EIPProcessEapSuccess: Got EAPCODE\_Success**  
*[1496] 16:30:39: EIEapEnd entered*  
*[1496] 16:30:39: EIEapDIIEnd called for EAP Index 1*  
**[1496] 16:30:39: EIPProcessEapSuccess: 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: EIEapEnd entered*  
**[1496] 16:30:39: FSMAuthenticated: Queued EIIPPnPWorker**  
**[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),  
lastauththtype=(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

```
[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
```

# Examining the RASTLS log

```
[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
```



# What's Ahead?

## The Future Directions of Identity-Based Networking

# What's Ahead? (lan's todo list)

- **Additional Policy capabilities**
  - QoS
  - Rate-Limiting
  - User name to port description
  - Failed authentication guest access
- **Increased integration into directory services**
  - Improved Active Directory Support
  - Improved LDAP support
- **Increased device support for IBNS**
  - IP Phones (supplicant)
  - WLAN APs (IBNS Conformance, supplicant)
  - 3<sup>rd</sup> party devices – Printers (HP)
- **Tighter integration into other Cisco solution sets**
  - Catalyst Integrated Security/Tunneling technologies
  - Antibody
  - CPS
  - NIDS
  - Firewall/FWSM

# More on my to-do list...

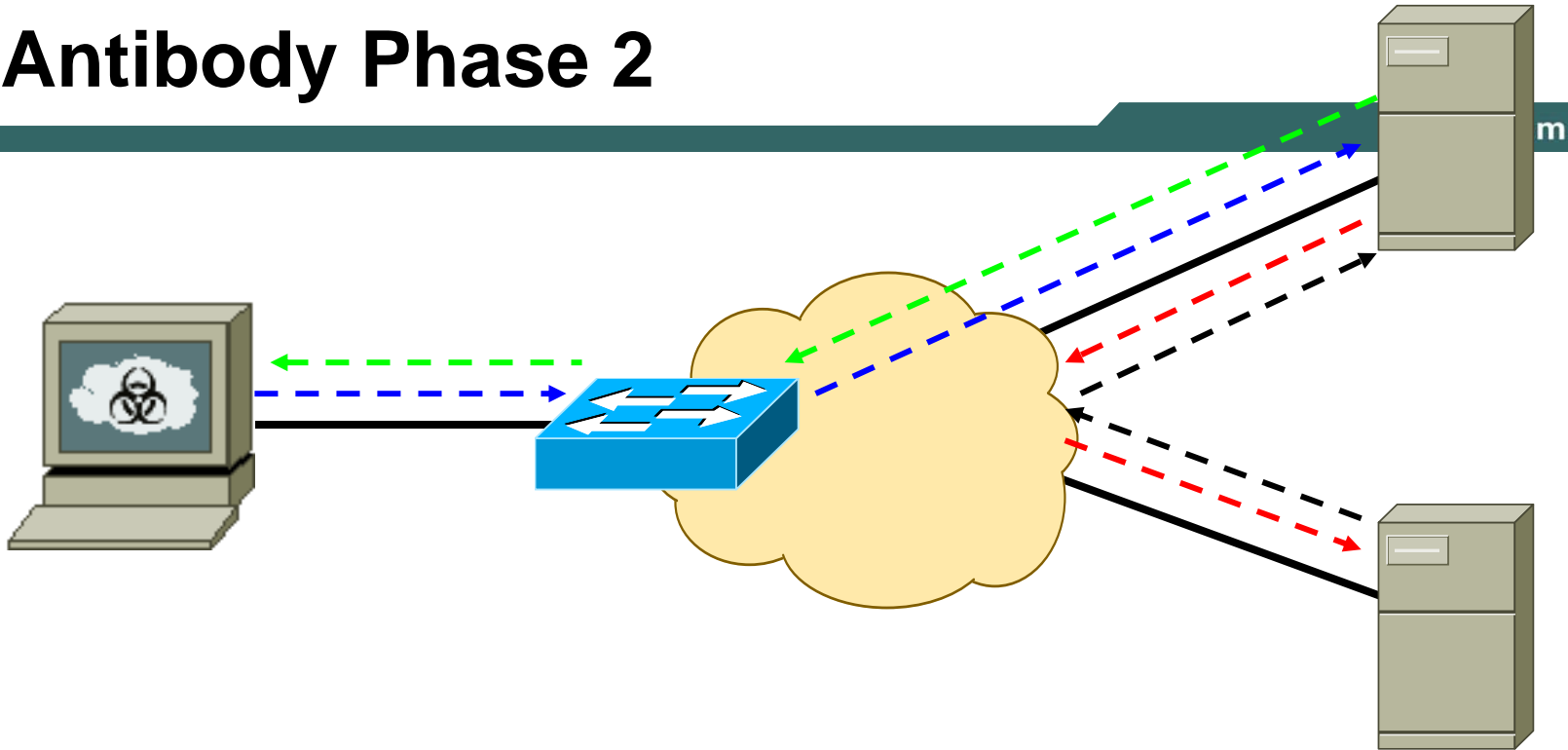
- **Switch Integrated Web Based 802.1x proxy**
  - Access switch HTTP/HTTPS based login (no supplicant required)
  - Leverage 802.1x backend
  - Leverage 802.1x gains
- **IBNS Management**
  - Phase 1 – Test & operate with existing tools
  - Phase 2 – Integration between Management platforms and IBNS components
- **Port Based RADIUS MAC Checking**
- **Link Layer IBNS Crypto (Ian's Wish List)**



# Antibody

**Avoid and Avert the Inevitable**

# Antibody Phase 2



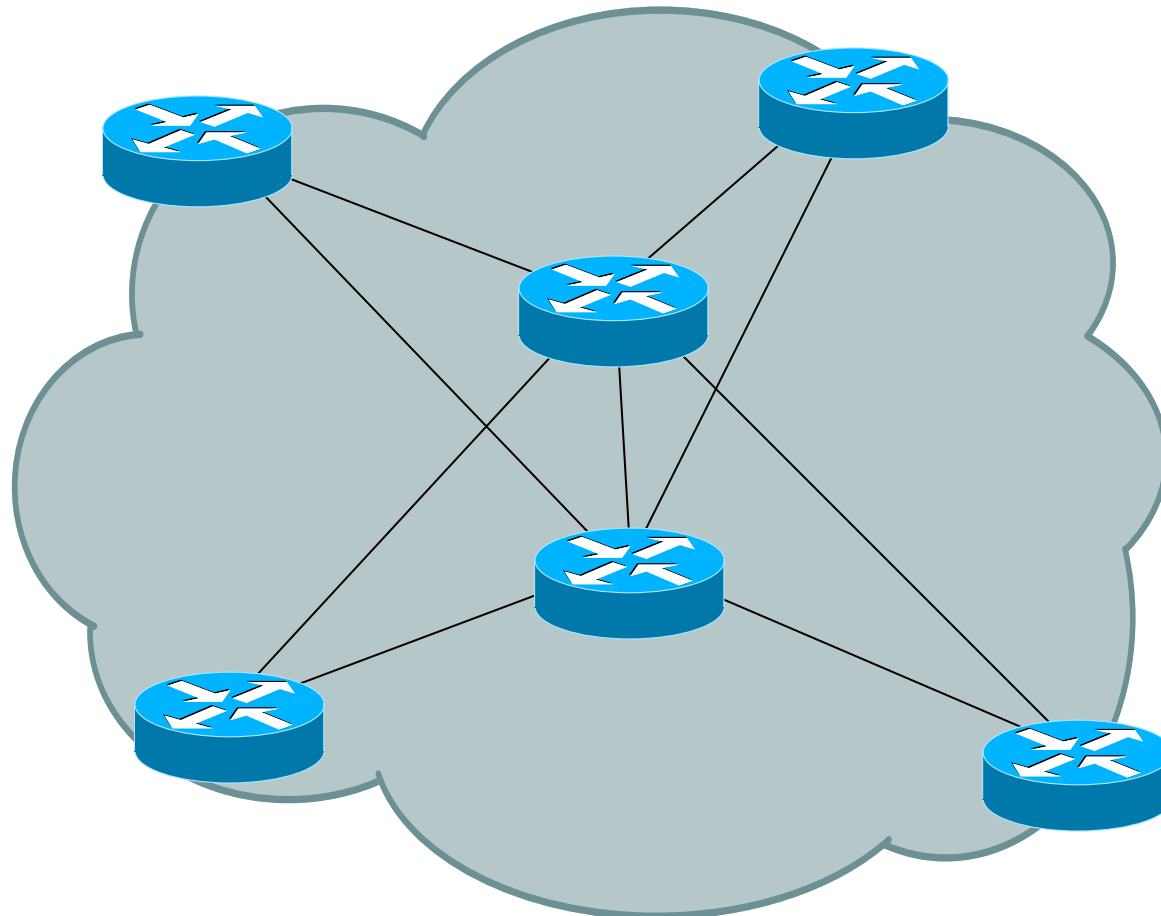
1. Antibody Agent gathers & sends posture information to AAA server.
2. AAA Server forwards posture information to validation server (Symantec, Trend, NAI, etc).
3. Validation Server compares information to acceptable values & sends response back to AAA Server.
4. AAA Server factors in posture information in intelligent decision process and updates network elements.



# Cisco Pervasive Security (CPS)

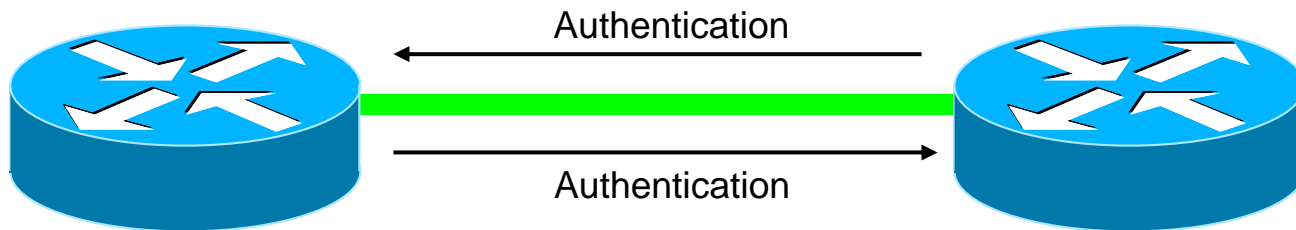
**Trusting the Network**

# Standard Network Core



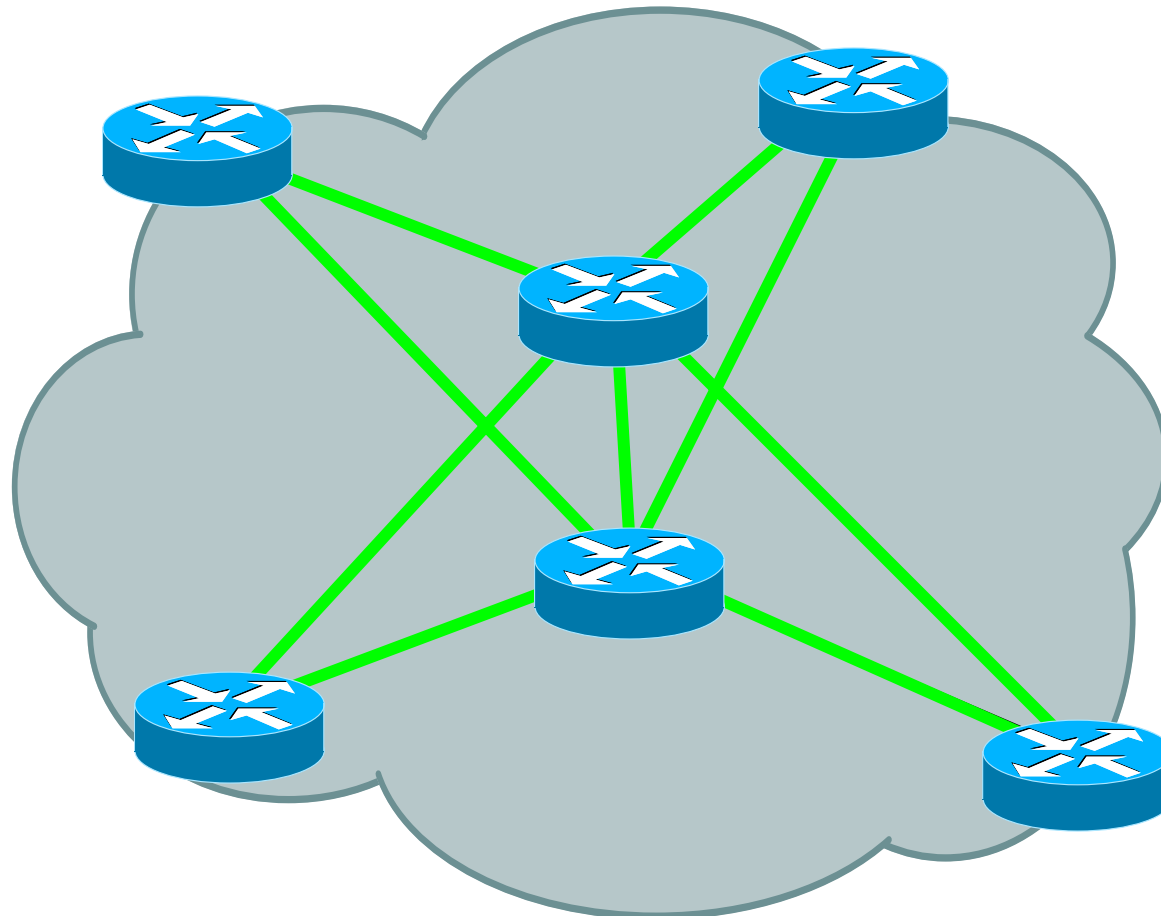
# CPS Protected Link

## 1. Mutual Authentication



## 2. Encrypted Channel

# CPS Protected Network Core

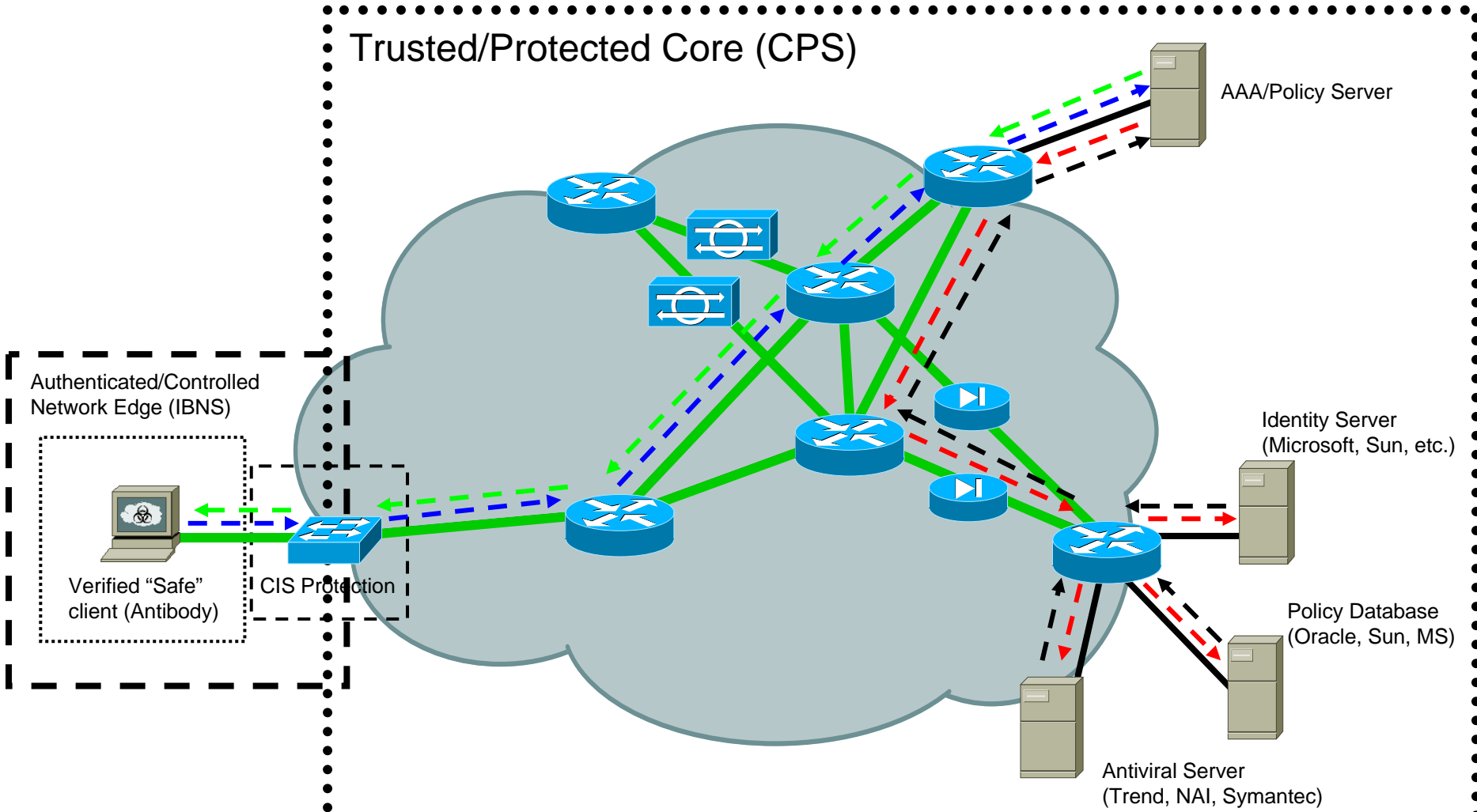




# Cisco Enterprise Security

**A Combined Cross-BU/Cross-Product Solution Space**

# Combined Solution Space



# Benefits?

- **Trusted core (CPS)**
- **Protected Core (CPS)**
- **Controlled network edge (IBNS & CIS)**
- **Usage monitoring, accountability, logging, & tracing (IBNS, IBNS w/NIDS & FW)**
- **Reduced risk insertion into stable environment (Antibody)**
- **Protected entry into trusted core (IBNS/Antibody)**
- **Privacy & Integrity across the network (IBNS, Antibody, CPS)**