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

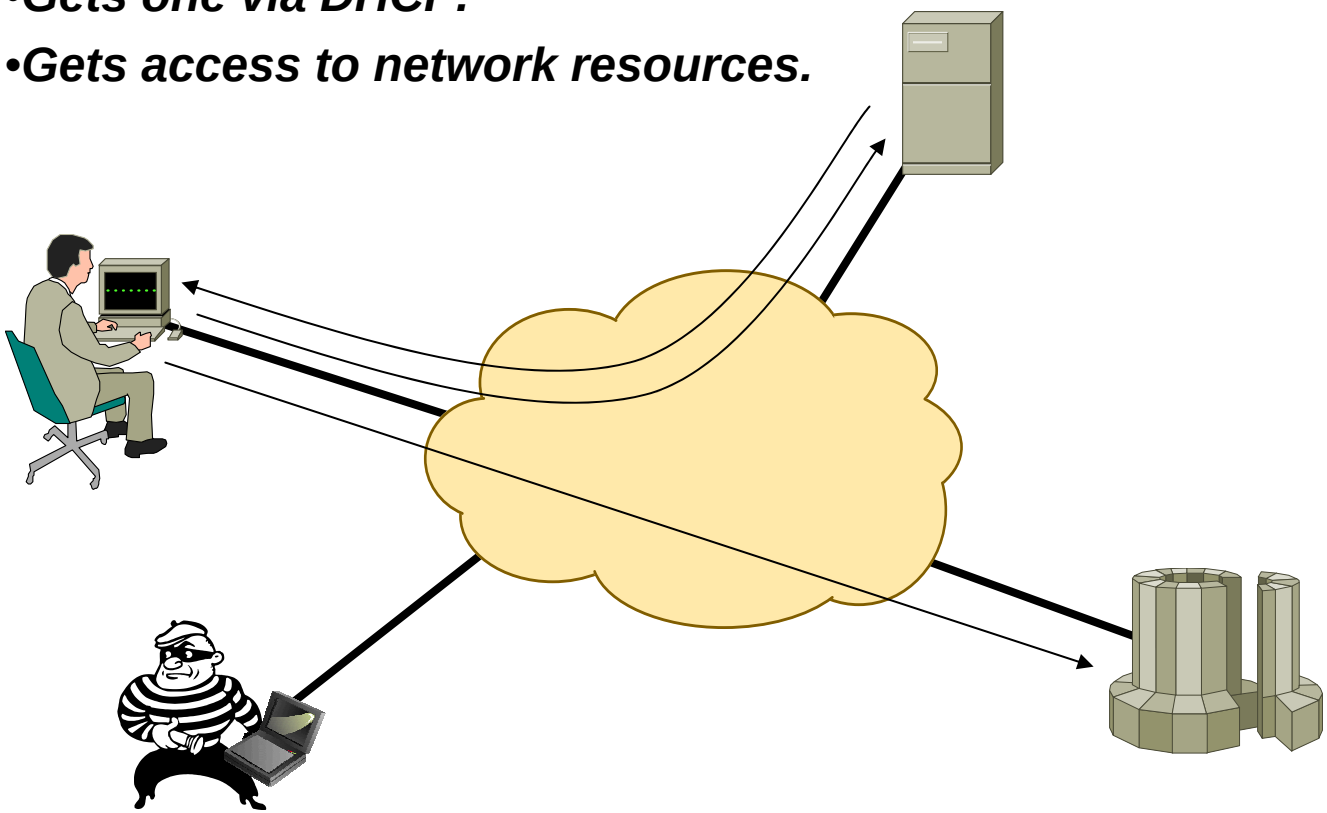
Providing Authentication and access control on network ports can significantly reduce the potential attacker community.

“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.**

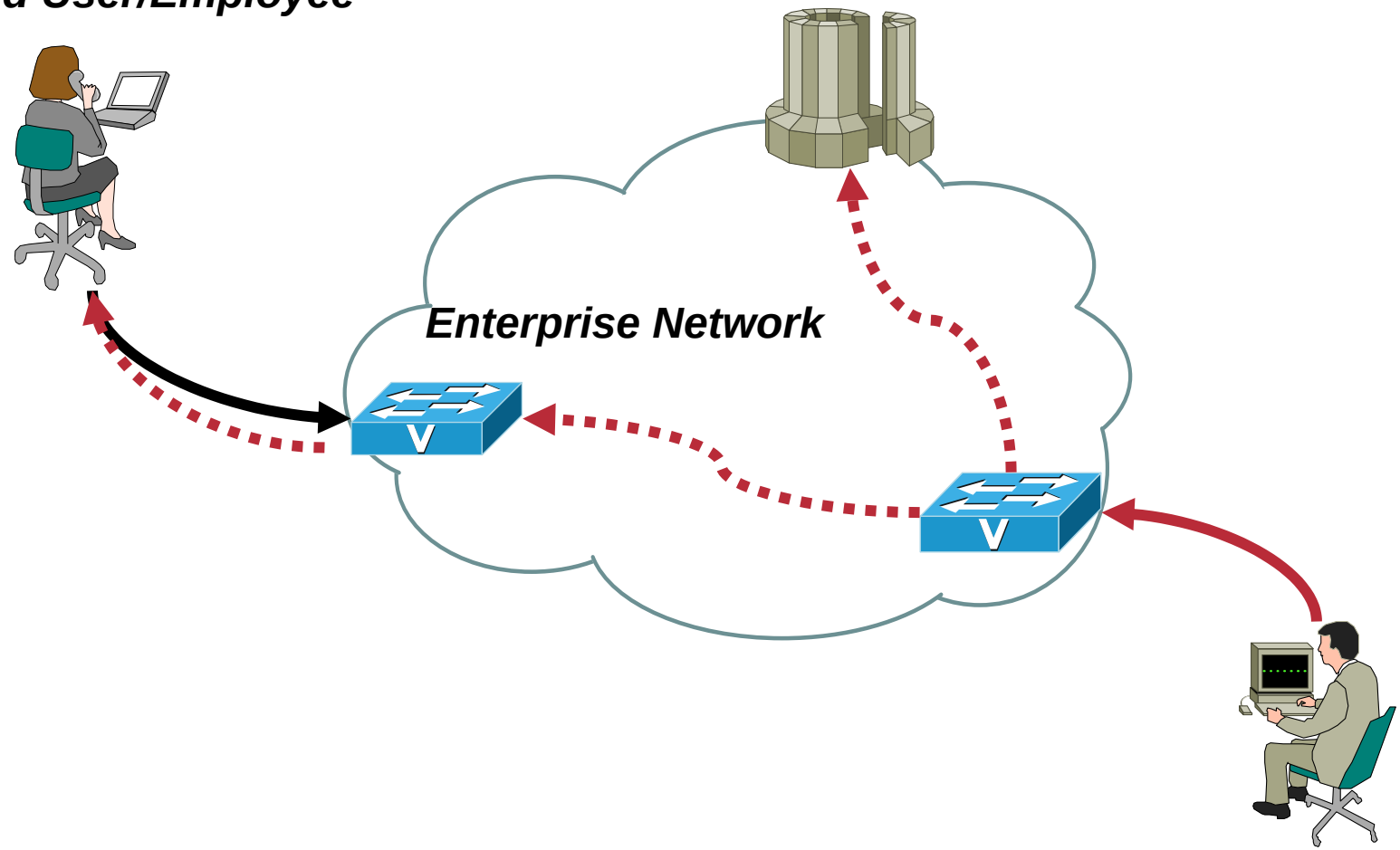
Insider attack by disgruntled employees was listed as likely source by **75%** of respondents

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

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

“Keep the insiders honest”

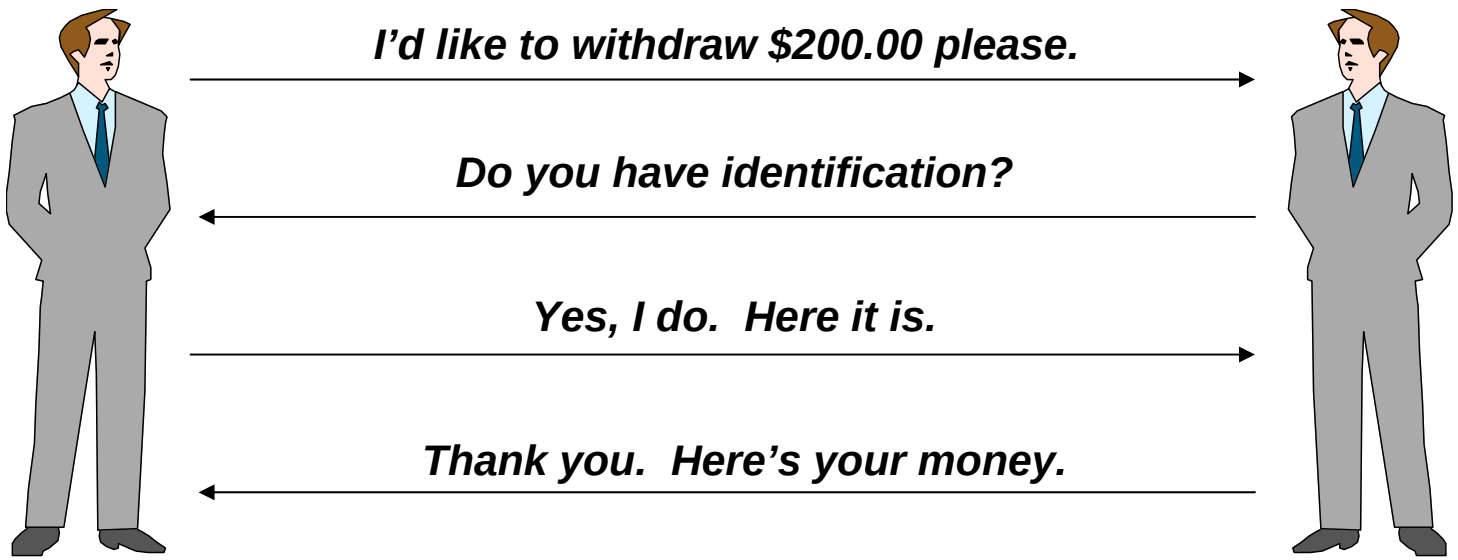
Unauthorized Use of the Network



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?

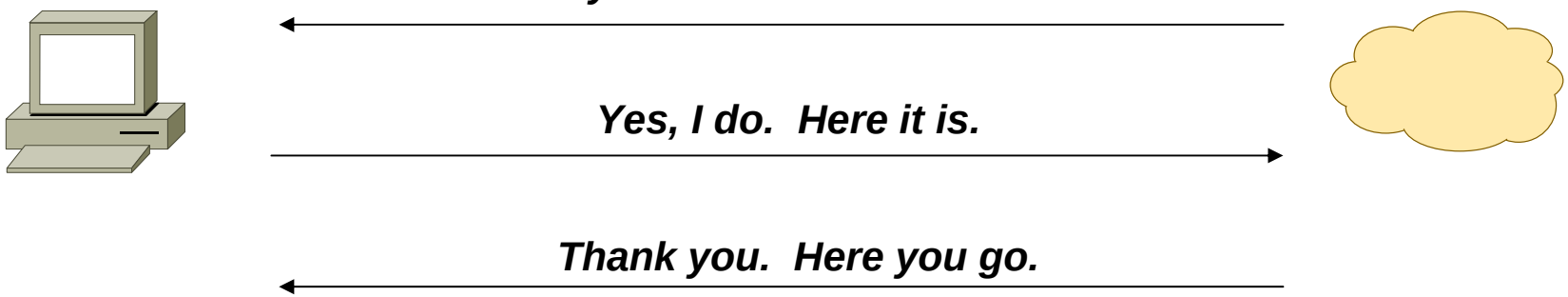
- **Because differentiation of services and rights control is critical in network environments.**
- **Not everyone has the same privileges. Not all resources or information have the same level of confidentiality.**

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



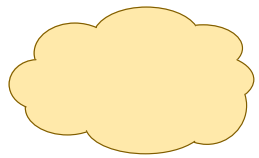
Applying the Authentication Model to the Network

I'd like to connect to the network

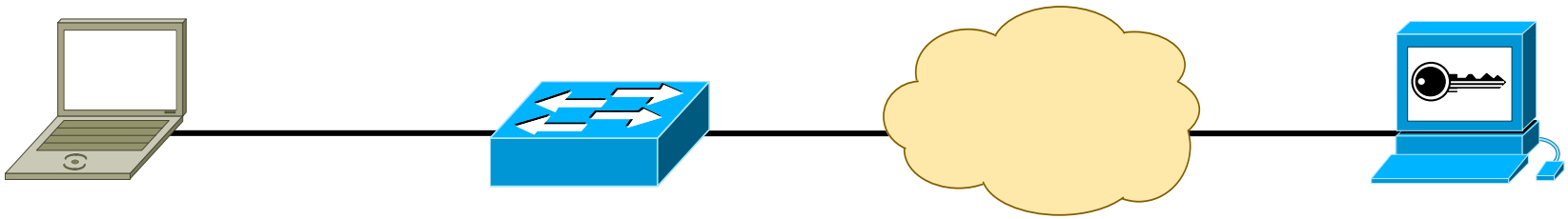
Do you have identification?

Yes, I do. Here it is.

Thank you. Here you go.



Wired Access Control Model



Client and Switch Talk 802.1x

Switch Speaks to Auth Server Using RADIUS

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

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.**

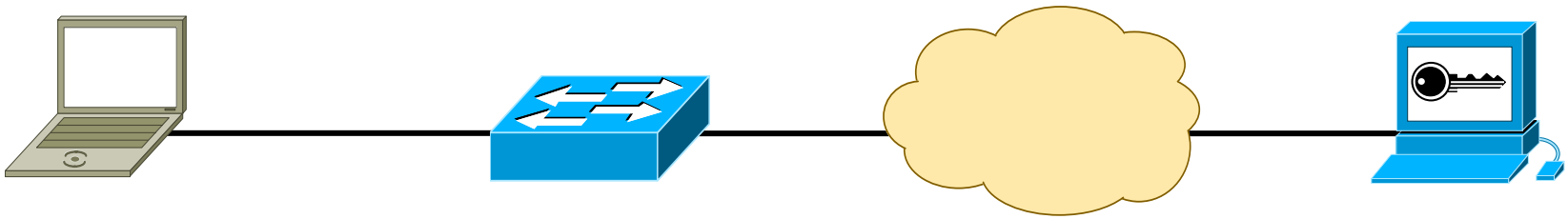
Some IEEE Terminology

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

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)

Wired Access Control Model

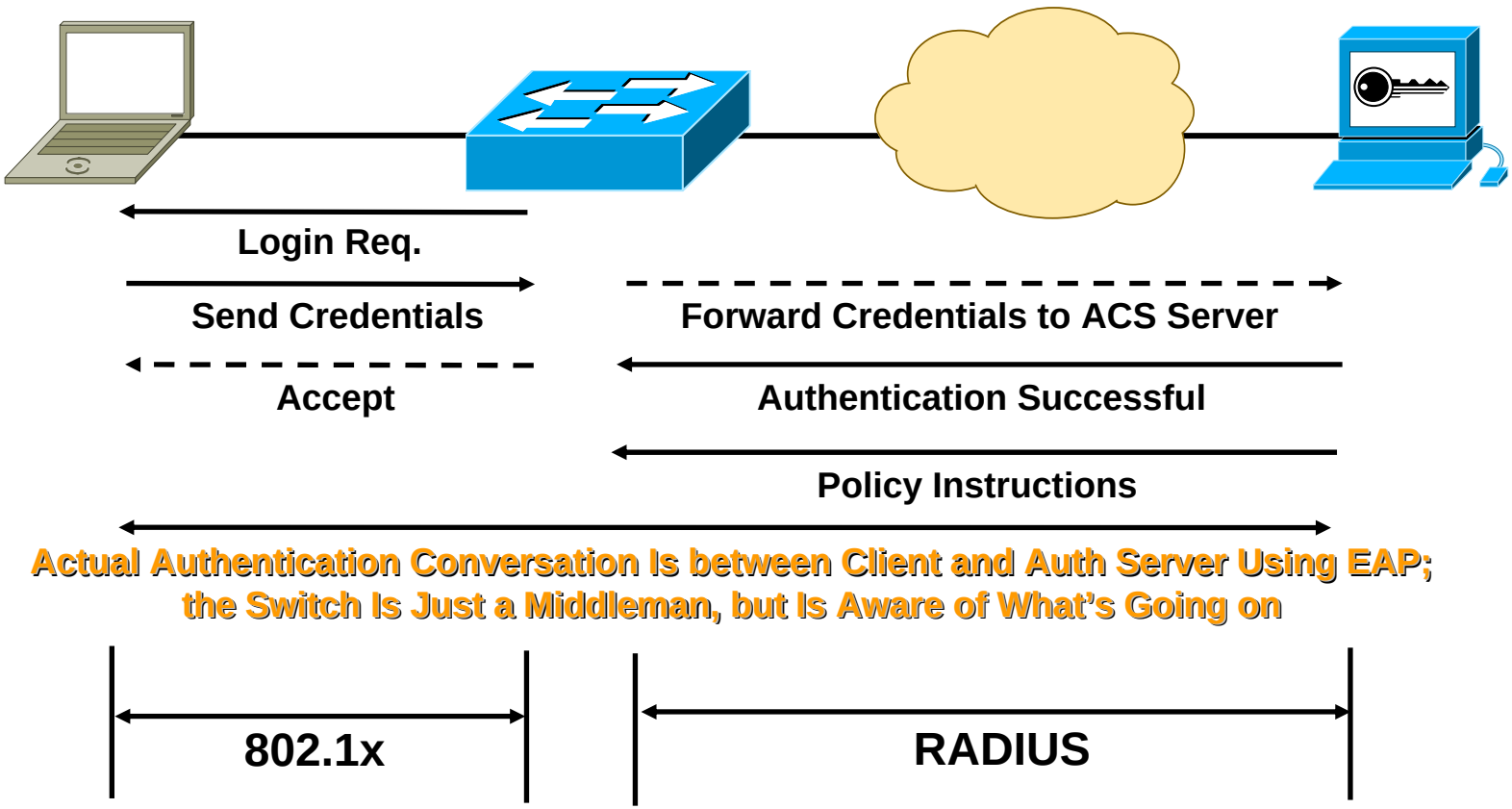


Client and Switch Talk 802.1x

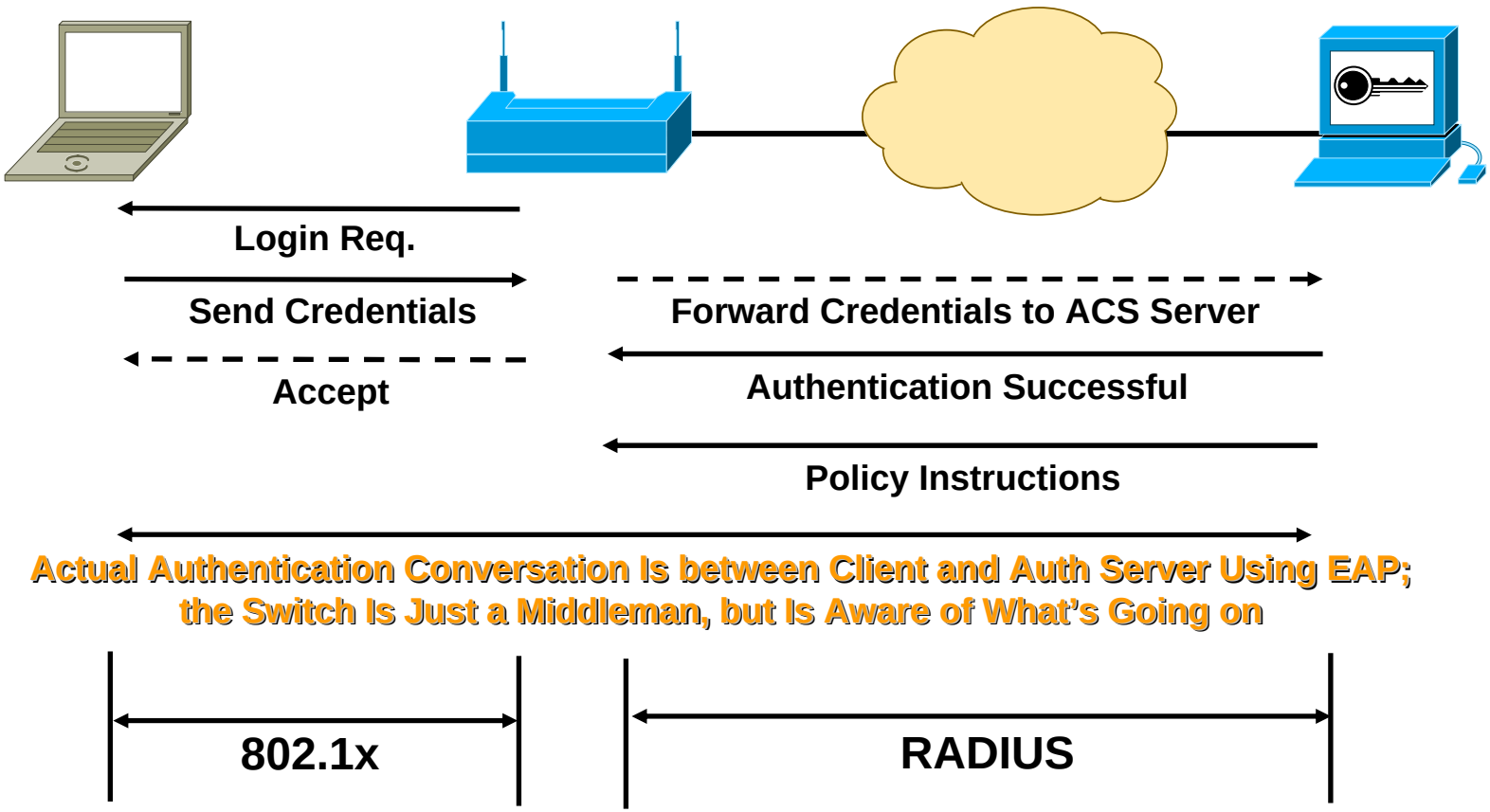
Switch Speaks to Auth Server Using RADIUS

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

A Closer Look…



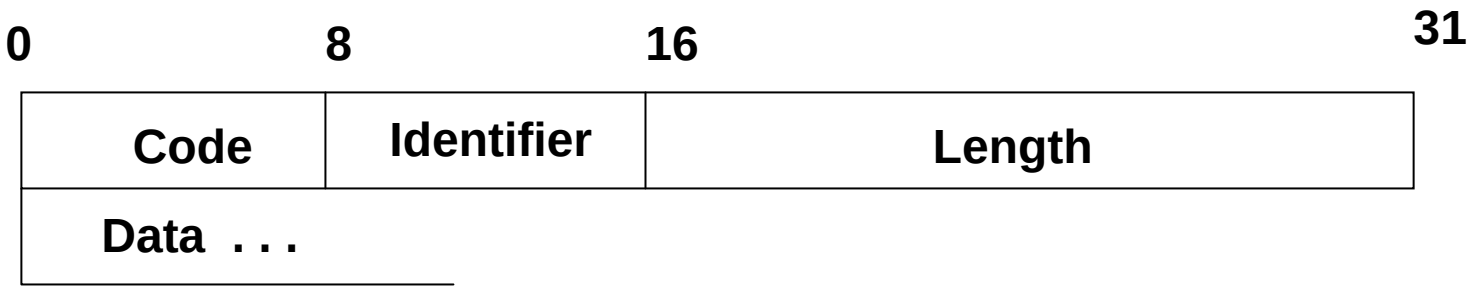
Wireless Access Control Model



What Is EAP?

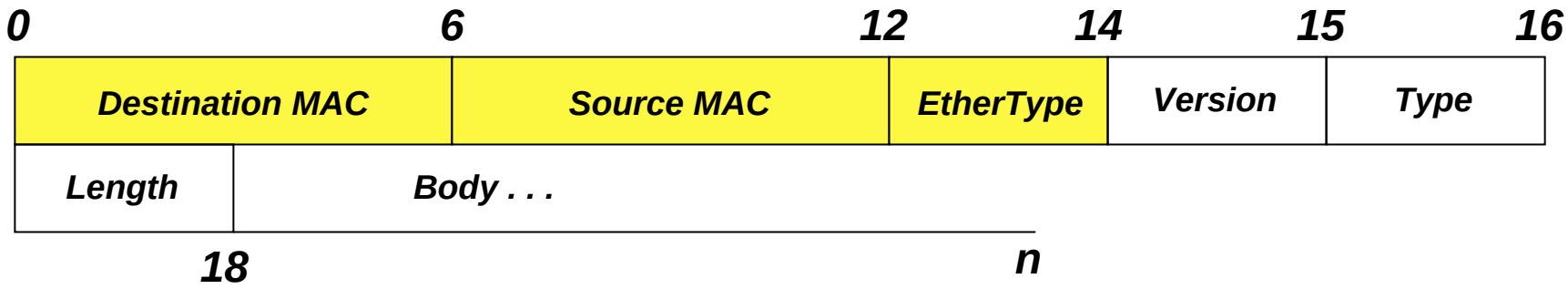
- EAP—The Extensible Authentication Protocol
- Defined in RFC 2284
- A flexible protocol used to carry arbitrary authentication information
- Typically rides on top of another protocol such as 802.1x or RADIUS (could be TACACS+, etc.)

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
EAP-MD5				
EAP-TLS				
EAP-MSCHAPv2				
LEAP				
PEAP				
EAP-GTC				
EAP-TTLS				

How Is RADIUS in 802.1x?

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

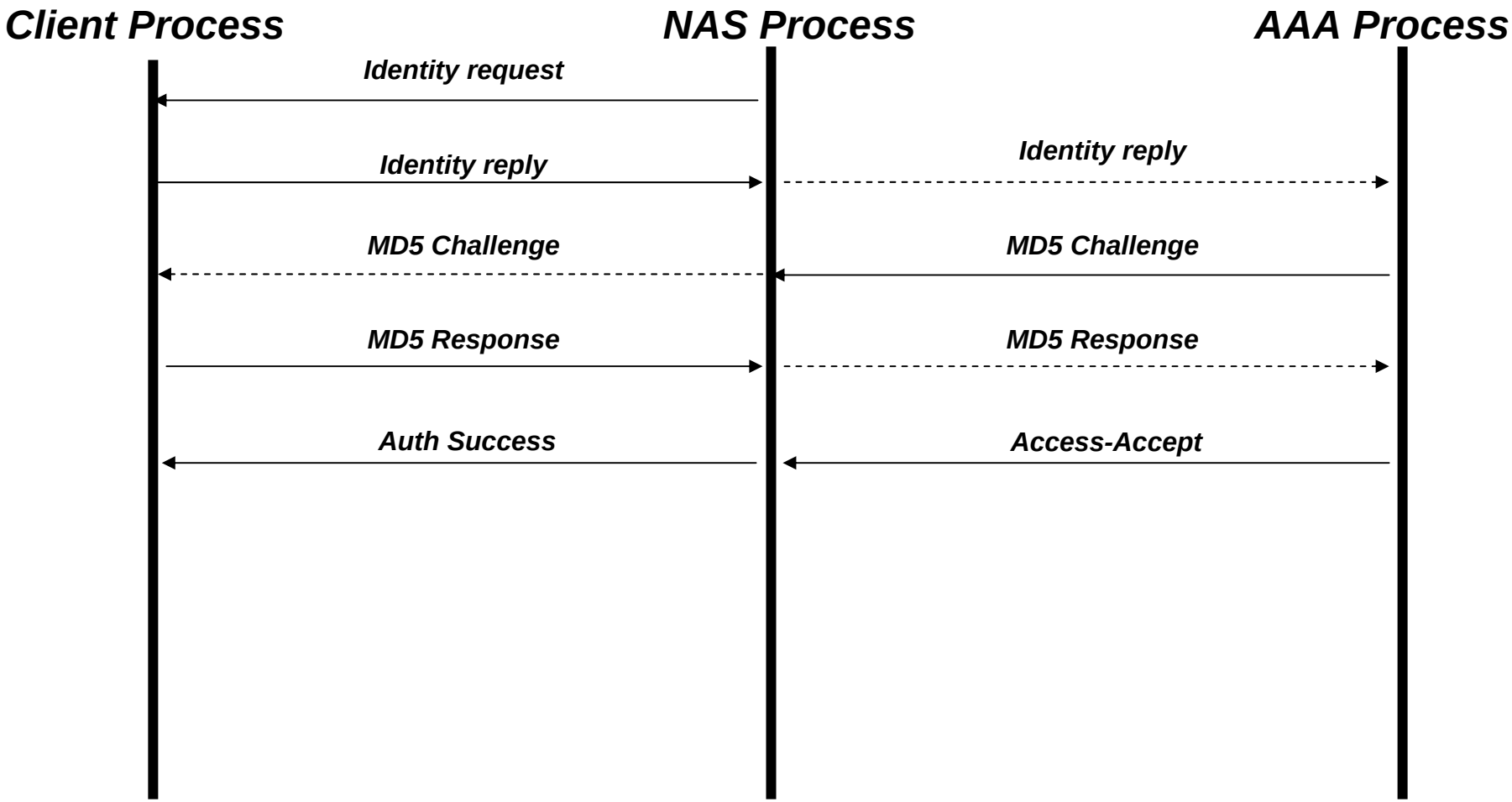
- **RADIUS is also used to carry policy instructions back to the authenticator in the form of AV pairs.**

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 accomodations 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

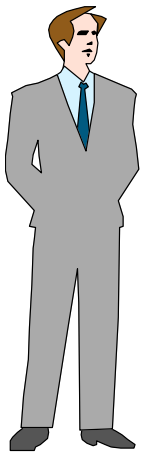
What Is a PKI Cert?

- 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

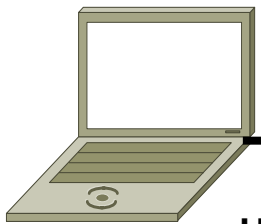
How Does a PKI Cert Work?

- 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

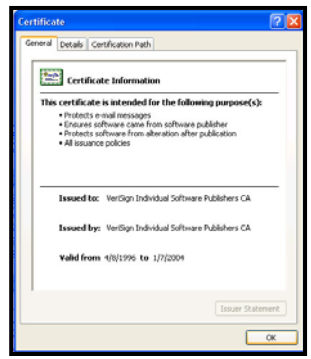
Using a PKI Certificate



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



Hello Authentication Server; I Have This to Validate My Identity



PKI Certs

- **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. Ie. 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

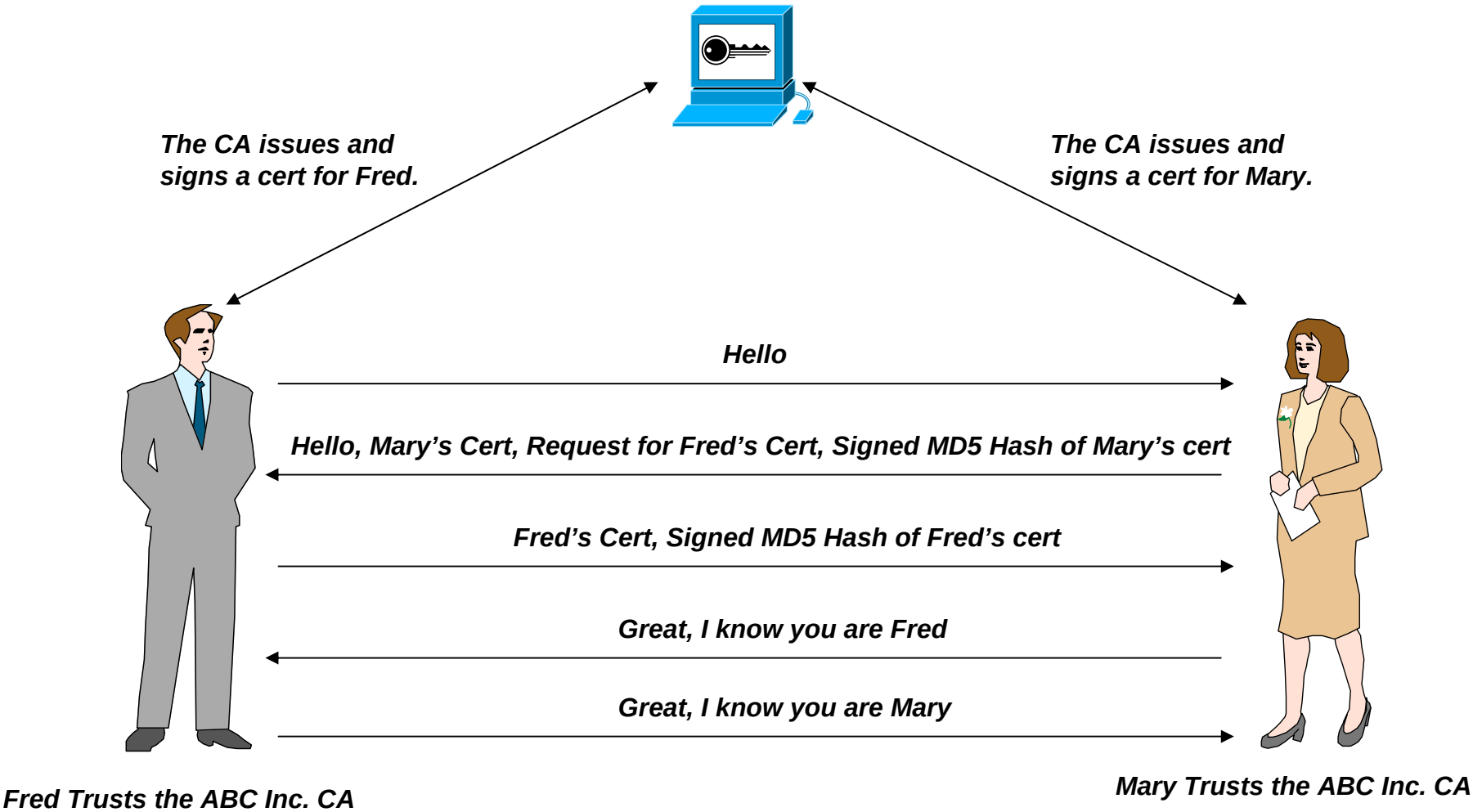
EAP-TLS Authentication

- **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 cetificates 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

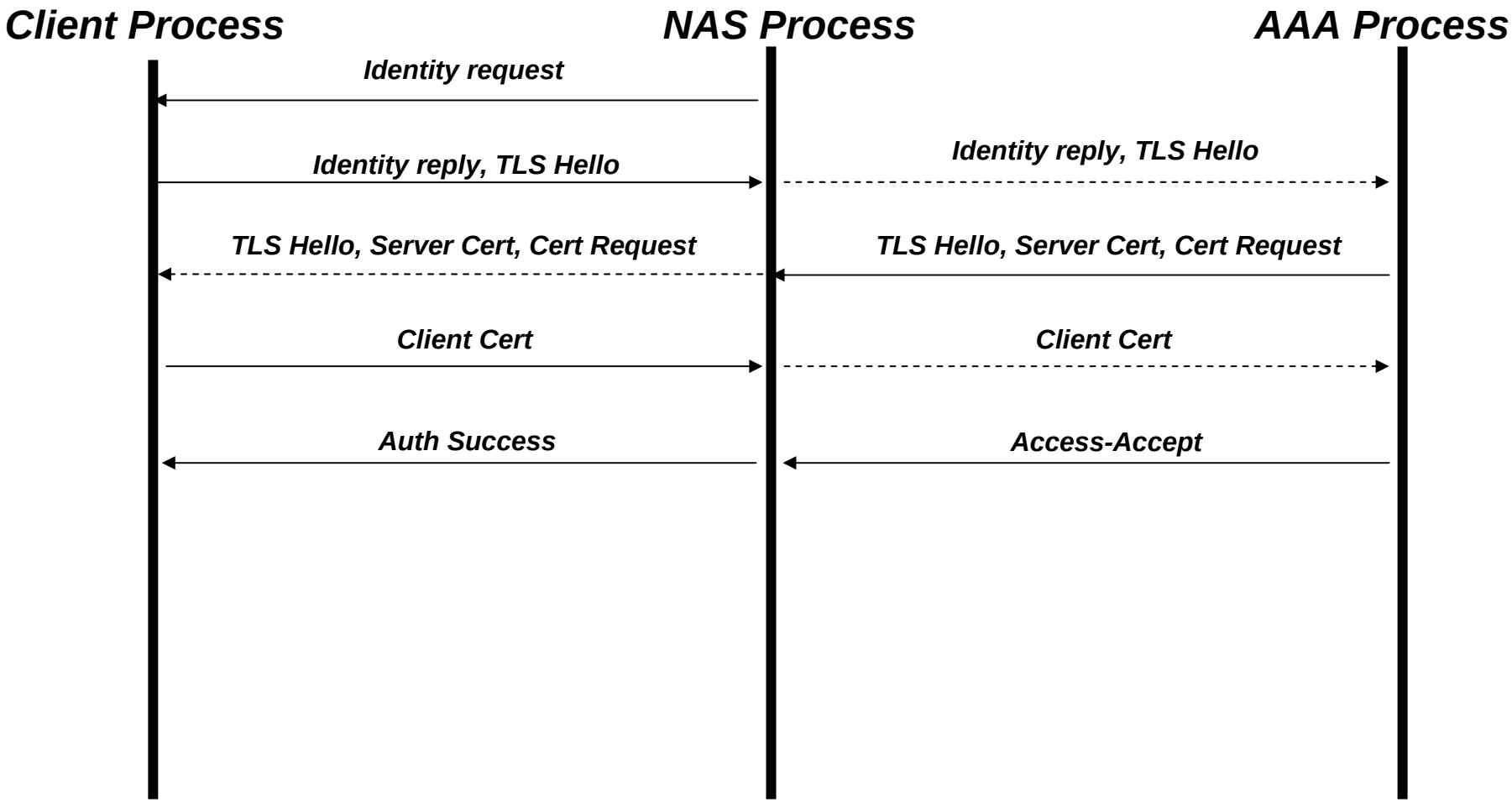
- **Is key distribution needed?**

  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 existance.
- Can be made a two factor system. Sometimes more.

Cons

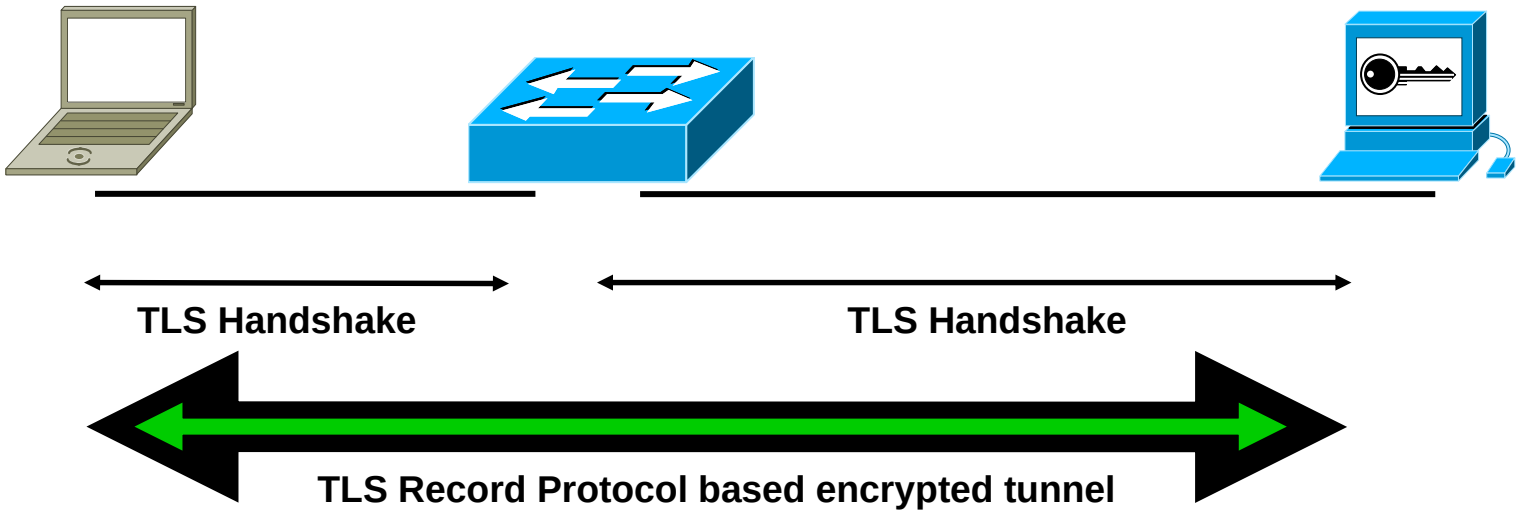
- Can be more complex to deploy – needs PKI.
- Computationally intensive.

Understanding PEAP

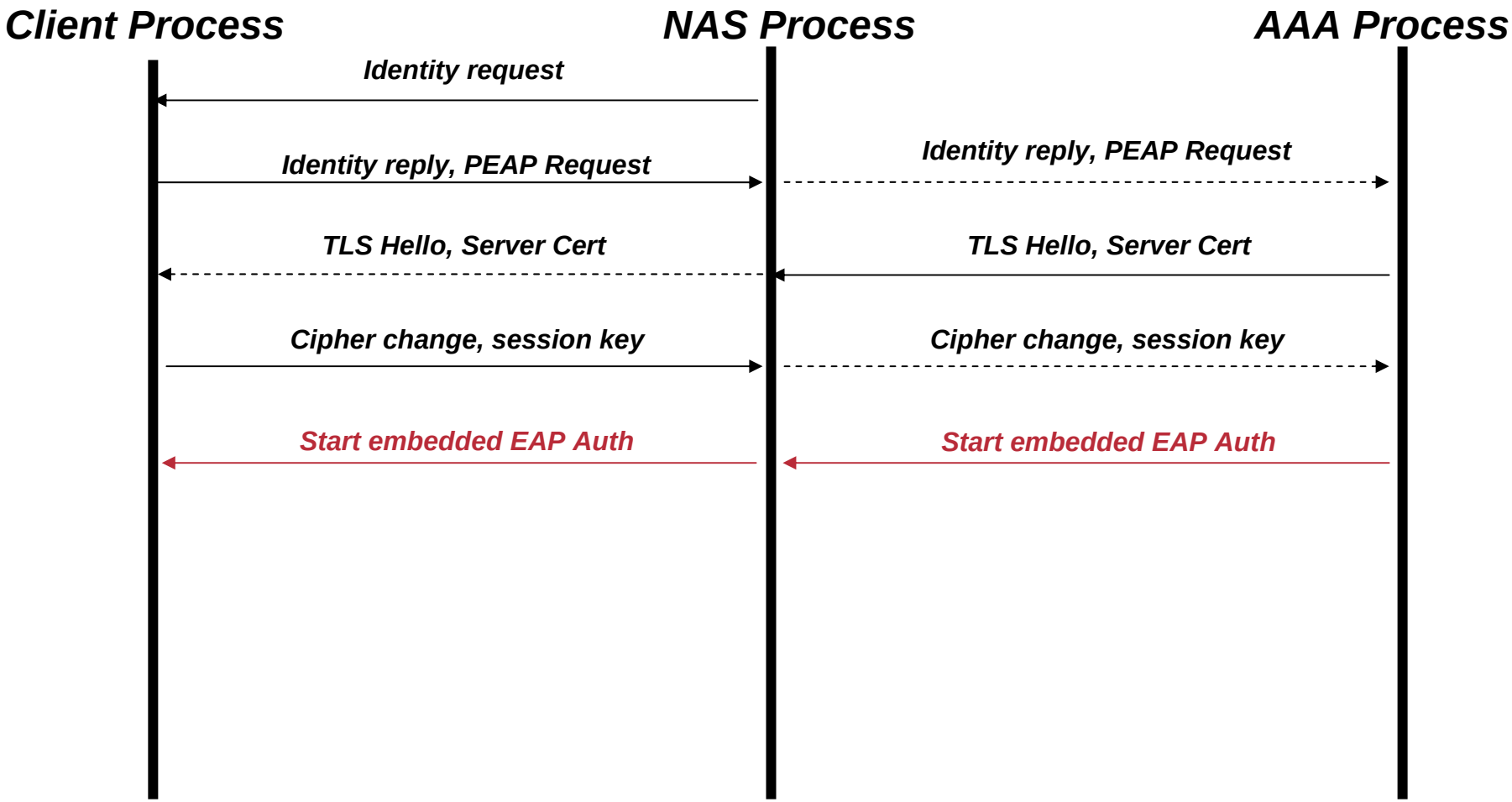
PEAP Authentication

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

Conceptual Overview of PEAP



PEAP Setup



PEAP Pros & Cons

Pros

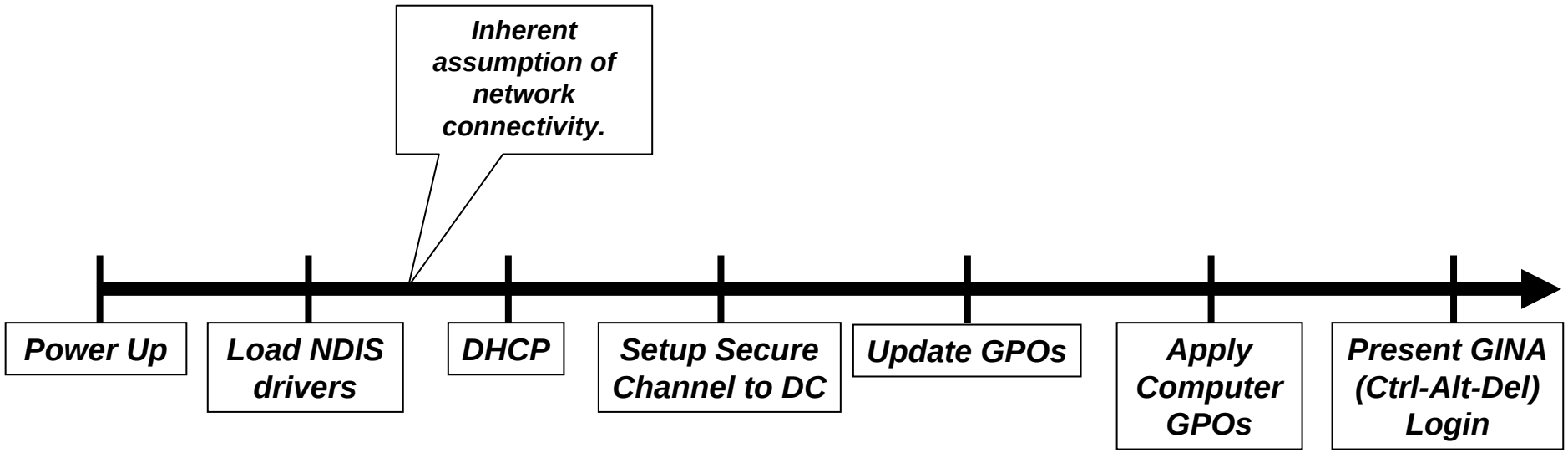
- Highly protected authentication using encrypted tunnel.
- Flexible credential options with multiple EAP sub-types.
- Doesn’t require client certs.

Cons

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

Understanding Microsoft Environments

Windows Boot Cycle Overview



Microsoft & Machine Authentication

- **What is Machine Authentication?**

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

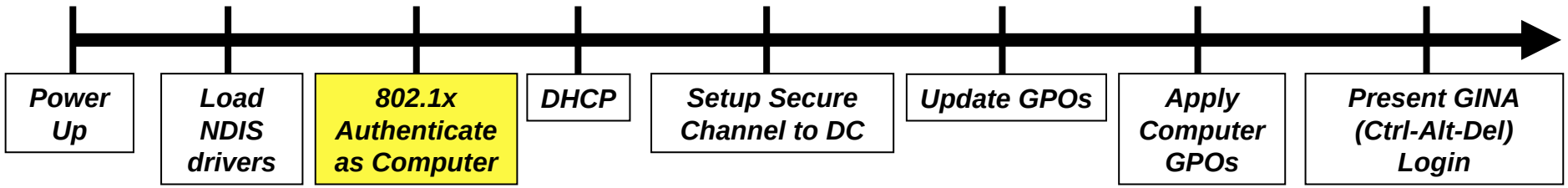
- **What is it used for?**

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

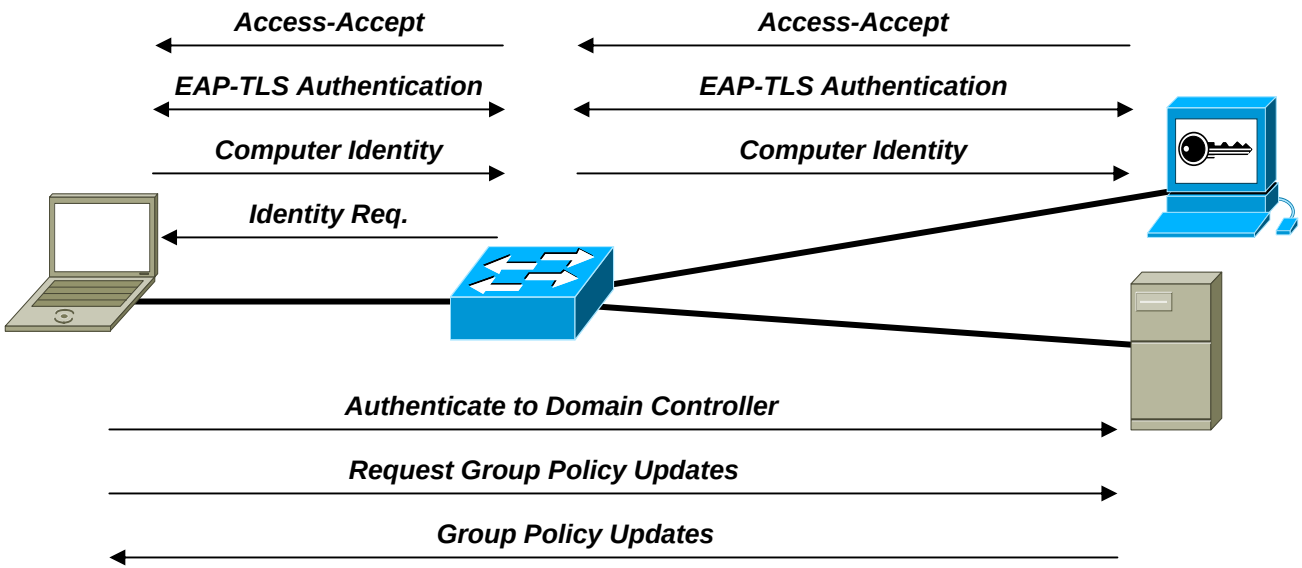
- **Why do we care?**

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

Windows Machine Authentication



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.

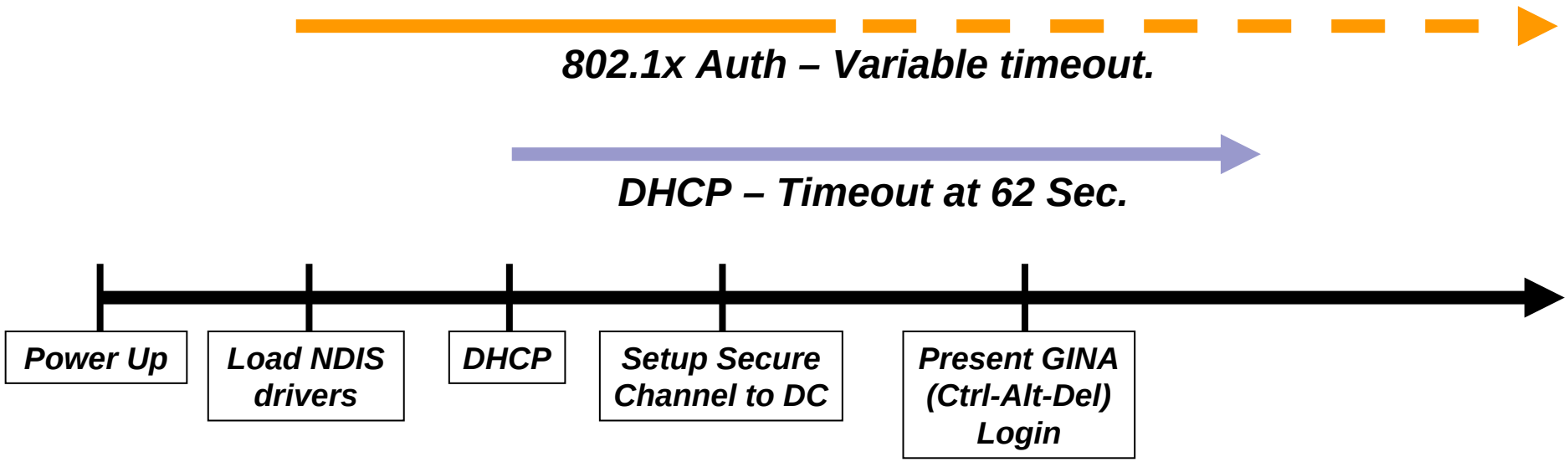
  No machine authentication taking place at all – be careful, this breaks group & system policies.
- Authentication by user and machine.

  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



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.

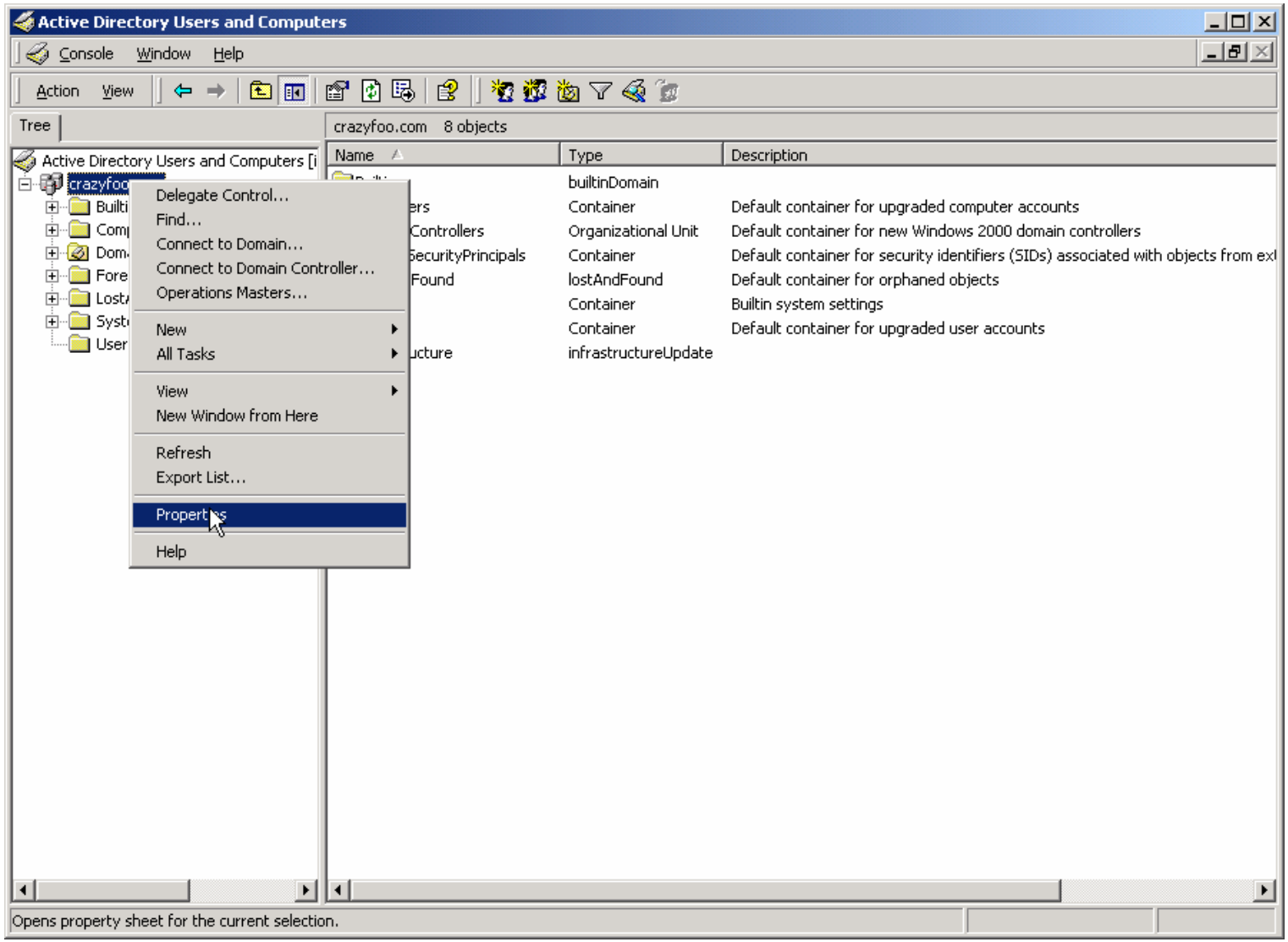
Machine Auth Using PEAP

- 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.

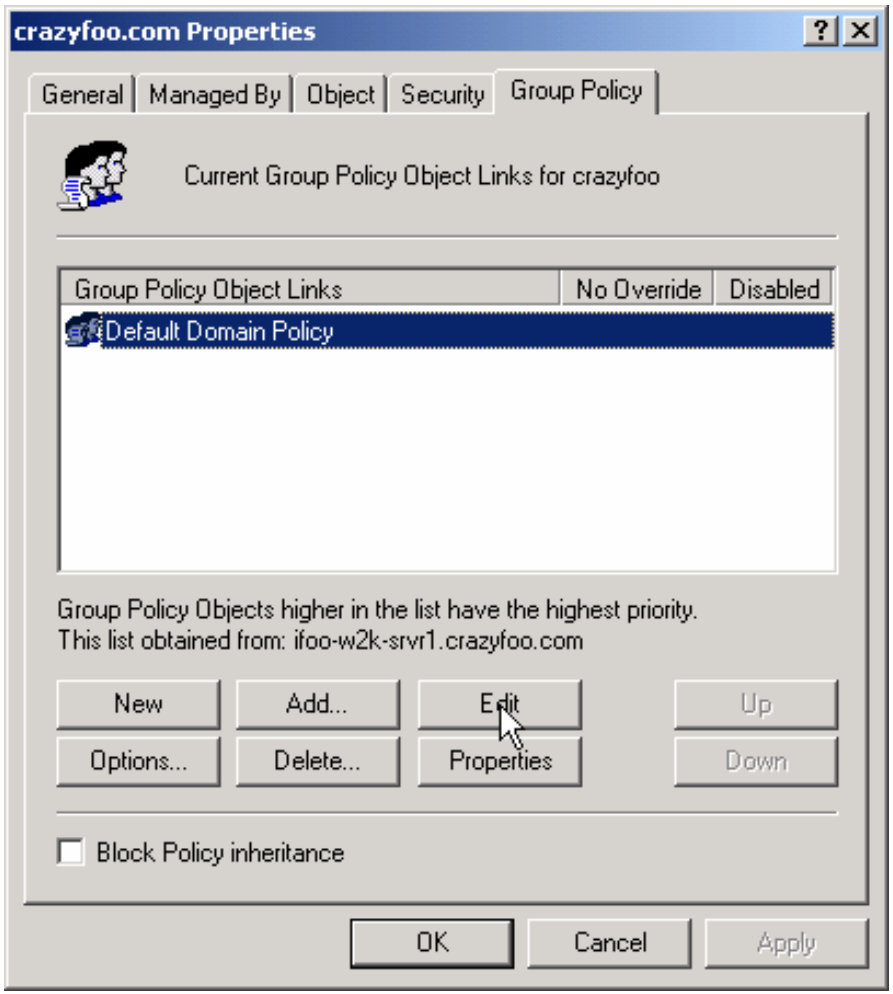
Machine Auth Using EAP-TLS

- **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.**

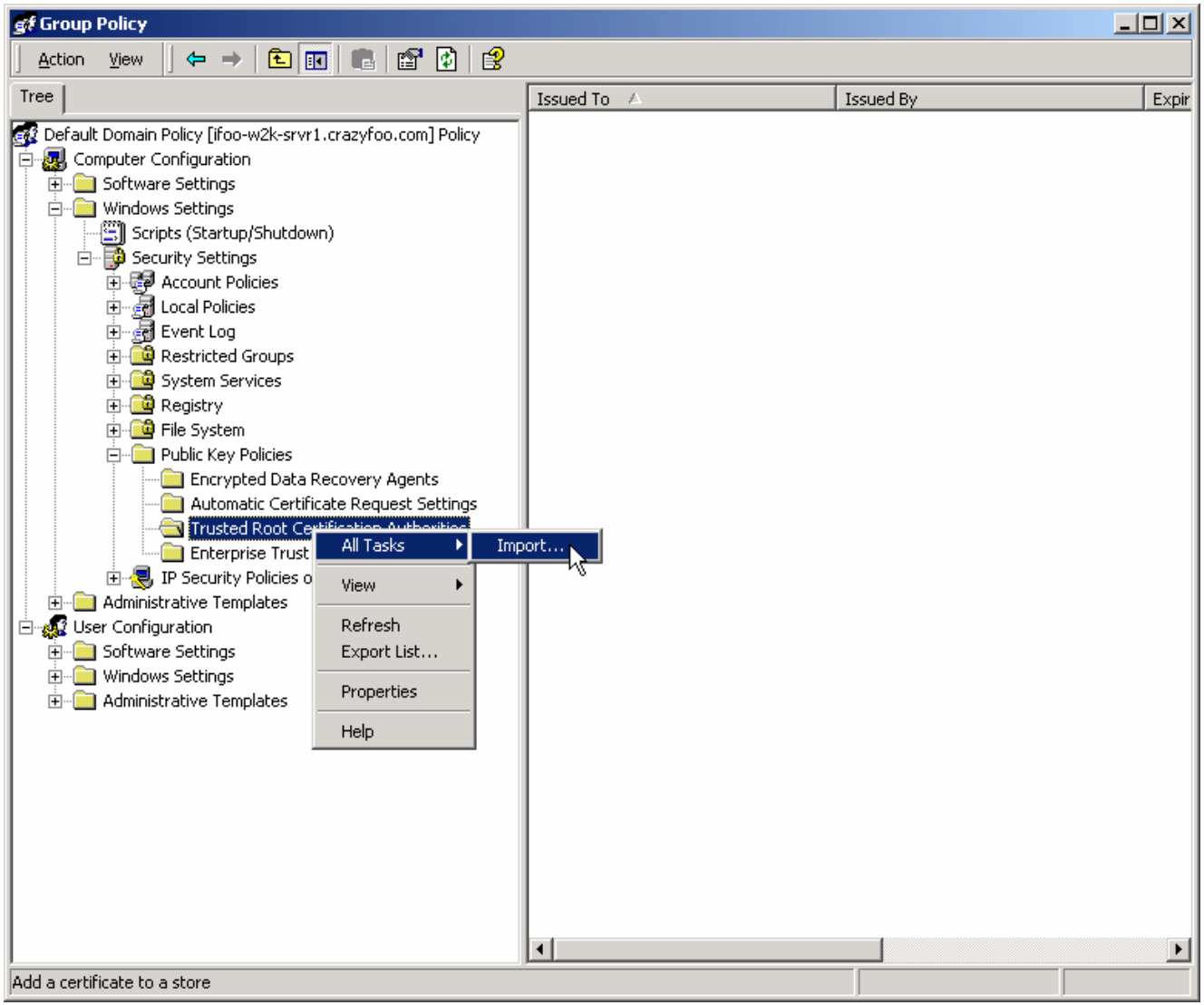
Using GPOs To Control Computer Certs



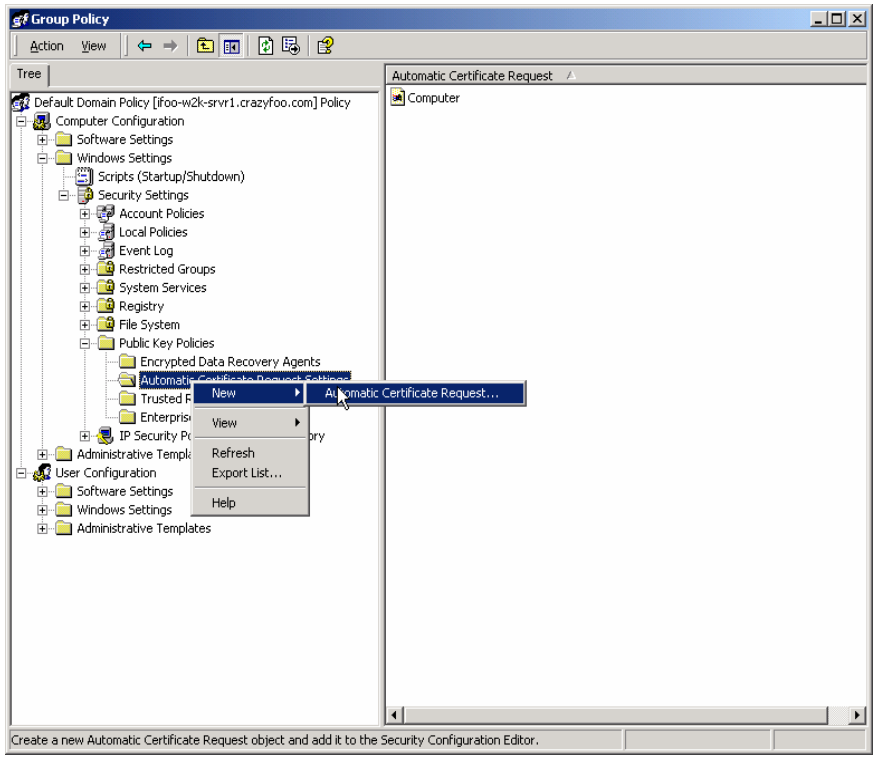
Using GPOs To Control Computer Certs



Using GPOs To Control Computer Certs



Using GPOs To Control Computer Certs



Machine Auth with “Dial-in Permission” Checking

- 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:

```
ldifde -i -f %systemRoot%\system32\mac8021x.ldf -c DC=DN DC=domain,DC=com
```

- See Microsoft KnowledgeBase Article #306260 for more details.

Identity Based Policy Enforcement

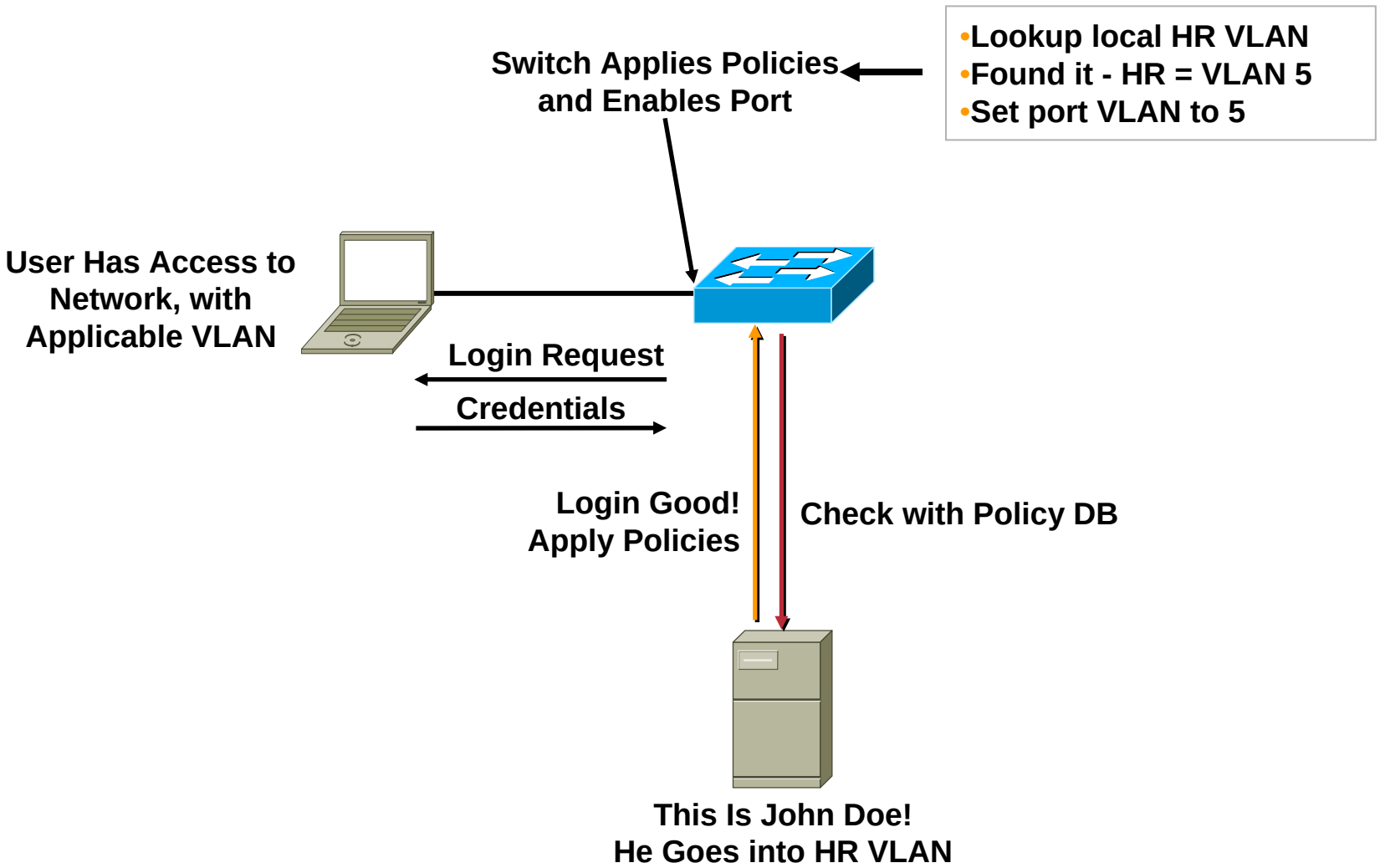
Authorization

- **Authorization is the embodiment of the ability to enforce policies on identities.**
- **Typically policies are applied using a group methodology – allows for easier manageablitiy.**
- **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

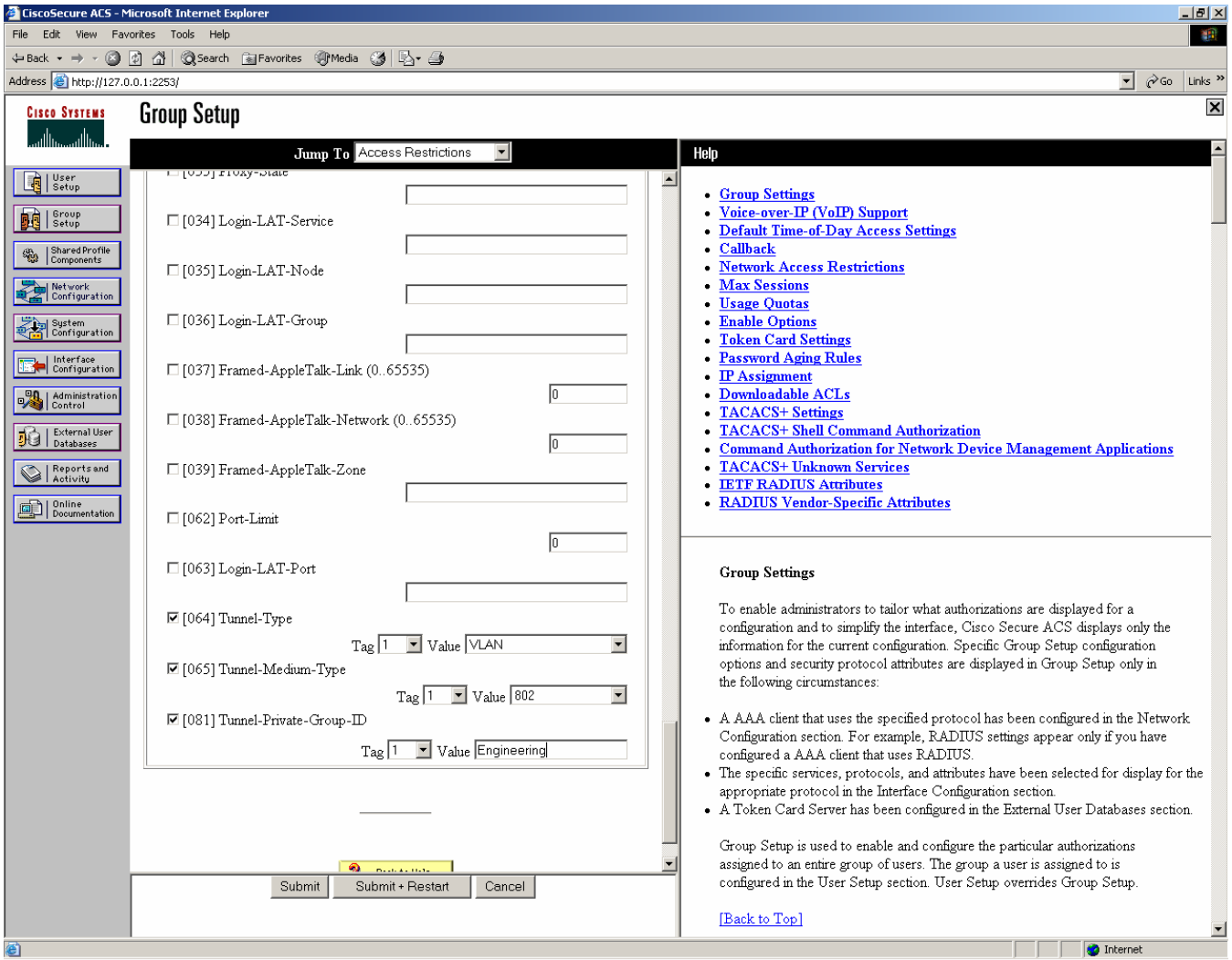
- **RADIUS AV-Pairs used to send back VLAN configuration information to authenticator.**
- **AV-Pair usage for VLANs is IEEE specified in the 802.1x standard.**
- **AV-Pairs used – all are IETF standard:**

  [64] Tunnel-Type – “VLAN” (13)

  [65] Tunnel-Medium-Type – “802” (6)

  [81] Tunnel-Private-Group-ID - <*VLAN name*>

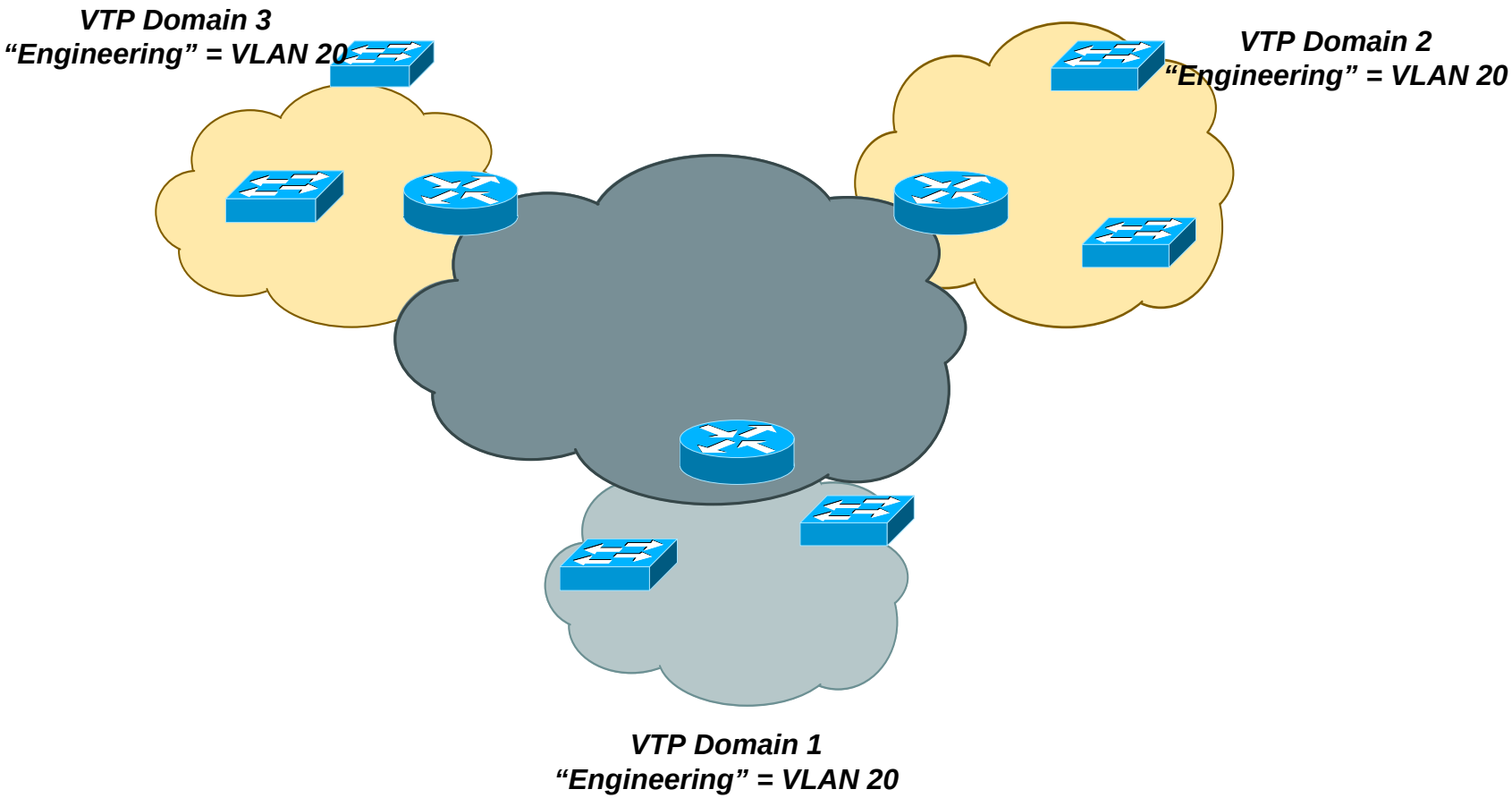
ACS Configuration
Group Policy Configuration – VLAN Assignment



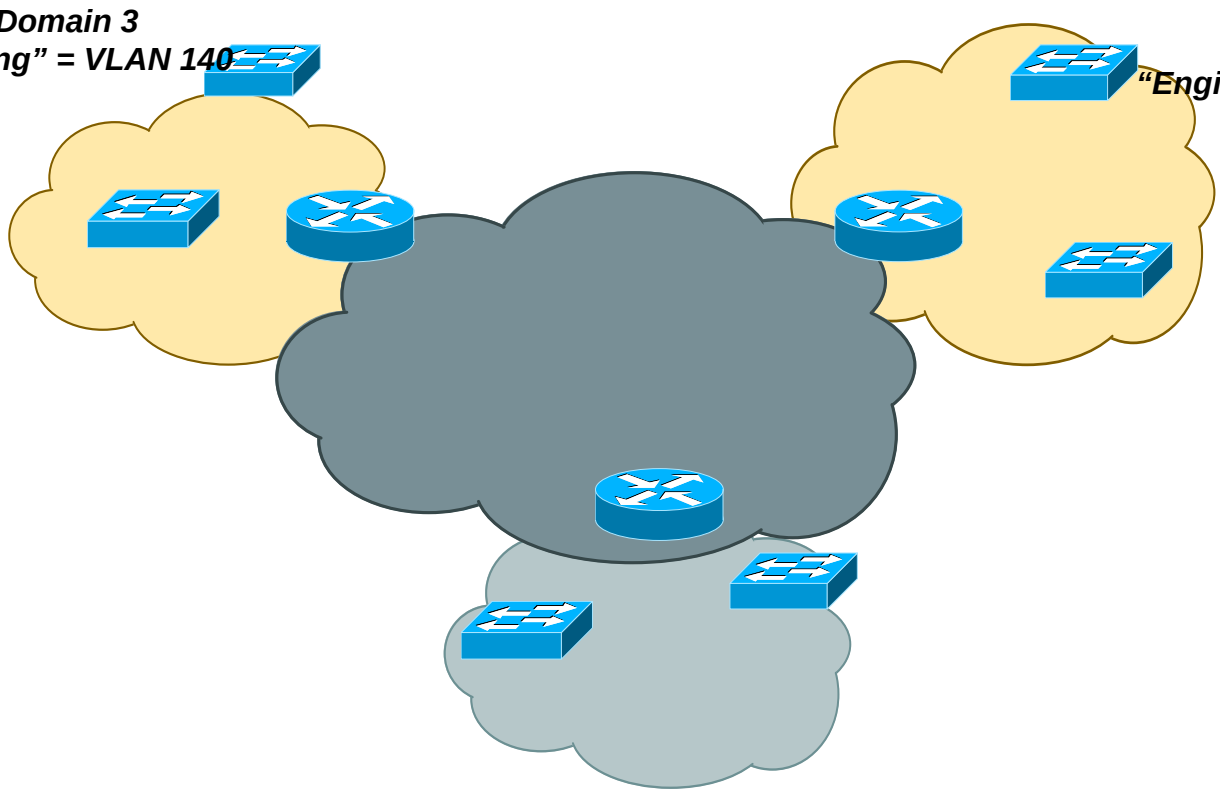
Dynamic VLAN Deployment Recommendations

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

Dynamic VLANs – VLAN ID Re-Use



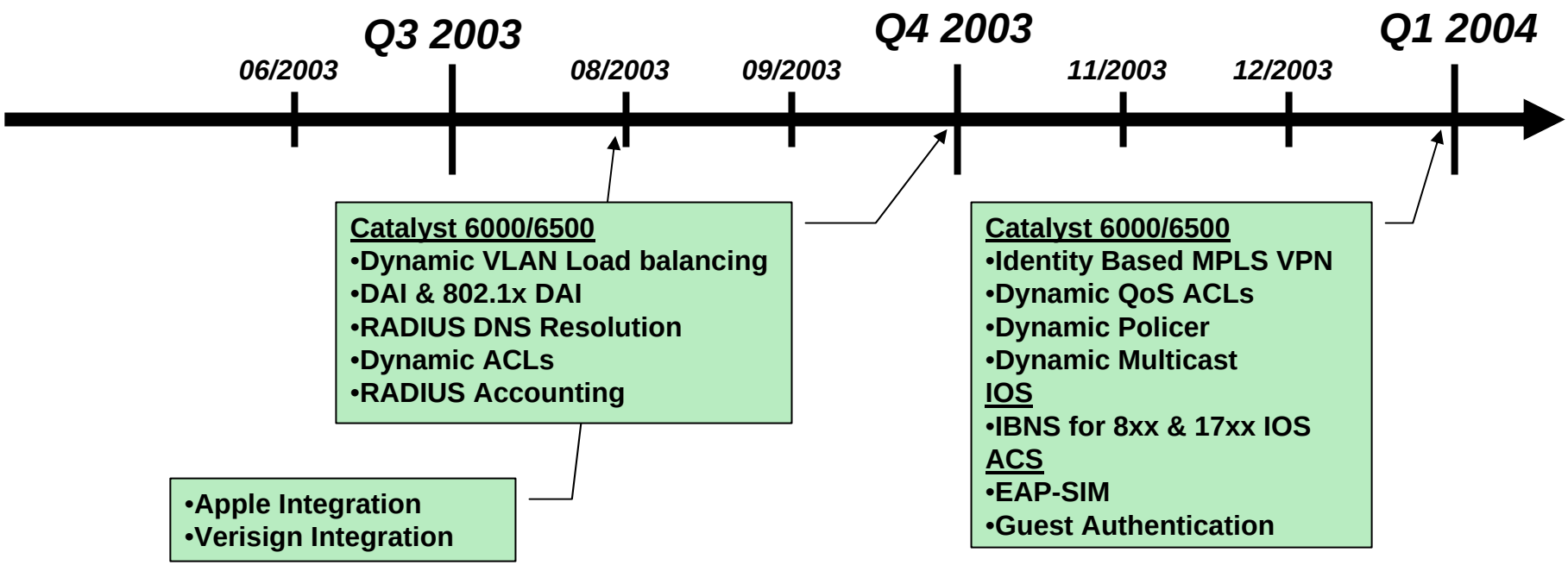
Dynamic VLAN – Unique VLAN IDs



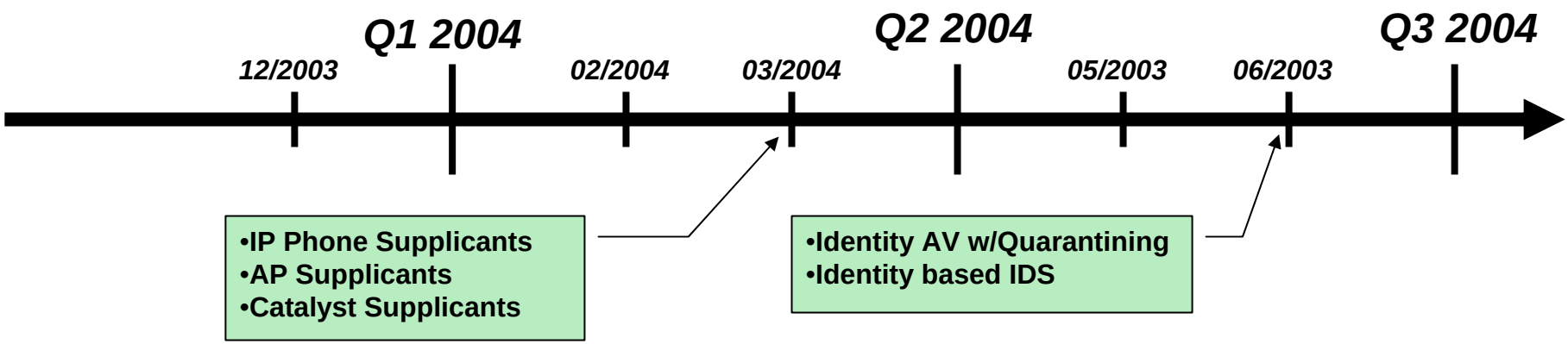
Future Policies via RADIUS

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

IBNS Roadmap – 6 month window



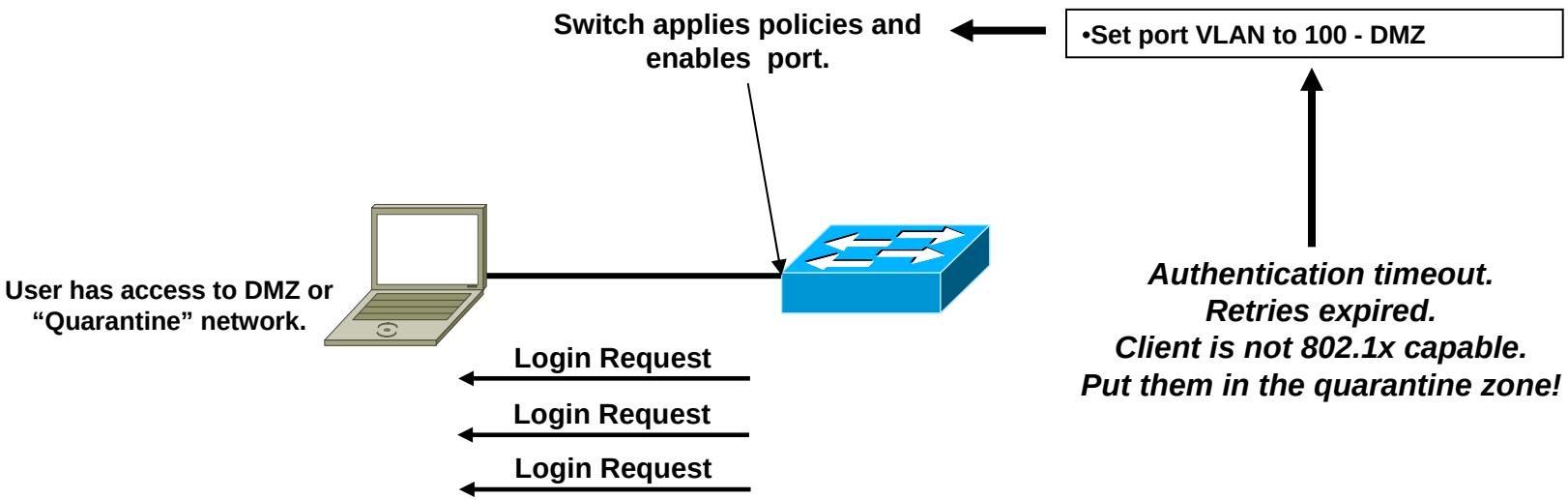
IBNS Roadmap – 12 month window



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	?	

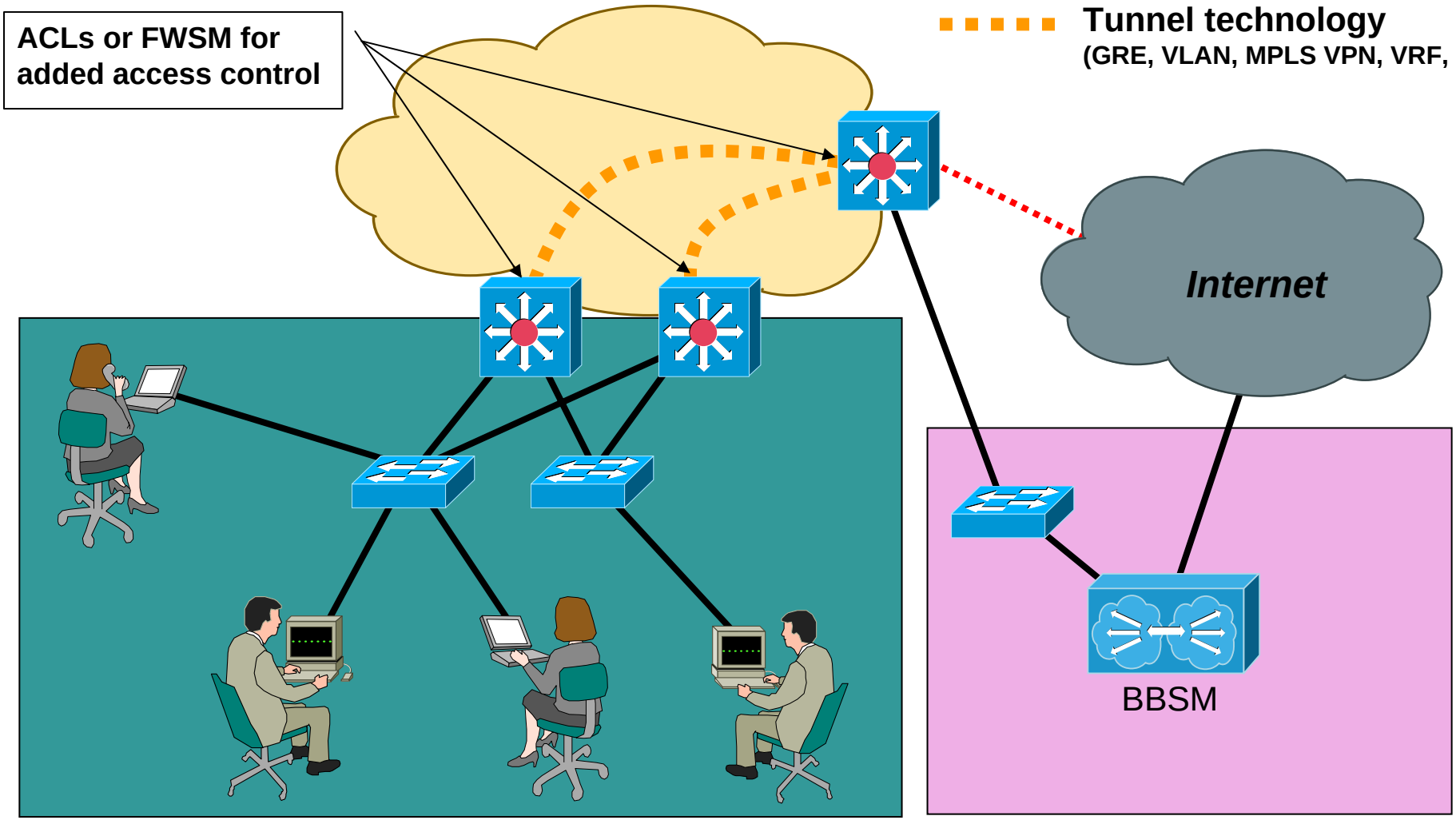
Guest Access Scenario 2

- **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



Migrating to 802.1x

Migration Strategies – 1st Method

- **Requirements: All clients are 802.1x capable.**

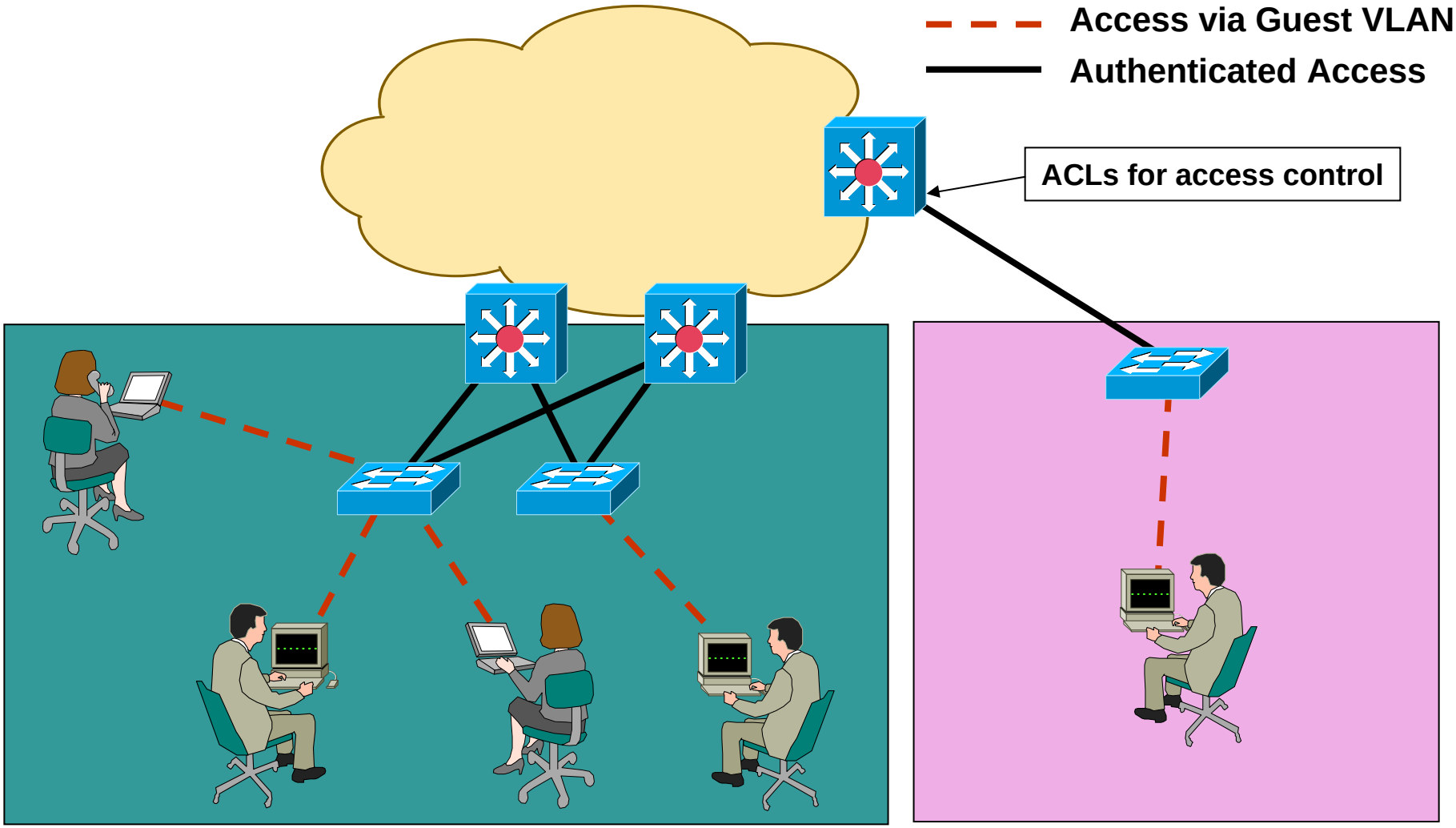
1. **Fully patch & migrate clients first.**
2. **If supporting Dynamic VLANs, build out VLAN support structure.**
3. **Enable authentication in sections of the network in modular windows.**

Migration Strategies – 2nd Method

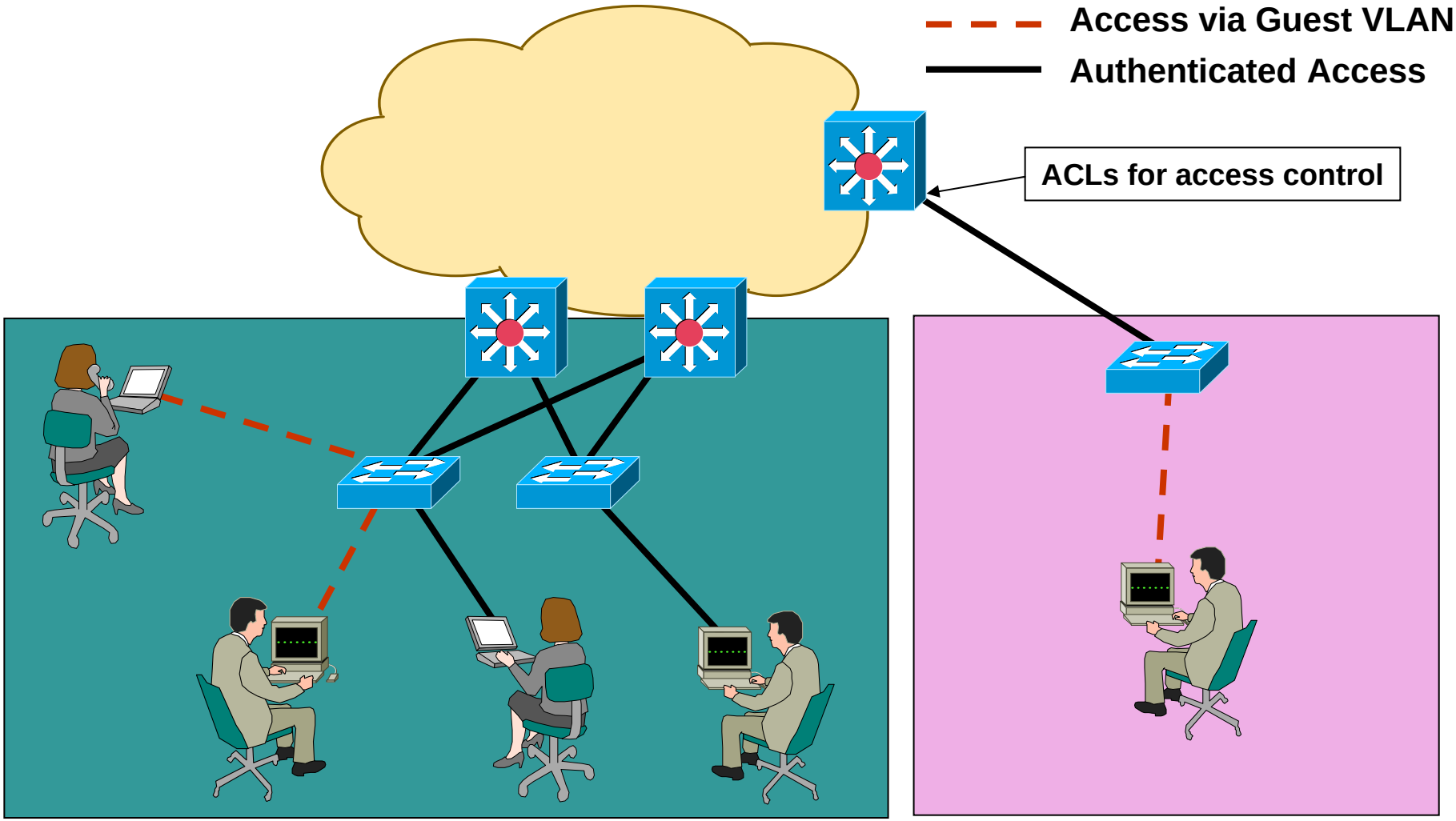
- Challenge: Not all clients are 802.1x capable.

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.

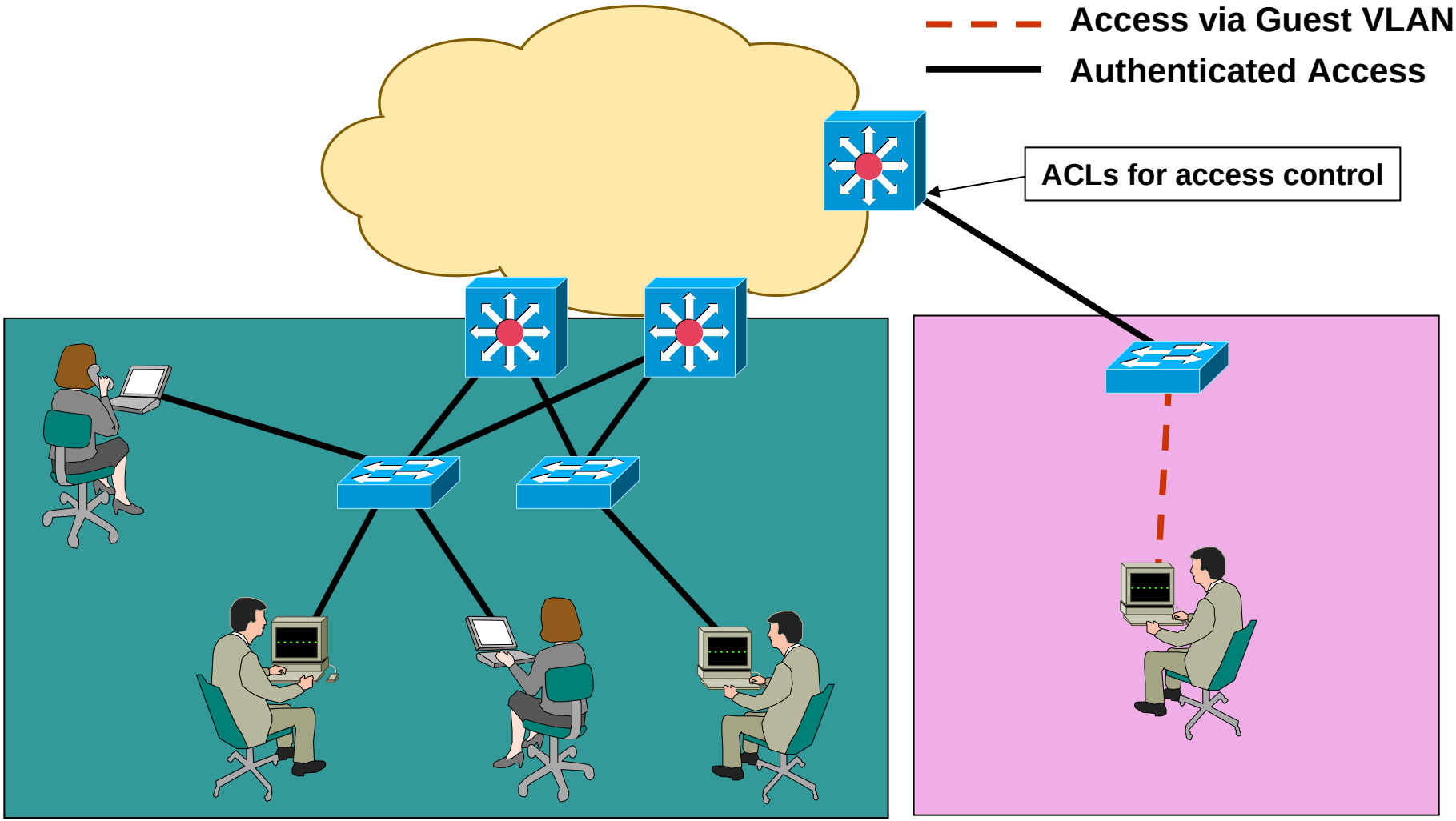
Initial Client Migration Stage – Majority Guest Access



Transient Client Migration Stage – Mixed Access



Completed Migration – Fully Authenticated Access



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

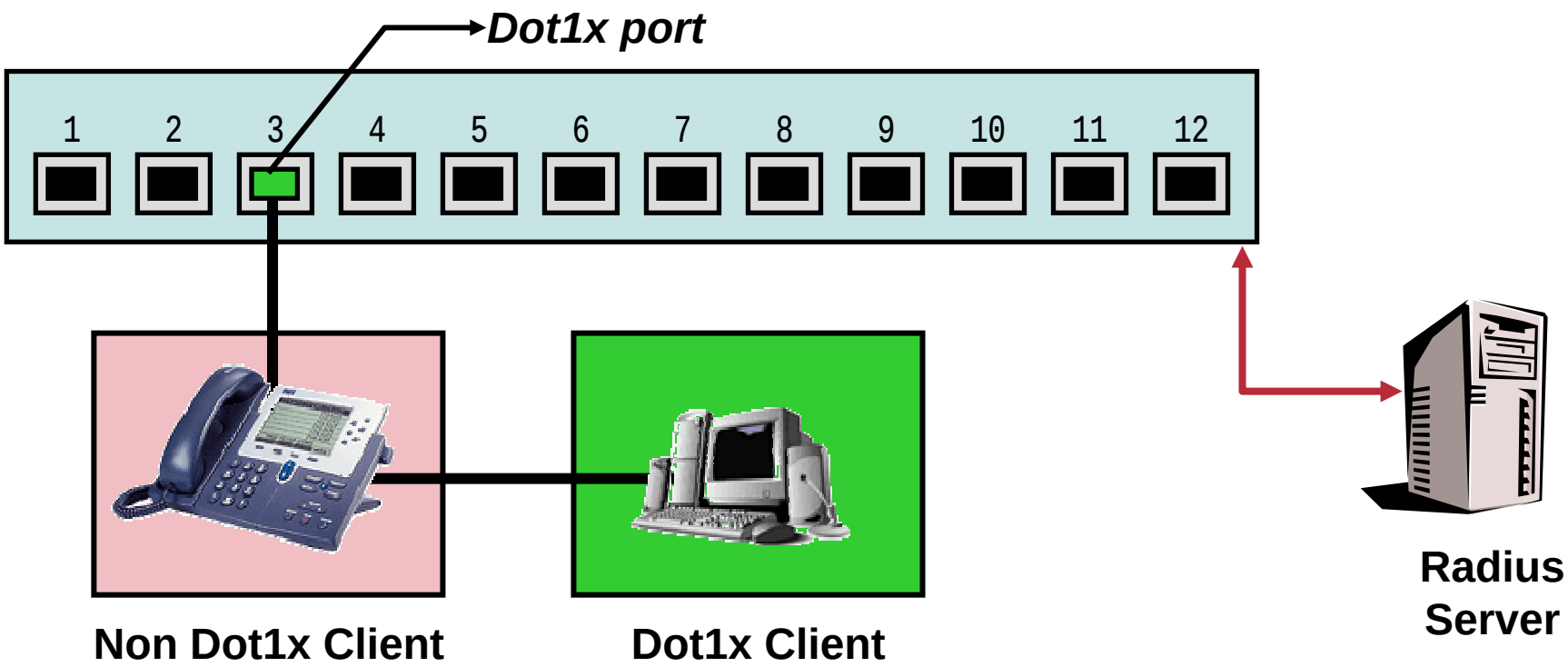
- **Two phases of VoIP and 802.1x support.**

  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.

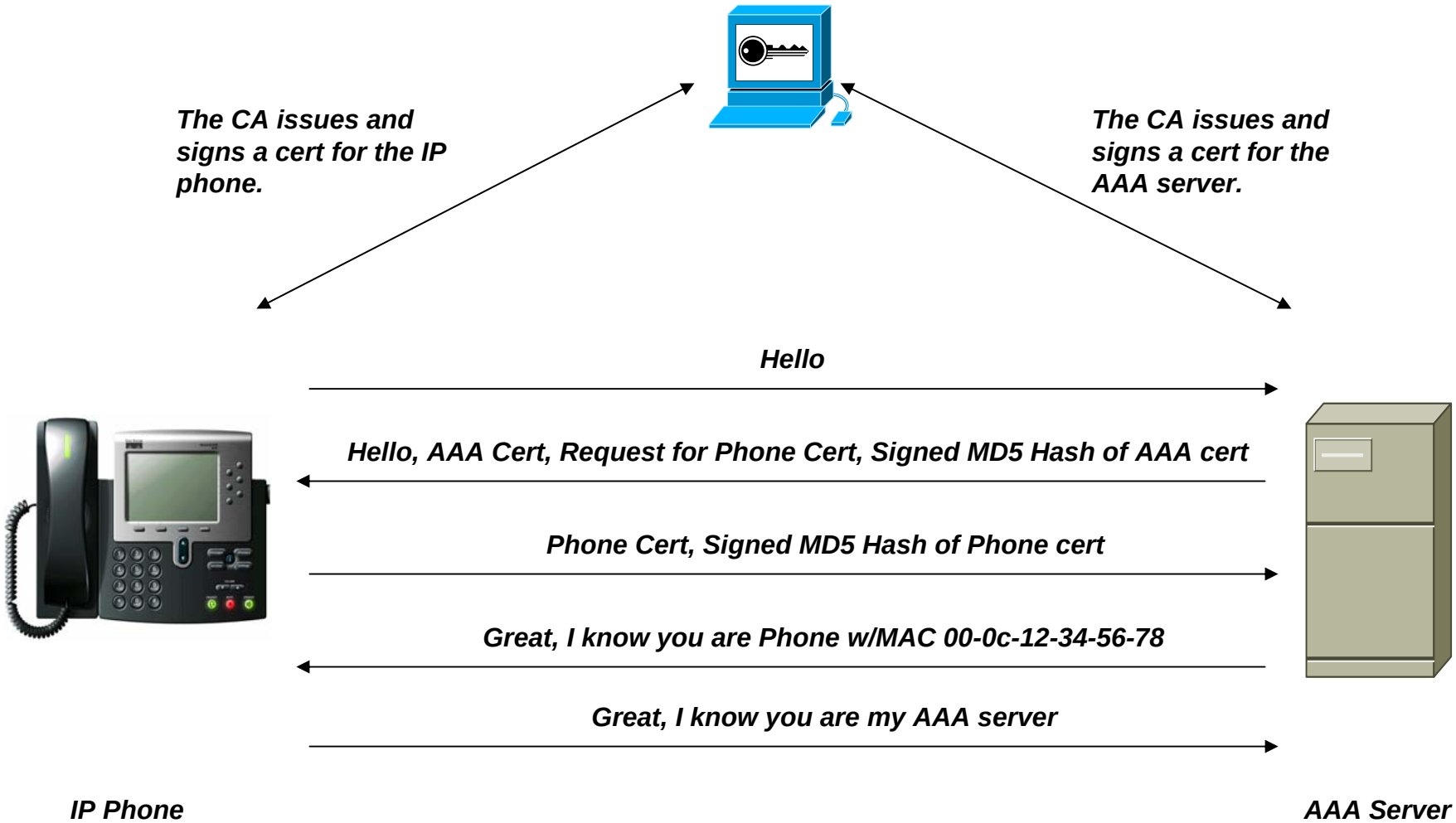
  802.1x supplicants in IP phones – Committed for next gen phones (7965) work in progress for existing phones (7960) – not yet committed. Phones will act as passthrough for PVID authentication.

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



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 3rd Party (MeetingHouse)**
- **Linux - Open Source or 3rd Party (MeetingHouse)**

  http://www.open1x.org
- **Solaris – Open Source or 3rd 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

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 Networking Service

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

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 3550/2950/375

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**

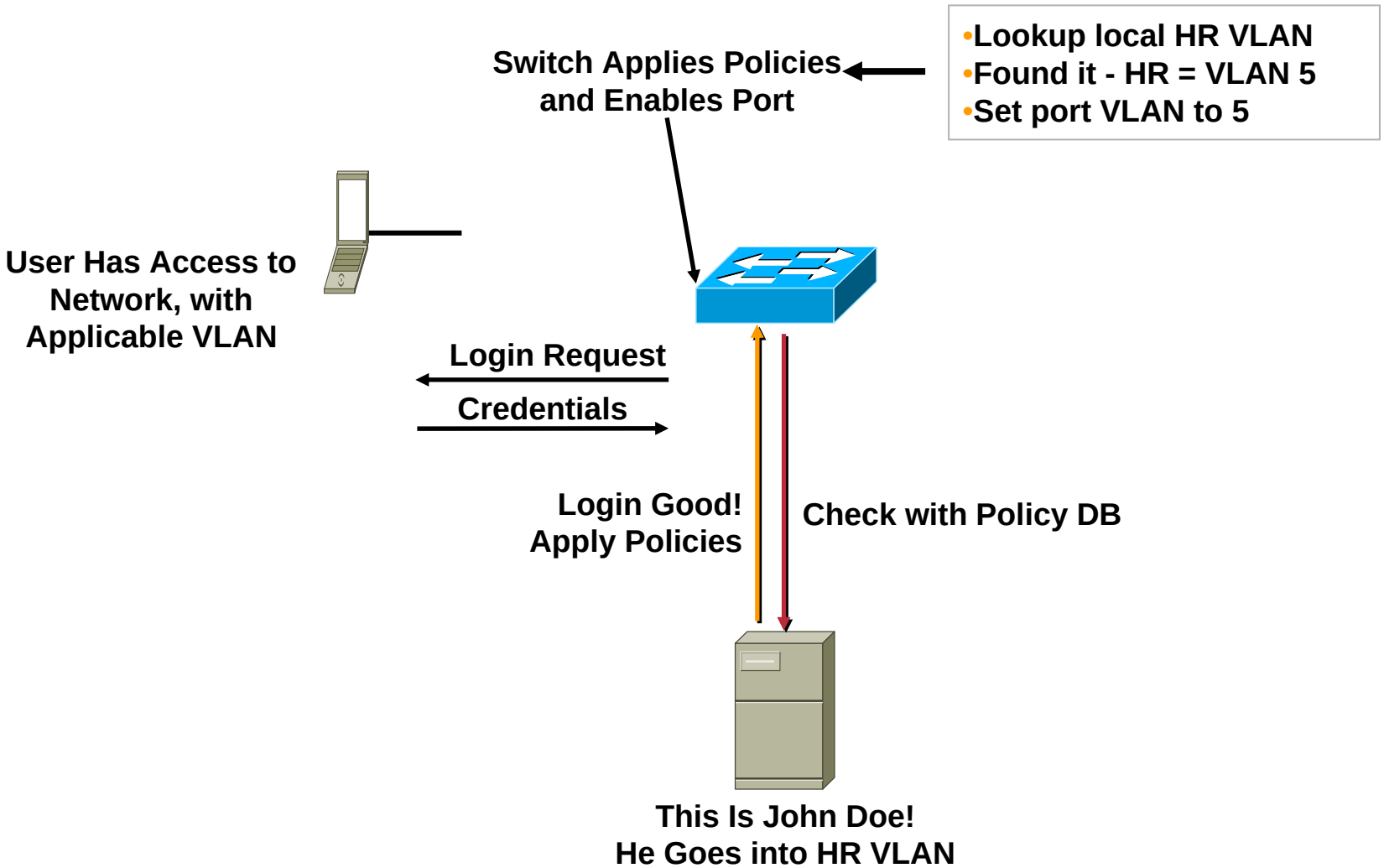
Identity Based Network Services (IBNS)
End-to-End Architecture

Products	Basic 802.1x	VVID Support	Dynamic VLAN Assignment	Guest VLAN and/or DHCP Assignment	Per-User QoS/Security Policies
2950	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
3550	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
4000/4500	CatOS 7.2.1+	Clearwater Release (Q3'02)	CatOS 7.2.2+	Clearwater Release (Q3'02)	???
6500	CatOS 7.2.1+ IOS (Achilles)	Clearwater Release (Q3'02)	CatOS 7.2.2+	Clearwater Release (Q3'02)	QoS – Q4CY2003 ACL – Not Supported
Aironet AP (Authenticator)	11.06	N/A	Twin Peaks (Q4 '02)		
Cisco 83x	CC in late Sept. '02			CC in late Sept. '02	
CiscoSecure ACS	V3.0 – Wireless PKI support for 802.1x	V3.1 – Catalyst support V3.1 – 802.1x and EAP	V3.0	N/A	
IP Phones	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

Cisco.com

- **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 3rd party (ie. Verisign) Certificate for ACS**

Basic Steps to Configuring 802.1x

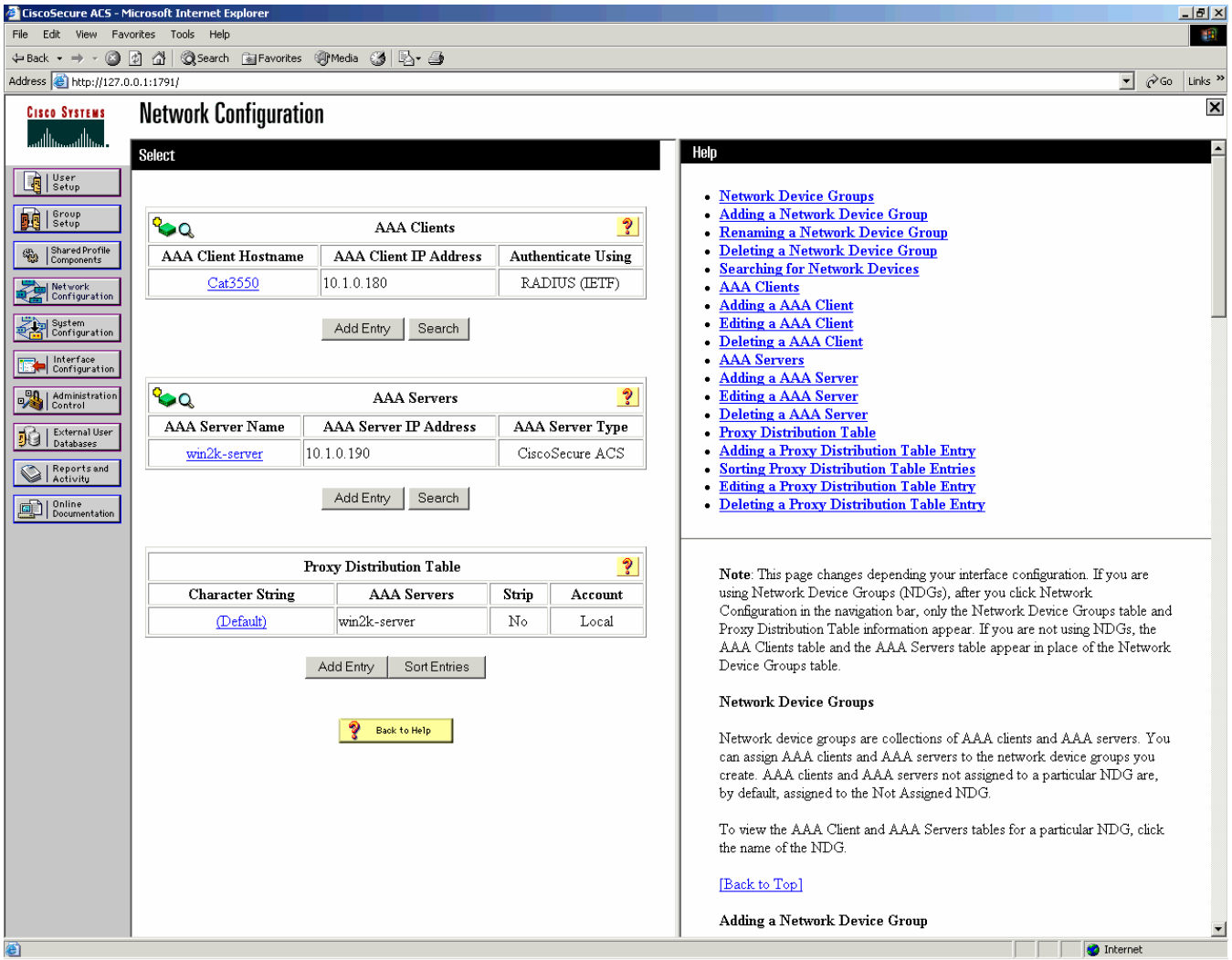
1. Configure the Authentication (RADIUS) Server
   - Add the relevant NAD.
   - Configure the required EAP Method.
   - Configure external DB access.
   - Configure policies and group mappings.
   - Create accounts.
2. Configure the Authenticator
   - Add the Authentication (RADIUS) Server.
   - Configure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

Authentication Server Configuration

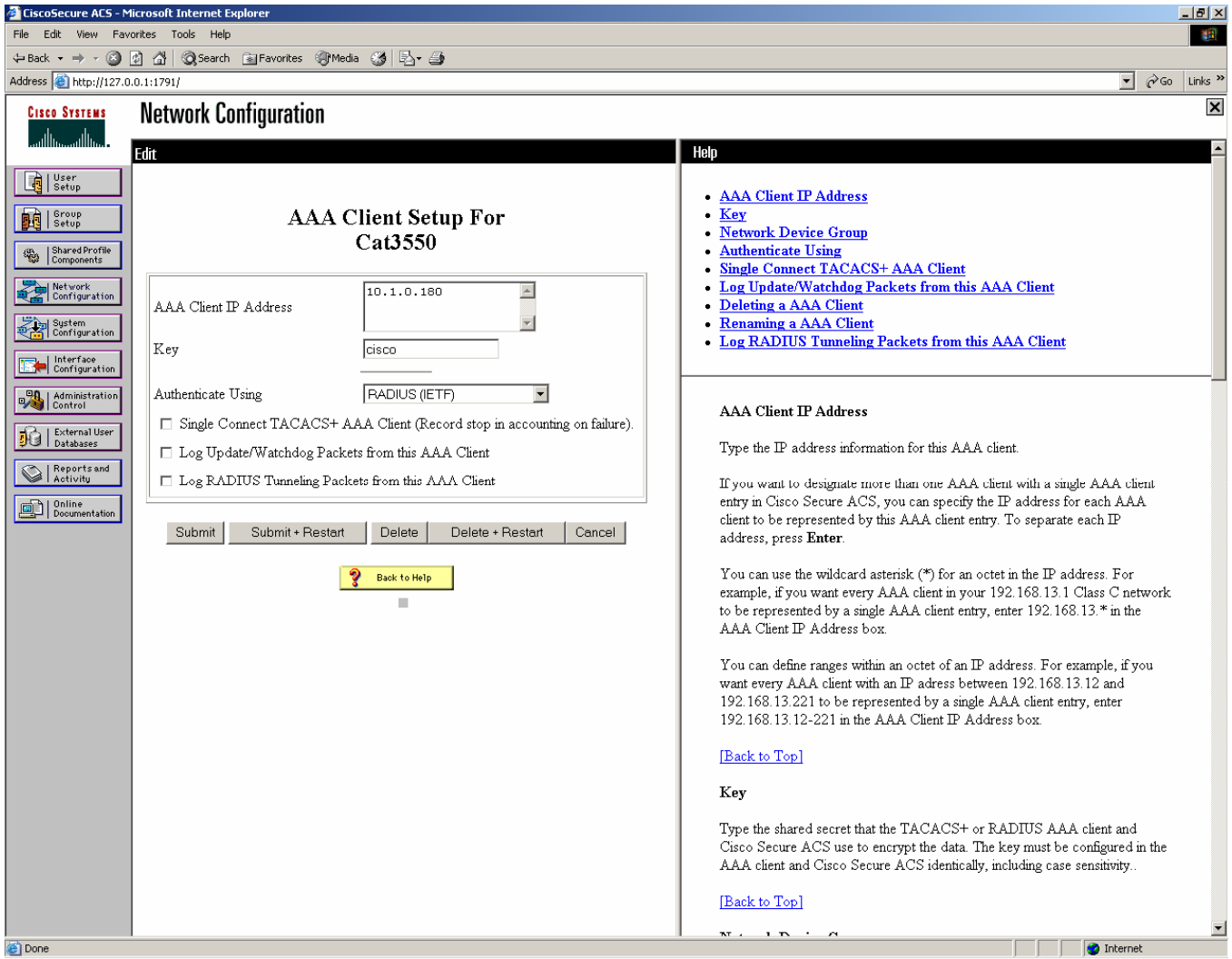
CiscoSecure ACS for Windows

CiscoSecure ACS Appliance

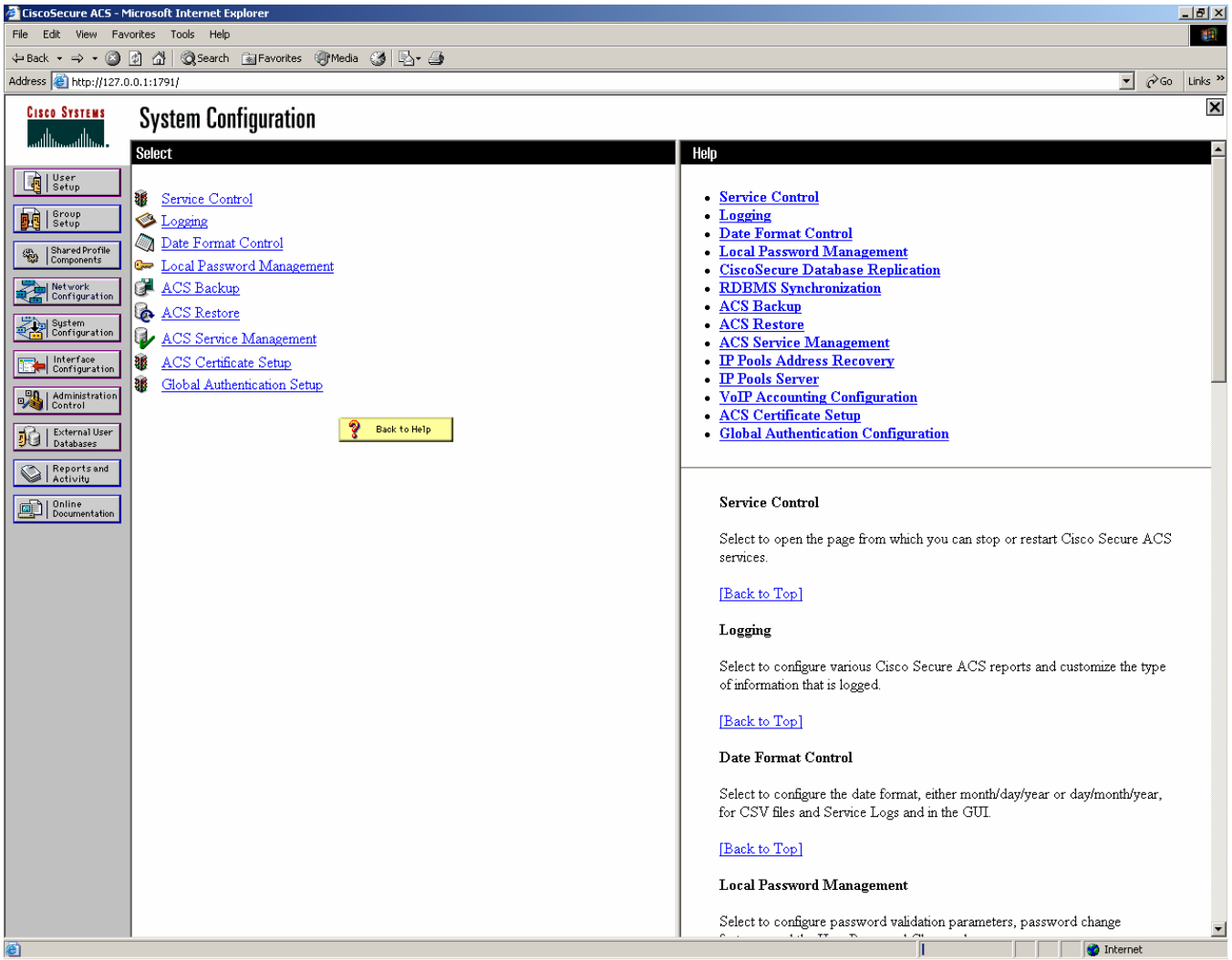
ACS Configuration
Adding The Network Access Device



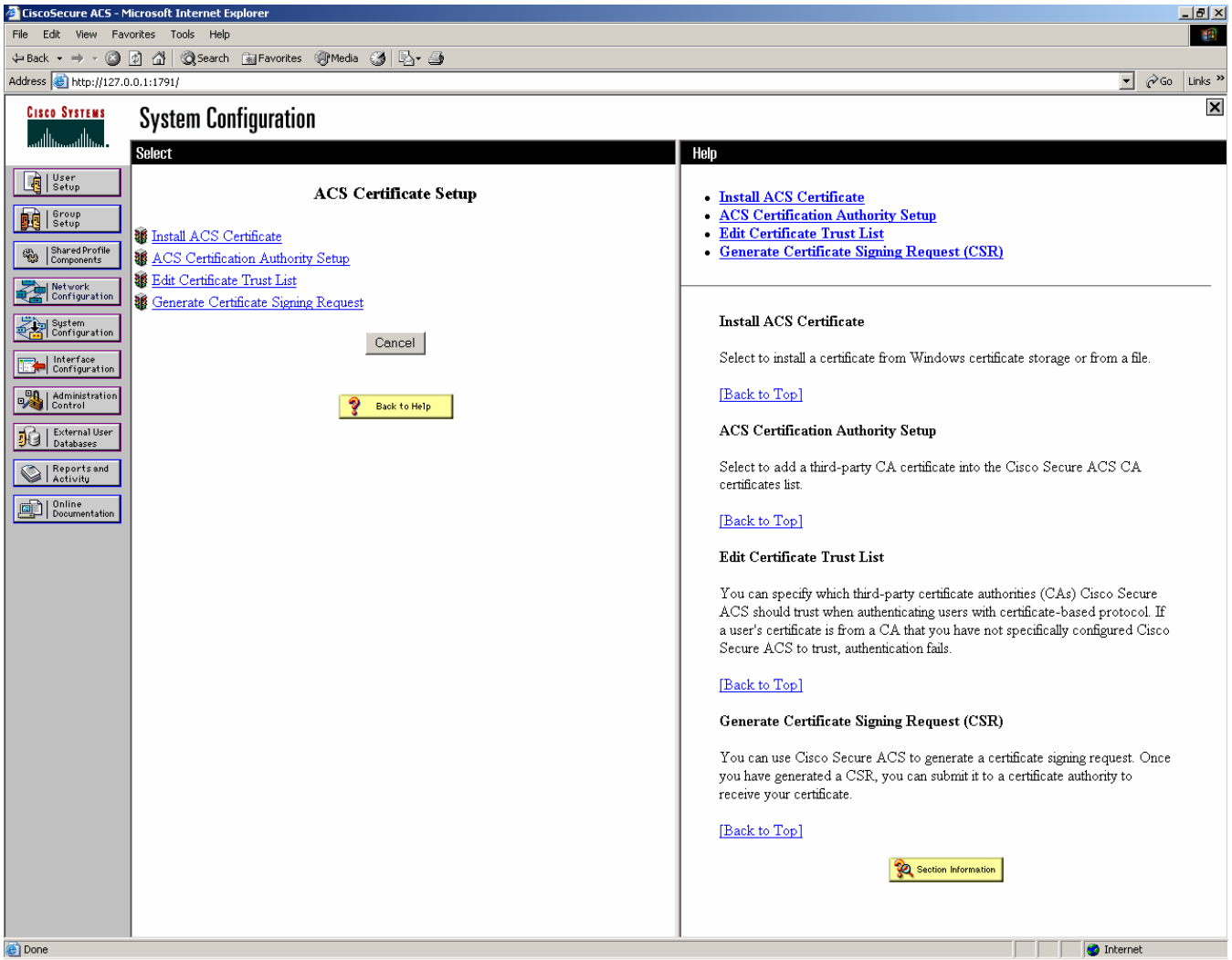
ACS Configuration
Adding The Network Access Device



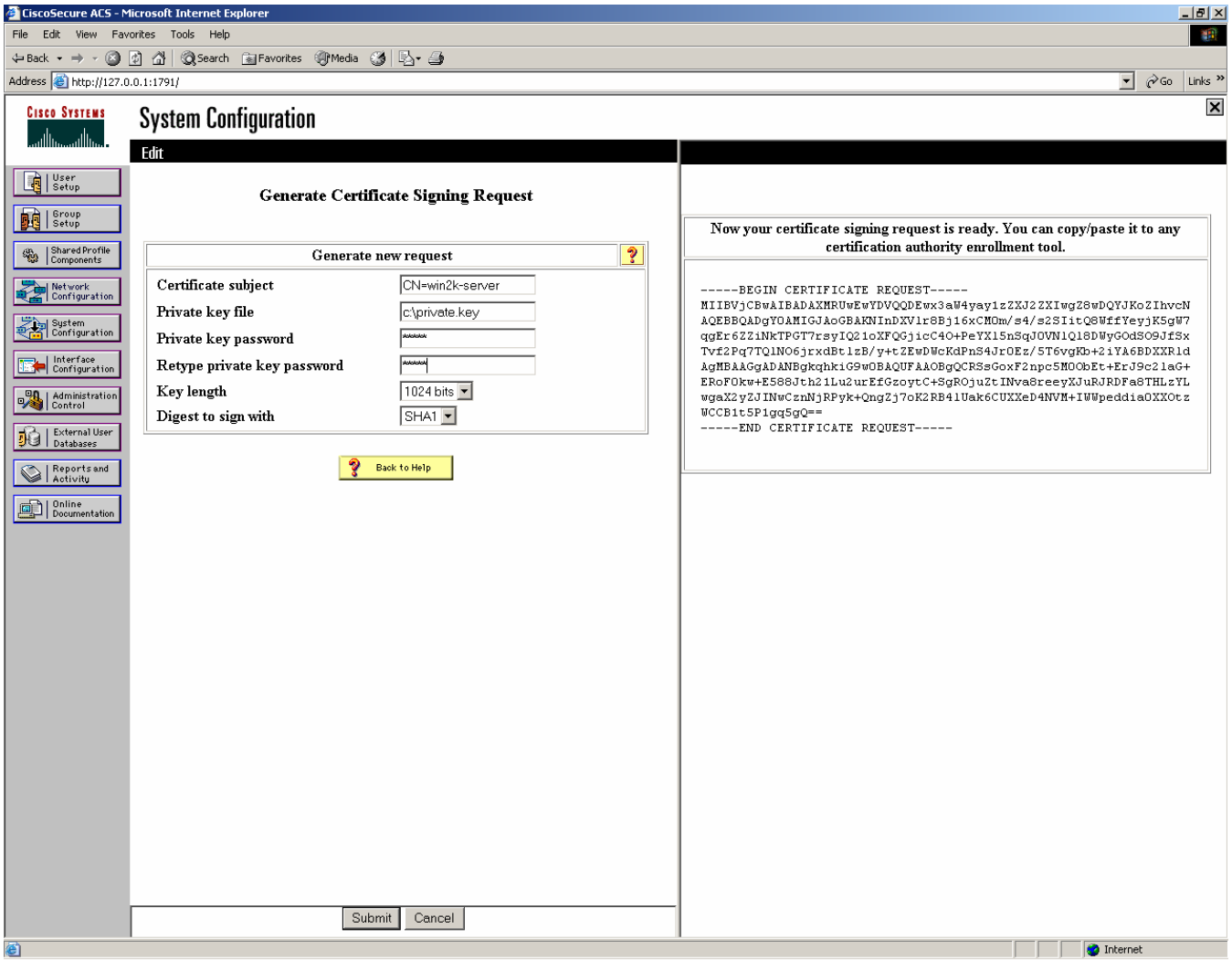
ACS Configuration
Server Certificate Setup



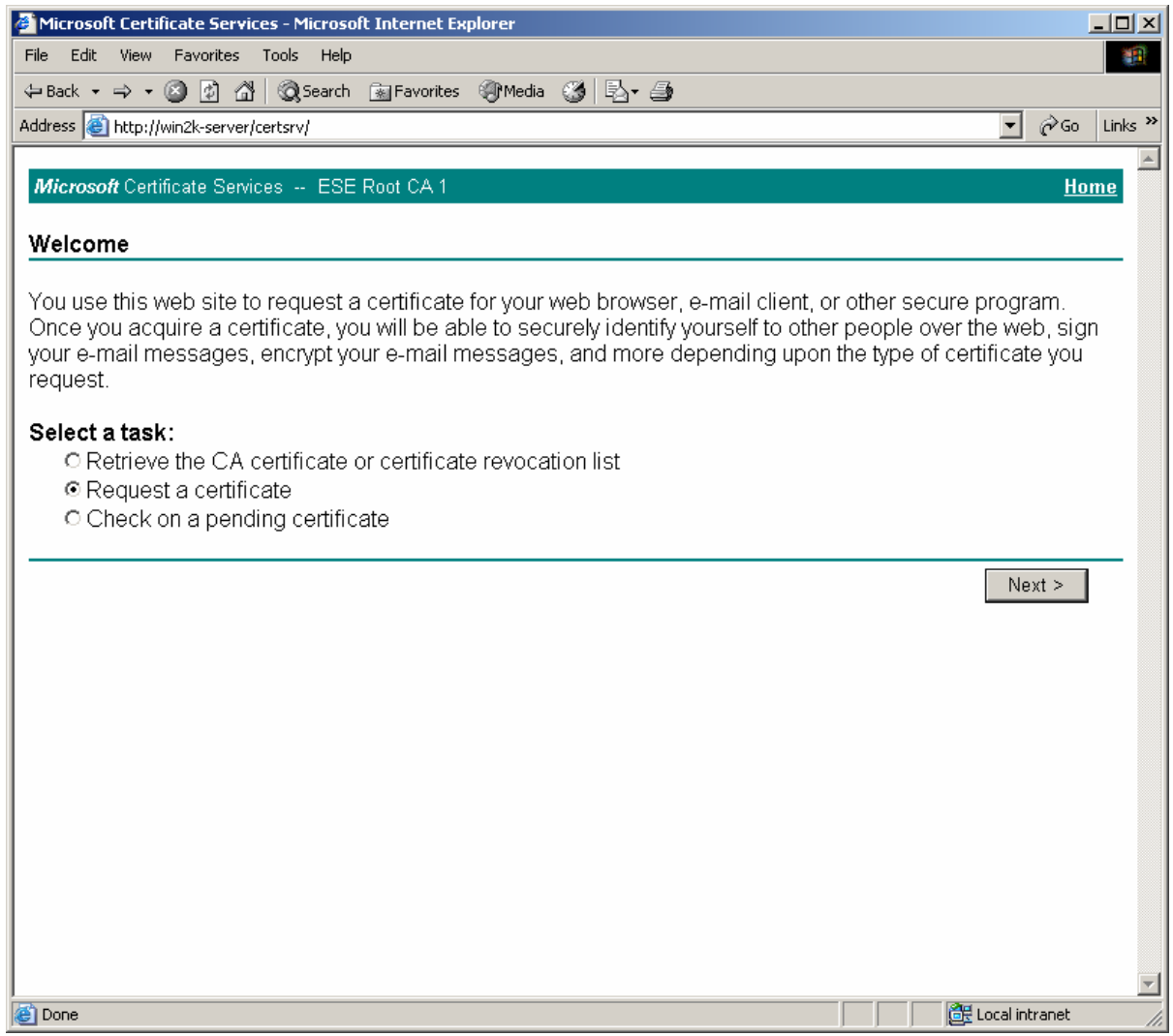
ACS Configuration
Server Certificate Setup



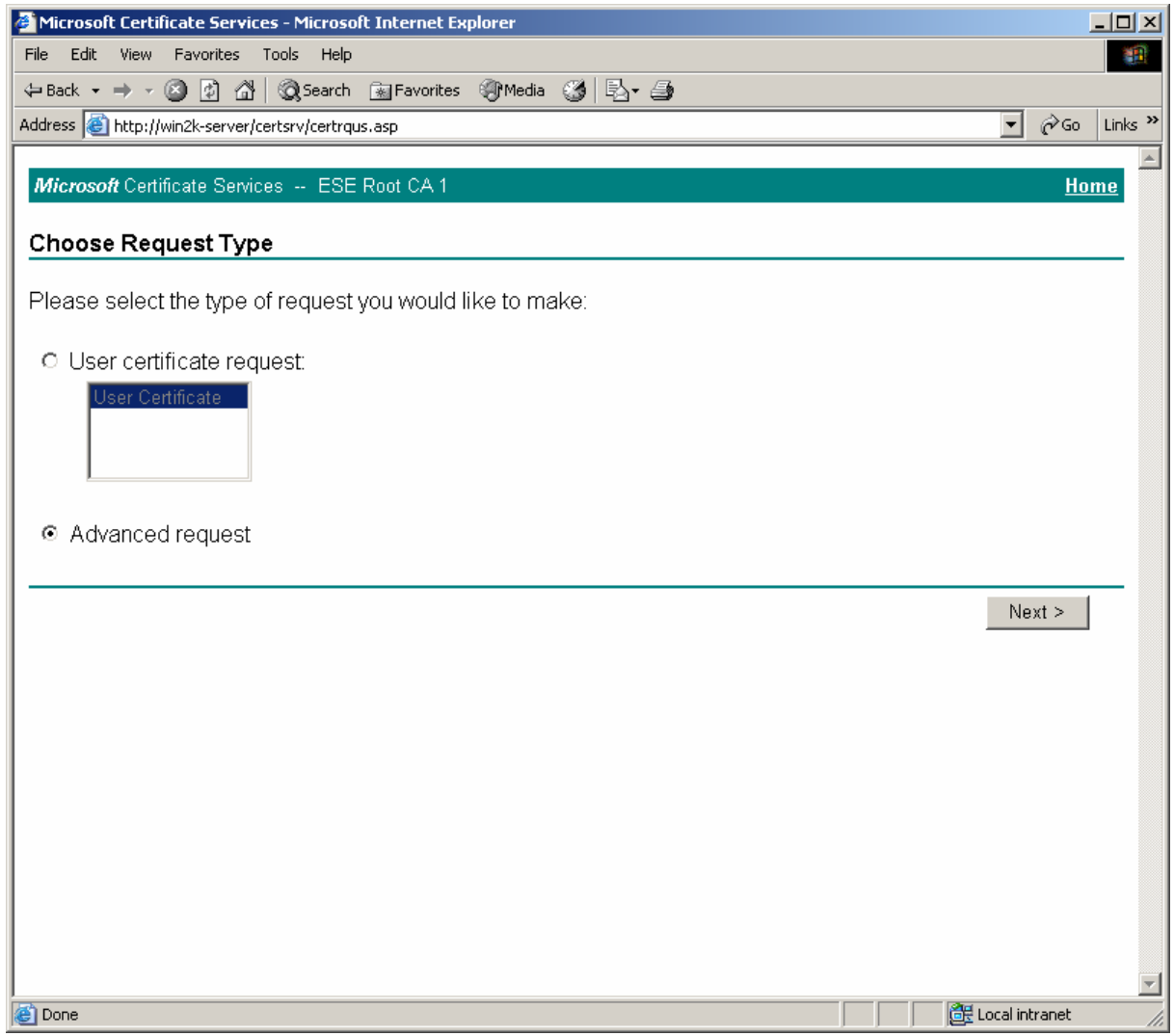
ACS Configuration
Server Certificate Setup – PKCS #7 Certificate Request



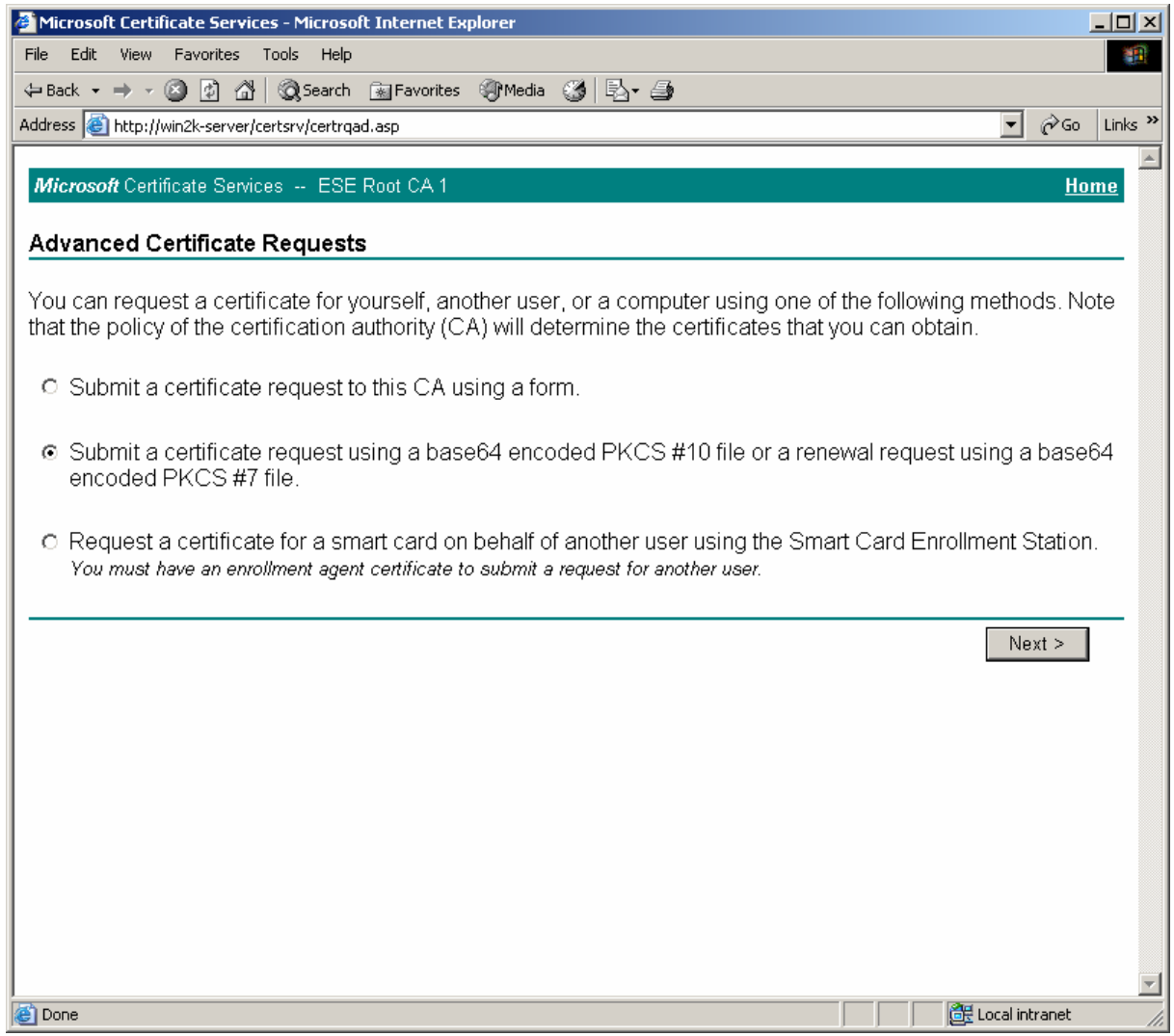
ACS Configuration
Server Certificate Request (MS Certificate Services)



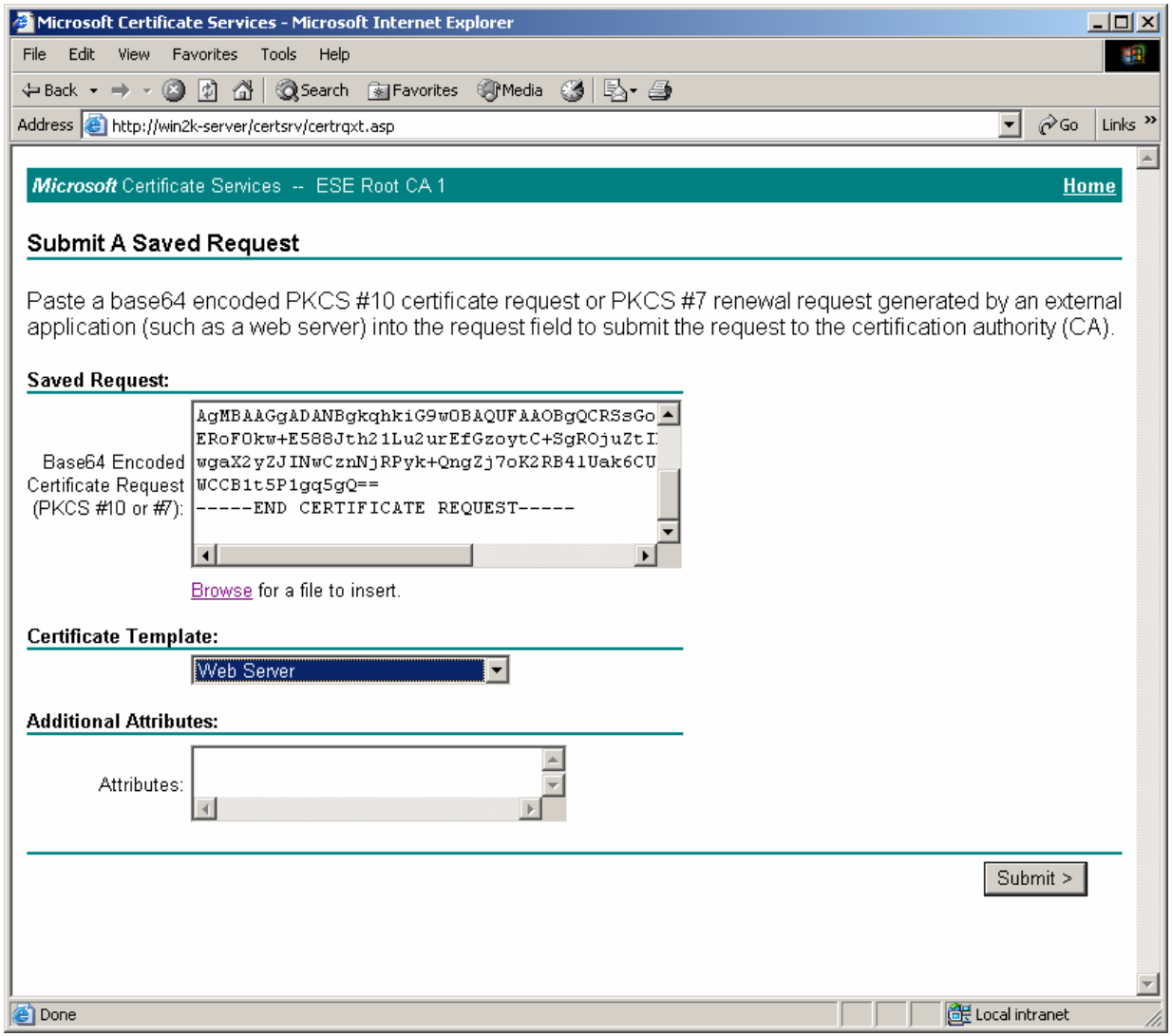
ACS Configuration
Server Certificate Request (MS Certificate Services)



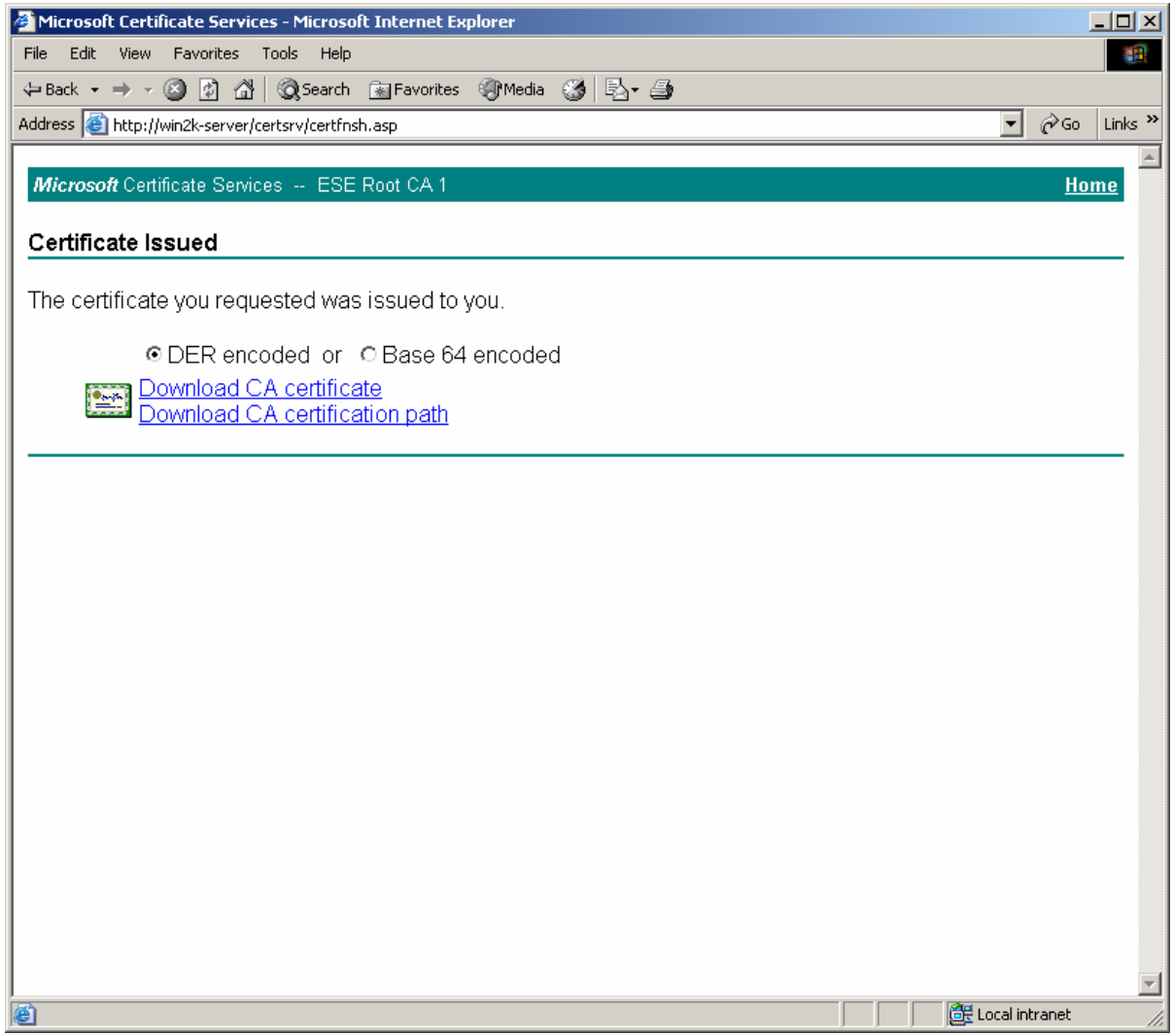
ACS Configuration
Server Certificate Request (MS Certificate Services)



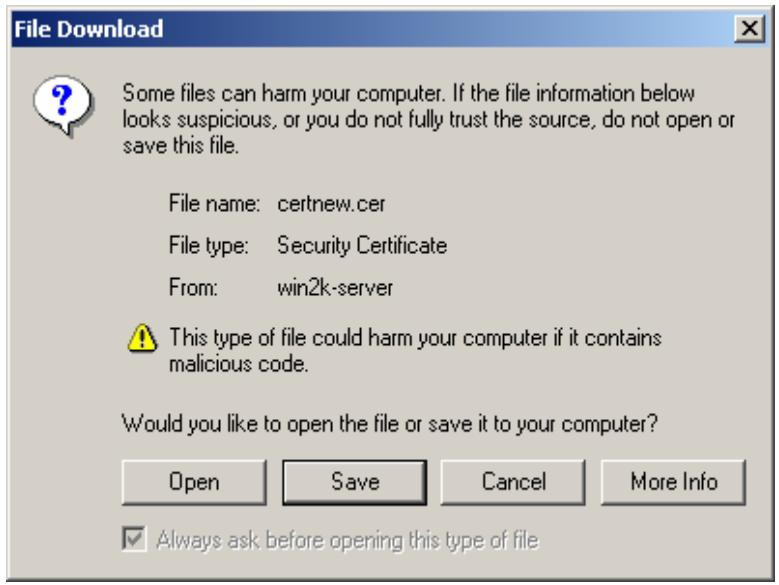
ACS Configuration
Server Certificate Request (MS Certificate Services)



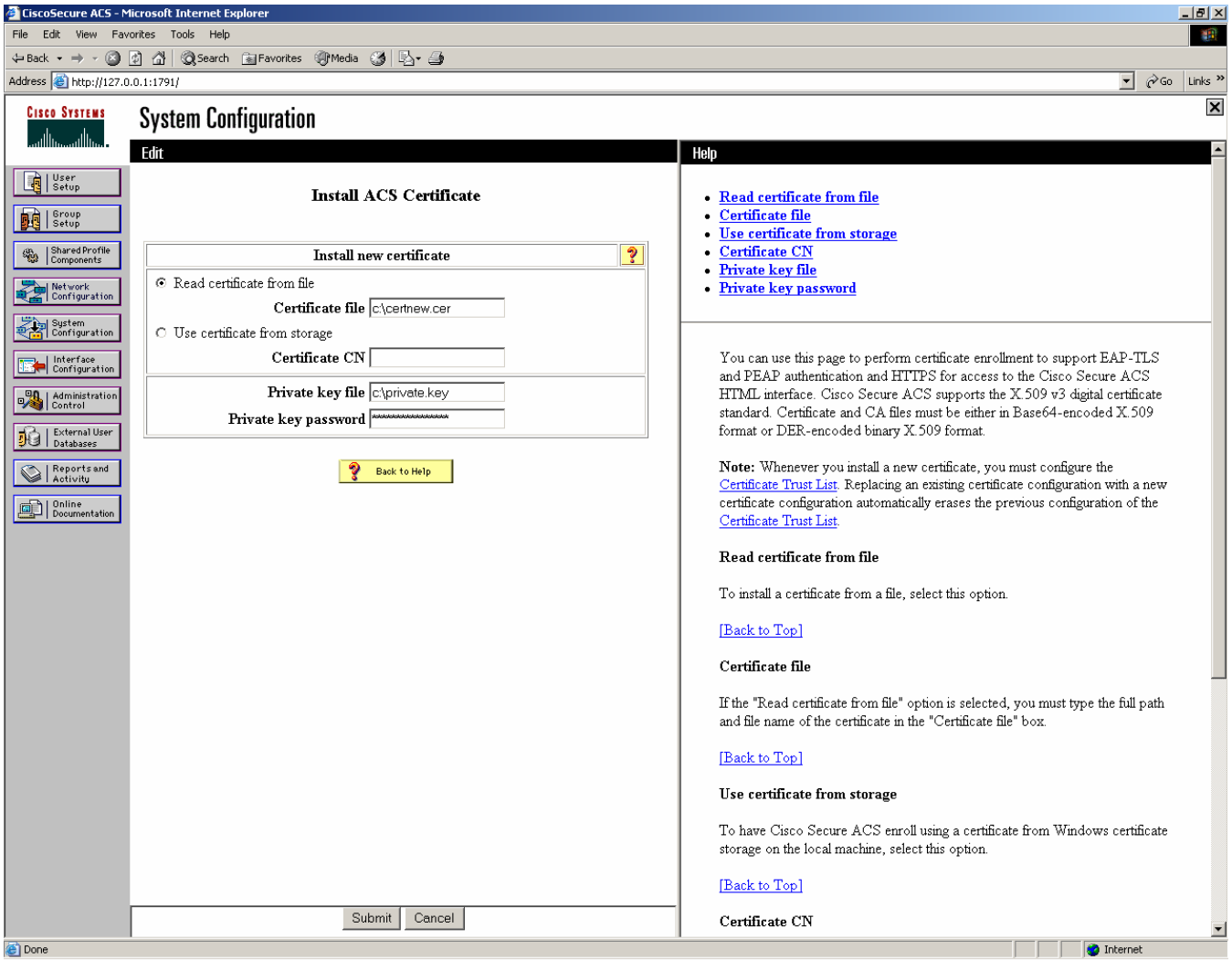
ACS Configuration
Server Certificate Request (MS Certificate Services)



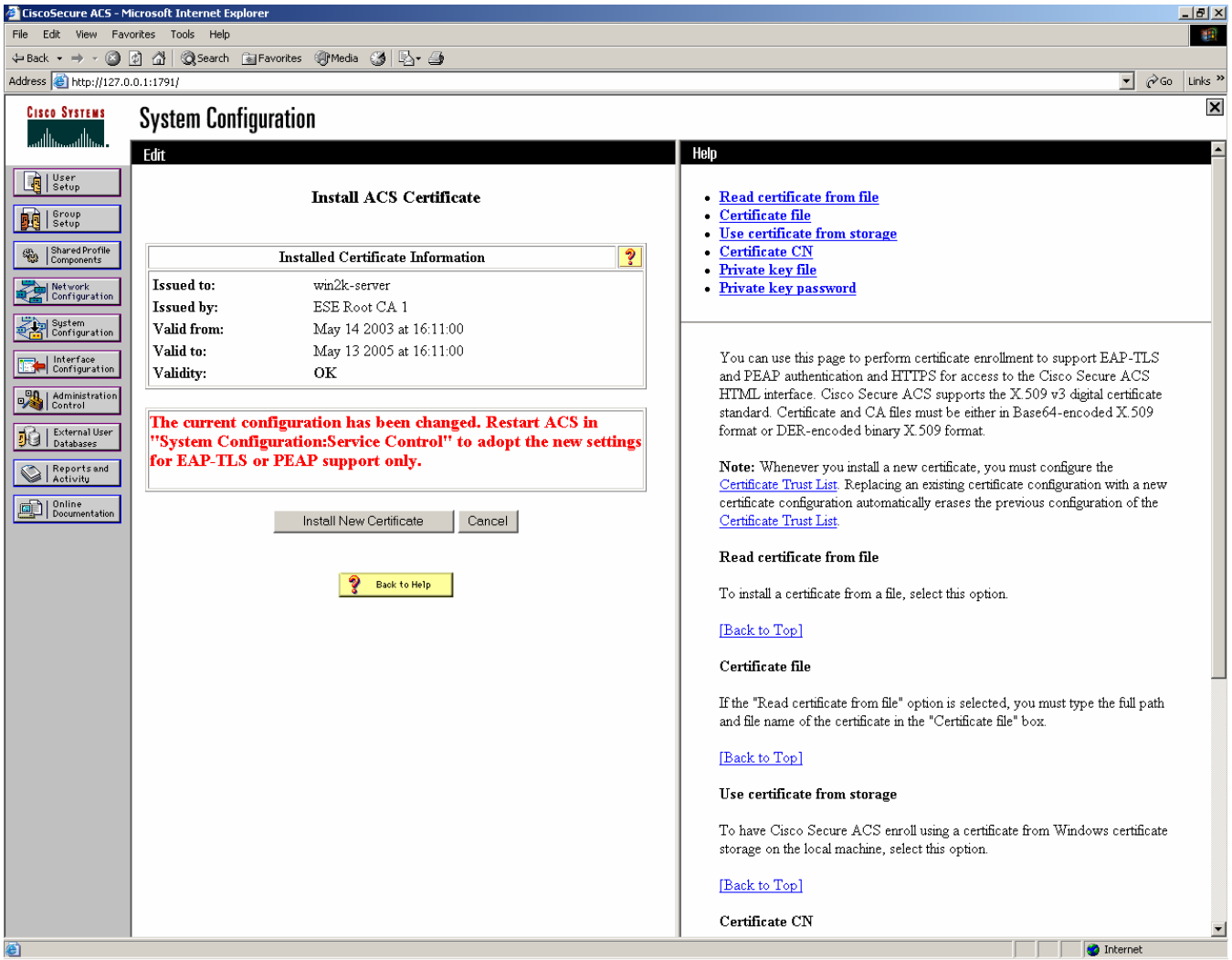
ACS Configuration
Server Certificate Request (MS Certificate Services)



ACS Configuration
Server Certificate Installation

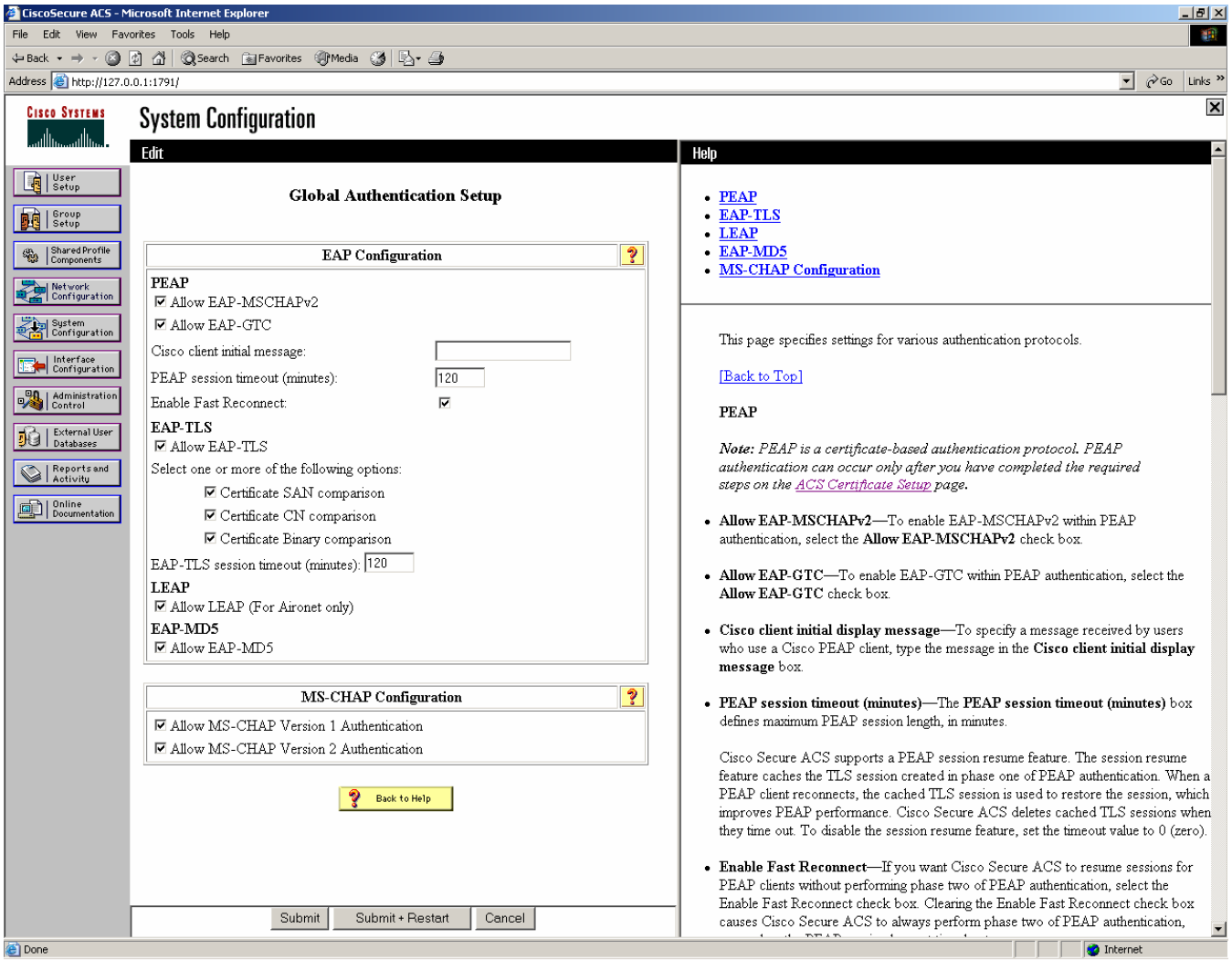


ACS Configuration
Server Certificate Installation

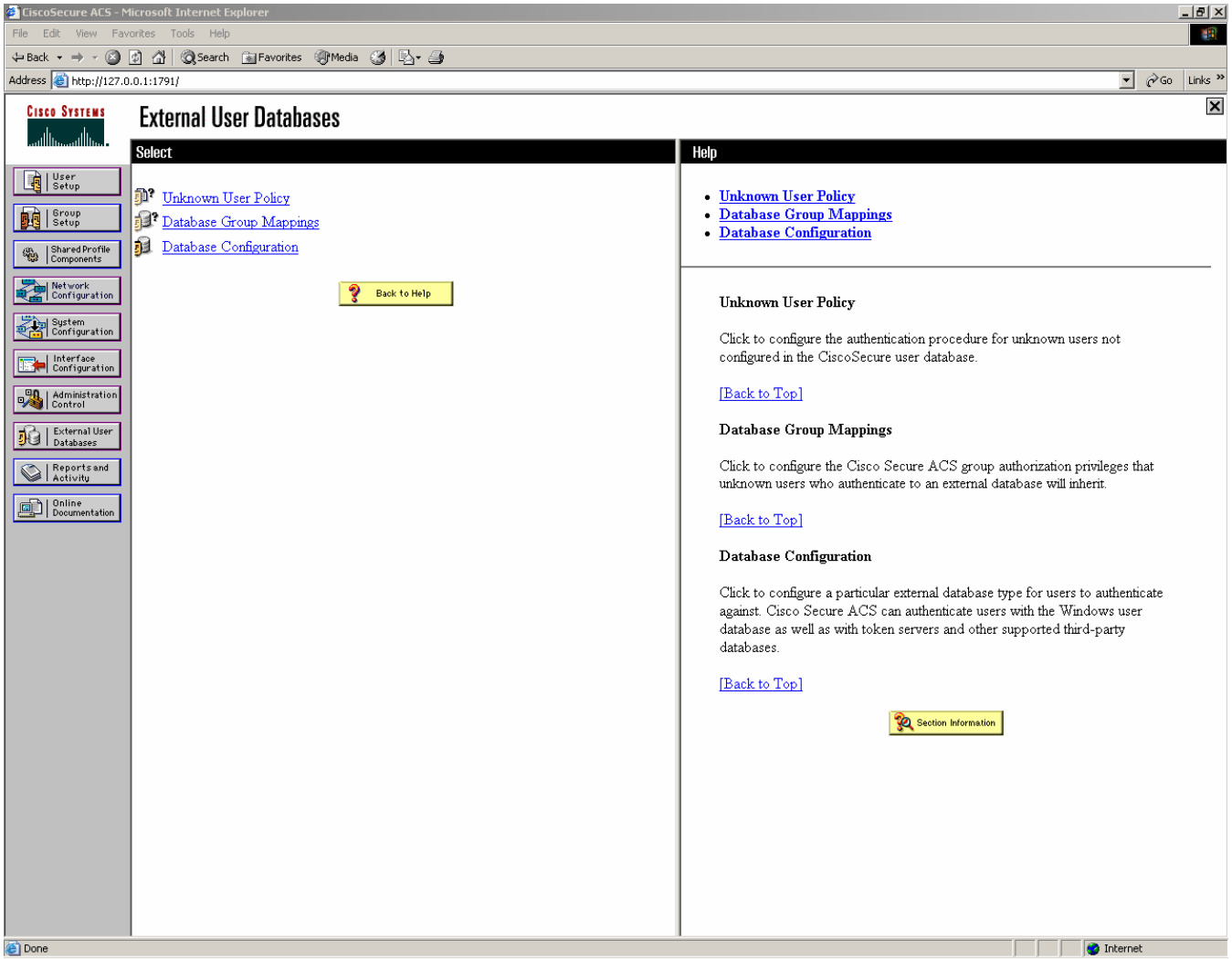


ACS Configuration
Global Authentication Setup – EAP Method Selection

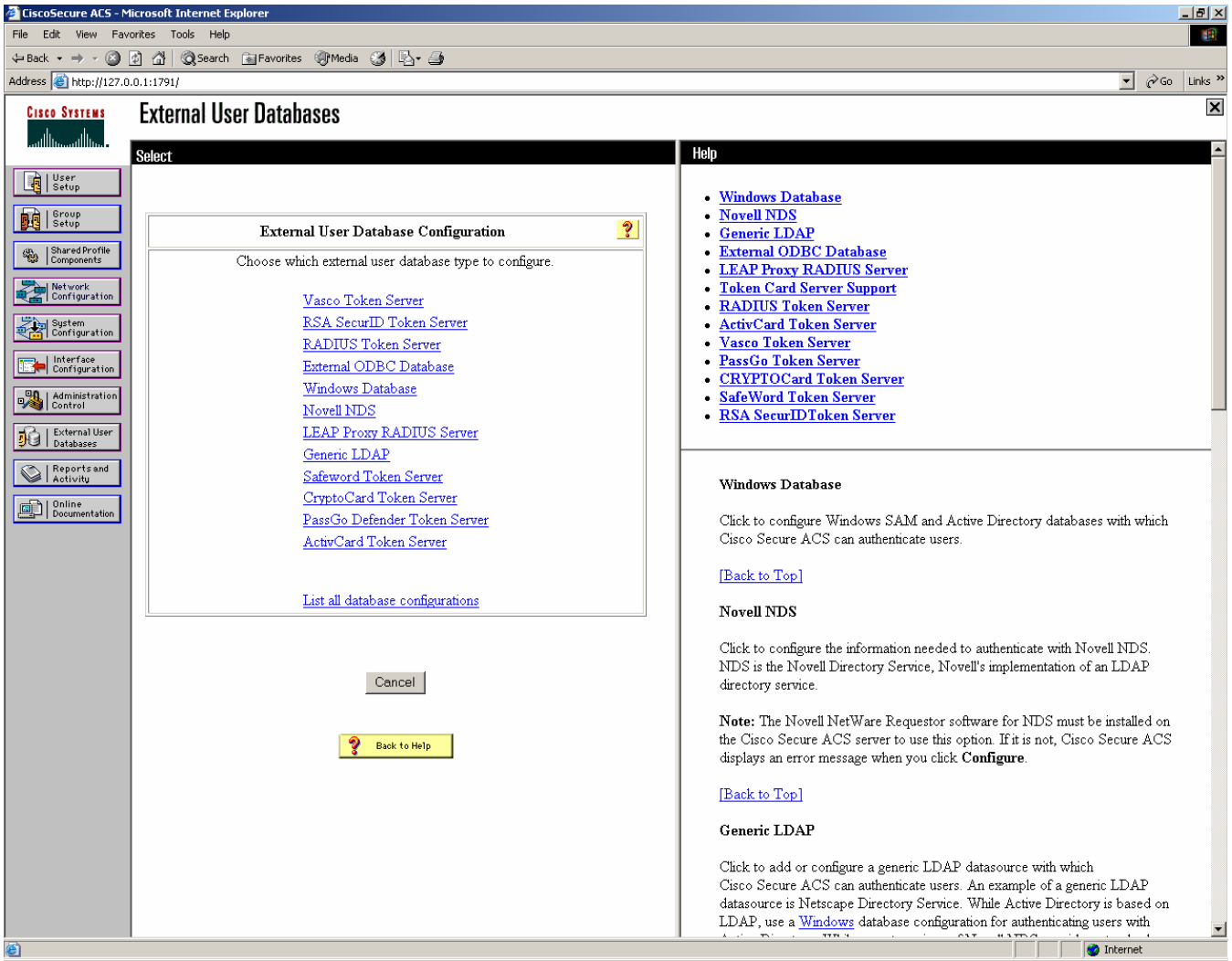
Cisco.com



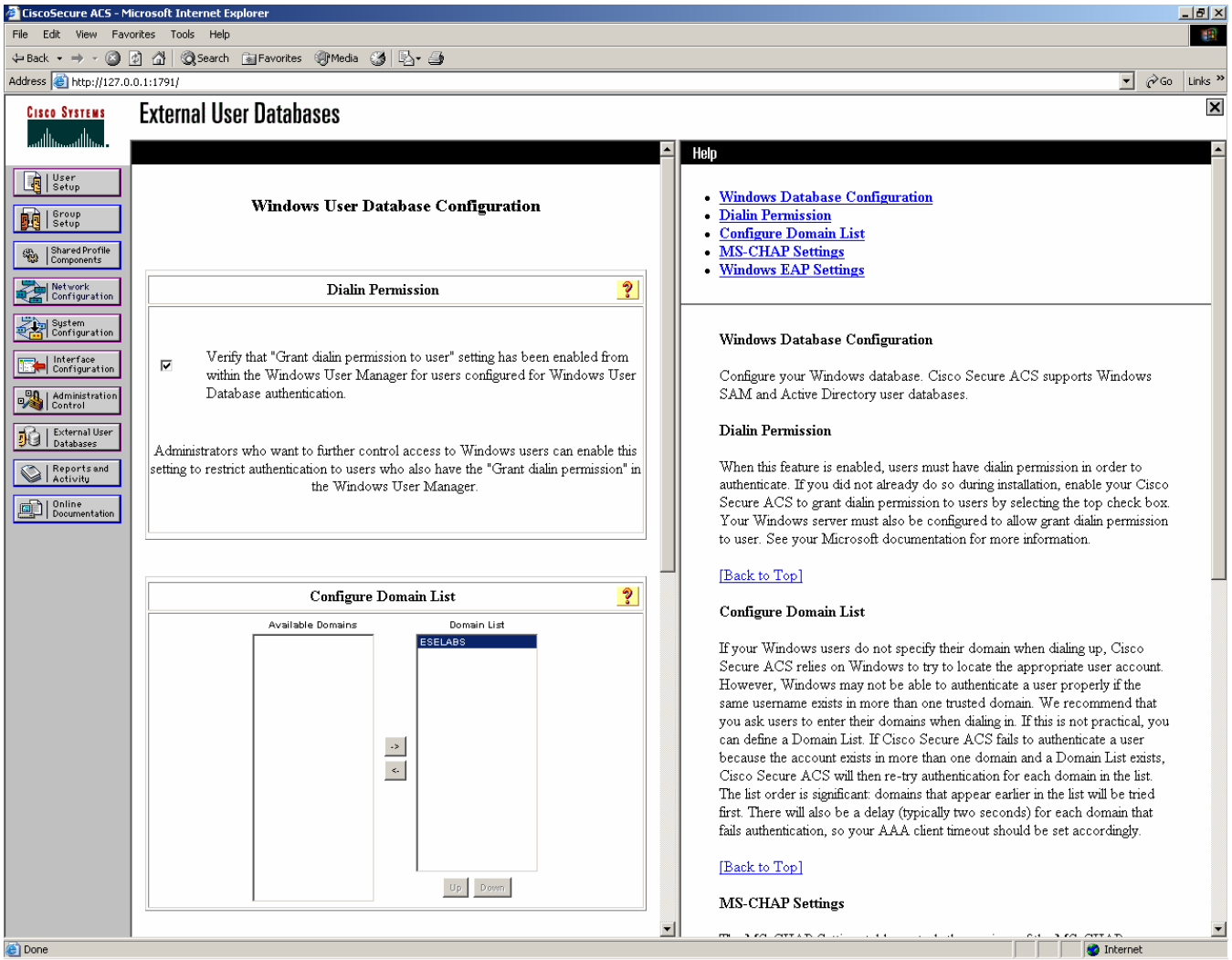
ACS Configuration
External User Database Configuration



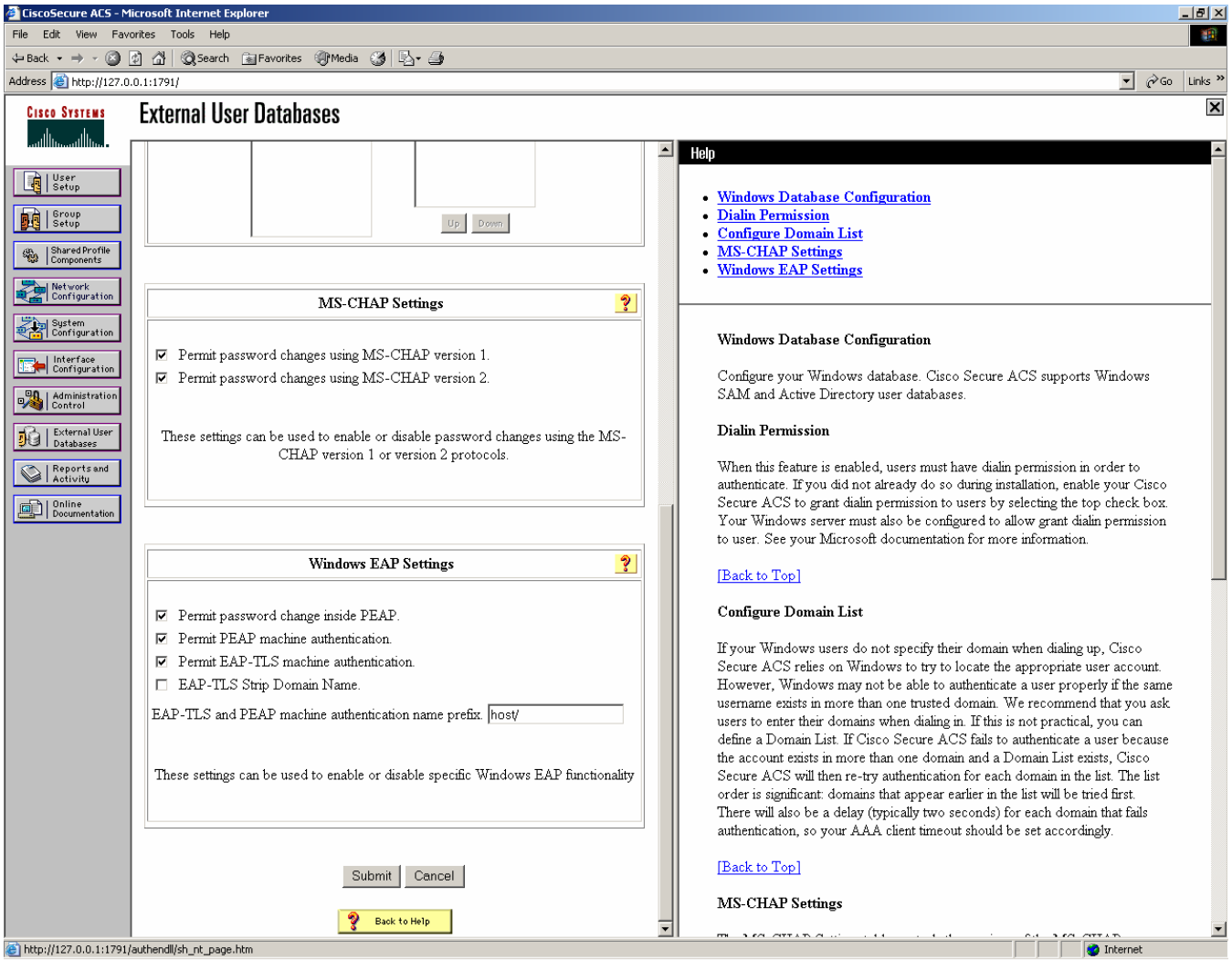
ACS Configuration
External User Database Configuration



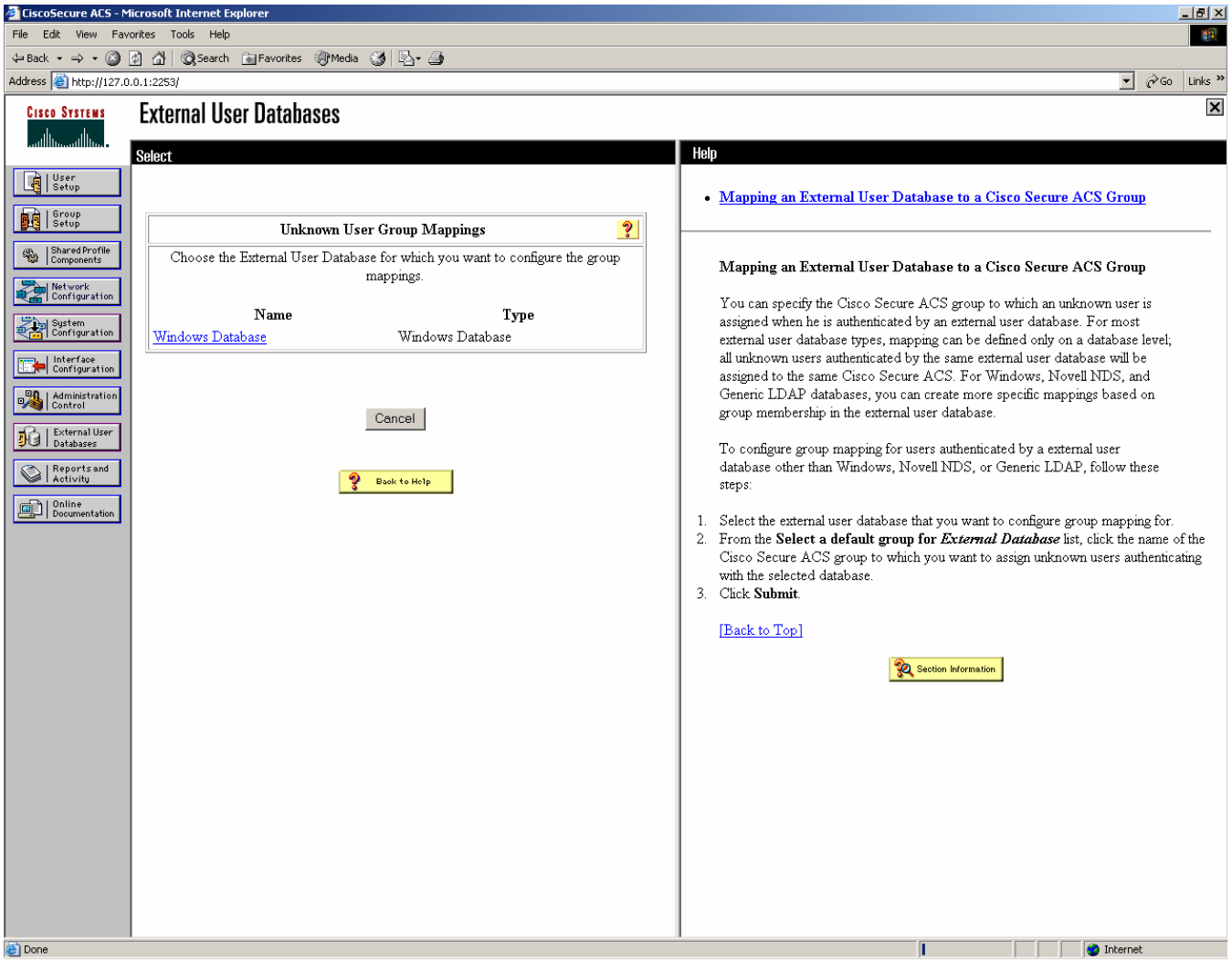
ACS Configuration
External User Database Configuration



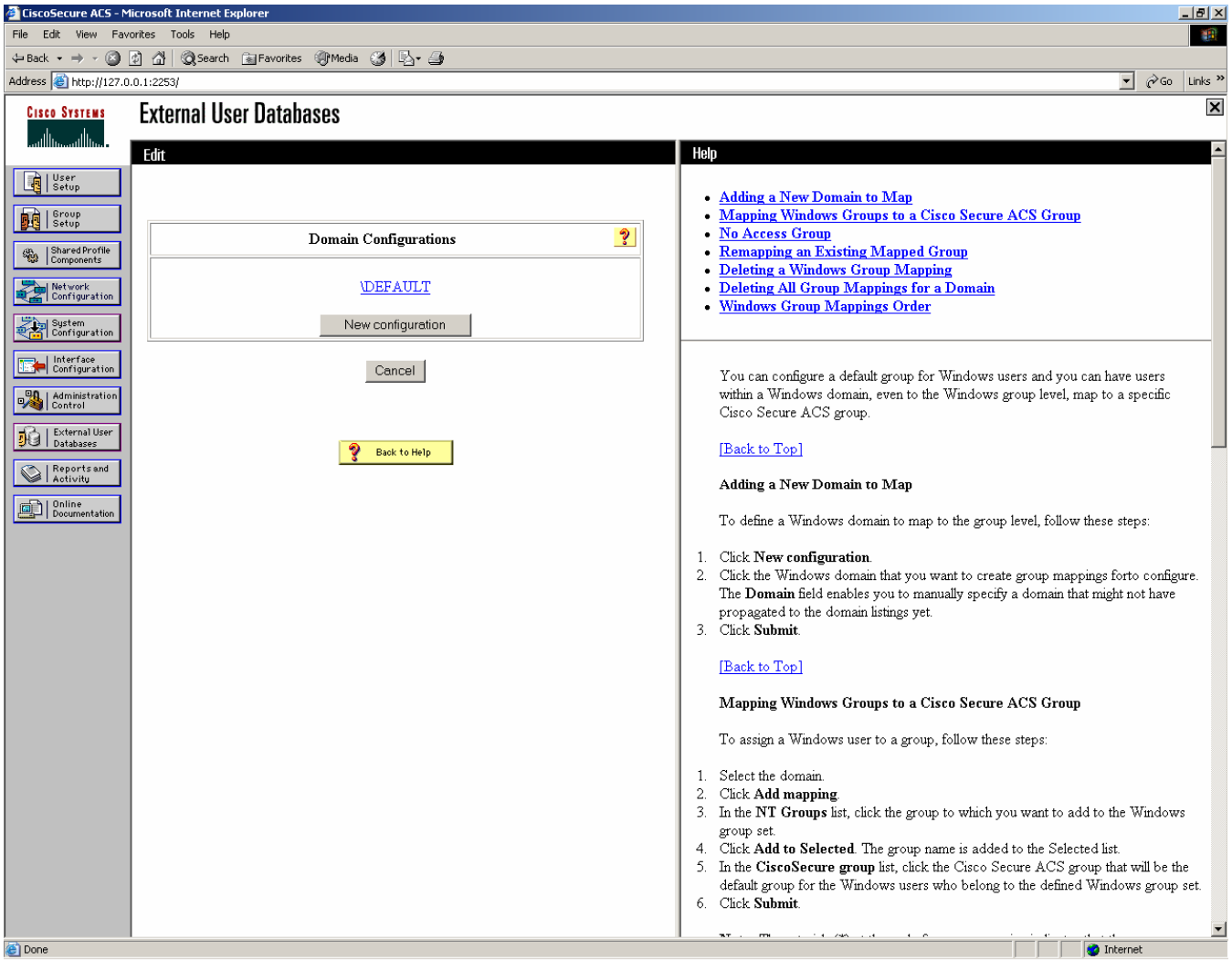
ACS Configuration
External User Database Configuration



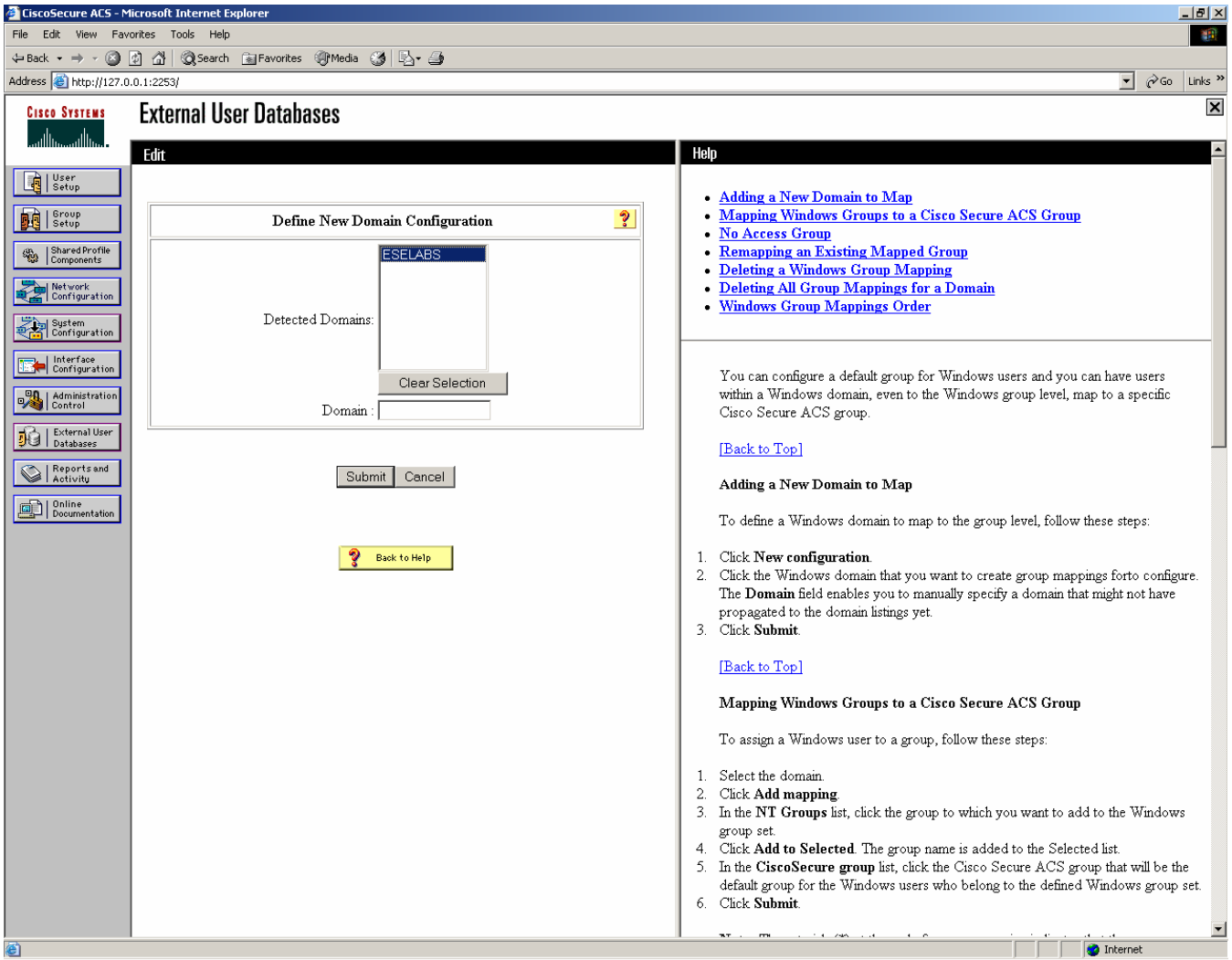
ACS Configuration
External User Database Group Mapping



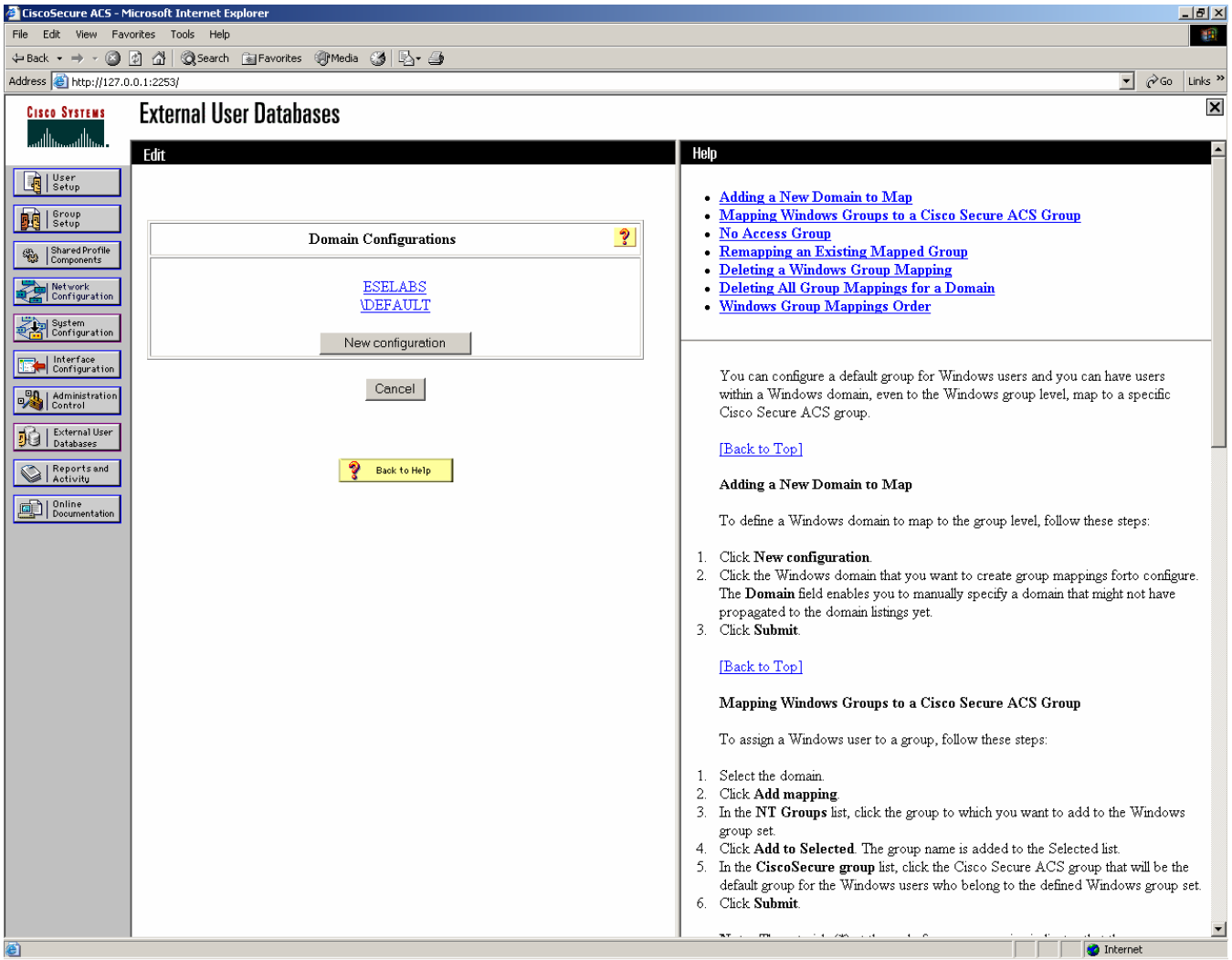
ACS Configuration
External User Database Group Mapping



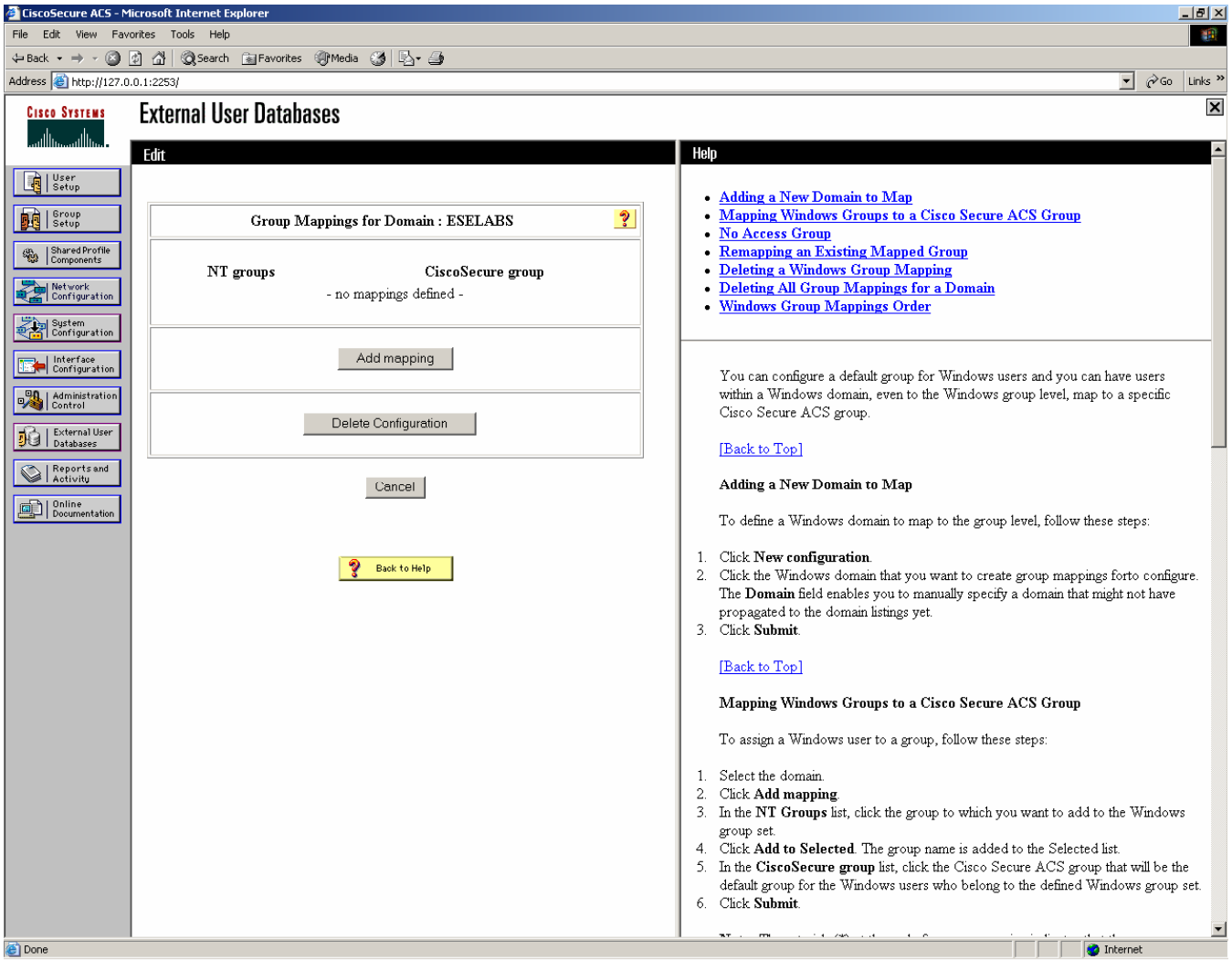
ACS Configuration
External User Database Group Mapping



ACS Configuration
External User Database Group Mapping

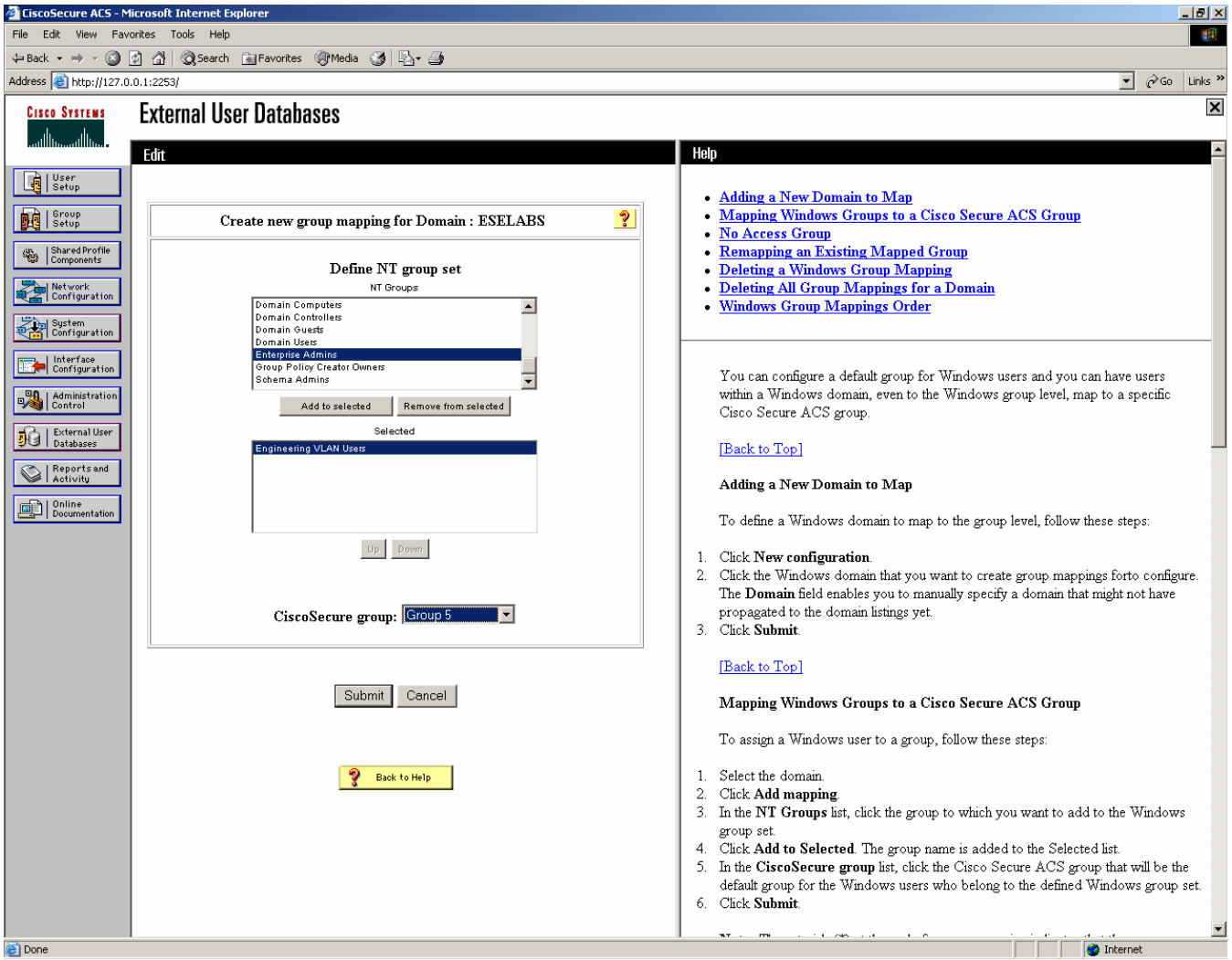


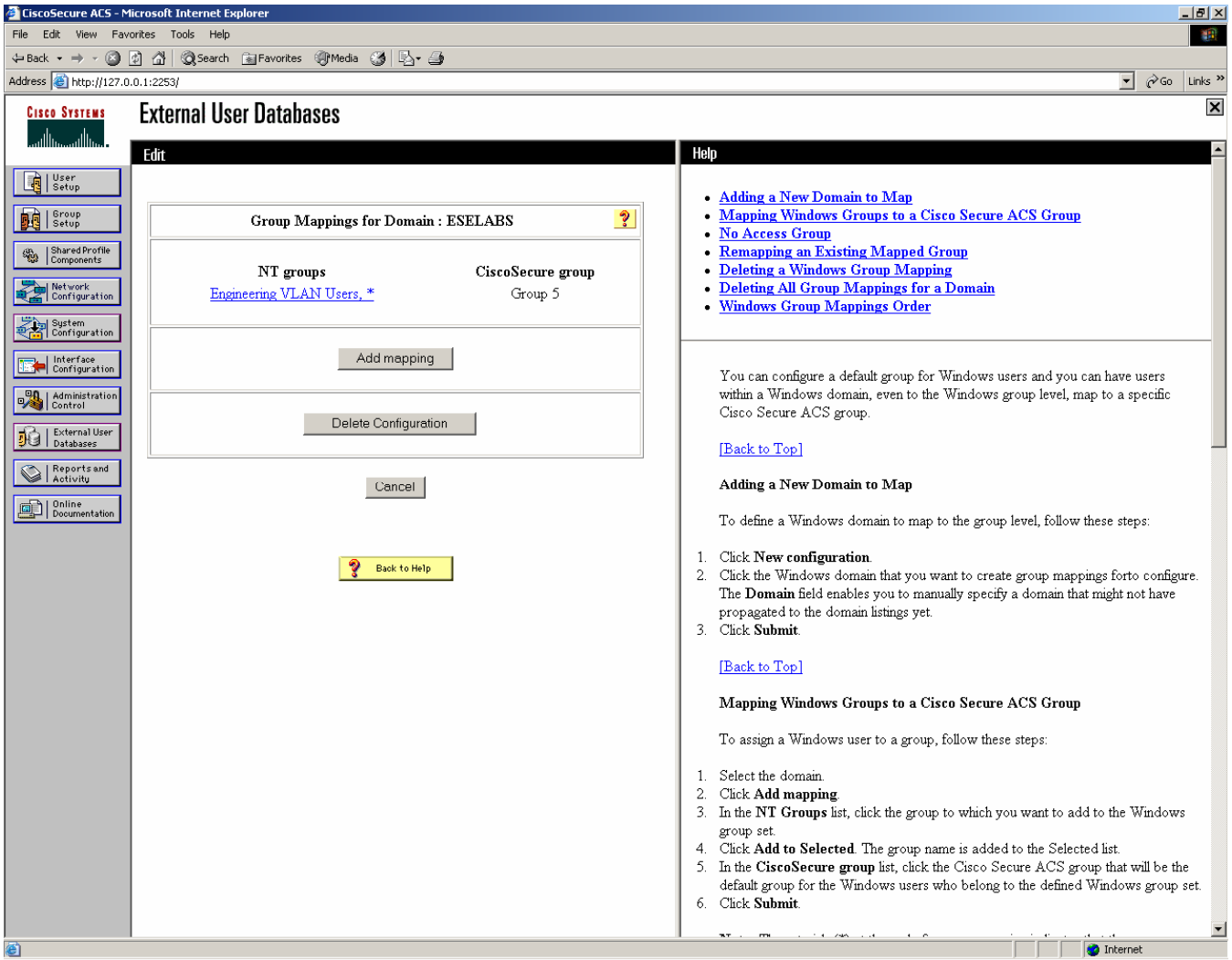
ACS Configuration
External User Database Group Mapping



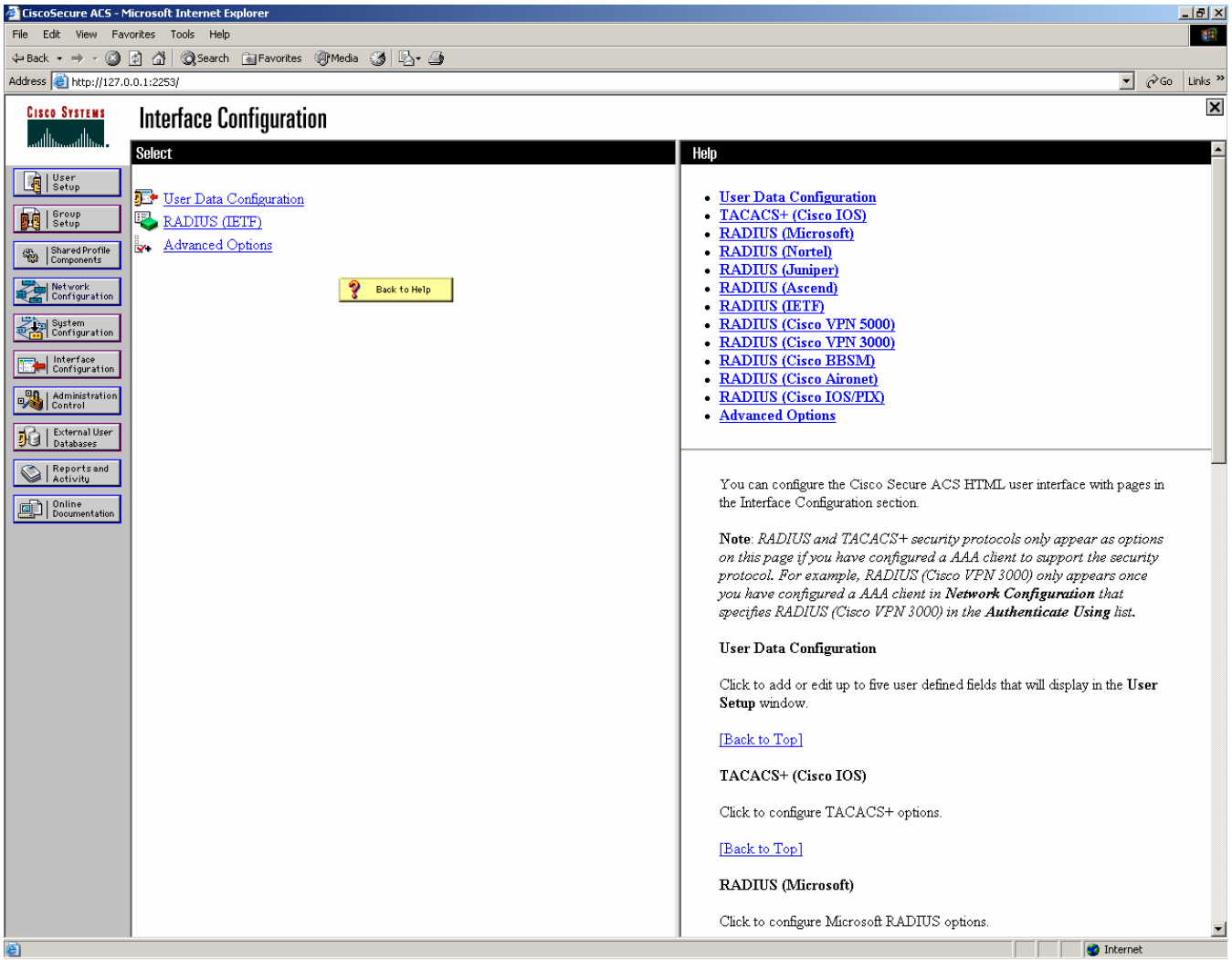
ACS Configuration
External User Database Group Mapping

Cisco.com

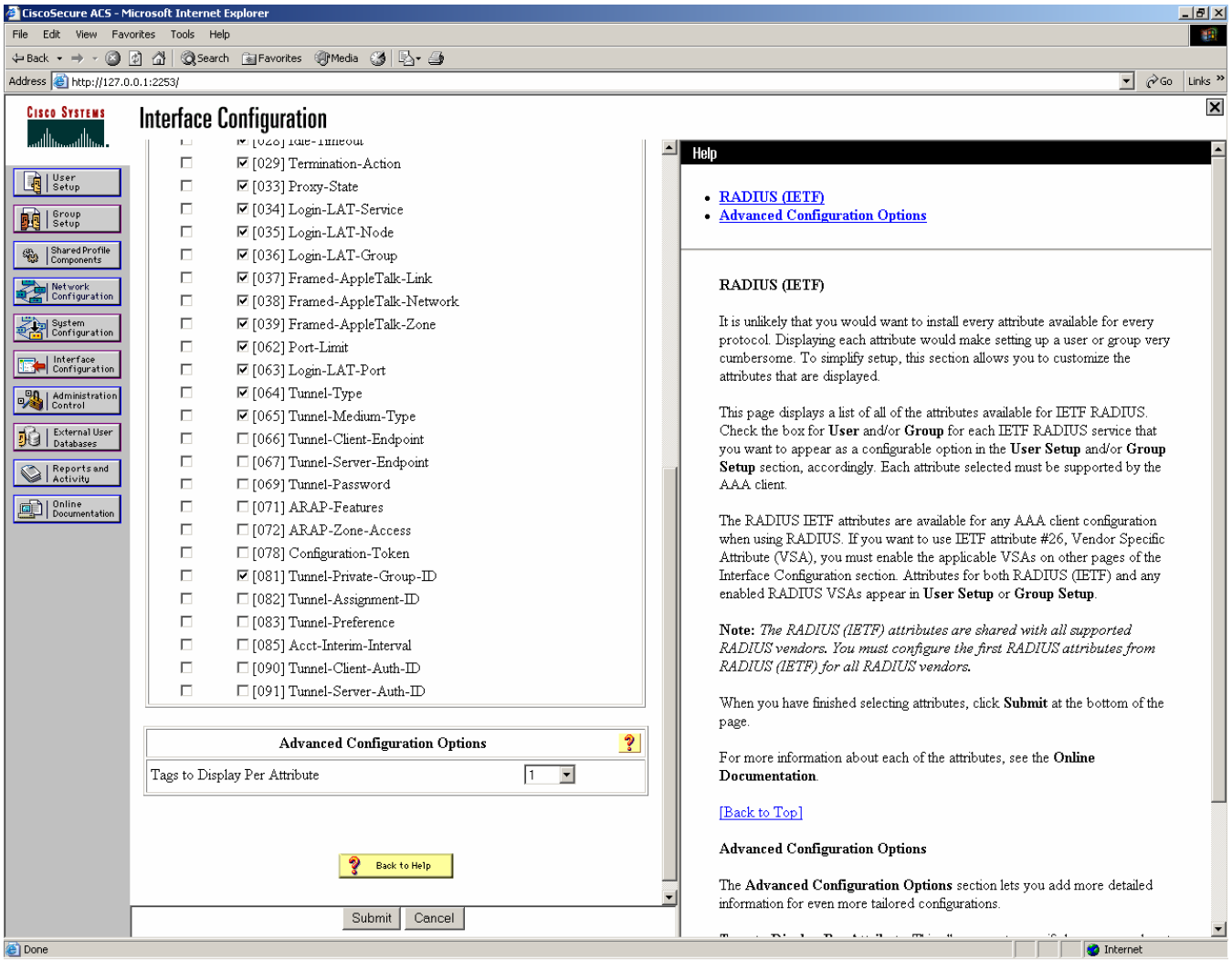




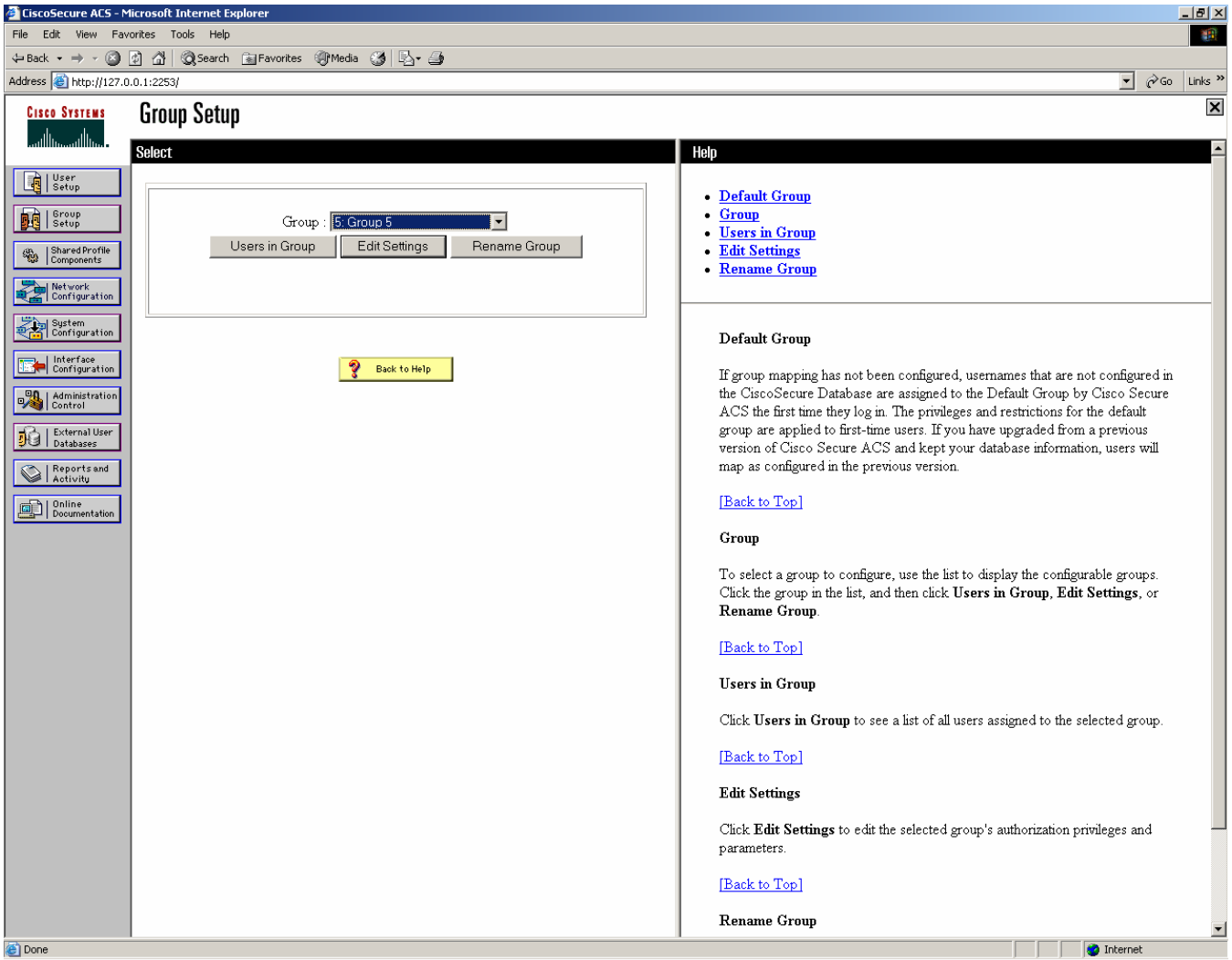
ACS Configuration
User Interface Option Configuration



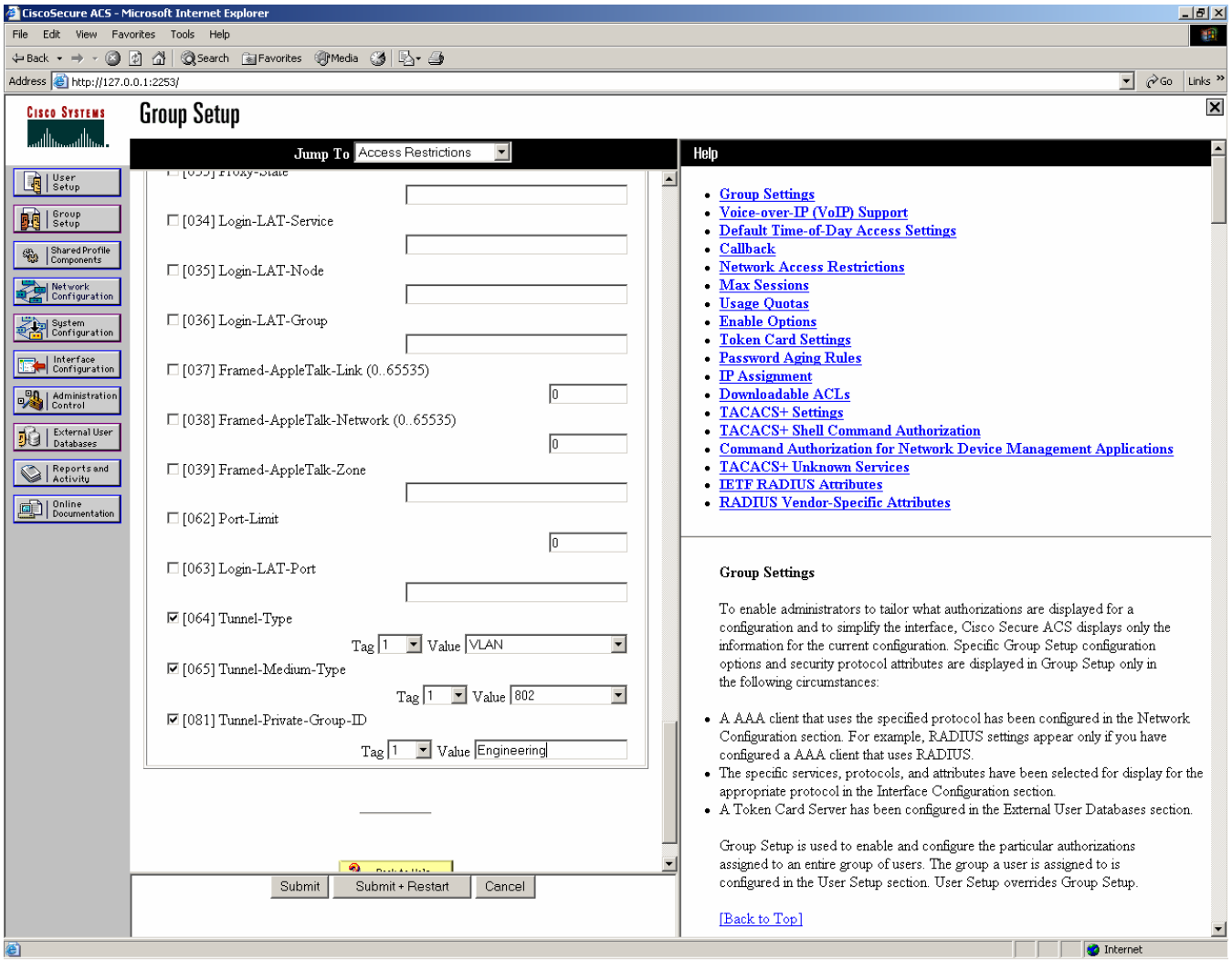
ACS Configuration
User Interface Options – RADIUS AV Pair Configuration



ACS Configuration
Group Policy Configuration



ACS Configuration
Group Policy Configuration – VLAN Assignment



Authenticator (Switch) Configuration

Catalyst 6500/4500/4000

Catalyst 2950/3550

Switch Configuration
CatOS Configuration – Global commands

Cisco.com

 # 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

Cisco.com

 # 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

Cisco.com

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

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

Switch Configuration
IOS Configuration – Per-port commands

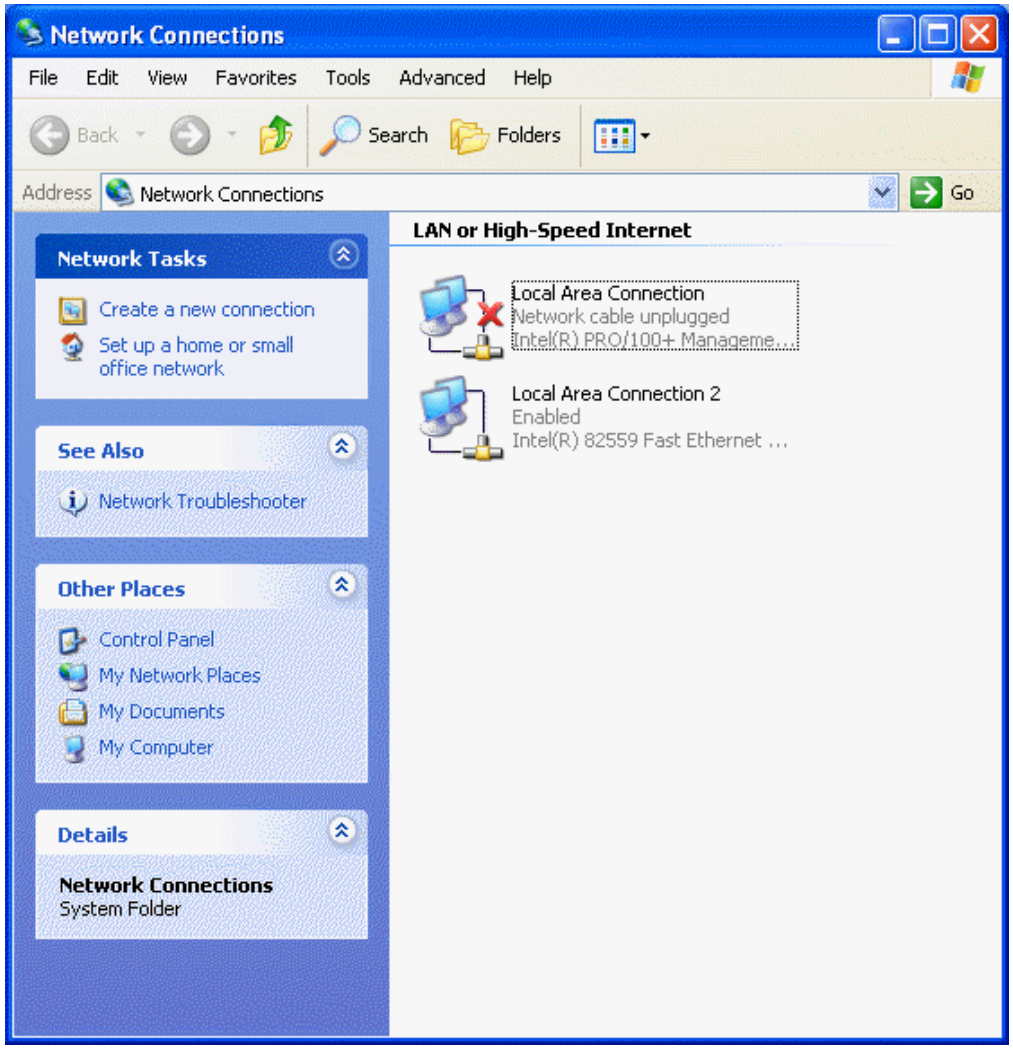
Cisco.com

 # IOS Per-port configuration
dot1x port-control auto

Client Supplicant Configuration

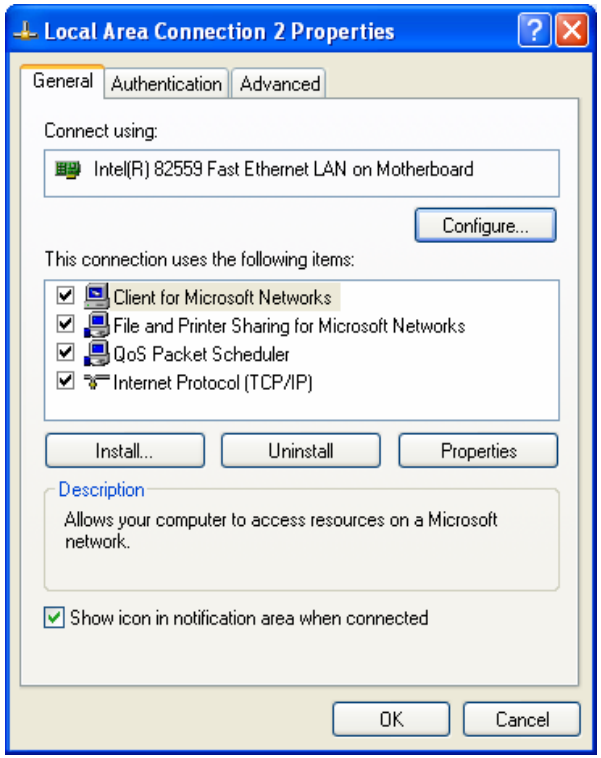
Windows XP SP1

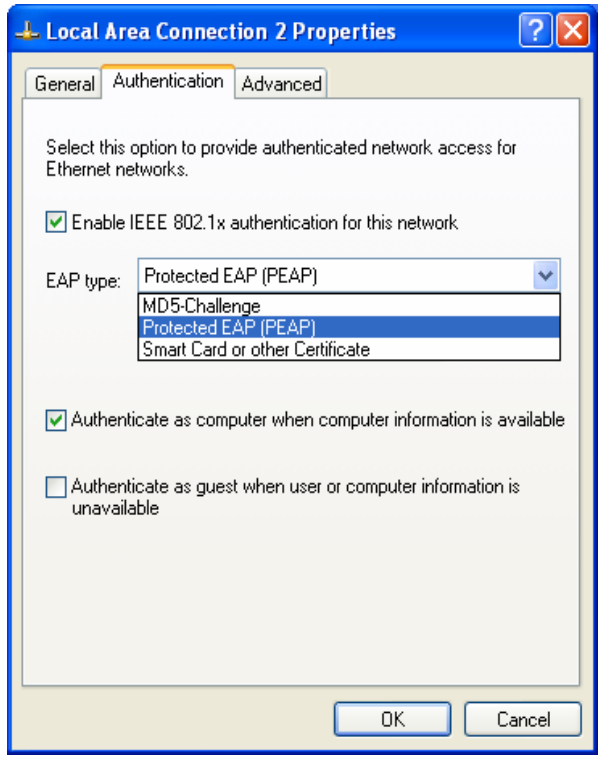
Supplicant Configuration
Network Connection Properties



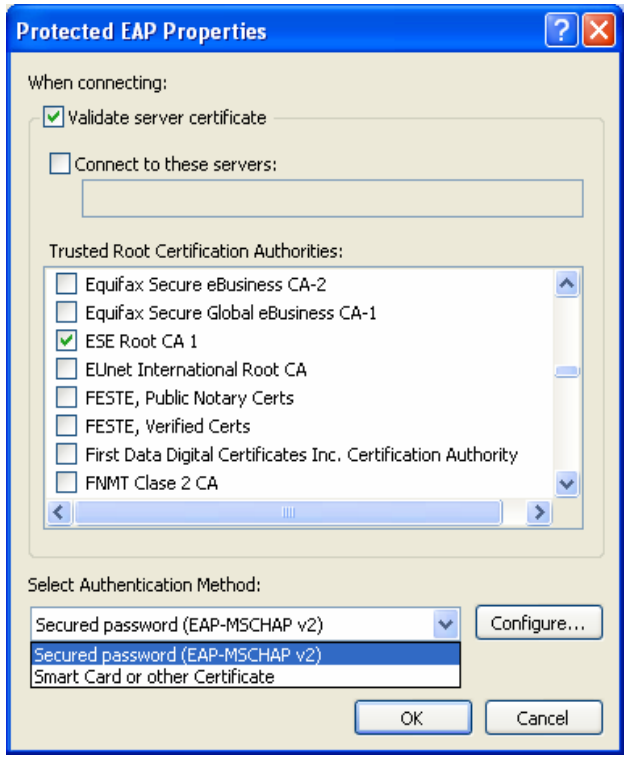
Supplicant Configuration
Network Interface Authentication Properties

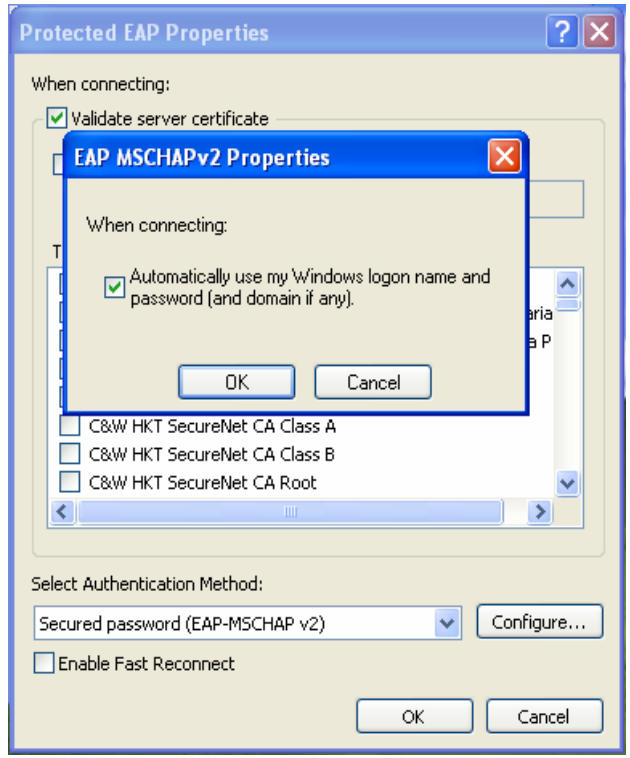
Cisco.com



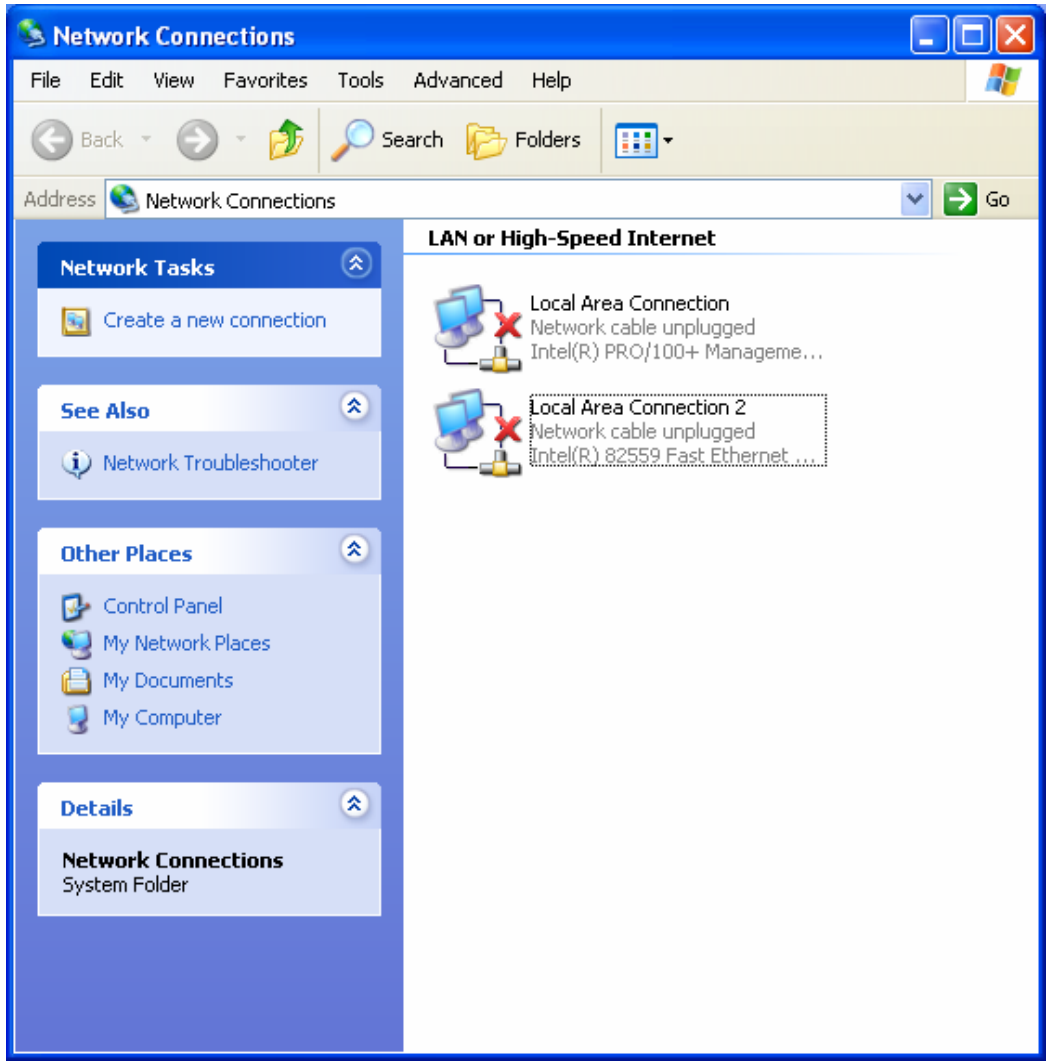


Supplicant Configuration Authentication Method - *PEAP Configuration*

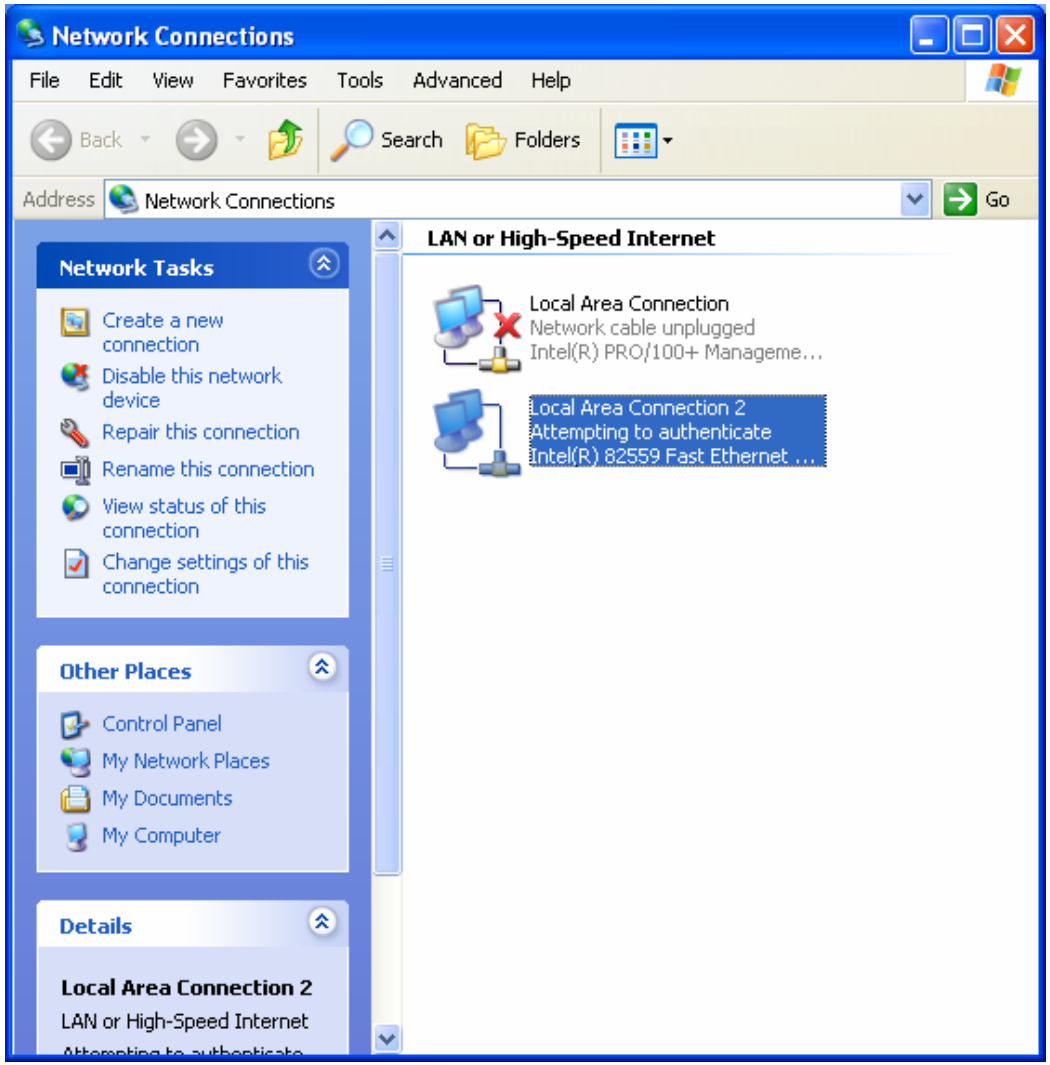




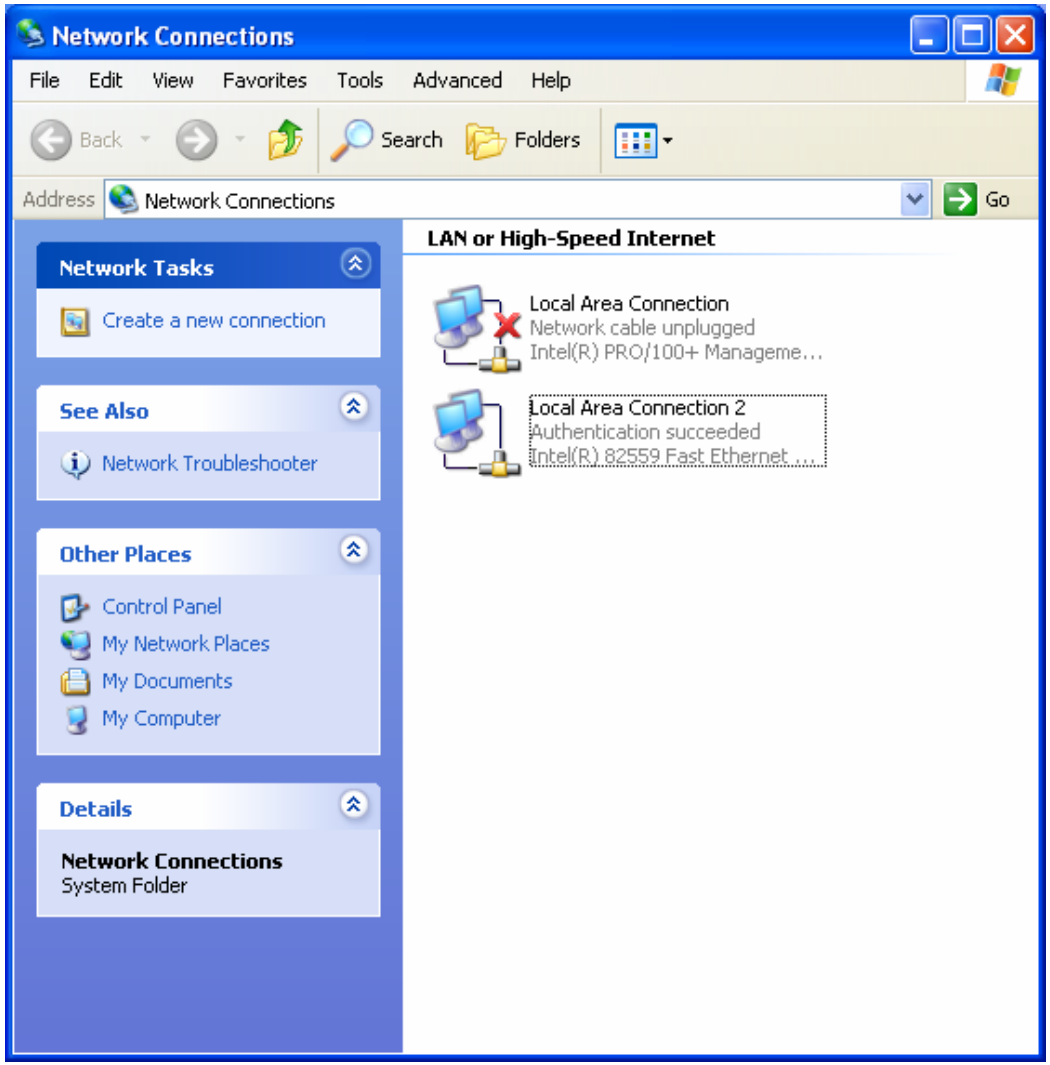
Supplicant Configuration
Interface Status – Disconnected State



Supplicant Configuration
Interface Status – Connected/Authenticating State



Supplicant Configuration
Interface Status – Auth Successful/Connected State



Troubleshooting

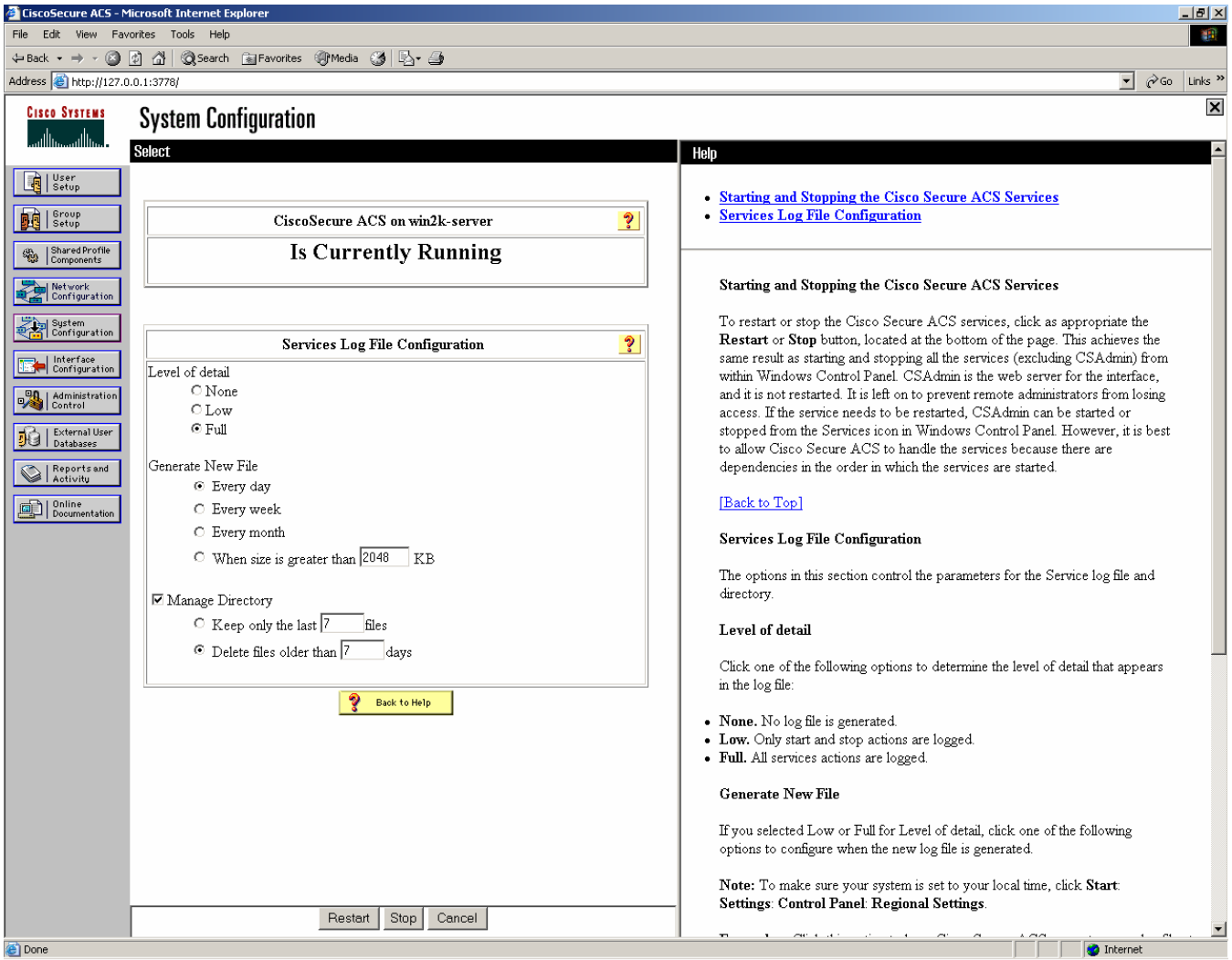
Authentication Server Troubleshooting

Cisco.com

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

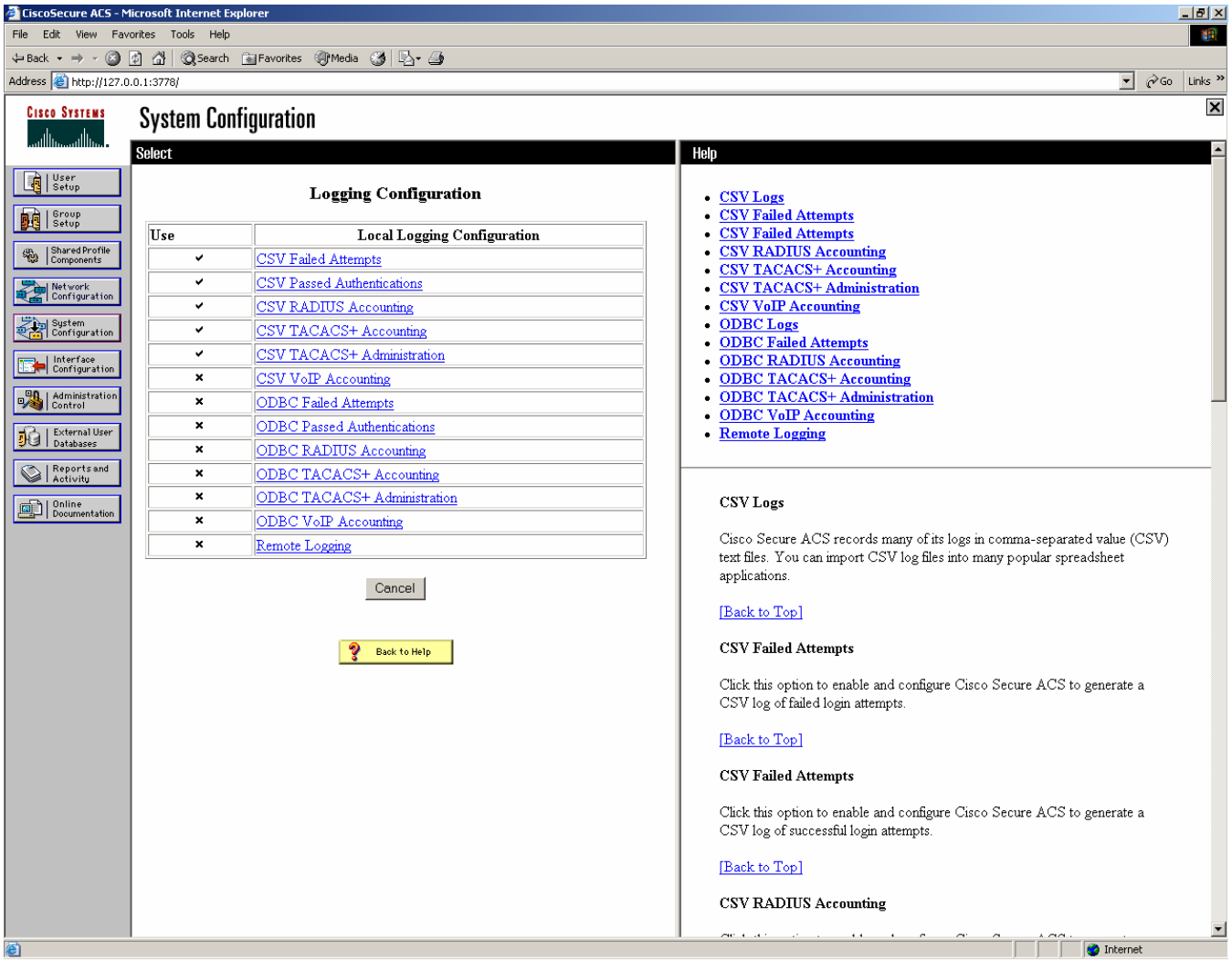
Authentication Server Troubleshooting
Logging Detail Level Configuration

Cisco.com



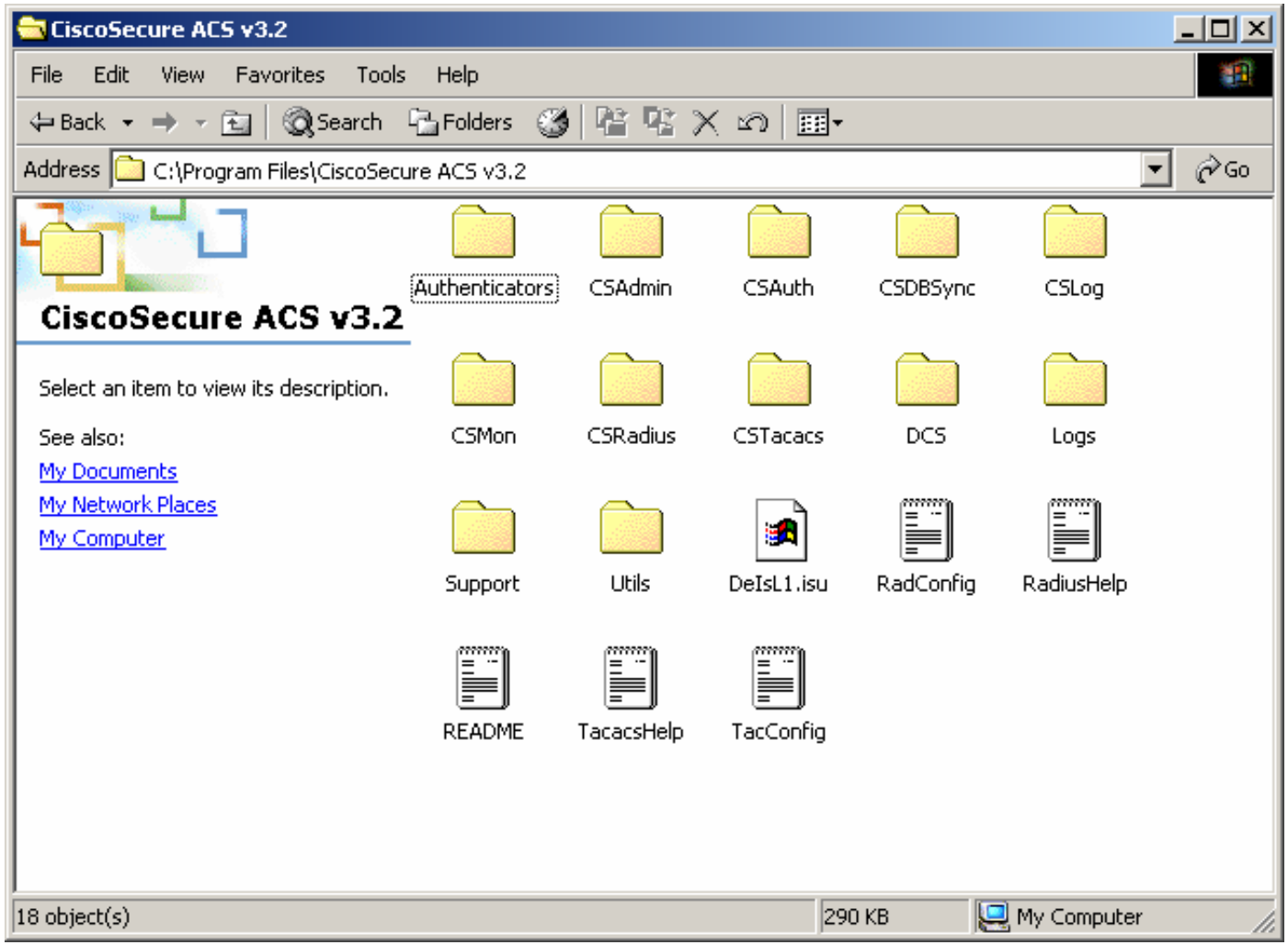
Authentication Server Troubleshooting
General Logging Configuration

Cisco.com



Authentication Server Troubleshooting
Additional Logging File Directories

Cisco.com



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

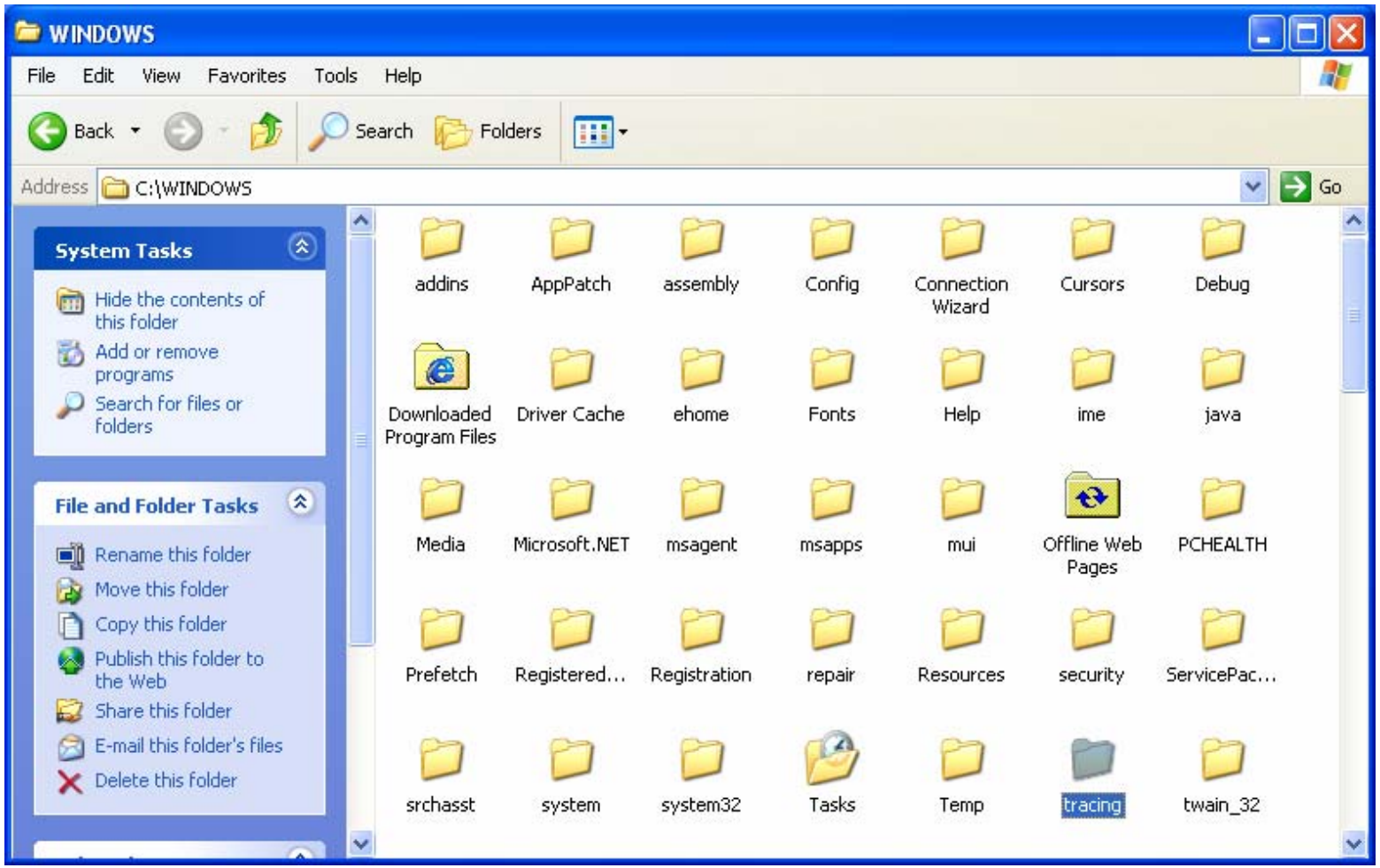
  core: core 802.1x subsystem

  reauthsm: re-authentication FSM

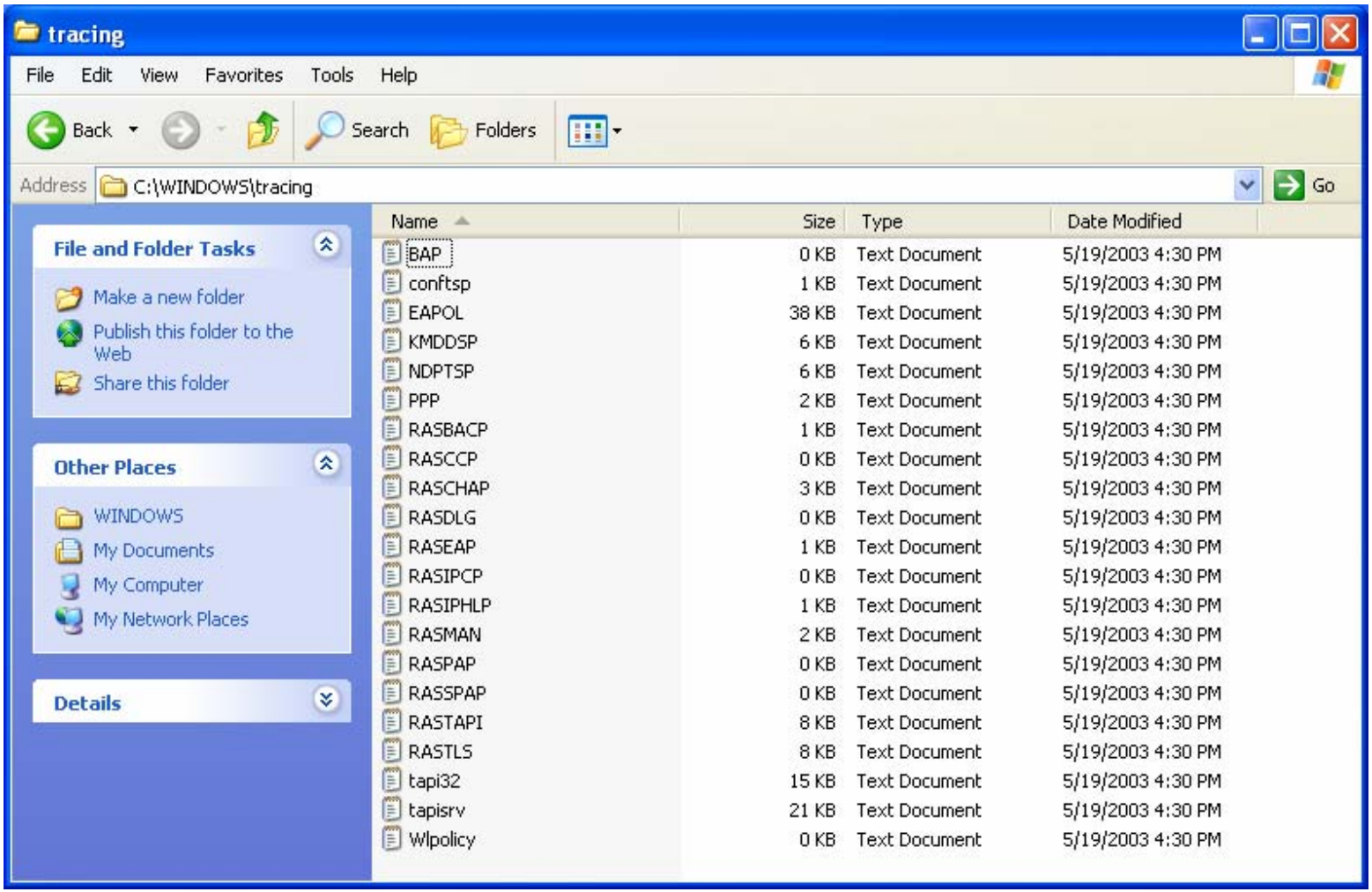
Windows XP/Windows 2000 Troubleshooting

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

Examining the EAPOL log

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

Examining the EAPOL log

[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: ElEapDllWork called for EAP Type 25
[1496] 16:30:37: EAP Dll returned Action=EAPACTION_Send
[1496] 16:30:37: ElEapDllWork finished for EAP Type 25 with error 0
[1496] 16:30:37: ElWriteToPort entered: Pkt Length = 12
[1496] 16:30:37: ElWriteToPort: pPCB = 0009FE78, RefCnt = 3
[1496] 16:30:37: ElWriteToInterface entered
[1496] 16:30:37: ElWriteToInterface completed, RetCode = 0

Examining the EAPOL log

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

Examining the EAPOL log

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

Examining the RASTLS log

[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? (Ian'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)
  - 3rd party devices – Printers (HP)
- **Tighter integration into other Cisco solution sets**
  - Catalyst Integrated Security/Tunneling technologies
  - Antibody
  - CPS
  - NIDS
  - Firewall/FWSM

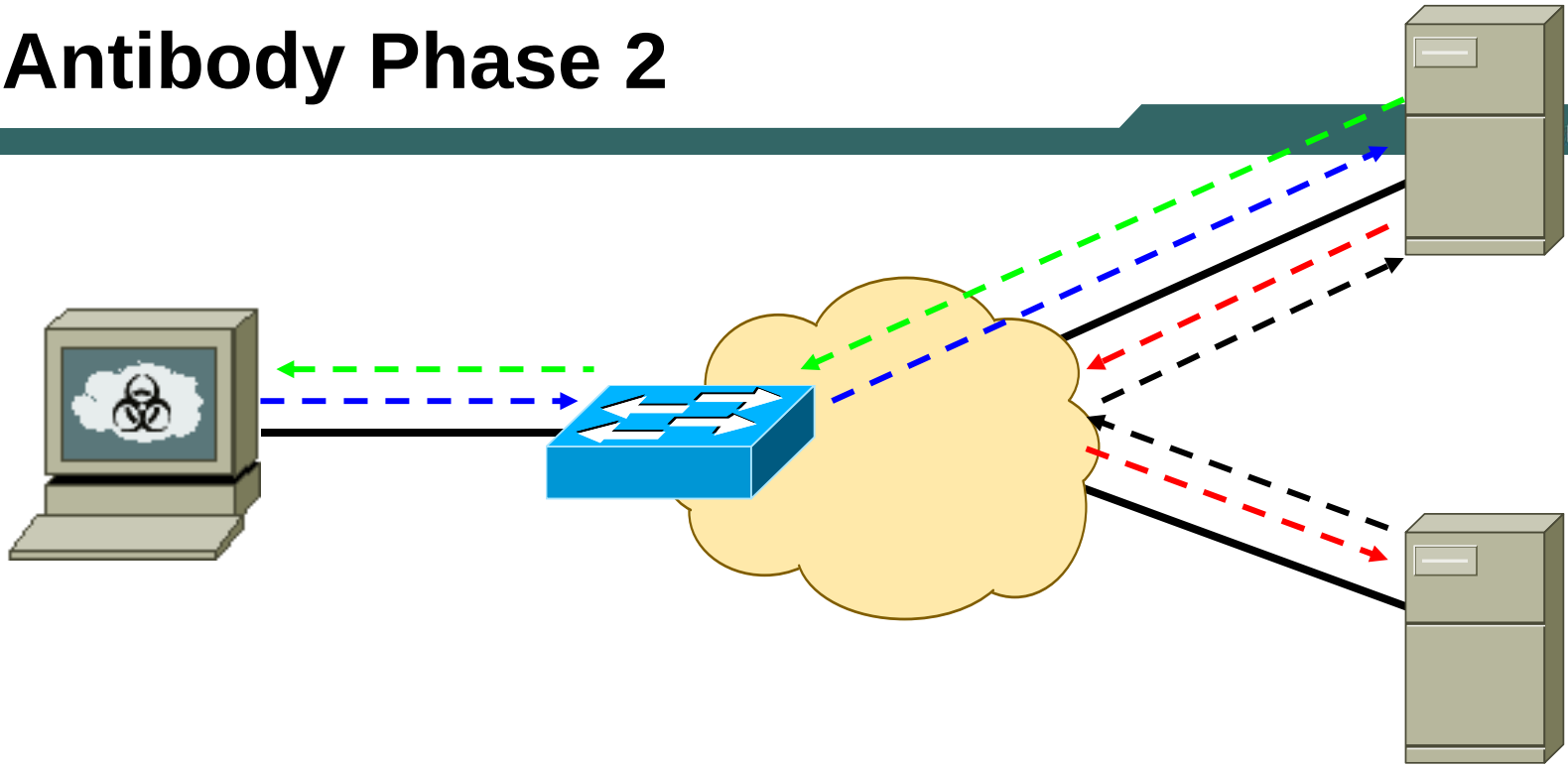
More on my to-do list…

- **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).

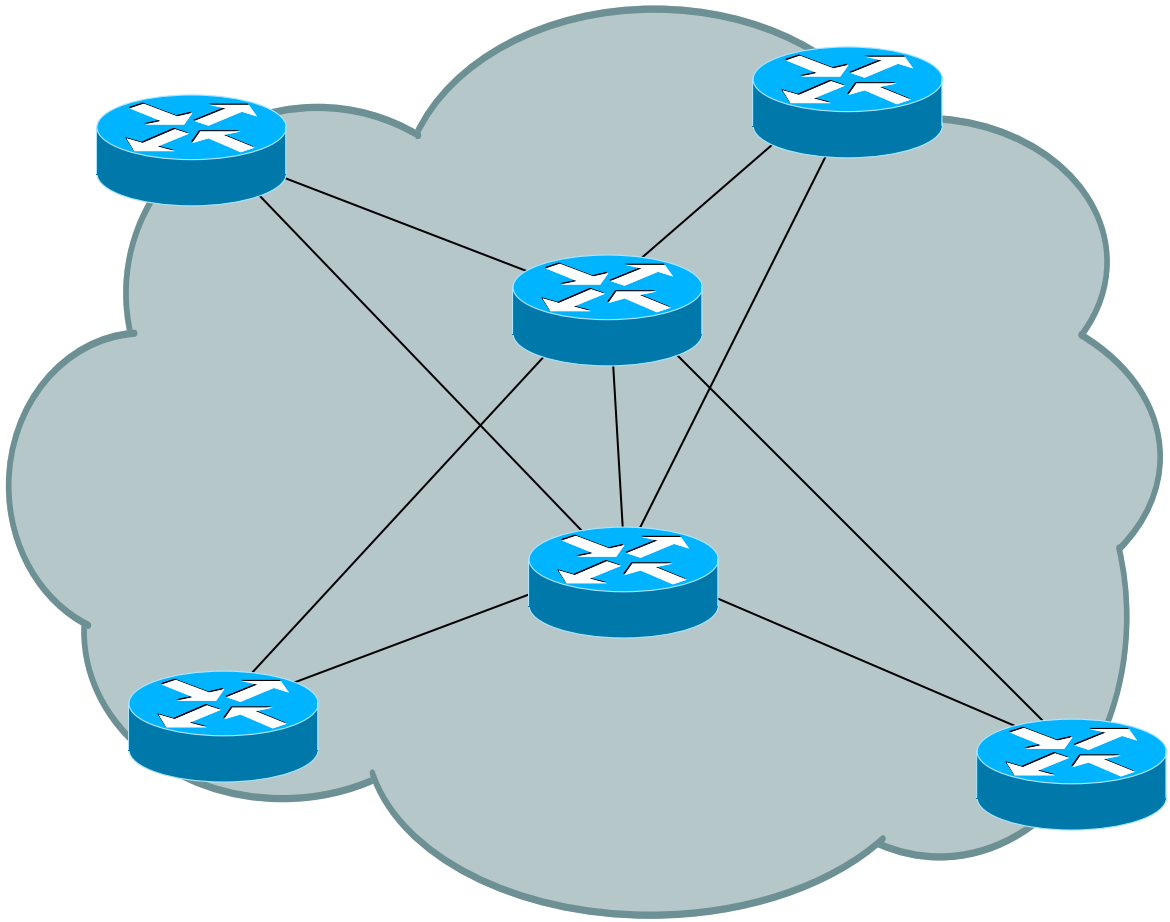
3. Validation Server compares information to acceptable values & sends response back to AAA Server.

4. AAA Server factors in posture information in intelligent decision process and updates network elements.

Cisco Pervasive Security (CPS)

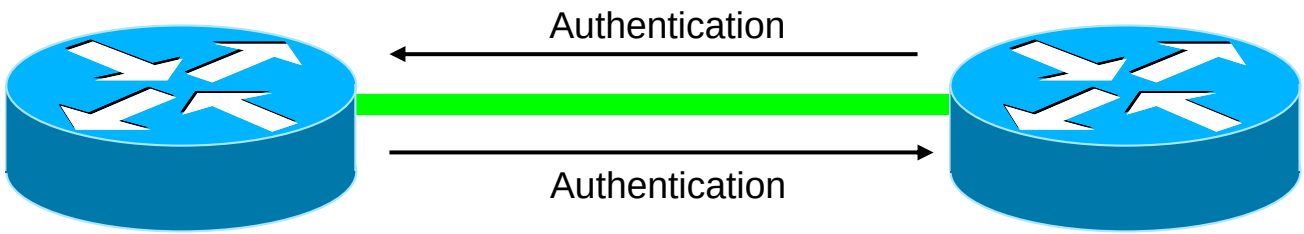
Trusting the Network

Standard Network Core



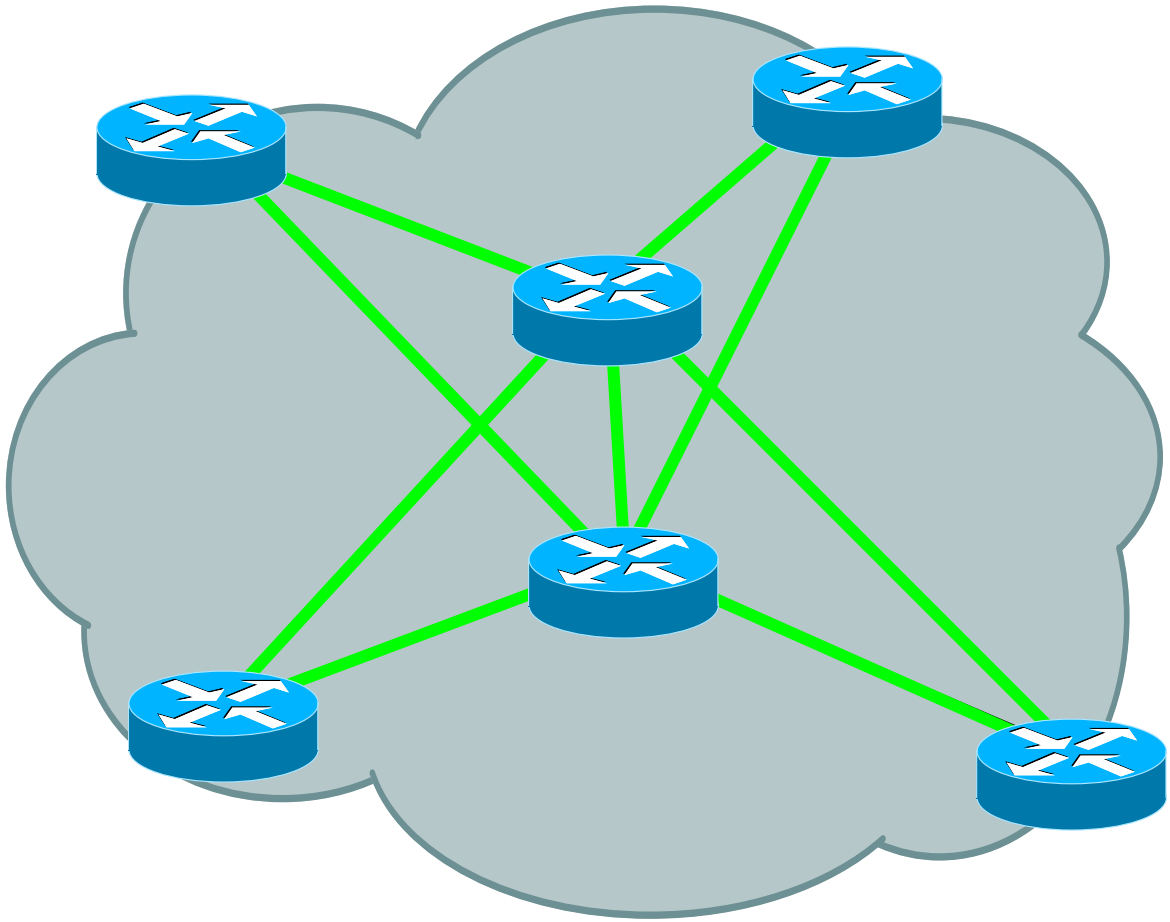
CPS Protected Link

1. Mutual Authentication



2. Encrypted Channel

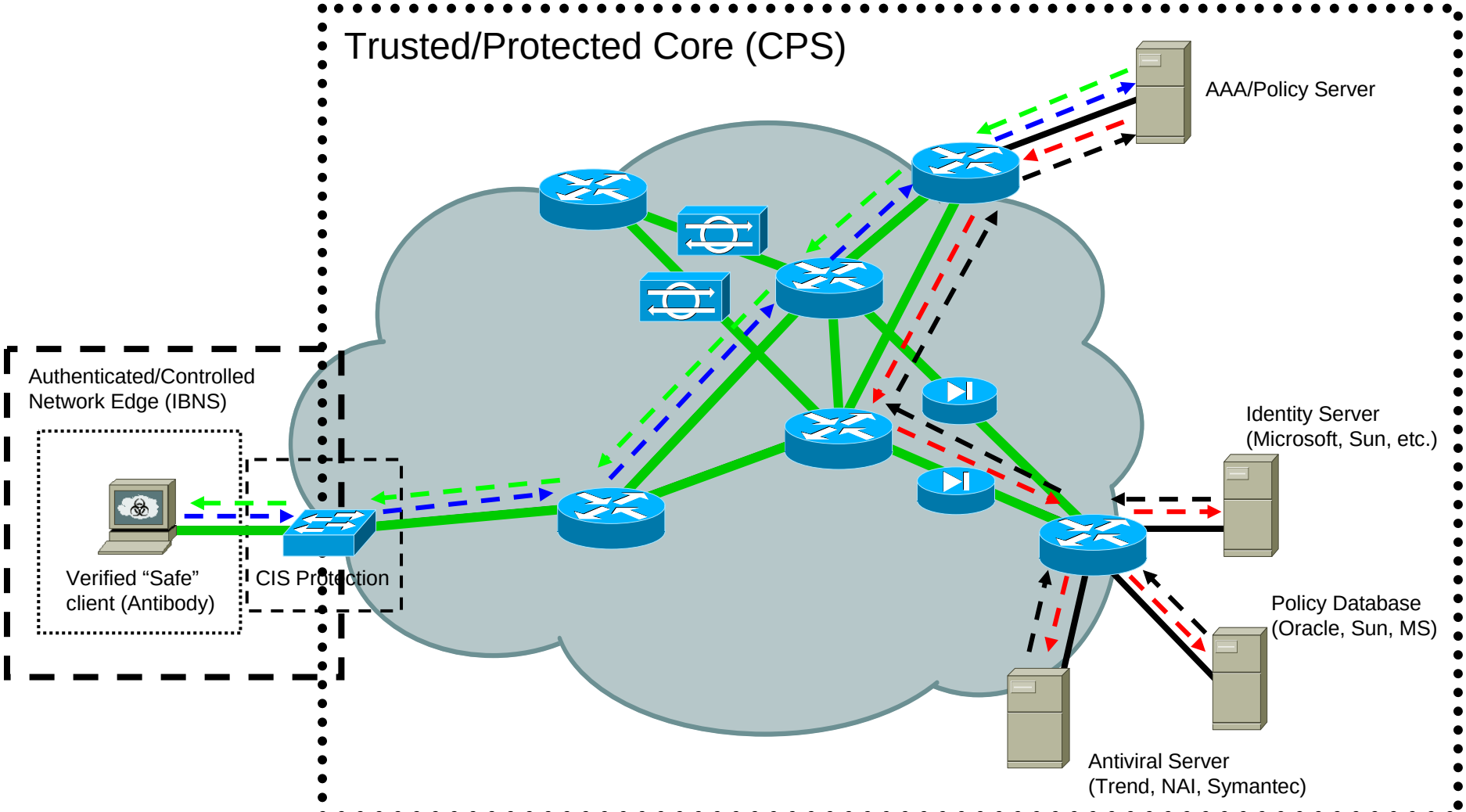
CPS Protected Network Core



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)