Migrating Your LAN to IEEE 802.1X

Gaweł Mikołajczyk
gmikolaj@cisco.com
Consulting Systems Engineer, Emerging Markets East
CCIE #24987, CISSP-ISSAP

Session Objectives

At the end of the session, you should understand:

- How 802.1X works
- The benefits of deploying 802.1X
- How to configure and deploy 802.1X using Cisco switches, ACS 5.1 and various supplicants.
- How to integrate existing technologies such as IP telephony, guest access, PXE, etc
- The value and application of deployment scenarios
- How to make this work when you get back to your lab

You should also:

- Provide us with feedback!

Identity and Authentication Overview

Why Identity Is Important

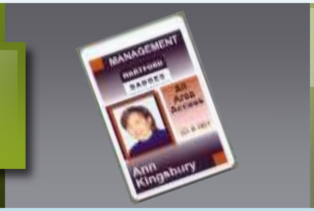
1

Who are you?

802.1X (or supplementary method) authenticates the user

Keep the Outsiders Out

2



Where can you go?

Based on authentication, user is placed in correct VLAN

Keep the Insiders Honest

3

What service level to you receive?

The user can be given per-user services (ACLs today, more to come)

Personalize the Network

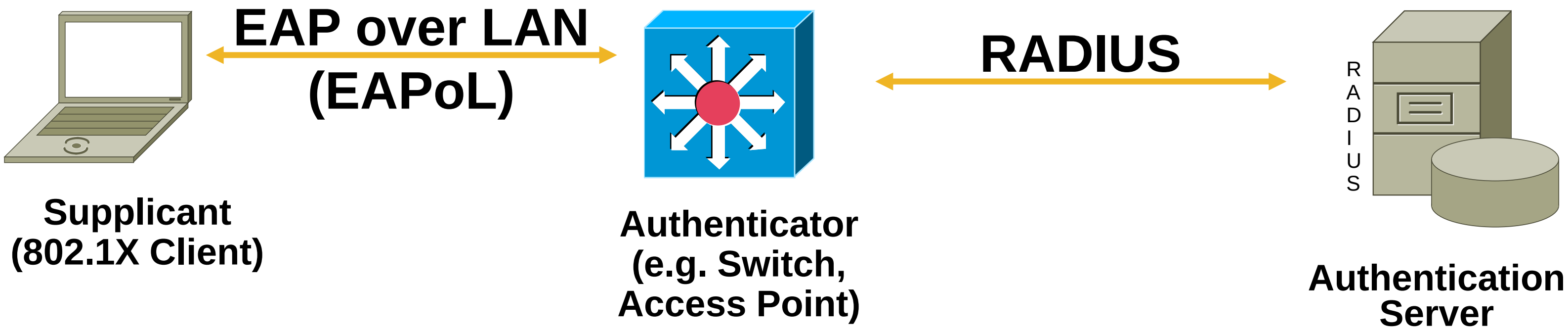
4

What are you doing?

The user's identity and location can be used for tracking and accounting

Increase Network Visibility

IEEE 802.1X: The Foundation of Identity



EAP over LAN (EAPoL)

RADIUS

Supplicant (802.1X Client)

Authenticator (e.g. Switch, Access Point)

Authentication Server

- ✓ IEEE 802.1 working group standard
- ✓ Provides port-based access control using authentication

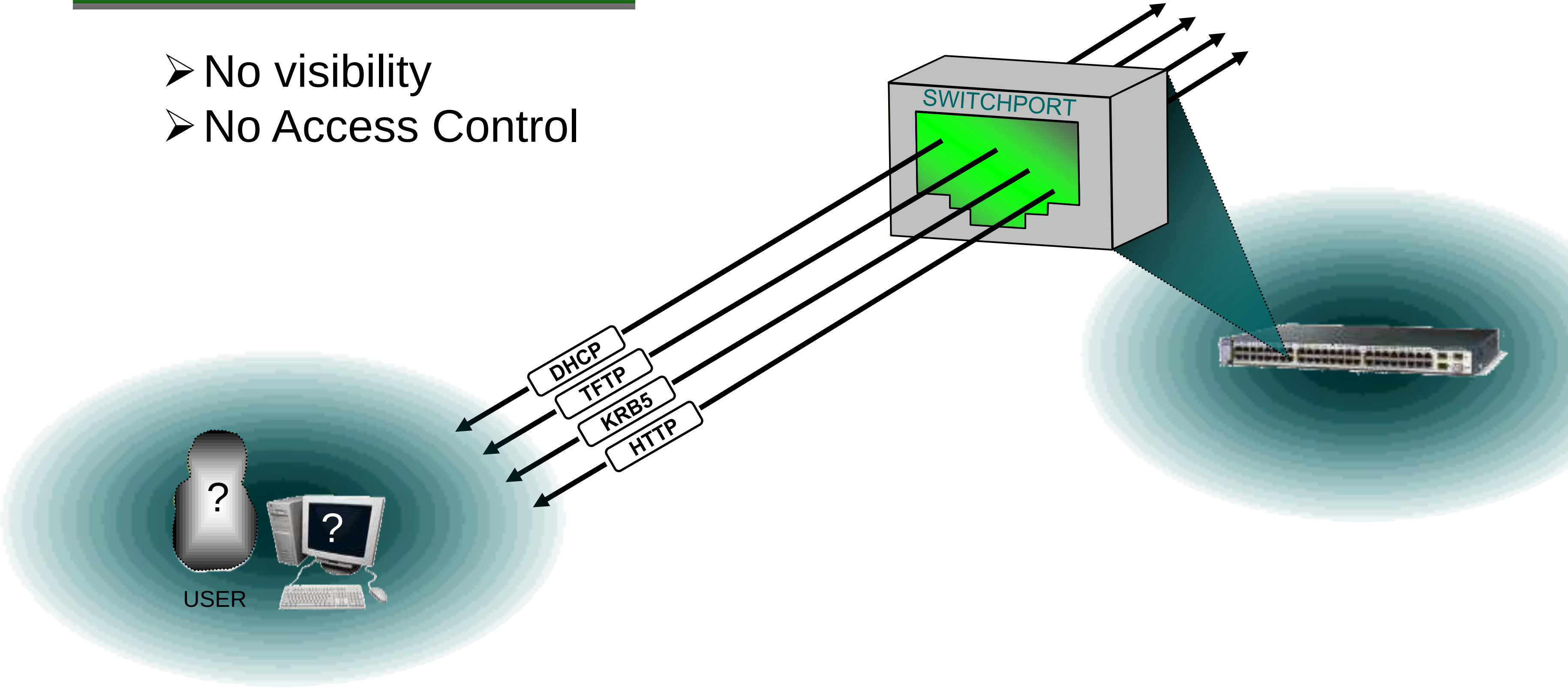
Enforcement via MAC-based filtering and port-state monitoring

Defines encapsulation for Extensible Authentication Protocol (EAP) over IEEE 802 media— “EAPoL”

Default Port State without 802.1X

No Authentication Required

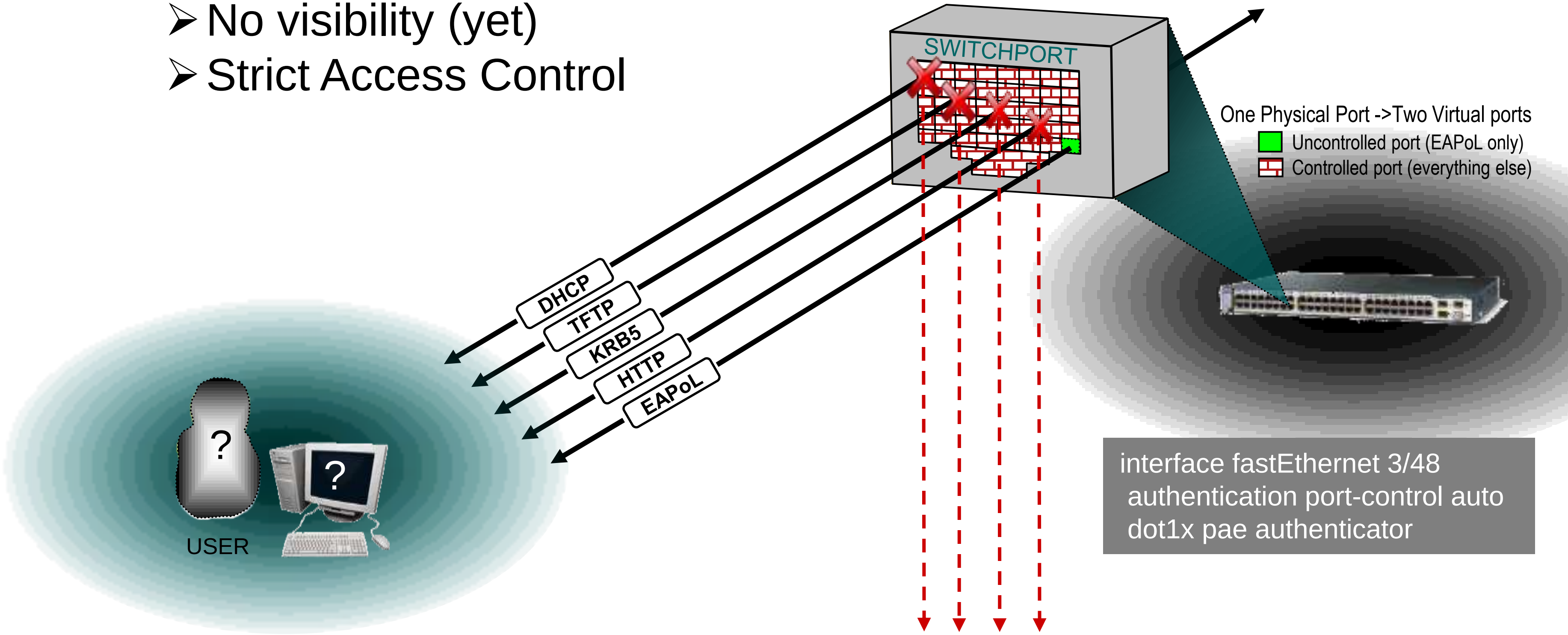
- ➢ No visibility
- ➢ No Access Control



Default Security with 802.1X

Before Authentication

- ➢ No visibility (yet)
- ➢ Strict Access Control


SWITCHPORT
DHCP
TFTP
KRB5
HTTP
EAPoL
?
?
USER
One Physical Port ->Two Virtual ports
🟩 Uncontrolled port (EAPoL only)
▨ Controlled port (everything else)

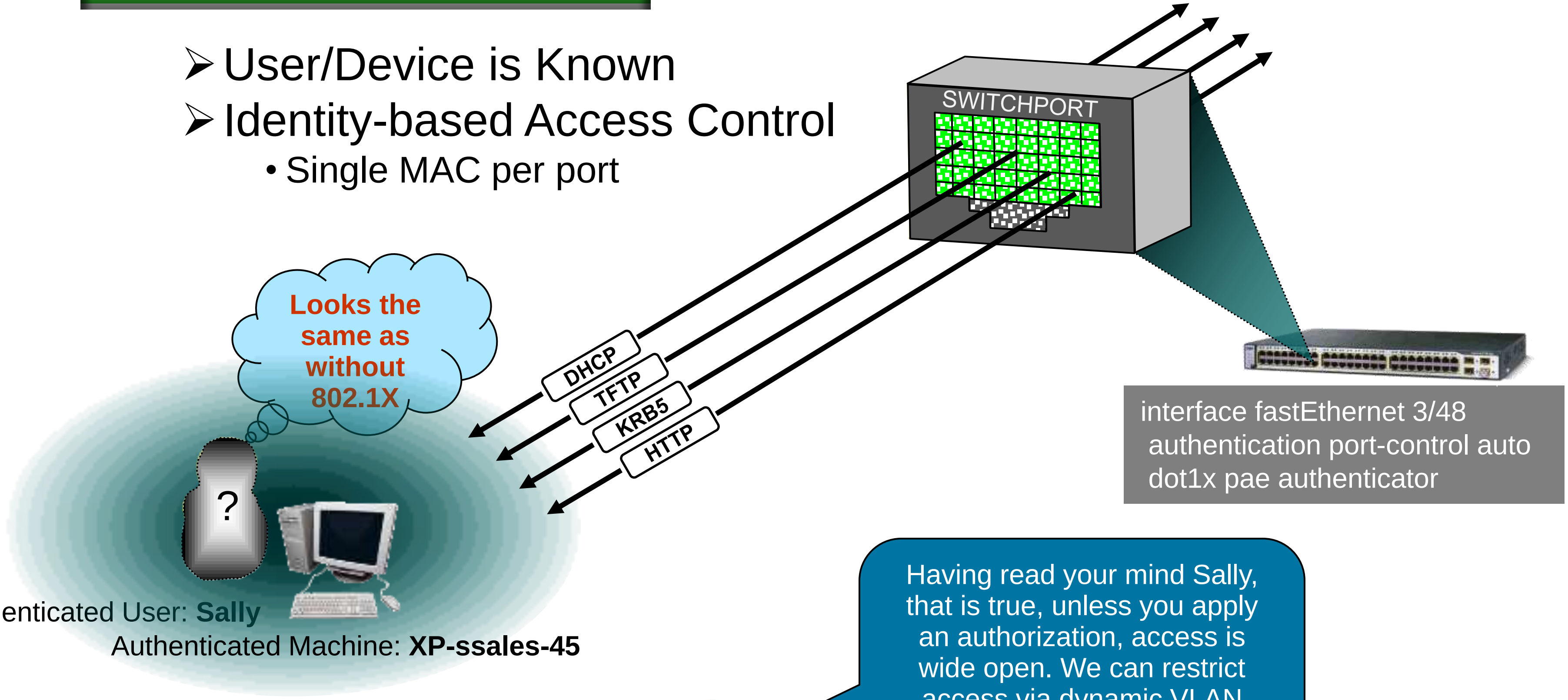
```
interface fastEthernet 3/48
 authentication port-control auto
 dot1x pae authenticator
```

ALL traffic *except* EAPoL is dropped

Default Security with 802.1X

After Authentication

- ➢ User/Device is Known
- ➢ Identity-based Access Control
  - Single MAC per port



Authenticated User: **Sally**

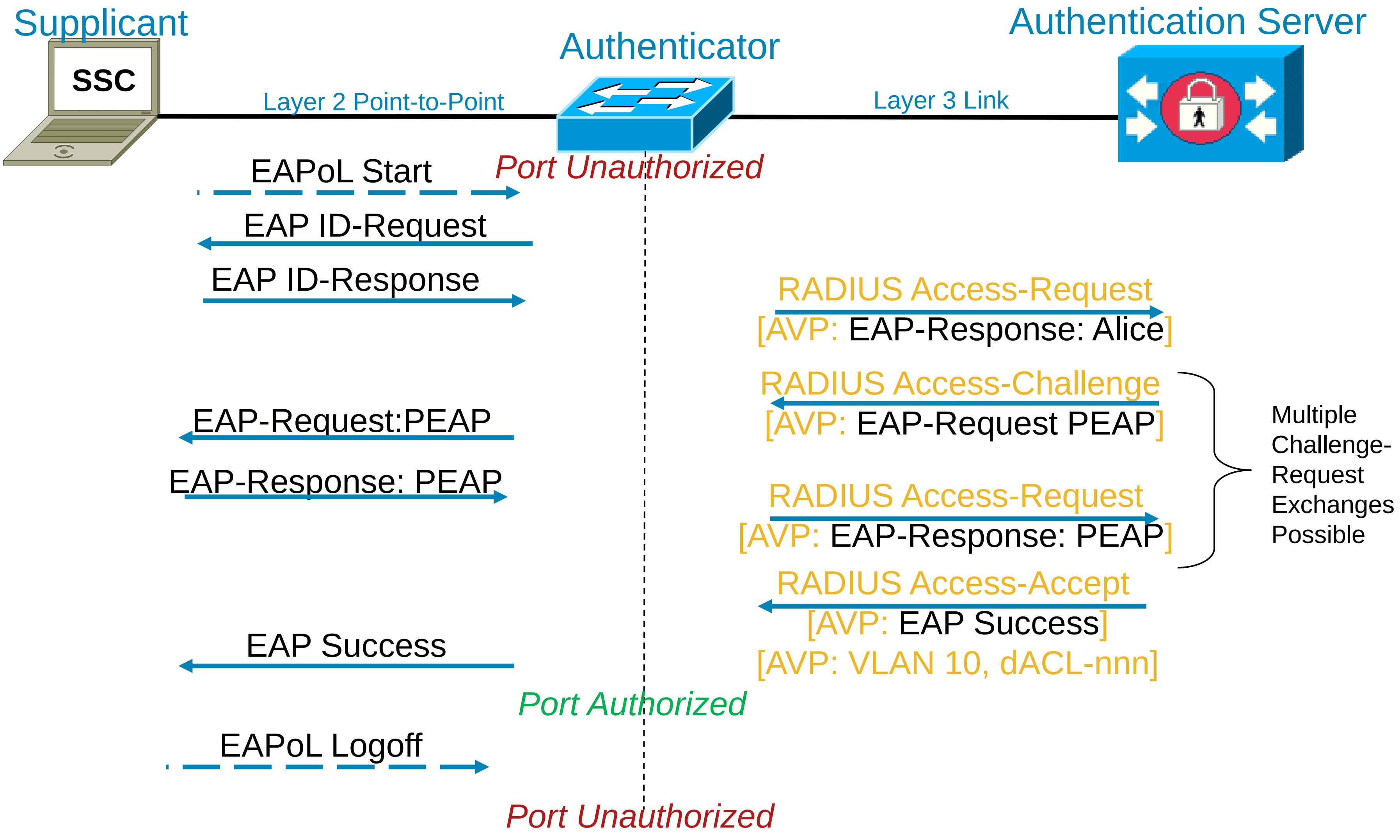
Authenticated Machine: **XP-ssales-45**

```
interface fastEthernet 3/48
 authentication port-control auto
 dot1x pae authenticator
```

Having read your mind Sally, that is true, unless you apply an authorization, access is wide open. We can restrict access via dynamic VLAN assignment or downloadable ACLs

Identity and Authentication
802.1X, EAP, and RADIUS

A Closer Look at 802.1X



Supplicant

SSC

Layer 2 Point-to-Point

Authenticator

Layer 3 Link

Authentication Server

EAPoL Start

Port Unauthorized

EAP ID-Request

EAP ID-Response

RADIUS Access-Request

[AVP: EAP-Response: Alice]

RADIUS Access-Challenge

[AVP: EAP-Request PEAP]

EAP-Request:PEAP

Multiple Challenge-Request Exchanges Possible

EAP-Response: PEAP

RADIUS Access-Request

[AVP: EAP-Response: PEAP]

RADIUS Access-Accept

[AVP: EAP Success]

[AVP: VLAN 10, dACL-nnn]

EAP Success

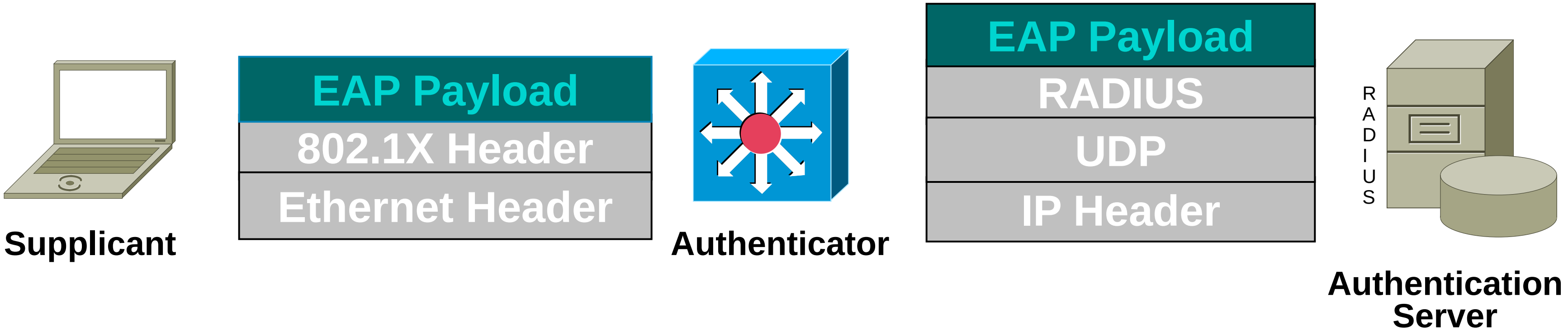
Port Authorized

EAPoL Logoff

Port Unauthorized

What Does EAP Do?

- Establishes and manages connection
- Allows authentication by encapsulating various types of authentication exchanges
  - Actual authentication exchanges are called *EAP Methods*
- Provides a flexible link layer security framework
  - Can run over any link layer (PPP, 802, etc.)
- Defined by RFC 3748



EAP Authentication Methods

Challenge-response-based

- MD5: uses MD5 based challenge-response for authentication
- LEAP: username/password authentication
- EAP-MSCHAPv2: username/password MSCHAPv2 challenge-response authentication

Cryptographic-based

- EAP-TLS: x.509 v3 PKI certificates and the TLS mechanism for authentication

Tunneling methods

- PEAP: encapsulates other EAP types in an encrypted tunnel
- EAP-TTLS: encapsulates other EAP types in an encrypted tunnel
- EAP-FAST: designed to not require client certificates

Other

- EAP-GTC: generic token and OTP authentication
- EAP-SIM : SIM-based authentication

Tunneling Methods

- Some EAP methods setup an encrypted tunnel and pass credentials through the tunnel
- Anonymous outer identity - Provides the ability to completely obfuscate the user’s credentials

  SSC / ACS – Yes

  Windows Native / IAS - No
- Some EAP methods require an EAP method inside the tunnel (PEAP and FAST)
- Some EAP methods do not require an EAP method inside the tunnel (TTLS) – used with legacy RADIUS

EAP Protocols: Feature Support

	EAP-TLS	PEAP	EAP-FAST
Single Sign-on	Yes	Yes	Yes
Login Scripts (Active Directory)	Yes	Yes	Yes
Password Expiration (AD)	N/A	Yes	Yes
Client and OS Availability	SSC, XP, Win7 and Others	SSC, XP, Win7 and Others	SSC, Win7 and Others
MS DB Support	Yes	Yes	Yes
LDAP DB Support	Yes	Yes	Yes
OTP Support	No	Yes	Yes
Off-line Dictionary Attacks	No	No	No
Server Certificates Required	Yes	Yes	No
Client Certificates Required	Yes	No	No
Computing Impact	High	Medium	Low

Factors that Drive EAP Method

Use as many methods as needed depending on devices

Enterprise security policy

- Certificate Authority deployment may drive EAP type
- Two factor authentication may require EAP-TLS
- Security vs. Convenience Trade-offs

Client support

- Windows supports EAP-TLS, PEAP w/EAP-MSCHAPv2, PEAP w/EAP-TLS
- 3rd party supplicants support a large variety of EAP types, but not all

Authentication server support

- RADIUS servers support a large variety of EAP types, but not all

Identity store

- PEAP w/EAP-MSCHAPv2 can only be used with authentication stores that store passwords in MSCHAPv2 format
- Not every identity store supports all the EAP types

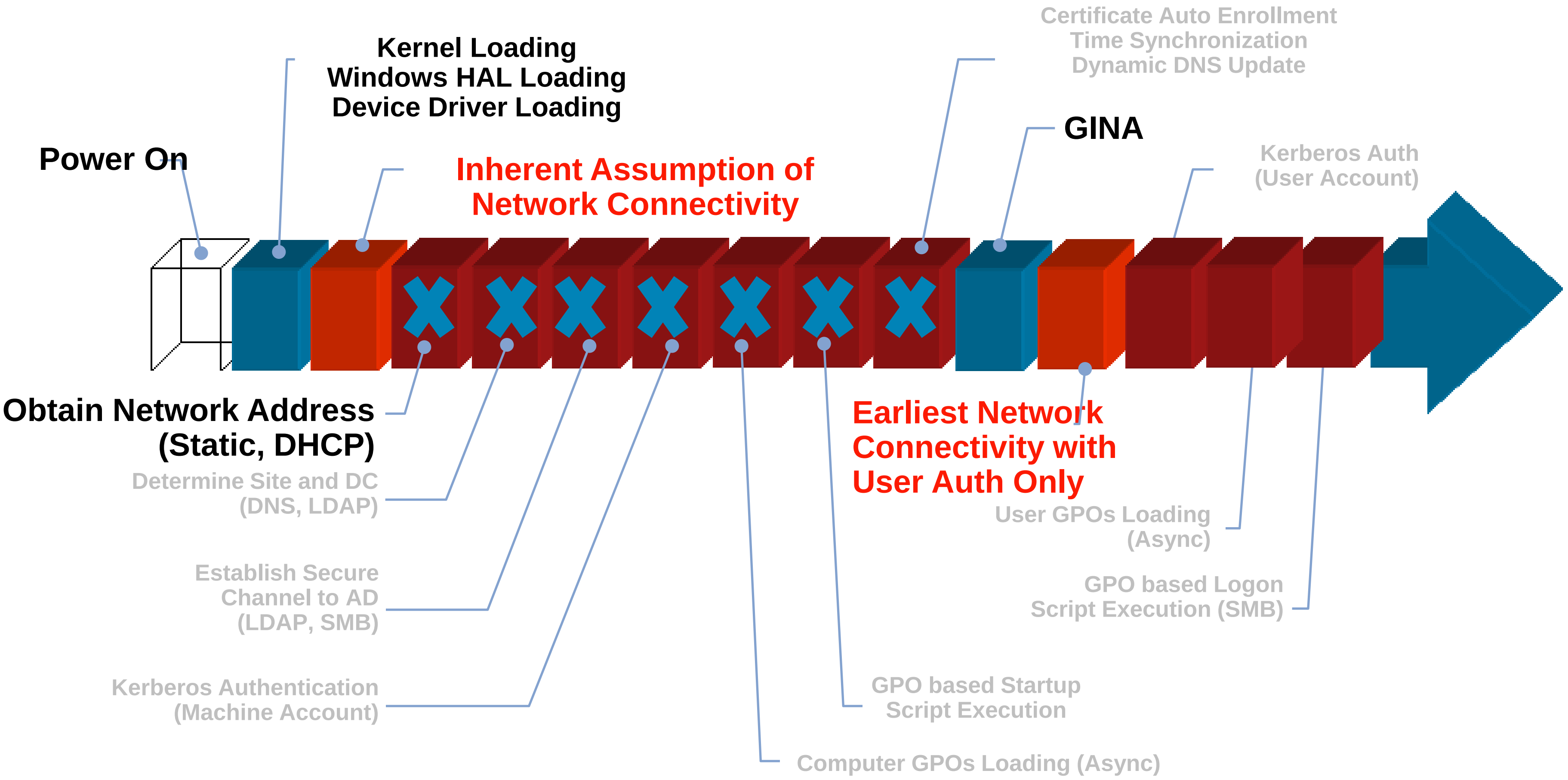
Identity & Authentication:
Who (or What) Authenticates?

Problem Statement

- Who should the network authenticate ?
  - A user using a device
  - A device
  - Both the user and the device
- Device boot process and network connectivity assumption
  - Boot without using network resource - Standalone
  - Boot from the network – Xterm, NetPC, PXE
  - Boot and use network resources – networked
    - Network File System
    - Managed devices : Connection to LDAP, Active Directory
    - Device health check : Patch level checker, Central AV system

Example: Network Assumption

Microsoft Windows



Power On

Kernel Loading
Windows HAL Loading
Device Driver Loading

Inherent Assumption of
Network Connectivity

Certificate Auto Enrollment
Time Synchronization
Dynamic DNS Update

GINA

Kerberos Auth
(User Account)

Obtain Network Address
(Static, DHCP)

Determine Site and DC
(DNS, LDAP)

Establish Secure
Channel to AD
(LDAP, SMB)

Kerberos Authentication
(Machine Account)

Earliest Network
Connectivity with
User Auth Only

User GPOs Loading
(Async)

GPO based Logon
Script Execution (SMB)

GPO based Startup
Script Execution

Computer GPOs Loading (Async)

🟥 Components that depend on network connectivity

✗ Components broken with 802.1X *user* authentication only

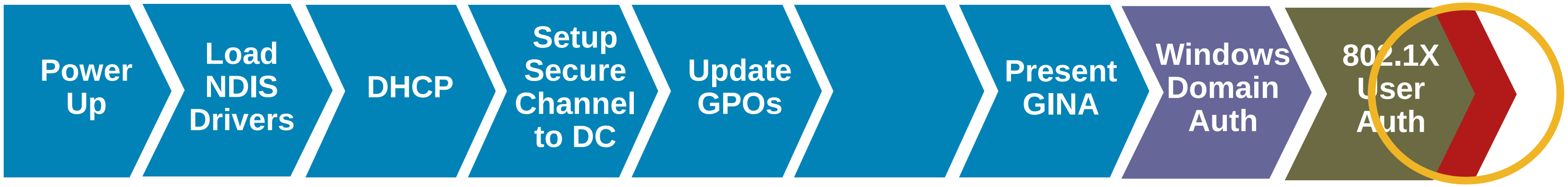
802.1X Device and User authentication

- User authentication ONLY
  - Possible when no dependency of the device used regarding network resources
  - Can run user script to access network resources post login.
  - Be careful, this can breaks Microsoft group and system policies
- Device authentication ONLY
  - Mandatory as soon as exist dependency of Network resources
  - Authorization is link to the device; not the user using the device
- Device and User
  - Authorization is highly flexible
    - Advanced features needed on supplicants
    - Synchronization needed with others applications & process on the client PC : DHCP, DNS, NFS, etc..
    - Switches contexts when going from one to the other

MICROSOFT Windows Example

User and Device Authentication

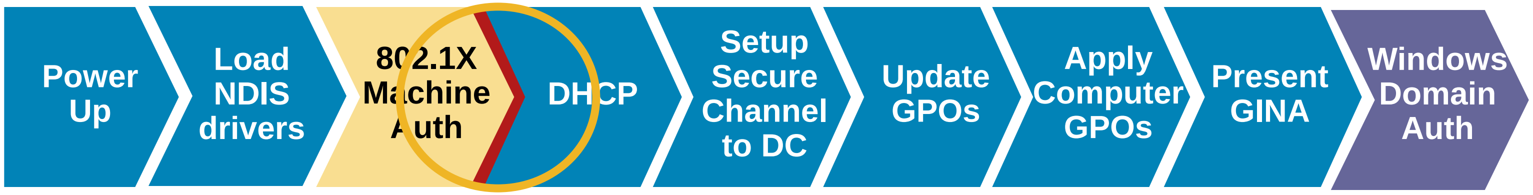
User Authentication



Power Up
Load NDIS Drivers
DHCP
Setup Secure Channel to DC
Update GPOs
Present GINA
Windows Domain Auth
802.1X User Auth

*** No Connectivity to Domain Controller Until User Logs In**

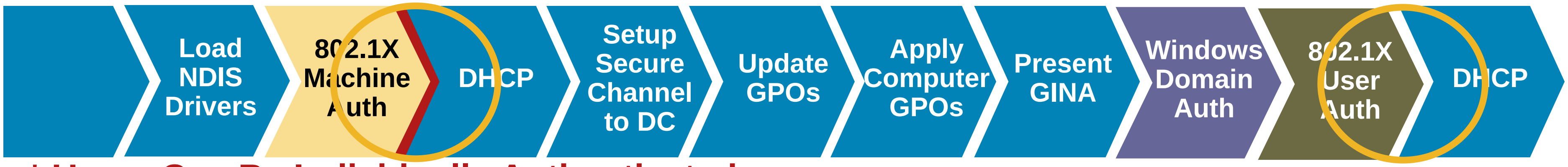
Machine Authentication



Power Up
Load NDIS drivers
802.1X Machine Auth
DHCP
Setup Secure Channel to DC
Update GPOs
Apply Computer GPOs
Present GINA
Windows Domain Auth

*** 802.1X Early in Boot Process**

User + Machine Authentication



Load NDIS Drivers
802.1X Machine Auth
DHCP
Setup Secure Channel to DC
Update GPOs
Apply Computer GPOs
Present GINA
Windows Domain Auth
802.1X User Auth
DHCP

*** Users Can Be Individually Authenticated**

▶ **Network Connectivity**

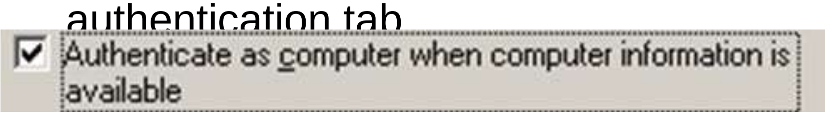
○ **Point of 802.1X Authorization**

Configuring Machine and/or User Auth

Microsoft Windows Example

- Mode is supplicant dependent
- Native MS supplicants pre-Win7

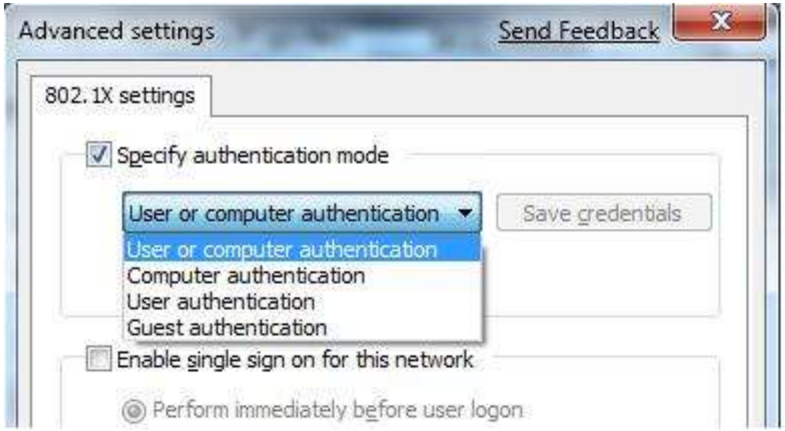
  Controlled by registry keys (SP2) or XML (SP3 & Vista) & network properties authentication tab



☑ Authenticate as computer when computer information is available

  Can be set by GPO (Wireless only for XP, Wired and Wireless for Vista)

- Win7 supplicants



☑ Specify authentication mode

User or computer authentication ▾ | Save credentials

User or computer authentication
Computer authentication
User authentication
Guest authentication

□ Enable single sign on for this network

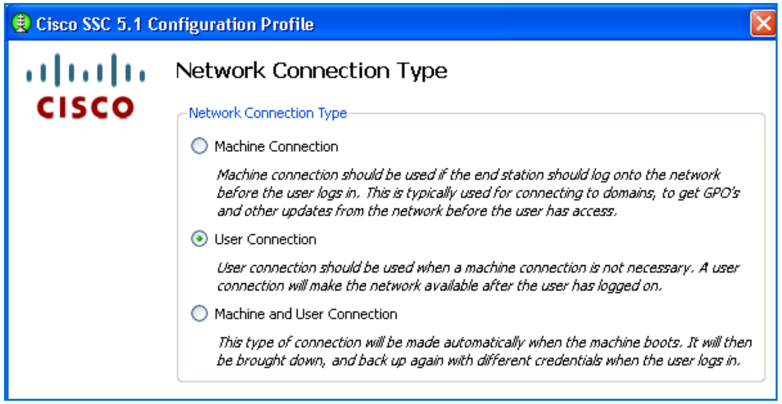
● Perform immediately before user logon

- Cisco SSC

  Can be configured per profile

  Centrally configured via Admin tool

  Deployed via MSI



Network Connection Type

Network Connection Type

○ Machine Connection

Machine connection should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

● User Connection

User connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on.

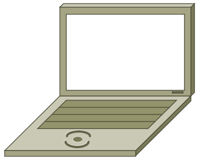
○ Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

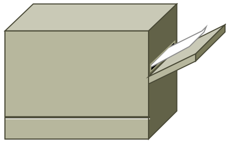
Identity & Authentication: 802.1X Supplicants

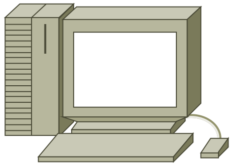
802.1X Supplicants

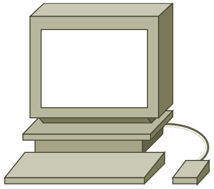
- Windows Win7— Yes
- Windows Vista —Yes
- Windows XP—Yes
- Windows 2000—Yes
- Windows CE / Mobile — Yes
- Linux —Yes
- HP-UX —Yes
- Solaris —Yes
- HP printers & switches —Yes
- Apple OS X —Yes
- Apple iPhone — Yes
- Nokia —Yes
- Cisco IP Phone —Yes
- Cisco AP —Yes
- Cisco Switches — Yes (12.2.50)

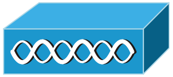

Windows

7921


HP Jet Direct


Solaris


Apple


WLAN APs

IP Phones

Pocket PC

PC Supplicants Types

- Operating System – MAC OS X, XP Wireless Zero Config, Vista Native, Win7 Native
- Hardware Specific – Intel Proset, Lenovo Access Connections
- Premium – Cisco Secure Services Client, Juniper Odyssey
- Open Source –

  Xsupplicant (Open 1X) – http://open1x.sourceforge.net/

  WPA supplicant - http://hostap.epitest.fi/wpa_supplicant/

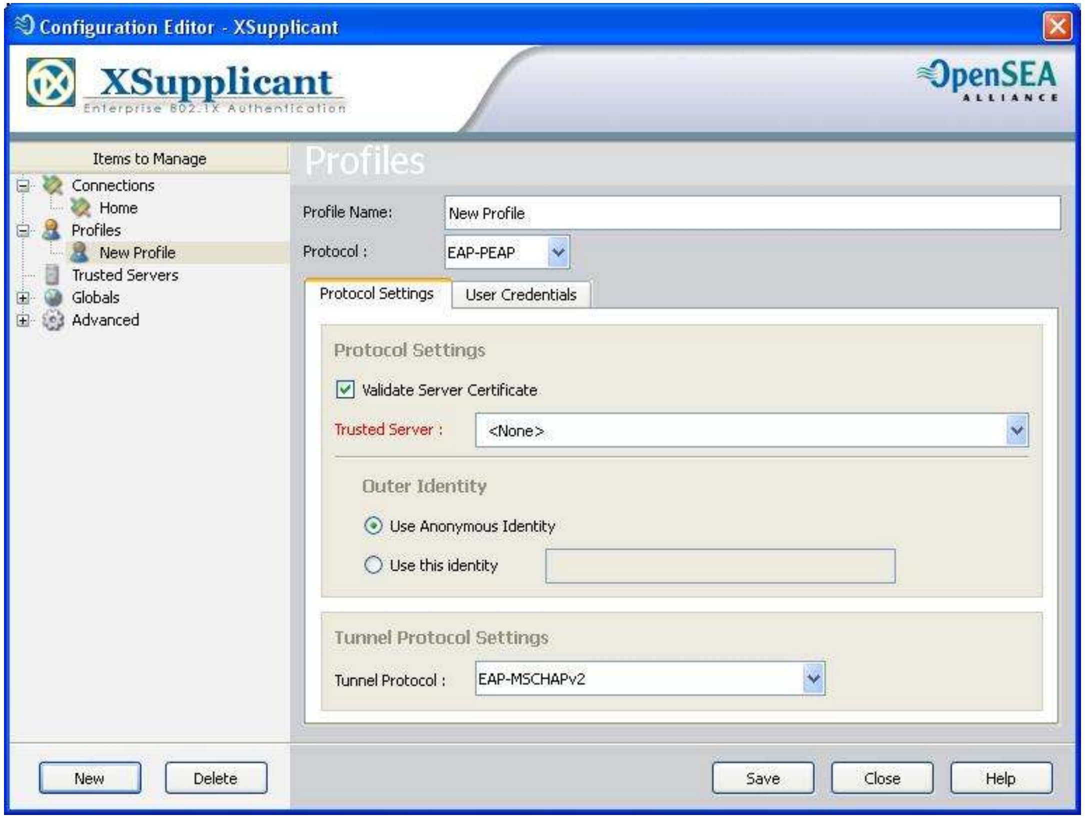
  Secure W2 - http://www.securew2.com/

Xsupplicant

- Open Source
- No additional up-front cost
- Username / Password
- Manual Connect
- User Authentication
- Server Validation
- Wired & wireless
- PEAP, TTLS, FAST, and MD5
- Application –

  Simple Authentication

  No outside support required



Configuration Editor - XSupplicant

XSupplicant
Enterprise 802.1X Authentication

Profiles

Profile Name: New Profile

Protocol : EAP-PEAP

Protocol Settings

☑ Validate Server Certificate

Trusted Server : <None>

Outer Identity

● Use Anonymous Identity

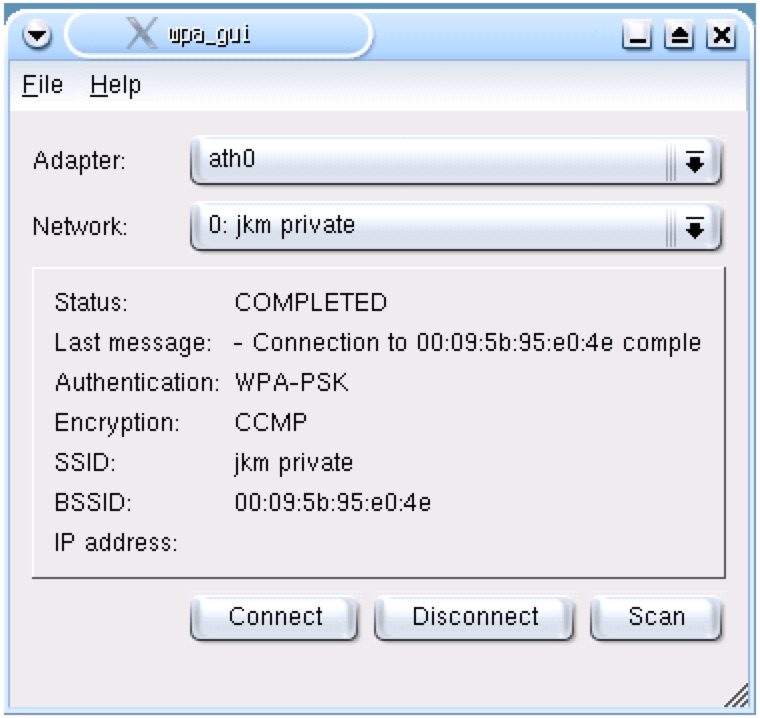
○ Use this identity

Tunnel Protocol Settings

Tunnel Protocol : EAP-MSCHAPv2

WPA Supplicant

- Open Source
- Linux, BSD, Mac OS X, and Windows
- No additional up-front cost
- Wired & wireless
- EAP-TLS EAP-PEAP/MSCHAPv2-TLS–GTC-OTP-MD5 EAP-TTLS/MD5-GTC-OTP-MSCHAPV2-TLS-PAP-CHAP EAP-SIM EAP-AKA EAP-PSK EAP-FAST EAP-PAX EAP-SAKE EAP-IKEv2 EAP-GPSK (experimental) LEAP



Adapter: ath0

Network: 0: jkm private

Status: COMPLETED

Last message: - Connection to 00:09:5b:95:e0:4e comple

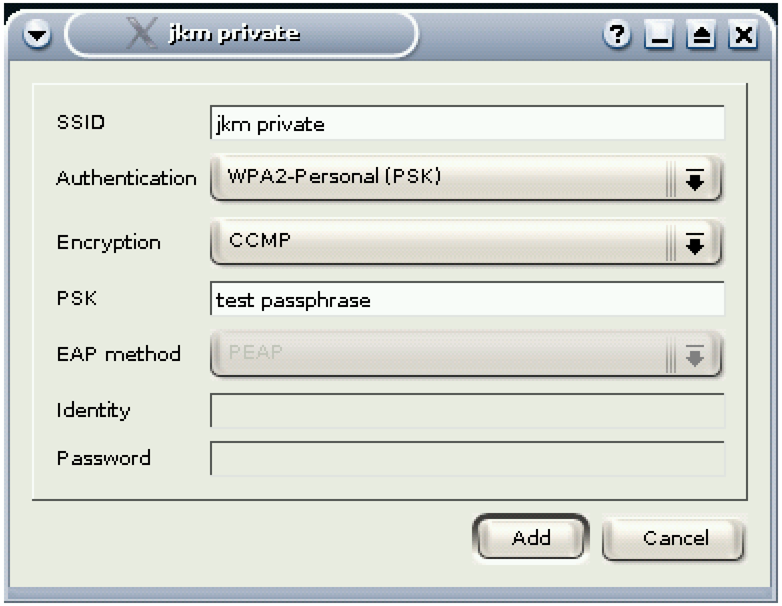
Authentication: WPA-PSK

Encryption: CCMP

SSID: jkm private

BSSID: 00:09:5b:95:e0:4e

IP address:



SSID: jkm private

Authentication: WPA2-Personal (PSK)

Encryption: CCMP

PSK: test passphrase

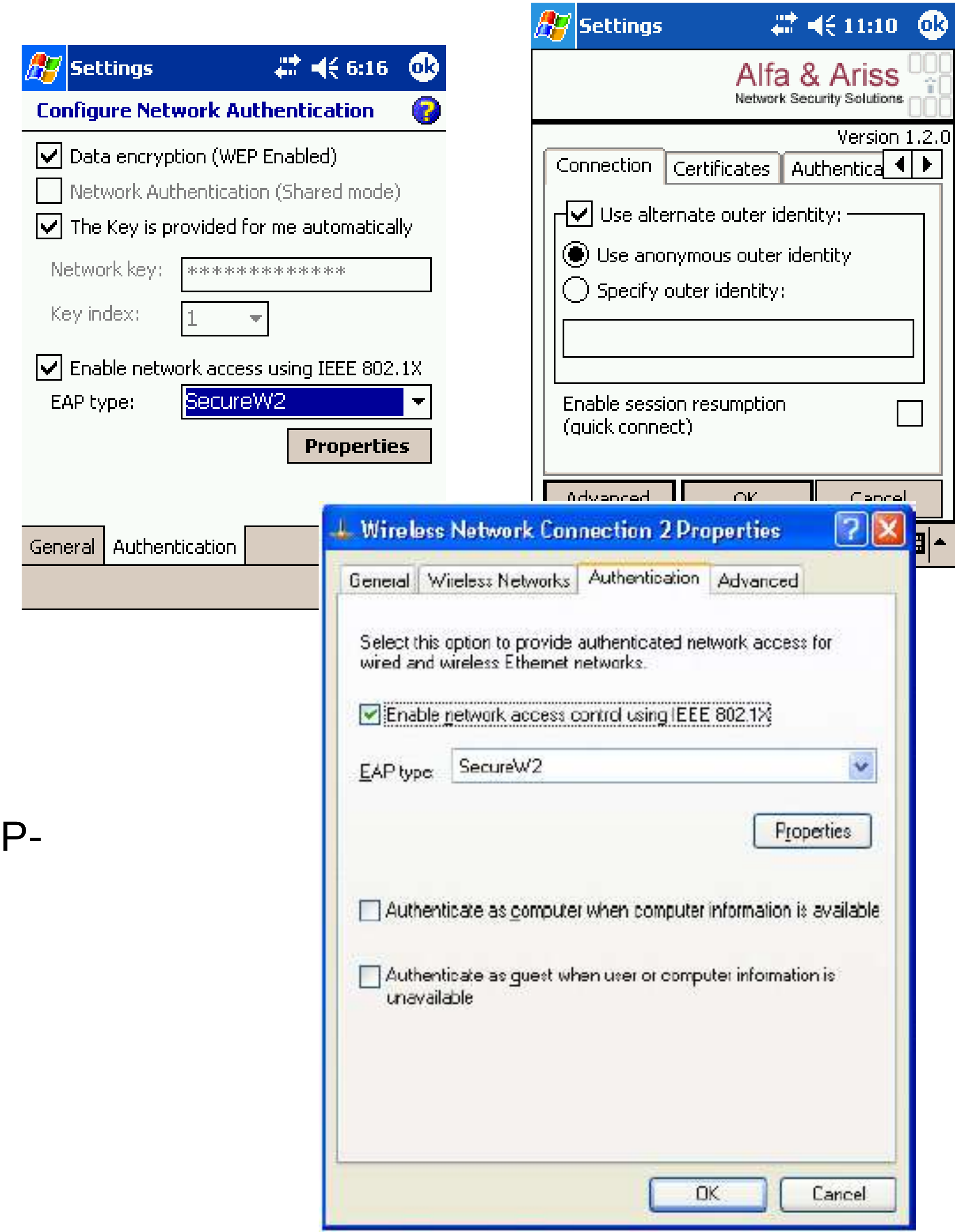
EAP method: PEAP

Identity:

Password:

Secure W2

- Open Source
- Windows suite with Windows Mobile 5/6 or Pocket PC 2003/2005 support and 2000/XP/Vista
- Support available
- Wired & wireless
- Plug-in in existing Microsoft 802.1X/EAP(EapHost)
- Support of EAP-TTLS and EAP-GTC



Configure Network Authentication

☑ Data encryption (WEP Enabled)

□ Network Authentication (Shared mode)

☑ The Key is provided for me automatically

Network key: *************

Key index: 1

☑ Enable network access using IEEE 802.1X

EAP type: SecureW2

Alfa & Ariss
Network Security Solutions

Version 1.2.0

☑ Use alternate outer identity:

● Use anonymous outer identity

○ Specify outer identity:

Enable session resumption (quick connect) □

Wireless Network Connection 2 Properties

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

☑ Enable network access control using IEEE 802.1X

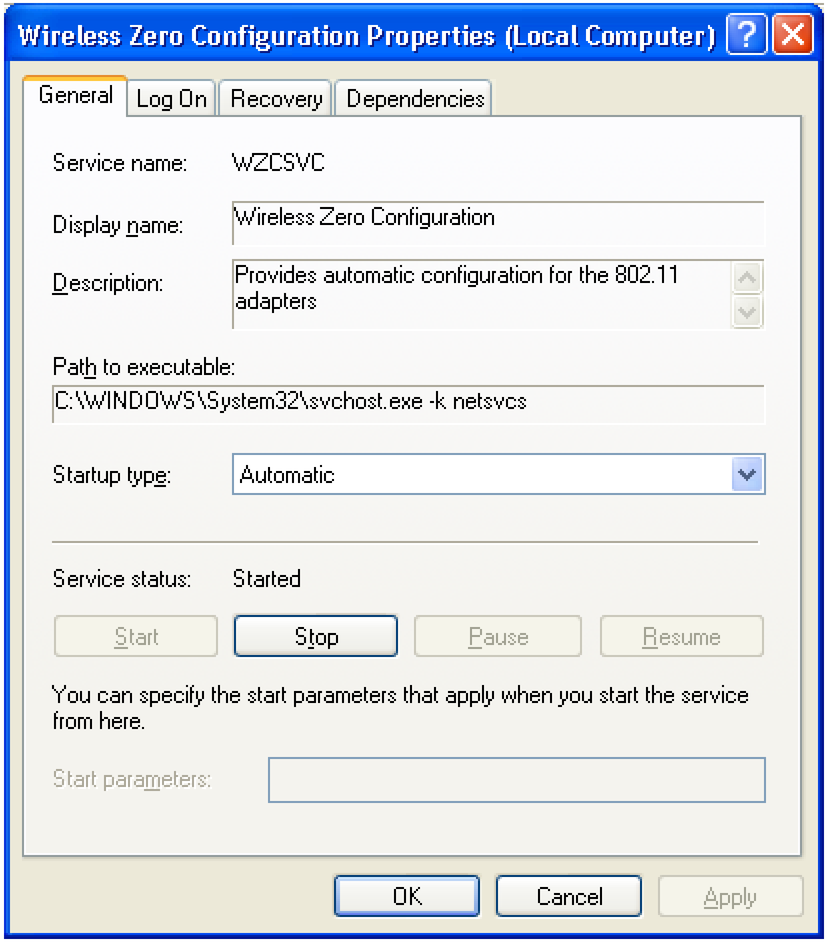
EAP type: SecureW2

□ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

Microsoft Native Supplicant: XP SP2

- Integral to operating system
  - nothing to deploy except configuration
  - No additional cost, licensed as part of OS
- Same service controls wireless and wired 802.1X
  - Wireless Zero Config (WZC)
- Integrated machine and user profile
- Registry changes required for proper operation of wired 802.1X
- **EAP Types** – PEAP/MSCHAPv2, PEAP/TLS, TLS, MD5



Wireless Zero Configuration Properties (Local Computer)

Service name: WZCSVC

Display name: Wireless Zero Configuration

Description: Provides automatic configuration for the 802.11 adapters

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Automatic

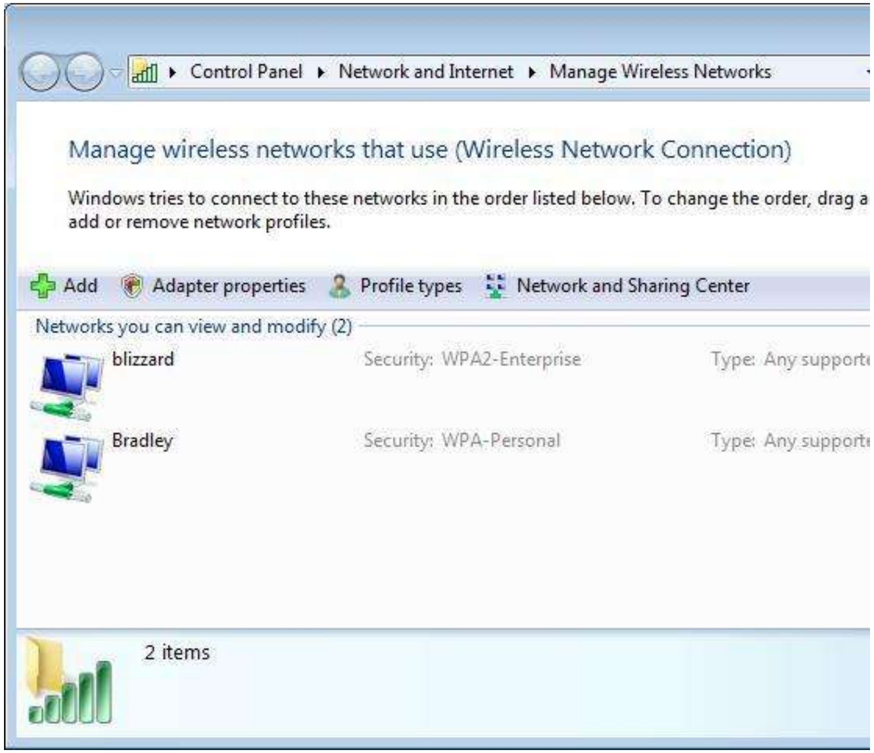
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Vista & XP SP3 Native Supplicant

- Integral to operating system
  - nothing to deploy except configuration
  - No additional cost, licensed as part of OS
- Separate services for wireless and wired 802.1X
  - Wireless Zero Config (WZC)
  - Wired AutoConfig (DOT3SVC)
- Machine & User Authentication
- PEAP-MSCHAPv2,PEAP-TLS, EAP-TLS
- Recommendations
  - Use NDIS 6 NIC drivers
  - Vista SP1
  - Auth Fail Hot-Fix:


Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Add
Adapter properties
Profile types
Network and Sharing Center

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below. To change the order, drag a
add or remove network profiles.

Networks you can view and modify (2)

blizzard	Security: WPA2-Enterprise	Type: Any support
Bradley	Security: WPA-Personal	Type: Any support

2 items

http://support.microsoft.com/default.aspx?scid=kb;en-us;957931&sd=rss&spid=11712

Windows 7 Native

- Integral to operating system

  nothing to deploy except configuration

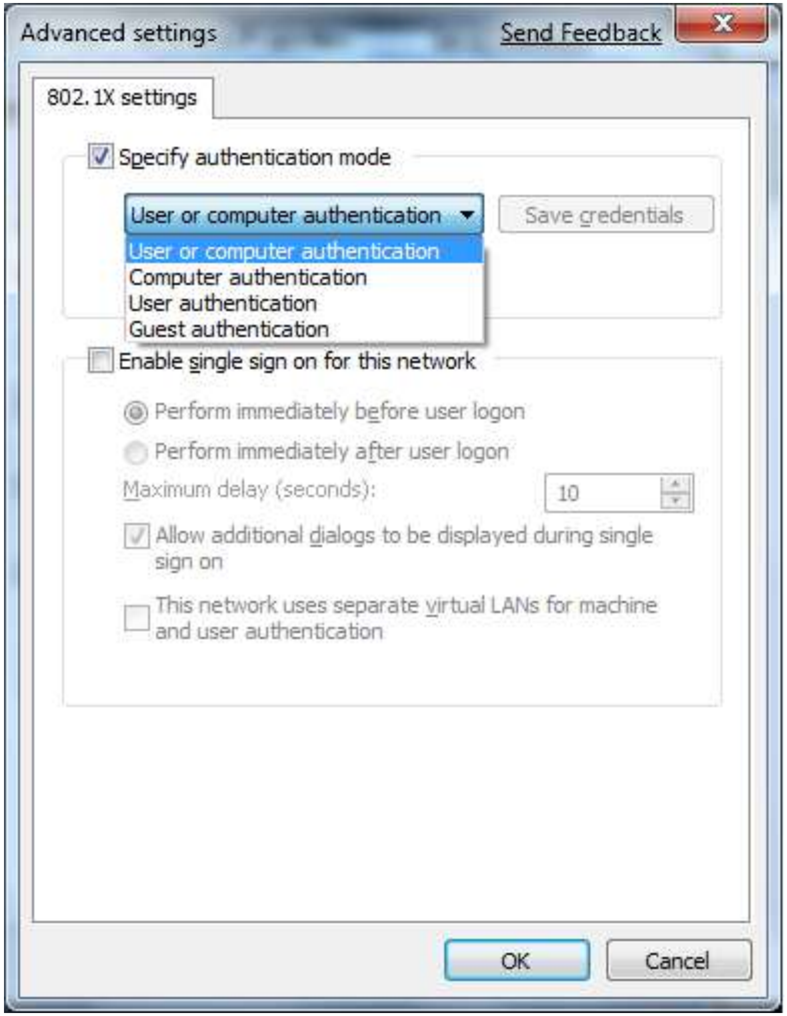
  No additional cost, licensed as part of OS

- Separate services for wireless and wired 802.1X

  Wireless Zero Config (WZC)

  Wired AutoConfig (DOT3SVC)

- Machine & User Authentication
- PEAP-MSCHAPv2,PEAP-TLS, EAP-TLS



Advanced settings

Send Feedback

802.1X settings

☑ Specify authentication mode

User or computer authentication ▾ Save credentials

User or computer authentication
Computer authentication
User authentication
Guest authentication

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

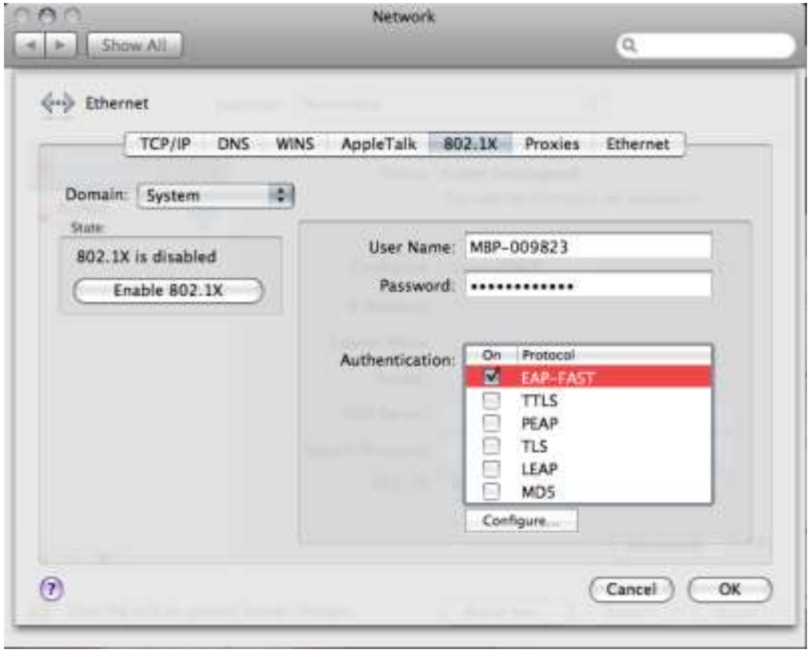
☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

OK Cancel

Mac OSX - 10.6

- Wired and wireless support
- Username / Password, Certificates, & Tokens
- Machine or User Authentication
- Broad EAP type support
- No up-front licensing cost
- Apple supported
- End-user focused



Domain: System

State:
802.1X is disabled

User Name: MBP-009823

Password: •••••••••••••

Authentication:

On	Protocol
☑	EAP-FAST
□	TTLS
□	PEAP
□	TLS
□	LEAP
□	MD5

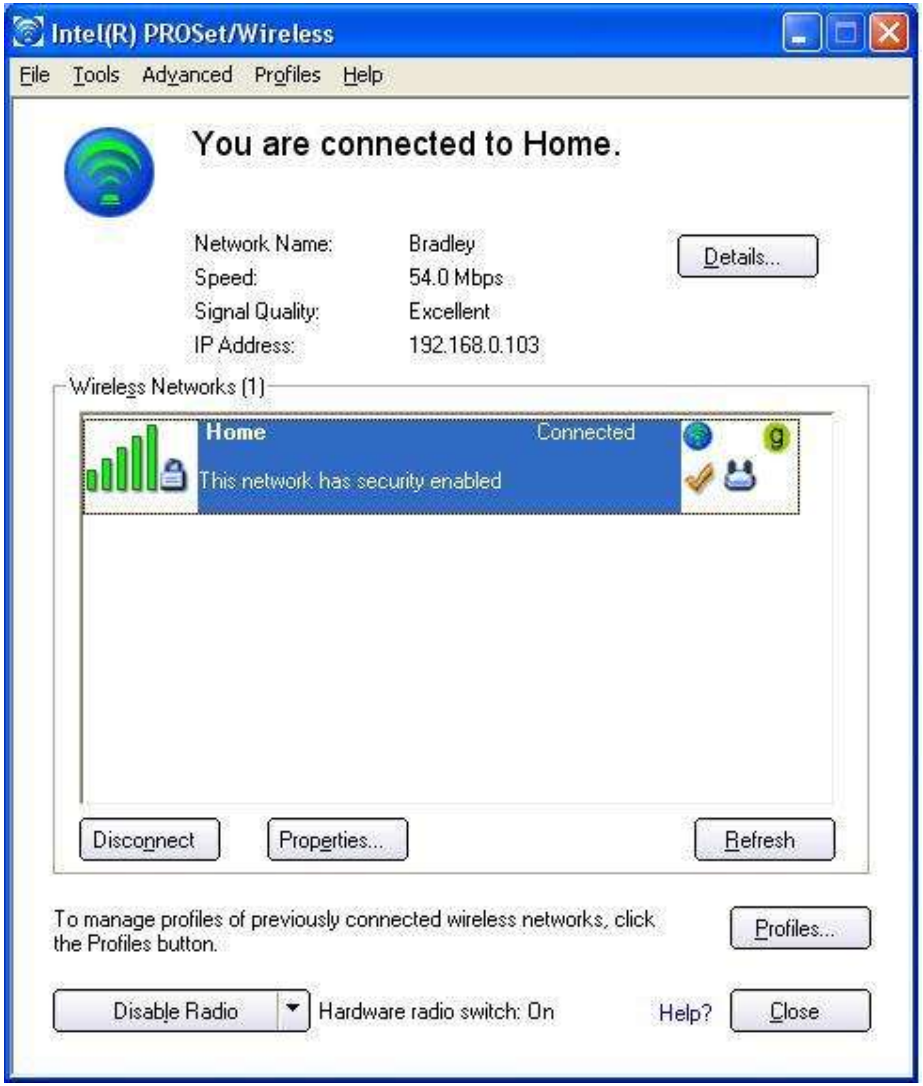
Intel Proset

- Driver Intimacy

  Adapter settings

  Radio On / Off

- No additional up-front costs
- Username / Password, Soft Certificates, Smartcards, & Tokens
- Broad EAP Type Support
- Wireless Only
- Supported by Intel
- Requires Intel NIC



You are connected to Home.

Network Name: Bradley
Speed: 54.0 Mbps
Signal Quality: Excellent
IP Address: 192.168.0.103

Home — Connected
This network has security enabled

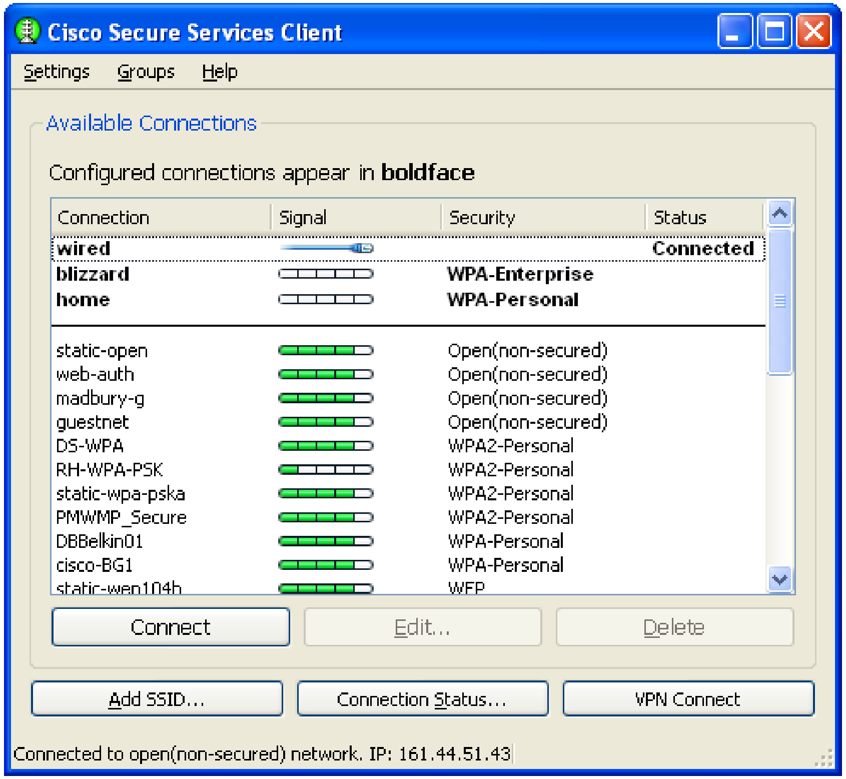
To manage profiles of previously connected wireless networks, click the Profiles button.

Hardware radio switch: On

Cisco Secure Services Client

- Wired and wireless support
- Username / Password, Soft Certificates, Smartcards, & Tokens
- Machine & User Authentication
- Broad EAP type support
- Up-front licensing cost
- Cisco supported
- End-user focused
- Applications –

  Enterprise environments



Available Connections

Configured connections appear in **boldface**

Connection	Signal	Security	Status
wired			**Connected**
blizzard		**WPA-Enterprise**	
home		**WPA-Personal**	
static-open		Open(non-secured)	
web-auth		Open(non-secured)	
madbury-g		Open(non-secured)	
guestnet		Open(non-secured)	
DS-WPA		WPA2-Personal	
RH-WPA-PSK		WPA2-Personal	
static-wpa-pska		WPA2-Personal	
PMWMP_Secure		WPA2-Personal	
DBBelkin01		WPA-Personal	
cisco-BG1		WPA-Personal	
static-wep104b		WEP	

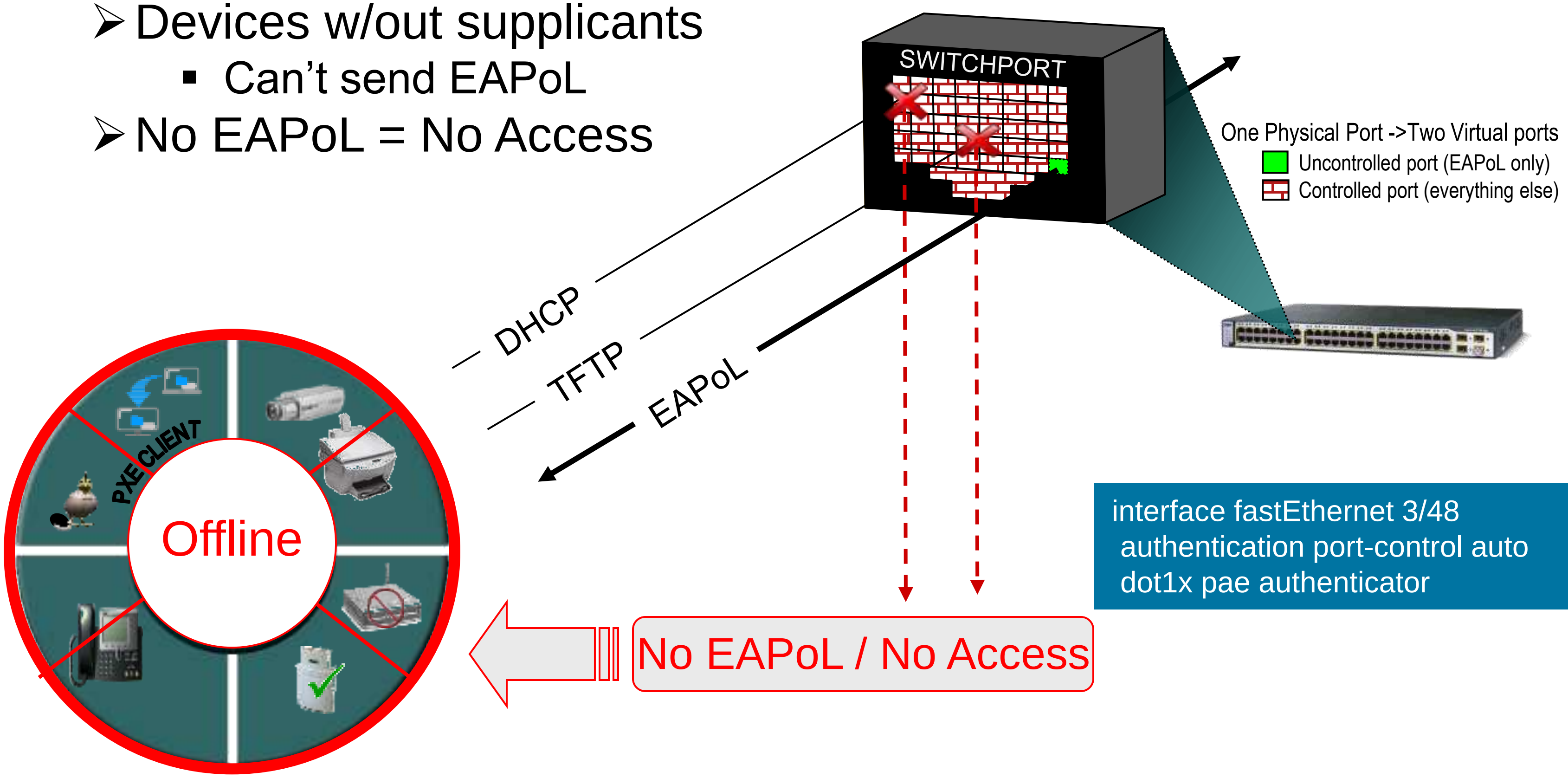
Connected to open(non-secured) network. IP: 161.44.51.43

Identity & Authentication
Non-802.1X Capable Devices & Users

Default Security: Consequences

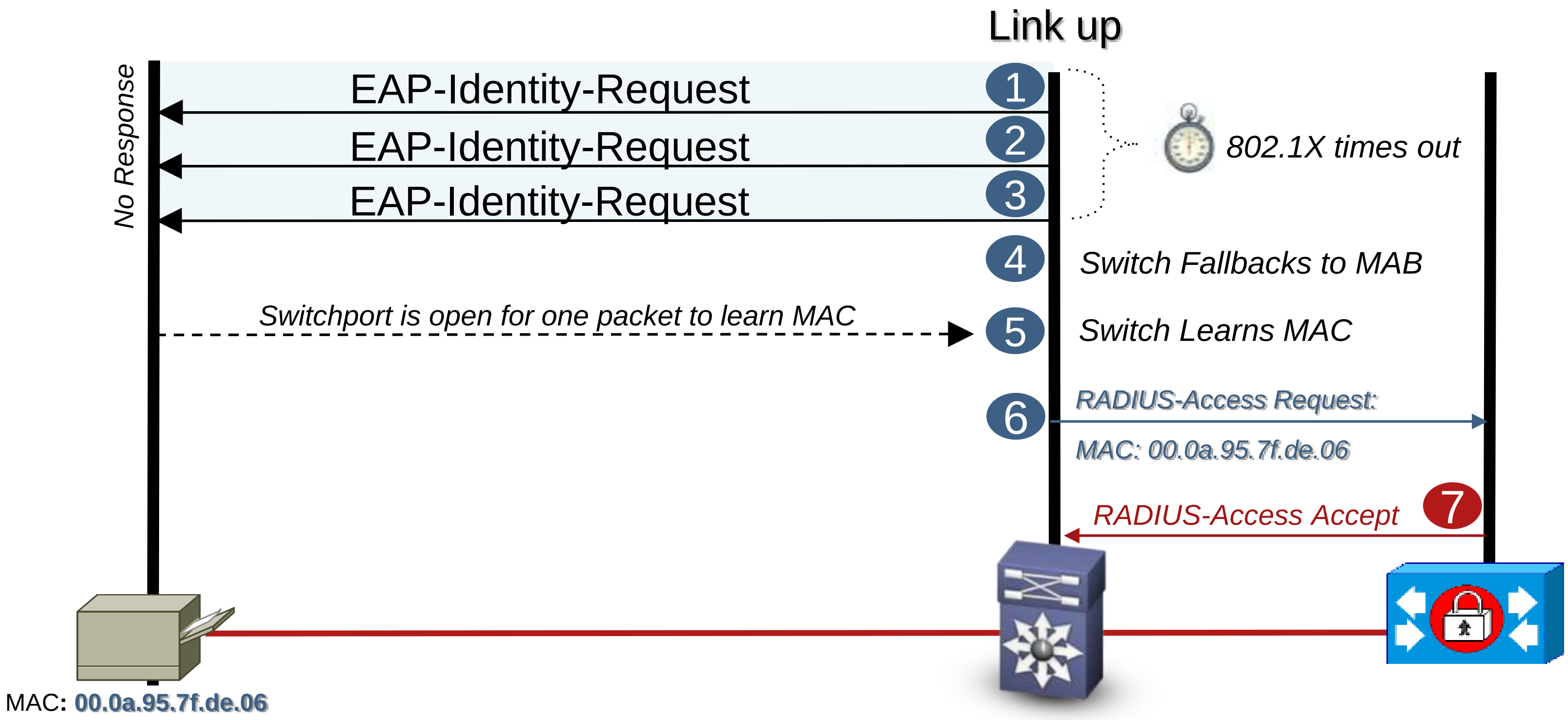
Default 802.1X Challenge

- Devices w/out supplicants
  - Can’t send EAPoL
- No EAPoL = No Access


SWITCHPORT
One Physical Port ->Two Virtual ports
🟩 Uncontrolled port (EAPoL only)
🟥 Controlled port (everything else)
DHCP
TFTP
EAPoL
PXE CLIENT
Offline
No EAPoL / No Access

```
interface fastEthernet 3/48
 authentication port-control auto
 dot1x pae authenticator
```

MAC Authentication Bypass (MAB) for Non-802.1X Devices



802.1X with MAB

Deployment Considerations

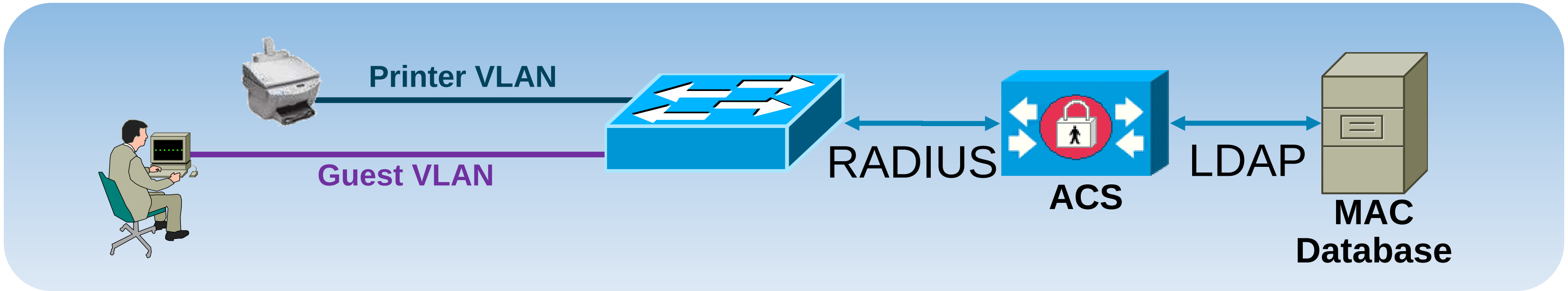
MAB enables differentiated access control

MAB leverages centralized policy on AAA server

Dependency on 802.1X timeout -> delayed network access

- Default timeout is 30 seconds with three retries (90 seconds total)
- 90 seconds > DHCP timeout.

MAB requires a database of known MAC addresses



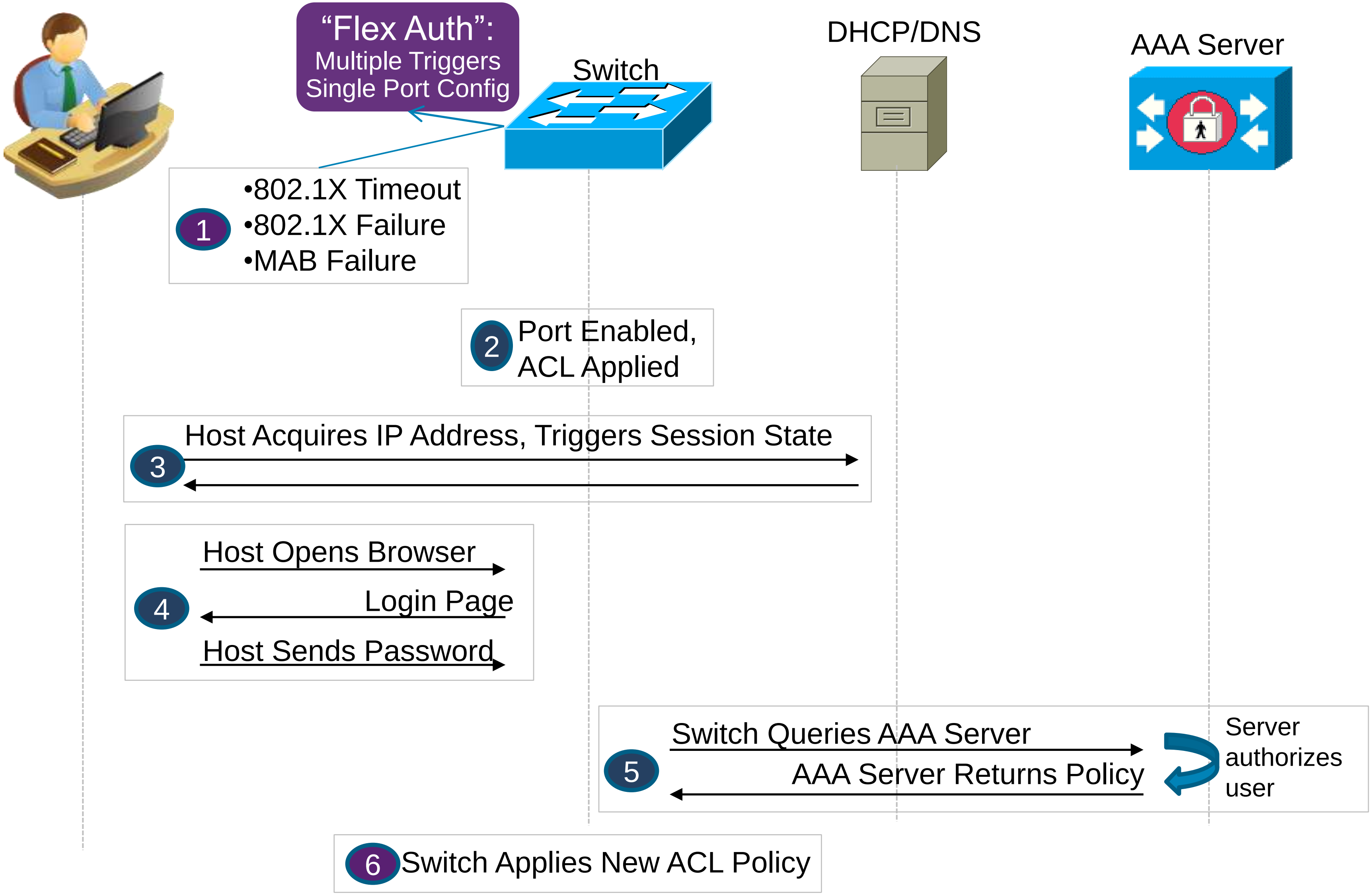
Considerations: MAC Databases

Method	What is it?	Advantages	Problems	Use Case
OUI Wildcards	Use 3-Byte Identifier	Easy to add lots of devices	No granularity	‘Add all HP printers’
ACS	Local database with Radius Server	Readily available	No central repository for all IDs	‘Radius only’
AD	Central Directory Service	Central repository	Should have support for [ieee802] object, password complexity	‘All in one’
NAC Profiler	Automatic building of MAC DB	Automated	Need certain methods to make it reliably identify devices	‘handle unknown devices’
LDAP	Central directory	Standards based	Manually populated and maintained	‘leverage existing db’

DEMO Time

MAB

Web Authentication for non-802.1X User



“Flex Auth”:
Multiple Triggers
Single Port Config

Switch

DHCP/DNS

AAA Server

1
- 802.1X Timeout
- 802.1X Failure
- MAB Failure

2 Port Enabled, ACL Applied

3 Host Acquires IP Address, Triggers Session State

4
Host Opens Browser
Login Page
Host Sends Password

5
Switch Queries AAA Server
AAA Server Returns Policy
Server authorizes user

6 Switch Applies New ACL Policy

802.1X with Web-Auth

Deployment Considerations

- Web-Auth is only for users (not devices)
  - browser required
  - manual entry of username/password

- Web-Auth can be a fallback from 802.1X or MAB.
- Web-Auth and Guest VLAN* are mutually exclusive
- Web-Auth supports ACL authorization only
- Web-Auth behind an IP Phone requires Multi-Domain Authentication* (MDA)

* To be discussed in later sections

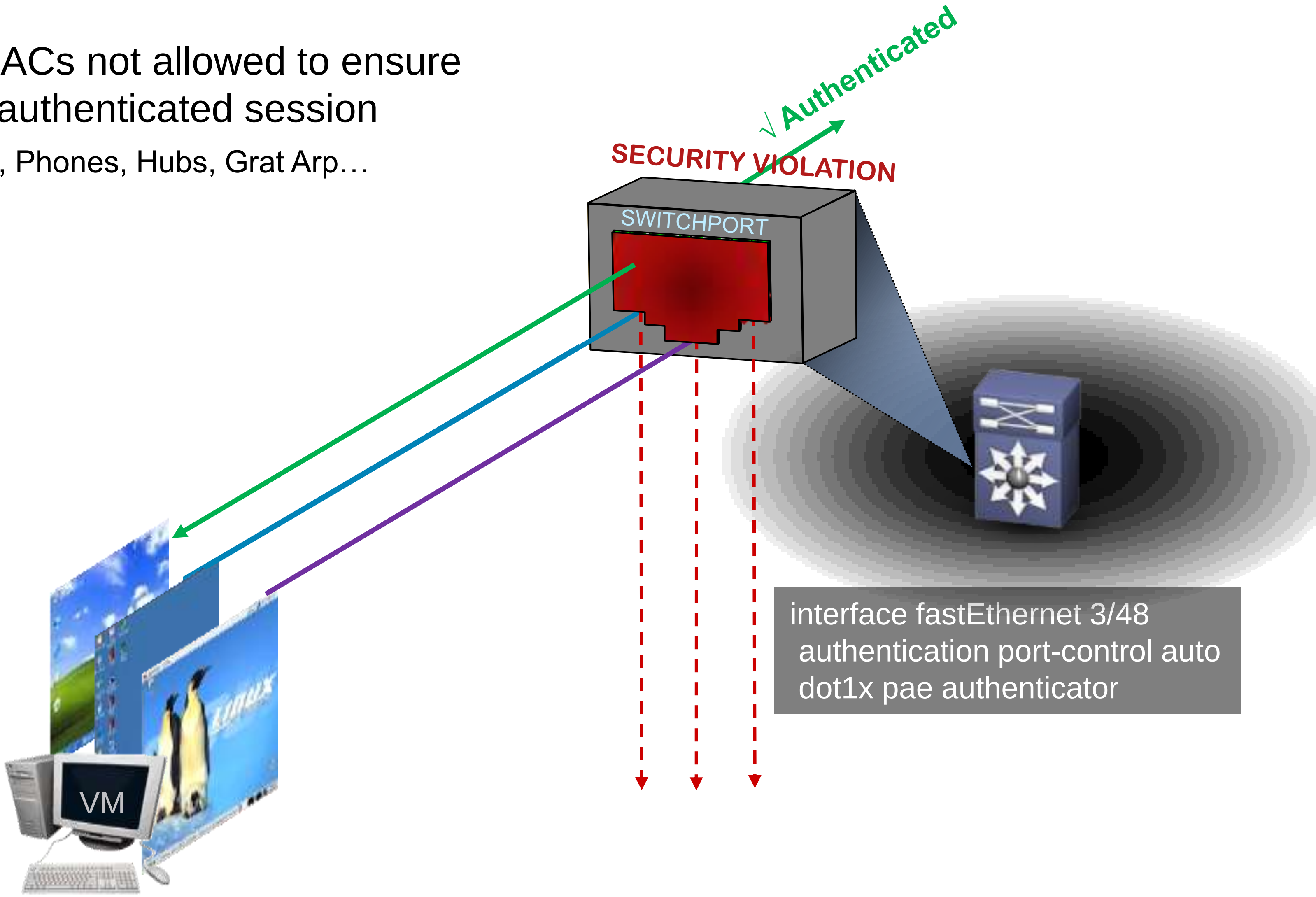
DEMO Time

Web-Auth

Identity & Authentication Further Restrictions

Default Security: More Consequences

- ➢ Multiple MACs not allowed to ensure validity of authenticated session
  - VMWare, Phones, Hubs, Grat Arp…



```
interface fastEthernet 3/48
 authentication port-control auto
 dot1x pae authenticator
```

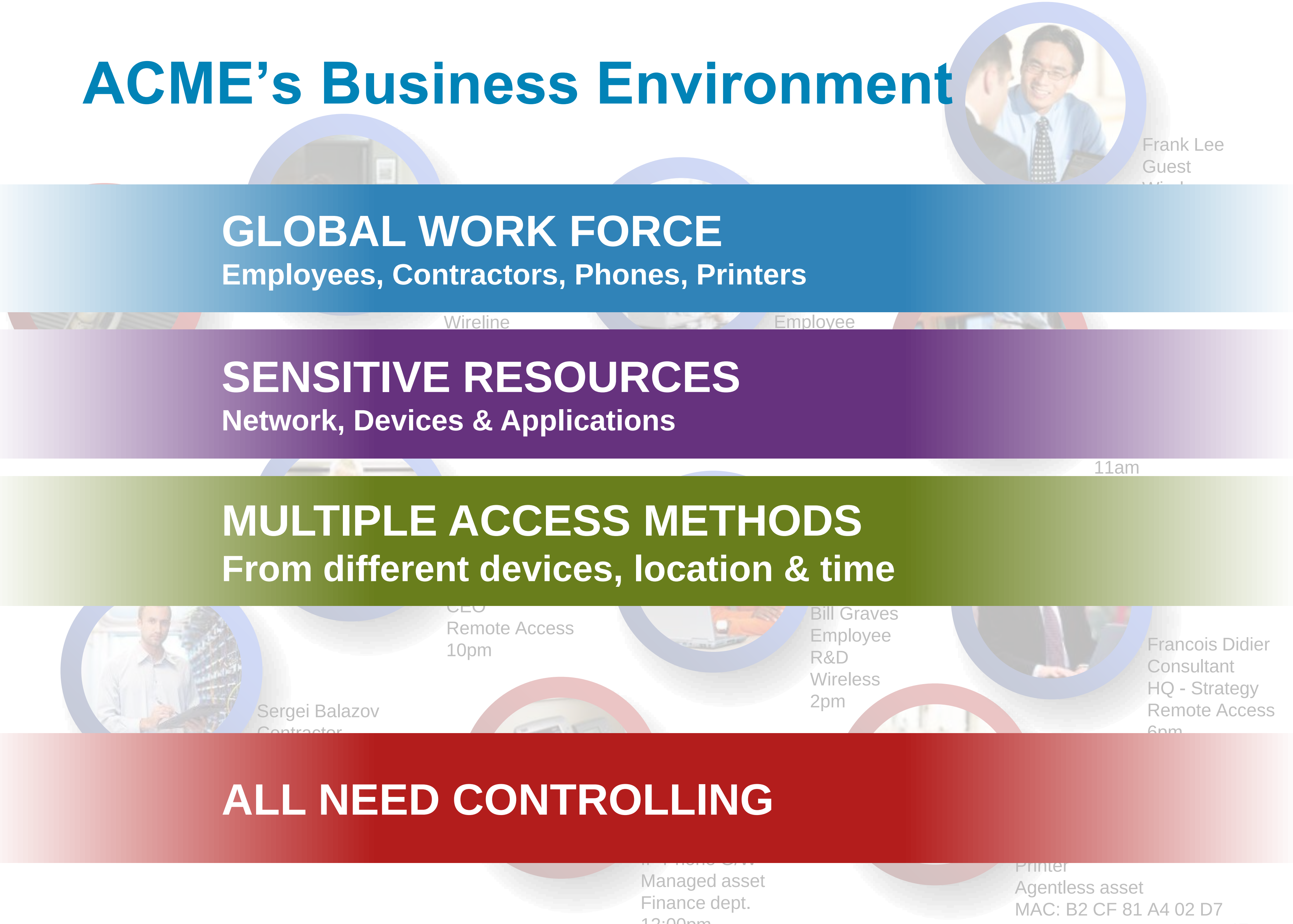
Phase 0: Pre-Deployment

Introduction to ACME Corp.

- Fictional Company, publishing house.
- Employees, free lancers, guests are using the corporate network infrastructure.
- The same infrastructure is used for other devices as well.
- *'One network to support them all.'*
- No access control in place as of today, everybody with physical access can connect.

The CIO decided to limit access. Only known devices must be allowed on the network

ACME's Business Environment



GLOBAL WORK FORCE

Employees, Contractors, Phones, Printers

SENSITIVE RESOURCES

Network, Devices & Applications

MULTIPLE ACCESS METHODS

From different devices, location & time

ALL NEED CONTROLLING

ACME's Goals

The Mission:

- Prevent Anonymous / Unauthorized Access
- Increase Network Visibility
- Solution deployment should be transparent to end users

  Employee end-user behavior should not change.

  Legacy devices must not be locked out.

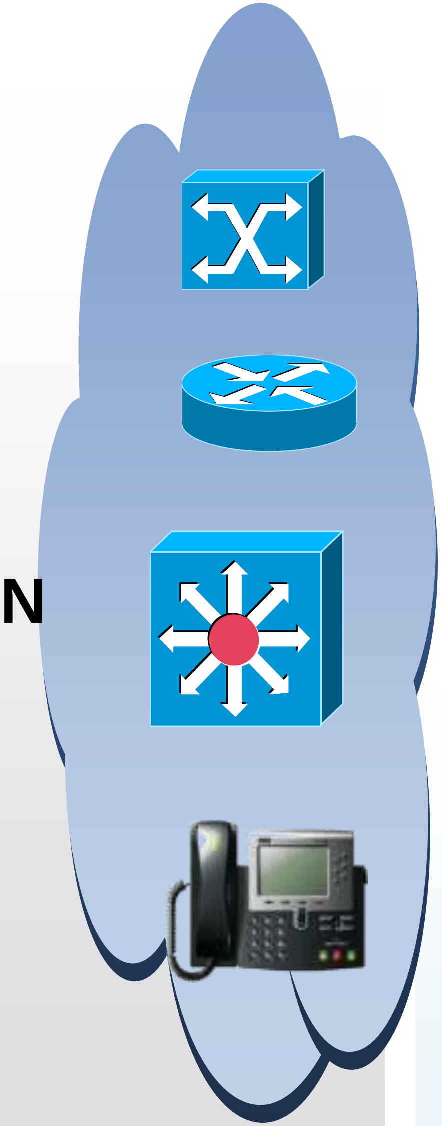
  Best authentication method based on device capabilities should be chosen.

ACME's Environment: Devices

- PC devices are primarily running in a Microsoft Windows environment.
- IP Telephony is Cisco, 50% are 802.1X ready and support EAP-TLS / certificate based authentication. No Certs deployed so far (MICs only).
- Printers are not-802.1X capable, must be authenticated via their MAC address.
- All sorts of other (legacy) devices from freelancers (Macs, Linux machines, …) and generic devices (e.g. building control).

ACME's Environment: Network

- ACME recently did a refresh on their access network.
- Devices are up-to-date and are running latest available code.
- Devices are configured according to L2 best practice (DHCP snooping, DAI, VLAN != VVLAN != Management VLAN).
- For conference rooms, only corporate owned and authorized devices may be cascaded to provide additional ports (Extended Edge concept).



ACME’s Environment: Back-End

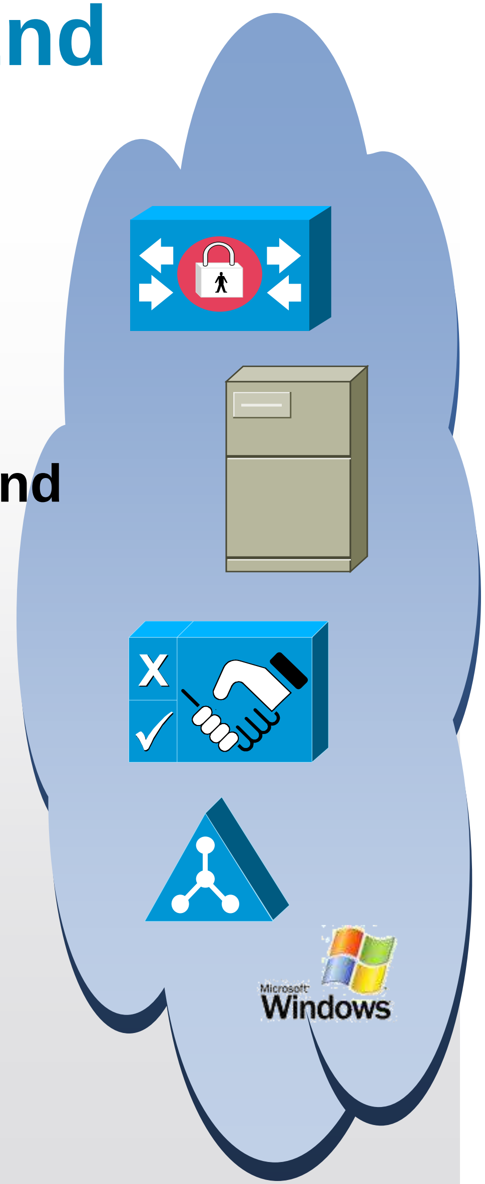
- Windows 2008 Active Directory

  Environment managed via AD Group Policy Objects (GPOs)

  GPOs enabled centralized management & distribution of policy for users, computers and other objects in the directory.

- Certificate Infrastructure is in place, Microsoft CA running on AD.

- ACS 5.1 will be used to provide AAA services.



ACME's Environment: Credentials

- Corporate machines are registered with the Windows domain
- Computers & Users log in with Name and Password to the domain
- Additional authentication is enforced at the application layer
- No authentication at all for all other devices

Considerations

- What Authentication Method(s) should be used?

- Which Operating Systems are to be supported?
- Where are Credentials stored?

  One Store vs. Many Stores

  How to Build and Manage a MAC Database?

Considerations: Authentication Method

Method	What's required?	Pros	Cons
802.1X	Supplicant Credentials	Highest Security	Supplicant may not be available on every platform
MAB	MAC address database	Works for all devices	Weak, can be easily snooped, DB needs to be created and maintained
Web-Auth	Portal (on switches or on dedicated NGS)	No supplicant needed, every device w/ browser can be used	Relies on initial connectivity, VLAN / IP address change after authentication is problematic

Further Considerations for 802.1X Authentication: EAP Methods

Method	What’s required?	Pros	Cons
EAP-MD5	Username, Password	Most devices with 802.1X support do at least EAP-MD5	Offline dictionary attack, one-way authentication
EAP-TLS	Certificate distribution	Most secure method	Certificate cost, distribution, renewal
PEAP	Username, Password	Readily available in Windows environments	Single factor authentication

Chosen by ACME for operational efficiency

Considerations: Operating Systems

What do we have to support…

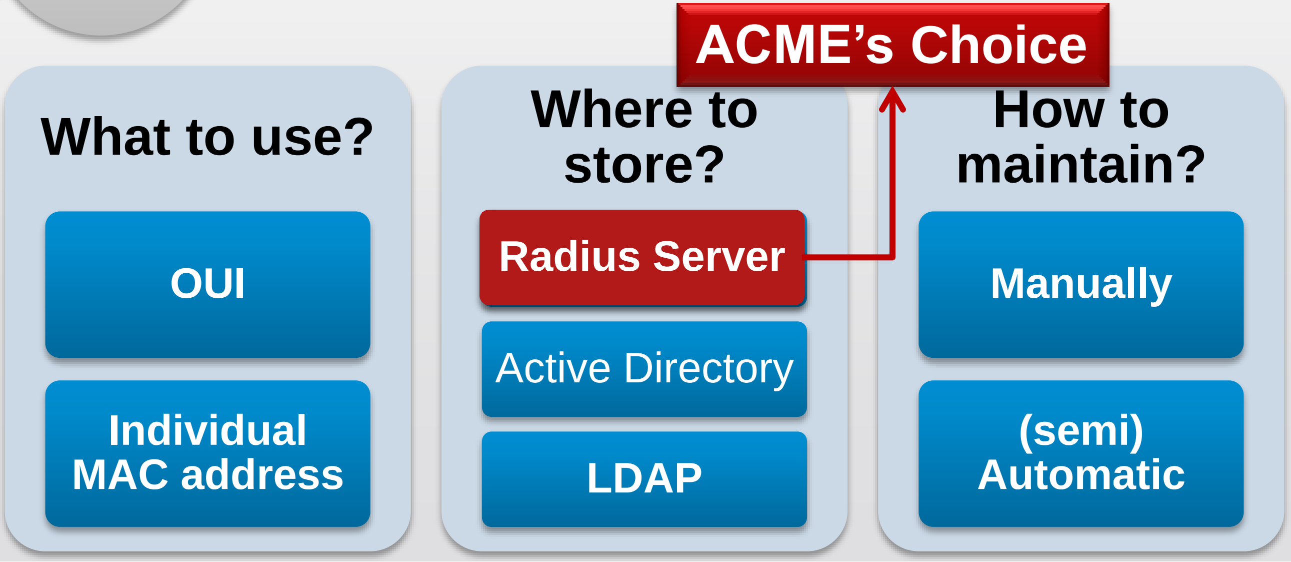
Considerations: Operating Systems

OS (corporate asset)	Supplicant	Methods supported	Remark
Windows XP and newer	Built-in or 3rd party	MD5, TLS, PEAP	No MD5 w/ Vista and newer
Older Windows	No support	MAB or WebAuth	
Apple Mac OS X	Built-in	TTLS, TLS, FAST, PEAP, LEAP, MD5	
802.1X-capable Cisco phones	Built-in	MD5, FAST, TLS	
Other devices	various	various	various

OS (non-corporate asset)	Supplicant	Methods supported	Remark
All	n/a	MAB or WebAuth	Guest Access

Considerations: MAC Databases

PCs	Non-PCs			
	UPS	Phone	Printer	AP


ACME's Choice

What to use?

- OUI
- Individual MAC address

Where to store?

- Radius Server
- Active Directory
- LDAP

How to maintain?

- Manually
- (semi) Automatic

ACME’s Starting Point

CREDENTIAL STORE

ACME WILL USE ACTIVE DIRECTORY

EAP-TYPE

USE PEAP WHEREVER POSSIBLE

UNMANAGED DEVICES

EVERYTHING ELSE USES MAB AND WEBAUTH

GUEST ACCESS

LEVERAGE NAC GUEST SERVER FOR GUESTS

ACME Summary & Goal

- Enforce admission control to wired network
- Use central identity store, Active Directory
- Control Plane is Radius
- Provide coherent solution for all devices

KEEP THE INSIDERS IN AND THE OUTSIDERS OUT!

Phase 1: Monitor Mode

ACME’s Goals : Phase 1

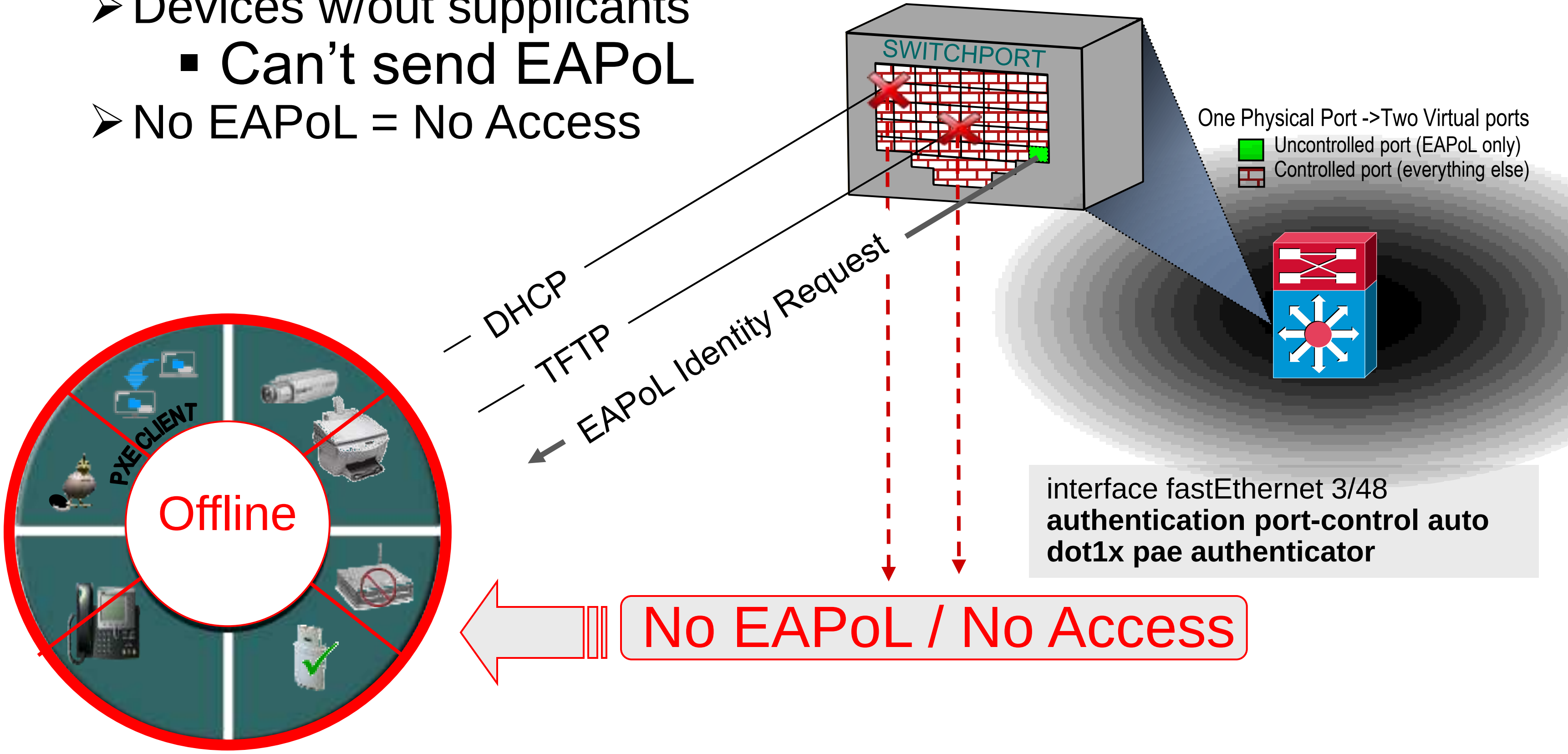
- Gain visibility of what’s currently on the network
    - Managed Assets
    - Agentless Assets
    - Unknown Devices
- Validate components are functioning as expected
- Identify non-functioning components and correct
- Be Transparent to Users and Current Network

ACME’s Goals Can Be Met With Monitor Mode

Default Security: Consequences

Default 802.1X Challenge

- ➢ Devices w/out supplicants
  - ▪ Can’t send EAPoL
- ➢ No EAPoL = No Access


SWITCHPORT
One Physical Port ->Two Virtual ports
🟩 Uncontrolled port (EAPoL only)
▨ Controlled port (everything else)
DHCP
TFTP
EAPoL Identity Request
PXE CLIENT
Offline

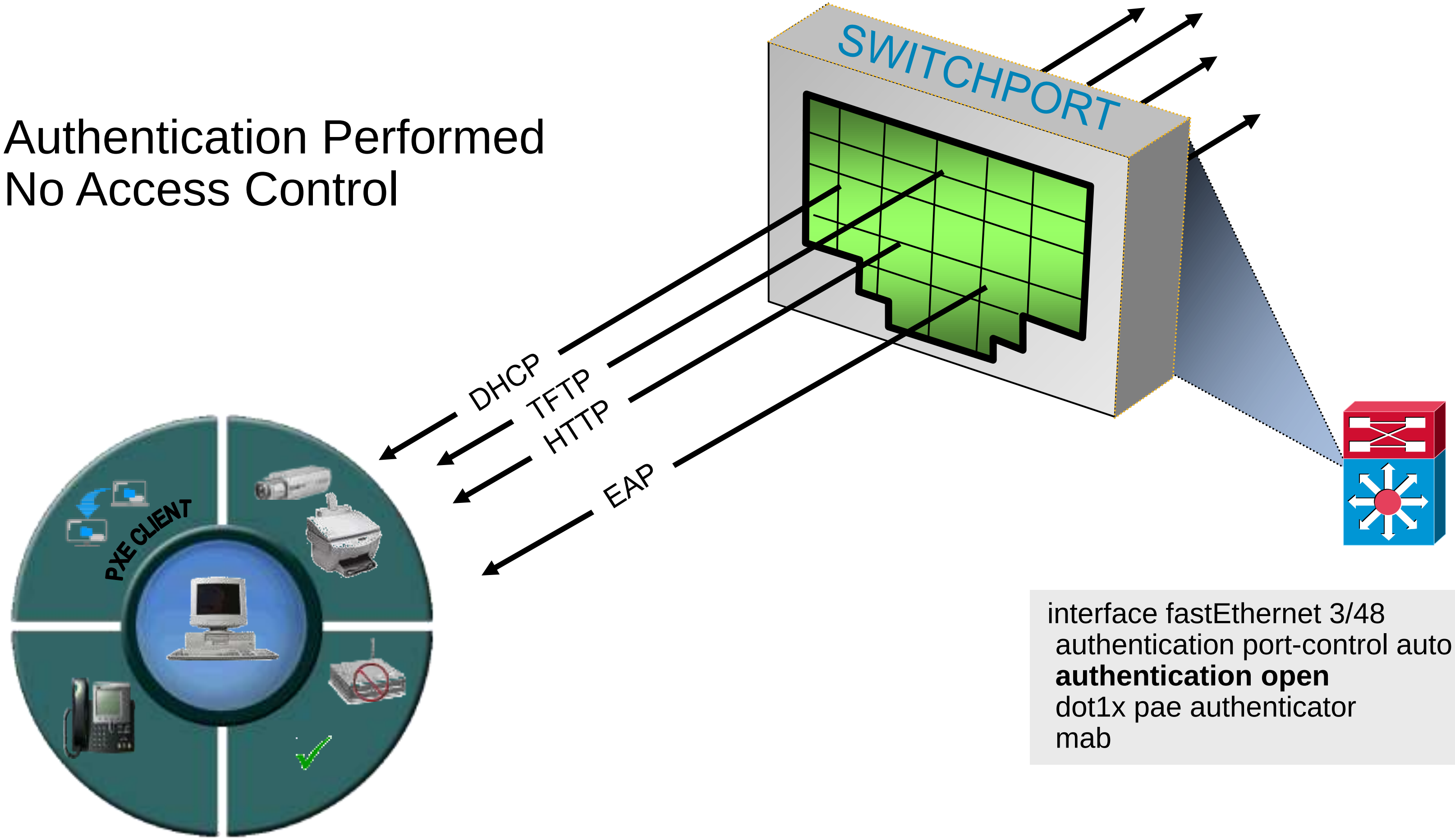
```
interface fastEthernet 3/48
authentication port-control auto
dot1x pae authenticator
```

No EAPoL / No Access

Changing the Default Authorization:
“Open Access”

Open Access (No Restrictions)

- ➢ Authentication Performed
- ➢ No Access Control

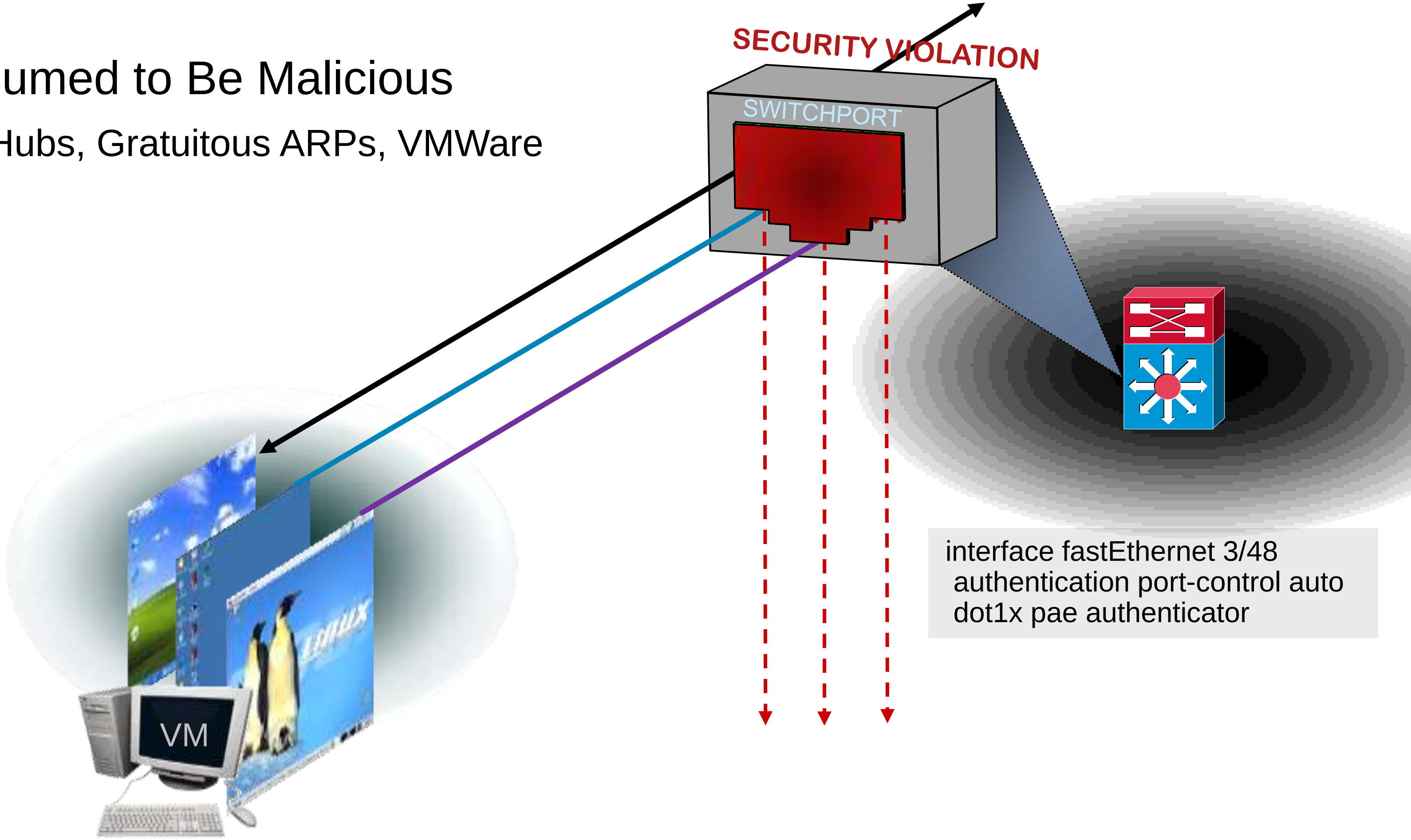


```
interface fastEthernet 3/48
 authentication port-control auto
 authentication open
 dot1x pae authenticator
 mab
```

Default Security: Consequences

Multiple MACs per Port

- Assumed to Be Malicious
  - Hubs, Gratuitous ARPs, VMWare



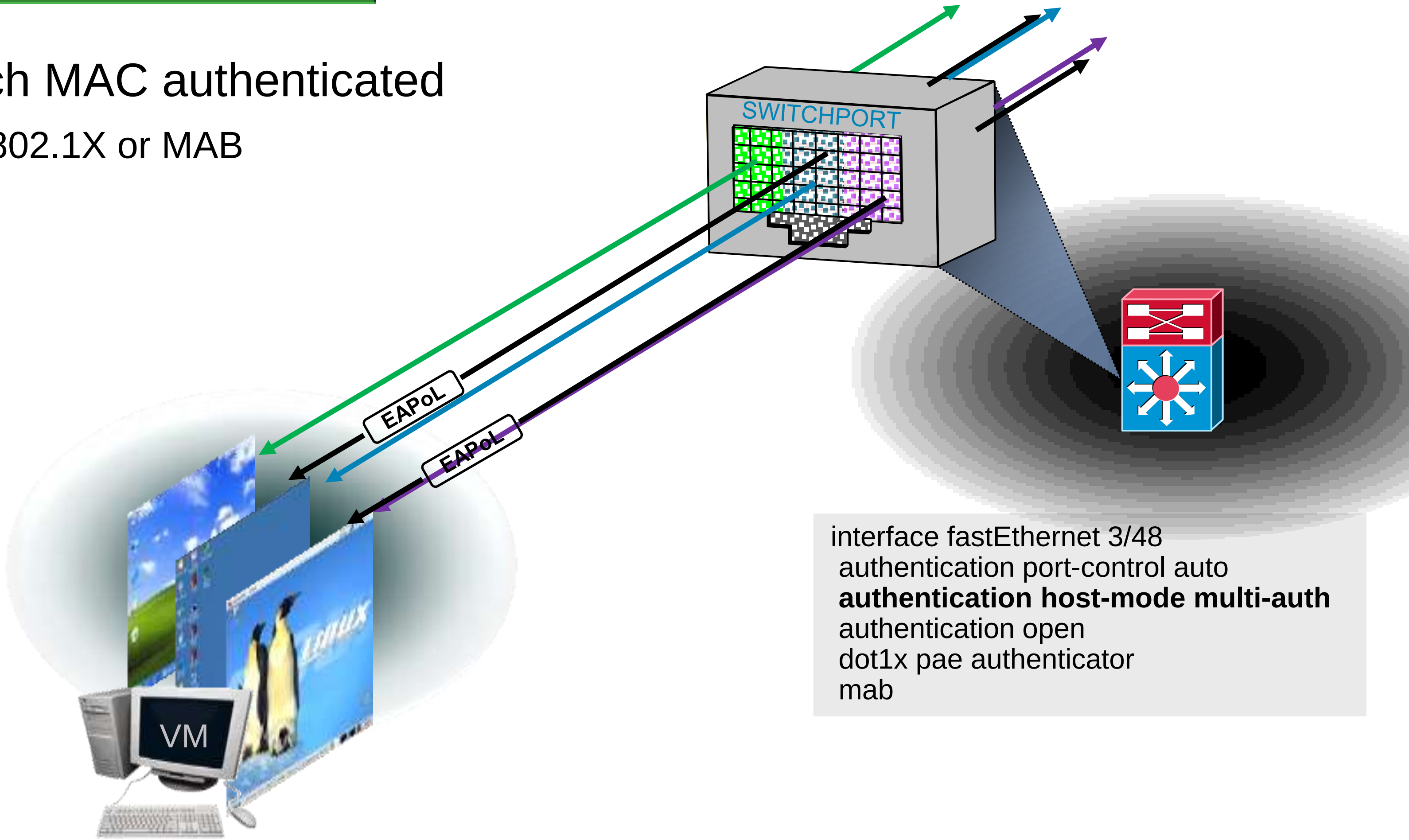
```
interface fastEthernet 3/48
 authentication port-control auto
 dot1x pae authenticator
```

Modifying the Default Security

“Multi-Auth”

Multiple MACs on Port

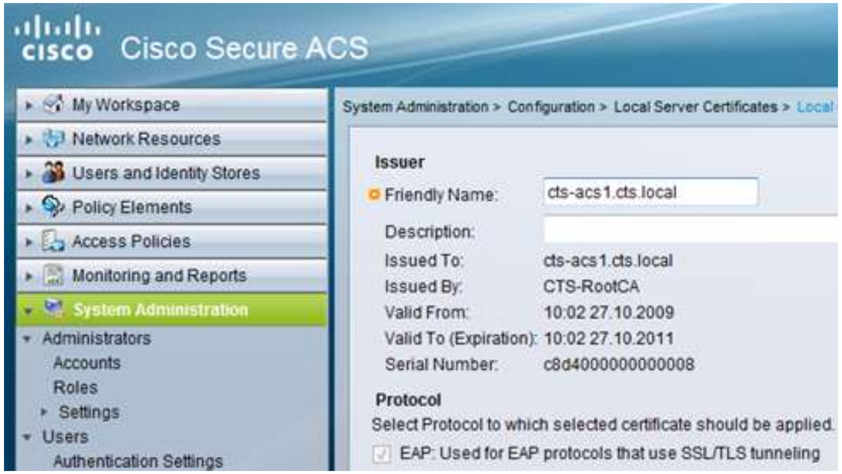
- Each MAC authenticated
  - 802.1X or MAB



```
interface fastEthernet 3/48
 authentication port-control auto
 authentication host-mode multi-auth
 authentication open
 dot1x pae authenticator
 mab
```

Enabling Monitor Mode – RADIUS Server

- Configure PKI and Identity Servers



System Administration > Configuration > Local Server Certificates > Local

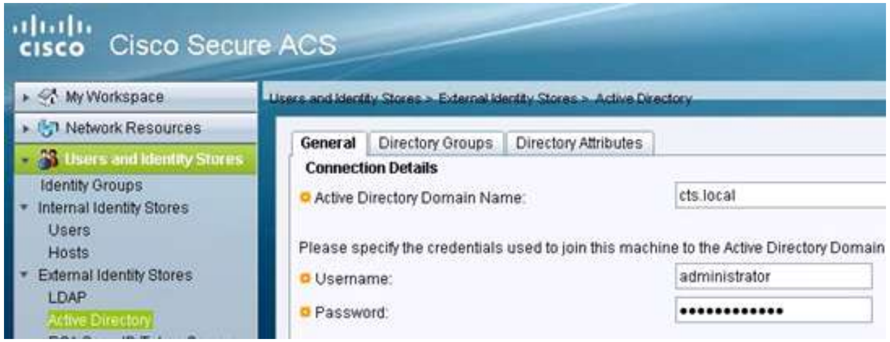
Issuer

Friendly Name:	cts-acs1.cts.local
Description:	
Issued To:	cts-acs1.cts.local
Issued By:	CTS-RootCA
Valid From:	10:02 27.10.2009
Valid To (Expiration):	10:02 27.10.2011
Serial Number:	c8d4000000000008

Protocol

Select Protocol to which selected certificate should be applied.

☑ EAP: Used for EAP protocols that use SSL/TLS tunneling



Users and Identity Stores > External Identity Stores > Active Directory

Connection Details

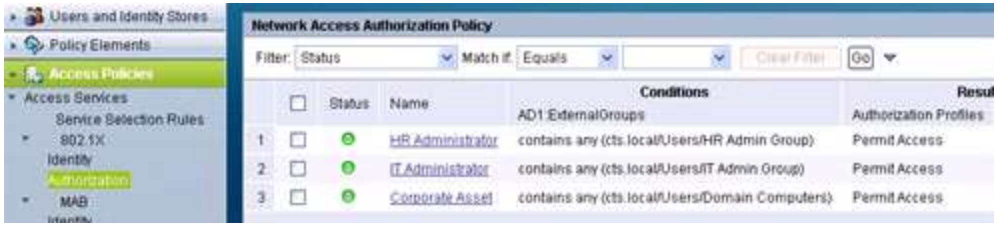
Active Directory Domain Name: cts.local

Please specify the credentials used to join this machine to the Active Directory Domain

Username: administrator

Password: •••••••••••••

- Create 802.1X & MAB Policies



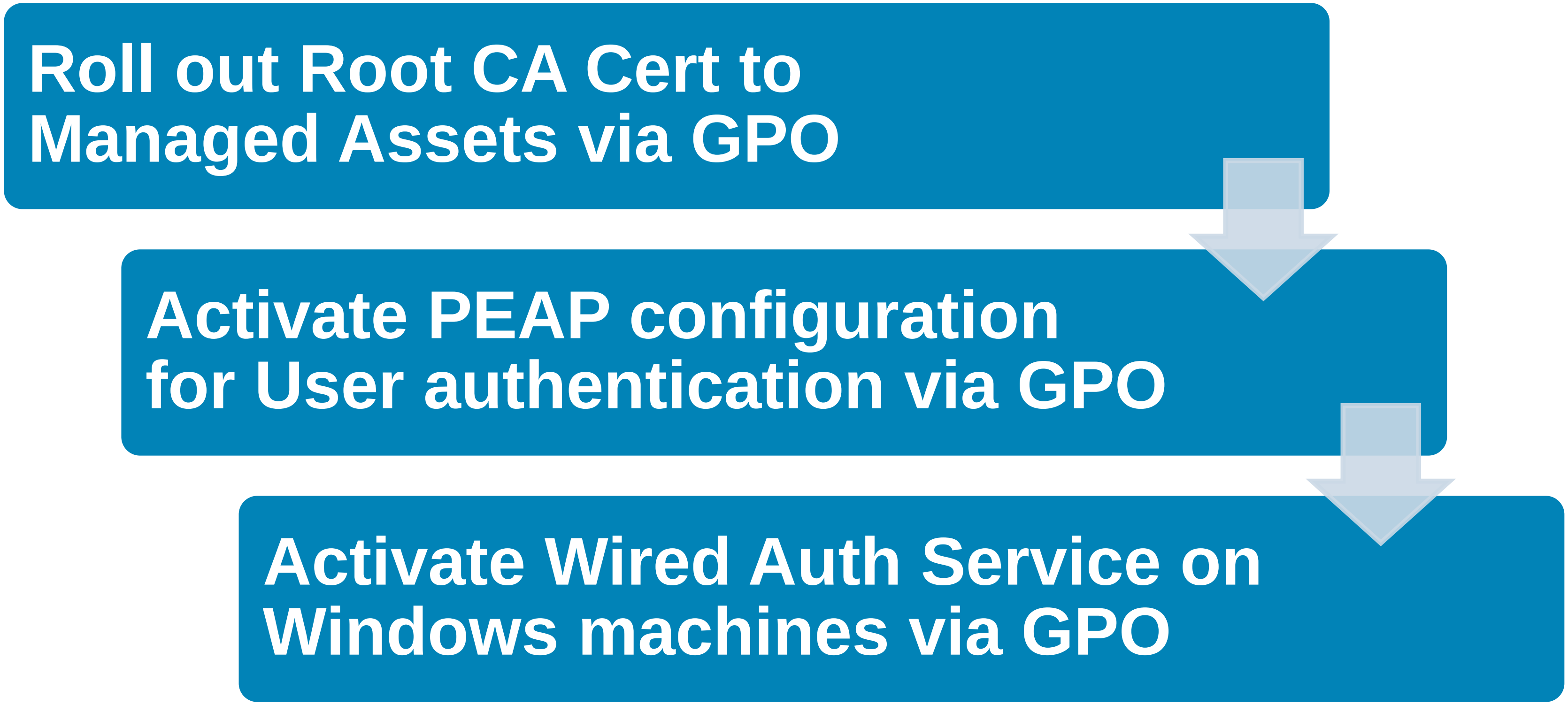
Network Access Authorization Policy

Filter: Status Match if: Equals

				Conditions	Resul
	□	Status	Name	AD1:ExternalGroups	Authorization Profiles
1	□	●	HR Administrator	contains any (cts.local/Users/HR Admin Group)	Permit Access
2	□	●	IT Administrator	contains any (cts.local/Users/IT Admin Group)	Permit Access
3	□	●	Corporate Asset	contains any (cts.local/Users/Domain Computers)	Permit Access

- Every user in AD is permitted
- Separate Rules can be used for reporting

Enabling Monitor Mode – Managed Assets



Roll out Root CA Cert to Managed Assets via GPO

Activate PEAP configuration for User authentication via GPO

Activate Wired Auth Service on Windows machines via GPO

All managed assets should be provisioned before the switches are configured for access control

DEMO Time

Managing 802.1X Parameters with Active Directory GPOs

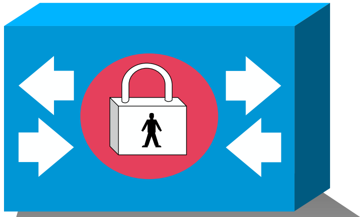
Phased Rollout

- Deploy supplicant configuration components first
- Configure RADIUS server second
- Deploy switches third
- Possibly start with one floor at a time
- Validating via case load that monitor mode is working as expected
- After successful floor rollouts expand to multiple floors or a building at a time

Monitor Mode: Monitoring

Monitor Mode – Monitoring and Reporting

Monitor the network, see who’s on, address future connectivity problems by installing supplicants and credentials, creating MAB database



RADIUS accounting logs provide visibility:

- Passed/Failed 802.1X/EAP attempts
  - List of valid dot1x capable
  - List of non-dotx capable
- Passed/Failed MAB attempts
  - List of Valid MACs
  - List of Invalid or unknown MACs

TO DO Before implementing access control:
•Confirm that all these should be on network
•Install supplicants on X, Y, Z clients
•Upgrade credentials on failed 802.1X clients
•Update MAC database with failed MABs
…

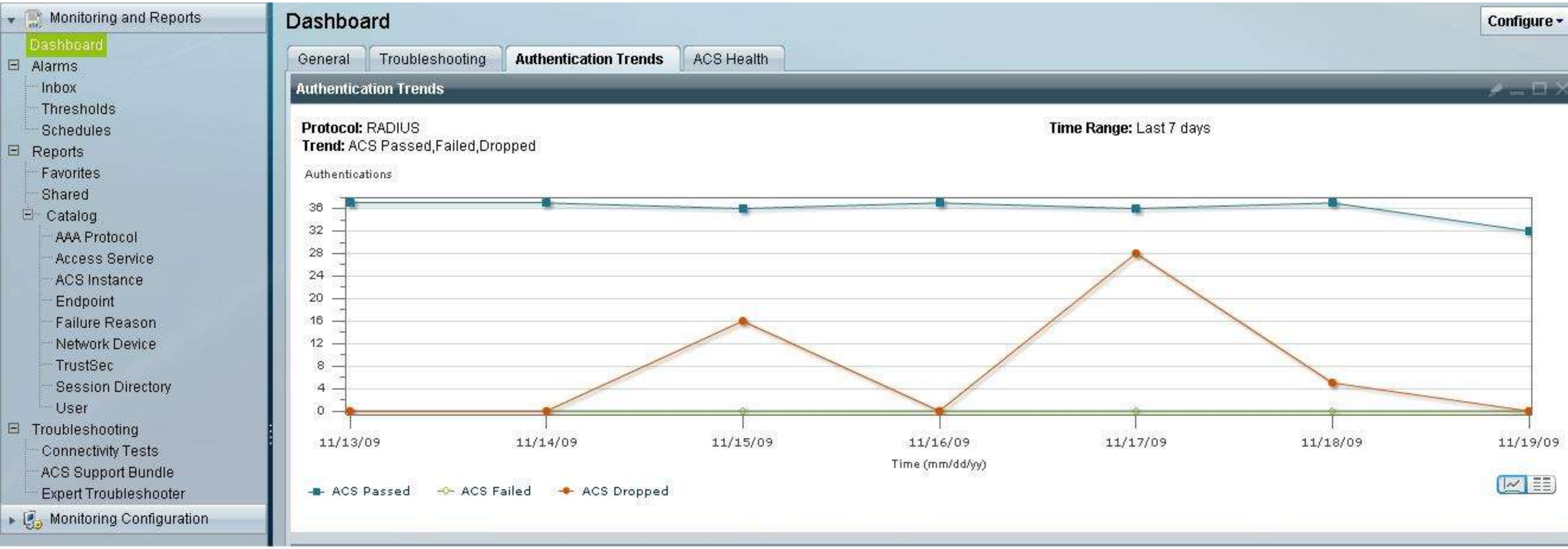
RADIUS Authentication

- ACME authentications can be monitored

  View Trends of Passed (should be high)

  View Trends of Failures (should be low)

  View Trends of Unknown MAC Addresses (should start high and lower as MAC Addresses are added to the database)



Protocol: RADIUS

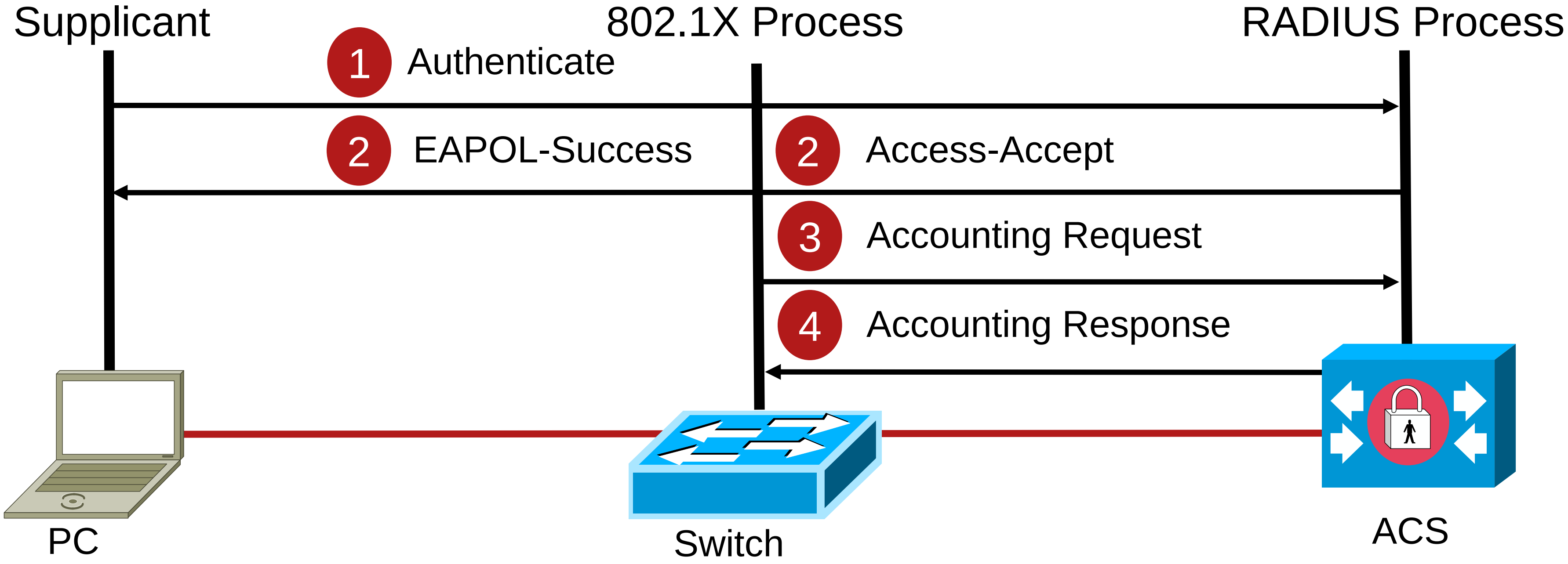
Trend: ACS Passed,Failed,Dropped

Time Range: Last 7 days

Active Monitoring

- Network Visibility is not just about passed/failed authentications
- The RADIUS server can have a session directory provided by RADIUS accounting.
- This provides ACME with a view of all active sessions as the session enter and leave the network
- This information can be used along with other security information for better incident response

802.1X with RADIUS Accounting

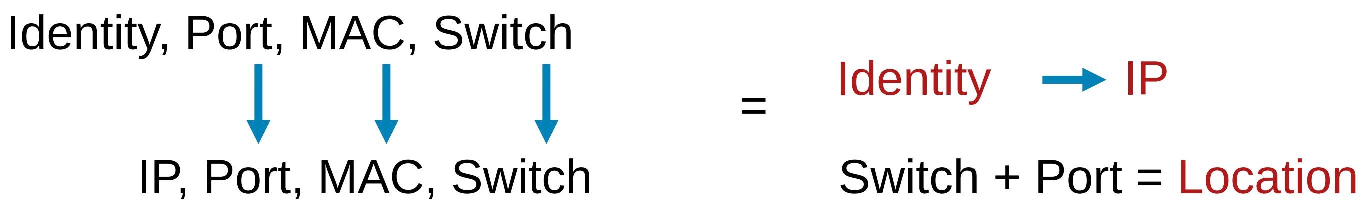


802.1X with RADIUS Accounting

- Similar to other accounting and tracking mechanisms that already exist using RADIUS

  Can now be done through 802.1X

- Increases network session awareness
- Provide information into a management infrastructure about who logs in, session duration, support basic billing usage reporting, etc.
- Provides a means to map the information of authenticated



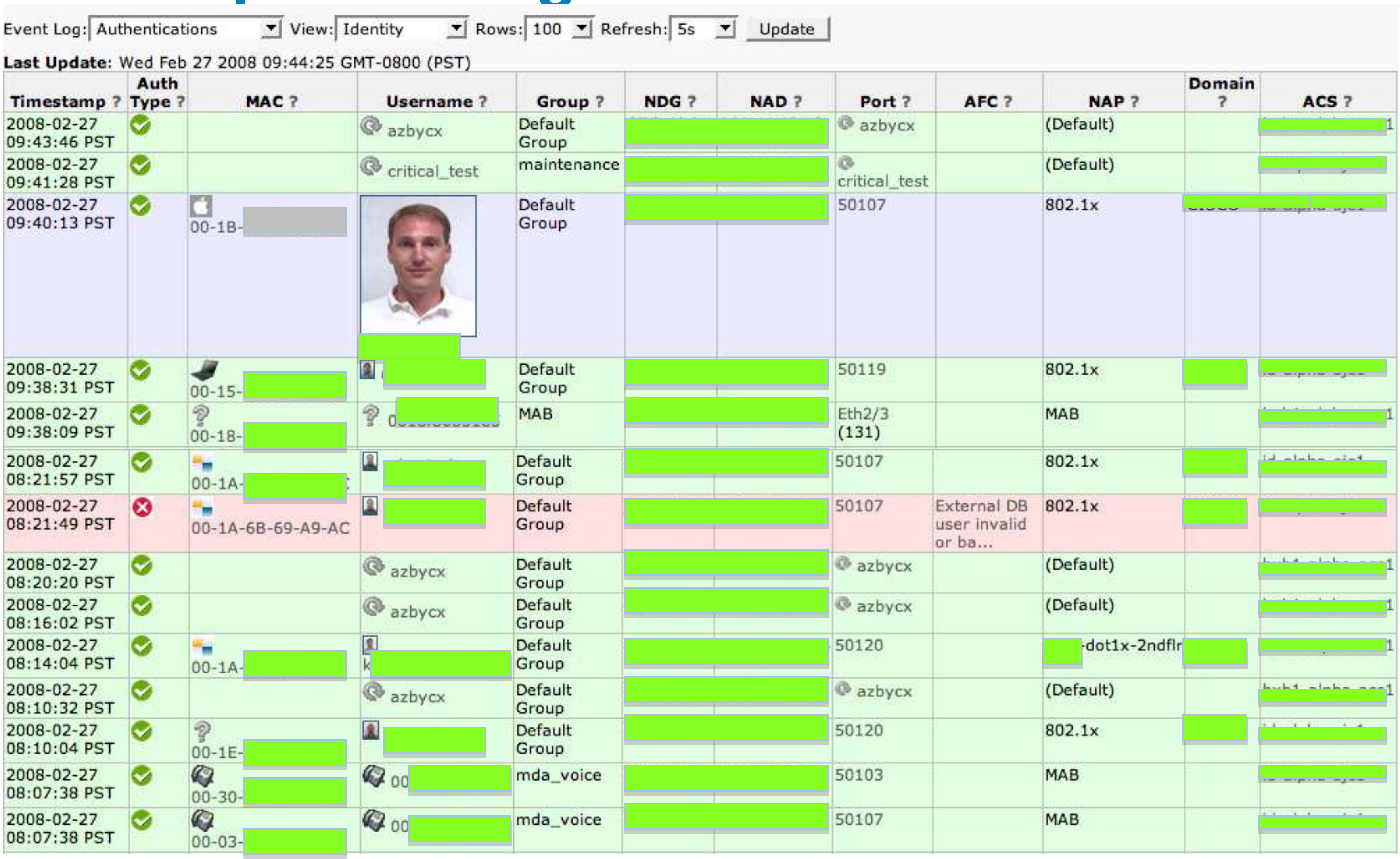
IOS

```
aaa accounting dot1x default start-stop group radius
```

Simple Homegrown Tools

- Switches logs all passed/failed sessions via syslog
- RADIUS servers typically all log information in plain text
- Relatively easy to run scripts against this information to create monitoring views
- Scripts can create database of mac addresses seen from the network

Simple Homegrown Tools



Event Log: Authentications ▼ View: Identity ▼ Rows: 100 ▼ Refresh: 5s ▼ Update

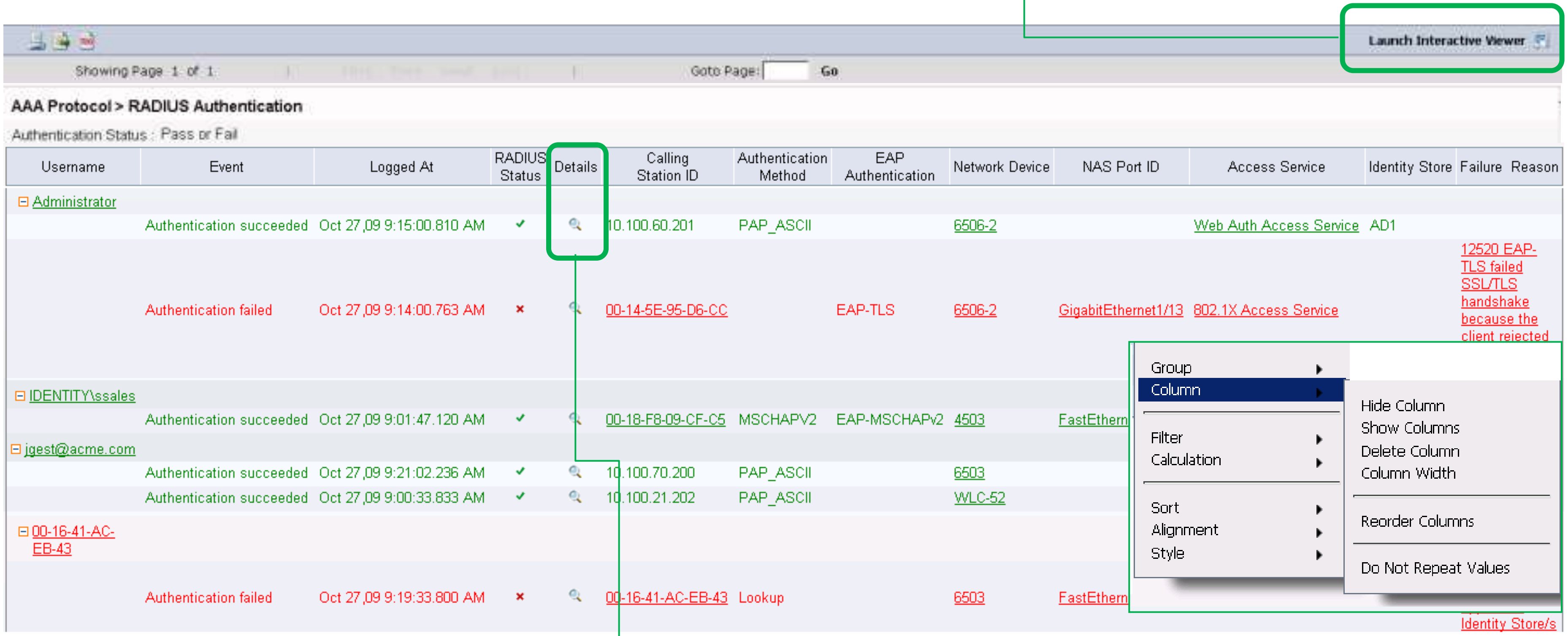
Last Update: Wed Feb 27 2008 09:44:25 GMT-0800 (PST)

Timestamp ?	Auth Type ?	MAC ?	Username ?	Group ?	NDG ?	NAD ?	Port ?	AFC ?	NAP ?	Domain ?	ACS ?
2008-02-27 09:43:46 PST	✓		azbycx	Default Group	[redacted]	[redacted]	azbycx		(Default)		[redacted]
2008-02-27 09:41:28 PST	✓		critical_test	maintenance	[redacted]	[redacted]	critical_test		(Default)		[redacted]
2008-02-27 09:40:13 PST	✓	00-1B-[redacted]	[redacted]	Default Group	[redacted]	[redacted]	50107		802.1x	[redacted]	[redacted]
2008-02-27 09:38:31 PST	✓	00-15-[redacted]	[redacted]	Default Group	[redacted]	[redacted]	50119		802.1x	[redacted]	[redacted]
2008-02-27 09:38:09 PST	✓	? 00-18-[redacted]	? [redacted]	MAB	[redacted]	[redacted]	Eth2/3 (131)		MAB		[redacted]
2008-02-27 08:21:57 PST	✓	00-1A-[redacted]	[redacted]	Default Group	[redacted]	[redacted]	50107		802.1x	[redacted]	[redacted]
2008-02-27 08:21:49 PST	✗	00-1A-6B-69-A9-AC	[redacted]	Default Group	[redacted]	[redacted]	50107	External DB user invalid or ba...	802.1x	[redacted]	[redacted]
2008-02-27 08:20:20 PST	✓		azbycx	Default Group	[redacted]	[redacted]	azbycx		(Default)		[redacted]
2008-02-27 08:16:02 PST	✓		azbycx	Default Group	[redacted]	[redacted]	azbycx		(Default)		[redacted]
2008-02-27 08:14:04 PST	✓	00-1A-[redacted]	k[redacted]	Default Group	[redacted]	[redacted]	50120		[redacted]-dot1x-2ndflr	[redacted]	[redacted]
2008-02-27 08:10:32 PST	✓		azbycx	Default Group	[redacted]	[redacted]	azbycx		(Default)		[redacted]
2008-02-27 08:10:04 PST	✓	? 00-1E-[redacted]	[redacted]	Default Group	[redacted]	[redacted]	50120		802.1x	[redacted]	[redacted]
2008-02-27 08:07:38 PST	✓	☎ 00-30-[redacted]	☎ 00[redacted]	mda_voice	[redacted]	[redacted]	50103		MAB		[redacted]
2008-02-27 08:07:38 PST	✓	☎ 00-03-[redacted]	☎ 00[redacted]	mda_voice	[redacted]	[redacted]	50107		MAB		[redacted]

Monitoring With ACS 5.1

Tip: Interactive Viewer Is Your Friend

Launch It, Then Right Click Inside the Report for Customization Options



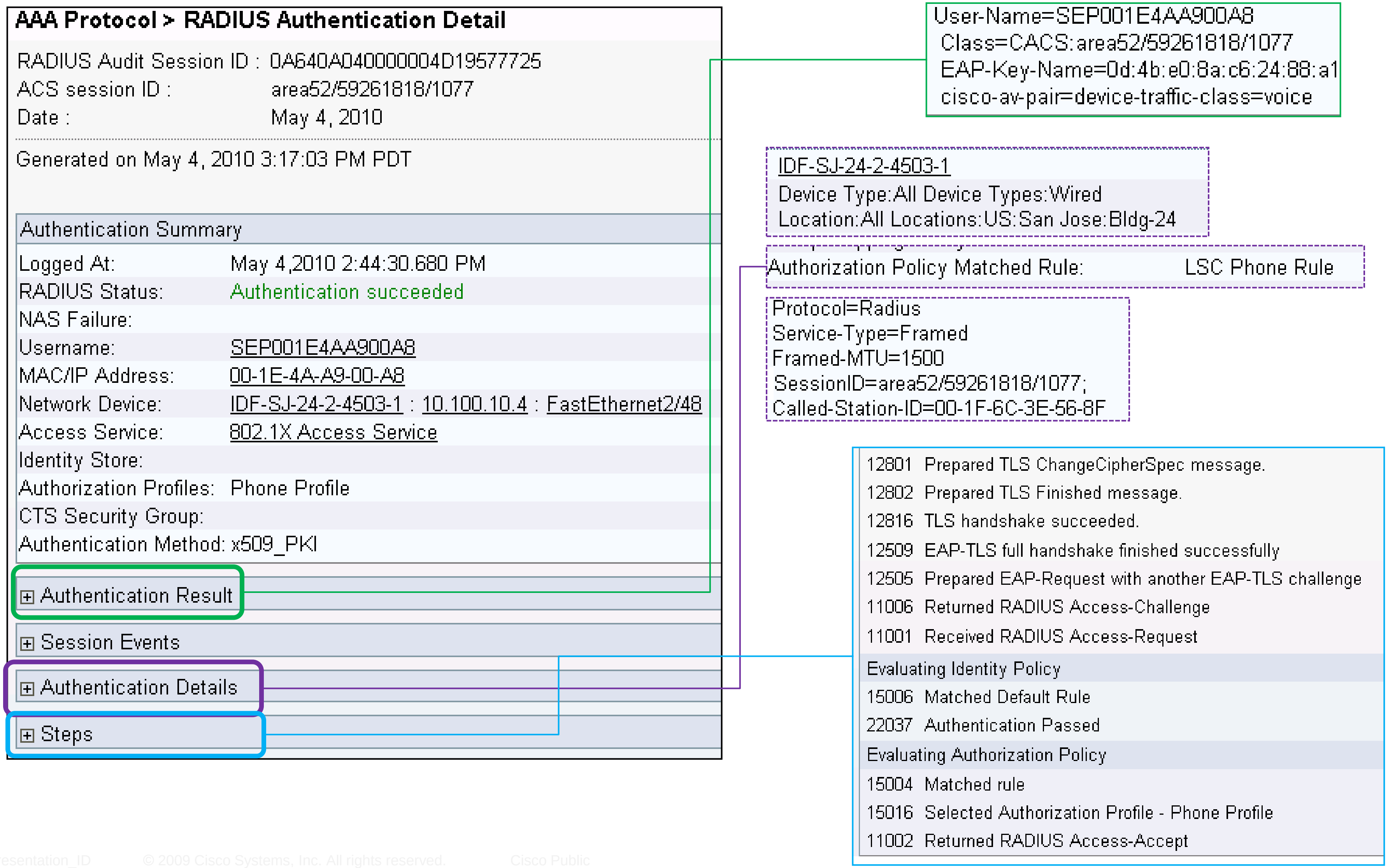
AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail

Username	Event	Logged At	RADIUS Status	Details	Calling Station ID	Authentication Method	EAP Authentication	Network Device	NAS Port ID	Access Service	Identity Store	Failure Reason
⊟ Administrator												
	Authentication succeeded	Oct 27,09 9:15:00.810 AM	✓	🔍	10.100.60.201	PAP_ASCII		6506-2		Web Auth Access Service	AD1	
	Authentication failed	Oct 27,09 9:14:00.763 AM	✗	🔍	00-14-5E-95-D6-CC		EAP-TLS	6506-2	GigabitEthernet1/13	802.1X Access Service		12520 EAP-TLS failed SSL/TLS handshake because the client rejected
⊟ IDENTITY\ssales												
	Authentication succeeded	Oct 27,09 9:01:47.120 AM	✓	🔍	00-18-F8-09-CF-C5	MSCHAPV2	EAP-MSCHAPv2	4503	FastEthern			
⊟ jgest@acme.com												
	Authentication succeeded	Oct 27,09 9:21:02.236 AM	✓	🔍	10.100.70.200	PAP_ASCII		6503				
	Authentication succeeded	Oct 27,09 9:00:33.833 AM	✓	🔍	10.100.21.202	PAP_ASCII		WLC-52				
⊟ 00-16-41-AC-EB-43												
	Authentication failed	Oct 27,09 9:19:33.800 AM	✗	🔍	00-16-41-AC-EB-43	Lookup		6503	FastEthern			Identity Store/s

Detailed Reports Are Lifesavers

ACS 5.1 Details Report



AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : 0A640A040000004D19577725
ACS session ID : area52/59261818/1077
Date : May 4, 2010

Generated on May 4, 2010 3:17:03 PM PDT

Authentication Summary

Logged At:	May 4,2010 2:44:30.680 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	SEP001E4AA900A8
MAC/IP Address:	00-1E-4A-A9-00-A8
Network Device:	IDF-SJ-24-2-4503-1 : 10.100.10.4 : FastEthernet2/48
Access Service:	802.1X Access Service
Identity Store:	
Authorization Profiles:	Phone Profile
CTS Security Group:	
Authentication Method:	x509_PKI

⊞ Authentication Result

⊞ Session Events

⊞ Authentication Details

⊞ Steps

```
User-Name=SEP001E4AA900A8
 Class=CACS:area52/59261818/1077
 EAP-Key-Name=0d:4b:e0:8a:c6:24:88:a1
 cisco-av-pair=device-traffic-class=voice
```

IDF-SJ-24-2-4503-1
Device Type:All Device Types:Wired
Location:All Locations:US:San Jose:Bldg-24

Authorization Policy Matched Rule: LSC Phone Rule

```
Protocol=Radius
Service-Type=Framed
Framed-MTU=1500
 SessionID=area52/59261818/1077;
Called-Station-ID=00-1F-6C-3E-56-8F
```

```
12801  Prepared TLS ChangeCipherSpec message.
12802  Prepared TLS Finished message.
12816  TLS handshake succeeded.
12509  EAP-TLS full handshake finished successfully
12505  Prepared EAP-Request with another EAP-TLS challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
Evaluating Identity Policy
15006  Matched Default Rule
22037  Authentication Passed
Evaluating Authorization Policy
15004  Matched rule
15016  Selected Authorization Profile - Phone Profile
11002  Returned RADIUS Access-Accept
```

Monitor Mode: Network Access Table

Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	Enterprise Access	Open authentication
Employees	802.1X Success	Enterprise Access	Open authentication
Corporate Asset	MAB Success	Enterprise Access	Open authentication
Phones	802.1X or MAB Success	Voice Access	Open authentication
Employees	802.1X Fail -> MAB	Enterprise Access	Open authentication
Sponsored Guest	802.1X Fail/Timeout -> MAB Fail	Enterprise Access	Open authentication
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail	Enterprise Access	Open authentication
All	None (AAA server down)	Enterprise Access	Open authentication

Low Impact Mode

ACME’s Goals: Phase 2

- Maintain Visibility
- Control Access to Sensitive Assets
- Preserve Network Access for Managed Assets

  Special Case: PXE boot

- Preserve Current Network Architecture

  No changes to VLAN infrastructure

ACME’s Goals Can Be Met With
Low Impact Mode

Access Control & Clientless Devices

The Timing Problem With MAB

- MAB depends on 802.1X timeout
- Many devices are time-sensitive
- DHCP is especially finicky

The Low Impact Solution

- Provide access to time-critical services **before** authentication
- Continue to restrict access to other services until after authentication

ACME's Time-Critical Services

- DHCP, DNS, TFTP
- This is enough for PXE devices to boot before MAB completes

Low Impact: Network Access Table

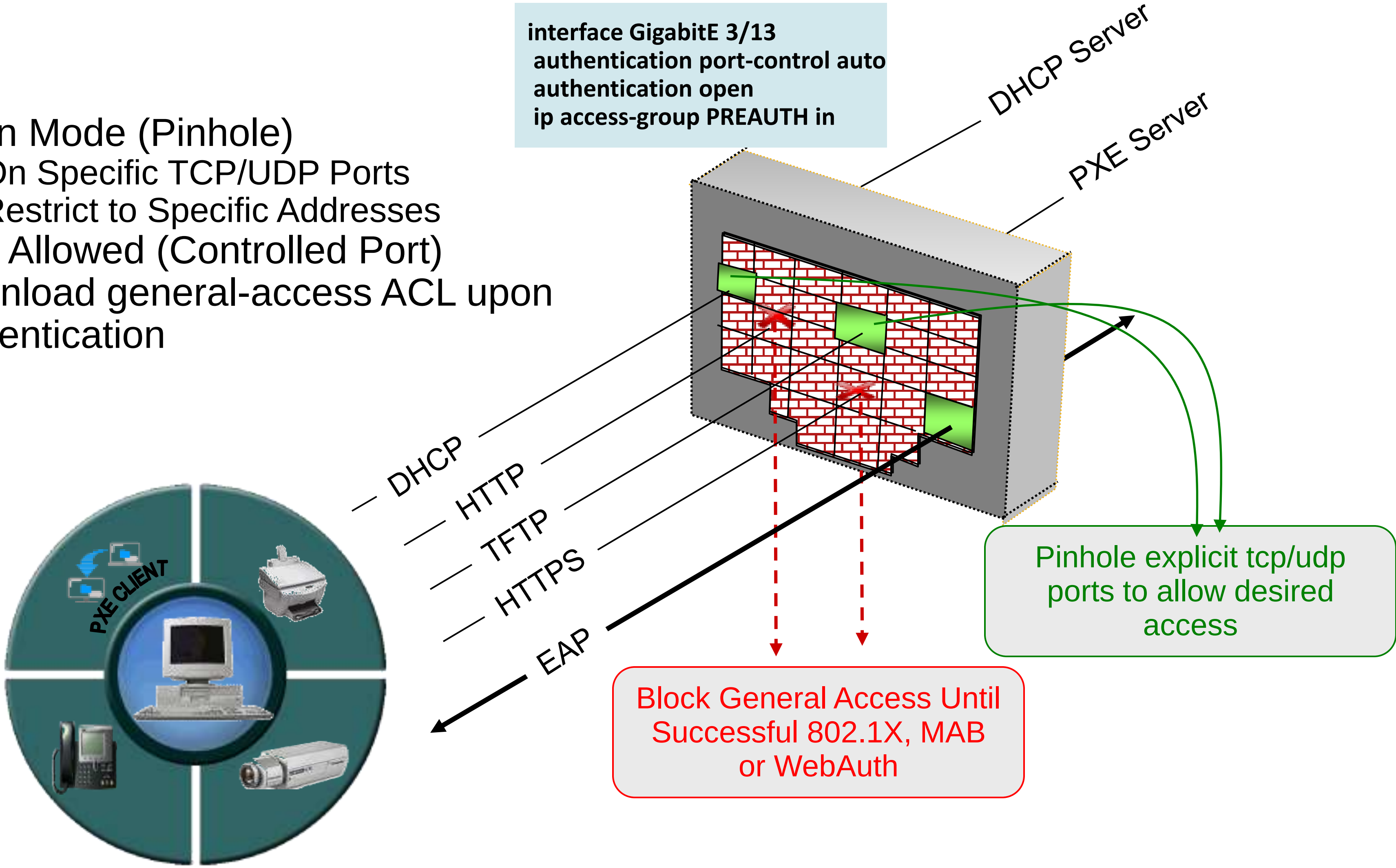
Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	Limited Access	
Employees	802.1X Success	Enterprise Access	
Corporate Asset	MAB Success	Enterprise Access	
Phones	802.1X or MAB Success	Voice Access	
Employees	802.1X Fail -> MAB or Web-Auth Success	Enterprise Access	
Sponsored Guest	802.1X Fail/Timeout -> MAB Fail -> Web-Auth Success	Limited + Internet Access	
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail -> Web-Auth Fail	Limited Access	
All	None (AAA server down)	Limited Access	

Low Impact Implementation

Limited (“Selectively Open”) Access

```
interface GigabitE 3/13
 authentication port-control auto
 authentication open
 ip access-group PREAUTH in
```

- Open Mode (Pinhole)
  - On Specific TCP/UDP Ports
  - Restrict to Specific Addresses
- EAP Allowed (Controlled Port)
- Download general-access ACL upon authentication



Pinhole explicit tcp/udp ports to allow desired access

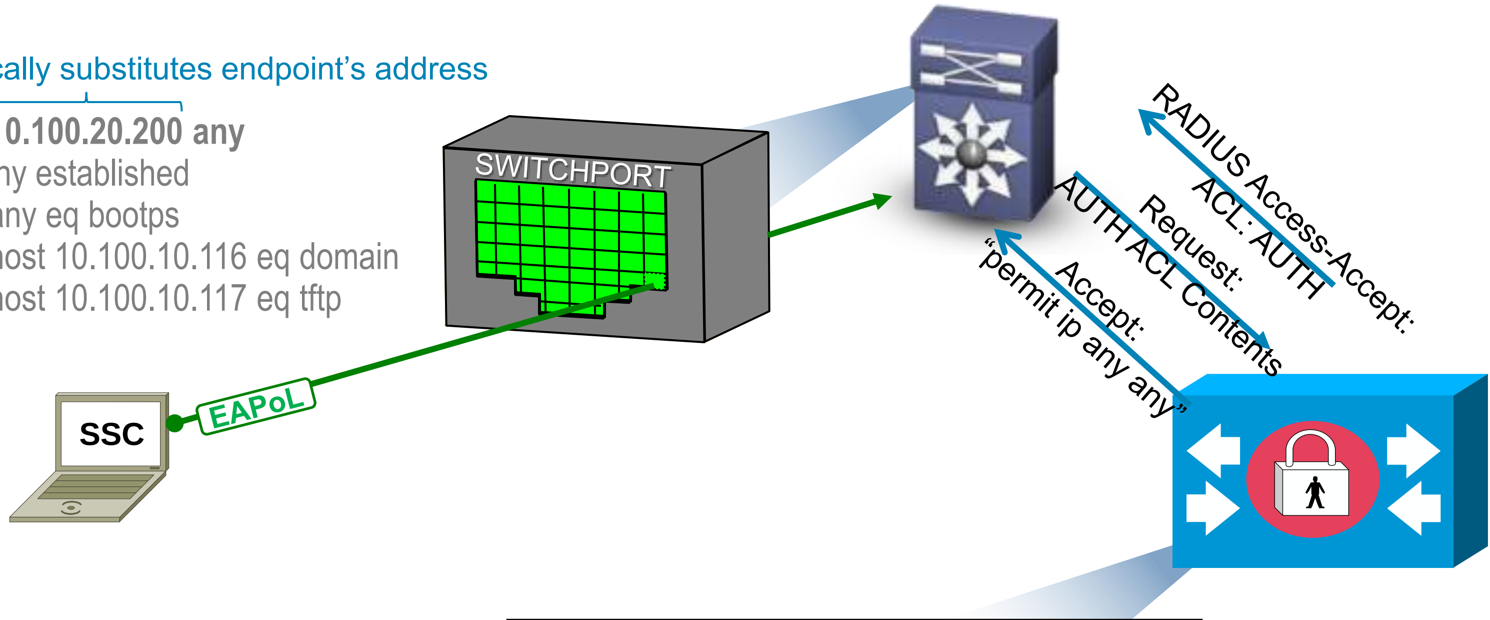
Block General Access Until Successful 802.1X, MAB or WebAuth

dACLs Open Port After Authentication

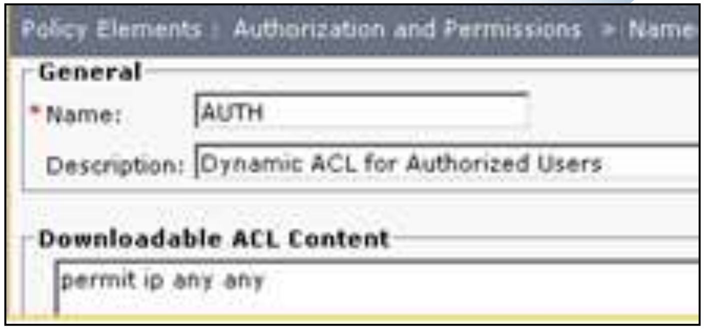
- Configure downloadable ACLs (dACL) for authenticated users

Switch dynamically substitutes endpoint's address

```
        permit ip host 10.100.20.200 any
        permit tcp any any established
PREAUTH permit udp any any eq bootps
ACL     permit udp any host 10.100.10.116 eq domain
        permit udp any host 10.100.10.117 eq tftp
```



- Contents of dACL are arbitrary.
- Can have as many unique dACLs are there are user permission groups
- Same principles as pre-auth port ACL



General

* Name: AUTH

Description: Dynamic ACL for Authorized Users

Downloadable ACL Content

```
permit ip any any
```

Low Impact: Network Access Table

Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	Limited Access	Pre-Auth ACL
Employees	802.1X Success	Enterprise Access	Permit-Any dACL
Corporate Asset	MAB Success	Enterprise Access	Permit-Any dACL
Phones	802.1X or MAB Success	Voice Access	
Employees	802.1X Fail -> MAB or Web-Auth Success	Enterprise Access	
Sponsored Guest	802.1X Fail/Timeout -> MAB Fail -> Web-Auth Success	Limited + Internet Access	
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail -> Web-Auth Fail	Limited Access	Pre-Auth ACL
All	None (AAA server down)	Limited Access	Pre-Auth ACL

DEMO Time

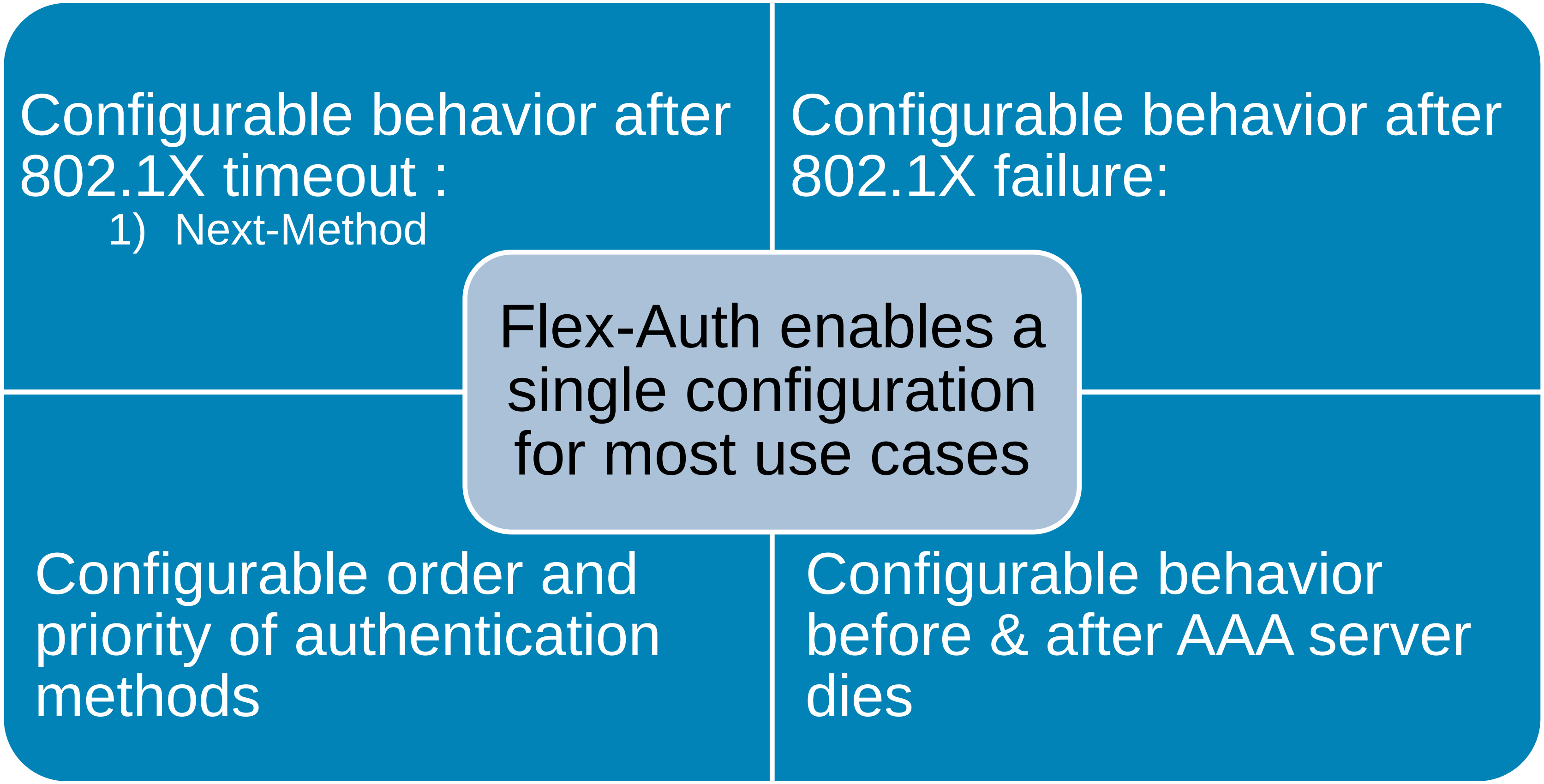
PXE boot and Enterprise Access

- pre-Auth ACL
- dACL

Low Impact Mode:
Flex Auth

Flexible Authentication: “Flex-Auth”

One Configuration Fits Most



Configurable behavior after 802.1X timeout :

1) Next-Method

Configurable behavior after 802.1X failure:

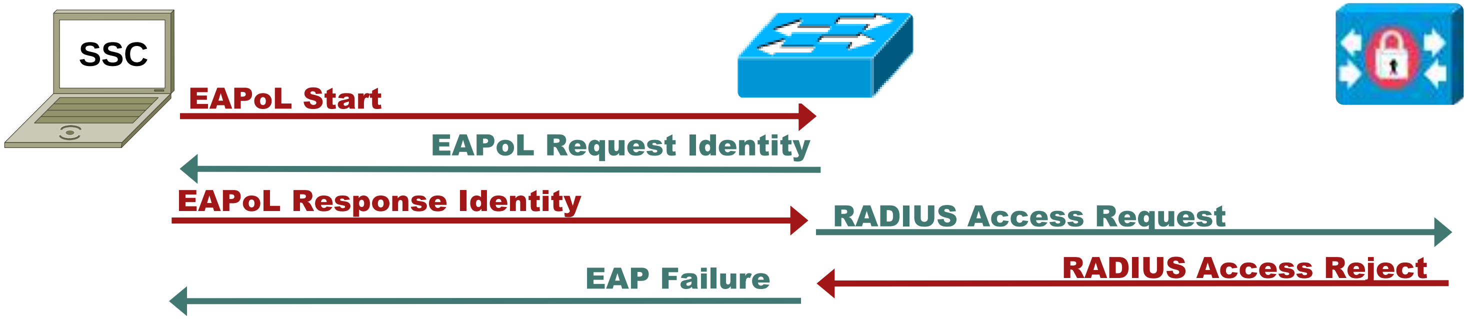
Flex-Auth enables a single configuration for most use cases

Configurable order and priority of authentication methods

Configurable behavior before & after AAA server dies

802.1X Failure vs. 802.1X Timeout

An 802.1X **failure** occurs when the AAA server rejects the request:



SSC

EAPoL Start

EAPoL Request Identity

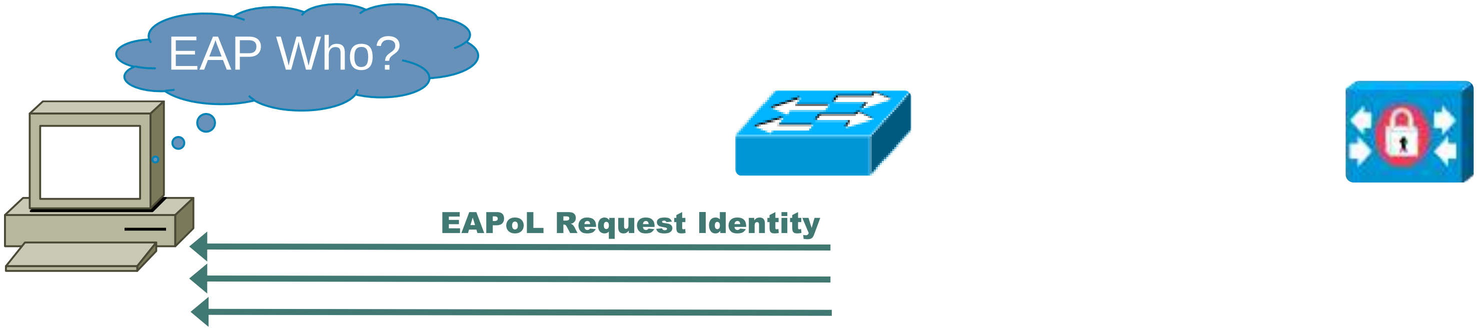
EAPoL Response Identity

RADIUS Access Request

EAP Failure

RADIUS Access Reject

A **timeout** occurs when an endpoint can’t speak 802.1X:

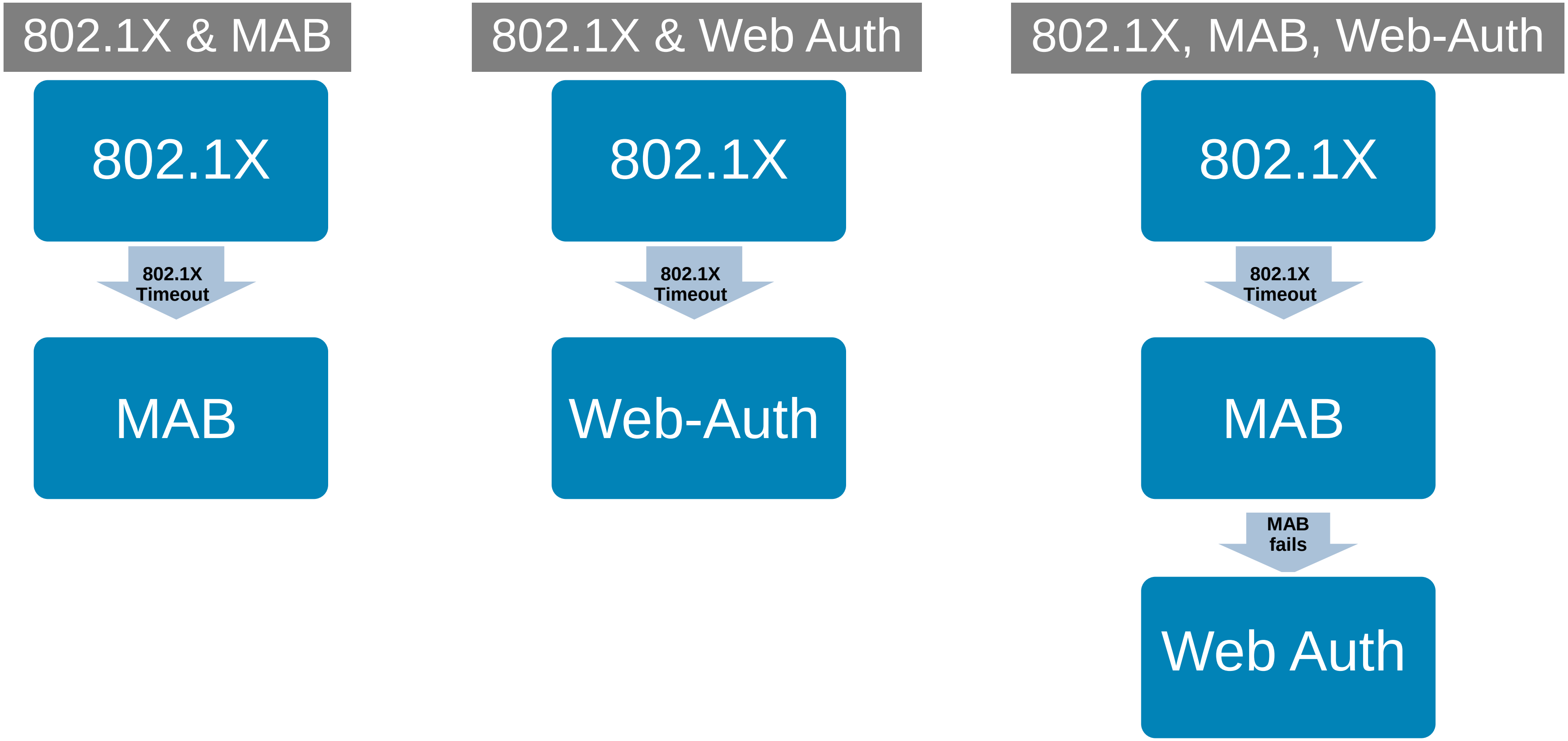


EAP Who?

EAPoL Request Identity

Default Behavior on 802.1X Timeout

- After 802.1X times out, port automatically falls back to “next-method” if another method is configured.



802.1X & MAB

802.1X

802.1X Timeout

MAB

802.1X & Web Auth

802.1X

802.1X Timeout

Web-Auth

802.1X, MAB, Web-Auth

802.1X

802.1X Timeout

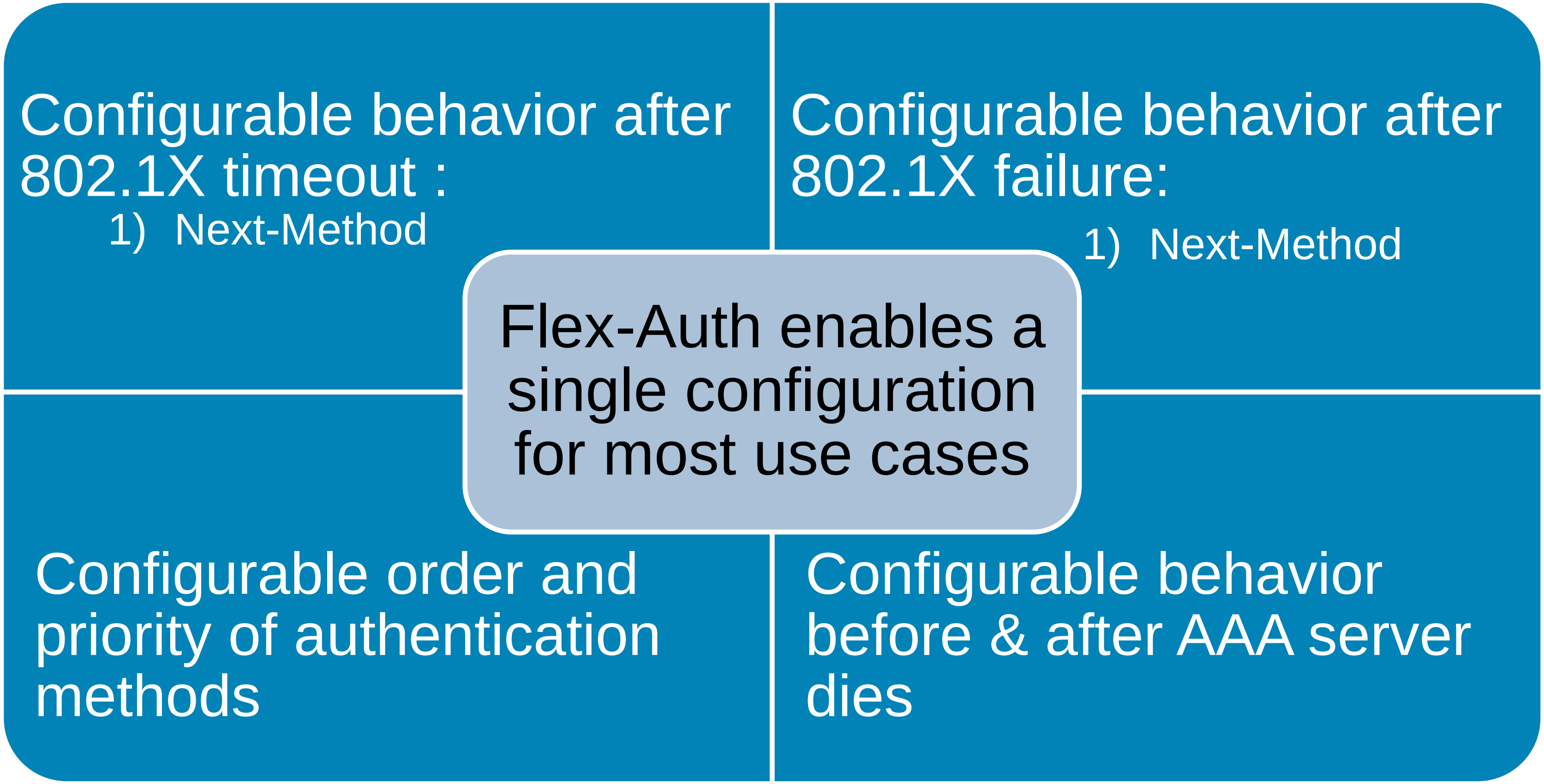
MAB

MAB fails

Web Auth

Flex-Auth for 802.1X Failures

Low Impact Mode



Configurable behavior after 802.1X timeout :

1) Next-Method

Configurable behavior after 802.1X failure:

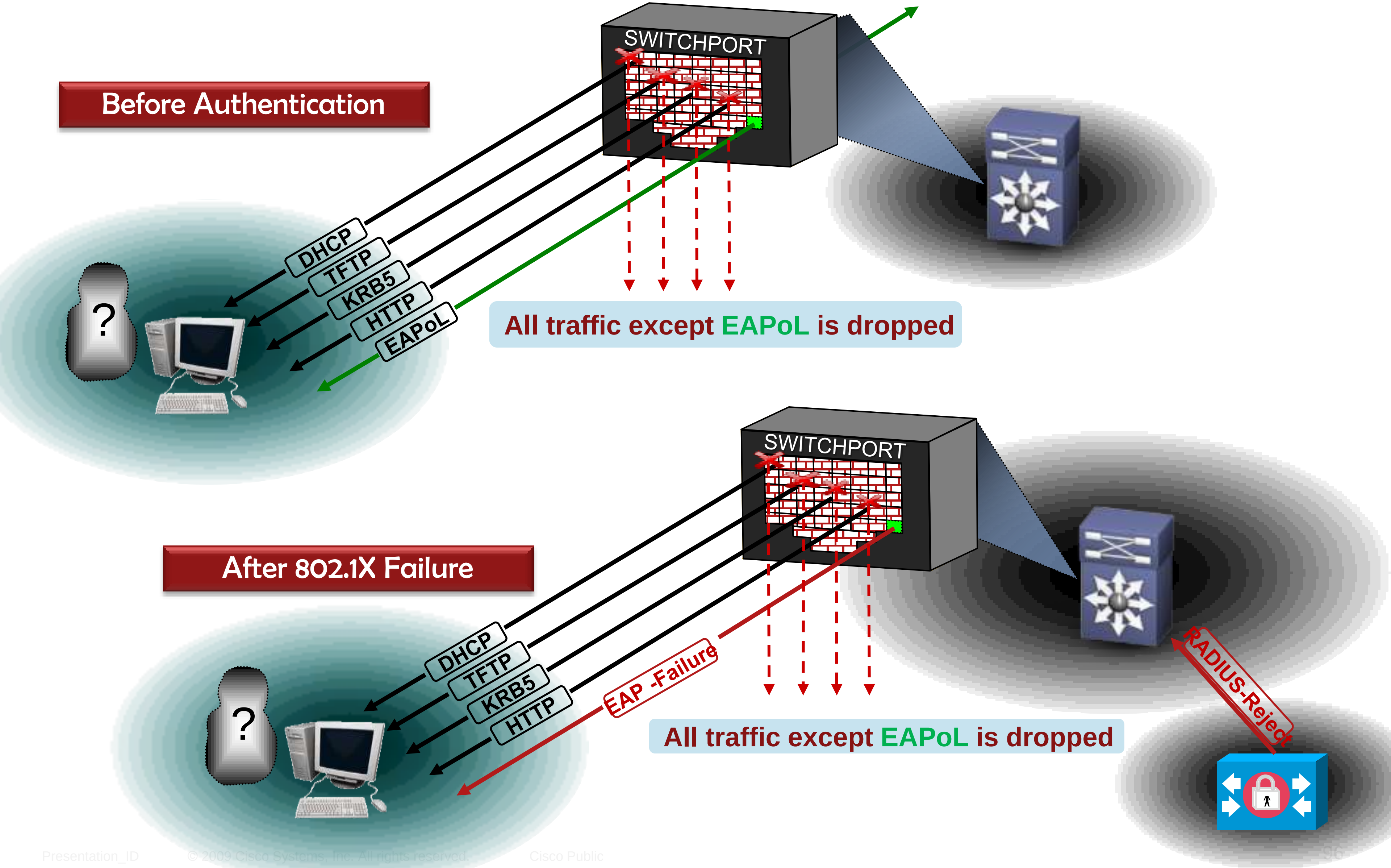
1) Next-Method

Flex-Auth enables a single configuration for most use cases

Configurable order and priority of authentication methods

Configurable behavior before & after AAA server dies

Default Security After 802.1X Failure



Before Authentication

All traffic except EAPoL is dropped

After 802.1X Failure

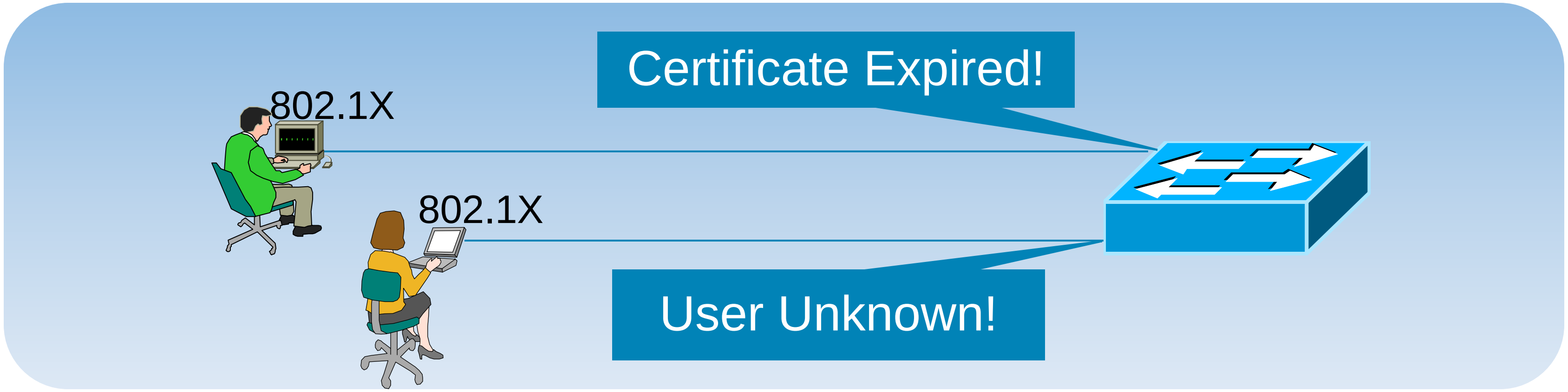
All traffic except EAPoL is dropped

Why Provide Access to Devices that Fail?

Employees' credentials expire or get entered incorrectly

As 802.1X becomes more prevalent, more guests will fail auth because they have 802.1X enabled by default.

Many enterprises require guests and failed corporate assets get conditional access to the network



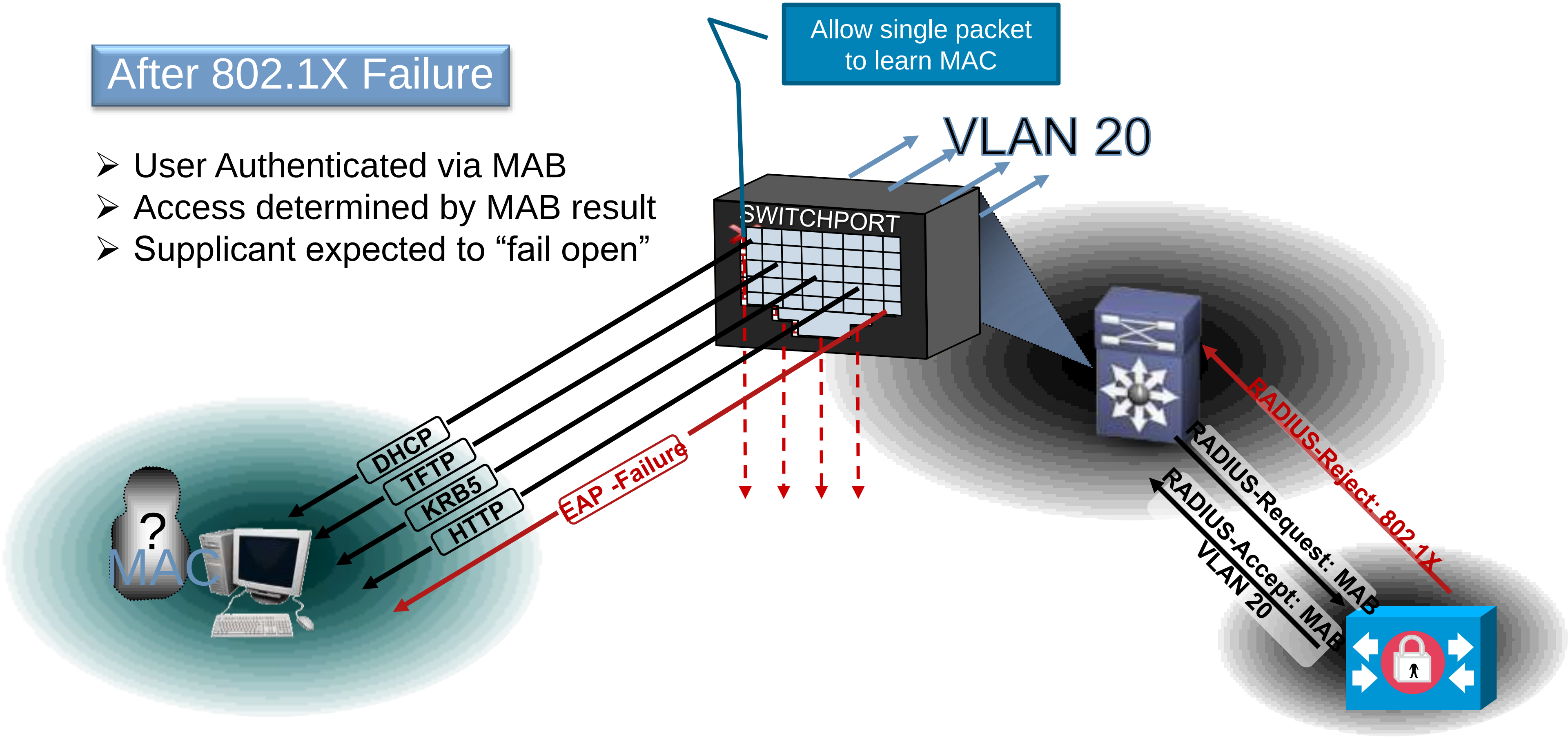
Certificate Expired!

User Unknown!

Failed Auth with Flex-auth: Next-method

After 802.1X Failure

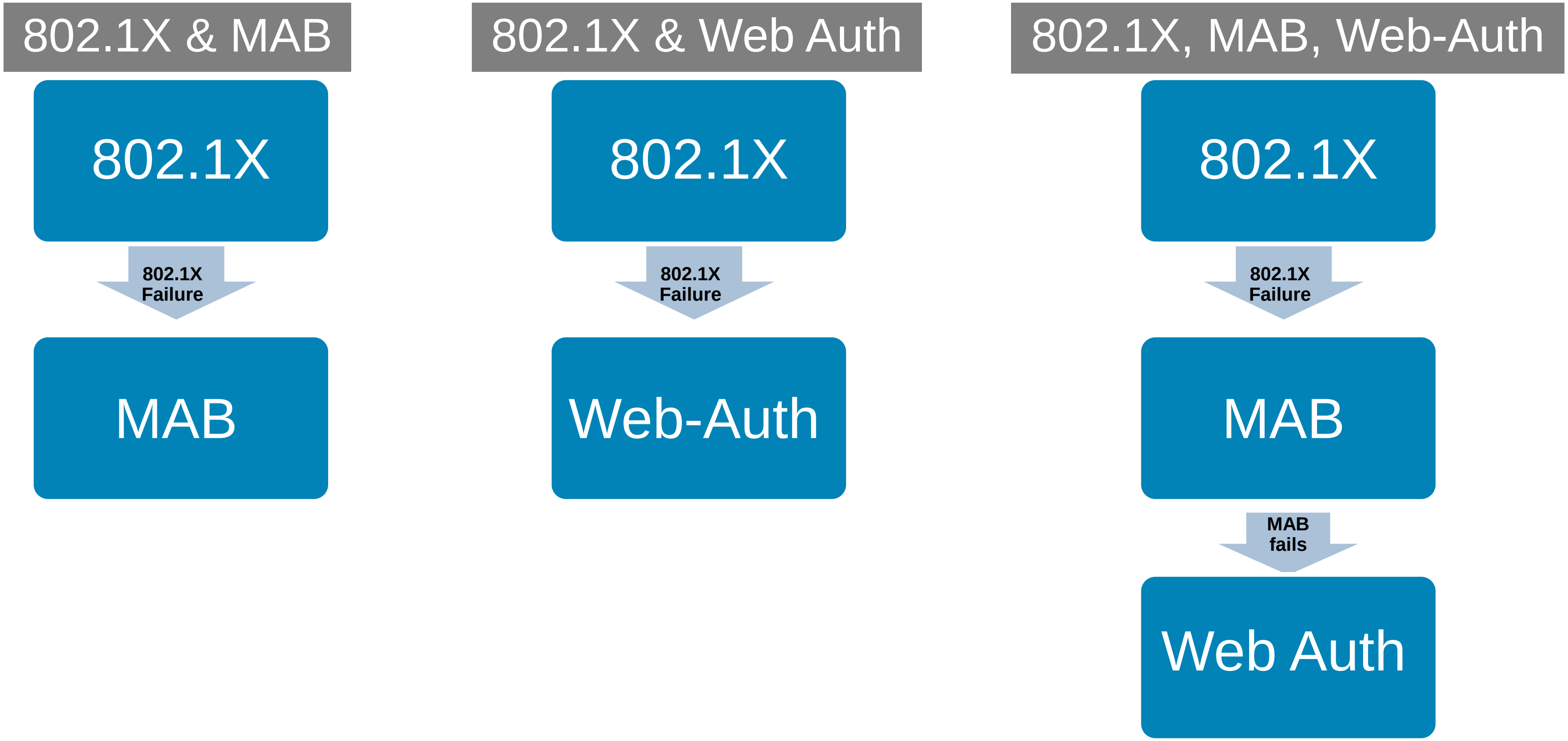
- ➢ User Authenticated via MAB
- ➢ Access determined by MAB result
- ➢ Supplicant expected to “fail open”



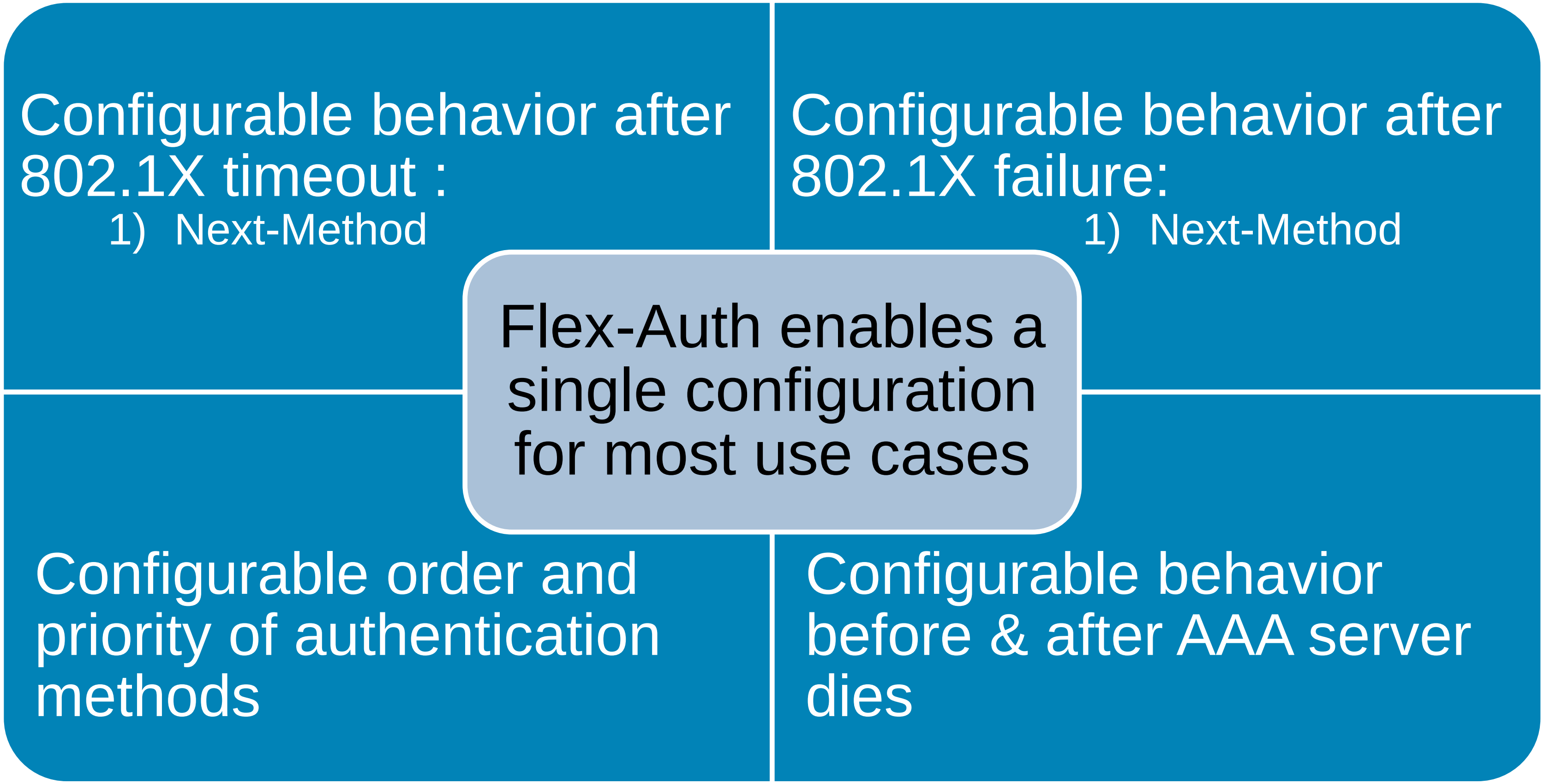
```
6506-2(config-if)#authentication event fail action next method
6506-2(config-if)#authentication order dot1x mab
```

802.1X Failure with Next-Method

- When port is configured to fail to next method, port falls back to “next-method” in the following order.



Flex-Auth Order & Priority



Configurable behavior after 802.1X timeout :

1) Next-Method

Configurable behavior after 802.1X failure:

1) Next-Method

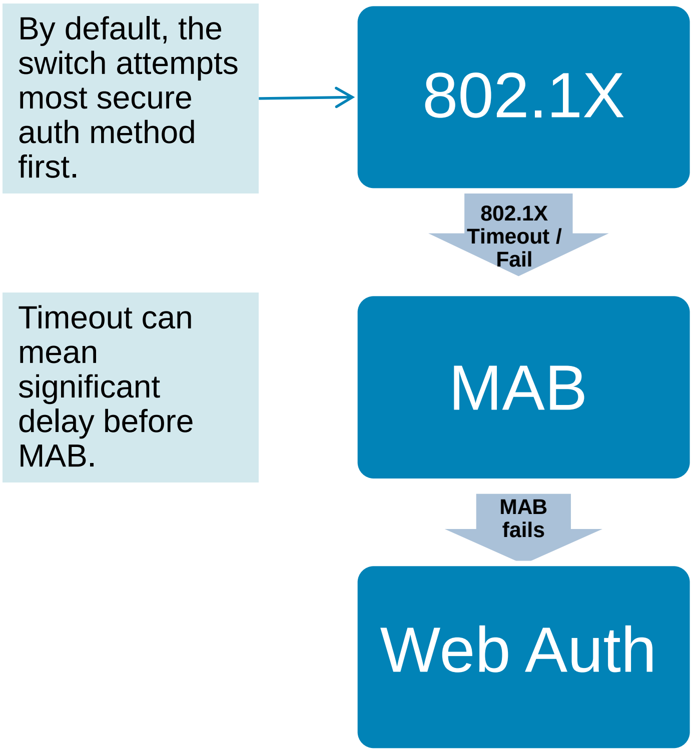
Flex-Auth enables a single configuration for most use cases

Configurable order and priority of authentication methods

Configurable behavior before & after AAA server dies

Flex-Auth Sequencing

Default Order: 802.1X First



By default, the switch attempts most secure auth method first.

802.1X

802.1X Timeout / Fail

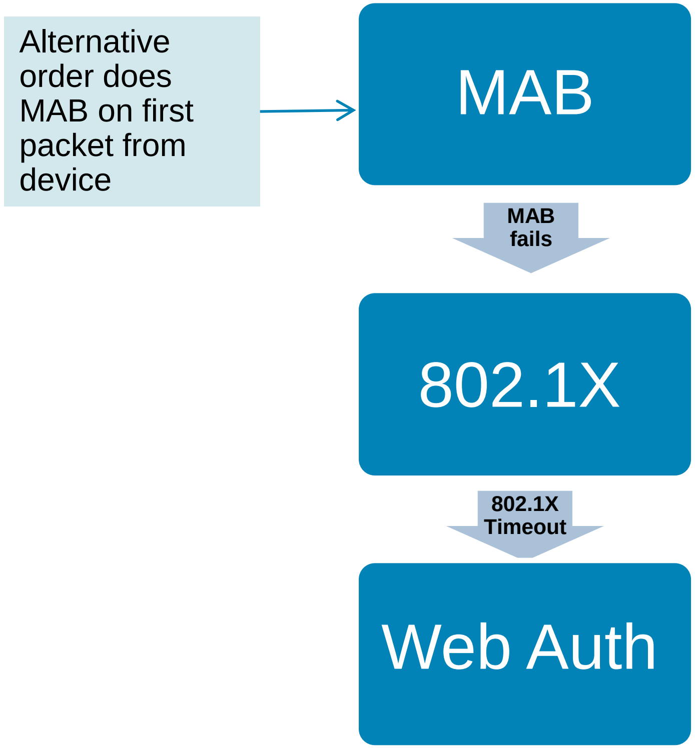
Timeout can mean significant delay before MAB.

MAB

MAB fails

Web Auth

Flex-Auth Order: MAB First



Alternative order does MAB on first packet from device

MAB

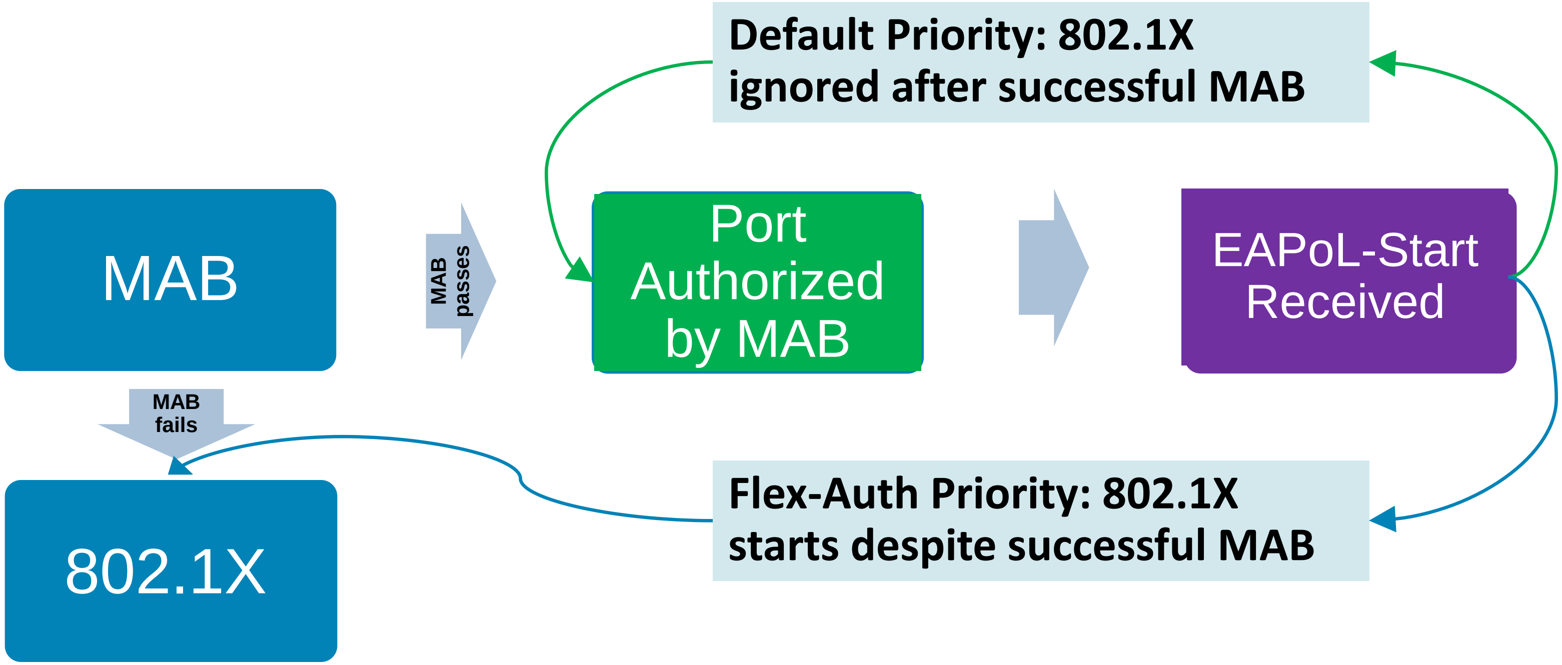
MAB fails

802.1X

802.1X Timeout

Web Auth

Flex-Auth Order with Flex-Auth Priority



Default Priority: 802.1X ignored after successful MAB

MAB

MAB passes

Port Authorized by MAB

EAPoL-Start Received

MAB fails

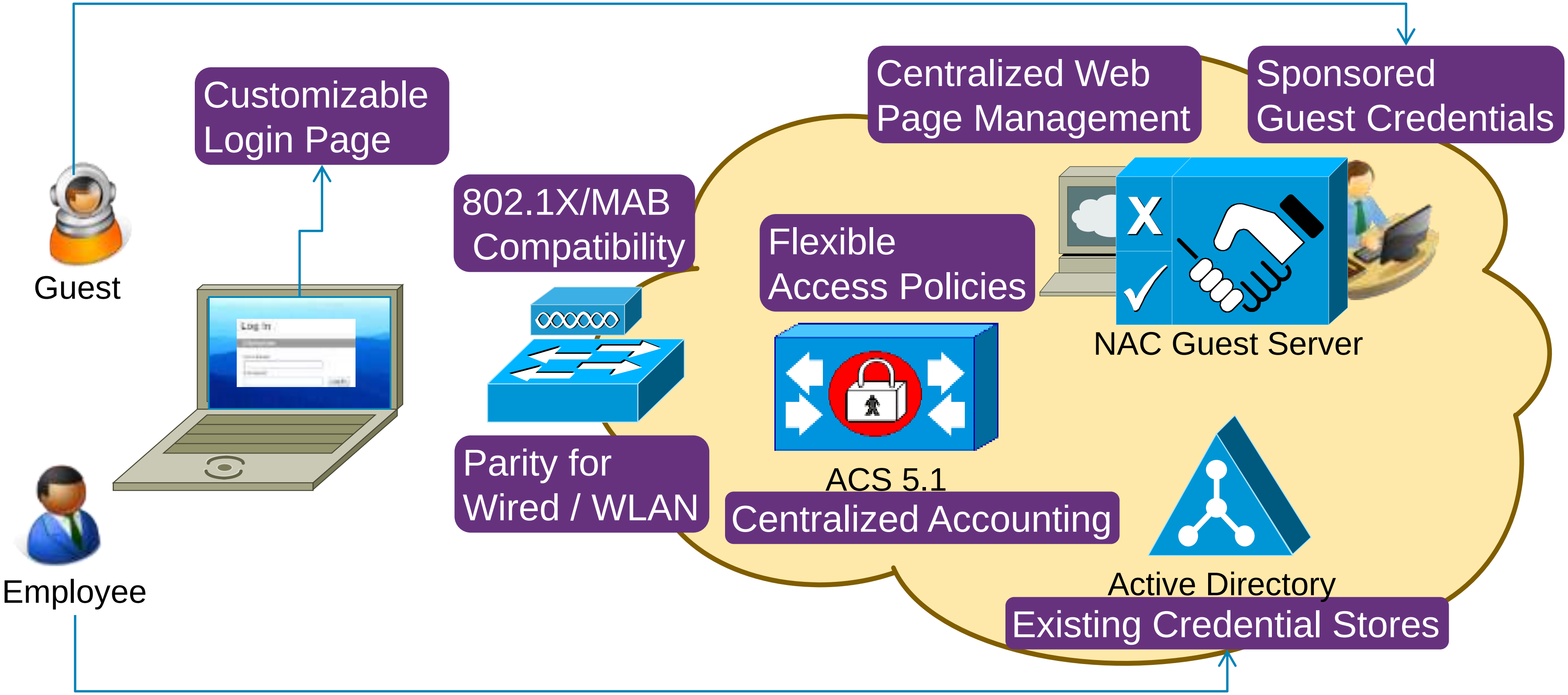
802.1X

Flex-Auth Priority: 802.1X starts despite successful MAB

- Priority determines which method can preempt other methods.
- By default, method sequence determines priority (first method has highest priority).
- If MAB has priority, EAPoL-Starts will be ignored if MAB passes.

Low Impact Mode:
Web Auth

What ACME Expects for Web Auth



Guest

Employee

Customizable Login Page

802.1X/MAB Compatibility

Parity for Wired / WLAN

Flexible Access Policies

ACS 5.1

Centralized Accounting

Centralized Web Page Management

Sponsored Guest Credentials

NAC Guest Server

Active Directory

Existing Credential Stores

Integrated Local Web Authentication

Introducing…Web-Auth's New Best Friend

NAC Guest Server (NGS)

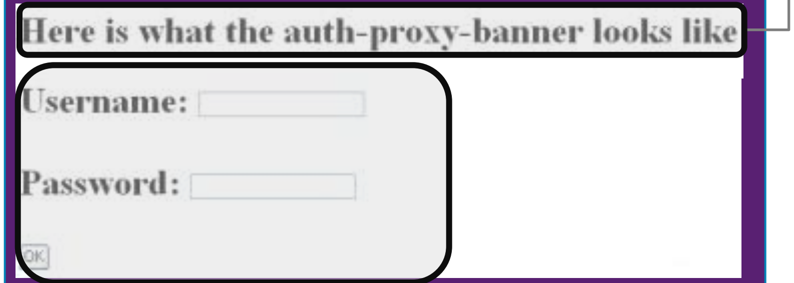
- Multi-Function Standalone Appliance
- Customizable Hotspot Hosting
- Sponsored Guest Access Provisioning, Verification, Management

Product Bulletin: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/prod_bulletin0900aecd806f3235.html
Data Sheet: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd806e98c9.html

Basic Wired: Distributed Login Pages

Default (Auth-Proxy Banner)

```
ip admission auth-proxy-banner http ^C Here is what the auth-proxy-banner looks like ^C
```



Here is what the auth-proxy-banner looks like

Username:

Password:

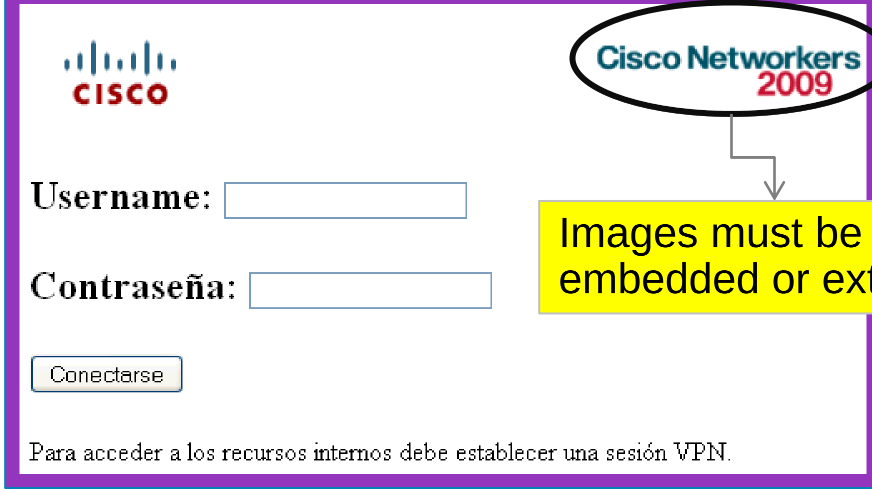
Text only

Fixed Text

Customized

4 files, 8KB max each

```
ip admission proxy http login expired page file bootflash:expired.html
ip admission proxy http login page file bootflash:login.html
ip admission proxy http success page file bootflash:success.html
ip admission proxy http failure page file bootflash:fail.html
```



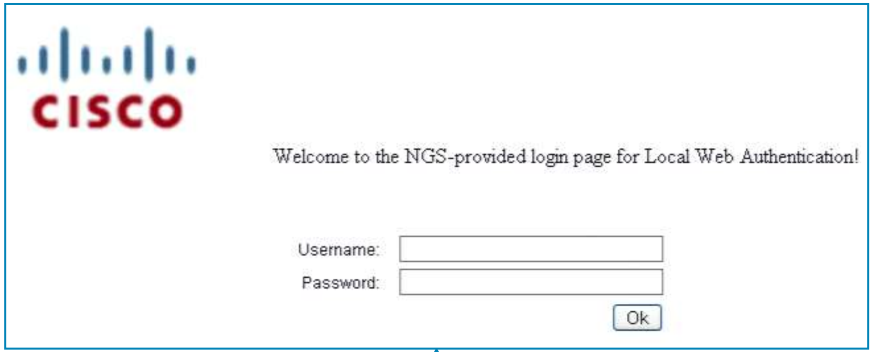
Username:

Contraseña:

Para acceder a los recursos internos debe establecer una sesión VPN.

Images must be embedded or external

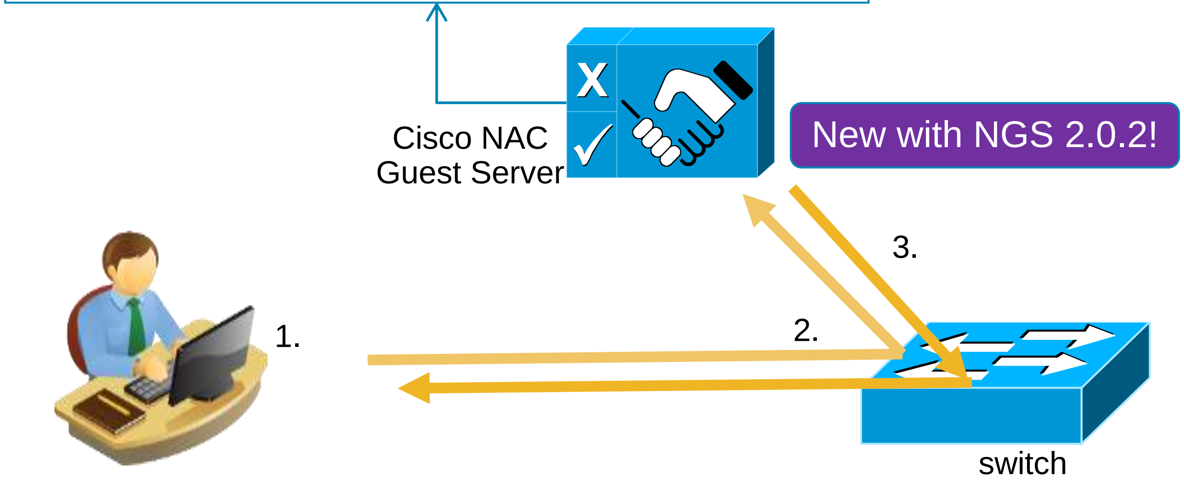
Enhanced Web Auth – Centralized Login Page



Welcome to the NGS-provided login page for Local Web Authentication!

Username:

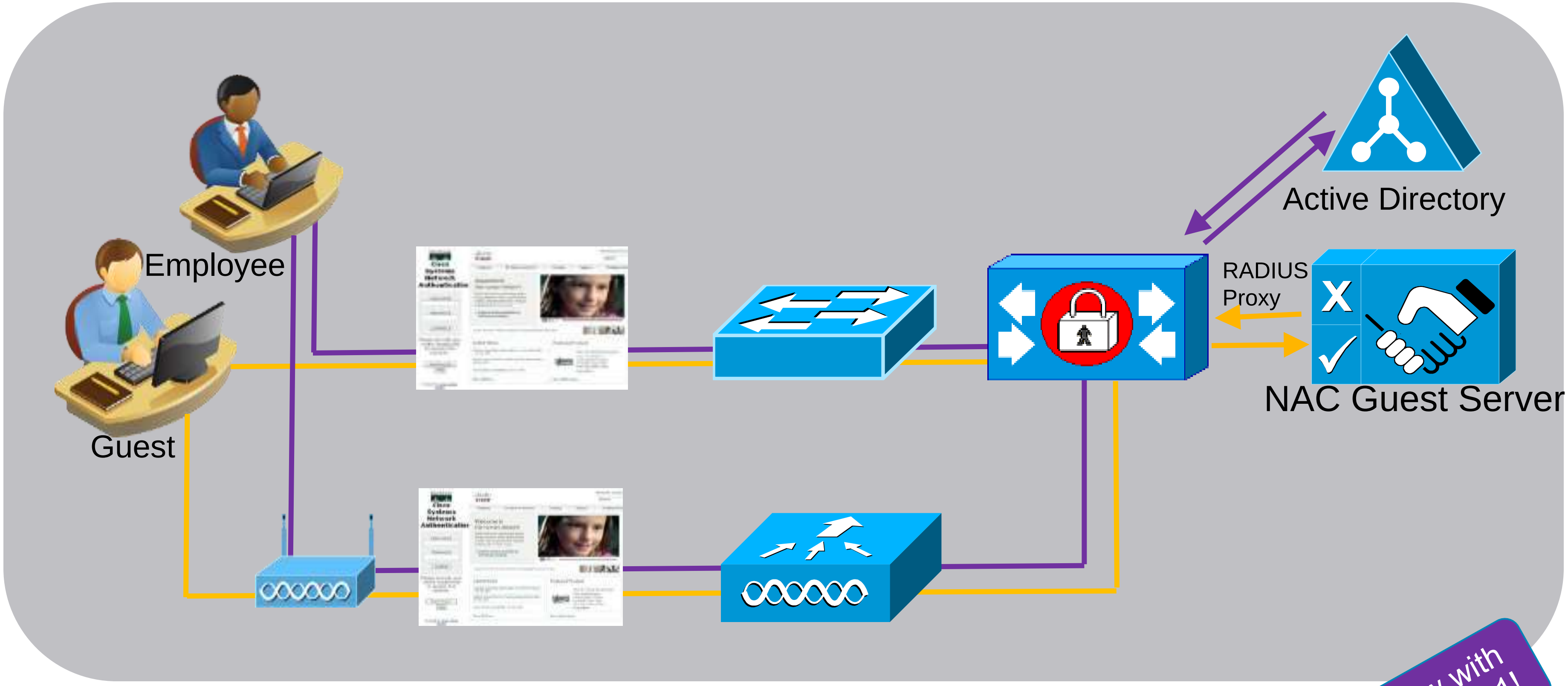
Password:



New with NGS 2.0.2!

1. Guest opens Web browser
2. Web traffic is intercepted by switch and redirected to Guest Server.
3. Guest Server returns centralized login page

Web Authentication Can Be Used For Guests and/or Employees



New with ACS 5.1!

- ACS can use RADIUS proxy to validate sponsored guest credentials on NGS
- ACS can query other ID stores (like AD) to validate employee credentials
- ACS policy can assign different levels of access to Guest and Employee

Low Impact: Network Access Table

Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	Limited Access	Pre-Auth ACL
Employees	802.1X Success	Enterprise Access	Permit-Any dACL
Corporate Asset	MAB Success	Enterprise Access	Permit-Any dACL
Phones	802.1X or MAB Success	Voice Access	
Employees	802.1X Fail -> MAB or Web-Auth Success	Enterprise Access	Permit-Any dACL
Sponsored Guest	802.1X Fail/Timeout -> MAB Fail -> Web-Auth Success	Limited + Internet Access	Permit-Internet dACL
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail -> Web-Auth Fail	Limited Access	Pre-Auth ACL
All	None (AAA server down)	Limited Access	Pre-Auth ACL

DEMO Time

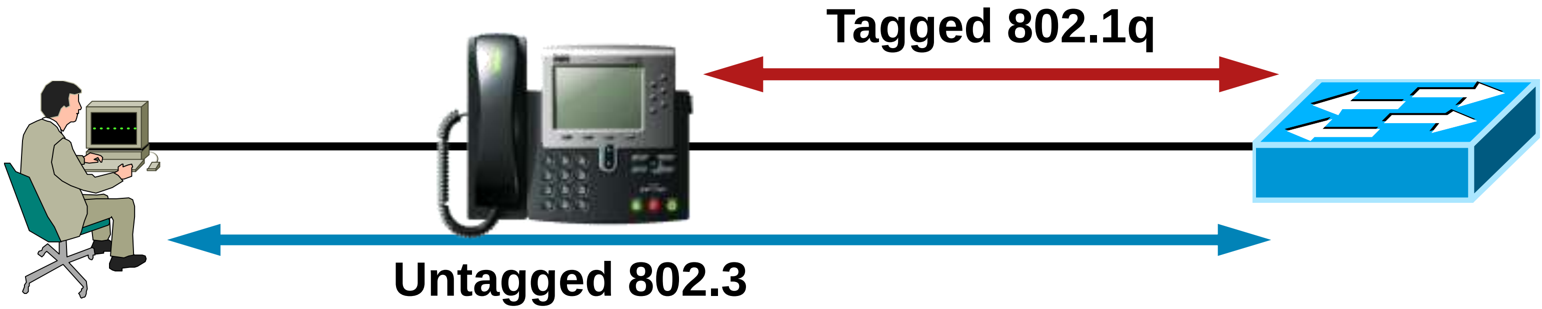
Next-Method for 802.1X Timeout & Fail

Web-Auth

Low Impact Mode:
IP Telephony

802.1X & IPT: A Special Case

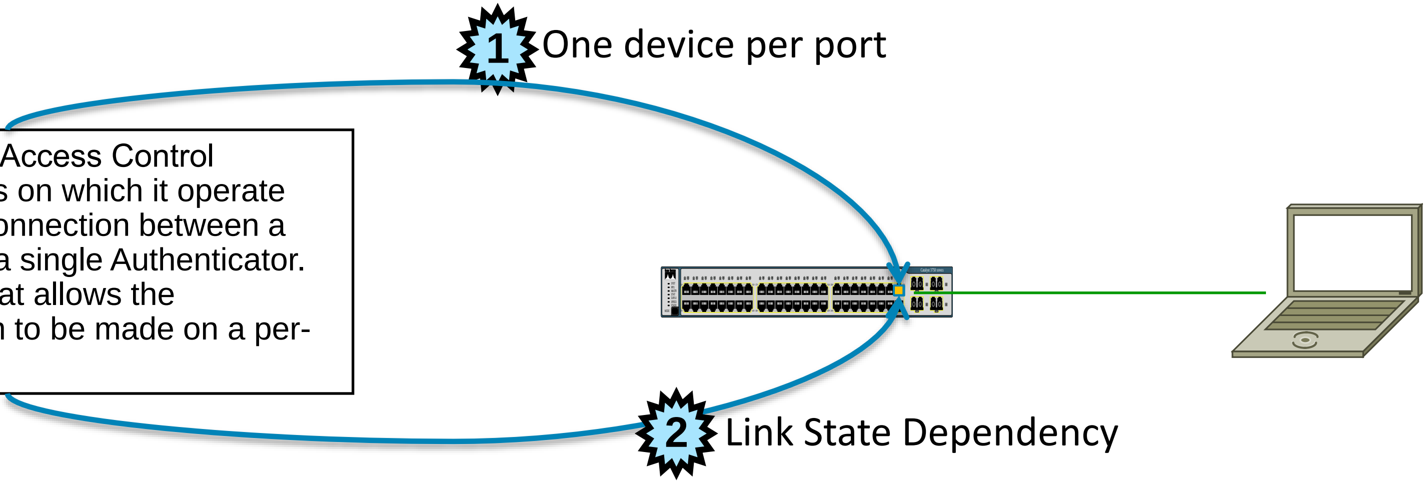
- **Voice Ports**
- With Voice Ports, a port can belong to two VLANs, while still allowing the separation of voice/data traffic while enabling you to configure 802.1X
- An access port able to handle two VLANs
  - Native or Port VLAN Identifier (PVID) / Authenticated by 802.1X
  - Auxiliary or Voice VLAN Identifier (VVID) / "Authenticated" by CDP
- Hardware set to dot1q trunk

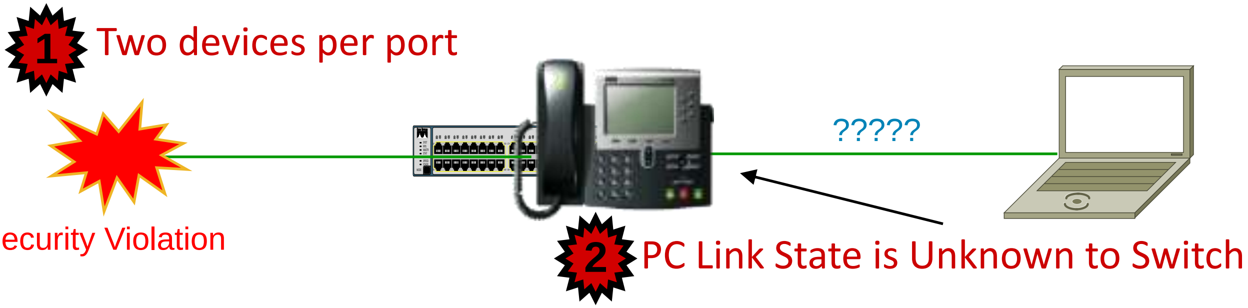


IPT & 802.1X: Fundamental Challenges

“The operation of Port Access Control assumes that the Ports on which it operate offer a point-to-point connection between a single Supplicant and a single Authenticator. It is this assumption that allows the authentication decision to be made on a per-Port basis.”

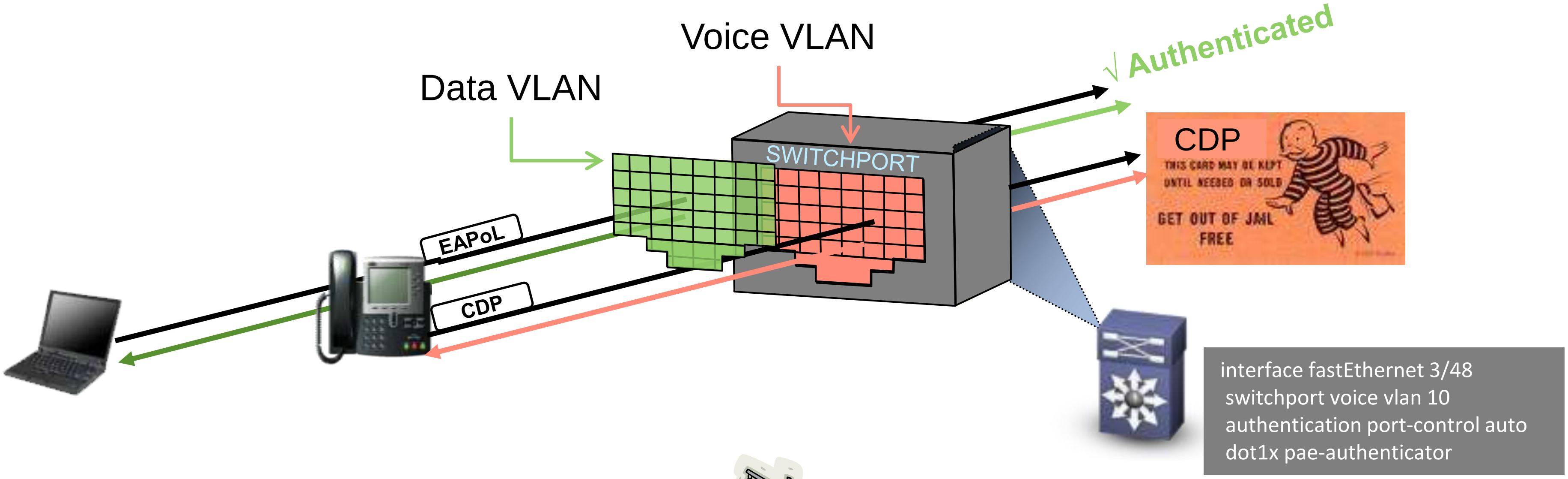
IEEE 802.1X rev 2004





IPT Breaks the Point-to-Point Model

First Solution: CDP Bypass



```
interface fastEthernet 3/48
 switchport voice vlan 10
 authentication port-control auto
 dot1x pae-authenticator
```

Benefits	Deployment Considerations
Access to voice VLAN after phone sends CDP	CDP-capable hackers get full access, too.
Default behavior: Cisco IP Phones get access if voice VLAN configured	No visibility, No access control
Works for all Cisco phone models	Incompatible with dynamic VVID, downloadable ACLs (dACLs), PC Web Auth

Second Solution: Multi-Domain Authentication (MDA) Host Mode

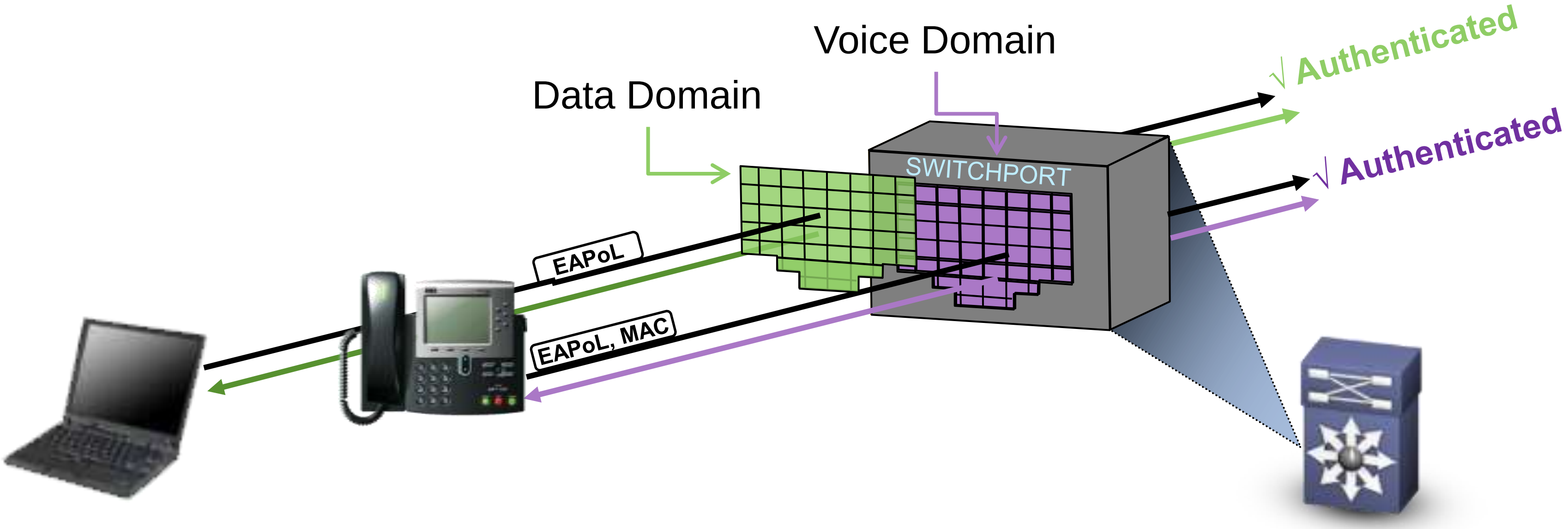
IEEE 802.1X

Single device per port

→

MDA

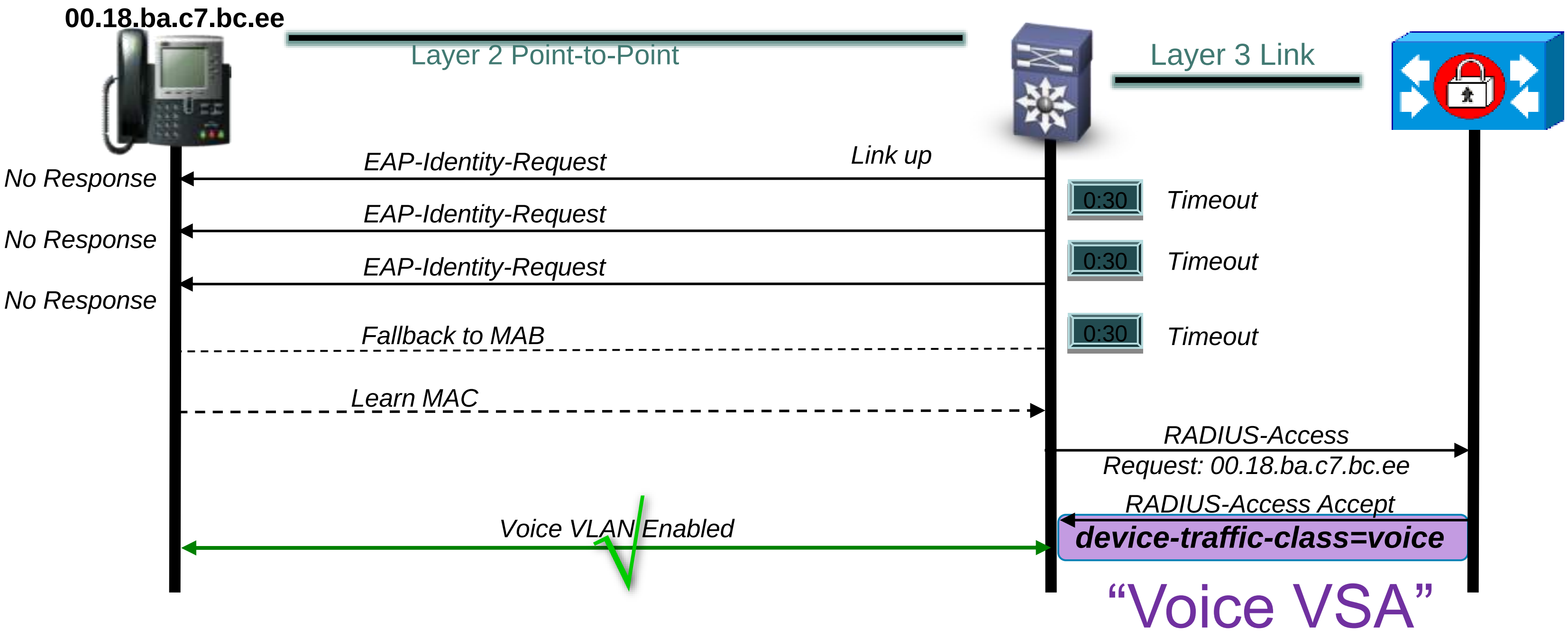
Single device *per domain* per port



- Phones and PCs use 802.1X or MAB
- MDA is a subset of Multi-Auth

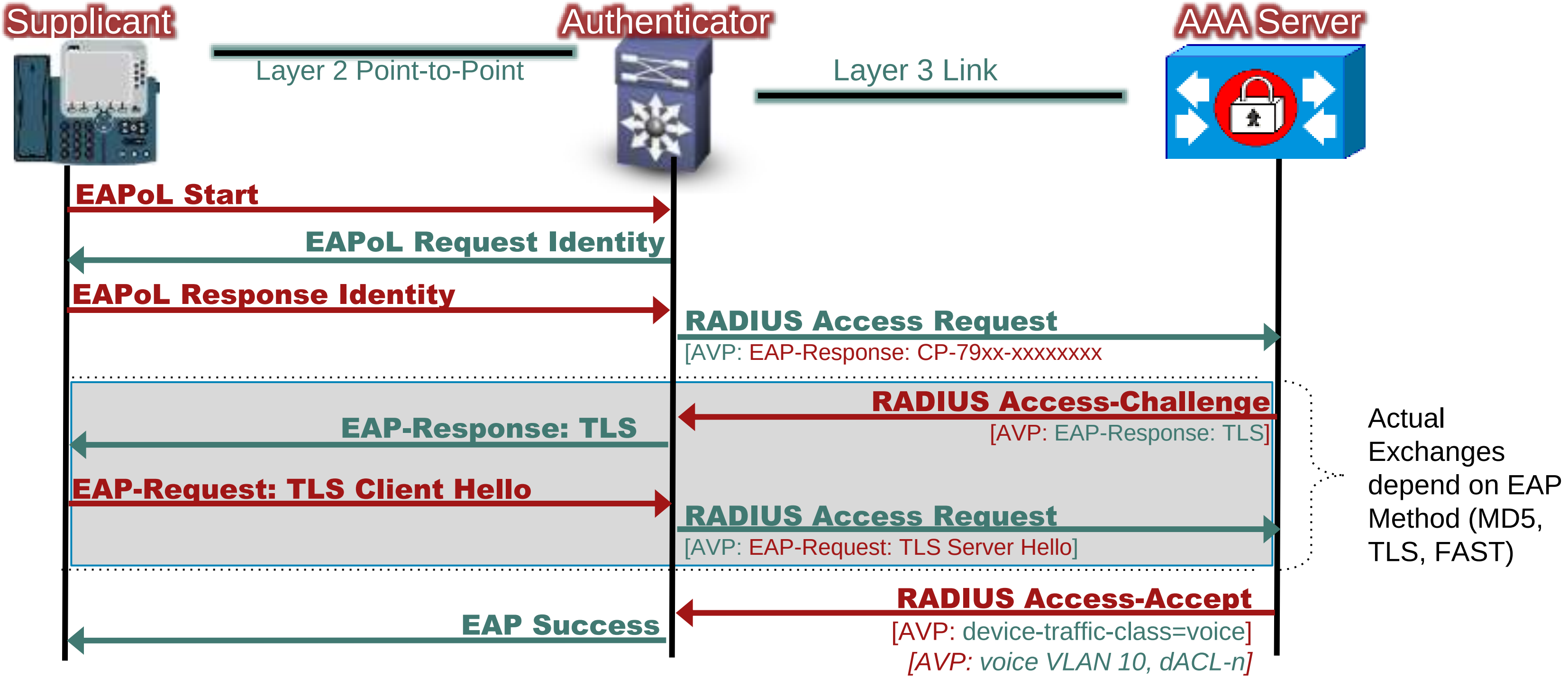
```
interface fastEthernet 3/48
  authentication host-mode multi-domain
```

MDA with MAC Authentication Bypass (MAB)



Benefits	Deployment Considerations
No client, no credential needed -> Works for all Cisco phone models	Dependency on AAA server
Enables visibility, access control	Must create & maintain phone MAC database
Compatible with 802.1X features	Default 802.1X timeout = 90 seconds latency (mitigated by Low Impact Mode)

MDA with 802.1X



Supplicant

Authenticator

AAA Server

Layer 2 Point-to-Point

Layer 3 Link

EAPoL Start

EAPoL Request Identity

EAPoL Response Identity

RADIUS Access Request
[AVP: EAP-Response: CP-79xx-xxxxxxxx

RADIUS Access-Challenge
[AVP: EAP-Response: TLS]

EAP-Response: TLS

EAP-Request: TLS Client Hello

RADIUS Access Request
[AVP: EAP-Request: TLS Server Hello]

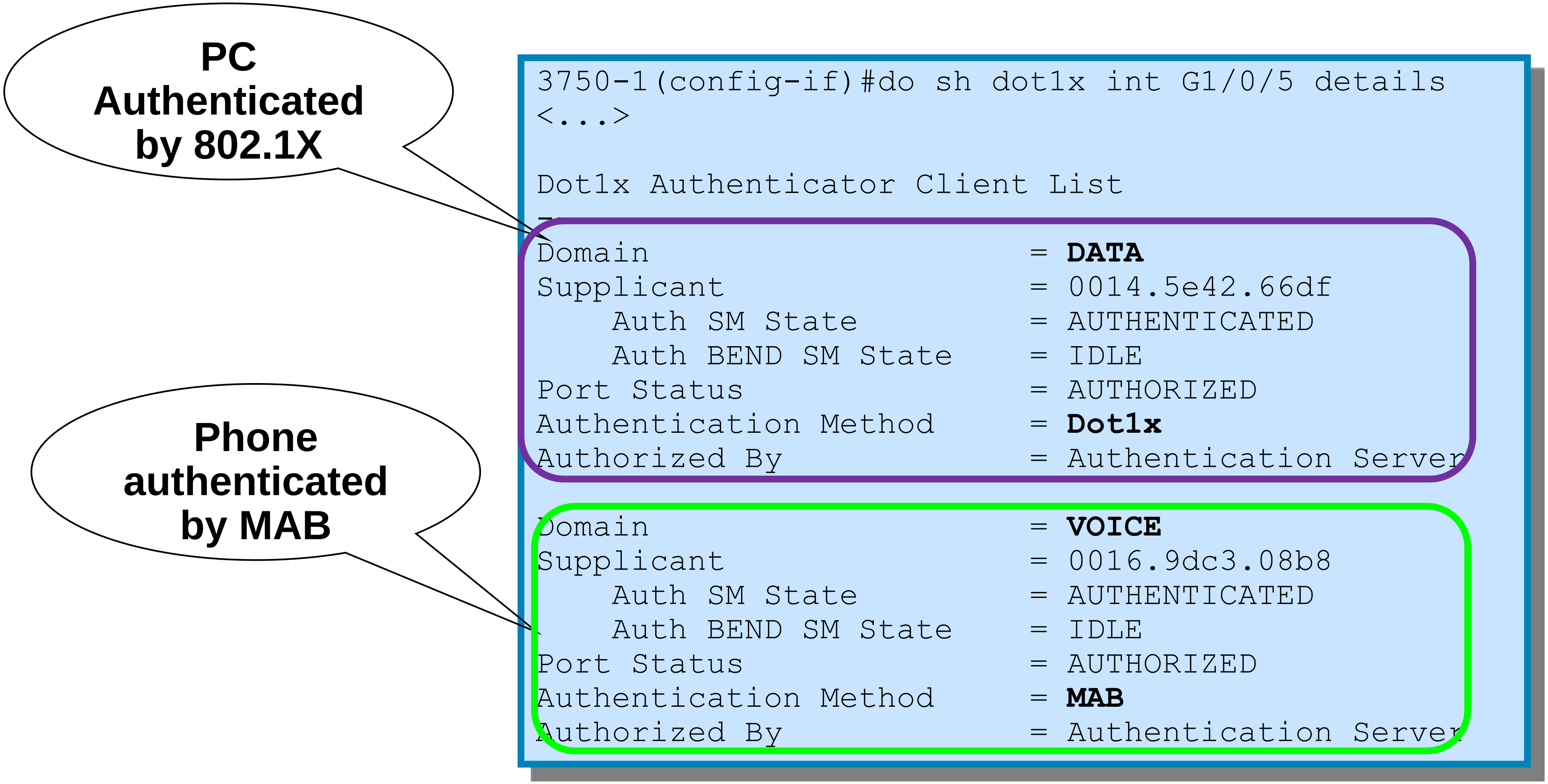
Actual Exchanges depend on EAP Method (MD5, TLS, FAST)

RADIUS Access-Accept
[AVP: device-traffic-class=voice]
[AVP: voice VLAN 10, dACL-n]

EAP Success

Benefits	Deployment Considerations
Strong Authentication with Minimal Delay	Choice of EAP Method impacts deployability
Can be deployed without touching the phone or creating a database.	Requires: 7970G, 79x1, 79x2, 79x5 *with X.509 cert support* & firmware 8.5(2)
Compatible with 802.1X features	AAA server dependency

MDA in Action



```
3750-1(config-if)#do sh dot1x int G1/0/5 details
<...>

Dot1x Authenticator Client List
-
Domain                          = DATA
Supplicant                      = 0014.5e42.66df
    Auth SM State               = AUTHENTICATED
    Auth BEND SM State          = IDLE
Port Status                     = AUTHORIZED
Authentication Method           = Dot1x
Authorized By                   = Authentication Server

Domain                          = VOICE
Supplicant                      = 0016.9dc3.08b8
    Auth SM State               = AUTHENTICATED
    Auth BEND SM State          = IDLE
Port Status                     = AUTHORIZED
Authentication Method           = MAB
Authorized By                   = Authentication Server
```

- Either 802.1X or MAB for phone
- Any combination of 802.1X, MAB, Guest-VLAN, Auth-Fail-VLAN, IAB for PC

Summary: Multiple Hosts per Port

Host Mode	Enforcement	Deployment Considerations
Single	Single mac address per port	• Second mac address triggers a security violation • VMs on the host must share the same mac address. • CDP Bypass is the only IPT solution.
Multi-Domain Auth (MDA)	One Voice Device + One Data Device per port	• Same as single host mode except phone authenticates • Supports third party phones
Multi-Auth	Superset of MDA with multiple Data Devices per port	• Authenticates every mac address in the data domain. • VMs on the host may use different mac addresses. • One VLAN (default port VLAN) for all devices on the port
Multi-Host	One authenticated device allows any number of subsequent mac addresses.	• Not recommended • VMs on the host may use different mac addresses. • CDP Bypass is the only IPT solution.

Low Impact: Network Access Table

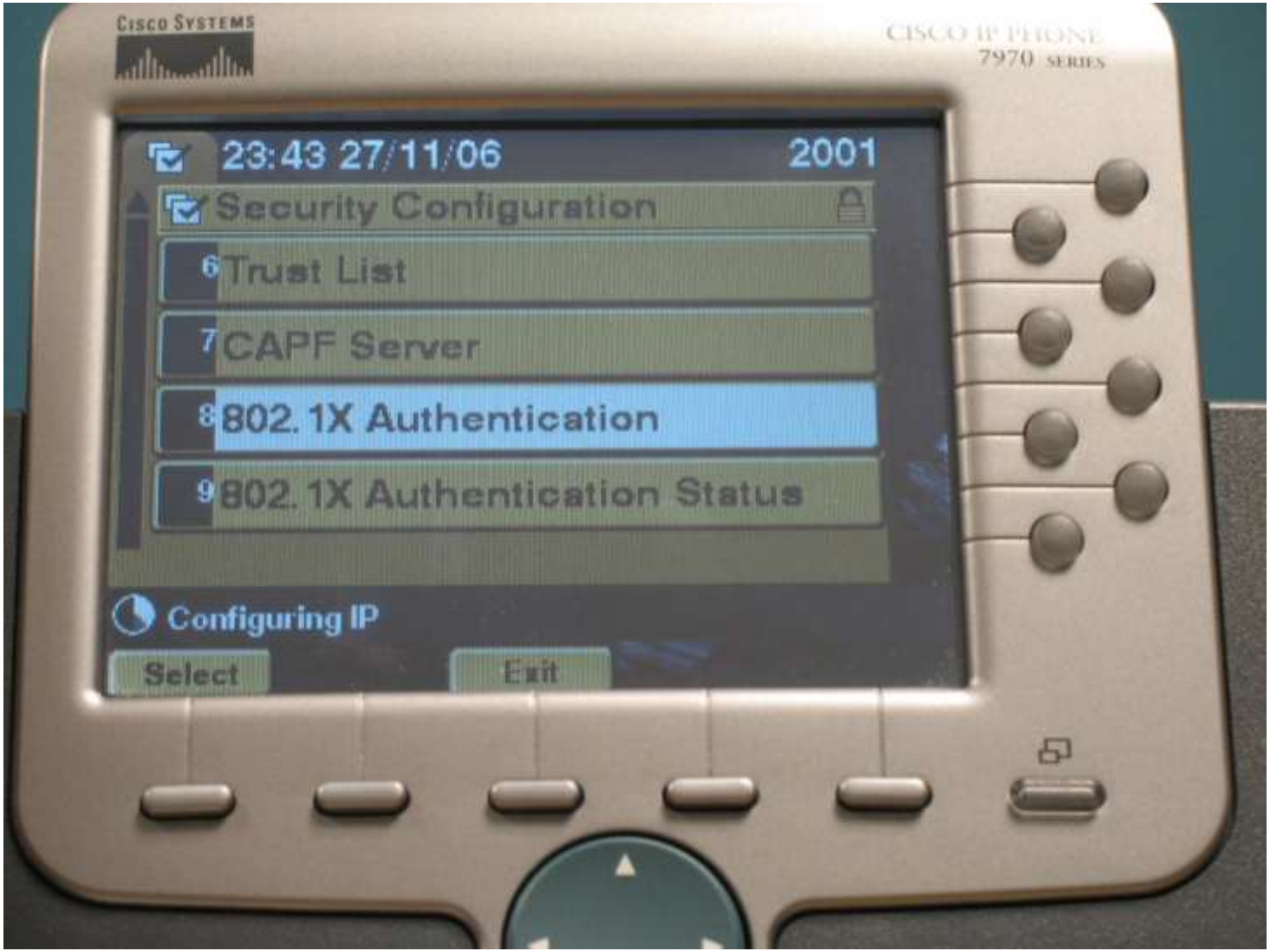
Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	Limited Access	Pre-Auth ACL
Employees	802.1X Success	Enterprise Access	Permit-Any dACL
Corporate Asset	MAB Success	Enterprise Access	Permit-Any dACL
Phones	802.1X or MAB Success	Voice Access	MDA with Voice VSA + Permit-Any dACL
Employees	802.1X Fail -> MAB or Web-Auth Success	Enterprise Access	Permit-Any dACL
Sponsored Guest	802.1X Fail/Timeout -> MAB Fail -> Web-Auth Success	Limited + Internet Access	Permit-Internet dACL
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail -> Web-Auth Fail	Limited Access	Pre-Auth ACL
All	None (AAA server down)	Limited Access	Pre-Auth ACL

Cisco IP-Phone 802.1X

Phone Booting

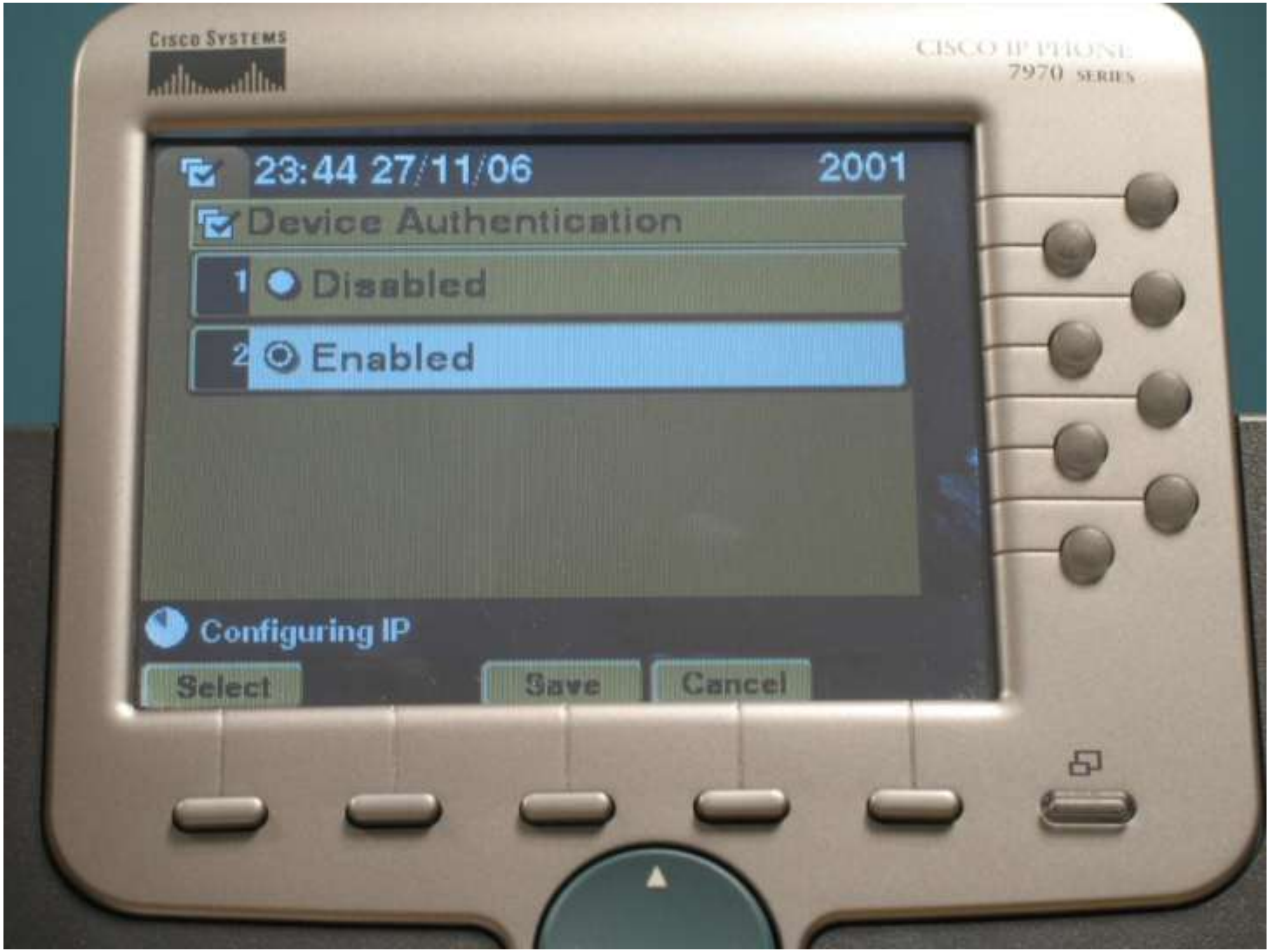
Cisco IP-Phone 802.1X

Access Via the Security Settings Menu



Cisco IP-Phone 802.1X

802.1X Off by Default



23:44 27/11/06 2001

Device Authentication

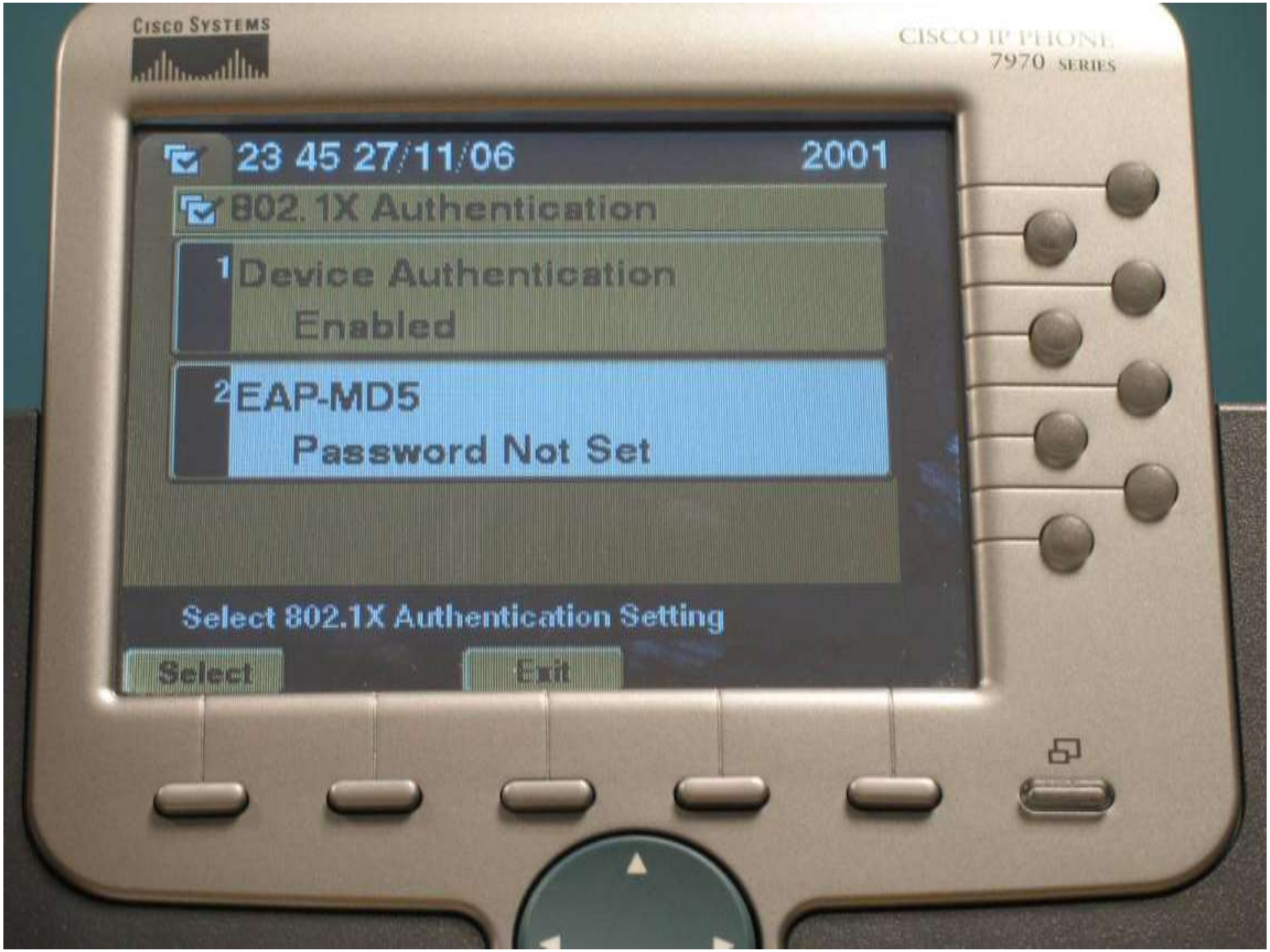
1 ○ Disabled

2 ◉ Enabled

Configuring IP

Cisco IP-Phone 802.1X

Set EAP-MD5 Password



23 45 27/11/06 2001

802. 1X Authentication

1 Device Authentication
Enabled

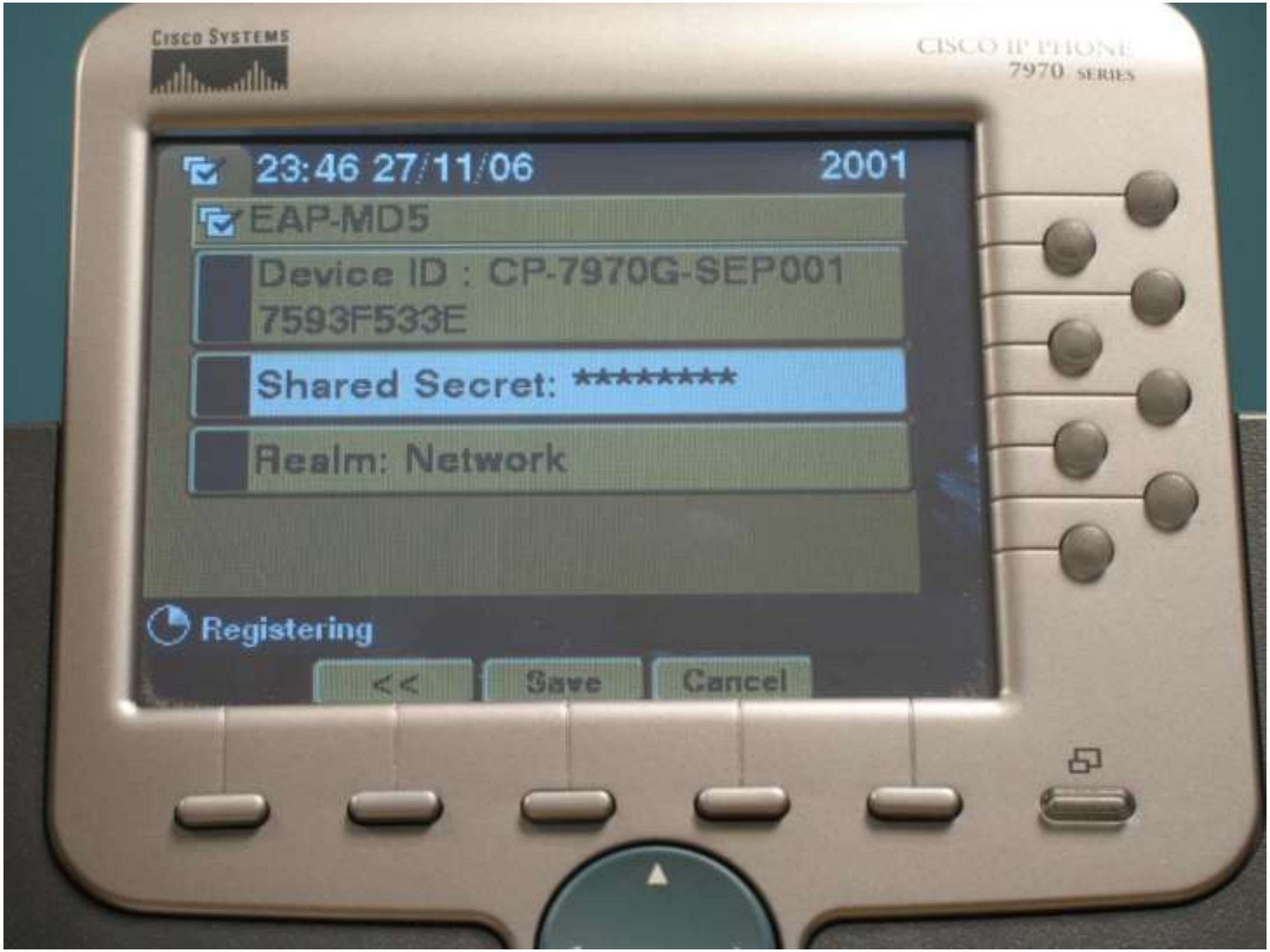
2 EAP-MD5
Password Not Set

Select 802.1X Authentication Setting

Select Exit

Cisco IP-Phone 802.1X

Device ID must = ACS User ID



23:46 27/11/06 2001

EAP-MD5

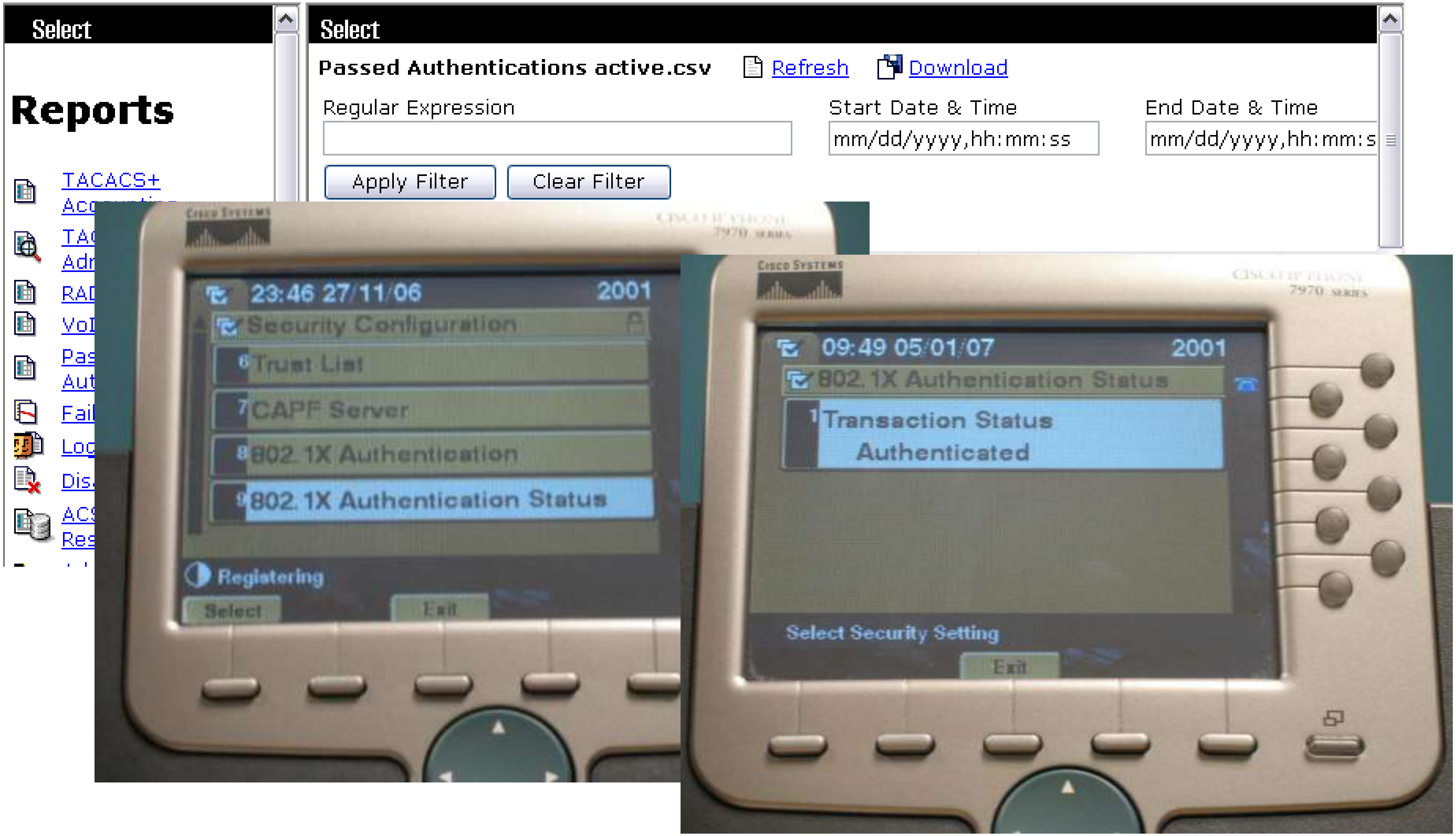
Device ID : CP-7970G-SEP001 7593F533E

Shared Secret: *********

Realm: Network

Registering

Checking Status



Reports and Activity

Select

Reports

TACACS+ Accounting

TA
Adr

RAD

VoI

Pas
Aut

Fail

Log

Dis

ACS
Res

Select

Passed Authentications active.csv Refresh Download

Regular Expression

Start Date & Time: mm/dd/yyyy,hh:mm:ss

End Date & Time: mm/dd/yyyy,hh:mm:s

23:46 27/11/06 2001

Security Configuration

6 Trust List

7 CAPF Server

8 802.1X Authentication

9 802.1X Authentication Status

Registering

09:49 05/01/07 2001

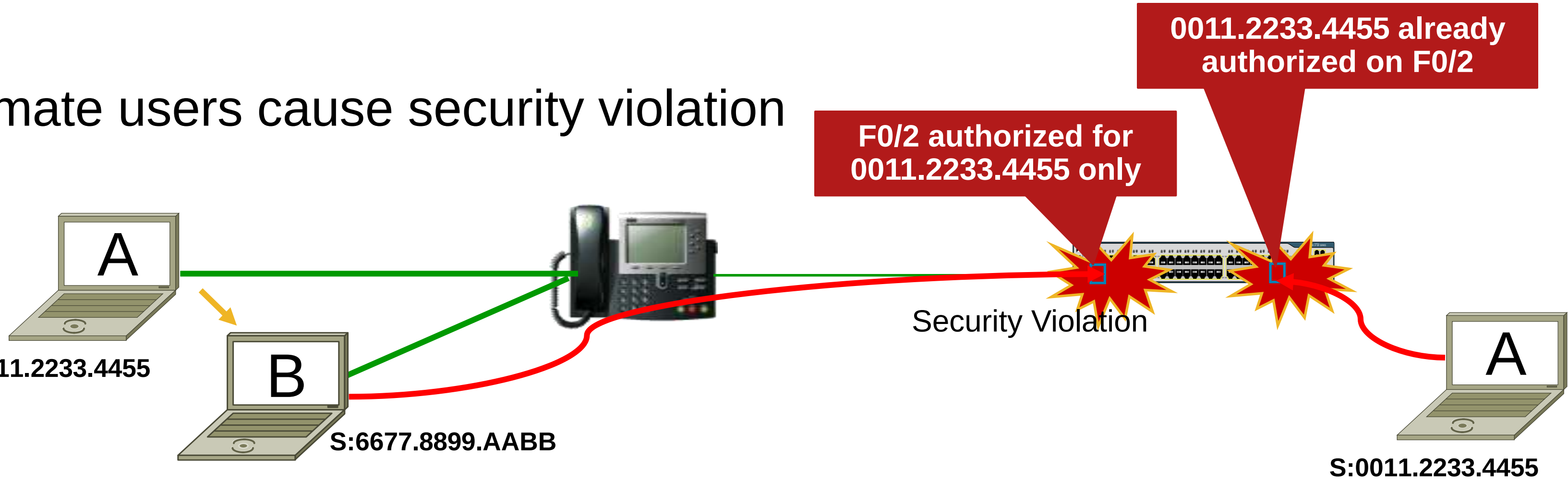
802.1X Authentication Status

1 Transaction Status
Authenticated

Select Security Setting

IPT & 802.1X: The Link-State Problem

1) Legitimate users cause security violation

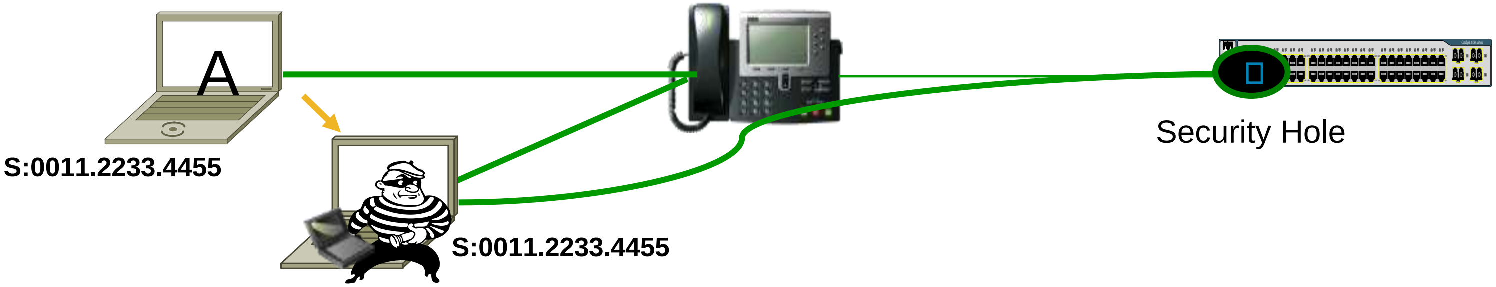


0011.2233.4455 already authorized on F0/2

F0/2 authorized for 0011.2233.4455 only

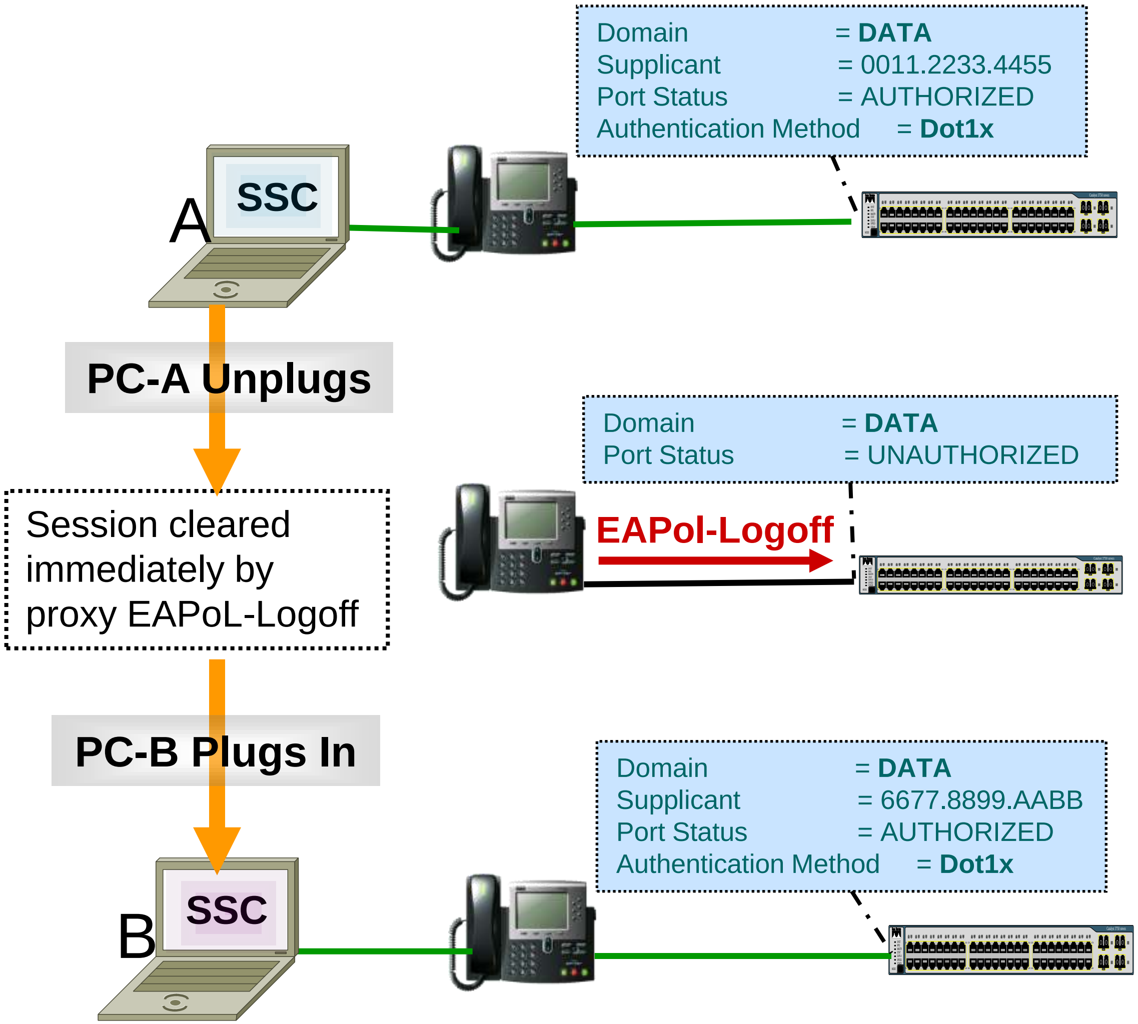
Security Violation

2) Hackers can spoof MAC to gain access without authenticating



Security Hole

Partial Solution: Proxy EAPoL-Logoff



Domain = **DATA**
Supplicant = 0011.2233.4455
Port Status = AUTHORIZED
Authentication Method = **Dot1x**

PC-A Unplugs

Session cleared
immediately by
proxy EAPoL-Logoff

Domain = **DATA**
Port Status = UNAUTHORIZED

PC-B Plugs In

Domain = **DATA**
Supplicant = 6677.8899.AABB
Port Status = AUTHORIZED
Authentication Method = **Dot1x**

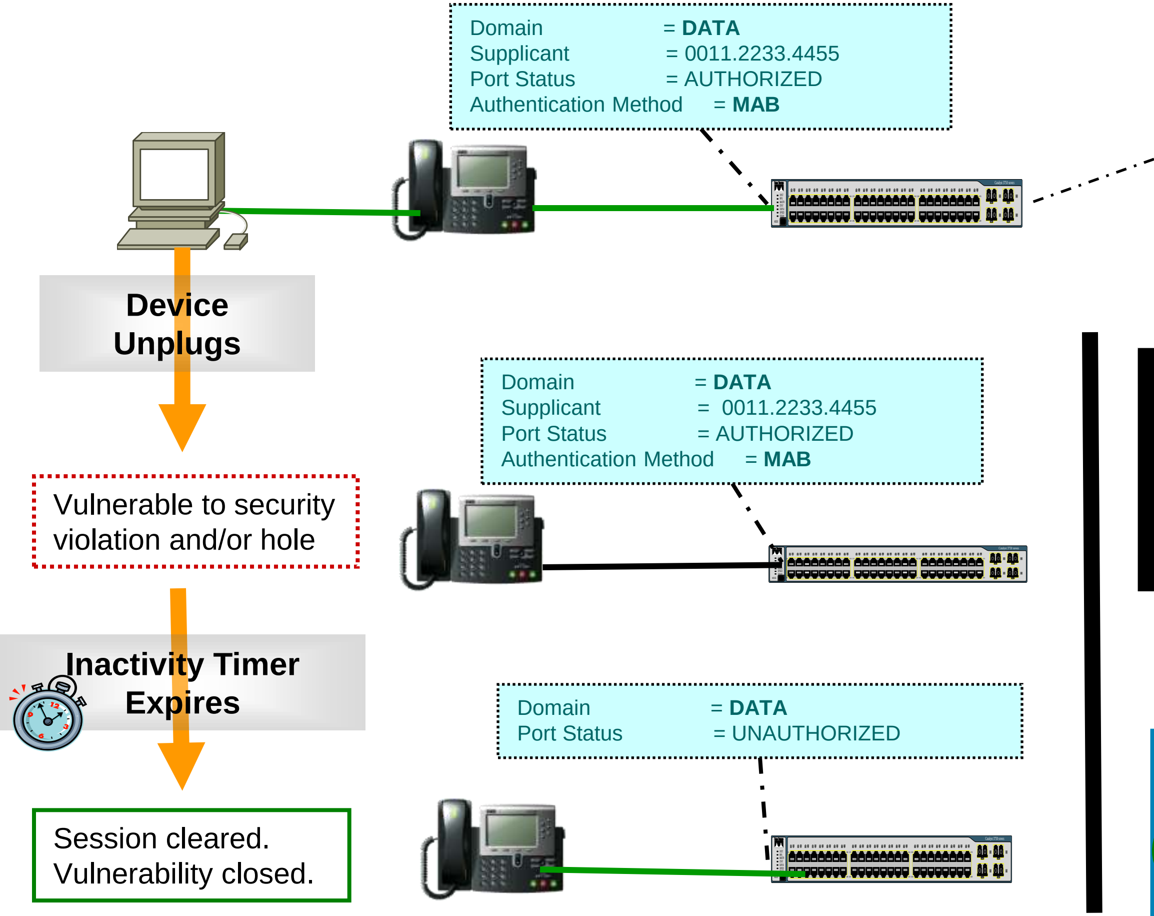
Caveats:

- Only for 802.1X devices behind phone

Requires:

Logoff-capable Phones

Partial Solution: Inactivity Timeout Options



Device Unplugs
Vulnerable to security violation and/or hole
Inactivity Timer Expires
Session cleared. Vulnerability closed.

```
Domain                  = DATA
Supplicant              = 0011.2233.4455
Port Status             = AUTHORIZED
Authentication Method     = MAB
```

```
Domain                  = DATA
Supplicant              =  0011.2233.4455
Port Status             = AUTHORIZED
Authentication Method     = MAB
```

```
Domain                  = DATA
Port Status             = UNAUTHORIZED
```

```
interface GigE 1/0/5
 switchport mode access
 switchport access vlan 2
 switchport voice vlan 12
 authentication host-mode multi-domain
 authentication port-control auto
 authentication timer inactivity [300 | server]
 mab
```

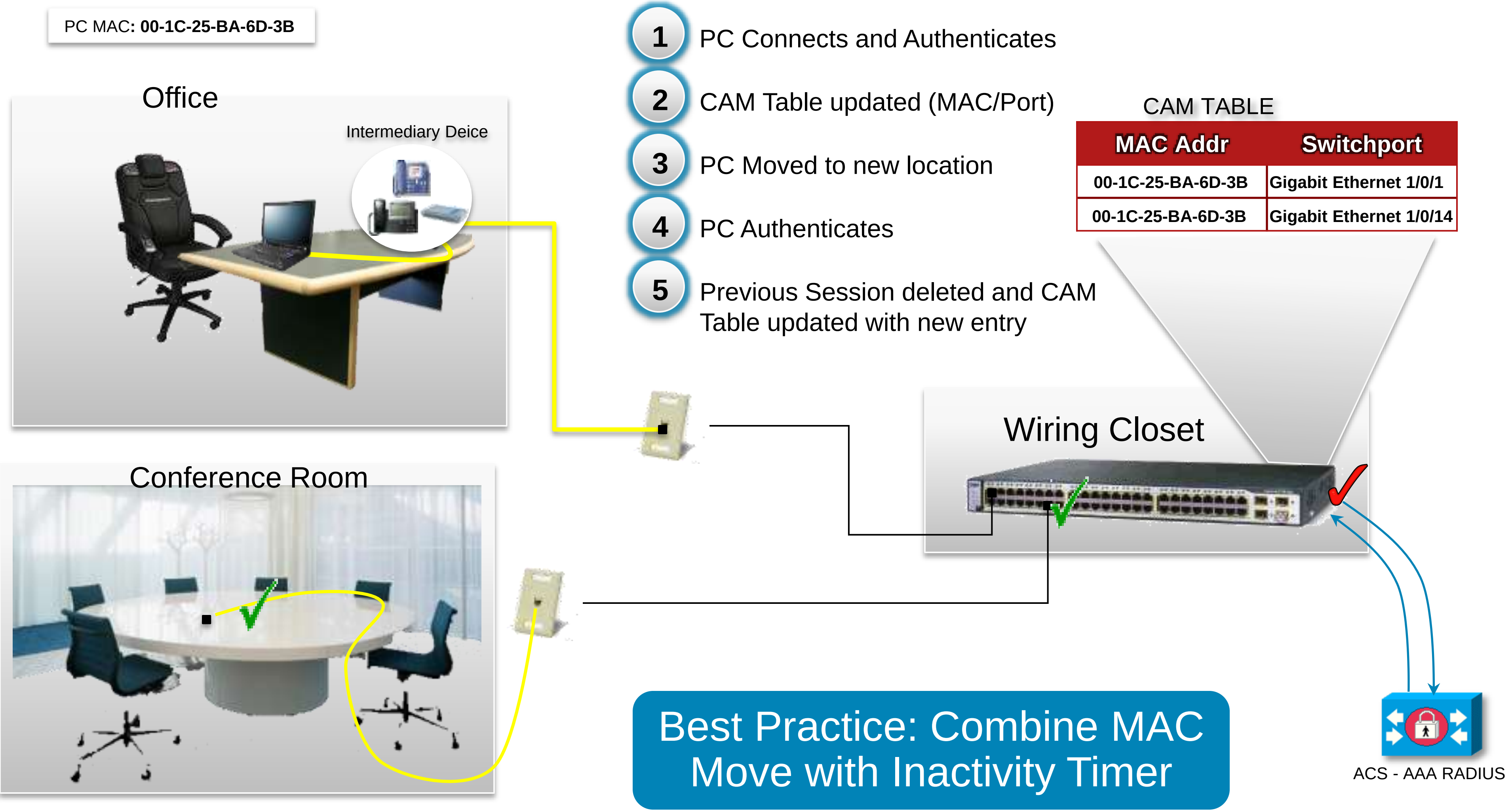
Caveats:

- ⚠ Quiet devices may have to re-auth; network access denied until re-auth completes.
- ⚠ Still a window of vulnerability.

New

```
3K: 12.2(50)SE*
4K: 12.2(50)SG
6K: 12.2(33)SXI
```

Partial Solution: MAC Move



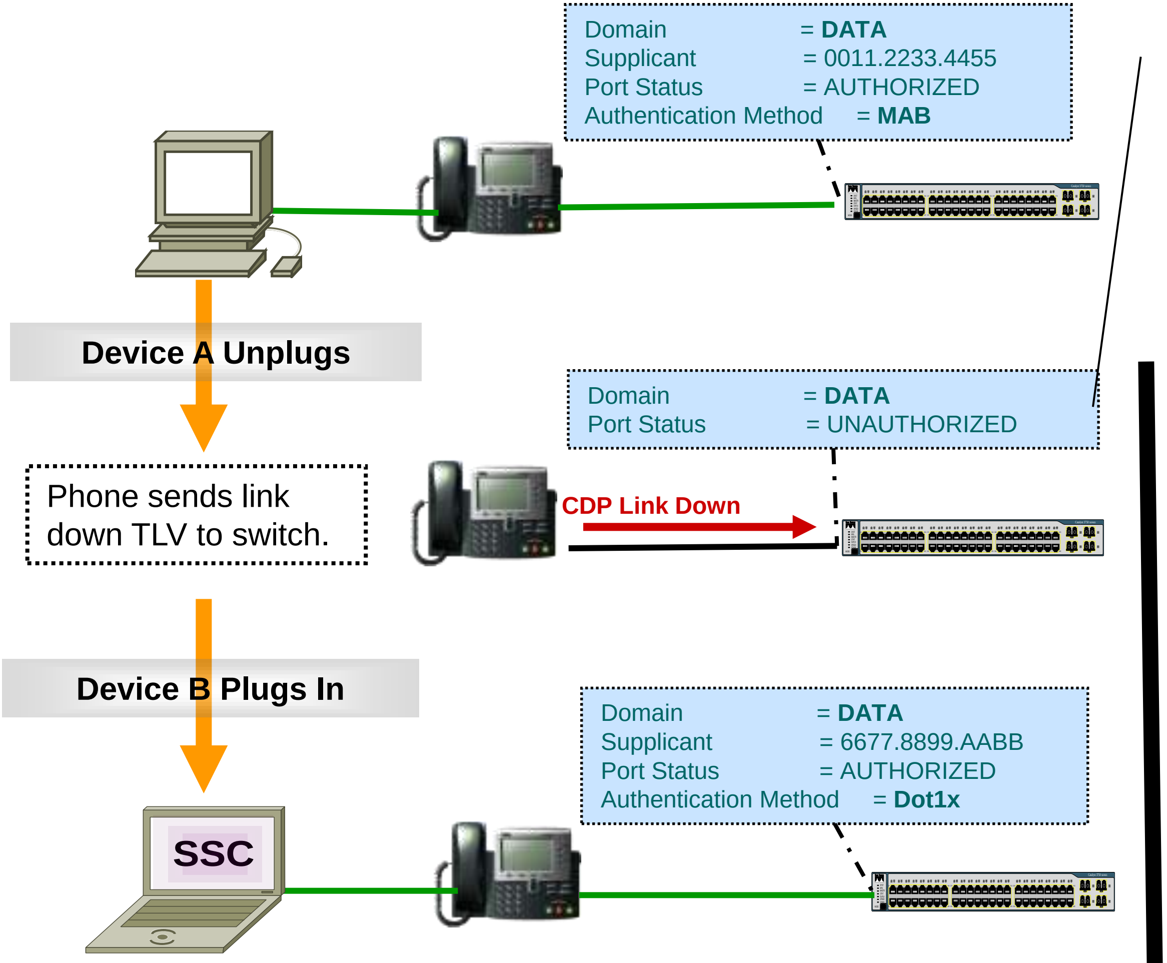
1. PC Connects and Authenticates
2. CAM Table updated (MAC/Port)
3. PC Moved to new location
4. PC Authenticates
5. Previous Session deleted and CAM Table updated with new entry

CAM TABLE

MAC Addr	Switchport
00-1C-25-BA-6D-3B	Gigabit Ethernet 1/0/1
00-1C-25-BA-6D-3B	Gigabit Ethernet 1/0/14

Best Practice: Combine MAC Move with Inactivity Timer

Full Solution: CDP 2nd Port Notification



Domain = **DATA**
Supplicant = 0011.2233.4455
Port Status = AUTHORIZED
Authentication Method = **MAB**

Domain = **DATA**
Port Status = UNAUTHORIZED

Domain = **DATA**
Supplicant = 6677.8899.AABB
Port Status = AUTHORIZED
Authentication Method = **Dot1x**

```
id-4503#sho cdp neigh  g2/1 detail
-------------------------
Device ID: SEP0015C696E22C
Entry address(es):
IP address: 10.1.200.10
Platform: Cisco IP Phone 7971,  Capabilities: Host
Phone Two-port Mac Relay
Interface: GigabitEthernet2/1,
Port ID (outgoing port):  Port 1 Holdtime : 168 sec
Second Port Status: Down
```

- ✓ **Link status msg addresses root cause**
- ✓ **Session cleared immediately.**
- ✓ **Works for MAB, 802.1X, and Web-Auth.**
- ✓ **Nothing to configure**

```
IP Phone: 8.4(1)
3K: 12.2(50)SE
4K: 12.2(50)SG
6K: 12.2(33)SXI
```

DEMO Time

CDP 2nd Port Notifications

Phase 3: High Security Access Control

Phase 3: ACME Gets Acquired by Widget, Inc.

New Security Policy & Network Requirements:

VLAN Segmentation

- Engineers on the ENG VLAN
- Machines on MACHINE VLAN
- Employees/managed assets on DATA VLAN.
- Unauthenticated devices on RESTRICTED VLAN only.

Branch Survivability

- “fail open” when AAA server is unreachable.

Widget’s Goals Can Be Met With High Security Mode

How this will happen

Policy Change	Solution Change
VLAN Segmentation	Dynamic Identity-based VLAN assignment
No unauthenticated traffic on DATA VLAN	Open mode -> Closed Mode
Unauthenticated devices on RESTRICTED VLAN only	Local authorization (AuthFail VLAN, Guest VLAN)
Branch Survivability	Critical Auth VLAN

High Security: Network Access Table

Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	None	
Employees	802.1X Success	Enterprise Access	
Corporate Asset	MAB Success	Enterprise Access	
Phones	802.1X or MAB Success	Voice Access	
Engineers	802.1X Success	Engineer Access	
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail	Limited Access	
All	None (AAA server down)	Enterprise Access	

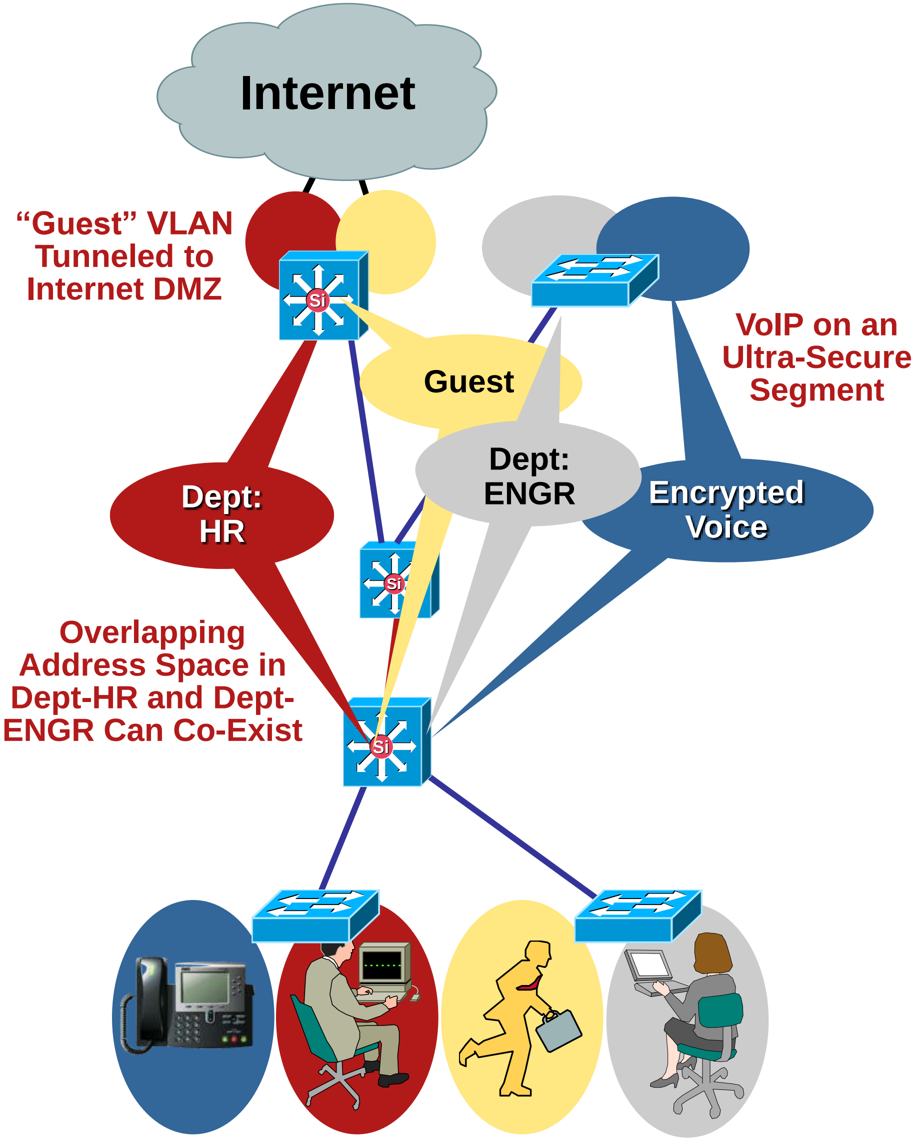
Dynamic Authorization:

VLAN Assignment

Identity-Based	• Assigned VLAN is based on identity at time of authentication • Identity can be individual or group
VLAN Name	• VLANs assigned by name (not number); allows for more flexible VLAN management • Assigned VLAN must match switch configuration; mismatch results in authentication failure.
Standards-Based	• Usage for VLANs is specified in the IEEE 802.1X standard • RFC 2868 defines tunnel attributes that AAA server uses to send to VLAN name to switch
Tunnel Attributes	• [64] Tunnel-type—“VLAN” (13) • [65] Tunnel-medium-type—“802” (6) • [81] Tunnel-private-group-ID—<VLAN name>

Segmenting Users, Devices and Networks

How to Extend IBNS Policy into the Network…



Internet
"Guest" VLAN Tunneled to Internet DMZ
Guest
VoIP on an Ultra-Secure Segment
Dept: ENGR
Dept: HR
Encrypted Voice
Si
Si
Si
Overlapping Address Space in Dept-HR and Dept-ENGR Can Co-Exist

Use the Network to Provide Isolation and Simplified Policy Enforcement

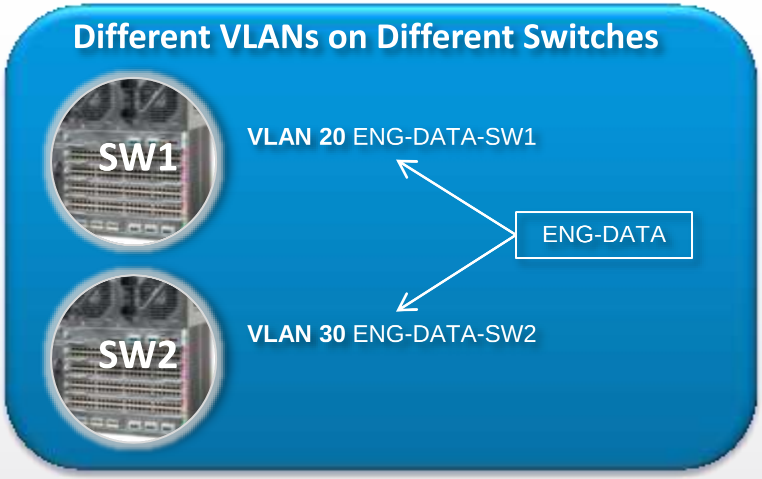
- GRE tunnels and policy routing
- VRF-Lite end-to-end—(virtual route forwarding)
- VRF-Lite at the distribution with MPLS L3 VPNs at the core
- MPLS L3 VPNs end-to-end

802.1X User Distribution

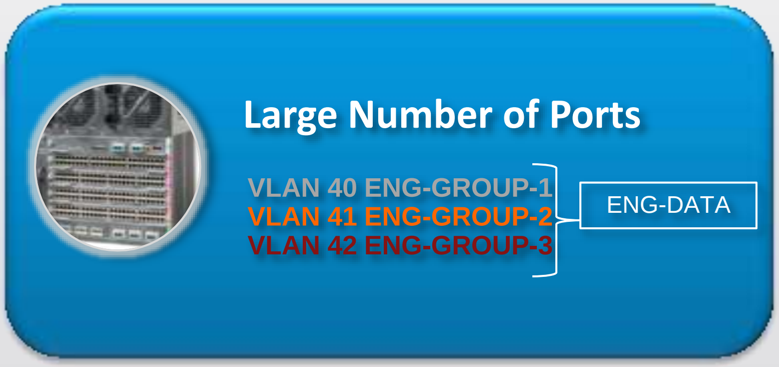
Enhances Dynamic VLAN Assignment

Addresses Two Use Cases:

- Allow ***mapping*** the Radius provided VLAN name to different VLANs on different switches *(no need to re-configure Radius provided VLAN name).*
- Allow ***distribution*** of Radius provided VLAN to multiple different VLANs locally available on the same logical switch (load balancing) *(reduces broadcast domain)*

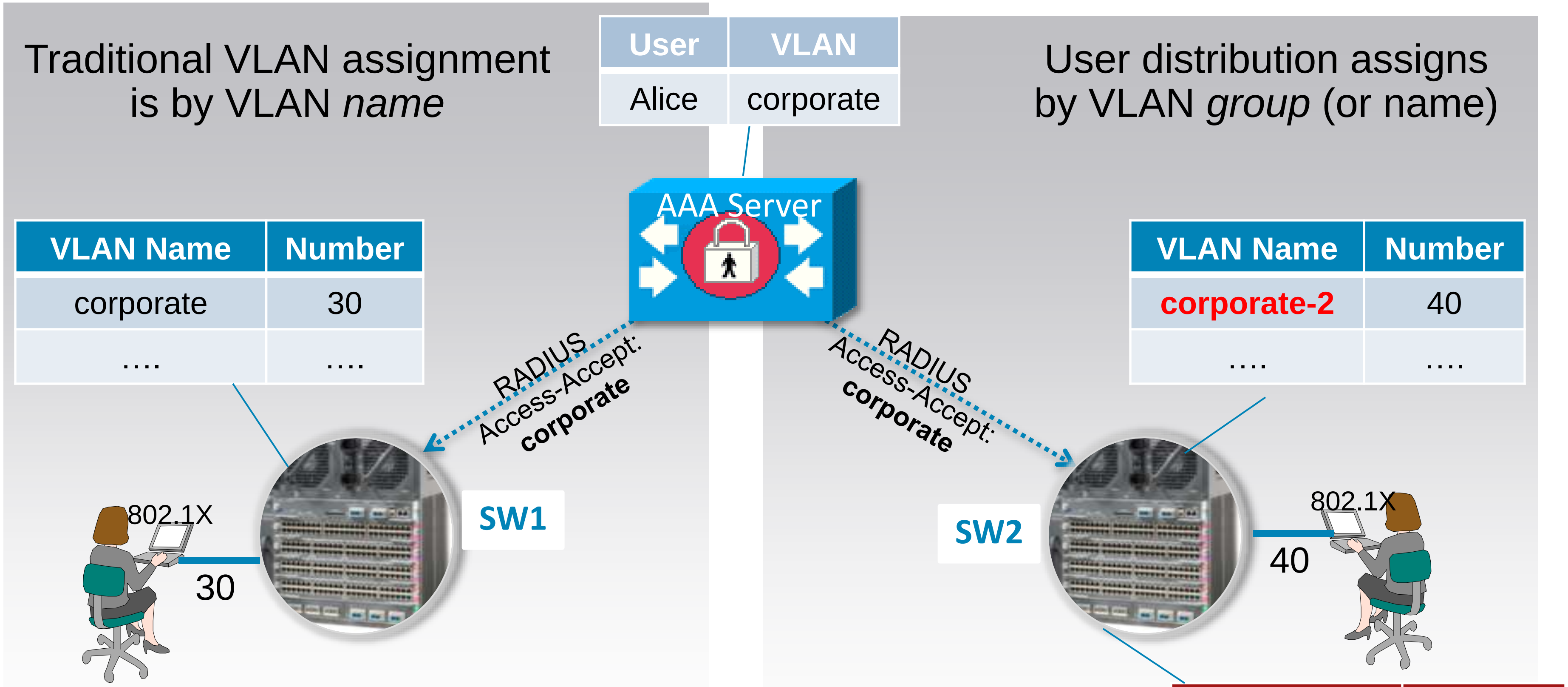


Different VLANs on Different Switches



Large Number of Ports

User Distribution “Mapping” Can Simplify Migration to Dynamic VLANs



Traditional VLAN assignment is by VLAN *name*

User distribution assigns by VLAN *group* (or name)

User	VLAN
Alice	corporate

VLAN Name	Number
corporate	30
….	….

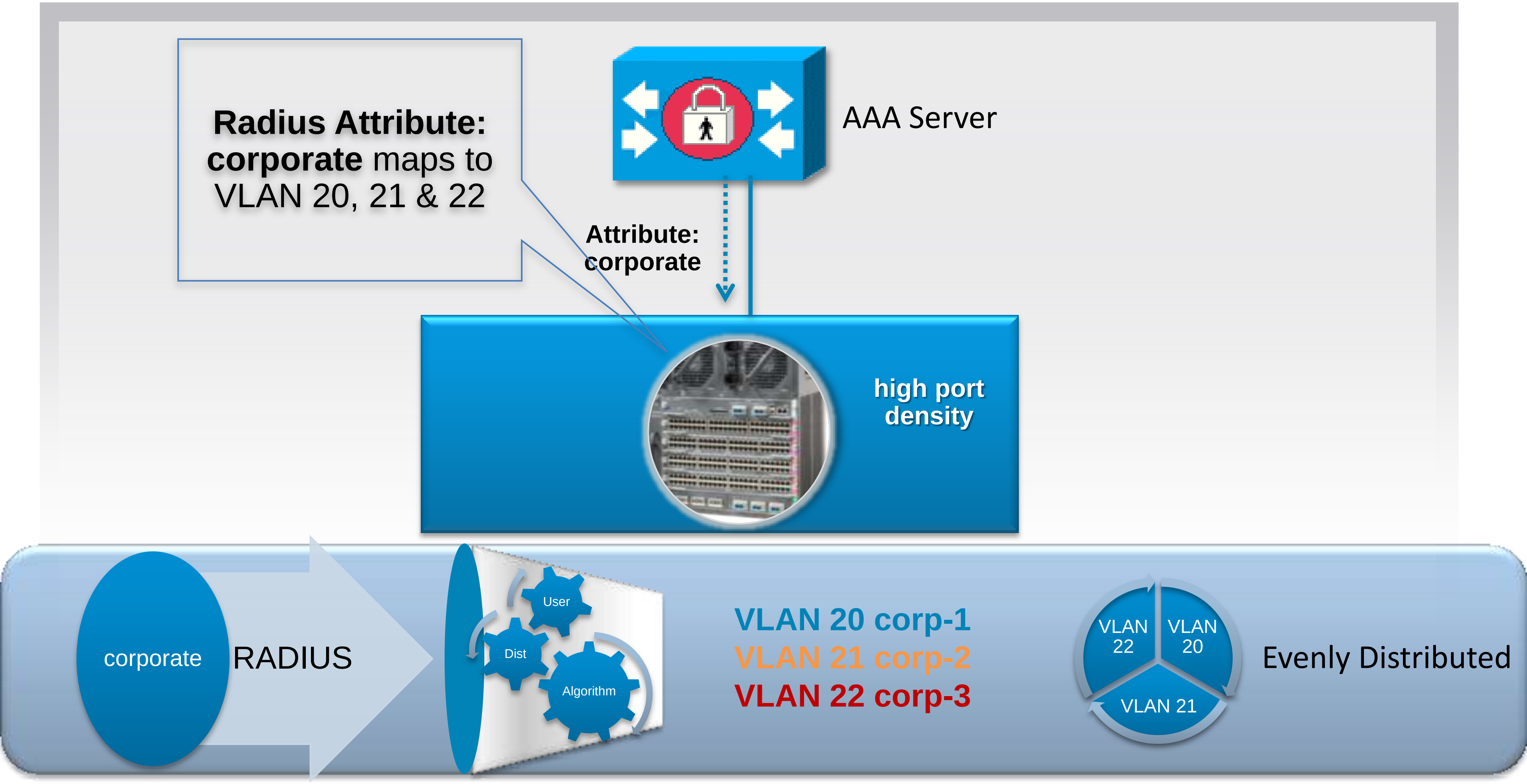
VLAN Name	Number
corporate-2	40
….	….

VLAN Group	Number
corporate	40
….	….

AAA Server
RADIUS Access-Accept: corporate
RADIUS Access-Accept: corporate
SW1
SW2
802.1X
30
802.1X
40

- ✓ **Allows flexible adoption in existing environments**
- ✓ **No need to reconfigure existing VLANs**
- ✓ **Simplifies Policy in AAA Server**

User Distribution: “Distribution”



Allows highly scalable 802.1X-based VLAN assignment in a large scale campus LAN deployment

Configuring VLAN groups

```
Switch(config)# vlan group <groupname> vlan-list <list of vlans>
```

<groupname>: Name for the VLAN group starting with an alphabet

<list of VLANs>: Comma separated VLANs or a range of VLANs or a single VLAN

```
Switch(config)#vlan group corporate vlan-list 4
Switch(config)#vlan group corporate vlan-list 40-50
Switch(config)#vlan group corporate vlan-list 12,52,75
```

High Security: Network Access Table

Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	None	Closed Mode
Employees	802.1X Success	Enterprise Access	Default DATA VLAN
Corporate Asset	MAB Success	Enterprise Access	Default DATA VLAN
Phones	802.1X or MAB Success	Voice Access	Voice VLAN
Engineers	802.1X Success	Engineer Access	ENG VLAN
Machines	802.1X Success	Machine Access	
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail	Limited Access	
All	None (AAA server down)	Enterprise Access	

User and Machine/Device Authorization

802.1X & Dynamic VLANs

Deployment Considerations

VLAN Proliferation

- Every access switch must support every assignable VLAN
- In multi-layer deployments, all these VLANs must be trunked to distribution layer.
- Every new VLAN will require a new subnet on every access switch (routed access & multi-layer*)

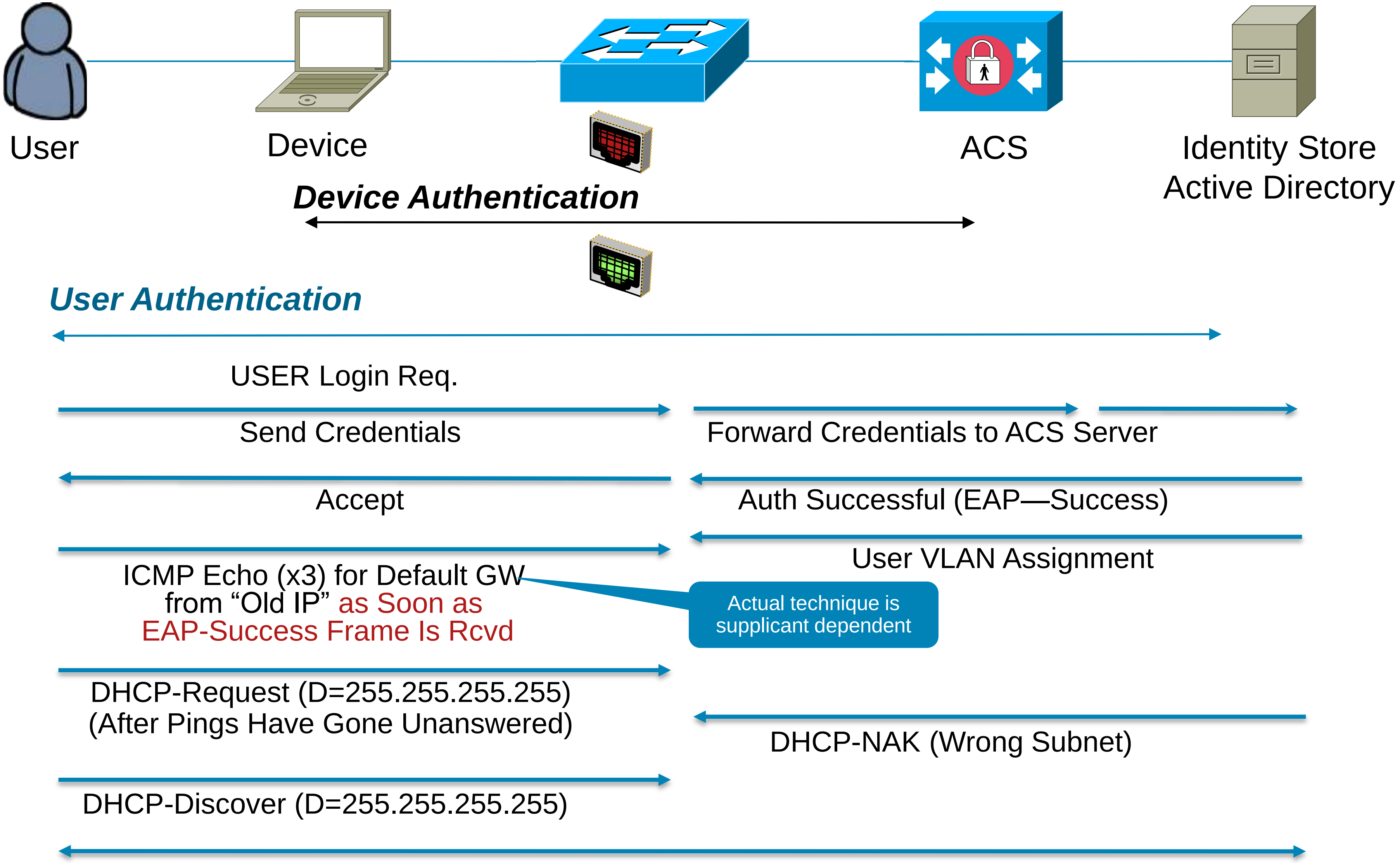
Address Changes

- Devices that change VLANs as a result of authentication MUST be capable of getting a new address on the new VLAN.
- Most supplicants CAN get a new address
- Most clientless devices CANNOT
- Even successful address changes can cause problems with end host functionality.

*VSS removes this requirement

Coping with VLAN Change

DHCP Renewal - Microsoft Windows Example



Device Authentication

User Authentication

USER Login Req.

Send Credentials

Forward Credentials to ACS Server

Accept

Auth Successful (EAP—Success)

User VLAN Assignment

ICMP Echo (x3) for Default GW
from “Old IP” as Soon as
EAP-Success Frame Is Rcvd

Actual technique is
supplicant dependent

DHCP-Request (D=255.255.255.255)
(After Pings Have Gone Unanswered)

DHCP-NAK (Wrong Subnet)

DHCP-Discover (D=255.255.255.255)

At This Point, DHCP Proceeds Normally

VLAN Changes Can Disrupt Desktop Operation

- In Legacy (pre-Vista) Microsoft environments, changing the VLAN can break user and/or machine GPOs.
- Windows XP cannot re-negotiate secure connection with AD if IP address changes during GPO download.

What's a GPO? And why should I care about breaking it?

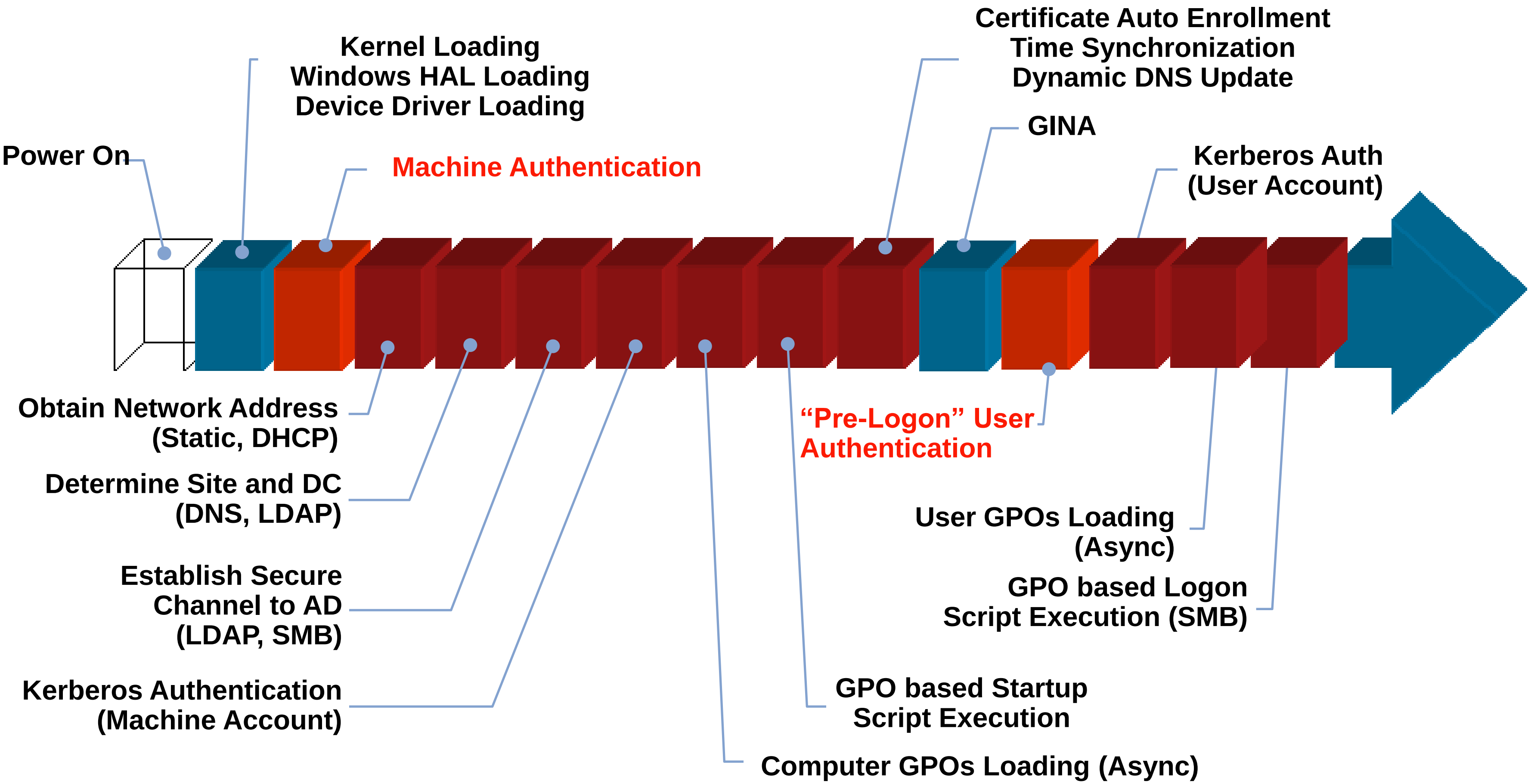
A Group Policy Object (GPO) is used to deliver and apply configurations or policy settings to a set of targeted users and computer within an Active Directory environment. Windows Admins use GPOs for system compliancy and security enforcement , e.g.:

Network Device mapping
Applying Logon / Logoff scripts to workstations
Batch mechanism to trigger applications
Security compliance enforcement such as password rule, etc.

Breaking GPOs is a RPE (Resume Producing Event)

“Ideal” Microsoft Boot Process

If Only It Were This Easy



Power On

Kernel Loading
Windows HAL Loading
Device Driver Loading

Machine Authentication

Obtain Network Address
(Static, DHCP)

Determine Site and DC
(DNS, LDAP)

Establish Secure
Channel to AD
(LDAP, SMB)

Kerberos Authentication
(Machine Account)

Computer GPOs Loading (Async)

GPO based Startup
Script Execution

Certificate Auto Enrollment
Time Synchronization
Dynamic DNS Update

GINA

“Pre-Logon” User
Authentication

Kerberos Auth
(User Account)

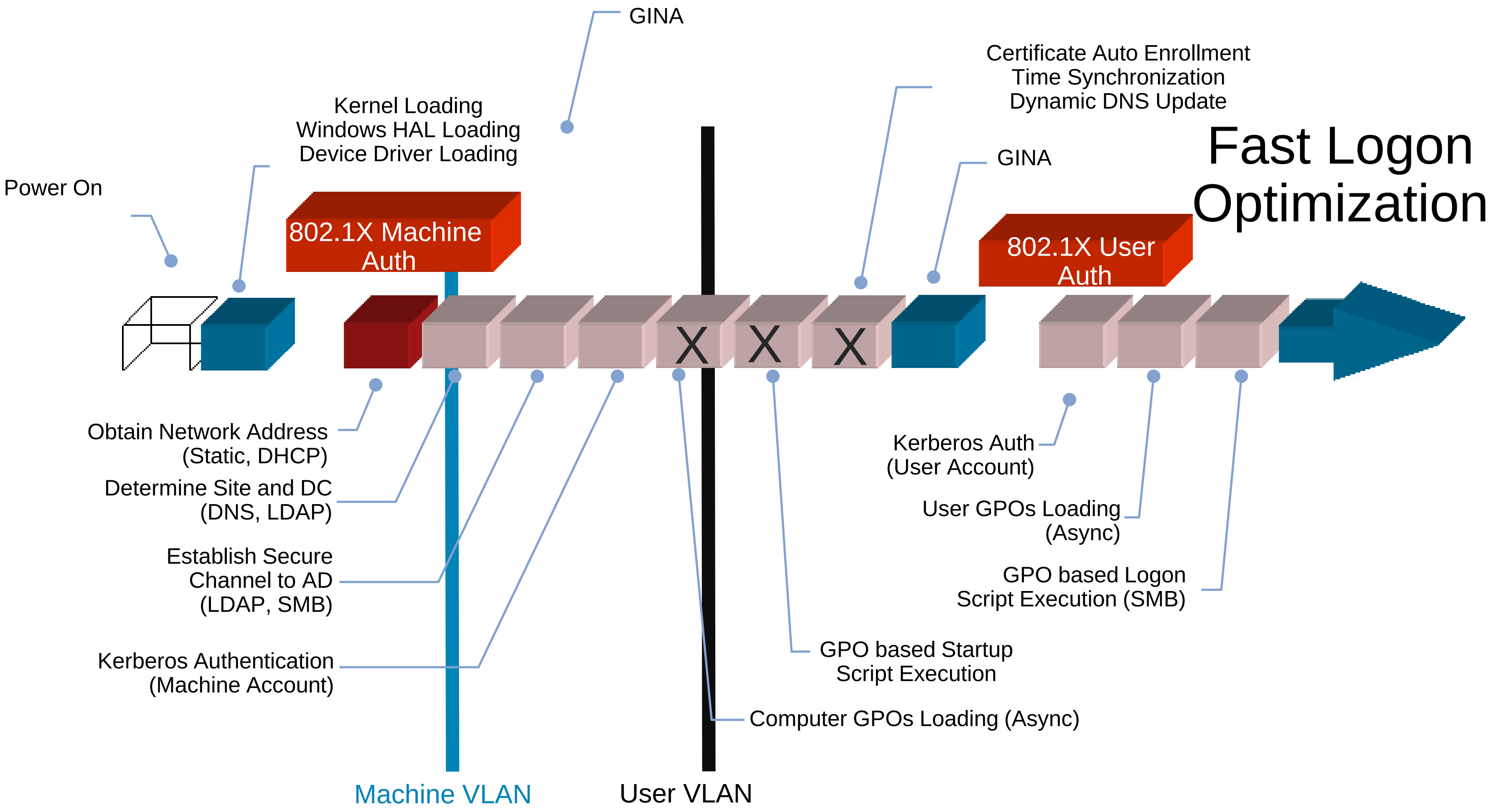
User GPOs Loading
(Async)

GPO based Logon
Script Execution (SMB)

🟥 Components that depend on network connectivity

Real Boot Process With Fast Logon

Machine GPOs will Break with XP

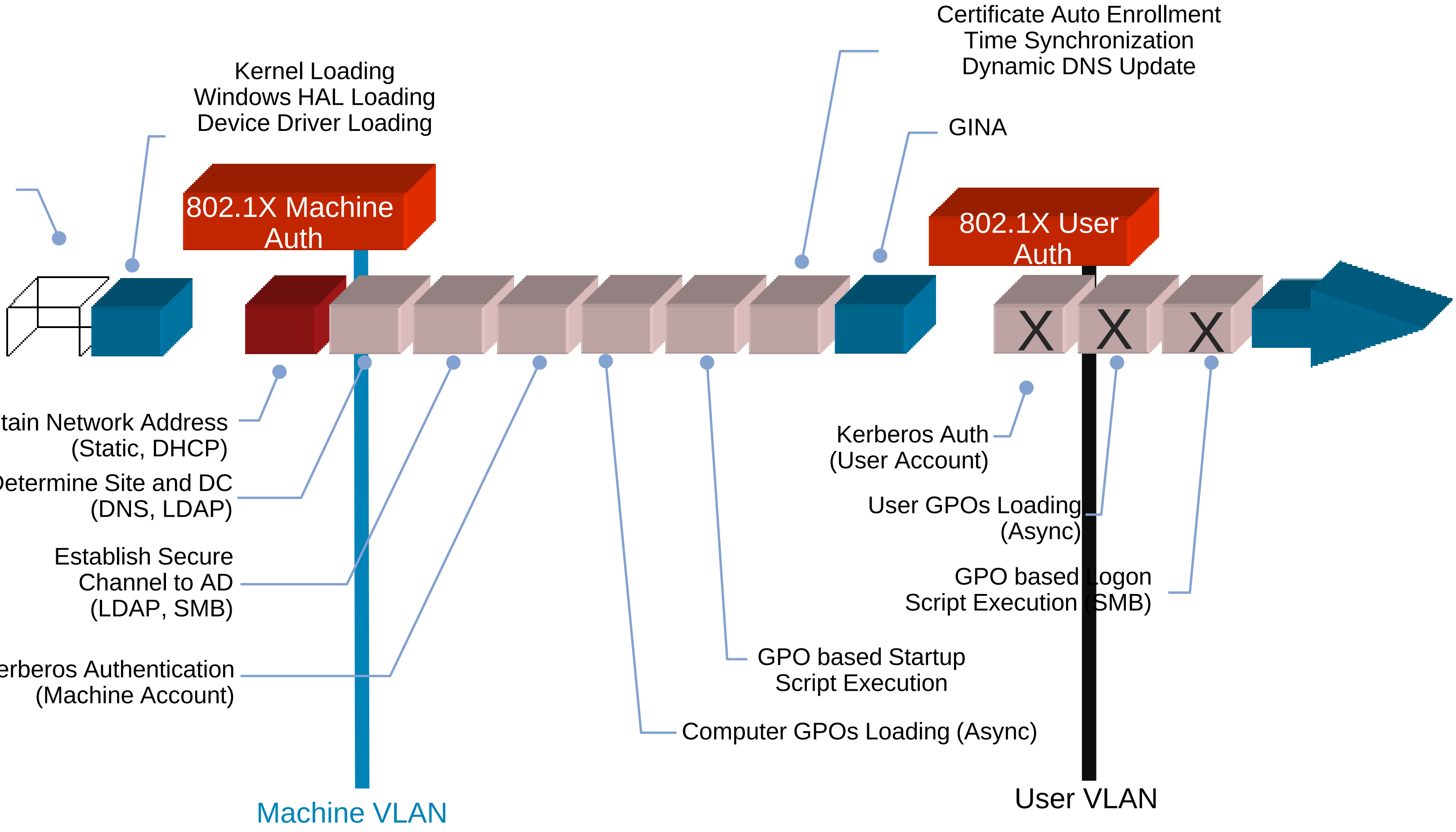

GINA
Certificate Auto Enrollment
Time Synchronization
Dynamic DNS Update
Kernel Loading
Windows HAL Loading
Device Driver Loading
GINA
Fast Logon Optimization
Power On
802.1X Machine Auth
802.1X User Auth
X
X
X
Obtain Network Address (Static, DHCP)
Determine Site and DC (DNS, LDAP)
Establish Secure Channel to AD (LDAP, SMB)
Kerberos Authentication (Machine Account)
Kerberos Auth (User Account)
User GPOs Loading (Async)
GPO based Logon Script Execution (SMB)
GPO based Startup Script Execution
Computer GPOs Loading (Async)
Machine VLAN
User VLAN

🟥 Start of 802.1X auth may vary among supplicants

▨ Components that are in race condition with 802.1X Auth

Real Boot Process With Race Conditions

User GPOs can Break with XP



Power On

Kernel Loading
Windows HAL Loading
Device Driver Loading

802.1X Machine Auth

Certificate Auto Enrollment
Time Synchronization
Dynamic DNS Update

GINA

802.1X User Auth

Obtain Network Address
(Static, DHCP)

Determine Site and DC
(DNS, LDAP)

Establish Secure
Channel to AD
(LDAP, SMB)

Kerberos Authentication
(Machine Account)

Kerberos Auth
(User Account)

User GPOs Loading
(Async)

GPO based Logon
Script Execution (SMB)

GPO based Startup
Script Execution

Computer GPOs Loading (Async)

Machine VLAN

User VLAN

🟥 Start of 802.1X auth may vary among supplicants

▨ Components that are in race condition with 802.1X Auth

Dynamic VLAN Assignment Best Practices

Vista SP2 or Windows 7:

- No Restrictions on VLAN assignment
- Vista and Win7 Can Renegotiate Secure Connection with AD when IP Address Changes

XP and earlier:

- Use Only Machine Authentication OR…
- Use the Same VLAN for User and Machine Authentication

Reconsider ACLs if you don’t need segmentation.

High Security: Network Access Table

Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	None	Closed Mode
Employees	802.1X Success	Enterprise Access	Default DATA VLAN
Corporate Asset	MAB Success	Enterprise Access	Default DATA VLAN
Phones	802.1X or MAB Success	Voice Access	Voice VLAN
Engineers	802.1X Success	Engineer Access	ENG VLAN
Machines	802.1X Success	Machine Access	MACHINE VLAN
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail	Limited Access	
All	None (AAA server down)	Enterprise Access	

DEMO Time

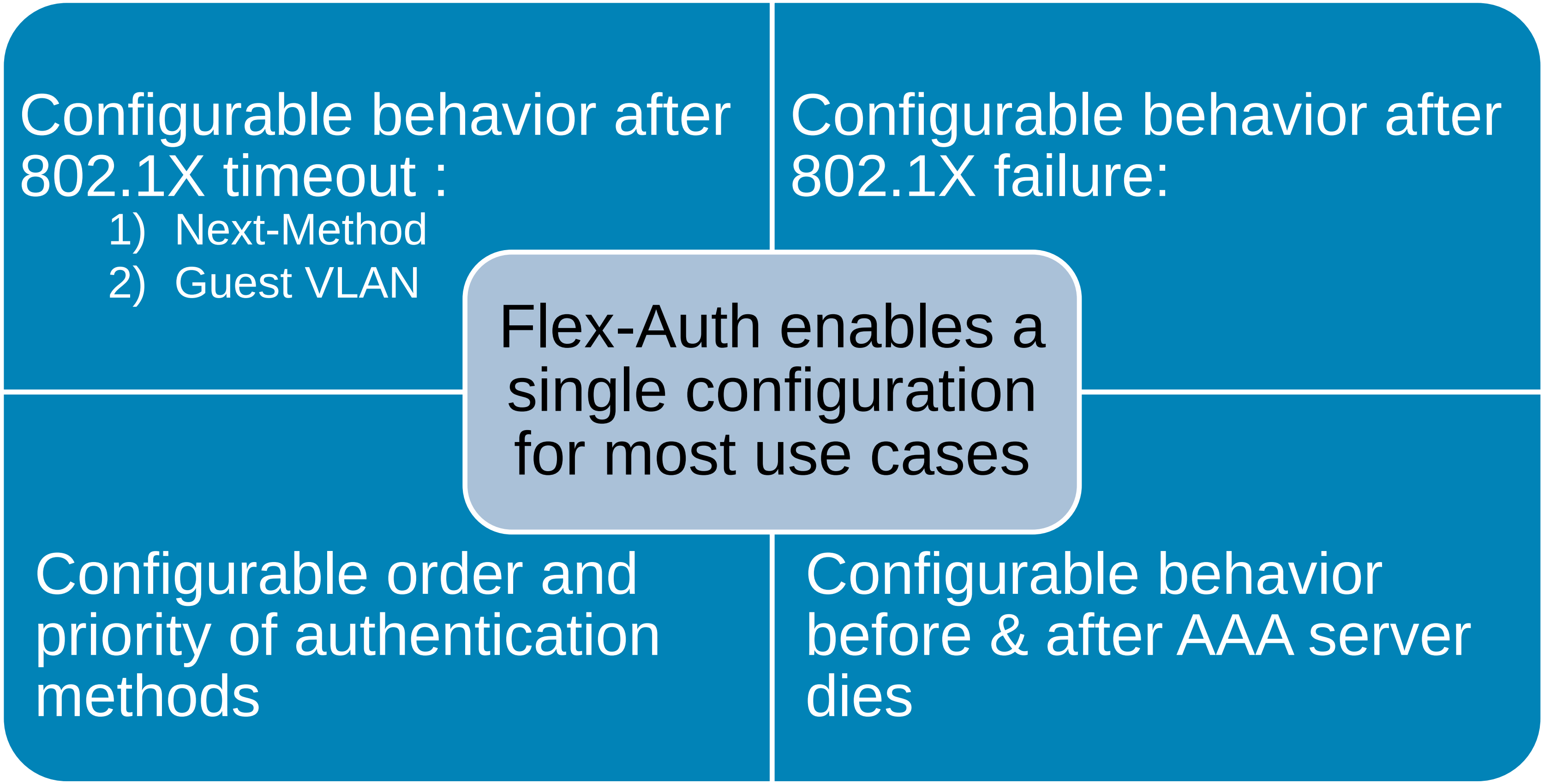
Machine VLAN

ACS: using AD groups for Authorization Rules

High Security: Unknown Devices

Flex-Auth for Unknown Devices

Agentless Devices in High Security Mode



Configurable behavior after 802.1X timeout :

1) Next-Method
2) Guest VLAN

Configurable behavior after 802.1X failure:

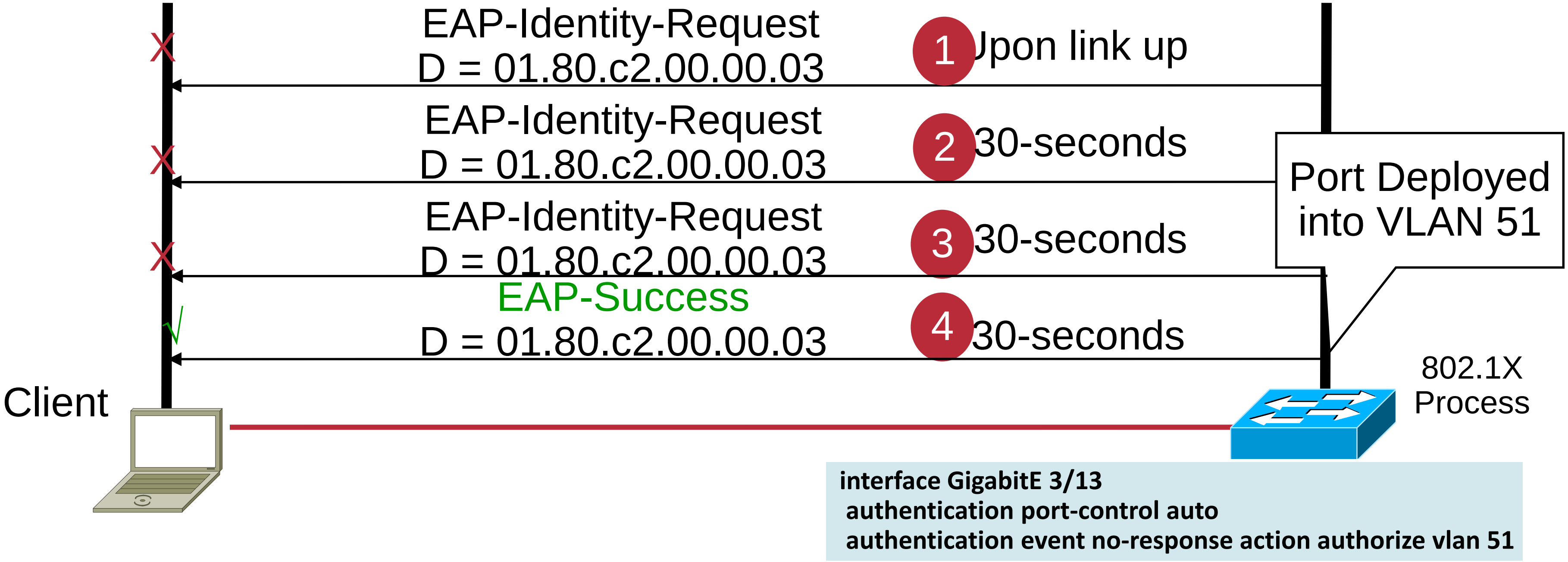
Flex-Auth enables a single configuration for most use cases

Configurable order and priority of authentication methods

Configurable behavior before & after AAA server dies

Non-802.1X Client

Guest VLAN



```
interface GigabitE 3/13
 authentication port-control auto
 authentication event no-response action authorize vlan 51
```

- Any 802.1X-enabled switchport will send EAPOL-Identity-Request frames on the wire (whether a supplicant is there or not)
- A device is only deployed into the guest VLAN based on the lack of response to the switch’s EAP-Request-Identity frames (which can be thought of as 802.1X hellos)
- No further security or authentication to be applied. It’s as if the administrator de-configured 802.1X, and hard-set the port into the specified VLAN

802.1X with Guest VLAN
Deployment Considerations

When a port moves to Guest VLAN, any number of additional MACs are allowed on the port without authenticating

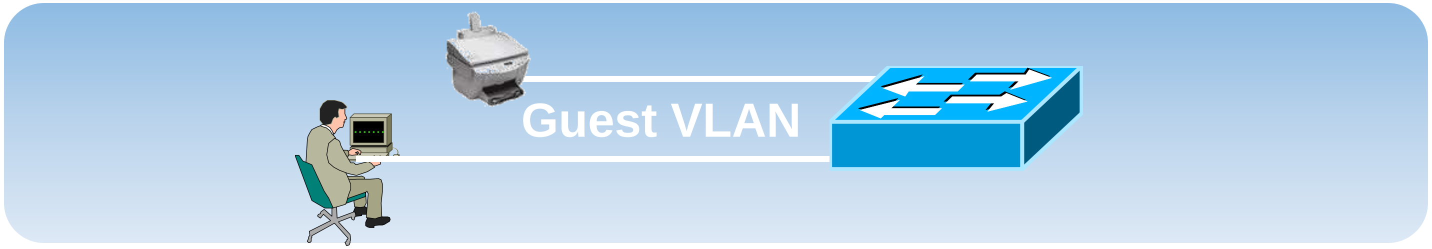
Guest VLAN is a switch-local authorization -> centralized policy on AAA server is not enforced

Guest VLAN does not differentiate, e.g. guest users get the same access as a corporate printer

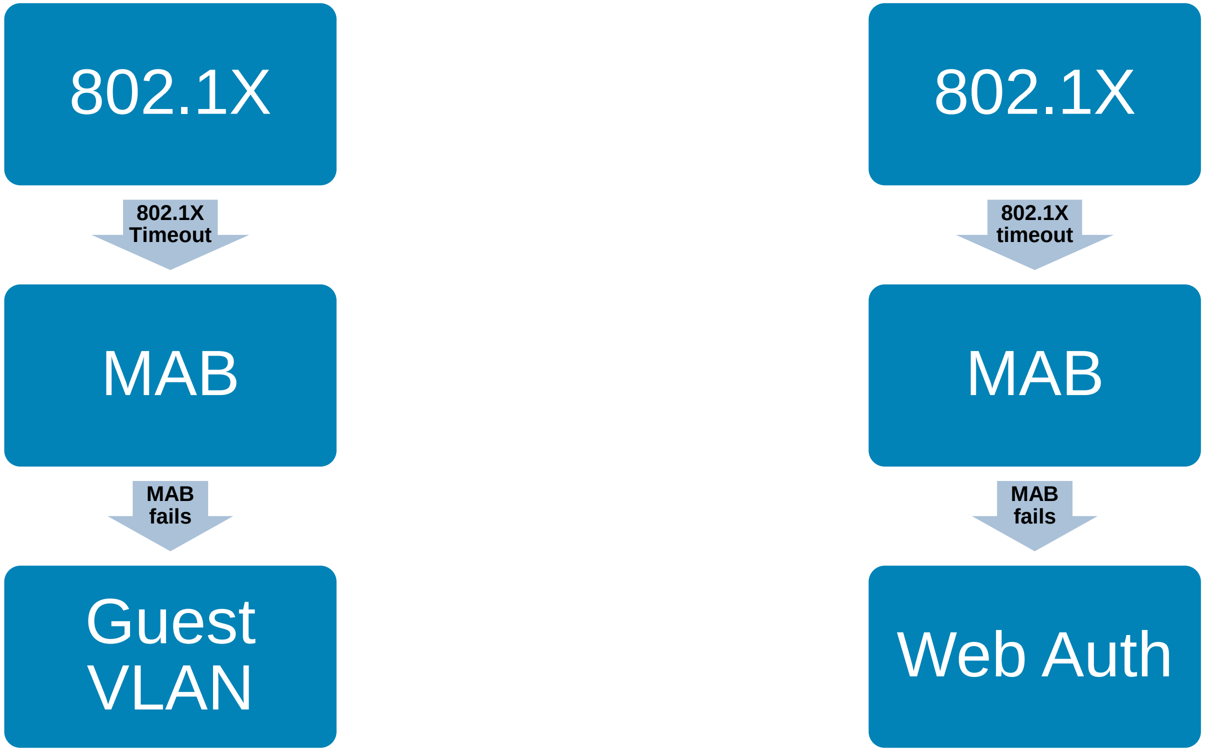
Guest VLAN can be fallback after 802.1X timeout and MAB fail

802.1X timeout dependency -> delayed network access.

- Default timeout is 30 seconds with three retries (90 seconds total)
- 90 seconds > DHCP timeout.



Guest VLAN and Web Auth Are Mutually Exclusive

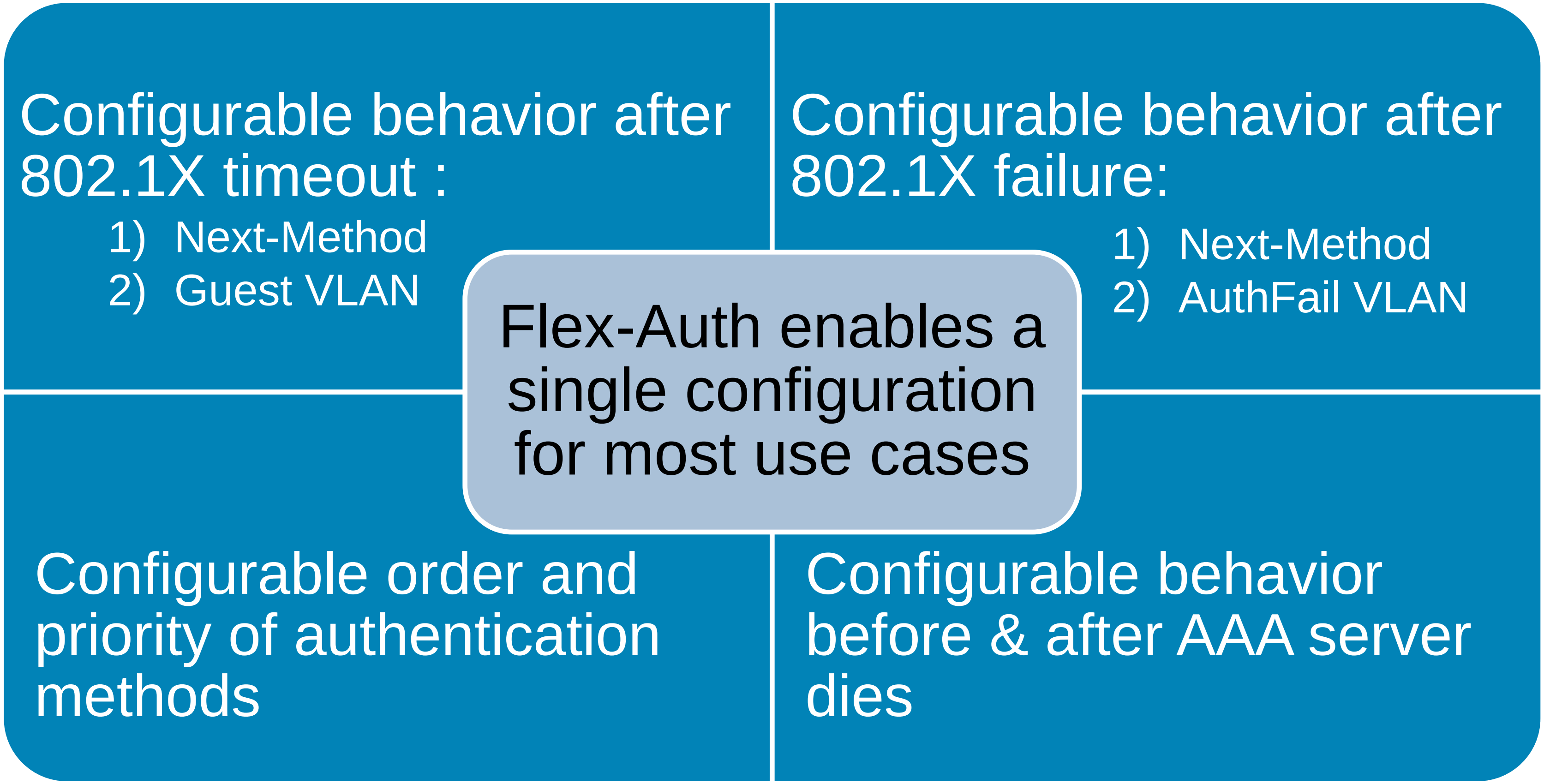


```
interface GigabitE 3/13
 authentication port-control auto
 dot1x  pae authenticator
 mab
 authentication event no-response  action authorize vlan 40
```

```
interface GigabitE 3/13
 authentication port-control auto
 dot1x  pae authenticator
 mab
 authentication fallback WEB-AUTH
```

Flex-Auth for Unknown Devices

Devices that Fail 802.1X in High Security Mode



Configurable behavior after 802.1X timeout :

1) Next-Method
2) Guest VLAN

Configurable behavior after 802.1X failure:

1) Next-Method
2) AuthFail VLAN

Flex-Auth enables a single configuration for most use cases

Configurable order and priority of authentication methods

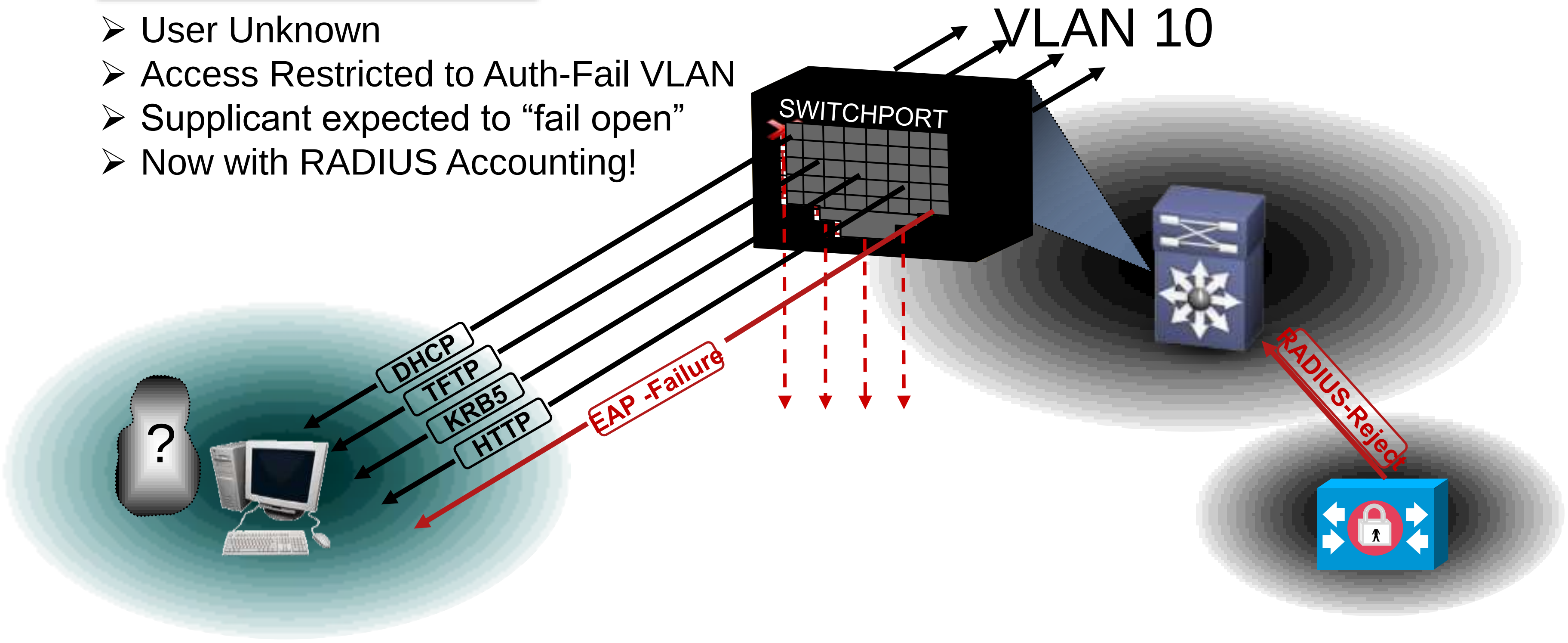
Configurable behavior before & after AAA server dies

Failed 802.1X

Auth-Fail VLAN Is An Alternative to Next-Method

After 802.1X Failure

- User Unknown
- Access Restricted to Auth-Fail VLAN
- Supplicant expected to “fail open”
- Now with RADIUS Accounting!



```
6506-2(config-if)#authentication event fail action authorize vlan 10
```

802.1X with Auth-Fail VLAN

Deployment Considerations

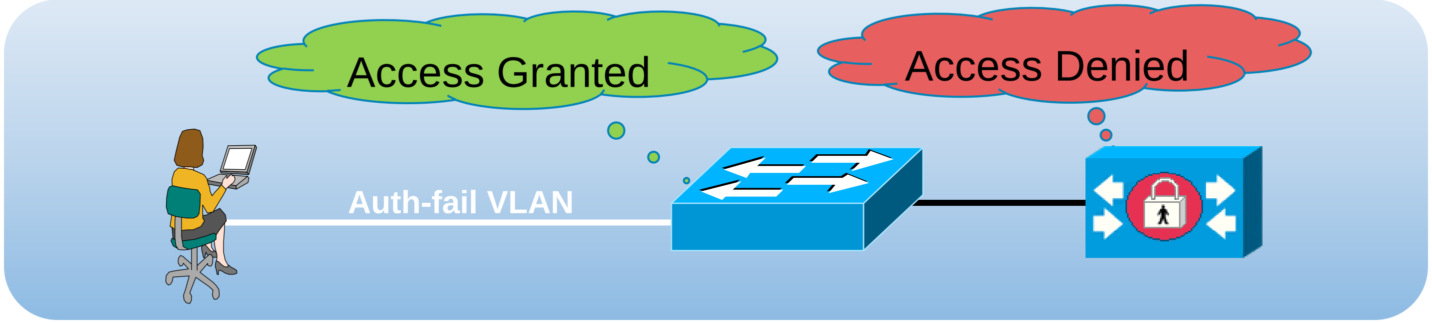
Supplicant cannot exit the Auth-Fail VLAN

- Only alternatives: switch-initiated re-authentication or port bounce

No Secondary Authentication Mechanism.

Auth-Fail VLAN, like Guest VLAN, is a switch-local authorization -> centralized policy on AAA server is not enforced

Switch and AAA server have conflicting views of network (mitigated by new RADIUS accounting)

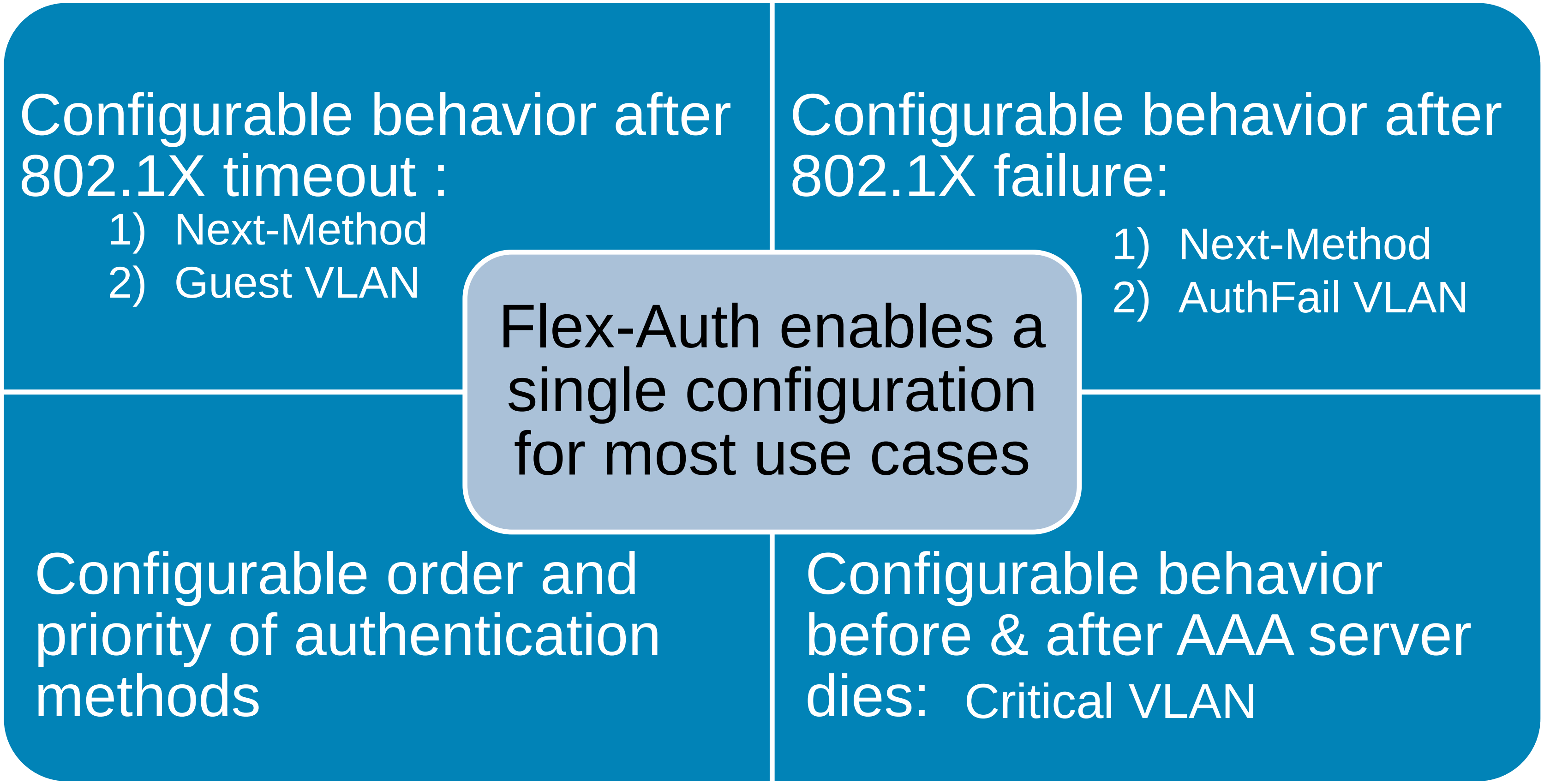


High Security: Network Access Table

Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	None	Closed Mode
Employees	802.1X Success	Enterprise Access	Default DATA VLAN
Corporate Asset	MAB Success	Enterprise Access	Default DATA VLAN
Phones	802.1X or MAB Success	Voice Access	Voice VLAN
Engineers	802.1X Success	Engineer Access	ENG VLAN
Machines	802.1X Success	Machine Access	MACHINE VLAN
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail	Limited Access	Auth-Fail VLAN = Guest VLAN = UNAUTH VLAN
All	None (AAA server down)	Enterprise Access	

Flex-Auth for Unknown Devices

Devices are Unknown because AAA is Down



Configurable behavior after 802.1X timeout :

1) Next-Method
2) Guest VLAN

Configurable behavior after 802.1X failure:

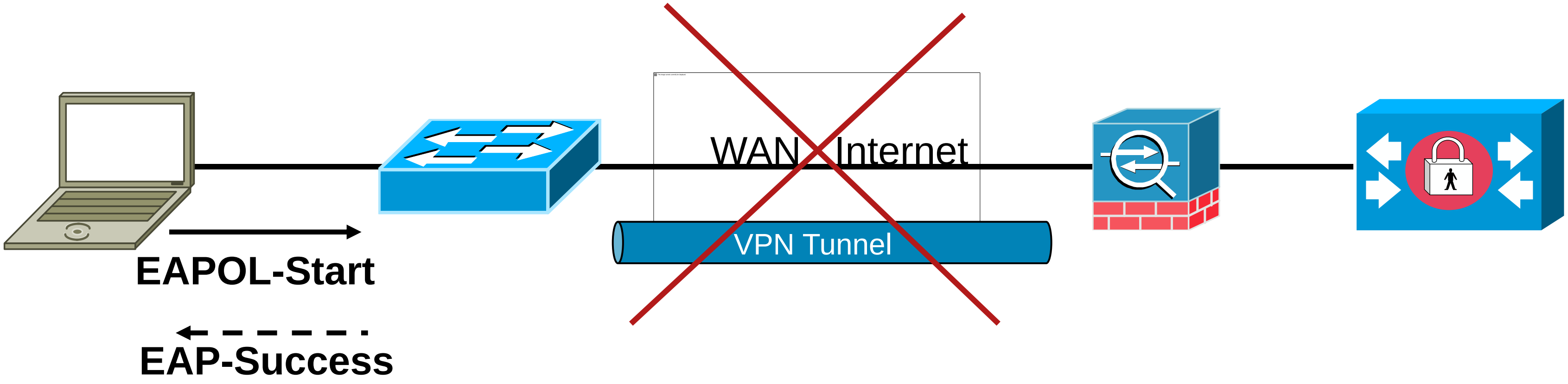
1) Next-Method
2) AuthFail VLAN

Flex-Auth enables a single configuration for most use cases

Configurable order and priority of authentication methods

Configurable behavior before & after AAA server dies: Critical VLAN

Inaccessible Authentication Bypass



- **Switch detects AAA unavailable by one of two methods**
  1. **Periodic probe**
  2. **Failure to respond to AAA request**
- **Enables port in critical VLAN if defined, otherwise to switchport VLAN**
- **Existing sessions retain authorization status**
- **Applies to data devices only**
- **Recovery action can re-initialize port when AAA returns**

RADIUS Server(s) Inaccessible

```
radius-server 10.1.10.50 test username KeepAliveUser key cisco
radius-server dead-criteria time 15 tries 3
radius-server deadtime 1

interface GigabitEthernet1/13
 description Dot1x Demo with Auth-Fail VLAN
 switchport access vlan 2
 switchport mode access
 switchport voice vlan 200
 authentication event fail action next-method
 authentication event server dead action authorize vlan 100
 authentication event server alive action reinitialize
 authentication order dot1x mab
 dot1x pae authenticator
 authentication port-control auto
 dot1x timeout tx-period 10
 dot1x max-req 2
 mab
 spanning-tree portfast
```

Critical VLAN can be anything:

- Static VLAN
- Same as guest/auth-fail VLAN
- New VLAN

High Security: Network Access Table

Endpoints	Authentication Status	Authorization	Implementation
All (including PXE)	Pre-Auth	None	Closed Mode
Employees	802.1X Success	Enterprise Access	Default DATA VLAN
Corporate Asset	MAB Success	Enterprise Access	Default DATA VLAN
Phones	802.1X or MAB Success	Voice Access	Voice VLAN
Engineers	802.1X Success	Engineer Access	ENG VLAN
Machines	802.1X Success	Machine Access	MACHINE VLAN
Unknown / Unauthorized	802.1X Fail/Timeout -> MAB Fail	Limited Access	Auth-Fail VLAN = Guest VLAN = UNAUTH VLAN
All	None (AAA server down)	Enterprise Access	Critical VLAN

Université de Montréal

Direction générale des technologies de l'information et de la communication

Mobility, Agility and Security Université de Montréal

Wired 802.1X Network Access control

Speaker: Michel L'Heureux, ing. PMP
Networking department manager at
Université de Montréal - DGTIC
June 2010

Université de Montréal

- **A Major University**
  - Founded in 1878, Université de Montréal, with its two affiliated schools: École Polytechnique and HEC Montréal, is now the largest university in Quebec and the second largest in Canada.
  - Deeply rooted in Montreal and dedicated to its international mission, the Université de Montréal is one of the top universities in the French-speaking world.
  - With its 13 programs, 80 departments and schools, the Université de Montréal offers programs in almost all academic fields
  - The University earmarks close to $460 million for basic and applied research each year, making it Canada's second most active university in the field.

A Network for the Future

- Network architecture project started in 2007
  - Objective: Become one of the best University Campus network
- Switching
  - Backbone upgrade to 10 Gb/s, MPLS in the Core
  - VSS for core redundancy and replace spanning-tree
  - Catalyst 6500E for Core and Distribution
  - Catalyst 4500E for 1 Gb/s network Access
- IP Telephony
  - 9000 IP Phones
  - Call manager v7, 2 Unity, 3 IPCC, 5 SRST
- Wifi
  - 2500 Access Points 802.11n
- Security
  - 802.1X authentication for all wired ports and wifi access

As we speak

- Switching – routing infrastructure
  - 80% completed
- IP Telephony
  - 80% completed
- Wifi
  - 60% completed
- Security
  - More than a thousand 802.1X-enabled wired ports
  - 25000 ports planned

Network security

An internal audit performed in 2005 demonstrated the University network access did not comply with security best practices.

- Private and distinct network from the Internet
  - 132.204.x.x -> 10.x.x.x
- Access control and secured (authentication)
  - 802.1X for each wired network port
- Network segmentation based on user role (Community).
  - Employee, Student and guest
  - Infrastructure community

Community segmentation

User community:

- Based on user role
- Assign from top security level.

Workstations	Security needs	Risk
Employees	Consult and manage confidential information	Lower risk for managed workstations (SCCM, Anti-virus, GPO)
Students	Basic + school work	High due to unmanaged workstation
Guest	Basic	Very High -- unknown workstation

Community segmentation

Isolating the communities

- Needs to reinforce new services for collaboration between different user communities
  - File sharing
  - Printing
  - Better use of central ressources

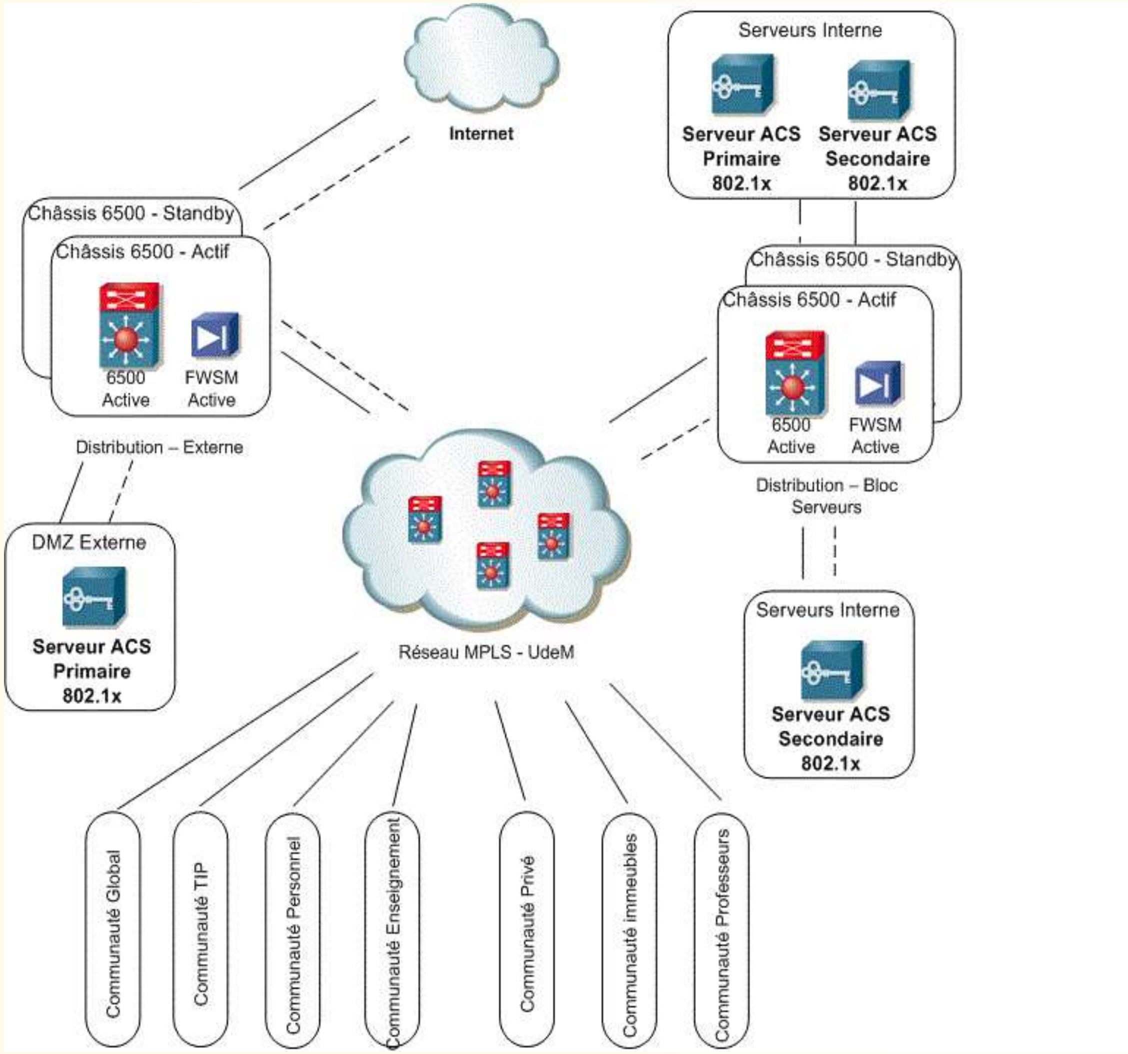
Univ de Montréal 802.1X deployment

- Use of centralized and unique AD accounts through Cisco ACS Radius servers
- Used of OS native « Supplicant » whenever possible. XP, Win7 and MAC
  - Credentials: AD Password
  - EAP Method: PEAP-MSCHAPv2
- A university managed workstation (registered on the AD domain) must do both Machine & User authentication. All others do only User auth.

Univ de Montréal 802.1X deployment (cont)

- Faculty Staff, students and guests are invited (and encouraged) to use 802.1X configuration with a supplicant
- Exceptions
  - IP Phones are not 802.1X aware (except G series) so CDP is used to bypass 802.1X
  - Web Auth is used for the first time user and for workstations not supporting supplicant
  - MAB (Mac Authentication Bypass) For device not supporting supplicant with no possibility to do Webauth (Printer, surveillance cameras, etc.)
  - Critical Auth VLAN

Dynamic VLAN assignment



Dynamic VLAN assignment

- How many VLANs are used?
  - One VRF for each “community”
- How do you managed VLAN assignment for users vs. machines ?
  - 1 VLAN per community per switch
  - Machines do not get a “community” Vlan. They land in a pre-auth VLAN

Environment Diversity snapshot

1. Remote access

- Remote access (RDP)
- Remote access Mac/Apple
- Net Support School

2. Licenses servers

- Windows 7
- Adobe, Sequencher, FileMaker, MatLab and others

3. Startup services

- NetBoot (Mac/Apple)

4. Linux

- SSH, LDAP, Kerberos, NIS, NFS / Samba, Rdist, rsync, scp, puppet

5. Other cold imaging, backup and recovery software

- GHOST
- RedHat Network / YUM, Yellowdog Updater Modifier
- SCCM2007 (System Center Configuration Manager)

Challenge and solutions

- « GHOSTing machines »
  - Use of MAB to configure GHOST environment
- Remote Desktop Windows
  - Must leave the desktop ‘’logged in’’ and locked

Challenge and solutions (cont)

- WebAuth on Catalyst 4500
  - « Authentication timeout », this issue produced a forced re-auth after 30 min. Users would loose their session everytime. Could not configure this through normal timeout control. This was escalated to Cisco.
  - Early Fix was supplied to correct this. Waiting for the next IOS release 12.2.53 SG3 for full permanent integration.
  - Webauth portal login page unable to display any custom images or logo.
  - Webauth portal login page cannot redirect the user to any other pages or Web site

Challenge and solutions (cont)

- « Apple Net Boot »
  - Very limited fonctionnality in a routed environment
  - Challenge implementing 802.1X config
  - Support for scripting is only available from 10.6.2 OS

Lessons Learned

- A few advises for proper deployment:
  - Problems are not so much in the 802.1X protocol but more in the operational aspect of the deployment.
  - Careful definition and identification of the users needs is mandatory.
  - Cisco doesn’t supply tools to integrate 802.1X in an heterogeneous environment like a university campus.
- Monitoring and troubleshooting
- At deployment time, prepare to cope with a flow of help-desk calls
  - Plan in building your own processes and tools.

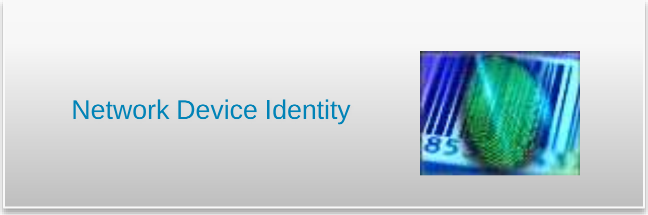
Questions

Advanced Features
NEAT

NEAT

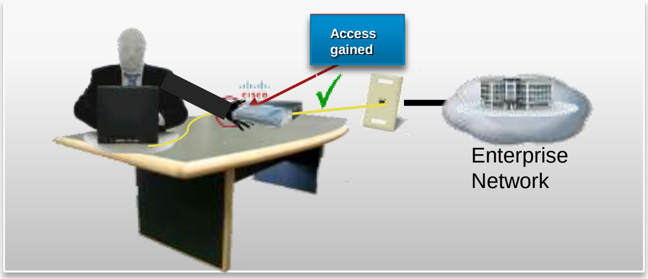
Problem Statement & Drivers

- Customers requirement is to have (network) device based access control for tighter security



- Compact switches like Cisco Catalyst 8-port 3560 or 2960 will be deployed in an unsecured area such as cubicles, conference rooms, etc.
  - outside the secured wiring closet

- These network devices can potentially be swapped with hacker devices to gain network access, compromising the network security

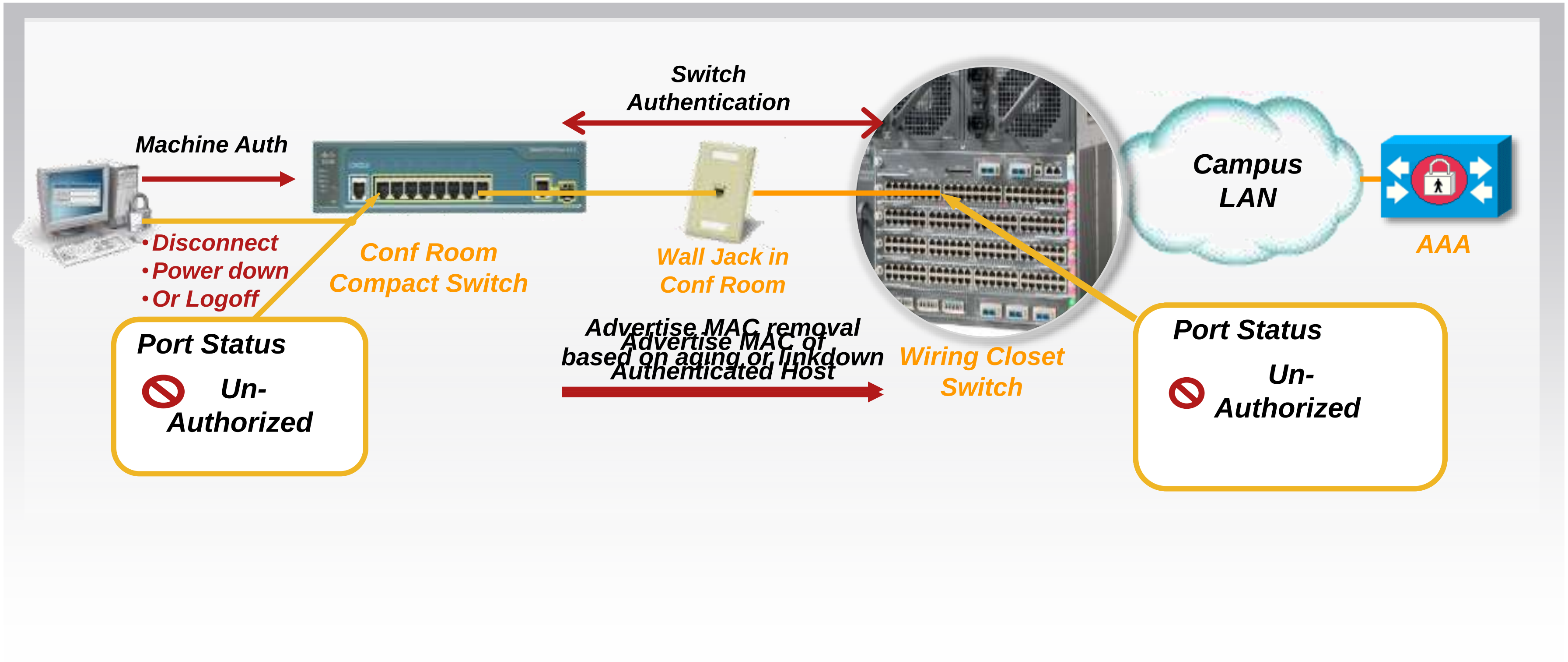


Result

Customers want ***network device authentication*** to ***mitigate*** these types of ***security threats***

Network Edge Authentication Topology

Network Edge Trust Extension



- Extend Trust to into physically unsecured locations (*e.g., conference room, cubical, etc.*)
- Secure access control for shared media access

Advanced Features
CoA

RADIUS Change of Authorization (CoA)

RFC 3576: Defines “Packet of Disconnect”

- Terminates session

Cisco has extended support for CoA

- Terminate session
- Re-authenticate
- Port bounce
- Port down

Each type of Action has specific use case support

CoA – Use Cases

Failed Authentication with Failed Auth VLAN

- CoA can reauth or terminate a session can retrigger authentication to try authentication after remediation

Adding new mac addresses to the network

- After Profiling or other change order an agentless devices may need it's IP changed
- CoA with Port Bounce can be used to reset the IP stack on an agentless device

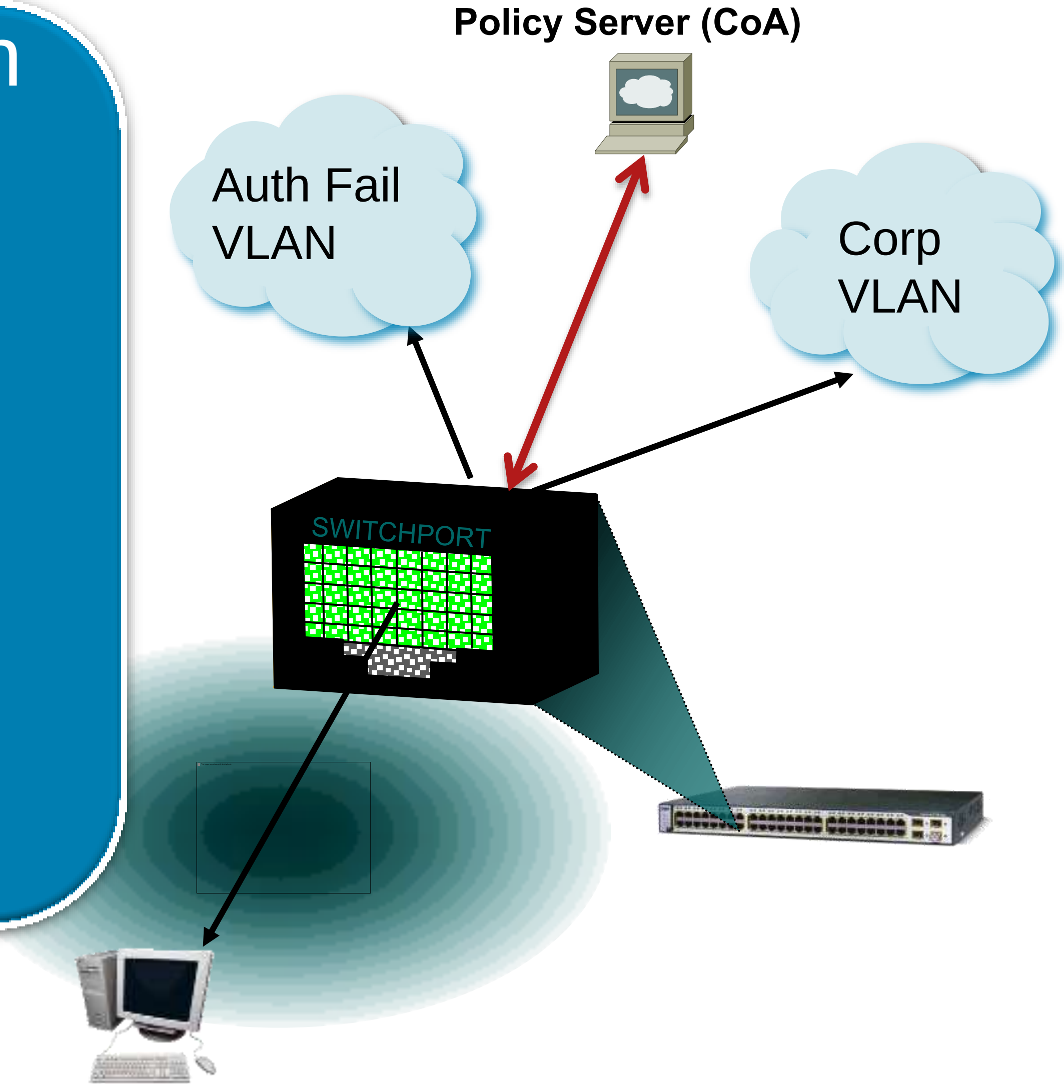
Abnormal/Destructive behavior is observed on the network

- CoA with Port Down is a emergency shut off of a port. It can only be re-enabled by CLI

RADIUS Change of Authorization (CoA)

Dynamic session control from a Policy server

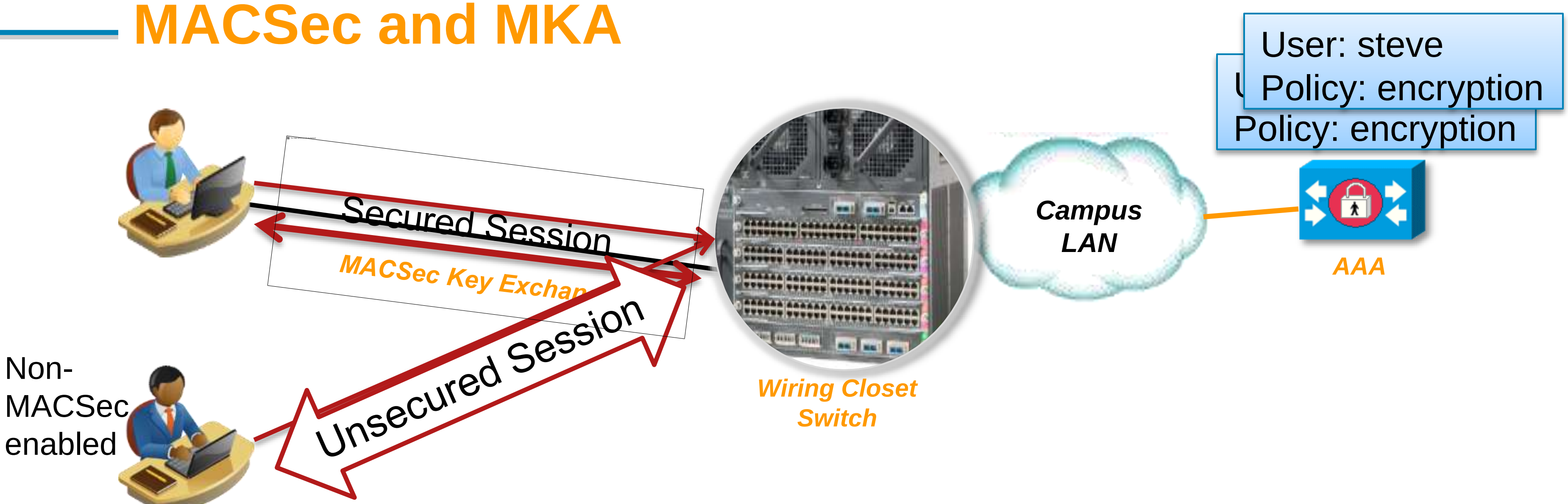
- Re-authenticate session
- Terminate session
- Terminate session with port bounce
- Disable host port
- Session Query
  - For Active Services
  - For Complete Identity
  - Service Specific
- Service Activate
- Service De-activate
- Service Query



Advanced Features
802.1X Rev

Identity 4.1 Feature: 802.1X-Rev

MACSec and MKA



1 User bob connects

2 Bob’s policy indicates end point must encrypt

3 Key exchange using MKA, 802.1AE encryption complete
User is placed in Corp VLAN
Session is secured

4 User steve connects

5 Steve’s policy indicates end point must encrypt

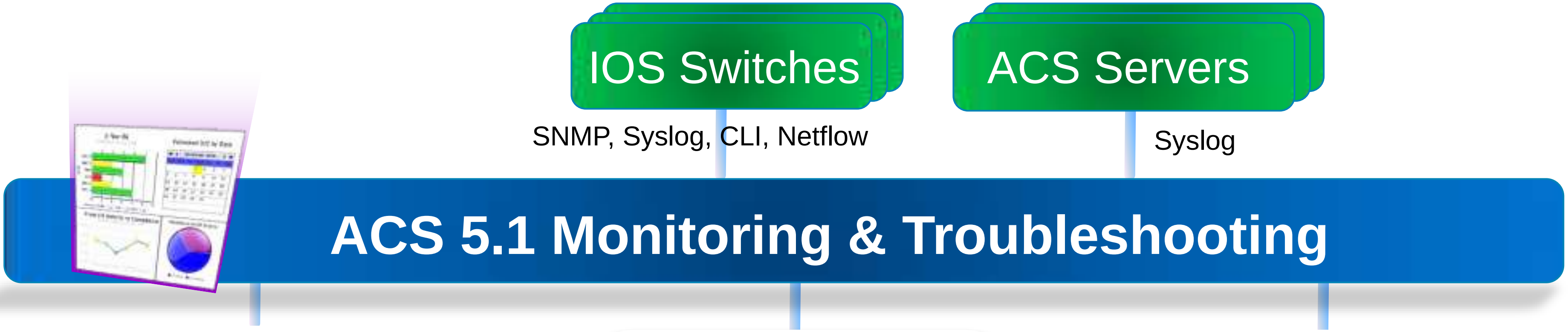
6 End point is not MACSec enabled
Assigned to Guest VLAN

802.1X-Rev Components

- MACSec enabled switches (Incredibles)
- AAA server 802.1X-Rev aware
- Supplicant supporting MKA and 802.1AE encryption

Advanced Features
Monitoring & Troubleshooting

Monitoring and Troubleshooting



IOS Switches

ACS Servers

SNMP, Syslog, CLI, Netflow

Syslog

ACS 5.1 Monitoring & Troubleshooting

Monitoring

User Reporting

- Where, when, how connected
- How long, how often
- Last passed, last failed
- Switch Log Reporting

System Reporting

- Pass/Fail ratio

Device Reporting

- Profile History
- Status of profiled device

Troubleshooting

- Expert Troubleshooting Tool
- Troubleshooting Workflow
  - –Authentication Failure
  - –Authorization Failure
- Switch log failure analysis

Alerts

- Unknown NAS
- New ACS, new NAD
- External DB unavailable
- Failed Auths thresholds
- Passed auths thresholds
- AAA down

ACS 5.1 Uses Multiple Sources of Information For Monitoring/Troubleshooting

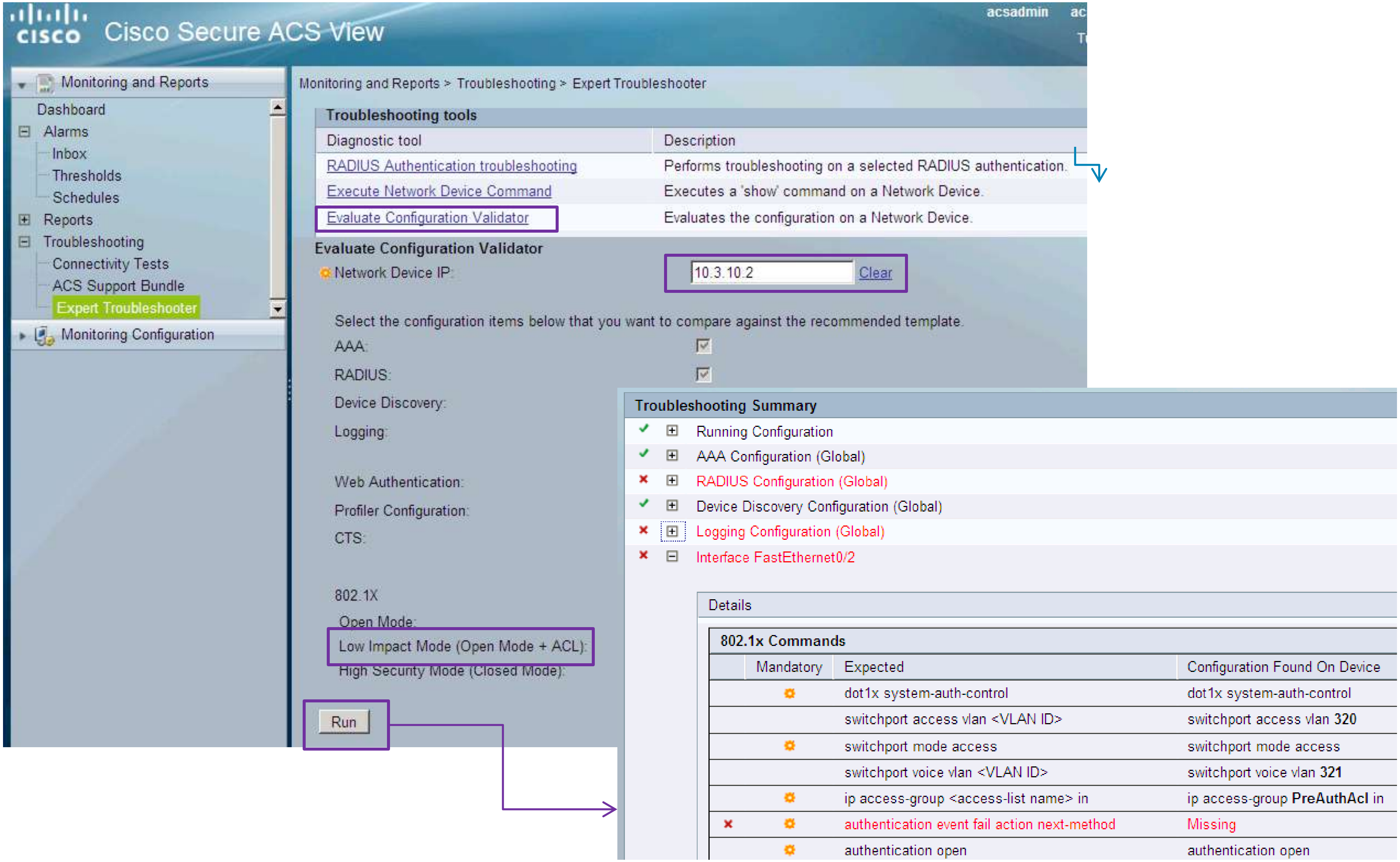
Sources

- RADIUS logs
- Syslog from ACS(s)
- Syslog from Switches
- CLI
- SNMP

ACS 5.1 Tools

- Authentication Reports
- Session Directory
- Configuration Validator
- Network Device & Session Details
- Expert Troubleshooter

Configuration Validator



Troubleshooting tools

Diagnostic tool	Description
RADIUS Authentication troubleshooting	Performs troubleshooting on a selected RADIUS authentication.
Execute Network Device Command	Executes a 'show' command on a Network Device.
Evaluate Configuration Validator	Evaluates the configuration on a Network Device.

Evaluate Configuration Validator

Network Device IP: 10.3.10.2

Select the configuration items below that you want to compare against the recommended template.

AAA: ☑

RADIUS: ☑

Device Discovery:

Logging:

Web Authentication:

Profiler Configuration:

CTS:

802.1X

Open Mode:

Low Impact Mode (Open Mode + ACL):

High Security Mode (Closed Mode):

Troubleshooting Summary

✓	⊞	Running Configuration
✓	⊞	AAA Configuration (Global)
✗	⊞	RADIUS Configuration (Global)
✓	⊞	Device Discovery Configuration (Global)
✗	⊞	Logging Configuration (Global)
✗	⊟	Interface FastEthernet0/2

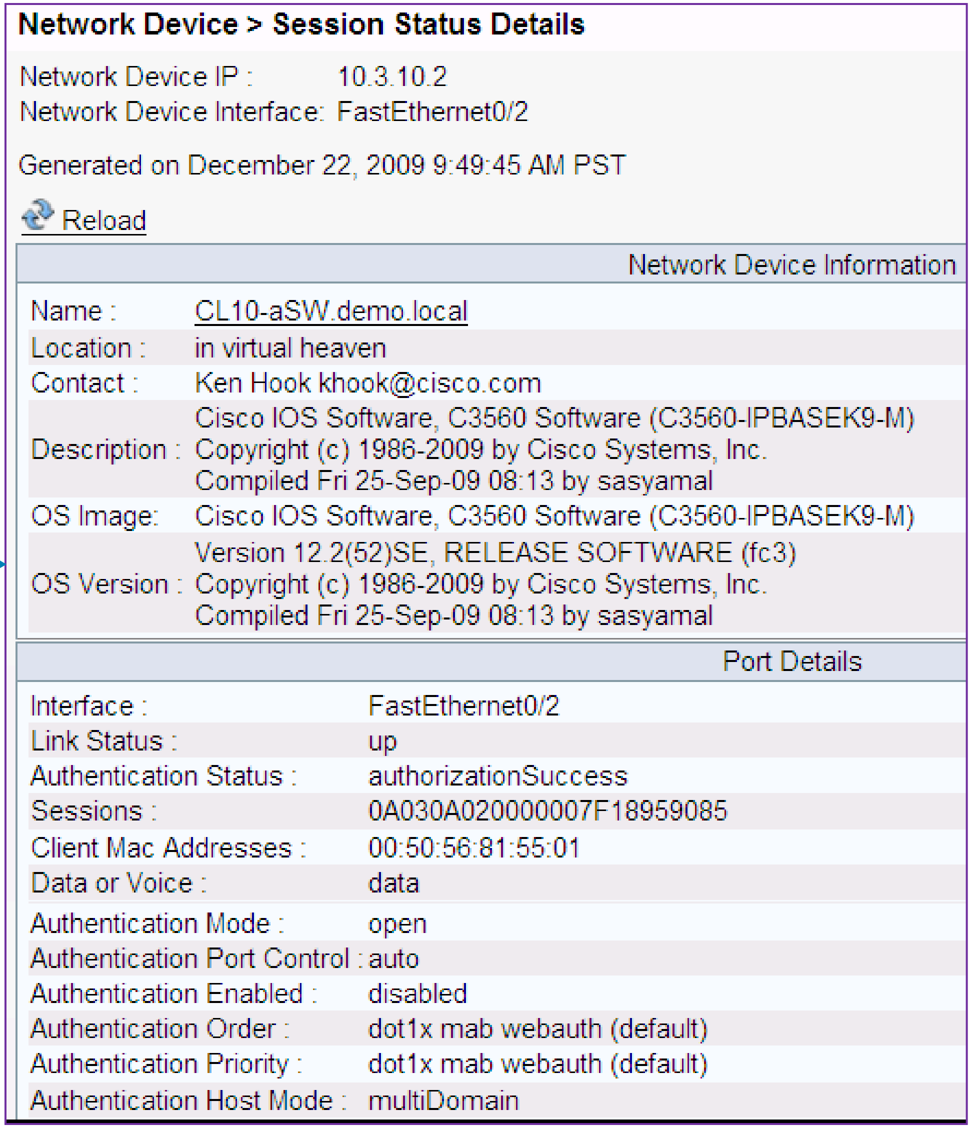
Details

802.1x Commands

	Mandatory	Expected	Configuration Found On Device
	✹	dot1x system-auth-control	dot1x system-auth-control
		switchport access vlan <VLAN ID>	switchport access vlan **320**
	✹	switchport mode access	switchport mode access
		switchport voice vlan <VLAN ID>	switchport voice vlan **321**
	✹	ip access-group <access-list name> in	ip access-group **PreAuthAcl** in
✗	✹	authentication event fail action next-method	Missing
	✹	authentication open	authentication open

On Demand SNMP Polling

MIB-II (RFC-1213-MIB)
INTERFACE-MIB
IEEEE8021-PAE-MIB
CISCO-PAE-MIB
CISCO-AUTH-FRAMEWORK-MIB
CISCO-MAB-MIB



Network Device > Session Status Details

Network Device IP : 10.3.10.2
Network Device Interface: FastEthernet0/2

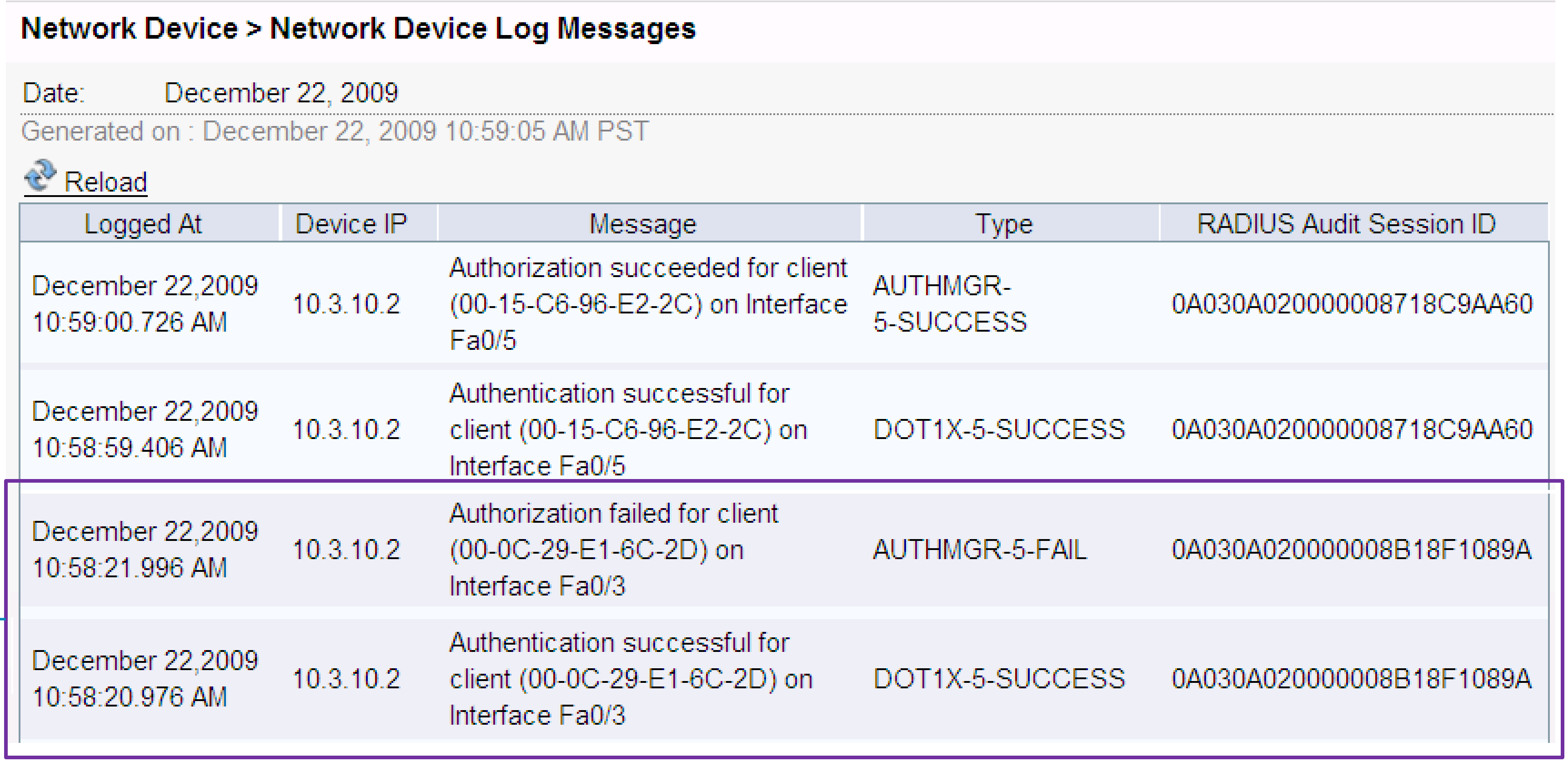
Generated on December 22, 2009 9:49:45 AM PST

Reload

	Network Device Information
Name :	CL10-aSW.demo.local
Location :	in virtual heaven
Contact :	Ken Hook khook@cisco.com
Description :	Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M) Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Fri 25-Sep-09 08:13 by sasyamal
OS Image:	Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M)
OS Version :	Version 12.2(52)SE, RELEASE SOFTWARE (fc3) Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Fri 25-Sep-09 08:13 by sasyamal

	Port Details
Interface :	FastEthernet0/2
Link Status :	up
Authentication Status :	authorizationSuccess
Sessions :	0A030A020000007F18959085
Client Mac Addresses :	00:50:56:81:55:01
Data or Voice :	data
Authentication Mode :	open
Authentication Port Control :	auto
Authentication Enabled :	disabled
Authentication Order :	dot1x mab webauth (default)
Authentication Priority :	dot1x mab webauth (default)
Authentication Host Mode :	multiDomain

Centralized View of Switch Syslogs



Network Device > Network Device Log Messages

Date: December 22, 2009

Generated on : December 22, 2009 10:59:05 AM PST

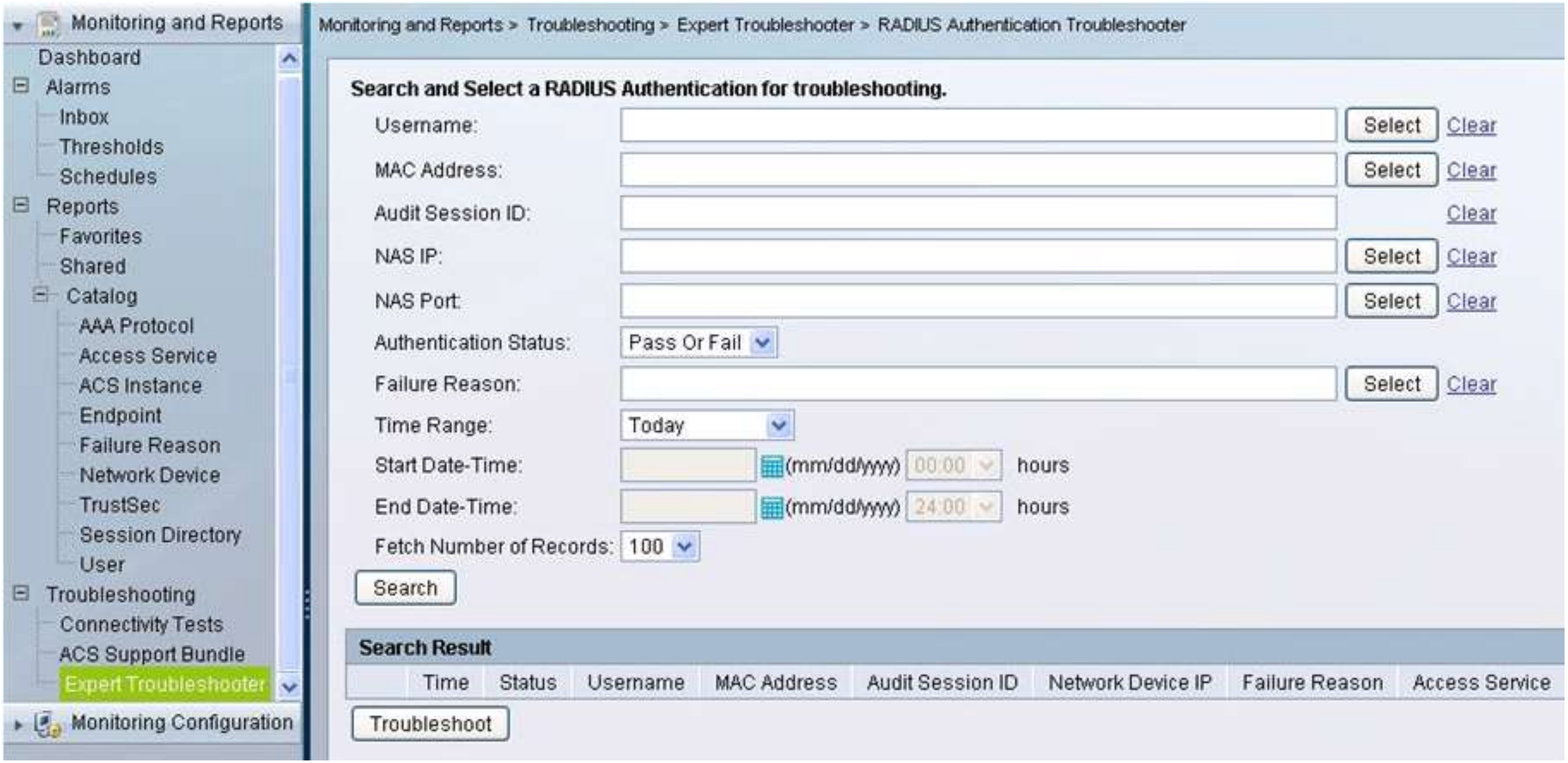
Reload

Logged At	Device IP	Message	Type	RADIUS Audit Session ID
December 22,2009 10:59:00.726 AM	10.3.10.2	Authorization succeeded for client (00-15-C6-96-E2-2C) on Interface Fa0/5	AUTHMGR-5-SUCCESS	0A030A02000008718C9AA60
December 22,2009 10:58:59.406 AM	10.3.10.2	Authentication successful for client (00-15-C6-96-E2-2C) on Interface Fa0/5	DOT1X-5-SUCCESS	0A030A02000008718C9AA60
December 22,2009 10:58:21.996 AM	10.3.10.2	Authorization failed for client (00-0C-29-E1-6C-2D) on Interface Fa0/3	AUTHMGR-5-FAIL	0A030A020000008B18F1089A
December 22,2009 10:58:20.976 AM	10.3.10.2	Authentication successful for client (00-0C-29-E1-6C-2D) on Interface Fa0/3	DOT1X-5-SUCCESS	0A030A020000008B18F1089A

Authentication passed (credentials were good) but switch was unable to apply authorization instructions (e.g. bad VLAN assignment).

Expert Troubleshooter

- Research failures by troubleshooting workflows



Monitoring and Reports > Troubleshooting > Expert Troubleshooter > RADIUS Authentication Troubleshooter

Search and Select a RADIUS Authentication for troubleshooting.

Username:

MAC Address:

Audit Session ID:

NAS IP:

NAS Port:

Authentication Status: Pass Or Fail

Failure Reason:

Time Range: Today

Start Date-Time: (mm/dd/yyyy) 00:00 hours

End Date-Time: (mm/dd/yyyy) 24:00 hours

Fetch Number of Records: 100

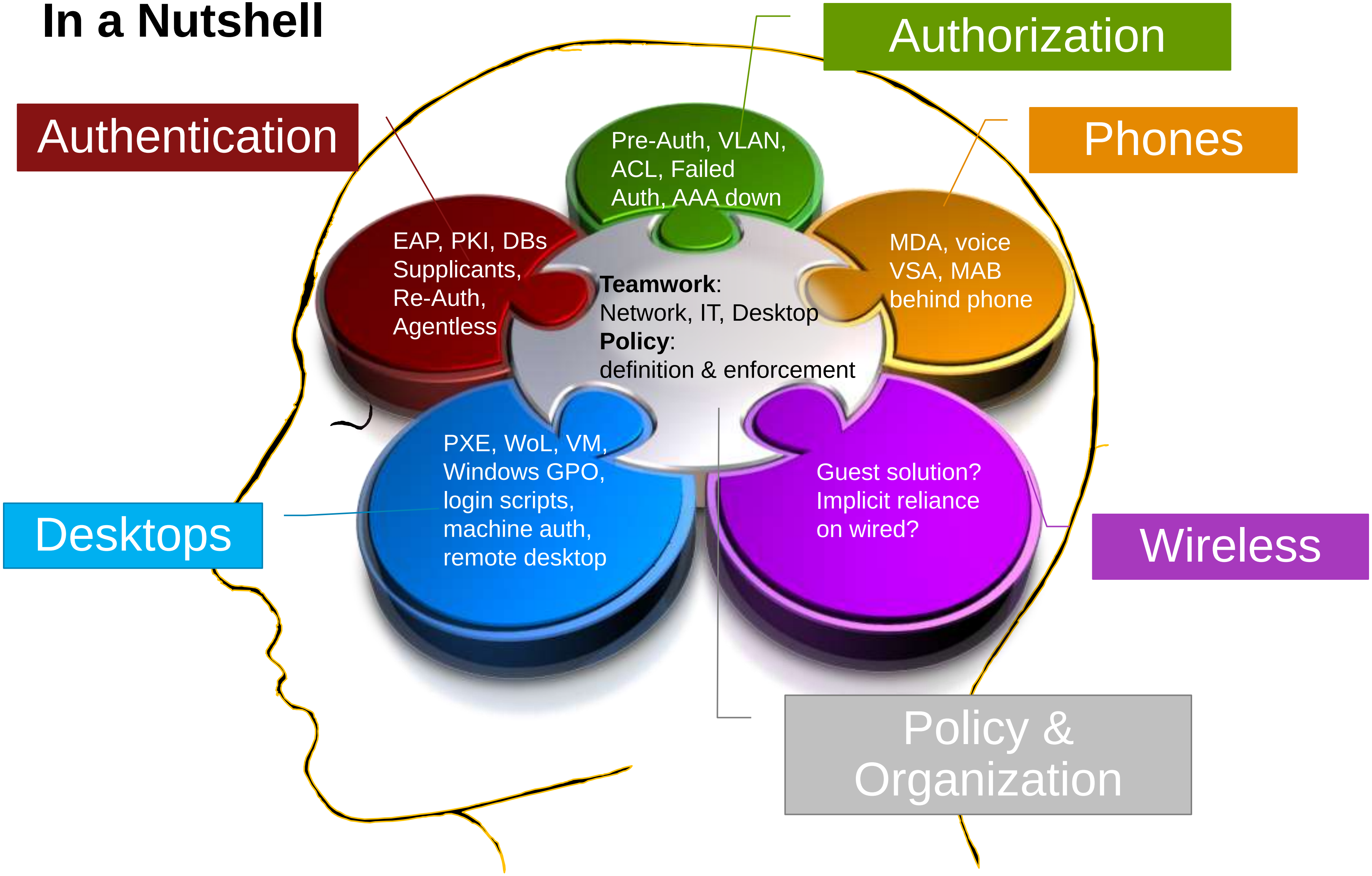
Search Result

	Time	Status	Username	MAC Address	Audit Session ID	Network Device IP	Failure Reason	Access Service

Session Summary

Deployment Considerations

In a Nutshell



Authentication

EAP, PKI, DBs Supplicants, Re-Auth, Agentless

Authorization

Pre-Auth, VLAN, ACL, Failed Auth, AAA down

Phones

MDA, voice VSA, MAB behind phone

Teamwork: Network, IT, Desktop

Policy: definition & enforcement

Desktops

PXE, WoL, VM, Windows GPO, login scripts, machine auth, remote desktop

Wireless

Guest solution? Implicit reliance on wired?

Policy & Organization

Summary

- 802.1X improves enterprise security
- 802.1X improves enterprise visibility
- 802.1X deployable now
  - New features have significantly simplified deployment
  - Deployment scenarios can be used as a starting point
- 802.1X is not only a network project, it affects the whole IT organization