



# Identity and Endpoint Solutions in the Campus



**Francesca Martucci**  
**Consulting System Engineer – Security**  
**[martucci@cisco.com](mailto:martucci@cisco.com)**

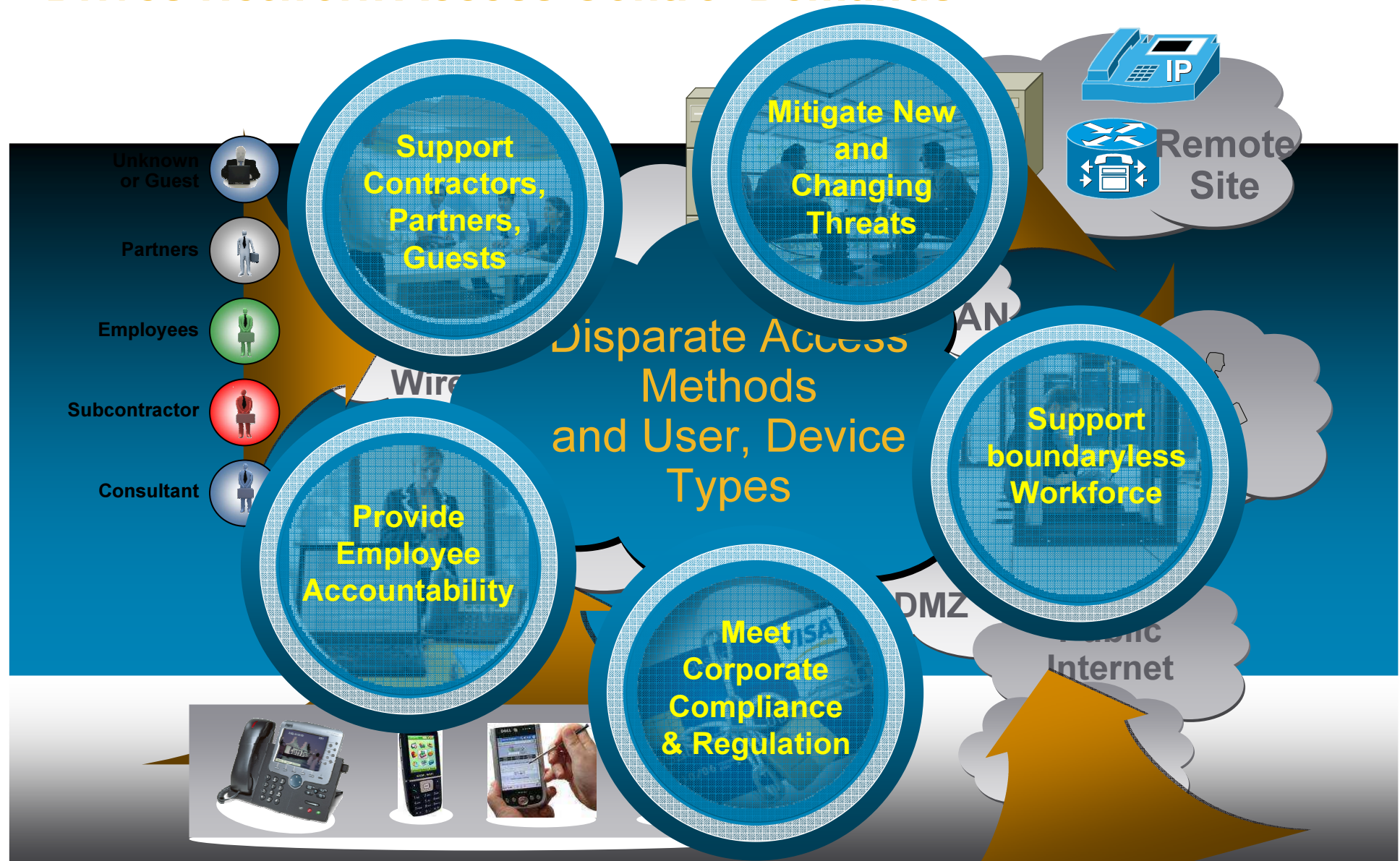
# Agenda

- The changing Business
- Identity deployment in phases
  - Introduce 802.1x without business disruption
  - Non 802.1x devices and guests
  - Policy management
  - Posturing
- Recent Cisco Security Updates
  - Botnet Filtering
  - Collaborative IPS
  - New Safe architecture



# Changing Business Environment

## Drives Network Access Control Demands



# Identity Key Drivers

## Market Trends

- Gartner forecasts 50% to 70% 802.1x adoption in 2011
- Several 10,000+ node and few 100,000+ node deployments are underway
- Forrester studies indicate 42% of network upgrade is for security
- Identity is an important component in Cisco's Network as a Platform initiative

## Compliance

- PCI: fines for credit card information security breach
- Sarbanes-Oxley, penalties for non-compliance, 10-20 years in Jail\*
- HIPAA: Up to \$250,000 in fines and 5 years in Jail—per violation
- Gramm-Leach-Bliley Act (GLBA): CIO-level staff can be held personally liable plus penalties and class-action suits
- Notification of Risk to Personal Data Act (NORPDA)/SB1386 (California): All customers must be notified of breach

### Measurable Impact:

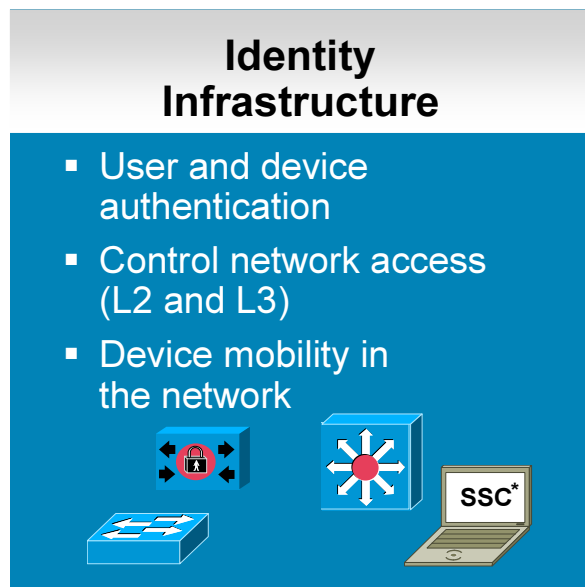
Fraud, downtime, man-hours, physical destruction, intellectual property, lawsuits

### Non-measurable Impact:

Reputation, customer privacy, medical information, productivity



# Identity-based network access



\* Cisco Secure Services Client

## Profiling Services



- Device profiling
- Behavioural monitoring
- Device reporting

## Guest Services



- Guest and sponsor portals
- Role-based AUP
- Provisioning and reporting

## Posture Services

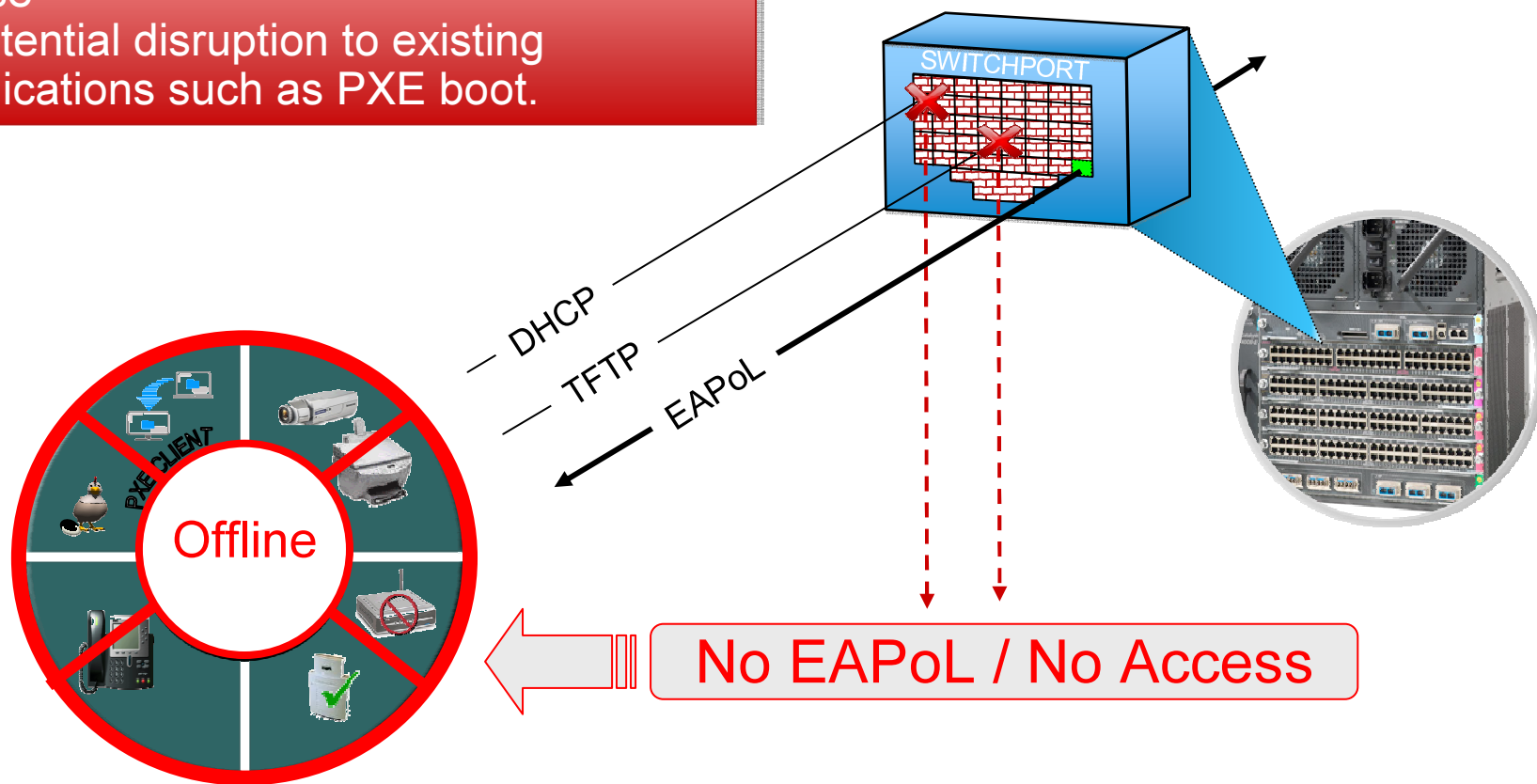


- Managed device posture
- Unmanaged device scanning
- Remediation

# IEEE 802.1X Default Security Behavior

## IEEE 802.1x Challenges

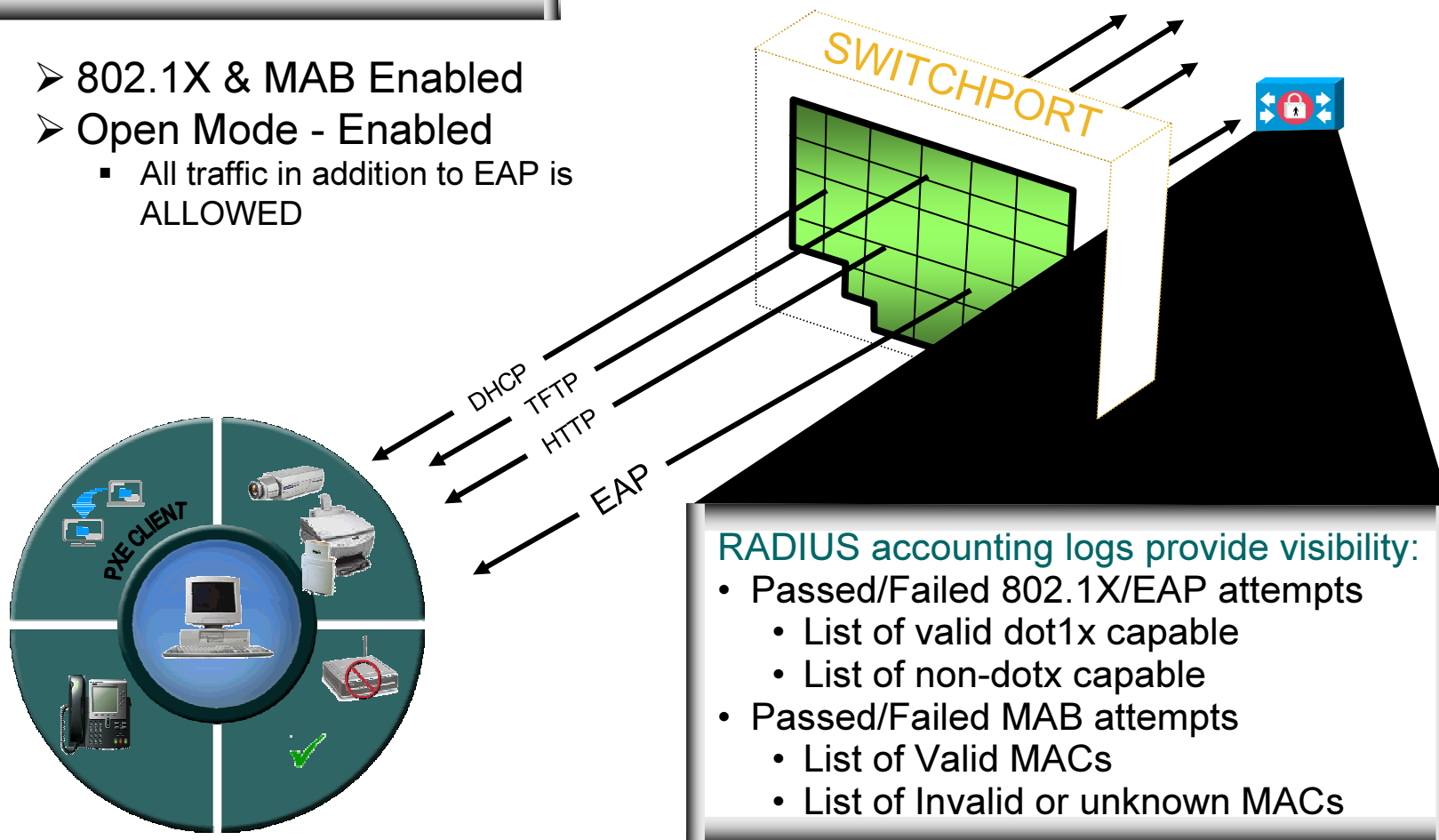
- Switch port changes from open → Close
- Potential disruption to existing applications such as PXE boot.



# 802.1X/MAB – Open Mode

Open Mode (No Restrictions)

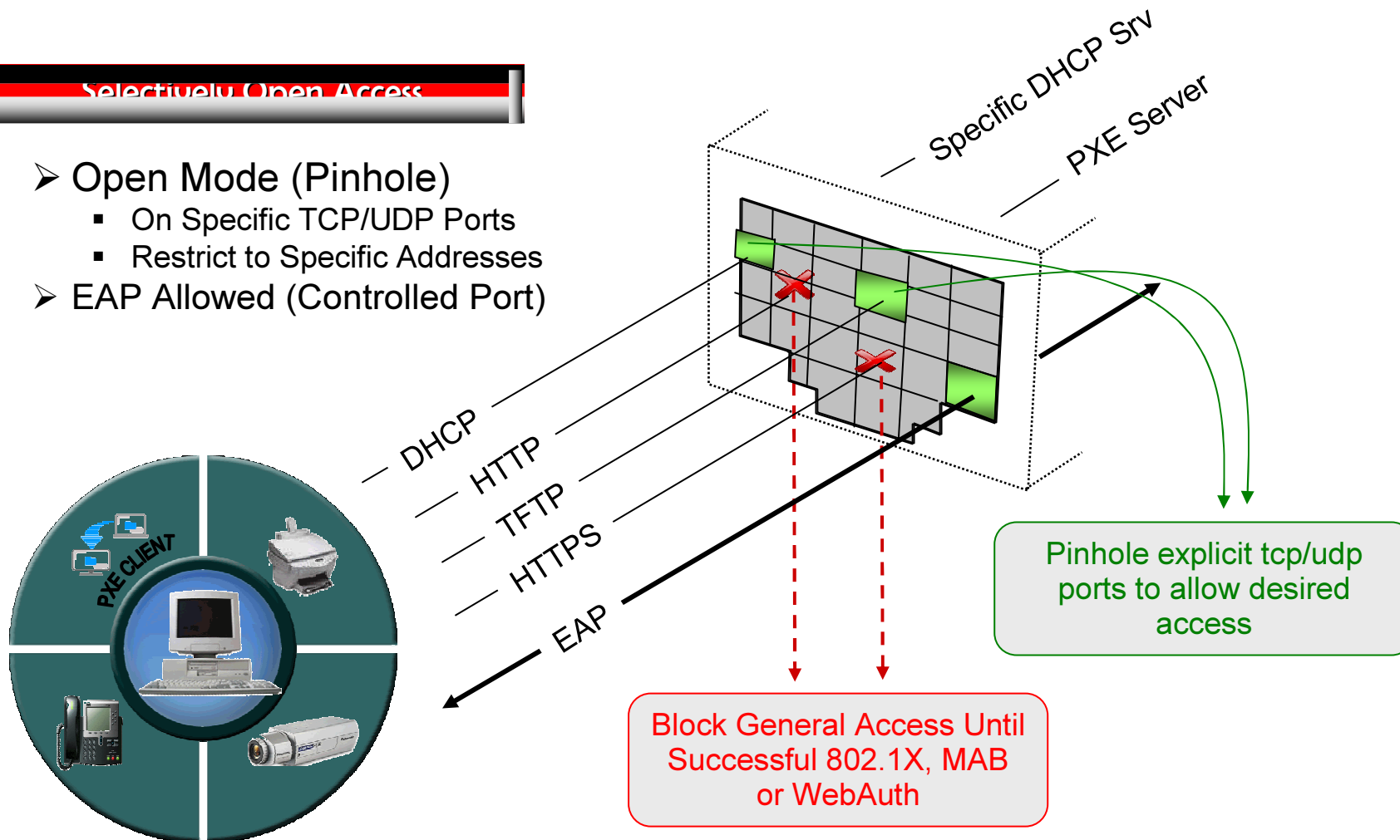
- 802.1X & MAB Enabled
- Open Mode - Enabled
  - All traffic in addition to EAP is ALLOWED



# 802.1X/MAB – Open Mode

## Selectively Open Access

- Open Mode (Pinhole)
  - On Specific TCP/UDP Ports
  - Restrict to Specific Addresses
- EAP Allowed (Controlled Port)

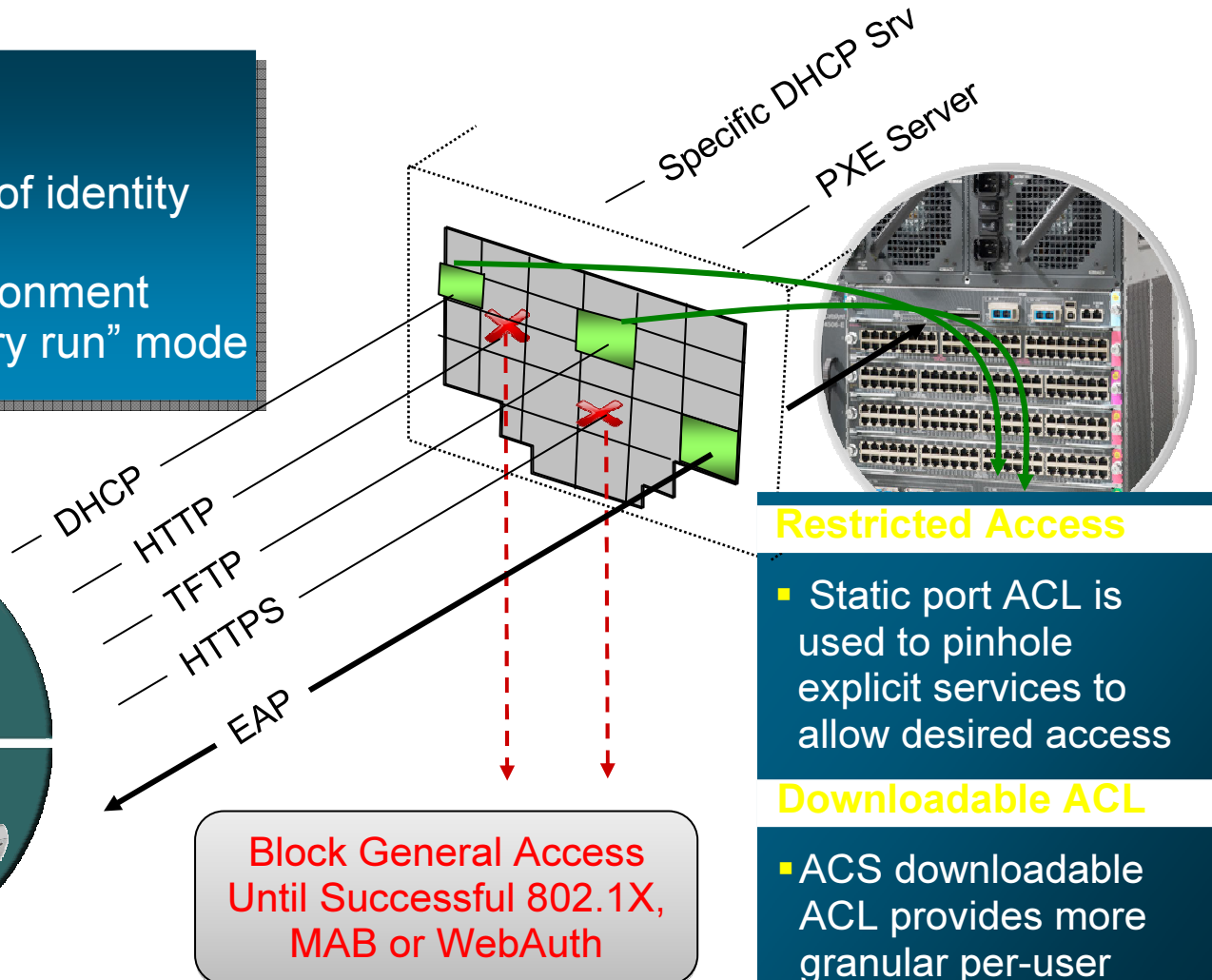


# Open Mode With Restricted Access

## Balancing Act

### Open Mode Benefits:

- Reduce Network impact of identity deployment
- Supports PXE boot environment
- Provides customers a “dry run” mode



### Restricted Access

- Static port ACL is used to pinhole explicit services to allow desired access

### Downloadable ACL

- ACS downloadable ACL provides more granular per-user access control after authentication

# Device Profiling With NAC Profiler

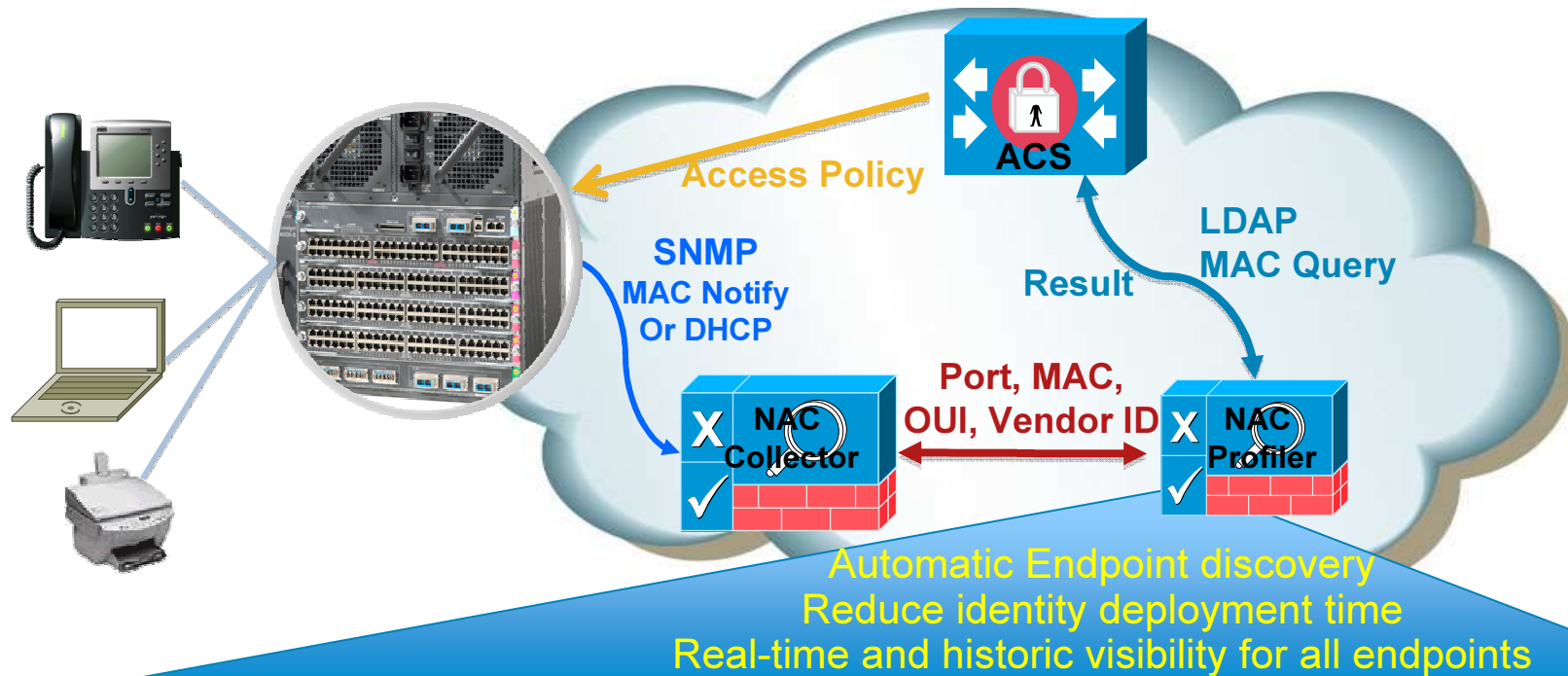


Table of Windows OS  
Total Profiles 9 Summary

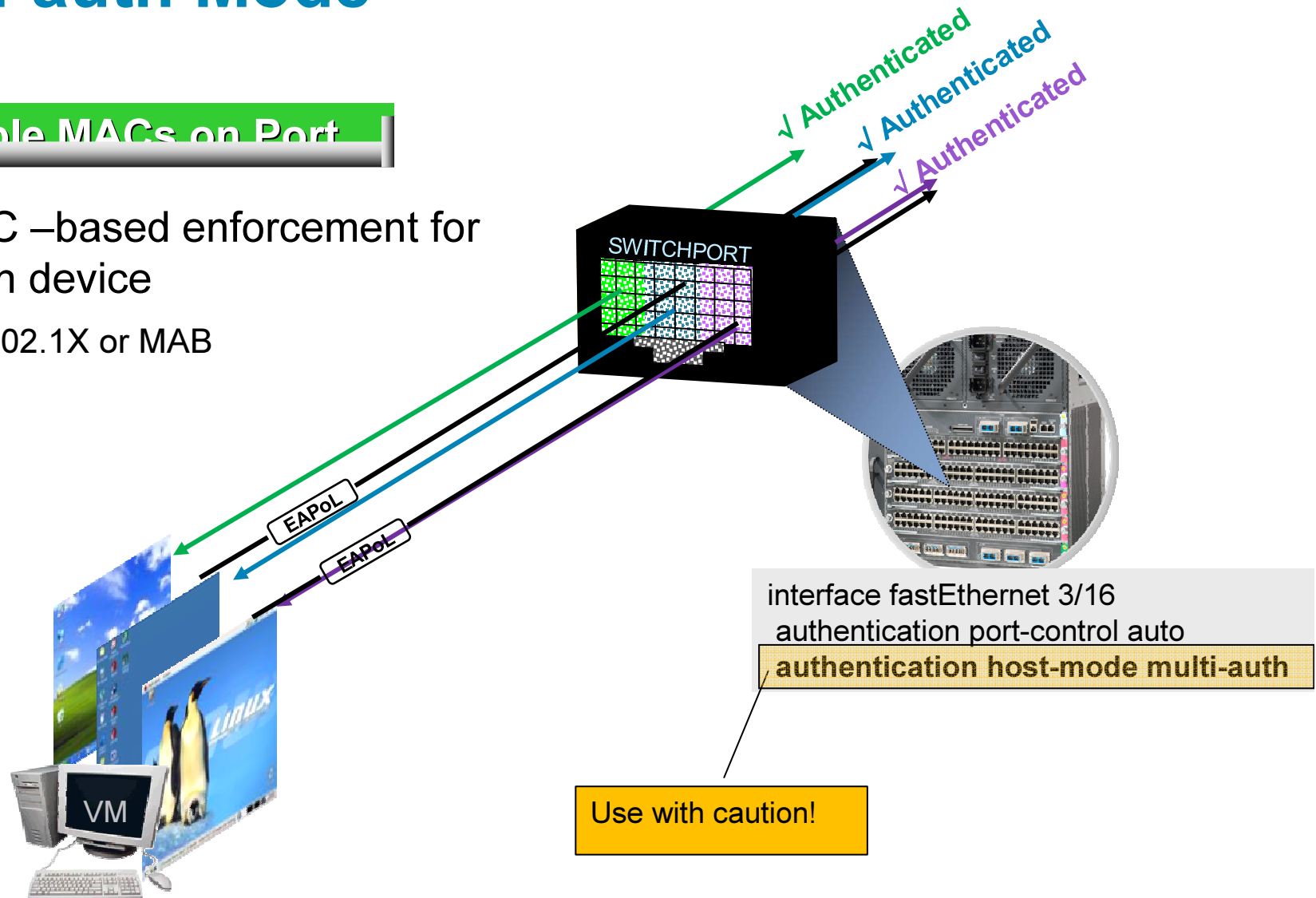
MAC	IP	Certainty	Switch IP port	Link	VLAN
00:1c:c4:03:b0:2d (Hewlett Packard)	10.100.10.122	60%	6506 Distribution Gi1/23	Up	1
00:18:f8:09:cf:d7 (Cisco-Linksys LLC)	10.100.30.201	60%	4506-2 Gi1/0/5	Up	30



# Multi-auth Mode

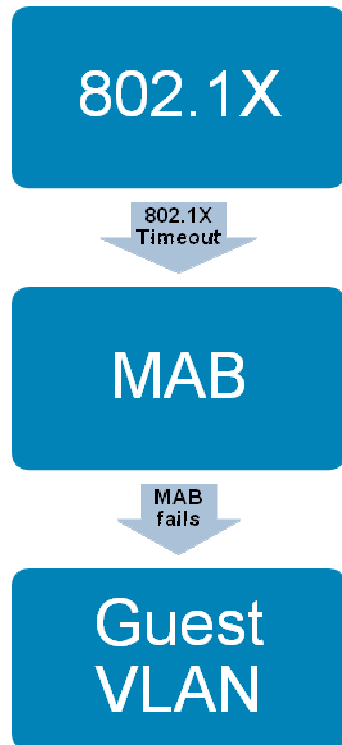
## Multiple MACs on Port

- MAC –based enforcement for each device
  - 802.1X or MAB

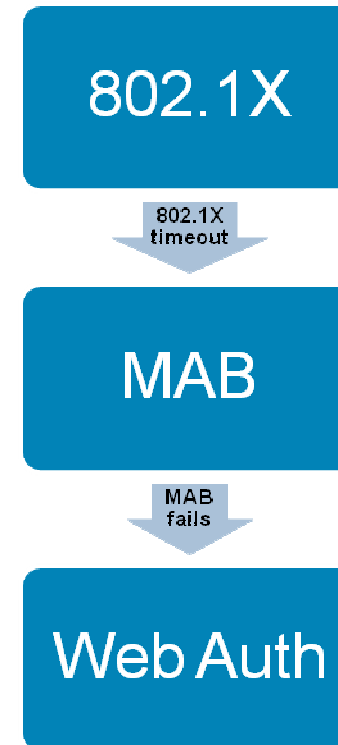


# Default Ordering:

## 802.1X, MAB, Web Auth, Guest VLAN interactions



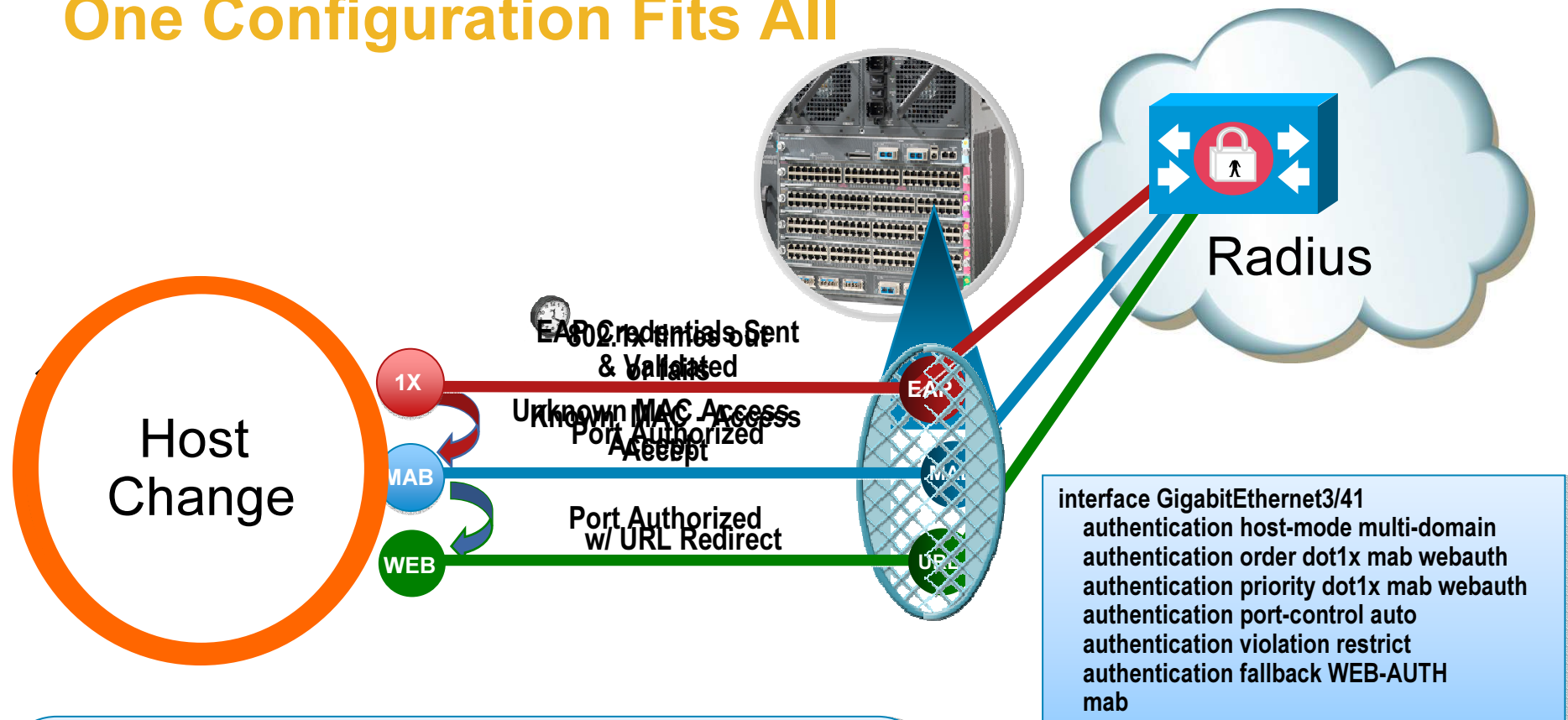
```
interface GigabitE 3/13
 authentication port-control auto
 dot1x pae authenticator
 mab
 authentication event no-response action authorize vlan 40
```



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

# Flexible Authentication

## One Configuration Fits All



- One configuration addresses all use cases, all host modes
- Controllable sequence of access control mechanisms, with flexible failure and fallback authorization
- Choice of policy enforcement mechanisms: VLAN, downloadable per-user ACL, URL
- Support single-host and multi-auth scenarios

# Identity Deployment Phases

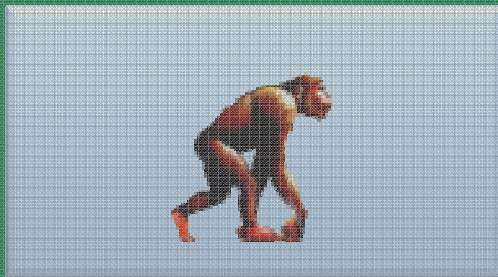
## Monitor Mode

### Primary Features

- Open mode
- Multi-Auth
- Flex Auth (Optional)

### Benefits

- Unobstructed Access
- No Impact on Productivity
- Gain Visibility AAA Logs



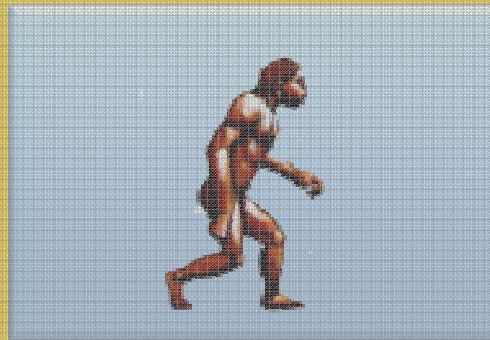
## Low Impact Mode

### Primary Features

- Open mode
- Multi-Domain
- Port & dACLs

### Benefits

- Maintain Basic Connectivity
- Increased Access Security
- Differentiated Access



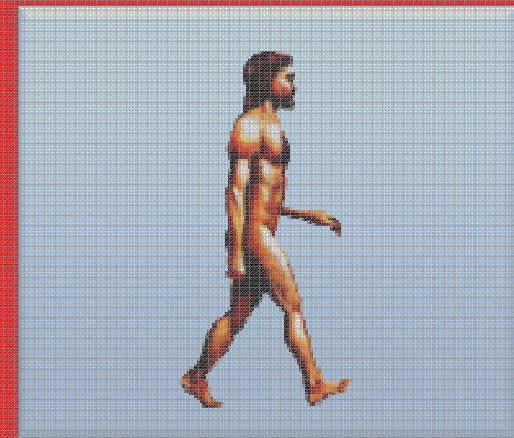
## High Security Mode

### Primary Features

- Traditional Closed Mode
- Dynamic VLANs

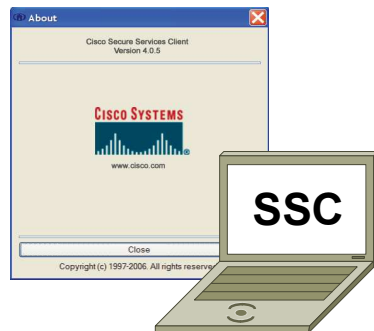
### Benefits

- Strict Access Control



# Optional: Cisco Secure Services Client (SSC)

- Introduces features over and above the native supplicants
  - EAP types
  - Management Interfaces
  - Automatic VPN initiation



## Secure Services Client

### Features

- Robust Profile Management
- Support for industry standards
  - Endpoint integrity
  - Single sign-on capable
- Enabling of group policies
  - Administrative control

### Benefits

- Simple, secure device connectivity
- Minimizes chances of network compromise from infected devices
  - Reduces complexity
- Restricts unauthorized network access
  - Centralised provisioning

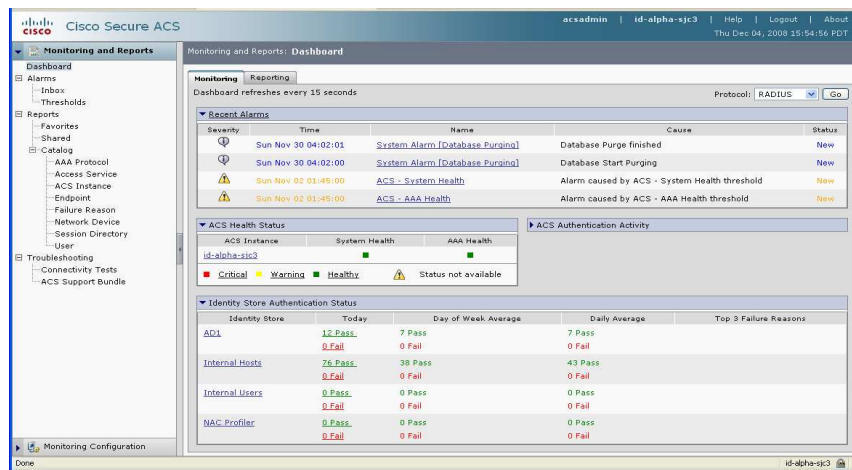
# Agenda

- The changing Business
- Identity deployment in phases
  - Introduce 802.1x without business disruption
  - Non 802.1x devices and guests
  - **Policy management**
  - Posturing
- Recent Cisco Security Updates
  - Botnet Filtering
  - Collaborative IPS
  - New Safe architecture





# Cisco Secure ACS 5.0



## Rule-based Policy Engine

- Attribute-driven approach enables dynamic, context based policy
- Compose-able policy
- Granular policy building blocks
- Policies that reflect the real world

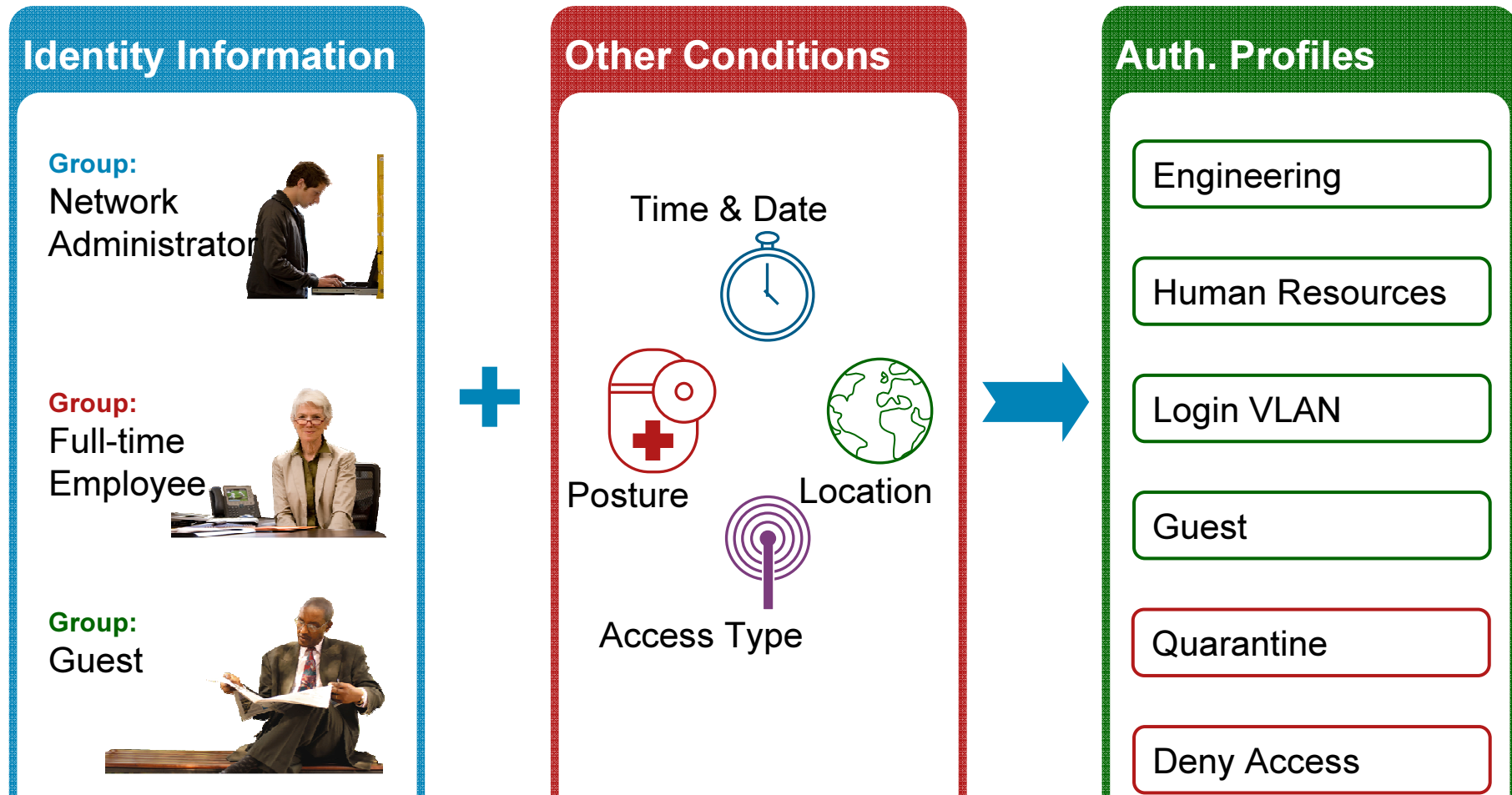
## Integrated Monitoring

- Integrated advanced monitoring, reporting & troubleshooting capabilities for maximum control and visibility
- Compliance

## Improved GUI

- Lightweight, secure, intuitive and easy to use web-based GUI
- Does not require additional client software for GUI access

# ACS 5: Rule-based policy



## Authorisation based on identity plus context

Conditions are specified as policy rules - IF <conditions> THEN <permission>

# Employee Authorization Profile



## Define Authorization Policy for Employees & Managed Assets

- Assign corporate VLAN & permit ip any any dACL

The screenshot displays the Cisco Secure ACS web interface. On the left, the 'Policy Elements' menu is expanded, with 'Authorization Profiles' selected. The main area shows a list of authorization profiles: Employee, Guest, Machine, and Phone. The 'Employee' profile is selected, and its configuration details are shown in a pop-up window.

**Policy Elements : Authorization and Permissions > Network Access > Authorization Profiles**

**Authorization Profiles** Items 1-4 of 4

Filter: Description Match if: Contains Profile Clear Filter

Name	Description
Employee	Employee Profile with Corporate VLAN and dACL assignment
Guest	Guest Profile with Guest VLAN Assignment
Machine	Machine Profile with Machine VLAN + ACL Assignment
Phone	Phone Profile with ACL assignment

**Policy Elements : Authorization and Permissions > Network Access > Authorization Profiles**

**General Common Tasks RADIUS Attributes**

VLAN ID/Name: Static Value corporate

URL for Redirect: Not in Use

URL Redirect ACL: Not in Use

**ACLs**

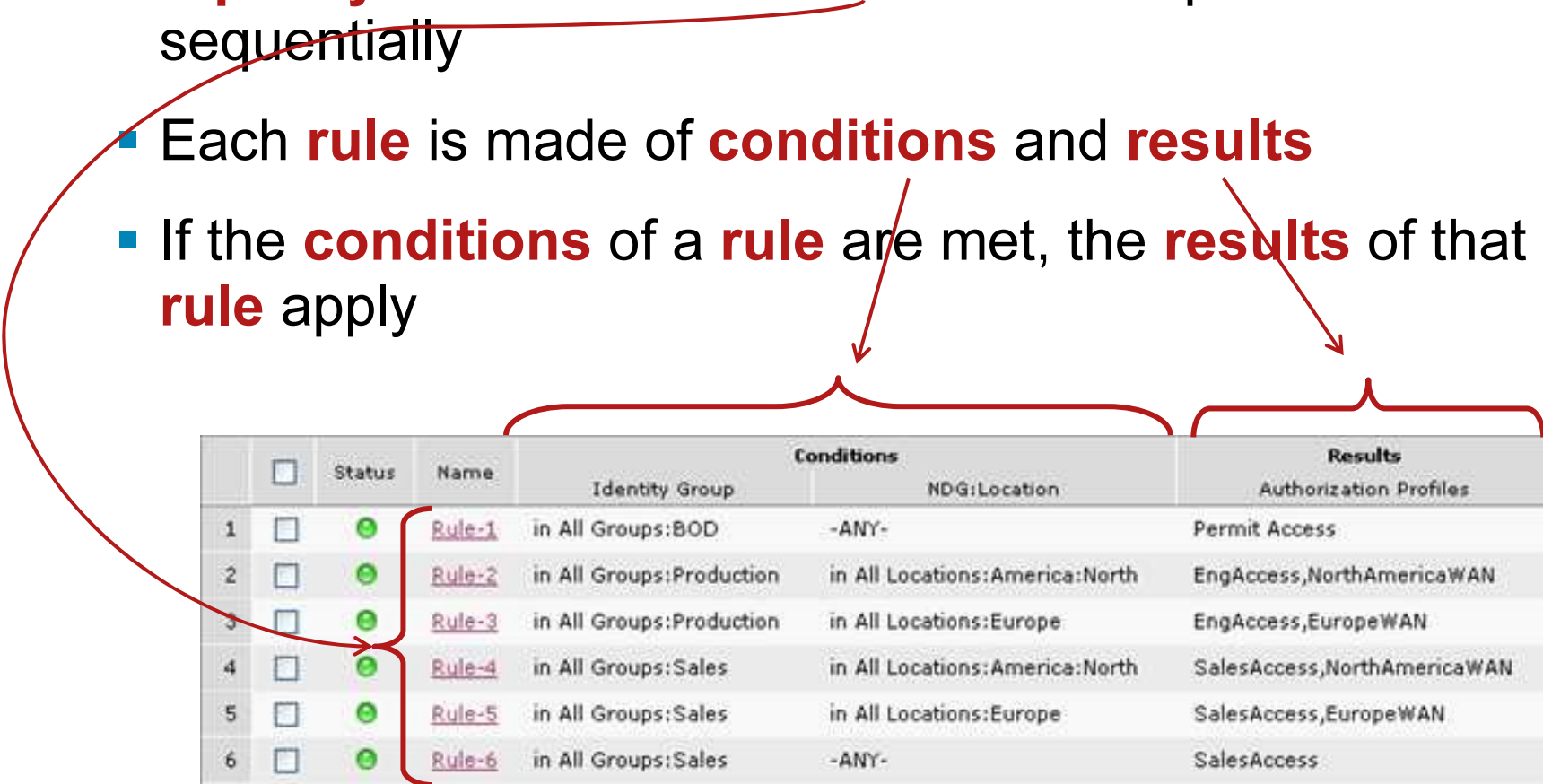
Downloadable ACL Name: Static Value PERMIT-ANY

IOS ACL Filter ID: Not in Use

Proxy ACL: Not in Use

# Policy Table – Structure

- A **policy** is a collection of **rules** that are processed sequentially
- Each **rule** is made of **conditions** and **results**
- If the **conditions** of a **rule** are met, the **results** of that **rule** apply



	<input type="checkbox"/>	Status	Name	Identity Group	Conditions	Results
					NDG:Location	Authorization Profiles
1	<input type="checkbox"/>	●	<a href="#">Rule-1</a>	in All Groups:BOD	-ANY-	Permit Access
2	<input type="checkbox"/>	●	<a href="#">Rule-2</a>	in All Groups:Production	in All Locations:America:North	EngAccess,NorthAmericaWAN
3	<input type="checkbox"/>	●	<a href="#">Rule-3</a>	in All Groups:Production	in All Locations:Europe	EngAccess,EuropeWAN
4	<input type="checkbox"/>	●	<a href="#">Rule-4</a>	in All Groups:Sales	in All Locations:America:North	SalesAccess,NorthAmericaWAN
5	<input type="checkbox"/>	●	<a href="#">Rule-5</a>	in All Groups:Sales	in All Locations:Europe	SalesAccess,EuropeWAN
6	<input type="checkbox"/>	●	<a href="#">Rule-6</a>	in All Groups:Sales	-ANY-	SalesAccess
**	<input type="checkbox"/>		<a href="#">Default</a>	Default - if no rule is defined in the table or none of the above enabled rules are matched.		DenyAccess

# ACS 5.0 Monitoring & Reports Component

- Integrated advanced monitoring, reporting & troubleshooting capabilities for maximum control and visibility
  - Easy to use GUI
  - Flexible presentation tools
- Consolidation of data across an ACS deployment

The screenshot displays the Cisco Secure ACS 5.0 Monitoring and Reports Dashboard. The interface includes a sidebar with navigation options such as Dashboard, Alarms, Reports, and Troubleshooting. The main content area is titled 'Monitoring and Reports: Dashboard' and features a 'Monitoring' tab. A notification states 'Dashboard refreshes every 15 seconds'. A 'Protocol' dropdown is set to 'RADIUS'.

**Recent Alarms**

Severity	Time	Name	Cause	Status
Info	Sun Nov 30 04:02:01	<a href="#">System Alarm [Database Purging]</a>	Database Purge finished	New
Info	Sun Nov 30 04:02:00	<a href="#">System Alarm [Database Purging]</a>	Database Start Purging	New
Warning	Sun Nov 02 01:45:00	<a href="#">ACS - System Health</a>	Alarm caused by ACS - System Health threshold	New
Warning	Sun Nov 02 01:45:00	<a href="#">ACS - AAA Health</a>	Alarm caused by ACS - AAA Health threshold	New

**ACS Health Status**

ACS Instance	System Health	AAA Health
<a href="#">id-alpha-sjc3</a>	Healthy	Healthy

Legend: Critical (Red), Warning (Yellow), Healthy (Green), Status not available (Yellow triangle with exclamation mark).

**Identity Store Authentication Status**

Identity Store	Today	Day of Week Average	Daily Average	Top 3 Failure Reasons
<a href="#">AD1</a>	12 Pass 0 Fail	7 Pass 0 Fail	7 Pass 0 Fail	
<a href="#">Internal Hosts</a>	76 Pass 0 Fail	38 Pass 0 Fail	43 Pass 0 Fail	
<a href="#">Internal Users</a>	0 Pass 0 Fail	0 Pass 0 Fail	0 Pass 0 Fail	
<a href="#">NAC Profiler</a>	0 Pass 0 Fail	0 Pass 0 Fail	0 Pass 0 Fail	



# Services in Action (ACSView)

**Cisco Secure ACS** acsadmin | ACS5-1 | Mor

**Monitoring and Reports**

- Dashboard
- Alarms
  - Inbox
  - Thresholds
- Reports
  - Favorites
  - Shared
  - Catalog
    - AAA Protocol
    - Access Service
    - ACS Instance
    - Endpoint
    - Failure Reason
    - Network Device
    - Session Directory
    - User
- Troubleshooting
  - Connectivity Tests
  - ACS Support Bundle

Showing Page 1 of 3 | [First](#) [Prev](#) **Next** [Last](#) | Goto Page:  **Go**

AAA Protocol > RADIUS Authentication

Authentication Status : Pass  
Date : February 23, 2009

Generated on February 23, 2009 8:50:14 PM UTC

[Reload](#)

✓=Pass ✗=Fail ⓘ=Click for details

Logged At	Status	Details	Username	Calling Station ID	Authentication Method	EAP Authentication	Selected Authorization Profiles	NAS IP Address	NAS Port	Access Service	Identity Store
8:48:22.630 PM	✓	ⓘ	host/imac-mcs-9	00-14-5E-66-66-66	MSCHAPV2	EAP-MSCHAPv2	Machine	10.100.10.2	50301	<a href="#">802.1X Access Service</a>	AD1
8:48:14.120 PM	✓	ⓘ	Administrator	00-14-5E-66-66-66	MSCHAPV2	EAP-MSCHAPv2	Employee	10.100.10.2	50301	<a href="#">802.1X Access Service</a>	AD1
8:43:26.570 PM	✓	ⓘ	Administrator	00-14-5E-95-D6-CC	x509_PKI	EAP-TLS	Employee	10.100.10.5	50113	<a href="#">802.1X Access Service</a>	
8:43:08.556 PM	✓	ⓘ	imac-mcs-11.identity.com	00-14-5E-95-D6-CC	x509_PKI	EAP-TLS	Machine	10.100.10.5	50113	<a href="#">802.1X Access Service</a>	
8:43:07.270 PM	✓	ⓘ	imac-mcs-11.identity.com	00-14-5E-95-D6-CC	x509_PKI	EAP-TLS	Machine	10.100.10.5	50113	<a href="#">802.1X Access Service</a>	
8:40:09.560 PM	✓	ⓘ	00-14-5E-95-D6-CC	00-14-5E-95-D6-CC	Lookup		Employee	10.100.10.5	50113	<a href="#">MAB Access Service</a>	NAC Profiler
8:39:02.176 PM	✓	ⓘ	imac-mcs-11.identity.com	00-14-5E-95-D6-CC	x509_PKI	EAP-TLS	Machine	10.100.10.5	50113	<a href="#">802.1X Access Service</a>	
8:30:10.246 PM	✓	ⓘ	00-1E-4A-A9-00-A8	00-1E-4A-A9-00-A8	Lookup		Phone	10.100.10.4	50248	<a href="#">MAB Access Service</a>	NAC Profiler
8:29:19.190 PM	✓	ⓘ	IDENTITY\Administrator	00-18-F8-09-CF-C4	MSCHAPV2	EAP-MSCHAPv2	Employee	10.100.10.4	50247	<a href="#">802.1X Access Service</a>	AD1
8:29:17.113 PM	✓	ⓘ	00-18-BA-C7-BC-CC	00-18-BA-C7-BC-CC	Lookup		Phone	10.100.10.4	50247	<a href="#">MAB Access Service</a>	NAC Profiler
8:29:01.093 PM	✓	ⓘ	00-18-F8-09-CF-C4	00-18-F8-09-CF-C4	Lookup		Employee	10.100.10.4	50247	<a href="#">MAB Access Service</a>	NAC Profiler
8:25:34.183 PM	✓	ⓘ	imac-mcs-11.identity.com	00-14-5E-95-D6-CC	x509_PKI	EAP-TLS	Employee	10.100.10.5	50113	<a href="#">802.1X Access Service</a>	
8:20:05.890 PM	✓	ⓘ	00-14-5E-66-66-66	00-14-5E-66-66-66	Lookup		Guest	10.100.10.2	50301	<a href="#">MAB Access Service</a>	NAC Profiler

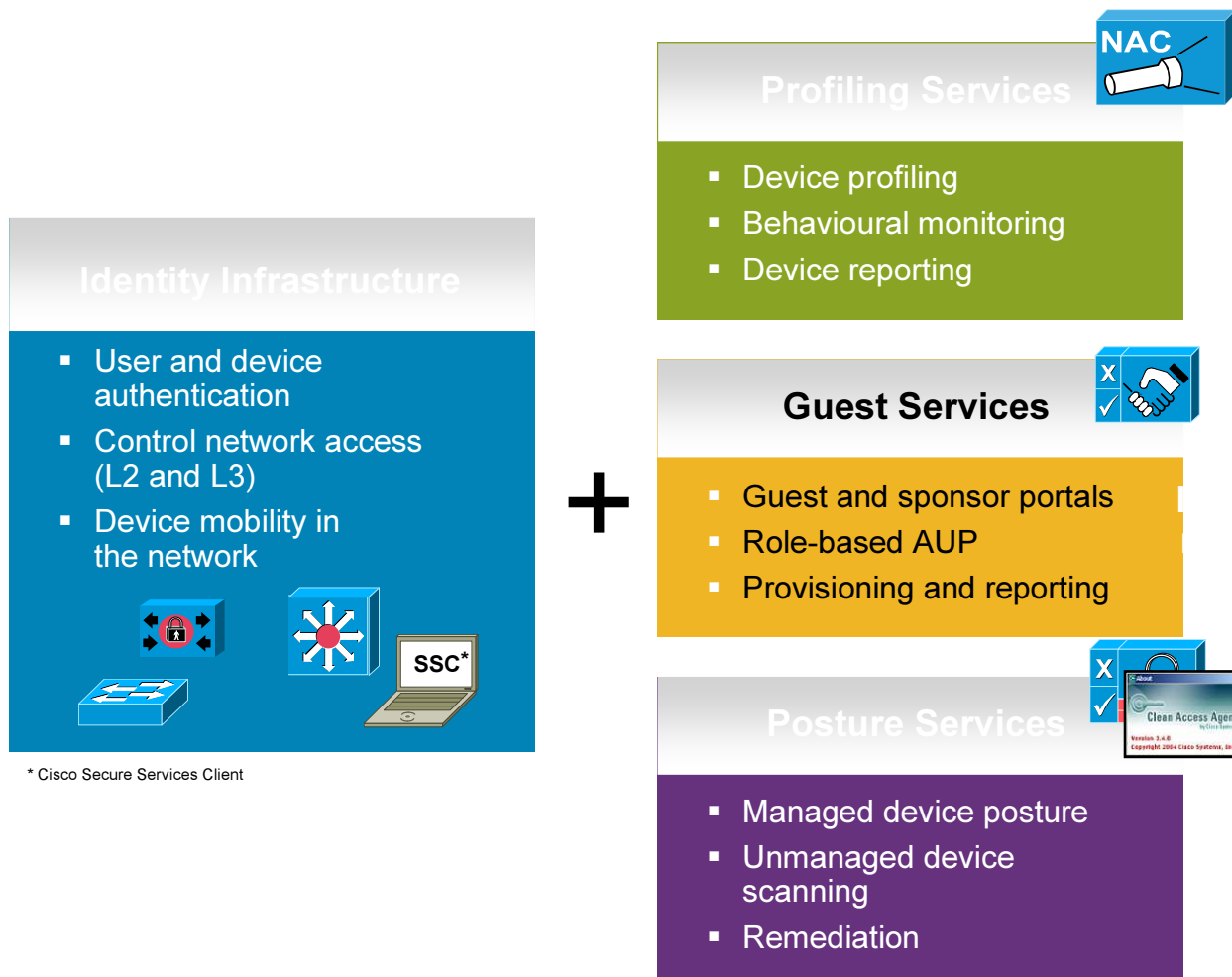


# Agenda

- The changing Business
- Identity deployment in phases
  - Introduce 802.1x without business disruption
  - Non 802.1x devices and guests
  - Policy management
  - **Posturing**
- Recent Cisco Security Updates
  - Botnet Filtering
  - Collaborative IPS
  - New Safe architecture



# Identity-based network access



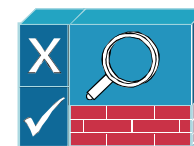
# Cisco NAC Key Components

## NAC Manager and Server (Required)



### NAC Manager

Centralized management, configuration, reporting, and policy store



### NAC Server

Posture, services and enforcement

## NAC Profiler, Guest Server and ACS (Optional)



### NAC Profiler

Profiles unmanaged devices



### NAC Guest Server

Full-featured guest provisioning server



### ACS Server

Access policy system for 802.1x termination

## Endpoint Components (Optional)



### NAC Agent

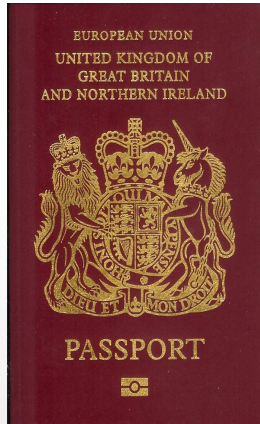
No-cost client: Persistent, dissolvable, or web



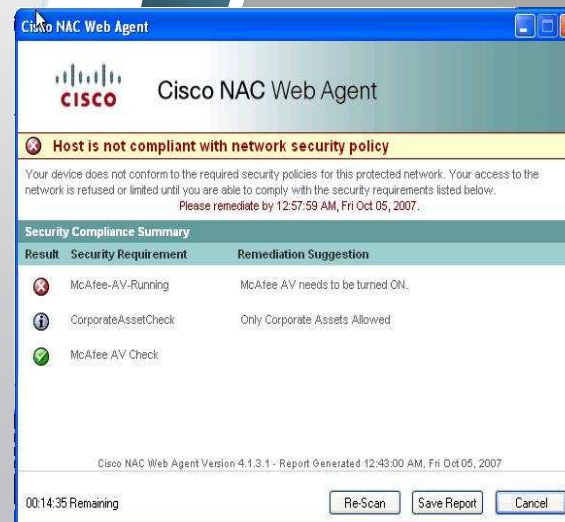
### 802.1x Supplicant

CSSC or Vista embedded supplicant

# Role-Based Access and Device Compliance



List of Roles	New Role	Traffic Control	Bandwidth	
Role Name	IPSec	Roam	VLAN	Description
Unauthenticated Role	deny	deny		Role for unauthenticated users
Temporary Role	deny	deny		Role for users to download requirements
Quarantine Role	deny	deny		Role for quarantined users
Allow All	deny	deny		Full Access
Guest Access	deny	deny	:666	guest privileges
consultant access	deny	deny	:55	consultant privileges



# Cisco NAC Service

## Automated Policy Updates

### Automated Cisco Rulesets

Simplify support for over 350+ security and management applications



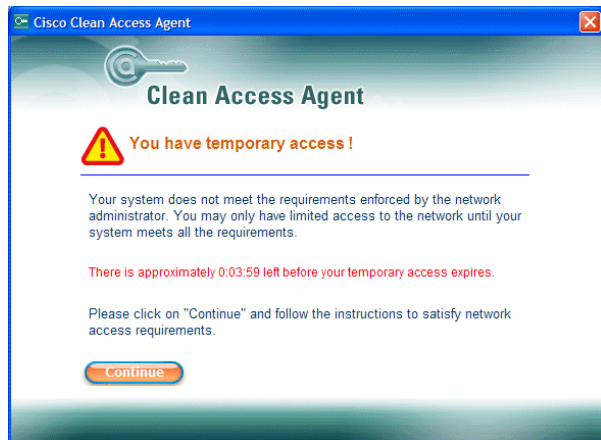
AutoUpdates Hotfixes,  
Service Packs  
(direct to WSUS Server)



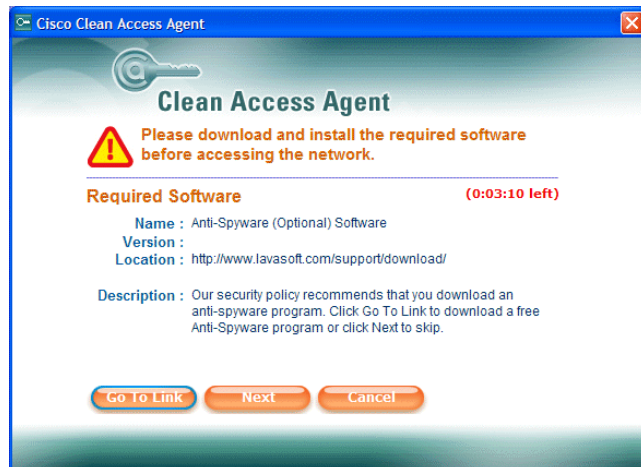
Cisco NAC Manager

# NAC Agent Options

## NAC Agent



Remediate



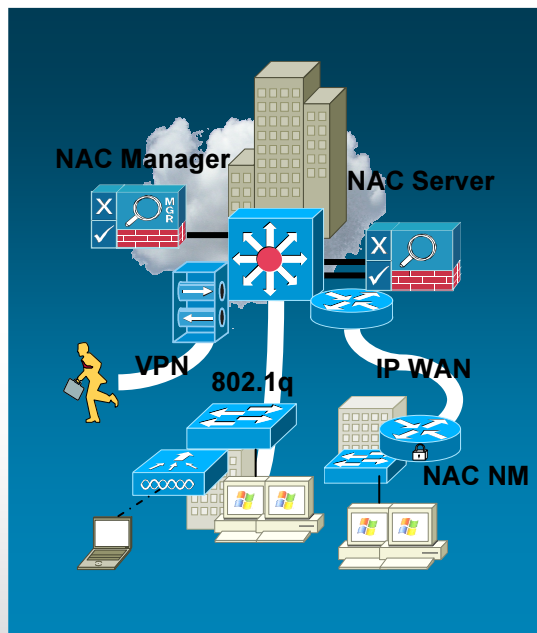
## Web Agent for Contractors & Guests





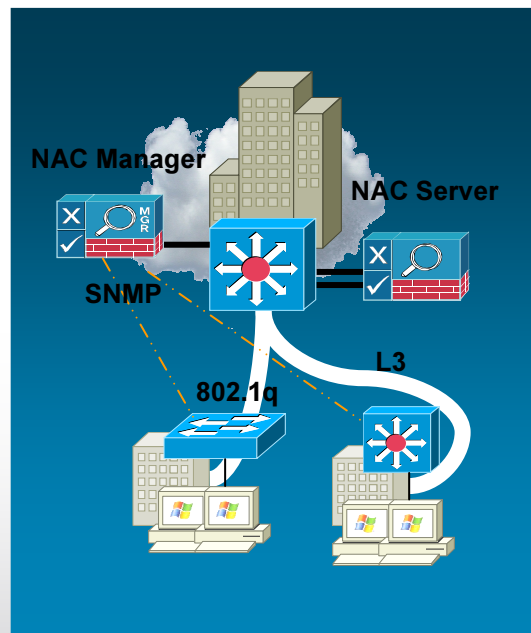
# How Cisco NAC works – design options

## In-Band



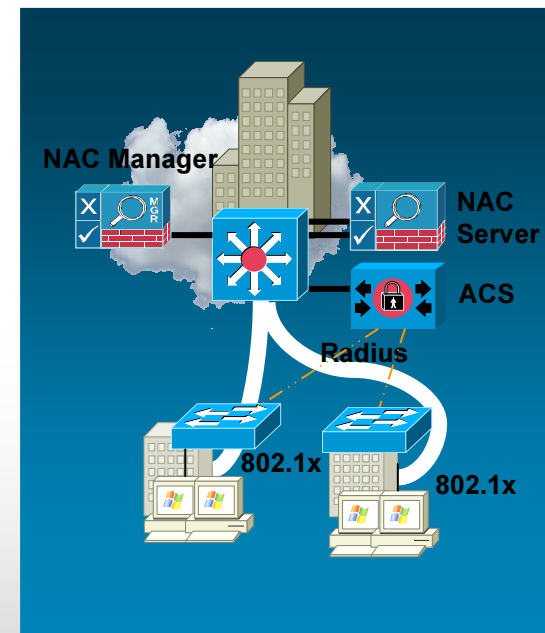
- VPN, wireless, campus, and remote LANs
- Enforcement via Appliance

## Out-of-Band



- Optimized for Cisco campus LANs (L2, L3)
- SNMP as control plane

## RADIUS\*

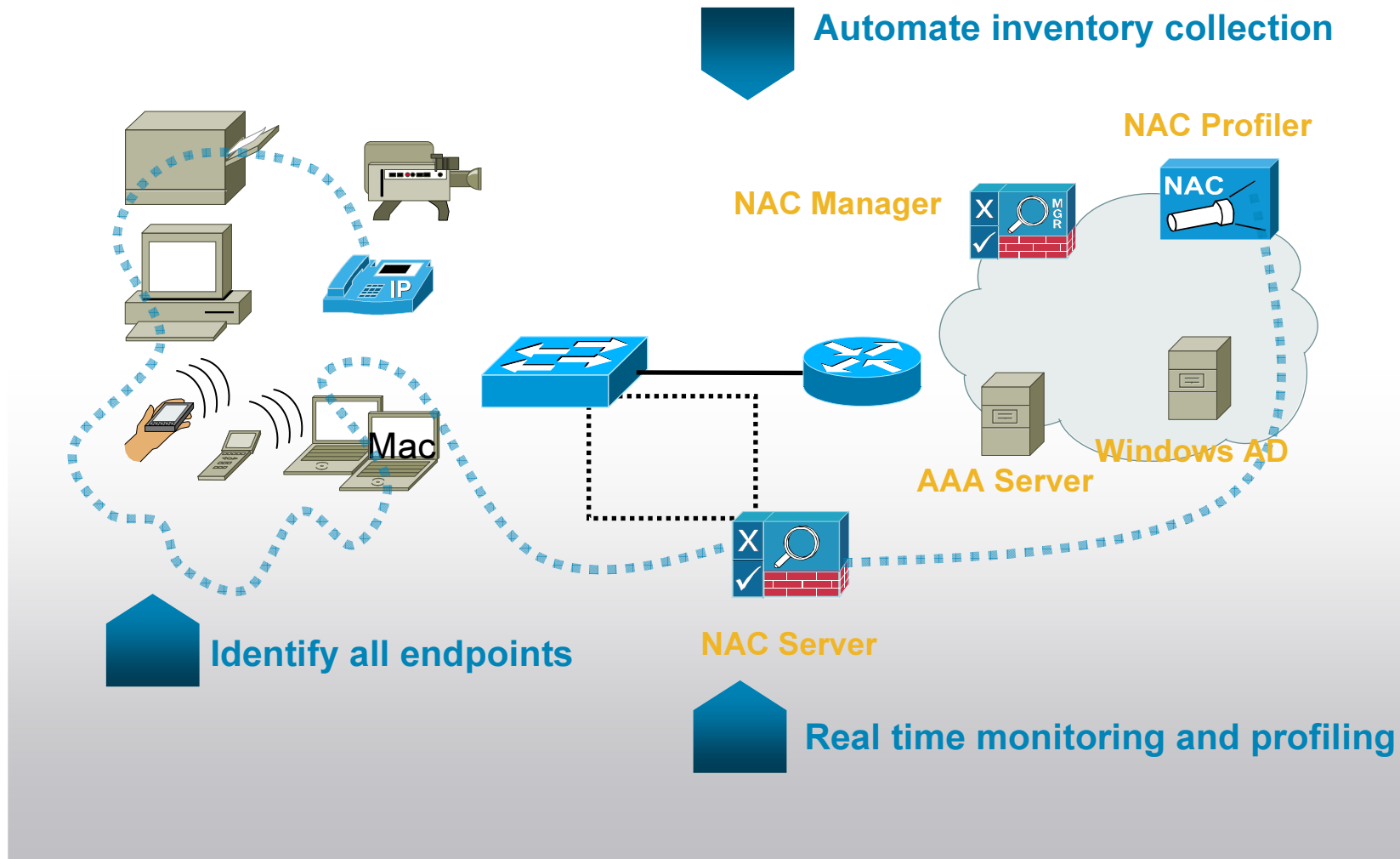


- Optimized for Cisco campus LANs (802.1x)
- RADIUS as control plane

**\*limited availability program for now – check with account team for more info.**

# Device Profiling

Cisco NAC Profiler: Visibility, Intelligence, and Automation



# NAC Guest Server

## PROVISIONING

### Create Guest Accounts



Create a single Guest Account

Create multiple Guest Accounts  
by Importing a CSV file

### Manage Guest Accounts



View, edit or suspend your  
Guest Accounts

Manage batches of accounts  
you have created

## MANAGEMENT

## NOTIFICATION

### Give Accounts to Guests



Print Account and Access Details

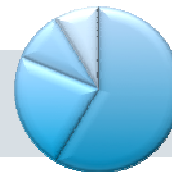


Send Account Details via Email



Send Account Details via SMS

### Report on Guests



View audit reports on individual  
Guest accounts

Display Management reports on  
Guest Access

## REPORTING

# NAC Guest Access with WIRED 802.1X enabled network

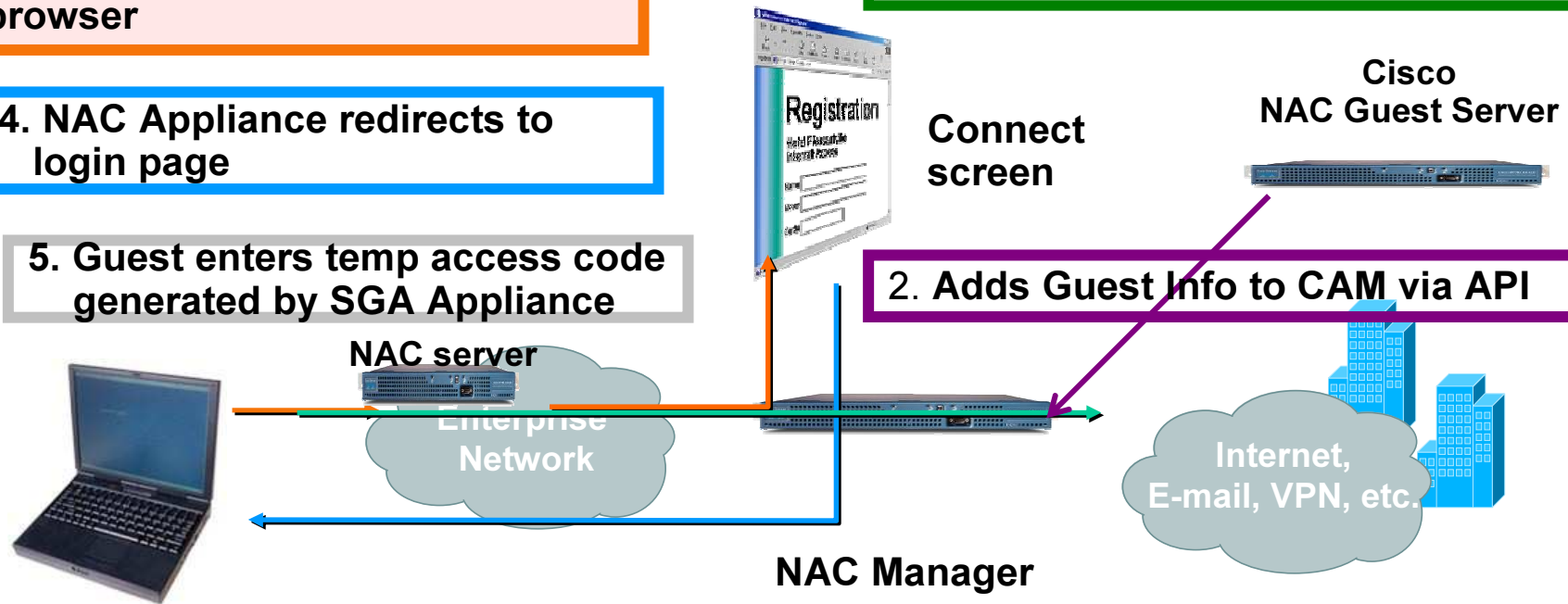
3. Guest fail into the GUEST VLAN, get an IP and starts Web browser

4. NAC Appliance redirects to login page

5. Guest enters temp access code generated by SGA Appliance

1. Employee creates account for Guest

2. Adds Guest Info to CAM via API



6. NAC Appliance put the user in the Specific Role

# Guest Accounts: Creation and Monitoring

The screenshot displays the Cisco NAC Guest Server web interface. The left sidebar contains navigation links: Home, Getting Started, My Settings, Create Accounts (with sub-links for Create Guest Account, Multiple Accounts, Import Accounts, and Random Accounts), and Summary Reports (with sub-links for Sponsors Activity Report and Access Report). The main content area is divided into two sections. The top section, titled 'Create Guest Account', contains a form for creating a new user account. The bottom section, titled 'Cisco NAC Guest Server Reporting', displays a table of existing accounts. Two blue callout boxes provide instructions: '1. Enter user details' points to the form fields, and '2. Specify start and end times' points to the 'Start Time' and 'End Time' columns in the reporting table. A third blue callout box, 'Send account information via print-out, email, or SMS', points to the action icons in the table. A fourth blue callout box, 'Account Created', points to a confirmation message on the right. A fifth blue callout box, 'Account Management', points to the action icons in the table. A sixth blue callout box, 'Guest Information', points to the 'First Name' and 'Last Name' columns. A seventh blue callout box, 'Sponsor Information', points to the 'Created By' column. A small inset image of a mobile phone is visible on the right side of the interface.

**1. Enter user details**

**2. Specify start and end times**

**Send account information via print-out, email, or SMS**

**Account Created**

**Account Management**

**Guest Information**

**Sponsor Information**

Created By	Username	Password	First Name	Last Name	Email	Status	Start Time	End Time	
duarte	lcarter@polycyapp.com	-sY5Nmzb	John	Carter	jcarter@polycyapp.com	Suspended	12-Jan-2009 7:42 AM America/Los_Angeles	12-Jan-2009 11:59 PM America/Los_Angeles	
mark	rooney@manutd.com	*ckl0IMT	Wayne	Rooney	rooney@manutd.com	Active	12-Jan-2009 7:41 AM America/Los_Angeles	12-Jan-2009 11:59 PM America/Los_Angeles	
niail	jsmith@mycustomer.com	ZYy:X9PW	John	Smith	jsmith@mycustomer.com	Inactive	12-Jan-2009 9:00 AM America/Los_Angeles	12-Jan-2009 5:30 PM America/Los_Angeles	
niail	jsmith@mycustomer.com	GpOCK8*	john	smith	jsmith@mycustomer.com	Expired	10-Jan-2009 5:52 PM America/Los_Angeles	10-Jan-2009 11:59 PM America/Los_Angeles	

# Cisco Identity End-to-End

Client	IP Telephony	Campus Access	Servers
<p><b>Cisco Identity</b></p> <ul style="list-style-type: none"><li>• Secure Services Client</li></ul> <p>Cisco NAC</p> <ul style="list-style-type: none"><li>• Clean Access Agent</li></ul> 	<p><b>Cisco</b></p> <ul style="list-style-type: none"><li>• IP Phones</li></ul> 	<p><b>Cisco LAN Switches</b></p> <ul style="list-style-type: none"><li>• Catalyst Switch Portfolio</li></ul> <p>Cisco WLAN</p> <ul style="list-style-type: none"><li>• Cisco APs &amp; Controllers</li></ul> 	<p><b>Cisco RADIUS</b></p> <ul style="list-style-type: none"><li>• Cisco ACS 5.0</li></ul> <p>NAC</p> <ul style="list-style-type: none"><li>• CAM/CAS/Profiler/Guest</li></ul> 

← **Solution Expertise** →

← **Single Vendor Support** →

← **Cisco Stability** →



# Summary

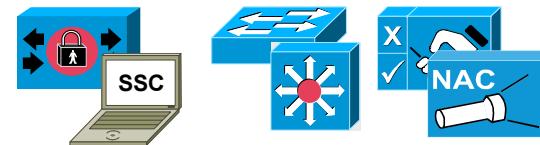
## 802.1X functions

**Switch-based authenticated LAN access for users & devices**

**Provides 802.1x authentication, guest, and profiling services with NAC Guest and Profiler components**

**Deploys in 802.1x enabled LAN**

**Can be used with NAC Appliance**



**For all of the features described today, please consider  
3K:12.2(50)SE, 4K: 12.2(50)SG and 6K: 12.2(33)SXI**

## Network Admission Control

**Appliance-based NAC solution**



**Provides authentication, posture, guest, and profiling services**

**Deploys in VPN, Wireless, and LAN, with or without 802.1X**

# Agenda

- The changing Business
- Identity deployment in phases
  - Introduce 802.1x without business disruption
  - Non 802.1x devices and guests
  - Policy management
  - Posturing
- Recent Cisco Security Updates
  - Botnet Filtering
  - Collaborative IPS
  - New Safe architecture



# Announced Global Correlation for Cisco ASA 5500 Series and Cisco IPS

## Cisco ASA 5500 Series Adaptive Security Appliances



### ASA Software Version 8.2

- Botnet Traffic Filter
- Detect infected clients through “phone home” connections

## Cisco Intrusion Prevention Systems



### IPS Software Version 7.0

- Accurate protection against broad range of threats
- Twice the coverage
- IPS Reputation Filtering with Global Correlation

# Cisco Security Intelligence Operations

Security Infrastructure That Dynamically Protect Against the Latest Threats Through:

Cisco SensorBase

The Most Comprehensive  
Vulnerability and Sender  
Reputation Database

Threat Operations  
Center

A Global Team of  
Security Researchers  
and Analysts

Analytics and  
Algorithms

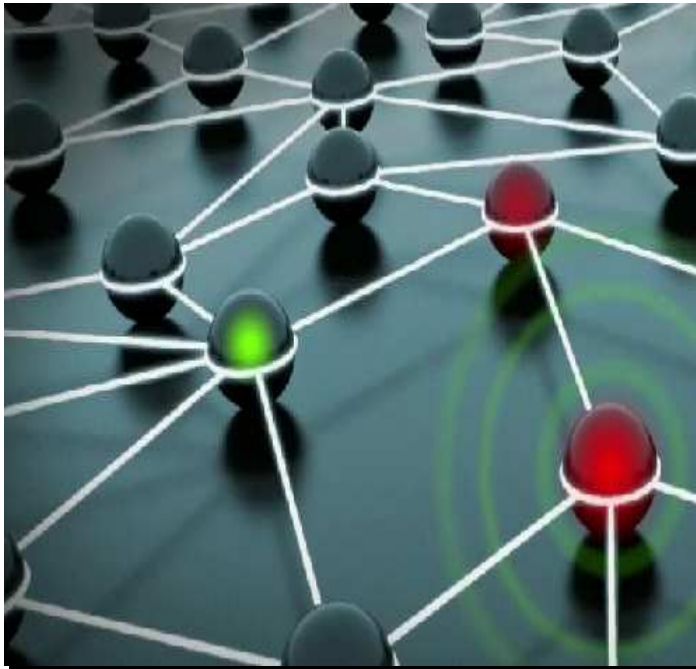
Automatic Updates  
and Best Practices

## Powered by Global Correlation



# Cisco IPS 7.0

## Network IPS to Global IPS



- **Coverage**  
Twice the effectiveness of signature-only IPS
- **Accuracy**  
Reputation analysis decreases false positives
- **Timeliness**  
100x faster than traditional signature-only methods

IPS Reputation Filtering powered by Global Correlation

# Detecting Client Infections

## Botnet Traffic Filters on ASA 5500 Series

- **Monitors malware traffic**

- Scans all traffic, ports & protocols
- Detects infected clients by tracking rogue “phone home” traffic

- **Highly accurate**

- Blocks 100,000s of malware connections per week
- Automatic rule updates



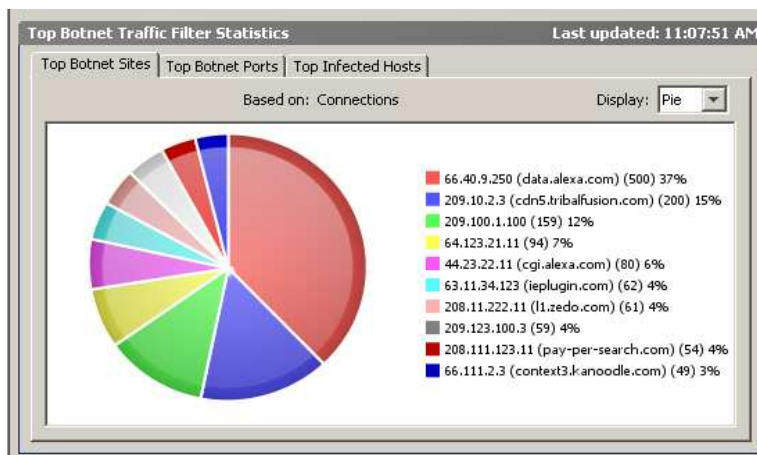
Command and Control



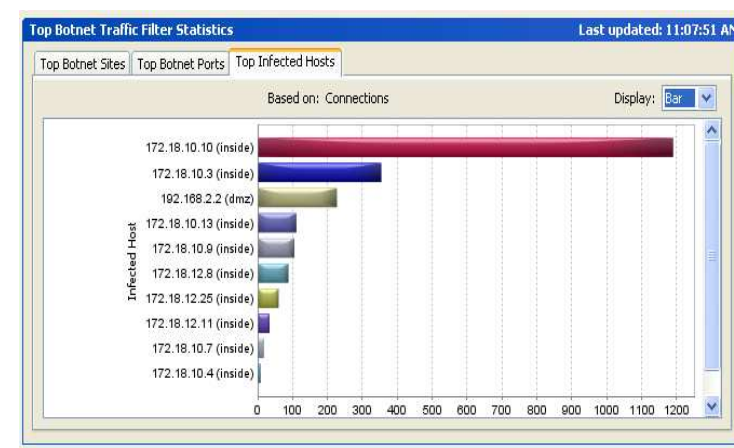
Cisco ASA



Infected Clients



Live Dashboard



Integrated Reporting



# Details: IPS for ASA 5505

## Dynamic Threat Protection for SOHO/SMB

- Extend Cisco ASA IPS solution into SMB market
- Address critical PCI & HIPAA compliance mandates
- Deliver leading SOHO/SMB IPS Performance



# Cisco SAFE

## Tested and Validated End-to-End Security Design and Technical Implementation Guide

- **Cisco Security Control Framework**

- Enables ongoing solution development

- Covers network PINs and cross-network solutions

- Integrates comprehensive services to support solution lifecycle

- **Benefits**

- Complements and validates software-defined network (SDN) messaging

- Eases transition from concept to design and implementation

- Offers Cisco® SAFE designs free of charge

- Enables simple updating and expansion through modular design



# Resources

- IBNS Resources:

<http://www.cisco.com/go/ibns>

- NAC Resources

<http://www.cisco.com/go/nac/appliance>

- ACS Resources

<http://www.cisco.com/go/acs>

[ACS 5.0 Policy model overview](#)

- SAFE architecture

<http://www.cisco.com/go/safe>