

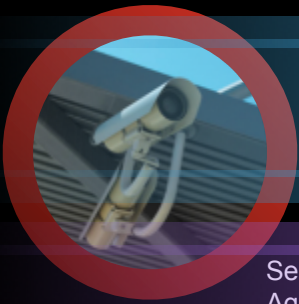
Cisco TrustSec

Goran Peteh

Enterprise Systems Engineer

gopeteh@cisco.com

Today's Dynamic Business Environment



GLOBAL WORK FORCE

Employees, Contractors, Phones, Printers

Vicky Sanchez
Employee
Marketing
Wireline
3 p.m.



Rossi Barks
Employee
HR
Wireline
11 a.m.



Laptop
Managed asset
Main Laboratory
11 a.m.

Security Camera G/W
Agentless asset
MAC: F5 AB 8B 65 00 D4

SENSITIVE RESOURCES

Network, Devices & Applications



MULTIPLE ACCESS METHODS

From different devices, location & time

Francois Didier
Employee
CEO
Remote Access
10 p.m.



Bill Graves
Employee
R&D
Wireless
2 p.m.



Francois Didier
Consultant
HQ - Strategy
Remote Access
6 p.m.

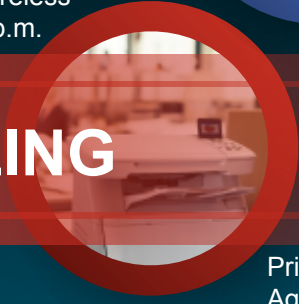


Sergei Balazov
Contractor
IT
Wireline
10 a.m.

ALL NEED CONTROLLING



IP Phone G/W
Managed asset
Finance dept.
12:00 p.m.



Printer
Agentless asset
MAC: B2 CF 81 A4 02 D7

Importance of Policy



Protecting Collaboration

As network boundaries disappear, you need to control access to resources

Regulatory Compliance

Meeting stricter corporate, government, and regulatory compliance requirements



Increasing Security

Enforcing policy compliance on users and devices critical to information security

Cisco TrustSec™

Helps customers secure their networks,
data and resources with

- policy-based access control
- identity-aware networking
- data integrity and confidentiality



Key Cisco TrustSec™ Functions



Policy-based Access Control

- Consistent policy for users and devices
- Distributed enforcement
- Topology- independent access control via Security Group Access Control (SGAC)



Identity-aware Networking

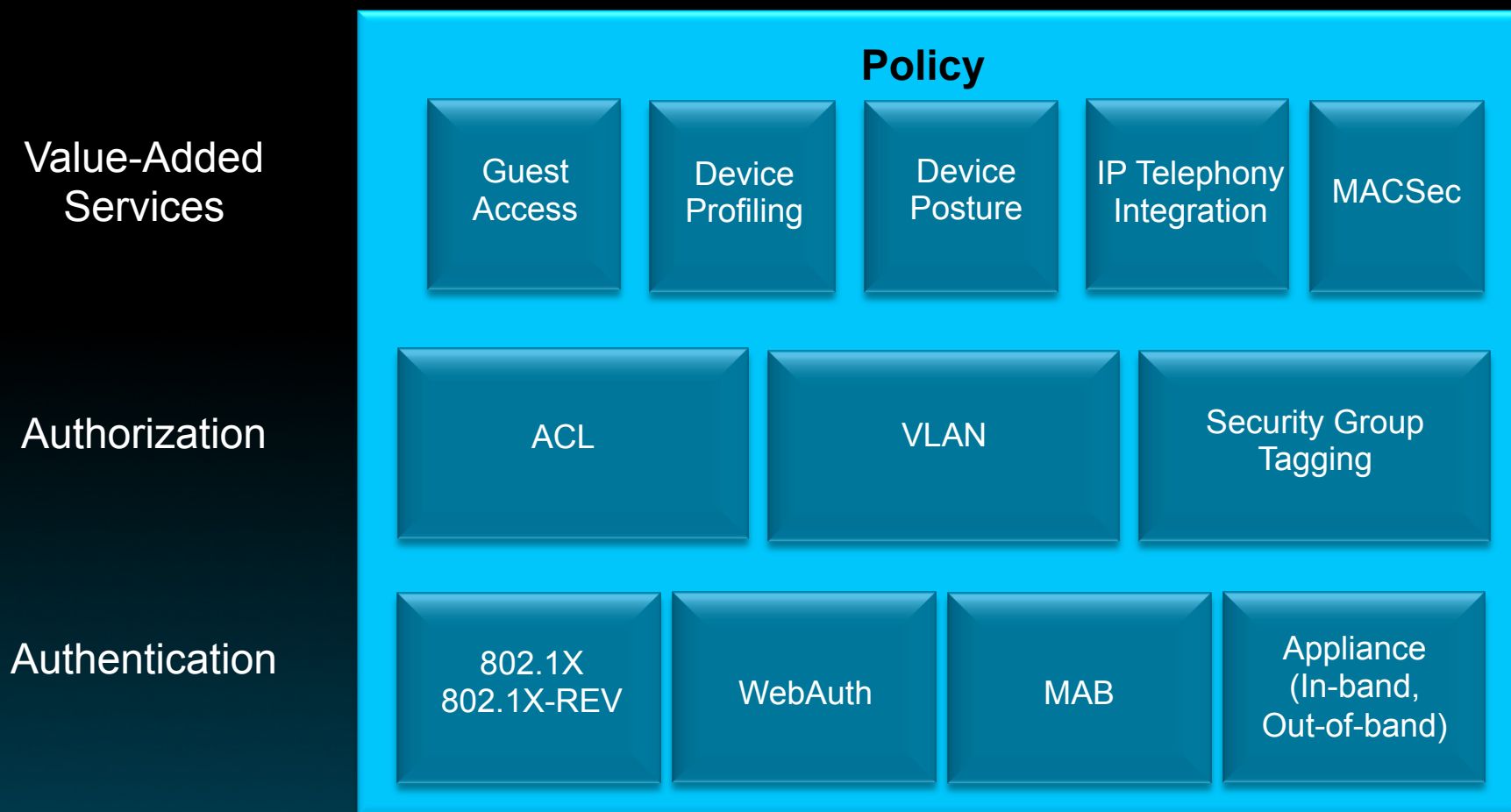
- Controls based on user/ device identity and attributes (time, location, access methods)
- Support for Cisco Medianet and QoS for business-critical applications associated with users in specific roles



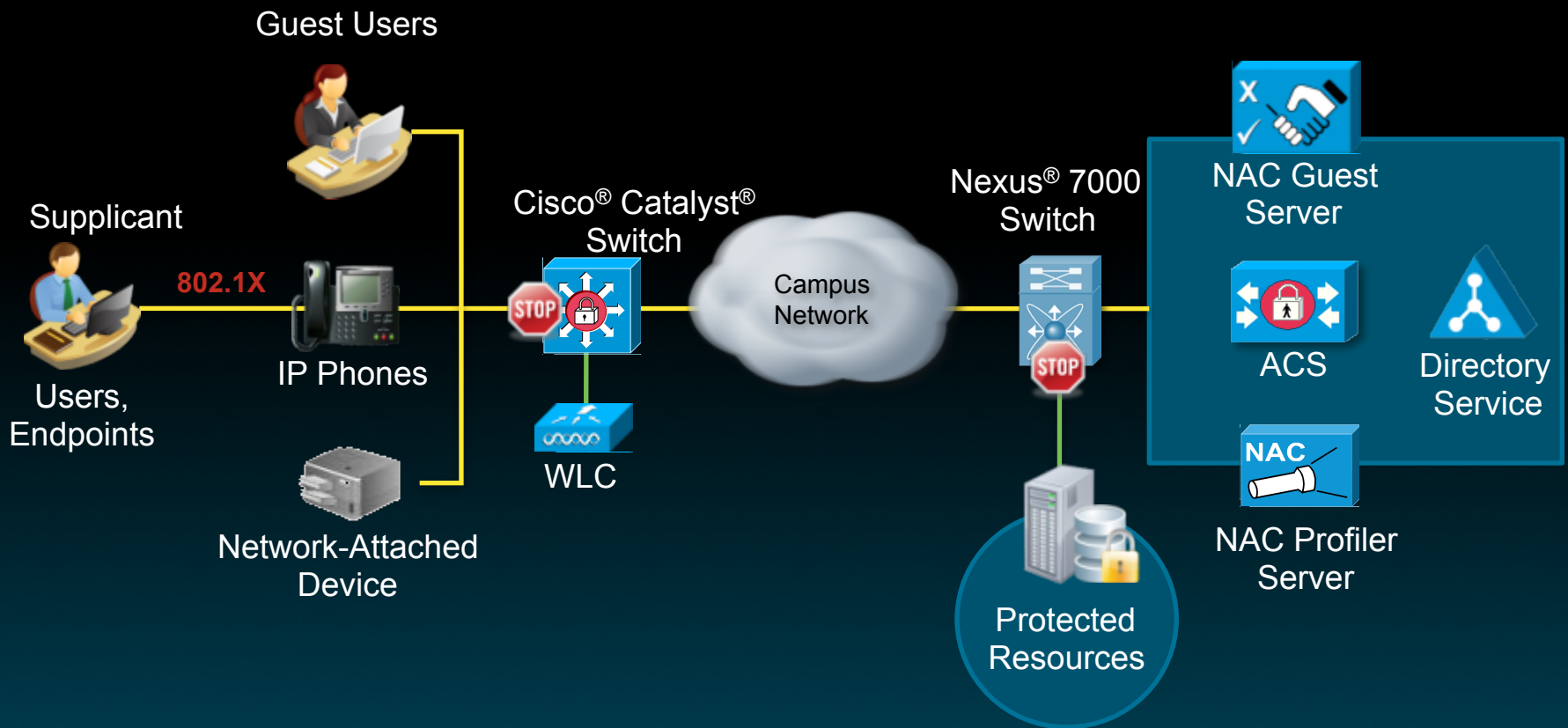
Data Integrity And Confidentiality

- Data confidentiality and integrity by securing data path in the switching environment
- IEEE 802.1AE standard based encryption with visibility into data stream to support critical security applications such as firewalls, IPS, and content inspection

Cisco TrustSec™ Architecture

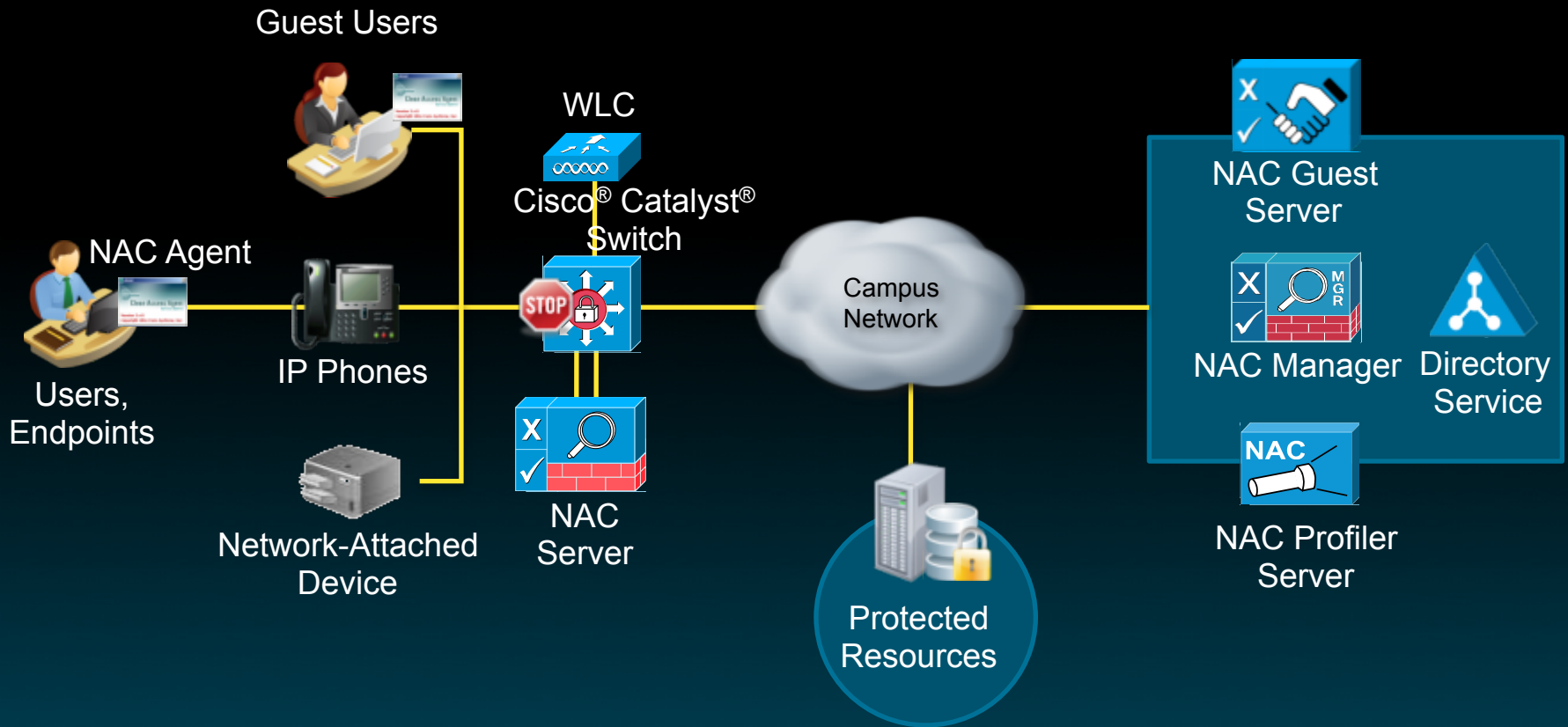


Cisco TrustSec™ 802.1X-Based Network Access Control



Control Plane: **RADIUS**

Cisco TrustSec™ Appliance-Based Network Access Control



Control Plane: **SNMP**

Comparing 802.1x Infrastructure with NAC Appliance Solution



	Cisco 802.1x Solution	NAC Appliance Solution
Is an agent or supplicant required?	Yes for 802.1X authentication. No for Web authentication	Agent required for SSO and Posture. Not required for WEB auth.
Posture assessment	No	Yes
Industry standard	Yes	No
Support for non 802.1X devices	MAC authentication bypass	Yes
Support for agent-less devices	Yes: Profiler	Yes: Profiler
Support for machine authentication	Yes	No
Support for guest	Yes	Yes
Control plane	RADIUS	SNMP

802.1X-based Network Access Control



Cisco TrustSec™

Cisco 802.1X-based Authentication

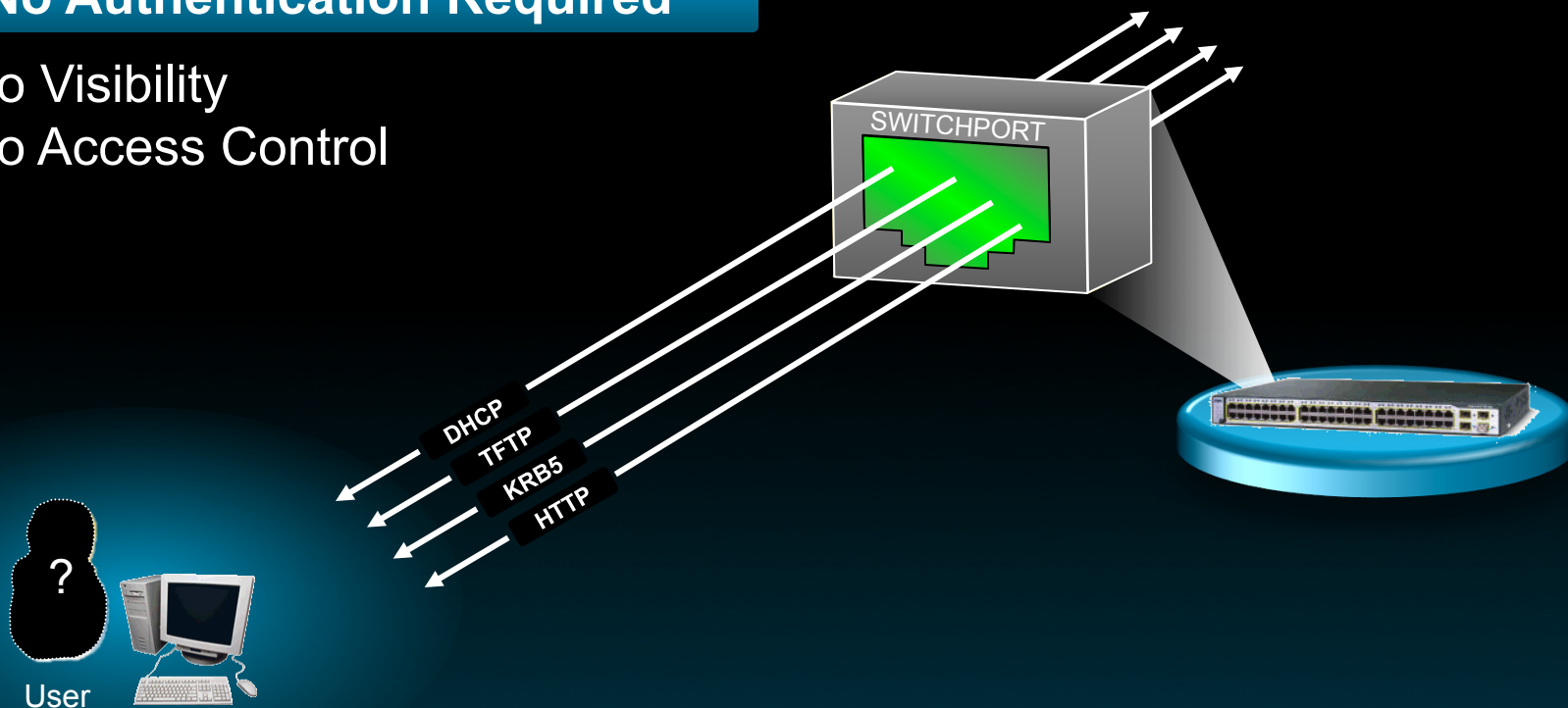
- IEEE802.1X User / Device Authentication
Standards-based port-based authentication provides strong Layer 2 authentication methods for user and device.
- MAC Authentication Bypass
Non-802.1X device can be authenticated using MAB (MAC address-based authentication).
- WEB Authentication
Guest / visitor can use web-based authentication for temporal network access.



Network Port without 802.1X

No Authentication Required

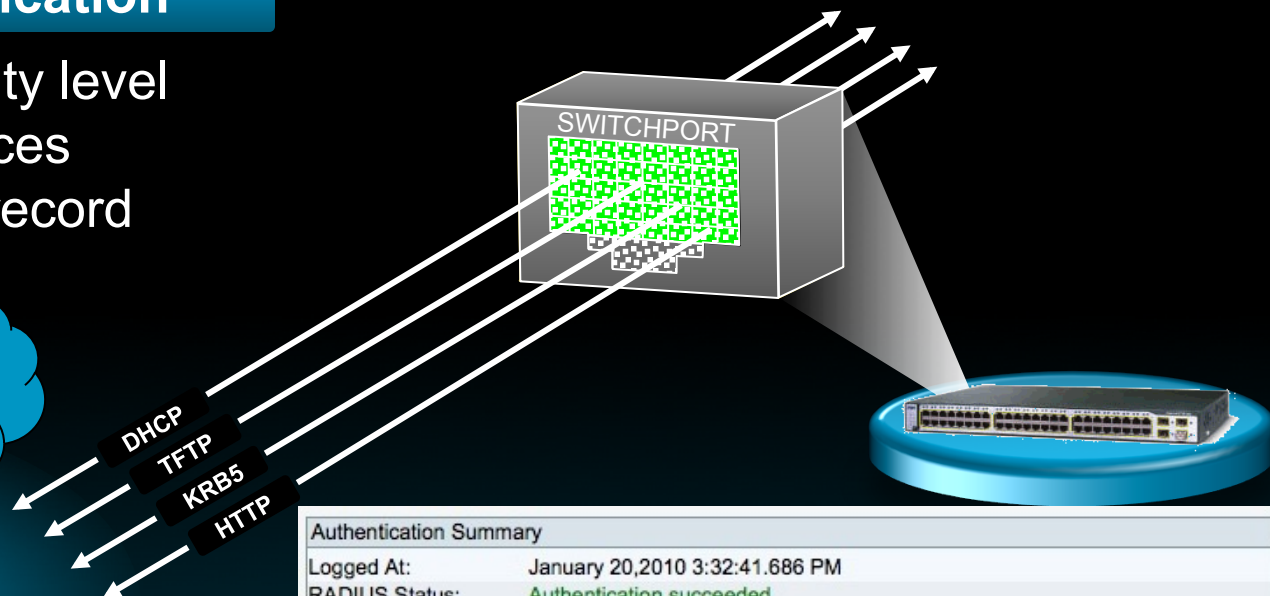
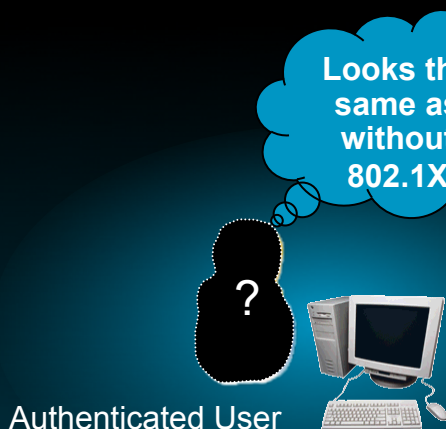
- No Visibility
- No Access Control



Network Port with 802.1X

After Authentication

- Increases security level
- Provisions services
- Leaves access record



Authentication Summary	
Logged At:	January 20,2010 3:32:41.686 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	hadmin
MAC/IP Address:	00-14-5E-42-9E-C3
Network Device:	CTS6K-AS : 10.1.3.2 : FastEthernet2/2
Access Service:	802.1X
Identity Store:	AD1
Authorization Profiles:	Permit Access
CTS Security Group:	HR Administrator
Authentication Method:	PEAP(EAP-MSCHAPv2)

Cisco TrustSec™

Flexible Authentication

- Flexible authentication allows:
- Three different authentication methods:
 - 802.1X for supplicant-capable devices
 - MAC Authentication Bypass (MAB)
 - Web Authentication (typical user ID / password pair)
- Provisioned per port
- In any combination
- In any order
- This reduces network OpEx because:
 - End users can move devices without network admin labor.
 - During transition from web auth to 802.1X, ports do not need to be reconfigured since each desktop/laptop is configured for 802.1X.



How Flexible Authentication Works

Any combination
Any sequence
On single port

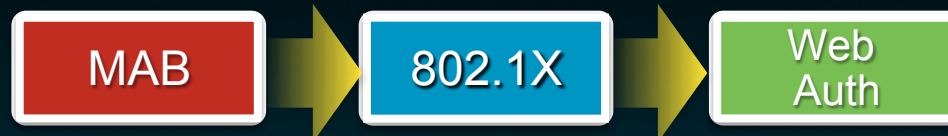
Available Methods on Port



User Authentication



Device Handling



Web Authentication

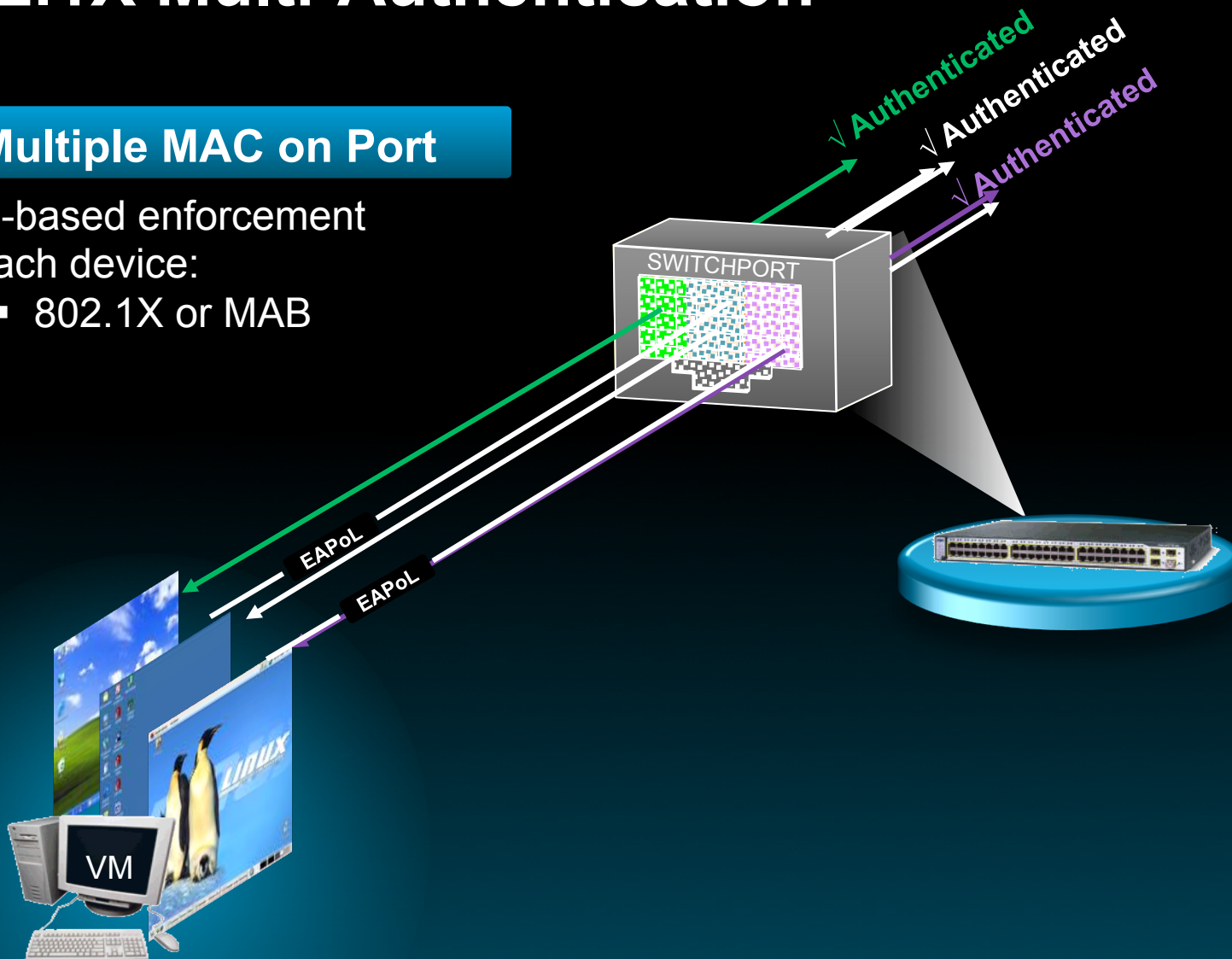


802.1X Multi-Authentication

Multiple MAC on Port

MAC-based enforcement for each device:

- 802.1X or MAB



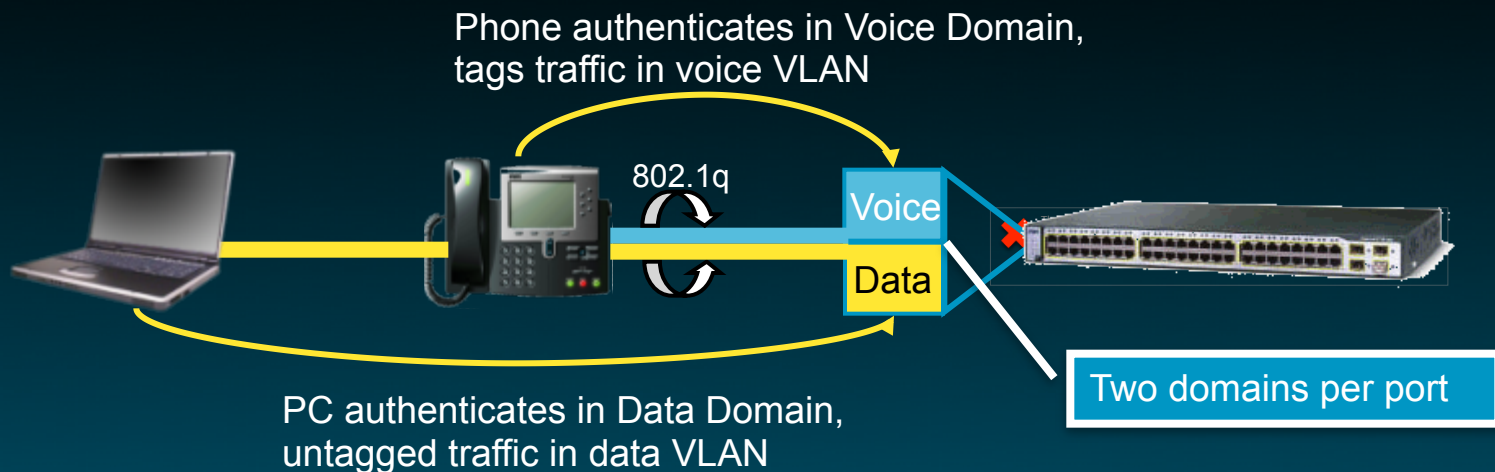
IP Telephony in 802.1X Environment

- Cisco TrustSec™ provides the most comprehensive IP Phone interoperability with 802.1X technology in the industry.
- 802.1X Multidomain Authentication authenticates / authorizes IP phone and PC behind the IP phone separately.
- Cisco 802.1X switch authenticates Cisco IP phones as well as third-party IP phones.
- Cisco IP phone has built-in supplicant, supporting EAP-MD5 and EAP-TLS for 802.1X.
- Various IP phone use cases are supported.

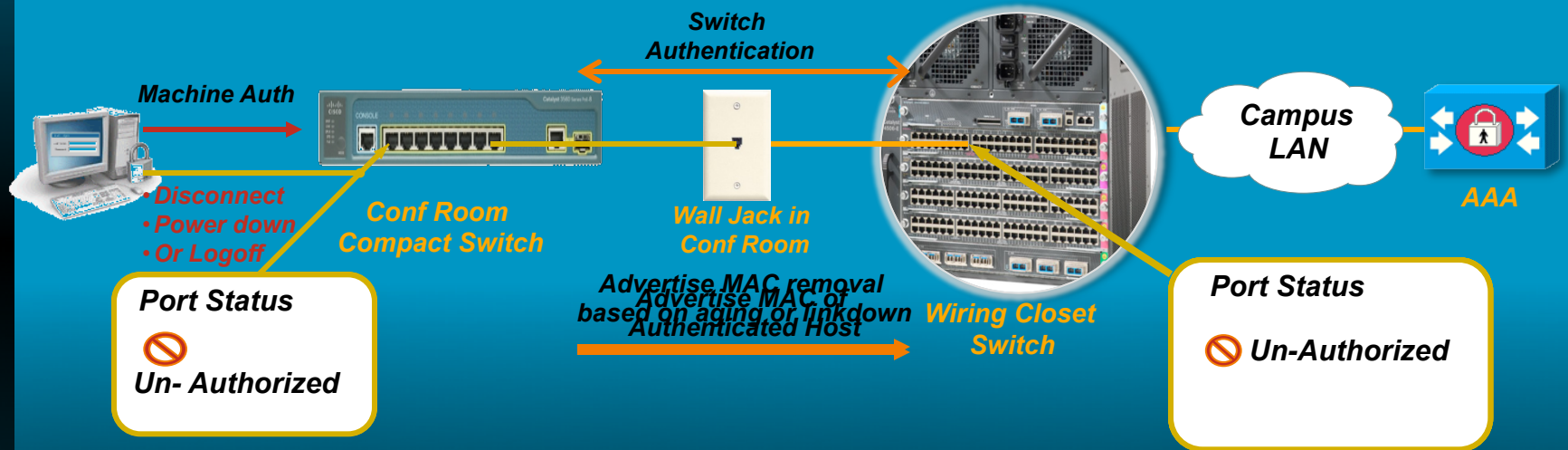


Multidomain Authentication (MDA)

- MDA separates the authentication domain for data (PC) and voice (IP phone) appropriately.
- MDA supports 802.1X or MAB for both data and voice domain authentication.
- Supports both Cisco IP phones and third-party vendor IP phones.



Rogue Device Mitigation: Network Edge Access Topology



- Extend trust to conference room deployment.
- Secure access control for shared media access.

Authorization and Policy Enforcement in the Network

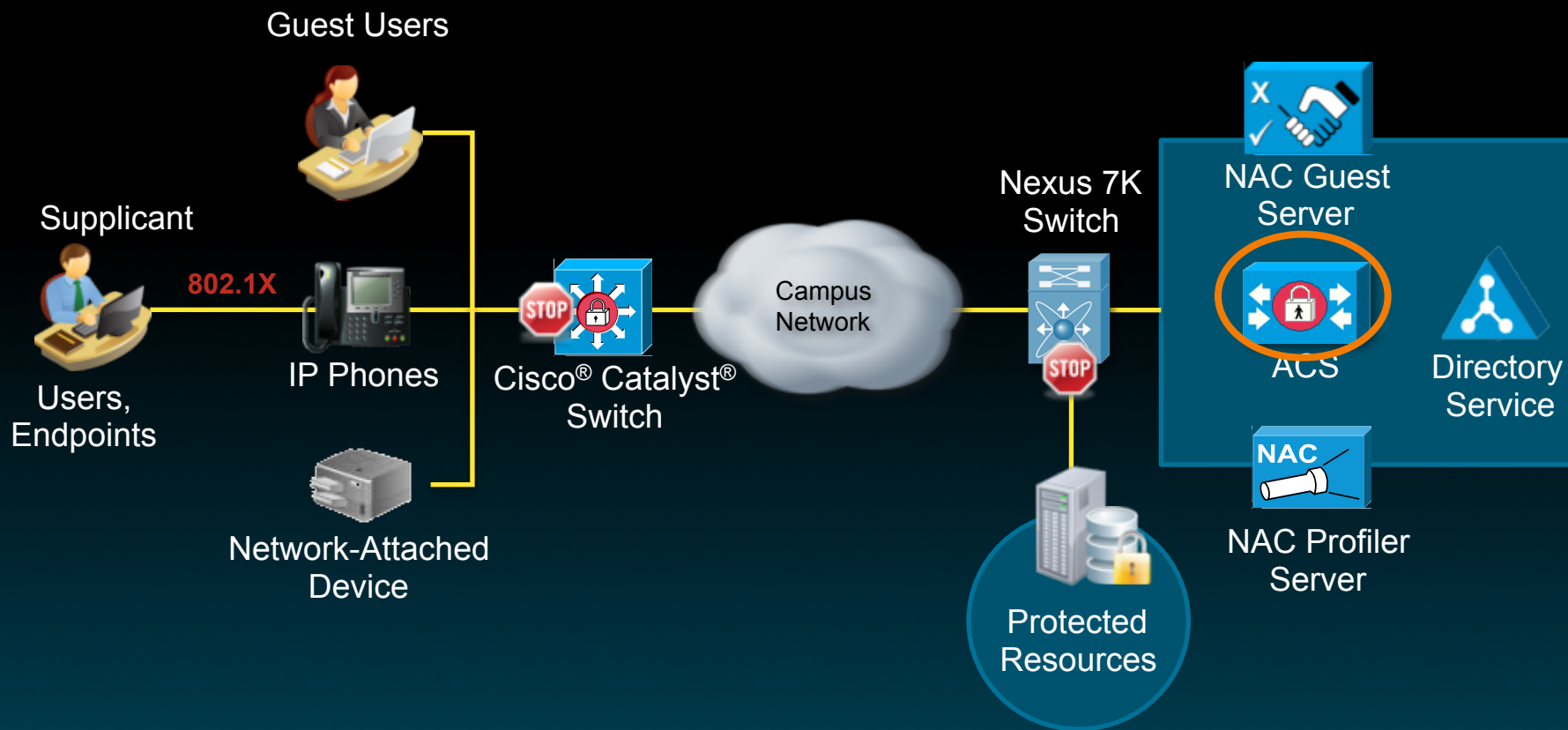


Various Authorization Mechanisms

- TrustSec™ provides various authorization mechanisms for policy enforcement.
- Three major enforcement / segmentation mechanisms:
 - Dynamic VLAN assignment – Ingress
 - Downloadable per session ACL – Ingress
 - Security Group Access Control List (SGACL) - Egress
- Three different enforcement modes:
 - Monitor Mode
 - Low Impact Mode (with Downloadable ACL)
 - High-Security Mode
- Session-Based on-demand authorization:
 - Change of Authorization (RFC3576 RADIUS Disconnect Messages)

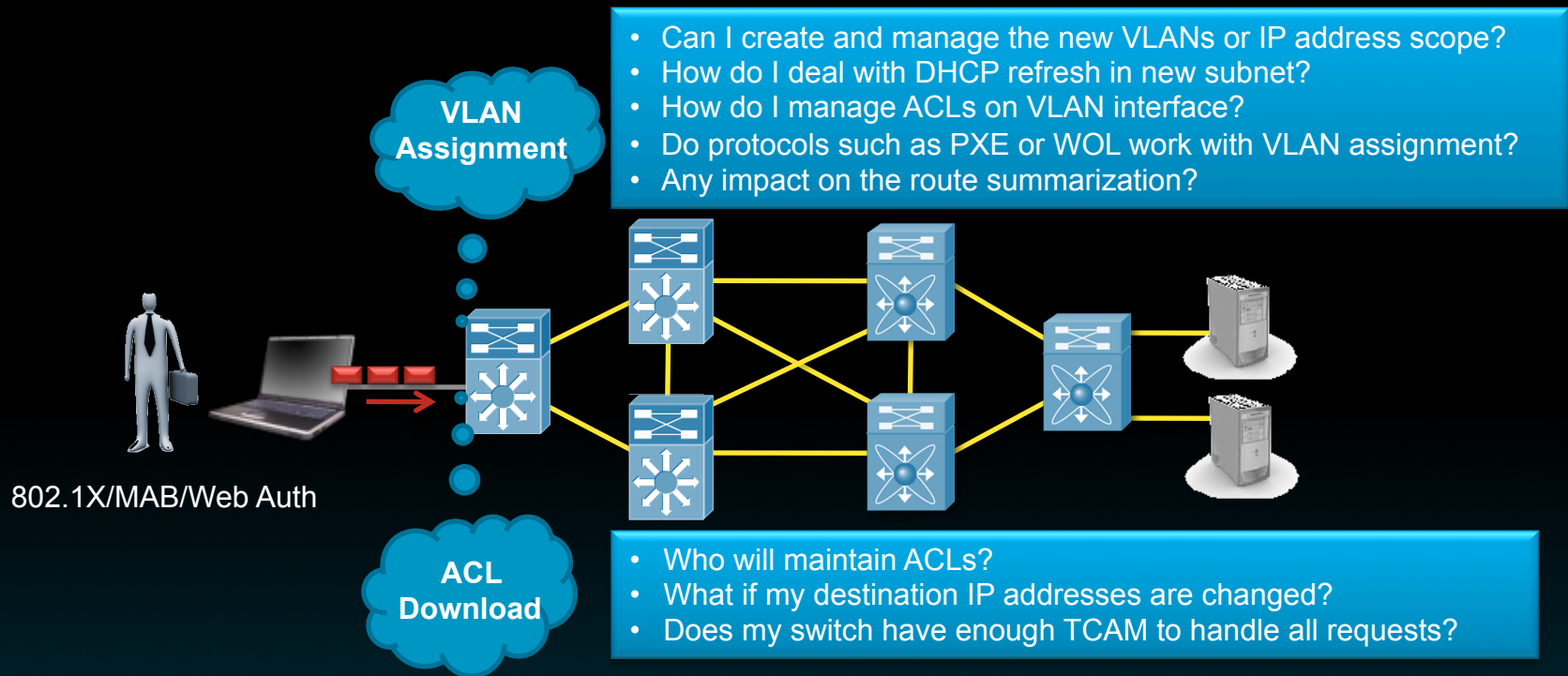


Cisco TrustSec™ Authorization and Enforcement Points



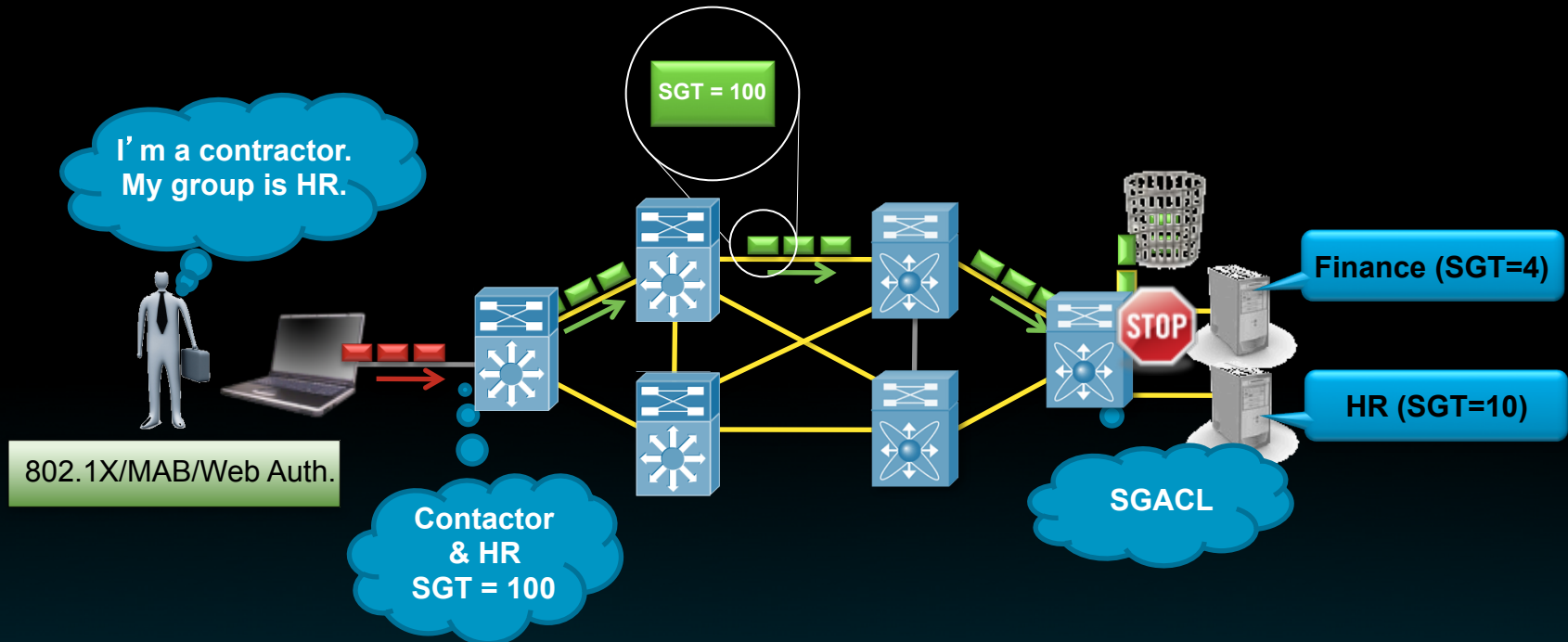
Control Plane: **RADIUS**

Ingress Access Control



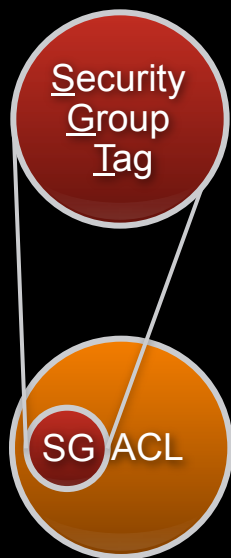
- Traditional access authorization methods leave some deployment concerns:
 - Detailed design before deployment is required, otherwise...
 - Not so flexible for changes required by today's business
 - Access control project ends up with redesigning whole network

Security Group Access (SGA)



- Security Group Access allows customers:
 - To keep existing logical design at the access layer
 - To change / apply policy to meet today's business requirements
 - To distribute policy from a central management server

Security Group Access (SGA)

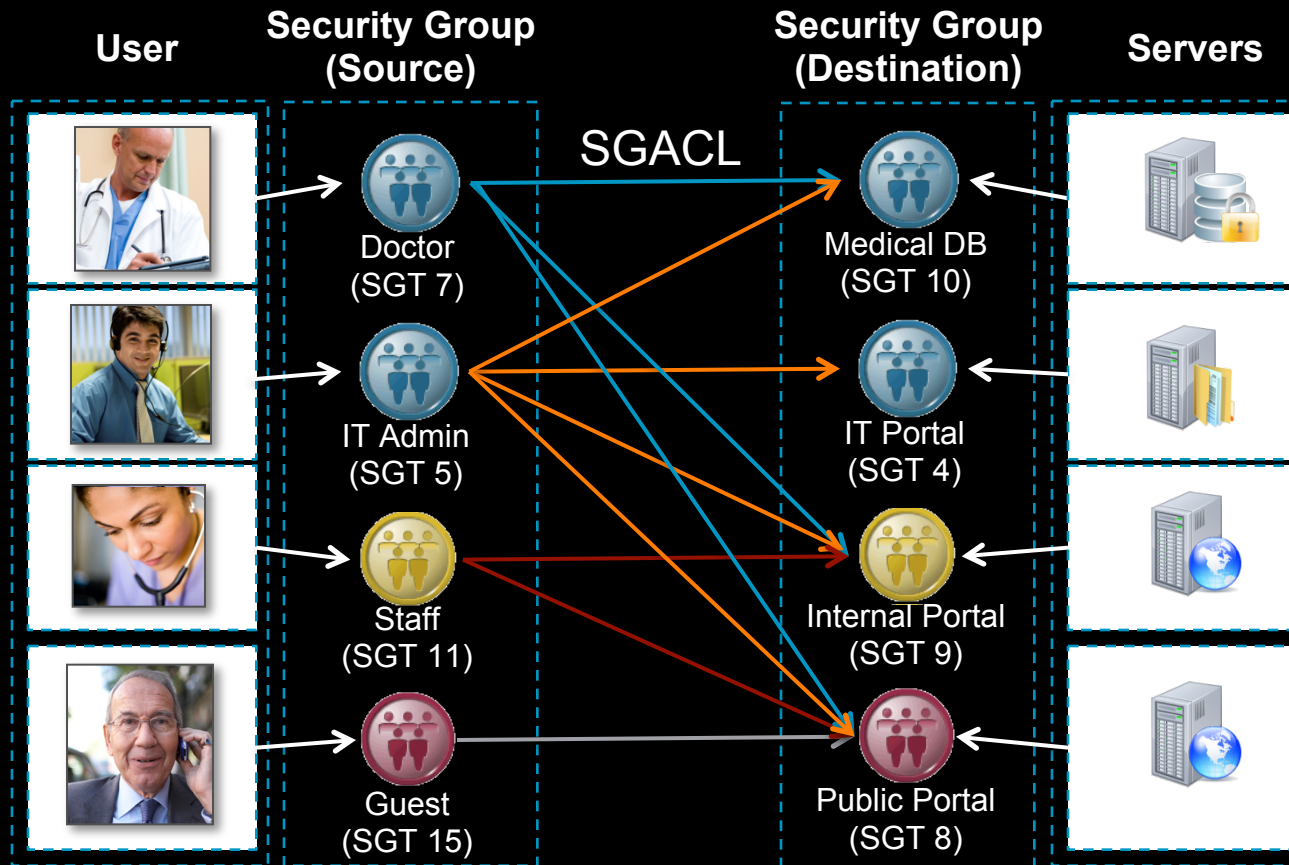


- **Unique 16 bit (65K) tag assigned to unique role**
- **Represents privilege of the source user, device, or entity**
- **Tagged at ingress of TrustSec™ domain**
- **Filtered (SGACL) at egress of TrustSec™ domain**
- **No IP address required in ACE (IP address is bound to SGT)**
- **Policy (ACL) is distributed from central policy server (ACS) or configured locally on TrustSec™ device**

Benefits

- Provides **topology-independent** policy
- Flexible and scalable policy based on user role
- **Centralized policy management** for dynamic policy provisioning
- Egress filtering **results to reduce TCAM impact**

How SGA Simplifies Access Control

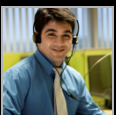
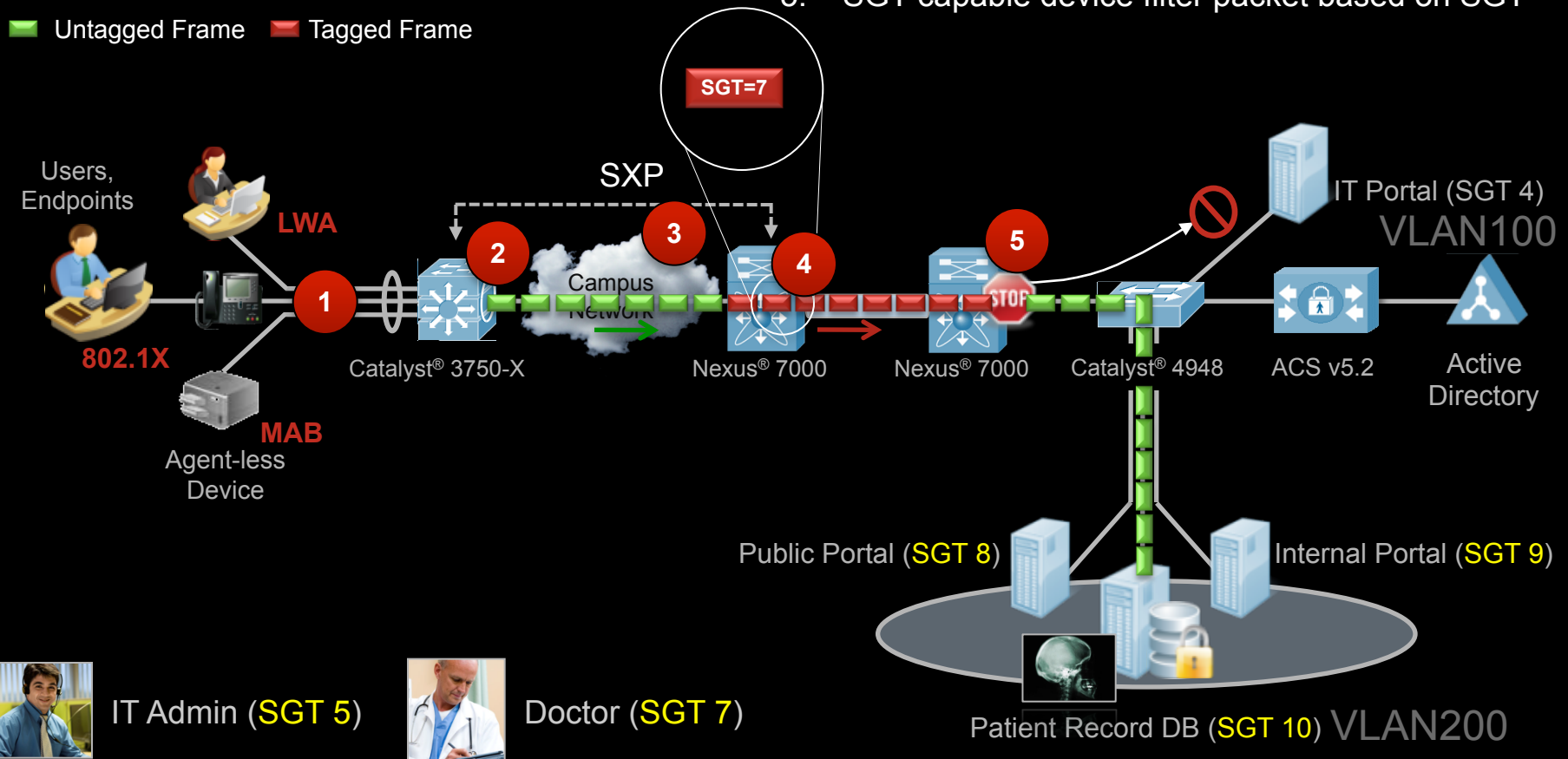


Security Group based Access Control

How It Works

1. Endpoint connects to network
2. Switch authenticates user and assign SGT
3. SXP exchange IP-to-SGT binding table with N7K
4. SGT capable device receives packet and insert SGT
5. SGT capable device filter packet based on SGT

■ Untagged Frame ■ Tagged Frame





IT Admin (SGT 5)



Doctor (SGT 7)

SGACL Policy Matrix

Source SGT \ Destination SGT	Public Portal (SGT 8)	Internal Portal (SGT 9)	IT Portal (SGT 4)	Patient Record DB (SGT 10)
 Doctor (SGT 7)			No Access	Web File Share
 IT Admin (SGT 3)			Full Access	SSH RDP File Share

IT Maintenance ACL

```

permit tcp dst eq 443
permit tcp dst eq 80
permit tcp dst eq 22
permit tcp dst eq 3389
permit tcp dst eq 135
permit tcp dst eq 136
permit tcp dst eq 137
permit tcp dst eq 138
permit tcp des eq 139
deny ip
    
```

Enforcement Modes

- Protecting Network Operations While Securing Network Access

Three enforcement modes for minimizing impacts:

- Addressing (DHCP)

- OS communication (KRB5, LDAP, DNS, etc.)

- Application-level policy (Group Policy Object)

Enforcement mode supports following use cases:

- PXE Protocol for bootstrap

- WoL for maintenance and patch management

Monitor Mode

Low Impact Mode

High Security Mode

TrustSec™ Enforcement Mode helps overcome 802.1X deployment problems

Enforcement Option 1

Monitor Mode



Monitor Mode

Provides easy deployment start

No impact to existing network access (no enforcement)

Increase visibility through accountability

Evaluate remaining risk

Prepare the network for access control in later phases

How?

Configure all components for 802.1X with MAB

Leverage IOS innovative features:

- Open mode

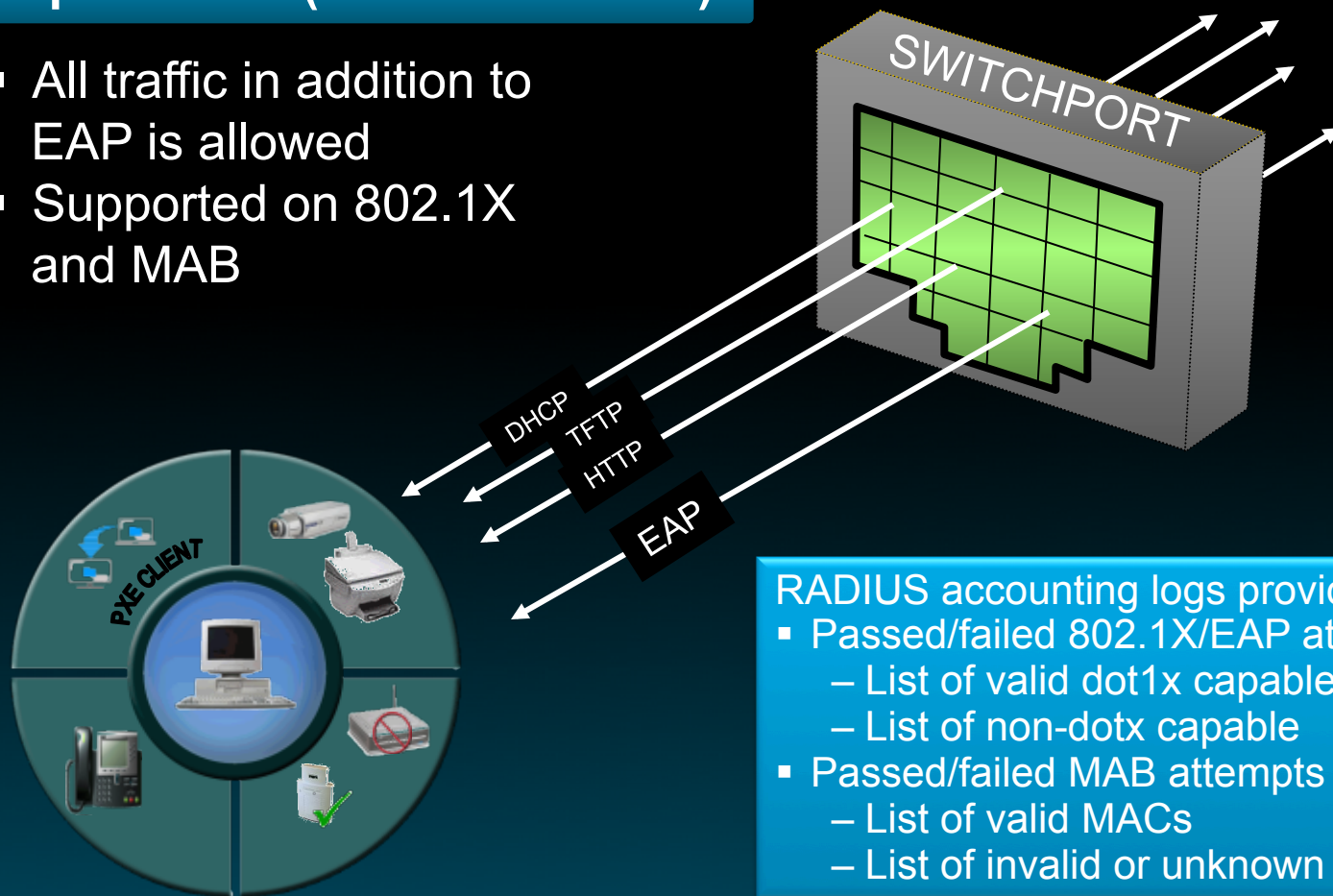
- Multi-authentication

Use ACS 5.1 M&T to evaluate network

802.1X/MAB – Open Mode

Open Mode (No Restrictions)

- All traffic in addition to EAP is allowed
- Supported on 802.1X and MAB



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

Enforcement Option 2

Low Impact Mode



Low Impact Mode

- Begin to control/differentiate network access
- Minimize impact on existing network access
- Retain visibility of Monitor Mode
- “Low impact” means no need to re-architect your network:
 - Keep existing VLAN design
 - LAN changes kept to minimum
 - No design impact

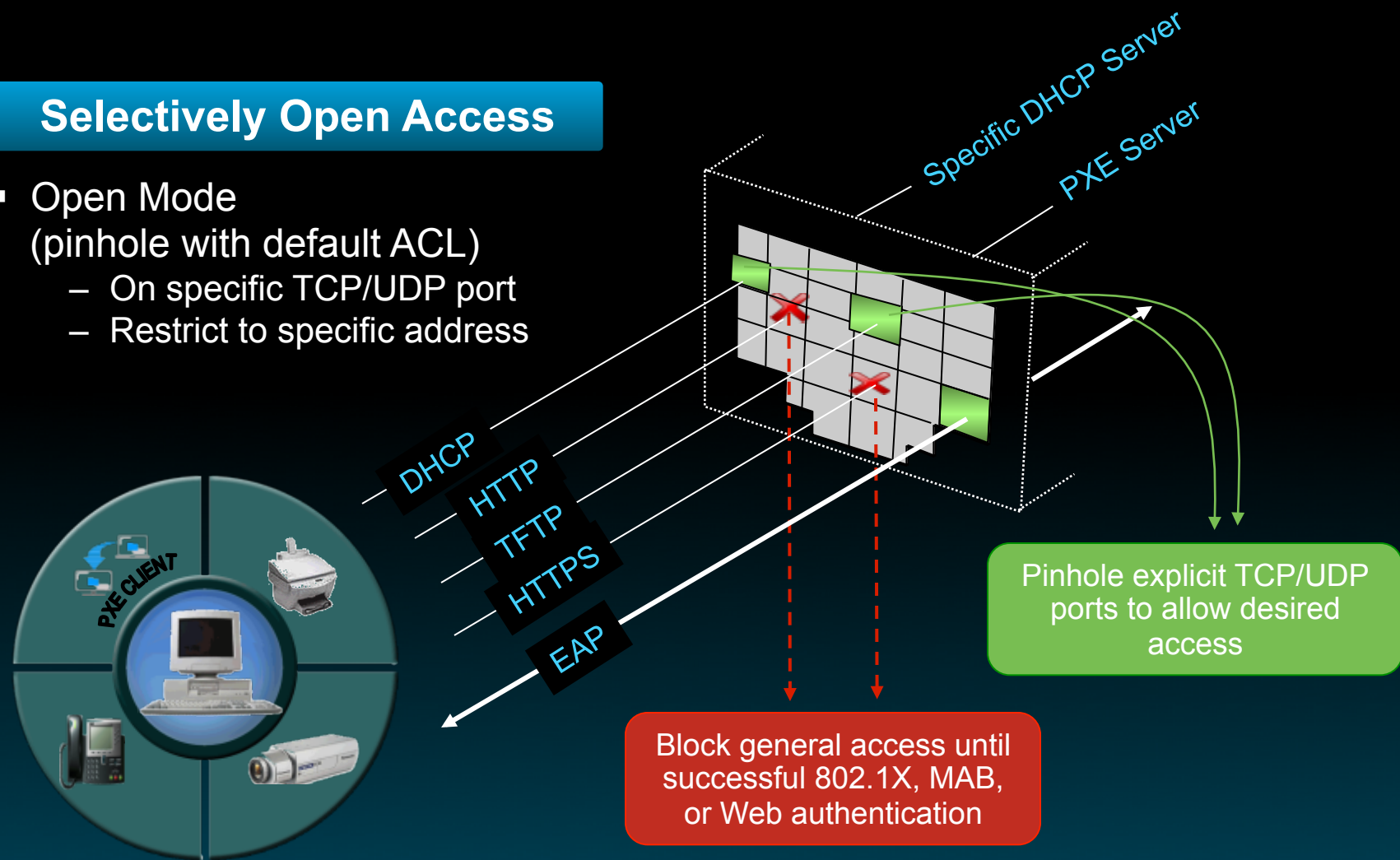
How?

- Authentication:
 - Deploy supplicants to manage device
 - Configure ACS with MAC Address of known non-802.1x device.
(We can use NAC Profiler here.)
- Add innovative IOS features for access control
 - Downloadable ACLs
 - Flexible authentication: failed event fallback to next method
- Specify and implement security policy

Low Impact Mode Access Control with Open Mode & ACLs

Selectively Open Access

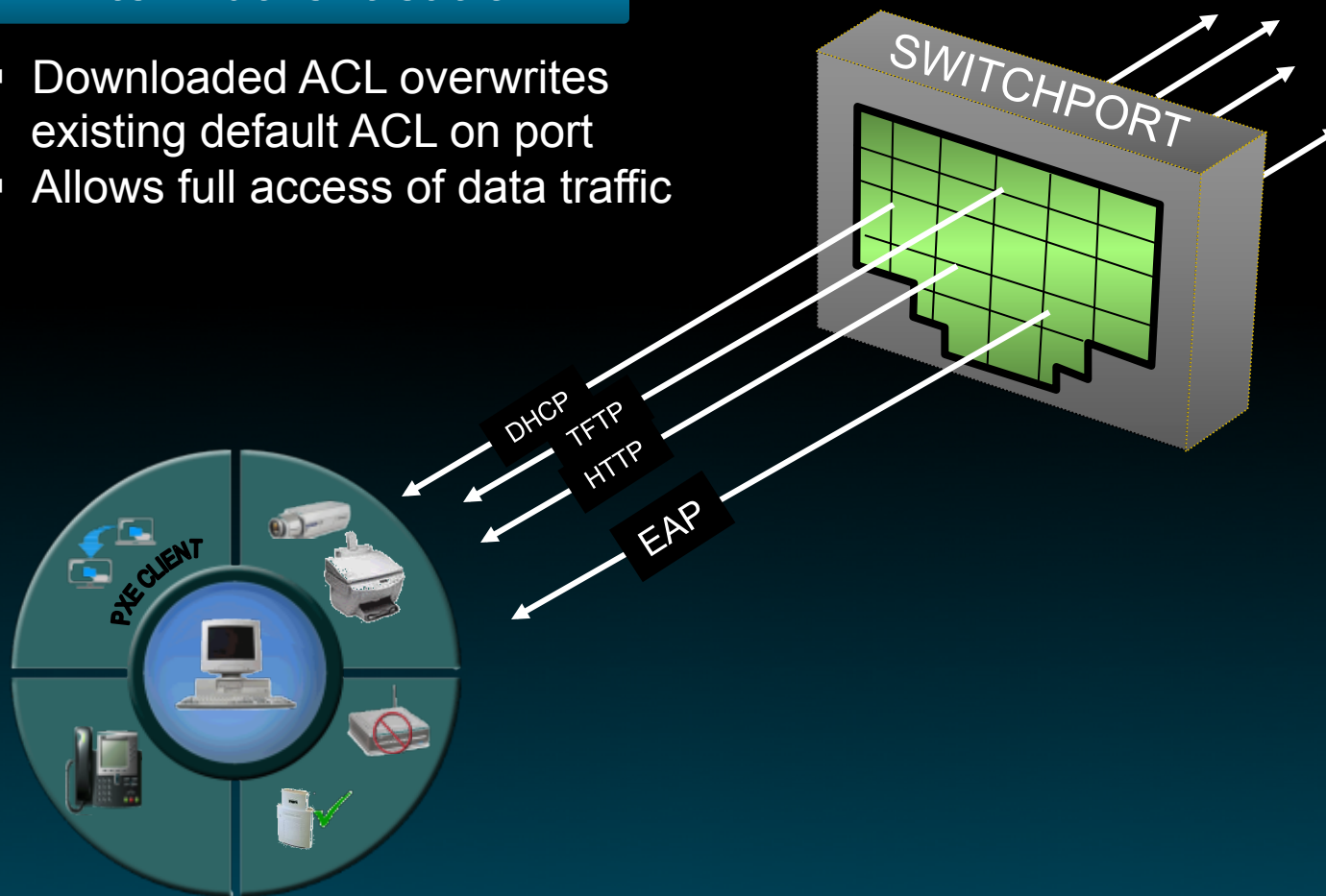
- Open Mode (pinhole with default ACL)
 - On specific TCP/UDP port
 - Restrict to specific address



Low Impact Mode Access Control with Open Mode & ACLs

After Authentication

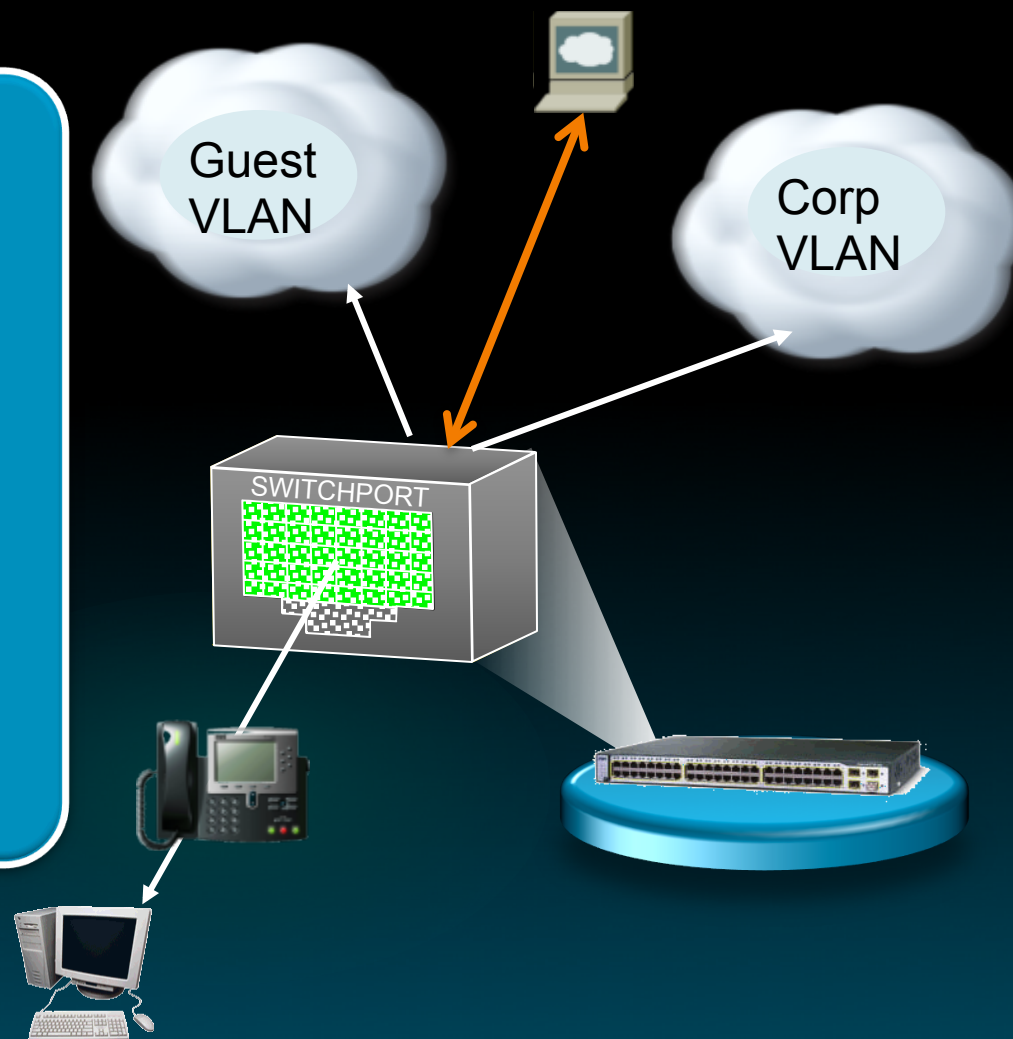
- Downloaded ACL overwrites existing default ACL on port
- Allows full access of data traffic



RADIUS Change of Authorization

Dynamic Session Control from a Policy Server

- Reauthenticate session
- Terminate session
- Terminate session with port bounce
- Disable host port
- Session query
 - For active services
 - For complete identity
 - Service specific
- Service activate
- Service deactivate
- Service query



Data Integrity and Confidentiality



Confidentiality and Integrity

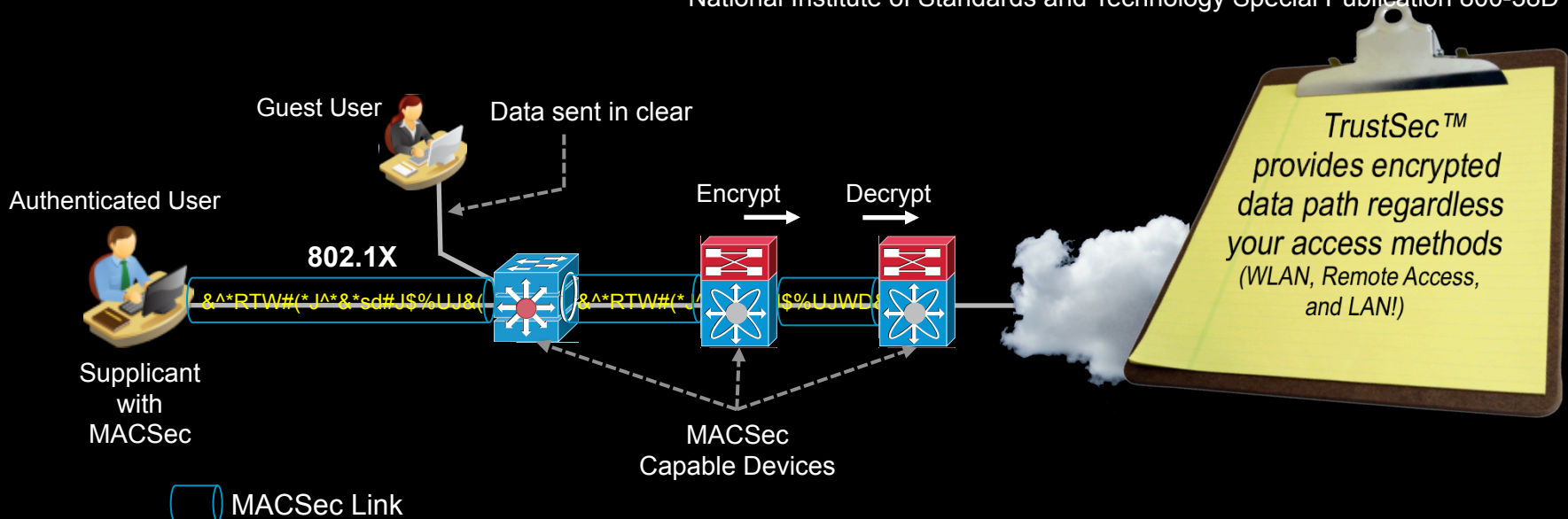
Securing Data Path with MACSec



Media Access Control Security (MACSec)

- Provides “WLAN / VPN equivalent” encryption (128bit AES GCM) to LAN connection
- NIST approved* encryption (IEEE802.1AE) + Key Management (IEEE802.1X-2010/MKA)
- Allows the network to continue to perform auditing (Security Services)

* National Institute of Standards and Technology Special Publication 800-38D



AnyConnect 3.0 for MACSec

- AnyConnect 3.0 provides
 - Unified access interface for SSL-VPN, IPSec and 802.1X for LAN / WLAN
 - Support MACSec / MKA (802.1X-REV) for data encryption in software (Performance is based on CPU of the endpoint)
 - MACSec capable hardware (network interface card) enhance performance with AnyConnect 3.0

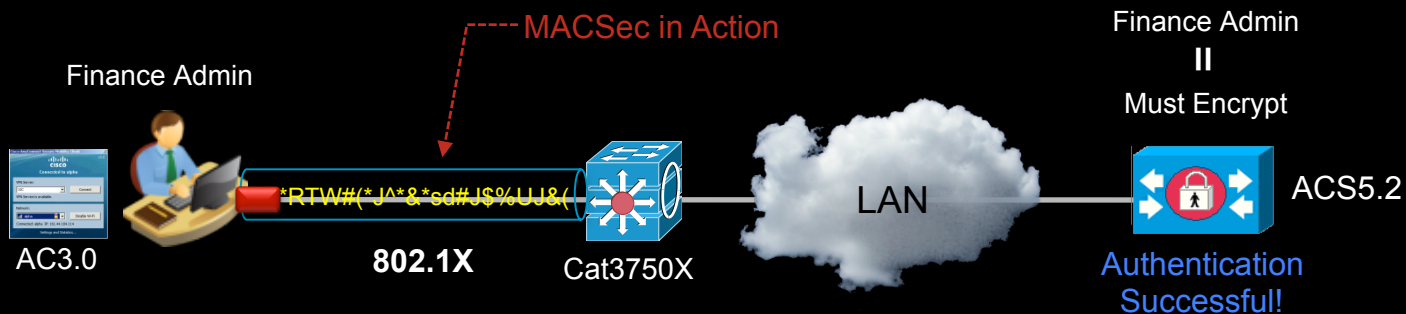


MACSec-ready hardware:

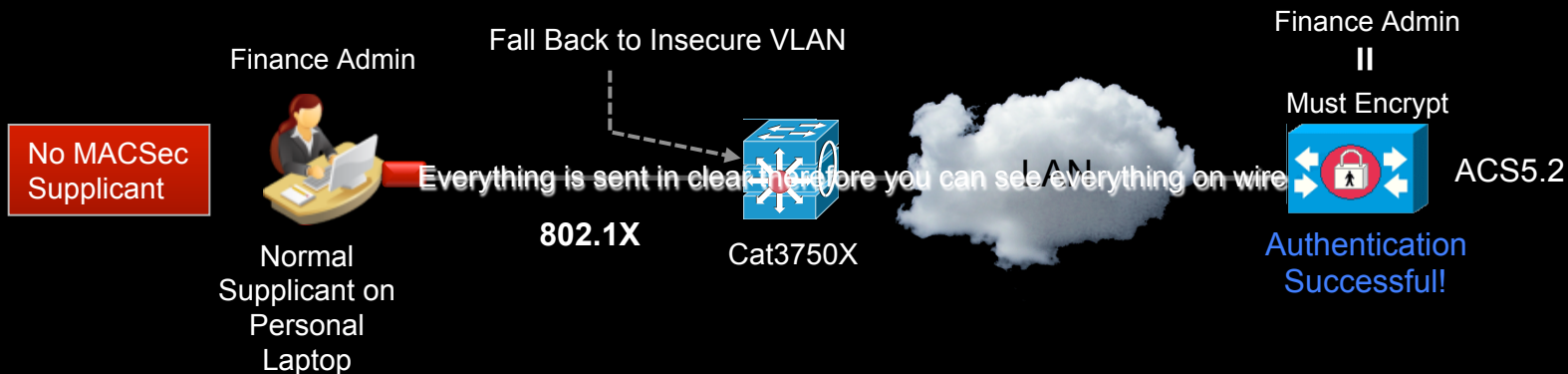
Intel 82576 Gigabit Ethernet Controller
 Intel 82599 10 Gigabit Ethernet Controller
 Intel ICH10 - Q45 Express Chipset (1Gbe LOM)
 (Dell, Lenova, Fujitsu, and HP have desktops shipping with this LOM.)

Policy Based Encryption using MACSec

Using AnyConnect 3.0



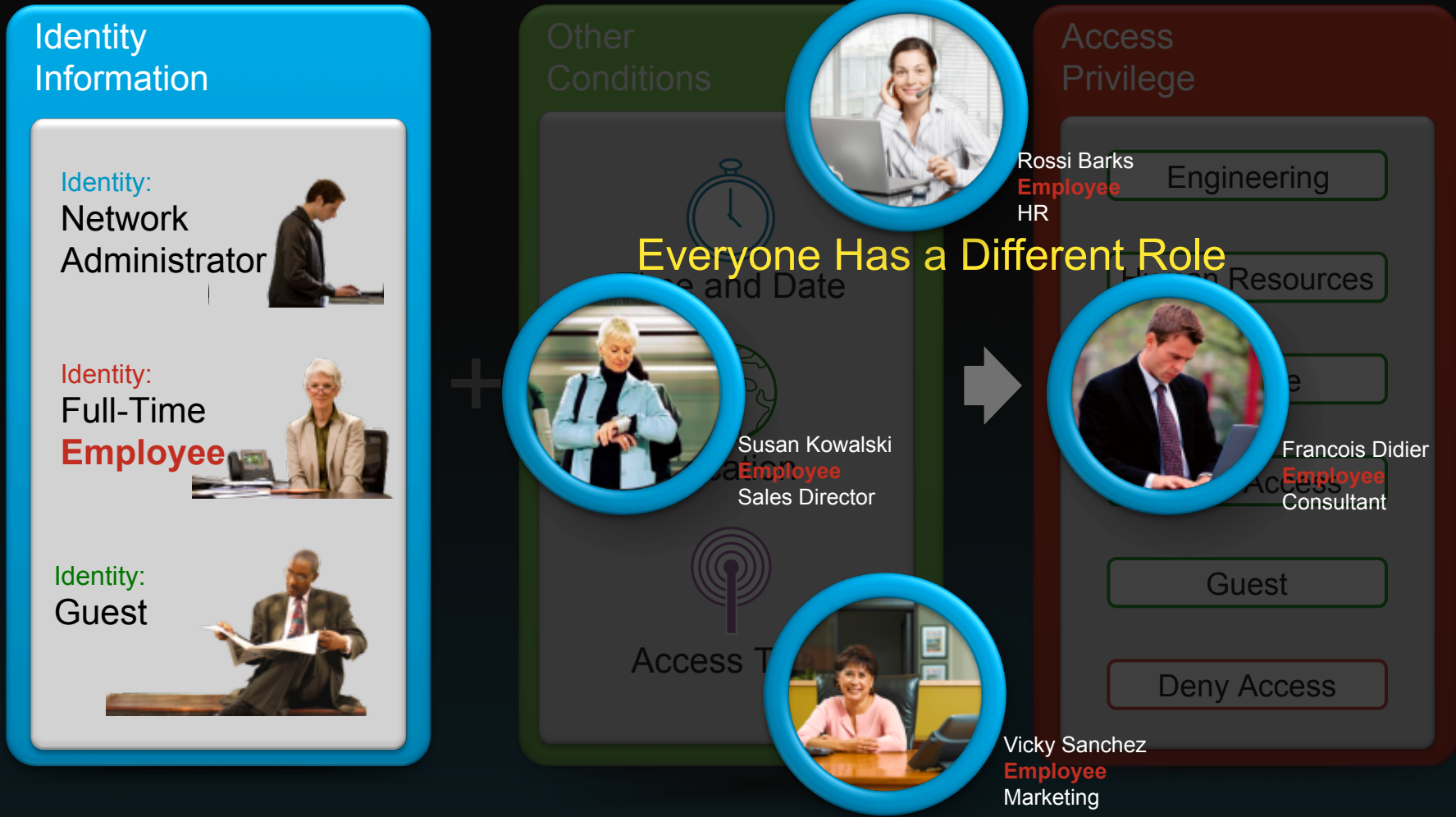
Using Normal Supplicant



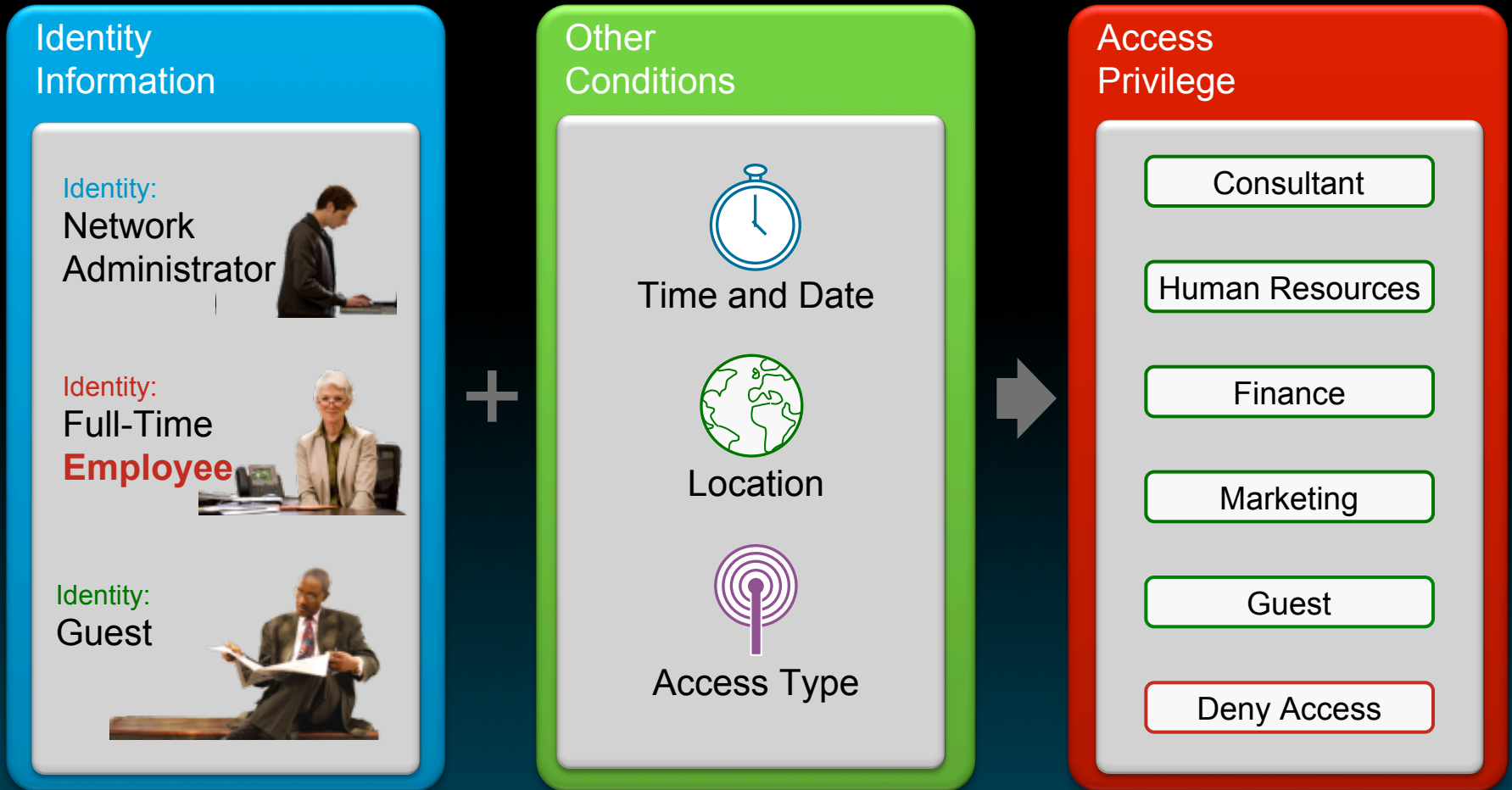
ACS for Policy-Based Access Control



More Flexible Policy with Role-Based Access Control



Policy for Today's Business Requirement



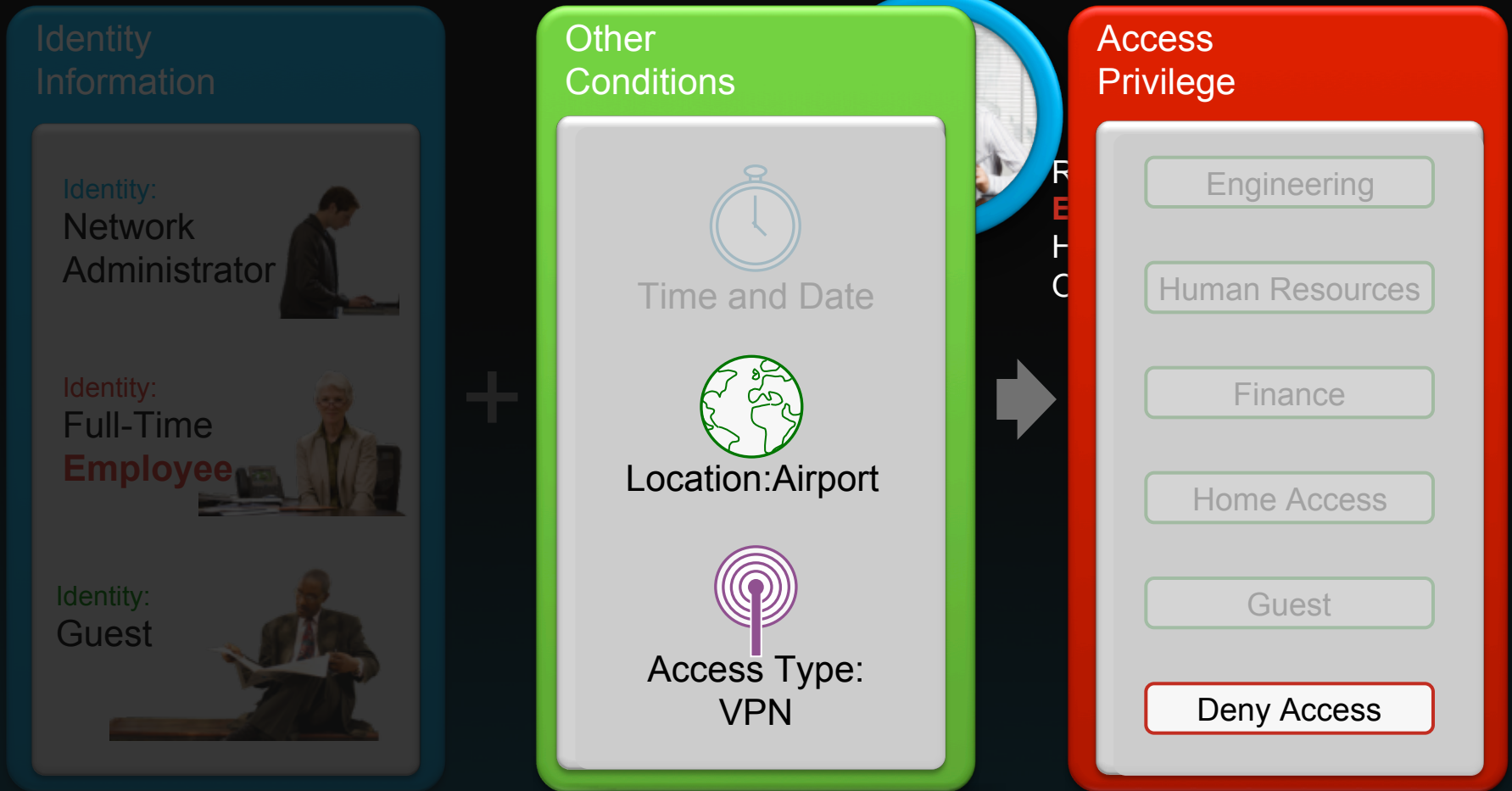
Role + Rule-Based Access Control

Example: Human Resources Role



Role + Rule-Based Access Control

Example: Human Resources Role



Policy Elements Sample



Rossi Barks
 Type: **Reg. Employee**
 Title: **Sr. HR Advisor**
 Group: **HR Admin Group**
 Dept ID: **240087**
 Office: **408-878-9097**
 Mail: rbarks@stsam.org

Policy Conditions

- Access Type
- Location
- Date and Time
- Network Device Type
- NAD IP Address
- EAP Auth Method
- Authentication Status
- AD Group
- LDAP Attributes**
- RADIUS Attribute

Rossi Barks Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

Job Title:
 Department:
 Company:
 Manager:
 Name:

Select Attributes

Search Filter

<input type="checkbox"/>	Attribute Name	Attribute Type	Attribute Value
<input type="checkbox"/>	accountExpires	Integer 64	9223372036854775807
<input type="checkbox"/>	badPasswordTime	Integer 64	0
<input type="checkbox"/>	badPwdCount	Integer 64	0
<input type="checkbox"/>	cn	String	Rossi Barks
<input type="checkbox"/>	codePage	Integer 64	0
<input type="checkbox"/>	company	String	St. SAM Inc.
<input type="checkbox"/>	countryCode	Integer 64	0
<input type="checkbox"/>	dSCorePropagationData	String	16010101000000.02
<input checked="" type="checkbox"/>	department	Integer 64	24008
<input type="checkbox"/>	displayName	String	Rossi Barks
<input type="checkbox"/>	distinguishedName	String	CN=Rossi Barks,CN=Users,DC=cts,DC=local
<input type="checkbox"/>	dn	String	CN=Rossi Barks,CN=Users,DC=cts,DC=local
<input type="checkbox"/>	givenName	String	Rossi

Access Rule Enforcement

Network Access Authorization Policy

Filter: Status Match If: Equals Enabled Clear Filter Go

	Status	Name	Conditions	AD1:department	AD1:title	Authorization Profiles	Security Group	Hit Count
1	<input type="checkbox"/>	HR Admin US	contains any (cts.local/Users/HR Admin Group)	equals 24008	-ANY-	Permit Access	HR Administrator	0
4	<input type="checkbox"/>	HR Admin Japan	contains any (cts.local/Users/HR Admin Group)	equals 33894	-ANY-	No-US-DB-Access	HR Administrator	1
2	<input type="checkbox"/>	IT Administrator	contains any (cts.local/Users/IT Admin Group)	-ANY-	-ANY-	Permit Access	IT Administrator	1
3	<input type="checkbox"/>	Corporate Asset	contains any (cts.local/Users/Domain Computers)	-ANY-	-ANY-	Permit Access	Corporate Asset	2

AD1:department	AD1:title	Authorization Profiles	Security Group
equals 24008	-ANY-	Permit Access	HR Administrator
equals 33894	-ANY-	No-US-DB-Access	HR Administrator

- Network Access Authorization Policy provides powerful “IF-THEN-ELSE” policy condition to apply detailed corporate policy.
- Authorization profile provides ingress policy enforcement methods.
- Security group can be also assigned to endpoint at the same time.

Authorization Methods

- VLAN Enforcement
- Downloadable ACL
- URL Redirection
- Security Group ACL

ACS Version 5.2

Form Factor

1121 Hardware Appliance

One rack-unit (1RU) security-hardened,
Linux-based appliance

VMware Appliance

Complete appliance image for installation
on VMware ESX 3.5 or 4.0

The VMware logo, consisting of the word "vmware" in a lowercase, sans-serif font, with a small "v" icon to the left.

Version 5.2 now supports

FIPS 140-2 Level 1 Compliance (in process)

SHA-256 Support

Internet Explorer 8 browser support for admin interface

Windows 2008 R2 support for AD authentication.

Cisco ACS Monitoring & Troubleshooting Tool



Alarms and Notifications

- Custom Triggers
- Alerts via Email and Syslog

Comprehensive Reporting

- Standard Reports
- Templates
- Customized Reports

The screenshot displays the Cisco Secure ACS View interface. The left sidebar contains a navigation menu with sections like 'Monitoring and Reports', 'Alarms', 'Inbox', 'Thresholds', 'Schedules', 'Reports', 'Favorites', 'Shared', 'Catalog', 'Troubleshooting', and 'Monitoring Configuration'. The main dashboard area is titled 'Dashboard' and includes tabs for 'General', 'Troubleshooting', 'Authentication Trends', and 'ACS Health'. It features several data visualization components: an 'Authentication Snapshot' bar chart, a 'Top N Authentications' line graph, a 'Top 5 Alarms' table, and a 'My Favorite Reports' table.

Authentication Snapshot

Time Range: Today Protocol: RADIUS Group By: Access Service

Categories: Default Network Acc...

Legend: Pass (blue), Average Day of Week Passed Count (green), Fail (orange), Average Day of Week Failed Count (purple)

Top N Authentications

Protocol: RADIUS Time Range: 6 Hours Top: 5 Status: Passed and Failed Trend: ACS

Top 5 Alarms

Severity	Name	Date	Cause
Critical Alarm	ACS - System Errors	Wed Nov 25 16:02:00	Alarm caused by ACS - System Errors threshold
Critical Alarm	ACS - System Errors	Wed Nov 25 15:48:00	Alarm caused by ACS - System Errors threshold

My Favorite Reports

Favorite Name	Report Name	Report Type
ACS - Configuration Audit - Today	ACS Instance>ACS_Configuration_Audit	System Report
ACS - System Errors - Today	ACS Instance>ACS_System_Diagnostics	System Report
Authentications - RADIUS - Today	AAA Protocol>RADIUS_Authentication	System Report
Authentications - RADIUS - Yesterday	AAA Protocol>RADIUS_Authentication	System Report
Authentications - TAGACS - Today	AAA Protocol>TACACS_Authentication	System Report
Authentications - TAGACS - Yesterday	AAA Protocol>TACACS_Authentication	System Report

Fully Configurable Dashboard

Dashboard Live Authentication Log

- Dashboard Live Authentication Log gives quick access to the real-time authentication record.
- Drilldown link from the log gives you more detailed information about authentication session, failure reason, network device configuration, etc.

Dashboard: Live Authentication Log

Dashboard

Troubleshooting | General | Authentication Trends | ACS Health

Live Authentications

Protocol: RADIUS

Auto Refresh Rate: 10 seconds

Filter: Username Match it: Contains

Time	Status	Details	Username	MAC	IP Address	NAD	NAS Port ID	Failure Reason	Access Service	Authentication	CTS Security Group
11:04:54.973 PM	✘	Details	ID\itadmin	00-14-5E-42-9C-69	10.1.10.101	10.1.3.2	FastEthernet2/2	Subject not found	802.1X	MSCHAPV2	
11:03:24.450 PM	✘	Details	CTS\quest	00-14-5E-42-9C-69	10.1.10.101	10.1.3.2	FastEthernet2/2	User authentication failed	802.1X	MSCHAPV2	
11:02:51.896 PM	✔	N/A	#CTSREQUEST#			10.1.50.2			NDAC_SGT_Service		HR Administrator
11:02:51.712 PM	✔	Details	CTS\itadmin	00-14-5E-42-9C-69	10.1.10.101	10.1.3.2	FastEthernet2/2		802.1X	MSCHAPV2	HR Administrator

Time	Status	Details	Username	MAC	IP Address	NAD
11:04:54.973 PM	✘	Details	ID\itadmin	00-14-5E-42-9C-69	10.1.10.101	10.1.3.2
11:03:24.450 PM	✘	Details	CTS\quest	00-14-5E-42-9C-69	10.1.10.101	10.1.3.2

Dashboard Live Authentication Log

- Drilldown Log Analysis View Example:
User Authentication Summary

User > User Authentication Summary

User : CTSitadmin
 Protocol : RADIUS
 Time Range : August 30, 2009 - September 28, 2009 ([Today](#) | [Yesterday](#) | [Last 7 Days](#) | [Last 30 Days](#))

Generated on September 29, 2009 11:08:34 PM PDT

Authentications

11 Passed Authentication(s)
 1 Failed Authentication(s)
 12 Total

Sessions

[Active Sessions](#)

Most Recent Authentication

Time: [September 29, 2009 11:06:32.676 PM](#)
 RADIUS Status: [24408 User authentication against Active Directory failed since user has entered the wrong password : Authentication failed](#)
 NAS Failure:
 MAC/IP Address: [00-14-5E-42-9C-69](#)
 Network Device: [CTS6K-AS : 10.1.3.2 : FastEthernet2/2](#)
 Access Service: [802.1X](#)
 Authorization Profiles:
 CTS Security Group:
 Authentication Method: PEAP(EAP-MSCHAPv2)

Authentications By Failure Reason

Failure Reason	Total
24408 User authentication against Active Directory failed since user has entered the wrong password	1

Authentications By Endpoint MAC Address

MAC Address	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
00-14-5E-42-9C-69	11	1	12	8.33	0.92	1

Authentications By Network Device

Network Device	Port	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
CTS6K-AS	FastEthernet2/2	11	1	12	8.33	0.92	1

Authentications By Access Service

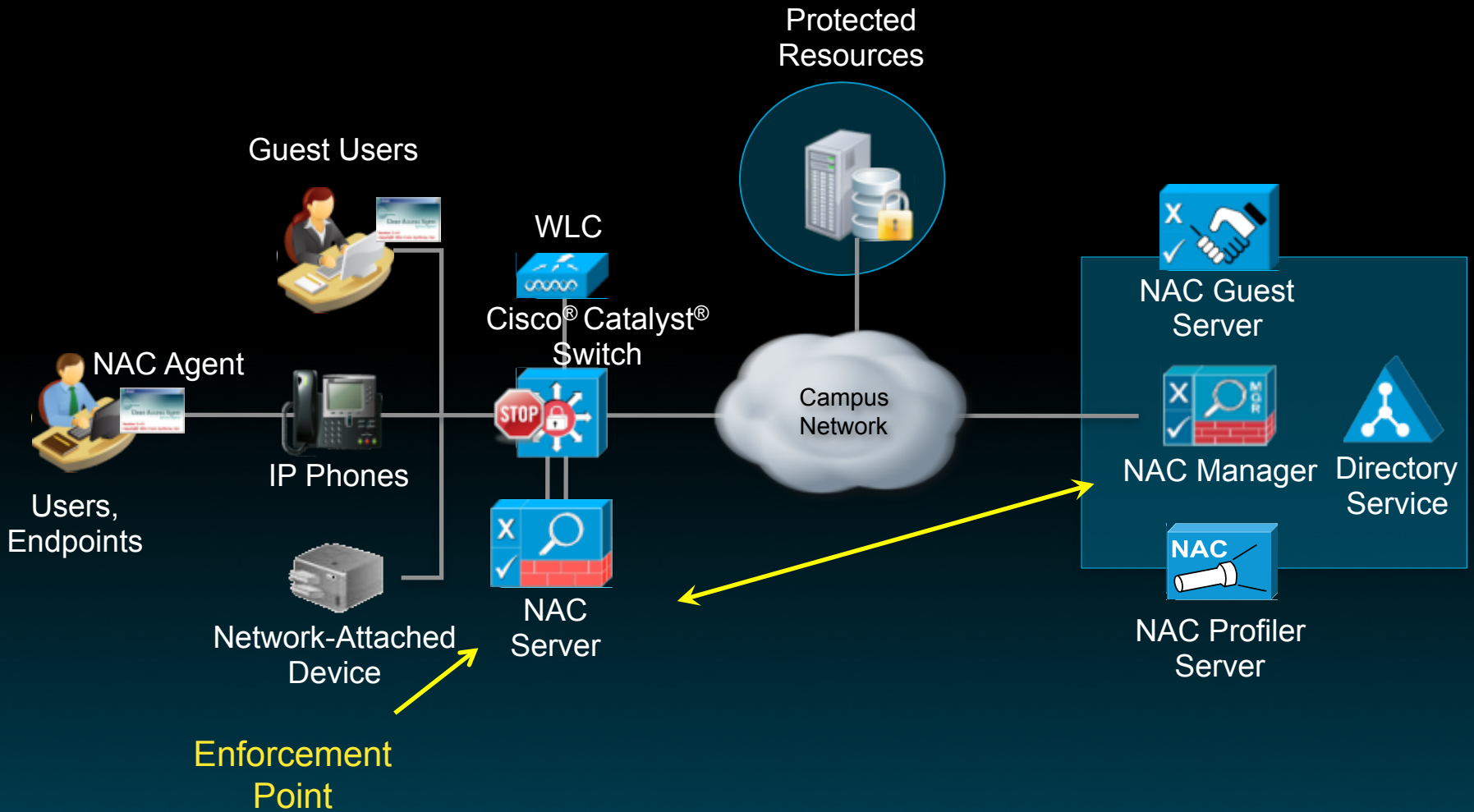
Authentications By Selected Authorization Profiles

NAC Appliance-Based Enforcement Model



Cisco TrustSec™

NAC Appliance for Non-802.1x Infrastructure



Control Plane: **SNMP**

TrustSec™ NAC Appliance Benefits



AUTHENTICATE
users and devices to the network.



Posture and Remediate
the device for policy compliance.

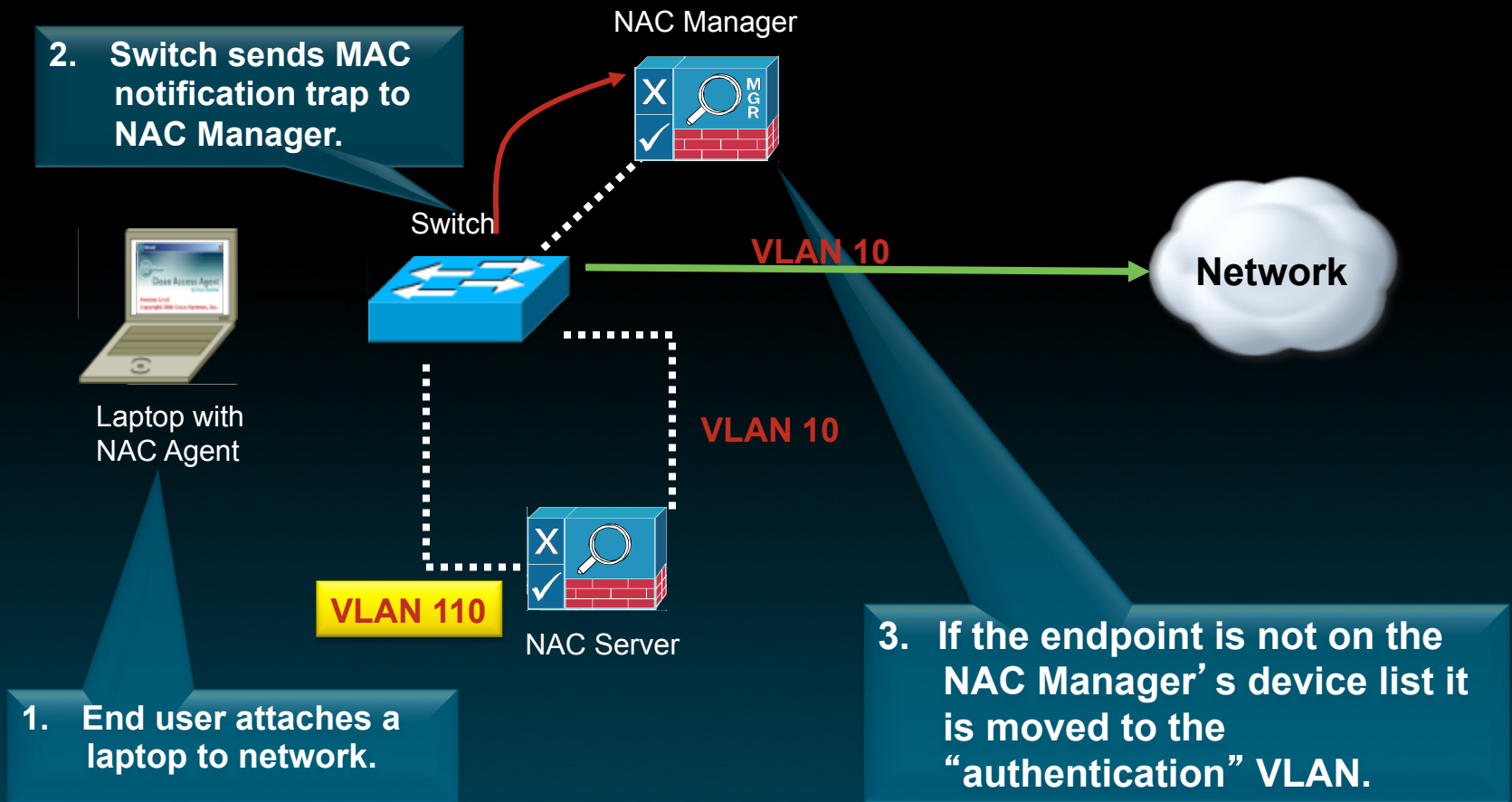


Differentiated Access
for role-based access control.

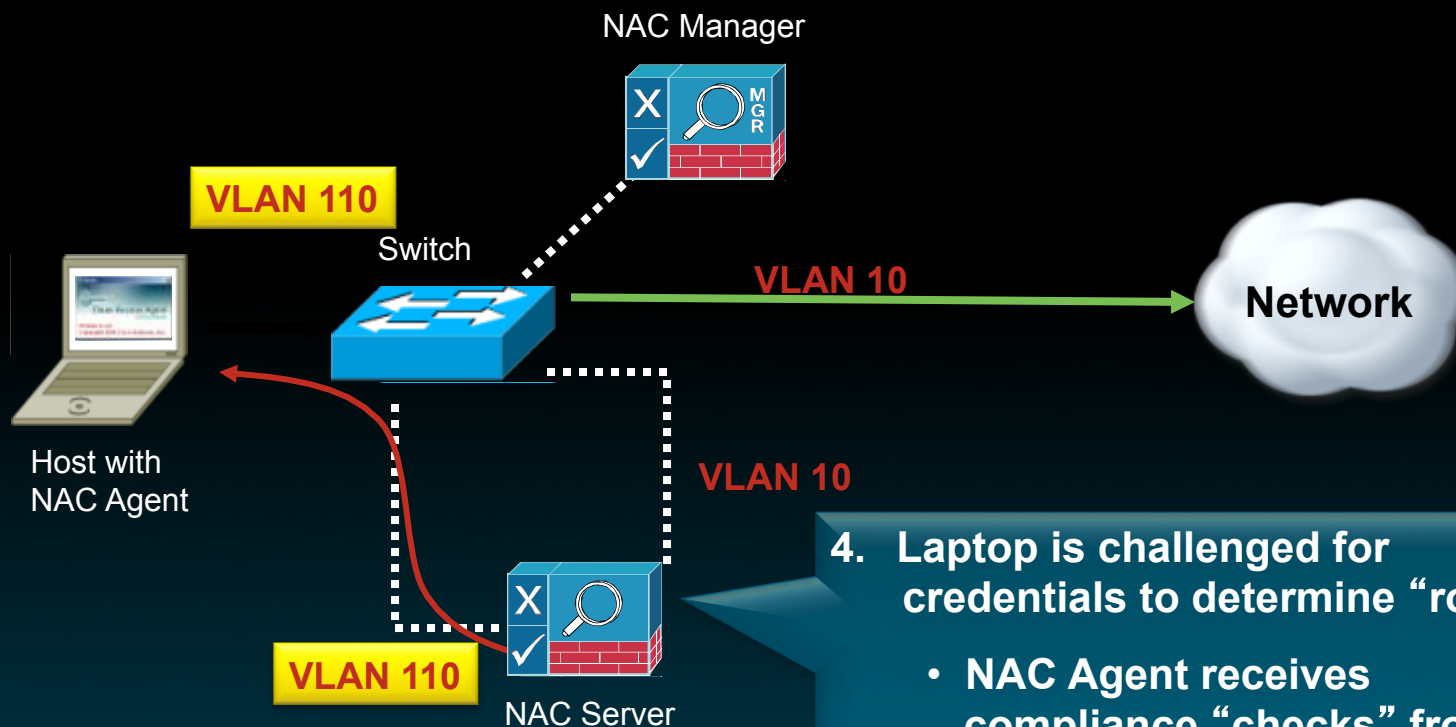


Audit and Report
Who is on my network?

NAC Appliance Process Flow for Authentication and Authorization: Out-of-Band

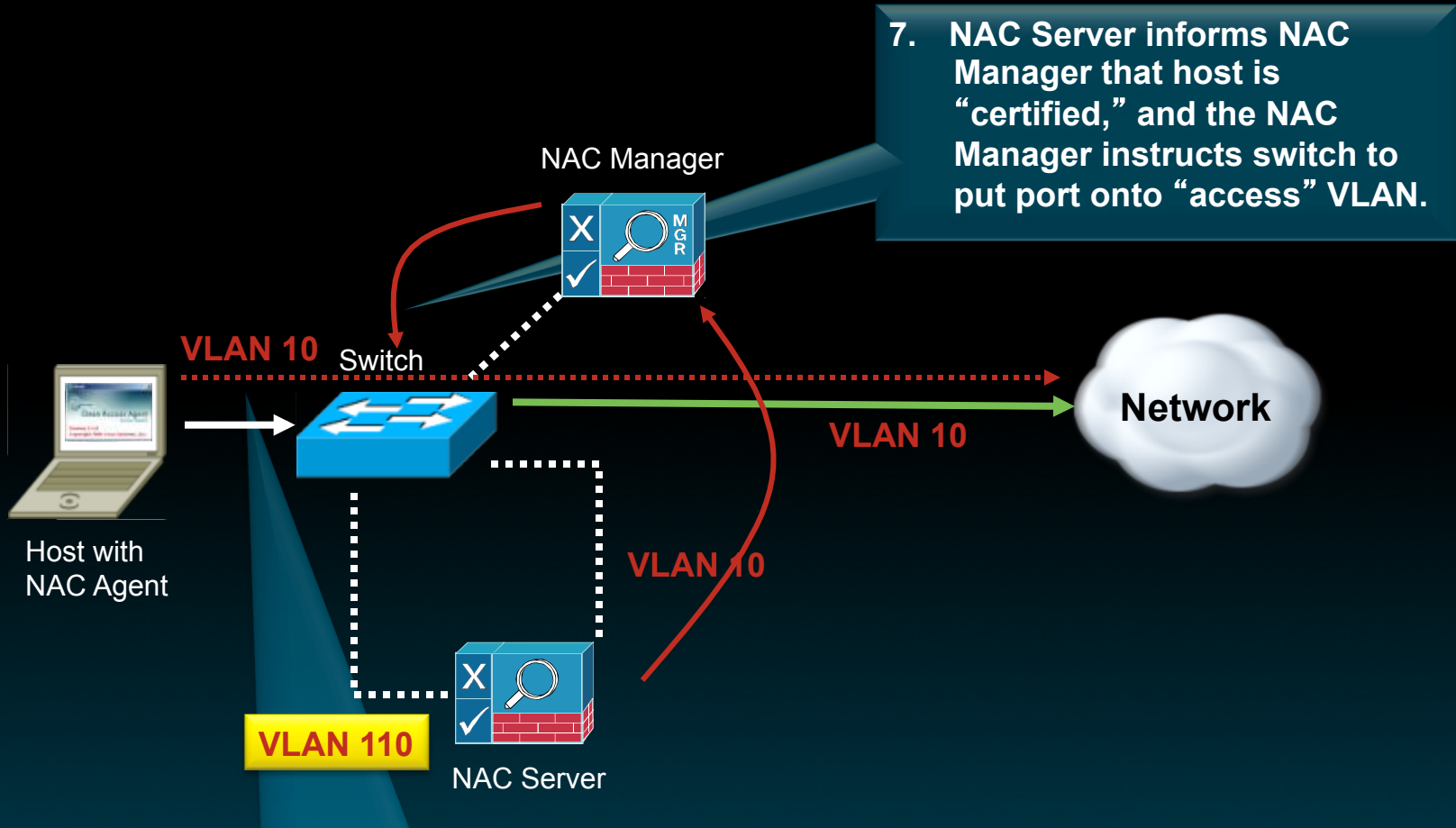


NAC Appliance Process Flow for Authentication and Authorization: Out-of-Band



4. Laptop is challenged for credentials to determine "role:"
 - NAC Agent receives compliance "checks" from NAC Server based on "role."
 - If required, remediation is offered.

NAC Appliance Process Flow for Authentication and Authorization: Out-of-Band



8. Laptop is now allowed access to the production network.

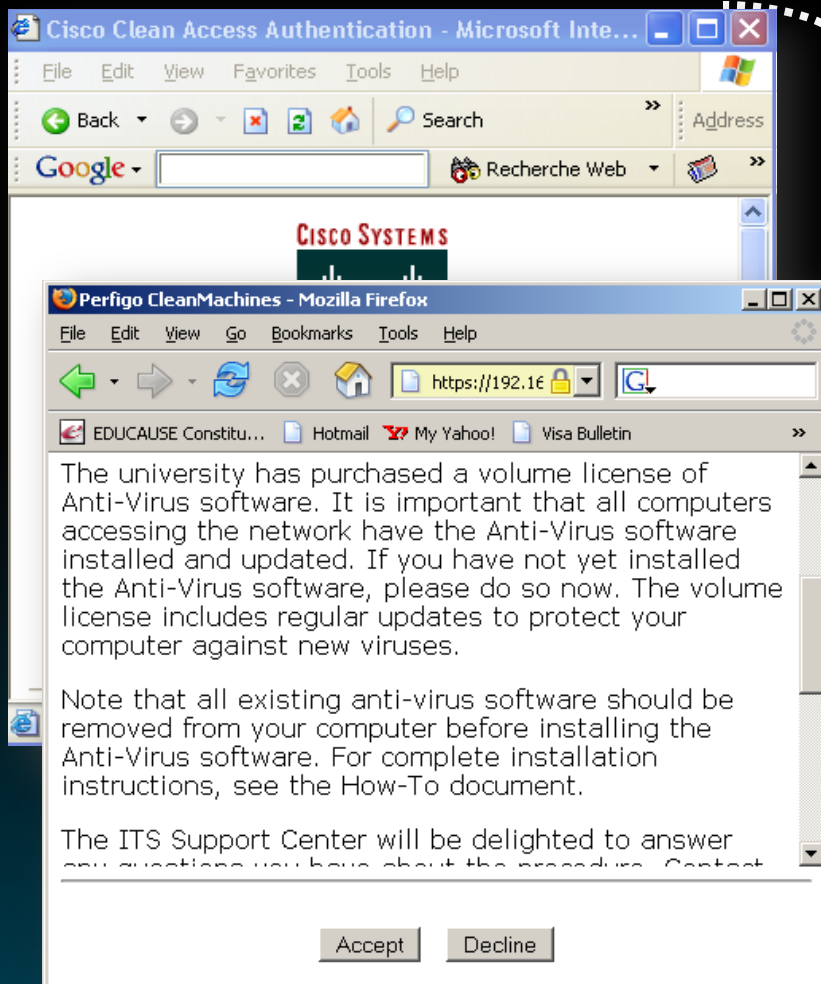
NAC Agent for Single Sign-On Authentication and Posture



Posture is analyzed
(types of checks depend on user role)

Remediation option

NAC Appliance Web Authentication



Web Agent for Contractors and Guests (providing posture and remediation)

Agentless for Web Authentication

NAC Manager Reporting

- Maintains the list of active users
- Stores the user roles and their corresponding policy controls
- Policies can be traffic control lists or VLANs by name or number



Active users: 1 (Max users since last reset: 1) Reset Max Users

Online Users 1 - 1 of 1 | First | Previous | Next | Last |

User Name	User IP	User MAC	Provider	Role	VLAN	OS	Login Time	
se space@SE.CCA.CISCO.COM	10.201.30.14	00:0C:29:03:21:D7	CCASE	Allow All	30	Windows 2000	01/11/07 18:35:10	<input type="checkbox"/>

List of Roles	New Role	Traffic Control	Bandwidth																																			
<table border="1"> <thead> <tr> <th>Role Name</th> <th>IPSec</th> <th>Roam</th> <th>VLAN</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Unauthenticated Role</td> <td>deny</td> <td>deny</td> <td></td> <td>Role for unauthenticated users</td> </tr> <tr> <td>Temporary Role</td> <td>deny</td> <td>deny</td> <td></td> <td>Role for users to download requirements</td> </tr> <tr> <td>Quarantine Role</td> <td>deny</td> <td>deny</td> <td></td> <td>Role for quarantined users</td> </tr> <tr> <td>Allow All</td> <td>deny</td> <td>deny</td> <td></td> <td>Full Access</td> </tr> <tr> <td>Guest Access</td> <td>deny</td> <td>deny</td> <td>:666</td> <td>guest privileges</td> </tr> <tr> <td>consultant access</td> <td>deny</td> <td>deny</td> <td>:55</td> <td>consultant privileges</td> </tr> </tbody> </table>				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
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																																		

NAC Profiler for Securing Userless Devices



NAC Profiler Benefits and Overview



Profiler



Collector

Categorization Profiling Example



Cisco IP Phone



HP Printer



Cisco Surveillance Camera



UPS



Nonsupplicant-Aware OS

Discovery

Endpoint Profiling

Discover all network endpoints by type and location.

Maintain real-time and historical contextual data for all endpoints.

Monitoring

Device Monitoring

Monitor the state of the network endpoints. Detect events such as MAC spoofing, port swapping, etc.

Managing Guest Access



Cisco Options for Providing Visitor Access Management

Three Options for Guest Access

- Local Web Authentication on Switch

Most commonly used for smaller deployments

Supported on wired



- Centralized NAC Guest Server

Most commonly used for larger deployments

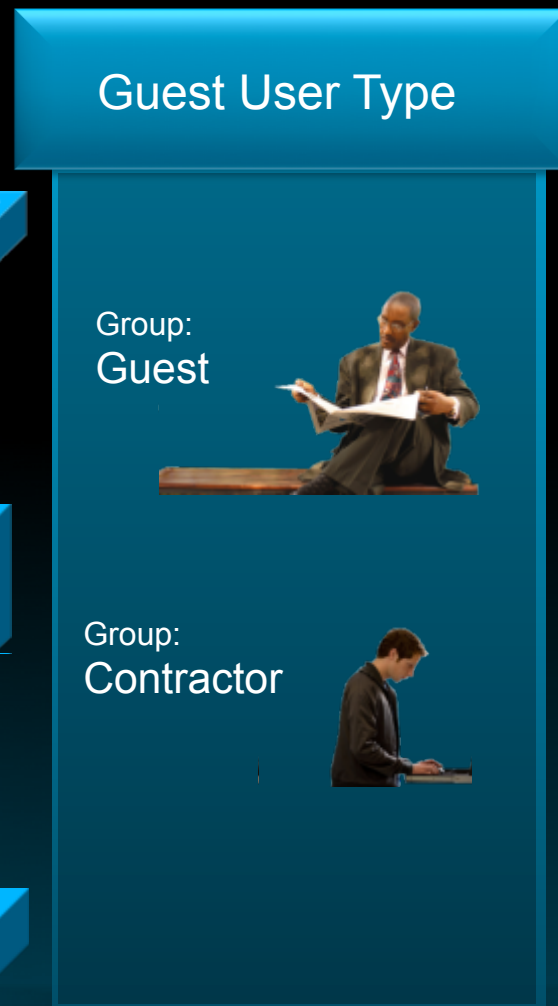
Supported on wired / wireless

Sophisticated guest sponsor capability



- Centralized on a Wireless Controller

Most commonly used when guests only have wireless access (no wired access for guests)



Managing the Guest User Lifecycle

PROVISIONING

Create Guest Accounts



Create a single guest account

Create multiple guest accounts by importing a CSV file

NOTIFICATION

Give Accounts to Guests



Print account and access details

Send account details via email

Send account details via SMS

Manage Guest Accounts



View, edit, or suspend your guest accounts

Manage batches of accounts you have created

Report on Guests



View audit reports on individual guest accounts

Display management reports on guest access

MANAGEMENT

REPORTING

Sponsor Portal

- Customizable web portal for internal sponsors
- Authentication with corporate credentials

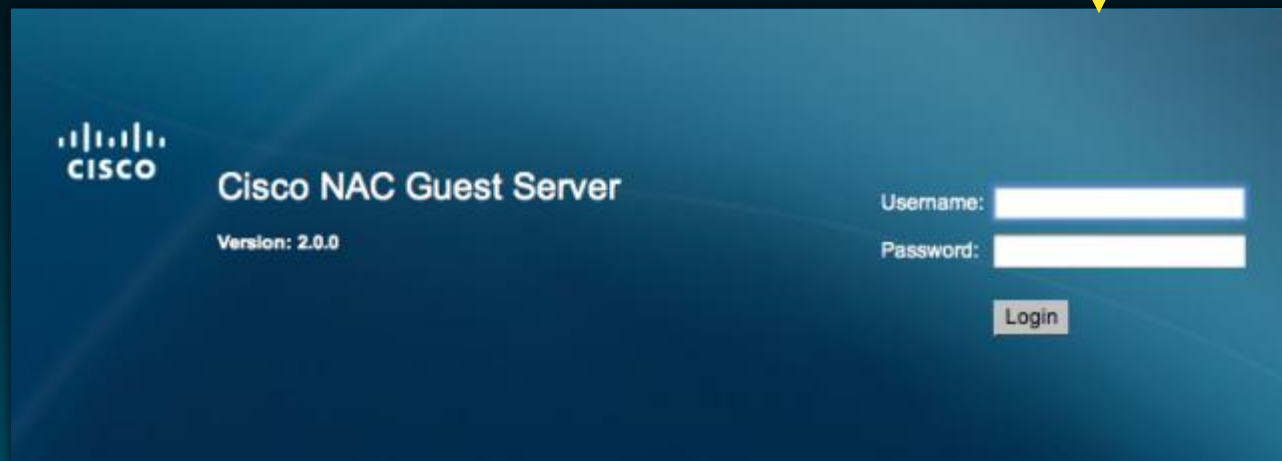
Local Database


Active Directory

LDAP

RADIUS

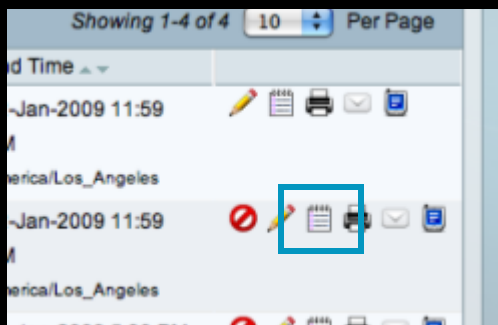
Kerberos


Cisco NAC Guest Server
 Version: 2.0.0

Username:
 Password:

Detailed Guest Audit Reporting



- **When** they logged in
- **Where** they logged in
- The guest's **address**
- **What** they did
- What was **allowed**
- What was **disallowed**

Detailed Login Report for: jsmith@mycustomer.com Showing 1-1 of 1 10 Per Page

NAS IP Address	Users IP Address	Logged In	Logged Out	Duration
192.168.137.20	1.0.0.7	12-Jan-2009 9:31 AM	12-Jan-2009 9:45 AM	14 Minute(s)

Page 1 of 1

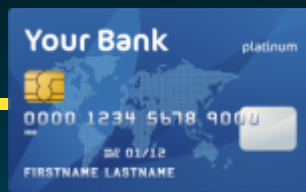
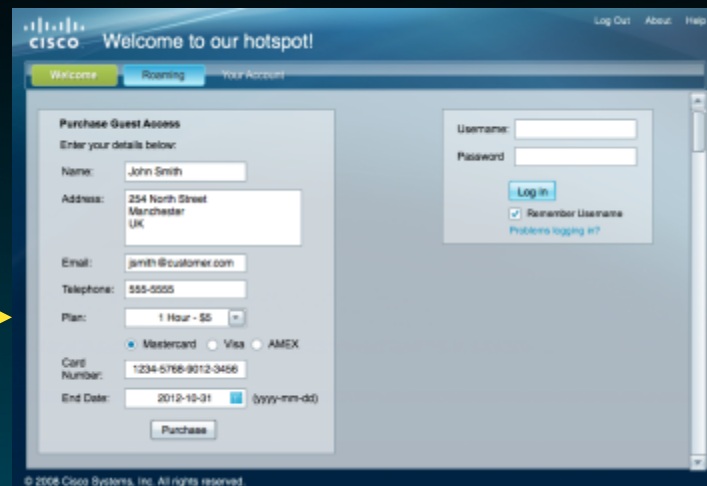
Activity Log: jsmith@mycustomer.com Showing 1-3 of 3 10 Per Page

Date/Time	Device	Message
12-Jan-2009 9:31 AM	192.168.137.20	1.0.0.7 TCP connection permitted to 198.133.219.25:80
12-Jan-2009 9:31 AM	192.168.137.20	1.0.0.7 accessed URL http://www.cisco.com
12-Jan-2009 9:32 AM	192.168.137.20	1.0.0.7 TCP connection denied to 204.65.34.23:4662

Page 1 of 1

Billing for Internet Access

- Billing support via credit card against Internet payment gateways
- Pregenerated accounts for scratch cards, handouts, etc.
- All delivered by built-in portal with full HTML customization



CISCO