Network Admission Control – Part I (NAC Appliance)

Ricky Elias

Security Architect

Advanced Technology (Security)

relias@cisco.com

Agenda

- NAC Design & Deployment
  - Building Blocks & Deployment Options
  - Mapping Policy into User Roles and Security Requirements
  - Managing Non-PC Devices & Guest Users
- Q&A

The Need for Differentiated Network Access

Corporate Employees

- Need internal network access
- User identities are usually known
- Device support
- May be further divided in separate internal groups

Contractors/ Consultants

- Need restricted internal access
  - Printers
  - File shares
  - Specific applications
- Internet access
- Possible Device support

Guests Users

- Internet access only
- No need to access internal systems
- Segment access completely
- Unsupported devices

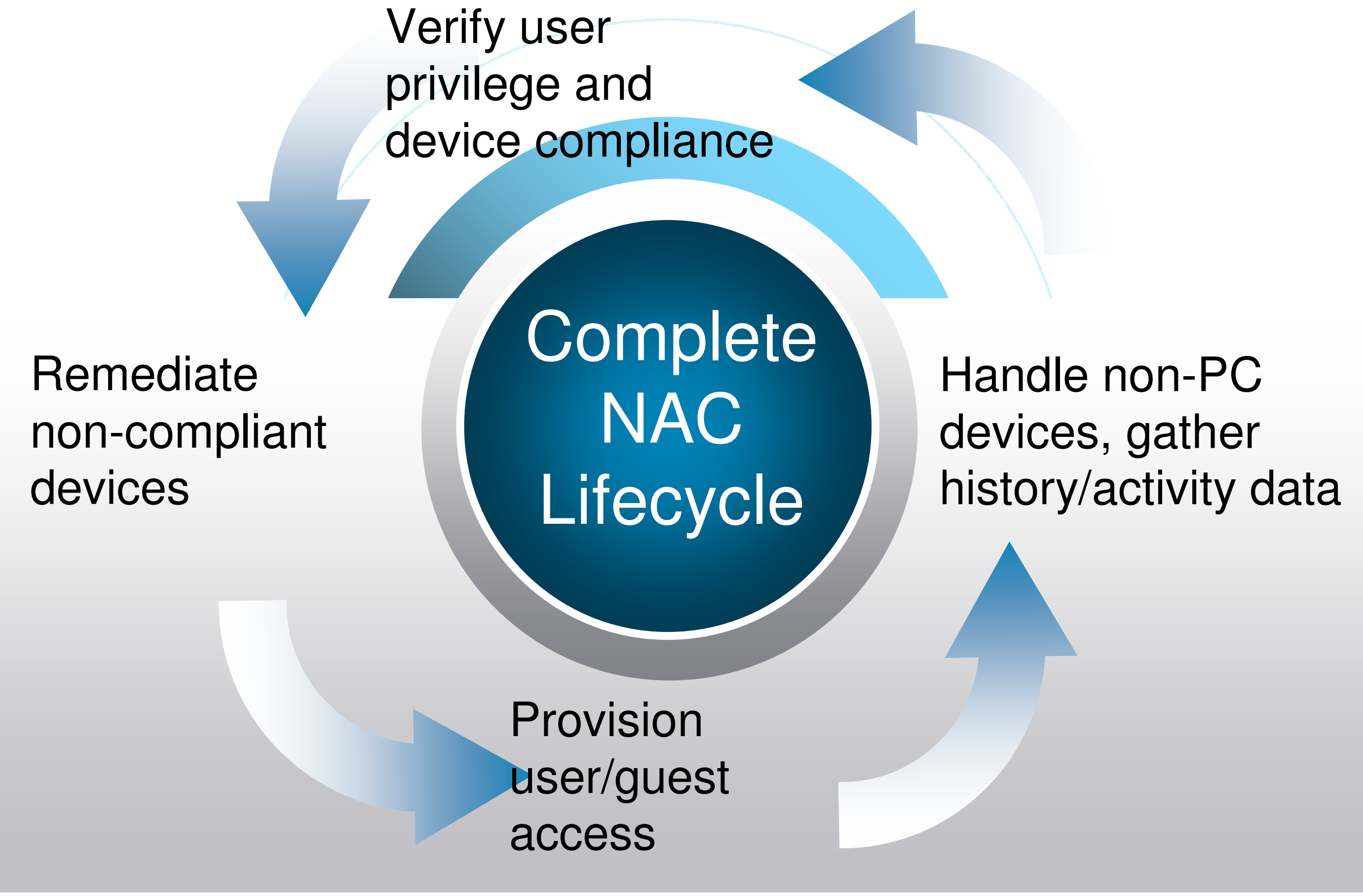
One solution to control all user types

Full Access
Full Policies

Internet Only
Basic Policies

NAC Functions Defined

Ensuring role-based access and endpoint security policy compliance



Complete NAC Lifecycle

Verify user privilege and device compliance

Handle non-PC devices, gather history/activity data

Provision user/guest access

Remediate non-compliant devices

Cisco NAC Key Components

NAC Manager and Server (Required)

NAC Manager

Centralized management, configuration, reporting, and policy store

NAC Server

Posture, services and enforcement

Ruleset Updates

Scheduled automatic rulesets for anti-virus, Microsoft hot-fixes and other applications

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)

Clean Access Agent

by Cisco Systems

Version 3.4.0

Copyright 2004 Cisco Systems, Inc.

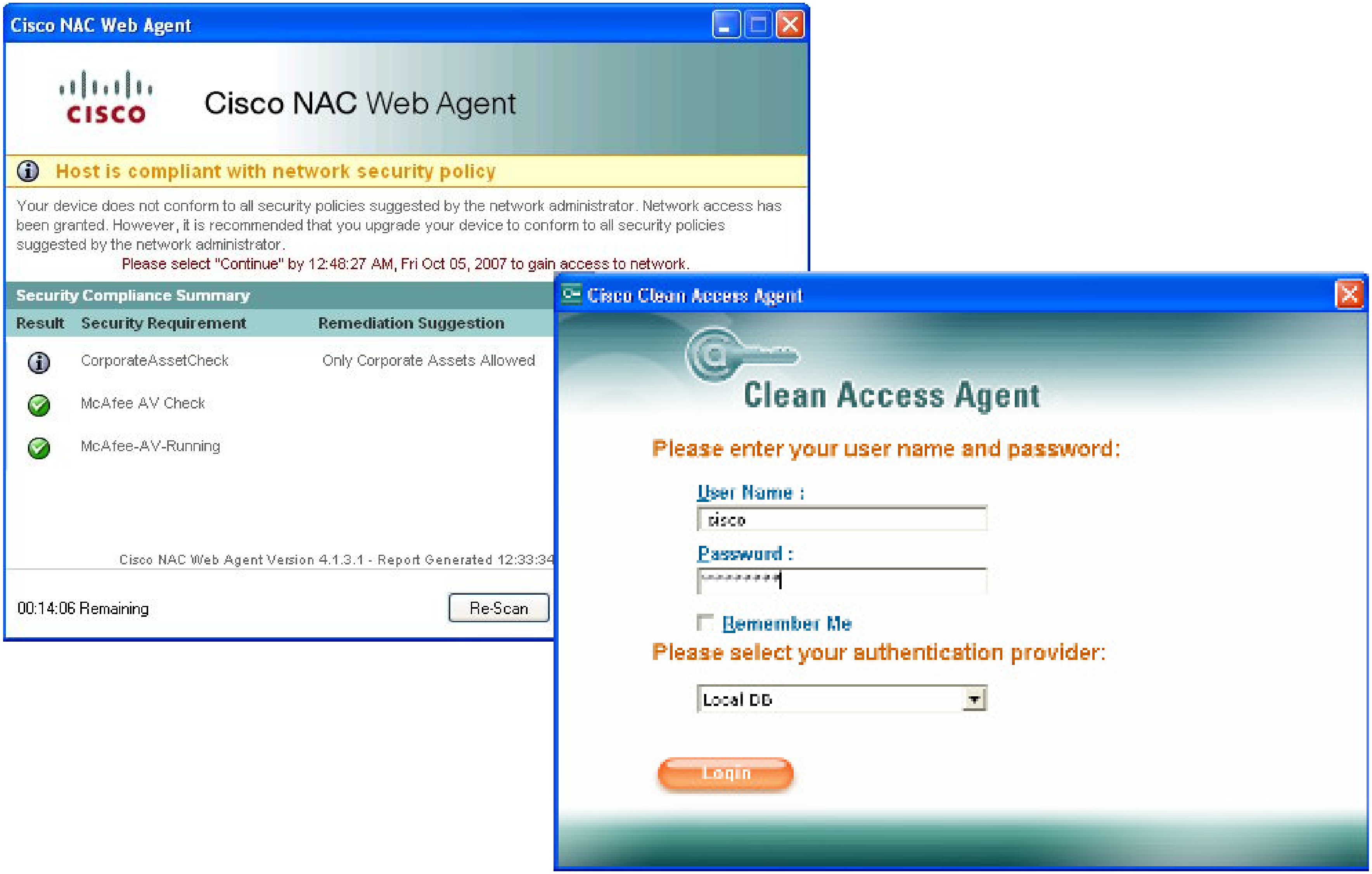
NAC Agent

No-cost client: Persistent, dissolvable, or web

802.1x Supplicant

CSSC or Vista embedded supplicant

Agent Options: Web and Persistent



Cisco NAC Web Agent

Cisco NAC Web Agent

ⓘ Host is compliant with network security policy

Your device does not conform to all security policies suggested by the network administrator. Network access has been granted. However, it is recommended that you upgrade your device to conform to all security policies suggested by the network administrator.

Please select "Continue" by 12:48:27 AM, Fri Oct 05, 2007 to gain access to network.

Security Compliance Summary

Result	Security Requirement	Remediation Suggestion
ⓘ	CorporateAssetCheck	Only Corporate Assets Allowed
✓	McAfee AV Check	
✓	McAfee-AV-Running	

Cisco NAC Web Agent Version 4.1.3.1 - Report Generated 12:33:34

00:14:06 Remaining

Cisco Clean Access Agent

Clean Access Agent

Please enter your user name and password:

User Name : cisco

Password : ********

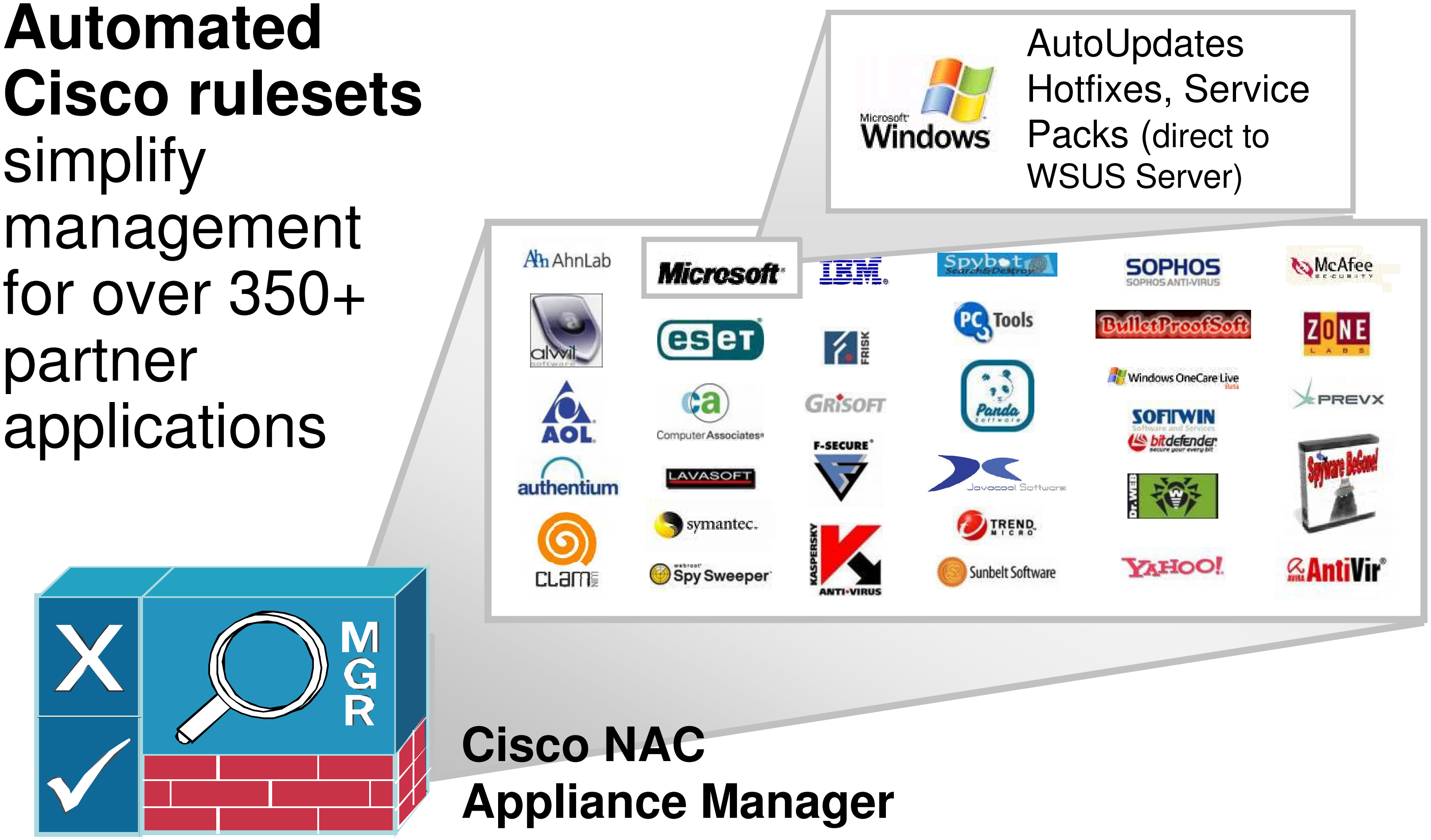
□ Remember Me

Please select your authentication provider:

Local DB

Automated Rulesets

Automated Cisco rulesets simplify management for over 350+ partner applications

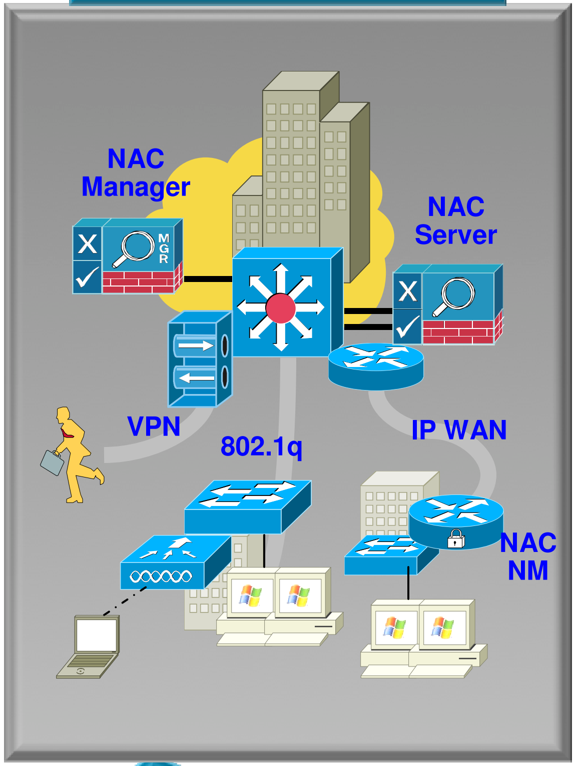


AutoUpdates Hotfixes, Service Packs (direct to WSUS Server)

Cisco NAC Appliance Manager

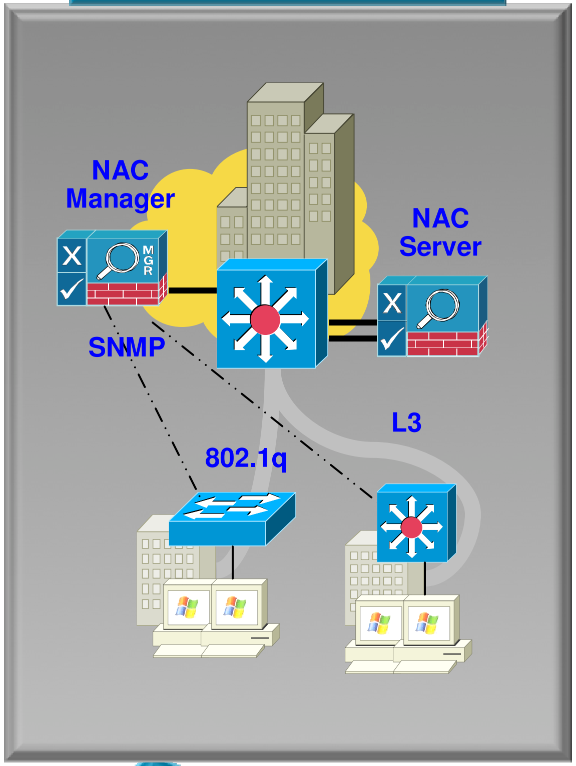
Flexible Deployment Options

In Band



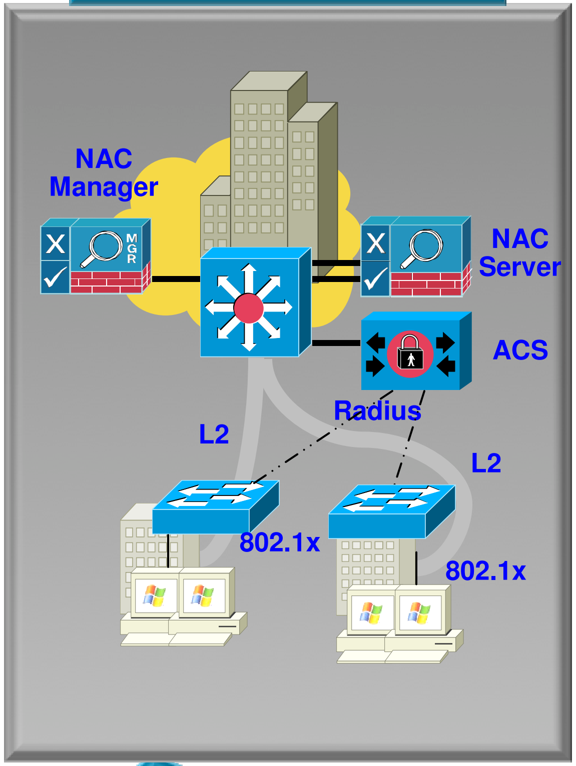
- VPN, wireless, campus, and remote LANs
- Enforcement via Appliance

Out of Band



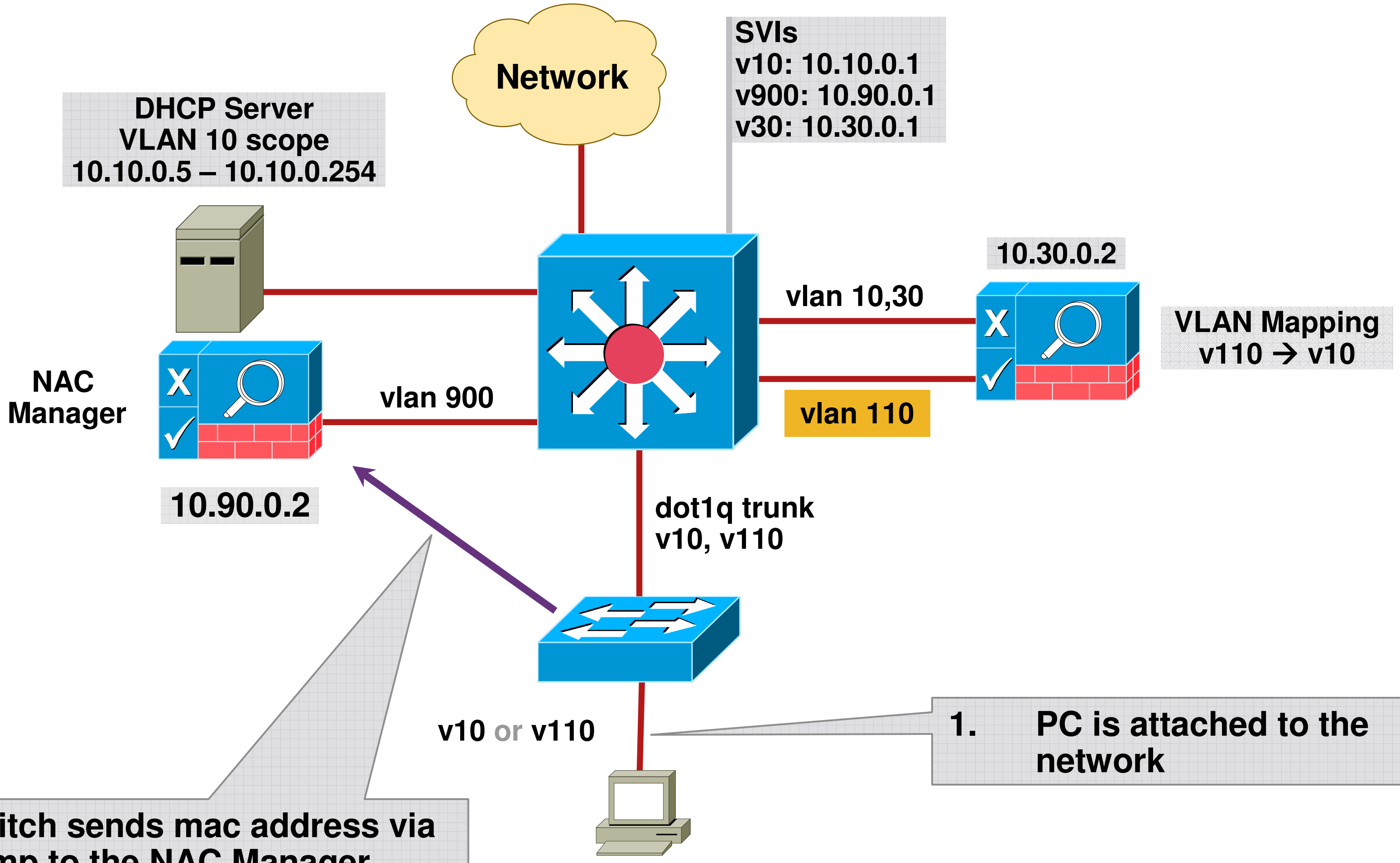
- Optimized for Cisco campus LANs (L2, L3)
- SNMP as control plane

RADIUS



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

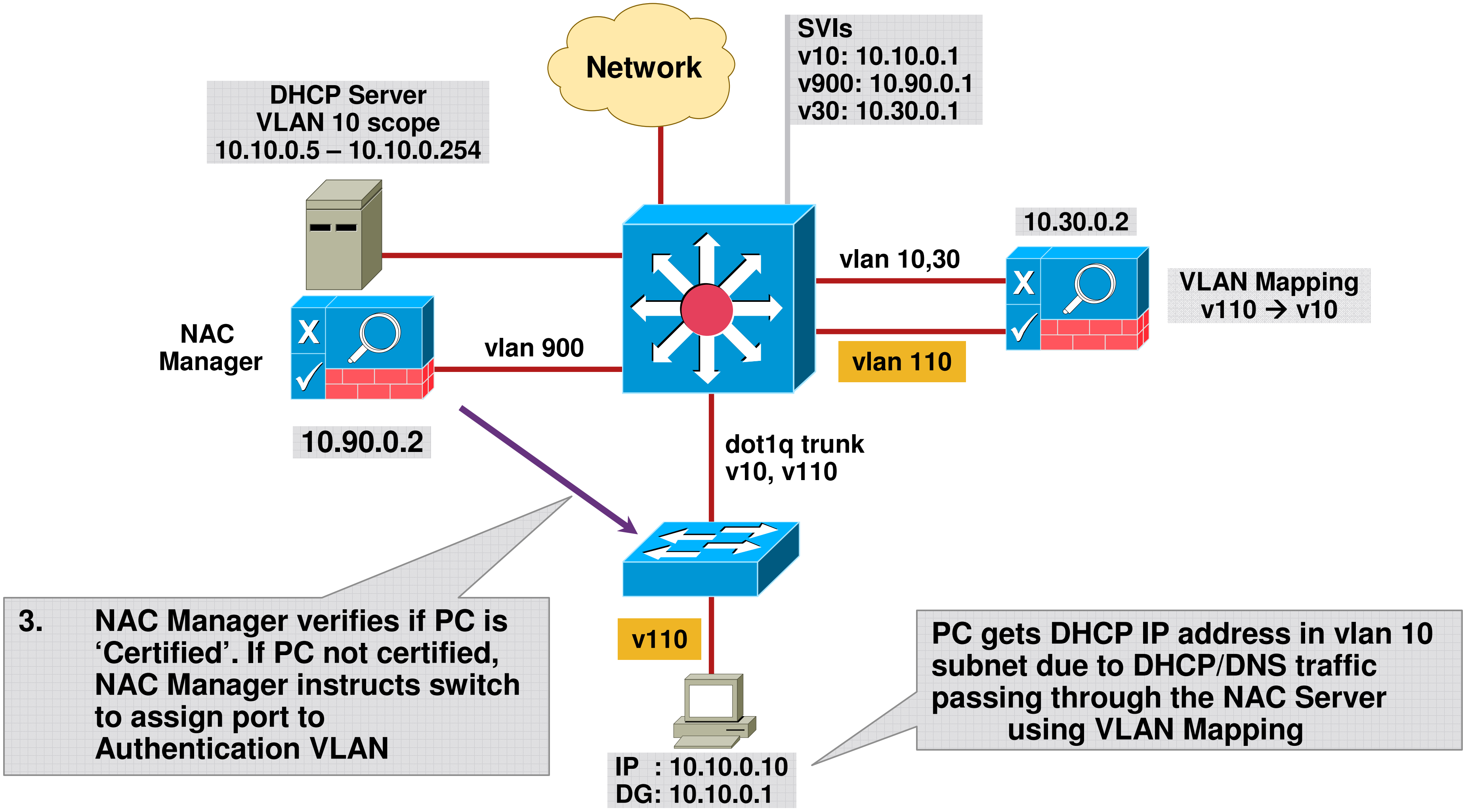
Out-of-Band Process Flow



1. PC is attached to the network

2. Switch sends mac address via snmp to the NAC Manager

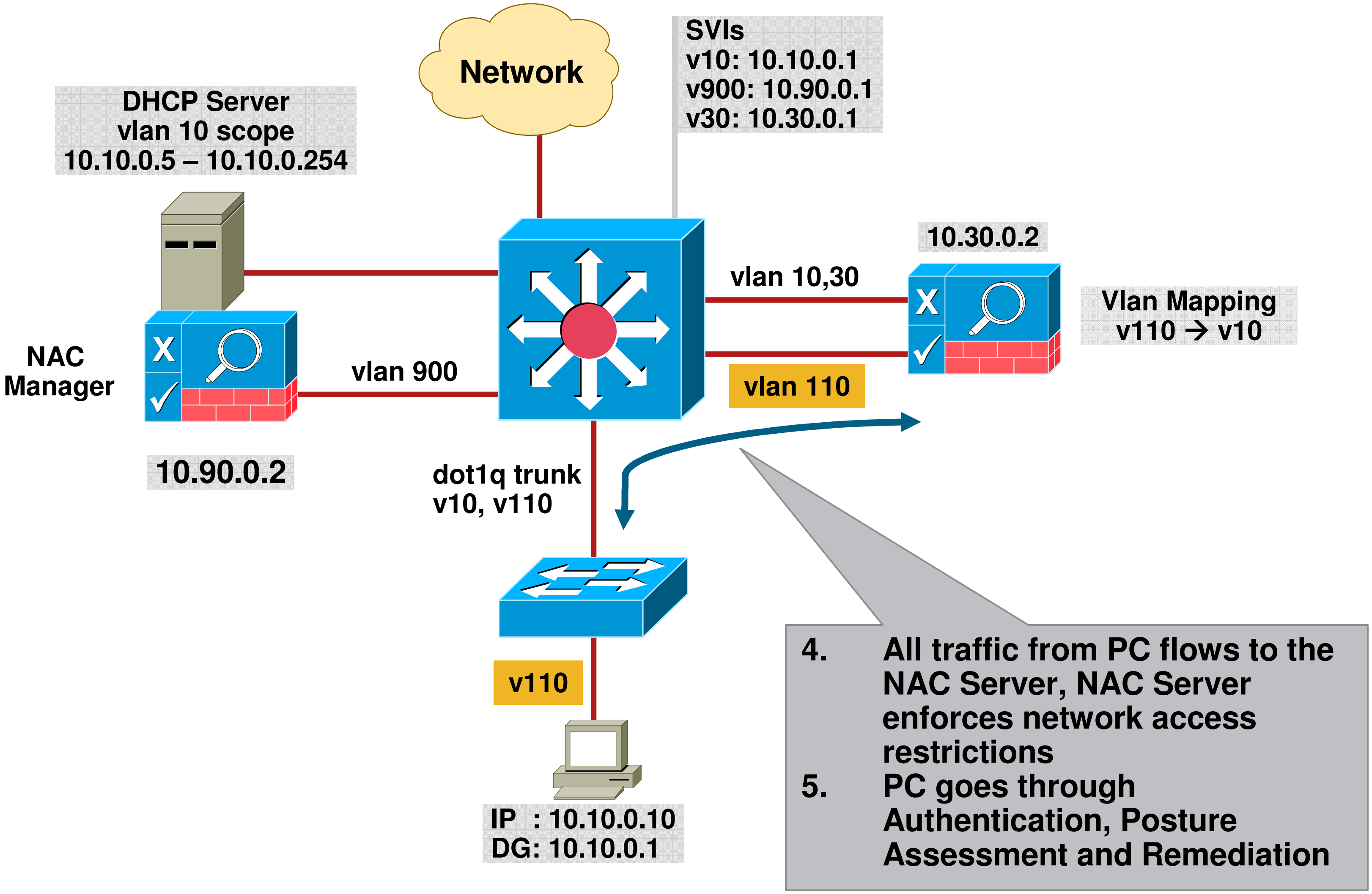
Out-of-Band Process Flow



3. NAC Manager verifies if PC is 'Certified'. If PC not certified, NAC Manager instructs switch to assign port to Authentication VLAN

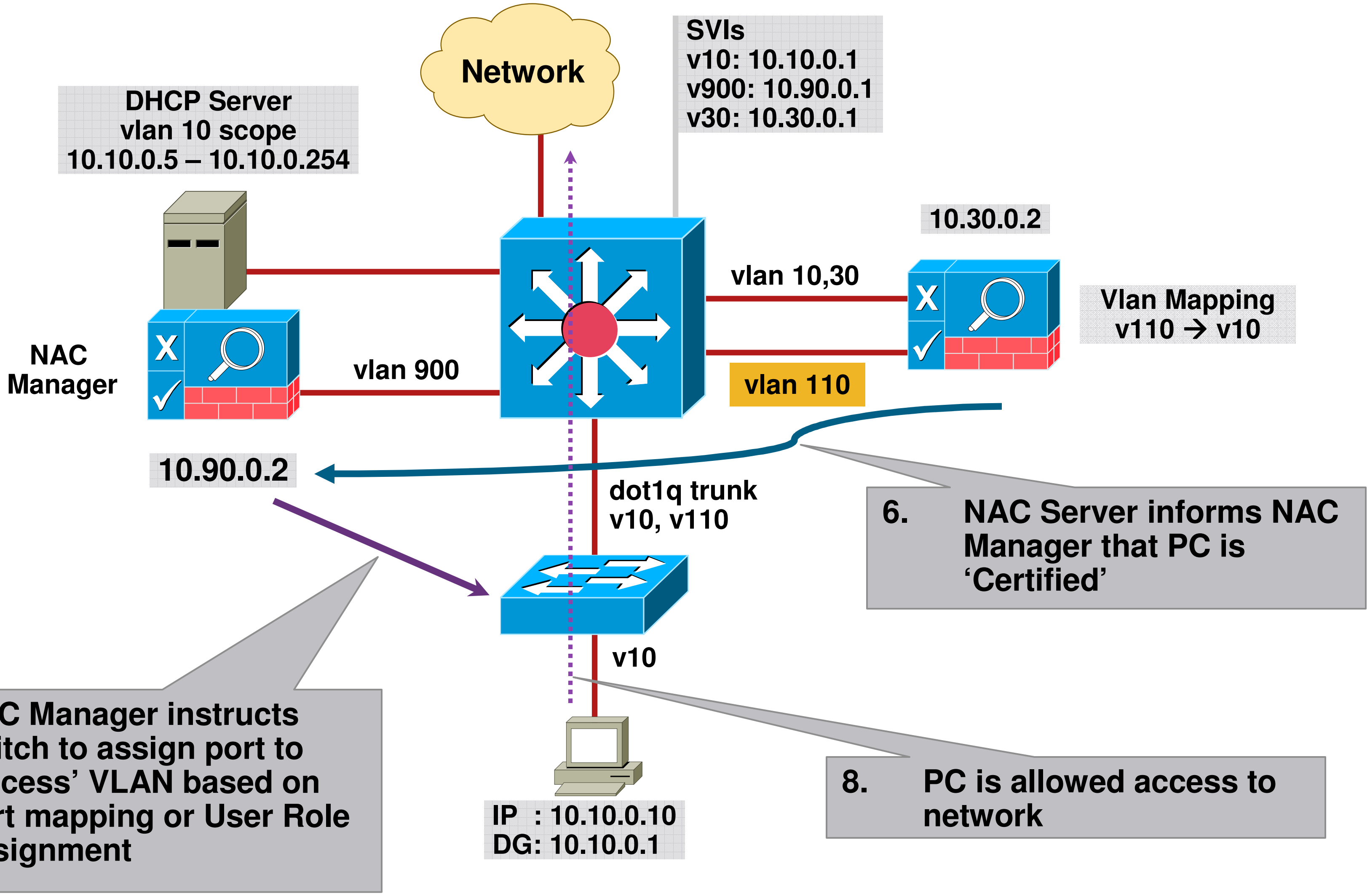
PC gets DHCP IP address in vlan 10 subnet due to DHCP/DNS traffic passing through the NAC Server using VLAN Mapping

Out-of-Band Process Flow



4. All traffic from PC flows to the NAC Server, NAC Server enforces network access restrictions
5. PC goes through Authentication, Posture Assessment and Remediation

Out-of-Band Process Flow



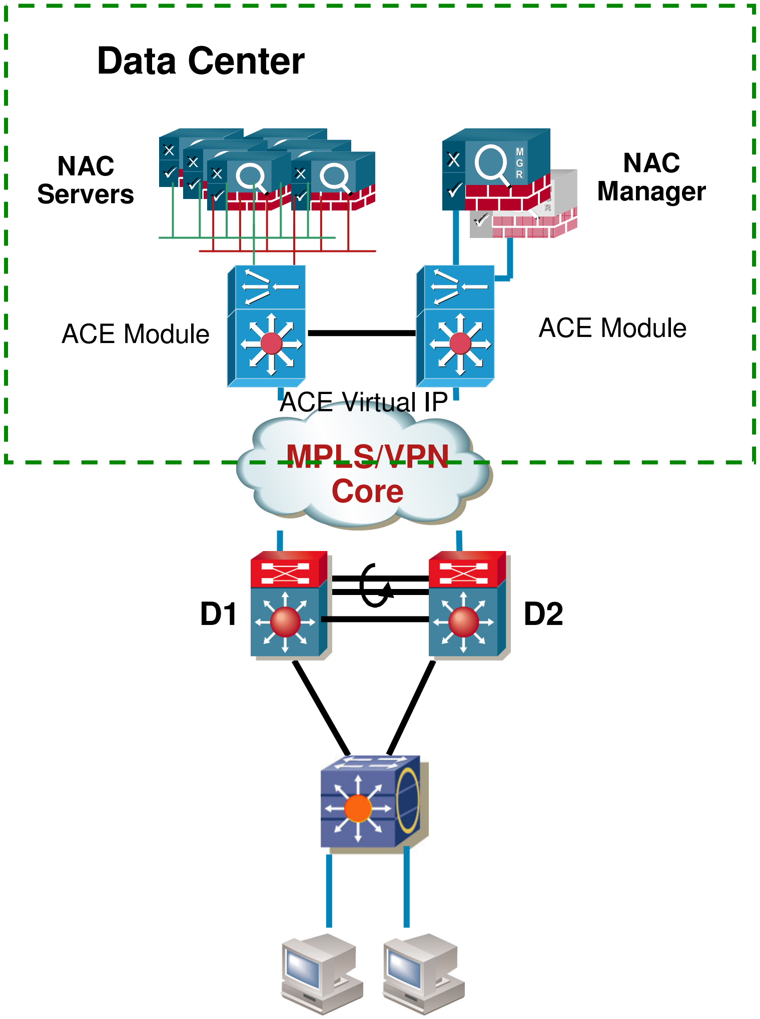
6. NAC Server informs NAC Manager that PC is 'Certified'

7. NAC Manager instructs switch to assign port to 'Access' VLAN based on Port mapping or User Role Assignment

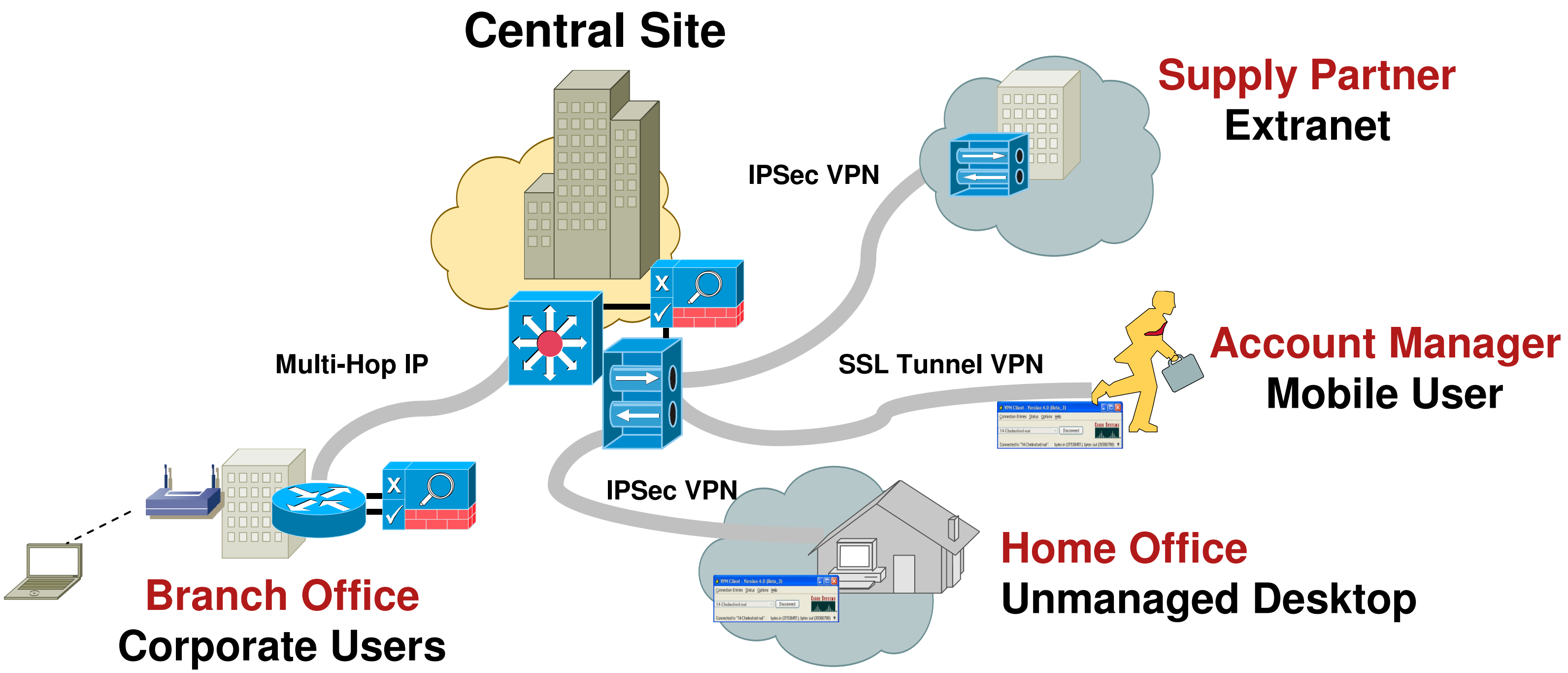
8. PC is allowed access to network

Virtualization using Load-Balanced Design

- All devices accessing the network must be checked for compliance before full network access is granted
- MPLS VPN for NAC Authentication networks
  - Allows NAC Authentication networks distributed across campus to all be isolated back to central NAC Server Farm
- Traffic from client in Auth VLAN can be sent to directed to ACE Virtual IP using
  - MPLS VPN
  - PBRs
  - VRF Lite
  - Discovery Host (Agent only)
- Cisco Application Control Engine (ACE) Module
  - Perform intelligent load-balancing and scaling of centralized NAC design

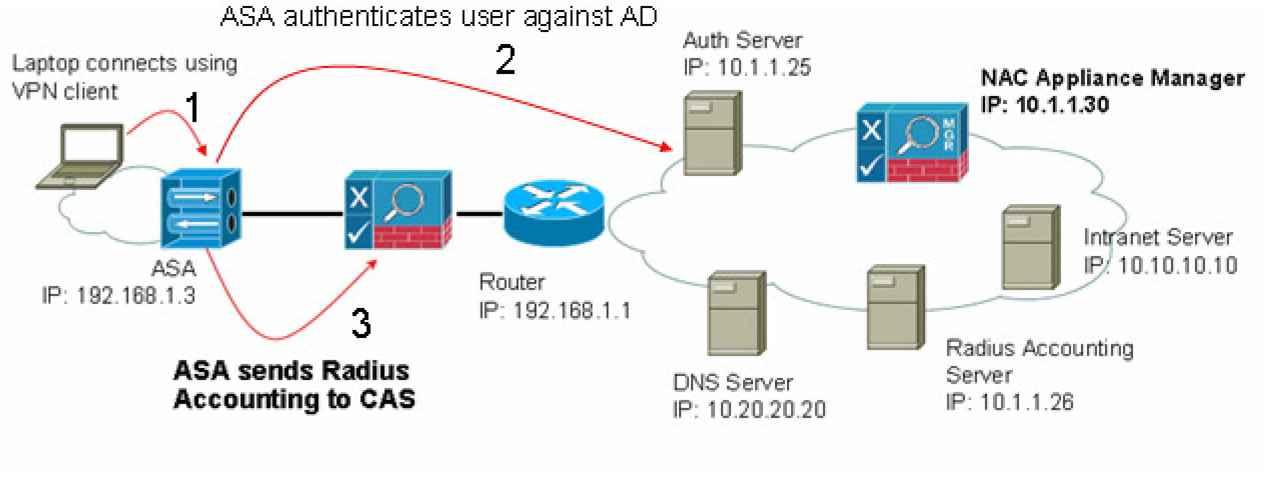


NAC Appliance for Remote Users



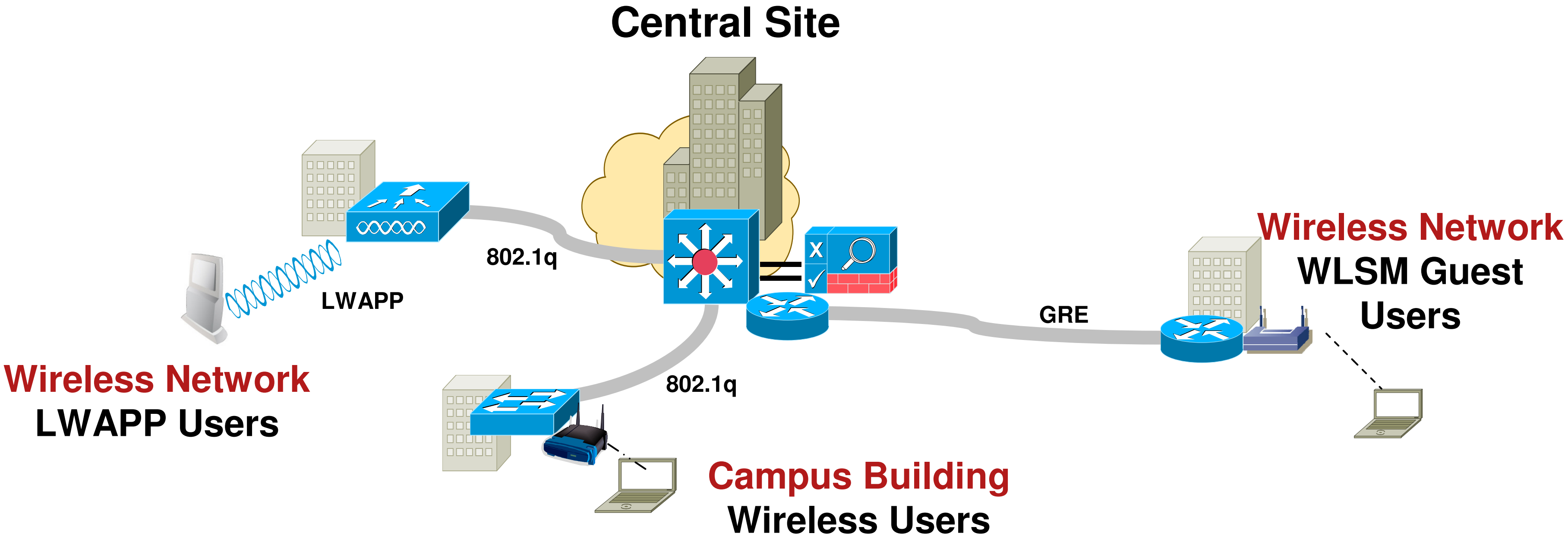
Features	Benefits
▪ Supports IPSec and SSL Tunnel VPNs ▪ Supports site-to-site VPNs ▪ Supports VPN user sign-on	▪ Extends policy enforcement and compliance to remote access and VPN users ▪ Extends enforcement to site-to-site VPN partners ▪ Leverages VPN sign-on for single-sign-on

Deploy VPN with Single Sign On (SSO)



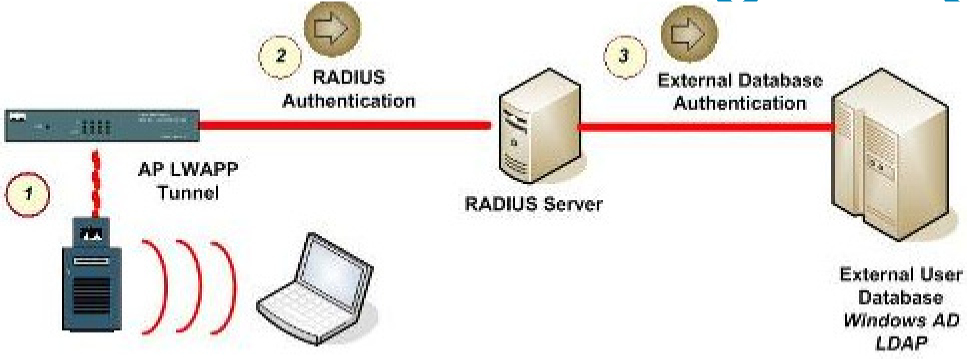
- User logs in using IPSEC or SSL VPN client.
- VPN server sends Radius Accounting packet to NAC Server
- NAC Server performs SSO for that user based on the Accounting packet
- NAC Server can optionally be configured to forward that Accounting packet to another Radius server

Cisco NAC for Wireless Users



Features	Benefits
▪ Supports 802.1q trunking ▪ Supports thin or thick wireless 802.11 APs ▪ Supports Wireless user single-sign-on	▪ Enables central deployment mode ▪ Extends enforcement to any wireless networks ▪ End user devices can be several hops away ▪ Leverages 802.1x sign-on for single-sign-on

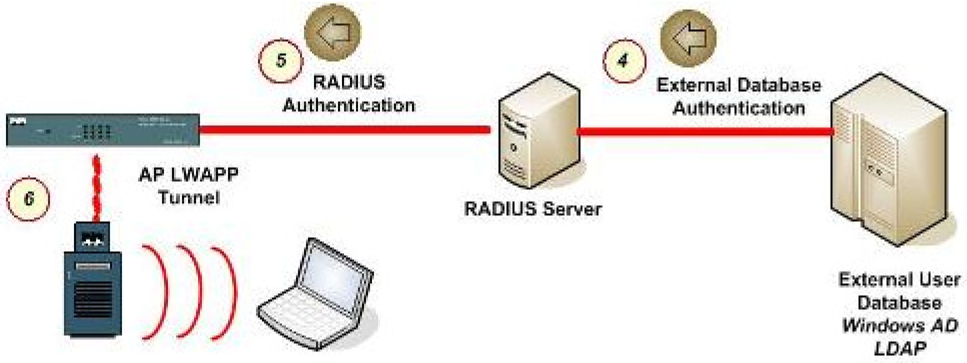
Wireless with Single Sign On (SSO)

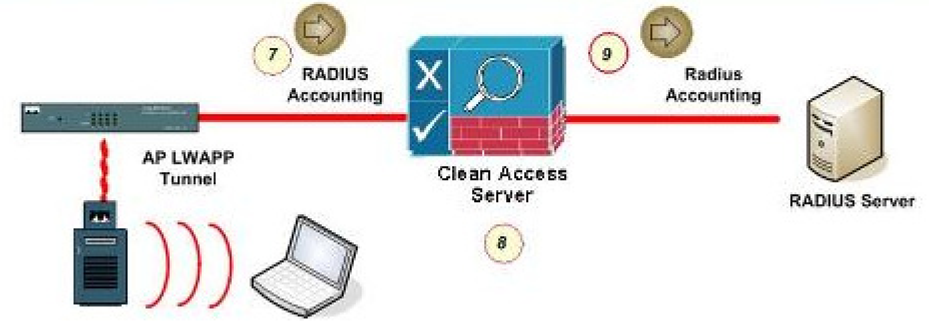


WLC performs Authentication

WLC sends Radius

Accounting to NAC Server





Clean Access Manager: Checks, Rules, and Roles

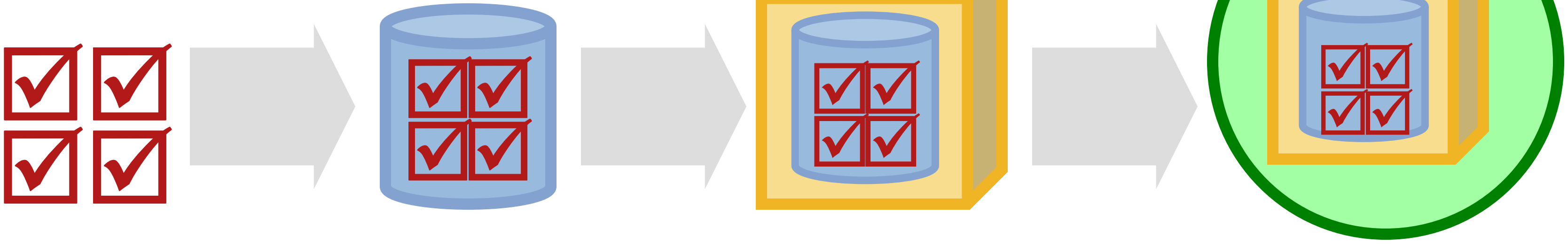
Clean Access posture validation is a hierarchical process with either pre-loaded or custom profiles

CHECKS
assess the state of a file, application, service, or registry key

RULES
contain single or multiple **Checks**

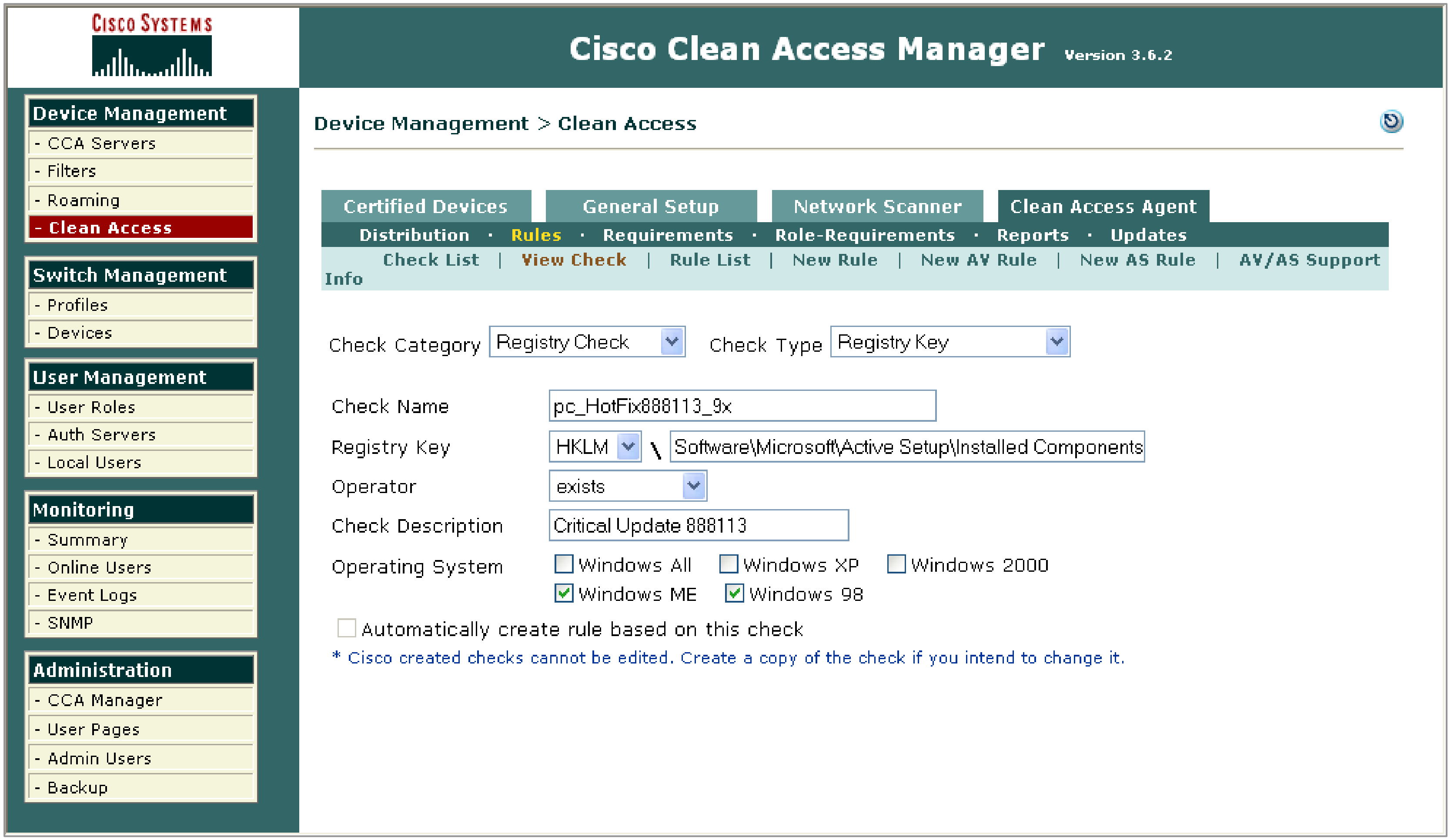
REQUIREMENTS
contain single or multiple **Rules**

ROLES
have one or more **Requirements**



Clean Access Manager: Checks, Rules, and Roles

Registry Key check for a Windows Hotfix



Device Management > Clean Access

Check Category: Registry Check

Check Type: Registry Key

Check Name: pc_HotFix888113_9x

Registry Key: HKLM \ Software\Microsoft\Active Setup\Installed Components

Operator: exists

Check Description: Critical Update 888113

Operating System: □ Windows All □ Windows XP □ Windows 2000 ☑ Windows ME ☑ Windows 98

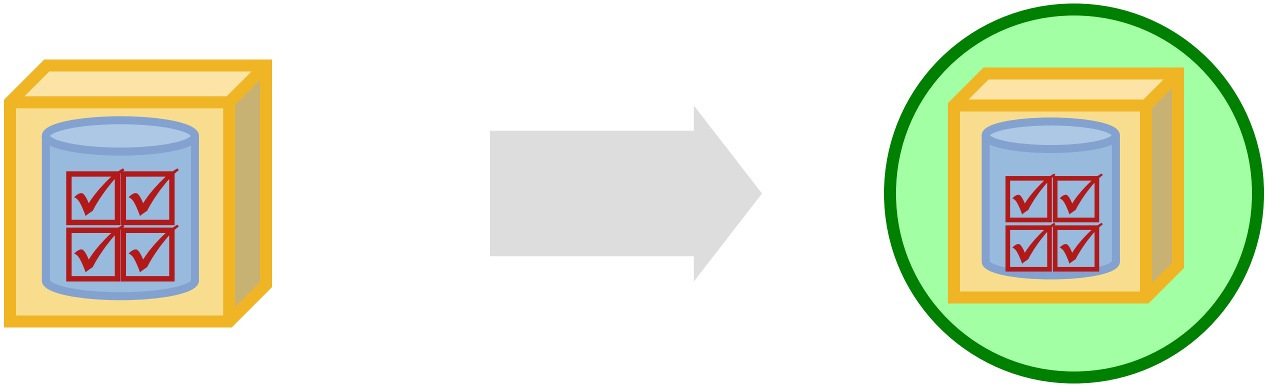
□ Automatically create rule based on this check

* Cisco created checks cannot be edited. Create a copy of the check if you intend to change it.

Clean Access Manager: Checks, Rules, and Roles

REQUIREMENTS
tie remediation actions directly to a rule

ROLES
determine which rules apply and what security filters are applied



Remediation methods include:

- **File Distribution** (“Download antispyware.exe”)
- **Link Distribution** (“windowsupdate.com”)
- **Local Check** (text instructions or messages)
- **Definition Update** (direct launch of supported AV or AS)
- **Launch WSUS and change its settings**
- **Launch Patch management software** (SMS, Altiris etc)

Option to dynamically assign VLANs

Apply individual URL redirection per role, as well as Acceptable Usage Policies, User Pages, and more

Agenda

- NAC Design & Deployment

  Building Blocks & Deployment Options

  Mapping Policy into User Roles and Security Requirements

  Managing Non-PC Devices & Guest Users

- Q&A

Identity Based Access Control (Device)

Printers

Fax Machines

Video Conferencing Stations

IP Phones

Hubs

IP Cameras

Wireless APs

Managed UPS

Cash Registers

Medical Imaging Machines

Alarm Systems

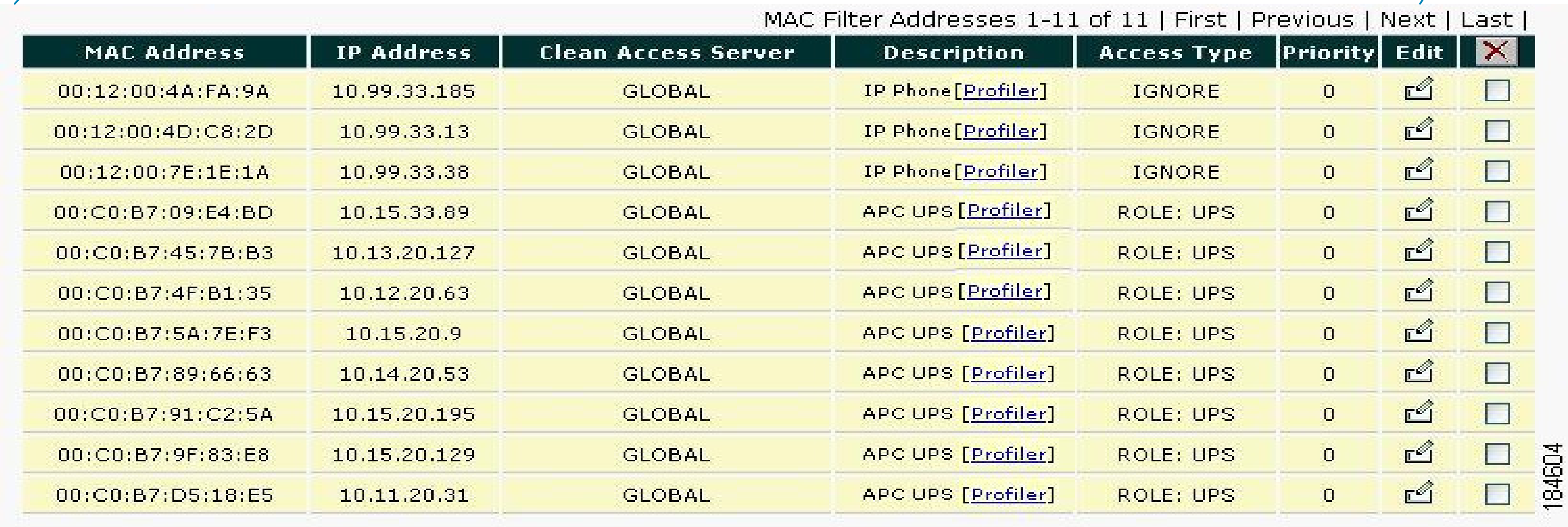
Turnstiles

HVAC Systems

RMON Probes

Vending Machines

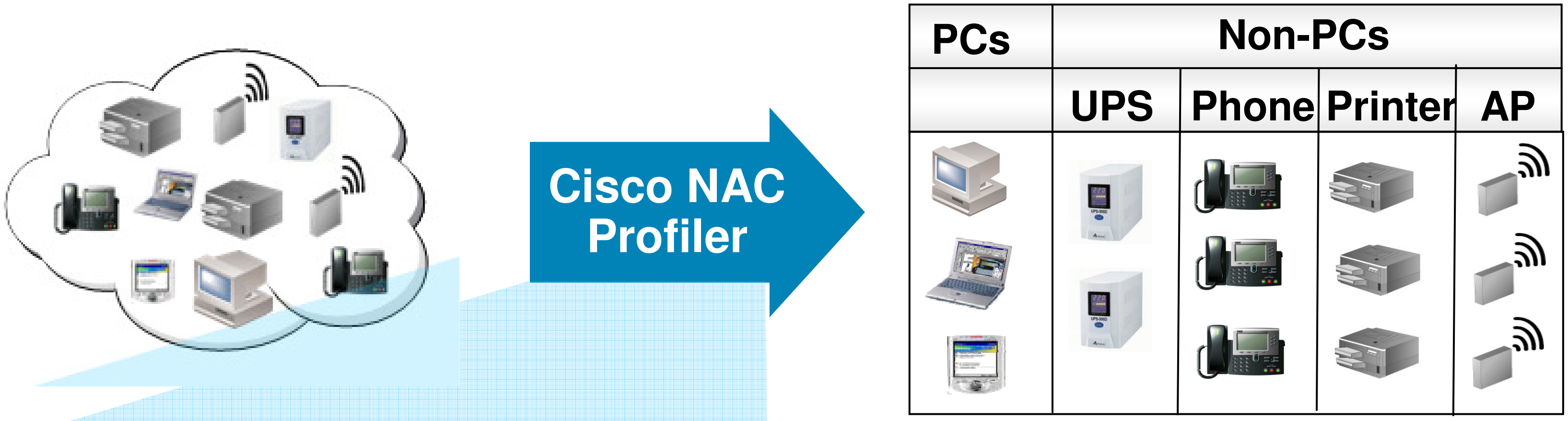
. . . and many others



MAC Filter Addresses 1-11 of 11 | First | Previous | Next | Last |

MAC Address	IP Address	Clean Access Server	Description	Access Type	Priority	Edit	☒
00:12:00:4A:FA:9A	10.99.33.185	GLOBAL	IP Phone[Profiler]	IGNORE	0	✎	□
00:12:00:4D:C8:2D	10.99.33.13	GLOBAL	IP Phone[Profiler]	IGNORE	0	✎	□
00:12:00:7E:1E:1A	10.99.33.38	GLOBAL	IP Phone[Profiler]	IGNORE	0	✎	□
00:C0:B7:09:E4:BD	10.15.33.89	GLOBAL	APC UPS [Profiler]	ROLE: UPS	0	✎	□
00:C0:B7:45:7B:B3	10.13.20.127	GLOBAL	APC UPS [Profiler]	ROLE: UPS	0	✎	□
00:C0:B7:4F:B1:35	10.12.20.63	GLOBAL	APC UPS [Profiler]	ROLE: UPS	0	✎	□
00:C0:B7:5A:7E:F3	10.15.20.9	GLOBAL	APC UPS [Profiler]	ROLE: UPS	0	✎	□
00:C0:B7:89:66:63	10.14.20.53	GLOBAL	APC UPS [Profiler]	ROLE: UPS	0	✎	□
00:C0:B7:91:C2:5A	10.15.20.195	GLOBAL	APC UPS [Profiler]	ROLE: UPS	0	✎	□
00:C0:B7:9F:83:E8	10.15.20.129	GLOBAL	APC UPS [Profiler]	ROLE: UPS	0	✎	□
00:C0:B7:D5:18:E5	10.11.20.31	GLOBAL	APC UPS [Profiler]	ROLE: UPS	0	✎	□

Cisco NAC Profiler: Secure Automation



Discovery

Endpoint Profiling

Discover all network endpoints by type and location

Maintain real time and historical contextual data for all endpoints

Monitoring

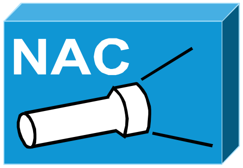
Behavior Monitoring

Monitor the state of the network endpoints

Detect events such as MAC spoofing, port swapping, etc.

Automated process populates devices into the NAC Manager; and subsequently, into appropriate NAC policy

Cisco NAC Profiler Components



NAC Profiler Server

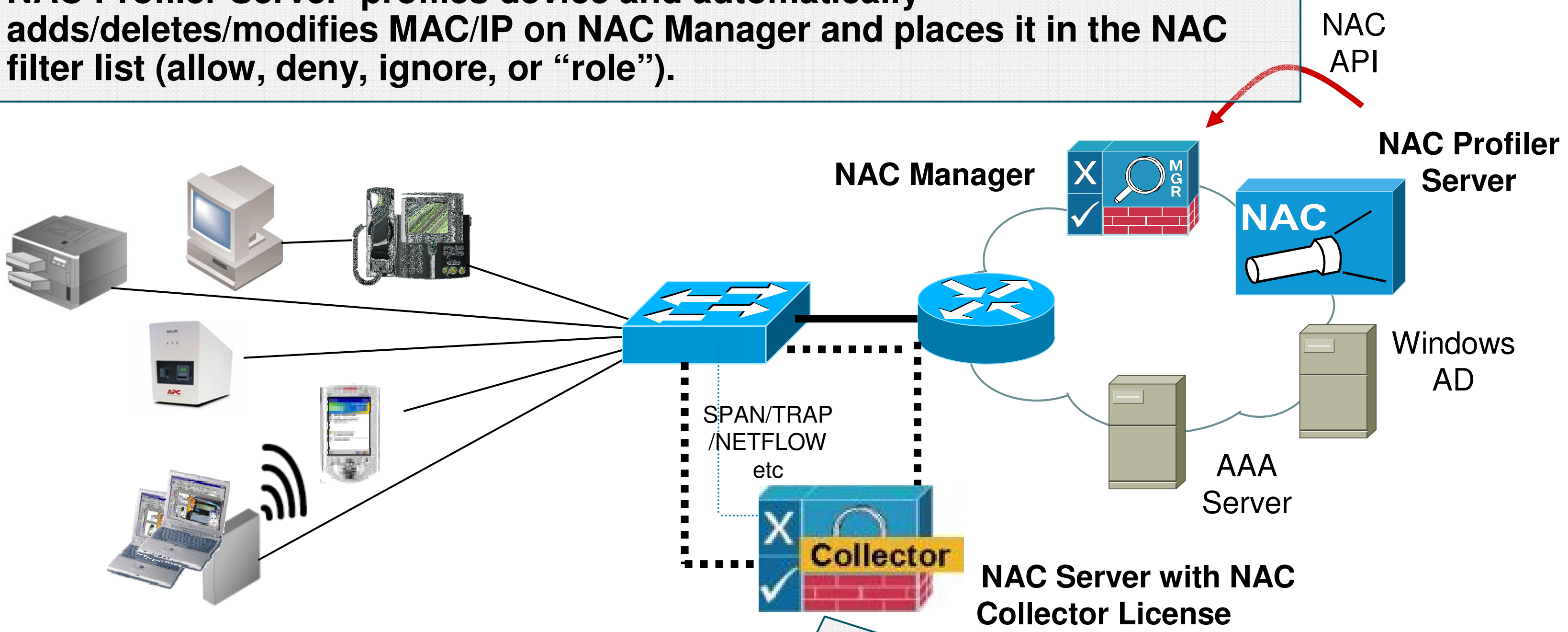
Aggregates and classifies data from Collectors and manages database of endpoint information. Updates the Cisco NAC Manager (CAM) list to place end points into appropriate access Roles.

NAC Collector

Gathers information about endpoints using SNMP, Netflow, DHCP, and active profiling

How It Works - NAC Profiler

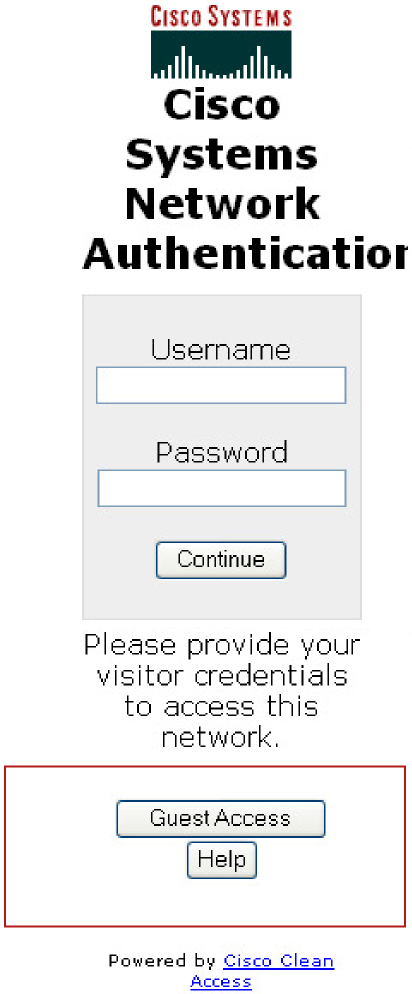
3. **NAC Profiler Server profiles device and automatically adds/deletes/modifies MAC/IP on NAC Manager and places it in the NAC filter list (allow, deny, ignore, or "role").**



1. **NAC Collector aggregates collection of relevant data (e.g. phones, printers, badge reader, modalities) and send to NAC Profiler Server**

2. **NAC Collector continuously monitor behavior of profiled devices (spoofing behavior) and updates Profiler Server**

Guest/Unmanaged Users



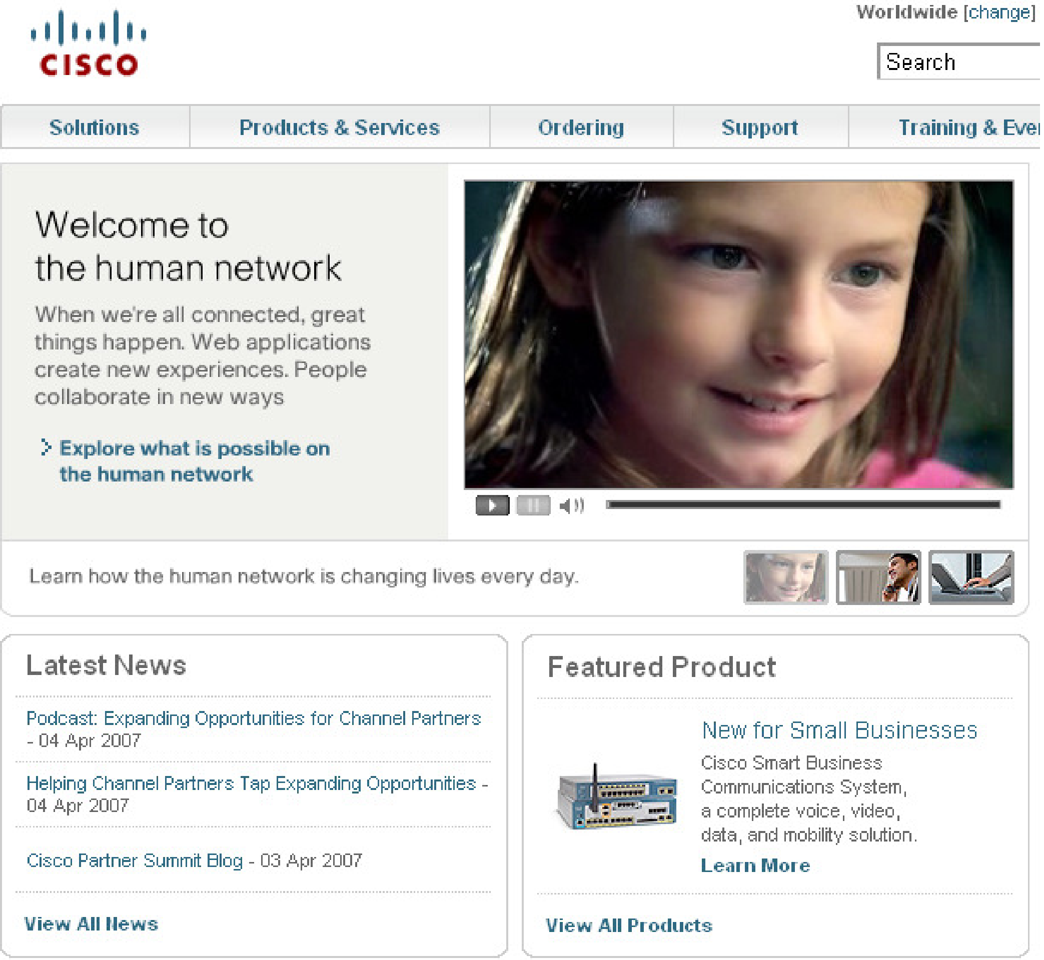
Cisco Systems Network Authenticatior

Username

Password

Please provide your visitor credentials to access this network.

Powered by Cisco Clean Access



Welcome to the human network

When we're all connected, great things happen. Web applications create new experiences. People collaborate in new ways

Explore what is possible on the human network

Learn how the human network is changing lives every day.

Latest News

Podcast: Expanding Opportunities for Channel Partners - 04 Apr 2007

Helping Channel Partners Tap Expanding Opportunities - 04 Apr 2007

Cisco Partner Summit Blog - 03 Apr 2007

View All News

Featured Product

New for Small Businesses

Cisco Smart Business Communications System, a complete voice, video, data, and mobility solution.

Learn More

View All Products

Cisco NAC Guest Access

Key Components

GUEST

The visitor who needs network access (usually internet only)

SPONSOR

The internal user who wants to be able to provide internet access to her guest

NETWORK ENFORCEMENT DEVICE

The device that authenticates the guest and grants network access

NAC GUEST SERVER

Enables sponsor to create guest account; audits; provisions account on network enforcement device

How It Works with – NAC Guest Access

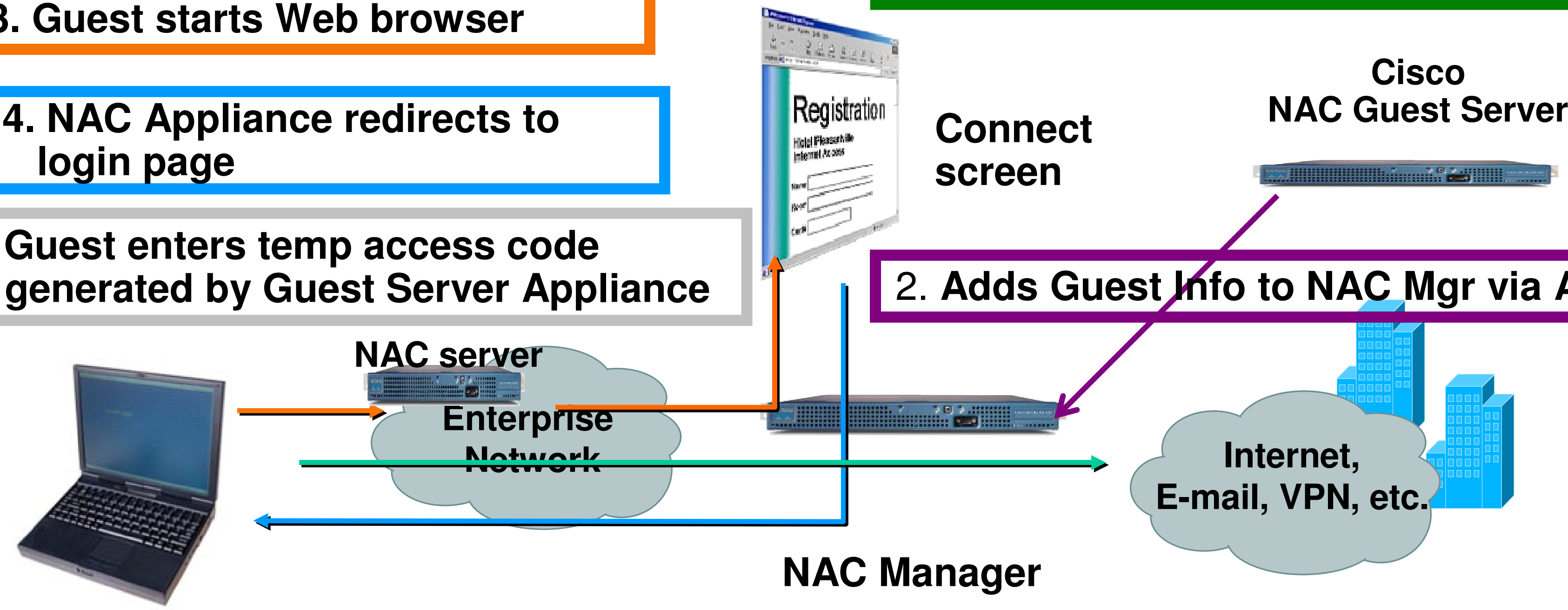
1. Employee creates account for Guest

2. Adds Guest Info to NAC Mgr via API

3. Guest starts Web browser

4. NAC Appliance redirects to login page

5. Guest enters temp access code generated by Guest Server Appliance



6. NAC Appliance put the user in the Specific Role

NAC Best Practices Strategy

Recommended best practices for success

- Aligned with business' pain points in order of priority

- "Bite-sized" stages for rolling out NAC

- Establish best practices for NAC deployment, then deepening NAC functions