Successful NAC Deployments

Thomas Howard

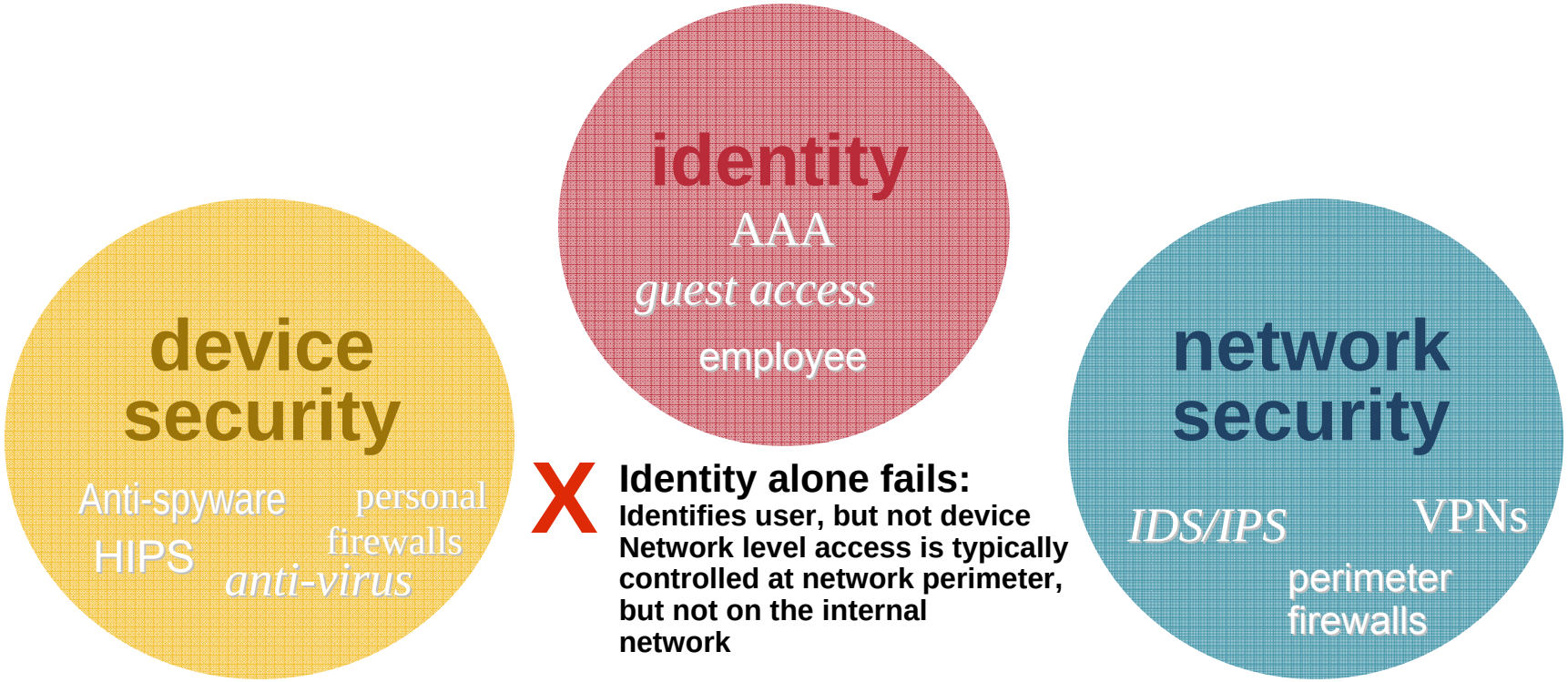
thomas@cisco.com

Security Solutions Engineer

Cisco Systems

Overview
Planning
Design
Implementation
Operation
Q&A

Traditional Security for the Network



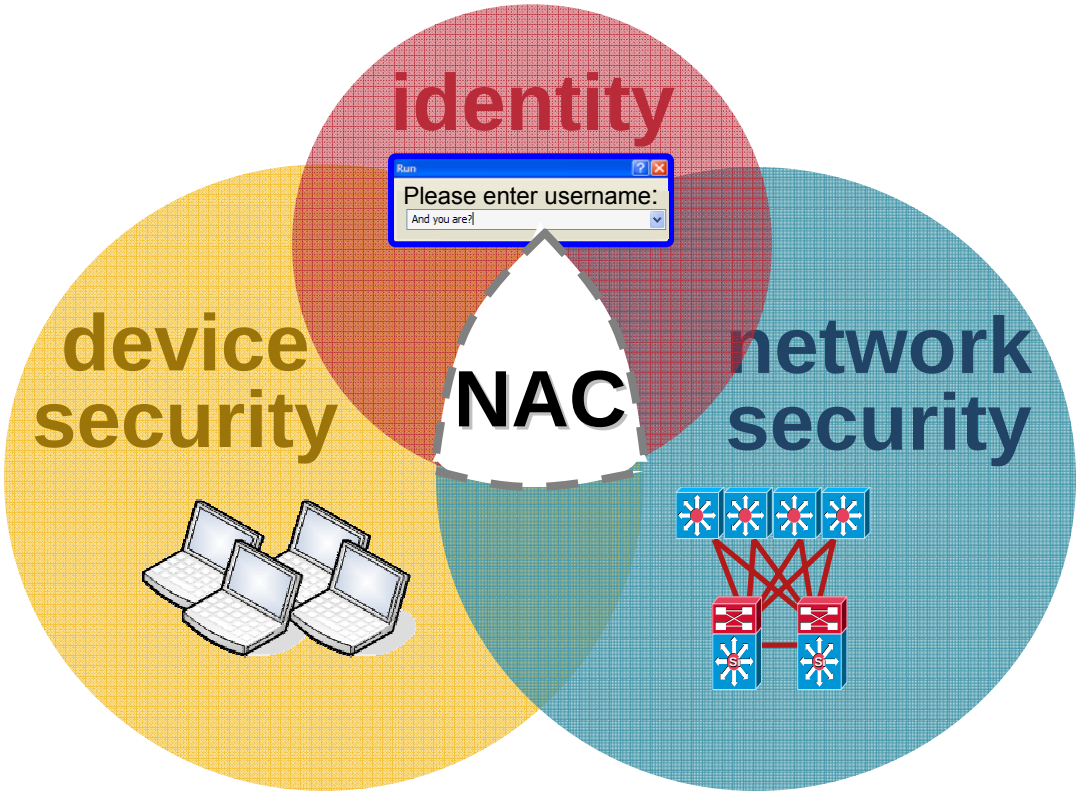
X Identity alone fails:
Identifies user, but not device
Network level access is typically controlled at network perimeter, but not on the internal network

X Endpoint security alone fails:
Most corporate assets have AV, but infections persist!
Host based apps are easily manipulated (even unintentionally)
Lag time between new viruses and anti-virus patch upgrade cycle
Non-corporate assets often do not meet security requirements

X Network security alone fails:
Firewalls cannot block legitimate ports
VPNs cannot block legitimate users
Detection often occurs after-the-fact
Difficult to implement access control if users are on the internal network

What Is Network Admission Control?

Network Admission Control (NAC) is a solution that uses the network infrastructure to ensure all devices seeking network access comply with an organization's security policy



Four Key Capabilities of NAC

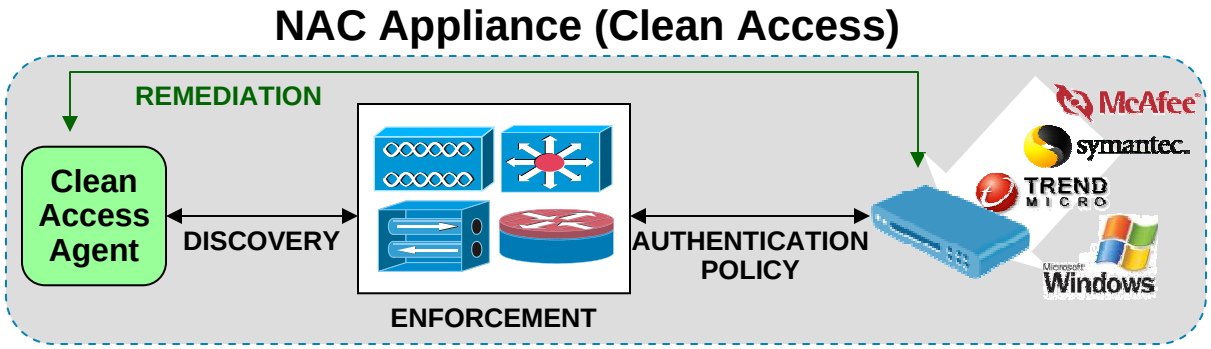
	SECURELY IDENTIFY DEVICE & USER	ENFORCE CONSISTENT POLICY	QUARANTINE AND REMEDIATE	CONFIGURE AND MANAGE
WHAT IT MEANS	**Uniquely identifies users and devices, and creates associations between the two**	**Ubiquitously assesses and enforces a policy across the entire network**	**Acts on posture assessment results, isolates device, and brings it into compliance**	**Easily creates comprehensive, granular policies that map quickly to user groups and roles**
WHY IT IS IMPORTANT	Associating users with devices enables granular enforcement in policies by role or group	Enforcement at the network level provides a solid foundation for holistic security	Quarantine critical to halt damage due to non-compliance; remediation addresses root cause problems	Policies that are easy to create and maintain lead to better system operations and adherence

A robust NAC solution must have all four capabilities.

Network Admission Control

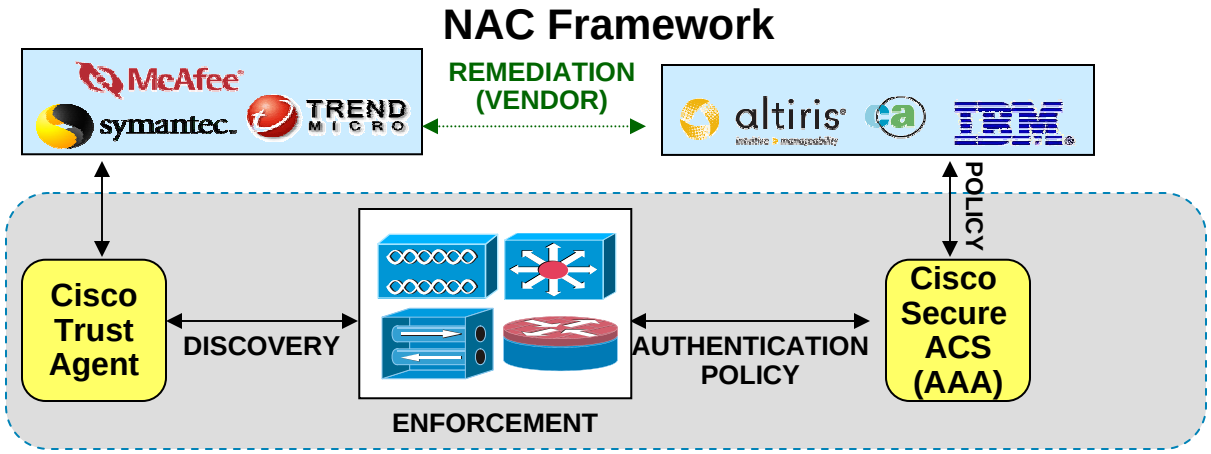
What is it? **NAC Controls access of all devices (managed, unmanaged, rogue)**

What does Cisco offer?



The best turnkey appliance product for all verticals

Address immediate pain-points with CCA



The best technological approach for Enterprise

Begin Long-Term Enterprise Solution with integrated product and services

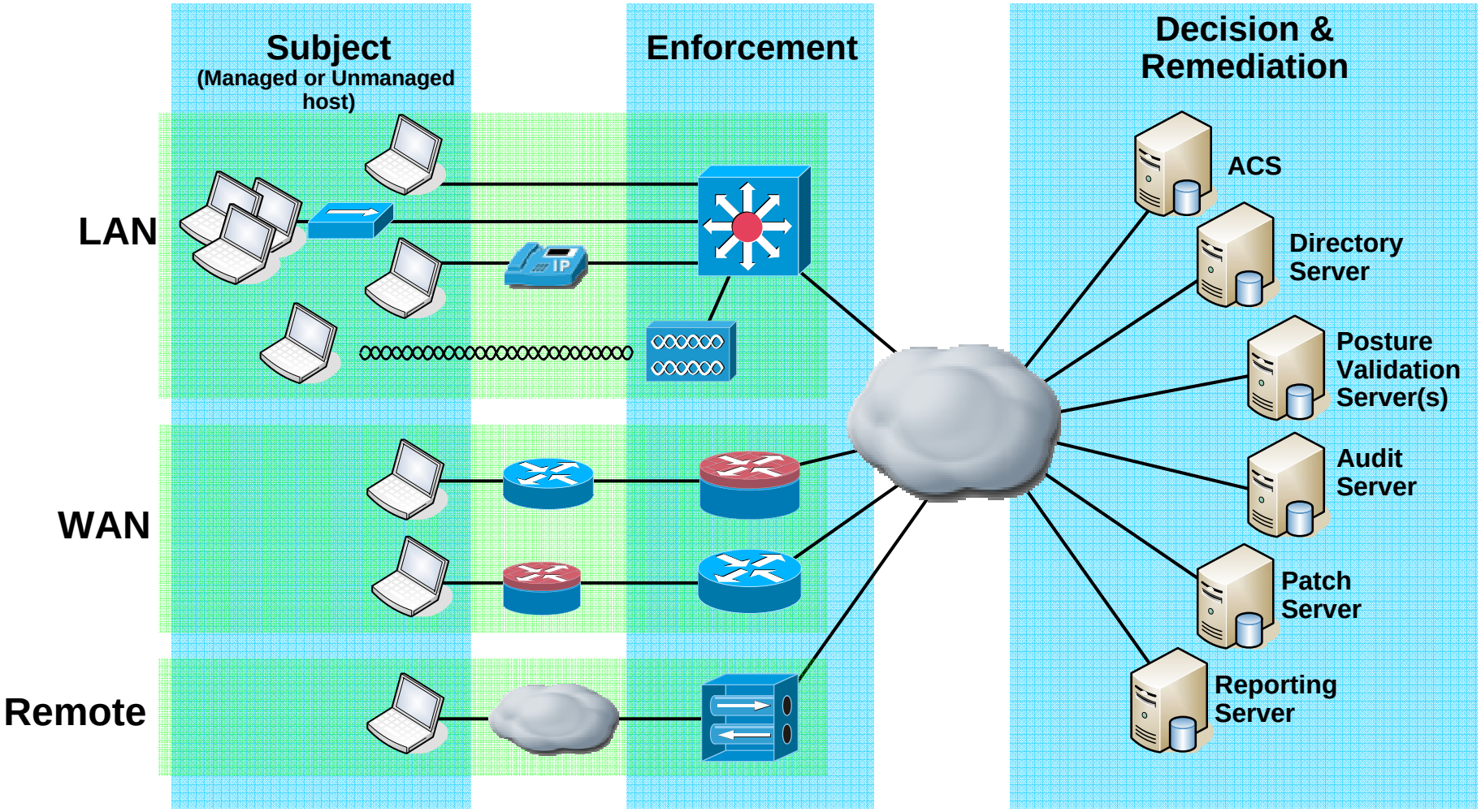
NAC Program Participants

http://www.cisco.com/go/nac/program

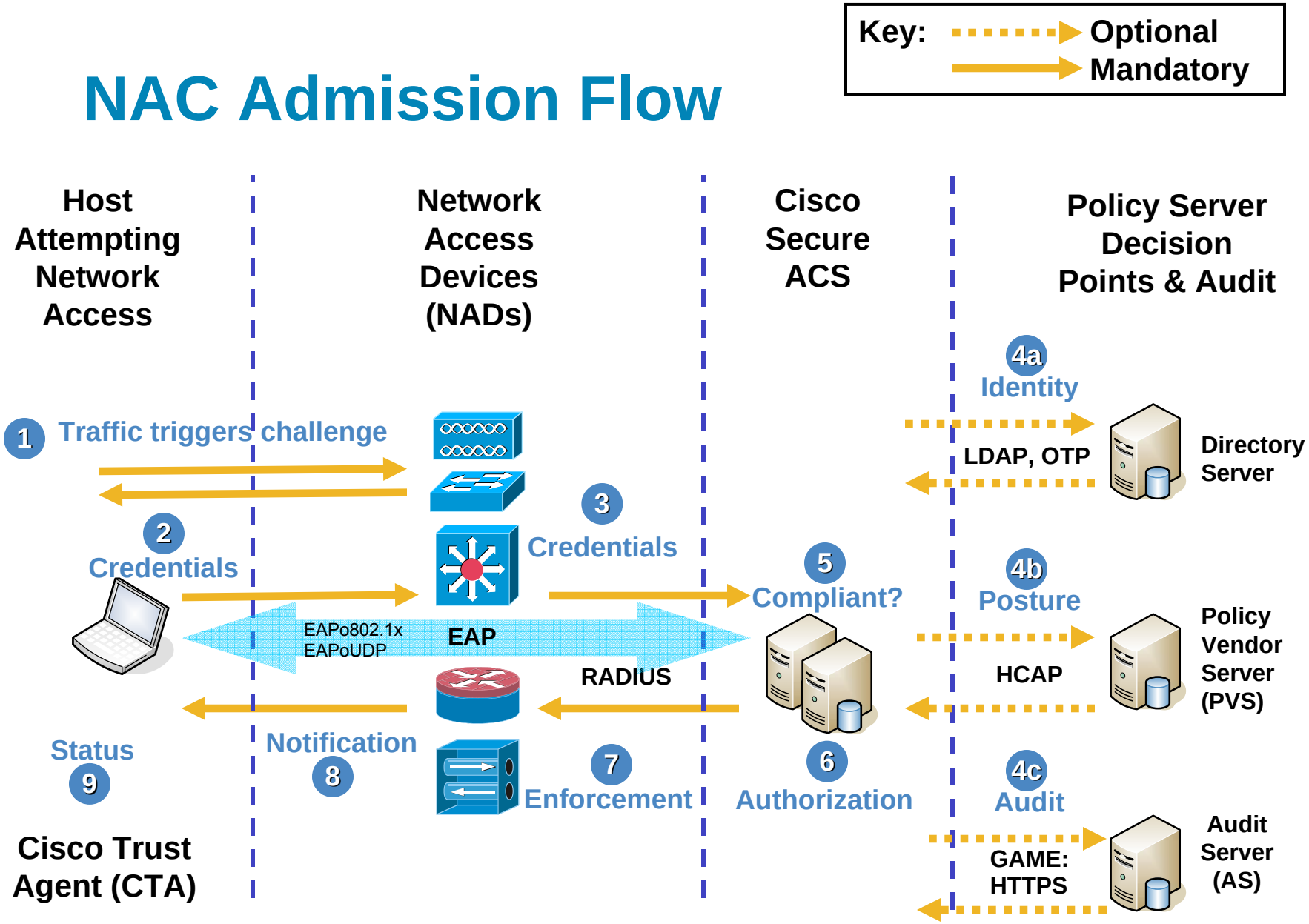
SHIPPING

DEVELOPING

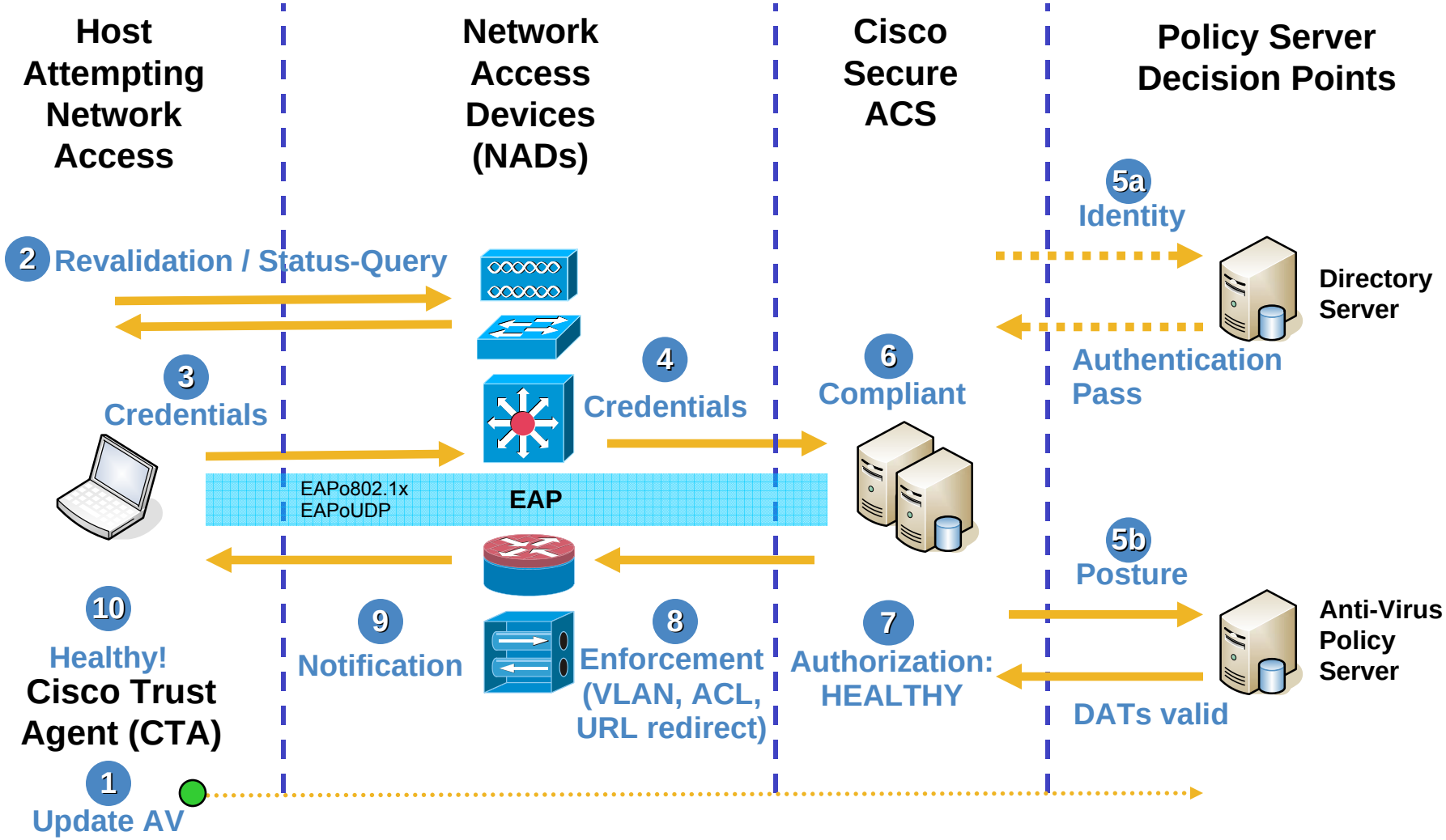
NAC Framework Architecture



NAC Admission Flow



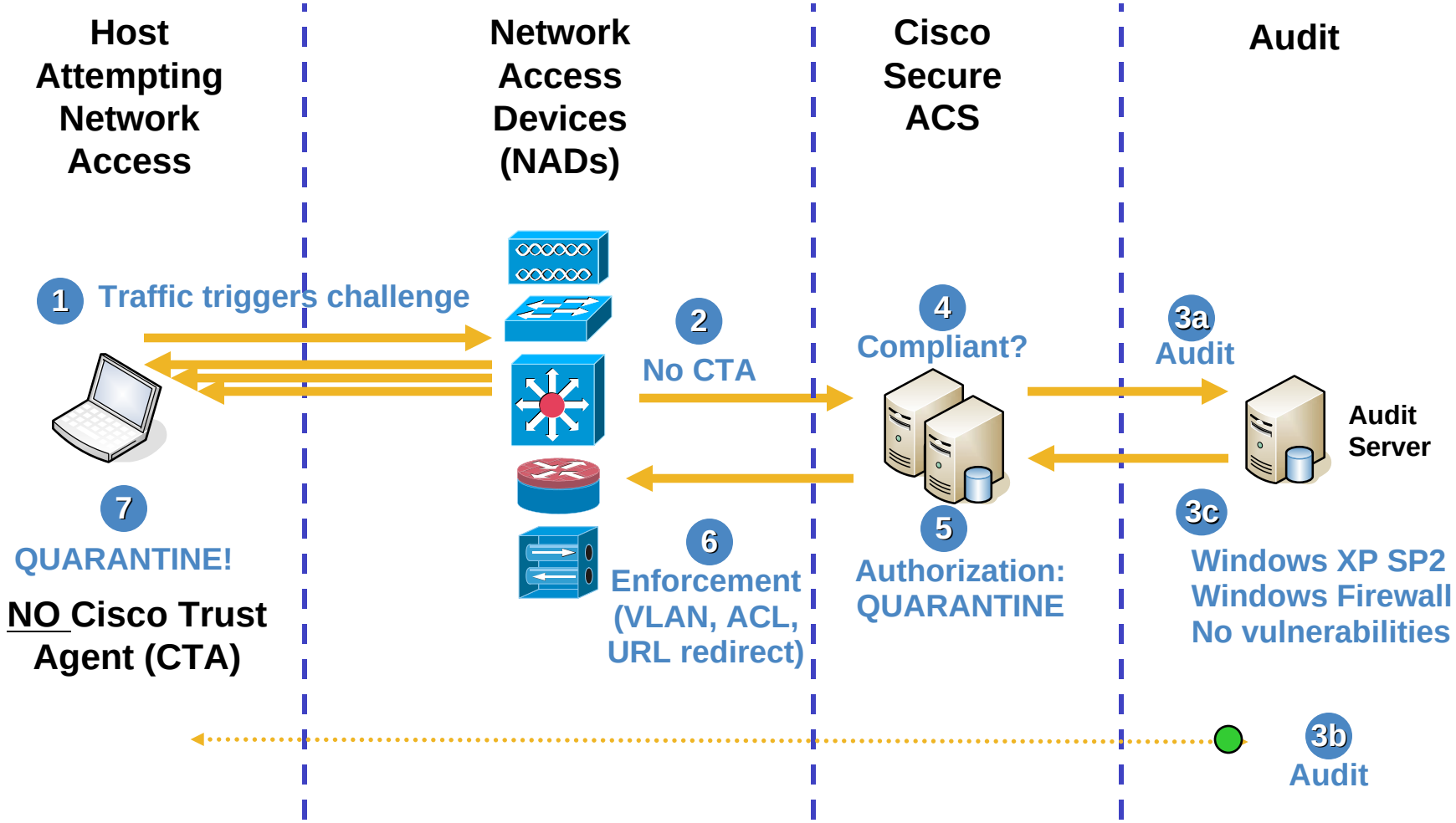
NAC Compliance: QUARANTINE to HEALTHY



NAC Posture States

Healthy	Host is compliant; no restrictions on network access
Checkup	Host is within policy but an update is available. Used to proactively remediate a host to the Healthy state
Transition	Host posturing is in process; give interim access pending full posture validation. Applicable during host boot when all services may not be running or audit results are not yet available
Quarantine	Host is out of compliance; restrict network access to a quarantine network for remediation. The host is not an active threat but is vulnerable to a known attack or infection
Infected	Host is an active threat to other endpoint devices; network access should be severely restricted or totally denied all network access
Unknown	Host posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined

NAC Agentless Host (NAH)



Note: NAH in 802.1x currently unsupported!

Overview

Planning

Design

Implementation

Operation

Q&A

Planning

- Use Cases
- Security Policy Creation
- Scalability
  - Server Count
  - Policy Replication
  - Load Balancing

Common Use Case Scenarios

- Make a list of access scenarios for **all** network attached devices:
  - Who – group role of the user or device (identity and/or posture)
  - Where – logical group, access method, or geography
  - When – any time of day (ToD) restrictions?
  - How – network access methods
  - What – authorized network services and resources (L3+)
- Understand how these factors affect policy decisions
- Examples:
  - LAN: employees, contractors, guests, printers, servers
  - Appliances: servers, office, manufacturing, security, operations
  - Remote: VPN, branches, extranet
  - New PC: PXE boot, re-imaging

Security Policy Creation

- Define your security policy based upon the documented use cases
- What are your biggest security threats from these scenarios?
- Does differentiated network access using Identity, Posture, and other credentials prevent these problems?
- Who is responsible for collaboratively creating the security policy?
  L9 Communication: Security (InfoSec, SecOps, etc.), Directory Services, Network Operations, Desktop & Server Management (Patch)

Who	Where	When	How	What
Employees	All	Any	LAN, WAN, VPN	Any
Employees	Call Center	Any	LAN	Customer Database, Intranet
Contractors	All	Any	LAN	Internet Only
Guests	HQ	7am-6pm	WLAN	Internet Only
New PC	All	Any	PXE	PXE Servers
Printers	All	Any	MAB	Print servers

Scalability

- AAA Performance
  Estimate the average number of AAA transactions (authorizations) per day per user/device based on desired timer settings and known user behaviors:
  - RADIUS Session-Timeout value
  - Multiple access methods: VPN, wired, wireless
  - Multi-homed access on wired and wireless network interfaces
  - Restarts due to patches, installations, and general operation
  - Multiple devices per user (desktops, laptops, PDAs, etc.)
  - How often the host posture might change
- ACS performance is about 20 - 30 transactions per second (TPS) for NAC
- AAA Server Estimation:
  This is an absolute **minimum** count assuming the same transaction rate all day and the server at 100% load:

```
Transactions_per_Day = Transactions_per_User_per_Day x Number_of_Users
Transactions_per_Second (TPS) = Transactions_per_Day / (24 x 60 x 60)
ACS_Servers = Transactions_per_Second / ACS_Protocol_Authorization_Rate
```

- AAA policy synchronization: Manually, Triggered, Periodic, Scheduled
- Load balancing is recommended for enterprise customers

Overview
Planning
Design
Implementation
Operation
Q&A

Design

- Protocols: EAP-over-UDP, EAP-FAST, HCAP, GAME
- NAC Methods: NAC L3 IP, NAC L2 IP, NAC L2 802.1x
- Architecture
  - Public Key Infrastructure (PKI)
  - Hosts: Managed and Unmanaged
  - Network Access Devices (NADs)
  - Policy Servers (e.g. ACS, Directory, Audit, Patch, etc.)
  - NAC Agentless Hosts (NAHs) & Auditing
  - Logging, Monitoring, and Reporting (e.g. MARS)

EAP (Extensible Authentication Protocol)

- Extensible Authentication Protocol (EAP)
- RFC 3748 (obsoletes 2284) http://www.ietf.org/rfc/rfc3748.txt
- An authentication framework which supports multiple authentication methods
- EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP
- Extensions to EAP for NAC with EAP-over-UDP:

  EAP-TLV: carry posture credentials, adding posture AVPs, posture notifications

  Status Query: new EAP method for securely querying the status of a peer without a full credential validation, L3 only

  EAPoUDP: use of EAP over IP for L3 transport

EAP-FAST Protocol

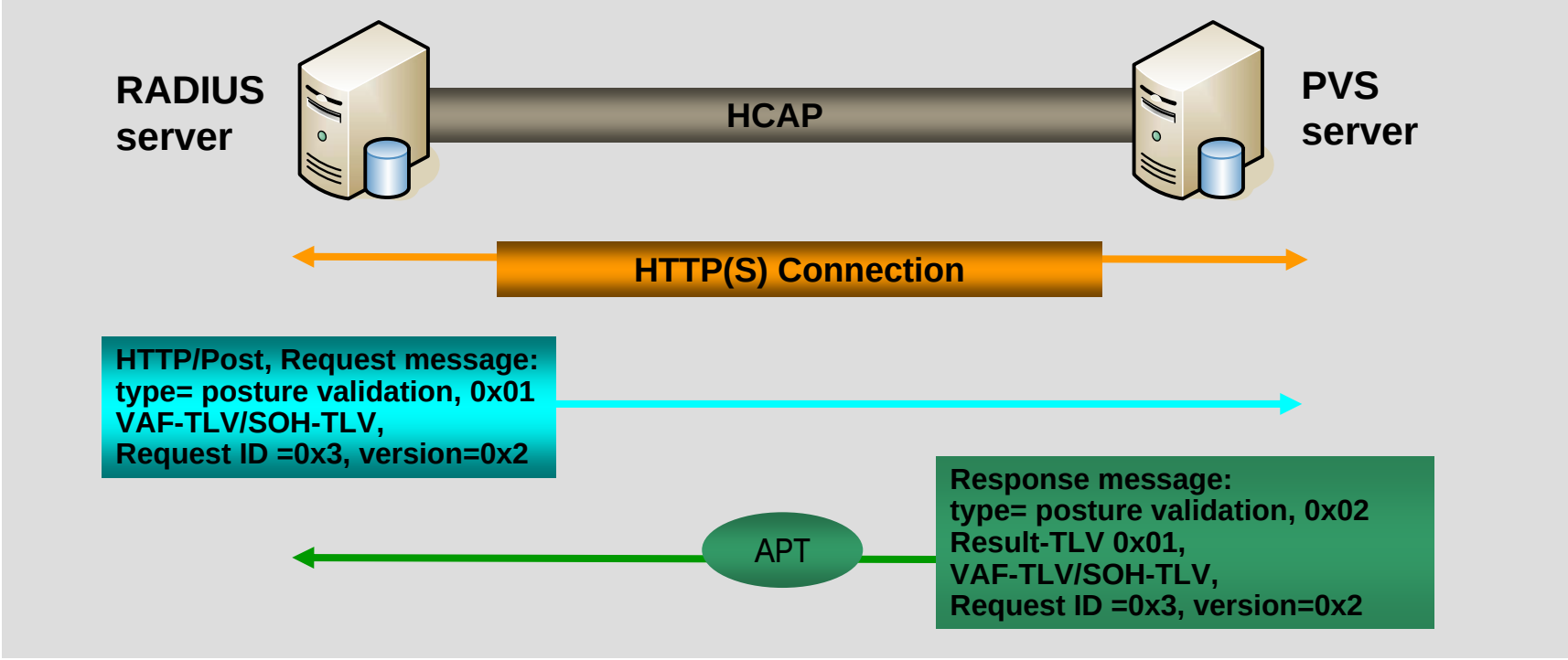
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a TLS based RFC3748 compliant EAP method.
- The tunnel establishment relies on a Protected Access Credential (PAC) that can be provisioned and managed dynamically by EAP-FAST through AAA server.
- PAC is a unique shared credential used to mutually authenticate client and server
- PAC is associated with a specific user-ID and an Authority ID
- PAC removes the need for PKI (digital certificates)
- EAP-FASTv1a now supports identity and posture chaining

NAC and Standards

- Cisco is participating in the NAC standardization process in 2006
- EAP-FAST and EAPoUDP currently published as informational Internet drafts
- Network Endpoint Assessment (NEA) BoF was held at IETF Spring 2006 meeting: co-chairs are Cisco and Juniper
- Working Group Charter is being established in October 2006
- Initial scope targeted at subset of protocols between client and AAA server
- Mailing list nea@ietf.org

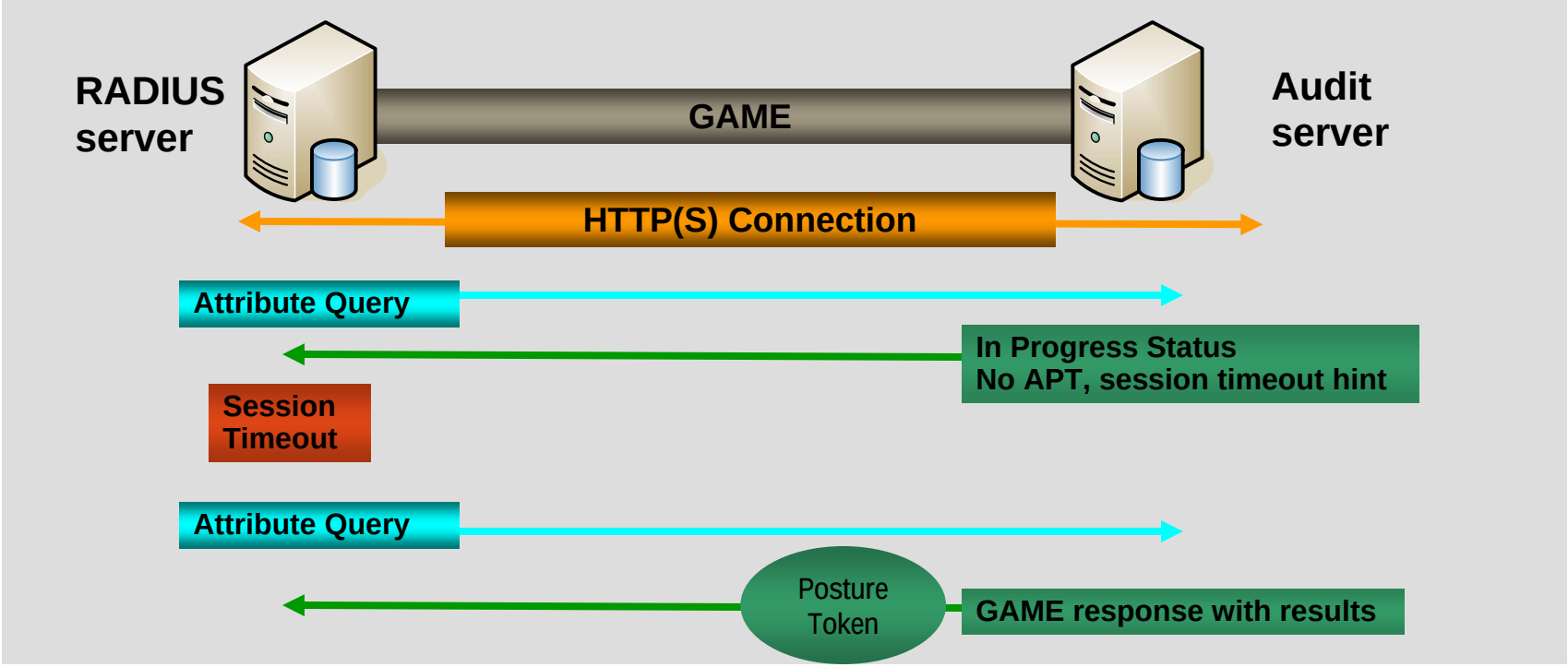
HCAP (Host Credential Authorization Protocol)

- HTTP(S) communication between ACS and Posture Validation Server (PVS)
- HTTP(S) session between ACS and vendor servers to forward credentials from the ACS EAP-session with the client
- ACS forwards client credentials to one or more vendor servers
- ACS receives posture token response and optional notification messages from each vendor server

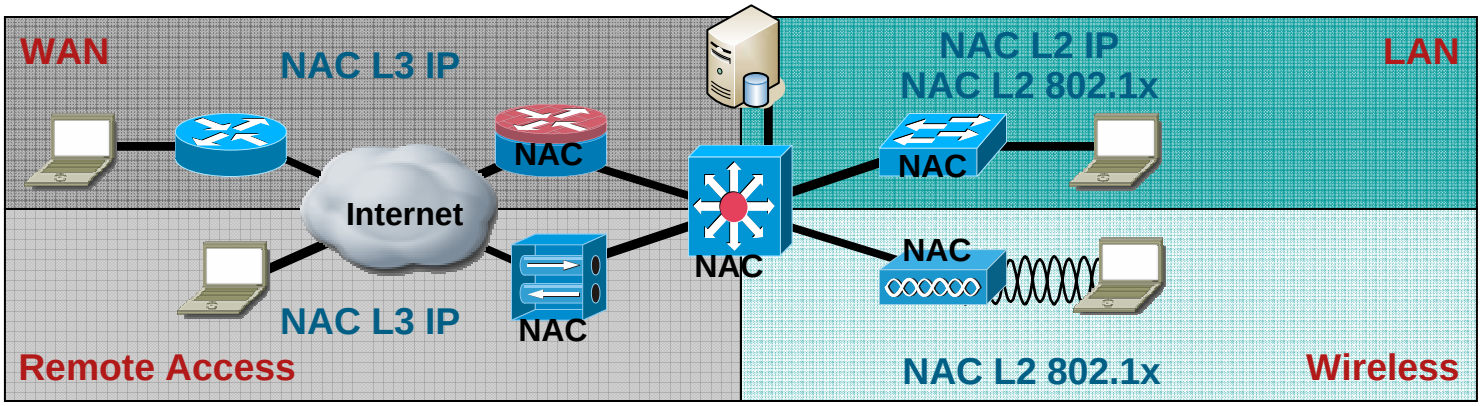


GAME (Generic Authorization Message Exchange)

- HTTP(S) session between ACS and vendor audit server extending Security Assertion Markup Language (SAML)
- ACS triggers posture validation of NAHs by the vendor audit server; polls periodically for audit decision
- Audit server responds with a posture state upon completion of the audit



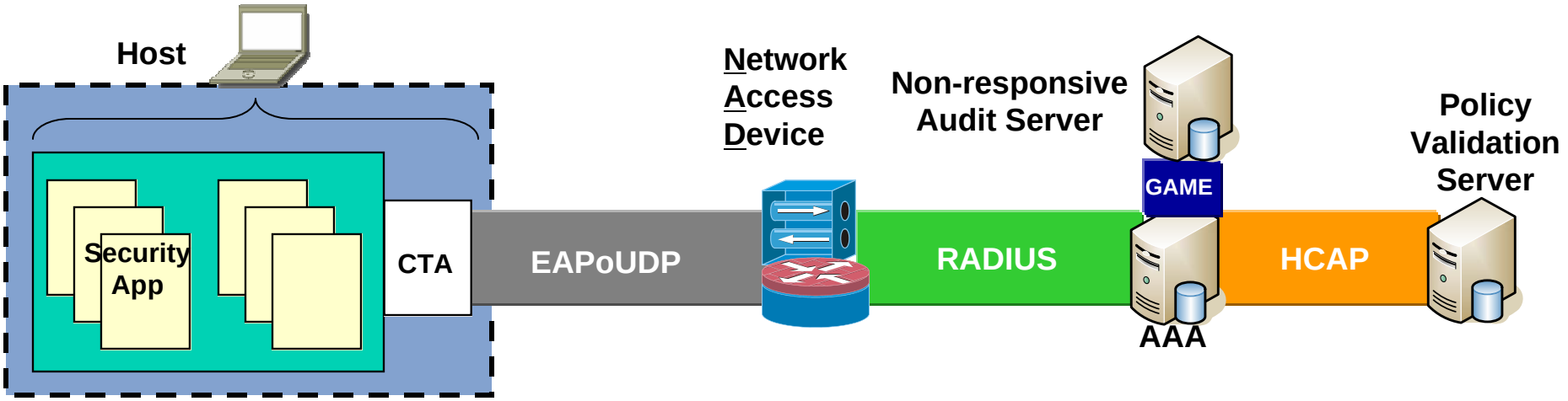
NAC Assessment Methods



- Methods to perform a posture assessment
  - **In-band**: obtain application state via CTA (an agent), and assess it in the policy system
  - **Out-of-band**: dynamic assessment (audit) of endpoint, mainly for 'Agentless' endpoints
  - **Exceptions**: create static exception handling for known assets (MAC, IP, port)
- NAC assessment methods
  - **NAC L3 IP**: at a layer 3 hop via IP, such as the perimeter, WAN, or distribution layer
  - **NAC L2 IP**: at a layer 2 switch port via IP, independent 802.1x
  - **NAC L2 802.1x**: via 802.1x at an L2 connection point (switch port or wireless AP)
- Agentless assessment useful for dynamic asset identification & risk
  - Called **NAC Agentless Host**, "non-responsive audit", or out-of-band assessment
  - Most Agentless technologies require IP connectivity to endpoint (scanning, login, or web download), others tie into inventory database systems

NAC L3 IP

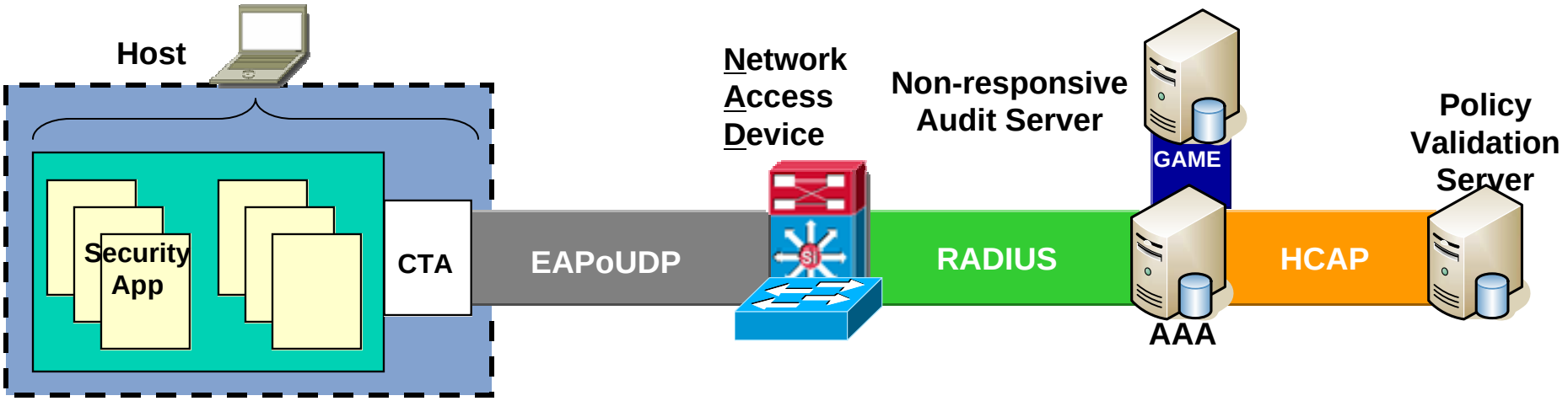
Assess Posture (Only) at the Perimeter using EAPoUDP



- Use Case Scenarios:
  - L3 perimeter: WAN edge, extranet, VPN/remote access
  - Interior network segmentation: non-production/lab networks, inter-department, distribution layer, data center access
  - Remote Access – IPsec and dial-in remote access aggregation ingress
- Trigger: IP packets forwarded from new source IP address
- Enforcement:ACLs (L3/4 controls) & URL redirection (provides NAH feedback)
- May be used serially for user & device validation (e.g. IPsec, auth-proxy)

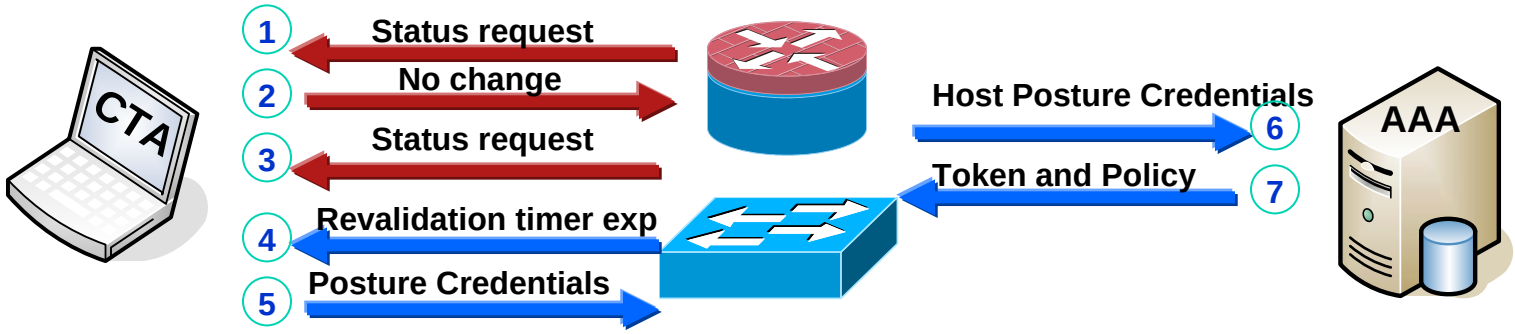
NAC L2 IP

Assess Posture (Only) at the Access-Layer using EAPoUDP



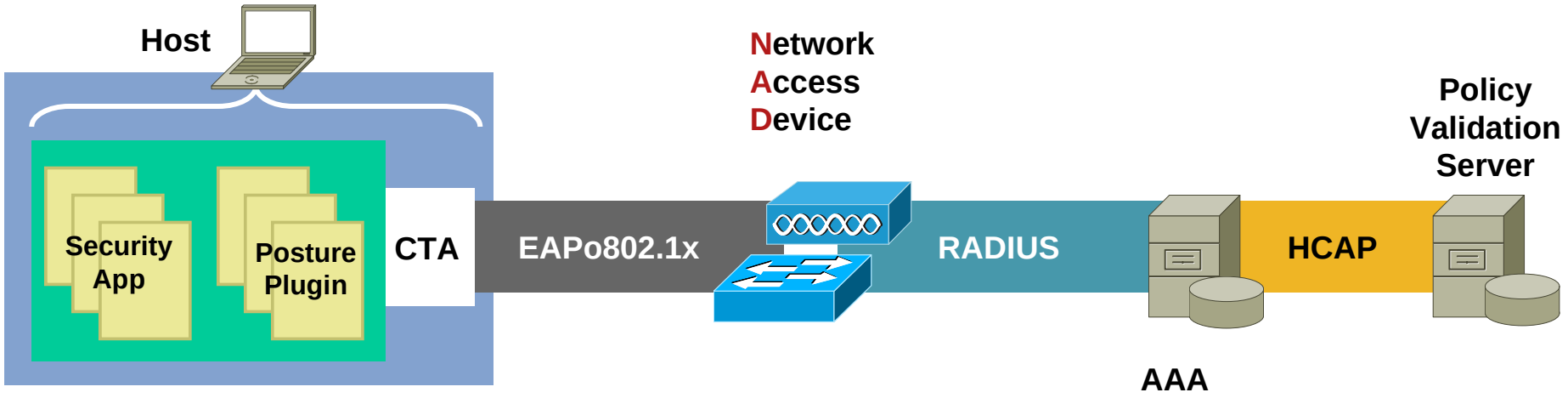
- Use Case Scenario: assess posture at the LAN access layer
- Trigger: Layer 3 via DHCP & ARP requests from new sources
- Enforcement:
  - Static VLAN assignment
  - ACLs (L3/4 controls) & URL redirection (provides NAH feedback)
  - There are different ACL technologies (Port ACLs, VLAN ACLs, Policy-Based ACLs)
- Can be performed after 802.1x authentication (totally independent)
- Microsoft 802.1x supplicant use-case (until it supports NAC)

NAC L2 IP & NAC L3 IP: Timers



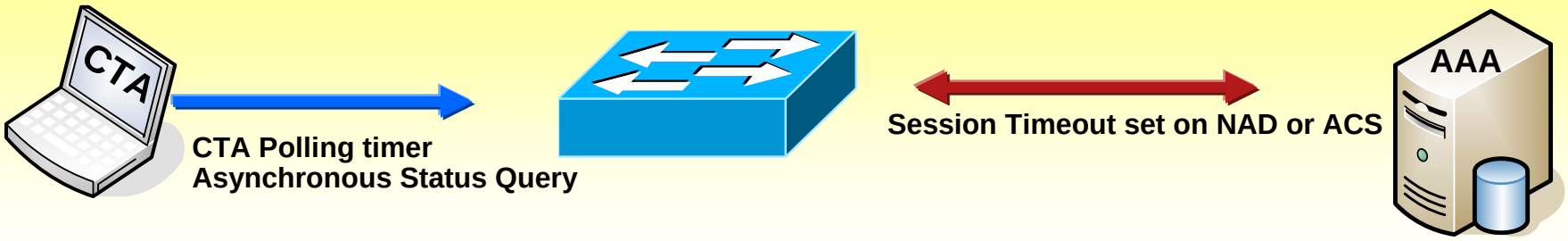
- Status Query Timer – confirm [in]active endpoint has not changed
  New EAP method between CTA and NADs (not ACS)
  Router periodically polls to make sure:
    1) CTA is still there
    2) It's the same validated device
    3) Posture hasn't changed
  Authentication based on keyed MAC - Uses keys derived in EAP-Posture (PEAP)
- Revalidation Timer – complete revalidation of host regardless of Status Query
- Timer Configuration – global setting on switch or per session from the ACS
  ACS timer values override any global or interface timers on the switch

NAC L2 802.1x
Identity and Posture Assessment



- Use Cases: the LAN access layer upon wired or wireless link
- Trigger: L2 link up via 802.1x protocol
- Enforcement: Static VLAN assignment or ACLs (L3/4: Port ACLs, VLAN ACLs, Policy-Based ACLs & URL redirection)
- Posture assessment triggered and performed at L2 in 802.1x
- May use user and/or device authentication with 802.1x
- EAP-FAST required for Identity + Posture assessment

NAC L2 802.1x: Timers



- **Cisco Trust Agent**: By default, CTA polls the posture plugins on the host every 5 minutes looking for status change.
- **Session Timeout**: Timeout for active 802.1x sessions. Forces reauthentication of host. Default is 3600 seconds.
- **Asynchronous Status Query**: Proactive notification from posture plugin to CTA of application status change on host. Forces reauthentication. Currently implemented in CSA and

NAC Method Comparison

Feature	NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP
Trigger mechanism	Data Link Up	DHCP or ARP	Forward Packet
Machine Identity	√		
User Identity	√		
Posture	√	√	√
VLAN assignment	√		
URL-Redirection		√	√
Downloadable ACLs	6500-only (PBACLs)	√	√
Posture Status Queries		√	√
Reauthentication/Revalidation	√	√	√
Device	Switch or AP	Switch	Router
EAP over	UDP	UDP	802.1x

NAC Agentless Hosts

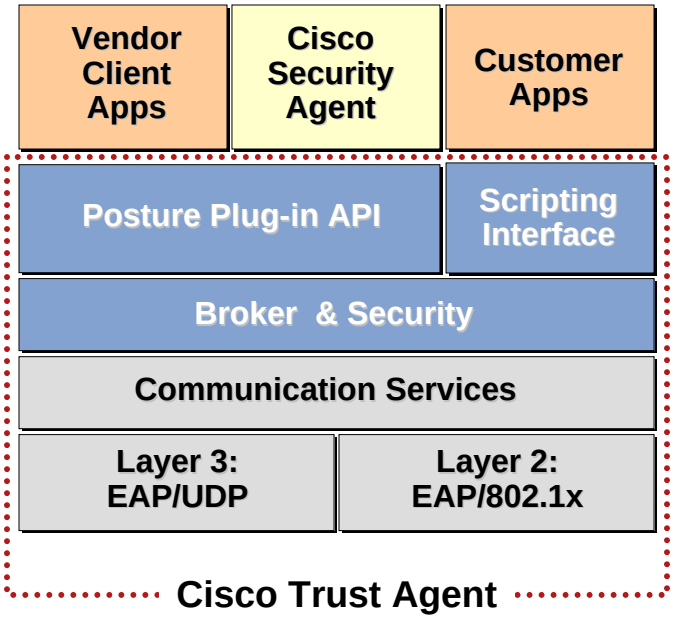
NAH Method	Credentials	Pros	Cons
Static NAD Whitelisting	MAC/IP address or CDP device type Wildcarding available	Simple, distributed configuration	Weak identity authentication Distributed lists of static addresses to maintain Lack of centralized logging
Centralized ACS Whitelisting	MAC / IP addresses Wildcarding available	Centralized address management	Weak identity authentication Static list of addresses to maintain
Dynamic Host Audit	Posture from network scan, remote login or browser object download	Dynamic, posture based assessment No static MAC / IP address lists to maintain	Additional NAC components to manage

Overview
Planning
Design
Implementation
Operation
Q&A

Implementation

- Components:
  - CTA / CSSC / Other Supplicants / Agentless
  - NADs
  - ACS
  - Optional: CSA, MARS
- Common Problems:
  - 802.1x, PXE, NAH, GPO, unmanaged devices
- Deployment Strategies:
  - Lab Verification
  - Small, Monitored Pilot
  - Small, Enforced Pilot
  - Increase deployment scale based on the results

Cisco Trust Agent (CTA) v2.1



- Supported on Windows 2000 / XP / 2003, Red Hat Linux, and MacOSX
- Supports 2 transport layers:
  - EAPoUDP - Layer 3
  - EAPo802.1x - Layer 2 (Windows only)
- Includes **wired-only** version of Cisco Secure Services Client (802.1x supplicant)
  - Wired functionality only
  - Can be replaced by the full version of Cisco Secure Services Client - both wired / wireless connections are supported
- Gathers OS info including patch and hotfixes
- Includes CTA Scripting Interface for custom posture information
- Backward compatible with CTA 1.0 and 2.0 posture plugins from NAC Program participants
- Expanded debug/diagnostic output

CTA and Supplicant Comparisons

Feature	Microsoft Windows	CTA 2.1	CSSC	Juniper Odyssey
Retail Cost	Free	Free	$	$
NAC L2/L3 IP		√		
NAC L2 802.1x Wired		√ (Windows)	√	
NAC L2 802.1x Wireless			√	
PEAP-GTC (EAPoUDP)		√	√	
EAP-FAST*		√	√	√
Others	√		√	√
Supported OSes	Windows XP, 2003	Windows 2000, XP, 2003, RedHat Ent Linux, Mac OS X	Windows NT4, 2000, XP, 2003; RedHat Ent Linux**	Expected on Windows NT4, 2000, XP, 2003; RedHat Ent Linux**

***Must use EAP-FAST for NAC L2 802.1x with identity + posture compliance**

Router Platform Support

- **NAC L3 IP shipped June 2004**
  - **T-train images with Security**
  - **The same image that includes firewall, NIPS, and crypto**
- **NAC Agentless Host (Audit) supported in IOS 12.4(6)T**
- **Network Module Switches**
  - **16, 24, 48 port NM**
  - **2800, 3700, 3800 router platforms**
  - **NAC L2 802.1x & NAC L2 IP**

Cisco 18xx, 28xx, 38xx	Yes
Cisco 72xx, 75xx	Yes
Cisco 37xx	Yes
Cisco 3640, 3660-ENT Series	Yes
Cisco 2600XM, 2691	Yes
Cisco 1701,1711, 1712, 1721, 1751, 1751-V, 1760	Yes
Cisco 83x	Yes
Cisco 74xx, 73xx, 71xx (S-train)	TBD
Cisco 5xxx	TBD
Cisco 4500	No
Cisco 3660-CO Series	No
Cisco 3620	No
Cisco 2600 non-XM Models	No
Cisco 1750, 1720, 1710	No

VPN Concentrators

- Models 3005-3080
- Release v4.7 supports NAC L3 IP
- VPN Client does not include CTA
- Works with IPSec and L2TP/IPSec remote access sessions.
  - NAC processing starts after an IPsec session is established
  - Communication with CTA is within IPsec SAs
  - NAC does not apply to PPTP, L2TP or LAN-to-LAN sessions
- Local exception lists also include OS type
- NAC Agentless Host assessment is not supported yet; timeline is TBD

Catalyst Switch NAC2 Framework Support

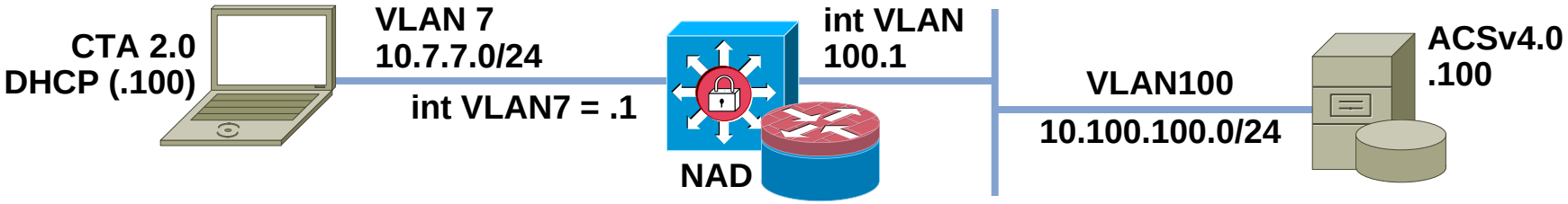
Progressive Functional Tiers

Platform, Supervisor	OS	NAC L2 802.1x	NAC L2 IP	NAC L3 IP	NAC Agentless Host
6500–Sup32, 720	Native IOS	Future	Yes	Future	NAC L2 IP
6500–Sup2	Native IOS	No	No	No	No
6500–Sup2, 32, 720	Hybrid	Yes	Yes	No	NAC L2 IP
6500–Sup2, 32, 720	CATOS	Yes	Yes	No	NAC L2 IP
4500 Series– SupII+, II+TS, II+10GE, IV, V, V-10GE	IOS	Yes	Yes	Future	NAC L2 IP
4900	IOS	Yes	Yes	Future	NAC L2 IP
3550,3560, 3750	IOS	Yes	Yes	No	NAC L2 IP
2950,2940, 2955, 2960, 2970	IOS	Yes	No	No	No
6500–Sup1A	All	No	No	No	No
5000	All	No	No	No	No
4000 Sup I, II, III (IOS)	CATOS	No	No	No	No
3500XL, 2900XM, 1900	All	No	No	No	No

NAC Wireless LAN – Network Access

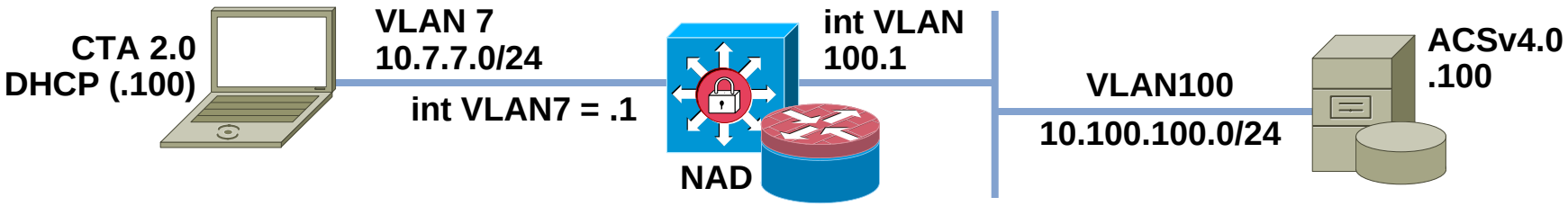
- NAC-Enabled Products
  - Cisco® Aironet® 1200, 1240 Series Access Points
  - Cisco Catalyst® 6500 Series Wireless LAN Services Module (WLSM)
  - Cisco Wireless LAN Controller 2006, 4100, 4400
  - Cisco Integrated Wireless Network
- WLAN enforces device security policy compliance at the access point when WLAN clients attempt to access the network
- Distributed WLAN solution via Cisco IOS® Software upgrade
- Cisco Aironet (Cisco IOS Software-based) access point in stand-alone or wireless domain services (WDS) mode. Cisco Catalyst 6500 Series WLSM as WDS device
- Centralized WLAN solution
- Cisco Aironet lightweight access points connected to Cisco WLAN Controller

NAC L2/L3 IP: Cisco IOS Required Common Configuration



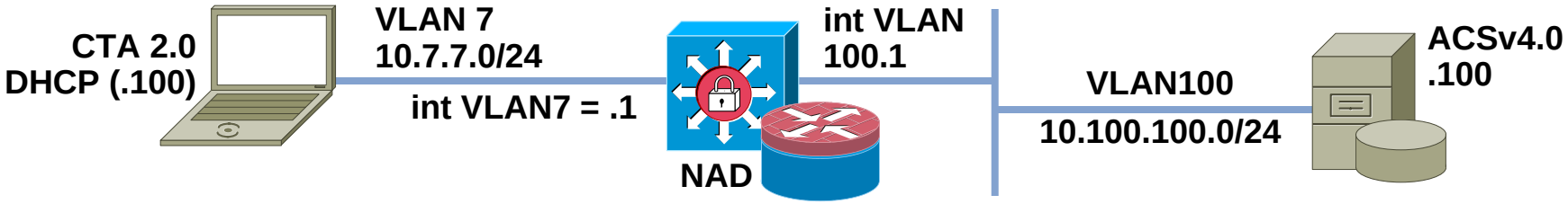

```
aaa new-model
aaa authentication eou default group radius

radius-server host 10.100.100.100 auth-port 1645 acct-port 1646
radius-server key cisco123

! Enable vendor specific RADIUS attributes
radius-server vsa send authentication

ip access-list extended NAC-Default-ACL
 remark Block traffic until NAC opens the interface
 remark 21862 is EAP over UDP
 permit udp any any eq 21862
 permit udp any eq bootpc any eq bootps
```

NAC L2/L3 IP: Cisco IOS Required Config



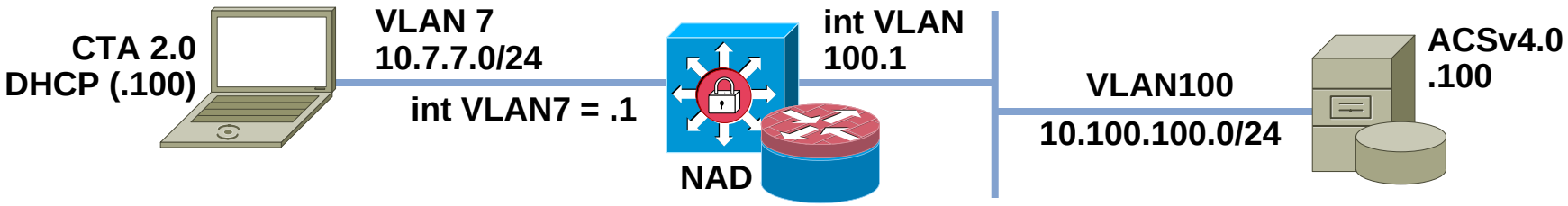

```
! Define NAC trigger, required on routers only

ip admission name NAC-L2-IP eapoudp
! –OR-
ip admission name NAC-L3-IP eapoudp list NAC-EoU-ACL

! What triggers NAC-L3-IP ?
ip access-list extended NAC-EoU-ACL
 remark DNS and HTTP to 10.100.100.101 do not trigger NAC
 deny udp any any eq domain
 deny tcp any host 10.100.100.101 eq www
 permit ip any any
```

NAC L2/L3 IP: Cisco IOS Optional Configuration




```
! Timers can be configured globally or per session by ACS

! Delay re-EAP after EAP failure
eou timeout hold-period 60
! Timeout to re-check all credentials
eou timeout revalidation 60
! How often check for status changes
eou timeout status-query 60
! Permit agentless hosts, used with external audit servers
eou allow clientless

! IOS web server is required for URL redirection
ip http server

! Logging for debugging
eou logging

! Optional, specify the local IP address of RADIUS packets
ip radius source-interface FastEthernet0/0
```

NAC L2/L3 IP: Cisco IOS Interface Configuration



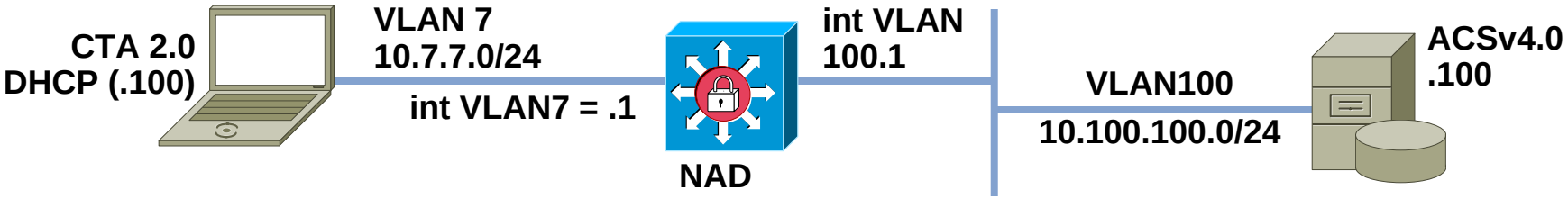
Routers with NAC L3 IP

```
interface FastEthernet0/0
 ip address 10.7.7.1 255.255.255.0
 ip access-group NAC-Default-ACL in
 ip admission NAC-L3-IP
```

Switches with NAC L2 IP

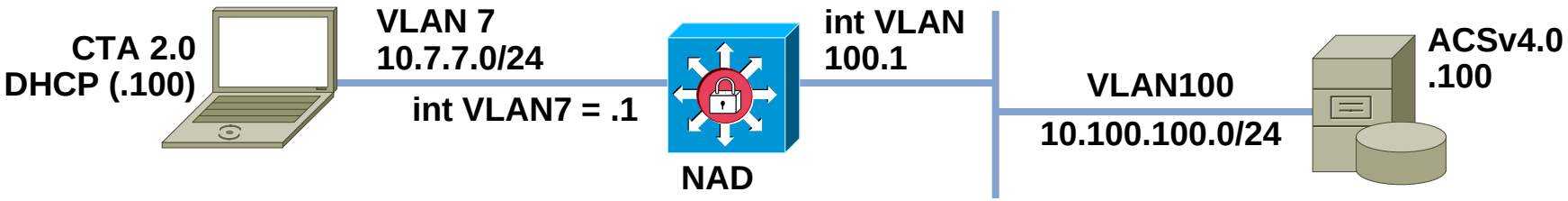
```
! Build device table of <IP, MAC>, user to trigger NAC L2 IP
ip device tracking

interface GigabitEthernet1/0/1
 switchport
 switchport mode access
 switchport access vlan 7
 ip access-group NAC-Default-ACL in
 ip admission NAC-L2-IP
```

NAC L2 IP: CatOS Required Configuration




```
set radius server 10.100.100.100 primary
set radius key cisco123

#Required – use only sc0 for NAC
set interface sc0 100 10.100.100.1 255.255.255.0

set security acl ip NAC-L2-IP permit arp

#VACL definition Required for CatOS
set security acl ip NAC-L2-IP permit dhcp-snooping
set security acl ip NAC-L2-IP permit arp-inspection any any
set security acl ip NAC-L2-IP permit eapoudp

#PBACL
set security acl ip NAC-L2-IP permit ip group Healthy_hosts any
set security acl ip NAC-L2-IP deny   ip group Infected_hosts any
set security acl ip NAC-L2-IP permit ip group Exception_hosts any
set security acl ip NAC-L2-IP permit ip group Clientless_hosts host 10.100.100.101

#Apply to VLAN 7
set security acl map NAC-L2-IP 7
```

NAC L2 IP: CatOS Configuration (Cont.)



Required Configuration (CatOS)

```
set eou enable
! Allow clientless access via ACS
set eou allow clientless enable
! Enable eou on port!
set port eou 3/1 enable
set vlan 7 3/1
```

Optional Configuration (CatOS)

```
! Static IP exception, wildcard too
set eou authorize ip 1.1.1.1 policy NAC
! Static MAC exception, wildcard too
set eou authorize mac 0000.0000.0001 policy NAC
```

NAC L2 802.1x Configuration

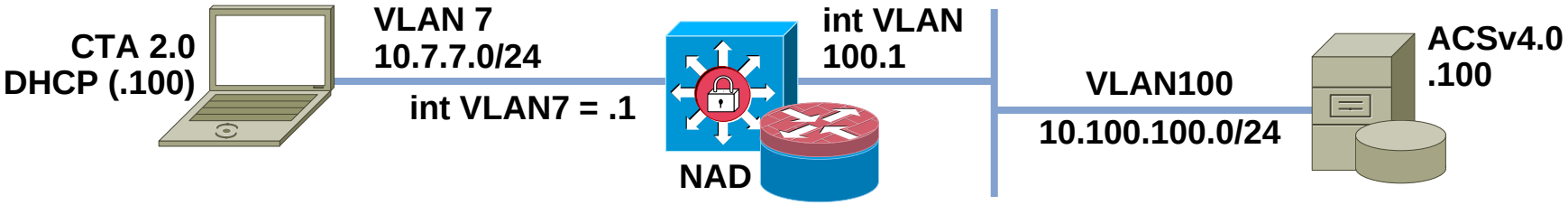
Cisco IOS®

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius

radius-server host 10.100.100.100 auth-port 1645 acct-port 1646
radius-server key cisco123

dot1x system-auth-control

interface GigabitEthernet1/0/1
 dot1x port-control auto
 dot1x timeout reauth-period server
 dot1x reauthentication
```

CatOS

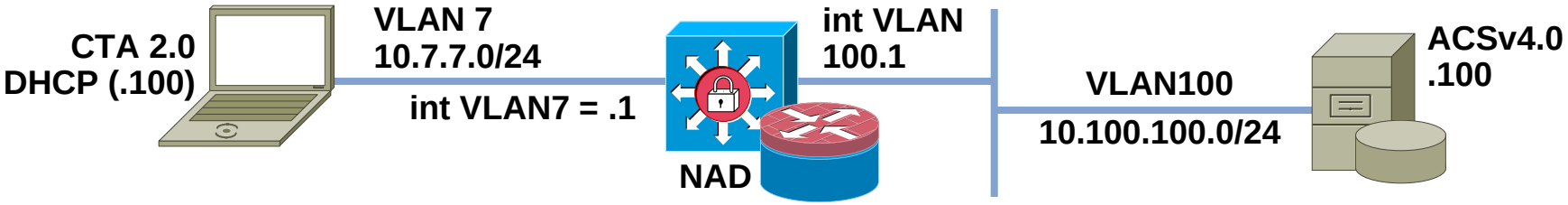
```
set radius server 10.100.100.100 auth-port 1812 primary
set radius key cisco123

set dot1x system-auth-control enable

set port dot1x 3/1 port-control auto
set port dot1x 3/1 re-authentication enable
```

NAC L2/L3 IP: Cisco IOS NAD Whitelisting




```
! Exception based method: CDP (IP PHONE), MAC, or IP
identity profile eapoudp
 device authorize type cisco ip phone policy No-NAC
 device authorize ip-address 10.7.7.100 policy No-NAC         # IP bypass
 device authorize mac-address 0010.a4c4.dfb4 policy No-NAC    # MAC bypass


identity policy No-NAC
 access-group NAC-Permit-All
 redirect url http://10.100.100.101/ match quarantine_url_redir_acl


! Statically permit access
ip access-list extended NAC-Permit-All
 permit ip any any
```

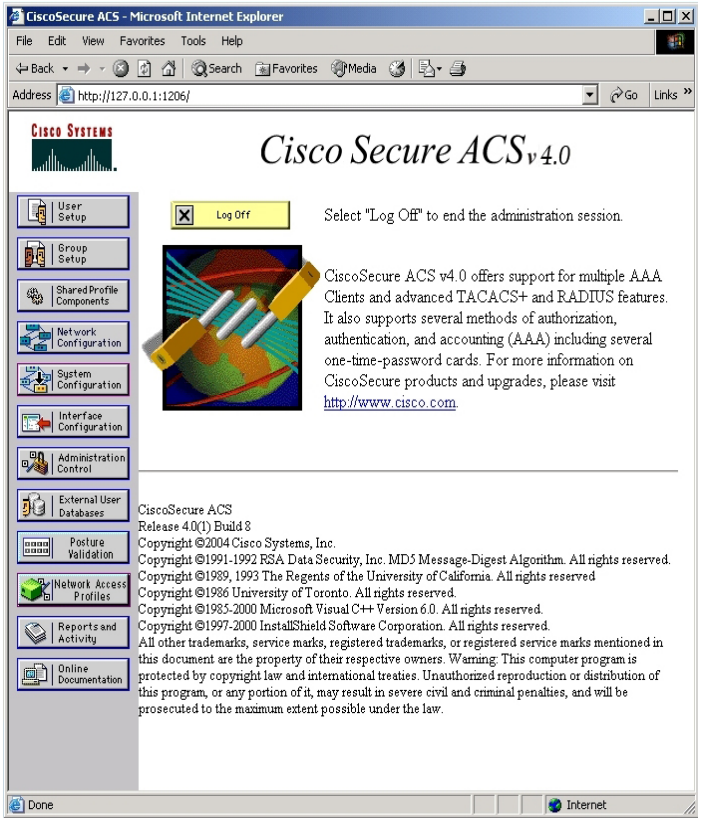
NAC L2/L3 IP: Cisco IOS NAD Whitelisting




```
! Option Sends IP address instead of MAC address (default)
eou allow ip-station-id


! Alternate method Sends clientless request to ACS
eou allow clientless
```

Access Control Server (ACS) v4.x

- Integration point for external policy servers, remediation servers, audit servers, reporting servers
- EAP-FAST, HCAP, GAME protocol support for NAC.
- Network Access Profiles
  - Services: Groups, Protocols, Attributes
  - Authentication: Protocols, Directories
  - Compliance: Posture & Audit Policies
  - Authorization: Groups, RACs, ACLs
- Template Configuration
- Configuration Cloning



ACS: MAC Authentication Bypass

- External MAC Authentication available in ACSv4.1
- Centralized MAC whitelisting configured under Network Access Profiles → Authentication
- Use default “agentless host” profile to get started

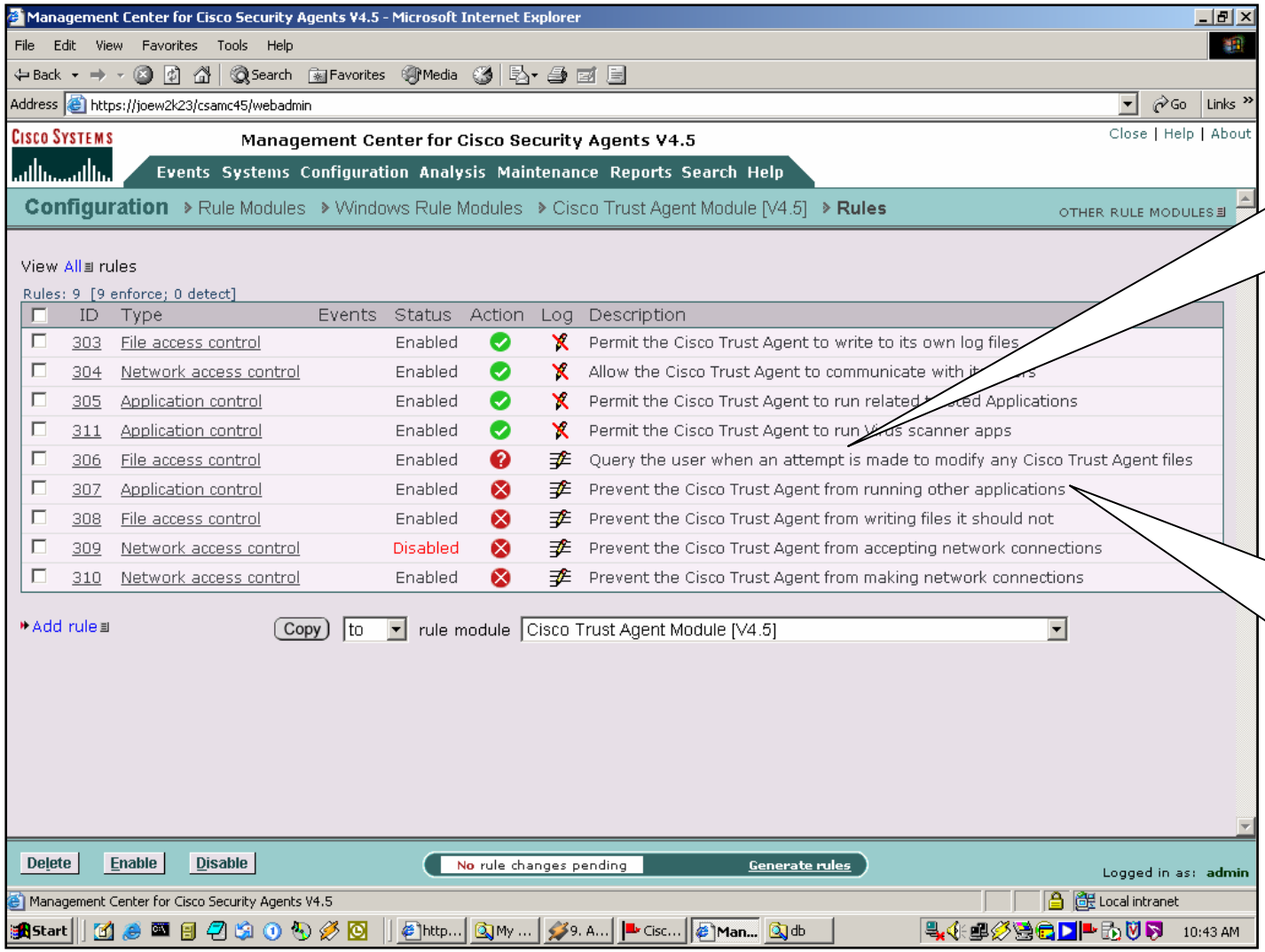
MAC Authentication Mapping for NAC-EOU-MAC-Except		
	MAC Addresses	User Group
○	000c.2999.fa96,	1: Employees (2 users)
If a MAC address is not defined or there is no matched mapping:		0: Default Group
Add Delete The Up/Down buttons submit and save the sort order to the database		
Submit Down		

Cisco Security Agent (CSA)

- CSA is an **optional** NAC component
- CSA v4.5 and later includes CTA v1.0
- CSA v5.0 bundles CTA v2.0 during installation
- HIPS technology is recommended to protect the integrity files of all host security applications, including CTA
- CSA policies can lockdown the host based on the posture received from a NAC authorization

  e.g., CSA can disable all host applications except patch management and antivirus upon NAC quarantine response

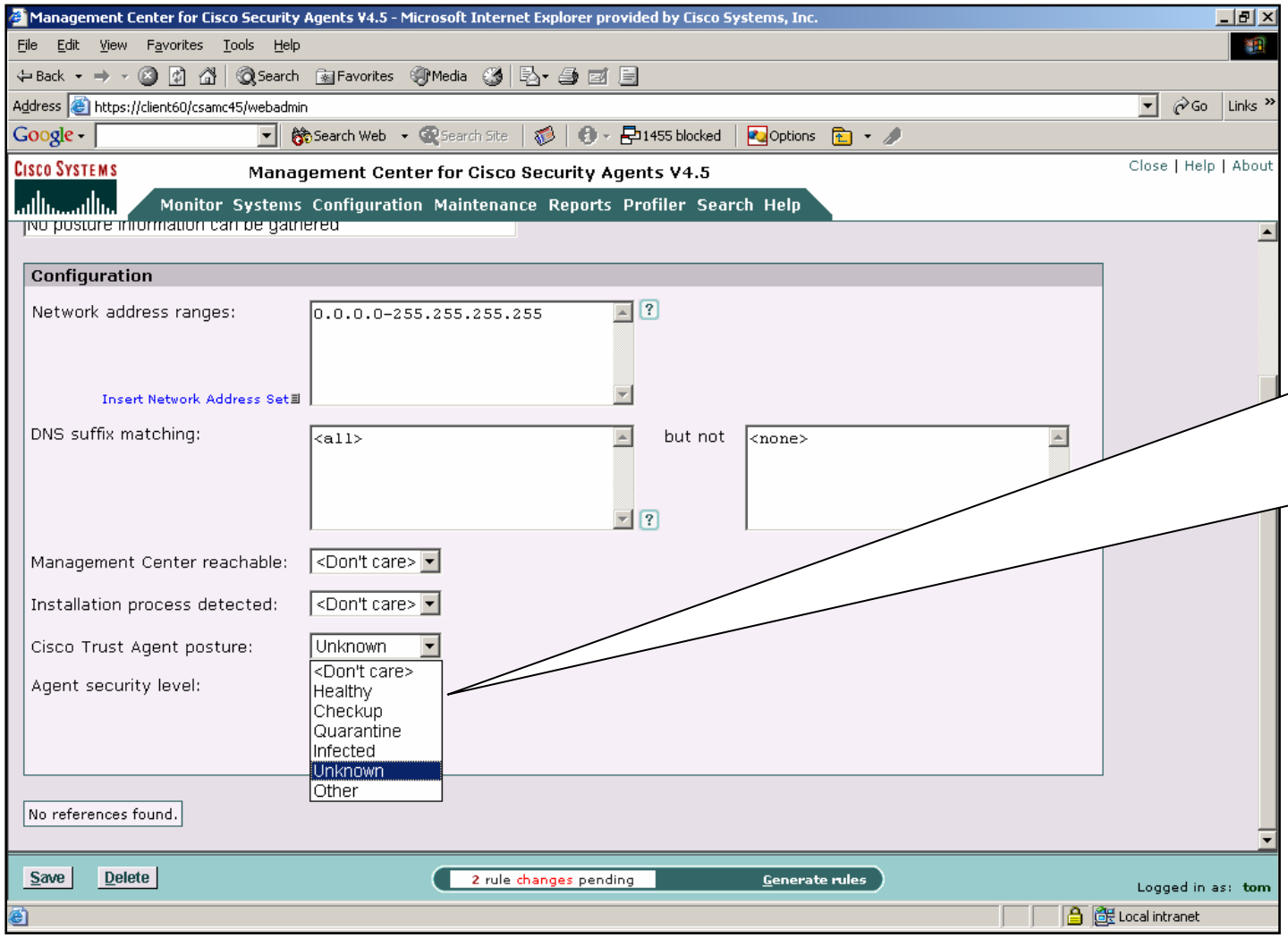
Guarding CTA integrity with CSA



CTA Needs to Be Protected from Unconscious Local, or Malicious Remote, Uninstall

CTA Needs to Be Protected so that It Is not Subject to “Witty Worm” Scenarios

CTA Posture Affects CSA Protection



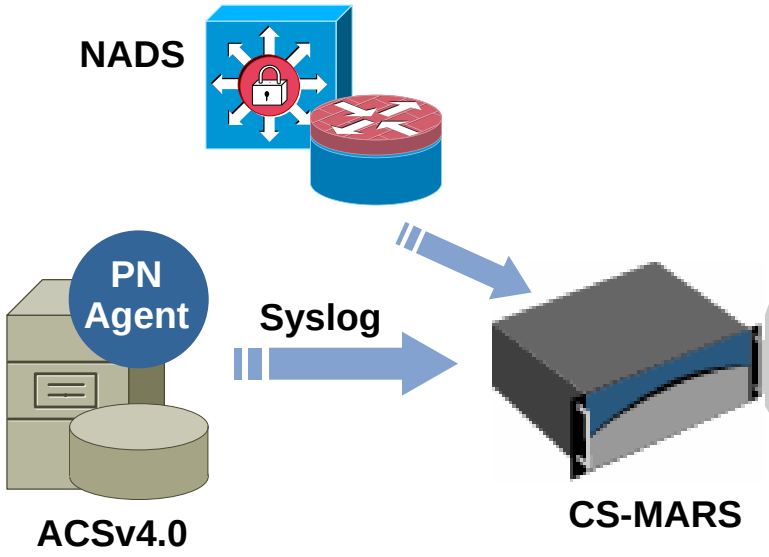
CTA System Token Used by CSA as a State Modifier for Policy

Important Protection for Noncompliant NAC Endpoints in the Time Before Remediation

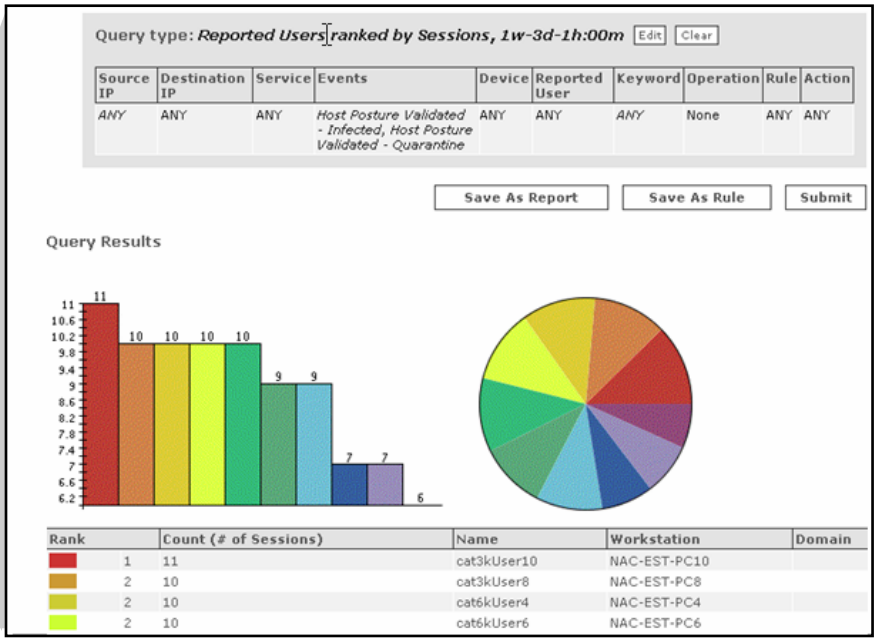
Important Protection for Noncompliant Endpoints when NAC Is Run in Monitor Mode

CS-MARS for NAC Monitoring and Reports

- CS-MARS provides a centralized monitoring and reporting point for NAC-related events from ACS, NADs, and third-party security servers
- PN log agent forwards Syslog information for NAC from ACS to CS-MARS
- Pinpoints where NAC events are occurring in the network, provides detailed logging information regarding events, and detailed NAC-related reports



NAC Infected/Quarantine—Top Hosts (Total View)

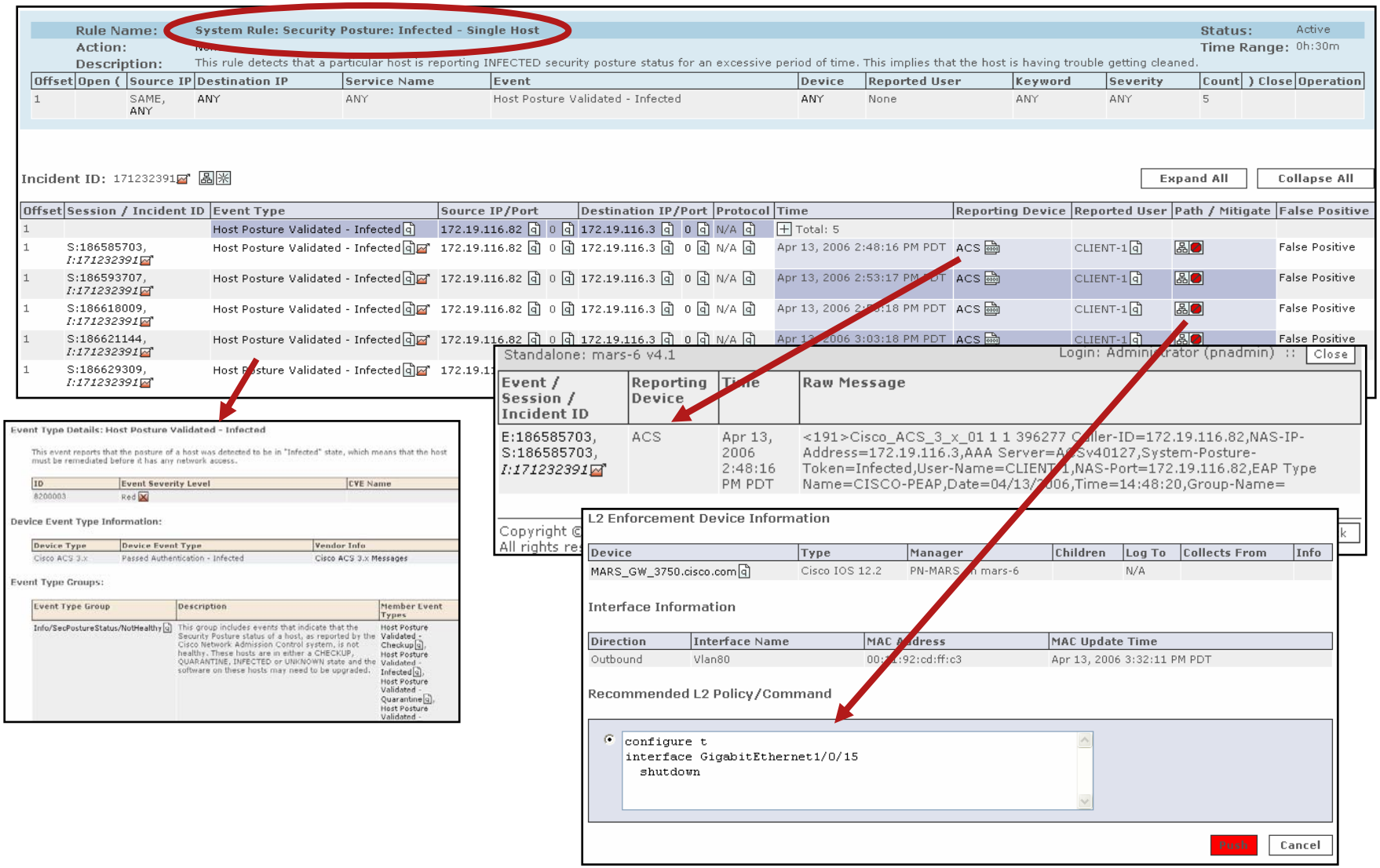


CS-MARS for NAC Monitoring and Reports

- Default NAC reports include:

- Custom reports can be created as well

NAC Incident Investigation Example



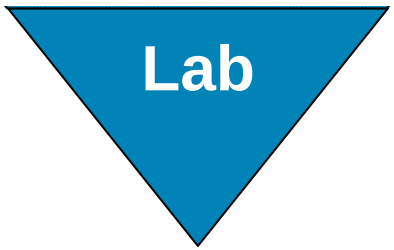
802.1x Implementation Challenges

- 802.1x Supplicants
  - Managability, protocol support, network policy rollout
- Preboot Execution Environment (PXE)
  - PXE timeout before 802.1x expiration
- Microsoft Group Policy Objects (GPO)
  - Machine GPO, User GPO, startup/logon scripts
- IP Phones
  - 802.1x Proxy EAPoL-Logon/Logoff
- Agentless Hosts: No 802.1x Supplicant
  - Old Operating Systems
  - Hardened / Embedded Operating System: IP phones, printers, photocopiers, sensors, etc.

802.1x Extensions

Feature	Use Case
802.1x Guest VLAN	No supplicant, Guests, Unmanaged, Old OSes
802.1x Auth-Fail VLAN	Guests, Temporary Access
802.1x VVID	IP Phones
802.1x Inaccessible Auth Bypass	AAA Server Down: minimum access, disaster recovery
802.1x Wake-on-LAN	WoL Compatibility (Not PXE)
MAC-Auth-Bypass (MAB)	No supplicant, Appliances
Web-Auth Proxy	No supplicant, Guest or User with identity

NAC Deployment Strategy



Deployment: Lab Verification

- Setup and configure all components in your lab
- DO NOT use self-signed certificates – they don't scale
- Verify operation of all desired NAC features
  - NAC L2 802.1x (EAPo802.1x)
  - NAC L2/L3 IP (EAPoUDP)
  - NAH: MAC-Auth-Bypass, GAME
  - Partners Integration: HCAP and GAME
  - Remediation Process: 3rd party and/or home-grown
- Verify NAC operation with all access scenarios
- Verify default and quarantine ACLs/VLANs allow any required **redirections** and **remediations**
- How will agentless hosts be handled?

Deployment: Small, Monitored Pilot

- Move lab configurations into very limited **production** network to validate normal operations
- **DO NOT** enforce network restrictions – allow full access!
- Verify **real world behavior** of hosts, users, groups, authentications, policies, log results, and scaling match expectations. If not, understand **why**!
- Visibility from logged compliance levels verify policy assumptions. **Adjust compliance policy** for Reality
- Verify **remediation** processes work as expected
- Verify **troubleshooting** processes with Help Desk
- Verify Agentless and Unmanaged (Guest) hosts work
- Adjust revalidation timers as needed for scaling

Deployment: Small, Enforced Pilot

- Enable **enforcement** of posture policies using real ACLs, VACLs, and VLANs
- Tune ACLs and VACLs as needed for **redirections** and **remediations** to work in the production network
- Verify IPs of external network dependencies

Deployment: Increase Pilot Scale

- After achieving a level of success with your initial pilot, expand the number, scope, and/or type of pilots
  - More ports, devices, access types, or geographies
  - More NAC methods: L3IP → L2IP → L2.1x
  - More user scenarios: Call Center, Sales, Engineering
- Tune policies, enforcement options, and timers as needed for handling the increased scope (previously unidentified users and applications)
- May need to create a network host registry and process for new or agentless devices

Overview
Planning
Design
Implementation
Operation
Q&A

Operations

- Policy Best Practices
- Logging & Reports
- Troubleshooting
- Performance Optimization

Policy Best Practices

- Communicate your compliance policy to End Users
  - NAC is a cultural change in security
  - Users need to understand what is required and why
  - Create a compliance website explaining this
- ACS Policy:
  - ACS Rule Ordering: First match wins
  - Use a default, CTA-Only Policy to catch missing applications
  - Use a master ACS to replicate policy to slave ACS servers
  - Test policies in lab environment before production deployment
  - Use the “contains” operator for string comparisons
  - Use OUI wildcards for MAC-Auth; 10,000 MAC limit per ACS NAP
  - External MAC-Auth via LDAP available in ACS v4.1

Operations: Logging

- Compliance visibility is enabled through logs

  AAA, Accounting, Syslog, NetFlow, Audit, PVSes, ….

- Syslog runs on UDP – critical logs may be lost!
- Short timers cause excessive syslogs – filter them
- Use a Security Information Management System (SIMS) for filtering, correlation, archiving, and reports

Operations: Reports

- What reports will assess your success with NAC?
- Top-N, Access Type, Group, Department, Asset Class, etc.
- May require correlation with other DBs: HR, Assets
- On-Demand End User Self-Service
- Compliance Audits: Sarbanes-Oxley (SOX), HIPAA
- Support Desk Reporting Tools
  - They must have complete access to AAA and other logs
  - May require web-based query tools by user, MAC, IP, etc.

Operations: CTA Troubleshooting

- Enable CTA logging – the default is **disabled**
- Log Configuration:
  C:\Program Files\Cisco Systems\CiscoTrustAgent\Logging\
- Rename ctalogd-temp.ini to ctalogd.ini
- Set log level to 15 for desired components
- Logs Files:
  C:\Program Files\Cisco Systems\CiscoTrustAgent\Logging\Logs
- Plugins:
  C:\Program Files\Common Files\PostureAgent\Plugins
- CTA Status:
  C:\Program Files\Cisco Systems\CiscoTrustAgent\ctastat

Operations: ACS Troubleshooting

- Successful auths stored in Passed Authentications log

  In ACS v4.x, posture attributes must appear in a posture validation rule to be logged. Create “dummy” rules if necessary.

- Failures stored in Failed Attempts log
- Auth.log:
  C:\Program Files\CiscoSecure ACS v4.0\CSAuth\Logs
- RDS.log:
  C:\Program Files\CiscoSecure ACS v4.0\CSRadius\Logs
- For the ACS appliance, these logs are found by creating a package.cab file under System Configuration > Support

Operations: ACS Common Failure Codes

Error Message	Solution
EAP-TLS or PEAP authentication failed during SSL handshake	Generally points to a certificate problem.
Posture Validation failed due to unmatched profile	Check NAPs and ensure that Posture Validation is allowed
User's credentials reside in an external DB that is not configured for this profile	Access profile matched without an external database selected or configured
No Token returned from external PV server	Communication problems with posture validation server. For example, an incorrect username/password.
Authentication protocol is not allowed for this profile	Check NAP Authentication settings. Ensure that current auth type is checked.
Access denied due to unmatched profile	No NAPs are being matched and default is set to “Deny access when no profile matches”

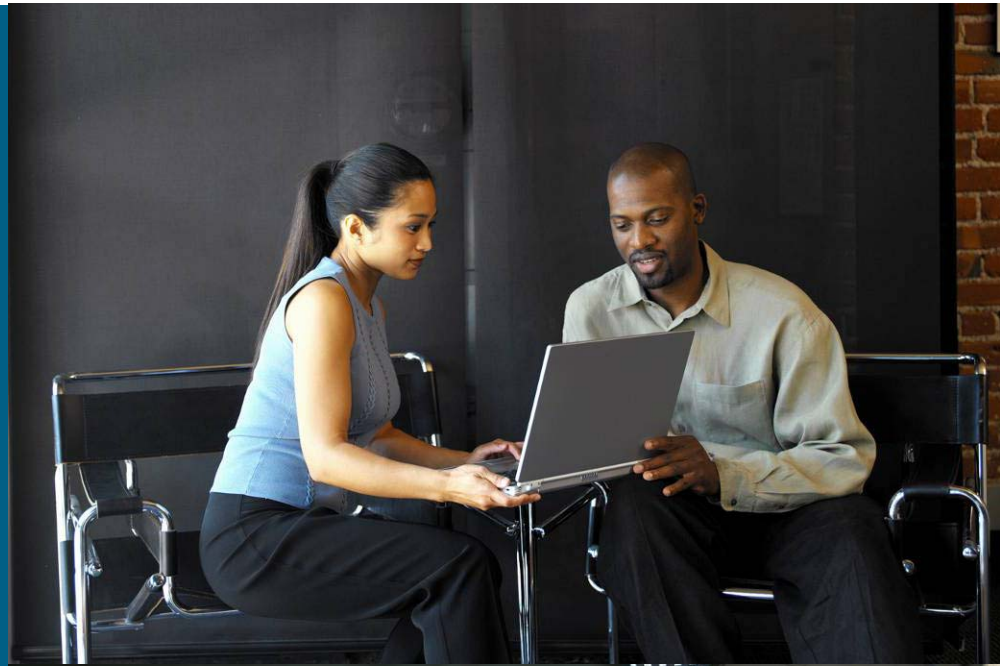
Performance Optimization: ACS

- Determine ACS performance for your environment
- ACS Policies:
  - Verify most frequently-matched policies are at the top
  - More rules slow performance
- Architecture
  - Co-locate policy servers to reduce latency
  - Load Balancing & Redundancy: ACS, Directory, AV, Patch

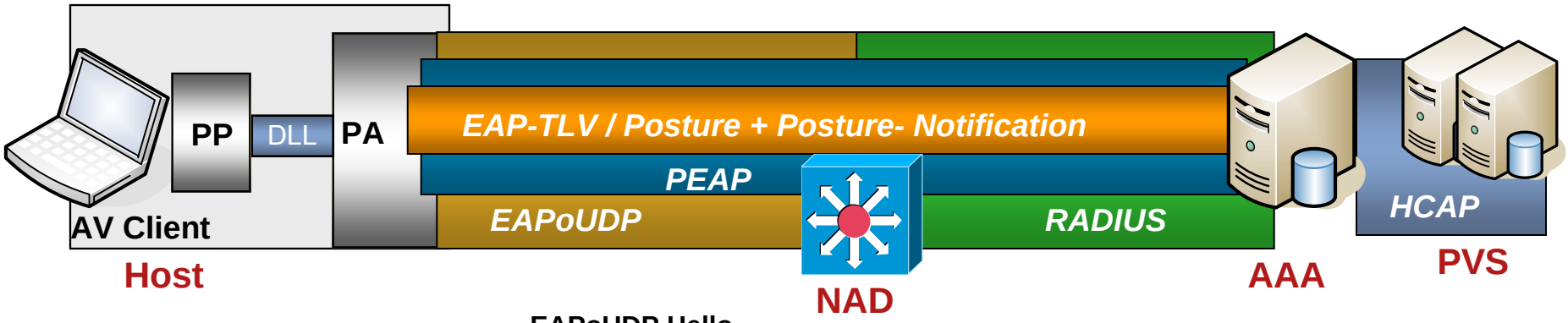
Performance Optimization: Timers

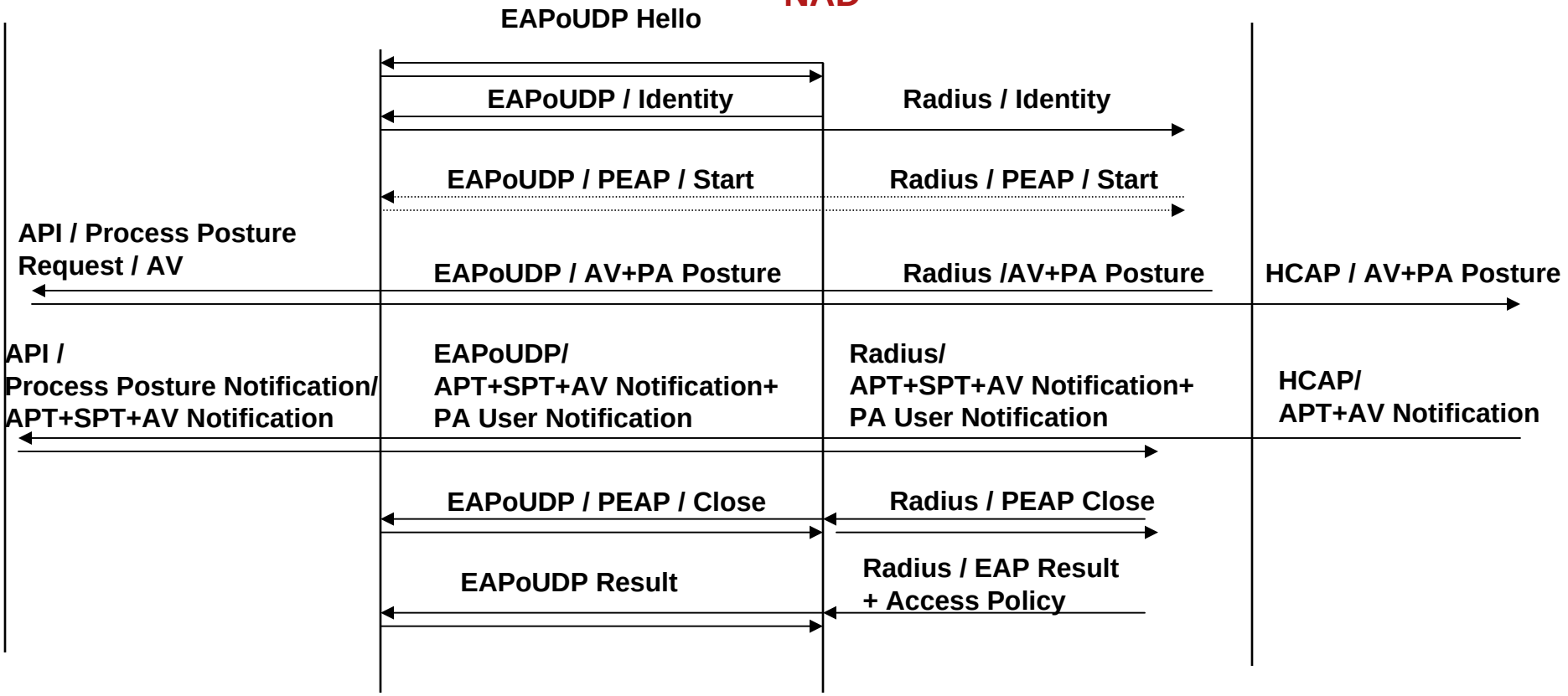
- "Revalidation" Timer: RADIUS Session Timeout (27)
- **`dot1x timeout tx-period 3`**
- **`dot1x timeout supp-timeout 3`**
- **`dot1x max-req 3`**
- **`eou timeout status-query 30`** (global / ACS)
- **`eou timeout revalidation 3600`** (global / ACS)

Overview
Planning
Design
Implementation
Operation
Q&A

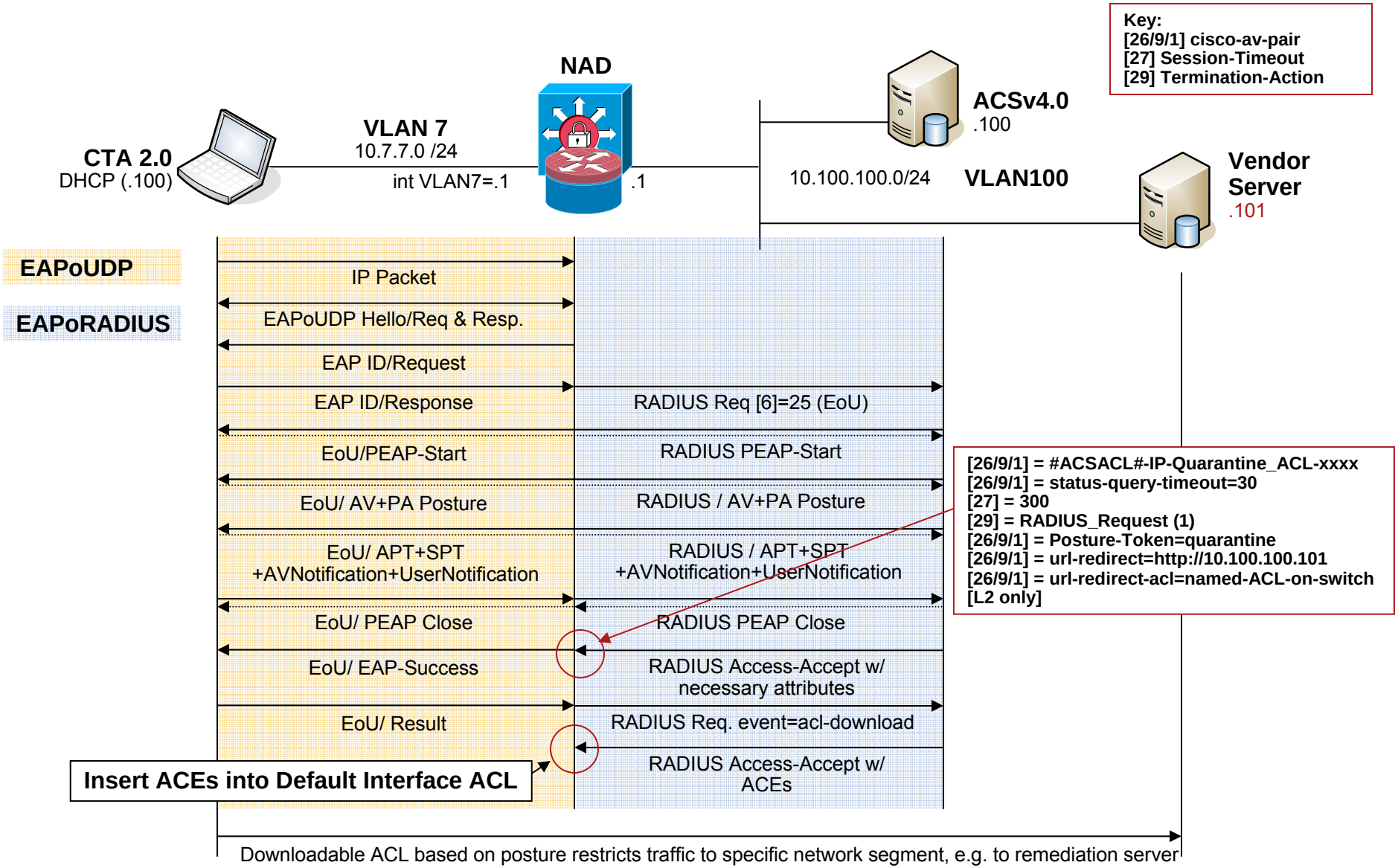


EoU (EAP over UDP) Posture Validation Flow



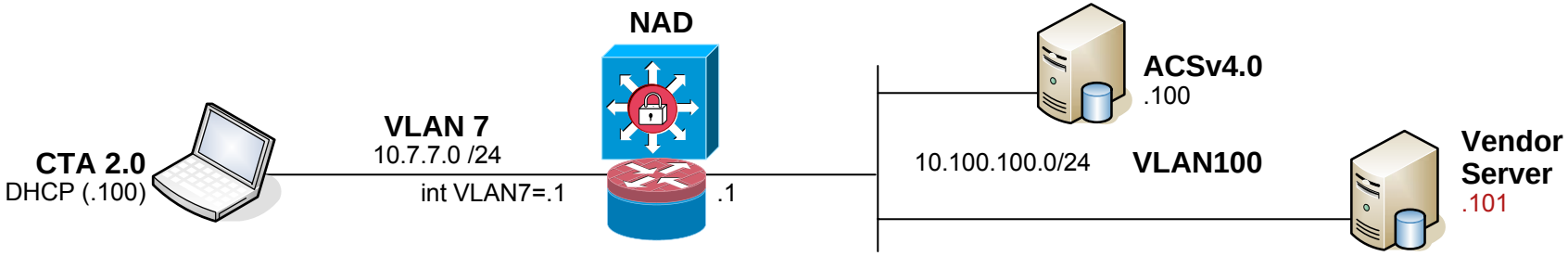


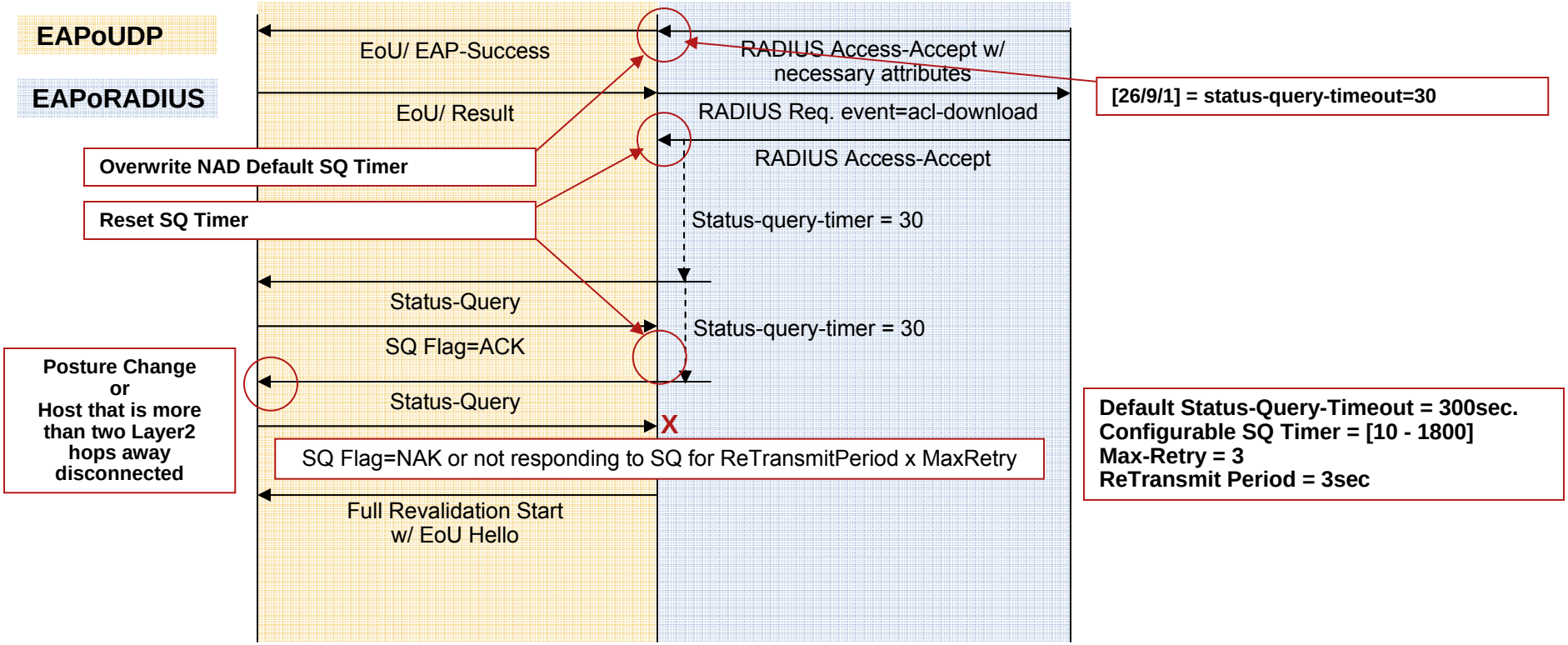
NAC-L2/L3-IP: Posture Validation



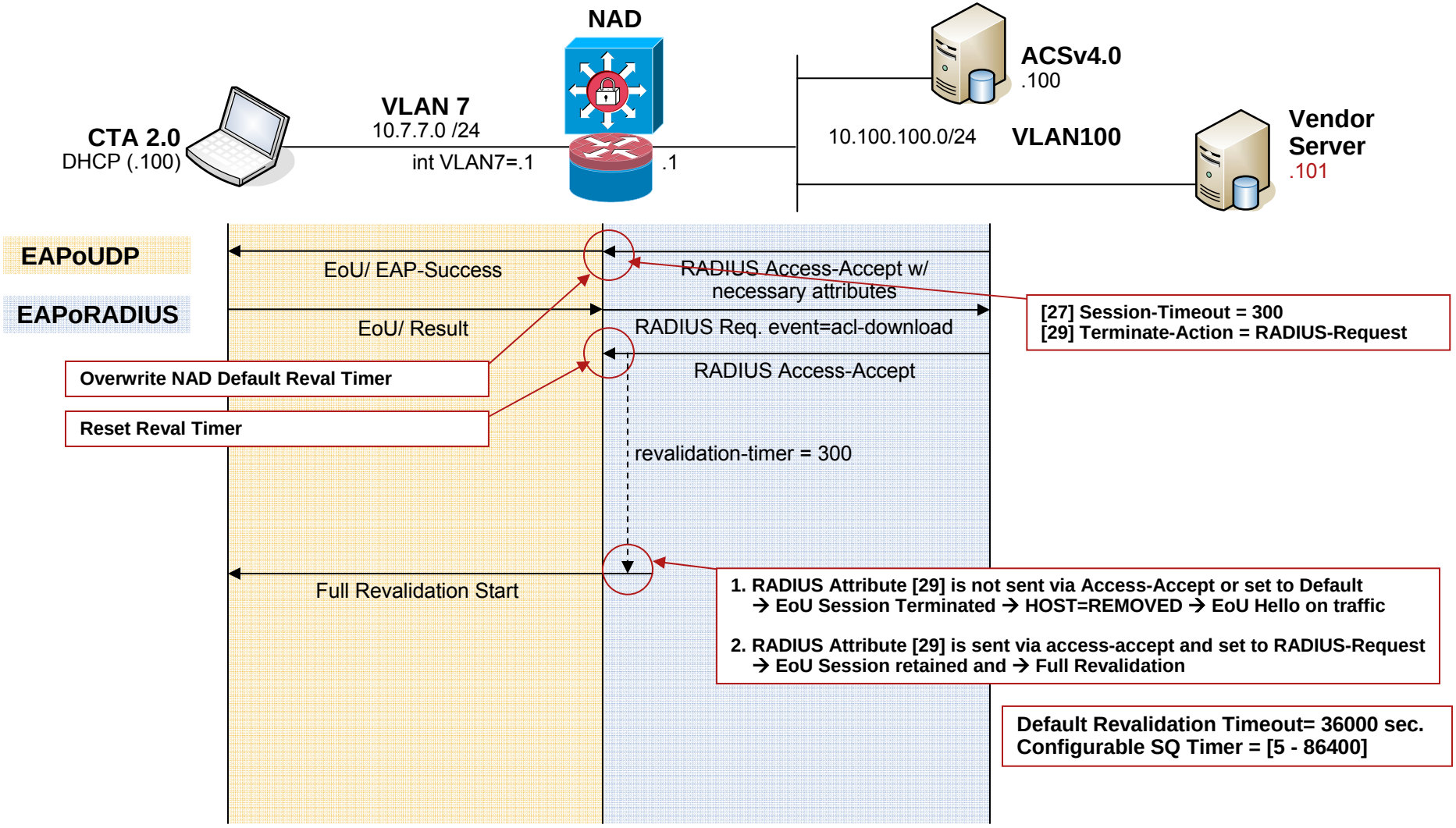
NAC-L2/L3-IP: Status-Query

Key:
[26/9/1] cisco-av-pair
[27] Session-Timeout
[29] Termination-Action

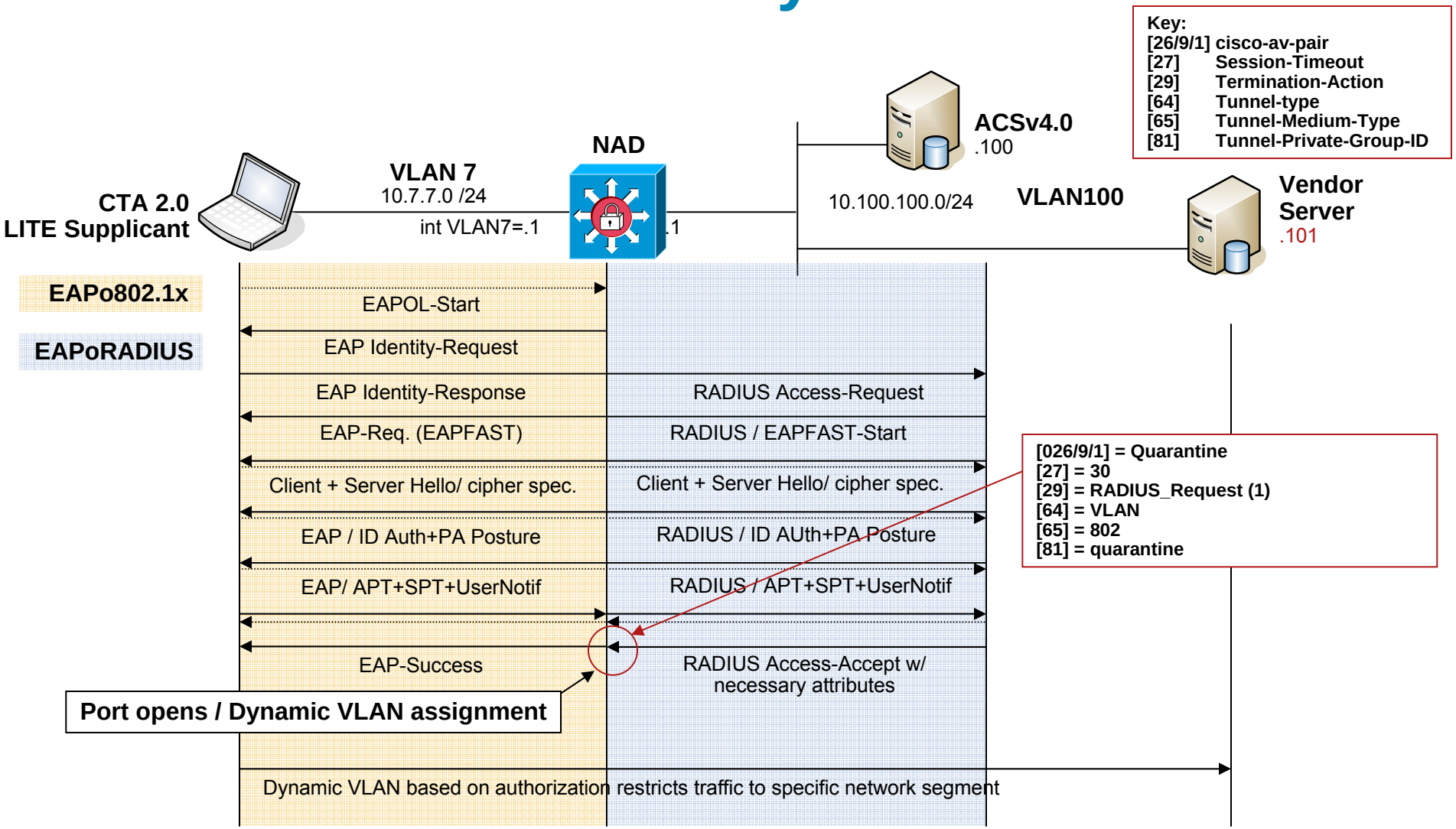




NAC-L2/L3-IP: Revalidation Process

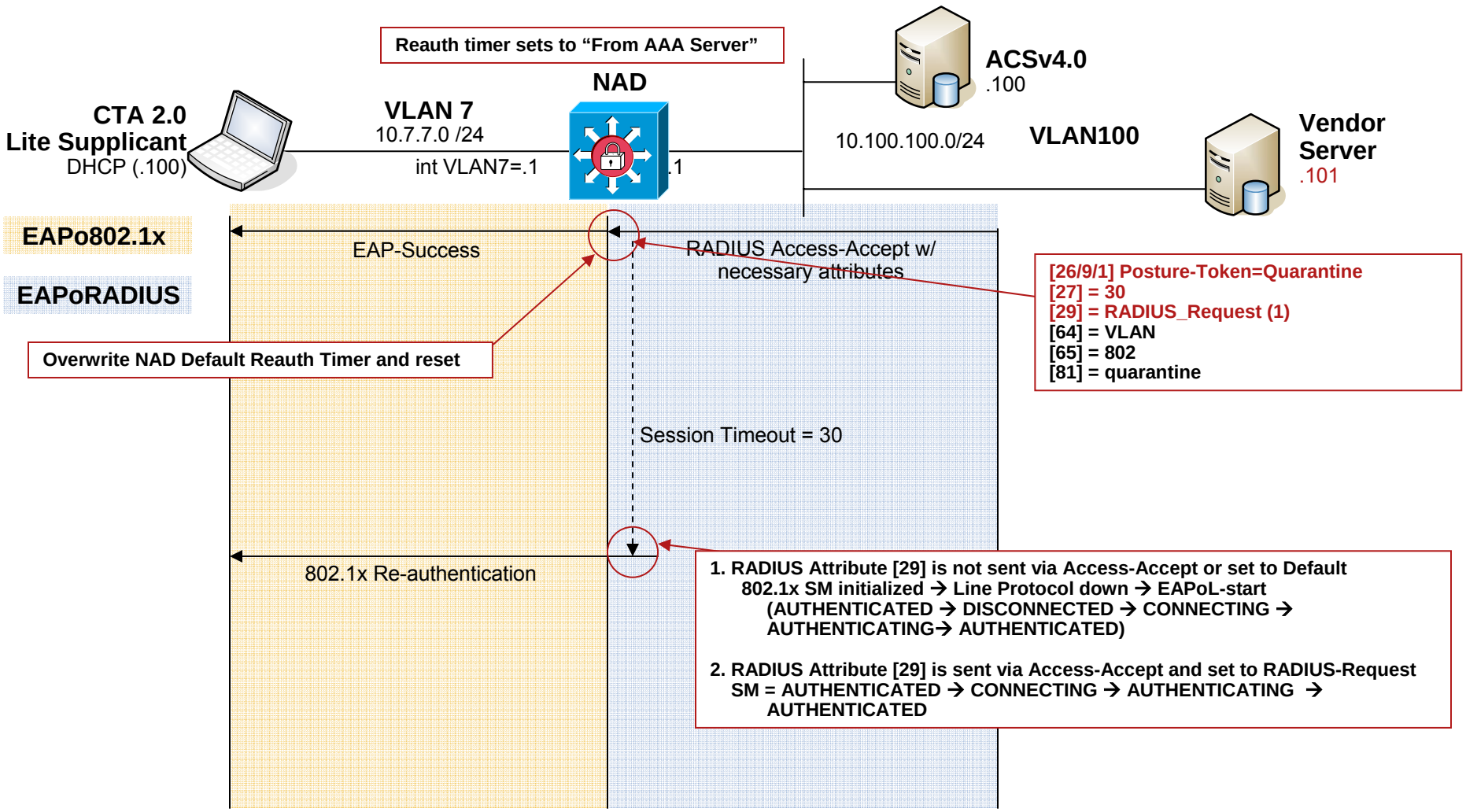


NAC-L2-802.1x: Identity and Posture



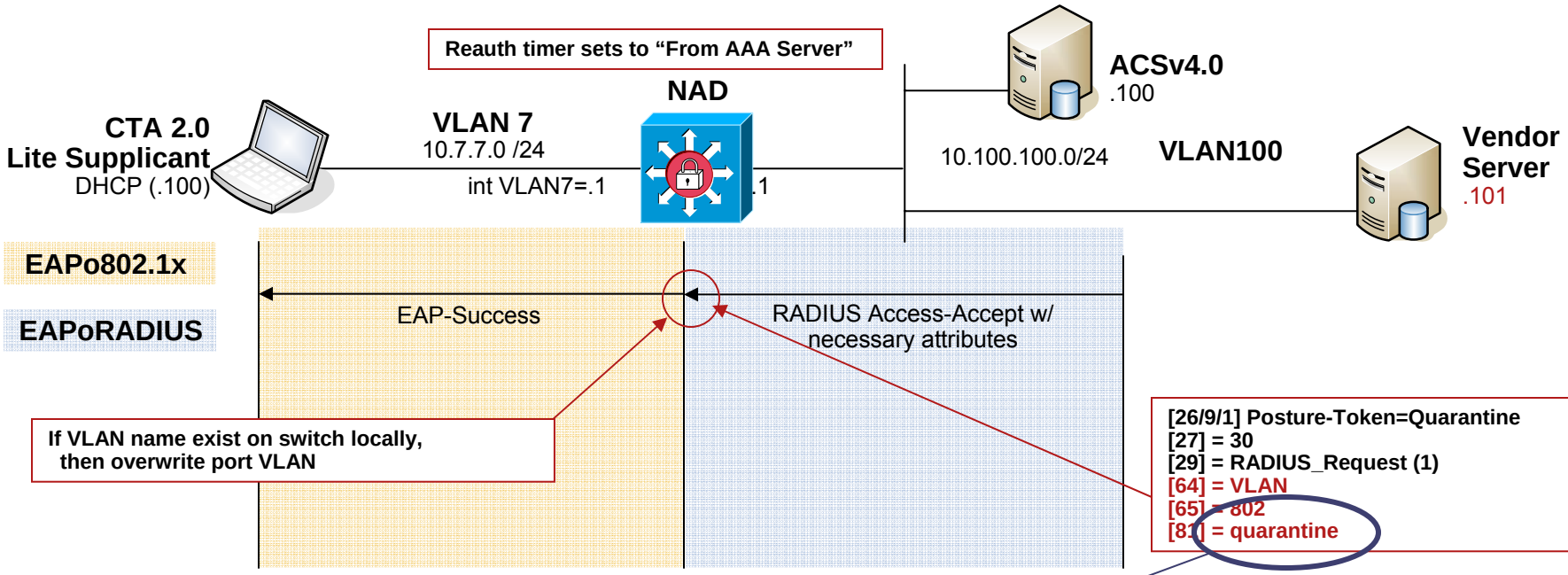
NAC-L2-802.1x assume that ACLs pre-exist on the device

NAC-L2-802.1x: Re-Authentication



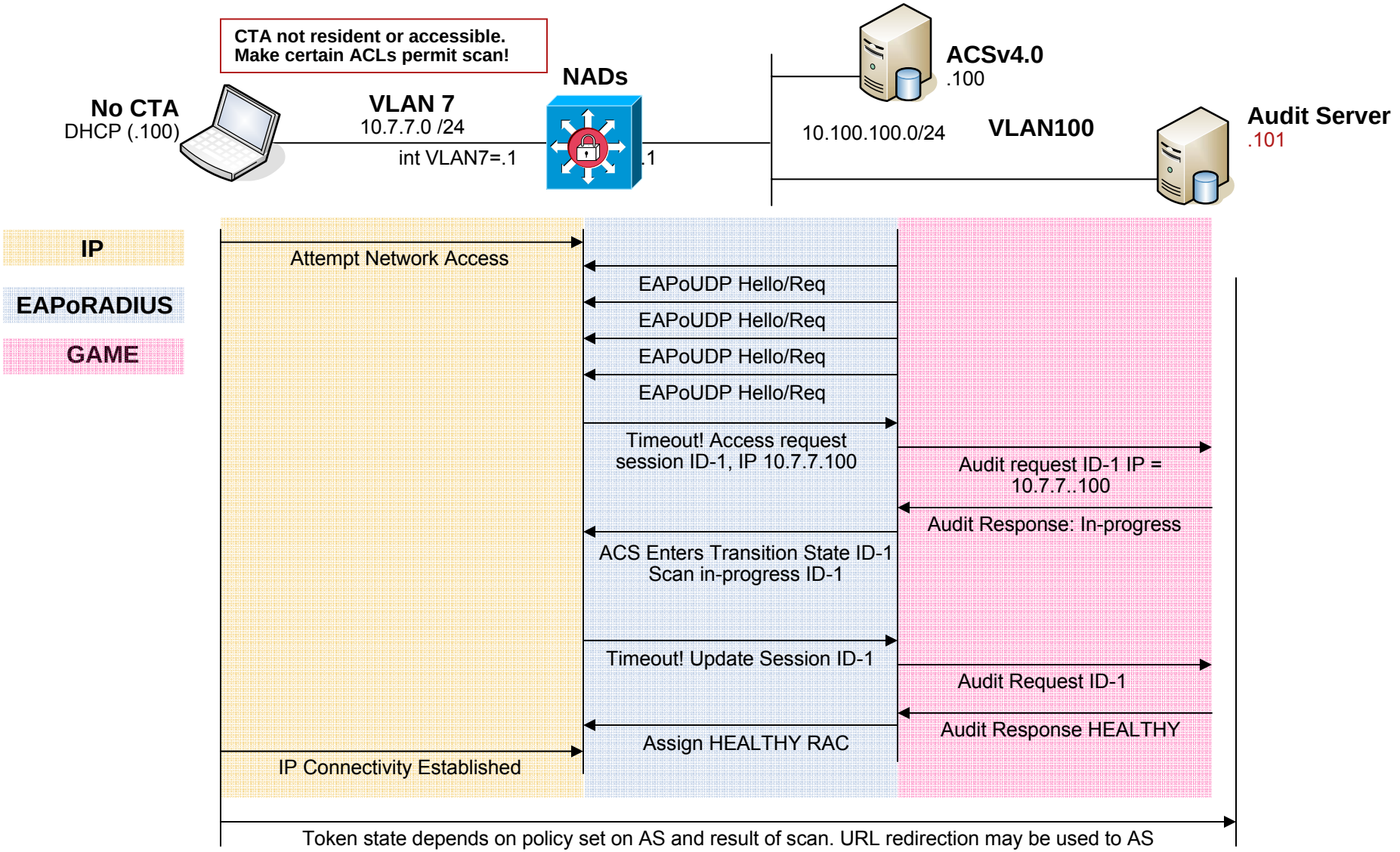
NAC-L2-802.1x: Quarantine

Key:
[26/9/1] cisco-av-pair
[27] Session-Timeout
[29] Termination-Action
[64] Tunnel-type
[65] Tunnel-Medium-Type
[81] Tunnel-Private-Group-ID

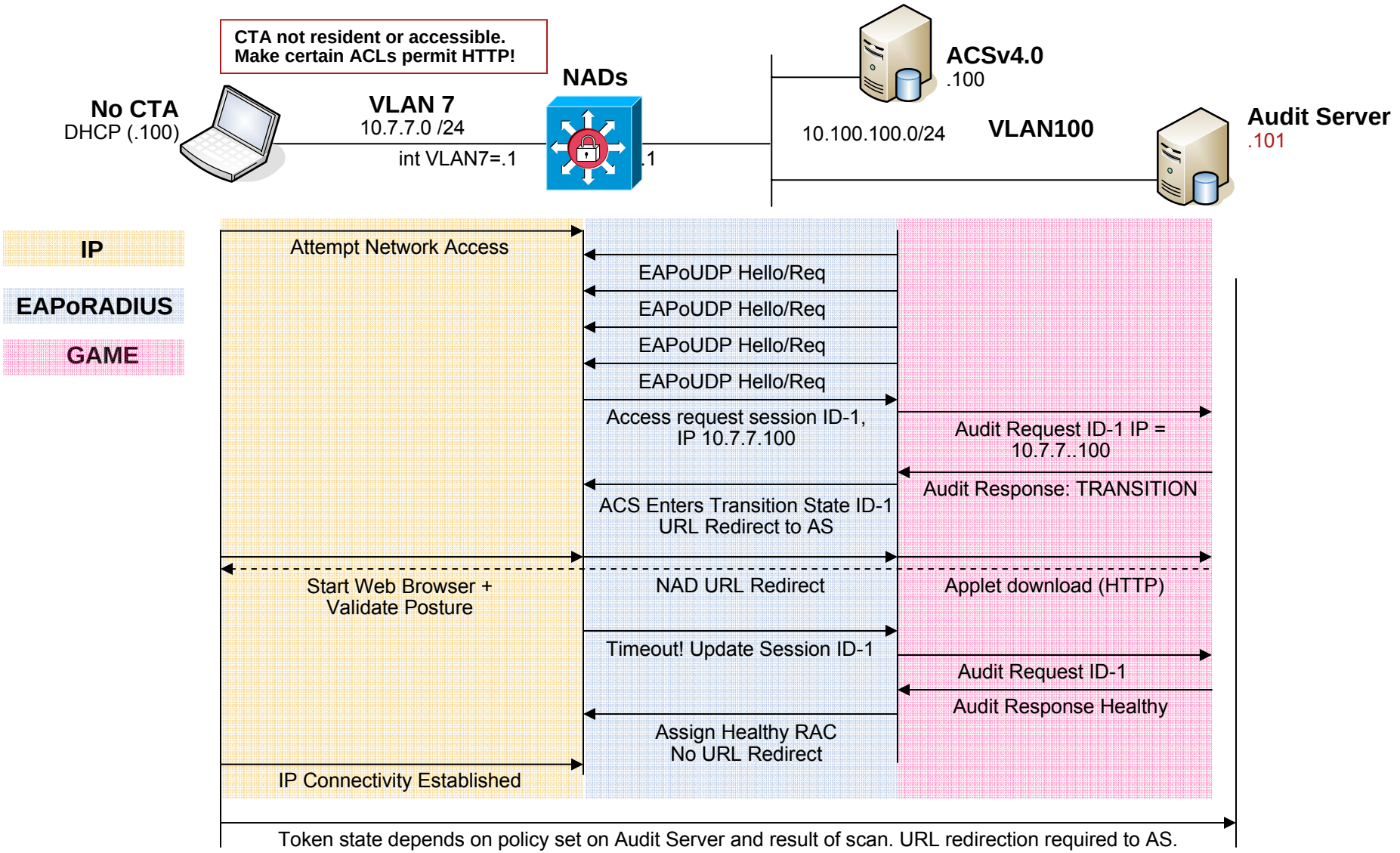



```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/11
10   client                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
11   quarantine                       active
12   temp                             active
13   Guests                           active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

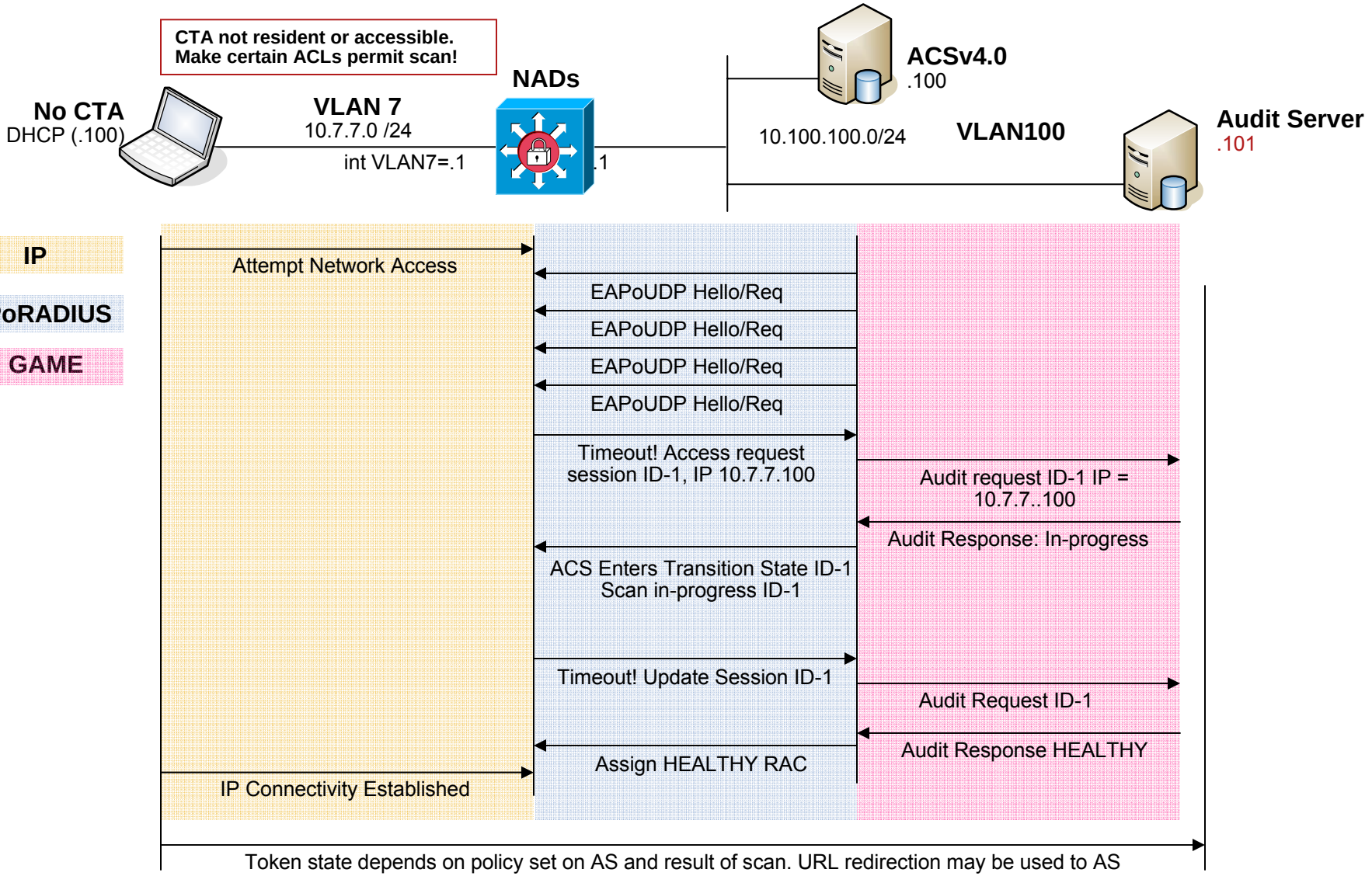
Audit Server: Network Scanning Method



Audit Server: URL Redirection-Applet



Audit Server: Network Scanning Method



Audit Server: URL Redirection-Applet Method