Network Admission Control (NAC)

Technical Overview

Agenda

- NAC Framework: Architecture Overview

  Landscape, components, policy considerations

- Design Considerations

  Modes of operation, component specifics

- Components in Depth

  CTA, ACS, Routers, VPN, Switches, Wireless, CSA

NAC Framework Architecture Overview

The Need for Admission Control

- Viruses, worms, spyware continue to plague organizations

  #1 cause of financial loss to enterprises

- Users are occasionally authenticated, BUT devices are not

- Non compliant and unmanaged devices pose an unacceptable risk

  Often source of infection

  Rogue assets untracked, invisible

- *Device compliance as important as user authentication*

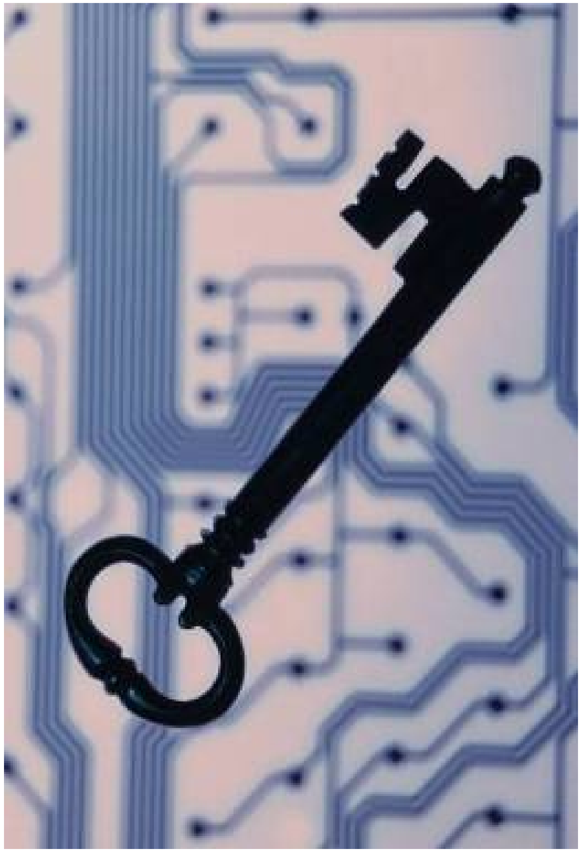
“**Endpoint systems are vulnerable** and represent the most likely point of infection from which a virus or worm can spread rapidly and cause serious disruption and economic damage.”

– Burton Group

***2005 FBI/CSI Report**

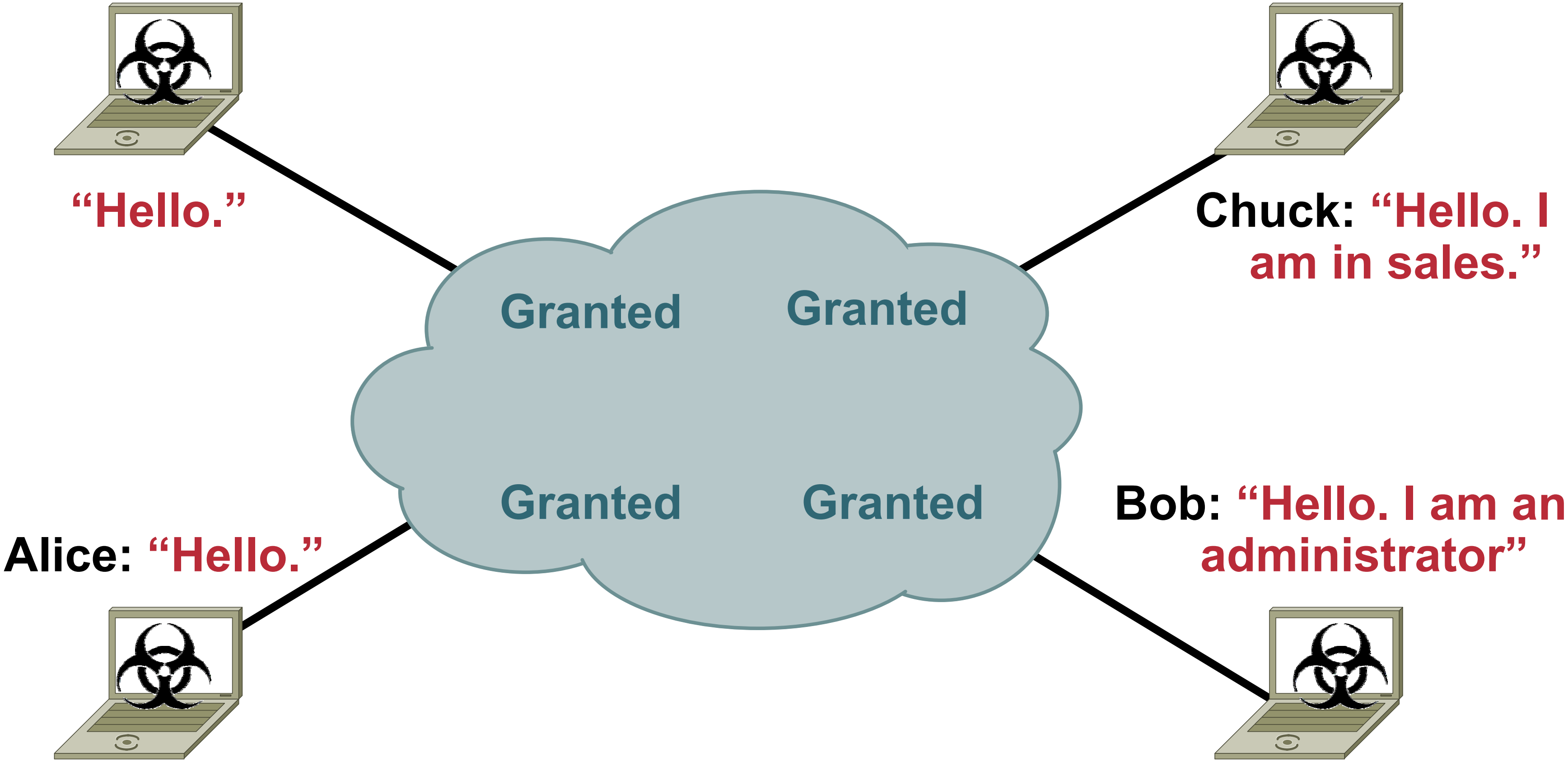
Why Use The Network?

- Every bit of data you are concerned about touches the network
- Every device you are concerned about is attached to the network.
- Gives you the ability to deploy the broadest possible security solution covering the largest number of networked devices
- Also leverages existing infrastructure, security, and management deployments, so it has the smallest IT footprint possible



Prior Methods for Network Admission

Chuck: "I am running an unpatched Windows 2000 system. I am Gigabit Ethernet connected with worm du jour and this one is really nasty. Have a nice day!"



"Hello."

Chuck: "Hello. I am in sales."

Alice: "Hello."

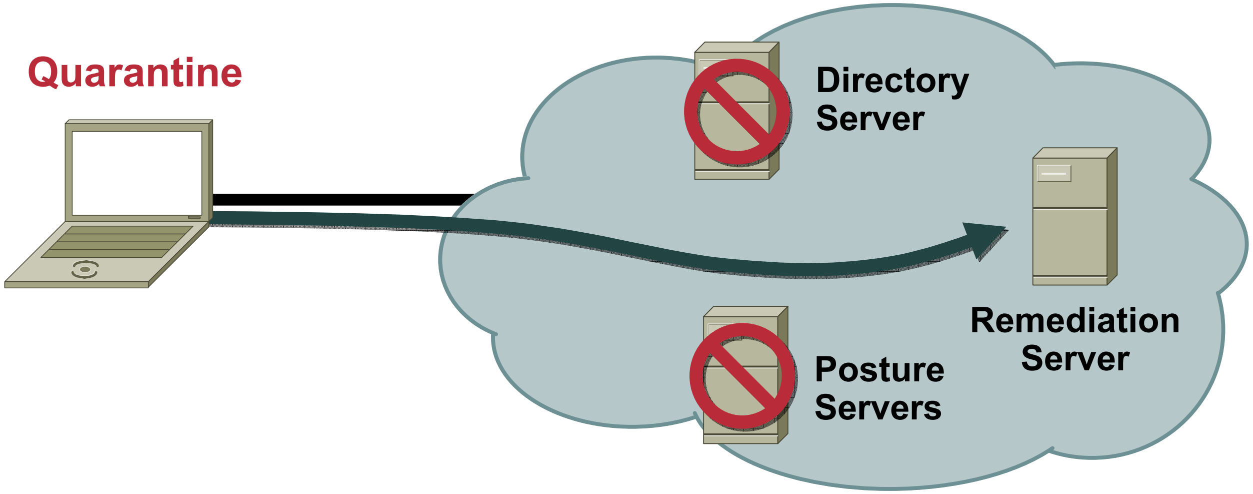
Bob: "Hello. I am an administrator"

The Right Way: Network Admission Control

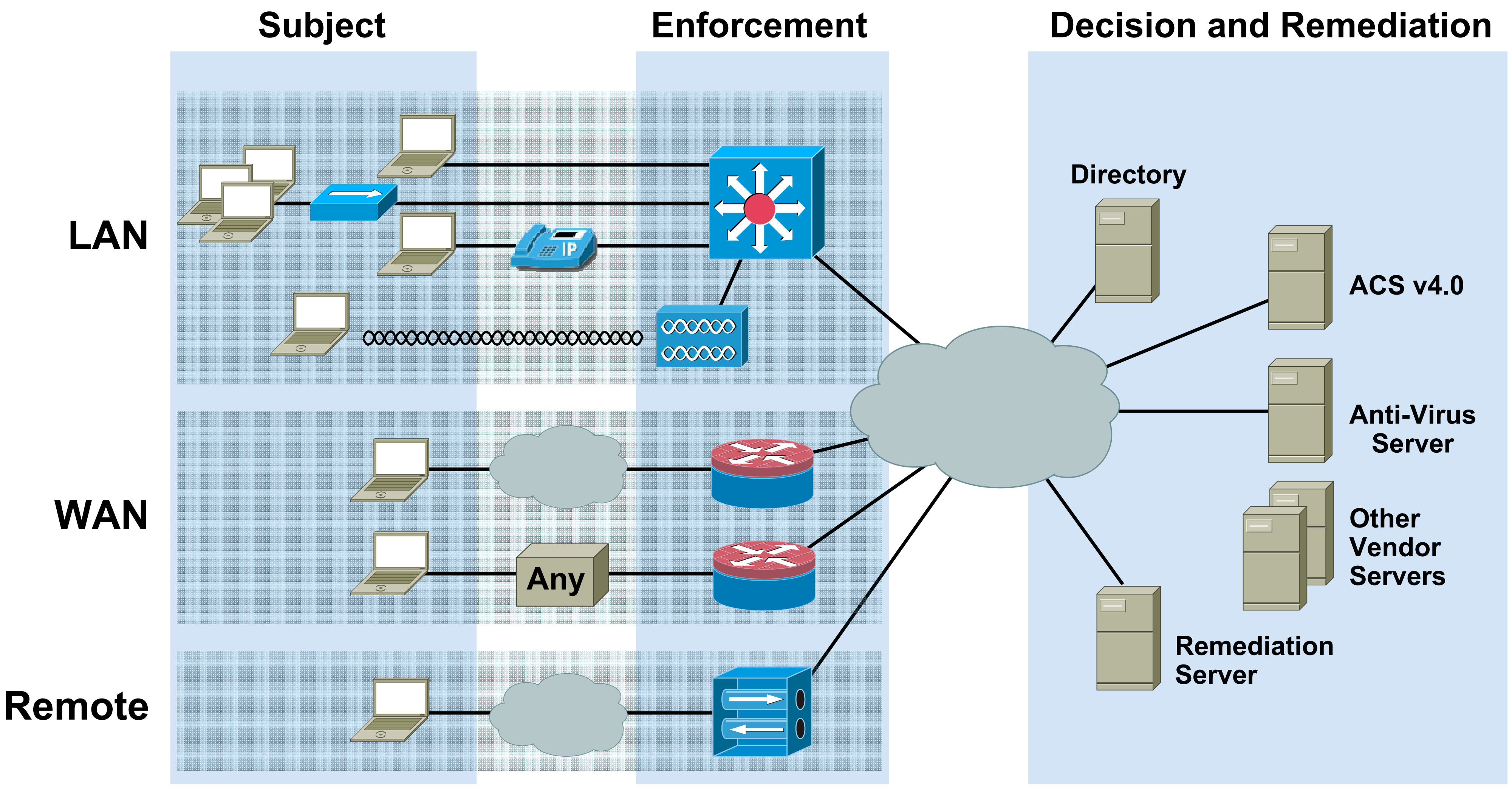
Chuck: Sales
Windows 2000
No Service Pack
No Anti-Virus
No Patch Management

Admission Policy:

1 Identity
1 Windows XP
1 Service Pack 2
1 CTA 2.0
1 Anti-Virus
1 Patch Management



NAC Framework Deployment Scenarios

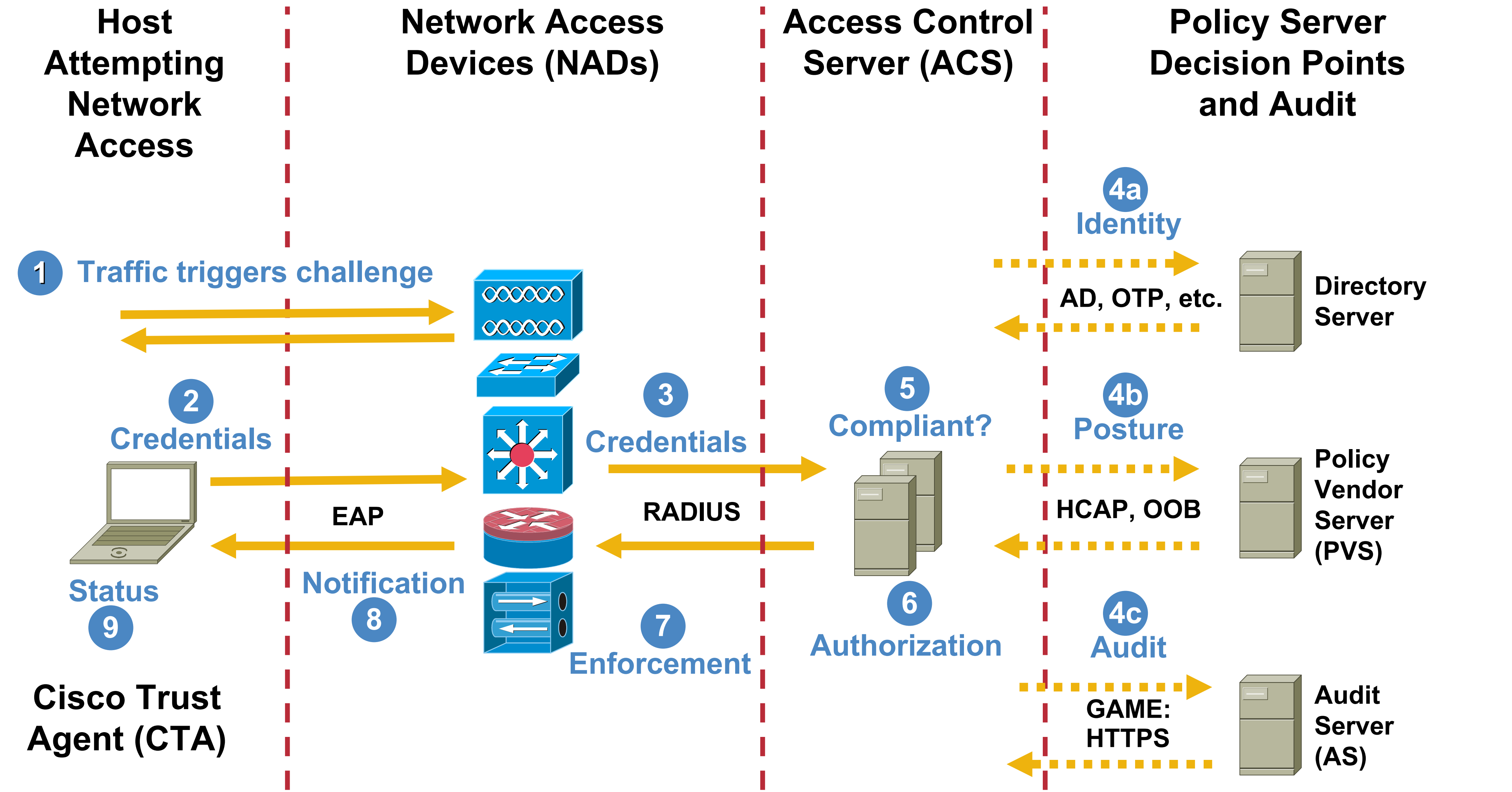


NAC Posture States

- 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.

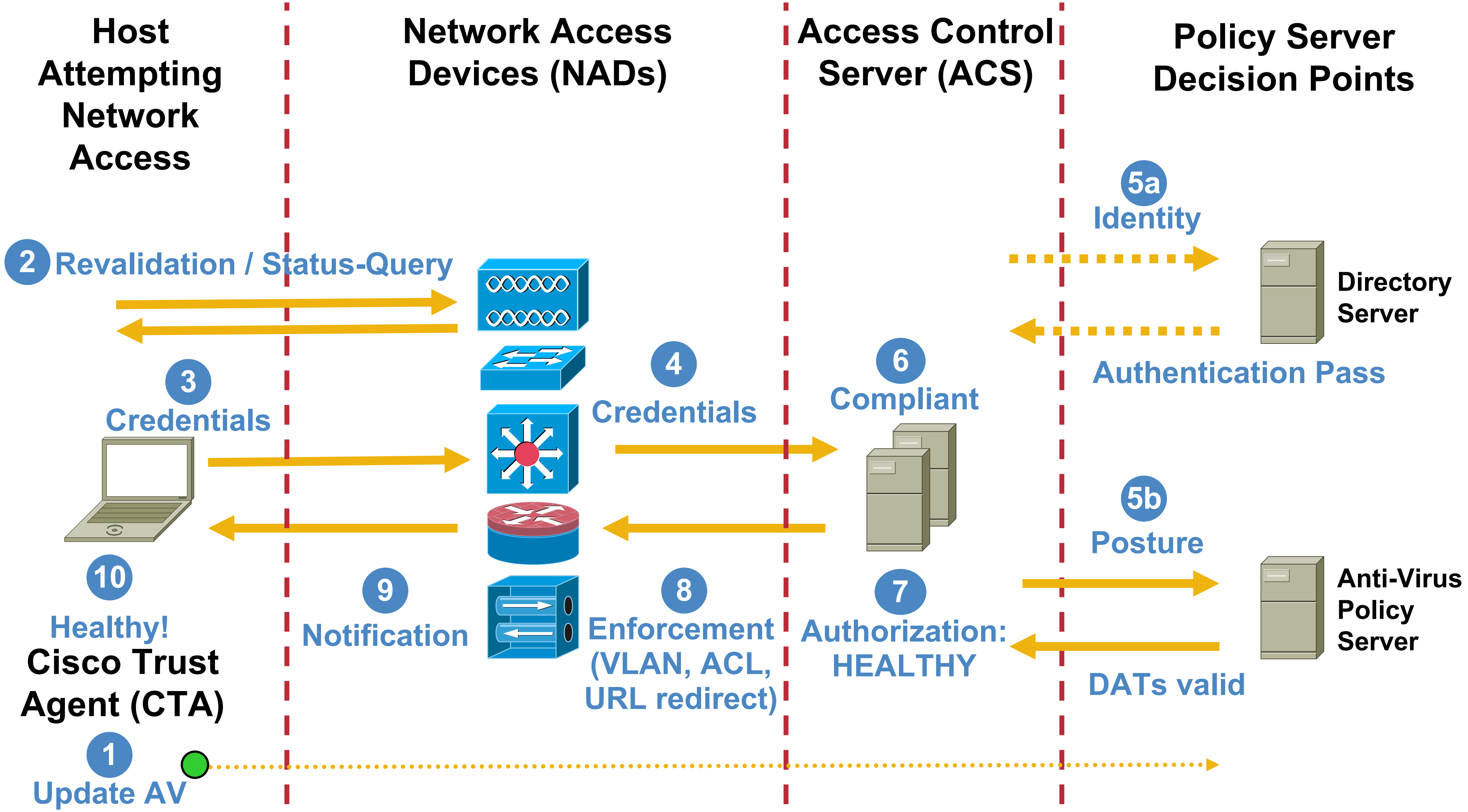
NAC Admission Flow

Key: Optional (dotted arrow) / Mandatory (solid arrow)



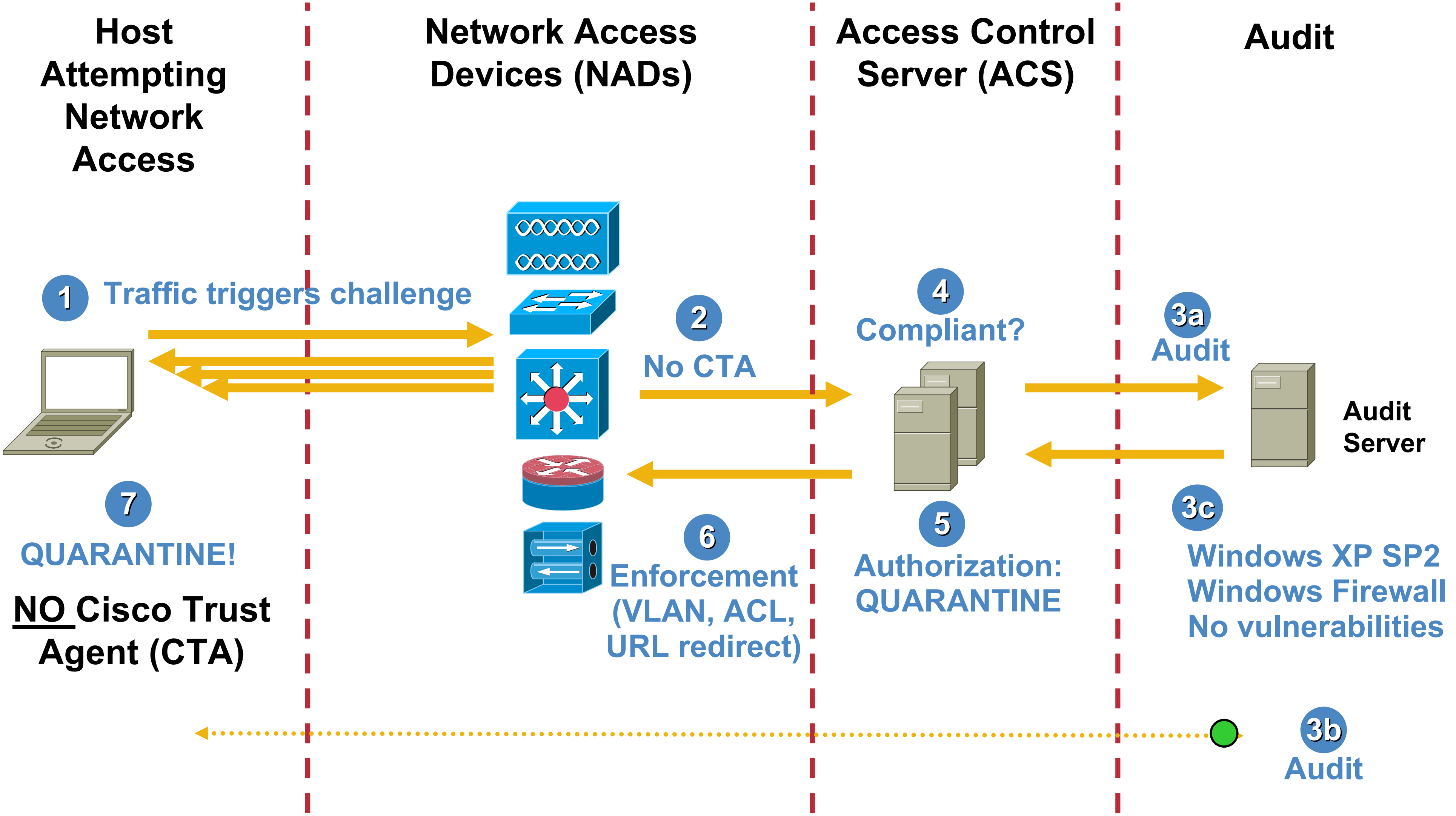
Status: Result of host’s interrogation determines access to network: Full access, limited access, no access, quarantined access

From QUARANTINE to HEALTHY State



Status: HEALTHY now that AV up to date. Could also check patch level, HIPS policy, etc. etc.
Filter may still be applied to provide group access (guest, administrator, HR) but optional.

NAC Agentless Host (NAH)


Host Attempting Network Access
Network Access Devices (NADs)
Access Control Server (ACS)
Audit
1 Traffic triggers challenge
2 No CTA
4 Compliant?
3a Audit
Audit Server
7 QUARANTINE!
NO Cisco Trust Agent (CTA)
6 Enforcement (VLAN, ACL, URL redirect)
5 Authorization: QUARANTINE
3c Windows XP SP2 Windows Firewall No vulnerabilities
3b Audit

Status: Quarantine because OS patch level is compliant except CTA is missing. After CTA is installed, on the next posture check the client would most likely become HEALTHY.

Protocols

- EAP-FAST
  - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a TLS based RFC3748 compliant EAP method.
  - EAP-FAST uses symmetric key algorithms to achieve a tunneled authentication process.
  - The tunnel establishment relies on a Protected Access Credential (PAC) that can be provisioned and managed dynamically by EAP-FAST through AAA server.
  - Allows identity and posture credentials in a single authorization
- Host Credential Authorization Protocol (HCAP)
  - HTTP(S) session between ACS and vendor servers for EAP-based credentials
  - ACS forwards client credentials to one or more vendor servers
  - ACS receives posture token response and optional notification messages from each vendor server
- Generic Authorization Message Exchange (GAME)
  - HTTPS 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 Data Types & Credentials

Attribute/Value pairs are packaged in EAP; 1KB limit per application

OctetArray	Integer32	Unsigned32	String (UTF-8)	IPv4Addr	IPv6Addr	Time (4 octets)	Version (4 x 2-octet sets)
=, !=	=, <, >, !=, >=, <=	=, <, >, !=, >=, <=	=, !=, contains, starts with, regex	wildcards & mask	wildcards & mask	=, <, >, !=, >=, <=	=, <, >, !=, >=, <=

Namespace: <Vendor>:<Application-Type>:<Attribute>

Application:	CTA	CTA	CSA	*Other*
Vendor:	Cisco	Cisco	Cisco	*Various*
App-Type:	PA	Host	HIP	AV, PFW, etc.
Attributes:	PA-Name PA-Version OS-Type OS-Version OS-Release OS-Kernel-Version Machine-Posture-State	ServicePacks HotFixes HostFQDN	CSAMCName, CSAOperationalState CSAStates CSAVersion TimeSinceLastSuccessfullPoll	Software-Name Software-ID Software-Version Scan-Engine-Version DAT-Version DAT-Date Protection-Enabled PFW-policy-version Etc.

Strong NAC Partner Program

http://www.cisco.com/en/US/partners/pr46/nac/partners.html

ANTI VIRUS

McAfee®

ca

SOPHOS

H+BEDV DATENTECHNIK GMBH

AhnLab

NORMAN®

symantec.

F-SECURE®

金山在线 www.kingsoft.com

TREND MICRO

RISING® 瑞星

Panda Software

REMEDIATION

altiris® intuitive > manageability

BIGFIX®

hp® invent

IBM®

iPass®

LANDesk SOFTWARE

PATCHLINK™ The Patch Management Experts™

AUDIT

altiris® intuitive > manageability

QUALYS™ SECURITY ON DEMAND

symantec.

CLIENT SECURITY

Aranda SOFTWARE CORPORATION

BELARC

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

INTERNET SECURITY SYSTEMS™

phoenix® technologies

SENFORCE

TRUST DIGITAL™

BIND VIEW Insight at Work

CITADEL SECURITY SOFTWARE

elemental security

PREDATORWATCH

StillSecure®

ENDFORCE

intel.

SkyRecon™

BLUECAT NETWORKS™ secure networks. simplified.

PREVENTSYS™

symantec.

NEW BOUNDARY TECHNOLOGIES

CONSENTRY™ NETWORKS

Safend

VERDASYS

OPSWAT

C A Y M A S SYSTEMS

CREDANT™ TECHNOLOGIES Be mobile. Be secure.

FIBERLINK

TriGeo Network Security

tenebril™

vmware®

PFU a Fujitsu company

infoexpress network integrity enforcement

ECUTEL

secure elements

WEBSENSE® SECURING PRODUCTIVITY.

Microsoft/Cisco Joint Announcement October 18, 2004

- **Cisco and Microsoft Team to Improve Network Security**

  Companies will work toward compatibility, interoperability of respective security architectures

  Cisco and Microsoft announced that they will work together to ensure compatibility and develop interoperability between their respective security architectures. For Cisco this collaboration further demonstrates the company's commitment to reinventing network security.

Interoperability **Integration** **Standardization**

NAC Advantages

- Appliance and Framework solutions
- Comprehensive span of control
  - Routers, Switches, VPNs, wireless, plus complex deployments, including IP Telephony
- 100% host and device compliance
  - No need to install multiple servers
- Controls managed, unmanaged, and guest endpoint devices
  - Only solution to integrate device posture and user identity
- Device health decisions made at the network, not on the endpoint device
  - Limits ability to misrepresent device as “healthy” to the network
- Enjoys widest use of any technology
  - Including the most robust partner program
- NAC Appliance interoperable with NAC Framework
  - Future integration will provide smooth transition to architecture-based approach

NAC Benefits

Dramatically Improves Security

- Ensures endpoints (laptops, PCs, PDAs, servers, etc.) conform to security policy
- Proactively protects against worms, viruses, spyware, and malware
- Focuses operations on prevention, not reaction

Extends Existing Investments

- Broad integration with multi-vendor antivirus, security, and management software
- Enhances investment in network infrastructure and vendor software

Increases Enterprise Resilience

- Comprehensive admission control across all access methods (LAN, WAN, Wireless, VPN, etc.)
- Prevents non-compliant and rogue endpoints from impacting network availability
- Reduces OpEx related to identifying and repairing non-compliant, rogue, and infected systems

Design Considerations

Getting Ready for NAC Framework

- You must consider your
    - Creation and Deployment of Security Policy
    - Public Key Infrastructure (PKI)
    - Software Deployment and Updates
    - Network Access Devices (NADs)
    - Policy Servers (ACS, Directory, Audit, Patch)
    - NAC Agentless Hosts (NAHs)
    - Logging, Monitoring, and Reporting
    - Support Desk & End-User Communications

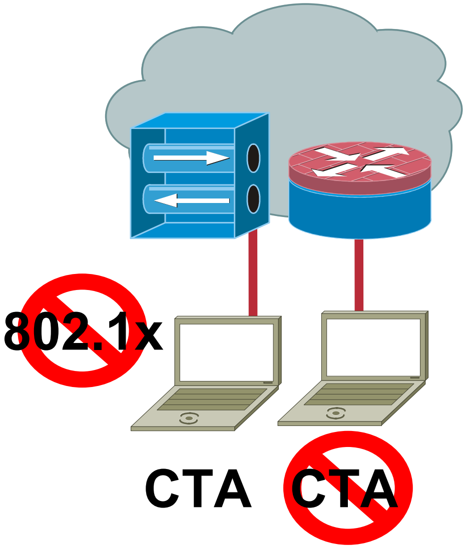
NAC Enforcement Features/Tradeoffs

- NAC L3 IP—EAPoUDP for posture only (Routers and VPN)
- NAC L2 IP—EAPoUDP for posture only (L2 switchports)
- NAC L2 802.1x—EAP over 802.1x (L2 switchports)

Feature	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
Trigger Mechanism	Data Link Up	DHCP or ARP	Forwarded Packet
Machine Identity	X		
User Identity	X		
Posture	X	X	X
VLAN Assignment	X		
URL-Redirection		X	X
Downloadable ACLs	6500-only (PBACLs)	X	X
Posture Status Queries		X	X
802.1x Posture Change	X		

NAC L3 IP: Overview

- Ideal for L3 multi-hop: routers and VPN concentrators only
- Posture-only authorization, PEAP-GTC
- EAPoUDP triggered by new IP packet
- Enforcement via per-host L3/L4 ACLs
- Status Query and URL redirection
- Clientless hosts supported with default posture
- Default ACL determines default access



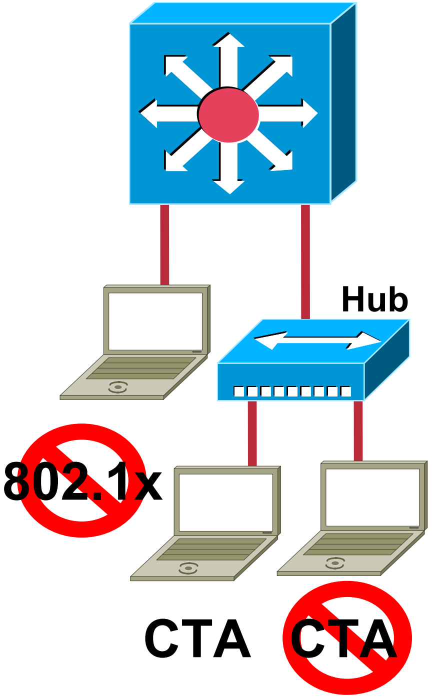
NAC L2 IP: Overview

- Ideal for “Dangling Hub Syndrome”: switches only
- Posture-only authorization, PEAP-GTC
- EAPoUDP triggered by ARP request:

    IOS: Port ACL, IP device tracking, & DHCP snooping

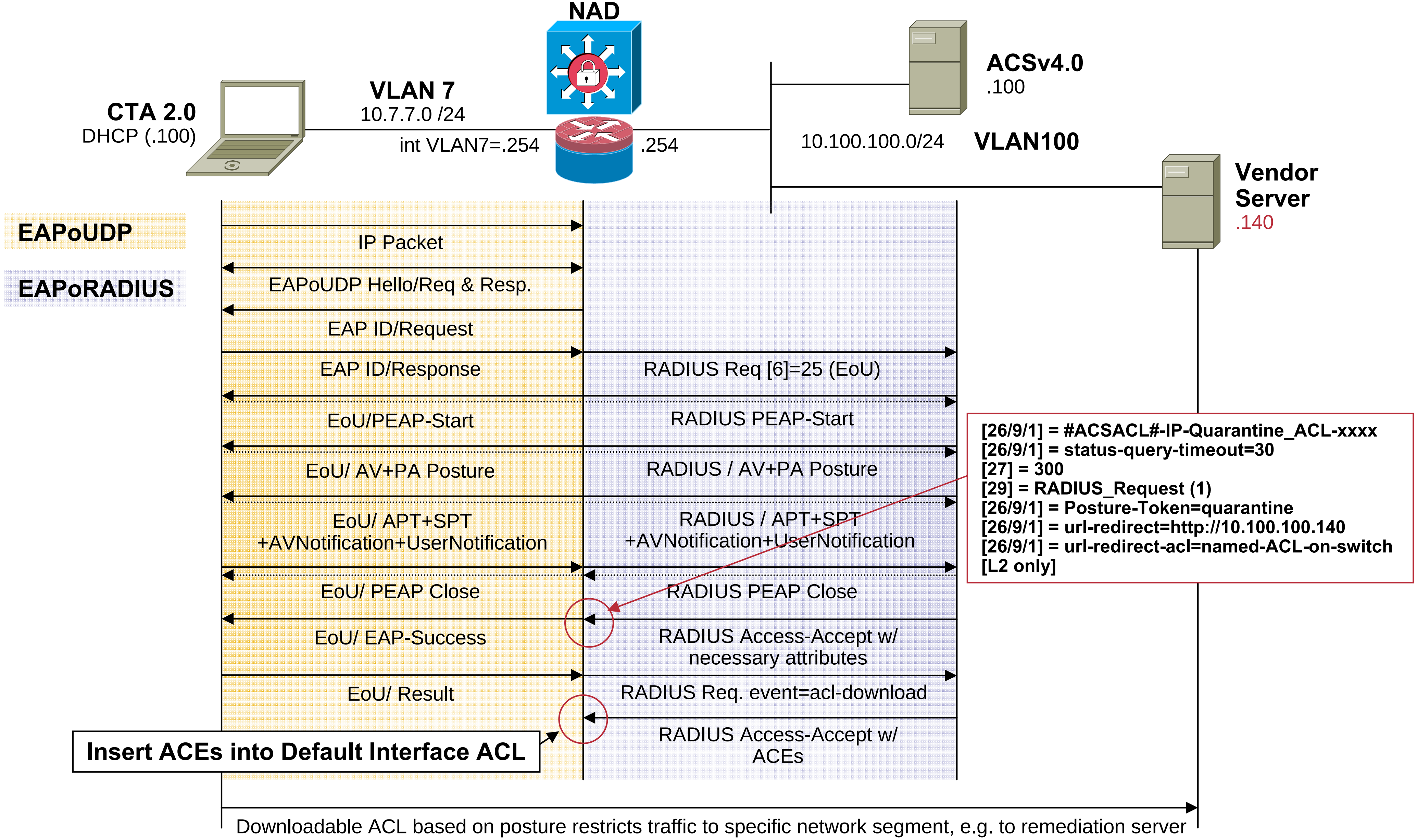
    CatOS: ARP inspection, DHCP snooping

- Enforcement via per-host L3/L4 ACLs
- Status Query and URL redirection
- CTA is not required with NAH Audit



NAC-L2/L3-IP: Posture Validation Flow

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

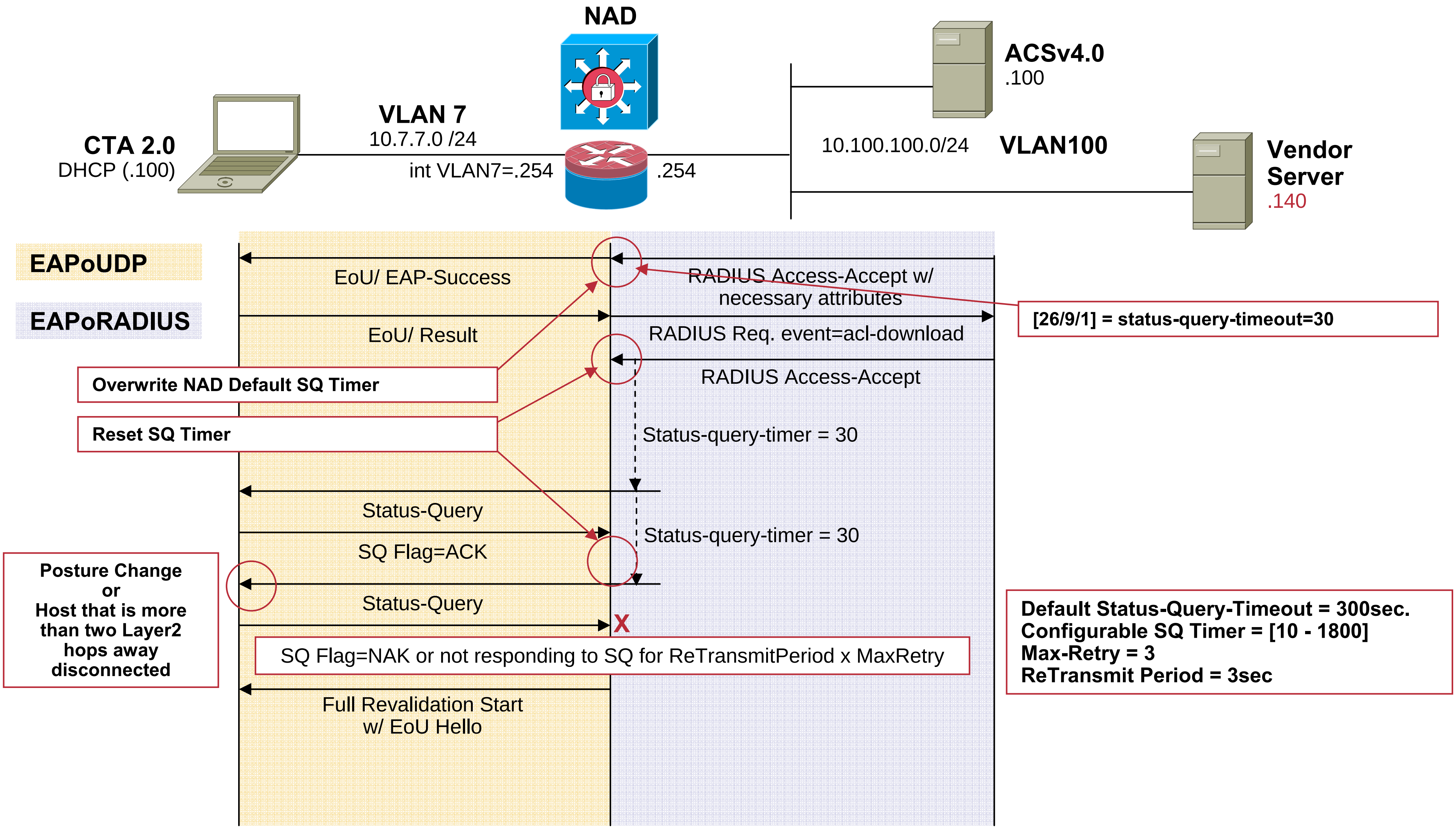


[26/9/1] = #ACSACL#-IP-Quarantine_ACL-xxxx
[26/9/1] = status-query-timeout=30
[27] = 300
[29] = RADIUS_Request (1)
[26/9/1] = Posture-Token=quarantine
[26/9/1] = url-redirect=http://10.100.100.140
[26/9/1] = url-redirect-acl=named-ACL-on-switch
[L2 only]

Insert ACEs into Default Interface ACL

Downloadable ACL based on posture restricts traffic to specific network segment, e.g. to remediation server

NAC-L2/L3-IP: Status-Query (Reassessment)



[26/9/1] = status-query-timeout=30

Overwrite NAD Default SQ Timer

Reset SQ Timer

Posture Change
or
Host that is more than two Layer2 hops away disconnected

SQ Flag=NAK or not responding to SQ for ReTransmitPeriod x MaxRetry

Default Status-Query-Timeout = 300sec.
Configurable SQ Timer = [10 - 1800]
Max-Retry = 3
ReTransmit Period = 3sec

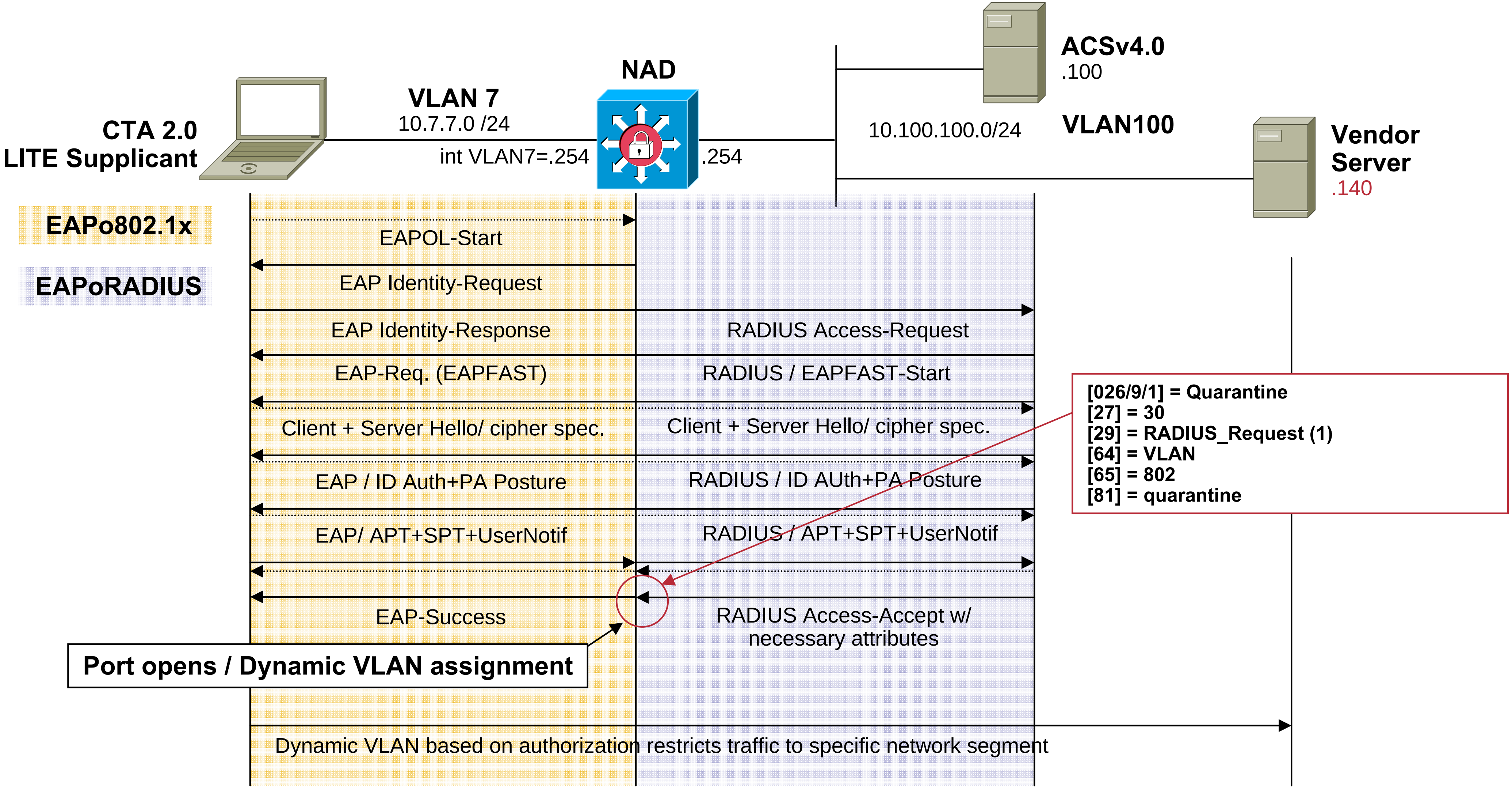
NAC L2 802.1x: Overview

- Identity and/or posture authorization: switches only
- Leverages existing 802.1x (EAP) L2 session to perform posture assessment and enforcement
  - EAP-FAST required for posture authorization
  - MSCHAPv2, EAP-TLS, and EAP-GTC
- Enforcement via dynamic VLANs
  - 6500 also supports Policy Based ACLs

NAC L2 802.1x:
Identity and Posture

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



CTA 2.0
LITE Supplicant

VLAN 7
10.7.7.0 /24
int VLAN7=.254

NAD
.254

10.100.100.0/24

ACSv4.0
.100

VLAN100

Vendor
Server
.140

EAPo802.1x

EAPoRADIUS

EAPOL-Start

EAP Identity-Request

EAP Identity-Response

RADIUS Access-Request

EAP-Req. (EAPFAST)

RADIUS / EAPFAST-Start

Client + Server Hello/ cipher spec.

Client + Server Hello/ cipher spec.

EAP / ID Auth+PA Posture

RADIUS / ID AUth+PA Posture

EAP/ APT+SPT+UserNotif

RADIUS / APT+SPT+UserNotif

EAP-Success

RADIUS Access-Accept w/
necessary attributes

[026/9/1] = Quarantine
[27] = 30
[29] = RADIUS_Request (1)
[64] = VLAN
[65] = 802
[81] = quarantine

Port opens / Dynamic VLAN assignment

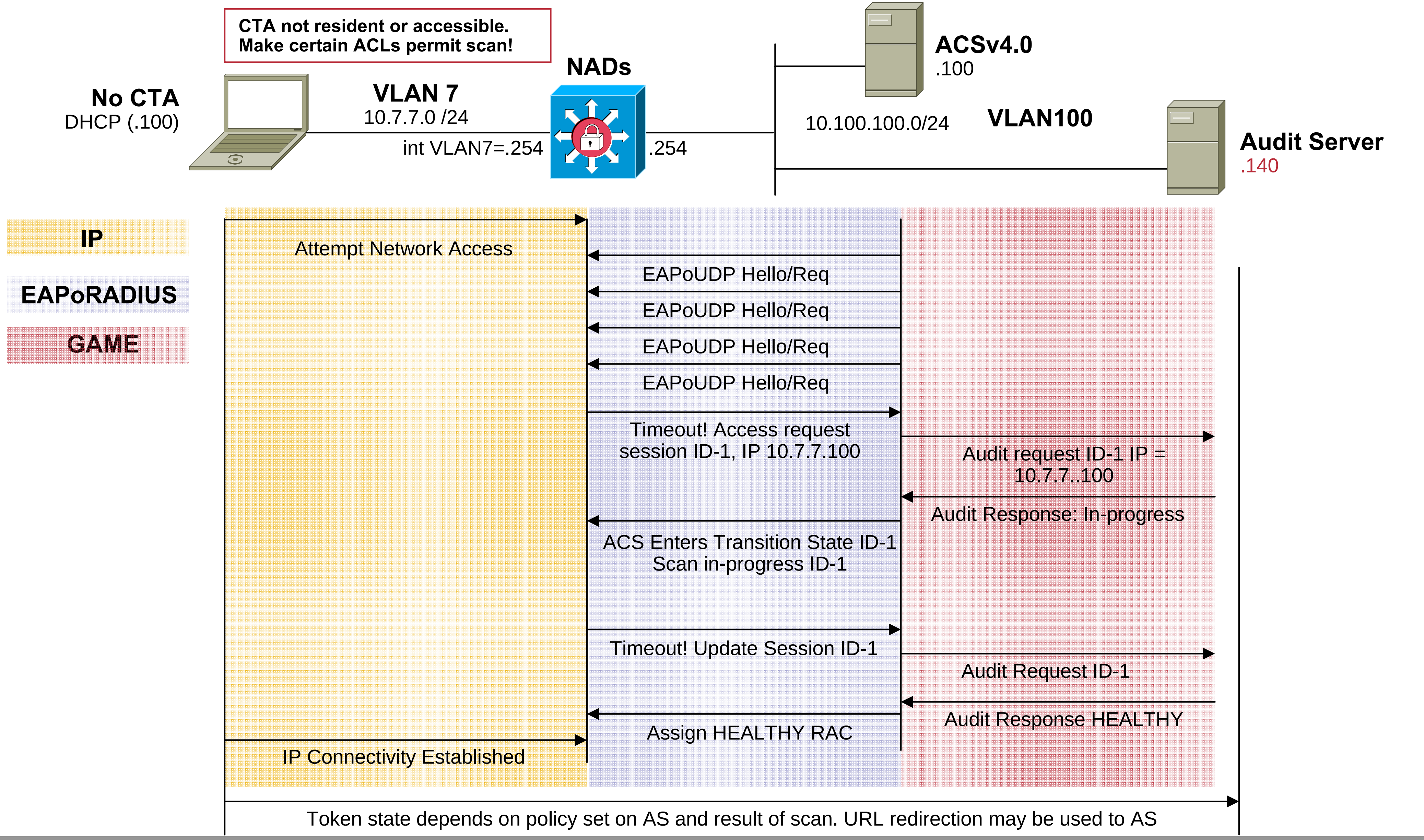
Dynamic VLAN based on authorization restricts traffic to specific network segment

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

NAH Exceptions and Whitelisting

Component	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
NAD (distributed)	MAC-Auth-Bypass (6500 only, identity + posture)	Device Type, IP, or MAC; Intercept ACL (IP/MAC)	Device Type, IP, or MAC; Intercept ACL (IP)
ACS whitelist (centralized)	MAC-Auth-Bypass (above)	MAC\IP wildcards (posture only)	MAC\IP wildcards (posture only)
Audit (centralized)	Active network scan, remote login, browser object, hardware/software inventory		

Audit Server: Network Scanning Method



CTA not resident or accessible.
Make certain ACLs permit scan!

Attempt Network Access

EAPoUDP Hello/Req

EAPoUDP Hello/Req

EAPoUDP Hello/Req

EAPoUDP Hello/Req

Timeout! Access request session ID-1, IP 10.7.7.100

Audit request ID-1 IP = 10.7.7..100

Audit Response: In-progress

ACS Enters Transition State ID-1
Scan in-progress ID-1

Timeout! Update Session ID-1

Audit Request ID-1

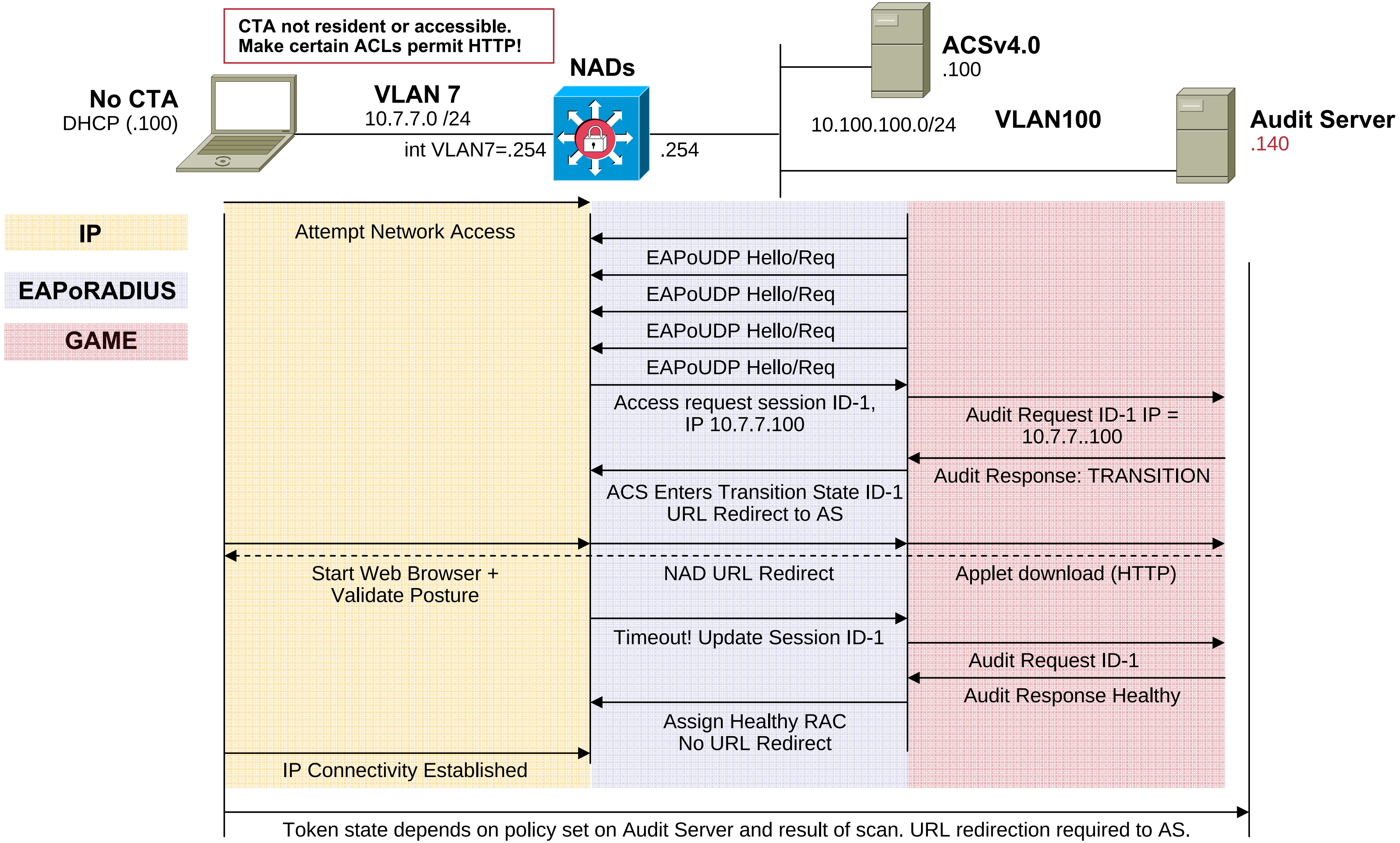
Audit Response HEALTHY

Assign HEALTHY RAC

IP Connectivity Established

Token state depends on policy set on AS and result of scan. URL redirection may be used to AS

Audit Server: URL Redirection-Applet Method



CTA not resident or accessible.
Make certain ACLs permit HTTP!

No CTA
DHCP (.100)

VLAN 7
10.7.7.0 /24
int VLAN7=.254

NADs
.254

ACSv4.0
.100

10.100.100.0/24
VLAN100

Audit Server
.140

IP

EAPoRADIUS

GAME

Attempt Network Access

EAPoUDP Hello/Req

EAPoUDP Hello/Req

EAPoUDP Hello/Req

EAPoUDP Hello/Req

Access request session ID-1,
IP 10.7.7.100

Audit Request ID-1 IP =
10.7.7..100

Audit Response: TRANSITION

ACS Enters Transition State ID-1
URL Redirect to AS

Start Web Browser +
Validate Posture

NAD URL Redirect

Applet download (HTTP)

Timeout! Update Session ID-1

Audit Request ID-1

Audit Response Healthy

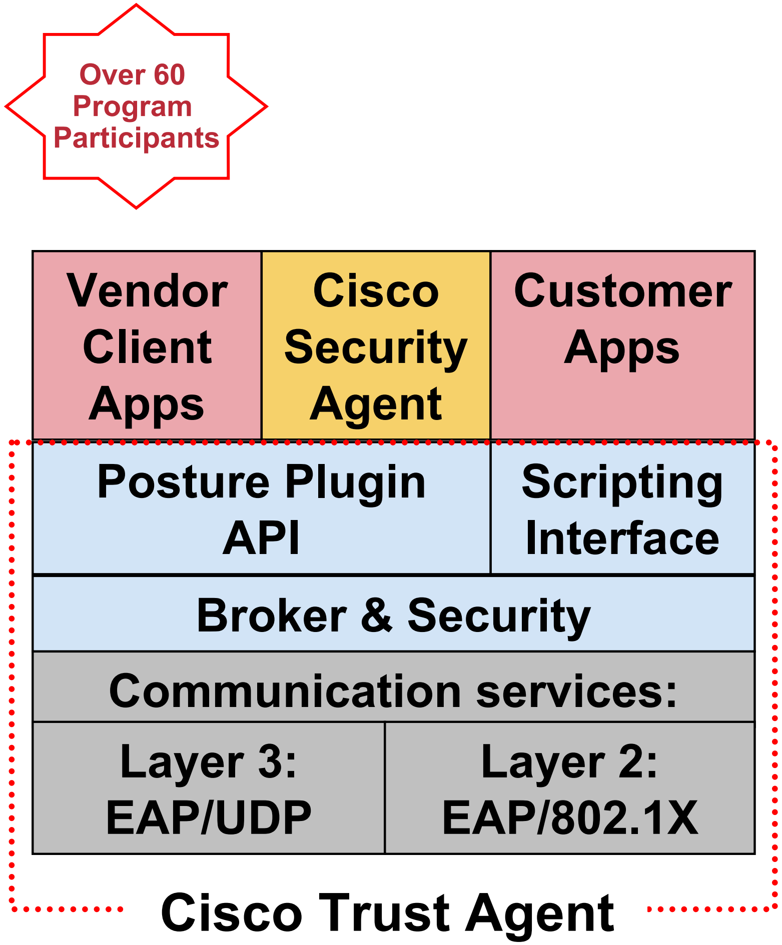
Assign Healthy RAC
No URL Redirect

IP Connectivity Established

Token state depends on policy set on Audit Server and result of scan. URL redirection required to AS.

Design Considerations: Components In Depth

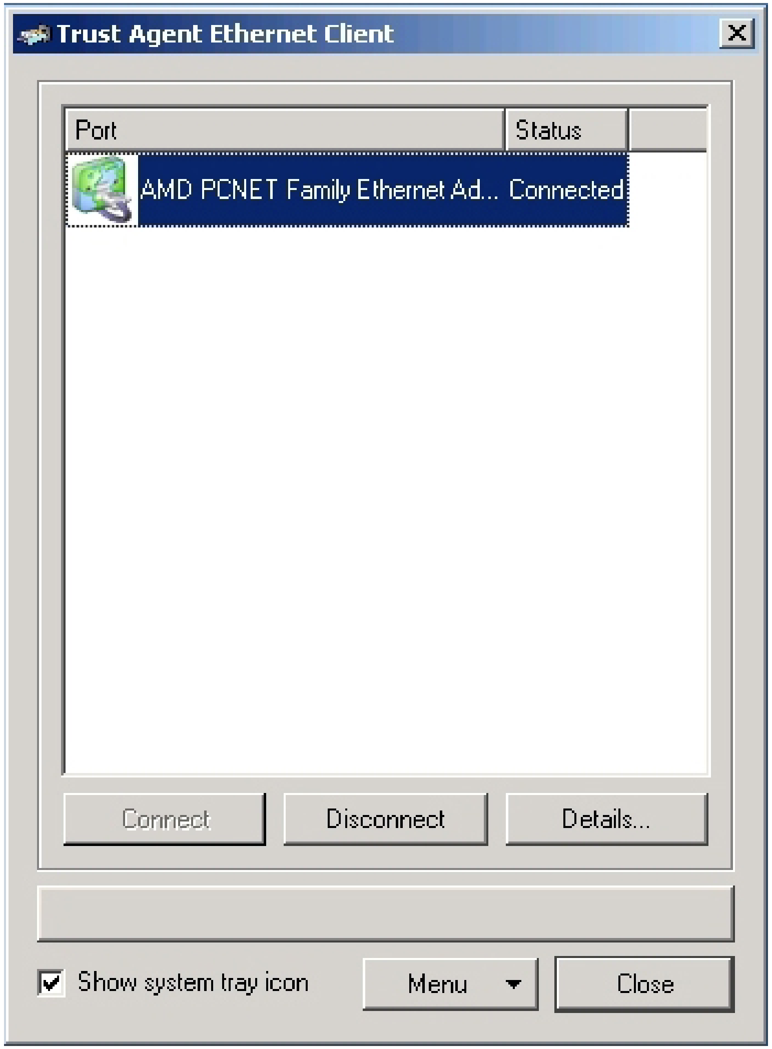
Cisco Trust Agent 2.0



- Supported on Windows 2000, XP, 2003 and Red Hat Linux
- Supports 2 transport layers
  - EAPoUDP - layer 3
  - EAPo802.1x - layer 2 (Windows only)
- Includes OEM 802.1x supplicant from Meetinghouse Data Communications (MDC)
  - Wired functionality only
  - Can be replaced by a retail version from either Funk or MDC for full feature support
- Gathers OS information including patch and hotfixes
- Includes Customer Scripting Interface for custom posture information gathering
- Backward compatible with CTA 1.0 posture plugins from NAC Program Participants
- Expanded debug/diagnostic output

Cisco Trust Agent (CTA) 2.0 Features

- **Free**
- **Wired only supplicant (on Windows platforms only)**
- **EAP-FAST only with MSCHAPv2, EAP-TLS, and EAP-GTC**
- **Initiates EAPoL-Start on posture plugin state change**
- **DHCP release/renews**



Port	Status
AMD PCNET Family Ethernet Ad...	Connected

☑ Show system tray icon

CTA and Supplicant Comparisons

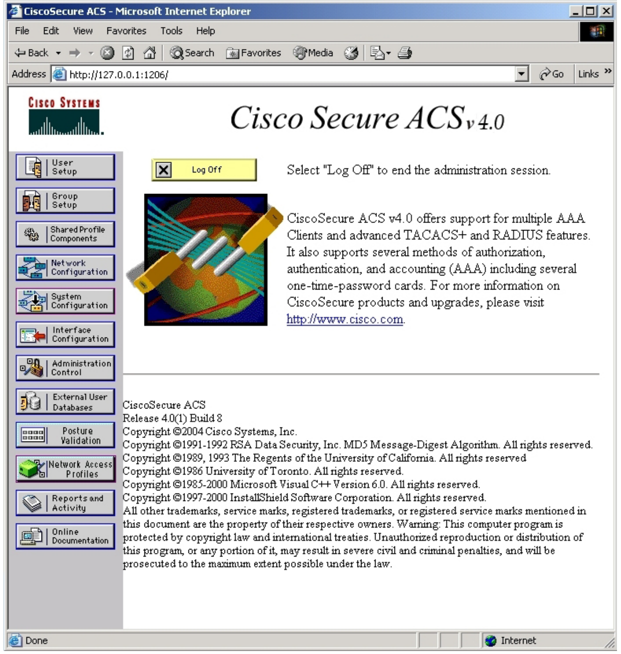
Feature	CTA 1.0	CTA 2.0	Meetinghouse Aegis	Funk Odyssey
Retail Cost	Free	Free	**	**
NAC-L2/L3-IP	X	X	?	?
NAC L2 802.1x Wired		X (Windows)	X	X
NAC L2 802.1x Wireless			X	X
PEAP-GTC	X	X	X	X
EAP-FAST*		X	X	X
Others			X	X
Supported OSes	Windows NT4, 2000, XP, 2003	Windows 2000, XP, 2003; RedHat Ent Linux (no supplicant)	Expected on 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

** Meetinghouse and Funk information given without any guarantee expressed or implied. For specific pricing and platform support information, please contact each vendor directly

Access Control Server (ACS) v4.0

- New Features
  - Network Access Profiles
    - Services: Groups, Protocols, Attributes
    - Authentication: Protocols, Directories
    - Compliance: Posture & Audit Policies
    - Authorization: Groups, RACs, ACLs
  - Audit Services
- Software only release
- Appliance update in v4.1



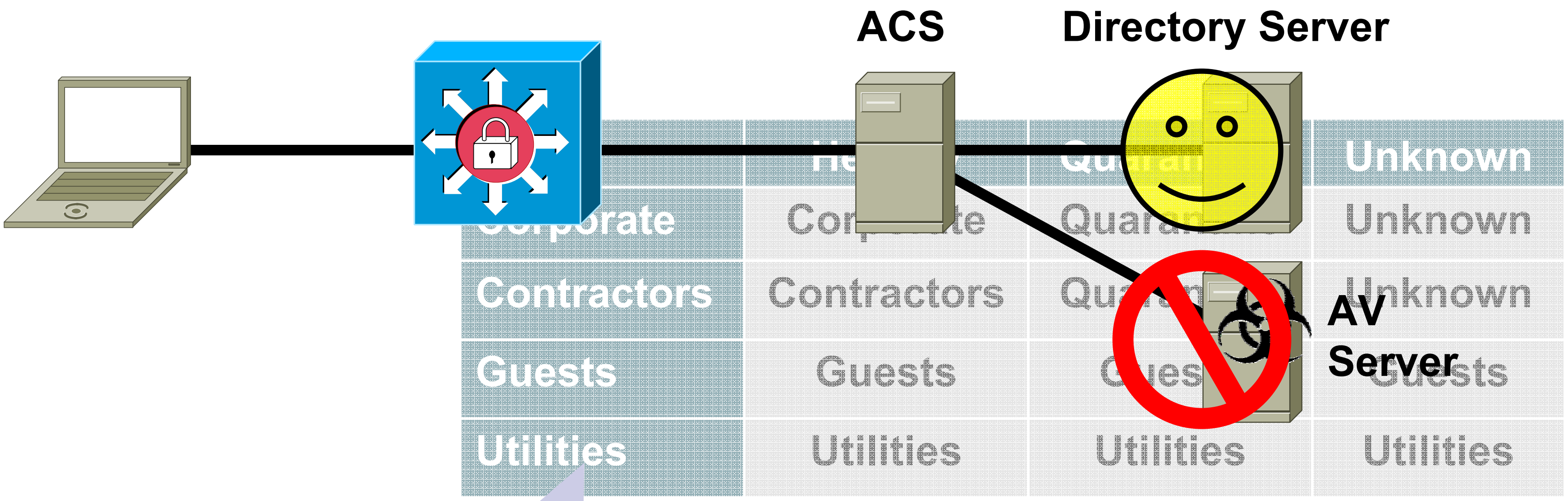
Cisco Secure ACS v 4.0

Select "Log Off" to end the administration session.

CiscoSecure ACS v4.0 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.

CiscoSecure ACS
Release 4.0(1) Build 8
Copyright ©2004 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

ACS v4.0: Identity x Posture Authorization



RADIUS Attribute Component: Quarantine

```
[26/9/1] = Quarantine
[27] = 30
[29] = RADIUS_Request (1)
[64] = VLAN
[65] = 802
[81] = quarantine
```

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 assessment expected soon

- Ethernet-switch support expected soon:

  16, 24, 48 port NM

  2800, 3700, 3800 switch 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

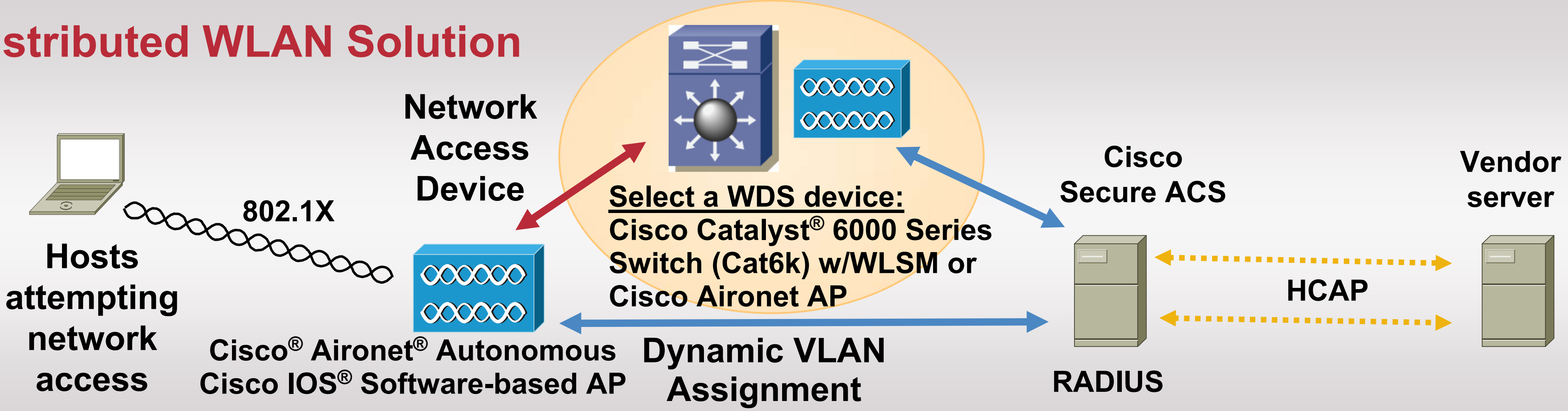
- Models 3005-3080
- Release v4.7 supports NAC L3 IP
- VPN Client does not include CTA
- Works with IPSec and L2TP/IPSec remote access sessions
  - NAC processing starts after an IPSec session is established
  - Communication with CTA is within IPSec SAs
  - NAC does not apply to PPTP, L2TP or LAN-to-LAN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

Switch Platforms
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	2.0	Future	2.0 (NAC L2 IP)
6500—Sup2	Native IOS	Future	2.0	No	2.0 (NAC L2 IP)
6500—Sup32, 720	Hybrid	2.0	2.0	Future	2.0 (NAC L2 IP)
6500—Sup2	Hybrid	2.0	2.0	No	2.0 (NAC L2 IP)
6500—Sup2, 32, 720	CATOS	2.0	2.0	No	2.0 (NAC L2 IP)
4000 Series—Sup2+, 3-5	IOS	2.0	2.0	Future	2.0 (NAC L2 IP)
3550, 3560, 3750	EMI, SMI	2.0	2.0	No	2.0 (NAC L2 IP)
2950	EI, SI	2.0	No	No	No
2940, 2955, 2970	All	2.0	No	No	No
6500—Sup1A	All	No	No	No	No
5000	All	No	No	No	No
4000/4500	CATOS	No	No	No	No
3500XL	All	No	No	No	No
2900XM	All	No	No	No	No

NAC Framework
WLAN Deployment

Distributed WLAN Solution



Hosts attempting network access

802.1X

Network Access Device

Cisco® Aironet® Autonomous Cisco IOS® Software-based AP

Select a WDS device:
Cisco Catalyst® 6000 Series Switch (Cat6k) w/WLSM or Cisco Aironet AP

Dynamic VLAN Assignment

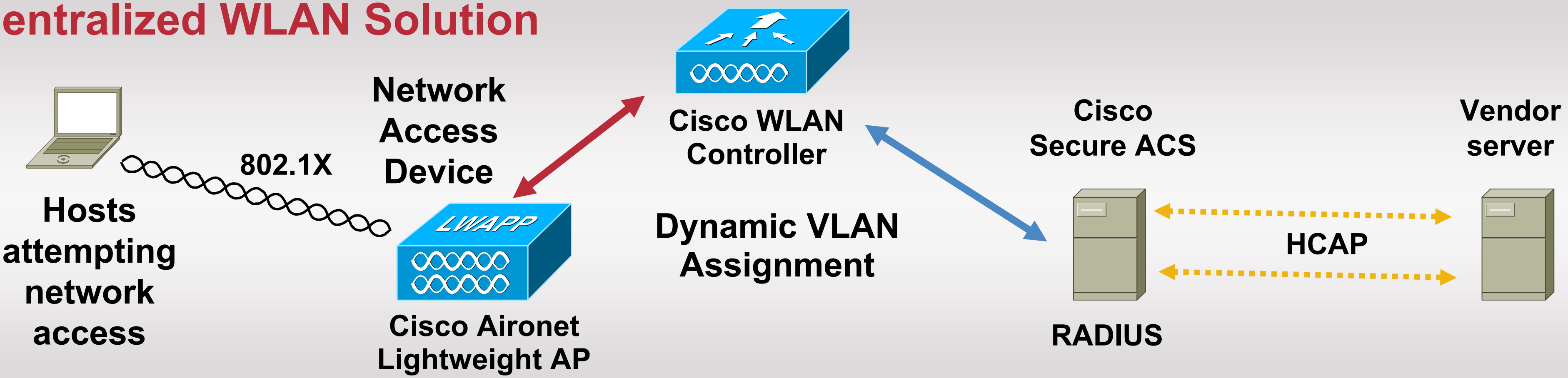
Cisco Secure ACS

RADIUS

HCAP

Vendor server

Centralized WLAN Solution



Hosts attempting network access

802.1X

Network Access Device

Cisco Aironet Lightweight AP

Cisco WLAN Controller

Dynamic VLAN Assignment

Cisco Secure ACS

RADIUS

HCAP

Vendor server

NAC Wireless LAN—Network Access

- Cisco® Aironet® 1200, 1240 Series Access Points, Cisco Catalyst® 6500 Series Wireless LAN Services Module (WLSM), Cisco Wireless LAN Controller 2006, 4100, 4400
  - NAC for WLAN enforces device security policy compliance at the access point when WLAN clients attempt to access the network
  - Access points implement NAC policy via VLAN assignment
- NAC support in Cisco Integrated Wireless 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–NAC framework and NAC appliance
    - Cisco Catalyst 6500 Series WLSM as WDS device–NAC framework only
  - Centralized WLAN solution
    - Cisco Aironet lightweight access points connected to Cisco WLAN Controller–NAC framework and NAC appliance

NAC Wireless LAN—Clients

- WLAN client devices require an IEEE 802.1X supplicant that supports NAC
  - Cisco®-supplied supplicant is for Ethernet adapter only, not WLAN adapter
- Meetinghouse and Funk will provide both wired and wireless L2 NAC supplicants
- NAC support in Cisco-compatible version 4
  - Cisco-compatible client devices (laptops, PDA, tablets, etc.)
  - Embedded into wireless client silicon chipset
  - Intel lead collaborator

Cisco Security Agent (CSA)

- CSA is an optional NAC component
- CSA v4.5 and later includes CTA v1.0

  CTA 2.0 bundling expected

- 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 anti-virus upon NAC Quarantine response

Cisco Systems®