NAC Tech Update

Christian Heinel cheinel@cisco.com

Tech Update

Jan. 2008

Cisco NAC By the Numbers

2200+
customers

47%
market share[1]

#1 NAC Vendor
based on Network World reader survey[3]

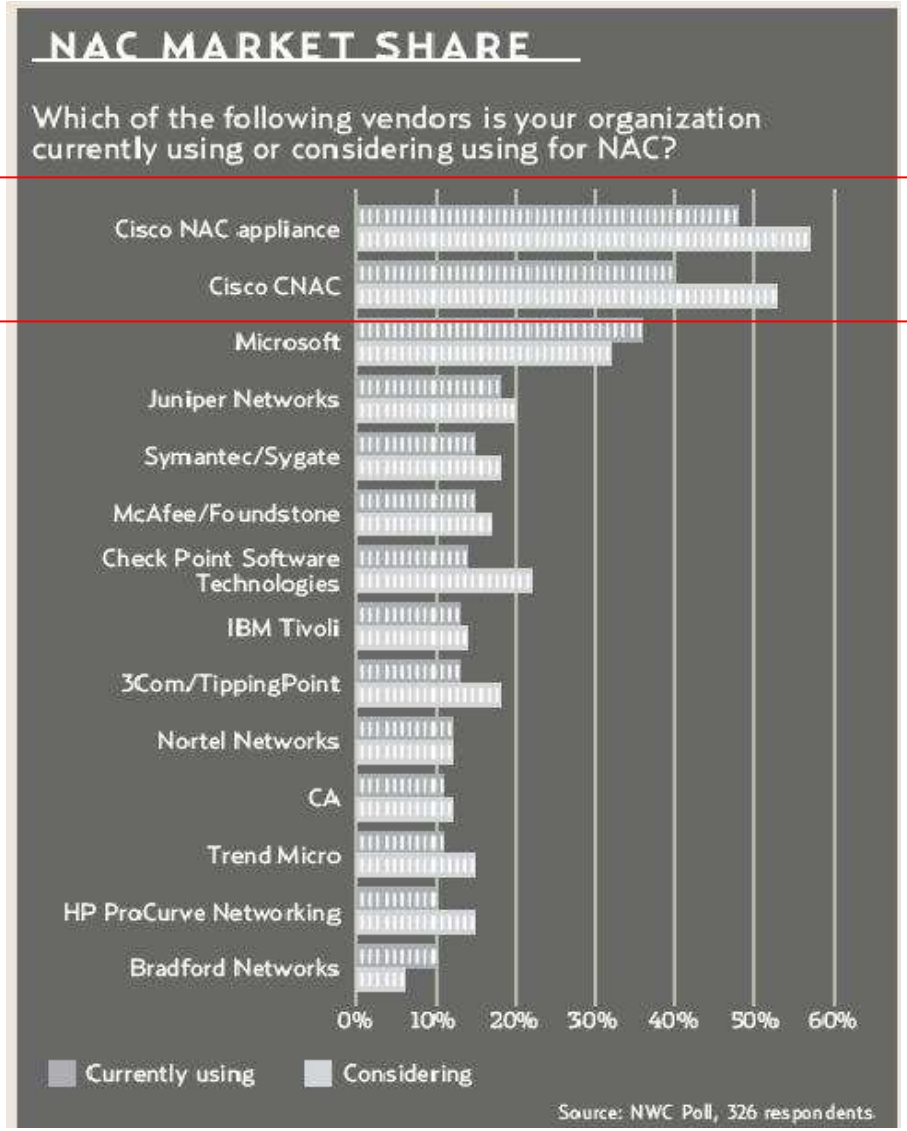
75%
of Infonetics survey respondents ranked Cisco **#1** among NAC vendors[1]

2007 Product Leadership Awards
SearchNetworking.com

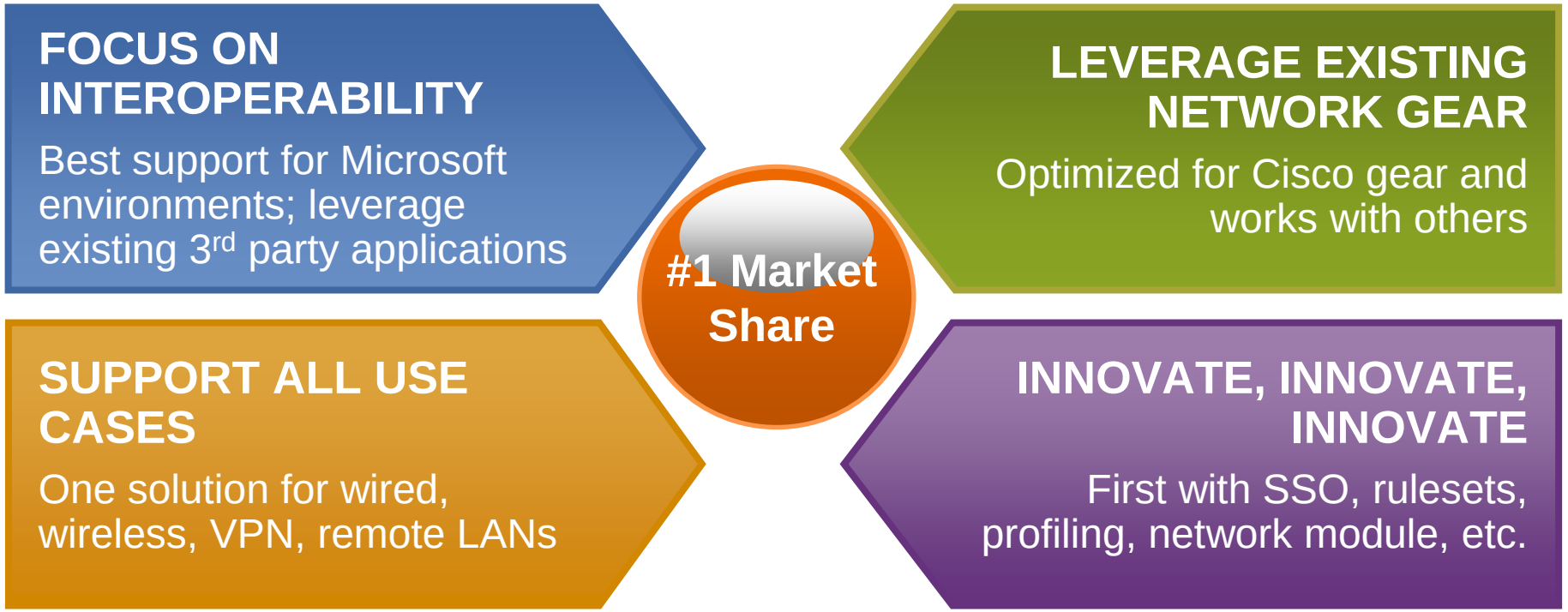
Gold Award:
Determined by reader survey[2]

1 Infonetics, May 2007
2 March 2007 http://searchnetworking.techtarget.com/productsOfTheYear/
3 May 2007 http://www.networkcomputing.com/channels/security/showArticle.jhtml?articleID=199204304

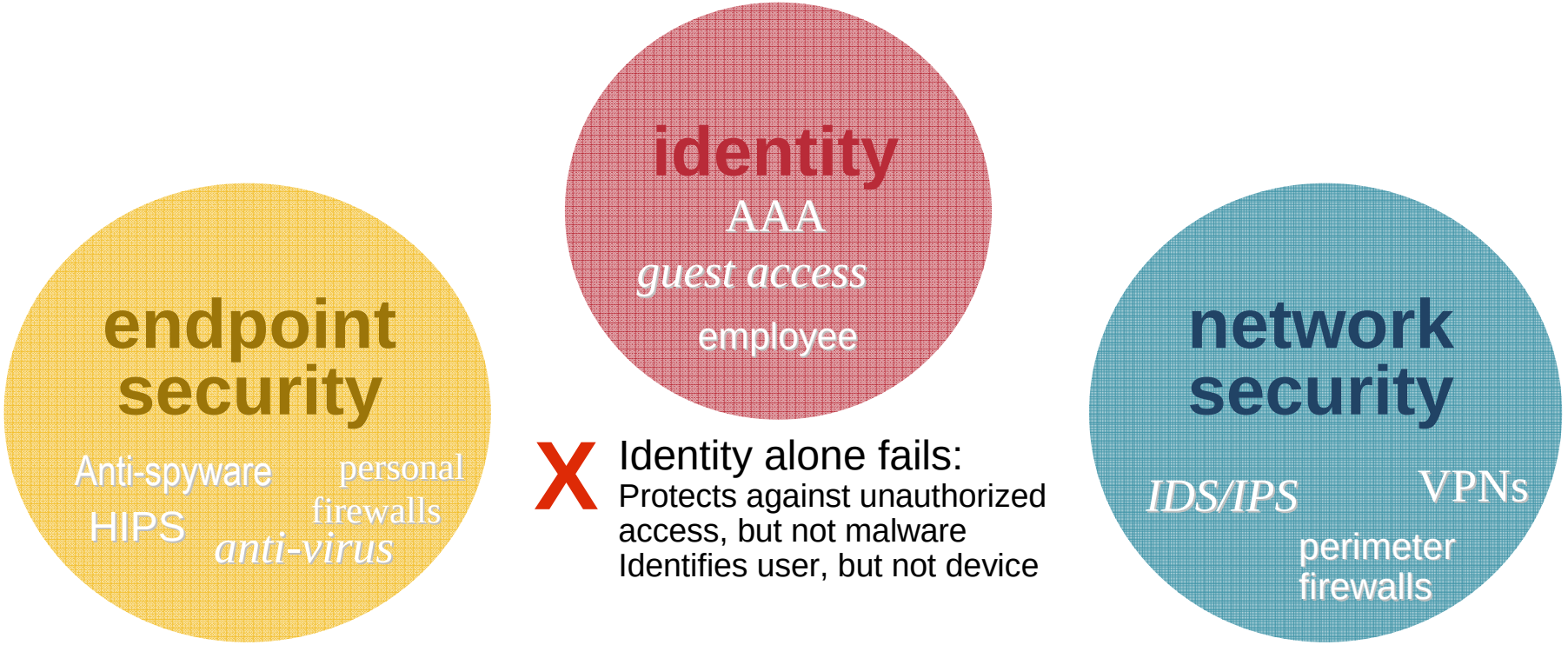
Cisco NAC is #1



Secrets of Success: Cisco NAC Strategy



Complexity Demands Defense-in-Depth



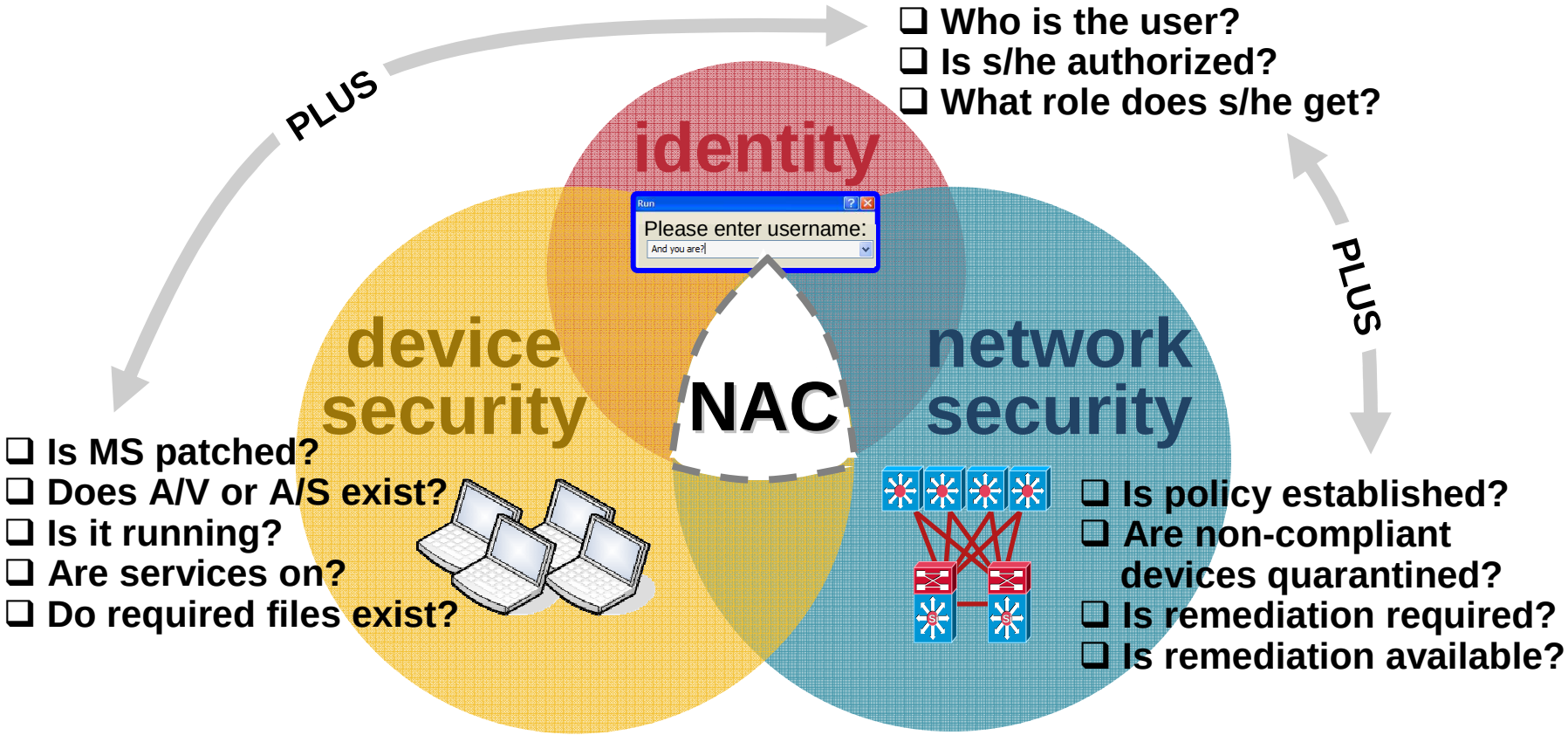
X Identity alone fails:
Protects against unauthorized access, but not malware
Identifies user, but not device

X Endpoint security alone fails:
99% have AV, but infections persist!
Host based apps are easily manipulated—even unintentionally
Time gap between virus and virus def/repair

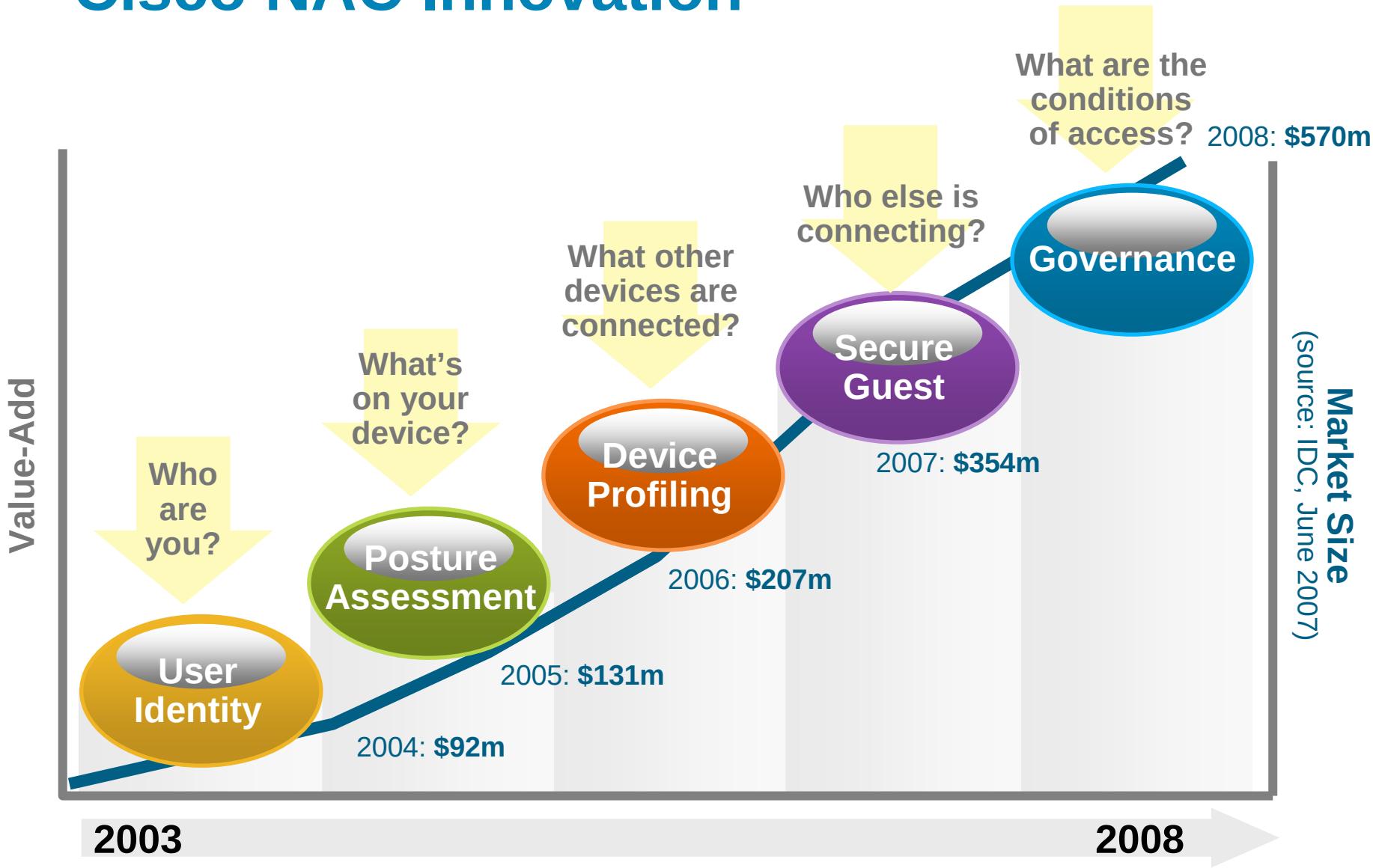
X Network security alone fails:
Firewalls cannot block legitimate ports
VPNs cannot block legitimate users
Malware signatures must be known
Detection often occurs after-the-fact

What Is Network Admission Control?

Using the network to enforce policies ensures that incoming devices are compliant.



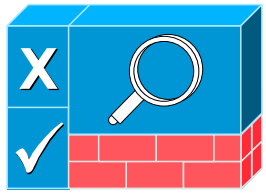
Cisco NAC Innovation



NAC Appliance Components

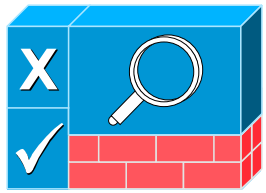
- NAC Manager (Clean Access Manager)

  Centralizes management for administrators, support personnel, and operators



- NAC Server (Clean Access Server)

  Serves as enforcement point for network access control

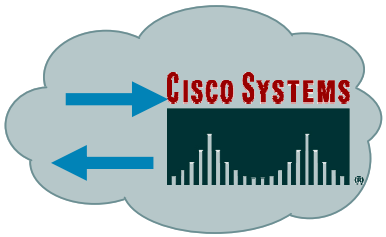


- NAC Agent (Clean Access Agent)

  Optional lightweight client for device-based registry scans in unmanaged environments

- Rule-set Updates

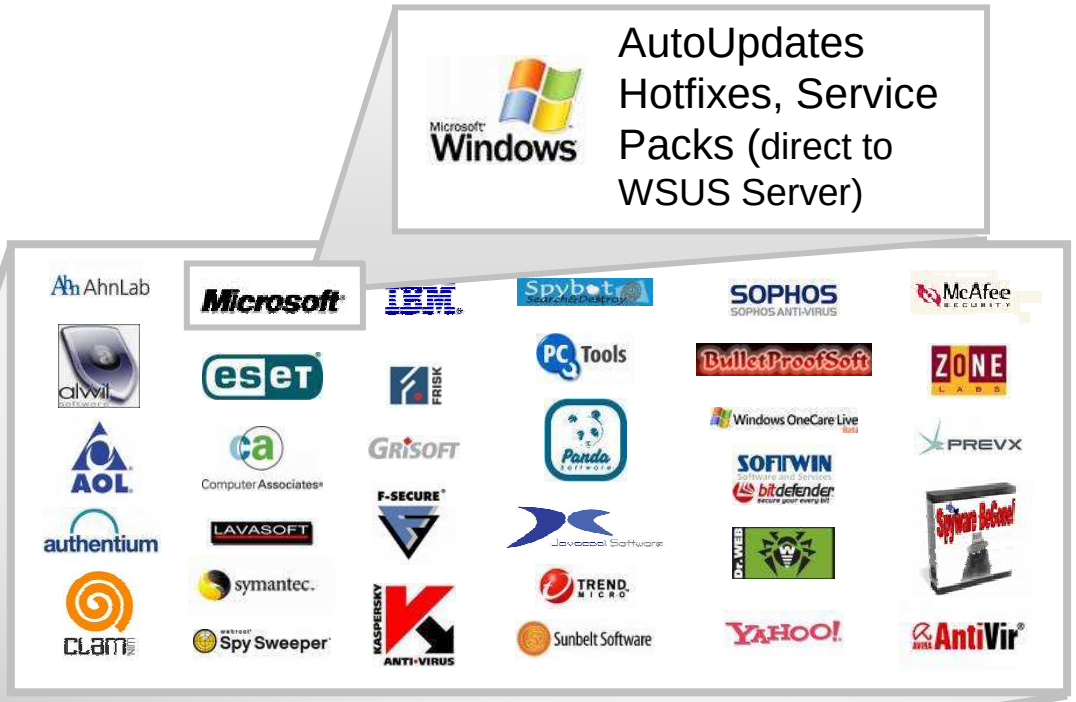
  Scheduled automatic updates for anti-virus, critical hot-fixes and other applications



Only NAC with Automated Rulesets

Automated Cisco rulesets simplify management for over 350+ partner applications

Cisco NAC Appliance Manager



NAC Solution Sizing and Platforms

NAC Management Components

Lite Manager
(up to 3 Servers)

Std Manager
(up to 20 Servers)

Super Manager
(up to 40 Servers)

NAC Server Components

ISR Network Module
50 or 100 users

Appliance: 100, 250, or 500 users

Appliance: 1500, 2500, or 3500 users

Hardware Platform Legend:

- **ISR NM**
- **3310**
- **3350**
- **3390**

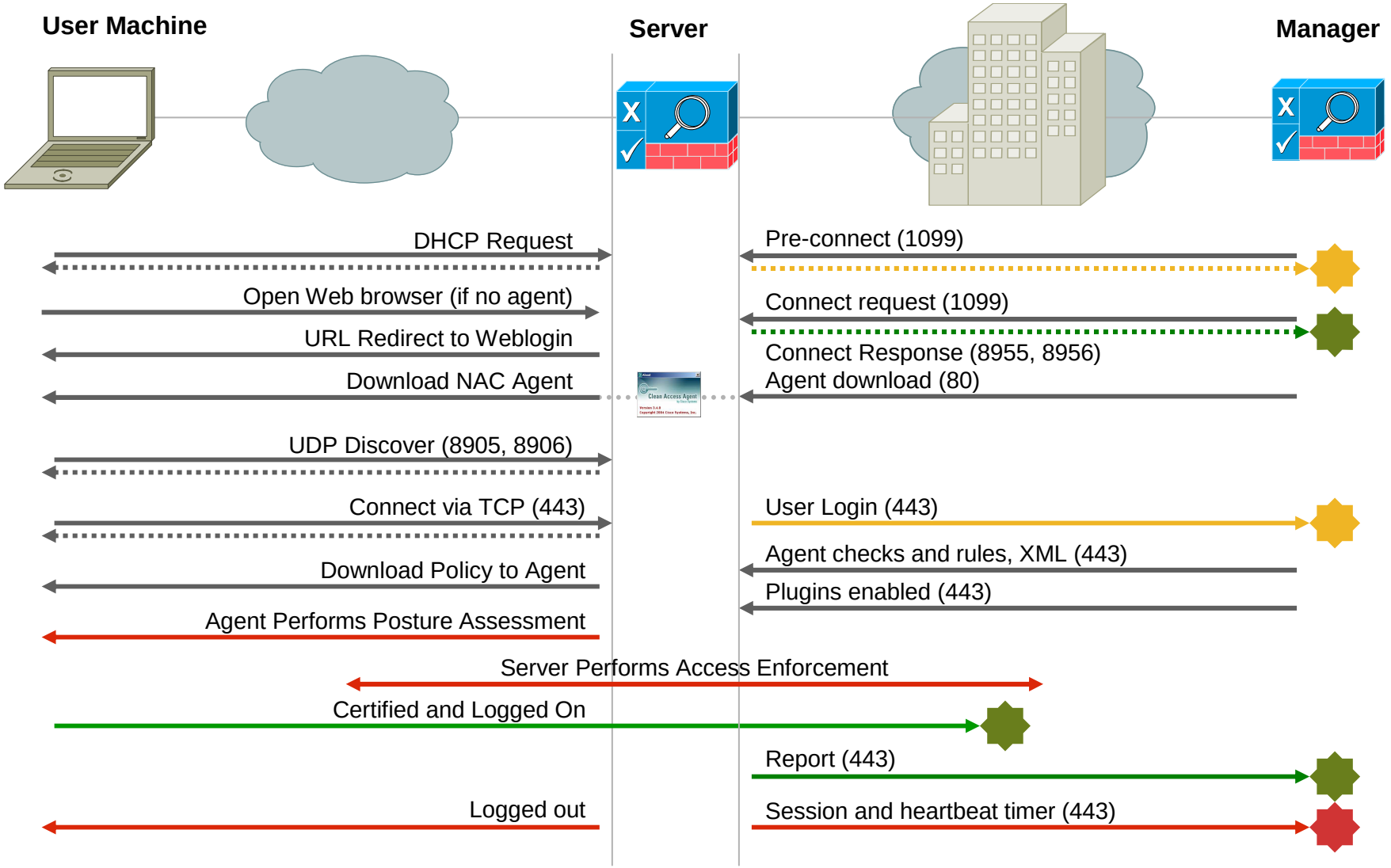
Users = online, concurrent

Additional NAC Services

Guest Server

Profiler Server

NAC Appliance Overview: Process Flow



NAC Server Foundation: Virtual Gateway and Real IP Gateway

- NAC Servers at the most basic level can pass traffic in one of two ways:

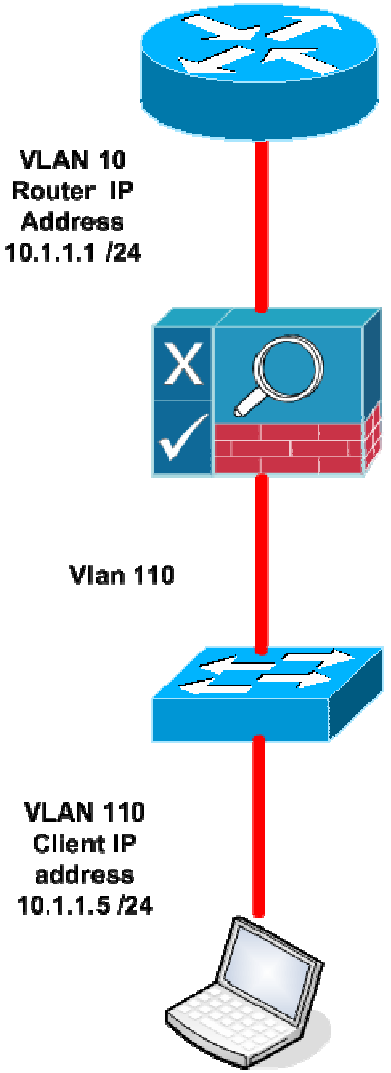
  Bridged Mode = Virtual Gateway

  Routed Mode = Real IP Gateway / NAT Gateway

- Any NAC Server can be configured for either method, but a NAC Server can only be one at a time
- Gateway mode selection affects the logical traffic path
- Does not affect whether a NAC Server is in Layer 2 mode, Layer 3 mode, In Band or Out of Band

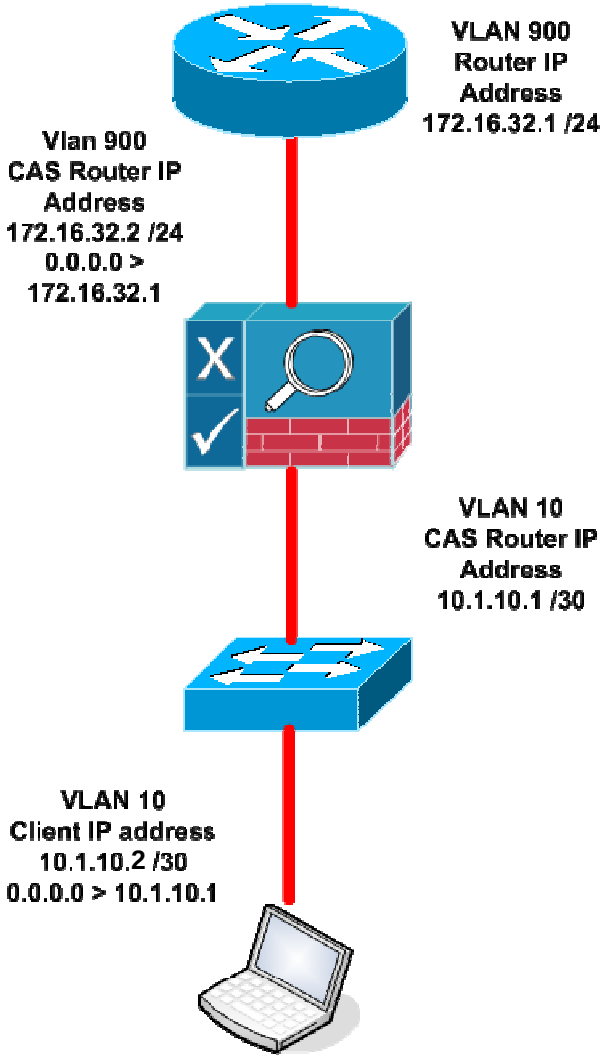
NAC Server Foundation: Virtual Gateway

- Direct Bridging: Frame Comes In, Frame Goes Out
- VLAN IDs are either passed through untouched or mapped from A to B
- DHCP and Client Routes point directly to network devices on the Trusted side
- NAC Server is an IP passive bump in the wire, like a transparent firewall



NAC Server Foundation: Real IP/NAT Gateway

- NAC Server is Routing, Packet Comes In, Packet Goes Out
- VLAN IDs terminate at the Server, no pass-through or mapping
- DHCP and Client Routes usually point to the Server for /30
- NAC Server is an active IP router, can also NAT outbound packets *



* Be aware of NAT performance limitations

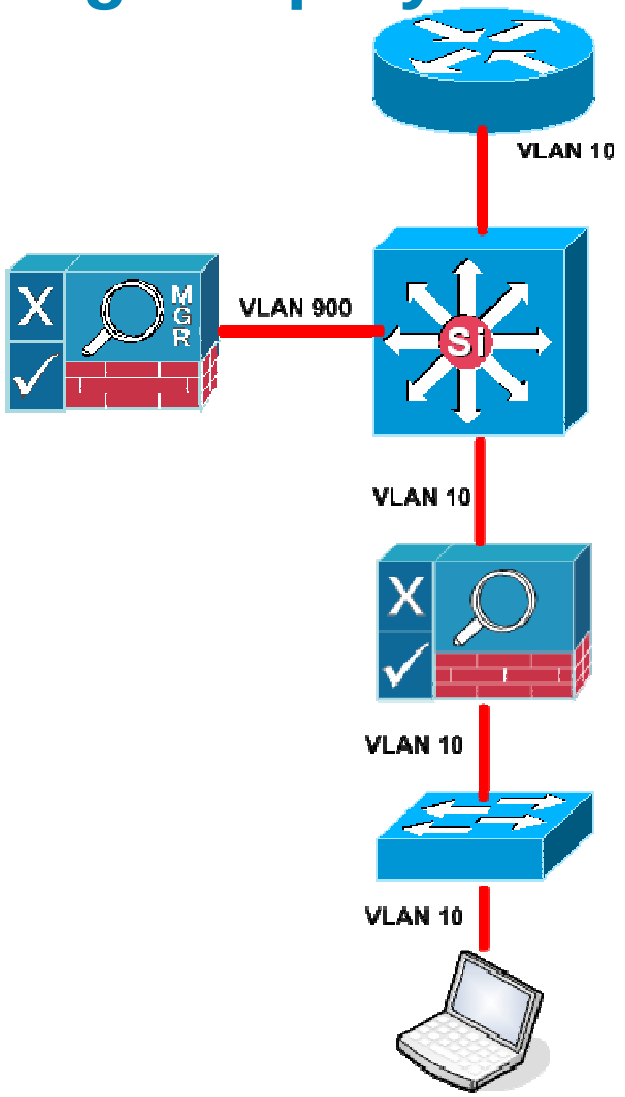
NAC Server Foundation: Edge and Central Deployment

- NAC Servers have two physical deployment models
  - Edge Deployment
  - Central Deployment
- Any NAC Server can be configured for either method
- Deployment mode selection affects the physical traffic path
- Does not affect whether a NAC Server is in Layer 2 mode, Layer 3 mode, In Band or Out of Band

NAC Server Foundation: Edge Deployment

- Easiest deployment option to understand
- NAC Server is logically inline, and Physically inline
- Supports all Catalyst Switches
- VLAN IDs are passed straight through when in VGW

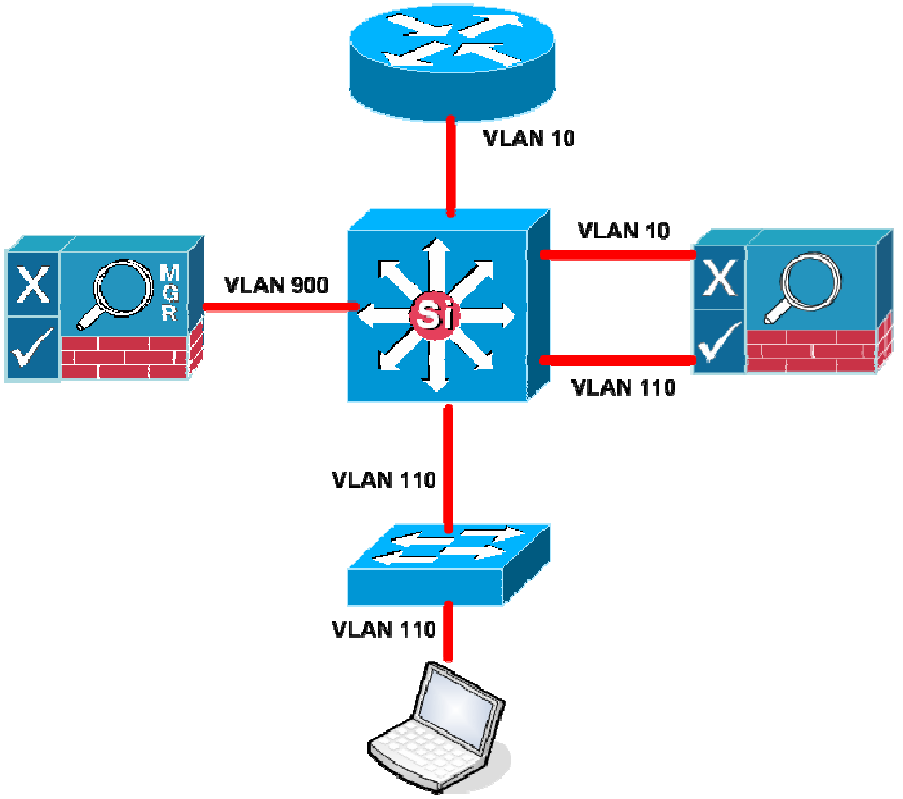
  10 → 10
- Installations with multiple Access Layer closets can become complex



NAC Server Foundation: Central Deployment

- Most common deployment option
- NAC Server is logically inline, NOT physically inline
- Supports 6500 / 4500 / 3750 / 3560
- VLAN IDs are mapped when in VGW

  110 → 10
- Easiest installation
- Most scalable in large environments



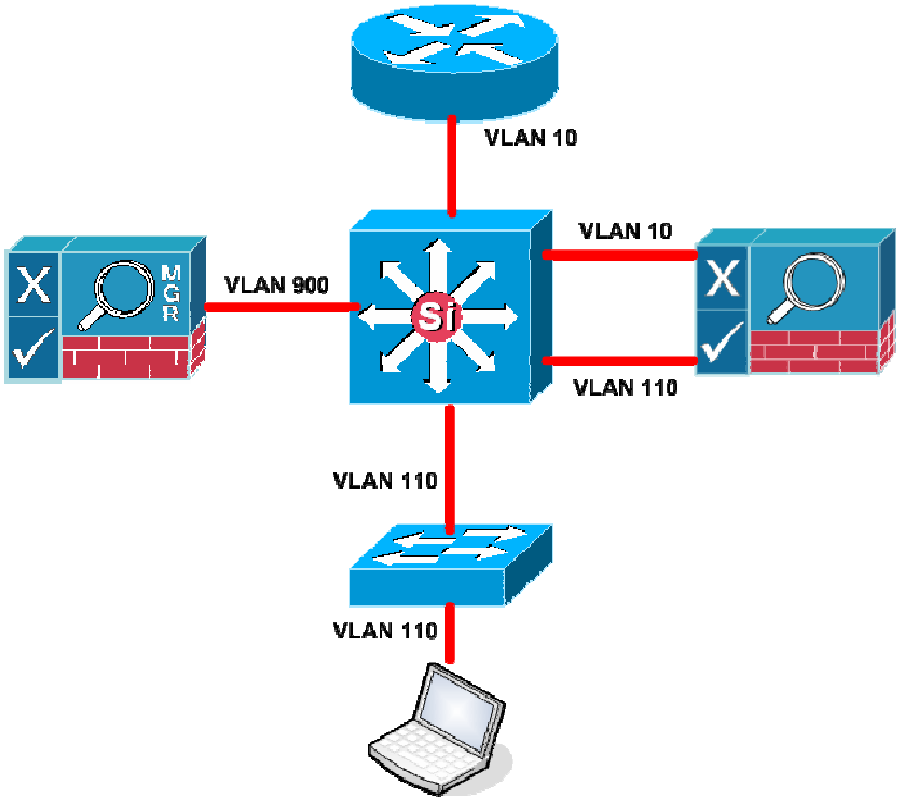
*3550 is not supported

NAC Server Foundation: Layer 2 Mode and Layer 3 Mode

- NAC Servers have two client access deployment models
  - Layer 2 Mode
  - Layer 3 Mode
- Any NAC Server can be configured for either method, but a NAC Server can only be one at a time
- Deployment mode selection is based on whether the client is Layer 2 adjacent to the NAC Server

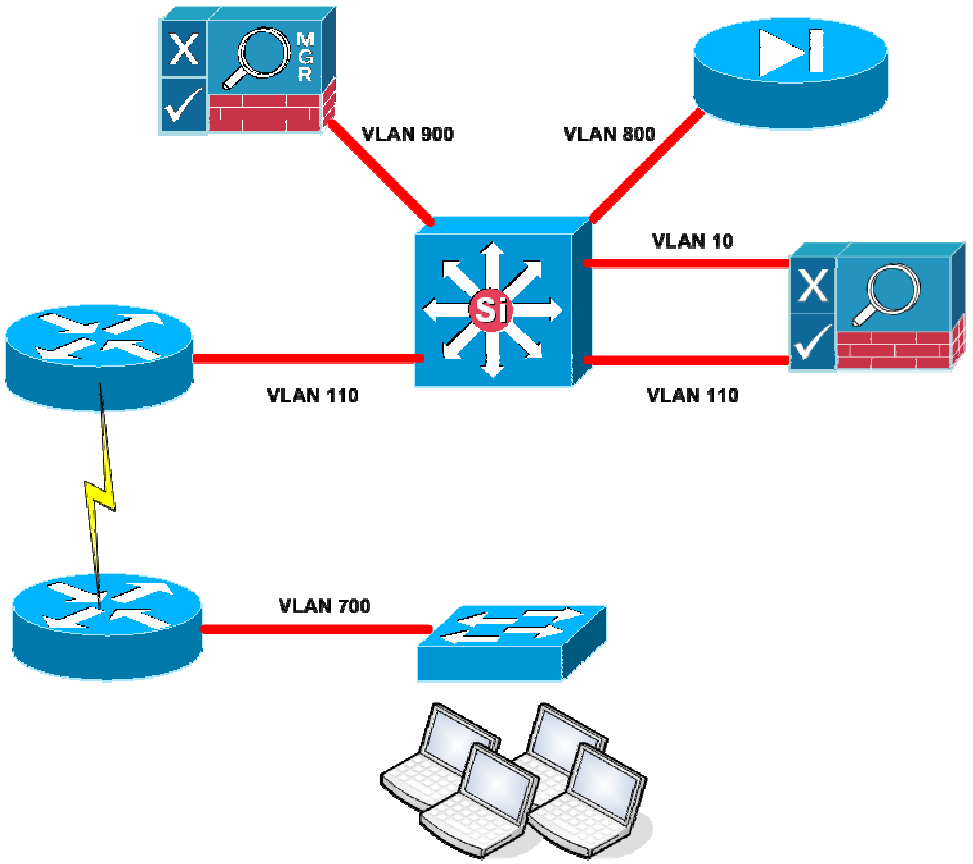
NAC Server Foundation: Layer 2 Mode

- Client is Layer 2 Adjacent to the Server
- MAC address is used as a unique identifier
- Supports both VGW and Real IP GW
- Supports both In Band and Out of Band
- Most common deployment model for LANs



NAC Server Foundation: Layer 3 Mode

- Client is NOT Layer 2 Adjacent to the NAC Server
- IP Address is used as a unique identifier
- Supports both VGW and Real IP GW
- Supports In Band Mode
- Needed for WAN and VPN deployments

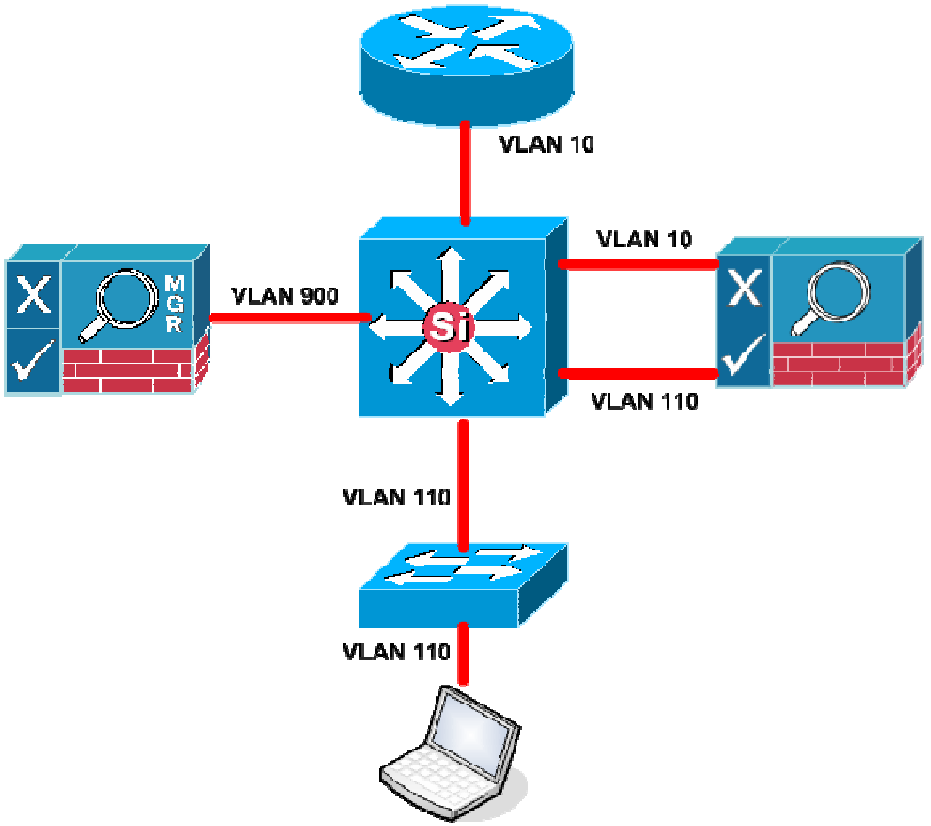


NAC Server Foundation: In Band and Out of Band

- NAC Servers have two traffic flow deployment models
  - In Band
  - Out of Band
- Any NAC Server can be configured for either method, but a NAC Server can only be one at a time
- Selection is based on whether the customer wants to remove the NAC Server from the data path
- NAC Server is ALWAYS inline during Posture Assessment

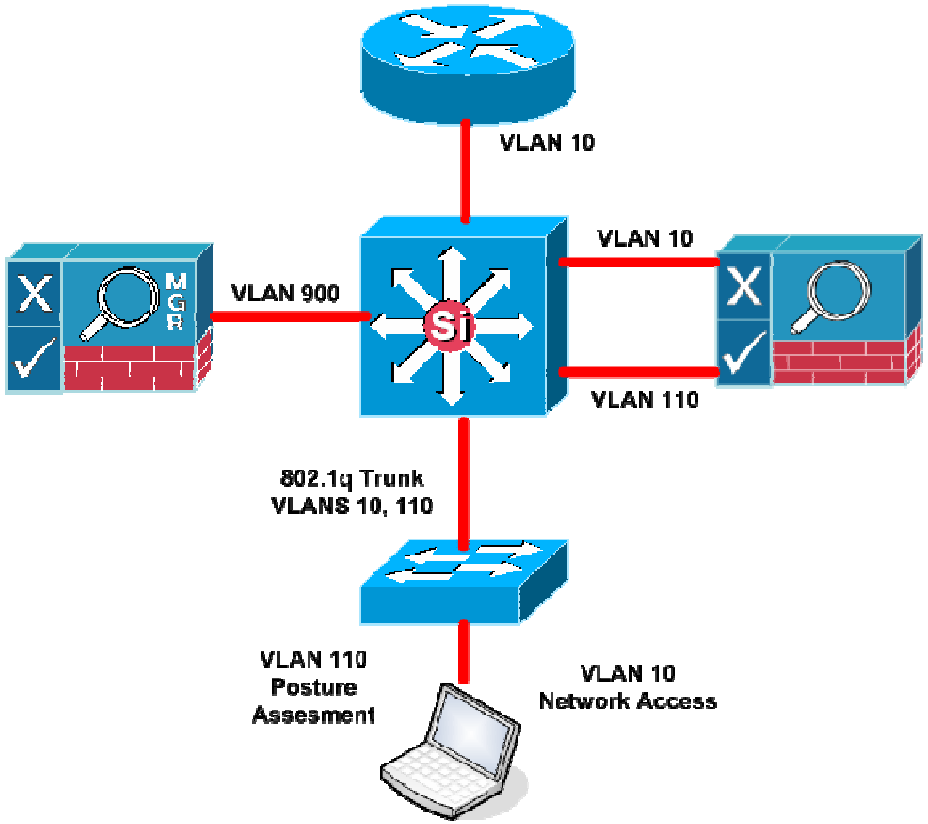
NAC Server Foundation: In Band

- Easiest deployment option
- NAC Server is Inline (in the data path) before and after posture assessment
- Supports any switch, any hub, any AP
- Role Based Access Control Guest, Contractor, Employee
- ACL Filtering and Bandwidth Throttling



NAC Server Foundation: Out of Band

- Multi-Gig Throughput deployment option
- NAC Server is Inline for Posture Assessment Only
- Supports most common Cisco Switches **
- Port VLAN Based and Role Based Access Control
- ACL Filtering and Bandwidth Throttling for Posture Assessment Only

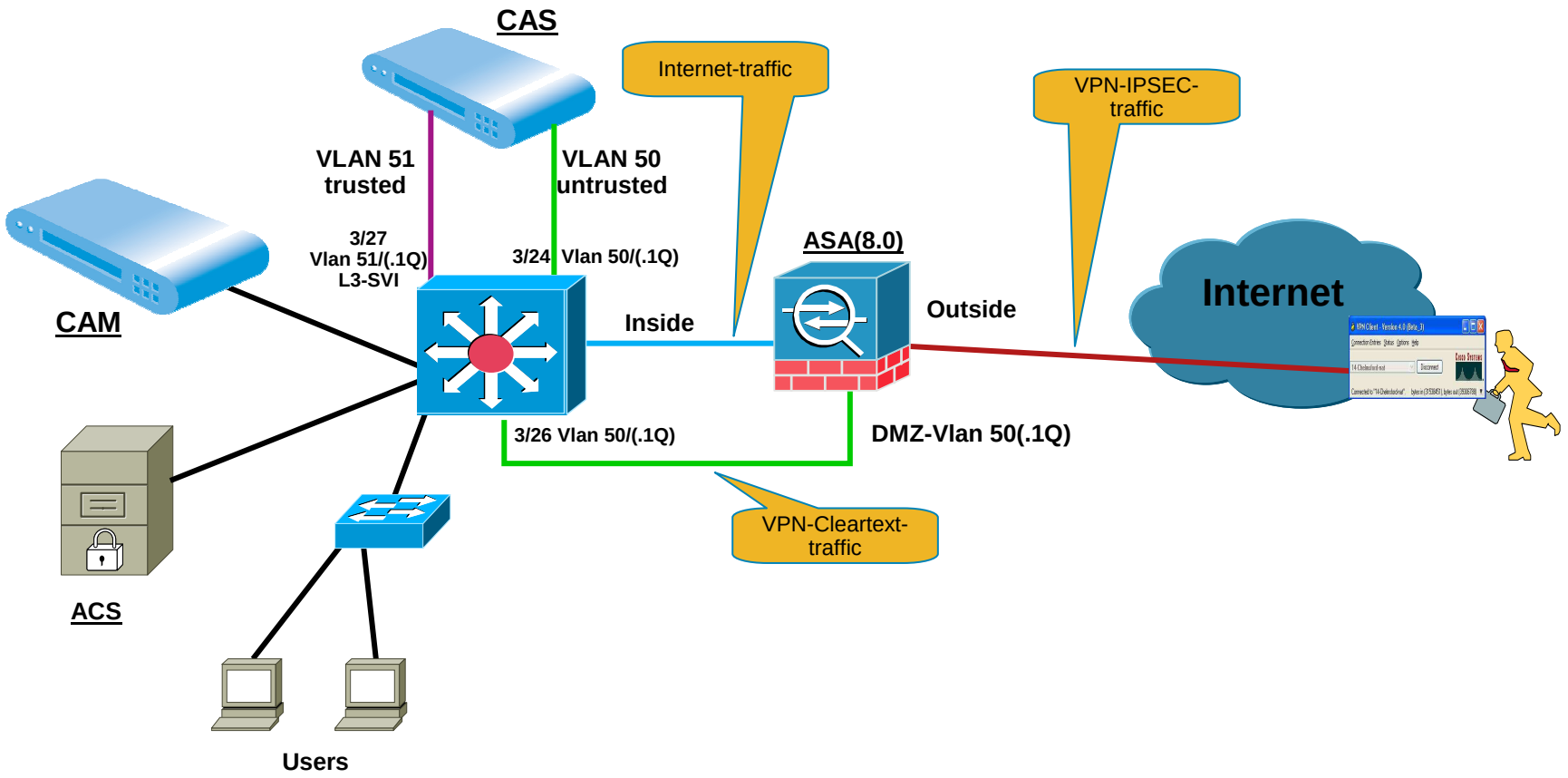


NAC Design for VPN

Challenge

- Use single ASA (8.0 release) for RAS-VPN & Clean Access & Internet firewall
- CAS sits “Inband, L3 Virtual GW” behind ASA
- ASA does not support PBR
- regular Internet traffic must not pass CAS (no statefulness etc.)

Network drawing

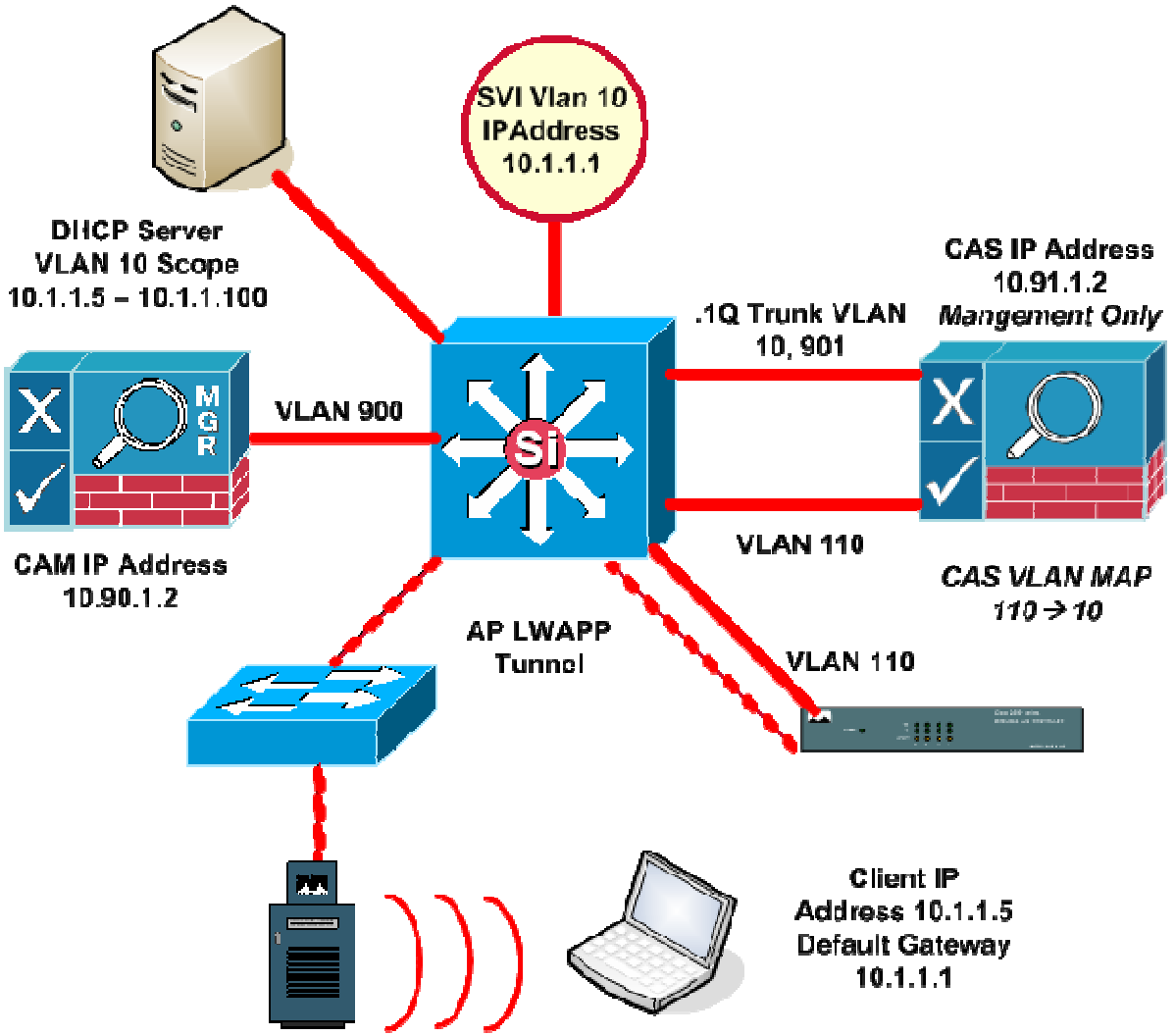


NAC Design for Wireless

NAC with Wireless

- NAC Server in Inband mode
- User Traffic exits the Wireless controller, not the AP
- Single Sign-on support with Radius accounting from WLC

L2 Virtual Gateway Inband

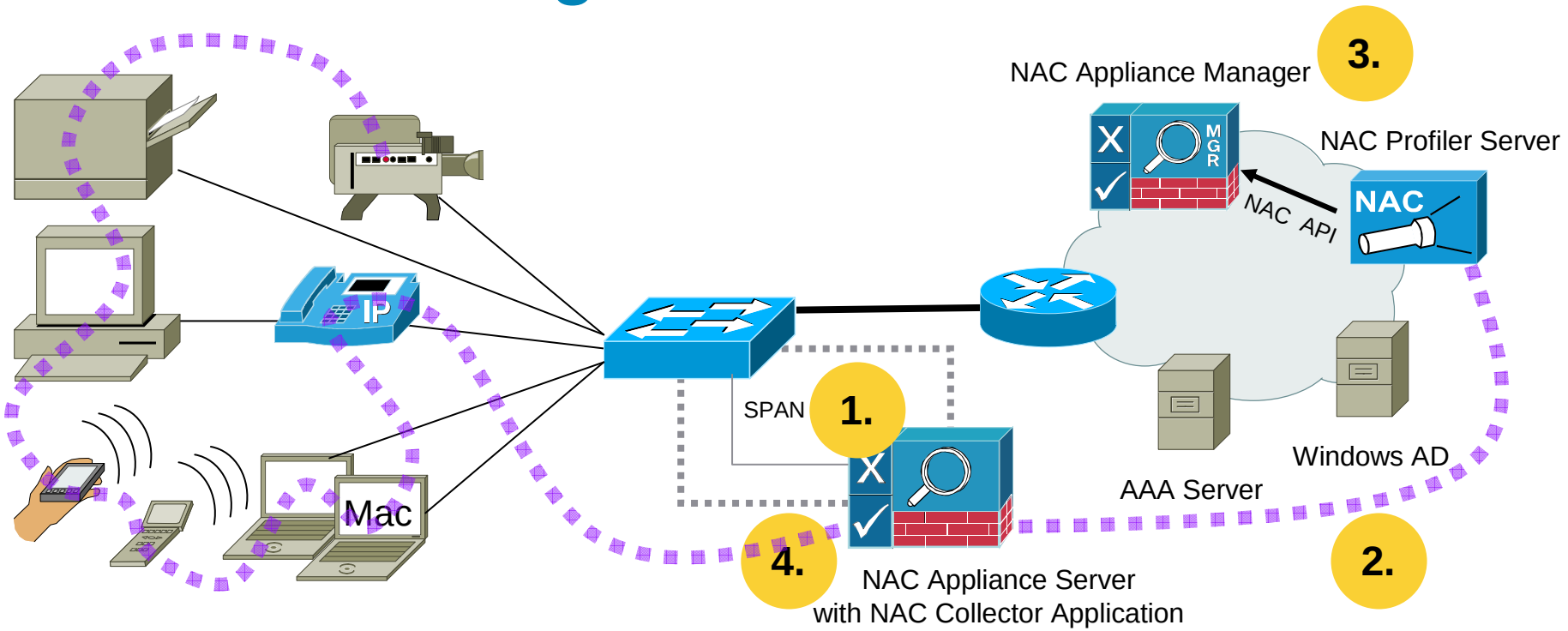


Design for Device Profiling

Component: NAC Profiler Server

- Aggregates all endpoint information from Collectors
  - Communicated over a secure encrypted channel
  - View by Profile type, Switch port, etc.
- Maintains Database of Endpoint information including:
  - Location
  - Current MAC/IP Addressing
  - Endpoint History
  - Endpoint Behavioral Attributes (protocol, application, hosts, etc.)
- Hosts the GUI
- Liaises with NAC Appliance's Clean Access Manager to:
  - Maintain Filters List
  - Communicate results of the ongoing Profiling function
  - Update new and retired assets
  - Provision policy attributes of non-PC endpoints

Understanding NAC Profiler Server



1. NAC Collector Application collects the relevant data and consolidates the information to send to the NAC Profiler Server
2. NAC Profiler Server aggregates all of the information from the Collectors and maintains a database of all network-attached endpoints (e.g. phones, printers, badge readers, modalities, etc.)
3. NAC Profiler Server continuously maintains the Filters List via the NAC API and provisions the appropriate access decisions (allow, deny, check, “role”, or ignore)
4. NAC Collector Application continuously monitors behavior of profiled devices (to prevent spoofing) and updates Profiler Server

Collector Modules & Description

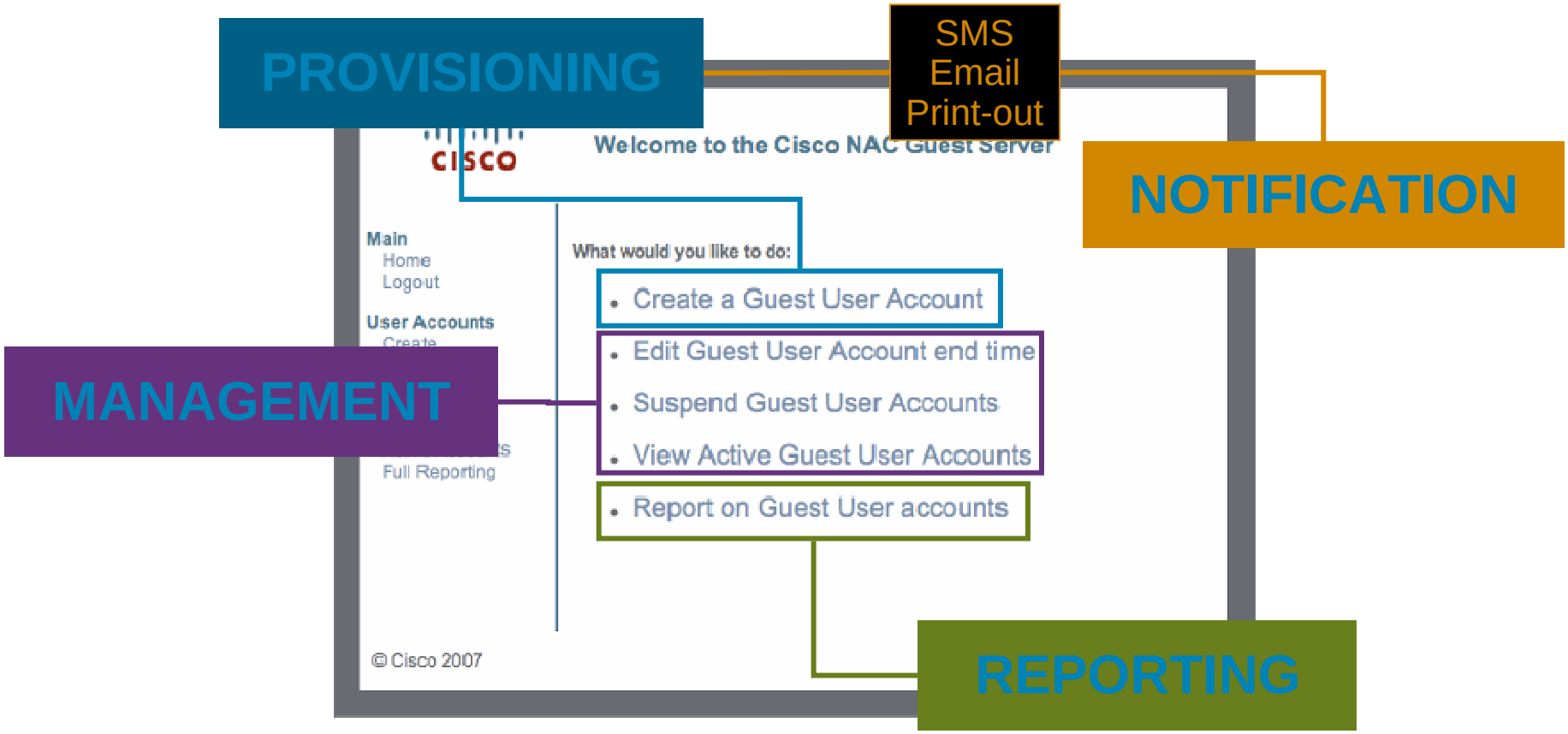
NetMap	**SNMP module that polls edge devices for specific information pertaining to connected devices, port states and other useful data for endpoint profiling and behavior analysis.**
NetTrap	**Receives port link state changes and New MAC notifications from edge devices useful for profiling and behavior analysis**
NetWatch	**Passive network traffic analyzer that gleans useful profiling information from network traffic**
NetInquiry	**Active profiling module that attempts to open ports on user defined networks to actively generate traffic for analysis**
NetRelay	**Receives NetFlow data directly from switches or other NetFlow data sources**

Profiling Design Summary

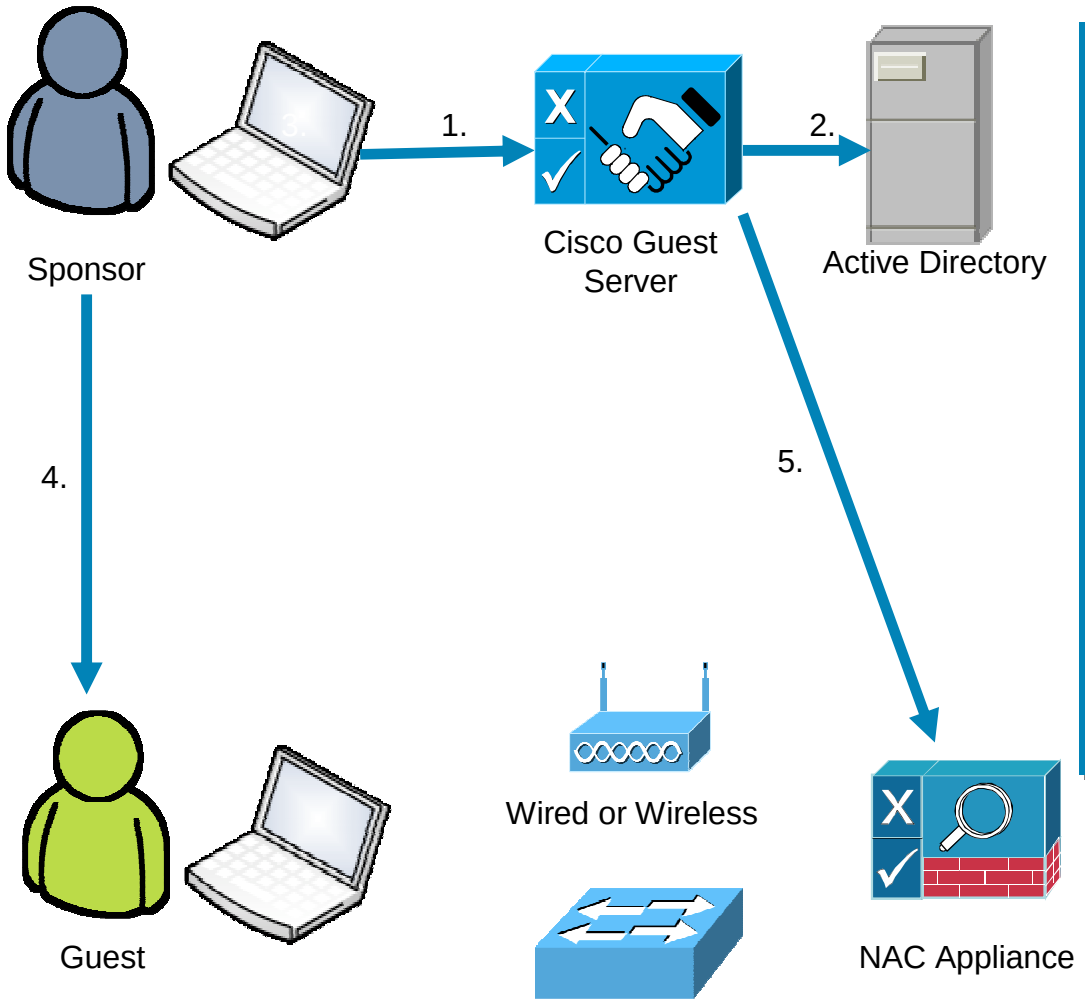
- Identify types of devices connected to network
- Determine collector modules which will be used to detect devices
- Determine network infrastructure capabilities
- Choose Profiling design that meets all collector capabilities required

Design for Guest Access

Managing the Guest User Lifecycle

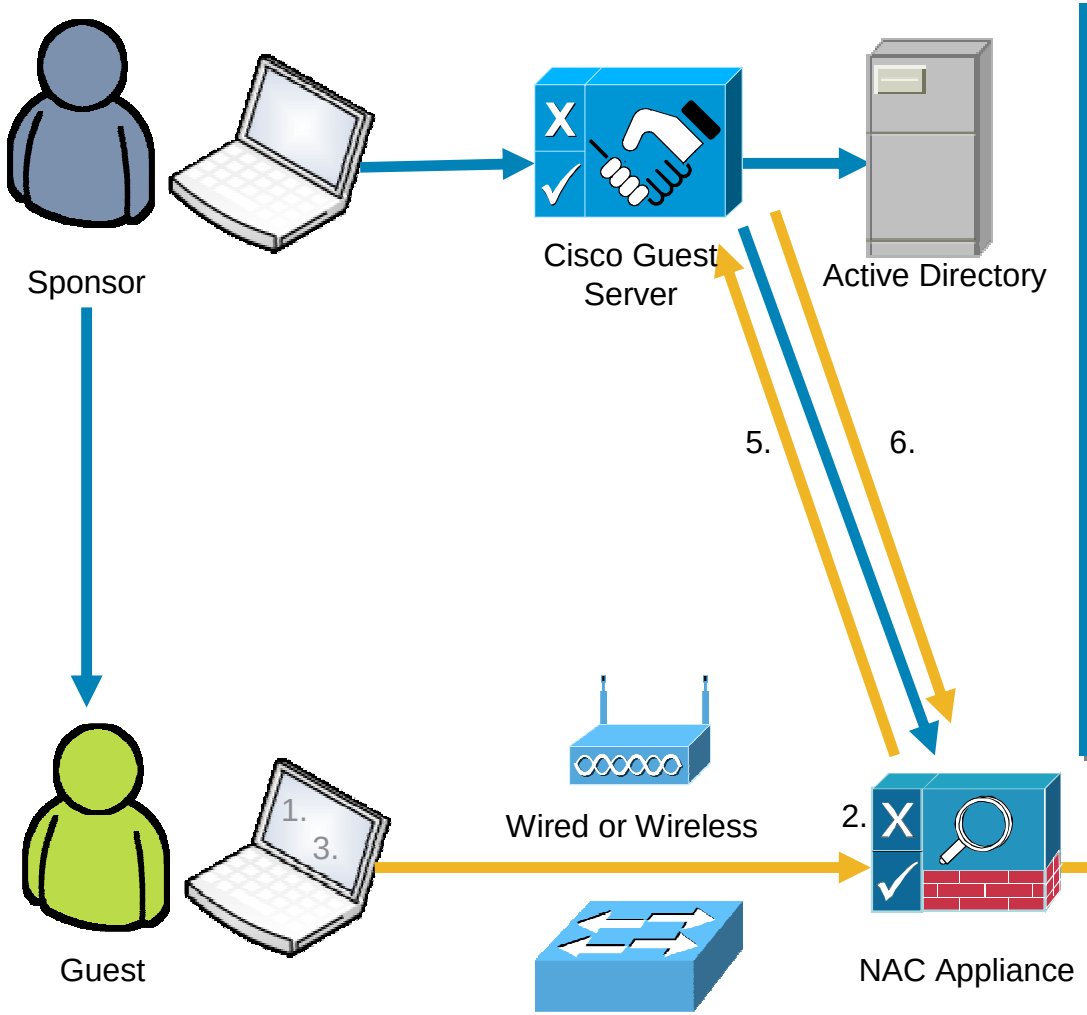


Guest Access Walkthrough - Sponsor



1. Sponsor accesses Cisco Guest Server, such as http://guests.yourcompany.com
2. Sponsor authenticates using corporate credentials
3. Sponsor Creates Account on the Cisco Guest Server
4. Sponsor gives guest account details (email/print/sms)
5. Guest Server Provisions Account on the Cisco NAC Appliance

Guest Access Walkthrough - Guest



1. Guest opens Web browser
2. Web traffic is intercepted by Network Enforcement Device and redirected to login page (captive portal)
3. Guest logs in with details provided by sponsor
4. Guest can now access the internet
5. Guest Access Recorded
6. Guest removed when session time expires