Cisco Expo 2008

Network Admission Control

János SIMON – Security CCIE #18522
system engineer
janos.simon@snt.hu

Agenda

- **NAC foundations**
- **Components**
- **Examples**
- **Guest access**

Network Admission Control

Foundations

Cisco Network Admission Control

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

Authenticate & Authorize

- Enforces authorization policies and privileges
- Supports multiple user roles

Quarantine & Enforce

- Isolate non-compliant devices from rest of network
- MAC and IP-based quarantine effective at a per-user level

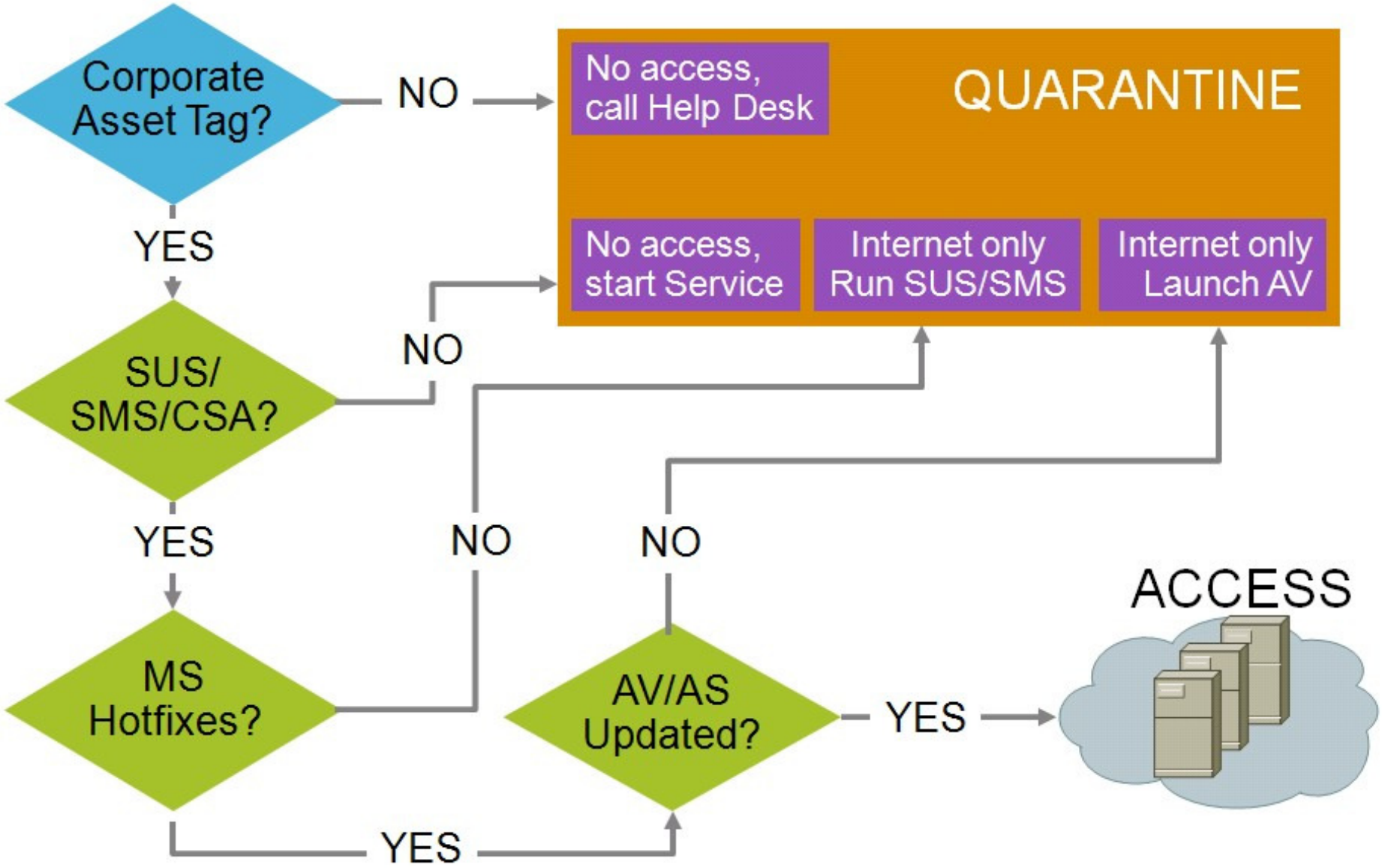
Scan & Evaluate

- Agent scan for required versions of hotfixes, AV, etc
- Network scan for virus and worm infections and port vulnerabilities

Update & Remediate

- Network-based tools for vulnerability and threat remediation
- Help-desk integration

Sample NAC Decision Tree: Employee

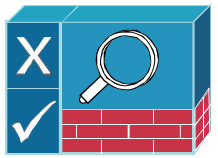


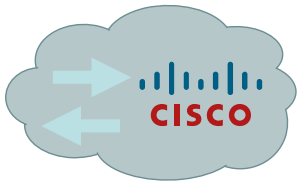
Network Admission Control

Components

NAC Appliance Components

- Cisco NAC Manager
  Centralized management
- Cisco NAC Server
  Serves as posture, remediation and enforcement access control
- Cisco NAC Profiler
  Optional component for device profiling, behavioral monitoring, and device reporting
- Cisco NAC Guest Server
  Optional component for full guest access lifecycle including provisioning, notification, management and reporting
- Cisco NAC 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





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

Additional NAC Services

Guest Server

Profiler Server

Hardware Platform Legend:

ISR NM
3310
3350
3390

Users = online, concurrent

CISCO PARTNER Gold Certified

NAC module

NME-NAC-K9

- supported routers:
  ISR 2811, 2821, 2851, 3825, 3845
- IOS: min. 12.4(11)T

- Processor: 1-GHz Intel Celeron-M
- Memory: 512-MB (DDR2)
- Flash : 64-MB Compact Flash
- Disk: 80-GB Serial ATA (SATA)

- High-Speed Intrachassis Module Interconnect (HIMI) support on ISR 3800 (internal bus capacity: 1 Gbps)

- **up to 100 concurrent users**

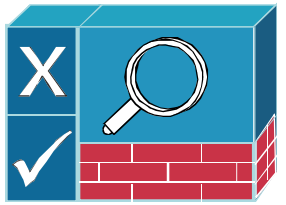
CAM – Clean Access Manager

Functions of CAM

- central management
- definition of requirements based on security policy
- evaluation of network access request
- configuration of CASs
- authentication of clients
  - Kerberos, LDAP, RADIUS, Active Directory, S/Ident, local DB
  - AD SSO support
- monitoring
- rule-set updates
- processes the SNMP messages of switches
- configuration of switches via SNMP

CISCO PARTNER
Gold Certified

CAS – Clean Access Server



Functions of CAS

- enforcement point of security policy
- detection of new users
- challenges for credentials (forwards to CAM, who judges the requests)
- isolation
- active component of the network
- WebLogin authentication, SSO
- does not store the security policy (only the CAM)
  - **Fallback:** what to do when the CAM is not available?

Clean Access Agent

- optional agent

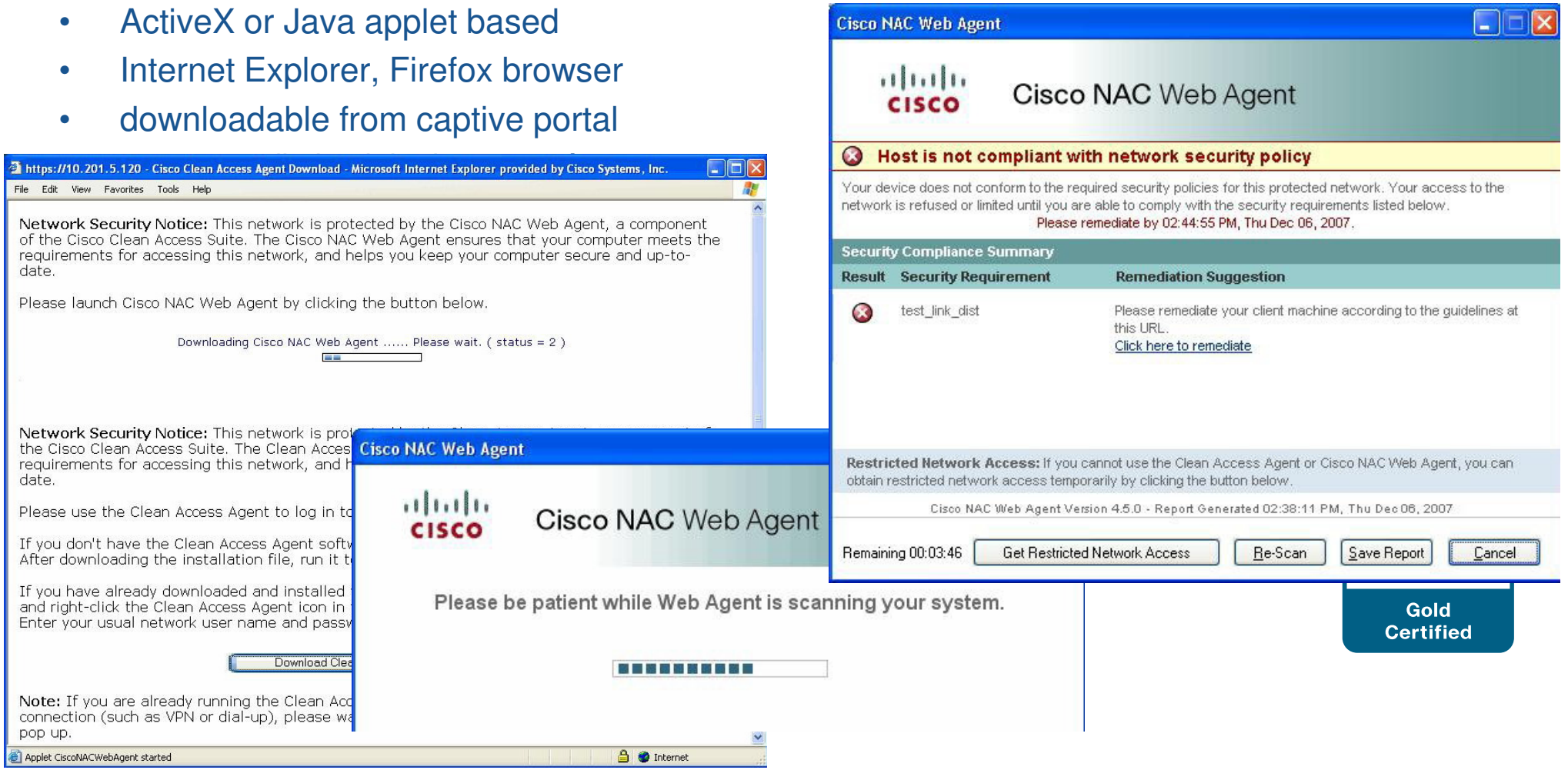
Functions of Clean Access Agent

- gathers information about the endpoint
- limited functions
  → no sense to compromise it
- does NOT do isolation, only the CAS and the network
- wizard-like remediation (even automatic)
- refreshing IP address
- SSO: Single-sign-on

- can be installed without administrator privileges when using the Clean Access Agent Stub (SMS)
- localized (based on the Localization settings of Windows)
- available for
  - Windows 2000, XP, Vista
  - MacOS (version10.4 and 10.5)

Web Agent

- doing posture assessment **without the native Clean Access Client**
  - **if the user does not have privilege to install the agent**
  - **occasional access (like guests and contractors)**
- available for Windows 2000, XP, Vista
- ActiveX or Java applet based
- Internet Explorer, Firefox browser
- downloadable from captive portal



Gold Certified

CAS operation modes

Operation mode	Options
Forwarding	Bridged mode (**virtual gateway**) Routed mode (**real IP gateway** / NAT gateway)
Location of CAS	**Central** **Edge**
Client access	**Layer 2** (client and CAS are L2 adjacent) **Layer 3** (client and CAS are NOT L2 adjacent)
Data path	**In-band** (CAS always in data path) **Out-of-band** (CAS in data path only during validation and posture assessment)

CAS operation modes
Most frequently used combinations

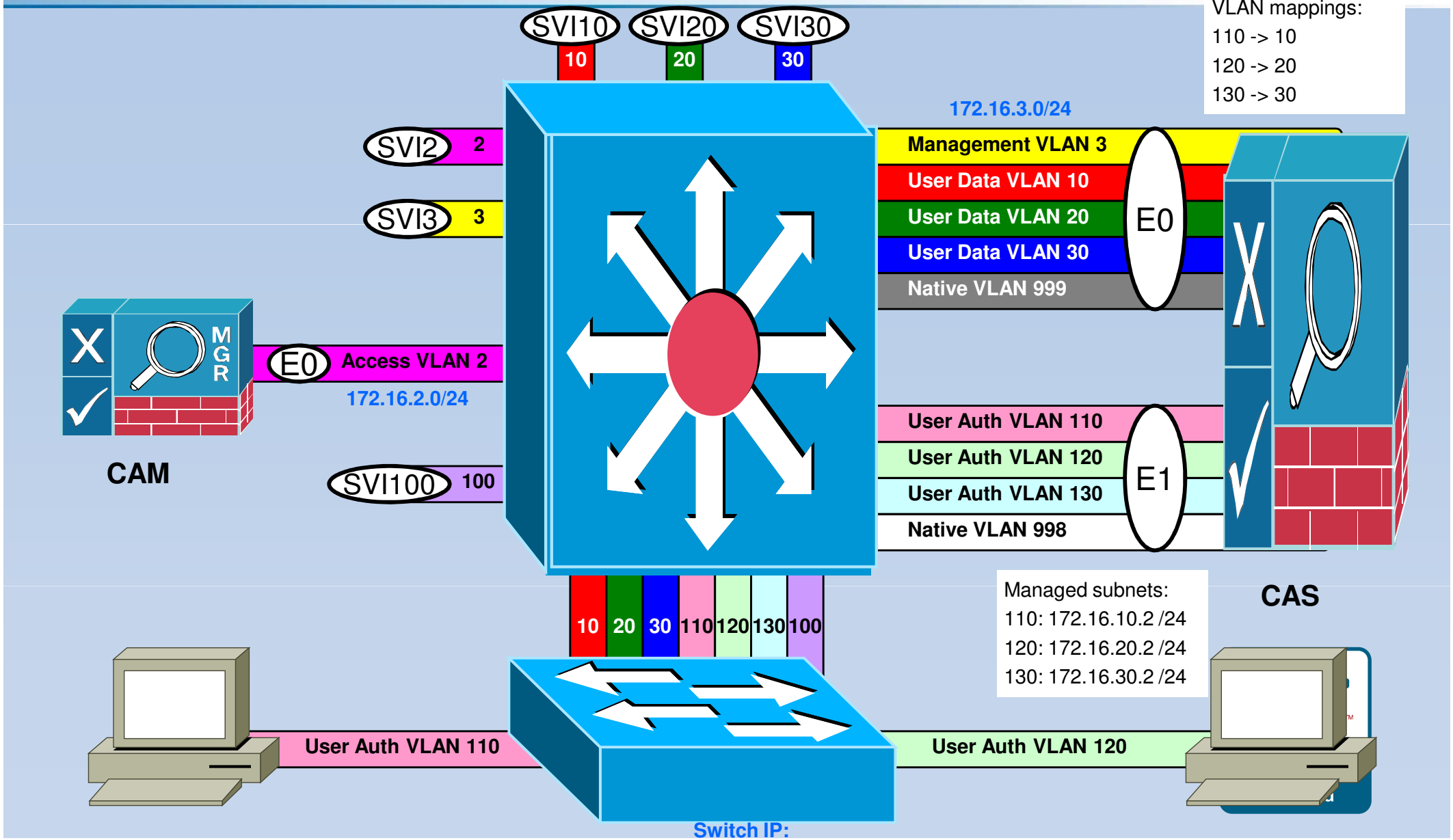
- **Wireless**
  - L2 – In-Band – Real-IP-Gateway
  - L2 – Out-of-Band – Virtual Gateway
- **Remote-access VPN (ASA, VPN 3000, IOS)**
  - L3 – In-Band – Real-IP-Gateway
- **Large-scale WAN network**
  - L3 – Out-of-Band – Real-IP Gateway
- **Campus**
  - L2 – Out-of-Band – Virtual Gateway

Solution: None

Examples

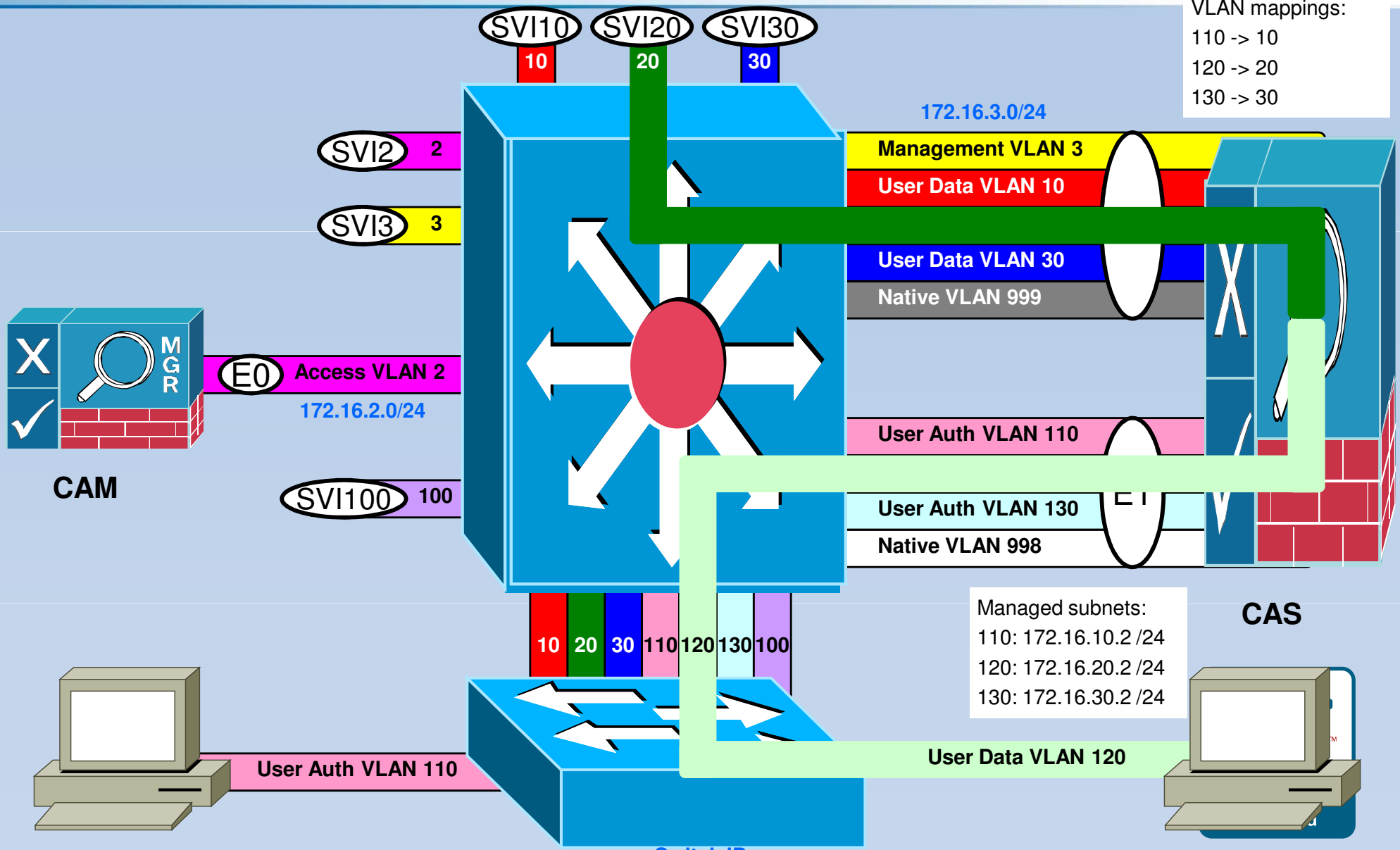
L2, Out-of-Band, Virtual Gateway

L2, OOB, Virtual Gateway topology



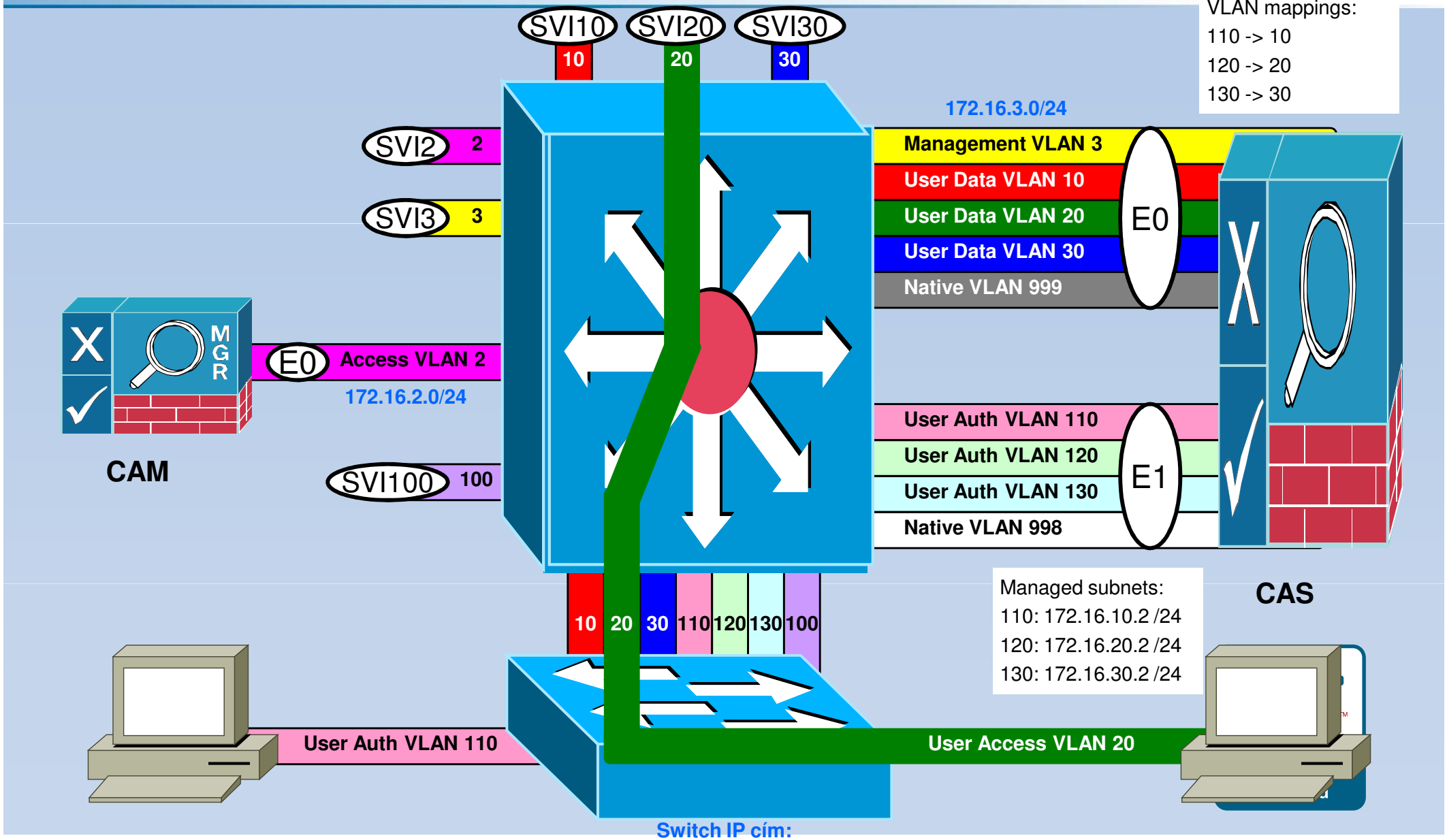
www.snt-world.com

L2, OOB, VGW – During posture assessment

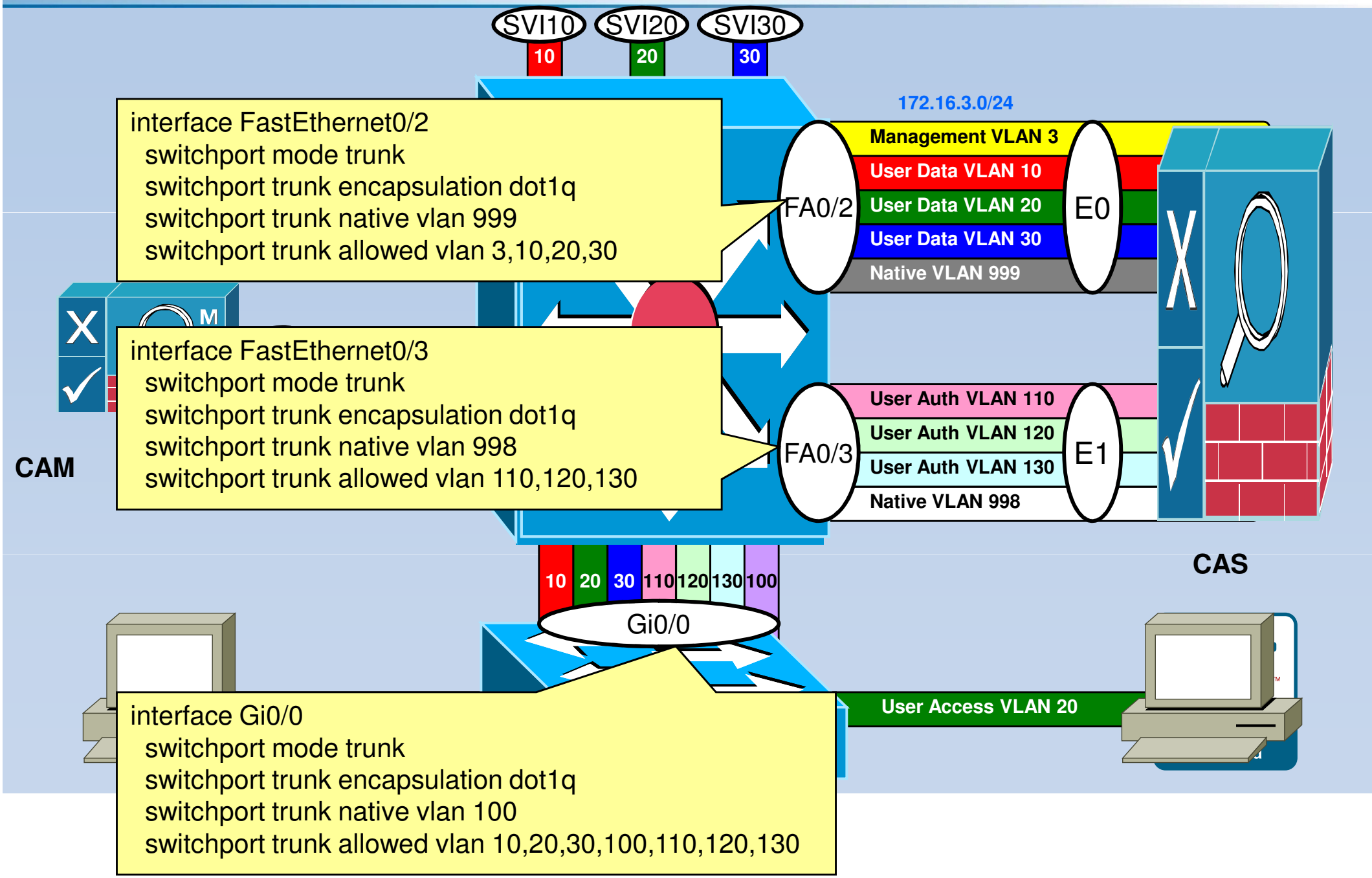


www.snt-world.com

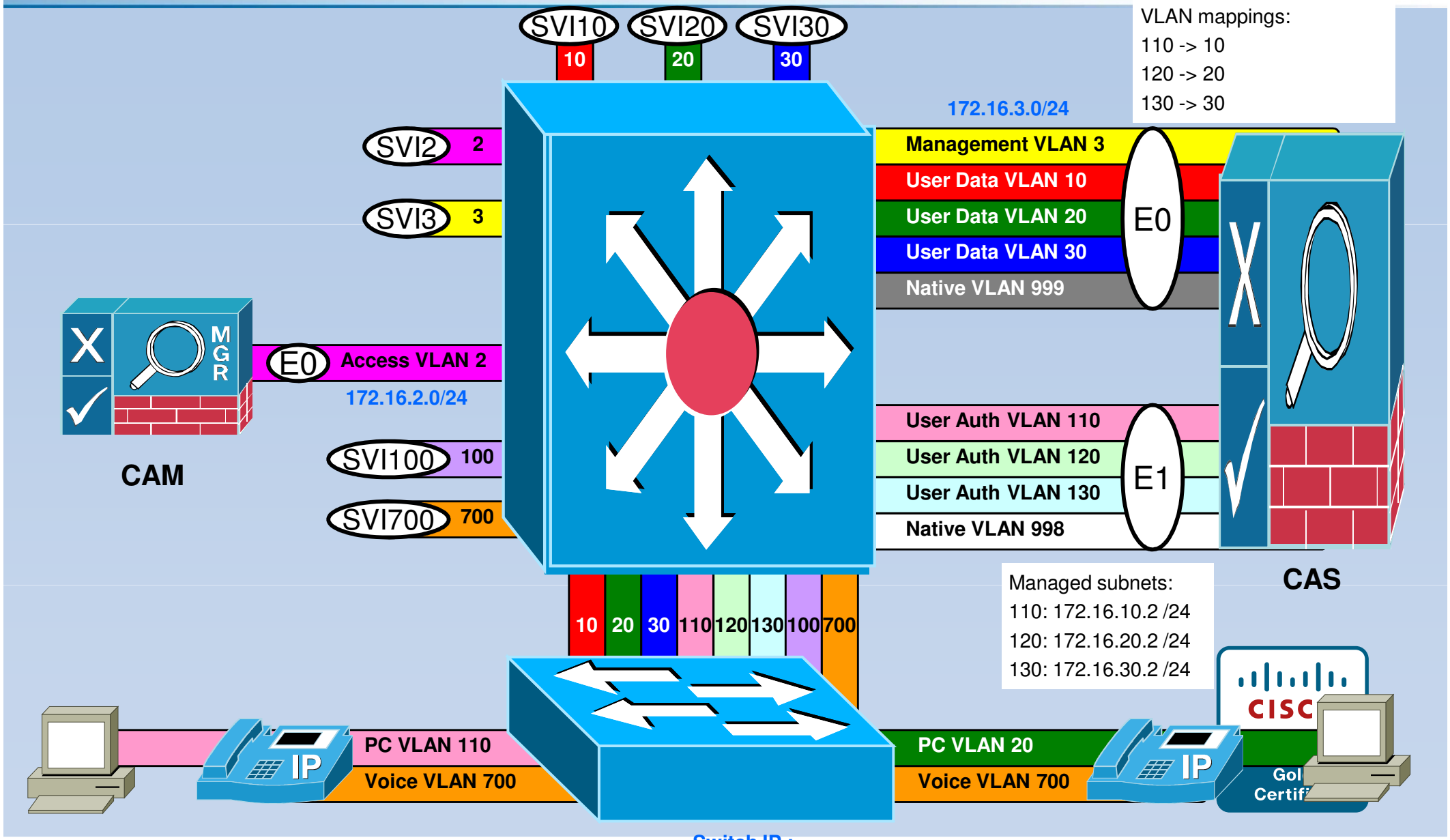
L2, OOB, VGW – After successful login



L2, OOB, VGW – Switch configuration



L2, OOB, Vgw + IP phone



Unauthenticated user
IP address:
172.16.10.100 /24

Switch IP :
172.16.100.2 /24

Authenticated user
IP address:
172.16.20.100 /24

L2, OOB, VGW + IPT: port configuration

Switch-port in **access** mode:

```
interface FastEthernet0/2
  description IPT and PC
  switchport mode access
  switchport access vlan 120
  switchport voice vlan 700
  snmp trap mac-notification added
  spanning-tree portfast trunk
```

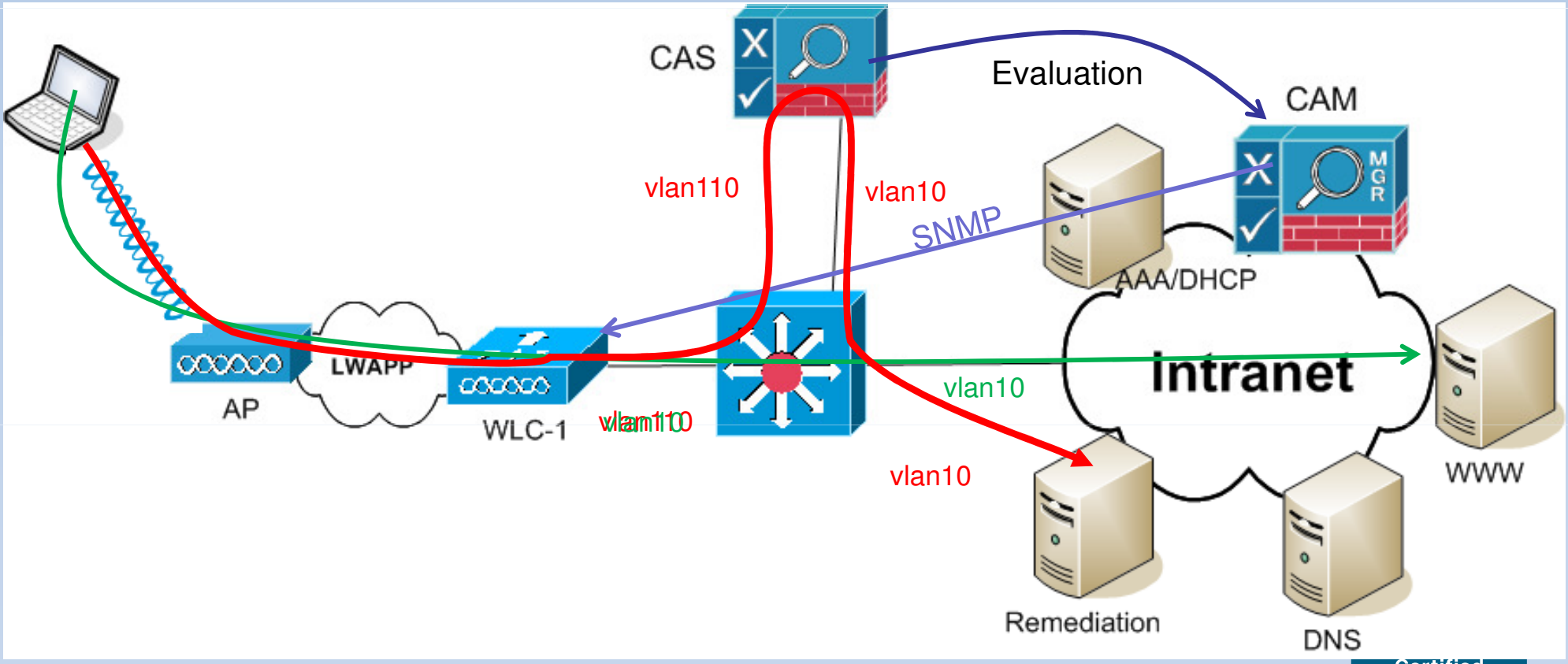
Switch-port in **trunk** mode:

```
interface FastEthernet0/3
  description VoIP and PC
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 120
  switchport mode trunk
  switchport trunk allowed vlan 20,120,700
  snmp trap mac-notification added
  spanning-tree portfast trunk
```

NAC login demo – What the end-user sees...

Wireless out-of-band operation (from 4.5)

CAS in the data path only during evaluation

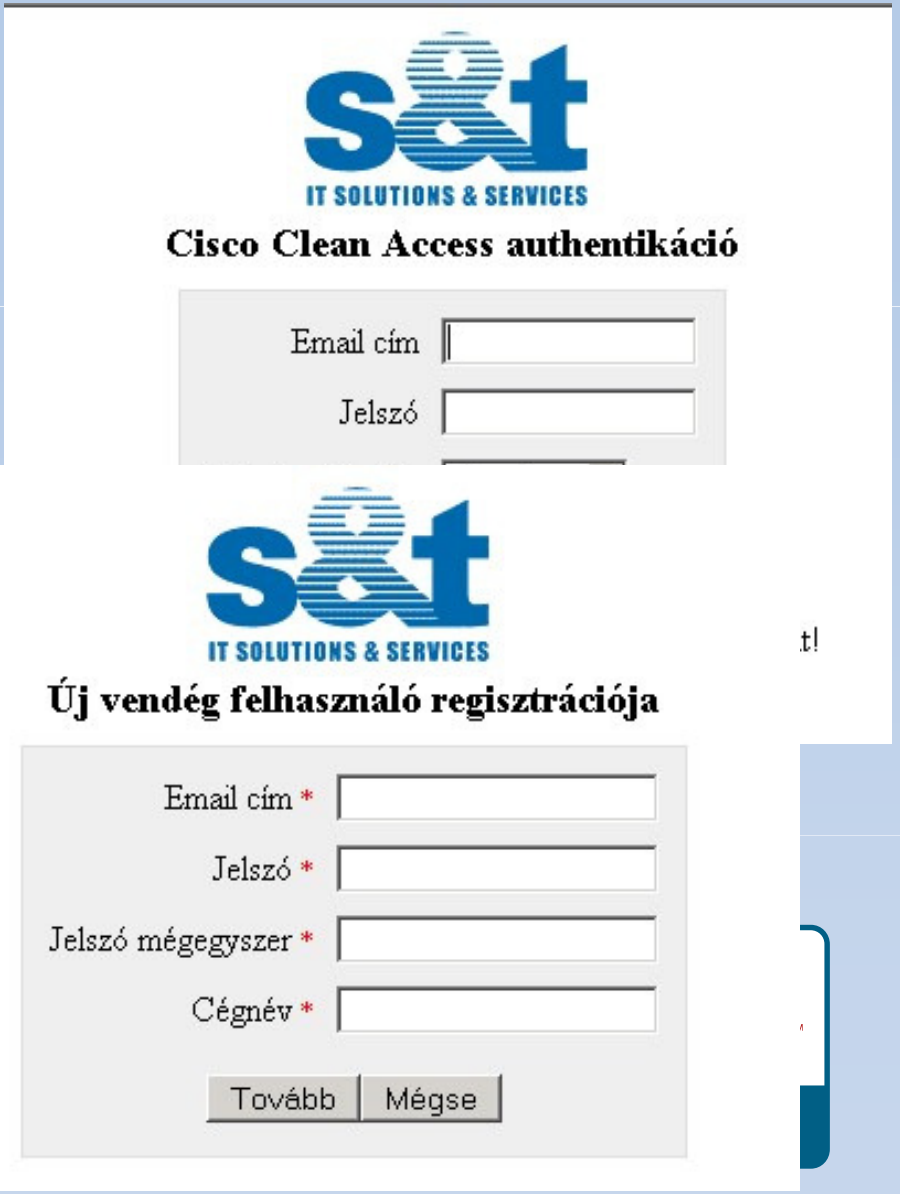


Guest access

CAM integrated guest functions

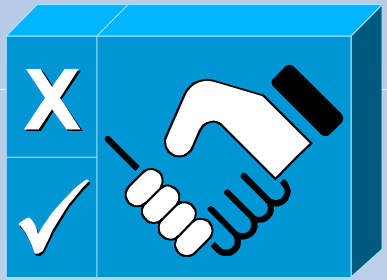
- **Guests can be authenticated using**
  - external AAA server (radius, ldap etc)
  - local database
  - self-registration page
  - built-in guest user account
    (no need to share the password)
- **Time-limited access**
- **Filtering functions**
  - URL filtering, ACL, QoS
  - customizable per CAS, VLAN
- **Monitoring and audit functions**
- **Customizable portal**

- **CAM integrated feature**



NAC Guest server

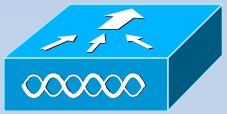
- **Extra component of NAC system**
- **Internal employees can grant the access for their own guests**



- **Benefits**
  - off-loading IT team
  - provisioning and reporting
  - Group based policy management
  - LDAP, AD, RADIUS integration
  - Delivery of credentials: email, SMS, printing
  - automatic guest account generation
  - customizable account scheduling

- **Supports multiple CAMS**

Guest server components



SPONZOR

Internal user who wants to be able to provide internet access to the guest

GUEST SERVER

Central management interface for registering and monitoring guest accounts

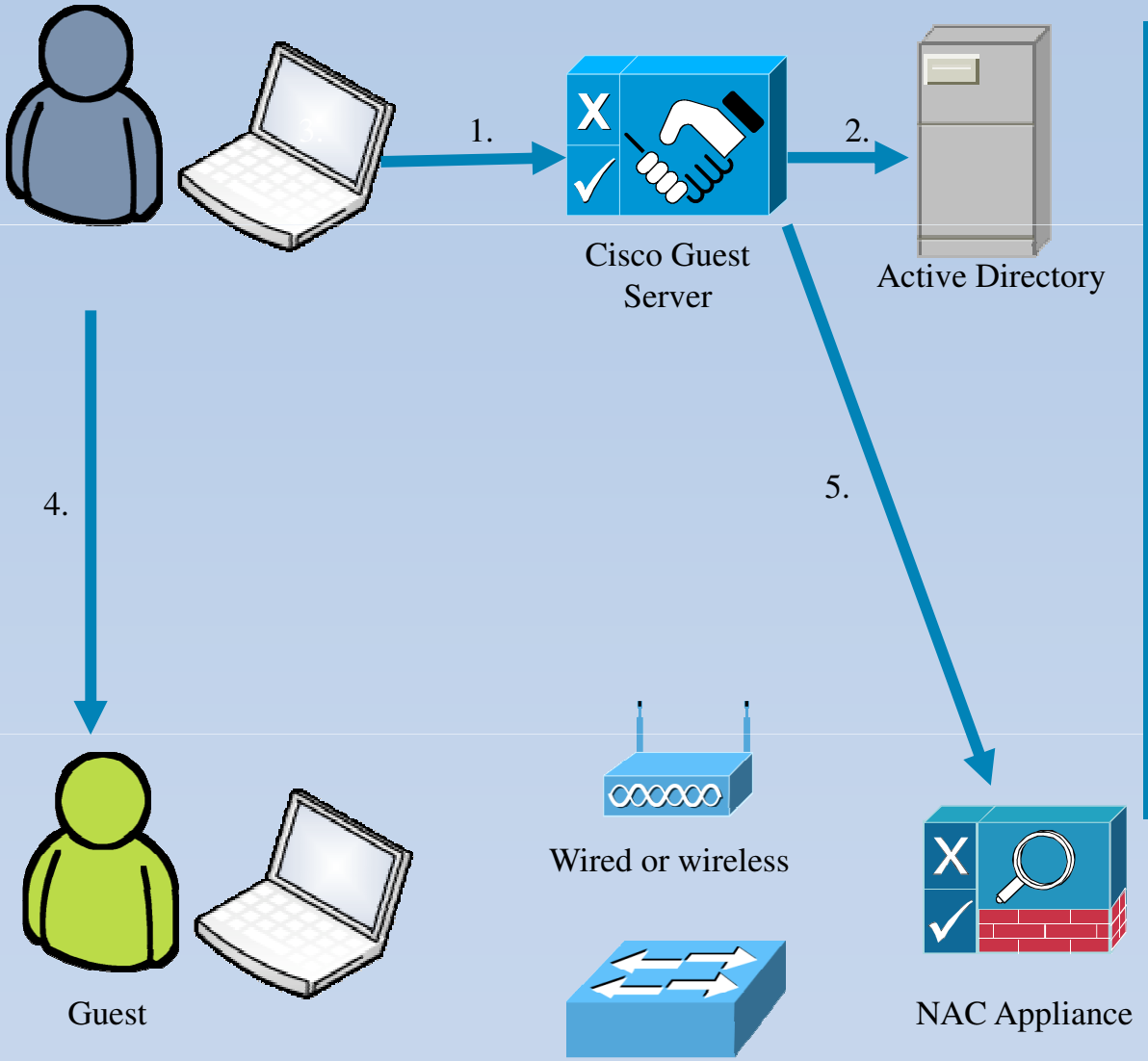
NETWORK ENFORCEMENT DEVICE

Device that authenticates the guests and grants network access

Guest

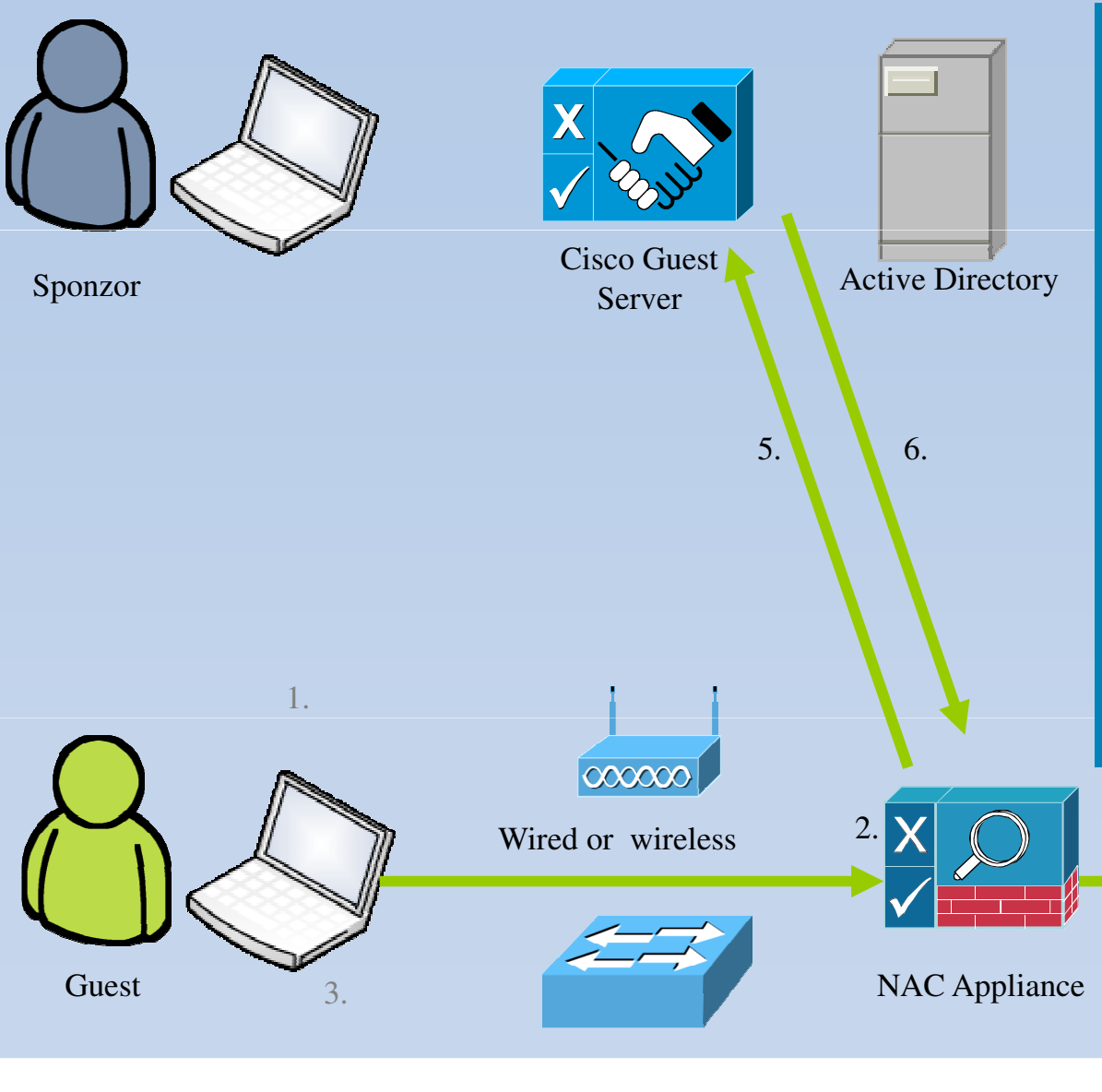
Visitor who needs network access (usually internet only)

Guest Access Walkthrough – Sponsor



1. Sponsor accesses Guest server portal, such as http://guests.snt.mk)
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 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

Creating guest accounts - demo

Thanks for your attention!
Questions are welcomed!

János György SIMON

janos.simon@snt.hu


CISCO


CISCO
PARTNER
Gold
Certified