Cisco Expo 2007

Cisco NAC Appliance

Dragan Novaković, sistem inženjer

dnovakov@cisco.com

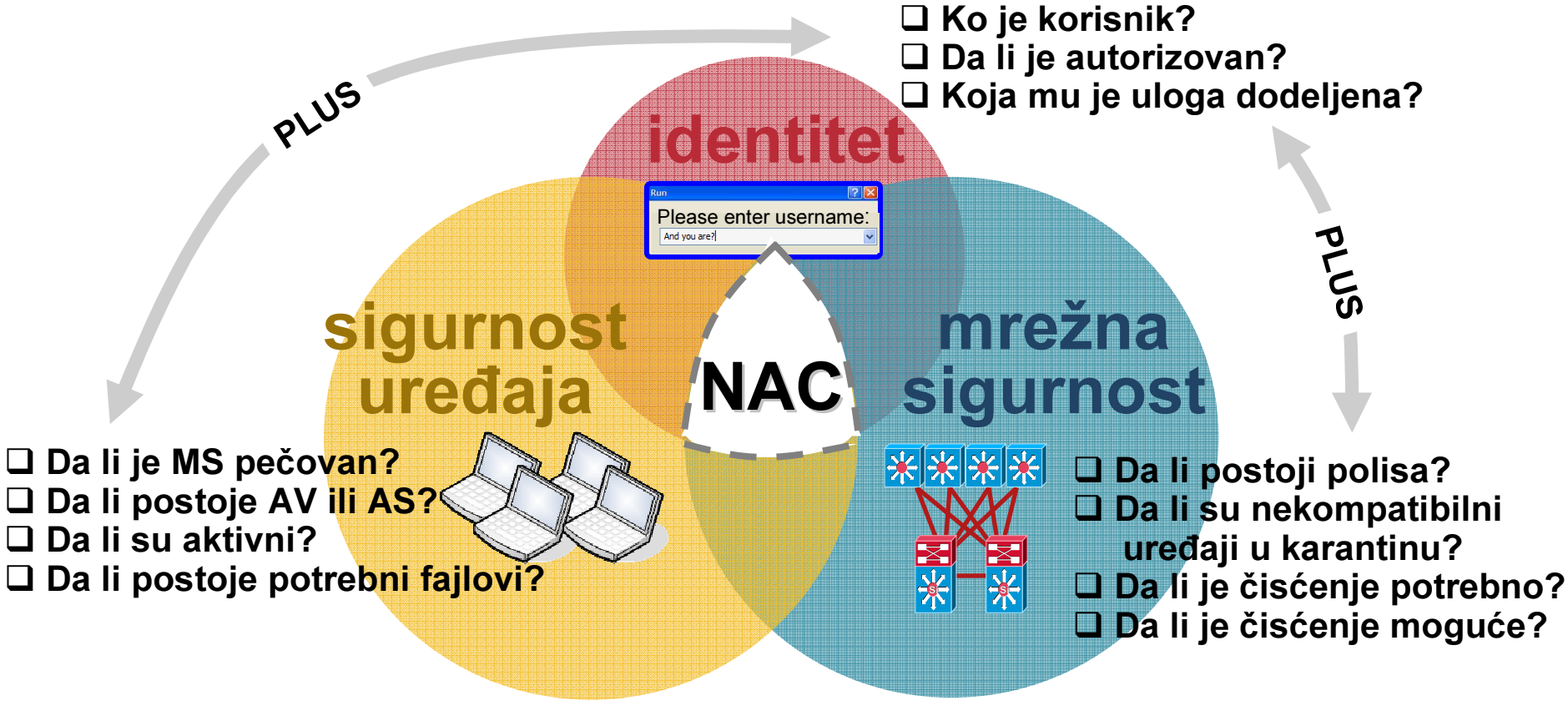
Enable Your Network
Empower Your Business

Agenda

- Šta je to NAC ?
- Komponente
- Pregled
- Dizajn i implementacija
- Pitanja i KVIZ !

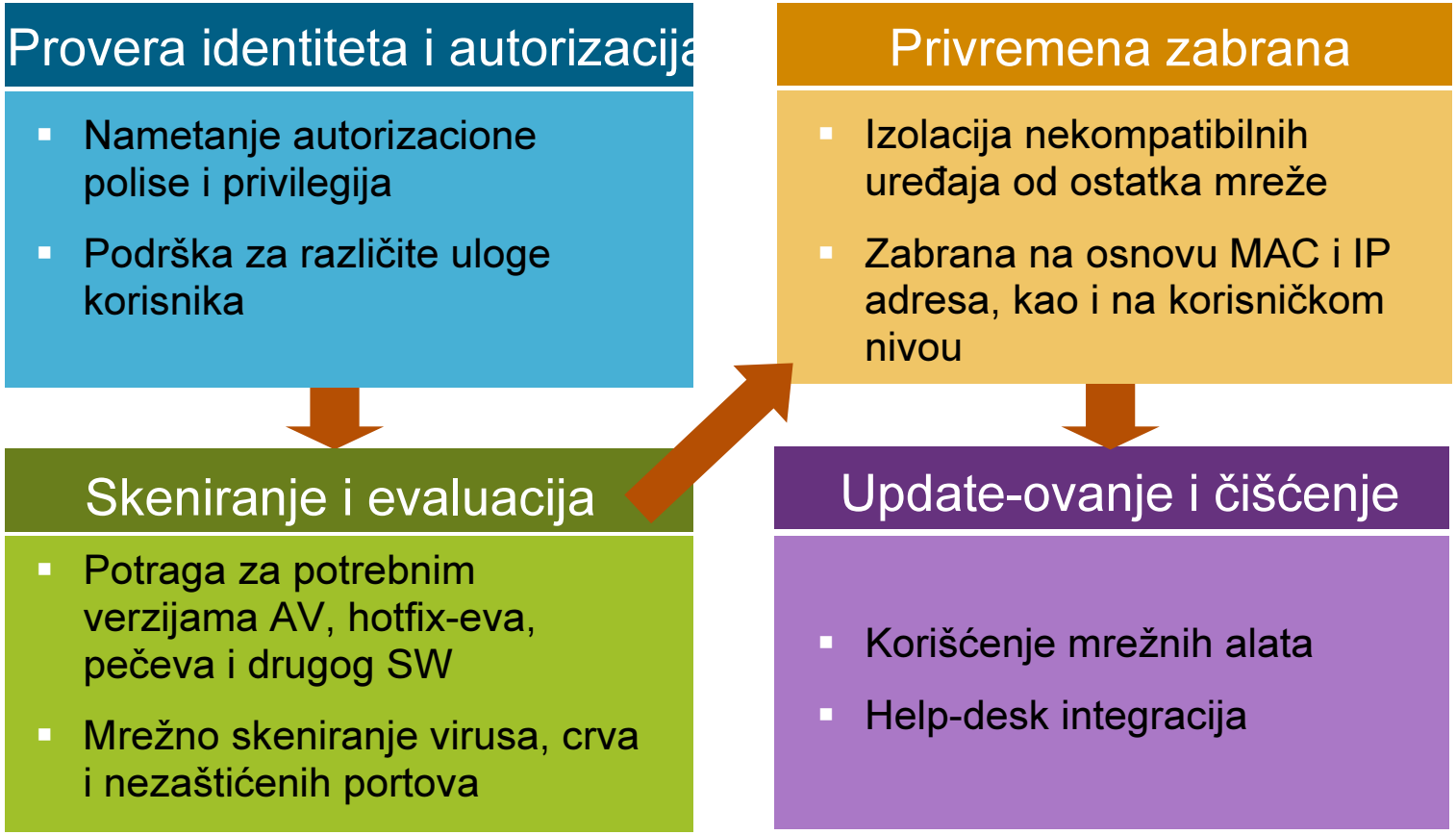
Šta je to Network Admission Control - NAC?

Korišćenje mreže za obezbeđivanje kontrole pristupa



Pristup mreži zavisi od usaglašenosti

Na osnovu polise pristupa mreži se:



NEMA USAGLAŠENOSTI = NEMA PRISTUPA MREŽI

Agenda

- Šta je to NAC ?
- Komponente
- Pregled
- Dizajn i implementacija
- Pitanja i KVIZ !

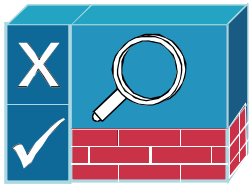
NAC Appliance komponente

- Cisco Clean Access Manager - CAM

  Centralizovani menadžment za administratore, tehničku podršku i operatore

- Cisco Clean Access Server - CAS

  Služi kao inicijator kontrole pristupa mreži (network access control)

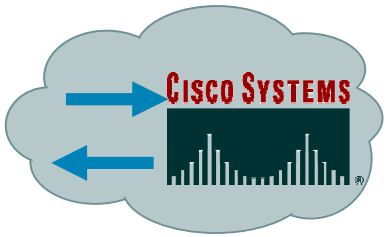


- Cisco Clean Access Agent - CAA

  Opcionalni klijent na krajnjem uređaju

- Rule-set Updates

  Redovni automatski update za anti-viruse, kritične hotfix-ove i druge aplikacije



NAC Appliance Product Portfolio

NAC Menadžeri - CAM

Manager Lite - do 3 Servera
(podržava do 500 korisnika po CAS i Modulu)

Standard Manager - do 20 Servera
(podržava sve Servere i Module)

Super Manager - do 40 Servera
(podržava sve Servere i Module)

NAC Serveri - CAS

Network Module

- 100 korisnika
- 250 korisnika
- 500 korisnika
- 50 korisnika
- 100 korisnika
- 1500 korisnika
- 2500 korisnika
- 3500 korisnika

korisnik = online, istovremen

Accessories

- NAC Profiler Server
- NAC Collector

Cisco NAC partnerstva

NAC podržava polise za više od 300 aplikacija i 50 partnera

Agenda

Šta je to NAC ?

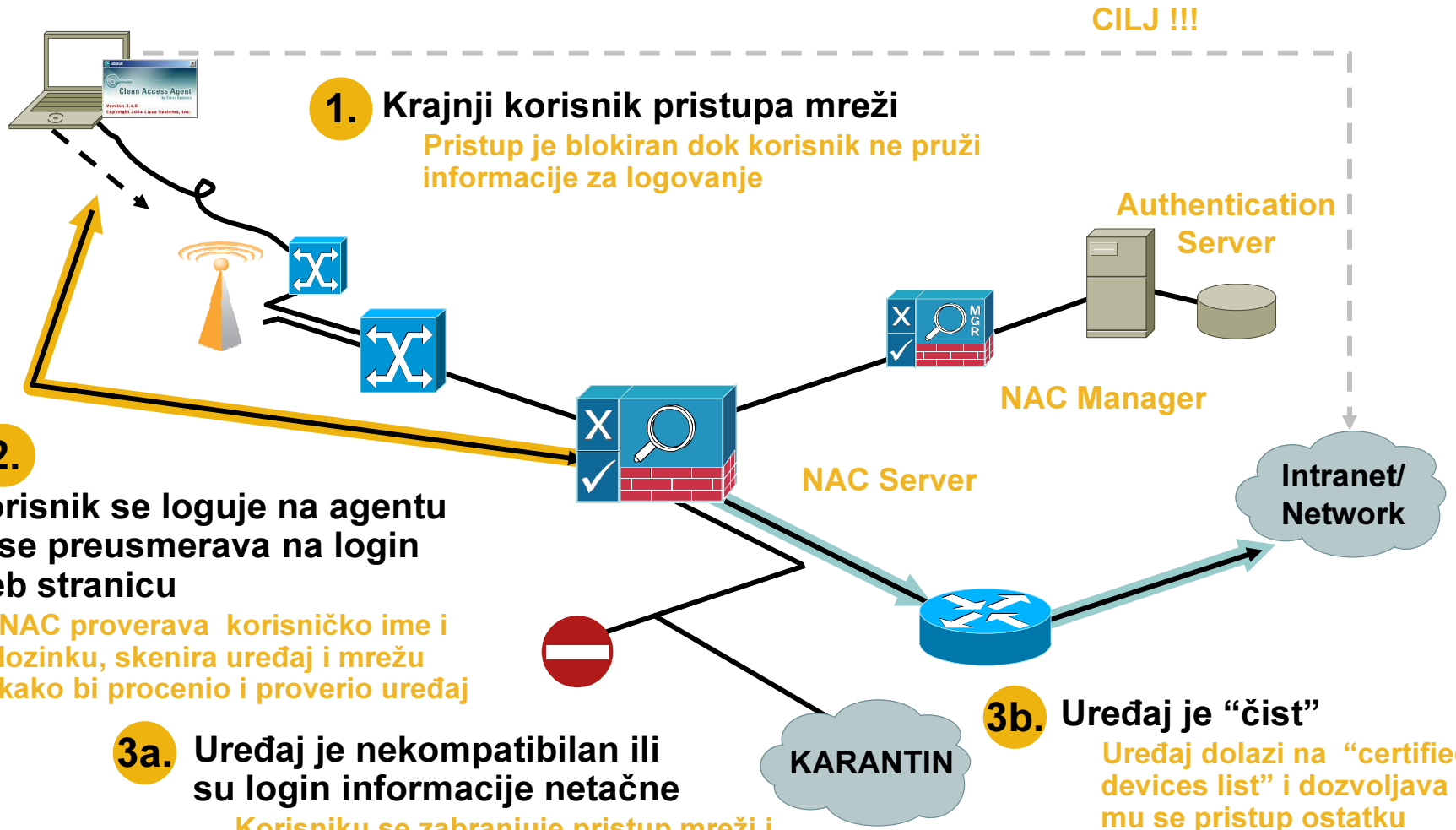
Komponente

Pregled tehnologije

Dizajn i implementacija

Pitanja i KVIZ !

Cisco NAC Appliance - Pregled



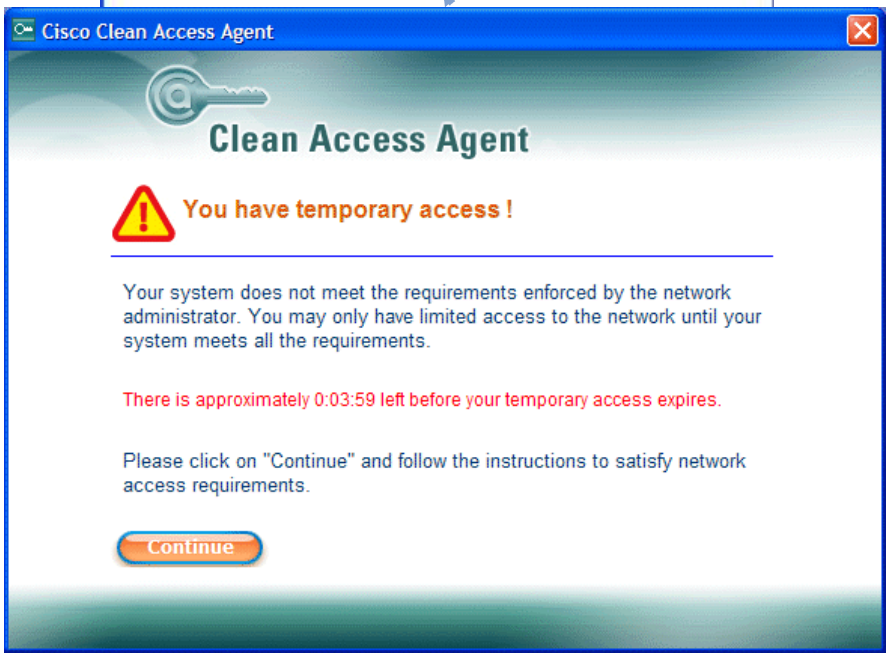
Agent

Login prozor

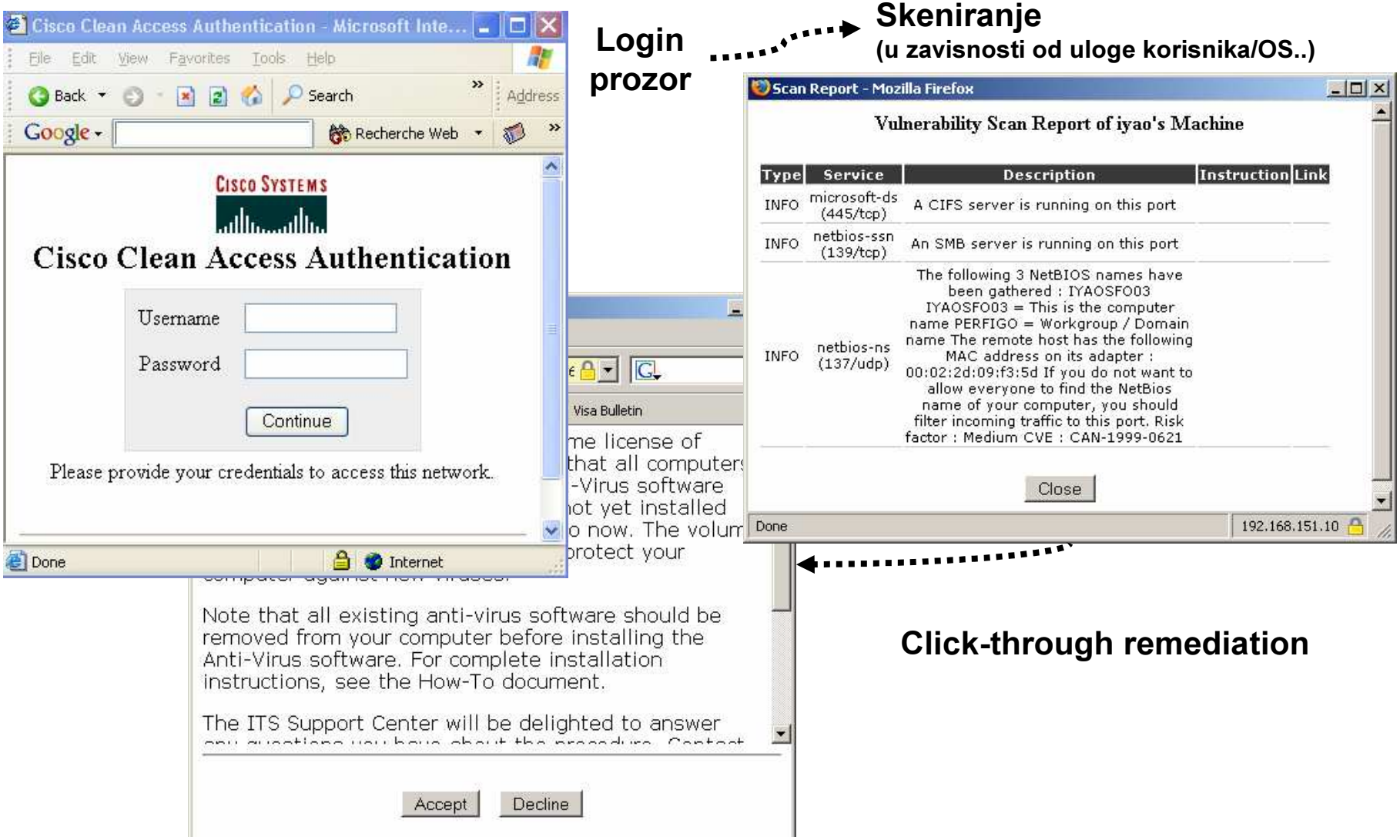
Skeniranje uređaja
(u zavisnosti od uloge korisnika...)

Greška !

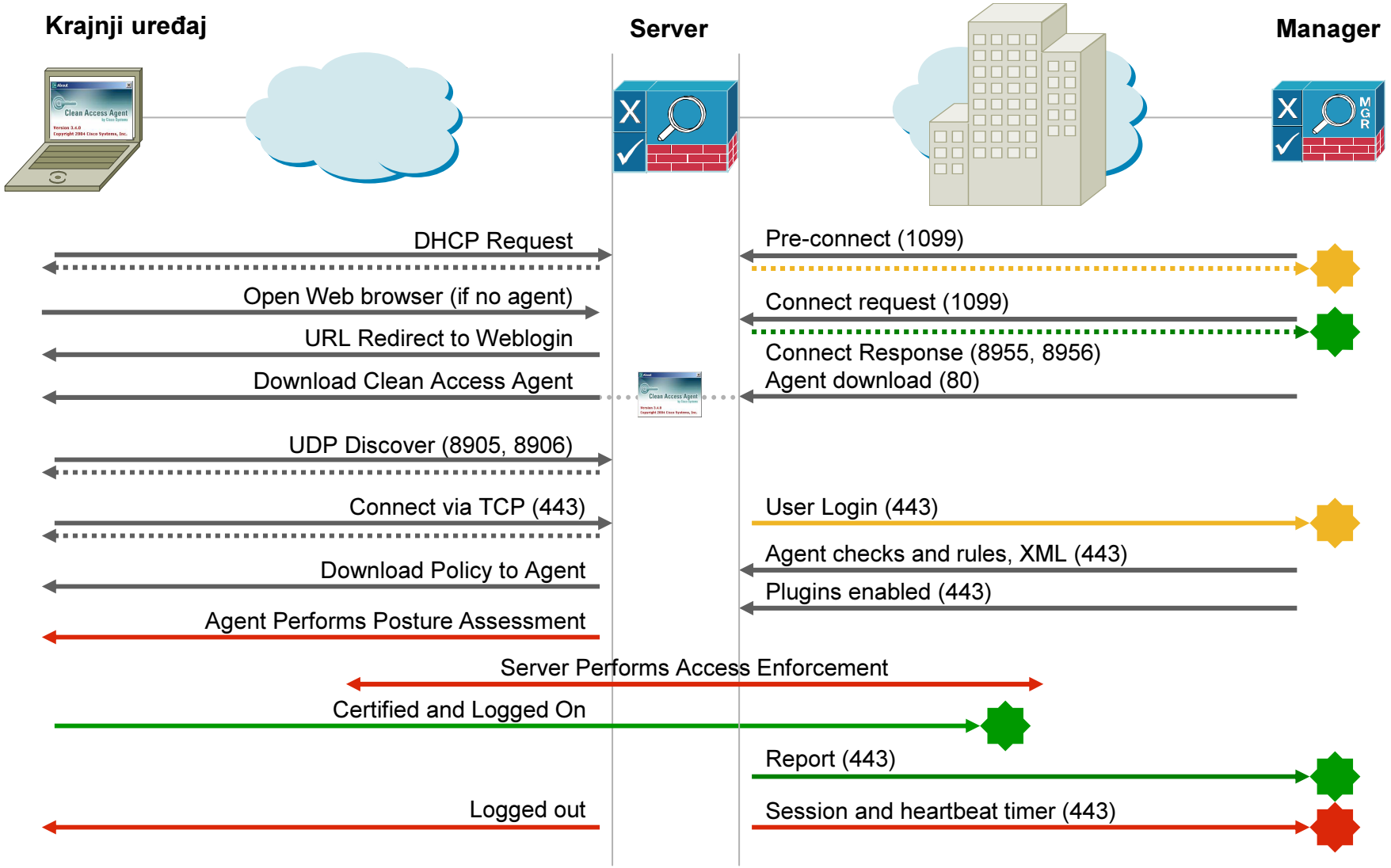
"čišćenje"



Web login



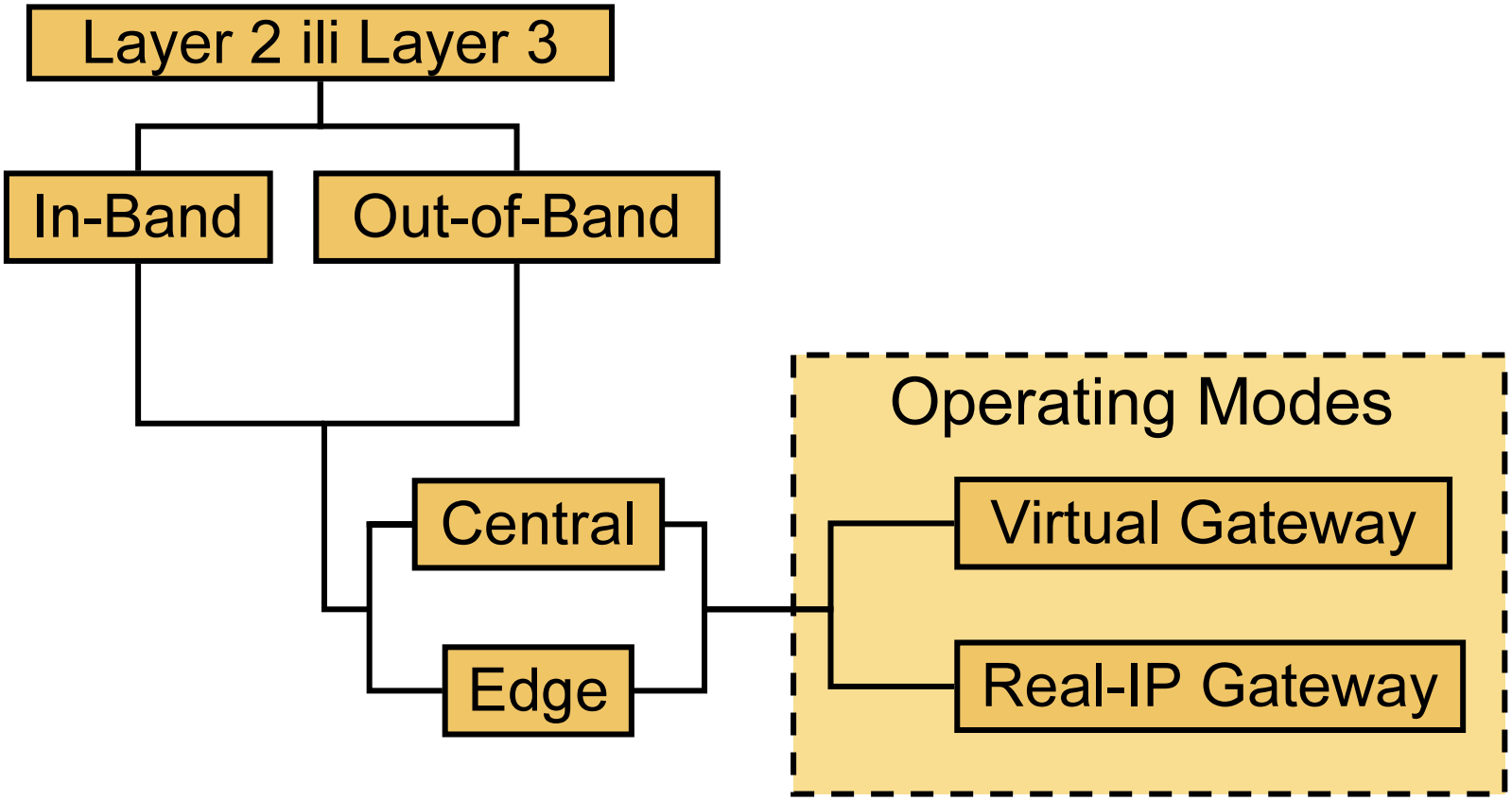
Tok procesa



Agenda

- Šta je to NAC ?
- Komponente
- Pregled
- Dizajn i implementacija
- Pitanja i KVIZ !

Cisco NAS implementacije



Virtual Gateway & Real IP Gateway

- Clean Access Server može da prosleđuje saobraćaj na dva načina:

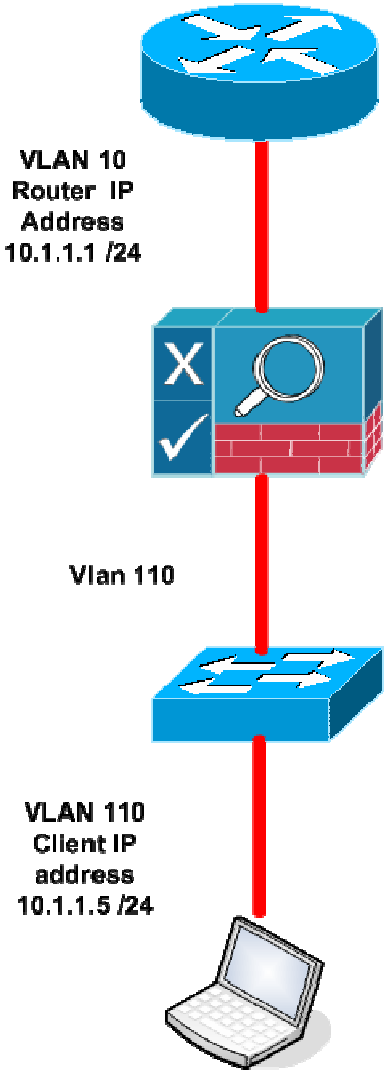
  Bridž Mod = Virtual Gateway

  Routed Mod = Real IP Gateway

- Bilo koji CAS može biti konfigurisan za bilo koji od ova dva metoda
- Logički tok saobraćaja zavisi od izbora Gateway moda
- Ne zavisi od toga da li je CAS u Layer 2 modu, Layer 3 modu, In Band ili Out of Band

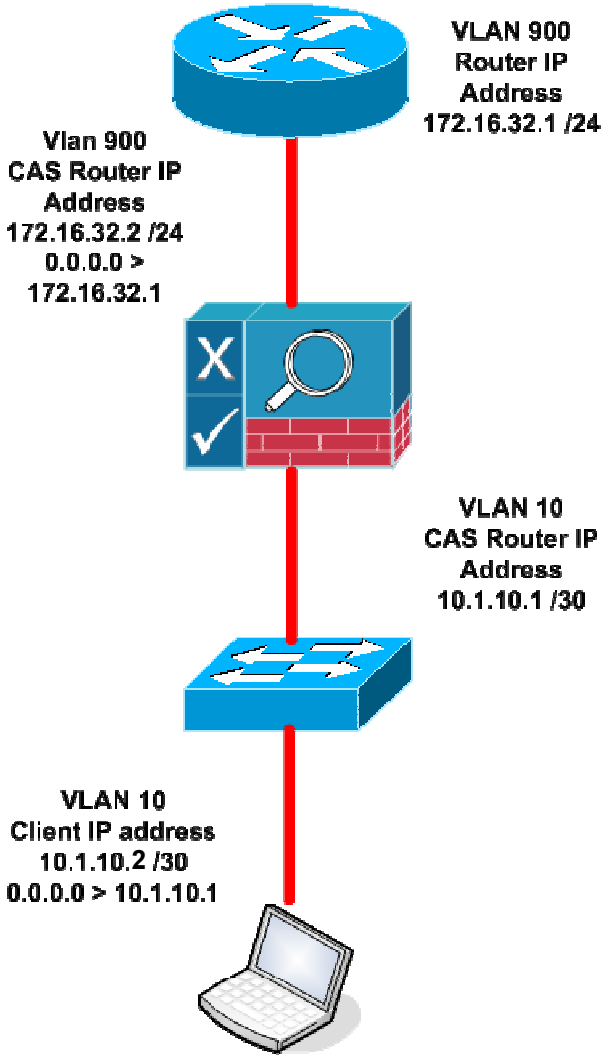
Virtual Gateway mod

- Bridžing mod: prosleđivanje frejmova, CAS – transparentni bridž
- source/destination MAC i IP adresa se prosleđuju ili bez menjanja
- def.gateway na tzv.“Trusted” strani



Real IP Gateway mod

- CAS je L3 uređaj, rutira saobraćaj između untrusted i trusted dela mreže
- Statičke rute na next hop uređaju
- CAS def.gateway
- CAS može biti DHCP server



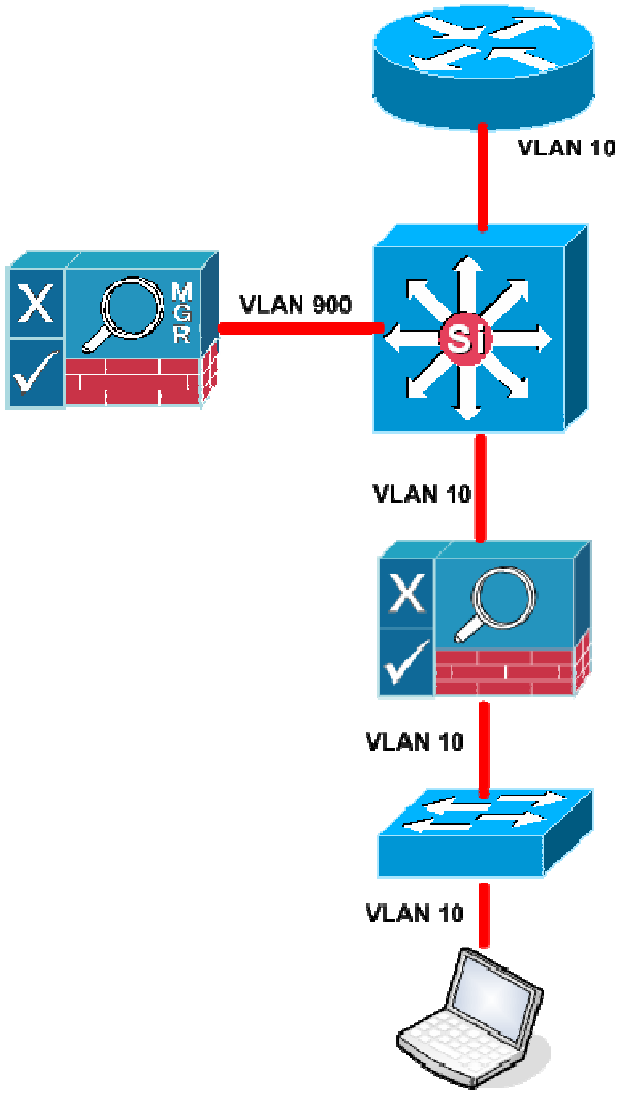
Edge i Central implementacija

- Clean Access Servers može da ima dve fizičke implementacije
  - Edge implementacija
  - Central implementacija
- Bilo koji CAS može biti konfigurisan za bilo koji od ova dva metoda
- Izbor implementacije utiče na fizičku putanju saobraćaja
- Ne zavisi od toga da li je CAS u Layer 2 modu, Layer 3 modu, In Band ili Out of Band

Edge implementacija

- CAS logički i fizički “inline”
- Podržan od svih Catalyst svičeva
- VLAN IDs se prosleđuju ako je CAS u VGW modu

  10 → 10
- Instalacije sa više Access Layer čvorišta postaju kompleksne

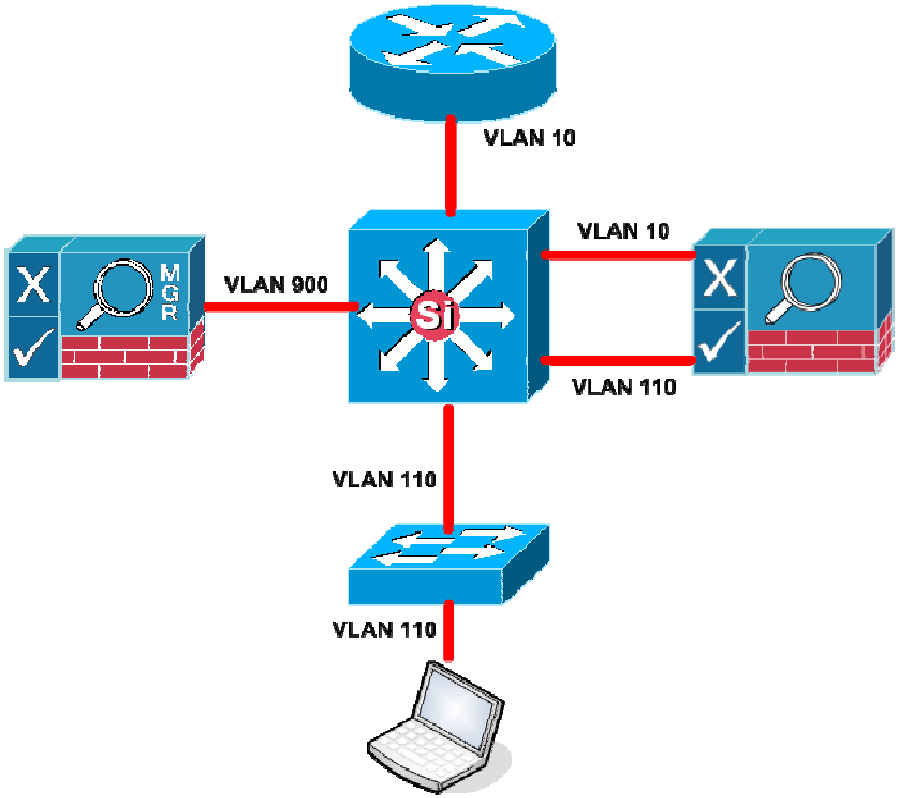


Centralna implementacija

- Najčešći slučaj implementacije
- CAS je samo logički “inline”
- Podržan od 6500 / 4500 / 3750 / 3560 *
- VLAN mapiranje u VGW modu

  110 → 10
- Najskalabilnije rešenje u većim mrežama

*3550 nije podržan

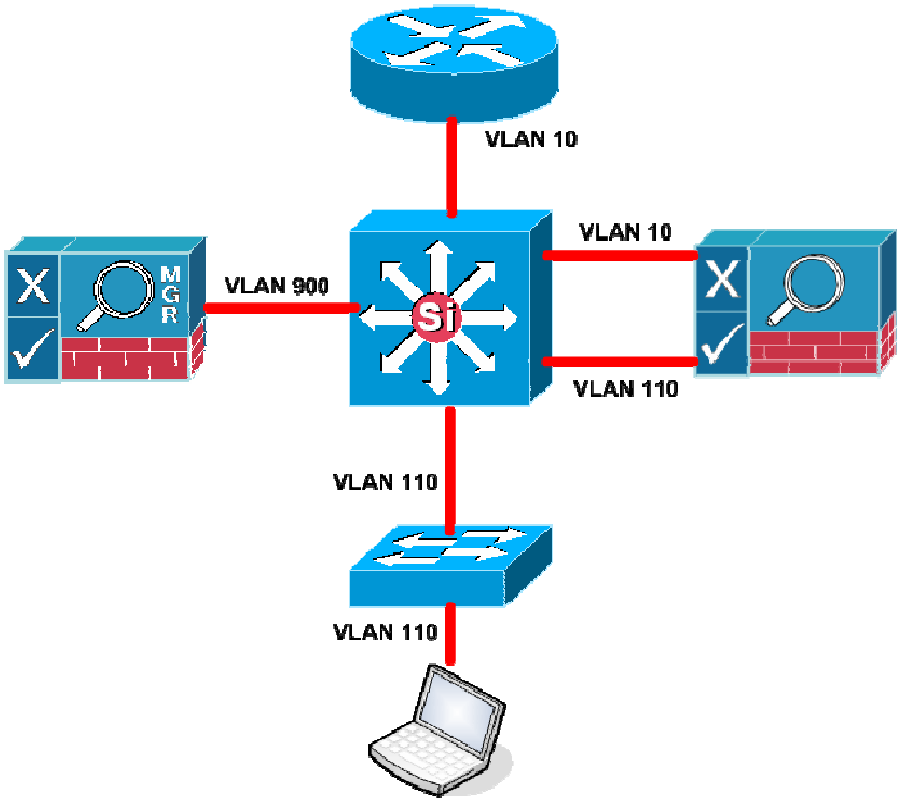


Layer 2 Mod i Layer 3 Mod

- Clean Access Serveri imaju dva modela pristupa klijenata:
  - Layer 2 Mod
  - Layer 3 Mod
- Bilo koji CAS može biti konfigurisan za neki od ova dva moda
- Model pristupa zavisi od toga da li je klijent ima ili nema L2 vezu sa CASom

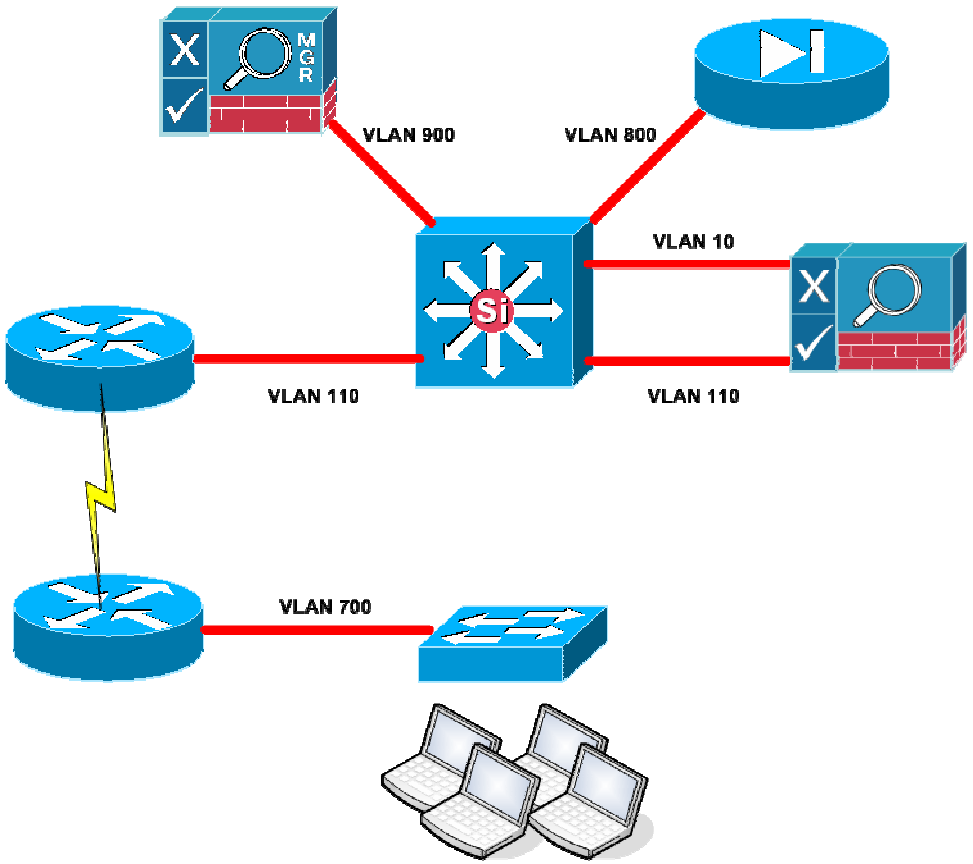
Layer 2 Mod

- Klijent ima Layer 2 vezu sa CASom
- MAC adresa se koristi kao jedinstveni identifikator
- Podržani i VGW i Real IP GW
- Podržani i In Band i Out of Band mod
- Najčešći model za LANove



Layer 3 Mod

- Klijent nema Layer 2 vezu sa CASom
- IP adresa se koristi kao jedinstveni identifikator
- Podržani i VGW i Real IP GW
- Podržan In Band i Out of Band Mod
- Potreban za WAN i VPN implementacije

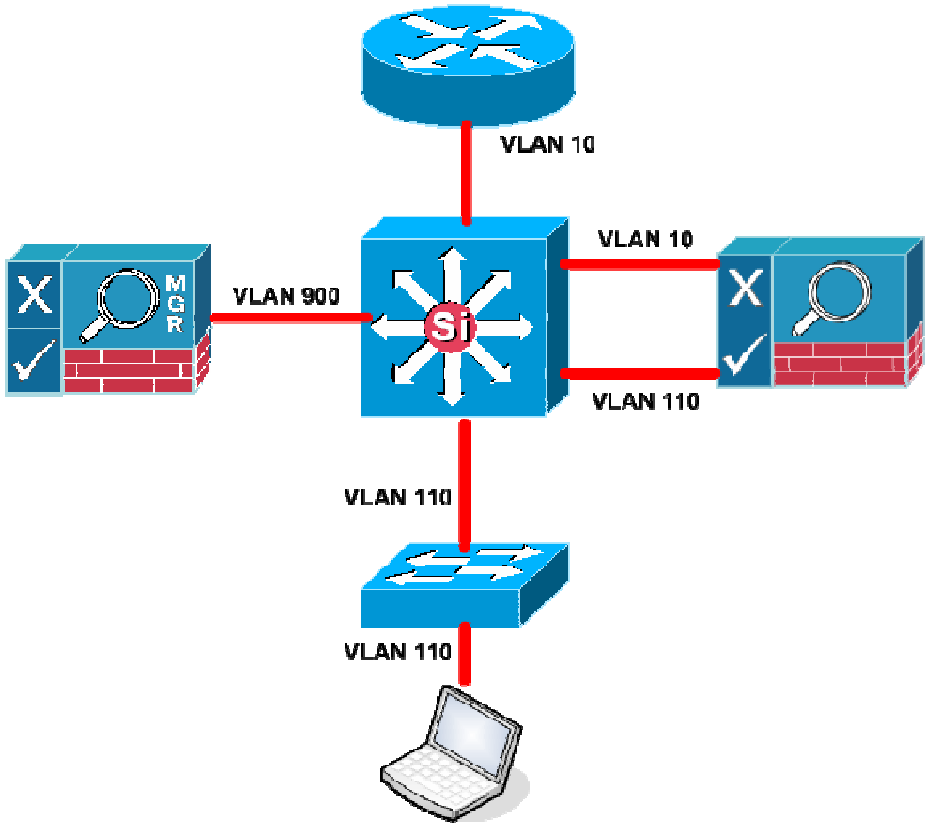


In Band & Out of Band

- Clean Access Server može da ima dva moda u zavisnosti od toka saobraćaja
  - In Band mod
  - Out of Band Mod
- Bilo koji CAS može biti konfigurisan za neki od ova dva moda, ali ne istovremeno u oba
- CAS je uvek “inline” za vreme ispitivanja klijenta

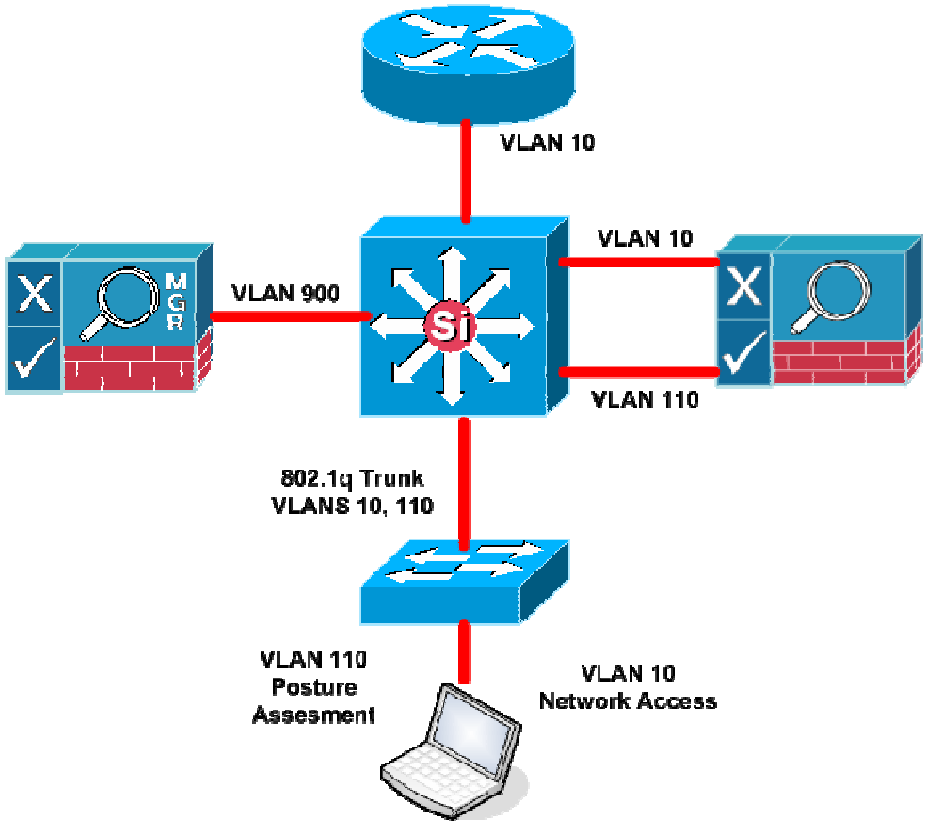
In Band

- Jednostavan za implementaciju
- CAS je Inline pre, za vreme i posle provere stanja krajnjeg uređaja
- Podrška za sve modele svičeva



Out of Band

- Preporučiv za Multi-Gig implementacije
- CAS je Inline samo za vreme ispitivanja stanja krajnjeg uređaja
- Podrška za većinu modela Cisco svičeva
- Kontrola pristupa na osnovu uloge korisnika i port VLANa



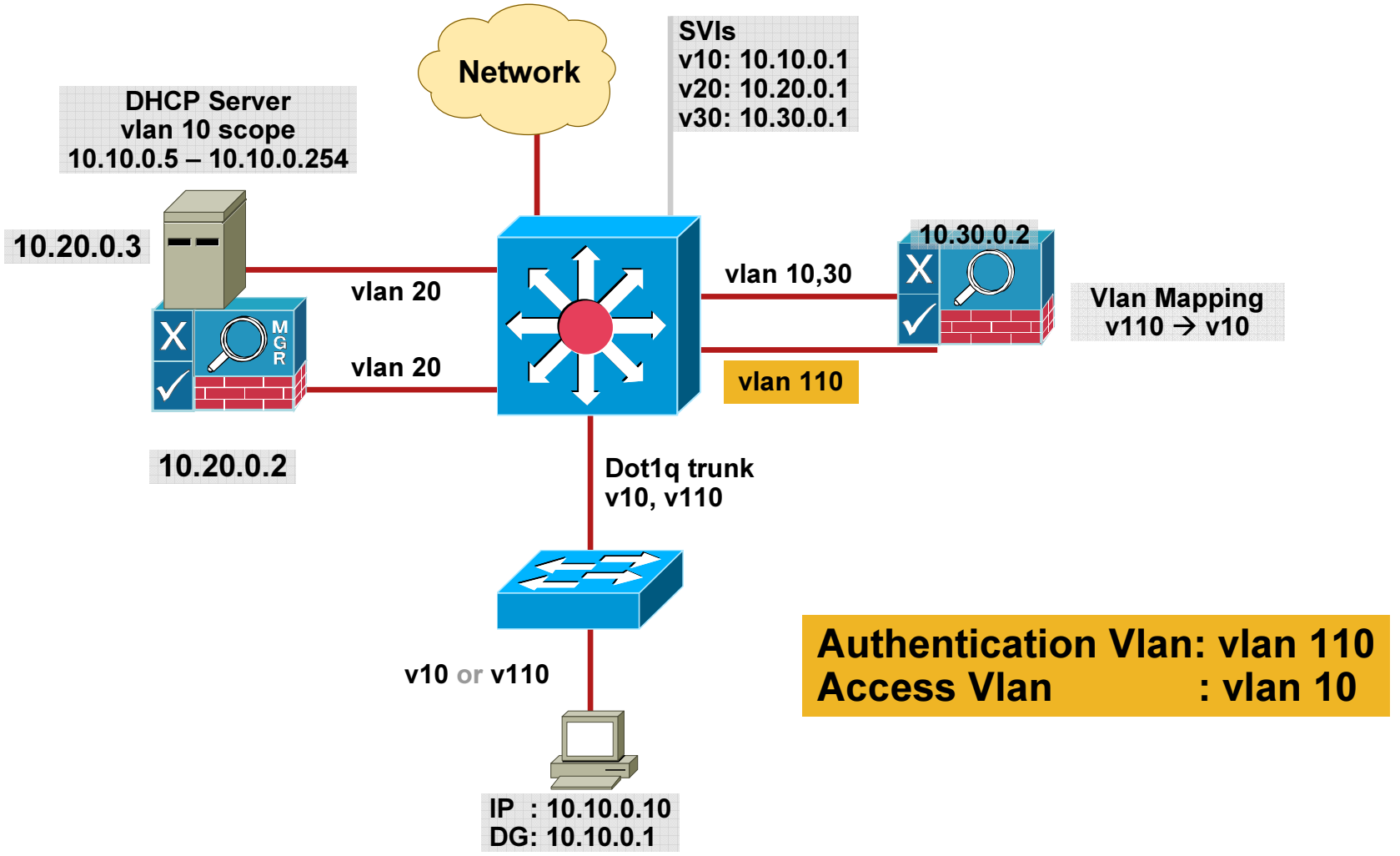
Podržani svičevi

L2/L3 Switch	Virtual Gateway		Real-IP
	Central	Edge	Central or Edge
6500	Da	Da	Da
4500	Da	Da	Da
3750/3560 (L3 switch)	Da, sa 12.2(25)SEE *	Da	Da
3550 (L3 switch)	Ne *	Da	Da
3750/3560 (L2 switch)	Da	Da	Da
3550 (L2 switch)	Da	Da	Da
2950/2960	N/A	Da	Da

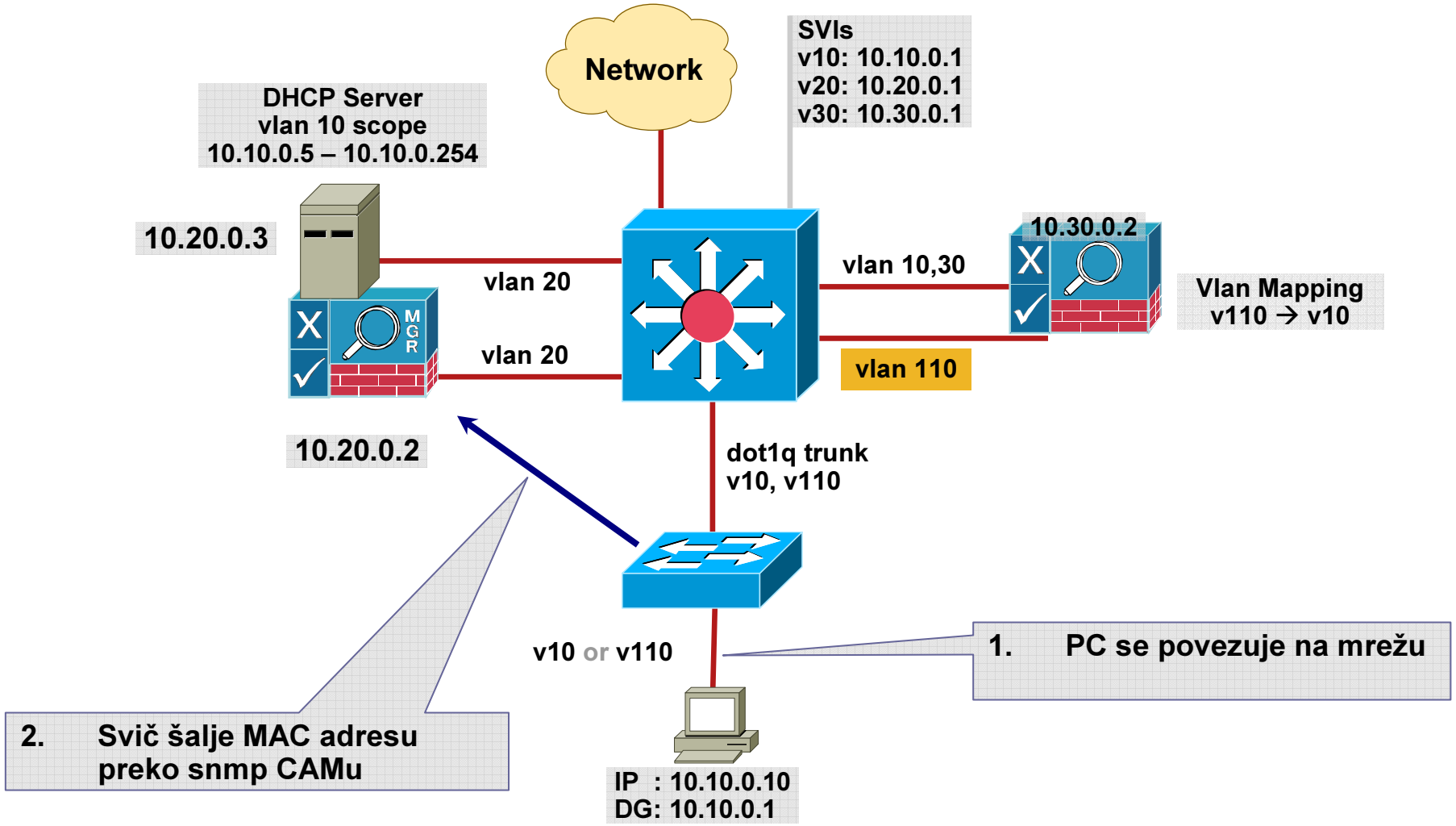
Lista podržanih Cisco svičeva i verzija:
http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca40/switch.htm

*** IOS bug CSCsb62432**

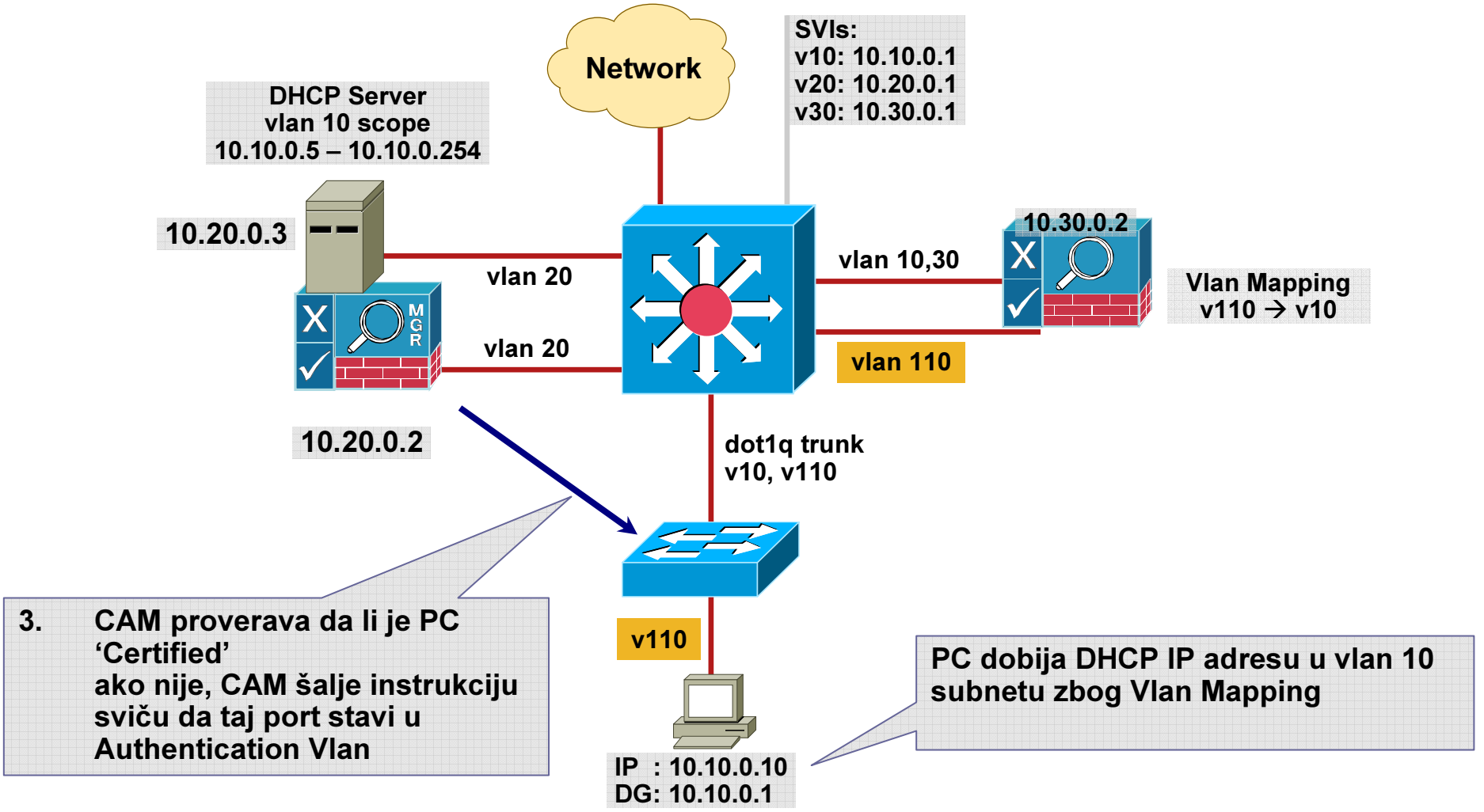
CAS u OOB L2 Virtual Gateway modu



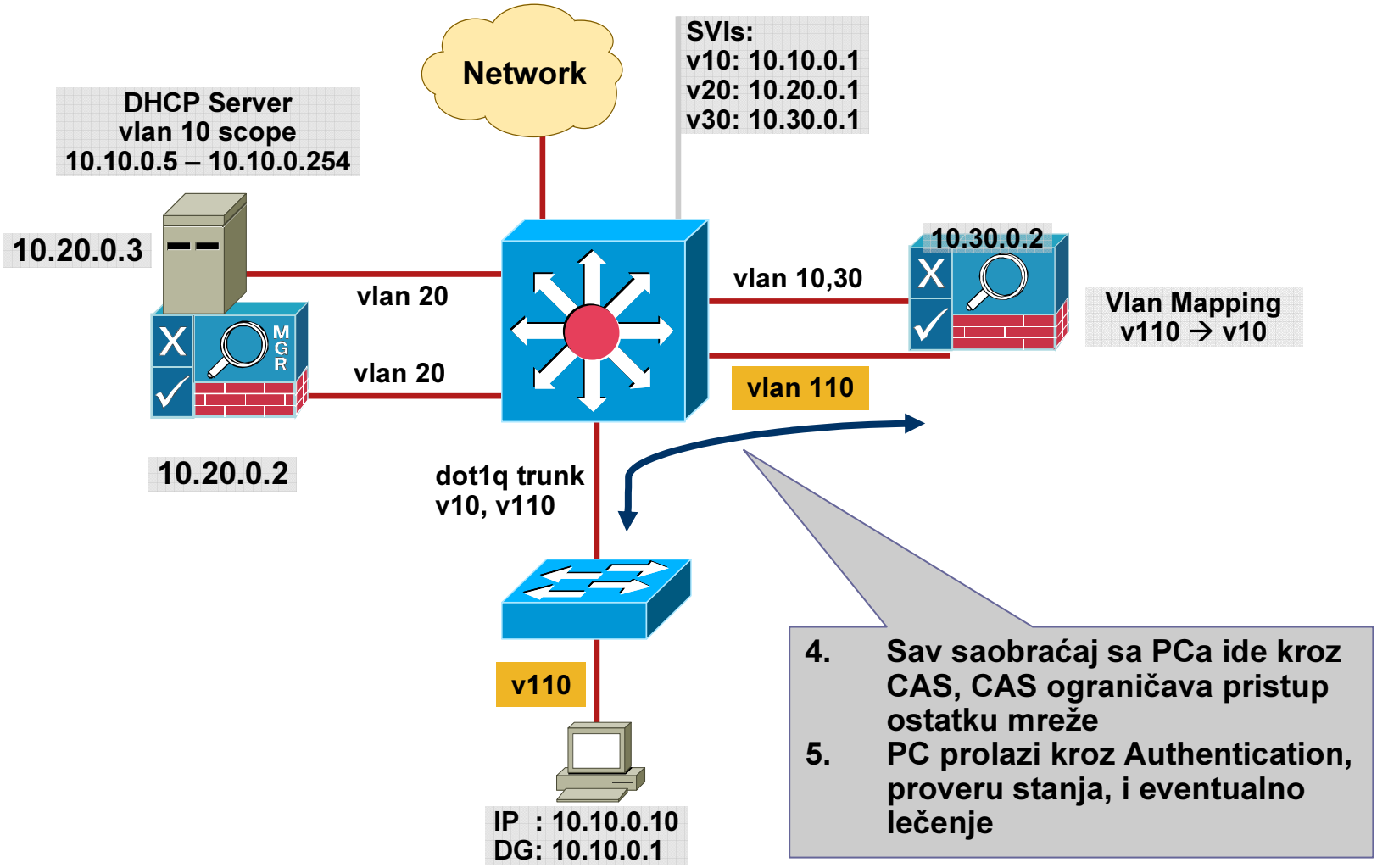
Tok procesa



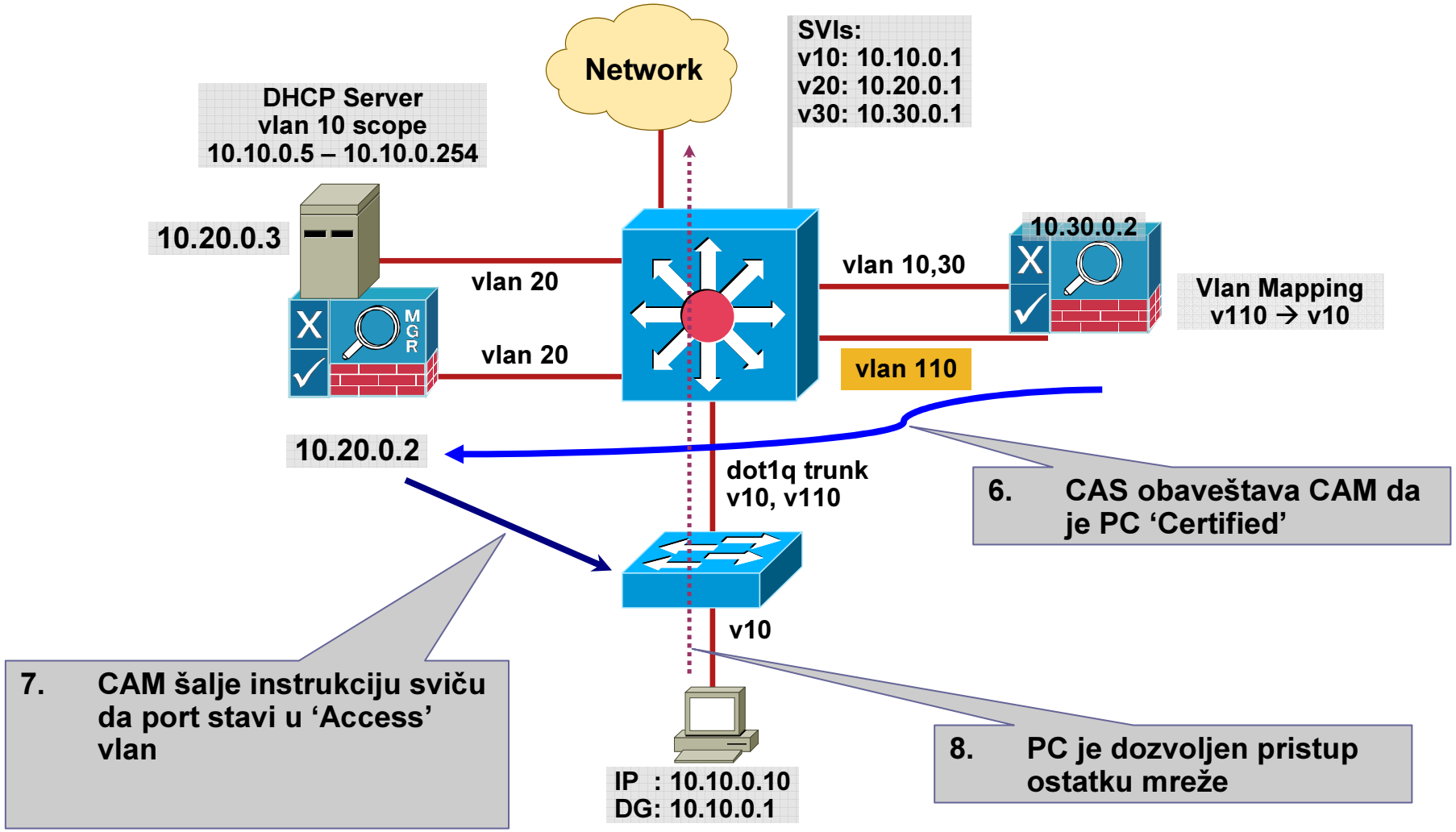
Tok procesa



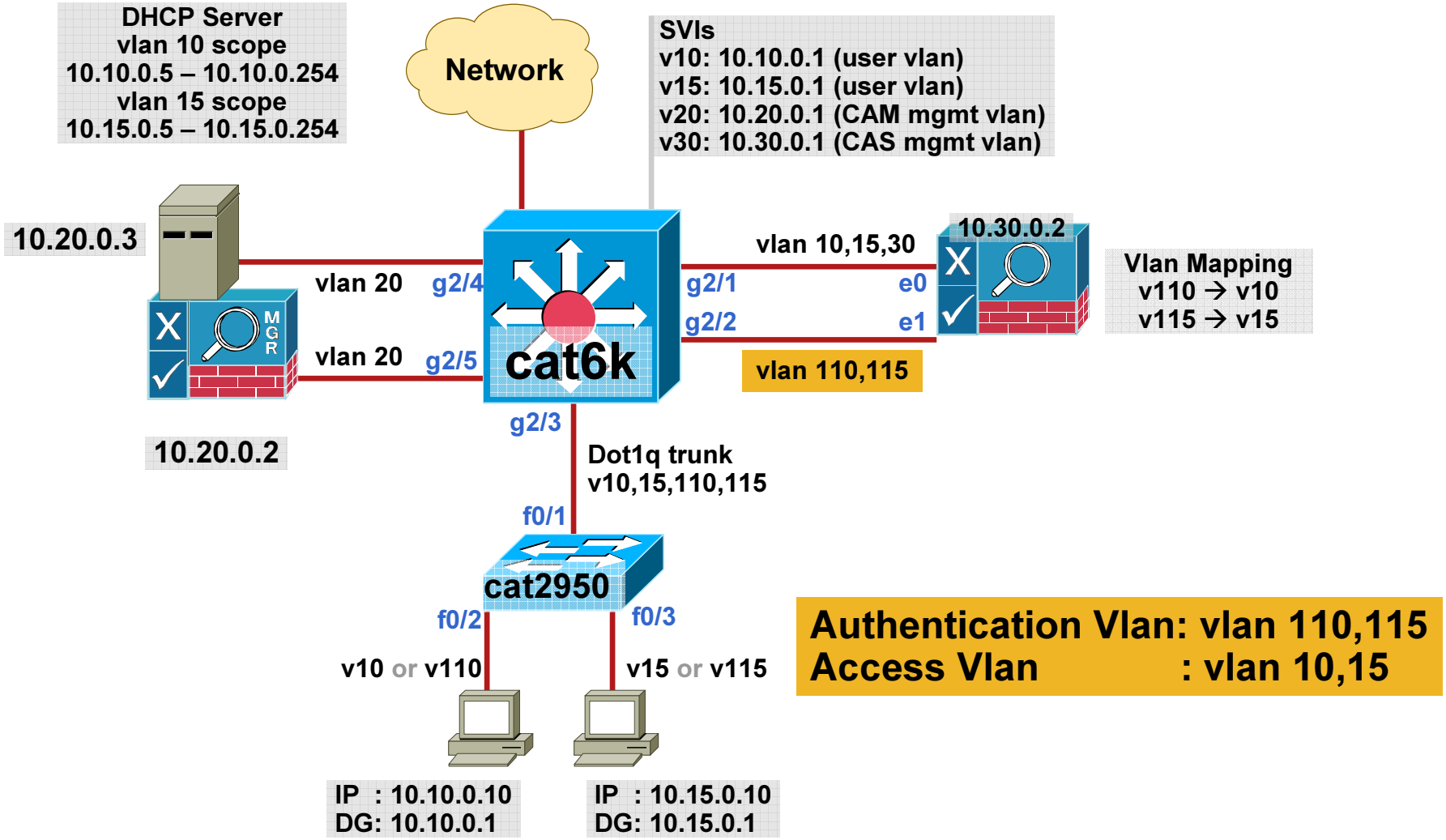
Tok procesa



Tok procesa



Topologija



Planiranje L2 Virtual Gateway OOB implementacije

- Staviti CAS i CAM u različite subnete
- Staviti CAS mgmt VLAN u različit VLAN od user VLANa
- Konfigurisati native VLAN različit od CAS mgmt VLANa
- Osigurati se da nema zajedničkih VLANova na switchport-ovima na kojima su vezani trusted (eth0) i untrusted (eth1) portovi CAS
- Za svaki VLAN koji je dozvoljen na trunku ka CAS, mora postojati odgovarajuće Vlan Mapiranje (osim za CAS mgmt VLAN)

Planiranje L2 Virtual Gateway OOB implementacije

- L3 Svič ne sme da ima SVI za Authentication VLANove (samo za access VLANove)
- Authentication VLANovi samo na CAS untrusted linku,
- Untrusted interface (eth1) na CAS ne sme biti priključen na svič dok se ne konfiguše VLAN mapiranje

Planiranje L2 Virtual Gateway OOB implementacije

CAM mgmt vlan	Vlan 20
CAS mgmt vlan	Vlan 30
User Access vlan User Auth vlan	Vlan 10, 15 Vlan 110, 115
Vlan mapiranje	V110 →V10 V115 →V15
Dummy Native vlan za Trusted port link Dummy Native vlan za Untrusted port link	Vlan 998 Vlan 999

Konfiguracije svičeva

Konfiguracija centralnog sviča

```
interface gig2/1 (Trusted)
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk native vlan 998
    switchport trunk allowed vlan 10,15,30

interface gig 2/2 (Untrusted)
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk native vlan 999
    switchport trunk allowed vlan 110,115

interface gig2/3 (link to access switch)
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan 10,15,110,115

interface gig 2/4 (dhcp server)
    switchport
    switchport mode access
    switchport access vlan 20
    spanning-tree portfast
```

```
interface gig 2/5 (CAM)
    switchport
    switchport mode access
    switchport access vlan 20
    spanning-tree portfast

interface vlan 10
    ip address 10.10.0.1 255.255.255.0
    ip helper-address 10.20.0.3

interface vlan 15
    ip address 10.15.0.1 255.255.255.0
    ip helper-address 10.20.0.3

interface vlan 20
    ip address 10.20.0.1 255.255.255.0

interface vlan 30
    ip address 10.30.0.1 255.255.255.0
```

Napomena:

Nema interface vlan 110 ili 115 !!!

Konfiguracija access sviča

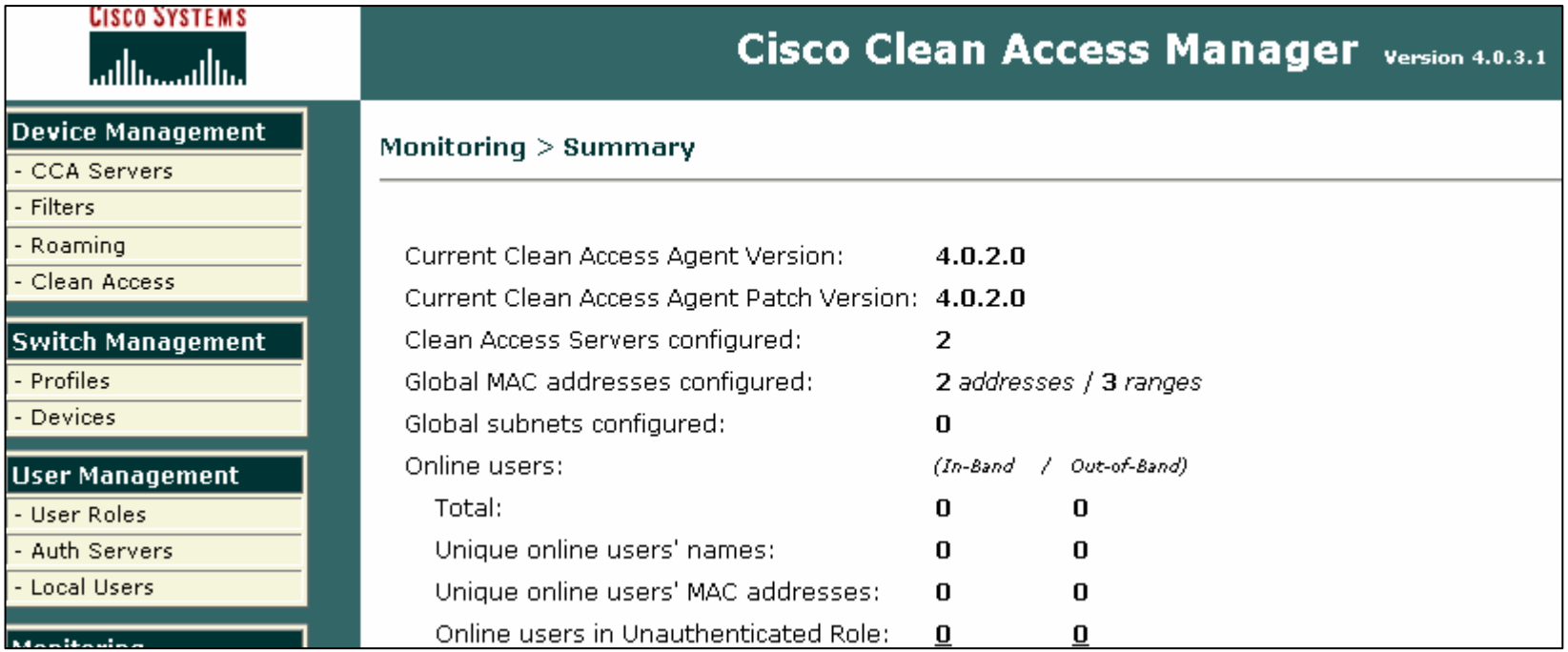
```
interface fa0/1 (Uplink to core)
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan 10,15,110,115

interface fa0/2 (User in vlan10)
    switchport
    switchport mode access
    switchport access vlan 10
    spanning-tree portfast

interface fa0/3 (User in vlan15)
    switchport
    switchport mode access
    switchport access vlan 15
    spanning-tree portfast
```

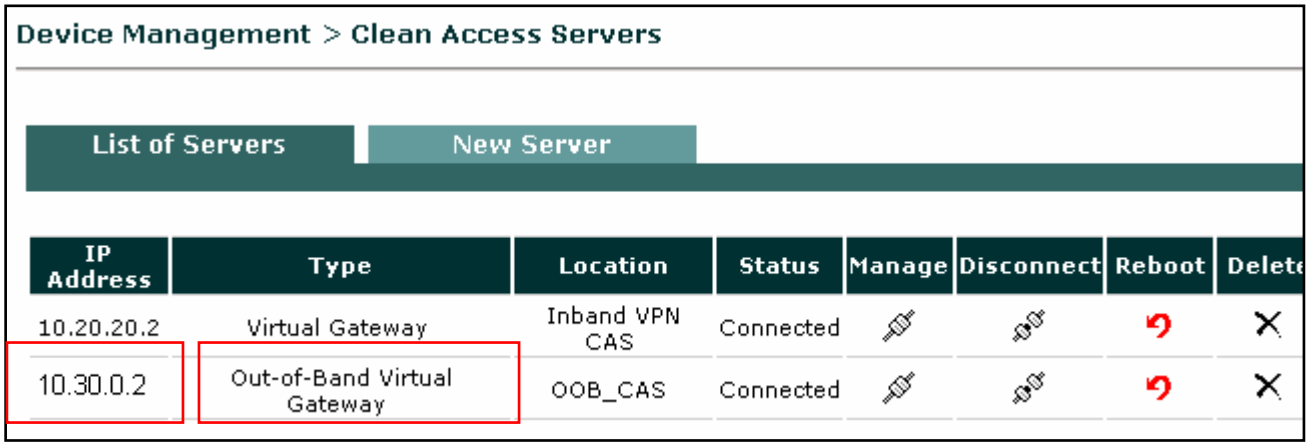
Povezivanje CAM

- Povezati CAM na centralni svič
- Obezbediti pristup Web GUI interfejsu CAM



Povezivanje CAS

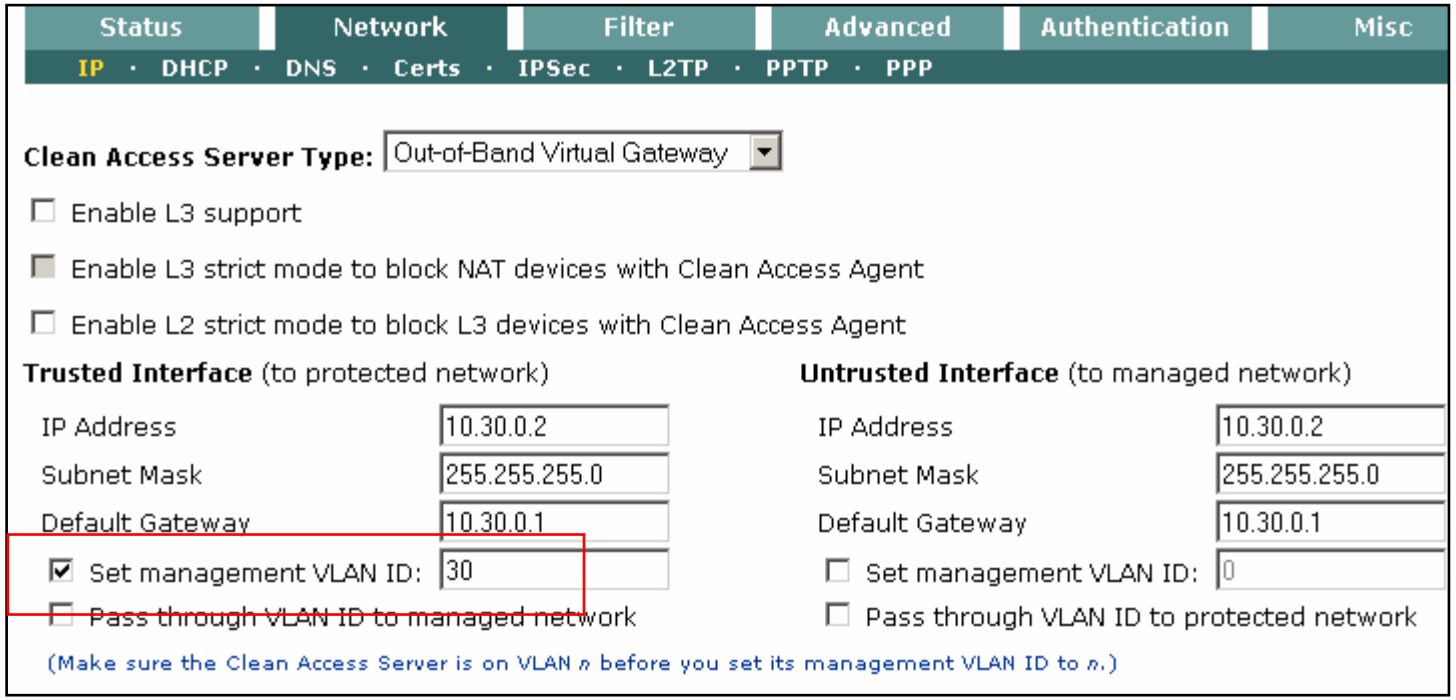
- Povezati samo eth0 (Trusted) interfejs CAS
- eth1 (untrusted) interfejs CAS ne treba povezivati
- Dodati CAS na CAM



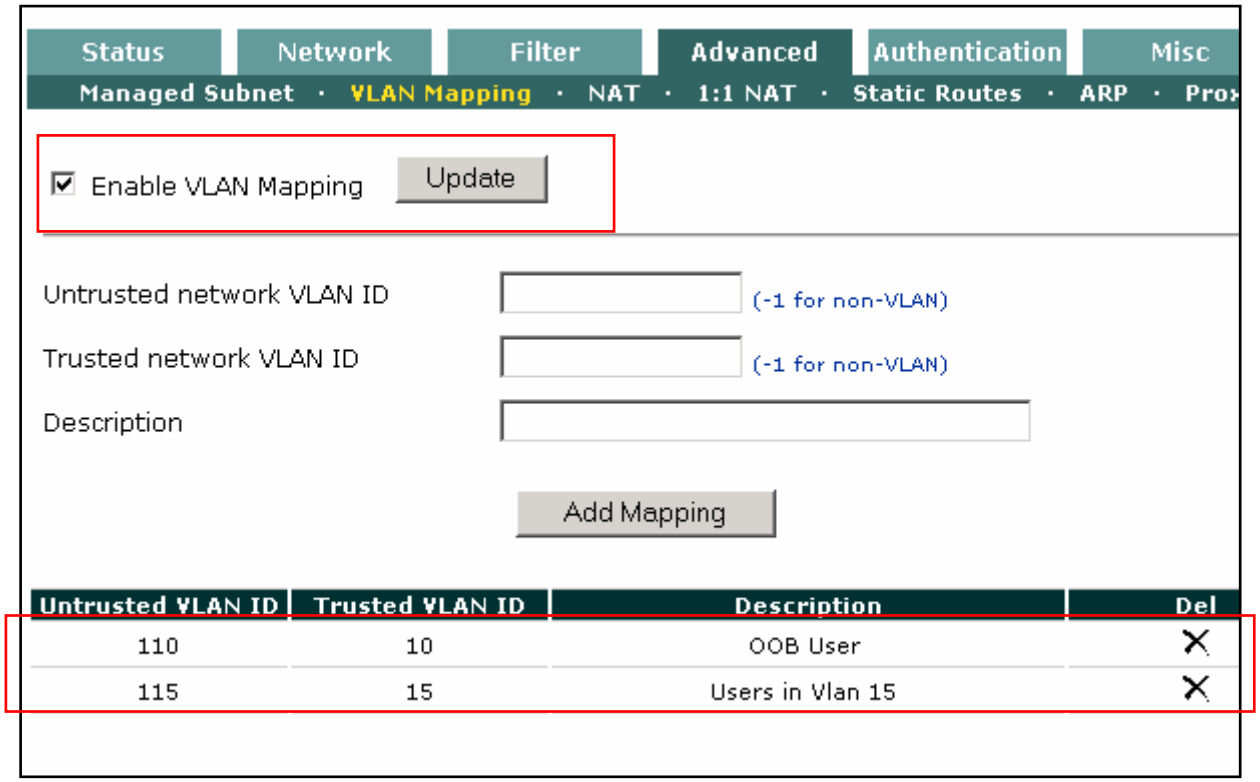
CAS podešavanja

- Management Vlan ID:

  Ako je enable-ovan, saobraćaj koji inicira CAS će biti tagovan sa vlan30



Konfiguracija VLAN mapiranja



Konfiguracija SNMP na sviču

- 2950 config for snmp v1

  snmp-server location cca_lab

  snmp-server contact chupa

  snmp-server community c2950_read ro

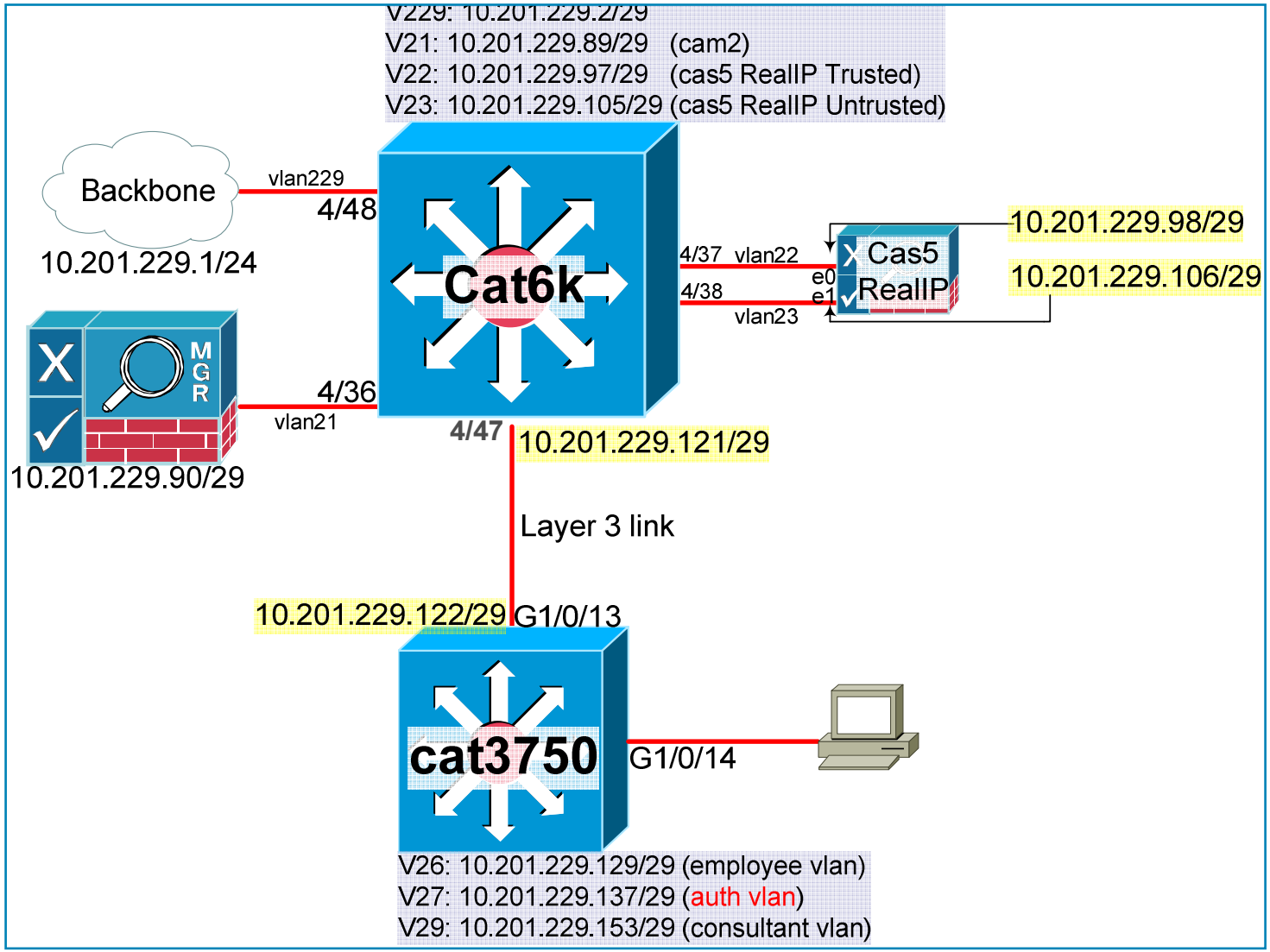
  snmp-server community c2950_write rw

  snmp-server enable traps mac-notification

  snmp-server enable traps snmp linkup linkdown

  snmp-server host 10.20.0.2 traps version 1 public mac-notification snmp

Layer 3 OOB Real-IP - Topologija



Layer 3 OOB korišćenjem Policy Based Routing-a

- Kad je korisnik u Auth VLAN, njegov saobraćaj treba da ide kroz CAS
- Na Layer 3 Access switch

  konfigurisati PBR na Auth VLAN SVI da pokazuje na next hop na distribution sviču

  PBR ne treba konfigurisati za user VLANove
- Access switch config

Match Interesting traffic

```
access-list 1 permit any
```

Configure Route map

```
route-map cas5 permit 10
match ip address 1
set ip next-hop 10.201.229.121
```

Apply Policy Route to Interface

```
interface VLAN27
 ip address 10.201.229.137 255.255.255.248
 ip policy route-map cas5
```

Layer 3 OOB korišćenjem Policy Based Routing

- Na Distribution sviču

  Konfigurisati PBR na dolazećem interfejsu za slanje saobraćaja iz Auth VLAN na Untrusted port CAS

  Saobraćaj sa user VLANa neće odgovarati route mapi pa će se normalno rutirati

- Distribution switch config:

Match Interesting traffic

```
access-list 101 permit ip 10.201.229.136 0.0.0.7 any
```

Configure Route map

```
route-map cca1 permit 10
  match ip address 101
  set ip next-hop
10.201.229.106
```

Apply Policy Route to Interface

```
interface FastEthernet4/47
 ip address 10.201.229.121 255.255.255.248
 ip policy route-map cca1
```

Layer 3 OOB korišćenjem PBR
Detaljne konfiguracije svičeva

```
cat6k# show run
vtp domain cca_40_testing
vtp mode transparent
!
VLAN 21,22,23,229
!
interface FastEthernet4/36
 switchport
 switchport access VLAN 21
 switchport mode access
 no ip address
!
interface FastEthernet4/37
 switchport
 switchport access VLAN 22
 switchport mode access
 no ip address
!
interface FastEthernet4/38
 switchport
 switchport access VLAN 23
 switchport mode access
 no ip address
!
interface FastEthernet4/47
 ip address 10.201.229.121255.255.255.248
 ip policy route-map cca1
!
interface FastEthernet4/48
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 229
 switchport mode trunk
 no ip address
```

```
interface VLAN21
 ip address 10.201.229.89 255.255.255.248
!
interface VLAN22
 ip address 10.201.229.97 255.255.255.248
!
interface VLAN23
 ip address 10.201.229.105 255.255.255.248
!
interface VLAN229
 ip address 10.201.229.2 255.255.255.248
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.201.229.1
ip route 10.201.229.128 255.255.255.248 10.201.229.122
ip route 10.201.229.136 255.255.255.248 10.201.229.122
ip route 10.201.229.152 255.255.255.248 10.201.229.122
!
access-list 101 permit ip 10.201.229.136 0.0.0.7 any
!
route-map cca1 permit 10
 match ip address 101
 set ip next-hop 10.201.229.106
!
snmp-server community public RW
snmp-server community c6500_read RO
snmp-server location ccalab
snmp-server contact Alok
snmp-server enable traps snmp linkdown linkup
snmp-server host 10.201.229.90 public  MAC-Notification snmp
!
end
```

Layer 3 OOB korišćenjem PBR
Detaljne konfiguracije svičeva

```
3750# show  run
!
vtp domain cca_40_testing
vtp mode transparent
ip dhcp excluded-address 10.201.229.129
ip dhcp excluded-address 10.201.229.137
ip dhcp excluded-address 10.201.229.153
!
ip dhcp pool VLAN26
   network 10.201.229.128 255.255.255.248
   default-router 10.201.229.129
   dns-server 171.70.168.183
!
ip dhcp pool VLAN27
   network 10.201.229.136 255.255.255.248
   default-router 10.201.229.137
   dns-server 171.70.168.183
!
ip dhcp pool VLAN29
   network 10.201.229.152 255.255.255.248
   default-router 10.201.229.153
!
VLAN 26
 name employee
!
VLAN 27
 name auth_VLAN
!
VLAN 29
 name consultant
!
interface GigabitEthernet1/0/13
 no switchport
 ip address 10.201.229.122 255.255.255.248
```

```
interface GigabitEthernet1/0/14
 switchport access VLAN 26
 switchport mode access
 snmp trap mac-notification added
 spanning-tree portfast
!
interface VLAN26
 ip address 10.201.229.129 255.255.255.248
!
interface VLAN27
 ip address 10.201.229.137 255.255.255.248
 ip policy route-map cas5
!
interface VLAN29
 ip address 10.201.229.153 255.255.255.248
!
ip route 0.0.0.0 0.0.0.0 10.201.229.121
!
access-list 1 permit any
route-map cas5 permit 10
 match ip address 1
 set ip next-hop 10.201.229.121
!
snmp-server community 3750_read RO
snmp-server community 3750_write RW
snmp-server location ccalab
snmp-server contact alok
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification
snmp-server host 10.201.229.90 public  mac-notification snmp
!
mac-address-table notification interval 0
mac-address-table notification
end
```

Zaključci

1	Virtual Gateway mod je najčešće najjednostavnije rešenje za integraciju sa postojećom mrežom
2	Centralna implementacija u 99% LAN slučajeva
3	Layer 2 / Layer 3 povezani klijenti u zavisnosti od toga kako su povezani sa CAS
4	Ukolko su potrebne različite implementacije – više CAS servera ..

Mrežni dizajn

Generalne smernice za izbor dizajna:

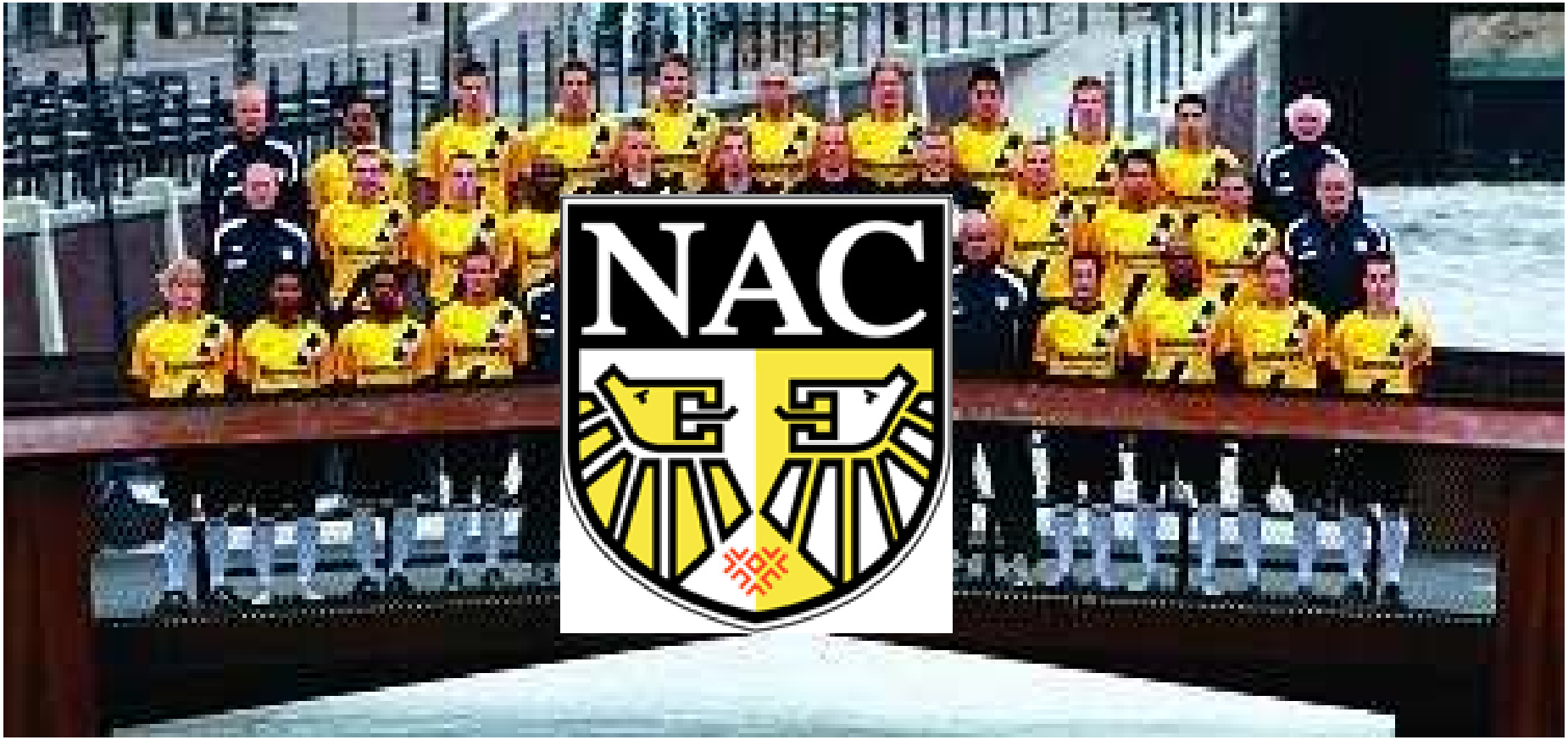
- Početi sa L2 IB VGW Central
- Preći na Real IP Gateway ako želimo /30
- Preći na Out of Band ako je potrebno više bandwidth-a
- Preći na L3 ako ne može da se odredi MAC adresa

- Što jednostavnija implementacija – jednostavnije održavanje i konfigurisanje !

Agenda

- Šta je to NAC ?
- Komponente
- Pregled
- Dizajn i implementacija
- Pitanja i KVIZ !

- KVIZ !



- Kakva veza postoji između fudbalera na slici i Cisco NAC appliance?

Ne zaboravite da se prijavite na Cisco Networkers 2008!

http://www.cisco.com/web/europe/cisco-networkers/2008/index.html