conf t: Zaštita mreže na L2 nivou

Dragan Novaković - Cisco Srbija

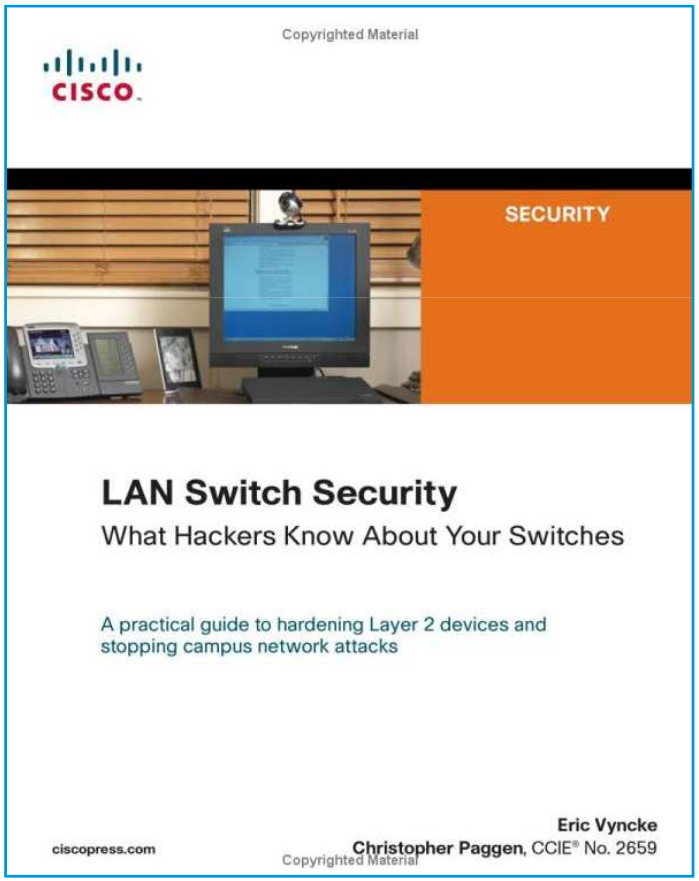
CCIE #26951

Agenda

- Pregled Layer 2 napada
- Napadi i kontramere
  - MAC napadi
  - VLAN Hopping
  - DHCP napadi
  - ARP napadi
  - Spoofing napadi
  - Napadi na druge LAN protocols
- Zaključak

Preporučeno za čitanje

- LAN Switch Security:
  What Hackers Know About Your Switches



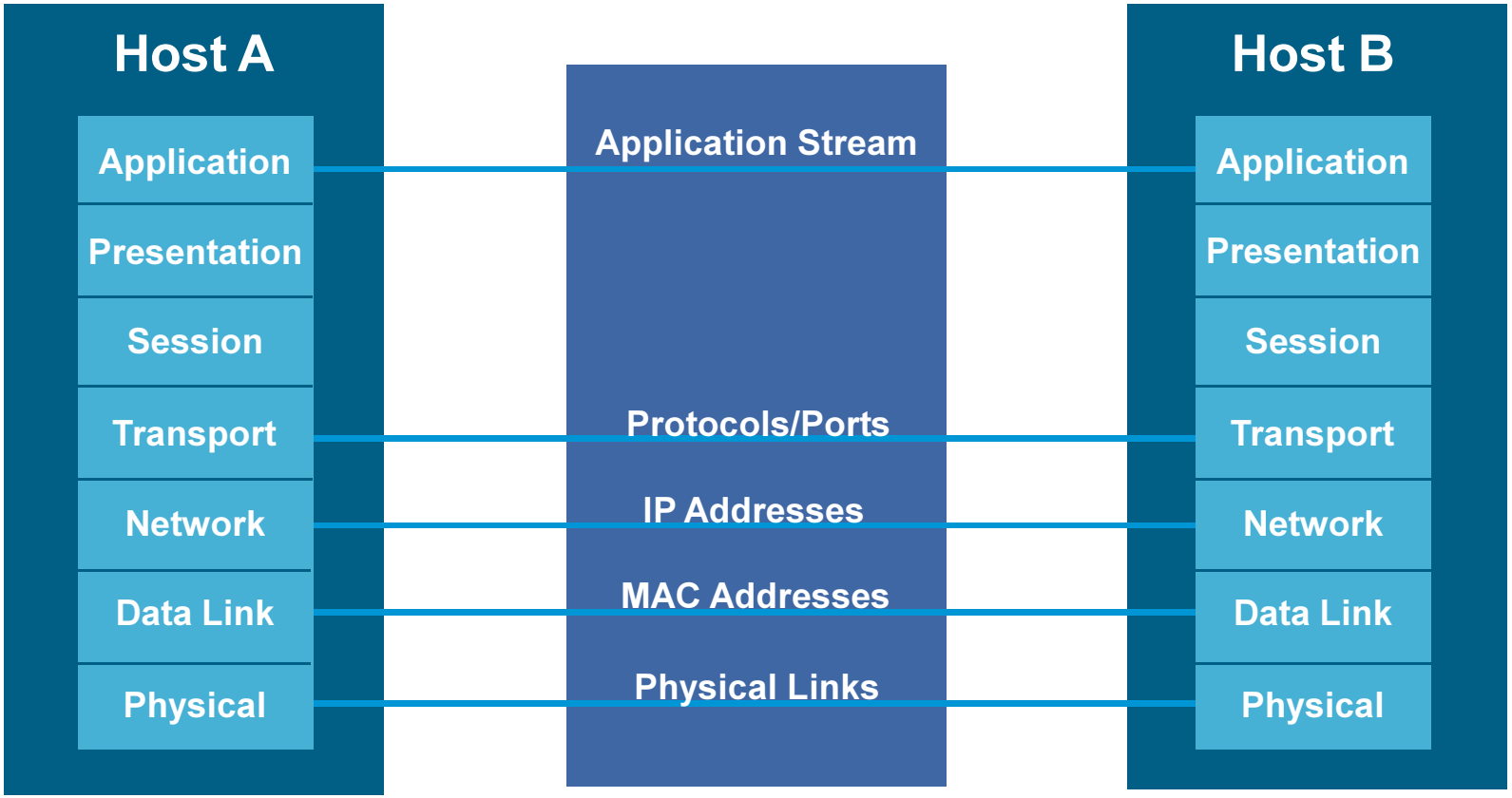
Nagradno pitanje?

Agenda

- Pregled Layer 2 napada
- Napadi i kontramere
  - MAC napadi
  - VLAN Hopping
  - DHCP napadi
  - ARP napadi
  - Spoofing napadi
  - Napadi na druge LAN protocols
- Zaključak

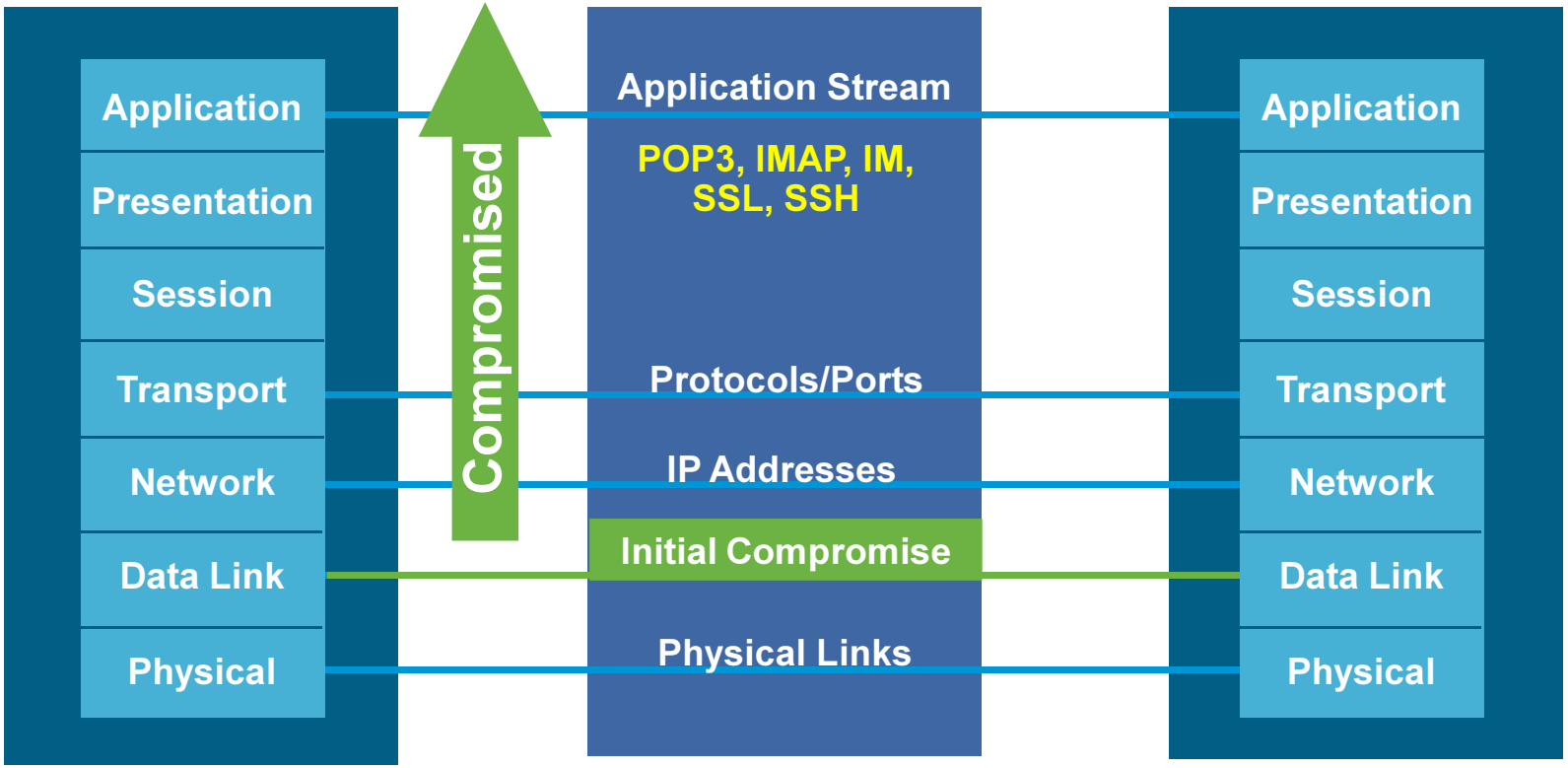
Zašto uopšte brinuti o Layer 2 bezbednosti?

OSI je zamišljen da dozvoli rad različitim slojevima bez znanja o tome šta je u drugim slojevima



Niži slojevi utiču na više slojeve

- Na žalost, to znači i da ako se jedan sloj hakuje, komunikacija na svim višim slojevima je kompromitovana bez njihovog znanja
- Bezbednost je dobra koliko i njen najslabiji link, a Sloj 2 je najčešće najslabiji ☹



FBI/CSI procena rizika*

- Mnoge kompanijske mreže imaju otvorene portove
- Najčešći slučaj je da bilo koji laptop koji se nakači na mrežu će dobiti i sam pristup
- Tipični gubici po incidentu su 289K
- 23% ispitanika ne zna koliko i da li su uopšte bili izloženi napadima
- 23% ispitanika izjavilo da nisu bili izloženi napadima iznutra ?
- 80% svih napada su iznutra

*CIS/FBI Computer Crime and Security Survey—2009
http://www.gocsi.com/

Agenda

- Pregled Layer 2 napada
- Napadi i kontramere
  - MAC napadi
  - VLAN Hopping
  - DHCP napadi
  - ARP napadi
  - Spoofing napadi
  - Generalni napadi
- Zaključak

MAC/CAM Tabela - pregled

48-Bit Hexadecimal broj kreira jedinstvanu L2 adresu

1234.5678.9ABC

Prva 24-Bita = Manufacture Code dodeljuje IEEE

0000.0cXX.XXXX

Druga 24-Bita = Specific Interface, dodeljuje proizvođač

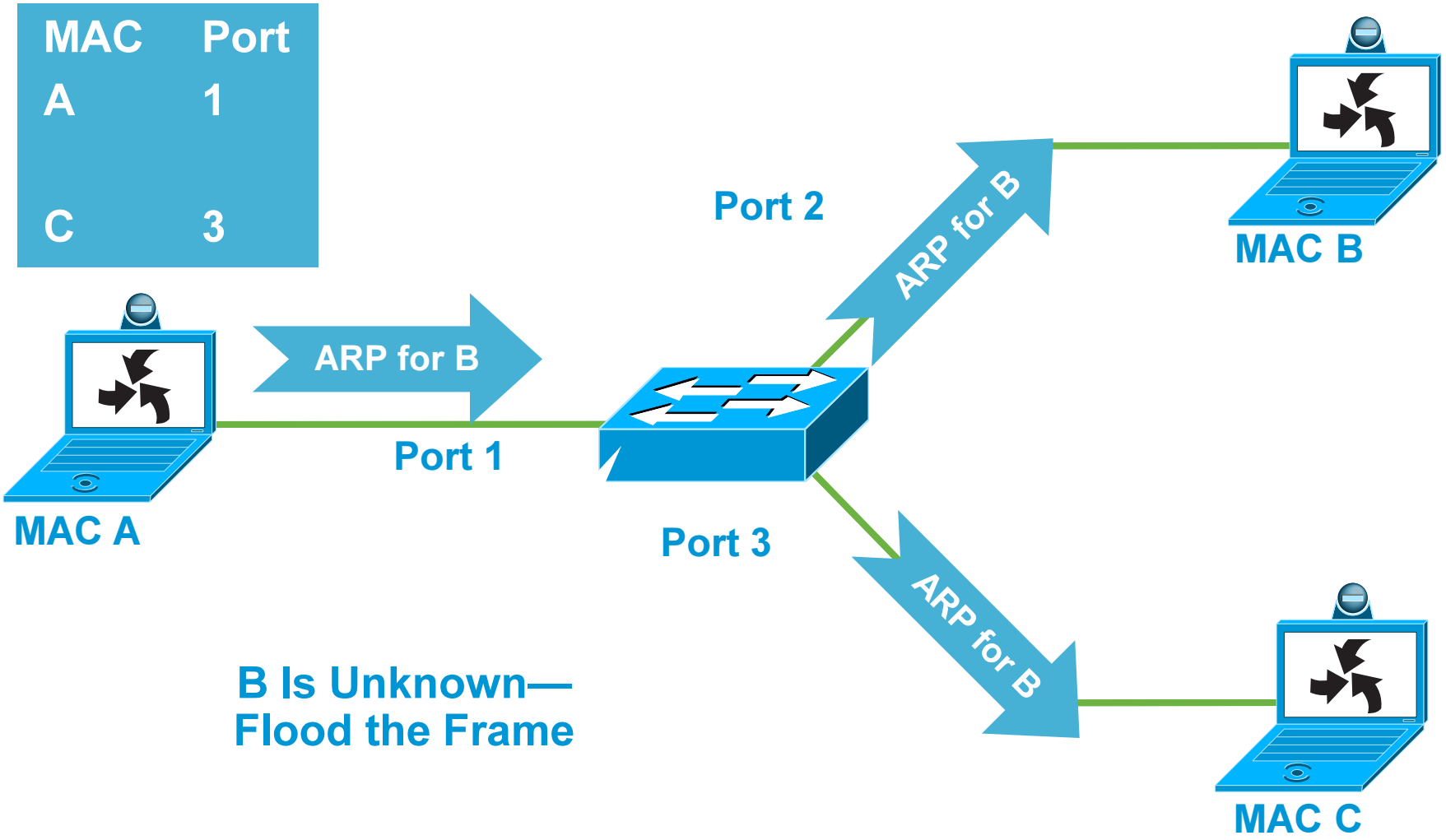
0000.0cXX.XXXX

sve F = Broadcast

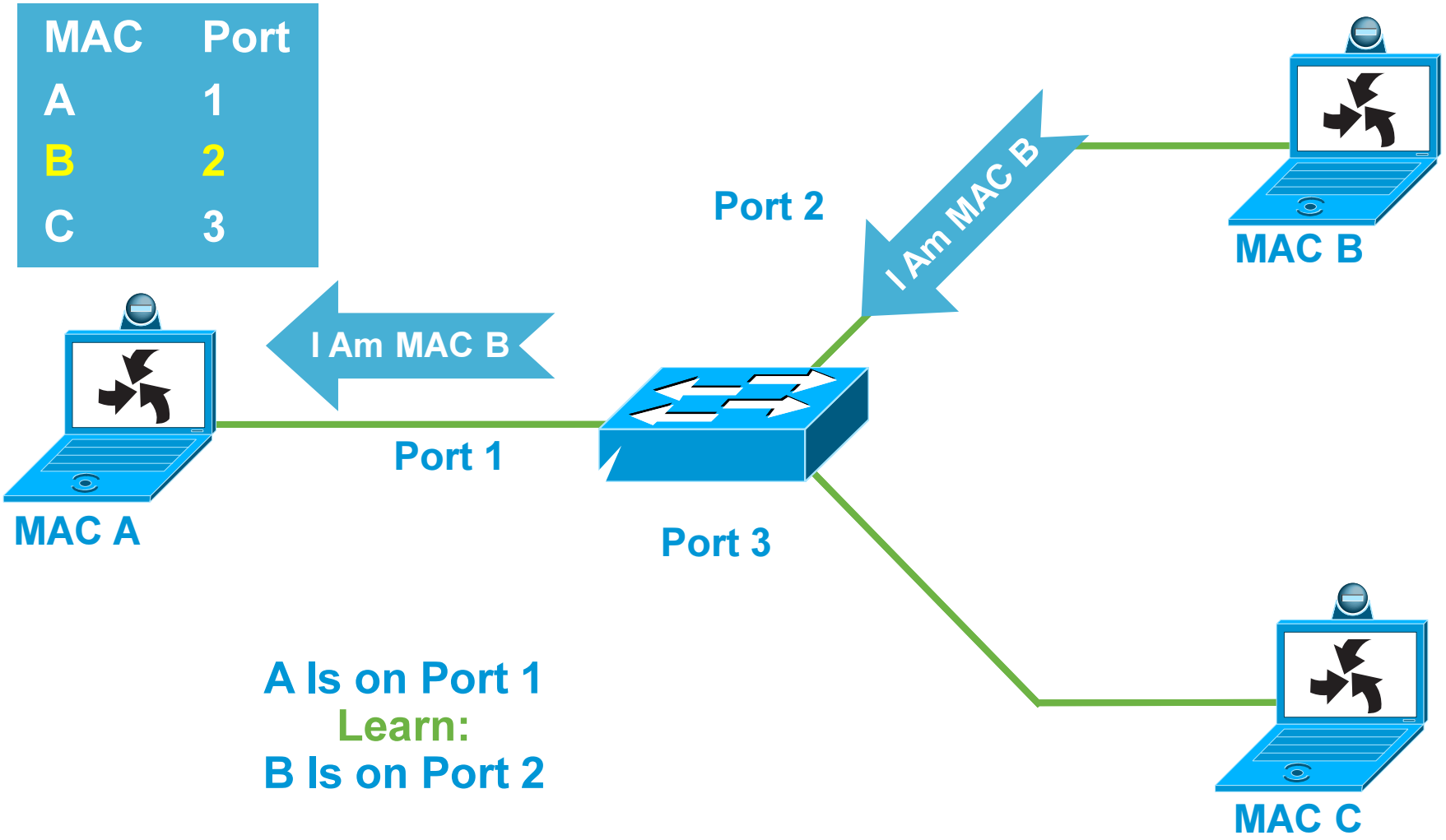
FFFF.FFFF.FFFF

- CAM tabela - Content Addressable Memory
- CAM tabela čuva informacije kao što su MAC adrese na fizičkim portovima i njihovi VLAN parametri
- Sve CAM tabele imaju fiksnu, ograničenu veličinu

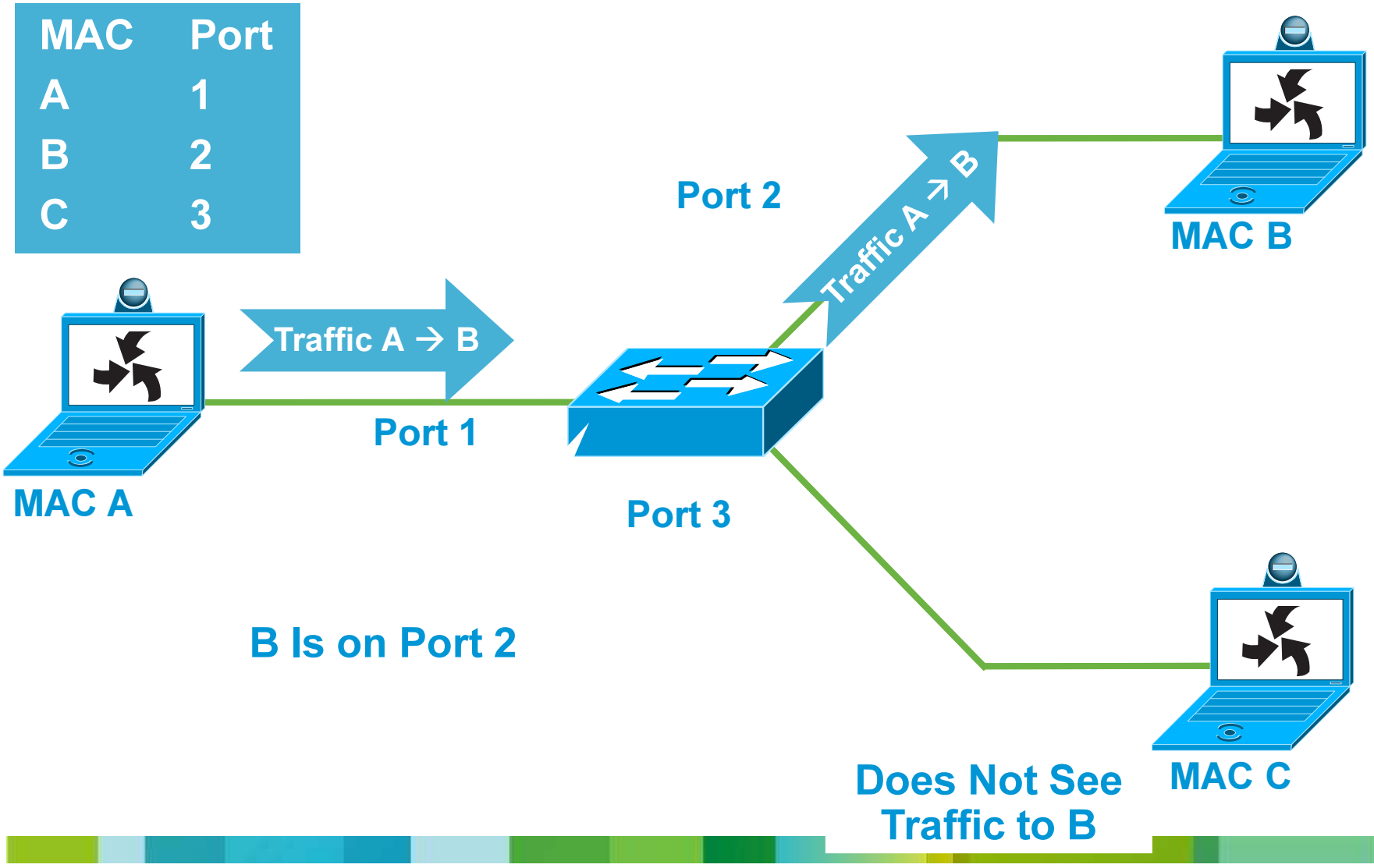
Normalno CAM ponašanje(1/3)



Normalno CAM ponašanje(2/3)



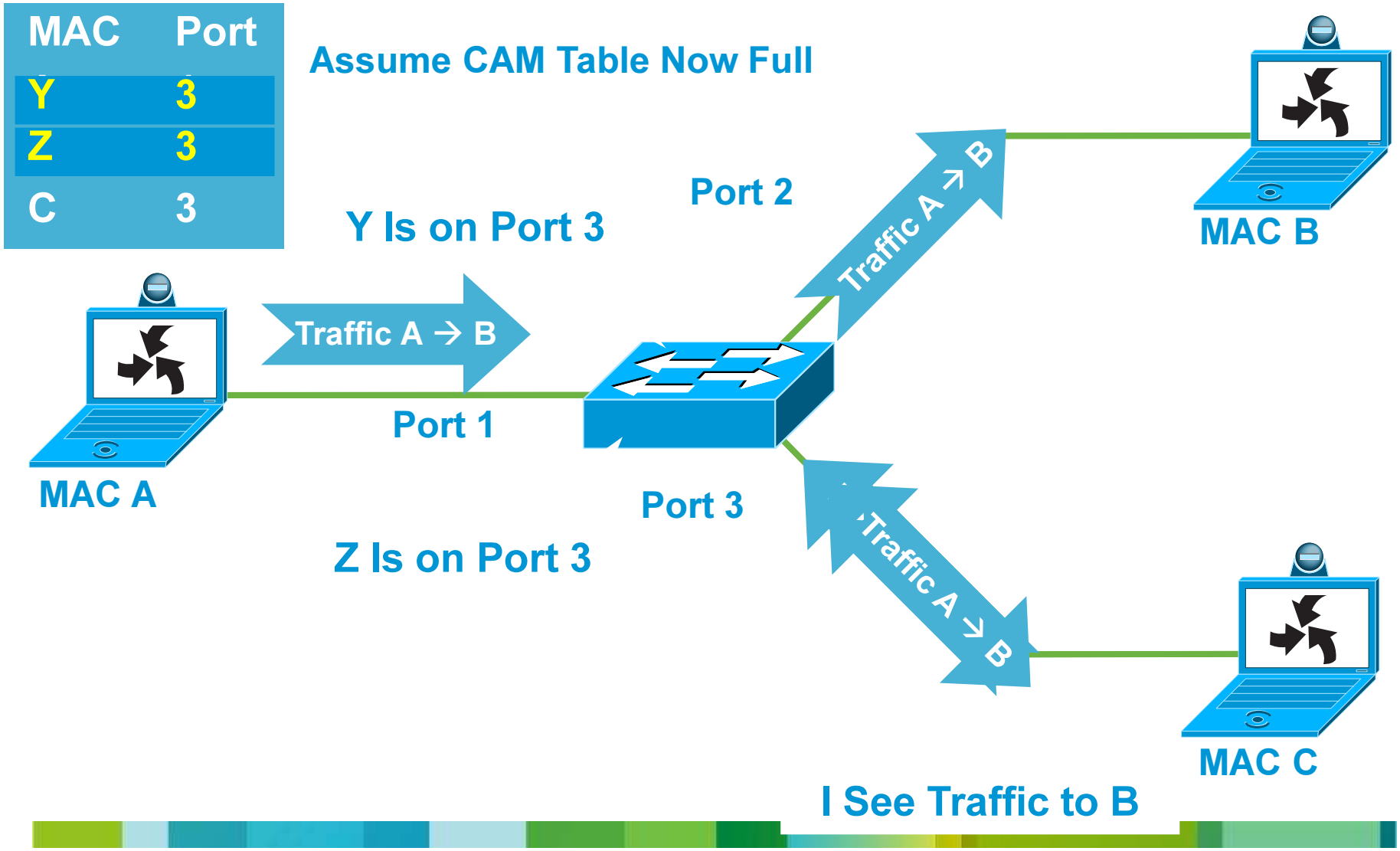
Normalno CAM ponašanje(3/3)



CAM Overflow—Tools (1/2)

- macof tool -1999
  - 100 linija u Perlu
  - Jedan od delova “dsniff”
- Napadi koji koriste ograničenu veličinu CAM tabela
- Yersinia: najveći i najbolji skup L2 napada

CAM Overflow (2/2)



Mac Flooding korišćenjem macof

```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

- Macof šalje random source MAC i IP adrese
- Mnogo agresivniji korišćenjem komande

  “macof -i eth1 2> /dev/null”

  macof (deo dsniff): http://monkey.org/~dugsong/dsniff/

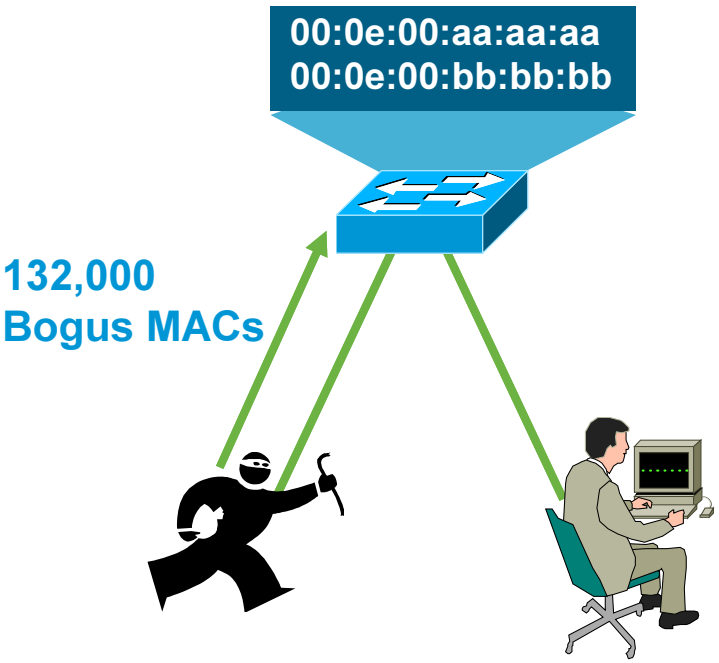
CAM Tabela je PUNA !

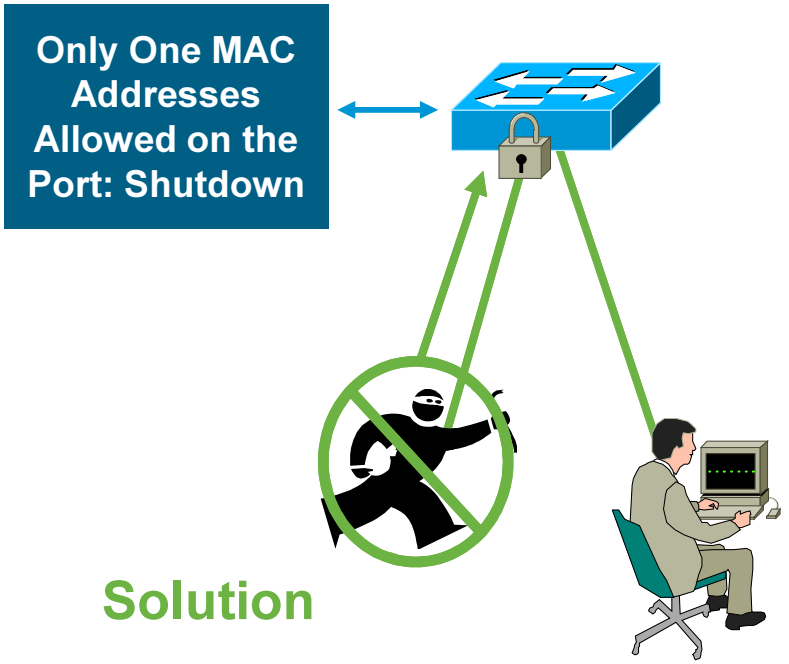
- Kada napunimo CAM tabelu sviča, sav saobraćaj se flood-uje na sve portove u tom VLANu
- Ovim pretvaramo svič u HUB !
- Ovaj napad će takođe preplaviti CAM tabele susednih svičeva

```
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.1, 10.1.1.1 ?
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.19, 10.1.1.19 ?
10.1.1.26 -> 10.1.1.25    ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS
10.1.1.25 -> 10.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```

Kontramere protiv MAC napada

Port Security ograničava broj MAC adresa na interfejsu



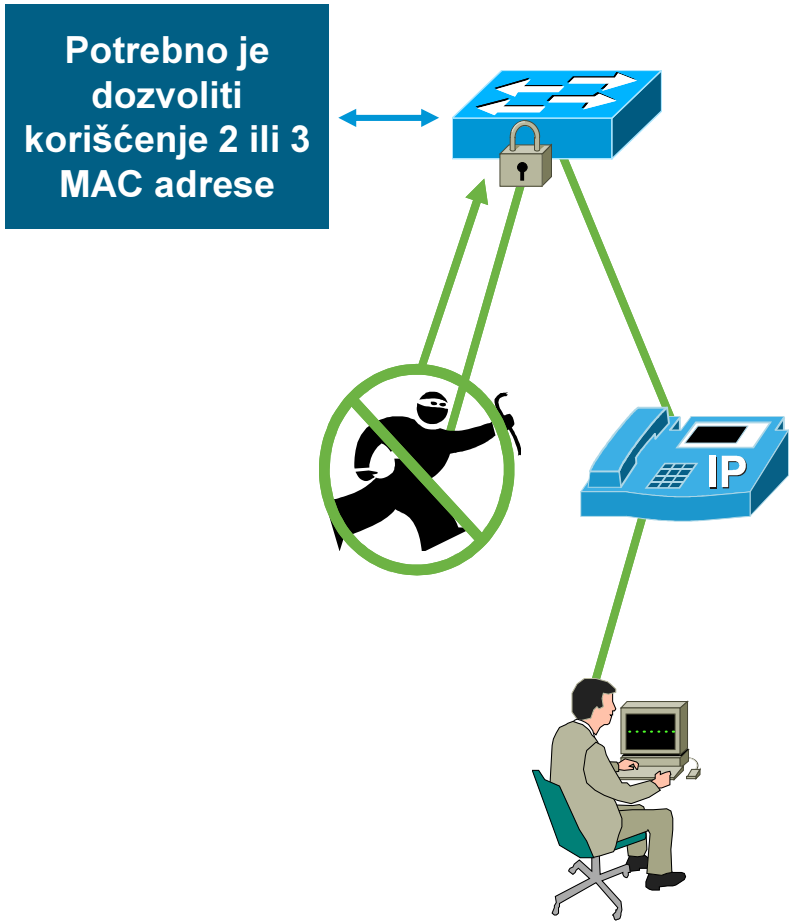


Solution

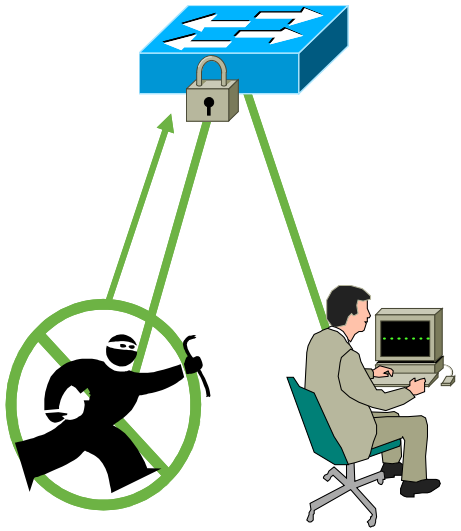
- Port Security sprečava MAC flooding napad, zaključava port i šalje SNMP trap

Kontramere protiv MAC napada sa IP telefonima

- IPT može da koristi dve ili tri adrese, u zavisnosti od hw i sw sviča
  - Neki svičevi broje-detektuju i CDP saobraćaj, neki ne, ako ne, potrebno 2 , ako da, 3 MAC adrese
  - Za neke svičeve (3550) uvek predvideti tri adrese
  - Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP)
- Default config je *disable* port, moguće samo *restrict* za VoIP



Port Security: Primer konfiguracije



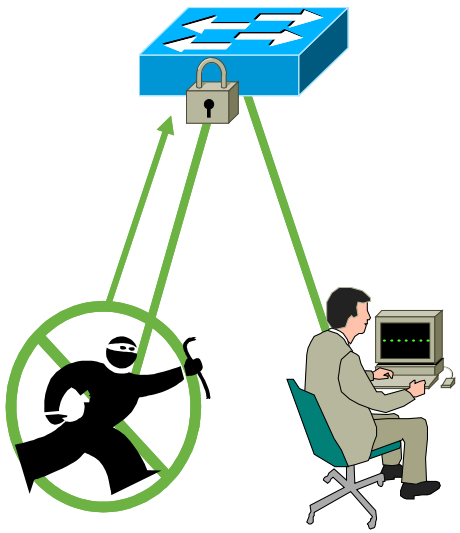
Omogućiće da radi Voice za vreme napada

```
Cisco Catalyst OS
set port security 5/1 enable
set port security 5/1 port max 3
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
Cisco IOS
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

- Cilj nije kontrola pristupa već sprečavanje i zaštita sviča od napada
- U zavisnosti od bezbednosne polise, *disable-ovanje* porta može biti preferirano

Violation error-disable log poruka: 4w6d: %PM-4-ERR_
DISABLE: Psecure-Violation Error Detected on Gi3/2, Putting Gi3/2 in Err-Disable State

Nova svojstva Port Security



Nove komande

```
Cisco IOS
switchport port-security
switchport port-security maximum 1 vlan voice
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
snmp-server enable traps port-security trap-rate 5
```

- Definisanje *Per port per VLAN* max broja MAC adresa
- *Restrict* akcija daje informaciju da se nešto desilo—šalje se SNMP trap
- “Sticky Port Security”; preživeće reboot

Port Security: Šta da očekujete?

Napomena: Kada je akcija *Restrict*, ako je svič pod napadom, može se videti pad performansi na CPU

- Pad performansi se pogotovo može videti u slučaju višestrukih napada-do 99% CPU zauzeća
- Telnet i management će i dalje biti dostupni
- Najbolje rešenje ograničiti SNMP poruke na razumnu meru
- Pomaže ako smo konfigurisali QoS
- Zamišljen za zaštitu sviča i limitiranje MAC adresa, nema autentikacije; za to je zadužen 802.1x
- Minimum podešavanja za IPT obično dva, nekad nije loše i nešto veći broj?

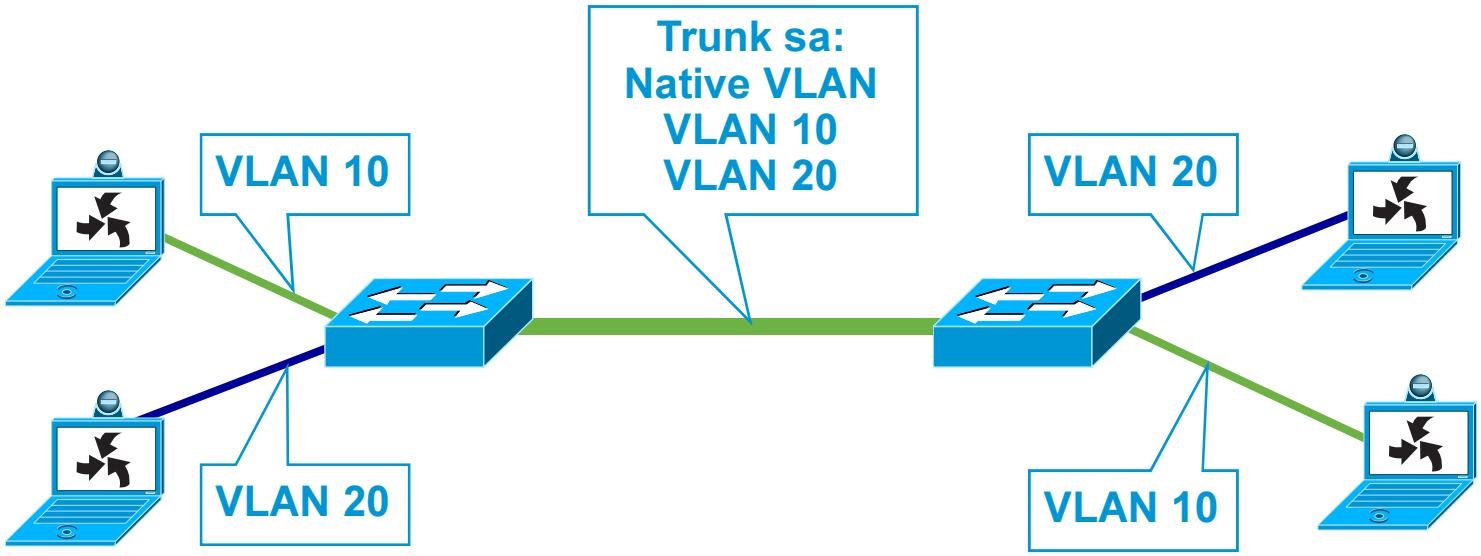
Izgradnja slojeva-piramide bezbednosti

- Port Security sprečava CAM napade(i neke DHCP napade)

Agenda

- Pregled Layer 2 napada
- Napadi i kontramere
  - MAC napadi
  - VLAN Hopping
  - DHCP napadi
  - ARP napadi
  - Spoofing napadi
  - Generalni napadi
- Zaključak

Basic Trunk Port definicija



- Trunk portovi imaju pristup do svih VLANova po default-u
- Koriste se da rutiraju saobraćaj za više VLANova preko istog fizičkog linka(generalno između svičeva ili telefona)
- Encapsulacija može biti 802.1q ili ISL

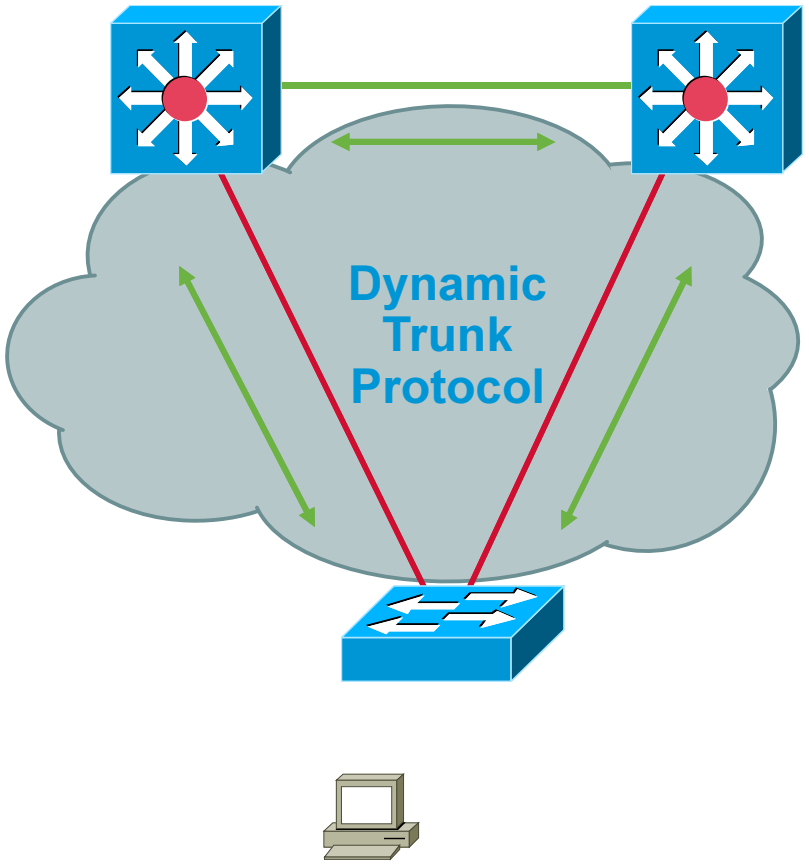
Dynamic Trunk Protocol (DTP)

- Šta je DTP?

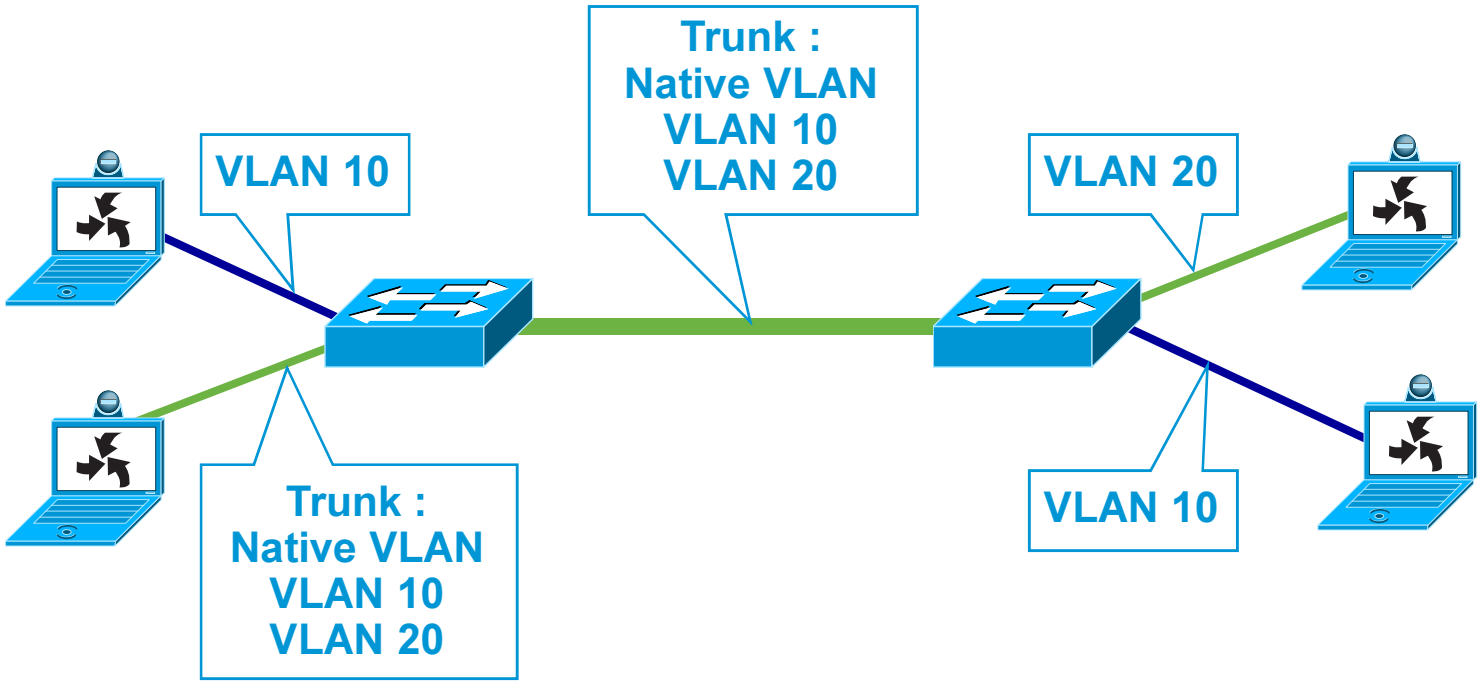
  Automatizuje 802.1q/ISL trunk konfiguraciju

  Radi između svičeva (Cisco IP phone je u suštini svič)

- DTP sinhronizuje trunking mode na linkovima
- DTP stanje na 802.1q/ISL trunking portovima može biti “Auto,” “On,” “Off,” “Desirable,” ili “Non-Negotiate”

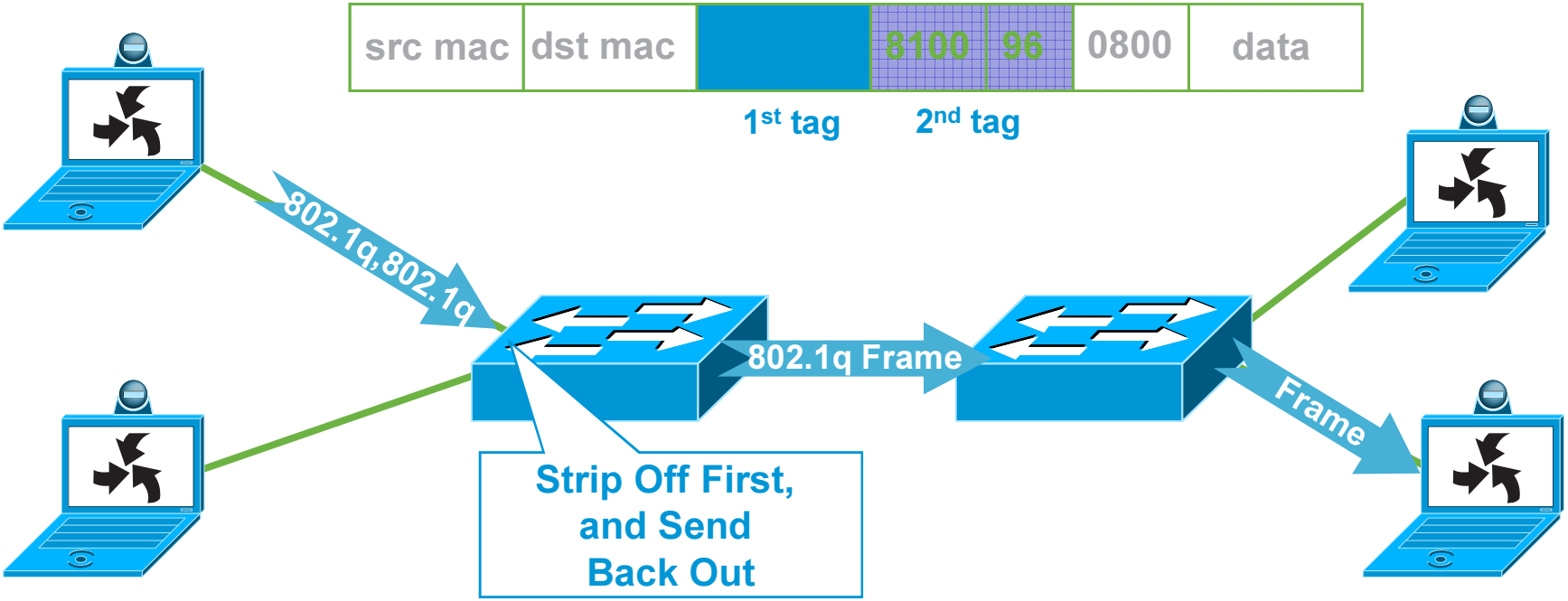


Osnovni VLAN Hopping napad



- Krajnja stanica može da se predstavi kao svič sa ISL ili 802.1q
- Krajnja stanica je tada član svih VLANova
- Zahteva trunking konfiguraciju sa native VLAN = VLAN 1

Double 802.1q Encapsulation VLAN Hopping napad

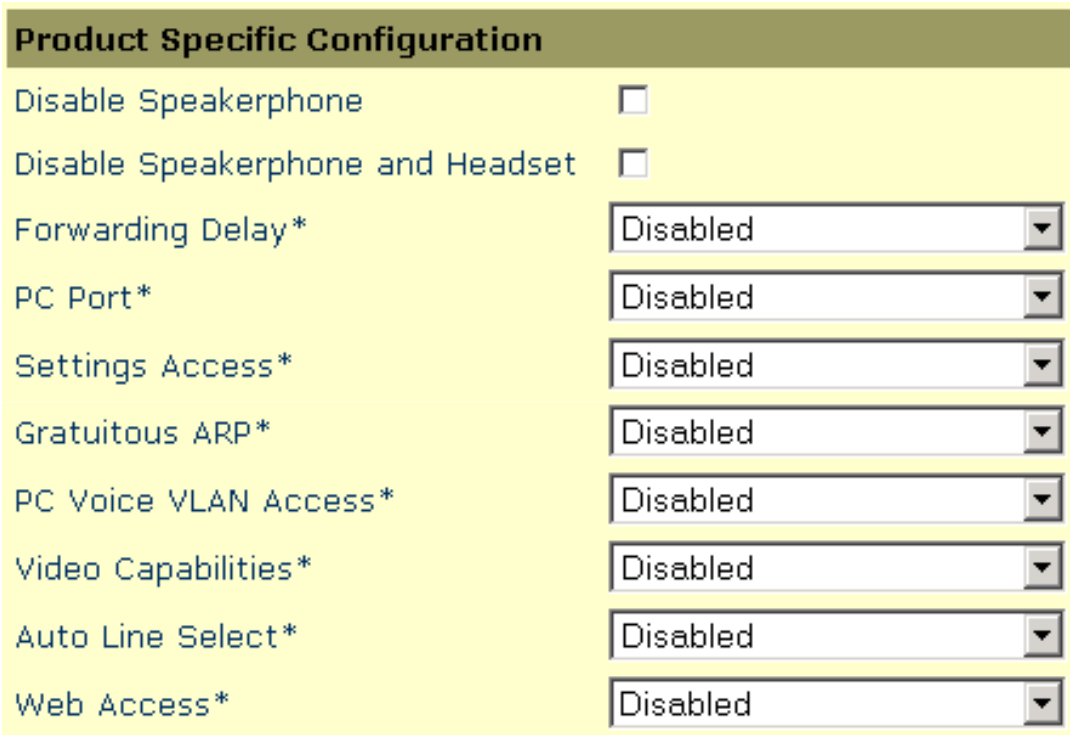


- Slanje 802.1q duplo enkapsuliranih frejmova
- Svič radi samo jedan nivo deenkapsulacije
- Unidirekcioni saobraćaj
- Radi čak iako je trunk port podešen na off

Note: Only works if trunk has the same VLAN as the attacker

IP Phones VLAN Security

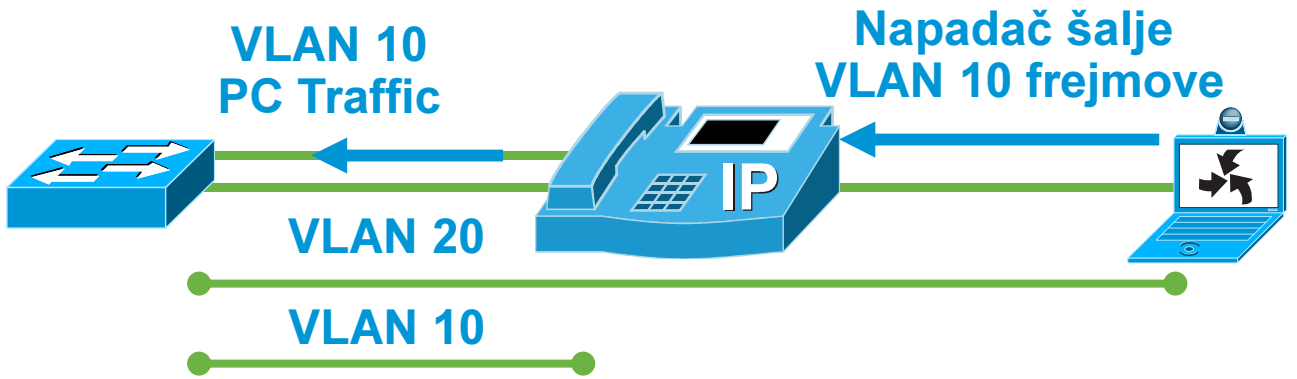
- Blokiranje voice VLAN sa PC porta
- Ignore Gratuitous ARPs (GARPs)



Voice VLAN

- Normalni VLAN način rada
  - VLAN 20 je native za PC i nije tagovan
  - VLAN 10 je voice VLAN, taguje se sa 10

Voice VLAN napad



- Napad na voice VLAN
  - Napadač šalje 802.1q tagovane frejmove sa PCa na telefon
  - Saobraćaj sa PCa je sada u voice VLANu

IP telefoni
PC Voice VLAN podešavanja

- Sprečavanje voice VLAN napada

  Tagovan saobraćaj na PC portu telefona će biti blokiran

- Razlike između modela telefona

  7940, 7960, 7941G, 7961G, i 7971G samo blokiraju voice VLAN, dozvoljavajući PC da radi 802.1Q na bilo kom drugom VLANu

  7970, 7961, i 7941 blokiraju sve pakete koji imaju 802.1Q header

  7912 ne blokira ništa

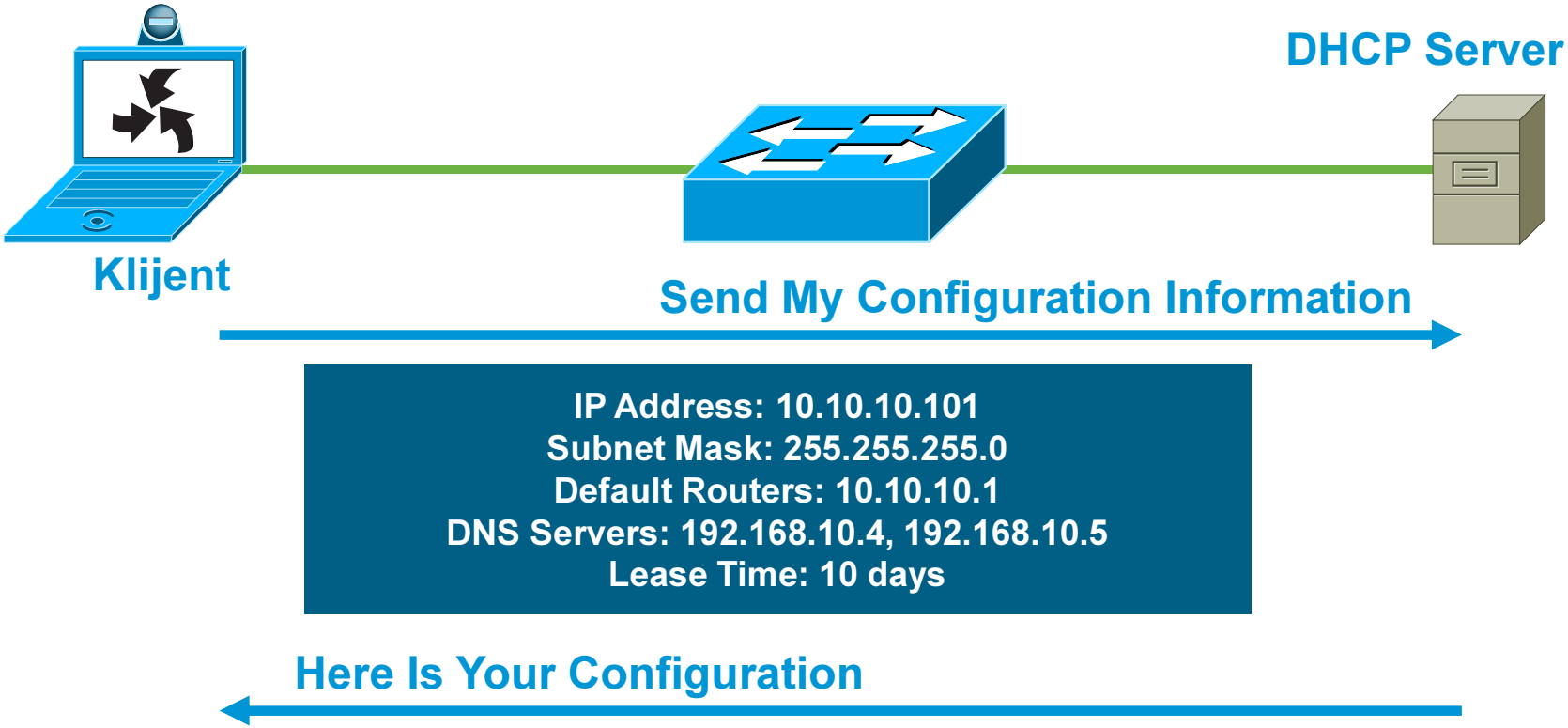
Security preporuke za VLANove i Trunking

- *Disable* portove koji se ne koriste i staviti ih u nekorišćeni VLAN
- Budite oprezni: ne koristiti VLAN 1
- *Disable* auto-trunking na *user facing* portovima (DTP off)
- Explicitno konfigurisati trunking na *infrastructure* portovima
- Koristiti *tagged mode* za native VLAN na trunkovima
- Koristiti PC voice VLAN *access* ograničenja ako ih telefon podržava
- Koristiti 802.1q tag na svim trunk portovima

Agenda

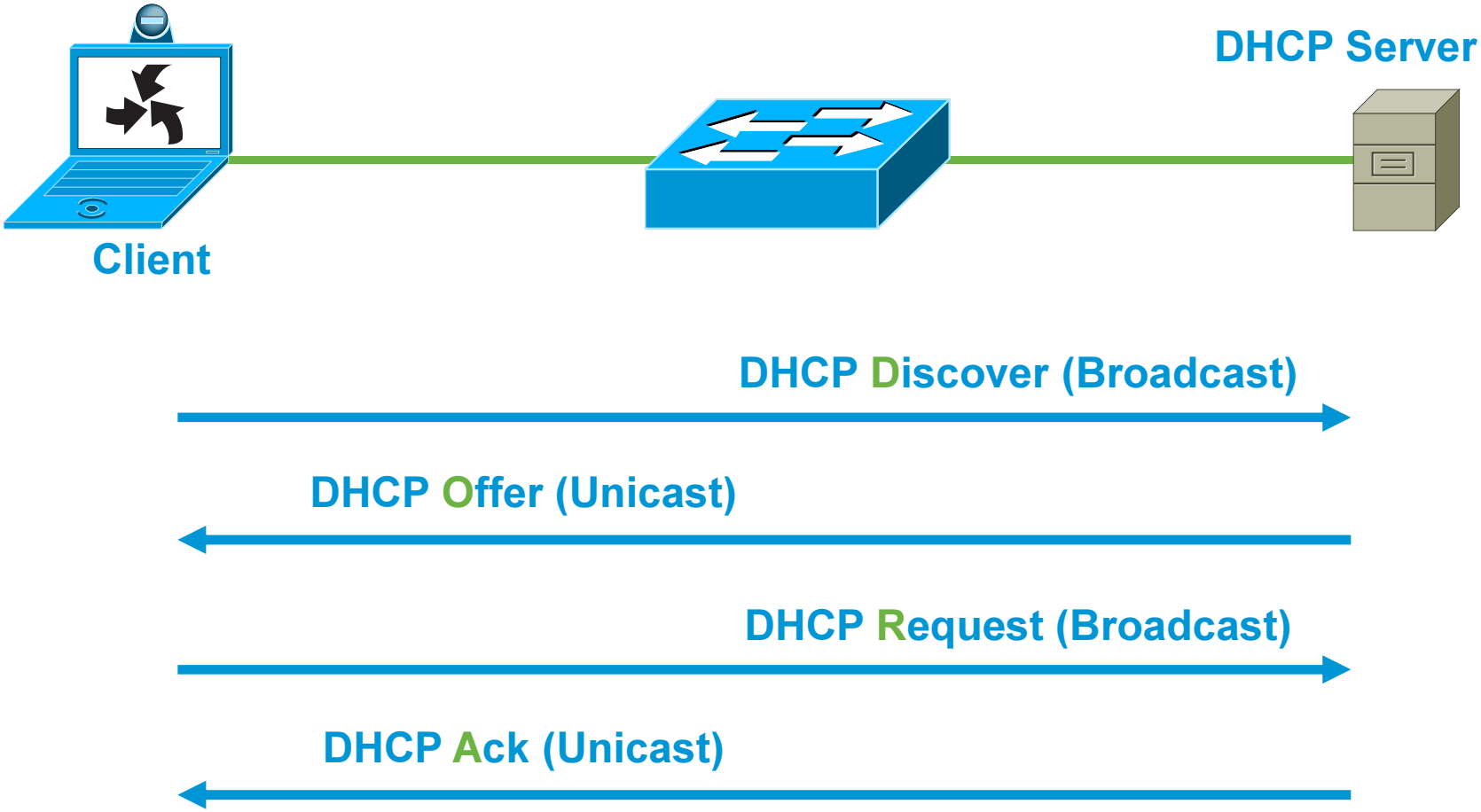
- Pregled Layer 2 napada
- Napadi i kontramere
  - VLAN Hopping
  - MAC napadi
  - DHCP napadi
  - ARP napadi
  - Spoofing napadi
  - Generalni napadi
- Zaključak

DHCP funkcionisanje



- Server dinamički dodeljuje IP adrese na osnovu zahteva
- Administrator kreira pool adresa koje se dodeljuju
- Adrese se dodeljuju sa periodom važenja – na određeno vreme
- DHCP kao opciju može da pošalje i ostale informacije

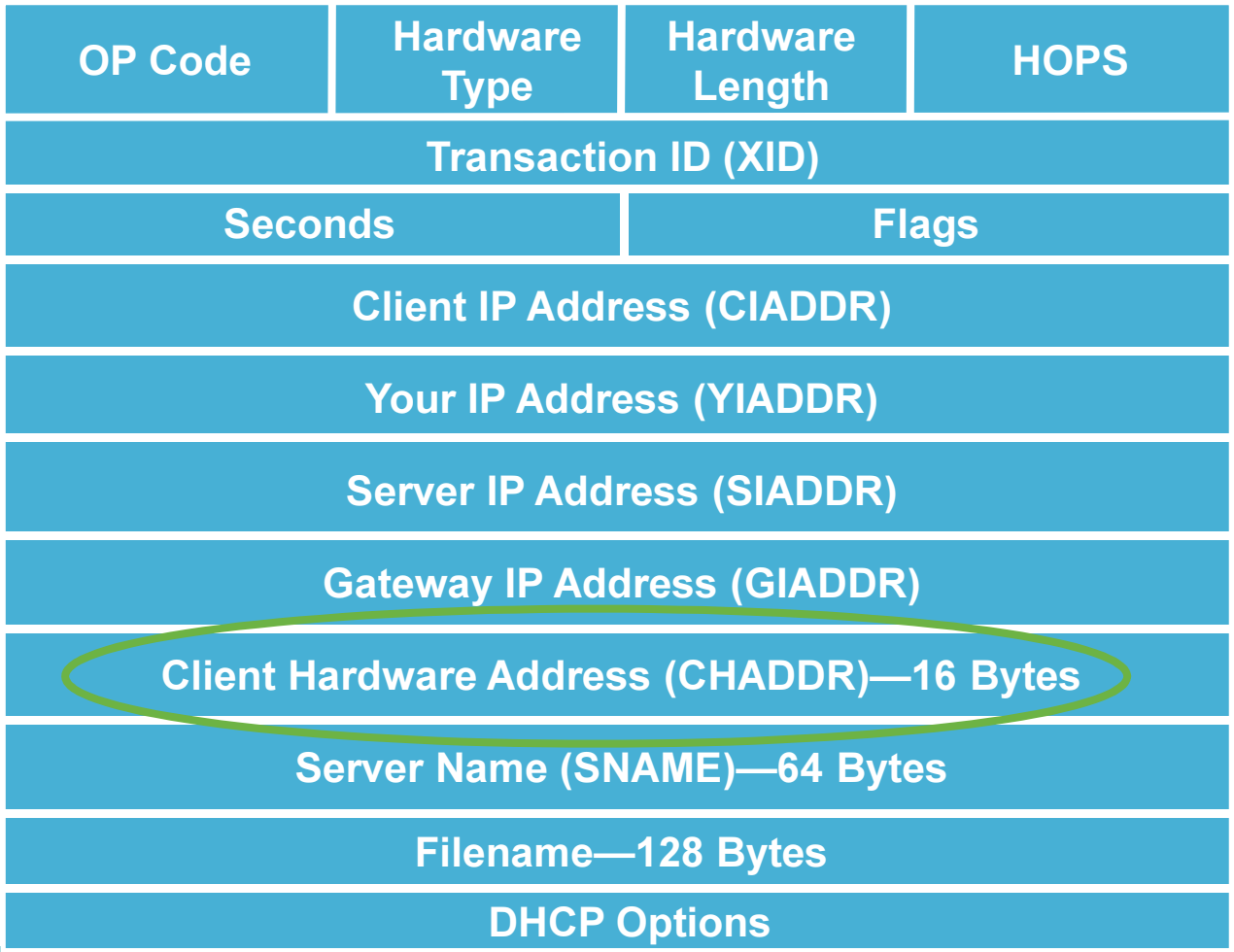
DHCP funkcionisanje



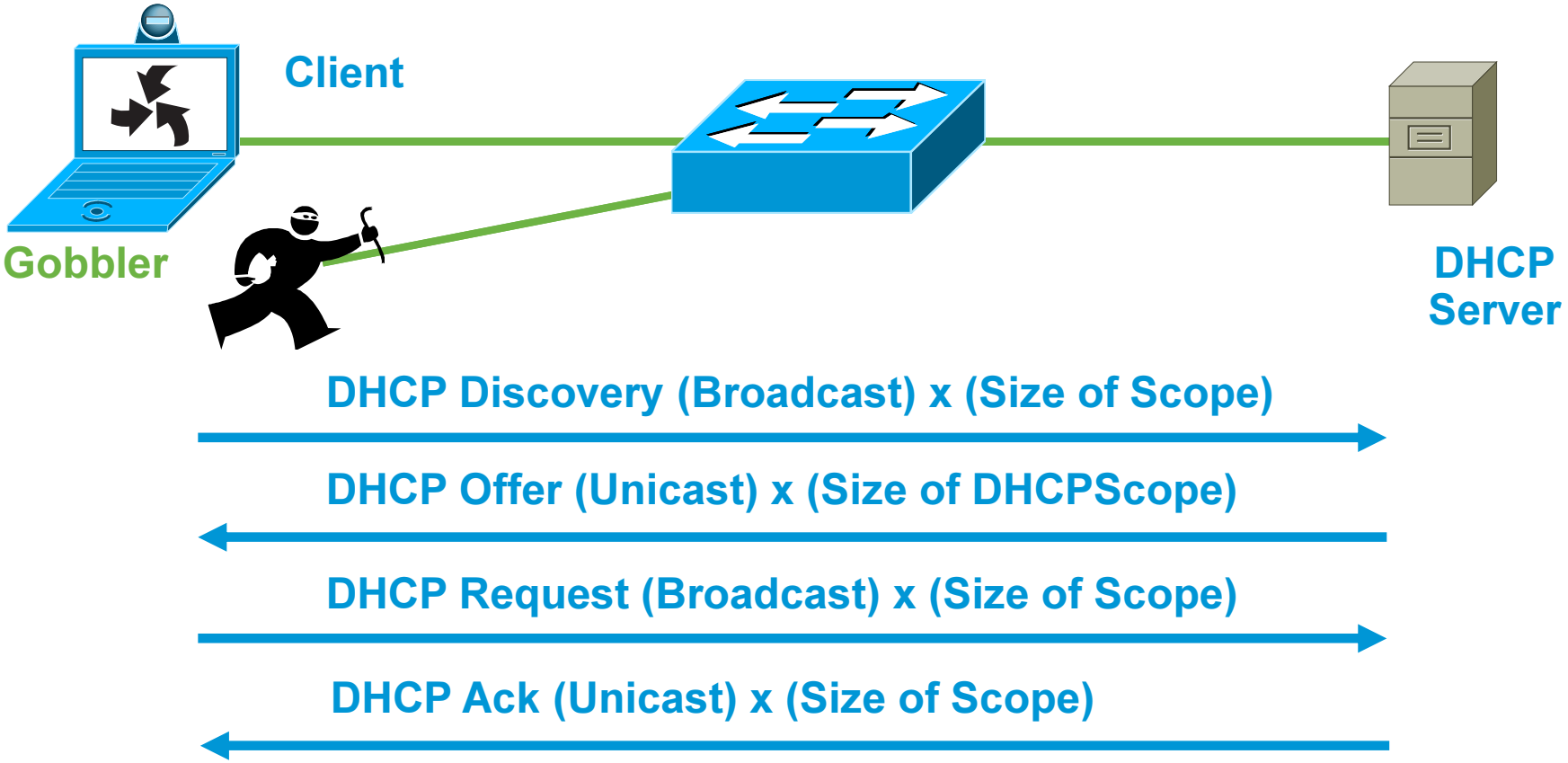
- DHCP definisan RFC 2131

DHCP funkcionisanje

IPv4 DHCP Format paketa

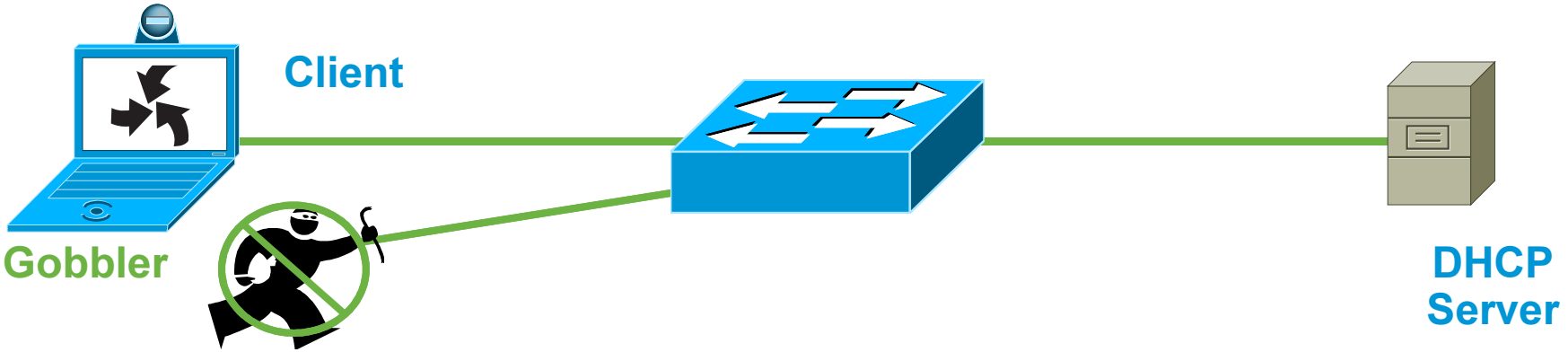


Prvi DHCP tip napada
DHCP napad izgladnjivanja - *Starvation*



- Gobbler pokušava da pokupi sve DHCP adrese iz DHCP pool-a
- Ovo je Denial of Service - DoS napad korišćenjem DHCPa

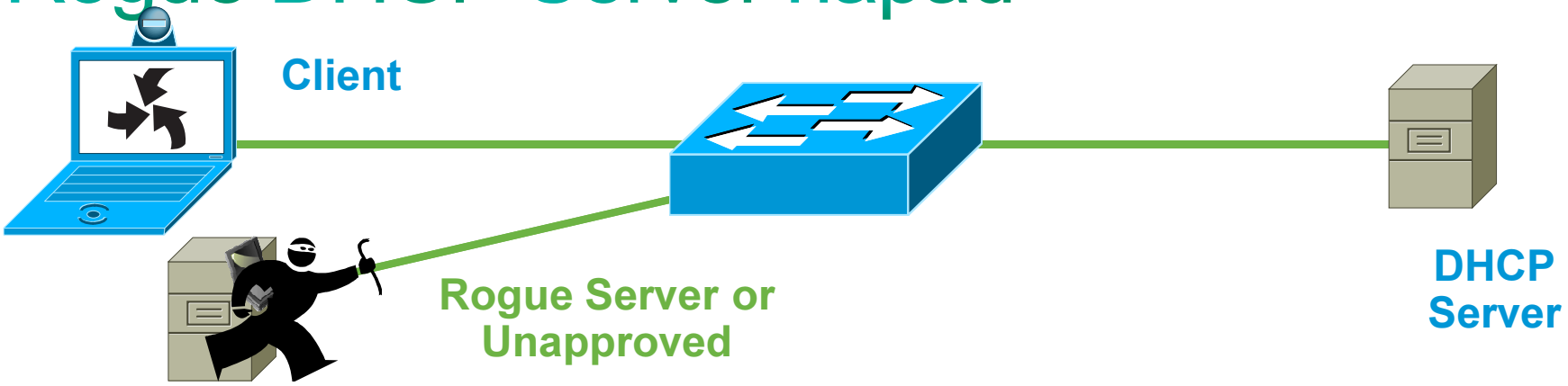
Kontramere za DHCP napade
DHCP Starvation napad= Port Security



- Gobbler koristi novu MAC adresu da traži novu DHCP adresu
- Ograničiti broj MAC adresa na portu
- Moguće dodeljivanje onog broja IP adresa koliko je MAC adresa dozvoljeno na tom portu

```
Cisco Catalyst OS
set port security 5/1 enable
set port security 5/1 port max 1
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
Cisco IOS
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

Tipovi DHCP napada
Rogue DHCP Server napad



DHCP Discovery (Broadcast)

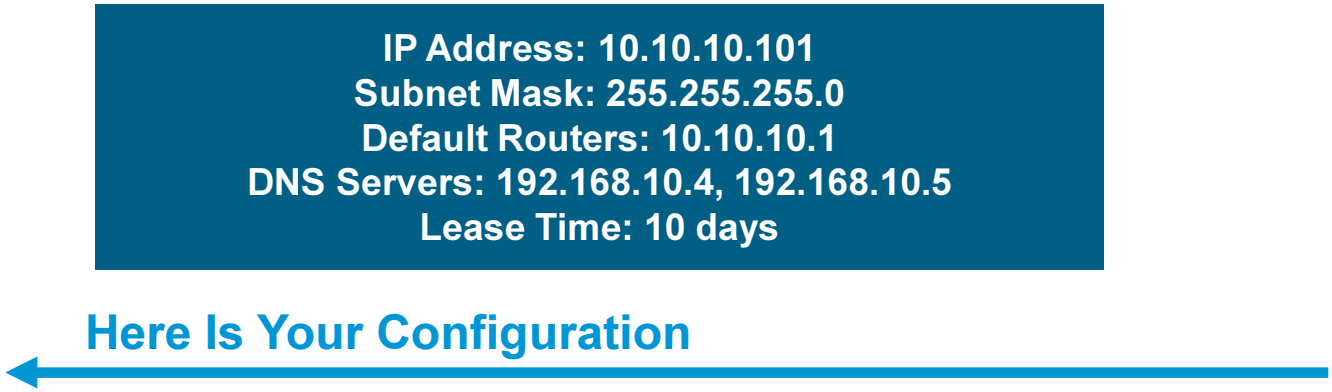
DHCP Offer (Unicast) from Rogue Server

DHCP Request (Broadcast)

DHCP Ack (Unicast) from Rogue Server

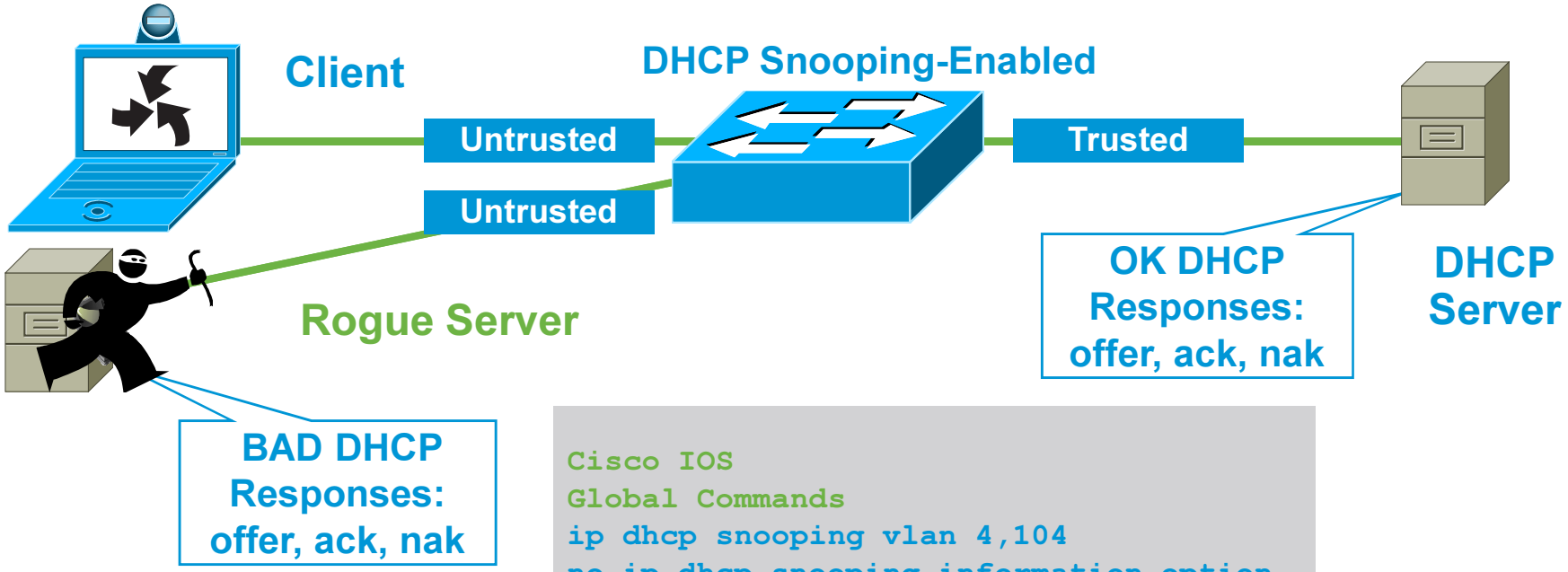
Tipovi DHCP napada
Rogue DHCP Server napad

- Šta sve napadač može da uradi ako je DHCP server?



- Zašto je to problem?
  - Pogrešan default gateway—Napadač je gateway
  - Pogrešan DNS server—Napadač je DNS server
  - Pogrešna IP adresa - Napadač radi DOS napad

Kontramere za DHCP napad
Rogue DHCP Server = DHCP Snooping




```
Cisco IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

DHCP Snooping Untrusted Client

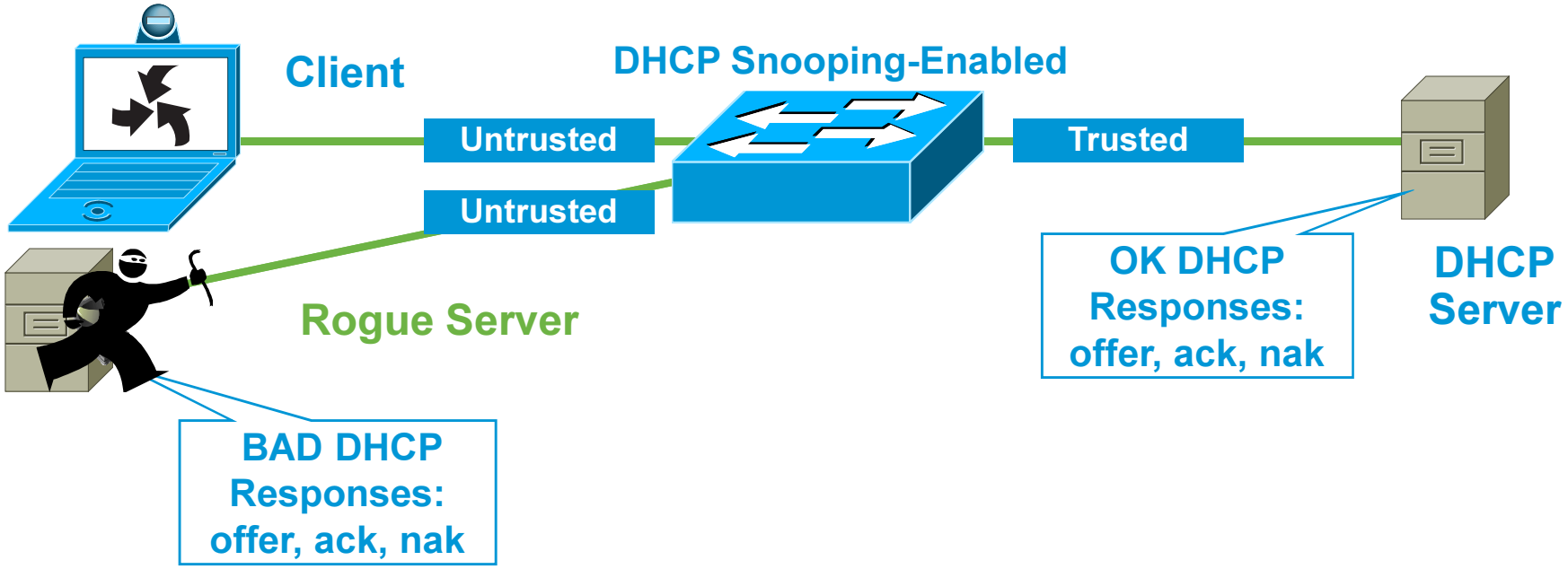
```
Interface Commands
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)
```

DHCP Snooping Trusted Server or Uplink

```
Interface Commands
ip dhcp snooping trust
```

- Po default-u svi portovi u VLANu su *untrusted*

Kontramere za DHCP napad
Rogue DHCP Server = DHCP Snooping



DHCP Snooping Binding Table

```
sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)   Type            VLAN    Interface
------------------- ---------------  ----------   -------------   ----    --------------------
00:03:47:B5:9F:AD   10.120.4.10      193185       dhcp-snooping   4       FastEthernet3/18
```

- Tabela se pravi “njuškajući” po DHCP odgovorima ka klijentima
  Ostaju u tabeli dok DHCP lease vreme ne istekne

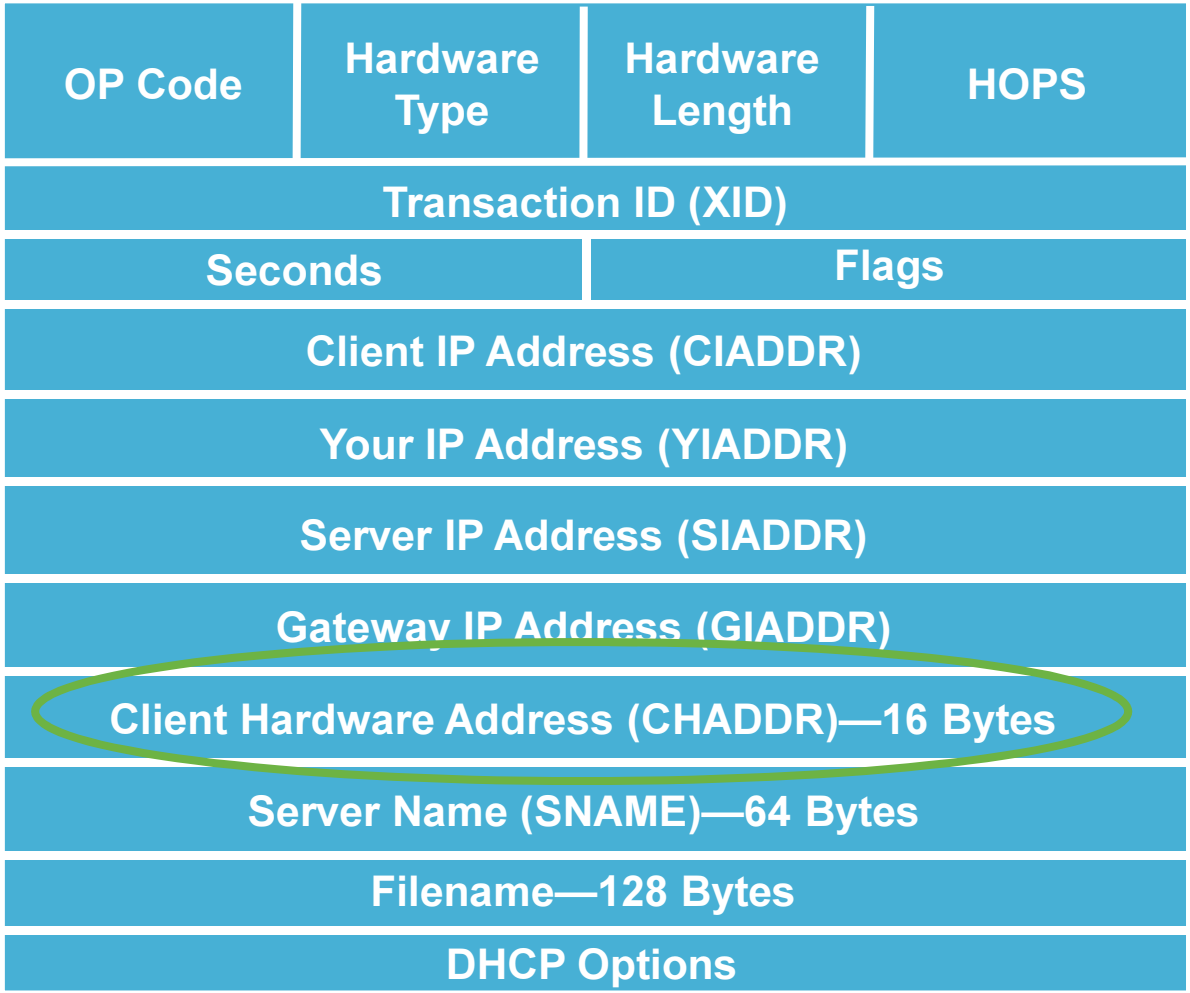
Napredna konfiguracija DHCP Snooping-a

- Neće svi OS(Linux) re DHCP u slučaju link down
- Za slučaj restarta/kvara sviča, DHCP snooping binding tabela se može čuvati na bootflash, ftp, rcp, slot0, i tftp serveru
- Ovo je posebno važno za sledeće sekcije - rešenja

```
ip dhcp snooping database tftp://172.26.168.10/tftpboot/tulledge/ngcs-4500-1-dhcpdb
ip dhcp snooping database write-delay 60
```

Napredna konfiguracija DHCP Snooping-a

- Gobbler koristi novu MAC za svaki DHCP request i port security sprečava Gobbler
- Šta ako se u napadu koristi ista interface MAC adresa, sa promenjenim *client hardware address* u request-u?
- Port security neće sprečiti taj napad
- Svič proverava CHADDR polje u request-u da bi bio siguran da je ista kao MAC u DHCP snooping binding tabeli
- Ako se ne poklapa, zahtev se odbacuje na interfejsu

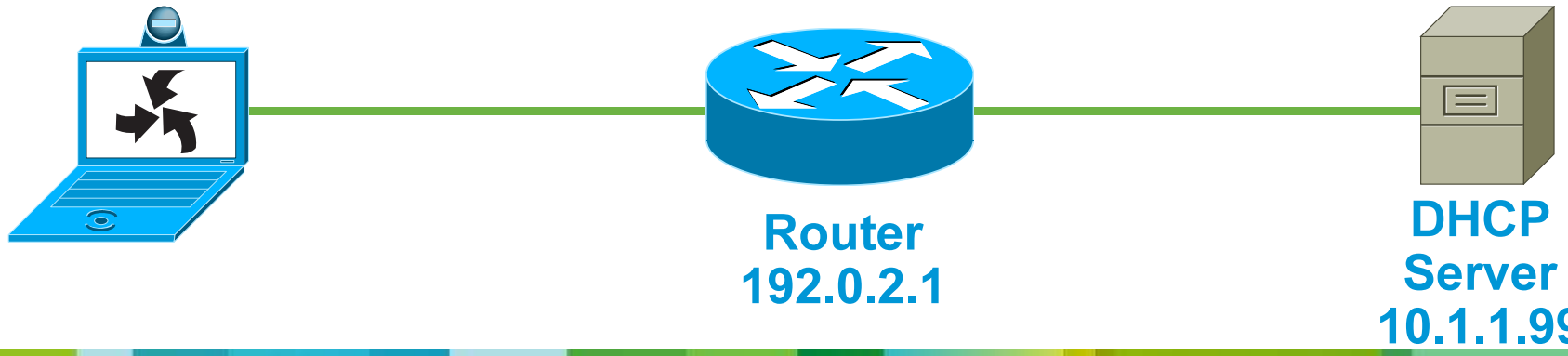


DHCP Rogue Server

- Ako neki svičevi ne podržavaju DHCP snooping, možemo konfigurisati VLAN ACL i blokirati UDP port 68

```
set security acl ip ROGUE-DHCP permit udp host 192.0.2.1 any eq 68
set security acl ip ROGUE-DHCP deny udp any any eq 68
set security acl ip ROGUE-DHCP permit ip any any
set security acl ip ROGUE-DHCP permit udp host 10.1.1.99 any eq 68
```

  - Ovo neće sprečiti CHADDR DHCP starvation napad



Rezime DHCP napada

- DHCP starvation napadi mogu se sprečiti port security komandama
- Rogue DHCP serveri mogu se sprečiti DHCP snooping komandama
- Kada se konfiguriše DHCP snooping, svi portovi u VLANu će biti “untrusted” za DHCP odgovore
- Proveriti default podešavanje sviča – da li gleda CHADDR polje u DHCP request-u ?
- Svičevi koji ne podržavaju DHCP snooping mogu da koriste ACL za delimično ograničavanje napada (ne proveravaju CHADDR polje)

DHCP Snooping mogućnosti

- Sve DHCP snooping binding tabele imaju ograničenu veličinu
- Svi podaci ostaju u binding tabeli dok l*ease* ne istekne
- Ako je okruženje mobilno, treba smanjiti *lease time* kako bi svi binding ulazi bili ažurni

```
sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------- ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10     193185      dhcp-snooping  4     FastEthernet3/18
```

Izgradnja slojeva-piramide bezbednosti

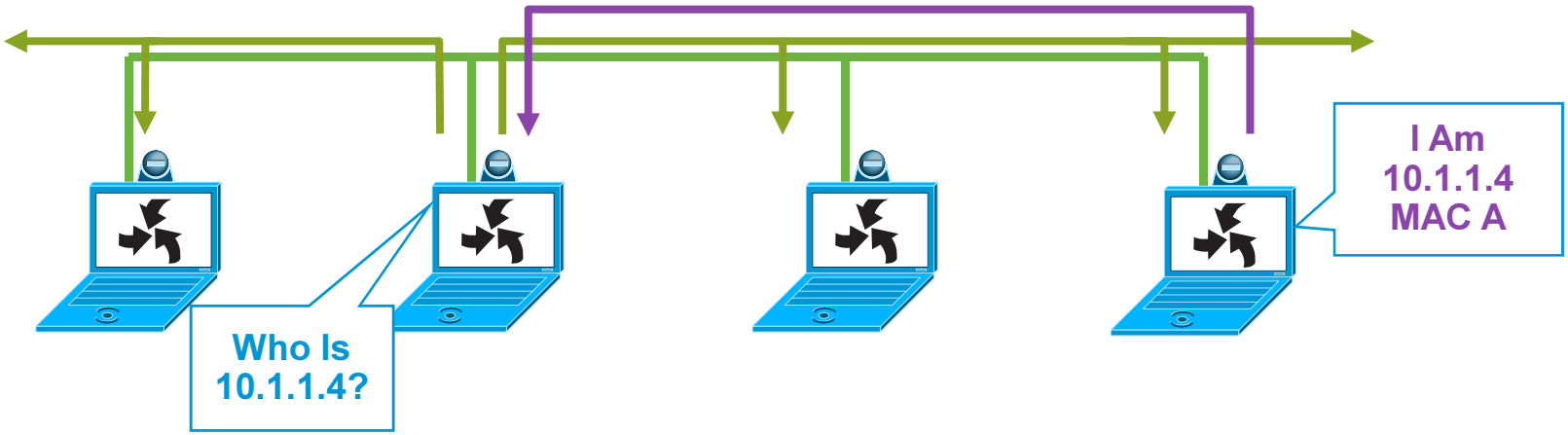
- Port Security sprečava CAM napade(i neke DHCP starvation napade)
- DHCP snooping sprečava rogue DHCP server napade

Agenda

- Pregled L2 napada
- Napadi i kontramere
  - VLAN Hopping
  - MAC napadi
  - DHCP napadi
  - ARP napadi
  - Spoofing napadi
  - Generalni napadi
- Zaključak

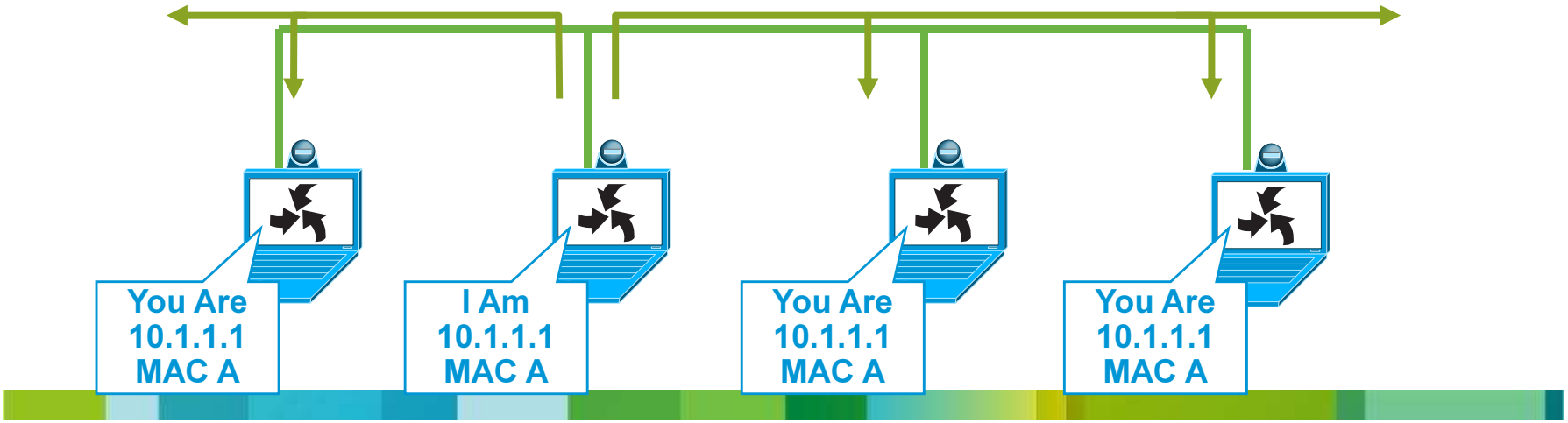
ARP Funkcija

- Pre no što stanica može da priča sa drugom stanicom on mora da šalje ARP request da mapira IP adresu u MAC adres
  - Ovaj ARP request se broadcast-uje korišćenjem protokola 0806
- Svi kompjuteri na tom subnetu će primiti i procesirati taj ARP request; stanica čija je to IP adresa u request-u će poslati ARP reply



ARP Funkcija

- U skladu sa ARP RFC, klijentu je dozvoljeno da šalje unsolicited (netražen) ARP reply; to se zove gratuitous ARP; drugi hostovi smeštaju ARP reply podatke u svojoj tabeli
- Bilo ko može da tvrdi da je vlasnik bilo koje IP/MAC adrese t
- ARP napadi se koriste da se redirektuje saobraćaj



Alati za ARP napad

- Na netu se mogu naći mnogi alati za ARP man-in-the-middle napade

  Dsniff, Cain & Abel, ettercap, Yersinia, itd.

- ettercap: http://ettercap.sourceforge.net/index.php

  Neki su druga ili treća generacija ARP attack alata

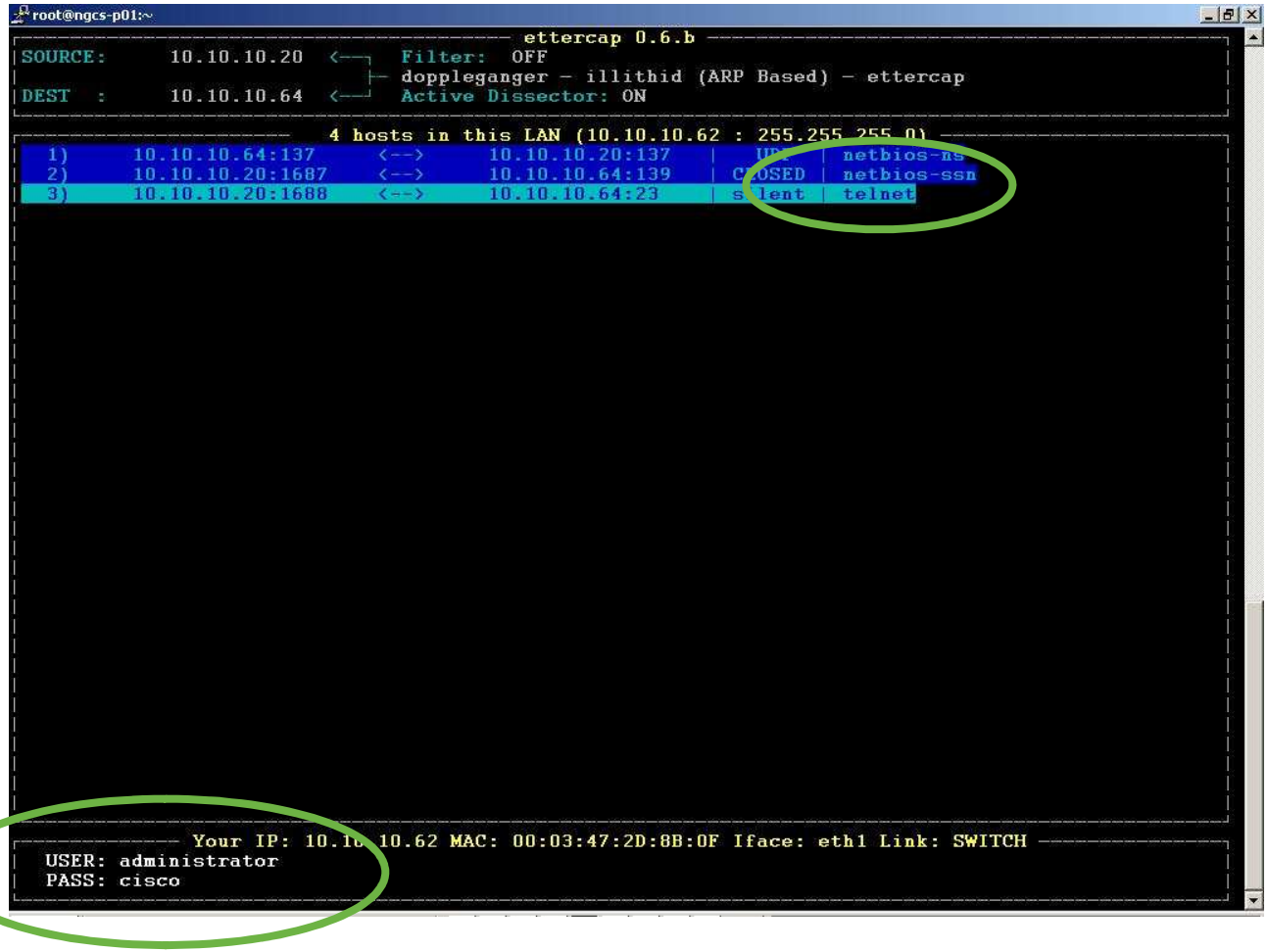
  Većina ima veoma lep GUI, skoro da je “point and click”

- Svaki od njih hvata saobraćaj i lozinke sledećih protokola:

  FTP, Telnet, SMTP, HTTP, POP, NNTP, IMAP, SNMP, LDAP, RIP, OSPF, PPTP, MS-CHAP, SOCKS, X11, IRC, ICQ, AIM, SMB, Microsoft SQL, etc.

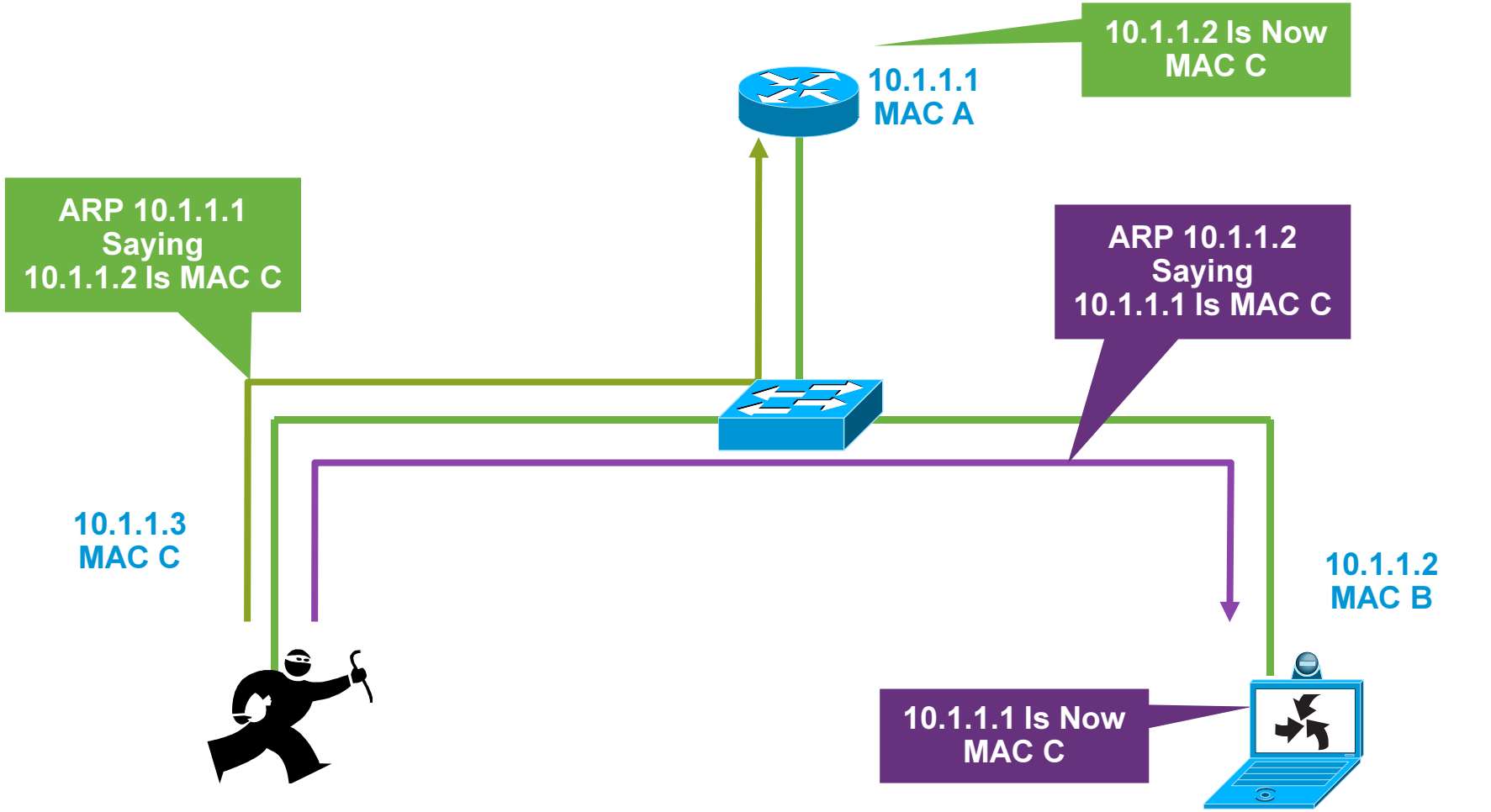
Alati za ARP napad

- Ettercap u akciji
- Radi za Window, Linux, Mac
- Dekoduje lozinke
- telnet username/ password je uhvaćen



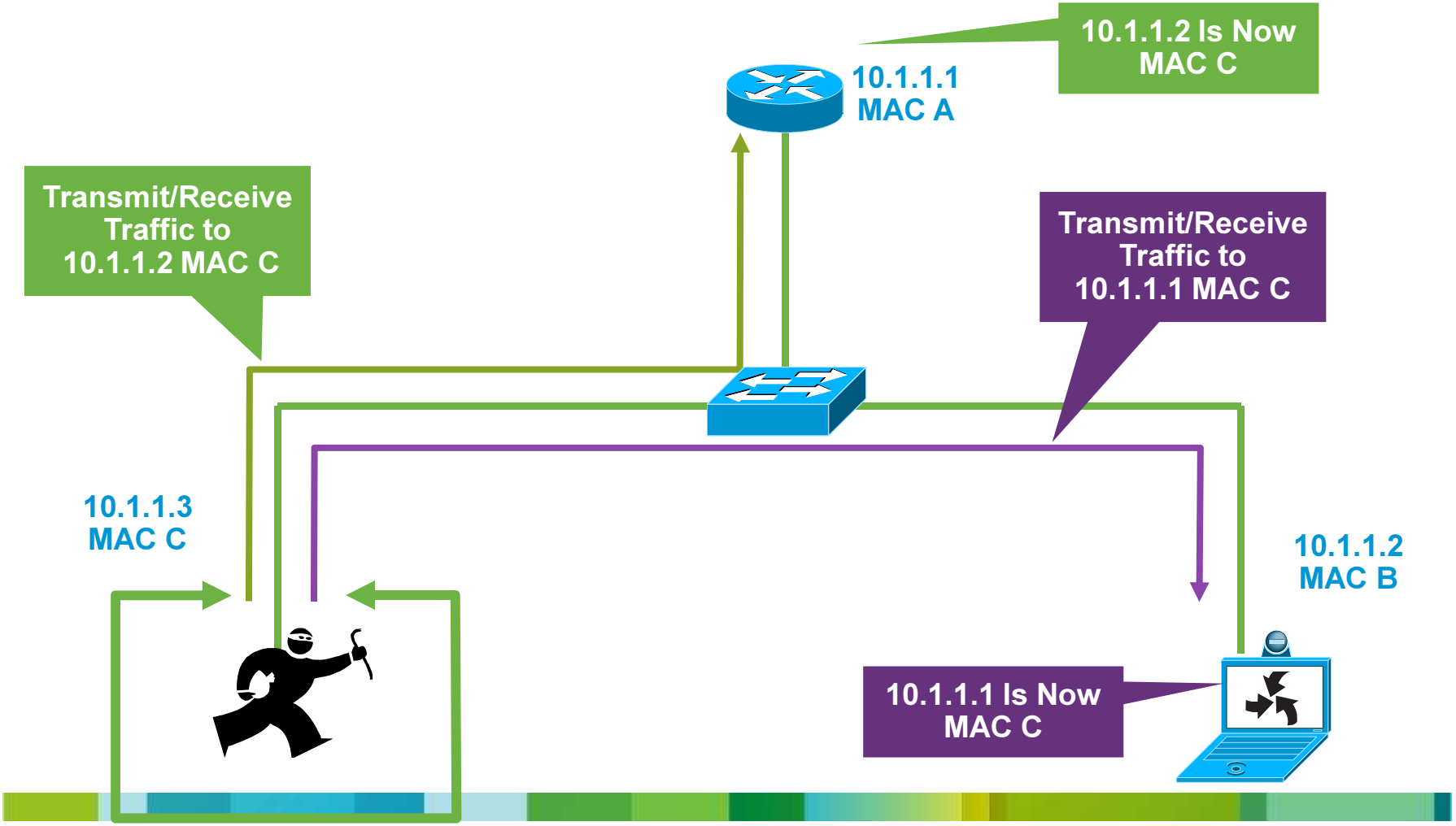
ARP napad

- Napadač “truje” ARP tabelu



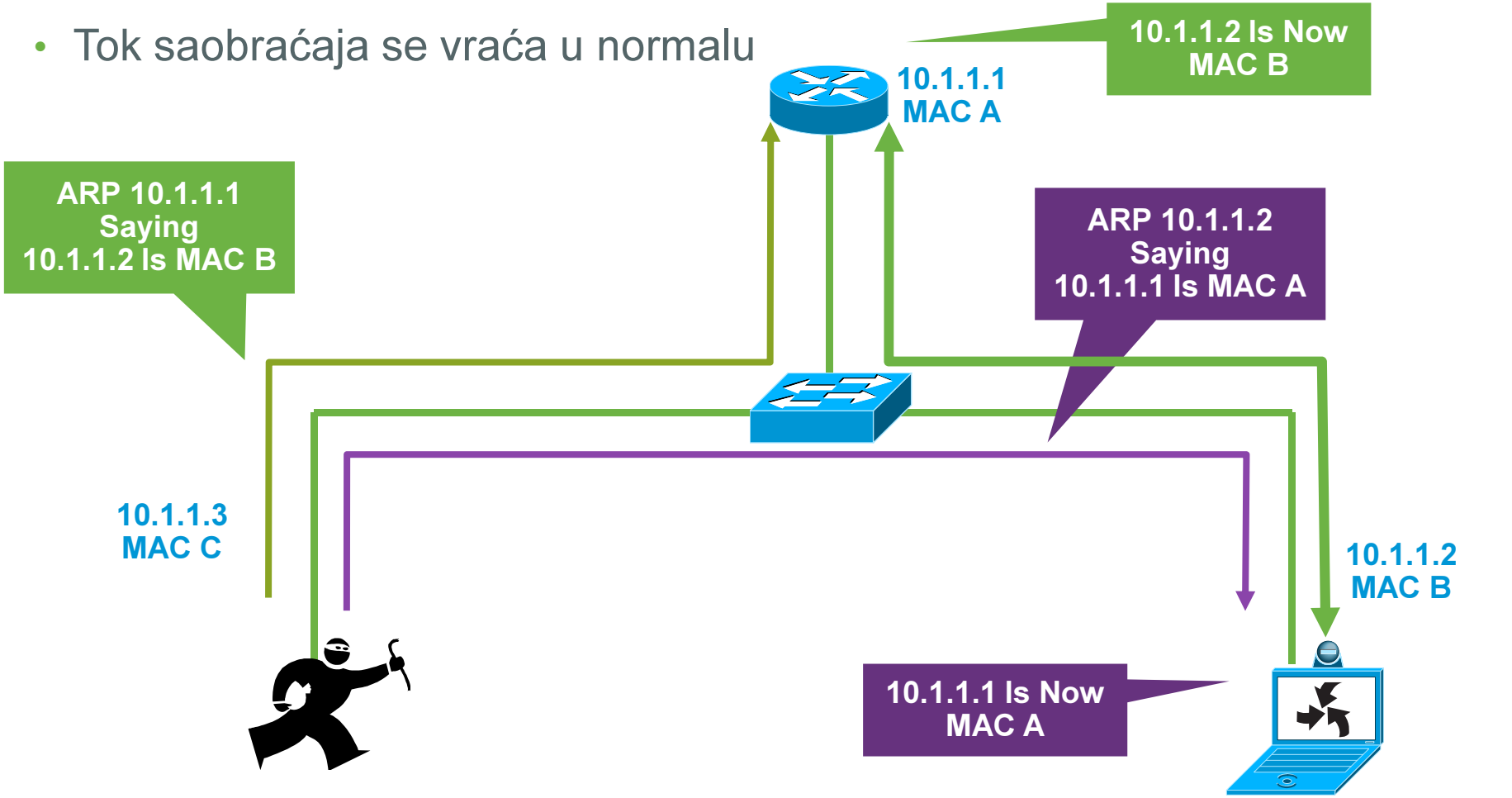
ARP napad

- Sav saobraćaj ide kroz napadača



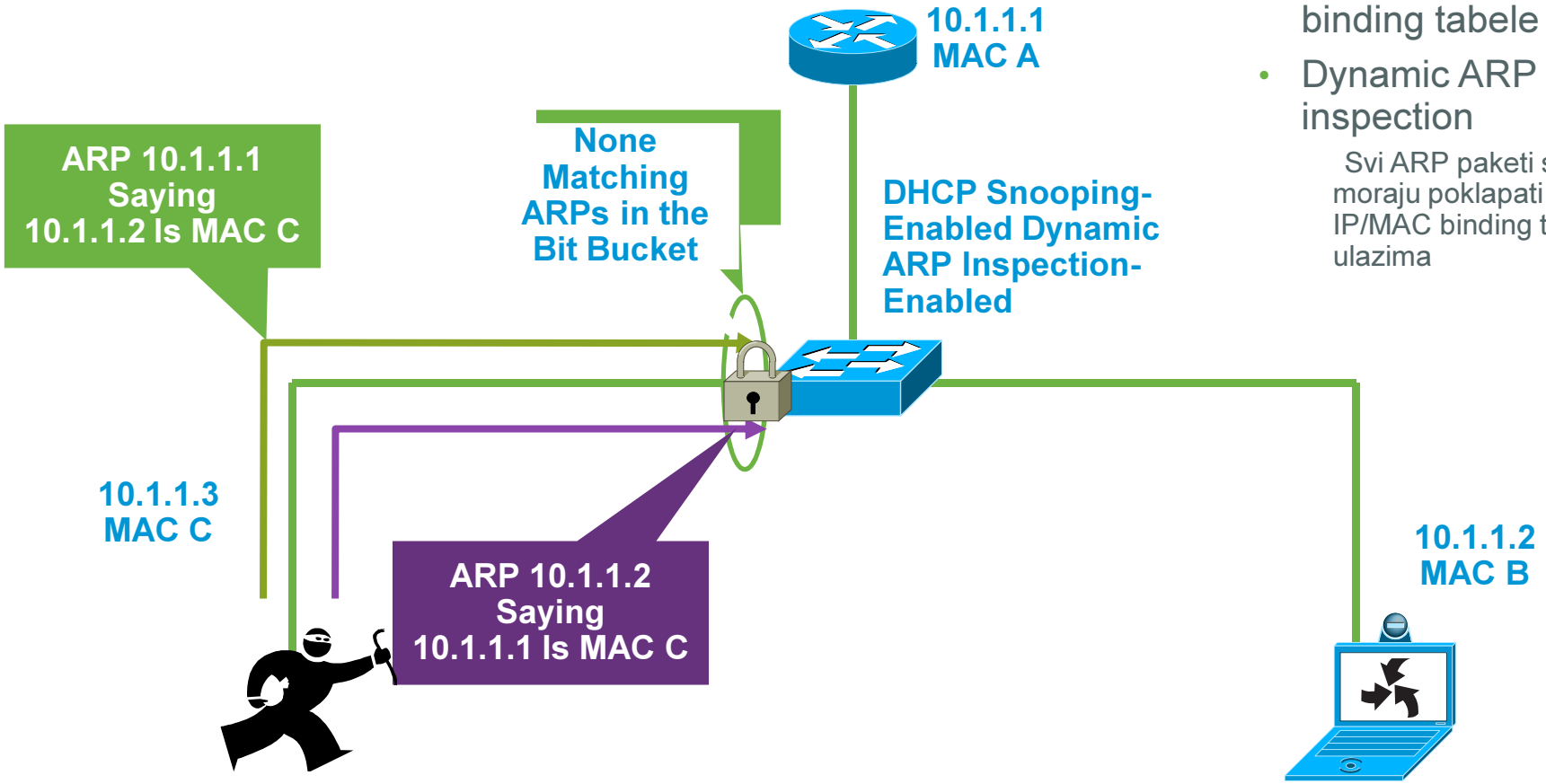
ARP napad - Clean Up

- Napadač ispravlja ARP tabelu ispravnim vrednostima
- Tok saobraćaja se vraća u normalu



Kontramere za ARP napad: Dynamic ARP Inspection

- Koristi informacije iz DHCP snooping binding tabele
- Dynamic ARP inspection
  - Svi ARP paketi se moraju poklapati sa IP/MAC binding table ulazima



Kontramere za ARP napad: Dynamic ARP Inspection

- Koristimo podatke iz DHCP snooping binding tabele

```
sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10      193185      dhcp-snooping  4     FastEthernet3/18
```

- Gledaju se MacAddress i IpAddress polja da bi se videlo da li je ARP legitiman ?

Kontramere za ARP napad: Dynamic ARP Inspection

Konfiguracija Dynamic ARP Inspection (DAI)

- DHCP snooping mora biti konfigurisan i tabela generisana
- DAI se konfiguriše po VLANu
- Možemo staviti *trust interface* kao kod DHCP snooping
- Oprezno sa *rate limitingom*—varira između platformi

Kontramere za ARP napad: Dynamic ARP Inspection

Dynamic ARP Inspection komande

```
Cisco IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 4,104
ip arp inspection log-buffer entries 1024
ip arp inspection log-buffer logs 1024 interval 10
Interface Commands
ip dhcp snooping trust
ip arp inspection trust
```

```
Cisco IOS
Interface Commands
no ip arp inspection trust
(default)
ip arp inspection limit rate 15
(pps)
```

Dodatne provere

- Može se proveravati destination i/ili source MAC i IP adresa

  Destination MAC: proverava destination MAC adresu u Ethernet headeru sa targetiranom MAC adresom u ARP telu poruke

  Source MAC: proverava source MAC adresu u Ethernet headeru sa sender MAC adresom u ARP telu poruke

  IP adresa: proverava ARP telo poruke za *invalid* ili *unexpected* IP adrese; to su npr. 0.0.0.0, 255.255.255.255, i sve IP multicast adrese

Cisco IOS komande

```
Cisco IOS
Global Commands
ip arp inspection validate dst-mac

ip arp inspection validate src-mac

ip arp inspection validate ip

Enable all commands
ip arp inspection validate src-mac dst-mac ip
```

- Svaka provera se radi nezavisno
  - Svaka zasebno ili sve zajedno
- Poslednja komanda *overwrites* prethodne komande
  - Npr. Ako imamo dst-mac i stavimo src-mac, dst-mac nije više aktivan

Kontramere za ARP napad: Dynamic ARP Inspection

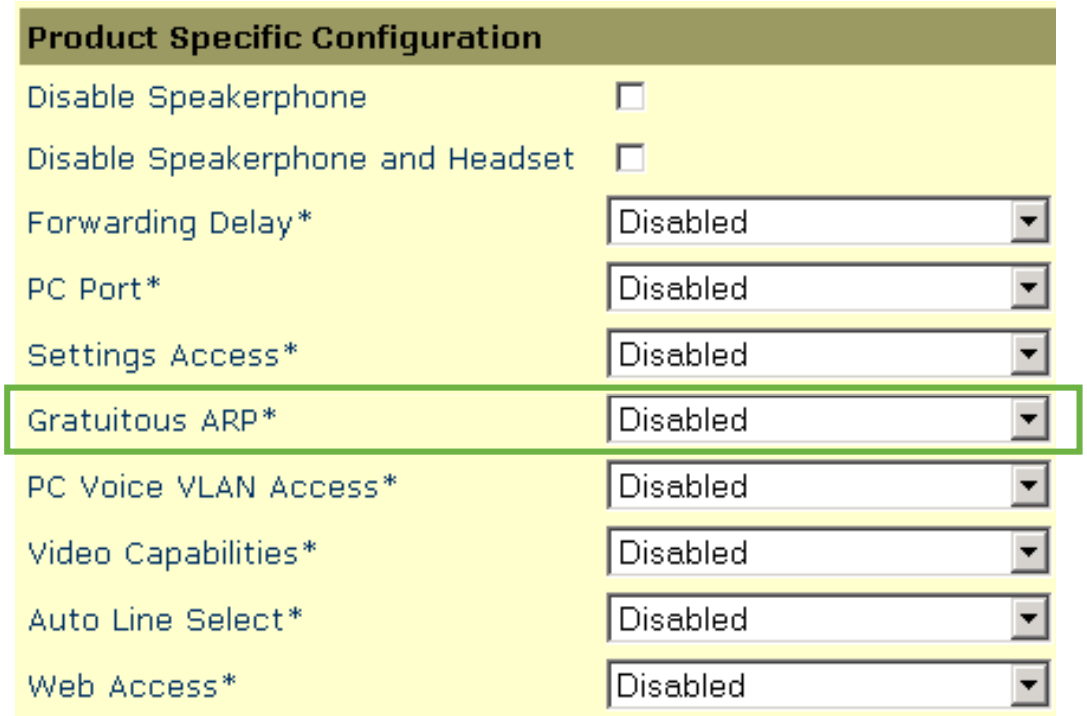
Error poruke u Show Log

```
sh log:
4w6d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 296 milliseconds on Gi3/2.
4w6d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/2, putting Gi3/2 in err-disable
state
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan
183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.2/12:19:27 UTC Wed Apr 19 2000])
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan
183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.3/12:19:27 UTC Wed Apr 19 2000])
```

Phone ARP funkcije

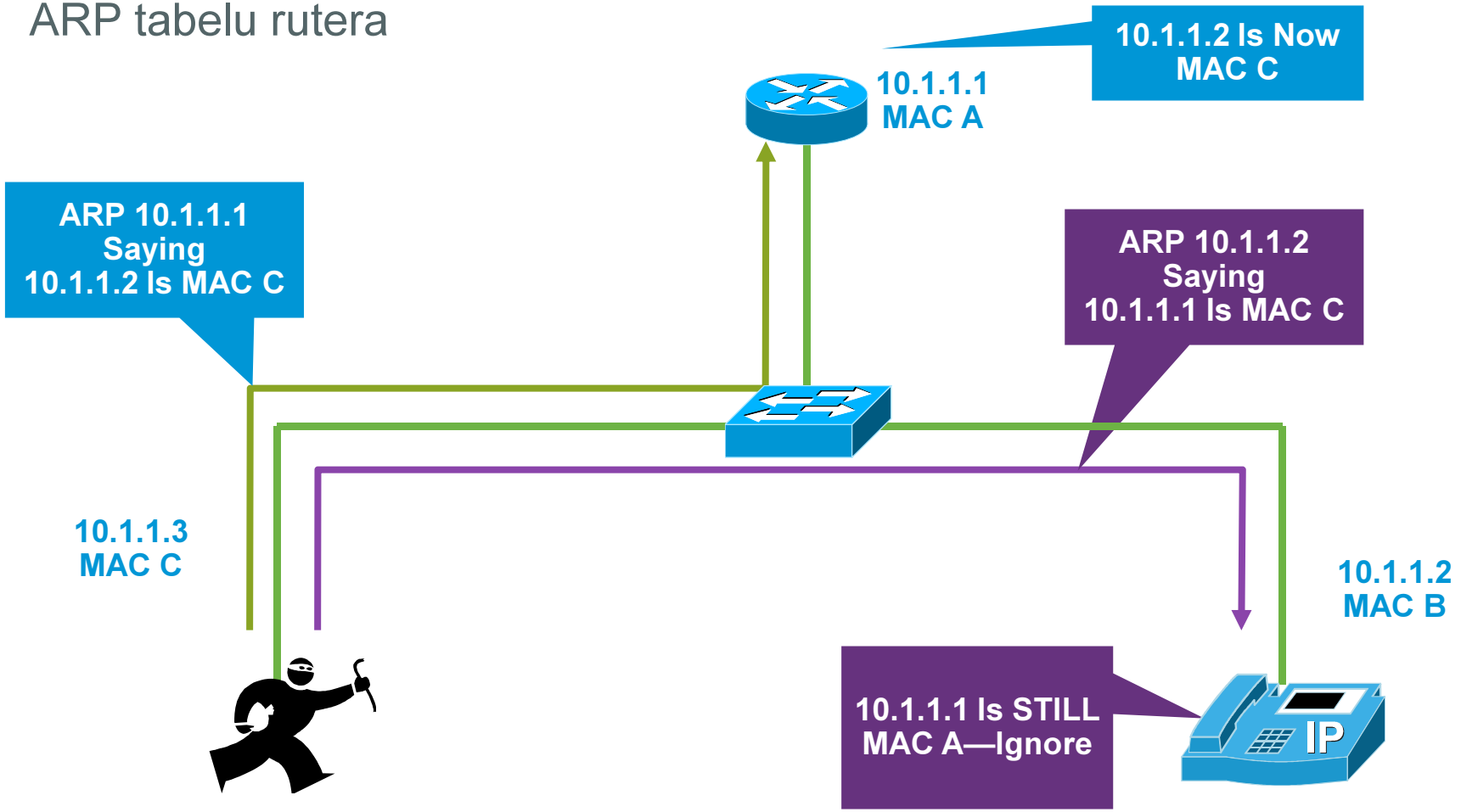
Konfigurabilne opcije

- Blokiranje voice VLAN sa PC porta
- Ignore Gratuitous ARPs (GARPs)



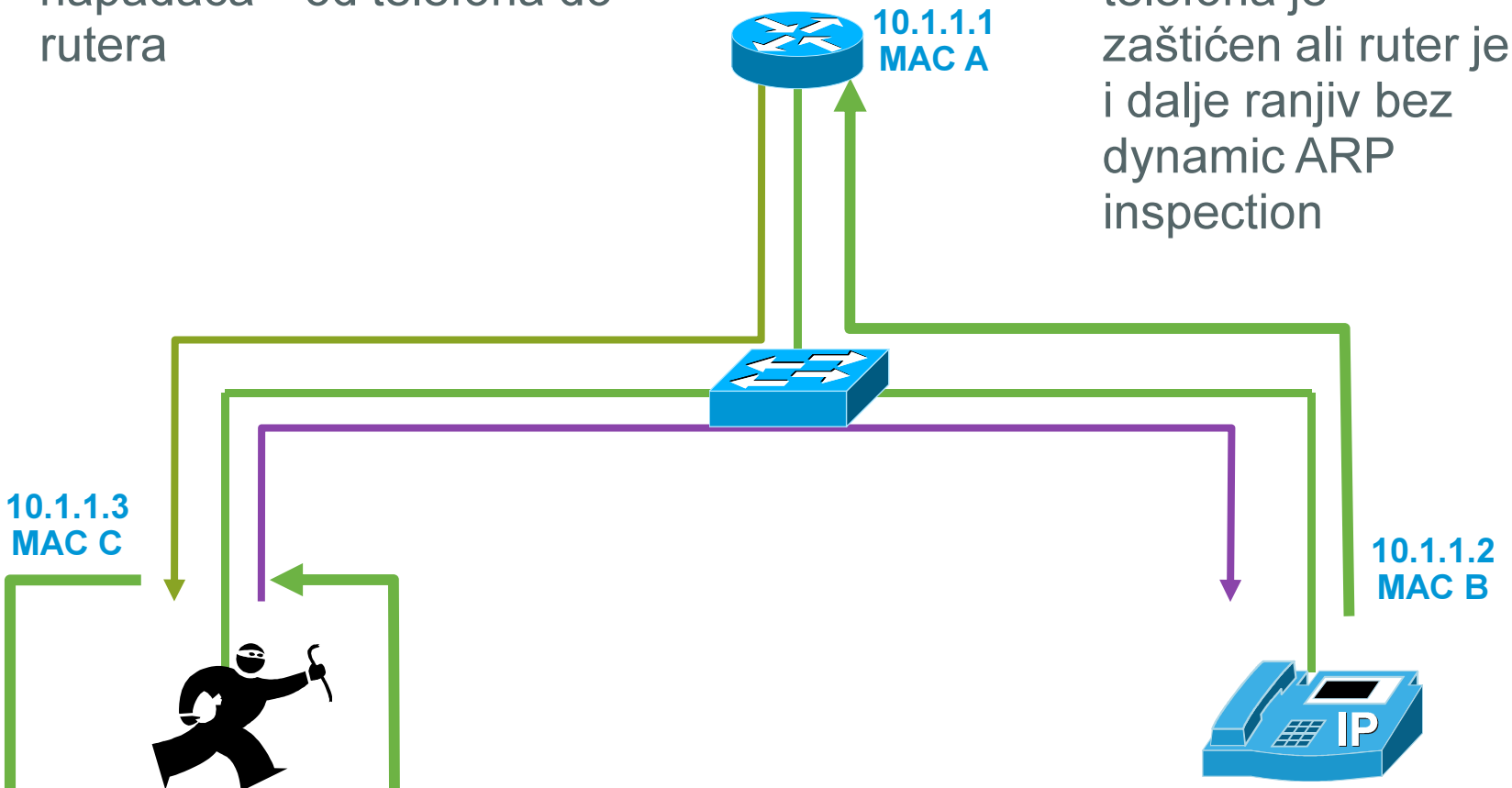
Phone ARP funkcije

- Napadač “truje” ARP tabelu rutera



Phone ARP funkcije

- Saobraćaj od rutera do napadača—od telefona do rutera
- Saobraćaj sa telefona je zaštićen ali ruter je i dalje ranjiv bez dynamic ARP inspection



Ne-DHCP uređaji

- Koristi se static binding u DHCP snooping binding tabeli

```
Cisco IOS
Global Commands
ip source binding 0000.0000.0001 vlan 4 10.0.10.200 interface fastethernet 3/1
```

- Static i dynamic ulazi u DHCP snooping binding tabeli su različiti

```
Cisco IOS
Show Commands
 show ip source binding
```

Binding Tabele - Info

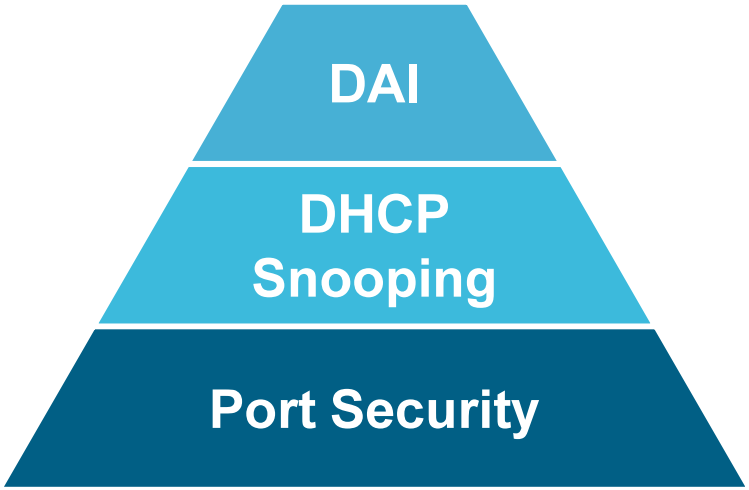
- Ako nema ulaza u binding tabeli —nema saobraćaja
- Sačekati da svi uređaji imaju *new leases* pre puštanja dynamic ARP Inspection
- Stoje u tabeli dok ne istekne *lease time*
- Veličine tabeli:
  - 3000 svičevi —2500 ulaza
  - 4000 svičevi—4000 ulaza(6000 za SupV-10GE)
  - 6000 svičevi—16,000 ulaza

Pregled ARP napada

- Dynamic ARP inspection sprečava ARP napade prekidajući ARP requests i responses
- DHCP snooping mora prvo biti konfigurisano, inače nećemo imati pravo da koristimo dynamic ARP Inspection
- DHCP snooping tabela se pravi iz DHCP request, ali možemo staviti i statičke ulaze

Izgradnja slojeva-piramide bezbednosti

- Port Security sprečava CAM napade(i neke DHCP starvation napade)
- DHCP snooping sprečava rogue DHCP server napade
- Dynamic ARP inspection sprečava ARP napade



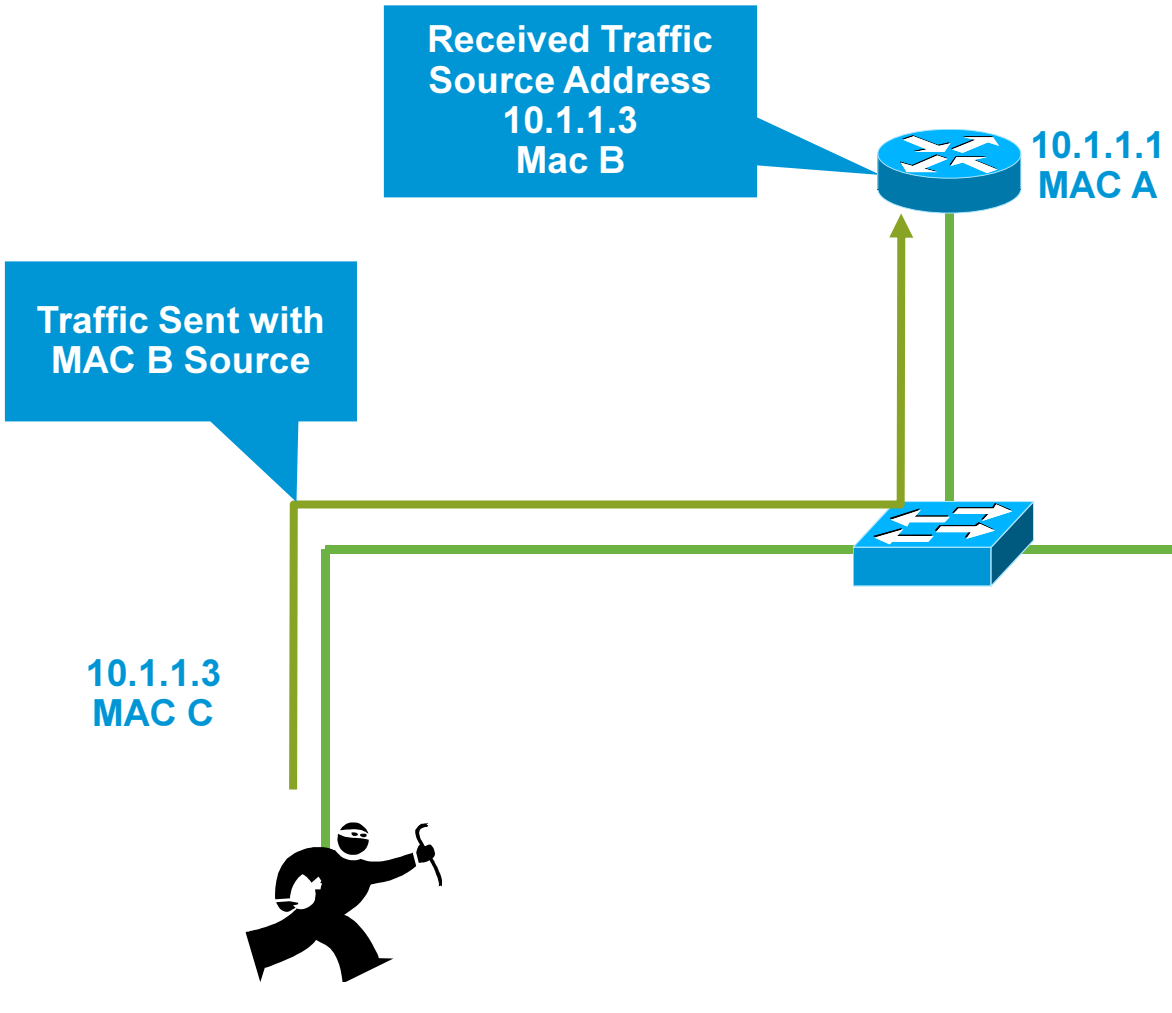
Agenda

- Pregled L2 napada
- Napadi i kontramere
  - VLAN Hopping
  - MAC napade
  - DHCP napadi
  - ARP napadi
  - Spoofing napadi
  - Generalni napadi
- Zaključak

Spoofing napadi

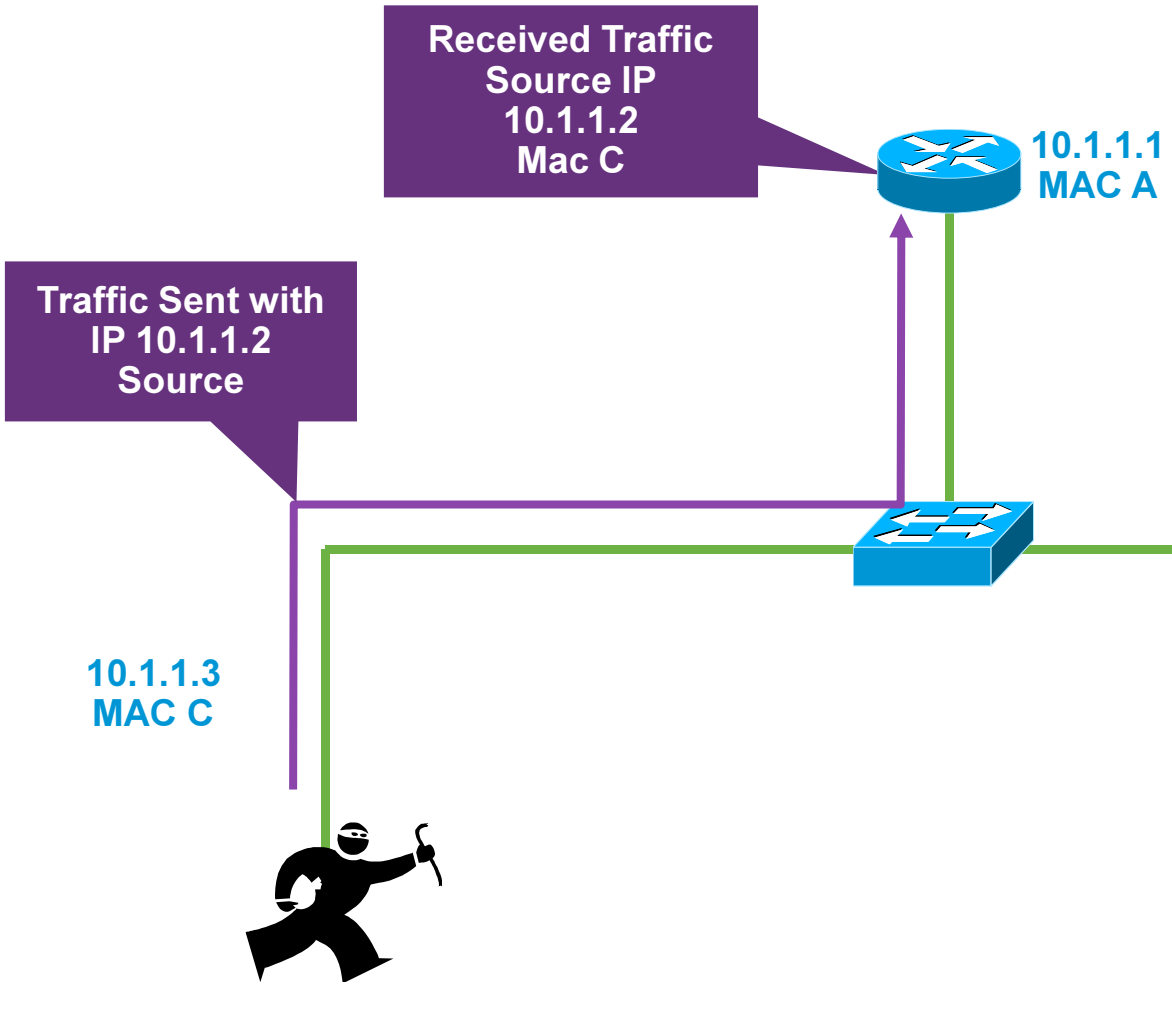
- MAC spoofing
  - MAC se koriste za pristup mreži
  - Takođe se koriste za krađu identiteta nekoga ko je već na mreži
- IP spoofing
  - Ping of death
  - ICMP unreachable storm
  - SYN flood

Spoofing napad: MAC



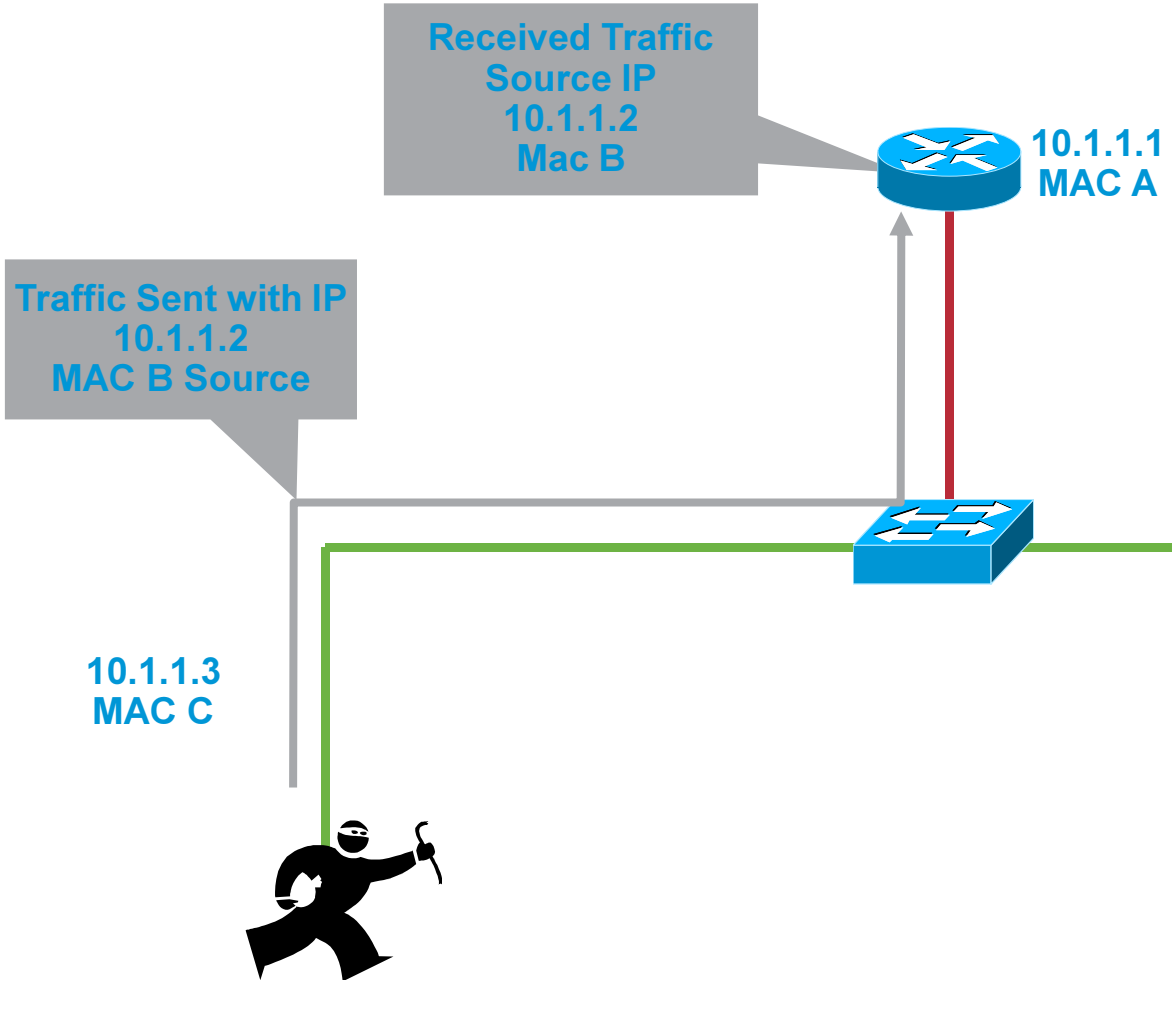
- Napadač šalje pakete sa netačnom source MAC adresom

Spoofing napad: IP



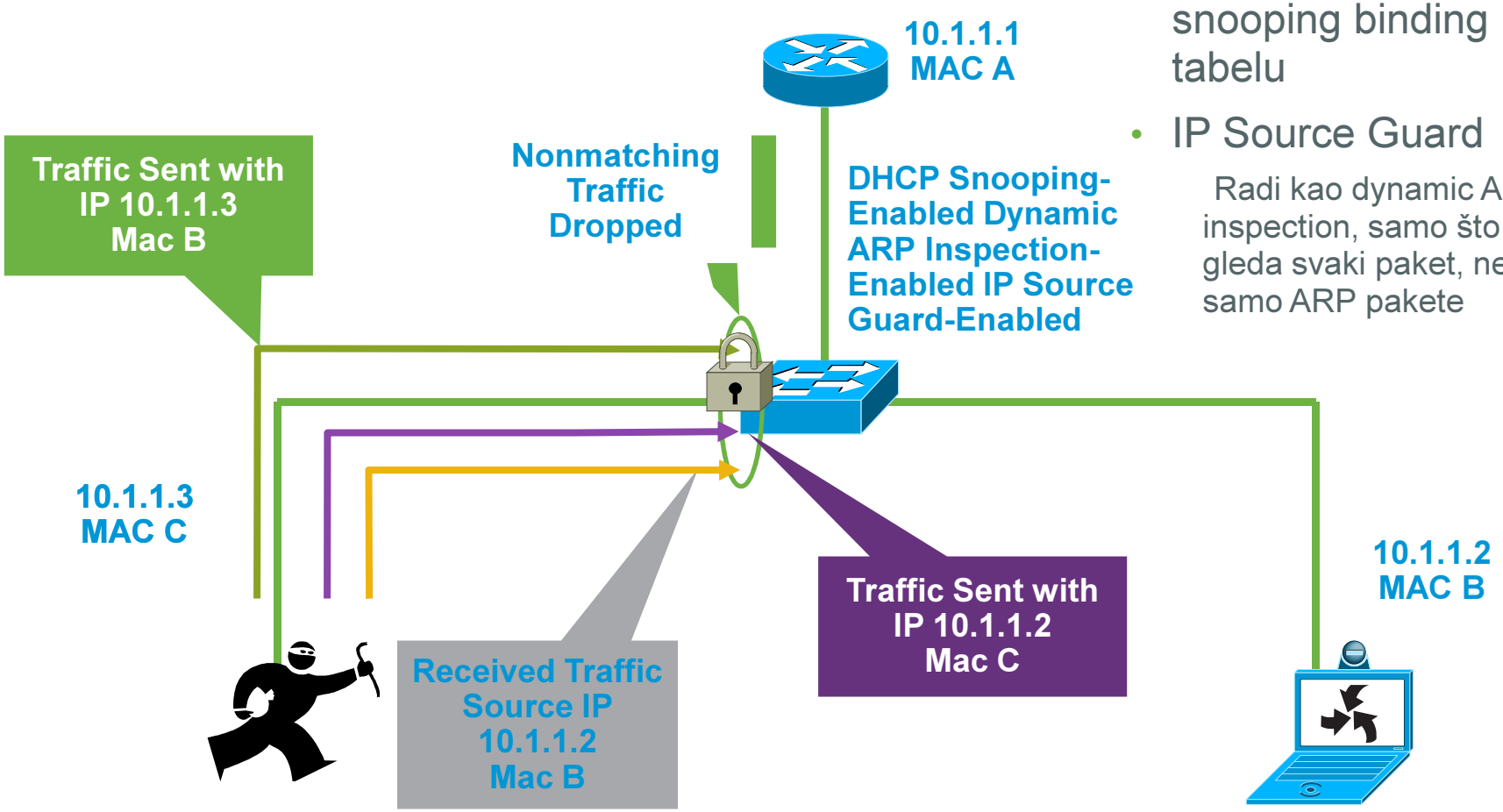
- Napadač šalje pakete sa netačnom source IP adresom
- Kome god da je poslat paketd on nikad neće odgovoriti napadaču

Spoofing napad: IP/MAC



- Napadač šalje pakete sa netačnom source MAC i IP adresom

Kontramere za Spoofing napade: IP Source Guard



- Koristi DHCP snooping binding tabelu
- IP Source Guard

  Radi kao dynamic ARP inspection, samo što gleda svaki paket, ne samo ARP pakete

Kontramere za Spoofing napade: IP Source Guard

- Koristi DHCP snooping binding tabelu

```
sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)   Type            VLAN  Interface
------------------  --------------- ----------   -------------   ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10     193185       dhcp-snooping   4     FastEthernet3/18
```

- Gleda MacAddress i IpAddress kako bi proverio da li se nalaze u tabeli, ako ne, paket se odbacuje

Kontramere za Spoofing napade: IP Source Guard

Konfiguracija IP Source Guard

- DHCP snooping mora biti konfigurisan kako bi izgradili tabelu
- IP Source Guard se konfigurise na portu
- IP Source Guard sa MAC ne uči MAC od povezanog uređaja već od DHCP offer
- Svega nekoliko tipova DHCP servera podržavaju Option 82 za DHCP

Clearing Up Source Guard

- MAC i IP provera može biti setovana zajedno i odvojeno
  - Za IP
    - Radiće sa informacijama u binding tabeli
  - Za MAC
    - Moramo imati Option 82-enabled DHCP server (Microsoft ne podržava Option 82)
    - Svi Layer 3 uređaji između DHCP klijenta i HCP servera treba da budu konfigurisani da veruju Option 82 DHCP request: **ip dhcp relay information trust**

Kontramere za Spoofing napade: IP Source Guard

IP Source Guard

IP Source Guard Configuration IP Checking Only (No Opt 82) What most Enterprises Will Run

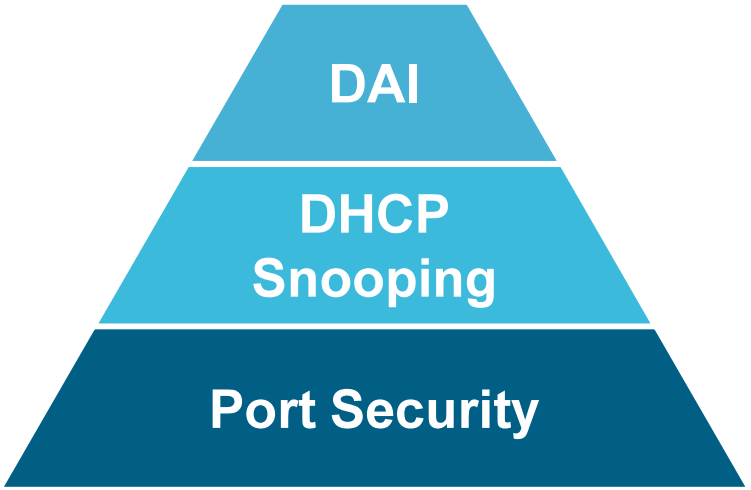
```
Cisco IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
Interface Commands
ip verify source vlan dhcp-snooping
```

IP Source Guard Configuration IP/MAC Checking Only (Opt 82)

```
Cisco IOS
Global Commands
ip dhcp snooping vlan 4,104
ip dhcp snooping information option
ip dhcp snooping
Interface Commands
ip verify source vlan dhcp-snooping
   port-security
```

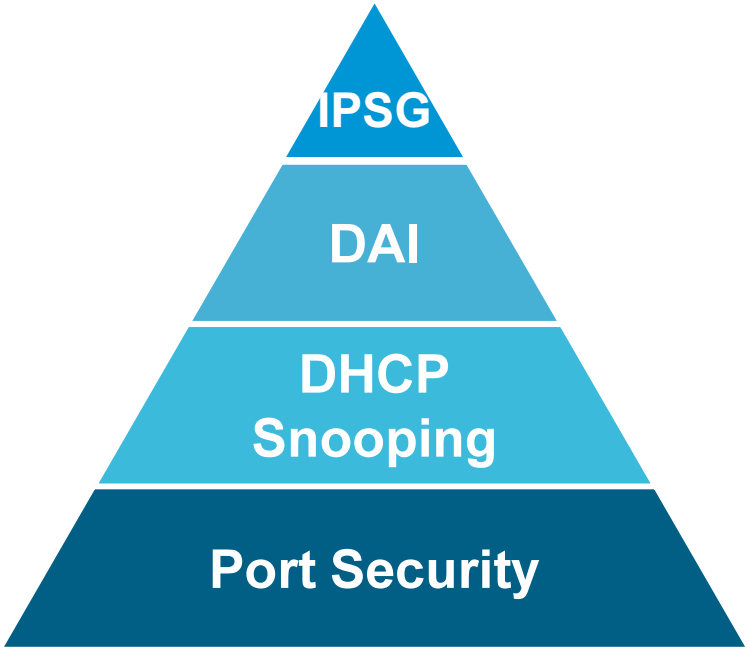
Izgradnja slojeva-piramide bezbednosti

- Port Security sprečava CAM napade(i neke DHCP starvation napade)
- DHCP snooping sprečava rogue DHCP server napade
- Dynamic ARP inspection sprečava ARP napade



Izgradnja slojeva-piramide bezbednosti

- Port Security sprečava CAM napade(i neke DHCP starvation napade)
- DHCP snooping sprečava rogue DHCP server napade
- Dynamic ARP inspection sprečava ARP napade
- IP Source Guard sprečava IP/MAC spoofing

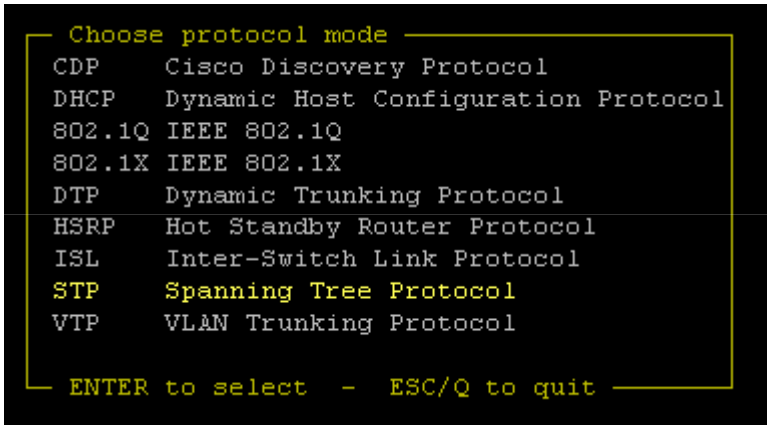


Agenda

- Pregled L2 napada
- Napadi i kontramere
  - VLAN Hopping
  - MAC napadi
  - DHCP napadi
  - ARP napadi
  - Spoofing napadi
  - Napadi na druge protokole
- Zaključak

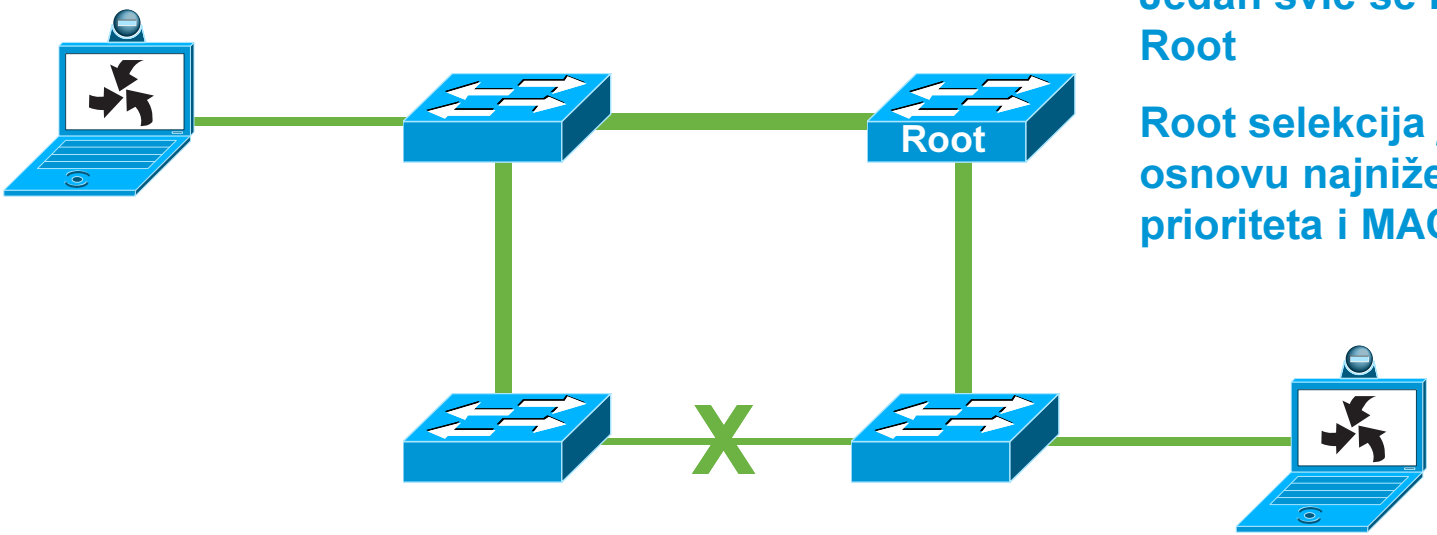
Drugi Protokoli?

- Yersinia može pomoći oko:
  - CDP
  - DHCP
  - 802.1Q
  - 802.1X
  - DTP
  - HSRP
  - STP
  - ISL
  - VTP



Spanning Tree osnove

- STP svrha : održavanje loop-free topologije u redundantnoj Layer 2 infrastrukturi



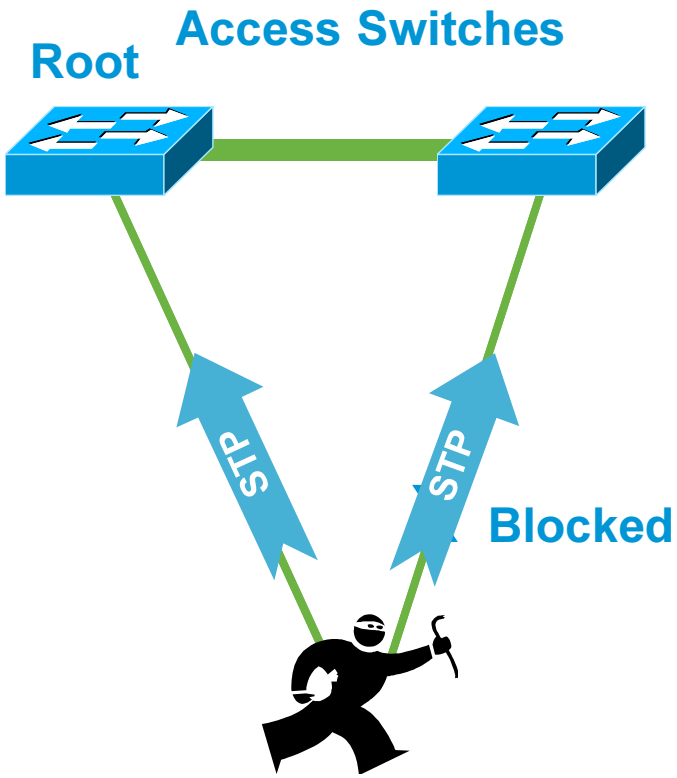
Jedan svič se bira za Root

Root selekcija je na osnovu najnižeg prioriteta i MAC

- STP je veoma prost; poruke se šalju korišćenjem Bridge Protocol Data Unit (BPDU); osnovne poruke sadrže: konfiguraciju, topology change notification/acknowledgment (TCN/TCA);
- Sprečavanje da broadcast saobraćaj ne preraste u *storm*

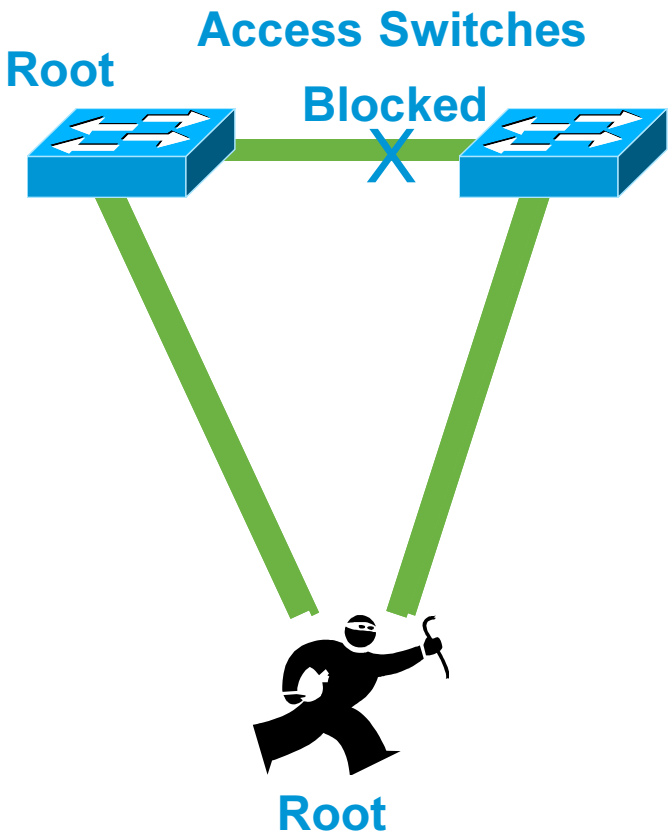
Spanning Tree napad

- Špalju se BPDU poruke da bi postao root bridge



Spanning Tree napad

- Špalju se BPDU poruke da bi postao root bridge
  - Napadač vidi frejmove koje ne bi trebalo
    - MITM, DoS napadi su mogući
    - Zahteva da je napadač *dual homed* na dva različita sviča



Sprečavanje STP napada

- Nikako ne isključivasti STP, petlje su potencijalno novi napad
- BPDU guard
- Treba da radi na svim *user facing* portovima

  Disable port - po detekciji BPDU poruke na portu

  Globalno enable-ovan na svim portfast portovima

  Dostupan na Cisco Catalyst OS 5.4.1 za Cisco Catalyst 2000 Series, Cisco Catalyst 4000 Series, Cisco Catalyst 5000 Series, i Cisco Catalyst 6000 Series; 12.0XE za native Cisco IOS 6000 Series; 12.1(8a)EW za Cisco 4000 Series IOS; 12.1(4)EA1 za 3550; 12.1(6)EA2 za 2950

```
CatOS> (enable)set spantree portfast bpdu-guard enable
IOS(config)#spanning-tree portfast bpduguard
```

Sprečavanje STP napada

- Root Guard

  Disable port koji bi da postane root bridge na osnovui svojih BPDU oglašavanja

  Konfigurisan na *per port* bazi

  Dostupan na Cisco Catalyst OS 6.1.1 za Cisco Catalyst 29XX, Cisco Catalyst 4000 Series, Cisco Catalyst 5000 Series, Cisco Catalyst 6000 Series; 12.0(7) XE za native Cisco IOS 6000 Series, 12.1(8a)EW for 4K Cisco IOS; 29/3500XL u12.0(5)XU; 3550 u12.1(4)EA1; 2950 u 12.1(6)EA2

```
CatOS> (enable) set spantree guard root 1/1
IOS(config)#spanning-tree guard root (or rootguard)
```

Agenda

- Pregled L2 napada
- Napadi i kontramere
  - VLAN Hopping
  - MAC napad
  - DHCP napad
  - ARP napad
  - Spoofing napad
  - Generalni napadi
- Zaključak

Važna napomena !

- Ako nemamo binding table entry, saobraćaj neće biti moguć na portu sa uključenim
  - Dynamic ARP inspection
  - IP Source Guard

Layer 2 Security Best Practices (1/2)

- Manadžment svičeva na siguran način (SSH, OOB, permit lists, etc.)
- Ne koristiti VLAN 1
- Staviti sve user portove u nontrunking (sem za Cisco VoIP)
- Uključiti port-security na user portovima
- Koristiti ARP security (ARP inspection, IDS, etc.)

Layer 2 Security Best Practices (2/2)

- Uključiti STP zaštitu
  (BPDU Guard, Root Guard)
- Zaštita od DHCP napada
  (DHCP snooping, VACL)
- Korisiti MD5 authentication za VTP
- Korisiti CDP samo ako ne potrebno – korisno za IPT
- Disable se portove koji se ne koriste i staviti ih u VLAN koji se ne koristi

Cisco live!

Registrujte se za Cisco Live Networkers u Londonu ili Bahreinu!
Više informacija na:
http://www.ciscolive.com/