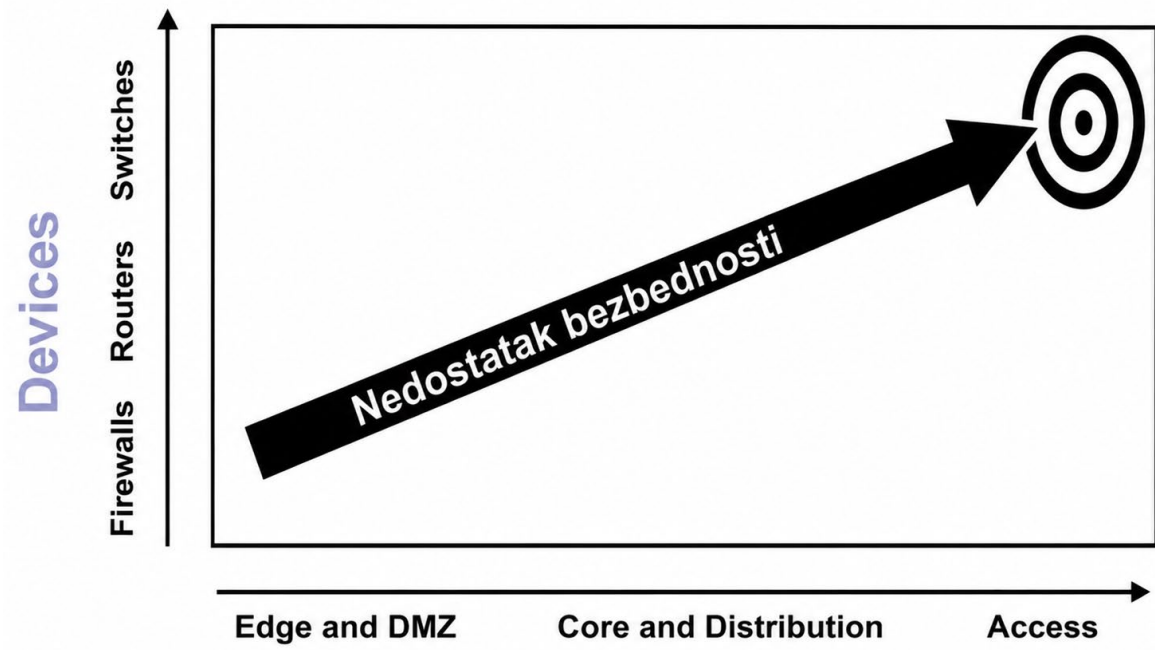
SPOOFING NAPADI

Predmet: Bezbednost aplikacija

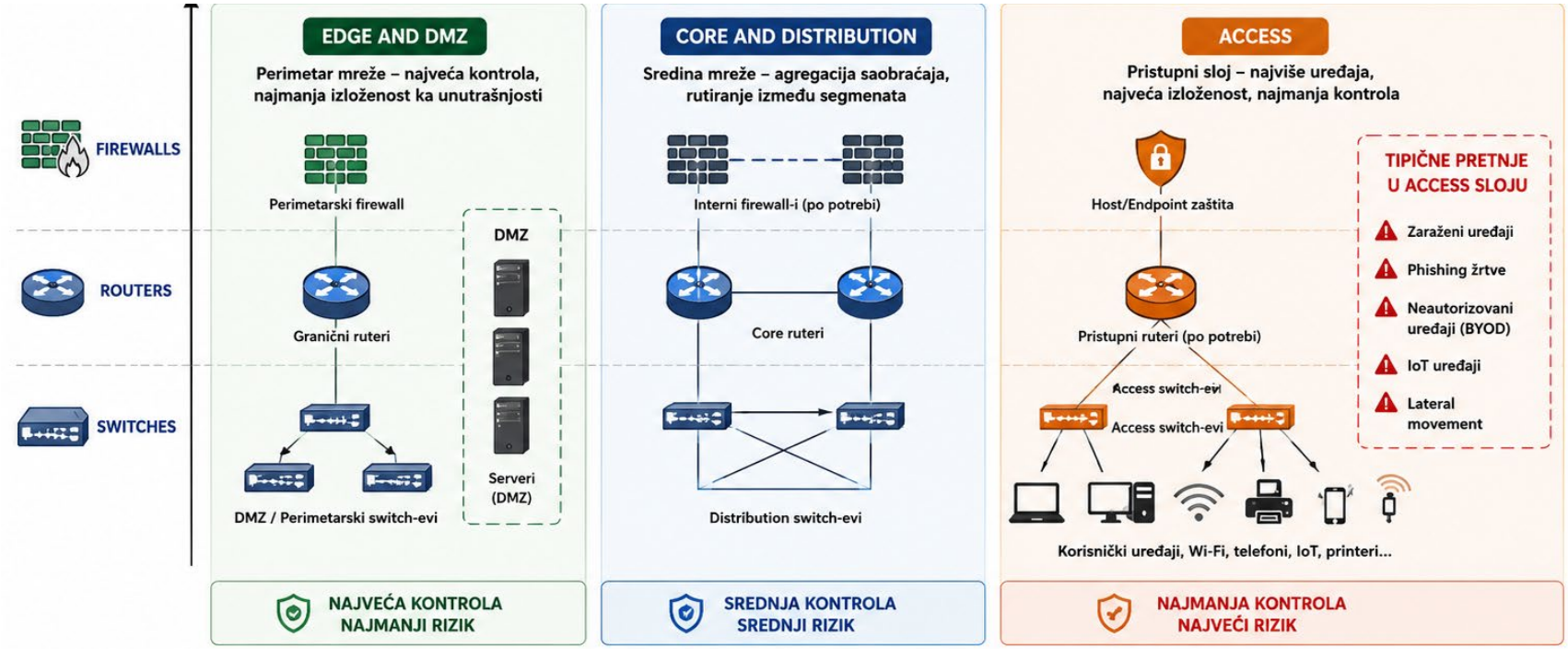
Predavač: dr Dušan Stefanović

ODAKLE NAPADI VREBAJU



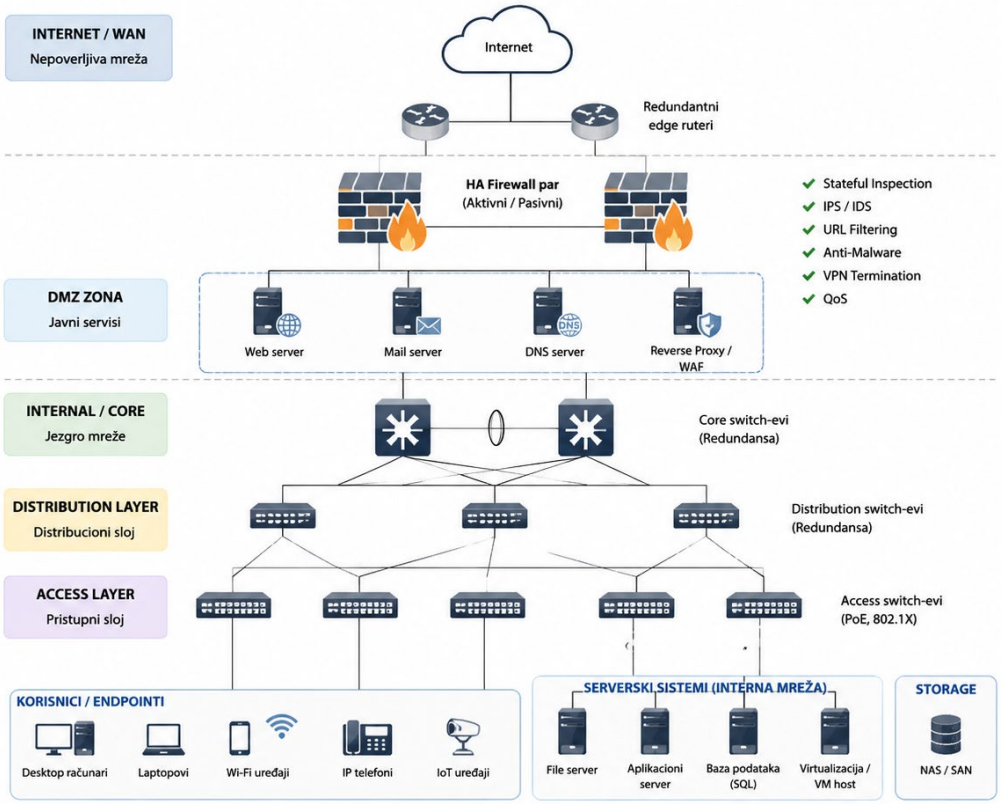
- Pažnja sistem inženjera okrenuta je napadima koji dolaze spolja što potvrđuje grafik iznad

ODAKLE NAPADI VREBAJU



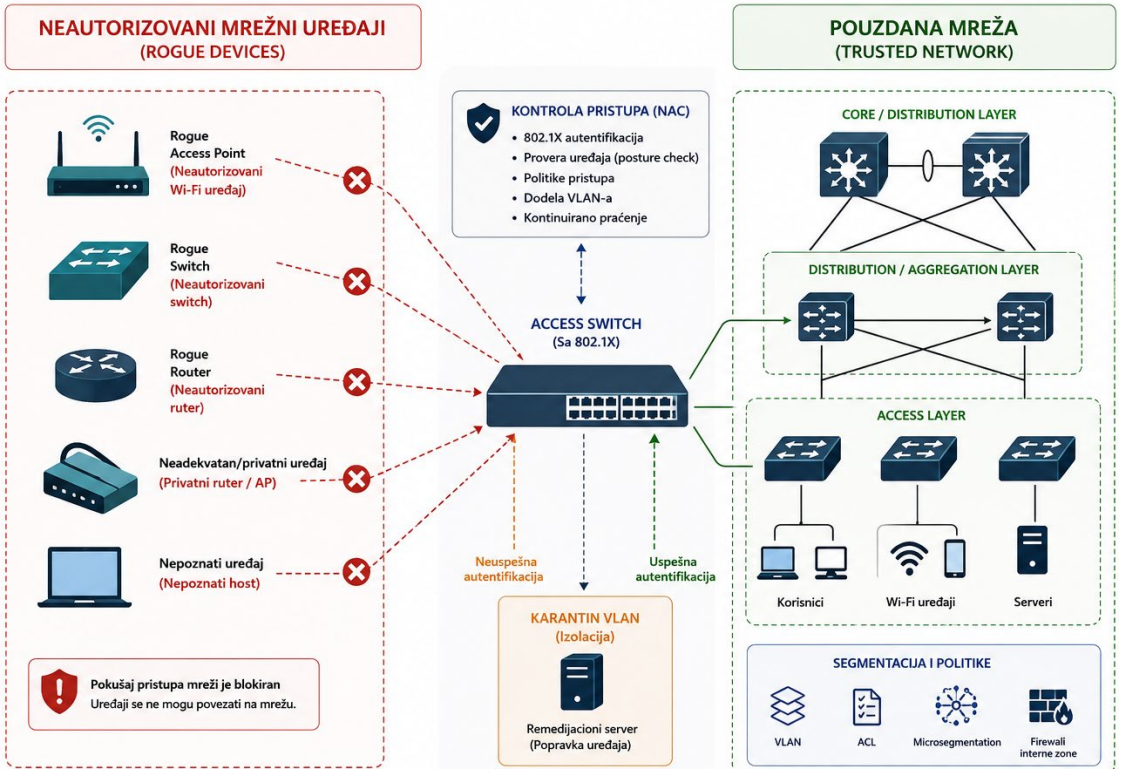
PODRAZUMEVANA ZAŠTITA NA UREĐAJIMA

- Podrazumevano stanje mrežne opreme:
  - **Firewall** (nalazi se na granici između spoljne i unutrašnje mreže)
    - Default: Kompletan saobraćaj je zabranjen, mora se konfigurisati da dozvoli komunikaciju.
  - **Ruteri i svičevi** (čine mrežnu infrastrukturu kompanije)
    - Default: Nisu podešeni da štite od napada, moraju se konfiguristi za zaštitu od napada.



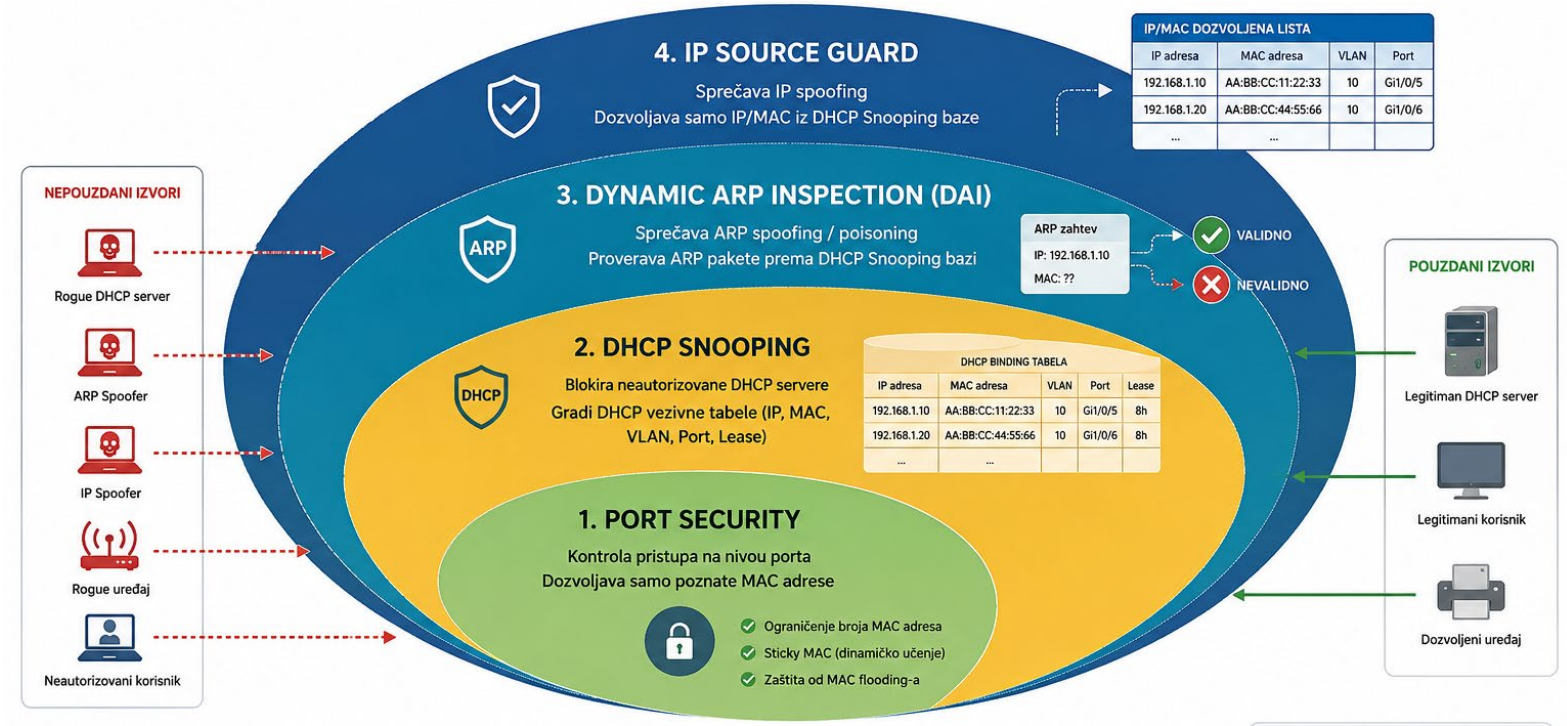
ZLONAMERNI MREŽNI UREĐAJI

– Zlonamerni mrežni uređaji mogu biti:
  - Wireless hub
  - Bežični uređaji
  - Pristupni svičevi
  - Hub-ovi
– Ovi uređaji se povezuju na Access svičeve.



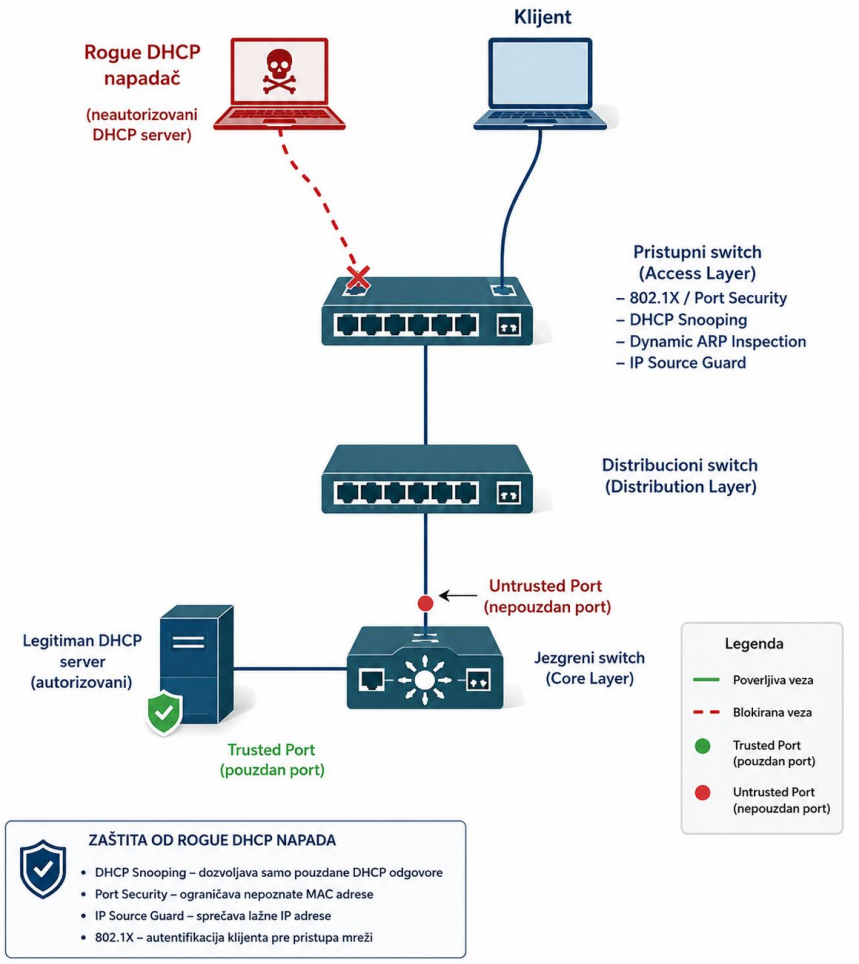
SPOOF NAPADI

- Napadač može da pošalje lažne (spoof) informacije kako bi prevario svič ili računar.
- Najčešći cilj napadača je da postane man in the middle.
- Tehnike koji nas štite od spoof napada su:

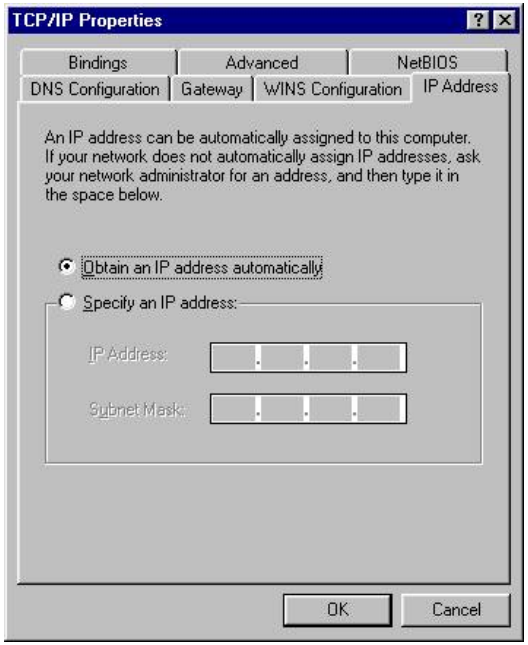


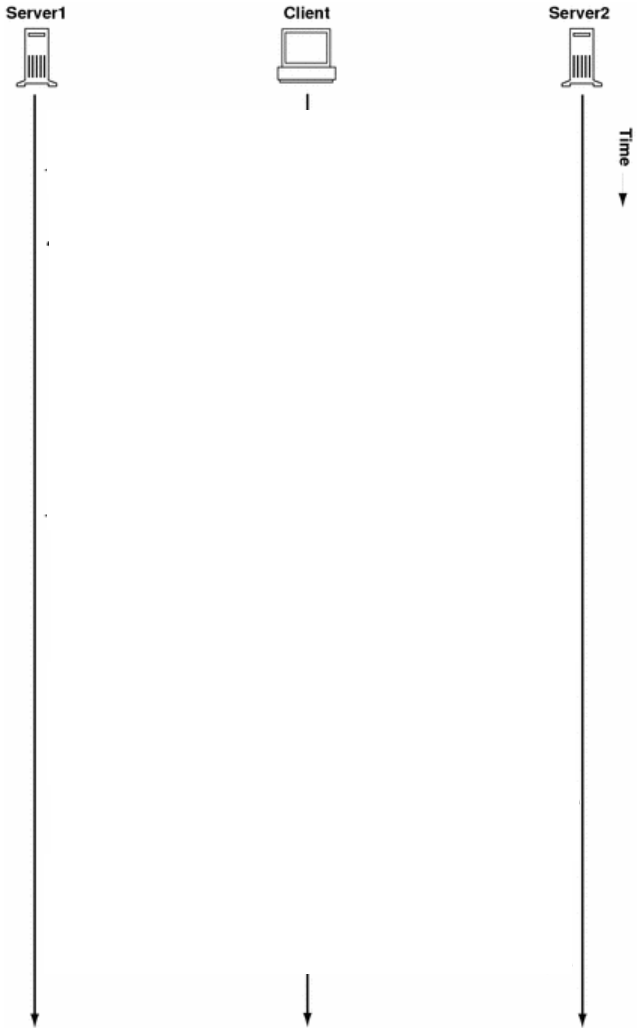
DHCP SPOOF NAPAD

- **Lažni (spoof) DHCP** uređaj odgovara na **DHCP requests** poruke koje šalju DHCP klijenti.
- Lažni **DHCP server nudi**:
  - ***IP adresu/Masku***
  - ***Default gateway***
  - ***Domain Name System (DNS) server***
- Klijenti prosleđuju pakete lažnom DHCP serveru (napadač) koji ih rutira ka željenom odredištu.
  - "**Man-in-the-middle**" napad .

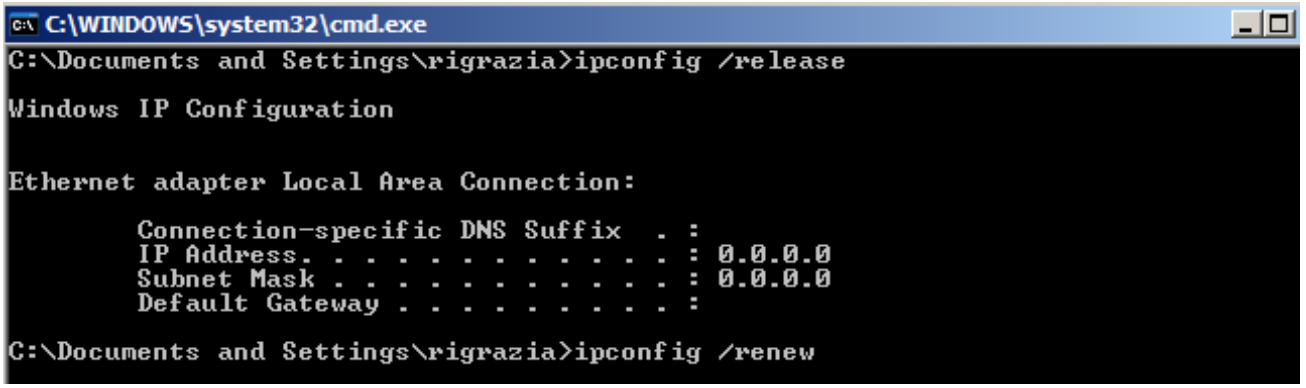


DHCP SERVIS


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel


Server1
Client
Server2
Time

Pokretanje DHCP Servisa

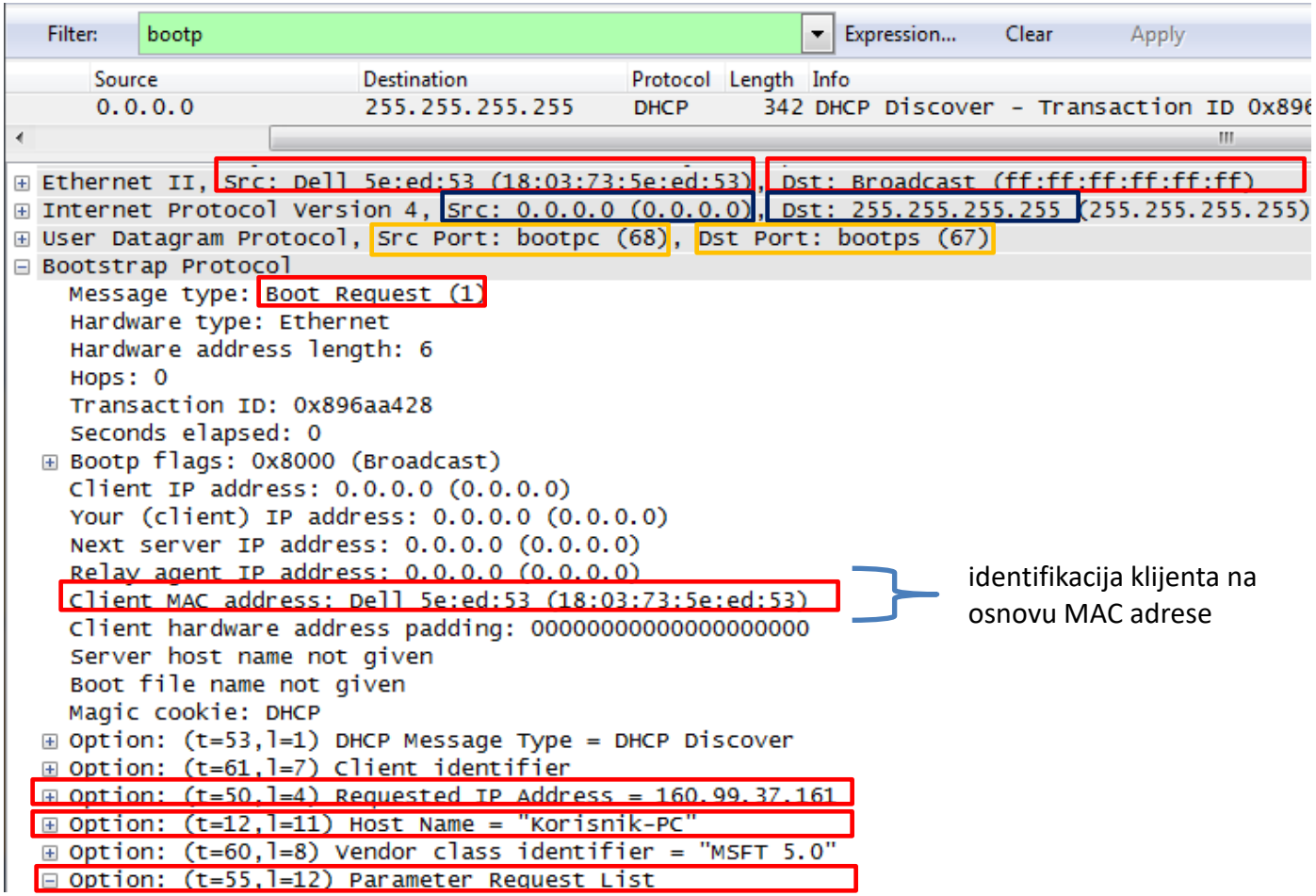


DHCP servis na klijentskom računaru se startuje nakon podizanja OS-a ili upotrebom komandi:

ipconfig /release

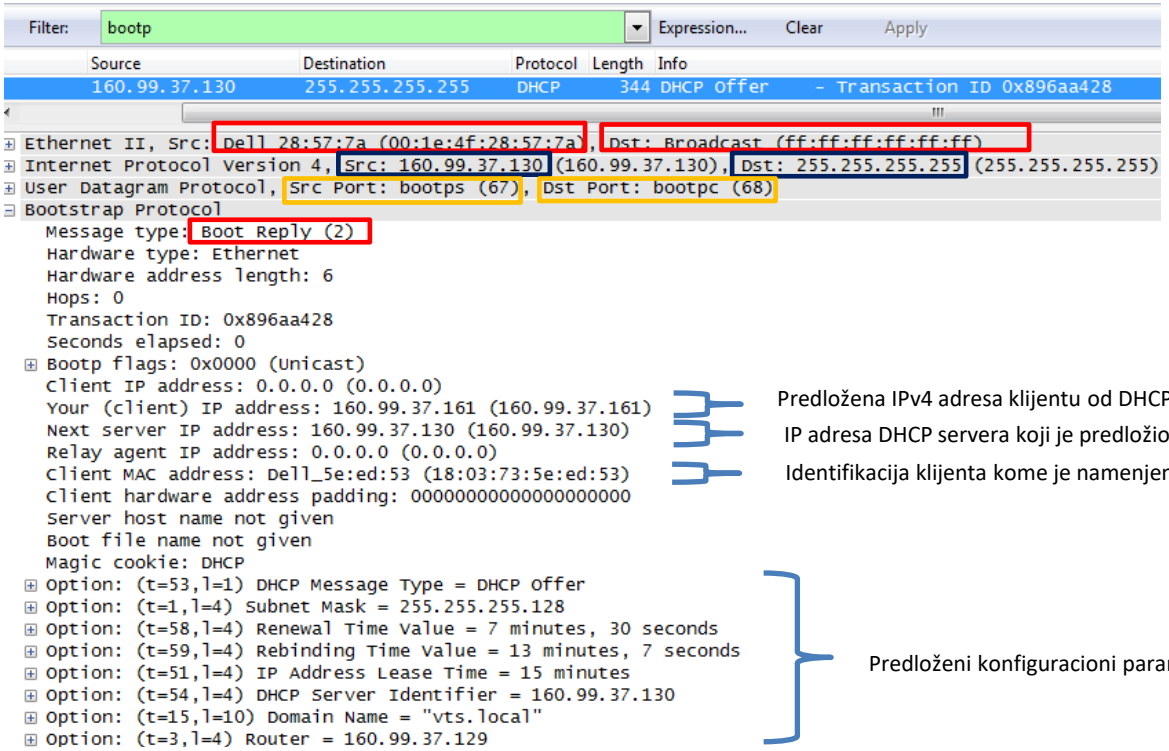
ipconfig /renew

DHCP Discovery Poruka



identifikacija klijenta na osnovu MAC adrese

DHCP OFFER



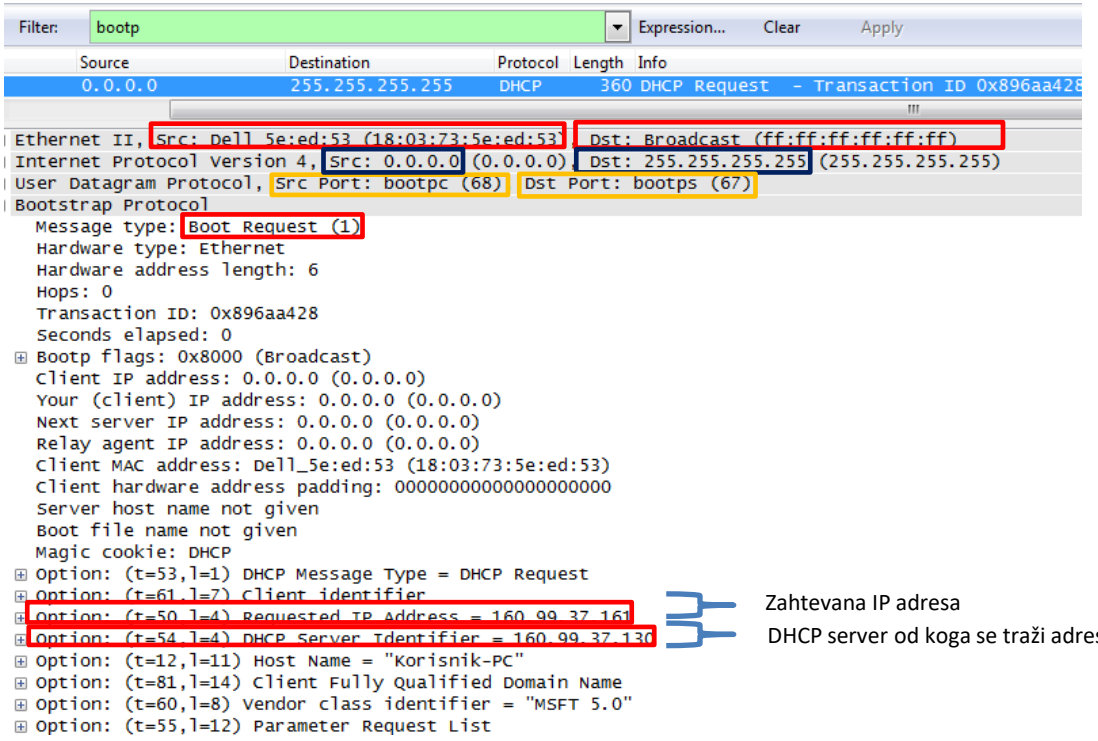
Predložena IPv4 adresa klijentu od DHCP servera

IP adresa DHCP servera koji je predložio adresu

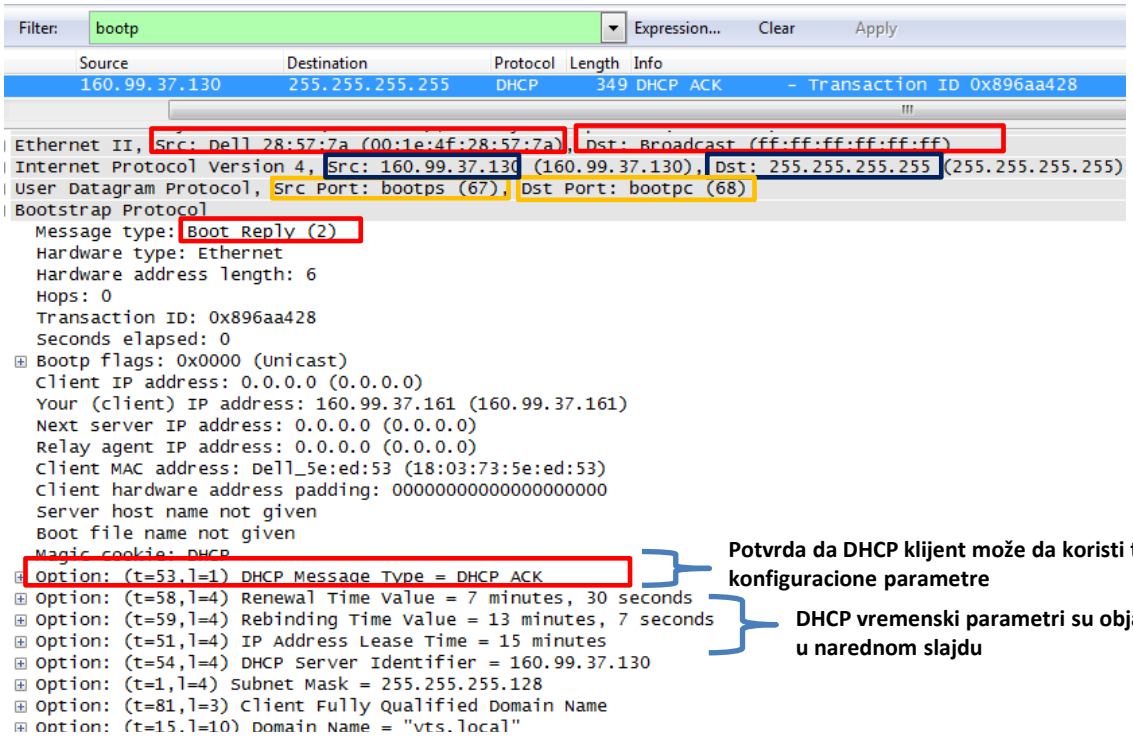
Identifikacija klijenta kome je namenjena ponuda

Predloženi konfiguracioni parametri

DHCP REQUEST



DHCP ACK

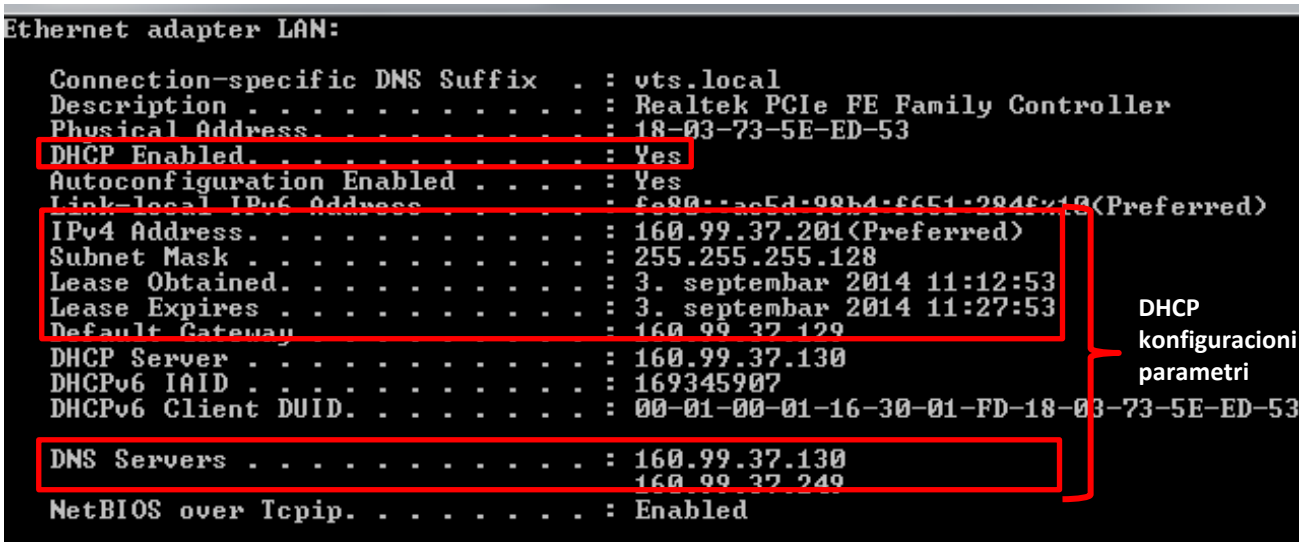


Potvrda da DHCP klijent može da koristi tražene konfiguracione parametre

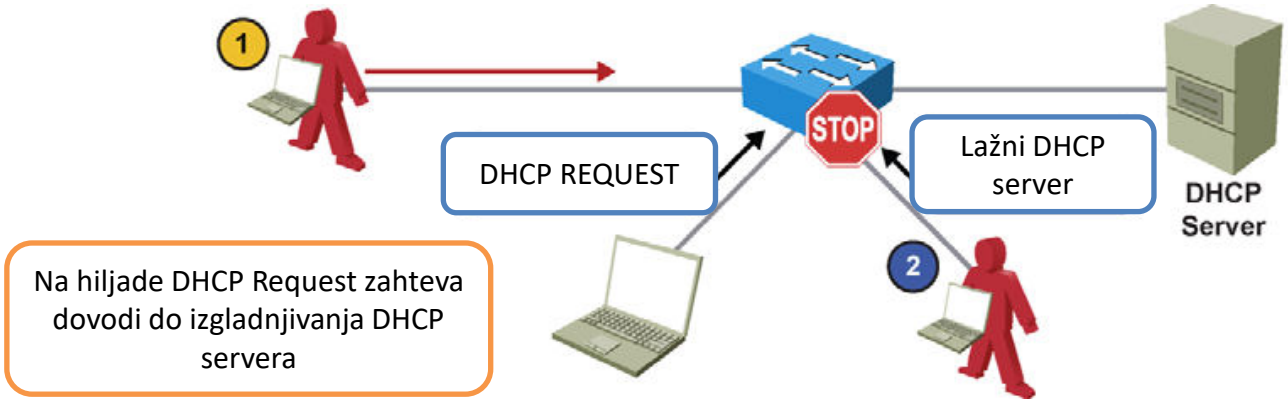
DHCP vremenski parametri su objašnjeni u narednom slajdu

Rezlutat DHCP Procesa

IPCONFIG /ALL

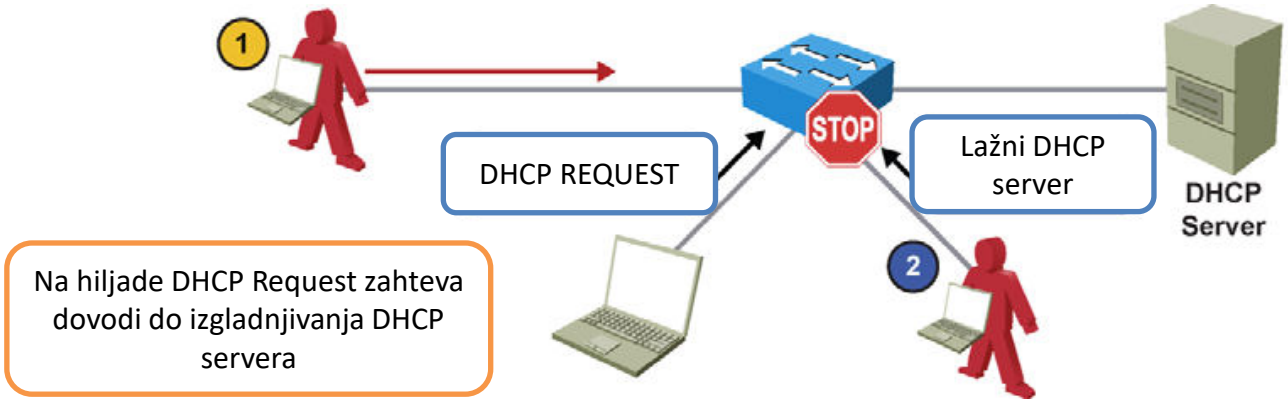


DHCP STARVATION – Scenario 1



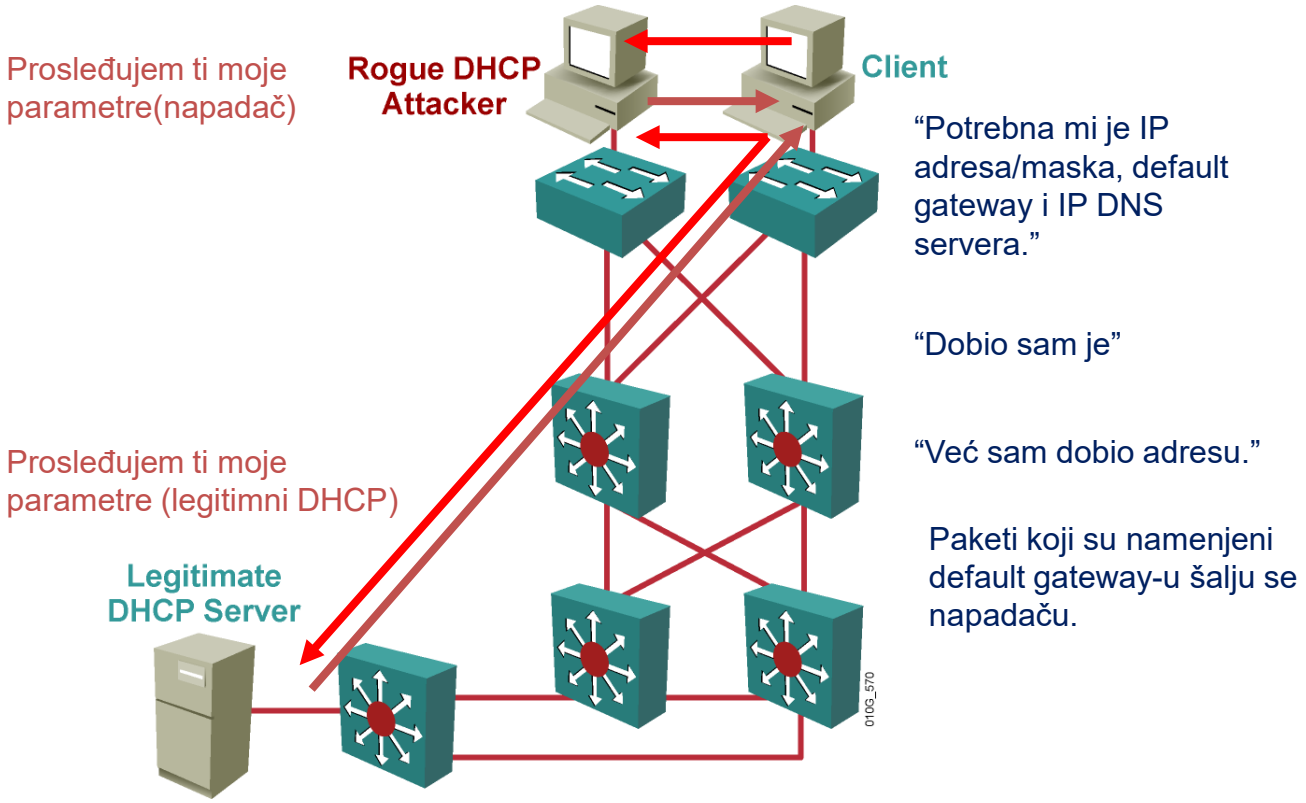
- U ovom scenariju napadač sprovodi DoS napad šaljući na hiljade DHCP request poruka.
- DHCP server nema mogućnost da detektuje pravi(validan) zahtev, može da se desi da DHCP server ostane bez validnih IP adresa.
- Rezlutat je da legitimni klijent ne može da dobije IP adresu od DHCP-a.

DHCP SPOOFING – Scenario 2



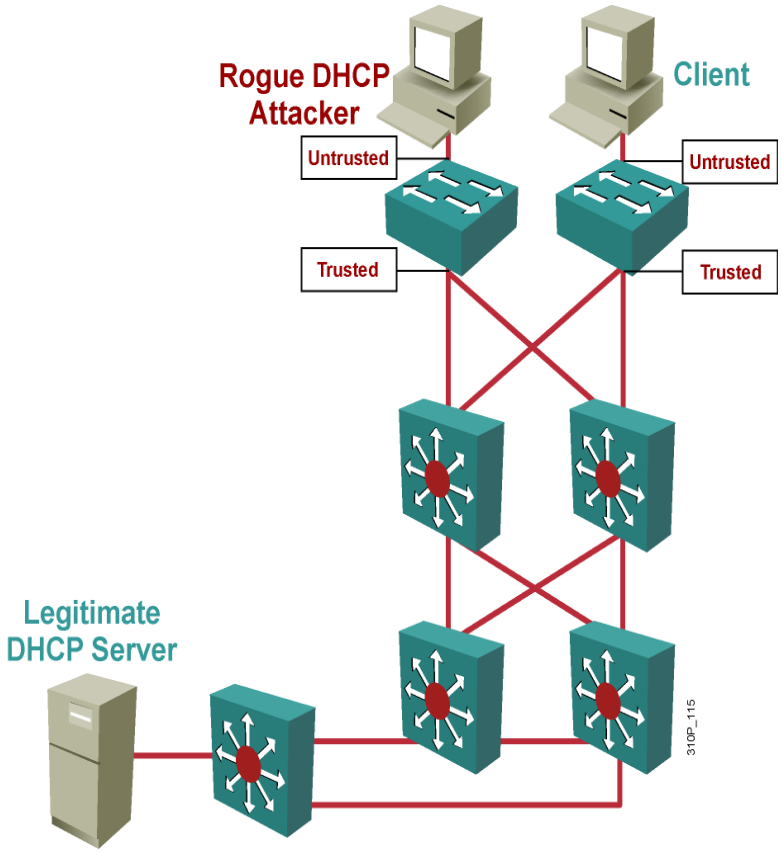
- U drugom scenariju napadač emulira ulogu DHCP servera
- Na ovaj način napadač prosleđuje DHCP klijentima pogrešne informacije o default gateway-u koji ukazuje na IP adresu napadača.
- Napadač realizuje *man-in-the-middle* napad i može na ovaj način da dođe u posed vrlo poverljivih informacija (lozinke) a pri tom korisnik nije svestan napada.

DHCP SPOOF NAPAD

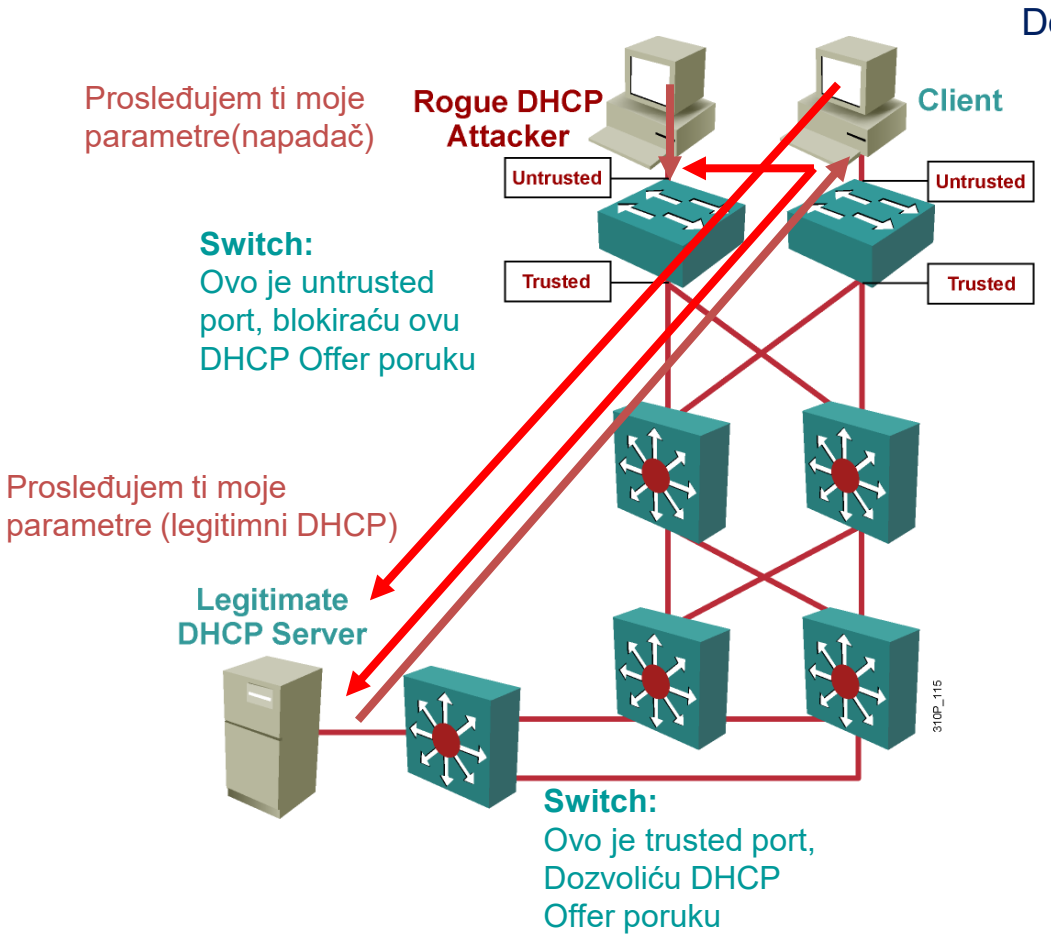


DHCP SNOOPING

- DHCP snooping je funkcionalnost Catalyst svičeva koja određuje koji portovi na sviču mogu da odgovaraju na DHCP request poruke.
- Portovi se identifikuju kao **trusted** i **untrusted**.
  - **Trusted** port prima sve DHCP poruke
  - **Untrusted** port može da primi samo poruke koje šalju DHCP klijenti(DHCP Request)
    - Ukoliko napadač sa untrusted porta pokuša da pošalje *DHCP respone* poruku, port će biti deaktiviran(error disable).
    - **DHCP binding tabela** se formira za untrusted portove
      - **Klijent *MAC adresa, IP adresa, lease time, binding type, VLAN number i port ID* se čuvaju.**
- Iz perspektive DHCP snooping opcije, untrusted access portovi ne prosleđuju poruke koje šalju DHCP serveri (DHCPOFFER, DHCPACK ili DHCPNAK).



DHCP SNOOPING



DHCP Snooping - Konfiguracija

DHCP SNOOPING

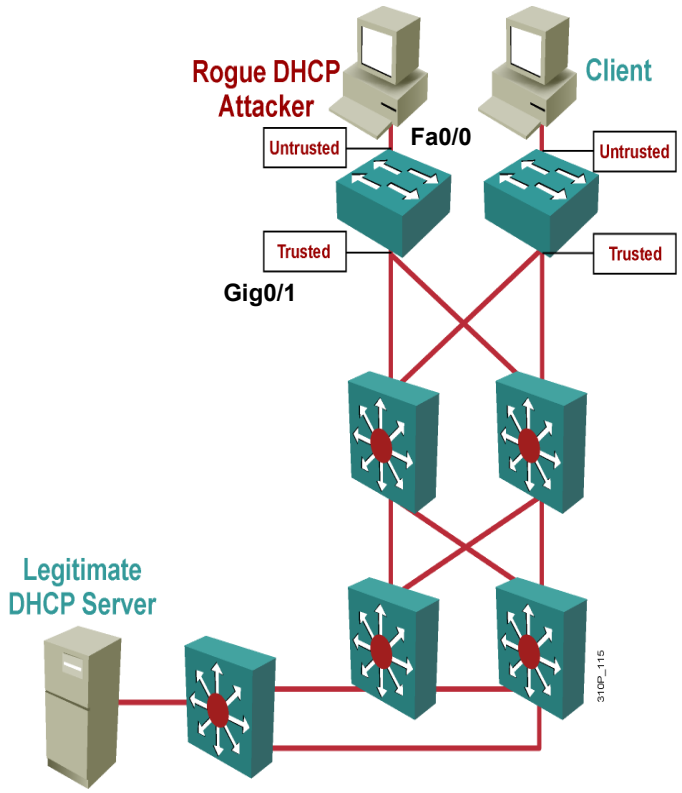
Korak 1:
Switch(config)# **ip dhcp snooping**

Korak 2:
Switch(config)# **ip dhcp snooping vlan 10 50**

Korak 3:
Switch(config)# **interface gig 0/1**
Switch(config-if)# **ip dhcp snooping trust**

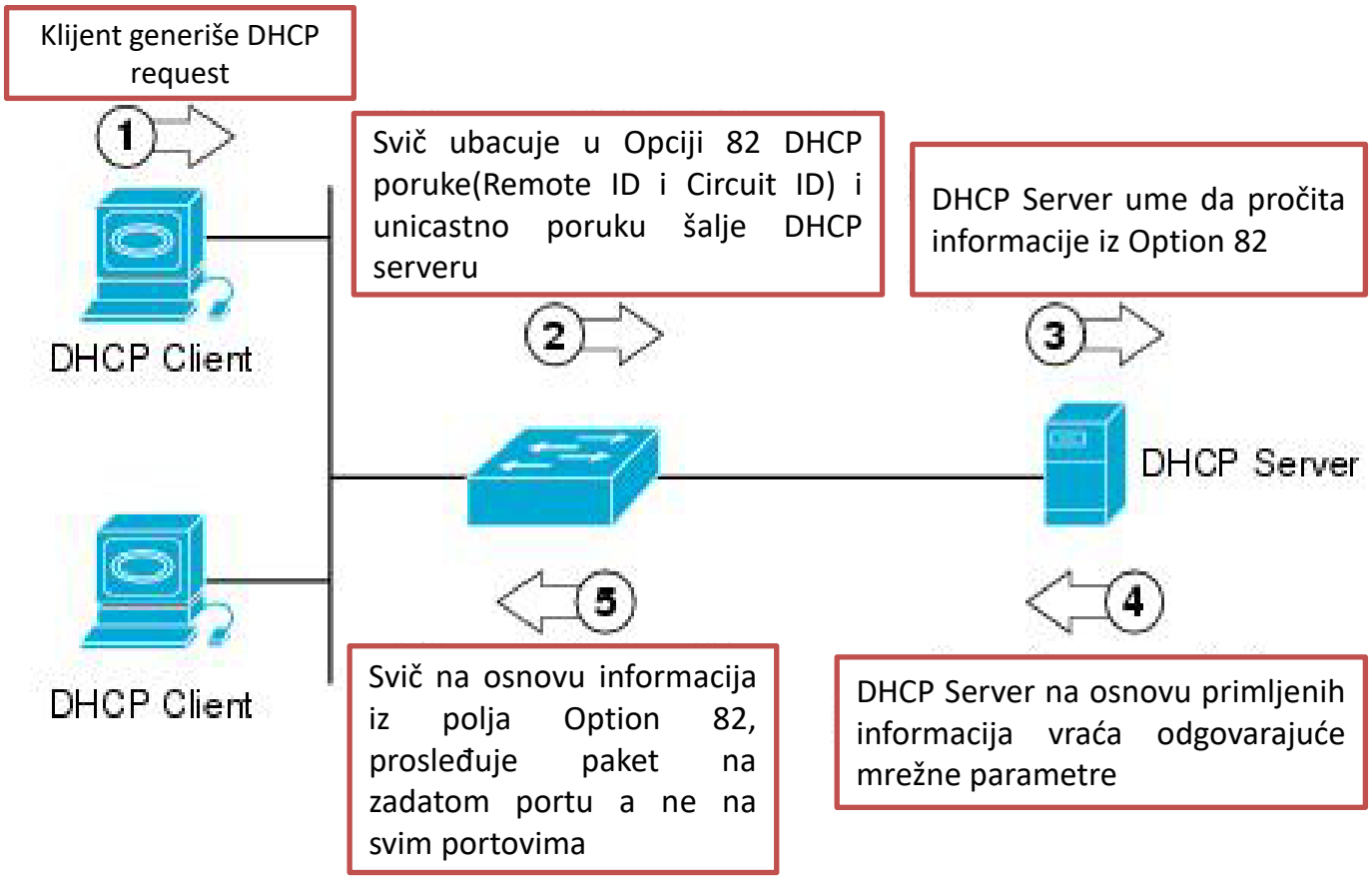
Korak 4:
Za portove koji su untrusted prihvatljiv je neograničen broj DHCP zahteva što može da predstavlja problem
Switch(config-if)# **ip dhcp snooping limit rate**

Korak 5:
Svič se može konfigurisati da koristi option 82.
To je DHCP Relay Agent Information Option
Kada se zahtev za DHCP-om presretne na untrusted portu, svič upisuje svoju **MAC adresu i broj porta u polju za option 82** koje obezbeđuje dodatne informacije o klijentu koji je poslao DHCP zahtev.
Svič presreće odgovor i na osnovu option 82 parametra prosleđuje paket tačnom portu u suprotnom on neće znati kom portu da prosledi paket i odbacuje paket.
Ova opcija je uključena(default)
Switch(config)#**ip dhcp snooping information option**



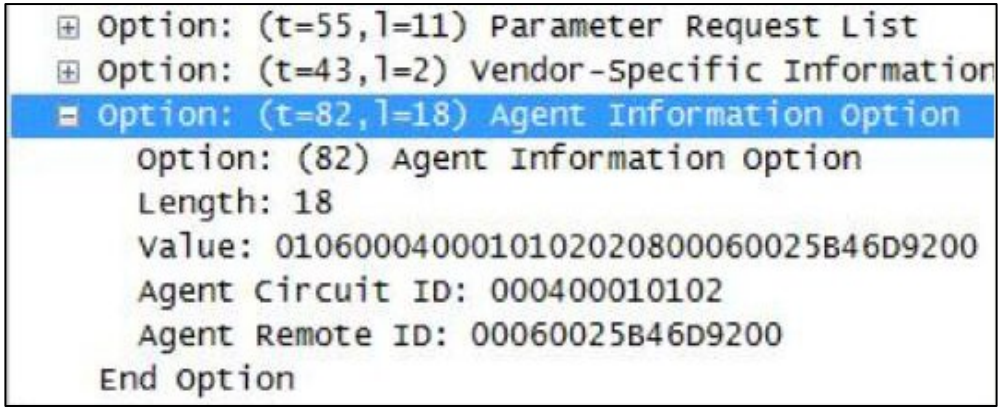
Svi interfejsi su untrasted (default).

DHCP OPTION 82



DHCP OPTION 82

- DHCP Snooping alat automatski uključuje opciju 82 koja se koristi za identifikaciju.
- Kada svič pošalje DHCP Request poruku, svič će dodati opcije:
  - *Client-id* je broj porta
  - *Remote-id* je identifikacija sviča (mac adresa)
- Na ovaj način paket može da se prati, kada svič primi odgovor od DHCP servera moći će da paket prosledi tačnom portu
- Option 82 je namenjena za DHCP Relay Agent, služi da se od broadcast DHCP poruke napravi unicast.



DHCP OPTION 82 - Problem

- Problem kod korišćenja option 82 kod DHCP snooping metode je što svič ne upisuje gateway ip adresu.
- Takvu DHCP poruku server smatra nepotpunom.
- Da bi DHCP server ovakvu poruku prihvatio potrebno je na Cisco DHCP serveru uneti komandu:

```
R(config)# ip dhcp relay information trust-all
```

- Problem se rešava na jedan od dva načina:
  - Rešenje 1: na sviču isključimo opciju 82
  - Rešenje 2: na DHCP serveru dozvolimo nepotpunu DHCP poruku.
- Ukoliko se opredelimo za Rešenje 1, problem se javlja ukoliko na tom sviču koristimo IPSG ili DAI jer DHCP Snooping tabela sadrži za svaki port mac,ip adresu i lease time.

Verifikacija DHCP SNOOPING

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP Snooping is configured on the following VLANs:10 30-40 50
Insertion of option 82 information is enabled.
Interface            Trusted        Rate limit (pps)
---------            -------        ----------------
GigibitEthernet0/1   yes            none
FastEthernet0/1      no             20

Switch#
```

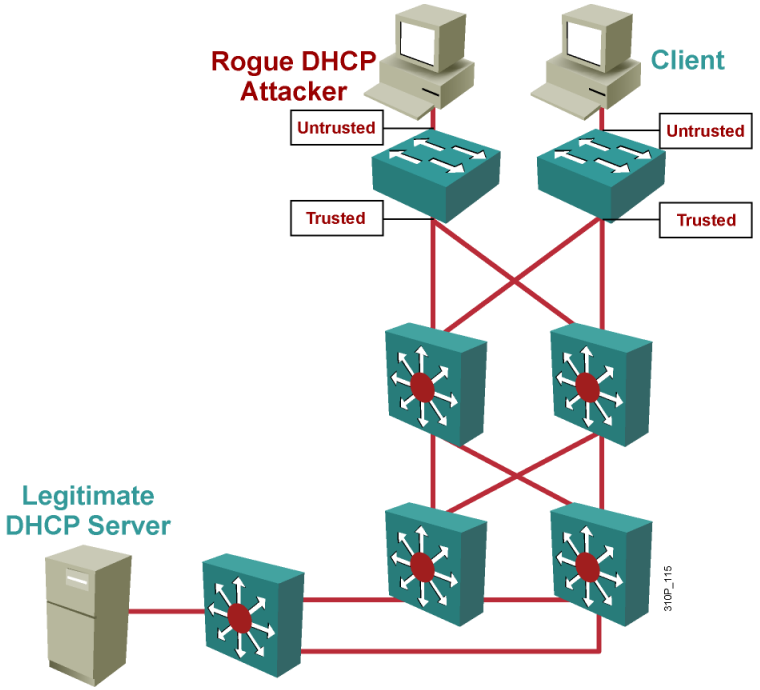
Switch# **show ip dhcp snooping binding**

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:01:00:01:00:01	10.10.10.1	4995	dhcp-snooping	10	FastEthernet2/1

- DHCP Snooping baza sadrži DHCP vezivanje za svakog klijenta.
- Baza za svakog klijenta sadrži njegovu MAC adresu,IP adresu,lease time,...

IP SPOOF NAPAD
IP SOURCE GUARD

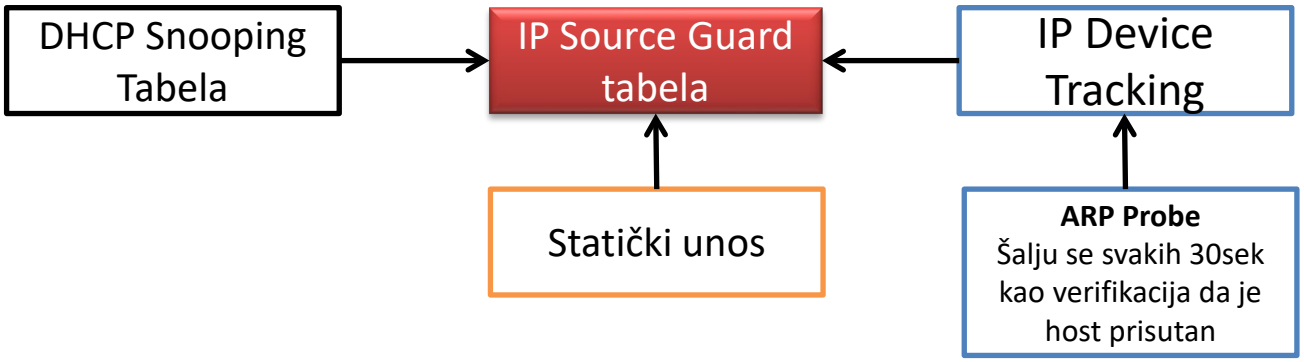
- IP Source Guard je sličan DHCP snooping opciji.
- Sprečava napad sa lažne IP adrese.
- Svič blokira sav IP saobraćaj koji dolazi na interfejs osim DHCP paketa koji su dozvoljeni od strane DHCP snooping opcije.
- Port access control list (ACL) se primenjuje na interfejsu.
- Port ACL dozvoljava samo IP saobraćaj sa source IP adresom koja se nalazi u IP *source binding* tabeli a odbija ostali saobraćaj.



IP source guard se konfiguriše na untrusted L2 interfejsima

IP SOURCE GUARD Tabela

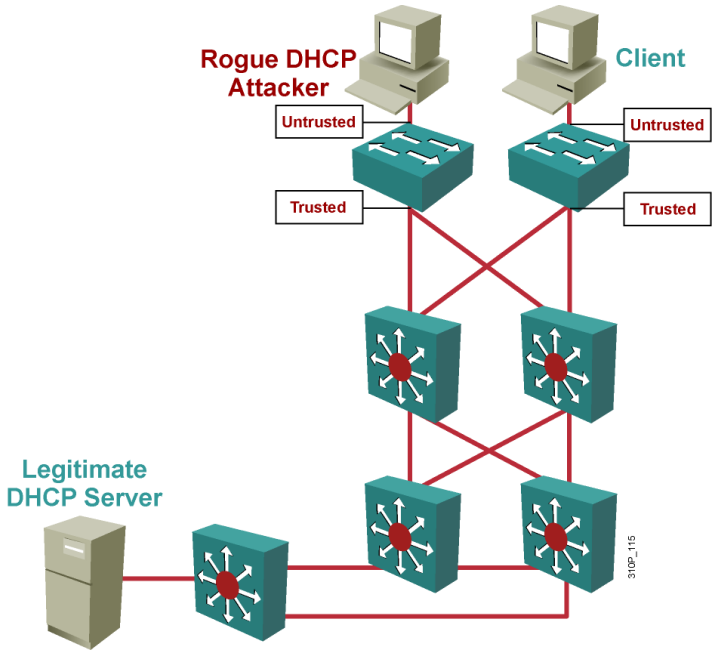
- U IPSG tabeli uključena je samo Layer 3 kontrola
- Layer 2 kontrola se uključuje dodavanjem Port-Security opcije
- Ne štiti nas od MITM napada, već od lažnih mac i ip adresa
- Metode formiranja IPSG tabele



- Ukoliko se koristi IP Device tracking opcija, tada se ne koristi DHCP Snooping opcija tj. moguće je DHCP Snooping tabelu kopirati u IP Device tracking tabelu a odatle u IPSG tabelu

IP SOURCE GUARD

- Paket koji dolazi na port sviča potrebno je da ispuni:
  - Source IP adresa bude identična IP adresi koja je naučena iz DHCP snooping baze ili statičkom unosu
  - Source MAC adresa mora da bude identična MAC adresi koju je svič naučio preko DHCP Snooping opcije



IP source guard se konfiguriše na untrusted L2 interfejsima

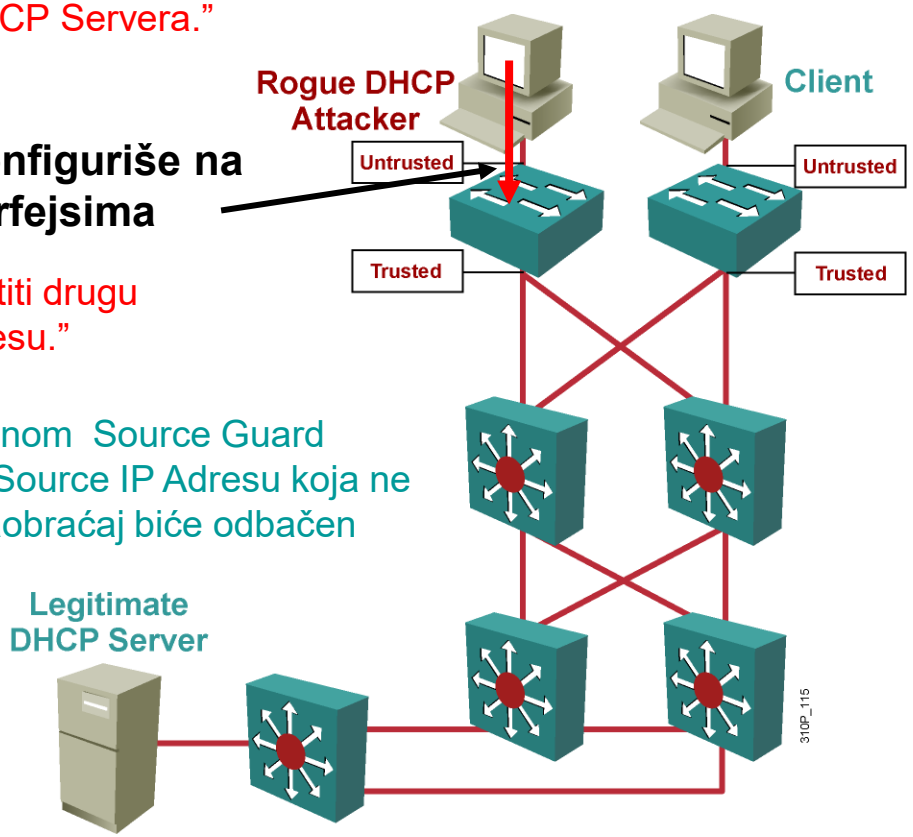
IP SOURCE GUARD

"Ja sam dobio IP adresu/mask, od DHCP Servera."

IP source guard se konfiguriše na untrusted L2 interfejsima

"Sada ću koristiti drugu Source IP Adresu."

Switch: Ovo je untrusted port, sa konfigurisanom Source Guard opcijom. Proveravam binding tabelu i tvoju Source IP Adresu koja ne odgovara onoj koju si dobio od DHCP-a. Saobraćaj biće odbačen



IP SOURCE GUARD - Aktivacija

Step 1	`Switch(config)# ip dhcp snooping`	Aktivacija DHCP snooping opcije
Step 2	`Switch(config)# ip dhcp snooping vlan number [number]`	Aktivacija DHCP snooping opcije za željene VLAN-ove
Step 3	`Switch(config)# ip dhcp snooping vlan number [number]`	Konfiguracija interfejsa (trusted/untrusted)
Step 4	`Switch(config-if)# ip verify source vlan dhcp-snooping port-security`	Aktivacija IP source guard opcije
Step 5	`Switch(config-if)# switchport port-security limit rate invalid-source-mac N`	Opciona opcija, podešava ograničenja za pakete koje šalje napadač.
Step 6	`Switch(config)# ip source binding ip-addr ip vlan number interface interface`	Konfiguracija IP adrese kojoj je dozvoljeno da se koristi na tom portu

IP SOURCE GUARD - Primer

Korak 1:
Switch(config)# **ip dhcp snooping**

Korak 2:
Switch(config)# **ip dhcp snooping vlan 10 50**

Korak 3:
Ukoliko želimo da detektujemo i lažne MAC adrese potrebno je da uključimo i port-security

Korak 4:
Za IP uređaje koji ne koriste DHCP potrebno je konfigurisati statičko IP Source vezivanje
Switch(config)# **ip source binding <mac adresa> vlan<vlan id> <ip adresa> <interfejs>**
Sw(config)# **ip dhcp snooping binding 0000.0000.0004 vlan 100 192.168.1.10 interface f0/5 expire [max]**

Korak 5:
- Potrebno je da omogućimo IPSG na jednom ili više interfejsa.
- Komanda *ip verify source proverava samo source IP adresu(default)*
- *Ukoliko daodamo* port-security vršiće se provera i source mac adrese **ali je potrebno konfigurisati port security opciju.**

Switch(config-if)# **ip verify source [port-security]**

Korak 6:
Prikaz interfejsa na kojima je primenjen IPSG.
Switch# **show ip source [interfejs]**

Korak 7:
Prikaz dinamičkih i statičkih ip source vezivanja
Switch# **show ip source binding**

IP SOURCE GUARD - Primer

- IP Source guard koji vrši filtriranje na osnovu source IP-a.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# ip verify source
```

- IP source guard koji vrši filtriranje na osnovu statičke source IP i MAC adrese za VLANove 10 i 11.

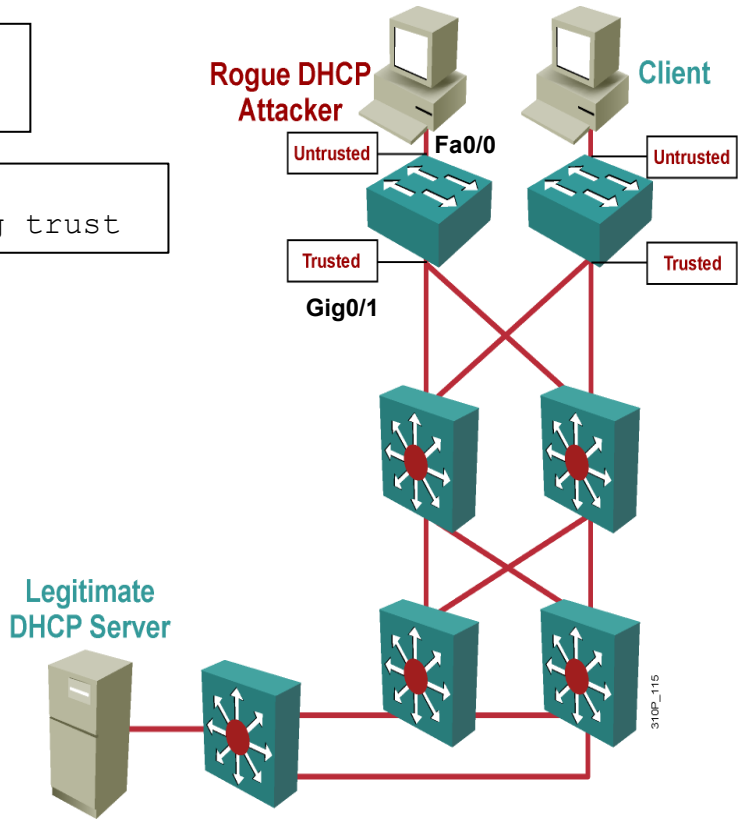
```
Switch(config)# interface fastethernet0/1
Switch(config-if)# ip verify source port-security

Switch(config)# ip source binding 0100.0022.0010 vlan 10
                10.0.0.2 interface gigabitethernet0/1

Switch(config)# ip source binding 0100.0230.0002 vlan 11
                 10.0.0.4 interface gigabitethernet0/1
```

IP SOURCE GUARD

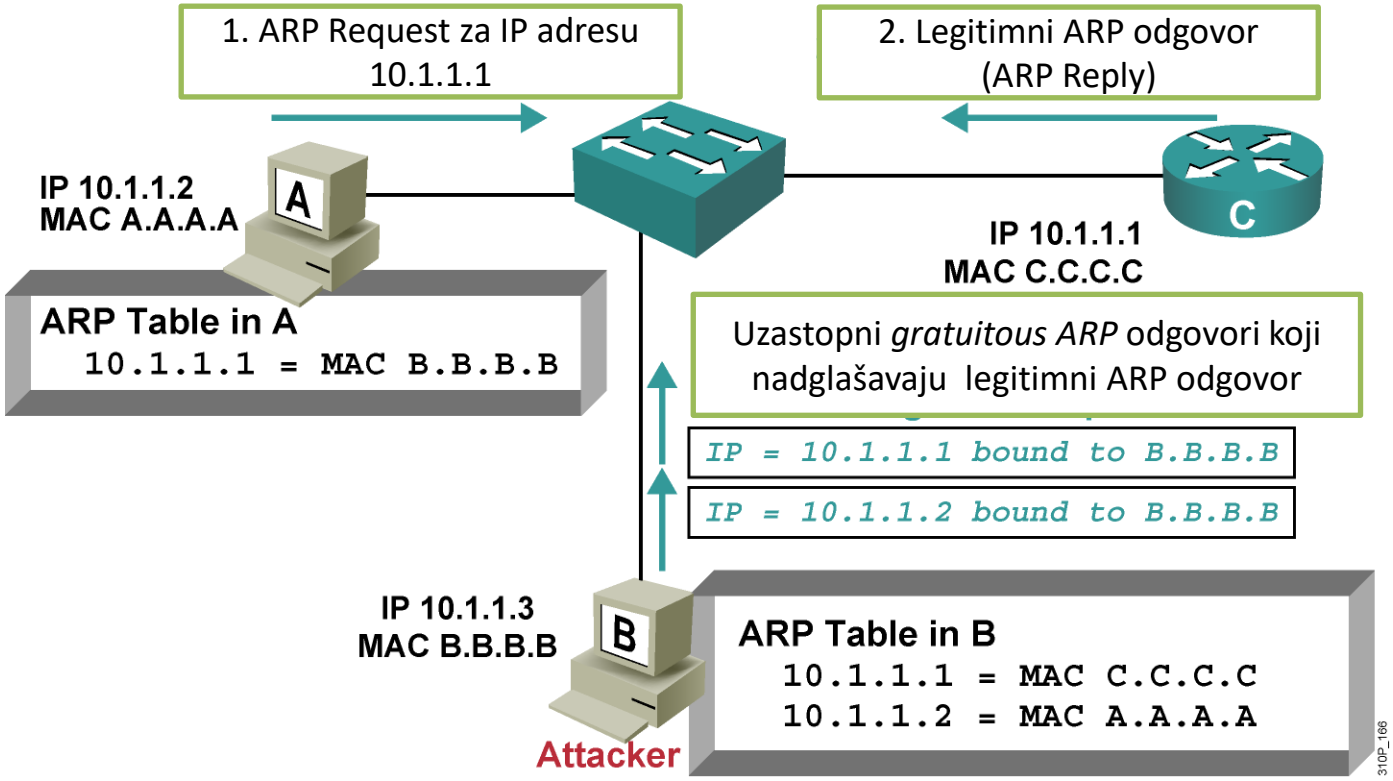
```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 50
```

```
Switch(config)# interface fa0/0
Switch(config-if)# ip verify source
```

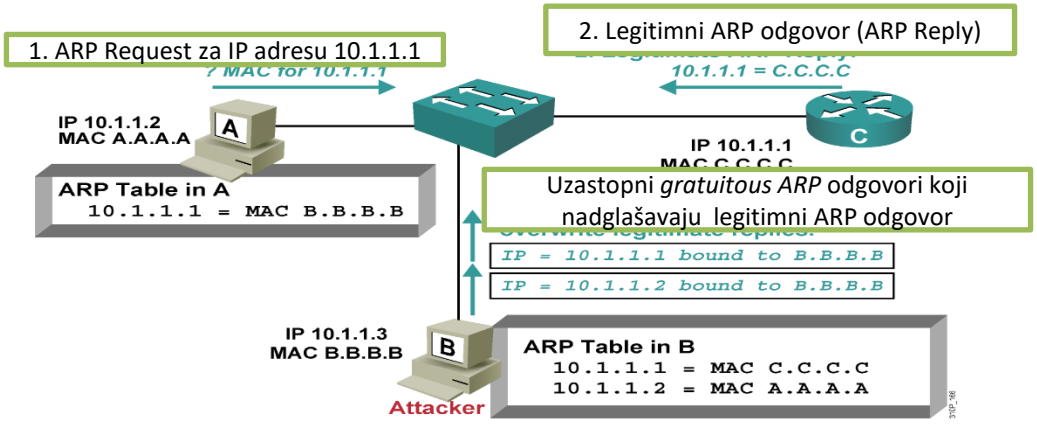
```
Switch(config)# interface gig 0/1
Switch(config-if)# ip dhcp snooping trust
```



ARP SPOOFING

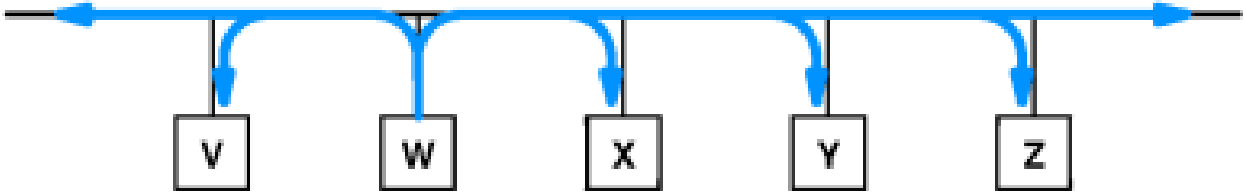


- Host šalje broadcast poruku da bi odredio MAC adresu uređaja sa kojim želi da komunicira (Normalni ARP zahtev)
- Kada primi odgovor, uređaj u ARP tabeli čuva mapiranje IP adrese i MAC adrese odredišta.
- Spoofing ARP odgovora od legitimnog uređaja koristeći *gratuitous ARP, napadač se prikazuje kao odredišni host*
- *ARP reply od napadača dovodi do toga da pošiljaoc u svojoj ARP keš tabeli zabeleži MAC adresu napadača*
- Svi paketi koji su namenjeni datom odredištu prosleđivaće se preko napadača



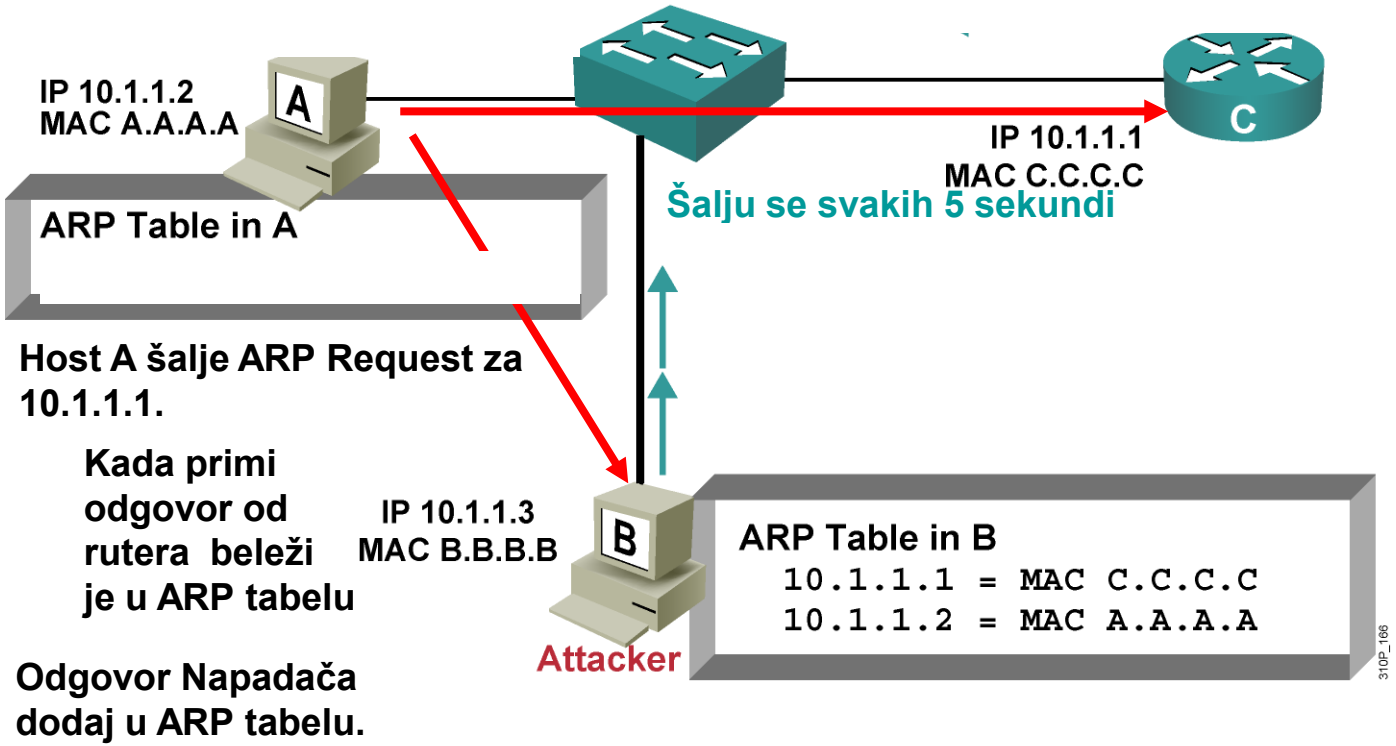
GRATUITOUS ARP

- Gratuitous ARP koristi host da oglasi svoju IP adresu u lokalnoj mreži kako bi izbegao duplikat IP adrese u mreži.
- Uređaji mogu da informacije iz Gratuitous ARP poruke keširaju kod sebe.
- Gratuitous ARP je broadcast paket (sličan ARP request)



- HOST W: “Ja sam host W, moja IP adresa je 1.2.3.4, moja MAC adresa je 12:34:56:78:9A:BC”

ARP nema ugrađenu autentifikaciju, napadač jednostavno može da lažira adrese koristeći alate ettercap, dsniff i arpspoof, da pogrešne adrese budu upisane u ARP tabele IP uređaja.



```
[root@sconvery-lnx dsniff-2.3]# ./arpspoof 15.1.1.1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
15.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
15.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
15.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
15.1.1.1 is-at 0:4:4e:f2:d8:1
```

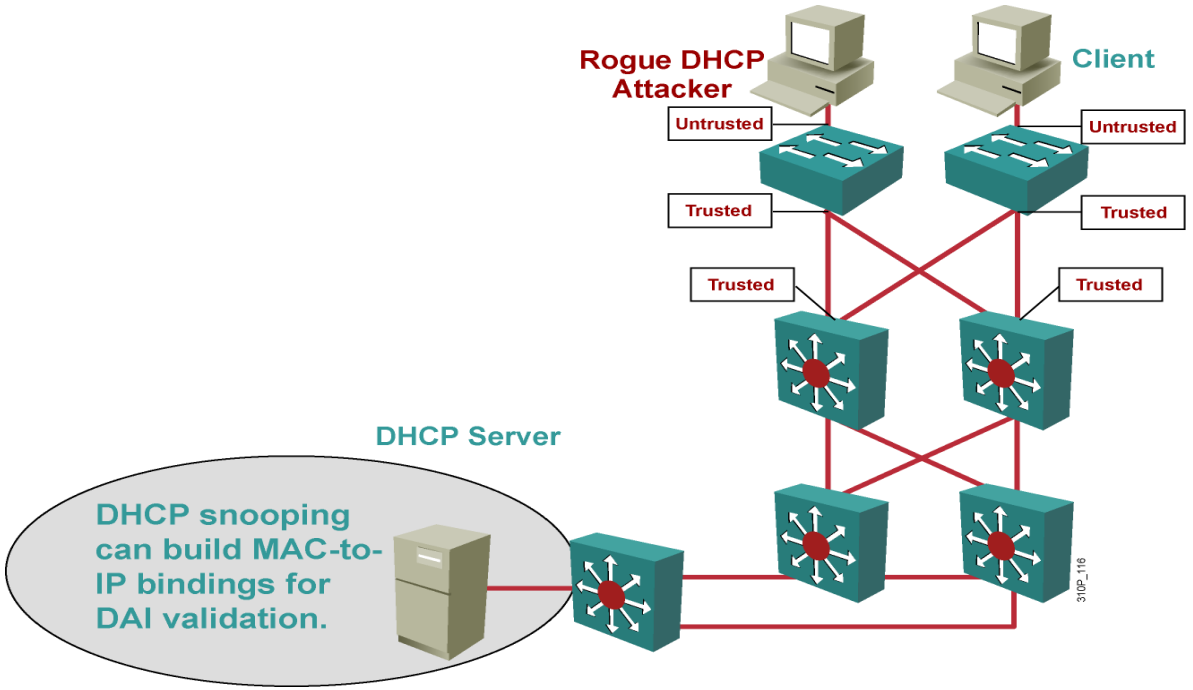
```
C:\>test

C:\>arp -d 15.1.1.1

C:\>ping -n 1 15.1.1.1

Pinging 15.1.1.1 with 32 byt

Reply from 15.1.1.1: bytes=32 time<10ms TTL=255

C:\>arp -a

Interface: 15.1.1.26 on Interface 2
  Internet Address      Physical Address      Type
  15.1.1.1              00-04-4e-f2-d8-01     dynamic
  15.1.1.25             00-10-83-34-29-72     dynamic
C:\>arp -a

Interface: 15.1.1.26 on Interface 2
  Internet Address      Physical Address      Type
  15.1.1.1              00-10-83-34-29-72     dynamic
  15.1.1.25             00-10-83-34-29-72     dynamic
```

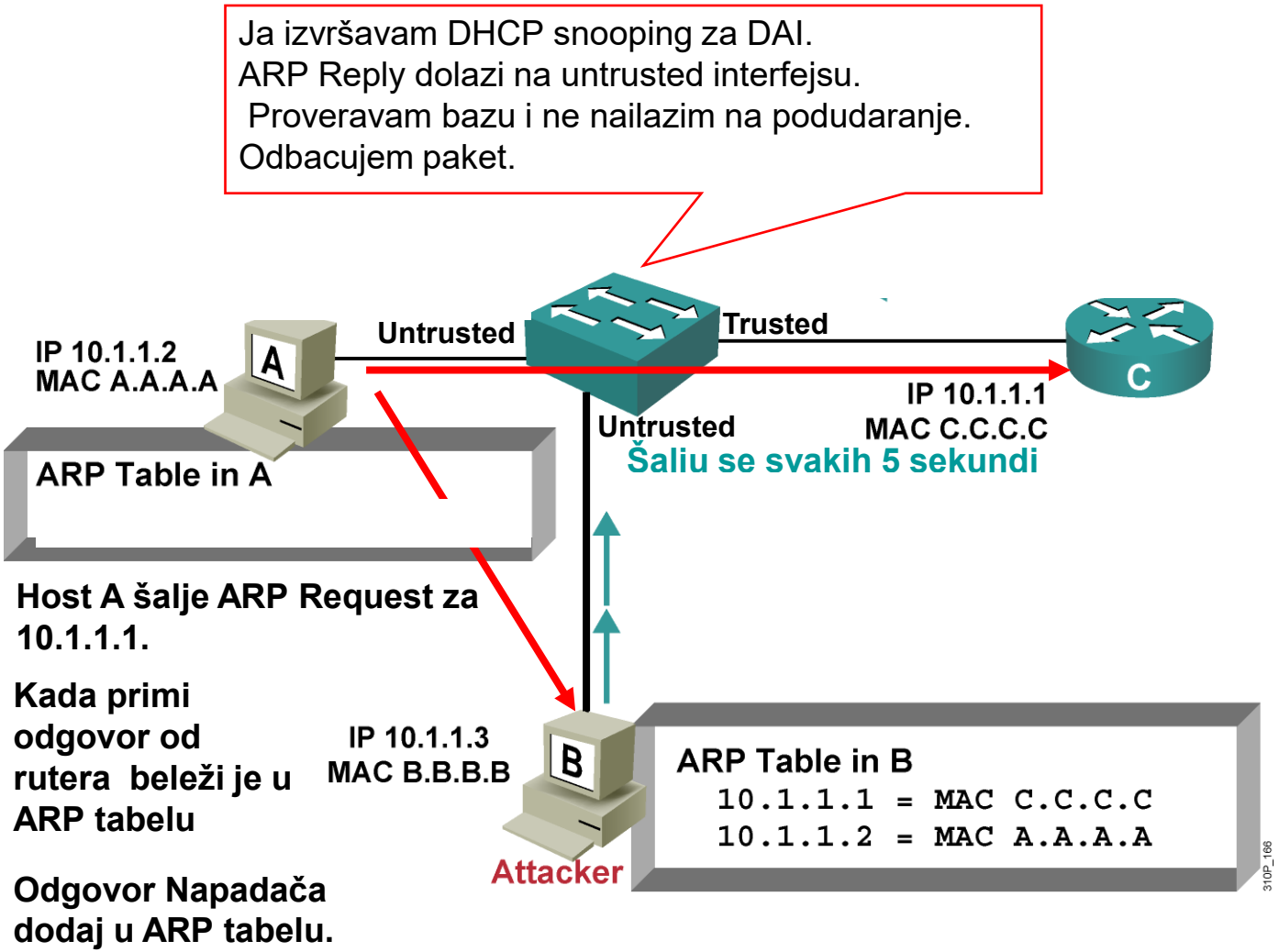
Dynamic ARP Inspection (DAI)

- Da bi smo sprečili ARP *spoofing* ili "*poisoning*," svič mora da obezbedi da su samo **validne ARP request** i **ARP response poruke** dozvoljene.
- DAI sprečava ove napade presretajući a zatim i proveravajući ARP request i response poruke.
- Svaka presretnuta ARP reply poruka se proverava (validna MAC–IP adresa) pre nego što se prosledi PC-u na ažuriranje u ARP keš.
- ARP odgovori koji nisu odgovarajući se odbacuju.
- **DAI** određuje ispravnost ARP paketa na osnovu baze koju formira **DHCP snooping** a koja sadrži vezivanje MAC adrese i odgovarajuće IP adrese.
- Da bi se obezbedili i uređaji koji imaju statičke IP adrese**, DAI proverava ARP pakete** na osnovu konfigurisane ARP ACL.

Dynamic ARP Inspection (DAI)

- DAI se povezuje sa interfejsima koji su trusted ili untrusted.
- Trusted interfejsi zaobilaze Dynamic ARP inspekciju.
- Untrusted interfejsi se nadgledaju od strane DAI.




Ja izvršavam DHCP snooping za DAI.
ARP Reply dolazi na untrusted interfejsu.
Proveravam bazu i ne nailazim na podudaranje.
Odbacujem paket.
IP 10.1.1.2
MAC A.A.A.A
A
Untrusted
Trusted
C
IP 10.1.1.1
MAC C.C.C.C
Untrusted
Šaliu se svakih 5 sekundi
ARP Table in A
Host A šalje ARP Request za 10.1.1.1.
Kada primi odgovor od rutera beleži je u ARP tabelu
Odgovor Napadača dodaj u ARP tabelu.
IP 10.1.1.3
MAC B.B.B.B
B
Attacker
ARP Table in B
10.1.1.1 = MAC C.C.C.C
10.1.1.2 = MAC A.A.A.A
310P_166

Dynamic ARP Inspection (DAI) Konfiguracija

Korak 1:
- Omogućimo DAI na jednom ili više interfejsa

Switch(config)# **ip arp inspection vlan<vlan opseg>**

Korak 2:
- Svi portovi na sviču su konfigurisani kao untrusted(default)
- Potrebno je konfigurisati trusted portove na trunk vezama

Switch(config-if)# **ip arp inspection trust**

Korak 3:
- Za IP uređaje koji ne koriste DHCP potrebno je konfigurisati **ARP ACL** koja definiše statičko MAC-IP vezivanje

Switch(config)# **arp access-list <ime>**
permit ip host <IP pošiljaoca> mac host <mac pošiljaoca> log

Korak 4:
- Primena ARP liste
- Ključna reč *static* saopštava DAI alatu da ne gleda DHCP Snooping bazu već samo ARP ACL

Switch(config)# **ip arp inspection filter <arp acl> vlan <vlan id> [static]**

- Kada se *ARP reply* presretne, sadržaj se prvo proverava u ACL
- Ukoliko nema podudaranja, DHCP Snooping baza se proverava sledeća
- Ukoliko se dodata *static* ključna reč sprečava se provera DHCP Snooping baze

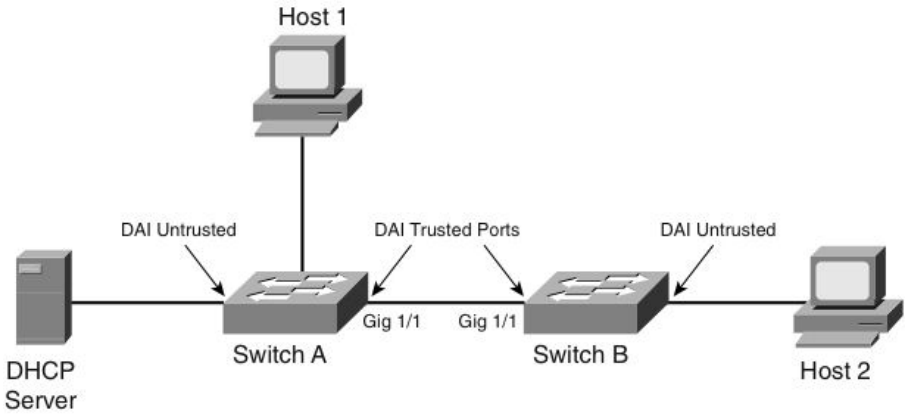
Dynamic ARP Inspection (DAI) Konfiguracija

- Može se definisati kako će se vršiti provera samog sadržaja u ARP paketu
- Proverava se samo **MAC i IP adresa** koja se nalazi **unutar ARP payload-a (default)**, ne proveravaju se MAC i IP adrese koje se nalaze u Ethernet zaglavlju.

Korak 5:
- Način provere sadržaja u samom ARP paketu
- **Src-Mac** proverava izvorišnu Mac adresu u Ethernet zaglavlju umesto izvorišne Mac adrese u ARP payload-u.
- **Dst-Mac** proverava odredišnu Mac adresu u Ethernet zaglavlju umesto odredišne(target) Mac adrese u ARP payload-u.
- **IP** proverava IP adresu pošiljaoca u svim zaglavljima

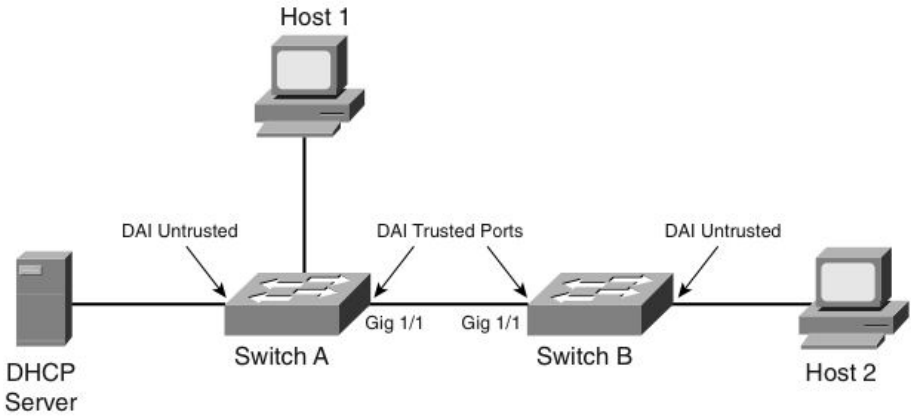
Switch(config)# **ip arp inspection validate [src-mac|dst-mac IP]**

Dynamic ARP Inspection (DAI)




```
SwitchA# configure terminal

SwitchA(config)# ip arp inspection vlan 10
SwitchA(config)# interface gigabitEthernet 1/1
SwitchA(config-if)# ip arp inspection trust
SwitchA(config-if)# end

SwitchB# configure terminal

SwitchB(config)# ip arp inspection vlan 10
SwitchB(config)# interface gigabitEthernet 1/1
SwitchB(config-if)# ip arp inspection trust
SwitchB(config-if)# end
```

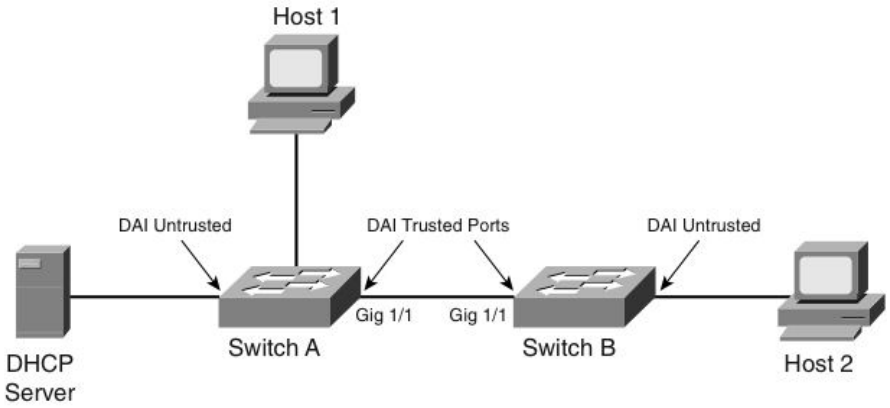
Dynamic ARP Inspection (DAI)



SwitchA# **show ip arp inspection interfaces**

Interface	Trust State	Rate (pps)	Burst Interval
Gi1/1	Trusted	None	N/A
Gi1/2	Untrusted	15	1
Fa2/1	Untrusted	15	1
Fa2/2	Untrusted	15	1

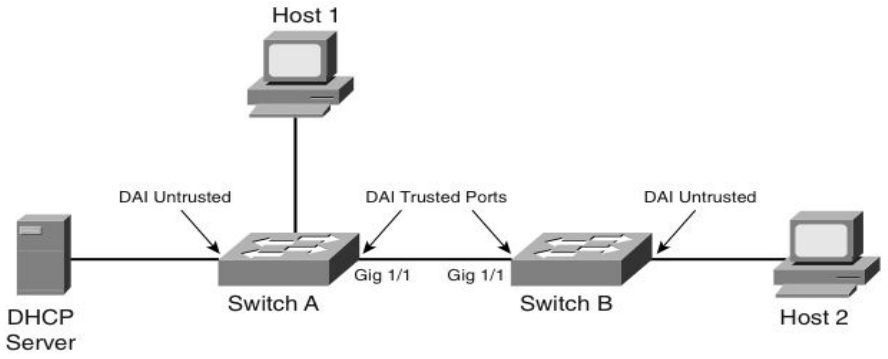
Dynamic ARP Inspection (DAI)



SwitchA# show ip dhcp snooping binding

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:01:00:01:00:01	10.10.10.1	4995	dhcp-snooping	10	FastEthernet2/1

Dynamic ARP Inspection (DAI)

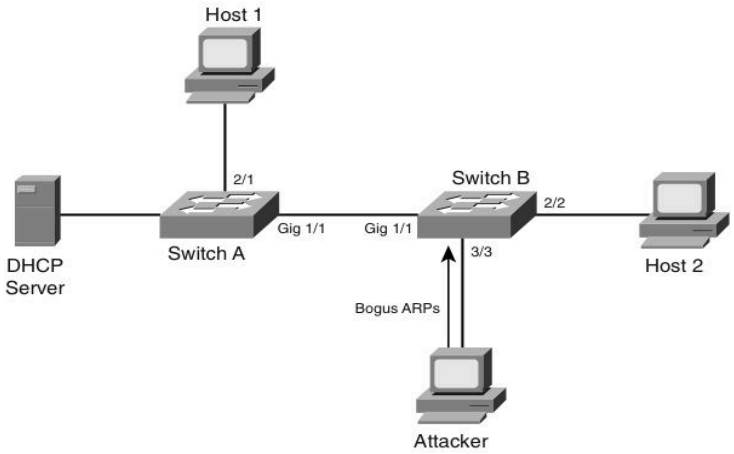


SwitchB# **show ip arp inspection interfaces**

Interface	Trust State	Rate (pps)	Burst Interval
Gi1/1	Trusted	None	N/A
Gi1/2	Untrusted	15	1
Fa2/1	Untrusted	15	1
Fa2/2	Untrusted	15	1
Fa2/3	Untrusted	15	1
Fa2/4	Untrusted	15	1

Dynamic ARP Inspection (DAI)

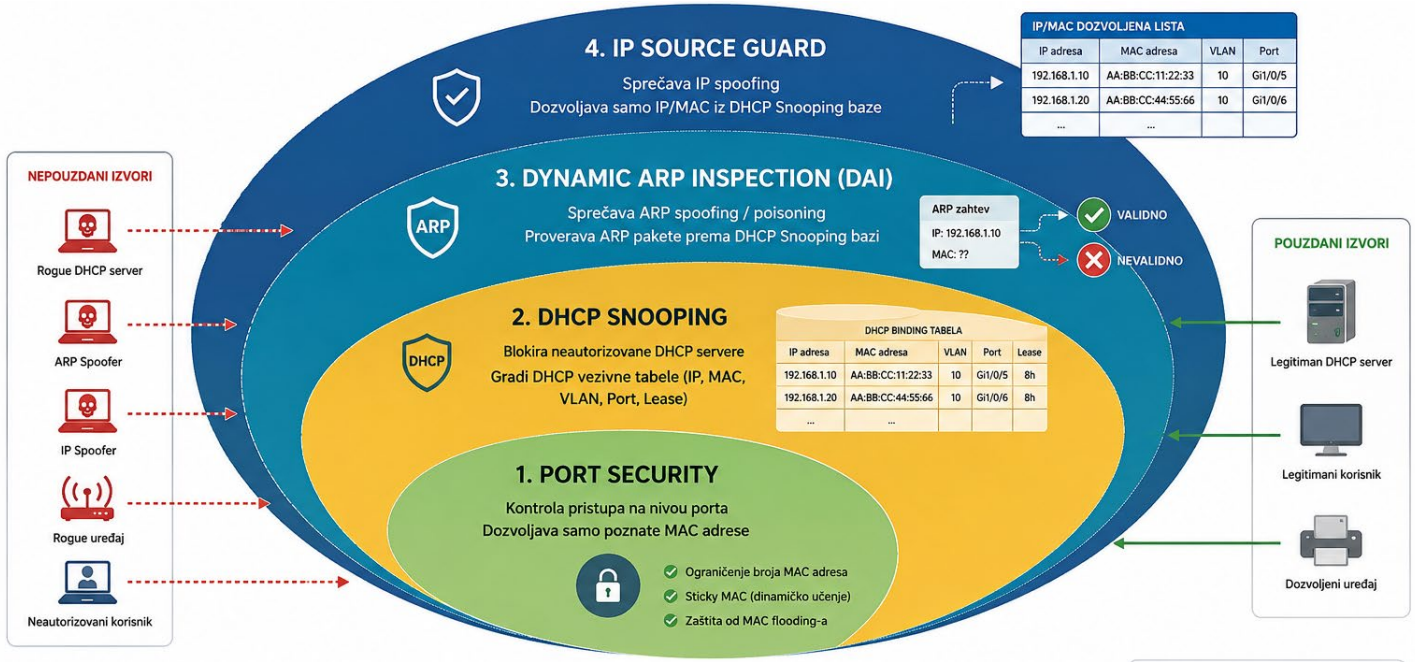
- Napadač koji je povezan na Switch B pokušava da pošalje neispravan ARP request.
- Switch B detektuje i odbacuje takav zahtev.
- Switch B može da port stavi u **errdisable** stanje i da generiše **log** poruku.



02:46:49: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa3/3, vlan 10.([0001.0001.0001/10.10.10.1/0000.0000.0000/0.0.0.0/09:23:24 UTC Thu Nov 27 2003])

VIŠESLOJNA ZAŠTITA PRISTUPNOG SLOJA

- **Dynamic Address Resolution Protocol inspection (DAI)** obezbeđuje ARP protokol koristeći DHCP snooping tabelu da bi minimizovao uticaj *ARP poisoning* i *spoofing* napada.
- **IP Source Guard (IPSG)** sprečava IP spoofing (lažiranje IP adresa) upotrebom DHCP snooping tabele.
- **Port security** sprečava *MAC flooding* napad.
- **DHCP snooping** sprečava napad na DHCP server i svič.



DNS Spoofing

DNS Spoofing (DNS cache poisoning) je cyber-napad u kojem napadač menja zapise u DNS (Domain Name System) kešu servera.

Preusmerava saobraćaj sa legitimnih web lokacija na lažne ili zlonamerne web lokacije.

Korisnici mogu nesvesno završiti na zlonamernim web sajtovima koji izgledaju identično kao pravi sajtovi.

Posledice su ukradene lozinke, lični podaci ili širenje malware (zlonamernog) programa

Izvođenje napada – DNS Spoofing

1. DNS Keširanje:

DNS keširanje je proces u kojem DNS resolveri (lokalni DNS server) privremeno čuvaju odgovore na DNS upite kako bi ubrzali buduće upite.

Na primer, kada korisnik pokuša da pristupi „akademijanis.edu.rs", njegov DNS resolver će zatražiti IP adresu za " akademijanis.edu.rs " i čuvati taj odgovor neko vreme.

2. Izvođenje Napada:

Unos lažnih informacija u DNS keš.

a. **Otrovni odgovori:**

Napadač šalje lažne odgovore DNS serveru sa informacijama koje nisu tražene, ali DNS server prihvata i kešira te lažne informacije.

b. **MiTM (Man-in-the-Middle) napadi:**

Ako napadač može presresti komunikaciju između korisnika i DNS servera, može ubaciti lažne DNS odgovore pre nego što stvarni DNS server odgovori.

c. **Eksploit ranjivosti u DNS softveru:**

Ako postoji poznata ranjivost u softveru koji koristi DNS server, napadač može iskoristiti tu ranjivost kako bi ubacio lažne zapise.

Izvođenje napada – DNS Spoofing

3. Preusmeravanje Saobraćaja:

Kada napadač uspe da ubaci lažne DNS zapise, svaki sledeći korisnik koji zatraži IP adresu za taj domen biće preusmeren na IP adresu koju je odredio napadač, umesto na stvarnu IP adresu.

4. Posledice:

Korisnici mogu završiti na lažnim web lokacijama koje izgledaju identično kao prave. Na ovim lokacijama napadači mogu krasti podatke za prijavu, instalirati malware na korisničke uređaje ili izvršiti druge zlonamerne aktivnosti.

Scenario: MiTM DNS Spoofing napad

1. Napadač se pozicionira između žrtve i DNS servera:

Napadač koristi tehniku kao što je **ARP spoofing** (Address Resolution Protocol spoofing) kako bi se pozicionirao između žrtve (korisnika) i DNS servera na lokalnoj mreži. Ovim načinom napadač može presretati sve podatke koji se razmenjuju između žrtve i DNS servera.

1. Žrtva šalje DNS upit:

Korisnik pokušava da pristupi web stranici, recimo "www.bank.com". Njegov računar šalje DNS upit DNS serveru kako bi dobio IP adresu za taj domen.

2. Napadač presreće DNS upit:

Pre nego što upit stigne do stvarnog DNS servera, napadač ga presreće. Napadač sada može odgovoriti na DNS upit umesto stvarnog DNS servera.

Scenario: MiTM DNS Spoofing napad

4. **Napadač šalje lažni DNS odgovor**:

   Napadač šalje lažni DNS odgovor žrtvi, pružajući IP adresu servera pod kontrolom napadača umesto stvarne IP adrese za "www.bank.com". Na primer, umesto stvarne IP adrese banke, korisnik dobija IP adresu phishing sajta koji izgleda identično kao prava banka.

5. **Žrtva pristupa lažnoj web stranici**:

   Korisnik, nesvestan prevare, unosi svoje pristupne podatke na lažnoj web stranici. Napadač sada može prikupiti te podatke i koristiti ih za dalje zlonamerne aktivnosti.

6. **Napadač prosleđuje pravi DNS odgovor (opciono)**:

   Da bi sakrio svoje tragove, napadač može proslediti pravi DNS odgovor nakon što je preusmerio korisnika na lažni sajt, kako bi korisnik na kraju završio na pravom sajtu.

Scenario: MiTM DNS Spoofing napad

Tok napada:

Korisnik šalje DNS upit: Korisnik pokušava da pristupi web stranici (npr. www.bank.com).

Napadač presreće DNS upit:

Napadač koristi Ettercap za ARP spoofing kako bi se pozicionirao između korisnika i routera/DNS servera.

Ettercap šalje lažni DNS odgovor:

Ettercap vraća lažni DNS odgovor korisniku sa IP adresom lažne web stranice pod kontrolom napadača.

Korisnik se povezuje na lažnu web stranicu Korisnik nesvesno pristupa lažnoj web stranici i unosi svoje podatke.

DNSSEC-a

DNSSEC (Domain Name System Security Extensions) je skup proširenja za DNS (Domain Name System) koji dodaje sloj sigurnosti kako bi se osigurala autentičnost i integritet DNS podataka.

DNSSEC je dizajniran da zaštiti korisnike od različitih vrsta napada na DNS, kao što su DNS spoofing i cache poisoning.

Osnovni koncepti DNSSEC-a

Digitalni potpisi:

DNSSEC koristi digitalne potpise za verifikaciju autentičnosti DNS odgovora. Svaki zapis u DNS zoni (skupu DNS podataka za domen) je potpisan digitalnim potpisom korišćenjem privatnog ključa.

Ključni parovi (public/private):

Svaka DNS zona ima par ključeva: privatni ključ, koji se koristi za potpisivanje DNS zapisa, i javni ključ, koji se distribuira kako bi se omogućila verifikacija tih potpisa. Privatni ključ se čuva tajno, dok je javni ključ dostupan svima.

RRSIG i DNSKEY zapisi:

RRSIG (Resource Record Signature):

Ovaj zapis sadrži digitalni potpis za druge DNS zapise u zoni.

DNSKEY (DNS Public Key):

Ovaj zapis sadrži javni ključ koji se koristi za verifikaciju RRSIG zapisa.

Delegation Signer (DS) zapisi:

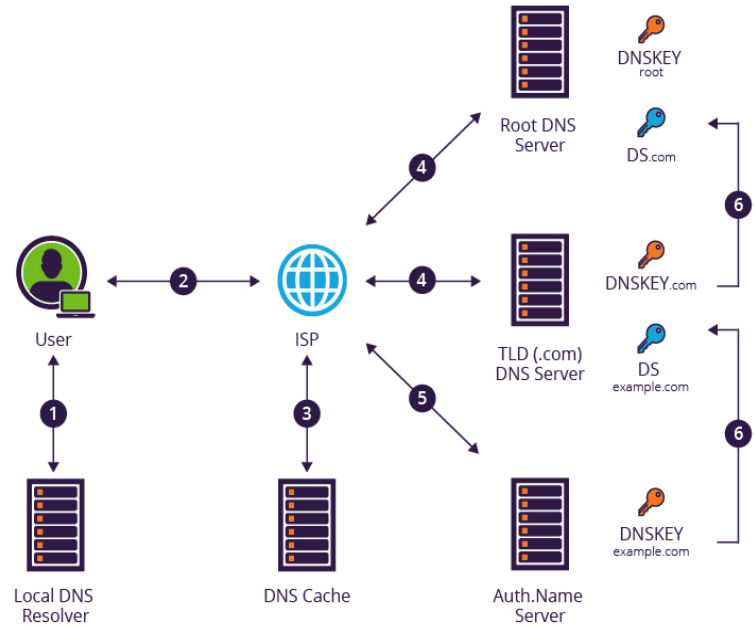
Kada se zona delegira (na primer, sa gTLD-a kao što je .com na example.com), DS zapis se postavlja u nadređenu zonu. DS zapis omogućava verifikaciju javnog ključa podređene zone, stvarajući lanac poverenja od korenskih DNS servera do određenih domena.

Način rada DNSSEC

Potpisivanje DNS zapisa:
Vlasnik domena koristi privatni ključ za potpisivanje svih DNS zapisa u svojoj zoni. Ovi potpisi se dodaju kao RRSIG zapisi.

Distribucija javnog ključa:
Javni ključ se dodaje u DNS kao DNSKEY zapis. DS zapis, koji sadrži otisak javnog ključa, postavlja se u nadređenu zonu (na primer, u .com zoni za domen example.com).

Rezolucija DNS upita sa DNSSEC-om:
Kada korisnikov resolver (DNS klijent) pošalje DNS upit, autoritativni DNS server vraća tražene zapise zajedno sa odgovarajućim RRSIG zapisima.
Resolver koristi DNSKEY zapis da verifikuje RRSIG zapise. Ako su potpisi validni i lanac poverenja je netaknut, resolver zna da su podaci autentični i nepromenjeni.



Prednosti DNSSEC-a

Zaštita od DNS spoofing i cache poisoning napada:
DNSSEC sprečava napadače da lažiraju DNS odgovore, jer svaki odgovor mora biti digitalno potpisan i verifikovan.

Integritet podataka:
DNSSEC osigurava da podaci nisu izmenjeni tokom prenosa između DNS servera i korisnika.

Autentičnost:
Korisnici mogu biti sigurni da informacije koje dobijaju dolaze od legitimnih DNS servera.

Implementacija DNSSEC-a

Generisanje ključeva:
Administrator domena generiše par ključeva (privatni i javni) za svoju DNS zonu.

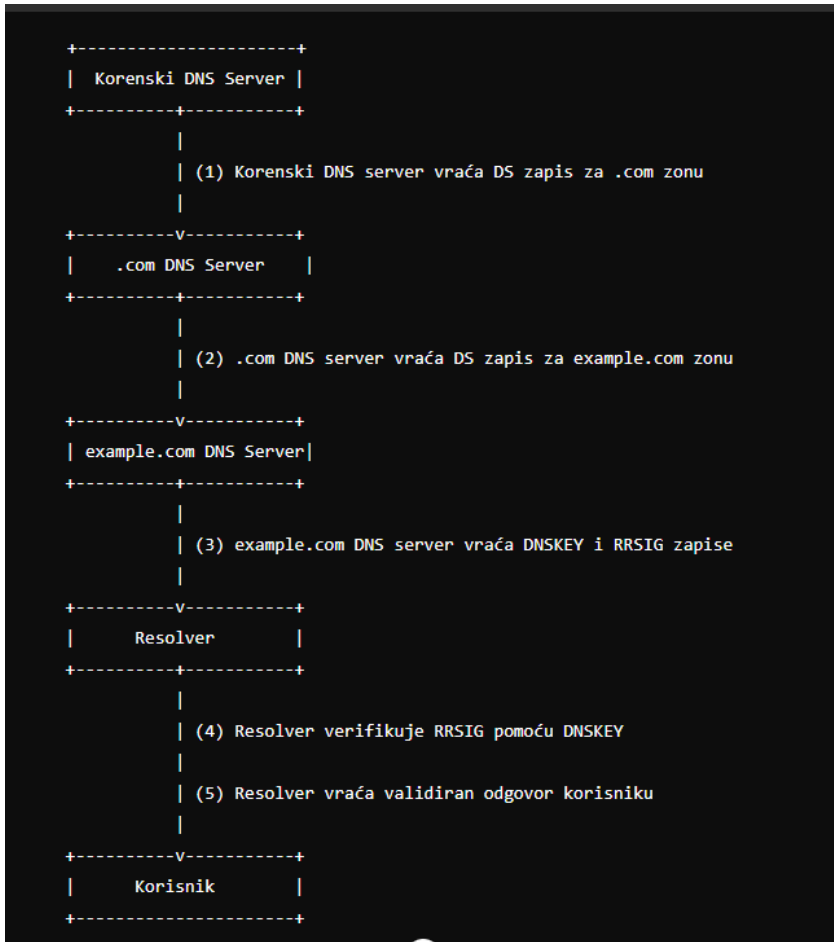
Potpisivanje DNS zapisa:
Privatni ključ se koristi za potpisivanje svih DNS zapisa u zoni, a rezultujući RRSIG zapisi se dodaju u DNS zonu.

Distribucija javnog ključa i DS zapisa:
DNSKEY zapis se dodaje u DNS zonu, a DS zapis se dostavlja nadređenoj zoni.Konfiguracija resolvera:DNS resolveri moraju biti konfigurisani da podržavaju DNSSEC verifikaciju.

Korenski DNS server:
Resolver započinje upit od korenskog DNS servera. Korenski DNS server vraća DS zapis za .com zonu, koji sadrži otisak javnog ključa za .com zonu.

.com DNS server:
Resolver koristi DS zapis da proveri DNSKEY zapis za .com zonu. Nakon toga, šalje upit .com DNS serveru za example.com. .com DNS server vraća DS zapis za example.com zonu

.example.com DNS server:
Resolver koristi DS zapis da proveri DNSKEY zapis za example.com zonu. Nakon toga, šalje upit example.com DNS serveru za konkretan DNS zapis (npr. A zapis za www.example.com). example.com DNS server vraća DNSKEY i RRSIG zapise zajedno sa traženim DNS zapisom.



Verifikacija RRSIG zapisa:
Resolver koristi DNSKEY zapis da verifikuje RRSIG zapise. Ako su potpisi validni, to znači da su DNS zapisi autentični i nepromenjeni.

Odgovor korisniku:
Ako je verifikacija uspešna, resolver vraća validiran DNS odgovor korisniku. Ako verifikacija nije uspešna, resolver vraća grešku (npr. SERVFAIL).