Vežba 3 – Adresiranje

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol je klijent-server protokol aplikativnog nivoa koji omogućava dinamičku distribuciju parametara konfiguracije mreže. Na ovaj način olakšava se posao administracije i konfiguracije mreže.

Korišćenjem dinamičkog adresiranja obezbeđuje se sigurnost da su sve ip adrese u mreži jedinstvene. Pored alokacije adrese, DHCP server omogućava računaru da sazna i neke potrebne informacije o konfiguraciji mreže, kao što su adresa najbližeg rutera (eng. *default gateway*), subnet maska i adresa lokalnog dns servera.

Zbog mogućnosti DHCP-a da automatizuje proces priključenja računara u mrežu, ovaj protokol se često referencira kao **plug-and-play protocol**. Alternativa DHCP-u bila bi **statičko adresiranje**, kada administratori mreža manualno podešavaju mrežne parametre na svakom od uređaja u mreži. Ovakav vid adresiranja znatno otežava rekonfigurisanje mreže.

U najvećem broju slučajeva klijenta predstavlja uređaj koji se tek priključio u mrežu i kome su potrebne informacije o konfiguraciji mreže, uključujući i ip adresu koja je njemu namenjena. Ovaj proces razmene informacija sistematizovan je u četiri koraka, čiji detaljan opis je dat u nastavku.

Slika 1 - Proces razmene informacija između DHCP klijenta i DHCP servera

1. **Otkrivanje DHCP servera**

   Operativni sistem kreira DHCP poruku i stavlja je u UDP segment sa portom primaoca 67 (DHCP server) i portom pošiljaoca 68 (DHCP klijent). Za komunikaciju se uvek koriste isti portovi. UDP segment se pakuje u IP datagram sa 255.255.255.255 broadcast logičkom adresom odredišta, jer računar ne zna na kojoj se tačno adresi nalazi DHCP server. Dokle god se klijentu ne dodeli nova adresa, on će koristiti adresu 0.0.0.0. IP datagram se stavlja u ethernet frejm i dodaje se fabrička fizička adresa mrežne kartice pošiljaoca kao i FF:FF:FF:FF:FF:FF za adresu primaoca, kako bi frejm primili svi uređaji koji su povezani na switch.

PDU	Značajno polje	Vrednost
DHCP podaci	Tip poruke	Discover
UDP segment	Port primaoca	67
	Port pošiljaoca	68
IP paket	Adresa primaoca	255.255.255.255
	Adresa pošiljaoca	0.0.0.0
Ethernet frejm	Adresa primaoca	FF:FF:FF:FF:FF:F
	Adresa pošiljaoca	02:02:02:02:02:02

Tabela 1 - DHCP Discover poruka

2. **Ponuda DHCP servera**

   DHCP server odabire adresu iz skupa slobodnih adresa i šalje ponudu klijentu. Ponuđena adresa se računaru ne dodeljuje permanentno, već na određeni vremenski period. Posle isteka definisanog perioda, adresa se vraća u skup slobodnih adresa i moguće ju je dodeliti nekom drugom računaru. Na ovaj način omogućeno je da se na javnim mestima poput aerodroma ili kafića lako pristupi wirelless mreži, bez potrebom da se uređaj konfiguriše.

PDU	Značajno polje	Vrednost
DHCP podaci	Tip poruke	Offer
	Ponuđena adresa	10.40.9.101
	Vremenski rok	3600 sekundi
UDP segment	Port primaoca	68
	Port pošiljaoca	67
IP paket	Adresa primaoca	10.40.9.101
	Adresa pošiljaoca	10.40.9.10
Ethernet frejm	Adresa primaoca	02:02:02:02:02:02
	Adresa pošiljaoca	01:01:01:01:01:01

Tabela 2 - DHCP Offer poruka

3. **Zahtev za dodelom adrese**

   Klijent može dobiti ponude od više različitih servera. Zbog toga je potrebno da klijent odabere jednu od ponuđenih adresa i pošalje zahtev za odobrenje korišćenja tražene adrese. Takođe, postoji mogućnost da klijent zatraži novu adresu pre nego što istekne propisani vremenski period.

PDU	Značajno polje	Vrednost
DHCP podaci	Tip poruke	Request
	Zahtevana adresa	10.40.9.101
	Vremenski rok	3600 sekundi
UDP segment	Port primaoca	67
	Port pošiljaoca	68
IP paket	Adresa primaoca	255.255.255.255
	Adresa pošiljaoca	0.0.0.0
Ethernet frejm	Adresa primaoca	FF:FF:FF:FF:FF:F
	Adresa pošiljaoca	02:02:02:02:02:02

Tabela 3 - DHCP Request poruka

4. **Odobrenje za korišćenje tražene adrese.**
   Ukoliko je tražena adresa još uvek slobodna, server šalje odobrenje.

PDU	Značajno polje	Vrednost
DHCP podaci	Tip poruke	Ack
	Odobrena adresa	10.40.9.101
	Vremenski rok	3600 sekundi
UDP segment	Port primaoca	68
	Port pošiljaoca	67
IP paket	Adresa primaoca	10.40.9.101
	Adresa pošiljaoca	10.40.9.10
Ethernet frejm	Adresa primaoca	02:02:02:02:02:02
	Adresa pošiljaoca	01:01:01:01:01:01

Tabela 4 - DHCP Ack poruka

Pošto je klijent primio DHCP ACK poruku, interakcija između klijenta i servera je završena i klijent može koristiti alociranu adresu na odobreni vremenski period.

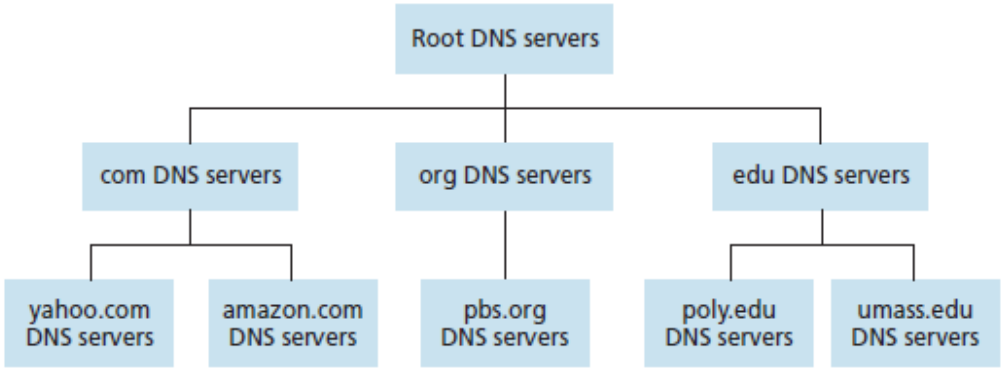
Domain Name Server (DNS)

Kao što je ranije napomenuto, za obeležavanje uređaja u mreži koriste se IP adrese. Međutim, kako su numeričke vrednosti većini ljudi teške za pamćenje, javila se potreba za uvođenjem **domenskih imena**. Tako je, na primer, mnogo lakše zapamtiti ime "*http://www.cisco.com*" nego "198.133.219.25", što bi bila numerička adresa tog servera.

Domain Name Server (DNS) je protokol aplikativnog nivoa koji omogućava prevođenje (mapiranje) alfa- numeričkih imena u IP adresu računara (eng. ***Forward Lookup***), ili obrnuto (eng. ***Reverse Lookup***).

Pored toga DNS omogućava još par bitnih servisa:

- Host aliasing - omogućava hostu da umesto svog imena (koje se označava kao kanonsko) koristi neko drugo ili više drugih imena za komunikaciju. Na primer, kanonsko ime "*relay1.west- coast.enterprise.com*" može imati "*www.enterprise.com*" i "*enterprise.com*".
- Mail server aliasing - krajnje je poželjno da email adresa bude laka za pamćenje. Uzmimo primer da želimo poslati poruku Petru Petroviću. Dovoljno je upisati petar.petrovic@hotmail.com umesto punog imena servera, što bi u našem slučaju bilo petar.petrovic@relay1.west- coast.hotmail.com.
- Load balancing - omogućava distribuciju opterećenja (saobraćaja) na repliciranе servere.

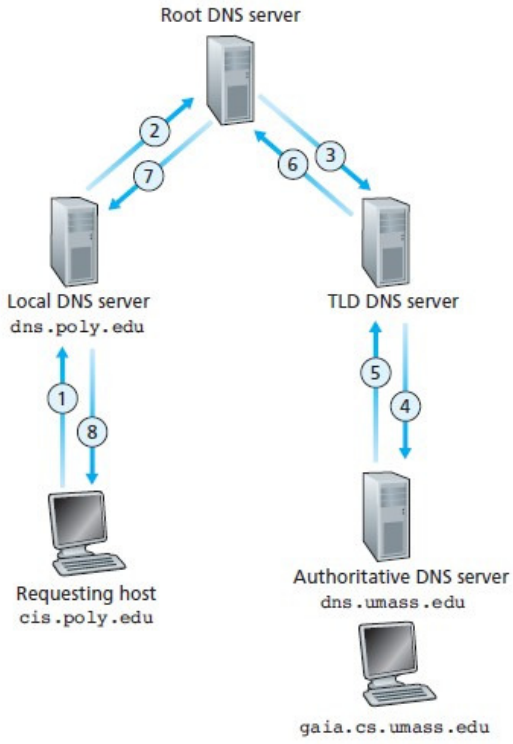


Slika 2 - Hijerarhija DNS servera

DNS koristi veliki broj servera organizovanih u hijerarhijskom obliku i distribuiranim po celom svetu. Serveri su podeljeni po klasama:

- Root serveri (".")
- Serveri najvišeg nivoa (com, org, ...)
- Autoritativni serveri (yahoo, amazon, ...)

Odgovore na DNS upite daju autoritativni serveri, kojima se dodeljuje određeni domen imena nad kojim imaju nadležnost. Ostali tipovi DNS servera samo prosleđuju upite ka drugim serverima, osim u slučaju kada u svojoj memoriji imaju keširanu traženu informaciju.



Slika 3 - DNS rekurzivan upit

Resource Record

DNS serveri zajedno koriste distribuiranu DNS bazu podataka koji čuvaju zapise o resursu (eng. **Resource Record**, RR, koji predstavlja osnovnu jedinicu podataka u DNS sistemu. Često se u literaturi RR prikazuje u formatu (Ime, Vrednost, Tip, TTL). U svakoj DNS poruci sa odgovorom nalazi se jedan ili više ovakvih zapisa o resursu.

Osnovna polja zapisa:

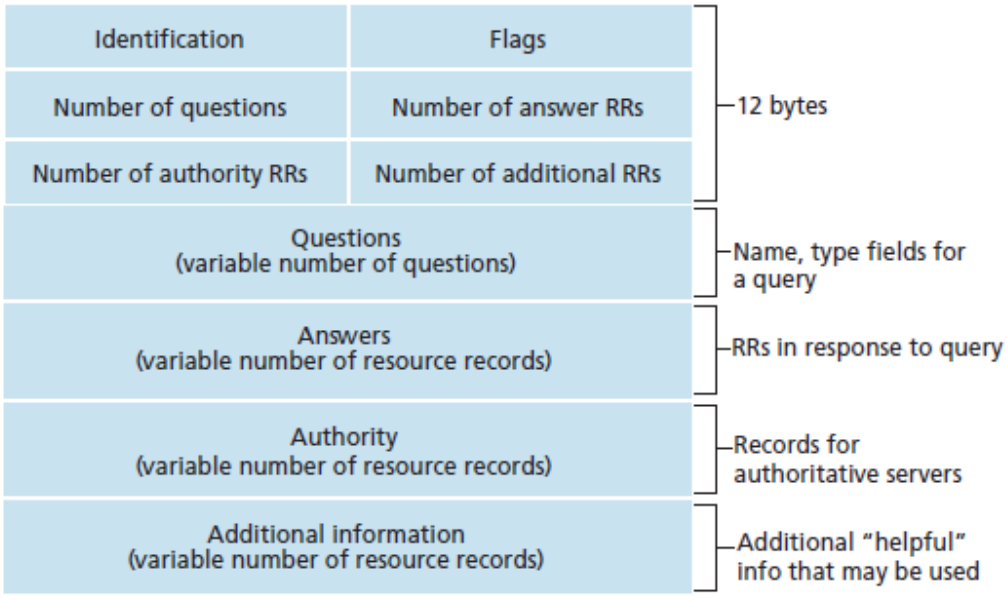
- **Ime** - Domensko ime računara.
- **Vrednost** - Najčešće vrednost ip adrese.
- **Tip** - Tip zapisa o resursu.
    - A - preslikavanje između domenskog imena i naziva krajnjeg računara.
        - (relay1.bar.foo.com, 145.37.93.126, A)
    - CNAME - povezuje ime jednog računara (kanonsko ime) sa imenom drugog računara (alias).

        - (foo.com, relay1.bar.foo.com, CNAME)
    - NS - izlistava servere koji mogu odgovoriti na lookup zahtev.
        - (foo.com, dns.foo.com, NS)
    - MX - specificira mail servera koji se koristi za rukovanje poštom u datom domenu.
        - (foo.com, mail.bar.foo.com, MX)
- TTL (eng. *Time To Live*) - vreme trajanja važnosti zapisa, izražena u sekundama. Pokazuje koliko će se neki zapis čuvati u kešu klijenata ili ostalih DNS servera.

Format poruke

Postoje dva tipa DNS poruka: **poruke upita** (eng *Query*) i **poruke odgovora** (eng. *Reply*). Oba ova tipa koriste isti format poruke. Za komunikaciju DNS najčešće koristi UDP protokol i port 53.

- Zaglavlje
    - Identifikacija - Identifikuje upit i njemu odgovarajući odgovor.
    - Flag - Tip poruke (0 - upit, 1 - odgovor).
    - Polja koja ukazuju na broj ponavljanja svakog od tipova sekcija podataka koji se nalaze iza poglavlja.
- Sekcije
    - Sekcija pitanja - Informacije o generisanom upitu.
    - Sekcija odgovora - Sadrži RR koje odgovara imenu za koje je poslat upit.
    - Sekcija autoritativnih servera.
    - Sekcija dodatnih informacija.



Slika 4 - Format DNS poruke

Prikaz svih keširanih DNS zapisa na lokalnom računaru moguć je npr. dobiti korišćenjem *ipconfig /displaydns* naredbe (Windows OS).

Slika 5 - Prikaz DNS zapisa

Address Resolution Protocol (ARP)

Address Resolution Protocol je protokol koji povezuje protokole **nivoa veze** (ethernet) i **mrežnog nivoa** (IPv4). Ovaj protokol omogućava da se pomoću poznate ip adrese sazna mac adresa nekog uređaja u mreži.

Za povezivanje adresa mrežnog nivoa i adresa nivoa veze koristi se **arp tabela**. Ova tabela se čuva u ram memoriji svakog uređaja i zbog toga se u literaturi često za nju koristi i pojam arp cache. Relacija između logičke i fizičke adrese se naziva mapiranje, jer omogućava da se lociranjem reda u tabeli ip adrese otkrije njena fizička adresa.

Logička adresa	Fizička adresa	Vremenski rok
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Tabela 5 - ARP tabela

ARP tabela takođe sadrži i kolonu vremenskog roka (eng. *Time-To-Live*) čija vrednost ukazuje na to kada će mapiranje biti uklonjeno iz tabele. Inicijalna vrednost vremenskog roka zavisi od samog uređaja i instaliranog operativnog sistema. Cilj je ukloniti iz tabele adrese uređaja koji duži vremenski period nisu aktivne u mreži.

Održavanje tabele vrši se dinamički. Uporedo se koriste dve metode za popunjavanje tabele.

1. **Praćenje lokalnog saobraćaja** - Za svaki primljeni frejm, kreira se novo mapiranje između IP i MAC adrese, ukoliko ono prethodno ne postoji u arp tabeli.
2. **Korišćenjem ARP zahteva - K**oristi se kada je potrebno da se pošalje poruka na adresu čije mapiranje nije zabeleženo u tabeli. U tom slučaju generiše se arp zahtev koji se šalje svima u lokalnoj mreži. Novi red (mapiranje) u tabelu unosi se nakon prijema odgovora na zahtev.

Slanje paketa unutar lokalne mreže

1) **Priprema za slanje poruke -** IP adresa primaoca se dobija od viših slojeva, dok je MAC adresu potrebno potražiti u ARP tabeli. Ukoliko tražena adresa ne postoji u ARP tabeli, potrebno je generisati ARP zahtev kako bi se saznala mac adresa primaoca.

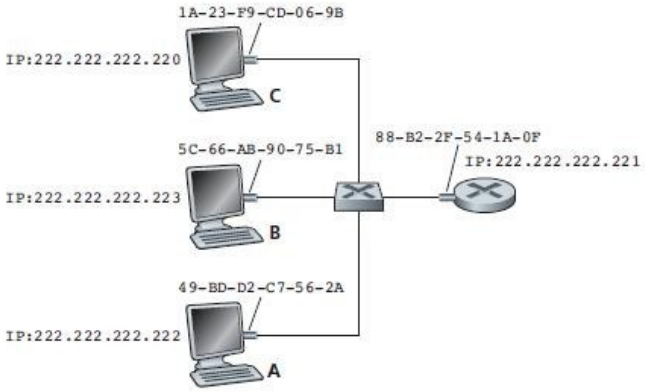


Tabela 6 - Slanje paketa unutar lokalne mreže

2) **ARP zahtev** - za MAC adresu primaoca navodi se broadcast adresa FF-FF-FF-FF-FF-FF, kako bi svi uređaji u mreži primili poruku. U delu podataka koji pripada ARP protokolu navodi se ciljana IP adresa, dok se za ciljanu MAC adresu stavlja 00:00:00:00:00:00, što indikuje da je mac adresa nepoznata.

PDU	Značajno polje	Vrednost
ARP	Tip protokola	Ethernet
	Veličina adrese protokola nivoa veze	6 bajta
	Tip protokola mrežnog	IP
	Veličina adrese protokola mrežnog	4 bajta
	Tip operacije	Request
	Mac adresa pošiljaoca	1A-23-F9-CD-06-
	IP adresa pošiljaoca	222.222.222.220
	Ciljana MAC adresa	00-00-00-00-00-00
	Ciljana IP adresa	222.222.222.223
Ethernet frejm	Tip protokola	ARP
	Adresa pošiljaoca	1A-23-F9-CD-06-
	Adresa primaoca	FF-FF-FF-FF-FF-FF

Tabela 7 - ARP zahtev

3) **ARP odgovor** - Uređaj na mreži može odgovoriti na zahtev slanjem **ARP reply** poruke ukoliko tražena adresa odgovara IP adresi uređaja. Odgovor se šalje samo na adresu uređaja koji je poslao zahtev.

PDU	Značajno polje	Vrednost
ARP	Tip protokola nivoa veze	Ethernet
	Veličina adrese protokola nivoa veze	6 bajta
	Tip protokola mrežnog	IP
	Veličina adrese protokola mrežnog nivoa	4 bajta
	Tip operacije	Reply
	Mac adresa pošiljaoca	5C-66-AB-90-75-B1
	IP adresa pošiljaoca	222.222.222.223
	Ciljana MAC adresa	1A-23-F9-CD-06-9B
	Ciljana IP adresa	222.222.222.220
Ethernet frejm	Tip protokola	ARP
	Adresa pošiljaoca	5C-66-AB-90-75-B1
	Adresa primaoca	1A-23-F9-CD-06-9B

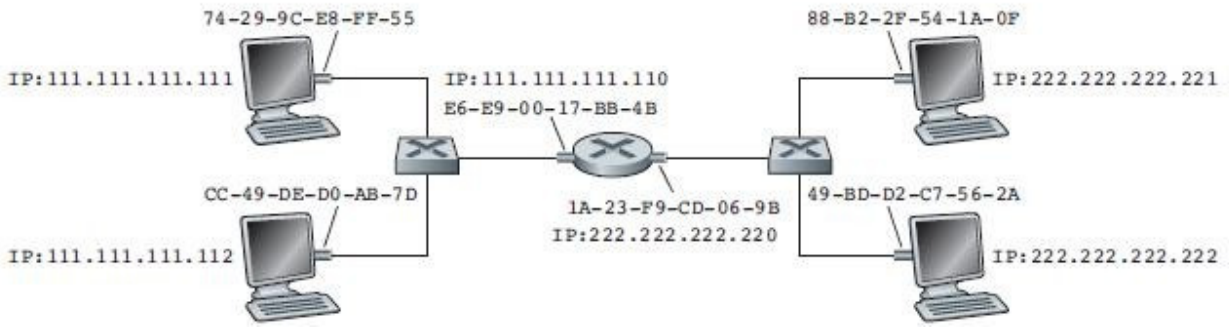
Tabela 8 - ARP odgovor

U slučaju da nijedan uređaj ne odgovori na ARP zahtev frejm za slanje se odbacuje i izveštaj o grešci se prosleđuje višem sloju.

4) **Tražena MAC adresa se smešta u ARP tabelu** - time se omogućava da sledeći put pošiljaocu bude poznata mac adresa odredišta.

Slanje paketa izvan lokalne mreže

Kao i svi ostali uređaji unutar lokalne mreže, gateway (ruter) prati ARP zahteve. U slučaju da se tražena adresa ne nalazi unutar lokalne mreže, ruter će poslati svoju MAC adresu. Drugim rečima rečeno, ruter će obavestiti pošiljaoca da se tražena adresa nalazi izvan lokalne mreže i da će ukoliko želi poslati frejm na traženu adresu to moći učiniti preko njega. Nakon prijema odgovora pošiljaoc zahteva smešta adresu rutera u ARP tabelu. Kada pošiljaoc sledeći put bude želeo poslati poruku na adresu koja se nalazi izvan lokalne mreže, umesto slanja novog ARP zahteva, direktno će proslediti frejm ruteru.



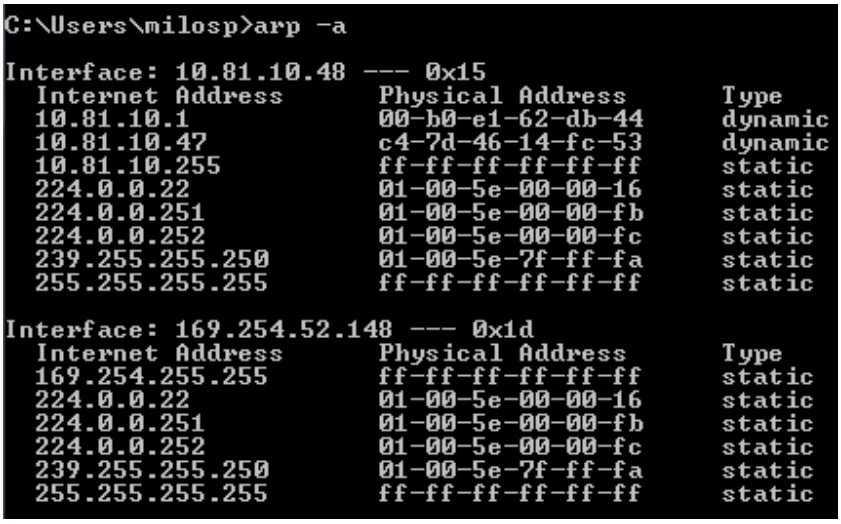
Slika 6 - Slanje paketa izvan lokalne mreže

Problem bezbednosti

ARP Spoofing napad je zasnovan na ARP reply poruci. Zlonameran korisnik može poslati veliki broj ARP reply poruka sa svojom MAC adresom i IP adresama koje se nalaze unutar iste mreže. Računar koji primi lažne ARP reply poruke dodaje adresu zlonamernog korisnika u svoju ARP tabelu. Na taj način sve poruke unutar mreže mogu biti usmerene na računar zlonamernog korisnika. Moguća zaštita od ovakvog napada je dozvoliti samo određenim uređajima sa liste pristup lokalnoj mreži.

Prikaz sadržaja ARP tabele

ARP tabela prikazuje mapiranje mrežnih adresa na fizičke adrese. Prikaz sadržaja ove tabele omogućen je pomoću *arp -a* naredbe (Windows OS kao i Raspbian OS).



Slika 7 - Sadržaj ARP tabele lokalnog računara