Komunikacijske mreže

Kristo Palić

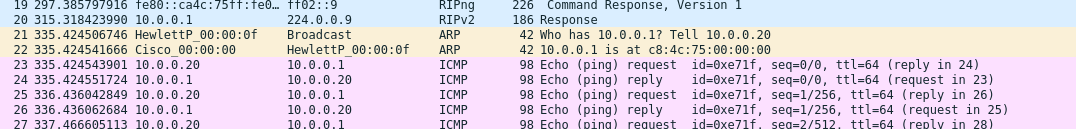
0246074767

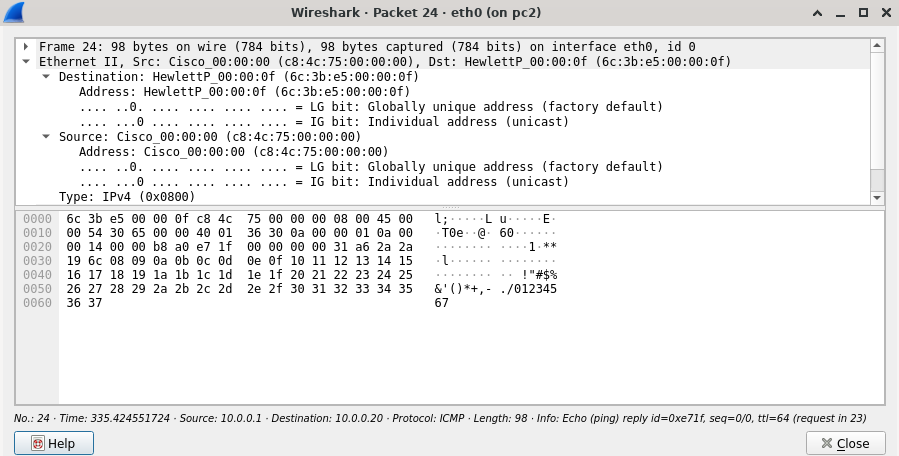
1. Laboratorijska vježba

1. zadatak

Učitamo Ping/ping.imn u IMUNES i stisnemo execute. Pokrenemo snimanje u alatu Wireshark. Otvorimo terminal za pc2 i naredbom ping 10.0.0.1 pošaljemo ICPM request prema pc1



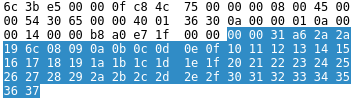


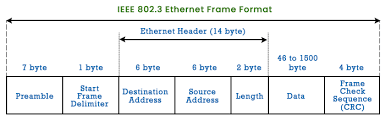


OUI – prva tri para heksadecimalnih brojeva : C8:4C:75 (Cisco systems inc.)

NIC – zadnja tri para heksadecimalnih brojeva : 00:00:00

2. zadatak





Ukupna veličina zaglavlja Ethernet okvira u Wiresharku je 14 bajtova (6 bajtova odredišna adresa + 6 bajtova izvorišna adresa + 2 bajta tip/dužina). Prepoznajemo zaglavlje koje sam već opisao i 46 bajtova namjenjenih za podatke.

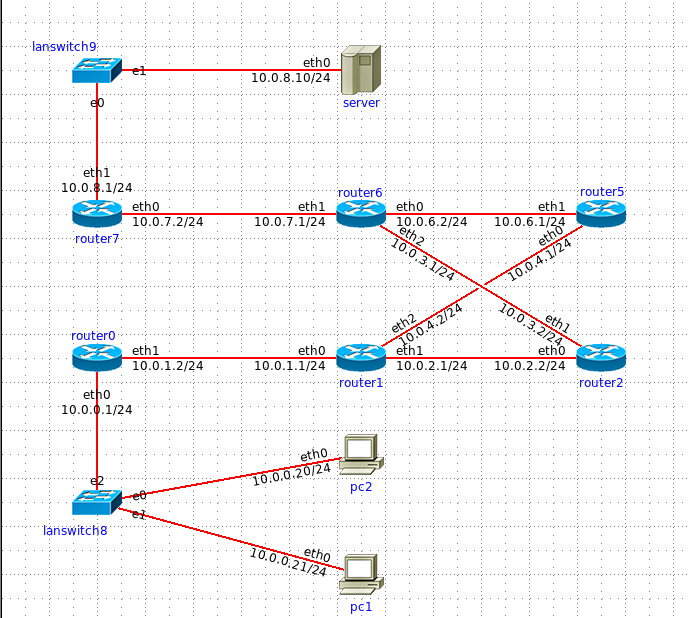
Preambula, SFD i CRC nisu prikazani u Wiresharku jer se oni obrađuju na razini fizičkog sloja (Layer 1).

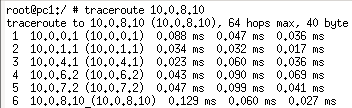
3. zadatak

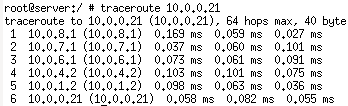
Pomoću polja Type u Ethernet zaglavlju. Dugo je dva bajta i nalazi se između izvorišne MAC adrese te podatkovnog polja okvira.

Polje Type sadrži Ethernet kod koji identificira protokol višeg sloja. (IP, ARP, VLAN itd.)

4. zadatak

¸





Putevi su simetrični.

5. zadatak

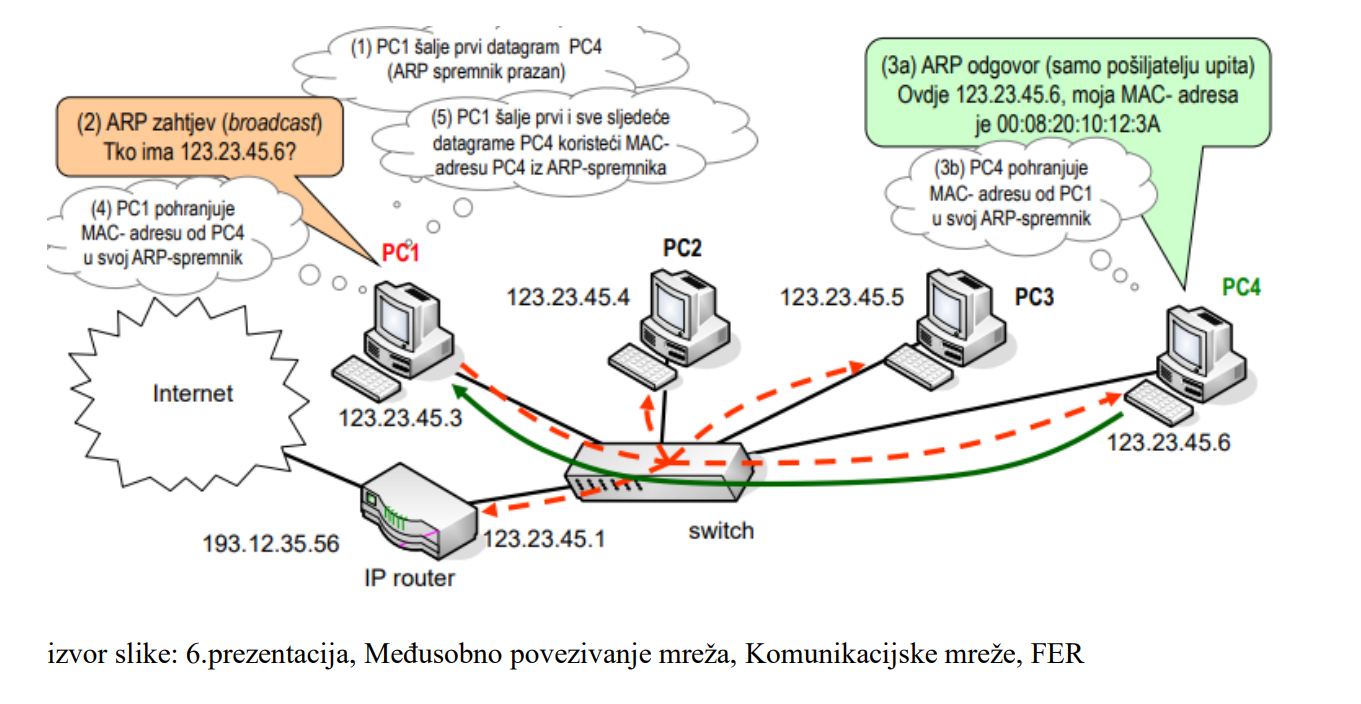
IP paketi se prenose Ethernet protokolom unutar lokalne mreže na podatkovnom sloju OSI modela i koristi MAC adrese kako bi pravilno usmjerio pakete unutar lokalne mreže.

Protokol ARP (Address Resolution Protocol) igra ključnu ulogu u tom procesu. Koristi se za mapiranje IP adresa (sloj 3) na odgovarajuće MAC adrese (sloj 2) uređaja unutar lokalne mreže. ARP šalje upit za IP-adresu mreži, tj. svim sučeljima. Svi primaju upit, no odgovor šalje samo uređaj s traženom IP adresom, no ne svima već samo prozivatelju. ARP spremnik pohranjuje uparene IP-MAC adrese na temelju navedenih upita i odgovora te ih u daljnoj komunikaciji koristi kako se ne bi ponavljao upit cijeloj mreži.

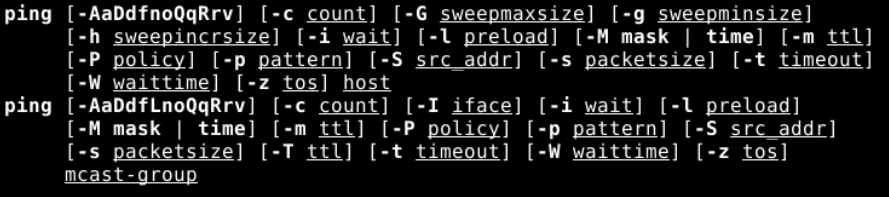
6. zadatak



* Kada uređaj želi poslati podatke drugom uređaju unutar iste lokalne mreže, ali zna samo njegovu IP adresu, šalje ARP zahtjev.
* ARP zahtjev sadrži IP adresu traženog uređaja i šalje se kao broadcast, što znači da ga svi uređaji u lokalnoj mreži primaju.
* Uređaj s traženom IP adresom prepoznaje zahtjev i šalje ARP odgovor, koji sadrži njegovu MAC adresu.
* Početni uređaj prima ARP odgovor i ažurira svoju ARP tablicu s MAC adresom traženog uređaja. Sada može poslati podatke na odgovarajuću MAC adresu.



7. zadatak



-c count – Određuje broj paketa prilikom slanja pinga

-G sweepmaxsize – Odrežuje maksimalnu veličinu ICMP datagrama prilikom pročešljavanja

-g sweepminsize – Određuje minimalnu veličinu ICMP datagrama prilikom pročešljavanja

-h sweepincrsize – Određuje koliko se veličina ICMP datagrama povećava nakon svake iteracije

-i wait – Određuje koliko će vremena proći između dva pinga

-l preload – Ako je specifičan argument, ping šalje taj broj paketa dok se ne vrati u normalno ponašanje

-M mask | time – Postavlja ICMP oznaku na echo ili repl, time je vrijeme slanja, primanja i transmisije

-m ttl – Postavlja Time To Live paketa

-P policy – Postavlja odredbe policy za odgovarajuću ping sjednicu

-p pattern – Puni pakete sa do 16 bajtova sadržanih u pattern

-S src\_addr – u odlaznim paketima koristi srd\_addr kao adresu pošiljatelja zahtjeva

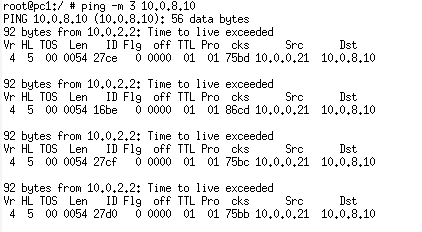
-s packetsize – Određuje veličinu paketa

-t timeout – Određuje vrijeme tijekom kojeg će se ping izvršavati

-W waittime – vrijeme čekanja odgovora u milisekundama. Zakašnjeli odgovori se ne ispisuju

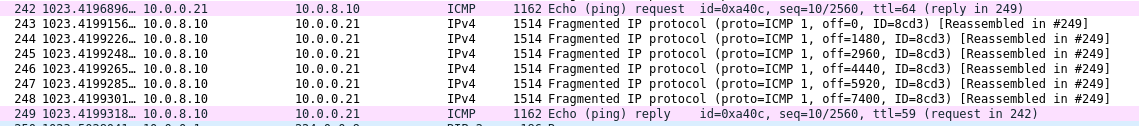
-z tos – određuje koji će se tip usluge koristiti

8. zadatak



TTL je dopušten broj skokova. S obzirom da je traženi server udaljen za više od 3 skoka, vraća nam se error poruka ttl exceeded

9. zadatak



Maksimalna transmisijska jedinica MTU iznosi 1500 okteta i to je najveća veličina koja se može prenijeti u jednom komadu. Tada je maksimalni IP datagram koji možemo poslati 1472 okteta + 8 okteta ICMP + 20 okteta zaglavlja = 1500.

Kada je ping velik 10000 okteta prvo mu se doda 8 za ICMP te iznosi 10008. Zatim se fragmentira na :

1. 1480 + 20
2. ...

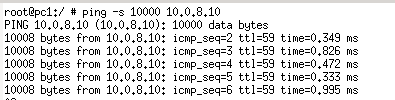
7. 80 + 20 + 8



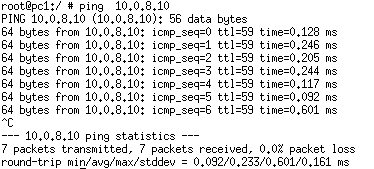
Najveći broj paketa je 65507 + 8 = 65515

10. zadatak

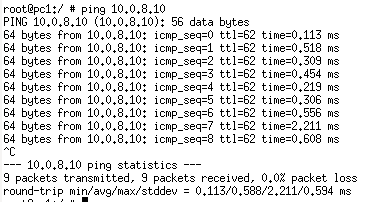
- veliki paket



- neizravno spojeni



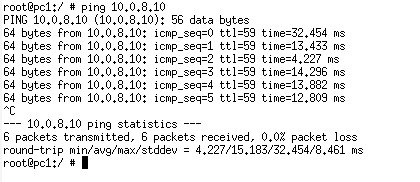
- izravno spojeni



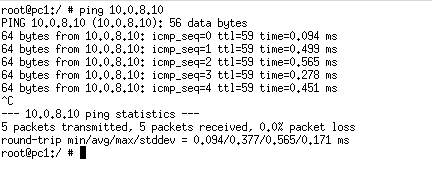
U nekom normalnom slučaju bi vrijeme izravno spojenih trebalo bit manje nego kod neizravno spojenih, ali je moje računalo odlučilo protestirat. TTL se promijeni jer postoji izravni skok sa r0 na r7

11. zadatak

Uz kašnjenje

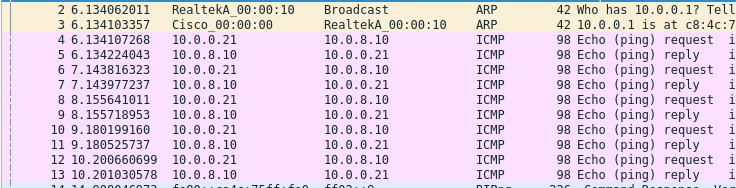


Bez kašnjenja



Propagacijsko kašnjenje ima veliki utjecaj na vrijeme prijenosa. U ovim primjerima smo dodali delay između pc1 i lanswitch8

12. zadatak



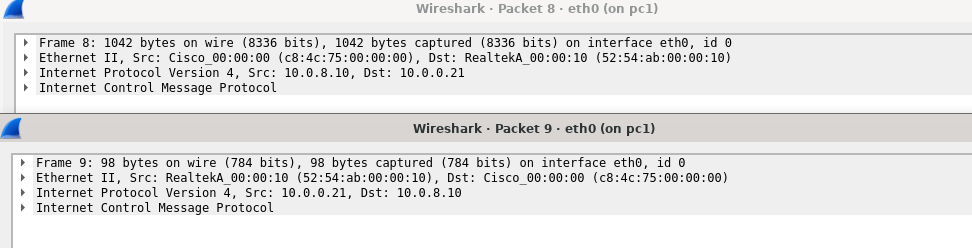
ICMP (Internet Control Message Protocol) – alat ping koristi ovaj protokol za slanje Echo Request poruka i primanje Echo Reply poruka. Pripada mrežnom sloju (sloj 3) u TCP/IP modelu.

IP – ICMP koristi IP za usmjeravanje između izvorišnog i odredišnog računala. Također pripada mrežnom sloju (sloj 3) u TCP/IP modelu

Ethernet – služi za prijenos IP paketa unutar LAN mreže između računala i mrežnih uređaja. Pripada sloju pristupa mreži (Data Access Layer) sloj 2

ARP – (Address Resolutin Protocol) – kada računalo treba poslati paket unutar LAN koristi protokol ARP kako bi pronašlo odgovarajuću MAC adresu za odredište. Pripada sloju pristupa mreži (sloj 2)

13. zadatak

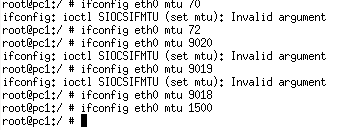


Mijenjaju se: polje podataka, duljina, padding ako je polje podataka premalo i FCS

14. zadatak

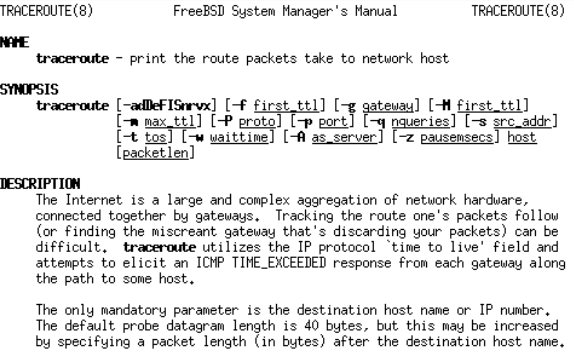
Kada pingamo loopback adresu (127.0.0.1), promet se ne šalje na ethernetsko sučelje računala. Umjesto toga, promet ostaje unutar lokalnog računala. ICMP Echo Request i ICMP Echo Reply poruke generirane naredbom ping neće napustiti računalo, već će se obraditi unutar IP sloja lokalnog računala. Kao rezultat toga, promet na ethernetskom sučelju računala ostaje nepromijenjen i neće biti vidljiv u alatu Wireshark ili drugim alatima za praćenje mrežnog prometa.

15. zadatak



Teoretski min i max za MTU su 46 i 1500, ali ako pokušamo podesiti vidimo da su rezultati 72 i 9018.

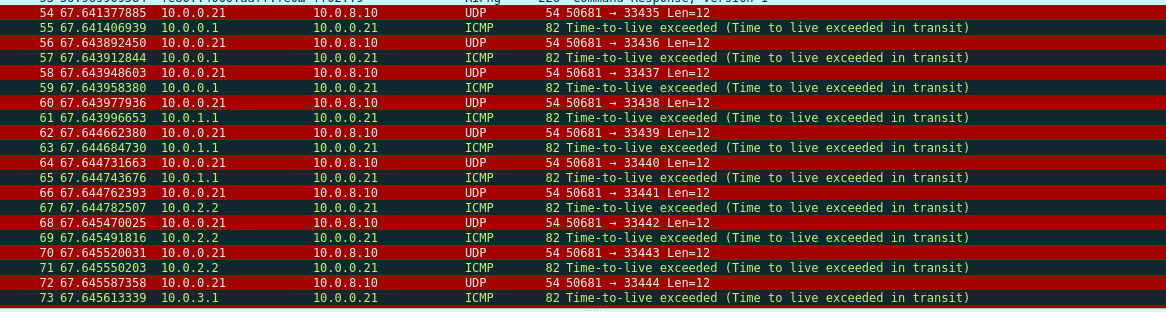
16. zadatak



Alat traceroute može proizvesti neispravne rezultate u nekoliko situacija:

1. **Loše rutiranje ili petlje**: TTL exceeded bez dostizanja odredišta
2. **Promjene na putanji usmjeravanja tijekom izvođenja traceroutea**: Ako se putanja paketa između izvora i odredišta promijeni tijekom izvođenja traceroutea (npr. zbog promjena u mrežnoj topologiji ili dinamičkog usmjeravanja), rezultati mogu biti neispravni ili zastarjeli.
3. **Korištenje drugih protokola**: Traceroute obično koristi ICMP poruke za dobivanje informacija o putanji, ali u nekim implementacijama može koristiti i druge protokole kao što su UDP ili TCP. Ovi protokoli mogu biti podložni različitim politikama filtriranja i usmjeravanja u mreži, što može dovesti do neispravnih ili nepotpunih rezultata.

17. zadatak



Mehanizam rada alata traceroute:

1. Traceroute šalje pakete s početnom vrijednošću TTL-a postavljenom na 1.
2. Svaki usmjeritelj koji primi paket smanjuje vrijednost TTL-a za 1. Ako TTL padne na 0, usmjeritelj ne šalje paket dalje i umjesto toga šalje ICMP Time Exceeded poruku natrag na izvorno računalo.
3. Kad izvorno računalo primi ICMP Time Exceeded poruku, može zaključiti da je paket stigao do usmjeritelja s TTL-om jednakim 1. Računalo tada povećava TTL za 1 (na 2) i šalje novi paket.
4. Proces se ponavlja, a svaki puta kad izvorno računalo primi ICMP Time Exceeded poruku, povećava TTL za 1 i šalje novi paket.
5. Konačno, paket stiže do odredišnog računala. Odredišno računalo šalje ICMP Echo Reply poruku natrag na izvorno računalo umjesto ICMP Time Exceeded poruke.
6. Traceroute se zaustavlja kad izvorno računalo primi ICMP Echo Reply poruku ili kad se dostigne maksimalna vrijednost TTL-a.

18. zadatak

Protokol IP "pamti" vrstu paketa koji se prenosi u podatkovnom dijelu IP-datagrama pomoću polja Protocol (ili polja Next Header u slučaju IPv6) unutar IP zaglavlja. Polje Protocol je 8-bitno polje koje sadrži identifikacijski broj koji označava vrstu protokola koji se koristi u podatkovnom dijelu IP-datagrama. Npr. TCP, UDP, ICMP

19. zadatak

Nije moguće. IP protokol je dizajniran da bude neovisan o načinu prolaska kroz mrežu, što znači da ne postoji način da rekonstruiramo put kojim je paket prošao. To možemo jedino pomoću alata traceroute koji nije 100% siguran.

20. zadatak

IP protokol sam po sebi ne pruža mehanizam za potvrdu primitka paketa na odredištu. IP protokol je nesiguran protokol, što znači da ne jamči isporuku paketa, redoslijed paketa ili ispravnost podataka u paketu. Jedino uz pomoć viših protokola kao što su TCP ili ICMP

21. zadatak

Što je veći broj paketa to je veće vrijeme čekanja da se pristigli podatci procesiraju. Veća je mogućnost gubitka paketa te je veći dodatni protokolni overhead. Svaki paket ima svoj IP header što rezultira povećanjem poslanih bitova za istu količinu informacije.