Ethernet, protokol ARP in protokol NAT

Komunikacije v avtomatiki – Laboratorijske Vaje

19. november 2013

Povzetek

V prvi vaji smo se ukvarjali z aplikacijskim slojem TCP/IP modela, kjer smo analizirali protokol HTTP. Nato smo se spustili en sloj nižje, na prenosni sloj, v katerem smo obravnavali TCP in UDP. V vaji 3 smo se spustili na mrežni sloj, znotraj katerega smo analizirali delovanje protokola IP. V teh vajah se bomo spustili na najnižji sloj, povezovalni sloj, znotraj katerega bomo obravnavali Ethernet in protokol ARP. To bo vsebina prvega dela vaje. V drugem delu pa se bomo povzpeli nazaj na mrežni in prenosni sloj, znotraj katerih bomo obravnavali protokol NAT (angl., network address translation). Naloge so razdeljene v več segmentov, vsak segment vsebuje nekaj vprašanj. Na ta vprašanja odgovorite, in jih zapišite v dokument (npr., uporabite MS Word). Da boste lažje argumentirali svoje odgovore, naredite izrise Wiresharka (angl., print screen), iz katerih so razvidni podatki, ki ste jih uporabili za odgovor, in jih priložite v dokument. Nekateri deli te vaje črpajo iz knjige *Computer Networks – A top down approach* [1], ki je na voljo tudi v fakultetni knjižnici, ter prosojnic s predavanj prof. Stanislava Kovačiča. Snov za te vaje najdete v knjigi [1] v poglavjih 5.5 (Ethernet), 5.4.1 (naslavljanje na povezovalnem sloju), 5.4.2 (protokol ARP) in 4.4 (protokol NAT).

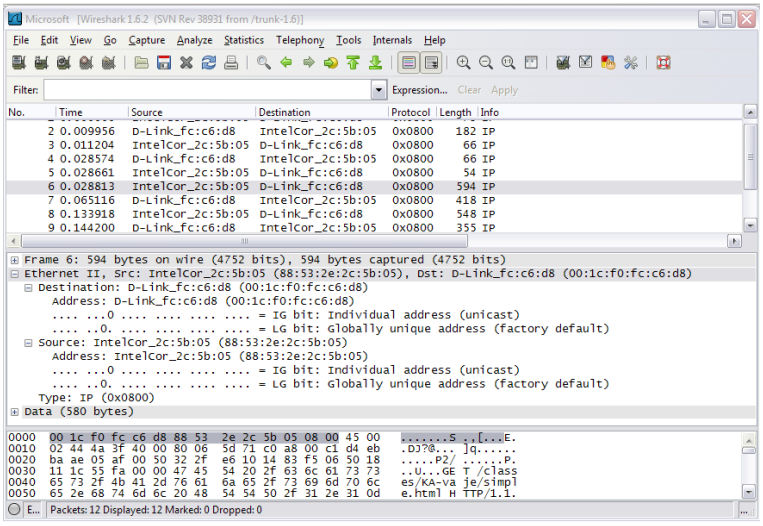
1 Zajem Ethernet okvirjev

Začeli bomo z zajemom Ethernet okvirjev. Sledite spodnjim točkam:

- Najprej izpraznite spomin v vašem spletnem brskalniku. V Firefoxu to storite tako, kot pri Vaji 1, preko *Tools→Private data*.
- Zaženite Wireshark, izberite aktivno mrežno kartico, in zaženite zajem podatkov.
- V spletni brskalnik vpišite naslov `http://www.ietf.org/rfc/rfc826.txt`. Prikaže se vam preprosta spletna stran.
- Ustavite zajem podatkov v Wiresharku. Najprej poiščite v Wiresharku dva paketa: (i) paket, ki ste ga poslali na strežnik `ietf.org` in vsebuje ukaz `HTTP GET`, (ii) kakor tudi HTTP paket s katerim vam strežnik odgovori.
- Ker se bomo v tem delu vaje ukvarjali s povezovalnim slojem, moramo odklopiti prikaz protokolov iz višjih slojev. Kakor v predhodnih vajah, poiščite *Analyze→Enabled Protocols* in izklopite kljukico pri protokolu IPv4. Sedaj bi izpis v vašem Wiresharku moral izgledati podoben izpisu v Sliki 1

Izberite Ethernet okvir, ki vsebuje sporočilo *HTTP GET*. Spomnite se, da se sporočilo HTTP prenaša znotraj segmenta TCP, ki ga nosi IP datagram, ta pa je vsebovan v Ethernet okvirju. Razširite zavihek pod Ethernet II tako, da vidite vse informacije, ki ustrezajo povezovalnemu sloju. Odgovorite na spodnja vprašanja:

1. Izpišite 48-bitni Ethernet naslov vašega računalnika.
2. Izpišite 48-bitni Ethernet naslov ponornega računalnika `ietf.org`, ki mu paket pošiljate. Ali je to Ethernet naslov *ietf.org*? Odgovor je ne – razložite zakaj je tako in katera naprava potem ima ta naslov?
3. Izpišite heksadecimalno številko polja `type`. Kaj to polje pomeni in kaj v vašem primeru pomeni njegova vsebina?



Slika 1: Primer izpisa Wiresharka, kjer prikazujemo pakete povezovalnega sloja.

4. Koliko bajtov po prvem bajtu v okvirju se nahaja ASCII znak `G` besede *GET*?
5. Preko katerih polj se izračuna vrednost CRC v Ethernet okvirjih?

Sedaj odgovorite na vprašanja, ki se tičejo paketa, ki vsebuje prvi del odgovora na poizvedbo HTTP, (HTTP response).

7. Izpišite vrednost izvornega Ethernet naslova. Ali je to naslov vašega računalnika, ali *ietf.org* ali katerega drugega? Odgovor je tretja od prej navedenih možnosti – obrazložite odgovor.
8. Kakšen je ponorni Ethernet naslov? Ali je to naslov vašega računalnika?
9. Izpišite heksadecimalno vrednost polja `type`.
10. Koliko bajtov po prvem bajtu v okvirju se nahaja ASCII znak `O` besede *OK*?

1.1 Protokol za razreševanje naslovov ARP

Sedaj si bomo ogledali primer delovanja protokola ARP. S predavanj se spomnite, da ARP v vašem računalniku hrani začasno tabelo prevedb IP naslovov v Ethernet naslove (MAC). Z vsebino tabele in protokolom ARP lahko upravljamo s klici programa `arp`. Odprite ukazno vrstico (terminal) in zaženite ukaz `arp -a`. Ta ukaz izpiše vsebino tabele ARP.

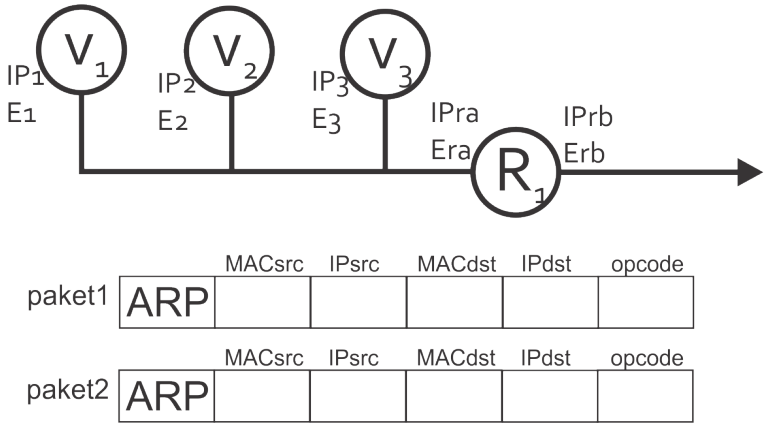
1. Izpišite si vsebino tabele ARP (sliko dodajte v poročilo) in razložite kaj pomeni posamezen stolpec.

Da bi lahko spremljali prejemanje in pošiljanje sporočil preko ARPa, moramo najprej zbrisati že vnesene Ethernet naslove iz tabele ARP. To storite tako, da v konzoli zaženete ukaz `ip neigh flush all`. Sledite spodnjim točkam, s katerimi bote posneli delovanje protokola ARP:

- Izbrišite shranjene strani (angl., cache) v svojem spletnem brskalniku.
- V Wiresharku zaženite zajem paketov.
- Izbrišite svojo ARP tabelo po postopku, ki smo ga opisali zgoraj.
- V brskalniku naredite dostop do spletne strani `http://www.ietf.org/rfc/rfc826.txt`.
- Ustavite zajem podatkov v Wiresharku. Ker nas ne zanimajo protokoli višjih slojev od Etherneta, zopet v *Analyze→Enabled Protocols* izklopite kljukico pri protokolu IPv4.

Ker na vašem računalniku verjetno teče več procesov, ki dostopajo do mrežnih storitev, je možno, da je že katera od njih sprožila ARP poizvedbo. To za reševanje te naloge ne predstavlja problema. Odgovorite na naslednja vprašanja:

2. Izpišite heksadecimalne izvorne in ponorne naslove v paketu, ki vsebuje ARP poizvedbo.



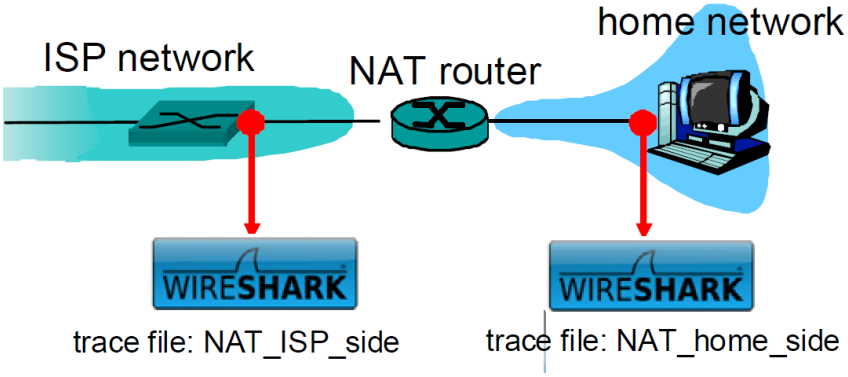
Slika 2: Primer mreže s tremi vozlišči in enim usmerjevalnikom.

3. Izpišite vrednost Ethernet polja `type`. Kaj pomeni vrednost tega polja v vašem paketu?
4. Prenesite si specifikacije protokola ARP iz `http://www.bebas.vlsm.org/v07/org/rfc-editor/rfc-ed-all/std/std37.txt`. Podrobno diskusijo najdete tudi na `http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html`.
   (a) Koliko bajtov po začetku Ethernet okvirja se nahaja značka `opcode`? Kaj ta značka pomeni v vašem paketu?
   (b) Ali vsebuje ARP sporočilo tudi naslov IP pošiljatelja?
5. Sedaj se postavite na paket odgovorni ARP, ki je poslan kot odgovor na poizvedovalni paket ARP.
   (a) Koliko bajtov po začetku Ethernet okvirja se nahaja značka `opcode`?
   (b) Kaj vrednost značka `opcode` pomeni v vašem paketu?
6. Izpišite heksadecimalne vrednosti izvornega in ponornega naslova v odgovornem paketu ARP.
7. V Sliki 2 imate primer mreže treh vozlišč (V_1,V_2 in V_3), ki so priklopljeni na usmerjevalnik R. Mrežni naslovi vozlišč so označeni z IP, fizični naslovi pa z E. Mreža je ravno začela delovati in vozlišče V_1 želi poslati paket vozlišču V_3. Ker je ARP tabela vozlišča V_1 prazna, mora to vozlišče uporabiti protokol ARP. Zato najprej pošlje poizvedbo v obliki poizvedovalnega ARP paketa (`paket1`). Ta paket dobijo vsa vozlišča in usmerjevalnik, prejme pa ga samo vozlišče V_3 in odgovori z odgovornim ARP paketom (`paket2`).
   (a) V Sliki 2 izpolnite manjkajoča polja v paketih.
   (b) Zakaj rečemo, da poizvedbeni paket prejmejo vsa vozlišča, vendar ga "odpre" samo vozlišče V_3?
   (c) Neobvezno vprašanje: kaj bi se zgodilo, če bi se vozlišče V_3 nahajalo na desni strani usmerjevalnika (na podmreži `b`, in ne `a`)?

2 Protokol prevedbe mrežnih naslovov NAT

V tem delu vaje se boste posvetili analizi protokola NAT. Za razliko od eksperimentov v prejšnjih vajah, boste v tej vaji uporabili v naprej zajet izpis iz Wiresharka. Ker moramo za analizo protokola NAT zajemati paketke z obeh strani NAT usmerjevalika, boste obdelovali dva izpisa Wiresharka, ki sta bila posneta kot prikazuje Slika 3.

Paketi so bili posneti ob dostopu računalnika do strežnika *google.com*. En izpis paketov smo dobili preko Wiresharka, ki je tekel na *domačem* računalniku (`NAT_home_side`). Drugi izpis smo dobili s prisluškovanjem mrežne povezave med domačim računalnikom in ISPjem (`NAT_ISP_side`). Paketki, ki jih zajamemo na tem koncu, so že prešli prevedbo NAT, zato



Slika 3: Skica zajema paketov pri eksperimentu z Wiresharkom. Slika je povzeta po [1].

lahko tudi opazujemo vpliv protokola NAT. Datoteko `NAT_home_side.pcap` si prenesite iz naslova `http://vision.fe.uni-lj.si/classes/KA-vaje/vaje/2012/NAT_home_side.pcap`, datoteko `NAT_ISP_side.pcap` pa iz `http://vision.fe.uni-lj.si/classes/KA-vaje/vaje/2012/NAT_ISP_side.pcap`.

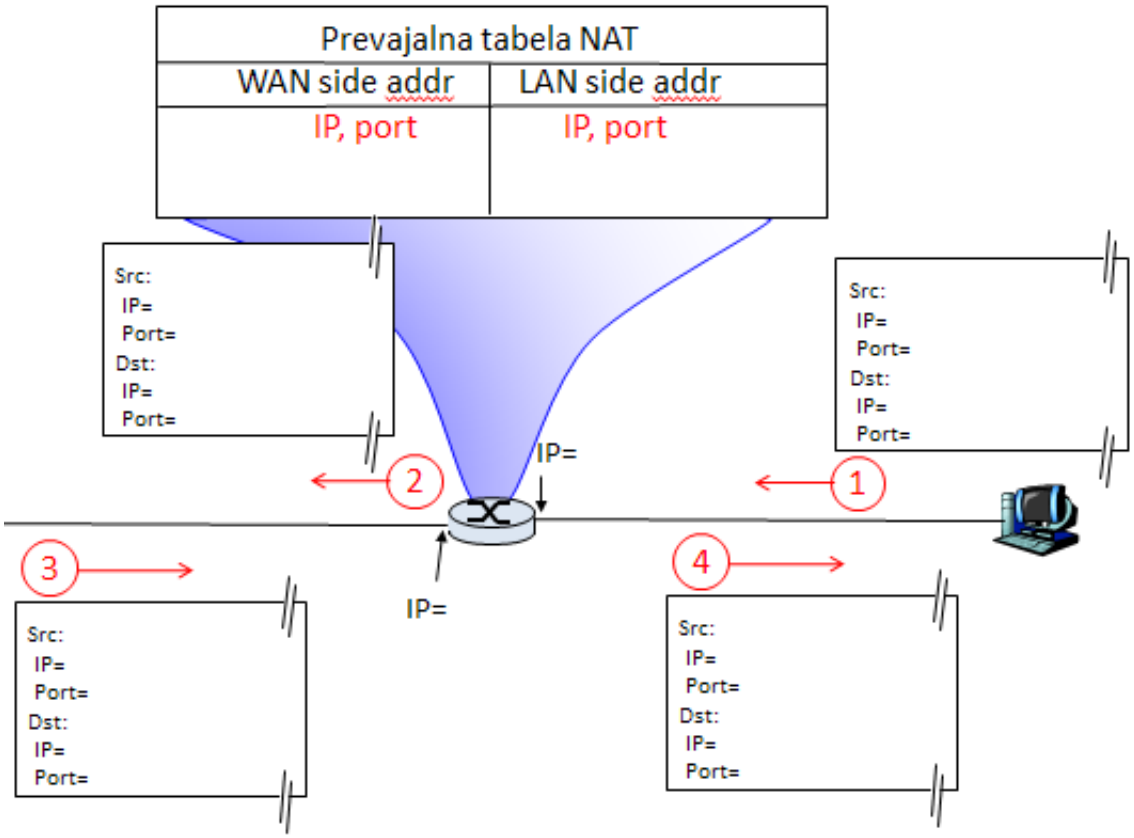
Odprite datoteko `NAT_home_side` v Wiresharku in odgovorite na naslednja vprašanja. V Wiresharku nastavite filter tako, da bo prikazoval le sporočila HTTP.

1. Kakšna je številka IP klienta (našega računalnika)?
2. Glavni Googlov strežnik, ki ga bomo spremljali v tem eksperimentu ima številko IP `64.233.169.104`. Nastavimo filter tako, da prikazujemo le HTTP paketke poslane/prejete iz tega naslova. To storite tako, da v filter vpišete `http && ip.addr==64.233.169.104`.
3. Najdite najprej paket s *HTTP GET*, ki ga klient pošlje Googlovemu strežniku ob času `7.109267`. Izpišite izvorno/ponorno številko IP in izvorni/ponorni naslov TCP porta v IP datagramu, ki nosi sporočilo *HTTP GET*.
4. Ob katerem času prejmemo odgovorni paket z vsebino *200 OK* z Googlovega strežnika?
5. Spomnite se, da se pred priklopom na HTTP strežnik vzpostavi TCP seja preko trostranskega rokovanja. Najdite paket *TCP SYN*, ki ga klient pošlje strežniku – izpišite izvorne/ponorne IP naslove in TCP porte. Izpišite izvorne/ponorne IP naslove in TCP porte potrditvenega paketka *ACK*, ki ga strežnik pošlje v trostranskem rokovanju. Pozor: da lahko najdete te paketke, boste morali filter sprazniti (*clear*) in v polje *filter* vpisati `tcp`.

V nadaljevanju se boste usredotočili na dve HTTP sporočili (*GET* in *200 OK*), ter TCP segmente *SYN* in *ACK*, ki smo jih izpostavili zgoraj. Vaša naloga bo poiskati ta dva HTTP paketa in dva TCP segmenta na strani ISPja v datoteki `NAT_ISP_side`. Bodite pozorni, da so bili ti paketi posredovani preko NAT usmerjevalnika, zato bodo IP naslovi in porti *nekoliko spremenjeni*.

V Wiresharku odprite datoteko `NAT_ISP_side`. Bodite pozorni na to, da ta datoteka ni časovna sinhronizirana z datoteko `NAT_home_side`.

6. V datoteki `NAT_ISP_side` poiščite HTTP paket z ukazom `GET`, ki ga je poslal klient. Izpišite izvorni/ponorni naslov IP ter številke TCP portov. Katere od teh vrednosti so enake in katere različne od paketa, ki ga je poslal klient usmerjevalniku (tistega v odgovoru na vprašanje 3 zgoraj)?
7. Ali so se katera polja v sporočilu *HTTP GET* spremenila? Katera polja v IP datagramu od navedenih polj so se spremenila: Version, Header Length, Flags, Checksum. Za vsako polje, ki se je spremenilo, razložite zakaj je do spremembe prišlo.
8. Najdite HTTP paket z ukazom `200 OK`, ki ga je poslal Googlov strežnik. Izpišite izvorno/ponorno številko IP in TCP porte. Katere od teh vrednosti so različne od vrednosti v paketu iz odgovora na vprašanje 4 zgoraj?



Slika 4: Skica zajema paketov pri eksperimentu z Wiresharkom. Slika je povzeta po [1].

9. Poiščite pakete TCP SYN in TCP ACK, ki odgovarjajo paketom iz vprašanja 5 zgoraj. Izpišite izvorne/ponorne številke IP in številke TCP portov. Katere vrednosti polj so enake kot pri ustreznih paketih iz vprašanja 5 zgoraj?
10. Slika 4 prikazuje tabelo NAT na usmerjevalniku. Z zaporednimi številkami 1 in 2 je označen paket TCP SYN ob prehodu preko usmerjevalnika izven notranje mreže, z zaporednimi številkami 3 in 4 pa paket TCP ACK, ki prehaja v notranjo mrežo. S podatki, ki ste jih pridobili zgoraj, izpolnite manjkajoče vrednosti v NAT tabeli, kakor tudi v paketih 1 do 4.

Literatura

[1] J.F. Kurose and K.W Ross, *Computer networking – a top-down approach*, Addison Wesley, 2009.