APLIKACIJSKI SLOJ INTERNETA

Stjepan Groš

07. 09. 2006.

Sadržaj

1. Uvod

Evolucija Interneta.

2. Multimedijalni protokoli

3. Protokoli za upravljanje računalnim mrežama

3.1. LDAP

3.2. SNMP

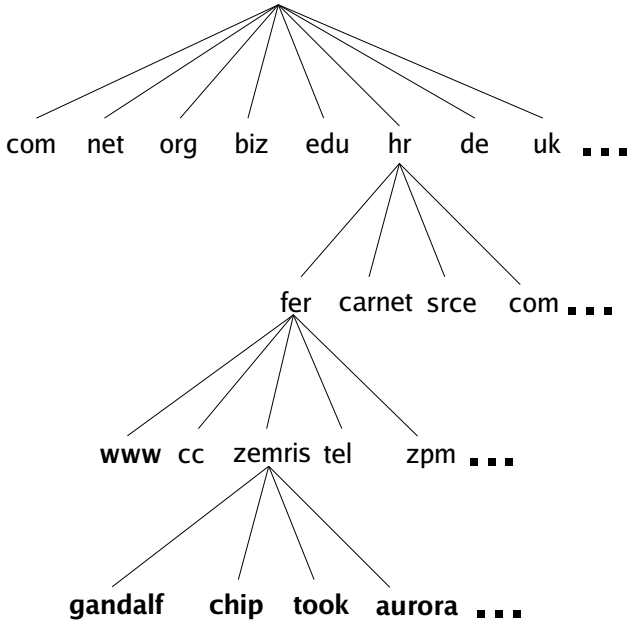
3.3. DNS

Kako je ljudima dosta teško pamtiti brojeve uvedena su simbolička imena za računala na Internetu. Određeno vrijeme, dok je Internet upotrebljavan samo za istraživačke potrebe, za pretvaranje imena u brojeve korištena je datoteka čiji format je imao sljedeći oblik [RFC952, RFC953]:

```
xxx
```

U toj datoteci za svaku IP adresu navođeno je odgovarajuće ime računala. Budući da su računala stalno dodavana najnovija verzija datoteke mogla se skinuti s jednog FTP poslužitelja na Internetu ili neke od njegovih kopija. Porastom Interneta bilo je jasno kako navedeni mehanizam ne slijedi potrebe, tj. njegova skalabilnost pokazala se izuzetno lošom. Zamjena je napravljena u vidu DNS protokola (engl. Domain Name Service) [RFC1034].

U DNS-u su sva imena hijerarhijski organizirana u tzv. **domene**, slično kao što je datotečni sustav hijerarhijski organiziran u direktorije. Cijeli sustav je distribuiran u smislu da se za svaku domenu brine posebna organizacija. Na slici 3.1 prikazana je hijerarhija domena koja vodi do glavnog poslužitelja ZEMRIS-a. Masnim slovima označena su računala.



Slika 3.1. Prikaz dijela DNS hijerarhije na Internetu

Za razliku od datotečnog sustava slika se iščitava odozdo prema gore, te se kao separator upotrebljava točka umjesto kose crte. Tako čitajući punu adresu računala Gandalf, ona ispada:

```
gandalf.zemris.fer.hr.
```

Kao primjer možemo uzeti i Web poslužitelj FER-a (IP adresa 161.53.72.11) čije puno ime je:

```
www.fer.hr.
```

Ta puna adresa još se označava i kao FQDN od engleskog izraza *Fully Qualified Domain Name*. Zadnja točka predstavlja tzv. root domenu i može se ispustiti. Prilikom pisanja imena ne postoji razlika između malih i velikih slova, tj. potpuno je ekvivalentno gandalf i GANDALF. U ovom potpunom imenu prva komponenta predstavlja računalo, dok svaka iduća predstavlja mrežu. To je slično (iako obratno) kao i kod IP adresa koje se sastoje od mrežnog i računalnog dijela.

O svakoj domeni brine se posebna organizacija. Tako se o zemris domeni brine administrator na ZEMRIS-u, o FER domeni se brine računski centar FER-a, o HR domeni se brine CARNet, itd. Zaduženje administracije je dodjela imena te otvaranje novih poddomena.

Prevođenje imena u IP adrese i obratno obavljaju posebni poslužitelji, a aplikacije komuniciraju sa poslužiteljima uz pomoć protokola koji se zove *Domain Name Service* (skraćeno **DNS**). Poslužitelji su također organizirani hijerarhijski, tj. poslužitelj za ZEMRIS domenu nalazi se na ZEMRIS-u, poslužitelj za FER domenu nalazi se u računskom centru, poslužitelj za HR domenu nalazi se u CARNet-u, itd.

RFC1034, RFC1035 Original specification

RFC4033, RFC4034, RFC4035 DNSSEC

RFC1123, RFC2181 Clarifications

3597, 2136, 1996, 1995, 3007 Major protocol enhancements

3833 Threat analysis for DNS

3.4. DHCP

3.5. RADIUS

3.6. DIAMETER

3.7. COPS

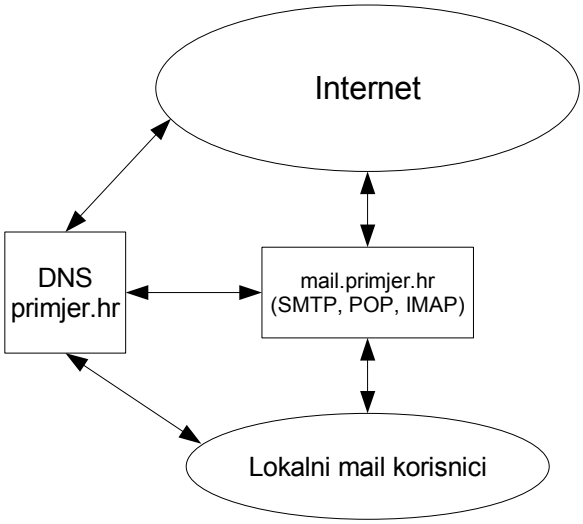
4. Elektronička pošta

Sustav elektroničke pošte bavi se elektroničkim porukama te u tu svrhu koristi nekoliko protokola. Najbitniji su protokol uz pomoć kojega se poruka predaje poslužitelju za daljnju isporuku (SMTP) te protokoli uz pomoć kojega se poruka dohvaća s poslužitelja (POP3/IMAP4).

Svaka poruka sastoji se od dva dijela. Prvi dio čini zaglavlje i u njemu se, između ostalog, nalaze podaci potrebni za rukovanje porukom tijekom njena prijenosa. Drugi dio je tijelo poruke koje se tijekom prijenosa ne mijenja. Granicu između ta dva dijela predstavlja prva prazna linija. Nakon toga, sve ostale prazne linije nemaju posebno značenje.

4.1. Rad sustava elektroničke pošte

Razmatranje rada sustava elektroničke pošte započeti ćemo od jednog jednostavnog sustava. Uzmimo primjer poslužitelj za jednu malu radnu sredinu čija domena je `primjer.hr`. Za tu domenu nužno je postaviti poslužitelj koji ima stalan pristup Internetu. Kako domena nije velika nema potrebe za zasebnim poslužiteljima koji će isporučivati mail korisnicima (POP/IMAP poslužitelji). Slika 4.1 shematski prikazuje konfiguraciju. Bitna komponenta mail sustava je i DNS sustav koji je također prikazan na slici. Za početak ćemo pretpostaviti kako je u DNS bazu dodan zapis za ime `mail.primjer.hr`.



Slika 4.1. Primjer konfiguracije poslužitelja elektroničke pošte

Da lokalni mail korisnici mogu početi primati i slati elektroničku poštu potrebno je u njihove mail klijente upisati adresu odlaznog mail poslužitelja i dolaznog mail poslužitelja. Kako jedan poslužitelj nudi obje funkcionalnosti to znači da se za obje usluge piše ime `mail.primjer.hr`. Razlika je u tome da se usluga za odlazni mail nalazi na pristupu 25 TCP protokola, dok se usluga za dolazni mail nalazi na pristupu 110 (pop3), odnosno na pristupu 143 (IMAP4).

Pretpostavimo da jedan od korisnika, čija mail adresa je `korisnik1@primjer.hr`, radi na računalu `pc1.primjer.hr` te da je napisao elektroničku poruku za drugog korisnika čija adresa je `korisnik2@primjer.hr`. Njegov mail klijent spaja se na odlazni mail poslužitelj i uz pomoć SMTP protokola šalje poruku. SMTP je prilično jednostavan protokol u kojemu SMTP klijent daje naredbe SMTP poslužitelju koji na njih odgovara upotrebom predefiniranih statusa. Za primjer slanja navedene poruke razmjena naredbi i podataka teče sljedećim tokom. Klijent otvara vezu i linije koje on šalje su označene sa C, a one koje šalje poslužitelj sa S:

```
S: 220 mail.primjer.hr ESMTP
```

```
C: EHLO pc1.primjer.hr
S: 250-mail.primjer.hr
S: 250 SIZE 5000000
```

Svaka linija mora završiti s CRLF nizom. Prvu liniju šalje poslužitelj odmah po otvaranju veze i u njoj daje svoje ime i niz ESMTP. Niz ESMTP je obavezan za poslužitelje koji podržavaju novije specifikacije SMTP protokola.

Nakon poslužiteljeva pozdrava klijent se identificira koristeći naredbu EHLO. Na tu naredbu poslužitelj odgovara pozitivno pri čemu se identificira i navodi proširenja koja podržava zajedno s odgovarajućim parametrima. U navedenom primjeru nema proširenja već poslužitelj samo informira klijenta kako maksimalna veličina maila što ga prihvaća iznosi 5000000 okteta.

Iz navedenog ispisa možemo vidjeti još dvije stvari. Prvo, ako se odgovor sastoji od više od jedne linije tada svaka linija, osim zadnje, odmah poslije numeričkog koda odgovora sadrži znak minus (-). Time se obavještava klijent da slijedi barem još jedna linija odgovora.

Druga stvar koja se može primjetiti je da se svaki odgovor sastoji od numeričkog i tekstualnog dijela. Numerički dio je relevantan u smislu da njegovom analizom klijent određuje odgovor. Tekstualni dio služi za čovjeka i moguće je da se izmjeni, tj. nije ga uputno analizirati prilikom izrade programa kako bi se odredio odgovor poslužitelja.

Nakon inicijalnog dogovora klijent šalje informaciju poslužitelju o onome tko šalje i kome se šalje elektronička poruka korištenjem naredbi MAIL FROM i RCPT TO na sljedeći način:

```
C: MAIL FROM: <korisnik1@primjer.hr>
S: 250 Ok
C: RCPT TO: <korisnik2@primjer.hr>
S: 250 Ok
```

Poslužitelj pozitivno odgovara na zahtijev klijenta za slanjem pošte i zbog toga može započeti prijenos. Početak poruke označava se korištenjem naredbe DATA:

```
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: Ovo je mail
C:
C: Ovo je tijelo poruke.
C: .
S: 250 Ok: queued as XXXXXXXXXX
```

Kada poslužitelj odgovori s OK nakon prihvata poruke od tog trenutka na dalje on se brine o njenoj isporuci ili o obavijesti kako nije bilo moguće isporučiti poruku. Po završenom prijenosu klijent inicira prekid veze korištenjem naredbe QUIT.

```
C: QUIT
S: 221 Bye
```

Budući da su obje mail adrese u istoj domeni koju opslužuje navedeni poslužitelj isporuka se obavlja odmah u poštanski sandučić korisnika 2. Korisnik čija mail adresa je korisnik2@primjer.hr pristupa poruci korištenjem protokola POP. POP je vrlo jednostavan protokol koji omogućava pristup poštanskim sandučićima. Odmah po spajanju klijent se autentificira poslužitelju:

```
S: +OK Hello there.
C: USER korisnik2
S: +OK Password required
C: PASS lozinka
S: +OK logged in.
```

Nakon što je logiran korisnikov klijent može izlistati sadržaj poštanskog sandučića korištenjem naredbe LIST. Izlaz naredbe LIST je niz linija od kojih se svaka sastoji od ID-a maila i njegove veličine. Dohvaćanje maila obavlja se korištenjem naredbe RETR. Argument naredbe RETR je ID maila. Konačno, ako je potrebno obrisati određenu poruku koristi se naredba DELE čiji parametar je ID poruke.

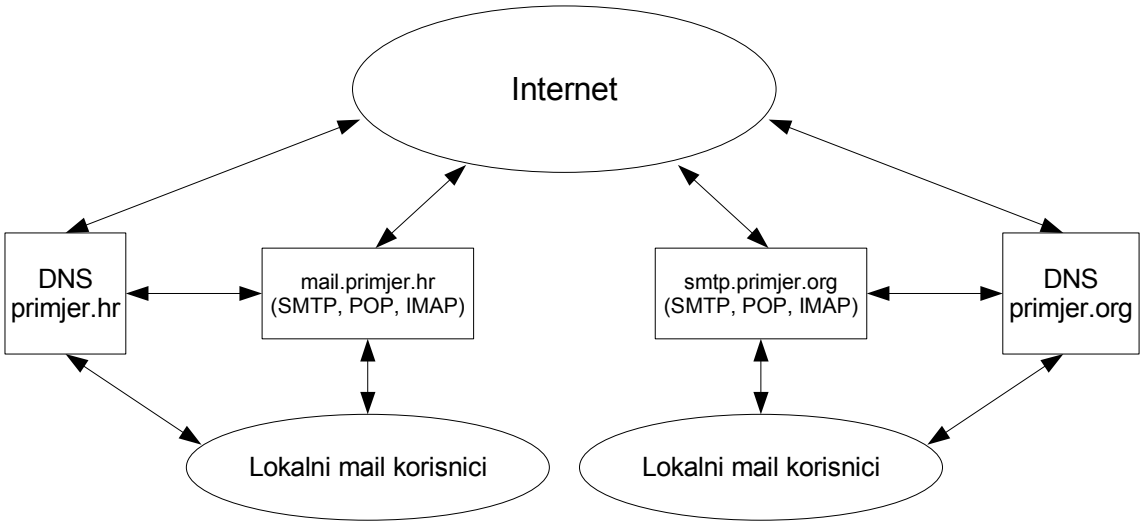
Kraj rada označava se naredbom QUIT.

```
C: QUIT
S: +OK bye-bye.
```

Upravo opisana konfiguracija omogućava slanje i primanje elektroničke pošte unutar lokalne mreže, a također omogućava slanje maila na Internet. Kako bi korisnici unutar lokalne mreže mogli primati mail od bilo koga potrebno je u DNS poslužitelj domene primjer.hr upisati MX zapis. MX zapis određuje koje računalo (ili računala) su zadužena za primanje poruka. U našem primjeru potrebno je DNS poslužitelju upisati sljedeći zapis

```
primjer.hr          IN        MX        10        mail.primjer.hr
```

Sada je moguće primati mail iz vana. Uzmimo primjer domene `primjer.org` čiji korisnik `korisnik3@primjer.org` želi poslati poštu korisniku `korisnik1@primjer.hr`. Shema mail sustava u tom slučaju prikazana je na slici 4.2.



Slika 4.2. Konfiguracija elektroničke pošte za dvije domene

Kada korisnik u domeni `primjer.org` složi mail poruku on ju šalje poslužitelju `smtp.primjer.org`. Razmjena naredbi i podataka slična je već navedenoj razmjeni poruka između korisnika u `primjer.hr` domeni, tj.

```
S: 220 smtp.primjer.org ESMTP
C: EHLO korisnik3.primjer.org
S: 250-smtp.primjer.org
S: 250 SIZE 1000000
C: MAIL FROM: <korisnik3@primjer.org>
S: 250 Ok
C: RCPT TO: <korisnik1@primjer.hr>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: franjo.tudman@fer.hr
C: Subject: Ovo je novi mail
```

```
C:
C: A ovo je tijelo poruke.
C: .
S: 250 Ok: queued as XXXXXXXXXXX
C: QUIT
S: 221 Bye
```

Nakon što je `smtp.primjer.org` prihvatio poruku on ju treba isporučiti na odredište. Prvo što mail poslužitelj obavlja je upit DNS poslužitelju koji mail poslužitelj je zadužen za domenu kojoj je namijenjen mail, tj. za `korisnik1@primjer.hr`.

Na osnovu informacije koja je upisana u DNS poslužitelj domene `primjer.hr` dobija se nazad informacija da je za nju zadužen `mail.primjer.hr` s preferencom 10, a također se dobija IP adresa poslužitelja. Poslužitelj `smtp.primjer.org` se potom spaja na navedenu IP adresu i ponavlja cjelokupni postupak razmjene podataka i informacija, odgovarajuće modificiran, tj.

```
S: 220 mail.primjer.hr ESMTP
C: EHLO smtp.primjer.org
S: 250-mail.primjer.hr
S: 250 SIZE 5000000
C: MAIL FROM: <korisnik3@primjer.org>
S: 250 Ok
C: RCPT TO: <korisnik1@primjer.hr>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: franjo.tudman@fer.hr
C: Subject: Ovo je novi mail
C:
C: A ovo je tijelo poruke.
C: .
S: 250 Ok: queued as XXXXXXXXXXX
C: QUIT
S: 221 Bye
```

U tom trenutku odredišni mail poslužitelj vrši isporuku poruke u poštanski sandučić. Očito je kako SMTP poslužitelji dosta vjeruju primatelju te se u naredbi `MAIL FROM` može navesti nepostojeća mail adresa isto kao što se u zaglavlju poruke mogu navesti lažirani podaci. Kako bi se riješio taj problem, tj. bar umanjila mogućnost lažiranja poruka uvedeni su neki dodaci.

Za početak, mail poslužitelj prihvatiti će poruku isključivo ako je zadovoljen jedan od sljedeća dva uvijeta:

1. Poruku šalje korisnik koji pripada domeni koju opslužuje sam poslužitelj. Ovaj uvijet provjerava se na jedan od dva načina. Prvi način je da su definirane "povjerljive" mreže. U tom slučaju dovoljno je da se korisnik spoji s računala čija IP adresa pripada toj mreži i može poslati mail bilo kome. Druga metoda je da se korisnik autentificira. U tom slučaju korisnik ne mora pripadati određenoj mreži već se može spojiti s proizvoljne mreže. Ovaj pristup je bolji sa stanovišta korisnika no potrebno je osigurati kako treća strana ne bi došla do povjerljivih podataka (lozinke).
2. Odredišna mail adresa je na domeni koju poslužuje mail poslužitelj. Primjerice, kada se šalje na adresu korisnik1@primjer.hr mail poslužitelj mail.primjer.hr će prihvatiti poruku od bilo kojeg mail poslužitelja, dok će ju poslužitelj smtp.primjer.org prihvatiti isključivo ako dolazi sa povjerljive mreže

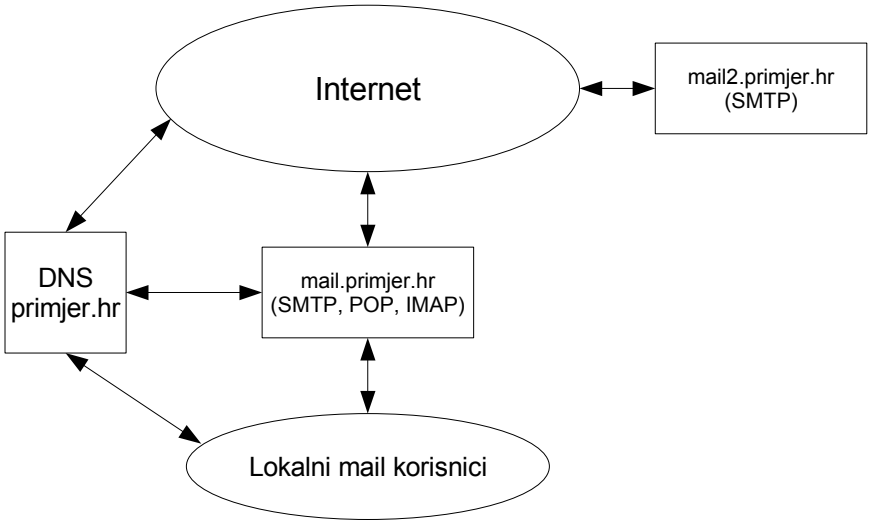
Uprkos ta dva ograničenja dosta često se dešava da poslužitelji nisu dobro konfigurirani te da omogućavaju slanje poruka s bilo koje adrese na bilo koju adresu. Izraz za takve mail poslužitelje je *open mail relay* i predstavljaju glavni problem na Internetu. Kako bi se donekle ublažio problem svaki mail poslužitelj dodaje posebno polje zaglavlju čiji opći izgled je otprilike sljedeći:

```
Received: from allevil.dishone.st
          (IDENT:A10h7hqBaNWiTCjQ8/Be6e1wWxeVZBH5@localhost [127.0.0.1])
          by allevil.dishone.st (8.12.8/8.12.8) with ESMTP id j0HEwT9w018532;
          Mon, 17 Jan 2005 15:00:44 GMT
```

Taj blok označava od koga je prihvaćena poruka (`from`), od koga (`by`) i datum kada je razmjenjena. Svaki novi zapis dodaje se ispred svih već postojećih pa za iščitavanje puta što ga je mail prošao treba krenuti od najnižeg zapisa `Received` prema vrhu.

4.1.1. Metode povećanjavanja pouzdanosti sustava elektroničke pošte

Zbog pouzdanosti sustava elektroničke pošte često se dodaju rezervni mail poslužitelji. Uzmimo primjer kada je navedena mala sredina postala prilično ovisna o usluzi elektroničke pošte, te si ne može dopustiti probleme sa primanjem maila. Prvi korak u tom smjeru je uvođenje rezervnog mail poslužitelja. Recimo da se zove `mail2.primjer.hr`, a smješten je negdje na Internetu kako to prikazuje slika 4.3.



Slika 4.3. Dodavanje rezervnog mail poslužitelja za domenu primjer.hr

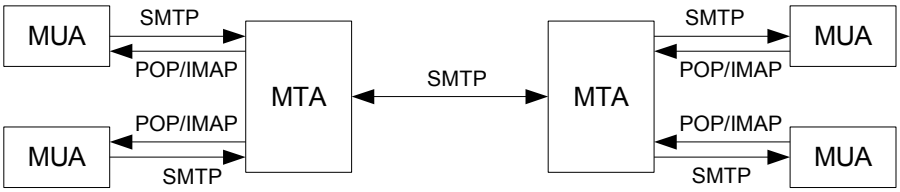
Dobro mjesto za smještanje novog mail poslužitelja je primjerice ISP od kojega je zakupljen stalan ili privremeni pristup na Internet. Još bolje je ako se taj dodatni mail poslužitelj nalazi kod drugog ISP-a jer se na taj način dodatno povećava pozdanost cjelokupnog sustava.

Rezervni mail poslužitelj počinje primati mail onog trenutka kada se informacija o njemu upiše u DNS, te se ona proširi po Internetu. Zapis može imati sljedeći oblik:

```
primjer.hr          IN        MX        20        mail2.primjer.hr
```

U navedenom zapisu smanjen je prioritet poslužitelja (20) budući da je on rezervni te je njegova namjena primanja elektroničke pošte primarno kada glavni poslužitelj ne radi ili je preopterećen.

Model usluge elektroničke pošte na Internetu prikazan je na slici 4.4.



Slika 4.4. Arhitektura sustava elektroničke pošte

Na slici dominiraju dvije bitne komponente; korisnički agenti (Mail User Agent, MUA) i prijenosni agenti (Mail Transport Agent, MTA). Korisnički agenti su različiti programi za čitanje elektroničke pošte, primjerice Evolution, Mozilla, Eudora ili Outlook. S druge strane, prijenosni agenti izvršavaju se na poslužiteljima i skriveni su od korisnika te o njima brinu administratori. Primjer popularnijih prijenosnih agenata su Postfix, Sendmail ili Exchange. Navedene komponente međusobno komuniciraju upotrebom odgovarajućih protokola. Za komunikaciju prema prijenosnom agentu koristi se SMTP protokol (engl. Simple Mail Transfer Protocol), dok se za komunikaciju prema korisničkom agentu upotrebljava POP (engl. Post Office Protocol) ili IMAP (engl. Internet Message Access Protocol) protokoli.

4.2. Format elektroničkih poruka

Format elektroničkih poruka specificiran je u više RFC-ova. Temeljna i prva specifikacija je [RFC0822]. Ta speficikacija je revidirana u [RFC2822] i opis u ovom tekstu temeljen je na toj reviziji. Navedene dvije specifikacije definiraju format isključivo tekstualnih poruka. Način prenošenja poruka s drugim sadržajem, primjerice video, audio ili sa slikama definiran je u proširenjima koja su opisana u zasebnim potpoglavljima.

Svaka poruka mora minimalno sadržavati vrijeme nastanka i adresu pošiljatelja. Sva ostala polja su opcionalna. Primjer jednostavne poruke sa navedenim zaglavljem

4.3. SMTP

Kategorije SMTP odgovora....

4.4. POP

4.5. IMAP

5. Protokoli za prijenos podataka

5.1. TFTP

TFTP (Trivial File Transfer Protocol) vrlo je jednostavan protokol za razmjenu datoteka. Njegova primarna namjena je za prijenos jezgre operacijskog sustava tijekom podizanja računalnih sustava i za pohranu konfiguracijskih datoteka mrežnih uređaja putem računalne mreža. Iako su to najčešće primjene protokola nisu jedine.

Kako bi se postigao što viši stupanj jednostavnosti iz protokola je izuzeto dosta mogućnosti, primjerice autentifikacija i autorizacija. Iz tog razloga preporuča se upotrebljavati TFTP u strogo kontroliranim sigurnosnim uvijetima u kojima je prilikom upotrebe protokola potrebno dobro kontrolirati pristup poslužitelju.

Za prijenos podataka putem mreže protokol koristi UDP prijenosni sloj.

RFC0906 Bootstrap

RFC1350 standard

RFC1785

RFC2347

RFC2348

RFC2349

RFC2090 Multicast option

RFC3617 URI

RFC1986

5.2. FTP

5.3. iSCSI

RFC3720, RFC3721, RFC3722, RFC3723

6. Telefonija

6.1. SIP

7. Web protokoli

7.1. HTTP

RFC1945, HTTP/1.0

RFC2616, HTTP/1.1

7.2. BEEP

RFC3080

7.3. WebDAV

RFC2518, WebDAV

8. Sigurnost

8.1. S/MIME

9. Primjeri

PRIMJER 1. Prijenos podataka TFTP protokolom

Prikazati prijenos datoteke *test.c* veličine 1024 okteta od klijenta do poslužitelja. Za prijenos se koristi mod *octet*. Izračunati broj razmjenjenih paketa i vrijeme prijenosa podataka ako kašnjenje prijenosa od klijenta do poslužitelja iznosi 1ms, a brzina prijenosa iznosi 1kb/s. Pretpostavite da nema izgubljenih ili oštećenih paketa.

Rješenje

Odmah nakon pokretanja klijent šalje zahtijev za pisanjem poslužitelju koji ima sljedeći oblik

1: IP(P_{IP}, K_{IP}, UDP(69, 32769, TFTP(WRQ, "test.c", "octet")))

Brojka ispred paketa samo služi kao referentna oznaka za kasniji grafički prikaz komunikacije. Po primitku tog zahtijeva poslužitelj uzima novi pristup i vraća odgovor klijentu sljedećeg oblika

2: IP(K_{IP}, P_{IP}, UDP(32769, 32800, TFTP(ACK, 0)))

Na potvrdu poslužitelja klijent šalje prvi blok podataka

3: IP(P_{IP}, K_{IP}, UDP(32800, 32769, TFTP(DATA, 1, 512)))

Poslužitelj potom potvrđuje taj blok podataka

4: IP(K_{IP}, P_{IP}, UDP(32769, 32800, TFTP(ACK, 1)))

Klijent šalje drugi blok podataka

5: IP(P_{IP}, K_{IP}, UDP(32800, 32769, TFTP(DATA, 2, 512)))

Poslužitelj odgovara s potvrdom

6: IP(K_{IP}, P_{IP}, UDP(32769, 32800, TFTP(ACK, 2)))

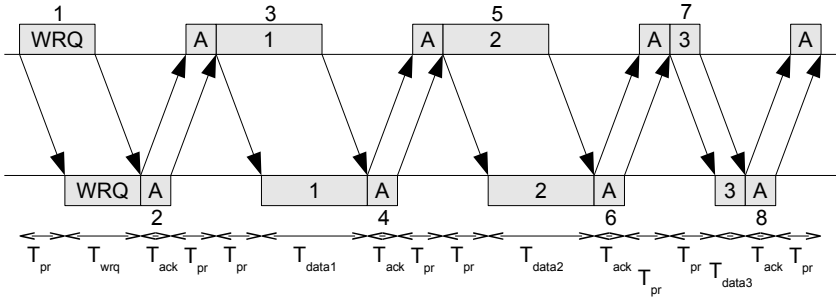
Konačno, kako je poslao cijelu datoteku klijent šalje zadnji podatkovni blok koji osim zaglavlja ne sadrži nikakve dodatne podatke

7: IP(P_{IP}, K_{IP}, UDP(32800, 32769, TFTP(DATA, 3, 0)))

Na što poslužitelj odgovara s potvrdom. Poslužitelj može još neko vrijeme čekati u slučaju da njegov ACK nije stigao do odredišta. Ako ACK nije stigao do odredišta ponovo će stići zadnji podatkovni paket.

8: IP(K_{IP}, P_{IP}, UDP(32769, 32800, TFTP(ACK, 3)))

Nakon što je završio s prijenosom poslužitelj čeka novi zahtijev za vezom. Grafički se navedena komunikacija može prikazati sljedećim vremenskim dijagramom. Na dijagramu je označeno i trajanje pojedinih vremenskih intervala.



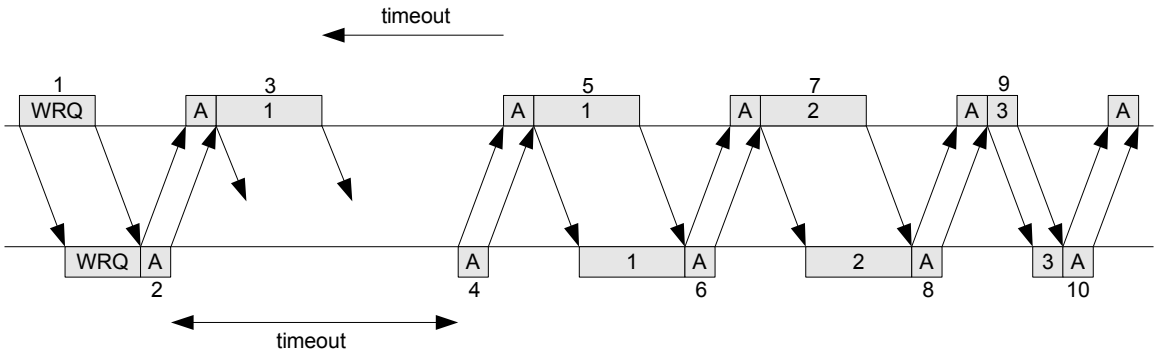
S T_{pr} označeno je vrijeme propagacije koje prema uvijetima zadatka iznosi 1ms, zatim s T_{wrq} je označeno vrijeme prijenosa paketa s zahtijevom za pisanje. S T_{ack} označeno je vrijeme prijenosa potvrde. Konačno, s T_{dataN} označeno je vrijeme prijenosa N-tog podatkovnog paketa. Vremena prijenosa svih podatkovnih paketa do zadnjega su ista.

PRIMJER 2. Prijenos podataka TFTP protokolom u prisustvu pogrešaka

Prikazati prijenos datoteke *test.c* veličine 1024 okteta od klijenta do poslužitelja. Za prijenos se koristi mod *octet*. Izračunati broj razmjenjenih paketa i vrijeme prijenosa podataka ako kašnjenje prijenosa od klijenta do poslužitelja iznosi 1ms, a brzina prijenosa iznosi 1kb/s. Pretpostavite da je prvi poslani podatkovni okvir izgubljen, a da je vremensko ograničenje na klijentu i poslužitelju 5s.

Rješenje

Na dijagramu je prikazan slijed događaja za zadani slučaj:



Kao i u prethodnom primjeru komunikacija kreće s zahtijevom klijenta za pisanjem.

1: IP(P_{IP}, K_{IP}, UDP(69, 32769, TFTP(WRQ, “test.c”, “octet”)))

Poslužitelj odobrava zahtijev s ACK paketom

2: IP(K_{IP}, P_{IP}, UDP(32769, 32800, TFTP(ACK, 0)))

Na potvrdu poslužitelja klijent šalje prvi blok podataka

3: IP(P_{IP}, K_{IP}, UDP(32800, 32769, TFTP(DATA, 1, 512)))

Međutim taj blok podataka se gubi. Nakon slanja svakog paketa i klijent i poslužitelj čekaju odgovor druge strane koji mora stići unutar određenog vremenskog perioda. Vremenski period mjeri se uz pomoć brojila koja signaliziraju kada je vrijeme isteklo. Ako po isteku vremenskog perioda nije primljen odgovor ponovo se šalje zadnji paket te se ponovo pokreće vremensko brojilo. U slučaju da opet nije prihvaćen nikakav odgovor postupak se ponavlja određen broj puta nakon čega se odustaje pod pretpostavkom da nešto nije u redu s drugom stranom ili mrežom koja spaja dvije strane.

Kako je u ovom slučaju poslužitelj prvi pokrenuo vremensko brojilo, a nije primio podatkovni paket, nakon isteka vremenskog ograničenja on ponovo šalje potvrdu zadnjeg primljenog paketa. Klijent, koji prihvaća tu potvrdu (koja ima slijedni broj prethodno poslanog okvira) primjećuje da nešto nije bilo u redu i ponovo šalje podatkovni paket. Treba primjetiti kako klijentu nije isteklo vremensko ograničenje te to slanje nije posljedica njegova isteka već primitka potvrde sa starim slijednim brojem.

Nako što je klijent ponovo poslao podatkovni paket on pristiže do poslužitelja i nakon toga nastavak razmjene je identičan prethodnom primjeru.

10. Literatura

[RFC0906] Finlayson, R., *Bootstrap loading using TFTP*, RFC906, IETF, June 1984. http://www.ietf.org/rfc/rfc0906.txt?number=906

[RFC1350] Sollins, K., *TFTP Protocol (Revision 2)*, RFC1350, IETF, July 1992. http://www.ietf.org/rfc/rfc1350.txt?number=1350

[RFC1785] Malkin, G., Harkin, A., *TFTP Option Negotiation Analysis*, RFC1785, IETF, March 1995. http://www.ietf.org/rfc/rfc1785.txt?number=1785

[RFC1986] Polites, W., Wollman, W., Woo, D., Langan, R., Experiments with a Simple File Transfer for Radio Links Using Enhanced Trivial Transfer Protocol (ETFTP), RFC1986, IETF, March 1995. http://www.ietf.org/rfc/rfc1986.txt?number=1986

[RFC2090] Emberson, A., *TFTP Multicast Option*, RFC2090, IETF, February 1997. http://www.ietf.org/rfc/rfc2090.txt?number=2090

[RFC2347] Malkin, G., Harkin, A., *TFTP Option Extension*, RFC2347, IETF, May1998. http://www.ietf.org/rfc/rfc2347.txt?number=2347

[RFC2348] Malkin, G., Harkin, A., *TFTP Blocksize Option*, RFC2348, IETF, May1998. http://www.ietf.org/rfc/rfc2348.txt?number=2348

[RFC2349] Malkin, G., Harkin, A., *TFTP Timeout Interval and Transfer Size Options*, RFC2349, IETF, May1998. http://www.ietf.org/rfc/rfc2349.txt?number=2349

RFC3617 URI