Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu
Zavod za elektroničke sustave i obradbu informacija
Laboratorij za sustave i signale

Sustavi za praćenje i vođenje procesa

vježba br. 4: **Internet**

O ČEMU JE RIJEČ...

U ovoj vježbi pažnja će se posvetiti osnovnim konceptima koji se javljaju na Internetu. Naglasak je dan na prijenosni i aplikacijski sloj OSI referentnog modela.

ŠTO BI TREBALO ZNATI NAKON VjEŽBE

Nakon vježbe očekuje se razumijevanje funkcija prijenosnog sloja OSI referentnog modela koji se javlja na Internetu, koncepta portova te znanje o mogućem načinu filtriranja mrežnih paketa.

DODATNA LITERATURA

Materijali s predavanja i skripta o temi: Internet

ZADACI

1. Mrežni sloj

1.1. Usmjeravanje IP paketa na Internetu

FER je spojen na CARNet-ovu računalnu mrežu i preko nje ostvaruje spoj prema Internetu.

Mreža CARNet privatna je WAN mreža hrvatske akademske i znanstveno-istraživačke zajednice. Mrežnu infrastrukturu posjeduje CARNet ustanova, a bakrene i optičke veze zakupljene su od Hrvatskih telekomunikacija. Ministarstvo znanosti i tehnologije Republike Hrvatske osnovalo je CARNet kao ustanovu kojoj je djelatnost razvoj, izgradnja i održavanje mreže.

Na usmjerniku (engl. router) u distribucijskom čvorištu SRCE, Zagreb ostvarena je veza prema evropskoj istraživačkoj mreži GEANT brzinom 1.2Gbps.

Slika 1. CARNet mreže u Hrvatskoj s prikazanim linkovima prema svijetu
(preuzeto sa http://www.carnet.hr/network/)

Na vježbi se koristi program ***VisualRoute*** (ikona se nalazi na desktopu). Pomoću njega se može vidjeti preko kojih računala (routera) paket prolazi na putu do njegovog odredišta. Nakon startanja možete upisivati adrese odredišta bilo preko punog imena ili samo IP adrese.

- Doznajte kuda putuju paketi npr. na putu do ovih odredišta:

`www.zesoi.fer.hr`

`pinus.cc.fer.hr`

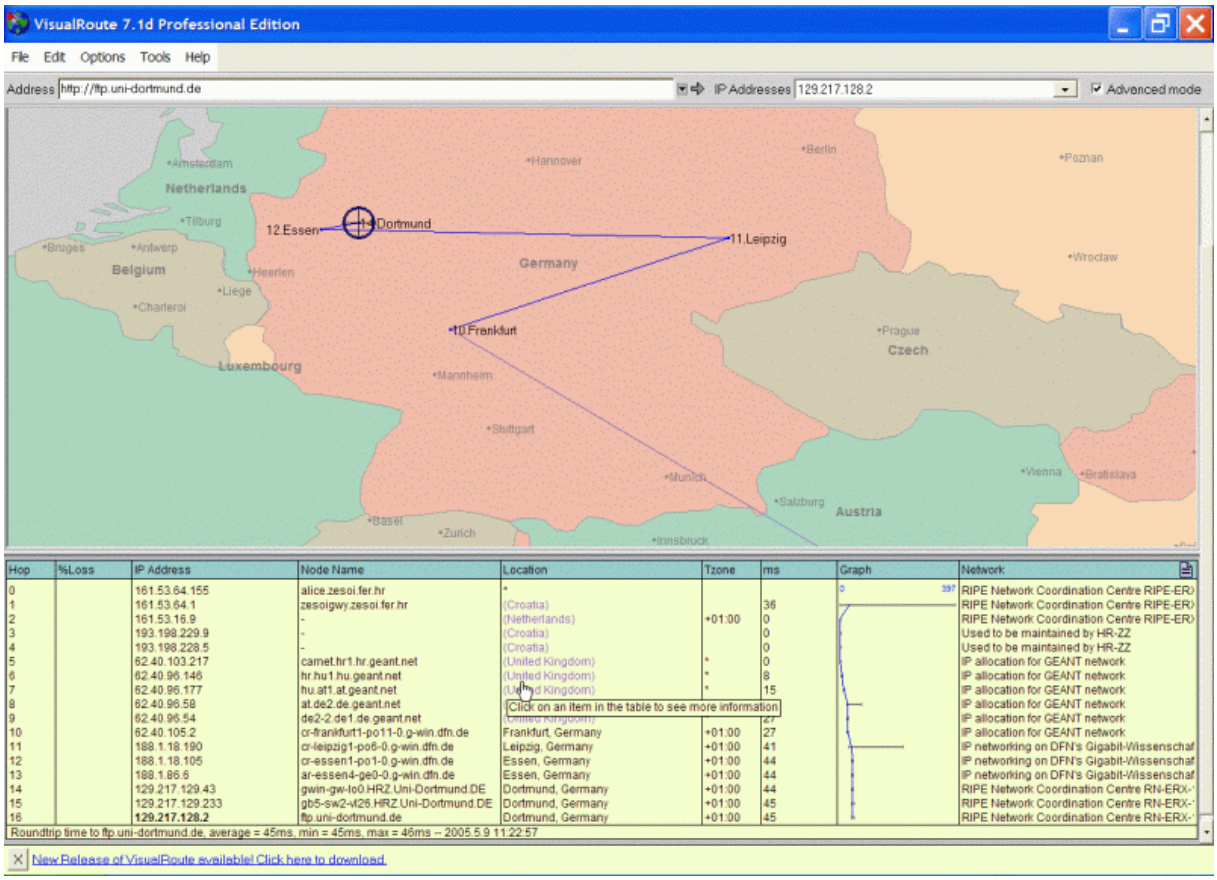
`ftp.uni-dortmund.de`

`www.google.com`

`www.gvc.com`

`www.auckland.ac.nz`

- Uočite tipične međukorake na putu do odredišta. Koji su svima zajednički?



Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		161.53.64.155	alice.zesoi.fer.hr	*			0 397	RIPE Network Coordination Centre RIPE-ERX
1		161.53.64.1	zesoigwy.zesoi.fer.hr	(Croatia)		36		RIPE Network Coordination Centre RIPE-ERX
2		161.53.16.9	-	(Netherlands)	+01:00	0		RIPE Network Coordination Centre RIPE-ERX
3		193.198.229.9	-	(Croatia)		0		Used to be maintained by HR-ZZ
4		193.198.228.5	-	(Croatia)		0		Used to be maintained by HR-ZZ
5		62.40.103.217	carnet.hr1.hr.geant.net	(United Kingdom)	*	0		IP allocation for GEANT network
6		62.40.96.146	hr.hu1.hu.geant.net	(United Kingdom)	*	8		IP allocation for GEANT network
7		62.40.96.177	hu.at1.at.geant.net	(United Kingdom)	*	15		IP allocation for GEANT network
8		62.40.96.58	at.de2.de.geant.net	(United Kingdom)		27		IP allocation for GEANT network
9		62.40.96.54	de2-2.de1.de.geant.net	(United Kingdom)		27		IP allocation for GEANT network
10		62.40.105.2	cr-frankfurt1-po11-0.g-win.dfn.de	Frankfurt, Germany	+01:00	27		IP allocation for GEANT network
11		188.1.18.190	cr-leipzig1-po6-0.g-win.dfn.de	Leipzig, Germany	+01:00	41		IP networking on DFN's Gigabit-Wissenschaf
12		188.1.18.105	cr-essen1-po1-0.g-win.dfn.de	Essen, Germany	+01:00	44		IP networking on DFN's Gigabit-Wissenschaf
13		188.1.86.6	ar-essen4-ge0-0.g-win.dfn.de	Essen, Germany	+01:00	44		IP networking on DFN's Gigabit-Wissenschaf
14		129.217.129.43	gwin-gw-lo0.HRZ.Uni-Dortmund.DE	Dortmund, Germany	+01:00	44		RIPE Network Coordination Centre RN-ERX-1
15		129.217.129.233	gb5-sw2-vl26.HRZ.Uni-Dortmund.DE	Dortmund, Germany	+01:00	45		RIPE Network Coordination Centre RN-ERX-1
16		129.217.128.2	ftp.uni-dortmund.de	Dortmund, Germany	+01:00	45		RIPE Network Coordination Centre RN-ERX-1

Roundtrip time to ftp.uni-dortmund.de, average = 45ms, min = 45ms, max = 46ms -- 2005.5.9 11:22:57

Slika 2. Rezultati ispitivanja puta paketa do odredišta ftp.uni-dortmund.de dobiveni korištenjem programa VisualRoute

Ovaj program pokazuje i ukupno vrijeme potrebno da paket stigne do odredišta i vrati se natrag. Uočite kako to vrijeme varira. Vidi se da su tipične vrijednosti od nekoliko ms do 100 ms. Pored toga, prikazano je i vrijeme potrebno da paket stigne do svakoga računala na putu do odredišta. To vrijeme varira pa su prikazane minimalna, maksimalna i srednja vrijednost dobivena iz nekoliko pokušaja.

- Možete kliknuti na polja u tablici koja opisuju mrežu i ime čvora (računala). Za neke čvorove tako možete saznati više informacija.

- (Za znatiželjne). Ustanovite koristeći *Ethereal* kako *VisualRoute* saznaje IP adrese računala preko kojih paket putuje. Hint: gledati ‘time-to-live’ polje unutar IP zaglavlja ICMP protokola.

2. Transportni sloj: TCP i UDP - koncept portova

Kako smo već rekli, svako sučelje računala prema mreži ima svoju IP adresu. Korištenjem koncepta portova omogućeno je da se na jednom sučelju može ostvariti više istovremenih veza prema više različitih aplikacija.

Zbog toga je moguće da se na računalu sa jednom IP adresom nalazi više mrežnih servisa (npr. *telnet*, *ftp* i *web* servis) jer svaki takav servis se javlja na drugom portu.

Većini je servisa dogovorom određen port na kojem se nalaze. Uglavnom portovi <1024 su rezervirani tj. već je dogovoreno čemu služe. Niže su navedeni servisi vezani uz prvih 110 portova. Tako se npr. *ftp* nalazi na portu 21, dok se *www* nalazi na portu 80.

Popis servisa i pripadajućih im portova:

```
tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp                          # message send protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
telnet          23/tcp
# 24 - private
smtp            25/tcp          mail
# 26 - unassigned
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp                          # Remote Mail Checking Protocol
domain          53/tcp          nameserver      # name-domain server
domain          53/udp          nameserver
mtp             57/tcp                          # deprecated
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
gopher          70/udp
rje             77/tcp          netrjs
finger          79/tcp
www             80/tcp          http            # WorldWideWeb HTTP
www             80/udp                          # HyperText Transfer Protocol
link            87/tcp          ttylink
kerberos        88/tcp          kerberos5 krb5  # Kerberos v5
kerberos        88/udp          kerberos5 krb5  # Kerberos v5
supdup          95/tcp
# 100 - reserved
hostnames       101/tcp         hostname        # usually from sri-nic
iso-tsap        102/tcp         tsap            # part of ISODE.
csnet-ns        105/tcp         cso-ns          # also used by CSO name server
csnet-ns        105/udp         cso-ns
rtelnet         107/tcp                         # Remote Telnet
rtelnet         107/udp
pop-2           109/tcp         postoffice      # POP version 2
pop-2           109/udp
pop-3           110/tcp                         # POP version 3
pop-3           110/udp
```

- Koji port koristi SMTP (Simple Mail Transport Protocol) protokol za slanje e-maila?

- Korištenjem programa ***Ostro Soft Internet Tools*** (ikona je na desktopu) doznajte koji su portovi "otvoreni" na računalu `diana.zesoi.fer.hr` (opcija `Port Scanner` u izborniku `Tools`).

Ta se operacija u praksi naziva skeniranje portova i nemojte je raditi na nekim drugim računalima van laboratorija osim ovog gore navedenoga. Naime, ovakvo ponašanje na mreži nije "pristojno" jer se može shvatiti kao traženje potencijalnih sigurnosnih rupa na računalu kojem se skeniraju portovi.

Koje TCP ili UDP konekcije vaše računalo očekuje (*listening*) ili je uspostavilo vezu (*established*) možete saznati naredbom (iz komandne linije `cmd`):

```
netstat –a
```

Time je moguće saznati koji portovi na vašem računalu su otvoreni. Inače je potrebno voditi računa da svaki otvoreni port može predstavljati određeni sigurnosni rizik. Naime pošto je aplikacija otvorena za konekcije i očekuje pakete moguće je da joj se «podvale» paketi koji će kompromitirati njeno uobičajeno djelovanje.

2.1. Transport Control Protocol (TCP)

IP koji je implementiran na mrežnom sloju je *bespojnog* (*connectionless*) tipa. Podaci se rastave na pakete koji se zatim šalju prema odredištu međutim IP ne vodi računa o tome da li su ti paketi uopće stigli i kada stignu da li su pravilno poredani onako kako su i poslani.

Za takve stvari se brine TCP sa sloja iznad tj. *prijenosnog sloja*. TCP je *connection-oriented* protokol i osim što uvodi koncept portova, TCP se brine za uspostavljanje i prekidanje veze te potvrđivanje primljenih paketa i njihov pravilan poredak. Veze se uspostavljaju *point-to-point* između dva računala tj. ne podržavaju se *broadcast* veze Ukratko TCP je dizajniran da osigura pouzdanu vezu preko nepouzdane mreže.

Svaka TCP konekcija između dva računala je identificirana parom (izvorišni port, odredišni port). Moguće je imati više veza između dva računala koje imaju isti odredišni port ali će tada svaka od njih imati različiti izvorišni (npr. dva *internet browsera* kontaktiraju isti *web server*).

Sve bitne stvari ovog protokola su vidljive iz zaglavlja paketa. Tamo se nalazi: izvorišni port, odredišni port, sequence broj (*seq*), acknowledgement broj (*ack*) i par zastavica (*flagova*). Od zastavica će nam biti bitne SYN, ACK i FIN. SYN se koristi za uspostavljanje veze. ACK označava da li je *ack* broj valjan (tj. da li se koristi).

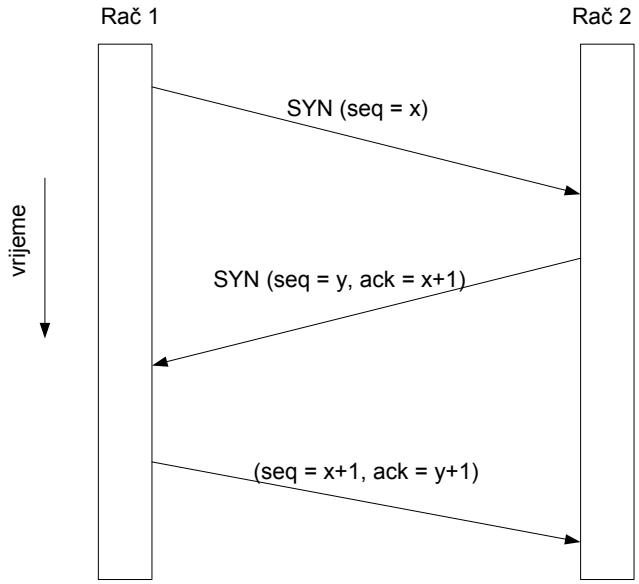
Da bi se osigurao siguran prijenos podataka prvo se mora uspostaviti veza između dva računala. Analogija postoji sa korištenjem telefona (prije početka razgovora mora se uspostaviti veza). Svi paketi koji se šalju sada imaju svoj redni broj (*seq*). Time se zna redoslijed koji ti paketi moraju imati. Isto tako ako stigne dva puta paket sa istim rednim brojem onda se zna da se jedan mora odbaciti. Kod slanja sljedećeg paketa *seq* se uveća za broj byteova prethodno poslanih.

Za svaki poslani paket se traži da se potvrdi njegov primitak. Ako potvrda ne stigne paket se šalje ponovno. Potvrda dolazi u paketu kojem je zastavica ACK=1 a *ack* pokazuje na sljedeći *seq* broj koji se očekuje (time se potvrđuju svi prethodni *seq* brojevi). Nije potrebno da se za svaki primljeni paket šalje posebni paket samo s potvrdom. Moguće je poslati potvrdu da se *šverca* na paketu koji je inače trebao biti poslan na drugu stranu. Dakle računalo kada primi paket ne šalje odmah potvrdu nego čeka neko vrijeme da li će

možda dobiti zahtjev da paket mora poslati na drugu stranu i ako to dobije tada potvrdu prilijepi njemu. To švercanje se zove *piggybacking* i dosta pridonosi efikasnosti.

Uspostava veze.

Prije nego krene razmjena podataka potrebno je uspostaviti vezu. Pri tome se razmijene početne vrijednosti *seq* polja tako da se zna od kuda kreće brojanje paketa. Šalje se SYN=1, ACK=0 te odgovarajući početni *seq* broj. Odgovor stiže u obliku SYN=1, ACK=1, *ack* polje potvrđuje *seq* broj i pri tom se šalje svoj početni *seq* broj čija se potvrda očekuje kao *piggyback* na prvom paketu s podacima.



Raskidanje veze.

Šalje se paket s FIN=1 i znači da nema više podataka za slati. Ako ne stigne odgovor potvrde u određenom roku veza se raskida. Isto to radi i druga stana. Iako je TCP full-duplex prijenos, veza se prekida kao dva simplexa.

Zadatak:

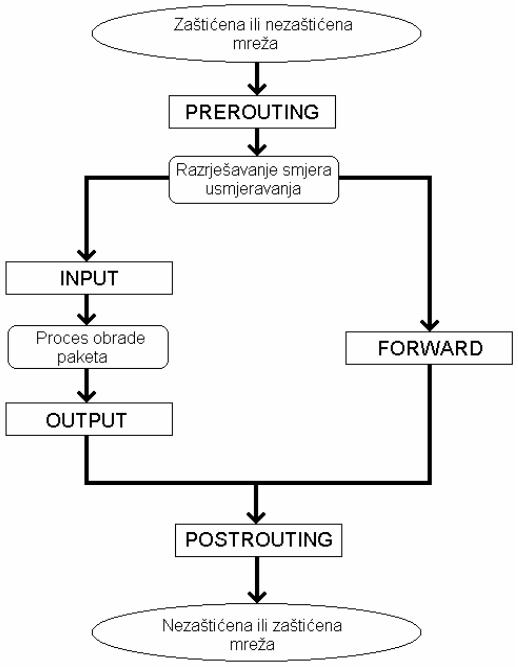
- Na primjeru komuniciranja Internet browsera sa nekim web serverom (npr. www.fer.hr) koristeći alat *Ethereal* uloviti pakete kojima se uspostavlja veza, prenose podaci i prekida veza. Uočiti kako se paketi međusobno potvrđuju. Koji port je Internet browser otvorio da bi primao odgovore od web servera? Koliko je zasebnih konekcija bilo potrebno da se svi podaci (text, slike) prenesu?

3. Filtriranje mrežnog prometa (Firewall)

Cilj ove vježbe je upoznavanje s filtriranjem mrežnog prometa. Filtriranje mrežnog prometa najuobičajenije je na usmjerivačima (engl. *router*) koji se onda zbog takve svoje zaštitne uloge nazivaju vatrozidi (engl. *firewall*). Ipak, vatrozidi se nalaze i na osobnim računalima pri čemu služe najčešće za zaštitu od računalnih virusa i crva, trojanaca i sličnih malicioznih programa. Nažalost filtriranje mrežnog prometa na usmjerivačima nije moguće izvesti u sklopu ovih laboratorijskih vježbi pa je stoga naglasak stavljen na filtriranje prometa na osobnom računalu.

3.1. Faze obrade mrežnih paketa u vatrozidu

Kada mrežni paket dođe na mrežno sučelje vatrozida, on prelazi preko mrežnog sklopovlja na odgovarajući upravljački program u jezgri operacijskog sustava zadužen za obradu paketa. Paket nakon toga prolazi kroz određene faze prije nego bude proslijeđen na drugu mrežu ili na neku višu aplikaciju u vatrozidu. Glavne faze obrade nazivaju se još i karike (engl. *chains*). Na slici 5.1. vidljive su glavne faze unutar vatrozida.



Slika 3.1: Usmjeravanje paketa unutar jezgre operacijskog sustava vatrozida

Ukoliko vatrozid dobije paket koji je namijenjen za sam vatrozid, paket će biti proslijeđen na INPUT (ulaznu) fazu. Tu je moguće definirati pravila u vezi s dolaznim paketom. Neka od tipičnih pravila bila bi da se paket proslijedi na neku drugu, na slici nespomenutu fazu koja je zadužena za obradu i provjeru paketa određenog tipa (npr. UDP ili TCP paketi). Nakon što paket uspješno prođe INPUT fazu paket odlazi na obradu određenom aplikacijskom procesu.

Ukoliko je riječ o slanju paketa od strane vatrozida, generirani paket prvo dolazi na OUTPUT fazu. Tu je moguće obaviti filtriranje paketa, tj. provesti zabranu prolaska neodgovarajućim paketima.

Ako paket treba samo proći s javne na internu, ili s interne na javnu mrežu, onda on mora proći preko FORWARD faze. U FORWARD fazi obavljaju se provjere prema pravilima koje određuju koji paketi smiju prolaziti na koju mrežu. Uobičajeni skup naredbi sadrži zabranu prosljeđivanju paketa s vanjske mreže prema zaštićenoj i dozvolu

prosljeđivanja odgovora s vanjske mreže prema zaštićenoj mreži. Također, često se korisnicima zaštićene mreže u FORWARD fazi zabranjuje pristup određenim ili vanjskim računalima (poslužitelji s Web igrama i sl.) ili određenim nesigurnim uslugama (ftp, tftp, itd...).

Faza PREROUTING omogućava manipulaciju paketima na razini promjene TOS (engl. *Type of Service*) varijabli i sl. Važnija primjena ove faze je DNAT (engl. *Destination Network Address Translation*) transformacija. DNAT transformacija koristi se za promjenu odredišne adrese.

Fazi POSTROUTING glavna je funkcija SNAT (engl. *Source Network Address Translation*) transformacija. SNAT transformacija koristi se za promjenu izvorišne adrese paketa. Umjesto SNAT-a u ovoj fazi moguće je koristiti i proces maskiranja (engl. *Masquerading*) privatnih adresa iz zaštićene mreže. Vatrozid mijenja IP adrese iz zaštićene mreže svojom adresom pridruženom vanjskom mrežnom sučelju i prosljeđuje tako modificirane pakete na vanjsku mrežu. Razlika između SNAT-a i maskiranja je u tome što SNAT zamjenjuje IP adrese s definiranom adresom, a maskiranje zamjenjuje IP adrese s adresom pridruženom određenom mrežnom sučelju. Ukoliko zaštićene mreže koriste privatne IP adrese nužno je koristiti jednu od spomenutih metoda jer se inače paketi nikad ne bi mogli vratiti na odgovarajuće računalo zbog toga što paketi s privatnim IP adresama nisu dozvoljeni na Internetu.

Vježba se izvodi korištenjem *Linux* operacijskog sustava (Knoppix distribucija na Live CD-u)

3.2. Konfiguracija mrežnih postavki računala

Nakon podizanja Linux operacijskog sustava potrebno je unutar grafičkog sučelja startati terminalski prozor (kliknuti na ikonu terminala u donjem toolbaru) u kojem izvršavate sve daljnje naredbe.

- Prva naredba koju je potrebno izvršiti služi za dobivanje administratorskih ovlasti:
  ```
  su
  ```

- Potom je potrebno definirati mrežno sučelje. Izlistavanje mrežnih sučelja postiže se pomoću naredbe:
  ```
  ifconfig
  ```

  Korištenjem iste naredbe potrebno je definirati mrežnu adresu koja je zapisana na stolu pokraj vašeg računala. Npr .173. definira IP adresu 161.53.64.173. U nastavku zadatka umjesto konkretne brojke koristit će se oznaka A: npr. 161.53.64.A. U daljnim naredbama A zamijenite sa vašim konkretnim brojem. Definiranje mrežne IP adrese postiže se sljedećom naredbom:
  ```
  ifconfig eth0 161.53.64.A netmask 255.255.255.0 broadcast 161.53.64.255 up
  ```

- Da bi računalo moglo pristupati Internetu potrebno je definirati izlaz iz mreže (eng. *gateway*). *Gateway* za mrežu 161.53.64.0/255.255.255.0 je IP adresa 161.53.64.1. Postavljanje izlaza obavlja se s naredbom:
  ```
  route add default gw 161.53.64.1 eth0
  ```

- Ispravnost postavljenih naredbi potrebno je testirati otvaranjem određene web stranice. Potrebno je otvoriti web browser iz grafičkog sučelja (kliknuti na ikonu guštera u donjem toolbaru). U njemu otvoriti primjerice http://www.fer.hr/.

- Ukoliko računalo nakon svih ovih unesenih naredbi ne može pristupati određenim web stranicama, potrebno je promijeniti datoteku `/etc/resolv.conf`. U njoj se definiraju IP adrese DNS poslužitelja. Sadržaj te datoteke mora biti jednak sljedećem:

```
search dhcp.zesoi.fer.hr
nameserver 161.53.64.4
nameserver 161.53.64.3
```

- Nakon što su sve naredbe postavljene potrebno je još podignuti HTTP poslužitelj na svom računalu. Isto se postiže upisivanjem naredbe

```
apachectl start
```

Nakon pokretanja Web poslužitelja na računalu vam je otvoren port 80 (HTTP port) i njemu možete pristupati tako da se u web pregledniku upiše http://localhost ili http://161.53.64.A

3.3. Definiranje pravila filtriranja i preusmjeravanja za mrežne pakete

Da bi se na računalu postavile određene naredbe za filtriranje mrežnih paketa potrebno je koristiti *IP Tables* programski alat. S njime se na jednostavan način definiraju pravila koja određene mrežne paket propuštaju, određene preusmjeruju na druga računala, a određene odbijaju i ne propuštaju.

Filtriranje mrežnih paketa odvija se u različitim grupacijama. Dolazni paketi namijenjeni samom računalu pregledavaju se u INPUT fazi, odlazni u OUTPUT, a paketi koji se prosljeđuju na druga računala u FORWARD fazi. Ispis svih naredbi u pojedinim od spomenutih grupacija dobiva se unosom sljedeće naredbe:

```
iptables -L
```

Uz svaku grupu (tzv. lanac ili karika – engl. *chain*) definirana je i globalna politika lanca: ACCEPT, REJECT ili DROP. Globalni ACCEPT označava da se sve prihvaća osim naredbi koje su navedene kao DROP ili REJECT u tom lancu. Globalni DROP ili REJECT označava da se ništa ne prihvaća osim naredbi koje su navedene kao ACCEPT u tom lancu. Na početku vježbe sve globalne politike trebaju biti ACCEPT. Što se postiže sljedećim naredbama:

```
iptables –P INPUT ACCEPT
iptables –P OUTPUT ACCEPT
iptables –P FORWARD ACCEPT
```

Osim što se s IP Tables-om mogu filtrirati mrežni paketi, oni se mogu i preusmjeravati. To se postiže u POSTROUTING i PREROUTING fazama. PREROUTING faza namijenjena je promijeni odredišnih postavki (odredišna IP adresa i port) dok je POSTROUTING faza namijenjena promijeni izvorišnih postavki (izvorišna IP adresa i port). Ispis svih naredbi u pojedinim od spomenutih faza dobiva se unosom sljedeće naredbe:

```
iptables –t nat -L
```

Globalne politike ovih lanaca postavljaju se sljedećim naredbama:

```
iptables –t nat –P PREROUTING ACCEPT
iptables –t nat –P POSTROUTING ACCEPT
```

3.4. Filtriranje dolaznih mrežnih paketa

Pravila koja služe za definiranje prihvaćanja tj. odbacivanja mrežnih paketa namijenjenih vašem računalu definiraju se u INPUT fazi. Prvi zadatak vezan uz filtriranje dolaznih paketa je omogućavanje, tj. onemogućavanje pristupa podignutom lokalnom HTTP poslužitelju. Vježba se obavlja samostalno te u kombinaciji s drugim računalom.

Između svake naredbe potrebno je unijeti sljedeću naredbu da se ukloni efekt svih prethodnih naredbi:

```
iptables -F INPUT
```

- Prva naredba koju je potrebno definirati zabranjuje pristup lokalnom HTTP poslužitelju. Prije unosa naredbe za onemogućavanje pristupa HTTP servisu prisutnom na portu 80, potrebno je provjeriti da li je isti podignut otvaranjem stranice http://localhost sa lokalnog računala te http://161.53.64.A sa susjednog računala. Naredba koju je potom potrebno upisati je sljedeća:

```
iptables -A INPUT -p TCP -i eth0 --destination-port 80 -j
DROP
```

- Navedena naredba unosi (–A : *append*) se na kraj INPUT lanca te definira da se sav TCP promet (-p TCP) usmjeren na mrežno sučelje eth0 (-i eth0) i na odredišni port 80 (–destination-port 80) odbaci. Nakon unošenja spomenute naredbe s drugog računala provjerite da li se može pristupiti vašem HTTP poslužitelju. Isti efekt ostvario bi se i sa sljedećom naredbom koju trebate unijeti nakon što ispraznite sadržaj INPUT lanca:

```
iptables -A INPUT -p TCP -d 161.53.64.A --destination-port 80
-j DROP
```

- Testirajte i prethodnu naredbu, ali prije nje ispraznite sadržaj INPUT lanca sa već navedenom naredbom:

```
iptables -F
```

- Druga funkcionalnost koju je potrebno testirati je zabrana ICMP protokola tj. *ping*-anja. Nakon što je ispražnjen INPUT lanac potrebno je prvo testirati sa susjednog računala da li se može računalo *ping*-ati. Nakon toga potrebno je unijeti novu naredbu koja zabranjuje ping na lokalno računalo:

```
iptables -A INPUT -p ICMP -d 161.53.64.A -j DROP
```

Testiranje navedene naredbe provedite sa susjednog računala korištenjem naredbe `ping`:

```
ping 161.53.64.A
```

Na kraju je potrebno isprazniti INPUT lanac. Navedeni način filtriranja primjenjuje se kad administrator računala želi zabraniti udaljenim korisnicima pristup određenim resursima lokalnog računala. Takav sustav naredbi naziva se *Black list*. Ukoliko bi sve bilo zabranjeno (globalna politika je DROP), osim definiranih naredbi, to bi bio slučaj *White list* sustava naredbi.

3.5. Filtriranje odlaznih mrežnih paketa

Pravila koja služe za definiranje prihvaćanja tj. odbacivanja mrežnih paketa generiranih od strane vašeg računala definiraju se u OUTPUT fazi. Prvi zadatak vezan uz filtriranje odlaznih paketa je omogućavanje, tj. onemogućavanje pristupa udaljenom HTTP http://www.google.com poslužitelju. Vježba se obavlja samostalno.

- Prva naredba koju je potrebno definirati zabranjuje pristup udaljenom HTTP poslužitelju. Prije unosa naredbe, potrebno je provjeriti da li je isti podignut otvaranjem stranice http://www.fer.hr. Naredba koju je potom potrebno upisati je sljedeća:

```
iptables –A OUTPUT –p TCP –d 161.53.72.111 --destination-port
80 –j DROP
```

Uspješnost navedene naredbe možete provjeriti otvaranjem FER-ove stranice. Također, provjerite da li možete `ping`-ati navedenu adresu.

- Sljedeću naredbu za onemogućavanje slanja *ICMP* zahtjeva unesite bez da ste ispraznili OUTPUT lanac. Na taj način će istodobno biti zabranjeno pristupanje FER-ovoj glavnoj web stranici te ping-anje samog računala:

```
iptables –A OUTPUT –p ICMP –d 161.53.72.111 –j DROP
```

Testiranje navedene naredbe provedite s lokalnog računala korištenjem naredbe ping:

```
ping 161.53.72.111
```

Izlistajte naredbe kako biste vidjeli način zapisa iptables naredbi u OUTPUT karici te potom uklonite sadržaj OUTPUT lanca:

```
iptables –L
iptables –F OUTPUT
```

- Zadnja naredba obuhvaća prve dvije, ali i više jer zabranjuje sav promet prema definiranoj IP adresi:

```
iptables –A OUTPUT –p ALL –d 161.53.72.111 –j DROP
```

Na kraju je potrebno isprazniti OUTPUT lanac. Navedeni način filtriranja primjenjuje se kad administrator računala želi zabraniti lokalnim korisnicima pristup određenim resursima, IP adresama i slično (engl. *Black list*).

3.6. Preusmjeravanje dolaznih mrežnih paketa

Pravila koja služe za preusmjeravanje mrežnih paketa generiranih od strane računala definiraju se u PREROUTING fazi. Prvi zadatak vezan uz preusmjeravanje mrežnih paketa odnosi se na preusmjeravanje ICMP dolaznih paketa na drugo računalo. Vježba se obavlja u kombinaciji sa susjednim računalom s kojeg se obavlja testiranje.

- Prvi preduvjet koji je potreban da bi se paket mogao preusmjeravati na neko drugo računalo je uključeno prosljeđivanje (*ip_forward*). Stoga je potrebno unijeti sljedeću naredbu:

```
echo “1” > /proc/sys/net/ipv4/ip_forward
```

- Drugi preduvjet koji je potreban da bi se paket mogao preusmjeravati na neko drugo računalo su naredbe u FORWARD lancu koje to dozvoljavaju. Za svaku naredbu redirekcije potrebno je unijeti pripadnu naredbu u FORWARD fazi koja će to preusmjeravanje ACCEPT-ati. Ipak, jednostavnije je prvo odrediti da je globalna politika FORWARD faze ACCEPT sljedećom naredbom:

```
iptables –P FORWARD ACCEPT
```

- Prva naredba služi za preusmjeravanje *ICMP* zahtjeva koji će se preusmjeravati na FER-ov web poslužitelj:

```
iptables –t nat –A PREROUTING –p ICMP –d 161.53.64.A –j DNAT
--to-destination 161.53.72.111
```

Testiranje navedene naredbe provedite sa susjednog računala korištenjem naredbe ping.:

```
ping 161.53.64.A
```

Koje računalo vam vraća poslane pakete?

Preusmjeravanje mrežnih paketa koristi se najčešće ukoliko je poslužitelj skriven. U tom slučaju adresirano računalo (najčešće vatrozid ili usmjerivač) prima pripadne mrežne pakete i prosljeđuje ih na skriveni poslužitelj.

4. Aplikacijski sloj

4.1. DNS – Domain Name System

Glavni zavodski DNS server je na adresi 161.53.64.4 imenom branka.zesoi.fer.hr. DNS server je zadužen za mapiranje simboličkih imena računala u njihove IP adrese. Upite lokalnom DNS serveru zadajemo naredbom `nslookup` iz komandne linije. Npr:

```
nslookup diana.zesoi.fer.hr

nslookup www.google.com
```

4.2. HTTP (Hyper Text Transport Protocol)

Što je sve potrebno za "surfanje" po webu? Na vašoj strani potreban je klijentski program. On će upite sa traženim www stranicama znati poslati HTTP protokolom web serveru koji te stranice ima. Ako mu ne naglasite posebno, vaš će klijent pretpostaviti da mora pristupiti portu 80 jer se baš na tom portu po dogovoru "priča" HTTP protokolom.

Da bi mogao primiti podatke koje mu web server pošalje, web klijent sa svoje strane otvara jedan slobodni port rednog broja > 1024 (jer su brojevi < 1024 rezervirani). Na serveru kojem pristupate mora biti aktivan *www servis* proces koji cijelo vrijeme osluškuje port 80 i odgovara na zahtjeve koji na njega pristignu. Isti je princip rada i ostalih mrežnih servisa: ftp, telnet …

Zanima li vas što vaš web browser uistinu prima kada želite pogledati neku web stranicu? Dovoljno je znati da se web server nalazi na portu 80 i da je adresa stranice `spvp.zesoi.fer.hr`.

Ovaj zadatak napravite korištenjem *telnet* klijenta. Pomoću *telnet* klijenta uspostavljamo TCP vezu sa odgovarajućim portom na udaljenom računalu a dalje ručno tipkanjem simuliramo protokol.

```
[22:16] ~% telnet spvp.zesoi.fer.hr 80      (80 je port na koji se spajamo)
Trying 161.53.64.3...
Connected to maja.zesoi.fer.hr.             (zapravo smo se spojili na maju, spvp je alias)
Escape character is '^]'.
GET / HTTP/1.1                              (default put, koristi se http protokol verzija 1.1)
HOST: spvp.zesoi.fer.hr                     (na kraju pritisnuti enter tipku)
                                            (i još jednom pritisnuti enter tipku)
```

Kao izlaz dobit ćemo čisti HTML kod stranice.

Ako nas zanima samo HTTP zaglavlje dokumenta onda umjesto naredbe GET treba staviti HEAD. To je korisno kod velikih dokumenata da možemo saznati neke osnovne informacije (npr. kad je file zadnji puta mijenjan) bez da download-amo cijeli dokument.

- Probajte se ponovo spojiti na port 80 i unijeti neku naredbu koja ne postoji.

Dobit ćete poruku o grešci, no primjetite da je i ona u HTML formatu.

```
[22:16] ~% telnet diana.zesoi.fer.hr 80
Trying 161.53.64.3...
Connected to maja.zesoi.fer.hr.
Escape character is '^]'.
bezveze
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method Not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
bezveze to /index.html not supported.<P>
Invalid method in request bezveze<P>
<HR>
<ADDRESS>Apache/1.3.6 Server at maja.zesoi.fer.hr Port 80</ADDRESS>
</BODY></HTML>
```

4.3. Za Kraj

Jedan od jednostavnijih protokola koristi *qotd* servis. Qotd dolazi of «Quote of the Day». Odnosi se na skup izreka (ne)poznatih osoba koje su obično poučne ili duhovite.

Kada se uspostavi TCP veza na port 17 *qotd* servis vam vrati «quote of the day» u tekstualnom obliku i zatvori vezu. Probajte (koliko god puta želite):

```
telnet sandra.zesoi.fer.hr 17
```

Nažalost malo računala poslužuje *quotove* drugima tj. ima taj port 17 otvoren.