Sveučilište u Zagrebu
PMF – Matematički odjel

Mreže računala

Vježbe 02

Matko Botinčan
Zvonimir Bujanović
Igor Jelaska
Maja Karaga

Osnovni mrežni alati

- ifconfig (ipconfig pod Windows-ima)
- ping
- traceroute (tracert pod Windows-ima)
- nslookup
- netstat

Nešto složeniji alati:

- nmap
- tcpdump (windump pod Windows-ima)

Osnovni mrežni alati

- iz sigurnosnih razloga većina ovih alata nije dostupna iz praktikuma (rade ifconfig, nslookup, netstat; za tcpdump trebaju administratorske ovlasti)
- ping i traceroute su dostupni sa računala student.math.hr
  - `$ ssh student`
  - `$ /etc/ping` (pokretanje pinga)
- nmap (http://insecure.org/nmap) možete sami instalirati na neko računalo sa Linux-om ili Windows-ima
- windump (http://www.winpcap.org/windump) možete sami instalirati na neko računalo sa Windows-ima

ifconfig / ipconfig

- osnovni podaci o mrežnim adapterima u računalu

```
bash $ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:93:EE:3E
          inet addr:192.168.255.128  Bcast:192.168.255.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe93:ee3e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2992 (2.9 KiB)  TX bytes:5598 (5.4 KiB)
          Interrupt:16 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:100 (100.0 b)  TX bytes:100 (100.0 b)
```

ping

- je li udaljeno računalo dostupno? Koliko je ukupno vrijeme od slanja upita do primanja odgovora (*round-trip time*)?
- šalje ICMP echo poruke udaljenom računalu i očekuje ICMP poruku echo-reply

```
[student]/math/zbujanov $ /etc/ping www.google.com
PING www.l.google.com: 64 byte packets
64 bytes from 209.85.129.147: icmp_seq=0. time=26. ms
64 bytes from 209.85.129.147: icmp_seq=1. time=26. ms
64 bytes from 209.85.129.147: icmp_seq=2. time=26. ms
64 bytes from 209.85.129.147: icmp_seq=3. time=26. ms
64 bytes from 209.85.129.147: icmp_seq=4. time=26. ms

----www.l.google.com PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 26/26/26
```


traceroute / tracert

- kojim putem putuje paket do udaljenog računala?
- šalje niz poruka (obično UDP, negdje se može i konfigurirati na ICMP ili TCP) udaljenom host-u postavljajući TTL (*time-to-live*) parametar redom na 1, 2, 3, ...
- svaki router na putu smanjuje TTL za 1; ako je TTL jednak 1, router odbacuje paket i vraća pošiljatelju ICMP poruku *time-exceeded*
- služi za detektiranje mrežih problema: gdje se gube paketi, gdje postoji vatrozid (*firewall*), da li dio mreže funkcionira itd.

traceroute / tracert

```
C:\>tracert www.ubuntu.com

Tracing route to www.ubuntu.com [91.189.94.158]
over a maximum of 30 hops:

  1    5 ms    74 ms    94 ms  dsldevice.lan [192.168.1.254]
  2   11 ms    11 ms    10 ms  zagreb5-ge-0-1.amis.net [194.146.109.23]
  3    *        9 ms    10 ms  zagreb2-ge-0-0-0-1.amis.net [194.146.109.1]
  4   50 ms   103 ms    14 ms  maribor2-so-0-2-0-0.amis.net [212.18.35.145]
  5   16 ms    16 ms    19 ms  80.120.176.181
  6   71 ms    17 ms    17 ms  195.3.70.69
  7   18 ms    17 ms    17 ms  195.3.70.82
  8   31 ms    17 ms    13 ms  212.73.202.1
  9   29 ms    36 ms    33 ms  ae-31-53.ebr1.Frankfurt1.Level3.net [4.68.118.94]
 10   30 ms    30 ms    34 ms  ae-1-100.ebr2.Frankfurt1.Level3.net [4.69.132.126]
 11   35 ms    37 ms    34 ms  ae-2.ebr1.Dusseldorf1.Level3.net [4.69.132.137]
 12   15 ms     9 ms    35 ms  ae-1-100.ebr2.Dusseldorf1.Level3.net [4.69.132.130]
 13   40 ms    37 ms    25 ms  ae-2.ebr1.Amsterdam1.Level3.net [4.69.133.89]
 14   40 ms    36 ms    10 ms  ae-1-100.ebr2.Amsterdam1.Level3.net [4.69.133.86]
 15   44 ms    11 ms    54 ms  ae-2.ebr2.London1.Level3.net [4.69.132.133]
 16   29 ms    54 ms    43 ms  ae-1-100.ebr1.London1.Level3.net [4.69.132.117]
 17   54 ms    43 ms    52 ms  ae-2.ebr2.London2.Level3.net [4.69.132.145]
 18   38 ms    37 ms    45 ms  ae-26-52.car2.London2.Level3.net [4.68.117.48]
 19   26 ms    45 ms    44 ms  195.50.121.2
 20   48 ms    12 ms    45 ms  gw0-0-gr.canonical.com [91.189.88.10]
 21   43 ms    49 ms    19 ms  arctowski.canonical.com [91.189.94.158]

Trace complete.
```

- opcije: `man traceroute` ili `tracert /?`

nslookup

- koja je IP-adresa ako je poznato simboličko ime?
- lagana provjera je li dobro konfiguriran DNS-server

```
bash $ nslookup gmail.google.com
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
gmail.google.com        canonical name = gmail.l.google.com.
Name:   gmail.l.google.com
Address: 209.85.137.107
```

netstat

- pregled prometa koji se trenutno odvija na lokalnom host-u
- možemo doznati:
  - tip protokola (TCP/UDP)
  - lokalnu i udaljenu adresu
  - port koji se koristi
  - stanje TCP veze (CLOSE_WAIT, CLOSED, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, LAST_ACK, LISTEN, SYN_RECEIVED, SYN_SEND, TIME_WAIT)
- dodatne opcije: `man netstat` ili `netstat /?`

netstat

```
janus@Gigabob:~$ netstat -atu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:printer               *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:auth                  *:*                     LISTEN
tcp        0      0 localhost.localdoma:ipp *:*                     LISTEN
tcp        0      0 localhost.localdom:smtp *:*                     LISTEN
tcp        0      0 Gigabob.local:47131     192.168.1.:microsoft-ds ESTABLISHED
tcp        0      0 Gigabob.local:45070     zelazny.freenode.n:ircd ESTABLISHED
tcp        0      0 Gigabob.local:45121     blah.jabber:xmpp-client ESTABLISHED
tcp        0      0 Gigabob.local:49453     mg-in-f125.:xmpp-client ESTABLISHED
tcp        0      1 Gigabob.local:50267     ip565221f6.speed.pl:592 SYN_SENT
tcp        0      0 localhost.localdo:36455 localhost.locald:sunrpc TIME_WAIT
tcp6       0      0 *:52                    *:*                     LISTEN
tcp6       0      0 *:ssh                   *:*                     LISTEN
udp        0      0 *:32768                 *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:sunrpc                *:*
udp        0      0 *:ipp                   *:*
janus@Gigabob:~$
```


nmap

- besplatan mrežni alat za:
  - skeniranje otvorenih portova na računalu
  - detekcija operativnog sustava udaljenog računala
- većina računala na internetu blokira (filtrira) portove i onemogućuje koritenje ovakvih alata koji mogu poslužiti za detektiranje slabosti

nmap

- primjenjen na lokalno računalo:

```
nmap 127.0.0.1

Starting Nmap 4.20 ( http://insecure.org ) at 2007-09-26 03:14 CEST
Interesting ports on localhost.localdomain (127.0.0.1):
Not shown: 1693 closed ports
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6000/tcp open  X11

Nmap finished: 1 IP address (1 host up) scanned in 0.148 seconds
```

- daje popis otvorenih portova – npr. na lokalnom računalu je pokrenut web-server (port 80), pa neko udaljeno računalo može npr. pomoću firefox-a pristupiti našem

nmap

- primjenjen na udaljeno računalo:

```
nmap ftp.carnet.hr

Starting Nmap 4.20 ( http://insecure.org ) at 2007-09-26 03:15 CEST
Interesting ports on ftp.CARNet.hr (161.53.160.21):
Not shown: 1683 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
80/tcp   open     http
135/tcp  filtered msrpc
136/tcp  filtered profile
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn
411/tcp  filtered rmt
445/tcp  filtered microsoft-ds
4444/tcp filtered krb524
6881/tcp filtered bittorent-tracker
7937/tcp open     nsrexecd
7938/tcp open     lgtomapper
8080/tcp filtered http-proxy

Nmap finished: 1 IP address (1 host up) scanned in 7.450 seconds
```

  - otvoreni su portovi 21 i 80, odnosno ftp i web-serveri, pa tom računalu možemo pristupiti pomoću odgovarajućih klijenata

nmap

- detekcija operacijskog sustava na udaljenom računalu

```
nmap -O www.monitor.hr

Starting Nmap 4.20 ( http://insecure.org ) at 2007-09-26 03:21 CEST
Interesting ports on 228.120.232.72.static.reverse.ltdomains.com (72.232.120.228):
Not shown: 1655 filtered ports, 30 closed ports
Device type: firewall|broadband router
Running (JUST GUESSING) : IPCop Linux 2.4.X (87%), Linksys embedded (85%)
Aggressive OS guesses: Ipcop V1.4.11 firewall (Linux 2.4.31) (87%), Linksys WRT54GS v4
running OpenWrt w/Linux kernel 2.4.30 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at
http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 45.705 seconds
```


tcpdump / windump

- prati cjelokupni promet, sve pakete u kojima sudjeluje lokalno računalo
- zbog velikog broja paketa, ima puno opcija za filtriranje

- detalji:
  - man tcpdump (Linux)
  - http://www.winpcap.org/windump/docs/manual.htm (Windows)

tcpdump / windump

```
C:\>windump
windump: listening on \Device\NPF_{64EA27B0-80FD-4D48-A19A-282031D4D04A}
21:20:44.086131 IP mu-in-f147.google.com.80 > ZvoneLaptop.lan.6668: F 1330584419:1330584419(0) ack 1554491093 win 8190
21:20:44.086269 IP ZvoneLaptop.lan.6668 > mu-in-f147.google.com.80: . ack 1 win 65206
21:20:44.215496 IP ZvoneLaptop.lan.1068 > dsldevice.lan.53:  54727+ PTR? 147.135.85.209.in-addr.arpa. (45)
21:20:44.220922 IP dsldevice.lan.53 > ZvoneLaptop.lan.1068:  54727 1/4/4 (216)
21:20:44.496571 arp who-has Skola.lan tell dsldevice.lan
21:20:44.496852 arp who-has ubuntu.lan tell dsldevice.lan
21:20:44.497042 arp who-has tomi.lan tell dsldevice.lan
21:20:44.497285 arp who-has Zvone.lan tell dsldevice.lan
21:20:44.497647 arp who-has ZvoneLaptop.lan tell dsldevice.lan
21:20:44.497661 arp reply ZvoneLaptop.lan is-at 00:90:f5:50:31:17 (oui Unknown)
21:20:44.524960 IP ZvoneLaptop.lan.1068 > dsldevice.lan.53:  63705+ PTR? 4.1.168.192.in-addr.arpa. (42)
21:20:44.525167 IP dsldevice.lan.53 > ZvoneLaptop.lan.1068:  63705* 1/0/0 PTR[|domain]
21:20:44.525702 IP ZvoneLaptop.lan.1068 > dsldevice.lan.53:  33499+ PTR? 241.4.254.169.in-addr.arpa. (44)
21:20:44.525973 IP dsldevice.lan.53 > ZvoneLaptop.lan.1068:  33499* 1/0/0 (68)
21:20:44.526474 IP ZvoneLaptop.lan.1068 > dsldevice.lan.53:  43997+ PTR? 2.1.168.192.in-addr.arpa. (42)
21:20:44.526922 IP dsldevice.lan.53 > ZvoneLaptop.lan.1068:  43997* 1/0/0 PTR[|domain]
21:20:44.527420 IP ZvoneLaptop.lan.1068 > dsldevice.lan.53:  29660+ PTR? 3.1.168.192.in-addr.arpa. (42)
21:20:44.527814 IP dsldevice.lan.53 > ZvoneLaptop.lan.1068:  29660* 1/0/0 PTR[|domain]
21:20:44.725279 IP ZvoneLaptop.lan.1068 > dsldevice.lan.53:  31455+ A? www.index.hr. (30)
21:20:44.739684 IP dsldevice.lan.53 > ZvoneLaptop.lan.1068:  31455 1/2/2 A www.index.hr (124)
21:20:44.756640 IP ZvoneLaptop.lan.6681 > www.index.hr.80: S 1319945961:1319945961(0) win 65535 <mss 1460,nop,nop,sackOK
>
21:20:44.764874 IP www.index.hr.80 > ZvoneLaptop.lan.6681: S 1498644170:1498644170(0) ack 1319945962 win 16384 <mss 1412
,nop,nop,sackOK>
21:20:44.765013 IP ZvoneLaptop.lan.6681 > www.index.hr.80: . ack 1 win 65535
21:20:44.765231 IP ZvoneLaptop.lan.6681 > www.index.hr.80: P 1:607(606) ack 1 win 65535
21:20:44.776343 IP www.index.hr.80 > ZvoneLaptop.lan.6681: . 1:1413(1412) ack 607 win 64929
21:20:44.781743 IP www.index.hr.80 > ZvoneLaptop.lan.6681: . 1413:2825(1412) ack 607 win 64929
21:20:44.781809 IP ZvoneLaptop.lan.6681 > www.index.hr.80: . ack 2825 win 65535
21:20:44.794082 IP www.index.hr.80 > ZvoneLaptop.lan.6681: . 2825:4237(1412) ack 607 win 64929
21:20:44.795262 IP www.index.hr.80 > ZvoneLaptop.lan.6681: . 4237:5649(1412) ack 607 win 64929
```

Zadaci

1. Otkrijte putanje paketa do računala www.iskon.hr, www.google.com, www.irb.hr. Što zaključujete?
2. Pomoću programa ping provjerite da li je računalo www.fer.hr dostupno.
3. Koristeći ICMP ECHO pakete i detaljni ispis odredite putanje do racunala www.dtu.dk
4. Otkrijte putanju paketa do računala student.math.hr
5. Pomoću programa ping na temelju 20 paketa saznajte srednje round-trip vrijeme do računala www.skype.com, uključite opširni prikaz.
6. Pomoću netstat alata utvrdite koji su portovi otvoreni za dolazne konekcije na lokalnom računalu.
7. Utvrdite koje su mrežne konekcije trenutno aktivne i prema kojim računalima na Internetu.