

Hálózatok építése és üzemeltetése

Szoftver szerszámok

Hálózati kommunikáció

► Layer 1-2-3



Hálózati interfész
neve: eth0, wlan1, ...

MAC cím
IP cím



Switch/kapcsoló
(a helyi hálózaton)

A továbbítás alapja:
MAC cím



Router/forgalomirányító
gateway

A továbbítás alapja:
IP cím

Hálózat megfigyelésére használható, egyszerű diagnosztikai eszközök

ping, traceroute, netstat,
tcpdump, wireshark

Ping

```
File Edit Options Buffers Tools Contents Man Help
PING(8) System Manager's Manual: iputils PING(8)
NAME
ping, ping6 - send ICMP ECHO_REQUEST to network hosts
SYNOPSIS
ping [-aAbBdDfhLnOqrRUvV] [-c count] [-F flowlabel] [-i interval] [-I interface]
[-l preload] [-m mark] [-M pmto[disc_option] [-N nodeinfo_option] [-w deadline]
[-W timeout] [-p pattern] [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T
timestamp_option] [hop ...] destination
DESCRIPTION
ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP
ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams ('pings') have
an IP and ICMP header, followed by a struct timeval and then an arbitrary number
of 'pad' bytes used to fill out the packet.
ping6 is IPv6 version of ping, and can also send Node Information Queries
(RFC4620). Intermediate hops may not be allowed, because IPv6 source routing
was deprecated (RFC5095).
OPTIONS
-a Audible ping.
-A Adaptive ping. Interpacket interval adapts to round-trip time, so that
effectively not more than one (or more, if preload is set) unanswered
probe is present in the network. Minimal interval is 200msec for not
super-user. On networks with low rtt this mode is essentially equivalent
to flood mode.
-b Allow pinging a broadcast address.
-B Do not allow ping to change source address of probes. The address is
bound to one selected when ping starts.
-c count
Stop after sending count ECHO_REQUEST packets. With deadline option, ping
waits for count ECHO_REPLY packets, until the timeout expires.
-d Set the SO_DEBUG option on the socket being used. Essentially, this
socket option is not used by Linux kernel.
-D Print timestamp (unix time + microseconds as in gettimeofday) before each
line.
-f Flood ping. For every ECHO_REQUEST sent a period '.' is printed, while
for ever ECHO_REPLY received a backspace is printed. This provides a
2:%%- *Man ping* {PING(8) page 1 of 1} Top L1 (Man) [100.0%]
```

```
nemethf@hsn: ~
nemethf@hsn:~$ ping www.bme.hu
PING inspiro.eik.bme.hu (152.66.115.203) 56(84) bytes of data.
64 bytes from inspiro.eik.bme.hu (152.66.115.203): icmp_seq=1 ttl=60 time=0.535 ms
64 bytes from inspiro.eik.bme.hu (152.66.115.203): icmp_seq=2 ttl=60 time=0.581 ms
64 bytes from inspiro.eik.bme.hu (152.66.115.203): icmp_seq=3 ttl=60 time=0.583 ms
64 bytes from inspiro.eik.bme.hu (152.66.115.203): icmp_seq=4 ttl=60 time=0.426 ms
^C
--- inspiro.eik.bme.hu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.426/0.531/0.583/0.065 ms
nemethf@hsn:~$
```

- ICMP echo request csomagokat küld a hálózatba
- körülfordulási idő mérésére, kapcsolat tesztelésére használják
- Google helyett a program használatát a 'man page'-ben érdemes megnézni

Traceroute – csomagútvonal felderítése

- ▶ Egyre nagyobb Time-To-Live értékkel küld IP csomagokat a célcímre.
- ▶ A routerek csomagtovábbításkor csökkentik a TTL értéket.
- ▶ Ha lejár a TTL, a router *általában* ICMP TIME_EXCEEDED csomagot küld a feladónak.
- ▶ (előfordulhat, hogy a hálózat más útvonalon továbbítja a felderítő csomagokat)

```
nemethf@hsn:~$ traceroute www.google.com
traceroute to www.google.com (216.58.214.36), 30 hops max, 60 byte packets
 1  244gw.tmit.bme.hu (152.66.244.254)  0.289 ms  0.308 ms  0.302 ms
 2  v1121.ixon.net.bme.hu (152.66.245.254)  0.992 ms  1.104 ms  1.272 ms
 3  xge4-2.styx.net.bme.hu (152.66.0.72)  0.879 ms  1.086 ms  1.254 ms
 4  xge2-2.taz.net.bme.hu (152.66.0.78)  0.943 ms  1.056 ms  1.058 ms
 5  tg0-1-0-1.rtr.bme.hbone.hu (152.66.0.126)  2.093 ms  2.091 ms  2.085 ms
 6  tg0-0-0-6.rtr1.vh.hbone.hu (195.111.100.43)  2.598 ms  2.097 ms  1.296 ms
 7  hungarnet-ias-geant-gw.bud.hu.geant.net (83.97.88.81)  1.010 ms  1.010 ms  1.002 ms
 8  google.mx1.fra.de.geant.net (62.40.125.201)  14.379 ms  14.039 ms  14.030 ms
 9  google-gw.mx1.fra.de.geant.net (62.40.125.202)  14.014 ms  14.013 ms  14.008 ms
10  209.85.243.17 (209.85.243.17)  14.942 ms  14.756 ms  209.85.244.5 (209.85.244.5)  16.202 ms
11  209.85.240.185 (209.85.240.185)  14.532 ms  209.85.240.187 (209.85.240.187)  15.774 ms  15.768 ms
12  fra15s09-in-f4.1e100.net (216.58.214.36)  15.729 ms  15.726 ms  15.721 ms
nemethf@hsn:~$
```

Traceroute – csomagútvonal felderítése 2.

- ▶ előfordulhat, hogy a hálózat más útvonalon továbbítja a felderítő csomagokat

```
7  tg0-0-0-1,rtr1.vh.hbone.hu (195.111.102.8) 1,261 ms 1,286 ms 1,353 ms
8  hungarnet-ias-geant-gw.bud.hu.geant.net (83.97.88.81) 0,924 ms 0,892 ms 1,079 ms
9  vie-ix.geant.net (193.203.0.172) 5,018 ms 5,023 ms 9,302 ms
10 ae22.pr01.vie1.tfbnw.net (103.4.98.176) 5,477 ms 9,147 ms 9,148 ms
11 po101.psw03.vie1.tfbnw.net (204.15.22.41) 9,204 ms po101.psw01.vie1.tfbnw.net (204.15.22.37) 9,185 ms po101.psw03.vie1.tfbnw.net (204.15.22.41) 9,061 ms
12 173.252.67.1 (173.252.67.1) 9,025 ms 173.252.67.55 (173.252.67.55) 4,731 ms 4,742 ms
13 edge-star-mini-shv-01-vie1.facebook.com (31.13.84.36) 9,137 ms 9,207 ms 9,127 ms
```

- ▶ Van, amikor egy router nem válaszol (időben)

```
1 244gw.tmit.bme.hu (152.66.244.254) 0,227 ms 0,222 ms 0,215 ms
2 vl121.ixion.net.bme.hu (152.66.245.254) 0,780 ms 0,916 ms 1,261 ms
3 xge4-2.styx.net.bme.hu (152.66.0.72) 0,766 ms 0,940 ms 1,029 ms
4 * * *
5 tg0-1-0-1,rtr.bme.hbone.hu (152.66.0.126) 1,480 ms 1,478 ms 1,618 ms
6 tg0-1-0-2,rtr.sztaki.hbone.hu (195.111.96.227) 2,249 ms 1,597 ms 1,584 ms
7 tg0-0-0-1,rtr1.vh.hbone.hu (195.111.102.8) 2,599 ms 1,264 ms 1,238 ms
8 niif-privat-peering.datanet.hu (194.149.11.41) 2,445 ms 2,437 ms 2,568 ms
9 * * *
10 * * *
11 index.hu (217.20.130.99) 1,834 ms 1,829 ms 1,891 ms
```

NETSTAT – hálózati kapcsolatok listázása

▶ Kapcsolat állapota

▶ Socket

- ▶ tcp, udp, unix
- ▶ LISTEN, CONNECTED, ...

▶ Továbbá:

- ▶ routing táblák,
- ▶ interfész statisztikák,
- ▶ multicastcsoport-tagság

```
nemethf@hsn:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 hsn.tmit.bme.hu:imap  betli.tmit.bme.hu:48719 ESTABLISHED
tcp    0      1 inflab.tmit.bme.hu:ssh 221.229.172.66:38771  FIN_WAIT1
tcp    0      0 hsn.tmit.bme.hu:git    113.247.97.118:5549   ESTABLISHED
tcp    0      240 hsn.tmit.bme.hu:ssh    betli.tmit.bme.hu:48422 ESTABLISHED
tcp6   1      0 localhost:56995        localhost:ipp          CLOSE_WAIT

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State      I-Node   Path
unix   2      [ ]     DGRAM     7953       /run/systemd/notify
unix   2      [ ]     DGRAM     7969       /run/systemd/shutdown
unix  17      [ ]     DGRAM     7974       /run/systemd/journal/dev-log
unix   7      [ ]     DGRAM     7983       /run/systemd/journal/socket
```

Netstat –aputne

- ▶ kapcsolódó program beazonosítható PID alapján
- ▶ A netstat helyet használható a modernebb “**ss**” socket statistics program az iproute2 csomagból

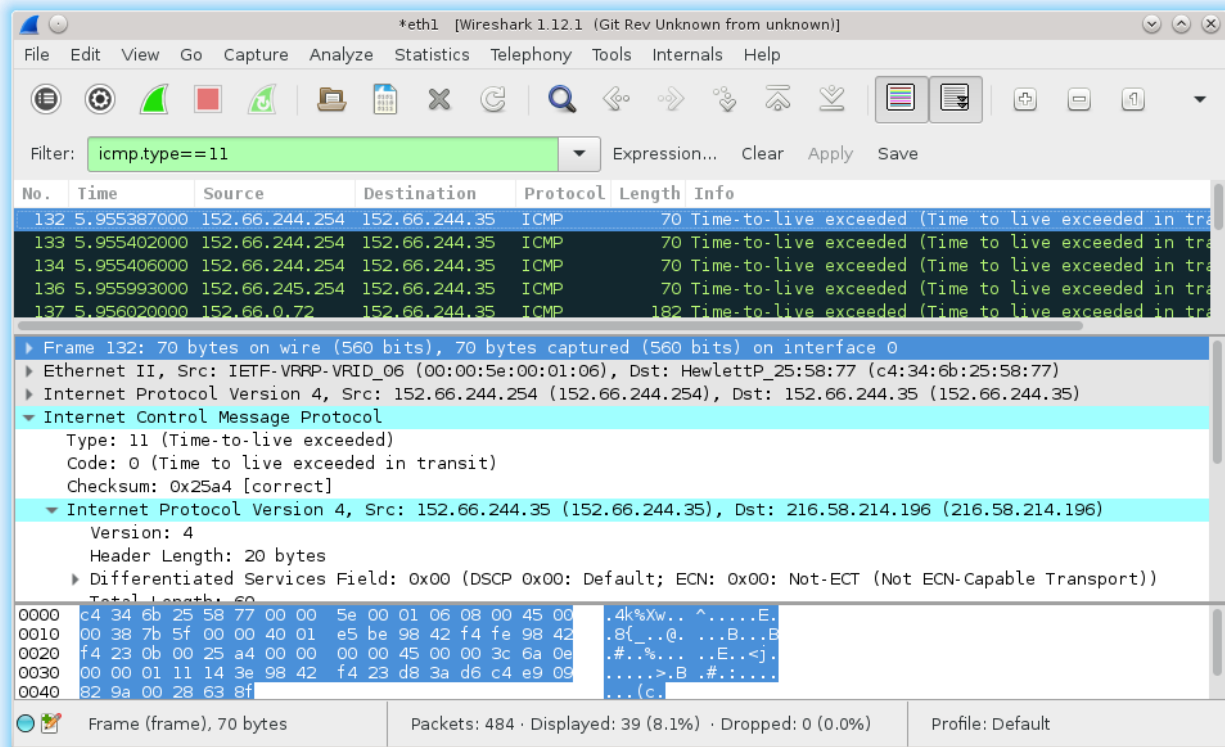
TCPDUMP – hálózati forgalom megfigyelése

- ▶ promiscuous mode: nem csak a gépnek küldött forgalom figyelése
 - ▶ -n címfeloldás kihagyása
 - ▶ -i *ifname*: a lehallgatott az interfész megadása (-i eth0)
 - ▶ -w *file*: az elfogott csomagok fájlba mentése *pcap* formátumban
 - ▶ -s *snaplen*: csak a csomag *snaplen* bájtját olvassa be (def: 65535)
- } Veszteségmentes megfigyelés
nagy sebesség mellett

```
root@betli:~# tcpdump -c 5 -p icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
07:28:14.010286 IP betli.tmit.bme.hu > site.tmit.bme.hu: ICMP echo request, id 6066, seq 23, length 64
07:28:14.010522 IP site.tmit.bme.hu > betli.tmit.bme.hu: ICMP echo reply, id 6066, seq 23, length 64
07:28:15.010330 IP betli.tmit.bme.hu > site.tmit.bme.hu: ICMP echo request, id 6066, seq 24, length 64
07:28:15.010633 IP site.tmit.bme.hu > betli.tmit.bme.hu: ICMP echo reply, id 6066, seq 24, length 64
07:28:16.010325 IP betli.tmit.bme.hu > site.tmit.bme.hu: ICMP echo request, id 6066, seq 25, length 64
5 packets captured
6 packets received by filter
0 packets dropped by kernel
root@betli:~# tcpdump -c 5 -p icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
07:28:39.706429 IP 244gw.tmit.bme.hu > betli.tmit.bme.hu: ICMP time exceeded in-transit, length 36
07:28:39.706454 IP 244gw.tmit.bme.hu > betli.tmit.bme.hu: ICMP time exceeded in-transit, length 36
07:28:39.706470 IP 244gw.tmit.bme.hu > betli.tmit.bme.hu: ICMP time exceeded in-transit, length 36
07:28:39.706998 IP vl121.ixion.net.bme.hu > betli.tmit.bme.hu: ICMP time exceeded in-transit, length 36
07:28:39.707097 IP vl121.ixion.net.bme.hu > betli.tmit.bme.hu: ICMP time exceeded in-transit, length 36
5 packets captured
50 packets received by filter
0 packets dropped by kernel
root@betli:~#
```


Wireshark – grafikus tcpdump

- ▶ Szintén pcap formátumot használ
- ▶ Moduláris felépítésű
 - ▶ *dissector* írja le egy protokoll működését
 - ▶ Python, Lua nyelven is írható hozzá dissector



Tshark: ~ a wiresharkra épülő okos tcpdump

```
root@betli:~# tshark -lni wlan1 -c2
Running as user "root" and group "root". This could be dangerous.
Capturing on 'wlan1'
  1 0.0000000000 fd96:f87d:9779::e9c → fd96:f87d:9779::1 SMB2 346 Create Request File: music\Ramones\1992-Anthology-(2CD)\Cd2\23-I_Don't_Wanna_Grow_Up.mp3
  2 0.002014293 fd96:f87d:9779::1 → fd96:f87d:9779::e9c SMB2 242 Create Response File: music\Ramones\1992-Anthology-(2CD)\Cd2\23-I_Don't_Wanna_Grow_Up.mp3
2 packets captured
root@betli:~#
```

```
root@betli:~# tshark -ni wlan1 -c1 -Tjson | head -n20
Running as user "root" and group "root". This could be da
Capturing on 'wlan1'
[
  {
    "_index": "packets-2022-09-20",
    "_type": "doc",
    "_score": null,
    "_source": {
      "layers": {
        "frame": {
```

Termshark: ~ a tsharkra épülő konzolos, nem túl okos wireshark

```
termshark 2.2.0 | wsvpn-20220805-embedded.pcap Analysis Misc
Filter:  <Apply> <Recent>
No. - Time - Source - Destination Protocol - Length Info -
4 0.01185 127.0.0.1 127.0.0.1 QUIC 1300 Handshake, SCID=230d9a81, PKN: 0,
5 0.01125 127.0.0.1 127.0.0.1 HTTP3 367 Protected Payload (KP0), PKN: 0, N
6 0.01411 127.0.0.1 127.0.0.1 QUIC 1300 Initial, DCID=230d9a81, PKN: 2, AC
7 0.01649 127.0.0.1 127.0.0.1 QUIC 123 Handshake, DCID=230d9a81, PKN: 0,
8 0.01706 127.0.0.1 127.0.0.1 QUIC 84 Handshake, SCID=230d9a81, PKN: 2,
9 0.01755 127.0.0.1 127.0.0.1 QUIC 303 Protected Payload (KP0), PKN: 1, D
10 0.01782 127.0.0.1 127.0.0.1 QUIC 77 Protected Payload (KP0), DCID=230d
11 0.01817 127.0.0.1 127.0.0.1 HTTP3 184 Protected Payload (KP0), DCID=a336
12 0.01843 127.0.0.1 127.0.0.1 QUIC 72 Protected Payload (KP0), PKN: 2, A
13 0.02862 127.0.0.1 127.0.0.1 HTTP3 123 Protected Payload (KP0), PKN: 3, S
14 0.02969 127.0.0.1 127.0.0.1 HTTP3 81 Protected Payload (KP0), DCID=a336
[+] Frame 9: 303 bytes on wire (2424 bits), 303 bytes captured (2424 bits) on interface unknown,
[+] Linux cooked capture v2
[+] Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
[+] User Datagram Protocol, Src Port: 9000, Dst Port: 58373
[-] QUIC IETF
  [+] QUIC Connection information
    Packet Length: 255
  [+] QUIC Short Header PKN=1
  [-] HANDSHAKE_DONE
    Frame Type: HANDSHAKE_DONE (0x000000000000001e)
  [+] NEW_TOKEN
  [+] TLSv1.3 Record Layer: Handshake Protocol: New Session Ticket
0000 08 00 00 00 00 00 01 03 04 00 06 00 00 00 00 . . . . .
0010 00 00 00 00 45 00 01 1b 00 00 40 00 40 11 3b d0 . . . E . . . @ , ; .
0020 7f 00 00 01 7f 00 00 01 23 28 e4 05 01 07 ff 1a . . . . . # ( . . . .
0030 4e 1c 97 4d fb 0d 39 32 60 67 af 87 97 00 f8 2b N . M . 92 g . . . +
0040 40 d3 5e c5 42 5b ad b3 64 aa cb 87 af 98 9b 49 @ ^ B [ . . . . I
0050 53 10 f3 61 94 df d6 24 4c 29 ab 06 7d 31 25 9f S . a . . $ L . . ) 1 % .
0060 33 a7 d9 8b b1 01 ba 46 bb 29 2a 11 de b0 8c e2 3 . . . . F . ) * . . . .
0070 41 ad eb 77 19 10 78 3d 4c f8 09 74 ca 5f 36 5a A . w . . x = L . t . _ 6 2
0080 fe 8c a1 a6 40 cd f3 c2 6b 7c 1a a2 10 e8 9c ca . . . @ . . k l . . . .
0090 5a 06 cd 3a 03 7f 78 3b 2e aa 14 4a f0 66 c0 fb Z . . . x ; . . . J . f . .
00a0 fc 26 2c ed ef f6 cb da b1 29 0c 7f de b8 8a e5 . & . . . . . ) . . . .
00b0 40 a6 bf 4e 1a 59 8a ad 76 69 9f 3a 1e 7b c3 5d @ . N . Y . . v i . . ( . ]
00c0 ec 7b df cf 67 1c 57 33 1b a4 84 35 1e d4 ac 27 . ( . g . W 3 . . . 5 . . '
```

Esetleg jól jöhet, ha

- ▶ nincs grafikus felületünk,
- ▶ valamit szöveggént szeretnénk kimásolni

Hálózat konfigurálása linux hoszton

Hálózati kommunikáció

▶ Layer 1-2-3



Hálózati interfész
neve: eth0, wlan1, ...



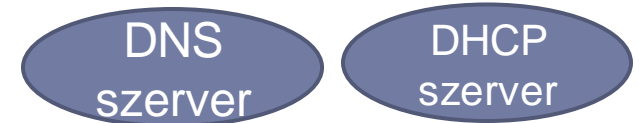
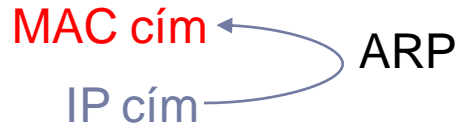
Switch/kapcsoló
(a helyi hálózaton)

MAC cím



Router/forgalomirányító
gateway

IP cím



Hálózat beállítási lehetőségei

- ▶ Disztribúciónként kicsit eltérő automatizmusok léteznek
 - ▶ De a “network manager”-t kell kikapcsolni, ha át akarjuk venni az irányítást
 - ▶ /etc/network könyvtár tartalmazza a konfigurációs fájlokat
- ▶ Félautomatikus megoldás: DHCP
 - ▶ Dynamic Host Configuration Protocol
 - ▶ # dhclient eth0
 - ▶ beállítható: IP address/netmask, default gateway, DNS, ...
- ▶ Manuális beállítás
 - ▶ ifconfig, ip (iproute2 csomag), route, iptables, ...

/etc/network/interfaces

```
auto lo
iface lo inet loopback
```

```
# Interfész konfigurálása dinamikus IP címmel (DHCP)
auto eth0
iface eth0 inet dhcp
```

```
# Interfész konfigurálása statikus IP cím hozzárendeléssel
auto eth1
iface eth1 inet static
address 192.168.1.3
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
up route add -net 192.168.1.0 netmask 255.255.255.0 gw 1
```

ifconfig

► Könnyen áttekinthető a használata, mégis az 'ip'-t preferáljuk

```
root@betli:~# /etc/init.d/network-manager stop
Stopping network-manager (via systemctl): network-manager.service.
root@betli:~# ifconfig eth1 down
root@betli:~# ifconfig
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:65536  Metric:1
            RX packets:96664 errors:0 dropped:0 overruns:0 frame:0
            TX packets:96664 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:15753772 (15.0 MiB)  TX bytes:15753772 (15.0 MiB)
root@betli:~# ifconfig eth1 up
root@betli:~# ifconfig eth1
eth1       Link encap:Ethernet  HWaddr c4:34:6b:25:58:77
            inet addr:152.66.244.35  Bcast:152.66.244.255  Mask:255.255.255.0
            inet6 addr: fe80::c634:6bff:fe25:5877/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:16969186 errors:0 dropped:56 overruns:0 frame:0
            TX packets:14331562 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:18852062080 (17.5 GiB)  TX bytes:12559976993 (11.6 GiB)
            Interrupt:20 Memory:d0700000-d0720000
```

```
root@betli:~# ifconfig eth1 152.66.244.35/24
root@betli:~# ifconfig
eth1       Link encap:Ethernet  HWaddr c4:34:6b:25:58:77
            inet addr:152.66.244.35  Bcast:152.66.244.255  Mask:255.255.255.0
            inet6 addr: fe80::c634:6bff:fe25:5877/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:16969664 errors:0 dropped:56 overruns:0 frame:0
            TX packets:14331565 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:18852095741 (17.5 GiB)  TX bytes:12559977231 (11.6 GiB)
            Interrupt:20 Memory:d0700000-d0720000
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:65536  Metric:1
            RX packets:96696 errors:0 dropped:0 overruns:0 frame:0
            TX packets:96696 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:15756140 (15.0 MiB)  TX bytes:15756140 (15.0 MiB)
root@betli:~# ping -c 1 152.66.244.189
64 bytes from 152.66.244.189: icmp_seq=1 ttl=64 time=0.419 ms
root@betli:~# ping -c 1 hsn.tmit.bme.hu
ping: unknown host hsn.tmit.bme.hu
root@betli:~# `
```

route

```
root@betli:~# route -n
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	152.66.159.254	0.0.0.0	UG	1024	0	0	wlan1
152.66.156.0	0.0.0.0	255.255.252.0	U	0	0	0	wlan1
152.66.244.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	eth1

```
root@betli:~#
```

- ▶ # route add default gw 152.66.159.254 eth1
- ▶ # ip route add 152.66.244.0/24 dev eth1
- ▶ # ip route add 152.66.244.0/24 via 152.66.159.254

Iproute2 – ip: egységes interface, moduláris felépítés

- ▶ # ip link set dev eth1 up
- ▶ # ip addr ls
- ▶ # ip addr del 152.66.244.35/24 dev eth1
- ▶ # ip addr add 152.66.244.35/32 dev eth1
- ▶ # ip link set dev eth1 mtu 1412
- ▶ # ip link set dev eth0 address 22:ce:e0:99:63:6f
- ▶ # ip link set eth0 arp off
- ▶ # ip route add default dev eth1
- ▶ # ip route add 152.66.244.0/24 dev eth1 metric 100
- ▶ # ip route add 152.66.244.0/24 dev eth2 metric 200
- ▶ # ip route add 152.66.244.0/24 via 152.66.159.254
- ▶ **Manages: address, route, link, link group, tun/tap devices, ARP/NDP tables, tunnels, police routing, ...**

DNS: hostname → IP address (vagy fordítva)

- ▶ /etc/resolv.conf
- ▶ Felhasználói programok nem direktben használják a DNS protokollt
- ▶ Libnss:
GNU Name Service Switch
 - ▶ Moduláris
 - ▶ Avahi module (zeroconf)
lan multicast query, response

```
root@betli:~# nslookup www.bme.hu
Server:         152.66.115.1
Address:        152.66.115.1#53

www.bme.hu      canonical name = inspiro.eik.bme.hu.
Name:   inspiro.eik.bme.hu
Address: 152.66.115.203

root@betli:~# host www.bme.hu
www.bme.hu is an alias for inspiro.eik.bme.hu.
inspiro.eik.bme.hu has address 152.66.115.203
inspiro.eik.bme.hu has IPv6 address 2001:738:2001:2001::f0c1
root@betli:~# dig www.bme.hu

;<<> DiG 9.9.5-9+deb8u6-Debian <<> www.bme.hu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9710
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.bme.hu.                IN      A

;; ANSWER SECTION:
www.bme.hu.                 14400  IN      CNAME   inspiro.eik.bme.hu.
inspiro.eik.bme.hu.        14400  IN      A       152.66.115.203

;; AUTHORITY SECTION:
bme.hu.                     14400  IN      NS      ns2.pantel.net.
bme.hu.                     14400  IN      NS      ns.bme.hu.
bme.hu.                     14400  IN      NS      nic.bme.hu.

;; ADDITIONAL SECTION:
ns.bme.hu.                  14400  IN      A       152.66.116.1
nic.bme.hu.                 14400  IN      A       152.66.115.1
ns2.pantel.net.             20516  IN      A       212.24.160.1
ns.bme.hu.                  14400  IN      AAAA   2001:738:2001:8001::2
nic.bme.hu.                 14400  IN      AAAA   2001:738:2001:2001::2

;; Query time: 1 msec
;; SERVER: 152.66.115.1#53(152.66.115.1)
;; WHEN: Mon Sep 19 10:45:59 CEST 2016
;; MSG SIZE rcvd: 248
```

ARP: IP address → MAC address

- ▶ ARP requestre ARP response a válasz,
- ▶ A kernel automatikusan karbantartja az ARP-táblát

```
root@betli:~# arp -i eth1 -s 10.0.0.10 aa:bb:cc:dd:ee:ff
root@betli:~# arp -n
```

Address	HWtype	HWaddress	Flags	Mask
152.66.159.160	ether	a4:5e:60:c1:12:75	C	
152.66.156.39	ether	b8:e8:56:0f:03:6c	C	
152.66.244.174	ether	00:0c:29:29:22:23	C	
152.66.158.251	ether	0c:8b:fd:63:be:33	C	
152.66.156.101	(incomplete)			
152.66.159.113	ether	00:24:d7:2a:81:10	C	
10.0.0.10	ether	aa:bb:cc:dd:ee:ff	CM	
152.66.158.252	ether	28:cf:e9:4d:8e:83	C	
152.66.159.231	(incomplete)			

```
root@betli:~#
```

```
root@betli:~# arping -c 3 -I eth1 152.66.244.189
```

```
ARPING 152.66.244.189 from 152.66.244.35 eth1
Unicast reply from 152.66.244.189 [00:0c:29:29:22:23] 0.738ms
Unicast reply from 152.66.244.189 [00:0c:29:29:22:23] 0.854ms
Unicast reply from 152.66.244.189 [00:0c:29:29:22:23] 0.720ms
Sent 3 probes (1 broadcast(s))
Received 3 response(s)
root@betli:~#
```

- ▶ Egyéb eszközök:

- ▶ arpswatch/arpmonitor, arpoison, arpspoof, arping, arp-sk

*eth1 [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
139	8.323850000	HewlettP_25:58	Vmware_29:22:23	ARP	42	Who has 152.66.244.189? Tell 152.66.244.35
140	8.324118000	Vmware_29:22:23	HewlettP_25:58	ARP	60	152.66.244.189 is at 00:0c:29:29:22:23

▶ Frame 140: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Ethernet II, Src: Vmware_29:22:23 (00:0c:29:29:22:23), Dst: HewlettP_25:58:77 (c4:34:6b:25:58:77)

▼ Address Resolution Protocol (reply)

- Hardware type: Ethernet (1)
- Protocol type: IP (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)
- Sender MAC address: Vmware_29:22:23 (00:0c:29:29:22:23)
- Sender IP address: 152.66.244.189 (152.66.244.189)
- Target MAC address: HewlettP_25:58:77 (c4:34:6b:25:58:77)
- Target IP address: 152.66.244.35 (152.66.244.35)

```
0000 c4 34 6b 25 58 77 00 0c 29 29 22 23 08 06 00 01  .4k%Xw... )#.#...
0010 08 00 06 04 00 02 00 0c 29 29 22 23 98 42 f4 bd  ..... )#.#.B...
0020 c4 34 6b 25 58 77 98 42 f4 23 00 00 00 00 00 00  .4k%Xw.B #.....
0030 00 00 00 00 00 00 00 00 00 00 00 00  ..... .....
```

iptables: tűzfal és NAT beállítása

- ▶ (későbbi órán tárgyaljuk)

(Az 'ip' sok mindenre jó: MPLS)

▶ Enable mpls support

- ▶ `sysctl -w net.mpls.conf.eth0.input=1`
- ▶ `sysctl -w net.mpls.conf.eth1.input=1`
- ▶ `sysctl -w net.mpls.platform_labels=1000`

▶ Routing 10.10.10.10/32 to 192.168.1.2 with label 100:

- ▶ `ip route add 10.10.10.10/32 encap mpls 100 via inet 192.168.1.2`

▶ Label swapping 100 for 200 and sent to 192.168.2.2:

- ▶ `ip -f mpls route add 100 as 200 via inet 192.168.2.2`

▶ Decapsulating label 300 and delivering locally:

- ▶ `ip -f mpls route add 300 dev lo`

▶ To show MPLS routes you can do:

- ▶ `ip -f mpls route show`

Több IP cím egy interfészen

▶ # ifconfig eth0:0 192.168.1.6 up

Egyéb hasznos eszközök

netcat

Xterm-1

▶ `$ nc -l 2389`

▶ `HI, server`

Xterm-2

▶ `$ nc localhost 2389`

▶ `HI, server`

telnet

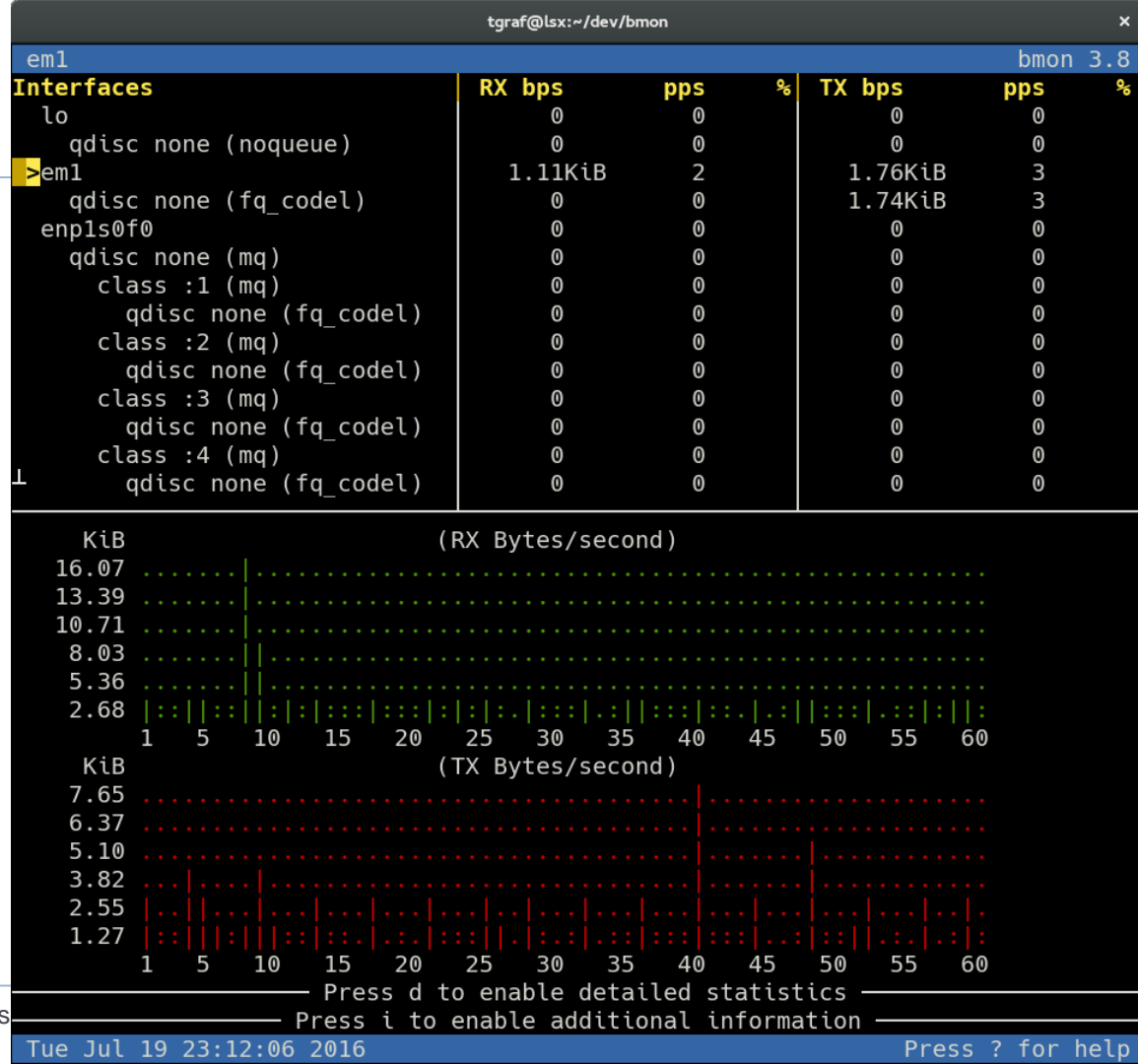
- ▶ Távoli terminál elérése **titkosítatlan** adatforgalommal
- ▶ Használjuk helyette az SSH-t
- ▶ Debuggolásra, fejlesztésre azért nagyszerű:
- ▶ Portkiosztás: /etc/services

```
root@betli:~# telnet www.bme.hu 80
Trying 2001:738:2001:2001::f0c1...
Connected to inspiro.eik.bme.hu.
Escape character is '^]'.
GET / HTTP/1.0
host: www.bme.hu

HTTP/1.1 200 OK
Date: Mon, 19 Sep 2016 09:20:40 GMT
Server: Apache
X-Powered-By: PHP/5.4.45-0+deb7u5
X-Drupal-Cache: HIT
Etag: "1474276784-0"
Content-Language: hu
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
```

bmon

- ▶ Bandwidth monitor
- ▶ Ideális gyors teszteléshez
- ▶ Vannak profibb monitoring toolok



Python

A hálózatos világban is jól használható szkript nyelv.
Otthon, önállóan kell megismerkedni vele

Scapy – python-based packet manipulator

```
>>> send(IP(dst="1.2.3.4")/ICMP())
.
Sent 1 packets.
>>> sendp(Ether()/IP(dst="1.2.3.4",ttl=(1,4)), iface="eth1")
.....
Sent 4 packets.
>>> sendp("I'm travelling on Ethernet", iface="eth1", loop=1, inter=0.2)
.....^C
Sent 16 packets.
>>> sendp(rdpcap("/tmp/pcapfile")) # tcpreplay
.....
Sent 11 packets.
```

```
>>> p=srl(IP(dst="www.slashdot.org")/ICMP())/XXXXXXXXXX"
Begin emission:
...Finished to send 1 packets.
.*
Received 5 packets, got 1 answers, remaining 0 packets
>>> p
<IP version=4L ihl=5L tos=0x0 len=39 id=15489 flags= frag=0L ttl=42 proto=ICMP
chksum=0x51dd src=66.35.250.151 dst=192.168.5.21 options='' |<ICMP type=echo-reply
code=0 chksum=0xee45 id=0x0 seq=0x0 |<Raw load='XXXXXXXXXX'
|<Padding load='\x00\x00\x00\x00' |>>>
>>> p.show()
---[ IP ]---
version   = 4L
ihl       = 5L
tos       = 0x0
len       = 39
id        = 15489
flags     =
frag      = 0L
ttl       = 42
proto     = ICMP
chksum    = 0x51dd
src       = 66.35.250.151
dst       = 192.168.5.21
options   = ''
---[ ICMP ]---
type      = echo-reply
code      = 0
chksum    = 0xee45
id        = 0x0
seq       = 0x0
---[ Raw ]---
load      = 'XXXXXXXXXX'
---[ Padding ]---
load      = '\x00\x00\x00\x00'
```

- ▶ UTScapy: unit testing with scapy

Házi feladat

- ▶ Az órai anyag átnézése
- ▶ `man ping` parancs kiadása és az kimenet elolvasása
- ▶ Egy `ping` parancs kiadása és a ping csomagok megkeresése a `tcpdump` vagy a `wireshark` segítségével