

Mérési jegyzőkönyv

Ethernet és TCP/IP protokollok vizsgálata

V03b (2014.01.28.)

A feladatokat összeállította: Kovácsházy Tamás, BME MIT, 2008-2010.

A jegyzőkönyvsablont módosította: Tóth Csaba, BME MIT, 2011.

A feladatokat és a sablont módosította: Huszerl Gábor, BME MIT, 2012-2013.

A jegyzőkönyvsablont módosította: Tóth Csaba, BME MIT, 2014.

A mérés helyszíne:	I.B141/IB142, ... mérőhely
A mérés időpontja:	2014. február 4.
A mérést végezték:	Varga Domonkos
Ennek a fájlnak a neve:	fájlnév ml4_vargad_1.doc
A mérésvezető neve:	Naszály Gábor

Tudnivalók:

- Csak a világossárga színnel jelölt részekre írjon! A fejléctet értelemszerűen töltse ki.
- A <<... képernyőkép>> emlékeztető szöveg helyére vagy alá illessze be a feladat megoldását igazoló képernyőképet!
- A feladatok egy részét az ellenőrzőmérésen csak az ötös osztályzathoz kell megoldani, ezeket *-gal jelöltük.
- A feladatok egy része fakultatív, ezek nem számítanak bele az értékelésbe, csak ha marad idő, akkor fogjanak hozzá! (Cserébe viszont szakmailag érdekesek.)
- A mérésekkel kapcsolatos észrevételeit jelezze a mérésvezetőnek vagy a tárgyfelelősnek (toth AT mit.bme.hu)!

1. feladat: Ethernet és TCP/IP beállítások megismerése

A feladat célja: Ethernet hálózati interfészek alapvető TCP/IP beállításainak megismerése az **ipconfig** és a **route print** program segítségével.

1.1. A számítógép (PC) hálózati interfészei és beállításai

Állapítsa meg, hogy milyen hálózati interfészei vannak a mérés során használt számítógépnek, majd határozza meg az egyes interfészek hálózati beállításait!

Adja ki a Windows Command Prompt ablakban az **ipconfig** majd az **ipconfig /all** parancsot, és másolja be a kapott képernyőábrát a jegyzőkönyvbe!

Tanácsok:

- A **cd ** paranccsal váltson át a gyökérkönyvtárba, hogy a fölösleges könyvtári útvonal ne zavarjon!
- A command ablak csúszkájával és a command ablak magasságával állítsa be úgy az ablakot, hogy csak a kívánt szövegrész látszódjék, és ALT+Print Screen-nel másolja ki az ablak tartalmát, majd illessze be a jegyzőkönyv megfelelő helyére CTRL+V-vel!
- Egy másik, nehezebb és kevésbé látványos megoldás, de hosszú szövegeknél szükség lehet rá: másolja ki a command ablakból a vonatkozó szöveget, és formázza olvashatóra a jegyzőkönyvben! (Ehhez a command ablak jobb egérgombos felugró menüjében válassza ki a Megjelölés (Mark) funkciót, jelölje ki az ablak tartalmának átmásolandó részét, és Enterrel másolja be a vágólapra a kijelölt részt, majd a CTRL+V-vel másolja be a jegyzőkönyvbe a megfelelő helyre! Ne feledkezzen meg a formázásról!)

ipconfig

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\student>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : mit.bme.hu
    Link-local IPv6 Address . . . . . : fe80::e4ce:9cba:1115:c2a0%10
    IPv4 Address. . . . . : 152.66.254.214
    Subnet Mask . . . . . : 255.255.255.192
    Default Gateway . . . . . : 152.66.254.254

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2961:5c10:eb86:427%15
    IPv4 Address. . . . . : 192.168.241.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::283c:5163:e772:ed42%17
    IPv4 Address. . . . . : 192.168.161.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Tunnel adapter {F187BDDD-B65C-49BC-8D7F-0E1EA8F580BA}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter 6T04 Adapter:

    Connection-specific DNS Suffix  . : mit.bme.hu
    IPv6 Address. . . . . : 2002:9842:fed6::9842:fed6
    Default Gateway . . . . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter {25D85670-AE92-4E82-BEDE-0DCC6B0AE0ED}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.mit.bme.hu:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : mit.bme.hu

C:\Users\student>
```

ipconfig /all

```
Command Prompt
C:\Users\student>ipconfig /all

Windows IP Configuration

Host Name . . . . . : alabi14
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : mit.bme.hu

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : mit.bme.hu
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 1C-6F-65-CD-CC-70
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e4ce:9cba:1115:c2a0%10(Preferred)
IPv4 Address. . . . . : 152.66.254.214(Preferred)
Subnet Mask . . . . . : 255.255.255.192
Lease Obtained. . . . . : 2014. február 4. 9:05:05
Lease Expires . . . . . : 2014. február 4. 13:05:12
Default Gateway . . . . . : 152.66.254.254
DHCP Server . . . . . : 152.66.254.253
DHCPv6 IAID . . . . . : 236744549
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-A3-67-BF-1C-6F-65-CD-CC-70
DNS Servers . . . . . : 152.66.115.1
                        152.66.116.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Physical Address. . . . . : 00-50-56-C0-00-01
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2961:5c10:eb86:427%15(Preferred)
IPv4 Address. . . . . : 192.168.241.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 335564886
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-A3-67-BF-1C-6F-65-CD-CC-70
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet8
Physical Address. . . . . : 00-50-56-C0-00-08
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::283c:5163:e772:ed42%17(Preferred)
IPv4 Address. . . . . : 192.168.161.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 369119318
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-A3-67-BF-1C-6F-65-CD-CC-70
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
```

Elemezze és hasonlítsa össze az **ipconfig** és az **ipconfig/all** parancsra kapott válaszokat, és ezek alapján töltsse ki az alábbi táblázatot! (A tunnel adapterekkel ne foglalkozzon, azok az IPv6-os funkciók IPv4-es környezetben való használatát támogatják. A mérésen nem használjuk őket.)

Hálózati interfészek beállításai:

Név	<i>Ethernet adapter Local Area Connection</i>	<i>Ethernet adapter VMware Network Adapter VMnet1</i>	<i>Ethernet adapter VMware Network Adapter VMnet8</i>
IP cím	152.66.254.214	192.168.241.1	192.168.161.1
Alhálózati maszk	255.255.255.192	255.255.255.0	255.255.255.0
Alapértelmezett átjáró	152.66.254.254	-----	-----
DHCP engedélyezve	Igen	Nem	Nem
DNS szerverek	152.66.115.1 152.66.116.1	fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1	fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1
Kapcsolatspecifikus DNS utótag	mit.bme.hu	-----	-----

Nézze meg az **ipconfig** parancs egyéb paramétereit is az **ipconfig /?** segítségével!
(Pl. a **/flushdns**-re szükség lesz a további mérésekben.)

ipconfig /?

```
Command Prompt
C:\Users\student>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid] ]

where
    adapter          Connection name
                     (wildcard characters * and ? allowed, see examples)

Options:
    /?              Display this help message
    /all            Display full configuration information.
    /release        Release the IPv4 address for the specified adapter.
    /release6       Release the IPv6 address for the specified adapter.
    /renew          Renew the IPv4 address for the specified adapter.
    /renew6         Renew the IPv6 address for the specified adapter.
    /flushdns       Purges the DNS Resolver cache.
    /registerdns    Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid    Displays all the dhcp class IDs allowed for adapter.
    /setclassid     Modifies the dhcp class id.
    /showclassid6  Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6   Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                ... Show information
    > ipconfig /all            ... Show detailed information
    > ipconfig /renew          ... renew all adapters
    > ipconfig /renew EL*      ... renew any connection that has its
                               name starting with EL
    > ipconfig /release *Con*  ... release all matching connections,
                               eg. "Local Area Connection 1" or
                               "Local Area Connection 2"
    > ipconfig /allcompartments ... Show information about all
                               compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                               compartments

C:\Users\student>
```

1.2. IP címtartományok

Mi a laborban használható IP címek tartománya?

IP címtartomány:	152.66.254.193 - 152.66.254.254
------------------	---------------------------------

1.3. Default gateway, subnet broadcast IP cím és a DHCP szerver címe

Mi az alapértelmezett átjáró (default gateway), a subnet broadcast IP cím és a DHCP szerver címe?

	IP-cím
Alapértelmezett átjáró:	152.66.254.254
Subnet broadcast:	152.66.254.255
DHCP szerver:	152.66.254.253

1.4. DNS szerver

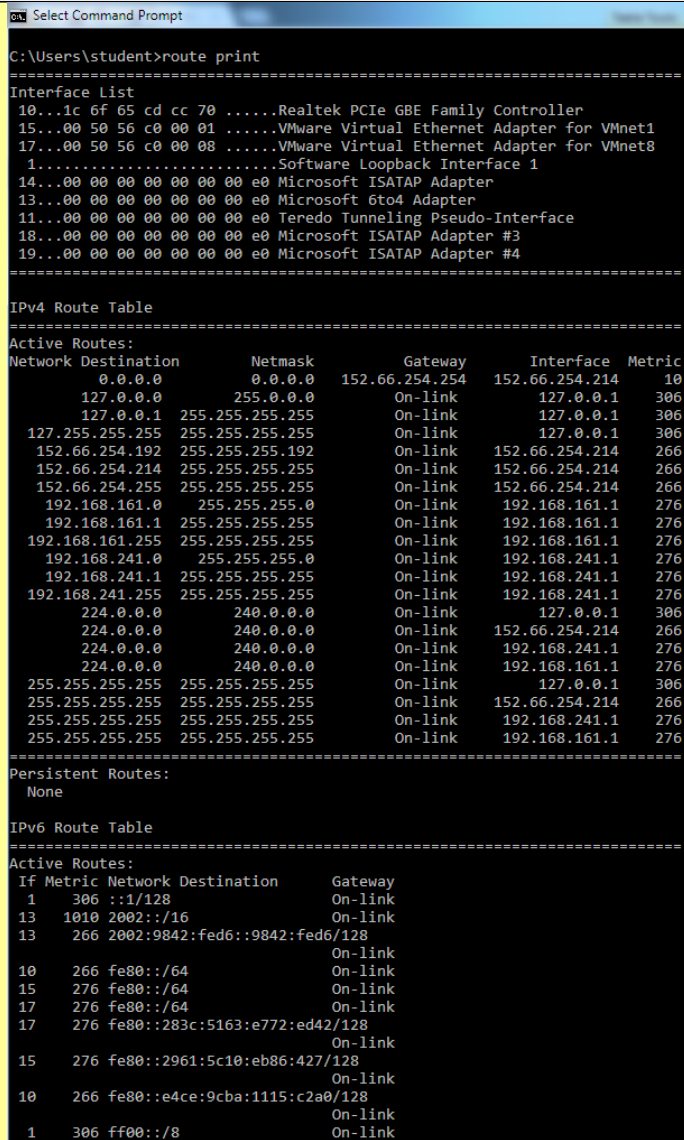
Mely DNS szervereket használja a gép? Mire kellenek ezek? (IP-cím, definíció)
152.66.115.1 152.66.116.1 A domain névhez társítják a megfelelő IP címet.
Miért szükséges több DNS szerver megadni?
A redundancia miatt.
Miért nem domain nevükkel adtuk meg a DNS szervereket?
A domain – IP cím fordítás miatt nem.

1.5. Internet útvonalak

Futtassa le a **route print** parancsot!

(A válasznak csak az „IPv4 Route Table” részével foglalkozzanak.)

route print



```

C:\Users\student>route print

Interface List
=====
10...1c 6f 65 cd cc 70 .....Realtek PCIe GBE Family Controller
15...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
17...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
1 .....Software Loopback Interface 1
14...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
11...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
18...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
19...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway             Interface           Metric
0.0.0.0                    0.0.0.0          152.66.254.254      152.66.254.214      10
127.0.0.0                  255.0.0.0         On-link             127.0.0.1           306
127.0.0.1                  255.255.255.255   On-link             127.0.0.1           306
127.255.255.255            255.255.255.255   On-link             127.0.0.1           306
152.66.254.192             255.255.255.192   On-link             152.66.254.214      266
152.66.254.214             255.255.255.255   On-link             152.66.254.214      266
152.66.254.255             255.255.255.255   On-link             152.66.254.214      266
192.168.161.0              255.255.255.0     On-link             192.168.161.1       276
192.168.161.1              255.255.255.255   On-link             192.168.161.1       276
192.168.161.255            255.255.255.255   On-link             192.168.161.1       276
192.168.241.0              255.255.255.0     On-link             192.168.241.1       276
192.168.241.1              255.255.255.255   On-link             192.168.241.1       276
192.168.241.255            255.255.255.255   On-link             192.168.241.1       276
224.0.0.0                  240.0.0.0         On-link             127.0.0.1           306
224.0.0.0                  240.0.0.0         On-link             152.66.254.214      266
224.0.0.0                  240.0.0.0         On-link             192.168.241.1       276
224.0.0.0                  240.0.0.0         On-link             192.168.161.1       276
255.255.255.255            255.255.255.255   On-link             127.0.0.1           306
255.255.255.255            255.255.255.255   On-link             152.66.254.214      266
255.255.255.255            255.255.255.255   On-link             192.168.241.1       276
255.255.255.255            255.255.255.255   On-link             192.168.161.1       276
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 306 ::1/128                      On-link
13 1010 2002::/16                  On-link
13 266 2002:9842:fed6::9842:fed6/128 On-link
10 266 fe80::/64                  On-link
15 276 fe80::/64                  On-link
17 276 fe80::/64                  On-link
17 276 fe80::283c:5163:e772:ed42/128 On-link
15 276 fe80::2961:5c10:eb86:427/128 On-link
10 266 fe80::e4ce:9cba:1115:c2a0/128 On-link
1 306 ff00::/8                    On-link

```

Magyarázza meg a program kimenetét!¹

A route print kimenete azt adja meg, hogy az IP cím alapján melyik interfészen lesz kiküldve a célállomáshoz.

Hogyan használja fel ezt az információt a számítógép TCP/IP protokoll-stackje?

A csomagokat ez alapján továbbítják.

¹ A Windowsban használt útvonalválasztásról itt találhat leírást: TCP/IP Fundamentals for Microsoft Windows, Chapter 5 IP Routing, <http://technet.microsoft.com/en-us/library/bb727001.aspx#EEAA>

Mik a kimenetben megjelenő **0.0.0.0** és **127.0.0.0** IP címekhez tartozó bejegyzések, és mikor/mire használják azokat?

0.0.0.0:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	152.66.254.254	152.66.254.214	10

127.0.0.0:

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306

Mik a **224.0.0.0** IP címekhez tartozó bejegyzések?

224.0.0.0:

224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	152.66.254.214	266
224.0.0.0	240.0.0.0	On-link	192.168.241.1	276
224.0.0.0	240.0.0.0	On-link	192.168.161.1	276

2. feladat: Ethernet címek és összerendelésük IP címekkel

A feladat célja: Ethernet címek és IP címek összerendelésének megértése a **ping** program segítségével.

A **ping** egy olyan hálózati tesztprogram, amely a paramétereként megadott IP című vagy domain nevű gépnek egy *ICMP Echo Request* üzenetet küld (alapbeállításban négyszer), amelyre a célállomás egy *ICMP Echo Reply* üzenettel válaszol (ha a telepített tűzfal nem tiltja).

A mérés során felhasználjuk az ARP-t (*Address Resolution Protocol*), amely az IP címekhez Ethernet címet rendel. Az ARP implementációk a kérések számának minimalizálására cache-ben tárolják az adatokat (pl. a Windows XP 10 percig tartja meg a bejegyzéseket). Az ARP cache tartalmát az **arp -a** paranccsal lehet megnézni, az **arp -d *** paranccsal pedig törölni. (Nézze meg az **arp** parancs egyéb paraméterezését is (**arp /?** segítségével)! A törléshez rendszergazdai jogosultságra van szükség. Ilyet emelt jogosultságú (elevated) command ablak használatával tud szerezni. Ehhez linket az asztalon talál.

Szintén használni fogjuk a DNS-t (Domain Name System), amely a domain nevekhez IP címeket rendel (erről a protokollról később még szó lesz). A Windows a DNS kérések számának minimalizálására fenntart egy DNS cache-t, alapértelmezésben 24 órás tárolási idővel. Az **ipconfig /displaydns** kiírja a DNS cache tartalmát, az **ipconfig /flushdns** pedig törli.

A mérés könnyítése érdekében a következő feladatokat egy virtuális gépből végezzék. Ezzel a többi mérőpár zavaró mellékhatásaitól tudnak megszabadulni. Indítsák el a VMware Player alkalmazást (taskbar), majd nyissa meg a 2meres_Win2013 nevű virtuális gépet. Ellenőrizze (Edit VM settings), hogy a hálózati adaptere NAT módban legyen, állítsa át erre, ha kell. Indítsa el a virtuális gépet. A meres felhasználó jelszava MeresLabor4.

A feladat során öt célállomást kell a **ping** parancs segítségével megszólítani, rögzíteni mind az öt alkalommal a teljes forgalmat Wireshark programmal, majd a hálózati forgalom elemzésével válaszolni a feltett kérdésekre.

A vizsgálandó gépek, domain nevek:

1. alapértelmezett átjáró (default gateway),
2. a labor DHCP szervere,
3. az alaplabor szervere (alaplab.mit.bme.hu),
4. egy nem létező, fantom.mit.bme.hu domain nevű gép,
5. a subnet broadcast cím.

A mérések előtt minden esetben törölje ki az ARP és DNS cache-t, hogy a protokoll teljes működését meg tudja figyelni! A feladathoz készítsen egy batch file-t! A batch fájl egy egyszerű, **bat** vagy **cmd** kiterjesztésű szöveges fájl, amelyben minden sorban egy-egy végrehajtandó parancs van. A batch fájlnak átadott paraméterekre a %1, %2 stb. változókkal lehet hivatkozni.

A mérés menete:

- Készítsen egy batch fájlt, amely törli az ARP és DNS cache-t, és egyúttal kiadja a **ping** parancsot! A batch fájl NE ping-nek nevezze el. Gondolja végig, hogy ez miért lenne rossz ötlet.
- Indítsa el a fizikai gépen Wiresharkban a forgalomrögzítést! Azt a hálózati interface-t figyelje, amelynek IP-címe a virtuális gép alhálózatának címtartományába esik. (A virtuális gép IP beállításai látszanak az asztala háttérképén, a Wiresharkban a hálózati interfészek címe olvasható az interface kiválasztásakor. Az interface címére kattintva válthat az IPv6-os és IPv4-es címek között.)

- A batch fájl segítségével **ping**-elje meg a megfelelő gépet/nevet!
- Állítsa le a forgalomrögzítést!
- Másolja be a jegyzőkönyvbe a cmd ablakot!
- Készítsen/alkalmazzon display filtert a Wiresharkhoz a zavaró forgalom kiszűrésére!
- Másolja be a jegyzőkönyvbe a Wireshark-ablak jellemző részletét vagy a teljes ablakot!
- Mentse el későbbi elemzés céljából a Wiresharkkal rögzített adatokat!
- Értelemszerűen ismételje meg a fentieket a többi célállomásra is!

2.1. Batch fájl szerkesztése

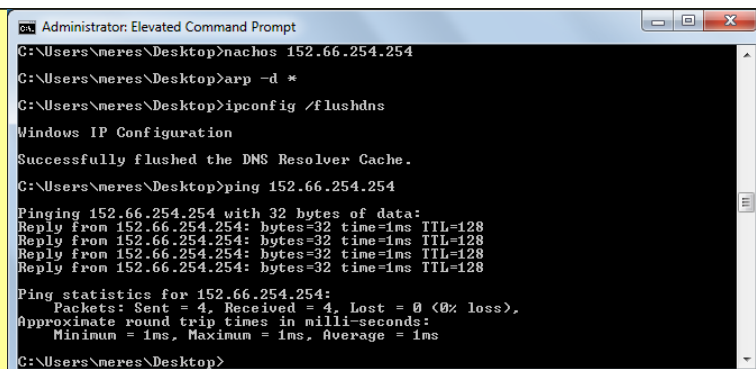
Készítsen egy batch fájlt, amely törli az ARP és DNS cache-t és kiadja a **ping** parancsot!

Másolja ide a fájl tartalmát!

```
arp -d *  
ipconfig /flushdns  
ping %1
```

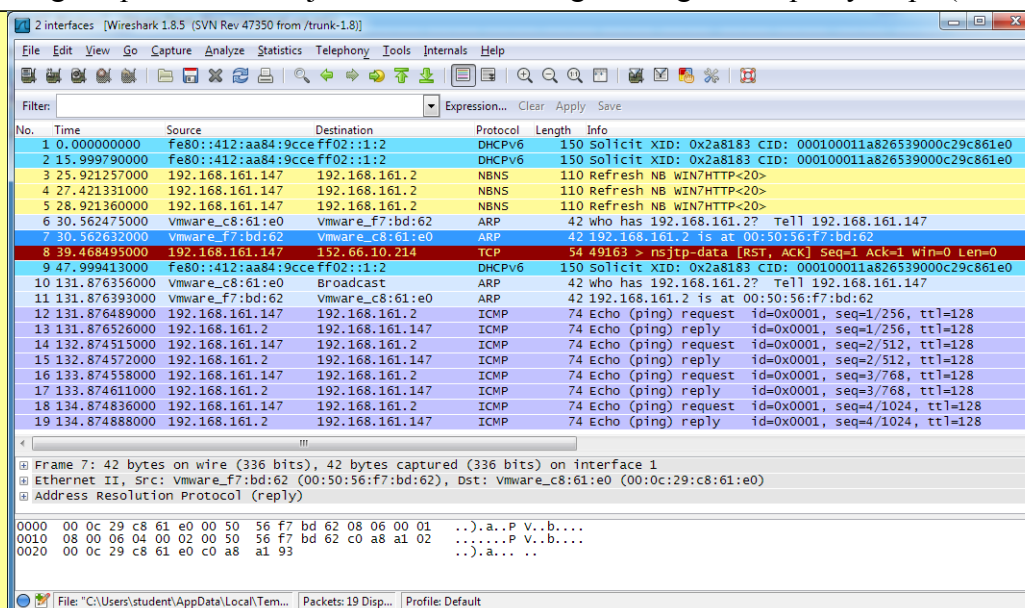
2.2. Alapértelmezett átjáró pingelése

Ping: alapértelmezett átjáró – cmd ablak képernyőképe



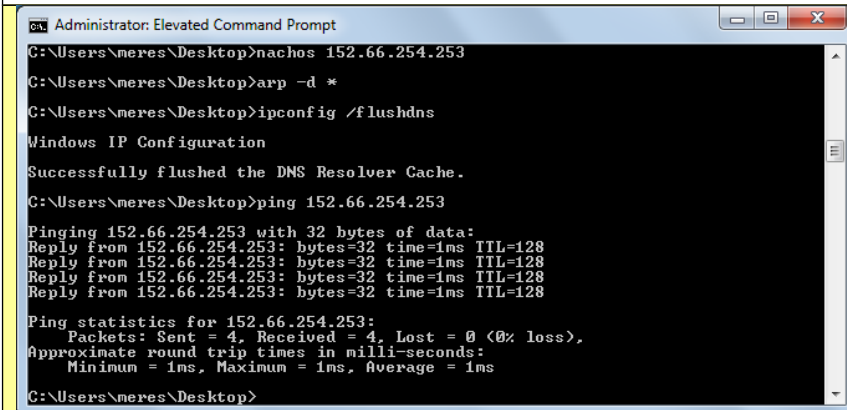
```
Administrator: Elevated Command Prompt  
C:\Users\meres\Desktop>nachos 152.66.254.254  
C:\Users\meres\Desktop>arp -d *  
C:\Users\meres\Desktop>ipconfig /flushdns  
Windows IP Configuration  
Successfully flushed the DNS Resolver Cache.  
C:\Users\meres\Desktop>ping 152.66.254.254  
Pinging 152.66.254.254 with 32 bytes of data:  
Reply from 152.66.254.254: bytes=32 time=1ms TTL=128  
Reply from 152.66.254.254: bytes=32 time=1ms TTL=128  
Reply from 152.66.254.254: bytes=32 time=1ms TTL=128  
Reply from 152.66.254.254: bytes=32 time=1ms TTL=128  
Ping statistics for 152.66.254.254:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 1ms, Average = 1ms  
C:\Users\meres\Desktop>
```

Ping: alapértelmezett átjáró – Wireshark forgalomrögzítés képernyőképe (szűrés nélkül)



2.3. A *labor* DHCP szervert pingelése

Ping: DHCP server – cmd ablak képernyőképe

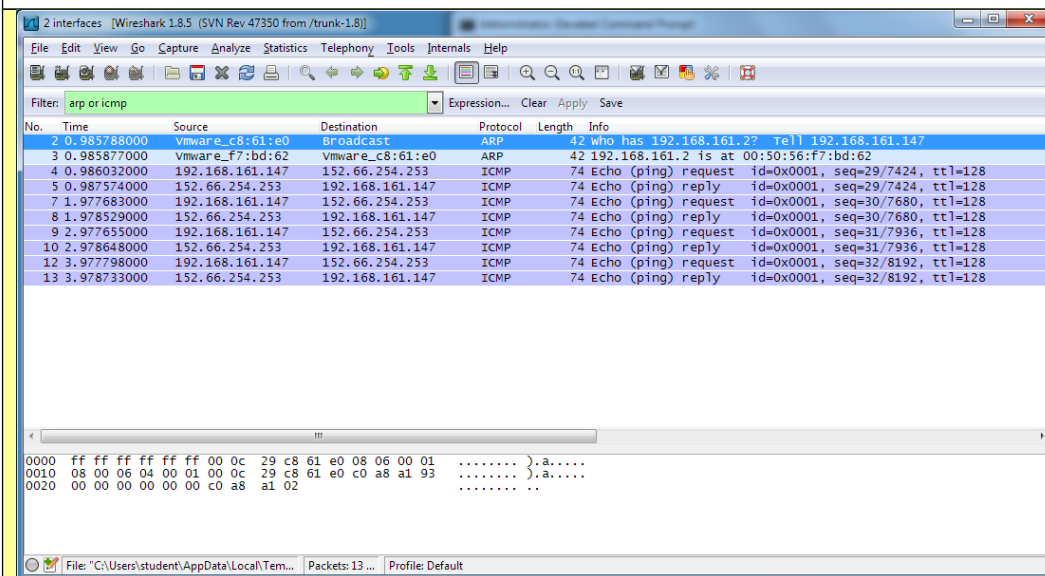


```
Administrator: Elevated Command Prompt
C:\Users\meres\Desktop>nachos 152.66.254.253
C:\Users\meres\Desktop>arp -d *
C:\Users\meres\Desktop>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\meres\Desktop>ping 152.66.254.253

Pinging 152.66.254.253 with 32 bytes of data:
Reply from 152.66.254.253: bytes=32 time=1ms TTL=128
Reply from 152.66.254.253: bytes=32 time=1ms TTL=128
Reply from 152.66.254.253: bytes=32 time=1ms TTL=128
Reply from 152.66.254.253: bytes=32 time=1ms TTL=128

Ping statistics for 152.66.254.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\meres\Desktop>
```

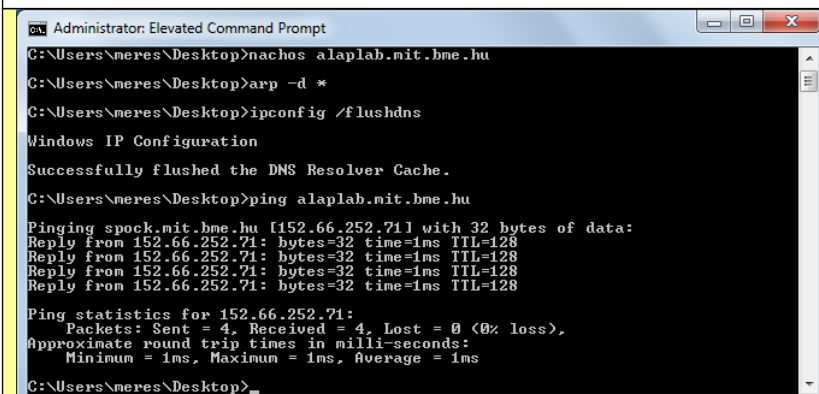
Ping: DHCP server – Wireshark forgalomrögzítés képernyőképe display filterrel



2.4. Az *alaplabor* szervert pingelése

Ez valójában már nem az aplalabor szervert, de ez a mostani eredmény szempontjából mellékes.

Ping: aplalab.mit.bme.hu – cmd ablak képernyőképe

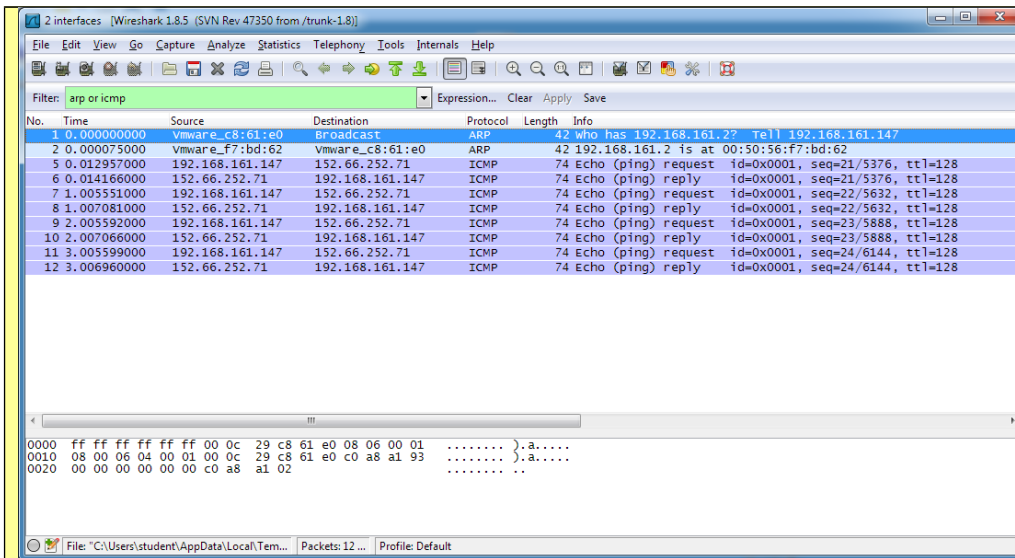


```
Administrator: Elevated Command Prompt
C:\Users\meres\Desktop>nachos aplalab.mit.bme.hu
C:\Users\meres\Desktop>arp -d *
C:\Users\meres\Desktop>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\meres\Desktop>ping aplalab.mit.bme.hu

Pinging spock.mit.bme.hu [152.66.252.71] with 32 bytes of data:
Reply from 152.66.252.71: bytes=32 time=1ms TTL=128
Reply from 152.66.252.71: bytes=32 time=1ms TTL=128
Reply from 152.66.252.71: bytes=32 time=1ms TTL=128
Reply from 152.66.252.71: bytes=32 time=1ms TTL=128

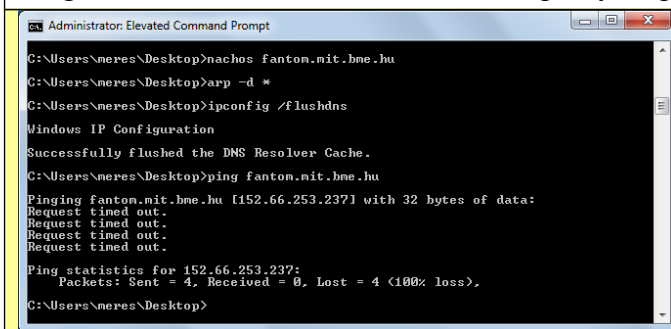
Ping statistics for 152.66.252.71:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\meres\Desktop>
```

Ping: aplalab.mit.bme.hu – Wireshark forgalomrögzítés képernyőképe display filterrel

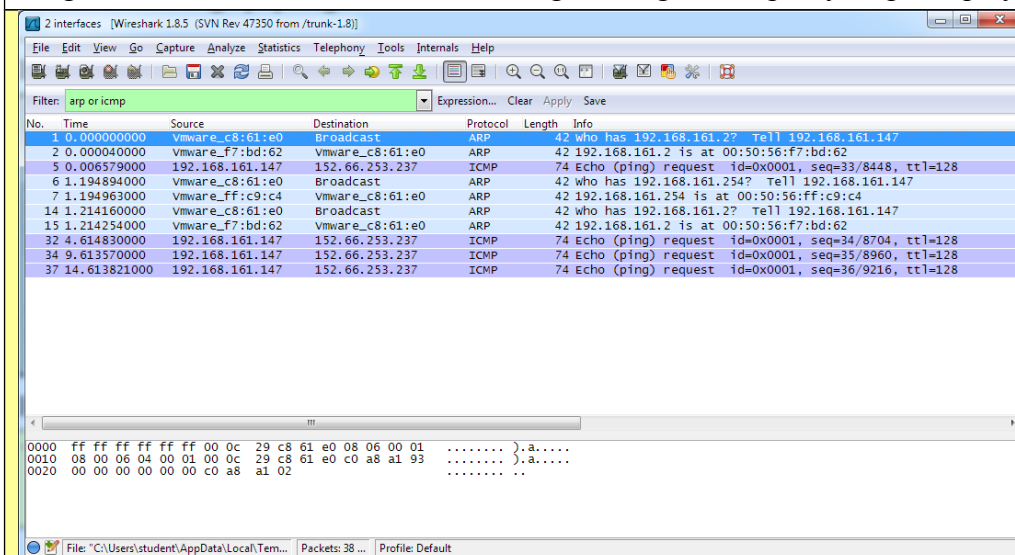


2.5. Fantom gép pingelése

Ping: fantom.mit.bme.hu – cmd ablak képernyőképe



Ping: fantom.mit.bme.hu – Wireshark forgalomrögzés képernyőképe display filterrel



2.6. Subnet broadcast cím pingelése

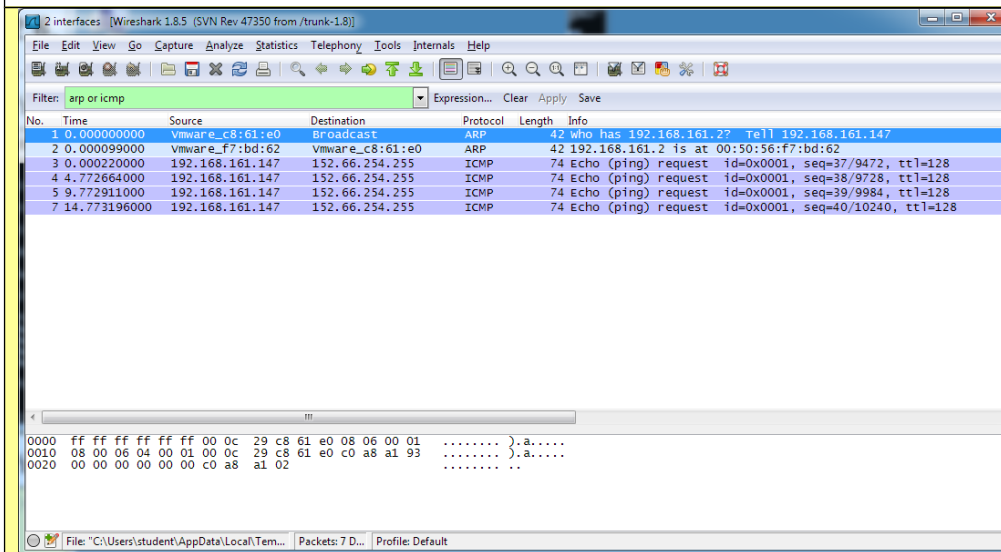
Ping: subnet broadcast cím – cmd ablak képernyőképe

```

Administrator: Elevated Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\neres\Desktop>nachos 152.66.254.255
C:\Users\neres\Desktop>arp -d *
C:\Users\neres\Desktop>ipconfig /Flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\neres\Desktop>ping 152.66.254.255
Pinging 152.66.254.255 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 152.66.254.255:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\neres\Desktop>
  
```

Ping: subnet broadcast cím – Wireshark forgalomrögzítés képernyőképe display filterrel



2.7. feladat

A következő esetekben sor került-e ARP és DNS kérésekre?

Ha igen, hány darabra, és mit kérdeztünk le? Ha nem, miért nem?

	ARP kérés(ek)	DNS kérés(ek)
Alapértelmezett átjáró:	1 db (192.168.161.2)	Nem
DHCP szerver:	1 db (192.168.161.2)	Nem
alaplab.mit.bme.hu:	1 db (192.168.161.2)	Igen

2.8. feladat

Milyen IP és Ethernet címeket használtunk a következő esetekben, és miért?		
	Cél Ethernet cím	Cél IP cím
Alapértelmezett átjáró	Cisco_f4:d4:00 (00:16:9c:f4:d4:00)	152.66.254.254
DHCP szerver	CadmusCo_6e:64:bf (08:00:27:6e:64:bf)	152.66.254.253
alaplab.mit.bme.hu	Cisco_f4:d4:00 (00:16:9c:f4:d4:00)	152.66.252.71
Indoklás: Az alapértelmezett átjárón fogja küldeni, mert ez kívül van a gateway-en.		

2.9. feladat

Hogyan kapcsolódik ez a mérés az előző feladatnál a route print parancsnál megismert kimeneti interfészválasztási megoldáshoz?
A routing táblázatot használja, amely a route print parancs kimenete. Interfészt választ és célcímet.

2.10. feladat

Az Ethernet címek alapján megállapítható az eszköz gyártója. Kik gyártották az egyes eszközöket? Mely eszközök gyártója nem ismerhető meg, és miért?	
	Gyártó
Saját gép	Gigabyte
Alapértelmezett átjáró:	Cisco
DHCP szerver:	Nem tudjuk megmondani, mert nem érhető el.
alaplab.mit.bme.hu	Nem tudjuk megmondani, mert nem érhető el.

2.11. feladat

Milyen címzést használ az ARP a kérdésben és a válaszban, és miért?
Kéréshez: Broadcast, mert mindenkire eljut. Válaszhoz: Unicast, mert csak a kérdezőhöz kell eljutnia.

2.12. feladat * (csak az ötösért)

Ehhez a két feladathoz a Wiresharkkal a fizikai hálózatra kapcsolódó interface-e kell figyelni. Azt a háttérforgalmat vizsgáljuk, amit az előző feladatoknál elkerültünk a virtuális hálózat használatával.

Milyen egyéb háttérforgalmat tapasztal a fizikai hálózaton? Ez miből származik?
Milyen protokoll az elsősorban háttérforgalomként megjelenő STP?
STP:
Milyen protokoll az elsősorban háttérforgalomként megjelenő LLDP?
LLDP:
Milyen protokoll az elsősorban háttérforgalomként megjelenő SSDP?
SSDP:

2.13. Forgalomrögzítés capture filterrel * (csak az ötösért)

A forgalom jellemzőinek megfigyelése alapján konstruáljon capture filtert a zavaró SSDP és STP forgalom kiszűrésére!
Ping: ... – cmd ablak képernyőképe
<<cmd képernyőábra>>
Ping: ... – Wireshark forgalomrögzítés képernyőképe capture filterrel
<<Wireshark képernyőábra>>

3. feladat: A DNS működése

A feladat célja: a DNS működés alapjainak megismerése az **nslookup** program segítségével.

A kéréseket továbbra is a virtuális gépen adjuk ki, és a gazdagép megfelelő virtuális interface-ét figyeljük.

A mérés során csupán a domain névhez tartozó IP címet vagy egy adott IP címhez tartozó domain nevet határozzunk meg az nslookup program segítségével.

Az nslookup futtatása előtt az előző méréshez hasonlóan törölje az ARP és DNS cache-t! Ennek a gyorsítására írjon batch file-et (mynslookup.bat)!

3.1. Batch fájl készítése: mynslookup

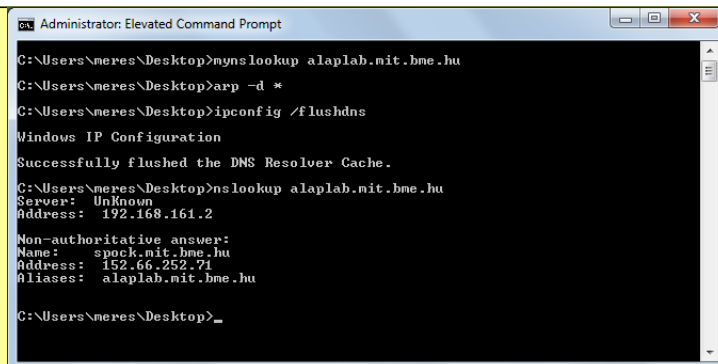
Adja meg a gyorsítótárak törlését, majd az **nslookup** meghívását elvégző batch fájl tartalmát!

```
arp -d *
ipconfig /flushdns
nslookup %1
```

3.2. IP cím meghatározása domain név alapján 1.

Kérdezze le az alaplab.mit.bme.hu IP-címét a következő módon:

mynslookup alaplab.mit.bme.hu



```
Administrator: Elevated Command Prompt

C:\Users\neres\Desktop>mynslookup alaplab.mit.bme.hu
C:\Users\neres\Desktop>arp -d *
C:\Users\neres\Desktop>ipconfig /flushdns
Windows IP Configuration

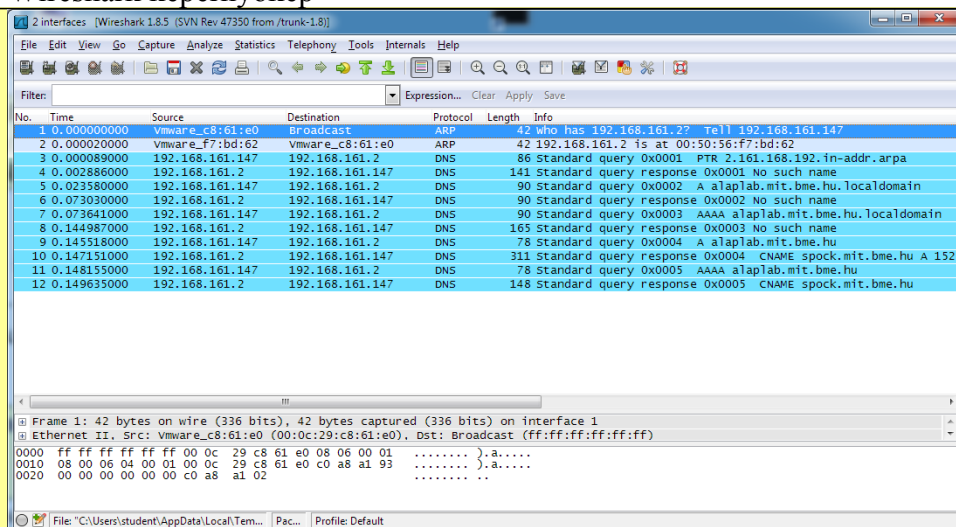
Successfully flushed the DNS Resolver Cache.

C:\Users\neres\Desktop>nslookup alaplab.mit.bme.hu
Server:      Unknown
Address:     192.168.161.2

Non-authoritative answer:
Name:       spock.mit.bme.hu
Address:    152.66.252.71
Aliases:    alaplab.mit.bme.hu

C:\Users\neres\Desktop>_
```

Wireshark képernyőkép



3.3. IP cím meghatározása domain név alapján 2.

Kérdezze le az alaplab.mit.bme.hu IP-címét a következő módon (ponttal a végén!):

mynslookup alaplab.mit.bme.hu.

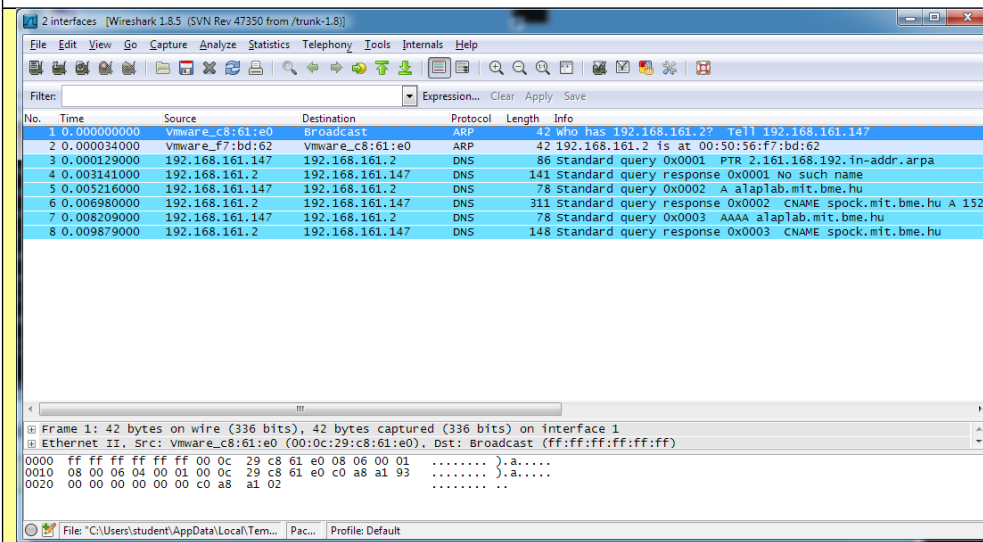
```
Administrator: Elevated Command Prompt
Address: 152.66.252.71
Aliases: alaplab.mit.bme.hu

C:\Users\neres\Desktop>mynslookup alaplab.mit.bme.hu.
C:\Users\neres\Desktop>arp -d *
C:\Users\neres\Desktop>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\neres\Desktop>nslookup alaplab.mit.bme.hu.
Server: Unknown
Address: 192.168.161.2

Non-authoritative answer:
Name: spock.mit.bme.hu
Address: 152.66.252.71
Aliases: alaplab.mit.bme.hu

C:\Users\neres\Desktop>
```

Wireshark képernyőkép



3.4. IP cím meghatározása domain név alapján: összehasonlítás

Mi a különbség a pont nélküli és a ponttal végződő lekérdezés között?

FQDN ponttal a végén és az ő IP címét kéri le. Pont nélkül DNS Suffix felhasználásával egészíti ki a címet.

3.5. Reverse lookup: domain név meghatározása IP cím alapján

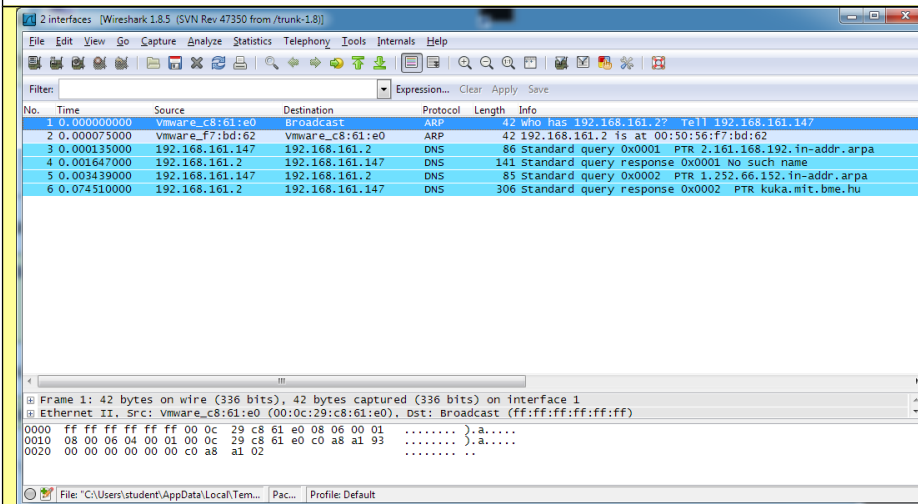
Tudja meg a 152.66.252.1 IP című gép domain nevét (reverse lookup)!

```

Administrator: Elevated Command Prompt
C:\Users\neres\Desktop>nbslookup 152.66.252.1
C:\Users\neres\Desktop>arp -d *
C:\Users\neres\Desktop>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\neres\Desktop>nbslookup 152.66.252.1
Server: Unknown
Address: 192.168.161.2
Name: kuka.mit.bme.hu
Address: 152.66.252.1
C:\Users\neres\Desktop>_

```

Wireshark képernyőábra



3.6. A DNS működésének vizsgálata

Elemezze a Wireshark programmal a tapasztalt forgalmat az alábbiak szerint!

a) Hogyan történik meg az IP cím beállításokban megadott DNS Suffix Search List: **mit.bme.hu** beállítás felhasználása?

A DNS suffix-xal egészíti ki a megadott címet.

b) Milyen alacsonyabb szintű protokollokat használ a DNS, és hogyan?

UDP, IP, Ethernet

c) Hogyan történik az IP címek reprezentálása a DNS-ben reverse lookup esetén? Mi az IP cím mezőinek sorrendje, és miért?

Balról jobbra egyre szűkebb tartományt reprezentál, balról kezd.

d) Mit jelent a Time-To-Live paraméter a válaszban? Hogyan használják ezt fel?

(**Figyelem:** ez kérdés a DNS kérdésben visszaadott TTL-re vonatkozik, és nem az IP csomag TTL-jére!)

A DNS gyorstár kezeléséhez kell a TTL. Amikor a TTL=0 a DNS szerver frissíti a rekordot.

A TTL értékéből debugolni lehet egy sikertelen elérés esetén.

e) Mi történik, ha egy adott domain névhez rendelt IP címet megváltoztattunk? Ki fogja elérni a

kérdéses gépet, és ki fog a régi IP című géphez fordulni?

A DNS szervereknek frissíteniük kell a táblájukat, hogy benne legyen az új IP. Ahol ez még nem történt meg vagy cacheben van a régi cím és nem frissítette, ott a régi IP címen fogják keresni.

3.7. feladat* (csak az ötösért)

Kérdezze le a **www.cnn.com** IP címét **nslookup**-pal!

<<cmd képernyőábra>>

<<Wireshark képernyőábra>>

Ismételje meg a **www.cnn.com** IP címének lekérdezését!

<<cmd képernyőábra>>

Wireshark képernyőábra

<<Wireshark képernyőábra>>

Hasonlítsa össze a kapott IP címeket! Mit tapasztalt? Miért hasznos a látott viselkedés? Vajon milyen két funkció ötvözésére használja ezt a CNN?

4. feladat: IP csomagok továbbításának útvonala

A feladat célja: útvonal-felderítés és nyomkövetés a **tracert** program segítségével.

Ezt a feladatot már a **fizikai gépen** végezze! Ügyeljen arra, hogy megfelelő hálózati interface-t figyeljen. Számítson a többi mérőpár forgalmának megjelenésére, használjon megjelenítési szűrőt.

A tracert egy olyan hálózati tesztprogram, amely a paraméterként megadott IP című vagy domain nevű gép és a tesztprogramot futtató gép között kísérletet tesz a köztes útvonalválasztók (routerek) meghatározására. (UNIX környezetben a traceroute vagy a tracepath látja el ugyanezt a feladatot. Tulajdonképpen ezek mintájára készült a tracert). A tracert futtatása előtt, az előző méréshez hasonlóan, törölje az ARP és DNS cache-t. Ennek a gyorsítására írjon batch file-et!

4.1. Batch fájl szerkesztése

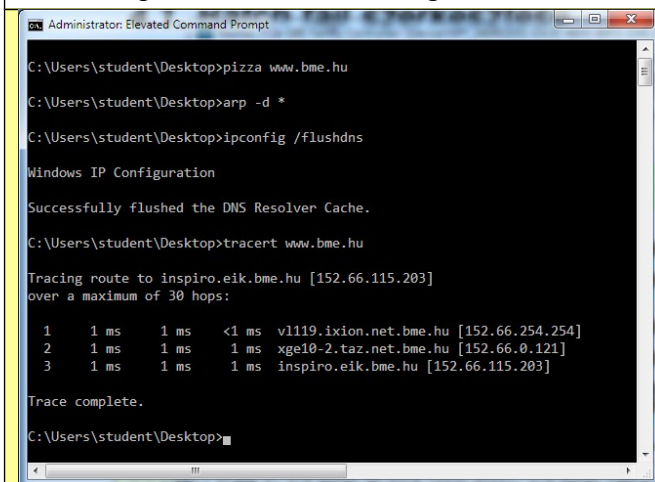
Készítsen egy batch fájlt, amely törli az ARP és DNS cache-t és kiadja a **tracert** parancsot!

Másolja ide a fájl tartalmát!

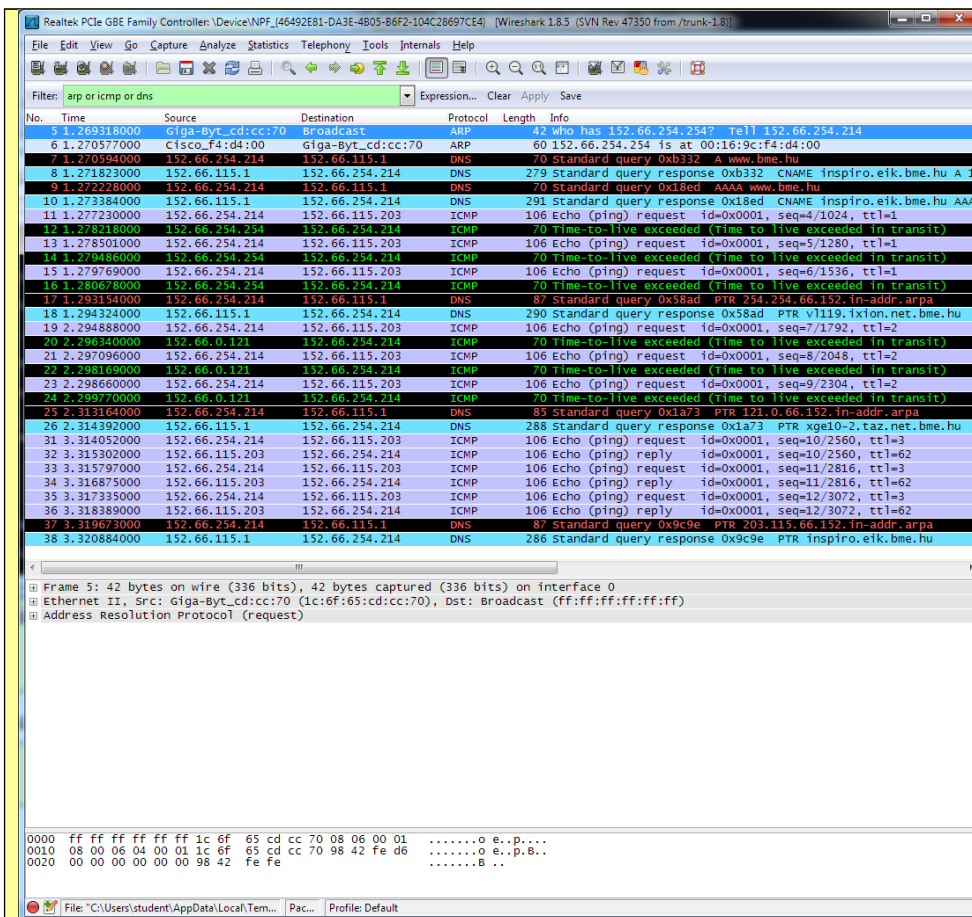
```
arp -d *  
ipconfig /flushdns  
tracert %1
```

4.2. Nyomkövetés egy serverig

A tracert paranccsal szólítsa meg a **www.bme.hu** szerveret!



```
Administrator: Elevated Command Prompt  
C:\Users\student\Desktop>ping www.bme.hu  
C:\Users\student\Desktop>arp -d *  
C:\Users\student\Desktop>ipconfig /flushdns  
Windows IP Configuration  
Successfully flushed the DNS Resolver Cache.  
C:\Users\student\Desktop>tracert www.bme.hu  
Tracing route to inspiro.eik.bme.hu [152.66.115.203]  
over a maximum of 30 hops:  
  0  1 ms    1 ms    <1 ms  vl119.ixion.net.bme.hu [152.66.254.254]  
  1  1 ms    1 ms    1 ms  xge10-2.taz.net.bme.hu [152.66.0.121]  
  2  1 ms    1 ms    1 ms  inspiro.eik.bme.hu [152.66.115.203]  
Trace complete.  
C:\Users\student\Desktop>
```

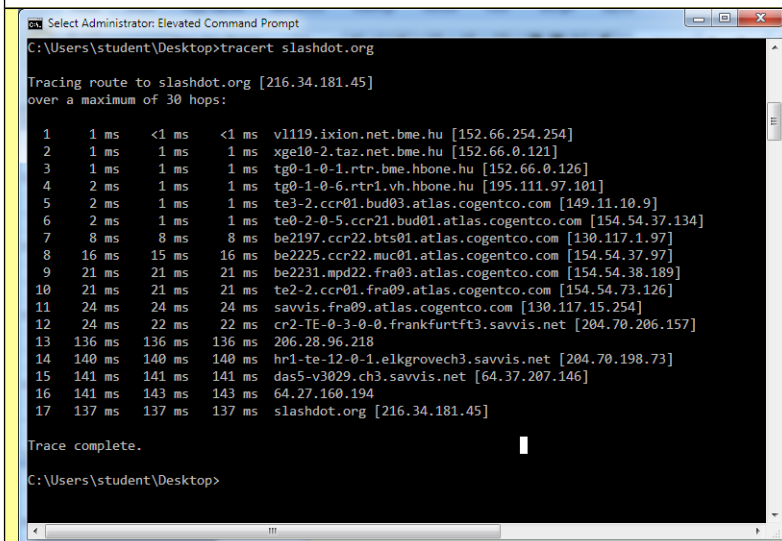


Elemezze a rögzített hálózati forgalmat.

TTL=1,2,... ICMP csomagokkal kapjuk meg a pontokat, amelyeken átmegy a csomag.

4.3. Nyomkövetés egy külföldi szerverig 1.

A **tracert** paranccsal szolgáltson meg egy külföldi, lehetőleg tengerentúli (nagyszámú köztes útvonalválasztón keresztül elérhető) szerver! (Pl.: slashdot.org)



The top screenshot shows a list of captured packets in Wireshark. The filter is set to 'arp or icmp or dns'. The packet list shows various protocols including ARP, DNS, and ICMP. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol, and Hypertext Transfer Protocol.

The bottom screenshot shows a detailed view of a packet, highlighting the Ethernet II, Internet Protocol, and Hypertext Transfer Protocol layers. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol, and Hypertext Transfer Protocol.

Elemezze a rögzített hálózati forgalmat!

A nagyobb válaszidő jelzi, hogy távoli a link. Hosszabb utat tesz meg egy csomag.

4.4. Nyomkövetés egy külföldi szerverig 2.

A **tracert** paranccsal szőlíson meg egy külföldi, lehetőleg tengerentúli (nagyszámú köztes útvonalválasztón keresztül elérhető) szervert! (Pl.: cnn.com)

```
Select Administrator: Elevated Command Prompt

C:\Users\student\Desktop>pizza cnn.com

C:\Users\student\Desktop>arp -d *

C:\Users\student\Desktop>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\student\Desktop>tracert cnn.com

Tracing route to cnn.com [157.166.226.26]
over a maximum of 30 hops:

  1  1 ms  1 ms  1 ms  v1119.ixion.net.bme.hu [152.66.254.254]
  2  1 ms  1 ms  1 ms  xge10-2.taz.net.bme.hu [152.66.0.121]
  3  1 ms  1 ms  1 ms  tg0-1-0-1.rtr.bme.hbone.hu [152.66.0.126]
  4  18 ms 16 ms 14 ms  tg0-1-0-6.rtr1.vh.hbone.hu [195.111.97.101]
  5  1 ms  1 ms  1 ms  te3-2.ccr01.bud03.atlas.cogentco.com [149.11.10.9]
  6  2 ms  1 ms  1 ms  te0-4-0-5.ccr21.bud01.atlas.cogentco.com [154.54.37.138]
  7  8 ms  8 ms  8 ms  be2196.ccr21.bts01.atlas.cogentco.com [130.117.1.37]
  8  16 ms 16 ms 16 ms  be2224.ccr21.muc01.atlas.cogentco.com [154.54.36.9]
  9  21 ms 21 ms 21 ms  be2228.ccr21.fra03.atlas.cogentco.com [154.54.38.49]
 10  28 ms 28 ms 28 ms  be2261.ccr21.ams03.atlas.cogentco.com [154.54.37.29]
 11  35 ms 35 ms 35 ms  be2275.ccr21.lon13.atlas.cogentco.com [130.117.51.253]
 12 107 ms 108 ms 108 ms  be2347.ccr21.jfk02.atlas.cogentco.com [154.54.27.141]
 13 108 ms 108 ms 107 ms  be2060.ccr21.jfk05.atlas.cogentco.com [154.54.31.10]
 14 107 ms 107 ms 107 ms  xo.jfk05.atlas.cogentco.com [154.54.11.190]
 15 130 ms 132 ms 131 ms  207.88.14.185.ptr.us.xo.net [207.88.14.185]
 16 129 ms 129 ms 129 ms  ael10.cir1.atlanta6-ga.us.xo.net [207.88.13.161]
 17 * * * Request timed out.
 18 * * * Request timed out.
 19 * * * Request timed out.
 20 * * * Request timed out.
 21 * * * Request timed out.
 22 * * * Request timed out.
 23 * * * Request timed out.
 24 * * * Request timed out.
 25 * * * Request timed out.
 26 * * * Request timed out.
 27 * * * Request timed out.
 28 * * * Request timed out.
 29 * * * Request timed out.
 30 * * * Request timed out.

Trace complete.

C:\Users\student\Desktop>
```

Realtek PCIe GBE Family Controller: \Device\NPF_{46492E81-DA3E-4B05-86F2-104C28697CE4} [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.012491000	Giga-Byt.cd:cc:70	BroadCast	ARP	60	Who has 152.66.254.254? Tell 152.66.254.214
4	0.913760000	Cisco.F4:d4:10:0	Giga-Byt.cd:cc:70	ARP	60	152.66.254.254 is at 00:16:9c:f4:d4:00
5	0.913777000	152.66.254.214	152.66.115.1	DNS	67	Standard query 0x0da6 A cnn.com
6	0.952719000	152.66.115.1	152.66.254.214	DNS	260	Standard query response 0x0da6 A 157.166.226.26 A 157.166.226.25
7	0.953206000	152.66.254.214	152.66.115.1	DNS	67	Standard query 0x8d05 AAAA cnn.com
8	0.954377000	152.66.115.1	152.66.254.214	DNS	139	Standard query response 0x8d05
9	0.959420000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=1
10	0.960449000	152.66.254.214	152.66.254.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
11	0.960851000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=1
12	0.961844000	152.66.254.214	152.66.254.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
13	0.962214000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=1
14	0.962306000	152.66.254.214	152.66.254.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
15	0.964218000	152.66.254.214	152.66.115.1	DNS	87	Standard query 0x2d2b PTR 254.254.66.152.in-addr.arpa
16	0.965336000	152.66.115.1	152.66.254.214	DNS	290	Standard query response 0x2d2b PTR v1119.ixion.net.bme.hu
17	1.965037000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=2
18	1.965686000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=69/17664, ttl=2
19	1.966854000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=70/17920, ttl=2
20	1.967973000	152.66.115.1	152.66.254.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
21	1.968388000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=71/18176, ttl=2
22	1.969566000	152.66.115.1	152.66.254.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	1.970529000	152.66.254.214	152.66.115.1	DNS	88	Standard query 0x4f2b PTR 126.0.66.152.in-addr.arpa
24	1.971147000	152.66.115.1	152.66.254.214	DNS	288	Standard query response 0x4f2b PTR xge10-2.taz.net.bme.hu
25	2.972071000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=72/18432, ttl=3
26	2.973815000	152.66.115.1	152.66.254.214	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
27	2.974507000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=73/18688, ttl=3
28	2.974507000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=74/18944, ttl=4
29	2.976399000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=75/19200, ttl=4
30	2.977870000	152.66.115.1	152.66.254.214	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
31	2.978736000	152.66.254.214	152.66.115.1	DNS	85	Standard query 0xa6de PTR 126.0.66.152.in-addr.arpa
32	2.979875000	152.66.115.1	152.66.254.214	DNS	296	Standard query response 0xa6de PTR tg0-1-0-1.rtr.bme.hbone.hu
33	3.980060000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=76/19456, ttl=4
34	3.980854000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=77/19712, ttl=4
35	3.999453000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=78/20000, ttl=4
36	4.015593000	195.111.97.101	152.66.254.214	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
37	4.016293000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=79/20256, ttl=4
38	4.020749000	195.111.97.101	152.66.254.214	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
40	4.031693000	152.66.254.214	152.66.115.1	DNS	87	Standard query 0x2f59 PTR 101.92.111.195.in-addr.arpa
41	4.038741000	152.66.115.1	152.66.254.214	DNS	324	Standard query response 0x2f59 PTR tg0-1-0-6.rtr1.vh.hbone.hu
42	5.026118000	152.66.254.214	157.166.226.26	ICMP	106	Echo (ping) request id=0x0001, seq=77/19712, ttl=5
43	5.027707000	149.11.10.9	152.66.254.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Giga-Byt.cd:cc:70 (1c:6f:65:cd:cc:70), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 1c 6f 65 cd cc 70 08 06 00 01o e..p...
0010 08 00 06 04 00 01 1c 6f 65 cd cc 70 98 42 fe d6o e..p.B..
0020 00 00 00 00 00 00 98 42 fe feB ..

File: C:\Users\student\AppData\Local\Temp... Packets: 731 Displayed: 348 M... Profile: Default

Wireshark packet capture showing network traffic. The packet list on the left shows various protocols including LLMNR, ICMP, and ARP. The packet details pane on the right shows the structure of a selected packet, including Ethernet II, Internet Protocol, and Address Resolution Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Elemesse a rögzített hálózati forgalmat!

Blokkolták a kérést, mert a 17. hoptól nem tudja feloldani a címeket.

4.5. A *tracert* működése

Hogyan működik a *tracert* parancs, hogyan határozza meg a köztes útvonalválasztókat? Milyen protokollokat használ, és hogyan?

Egyre nagyobb TTL értékű ICMP csomagokkal deríti fel a hálózatot. Közben ARP segítségével végez címfeloldást.

4.6. feladat * (csak az ötösért)

Mi történik, ha a *tracert* paranccsal megszólított gép ki van kapcsolva vagy a rajta konfigurált tűzfal tiltja a program által küldött csomagokra történő választ? Produkálja a jelenséget!

<<cmd képernyőábra>>

<<Wireshark képernyőábra>>

Magyarázat:

5. feladat: TCP adatfolyamok vizsgálata a netstat programmal

A feladat célja: TCP adatfolyamok vizsgálata a **netstat** és a Wireshark programmal.

Ez a mérés akár a virtuális, akár a fizikai gépen is elvégezhető. Ügyeljen arra, hogy megfelelő hálózati interface-t figyeljen.

A mérés során egy webböngészővel le kell tölteni egy honlapot, és az így kialakuló forgalmat kell vizsgálni a megfelelő időközökben futtatott a **netstat** programmal. A webböngészők a letöltött tartalmat cache-elik. A cache és a HTTP protokoll vizsgálata a következő laborfoglalkozás témája lesz, most csupán azt kell elérni, hogy a teljes weblap letöltődjön.

A mérés során az alábbi részfeladatokat kell elvégezni:

- Futtassa le a **netstat-a** parancsot! A kimenetet tárolja el egy file-ba (pl. netstat_pre.txt)!
- Indítsa le a webböngészőt, és törölje a böngésző cache-ét!
- Törölje az ARP és DNS cache-t!
- Indítsa el a forgalomrögzítést!
- Töltse le a **www.bme.hu** weblapot!
- Futtassa le a **netstat-a** parancsot! A kimenetet tárolja el egy file-ba (pl. netstat_web.txt)!
- Lépjen ki a böngészőből!
- Futtassa le a **netstat-a** parancsot, a kimenetet tárolja el egy file-ba (pl. netstat_post.txt)!
- Állítsa le a forgalomrögzítést!

5.1. feladat: „pre”

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	alabi14:0	LISTENING
TCP	0.0.0.0:445	alabi14:0	LISTENING
TCP	0.0.0.0:902	alabi14:0	LISTENING
TCP	0.0.0.0:912	alabi14:0	LISTENING
TCP	0.0.0.0:49152	alabi14:0	LISTENING
TCP	0.0.0.0:49153	alabi14:0	LISTENING
TCP	0.0.0.0:49154	alabi14:0	LISTENING
TCP	0.0.0.0:49156	alabi14:0	LISTENING
TCP	0.0.0.0:49170	alabi14:0	LISTENING
TCP	127.0.0.1:12080	alabi14:0	LISTENING
TCP	127.0.0.1:27275	alabi14:0	LISTENING
TCP	127.0.0.1:49323	alabi14:49324	ESTABLISHED
TCP	127.0.0.1:49324	alabi14:49323	ESTABLISHED
TCP	127.0.0.1:49325	alabi14:49326	ESTABLISHED
TCP	127.0.0.1:49326	alabi14:49325	ESTABLISHED
TCP	152.66.254.214:139	alabi14:0	LISTENING
TCP	152.66.254.214:49158	r-052-042-234-077:http	ESTABLISHED
TCP	152.66.254.214:49247	a345vg:https	CLOSE_WAIT
TCP	152.66.254.214:49248	fra07s31-in-f30:https	CLOSE_WAIT
TCP	152.66.254.214:49249	fra07s31-in-f30:https	CLOSE_WAIT
TCP	152.66.254.214:49250	a92-123-150-13:https	CLOSE_WAIT
TCP	152.66.254.214:49251	a92-123-150-13:https	CLOSE_WAIT
TCP	152.66.254.214:49277	fileshare.microsoft-ds	ESTABLISHED
TCP	192.168.161.1:139	alabi14:0	LISTENING
TCP	192.168.241.1:139	alabi14:0	LISTENING
TCP	:::135	alabi14:0	LISTENING
TCP	:::445	alabi14:0	LISTENING
TCP	:::49152	alabi14:0	LISTENING
TCP	:::49153	alabi14:0	LISTENING
TCP	:::49154	alabi14:0	LISTENING
TCP	:::49156	alabi14:0	LISTENING
TCP	:::49170	alabi14:0	LISTENING
UDP	0.0.0.0:5355	.*.*	

```

UDP 127.0.0.1:1900 *.*
UDP 127.0.0.1:52836 *.*
UDP 152.66.254.214:137 *.*
UDP 152.66.254.214:138 *.*
UDP 152.66.254.214:1900 *.*
UDP 152.66.254.214:52835 *.*
UDP 192.168.161.1:137 *.*
UDP 192.168.161.1:138 *.*
UDP 192.168.161.1:1900 *.*
UDP 192.168.241.1:137 *.*
UDP 192.168.241.1:138 *.*
UDP 192.168.241.1:1900 *.*
UDP [::]:5355 *.*
UDP [::1]:1900 *.*
UDP [::1]:52834 *.*
UDP [fe80::283c:5163:e772:ed42%17]:546 *.*
UDP [fe80::283c:5163:e772:ed42%17]:1900 *.*
UDP [fe80::2961:5c10:eb86:427%15]:546 *.*
UDP [fe80::2961:5c10:eb86:427%15]:1900 *.*
UDP [fe80::e4ce:9cba:1115:c2a0%10]:546 *.*
UDP [fe80::e4ce:9cba:1115:c2a0%10]:1900 *.*
UDP [fe80::e4ce:9cba:1115:c2a0%10]:52833 *.*

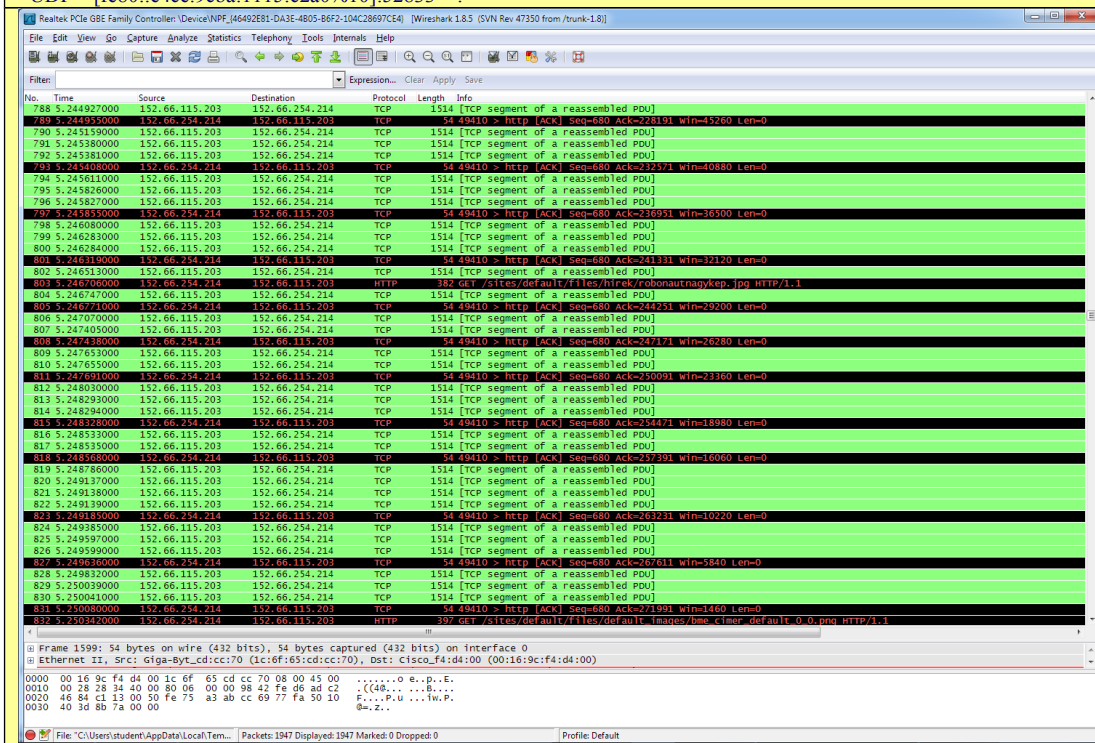
```

5.2. feladat: „web”

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	alabi14:0	LISTENING
TCP	0.0.0.0:445	alabi14:0	LISTENING
TCP	0.0.0.0:902	alabi14:0	LISTENING
TCP	0.0.0.0:912	alabi14:0	LISTENING
TCP	0.0.0.0:49152	alabi14:0	LISTENING
TCP	0.0.0.0:49153	alabi14:0	LISTENING
TCP	0.0.0.0:49154	alabi14:0	LISTENING
TCP	0.0.0.0:49156	alabi14:0	LISTENING
TCP	0.0.0.0:49170	alabi14:0	LISTENING
TCP	127.0.0.1:12080	alabi14:0	LISTENING
TCP	127.0.0.1:12080	alabi14:49405	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49407	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49408	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49409	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49411	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49412	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49417	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49418	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49422	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49423	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49424	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49426	ESTABLISHED
TCP	127.0.0.1:12080	alabi14:49429	ESTABLISHED
TCP	127.0.0.1:27275	alabi14:0	LISTENING
TCP	127.0.0.1:49323	alabi14:49324	ESTABLISHED
TCP	127.0.0.1:49324	alabi14:49323	ESTABLISHED
TCP	127.0.0.1:49325	alabi14:49326	ESTABLISHED
TCP	127.0.0.1:49326	alabi14:49325	ESTABLISHED
TCP	127.0.0.1:49374	alabi14:49375	ESTABLISHED
TCP	127.0.0.1:49375	alabi14:49374	ESTABLISHED
TCP	127.0.0.1:49405	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49407	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49408	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49409	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49411	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49412	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49417	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49418	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49422	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49423	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49424	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49426	alabi14:12080	ESTABLISHED
TCP	127.0.0.1:49429	alabi14:12080	ESTABLISHED
TCP	152.66.254.214:139	alabi14:0	LISTENING
TCP	152.66.254.214:49158	r-052-042-234-077:http	ESTABLISHED
TCP	152.66.254.214:49247	a345vg:https	CLOSE_WAIT
TCP	152.66.254.214:49248	fra07s31-in-f30:https	CLOSE_WAIT
TCP	152.66.254.214:49249	fra07s31-in-f30:https	CLOSE_WAIT

```
TCP 152.66.254.214:49250 a92-123-150-13:https CLOSE_WAIT
TCP 152.66.254.214:49251 a92-123-150-13:https CLOSE_WAIT
TCP 152.66.254.214:49277 fileshare:microsoft-ds ESTABLISHED
TCP 152.66.254.214:49394 fa-in-f101:http TIME_WAIT
TCP 152.66.254.214:49395 fa-in-f101:http TIME_WAIT
TCP 152.66.254.214:49406 inspiro:http ESTABLISHED
TCP 152.66.254.214:49410 inspiro:http ESTABLISHED
TCP 152.66.254.214:49413 inspiro:http ESTABLISHED
TCP 152.66.254.214:49414 inspiro:http ESTABLISHED
TCP 152.66.254.214:49415 inspiro:http ESTABLISHED
TCP 152.66.254.214:49416 inspiro:http ESTABLISHED
TCP 152.66.254.214:49419 fa-in-f95:http ESTABLISHED
TCP 152.66.254.214:49420 fa-in-f95:http ESTABLISHED
TCP 152.66.254.214:49425 fa-in-f132:http ESTABLISHED
TCP 152.66.254.214:49427 fa-in-f132:http ESTABLISHED
TCP 152.66.254.214:49428 fa-in-f132:http ESTABLISHED
TCP 152.66.254.214:49430 fa-in-f132:http ESTABLISHED
TCP 152.66.254.214:49431 fa-in-f132:http ESTABLISHED
TCP 192.168.161.1:139 alabi14:0 LISTENING
TCP 192.168.241.1:139 alabi14:0 LISTENING
TCP [::]:135 alabi14:0 LISTENING
TCP [::]:445 alabi14:0 LISTENING
TCP [::]:49152 alabi14:0 LISTENING
TCP [::]:49153 alabi14:0 LISTENING
TCP [::]:49154 alabi14:0 LISTENING
TCP [::]:49156 alabi14:0 LISTENING
TCP [::]:49170 alabi14:0 LISTENING
UDP 0.0.0.0:5355 *.*
UDP 127.0.0.1:1900 *.*
UDP 127.0.0.1:52836 *.*
UDP 152.66.254.214:137 *.*
UDP 152.66.254.214:138 *.*
UDP 152.66.254.214:1900 *.*
UDP 152.66.254.214:52835 *.*
UDP 192.168.161.1:137 *.*
UDP 192.168.161.1:138 *.*
UDP 192.168.161.1:1900 *.*
UDP 192.168.241.1:137 *.*
UDP 192.168.241.1:138 *.*
UDP 192.168.241.1:1900 *.*
UDP [::]:5355 *.*
UDP [::]:1900 *.*
UDP [::]:52834 *.*
UDP [fe80::283c:5163:e772:ed42%17]:1900 *.*
UDP [fe80::2961:5c10:eb86:427%15]:1900 *.*
UDP [fe80::e4ce:9cba:1115:c2a0%10]:1900 *.*
UDP [fe80::e4ce:9cba:1115:c2a0%10]:52833 *.*
```



5.3. feladat: „post”

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	alabi14:0	LISTENING
TCP	0.0.0.0:445	alabi14:0	LISTENING
TCP	0.0.0.0:902	alabi14:0	LISTENING
TCP	0.0.0.0:912	alabi14:0	LISTENING
TCP	0.0.0.0:49152	alabi14:0	LISTENING
TCP	0.0.0.0:49153	alabi14:0	LISTENING
TCP	0.0.0.0:49154	alabi14:0	LISTENING
TCP	0.0.0.0:49156	alabi14:0	LISTENING
TCP	0.0.0.0:49170	alabi14:0	LISTENING
TCP	127.0.0.1:12080	alabi14:0	LISTENING
TCP	127.0.0.1:27275	alabi14:0	LISTENING
TCP	127.0.0.1:49323	alabi14:49324	ESTABLISHED
TCP	127.0.0.1:49324	alabi14:49323	ESTABLISHED
TCP	127.0.0.1:49325	alabi14:49326	ESTABLISHED
TCP	127.0.0.1:49326	alabi14:49325	ESTABLISHED
TCP	127.0.0.1:49375	alabi14:49374	TIME_WAIT
TCP	152.66.254.214:139	alabi14:0	LISTENING
TCP	152.66.254.214:49158	r-052-042-234-077:http	ESTABLISHED
TCP	152.66.254.214:49247	a345vg:https	CLOSE_WAIT
TCP	152.66.254.214:49248	fra07s31-in-f30:https	CLOSE_WAIT
TCP	152.66.254.214:49249	fra07s31-in-f30:https	CLOSE_WAIT
TCP	152.66.254.214:49250	a92-123-150-13:https	CLOSE_WAIT
TCP	152.66.254.214:49251	a92-123-150-13:https	CLOSE_WAIT
TCP	152.66.254.214:49277	fileshare:microsoft-ds	ESTABLISHED
TCP	152.66.254.214:49394	fa-in-f101:http	TIME_WAIT
TCP	152.66.254.214:49395	fa-in-f101:http	TIME_WAIT
TCP	152.66.254.214:49419	fa-in-f95:http	TIME_WAIT
TCP	152.66.254.214:49420	fa-in-f95:http	TIME_WAIT
TCP	152.66.254.214:49425	fa-in-f132:http	TIME_WAIT
TCP	152.66.254.214:49427	fa-in-f132:http	TIME_WAIT
TCP	152.66.254.214:49428	fa-in-f132:http	TIME_WAIT
TCP	152.66.254.214:49430	fa-in-f132:http	TIME_WAIT
TCP	152.66.254.214:49431	fa-in-f132:http	TIME_WAIT
TCP	192.168.161.1:139	alabi14:0	LISTENING
TCP	192.168.241.1:139	alabi14:0	LISTENING
TCP	:::135	alabi14:0	LISTENING
TCP	:::445	alabi14:0	LISTENING
TCP	:::49152	alabi14:0	LISTENING
TCP	:::49153	alabi14:0	LISTENING
TCP	:::49154	alabi14:0	LISTENING
TCP	:::49156	alabi14:0	LISTENING
TCP	:::49170	alabi14:0	LISTENING
UDP	0.0.0.0:5355	.*.*	
UDP	127.0.0.1:1900	.*.*	
UDP	127.0.0.1:52836	.*.*	
UDP	152.66.254.214:137	.*.*	
UDP	152.66.254.214:138	.*.*	
UDP	152.66.254.214:1900	.*.*	
UDP	152.66.254.214:52835	.*.*	
UDP	192.168.161.1:137	.*.*	
UDP	192.168.161.1:138	.*.*	
UDP	192.168.161.1:1900	.*.*	
UDP	192.168.241.1:137	.*.*	
UDP	192.168.241.1:138	.*.*	
UDP	192.168.241.1:1900	.*.*	
UDP	:::5355	.*.*	
UDP	:::1:1900	.*.*	
UDP	:::1:52834	.*.*	
UDP	[fe80::283c:5163:e772:ed42%17]:1900	.*.*	
UDP	[fe80::2961:5c10:eb86:427%15]:1900	.*.*	
UDP	[fe80::e4ce:9cba:1115:c2a0%10]:1900	.*.*	
UDP	[fe80::e4ce:9cba:1115:c2a0%10]:52833	.*.*	

5.4. A letöltéskor használt protokoll azonosítása

Milyen protokollokat használ a webböngésző a tartalom letöltése során, és milyen célból?

HTTP – alkalmazási rétegbeli protokoll, a weblapot leíró adatok érkeznek vele

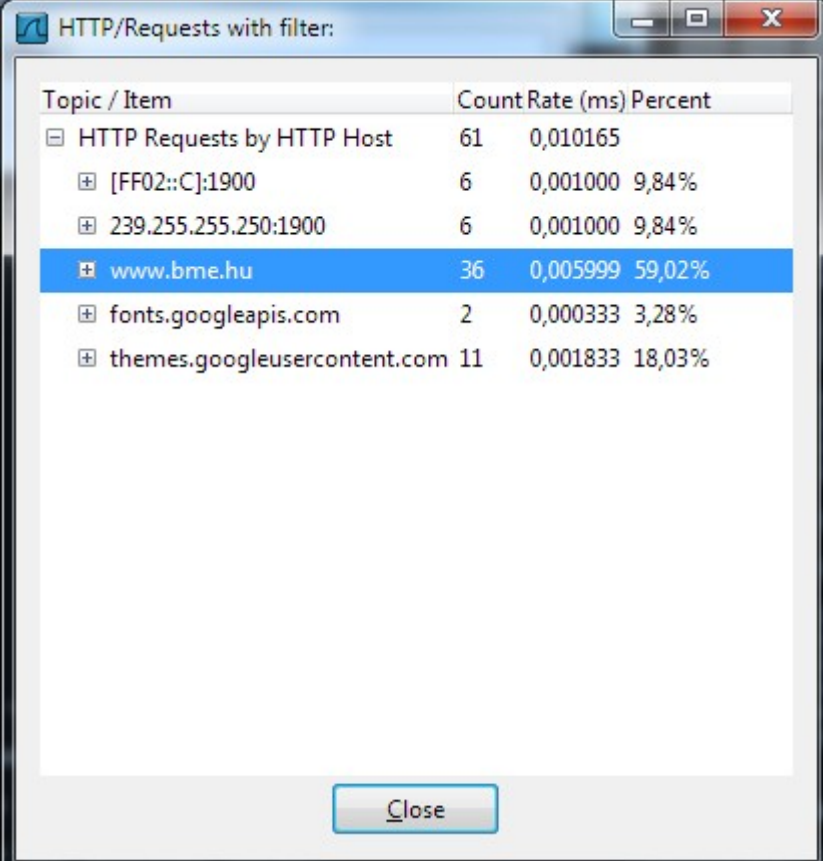
TCP – szállítási rétegbeli protokoll, a weblaphoz kapcsolódó adatok (képek, js) érkeznek rajta

5.5. A TCP folyamat számának meghatározása

A mért forgalom alapján határozza meg, hogy a böngésző hány párhuzamos TCP folyamat nyitott meg a **www.bme.hu** szerverhez!

Indokolja a választ! Használja a megjelenítés/analízis szűrőt és a **netstat** outputját is a feladat megoldásához!

36 darab



Topic / Item	Count	Rate (ms)	Percent
HTTP Requests by HTTP Host	61	0,010165	
[FF02::C]:1900	6	0,001000	9,84%
239.255.255.250:1900	6	0,001000	9,84%
www.bme.hu	36	0,005999	59,02%
fonts.googleapis.com	2	0,000333	3,28%
themes.googleusercontent.com	11	0,001833	18,03%

5.6. Kapcsolatbontás

Hogyan és mikor történik a kapcsolat lebontása?

Készítsen a lebontás megtalálásához megjelenítés/analízis szűrőt, és használja a netstat outputot is!

Realtek PCIe GBE Family Controller: \Device\NPF_{46492E81-DA3E-4B05-B6F2-104C28697CE4} [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

Filter: tcp.flags.fin == 1

No.	Time	Source	Destination	Protocol	Length	Info
2106	22.35215200	152.66.115.203	152.66.254.215	TCP	60	http > 50270 [FIN, ACK] Seq=50975 Ack=3238 win=14464 Len=0
2108	22.35283000	152.66.115.203	152.66.254.215	TCP	60	http > 50277 [FIN, ACK] Seq=175293 Ack=2054 win=11264 Len=0
2110	22.35257500	152.66.115.203	152.66.254.215	TCP	60	http > 50275 [FIN, ACK] Seq=272806 Ack=1646 win=10240 Len=0
2111	22.35260300	152.66.115.203	152.66.254.215	TCP	60	http > 50278 [FIN, ACK] Seq=78652 Ack=3277 win=14464 Len=0
2114	22.36779200	152.66.115.203	152.66.254.215	TCP	60	http > 50279 [FIN, ACK] Seq=245966 Ack=2414 win=12288 Len=0
2116	22.52453400	152.66.115.203	152.66.254.215	TCP	60	http > 50276 [FIN, ACK] Seq=533953 Ack=2032 win=11264 Len=0
2178	38.38955300	152.66.254.215	173.194.70.101	TCP	54	50264 > https [FIN, ACK] Seq=2 Ack=1 win=256 Len=0
2179	38.38988800	152.66.254.215	173.194.70.120	TCP	54	50266 > https [FIN, ACK] Seq=2 Ack=1 win=256 Len=0
2180	38.39038200	152.66.254.215	173.194.70.101	TCP	54	50265 > https [FIN, ACK] Seq=2 Ack=1 win=256 Len=0
2181	38.39095300	152.66.254.215	173.194.70.156	TCP	54	50249 > http [FIN, ACK] Seq=1 Ack=1 win=16148 Len=0
2182	38.39122800	152.66.254.215	173.194.70.95	TCP	54	50283 > http [FIN, ACK] Seq=460 Ack=882 win=64896 Len=0
2183	38.39167500	152.66.254.215	173.194.70.132	TCP	54	50291 > http [FIN, ACK] Seq=865 Ack=75979 win=64592 Len=0
2184	38.39265200	152.66.254.215	152.66.115.203	TCP	54	50276 > http [FIN, ACK] Seq=2032 Ack=533954 win=65104 Len=0
2185	38.39301000	152.66.254.215	152.66.252.13	TCP	54	50220 > http [FIN, ACK] Seq=1 Ack=1 win=16194 Len=0
2186	38.39366100	152.66.254.215	173.194.70.95	TCP	54	50281 > http [FIN, ACK] Seq=413 Ack=666 win=65112 Len=0
2187	38.39384600	152.66.254.215	152.66.252.13	TCP	54	50267 > http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
2190	38.39531900	152.66.254.215	152.66.115.203	TCP	54	50275 > http [FIN, ACK] Seq=1646 Ack=272807 win=65700 Len=0
2191	38.39574900	152.66.254.215	173.194.44.18	TCP	54	50252 > http [FIN, ACK] Seq=1 Ack=1 win=16220 Len=0
2193	38.39732800	152.66.254.215	173.194.70.132	TCP	54	50295 > http [FIN, ACK] Seq=410 Ack=29902 win=65780 Len=0
2194	38.39755000	152.66.254.215	173.194.70.132	TCP	54	50292 > http [FIN, ACK] Seq=865 Ack=76135 win=64576 Len=0
2195	38.39789500	152.66.254.215	173.194.70.132	TCP	54	50293 > http [FIN, ACK] Seq=865 Ack=75767 win=65780 Len=0
2196	38.39847700	152.66.254.215	152.66.115.203	TCP	54	50277 > http [FIN, ACK] Seq=2054 Ack=175294 win=65700 Len=0
2197	38.39867100	152.66.254.215	152.66.115.203	TCP	54	50278 > http [FIN, ACK] Seq=3277 Ack=78653 win=65096 Len=0
2198	38.39888400	152.66.254.215	173.194.70.156	TCP	54	50241 > http [FIN, ACK] Seq=1 Ack=1 win=16270 Len=0
2199	38.39906300	152.66.254.215	173.194.70.132	TCP	54	50294 > http [FIN, ACK] Seq=861 Ack=58151 win=65780 Len=0
2200	38.39925600	152.66.254.215	152.66.115.203	TCP	54	50270 > http [FIN, ACK] Seq=3238 Ack=50976 win=65700 Len=0
2201	38.39944000	152.66.254.215	152.66.115.203	TCP	54	50279 > http [FIN, ACK] Seq=2414 Ack=245967 win=65136 Len=0
2202	38.39977800	152.66.254.215	173.194.70.156	TCP	54	50248 > http [FIN, ACK] Seq=1 Ack=1 win=16445 Len=0
2203	38.39996300	152.66.254.215	173.194.70.132	TCP	54	50290 > http [FIN, ACK] Seq=865 Ack=74999 win=64616 Len=0
2204	38.40017900	152.66.254.215	152.66.252.13	TCP	54	50218 > http [FIN, ACK] Seq=1 Ack=1 win=16230 Len=0
2209	38.40074700	152.66.254.215	152.66.252.13	TCP	54	50221 > http [FIN, ACK] Seq=1 Ack=1 win=16138 Len=0
2210	38.40103100	152.66.254.215	152.66.252.13	TCP	54	50217 > http [FIN, ACK] Seq=1 Ack=1 win=16069 Len=0
2211	38.40121600	152.66.254.215	152.66.252.13	TCP	54	50213 > http [FIN, ACK] Seq=1 Ack=1 win=16425 Len=0
2212	38.40140500	152.66.254.215	173.194.70.156	TCP	54	50246 > http [FIN, ACK] Seq=1 Ack=1 win=16177 Len=0
2213	38.40218900	152.66.254.215	173.194.70.113	TCP	54	50227 > http [FIN, ACK] Seq=1 Ack=1 win=16155 Len=0
2214	38.40236500	152.66.254.215	173.194.44.18	TCP	54	50255 > http [FIN, ACK] Seq=1 Ack=1 win=16220 Len=0
2215	38.40267700	152.66.254.215	173.194.70.120	TCP	54	50254 > http [FIN, ACK] Seq=1 Ack=1 win=16177 Len=0
2216	38.40594200	173.194.70.101	152.66.254.215	TCP	60	https > 50264 [FIN, ACK] Seq=1 Ack=3 win=661 Len=0
2218	38.40659500	173.194.70.120	152.66.254.215	TCP	60	https > 50266 [FIN, ACK] Seq=1 Ack=3 win=661 Len=0
2220	38.40697100	152.66.254.215	173.194.70.138	TCP	54	50214 > http [FIN, ACK] Seq=2 Ack=1 win=252 Len=0
2221	38.40736600	173.194.70.101	152.66.254.215	TCP	60	https > 50265 [FIN, ACK] Seq=1 Ack=3 win=662 Len=0

Frame 2114: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Cisco_F4:d4:00 (00:16:9c:f4:d4:00), Dst: Giga-Byt_cd:5d:c1 (1c:6f:65:cd:5d:c1)
 Internet Protocol Version 4, Src: 152.66.115.203 (152.66.115.203), Dst: 152.66.254.215 (152.66.254.215)
 Transmission Control Protocol, Src Port: http (80), Dst Port: http (80), Seq: 50279 (50279), Seq: 245966, Ack: 2414, Len: 0

0000 1c 6f 65 cd 5d c1 00 16 9c f4 d4 00 08 00 45 00 .oe.]... ..E.
 0010 00 28 0d 54 40 00 3e 06 8c 54 98 42 73 cd 98 42 (.T8>. .T.Bs..B
 0020 fe d7 00 50 c4 67 4f 89 23 d1 75 4b e2 72 50 11 :P.go. #.UK.rP.
 0030 00 60 7c 7b 00 00 00 00 00 00 00 00 00 00 00 00 .{.....

File: "C:\Users\student\AppData\Local\Temp\... Packets: 2349 Displayed: 87 M... Profile: Default

5.7. TCP folyam tulajdonságai

Szűrjük ki az egyik rövidebb (~10-15 üzenetből álló) TCP folyamhoz tartozó csomagokat (jobb gomb az egyik csomagon, majd *Conversation Filter / TCP*).

Realtek PCIe GBE Family Controller: \Device\NPF_{46492E81-DA3E-4B05-B6F2-104C28697CE4} [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

Filter: (ip.addr eq 152.66.254.214 and ip.addr eq 173.194.70.95) and (tcp.port eq 80)

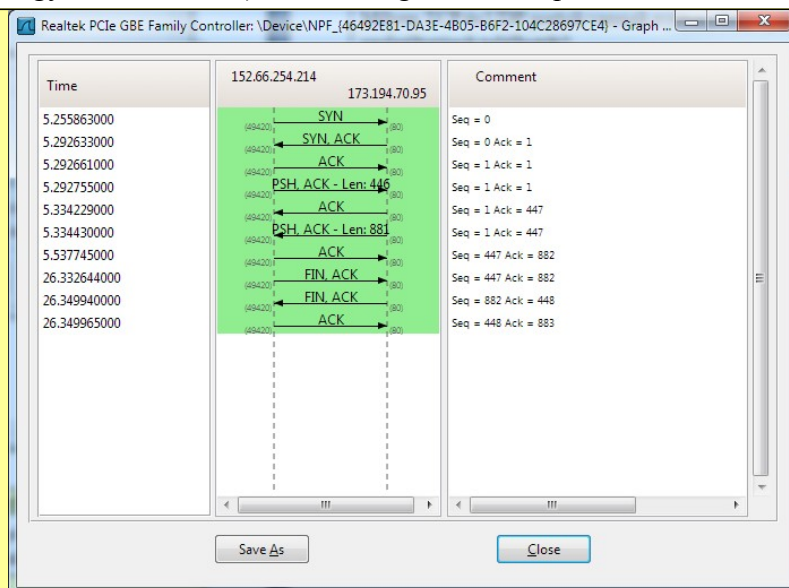
No.	Time	Source	Destination	Protocol	Length	Info
853	5.255863000	152.66.254.214	173.194.70.95	TCP	66	49420 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1064	5.292633000	173.194.70.95	152.66.254.214	TCP	66	http > 49420 [SYN, ACK] Seq=0 Ack=1 win=42900 Len=0 MSS=1430 SACK_PERM=1 WS=64
1065	5.292661000	152.66.254.214	173.194.70.95	TCP	54	49420 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
1066	5.292755000	152.66.254.214	173.194.70.95	HTTP	500	GET /css?family=open+Sans:300italic,400italic,600italic,700italic,700,600,400,300&subset=latin-ext HTTP/1.1
1349	5.334229000	173.194.70.95	152.66.254.214	TCP	60	http > 49420 [ACK] Seq=1 Ack=447 win=42496 Len=0
1351	5.334430000	173.194.70.95	152.66.254.214	HTTP	935	HTTP/1.1 200 OK (text/css)
1501	5.337745000	152.66.254.214	173.194.70.95	TCP	54	49420 > http [ACK] Seq=447 Ack=882 win=64896 Len=0
1913	26.332640000	152.66.254.214	173.194.70.95	TCP	54	49420 > http [FIN, ACK] Seq=447 Ack=882 win=64896 Len=0
1928	26.349040000	173.194.70.95	152.66.254.214	TCP	60	http > 49420 [FIN, ACK] Seq=882 Ack=448 win=42496 Len=0
1930	26.349363000	152.66.254.214	173.194.70.95	TCP	54	49420 > http [ACK] Seq=448 Ack=883 win=64896 Len=0

File: "C:\Users\student\AppData\Local\Temp\... Packets: 1947 Displayed: 10 Marked: 0 Dropped: 0 Profile: Default

Sorrendben érkeztek a csomagok? Hogyan tudja ezt megállapítani?

Sorrendben jöttek. A No. És Time oszlop tanulmányozásával lehet megmondani.

Vizsgálja meg a TCP folyamatban az üzenetküldések menetét (*Statistics / Flow Graph*, és a *TCP flow* legyen kiválasztva)! Mire szolgálnak a Sequence number és Acknowledgment number mezők?

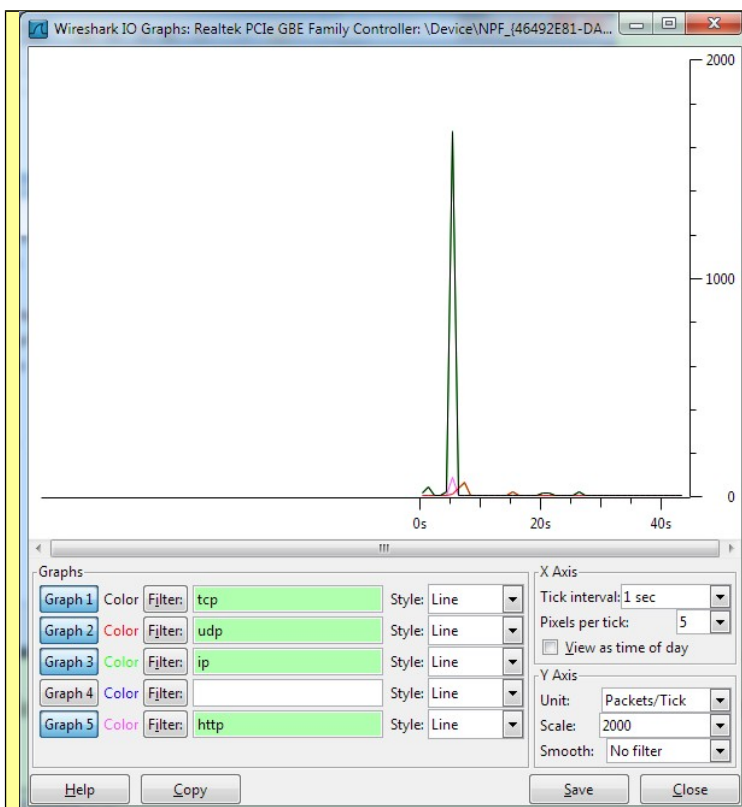


5.8. Protokollok sávszélesség-igénye

Ábrázolja a különböző protokollok által használt sávszélességet (byte/s) és csomaggyakoriságot (packet/s)! Indokolja a látottakat!

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	1947	100,00 %	1677842	0,308	0	0	0,000
Ethernet	100,00 %	1947	100,00 %	1677842	0,308	0	0	0,000
Internet Protocol Version 4	98,66 %	1921	99,83 %	1675067	0,308	0	0	0,000
Transmission Control Protocol	91,88 %	1789	98,70 %	1656004	0,304	1677	1604384	0,295
Secure Sockets Layer	1,28 %	25	0,14 %	2365	0,000	25	2365	0,000
Hypertext Transfer Protocol	4,42 %	86	2,93 %	49195	0,009	43	18265	0,003
Line-based text data	0,41 %	8	0,44 %	7339	0,001	8	7339	0,001
Media Type	0,51 %	10	0,46 %	7649	0,001	10	7649	0,001
Portable Network Graphics	0,87 %	17	0,60 %	10090	0,002	17	10090	0,002
JPEG File Interchange Format	0,41 %	8	0,35 %	5852	0,001	8	5852	0,001
NetBIOS Session Service	0,05 %	1	0,00 %	60	0,000	1	60	0,000
User Datagram Protocol	6,78 %	132	1,14 %	19063	0,004	0	0	0,000
Domain Name Service	6,47 %	126	1,11 %	18607	0,003	126	18607	0,003
NetBIOS Name Service	0,15 %	3	0,02 %	276	0,000	3	276	0,000
Data	0,15 %	3	0,01 %	180	0,000	3	180	0,000
Internet Protocol Version 6	0,77 %	15	0,13 %	2151	0,000	0	0	0,000
User Datagram Protocol	0,77 %	15	0,13 %	2151	0,000	0	0	0,000
DHCPv6	0,67 %	13	0,12 %	1937	0,000	13	1937	0,000
Domain Name Service	0,10 %	2	0,01 %	214	0,000	2	214	0,000
Address Resolution Protocol	0,56 %	11	0,04 %	624	0,000	11	624	0,000

A forgalom lényegében a TCP-n zajlott.



A http kis forgalommal jár.

5.9. Helyi hálózati szolgáltatások azonosítása * (csak az ötösért)

Milyen TCP és UDP portok vannak nyitva a helyi gépen a **netstat** alapján, és azokon milyen szolgáltatások találhatók?