

# **Az internet ökoszisztémája és evolúciója**

## **Gyakorlat 6**

**Internet monitorok, autonóm rendszerek,  
címtartományok, routing információk**

# Információk az Internetről

- Az Internet működésével (és működészavaraival) kapcsolatos információk gyakran nem, vagy csak különböző adatbázisokba szétszórva érhetők el
  - Melyik AS-hez tartozik egy IP címtartomány?
  - Melyik AS melyik másik AS-hez kapcsolódik?
  - Kit értesítsünk, ha spam jön valahonnan?
  - Miért nem érik el a hálózatomat Hong Kongból?
- Nem az a probléma, hogy *mi* a válasz, hanem hogy *megválaszolható-e* a kérdés egyáltalán!

# „Közismert” eszközök

- Kétirányú elérhetőség a lokális és egy távoli hoszt között: `ping`
- Útvonal egy távoli hosztra: `traceroute`
  - TCP SYN csomagok növekvő TTL-lel (1, 2,...)
  - ahol a TTL=0, ICMP Time Exceeded
- Doménnév ↔ IP cím megfeleltetés: `host`, `dig`

```
$ host index.hu
index.hu has address 217.20.130.99
index.hu mail is handled by 10 mail27.indamail.hu.
...
$ host 217.20.130.99
99.130.20.217.in-addr.arpa domain name pointer index.hu.
```

# WHOIS

- Protokoll Internet-erőforrások lekérdezésére:
  - domén nevek
  - IP címtartományok és tulajdonosaik
  - Autonóm Rendszerek azonosítói (AS számok)
- Egyszerű „command line” protokoll
  - **Web:** `https://apps.db.ripe.net/search/query.html`
  - **telnet:** `telnet whois.ripe.net 43`
  - **CLI:** `whois 152.66.244.111`
- Nyílt adatbázisok, szabványos (RPSL) kimenet

# WHOIS: IP prefix lekérdezése

```
$ whois 152.66.244.111
[...]
% Information related to '152.66.0.0 - 152.66.255.255'

% Abuse contact for '152.66.0.0 - 152.66.255.255' is 'abuse@bme.hu'

inetnum:                152.66.0.0 - 152.66.255.255
netname:                 BMENET
descr:                  Budapest University of Technology and Economics
descr:                  Budapesti Muszaki es Gazdasagtudomanyi Egyetem
country:                HU
[...]
% Information related to '152.66.0.0/16AS2547'

route:                  152.66.0.0/16
descr:                 BMENET
org:                   ORG-BME1-RIPE
origin:                AS2547
mnt-by:                AS2547-MNT
source:                RIPE # Filtered
[...]
organisation:          ORG-BME1-RIPE
org-name:              BME
```

# WHOIS: fontos RPSL objektumok

- `inetnum`: információk egy prefixről (`netname`, `country`, `org`, `admin`)
  - `152.66.0.0 - 152.66.255.255`
- `organization`: egy szervezet neve, erre hivatkozik az `inetnum` tulajdonosként (`org`):
  - `ORG-BME1-RIPE`
- `person`: adminisztrátor leírása (`address`,...)
- `route`: egy routing bejegyzés
- `abuse-mailbox`: értesítendő, ha nemkívánatos aktivitást tapasztalunk a prefix felől

# WHOIS: AS-szám lekérdezése

```
$ whois AS2547
```

```
...
```

```
aut-num:          AS2547
as-name:          BMENET-AS
org:              ORG-BME1-RIPE
descr:           Budapest University of Technology and Economics
import:          from AS1955 accept ANY
export:          to AS1955 announce AS2547
```

```
...
```

```
person:          Andras Jako
address:         Budapest University of Technology and Economics
address:         Division of Telecommunications and Informatics
address:         Muegyetem rkp. 9. R310
address:         H-1111 Budapest
address:         Hungary
phone:           +36 1 4631672
fax-no:          +36 1 4632420
nic-hdl:         GOYA-RIPE
org:             ORG-BME1-RIPE
source:          RIPE # Filtered
mnt-by:          AS2547-MNT
```



# WHOIS: prefix-hierarchia

```
$ whois -L 152.66.0.0/16      # kevésbé specifikus prefixek
inetnum:      0.0.0.0 - 255.255.255.255
netname:      IANA-BLK
descr:        The whole IPv4 address space
...
inetnum:      152.0.0.0 - 152.255.255.255
netname:      EU-ZZ-152
descr:        RIPE NCC
...
inetnum:      152.66.0.0 - 152.66.255.255
netname:      BMENET
descr:        Budapest University of Technology and Economics

$ whois -M 152.66.0.0/16      # specifikusabb prefixek
...
route:        152.66.127.0/24
descr:        BMENET-MPTCP-TEST
origin:       AS2547
mnt-by:       AS2547-MNT
source:       RIPE # Filtered
```

# HE Internet Services

- A Hurricane Electric nevű ISP által fenntartott Internet információs szolgáltatás (egyik legnagyobb IPv6 szolgáltató)



## Internet Statistics

Autonomous Systems with IPv4 Announcements Observed: 50,245

Autonomous Systems with IPv6 Announcements Observed: 9,712

IPv4 Prefixes Observed: 593,717

IPv6 Prefixes Observed: 25,829

Domains Observed: 170,696,024

Hosting Companies Observed: 18,700

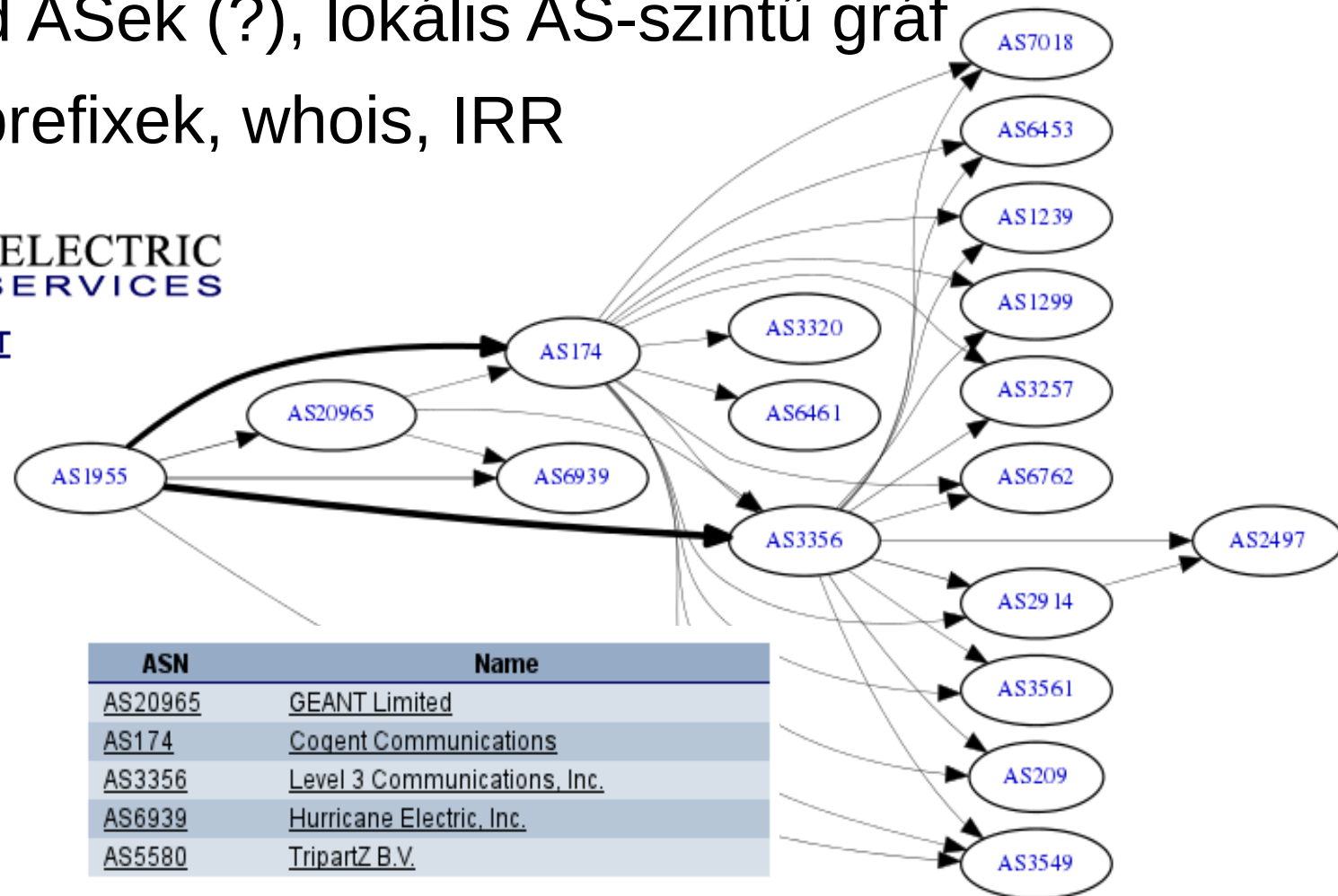
# HE Internet Services

- AS információk: <http://bgp.he.net/AS1955>
  - szomszéd ASek (?), lokális AS-szintű gráf
  - hirdetett prefixek, whois, IRR

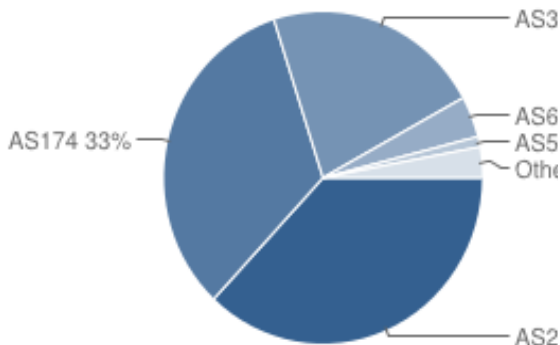


HURRICANE ELECTRIC  
INTERNET SERVICES

AS1955 HUNGARNET



AS1955 IPv4 Peers



ASN	Name
<a href="#">AS20965</a>	<a href="#">GEANT Limited</a>
<a href="#">AS174</a>	<a href="#">Cogent Communications</a>
<a href="#">AS3356</a>	<a href="#">Level 3 Communications, Inc.</a>
<a href="#">AS6939</a>	<a href="#">Hurricane Electric, Inc.</a>
<a href="#">AS5580</a>	<a href="#">TripartZ B.V.</a>

# RIPEstat

- Információk a 152.66.244.111 IP címről  
<https://stat.ripe.net/152.66.244.111>

### Prefix Overview (152.66.244.111)

**Announced**


This prefix is part of 152.66.0.0/16 announced by  
**AS2547**  
**BMENET-AS Budapest University of Technology and Economics,HU**  
and is part of 152.0.0.0/8, Legacy space, administered by ARIN. [i](#)

Showing results for 152.66.0.0/16 as of 2015-02-23 16:00:00 UTC

**!** Given resource is not announced but result has been aligned to first-level less-specific (152.66.0.0/16).

[source data](#) [embed code](#) [permalink](#) [info](#)

### Geoloc (152.66.244.111)



**Geoloc details**

**i** Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for 152.66.244.111 as of 2015-02-03 00:00:00 UTC

[source data](#) [embed code](#) [permalink](#) [info](#)

# RIPEstat

- Információk a 152.66.244.111 IP címről  
<https://stat.ripe.net/152.66.244.111>

### Registry Browser (152.66.244.111)

Last updated on 2014-05-27 at 13:09:34 UTC. [Show more](#)

**inetnum:**  
**152.66.0.0/16**

<b>netname</b>	BMENET
<b>descr</b>	Budapest University of Technology and Economics
<b>country</b>	HU
<b>org</b>	ORG-BME1-RIPE
<b>admin-c</b>	TR4020-RIPE
<b>tech-c</b>	IOS2-RIPE
<b>tech-c</b>	GOYA-RIPE
<b>tech-c</b>	THU-RIPE
<b>status</b>	LEGACY
<b>mnt-by</b>	AS2547-MNT

Showing results for 152.66.0.0/16 as of 2015-02-23 20:15:13 UTC

### Routing Status (152.66.244.111)

At 2015-02-23 16:00:00 UTC,  
✓ 152.66.0.0/16 was 100% visible (by 102 of 102 RIS full peers).

🕒 First ever seen before **Jan 2004** (= beginning of available data).

Originated by: **AS2547** (valid route object in RIPE)

No less-specific covering prefixes.

1 more-specific prefix existing: 152.66.127.0/24 (announced by AS2547)

⚙️ [Advanced Settings](#)

Showing results for 152.66.0.0/16 as of 2015-02-23 16:00:00 UTC

# PeeringDB

- Emlékeztető: két AS-ek közt peer kapcsolat építhető ki, ekkor ellenszolgáltatás nélkül kicserélik egymás forgalmát
- **Peering policy:** milyen feltételek mellett hajlandó egy AS peer kapcsolatot létesíteni
- PeeringDB: peering policy-k, IXP-ken való jelenlét, privát peering lehetőségek

# PeeringDB: Facebook

Company Information	
Company Name	Facebook
Also Known As	Facebook, Instagram
Company Website	<a href="https://www.facebook.com/">https://www.facebook.com/</a>
Primary ASN	32934
IRR Record	AS-FACEBOOK
Network Type	Content
Approx Prefixes	100
Traffic Levels	1 Tbps+
Traffic Ratios	Mostly Outbound
Geographic Scope	Global
Looking Glass URL	
Route Server URL	
Notes	<p>We have a selective peering policy requiring a minimum of 50 Mbps of in-continent traffic destined to or through your network. We welcome the opportunity to engage in peering with responsible BGP speakers in an effort to improve the experience of our millions of users throughout the globe.</p> <p>We require an up-to-date peeringdb entry for all public peering requests, including exchange information with properly formatted public fabric addresses, asns, and noc/peering contact information.</p> <p>We ask that peers also maintain their private peering facilities, as we use this information for private peering (PNI) targeting.</p>
Protocols Supported	Unicast IPv4 <input checked="" type="checkbox"/> Multicast <input type="checkbox"/> IPv6 <input checked="" type="checkbox"/>
Date Last Updated	2015-03-06 08:17:33 UTC
Peering Policy Information	
Peering Policy URL	<a href="https://www.facebook.com/peering/">https://www.facebook.com/peering/</a>
General Policy	Selective
Multiple Locations	Not Required
Ratio Requirement	No
Contract Requirement	Not Required

Public Peering Exchange Points	
Exchange Point Name	ASN
<a href="#">AMS-IX</a>	32934
<a href="#">AMS-IX</a>	32934
<a href="#">AMS-IX</a>	32934
<a href="#">AMS-IX</a>	32934
<a href="#">BBIX Tokyo</a>	32934
<a href="#">BBIX Tokyo</a>	32934
<a href="#">BNIX</a>	32934
<a href="#">BNIX</a>	32934
<a href="#">CoreSite - Any2 California</a>	32934
<a href="#">CoreSite - Any2 California</a>	32934
<a href="#">CoreSite - Any2 California</a>	32934
<a href="#">CoreSite - Any2 California</a>	32934

Private Peering Facilities	
Facility Name	ASN
<a href="#">Chief LY Building Taipei</a>	32934
<a href="#">CoreSite - LA1 - One Wilshire</a>	32934
<a href="#">CSF CX1 Cyberjaya</a>	32934
<a href="#">Equinix Amsterdam (AM3)</a>	32934
<a href="#">Equinix Ashburn (DC1-DC11)</a>	32934
<a href="#">Equinix Chicago (CH1/CH2)</a>	32934
<a href="#">Equinix Dallas (DA1)</a>	32934

# Route server és looking glass

- Mit lát egy távoli ISP? Látja-e a prefixünket?
- Egyes ISP-k megfigyelőpontokat tartanak fenn, ahonnan „bele lehet nézni” az Internetbe
- Távolról elérhető hoszt, korlátozott parancssorral (route-server) vagy webes felülettel (looking glass)
- Szolgáltatások: ping, traceroute, BGP AS info
  - `routeserver.org`: route szerverek (hiányos) listája
  - `www.bgp4.as/looking-glasses`: looking glass lista
  - `traceroute.org`: dedikált traceroute szerverek listája



# Route server és looking glass

- Van-e kétirányú elérhetőség a SwissCom felől a 152.66.130.2 IP címre?

```
$ telnet route-server.ip-plus.net
Trying 164.128.251.50...
Connected to route-server.ip-plus.net.
Escape character is '^]'.

*** Swisscom IP+ route server (AS3303) ***

RS_AS3303>ping 152.66.130.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 152.66.130.2, ...
!!!!
Success rate is 100 percent (5/5), ...
```

# Route server és looking glass

- Milyen útvonalon halad a forgalom Albertából?

```
$ telnet route-views.on.bb.telus.com
Trying 154.11.63.86...
Connected to route-views.on.bb.telus.com.
...
route-views.on>traceroute 152.66.130.2
 1 toroonxngr00.bb.telus.com (154.11.63.85) [AS 852]
 2 154.11.6.100 [AS 852] 0 msec 0 msec 0 msec
 3 NYCMNY83CI01.bb.telus.com (75.154.223.252)
 4 te0-7-0-10.ccr21.jfk05.atlas.cogentco.com [AS 174]
...
13 te0-0-2-0.nr11.b020664-1.bud01.atlas.cogentco.com ...
14 149.11.10.10 [AS 174] 120 msec 116 msec 120 msec
15 te0-1-0-0.rtr.bme.hbone.hu (195.111.97.102) [AS 1955]
16 xge12-1.taz.net.bme.hu (152.66.0.125) [AS 2547]
17 ural2.hszk.bme.hu (152.66.130.2) [AS 2547]
```

# Route server és looking glass

- Mi az AS-szintű útvonal Japánból? Milyen BGP hirdetések láthatók onnan a BME felé?

```
$ telnet route-views.wide.routeviews.org
...
route-views.wide.routeviews.org> show ip bgp 152.66.130.2
BGP routing table entry for 152.66.0.0/16
Paths: (2 available, best #1, table ...)
  Not advertised to any peer
  2497 3356 1955 2547
    202.249.2.169 from 202.249.2.169 (58.138.96.157)
      Origin IGP, localpref 100, valid, external, best
      Last update: Fri Jan 30 11:40:00 2015

  7500 2497 3356 1955 2547
    202.249.2.169 from 202.249.2.86 (202.249.2.86)
      Origin IGP, localpref 100, valid, external
      Last update: Fri Jan 30 11:40:23 2015
```



# Feladatok

- Melyik AS tartalmazza 9.9.9.9 IP címet?
- Kié az AS 1 azonosító?
- Mi a Yale Egyetem AS száma, mely IP címeket hirdet ez az AS, és mikor történt utoljára említésre méltó esemény ezzel a prefixszel?  
(HE, BGPplay)
- Melyik szervezet a 200.200.200.200 IP cím használója jelenleg, melyik országban van bejegyezve, és milyen email címre kell írni, ha spam-et kapunk erről az IP címről (abuse)?

# Feladatok

- Hány IP prefixet hirdet az `AS100`, ezek összesen hány IP címet tartalmaznak, és mikor történt utoljára említésre méltó BGP esemény ezzel az ASsel?
- Mi a `twitter.com` elsődleges ASének száma, legalább mekkora kétirányú forgalom esetén hajlandó peer kapcsolatba lépni egy másik ASsel, és mely publikus IXPken van jelen?
- Soroljon fel 10-10 belföldi és külföldi ISP-t, amely jelen van a BIXen! Üzemeltet a BIX looking glass szervert? (`bix.hu`)