The Internet Ecosystem and Evolution

Lab 3

Internet monitoring

Obtain info from the Internet

- It is particularly difficult for an operator to acquire timely information on the function (or the misfunction) of the Internet
- An AS perceives only its own network plus, possibly, ASes in its vicinity, but how to learn about remote ASes?
- Relevant information is scattered around disconnected databases
  - Which AS owns an IP address range? (e.g., we receive DOS traffic from some address an we want to identify the culprit)
  - How do two remote ASes connect to each other? (e.g., if I connect to `AS1`, will I get good connectivity to `AS2`?)
  - Who to contact if we get spam from some IP address?
  - Why can't my network be reached from, say, Hong Kong?
- **The problem is not how to answer these questions, but rather whether what we ask can be answered at all**!

„Well-known” tools

- Check two-way IP connectivity between two hosts: `ping`
- Path to a remote host: `traceroute`
  - TCP SYN packets with increasing TTL (1, 2,...)
  - whenever TTL expires at a router along the path we get an `ICMP Time Exceeded` message from that router
  - intermediaries between us and the destination are traced
- Domain name ↔ IP address correspondence: `host`, `dig`

```
$ host ebay.com
ebay.com has address 66.211.181.123
ebay.com has address 66.211.185.25
…
$ host  66.211.181.123
123.181.211.66.in-addr.arpa domain name pointer ebay.com.
```

WHOIS

- A mechanism to query Internet resources:
  - domain names
  - IP address ranges and owners
  - Autonomous Systems and identifiers (AS numbers)
- By default, a simple „command line” (CLI) tool
  - Web: `https://apps.db.ripe.net/search/query.html`
  - telnet: `telnet whois.ripe.net 43`
  - CLI: `whois 152.66.244.111`
- Open databases, standard machine parseable (RPSL) format

WHOIS: Querying an IP prefix

```
$ 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: Important RPSL objects

- `inetnum:` information on an IP prefix (netname, country, org, admin)
  - `152.66.0.0 - 152.66.255.255`
- `organization:` the name of the organization that “owns” the prefix (org):
  - `ORG-BME1-RIPE`
- `person:` id an administrator (`address`,...)
- `route:` a routing entry (if address is routable, which AS will terminate traffic to that address)
- `abuse-mailbox:` whom to contact if malicious traffic (say, spam) from the prefix is seen in our own network

WHOIS: Querying an AS number

```
$ 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
```

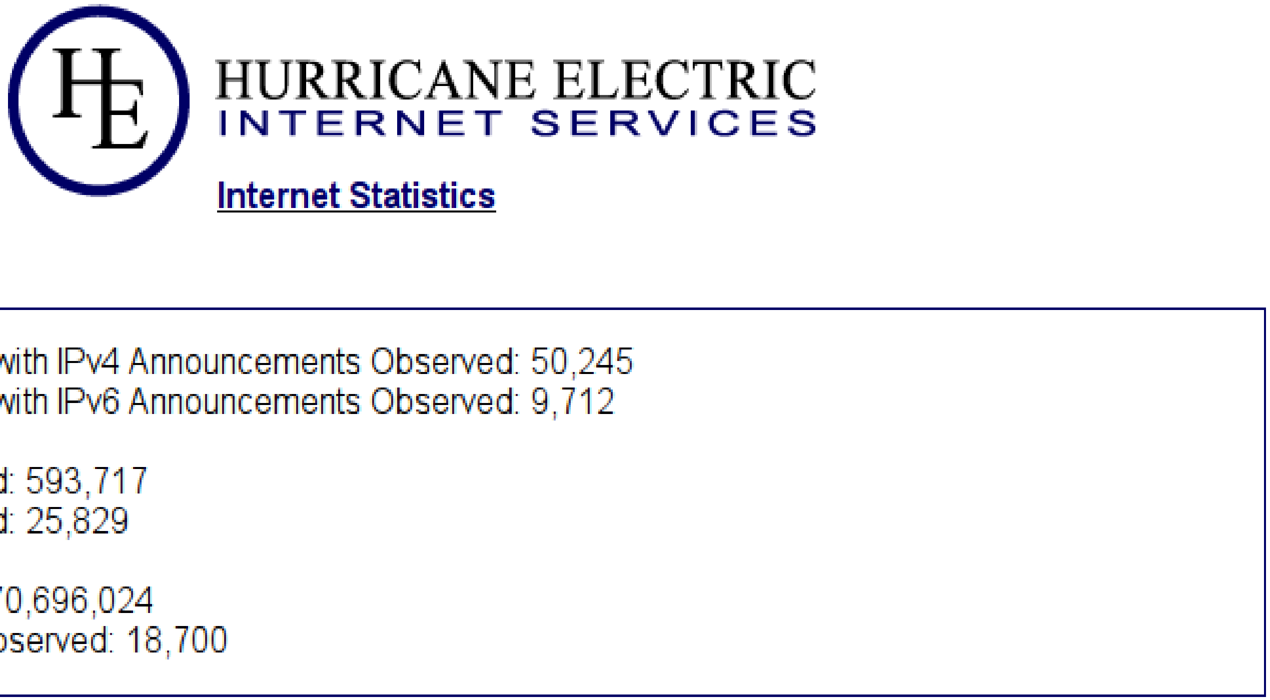
WHOIS: Prefix hierarchy

```
$ whois -L 152.66.0.0/16     # less spcific prefixes
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     # more specific prefixes
...
route:          152.66.127.0/24
descr:          BMENET-MPTCP-TEST
origin:         AS2547
mnt-by:         AS2547-MNT
source:         RIPE # Filtered
```

HE Internet Services

- The Internet information service operated by Hurricane Electric (one of the largest IPv6 service providers)



HURRICANE ELECTRIC
INTERNET SERVICES

Internet Statistics

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

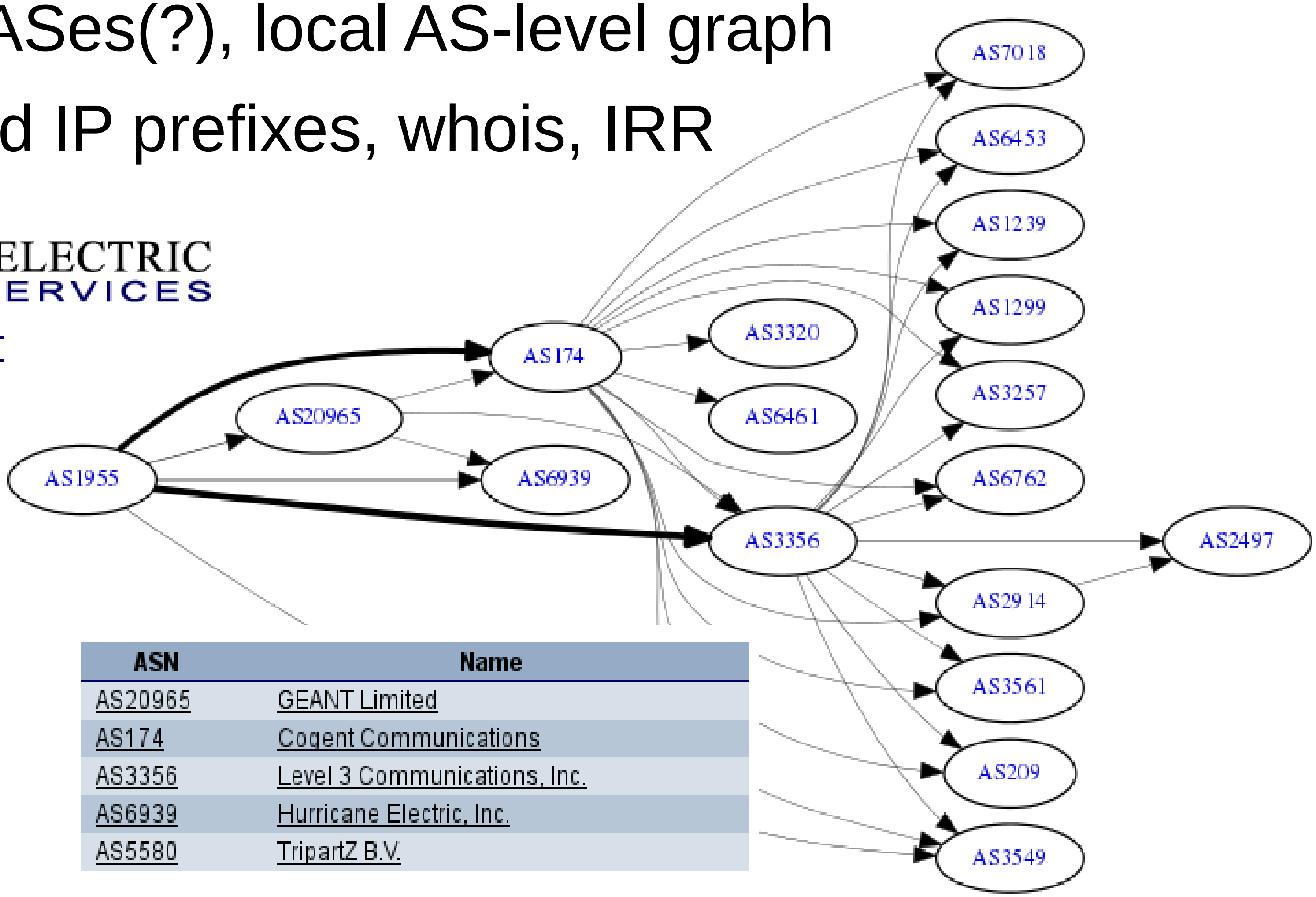
Domains Observed: 170,696,024
Hosting Companies Observed: 18,700

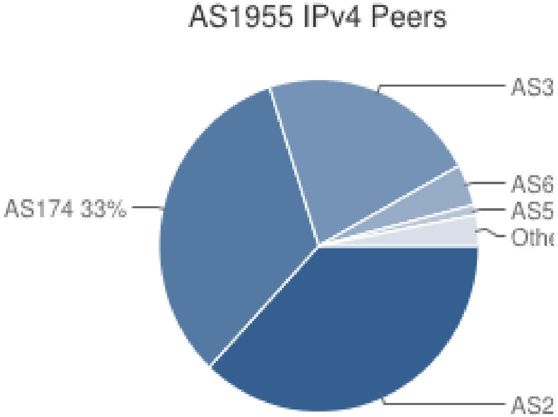
HE Internet Services

- AS information: `http://bgp.he.net/AS1955`
  - neighbor ASes(?), local AS-level graph
  - announced IP prefixes, whois, IRR

HURRICANE ELECTRIC
INTERNET SERVICES

AS1955 HUNGARNET

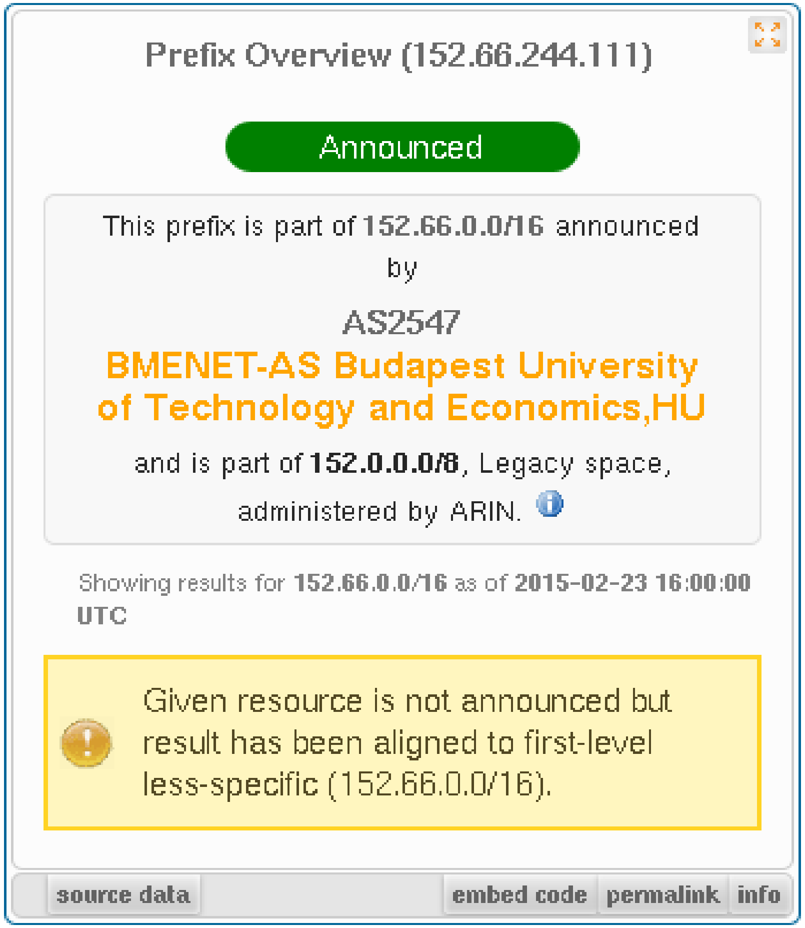




ASN	Name
AS20965	GEANT Limited
AS174	Cogent Communications
AS3356	Level 3 Communications, Inc.
AS6939	Hurricane Electric, Inc.
AS5580	TripartZ B.V.

RIPEstat

- Information on address `152.66.244.111`:
  `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

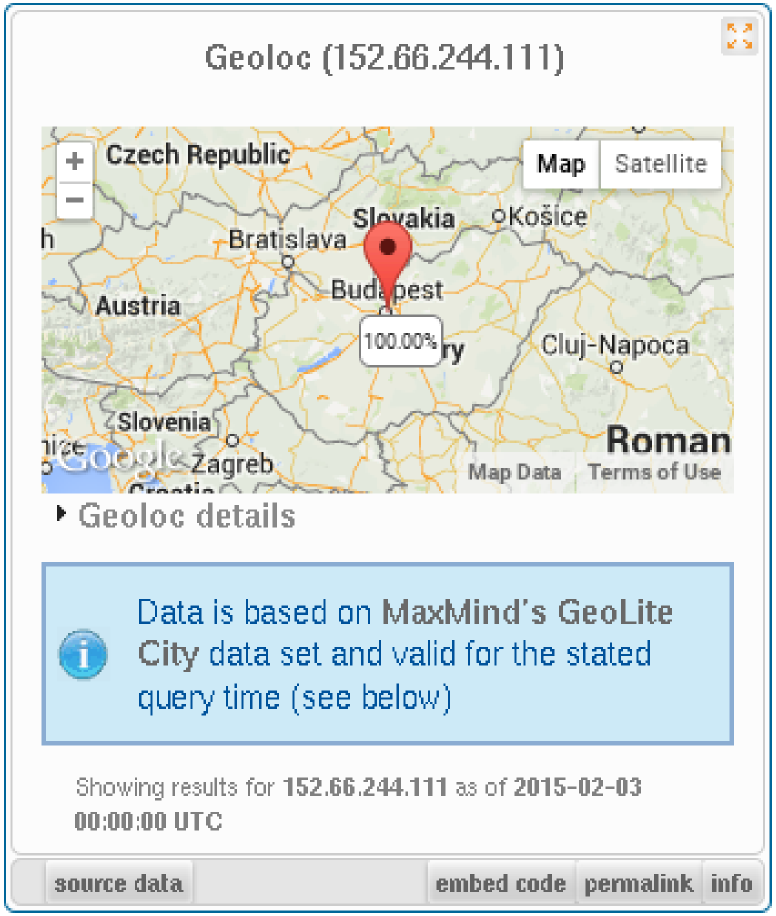
AS2547

BMENET-AS Budapest University of Technology and Economics,HU

and is part of **152.0.0.0/8**, Legacy space, administered by ARIN.

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).



Geoloc (152.66.244.111)

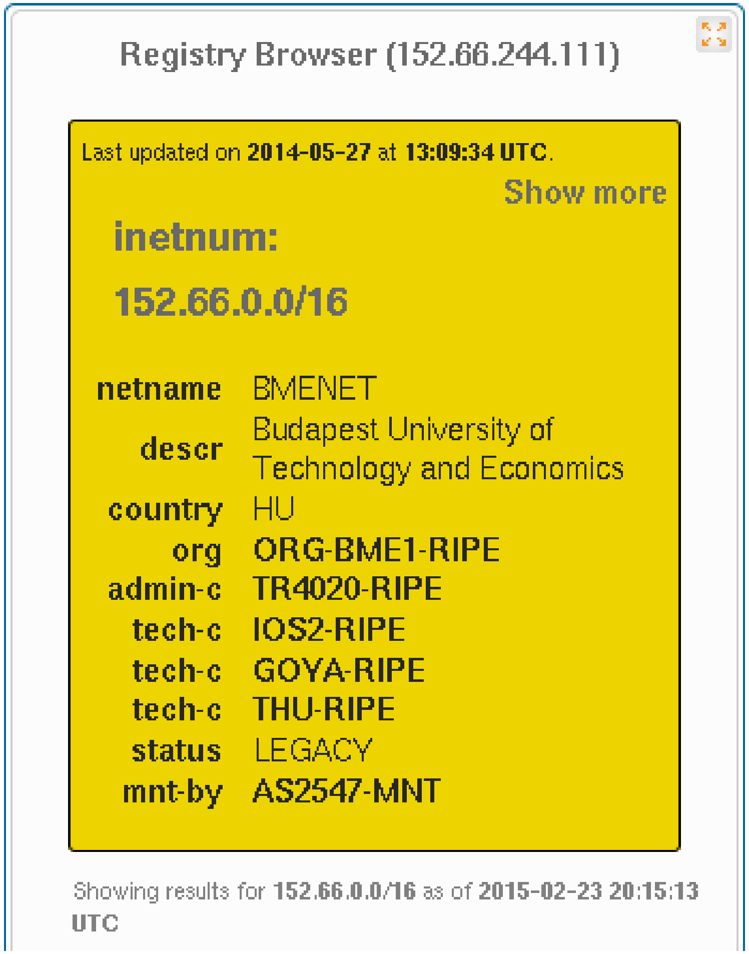
Geoloc details

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**

RIPEstat

- Information on address `152.66.244.111`: `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**.

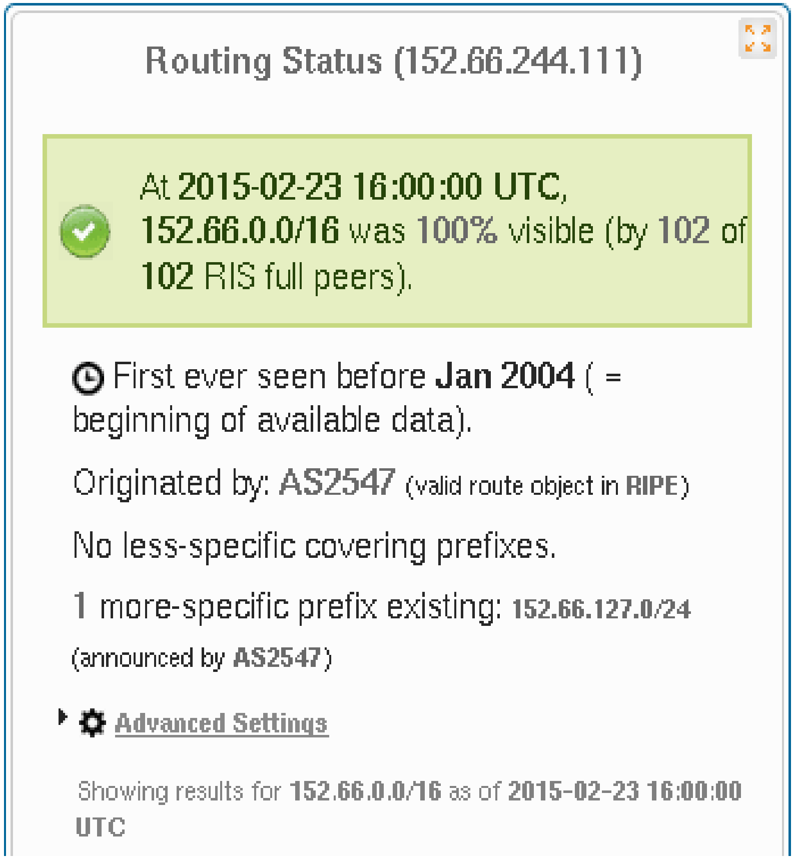
Show more

inetnum:

152.66.0.0/16

netname	BMENET
descr	Budapest University of Technology and Economics
country	HU
org	ORG-BME1-RIPE
admin-c	TR4020-RIPE
tech-c	IOS2-RIPE
tech-c	GOYA-RIPE
tech-c	THU-RIPE
status	LEGACY
mnt-by	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**)

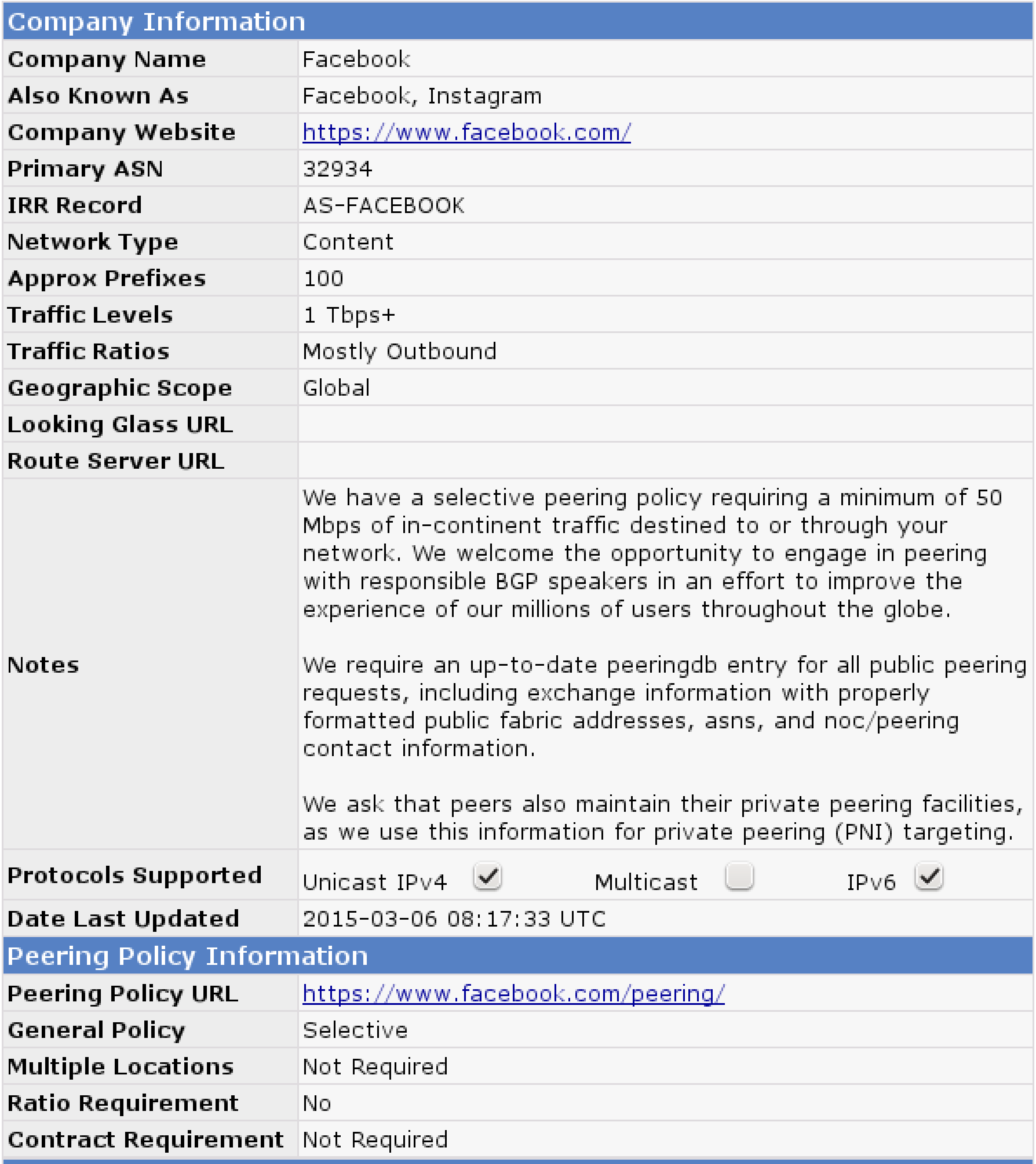
Advanced Settings

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

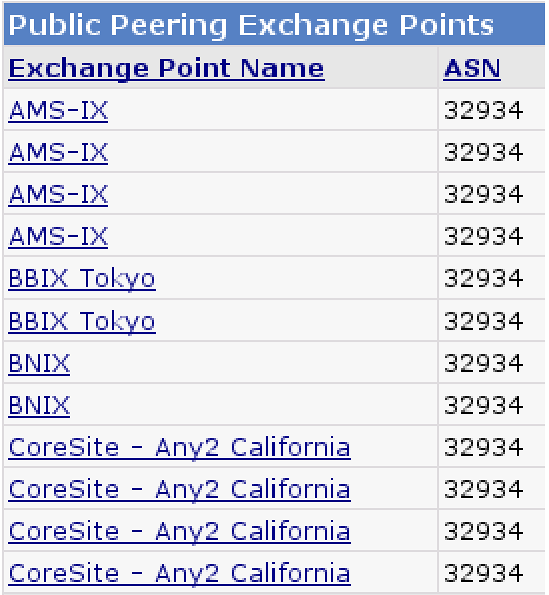
PeeringDB

- **Recall:** two ASes may enter into a settlement free **peering** relationship, whereas they directly exchange traffic between themselves and their customers
- **Peering policy:** the conditions under which an AS is willing to enter into a peering relationship with some other AS (open/selective)
- **PeeringDB:** a common database for ISPs to publish their peering policies, availability at IXPs (where to establish a peer link), private peering possibilities, etc.
- Information is voluntarily provided by ISPs, so it may contain errors, be outdated, or would not exist at all

PeeringDB: Facebook

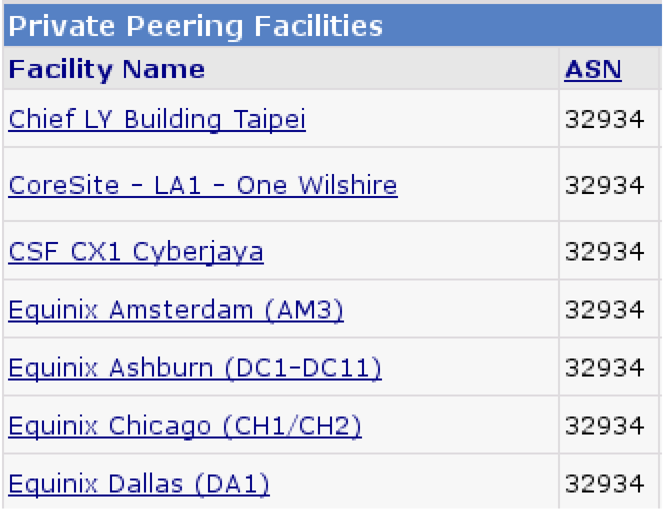


Company Information	
Company Name	Facebook
Also Known As	Facebook, Instagram
Company Website	https://www.facebook.com/
Primary ASN	32934
IRR Record	AS-FACEBOOK
Network Type	Content
Approx Prefixes	100
Traffic Levels	1 Tbps+
Traffic Ratios	Mostly Outbound
Geographic Scope	Global
Looking Glass URL	
Route Server URL	
Notes	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. 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. We ask that peers also maintain their private peering facilities, as we use this information for private peering (PNI) targeting.
Protocols Supported	Unicast IPv4 ☑ Multicast □ IPv6 ☑
Date Last Updated	2015-03-06 08:17:33 UTC
Peering Policy Information	
Peering Policy URL	https://www.facebook.com/peering/
General Policy	Selective
Multiple Locations	Not Required
Ratio Requirement	No
Contract Requirement	Not Required



Public Peering Exchange Points

Exchange Point Name	ASN
AMS-IX	32934
AMS-IX	32934
AMS-IX	32934
AMS-IX	32934
BBIX Tokyo	32934
BBIX Tokyo	32934
BNIX	32934
BNIX	32934
CoreSite - Any2 California	32934
CoreSite - Any2 California	32934
CoreSite - Any2 California	32934
CoreSite - Any2 California	32934



Private Peering Facilities

Facility Name	ASN
Chief LY Building Taipei	32934
CoreSite - LA1 - One Wilshire	32934
CSF CX1 Cyberjaya	32934
Equinix Amsterdam (AM3)	32934
Equinix Ashburn (DC1-DC11)	32934
Equinix Chicago (CH1/CH2)	32934
Equinix Dallas (DA1)	32934

Route servers/looking glasses

- How does a remote AS “see” the Internet? Do they have connectivity to my prefix?
- Certain ISPs maintain vantage points from where we can freely “look into” the Internet
- Either a remotely available IP host running a stripped-down version of BGP (**route-server**) or exposing a web GUI (**looking glass**)
- Common services: `ping`, `traceroute`, BGP AS info
  - `routeserver.org`: list of route servers (unmaintained)
  - `www.bgp4.as/looking-glasses`: list of looking glasses
  - `traceroute.org`:list of dedicated `traceroute` servers

Route servers/looking glasses

- Is there two-way connectivity from SwissCom to the IP address `152.66.130.2`?

```
$ 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 servers/looking glasses

- Which path traffic takes from Alberta?

```
$ 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]
 2 154.11.6.33 [AS 852]
 3 75.154.223.254
 4 lag-113.ear3.NewYork1.Level3.net (4.15.212.245) [AS 3356]
 5 ae-2-3101.bar1.Budapest1.Level3.net (4.69.201.150) ...
 6 ae-2-3101.bar1.Budapest1.Level3.net (4.69.201.150) ...
 7 DANTE.bar1.Budapest1.Level3.net (212.162.26.2) [AS 3356]
 8 tg0-1-0-0.rtr.bme.hbone.hu (195.111.100.42) [AS 1955]
 9 xge2-1.taz.net.bme.hu (152.66.0.125) [AS 2547]
10 ural2.hszk.bme.hu (152.66.130.2) [AS 2547]
```

- First we need a traceroute server/looking glass in Alberta!

Route servers/looking glasses

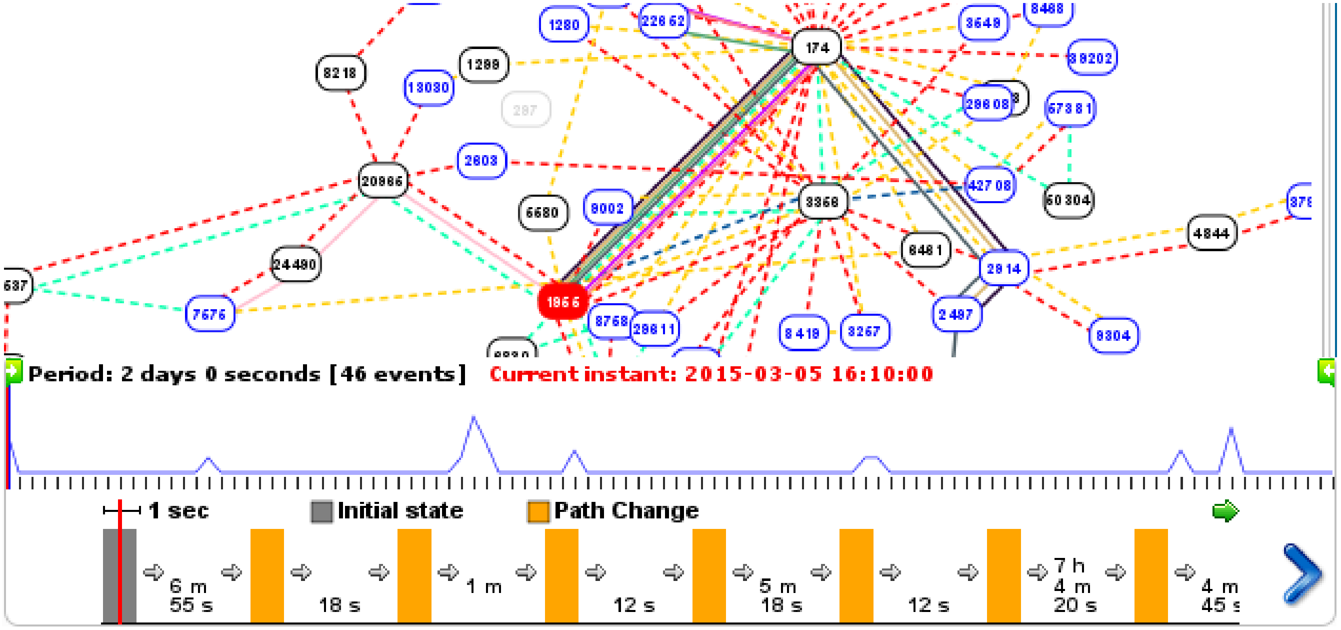
- Which is the AS-level path from Japan? Which BGP announcements to BMEnet exist there?

```
$ 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
```

Other sources of information

- **robtex.com:** alternative to RIPEstat
  - AS info: www.robtex.com/as/as1955.html
  - prefix: www.robtex.com/route/152.66.0.0-16.html
- **downdetector.com:** status, reachability, tickets
- **BGPlay:** `stat.ripe.net/widget/bgplay#w.resource=AS1955`


Period: 2 days 0 seconds [46 events]

Current instant: 2015-03-05 16:10:00

Exercises

- Which AS owns the IPv4 address `9.9.9.9`?
- Who owns AS number 1 (`AS1`)?
- Which is the AS number of the Yale University, which IP addresses does this AS announce, when was the last time anything relevant happened to these prefixes? (HE, `BGPlay`)
- Which organization uses the IP address `200.200.200.200` currently, which country it is located in, whom to email if we get spam from this IP address (abuse)?

Exercises

- How many IP prefixes are announced by `AS100` and how many IP addresses these contain in total?
- Which is the primary AS number of `twitter.com`, which is the AS type (eyeball/content/transit) and peering policy (open/selective), at which public IXPs does Twitter have a POP?
- Name at least 10 incumbent and 10 foreign ISPs that can be connected to in the IXPs BIX (`bix.hu`) and DE-CIX/Frankfurt (`de-cix.net`)! Do these IXPs operate a looking glass? (use google search!)