

# Active and Passive Measurements: Measuring Networks

Prof. Anja Feldmann, Ph.D.

Dr. Ramin Khalili

Georgios Smaragdakis, Ph.D.

# Outline

- Whois
- Looking Glasses
- Internet ATLAS
- BGP data

# Whois

- Who is who in the Internet?
- Internet domain name and network number directory service
- Information about
  - Domains: e.g., google.com, microsoft.com,...
  - Internet address space allocation
  - Networks: AS number, e.g., AS3320
- Databases maintained by the local Internet routing registries:
  - ARIN: Northern America
  - RIPE: Europe
  - APNIC: Asia–Pacific
  - LACNIC: Latin America
  - AFRINIC: Africa

# Whois

```
whois [-h host] [-p port] name ...
```

```
-h host
```

Use the specified host instead of the default variant. Either a host name or an IP address may be specified.

```
-p port
```

Connect to the whois server on port. If this option is not specified, whois defaults to port 43.

- **Examples (Google)**
  - **whois www.google.com**
  - **whois 173.194.32.240**
  - **whois AS15169**

# Outline

- Whois
- Looking Glasses
- Internet ATLAS
- BGP data

# Looking glasses (LGes)

- Publicly available remote servers that run BGP commands and traceroutes:
  - show ip bgp
  - show bgp neighbors
  - show ip bgp regexp
  - show thread cpu
  - traceroute
  - traceroute with AS numbers (IPv4 only)
- Operated by ISPs or NOCs, e.g. DTAG.
- Wide list available at:  
<http://www.bgp4.as/looking-glasses>  
e.g., Level(3) looking glass: lg.level3.net

# RIPE Routing Information Service (RIS)

- RIPE Routing Information Service:

<http://www.ris.ripe.net>

- General routing statistics
  - Prefix size distribution
  - Neighbors
  - AS path lengths
  - Whois
  - Bogon filtering
- Looking glass
  - BGP summary
  - BGP neighbors
  - show CPU
  - traceroute with AS numbers

# Outline

- Whois
- Looking Glasses
- Internet ATLAS
- BGP data



# Routing ATLAS

- ATLAS: “book of maps or charts”
- Tool to explore and compare networks:
  - CAIDA ([as-rank.caida.org](http://as-rank.caida.org))
  - Fixedorbit ([www.fixedorbit.com](http://www.fixedorbit.com))
  - NetConfigs ([www.netconfigs.com](http://www.netconfigs.com))
- Metrics to compare networks:
  - IP space originated
  - Number of peers
  - Customers
  - Average path length

# Internet ATLAS

- TeleGeography ([www.telegeography.com](http://www.telegeography.com))
- Information about
  - Pricing: access, IP transit, enterprise networks
  - Internet: bandwidth growth, IXPs
  - Communication infrastructure: fiber layout and plans, hosting,
  - Business: Internet and mobile phone market, 4G
  - Maps: submarine cables, Internet, global traffic

# Outline

- Whois
- Looking Glasses
- Internet ATLAS
- BGP data

# BGP routing data

- Oregon RouteViews ([www.routeviews.org](http://www.routeviews.org))
- RIPE RIS ([www.ris.ripe.net](http://www.ris.ripe.net))
- Public Internet Exchange Points (IXP) LGeS:  
[www.bgp4.as/internet-exchanges](http://www.bgp4.as/internet-exchanges)
- Example: Cyclops ([cyclops.cs.ucla.edu](http://cyclops.cs.ucla.edu))
  - Collects public BGP data + looking glasses
  - Statistics about
    - Global visibility
    - AS classification
    - Peering relationships

# BGP routing data

- Source: RIPE RIS raw data

<http://www.ripe.net/data-tools/stats/ris/ris-raw-data>

- There are two types of files: updates (every 5 mins) and aggregated views (bview, every 8 hours)
- Follow the links, and e.g., download

<http://data.ris.ripe.net/rrc00/2014.04/bview.20140405.0800.gz>

Use bgpdump:

```
$ ssh tst1.inet.tu-berlin.de
```

```
Login: measurement14
```

```
Password: Meter14
```

(or install bgpdump in your local machine)

# BGP routing data

- Reading BGP data: bgpdump

Basic command: `bgp <file>`

TIME: 04/05/14 08:00

TYPE: TABLE\_DUMP\_V2/IPV4\_UNICAST

PREFIX: 1.0.0.0/24

SEQUENCE: 0

FROM: 218.189.6.2 AS9304

ORIGINATED: 03/27/14 22:32:41

ORIGIN: IGP

ASPATH: 9304 15169

NEXT\_HOP: 218.189.6.2

COMMUNITY: 9304:171 9304:401 9304:5000 9304:17111 65171:15169

# BGP routing data

- Reading BGP data: bgpdump
  - `bgpdump -m bgpfile` → one line output
  - Routing table output:

```
1265313600|B|96.4.0.55|11686|0.0.0.0/0|11686 2914|IGP|96.4.0.55|0|0||  
Timestamp Peer-router Prefix AS_path
```

Human readable time: `date -d @1265313600`

- BGP updates (for the `updates.XXXX.XXX.gz` files):

```
1272672012|A|195.22.216.188|6762|109.194.96.0/22|...|IGP|195.22.216.188|0|0||  
1272672012|W|154.11.11.113|852|207.219.26.0/2  
Timestamp Withdraw_or_Update Prefix
```

# BGP routing data

Find how many announcements are in a file:

```
$ bgpdump -m bview.20140405.0800 | wc -l  
8,457,852
```

Find how many unique subnets are announced:

```
$ bgpdump -m bview.20140405.0800 | awk '{split($0,a,"|"); print a[6]}' |  
    sort -S5G | uniq | wc -l  
530060
```

Notice that some of the prefixes may be more/less specific, private/unroutable



# BGP routing data

## Show the AS-level path length

```
$ bgpdump -m bview.20140405.0800 | awk '{split($0,a,"|"); print a[7]}'
```

Notice that there may be AS-path prepending (e.g., ASA ASB ASB ASB ASC)

## Find the average AS-level path length

```
$ bgpdump -m bview.20140405.0800 | awk '{split($0,a,"|"); print a[7]}'  
  | awk '{n=split($0,b," "); print n}' > as-level.path.length.dat
```

Use R to find the statistics (as we did for the ping delay analysis)