Fundamentals of Data Analytics

SEN163A

Internet measurements

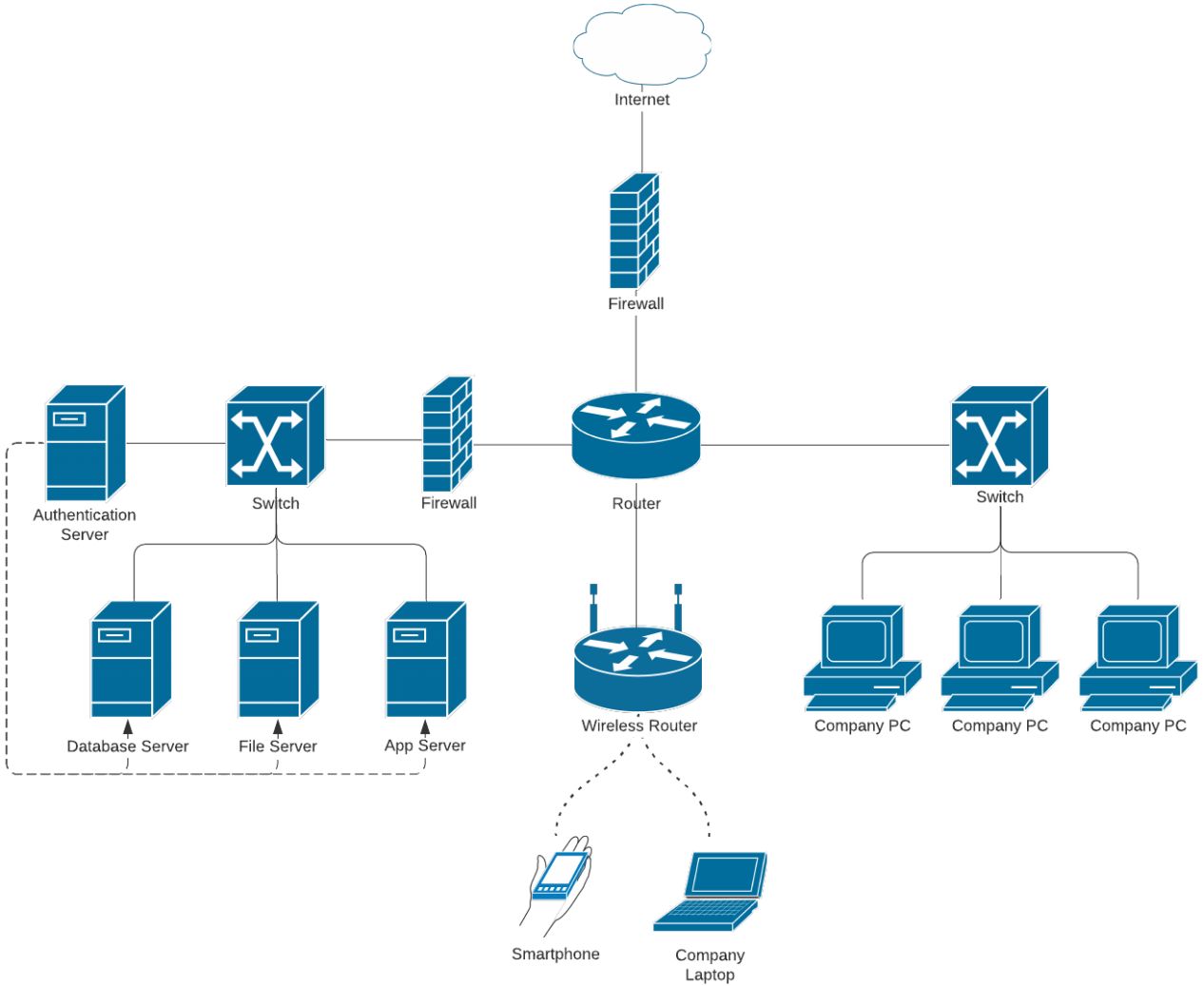
Jacopo De Stefani

Based on the material by Tobias Fiebig

TU Delft

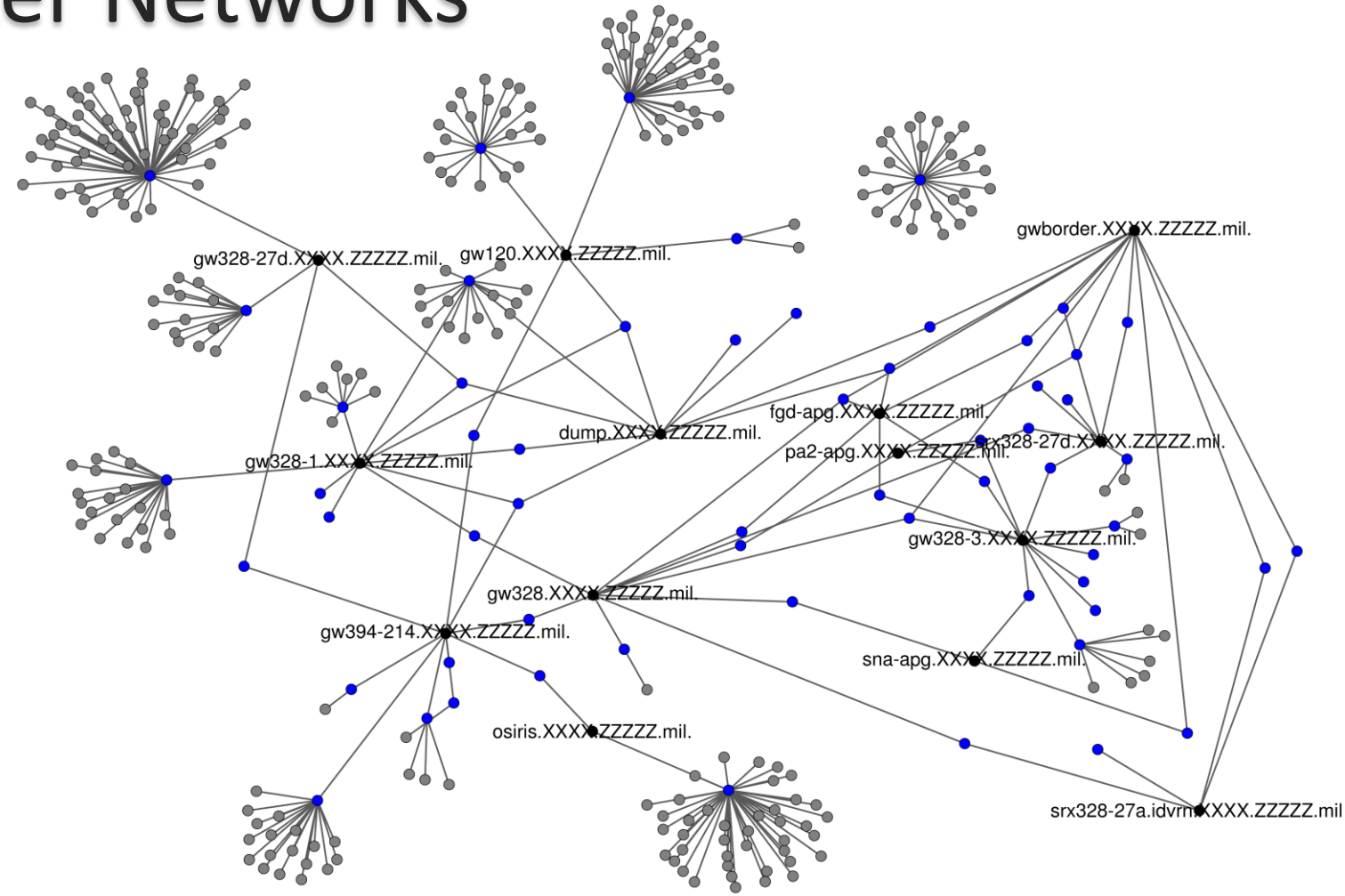
Outline of the lecture

- Review of the basic networking concepts
- Types of internet measurements: passive vs active measurements with examples
- Internet measurement in practice


Internet
Firewall
Authentication Server
Switch
Firewall
Router
Switch
Database Server
File Server
App Server
Wireless Router
Company PC
Company PC
Company PC
Smartphone
Company Laptop

TU Delft

Computer Networks



TU Delft

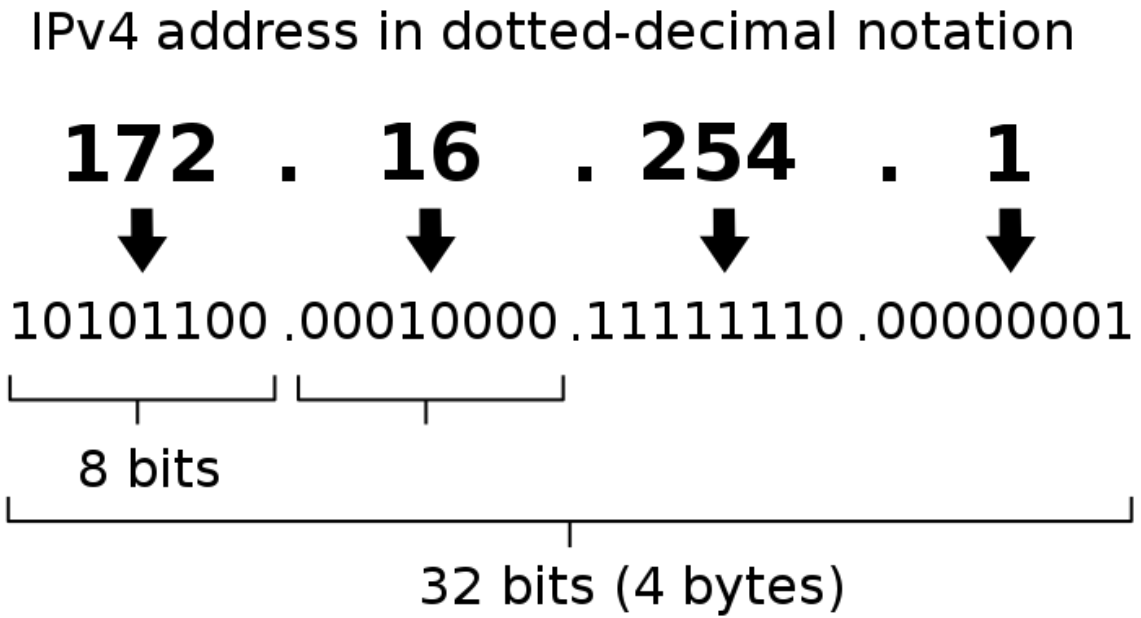
Key Concepts

- Host
- IP
- Port
- DNS : Host <-> IP

Key Terms

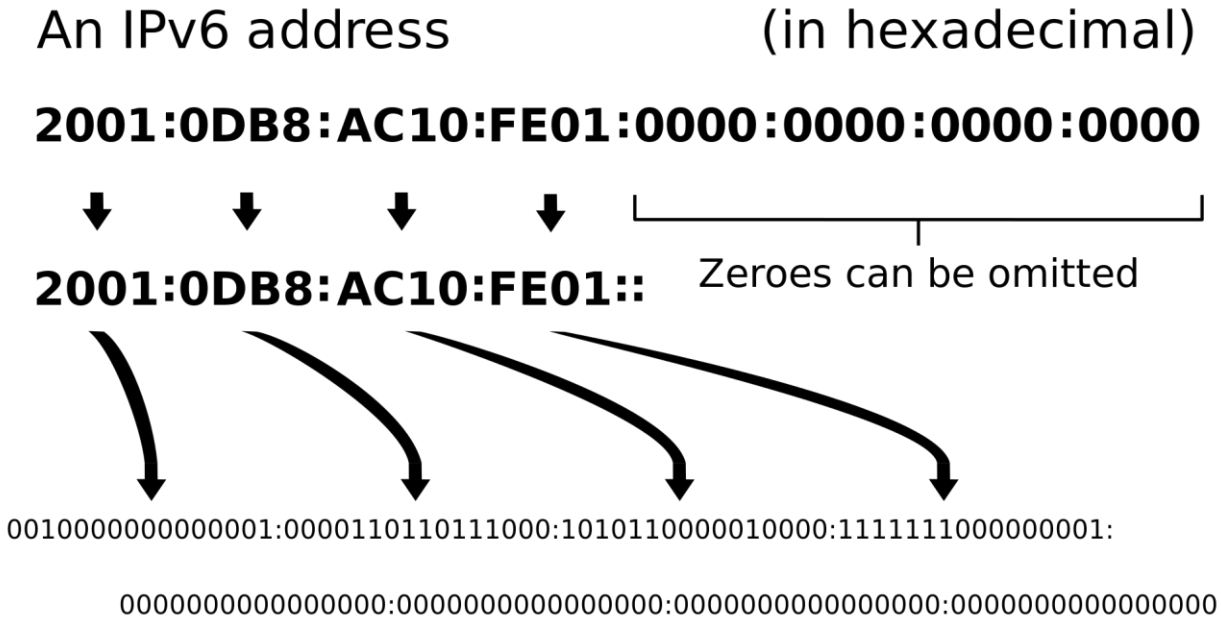
- Autonomous Systems (AS): The individual networks which make up the Internet. Also has a more technical dimension
- Network: A set (or block) of IP addresses. ASes use (advertise) one or multiple networks.
- Prefix size: Determines the number of IP addresses in a Network (usually in CIDR notation)

IPv4 addresses



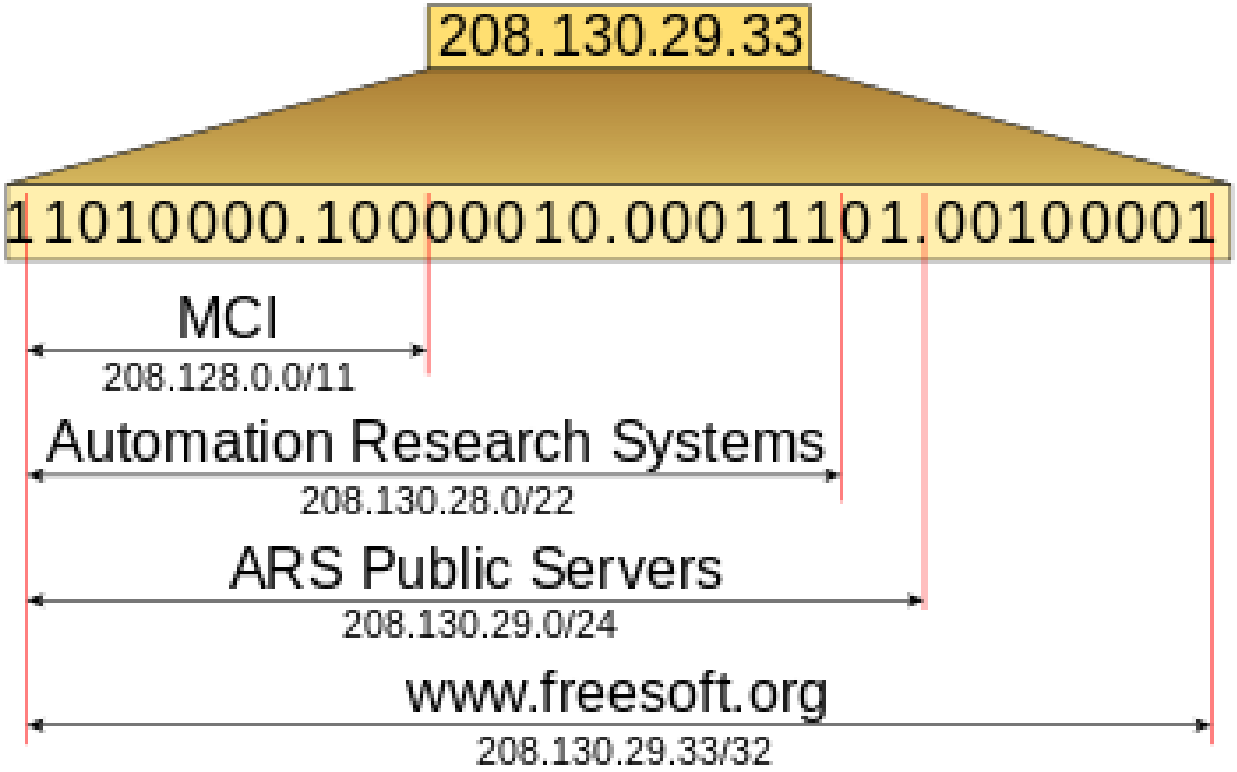
Source: https://en.wikipedia.org/wiki/IPv4

IPv6 addresses



Source: https://en.wikipedia.org/wiki/IPv6

CIDR Notation



Source: Wikipedia ☺

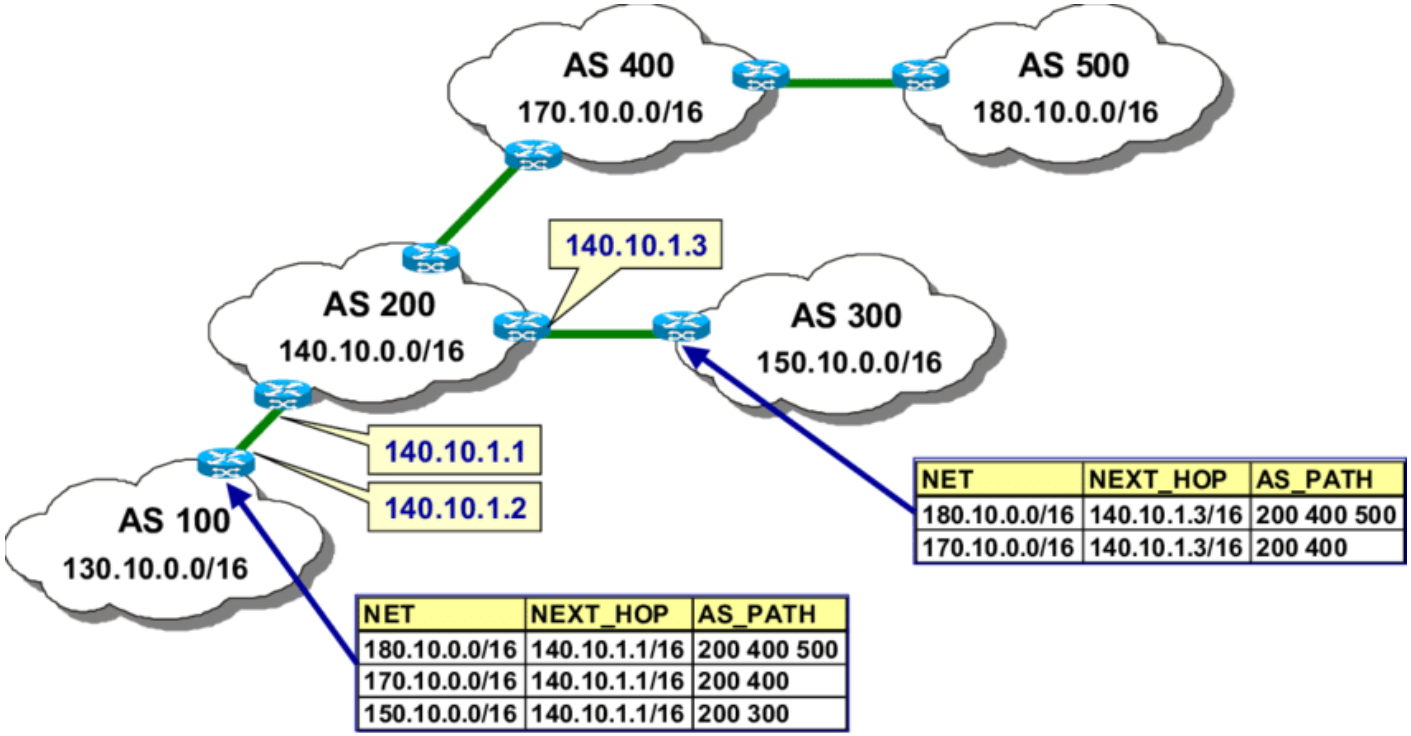
Hosts and names

- Hosts should have names
- We usually look at the forward direction (name to IP)
- There are also DNS measures to resolve the name for an IP (if configured by the operators)
  - 2a01:4f8:10b:37ef::186:
    6.8.1.0.0.0.0.0.0.0.0.0.0.0.0.0.f.e.7.3.b.0.1.0.8.f.4.0.1.0.a.2.ip6.arpa
    domain name pointer mail.aperture-labs.org.
  - 94.130.126.186
    186.126.130.94.in-addr.arpa
    domain name pointer mail.aperture-labs.org.

TU Delft


The Internet is a network of networks…

BGP: Finding a path for your packets

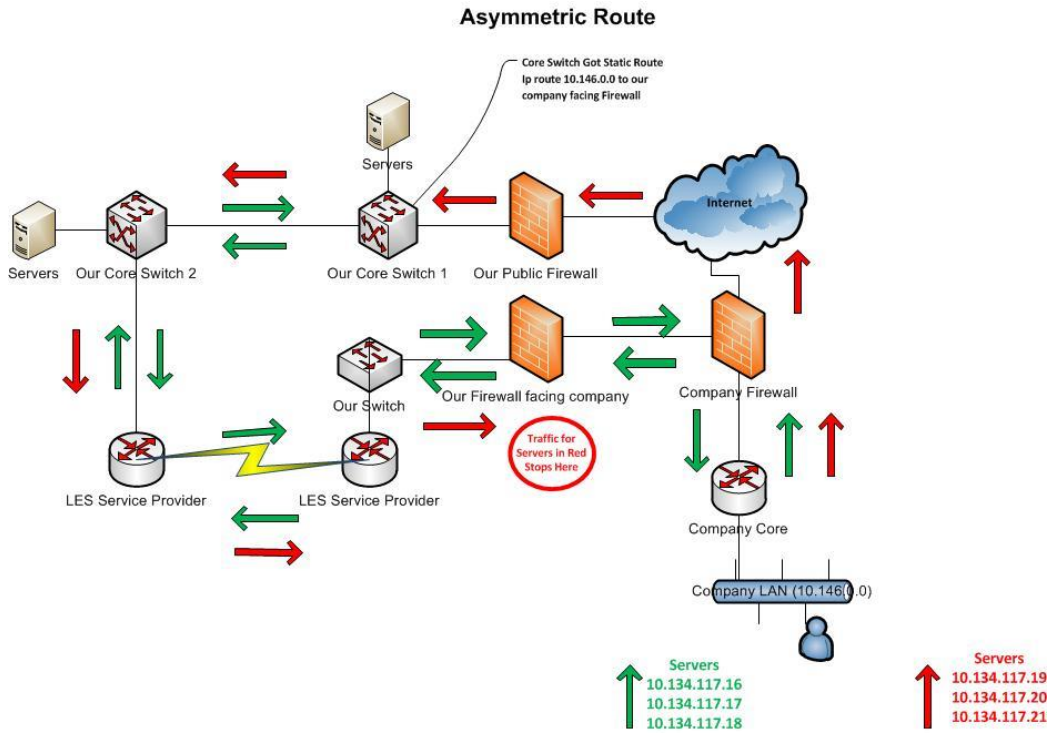


NET	NEXT_HOP	AS_PATH
180.10.0.0/16	140.10.1.3/16	200 400 500
170.10.0.0/16	140.10.1.3/16	200 400

NET	NEXT_HOP	AS_PATH
180.10.0.0/16	140.10.1.1/16	200 400 500
170.10.0.0/16	140.10.1.1/16	200 400
150.10.0.0/16	140.10.1.1/16	200 300

Source: https://www.researchgate.net/figure/BGP-routing-table-example_fig7_34930048

Asymmetric Routing



Source: https://skminhaj.wordpress.com/2016/02/15/the-concept-of-asymmetric-routing/


Break

Types of internet measurements


Passive measurement…

Passive measurement

- We just listen in somewhere
  - At your ISP
  - Your university
  - …

Demo

~~Local WiFi traffic~~

Local Network Traffic


Active measurement...

Active measurement…

- We do something to solicit a (measurable) response
- Example: Traceroutes and RTT measurements, Portscans

Demo

Portscan and RTT measurements

RTT (Round Trip Time)

TU Delft

RTT Measurements

- Send a packet and note down when you sent it
- Ask the recipient to sent a reply
- Check time when the reply comes in

-> You know how long a round trip takes.

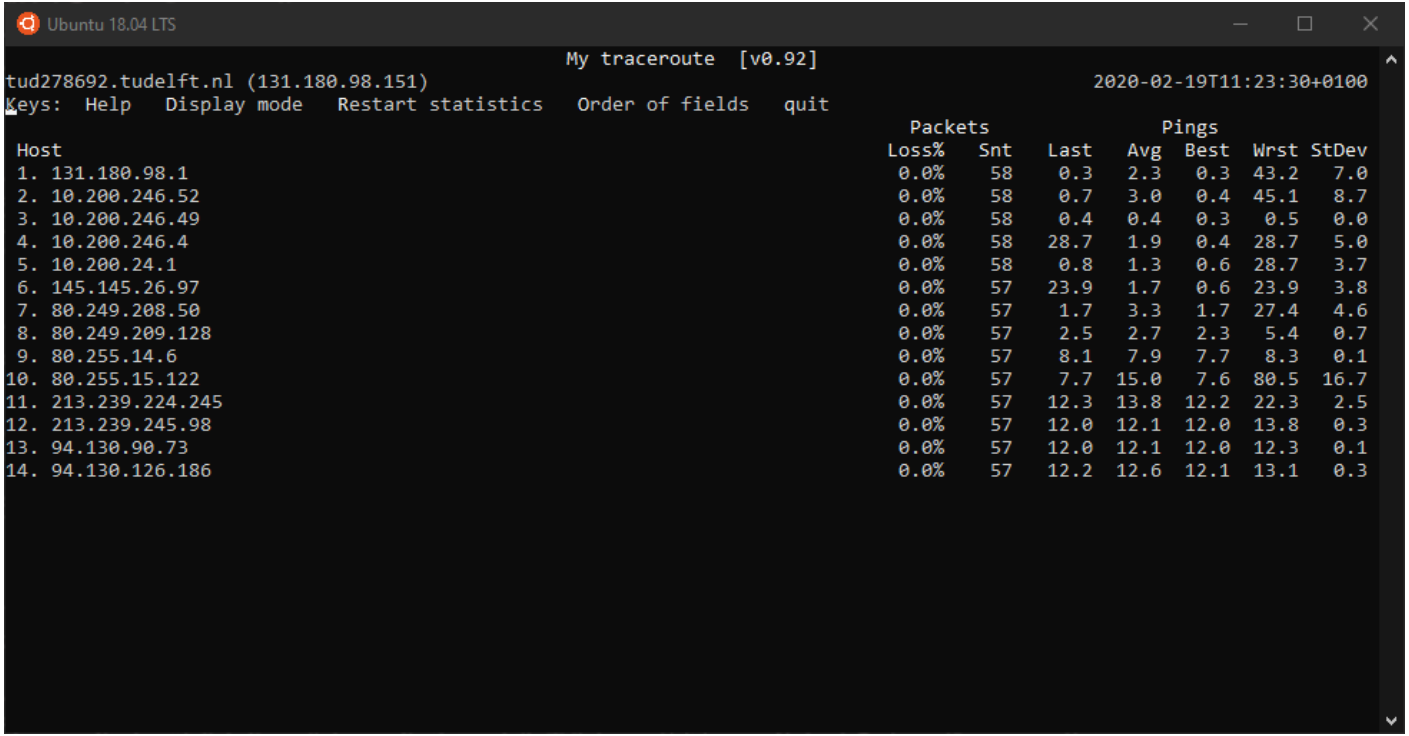
Implications for active (path) measurements

- You never know the return path of your packets
- Hence: We can only do an RTT
- We can guestimate 1-directional TT using a traceroute (by looking at the path RTTs

TTL

- IP Packets come with a TTL field
- Practical default value for the Internet: 64
- Idea:
  - Each host decrements the TTL by 1
  - If the TTL reaches 0, the packet is discarded and the sender notified of the discard
- We can measure the path we take to a destination with it. How?

Traceroutes



Routers are not pingers

- Remote sites might rate-limit ICMP requests
- If you see packets dropping at 8.8.8.8 or at an intermediate router, it might just be that these hosts are currently seeing too many packets
- The actual services (google DNS, packet forwarding) take precedence over ICMP

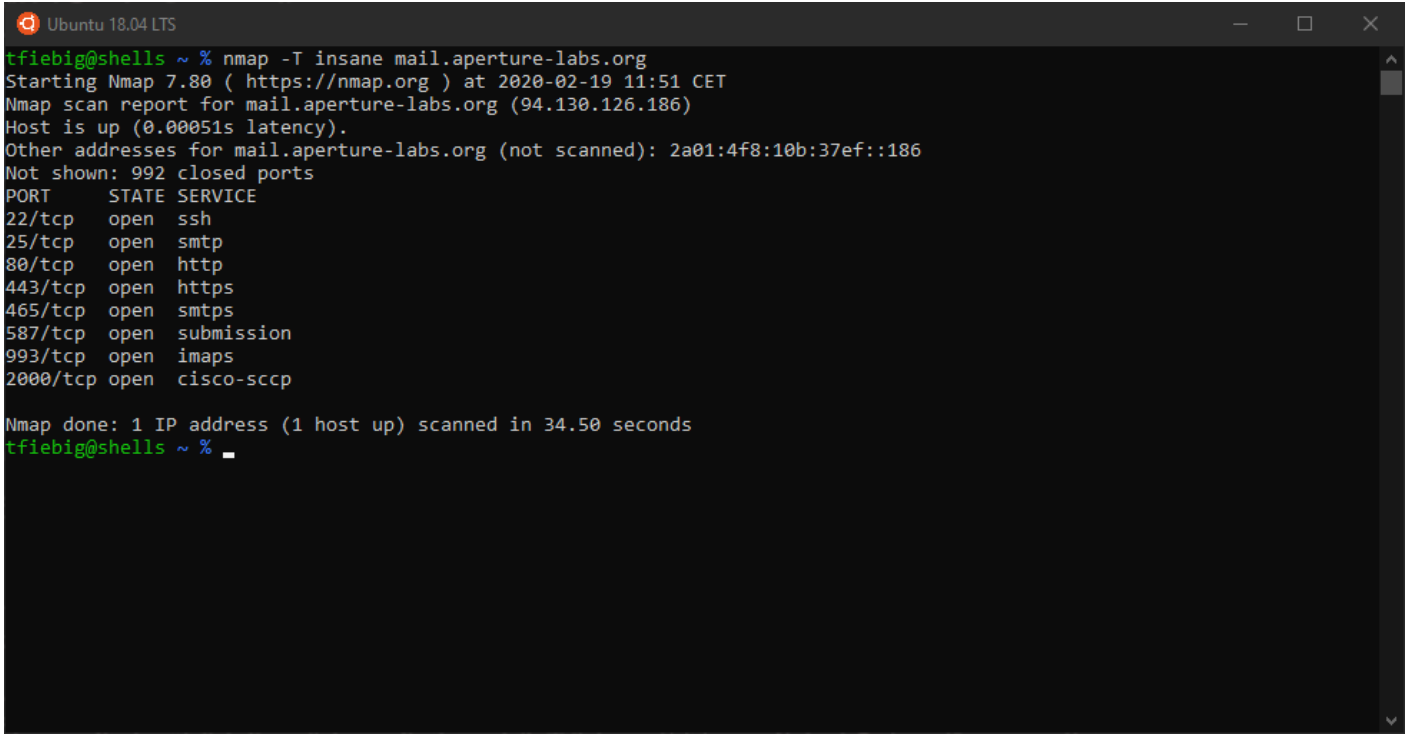
Scanning

- ICMP (Like RTT checks for system liveness)
- Portscans
  - See if a port is reachable
- Banner Scans
  - See what is running on a port

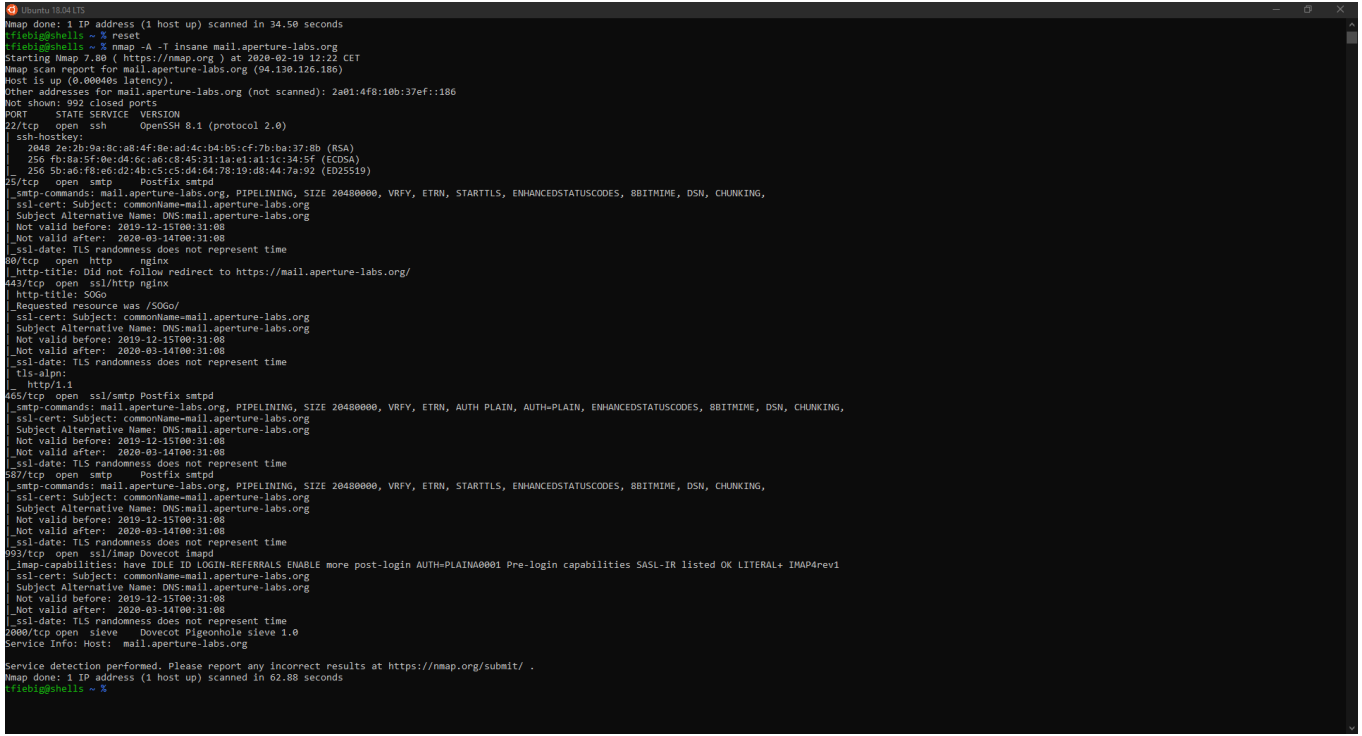
Scanning

- Usually a multi-step process:
  - Check liveness (ICMP)
  - Check if ports are open
  - Do banner scans for open ports

Scanning


Ubuntu 18.04 LTS
tfiebig@shells ~ % nmap -T insane mail.aperture-labs.org
Starting Nmap 7.80 (https://nmap.org) at 2020-02-19 11:51 CET
Nmap scan report for mail.aperture-labs.org (94.130.126.186)
Host is up (0.00051s latency).
Other addresses for mail.aperture-labs.org (not scanned): 2a01:4f8:10b:37ef::186
Not shown: 992 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
80/tcp open http
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
2000/tcp open cisco-sccp
Nmap done: 1 IP address (1 host up) scanned in 34.50 seconds
tfiebig@shells ~ %

Scanning (with banners etc.)



State in scanning

- If we wait for every host to reply, then check ports, then check banners, things get slow
- This works for a /24, but not for 0.0.0.0/0
- Tools like zMap abandon state and just put out packets
- If doing this, be careful what your machine/network/middleboxes can handle (see later)

Scanning IPv6

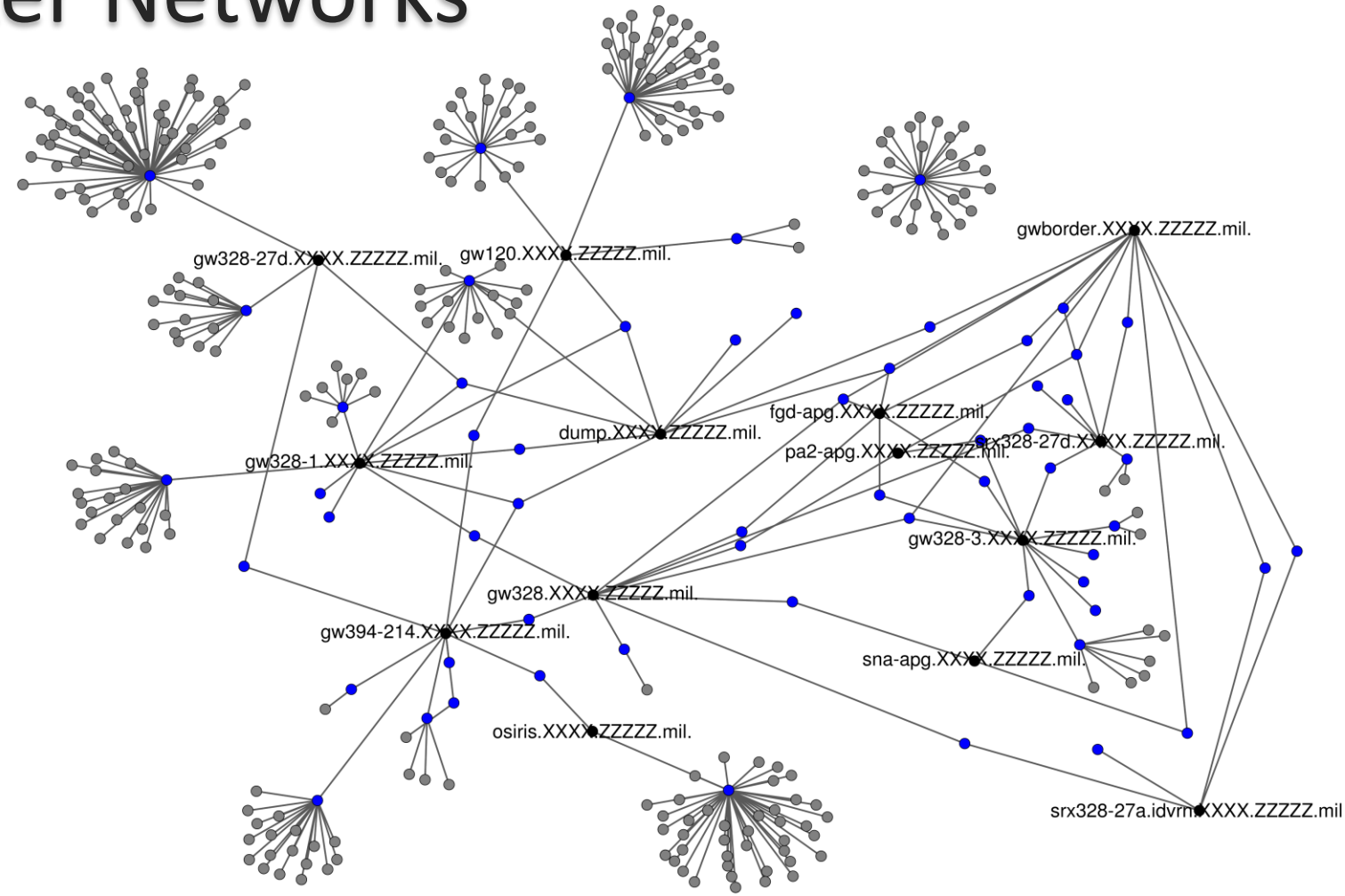
- The 2^{32} addresses in IPv4 are easy
- The 2^{128} in IPv6 are *hard*
- Solution:
  - Generate hitlists
    - Passive measurements
    - Active measurements (DNS/rDNS)
  - Generate scan-targets from hitlists using ‘ML’

Enumerating IPv6 Reverse DNS

- RFC 8020 says ‘NXDOMAIN means nothing there or anywhere thereunder’
- We start with querying, e.g.: 2.ip6.arpa.
- Get a NOERROR instead of NXDOMAIN
  - We know there is something there below, so we can continue with 0.2.ip6.arpa.
- Allows us to prune the search-tree

TU Delft

Computer Networks



TU Delft

Finding the AS to an IP

- Asking the RIRs (you should know this from TB321 (Internet governance lecture)
- Run whois services + there are some collectors
- Under Linux: whois $IP

```
tfiebig@TUD255721 ~ % whois 195.191.196.23
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '195.191.196.0 - 195.191.197.255'

% Abuse contact for '195.191.196.0 - 195.191.197.255' is 'tobias+abuse@fiebig.nl'

inetnum:        195.191.196.0 - 195.191.197.255
netname:        WYBT-NET
remarks:        WYBT-NET assigned PI Space
country:        DE
org:            ORG-wA159-RIPE
admin-c:        WYBT-RIPE
tech-c:         WYBT-RIPE
status:         ASSIGNED PI
```

```
mnt-by:         WYBT-MNT
mnt-by:         LWL-MNT
created:        2016-09-24T12:31:22Z
last-modified:  2016-09-24T12:31:22Z
source:         RIPE

% Information related to '195.191.196.0/23AS51827'

route:          195.191.196.0/23
descr:          wybt.net via AS51827/Fremaks
origin:         AS51827
mnt-by:         FRMA-MNT
mnt-by:         WYBT-MNT
created:        2013-12-09T11:55:54Z
last-modified:  2013-12-09T11:59:07Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.92.6 (ANGUS)
```

TUDelft

```
tfiebig@TUD255721 ~ %
```

Whois data on ASes

- Not always well maintained
- Lengthy to work with…

Looking glasses

- Famous one: https://bgp.he.net/
- Check which networks are announced by which AS

- (Demo)

Finding an AS for a company

- Google
- https://apps.db.ripe.net/db-web-ui/#/fulltextsearch
- Also: https://bgp.he.net/
- And: https://ipinfo.io/countries/nl

GRT

- The GRT (global routing table) is the ‘combined knowledge’ of all BGP routers out there
- It looks different depending on from ‘where’ you look at it
- Different projects aggregate routeviews across the Internet to give you a look at global topology.
  - RIPE-RIS, Routeviews

Practical issues of measurements

Time

- Time is a crucial element
- Deviations as small as a second might make you unable to correlate datasets
- Clocks on computers will not always be accurate

Fixing time

- Bet way forward:
  - Use NTP (Network Time Protocol) to sync time between your nodes
  - Special network measurement cards come with a dedicated time-sync feature (to ensure internal consistency)
  - If you can not NTP sync, you need an RTC

Timezones

- The world is round
- Turns out: This means we do not have the same Time-of-Day everywhere
- This is a great source for confusion
- Make sure to record the time-stamps *and* the time-zones in which you collected data along with it!
- Bet practice: Use UTC. Everywhere.

Storage needs

- Internet measurement data is usually big
- In really common projects you will see dataset sizes of 100s of GB/day or even hour
- Plan your storage needs ahead of time
  - Prevents: Dropping data during the project
- Keep in mind that you also need space for analyzing data!

High PPS (Packets per Second)

- When you are measuring data, you will inevitable run into problems where the link is faster than you can capture
- This can also happen when sending many small packets (being unable to handle the returns; zMap)

Handling high PPS measurements

- There are dedicated measurement cards for these kinds of workloads (e.g., endace) who have their own on-card buffer to allow for, e.g., 100gE line-rate small PPS measurements
- Maybe limit your outbound PPS ☺

You building it right does not mean that it works

- Monitor your measurements
- Make sure they keep running and recording data
- Make sure they record the right data
- Make sure to also save intermediate state.
  - There is nothing more frustrating than running a 1 week measurement job, where you throw away intermediate data, and had a typo in your final aggregation.
- Have some kind of progress/state indicator

TU Delft

Vantage points

- In network measurement, we call the place (from) where we measure a vantage point
- In passive measurements, this is the place where we snoop data
- In active measurements, this is the place from where we originate requests

Question

Does the vantage point matter for active measurements?

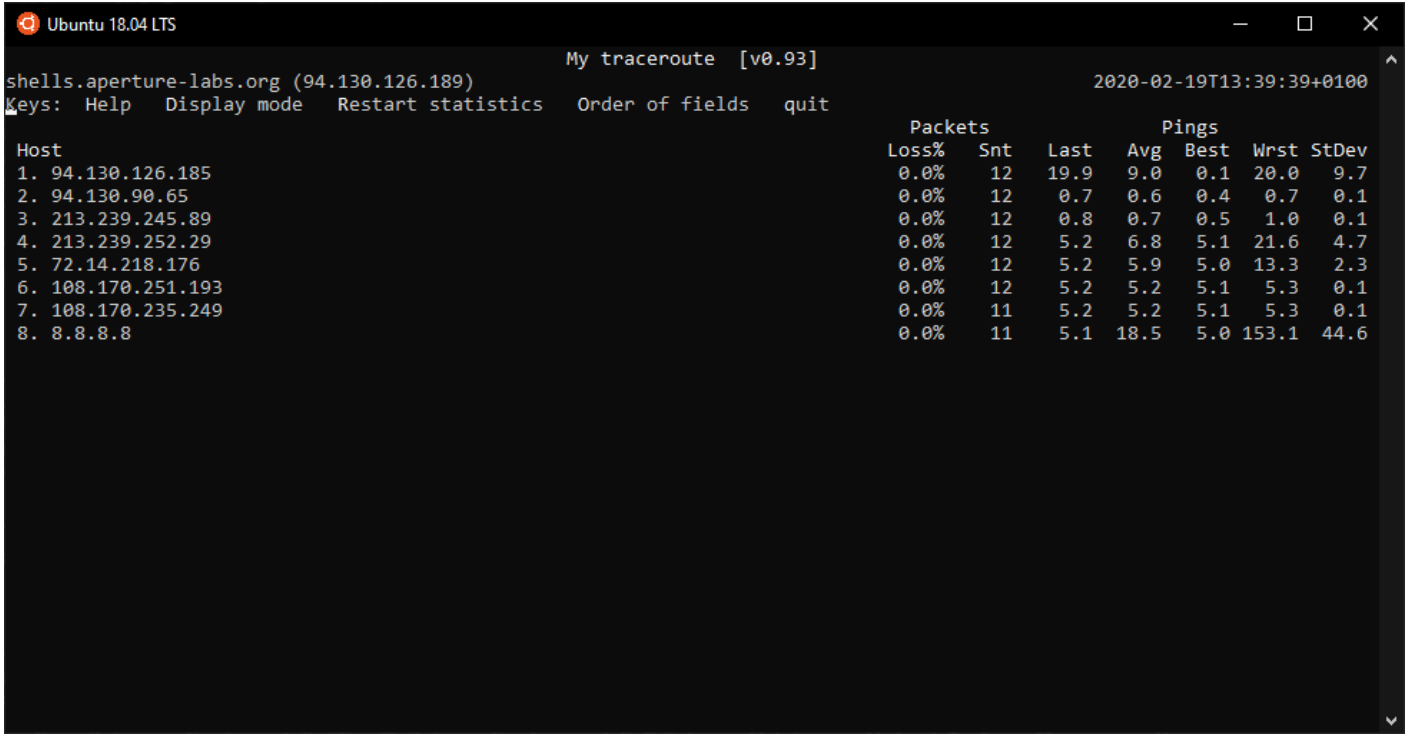
Vantage points matter

- Our view on the Internet might be different, depending on from where we measure
  - BGP views/paths will differ.
  - RTT to a service in SFO is a lot quicker from LAX than from AMS
  - DNS often has location dependent replies
  - Anycast is a thing

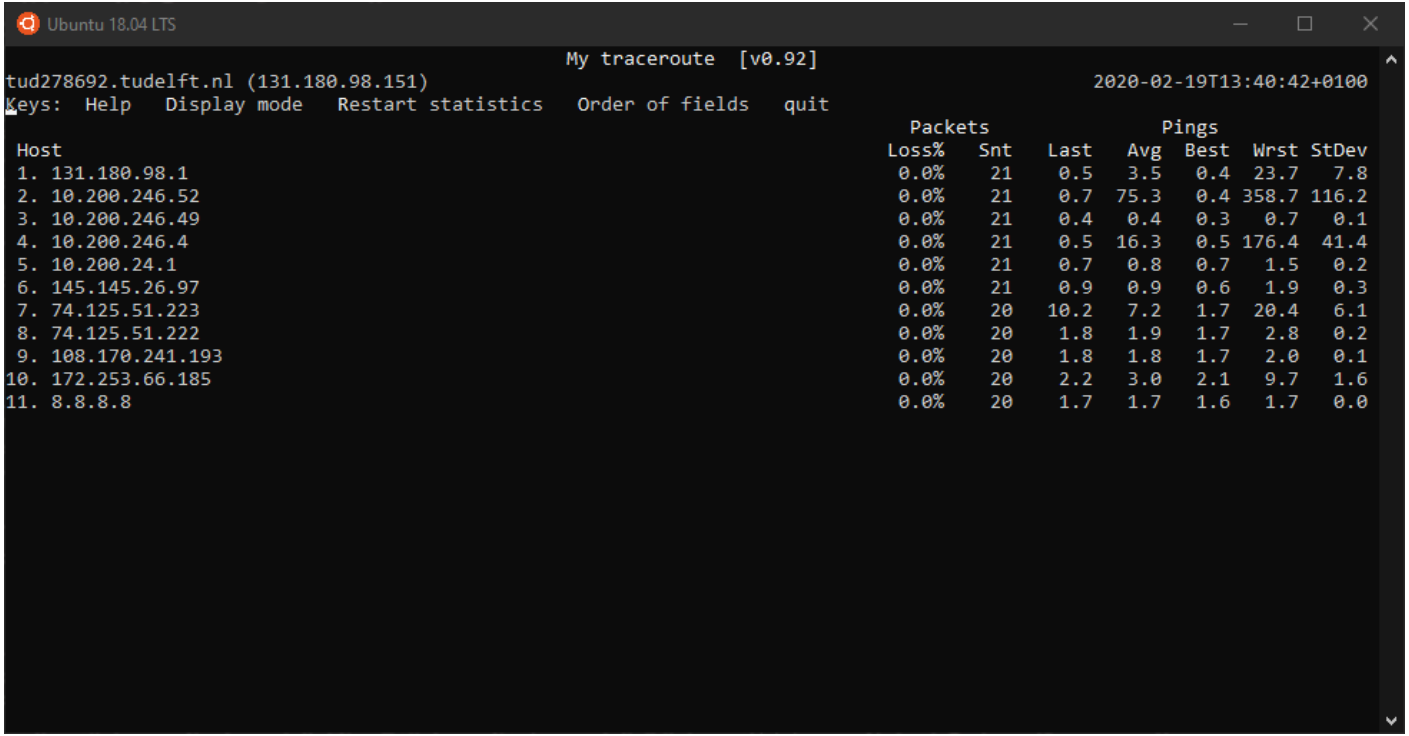
Vantage points matter

- There will be things ‘special’ about our local network
- These can have an impact on our measurements

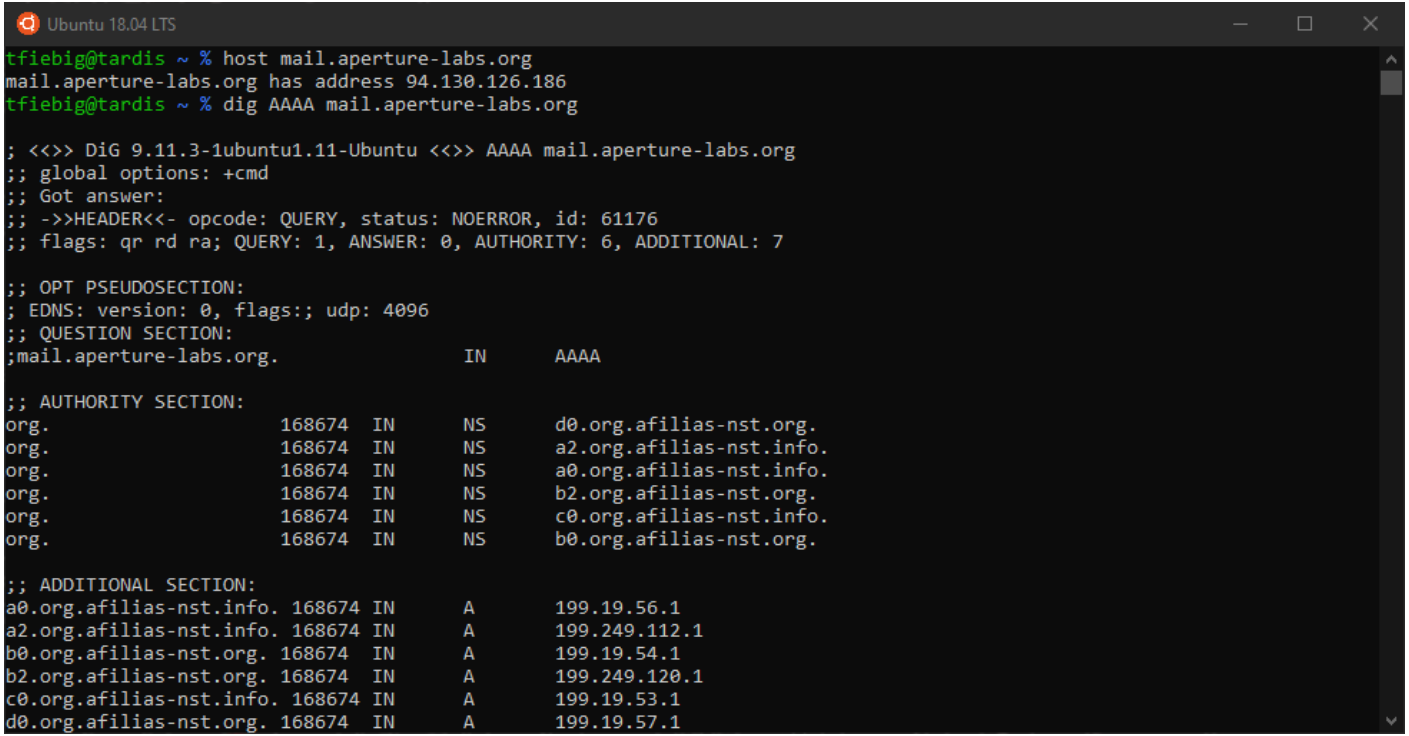
8.8.8.8 from Hetzner



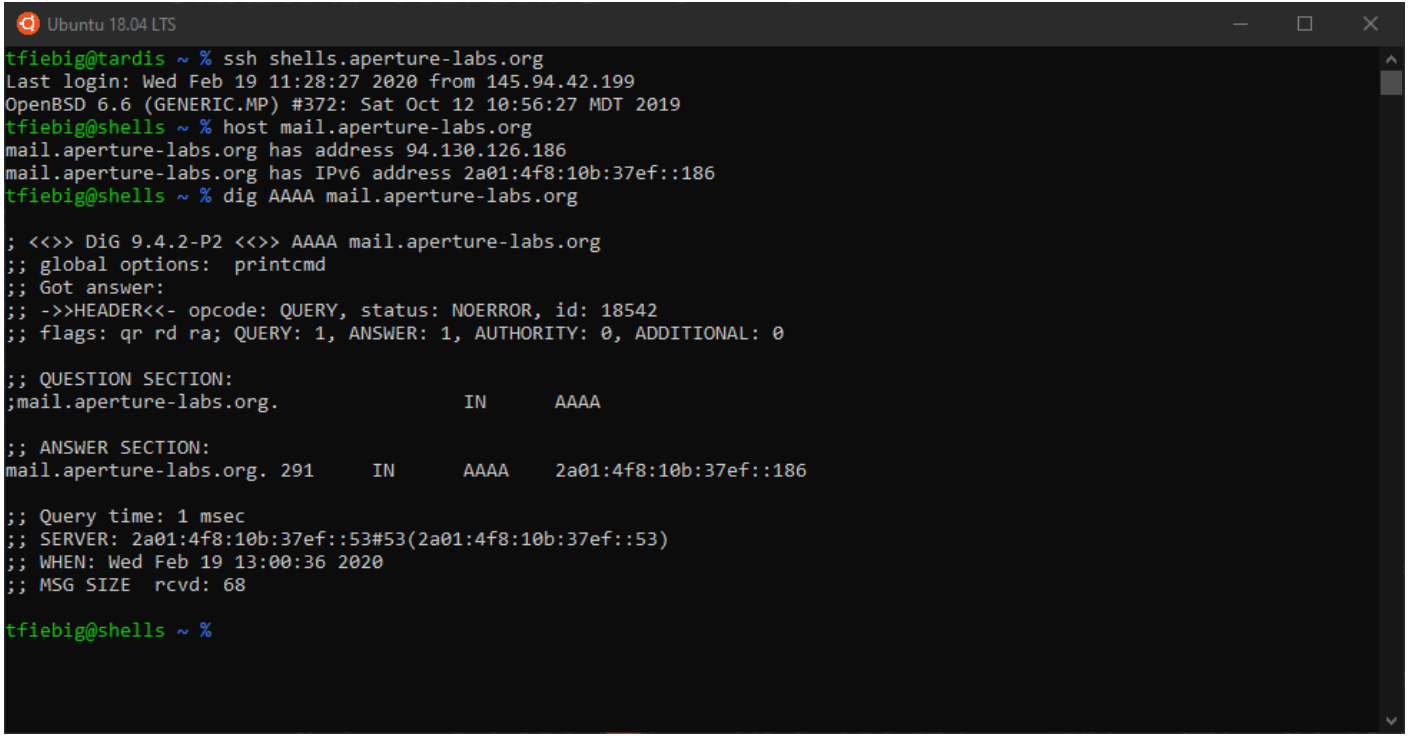
8.8.8.8 from TU Delft



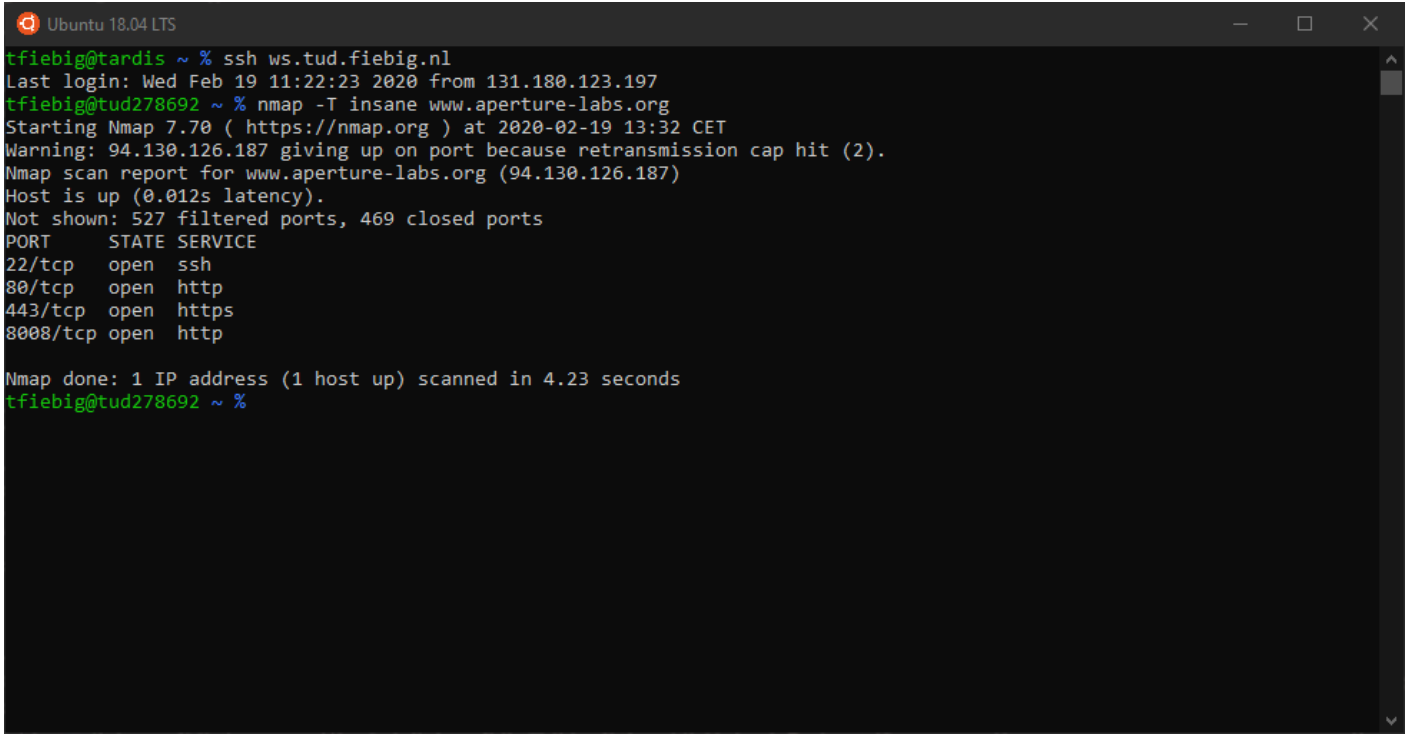
DNS Interception



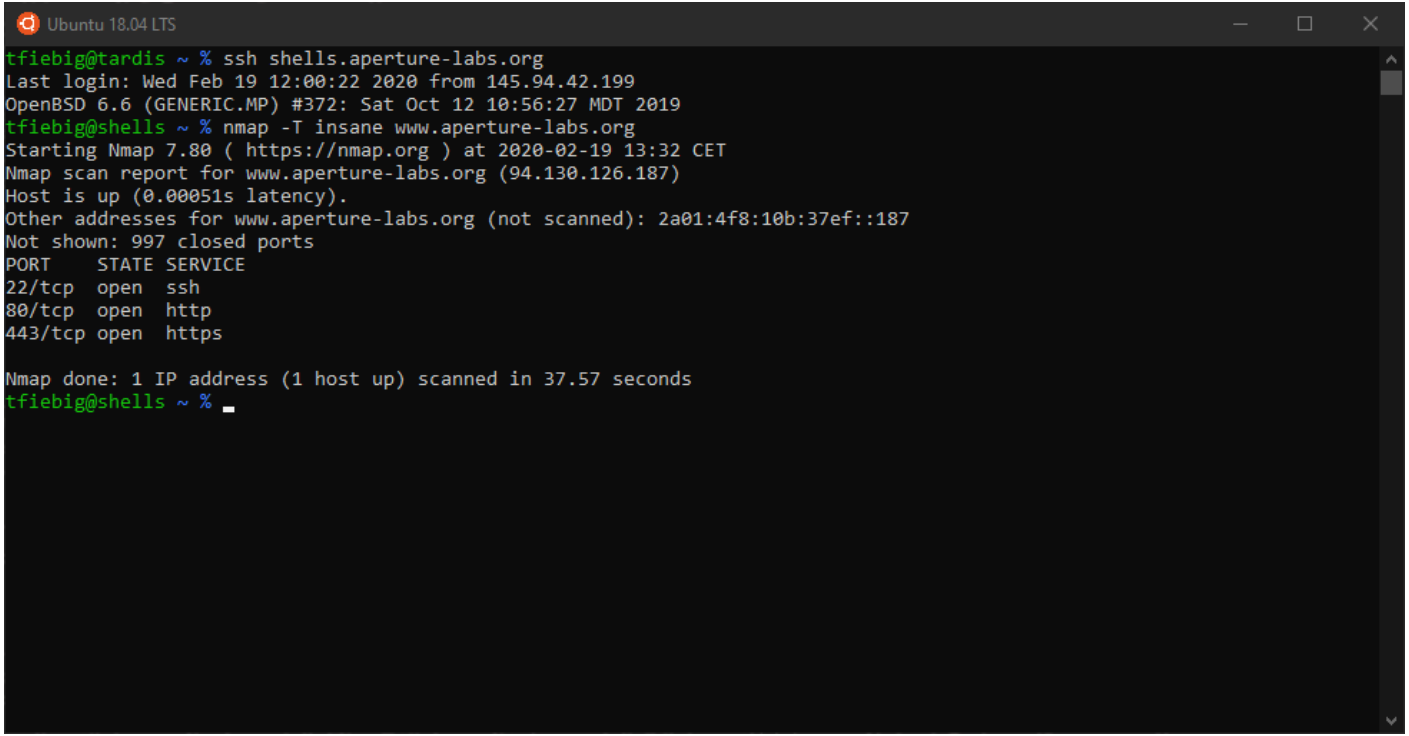
DNS Interception



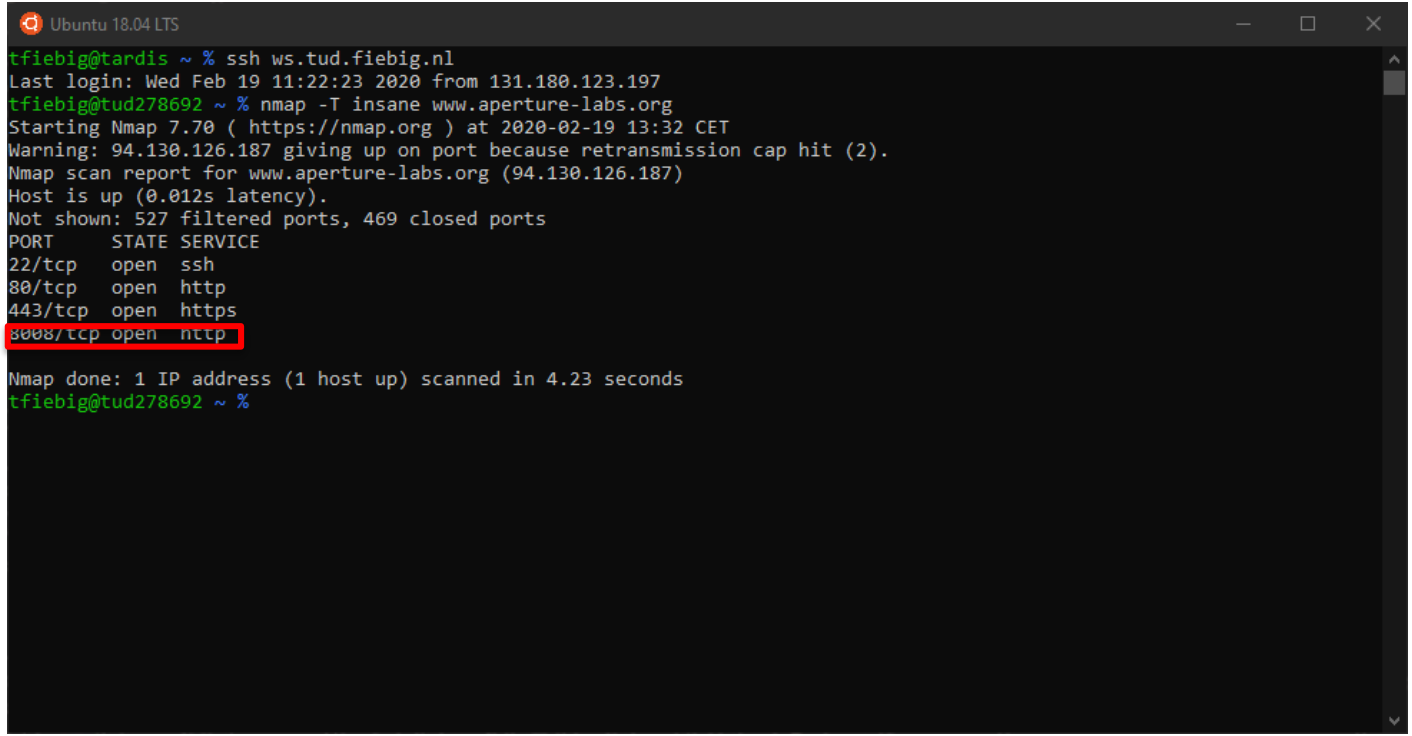
Funny Middleboxes



Funny Middleboxes



Funny Middleboxes



Funny Middleboxes

- First problem is TU Delft's DNS servers filtering all AAAA/IPv6 related queries
- Second problem is TU Delft using a standard censorship/user-monitoring system to observe users' web-access for security reasons
- Middleboxes/firewalls may also filter things

Blowing up state

- Firewalls/Middleboxes are often stateful
- Means: For each packet/connection they record state
- These state-tables have a limited size
- If one client, e.g., zMap's the Internet, the state table blows up and the network goes down

In general: Watch out for bottlenecks

- Your local DNS cache might get overloaded by your queries
- An upstream network provider might get congested
- The site you are measuring (when web-scraping) might go down
- Etc.

Being a good netizen

Six rules to less hazzle…

1. Rule: If you do measurements, involve you HREC

- Collecting data (active or passive) always has ethical constraints with it
- Involve your Human Research Ethics Council and get their approval
- If you do not have one, follow the Menlo report
  - https://en.wikipedia.org/wiki/Menlo_Report

2. Rule: Ensure data is protected

- FDE on research devices (especially if mobile)
- Proper anonymization if you share data
- Proper wiping of old disks etc.

3. Rule: Involve your local IT

- Internet measurements may impact your local network
- Tell your IT what you do, and get approval from them
- If they know what you are doing, they will be less pissed if you break something
- Also: They are the best ones to tell you what kind of funny middle boxes they run

TU Delft

4. Rule: Provide information on your measurement systems

- Set an informative reverse DNS entry on the involved hosts
- Have a website on these hosts explaining your research, how to opt out (see next slide), whom to contact in case of problems etc. Have the website on what the name resolves to as well

5. Rule: Provide an opt-out mechanism

- People will not like it, if you scan their network
- Integrate a mechanism in your process, which allows them to ‘opt-out’, i.e., be no longer visited by your scans in the future
- Make sure that mechanism works

6. Rule: Be nice to the network

- You will cause load on networks (local/remote)
- Make sure you do not hurt smaller networks due to too many packets/bandwidth being inbound
- If you are doing higher-level protocol scans, other load considerations and bottlenecks apply!