RIPE NCC
RIPE Atlas

Studying DNS Infrastructures

Guillaume Bonnoron, Damien Crémilleux, Sravani Teja Bulusu, Xiaoyang Zhu
Support: Guillaume Lavadon, ANSSI

October 28, 2016

REDOCS 2016

Contents

1. Introduction

2. Our Experiments

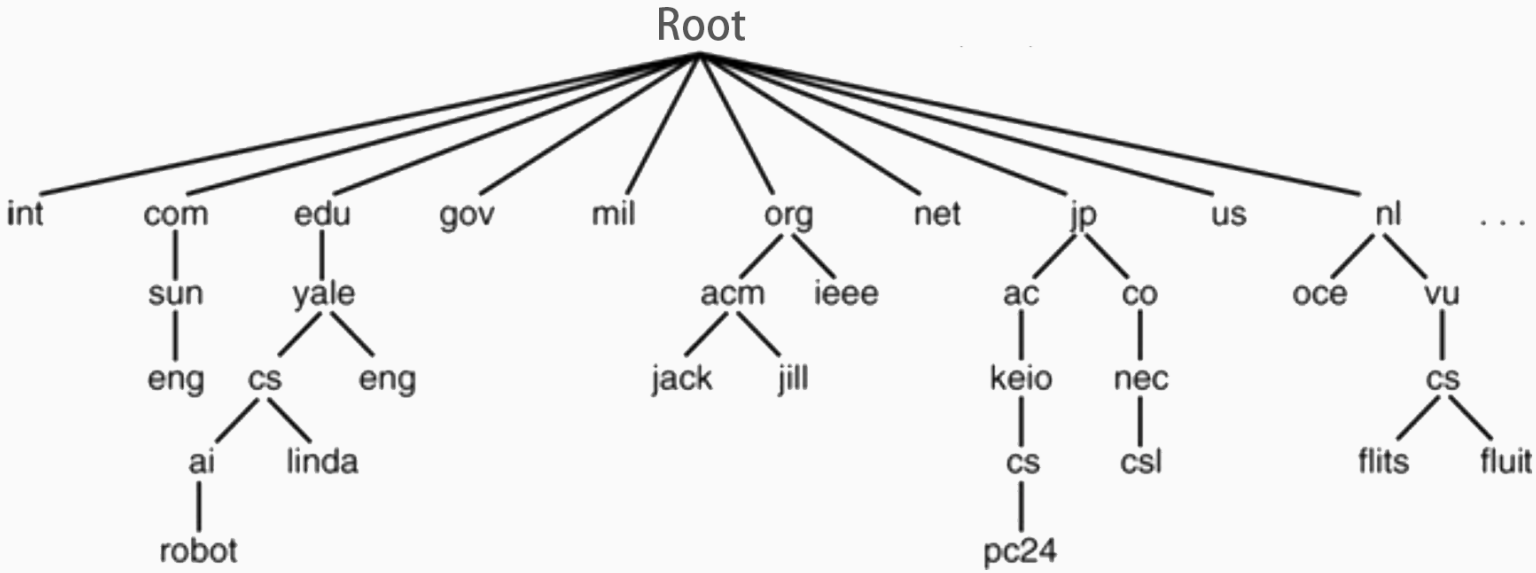
3. Detailed Analysis

4. Conclusion

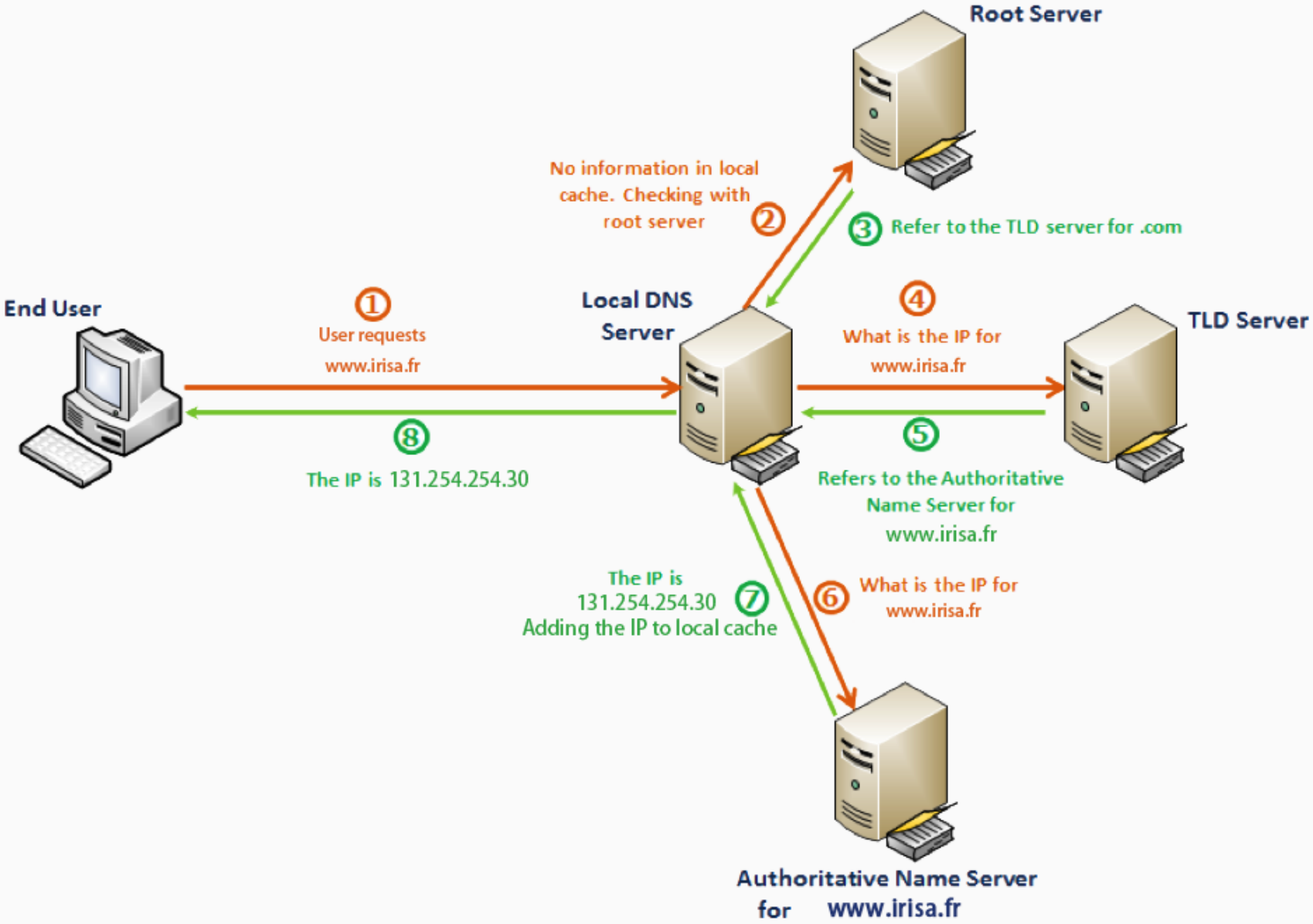
Introduction

Domain Name Space (DNS)

1. Translating more readily memorized domain names to the numerical IP addresses (www.google.fr $\leftrightarrow$ 74.125.206.94)
2. A hierarchical decentralized naming system

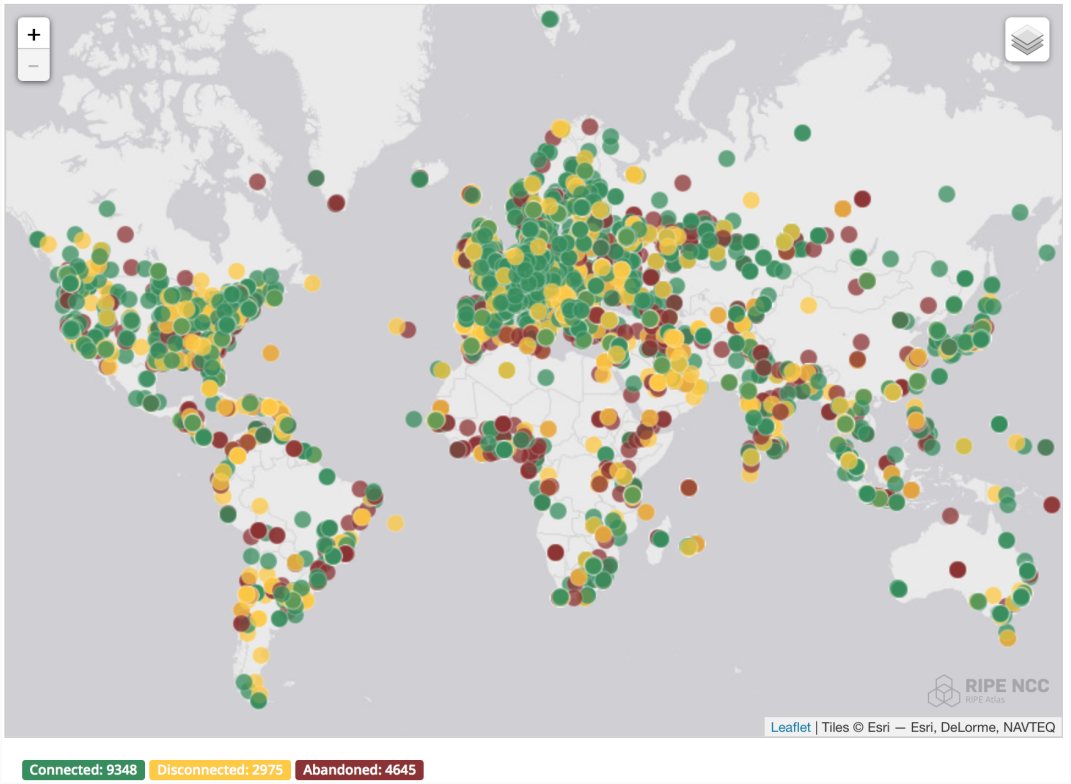


Use Case


Root Server
No information in local cache. Checking with root server
2
3
Refer to the TLD server for .com
End User
1
User requests www.irisa.fr
Local DNS Server
4
What is the IP for www.irisa.fr
TLD Server
8
The IP is 131.254.254.30
5
Refers to the Authoritative Name Server for www.irisa.fr
The IP is 131.254.254.30
Adding the IP to local cache
7
6
What is the IP for www.irisa.fr
Authoritative Name Server for www.irisa.fr

RIPE Atlas and Probs

RIPE Atlas is the RIPE NCC's **Internet data collection system**, which is composed of probes and anchors all over the world.



Probes actively take measurements, including:

- Ping
- Traceroute
- DNS
- SSL/TLS
- NTP

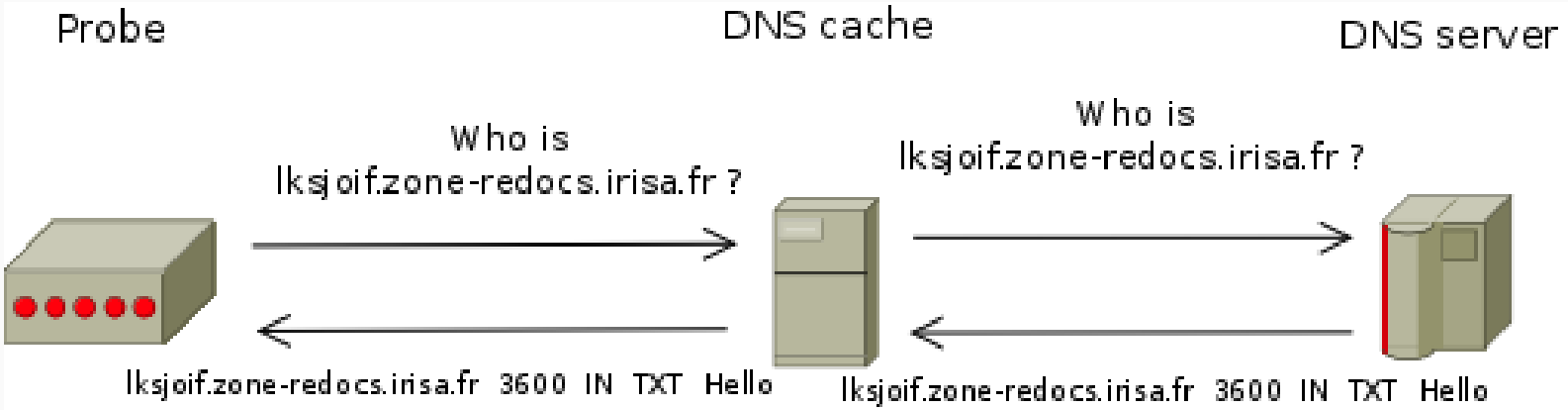
Issues

We want to discover

- the number of queries generated
- the structure of DNS caches
- the differences between ISPs
- and just explore the data to discover patterns

Our Experiments

Simple Example



1. Development of simple DNS server program (`python`)
2. Handle the measurements
   - Creation of script to give tasks to probes (`python` API)
   - Another script to retrieve the measurement result (`python` API)
   - Several analysis scripts (well... `python` again ;-))

Scale of the experiment

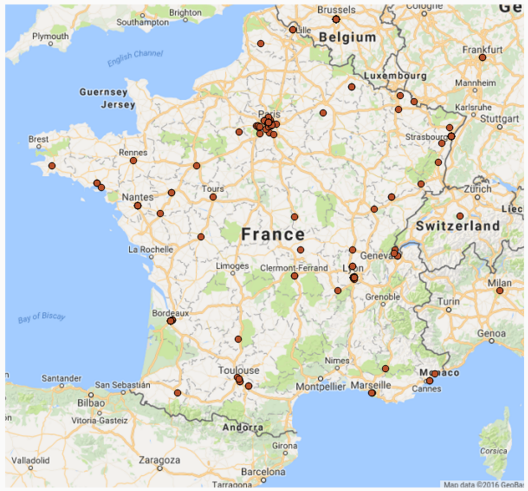
France - about 1h

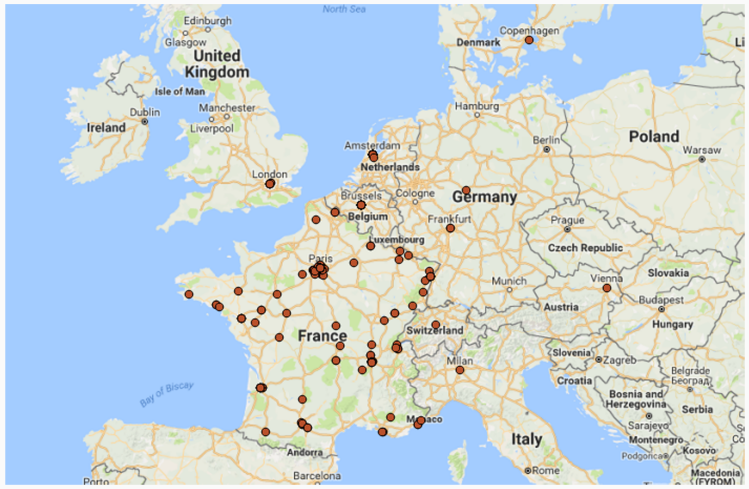
- 724 connected probes
- 651 usable probes
- 1 109 queries made by the probes
- 1 198 queries received at our DNS server

World - about 7h

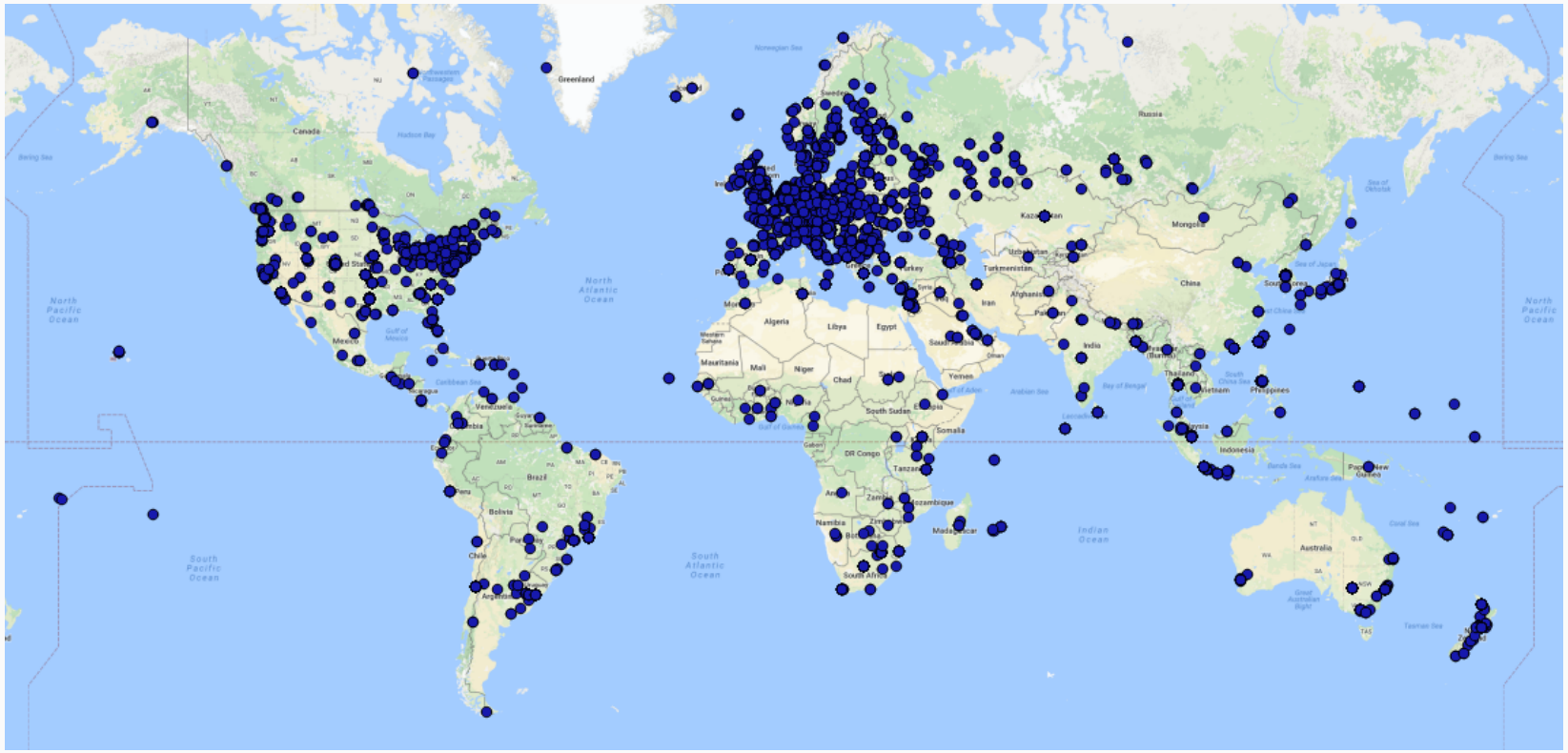
- 9 352 connected probes
- 8 605 usable probes
- 15 024 queries made by the probes
- 15 161 queries received at our DNS server

DNS caches used by French probes





DNS caches used by all probes



Detailed Analysis

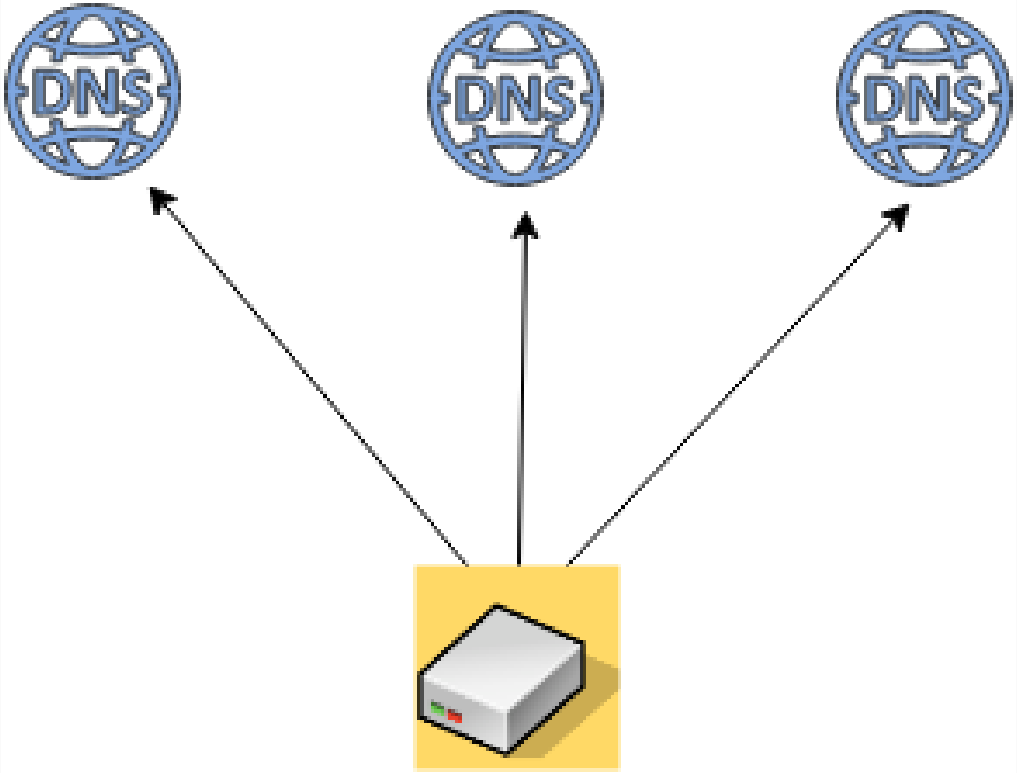
Patterns study

- We had a few cases to test
- When looking for them we found new behaviours

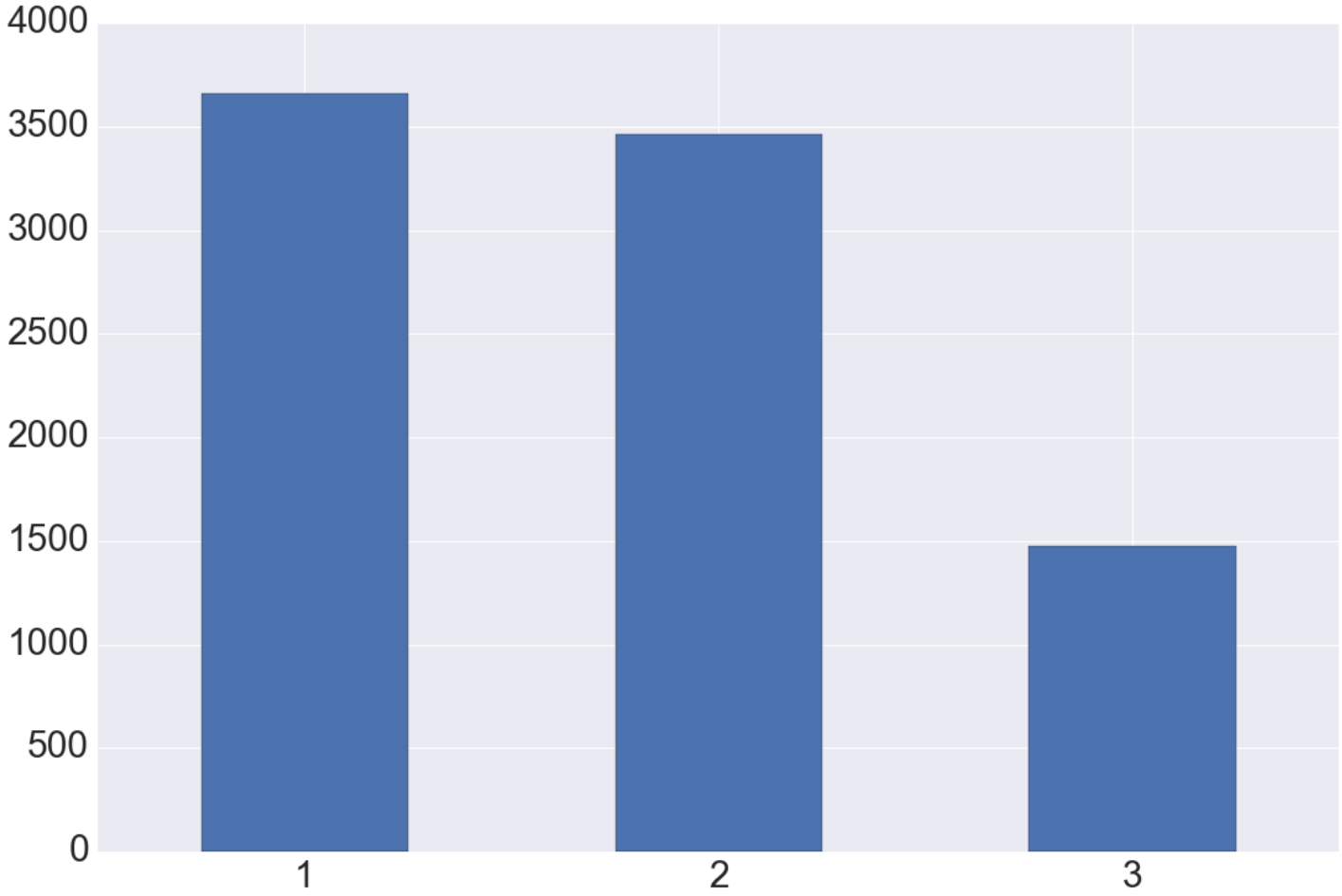
Currently: 6 different studied

Pattern 1

The probe queries explicitly 1, 2 or 3 DNS caches.



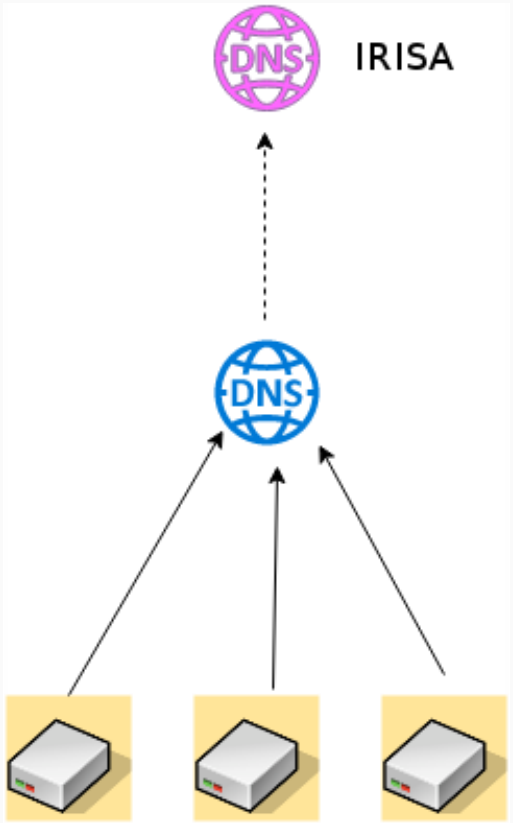
Pattern 1



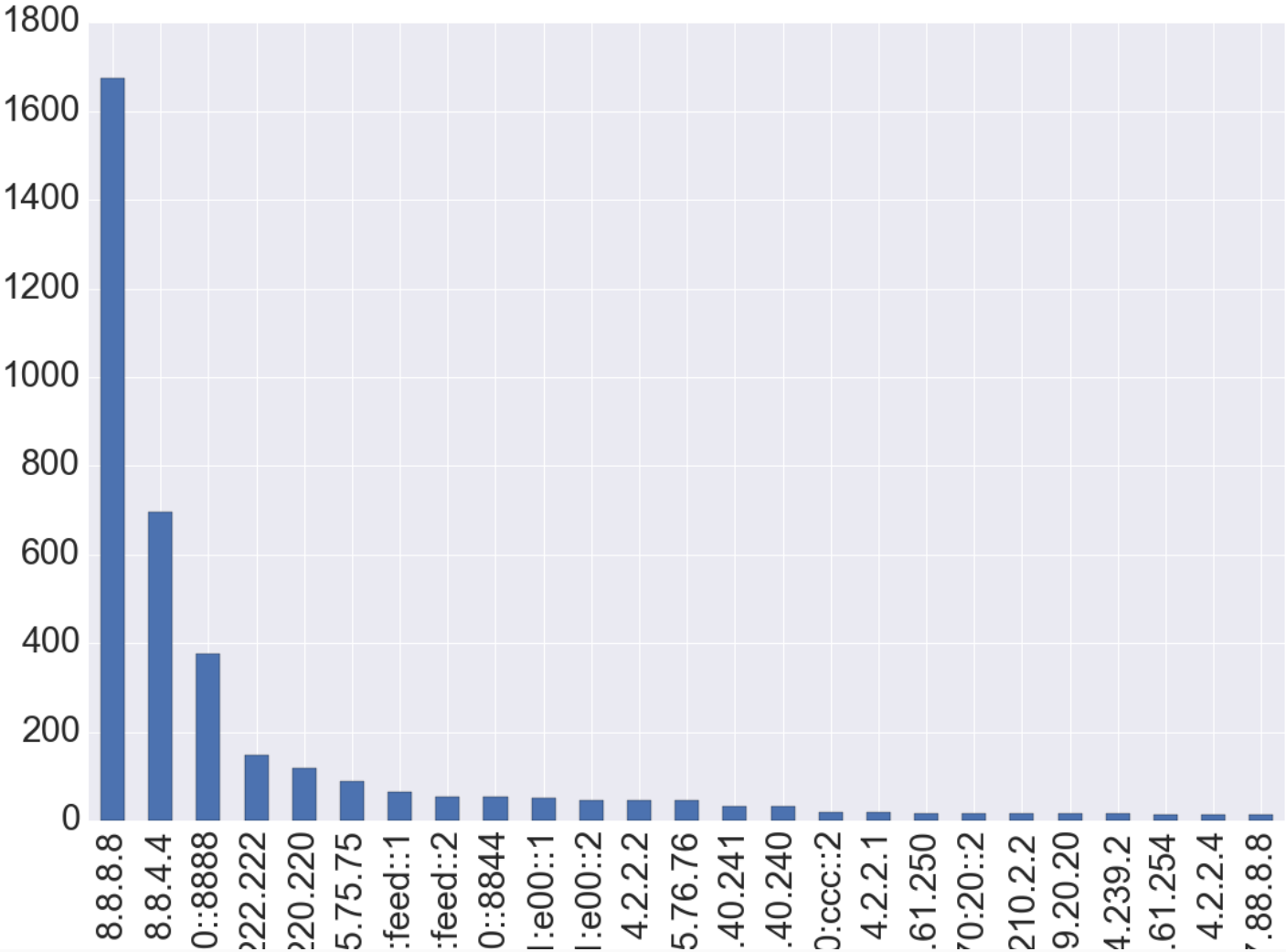
Number of queries for one probe

Pattern 2

Several probes use the same cache.



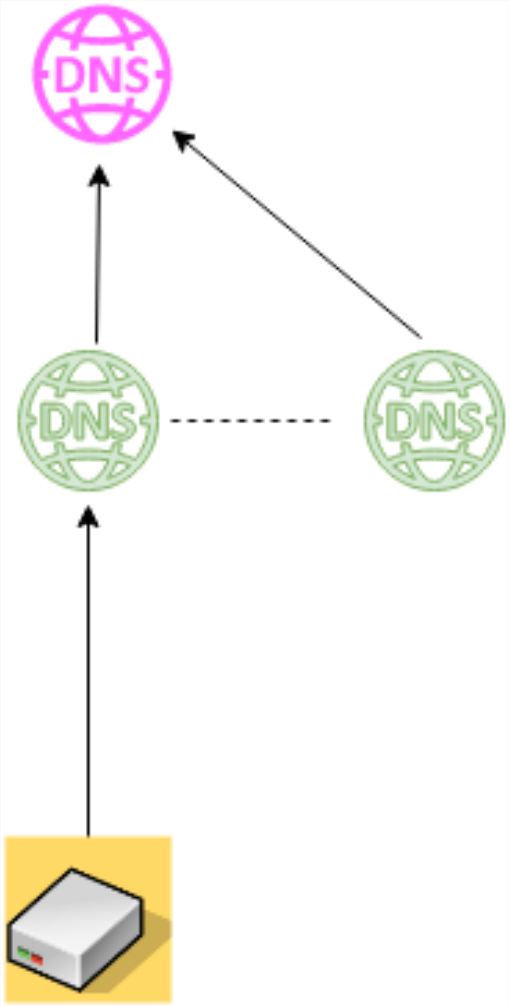
Pattern 2 - 51.6 % are Google!



DNS caches used

Pattern 3

One probe uses 1 cache and trigger queries from other caches



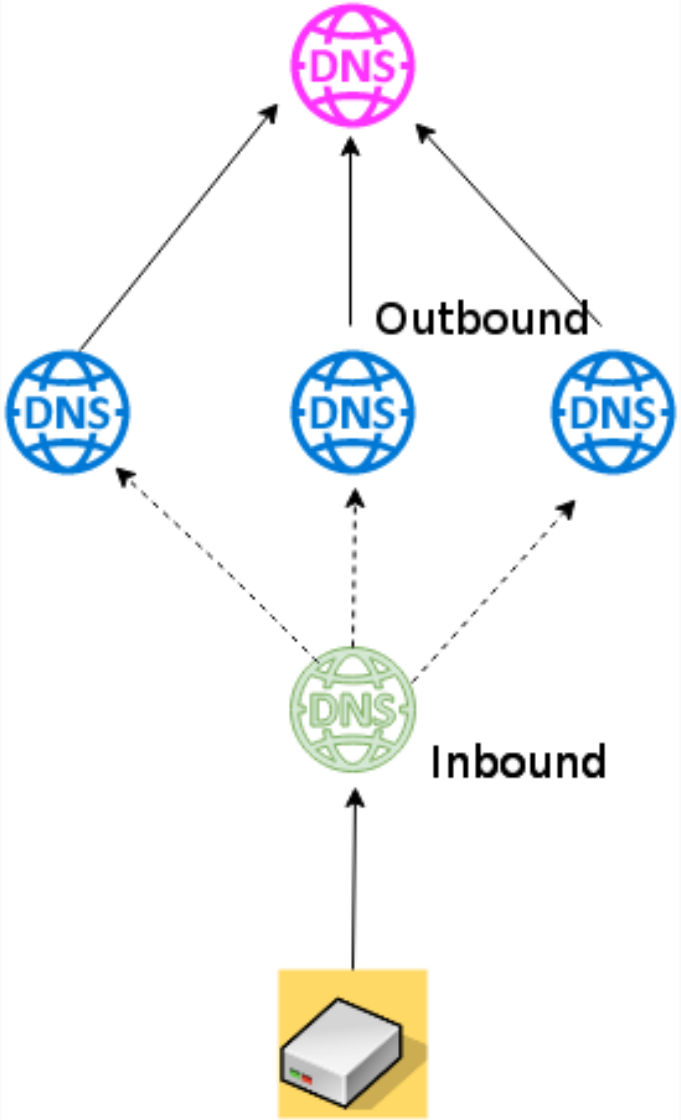
Pattern 3

- Number of DNS caches queries per probe: 1.0692
- Top amplification

Probe id	Probe queries	DNS cache queries
121	1	29
23857	1	26
17382	2	19
12155	2	17
3189	2	12

Pattern 4

N-layers caches, with load-balancing

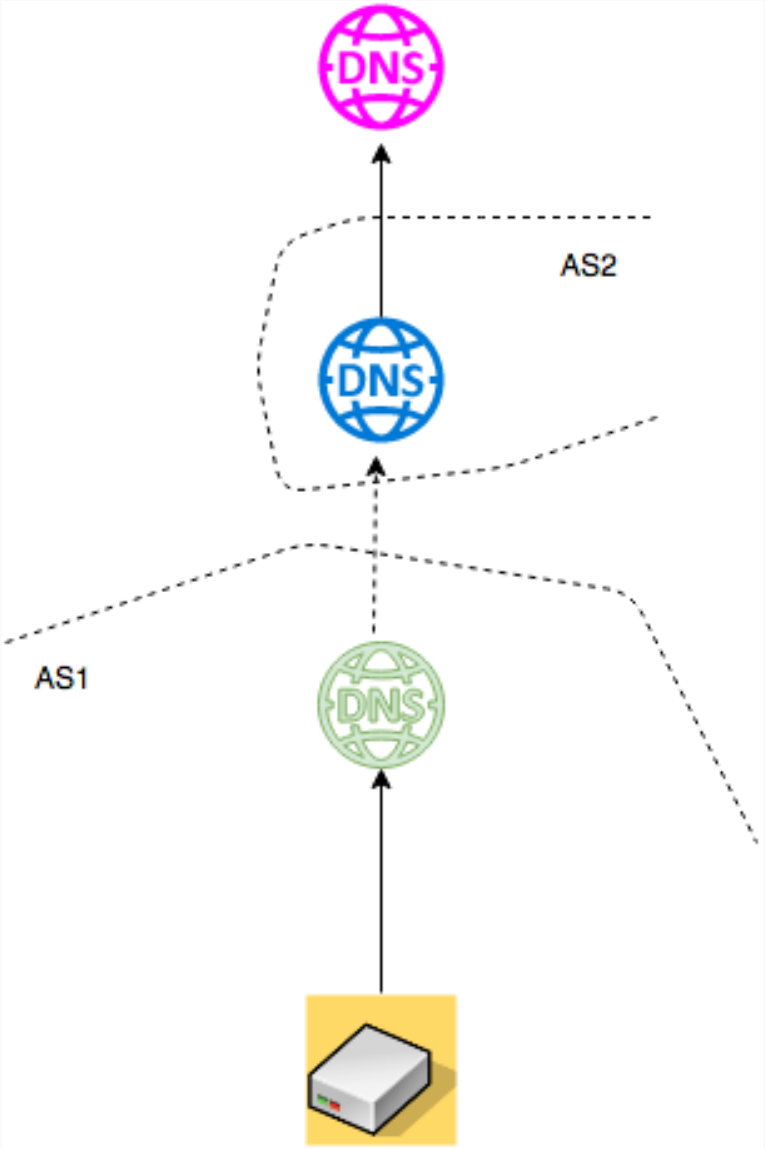


Pattern 4

- number of inbound DNS caches : 281
- number of outbound DNS caches : 1 024

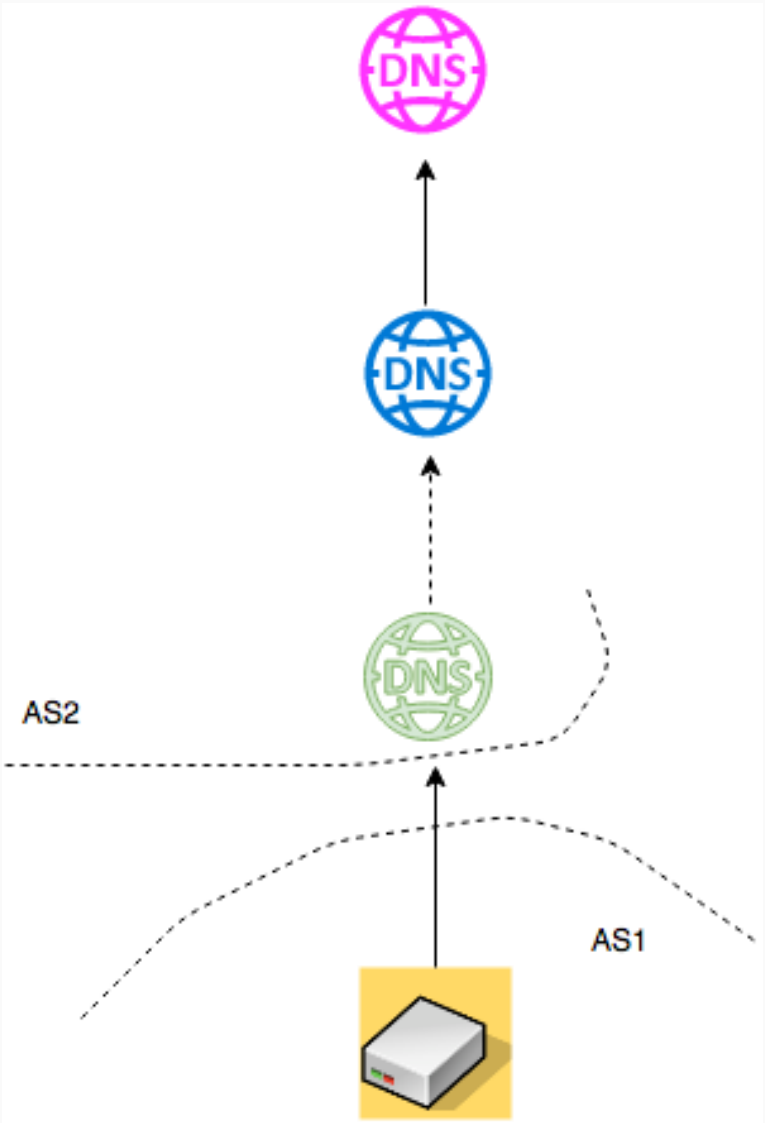
Pattern 5: 1263 probes

An ISP DNS cache asks to another ISP DNS cache



Pattern 6: 2624 probes

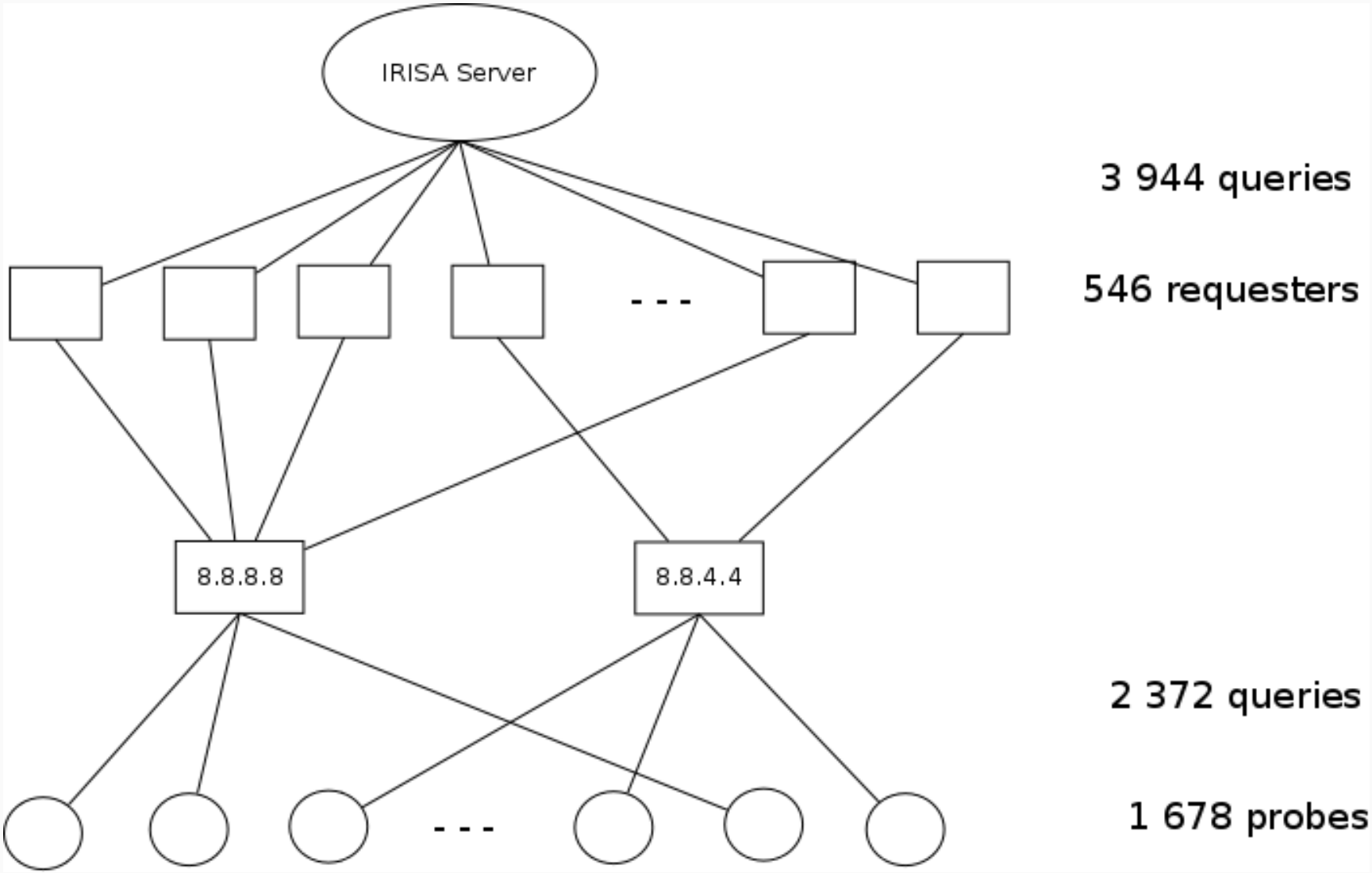
Probe IP and DNS local IP are in different AS



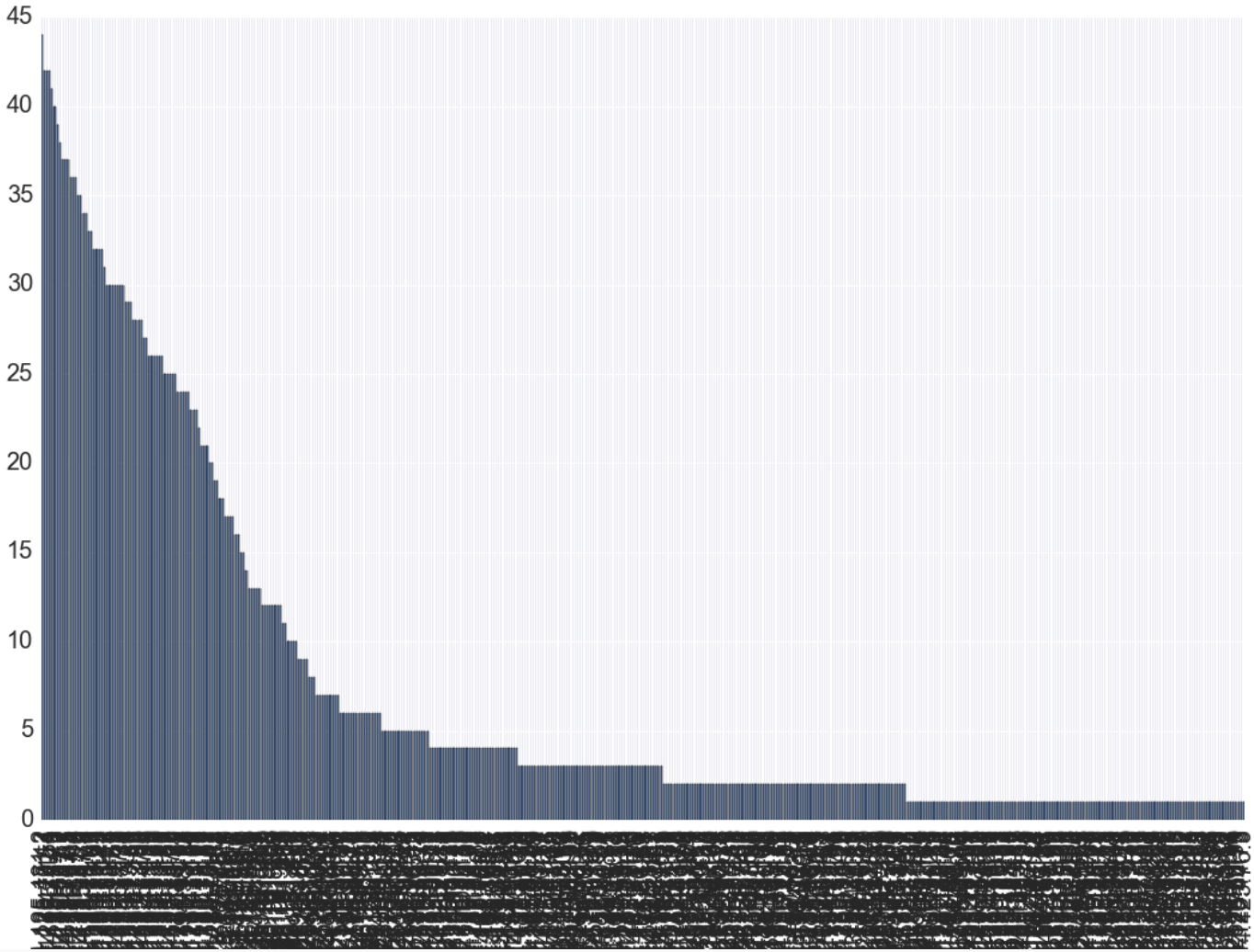
Google

- Number of DNS caches for Google: 546
- Number of queries from Google: 3 944

Google

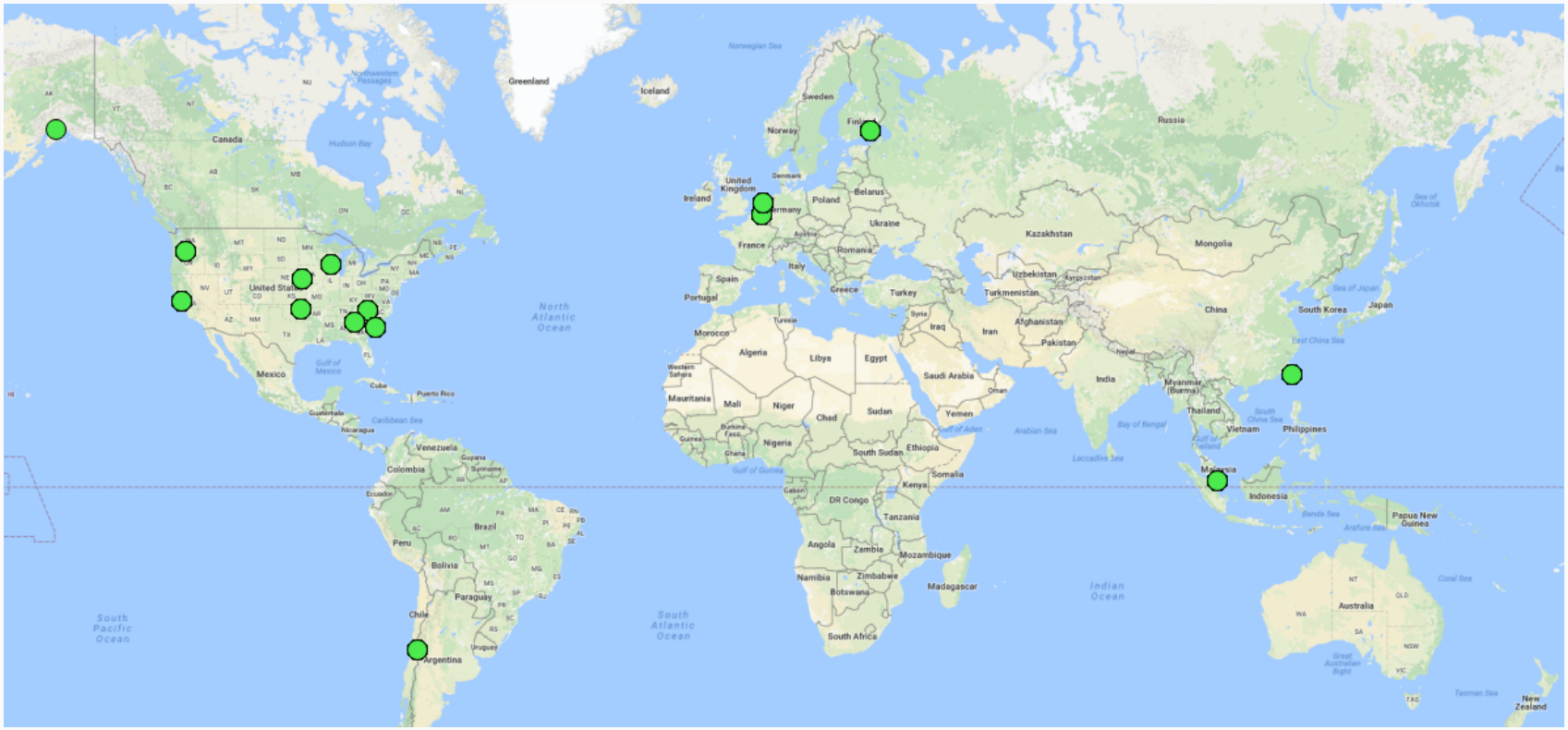

IRISA Server
3 944 queries
546 requesters
8.8.8.8
8.8.4.4
2 372 queries
1 678 probes

Google



Distribution of the queries per DNS cache

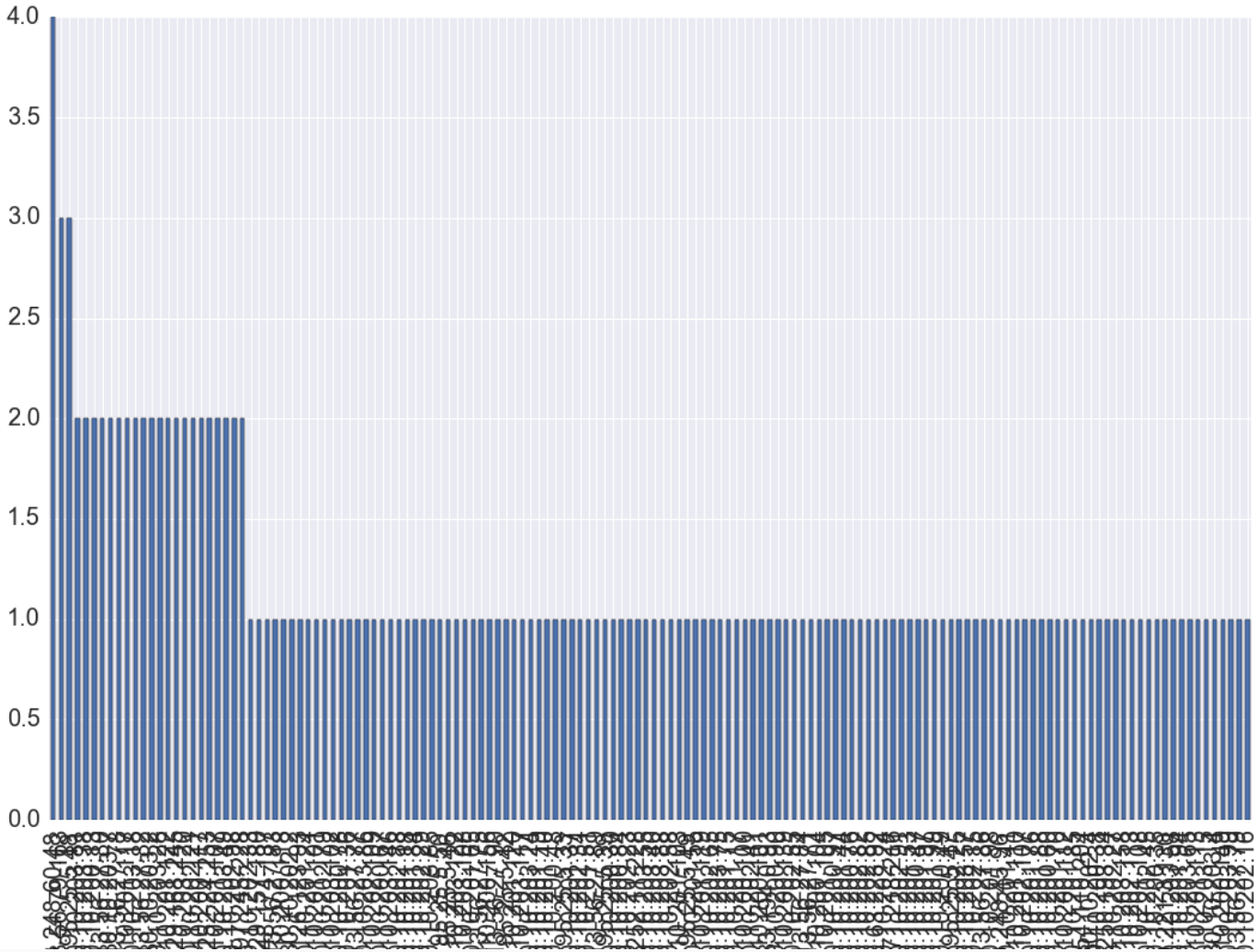
Google


Greenland
Iceland
Canada
Russia
Sweden
Norway
Finland
United Kingdom
Ireland
Poland
Belarus
Ukraine
France
Romania
Italy
Spain
Portugal
Greece
Turkey
Kazakhstan
Mongolia
Uzbekistan
Turkmenistan
China
South Korea
Japan
Afghanistan
Iraq
Iran
Pakistan
India
Morocco
Algeria
Libya
Egypt
Saudi Arabia
Mauritania
Mali
Niger
Chad
Sudan
Yemen
Myanmar (Burma)
Thailand
Vietnam
Philippines
Malaysia
Indonesia
Nigeria
South Sudan
Ethiopia
Somalia
Kenya
DR Congo
Tanzania
Angola
Zambia
Mozambique
Namibia
Zimbabwe
Botswana
Madagascar
South Africa
Australia
Papua New Guinea
New Zealand
Mexico
Venezuela
Colombia
Brazil
Peru
Bolivia
Paraguay
Chile
Argentina
North Atlantic Ocean
South Atlantic Ocean
South Pacific Ocean
Indian Ocean

Orange

- Number of DNS caches for Orange: 146
- Number of queries from Orange: 174

Orange

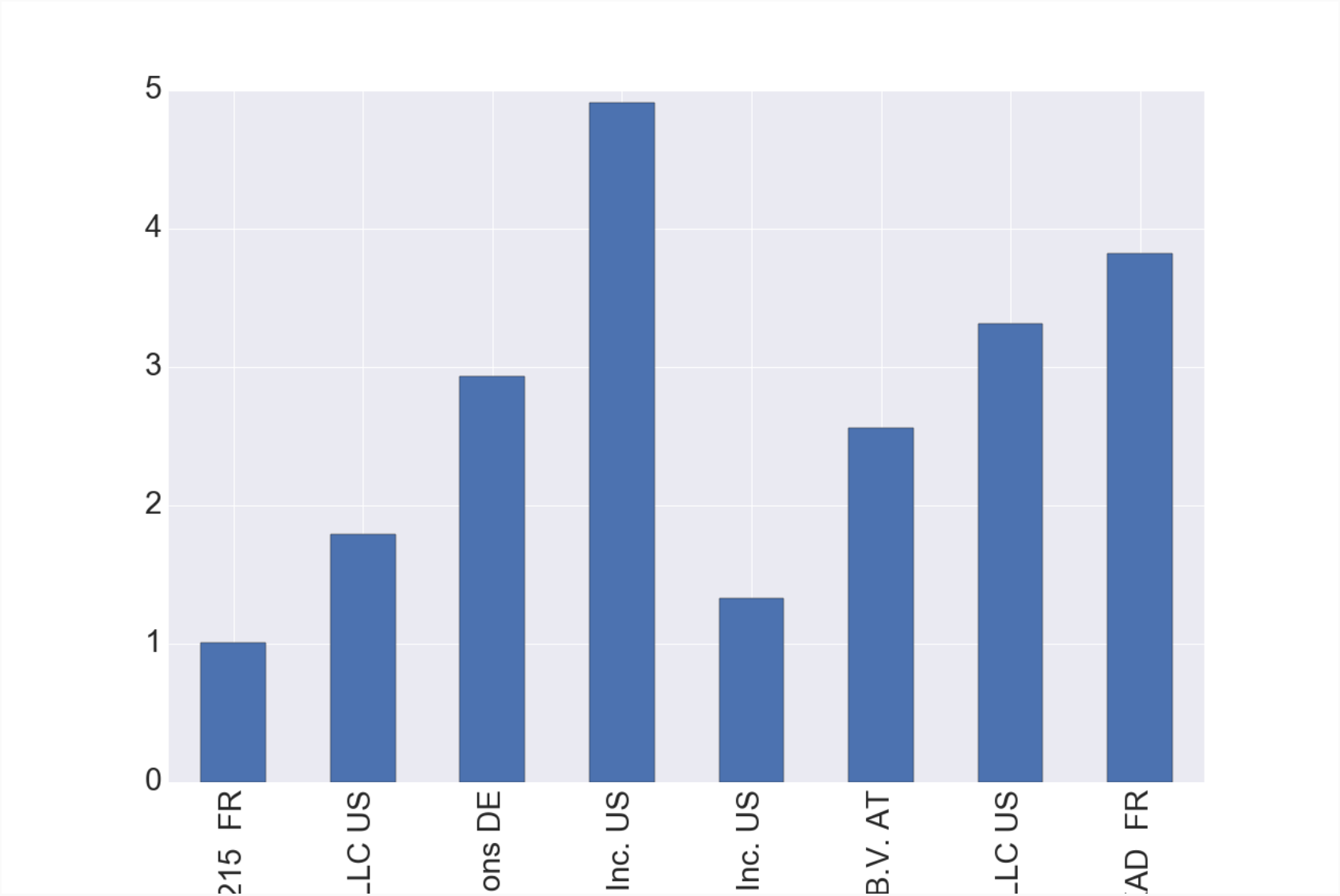


Distribution of the queries per DNS cache

Orange

Belgium
France
Switzerland
Paris
Versailles
Le Havre
Rouen
Amiens
Caen
Reims
Metz
Nancy
Strasbourg
Troyes
Orleans
Le Mans
Tours
Angers
Nantes
Rennes
Brest
Quimper
Lorient
Vannes
St-Malo
Dijon
Besançon
Bourges
Poitiers
Niort
La Rochelle
Limoges
Angoulême
Bordeaux
Bergerac
Périgueux
Brive-la-Gaillarde
Clermont-Ferrand
Vichy
Lyon
Saint-Étienne
Grenoble
Chambéry
Annecy
Geneva
Lausanne
Bern
Zürich
Basel
Turin
Valence
Avignon
Nîmes
Montpellier
Marseille
Nice
Cannes
Toulon
Aix-en-Provence
Toulouse
Montauban
Albi
Agen
Carcassonne
Béziers
Sète
Pau
Bayonne
Bilbao
San Sebastián
Santander
Torrelavega
Lourdes
Auch
Guernsey
Jersey
English Channel
Bay of Biscay
Parc naturel régional du Perche
Parc Naturel Régional du Morvan
Parc naturel régional des Ballons des Vosges
Parc Naturel Régional de Millevaches en Limousin
Parc Naturel Régional Périgord Limousin
Parc naturel régional des Landes de Gascogne
Parc national des Cévennes
Parc national des Écrins
Parc national de la Vanoise
Parc national du Mercantour

Top operators



Distribution of the queries per DNS cache

Conclusion

Conclusion

- Better understanding of the DNS caches
- We have discovered several patterns
- We have identified differences between ISPs

Conclusion

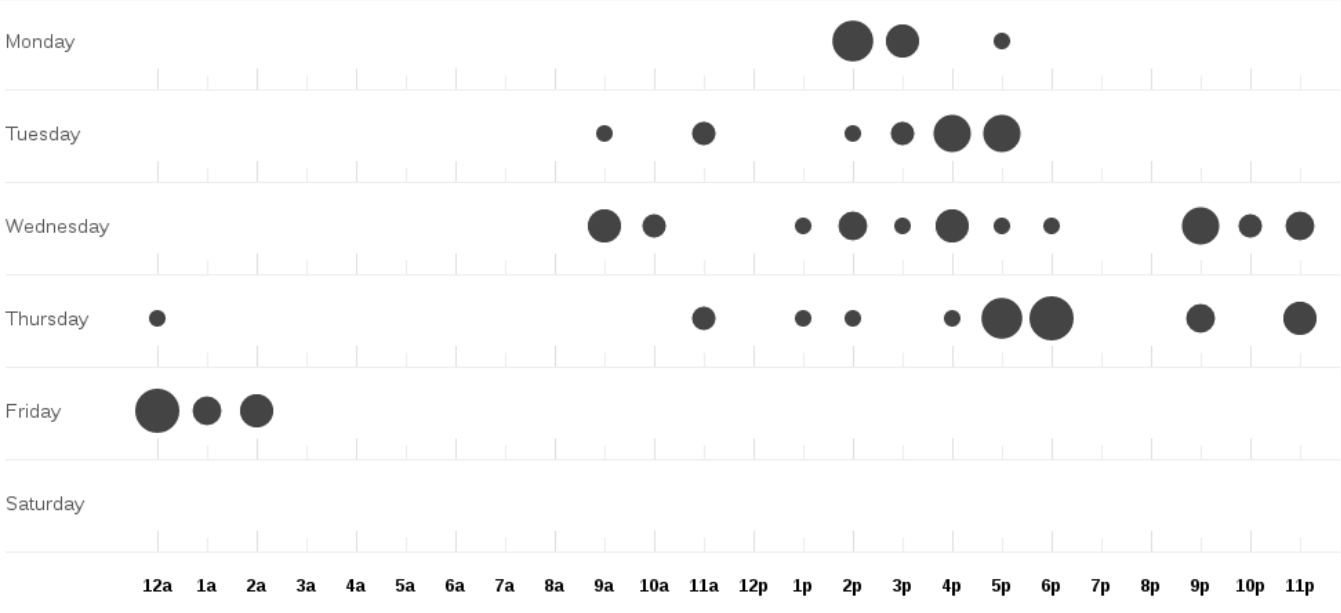
Future Work

- Compulsory
  - Write the report
- Optional
  - Still many patterns to study
  - ...even more to discover
  - Other campaigns can be launch with specific objectives

Questions?

BONUS

- Efficient team work: task assignments, regular "meeting"...
- Good subject, many stuffs to, good scope for a week
  $\rightarrow$ Thank you Guillaume!
- Smooth logistics, perfect setup, good foods, good mood
  $\rightarrow$ Thank you Pascal!



$\Rightarrow$ intense week, very interesting!