afnic

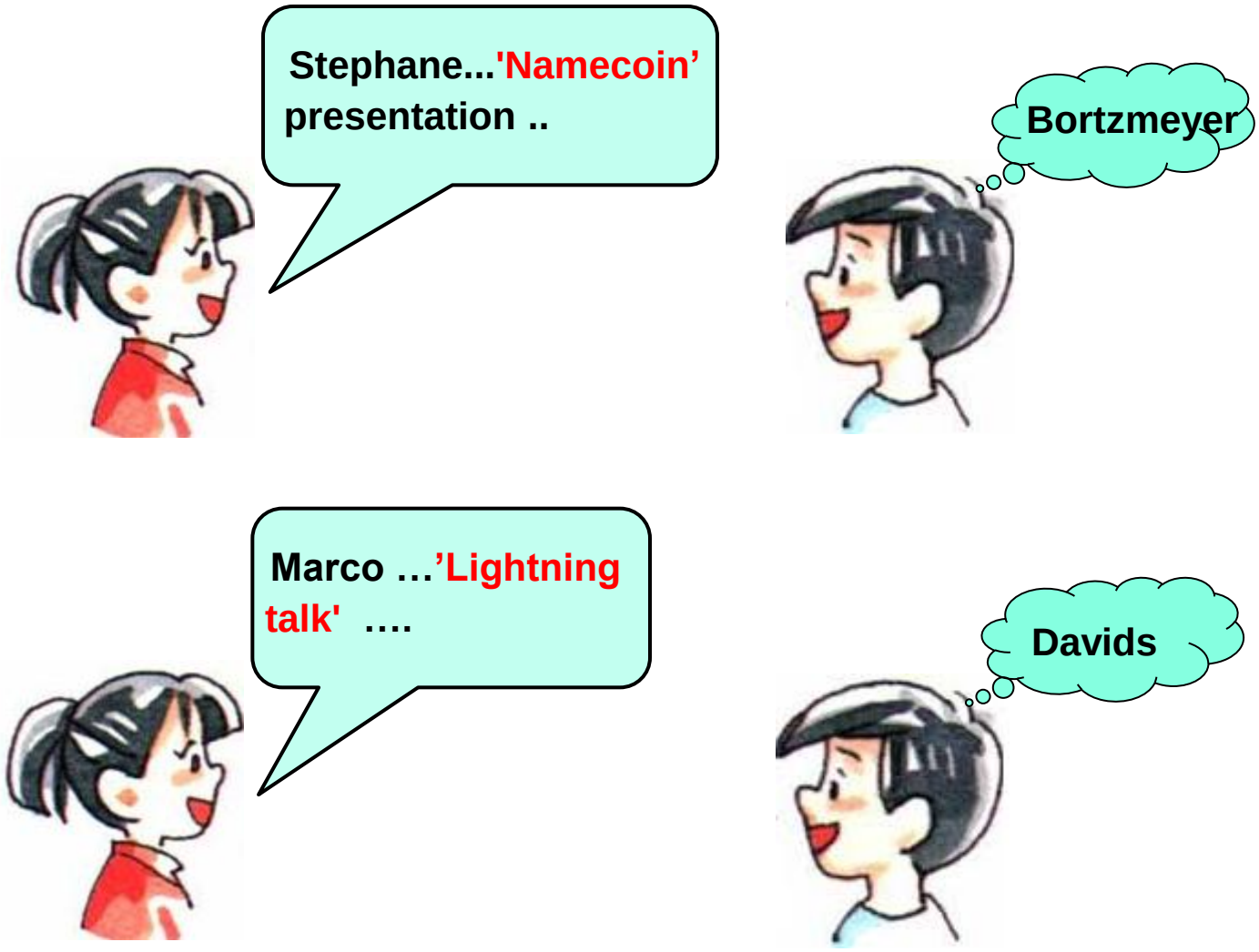
Name collisions : Can it be mitigated definitely?

04/05/2014

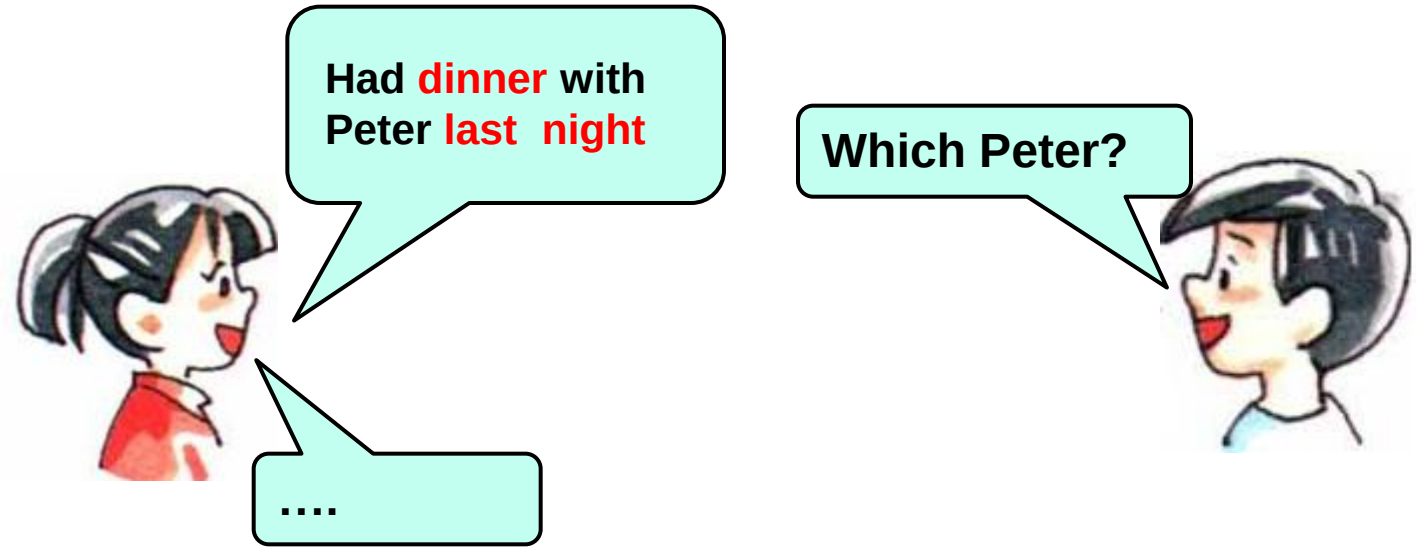


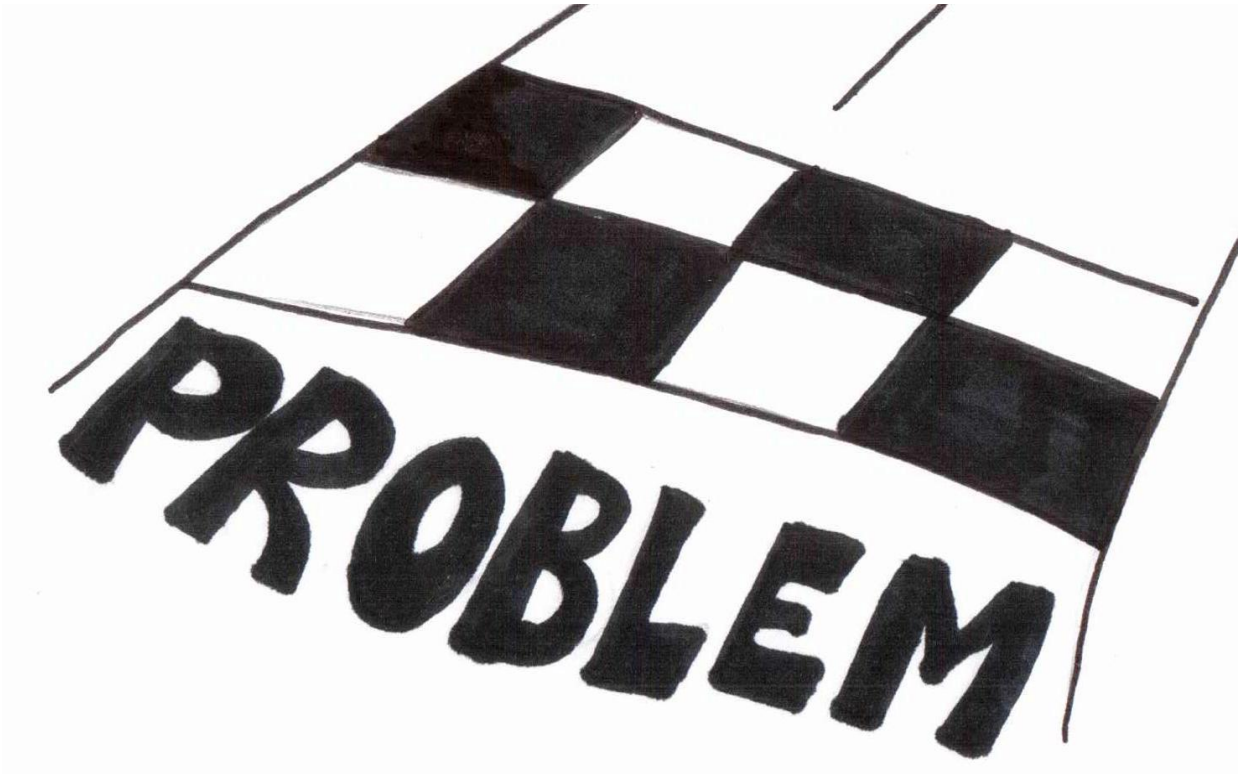

CONTEXT

A discussion between two CENTR R&D attendees



A discussion between two CENTR Jamboree attendees

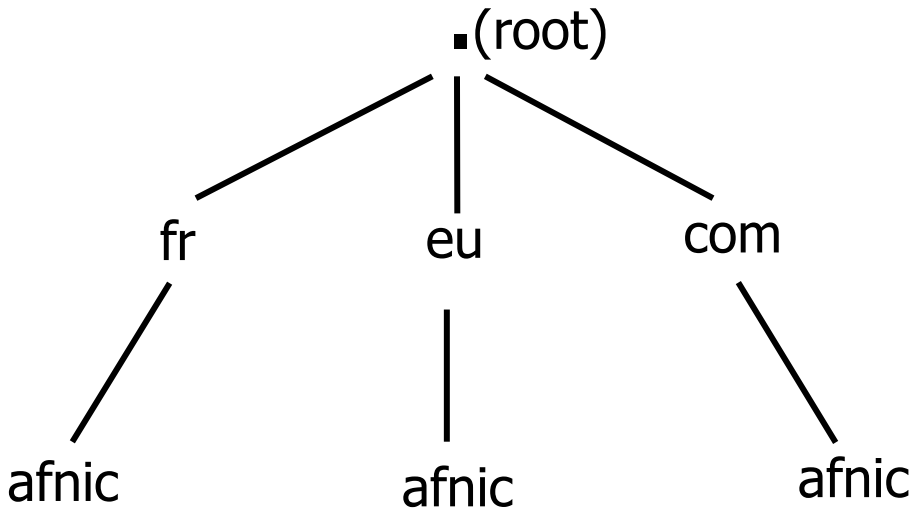



PROBLEM

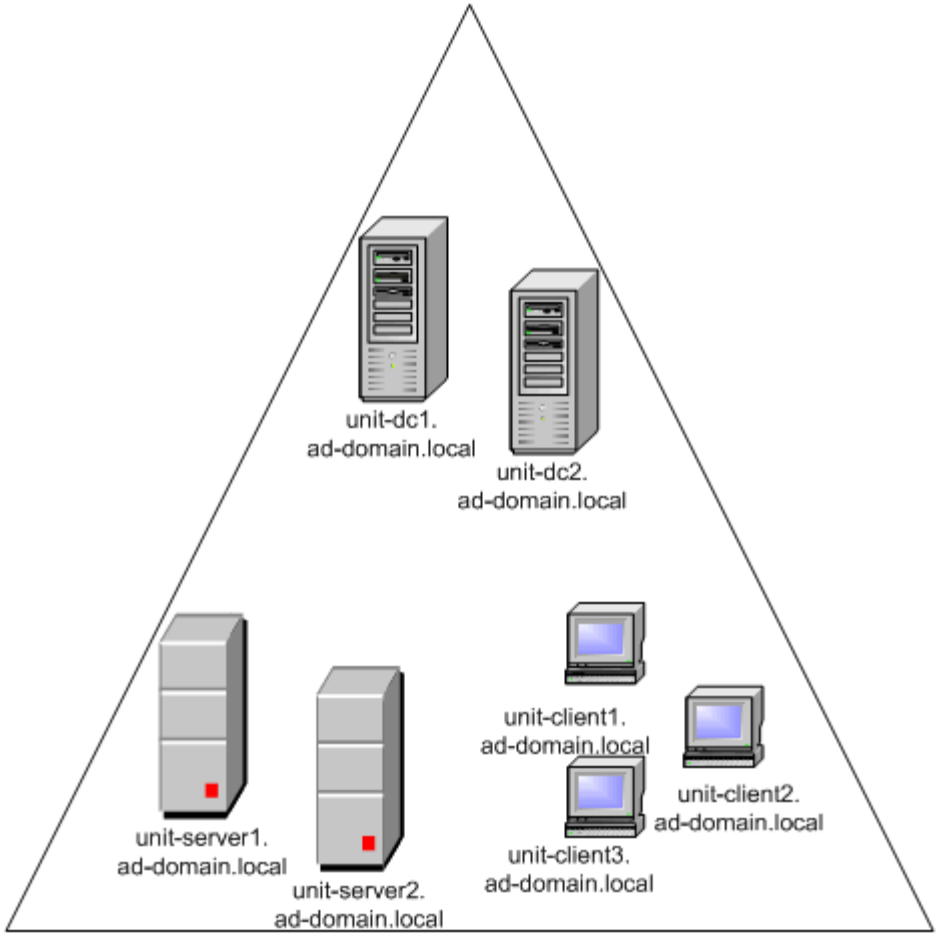
Computers



DNS

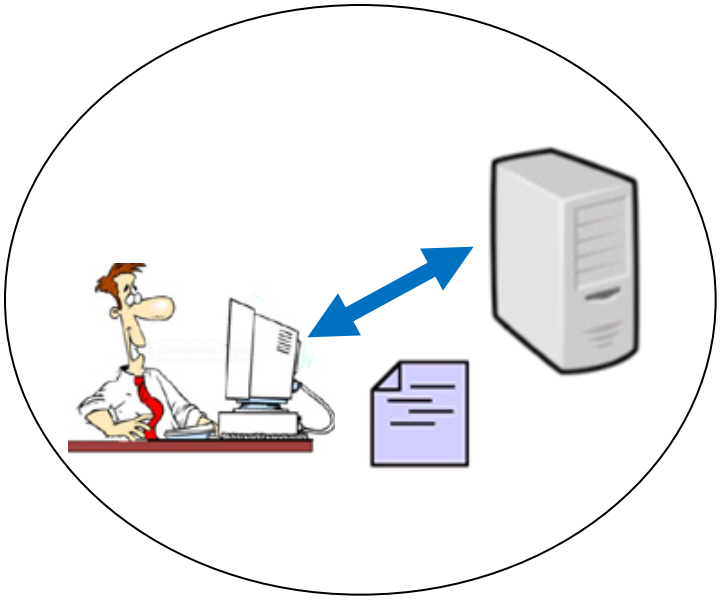


Private TLDs

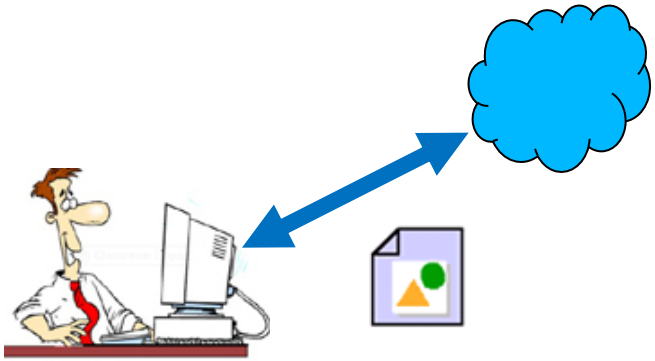


Internal Active Directory Namespace

Problem 1 : Name resolution ambiguity

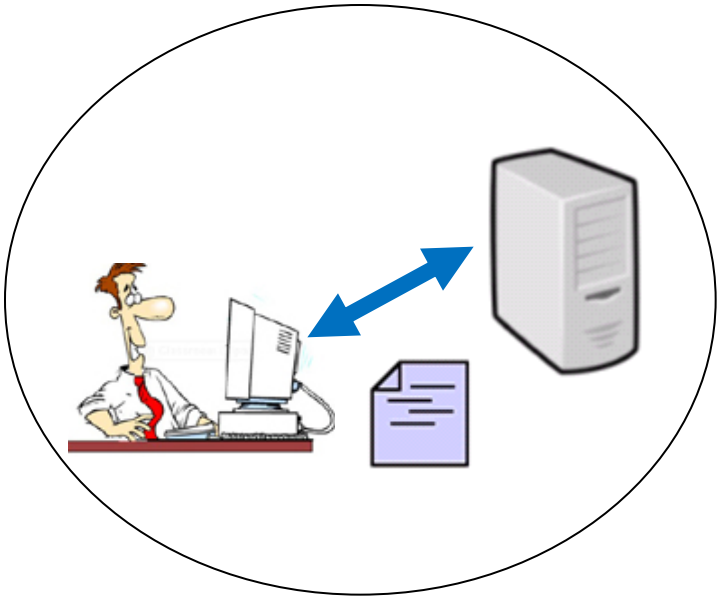


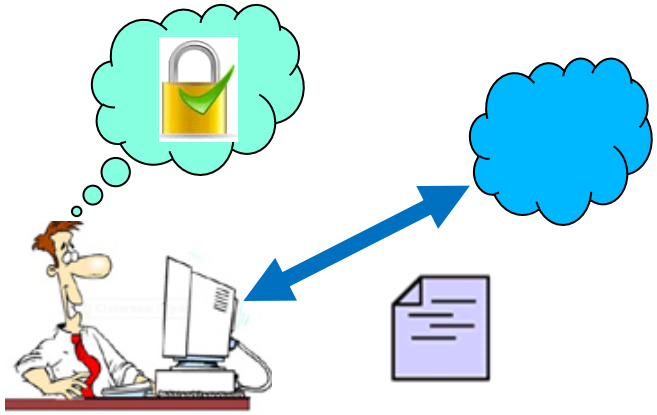
.local (gTLD)



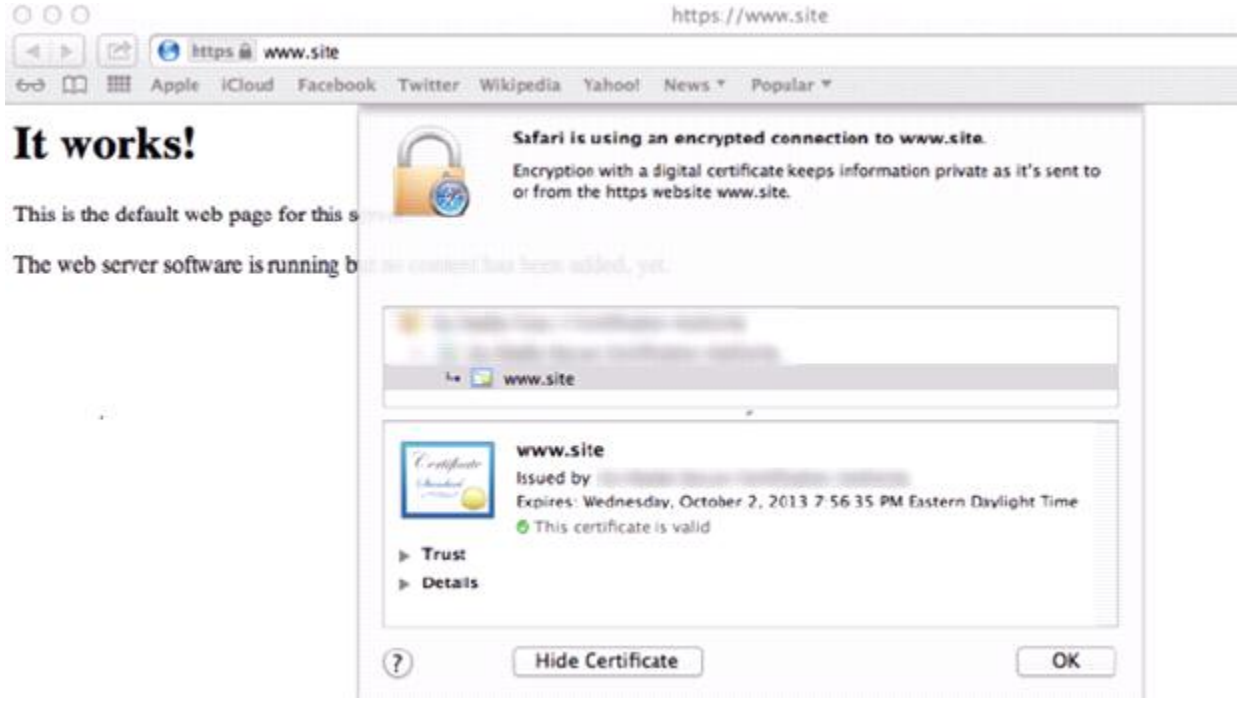
Problem 2 : Name collision (Certificates)

***.local**





Problem 2 : Real use case



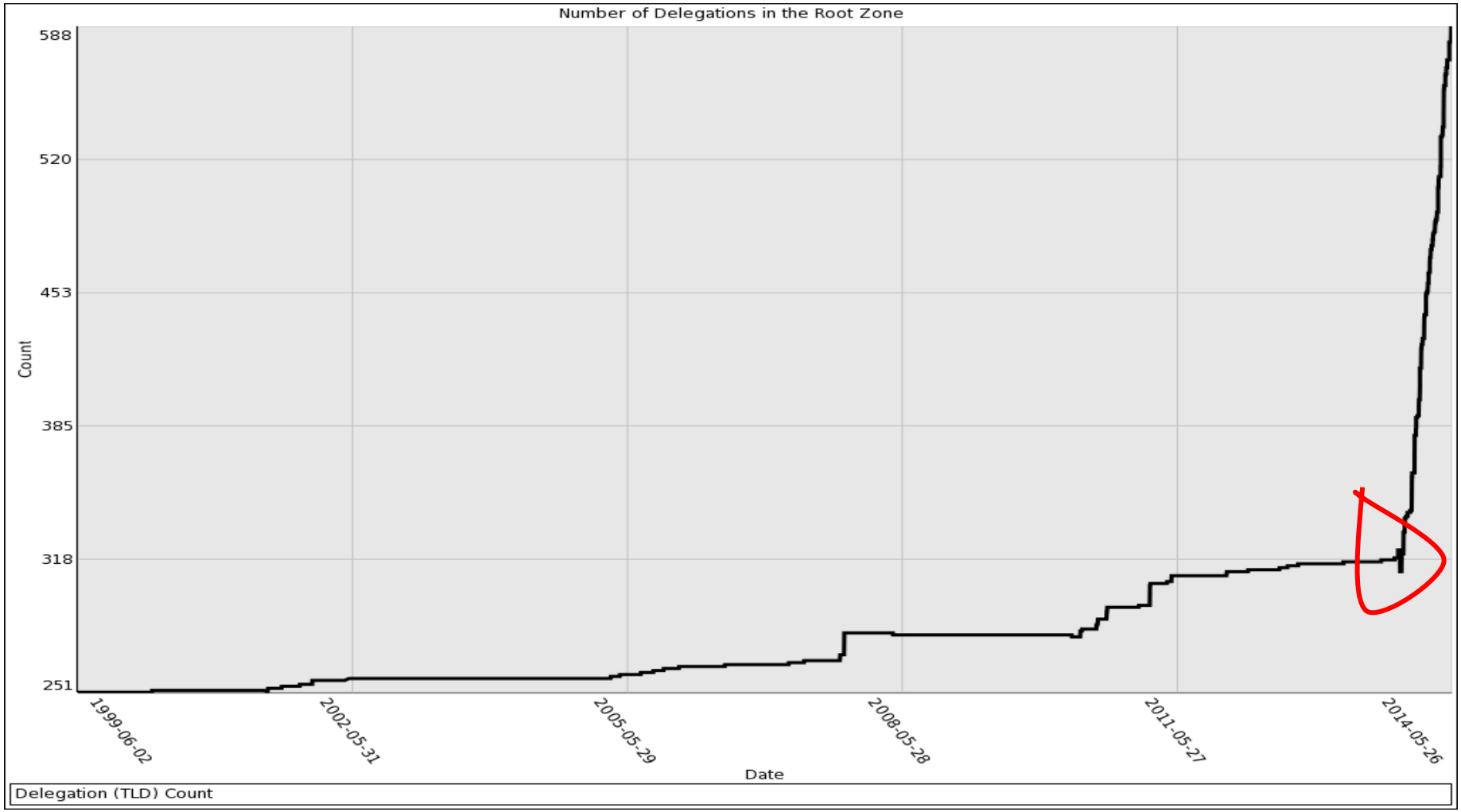
✓ Existing Internal Certificats : 11615 GoDaddy, 6663 Positive SSL, 4807 DigiCert …


This is not a new problem.

TLDs History

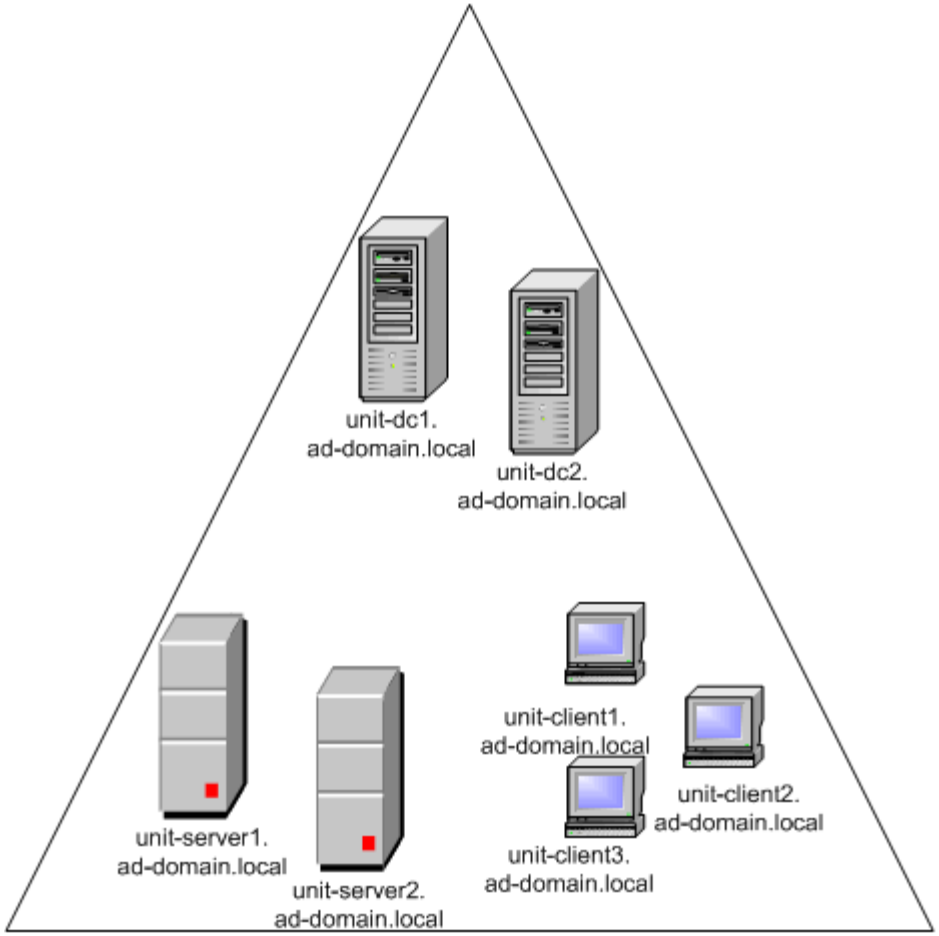
- ✓ .cs
- ✓ .at

Why so much noise now?





Private TLDs



Internal Active Directory Namespace

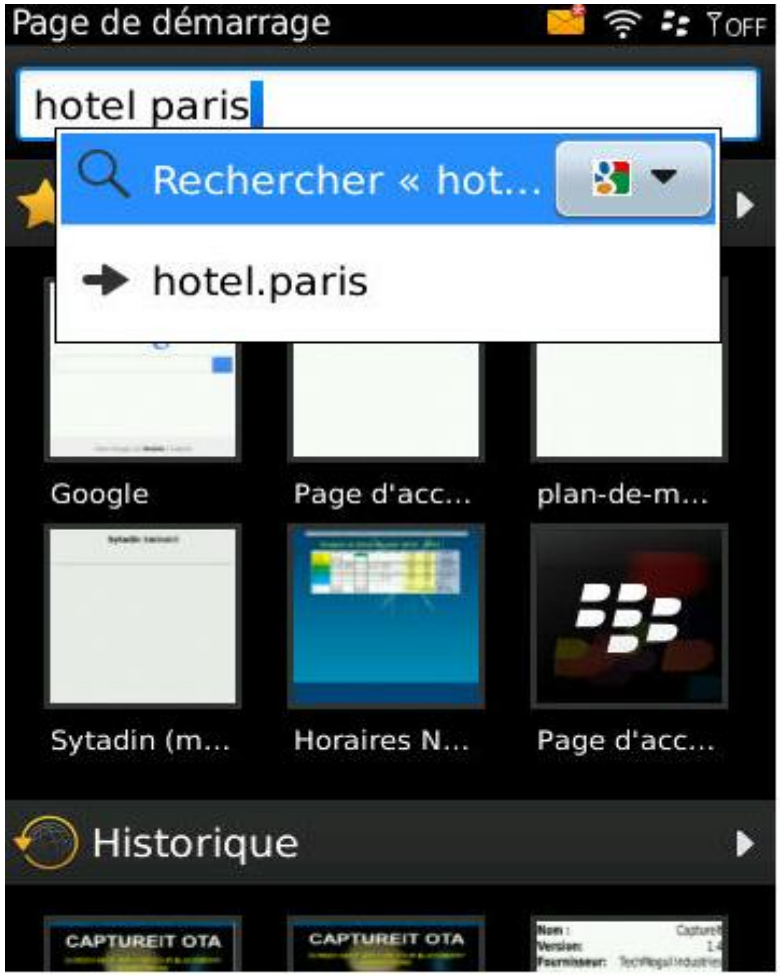
Search list

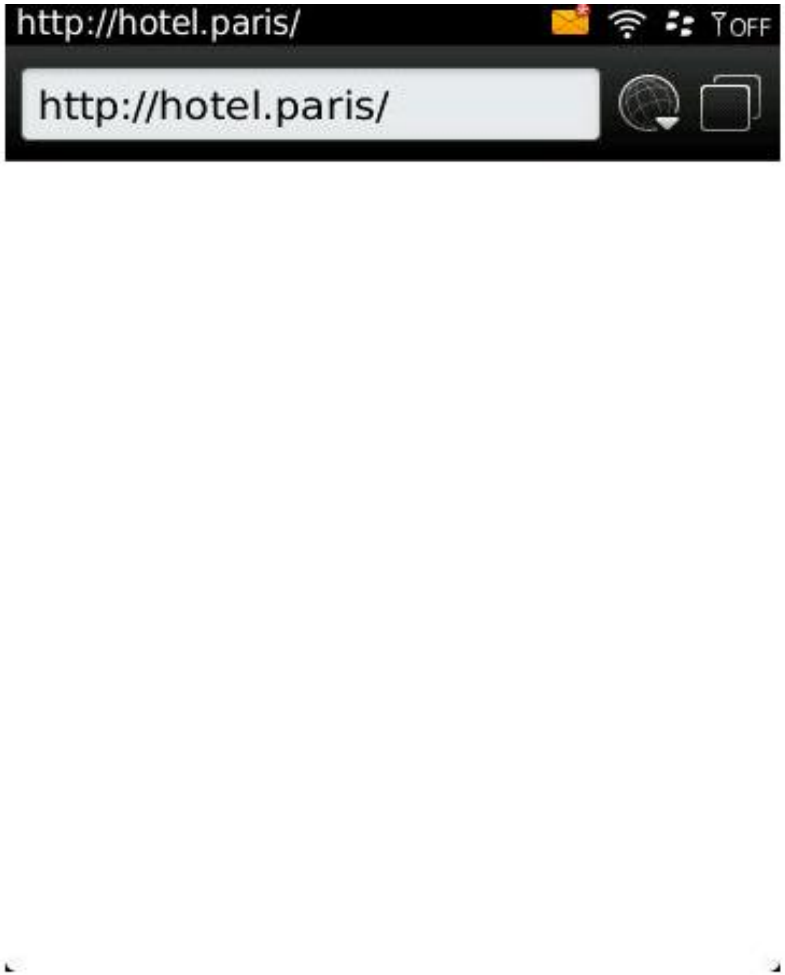
Name + Search List + Behavior -> DNS Query List

Example

Name: "www"
Suffix Search list: ["hotel.paris"]
Behaviour: Windows XP; **Query list:** [www.hotel.paris]
Behaviour: Linux; **Query list:** [www.hotl.paris, "www"]

Device behaviors






METHODOLOGY

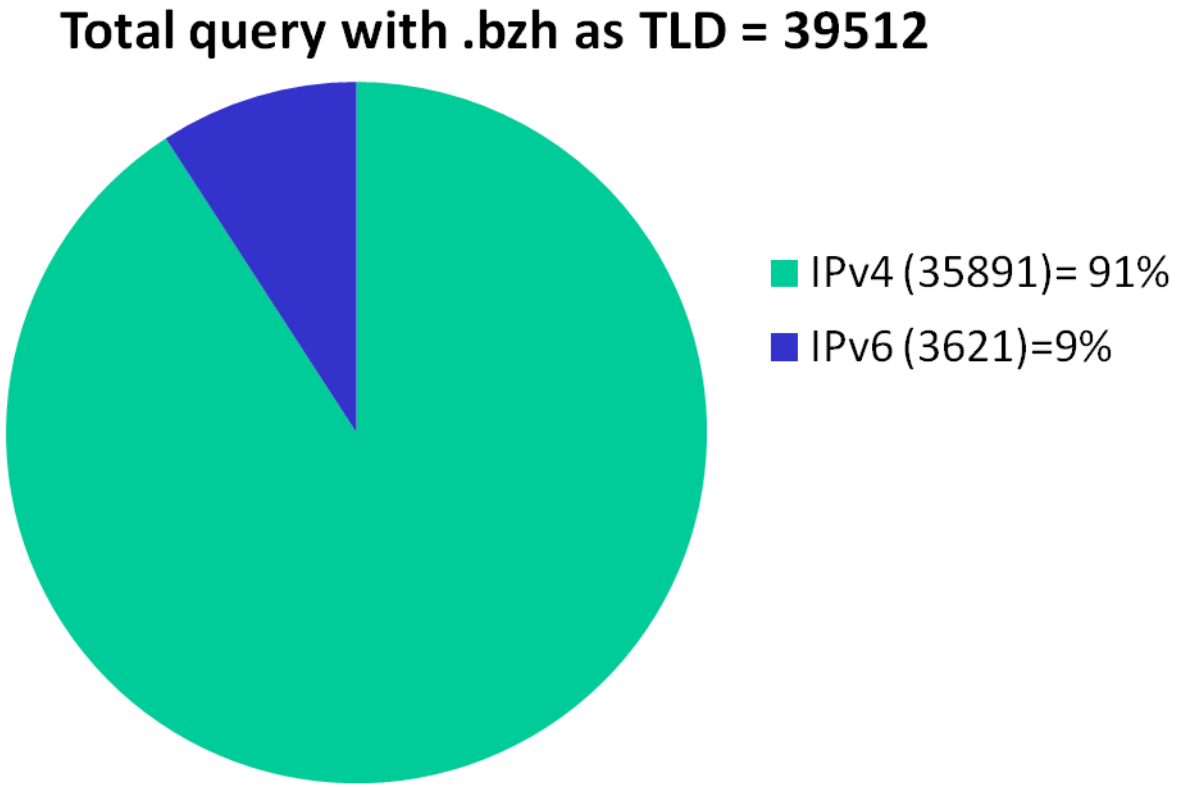
DITL

- ✓ Started from 2006
- ✓ DNS Queries captured for 48 hrs.
- ✓ 7 TB data in compressed PCAP
- ✓ Stored in DNS-OARC servers
- ✓ Access to this data only for DNS-OARC members

DITL 2013

- ✓ 1.7 TB
- ✓ ~ 39 Billion DNS queries

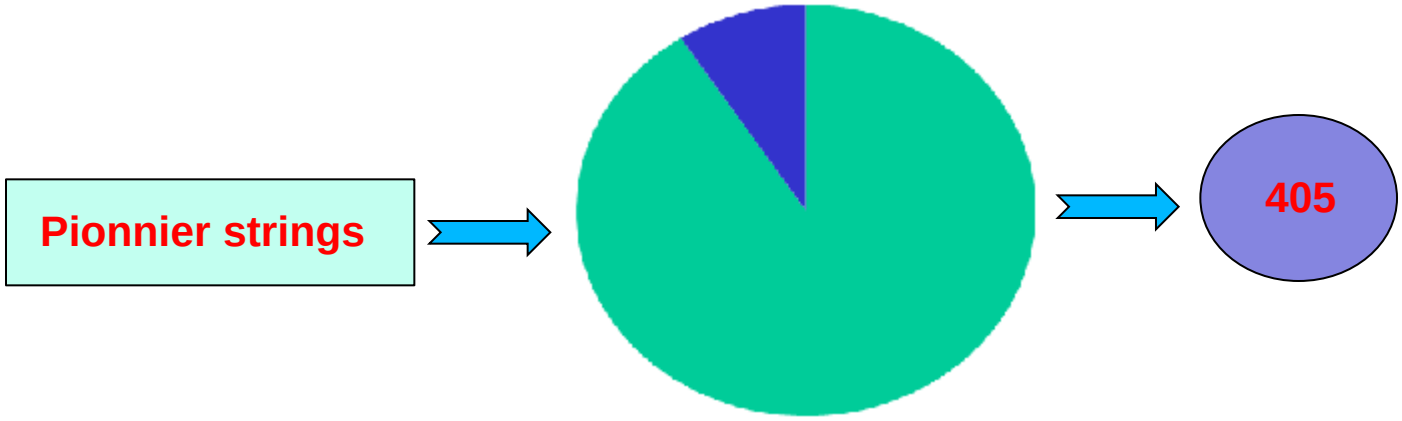
.bzh exemple



Pioneer strings

- ✓ géographique
- ✓ marques
- ✓ association
- ✓ bretagne
- ✓ lorient
- ✓ brest
- ✓ rennes
- ✓ kemper
- ✓ pennarbed
- ✓ ovh
- ✓ orange
- ✓ institut-locarn
- ✓ www

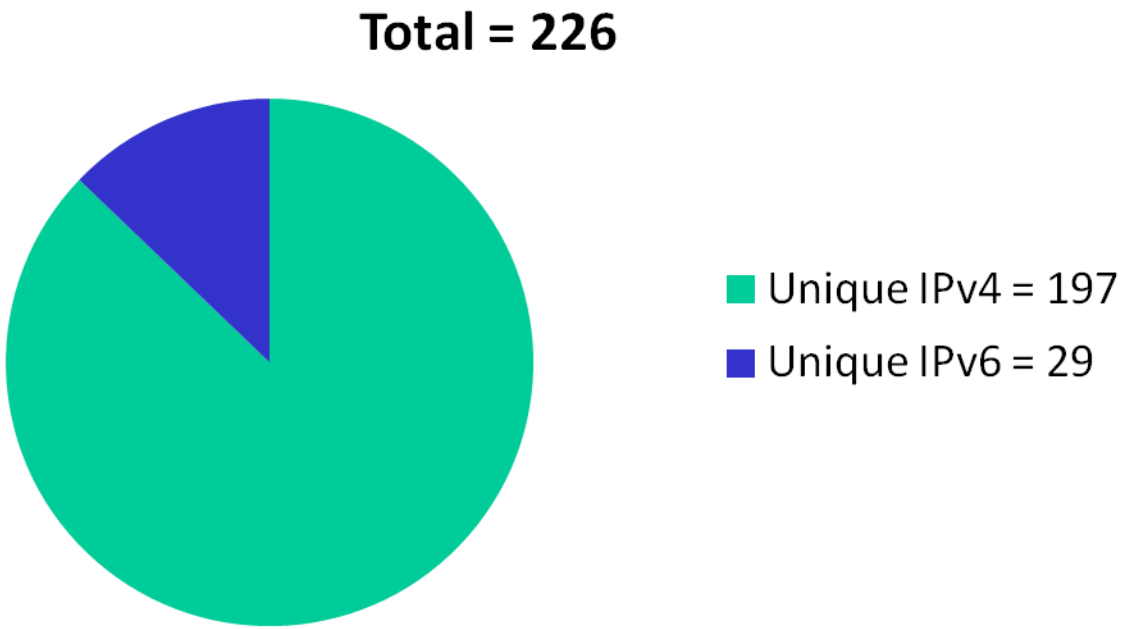
Filtered queries that had pioneer strings



www.institut-locarn.bzh

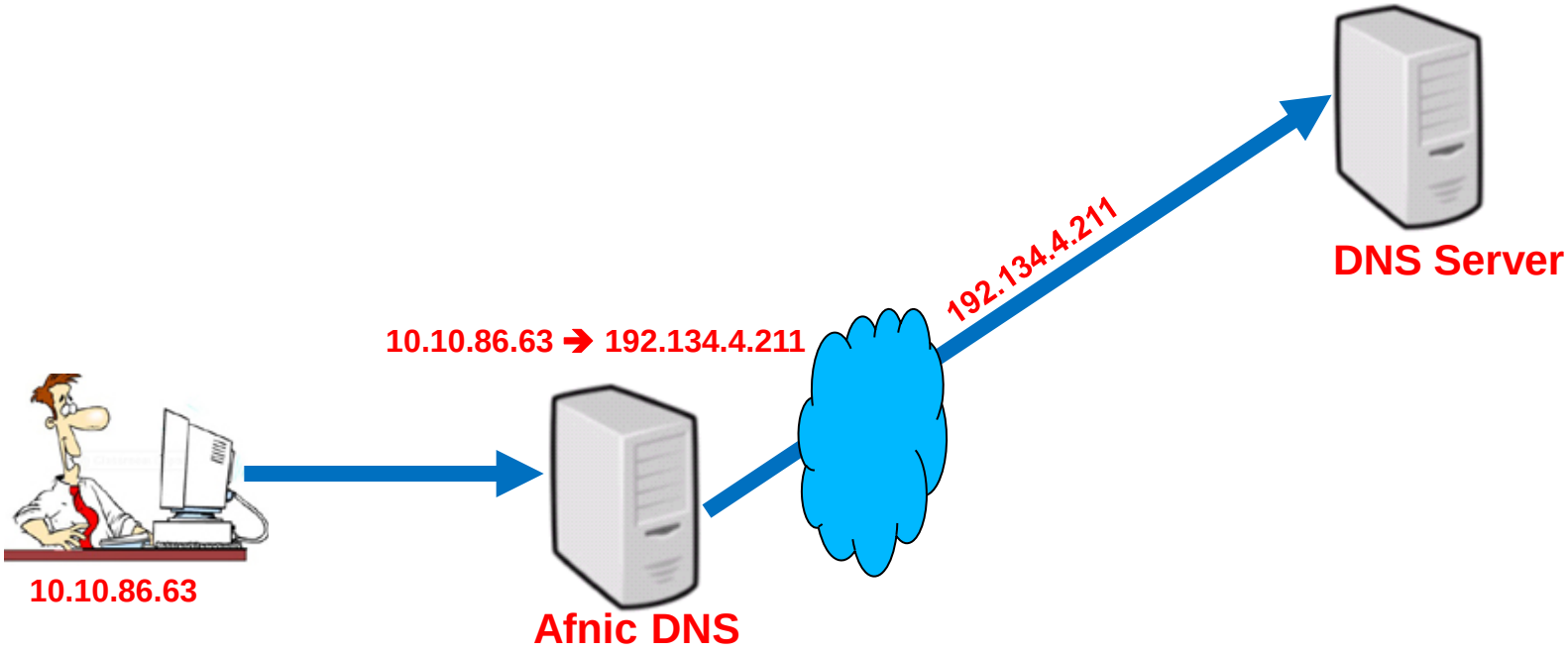
www.ovh.bzh

(Unique)

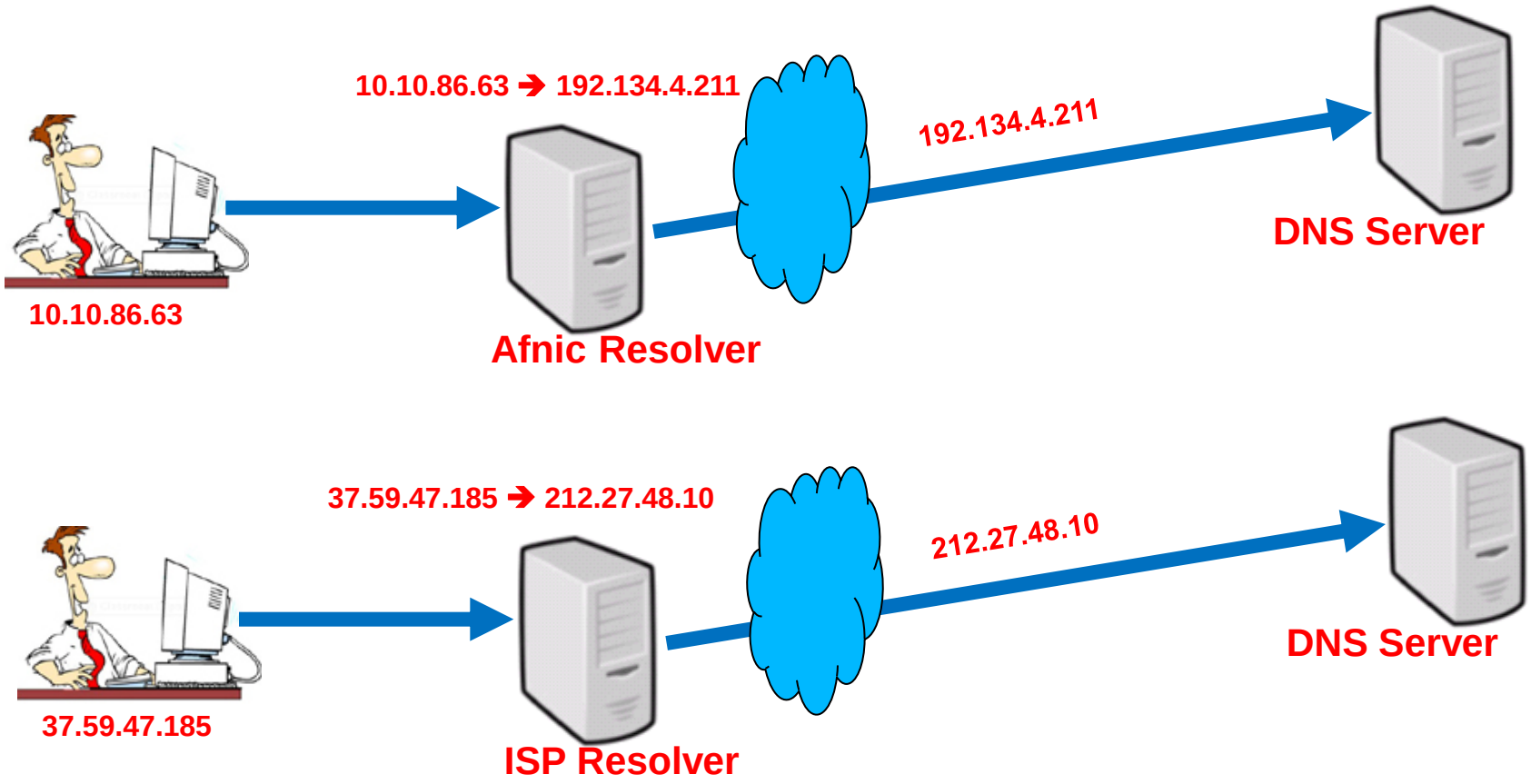


www.institut-locarn.bzh
www.institut-locarn.bzh → www.institut-locarn.bzh

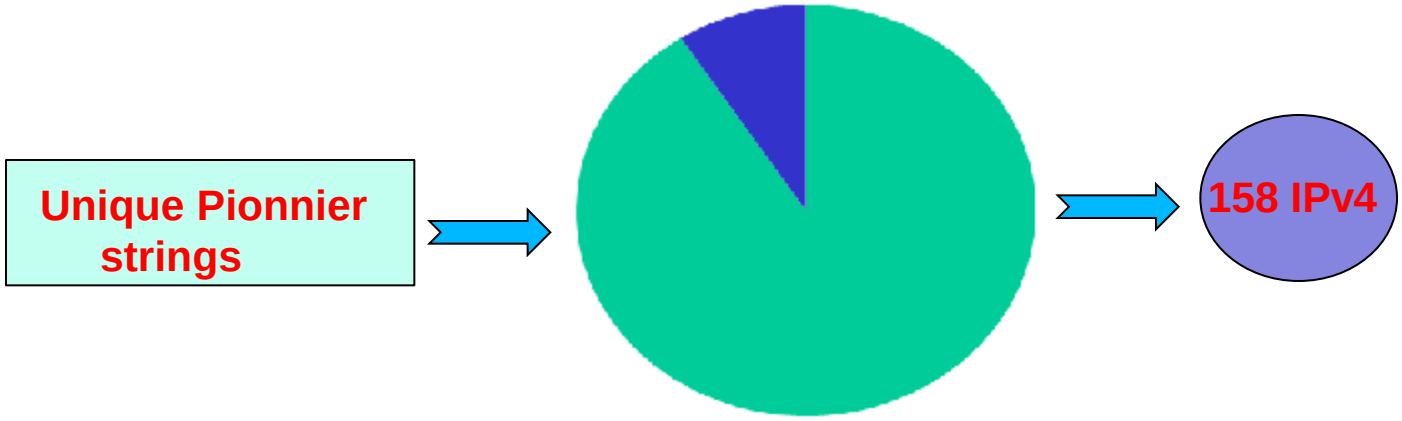
RFC 1918


10.10.86.63 ➔ 192.134.4.211
192.134.4.211
DNS Server
10.10.86.63
Afnic DNS

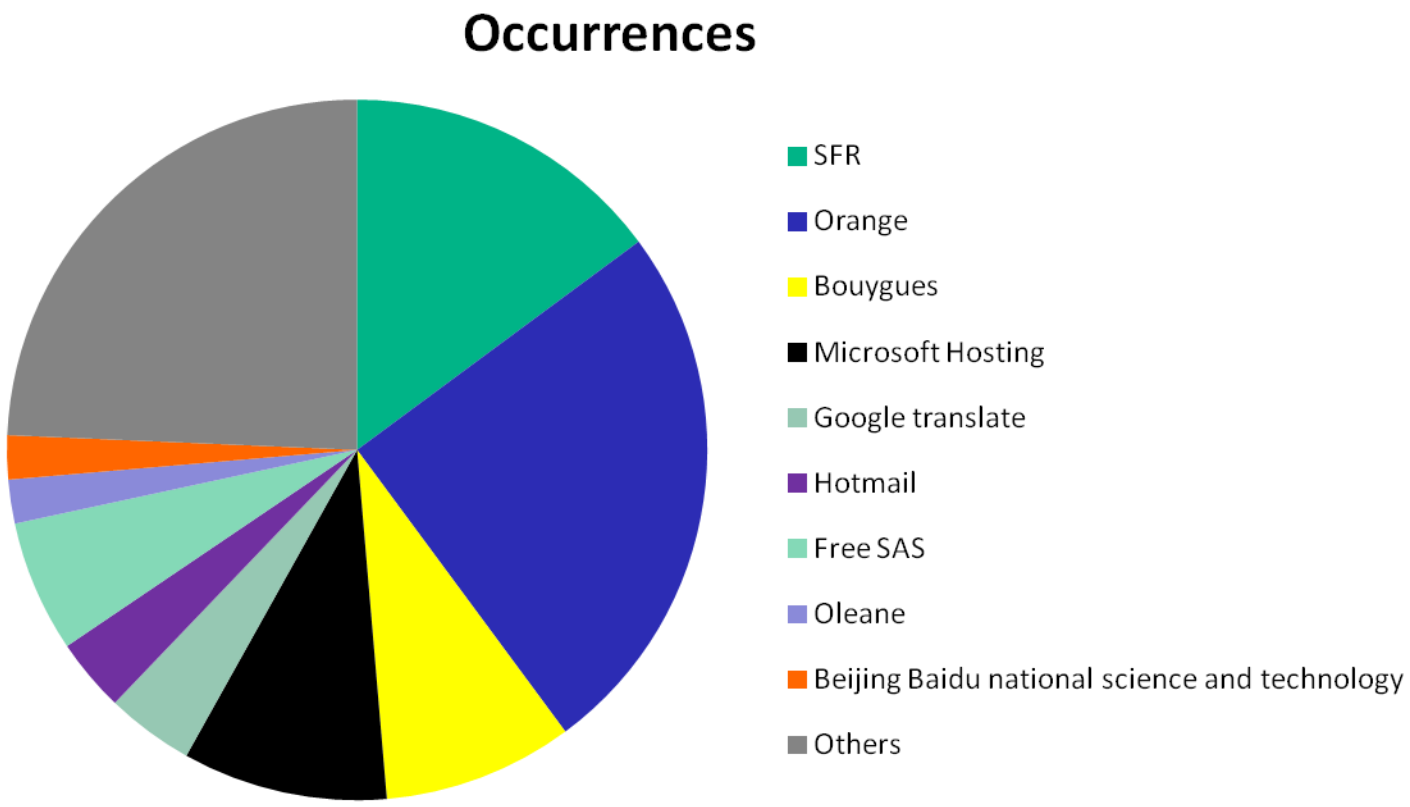
Identification possibility



Filtering RFC 1918 adresse



Different sources (At organization or ISP level)



Reducing the scope

✓ Most queries seen at the DITL will not have come from the end user

✓ Possible to obtain the end-user query by asking the ISP or the organization to look at the query logs based on "Timestamp". But, time consuming and legal issues prevail

✓ What we could do is to reduce the scope



Mitigation

- ✓ Several reasons for name collisions
- ✓ There is no one magic solution
- ✓ Number of solutions
  - ✓ Revoke internal certs
  - ✓ Turn off search list
  - ✓ Internal private TLD to use a delegation from the global DNS
  - ✓ Monitor