IoTRoam – An open LoRaWAN Roaming Initiative

Sandoche Balakrichenan (Afnic)

27/04/2020



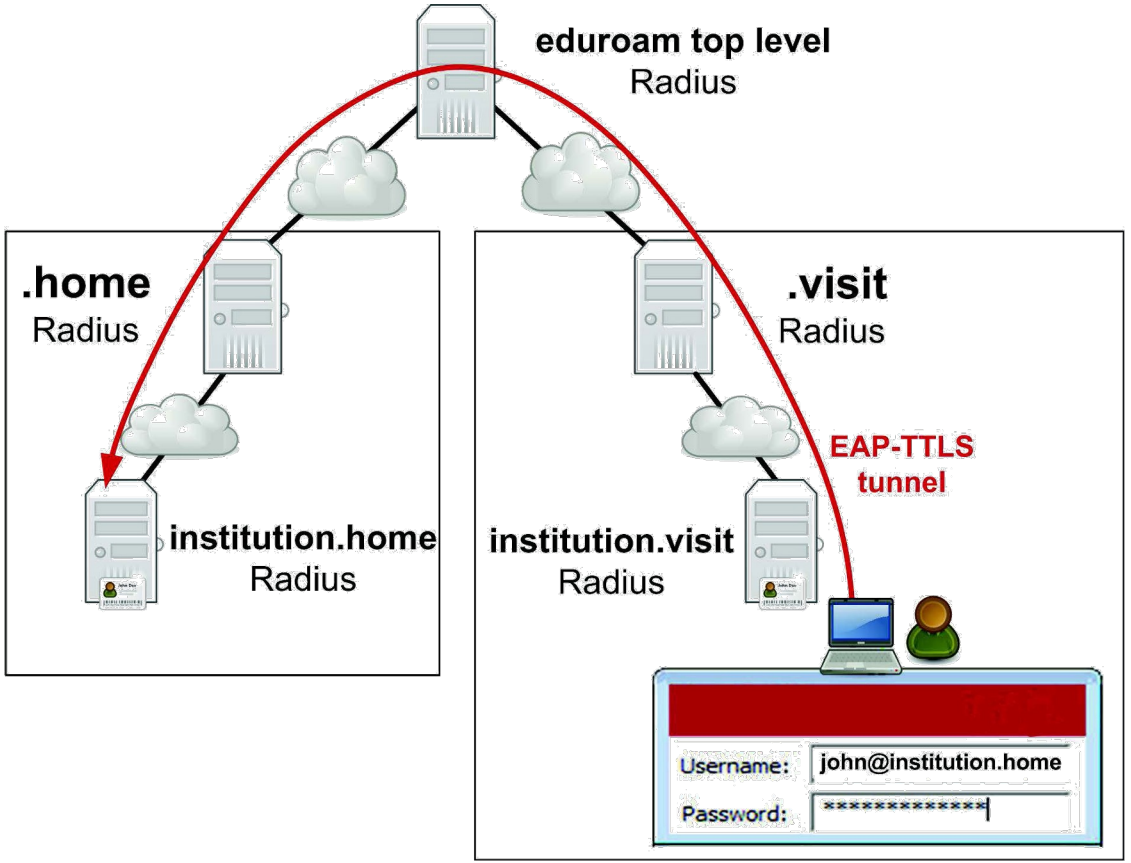
LoRaWAN®

Creating Valuable IoT Connections

Motivation

- To set up an Open/Free LoRaWAN roaming infrastructure
- Interaction with Roaming-Hub & other Industrial solutions
- Enable interop testing
- Feedback to LoRaWAN Backend specifications
- Accelerate LoRaWAN roaming adoption


eduroam
101
territories


eduroam top level
Radius
.home
Radius
institution.home
Radius
.visit
Radius
institution.visit
Radius
EAP-TTLS
tunnel
Username:
john@institution.home
Password:

Thoughts on a Roaming infrastructure for research using LoRaWAN





- Etudier le passage à l'échelle au niveau national ?
  - Mobilité des objets et instruments scientifiques
  - Eduroam pour l'IoT



The involvement of National Research and Education Networks (NREN) in East Africa is key for the growth of Internet of Things (IoT) applications in the region, as they can host the access infrastructure to foster research in IoT and to serve the IoT community at large.

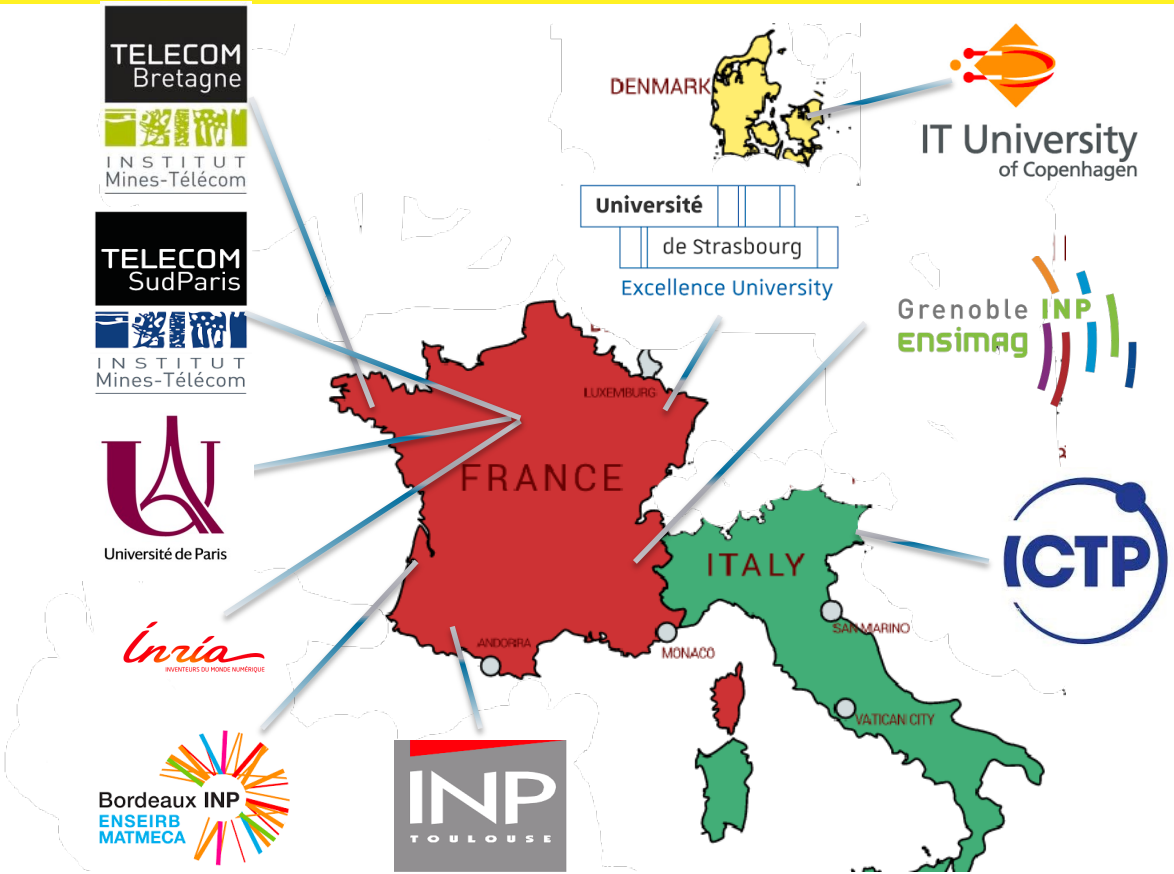
Directors:

N. MBONIMPA
Research and Education Network for Uganda (RENU), Uganda
L. CHEMANE
Mozambique Research and Education Network (MoRENet), Mozambique



With the success of eduroam and data management solutions in mind, SURF investigates the possibility to create an 'open common IoT platform' and infrastructure

10 Institutions who have expressed interests – Tested with 2



Requirements

- Should work with any ED compatible to LoRa Speciifcations
- Should work with any NS, AS, JS software compatible with LoRa and LoRaWAN backend specifications
- Minimum Out of Band Configurations
- Dynamic discovery
- Federated Identity providers
- A trust anchor acceptable by all

.

Issues and Solutions

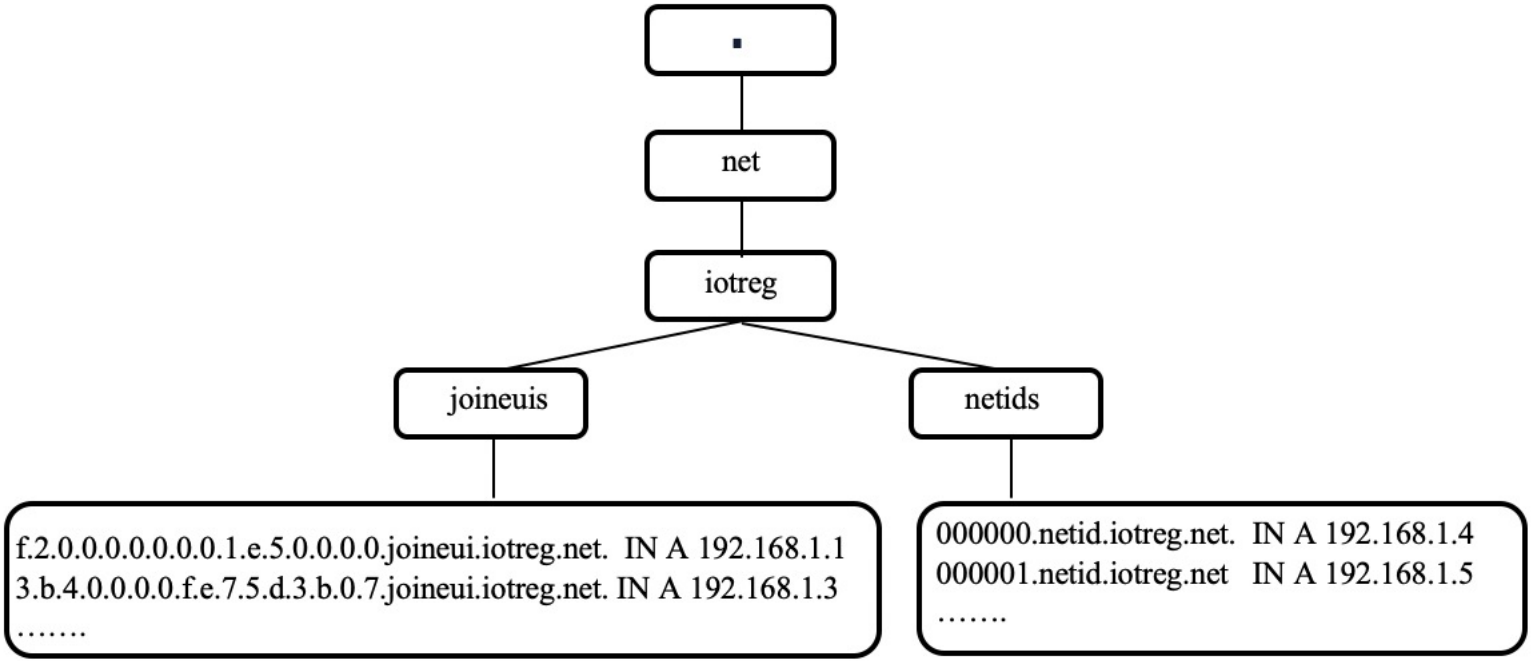
- Issue – DNS Compatible Software
  - Solution - Chirpstack (chirpstack.io)
- Issue – LoRaWAN DNS Service
  - Solution – iotreg.net (Operated by Afnic)
- Issue – Securing the backend elements
  - Solution – Use the well tested PKI infrastructure (Afnic as Root CA)

.

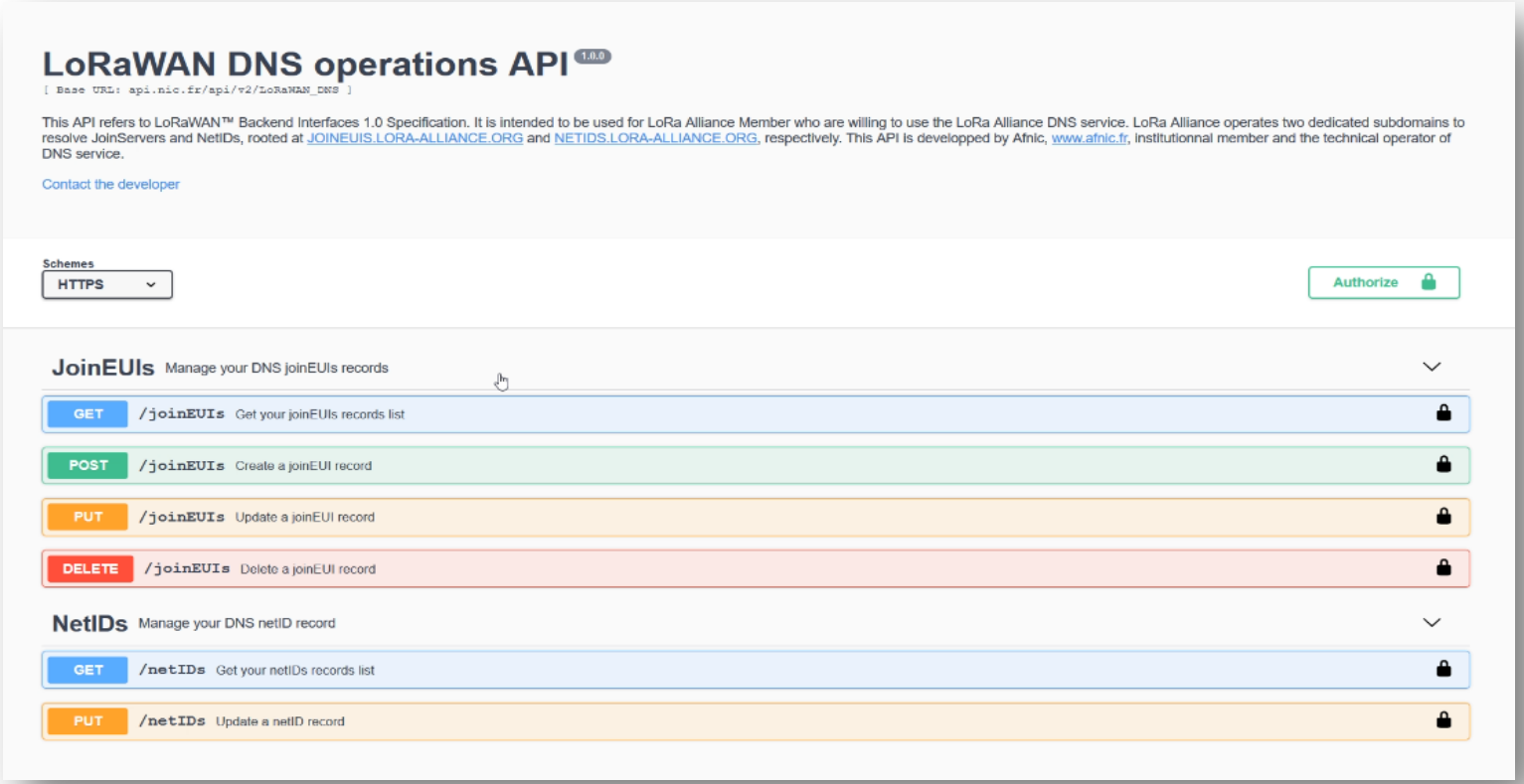
Issues – Required Configuration Parameters

Peer Net-ID	
Roaming Policy	
Peer's channel plan	
UDR Type	
Peer's fNS URL	
Peer's sNS URL	
Peer's NS IP address	
Peer JS URL	
Peer JS IP Address	
Peer JS Http Credentials	

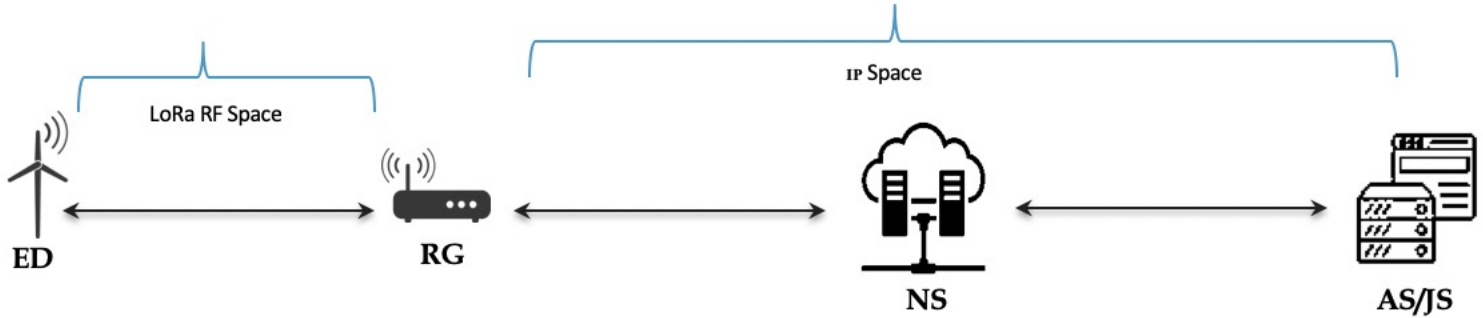
Dynamic Discovery - Using DNS for Roaming & 0TAA



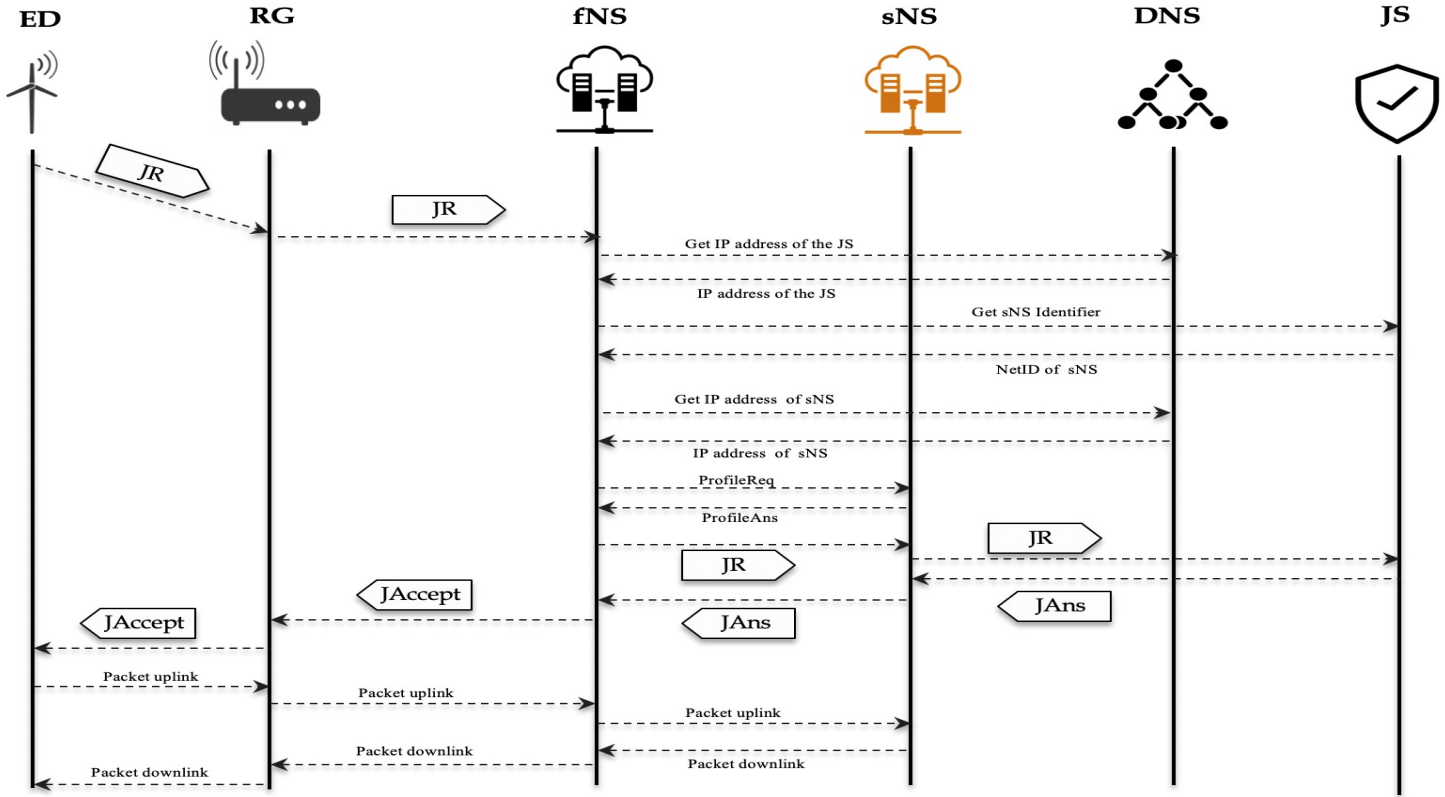
Afnic's API for DNS Provisioning



RF & IP Space



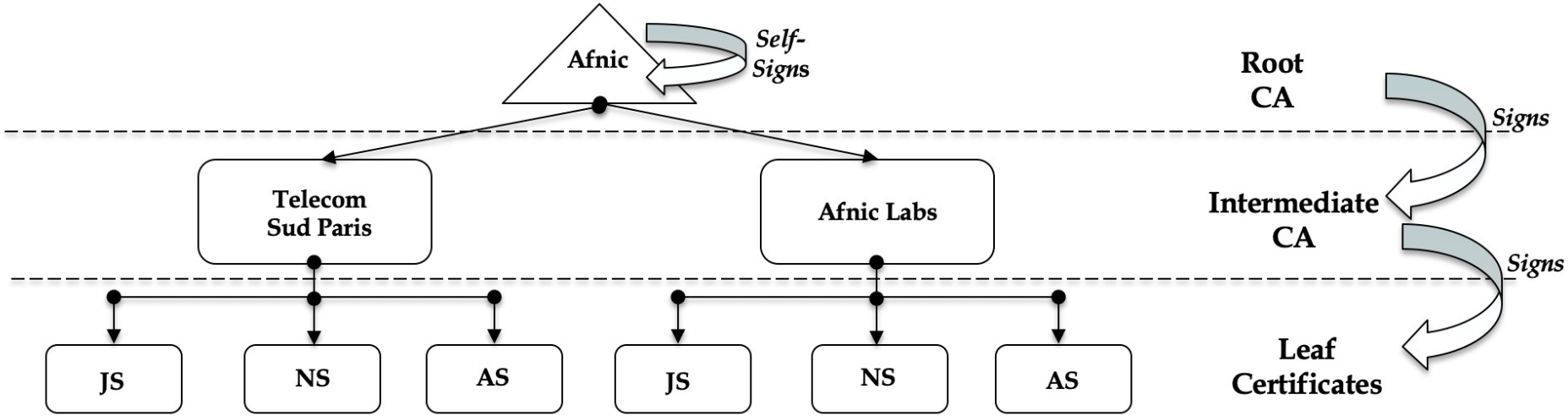
Message Flow using DNS for Passive Roaming



Configuration Parameters - DNS based Roaming

Peer Net-ID	Not needed
Roaming Policy	DNS Whitelist/Blacklist
Peer's channel plan	?
UDR Type	?
Peer's fNS URL	Not needed
Peer's sNS URL	Not needed
Peer's NS IP address	Not needed
Peer JS URL	Not needed
Peer JS IP Address	Not needed
Peer JS Http Credentials	Not needed

Trust Anchor – Certificate Provisioning

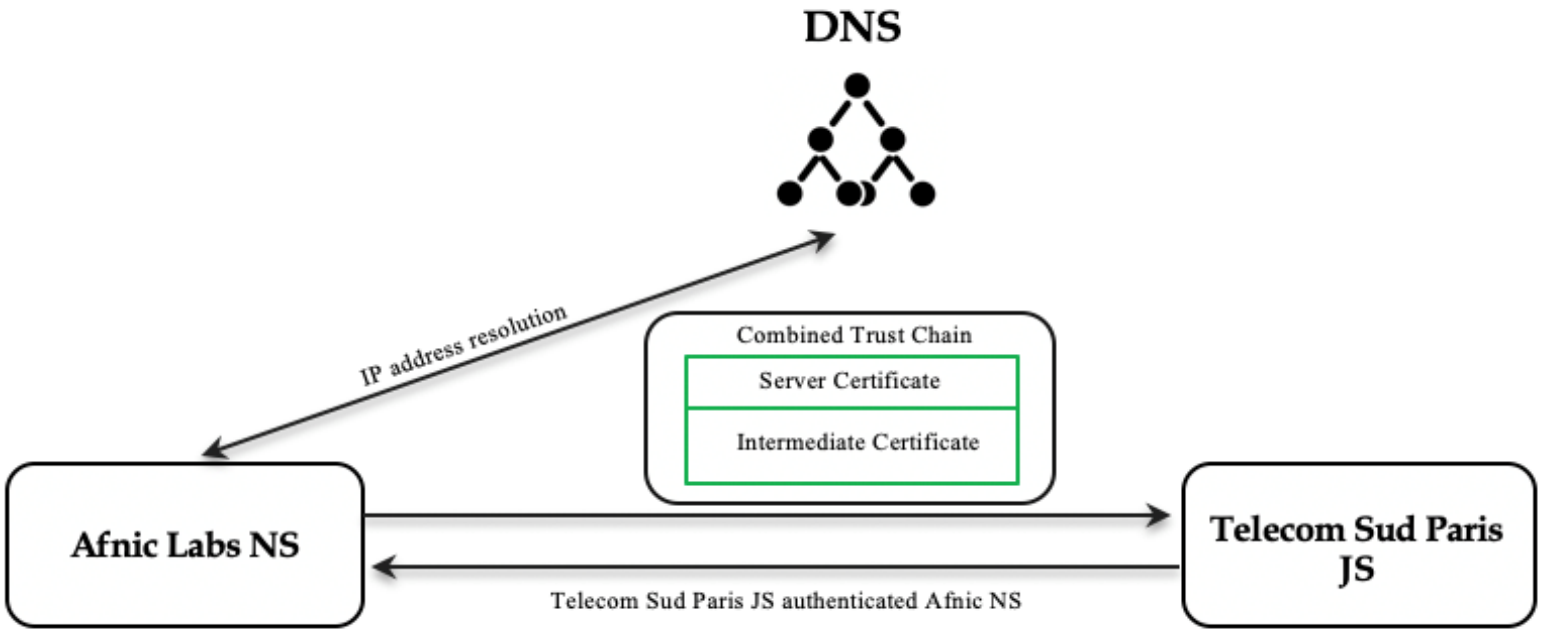


Certificate Provisioning – How to for an IdP?

- https://github.com/AFNIC/IoTRoam-Tutorial/blob/master/QuickStart.md

7. For the Certificates
    - a.) Clone/Copy the required Files
    - b.) The directory structure is as here
    - b.) Modify intermediate-csr.json to suit you
    - c.) Modify "Certificate.json" in all subdirectories to suit your "CN" and host "IP addresses"
    - d.) For roaming, You have to modify the directory name to suit your NetId. In the example, the NetID is "000000"
8. Install cfssl. A Short installation tutorial
9. Following has to be done to run the Makefile
    - a.) Request your intermediate public and private certificate by sending mail to `"sandoche.balakrichenan@afnic.fr"` AND `"antoine.bernard@afnic.fr"`
    - b.) Copy the intermediate public and private certificate to the intermediate directory as specified in the directory structure as here:
    - c.) Modify the `NetId` in the top of the `Makefile` to suit your `NetId`
    - d.) Run `make`

Certificate Validation



Configuration Parameters - DNS based Roaming

Peer Net-ID	Not needed
Roaming Policy	DNS Whitelist/Blacklist
Peer's channel plan	?
UDR Type	?
Peer's fNS URL	Not needed
Peer's sNS URL	Not needed
Peer's NS IP address	Not needed
Peer JS URL	Not needed
Peer JS IP Address	Not needed
Peer JS Http Credentials	Not needed

IoTRoam Advantages

- No out of band configuration for NS/JS/AS authentication
- Authentication using port 443. Hence no worry about firewall settings
- Scalable: Ready for billions of devices as the platform uses the classical DNS and TLS infrastructure that has been operationally tested in the Internet
- No cost involved – Self-Signed Certificates and Open DNS infrastructure
- For more info : https://github.com/AFNIC/IoTRoam-Tutorial/
- To participate in testing the Roaming Platform; contact Sandoche.Balakrichenan@afnic.fr AND antoine.bernard@afnic.fr

LoRaWAN®

Creating Valuable IoT Connections

@LoRaAlliance

linkedin.com/company/loraalliance/

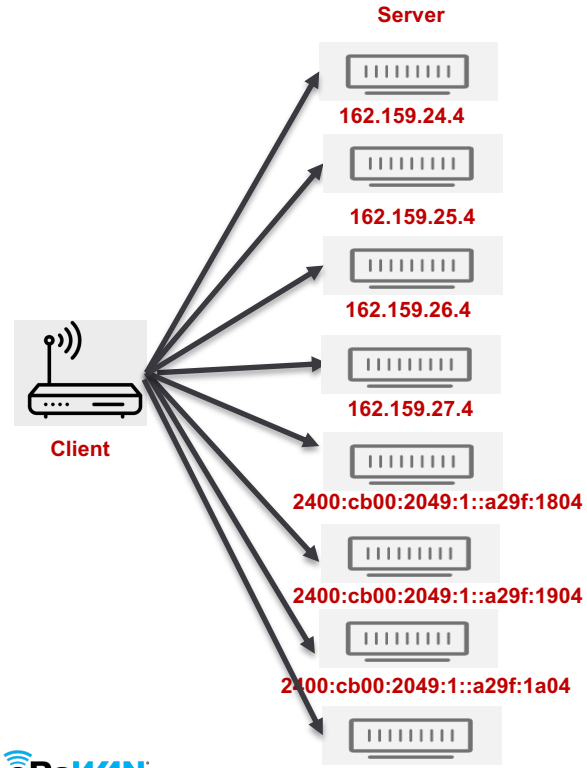
marcom@lora-alliance.com

lora-alliance.org

LoRa Alliance®

DNS Resiliency

- Using Multiple Nameservers



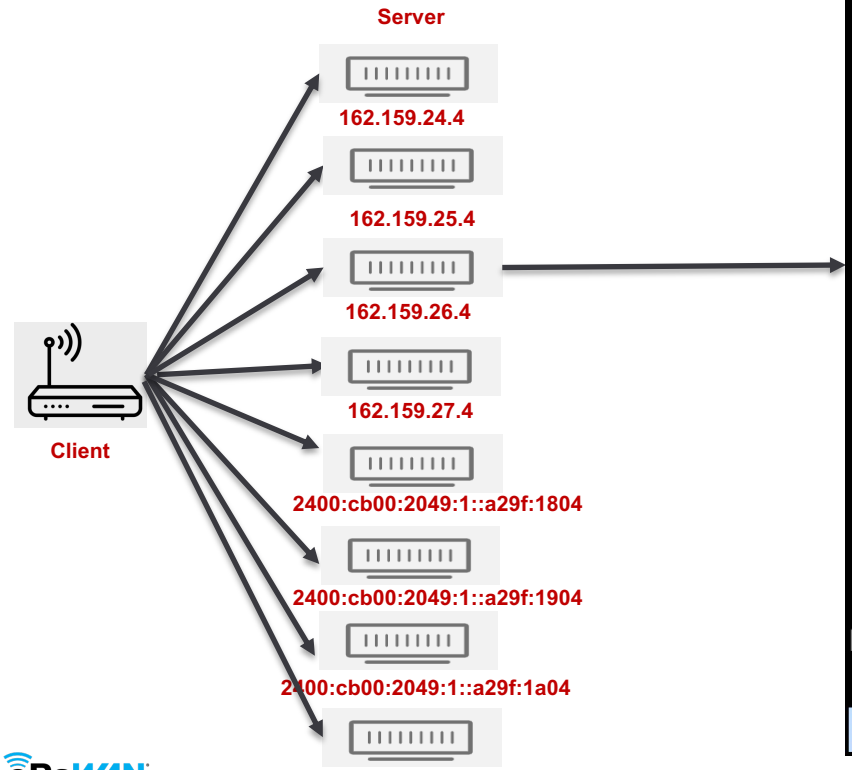

```
;; QUESTION SECTION:
;lora-alliance.org.             IN      NS

;; ANSWER SECTION:
lora-alliance.org.      3600    IN      NS      ns1.dnsimple.com.
lora-alliance.org.      3600    IN      NS      ns4.dnsimple.com.
lora-alliance.org.      3600    IN      NS      ns3.dnsimple.com.
lora-alliance.org.      3600    IN      NS      ns2.dnsimple.com.

;; ADDITIONAL SECTION:
ns1.dnsimple.com.       30034   IN      A       162.159.24.4
ns2.dnsimple.com.       30034   IN      A       162.159.25.4
ns3.dnsimple.com.       30034   IN      A       162.159.26.4
ns4.dnsimple.com.       30034   IN      A       162.159.27.4
ns1.dnsimple.com.       112844  IN      AAAA    2400:cb00:2049:1::a29f:1804
ns2.dnsimple.com.       112844  IN      AAAA    2400:cb00:2049:1::a29f:1904
ns3.dnsimple.com.       112844  IN      AAAA    2400:cb00:2049:1::a29f:1a04
ns4.dnsimple.com.       112844  IN      AAAA    2400:cb00:2049:1::a29f:1b04
```

DNS Resiliency + Latency (1/2)

- Using Multiple Nameservers + Anycast




```
; <<>> DiG 9.10.6 <<>> @162.159.26.4 hostname.bind TXT chaos
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2494
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

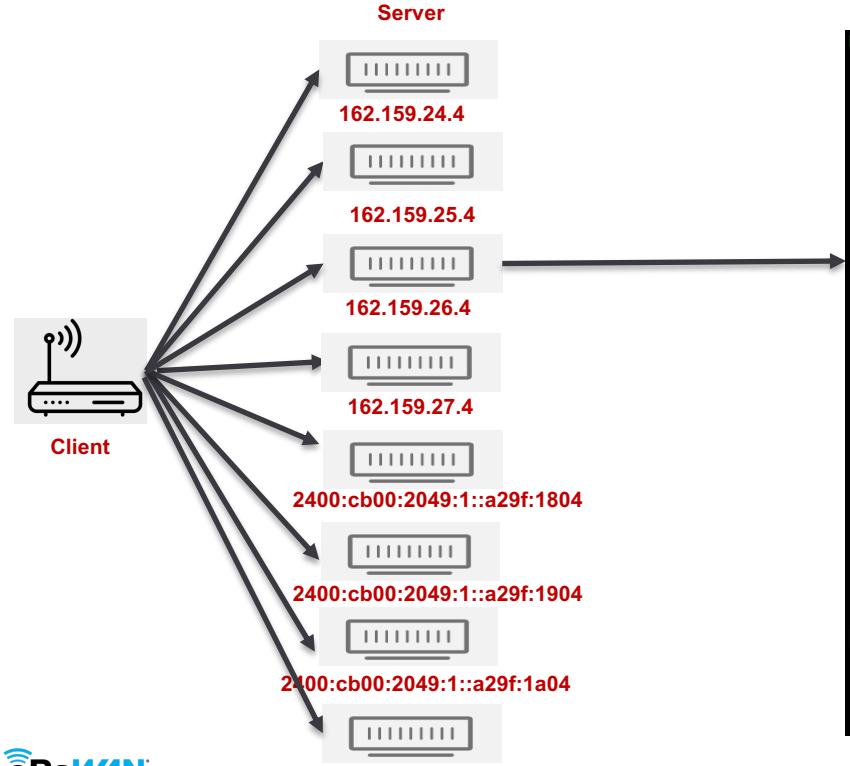
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;hostname.bind.                 CH      TXT

;; ANSWER SECTION:
hostname.bind.          60      CH      TXT     "CDG"

;; Query time: 21 msec
```

DNS Resiliency + Latency (2/2)

- Using Multiple Nameservers + Anycast




```
ubuntu@ip-172-31-10-125:~$ dig @162.159.26.4 hostname.bind TXT chaos

; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> @162.159.26.4 hostname.bind TXT chaos
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4741
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

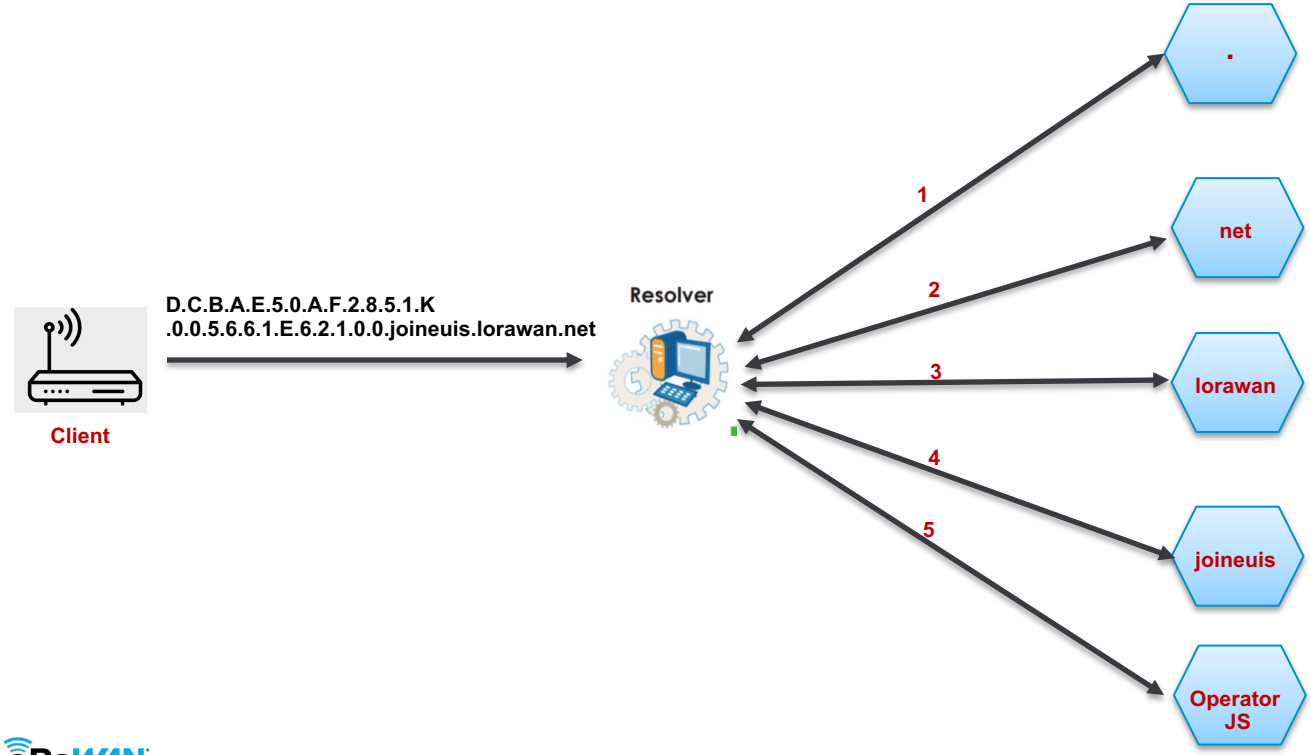
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;hostname.bind.                 CH      TXT

;; ANSWER SECTION:
hostname.bind.          60      CH      TXT     "SJC"

;; Query time: 1 msec
```

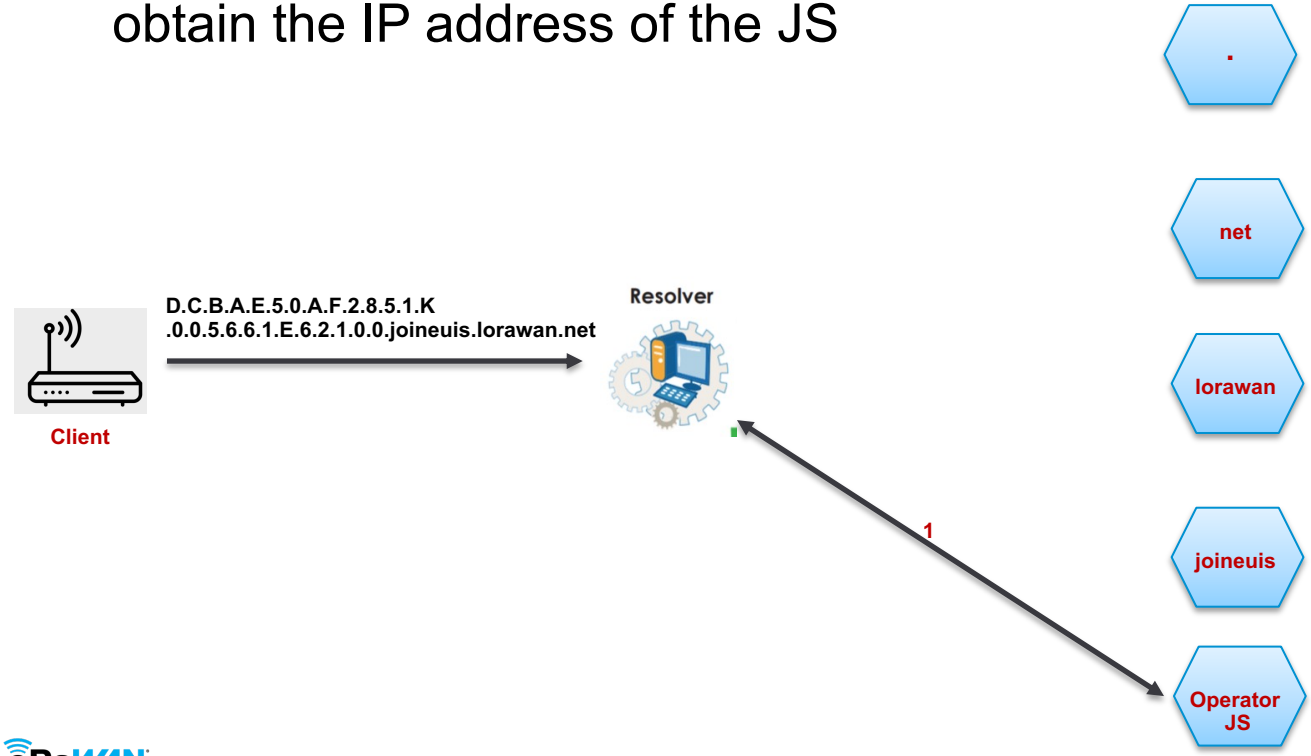
DNS Caching (1/2)

- Number of Queries initially to obtain the IP address of the JS



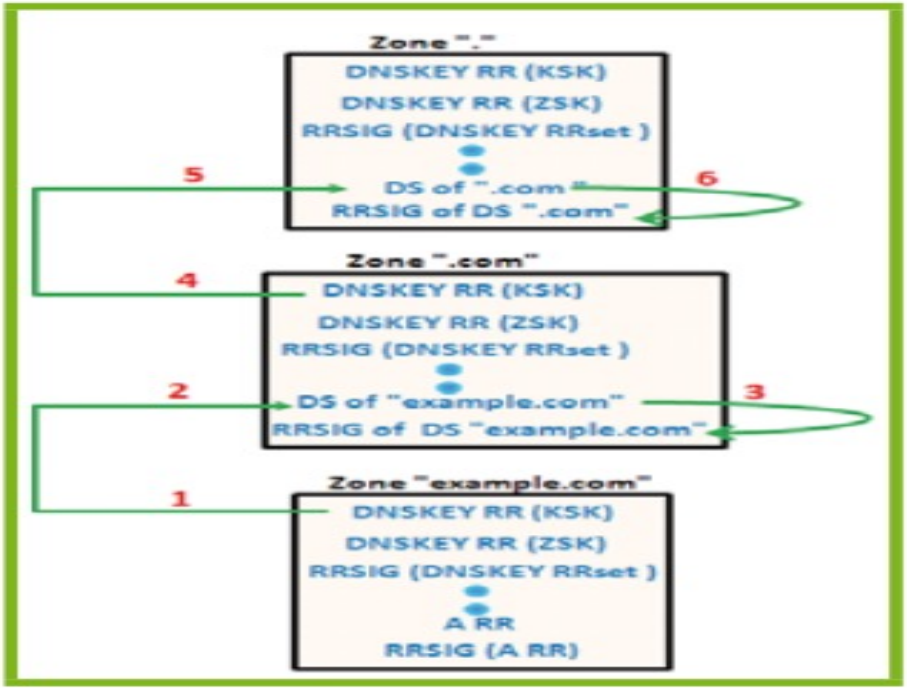
DNS Caching (2/2)

- After caching, most of the time only one DNS query is needed to obtain the IP address of the JS



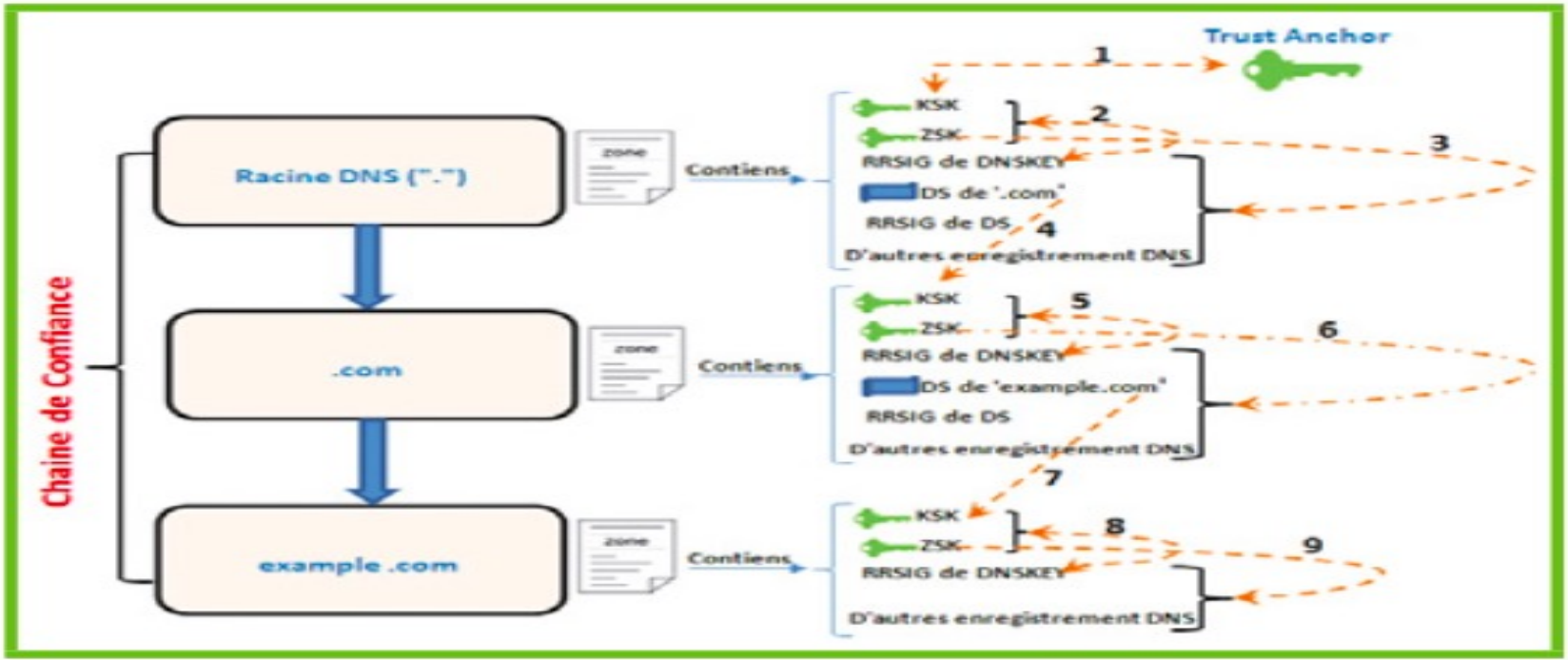
Security (1/2)

- What happens if an attacker gets access to the Zone file and modifies the information provisioned in the server?



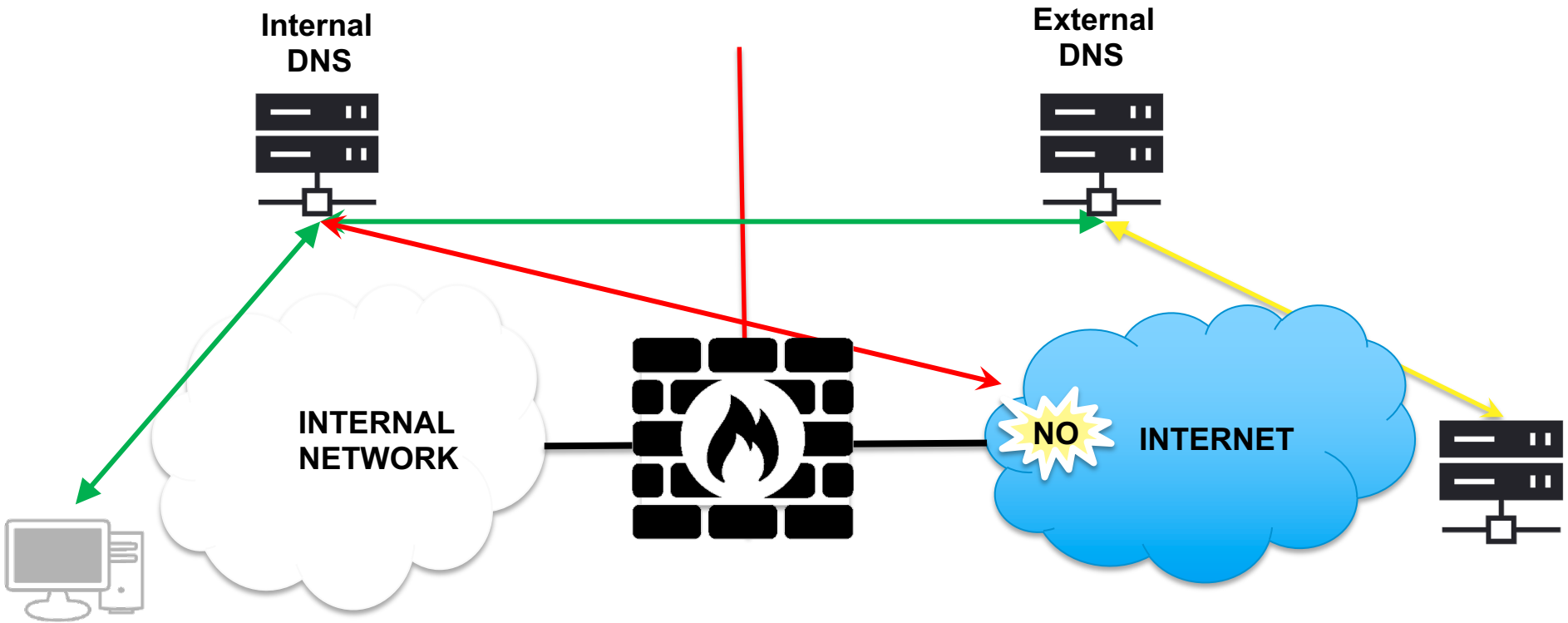
Security (2/2)

- What happens if an attacker spoofs the query and modifies the resolved IP address in the wire?



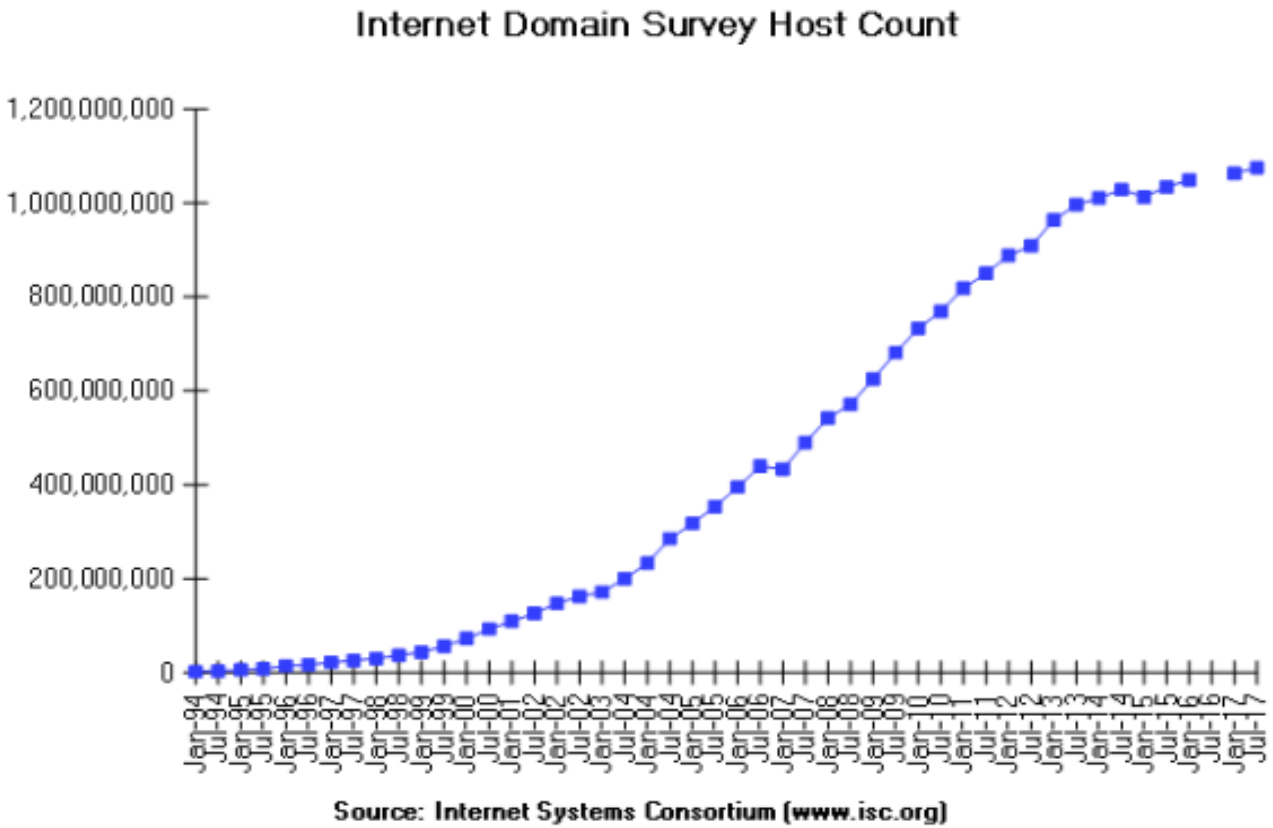
Split DNS

If you do not want to expose your DNS servers to the public



DNS scalability

Date	Domains
07/88	900
10/88	1,280
01/89	2,600
07/89	3,900
10/89	4,800
10/90	9,300
01/91	11,200
07/91	16,000
10/91	18,000
01/92	17,000



SLA agreement for DNS technical operators (Source: ICANN)

	Performance Specification Description	Nameserver
1	Service Availability	99.999% per calendar year
2	Processing Time Add, Modify, Delete	NA
3	Processing Time Query Domain	NA
4	Processing Time Whois	NA
5	Processing Time Nameserver Resolution	1.5 sec for 95%
6	Update Frequency	15 min for 95%
7	Planned Outage Duration	not allowed
8	Planned Outage Timeframe	not allowed
9	Planned Outage Notification	not allowed
10	Extended Planned Outage Duration	not allowed
11	Extended Planned Outage Timeframe	not allowed
12	Extended Planned Outage Notification	not allowed
13	Cross-Network Nameserver Performance	300 ms RTT and 10% packet loss