IOTROAM – ROAMING INITIATIVE BASED ON OPEN STANDARDS

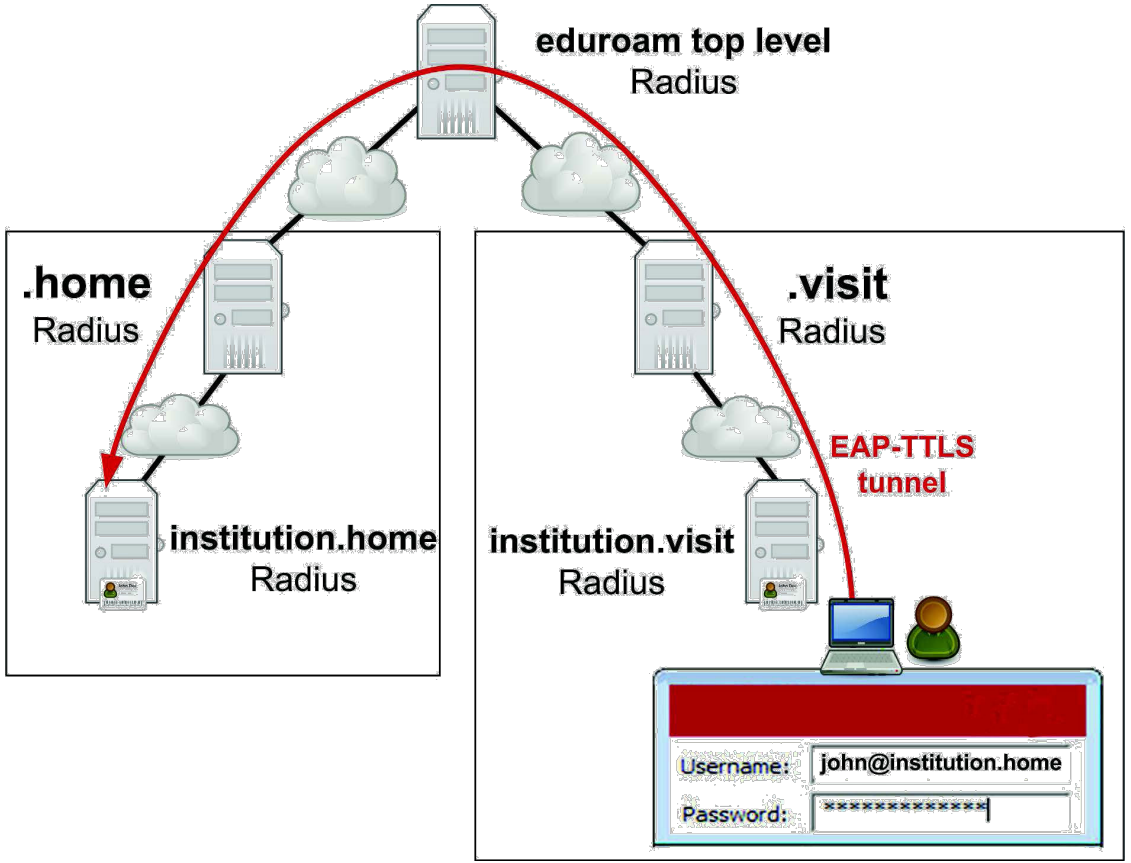
Presented by Sandoche Balackrichenan - Afnic

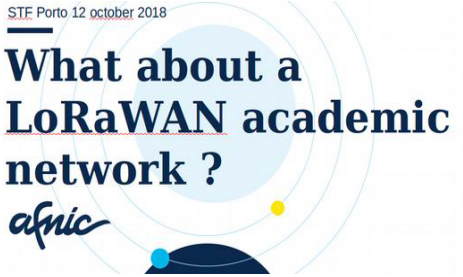
May 05, 2021

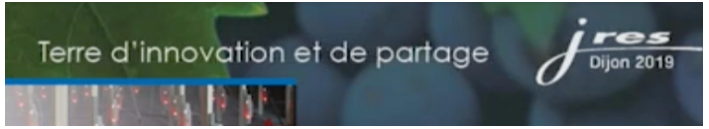
LoRa Alliance® Confidential

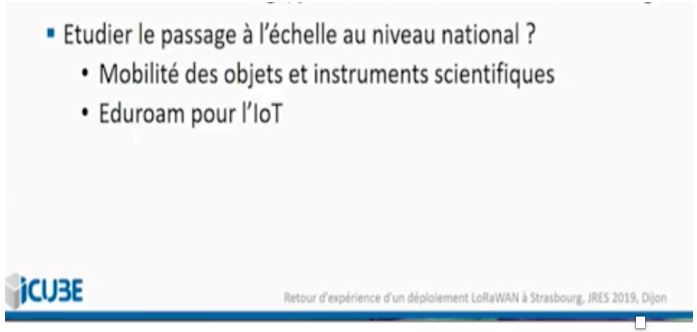
- IoT is an extension of Internet adding Constrained devices and networks
- Test a LoRaWAN roaming infrastructure using tested solutions in the Internet
- A PoC that is Open applicable for research purposes interoperable with other roaming solutions
- Feedback to LoRaWAN backend specifications
- Accelerate 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:









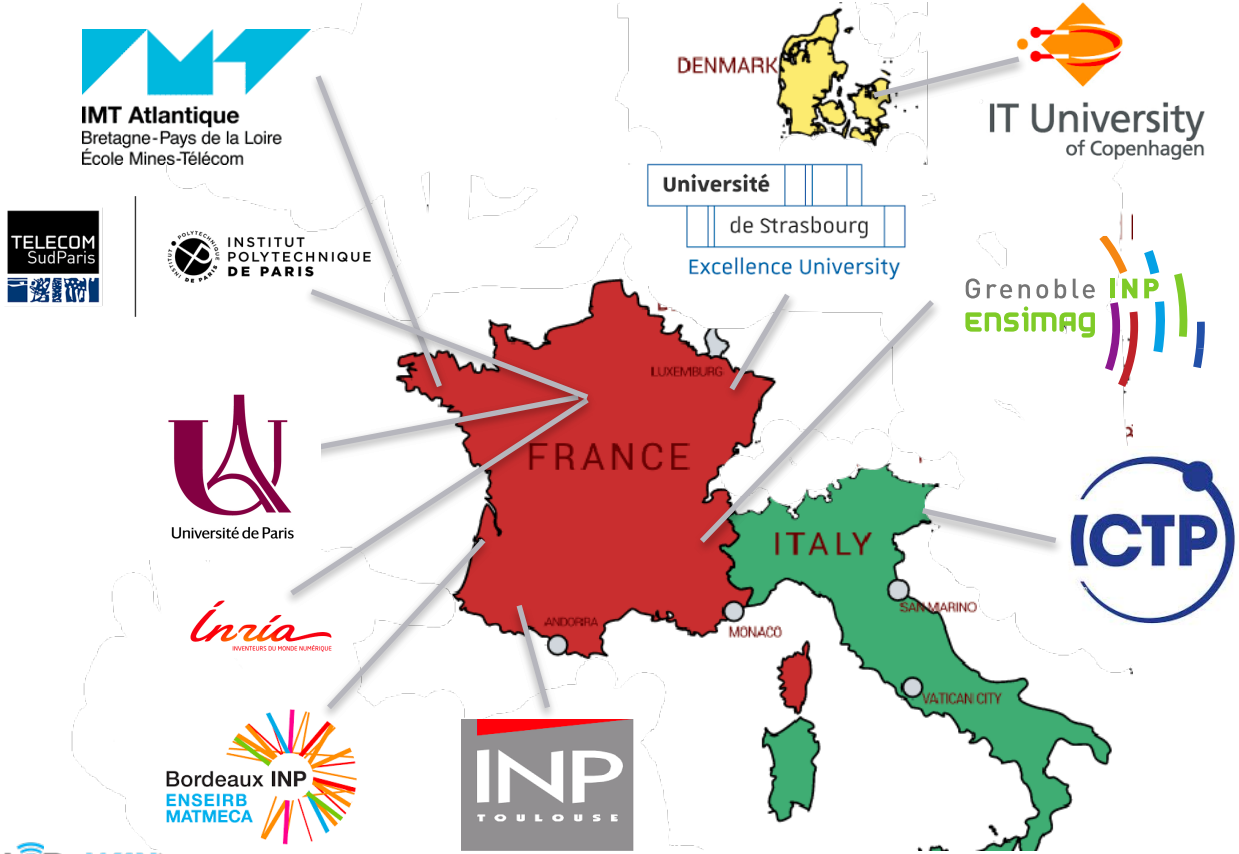
The involvement of National Research and Education Networks (NREN) in East Africa is key for the growth of Internet of Things (IoT) applications in the region, as they can host the access infrastructure to foster research in IoT and to serve the IoT community at large.

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 INTEREST



Already tested with

TELECOM SudParis

INSTITUT POLYTECHNIQUE DE PARIS

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Should work with any ED compatible to LoRaWAN Specifications

Should work with any NS, AS, JS software compatible with LoRa and LoRaWAN backend specifications

Need for minimum Out of Band Configurations

Provide dynamic discovery

Support for federated Identity providers

Setup a anchor trustable by all (LA)

…to experiment the designed architecture…

Issue – Use DNS Compatible Network Server stack

- Solution : Contribution to Chirpstack (chirpstack.io)

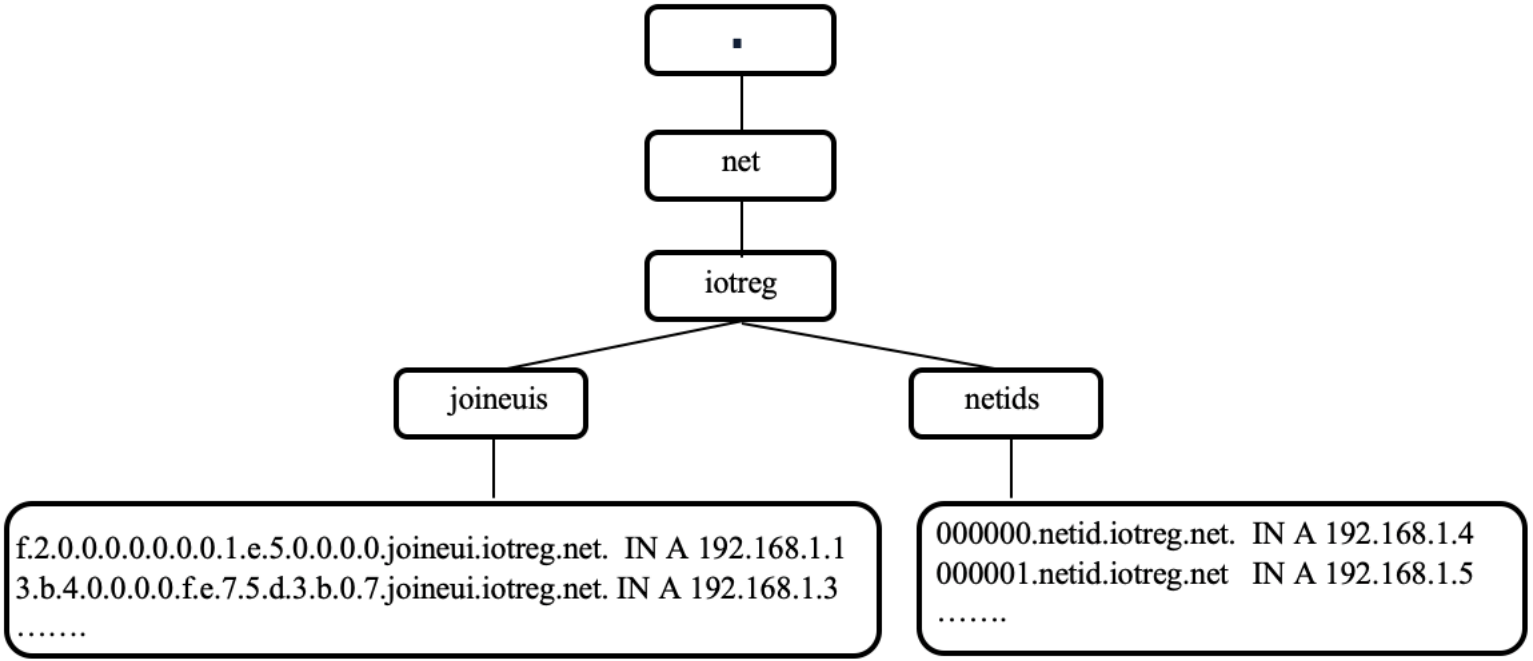
Issue – Use a LoRaWAN DNS Service

- Solution : Setup of iotreg.net DNS Service (operated by Afnic)

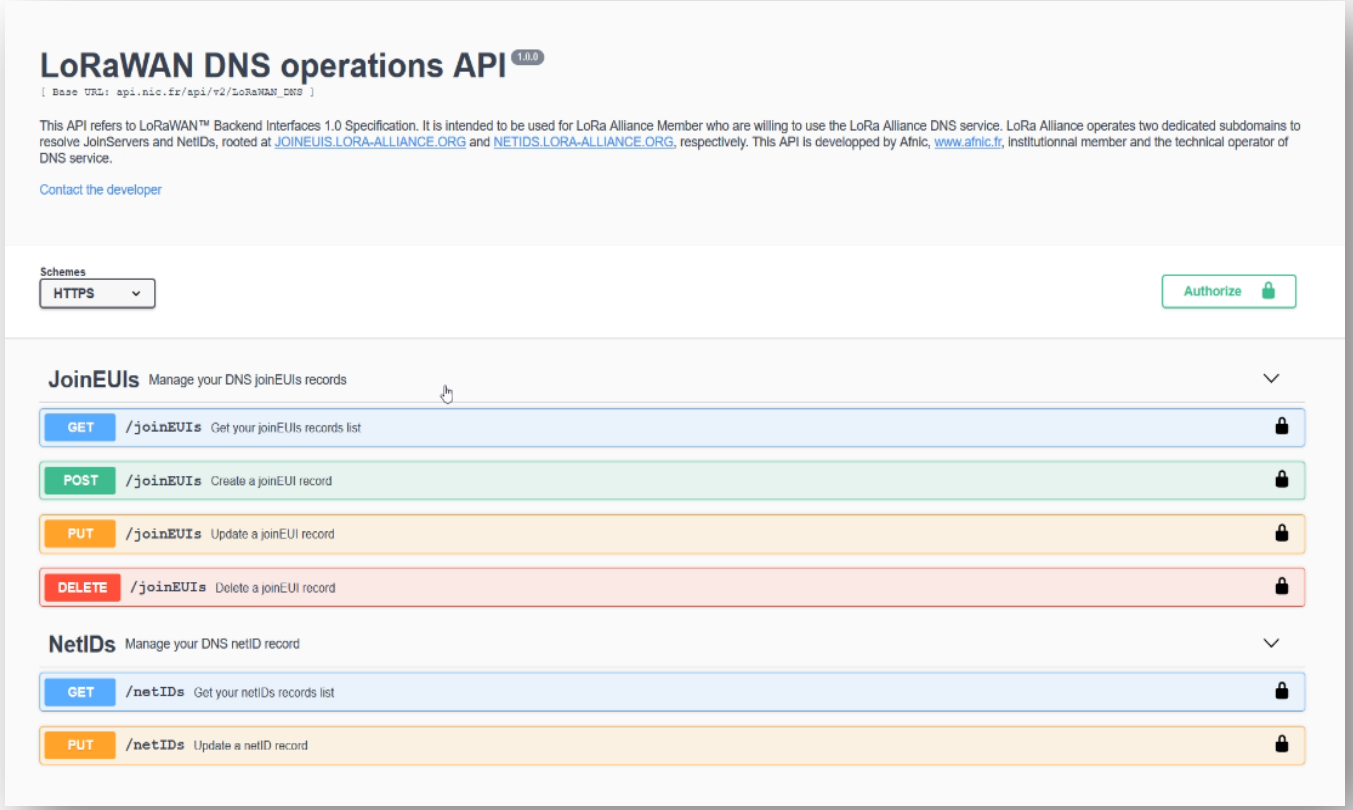
Issue – Securing Network backend components

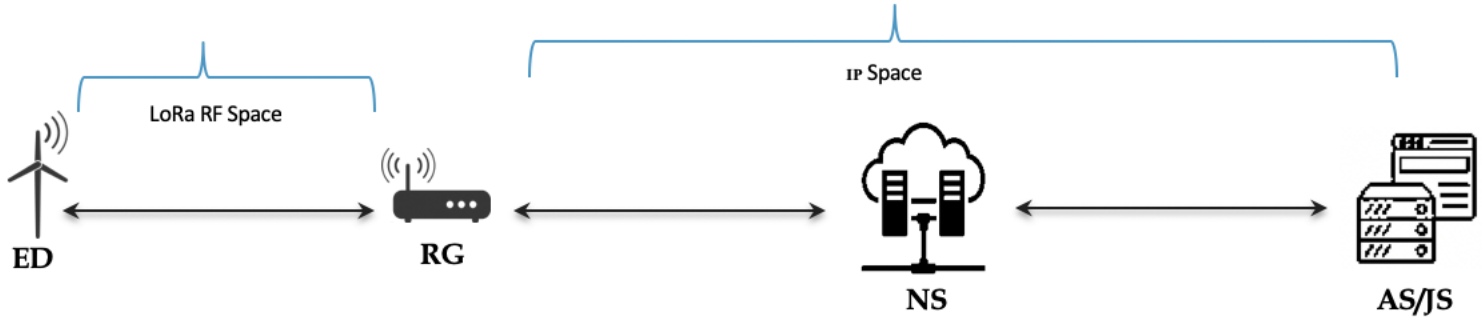
- Solution – Setup of a DNS PKI infrastructure (Afnic as Root CA)

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	

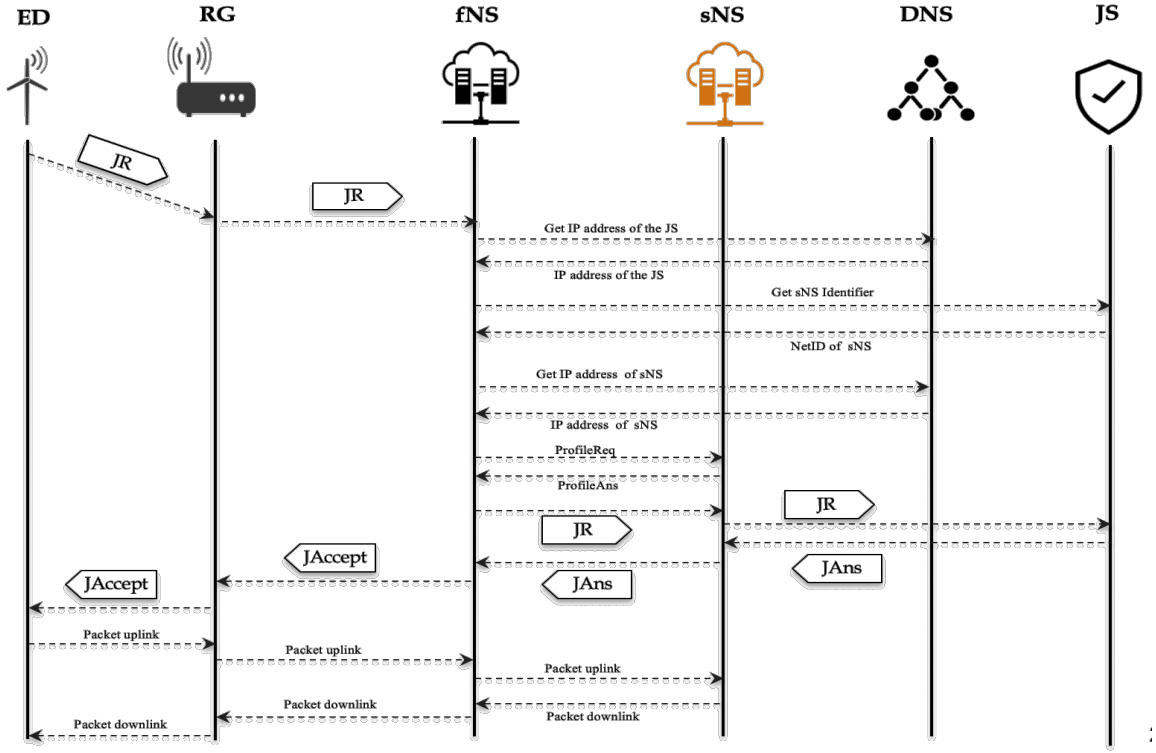

.
net
iotreg
joineuis
netids
f.2.0.0.0.0.0.0.0.1.e.5.0.0.0.0.joineui.iotreg.net. IN A 192.168.1.1
3.b.4.0.0.0.0.f.e.7.5.d.3.b.0.7.joineui.iotreg.net. IN A 192.168.1.3
…….
000000.netid.iotreg.net. IN A 192.168.1.4
000001.netid.iotreg.net IN A 192.168.1.5
…….

AFNIC'S API FOR DNS PROVISIONING

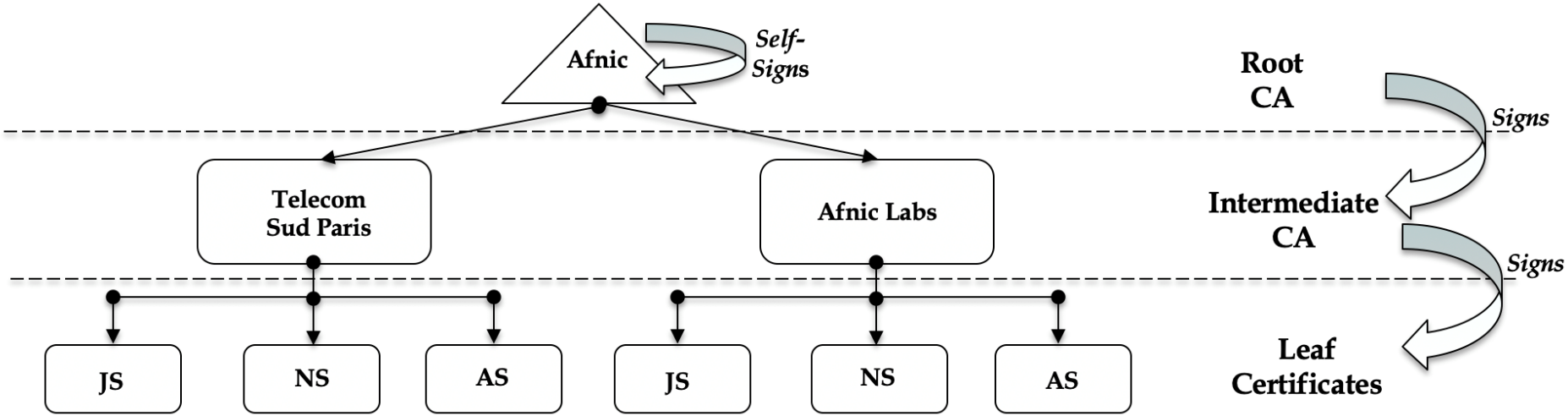



IP Space
LoRa RF Space
ED
RG
NS
AS/JS

MESSAGE FLOW USING DNS FOR PASSIVE 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	?


Afnic
Self-
Signs
Root
CA
Signs
Telecom
Sud Paris
Afnic Labs
Intermediate
CA
Signs
JS
NS
AS
JS
NS
AS
Leaf
Certificates

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

7. For the Certificates

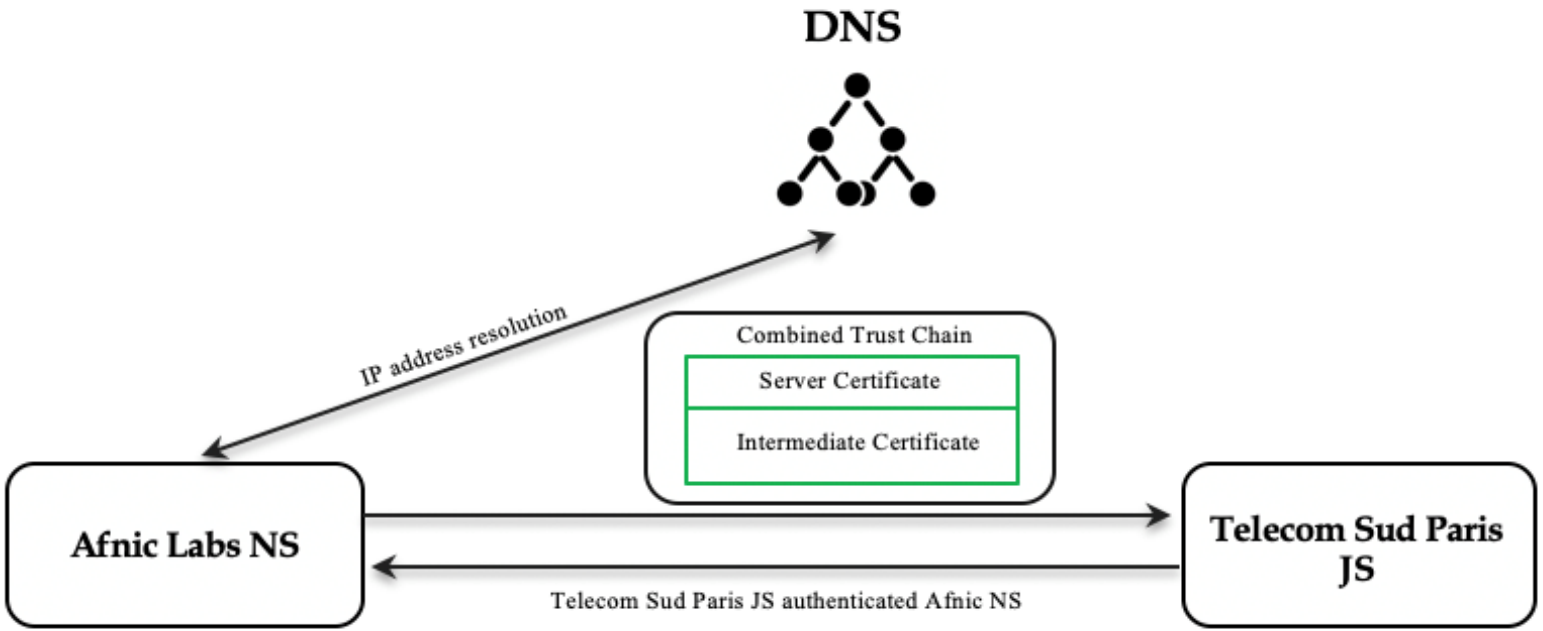
    - a.) Clone/Copy the required Files
    - b.) The directory structure is as here
    - b.) Modify intermediate-csr.json to suit you
    - c.) Modify "Certificate.json" in all subdirectories to suit your "CN" and host "IP addresses"
    - d.) For roaming, You have to modify the directory name to suit 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



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

- 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



ANR Work programme 2019

DiNS

DiNS: DNS Naming and Services for Secure Seamless IoT

The DiNS Consortium

Short Name	Full Name
INP	Grenoble INP, Laboratoire d'Informatique de Grenoble
AFNIC	Association française pour le nommage Internet en coopération
ACKLIO	Acklio SAS
BT	Bouygues Telecom/Objenious SA
IMT	IMT Atlantique, Laboratoire IRISA

LoRa Alliance®



@LoRaAlliance



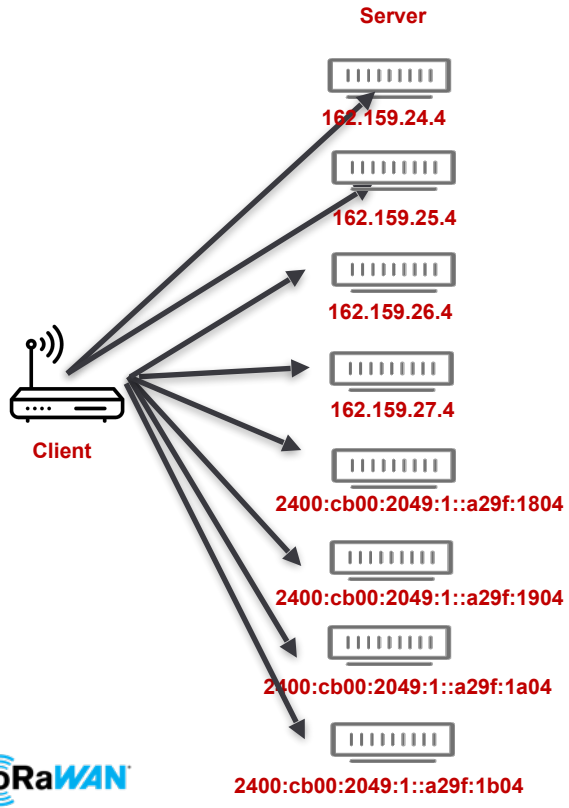
linkedin.com/company/loraalliance/



lora-alliance.org

LoRa Alliance® Confidential

- Using Multiple Nameservers

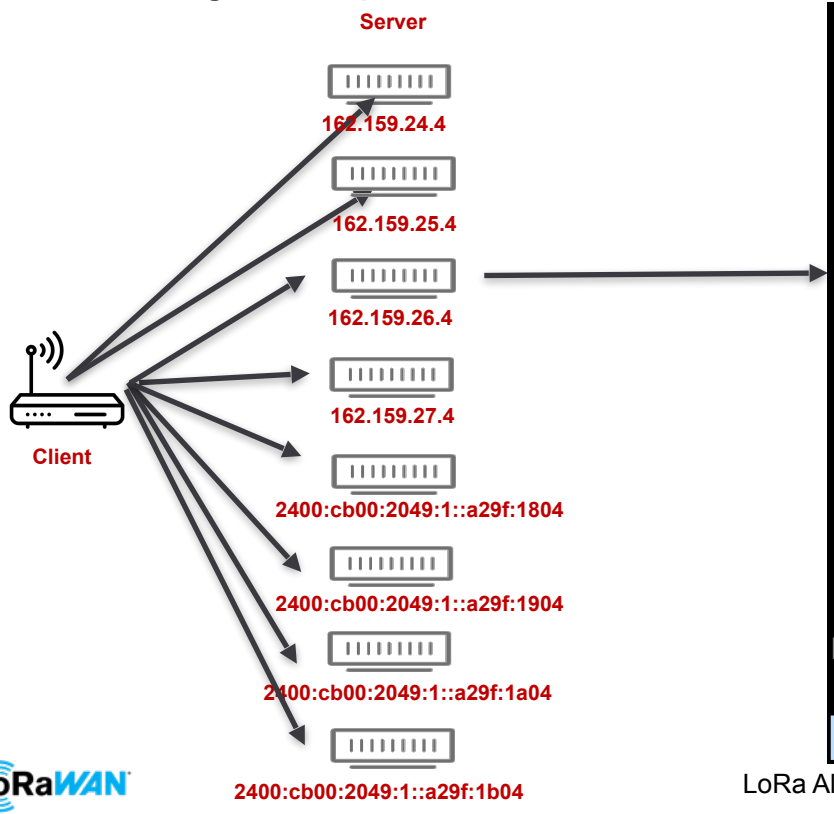



```
;; QUESTION SECTION:
;lora-alliance.org.             IN      NS

;; 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
```

- Using Multiple Nameservers + Anycast



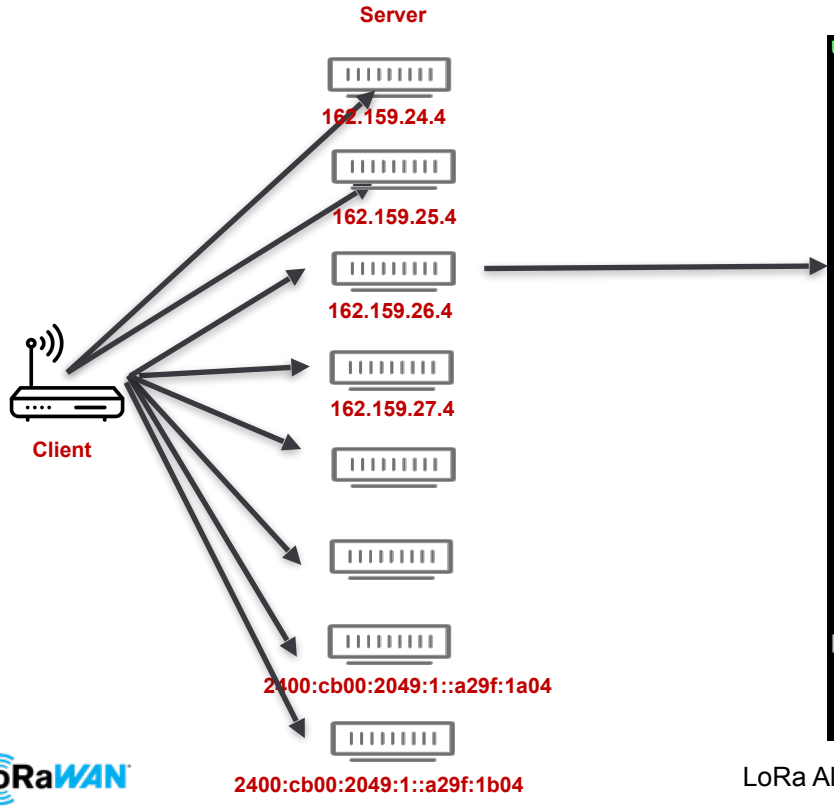

```
; <<>> DiG 9.10.6 <<>> @162.159.26.4 hostname.bind TXT chaos
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2494
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; 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
```

- Using Multiple Nameservers + Anycast




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

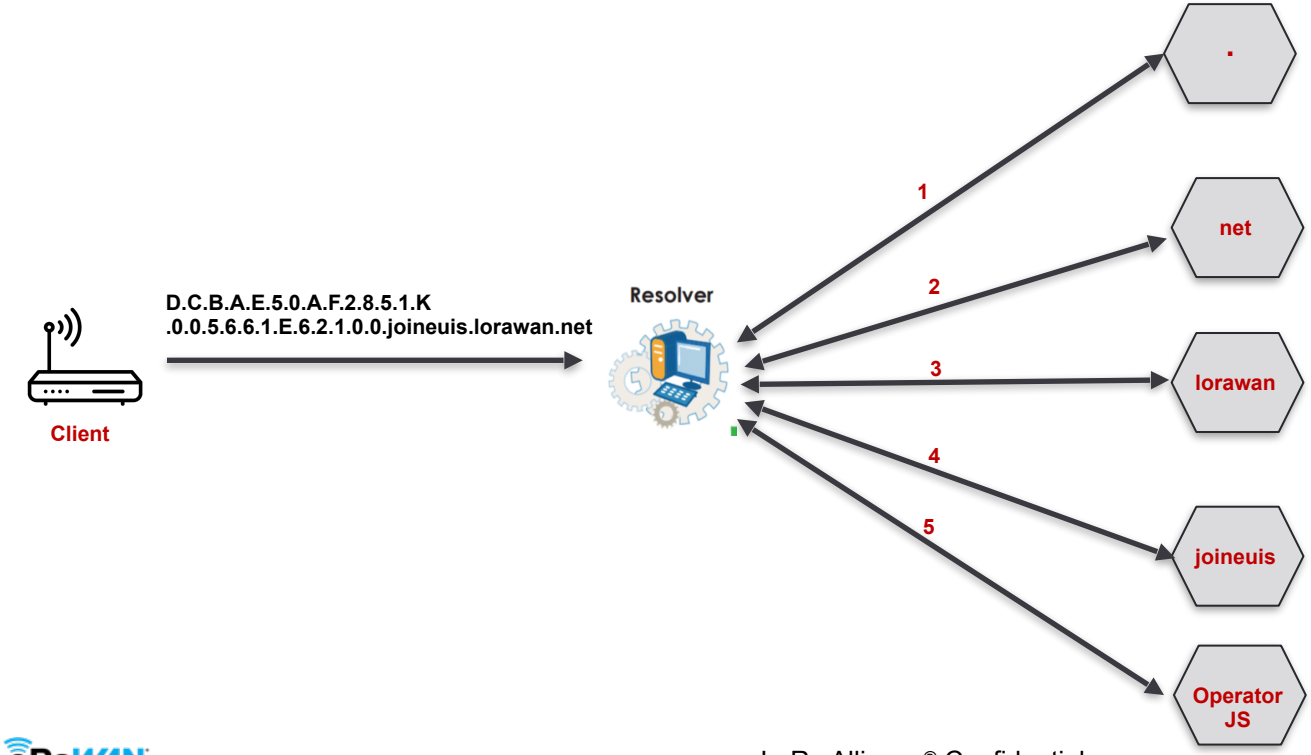
; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> @162.159.26.4 hostname.bind TXT chaos
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4741
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not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

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

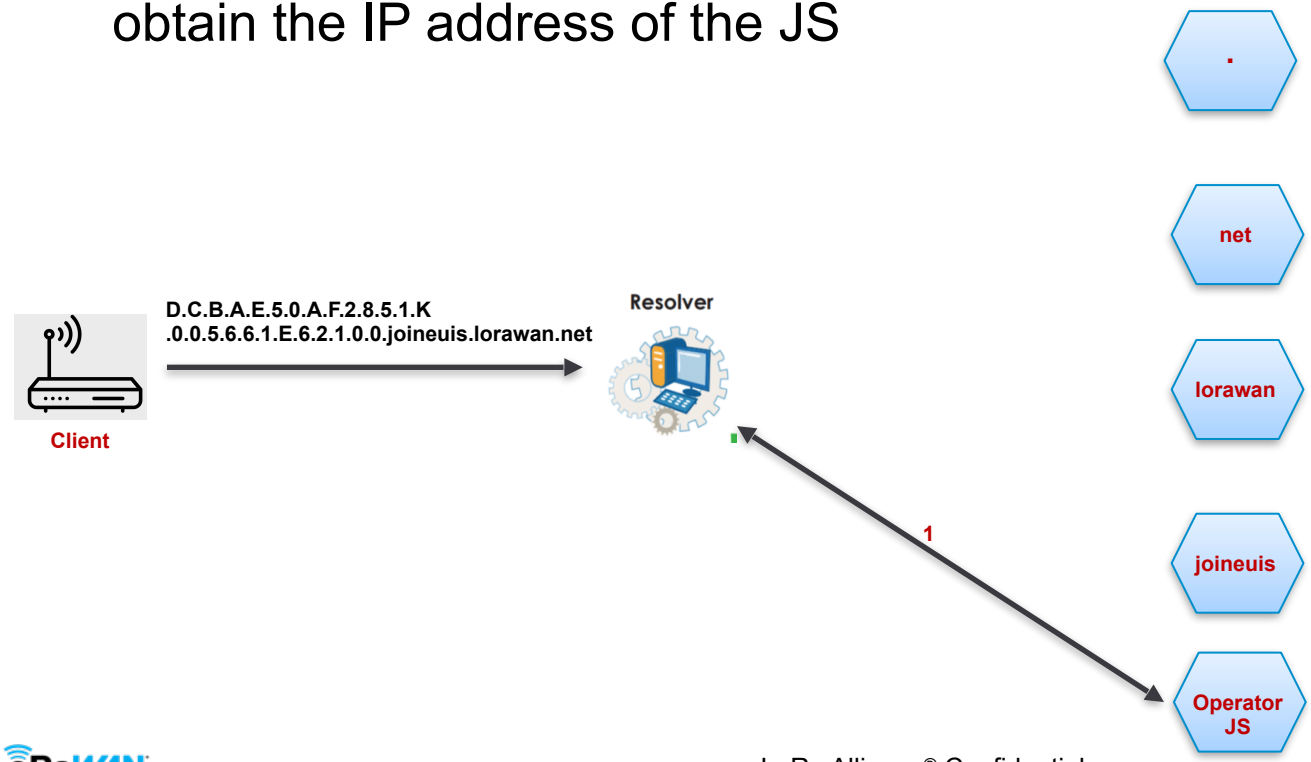
;; ANSWER SECTION:
hostname.bind.          60      CH      TXT     "SJC"

;; Query time: 1 msec
```

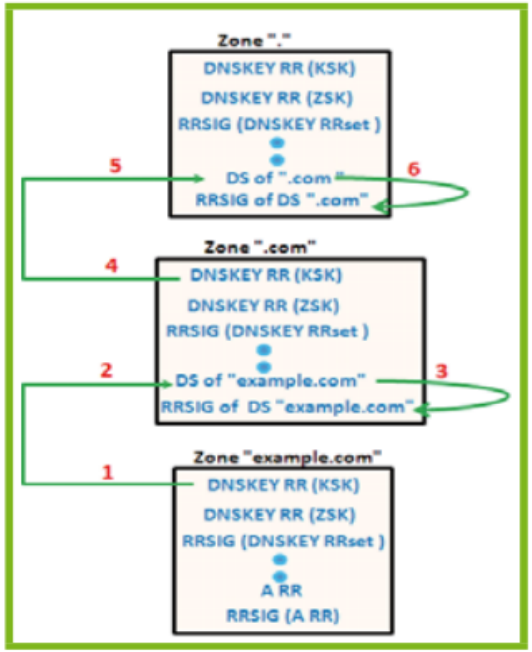
- Number of Queries initially to obtain the IP address of the JS



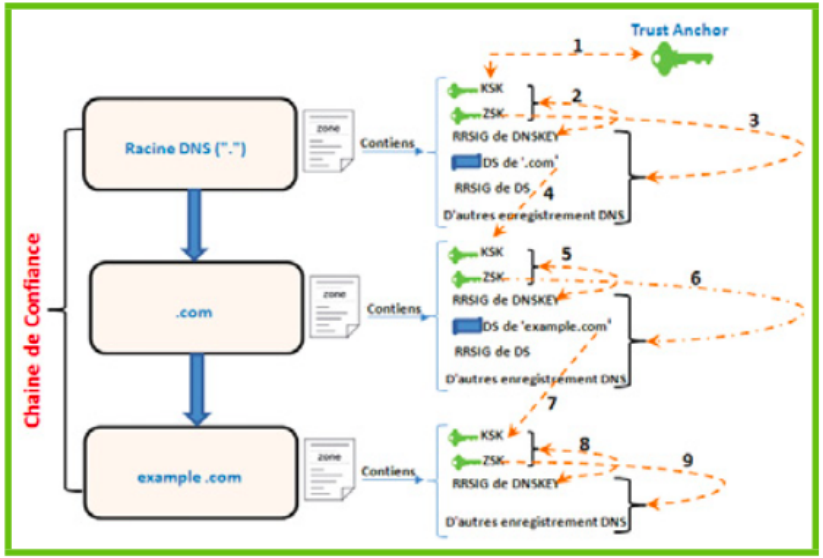
- After caching, most of the time only one DNS query is needed to obtain the IP address of the JS



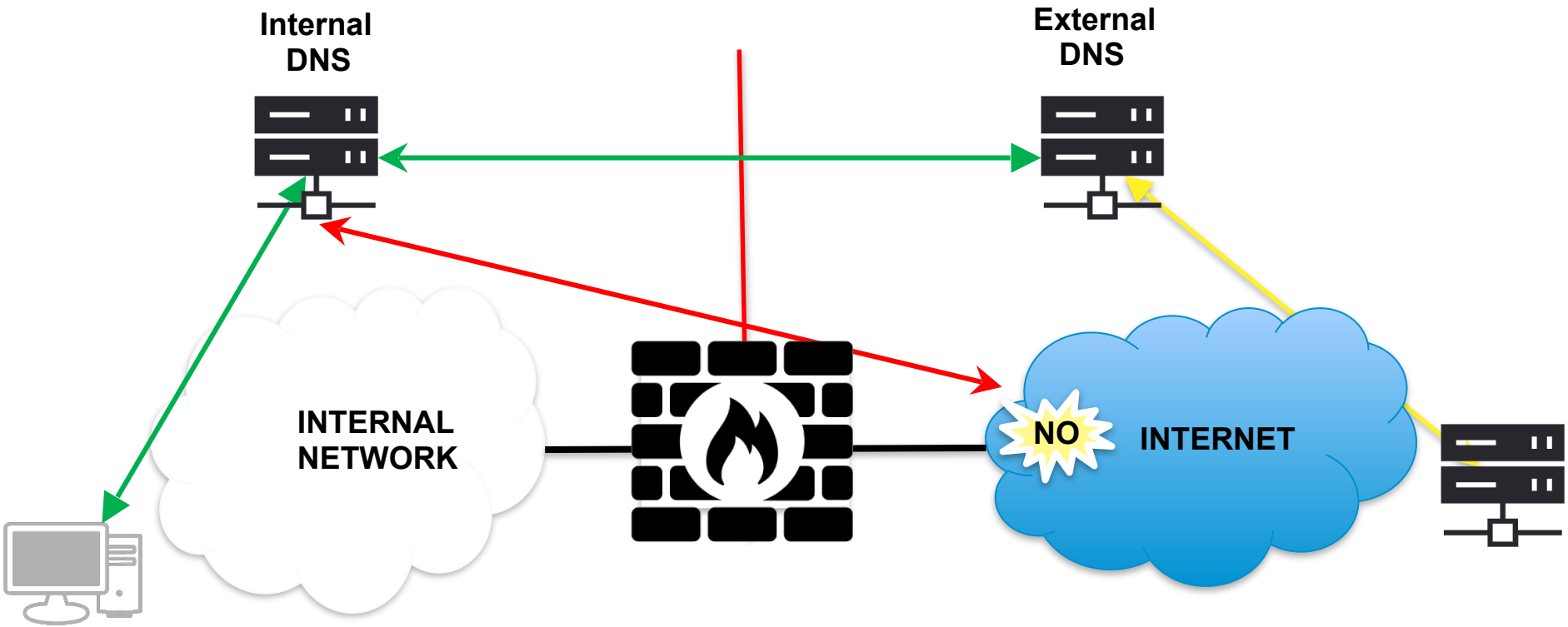
- What happens if an attacker gets access to the Zone file and modifies the information provisioned in the server?



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



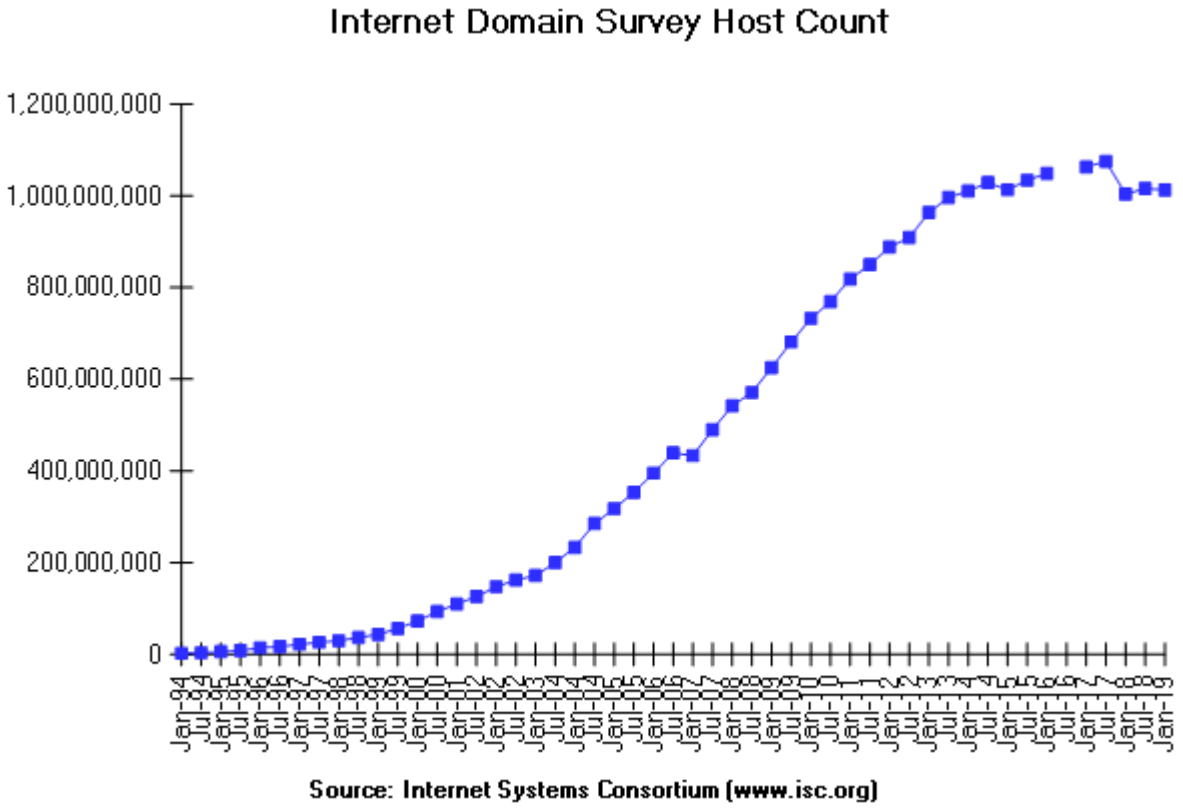
Split DNS
If you do not want to expose your DNS servers to the public



Internet Domain Survey, January, 2019

Number of Hosts advertised in the DNS

Date	Survey Host Count	Adjusted Host Count	Replied To Ping*
Jan 2019	1,012,695,272		-
Jul 2018	1,015,787,389		-
Jan 2018	1,003,604,363		-
Jul 2017	1,074,971,748		-
Jan 2017	1,062,660,523		-
Jan 2016	1,048,766,623		-
Jul 2015	1,033,836,245		-
Jan 2015	1,012,706,608		-
Jul 2014	1,028,544,414		-
Jan 2014	1,010,251,829		-
Jul 2013	996,230,757		-
Jan 2013	963,518,598		-
Jul 2012	908,585,739		-
Jan 2012	888,239,420		-
Jul 2011	849,869,781		-
Jan 2011	818,374,269		-
Jul 2010	768,913,036		-
Jan 2010	732,740,444		-
Jul 2009	681,064,561		-
Jan 2009	625,226,456		-



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