

# Esclavizando la zona raíz

*Carlos M. Martínez (@carlosm3011)*

LACNOG 2016

San José de Costa Rica – Setiembre 2016

# Introducción al DNS

- "Mapeo de nombres a números"
  - ¿que dirección IP le corresponde a [www.facebook.com](http://www.facebook.com)?
- Y además
  - Delegación de autoridad
  - Apoya diferentes tipos de aplicaciones (correo electrónico, hosting virtual, alias, etc.)
  - Redundancia (primarios y secundarios)

# Registros

- El DNS es una base de datos distribuida
- Los 'registros' son 5-tuplas con los siguientes campos
  - Nombre
  - Clase (siempre *IN* para nosotros)
  - TTL
  - Tipo
  - Valor
- Ejemplo
  - `www.example.com. 3600 IN A 192.168.1.10`

# Zonas

- Grupo de registros bajo el mismo sufijo y bajo la misma autoridad administrativa
- ¿Como se crean? Mediante la delegación, usando el registro NS

```
carlos -- -bash -- 89x21
~ -- -bash
...
~ -- carlos@coati: ~ -- -bash
~ -- -bash
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;labs.lacnic.net.          IN      SOA

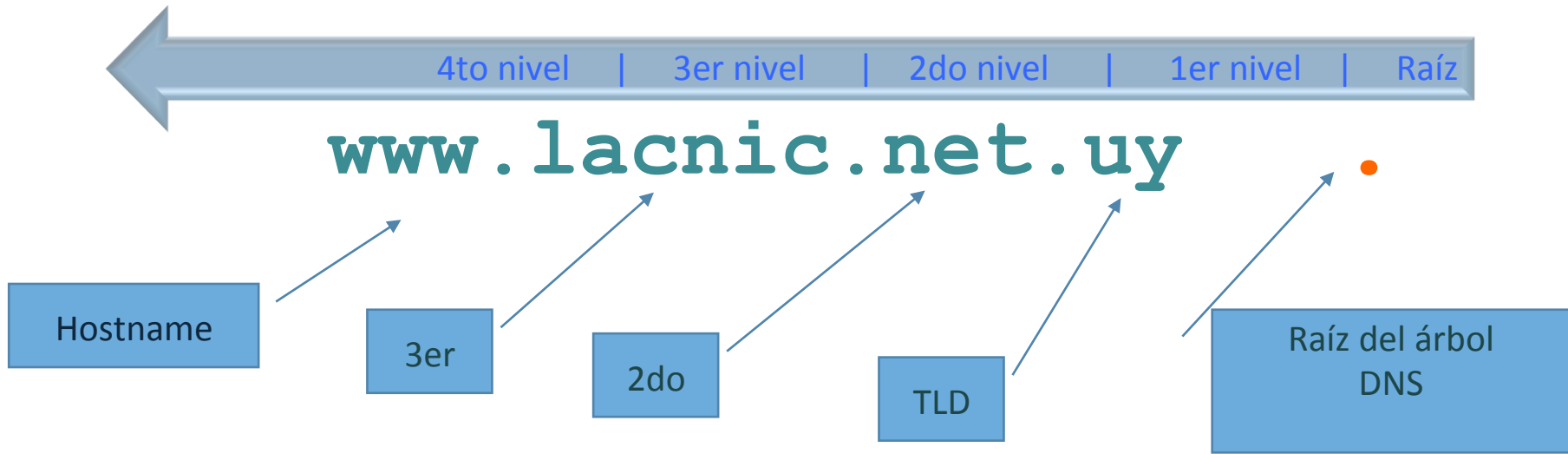
;; ANSWER SECTION:
labs.lacnic.net.         180    IN      SOA     labs.lacnic.net.  eng.lacnic.net.  20160922
00 4800 3600 2419200 3600

;; AUTHORITY SECTION:
labs.lacnic.net.         180    IN      NS      ns3.labs.lacnic.net.
labs.lacnic.net.         180    IN      NS      ns2.labs.lacnic.net.
labs.lacnic.net.         180    IN      NS      ns1.labs.lacnic.net.

;; Query time: 66 msec
;; SERVER: 200.7.84.5#53(200.7.84.5)
;; WHEN: Fri Sep 23 22:20:25 2016
;; MSG SIZE rcvd: 259

oliver:~ carlos$
```

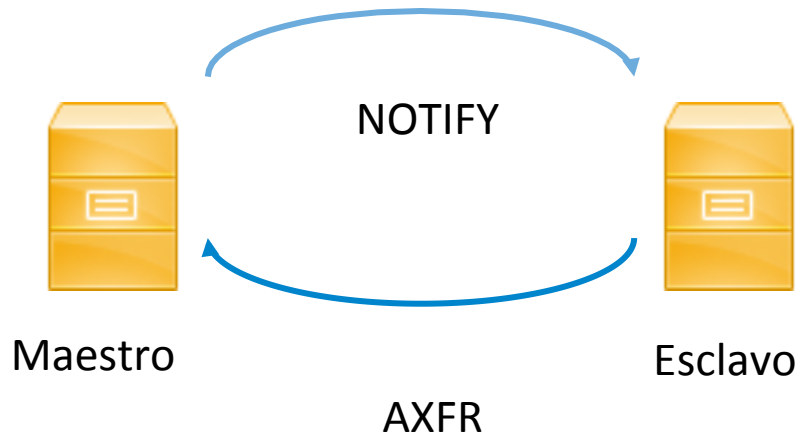
# Estructura de un nombre de dominio



- Los niveles del árbol reflejan las divisiones administrativas
- El root del arbol esta siempre presente de forma ímplicita
- Restricciones:
  - 127 niveles, 63 caracteres por etiqueta
- Los niveles superiores “delegan” hacia los inferiores

# Primarios y secundarios

- Redundancia, DNS-style



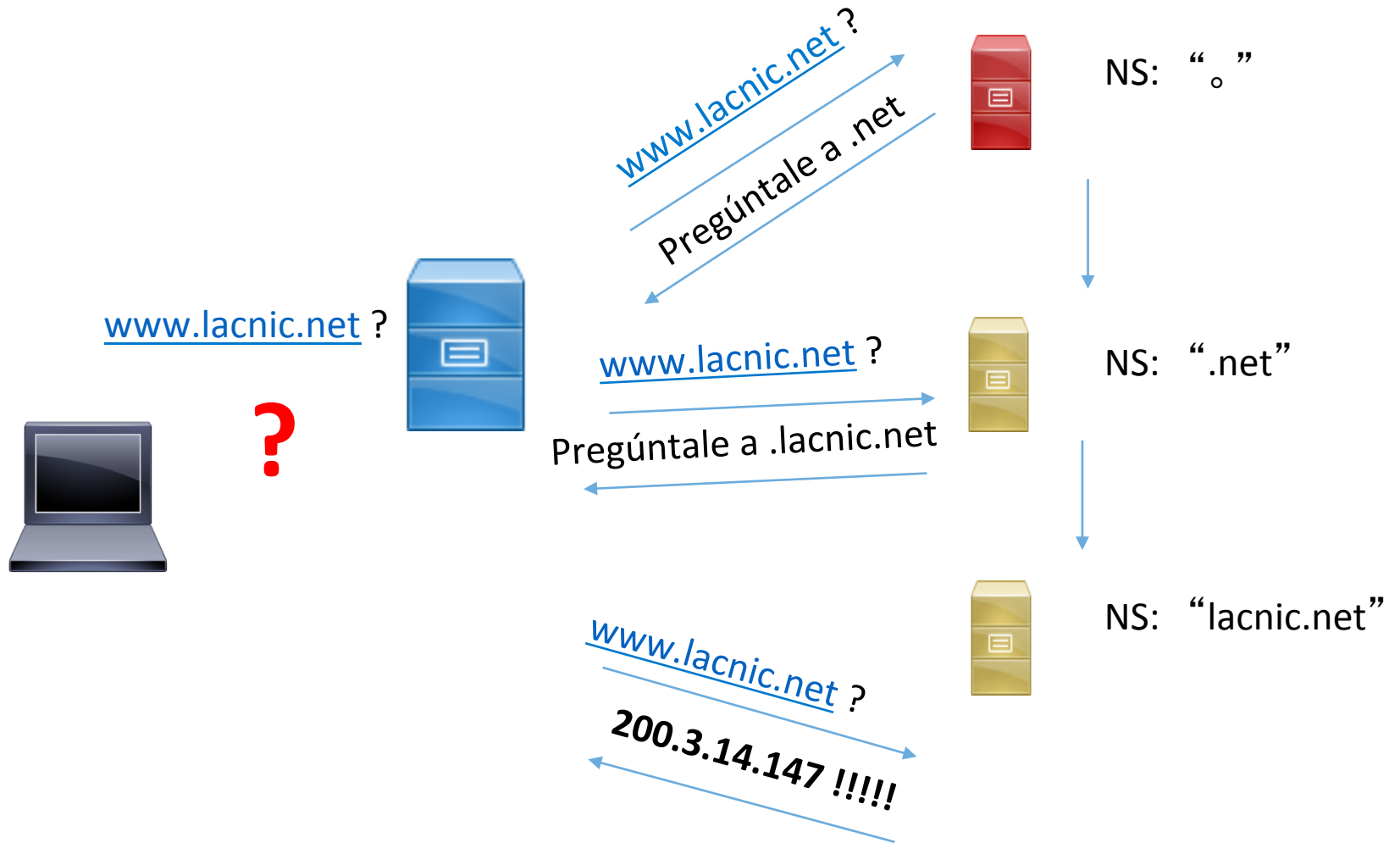
- AXFR es un pseudo-tipo de registro, simboliza la operación de transferencia de zona
- ¿Como saber si la zona cambió? Se compara el número de serie del registro SOA

# Transferencias de zona

- Usando dig:

```
carlos — -bash — 89x21
~ — -bash
~ — carlos@coati: ~ — -bash
~ — -bash
zuerich.      86400  IN      NSEC    zw. NS DS RRSIG NSEC
zw.           172800 IN      NS      ns1.telone.co.zw.
zw.           172800 IN      NS      ns2.gip.net.
zw.           172800 IN      NS      ns2.telone.co.zw.
zw.           172800 IN      NS      ns3.telone.co.zw.
zw.           86400  IN      NSEC    . NS RRSIG NSEC
zw.           86400  IN      RRSIG   NSEC 8 1 86400 20161006170000 20160923160
000 46551 . gFCukJJqhZ0Zdix9hcon5S1G58ctqfgwW0L5ccGL8mArjPCUIQOMK/ED jM21YrA1fHLFP8B82AMv
VKy0b1ONBTJpaXKQJySsz3Tl6pQELdS959m+ Ppu8rCvSkhzHCIvHhs0mCouSe0Kgm/UjvpzhrSdwY+/V2j/1FlmK
r5ZN yJM=
ns1.telone.co.zw. 172800 IN      A       194.133.122.47
ns2.telone.co.zw. 172800 IN      A       194.133.122.42
ns3.telone.co.zw. 172800 IN      A       194.133.122.34
.                86400  IN      SOA     a.root-servers.net. nstld.verisign-grs.co
m. 2016092301 1800 900 604800 86400
;; Query time: 4782 msec
;; SERVER: 192.0.32.132#53(192.0.32.132)
;; WHEN: Fri Sep 23 22:12:07 2016
;; XFR size: 21215 records (messages 56, bytes 902188)
oliver:~ carlos$ dig axfr . @lax.xfr.dns.icann.org +tcp
```

# Resolución recursiva





# La zona raíz

- ¿Que encontramos en la zona raíz?
- Tenemos los registros de delegación a todas las zonas de primer nivel (TLDs)

```
cr. 172800 IN NS a.ns.cr.
cr. 172800 IN NS a.lactld.org.
cr. 172800 IN NS c.ns.cr.
cr. 172800 IN NS p.nic.cr.
cr. 172800 IN NS de.nic.cr.
cr. 172800 IN NS ns3.nic.mx.
cr. 172800 IN NS ns-ext.nic.cl.
de.nic.cr. 172800 IN NS AAAA 2001:678:e:107::53
de.nic.cr. 172800 IN NS A 194.0.11.107
```

# Servidores raíz

- La recursión comienza en la raíz
- Por motivos históricos la Internet cuenta al día de hoy con 13 servidores raíz “principales”
  - Más de 300 en total si contamos las copias anycast
- Los servidores raíz están bajo el dominio “*root-servers.net*”
- Se llaman con una letra, desde la A a la M
- Ejemplo “i.root-servers.net”

# La zona raíz en BIND

- La zona raíz se configura de una manera particular en diferentes software de DNS
- En bind se utiliza un tipo especial de zona conocido como *'root hints'*

```
zone "." in {  
    type hint;  
    file "/v/named.root";  
};
```

- El archivo de *'hints'* contiene una lista de root servers

# El archivo de 'root hints'

```
;      last update:      August 25, 2016
;      related version of root zone:  2016082500;
; formerly NS.INTERNIC.NET
;
.          3600000          NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.  3600000          A      198.41.0.4
A.ROOT-SERVERS.NET.  3600000          AAAA   2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU;
.          3600000          NS      B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.  3600000          A      192.228.79.201
B.ROOT-SERVERS.NET.  3600000          AAAA   2001:500:84::b
```

- *El archivo hints se 'parece' a zona zona DNS pero no lo es.*
- *Notablemente NO tiene SOA.*

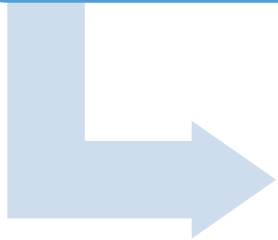
# ‘Root Priming’

- ¿Alguna vez se preguntaron si las direcciones IP de los servidores raíz cambian?
- Y si cambian, ¿porque mi archivo root.hints no está siempre desactualizado?
  - [ <https://deephought.isc.org/article/AA-01309/0/Root-hints-a-collection-of-operational-and-configuration-FAQs.html> ]
- En corto, el contenido del archivo de “root hints” es solo una *pista*. El servidor de DNS va a tratar de obtener una lista de registros NS para “.” a partir del primer servidor de la lista de hints que le responda

# 'Root Priming'

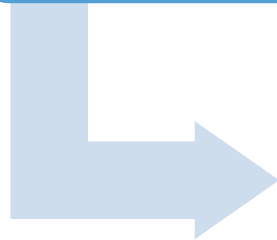
Leer el 'root hints'

- Archivo de texto **local**



Confirmar los hints

- Consultar a la lista de hints por los NS de la raíz

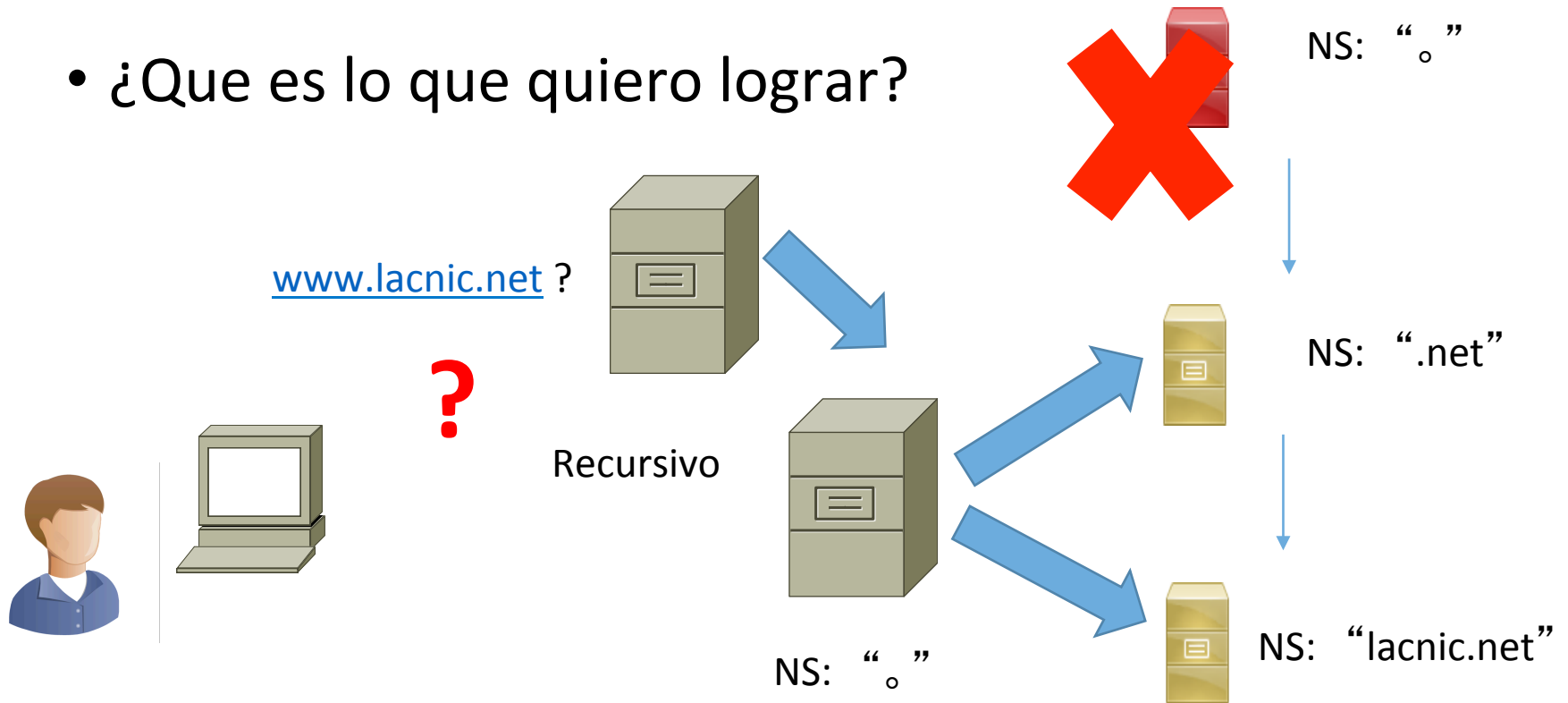


Usar la lista de roots confirmada

- Al final del priming los hints no se utilizan más

# Planteo del experimento

- ¿Que es lo que quiero lograr?



- ***Tener un root server local***

# AXFR de la raíz

- Es posible hacer AXFR de la zona raíz desde diferentes lugares
  - Varios root servers
  - Servidores de AXFR de ICANN
    - lax.xfr.dns.icann.org
    - iad.xfr.dns.icann.org
  - [ <http://www.dns.icann.org/services/axfr/> ]
- ¿Cómo?

```
$ dig @iad.xfr.dns.icann.org axfr . | tee mi.root.txt
```

```
$ ls -lh mi.root.txt
```

```
-rw-r--r--  1 carlos  staff   1.6M Sep 28 18:05 mi.root.txt
```



# Configuración de BIND

- ¿Que elementos necesitamos?
- Un archivo de 'root hints' que contenga solamente nuestro root local
- ¿Que hacemos con el *primming*?
  - Si usamos la zona raíz tal como la trajimos, el root server va a solamente usar los hints para consultar nuevamente por los NS de la zona raíz
  - ***Pero lo podemos engañar un poco***

# ¡Mi propio servidor raíz!

- Configuración del recursivo

```
// RECURSIVE CLIENT OF THE SLAVE ROOT
options {
    directory "/opt/bbsigner";
    notify no;
    allow-recursion {...};
    listen-on port 53 { any; };
};

zone "." in {
    type hint;
    file "/v/named.root.local";
};
```

# ¡Mi propio servidor raíz!

- *root hints* local

```
; -----  
; named.root.local  
; root hints file used for locally slaving the root zone  
;  
; -----  
.           360      NS    a.root-loc.  
a.root-loc. 360      A     172.19.0.2
```

# ¡Mi propio servidor raíz!

- Configuración del autoritativo (el raíz privado)

```
options {  
    ...  
};  
  
zone "." in {  
    type master;  
    file "/v/db.root.full";};  
  
zone "root-loc" {  
    type master;  
    file "/v/db.root-loc";  
};
```

# ¡Mi propio servidor raíz!

- ¡Probando!

```
$ dig +trace www.lacnic.net | tee trace.lacnic.net.txt
```

# ¡Mi propio servidor raíz!



'priming' en acción!

```
<signer/bin/dig @localhost www.lacnic.net +trace |
<signer/bin/dig @localhost www.lacnic.net +trace | grep -v RRSIG
1 <signer/bin/dig @localhost www.lacnic.net +trace | grep -v RRSIG
2
3 ; <<>> DiG 9.10.2 <<>> @localhost www.lacnic.net +trace
4 .          518400 IN NS G.ROOT-SERVERS.NET.
5 .          518400 IN NS I.ROOT-SERVERS.NET.
6 .          518400 IN NS M.ROOT-SERVERS.NET.
7 .....
8 .          518400 IN NS J.ROOT-SERVERS.NET.
9 .          518400 IN NS C.ROOT-SERVERS.NET.
10 ;; Received 825 bytes from 127.0.0.1#53(localhost) in 0 ms
11
12 net.       172800 IN NS d.gtld-servers.net.
13 net.       172800 IN NS i.gtld-servers.net.
14 .....
15 net.       172800 IN NS e.gtld-servers.net.
16 ;; Received 735 bytes from 192.36.148.17#53(I.ROOT-SERVERS.NET) in 70 ms
17
18 lacnic.net. 172800 IN NS ns2.dns.br.
19 lacnic.net. 172800 IN NS sec3.apnic.net.
20 lacnic.net. 172800 IN NS ns2.lacnic.net.
21 lacnic.net. 172800 IN NS dns.anycast.lacnic.net.
22 ;; Received 598 bytes from 192.26.92.30#53(c.gtld-servers.net) in 76 ms
23
24 www.LACNIC.NET. 7200 IN A 200.3.14.147
25 LACNIC.NET. 7200 IN NS ns2.dns.br.
26 LACNIC.NET. 7200 IN NS NS.LACNIC.NET.
27 LACNIC.NET. 7200 IN NS TINNIE.ARIN.NET.
28 ;; Received 2136 bytes from 200.3.13.10#53(ns.lacnic.net) in 154 ms
```

# La raíz, completamente local

- Para hacer que la zona raíz sea completamente local debemos lograr que el *priming también devuelva servidores locales*
- Para eso modificamos la zona raíz y cambiamos los registros NS por los locales, y creamos una zona similar a 'root-servers.net' pero local

# Zona raíz modificada

- NS-Set

```
14065 IN SOA a.  
<signer/bin/dig @localhost www.lacnic.net +trace | . 14065 IN SOA a.  
1 . 14065 IN SOA a.root-loc.  
nstd.verisign-grs.com. 2016092702 180  
2 0 900 604800 86400  
3  
4 . 10 IN NS a.root-loc.  
5 root-loc. 10 IN NS a.root-loc.  
6 a.root-loc. 10 IN A 172.19.0.2  
7  
8 aaa. 172800 IN NS ns1.dns.nic.aaa.  
9 aaa. 172800 IN NS ns2.dns.nic.aaa.  
10 aaa. 172800 IN NS ns3.dns.nic.aaa.  
11 aaa. 172800 IN NS ns4.dns.nic.aaa.
```



# La zona raíz completamente local

```
<gner/bin/dig +trace www.lacnic.net | grep -v RRSI
UNF
<signer/bin/dig @localhost www.lacnic.net +trace |
14065 IN SOA a. www.lacnic.net | grep -v RR
1 <gner/bin/dig +trace www.lacnic.net | grep -v RRSIG | grep -v DS
2
3 ; <<>> DiG 9.10.2 <<>> +trace www.lacnic.net
4 ;; global options: +cmd
5 . 5 IN NS a.root-loc.
6 ;; Received 67 bytes from 127.0.0.11#53(127.0.0.11) in 1 ms
7
8 net. 172800 IN NS k.gtld-servers.net.
9 net. 172800 IN NS t.gtld-servers.net.
10 ...
11 net. 172800 IN NS g.gtld-servers.net.
12 net. 172800 IN NS d.gtld-servers.net.
13 ;; Received 570 bytes from 172.19.0.2#53(a.root-loc) in 0 ms
14
15 lacnic.net. 172800 IN NS ns2.dns.br.
16 ...
17 lacnic.net. 172800 IN NS dns.anycast.lacnic.net.
18 ;; Received 598 bytes from 192.31.80.30#53(d.gtld-servers.net) in 76 ms
19
20 www.LACNIC.NET. 7200 IN A 200.3.14.147
21 LACNIC.NET. 7200 IN NS ns2.dns.br.
22 ...
23 LACNIC.NET. 7200 IN NS NS2.LACNIC.NET.
24 LACNIC.NET. 7200 IN NS NS.LACNIC.NET.
25 ;; Received 2092 bytes from 200.192.232.53#53(ns2.dns.br) in 149 ms
26
```



El priming también es local!!

# ¿Por que? Aspectos positivos

- Aprendizaje sobre como funciona el DNS y la raíz en general
  - Priming
  - Recursión
  - Servidores raíz
- Operativamente
  - Redes con riesgo de quedar desconectadas
    - Situaciones de conectividad limitada
  - Redes con restricciones severas de ancho de banda o grandes retardos
    - Redes satelitales

# Precauciones

- Se deben tomar precauciones para garantizar que la raíz local sea verificable por DNSSEC
- En el caso *‘parcialmente local’*
  - Ocurre naturalmente
  - Se verifica con la misma clave
- En el caso *‘totalmente local’*
  - Al estar modificando el **contenido** de la zona hay algunas firmas que se invalidan
  - Se debe **refirmar** con una nueva clave, local

# Referencias

- RFC 7706, “Decreasing access time to the root zone”
  - [ <https://tools.ietf.org/html/rfc7706> ]
- ISC FAQ on root hints and root priming
  - [ <https://deephought.isc.org/article/AA-01309/0/Root-hints-a-collection-of-operational-and-configuration-FAQs.html> ]

**¡Muchas gracias!**

@carlosm3011