Esclavizando la zona raíz

Carlos M. Martínez (@carlosm3011)

LACNOG 2016

San José de Costa Rica – Setiembre 2016

Introducción al DNS

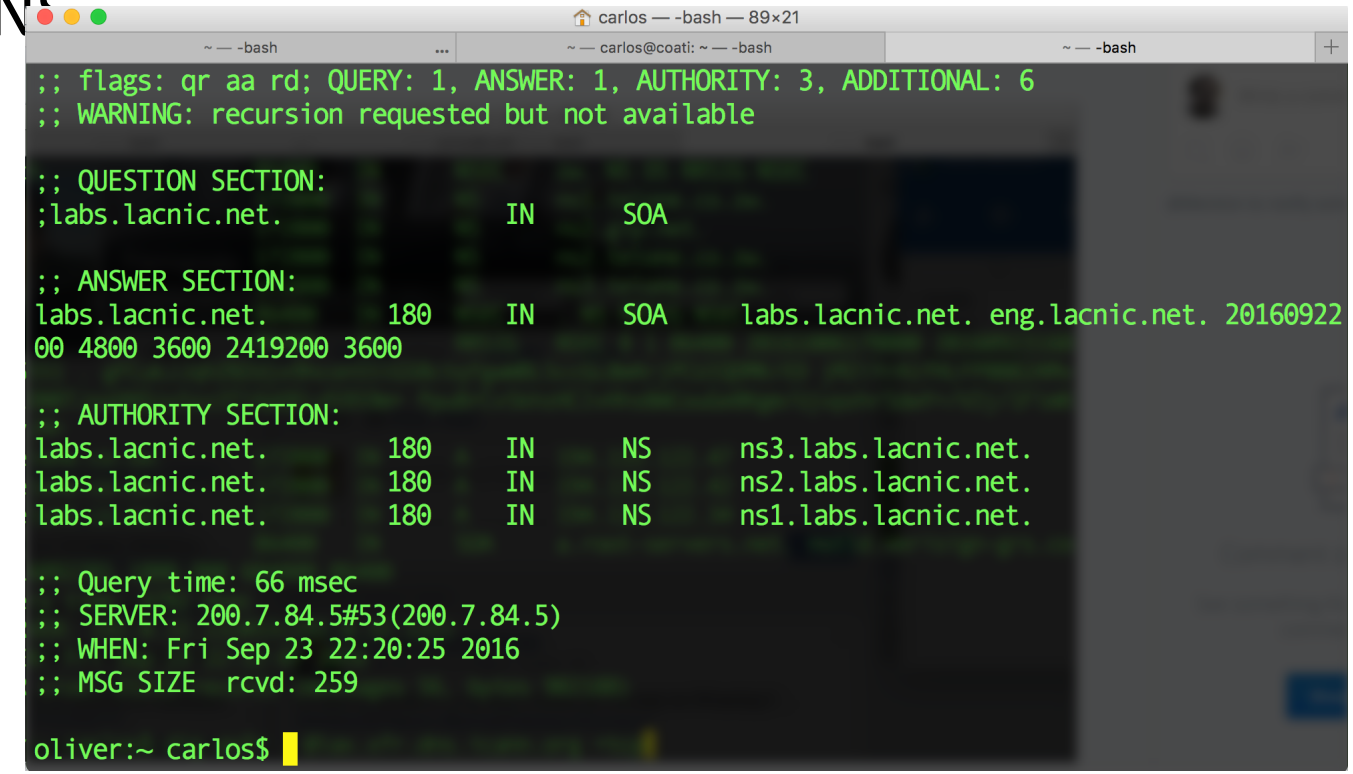
- ”Mapeo de nombres a números”
  - ¿que dirección IP le corresponde a www.facebook.com?
- Y además
  - Delegación de autoridad
  - Apoya diferentes tipos de aplicaciones (correo electronico, hosting virtual, aliases, etc.)
  - Redundancia (primarios y secundarios)

Registros

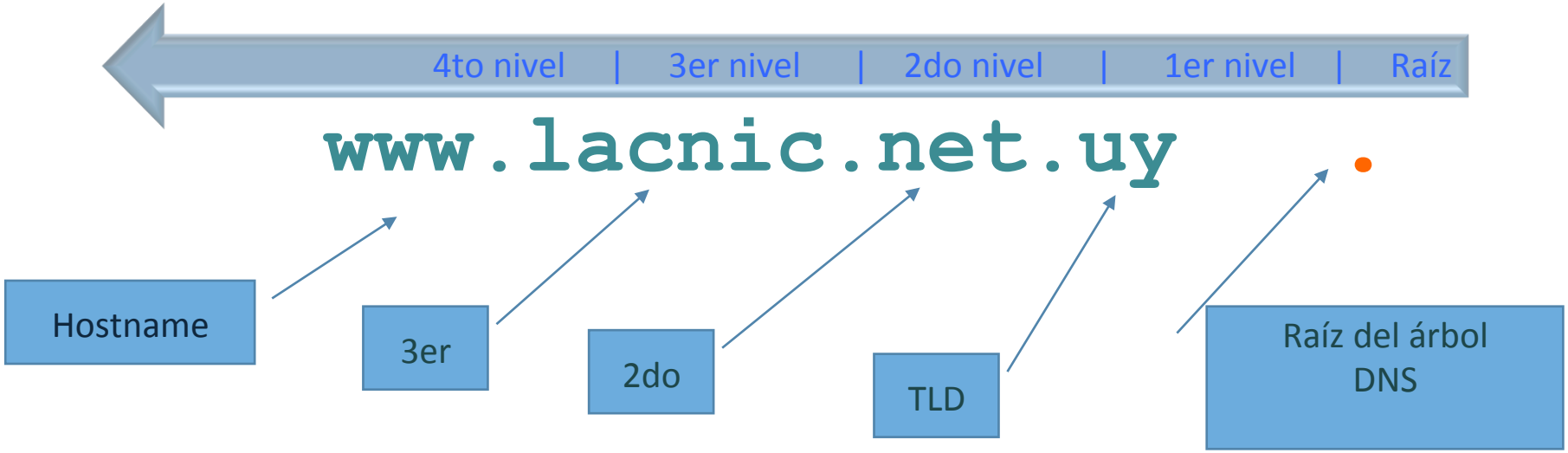
- El DNS es una base de datos distribuida
- Los ‘registros’ son 5-tuplas con los siguientes campos
  - Nombre
  - Clase (siempre *IN* para nosotros)
  - TTL
  - Tipo
  - Valor
- Ejemplo
  - `www.example.com. 3600 IN A 192.168.1.10`

Zonas

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



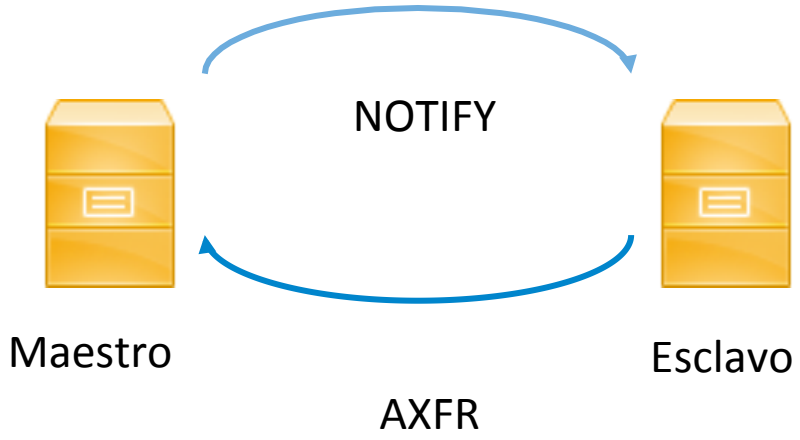
Estructura de un nombre de dominio



- 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

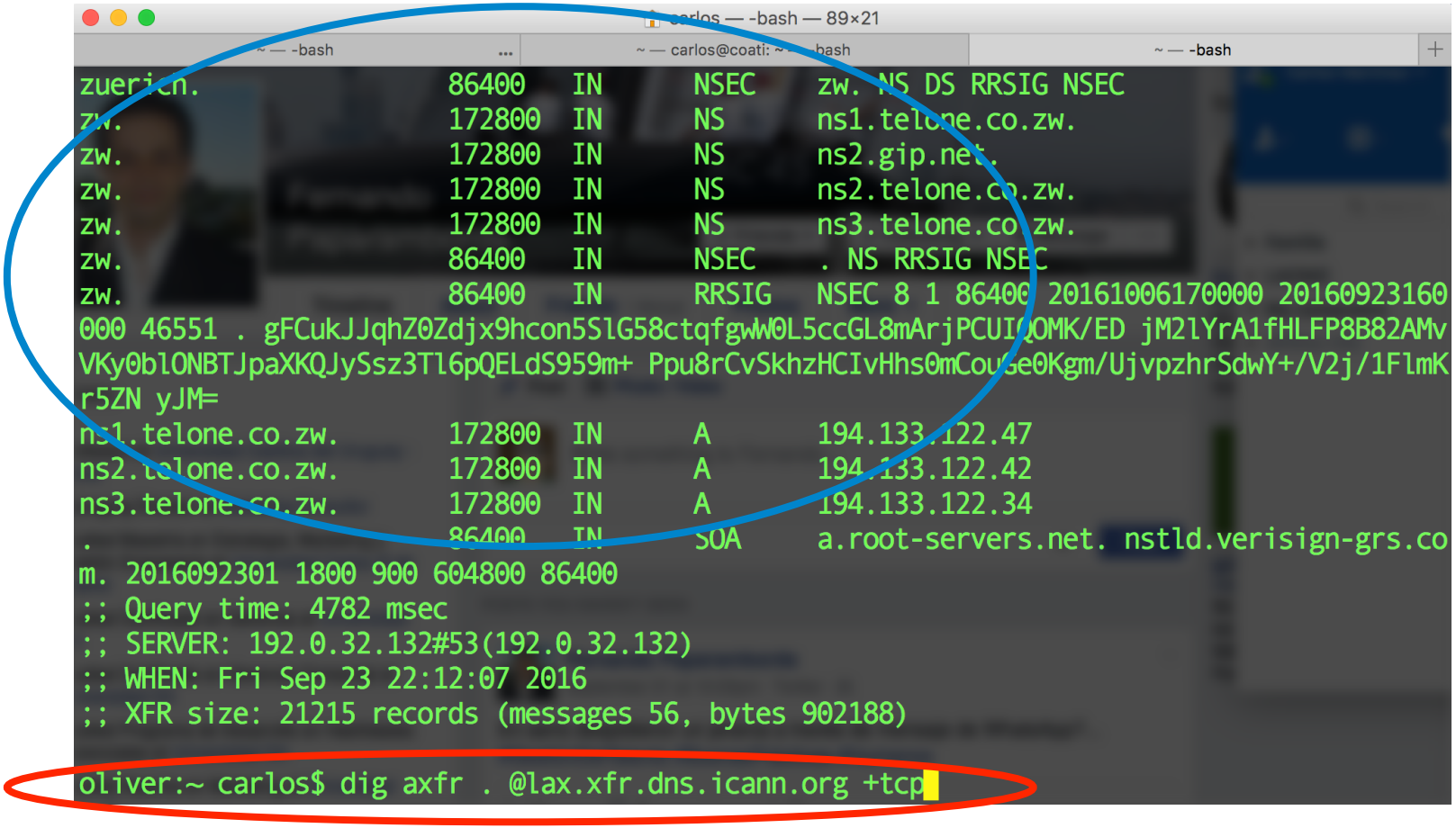
- Redundancia, DNS-style



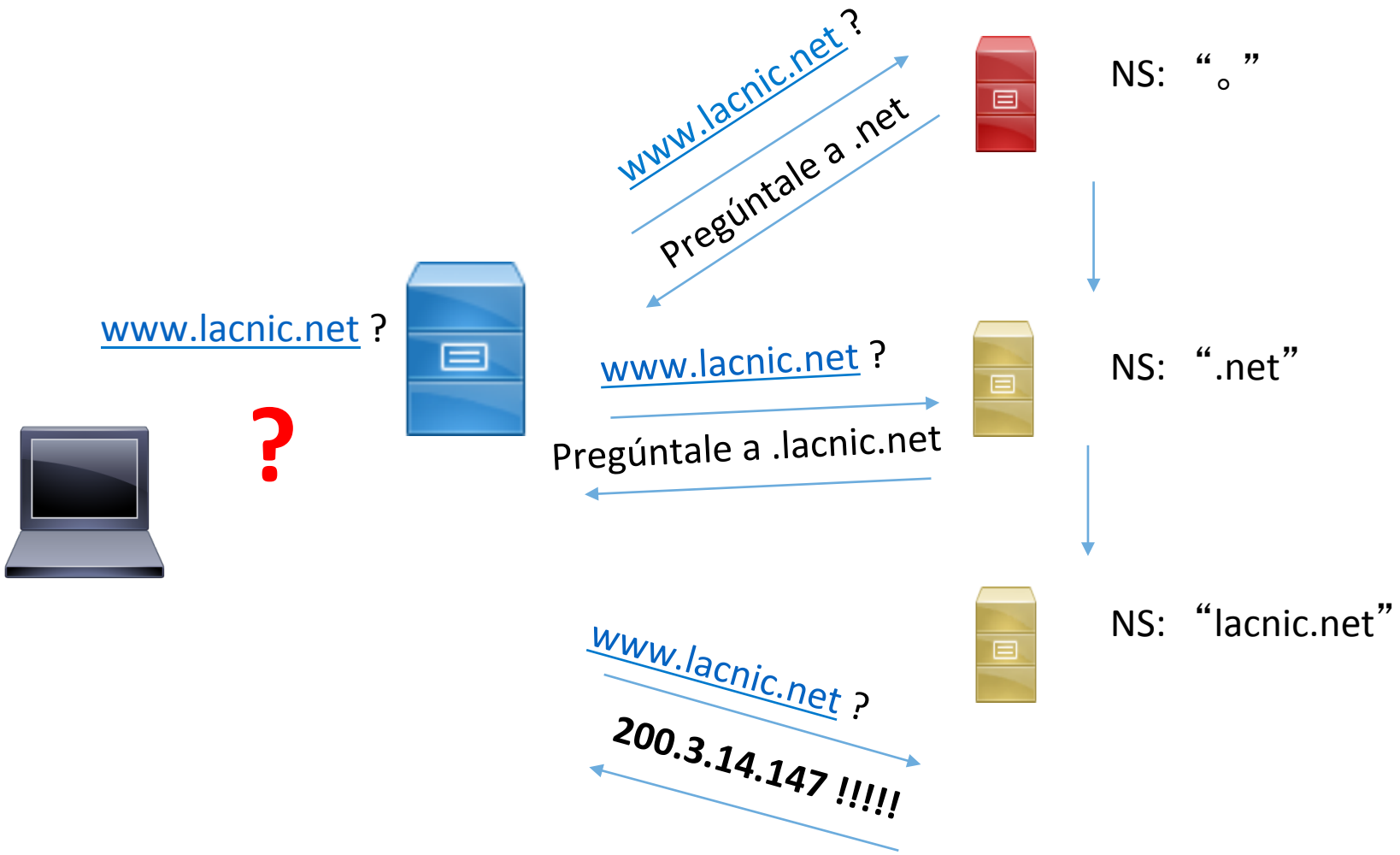
- AXFR es un pseudo-tipo de registro, simboliza la operación de transferencia de zona
- ¿Como saber si la zona cambió? Se compara el número de serie del registro SOA

Transferencias de zona

- Usando dig:

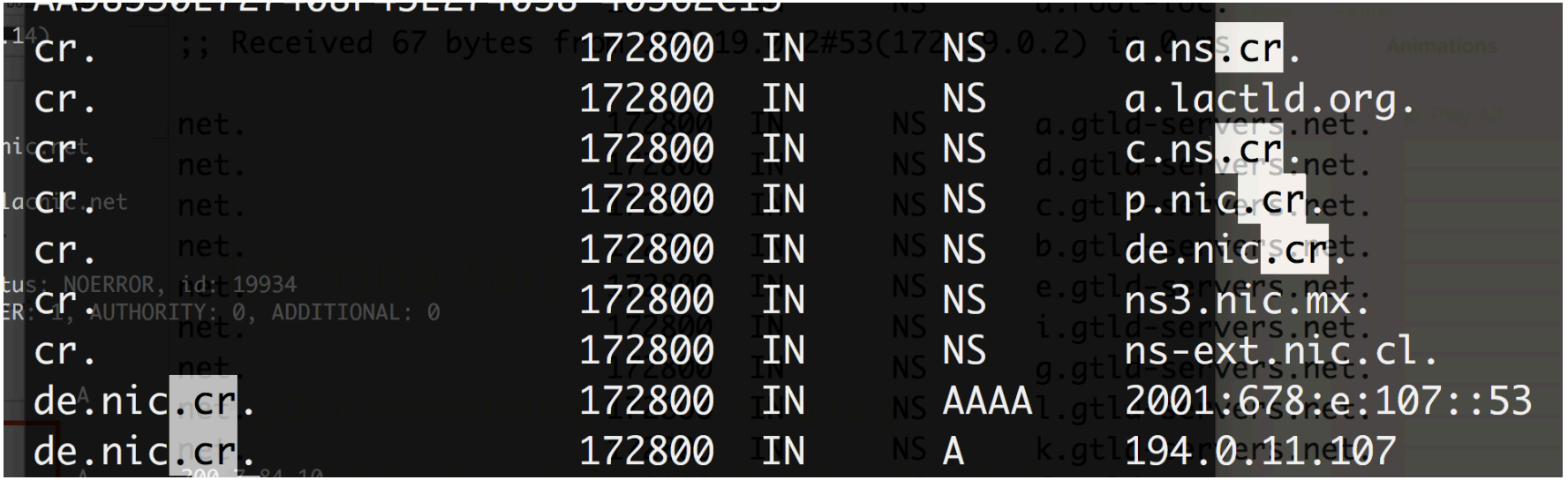


Resolución recursiva



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      AAAA    2001:678:e:107::53
de.nic.cr.      172800  IN      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’

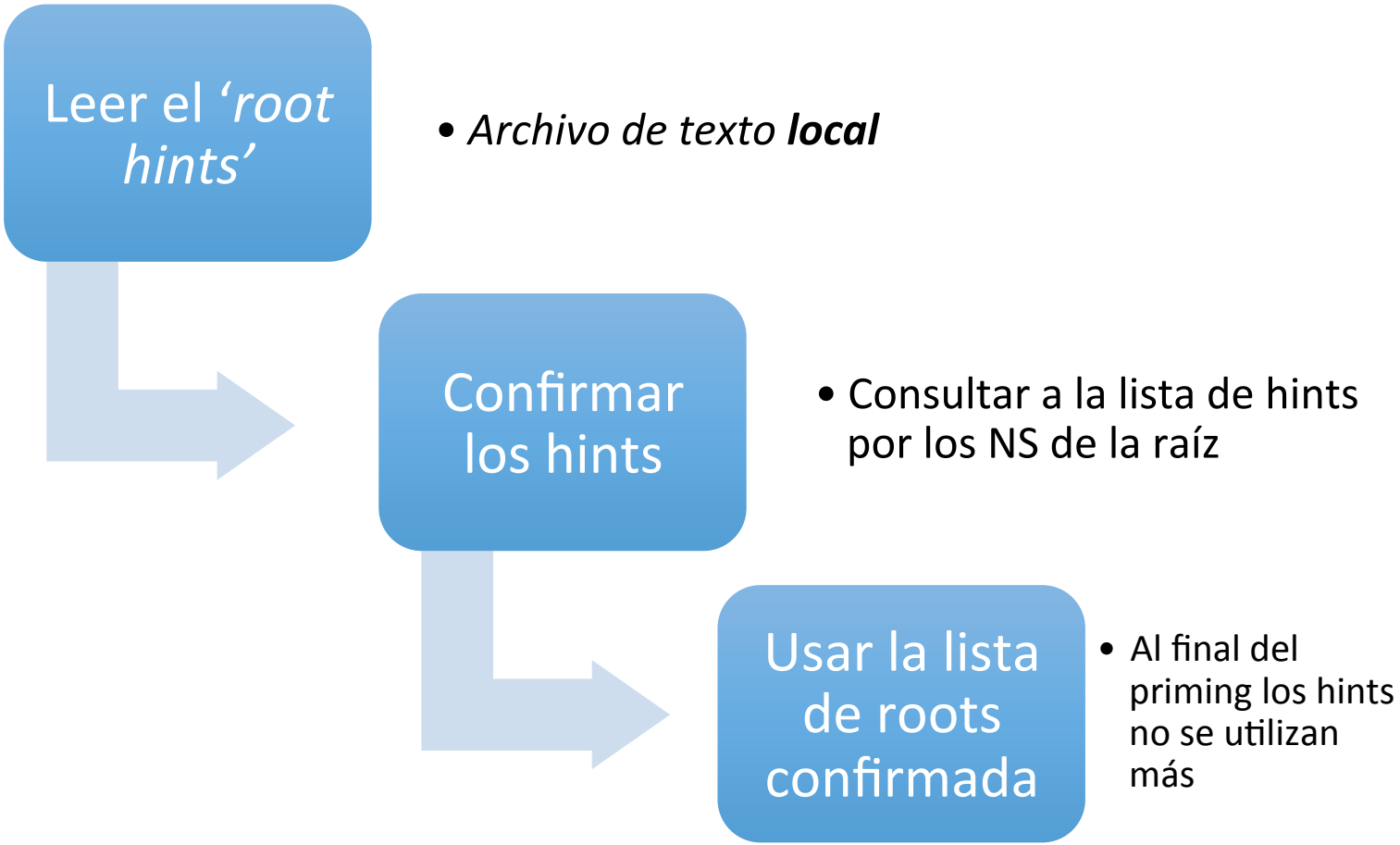
```
;       last update:    August 25, 2016
;       related version of root zone:   2016082500;
; formerly NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; 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’

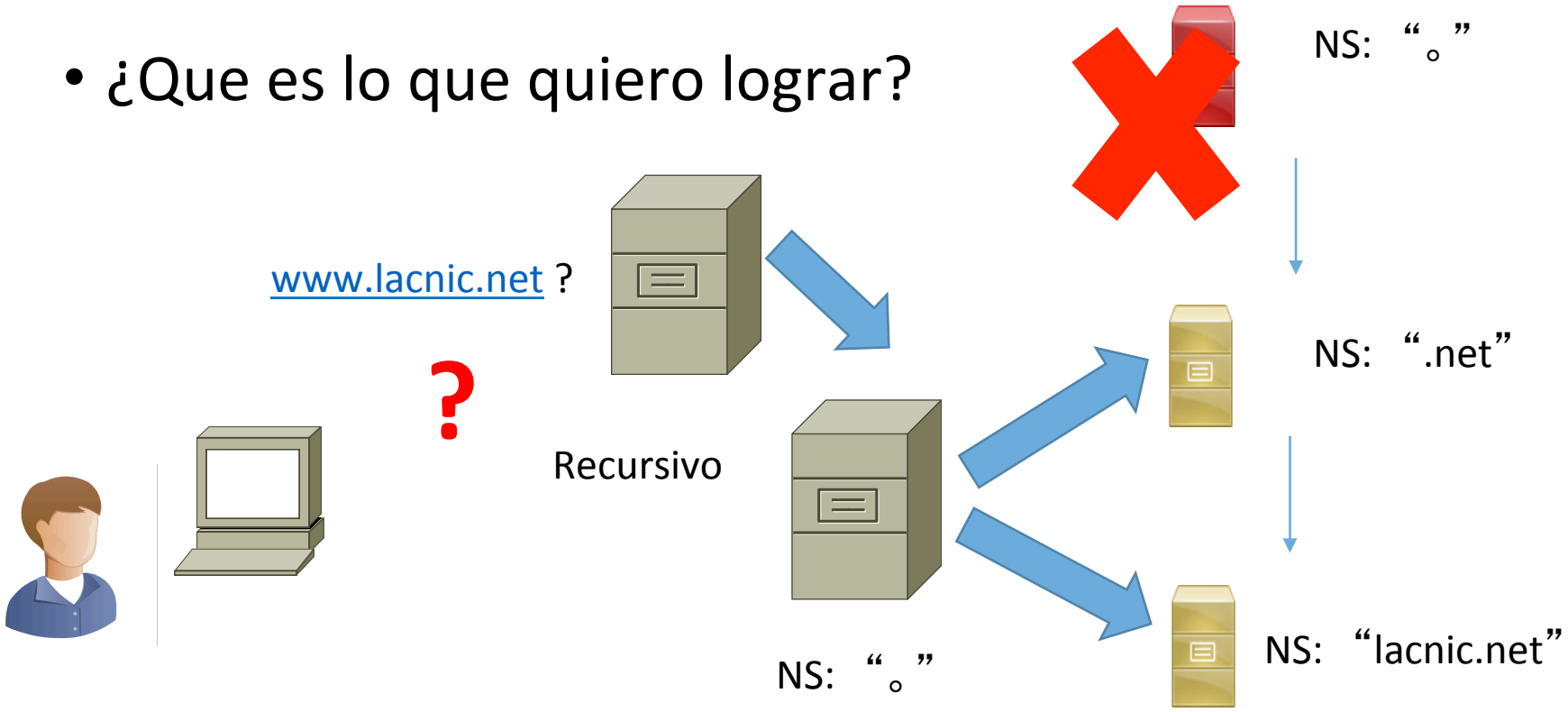
- ¿Alguna vez se preguntaron si las direcciones IP de los servidores raíz cambian?
- Y si cambian, ¿porque mi archivo root.hints no está siempre desactualizado?
  - [https://deepthought.isc.org/article/AA-01309/0/Root-hints-a-collection-of-operational-and-configuration-FAQs.html]
- En corto, el contenido 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’



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 |

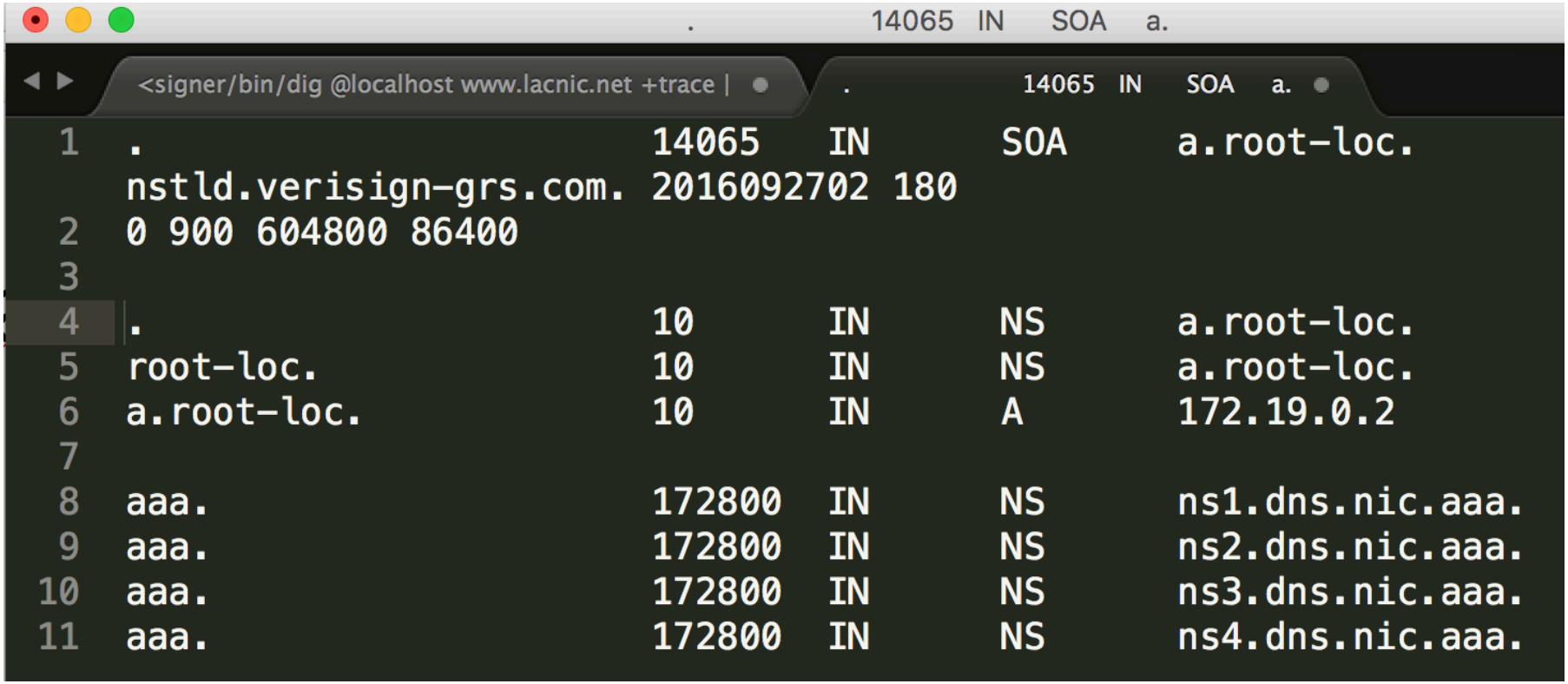
```
<signer/bin/dig @localhost www.lacnic.net +trace | grep -v RRSIG

; <<>> DiG 9.10.2 <<>> @localhost www.lacnic.net +trace
.            518400  IN  NS  G.ROOT-SERVERS.NET.
.            518400  IN  NS  I.ROOT-SERVERS.NET.
.            518400  IN  NS  M.ROOT-SERVERS.NET.
....
.            518400  IN  NS  J.ROOT-SERVERS.NET.
.            518400  IN  NS  C.ROOT-SERVERS.NET.
;; Received 825 bytes from 127.0.0.1#53(localhost) in 0 ms

net.            172800  IN  NS  d.gtld-servers.net.
net.            172800  IN  NS  i.gtld-servers.net.
.....
net.            172800  IN  NS  e.gtld-servers.net.
;; Received 735 bytes from 192.36.148.17#53(I.ROOT-SERVERS.NET) in 70 ms

lacnic.net.     172800  IN  NS  sec3.apnic.net.
lacnic.net.     172800  IN  NS  ns2.lacnic.net.
lacnic.net.     172800  IN  NS  dns.anycast.lacnic.net.
;; Received 598 bytes from 192.26.92.30#53(c.gtld-servers.net) in 76 ms

www.LACNIC.NET.     7200    IN  A   200.3.14.147
LACNIC.NET.     7200    IN  NS  ns2.dns.br.
LACNIC.NET.     7200    IN  NS  NS.LACNIC.NET.
LACNIC.NET.     7200    IN  NS  TINNIE.ARIN.NET.
;; Received 2136 bytes from 200.3.13.10#53(ns.lacnic.net) in 154 ms
```

La raíz, completamente local

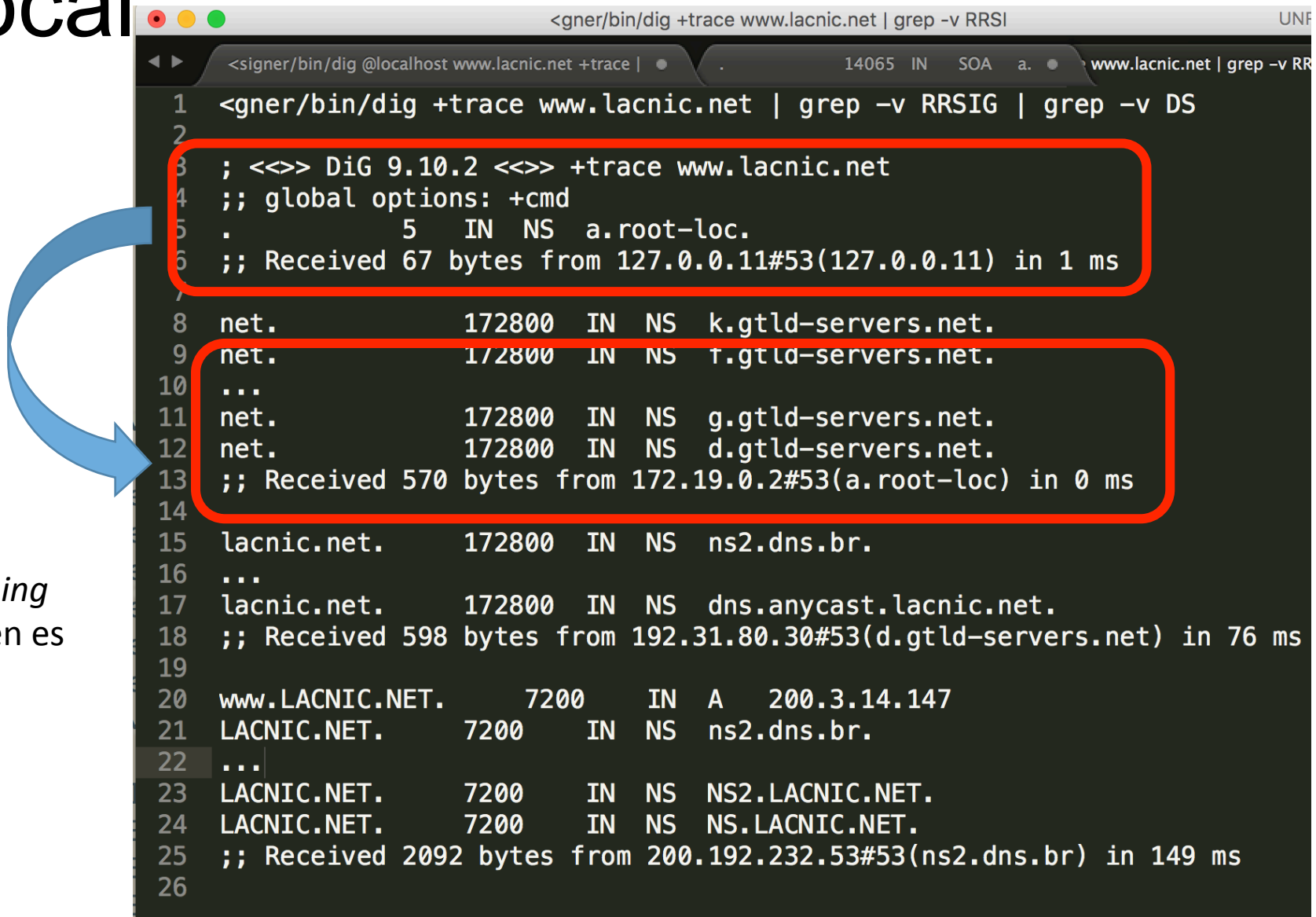
- Para hacer que la zona raíz sea completamente local debemos lograr que el *priming también devuelva servidores locales*
- Para eso modificamos la zona raíz y cambiamos los registros NS por los locales, y creamos una zona similar a ‘root-servers.net’ pero local

Zona raíz modificada

- NS-Set



La zona raíz completamente local



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://deepthought.isc.org/article/AA-01309/0/Root-hints-a-collection-of-operational-and-configuration-FAQs.html]

¡Muchas gracias!

@carlosm3011