DNS: Domain Name System

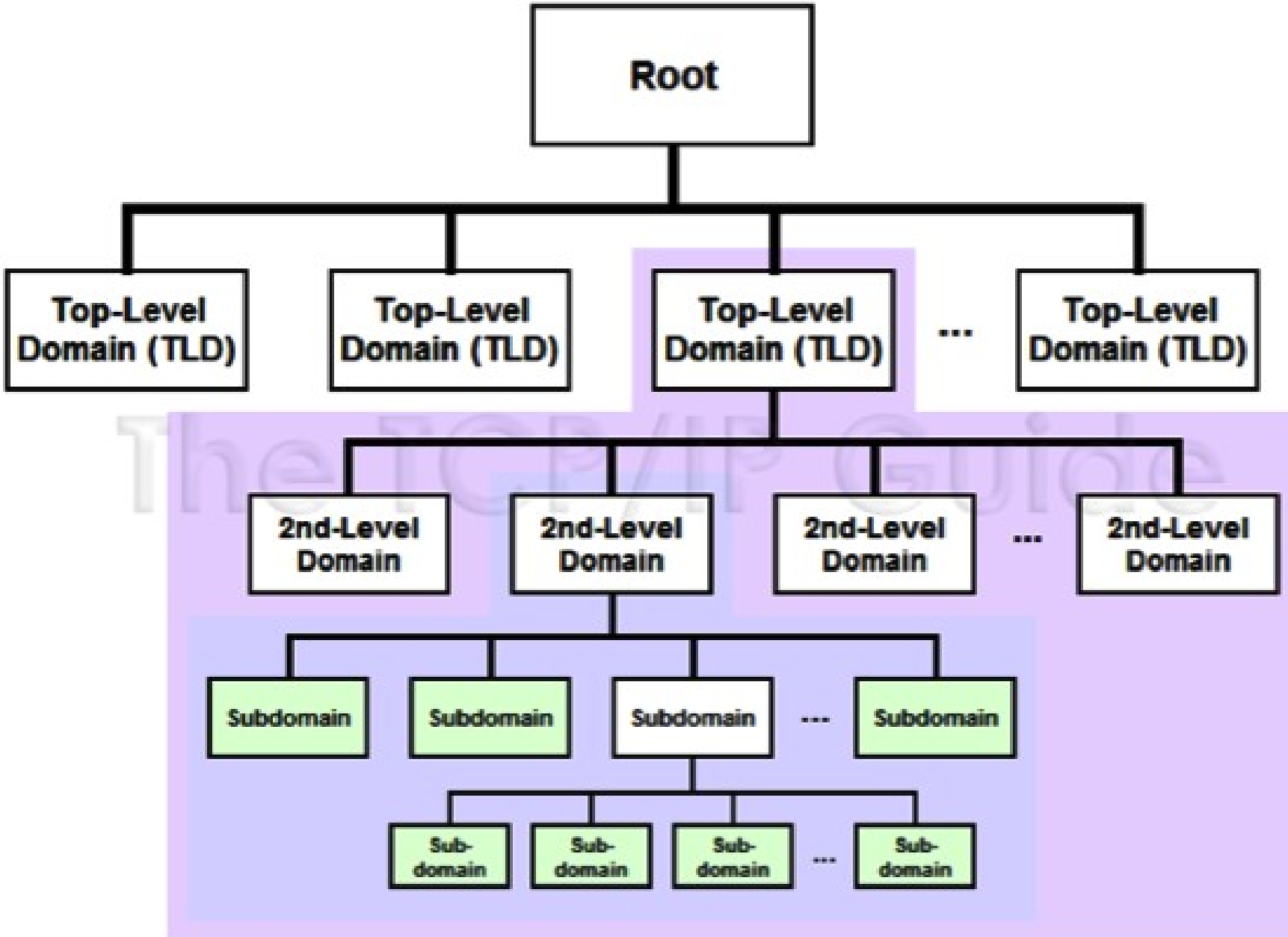
Introducción

- DNS: Domain Name System
  - Propósito básico: Traducir números IP en nombres textuales más amigables para los usuarios “humanos” de la red.
  - Propósitos adicionales: Soporte a diferentes servicios a dar sobre la red.
    - Correo electrónico
    - Sub-delegaciones de nombres
    - Resolución inversa
      - Reverso: correspondencia dirección IP -> nombre

Introducción (Cont.)

- DNS como base de datos:
  - El objetivo principal del DNS es entonces almacenar información de mapeo entre nombres y números IP (Directa e inversa)
  - El sistema opera entonces como una base de datos distribuida en la que existe la posibilidad de delegar la administración de sectores del espacio de nombres a diferentes organizaciones.

Introducción (Cont.)



Recursión

- Distribución:
  - Sistema dividido en “islas” de control (“Zonas”)
- ¿Cómo consultar cualquier zona?
  - Consultas recursivas
  - Siguiendo la estructura del árbol
  - Cada zona tiene el potencial de “delegar” a las zonas siguientes

Resource Records

- La información en la base de datos del DNS está estructurada en un conjunto de *resource records*:
  - SOA, A, NS, MX, PTR, TXT, etc.
- Cada RR representa un ítem de información en la base de datos de DNS que puede ser consultado.
- Un RR está definido por cinco campos:
  - Class, Type, Value, Name, TTL

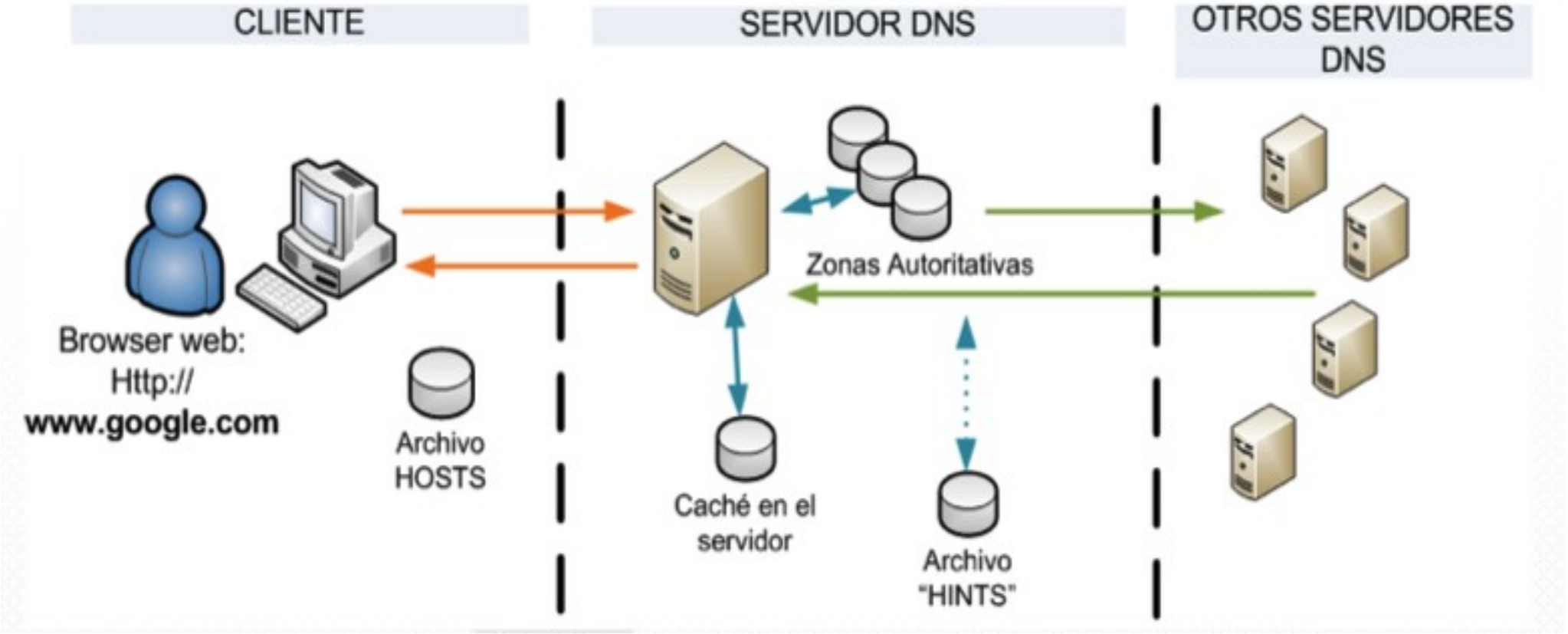
Registros “A”

- RR “A”: Address
  - Los registros A establecen las correspondencias entre direcciones IP y nombres de dominio.
  - Ídem Ipv6: “AAAA”
- Formato “Zone File” de BIND
  - www IN A 200.3.14.10
  - www IN AAAA 2001:13c7:7002:4000::10

Registros “PTR”

- RR “PTR”: Pointer
  - Los registros PTR establecen enlaces o punteros entre nombres de DNS.
    - El principal uso es construir los dominios in-addr.arpa e ip6.arpa que contienen los reversos
  - Los clientes DNS transforman una consulta por IP, asumiendo que es una reversa, por una consulta bajo “in-addr.arpa” o “ip6.arpa”
  - Ejemplo:
    - 10.14.3.200.in-addr-arpa. 82136 IN PTR www.lacnic.net.
    - 0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.2.0.0.7.7.c.3.1.1.0.0.2.ip6.arpa. 86400IN PTR www.lacnic.net.

Operación: Consultas



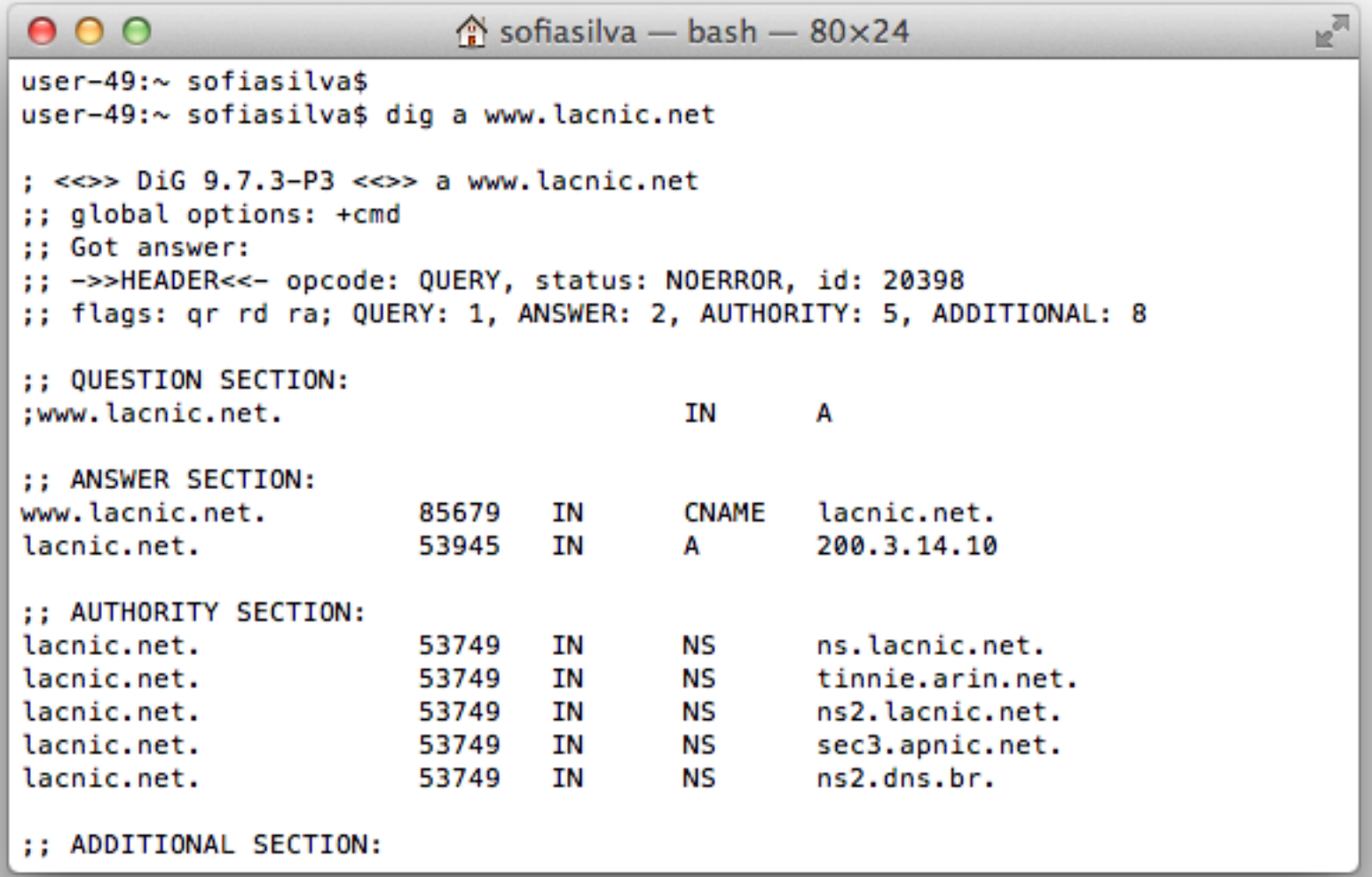
"resolver" local

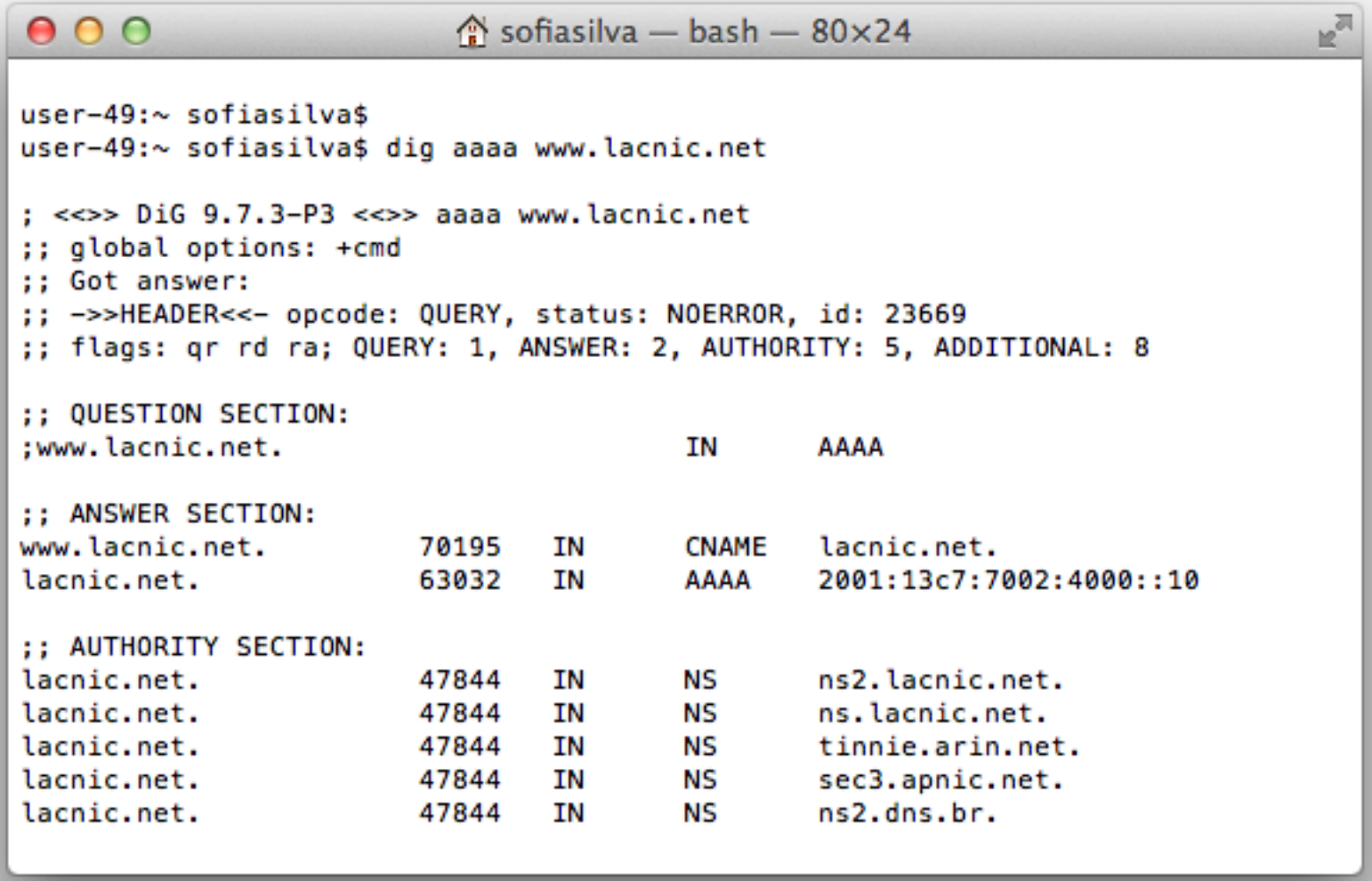
DNS recursivo local

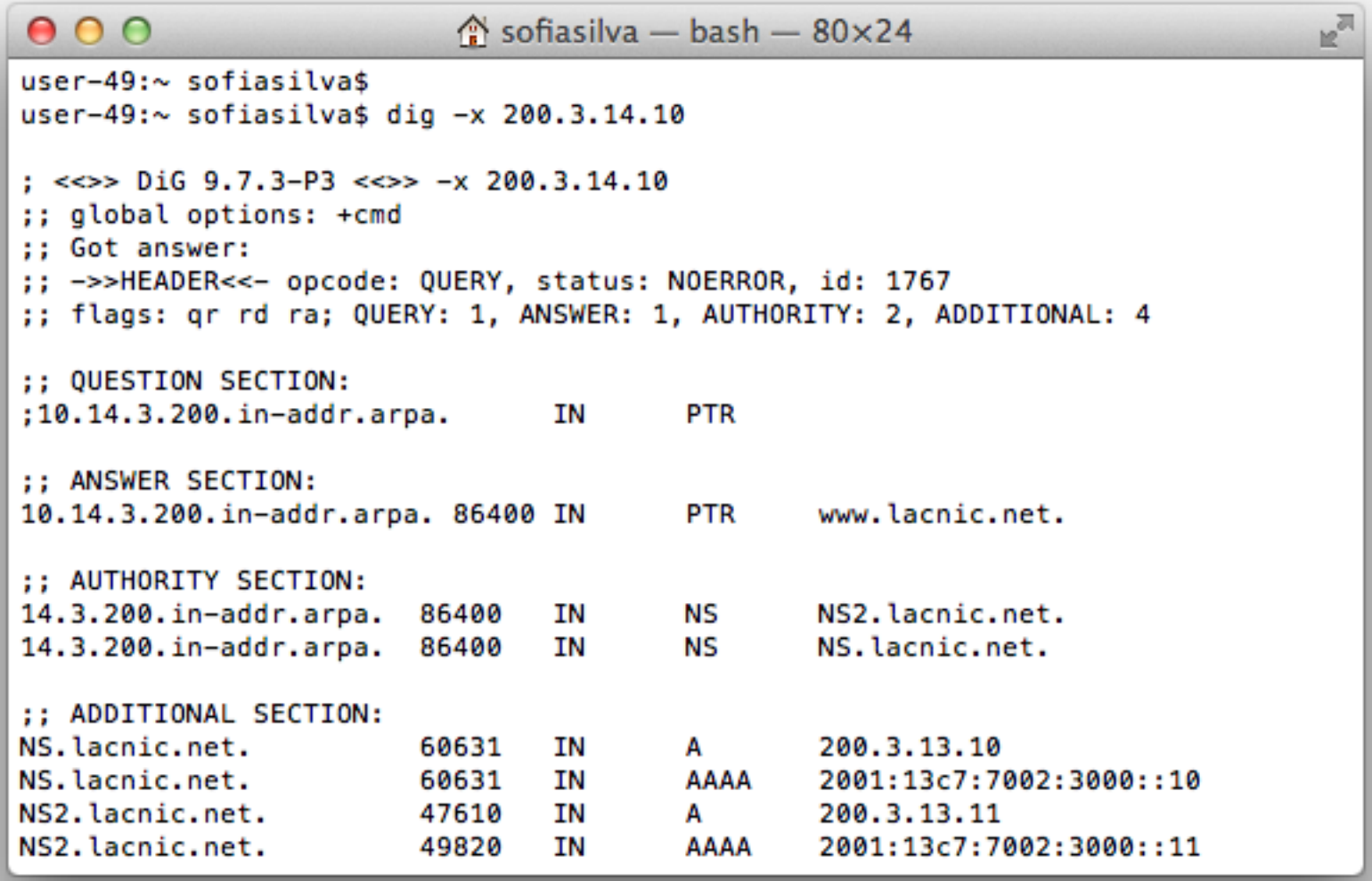
Otros servidores autoritativos

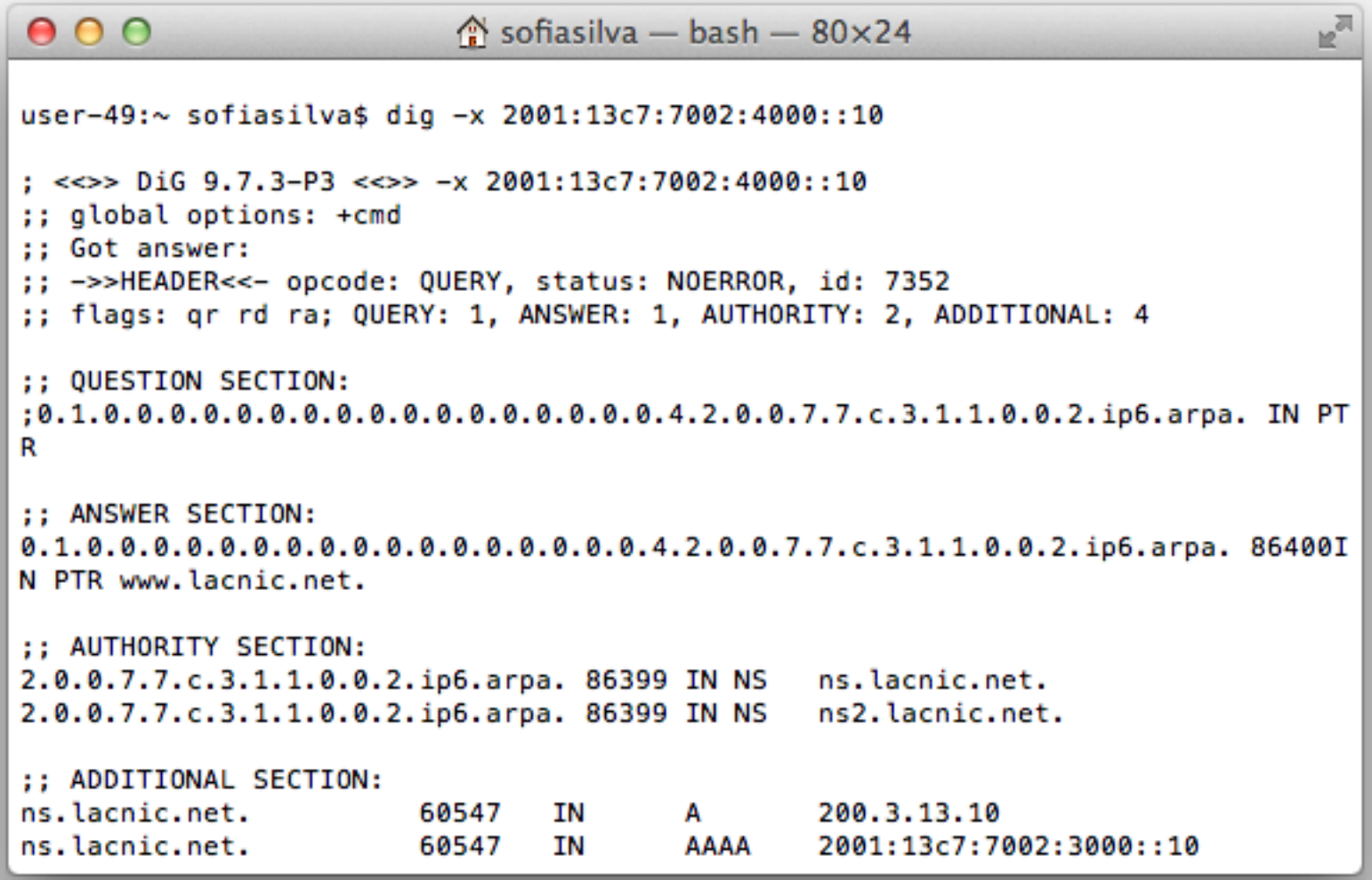
Herramientas: Dig

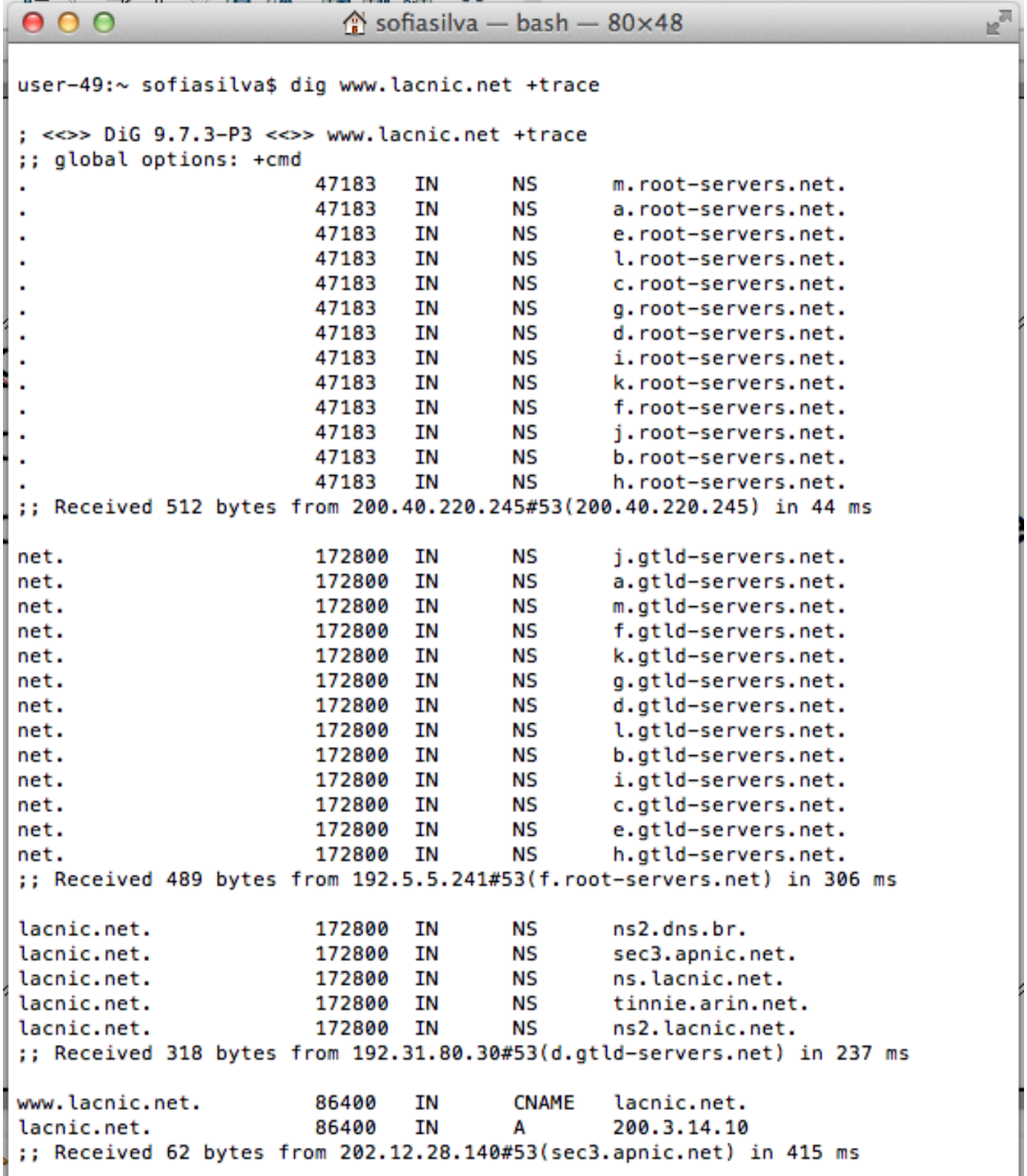
- dig A ns1.lacnic.net
- Consulta reversa: dig -x 200.7.85.220
- Consulta con traza: dig www.lacnic.net +trace


sofiasilva — bash — 80×24
user-49:~ sofiasilva$
user-49:~ sofiasilva$ dig a www.lacnic.net
; <<>> DiG 9.7.3-P3 <<>> a www.lacnic.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20398
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 8
;; QUESTION SECTION:
;www.lacnic.net. IN A
;; ANSWER SECTION:
www.lacnic.net. 85679 IN CNAME lacnic.net.
lacnic.net. 53945 IN A 200.3.14.10
;; AUTHORITY SECTION:
lacnic.net. 53749 IN NS ns.lacnic.net.
lacnic.net. 53749 IN NS tinnie.arin.net.
lacnic.net. 53749 IN NS ns2.lacnic.net.
lacnic.net. 53749 IN NS sec3.apnic.net.
lacnic.net. 53749 IN NS ns2.dns.br.
;; ADDITIONAL SECTION:

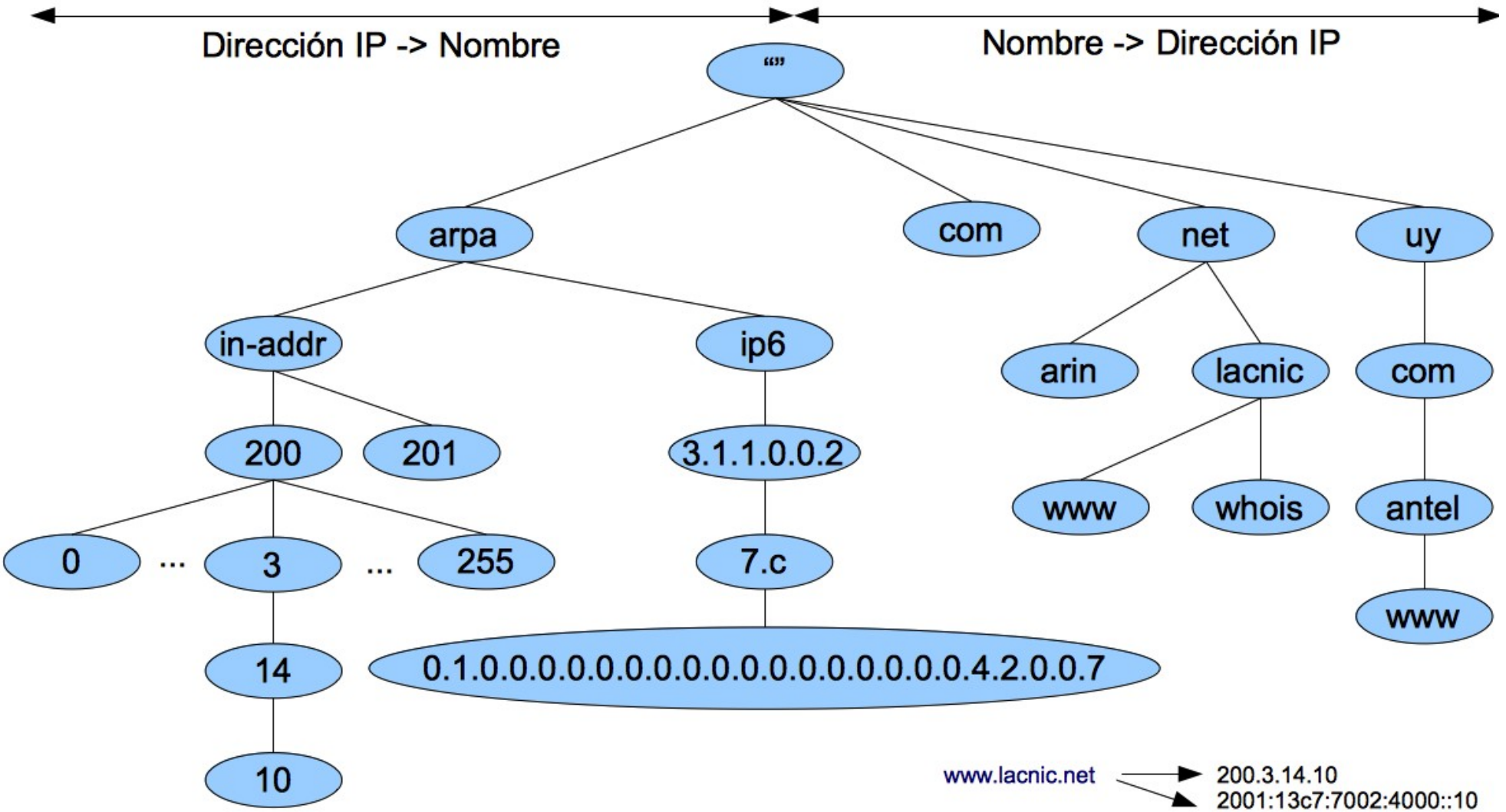

sofiasilva — bash — 80×24
user-49:~ sofiasilva$
user-49:~ sofiasilva$ dig aaaa www.lacnic.net
; <<>> DiG 9.7.3-P3 <<>> aaaa www.lacnic.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23669
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 8
;; QUESTION SECTION:
;www.lacnic.net. IN AAAA
;; ANSWER SECTION:
www.lacnic.net. 70195 IN CNAME lacnic.net.
lacnic.net. 63032 IN AAAA 2001:13c7:7002:4000::10
;; AUTHORITY SECTION:
lacnic.net. 47844 IN NS ns2.lacnic.net.
lacnic.net. 47844 IN NS ns.lacnic.net.
lacnic.net. 47844 IN NS tinnie.arin.net.
lacnic.net. 47844 IN NS sec3.apnic.net.
lacnic.net. 47844 IN NS ns2.dns.br.


sofiasilva — bash — 80×24
user-49:~ sofiasilva$
user-49:~ sofiasilva$ dig -x 200.3.14.10
; <<>> DiG 9.7.3-P3 <<>> -x 200.3.14.10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1767
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4
;; QUESTION SECTION:
;10.14.3.200.in-addr.arpa. IN PTR
;; ANSWER SECTION:
10.14.3.200.in-addr.arpa. 86400 IN PTR www.lacnic.net.
;; AUTHORITY SECTION:
14.3.200.in-addr.arpa. 86400 IN NS NS2.lacnic.net.
14.3.200.in-addr.arpa. 86400 IN NS NS.lacnic.net.
;; ADDITIONAL SECTION:
NS.lacnic.net. 60631 IN A 200.3.13.10
NS.lacnic.net. 60631 IN AAAA 2001:13c7:7002:3000::10
NS2.lacnic.net. 47610 IN A 200.3.13.11
NS2.lacnic.net. 49820 IN AAAA 2001:13c7:7002:3000::11


sofiasilva — bash — 80×24
user-49:~ sofiasilva$ dig -x 2001:13c7:7002:4000::10
; <<>> DiG 9.7.3-P3 <<>> -x 2001:13c7:7002:4000::10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7352
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4
;; QUESTION SECTION:
;0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.2.0.0.7.7.c.3.1.1.0.0.2.ip6.arpa. IN PT
R
;; ANSWER SECTION:
0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.2.0.0.7.7.c.3.1.1.0.0.2.ip6.arpa. 86400I
N PTR www.lacnic.net.
;; AUTHORITY SECTION:
2.0.0.7.7.c.3.1.1.0.0.2.ip6.arpa. 86399 IN NS ns.lacnic.net.
2.0.0.7.7.c.3.1.1.0.0.2.ip6.arpa. 86399 IN NS ns2.lacnic.net.
;; ADDITIONAL SECTION:
ns.lacnic.net. 60547 IN A 200.3.13.10
ns.lacnic.net. 60547 IN AAAA 2001:13c7:7002:3000::10


sofiasilva — bash — 80×48
user-49:~ sofiasilva$ dig www.lacnic.net +trace
; <<>> DiG 9.7.3-P3 <<>> www.lacnic.net +trace
;; global options: +cmd
. 47183 IN NS m.root-servers.net.
. 47183 IN NS a.root-servers.net.
. 47183 IN NS e.root-servers.net.
. 47183 IN NS l.root-servers.net.
. 47183 IN NS c.root-servers.net.
. 47183 IN NS g.root-servers.net.
. 47183 IN NS d.root-servers.net.
. 47183 IN NS i.root-servers.net.
. 47183 IN NS k.root-servers.net.
. 47183 IN NS f.root-servers.net.
. 47183 IN NS j.root-servers.net.
. 47183 IN NS b.root-servers.net.
. 47183 IN NS h.root-servers.net.
;; Received 512 bytes from 200.40.220.245#53(200.40.220.245) in 44 ms
net. 172800 IN NS j.gtld-servers.net.
net. 172800 IN NS a.gtld-servers.net.
net. 172800 IN NS m.gtld-servers.net.
net. 172800 IN NS f.gtld-servers.net.
net. 172800 IN NS k.gtld-servers.net.
net. 172800 IN NS g.gtld-servers.net.
net. 172800 IN NS d.gtld-servers.net.
net. 172800 IN NS l.gtld-servers.net.
net. 172800 IN NS b.gtld-servers.net.
net. 172800 IN NS i.gtld-servers.net.
net. 172800 IN NS c.gtld-servers.net.
net. 172800 IN NS e.gtld-servers.net.
net. 172800 IN NS h.gtld-servers.net.
;; Received 489 bytes from 192.5.5.241#53(f.root-servers.net) in 306 ms
lacnic.net. 172800 IN NS ns2.dns.br.
lacnic.net. 172800 IN NS sec3.apnic.net.
lacnic.net. 172800 IN NS ns.lacnic.net.
lacnic.net. 172800 IN NS tinnie.arin.net.
lacnic.net. 172800 IN NS ns2.lacnic.net.
;; Received 318 bytes from 192.31.80.30#53(d.gtld-servers.net) in 237 ms
www.lacnic.net. 86400 IN CNAME lacnic.net.
lacnic.net. 86400 IN A 200.3.14.10
;; Received 62 bytes from 202.12.28.140#53(sec3.apnic.net) in 415 ms

Búsqueda en un árbol DNS con IPv6



DNS y servidores raíz en IPv6

Los servidores DNS raíz son recursos críticos

Hay 13 servidores raíz en el mundo

- Desde el año 2008 6 de ellos tienen Ipv6 habilitado
- Y son alcanzables a través de redes Ipv6
- A, F, H, J, K & M

Requerimientos operativos & recomendaciones para DNSv6

El objetivo NO es la transición de un entorno IPv4-only a un entorno IPv6-only

¿Cómo lo logramos?

- Empezar probando DNSv6 en una red pequeña y sacar sus propias conclusiones de que DNSv6 es inofensivo, pero recordar:
  - El servidor (host) debe soportar IPv6
  - El software servidor DNS debe soportar IPv6
- Implementar DNSv6 de forma incremental en redes existentes
- NO ROMPER algo que funciona bien (DNS IPv4 en producción)

NAT64 / DNS64
Comunicando los mundos
v4 – v6

Adopción de IPv6

- La adopción de IPv6 no va a ser todo lo rápida que hubiésemos deseado
- La realidad dicta:
  - El espacio IPv4 esta llegando a su fin
  - Pero el grueso del contenido en Internet sigue estando solamente en v4
- Necesitamos **técnicas** que permitan a **usuarios que solo tienen IPv6** acceder a contenido que **solo está disponible en IPv4**

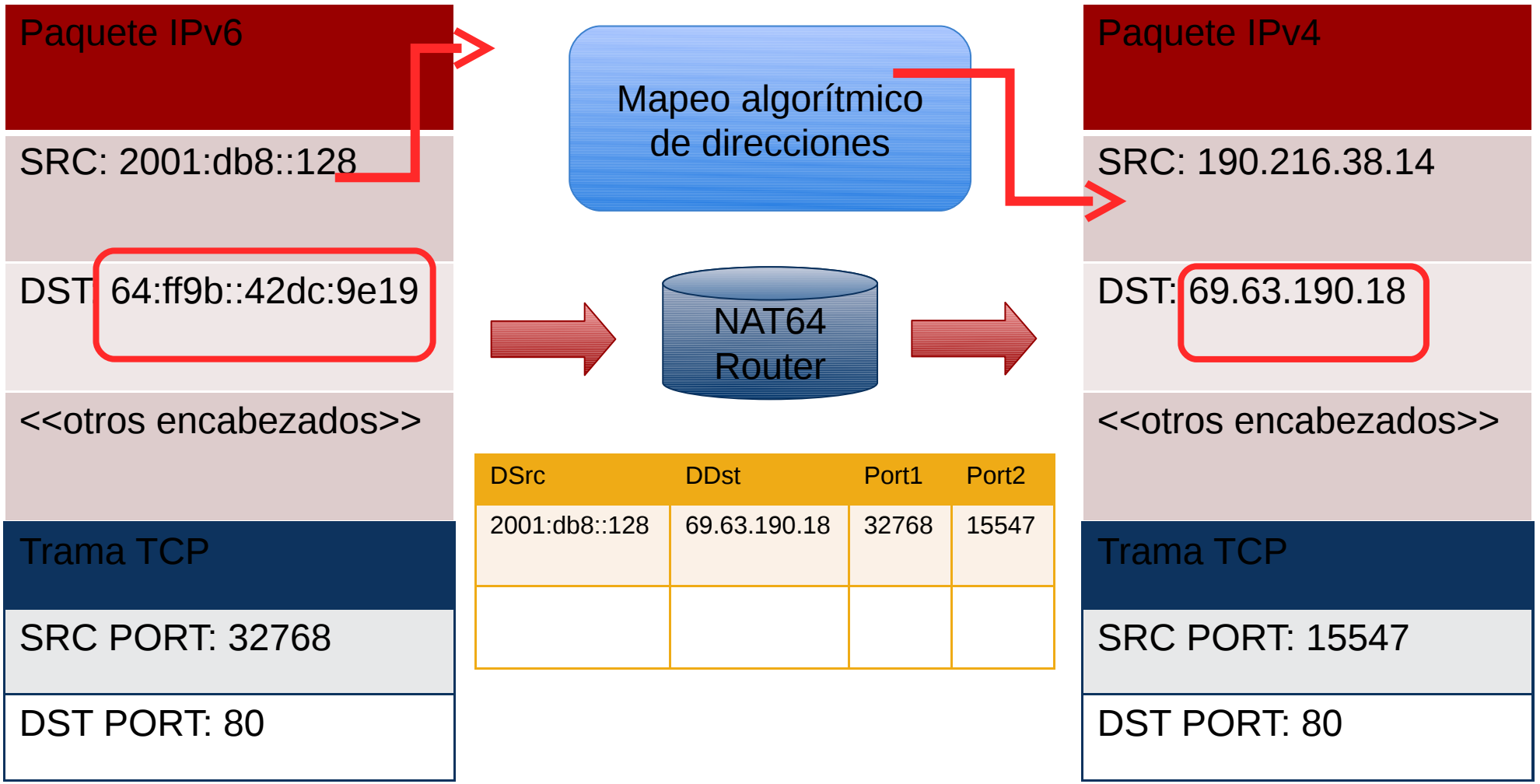
NAT64

- NAT64 es una técnica de este tipo
  - Acceso a sistemas que solo tienen pila IPv4 desde hosts que solo tienen pila IPv6
- A muy alto nivel:
  - Traslación de protocolos y traslación de direcciones
    - El mapeo de direcciones obviamente no puede ser 1 a 1
  - Se define (por cada instalación) un prefijo v6 en el cual mapear todo el espacio IPv4
    - Un /96 alcanza, usualmente se utiliza 64:ff9b::/96
- La caja NAT64 realiza la conversión de protocolos y de las direcciones

NAT64 (ii)

- Traslación de protocolos
  - Por cada paquete IPv6 que recibe el enrutador NAT64 debe construir un paquete IPv4
    - Mapeo de campos del encabezado
    - Traslación de direcciones IPv6 -> IPv4
      - El mapeo 1 a 1 no es posible
  - El enrutador NAT64 usa al menos una dirección IPv4 para los paquetes salientes
    - Debe mantener una tabla con estado

NAT64 (iii)

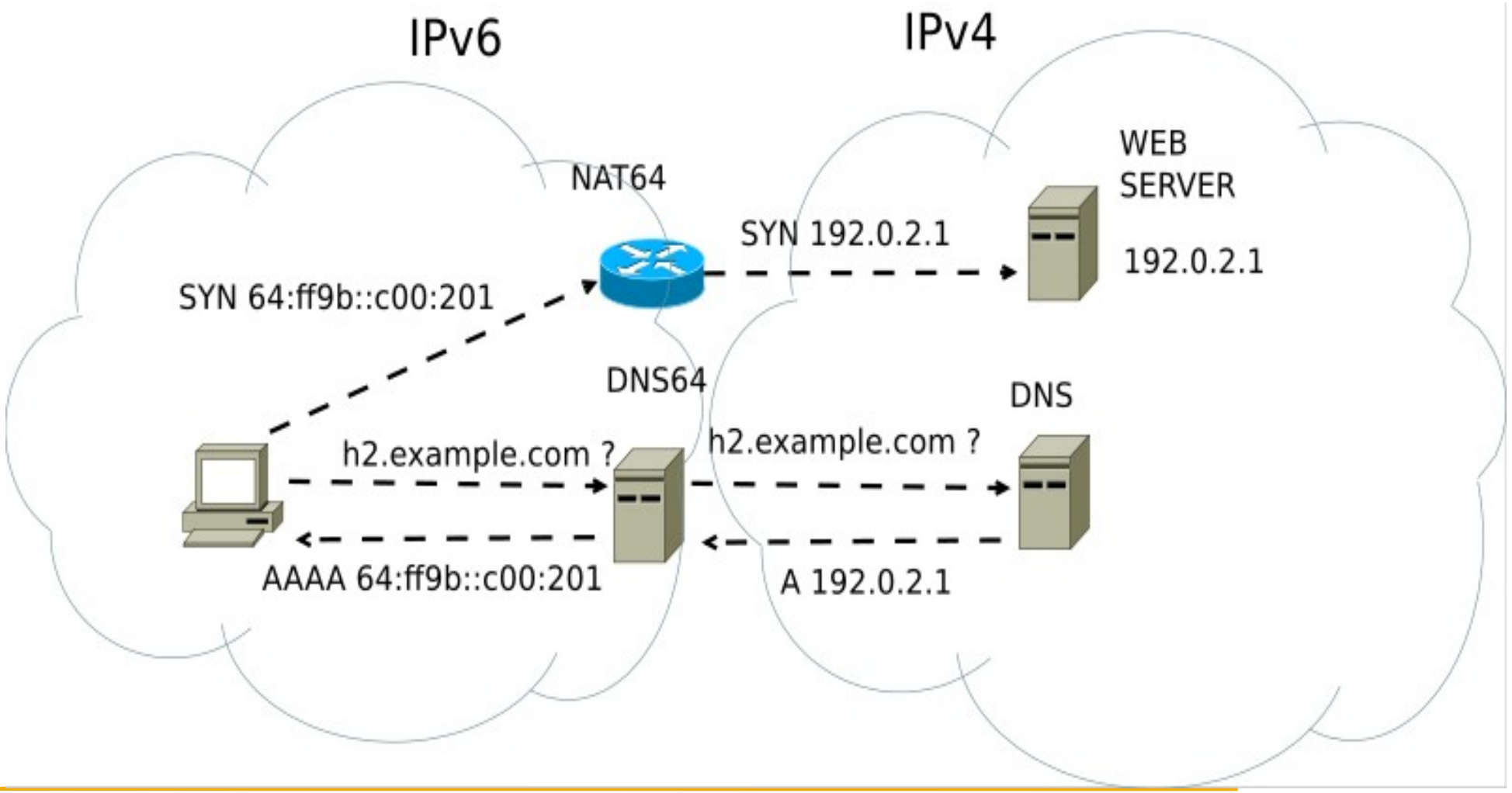


DSrc	DDst	Port1	Port2
2001:db8::128	69.63.190.18	32768	15547

DNS64

- DNS64 es una traducción a nivel de DNS que obra como complemento de NAT64 para permitir que los clientes v6 “vean” el contenido solo-v4
- ¿Cómo?
  - A través de un servidor recursivo especialmente adaptado
  - Cuando recibe una pregunta por un AAAA
    - Pregunta hacia afuera por A y AAAA
      - Si recibe un A solamente, lo convierte en un AAAA, aplicando el mismo algoritmo de mapeo de direcciones

Arquitectura de red con NAT64



Implementaciones

- Viagenie
  - http://ecdysis.viagenie.ca
  - Modulo de kernel para Linux (NAT64)
  - Patches para Unbound y BIND 9.7 (DNS64)
- ISC
  - DNS64 es incorporado a partir de la versión 9.8.0
- ¿Otras?

Instalación NAT64/DNS64

- Dependiendo de la escala de la solución
  - Se puede correr el NAT y el DNS en la misma maquina
    - Incluso en una VM si estamos hablando de pocos clientes
  - Se pueden desdoblar las funciones del NAT y del DNS
    - En diferente hardware
- Se debe compilar el software
  - Modulo de kernel
  - DNS64
- Seleccionar el prefijo para utilizar para el mapeo

Instalación: Viagenie

- Modulo de kernel:
  - Abrir el fuente, ejecutar make
  - Ejecutar make install y luego depmod –a
  - Editar el script nat64-config.sh
    - Configurar la dirección IPv4 a usar para el mapeo
    - Ejecutar el script

Instalación: Viagenie

- DNS64 (Unbound)
  - Abrir el fuente, ejecutar ./configure –disable-gost
  - Ejecutar make install
  - Editar /usr/local/etc/unbound/unbound.conf
    - Configurar el prefijo para la traducción (que debe coincidir con el elegido para el mapeo)
  - Arrancar el unbound con /usr/local/sbin/unbound-control start

Enlaces

- RFCs
  - 6146
  - 6147
  - 6052
- Ecdysis
  - http://ecdysis.viagenie.ca