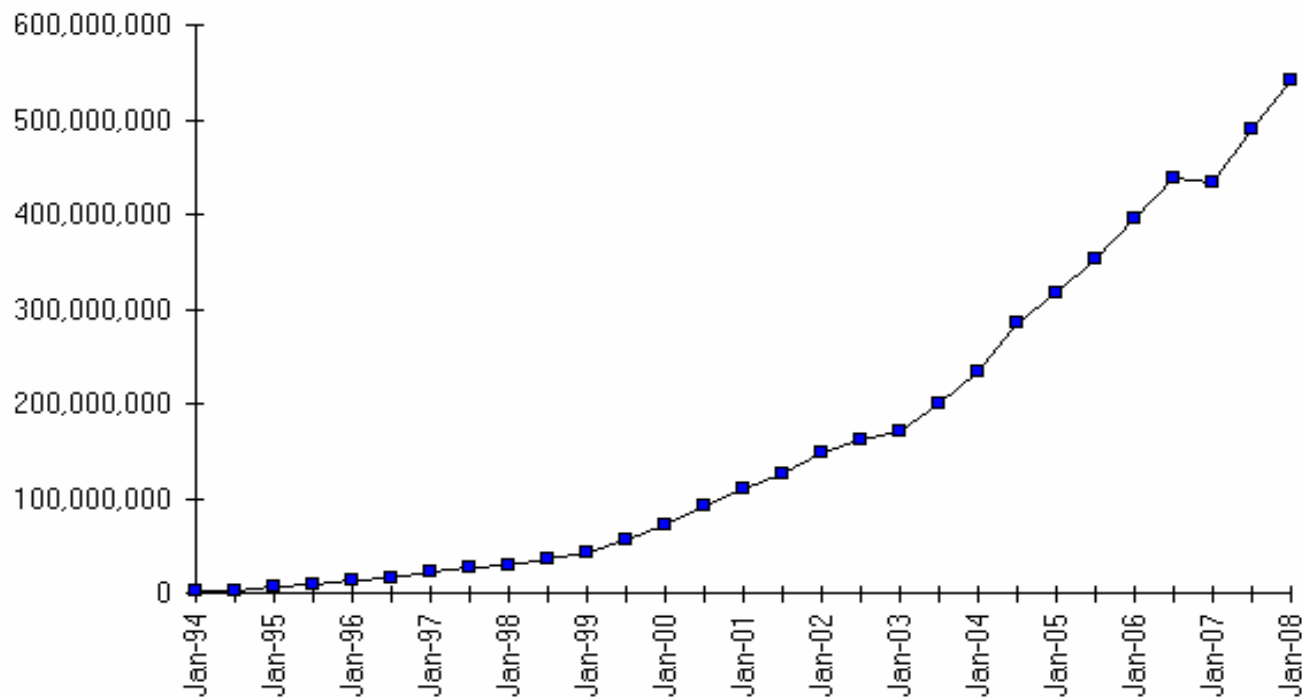

DNS

Servicio de resolución de nombres
para Internet



Internet y el DNS

Internet Domain Survey Host Count



Source: Internet Systems Consortium (www.isc.org)

Redes de Datos – Ing. Marcelo Utard / Ing. Pablo Ronco

Motivación para el DNS

Conveniencia de usar nombres en vez de números

- Establecen contexto
- Desacopla el elemento referencial (lo que se utiliza para identificar) del punto de conexión física a la Internet. Si un servidor se cambia de ISP, cambia su numeración de IP, routing a nivel IP, etc.; pero el nombre dns no necesita cambiarse.
- Surge ante la necesidad de escalar adecuadamente la funcionalidad de resolución de nombres, implementada anteriormente como una tabla en formato texto, que se distribuía manualmente y se mantenía centralizadamente.

DNS - Domain Name Service

Es una única base de datos

Se consulta en modalidad cliente-servidor:

El cliente se llama “resolver”

El “server” está distribuido

La base de datos se distribuye entre muchos servidores individuales, que forman una federación de nodos que en conjunto brinda el servicio DNS (el servicio DNS se implementa en forma distribuida, no centralizada)

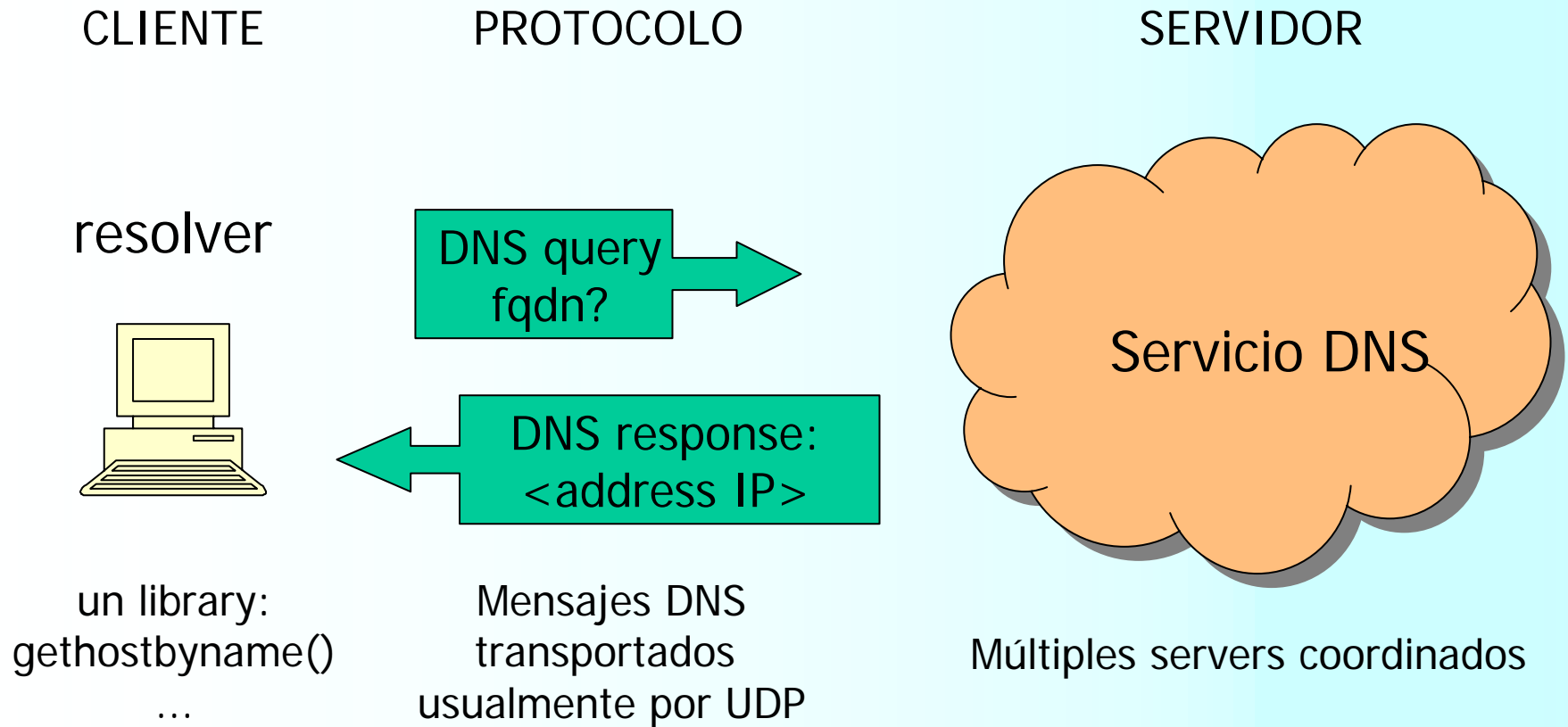
Las altas, bajas y modificaciones a los datos también se hacen descentralizadamente. El conjunto de los datos se divide en partes llamadas zonas. Para cada zona se designa una entidad administrativa que tiene permiso para modificar datos incluidos en la zona.

Los datos del DNS están estructurados según un modelo jerárquico (árbol) para organizar los datos.

Para la comunicación entre cliente y servidor se utiliza un protocolo específico (protocolo del DNS) cuyos mensajes se transportan mediante UDP y TCP



Arquitectura para consultas



Estructura de datos en en DNS

Los datos se estructuran según un árbol n-ario, no balanceado

Los nodos del árbol llevan etiquetas (labels)

Existe una forma estandarizada de denominar cada nodo del árbol: se utiliza la secuencia de las etiquetas obtenidas de recorrer el árbol partiendo del nodo hacia el nodo raíz. Las etiquetas se concatenan separándolas con un ‘.’ ; y el “.” final se incluye.

Ejemplo protocolo DNS

Frame 1: query a un DNS server:

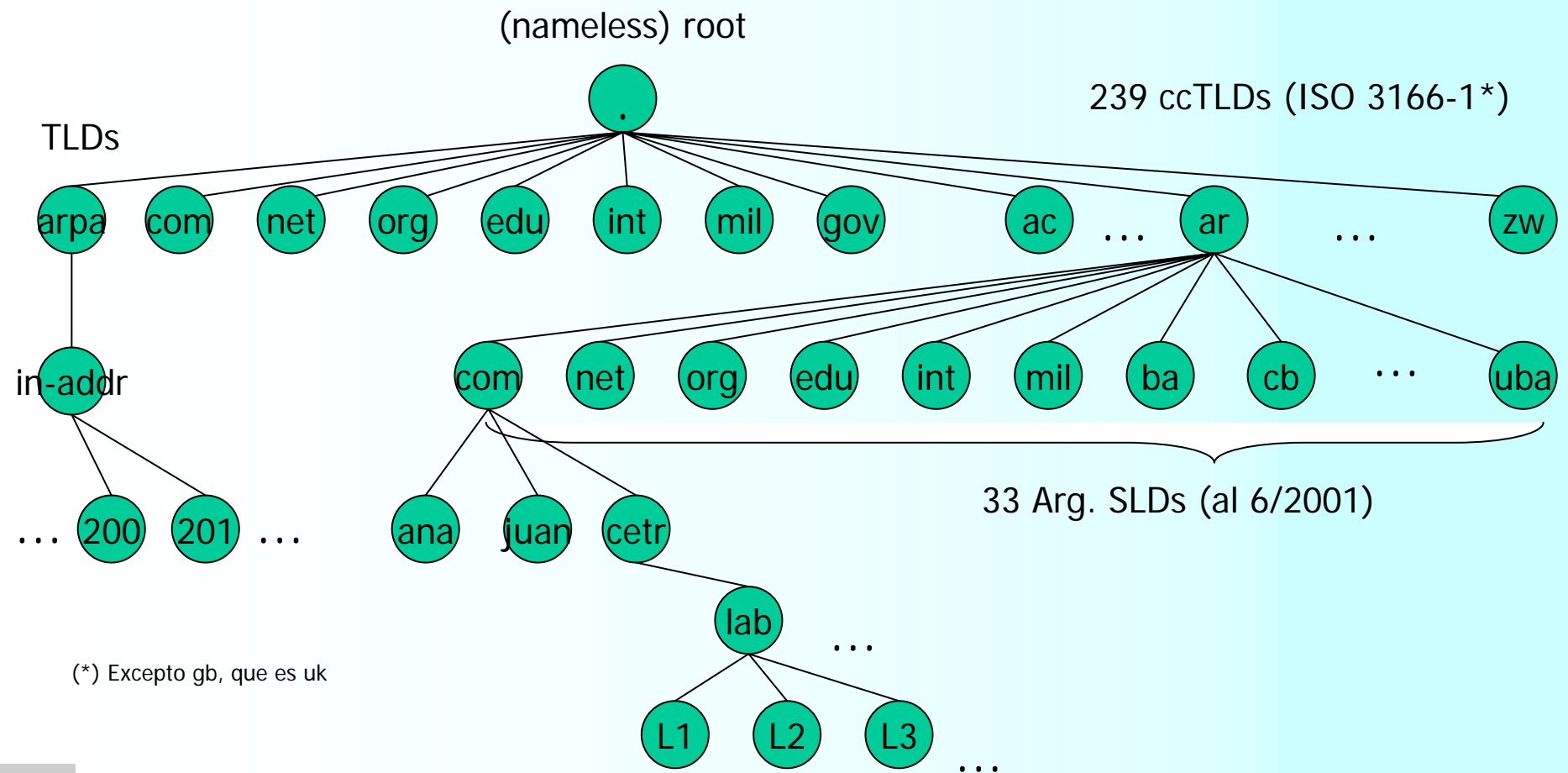
La pregunta es: “indíqueme el address de IP correspondiente al host que se llama neptune.ethz.ch”,
y está dirigida al server DNS cuyo address de IP es 130.59.211.10, conocido previamente

Frame 2: respuesta del DNS server

El DNS server 130.59.211.10 nos contesta que el nombre “neptune.ethz.ch” es en realidad un alias a una máquina cuyo nombre canónico es “core.inf.ethz.ch”. Además, en la misma respuesta se nos informa que el address de IP de core.inf.ethz.ch es 129.132.178.196

Nota: esta transacción es parte de una serie de consultas y respuestas que tienen lugar durante la resolución del nombre, que en muchos casos involucran varias rondas de consultas similares a la ejemplificada aquí.

Estructura de datos



(*) Excepto gb, que es uk

FQDN

Secuencia de “labels”, separados por “.”, terminados con “.”

[a-z, A-Z, 0-9, -]

Mayúsculas y minúsculas son equivalentes (case insensitive)

Long. máxima label: 63 caracteres

Ejemplo:

www.acme.com.ar.

No confundir con

Address de e-mail: username@mail.acme.com.ar

URL del WWW: <http://www.acme.com.ar/indo/novedades.html>

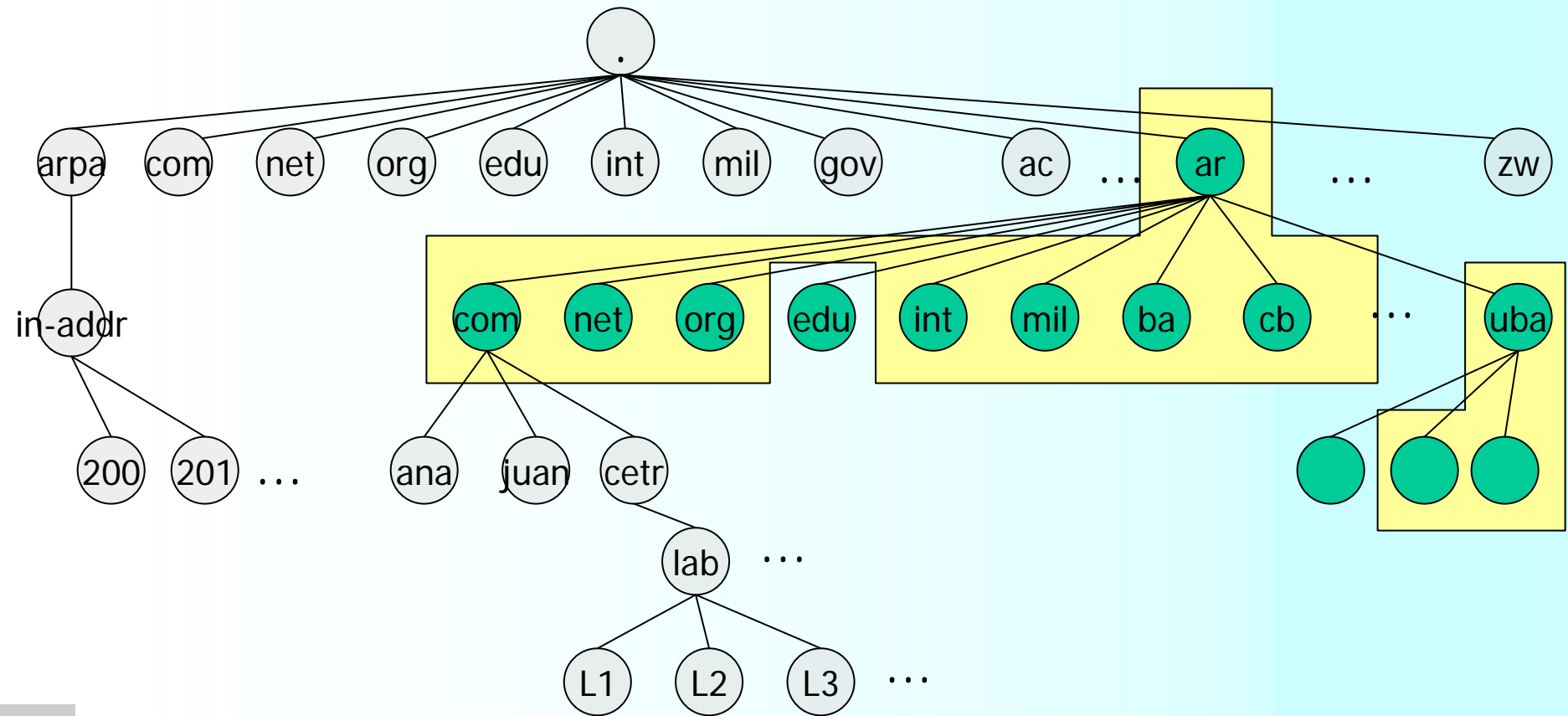
(aunque en ambos casos el elemento contiene un fqdn)

Dominios y zonas

Dominio: la totalidad de los nodos descendientes de un cierto nodo (un sub-árbol)

Zona: una porción de un dominio, administrada por una entidad administradora. Los límites de las zonas están establecidos por la forma con que se particiona y distribuye la base de datos.

Autoridad sobre zonas del DNS



Redes de Datos – Ing. Marcelo Utard / Ing. Pablo Ronco

Estructura de autoridad sobre el árbol del DNS

Para su administración, el árbol (único) del DNS se divide en zonas.

La entidad administrativa que tiene autoridad sobre una porción (zona) del espacio de nombres, puede agregar, eliminar o cambiar labels dentro de esa zona. Por ejemplo, la entidad administrativa que tiene dominio sobre la zona que comienza en .com.ar es el NIC de Argentina, dependiente del MREyC (ver <http://www.nic.ar>).

Una zona comienza en un cierto nodo, e incluye todos los nodos descendientes de éste, excepto los nodos pertenecientes a sub-zonas cuya autoridad haya sido previamente delegada a otras entidades.

DNS

La entidad que tiene autoridad sobre una zona se ocupa de mantener los servidores de DNS correspondientes a esa zona (*authoritative servers*)

Hay 2 tipos de *authoritative servers*:

primario (sólo uno) y secundarios.

Los secundarios actualizan su información automáticamente, consultando al primario.

Nota: del lado cliente, la resolución suele ser mediada por un server especial, llamado caching-only nameserver, en el cual no se configura información sobre ninguna zonas. En estos servers se configuran solamente los addresses de IP de los “root nameservers”

Delegación en la zona in-addr.arpa

En el DNS se reserva un TLD (top level domain) para una zona que permite resolver nombres a partir de addresses de IP.

Los administradores deciden qué datos se colocan allí. Éstos deben asegurar que la información sea coherente (el sistema no incluye chequeos de consistencia de la información ingresada para las distintas ramas del árbol)

Los root-nameservers son autoritativos para las zonas correspondientes a la zona in-addr.arpa, y delegan a otros nameservers con correspondencia a las clases IP tradicionales (A, B y C). Éstos a su vez pueden sub-delegar siguiendo la serie de números decimales que representan los bytes del address de IP.

DNS – Características de la arquitectura

El mapeo de números de IP a nombres en el DNS es arbitrario

cualquier número de IP (independientemente de, por ejemplo, su parte de net-id) puede asociarse con cualquier nombre en el DNS (la asignación de nombres es independiente de la numeración de IP)

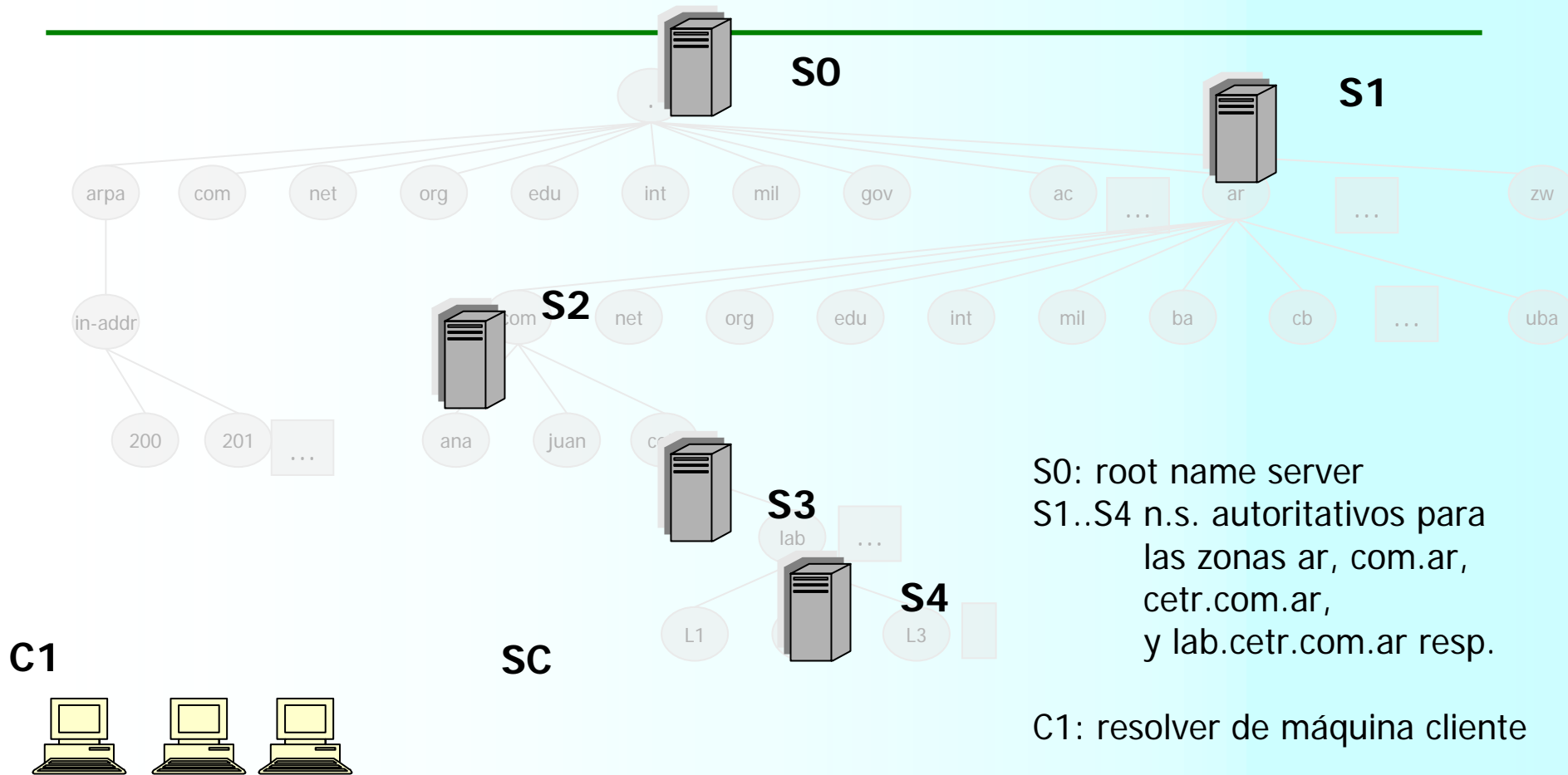
La ubicación de un host en el sistema DNS es independiente del ruteo de los datagramas (éste se hace exclusivamente a partir del id de net -o sub/super-net del número de IP)

La autoridad en el dominio in-addr.arpa sí está relacionada con la conexión física (se delega según las componentes del número de IP)



DNS – Sistema distribuido de servidores

Estructura para los servers del DNS



Servers autoritativos del DNS

Para cada nodo no terminal del árbol del dns se dispone un server DNS correspondiente a la zona que el nodo representa. En ese server se configura manualmente la información relacionada con la zona.

El responsable del mantenimiento del servidor y de la correctitud de los datos que contiene es la entidad que tiene autoridad administrativa sobre la zona.

Se usa más de un server replicado: el conjunto de servidores contiene un primario y uno o más secundarios; todos ellos se denominan autoritativos para la zona

Límites de las zonas

Las zonas se delimitan cuando se delega autoridad sobre una porción de la zona a otra entidad administrativa.

La delegación implica

imposibilidad de modificar datos de la zona delegada mientras la delegación sea efectiva (se mantiene la posibilidad de revocar la delegación)

la necesidad por parte de la entidad a la que se delega de mantener un name server para la zona delegada.



Delegación incorrecta (lame delegation)

Ocurre cuando un server delega en otro autoridad sobre una zona, pero éste no ha sido configurado como autoritativo para esa zona.

Se genera tráfico innecesario sobre la Internet, y demoras debido a las consultas no respondidas hechas a los lame servers.

Se compromete la disponibilidad debido a una falsa percepción de redundancia.

Mecanismo de delegación

Se utilizan registros especiales (registros NS) en el server de la zona “padre” (parent), que indican el número de IP del nameserver de la zona “hija” (child).

El nameserver hijo también incluye registros NS correspondientes a los nameservers autoritativos para su zona. Estos deben corresponder con los consignados en el padre.

glue A records: se utilizan en el padre para indicar el address de IP de los nameservers autoritativos para la zona hija. Sólo son necesarios si el nombre de éstos está dentro de la zona hija.

Tipos de server del DNS

Autoritativos para un dominio
en ellos se incluye la información del DNS

Primario

Secundario(s)

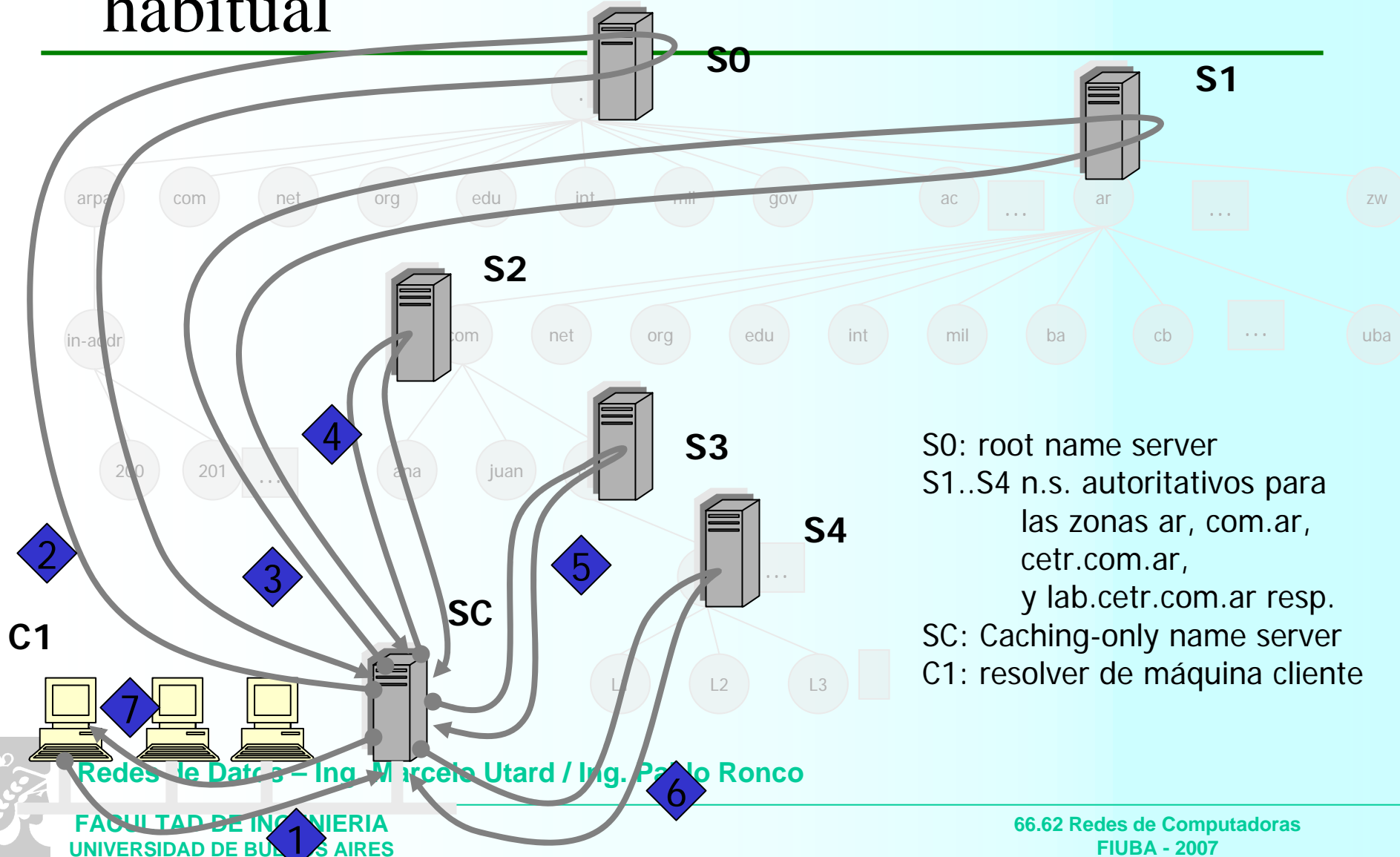
Sincronizan la información con el primario mediante una operación llamada “zone transfer”

Caching-only

Asisten a los clientes en la resolución de nombres.
Permiten acelerar las respuestas y disminuir el tráfico DNS sobre la red.

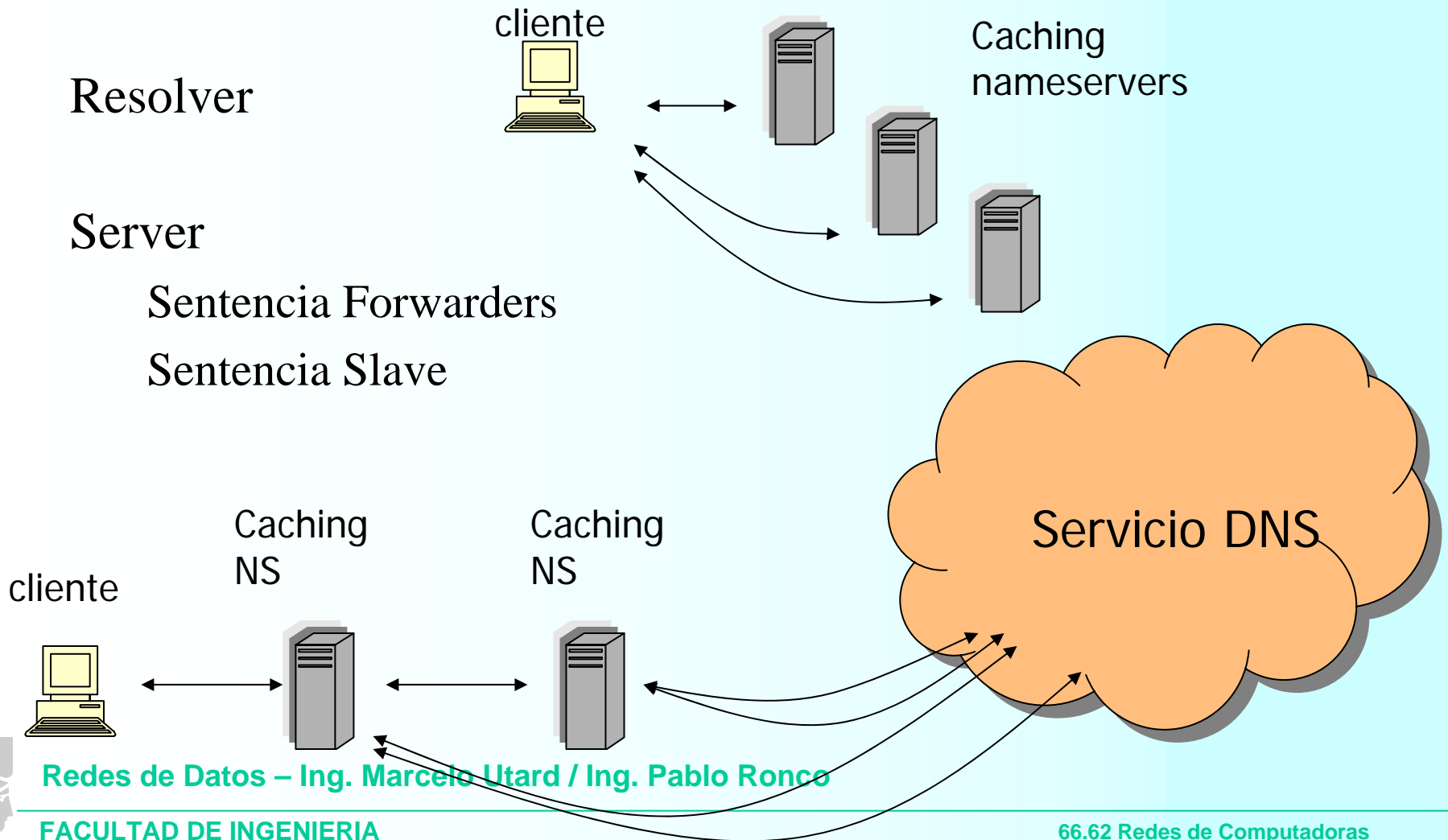
Mecanismos de resolución

Ejemplo de secuencia de resolución habitual



S0: root name server
S1..S4 n.s. autoritativos para las zonas ar, com.ar, cetr.com.ar, y lab.cetr.com.ar resp.
SC: Caching-only name server
C1: resolver de máquina cliente

Forwarders - Slave



Redes de Datos – Ing. Marcelo Utard / Ing. Pablo Ronco

Información contenida en el DNS

Registros en el DNS

- SOA
- A
- NS
- PTR
- CNAME
- MX
- Otros
 - TEXT
 - INFO
 - AAAA
 - ...

Campos del registro SOA

```
@ IN SOA ns1.cetr.com.ar. admin.cetr.com.ar.
2001060606 ; Numero de serie
10800 ; Int. de refresco
; de los secundarios
1800 ; Int. para reintentos
3600000 ; Expiración info. si no se
; puede contactar al primario
86400 ) ; Tiempo de vida mín.en cache
```

Nombre de la zona (\$ORIGIN)
(ver “@”)

Nombre del servidor primario

E-mail administrador de la zona
(com “.” en vez de “@”)

Número de serie de la
información de esta zona

■ Timers

- **Refresh:** cada cuánto tiempo debe el secundario contactar al primario para verificar si su información está actualizada
- **Expire:** si el sec. no puede contactar al primario, cuánto tiempo debe seguir brindando información autoritativa sobre la zona.
- **TTL:** Tiempo mínimo de permanencia de la información en los dns caches. Puede especificarse individualmente en los RRs también.

Registros NS

Se utilizan en las zonas parent para delegar subdominios a servers autoritativos para sus zonas child.

Se especifican en las zonas child para indicar qué servers forman el grupo autoritativo para la zona

Los registros NS que figuran en la zona parent deben ser los mismos que figuran en la zona child.

Debe evitarse la delegación incorrecta “lame delegation”



Registros NS

lab	IN	NS	ns1.lab.cetr.com.ar.
	IN	NS	ns1.cetr.com.ar.
ns1.lab	IN	A	10.0.2.20
ns1	IN	A	10.0.1.20

Glue record

En server autoritativo para la zona parent

```

@                IN SOA  ns1.cetr.com.ar.  admin.cetr.com.ar. (
                2001060606      ; Numero de serie
                10800           ; Int. de refresco
                                ; de los secundarios
                1800            ; Int. para reintentos
                3600000         ; Expiración info. si no se
                                ; puede contactar al primario
                86400 )         ; Tiempo de vida mín.en cache
                IN  NS          ns1.cetr.com.ar.
                IN  NS          ns1.lab.cetr.com.ar.
    
```

En server autoritativo de la zona delegada (child)

Registros A, AAAA y PTR

A: Se utilizan para indicar el mapeo
fqdn -> address de IP.

Puede haber más de un registro A para un cierto fqdn

Puede especificarse más de un address de IP en un registro A

AAAA: similares a A, pero para IPv6

PTR: Se utilizan para indicar el mapeo
address de IP -> fqdn (en la zona in-addr.arpa.)

Registros MX

El DNS colabora con el routing de e-mail (no confundir con el routing de IP) especificando a los mail routers qué servidores de email se deben utilizar para las direcciones de email que correspondan a un cierto dominio del DNS. Se utiliza un tipo especial de registro, llamado MX

```
cetr.com.ar.      IN      MX      10      mail.cetr.com.ar.  
                  IN      MX      20      mail.uyr.com.ar.
```



Dominio en el email address



preferencia



Mail server

Configuración de servidores DNS y de clientes

DNS servers

Un solo proceso puede implementar el servicio DNS para varias zonas a la vez (tanto en rol de primario como de secundario)

El mismo proceso puede ser a la vez un *caching nameserver* para los clientes locales.

Configuración sencilla: un archivo base (/etc/named.conf) lista las zonas y sus opciones, y en un directorio común se ubican un archivo por cada zona



Archivo named.conf (bind 8 y 9)

Define opciones globales

- Access lists

- Directorio para los archivos de las zonas

Define las zonas sobre las cuales este nameserver es autoritativo, y declara si es primario (master) o secundario (slave)

Zonas a incluir siempre:

- 0.0.127.in-addr.arpa

- 0.0.0.in-addr.arpa



Configuración principal: /etc/named.conf

```
options {
    directory "/etc/named.d";
    named-xfer "/usr/sbin/named-xfer";
    allow-transfer { 200.49.33.20; };
    query-source address 200.49.33.19 port 53;
};

zone "10.in-addr.arpa" {
    type master;
    file "10.in-addr.arpa.hosts";
    allow-transfer { 10.0.0.1; };
};

zone "cetr.com.ar" {
    type master;
    file "cetr.com.ar.hosts";
};
```

```
zone "." {
    type hint;
    file "root.cache";
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "named.local";
};

logging {
    channel lame_channel {
        file "/var/adm/lamers_dns_info";
        severity debug;
    };
    category lame-servers { lame_channel; };
};
```

Redes de Datos – Ing. Marcelo Utard / Ing. Pablo Ronco

Configuración de una zona: /var/named.d/cetr.com.ar.hosts

```
@           IN SOA  gogh.uyr.com.ar.  admin.uyr.com.ar. (
                2001060606      ; Numero de serie
                10800           ; Int. de refresco
                                ; de los secundarios
                1800            ; Int. para reintentos
                3600000         ; Expiración info. si no se
                                ; puede contactar al primario
                86400 )         ; Tiempo de vida mín.en cache

                IN   NS      gogh.uyr.com.ar.
                IN   NS      klee.uyr.com.ar.
cetr.com.ar.  IN   MX      10  gogh.uyr.com.ar.
localhost    IN   A        127.0.0.1
www          IN   A        10.0.100.100
lab          IN   NS      ns1.cetr.com.ar.
                IN   NS      ns2.cetr.com.ar.
ns1          IN   A        10.0.1.20
ns2          IN   A        10.0.1.20
```

Configuración

Server primario

En /etc/named.conf:

```
zone "cetr.com.ar" {  
    type master;  
    file "cetr.com.ar.hosts";  
};
```

Server secundario

En /etc/named.conf:

```
zone "acme.com.ar" {  
    type slave;  
    file "cetr.com.ar.secondary";  
    masters { 200.1.2.3 ; };  
};
```

Configuración - resolver

nameserver

search

options ndots=3



Root nameservers. Cache hints.

Obtención de la lista actualizada de root nameservers: via ftp y dig

El archivo root.cache se utiliza para indicar root nameservers candidatos.

Si al menos un server de la lista root.cache está operativo, el sistema aprende los demás actuales al consultar los registros NS que figuran en el nameserver activo.

Root name servers

#dig @202.12.27.33 . NS

C.ROOT-SERVERS.NET.	192.33.4.12
G.ROOT-SERVERS.NET.	192.112.36.4
F.ROOT-SERVERS.NET.	192.5.5.241
B.ROOT-SERVERS.NET.	128.9.0.107
J.ROOT-SERVERS.NET.	198.41.0.10
K.ROOT-SERVERS.NET.	193.0.14.129
L.ROOT-SERVERS.NET.	198.32.64.12
M.ROOT-SERVERS.NET.	202.12.27.33
I.ROOT-SERVERS.NET.	192.36.148.17
E.ROOT-SERVERS.NET.	192.203.230.10
D.ROOT-SERVERS.NET.	128.8.10.90
A.ROOT-SERVERS.NET.	198.41.0.4

Temas adicionales

Balanceo de carga utilizando DNS

Selección según esquema circular (round-robin)

Sorting en el resolver



Troubleshooting - Herramientas

Herramientas cliente

nslookup

```
>server athea.ar
```

```
>set type=NS
```

```
>ctr.com.ar.
```

```
...
```

```
>ls ctr.com.ar.
```

dig

```
dig @athea.ar ctr.com.ar. ns
```

```
dig @ns1.ctr.com.ar ctr.com.ar. soa
```

```
dig @ns2.ctr.com.ar ctr.com.ar. soa
```

```
dig @ns1.ctr.com.ar ctr.com.ar. axfr
```

Configuración BIND – Puntos importantes

Evitar utilizar CNAMEs, salvo para referir a los servidores de los principales servicios

```
www      IN CNAME h1.acme.com.ar
```

```
ftp      IN CNAME h1.acme.com.ar
```

```
mail IN CNAME h23.acme.com.ar
```

Identificadores usados en regs. NS, MX no deben ser CNAMEs

En todos los servers:

Incluir zona primaria para 0.0.127.in-addr.arpa.

Incluir registro para localhost.dom.com.ar en la zona:

```
localhost IN A 127.0.0.
```