DNS

Conceptos generales

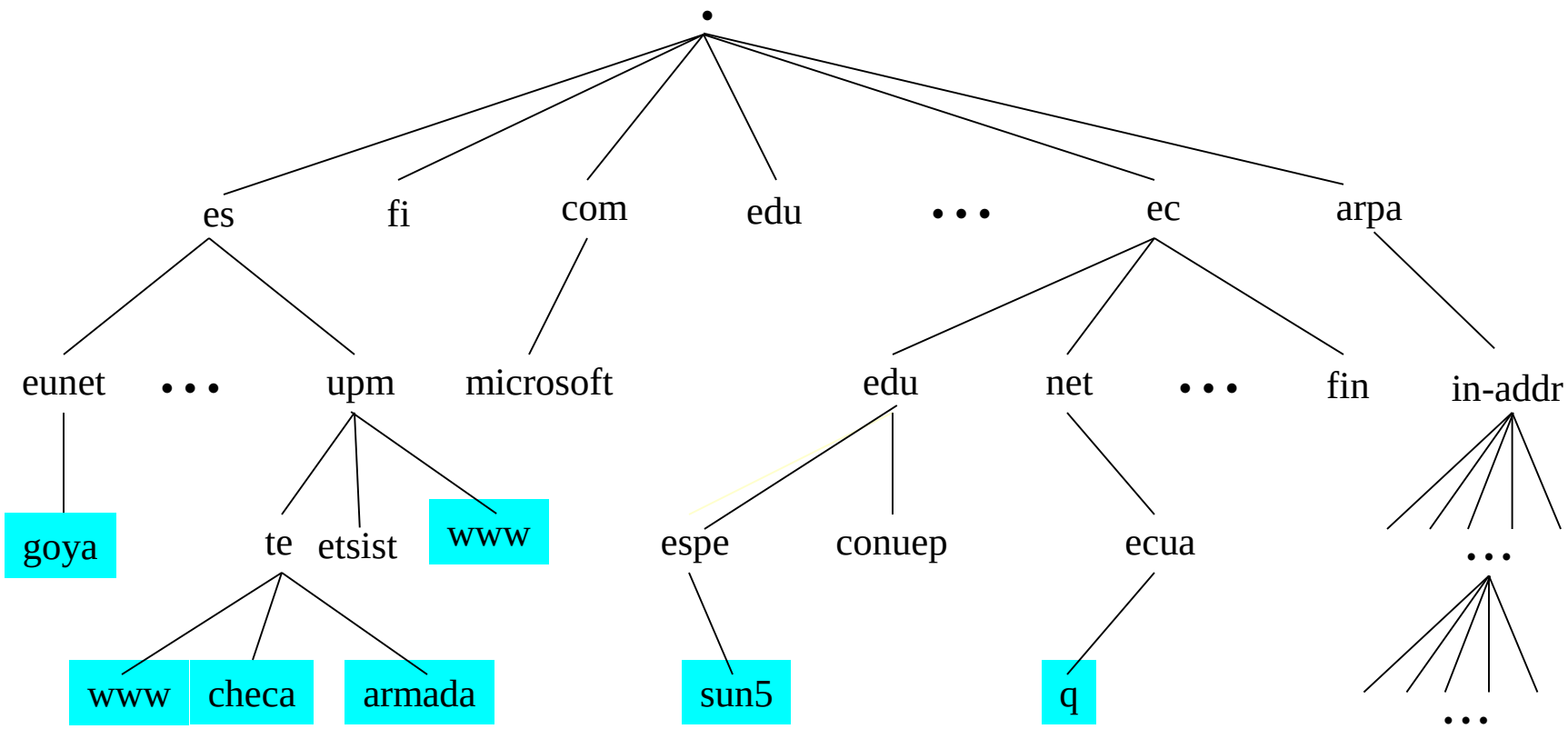
Características del DNS

- Servicio de información
- Jerárquico
- Distribuido
- Replicado (maestro/esclavo)
- Cliente/servidor
- Búsqueda descendente

Funciones del DNS

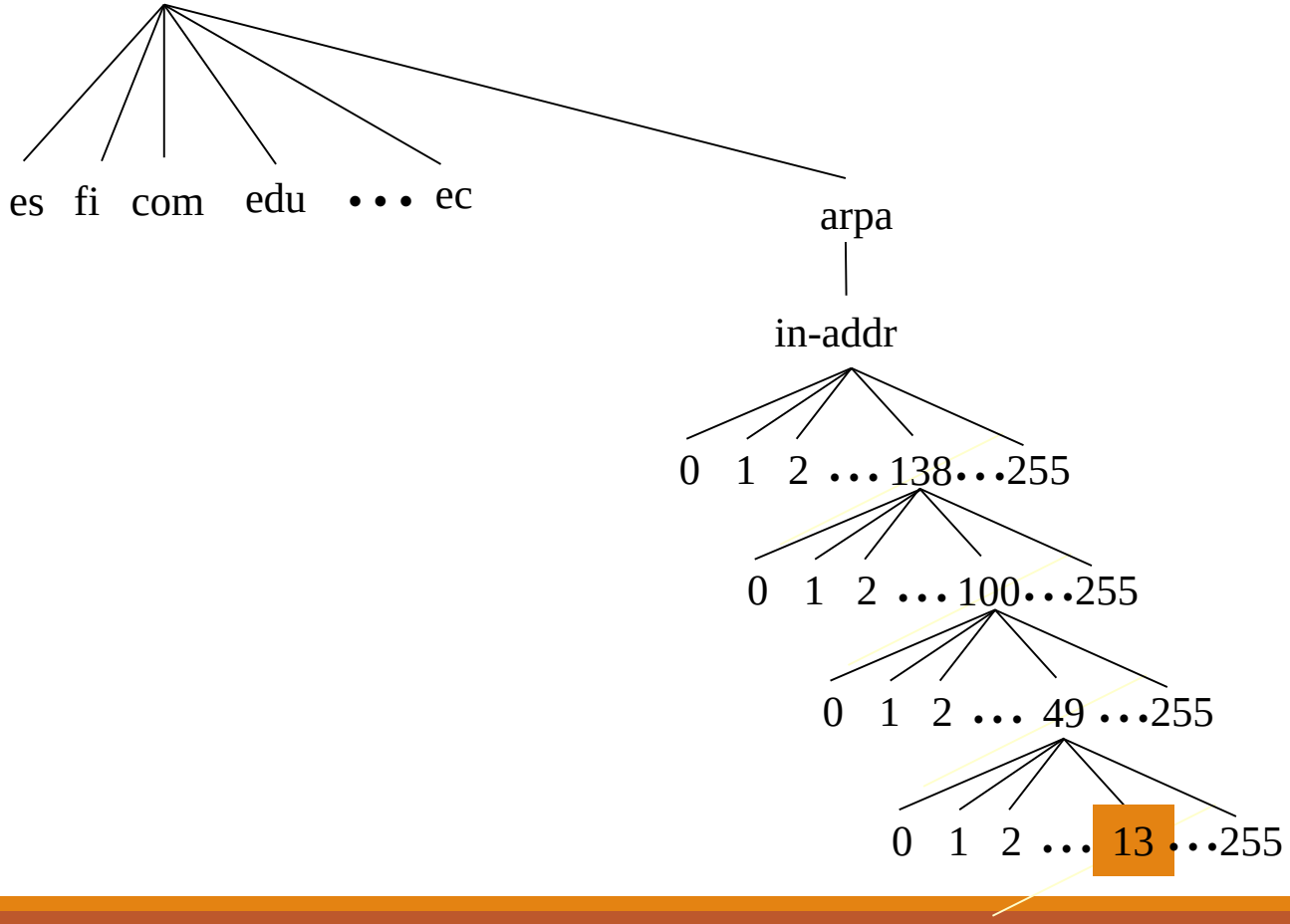
Traducción de nombres a IP	• Directa • Inversa
Encaminamiento del correo electrónico	• MX
Localización de servidores	• SRV • TXT
Otras: p.e., ayuda contra el spam	• SPF, DKIM…

Árbol de DNS

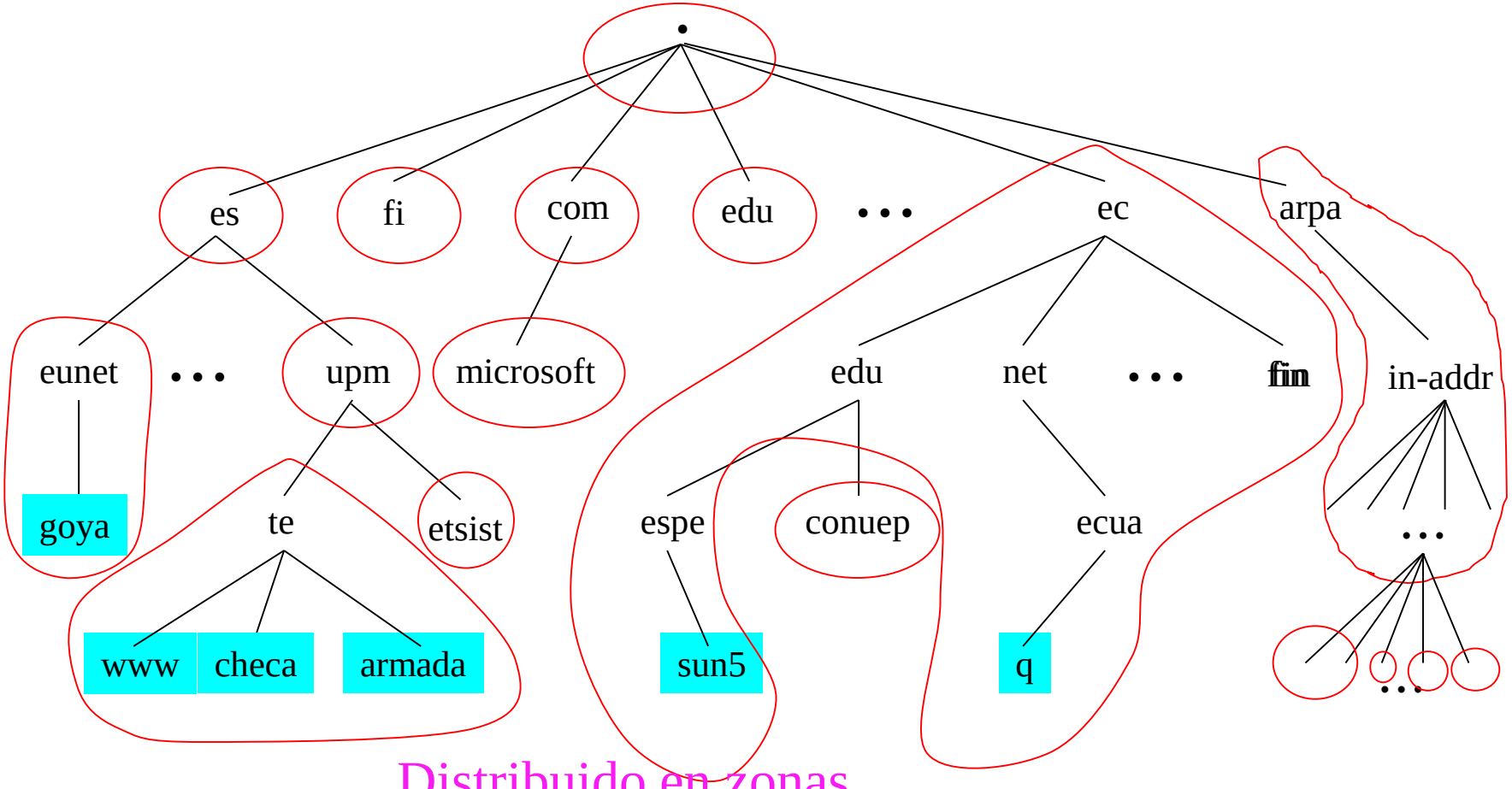


Organizado en dominios y registros

Traducción inversa (PTR)



Distribución de la base de datos

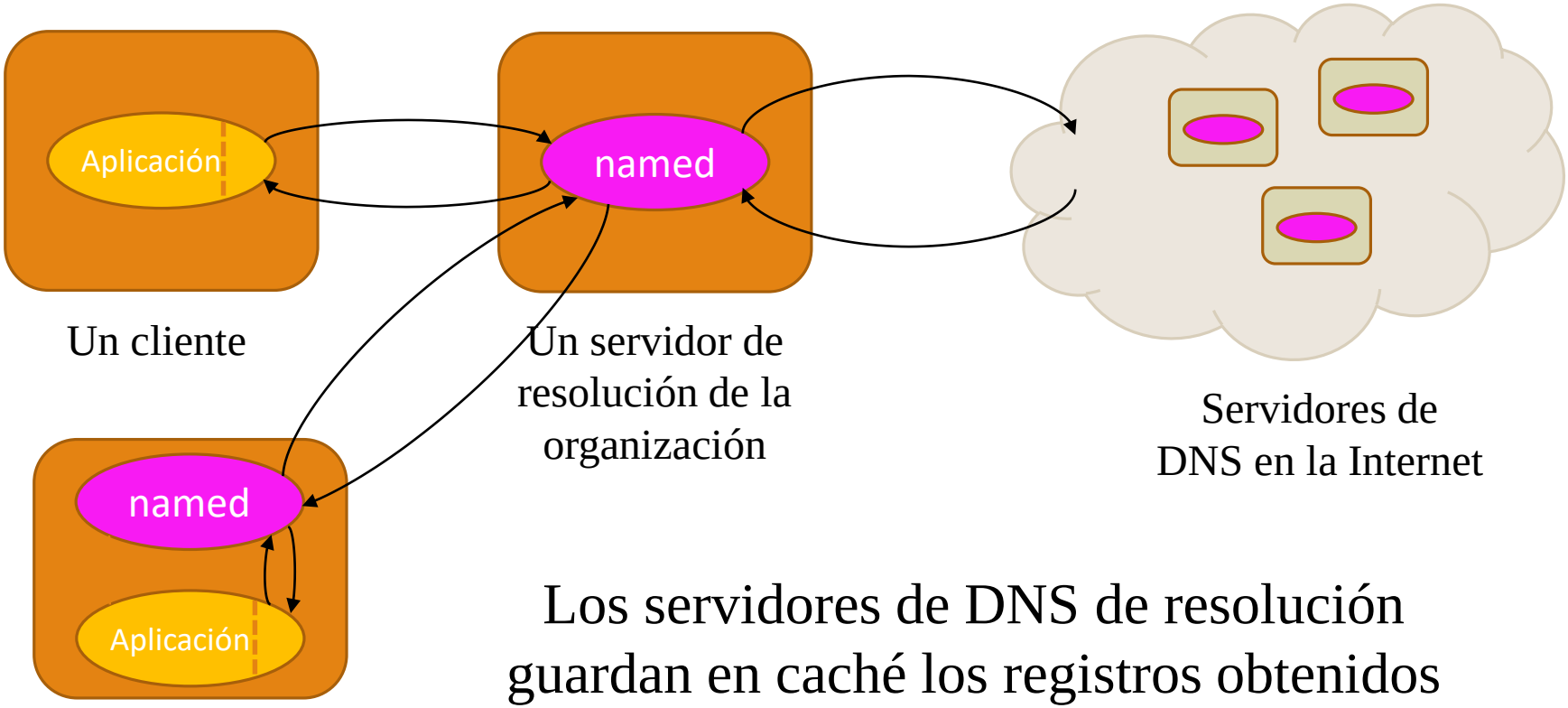


Distribuido en zonas

Elementos del DNS

Servidores con autoridad	• Raíz • Primario • Secundario
Servidores de resolución	• Recursivo • Forwarder
Clientes	• Resolver

Consultas de DNS



Los servidores de DNS de resolución guardan en caché los registros obtenidos (según su TTL)

BIND: resolver

/etc/resolv.conf

```
nameserver 10.49.8.100
nameserver 138.100.52.102
search te.upm.es
```

(Se suele generar automáticamente a partir de la información de DHCP)

Consultas con drill

drill

drill [OPCIONES] nombre [@servidor] [tipo] [clase]

BITS CABECERA:

- qr: QueRy
- aa: Authoritative Answer
- tc: TrunCated
- rd: Recursion Desired
- cd: Checking Disabled
- ra: Recursion Available
- ad: Authenticated Data

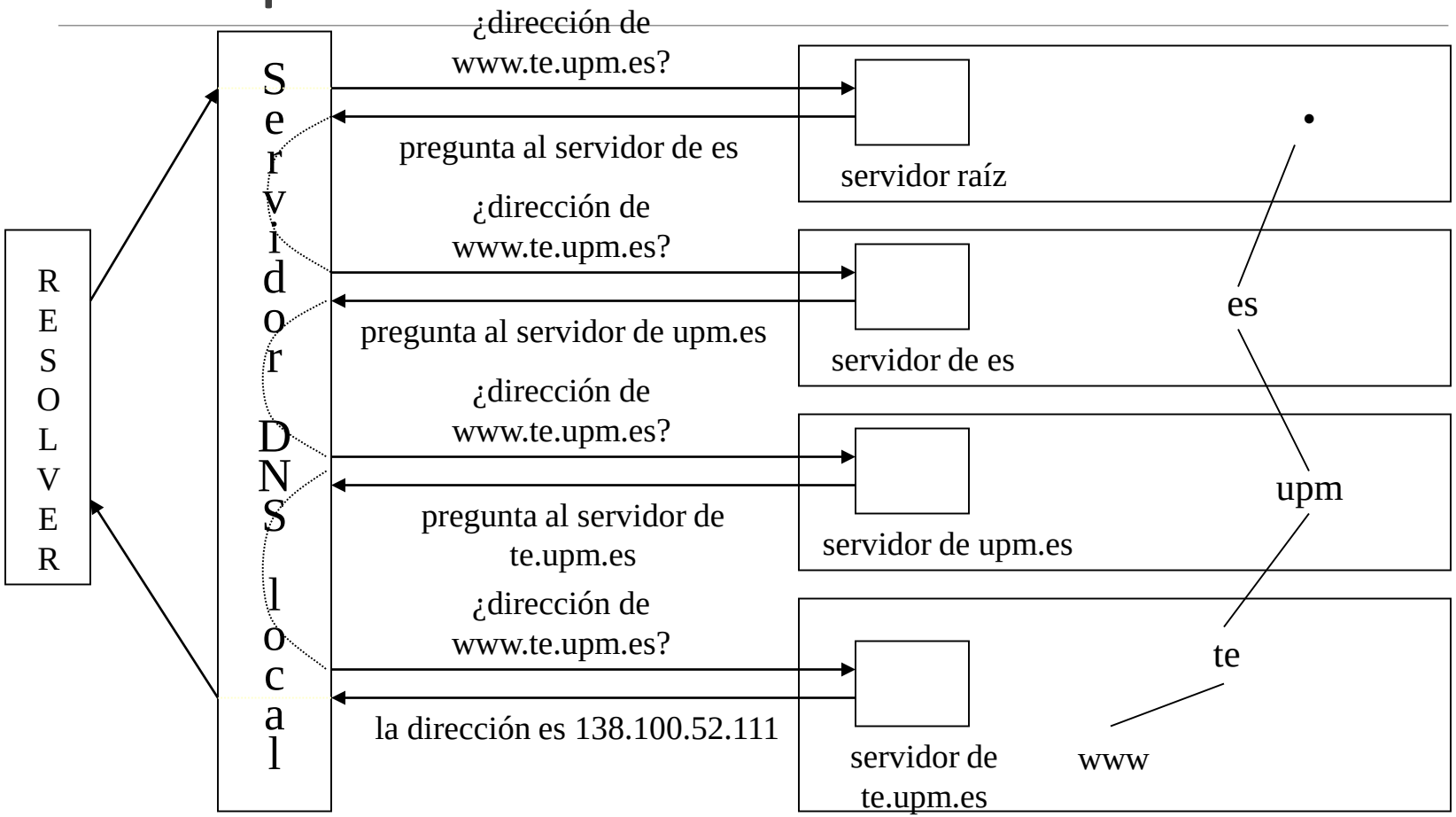
Tipos de registros

clave TTL clase(IN) tipo valor

Tipos

- SOA = Comienzo de autoridad
- NS = Servidor de nombres
- A, AAAA = Nombre -> Dirección IP
- PTR = Dirección IP -> Nombre
- MX = Encaminamiento de correo electrónico
- CNAME = Alias
- SRV = Servicios
- TXT = Texto (ejemplo de uso: SPF)
- Otros

Búsqueda recursiva



Servidor ISC BIND

Servidor de DNS ISC BIND

Demonio **`named`**

Configuración cliente: **`/etc/resolv.conf`**

Configuración servidor: **`/usr/local/etc/namedb`**

- **`named.conf`**: Configuración general
- **`named.root`**: precarga de servidores de la raíz
- **`master`**: ficheros de zona para servidor primario
- **`slave`**: ficheros de zona para servidor secundario

Admite registros SRV, actualización dinámica, IXFR, DNSSEC…

BIND: named.conf

```
// Opciones generales
options { … }
// Punteros a los servidores de la raíz
zone "." { type hint; file "named.root"; };
zone "arpa", "in-addr.arpa" { type slave; … };
// Zonas para anular consultas externas inútiles
zone "localhost", "127.in-addr.arpa", "10.in-addr.arpa" … { type master; file "empty.db"; };
// Ejemplos diversos
zone "example.org" …
```

Operaciones con BIND (I)

Cambios de configuración

Editar named.conf, master/xxx…

named-checkconf

named-checkzone ZONA master/xxx

service named reload / rndc reload

Operaciones con BIND (II)

Consulta de estado y comprobaciones

`rndc status`

`rndc stats`

`rndc dumpdb` (ver opción **`dump-file`**)

`drill / dig`

Operaciones con BIND (III)

Forzar una sincronización con el maestro

```
rndc retransfer prueba.es
```

Modificación manual de zonas dinámicas

```
rndc freeze prueba.es
// Editar zonas
rndc thaw prueba.es
```

Servidores de resolución

BIND: servidor de resolución recursivo (I)

/usr/local/etc/namedb/named.conf

```
options {
   …
   listen-on { any; };
};

zone "." { type hint; file "named.root"; };

// Revisar zonas redes privadas
```

BIND: servidor de resolución recursivo (II)

/usr/local/etc/namedb/named.root

```
. 3600000   IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.  3600000      A     198.41.0.4
. 3600000       NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.  3600000      A     128.9.0.107
. 3600000       NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.  3600000      A     192.33.4.12
. 3600000       NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.  3600000      A     128.8.10.90
```

BIND: servidor de resolución *forwarder*

/usr/local/etc/namedb/named.conf

```
options {
   …
   forwarders { 10.49.8.100; };
   forward only;
};

// Las zonas . ya no se usan.
// Las zonas de redes privadas pueden mantenerse
```

BIND: control de acceso

/usr/local/etc/namedb/named.conf

```
acl miorg { 172.30.99.0/24; 127.0.0.1; ::1; };

options {
   …
   allow-query { any; };
   allow-recursion { miorg; };
};

// Hay más allow-xxx para otras operaciones
```

Servidores autoritativos (primarios)

Registro de dominios

BIND: servidor primario (I)

/usr/local/etc/namedb/named.conf

```
options {
   …
   allow-query { any; };
};

zone "prueba.es" {
 type master;
 file "../master/prueba.es";
};
```

BIND: servidor primario (II)

/usr/local/etc/namedb/master/prueba.es

```
$TTL 60 ; TTL reducido
@  IN SOA    ozono.prueba.es. hostmaster.prueba.es.  (
                    1001          ; N.Serie
                    7200          ; Refresco (2h)
                    1200          ; Reintento (20m)
                    432000        ; Expiración (5d)
                    10 )          ; TTL mínimo (10s)
@                   IN     NS     ozono
@                   IN     NS     helio
@                   IN     MX     100 cerezo.ejemplo.org.
ozono          IN     A      172.30.99.10
argon          IN 90  A      172.30.99.33
metano         IN     A      172.30.99.66
helio          IN     A      10.25.1.45
www            IN     CNAME  metano
```

TTL

Selección del valor adecuado

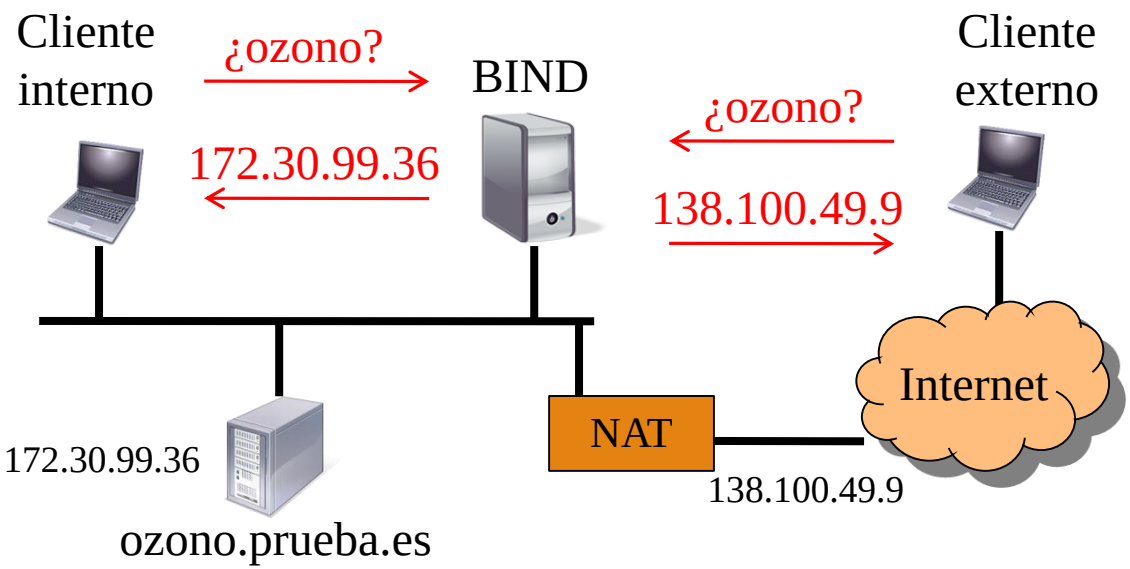
- Elevado: rigidez en los cambios
- Reducido: sobrecarga de consultas

Actualización de registros

- Reducir TTL del registro antiguo
- Esperar antiguo TTL
- Hacer cambio y restaurar TTL habitual

Vistas

Vistas



- Responden diferente según quién pregunte
  - NAT
  - Ocultación de máquinas internas

Vistas

/usr/local/etc/namedb/named.conf

```
options { ... };
acl internas { 172.30.99.0/24; 127.0.0.1; ::1; };
view "red_interna" {
  match-clients { internas; };
  allow-query { internas; };
  allow-recursion { internas; };
  zone . / localhost / in-addr.arpa / ...
  zone "prueba.es" { file "../master/prueba.es.interna"; };
};
view "red_externa" {
  match-clients { any; };
  allow-query { any; };
  allow-recursion { none; };
  zone "prueba.es" { file "../master/prueba.es.externa"; };
};
```

Zonas para traducción inversa

BIND: zona inversa (I)

/usr/local/etc/namedb/named.conf

```
zone "99.30.172.in-addr.arpa" {
 type master;
 file "../master/99.30.172.in-addr.arpa";
};
```

BIND: zona inversa (II)

/usr/local/etc/namedb/master/99.30.172.in-addr.arpa

```
$TTL 60
@   IN SOA    ozono.prueba.es. hostmaster.prueba.es.   (
                    1001          ; N.Serie
                    36000         ; Refresco (10h)
                    1800          ; Reintento (30m)
                    432000        ; Expiración (5d)
                    10 )          ; TTL mínimo (10s)
@   IN        NS    ozono.prueba.es.
@   IN        NS    helio.prueba.es.
10  IN        PTR   ozono.prueba.es.
33  IN        PTR   argon.prueba.es.
66  IN        PTR   metano.prueba.es.
```

Replicación primario-secundarios

Replicación primario-secundarios

El registro SOA de una zona indica a los secundarios:

- Número de serie (para detectar versiones nuevas)
- Intervalo de refresco (sondeo al primario)
- Espera entre reintentos (por si el primario está caído)
- Expiración de los datos (si no se pueden refrescar)

Cuando se modifica el SOA en el primario, éste envía un NOTIFY a todos los secundarios para que se sincronicen

La sincronización se hace mediante una "transferencia de zona". También existen transferencias de zona incrementales (IXFR)

Replicación: servidor primario

/usr/local/etc/namedb/named.conf

```
acl secundarios { 172.30.99.66; 138.100.190.1; };

options {
  …
  allow-transfer { secundarios; };
};
```

Replicación: servidor secundario

/usr/local/etc/namedb/named.conf

```
options {
  allow-query { any; };
  allow-recursion { none; };
  allow-transfer { none; };
  recursion no;
};

zone "prueba.es" {
 type slave;
 file "../slave/prueba.es";
 masters { 172.30.99.10; };
};
```

Otros temas

DNS dinámico (I)

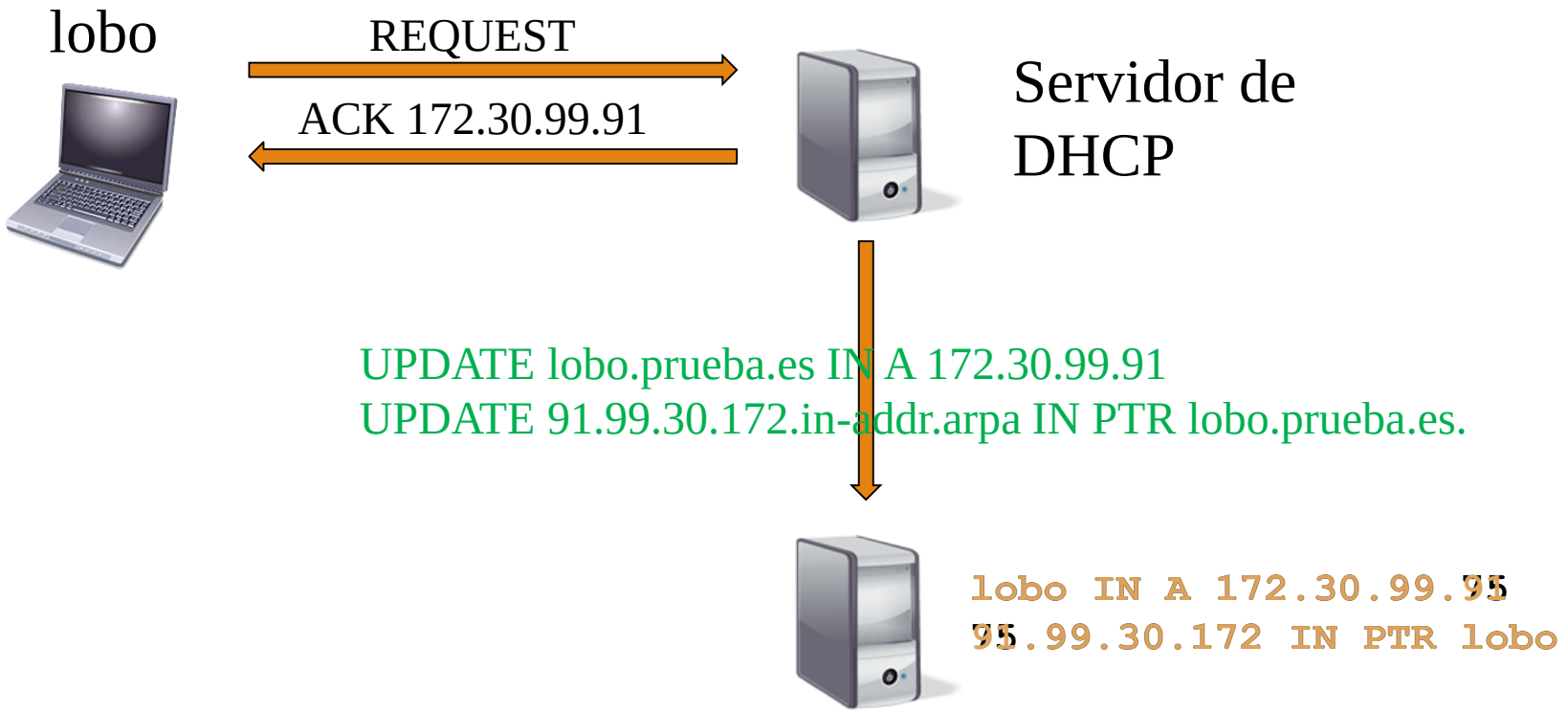
Permite que los clientes actualicen los registros del DNS (RFC 2136 y 3007)

Ejemplos de uso:

- Mantener coherencia directa-inversa con asignación dinámica de direcciones IP
- Actualizaciones de DNS iniciadas por aplicaciones

Riesgo de ataques de suplantación si no se utiliza autenticación segura (por ejemplo, TSIG)

DNS dinámico (II)



GeoIP

Respuesta en función del origen de la consulta

```
options {
  geoip-directory "/var/db/base-datos.mmdb";
};
acl "españoles" {
  geoip country ES;
};

view "españa" {
  match-clients { españoles; };
  zone "prueba.es" { … };
};

view "default" {
  zone "prueba.es" { … };
};
```

Reparto de carga

Reparto de carga mediante *round-robin*

```
ozono       IN    A      172.30.99.101
ozono       IN    A      172.30.99.102
ozono       IN    A      172.30.99.103
```

Reparto de carga en base al estado de los servidores traseros

Reparto de carga en base a la geolocalización del cliente

DNSSEC

Securiza el DNS usando técnicas criptográficas

- Integridad de los datos
- Autenticación del origen de los datos

La información del DNS es pública

- No se cifra la información transmitida
- No se autentica a los clientes

RFC 3008, 3658, 3833