TEMA 1.3. Servicios de Red: DNS

PROFESORES:
Rubén Santiago Montero
Eduardo Huedo Cuesta
Rafael Rodríguez Sánchez

Domain Name System (DNS)

- Mantiene, entre otras cosas, la asignación entre nombres de dominio y direcciones IP
- DNS está implementado como una BD distribuida:
  - Cada sitio guarda información únicamente de sus sistemas
  - Se intercambia y comparte la información con otros sitios
  - DNS recibe y realiza consultas sobre los nombres de dominio
- DNS es un sistema muy complejo:
  - Definido en aproximadamente 108 RFCs
  - Múltiples implementaciones con diferente funcionalidad, por ejemplo:
    - BIND (el más usado)
    - Microsoft DNS, djbdns, NSD, Unbound, PowerDNS
- DNS define:
  - Un espacio de nombres jerárquico de nombres de dominio y direcciones IP
  - Una BD distribuida
  - Un mecanismo para encontrar servicios de red
  - Un protocolo para intercambiar información
  - Herramientas cliente (*resolvers*) para consultar la BD

Zonas y Dominios

Dominio raíz

- Contienen referencias a los servidores de nombres de los dominios de 1er nivel
- 13 servidores de nombres [a-m].root-servers.net (múltiples máquinas - anycast)

Top Level Domains (TLDs)

- Gestionados por ICANN
- Lista completa en http://www.iana.org/domains/root/db
- Cada zona incluye los servidores de nombres autorizados y los servidores de nombres de los subdominios delegados

Generic (gTLD)						Country code (ccTLD)				
com	gov	net	edu	…	org	uk	eu	fi	…	es (www.dominios.es)

google	…	ucm - www - mail

fdi	fis

Dominio

- Subárbol del espacio de nombres de dominio
- Gestión delegada en varias organizaciones

Zona

- Una organización de gestión
- Contiene información de la zona y servidores de nombres de subdominios delegados

Nombres de Dominio

Nombre de dominio completo (FQDN, *Fully Qualified Domain Name*)

- Lista de nombres de nodo o etiquetas de dominio (ej. www, printer-server...) que representan la jerarquía desde el nivel más bajo hasta el raíz (aunque se suele omitir), utilizando el carácter de punto como separador entre etiquetas
  - Ejemplo: www.ucm.es. (parte más significativa, “.”, a la derecha)

Espacio de nombres para direcciones IP

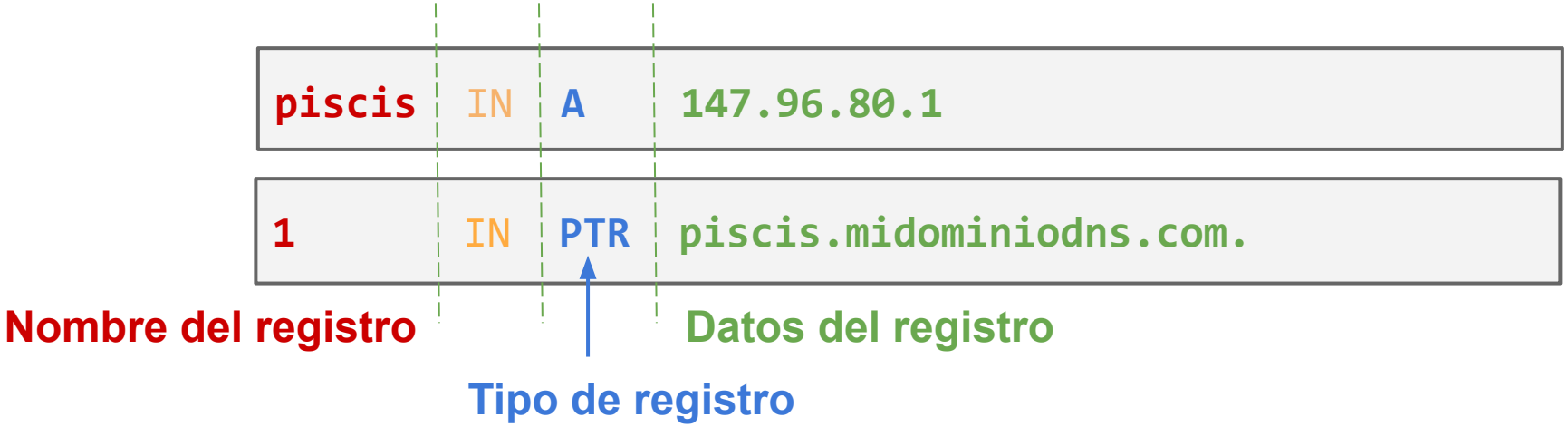
- Para búsqueda inversa: obtener el nombre de dominio asociado a una IP
- La dirección IP se invierte para que la parte más significativa esté a la derecha
- Para IPv4 se usa el dominio in-addr.arpa.
  - Ejemplo: 63.173.189.1 → 1.189.173.63.in-addr.arpa.

Restricciones en los nombres de dominios

- No hay límite en el número de subdominios de la jerarquía
- El FQDN puede ocupar un máximo de 256 caracteres (incluyendo los puntos)
- Cada sección del FQDN puede tener un máximo de 63 caracteres
- No diferencia entre mayúsculas y minúsculas
- Formados por caracteres alfanuméricos y guiones

Funcionamiento: Registros

- La BD de DNS se estructura en registros (*Resource Records*, RR)
  - DNS gestiona diferentes tipos de registros para almacenar servidores de nombres, asignaciones nombre-IP e IP-nombre, servidores de mail…
  - Los registros son estándar e independientes de la implementación
  - Son la información básica que se intercambia y cachea en los servidores
- Los servidores guardan los registros de sus dominios en ficheros de zona (*zone file*) en formato de texto
  - Ejemplo: piscis.midominiodns.com ↔ 147.96.80.1



Funcionamiento: Protocolo DNS

Protocolo de Transporte

- Principalmente, UDP en el puerto 53
- TCP para transferencias de zona o respuestas de más 512 bytes (RFC 5966)

Mensajes (RFC 1035)

ID (16 bits)	**Flags** (16 bits)
Nº RR pregunta	Nº RR respuesta
Nº RR autoridad	Nº RR adicional

- QR: pregunta (0)/respuesta (1)
- Opcode: query (0), status (2), notify (4), update (5)
- AA: respuesta autoritativa (1)
- TC: truncado (1), usar TCP si tamaño > 512 bytes
- RD: recursión deseada (1)
- RA: recursión disponible (1)
- RCode: no error (0), format error (1), server failure (2)...

- La sección Pregunta (en preguntas y respuestas) incluye el nombre de dominio y el tipo de registro por el que se pregunta
- La sección Autoridad especifica los servidores autoritativos de los dominios
- La sección Adicional incluye registros que pueden ser de ayuda (*resolver*)

Funcionamiento: Protocolo DNS

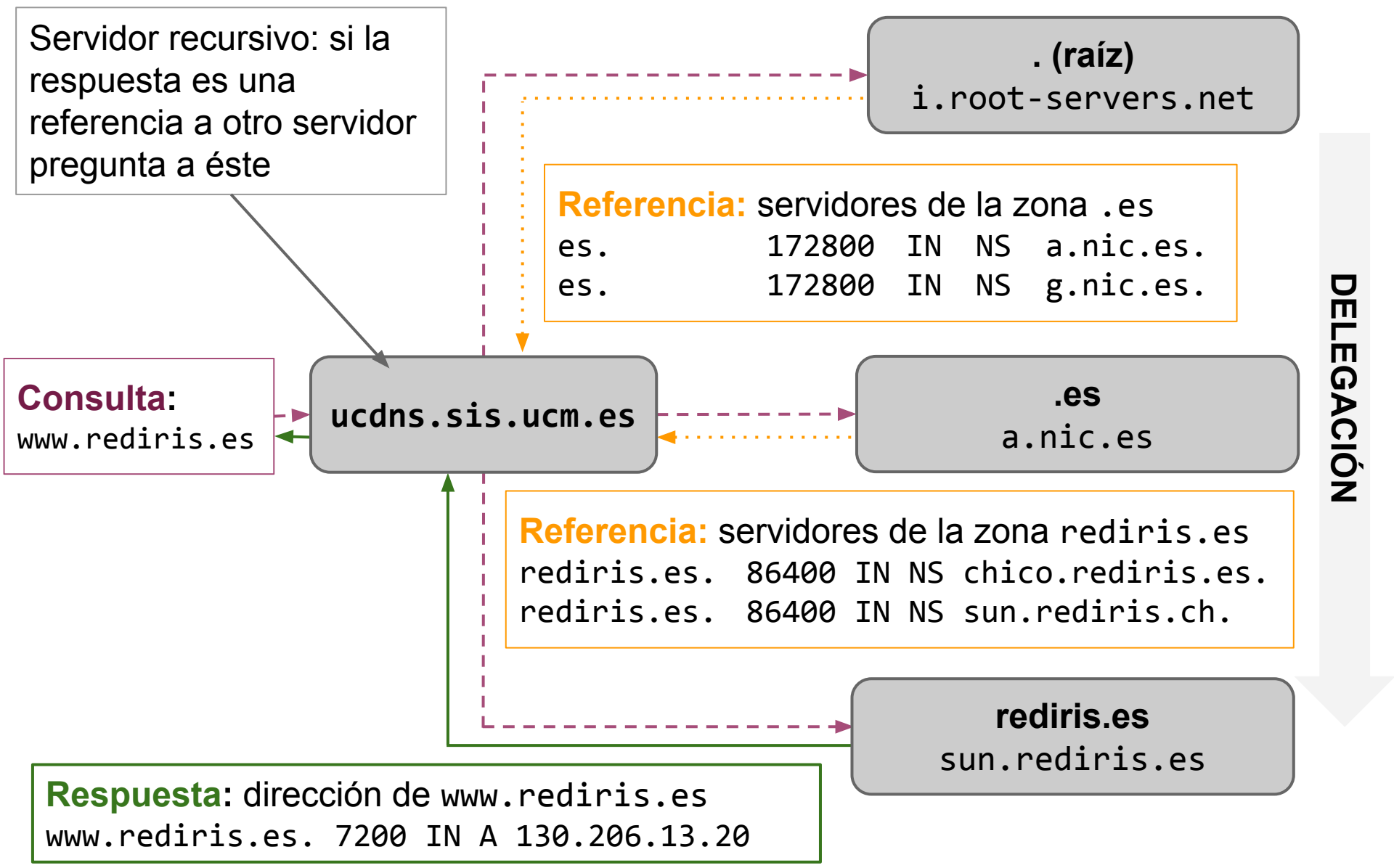
```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19305
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 7, ADDITIONAL: 14
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;informatica.ucm.es.            IN  A

;; AUTHORITY SECTION:
es.                     172800  IN  NS      f.nic.es.
es.                     172800  IN  NS      g.nic.es.
es.                     172800  IN  NS      a.nic.es.
...

;; ADDITIONAL SECTION:
a.nic.es.               172800  IN  A       194.69.254.1
a.nic.es.               172800  IN  AAAA    2001:67c:21cc:2000::64:41
...
```

Funcionamiento: Delegación y Resolución



Funcionamiento: Caching

- Cachear la resolución de direcciones mejora notablemente la eficiencia
  - La relación nombre-IP es prácticamente estática
- Las respuestas se cachean durante un TTL (“time-to-live”), que varía para cada entrada según su probabilidad de cambio:
  - Servidores de “.es”, 2 días (172800)
  - Servidores de “.rediris.es”, 1 día (86400)
  - IP de www.rediris.es, 2 horas (7200)
- Los clientes y servidores de cache pueden observar o no el TTL
- Cache negativa, cuando una búsqueda falla:
  - Ningún dominio encaja en el nombre buscado
  - El registro solicitado no existe para el recurso
  - El servidor no responde o no se puede alcanzar por problemas de red

```
www.google.es.     102 IN  A   173.194.41.248
www.google.es.     102 IN  A   173.194.41.255
www.google.es.     102 IN  A   173.194.41.247
```

- Una búsqueda puede devolver varios resultados
- Forma primitiva de equilibrado de carga

- Más tráfico
- Alta disponibilidad

Servidores de Nombres

Autoritativos (*authoritative*)

- Representan oficialmente a la zona
- Primario o maestro: tiene la copia oficial en disco de la BD
- Secundarios o esclavos: obtienen la BD de los primarios (*zone transfer*)
- La especificación de DNS establece que debe haber un servidor primario y al menos uno secundario por zona

De cache (*caching-only*)

- Guardan los resultados de las búsquedas realizadas partiendo de una lista de servidores del dominio raíz
- No tienen ningún registro DNS propio, ni son autoritativos para ninguna zona
- Reducen la latencia de las consultas y el tráfico DNS en la red

Recursivos y no-recursivos

- No-recursivos: cuando no disponen el registro de la consulta, devuelven una referencia al servidor de nombres que puede tenerlo
- Recursivos: resuelven cada referencia hasta devolver la respuesta al cliente
- Los servidores autoritativos suelen ser no-recursivos
- En la configuración de los clientes deben usarse servidores recursivos

La Base de Datos de DNS

- Archivos de texto (*zone files)* mantenidos en el servidor primario de la zona
- **Directivas**, que especifican cómo interpretar los registros. Directivas estándar:
  - `$ORIGIN`: dominio por defecto que se añade a todos los nombres que no sean FQDN
  - `$INCLUDE`: incluye un archivo con registros, permite mantener separados los registros de datos en diferentes archivos
  - `$TTL`: valor por defecto para el TTL de los registros
- **Registros de Recursos (RR)**, que se asocian a la zona

Formato de los registros (RFCs 1034 y 2181)

```
[nombre] [ttl] [clase] tipo datos
```

- `nombre`: que identifica el registro, normalmente nombre de host o dominio
- `ttl`: tiempo en segundos que se puede cachear y considerarse válido
- `clase`: normalmente IN (Internet)
- `tipo`: Clasificados en 4 grupos (Zona, Básicos, Seguridad y Opcionales), hay gran cantidad de tipos aunque sólo unos pocos se usan habitualmente
- `datos`: Depende del tipo de registro

La Base de Datos de DNS: Registro SOA

- El registro Start of Authority (**SOA**) marca el comienzo de definición de una zona
- La zona incluye los registros dentro del espacio de nombres DNS
- Un servidor DNS tiene normalmente dos zonas:
  - Zona directa (*forward*): traducción nombre → IP
  - Zona inversa (*reverse*): traducción IP → nombre

nombre de la zona (@ se refiere al nombre en `named.conf`)

email de contacto en notación (user.host.) → hostmaster@example.com

servidor primario de nombres de la zona

```
example.com.  IN    SOA   ns.example.com. hostmaster.example.com. (
                                2003080800 ; sn = serial number
                                172800     ; ref = refresh = 2d
                                900        ; ret = update retry = 15m
                                1209600    ; ex = expiry = 2w
                                3600)      ; nx = nxdomain ttl = 1h
```

Entero de 32 bits, que debe crecer con cada versión y actualizarse cuando se modifica la BD

Temporizadores: secundario comprueba cambios cada `ref` segundos, en caso de fallo reintenta cada `ret` segundos, sirve `ex` segundos el dominio si no hay primario y establece TTL de las respuestas negativas a `nx` segundos

La Base de Datos de DNS: Registro NS

- El registro Name Server (**NS**) especifica los servidores autoritativos para la zona
- Además se incluyen los servidores de nombres de los subdominios delegados a otras organizaciones
- Normalmente se añaden después del registro SOA (puede omitirse el nombre por ser el mismo)

Hace referencia a example.com del SOA anterior)

```
        NS  ns.example.com.
        NS  ns1.example.com.
        NS  ns-ha.example.com.
sub     NS  ns.sub.example.com.
        NS  ns.example.com.
```

Notar el "." final para los FQDN

Se incluyen los subdominios para que funcione la delegación, aunque la información corresponde a la zona del subdominio (*glue records*)
Ejemplo: NS de .com debe incluir los NS listados en esta zona (example.com)

La Base de Datos de DNS: Registros A y PTR

Registro A y AAAA

- El registro Address (**A** para IPv4 y **AAAA** para IPv6) es la base de DNS
- Incluye la traducción directa (nombre → IP)

```
ns                  IN  A     63.175.177.1
                    IN  A     63.175.177.4
                    IN  AAAA  2001:501:2f::a01b
ns1.example.com.    IN  A     63.175.177.2
```

No es FQDN, por lo que se completa con `$ORIGIN`. Hay múltiples registros para ns.example.com

Registro PTR

- El registro Pointer (**PTR**) contiene la traducción inversa (IP → nombre)
- Se organizan en diferentes zonas para cada subred (o redefiniendo `$ORIGIN`)

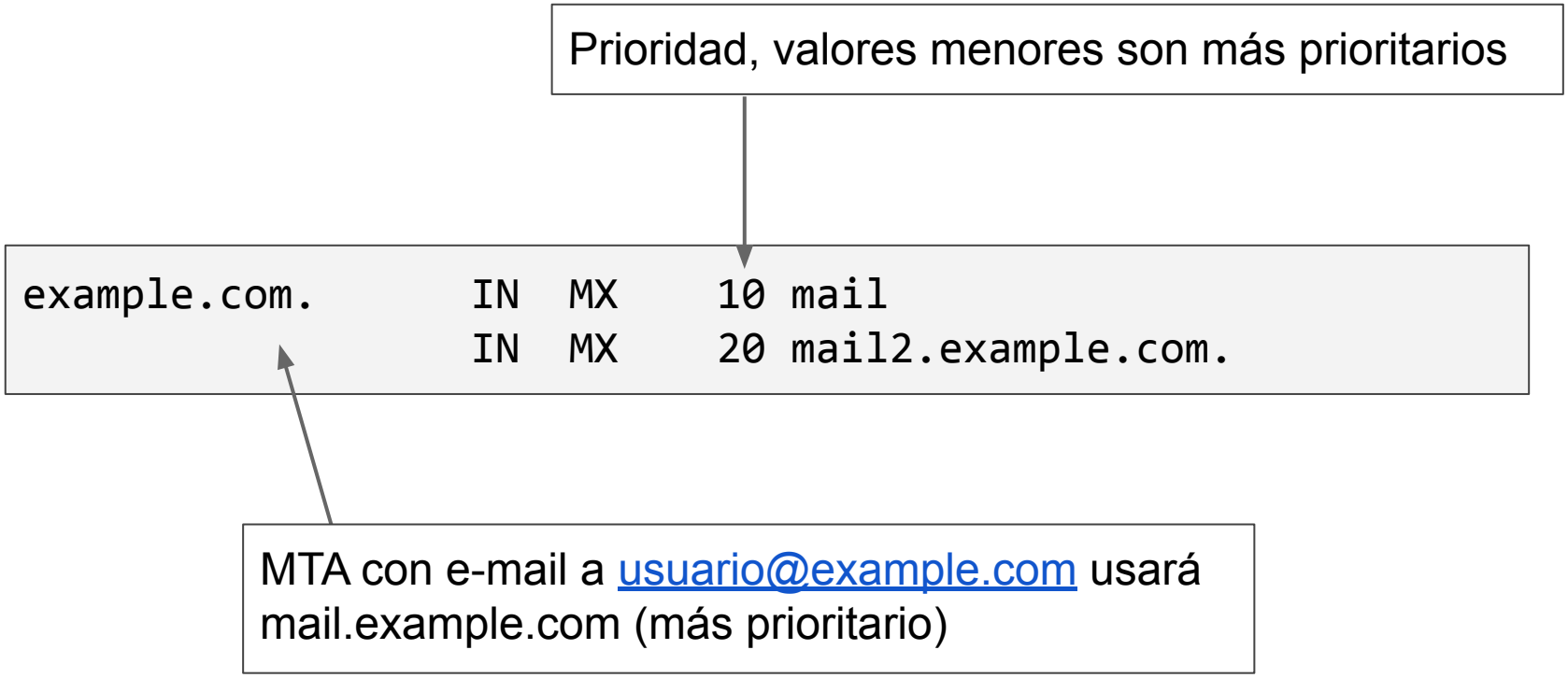
```
1.177               IN  PTR   ns.example.com.
```

Relativo a 175.63.in-addr.arpa

Usar FQDN para que no añada `$ORIGIN`

La Base de Datos de DNS: Registro MX

- El registro Mail eXchanger (**MX**) es usado por los sistemas de correo para encaminar los mensajes eficientemente
- Permite recibir de forma centralizada el correo de una organización y realizar operaciones centralizadas (ej. filtrar spam)



La Base de Datos de DNS: Registro CNAME

- El registro Canonical Name (**CNAME**) se usa para definir el nombre canónico de un nombre de dominio, lo que permite definir un *alias* para el nombre canónico
- Deben siempre apuntar a un dominio (nunca a una IP)
- Un *alias* definido por un CNAME no debe tener otros registros
- MX y NS no pueden apuntar a un CNAME

Este es el nombre canónico

```
informatica.ucm.es.   86400   IN  CNAME   ucm.es.
ucm.es.               86400   IN  A   147.96.1.15
```

- informatica.ucm.es. es un alias de ucm.es.
- También se resuelve el nombre canónico

La Base de Datos de DNS: Ejemplo

```
; Ejemplo para la zona example.com
$TTL 2d ; TTL por defecto = 2 días o 172800 segundos
$ORIGIN example.com.
example.com.  IN    SOA  ns.example.com. admin.example.com. (
                  2003080800 ; serial number (año,mes,día,secuencia)
                  3h         ; refresh = 3 horas
                  15M        ; update retry = 15 minutos
                  3W12h      ; expiry = 3 semanas + 12 horas
                  2h20M)     ; nx ttl = 2 horas + 20 minutos
              IN    NS   ns
              IN    NS   ns-backup
              IN    MX   10 mail ; equivale a mail.example.com.
              IN    MX   20 mail2.example.com. ; servidor de respaldo
; todos los servidores necesitan un registro A
ns            IN    A    192.168.0.10
ns-backup     IN    A    192.168.0.11
mail          IN    A    192.168.0.12
mail2         IN    A    192.168.0.13
www           IN    A    192.168.0.50
```

BIND

- Berkeley Internet Name Domain (BIND) es una implementación *open source* del protocolo DNS
- Las versiones comunes son BIND9 y BIND10
- Componentes:
  - Servidor de nombres: `named`
  - Programa de gestión remota del servidor: `rndc`
  - Clientes: `dig`, `nslookup` and `host`
  - Librerías clientes asociadas para la consulta de servidores DNS
- **Archivos de configuración:**
  - `named.conf`, que especifica las configuración del servidor (tipo, control de acceso…)
  - Archivos de texto con la BD de la zona