



AMPLIACIÓN DE SISTEMAS OPERATIVOS Y REDES

Grado en Ingeniería Informática / Doble Grado

Universidad Complutense de Madrid

TEMA 1.3. Servicios de Red: Filtrado y NAT

PROFESORES:

Rubén Santiago Montero

Eduardo Huedo Cuesta

Luis M. Costero Valero

Cortafuegos

- Un cortafuegos es un componente de seguridad que analiza el tráfico de red y determina si debe permitir su paso (filtrado de paquetes)
 - Otras funciones: Registro de actividad y traducción de direcciones de red
- **Tipos de cortafuegos:**
 - En función del estado (*stateless/stateful*): Si consideran únicamente las características de los paquetes individuales o si además consideran el estado de las conexiones lógicas
 - En función de la capa (de red o de aplicación): Si comprueban las cabeceras de los protocolos de red de los paquetes (IP, ICMP, TCP o UDP) o si también consideran sus datos que pertenecen a protocolos de aplicación (ej. HTTP)
 - En función del elemento protegido (de host o de red): Si protege un solo host o una red completa
- Netfilter/iptables
 - Permite manipular reglas asociadas a tablas
 - Las tablas son una funcionalidad ofrecida por el núcleo del SO (Netfilter)
 - Incluye un programa en el espacio de usuario para la gestión (iptables)

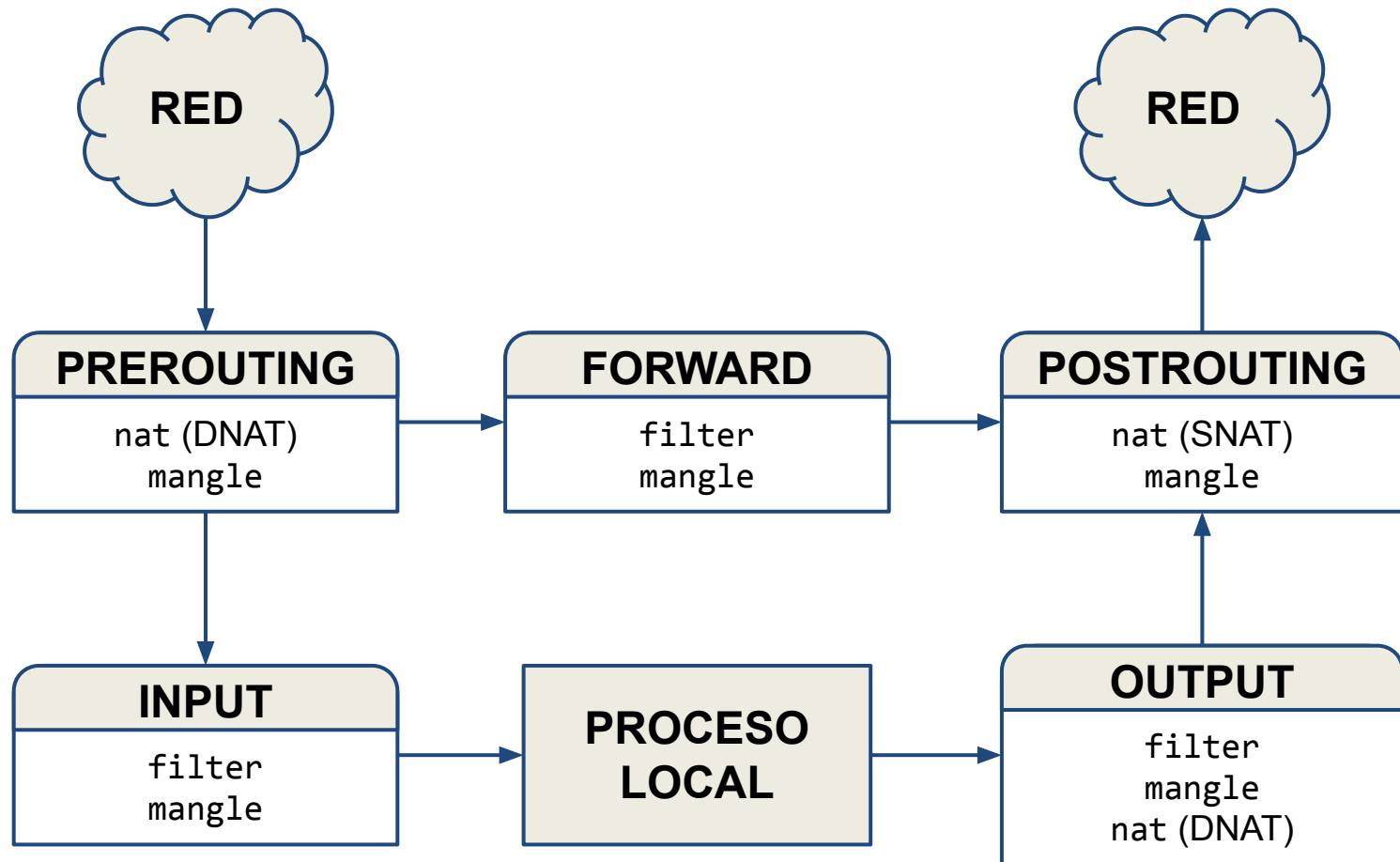
Tablas, cadenas y reglas

- Netfilter/iptables se basa en reglas, cadenas y tablas
- **Reglas:** definen qué hacer (ej. descartar o aceptar) con un paquete que cumple unos determinados criterios (ej. puerto origen, dirección IP destino...)
- **Cadenas:** listas de reglas que se aplican en orden a los paquetes en un punto determinado de su procesamiento
 - Todo paquete de entrada/salida del sistema atraviesa al menos una cadena
 - Si un paquete no encaja en ninguna de las reglas, se aplica la política de la cadena
 - Una regla puede mover un paquete a otra cadena
- **Tablas:** conjuntos de cadenas destinados a diferentes tipos de procesamiento (filtrado de paquetes, NAT...)

Tablas, cadenas y reglas

- Netfilter/iptables incluye algunas tablas y cadenas predefinidas
- La tabla `filter` bloquea o permite el tránsito de un paquete
 - Cadena `INPUT`: paquetes destinados al sistema
 - Cadena `OUTPUT`: paquetes generados en el sistema
 - Cadena `FORWARD`: paquetes que atraviesan el sistema (encaminados)
- La tabla `nat` re-escribe las direcciones origen/destino y puertos de un paquete
 - Cadena `PREROUTING`: paquetes de entrada antes de la decisión de encaminamiento, para DNAT (Destination NAT)
 - Cadena `POSTROUTING`: paquetes de salida después de la decisión de encaminamiento, para SNAT (Source NAT)
 - Cadena `OUTPUT`: paquetes de salida generados localmente, para DNAT
- La tabla `mangle` permite cambiar algunos campos de un paquete (ej. TOS/DS, TTL, MSS...)
 - Tiene las 5 cadenas anteriores

Tablas, cadenas y reglas



Versión simplificada de cadenas y tablas

Comandos

- Se usa la tabla `filter` por defecto
 - Se puede especificar otra con `-t table`
- Comandos para gestión de reglas:
 - `-A chain rulespec`: Añadir regla
 - `-L`: Enumerar todas las reglas
 - `-F`: Borrar todas las reglas
 - `-I chain [rulenum] rulespec`: Insertar regla (`rulenum` es 1 por defecto)
 - `-D chain rulenum`: Borrar regla
 - `-R chain rulenum rulespec`: Reemplazar regla
 - `-P chain target`: Establecer la política por defecto de una cadena

Definición de Reglas

- Las reglas se pueden definir según la información del paquete

Opción/Ejemplo	Significado
<code>-s 192.168.1.1</code> <code>-d 140.10.15.1</code>	Dirección IP origen Dirección IP destino
<code>-p tcp</code> <code>-p udp</code> <code>-p icmp</code>	Paquetes TCP Paquetes UDP Paquetes ICMP
<code>--sport 3000</code> <code>--dport 80</code> <code>--icmp_type 8</code>	Número de puerto origen (TCP o UDP) Número de puerto destino (TCP o UDP) Tipo de mensaje (ICMP)
<code>-i eth0</code> <code>-o eth1</code>	Interfaz de red por el que se recibió el paquete Interfaz de red por el que se enviará el paquete
<code>--tcp-flags ALL SYN,ACK</code>	<i>Flags</i> TCP, donde el primer argumento es la lista de <i>flags</i> a examinar y el segundo argumento es la lista de <i>flags</i> que deben estar activos

Definición de Reglas

- Las reglas también pueden definirse según el estado de la conexión

Opción/Ejemplo	Significado
<code>-m state --state NEW</code>	Paquetes que inician nuevas conexiones (el primer paquete)
<code>-m state --state ESTABLISHED</code>	Paquetes de conexiones establecidas (que han visto paquetes en ambas direcciones)
<code>-m state --state RELATED</code>	Paquetes que inician nuevas conexiones, pero asociadas a una conexión establecida (transferencias de datos FTP, error ICMP...)

Definición de Reglas

- Las reglas deben incluir un objetivo con la opción `-j` (*jump*) para especificar qué hacer con los paquetes que concuerden
- Objetivos para filtrado de paquetes:
 - ACCEPT: deja que el procesamiento del paquete continúe
 - DROP: descartar silenciosamente el paquete
 - REJECT: descarta el paquete y envía un mensaje ICMP de puerto no alcanzable
 - El mensaje se puede cambiar con la opción `--reject-with` (ej. `icmp-net-unreachable`, `icmp-host-unreachable`, `icmp-net-prohibited`...)
 - LOG: registra el paquete (no termina el procesamiento)

Filtrado: Ejemplo (Host)

```
# Política por defecto para cadenas INPUT, OUTPUT y FORWARD
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# Dejar entrar o salir paquetes de conexiones establecidas/relacionadas
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Permitir conexiones entrantes: SSH (tcp/22) desde pc-oficina
iptables -A INPUT -s 200.1.1.1 -p tcp --dport 22 -m state \
    --state NEW -j ACCEPT
# Permitir conexiones salientes: web (tcp/80) a cualquier destino, pop3
(tcp/110) a servidor de correo y DNS (udp/53) a servidor DNS
iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -d 22.1.1.1 -p tcp --dport 110 -m state \
    --state NEW -j ACCEPT
iptables -A OUTPUT -d 22.1.1.2 -p udp --dport 53 -m state \
    --state NEW -j ACCEPT
```

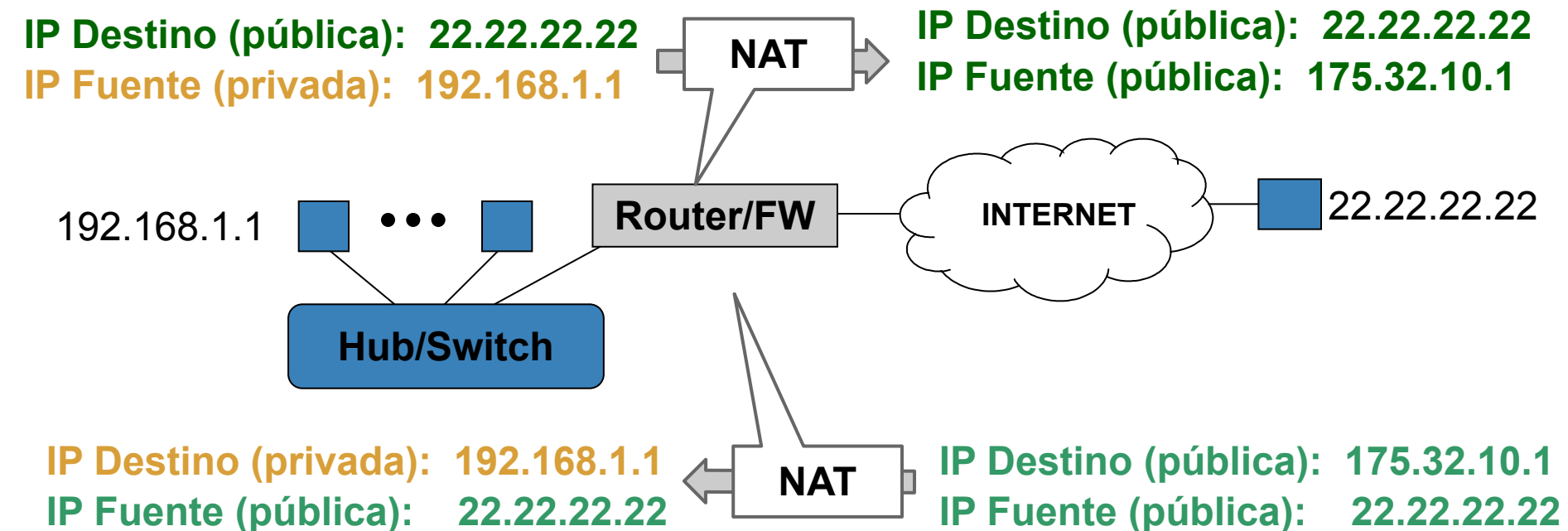
Filtrado: Ejemplo (Red)

```
# Política por defecto para cadenas INPUT, OUTPUT y FORWARD
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# Dejar entrar o salir paquetes de conexiones establecidas/relacionadas
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
# Permitir conexiones salientes: todas
iptables -A FORWARD -i eth0 -m state --state NEW -j ACCEPT
# Permitir conexiones entrantes: servidores web (tcp/80) y DNS (udp/53)
iptables -A FORWARD -i eth1 -d 22.1.1.3 -p tcp --dport 80 -m state \
    --state NEW -j ACCEPT
iptables -A FORWARD -i eth1 -d 22.1.1.2 -p udp --dport 53 -m state \
    --state NEW -j ACCEPT
```

Network Address Translation (NAT)

Redes Privadas IPv4

- Permite aliviar el problema del número limitado de direcciones IPv4
- El objetivo es dar acceso a Internet a máquinas en redes privadas



NAT: Traducción Estática

- Asignación de N direcciones privadas a N direcciones públicas
- Asignación fija
- Ejemplo de tabla de traducción estática para N=7

IP Privada	IP Pública
192.168.1.3	147.96.80.132
192.168.1.23	147.96.80.12
192.168.1.2	147.96.80.122
192.168.1.5	147.96.81.2
192.168.1.4	147.96.81.23
192.168.1.7	147.96.81.77
192.168.1.56	147.96.81.4

NAT: Traducción Dinámica

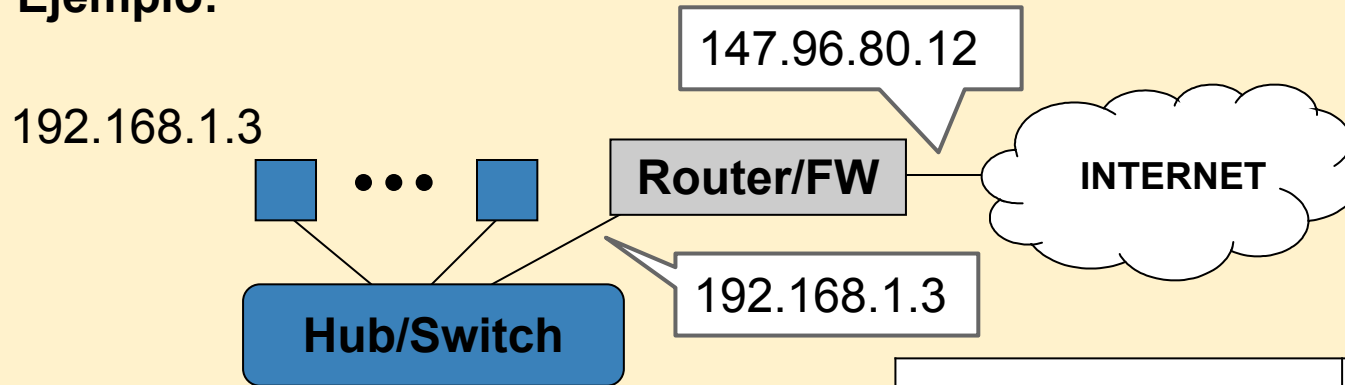
- Asignación de N direcciones privadas a M direcciones públicas ($M < N$)
- Asignación dinámica, sólo pueden acceder a Internet M máquinas a la vez
- Ejemplo de tabla de traducción dinámica para $N=7$, $M=3$

IP Privada	IP Pública
192.168.1.3	147.96.80.132
192.168.1.23	147.96.80.12
192.168.1.2	147.96.80.122
192.168.1.5	Sin posibilidad de acceso a Internet hasta que se libere una IP pública
192.168.1.4	
192.168.1.7	
192.168.1.56	

NAT: NAPT - Masquerading

- NAPT (Network Address and Port Translation)
- Asignación de N direcciones privadas a **1 dirección pública**
- **Funcionamiento:**
 - La única dirección IP pública disponible es la dirección IP pública del router
 - El nº de puerto origen del cliente se traduce a un puerto libre del router

Ejemplo:



IP Privada	IP Pública
192.168.1.3:3453	147.96.80.12:6782
192.168.1.7:2380	147.96.80.12:3342
192.168.1.5:6790	147.96.80.12:4390

NAT: NAT - Masquerading

- El objetivo SNAT de la tabla nat permite cambiar la dirección origen a una dirección IP pública fija
 - Se aplica a la cadena POSTROUTING
 - La traducción se aplica a todos los paquetes salientes de la conexión y se revierte (en la dirección destino) en todos los paquetes entrantes

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 175.20.12.1
```

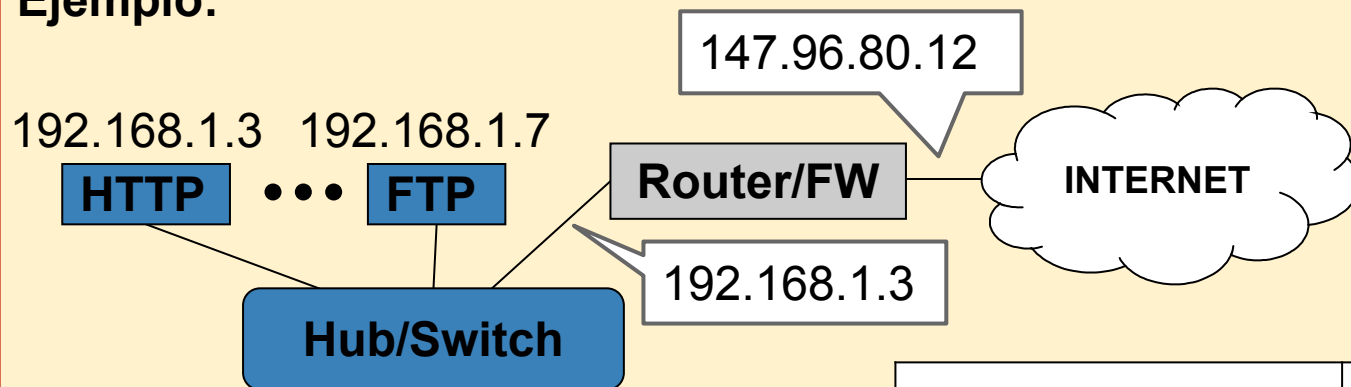
- El objetivo MASQUERADE de la tabla nat permite usar una dirección IP pública dinámica
 - Usa la dirección IP del interfaz como dirección IP origen
 - Al ser dinámica, puede cambiar de una conexión a otra, por lo que realiza un seguimiento de las conexiones activas para aplicar el cambio

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```


NAT: Port Forwarding - Virtual Servers

- Permite tener servidores en la red privada “visibles” desde Internet
- Asignación de **1 dirección pública** a N direcciones privadas
- **Funcionamiento:**
 - Desde Internet, todos los servidores usan la dirección IP pública del router
 - El router traduce y reenvía los paquetes al servidor real de la red interna

Ejemplo:



IP Privada	IP Pública
192.168.1.3:8080	147.96.80.12:80
192.168.1.7:20	147.96.80.12:20
192.168.1.7:21	147.96.80.12:21

NAT: Port Forwarding - Virtual Servers

- El objetivo DNAT de la tabla nat permite modificar la dirección destino de un paquete y, opcionalmente, el puerto
 - Se aplica a las cadenas PREROUTING y OUTPUT
 - La traducción se aplica a todos los paquetes entrantes y se revierte (en la dirección origen) en todos los paquetes salientes

```
iptables -t nat -A PREROUTING -d 175.20.12.1 -p tcp --dport 80 \
-j DNAT --to 192.168.1.1:8080

iptables -t nat -A PREROUTING -d 175.20.12.1 -p tcp --dport 25 \
-j DNAT --to 192.168.1.2

iptables -t nat -A PREROUTING -d 175.20.12.1 -p tcp --dport 20 \
-j DNAT --to 192.168.1.7

iptables -t nat -A PREROUTING -d 175.20.12.1 -p tcp --dport 21 \
-j DNAT --to 192.168.1.7
```

Ejemplos de Preguntas Teóricas

La tabla `filter` de `iptables` sirve para...

- ☐ Cambiar algunos campos de un paquete, como TOS o TTL.
- ☐ Bloquear o permitir el tránsito de un paquete.
- ☐ Reescribir las direcciones origen/destino y puertos de un paquete.

La tabla `nat` de `iptables` sirve para...

- ☐ Cambiar algunos campos de un paquete, como TOS o TTL.
- ☐ Bloquear o permitir el tránsito de un paquete.
- ☐ Reescribir las direcciones y puertos origen/destino de un paquete.



AMPLIACIÓN DE SISTEMAS OPERATIVOS Y REDES

Grado en Ingeniería Informática / Doble Grado

Universidad Complutense de Madrid

TEMA 1.3. Servicios de Red: DNS

PROFESORES:

Rubén Santiago Montero

Eduardo Huedo Cuesta

Luis M. Costero Valero

Domain Name System (DNS)

- Mantiene, entre otras cosas, la asignación entre nombres de dominio y direcciones IP
- 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
- 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
- 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 1^{er} nivel
- 13 servidores [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)

com gov net edu ... org

Country code (ccTLD)

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

Estructura: 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)
- Un nombre que no es FQDN, se denomina **PQDN** (*Partially Qualified Domain Name*)

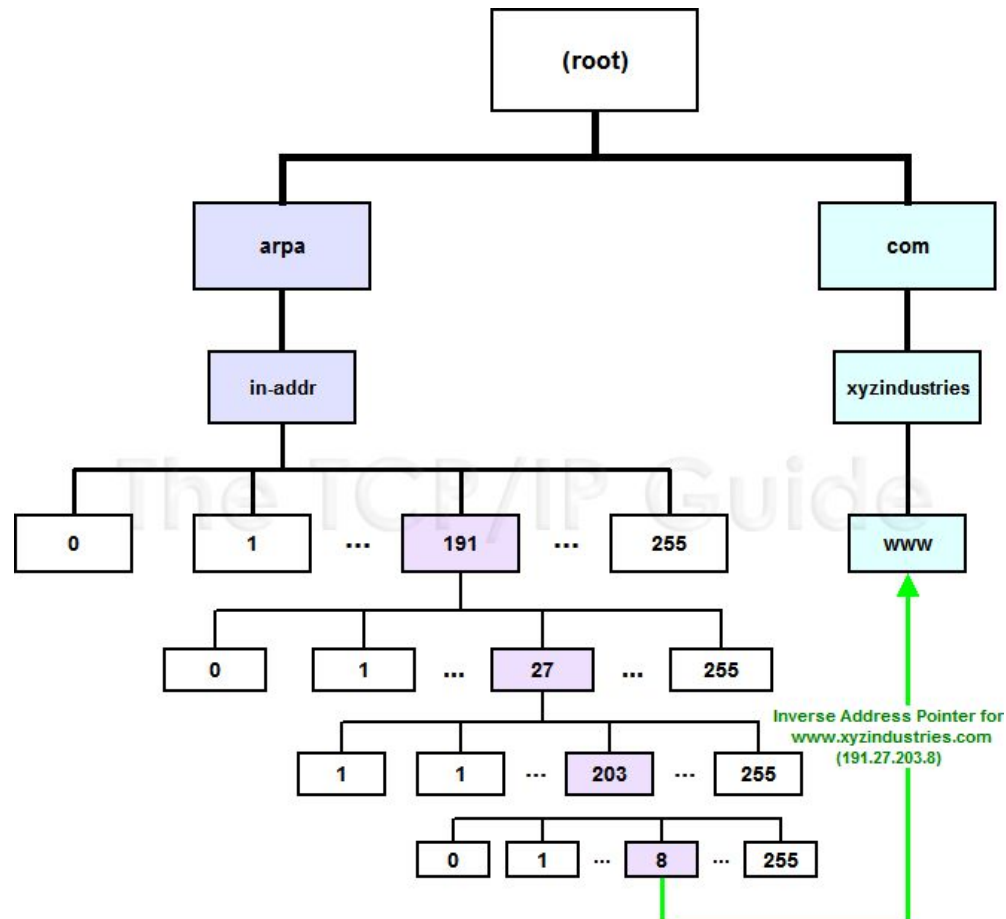
Restricciones en los nombres de dominios

- 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

Espacio de Nombres Inverso

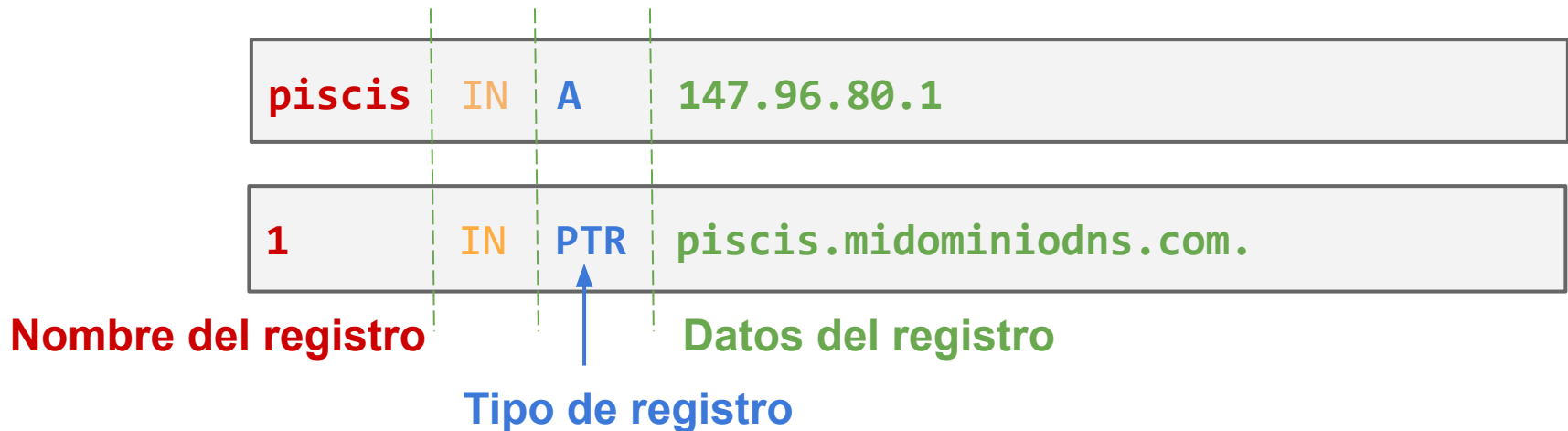
Espacio de nombres para direcciones IP

- 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: 191.27.203.8 → 8.203.27.191.in-addr.arpa.



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 correo...
 - Los registros son estándar e independientes de la implementación
 - Son la información básica que se intercambia y almacena 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`

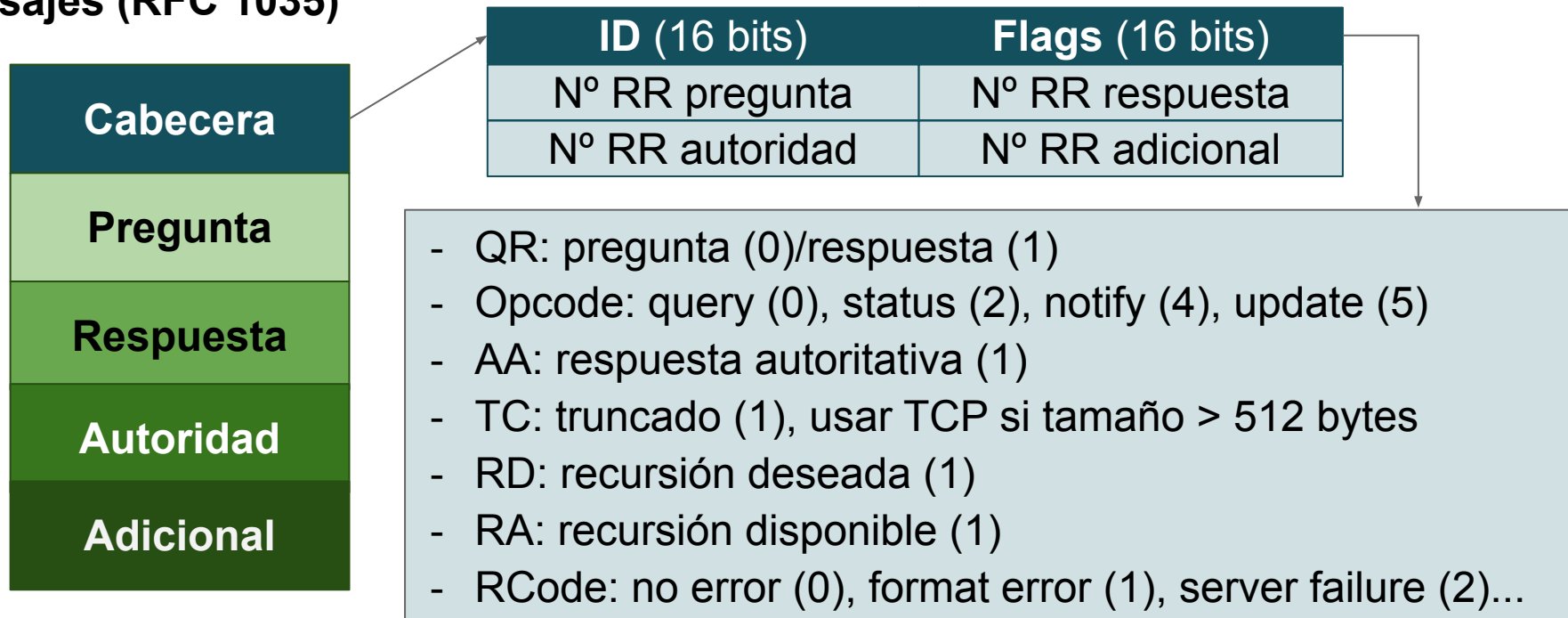


Funcionamiento: Protocolo DNS

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)



- 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

```
$ dig @8.8.8.8 www.rediris.es
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40617
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
```

```
;www.rediris.es.          IN  A
```

```
;; ANSWER SECTION:
```

```
www.rediris.es.          7073    IN  A    130.206.13.20
```

```
...
```

Funcionamiento: Protocolo DNS

```
$ dig @a.root-servers.net www.rediris.es
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26550
```

```
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 8
```

```
;; WARNING: recursion requested but not available
```

```
;; QUESTION SECTION:
```

```
;www.rediris.es.          IN  A
```

```
;; AUTHORITY SECTION:
```

```
es.          172800 IN  NS  g.nic.es.
```

```
es.          172800 IN  NS  c.nic.es.
```

```
es.          172800 IN  NS  a.nic.es.
```

```
es.          172800 IN  NS  h.nic.es.
```

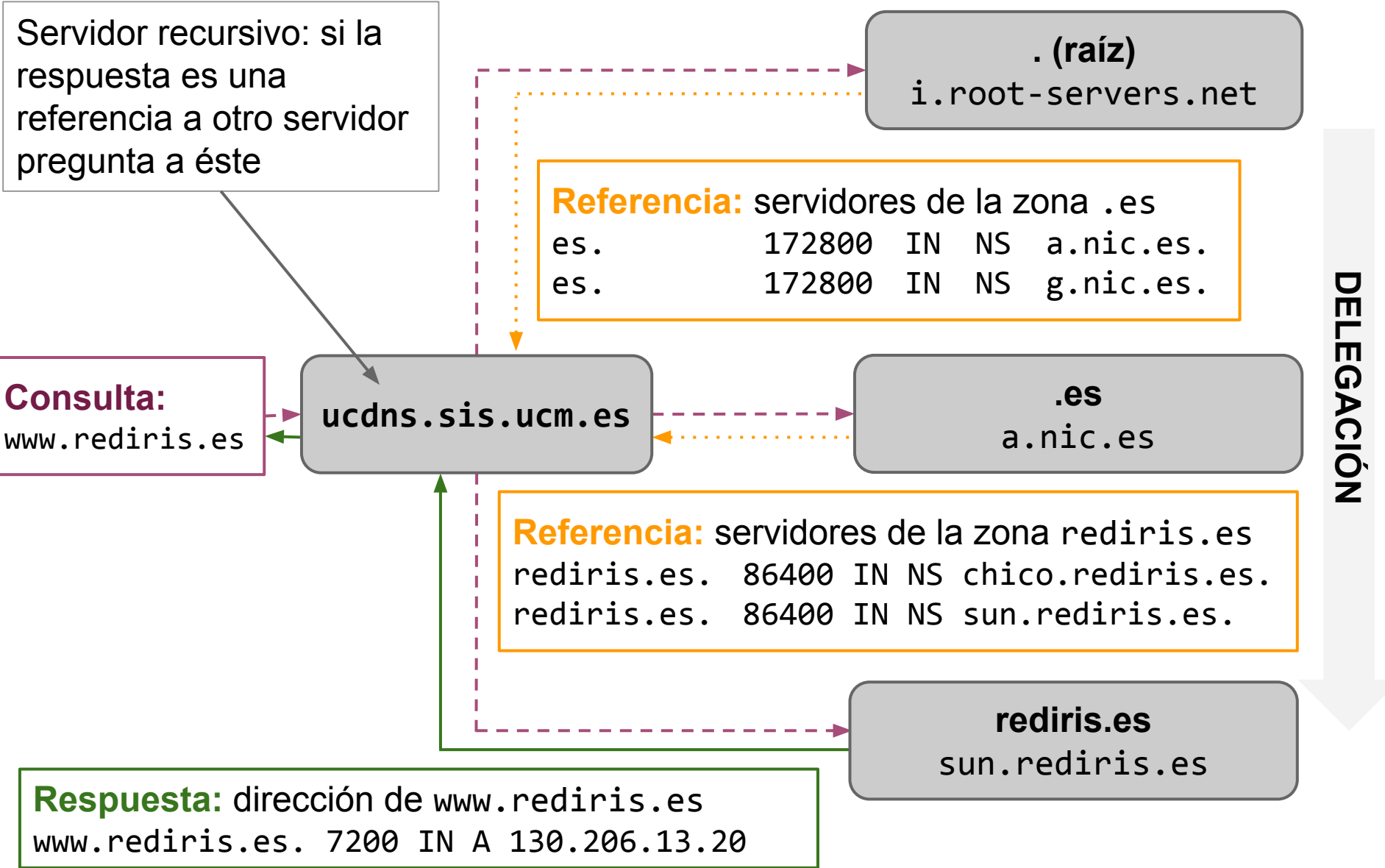
```
;; ADDITIONAL SECTION:
```

```
g.nic.es.    172800 IN  A    204.61.217.1
```

```
g.nic.es.    172800 IN  AAAA  2001:500:14:7001:ad::1
```

```
...
```

Funcionamiento: Delegación y Resolución



Funcionamiento: *Caching*

- Almacenar la resolución de direcciones mejora notablemente la eficiencia
 - La relación nombre-IP es prácticamente estática
- Las respuestas se almacenan durante un TTL (*time-to-live*), que varía para cada entrada según su probabilidad de cambio:
 - Servidores de .es: 2 días (172.800 s)
 - Servidores de .rediris.es: 1 día (86.400 s)
 - IP de `www.rediris.es`: 2 horas (7.200 s)
- 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

<code>www.google.es.</code>	102	IN	A	173.194.41.248
<code>www.google.es.</code>	102	IN	A	173.194.41.255
<code>www.google.es.</code>	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:** tiene la copia oficial de la BD en disco
 - **Secundarios:** obtienen la BD del primario a través de la red mediante una operación de transferencia de zona
 - 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
- **No-recursive:** Cuando no disponen el registro de la consulta, devuelven una referencia al servidor de nombres que puede tenerlo
 - Los servidores autoritativos suelen ser no-recursive (y deben serlo)
- **Recursive:** Resuelven cada referencia hasta devolver la respuesta al cliente
 - En la configuración de los clientes deben usarse servidores recursive (fichero `/etc/resolv.conf`)

La Base de Datos de DNS

- Ficheros 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 fichero con registros, permite mantener separados los registros de datos en diferentes ficheros
 - \$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 almacenar 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`)

Contacto en notación `user.host.` → `hostmaster@example.com`

Servidor primario 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 se incrementa cuando se actualiza cualquier registro de la zona

Temporizadores: secundario actualiza cada ref s, reintenta cada ret s, sirve el dominio ex s si no hay primario y establece TTL de respuestas negativas a nx s

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)

Nombre del registro anterior (example.com en SOA)

The diagram shows a DNS record for a subdomain. A box labeled 'sub' has an arrow pointing to the 'sub' part of the record. A box labeled 'Nombre del registro anterior (example.com en SOA)' has an arrow pointing to the first NS record. A box labeled '"." al final para los FQDN' has an arrow pointing to the trailing dot of the first NS record.

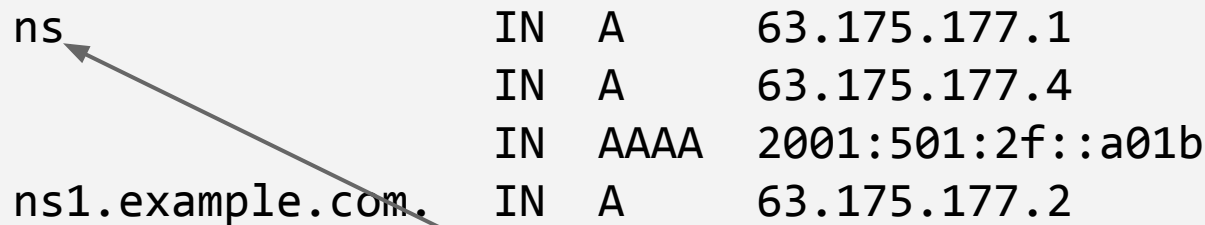
```
sub NS ns.example.com.  
NS ns1.example.com.  
NS ns-ha.example.com.  
NS ns.sub.example.com.  
NS ns.example.com.
```

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

La Base de Datos de DNS: Registros A y PTR

- El registro Address (**A** para IPv4 y **AAAA** para IPv6) es la base de DNS, ya que proporciona 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.

- 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**) especifica el servidor de correo de un dominio
- Indica cómo se deben encaminar los mensajes de correo electrónico de acuerdo con SMTP (*Simple Mail Transfer Protocol*)
- Un registro MX contiene un nombre de dominio

Prioridad, valores menores son más prioritarios

example.com.	IN	MX	10	mail
	IN	MX	20	mail2.example.com.

MTA con e-mail a usuario@example.com
usará mail.example.com (más prioritario)

La Base de Datos de DNS: Registro CNAME

- El registro Canonical Name (**CNAME**) define el nombre canónico de un nombre de dominio, lo que permite definir un *alias* para el nombre canónico
- Un registro definido por un CNAME no puede tener otros registros
- Los registros MX y NS no pueden apuntar a un CNAME

- ucm.es. es el nombre canónico de informatica.ucm.es.
- informatica.ucm.es. es un alias de ucm.es.

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

Se proporciona la dirección del 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
- Ficheros de configuración:
 - `named.conf`, que especifica las configuración del servidor (tipo, control de acceso...)
 - Ficheros de texto con la BD de la zona

Ejemplos de Preguntas Teóricas

Respecto a las direcciones IP, el servicio de nombres de dominio (DNS)...

- ☐ Establece un dominio específico para buscar su nombre de dominio asociado.
- ☐ DNS solo maneja la traducción de nombres de dominio en IP.
- ☐ Solo permite las búsquedas inversas para los TLDs (*top level domains*).

Los servidores autoritativos de una base de datos DNS...

- ☐ Guardan los resultados de las búsquedas realizadas.
- ☐ Suelen ser recursivos.
- ☐ Representan oficialmente a la zona.

¿De qué tipo debe ser el registro con nombre de dominio 2.1.96.147.in-addr.arpa.?

- ☐ A.
- ☐ PTR.
- ☐ CNAME.