Bloque II: El nivel de aplicación

Tema 4: Aplicaciones no orientadas a conexión

Índice

- Bloque II: El nivel de aplicación
  - Tema 4: Aplicaciones no orientadas a conexión
    - DNS
      - Introducción
      - Dominios DNS
      - Mensajes DNS
      - Peticiones DNS

- **Referencias**
  - Capítulo 2 de “Redes de Computadores: Un enfoque descendente basdado en Internet”. James F. Kurose, Keith W. Ross. Addison Wesley, 2ª edición. 2003.
  - Capítulo 14 de “TCP/IP Illustrated, Volume 1: The Protocols”, W. Richard Stevens, Addison Wesley, 1994.

DNS

- Domain Name System
- Base de datos distribuida utilizada por TCP/IP que hace la correspondencia entre nombres de máquinas y direcciones IP, y proporciona información de enrutamiento para e-mail.
- Especificaciones: RFC 1034 (conceptos) y RFC 1035 (implementación y especificación).
- Se implementa sobre UDP, aunque puede utilizar también TCP.
- Cada organización mantiene su propia base de datos de información.
  - Mantiene un servidor que otros sistemas (clientes) a través de Internet pueden consultar.
- DNS proporciona el protocolo que permite a los clientes y servidores comunicarse.

Pre-DNS: Fichero hosts

- Su finalidad es facilitar el manejo de direcciones IP.
- Antiguamente se utilizaba y se utiliza en Unix el fichero "/etc/hosts":
  - Centralizado en un servidor con la relación de todos los nombres de forma exhaustiva
  - Copias periódicas a los hosts locales
- Inconvenientes: poco escalable, inconsistente con las copias locales y facilidad para nombres duplicados.
- En Windows, se encuentra en c:/windows/…/hosts
- El fichero "hosts" puede servir para una solución simple en una red local donde no tengan configurado un servidor DNS.
- Ejemplo de una entrada:
- 38.25.63.10 x.acme.com # host cliente x

DNS: Introducción

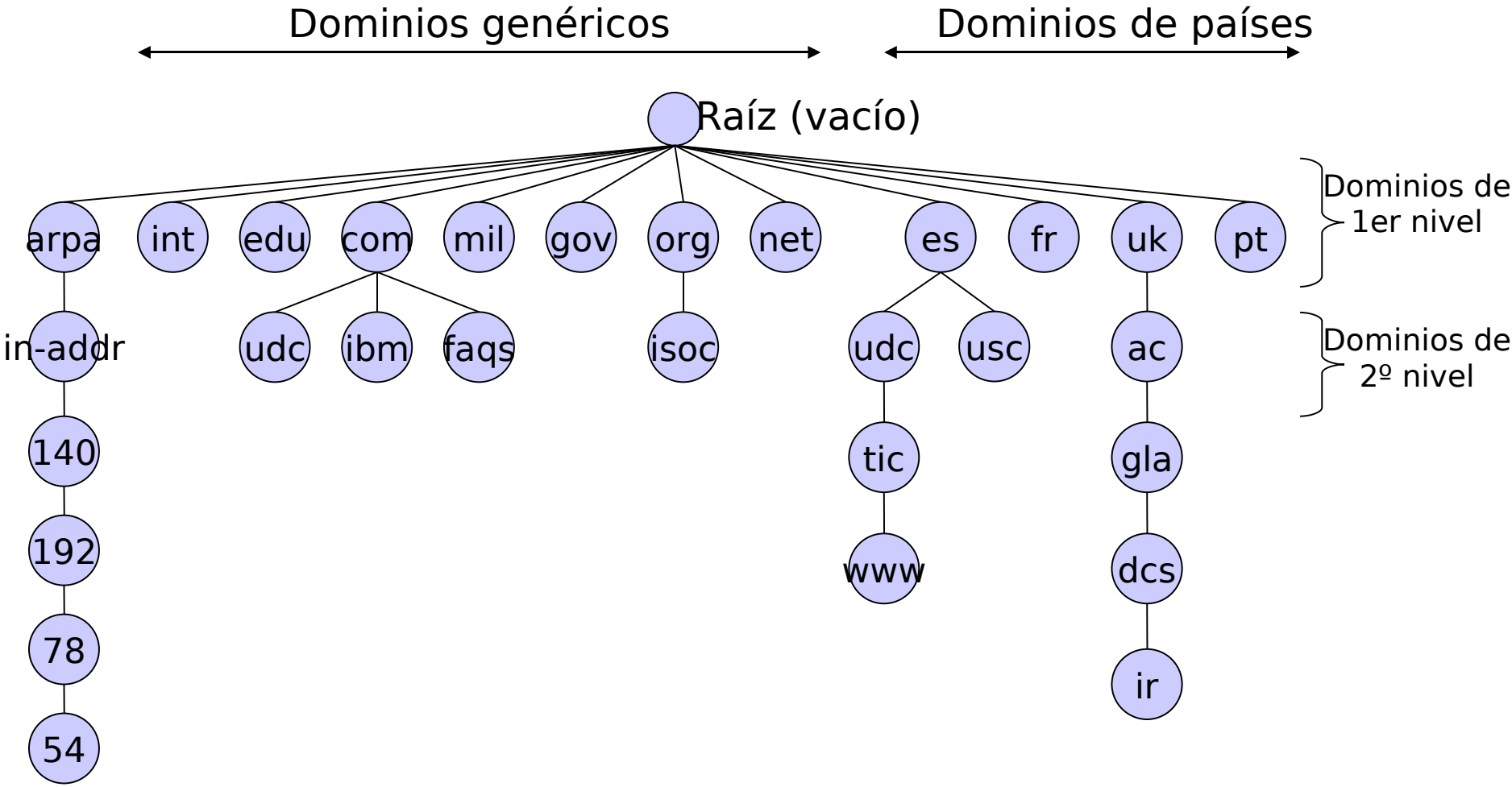
- Las consultas al DNS son realizadas por los clientes a través de las rutinas de resolución (“resolver”) ➔ Estas funciones son llamadas en cada host desde las aplicaciones de red.
- Las funciones del “resolver” sirven para hacer peticiones e interpretan las respuestas de los servidores de DNS.
- El resolver se comunica con uno o más servidores para hacer el mapeo nombre-dirección IP.
  - Antes de enviar un datagrama UDP o establecer una conexión es necesario obtener una dirección IP.
- Ventajas:
  - Desaparece la sobrecarga en la red y en los hosts ➔ Información distribuida por toda la red (BdD distribuida).
  - No hay duplicidad de nombres: cada dominio es controlado por un único administrador. Son posibles nombres iguales en dominios diferentes.
  - Consistencia de la información: la información que está distribuida es actualizada automáticamente sin intervención de ningún administrador.

Nombres de dominios

- Nombre de dominio: cadena de caracteres de menos de 255 caracteres, formada por etiquetas separadas por puntos organizadas de forma jerárquica o por niveles.
  - Cada etiqueta inferior a 63 caracteres.
  - El nivel superior es el de más a la derecha.
  - No se distinguen mayúsculas y minúsculas (esto no se aplica a la parte izquierda de @ en las direcciones de correo).
- Ejemplo: www.tic.udc.es
  - Dominio de primer nivel: “es.”
  - Dominio de segundo nivel: “udc.es.”
  - Dominio de tercer nivel: “tic.udc.es.”

Nombres de dominios

- Organización jerárquica del DNS

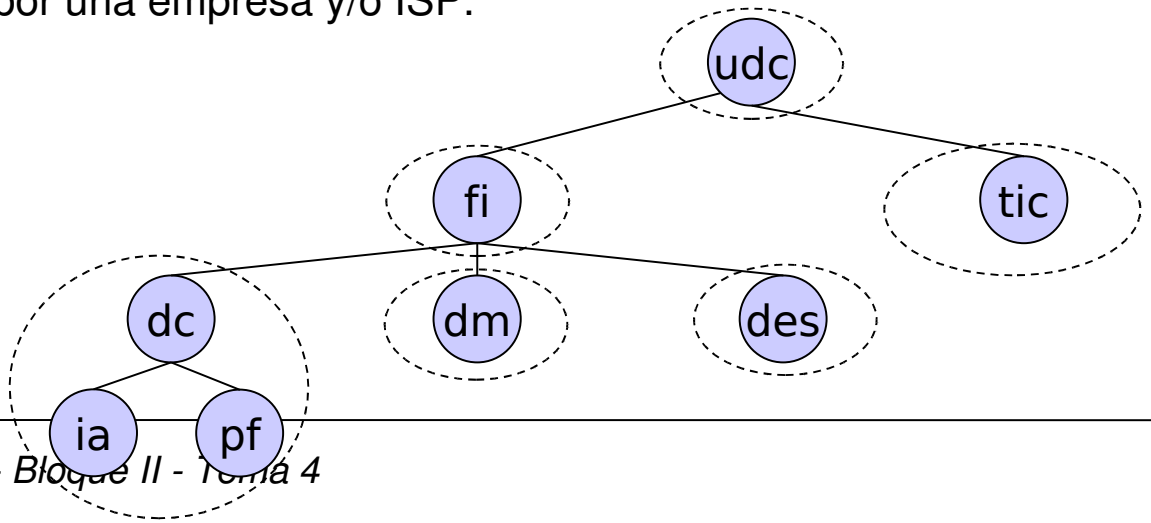


Nombres de dominios

- Dominios de primer nivel:
  - arpa: dominio especial utilizado para el mapeo de direcciones IP a nombres de máquina.
  - Dominios genéricos: división en función del tipo de organización
    - Dominios de 3 caracteres
  - Dominios geográficos: división por países
    - Dominios de 2 caracteres
- Dominios absolutos: finalizan con un ".".
  - Fully Qualified Domain Name (FQDN)
  - Por ejemplo: www.tic.udc.es.
  - Si el dominio no finaliza con un punto ➔ Relativo y necesita completarse.
    - Si el nombre consiste en 2 ó más etiquetas ➔ Se puede considerar absoluto
    - En otro caso, se añade un nombre de dominio a la derecha.

Zonas y dominios

- El árbol de nombres de una organización se compone de una o más zonas:
  - Una zona es una parte contigua del árbol de nombres que se administra como una unidad.
- Cada organización que posee un nombre de dominio es responsable del funcionamiento y mantenimiento de los servidores de nombres.
  - Esta área de influencia se llama **zona de autoridad**.
- En cada zona existe un administrador local, que a su vez puede delegar en otros administradores.
  - Por ejemplo, “udc.es.” delega en el Dpto. TIC para gestionar el dominio “tic.udc.es.” para asignar nombres.
- La solicitud de registro se realiza a una autoridad competente, por ejemplo, InterNIC (http://www.internic.net/) es una autoridad de registro.
- Otra opción para solicitar un dominio, es contactar con los servicios ofrecidos por una empresa y/o ISP.



Servidores DNS

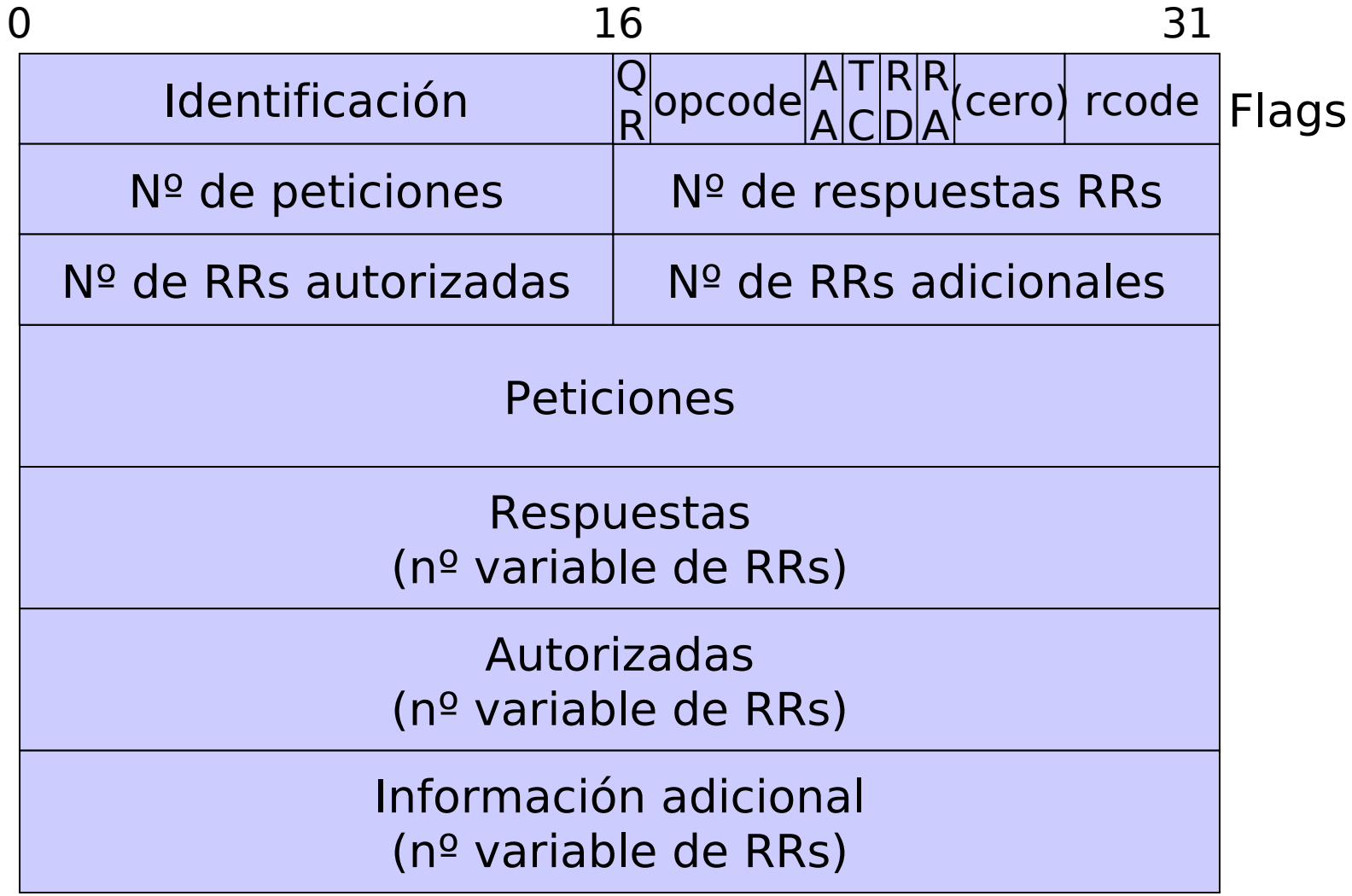
- Los servidores DNS tienen información completa para una zona de autoridad.
- La zona de autoridad abarca al menos un dominio, pudiendo incluir dominios de nivel inferior y tendrá normalmente un servidor de nombres "**primario**".
  - Los dominios de nivel inferior se pueden delegar en otros servidores locales.
- Según las características de la zona, los servidores DNS se pueden clasificar en: primarios y secundarios.
- Primarios (Primary Name Servers): Almacenan la información de su zona en una base de datos local (almacenamiento en disco).
  - Son responsables de mantener la información actualizada y cualquier cambio debe ser notificado a este servidor.
  - Cada zona sólo tendrá un servidor primario.
- Secundarios (Secundary Name Servers): Son aquellos que obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona.
  - El secundario obtiene la información del primario regularmente ➔ Transferencia de zona.
  - Cada zona podrá tener uno o más servidores secundarios (tolerancia a fallos).
- Servidores raíz (root name servers): conocen el nombre y dirección IP de todos los servidores de los dominios de primer nivel.
  - Cada servidor primario conoce a los servidores raíz.
  - Cuando un servidor primario no puede resolver una correspondencia contacta con un servidor raíz, que le devuelve el servidor de primer nivel a contactar, y así sucesivamente.

Cliente DNS

- En las máquinas cliente, las aplicaciones hacen uso del “resolver” cada vez que deben resolver una dirección IP.
- El resolver se encarga de:
  - Interrogar al servidor DNS
  - Interpretar las respuestas que pueden ser registros de recursos (RRs) o errores.
  - Devolver la información al programa que realiza la petición al cliente DNS.
- Toda esta comunicación se realiza mediante el protocolo DNS.

- ¿Caché en el cliente o en el servidor?
  - En el servidor, ¿por qué?

Mensaje DNS

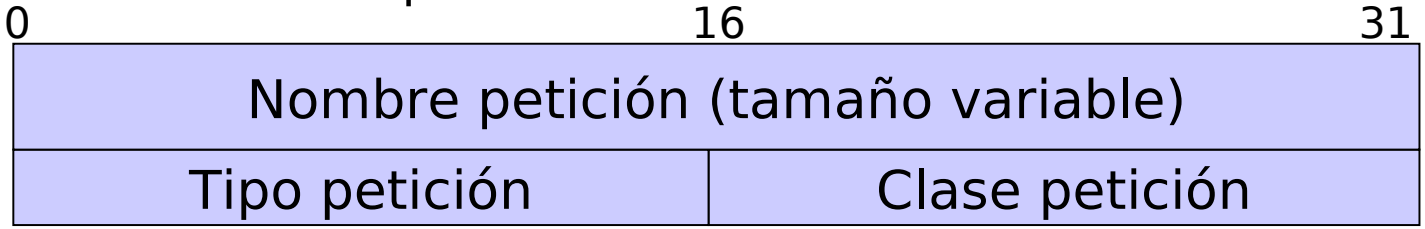

0
16
31
Identificación
QR
opcode
AA
TC
RD
RA
(cero)
rcode
Flags
Nº de peticiones
Nº de respuestas RRs
Nº de RRs autorizadas
Nº de RRs adicionales
Peticiones
Respuestas
(nº variable de RRs)
Autorizadas
(nº variable de RRs)
Información adicional
(nº variable de RRs)

Mensaje DNS

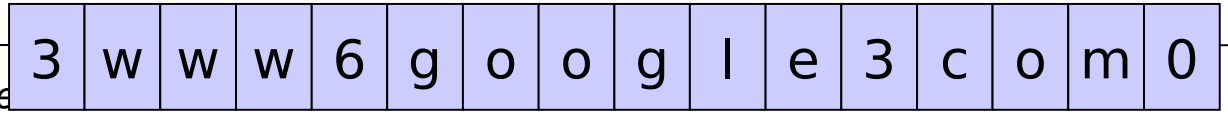
- Identificación: enviado por el cliente y devuelto por el servidor.
  - Permite asociar peticiones y respuestas
- Flags:
  - QR (1 bit): 0 ➔ Peticion /1 ➔ Respuesta
  - opcode (4 bits):
    - 0 ➔ Petición standard (nombre -> dirección IP)
    - 1 ➔ Petición inversa (dirección IP -> nombre)
    - 2➔ Solicitud de estado del servidor
  - AA (1 bit): Authoritative Answer ➔ El servidor es “autoritativo” para el dominio de la consulta.
  - TC (1 bit): Truncated ➔ Con UDP, la respuesta es mayor de 512 bytes, y sólo se han enviado los primeros 512 bytes.
  - RD (1 bit): “Recursion Desired”
    - 1 ➔ Consulta recursiva: el servidor de nombres debe interrogar recursivamente a otros servidores hasta obtener la respuesta.
    - 0 ➔ Consulta iterativa: si el servidor de nombres no dispone de una respuesta autoritativa, responde con una lista de servidores de nombres.
  - RA (1 bit): “Recursion Available” -> Si 1, el servidor anuncia que soporta recusividad.
  - Cero (3 bits)
  - rcode (4 bits): contiene un código de respuesta
    - 0 ➔ Sin errores
    - 3 ➔ Error de nombre: devuelto por un servidor autoritativo para un dominio e implica que no existe la máquina de la petición.

Mensaje DNS

- Nº de peticiones, nº de RRs, nº de RRs autorizadas y nº de RRs adicionales: número de entradas en los 4 campos adicionales.
  - En una consulta el número de peticiones es 1 normalmente, y 0 el resto.
  - En una respuesta, el número de RRs es 1, y los otros dos pueden ser distintos de cero.
- Formato del campo Petición:



  - Nombre petición: secuencia de una o más etiquetas. Cada etiqueta es precedida por un byte que indica el número de bytes (caracteres) que la componen.
    - El nombre finaliza con un byte a cero.
    - Cada byte está entre 0 y 63 (limitación etiquetas a 63 caracteres).

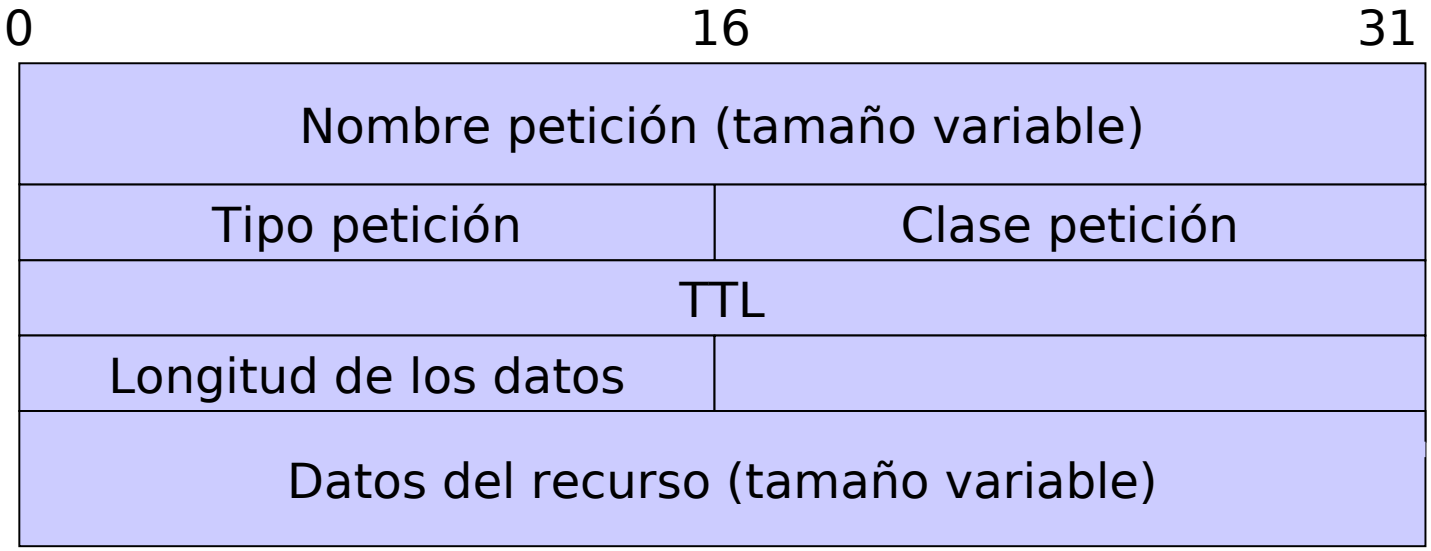


Peticiones

- Tipo de petición: especifica el tipo de petición/respuesta realizado.
  - A: dirección IP (petición estándar)
  - NS: solicita los servidores de dominio autorizados para un dominio
  - CNAME: nombre canónico (alias)
  - PTR: petición inversa
  - HINFO: información de la máquina
  - MX: registro de correo electrónico.
  - WKS: lista los servicios de las aplicaciones disponibles en el host (Well Known Services)
  - */ANY: solicitud de toda la información.

Registro de Recursos (RR)

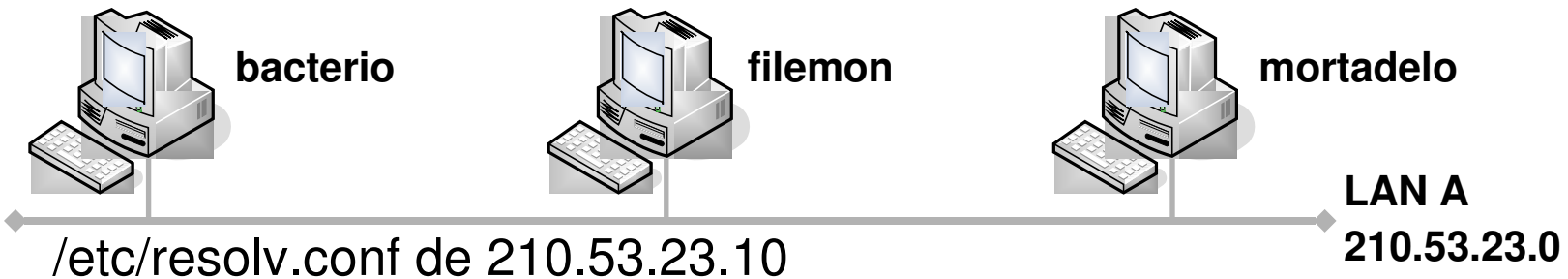
- Formato de los campos RRs



- Nombre de Petición, tipo y clase: son los mismos que los incluidos en la petición.
- TTL: número de segundos que se puede almacenar en cache (normalmente 2 días).
- Longitud datos: tamaño del campo “Datos del recurso”. Depende del tipo de petición:
  - A ➔ La respuesta es una dirección IP de 4 bytes.
- Datos del recurso: respuesta del servidor
  - A ➔ Dirección IP
  - PTR ➔ Nombre de máquina

DNS: Petición standard

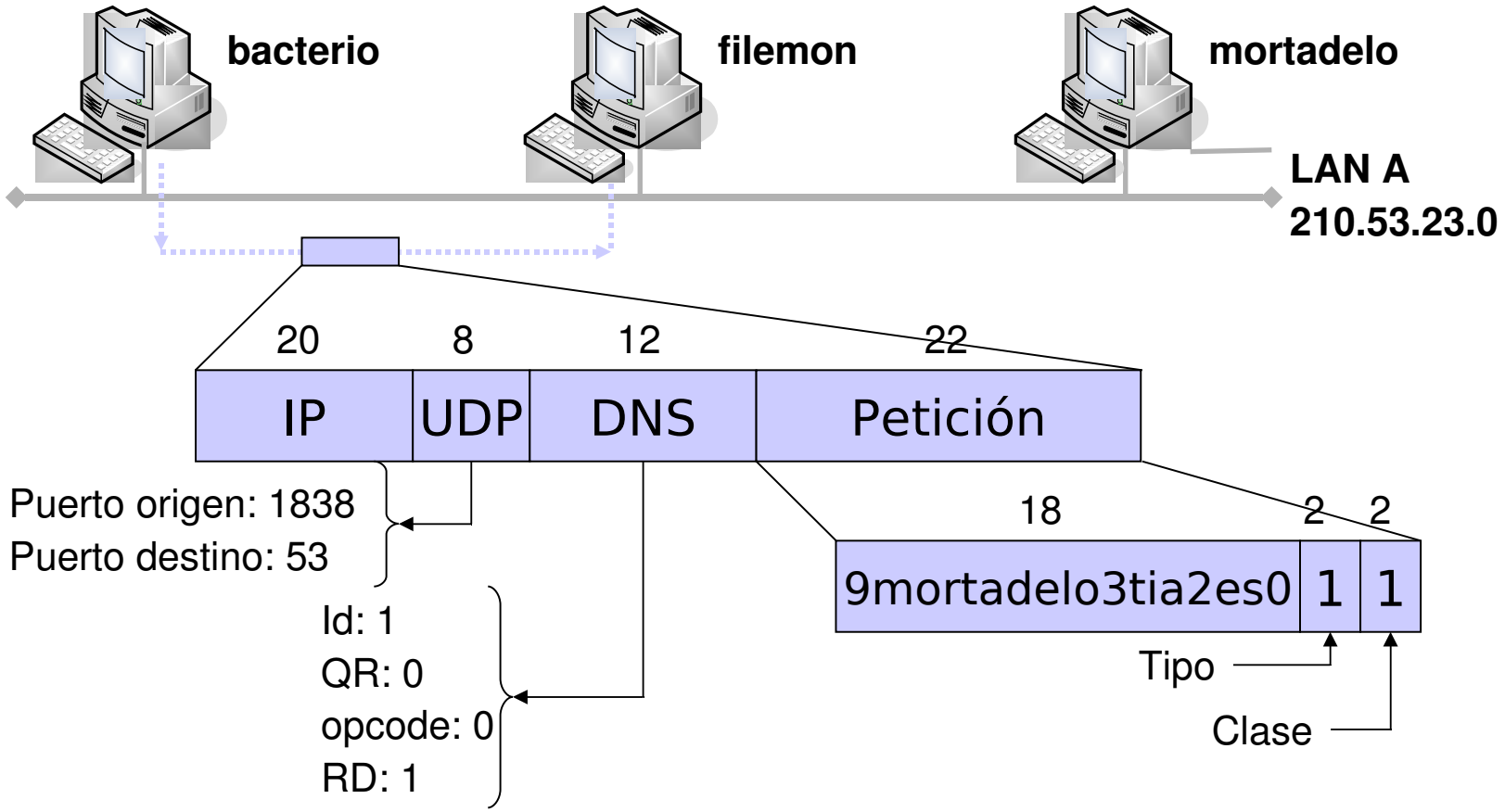
- bacterio % telnet mortadelo daytime



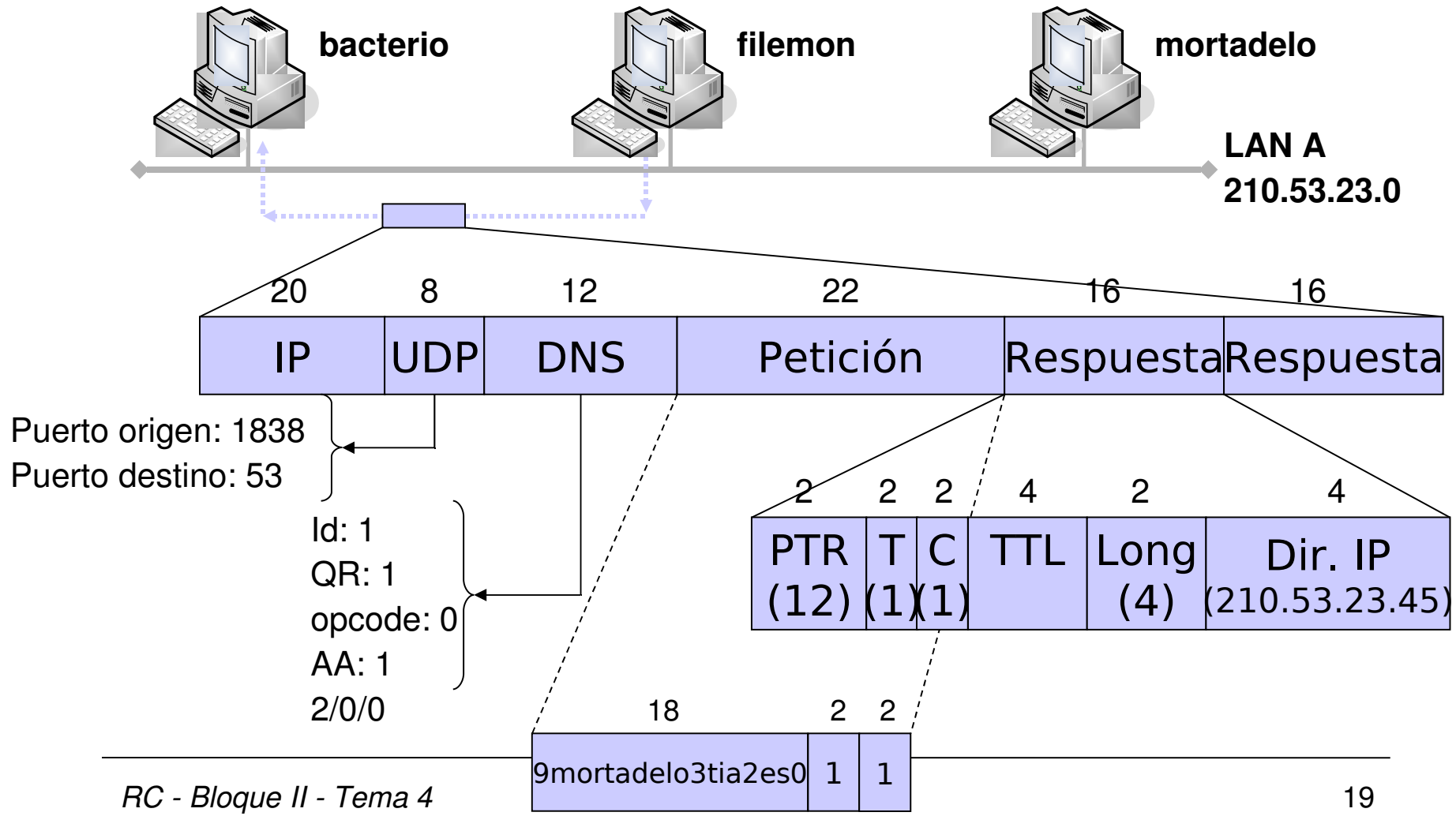
- /etc/resolv.conf de 210.53.23.10
  - nameserver 210.53.23.15
  - domain tia.es

- Resolver: parte del cliente, que se conecta con el servidor DNS (antes del telnet) para obtener la dirección IP.
  - Si el nombre no está completo ➔ Completar con el dominio: mortadelo.tia.es
- El resolver envía una consulta DNS al servidor DNS (210.53.23.15) solicitando la IP de “mortadelo.tia.es”
- El servidor DNS responde con la/s IP/s de la máquina.

DNS: Petición standard



DNS: Petición standard



DNS: Petición standard

- Para ahorrar espacio en las respuestas se utiliza un puntero a la petición. ¿Cómo?
- En las etiquetas del nombre del host, el contador (entre 0 y 63) se convierte en un puntero poniendo a “11” los dos primeros bits:
  - Puntero de 16 bits o contador de 8 bits.
- Puede aparecer en cualquier posición del nombre, no sólo al principio.

DNS: Petición recursiva

- Petición recursiva: www.udc.es (desde fuera de la Universidad)

2. El servidor local es el responsable de resolver la pregunta, aunque para ello tenga que reenviar la pregunta a otros servidores.
   - Si se ha solicitado información local, el servidor extrae la respuesta de su propia base de datos.
   - Si es sobre un ordenador externo, el servidor comprueba su caché. Si no tiene dirección IP entonces formulará una pregunta iterativa al servidor del dominio raíz.

- El servidor del dominio raíz no conoce la dirección IP solicitada ➔ Devuelve la dirección del servidor del dominio es.
- El servidor local reenvía la pregunta iterativa al servidor del dominio es. que tampoco conoce la dirección IP preguntada ➔ Conoce la dirección del servidor del dominio udc.es.
- El servidor local vuelve a reenviar la pregunta iterativa al servidor del dominio udc.es. Conoce la dirección IP de www.udc.es y devuelve esta dirección al servidor local.
- El servidor local se la reenvía al ordenador que lo solicitó, al mismo tiempo que la almacena en la propia caché.

DNS: Petición iterativa

- Petición iterativa: www.udc.es (desde fuera de la Universidad)

2. El resolver es el encargado de resolver la petición, preguntando a otros servidores.
3. El resolver envía la petición al servidor de nombres local, que contesta con la dirección del servidor del dominio raíz.
   - Esta dirección se envía al resolver del host local.

- El servidor del dominio raíz no conoce la dirección IP solicitada ➔ Devuelve la dirección del servidor del dominio es.
- El resolver reenvía la pregunta iterativa al servidor del dominio es. que tampoco conoce la dirección IP preguntada ➔ Conoce la dirección del servidor del dominio udc.es.
- El resolver reenvía la pregunta iterativa al servidor del dominio udc.es. Conoce la dirección IP de www.udc.es y devuelve esta dirección al resolver.

DNS: Petición inversa

- Pointer queries (PTR)
- Se utiliza un dominio especial: in-addr.arpa.
- Un cliente DNS necesita conocer el nombre de dominio asociado a la dirección IP 210.53.23.45
  - Petición inversa a 45.23.53.210.in-addr.arpa.
- Es necesario invertir la dirección IP, ya que los nombres de dominio son más genéricos por la derecha (al contrario que las direcciones IP).

DNS: Petición MX

- ¿Cómo se conoce el servidor de correo a partir de una dirección de correo?
- fidel@udc.es ➔ Petición DNS tipo MX para el dominio udc.es

```
> set type=MX
> udc.es
Servidor:  zipi.udc.es
Address:  193.144.48.30

udc.es  MX preference = 20, mail exchanger = mail.rediris.es
udc.es  MX preference = 10, mail exchanger = unica.udc.es
udc.es  nameserver = zape.udc.es
udc.es  nameserver = zipi.udc.es
udc.es  nameserver = chico.rediris.es
udc.es  nameserver = ineco.nic.es
udc.es  nameserver = sun.rediris.es
unica.udc.es    internet address = 193.147.41.3
mail.rediris.es internet address = 130.206.1.11
sun.rediris.es  internet address = 130.206.1.2
zape.udc.es     internet address = 193.144.52.2
zipi.udc.es     internet address = 193.144.48.30
chico.rediris.es        internet address = 130.206.1.3
ineco.nic.es    internet address = 194.69.254.2
```

DNS: UDP o TCP

- Los mensajes DNS se envían mediante UDP, aunque se puede utilizar TCP:
  - Si deben transmitir más de 512 bytes, la respuesta vendrá truncada (Flag TC) y el cliente deberá establecer una conexión TCP para esa petición.
  - Las transferencias de zona (actualizaciones periódicas de servidores secundarios) se hacen también con TCP.
  - DNS es una aplicación que usualmente no está limitada a una LAN ➔ Al usar preferentemente UDP exige que los clientes tengan un buen algoritmo de timeout y retransmisiones.

- Comando nslookup (Windows y UNIX),
- Comando hosts y fichero /etc/resolv.conf (UNIX)
- Servidores DNS = “named”

DNS: nslookup

```
C:\Documents and
    Settings\Fidel>nslookup
Servidor predeterminado:  zipi.udc.es
Address:  193.144.48.30

> www.tic.udc.es
Servidor:  zipi.udc.es
Address:  193.144.48.30

Nombre:  www.tic.udc.es
Address:  193.147.36.135

> www.google.com
Servidor:  zipi.udc.es
Address:  193.144.48.30

Respuesta no autoritativa:
Nombre:  www.google.akadns.net
Addresses:  66.102.11.99,
    66.102.11.104
Aliases:  www.google.com

> set type=CNAME
> www.google.com
Servidor:  zipi.udc.es
Address:  193.144.48.30

Respuesta no autoritativa:
www.google.com  canonical name =
    www.google.akadns.net

google.com      nameserver =
    ns2.google.com
google.com      nameserver =
    ns3.google.com
google.com      nameserver =
    ns4.google.com
google.com      nameserver =
    ns1.google.com
ns1.google.com  internet address =
    216.239.32.10
ns2.google.com  internet address =
    216.239.34.10
ns3.google.com  internet address =
    216.239.36.10
ns4.google.com  internet address =
    216.239.38.10
```

DNS: nslookup

```
> set type=PTR
> 198.133.219.25
Servidor:  zipi.udc.es
Address:  193.144.48.30

Respuesta no autoritativa:
25.219.133.198.in-addr.arpa     name =
      www.cisco.com

219.133.198.in-addr.arpa
      nameserver = ns1.cisco.com
219.133.198.in-addr.arpa
      nameserver = ns2.cisco.com
ns1.cisco.com   internet address =
      128.107.241.185
ns2.cisco.com   internet address =
      64.102.255.44
>
```

```
> set type=NS
> udc.es
Servidor:  zipi.udc.es
Address:  193.144.48.30

udc.es  nameserver = zape.udc.es
udc.es  nameserver = zipi.udc.es
udc.es  nameserver = chico.rediris.es
udc.es  nameserver = ineco.nic.es
udc.es  nameserver = sun.rediris.es
sun.rediris.es  internet address =
      130.206.1.2
zape.udc.es     internet address =
      193.144.52.2
zipi.udc.es     internet address =
      193.144.48.30
chico.rediris.es        internet address =
      130.206.1.3
ineco.nic.es    internet address =
      194.69.254.2
>
```

DNS: nslookup

```
> set q=any
> udc.es
Servidor:  zipi.udc.es
Address:  193.144.48.30

udc.es
        primary name server = zipi.udc.es
        responsible mail addr =
      rede.udc.es
        serial  = 2004101802
        refresh = 86400 (1 day)
        retry   = 172800 (2 days)
        expire  = 2592000 (30 days)
        default TTL = 172800 (2 days)
udc.es  nameserver = zape.udc.es
udc.es  nameserver = zipi.udc.es
udc.es  nameserver = chico.rediris.es
udc.es  nameserver = ineco.nic.es
udc.es  nameserver = sun.rediris.es
udc.es  MX preference = 20, mail
      exchanger = mail.rediris.es
udc.es  MX preference = 10, mail
      exchanger = unica.udc.es
udc.es  text =
        "v=spf1 mx -all"
udc.es  internet address = 193.144.63.4
sun.rediris.es  internet address =
      130.206.1.2
zape.udc.es     internet address =
      193.144.52.2
zipi.udc.es     internet address =
      193.144.48.30
chico.rediris.es        internet address =
      130.206.1.3
ineco.nic.es    internet address =
      194.69.254.2
unica.udc.es    internet address =
      193.147.41.3
mail.rediris.es internet address =
      130.206.1.11
>
```