UNIVERSIDAD DE MÁLAGA

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

TEMA 3.1

Servidores DNS

"Domain Name System"

30 de octubre de 2018

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

Grado en Ingeniería Informática

DNS – Domain Name System

UNIVERSIDAD DE MÁLAGA

- Un SERVIDOR es un programa residente (está siempre ejecutándose) que permanece a la espera de las distintas peticiones que hacen otros programas llamados CLIENTES

- Dichas peticiones se realizan usando un PROTOCOLO, que no es más que un conjunto de reglas que rigen la comunicación entre dos entidades

- El concepto de DNS es similar al de una agenda telefónica, donde a cada nombre de persona se el asigna un número de teléfono

- Un servidor DNS asocia a cada nombre de máquina la dirección IP de dicha máquina

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

UNIVERSIDAD DE MÁLAGA

- DNS (Domain Name System) se define inicialmente en 1983 a través de los documentos RFC 882 y RFC 883.

- Posteriormente se revisa en 1987 con la publicación de los RFC 1034 y RFC 1035.

- DNS define una nomenclatura descentralizada y jerárquica que permite asociar a cada computadora conectada a Intenet un nombre único, inteligible y fácil de recordar.

- El OBJETIVO es facilitar la traducción del nombre de cualquier computadora conectada a Internet a la correspondiente dirección IP.

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

UNIVERSIDAD DE MÁLAGA

- Los nombres de las máquinas se forman como una secuencia de etiquetas separadas por puntos.

- La etiqueta que aparece más a la derecha es el dominio de alto nivel que implica una división de todas la máquinas en conjuntos que hacen referencia al tipo de organización (com, org, edu,…) o a su ubicación geográfica (es, uk,fr,…).

- Cada uno de estos dominios de alto nivel se divide en otros dominios de menor nivel (como ramas de un árbol)

- Estos dominios engloban conjuntos de máquinas más reducidos (dentro del dominio ".es" están uma.es, ugr.es,…)

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

- Cada etiqueta que se coloca a la izquierda de un nombre de dominio hace referencia a un subconjunto de dicho dominio.

- Distintos servidores DNS almacenan tablas nombre/IP relativas a cada de las partes de este “árbol” de dominios

- De esta forma la información se distribuye siguiendo el esquema jerárquico con el que se nombran las máquinas

- Dado un nombre de dominio, se coloca una última etiqueta a modo de prefijo (como www dentro de www.sci.uma.es) que hace referencia una máquina en concreto de la red que ofrece un servicio determinado.

LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

- Una de dichas máquinas será el servidor DNS de la red es el encargado de mantener la información necesaria para hacer la conversión nombre/IP de las máquinas de la red a la que pertenece. A esta red se le suele llamar “zona de autoridad”.

HAY TRES TIPOS DE SERVIDORES DNS:

- **MAESTRO o PRIMARIO**
- **ESCLAVO o SECUNDARIO**
- **LOCAL o CACHÉ**

- Los servidores **DNS maestro** almacenan de forma permanente la información necesaria para resolver (convertir de nombre de máquina a IP) solamente las peticiones referentes a la zona a la que solo ese servidor está autorizado, evitando la duplicidad de dicha información en otros servidores DNS maestros.

LENGUAJES Y
CIENCIAS DE LA
COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

UNIVERSIDAD DE MÁLAGA

- El administrador de la red irá añadiendo las entradas necesarias para resolver las peticiones asociadas a cada una de las computadoras que se vayan añadiendo a la red (los cambios se hacen solo en el DNS maestro)

- Es posible cambiar la IP de una computadora y seguir accediendo a la misma usando el mismo nombre de dominio, bastando tan solo una pequeña actualización de los ficheros pertinentes.

- Un segundo tipo, los servidores **DNS esclavos** mantienen una copia actualizada de la información del servidor DNS maestro asociado y pueden usarse para descargar de tráfico al DNS maestro, siendo posible un balanceo de carga

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

UNIVERSIDAD DE MÁLAGA

- Un tercer tipo de servidor, **DNS caché** , no tienen información permanente para resolver las peticiones.

- En realidad, se limitan recibir peticiones de los clientes y tratan de obtener la IP correspondiente preguntando a otros servidores DNS que tienen en una lista.

- A medida que van recibiendo respuestas, guardan en una caché temporal una copia de dicha información (que caduca pasado un tiempo) que podrá utilizar en otras peticiones evitando consultas externas, de forma que así se agiliza el proceso de resolución.

- Es común que un servidor DNS funcione a la vez como maestro y caché, o como esclavo y caché, o incluso es posible que sea maestro de una zona y esclavo de otra…

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

UNIVERSIDAD DE MÁLAGA

Cuando un cliente DNS solicita resolver un nombre de dominio y obtener una IP, se inicia el proceso

EXISTEN DOS MÉTODOS DE RESOLUCIÓN:

MÉTODO RECURSIVO

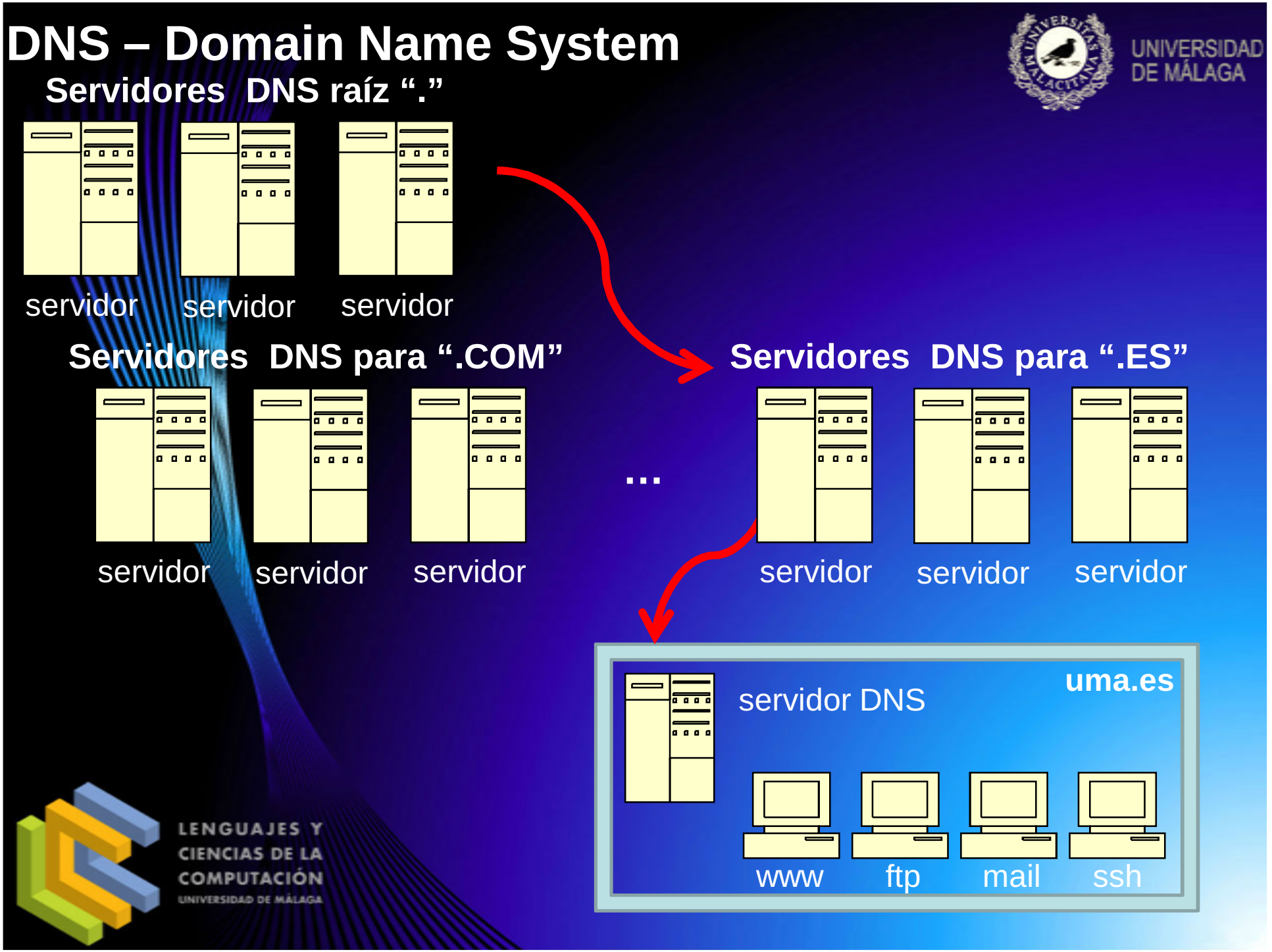
El cliente hace una única petición al servidor DNS y este último se encargará de hacer todo el proceso, lo que podría incluir otras peticiones a otros servidores DNS externos (si no tiene la información necesaria almacenada en su caché) o la información está caducada)

MÉTODO ITERATIVO

Siguiendo las distintas etiquetas que forman parte del nombre del dominio (p.e. www.uma.es) se hacen consultas sucesivas a distintos servidores DNS cada vez más específicos hasta obtener la IP de la máquina deseada.

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System



UNIVERSIDAD DE MÁLAGA

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

MÉTODO ITERATIVO

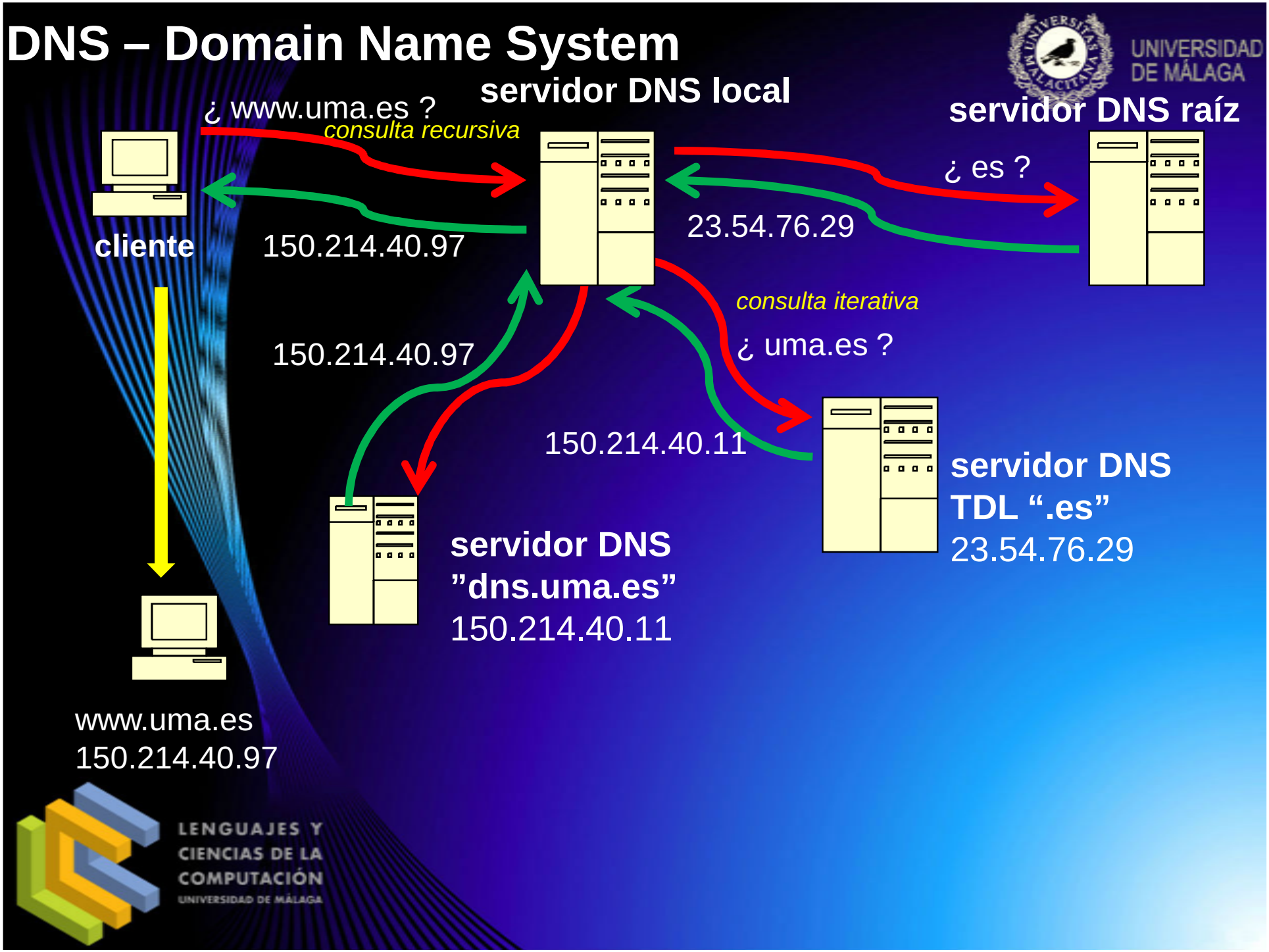
(p.e. para resolver www.uma.es)

1. Se pregunta al servidor DNS raíz por la IP del servidor DNS encargado del dominio de alto nivel es (.ES server)

2. Vamos a ese segundo servidor (.ES server) , y se le pregunta por el servidor DNS autorizado para resolver las IP de las máquinas de la red que indique el dominio de segundo nivel (en nuestro caso uma.es, de forma que obtenemos la IP del servidor DNS de la UMA)

3. Hacemos una tercera consulta a ese último servidor (servidor DNS de la UMA), que nos dará la IP de la máquina que se deseaba inicialmente (como resultado obtenemos la IP del servidor web de la red de la **UMA**)

DNS – Domain Name System



UNIVERSIDAD DE MÁLAGA

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

BIND: A “Domain Name System” Server

UNIVERSIDAD DE MÁLAGA

BIND es el servidor DNS más ampliamente utilizado
Actualmente casi todo el mundo usa la versión 9 (bind9)

BIND tiene 3 componentes:
-named: demonio que funciona a modo de servidor DNS
es el encargado de responder a las peticiones de los clientes
-librería resolutora: es el código que realiza la conversión de nombre de máquina a IP (o a la inversa) que a su vez lanza peticiones a otros servidores DNS de otras subredes. Se dispone de una lista de otros servidores DNS, de manera que si uno falla se llama al siguiente
-conjunto de herramientas de test y diagnóstico (como dig)

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

BIND – Instalación de BIND

UNIVERSIDAD DE MÁLAGA

Primero abriremos una consola con permisos de administrador:

```
# sudo -i
```

Actualizamos la base de datos de paquetes disponibles/versiones

```
# apt-get update
```

Instalamos el bind9 y su documentación

```
# apt-get –V install bind9 bind9-doc
```

(-V muestra más información)

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  bind9 bind9-doc
…
        Adding group `bind' (GID 135) ...
        Adding system user `bind' (UID 126) ...
        Adding new user `bind' (UID 126) with group `bind' …
```

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

BIND – Instalación de BIND

• El demonio bind está en la carpeta /etc/init.d

... y podemos iniciarlo, pararlo, reiniciarlo o ver su estado:

/etc/init.d/bind9 start | stop | restart | status

Por ejemplo:

/etc/init.d/bind9 start | stop | restart | status

bind9.service - BIND Domain Name Server

…

Active: active (running) since Fri 2018-11-02 21:21:04 CET

…

•También podemos comprobar que toda va bien usando el comando “rndc” con su opción “status”:

rndc status

version: BIND 9.10.3-P4-Ubuntu <id:ebd72b3>

boot time: Fri, 02 Nov 2018 20:21:04 GMT

…

server is up and running

BIND – Configurando las zonas

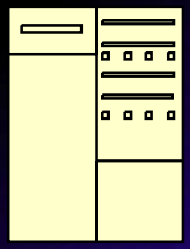
Un servidor DNS puede funcionar como MAESTRO para varios dominio de forma que tendremos que configurar varias zonas de autoridad por separado. Al registrar y pagar un dominio, se exige indicar la dirección IP del servidor DNS maestro capaz de resolver las IP de las computadoras del dominio

En el archivo /etc/bind/named.conf tiene la lista de todas las zonas que el servidor DNS administra, donde cada entrada contiene una referencia a un fichero específico para describir cada zona

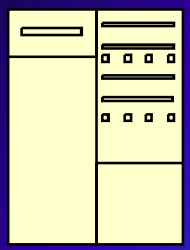
DNS – Domain Name System

cliente

resolv.conf
nameserver 150.214.57.7
nameserver 150.214.57.8



servidor DNS
primario
150.214.57.7

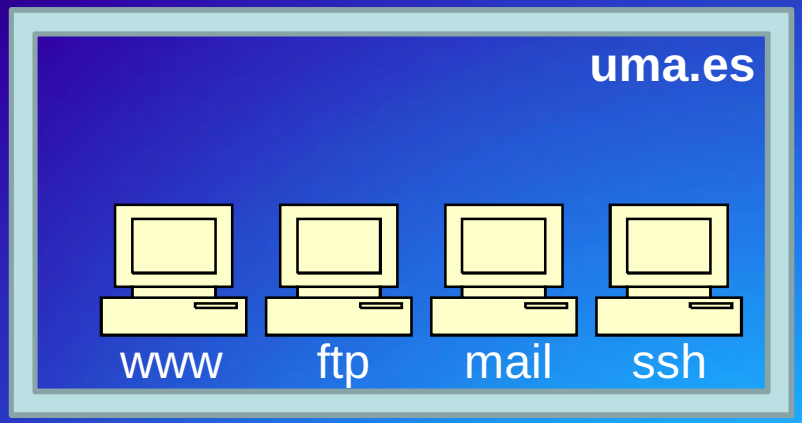


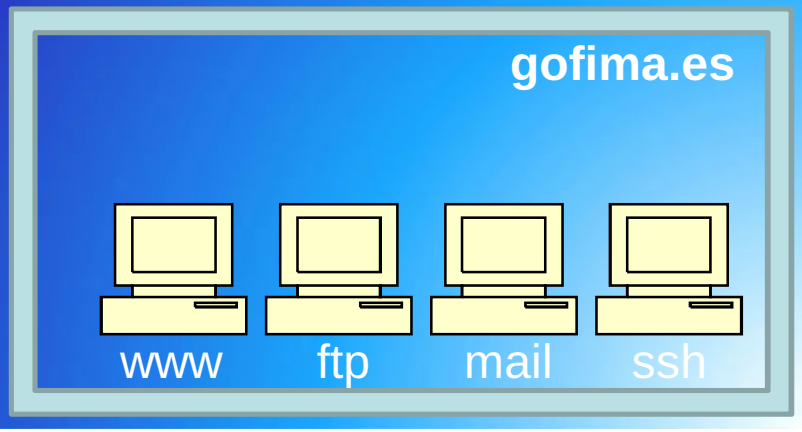
servidor DNS
secundario
150.214.57.8

named.conf
zone uma.es { … }
zone gofima.es { … }

uma.es

gofima.es





LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

UNIVERSIDAD DE MÁLAGA

named.conf

```
options {
        pid-file "/var/run/bind/run/named.pid";
        directory "/etc/bind";

  // query-source address * port 53; };
//  master nameserver config

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

zone “uma.es" {
   type master;
   file “uma.db";
};

zone “oceano.es" {
   type master;
   file “oceano.db";
};
```

fichero que tiene el PID del proceso named

directorio donde están los fichero de zona

indica el fichero que tiene las IP de los servidores DNS raíz

indica el fichero que tiene las IP de las máquinas del dominio *uma.es*

indica el fichero que tiene las IP de las máquinas del dominio *oceano.es*

named.conf (cont)

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

zone “57.214.150.in-addr.arpa" {
   type master;
   file “uma.rev";
};

zone “40.214.150.in-addr.arpa" {
   type master;
   file “oceano.rev";
};
```

fichero de conversión inversa para localhost

fichero de conversión inversa para zona uma.es

fichero de conversión inversa para zona oceano.es

CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

UNIVERSIDAD DE MÁLAGA

uma.db

@ IN SOA dns1.uma.es. michel.uma.es. (
2018110503; *serial-no*
28800; *refresh, segundos(8h)*
7200; *retry, segundos(2h)*
604800; *expiry, segundos(7d)*
86400);*minimum-TTL, segundos (1d)*
;
...

SOA(start of authority)- registro que especifica que el servidor es autorizado (maestro o esclavo)

configuración de la sincronización del DNS maestro con el esclavo/s

@ ***alias del nombre de la "uma.es"***
IN **indica el tipo de servidor DNS (IN=Internet)**
SOA ***tipo de registro***
dns.uma.es - nombre completo del servidor DNS
¡¡¡ Debe acabar en punto "." !!!
michel.uma.es - email del administrador
¡¡¡ la @ se cambia por "." y acaba en punto "." !!!

Nº serie = lo incrementamos cuando modificamos el fichero y asi sabe el esclavo que ha habido cambios
Refresh = cada cuánto tiempo el esclavo debe sondear al maestro
Retry = si la conexión falla, cuando debe volver a intentrlo
Expiry = en caso fallo de conecxión, indica el tiempo máximo que se pueden usar los datos
Minimum TTL =
tiempo de vida por defecto
(si no se indica lo contrario la duración de un registro es este tiempo)

DNS – Domain Name System

uma.db (cont)

...

@ IN NS dns1.uma.es. ;

@ IN NS dns2.uma.es. ; *dns secundario*

@ IN MX 10 buzon.uma.es.

@ IN MX 20 mail.uma.es.

www IN A 150.214.57.23

ftp IN A 150.214.57.31

ssh IN A 150.214.57.43

dns1 IN A 150.214.57.7

dns2 IN A 150.214.57.8

buzon IN A 150.214.57.11

mail IN A 150.214.57.12

Los registros de tipo NS sirven para identificar los servidores DNS de la zona (maestro y esclavos)

Los registros de tipo MX sirven para identificar los servidores de correo de la zona- 10 y 20 sirven para priorizar los servidores

Los registros A asocian a cada nombre de máquina una dirección IP concreta

www IN A 150.214.57.23

significa que al nombre de máquina

www.uma.es

se le debe asociar la IP

150.214.57.23

El punto al final del nombre de máquina es OBLIGATORIO => No ponerlo es error de sintaxis

El "punto y coma" al final es opcional ... solo es obligatorio si queremos poner un comentario

UNIVERSIDAD DE MÁLAGA

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

DNS – Domain Name System

uma.rev

@ IN SOA dns1.uma.es. michel.uma.es. (
2018110503; *serial-no*
28800; *refresh, segundos(8h)*
7200; *retry, segundos(2h)*
604800; *expiry, segundos(7d)*
86400);*minimum-TTL, segundos (1d)*
@ IN NS dns1.uma.es.
@ IN NS dns2.uma.es.

23 IN PTR www.uma.es.
31 IN PTR ftp.uma.es.
43 IN PTR ssh.uma.es.
7 IN PTR dns1.uma.es.
8 IN PTR dns2.uma.es.
11 IN PTR buzon.uma.es.
12 IN PTR mail.uma.es.

el registro SOA de la zona inversa es idéntico al de la zona directa

Solo ponemos los registros NS para indicar los nombres de los servidores DNS de la zona

Los registros PTR asocian a cada IP un nombre de máquina

23 IN PTR www.uma.es.
significa que a la IP
150.214.57.23
se le debe asociar el nombre de máquina
www.uma.es

El prefijo 150.214.57 …
viene del nombre de la zona en el fichero
/etc/bind/named.conf

UNIVERSIDAD DE MÁLAGA

COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

BIND – Aumentando la seguridad

UNIVERSIDAD DE MÁLAGA

-Indicamos que el directorio raíz del usuario bind es /var/lib/named
Editamos el fichero /etc/default/bind9
…y cambiamos la línea OPTIONS="-u bind"
… por OPTIONS="-u bind -t /var/lib/named/”

- Movemos los ficheros de definición de las zonas a su nueva ubicación /var/lib/named/etc/bind:
mv /var/cache/bind /var/lib/named/var/cache

- También movemos los ficheros con la base de datos temporal a su nueva ubicación /chroot/bind/var/cache/bind:
mv /var/cache/bind /var/lib/named/var/cache

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

BIND – Aumentando la seguridad

UNIVERSIDAD DE MÁLAGA

- Para que el bind se actualice correctamente es necesario crear un enlace simbólico en la carpeta /etc/bind que apunte a la nueva ubicación:

```
# ln -s  /var/lib/named/etc/bind   /etc/bind
```

- Bind usa los dispositivo /dev/null y /dev/random… y por lo tanto tenemos que crearlos en el nuevo entorno (no se pueden copiar)

```
# mknod /chroot/bind/dev/null c 1 3
# mknod /chroot/bind/dev/random c 1 8
```

- Cambiaremos el propietario de los ficheros movidos :

```
 # chown   bind:bind   /chroot/bind/{etc/bind/*,var/cache/bind/*}
```

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

BIND – Aumentando la seguridad

UNIVERSIDAD DE MÁLAGA

- Cambiamos los permisos de los dispositivos :

```
# chmod a=rw /var/lib/named/dev/{null,random}
```

-Configuramos el registro de eventos para que capture los eventos de bind9 en su nueva ubicación. Editamos /etc/deafult/sysklog

…y cambiamos SYSLOGD_OPTIONS=“ ”

… por SYSLOGD_OPTIONS=“-a /var/lib/named/dev/log”

- Iniciamos el demonio bind …

```
# /etc/init.d/bind9 start
 [ ok ] Starting bind9 (via systemctl): bind9.service.
```

• Para comprobar que bind está funcionando introducimos:

```
# /etc/init.d/bind9 status
```

Active: **Active (running)**

```
# rndc status
 version: BIND 9 …. Server is up and running.
```

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

UNIVERSIDAD DE MÁLAGA

Gracias por su atención

LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA