
SMIX M07

UF1: DNS

Marta Moreno

INDICE

1. Servicio DNS
2. DNS en Windows y Linux
3. Jerarquía de dominios en DNS
4. Dominio y Zona DNS
5. Servidores DNS
6. Consulta recursiva
7. Consulta iterativa

1. SERVICIO DNS

- ❖ El **Domain Name System** (DNS) es una base de datos distribuida y jerárquica que gestiona y mantiene información asociada a nombres de dominio en redes como Internet.
- ❖ Su uso más común es la asignación de nombres de dominio a direcciones IP de los nodos de Internet y la localización de los servidores de correo electrónico de cada dominio.
- ❖ DNS permite traducir los nombres de dominio (campus.stucom.com) a sus respectivas direcciones IP (82.223.162.102)

1. SERVICIO DNS

- ❖ Cuando queramos acceder a una máquina (Web, Ftp, Telnet, ...) en vez de recordar su @ IP, basta recordar el nombre del servidor:

`ftp ftp.smbserver.com → ftp 178.98.56.23`

`http://www.elmundo.es → http://132.56.23.22`

- ❖ DNS permite recordar fácilmente los nombres de todos los servidores conectados a Internet.
- ❖ El nombre es más fiable. La dirección numérica podría cambiar por muchas razones, pero no el nombre que identifica el servidor.

1. HISTORIA DNS

- ❖ En un inicio, SRI (ahora SRI International) alojaba un archivo llamado *HOSTS* que contenía todos los nombres de dominio conocidos (la mayoría de los sistemas operativos actuales todavía pueden ser configurados para revisar su archivo hosts).
- ❖ El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo *HOSTS* no resultara práctico.
- ❖ En 1983 apareció el primer sistema DNS, el cual ha ido evolucionado hasta el DNS moderno.

1. CARACTERÍSTICAS BÁSICAS DNS

- ❖ Es una base de datos jerárquica que contiene asociaciones de nombres de dominios a @ IP.
- ❖ Está formada por un conjunto de servidores distribuidos por todo Internet, en lugar de mantenerla centralizada en un único servidor.
- ❖ Sigue el paradigma cliente/servidor con nivel de transporte TCP/UDP y puerto 53.
- ❖ Usa un resolvedor ("resolver") que permite realizar las consultas a la bbdd.
- ❖ Utiliza un protocolo para intercambiar información de nombres.

2. DNS EN WINDOWS

C:\windows\system32\drivers\etc

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Éste es un ejemplo de archivo HOSTS usado por Microsoft TCP/IP para Windows.
#
# Este archivo contiene las asignaciones de las direcciones IP a los nombres de
# host. Cada entrada debe permanecer en una línea individual. La dirección IP
# debe ponerse en la primera columna, seguida del nombre de host correspondiente.
# La dirección IP y el nombre de host deben separarse con al menos un espacio.
#
# También pueden insertarse comentarios (como éste) en líneas individuales
# o a continuación del nombre de equipo indicándolos con el símbolo "#"
#
# Por ejemplo:
#
# 102.54.94.97    rhino.acme.com    # servidor origen
# 38.25.63.10    x.acme.com        # host cliente x
#
127.0.0.1    localhost
```

2. DNS EN LINUX

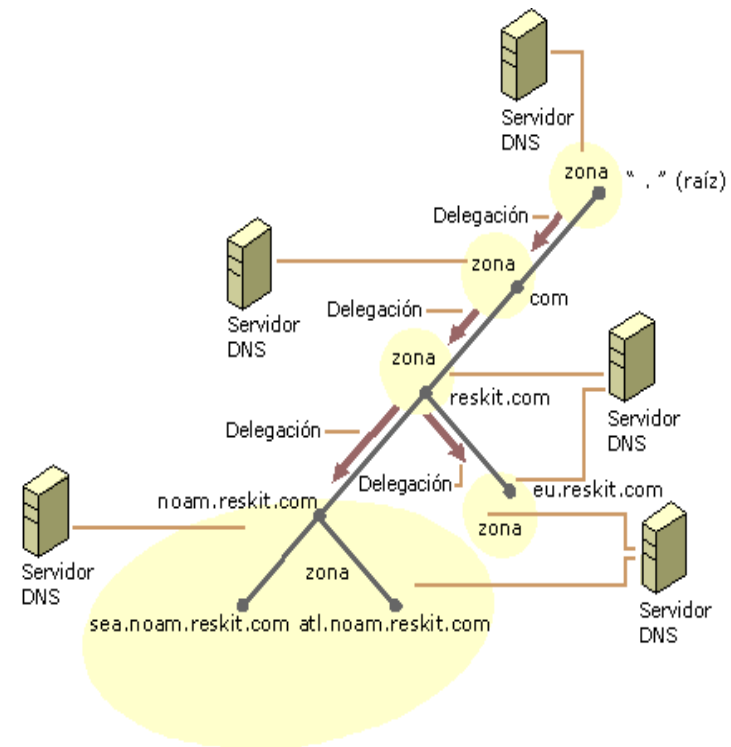
```
exemple# cat /etc/hosts
127.0.0.1 localhost
201.24.31.87 pc1.uu.vi.com pc1
201.24.31.105 pc2.uu.vi.com pc2
201.24.31.106 pc3.uu.vi.com pc3
```

```
exemple# cat /etc/resolv.conf
domain uu.vi.com
nameserver 201.24.31.3
nameserver 201.24.31.4
```

- ❖ Las aplicaciones que acceden al sistema DNS consultan inicialmente el fichero /etc/host donde está la correspondencia nombre-@IP.
- ❖ Si no puede resolver el nombre, entonces intenta contactar con un servidor DNS.
- ❖ En el fichero /etc/resolv.conf se guarda la @ IP de los servidores DNS primario y secundario y el dominio local

3. JERARQUIA DE DOMINIOS DNS

- ❖ La jerarquía de DNS esta organizada en dominios o zonas.
- ❖ Un dominio es un mecanismo de identificación utilizado en Internet.
- ❖ Es una rama en un árbol invertido llamado **espacio de nombres de dominio**

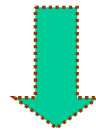


3. JERARQUIA DE DOMINIOS DNS

❖ Un nombre de dominio consiste en dos o más etiquetas, separadas por puntos (formato texto)

→ host.....Subdominio1.Dominio.TLD

→ rogent.ac.upc.edu



Fully Qualified Domain Name:

Cuando el nombre incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo



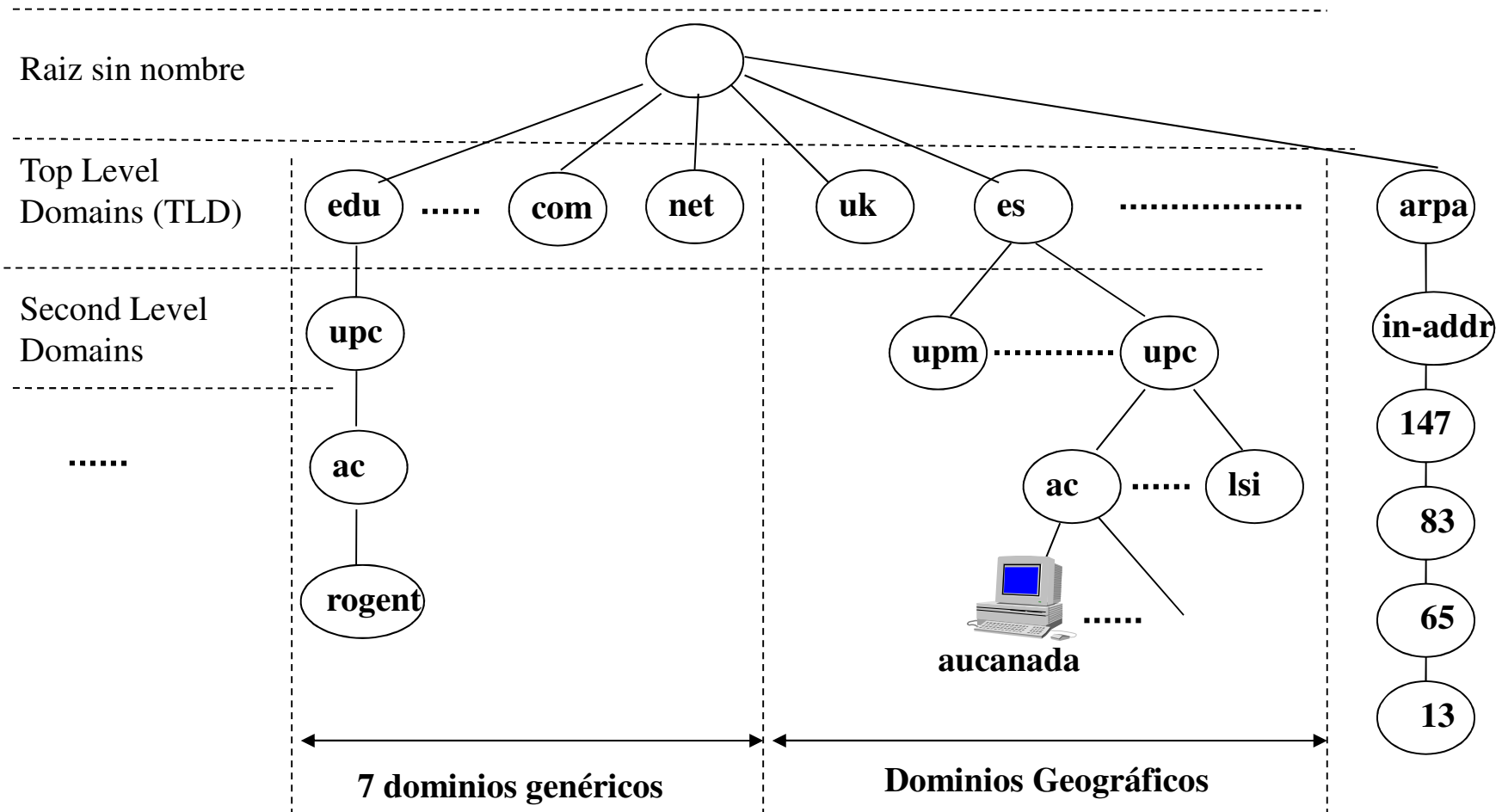
Dominio de nivel superior

(*Top Level Domain*)
Parte final de un dominio de Internet

3. JERARQUIA DE DOMINIOS DNS

- ❖ Cada etiqueta a la izquierda especifica una subdivisión o **subdominio**.
- ❖ El dominio y subdominio indican un conjunto de nombres que identifican a la organización:
 - "ac.upc" designa el departamento de Arquitectura de Computadores de la UPC.
- ❖ La parte más a la izquierda del dominio suele expresar el nombre de la máquina
- ❖ Las empresas deben **registrar** su nombre para que pase a ser su marca en Internet (problemas con marcas ya registradas)

3. JERARQUÍA DE DOMINIOS DNS



3. JERARQUÍA DE DOMINIOS DNS

Dominio raíz sin nombre

Los servidores raíz se encuentran al inicio de la jerarquía. Son los que responden cuando se busca resolver un dominio de 1º y 2º nivel.


Actualmente está formado por 13 servidores root-servers que tienen las direcciones de los TLD (top level domains):

a.root-server.net

b.root-server.net

...

m.root-server.net



Están distribuidos
por todo el mundo.

3. JERARQUÍA DE DOMINIOS DNS

Top Level Domain (TLD)

La IANA clasifica los TLDs en 3 clases dominios:

1) 7 dominios genéricos:

.com → comercial	.int → org. Internacional
.mil → militar	.org → org. no gubernamental
.edu → educación	.gov → institución gubernamental
.net → centros soporte de red	

Propuesta (de CORE) para ampliar el número de dominios genéricos: .firm, .shop, .info, .web, .nom, .arts, .rec

3. JERARQUÍA DE DOMINIOS DNS

Top Level Domain (TLD)

2) Dominios geográficos por países: .
es, .fr, .uk, .it, ...

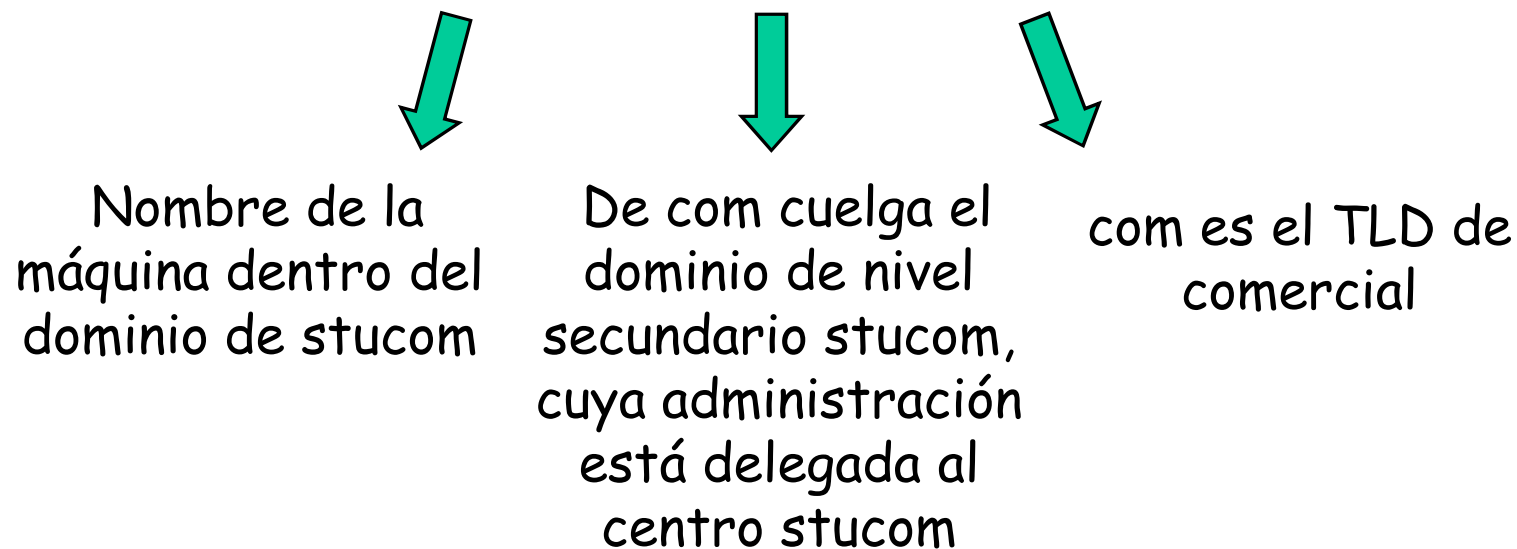
3) 1 dominio de infraestructura: .arpa. Permite la resolución inversa de direcciones. Cada servidor gestiona una rama que comienza con la etiqueta "in-addr" de la que cuelgan las direcciones en sentido numérico inverso: @IP 147.83.65.13 estaría como 13.65.83.147.in-addr.arpa.

3. JERARQUÍA DE DOMINIOS DNS

Second Level Domain (SLD)

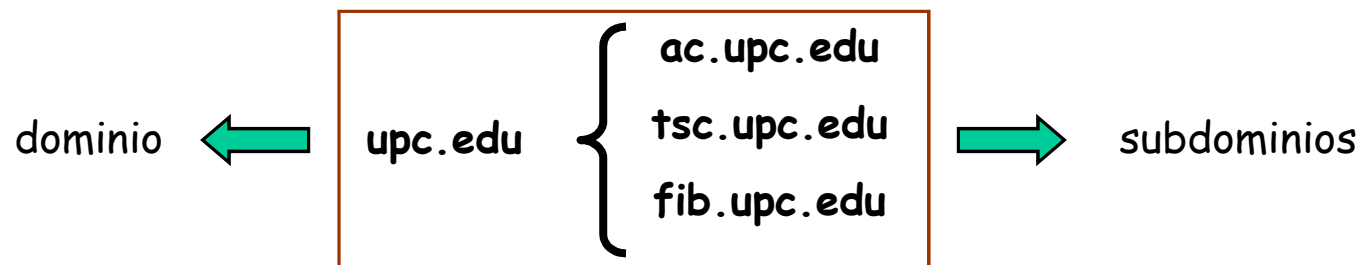
Cada uno de los TLD tiene un administrador (*registrar* en el argot DNS) que delega parte de su dominio en subdominios secundarios.

❖ Ejemplo: campus.stucom.com



4. DOMINIO Y ZONA DNS

- ❖ El **dominio** es un subárbol del espacio de nombres de dominio, es decir, un nodo con todos los nodos por debajo de él. El dominio contiene máquinas y otros dominios llamados subdominios.
- ❖ La **zona** es un archivo que contiene ciertos registros de la BBDD del espacio de nombres de dominio, que pueden identificar a un dominio o más y permiten atender las peticiones de los clientes.



4. ZONAS DE AUTORIDAD DNS

- ❖ Un servidor DNS almacena información acerca algunas partes del espacio de nombres del dominio
- ❖ Cada una de esas partes se llama **zona**. Se dice el servidor DNS tiene **autoridad sobre la zona**.
- ❖ Cada dominio o subdominio tiene una o más **zonas de autoridad** que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido.
- ❖ Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos no han sido delegados a otras zonas de autoridad.

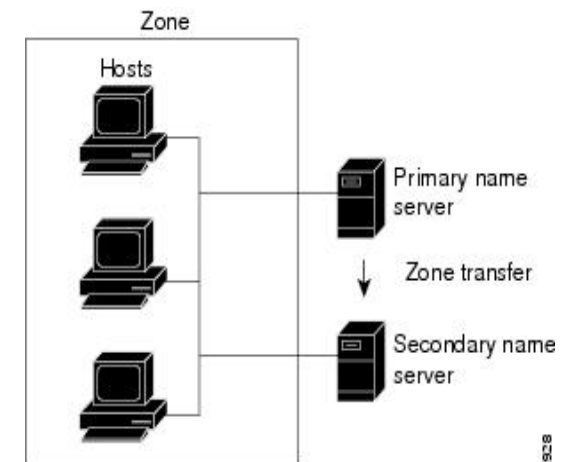
4. DELEGACIÓN DE AUTORIDAD

- ❖ La división de un dominio en subdominios no implica siempre la cesión de la autoridad sobre ellos.
- ❖ En principio un dominio puede mantener la autoridad sobre ellos. Pero también puede, si así lo decide delegar la autoridad de alguno/s de sus subdominios.
- ❖ Se define un **servidor de nombres de dominio DNS autoritario** para una zona como aquel que contiene los registros para dicha zona.
- ❖ Para ello se utilizan los registros de recursos SOA y NS.

5. SERVIDORES DNS

Los servidores de nombres se pueden clasificar en:

- Servidor primario (Primary name)
- Servidor secundario (Secondary name)
- Servidor caché (solamente)

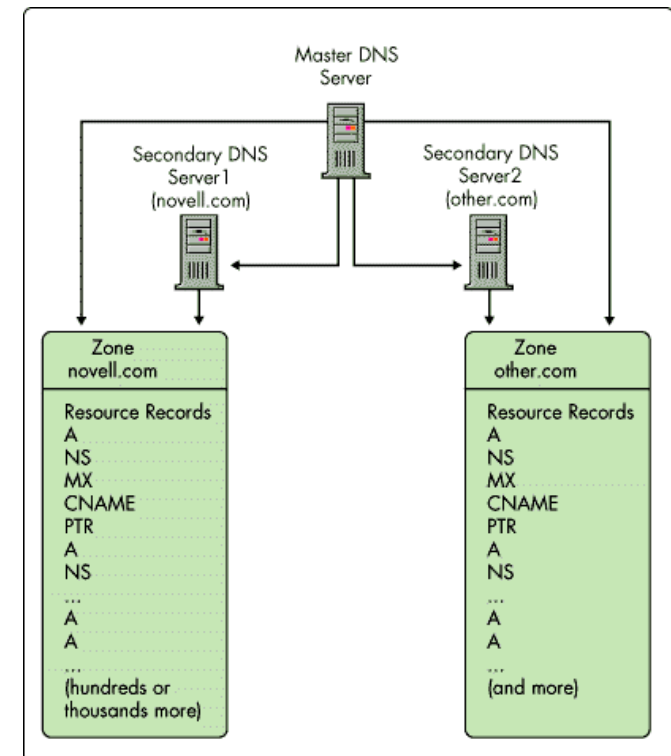


Transferencia de la zona:

Es un proceso mediante el cual se obtiene información actualizada de la zona por medio de la red.

5. SERVIDORES DNS

- ❖ Cada administrador de sistemas de una zona (dominio o subdominio) es responsable de:
- ❖ Mantener un servidor primario (disk file), que tiene la información de una zona y la autoridad sobre ella.
- ❖ Mantener uno o varios servidores de DNS secundarios (backups) independientes del primario pero que obtienen la información a partir de él.
- ❖ Son servidores conocidos como "authority" del dominio.



5. SERVIDORES DNS

- ❖ La información nueva {@IP, nombre} se añade al primario. Los secundarios la obtendrán ya que hacen "querys" del primario cada 2/3 horas.
- ❖ En estos servidores han de estar los nombres de los hosts que cuelgan de su dominio y el nombre y dirección de los servidores primarios y secundarios de las autoridades de los subdominios que haya delegado.
- ❖ Si la información no está en el DNS de la zona, los servidores DNS deben conocer la @IP de los root-servers para acceder y obtenerla.

5. SERVIDORES DNS

Domain Name: IEMAILAX.COM

Registrar: GO DADDY SOFTWARE, INC.

Whois Server: whois.godaddy.com

Referral URL: <http://registrar.godaddy.com>

Name Server: NS45.DOMAINCONTROL.COM

Name Server: NS46.DOMAINCONTROL.COM

Status: clientDeleteProhibited

Status: clientRenewProhibited

Status: clientTransferProhibited

Status: clientUpdateProhibited

Updated Date: 17-apr-2007

Creation Date: 17-apr-2007

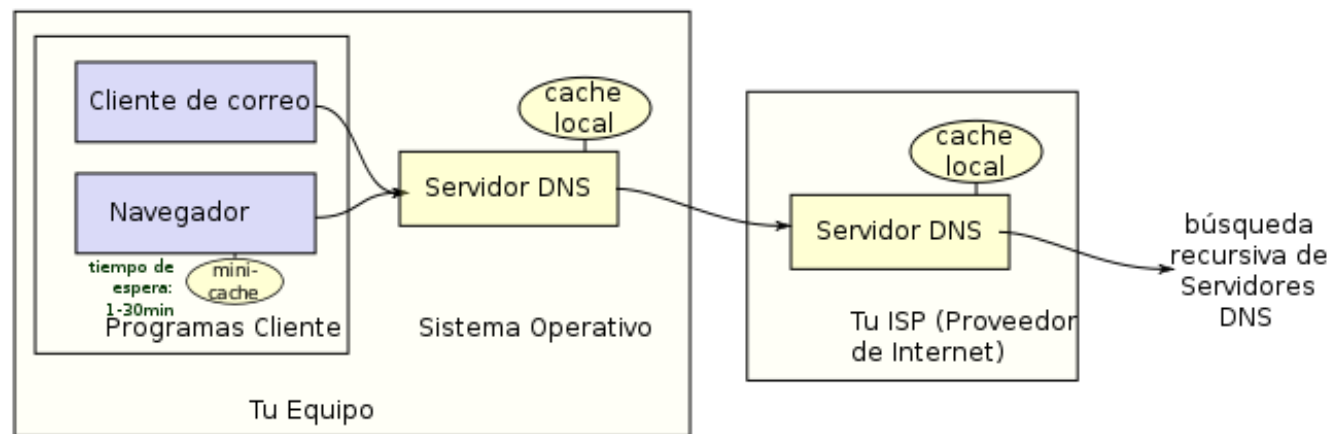
Expiration Date: 17-apr-2008

5. SERVIDORES DNS

- ❖ Los servidores DNS (no los resolver de la aplicación) disponen de *caches* para resolver nombres que han mapeado recientemente
- ❖ *Caching*: Los servidores DNS guardan en su cache las direcciones IP solicitadas un cierto tiempo indicado por TTL (TTL típico 2 días). De esta manera, si el mismo host u otro vuelve a solicitar la resolución del mismo nombre, devolverá la dirección inmediatamente sin tener que hacer de nuevo la resolución.

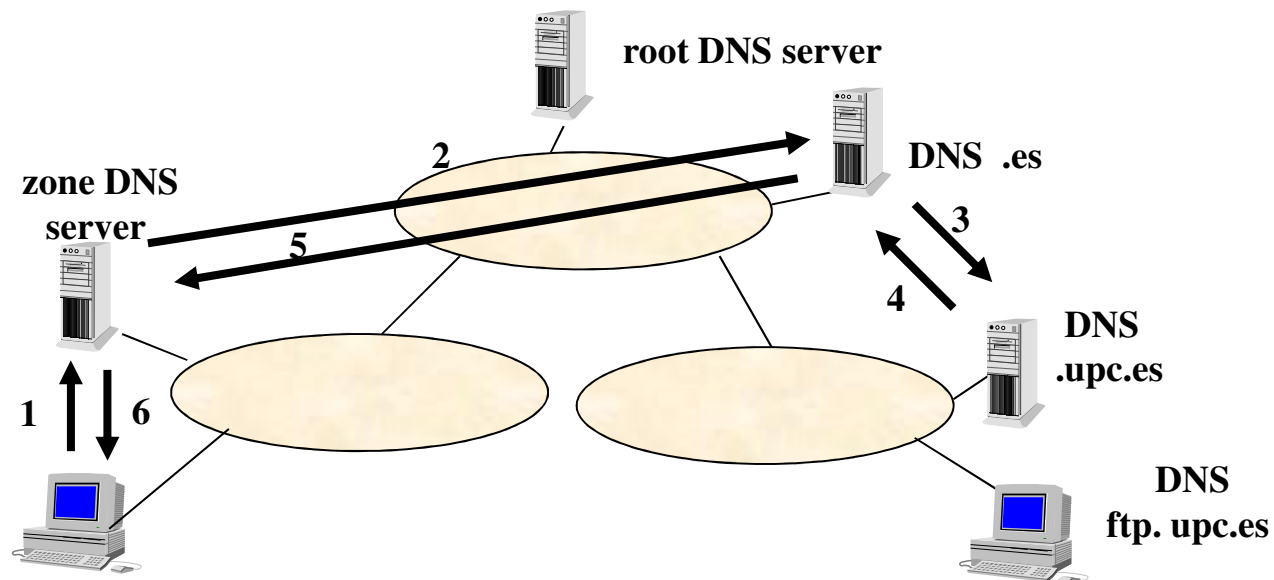
6. CONSULTA RECURSIVA

Se realiza una petición de resolución de nombres al servidor DNS local. Si el servidor no dispone de dicha información reenvía la petición al servidor de nombres con autoridad que la contiene. De forma recursiva se buscará la información y será devuelta al cliente.



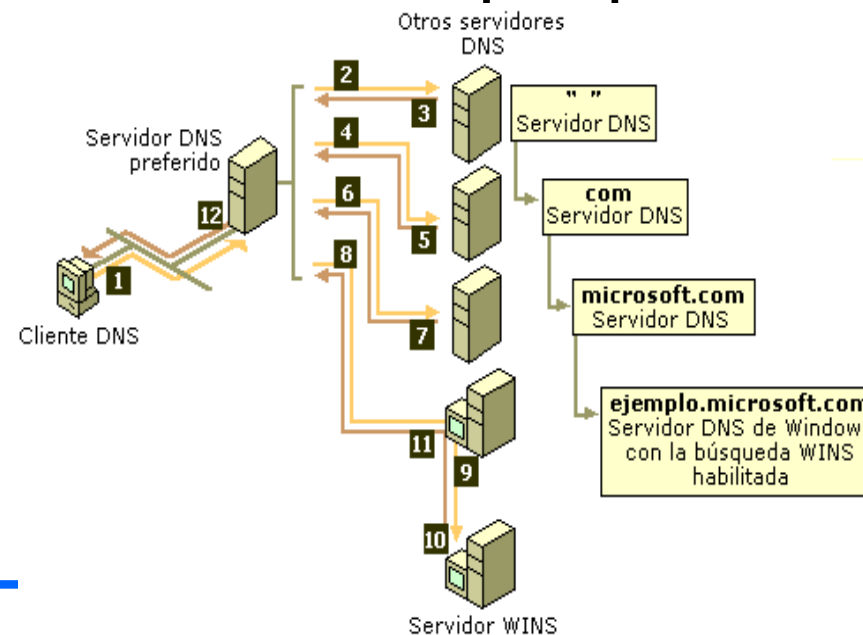
6. CONSULTA RECURSIVA

- (1) - Host pregunta por ftp.upc.es al servidor DNS de su zona (dominio)
- (2) - El servidor DNS de la zona pregunta al DNS server con dominio .es
- (3) - El servidor DNS .es pregunta al servidor DNS con dominio .upc.es
- (4) - El servidor DNS .upc.es le devuelve la @IP del servidor ftp.upc.es al dominio .es
- (5) (6) - Se devuelve la @IP del servidor ftp.upc.es al cliente.



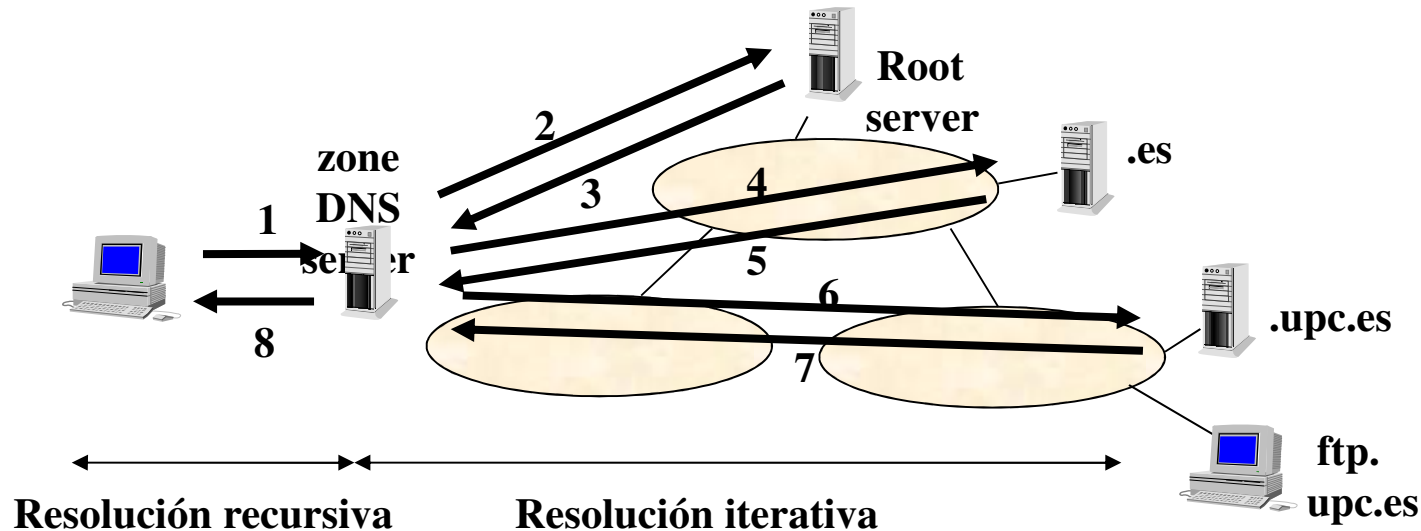
7. CONSULTA ITERATIVA (AKAMAI)

El servidor DNS local responde al cliente en función del contenido de su caché. Si no dispone de la información solicitada, entonces realiza una resolución iterativa: consulta iterativamente los servidores de los dominios hasta resolver la dirección buscada, comenzando siempre por un servidor raíz.



7. CONSULTA ITERATIVA (AKAMAI)

- (1) - Host pregunta por ftp.upc.es a su servidor DNS
- (2) - El server Zone DNS pregunta a su root server DNS
- (3) - El root server DNS le devuelve la @IP del servidor DNS con dominio .es
- (4) - Zone DNS pregunta al DNS .es.
- (5) - DNS .es devuelve la @IP de DNS .upc.es.
- (6) - Zone DNS pregunta a DNS .upc.es.
- (7) - DNS .upc.es devuelve @IP de server ftp.upc.es.
- (8) - Zone DNS devuelve la @IP del server al host.

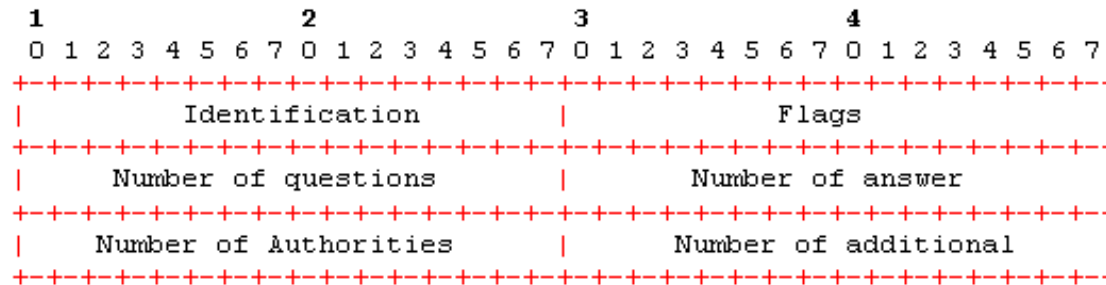


```

1      2      3      4
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               Header (12 bytes)                               /
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               Questions (variable)                           /
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               Answers (variable)                             /
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               Authority (variable)                           /
+-----+-----+-----+-----+-----+-----+-----+-----+
/                               Additional information (variable)               /
+-----+-----+-----+-----+-----+-----+-----+-----+

```

FORMATO CAMPO HEADER



- ❖ Identification: permite relacionar los mensajes de query (pregunta) y reply (respuesta). Es activado por el cliente y retornado por el servidor.
- ❖ 16-bit flags: Estan divididos en múltiples campos. Los flags más importantes son:
 - Flag QR (Query-Response): Si QR=0 mensaje de query (pregunta). Si QR=1 mensaje de reply (respuesta).
 - Flag AA (Authoritative Answer): Si AA=1 indica que ha respondido la autoridad del dominio. Si AA=0 indica que la respuesta estaba en la cache del servidor donde se ha hecho la pregunta. La respuesta no autoritativa si el DNS tiene que consultar otro DNS para obtener la respuesta. La respuesta puede ser autoritativa si el DNS tiene autoridad sobre el dominio consultado.
 - Flag RD (Recursion-Desired): Si la resolución será recursiva o iterativa.
- ❖ Number of questions: N° de entradas en la sección "Questions".
- ❖ Number of answer RRs: N° de entradas de la sección "Answers".
- ❖ Number of Authority RRs: N° de entradas de la sección "Authority".
- ❖ Number of additional RRs: N° de entradas de la sección "Additional".

FORMATO CAMPO QUESTION

Contiene las consultas al servidor de nombres. Normalmente tiene una sola cuestión.

```

      1           2           3           4
      0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
+-----+-----+-----+-----+-----+-----+-----+-----+
|6 r o g e n t 2 a c 3 u p c 3 e d u 0      Query name      |
+-----+-----+-----+-----+-----+-----+-----+-----+
|               Query type               |               Query class               |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

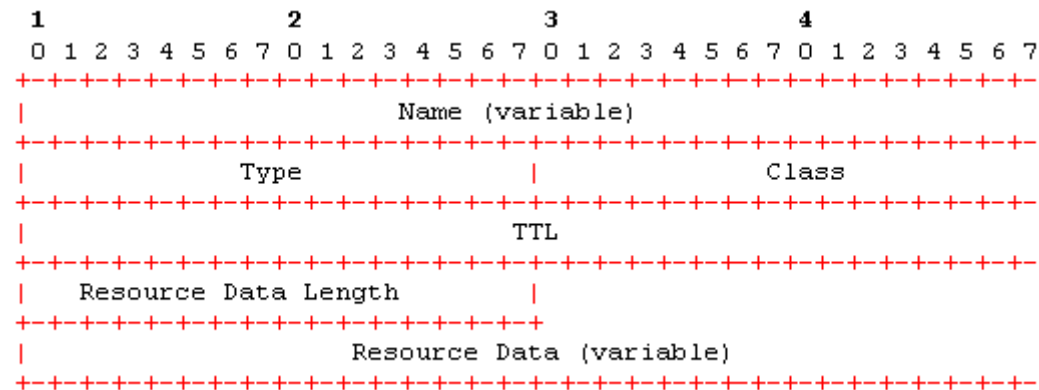
- ❖ Query name: Especifica el nombre que se quiere resolver (e.g. rogent.ac.upc.edu). Es un campo que contiene un contador + string: (e.g 8 rogent 2 ac ...)
- ❖ Query type: Especifica el tipo de pregunta. Hay hasta 20 valores diferentes.
 - Query type = 1 → Tipo A (Address) o resolución de @IP a partir del nombre.
 - Query type = 2 → Tipo NS (Name Server) o resolución de un name server
 - Query type = 12 → Tipo PTR (Pointer Record) o resolución inversa (conozco la @IP y quiero el nombre). Se da un nombre del tipo 7.40.45.180.in-addr.arpa
 - Query type = 13 → Tipo MX (Mail Exchange) para encaminar correo electrónico.
- ❖ Query class: Especifica el tipo de dirección que se quiere resolver. En el caso de referirse a una dirección de Internet vale 1.

TIPOS REGISTROS DNS

Nombre del recurso	Tipo de registro	Función
Inicio de autoridad	SOA	Identifica al servidor autoritario de una zona y sus parámetros de configuración.
Servidor de nombres	NS	Identifica servidores de nombres autorizados para una zona.
Dirección	A	Asocia un nombre de dominio FQDN con una dirección IP.
Puntero	PTR	Asocia una dirección IP a un nombre de dominio FQDN. Para las búsquedas inversas.
Registro de correo	MX	Indica máquinas encargadas de la entrega de correo en el dominio.
Nombre canónico	CNAME	Permite asignar uno o más nombres a una máquina. Alias.
Text	TXT	Almacena cualquier información.
Servicio	SRV	Ubicación de los servidores para un servicio.

FORMATO CAMPOS ANSWER, AUTHORITY

Los campos *Answer*, *Authority* y *Additional* estan formados por secuencias de uno o más *Resource Records*. La siguiente figura muestra el formato de un RR.



- ❖ Los tres primeros campos (*Name*, *Type* y *Class*) tienen el mismo significado que en el campo *Question*.
- ❖ TTL (Time-to-live): Es el número de segundos que un RR puede permanecer en la cache del cliente (normalmente 2 días)
- ❖ Resource data length: la cantidad de bytes del "Resource Data"
- ❖ Resource data: Depende del campo "type". Si Type = 1 (Tipo A) es una @IP y por tanto tiene 4 bytes. Si Type = 2 (Tipo NS) es el nombre de la autoridad (resolución de un name server)

GESTIÓN ASIGNACIÓN DOMINIOS

- ❖ La asignación de dominios es gestionada por la ICANN, entidad privada sin ánimo de lucro, que se encarga de dar tanto dominios genéricos como @IP.
- ❖ Los dominios genéricos son registrados por compañías a las que ICANN da el derecho a que actúen como tales bajo ciertas restricciones (Accredited Registrars)
- ❖ En España, el Ministerio de Fomento (servicio es-nic, <http://www.nic.es>) gestionado por INECO (empresa pública), se encarga del registro y asignación del dominio .es
- ❖ En España, se puede pedir dominios a Nominalia (<http://www.nominalia.com>) o <http://www.interdomain.es>
- ❖ La información de los administradores de los TLD se pueden encontrar en <http://www.internic.net>. Internic tiene un listado de empresas que efectúan esta asignación. Internic es la autoridad que añade la información al DNS.

PRACTICA 1. SERVIDORES DNS Y WINS EN WINDOWS 2016

Paso 1. Arrancar la máquina virtual de un equipo Windows 2016 Server sin ningún servidor instalado

Paso 2. Como no tenemos dominio todavía, ya que no está instalado el Active Directory, sumaremos el equipo Windows 2003 server al grupo de trabajo "practica.com". Poner el siguiente nombre al equipo: **vuestronombreDNS**.

Paso 3. Configurar la tarjeta de red del equipo:

Dirección IP: 192.168.1.1

Mascara: 255.255.255.0

Puerta de enlace: 192.168.1.1

Dirección DNS Primario: 127.0.0.1

Paso 4. Situar el servidor dentro de la vmnet 3.

PRACTICA 1. SERVIDORES DNS Y WINS EN WINDOWS 2016

Paso 5. Instalar el servidor DNS en el equipo, mediante la herramienta "Administre su servidor". Indicar las opciones:

- Crear zonas de búsqueda directa e inversa (recomendado para ..)
 - Si, crear una zona de búsqueda directa ahora (recomendado)
 - Tipo zona: **Zona principal**
 - Nombre de zona: **nuevazona.tunombre.com**
 - Archivo de zona: **nuevazona.tunombre.com.dns**
 - No admitir actualizaciones dinámicas
 - Si, crear una zona de búsqueda inversa ahora
 - Tipo zona: **Zona Principal**
 - Nombre de la zona de búsqueda inversa: **192.168.1.X**
 - Archivo de zona: **1.168.192.in-addr-arpa.dns**
 - No admitir actualizaciones dinámicas
 - Reenviadores: **No, no reenviar consultas**
-

PRACTICA 1. SERVIDORES DNS Y WINS EN WINDOWS 2016

Paso 6. Obtener una captura desde la herramienta de administración del servidor DNS. Desplegar las zonas de búsqueda directa (para resolver consultas de nombres para darnos la ip) y las zonas de búsqueda inversa (que nos dará el nombre de la máquina a partir de la dirección IP).

Paso 7. Borrar la zona de búsqueda directa: nuevazona.tunombre.com

Paso 8. Crear nueva zona de búsqueda directa:

- Tipo de zona: Zona principal
- Nombre de zona: **practica.com**
- Archivo de zona: **practica.com.dns**
- No admitir actualizaciones dinámicas

Paso 9. Después de la configuración podemos ejecutar una prueba del sistema para ver su funcionamiento. Ir a Propiedades del servidor DNS + Pestaña Supervisión. Realizar una consulta simple y otra recursiva a otros servidores DNS ¿Cuál da error? ¿porqué?

PRACTICA 1. SERVIDORES DNS Y WINS EN WINDOWS 2016

Paso 10. Crear un registro de tipo A → Nuevo Host

dns2.practica.com ↔ 192.168.1.2

Paso 12. Clonar el equipo windows server.

Paso 13. Cambiar la dirección IP del equipo clonado a 192.168.1.2.
Cambiar su nombre del equipo clonado a dns2.

Paso 14. Borra el registro de tipo A dns2 en el primer servidor.

Paso 15. Programar un reenviador en el primer servidor de manera que apunte a la dirección 192.168.1.2 (servidor dns2). Ir a propiedades del servidor DNS + Pestaña Reenviadores.

Paso 16. Probar que ping dns2 funciona correctamente y que la resolución funciona

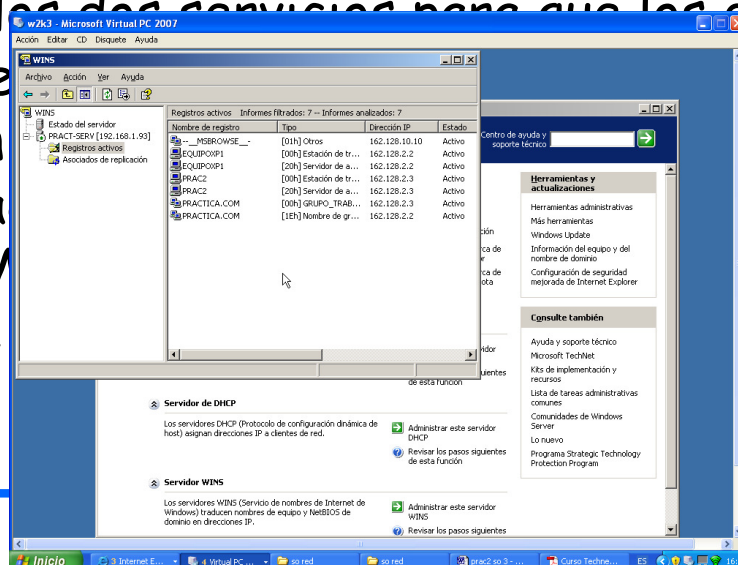
PRACTICA 1. SERVIDORES DNS Y WINS EN WINDOWS 2016

Servidor WINS

Paso 17. Iniciamos la instalación del servidor WINS (para permitir la resolución de nombres NetBios a través de este servicio sin DNS) a través de la herramienta Administre su servidor.

Paso 18. Una vez está instalado el servidor DNS, al iniciarse los equipos XP se registran en la base de datos de WINS. Arrancar el equipo XP y obtener una imagen del servidor WINS.

Paso 19. Finalmente, debido a que conviven DNS y WINS se puede integrar los dos servicios para que los equipos basados en Windows puedan resolver los nombres de dominio. Para configurar este servicio, en la herramienta de administración de servidores de "practica.com" + "Usar búsqueda directa al propio servidor."



PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 1. Arranca un cliente Linux Desktop en el Vmware o virtual box. Deshabilita la IP que pudiera tener el Linux, sino no tendríamos conexión a Internet desde la maquina virtual

Paso 2. Abre un terminal y ejecutar los siguientes comandos para instalar el servidor DNS estandar para Linux.

sudo apt update (actualización herramienta descarga aplicaciones)

sudo apt install bind9 (instalación servidor DNS)

```
marta@marta-virtual-machine:/etc/netplan$ sudo apt-get install bind9
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  bind9-utils python3-ply
Paquetes sugeridos:
  bind-doc resolvconf python-ply-doc
Se instalarán los siguientes paquetes NUEVOS:
  bind9 bind9-utils python3-ply
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 451 kB de archivos.
Se utilizarán 1.909 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```


PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 4. Comandos para iniciar, parar y reiniciar el servidor DNS:

sudo service bind9 start

sudo service bind9 stop

sudo service bind9 restart

Comando para recargar el fichero de zona o de configuracion de cambios:

sudo service bind9 reload

Comando para ver el estado actual del servidor BIND:

sudo service bind9 status

```
marta@marta-virtual-machine:~$ sudo service bind9 start
[sudo] contraseña para marta:
marta@marta-virtual-machine:~$ sudo service bind9 stop
marta@marta-virtual-machine:~$ sudo service bind9 restart
marta@marta-virtual-machine:~$ sudo service bind9 status
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-12-03 12:05:52 CET; 17s ago
     Docs: man:named(8)
   Main PID: 2479 (named)
    Tasks: 5 (limit: 2183)
   Memory: 12.3M
    CGroup: /system.slice/named.service
            └─2479 /usr/sbin/named -f -u bind

dic 03 12:05:52 marta-virtual-machine named[2479]: network unreachable resolv
dic 03 12:05:52 marta-virtual-machine named[2479]: network unreachable resolv
dic 03 12:05:52 marta-virtual-machine named[2479]: network unreachable resolv
dic 03 12:05:52 marta-virtual-machine named[2479]: network unreachable resolv
dic 03 12:05:52 marta-virtual-machine named[2479]: network unreachable resolv
dic 03 12:05:52 marta-virtual-machine named[2479]: network unreachable resolv
dic 03 12:05:52 marta-virtual-machine named[2479]: network unreachable resolv
dic 03 12:05:52 marta-virtual-machine named[2479]: network unreachable resolv
dic 03 12:05:52 marta-virtual-machine named[2479]: managed-keys-zone: Key 2032
dic 03 12:05:52 marta-virtual-machine named[2479]: resolver priming query comp
lines 1-20/20 (END)
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 5. Una vez se ha realizado la instalación, el servidor DNS ya esta en funcionamiento. Comprueba que bind9 trabaja correctamente mediante el comando:

nslookup google.com 127.0.0.1

```
marta@marta-virtual-machine:/etc/bind$ nslookup google.com 127.0.0.1
Server:          127.0.0.1
Address:         127.0.0.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.184.174
Name:   google.com
Address: 2a00:1450:4003:80c::200e
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 6. El principal fichero del servidor dns es `/etc/bind/named.conf`. Incluye los 3 ficheros donde se realiza la configuración propiamente del servidor:

- `named.conf.options`
- `named.conf.local`
- `named.conf.default-zones`

```
GNU nano 4.8                                named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 7. El primer fichero de configuración es **named.conf.options**.

- La directiva **listen-on** permite especificar las redes que el servidor DNS servirá. "any;" permite trabajar con todas las redes.
- BIND9 solo permite consultas locales por defecto. La directiva **allow-query** con "any;" permite todas las consultas
- **Forwarders** contiene las direcciones IP de los servidores DNS a los cuales redirigir las consultas si nuestro servidor no contiene los datos requeridos

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and your clients, you may need to fix
    // ports to talk.  See http://www.isc.org/bindfaq

    // If your ISP provided one or more IP addresses for upstream
    // nameservers, you probably want to use them, so you can turn off
    // Uncomment the following block,
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about
    // you will need to update your keys
    //=====
    dnssec-validation auto;

    listen-on-v6 { any; };
};
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 8. Abre el fichero e introduce las siguientes opciones:

sudo nano /etc/bind/named.conf.options

```
options {
    directory "/var/cache/bind";
    // If there is a firewall betw
    // to talk to, you may need to
    // ports to talk. See http://
    // If your ISP provided one or
    // nameservers, you probably w
    // Uncomment the following blo
    // the all-0's placeholder.
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    //=====
    // If BIND logs error messages
    // you will need to update you
    //=====
    dnssec-validation auto;
    listen-on-v6 { any; };
    listen-on { any; };
    allow-query { any; };
};
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 9. Salva y cierra el fichero. Comprueba la configuración:

sudo named-checkconf

Si no aparecen errores, significa que todo es correcto. Reinicia el servicio para que los cambios tomen efecto

sudo systemctl restart bind9

Para comprobar que el servidor DNS esta funcionando

correctamente:

**nslookup ubuntu.com
127.0.0.1**

```
marta@marta-virtual-machine:/etc/bind$ sudo named-checkconf
marta@marta-virtual-machine:/etc/bind$ sudo systemctl restart bind9
marta@marta-virtual-machine:/etc/bind$ nslookup ubuntu.com 127.0.0.1
Server:          127.0.0.1
Address:         127.0.0.1#53

Non-authoritative answer:
Name:   ubuntu.com
Address: 185.125.190.20
Name:   ubuntu.com
Address: 185.125.190.29
Name:   ubuntu.com
Address: 185.125.190.21
Name:   ubuntu.com
Address: 91.189.88.181
Name:   ubuntu.com
Address: 91.189.88.180
Name:   ubuntu.com
Address: 2001:67c:1360:8001::2c
Name:   ubuntu.com
Address: 2001:67c:1360:8001::2b
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

BIND9 COMO SERVIDOR DNS PRIMARIO

Paso 10. Editaremos el segundo archivo de configuración de bind:

sudo nano /etc/bind/named.conf.local

Agregaremos la zona que corresponde a nuestro dominio "practica.com". El servidor DNS se encargará de resolver los nombres de dominio a sus respectivas Ips dentro de este dominio

```
GNU nano 4.8 /etc/bind/named.conf.local
//
// Do any local configuration here
//

zone "practica.com" {
    type master;
    file "/etc/bind/db.practica";
    //allow-transfer { 192.168.1.1; };
    //also-notify { 192.168.1.1; };
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 10bis. Los parámetros del archivo `named.conf.local` son los siguientes:

- **type:** master, slave, forward, hint;
- **file:** indica el path al fichero de zona;
- **allow-transfer:** lista de servidores DNS permitidos para transferir la zona
- **also-notify:** el servidor DNS primario que notificará a estos servidores de los cambios de zona

Paso 11. Reinicia el servicio y comprueba su estado

sudo service bind9 restart

sudo service bind9 status

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 12. Crea el fichero de configuración de zona "db.practica" a partir de "db.local" y abrelo:

sudo cp db.local db.practica

sudo nano db.practica

```
GNU nano 4.8                                db.practica
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      localhost. root.localhost. (
                                2           ; Serial
                                604800      ; Refresh
                                86400       ; Retry
                                2419200     ; Expire
                                604800 )    ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      A        127.0.0.1
@         IN      AAAA     ::1
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

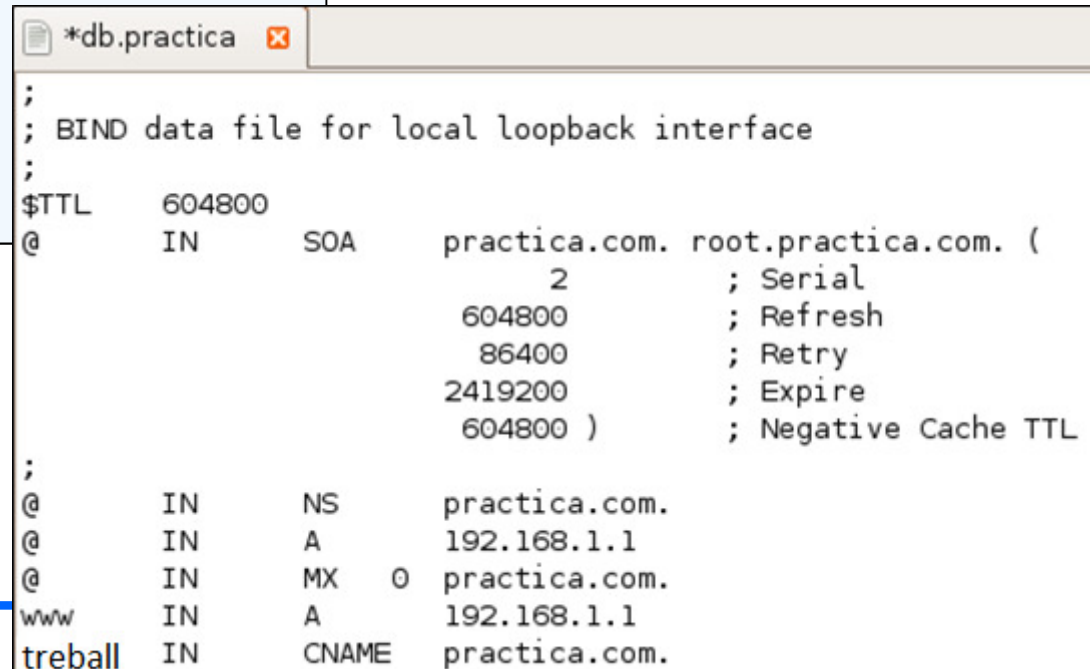
Paso 13. Editamos el fichero creado "db.practica". Hacer el siguiente reemplazo de líneas:

- Reemplaza la palabra "localhost." en el registro SOA por "practica.com."
- Cambia la IP "127.0.0.1" por la que queramos asignar al dominio 192.168.1.1 y añadimos al final del fichero todos los registros A, MX y CNAME que queramos
- El numero de Serie del cambio se debe de incrementar manualmente cada vez que cambie el archivo de zona. El servidor secundario monitorea los cambios en la zona usando este parámetro.

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 13bis. Editamos el fichero creado "db.practica" de la siguiente manera

```
$TTL      604800
@         IN      SOA     ns.domain-name.com. admin.domain-name.com. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS      ns.domain-name.com.
@         IN      A       10.1.1.1
ns        IN      A       10.1.1.9
ns2       IN      A       10.1.1.10
mx        IN      A       10.1.1.15
```



```
*db.practica
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA     practica.com. root.practica.com. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS      practica.com.
@         IN      A       192.168.1.1
@         IN      MX      0   practica.com.
www       IN      A       192.168.1.1
treball   IN      CNAME   practica.com.
```

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Explicación de parámetros

En este ejemplo vemos primero el dominio a resolver, "practica.com." y después la cuenta de correo del administrador, "root.practica.com." (sustituyendo el primer punto por arroba, lo que dejaría "root@practica.com"). Debemos notar que al final de cada dominio viene un punto, que identifica la raíz de este.

El resto de los parámetros son:

- Serial: es un identificador del archivo, puede tener un valor arbitrario pero se recomienda que tenga la fecha con una estructura AAAA-MM-DD y un consecutivo.
- Refresco: N° de segundos que un servidor de nombres secundario debe esperar para comprobar de nuevo los valores de un registro.
- Reintentos: N° de segundos que un servidor de nombres secundario debe esperar después de un intento fallido de recuperación de datos del servidor primario.

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

- Expiración: número de segundos máximo que los servidores de nombre secundarios retendrán los valores antes de expirarlos.
- TTL mínimo: Significa Time To Live y es el número de segundos que los registros se mantienen activos en los servidores NS caché antes de volver a preguntar su valor real.

Los registros definidos son:

A (Address)	Define una @ IP y el nombre asignado al host.
MX (Mail)	Se usa para identificar servidores de correo
CNAME (Canonical Name).	Alias que se asigna a un host que tiene una @ IP valida y que responde a diversos nombres. Pueden declararse varios para un host.
NS (Name Server).	Define los servidores de nombre principales de un dominio.
SOA (Start Of Authority).	Especifica el servidor DNS primario del dominio, la cuenta de correo del administrador y tiempo de refresco de los servidores secundarios

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Tipos de registros

El final del fichero contiene registros DNS. El formato del registro: hostname \leftrightarrow clase \leftrightarrow tab \leftrightarrow tipo registro DNS \leftrightarrow valor. donde:

- hostname - Es el dominio de tercer nivel del dominio. Por ejemplo **www.practica.com** o **treball.practica.com**. @ o nada significa una entrada para el nombre de zona (en este caso, practica.com).
 - clase es IN (Internet), indica el tipo de red;
 - Tipos de registros DNS mas comunes: A, NS, MX, CNAME, TXT.
 - "A" contiene la dirección IP del nombre de dominio
 - "NS" es la dirección IP del servidor DNS de la zona
 - "MX" el servidor de mail
 - "CNAME" - alias referenciando al valor del registro especificado,
 - "TXT" - entrada a medida;
 - valor - dirección IP, nombre de host, información de texto.
-

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 14. Editar el fichero `/etc/resolv.conf`, para que nuestra máquina utilice el servidor de DNS que hemos configurado. Dejar la línea:

nameserver 127.0.0.1

Se debería hacer lo mismo con el resto de máquinas de la red que vayan a utilizar el servidor, con la única diferencia que habrá que sustituir la IP 127.0.0.1 por la IP del servidor 192.168.1.1.

Paso 15. Cada vez que se cambia la configuración de BIND9, debemos reiniciar el demonio:

sudo service bind9 restart

Paso 16. Para comprobar el correcto funcionamiento, utilizamos el comando "host" el cual sirve para resolver dominios:

host principal.com

host treball.principal.com

PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Resolución inversa

Paso 17. Si deseamos también disponer de resolución de dominios inversa, es decir, que podamos preguntar por la IP "192.168.1.1" y el servidor DNS nos diga que pertenece a "practica.com", debemos añadir a "/etc/bind/named.conf":

```
zone "192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.192";  
};
```

Paso 18. Creamos el archivo de configuración "/etc/bind/db.192" a partir del "/etc/bind/db.127":

```
cp db.127 db.192
```


PRACTICA 2. INSTALACIÓN SERVIDOR DNS BIND EN LINUX UBUNTU

Paso 20. Podemos comprobar su funcionamiento reiniciando el demonio BIND9 y realizando una consulta:

sudo service bind9 restart

host 192.168.1.1