2º DAW

DESPLIEGUE DE APLICACIONES WEB

Unidad 3 - Servicio de configuración dinámica DNS + LDAP + Active directory

Profesora:
blanca.palao@murciaeduca.es

Contenidos

- Resolutores de nombres. Proceso de resolución de un nombre de dominio.

- Servidores raíz.

- Dominios de primer nivel y sucesivos.

- Parámetros de configuración y registros del servidor de nombres afectados en el despliegue.

- Servicio de directorios: características y funcionalidad.

- Archivos básicos de configuración. Interpretación y uso.

- Autenticación de usuarios en el servicio de directorios.

- Adaptación de la configuración del servidor de directorios para el despliegue de la aplicación. Usuarios centralizados.

Resultados de aprendizaje y criterios de evaluación

5. Verifica la ejecución de aplicaciones Web comprobando los parámetros de configuración de **servicios de red**.

Criterios de evaluación:

a) Se ha descrito la estructura, nomenclatura y funcionalidad de los sistemas de nombres jerárquicos.

b) Se han identificado las necesidades de configuración del servidor de nombres en función de los requerimientos de ejecución de las aplicaciones Web desplegadas.

c) Se han identificado la función, elementos y estructuras lógicas del servicio de directorio.

d) Se ha analizado la configuración y personalización del servicio de directorio.

e) Se ha analizado la capacidad del servicio de directorio como mecanismo de autenticación centralizada de los usuarios en una red.

f) Se han especificado los parámetros de configuración en el servicio de directorios adecuados para el proceso de validación de usuarios de la aplicación Web.

g) Se ha elaborado documentación relativa a las adaptaciones realizadas en los servicios de red.

Índice

Índice

1.Historia del servicio DNS

En los 70 la red **ARPANET**, antecesora de Internet, estaba formada por un número pequeño de servidores.

La **traducción nombre-IP** de todas las máquinas conectadas a la red se mantenía en un fichero de texto (**HOSTS**) que curiosamente se sigue manteniendo en nuestros días para resolver nombre de máquinas cuando nos conectamos a ellas por el nombre:

–Actualmente los **sistemas operativos UNIX**, mantienen un fichero con características similares en **/etc/hosts** y en Windows **/windows0/system32/drivers/etc/hosts**.

– Contiene, para cada máquina, una línea con su dirección IP y el nombre asociado separados por espacios en blanco o tabuladores.

1.Historia del servicio DNS

Ejemplo de fichero hosts

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windo
#
# This file contains the mappings of IP addresses to host names.
# entry should be kept on an individual line. The IP address sho
# be placed in the first column followed by the corresponding hos
# The IP address and the host name should be separated by at leas
# space.
#
# Additionally, comments (such as these) may be inserted on indi
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
123.123.123.123 yourdomain.com
123.123.123.123 www.yourdomain.com
```

1.Historia del servicio DNS

Problemas con el HOSTS

– Al crecer el número de computadoras, el archivo se hizo demasiado grande y difícil de manejar.

– Cada vez un número mayor de administradores de red se conectaban al servidor FTP del SRI-NIC para descargar un archivo que además crecía rápidamente.

– Las instalaciones del SRI-NIC no podían soportar semejante carga.

– Por otro lado, no existía un mecanismo eficaz para evitar que aparecieran nombres duplicados. Pronto se hicieron frecuentes problemas de este tipo.

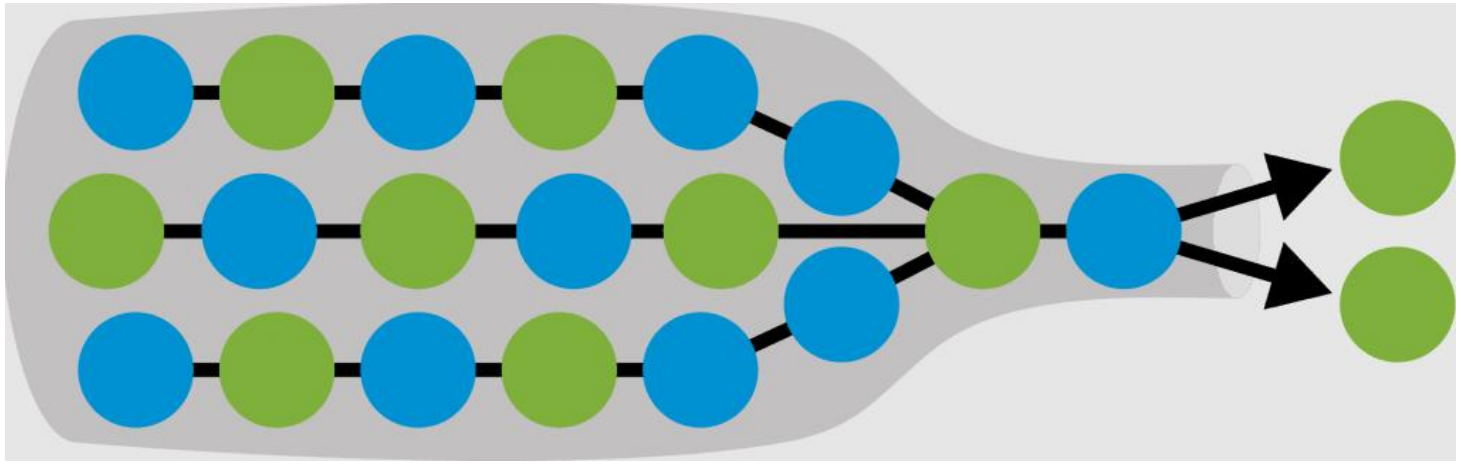
– También era cada vez más difícil mantener la consistencia del sistema de nombres, los cambios tardaban mucho en hacerse efectivos en todos los hosts.

1.Historia del servicio DNS

Solución

–Debía ser posible repartir la carga entre varias máquinas, cada una debería poder mantener información local, pero hacerla accesible globalmente.

–Descentralizar la administración, es decir no concentrar toda la carga en un solo hosts, evitando así los **cuellos de botella**.



2. ¿Qué es el servicio DNS?

En recursos extra, he dejado este mismo vídeo explicación gráfica sencilla.

- El **servicio DNS** (Domain Name System), o sistema de nombres de dominio, gestiona y mantiene de forma distribuida las direcciones de Internet y los nombres de dominio. Se trata de un servicio de búsqueda de direcciones IP y de nombres de dominios para una red TCP/IP.
- El **servicio DNS** se compone de una base de datos distribuida (en varias máquinas conectadas en red) y jerárquica en la que se almacenan las asociaciones de nombres de dominios y direcciones IP.

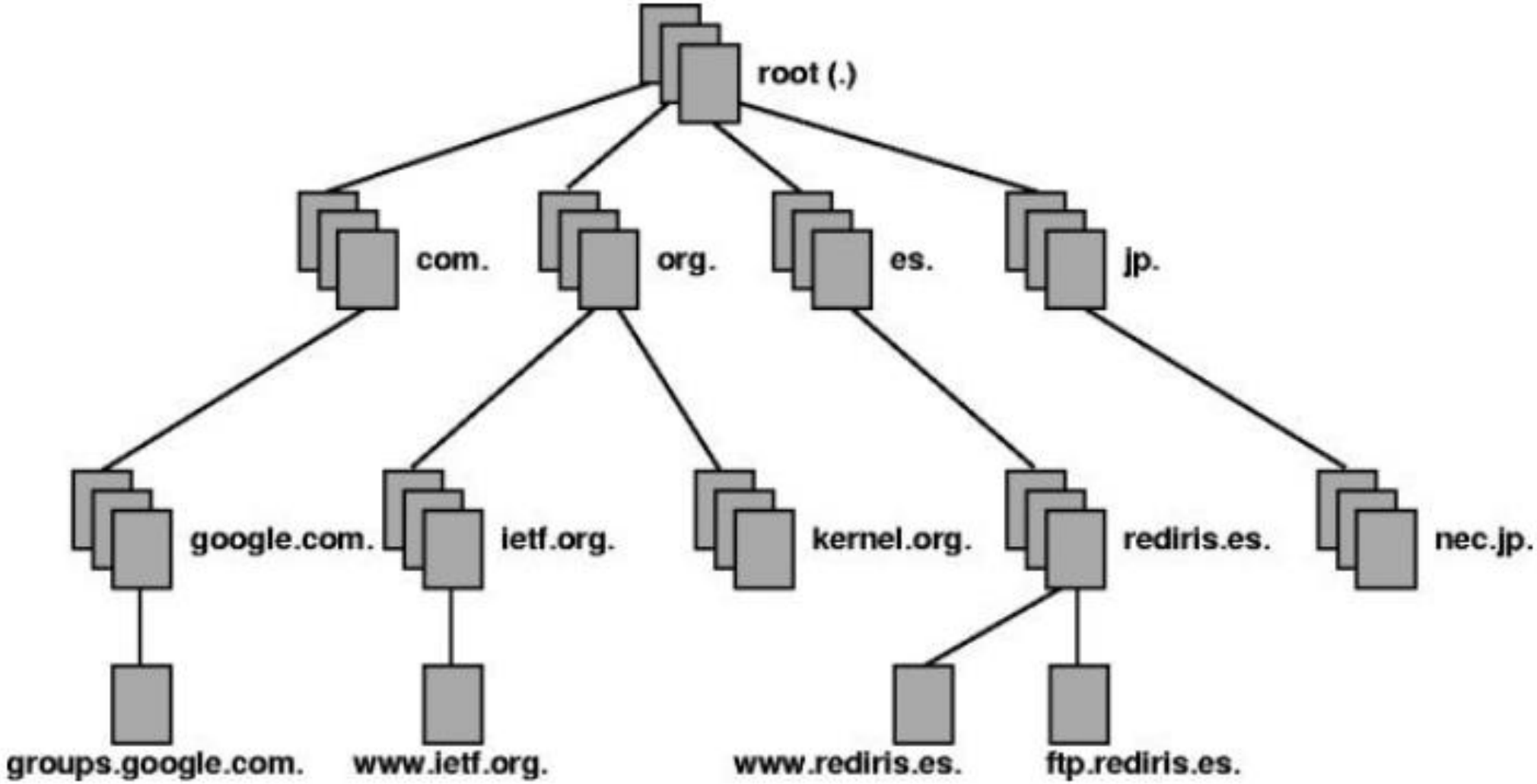
2.¿Qué es el servicio DNS?

- Esta **base de datos** está clasificada por nombres de dominio, donde cada nombre de dominio es una rama de una árbol invertido llamado espacio de nombres de dominio.
- Los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.
- Es una base de datos distribuida que se consulta según el modelo cliente/servidor.
- Los nombres de las máquinas se agrupan en dominios.
- Los dominios se organizan en forma de árbol jerárquico. La información se mantiene en servidores de nombres.

2.¿Qué es el servicio DNS?

- El árbol comienza en el nodo raíz situado en el nivel superior. Por debajo de él pueden existir un número indeterminado de nodos de nivel superior. Normalmente se utilizan hasta 5 niveles.Por ejemplo, www.ite.educacion.es. tiene **tres** niveles.
- Los nodos se identifican mediante nombres no nulos, cada uno de los cuales pueden contener un determinado número de caracteres. El nodo raíz se identifica mediante un nombre nulo (cero caracteres), el punto ".".
- El nombre del dominio en el que se encuentra una máquina incluye la concatenación (separada por puntos) de todos los nombres de dominios desde las hojas hasta la raíz del árbol.

2.¿Qué es el servicio DNS?



2.¿Qué es el servicio DNS?

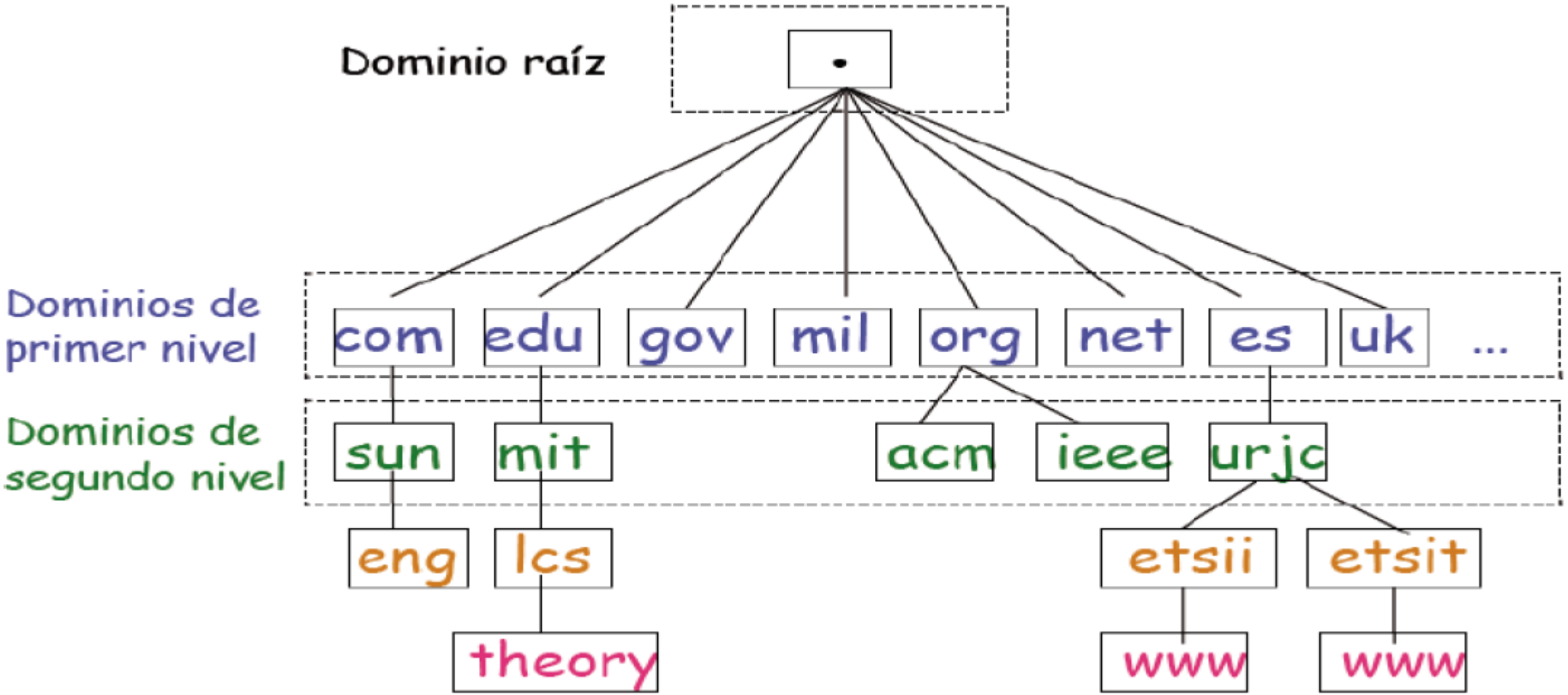
- El nombre completo de una máquina se llama **nombre de dominio completamente cualifcado** (**FQDN**, Fully Qualified Domain Name) e incluye el nombre de la máquina y el nombre del dominio en que se encuentra: ejemplo.rte.upv.es.
- Estrictamente, un **FQDN** termina siempre en el punto "**.**" (aunque normalmente se omite excepto en los mapas de DNS).
- Cada nodo del árbol representa una partición o dominio, el cual puede ser dividido a su vez en subdominios.
- Por tanto, el dominio es cada uno de los subárboles del espacio de nombres del dominio (árbol nombres del dominio).

Ejemplo, dada la computadora llamada «serv1» y el nombre de dominio «bar.com.», el **FQDN** será «serv1.bar.com.»

2.¿Qué es el servicio DNS?

- Los diferentes servidores DNS que existen en la red almacenan la información relativa a los nombres de dominio DNS en los llamados registros de recursos. Un servidor DNS tendrá aquellos registros de recursos que le permitan responder a las peticiones de **nombres relativas a la parte del espacio de nombres de dominio sobre la que tiene autoridad** dicho servidor.
- El **servicio DNS** utiliza el puerto **53**/UDP para atender las consultas de nombres y el puerto **53**/TCP para transferencias de zona entre servidores.

2.¿Qué es el servicio DNS?



3. Dominios y zonas

Jerarquía de dominios

–Dominio Root

- Es el más alto en la jerarquía, se expresa con un punto (.).
- Gestionado por **ICANN** (Internet Corporation for Assigned Names and Numbers).
- Lo sirven servidores llamados **root nameservers**.

–**Dominios de primer nivel TLDs** (Top-Level Domains)

- Dominios genéricos tradicionales: com, edu, gov, mil, org, net, int.
- Dominios genéricos modernos: aero, biz, coop, info, museum, name, pro, jobs, mobi, tel, travel, cat, asia.
- Dominio para la infraestructura del DNS: arpa
- Dominios por código ISO Code 2 del país: uk, mx, ar, de, es, jp. . .

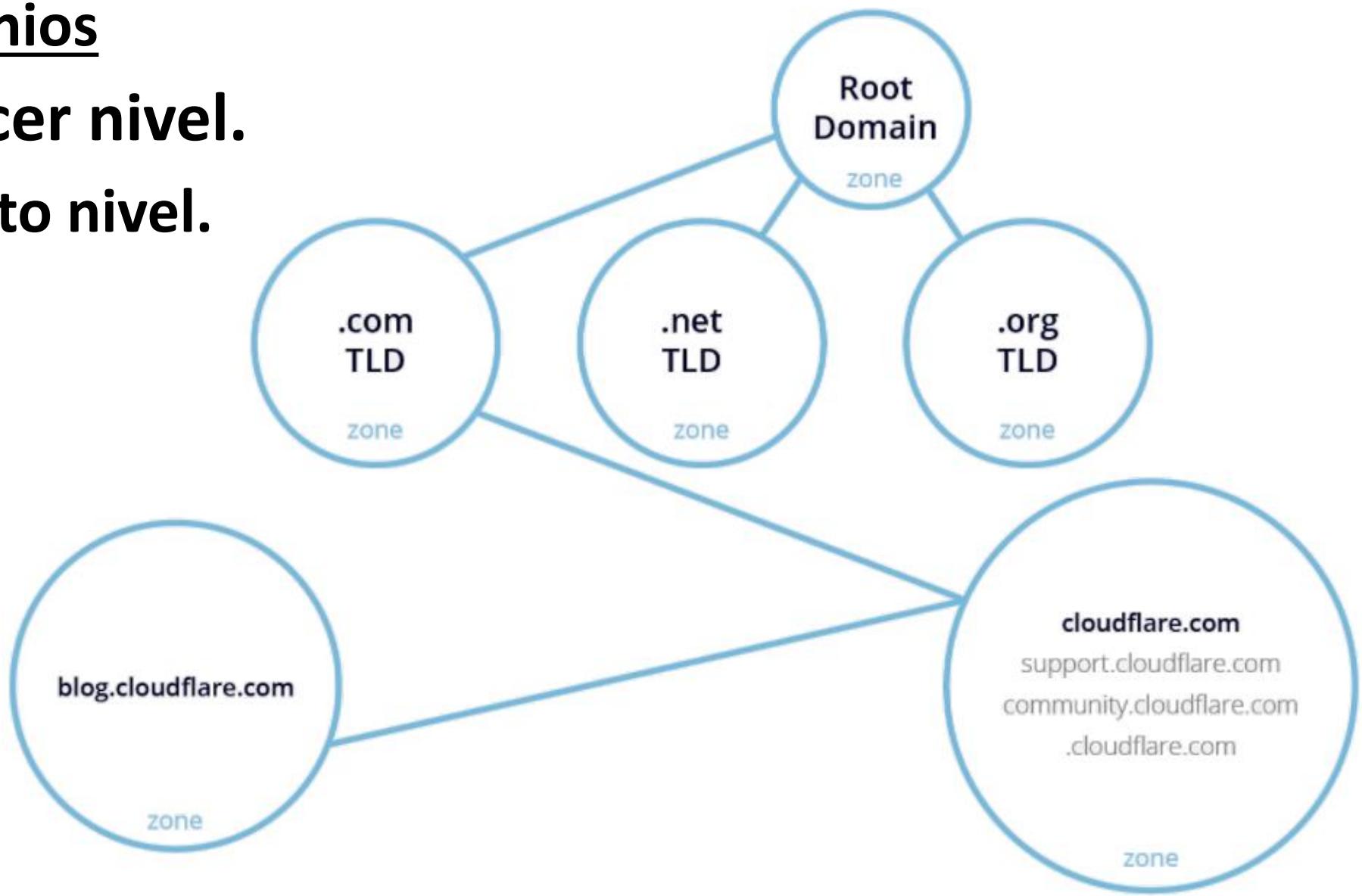
3. Dominios y zonas

Jerarquía de dominios

–Dominio de tercer nivel.

– Dominio de cuarto nivel.

…



3. Dominios y zonas

Nivel 0

Raíz

Preguntamos a un servidor DNS raíz donde están los servidores DNS de los .com

Nivel 1

Dominios TLD (Top Level Domains) o de primer nivel

Preguntamos a un DNS .com donde está el DNS de humanlevel

Nivel 2

Nuestro nombre de dominio o dominio de segundo nivel (técnicamente es un subdominio del TLD pero se le llama siemplemente dominio)

Preguntamos al DNS de humanlevel por www.humanlevel.com

Nivel 3

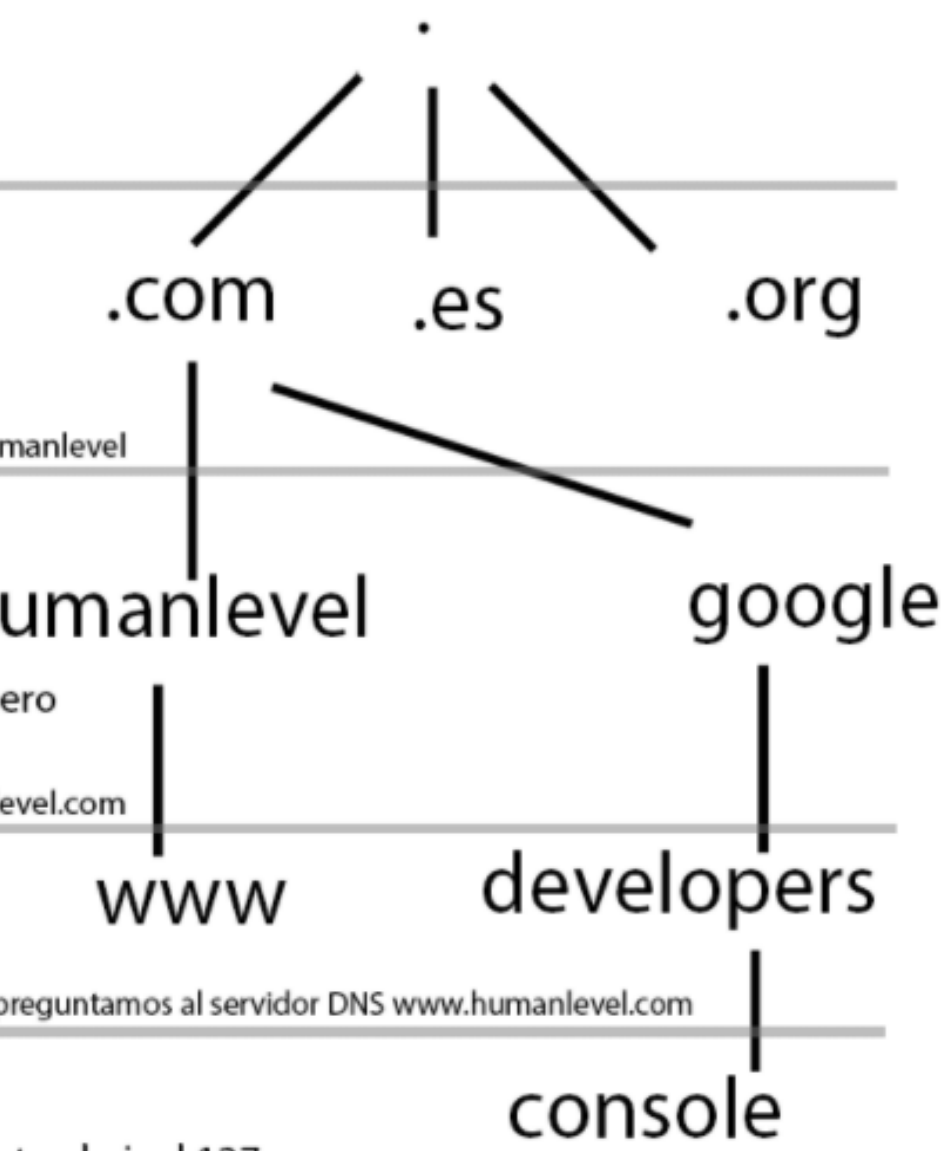
Subdominio o dominio de tercer nivel

Si el DNS del nivel anterior no ha dado la respuesta final preguntamos al servidor DNS www.humanlevel.com

Nivel 4

Otro subdominio, así podriamos seguir hasta el nivel 127.

Aquí estaríamos preguntando por console.developers.google.org.
Cada nivel tiene la autoridad de su zona (etiqueta de dominio) y de todos sus subdominios, de forma que el servidor DNS de un nivel, ante una pregunta por subdominio, puede decidir dar la IP de respuesta directamente o darle la autoridad a un servidor DNS del siguiente nivel.



3. Dominios y zonas

Ejemplo

- Tecleamos en nuestro navegador www.theguardian.com
- El sistema operativo de nuestro equipo comprueba la petición y ve que no tiene en su memoria caché la dirección de ese dominio (porque no habéis visitado nunca desde ese ordenador ese periódico), entonces realiza la petición al servidor DNS configurado manualmente en nuestra red (por ejemplo, 8.8.8.8 y 8.8.4.4, los DNS de Google).
- El servidor DNS que tenemos configurado tampoco tiene memorizada la dirección IP de ese dominio, por lo que realiza una petición al servidor encargado de la **zona de autoridad .com**.
- El servidor encargado de la zona de autoridad **.com** tiene una tabla de datos en los que están almacenados las direcciones IP de las máquinas y sus dominios. Lo busca y le responde al servidor DNS que realiza la petición, que está almacenado en la máquina con dirección amazon-gw.ip4.tinet.net (en AWS).

3. Dominios y zonas

Ejemplo

- Es entonces cuando el servidor DNS que tenemos configurado realiza una petición a amazon-gw.ip4.tinet.net para saber en qué parte de su máquina está www.theguardian.com
- El servidor donde está la página web alojada busca en su tabla de correspondencias y le responde diciendo que está en la dirección IP 178.236.0.213.
- Es entonces cuando 178.236.0.213 le devuelve la consulta a nuestra aplicación/cliente (navegador web en esta ocasión) y se comienzan a intercambiar paquetes para procesar el proceso de descarga de información al navegador del cliente.
- El cliente en este punto (¡tras varios microsegundos!) ya visualizaría la web del periódico.

3. Dominios y zonas

Dominios genéricos tradicionales.

com	Organizaciones comerciales
edu	Organizaciones educativas
gov	Organizaciones gubernamentales
mil	Organizaciones militares
net	Organizaciones administradoras de redes globales
org	Organizaciones sin fines de lucro
int	Organizaciones internacionales (como la OTAN, la ONU, etc.)
...	

3. Dominios y zonas

Dominios por código ISO del país.

es	España
us	Estados Unidos
ar	Argentina
mx	México
uk	Gran Bretaña
fr	Francia
jp	Japón
...	

3. Dominios y zonas

- La organización o autoridad encargada de la administración de un dominio puede decidir dividirlo en **subdominios**.
- Los **subdominios** pueden seguir administrados por la misma autoridad, o puede delegarse la responsabilidad de su administración a otras organizaciones.
  - –Ejemplo: Una universidad con varios departamentos puede decidir dividir el dominio de la universidad en diferentes subdominios, uno por cada departamento. Los departamentos con conocimientos telemáticos pueden querer gestionar su propio subdominio.
- **Zona**: Subárbol de DNS administrado por una organización diferente a la organización que administra el dominio padre de ese subárbol.

3. Dominios y zonas

Dominio Directo y Dominio Inverso

– **Dominio Directo**: Proporciona para cada nombre una dirección IP.

– **Dominio Inverso**: Proporciona para cada dirección IP un nombre.

• Algunas consideraciones respecto al **Dominio Inverso**:

– El dominio inverso también se conoce como dominio **in-addr.arpa**.

3. Dominios y zonas

Root nameservers Actualmente existen 13 root nameservers en todo el mundo:

- A.root-servers.net
- B.root-servers.net
- . . .
- M.root-servers.net

–Hay varias copias de cada uno de estos 13 root nameservers.

–Actualmente son muchas máquinas repartidas en el mundo las que hacen de root nameservers.

–Los mapas del dominio raíz se transfieren entre los root nameservers por mecanismos externos al DNS.

Actividad aula – Mayor caída de Facebook de la historia.

Buscad en Internet información detallada de las causas por las que se produjo la caída a nivel global de los servidores de Facebook a principios del mes de octubre del pasado año.

¡Ninguna de sus aplicaciones web funcionario durante horas!

¿Qué relación tuvo el incidente con respecto a la resolución de nombres de dominios?

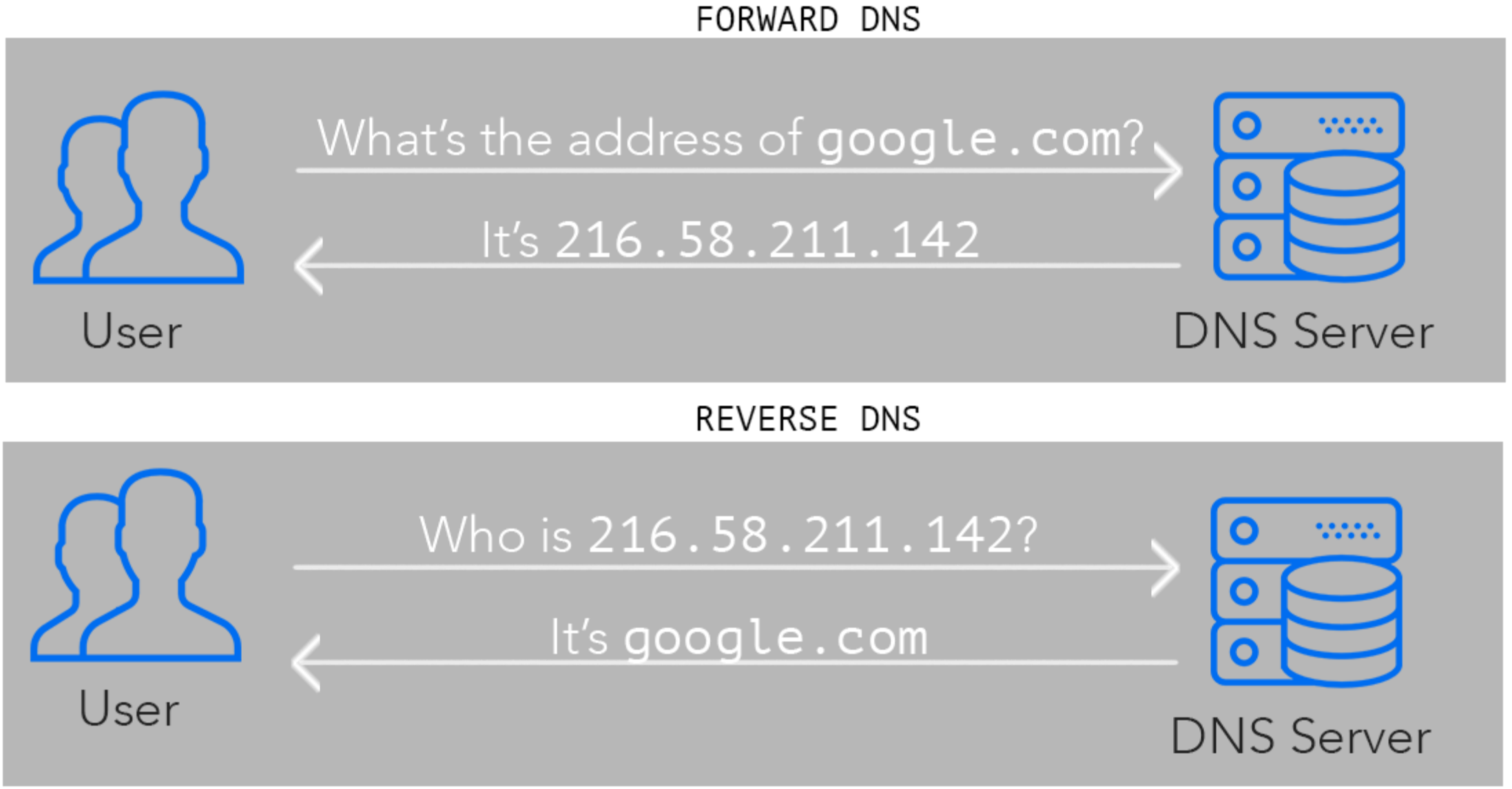
5. Servidor forwarder (reenviador)

- **Forward confirmed reverse DNS (FCrDNS)**, también llamado como inverso DNS de círculo completo, DNS inverso doble o iprev.

Realiza la autenticación de que existe una relación válida entre el titular de un nombre de dominio y el propietario de la red que se ha dado una dirección IP.

https://www.debouncer.com/reverse-dns-check -> **¡Probad!**

5. Servidor forwarder (reenviador)



6. Administración de DNS

- La organización/empresa que posee un nombre de dominio, es responsable del funcionamiento y mantenimiento de sus servidores de nombres. Este área de influencia se llama **zona de autoridad**.
- Una organización encargada de un dominio puede decidir dividirlo en subdominios y delegar la responsabilidad de su administración en otras organizaciones.
- La división no tiene porque corresponder con dominios enteros, sino que puede llevarse a cabo de manera más flexible, dando origen a lo que se llaman **Zonas**.
- Los dominios, además de contener subdominios, pueden contener hosts.

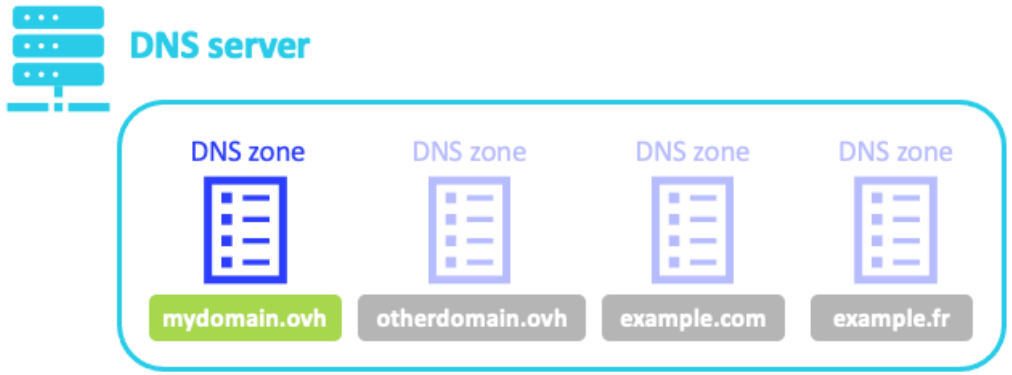
6. Administración de DNS

Zonas DNS

–Un servidor DNS puede encargarse de gestionar los datos de un dominio completo o parte de un dominio.

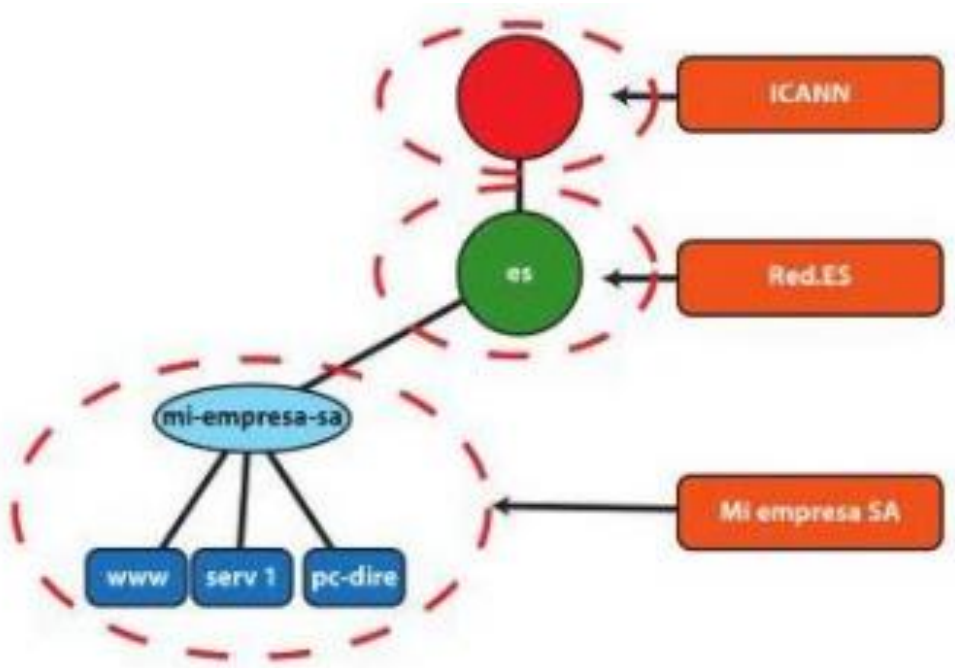
–El conjunto de datos que puede administrar un servidor de nombres recibe el nombre de zona.

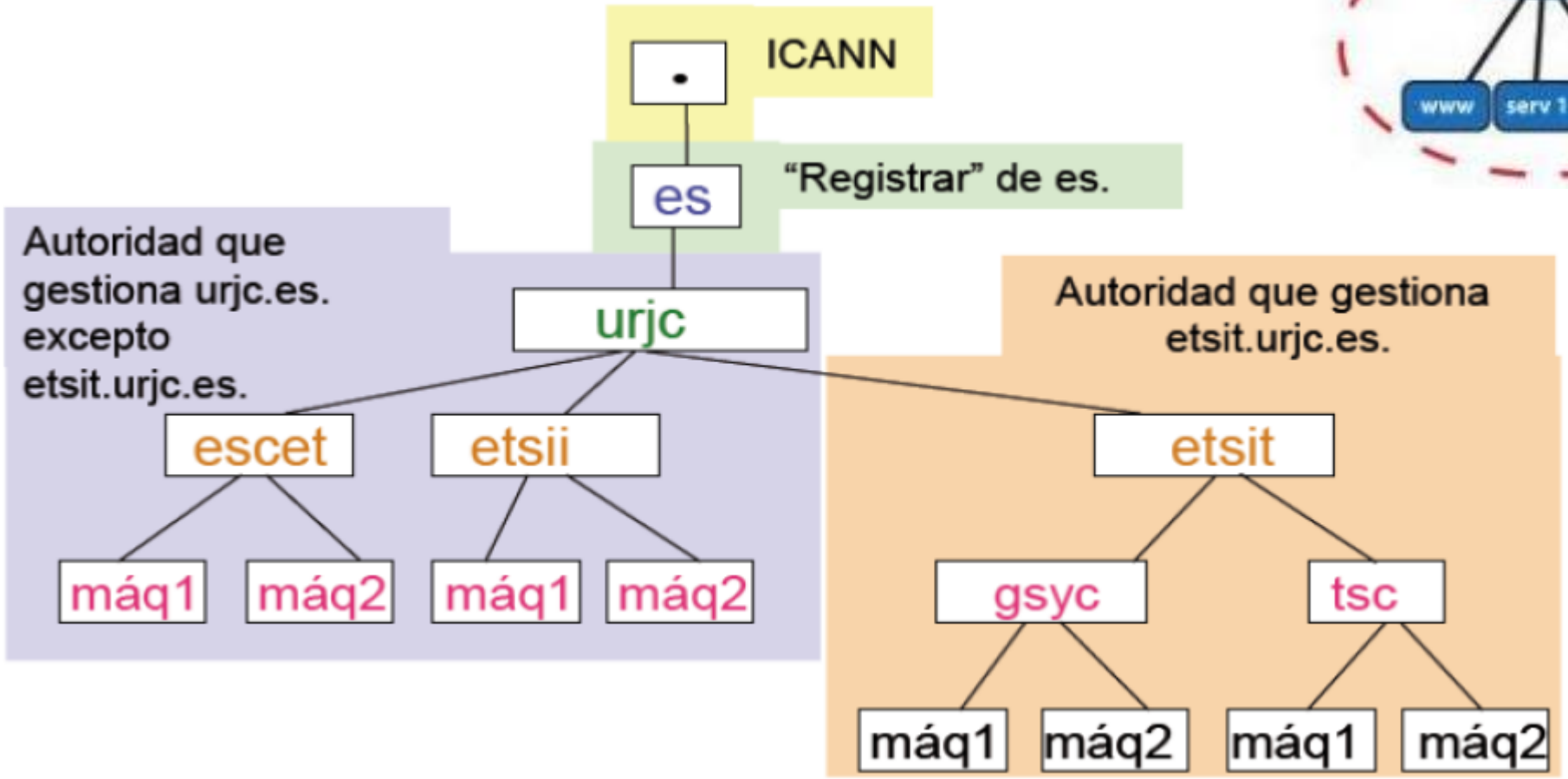
–Una zona o mapa de dominio se define en un archivo físico que contiene registros de los recursos RR de un grupo de dominios. El tipo de estos registros de recursos depende del archivo de zona en el que se vaya a configurar.



6. Administración de DNS

Zonas DNS





7. Componentes del servicio: Servidores/Clientes.

Se utiliza un mecanismo Cliente/Servidor, donde unos programas llamados **servidores de nombres** contienen información acerca de un segmento de la base de datos y la ponen a disposición de los clientes.

- **Componentes servicio DNS**
  - Servidores de Nombres
  - Clientes (RESOLVERS)
- **Servidores de nombres**

– Almacenan información sobre el espacio de nombres de dominio.

– Contienen información sobre fragmentos de la base de datos, zonas.

Los utilizan para responder a las peticiones de los clientes. Saben donde buscar los datos que no administran.

7. Componentes del servicio: Servidores/Clientes.

- **Servidores de nombres**

– Tiene información completa sobre una o varias zonas del espacio de nombres de dominio. Se dice que mantiene información autorizada para dichas zonas.

– Si hay delegación de zonas, el servidor almacenará también referencias a los servidores que contienen información autorizada para dichas zonas.

*ISP: Proveedor de servicios de Internet.

7. Componentes del servicio: Servidores/Clientes.

Clientes (Resolvers)

La consulta normalmente sigue los pasos siguientes (en una máquina GNU/Linux):

1. Consulta en el fichero /etc/hosts.
2. Si no se resuelve, consulta en un servidor de DNS, cuya dirección IP está en /etc/resolv.conf.

– El fichero /etc/nsswitch.conf (o en el que corresponda, según la distribución de Linux que usemos) determina si se consulta el fichero y/o el DNS, y en qué orden.

8. Resolución

- **Def**: **Proceso por el cuál se busca en el espacio de nombres de dominio la información correspondiente a un dominio concreto**.
- Cuando un servidor recibe una consulta de un resolver, busca en sus registros la información correspondiente, si la encuentra, la devuelve.
- Los servidores DNS responden a **dos tipos de consultas**:
  - Iterativas (no recursivas).
  - Recursivas.

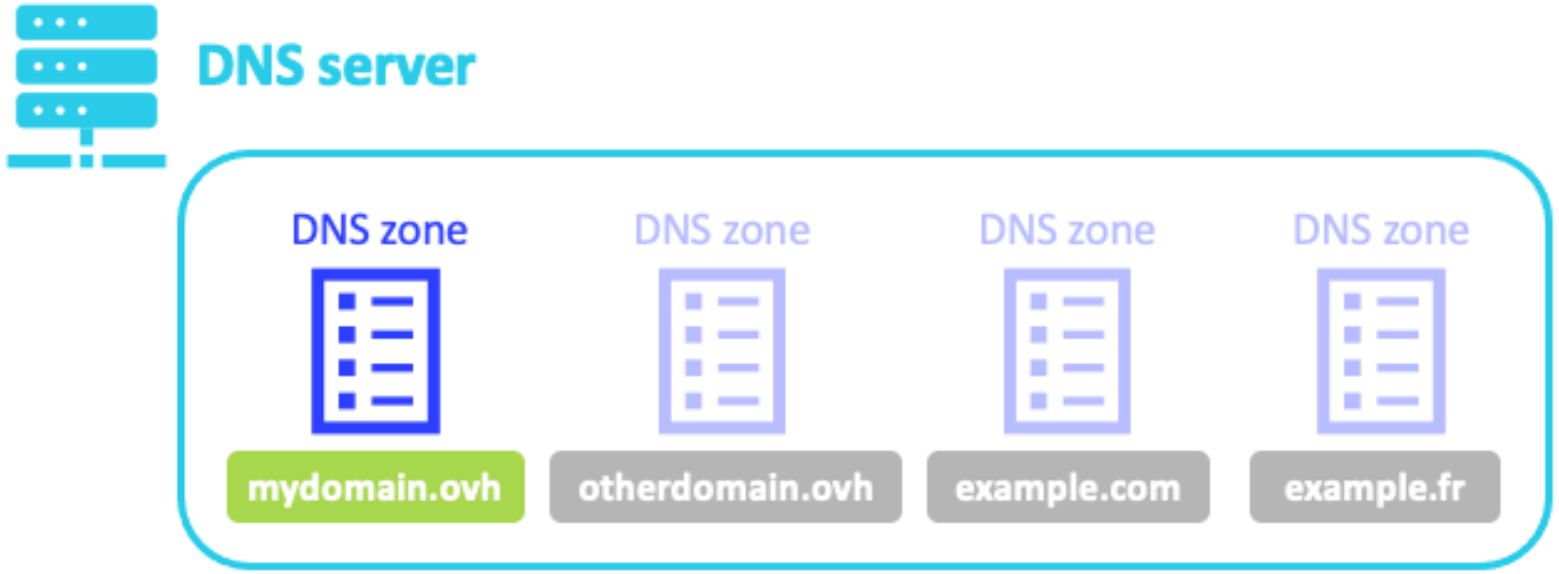
9. Zonas de autoridad

Como ya se ha indicado, un servidor DNS almacena información acerca de algunas de las partes del espacio de nombres de dominio, que no necesariamente tiene que coincidir con un dominio. Cada una de esas partes se llama **zona**, y se dice que el servidor de nombres tiene autoridad sobre la zona. Por tanto, un servidor de nombres podrá tener autoridad sobre varias zonas.

- La información relacionada con la resolución de nombres de un dominio determinado se guarda en un fichero que se denomina mapa del dominio o de zona.
- En la **zona o mapa de un dominio** están, entre otros datos:
  – Los nombres de máquinas del dominio, con sus correspondientes direcciones IP.
  – Los nombres de los subdominios directos de él, junto con las direcciones IP de los servidores de DNS que sirven esos subdominios.

9. Zonas de autoridad

- **El mapa de un dominio** lo edita el administrador de sistemas de ese dominio y se encuentra almacenado en la máquina que funciona como **servidor de DNS de ese dominio**.
- Un servidor de DNS que contenga **varios ficheros de zona servirá todos los dominios correspondientes a dichos ficheros**.



9. Zonas de autoridad

- La información de cada **Zona de Autoridad** es almacenada de forma local en un fichero de texto en el servidor DNS.
- En realidad, **la zona es un archivo que contiene registros de recursos** de la base de datos del espacio de nombres de dominio.
- Estos registros identifican parte o un dominio, pudiendo incluir sus subdominios. Mediante estos registros el servidor puede atender directamente las peticiones de los clientes y otros servidores que correspondan a la información contenida en ellos.
- La autoridad de una zona puede delegar la autoridad de parte de un domino suyo en otro servidor DNS.

9. Zonas de autoridad

Nomb_dominio	TTL	Clase	Tipo	Valor

Zonas o mapas de dominio

- Cada mapa de dominio incluye un conjunto de Registros de Recursos (RRs):
  - Son la unidad de consulta.
- Cada registro de recurso tiene 5 campos:
  - **Nombre**: Nombre del RR que se define.
  - **Tiempo de vida**: Tiempo de validez del registro en las cachés de los clientes (TTL).
  - **Clase**: Clase de direccionamiento, IN para Internet.
  - **Tipo**: Tipo del RR.
  - **Valor**: Valor del RR asociado al Nombre (en función del Tipo).

9. Zonas de autoridad

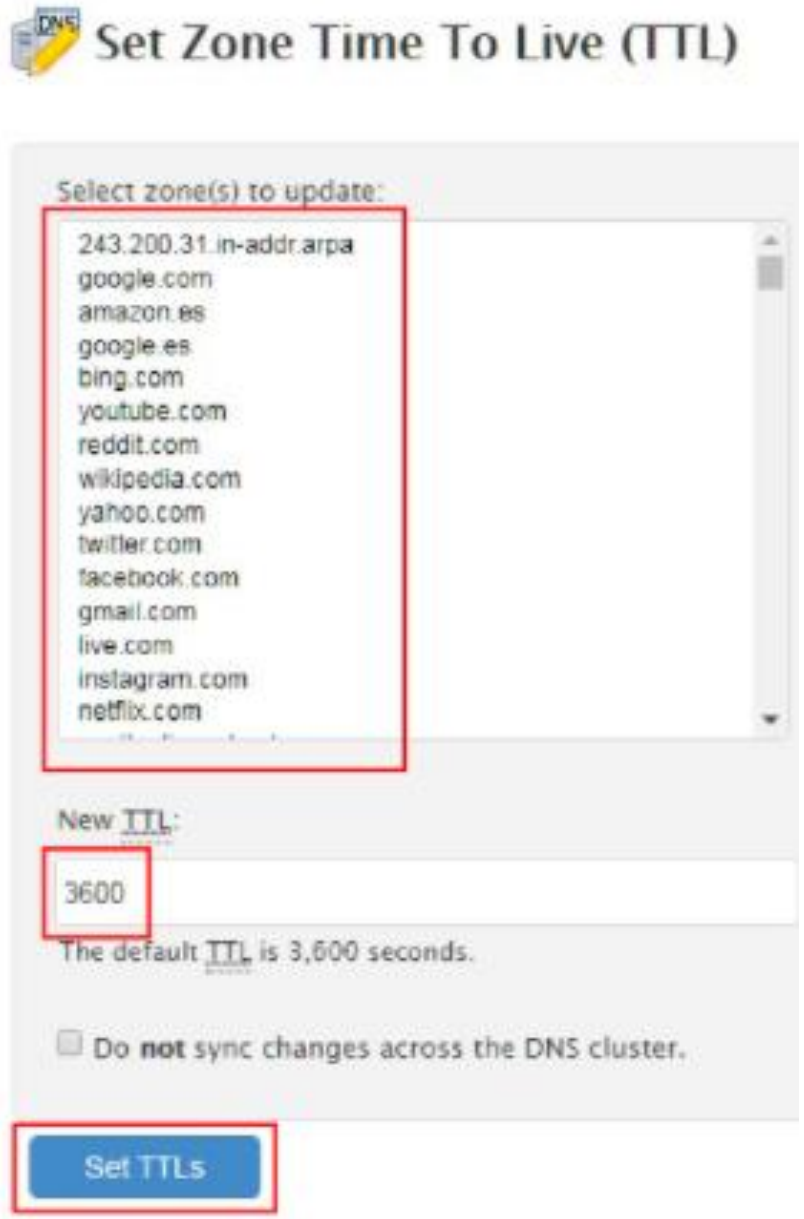
Zonas o mapas de dominio

- **Nombre_dominio**: Dominio DNS al que pertenece el recurso. Puede ser de tres formas:
  - FQDN de máquina o dominio sobre el que trata el registro.
  - Símbolo @, que hace referencia al nombre de la zona, que se toma de la configuración del servidor.
  - En blanco, que toma el valor del anterior registro que tenga definido algún propietario, bien mediante FQDN o mediante @.

9. Zonas de autoridad

Zonas o mapas de dominio

- **TTL** (Time To Live): Número de segundos que puede estar el registro en la caché de un cliente.
  - Se puede expresar en días (d), horas (h), minutos (m) y segundos (s).
  - Por ejemplo “4h30m”.
  - Si contiene un 0 indica que el registro no debe quedar en la caché.



9. Zonas de autoridad

Zonas o mapas de dominio

- **Clase**: Define la familia de protocolos en uso. Siempre será IN de Internet, que representa una red TCP/IP.
- **Tipo**: Identifica el tipo de registro, para definir distintos recursos. Tipos:

- **SOA**. **Inicio de autoridad**. Identifica al servidor autoritario de la zona y sus parámetros de configuración.
- **NS**. **Servidor de nombres**. Identifica servidores de nombres autorizados para la zona, ya que puede haber más de uno (primarios, secundarios).
- **A**. **Dirección**. Asocia un FQDN a una dirección IP.
- **PTR**. **Puntero**. Asocia una dirección IP a un FQDN. Se usa en las zonas de resolución inversas.
- **MX**. Identifica las máquinas encargadas de la entrega de **correo** en el dominio.
- **CNAME**. Permite asignar un **alias** a un recurso que ya tiene un nombre FQDN.
- Otros: **TXT**, **SRV**.

9. Zonas de autoridad

Tipo de registro	Descripción
A	Resuelve un nombre de host en una dirección IP
PTR	Resuelven una dirección IP en un nombre de host
SOA	El primer registro en cualquier archivo de zona
SRV	Resuelve nombres de servidores que proporcionan servicios
NS	Identifica el servidor DNS para cada zona
MX	El servidor de correo
CNAME	Resuelve un nombre de host en otro nombre de host

9. Zonas de autoridad

A partir de esta diapositiva, veremos las configuraciones disponibles para los dominios.

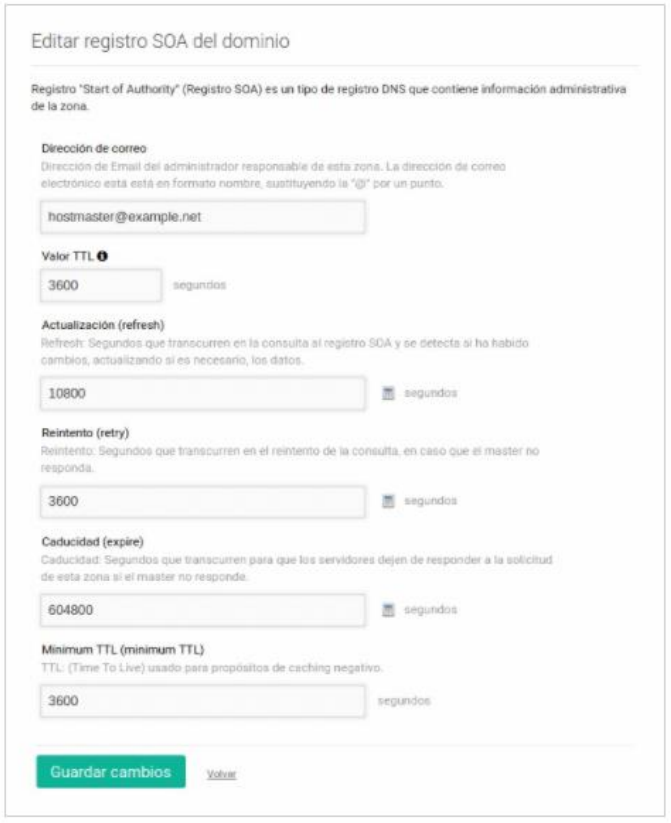
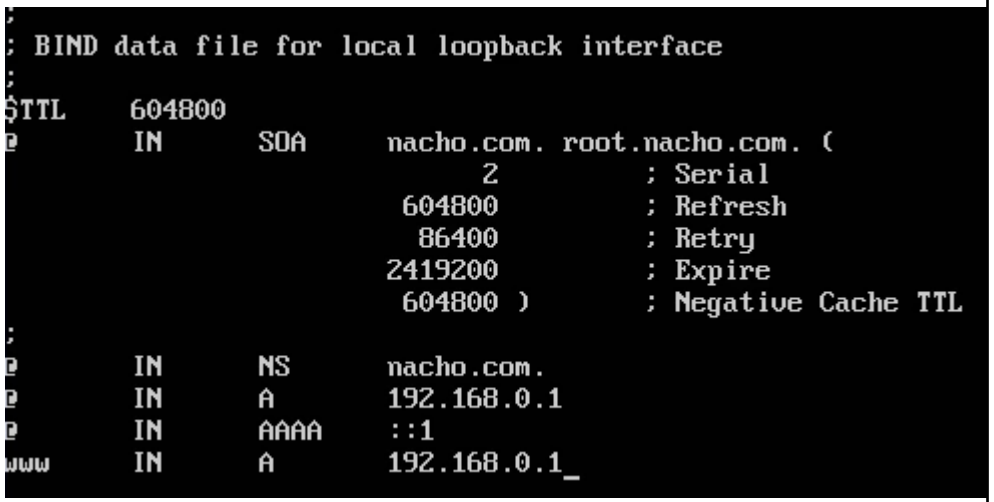
- **Inicio de autoridad, Start Of Authority (SOA)** es un tipo de registro que especifica información del DNS. Todos los nombres de dominios tienen un registro **SOA** que muestra las características básicas del dominio y de la zona en la que se encuentra.

  El registro de recursos SOA indica que este servidor de nombre DNS es la mejor fuente de información de los datos para este dominio. Dependiendo del sistema/servidor, podremos configurar el DNS mediante la edición de un archivo o a través de GUI.

9. Zonas de autoridad

Zonas o mapas de dominio

➢ Inicio de autoridad, Start Of Authority (SOA)

Sintaxis SOA (Linux)	GUI servidores de CDmon	Archivo de configuración BIND (Linux)
FQDN_dominio IN SOA FQDN_servidor ***correo_administrador*** *(* ***num_serie*** *; comentario* ***actualizacion*** *; comentario* ***reintentos*** *; comentario* ***caducidad*** *; comentario TTL) ; comentario*		


```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     nacho.com. root.nacho.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      nacho.com.
@       IN      A       192.168.0.1
@       IN      AAAA    ::1
www     IN      A       192.168.0.1_
```

9. Zonas de autoridad

Zonas o mapas de dominio

➢ Inicio de autoridad, Start Of Authority (SOA)

- **correo_administrador.** Email del administrador de zona del dominio.
- **num_serie**. Número de serie del archivo de zona, aumenta con cada actualización.
- **caducidad** (Expire Time). Indica el tiempo, en segundos, de la información acerca de la zona en un servidor secundario.
- **TTL** (Time To Live). Especifica el tiempo, en segundos, que tardara el servidor en descartar los datos de zona si no ha podido contactar con el servidor primario. Normalmente será elevado este tiempo.
- **actualización** (refresh): número de segundos que un servidor de nombre secundario debe esperar para comprobar de nuevo los valores de un registro.
- **reintento** (retry): número de segundos que un servidor de nombre secundario debe esperar después de un intento fallido de recuperación de datos del servidor primario.

9. Zonas de autoridad

Zonas o mapas de dominio

- **Servidor de nombres (NS)**
  - Establece los servidores de nombres autorizados para la zona.
  - Cada zona debe tener registros indicando tanto los servidores de nombres primarios como los secundarios.
  - Cada zona debe tener al menos un registro NS.
  - Debe tener un registro NS por cada subdominio delegado.

FQDN_propietario IN NS FQDN_servidor

- **FQDN_propietario**. Puede ser el dominio que define el servidor que se indica o el subdominio que se delega en el servidor que se indica.

9. Zonas de autoridad

Zonas o mapas de dominio

- **Servidor de nombres (NS)**
  - **FQDN_servidor**. Es el FQDN del servidor que se está definiendo en el registro.
    - – Terminan en punto para indicar que su origen está en la raíz.
    - – Pueden comenzar por @ para indicar “nombre de dominio”. Si se omite, se hace referencia al dominio implícito.
- Ejemplo de **servidor primario y secundario**:
  micentro.edu. IN NS svdns.micentro.edu.
  micentro.edu. IN NS svdnssec.micentro.edu.
- Ejemplo de **delegación**:
  dpto1.micentro.edu. IN NS svdns.dpto1.micentro.edu.

9. Zonas de autoridad

Zonas o mapas de dominio

➢ Registro de Dirección (A)

- Establece una **correspondencia entre un FQDN y una dirección IP**.
- Cada registro **A** identifica un nombre de máquina y el cliente DNS puede obtener a través de él su dirección IP. Es el tipo de registro más importante y numeroso.
- Si un host dispone de más de una interfaz de red, deberá tener un registro **A** por cada una de ellas.
- Todo nombre de host resuelto por DNS debe especificarse mediante un registro de dirección:

FQDN_máquina IN A dir_IP

9. Zonas de autoridad

Zonas o mapas de dominio

➢ Registro de Dirección (A)

FQDN_máquina IN A dir_IP

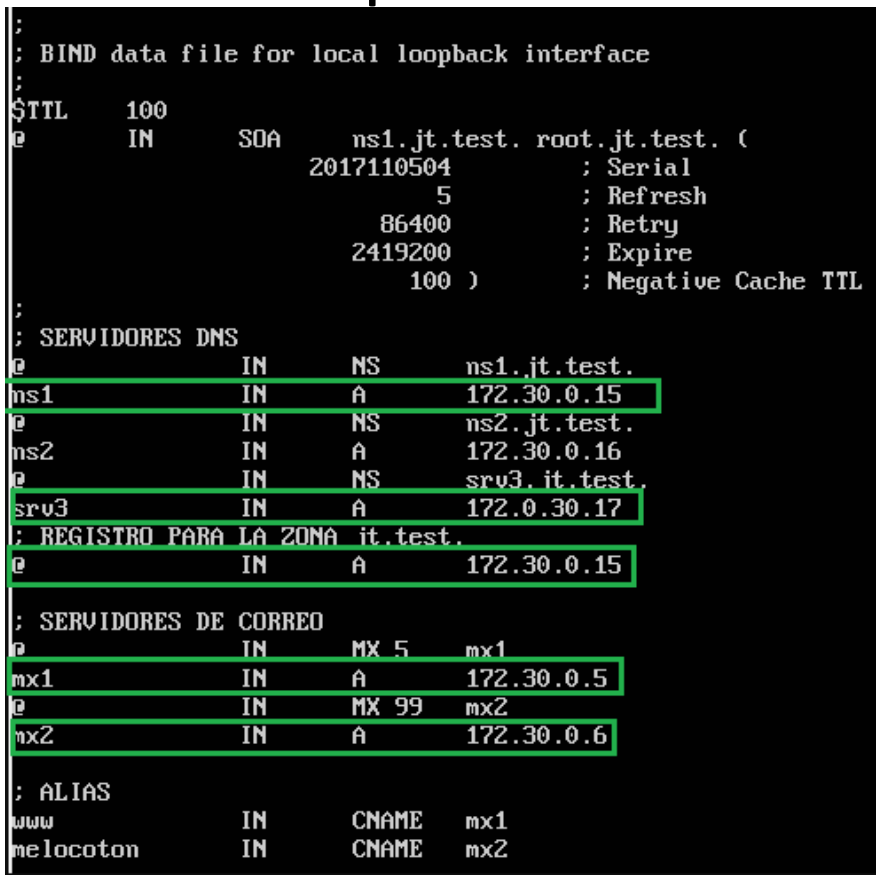
- **FQDN_máquina**. Nombre completamente cualificado que vamos a asociar a una IP.
- **dir_IP**. Dirección IP que asociamos al nombre.

Ejemplos:

pc01.micentro.edu. IN A 192.168.10.21

www.miempresa.com. IN A 10.0.0.1

ftp.miempresa.com. IN A 10.0.0.1



9. Zonas de autoridad

Zonas o mapas de dominio

- **Registro de Puntero (PTR)**

El registro de recurso PTR (puntero) **hace lo contrario que el registro A**, es decir, **asigna una dirección IP a un FQDN**. Este tipo de recursos sólo se usa en el archivo que define la zona de resolución inversa.

Para definir la resolución inversa el sistema DNS tiene un dominio especial llamado in-addr.arpa.

Los subdominios de este dominio tienen nombre numérico y corresponden a los valores decimales de las direcciones IP pero en orden inverso. Así, podríamos decir que la dirección IP 192.168.10.21 tiene el FQDN en el dominio in-addr.arpa 21.10.168.192.in-addr.arpa.

9. Zonas de autoridad

Zonas o mapas de dominio

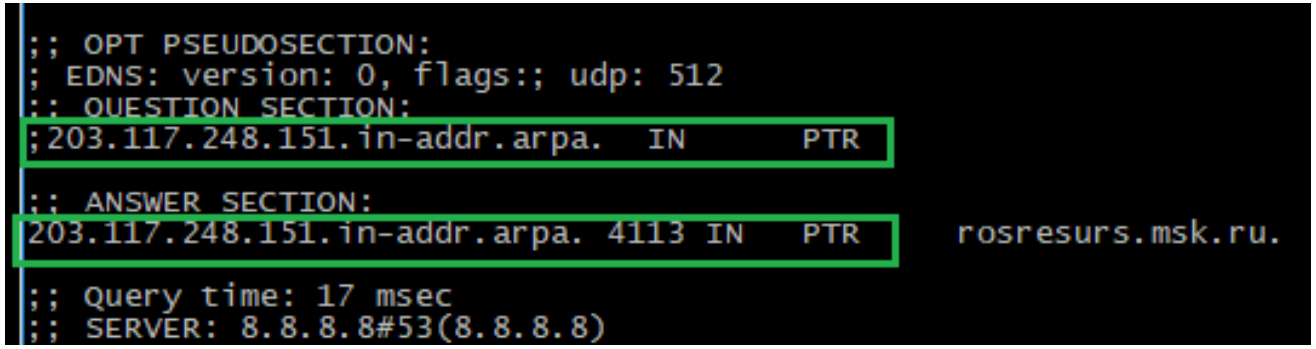
- **Registro de Puntero (PTR)**

Para cada equipo en el dominio necesitamos una entrada PTR en el archivo de resolución inversa.

FQDN_in.addr.arpa. IN PTR FQDN_máquina

Ejemplo:

21.10.168.192.inaddr.arpa. IN PTR pc01.micentro.edu.



9. Zonas de autoridad

Zonas o mapas de dominio

- **Registro de Nombre Canónico(CNAME)**

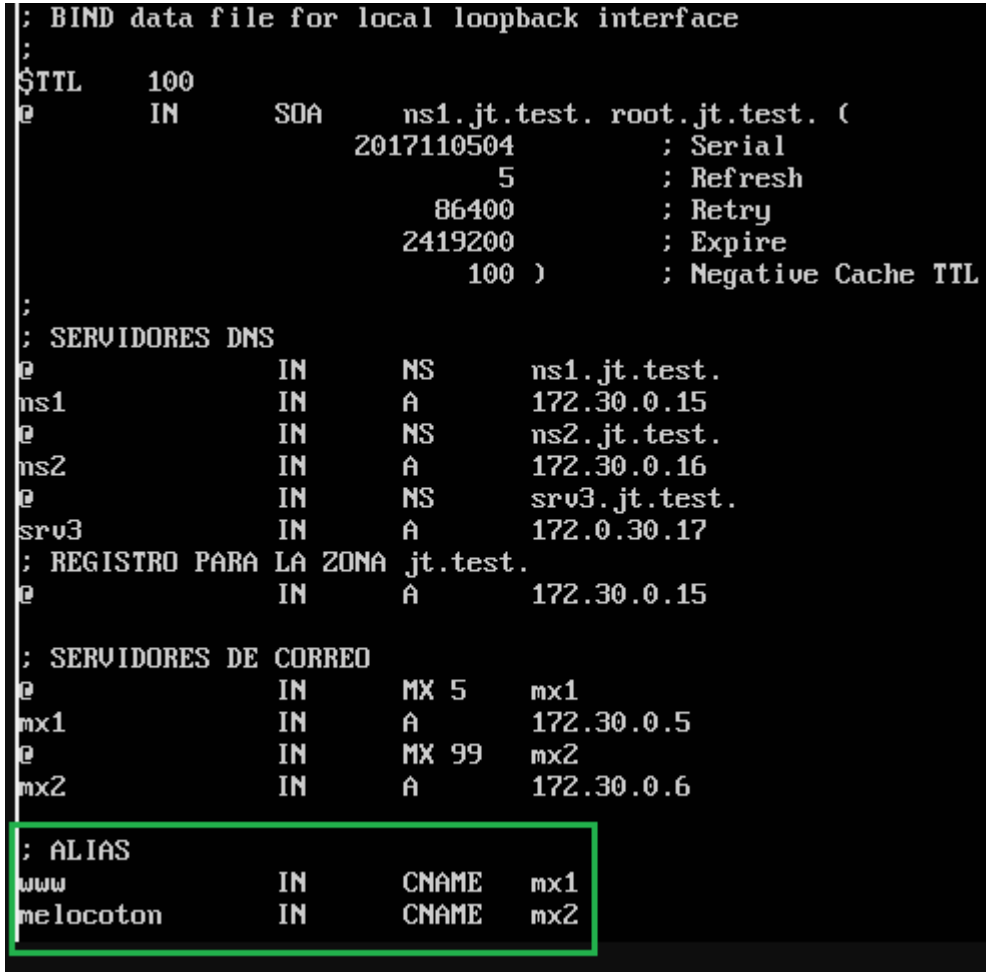
Crea un **alias** para un FQDN, es decir, añade otro nombre a una máquina que ya tiene un FQDN.

FQDN_nuevo IN CNAME FQDN_existente

Ejemplo:

mail.miempresa.com. IN CNAME www.miempresa.com.

La dirección de mail.miempresa.com es la misma que www.miempresa.com



9. Zonas de autoridad

Zonas o mapas de dominio

- **Registro de Intercambio de Correo (MX)**

- Indica qué máquina o máquinas se encargan de la entrega de correo en el dominio.
- Si el domino tiene varios servidores de correo, se indica la prioridad con un valor numérico (el correo se dirige hacia la máquina con menor valor, cuanto más bajo sea el valor mayor será la prioridad).
- El servidores de correo principal es mail.micentro.edu y el secundario es auxmail.micentro.edu.
- Número más bajo mayor prioridad (0 , 10).

FQDN_dominio IN MX prioridad FQDN_sv_correo.

Ejemplos:

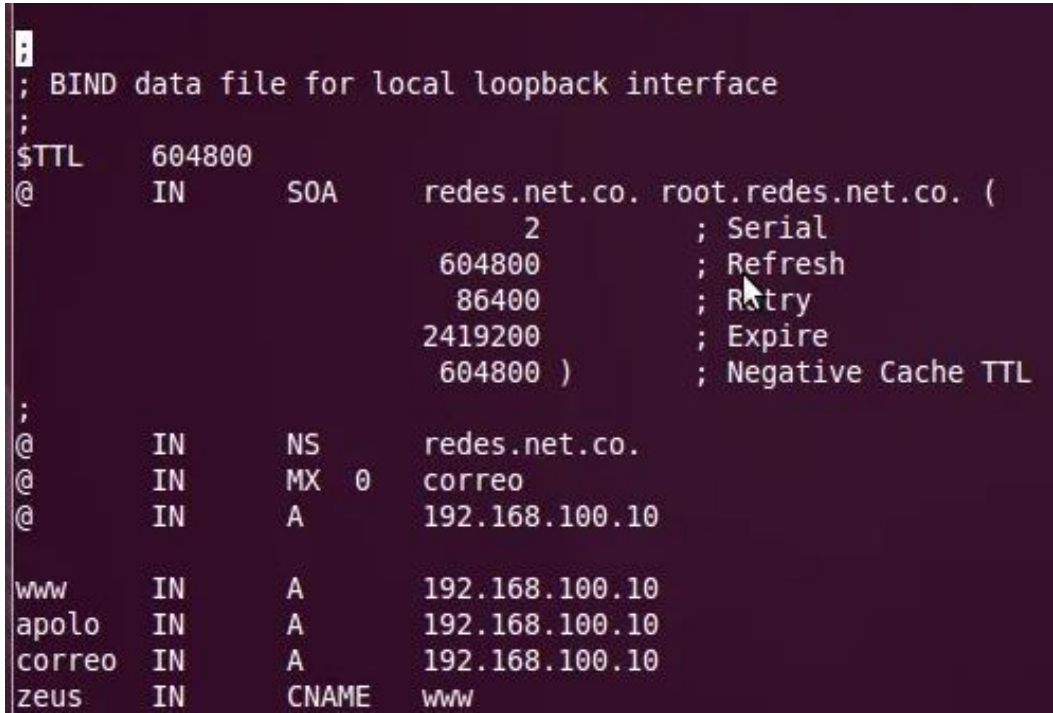
micentro.edu. IN MX 0 mail.micentro.edu.

micentro.edu. IN MX 10 auxmail.micentro.edu.

Actividad de aula – Revisión fichero BIND

Dado la siguiente imagen de un fichero BIND, resuelve las cuestiones:

1. ¿Cuál es el nombre del servidor de nombres autorizado para la zona?
2. La dirección zeus, ¿a qué nombre de máquina equivale?
3. ¿Cuál es la ip de zeus?
4. Añade una línea al fichero para añadir un servidor de correo secundario.



```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     redes.net.co. root.redes.net.co. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      redes.net.co.
@       IN      MX  0   correo
@       IN      A       192.168.100.10

www     IN      A       192.168.100.10
apolo   IN      A       192.168.100.10
correo  IN      A       192.168.100.10
zeus    IN      CNAME   www
```

9. Zonas de autoridad

Zonas o mapas de dominio

- **Registro de servicio (SRV)**

Especifica los servidores disponibles para un servicio o protocolo determinados, como www o ftp.

servicio.protocolo.FQDN_dominio IN SRV prioridad peso puerto FQDN_servidor

- **servicio**: nombre del servicio (http, telnet, etc.).
- **protocolo**: protocolo usado (tcp, udp).
- **prioridad**: valor numérico que se usa de forma similar a la prioridad usada en los registros tipo MX.
- **peso**: valor que permite un balanceo de equilibrio de carga, para repartir el trabajo equitativamente.
- **puerto**: puerto de la máquina en la que se ofrece el servicio.

http.tcp.micentro.edu. IN SRV 0 0 80 www.micentro.edu.

9. Zonas de autoridad

Ejemplo 1.1 de archivo de zona directa:

```
;Fichero Configuración
;Datos autorizados para micentro.edu
;
micentro.edu. IN SOA      servidor.micentro.edu. correo_admin.micentro.edu. (
                          2009112801          ; número de serie
                          3H                  ; Refrescar cada 3 horas
                          15M                 ; reintentos 15 minutos
                          1W                  ; caducidad 1 semana
                          1D )                ; TTL por defecto 1 día
;Servidores de correo
;
micentro.edu.     IN      MX      mail.micentro.edu.
; Servidores de nombres
;
micentro.edu.     IN      NS      dns.micentro.edu.
micentro.edu.     IN      NS      dns2.micentro.edu.
```

Actividad de aula – Modificar fichero BIND

Ejemplo 1.1 de archivo de zona directa:

Dado el archivo BIND de la diapositiva anterior, ¿qué cambios habría que hacer en él para?

1. Cambiar actualización del servidor de nombre para que espere 4 horas para comprobar de nuevo los valores de un registro.
2. La IP del servidor de correos de la zona es 192.168.10.20.
3. El servidor autoritario de la zona tiene la IP 192.168.10.1.
4. El servidor DNS primario tiene la IP 192.168.10.11.
5. El servidor DNS secundario tiene la IP 192.168.10.12.
6. Añade al fichero los alias:

router.micentro.edu. = servidor.micentro.edu.

www.micentro.edu. = servidor.micentro.edu.

9. Zonas de autoridad

Preguntas inversas:

- Los clientes DNS también pueden formular preguntas inversas, es decir, conocer el nombre de dominio dada una dirección IP. Para evitar una búsqueda exhaustiva por todo el espacio de nombres de dominio, se ha creado un **dominio especial llamado in-addr.arpa**.

- Cuando un cliente DNS desea conocer el nombre de dominio asociado a la dirección IP w.x.y.z formula una pregunta inversa a z.y.x.w.in-addr.arpa.

- La inversión de los bytes es necesaria debido a que los nombres de dominio son más genéricos por la derecha, al contrario que ocurre con las direcciones IP.

9. Zonas de autoridad

Ejemplo 2.1 de archivo de zona inversa:

10.186.192.inaddr.arpa IN SOA servidor.micentro.edu. mail_admin.micentro.edu. (
2009112801 ; número de serie
3H ; actualización 3 horas
15M ; reintentos 15 minutos
1W ; caducidad 1 semana
1D) ; TTL por defecto 1 día
micentro.edu. IN NS dns.micentro.edu.
micentro.edu. IN NS dns2.micentro.edu.
1.10.186.192.inaddr.arpa IN PTR servidor.micentro.edu.
1.10.186.192.inaddr.arpa IN PTR router.micentro.edu.
1.10.186.192.inaddr.arpa IN PTR www.micentro.edu.
11.10.186.192.inaddr.arpa IN PTR dns.micentro.edu.
12.10.186.192.inaddr.arpa IN PTR dns2.micentro.edu.
20.10.186.192.inaddr.arpa IN PTR mail.micentro.edu.

9. Zonas de autoridad

Ejemplo 2.2 de archivo de zona inversa:

```
$ORIGIN 10.168.192.inaddr.arpa.
@ IN SOA servidor.micentro.edu. correo_admin.micentro.edu. (
2009112801 ; número de serie
3H ; actualización 3 horas
15M ; reintentos 15 minutos
1W ; caducidad 1 semana
1D ) ; TTL por defecto 1 día
IN NS dns.micentro.edu.
IN NS dns2.micentro.edu.
1 IN PTR servidor.micentro.edu.
1 IN PTR router.micentro.edu.
1 IN PTR www.micentro.edu.
1 IN PTR dns.micentro.edu.
12 IN PTR dns2.micentro.edu.
20 IN PTR mail.micentro.edu.
```

Prácticas DNS

Ver en Aula Virtual todas las prácticas de **DNS**. Se realizarán en máquina virtual, **con Virtual Box**, en ambos servidores Ubuntu y Windows.

10. Servicio de directorios

10. Servicio de directorios

Directorio: Es una base de datos que almacena información sobre los recursos o las entidades como usuarios, ordenadores o impresoras.

Servicio de directorios: Conjunto de aplicaciones que almacena, organiza y gestiona la información sobre los usuarios y los recursos de una red.

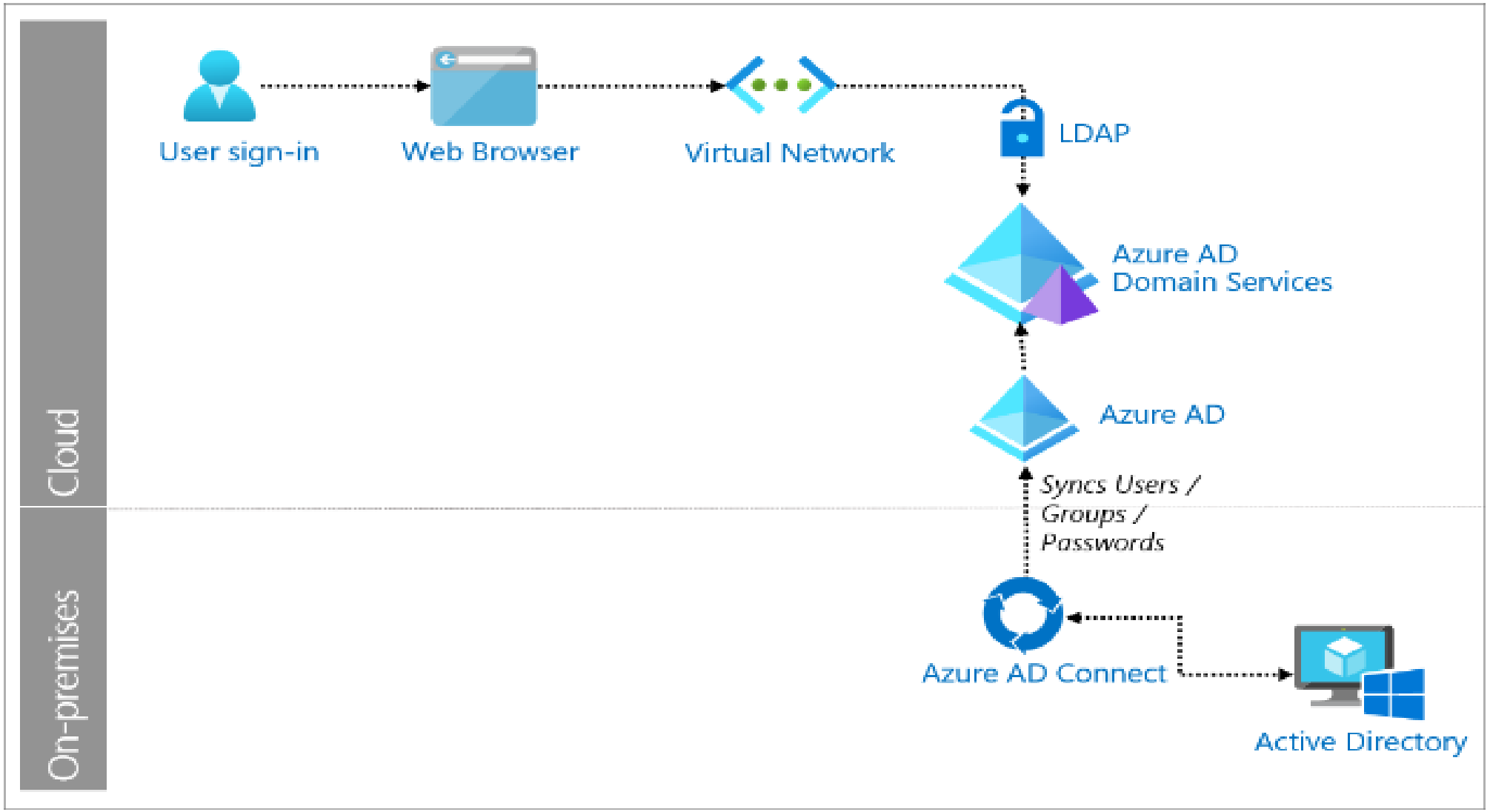
- **Características**: Uno o más servidores contienen los datos que conforman la información del **árbol del directorio.** El cliente se conecta a los servidores y les preguntas. Los servidores responden con una respuesta o un punto donde el cliente puede obtener información adicional.

10. Servicio de directorios

Protocolos principales:

- **LDAP** *(protocolo ligero de acceso a directorios):* protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
- **Kerberos**: protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.
- **DNS y DHCP**: Servicios que ya conocemos un poco mejor.

10. Servicio de directorios



10. Servicio de directorios

Explicación imagen anterior:

•Los usuarios llegan a la página de inicio de sesión de la aplicación web con la que trabajan e intentan un inicio de sesión con su nombre de usuario y contraseña proporcionados por el sistema LDAP de su empresa.

•La página de inicio de sesión de la aplicación enviará de forma segura las credenciales de inicio de sesión (encriptadas y con hash en algún formato acordado) a la URL de "autenticación remota" proporcionada por Azure.

• Azure Active Directory autenticará al usuario y luego lo redirigirá a nuestro sitio con el "estado de autenticación“ KO/OK.

• La página de la aplicación web analizará el "estado de autenticación" y aceptará al usuario como conectado o no.

10. Servicio de directorios

Servicios de directorios más conocidos:

- Microsoft Active Directory
- Red Hat Directory Server / Fedora Directory Server
- Oracle Directory Server Enterprise Edition
- LDAP (Lightweight Directory Access Protocol)

11. LDAP

LDAP *(Lightweight Directory Access Protocol o Protocolo Ligero de Acceso a Directorios)* es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

11. LDAP

Funciones de LDAP

Estas son algunas de las funciones que podemos aplicar con LDAP:

- Empleo como sustituto para el servicio NIS.
- Autenticación de usuarios de aplicaciones web.
- Autenticación de usuarios de sistemas operativos.
- Autenticación de usuarios con NFS en redes Unix.
- Autenticación de usuarios con Samba en redes heterogéneas.
- Encaminamiento de correo (postfix, sendmail).
- Libretas de direcciones para clientes de correo como Mozilla, Evolution y Outlook.
- Administración de descripciones de zona para un servidor de nombres BIND9.

11. LDAP

Estructura del Árbol de Directorio (DIT)

DIT (Directory Information Tree ó Arbol de Información del Directorio) es la estructura de un servidor LDAP donde las ramas de árbol pueden ser contenedores o hojas.

Los contenedores pueden a su vez contener otros objetos. Tales clases de objetos son **root** (el elemento raíz del árbol de directorios, que no existe realmente), **c** (país), **ou** (unidad organizativa) y **dc** (componente de dominio). Este modelo es comparable con los directorios (carpetas) de un sistema de archivos.

Las **hojas** contienen la parte final de una rama y no contienen objetos. Algunos ejemplos serían: person, InetOrgPerson o groupofNames.

11. LDAP

Estructura del Árbol de Directorio (DIT)

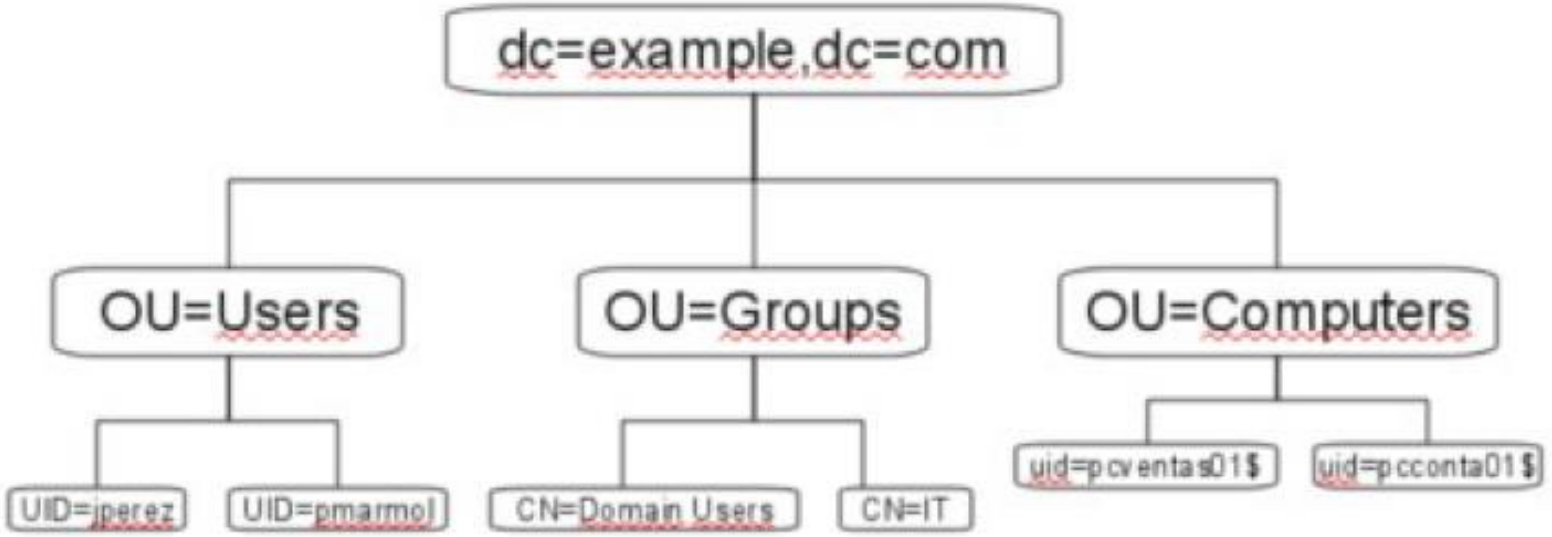
Las **clases de objeto** que vamos a tener en nuestro árbol van a ser:

- **dcObject**: Objeto domainComponent o componentes del nombre del dominio. Atributo obligatorio: **dc**
- **organizationalUnit**: Unidad organizativa. Atributo **ou**.
- **InetOrgPerson**: Datos relacionados con la persona para la intranet o Internet. Atributos **sn** y **cn**.

Cada entrada en el árbol posee un identificador único llamado Distinguished Name o DN.

11. LDAP

- **dc**=profesordeinformatica,dc=com (Raíz del directorio
- **ou**=Users (Contenedor para almacenar cuentas de usuario para sistemas Linux/Unix y Windows)
- **ou**=Computers (Contenedor para las cuentas de Ordenadores para sistemas Windows (los de Linux serían Hosts))
- **ou**=Groups (Contenedor para alamacenar Grupos de sistema para sistemas Unix y Windows)



11. ¿Qué es el Active Directory?

Active Directory (AD) es el términos que utiliza **Microsoft** para referirse a su implementación de servicio de directorio en una red distribuida de computadoras. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

De forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de **administrar los inicios de sesión en los equipos** conectados a la red, así como también la administración de políticas en toda la red.

11. ¿Qué es el Active Directory?

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera.

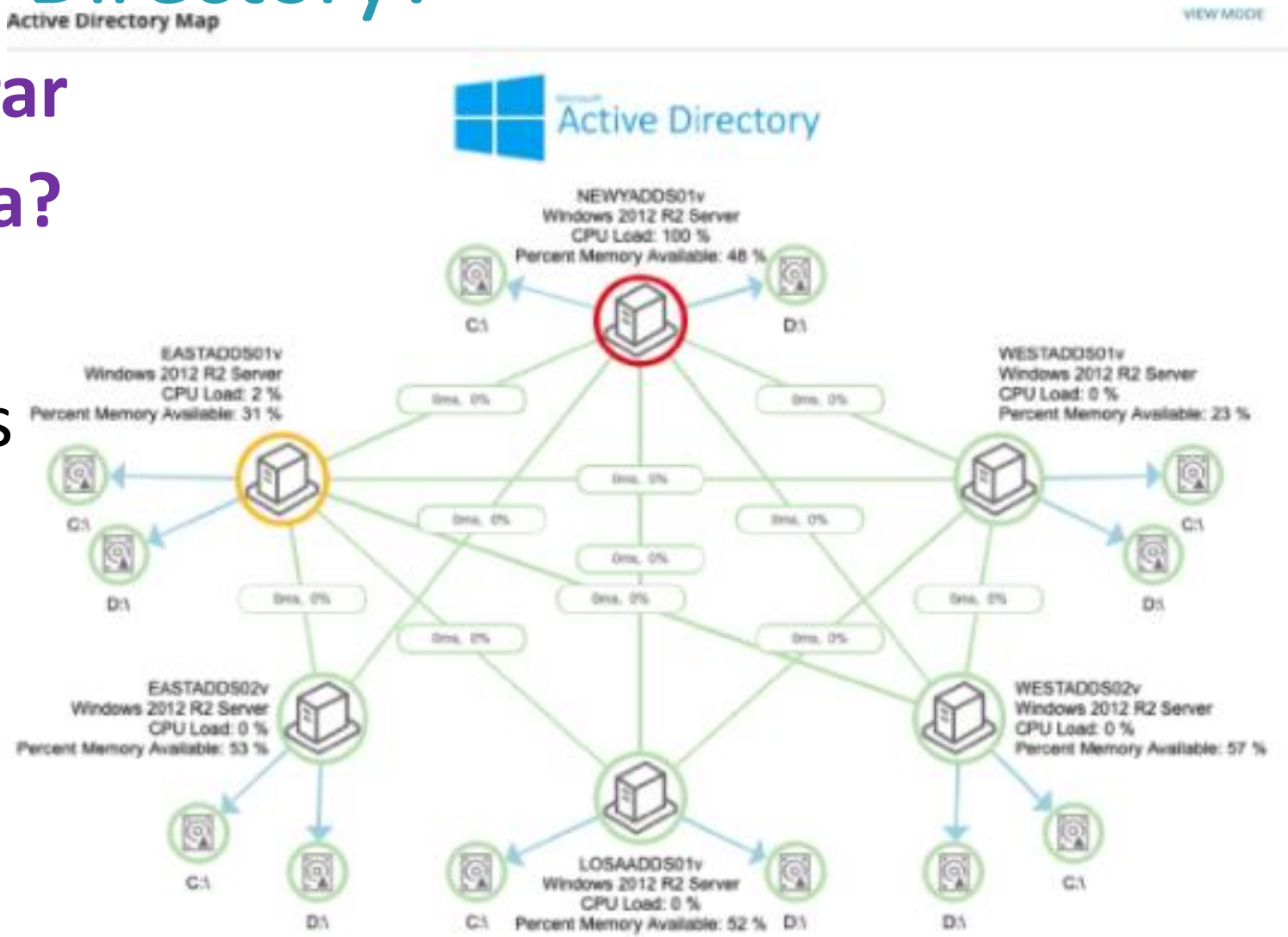
Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

Más información en recursos extra.

11. ¿Qué es el Active Directory?

¿Y si pudiéramos configurar Active Directory en el aula?

Solo con identificarnos con user/pass, tendríamos directamente acceso a AulaVirtual, Mirador y al correo de educación.



Vídeo explicativo ->
https://www.youtube.com/watch?v=gmMXfkF6uMs

Prácticas – Servicios de directorio

Ver en Aula Virtual todas las prácticas de:

- **OpenLDAP** en Ubuntu.
- **Active Directory** en Windows.

Se realizarán en máquina virtual, **con Virtual Box**, en ambos servidores Ubuntu y Windows.