TEMA 1.
SERVICIO DE NOMBRES DE DOMINIO DNS

ÍNDICE

1. Definición de DNS
2. Ventajas y riesgos
3. Espacio de nombres de dominio
4. Conceptos básicos: FQDN, dominio, TLD, URL, ...
5. Organismos de gestión de dominios
6. Delegación de dominios. Zonas
7. Tipos de servidores DNS
8. Funcionamiento del sistema DNS
9. Ficheros de zona
10. DDNS

1. DEFINICIÓN DE DNS

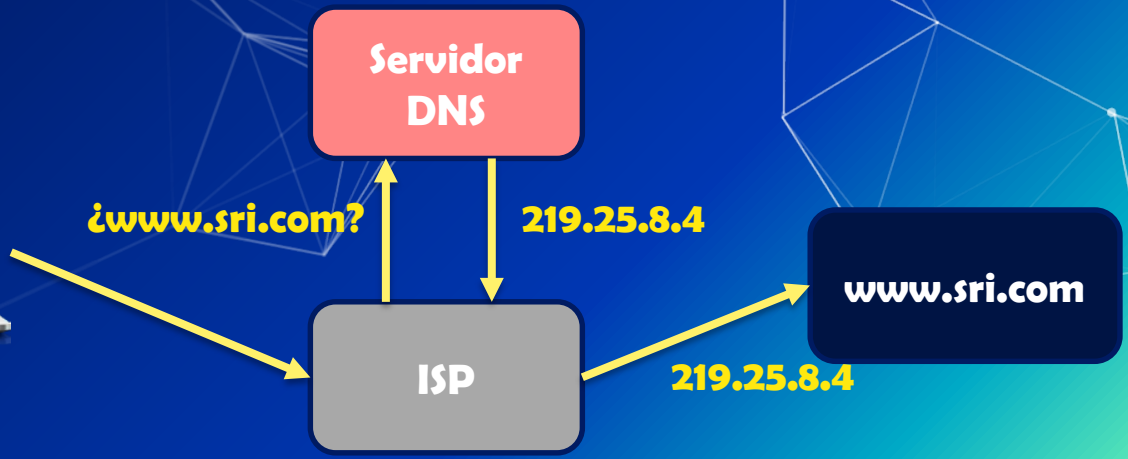
- Internet se basa en direcciones IP numéricas
- Es más fácil recordar nombres que números
- Conversión entre nombres y direcciones IP

SERVICIO DNS

¡OJO!
También traducción inversa

1. DEFINICIÓN DE DNS

- DNS: Domain Name Server
- DNS se originó en Arpanet (1969)
- Fue un sistema ideado por Paul Mockapetris (1983)



2. VENTAJAS Y RIESGOS

Ventajas

- Comodidad: no hay que recordar decenas de direcciones IP
- Fiabilidad: los cambios en las direcciones IP de los servidores se registran en los servidores DNS

2. VENTAJAS Y RIESGOS

Riesgos

- DDoS: ataques de denegación de servicios distribuidos a los servidores DNS
- Cache poisoning o DNS spoofing: modificación por parte de un intruso de los datos del DNS almacenados en caché
- Typosquatting: construcción de nombres de dominio falsos similares a dominios reales

3. ESPACIO DE NOMBRES DE DOMINIO

Espacio de nombres de dominio

Está formado por los nombres válidos utilizados para identificar servicios o máquinas en una red. Se puede representar mediante una estructura en forma de árbol, es decir, todos los nombres forman un árbol invertido donde cada nodo se separa de los otros nodos por un punto (.)

En los nombres no se distinguen mayúsculas de minúsculas

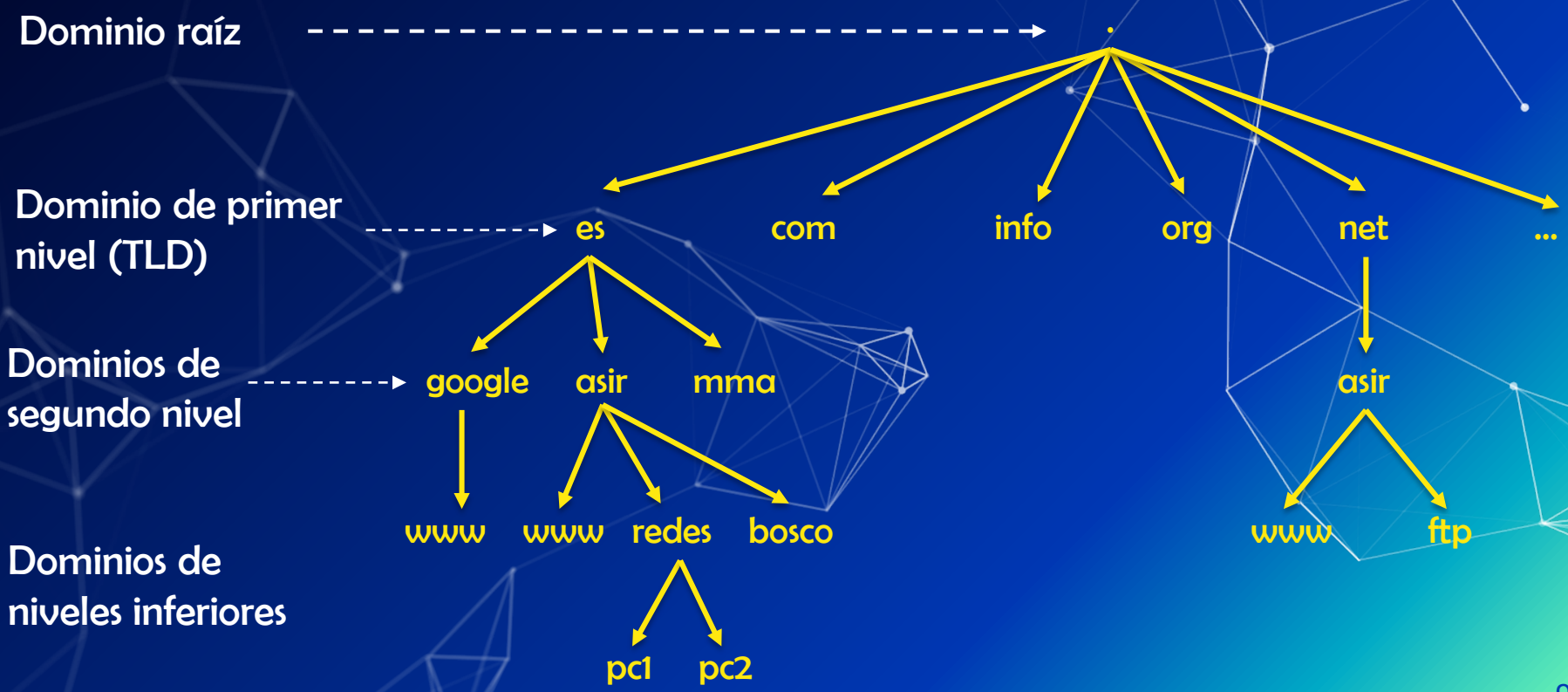
3. ESPACIO DE NOMBRES DE DOMINIO

El servicio DNS utiliza nombres jerárquicos

En los nombres jerárquicos del servicio DNS se separa la información con puntos (ej: www.sri.es.)

Frente a los nombres jerárquicos (que proporcionan información adicional) están los nombres planos (que solo identifican a un elemento de un conjunto, sin información adicional)

3. ESPACIO DE NOMBRES DE DOMINIO



3. ESPACIO DE NOMBRES DE DOMINIO

- Para nombrar un equipo se va navegando recorriendo toda la estructura.

  Ejemplo: pc1.redes.asir.es.

  (¡OJO! El punto final no se suele poner aunque está)

- Cada nivel es administrado por una entidad que establece una normativa concreta

3. ESPACIO DE NOMBRES DE DOMINIO

- Dominio raíz: representado por un punto (.). De ahí parten todos los nombres de dominio.
- Dominios de nivel superior (TLD – Top Level Domain)
  - Dominios genéricos (gTLD): .com, .org, .net, ...
  - Dominios geográficos o de país: .es, .uk, .fr, ...
- Dominios de segundo nivel (SLD): parte personalizable
- Dominios de niveles inferiores: utilizado para organizar el sitio web y quitar carga de la página principal

4. CONCEPTOS BÁSICOS

- FQDN (Full Qualified Domain Name): nombre completo del equipo, que incluye tanto su nombre como el dominio

  Ejemplo: pc1.redes.asir.es.

- Dominio: sirve para nombrar a un conjunto de hosts o subdominios o ambos a la vez, que se agrupan según algún criterio.

4. CONCEPTOS BÁSICOS

- URL (Uniform Resource Locator): dirección única y específica de cada página o recurso de internet

- Zona: conjunto de nombres contiguos asociados a una parte del árbol. Parte del espacio de nombres gestionado por una entidad específica (organización o administrador individual)

4. CONCEPTOS BÁSICOS

Ejemplos:

- https://www.google.com
  - URL: https://www.google.com
  - Protocolo: HTTP
  - FQDN: www.google.com
  - Dominio: google.com
  - Equipo: www
  - TLD: com

4. CONCEPTOS BÁSICOS

Ejemplos:

- ftp://www.webonline.empresa.com:3000
  - URL: ftp://www.webonline.empresa.com:3000
  - Protocolo: FTP
  - FQDN: www.webonline.empresa.com
  - Dominio: webonline.empresa.com
  - Equipo: www
  - TLD: com
  - Puerto: 3000

5. ORGANISMOS DE GESTIÓN DE DOMINIOS

- En un principio la gestión de dominios raíz la llevaba IANA, que luego fue sustituida por la ICANN
- ICANN delega en los registradores acreditados
  - gTLD: autoritativamente administrados por la ICANN
  - ccTLD o geográficos: delegados individualmente a los países
- ESNIC es la autoridad competente para la gestión de registros de dominios .es. Lo hace a través de la entidad Red.es

5. ORGANISMOS DE GESTIÓN DE DOMINIOS

Gestiona el sistema de nombres de dominio

Registry - Registro
Gestionan las extensiones DNS

Registrar – Agentes Registradores
Organizaciones acreditadas que procesan los registros de nombre de dominio

Registrant- Usuario
Propietarios de los nombres de dominio

5. ORGANISMOS DE GESTIÓN DE DOMINIOS

Dominio raíz

Verisign, EURid, PIR, ESNIC, Afnic, ...

IONOS, Arsys, Cdmon, Dinahosting, Hostinet, ...

6. DELEGACIÓN DE DOMINIOS. ZONAS

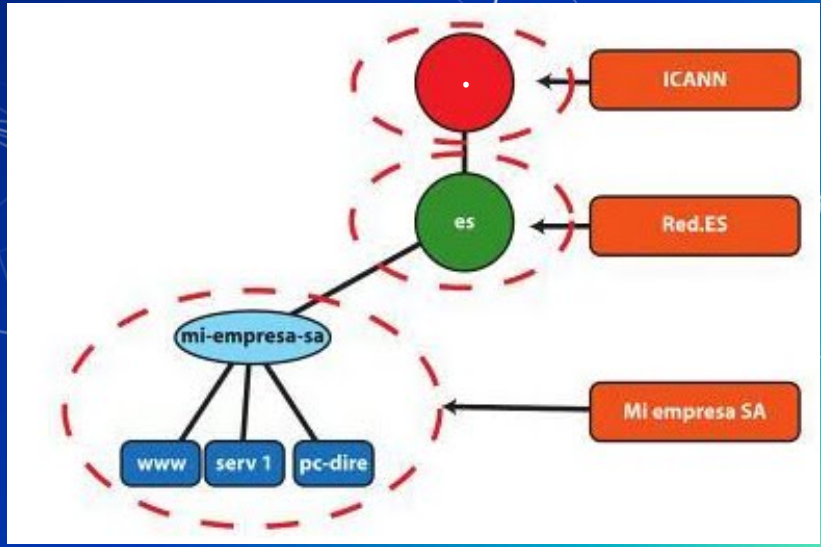
- Esta administración descentralizada se basa en la delegación
- Delegación de dominios DNS: consiste en que la organización que administra un dominio transfiere a otras organizaciones uno, varios o todos los dominios que administra.
- La parte del espacio de nombres administrado por una organización se denomina ZONA

6. DELEGACIÓN DE DOMINIOS. ZONAS

- La ICANN administra el dominio raíz y delega en otras organizaciones los dominios TLD.
- Las organizaciones que administran los dominios TLD, pueden delegar en otras organizaciones los dominios de segundo nivel.
- Y cada organización puede delegar la administración de sus subdominios en otras organizaciones.

6. DELEGACIÓN DE DOMINIOS. ZONAS

- La organización que administra un dominio es la responsable de los nombres usados en ese dominio, las IPs asociadas a dichos nombres y el mantenimiento y la administración de los servidores de nombre que alojan dichos dominios.



7. TIPOS DE SERVIDORES DNS

Servidor primario

Maestro

Servidor principal. Es al que se accede de forma habitual

En él se realizan las altas y bajas de nombres

Servidor secundario

Esclavo

Se recurre a él cuando falla el primario

Copia exacta de la información del primaria

Tolerancia a fallos

Servidor caché

Hace las consultas que le llegan y almacena los resultados en la caché para responder de forma más rápida futuras consultas

7. TIPOS DE SERVIDORES DNS

Servidor reenviador

Forwarder

Si no tiene respuesta a la pregunta se la reenvía a otros servidores DNS

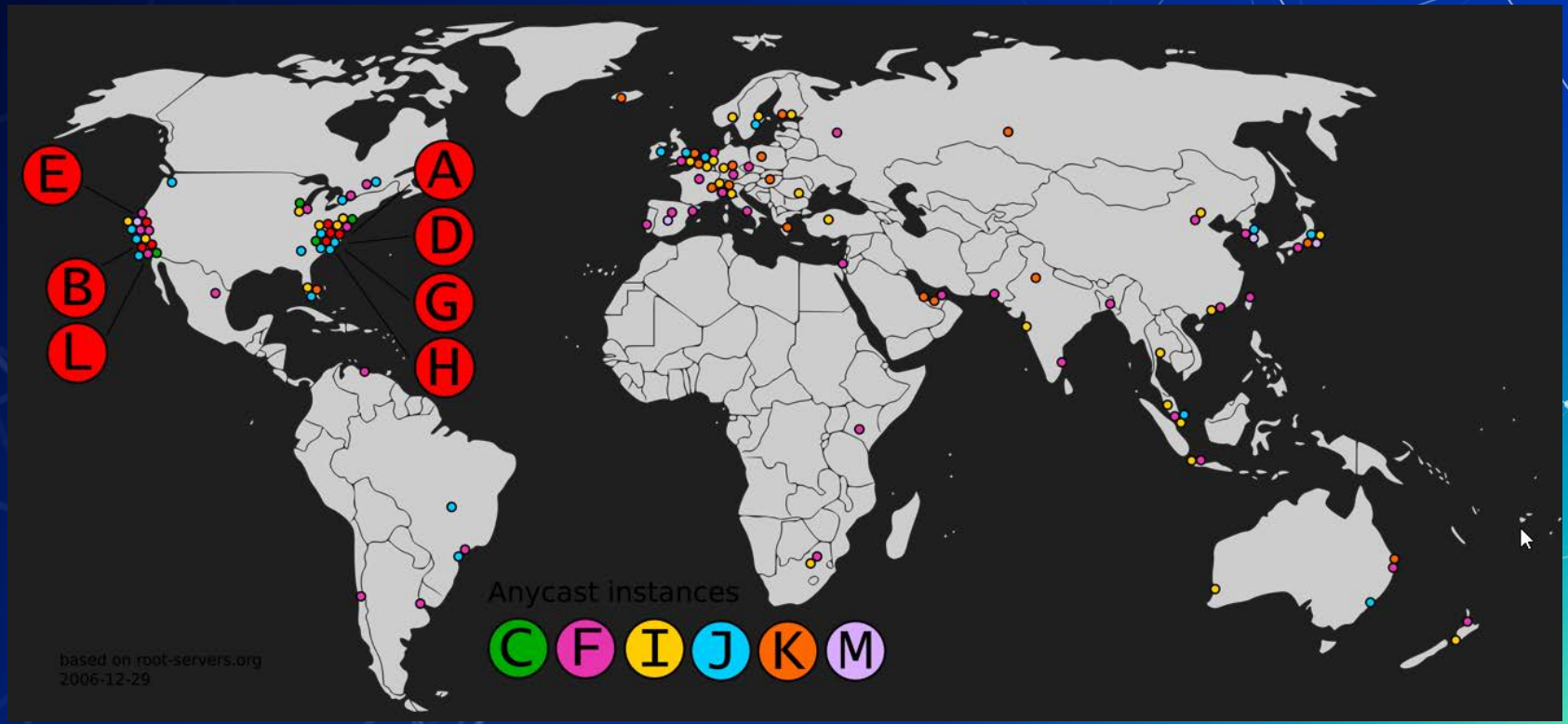
Servidor solo autorizado

Solo responde a preguntas de su zona. No es reenviador y no actúa como caché

Servidor raíz o root

Contienen el fichero de la zona ".". Hay 13 en el mundo conocidos por todos y son responsabilidad de la ICANN

7. TIPOS DE SERVIDORES DNS



7. TIPOS DE SERVIDORES DNS

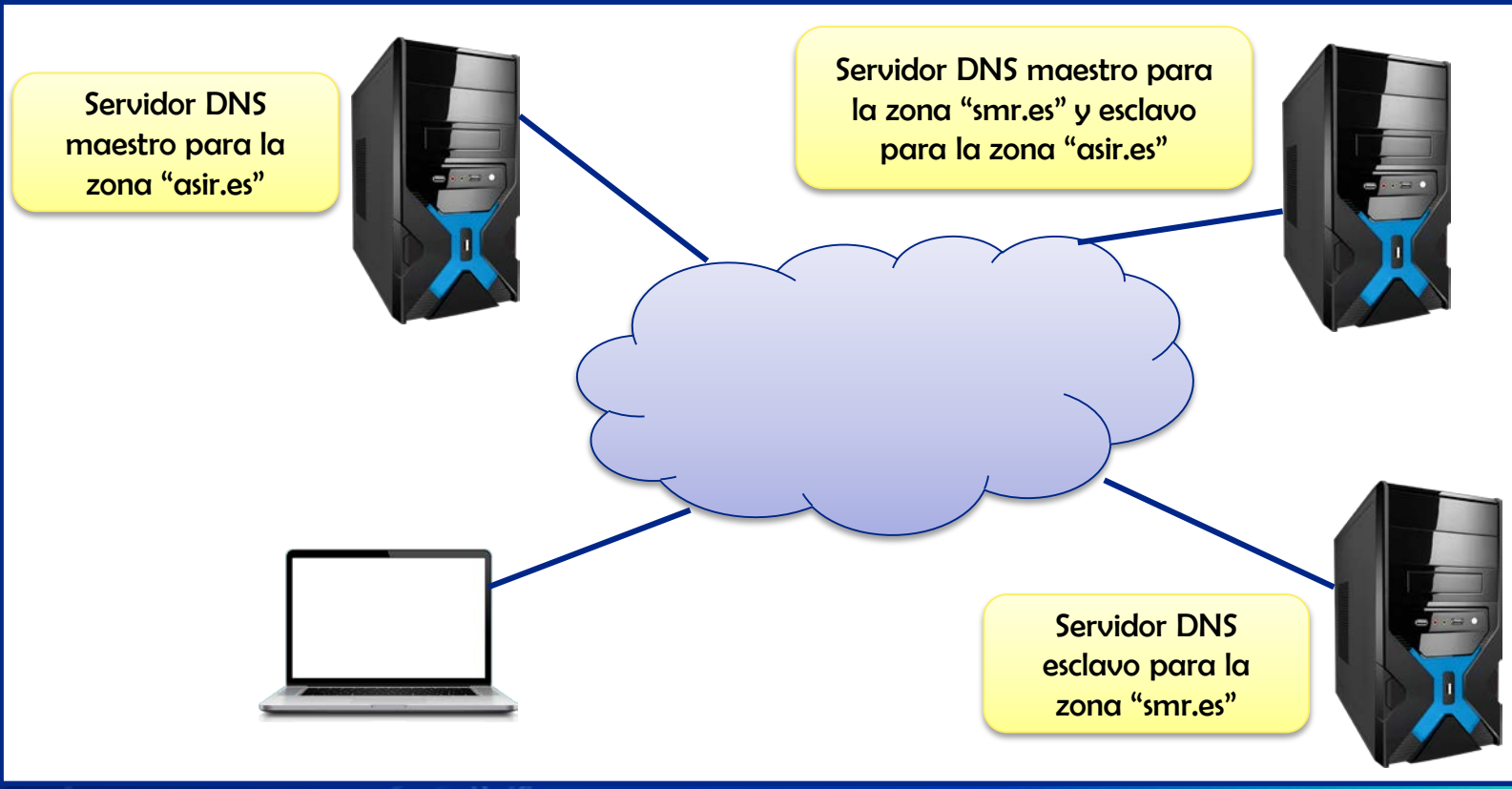
- Por cada zona debe haber un servidor primario y puede haber uno o varios secundarios
- Tanto el primario como el secundario son autoritarios o autoritativos de su zona
- Los servidores caché no son autoritativos

7. TIPOS DE SERVIDORES DNS

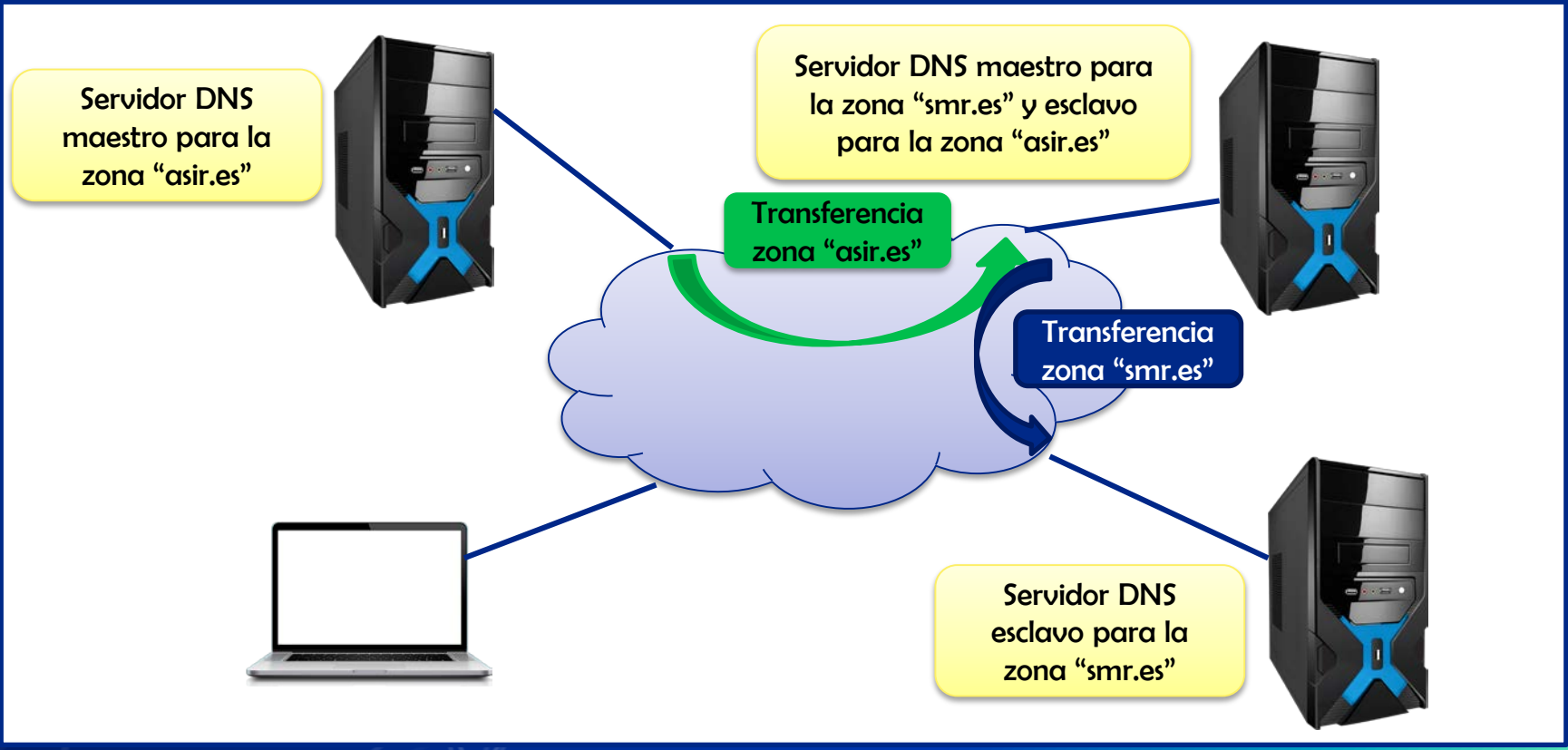
- La información de cada zona se almacena en ficheros de texto
- La información del servidor primario debe ser la misma que la de los servidores secundarios

TRANSFERENCIA DE ZONA

7. TIPOS DE SERVIDORES DNS



7. TIPOS DE SERVIDORES DNS



7. TIPOS DE SERVIDORES DNS

Dos tipos de transferencia de zona:

- Transferencia de zona completa (AXFR)
- Transferencia de zona incremental (IXFR)

Se produce por dos motivos:

- El esclavo pregunta al maestro si hay cambios cada cierto tiempo o al reiniciarse el servicio
- El maestro notifica al esclavo que ha habido cambios (NOTIFY)

8. FUNCIONAMIENTO DEL SISTEMA DNS

1. Una aplicación necesita conocer una dirección IP (navegador, cliente correo, ...)

2. Se comunica con unas librerías del sistema operativo que se encargan de estas funciones (cliente DNS - resolver)

3. El cliente DNS consulta previamente su caché por si ya tuviera respuesta para la consulta DNS

8. FUNCIONAMIENTO DEL SISTEMA DNS

4. Si no tiene esa información en caché la busca en el fichero hosts

5. Si tampoco estuviera allí, pide información al servidor DNS primario que tenga configurado

6. El servidor DNS consultado puede tener la respuesta en caché o en sus propios ficheros de zona

8. FUNCIONAMIENTO DEL SISTEMA DNS

7. Si no la tiene preguntará a otros servidores DNS mediante dos tipos de consultas:
   - Consultas recursivas
   - Consultas iterativas

8. Cuando obtenga la respuesta se la devolverá al cliente DNS o resolver y él a la aplicación correspondiente

8. FUNCIONAMIENTO DEL SISTEMA DNS

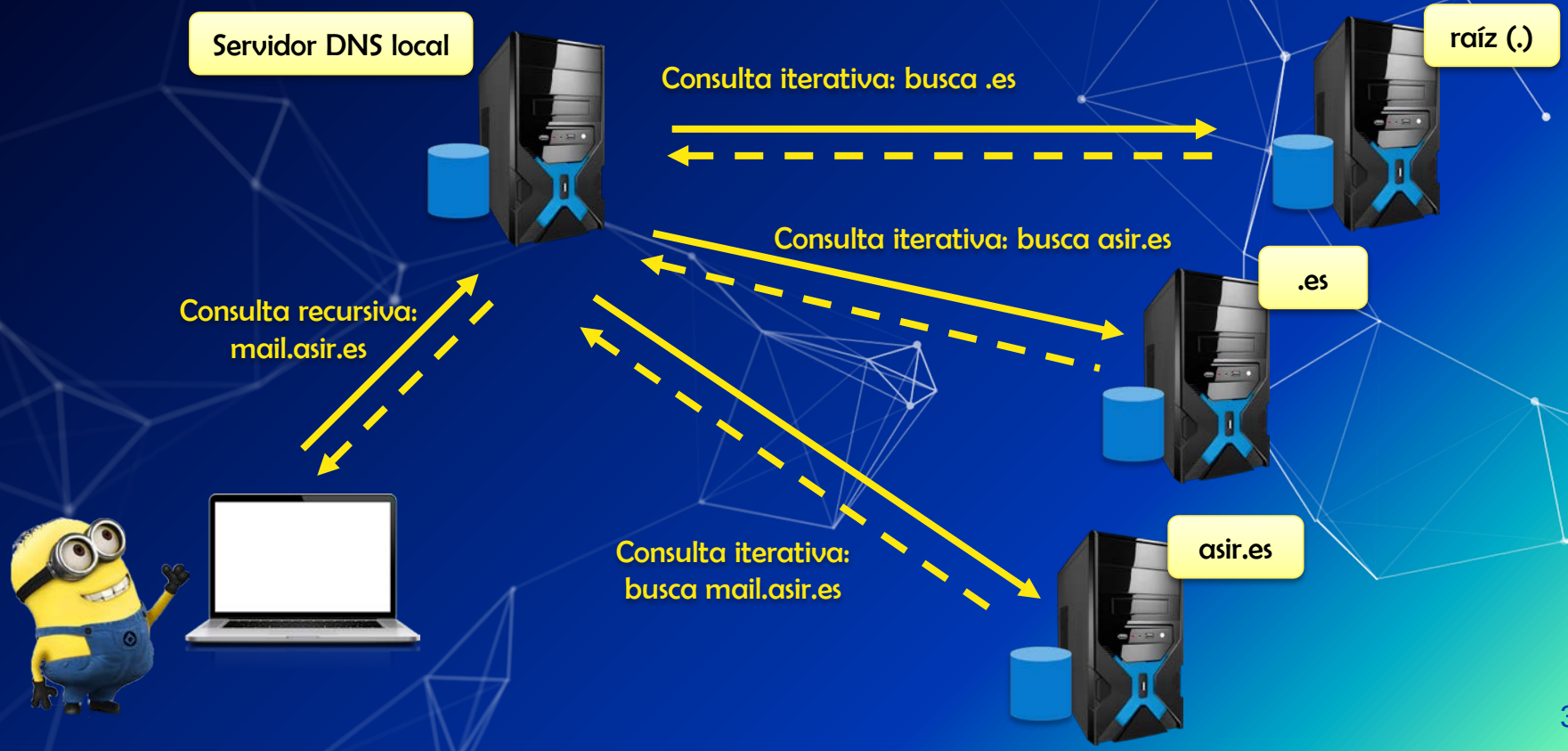
Consultas recursivas

- Se suele dar entre cliente y servidor. Es aquella en la que el servidor DNS da una respuesta completa o exacta.

Consultas iterativas

- Se suele dar entre servidores. El servidor de nombres dará una respuesta parcial a la consulta. El servidor DNS procesa la consulta preguntando a diversos servidores DNS y empezando por los servidores DNS raíz

8. FUNCIONAMIENTO DEL SISTEMA DNS

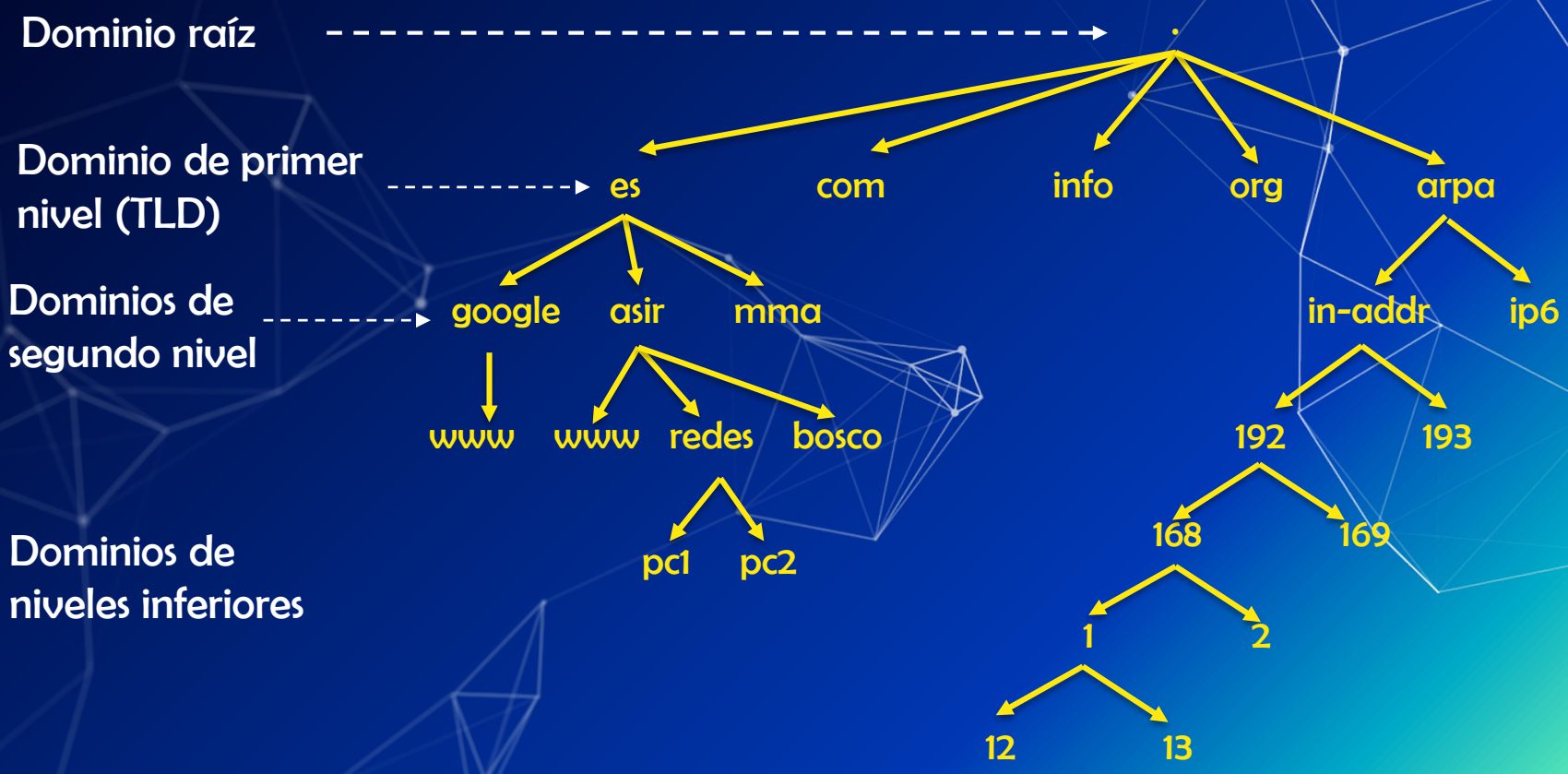


8. FUNCIONAMIENTO DEL SISTEMA DNS

Consultas inversas

- Son aquellas en las que el usuario quiere saber el nombre del dominio asociado a una dirección IP concreta.
- Para estas consultas inversas se utiliza el dominio .arpa
- Las direcciones IP se tratan como direcciones que cuelgan del dominio “in-addr.arpa” para IPv4 y “ip6.arpa” para IPv6

8. FUNCIONAMIENTO DEL SISTEMA DNS



8. FUNCIONAMIENTO DEL SISTEMA DNS

Consultas inversas

- A la hora de preguntar por la dirección 192.168.1.13 realmente estamos buscando el nombre de dominio "13.1.168.192.in-addr.arpa"

- Estos nombres de dominio se almacenarán igual que el resto en ficheros de zona denominados archivos de zona de resolución inversa (PTR)

9. FICHEROS DE ZONA

- La información de las zonas se almacena en una base de datos formada por uno o varios ficheros de texto (ficheros de zona)
- A cada una de las líneas de este fichero se las conoce como registro de recursos (RR: Resource Record)
- Estas líneas definen los tipos de datos y la información del DNS

9. FICHEROS DE ZONA

- Ejemplo de fichero de zona:

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     webebre.net. root.webebre.net. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@                       IN      NS      webebre.net.
webebre.net.            IN      A       192.168.83.1
dns.webebre.net.        IN      A       192.168.83.1
dns2.webebre.net.       IN      A       192.168.83.10
pc1.webebre.net.        IN      A       192.168.83.2
pc2.webebre.net.        IN      A       192.168.83.3
```

9. FICHEROS DE ZONA

Estos ficheros contienen información de distinto tipo:

- **Comentarios:** comienzan por ; y contienen notas aclaratorias
- **Directivas:** valores que especifican aspectos del RR. Comienzan por $. Algunas son:
  - $ORIGIN: nombre de dominio que se incluirá al final de cualquier nombre que se defina en el RR y que no acabe en punto. Directiva no obligatoria
  - $TTL: tiempo predeterminado (en segundos) que un RR es válido

9. FICHEROS DE ZONA

- **Registros de recurso:** definen las diversas entidades dentro del dominio. De forma general el formato es:

```
propietario [TTL] Clase Tipo RDATA
```

propietario: nombre host o dominio.
TTL: tiempo de vida. Si no aparece se usa el valor general
Clase: familia de protocolos en uso. Suele ser IN (Internet)
Tipo: identifica el tipo de registro
RDATA: los datos del registro de recursos

9. FICHEROS DE ZONA

Tipos de registros de recursos

- SOA
- NS
- A
- AAAA
- MX
- CNAME
- PTR

9. FICHEROS DE ZONA

- SOA: define el comienzo de la zona. Se coloca detrás de las directivas y tiene información importante acerca de la autoridad de los RR para la zona. Es obligatorio.

  @ IN SOA <DNS_primario> <email administrador> (

  <numero de serie>

  <tiempo de refresco>

  <tiempo de reintento>

  <tiempo de expiración>

  TTL mínimo)

9. FICHEROS DE ZONA

- NS: define los nombres de los servidores autoritarios para una zona concreta. Obligatorio al menos uno.
  IN NS <nombre del servidor>

- A: define y asigna una dirección IPv4 a un nombre
  <host> IN A <direccion IPv4>

- AAAA: igual que A pero para direcciones IPv6
  <host> IN AAAA <direccion IPv4>

9. FICHEROS DE ZONA

- MX: define un servidor de correo electrónico para el dominio
  IN MX <valor preferencia> <nombre servidor email>

- CNAME: define alias a nombres de dominio. Estos nombres de dominio deben tener un registro A.
  <nombre alias> IN CNAME <nombre real>

- PTR: utilizado en la resolución inversa
  <ip-host> IN PTR <nombre-host>

9. FICHEROS DE ZONA

```
$TTL 2d
$ORIGIN asir.com.
@   IN    SOA   ns.asir.com. hostmaster.asir.com. (
                2010121500  ; serial number
                1d12h       ; refresh = 1 dia 12 horas
                15m         ; refresh retry = 15 minutos
                3w12h       ; expiry = 3 semanas + 12 horas
                2h20m       ; nx = 2 horas + 20 minutos
                )
    IN    NS    ns.asir.com.
    IN    NS    ns.asir.net.

ns  IN    A     192.168.1.1
```

```
$TTL 2d
$ORIGIN asir.com.
prof          IN    A    192.168.1.12
www    4d     IN    A    172.16.0.13
```

```
              IN    MX       mail
mail          IN    A        192.168.1.1
www           IN    CNAME    mail
```

```
$ORIGIN fp.com.
prof        IN    A        192.168.1.12
www         IN    CNAME    prof
ftp         IN    CNAME    prof
```

9. FICHEROS DE ZONA

TIPO	PROP.	RDATA	EJEMPLO
A	FQDN	IP	www.google.com → 83.0.1.2
CNAME	FQDN	FQDN	www.google.com → www.google.es
MX	Dominio de correo	Servidor de correo	gmail.com → serv.mail.google.com
PTR	IP	FQDN	83.0.1.2 → www.google.com
TXT	FQDN	Texto	anuncio.emp.com → "Vendo Opel Corsa"
SOA	Propietario dominio	-	-
NS	Dominio	Servidor DNS	empresa.com → ns1.data.es

10. DDNS

- Servicio que nos permite asociar nuestra IP pública dinámica a un dominio
- El objetivo es permitir conocer la IP de un equipo aunque ésta cambie
- Ejemplos de servicios DynDNS:
  - No-IP (https://www.noip.com)
  - Duck DNS (https://www.duckdns.org)
  - DynDNS (https://account.dyn.com)

10. DDNS

Dirección IP privada

Actualización DDNS

Servidor DDNS

Dirección IP pública

Consulta DDNS

Dirección IP privada

Cliente externo

PRÁCTICAS

- Instalación y configuración de servidor DNS en Linux
- Instalación y configuración de servidor DNS en Windows
- Puesta en marcha y configuración de servidor DNS en entorno cloud
- Configuración de un DNS Dinámico