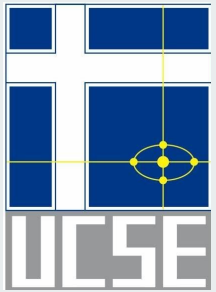
DNS

UCSE - SEIA



El problema que resuelve DNS

- Las computadoras tienen direcciones de red.
- El usuario quiere acceder desde su computadora, a un servicio provisto por otra computadora (ej: con su navegador web entrar a Facebook).
- No podemos esperar que el usuario memorice direcciones de red, pero sí "nombres" humanamente entendibles.

Solución: necesitamos una "libreta de direcciones" que mapee nombres a direcciones de red, y que se mantenga actualizada.

Que el usuario pueda escribir un nombre, y la computadora pueda buscar en qué dirección de red "vive" ese nombre.

Eso es el DNS: el sistema de nombres de dominios

Cómo funciona DNS?

La idea central es esta:

1) Un programa requiere comunicarse con "www.unsitio.com"
2) El programa "resuelve" el dominio: esto es, traduce "www.unsitio.com" a una dirección de red como 192.185.25.217.
3) El programa inicia la comunicación con la computadora que se encuentre en 192.185.25.217.

La parte más importante, donde realmente entra el DNS, es el segundo paso: la resolución de dominio.

Y es un proceso con un poco de complejidad, así que lo vamos a ver de a partes...

Resolver normalmente implica preguntar a otros

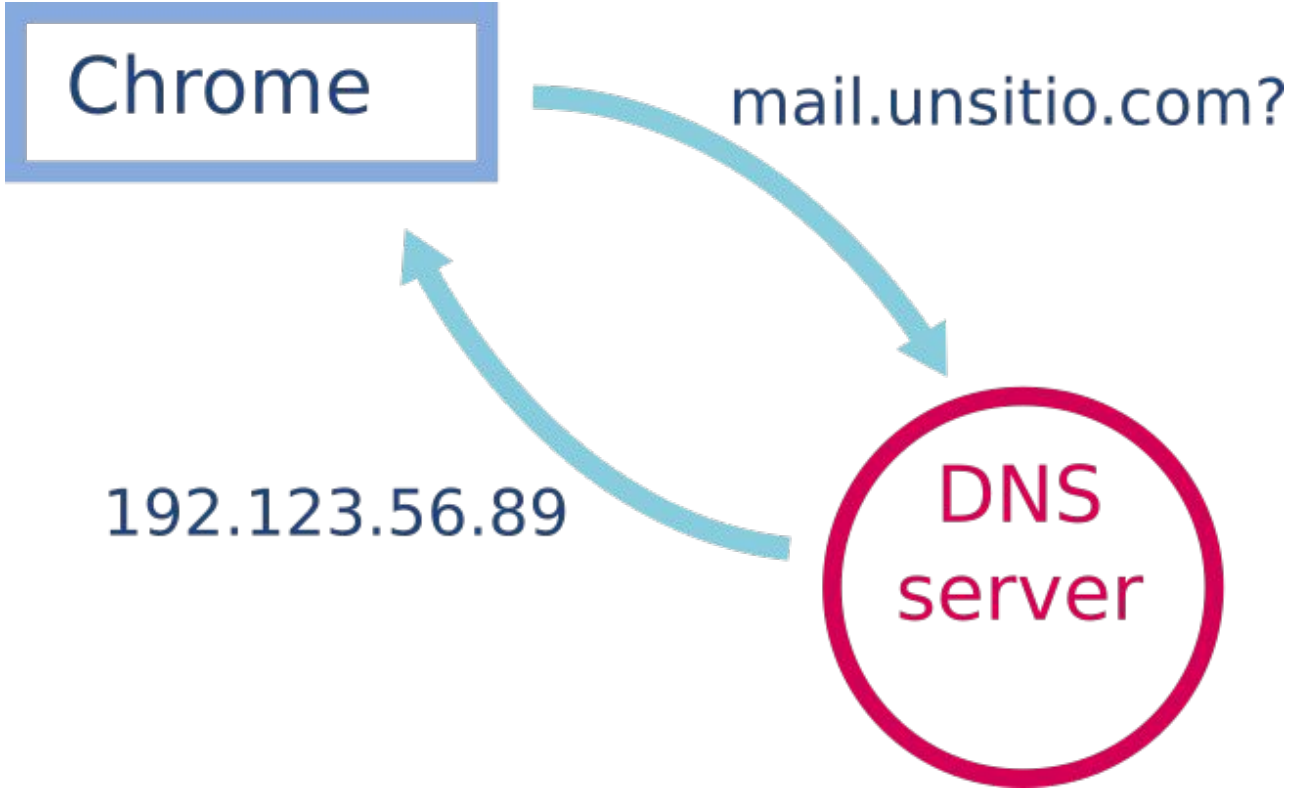
No podríamos tener en nuestra máquina, una "libreta de direcciones" actualizada de todos los dominios del mundo.

Si google cambia la dirección de red de un server, cómo sabemos y actualizamos eso en nuestra libreta?

Eso **no escala!**.

En cambio, para resolver dominios normalmente nuestra computadora va a enviar **Consultas DNS** a servidores específicamente encargados de tener esa libreta y responder a quienes consulten, los **Servidores DNS** o **Servidores de nombres**.

Resolver normalmente implica preguntar a otros



Resolver normalmente implica preguntar a otros

Y cómo sabemos en qué dirección están los **Servidores de nombres**?

Normalmente tenemos las ips de esos servidores configuradas, tanto en el sistema operativo como en programas que lo permitan.

Ej: **8.8.4.4** es un DNS público que ofrece Google.

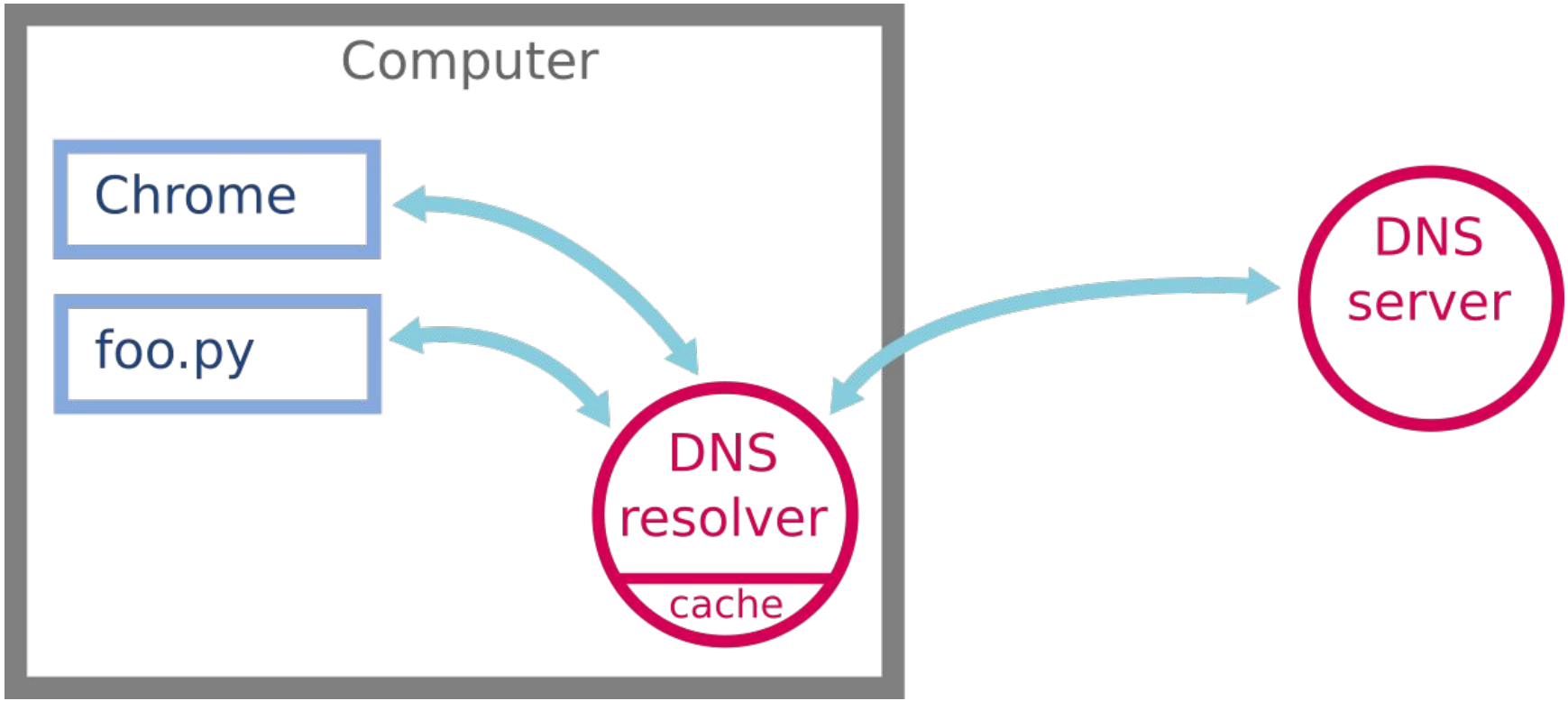
Ahorrando preguntas, paso 1

Si nuestra computadora hace 200 requests seguidas preguntando por la misma dirección, estamos desperdiciando muchísima red, y sobrecargando al servidor DNS innecesariamente.

Normalmente los programas no hacen la consulta directamente al servidor, sino que hacen la consulta al sistema operativo, que tiene una especie de servidor de DNS local, en nuestra máquina. Tiene un Resolvedor de DNS.

Si no conoce la dirección, este se encarga de pedirla al servidor externo. Pero tiene caché!, para recordar las direcciones que le estuvieron pidiendo recientemente, evitando hacer consultas cada vez.

Ahorrando preguntas, paso 1

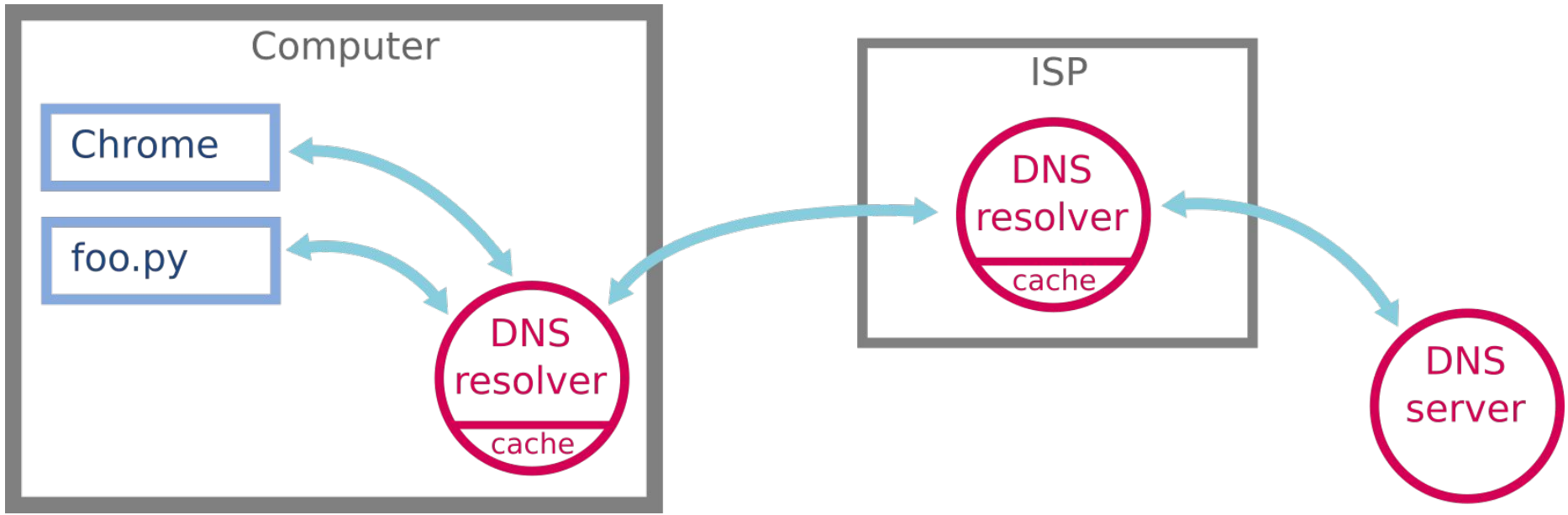


Ahorrando preguntas, paso 2

Y normalmente tampoco hablamos de forma "directa" con servidores DNS globales. Nuestro proveedor de internet tienen sus propios servidores de DNS, con sus propias cachés, etc. Y el proveedor que le da internet a nuestro proveedor, también. Y así sucesivamente.

Nuestras consultas DNS suelen recorrer un camino, saltando de servidor en servidor, hasta que alguno tenga la dirección en caché o hasta que lleguen al servidor "autoritativo" que conoce esa dirección.

Ahorrando preguntas, paso 2



Servidores DNS autoritativos

El servidor "dueño" de la dirección, que la conoce porque alguien (ej: el dueño del dominio) configuró allí la dirección de red del dominio, es el servidor **Autoritativo**.

Los demás servidores intermedios pueden tener esa dirección gracias a haberla preguntado a servidores de mayor jerarquía, pero son solo intermediarios con caché.

Problemas de caché

Qué pasa si los resolvedores intermedios tienen cacheada una dirección, y esa dirección cambia en el servidor de nombres??

Hasta que esas cachés no se venzan, los intermedios van a resolver incorrectamente la dirección!

Es un problema que sucede. Por eso solemos evitar cachear por mucho tiempo, y solemos evitar cambiar direcciones muy seguido.

Y se complica más... una segunda jerarquía

No existe un único servidor global autoritativo, sino que existe una jerarquía de servidores de dominios.

Tomemos un ejemplo de dominio: "mail.misitio.com"

Cuando le preguntemos al servidor de nombres, "en qué dirección está mail.sitio.com?", nos va a responder algo como "no se! andá a preguntarle a el servidor que conoce las .com, que está en la dirección x.x.x.x"

Hay diferentes servidores "top level", uno para cada terminación posible: ".com", ".org", ".net", ".ar", ".us", etc. Y el servidor "root" nos sabe redirigir al que corresponda.

Algunos de esos servers son administrados por países. Por ejemplo, el server que responde por los ".ar", es administrado por Argentina (por NIC.AR específicamente).

Y más!...

Nuestro servidor de NIC.AR conoce dónde está todo lo que termine en ".ar".... o no. Por ejemplo, podría haber un servidor que sabe de ".com.ar" y otro diferente para ".gob.ar".

En ese caso, si preguntamos por "dónde está elecciones.gob.ar", pasaría lo siguiente:

1. Le preguntamos a ROOT, el server de dns global (asumimos que ningún intermediario tenía la respuesta). ROOT nos dice "preguntale a AR, que está en x.x.x.x".
2. Le preguntamos a AR. AR nos responde "preguntale a GOB.AR, que está en y.y.y.y"
3. Le preguntamos a GOB.AR. Este finalmente nos responde con la dirección de elecciones.gob.ar.

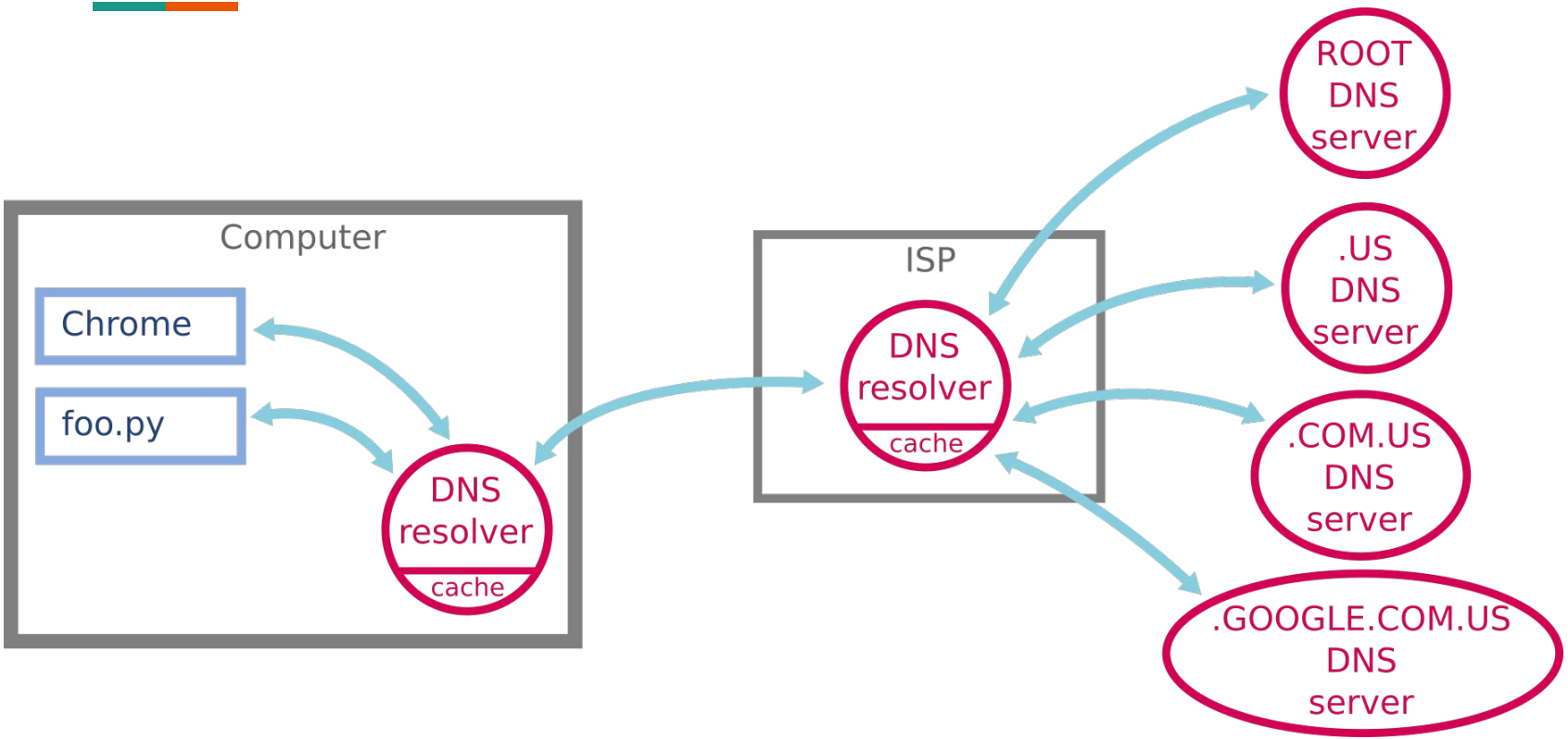
Y máááás !...

Incluso es posible que las personas y empresas monten sus propios servidores de DNS, para responder a subdominios propios. Por ejemplo, google tiene su propio DNS para responder a todas las consultas del estilo "x.google.(...)"

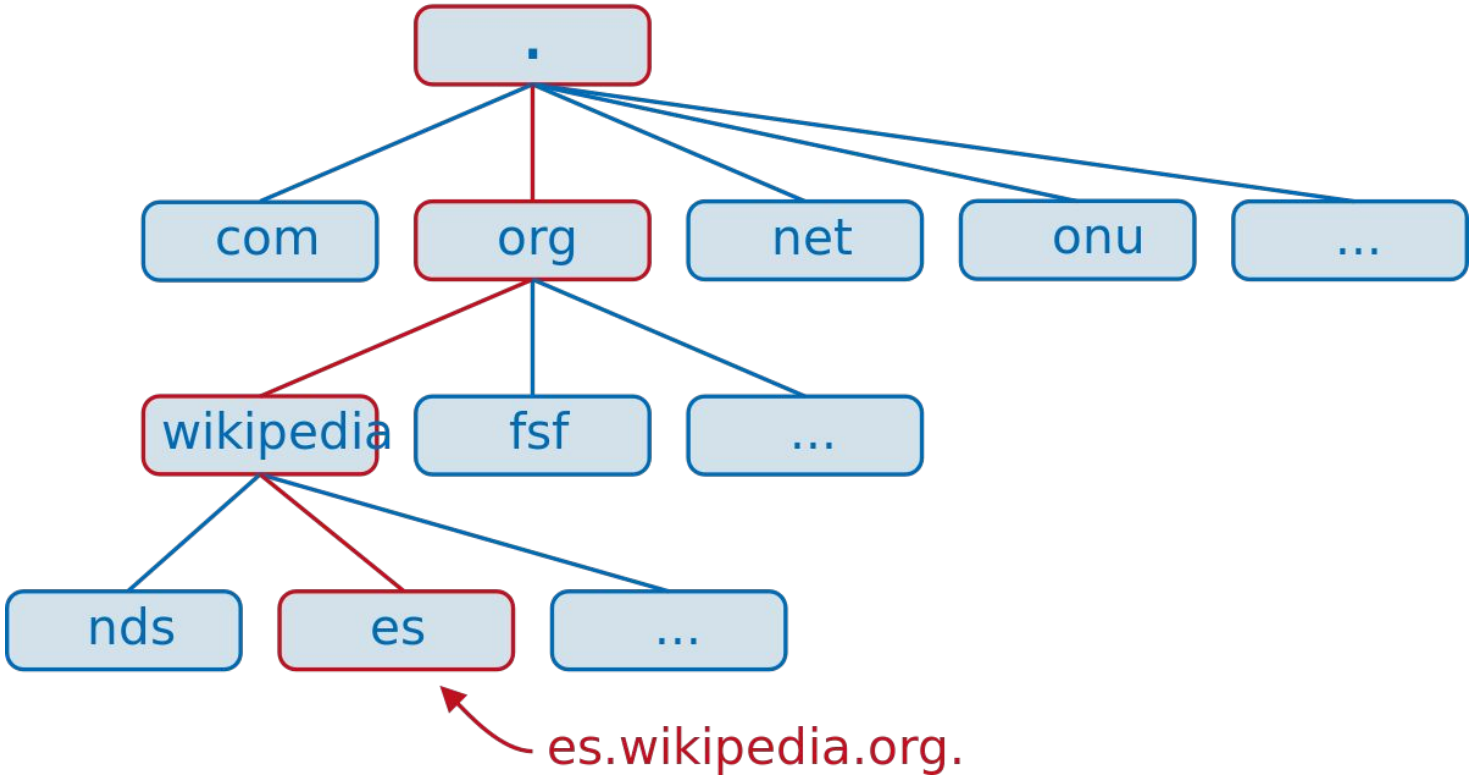
Ejemplo: "mail.google.com.us"

1. Le preguntamos a ROOT, el server de dns global (asumimos que ningún intermediario tenía la respuesta). ROOT nos dice "preguntale a US, que está en x.x.x.x".
2. Le preguntamos a US, nos responde "preguntale a COM.US, que está en y.y.y.y"
3. Le preguntamos a COM.US, nos responde con "preguntale a GOOGLE.COM.US, que está en z.z.z.z"
4. Le preguntamos a GOOGLE.COM.US, y este finalmente nos sabe responder dónde está mail.google.com.us

Y máááás !...


Computer
Chrome
foo.py
DNS
resolver
cache
ISP
DNS
resolver
cache
ROOT
DNS
server
.US
DNS
server
.COM.US
DNS
server
.GOOGLE.COM.US
DNS
server

Y máááás !...



DNS y privacidad (i)

Problema de privacidad 1: resolvers intermedios pueden saber qué dominios estamos intentando resolver.

Solución: si no confiamos en alguno de esos intermediarios (por ejemplo: el proveedor de internet) podemos configurar nuestro navegador o computadora para que los saltee y consulte directamente a algún servidor dns específico (hay varios públicos).

DNS y privacidad (ii)

Problema de privacidad 2: el servidor de DNS igualmente va a saber a qué dominios estamos accediendo.

No hay una solución para esto, pero al menos eligiendo un root confiable, podemos mitigar un poco el problema.

DNS y privacidad (iii)

Problema de privacidad 3: Las consultas de DNS no viajan encriptadas! Todo intermediario en la red va a poder ver qué dominios estamos intentando resolver, sin importar que no los usemos a los intermediarios para resolver los dominios.

Solución: no hay mucho que hacer actualmente. "DNS over HTTPS" es algo que aún se encuentra en etapa de pruebas.

Cómo registro un dominio?

Depende. Cada top level (.com, .ar, .org) administra sus dominios de forma diferente.

Para tener un .com (no .com.ar), hay muchos registradores posibles. Les recomendamos Namecheap (barato, pero de buena calidad). La mayoría ofrece gratuitamente todo lo necesario para hacer que nuestro dominio responda con la ip de nuestro servidor, e incluso que la ip se actualice automáticamente si cambia.

Para tener un .ar (por ejemplo, .com.ar) hace falta registrar el dominio en NIC.ar. El proceso es bastante más engorroso, y solo ofrece la registración del nombre, pero exige que nosotros tengamos nuestro propio servidor de DNS para resolver el dominio y subdominios (se puede contratar en otros proveedores).

DNS

UCSE - SEIA