DNS

Fundamentos de Redes de Ordenadores

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Enero de 2021

Contenidos

Contenidos

Motivación

- Es más cómodo manejar y **recordar nombres** que direcciones IP (ej: `hielo.gsyc.urjc.es` frente a `212.128.1.44`).
- **Las direcciones IP están ligadas a la estructura de la red**, pero eso no tiene que reflejarse en el nombrado de máquinas (ej: `www.google.com` y `www.google.es` tendrán IPs muy diferentes).
- **Las direcciones IP están ligadas a máquinas concretas**, y puede ser conveniente un nivel de abstracción independiente de ello (ej: `www.urjc.es` puede cambiar de máquina, y por lo tanto de IP, pero no tiene por qué cambiar de nombre).
- Por todo ello, es conveniente establecer un sistema de nombrado de máquinas y una correspondencia entre dichos nombres y las direcciones IP: DNS *(Domain Name System)*
- DNS es un protocolo de nivel de aplicación. Funciona sobre UDP y sobre TCP.

Historia

- Originalmente (años 70) la correspondencia entre nombres y direcciones IP se mantenía en un único fichero (`HOSTS.TXT`) con los nombres y las direcciones IP de todas las máquinas de ARPANET.
  - El fichero se obtenía periódicamente por FTP: gestión completamente manual.
- Con el crecimiento de ARPANET este mecanismo se hizo inmanejable.
- En 1983, Paul Mockapetris publicó las primeras RFCs que describen un servicio de nombres basado en dominios.
- En 1987, las revisó en las RFC 1034 y 1035, que definen el DNS. Estas RFCs han sido a su vez revisadas y ampliadas más adelante por otras muchas RFCs.

Fundamentos

- **DNS**: 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.
- 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.
- El nombre completo de una máquina (FQDN, *Fully Qualified Domain Name*) incluye el nombre de la máquina y el nombre del dominio en que se encuentra:

  `hielo.gsyc.urjc.es.`

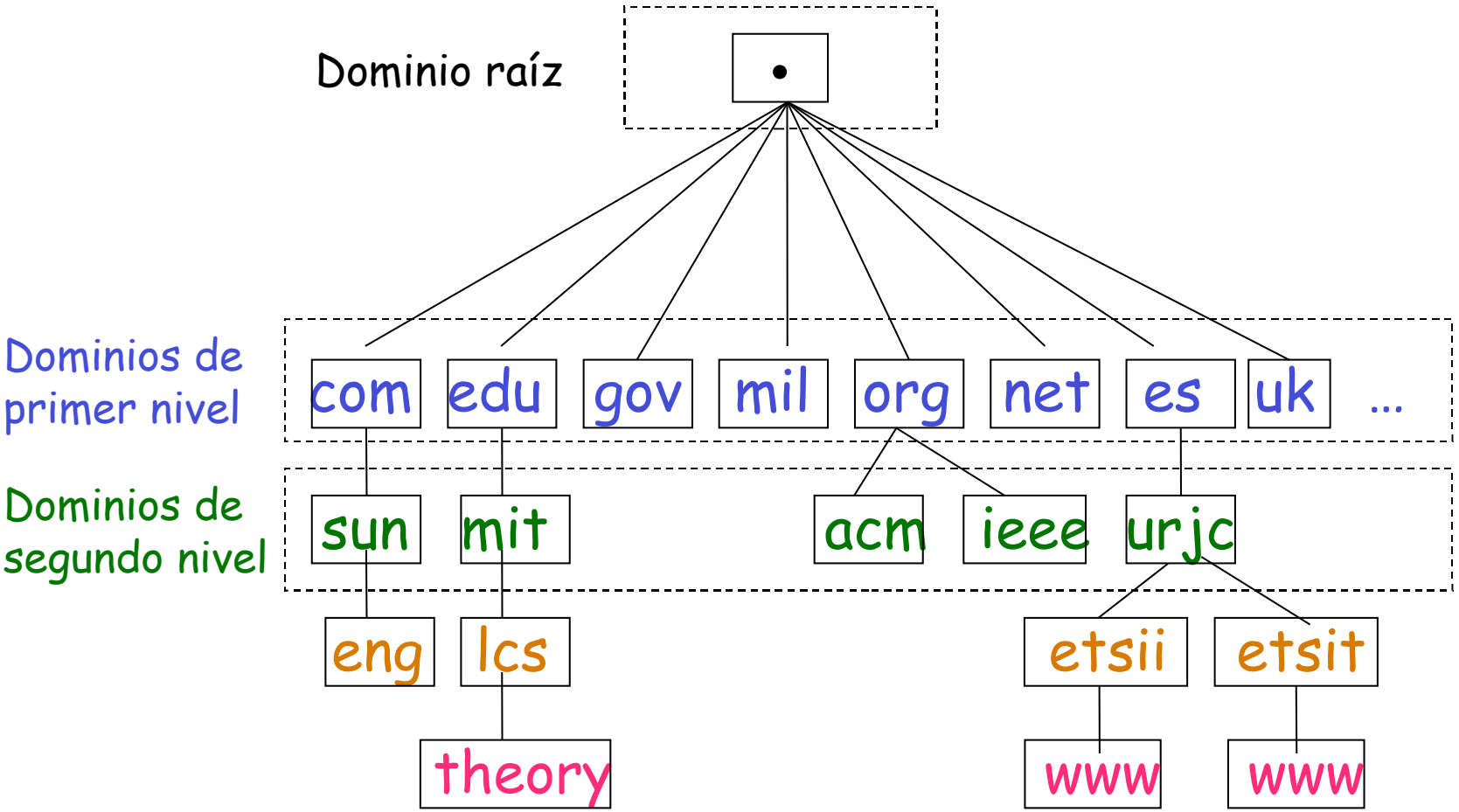
- Estrictamente, un FQDN termina siempre en el carácter "." (aunque normalmente puede omitirse, excepto en los mapas de DNS).

Contenidos

Jerarquía de dominios

- **Dominio raíz** (*root domain* o dominio "."):
  - 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 del país:
    `uk`, `mx`, `ar`, `de`, `es`, `jp`...
- **Dominios de segundo nivel**
- **Dominios de tercer nivel**
- ...

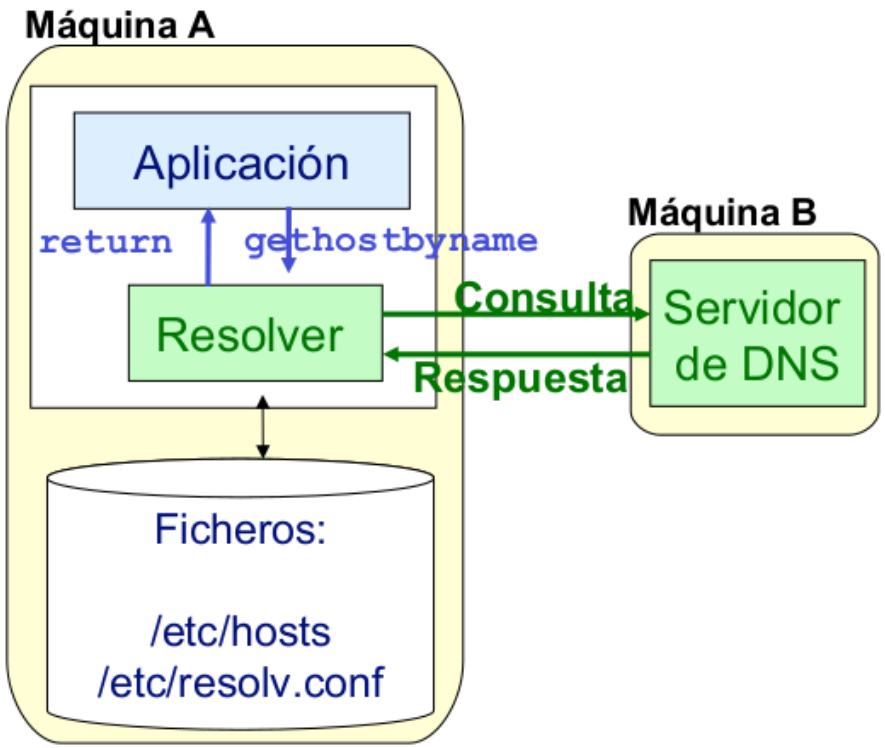
Árbol de dominios



Contenidos

Consulta de nombres desde las aplicaciones

- Cuando una aplicación tiene un nombre de máquina y necesita su IP, consulta al DNS, invocando en su código llamadas a funciones como `gethostbyname()` o `To_IP()`.
- Las aplicaciones van enlazadas con una librería de consulta al DNS (llamada "`resolver`").



- 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`

Ejemplo de fichero /etc/hosts

```
127.0.0.1 localhost
127.0.1.1 cacharro

#  Laboratorio 04 - Edif. Lab II
193.147.49.21 epsilon01.aulas.gsyc.es epsilon01
193.147.49.22 epsilon02.aulas.gsyc.es epsilon02
193.147.49.23 epsilon03.aulas.gsyc.es epsilon03
193.147.49.24 epsilon04.aulas.gsyc.es epsilon04
193.147.49.25 epsilon05.aulas.gsyc.es epsilon05
193.147.49.26 epsilon06.aulas.gsyc.es epsilon06
193.147.49.27 epsilon07.aulas.gsyc.es epsilon07
193.147.49.28 epsilon08.aulas.gsyc.es epsilon08
193.147.49.29 epsilon09.aulas.gsyc.es epsilon09
```

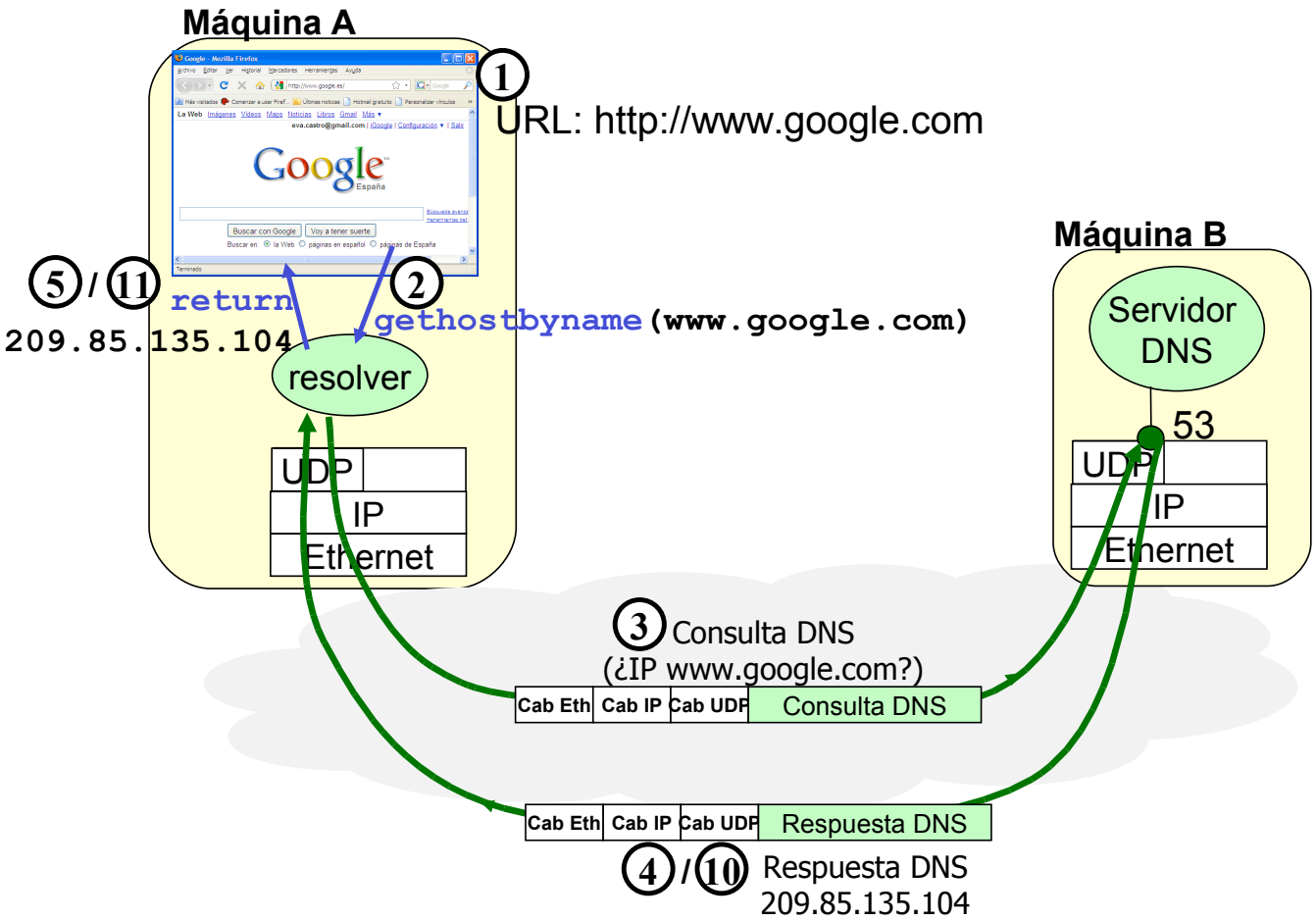
- En cada línea, detrás de una dirección IP pueden aparecer uno o más nombres (con o sin dominio) separados por blancos, que quedan asociados a esa dirección.
- Los nombres e IPs que aparecen en este fichero pueden no tener nada que ver con los del DNS.

Ejemplo de fichero /etc/resolv.conf

```
search gsyc.urjc.es aulas.gsyc.urjc.es pantuflo.es
nameserver 212.128.4.2
nameserver 193.147.184.7
```

- La línea search incluye una lista de dominios separados por blancos. Estos dominios se concatenarán a los nombres no–FQDN que utilicen las aplicaciones al consultar al DNS.
  - Ej: si se ha escrito ping hielo, se preguntará al DNS en primer lugar por hielo.gsyc.urjc.es. Si no existiera, se preguntará por hielo.aulas.gsyc.urjc.es, y así sucesivamente.
- Las líneas nameserver contienen la IP del servidor de DNS al que consultará la máquina.
- Si hay más de una línea nameserver, las restantes se utilizarán (por orden) si los servidores anteriores no responden.
  - NOTA: si un servidor responde que un nombre no existe, no se pregunta a ningún otro servidor.

Consulta desde el *resolver* a un servidor de DNS



- El *resolver* envía a su servidor de DNS una consulta con el nombre buscado
- El servidor de DNS le responde con la IP pedida
  - si el servidor la sabe, contesta inmediatamente
  - si el servidor no la sabe, investiga por su cuenta y cuando la obtiene, responde al *resolver*

Servidor de DNS de un dominio

- La información relacionada con la resolución de nombres de un dominio determinado se guarda en un fichero que se denomina mapa del dominio. En el 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.
- 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. Por fiabilidad, el mapa de un dominio puede encontrarse en otras máquinas que también son servidores de DNS. Se dice que todos estos servidores sirven ese dominio.
- Un servidor de DNS que contenga varios ficheros de mapa de dominio servirá todos los dominios correspondientes a dichos ficheros.

Consulta a un servidor de DNS

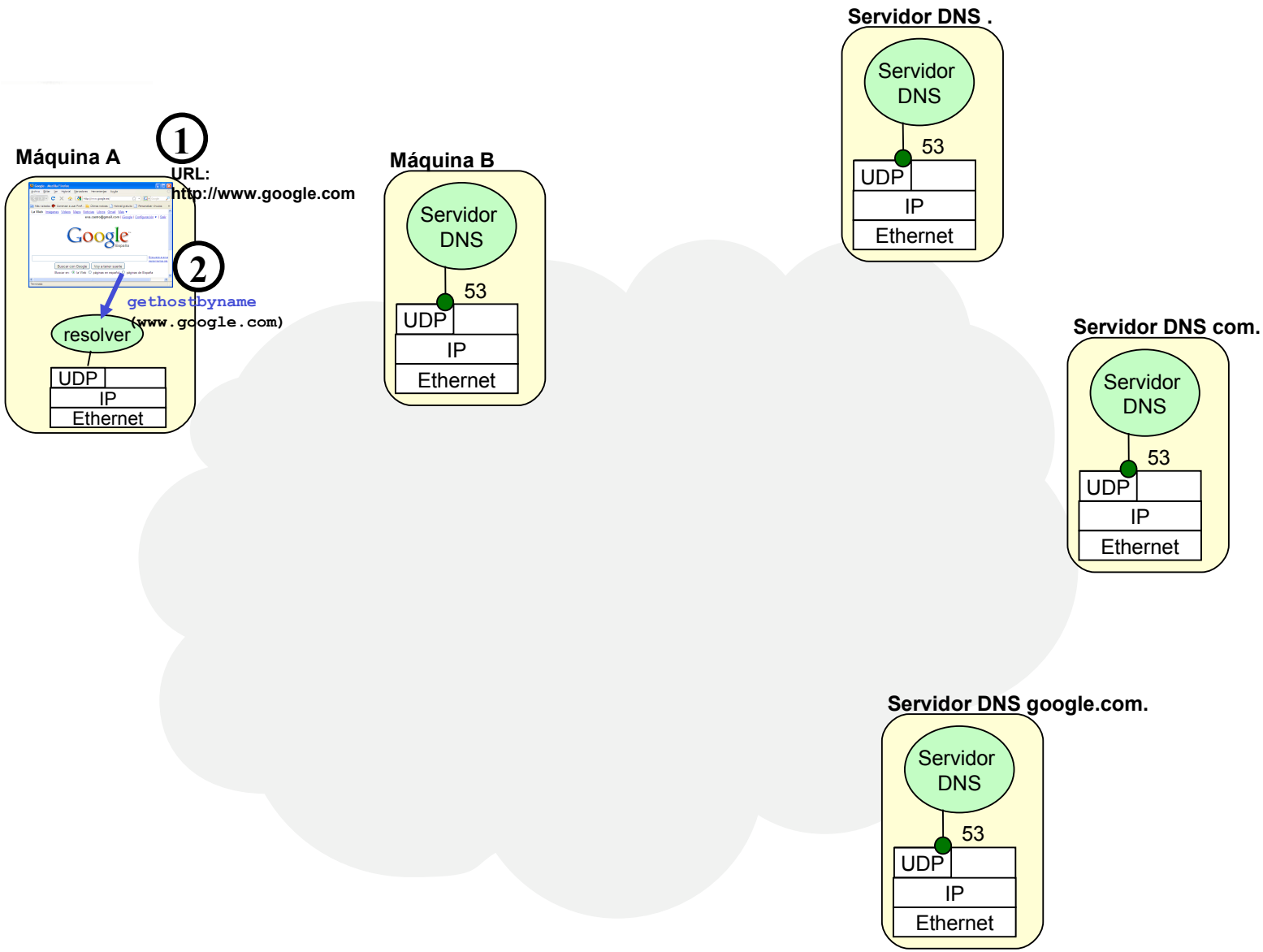
Cuando un servidor de DNS recibe una consulta puede ocurrir que:

- El servidor de DNS sirva el dominio al que pertenece la consulta. En ese caso el servidor podrá leer el mapa del dominio directamente, porque lo tiene almacenado, y generar una respuesta.
- El servidor de DNS no sirva el dominio al que pertenece la consulta. En ese caso, dependiendo del modo en el que se realiza la consulta se comportará de una de las siguientes formas:
  - **responderá con la dirección IP de otro servidor de DNS** que sirva un subdominio al que se refiere la consulta. Esta información la extraerá de su/s mapa/s de dominio.
  - **preguntará a otro servidor de DNS** para tratar de conseguir la repuesta a dicha solicitud.
    - Todos los servidores de DNS saben las direcciones IP de los *root nameservers* (servidores del dominio raíz).

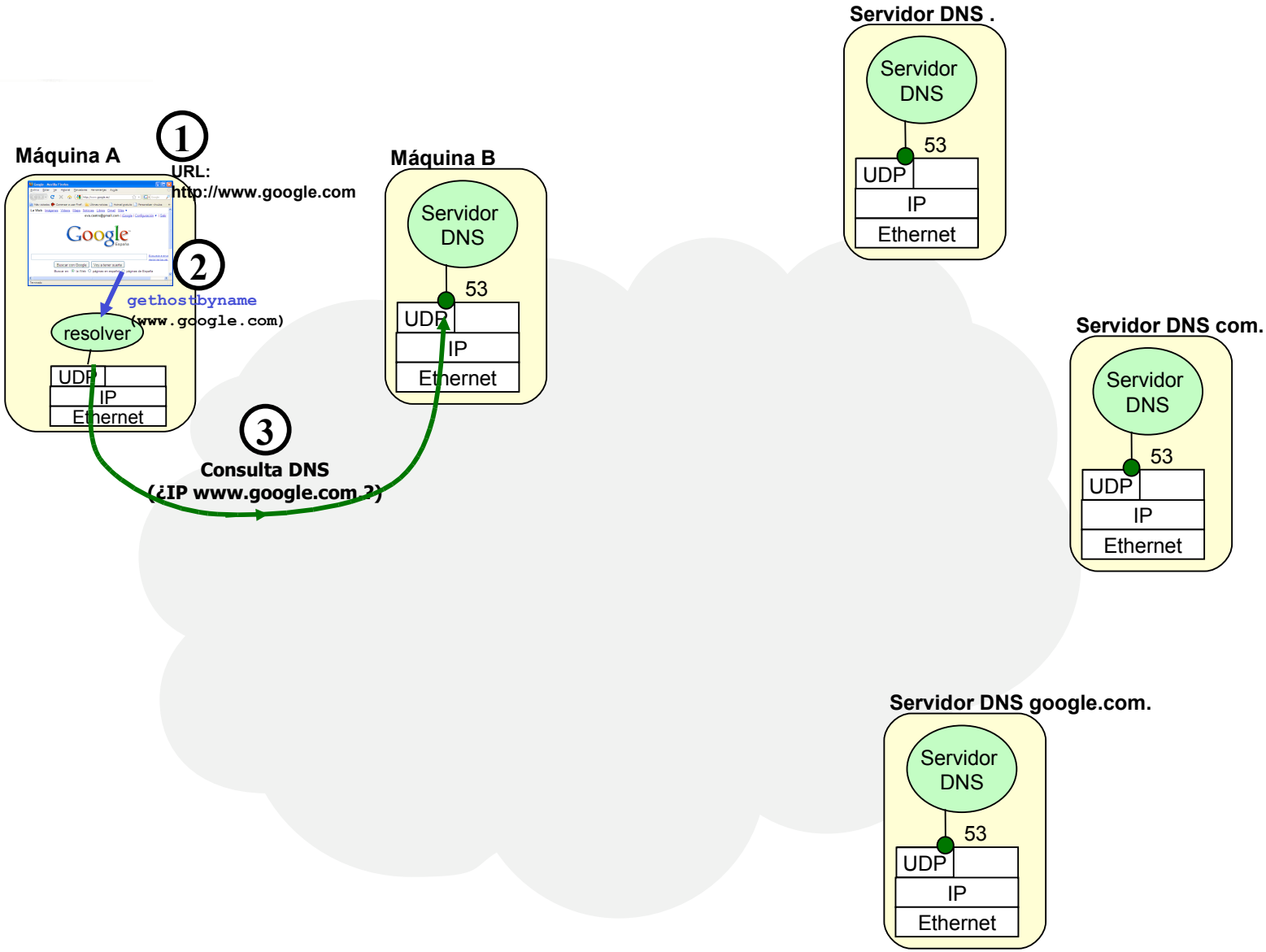
Resolución de nombres en un servidor de DNS

- Cuando un servidor S recibe una consulta para resolver un nombre (ejemplo: `www.google.com`):
  - S comprueba si el nombre pertenece a alguno de los dominios que sirve (si es que sirve alguno). Si S lo sirve, busca el nombre en su mapa y devuelve la dirección IP correspondiente.
  - Si el nombre no es de ningún dominio que sirva S:
    1. S pregunta a un servidor del dominio raíz, que le contestará con la dirección IP de un servidor de DNS del TLD incluido en el FQDN (en este caso: `com.`)
    2. S pregunta al servidor de DNS del TLD (`com.`), que le responde con la dirección IP de un servidor de DNS del dominio de segundo nivel (en este caso: `google.com.`)
    3. Si el FQDN de la pregunta contuviera más dominios, se repite el proceso hasta que S obtenga la IP del servidor del dominio en que el que directamente reside la máquina por la que se pregunta.
    4. S pregunta al servidor del último nivel (`google.com.`), que por servir ese dominio, tendrá en sus mapas la dirección IP pedida, y se la dará a S
    5. S devuelve a la IP pedida a quien se la pidió.

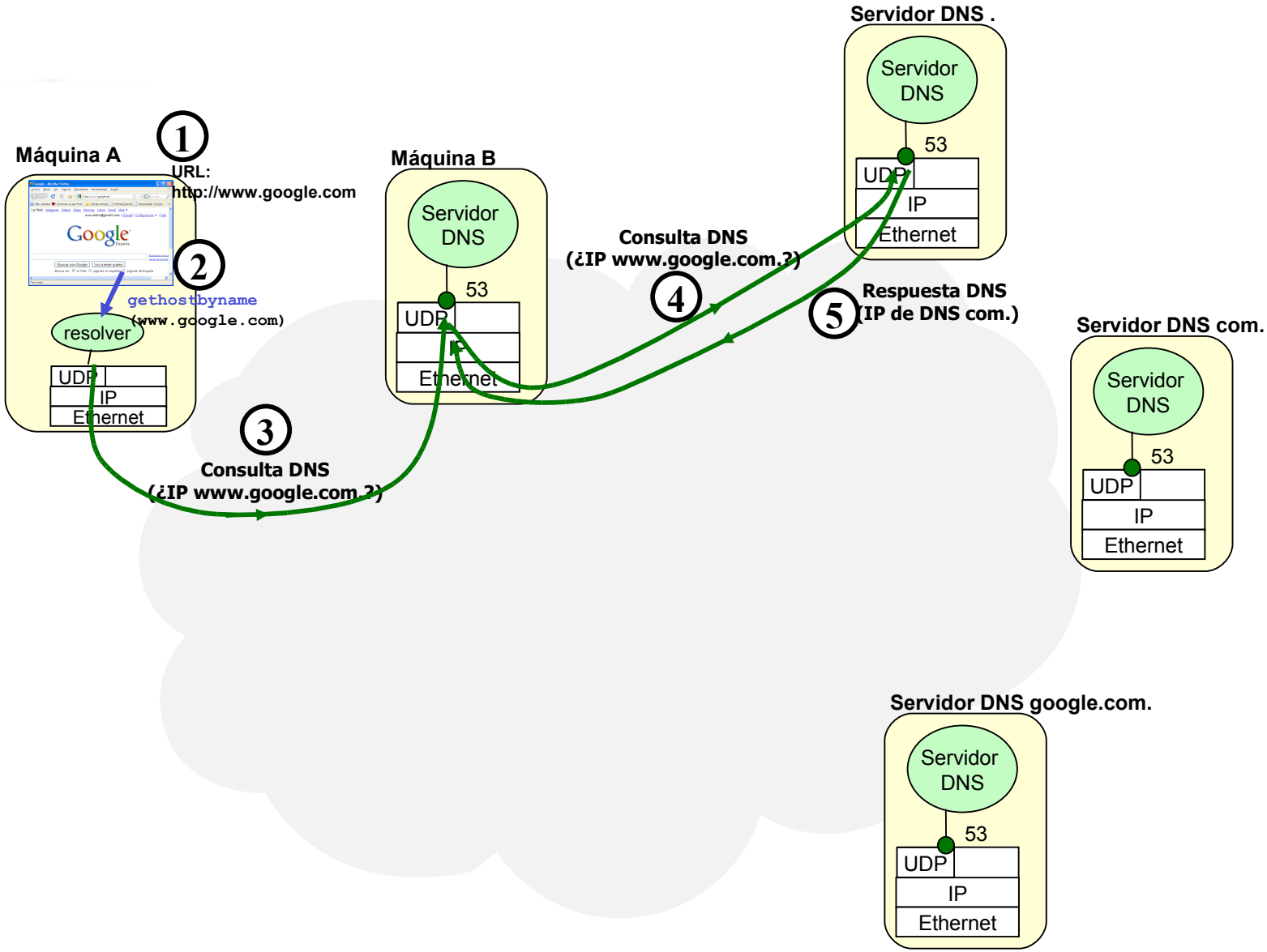
Ejemplo (I)


Servidor DNS .
Servidor DNS
53
UDP
IP
Ethernet
Máquina A
1
URL:
http://www.google.com
2
gethostbyname
(www.google.com)
resolver
UDP
IP
Ethernet
Máquina B
Servidor DNS
53
UDP
IP
Ethernet
Servidor DNS com.
Servidor DNS
53
UDP
IP
Ethernet
Servidor DNS google.com.
Servidor DNS
53
UDP
IP
Ethernet

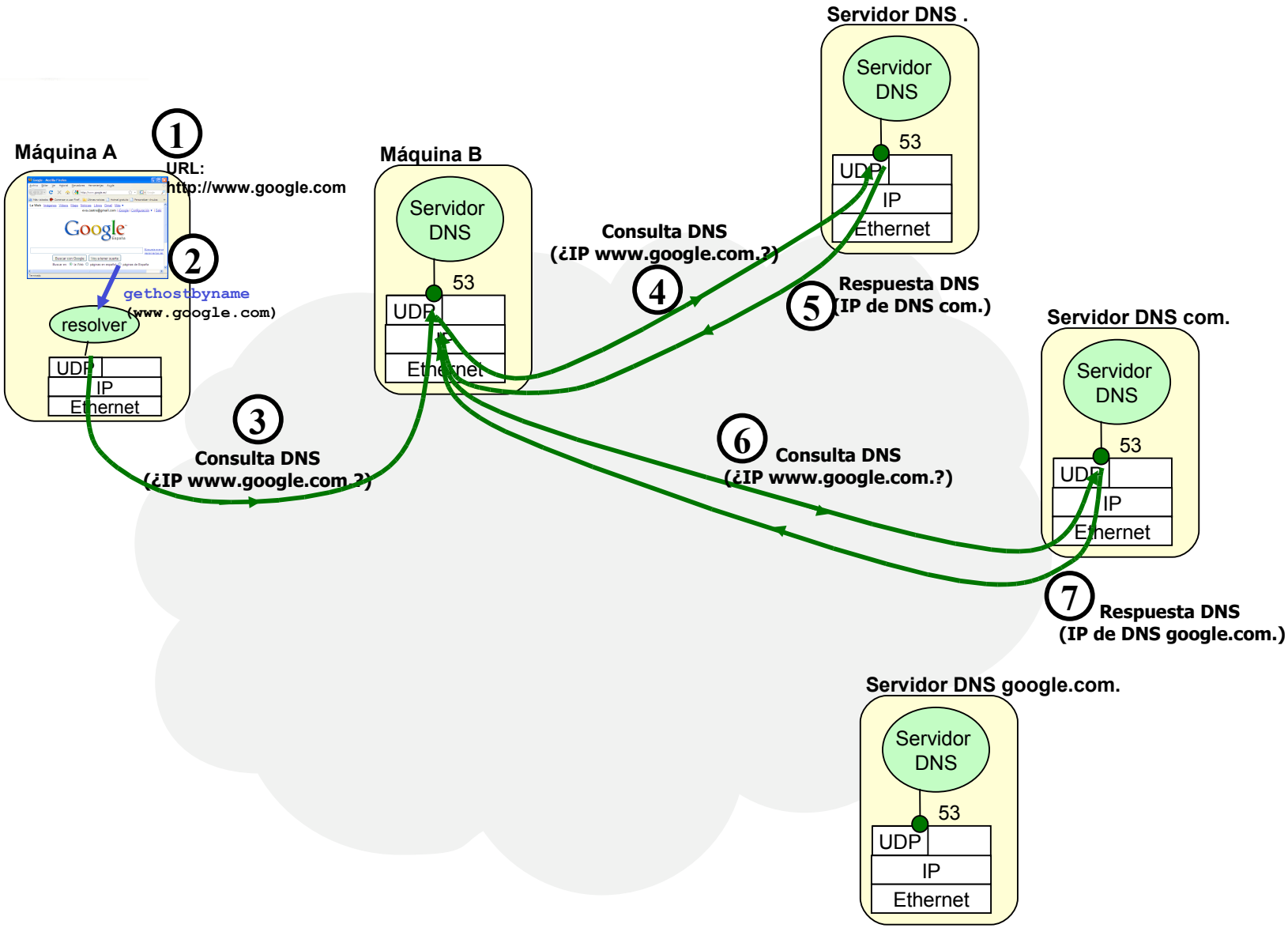
Ejemplo (II)


Servidor DNS .
Servidor DNS
53
UDP
IP
Ethernet
Máquina A
1
URL:
http://www.google.com
Google
2
gethostbyname
(www.google.com)
resolver
UDP
IP
Ethernet
Máquina B
Servidor DNS
53
UDP
IP
Ethernet
3
Consulta DNS
(¿IP www.google.com ?)
Servidor DNS com.
Servidor DNS
53
UDP
IP
Ethernet
Servidor DNS google.com.
Servidor DNS
53
UDP
IP
Ethernet

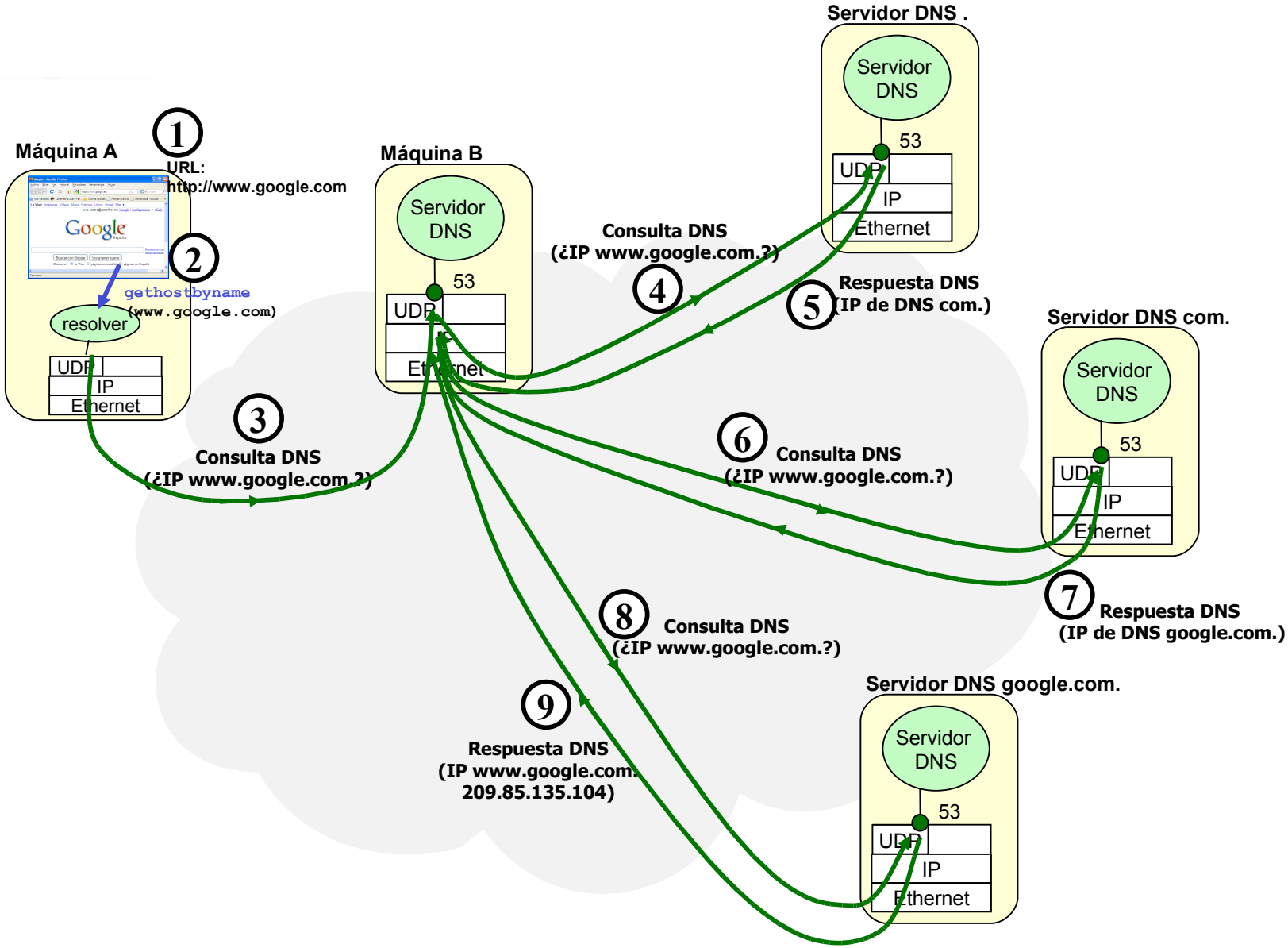
Ejemplo (III)


Servidor DNS .
Servidor DNS
53
UDP
IP
Ethernet
Máquina A
1
URL:
http://www.google.com
Google
2
gethostbyname
(www.google.com)
resolver
UDP
IP
Ethernet
Máquina B
Servidor DNS
53
UDP
IP
Ethernet
Consulta DNS
(¿IP www.google.com.?)
4
5
Respuesta DNS
(IP de DNS com.)
Servidor DNS com.
Servidor DNS
53
UDP
IP
Ethernet
3
Consulta DNS
(¿IP www.google.com.?)
Servidor DNS google.com.
Servidor DNS
53
UDP
IP
Ethernet

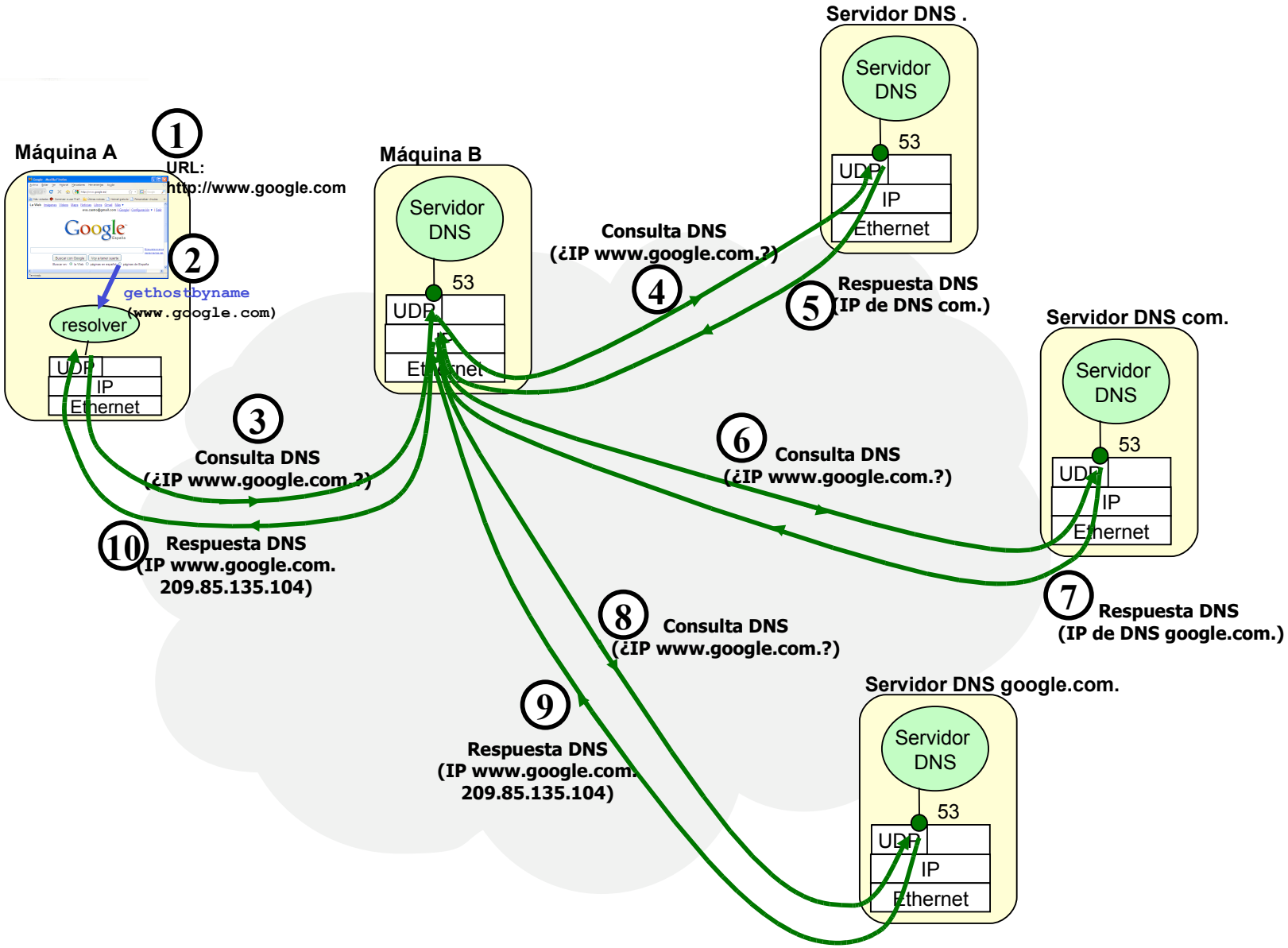
Ejemplo (IV)


Servidor DNS .
Servidor DNS
53
UDP
IP
Ethernet
Máquina A
1
URL:
http://www.google.com
Google
2
gethostbyname
(www.google.com)
resolver
UDP
IP
Ethernet
Máquina B
Servidor DNS
53
UDP
Ethernet
Consulta DNS
(¿IP www.google.com.?)
4
5
Respuesta DNS
(IP de DNS com.)
Servidor DNS com.
Servidor DNS
53
UDP
IP
Ethernet
3
Consulta DNS
(¿IP www.google.com.?)
6
Consulta DNS
(¿IP www.google.com.?)
7
Respuesta DNS
(IP de DNS google.com.)
Servidor DNS google.com.
Servidor DNS
53
UDP
IP
Ethernet

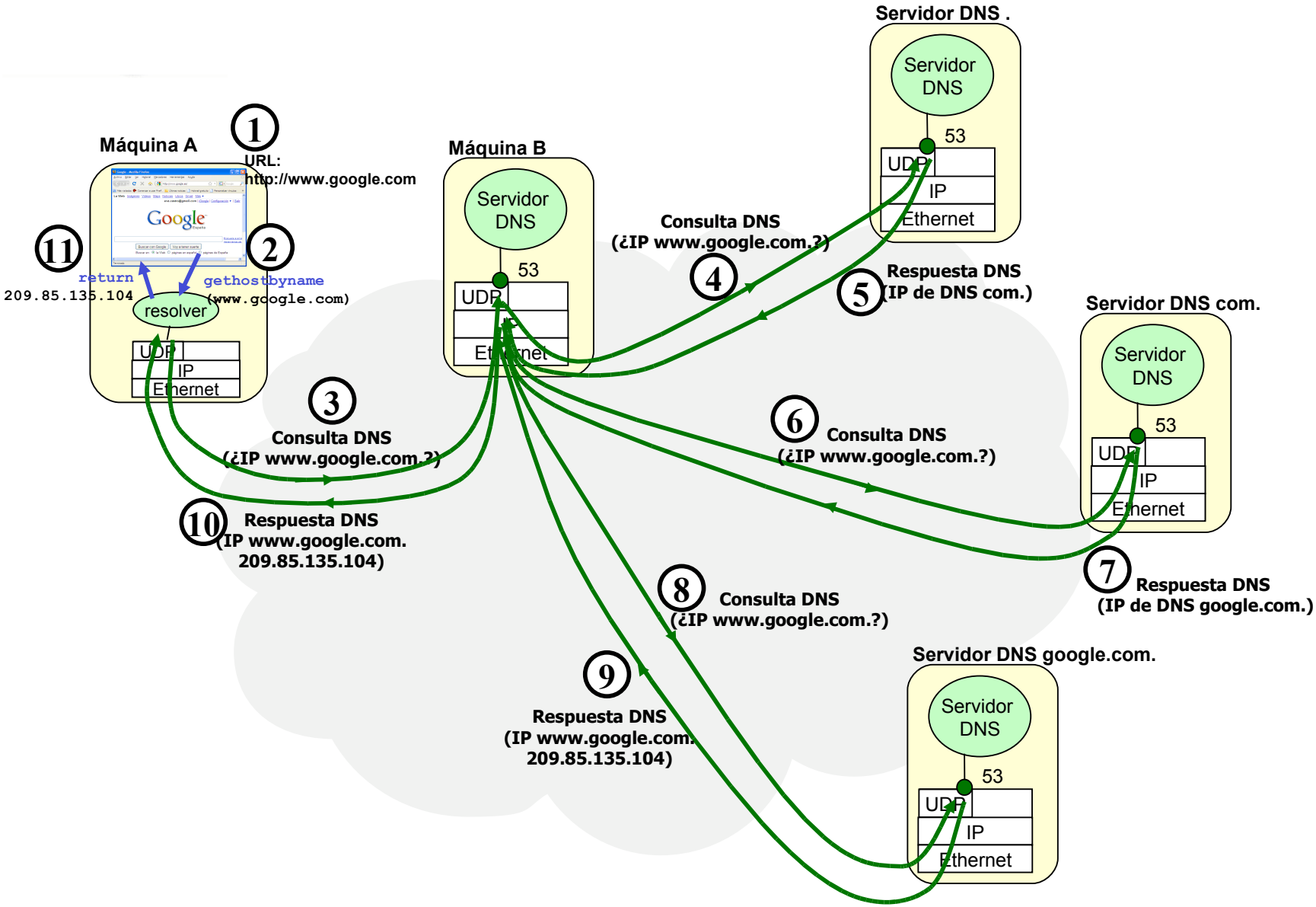
Ejemplo (V)


Máquina A
1
URL:
http://www.google.com
2
gethostbyname
(www.google.com)
resolver
UDP
IP
Ethernet
3
Consulta DNS
(¿IP www.google.com.?)
Máquina B
Servidor DNS
53
UDP
IP
Ethernet
Consulta DNS
(¿IP www.google.com.?)
4
Servidor DNS .
Servidor DNS
53
UDP
IP
Ethernet
5
Respuesta DNS
(IP de DNS com.)
6
Consulta DNS
(¿IP www.google.com.?)
Servidor DNS com.
Servidor DNS
53
UDP
IP
Ethernet
7
Respuesta DNS
(IP de DNS google.com.)
8
Consulta DNS
(¿IP www.google.com.?)
9
Respuesta DNS
(IP www.google.com.
209.85.135.104)
Servidor DNS google.com.
Servidor DNS
53
UDP
IP
Ethernet

Ejemplo (VI)


Servidor DNS .
Servidor DNS
53
UDP
IP
Ethernet
Máquina A
1
URL:
http://www.google.com
Google
2
gethostbyname
(www.google.com)
resolver
UDP
IP
Ethernet
Máquina B
Servidor DNS
53
UDP
IP
Ethernet
Consulta DNS
(¿IP www.google.com.?)
4
5
Respuesta DNS
(IP de DNS com.)
Servidor DNS com.
Servidor DNS
53
UDP
IP
Ethernet
3
Consulta DNS
(¿IP www.google.com.?)
6
Consulta DNS
(¿IP www.google.com.?)
10
Respuesta DNS
(IP www.google.com.
209.85.135.104)
7
Respuesta DNS
(IP de DNS google.com.)
8
Consulta DNS
(¿IP www.google.com.?)
9
Respuesta DNS
(IP www.google.com.
209.85.135.104)
Servidor DNS google.com.
Servidor DNS
53
UDP
IP
Ethernet

Ejemplo (VII)


Servidor DNS .
Servidor DNS
53
UDP
IP
Ethernet
Máquina A
1
URL:
http://www.google.com
Máquina B
Servidor DNS
53
UDP
Ethernet
11
return
209.85.135.104
2
gethostbyname
(www.google.com)
resolver
UDP
IP
Ethernet
Consulta DNS
(¿IP www.google.com.?)
4
5
Respuesta DNS
(IP de DNS com.)
Servidor DNS com.
Servidor DNS
53
UDP
IP
Ethernet
3
Consulta DNS
(¿IP www.google.com.?)
6
Consulta DNS
(¿IP www.google.com.?)
10
Respuesta DNS
(IP www.google.com.
209.85.135.104)
7
Respuesta DNS
(IP de DNS google.com.)
8
Consulta DNS
(¿IP www.google.com.?)
Servidor DNS google.com.
9
Respuesta DNS
(IP www.google.com.
209.85.135.104)
Servidor DNS
53
UDP
IP
Ethernet

Cachés en el servicio de DNS

- Cuando un servidor, al realizar una búsqueda, aprende un dato que no sabía, lo guarda en una caché. Si vuelve a necesitar ese dato, lo saca de la caché en vez de volver a preguntar.
- Los mapas especifican cuánto tiempo (ttl) puede estar en una **caché** un dato que se saca de dicho mapa.
- Cuando un dato se almacena en la **caché** de un servidor el valor de ttl de ese dato va disminuyendo según pasa el tiempo. Si llega a cero el dato caduca y se borra de la **caché**.
- En cualquier consulta los servidores **aprovechan cualquier información que tengan en la caché** para responder directamente o para "atajar" en el cadena de búsquedas.
  - Ej.: Si un servidor recibe una consulta por `www.google.com`, y ya tiene en su caché la IP de un servidor de `com`, empieza preguntándole a él y no a un *root nameserver*.

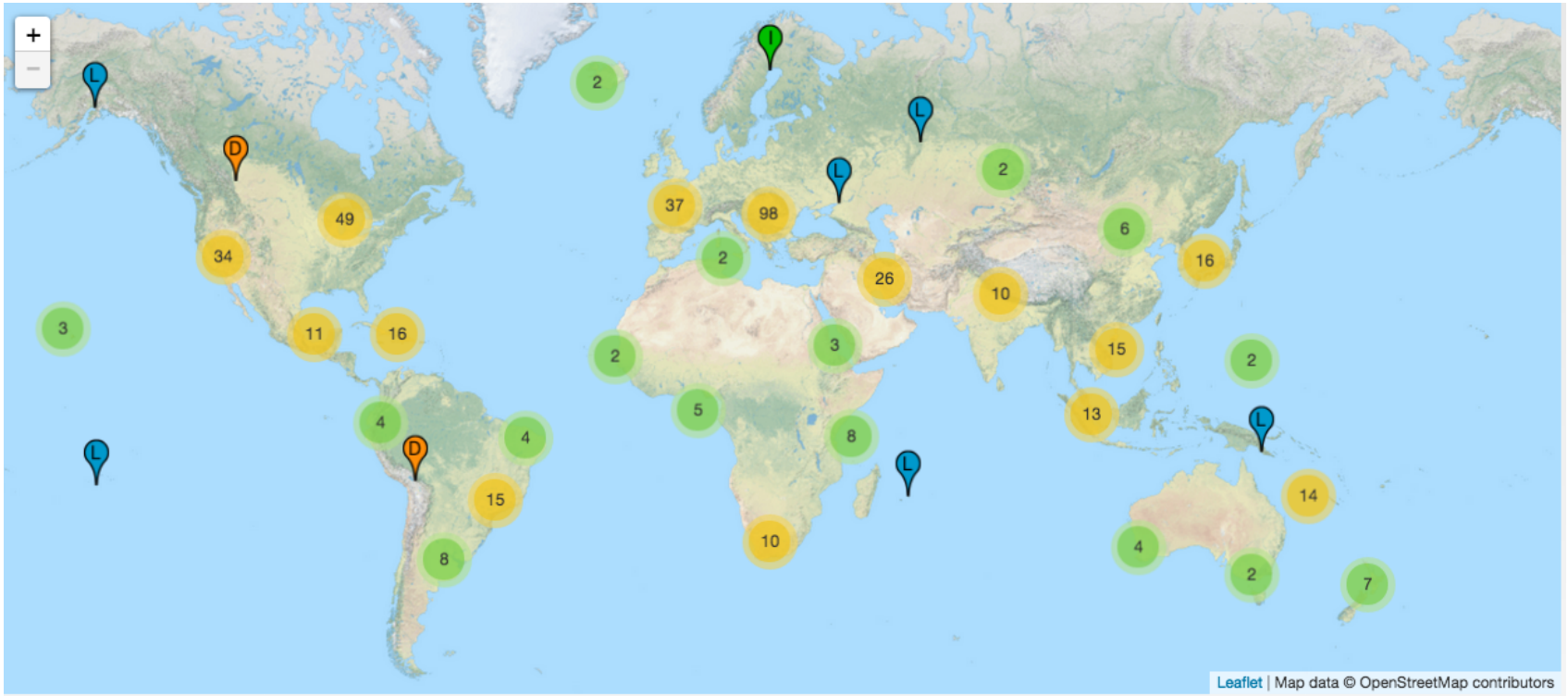
Tipos de consultas recibidas por un servidor

- Consultas Recursivas:
  - Obligan al servidor que las recibe a hacer todas las consultas necesarias para encontrar la dirección pedida y contestar con ella.
  - De este tipo son las consultas que hace un *resolver*.
- Consultas Iterativas:
  - Hacen que el servidor que las recibe conteste con lo máximo que el sepa de esa búsqueda sin preguntar a nadie más
    - suele ser la IP del servidor del siguiente subdominio en la cadena de búsqueda
  - De este tipo son las consultas que hace un servidor de DNS a otro servidor de DNS.

Root nameservers

- Actualmente están definidos 13 *root nameservers*:
  - `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 unas 200 máquinas en el mundo las que son *root nameservers*.
- Los mapas del dominio raíz se transfieren entre los *root nameservers* por mecanismos externos al DNS.

Ubicación de los *Root nameservers*



- La figura es de Abril de 2015
- Una versión actualizada disponible en `http://root-servers.org/`

Contenidos

Mapas de dominio

- Cada mapa de dominio incluye un conjunto de Registros de Recurso (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
    - Clase: Clase de direccionamiento, `IN` para Internet
    - Tipo: Tipo del RR
    - Valor: Valor del RR asociado al Nombre (en función del Tipo)

Principales tipos de RR

- `SOA` *(Start Of Authority)*: Contiene información sobre todo el dominio: servidor maestro primario, administrador, número de serie del mapa, tiempos de refresco...
- `NS` *(Nameserver)*: Identifica un servidor de nombres.
- `A`: Asocia a un nombre una dirección IP.
- `MX`: Define un servidor de correo para el dominio.
- `CNAME`: Asocia un alias a otro nombre.
- `HINFO`: Da información del tipo de máquina y sistema operativo para un nombre.
- `TXT`: Da información adicional para un nombre.
- `SRV`: Define qué máquina ofrece un determinado servicio (generalización de `MX`).
- `PTR`: Asocia a una IP un nombre en el dominio inverso (aunque también tiene otros usos).

Ejemplo de mapa

Nombre	TTL	Clase	Tipo	Valor

```
$ORIGIN gsyc.es.          ; añadido a los nombres no terminados en punto
$TTL    86400             ; ttl por defecto en segundos. Otras sintaxis: 1d o 24h
gsyc.es.                  IN   SOA   ns1.gsyc.es.  admin-gsyc.gmail.com. (
                                     2016030201 ; Nº de serie
                                     8h         ; Refresco
                                     2h         ; Reintento
                                     7d         ; Expiración
                                     1d )       ; ttl para respuestas negativas
                                                ; (de nombre inexistente)
gsyc.es.                  IN   NS    ns1.gsyc.es.
gsyc.es.                  IN   NS    ns2.gsyc.es.
gsyc.es.                2h IN   MX    mail.gsyc.es.
ns1.gsyc.es.              IN   A     193.147.71.5
ns2.gsyc.es.              IN   A     193.147.71.6
tierra.gsyc.es.           IN   A     193.147.71.7
hielo.gsyc.es.            IN   A     193.147.71.8
agua.gsyc.es.             IN   A     193.147.71.9
fuego.gsyc.es.            IN   A     193.147.71.10
www.gsyc.es.            4h IN   CNAME agua.gsyc.es.
mail.gsyc.es.           4h IN   CNAME fuego.gsyc.es.
aulas.gsyc.es.            IN   NS    ns.aulas.gsyc.es.
ns.aulas.gsyc.es.         IN   A     212.135.11.45
```

Contenidos

Protocolo de transporte

- DNS utiliza normalmente UDP como protocolo de transporte, y en algunas ocasiones utiliza también TCP.
- Un servidor de DNS escucha en el puerto 53 de TCP y en el 53 de UDP.
  - Normalmente un *resolver* hace consultas usando UDP.
  - Normalmente un servidor responde usando el mismo protocolo que el protocolo recibido en la consulta.
  - Si un servidor contesta por UDP y la **respuesta ocupa más de 512 bytes**:
    - el servidor envía sólo los primeros 512 bytes de la respuesta, indicando con un **flag que dicha respuesta está truncada**
    - quien preguntó, al ver la respuesta truncada, repite la consulta utilizando **TCP**
    - el servidor responde utilizando TCP
  - Las transferencias de zona de maestro a esclavo utilizan TCP.

Mensaje de Consulta

Transaction ID	número que identifica la consulta
Flags	**Response Flag**: Indica si es una consulta (flag=0) o una respuesta (flag=1). En este caso valdrá 0. ... **Recursion desired**: Indica si se la consulta se realiza en modo recursivo (flag=1) o iterativo (flag=0). ...
Questions	1
Answer RRs	0
Authority RRs	0
Additional RRs	0
Queries	Registro que se solicita en la consulta al servidor de DNS. Al realizar una resolución directa, aparecerá el nombre de la máquina que se está consultando y el tipo de registro que se solicita, registro A. Ejemplo: ▽ Queries → pc2.emp2.net: type A, class IN

Mensaje de Respuesta con el registro solicitado

Transaction ID	mismo número que venía en el mensaje de consulta
Flags	**Response Flag**: Indica si es una consulta (flag=0) o una respuesta (flag=1). En este caso valdrá 1. ...
Questions	1
Answer RRs	1
Authority RRs	1
Additional RRs	1
Queries	Registro que se solicita en la consulta al servidor de DNS. Al realizar una resolución directa, aparecerá el nombre de la máquina que se está consultando y el tipo de registro que se solicita, registro A. Ejemplo: ▽ Queries → pc2.emp2.net: type A, class IN
Answers	Registro que responde el servidor de DNS a la solicitud que se le hizo en el campo Queries. Al realizar una resolución directa, aparecerá el registro completo A. Ejemplo: ▽ Answers → ▽ pc2.emp2.net: type A, class IN, addr 14.0.0.100 Name: pc2.emp2.net Type: A (Host address) Class: IN (0x0001) Time to live: 1 day Data length: 4 Addr: 14.0.0.100
Authoritative nameservers	Registro NS del servidor de nombres que ha proporcionado la respuesta. Ejemplo: ▽ Authoritative nameservers → emp2.net: type NS, class IN, ns dnsemp2.emp2.net
Additional records	Registro A del servidor de nombres dado en Authoritative nameservers. Ejemplo: ▽ Additional records → dnsemp2.emp2.net: type A, class IN, addr 14.0.0.10

Mensaje de Respuesta sin el registro solicitado, remite a otro servidor de DNS

Transaction ID	mismo número que venía en el mensaje de consulta
Flags	**Response Flag**: Indica si es una consulta (flag=0) o una respuesta (flag=1). En este caso valdrá 1. ...
Questions	1
Answer RRs	0
Authority RRs	1
Additional RRs	1
Queries	Registro que se solicita en la consulta al servidor de DNS. Al realizar una resolución directa, aparecerá el nombre de la máquina que se está consultando y el tipo de registro que se solicita, registro A. Ejemplo: ▽ Queries → pc2.emp2.net: type A, class IN
Authoritative nameservers	Registro NS de otro servidor de DNS que puede ayudarnos a realizar la resolución. Ejemplo: ▽ Authoritative nameservers → net: type NS, class IN, ns dnsnet.net
Additional records	Registro A del servidor de nombres dado en Authoritative nameservers. Ejemplo: ▽ Additional records → dnsnet.net: type A, class IN, addr 13.0.0.10

Contenidos

Referencias

- J.J. Kurose y K.W. Ross, **Redes de Computadores: un enfoque descendente basado en Internet**, Pearson Educación, 2ª edición: capítulo 2.
- W. Richard Stevens, **TCP/IP Illustrated, vol 1**, Addisson Wesley: capítulo 14.
- Charles M. Kozierok, **TCP/IP GUIDE. A Comprehensive, Illustrated Internet Protocols Reference**, No Starch Press, 2005:

  `http://www.tcpipguide.com/free/t_TCPIPNameSystemsHostTablesandDomainNameSystemDNS.htm`
- RFC 1034, **Domain Names: Concepts and Facilities**: `http://www.faqs.org/rfcs/rfc1034.html`
- RFC 1035, **Domain Names: Implementation and Specification**: `http://www.faqs.org/rfcs/rfc1035.html`