

2.8. Domain Name System (DNS)

Todos los protocolos de la pila TCP/IP utilizan direcciones IP binarias, pero los seres humanos no somos demasiado buenos recordando secuencias de números, así que enseguida surgió la necesidad de asociar nombres (mucho más memorizables y fáciles que reconocer que las direcciones IP) a las direcciones IP. Originalmente, cuando Internet consistía en una decena de nodos, simplemente se distribuía periódicamente un fichero HOSTS con los nombres asociados a todas las direcciones IP en uso. Ese mecanismo perdura hoy en día, y todos los sistemas operativos tienen un fichero HOSTS ('C:\Windows\System32\drivers\etc\hosts' en Windows y '/etc/hosts' en Linux/UNIX), que se consulta antes que el DNS, por lo que puede ser muy útil para asociar un nombre de dominio a una IP alternativa para simplificar la captura de tráfico.

Obviamente ese sistema dejó de escalar en cuanto Internet paso a tener miles de nodos, lo que motivó la creación del sistema de resolución de nombres DNS [[RFC1035](#)]. DNS es sistema de nombres distribuido y jerárquico, que permite a los responsables de un dominio publicar información relacionada con el mismo, como por ejemplo su dirección IP asociada. Un dominio no es nada más que una secuencia de etiquetas (que no distinguen entre mayúsculas y minúsculas), separadas mediante puntos (e.g. "www.example.com").

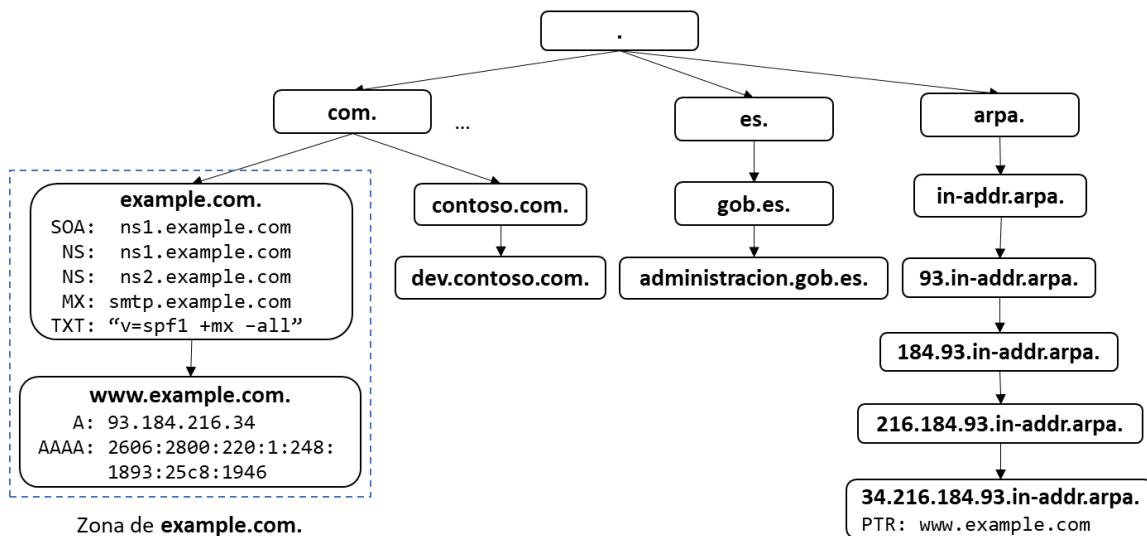


Figura 2.14 – Jerarquía del Sistema de Nombres de Dominio (DNS)

El sistema DNS tiene forma de árbol (**Figura 2.14**) y comienza en la raíz, que se representa como un punto '.'. Debajo de la raíz se encuentran los dominios TLD de primer nivel ("com", "org", "edu", "arpa", etc.) y los códigos de país ccTLD ("es", "uk", "us", etc.). Debajo se encuentran los dominios de segundo nivel (e.g. "example.com", "gob.es", "google.com", etc.), que suelen estar bajo el control de los diferentes tipos de organizaciones, y por debajo se pueden seguir creando subdominios, hasta llegar a un máximo de 253 caracteres. Cada nombre de dominio puede tener asociado uno o más **Registros de Recurso** (RR – Resource Records), que almacenan diferentes tipos de información. Los más importantes son:

- **A (Type=1):** Dirección IPv4 asociada a ese nombre de dominio.
- **AAAA (Type=28):** Dirección IPv6 asociada a ese nombre de dominio.
- **CNAME (Type=5):** Indica que este nombre de dominio es un alias de otro (e.g. www.example.com CNAME server1.example.com).
- **PTR (Type=12):** Apunta a otra parte del sistema DNS. Se utilizan para la resolución inversa de nombres (i.e. dirección IP → nombre de dominio asociado).
- **SOA (Type=6):** Marca el inicio de una autoridad de zona y define los parámetros comunes de la misma, como el servidor de nombres primario de la zona, una dirección de correo de contacto o cada cuanto tiempo deben replicar la información de zona los servidores de nombre secundarios.
- **NS (Type=2):** Servidor de nombres autoritativo de ese dominio. Todas las zonas deben tener al menos dos servidores de nombres: uno primario y el resto secundarios, que se sincronizan periódicamente con el primario.
- **MX (Type=15):** Servidor de correo entrante para ese dominio.

- **TXT** (*Type=16*): Permite publicar cadenas de texto. Algunas aplicaciones (e.g. SPF) los utilizan para publicar información en el DNS si necesidad de definir un nuevo tipo de registro.

Los dominios se agrupan en zonas, que están bajo el control una única entidad, aunque se puede delegar el control de cualquier subdominio a otra entidad (y por tanto se crea otra zona). Cada zona tiene uno o más servidores de nombres autoritativos, que son los responsables de mantener la información de la zona y responder a las consultas que les realizan otros clientes o servidores, mediante el protocolo DNS.

A) DNS Message Format:

```

      1 1 1 1 1 1
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
      +---+---+---+---+---+---+---+---+---+
      |           ID           |
      +---+---+---+---+---+---+---+---+---+
      |QR| Opcode |AA|TC|RD|RA| Z | RCODE |
      +---+---+---+---+---+---+---+---+---+
      |           QDCOUNT        |
      +---+---+---+---+---+---+---+---+---+
      |           ANCOUNT        |
      +---+---+---+---+---+---+---+---+---+
      |           NSCOUNT         |
      +---+---+---+---+---+---+---+---+---+
      |           ARCOUNT         |
      +---+---+---+---+---+---+---+---+---+
      /           Question        /
      +---+---+---+---+---+---+---+---+---+
      /           Answer          /
      +---+---+---+---+---+---+---+---+---+
      /           Autority        /
      +---+---+---+---+---+---+---+---+---+
      /           Additional       /
      +---+---+---+---+---+---+---+---+---+

```

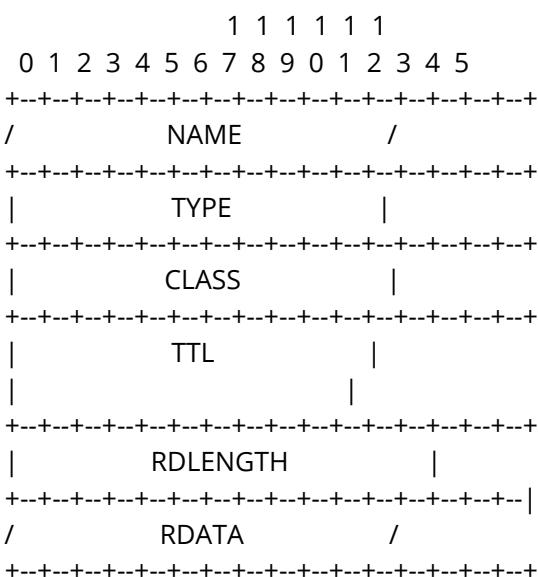
B) Question Section Format:

```

      1 1 1 1 1 1
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
      +---+---+---+---+---+---+---+---+---+
      /           QNAME          /
      +---+---+---+---+---+---+---+---+---+
      |           QTYPE          |
      +---+---+---+---+---+---+---+---+---+
      |           QCLASS         |
      +---+---+---+---+---+---+---+---+---+

```

C) Resource Record Format:

**Figura 2.15** – Formato de los mensajes y secciones del protocolo DNS [[RFC1035](#)]

DNS es un protocolo cliente-servidor basado en UDP, y que por defecto está limitado a mensajes de 512 octetos, aunque la extensión EDNS [[RFC6891](#)] permite ampliar este tamaño. Los mensajes DNS (**Figura 2.15**) están formados por una cabecera fija, y varias secciones de tamaño variable, que pueden incluir múltiples registros de recurso (RRs). En DNS solo hay dos tipos de mensajes: peticiones (QR=0; *Opcode*=0) y respuestas (QR=1, *Opcode*=0).

Las peticiones recursivas (RD=1) tienen un identificador de 16 bits, que el servidor debe incluir en su respuesta, y suelen incluir una única consulta (QDCOUNT=1), que incluye el nombre de dominio que se quiere consultar (QNAME) y el tipo de registro que se solicita (QTYPE), porque en Internet la clase siempre es IN (QCLASS=1).

Las respuestas usan el campo RCODE para indicar si se ha producido algún error, como por ejemplo si el dominio no existe (*NXDomain*). Además, los *flags* permiten especificar si la respuesta viene del servidor autoritativo de la zona (AA=1), si el servidor soporta consultas recursivas (RA=1), o si la respuesta está truncada (TC=1), en cuyo caso el cliente debería reintentar la consulta con TCP, que no tiene límite de tamaño. Las respuestas pueden copiar la sección de consulta, y utilizan la sección *Answer* para incluir los RRs solicitados si los conocen o, en caso contrario, envían información sobre los servidores de nombres autoritativos del dominio (*Authority*). Las respuestas DNS pueden incluir además información adicional (*Additional*), como las direcciones IP de los servidores de nombres autoritativos. Para mejorar el rendimiento de DNS, los RRs obtenidos pueden cachearse durante TTL segundos.

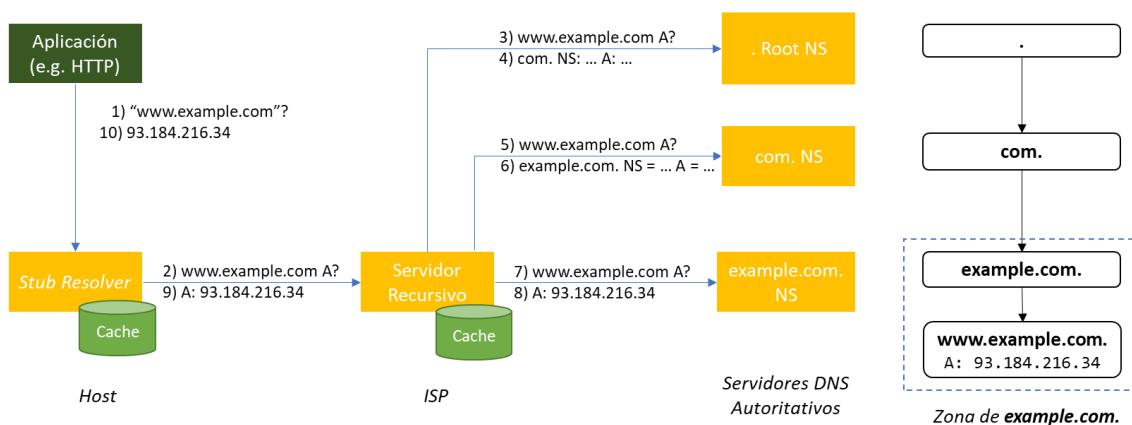


Figura 2.16 – Ejemplo de proceso de resolución de nombres DNS

Cuando una aplicación desea resolver un nombre DNS (**Figura 2.16**), normalmente no implementa directamente el protocolo DNS, sino que consulta a un servicio local denominado **Stub Resolver**, que es el que realmente implementa la parte cliente del protocolo DNS, y envía la consulta DNS al **Servidor de Nombres Recursivo** que tiene configurado, y que normalmente es un servicio que proporciona la organización o el proveedor de acceso a Internet de los usuarios. Se denomina recursivo porque es capaz de responder a una consulta DNS, incluso si no la sabe y necesita contactar con más servidores DNS hasta encontrar la respuesta. Y es que, como el sistema DNS es un sistema distribuido, para poder resolver un nombre DNS, primero hay que localizar al **Servidor de Nombres Autoritativo** que se encarga de esa zona. Para ello, como el sistema DNS es un sistema jerárquico, los servidores DNS recursivos pueden empezar preguntando a uno de los 13 **Servidores de Nombres Raíz** que hay en Internet (aunque realmente están replicados en cientos de localizaciones por todo el mundo). Éste le indicará al servidor recursivo que no conoce la respuesta, pero le indicará el servidor de nombres (NS) asociado al dominio de primer nivel (e.g. "com."), así como su dirección IP (A). Así que el servidor recursivo volverá a preguntar a ese servidor DNS, que típicamente tampoco conoce la respuesta, por lo que devuelve al servidor recursivo el servidor de nombres (NS) del subdominio consultado (e.g. "example.com"). El servidor recursivo seguirá preguntando a servidores de nombres autoritativos, hasta que uno de ellos sea el responsable de la zona que contiene el nombre consultado, y éste por fin le devolverá la respuesta deseada (e.g. la dirección IPv4 93.184.216.32). El servidor de nombres recursivo almacenará toda la información recopilada, incluyendo la respuesta y la información sobre todos los servidores autoritativos en su cache, de forma que, cuando un cliente vuelva a preguntar por alguno de esos dominios, pueda consultar directamente al servidor de nombres autoritativo más apropiado (en lugar de repetir todo el camino desde la raíz), y enviará la respuesta al cliente DNS (que también puede tener una caché local), y éste le enviará finalmente la información a la aplicación.

El *malware* utiliza a veces el tráfico DNS para exfiltrar información (e.g. a través de recursos TXT o codificando la información en las consultas que realiza) y sobre todo para localizar sus servidores de *Command and Control* (C&C/C2), de forma que puedan cambiarlos en caso de que su dirección IP sea descubierta. Para evitar que las organizaciones también filtren el dominio DNS del C2, algunas familias de *malware* incluyen un *Domain Generated Algorithm* (DGA) que, en función del tiempo, es capaz de generar dominios DNS pseudo-aleatorios, de forma que cada cierto tiempo el servidor de C2 se mueve a un dominio DNS diferente, por lo que es mucho más difícil filtrarlo.