Tema 4-Protocolos de nivel de aplicación II

El DNS (Domain Name System) es un sistema que se encarga de hacer la correspondencia entre los nombres de las máquinas (por ejemplo, www.google.com) y sus direcciones IP (por ejemplo, 209.85.227.104). TCP/IP, el protocolo utilizado para la comunicación en Internet, requiere que las máquinas se comuniquen entre sí mediante direcciones IP, pero es más fácil para las personas recordar nombres que números.

Proporciona información sobre los servidores de correo electrónico, lo que ayuda en la entrega de correo electrónico y otros servicios en línea. Se implementa utilizando el modelo cliente-servidor, y utiliza el protocolo UDP (puerto 53) aunque también puede utilizar TCP.

Antes del DNS, se utilizaba un archivo de hosts que contenía las direcciones IP de las máquinas y sus correspondientes nombres en una sola máquina o en una pequeña red. Sin embargo, este sistema era poco escalable, inconsistente con las copias locales y propenso a nombres duplicados. Aunque todavía puede ser utilizado en redes muy pequeñas sin servidor DNS, el DNS es el método preferido para hacer la correspondencia entre nombres de máquinas y direcciones IP en la mayoría de las redes.

El DNS está definido por dos especificaciones técnicas importantes: la RFC 1034, que establece los conceptos fundamentales del DNS, y la RFC 1035, que describe la implementación y especificaciones técnicas más detalladas. También hay varias actualizaciones posteriores a estas especificaciones.

Cliente DNS

DNS no solo es un sistema que permite la correspondencia entre nombres de dominio y direcciones IP, sino que también es un protocolo que permite la comunicación entre clientes y servidores DNS. Cada máquina tiene un cliente DNS (también llamado resolver) instalado en ella.

Cada vez que una aplicación en una máquina necesita averiguar la dirección IP de un nombre de dominio, la aplicación hace una consulta al cliente DNS pasándole el nombre de dominio. El cliente DNS envía la consulta al servidor DNS que esté configurado en la máquina, y espera la respuesta.

Cuando el servidor DNS recibe la consulta, busca en su base de datos la dirección IP correspondiente al nombre de dominio, y envía la respuesta al cliente DNS. Luego, el cliente DNS devuelve la respuesta a la aplicación que hizo la consulta inicial.

Por ejemplo, si una aplicación necesita conocer la dirección IP de "www.google.com", le pasará la consulta al cliente DNS, que a su vez la enviará al servidor DNS configurado en la máquina. El servidor DNS buscará la dirección IP correspondiente a "www.google.com" y enviará la respuesta al cliente DNS, que finalmente la devolverá a la aplicación.

Servidor DNS

Cada red, como por ejemplo la wifi de la UDC o un proveedor de servicios de internet (ISP), tiene su propio servidor DNS. Este servidor recibe consultas DNS de los clientes (por ejemplo, las máquinas que se conectan a la red) y averigua la dirección IP correspondiente al nombre de dominio solicitado.

Para averiguar la dirección IP correspondiente a un nombre de dominio, el servidor DNS no tiene toda la información almacenada en una sola base de datos. En cambio, utiliza una base de datos distribuida, en la que múltiples servidores DNS están organizados jerárquicamente.

Cuando un cliente DNS hace una consulta para averiguar una dirección IP, su servidor DNS no conoce la respuesta de antemano. Entonces, el servidor DNS hace una serie de preguntas a otros servidores DNS, comenzando por los servidores DNS de nivel superior que conocen toda la información de los dominios de nivel superior como ".com", ".edu", etc. Luego, el servidor DNS consulta los servidores DNS que almacenan información sobre el dominio en cuestión, y continúa haciendo consultas a servidores DNS de niveles inferiores hasta encontrar la dirección IP correspondiente al nombre de dominio solicitado.

Espacio de nombres DNS

El espacio de nombres DNS es una estructura jerárquica de nombres de dominio que se organiza como un árbol. En la parte superior del árbol se encuentra la raíz, que no tiene nombre y está representada por un punto (.).

Debajo de la raíz, hay varios dominios de nivel superior (TLDs) como ".com", ".edu", ".org", ".net", etc. Estos TLDs se dividen en dominios de segundo nivel (SLDs) como "google.com", "udc.es", "ibm.com", etc. Por debajo de los SLDs, pueden existir dominios de tercer nivel y así sucesivamente.

Cada nombre de dominio único en el espacio de nombres DNS identifica una máquina o un servicio en Internet. Por ejemplo, "www.fic.udc.es" es un nombre de dominio completo que identifica un sitio web alojado en la Facultad de Informática de la Universidad de A Coruña.

Los nombres de dominio no distinguen entre mayúsculas y minúsculas. Para especificar un nombre de dominio completo se debe utilizar la notación formalmente acabada en "." llamada FQDN (Fully Qualified Domain Name). Si el nombre de dominio está incompleto, se rellena con el dominio especificado en el archivo de configuración "/etc/resolv.conf".

Los TDL pueden ser:

- **ccTLDs (country-code TLDs)**: son los TLDs basados en códigos de país de dos letras, como ".es" para España, ".fr" para Francia, ".jp" para Japón, etc. Cada país tiene su propio ccTLD que se utiliza para identificar sitios web y otros recursos en línea de ese país.
- **gTLDs (generic TLDs)**: son los TLDs genéricos que no están relacionados con un país específico. Incluyen TLDs como ".com", ".org", ".net", ".info", ".biz", etc. Los gTLDs se dividen en tres tipos:
  - **Generic gTLDs**: son TLDs genéricos abiertos a cualquier persona o entidad que cumpla con los requisitos de registro establecidos por la organización que administra el TLD. Ejemplos de estos incluyen ".com", ".net" y ".org".
  - **Generic-restricted gTLDs**: son TLDs genéricos que tienen restricciones en su uso. Por ejemplo, ".edu" está reservado para instituciones educativas, ".gov" está reservado para agencias gubernamentales de EE. UU., ".mil" está reservado para el uso del Departamento de Defensa de EE. UU., etc.
  - **Sponsored gTLDs**: son TLDs patrocinados por organizaciones o entidades específicas que establecen las reglas de registro y uso para el TLD. Por ejemplo, ".aero" está patrocinado por la Asociación de Transporte Aéreo Internacional (IATA) y solo se puede registrar por parte de empresas y organizaciones de la industria aérea.
- **IDN ccTLDs (internationalized country-code TLDs)**: son los ccTLDs que permiten caracteres no ASCII, lo que permite que los nombres de dominio se escriban en diferentes idiomas y scripts. Por ejemplo, ".рф" es el ccTLD para Rusia, pero escrito en caracteres cirílicos.

En cada nivel de la jerarquía de nombres de dominio, existen servidores DNS que se encargan de distribuir la carga y de la delegación de la administración de los servidores de nombres.

En la parte superior de la jerarquía, se encuentran los servidores raíz, que son críticos para el funcionamiento de Internet. Existen 13 servidores raíz (A-M) distribuidos en diferentes partes del mundo, y están replicados por seguridad y fiabilidad. Estos servidores conocen a todos los TLDs (Top-Level Domains) y delegan en ellos.

Cada dominio de primer nivel tiene su servidor TLD asociado, que se encarga de la gestión de los sub-dominios. Los servidores TLD delegan la gestión de los sub-dominios a servidores de segundo nivel. Por último, los servidores DNS inferiores conocen a todos los equipos de su dominio, a los servidores DNS raíz y, ante una consulta, si no conocen la IP, le preguntan a un servidor raíz. Todo esto se hace para asegurar que las consultas DNS se resuelvan de manera rápida y eficiente en todo momento.

Funcionamiento

1. El cliente hace una consulta DNS preguntando por la dirección IP de www.google.com a su servidor DNS local.
2. Si el servidor DNS local no tiene la información en su caché, enviará la consulta al servidor raíz.
3. El servidor raíz no conoce la dirección IP de www.google.com, pero conoce el servidor TLD para el dominio .com y responde con esta información al servidor DNS local.
4. El servidor DNS local envía la consulta al servidor TLD para el dominio .com.
5. El servidor TLD para el dominio .com no conoce la dirección IP de www.google.com, pero conoce el servidor autoritativo para el dominio .google.com y responde con esta información al servidor DNS local.
6. El servidor DNS local envía la consulta al servidor autoritativo para el dominio .google.com.
7. El servidor autoritativo para el dominio .google.com conoce la dirección IP de www.google.com y responde con esta información al servidor DNS local.
8. El servidor DNS local guarda la respuesta en su caché y envía la dirección IP de www.google.com al cliente que realizó la consulta inicial.
9. El cliente puede ahora acceder a www.google.com mediante la dirección IP obtenida.

Tipos de consultas

- **Recursivas**: el servidor DNS hará todo el trabajo necesario para devolver la respuesta completa a la petición. Esto puede implicar múltiples transacciones del servidor con otros servidores DNS. Si el servidor DNS que recibe la consulta no tiene la respuesta, entonces él mismo se encargará de buscarla en otros servidores DNS hasta encontrarla y devolverla al solicitante. Por lo general, los servidores DNS que utilizamos en nuestra red son recursivos, lo que significa que realizan este tipo de consultas.
- **Iterativas**: se utilizan cuando el servidor DNS tiene la respuesta a la consulta o si tiene información útil, pero no puede resolver la consulta por sí solo. En este caso, en lugar de buscar en otros servidores DNS, el servidor DNS devuelve información útil al

solicitante. Los servidores raíz y TLD son no recursivos y solo devolverán información útil al solicitante si no pueden resolver la consulta por sí mismos.

Caché DNS

La caché DNS es una función que permite a los servidores DNS almacenar temporalmente las respuestas a las consultas realizadas por los clientes. Esto se hace para reducir el tiempo de respuesta en futuras consultas y reducir la carga de trabajo en los servidores DNS de niveles superiores.

Cuando un servidor DNS resuelve una consulta de un cliente, almacena la respuesta en su caché junto con el tiempo de vida (TTL) asociado a esa respuesta. El TTL indica durante cuánto tiempo la respuesta puede ser almacenada en caché antes de que deba ser eliminada. Si otro cliente realiza la misma consulta mientras la respuesta todavía está en caché, el servidor DNS puede proporcionar la respuesta almacenada en lugar de tener que buscar la respuesta de nuevo en otros servidores DNS.

Además de almacenar en caché las respuestas correctas a las consultas DNS, los servidores DNS también pueden almacenar en caché las respuestas negativas, es decir, cuando un nombre de dominio no existe o no está disponible. Esto se conoce como Negative Caching.

Una respuesta autoritativa es una respuesta que proviene directamente de un servidor DNS que tiene la autoridad sobre un nombre de dominio específico. En otras palabras, un servidor DNS que aloja la zona de un dominio en particular se considera autoritativo para ese dominio. Cuando un servidor DNS recibe una consulta para un nombre de dominio, primero verifica si tiene la respuesta en su caché.

La tendencia actual es que los clientes también tengan su propia caché DNS, para evitar consultar al servidor DNS cada vez que se accede a un nombre de dominio. Esto se puede hacer mediante la configuración de un servidor DNS local en el cliente o mediante el uso de un servicio de caché DNS como dnsComandos nslookup y dig:
– Envía peticiones DNS al servidor DNS por defecto
– Por defecto, envían peticiones estándar.
– Permiten especificar otros tipos de peticiones.
• Comando bind:
– Berkeley Internet Name Domain
– Servidor DNS más utilizado en Internet.
– Incluido en Linuxmasq en Linux. Sin embargo, es importante tener en cuenta que la caché del cliente solo se utiliza para resolver nombres de dominio en el equipo local y no se comparte con otros equipos en la red.

Servidor DNS de Forwarding

Un servidor DNS de Forwarding es un tipo de servidor DNS que se utiliza para reenviar las consultas DNS a otros servidores DNS. Este servidor no tiene ninguna zona responsable de la que sea dueño y, por lo tanto, no almacena ninguna información en disco. En lugar de eso, se encarga de enviar las solicitudes de consulta a otros servidores DNS y reenviar las respuestas a los clientes que las solicitaron.

Este tipo de servidor DNS se utiliza comúnmente en entornos de red empresariales o en hogares donde se desea una respuesta rápida y eficiente para consultas DNS frecuentes. Los servidores DNS de forwarding también suelen utilizar una caché para almacenar las respuestas a consultas frecuentes, lo que permite una respuesta más rápida para las solicitudes futuras.

Es común que los routers inalámbricos incorporen un servidor DNS de forwarding para reenviar las consultas de DNS a los servidores DNS del ISP. De esta manera, se evita el acceso a la red del ISP, y las consultas en caché se resuelven en la LAN local, lo que mejora la velocidad y eficiencia de la resolución de nombres de dominio.

Consultas DNS

- **Consulta A (Estándar)**: se utiliza para obtener la dirección IP asociada a un nombre de dominio. Por ejemplo, si quieres saber la dirección IP de www.google.com, puedes hacer una consulta A como "dig www.google.com". Esto devolverá la dirección IP asociada a ese nombre de dominio.
- **Consulta CNAME**: se utiliza para obtener el nombre de un alias. Un alias es un nombre de dominio alternativo que se utiliza para referirse a otro nombre de dominio. Por ejemplo, si un sitio web tiene un alias "www2.misitio.com" para "www.misitio.com", una consulta CNAME para "www2.misitio.com" devolverá el nombre de dominio real "www.misitio.com".
- **Consulta PTR (Consulta inversa – Pointer)**: se utiliza para obtener el nombre de dominio asociado a una dirección IP. Esta consulta es inversa a la consulta A, ya que en vez de buscar la dirección IP a partir de un nombre de dominio, se busca el nombre de dominio a partir de una dirección IP. Para hacer una consulta PTR, se necesita invertir la dirección IP y agregar ".in-addr.arpa" al final. Por ejemplo, si quieres saber el nombre de dominio asociado a la dirección IP 88.221.32.170, debes hacer una consulta PTR como "dig -x 88.221.32.170".
- **Consulta MX (Mail Exchanger)**: es utilizada por los servidores de correo electrónico para buscar información sobre los servidores de correo disponibles para un dominio de destino. Cuando un servidor de correo electrónico intenta enviar un correo a un destinatario en un dominio determinado (por ejemplo, gmail.com), primero realiza una

consulta MX al servidor DNS de su propio dominio, para obtener una lista de los servidores de correo disponibles en el dominio de destino. La respuesta a la consulta MX incluye una lista de servidores de correo disponibles para el dominio de destino, ordenados por preferencia. Los servidores de correo con una preferencia menor deben intentarse primero antes que los de preferencia mayor. Esto se debe a que un servidor de correo con una preferencia menor se considera más confiable o preferido que uno con una preferencia mayor.

Comandos

- **nslookup**: está disponible en la mayoría de los sistemas operativos, incluyendo Windows y Linux. Por defecto, envía consultas DNS estándar al servidor DNS por defecto configurado en el sistema. Sin embargo, también se pueden especificar otros servidores DNS con la opción "-server" y otros tipos de consulta con la opción "-type".
- **dig**: es una herramienta más avanzada que también se utiliza para realizar consultas DNS. Al igual que nslookup, puede enviar consultas DNS a un servidor DNS específico y especificar el tipo de consulta. Además, proporciona una salida más detallada, lo que lo hace útil para la resolución de problemas de DNS. También permite la realización de consultas recursivas y no recursivas.
- **bind (Berkeley Internet Name Domain)**: es un servidor DNS de código abierto que es el más utilizado en Internet. Incluido en la mayoría de las distribuciones de Linux, el servidor BIND es altamente configurable y escalable, lo que lo hace popular entre los administradores de sistemas. BIND soporta todos los tipos de consulta DNS y puede ser configurado para actuar como servidor DNS autoritativo o como servidor de forwarding. Además, BIND es capaz de realizar la resolución de nombres de dominio inversa (PTR).