Redes y Comunicaciones 2017

Práctica 3

Autor: Fermín Minetto (http://www.github.com/ferminmine)

1) Investigue y describa cómo funciona el protocolo DNS

El protocolo DNS es un protocolo de la capa de aplicación que se ejecuta entre sistemas terminales que están en comunicación utilizando el paradigma cliente-servidor y se asa en un protocolo de transporte subyacente extremo a extremo para transferir los mensajes DNS entre los sistemas terminales en comunicación. DNS lleva a cabo una de las funciones básicas de Internet: traducir los nombres de hosts en sus direcciones IP.

Funcionamiento

Primero la app invocará al lado cliente del servidor DNS, especificando el nombre del host del que necesita una traducción a dirección IP. La aplicación DNS entra en funcionamiento y envía un mensaje a la red, utilizando el protocolo de transporte UDP en el puerto 53 (si el mensaje supera los 512 bytes se utiliza TCP). Transcurrido un cierto retardo, del orden de los milisegundos a los segundos, el servicio DNS del host del usuario recibe un mensaje de respuesta DNS que proporciona la traducción deseada. Por eso, *desde la perspectiva de dicha aplicación que se ejecuta en el host del usuario, DNS es una caja negra que proporciona un servicio de traducción simple y directo*. La consulta realizada por el cliente DNS no se realiza a un único servidor, sino que es una consulta que se va *delegando entre distintos servidores jerárquicos distribuidos a lo largo del mundo*, puesto que el diseño del servicio DNS no se encuentra centralizado debido a características como el volumen del tráfico recibido, la distancia ante millones de peticiones de todo el mundo, mantenimiento para estar actualizado y que sería un único punto de fallo. *Una base de datos centralizada almacenada en un único servidor DNS simplemente no podría escalarse*.

2) ¿Qué es un root server? ¿Qué es un generic top-level domain (gtld)?

Como los servidores DNS están organizados de manera jerárquica, se pueden diferenciar distintos niveles entre ellos. *En el nivel superior de la jerarquía se encuentran los servidores raíz, o los root servers*. La solicitud DNS comienza llegando a uno de los servidores raíces, que la devolverá indicando la dirección del servidor TLD que le corresponde autoridad sobre el dominio. A su vez el TLD devolverá la solicitud con la dirección del servidor autoritativo que podrá devolver la dirección IP.

Los servidores TLD se pueden clasificar en tres grupos gTLD, ccTLD y arpaTLD. Los gTLD, contienen dominios con propósitos específicos: tales como .com (comercial), .edu (educación), etcétera. Los country-codeTLD contienen dominios delegados a diferentes países del mundo: por ejemplo .ar, .es, etc.
No sería lo mismo un www.prueba.com a un www.hola.com.ar. En el primero sería un gTLD, y en el segundo un ccTLD.

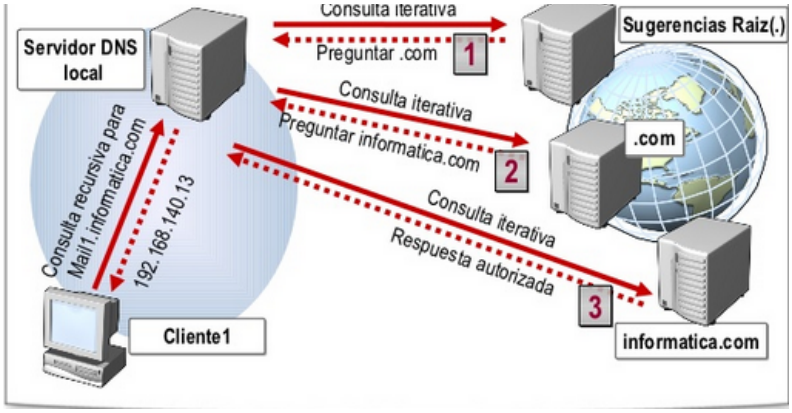
Los servidores autoritativos son los que almacenan efectivamente los registros DNS que establecen la correspondencia entre el nombre de host y una IP.

3) ¿Qué es una respuesta del tipo autoritativa?

Una respuesta del tipo autoritativa es aquella en la que el que nos provee de la respuesta DNS no es aquél servidor que contiene el registro DNS con la correspondencia entre la IP y el host, es decir, el que posee la autoridad sobre la misma correspondencia. Es común que nuestro host reciba respuestas no autoritativas ya que la mayor parte de las consultas se hacen sobre un servidor DNS local sobre una LAN, o configurado por nuestro ISP, que actúa como proxy, por lo que el que nos respondería las consultas sería nuestro servidor DNS local, el cual hizo una consulta que probablemente si recibió una respuesta autoritativa.
En NSLOOKUP en caso de ser una respuesta no autoritativa lo aclara, en caso que sea autoritativa no lo hace.

4) ¿Qué diferencia una consulta DNS recursiva de una iterativa?

Una consulta recursiva es aquella en la cual se le pide a un servidor que resuelva la correspondencia entre host y servidor por si mismo, realizando las consultas extras a otros servidores necesarias por su cuenta.
Las consultas iterativas son las consultas realizadas a los servidores DNS sobre un determinado nombre de host hasta llegar a un servidor autoritativo que pueda devolver la correspondencia definitiva entre el host solicitado y la IP.
Por lo general la consulta de un host a su servidor de DNS local suele ser una consulta recursiva, mientras que las consultas restantes hechas por partes del servidor DNS local hacia el resto de los servidores DNS de la jerarquía serán iterativas.



5) ¿Qué es el resolver?

El resolver es el servidor DNS al que nuestra computadora solicita que resuelva un nombre de host en dirección IP. La dirección IP del servidor DNS al que consultaremos se configura en */etc/resolv.conf*.

6) Describa para que se utilizan los siguientes registros: A, MX, PTR, AAAA, SRV, NS, SOA, CNAME, TXT

Los servidores DNS que implementan conjuntamente la base de datos distribuída DNS almacenan los registros de recursos (RR), incluyendo los que proporcionan las correspondencias entre nombre de host y dirección IP. Cada mensaje de respuesta DNS transporta uno o más registros de recursos. Un registro esta compuesta por los siguientes cuatro campos: (Nombre, Valor, Tipo, TTL). El significado de nombre y valor dependen del tipo.

- **A:** Nombre es un host y valor es la dirección IP
- **MX:** Nombre es un alias de correo electrónico y valor el nombre canónico
- **CNAME:** Nombre es un alias de un host y el valor es un nombre canónico
- **PTR:** Almacena de manera inversa al A; para el “nombre” de una IP (dirección con un postfijo) el valor que sería el host al que está asociado. Aunque sea lo más habitual preguntar por la dirección de un host, a veces resulta necesario consultar de manera inversa para alguna operación de control.
- **AAAA:** Análogo al registro A, pero en lugar de almacenar una direcion IPv4 almacena una dirección IPv6.
- **SRV:** -
- **NS:** Nombre es un dominio y valor es el nombre de host de un servidor DNS autoritativo que sabe como obtener las direcciones IP de los hosts del dominio.
- **SOA: “**Contiene identificadores del servidor de nombres con autoridad sobre la denominación y su operador, y diversos contadores que regulan el funcionamiento general del sistema de nombres de dominio (DNS) para la denominación”
- **TXT:** Proporciona información extra del dominio.

7) dig www.redes.unlp.edu.ar

La consulta fue recursiva y autoritativa. Esto significa que el servidor DNS local al que le hicimos la consulta tenía registros con información del sitio www.redes.unlp.edu.ar y fue recursiva porque es nuestro servidor DNS local al que le delegamos la responsabilidad de hacer las consultas iterativas extras necesarias para poder traducir el host en una dirección IP.
En los flags de respuesta nos dice si la respuesta fue autoritativa o recursiva.
Flag aa: authoritative answer.
Flag ra: recursive available.
En la parte de la respuesta, hay que chequear la respuesta con el registro NS, ya que el registro de tipo NS almacena quien es el servidor que almacena el registro (A) con la correspondencia entre nombre de host y dirección IP.
Es posible obtener esta misma informción con el comando host, simplemente se añade el parametro -v (host -v www.redes.unlp.edu.ar) .
En la parte de SERVER aclara a que server nuestra computadora le hizo la solicitud recursiva, y si se quiere utilizar un server distinto se puede hacer añadiendo al final del comando @IP. Ejemplo: dig google.com. @216.221.235.12.

8,9 y 10) dig www.google.com

Los números antes del resultado es el TTL del registro en la caché local e intermedias. Pasado ese tiempo debe borrar esa entrada de la caché y volverse a pedir.
El orden de los servidores autoritativos para resolver el host de google aparece en distinto orden para balancear la carga de los servidores DNS asociados.
Los servidores de correo asociados al dominio google.com se pueden averiguar utilizando el comando *dig -t mx google.com*. Los servidores de correo a utilizar estará dado por el número de prioridad más pequeño de todos.
Para averiguar la cantidad de servidores DNS que tiene un dominio, por ejemplo, unlp.edu.ar, es necesario hacer *dig -t ns info.unlp.edu.ar*.

11) host y nslookup

Host funciona de manera similar a dig, para averiguar los servidores de correo electrónico de un dominio, por ejemplo de google, se utiliza host -t mx google.com.
Para los servidores DNS funciona de manera análoga al dig.

12) ¿Qué función cumple en Linux el archivo /etc/hosts o en Windows el archivo \WINDOWS\sys-tem32\drivers\etc\hosts?

El archivo hosts de un ordenador es usado por el sistema operativo para guardar la correspondencia entre dominios de internet y direcciones IP. Este es uno de los diferentes métodos que usa el sistema operativo para resolver nombres de dominios.
Antiguamente cuando no había servidores DNS que resolvieran los dominios, el

archivo hosts era el único encargado de hacerlo, pero dejó de utilizarse cuando Internet empezó a crecer en nombres de dominio

14) ¿Qué tipo de consultas (iterativas o recursivas) realiza la PC a su servidor de DNS? ¿Qué tipo de consultas realiza el servidor de DNS para resolver requerimientos de usuario como el anterior? ¿A quién le realiza estas consultas?

La computadora realiza una **consulta recursiva al resolver** ya que le indicara que va esperar una respuesta de la resolución a IP. Este resolver o servidor DNS local **va a tener que hacer consultas iterativas a los otros servidores DNS** (en caso que no tenga la información solicitada en la caché), comenzando por un root server y pasando por gTLDs o ccTLDs hasta llegar a un servidor autoritativo que contenga el registro con la dirección efectiva del host solicitado.

15) Relacione DNS con HTTP. ¿Se puede navegar si no hay servicio DNS?

DNS y HTTP son protocolos que se ejecutan en la capa de aplicación. Aunque ambos son muy importantes para el funcionamiento de Internet, proveen funcionalidades distintas. HTTP es el protocolo utilizado para recuperar documentos (páginas web o de otro tipo) en servidores. DNS traduce nombres de dominio en direcciones IP.
En el momento en que un usuario escribe el nombre de un sitio en el navegador, el usuario esperaria que la página cargue. Para poder cargar la página, primero debe recuperarse y para eso se utiliza el protocolo HTTP. Antes de que se pueda enviar un mensaje HTTP al sitio para recuperar la página, primero es necesario averiguar la dirección IP del sitio, y para eso se utilizaria el servicio de traducción de direccion de host a direccion IP que provee DNS.
Sería posible navegar en Internet sin servicio DNS, pero sería necesario conocer de antemano las direcciones IP de los sitios que se desean visitar. Para esto se podría hacer como antes, que se agregaban las correspondencias entre nombre de host y dirección IP de manera manual al archivo hosts del sistema, o utilizar de forma directa la dirección IP.

16) Topología: Si desde PC-A se desea obtener la IP de www.unlp.edu.ar, cuáles serían, y en qué orden, los pasos que se ejecutarán para obtener la respuesta. ¿Dónde es recursiva la consulta? ¿Y dónde iterativa? ¿Qué root-server debería ser elegido para responder? ¿Por qué?

Asumiendo que DNS Server es el servidor DNS resolver de PC-A, entonces primero PC-A le haría una consulta recursiva pidiendo la direccion IP de www.unlp.edu.ar a DNS Server. Luego, DNS Server haría las consultas iterativas que hagan falta para resolver la petición. La primera de ellas sería al root server que tenga configurado, posiblemente el A, puesto que queda a un router de distancia menos que el B. on la dirección IP del servidor DNS con autoridad sobre el dominio .ar, y luego de realizarle una consulta a este último recibiría la dirección IP del servidor DNS con autoridad sobre unlp.edu.ar. **[DUDA]**

17) ¿A quién debería consultar para que la respuesta sobre www.google.com.ar sea autoritativa? ¿Qué sucede si al servidor elegido en el paso anterior se lo consulta por www.info.unlp.edu.ar? ¿Y si la consulta es al servidor 8.8.8.8?

Debería consultarle al servidor DNS de google. Para eso haria dig -t ns google.com.ar y luego un dig www.google.com.ar @(Dirección IP de algun servidor DNS que devolvió el comando anterior).

18) ¿Qué sucede si al servidor elegido en el paso anterior se lo consulta por www.info.unlp.edu.ar? ¿Y si la consulta es al servidor 8.8.8.8?

No respondería ya que no tendría habilitada la recursión. Si la consulta se hiciera al servidor 8.8.8.8 sería posible, puesto que es un servidor DNS público al que se le pueden hacer consultas recursivas.

Topología

Ver configuración de un root server: /etc/bind/db.
Ver configuración de un DNS: /etc/bind/db.myzone.
Después de modificar la tabla de un DNS, se tiene que incrementar el número de serie y luego reiniciar el servidor DNS ejecutando el comando /etc/init.d/bind9 restart.