Redes y Comunicaciones

Ulises J. Cornejo Fandos

Marzo 2017

Practica 3

1.1 Capa de Aplicación - DNS

1. **Investigue y describa cómo funciona el DNS. ¿Cuál es su objetivo?**

   El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. De esta manera, al buscar el IP de una página, se comienza buscando el GTLD(generic top level domain) en los root server, que son servidores DNS encargados de proporcionar la IP de algún servidor DNS que contenga el subdominio siguiente (de existir) o la IP de algún servidor que contenga la IP de la página completa.

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

   Un root server es un servidor DNS encargado de almacenar todas las direcciones IP de los servidores que alojan los GTLD(generic top level domain). Un GTLD es un dominio perteneciente a la jerarquía más alta, es decir, que no lo precede ningún otro dominio en las direcciones URL de una página.

3. **¿Qué es una respuesta del tipo autoritativa?**

   Una respuesta de tipo autoritativa es una respuesta realizada por un servidor de tipo autoritativo.

4. **¿Qué diferencia una consulta DNS recursiva de una iterativa?**

   Una respuesta recursiva es aquella que te retorna una respuesta completa, el servidor DNS comprueba la zona de búsqueda directa y la caché para encontrar una respuesta a la consulta. En cambio una respuesta iterativa es aquélla efectuada a un servidor DNS en la que el cliente DNS solicita la mejor respuesta que el servidor DNS puede proporcionar sin buscar ayuda adicional de otros servidores DNS. El resultado de una consulta iterativa suele ser una referencia a otro servidor DNS de nivel inferior en el árbol DNS Consulta iterativa. En si, una respuesta recursiva utiliza las respuestas iterativas para poder resolver completamente la consulta.

5. **¿Qué es el resolver?**

   El resolver es un conjunto de rutinas de la biblioteca C, que proporciona acceso al Sistema de Nombres de Dominio de Internet (DNS). El archivo de configuración del resolver contiene información que es leída por las subrutinas cada vez que un proceso le reclama. El archivo está diseñado para ser fácilmente comprensible y contiene una lista de palabras claves con valores que proporcionan diferentes tipos de información del resolver.

6. **Describa para qué se utilizan los siguientes tipos de registros de DNS**

   - **A:** Dirección (address). Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.

- **MX:** Intercambio de correo (mail exchange). Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.
- **PTR:** Indicador (pointer). También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración de la zona DNS inversa.
- **AAAA:** Dirección (address). Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.
- **SRV:** Registro de ubicación de servicio generalizado, utilizado para protocolos más nuevos en vez de crear protocolo-registros concretos como MX.
- **NS:** Servidor de nombres (name server). Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.
- **CNAME:** Nombre canónico (canonical Name). Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como FTP y servidor web) en un servidor con una sola dirección IP. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). Esto también es usado cuando corres múltiples servidores HTTP, con diferentes nombres, sobre el mismo host. Se escribe primero el alias y luego el nombre real.
- **SOA:** Autoridad de la zona (start of authority). Proporciona información sobre el servidor DNS primario de la zona.
- **TXT:** Originalmente para arbitrario humano-texto legible en un DNS registro. Desde el temprano @1990s, aun así, esto graba más a menudo lleva máquina-dato legible, como especificado por RFC 1464, opportunistic encriptación, Sender Marco de Política, DKIM, DMARC, DNS-SD, etc.

7. **En la VM, utilice el comando dig para obtener la dirección IP del host www.redes.unlp.edu.ar. Responda:**

   (a) **¿La solicitud fue recursiva? ¿Y la respuesta? ¿Cómo lo sabe?**
   La solicitud fue recursiva ya que las solicitudes realizadas por un user agent al servidor DNS local son de ese tipo. La respuesta es recursiva.

   (b) **¿Puede indicar si se trata de una respuesta autoritativa?**
   Puedo indicarlo ya que existe un flag que se activa cuando se trata de una respuesta autoritativa.

   (c) **¿Cuál es la dirección IP del servidor de DNS al que le realizó la consulta? ¿Cómo lo sabe?**
   La dirección IP del servidor DNS al que se le realizó la consulta es 127.28.0.29. Esto lo se ya que el comando dig me devuelve esta información en el campo SERVER.

   (d) **¿Es posible obtener la misma información con el comando host? ¿Cómo?**
   Es posible ejecutando el siguiente comando:

   ```
   host -v/d www.redes.unlp.edu.ar
   ```

   Pero este último es mucho menos específico que el comando dig.

8. **Usando el comando dig, averigüe la dirección IP de www.google.com. Observe los números que aparecen antes de la palabra IN. Vuelva a ejecutar la misma consulta y observe nuevamente esos números. ¿Qué ocurrió? ¿Por qué? ¿Qué significado cree que tienen dichos números?**

9. **Observe nuevamente las respuestas del paso anterior, ¿el orden de los servidores en la respuesta es siempre el mismo? ¿Por qué piensa que sucede esto?**

   Deben cambiar su orden dependiendo de cual tiene menor tiempo de respuesta al momento de ejecutar el comando.

10. **Utilizando el comando dig responda (debe tener conexión a Internet para realizar este ejercicio):**

    (a) **Cantidad de servidores que aceptan correos para el dominio gmail.com.**

    Se ejecuta el comando:

    dig -t mx gmail.com

    Hay 5 servidores que aceptan correos para el dominio gmail.com. Esto puedo saberlo por el campo ANSWER del header, y puedo visualizar los servidores correspondientes en la ANSER SECTION.

    (b) **Cuándo se envía un correo a una cuenta gmail.com, ¿cuál de los servidores recibirá el correo? Justifique.**

    Lo va a buscar recibir el servidor cuya prioridad sea mayor(menor número), aunque si el servidor está muy saturado, puede que lo reciba otro (el siguiente siguiendo la prioridad).

    (c) **¿En qué ocasión los demás servidores de correo recibirían correos dirigidos al dominio gmail.com? ¿Qué sucede luego de que uno de estos servidores recibe algún correo para el mencionado dominio?**

    En el caso que un servidor esté muy saturado, puede que lo reciba el siguiente. Cuando uno de los servidores recibe un correo, lo envía al servidor local del usuario.

    (d) **Cantidad de servidores de DNS del dominio unlp.edu.ar.**

    (e) **Dirección IP del host www.info.unlp.edu.ar.**

    - 163.10.5.71

    Comando utilizado:

    - dig -t a www.info.unlp.edu.ar
    - host -t a www.info.unlp.edu.ar
      ↪ www.info.unlp.edu.ar has address 163.10.5.71

11. **Investigue los comando nslookup y host. ¿Para qué sirven? Intente con ambos comandos obtener:**

    (a) **Dirección IP de www.redes.unlp.edu.ar.**

    Se podría consultar con los siguientes comandos:

    - host www.redes.unlp.edu.ar
    - nslookup www.redes.unlp.edu.ar

    (b) **Servidores de correo del dominio redes.unlp.edu.ar.**

    Se podría consultar con los siguientes comandos:

    - host -t mx www.redes.unlp.edu.ar
    - nslookup -querytype=mx www.redes.unlp.edu.ar

    (c) **Servidores de DNS del dominio redes.unlp.edu.ar**

12. **¿Qué función cumple en Linux/Unix el archivo /etc/hosts?**

    Este fichero se utiliza para obtener una relación entre un nombre de máquina y una dirección IP.

13. **Abra el programa Wireshark para comenzar a capturar el tráfico de red en la interfaz con IP 172.28.0.1. Una vez abierto realice una consulta DNS con el comando dig para averiguar el registro MX de redes.unlp.edu.ar y luego, otra para averiguar los registros NS correspondientes al dominio redes.unlp.edu.ar. Analice la información proporcionada por dig y compárelo con la captura.**

14. **Dada la siguiente situación: Una PC en una red determinada, con acceso a Internet, utiliza los servicios de DNS de un servidor de la red". Analice:**

(a) **¿Qué tipo de consultas (iterativas o recursivas) realiza la PC a su servidor de DNS?**

Realiza ambos tipos de consultas, ya que para conseguir la dirección IP de una página determinada, es necesario realizar una consulta de tipo recursiva (las cuales utilizan consultas iterativas internamente) o muchas consultas iterativas (en dicho caso podrí obviarse el uso de consultas recursivas).

(b) **¿Qué tipo de consultas (iterativas o recursivas) realiza el servidor de DNS para resolver requerimientos de usuario como el anterior? ¿A quién le realiza estas consultas?**

Realiza consultas iterativas al siguiente servidor de la jerarquía.

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

Se podría llegar a navegar se si conociera la dirección IP de cada página a la que se quiera acceder, aunque la comodidad se vería disminuida notablemente. Tambien se podría optar por utilizar un sistema similar al que se usaba antes de usar DNS, que sería contar con un archivo HOSTS configurado con cada página que se quiera acceder.

16. **Observar el siguiente gráfico y contestar:**

(a) **Si desde PC-A se desea obtener la IP de www.unlp.edu.ar, cuales serían y en que orden, los pasos que se ejecutarán para obtener la respuesta.**

Como primera instancia se consultaría el servidor DNS local, de no encontrarse en el mismo. ***Consulta Recursiva***

El servidor DNS local realizaría una consulta a cualquiera de los root-server, el root-server le contestaría con la dirección del servidor que contiene la dirección IP del dominio .ar (a.dns.ar). ***Consulta Iterativa***

Automaticamente el servidor DNS local consultará al servidor a.dns.ar, cual es la dirección del servidor que contiene información del dominio edu.ar (ns1.riu.edi.ar). ***Consulta Iterativa***

Nuevamente el servidor DNS local lo consulta al servidor ns1.riu.edu.ar cual es la dirección del servidor que contiene el dominio unlp.edu.ar (unlp.unlp.edu.ar). ***Consulta Iterativa***

Finalmente, el servidor DNS local consulta cual es la dirección de servidor que contiene la página www.unlp.edu.ar al servidor previamente conseguido. ***Consulta Iterativa***

(b) **¿Dónde es recursiva la consulta? ¿Y dónde es iterativa?**

La consulta es recursiva en primera instancia, luego, todas las consultas son iterativas.

(c) **¿Que root-server debería ser elegido para responder?**

Debería ser seleccionado el que tenga menor tiempo de respuesta, que seguramente sea el que tenga menos puntos intermedios de redirección. En este caso, sería el que se encuentra en la parte superior izquierda.

17. **¿A quién debería consultar para que la respuesta sobre www.google.com sea autoritativa?**

A cualquiera de los servidores autoritativos:

- ns1.google.com.
- ns2.google.com.
- ns3.google.com.
- ns4.google.com.

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?**