Taller 3: Distributed Name System (DNS)

Teoría de las Comunicaciones
Departamento de Computación
FCEN - UBA

19.10.2022

1. Objetivos

En este trabajo práctico nos proponemos experimentar con el sistema de resolución de nombres DNS y el proceso de resolución de consultas programando en la biblioteca Scapy de Python.

2. Normativa

- Fecha de entrega: hasta el 09-11-2022.
- El trabajo práctico se deberá enviar por correo electrónico con el siguiente formato:
  to: tdc-doc at dc uba ar
  subject: debe tener el prefijo [tdc-dns]
  body: nombres de los integrantes y las respectivas direcciones de correo electrónico. También pueden agregar una oración explicando en cual parte del trabajo tuvo mayor participación cada integrante.
  attachments: el informe en formato pdf + el código fuente en formato zip.
- No esperar confirmación a menos que reciban una respuesta indicando explícitamente que el mail fue rechazado. Notar que los avisos por exceso de tamaño no son rechazos.

3. Enunciado

3.1. Introducción

DNS es un sistema distrubuido de resolución de nombres. La idea es que cuando una aplicación necesita conectarse con un dispositivo en Internet, usualmente se hace a través de un nombre de dominio en parte debido al gran dinamismo con el que pueden cambiar las direcciones IP y también debido que a los humanos se nos da mejor con los nombres que con los números. Para esto todos los proveedores de servicios de Internet ofrecen el servicio de resolución de nombres mediante servidores denominados **Resolvers**, dedicados específicamente a este proceso. El proceso de resolución de nombres consiste en sucesivas consultas y respuestas por parte de todos los servidores DNS involucrados. Las consultas suelen ser **recursivas** cuando las PC quieren resolver un nombre y le preguntan al Resolver local y suelen ser **iterativas** cuando los Resolvers le pasan las consultas a los servidores **Autoritativos** responsables de cada zona. Por esa razón, en una consulta determinada, puede haber subconsultas recursivas e iterativas.

Además de los servidores autoritativos de cada zona, el sistema DNS no podría funcionar si no existieran servidores por encima de toda la jerarquía de zonas que funcionen como punto de partida para comenzar las consultas iterativas. Estos servidores se llaman **Root Name Servers** y tienen direcciones IP asignadas fijas, que nunca cambian de manera que no haga falta hacer una consulta DNS para resolverlos porque sino no se podría empezar. Estos servidores y sus direcciones IP están listados en la siguiente tabla:

Nombre del Servidor	Direcciones IP (IPv4, IPv6)	Entidad propietaria
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

También se pueden hacer consultas DNS usando `dig` [1] (o `nslookup` [2] en Windows). Este comando es de especial importancia para testear la respuesta de servidores DNS si por alguna razón se sospecha que algo puede no estar funcionando bien. A continuación se muestra la salida del comando `dig www.dc.uba.ar`

```
; <<>> DiG 9.11.5-P4-5.1ubuntu2.2-Ubuntu <<>> www.dc.uba.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50599
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.dc.uba.ar. IN A

;; ANSWER SECTION:
www.dc.uba.ar. 600 IN CNAME www-1.dc.uba.ar.
www-1.dc.uba.ar. 599 IN CNAME dc.uba.ar.
dc.uba.ar. 599 IN A 157.92.27.128

;; Query time: 90 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: dom jun 07 13:32:07 -03 2020
;; MSG SIZE  rcvd: 92
```

Ese sería el resultado de una consulta **recursiva** al Resolver local. Sin embargo, tambien se puede realizar una consulta DNS a un servidor en particular. En `dig` se puede especificar este servidor utilizando el caracter `@` previo a la dirección IP a la que se desea solicitar la consulta. A continuación se muestra el resultado de ejecutar el comando `dig @199.9.14.201 www.dc.uba.ar`

```
; <<>> DiG 9.11.5-P4-5.1ubuntu2.2-Ubuntu <<>> @199.9.14.201 www.dc.uba.ar
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35998
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 7, ADDITIONAL: 15
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 69c520aa52705bae48f7572a5edd19f0e0b59724022f4137 (good)
;; QUESTION SECTION:
;www.dc.uba.ar. IN A
```

```
;; AUTHORITY SECTION:
ar. 172800 IN NS f.dns.ar.
ar. 172800 IN NS b.dns.ar.
ar. 172800 IN NS c.dns.ar.
ar. 172800 IN NS ar.cctld.authdns.ripe.net.
ar. 172800 IN NS d.dns.ar.
ar. 172800 IN NS a.dns.ar.
ar. 172800 IN NS e.dns.ar.

;; ADDITIONAL SECTION:
a.dns.ar. 172800 IN A 200.108.145.50
b.dns.ar. 172800 IN A 200.108.147.50
c.dns.ar. 172800 IN A 200.108.148.50
d.dns.ar. 172800 IN A 192.140.126.50
e.dns.ar. 172800 IN A 170.238.66.50
f.dns.ar. 172800 IN A 130.59.31.20
ar.cctld.authdns.ripe.net. 172800 IN A 193.0.9.59
a.dns.ar. 172800 IN AAAA 2801:140::10
b.dns.ar. 172800 IN AAAA 2801:140:11::50
c.dns.ar. 172800 IN AAAA 2801:140:10::10
d.dns.ar. 172800 IN AAAA 2801:140:dddd::50
e.dns.ar. 172800 IN AAAA 2801:140:eeee::50
f.dns.ar. 172800 IN AAAA 2001:620:0:ff::20
ar.cctld.authdns.ripe.net. 172800 IN AAAA 2001:67c:e0::59

;; Query time: 186 msec
;; SERVER: 199.9.14.201#53(199.9.14.201)
;; WHEN: dom jun 07 13:46:40 -03 2020
;; MSG SIZE  rcvd: 517
```

Como se puede ver, la respuesta no es la misma, sino que este servidor nos responde con el primer nivel de la jerarquía de zonas para que se pueda continuar con la resolución de nombres.

3.2. Primera consigna: Realizando consultas DNS

A continuación se presenta un ejemplo para realizar una consulta a uno de los servidores DNS Root. La consulta es por el registro A del dominio `www.dc.uba.ar` y se hace a uno de los servidores DNS Root que aparecen en la tabla anteriormente.

```
from scapy.all import *

dns = DNS(rd=1,qd=DNSQR(qname="www.dc.uba.ar"))
udp = UDP(sport=RandShort(), dport=53)
ip = IP(dst="199.9.14.201")

answer = sr1( ip / udp / dns , verbose=0, timeout=10)

if answer.haslayer(DNS) and answer[DNS].qd.qtype == 1:
    print "AUTHORITY"
    for i in range( answer[DNS].arcount):
        print answer[DNS].ar[i].rrname, answer[DNS].ar[i].rdata
    print "NAME SERVERS"
    for i in range( answer[DNS].nscount):
        print answer[DNS].ns[i].rrname, answer[DNS].ns[i].rdata
    print "ANSWER"
    for i in range( answer[DNS].ancount):
        print answer[DNS].an[i].rrname, answer[DNS].an[i].rdata
```

Al ejecutarse el código es de esperarse que la sección ANSWER esté vacía dado que la estamos realizando a un servidor Root y nos devuelve los nombres y direcciones IP del primer nivel de la jerarquía de zonas por la cual se podrían continuar las consultas **Iterativas** hasta obtener el registro solicitado. Luego de ejecutar el código, debería obtenerse una salida como la siguiente:

```
AUTHORITY
a.dns.ar. 200.108.145.50
b.dns.ar. 200.108.147.50
c.dns.ar. 200.108.148.50
d.dns.ar. 192.140.126.50
e.dns.ar. 170.238.66.50
f.dns.ar. 130.59.31.20
ar.cctld.authdns.ripe.net. 193.0.9.59
a.dns.ar. 2801:140::10
b.dns.ar. 2801:140:11::50
c.dns.ar. 2801:140:10::10
d.dns.ar. 2801:140:dddd::50
e.dns.ar. 2801:140:eeee::50
f.dns.ar. 2001:620:0:ff::20
ar.cctld.authdns.ripe.net. 2001:67c:e0::59
NAME SERVERS
ar. ar.cctld.authdns.ripe.net.
ar. e.dns.ar.
ar. c.dns.ar.
ar. d.dns.ar.
ar. f.dns.ar.
ar. a.dns.ar.
ar. b.dns.ar.
ANSWER
```

Adaptar el código anterior de manera que, a través de sucesivas consultas iterativas se obtenga el registro MX de un dominio dado. Para esto, tener en cuenta que en cada consulta DNS puede tener 3 tipos de respuestas: i) nos devuelven los servidores DNS a los cuales seguir preguntando, ii) nos devuelven la respuesta a la consulta que estamos haciendo o iii) nos devuelven el registro SOA de la zona indicando que el registro solicitado no forma parte de la base de datos de nombres de la zona.

3.3. Segunda consigna: Experimentación e Informe

Usando la herramienta desarrollada, consultar por los servidores de mail que atienden los correos del dominio de una universidad (su nombre de dominio) en algún lugar del mundo. **Se deben probar tantos dominios como integrantes en el grupo.** Analizar si los servidores de mail que tienen nombres en el mismo dominio que el de la universidad o pertenecen a otro dominio. Si es posible, averiguar también si dichos servidores de mail se encuentran en la misma **zona geográfica**, sólo aproximadamente si es el mismo país, misma región o mismo continente.

El informe debe seguir la siguiente estructura, intentando cumplir con los límites de palabras sugeridos:

- **Introducción (máximo 200 palabras):** Breve explicación de los experimentos que se van a realizar.
- **Métodos y condiciones de los experimentos (máximo 400 palabras):** Explicar el del código implementado y como se realizan las sucesivas consultas iterativas. Además, aclarar las características de las pruebas -horario, día de la semana, etc.-
- **Resultados de los experimentos (máximo 600 palabras):** En esta sección deben presentarse figuras y/o tablas que muestren de manera integral los resultados observados. A modo de sugerencia, se puede mostrar un esquema o una tabla con las consultas y respuestas realizadas para cada dominio que se haya probado.
- **Conclusiones (máximo 200 palabras):** Breve reseña que sintetize las principales dificultades y descubrimientos.

A continuación se sugieren preguntas que se pueden intentar responder una vez obtenidas. No hace falta transcribirlas en el informe y se valorará significativamente el planteo de nuevas preguntas.

- ¿Cuántos niveles de servidores DNS se recorrieron en las sucesivas consultas hasta obtener la información solicitada?

- ¿Todos los servidores DNS Autoritativos que aparecen en las sucesivas respuestas responden a las consultas realizadas?
- ¿Cuántos nombres de servidores de mail encontraron?, ¿Tienen nombres en el mismo dominio que la universidad?
- ¿Cuántas direcciones IP distintas hay? ¿Estas direcciones IP corresponden a dispositivos que están prendidos? (*Hint*: probar con **ping** si responden)
- ¿Coinciden las IPs de los servidores de correo con las IPs de los servidores Web?

3.4. Tercera consigna (OPCIONAL):

En este apartado trataremos de hacer una exploración de las zonas de autoridad en las cuales se sitúan en el espacio de nombres las universidades utilizadas en el apartado anterior. La idea es que se pueda estimar la geolocalización de los nameservers primarios y/o secundarios (con capacidad de respuesta autoritativa) de una zona con respecto a la geolocalización de los hosts a los cuales dan nombre. La flexibilidad del sistema DNS permite que los servers autoritativos de una zona determinada se encuentren arbitrariamente alejados de la zona geográfica a la que brindan el servicio. Sin embargo, cuanto más específica sea una zona (más abajo en el árbol del espacio de nombres), mayores son las chances que los nameservers de la misma se encuentren geolocalizados cerca de los hosts a los cuales dan nombre. Se recomienda usar herramientas de geolocalización, con las IPs encontradas, como la que se encuentra en `https://geotraceroute.com/`.

A modo de sugerencia, en esta actividad se puede graficar, la geolocalización de los nameservers de la zona y de alguno/s de los servidor/es de la universidad. Algunas preguntas que se pueden intentar responder serían:

- ¿Qué grado de cercanía tienen los nameservers a los servers de las universidades? Explique brevemente el resultado de los experimentos realizados.
- ¿El subdominio de la universidad define una zona de autoridad?
- Intente investigar el subdominio de la carrera *Computer Science* dentro del dominio de una universidad (Por ejemplo: `csonline.eng.auburn.edu`) ¿Define una zona de autoridad? Compare con otras carreras de la misma universidad.

Referencias

[1] Comando `dig` `https://en.wikipedia.org/wiki/Dig_(command)`

[2] Comando `nslookup` `https://en.wikipedia.org/wiki/Nslookup`

[3] Internet Assigned Numbers Authority (IANA) `https://www.iana.org/domains/root/servers`