IPv6 – Servicios DNS

Objetivo

El objetivo principal de este laboratorio es presentar el funcionamiento del servicio DNS (*Domain Name System*) en una red IPv6 utilizando el *software* BIND. Para esto, el laboratorio será dividido en dos ejercicios. El primero presentara dos aspectos: la capacidad de los servidores DNS de almacenar tanto registros del tipo A, para direcciones IPv4; y registro del tipo AAAA (quad-A), para direcciones IPv6; y el hecho de que las consultas DNS serán independientes del protocolo de red utilizado, o sea: un servidor DNS será capaz de responder consultas por registros A o AAAA igualmente aunque se disponga de conexión IPv4 o IPv6 solamente.

En el segundo experimento, será trabajada la configuración de un servidor DNS autoritativo para responder a las consultas por registros del tipo AAAA y la resolución de direccionamiento reverso IPv6, destacando algunos puntos relacionados a la utilización de este servicio en una red de doble-pila, o sea con conectividad IPv4 e IPv6.

Para la realización de estos ejercicios serán utilizadas las topologías descriptas en los archivos **servicios-dns1.imn** y **servicios-dns2.imn**.

Introducción Teórica

El protocolo *Domain Name System* (DNS) es una inmensa base de datos distribuida en una estructura jerárquica utilizada para la traducción de nombres de dominios en direcciones IP y vice-versa.

Los datos asociados a los nombres de dominio están contenidos en registro llamados *Resource Records* o RRs (Registro de Recursos). Actualmente existe una gran variedad de tipos de RRs, siendo los mas comunes:

- **SOA** - Indica donde comienza la autoridad sobre una zona;
- **NS** - Indica un servidor de nombres para una zona;
- **A** – Mapeo de nombre a dirección (IPv4);
- **AAAA** – Mapeo de nombre a dirección (IPv6);
- **MX** - Indica un *mail exchanger* para un nombre (servidor de email);
- **CNAME** – Mapea un nombre alternativo (alias);
- **PTR** – Mapeo de dirección a nombre.

El funcionamiento del servicio DNS se basa en una arquitectura cliente/servidor, donde el cliente realiza consultas por RRs a los Servidores Recursivos.

Al recibir consultas, los Servidores Recursivos las encaminan a los Servidores Autoritativos y de acuerdo a la respuesta recibida, continúan el encaminado de las consultas para otros Servidores Autoritativos hasta obtener una respuesta satisfactoria. Dentro de la estructura jerárquica de los DNS, los Servidores Autoritativos responden las consultas sobre las zonas o dominios por los cuales poseen autoridad o una referencia en caso de que conozcan el camino para la respuesta, o una negación en caso de que no la conozcan.

Para que el DNS trabaje con la versión 6 del protocolo de Internet, alguno cambios fueron definidos en el **RFC 3596**.

- Un nuevo tipo de RR fue creado para almacenar las direcciones IPv6 de 128 bits, o AAAA (quad-A). Su función es la de traducir nombres a direcciones IPv6, de forma equivalente al registro del tipo A en IPv4. En caso que un dispositivo posea mas de una dirección IPv6, deberá tener un registro quad-A para cada una de las direcciones. Los registros son expresados de la siguiente forma:

```
Ejemplo:    www.lacnic.net.     IN     A        200.3.14.147
            www.lacnic.net.     IN     AAAA     2001:13c7:7002:4128::147
```

- Para la resolución inversa, fue agregado un registro PTR al dominio *ip6.arpa*, responsable por traducir direcciones IPv6 a nombres. En su representación, la dirección es expresada con el bit menos significativo colocado mas a la izquierda, como se muestra en el siguiente ejemplo:

```
Ejemplo:
        14.3.200.in-addr.arpa     PTR     www.lacnic.net.
        7.4.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.2.1.4.2.0.0.7.7.c.3.1.1.0.0.2.ip6.arpa    PTR    www.lacnic.net.
```

Todos los demás tipos de registro DNS no fueron modificados en su forma de configurarlos, solamente fueron adaptados para soportar el nuevo formato de direcciones de 128 bits.

Descripción de la Práctica

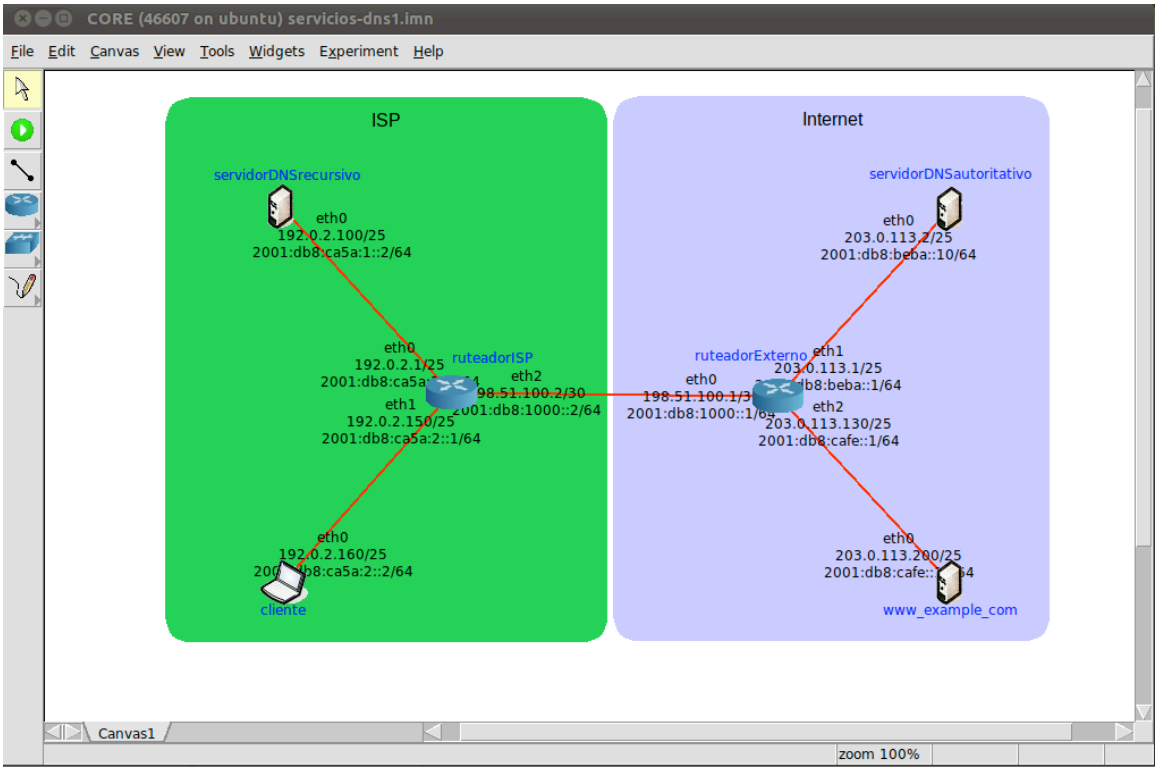
Experimento 1 - Consultas DNS

1. En caso de que este utilizando la maquina virtual provista por LACNIC pase directamente al paso nro. 2. En caso contrario instale el programa BIND, que es una de las implementaciones DNS, en una versión superior a 9.8. En la maquina virtual utilice una Terminal para realizar los comandos:

```
$ wget ftp://ftp.isc.org/isc/bind9/9.8.1-P1/bind-9.8.1-P1.tar.gz
$ tar xvzf bind-9.8.1-P1.tar.gz
$ cd xvzf bind-9.8.1-P1
$ ./configure
$ make
$ sudo make install
```

Para verificar cual es la versión actualizada de BIND ir a www.isc.org/products/BIND

2. Inicie el emulador CORE y abra el archivo "**servicios-dns1.imn**" ubicado en el directorio /home/core/Desktop/servicios/DNS, de la maquina virtual. La siguiente topología debe aparecer:



En esta topología tenemos, localizados en la Internet, la representación de un servidor 'www_example_com' que se corresponde con el nombre de dominio www.example.com y un servidor DNS, con nombre 'servidorDNSautoritativo', que posee autoridad sobre ese dominio. Tenemos también, localizados en el ISP, un servidor DNS recursivo 'servidorDNSrecursivo', que recibe las consultas de resolución de nombres, realizadas por la maquina 'cliente', y las encamina para 'servidorDNSautoritativo'.

3. Verifique la configuración de los nodos de la topología:

   a. Inicie la simulación realizando uno de los siguientes pasos:

      i. Haba ´click´en el botón  ; o
      ii. Utilice el menú Experiment > Start.

4. En este laboratorio, las configuraciones serán realizadas solamente en el equipamiento del ISP y serán iniciadas por el 'servidorDNSrecursivo'. Cree el archivo "named.conf" en el directorio "/etc/named/":

a. Acceda a una Terminal en la maquina 'servidorDNSrecursivo' (doble click sobre el icono) y digite los comandos:

```
# nano /etc/named/named.conf
```

b. Agregue las siguientes línea en el archivo creado:

```
options {
  allow-query {192.0.2.0/24;};
  forward only;
  forwarders {203.0.113.2;};
};
```

Pulse Ctrl+X para salir del ´nano´ y luego 'Y' para confirmar la modificación del archivo.

En caso que este usando la maquina virtual provista por LACNIC el contenido de este archivo puede ser visto en:

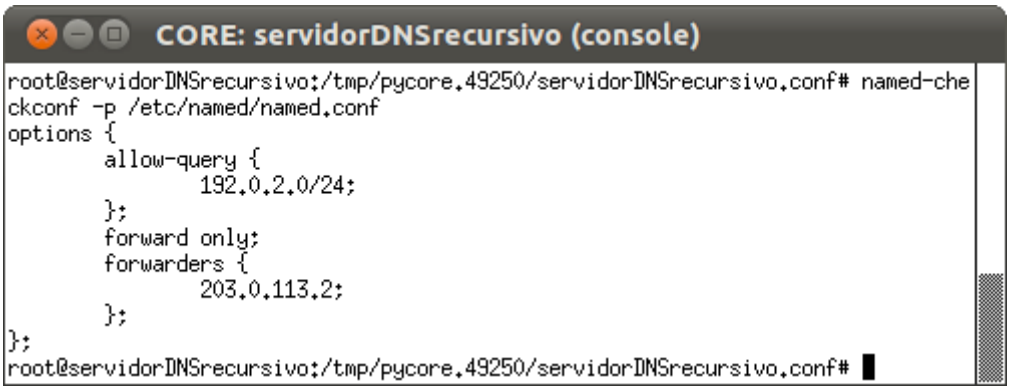
```
/home/core/Desktop/servicios/DNS/named.conf1
```

Este archivo contiene las configuraciones mínimas para el funcionamiento de un servidor DNS recursivo. La opción "allow-query" indica el bloque de direcciones IP que tienen permisos para realizar consultas al servidor; la opción "forward only" indica que este servidor no tiene autoridad sobre ningún dominio, solo encamina consultas para otros servidores, funcionando como un cache de DNS; finalmente la opción "forwarders" define una lista de direcciones IP de servidores DNS para los cuales las consultas deben ser encaminadas. Observe que este servidor recursivo solamente recibe y encamina consultas vía IPv4.

5. El BIND dispone de herramientas que verifican la sintaxis de los archivos de configuración y que puede ayudarnos en la solución de problemas relacionados con el funcionamiento del DNS. De este modo, antes de iniciar el proceso BIND, verifique que el archivo "named.conf" fue generado correctamente:

```
# named-checkconf -p /etc/named/named.conf
```

El resultado debe ser:



6. En caso de que el paso anterior no haya presentado errores de ejecución, inicie el proceso de BIND con el siguiente comando:

```
# named -c /etc/named/named.conf
```

El resultado debe ser:

7. Abra una Terminal en la maquina 'cliente' y configure el archivo "resolv.conf", localizado en el directorio "/etc/", de forma que la maquina comience a utilizar al servidor 'servidorDNSrecursivo' para la realización de las consultas DNS:

   a. Acceda a una Terminal en la maquina ´cliente´ (doble click sobre el icono) y digite el siguiente comando:

      ```
      # nano /etc/resolv.conf
      ```

   b. Agregue el siguiente contenido al archivo resolv.conf:

      ```
      nameserver 192.0.2.100
      ```

      Pulse Ctrl+X para salir del ´nano´ y luego 'Y' para confirmar la modificación del archivo.

      Note que esa regla configura solamente la dirección IPv4 del servidor 'servidorDNSrecursivo'.

8. Desde la máquina 'cliente', realice una consulta DNS al registro AAAA del dominio www.example.com, o sea a la dirección IPv6 asociada a este host.

a. Esta consulta puede ser realizada con la utilización del comando host:

```
# host -t AAAA www.example.com
```

El resultado debe ser:

Aunque el server 'servidorDNSrecursivo' se haya configurado para ser accedido solamente vía IPv4, es capaz de responder a consultas de direcciones IPv6. Esto demuestra que la información almacenada en la base de datos del servidor DNS es independiente de la versión del protocolo de red utilizado en la comunicación.

b. Realice ahora una consulta sin el parámetro "-t AAAA":

```
# host www.example.com
```

El resultado debe ser:

Se puede observar que la respuesta contiene tanto direcciones IPv4 como direcciones IPv6 asociadas al dominio buscado.

9. El próximo paso será habilitar el servidor DNS recursivo para aceptar consultas via IPv6.

a. Para esto, abra una Terminal en la maquina 'servidorDNSrecursivo' (doble click sobre el icono) y digite los siguientes comandos:

```
# nano /etc/named/named.conf
```

b. Agregue la línea "listen-on-v6 { any; };" y agregue en la opción "allow-query" la red IPv6 del ISP. El archivo "named.conf" deberá quedar de la siguiente forma:

```
options {
        allow-query {192.0.2.0/24; 2001:db8:ca5a::/48;};
        forward only;
        forwarders {203.0.113.2;};
```

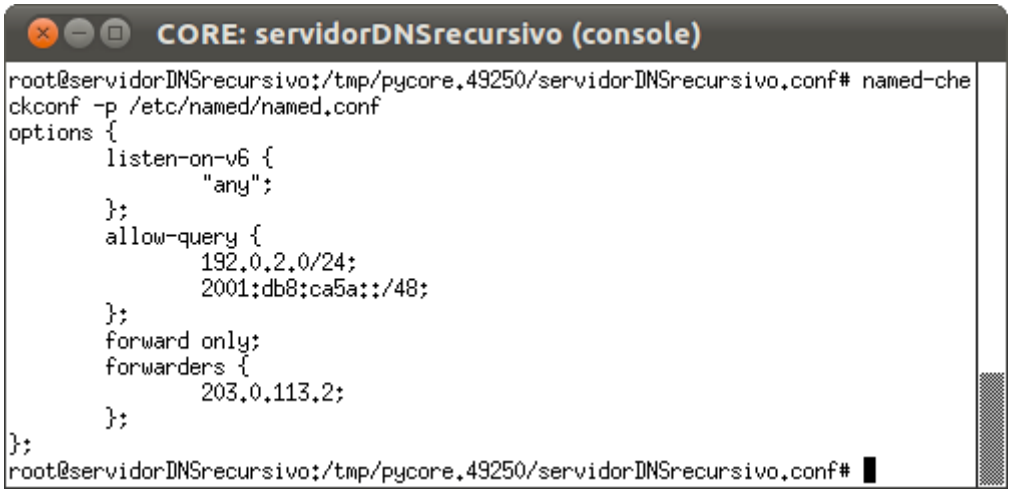
```
        listen-on-v6 { any; };
};
```

Pulse Ctrl+X para salir del 'nano' y luego 'Y' para confirmar la modificación del archivo.

c. Antes de iniciar el proceso BIND, verifique si el archivo "named.conf" fue generado correctamente. Esto puede ser hecho a través del siguiente comando:

```
# named-checkconf -p /etc/named/named.conf
```

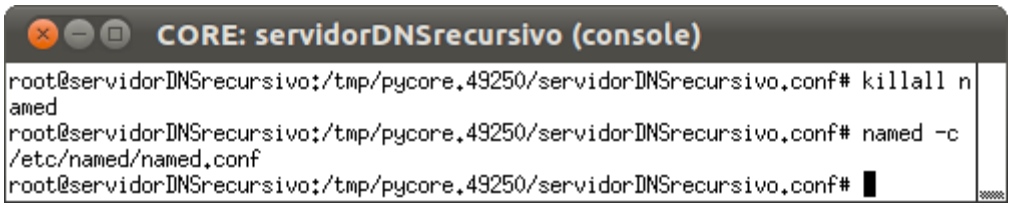
El resultado debe ser:



d. En caso de que el paso anterior no haya presentado errores de ejecución, reinicie el proceso de BIND para que los cambios sean aplicados. Para esto, digite los siguientes comandos:

```
# killall named
# named -c /etc/named/named.conf
```

El resultado debe ser:



10. Abra una Terminal en la maquina 'cliente' y edite el archivo "resolv.conf", ubicado en el directorio "/etc/", de forma que la maquina comience a utilizar también la dirección IPv6 del servidor 'servidorDNSrecursivo' para la realización de las consultas DNS:

a. Abra una Terminal en la maquina 'cliente' (doble click sobre el icono) y digite el siguiente comando:

```
# nano /etc/resolv.conf
```

b. Agregue al contenido existente del archivo “resolv.conf” la siguiente línea:

```
nameserver 2001:db8:ca5a:1::2
```

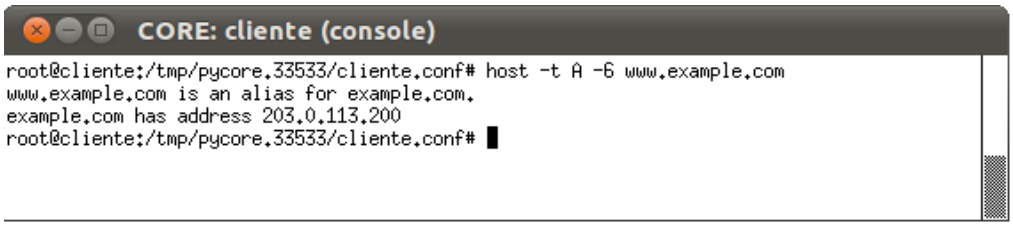
Pulse Ctrl+X para salir del ‘nano’ y luego ‘Y’ para las modificaciones realizadas.

11. Aun en la maquina ‘cliente’, realice una consulta DNS al registro ‘A’ del dominio www.example.com, o sea, a la dirección IPv4 asociada a este host, sin embargo la consulta se fuerza para que se realice vía IPv6

a. Utilice el comando *host* con la opción ‘-6’:

```
# host -t A -6 www.example.com
```

El resultado debe ser:



Así como ocurrió en el punto 8, el servidor DNS recursivo fue capaz de responder por direcciones IPv4.

b. Es posible realizar una serie de pruebas para verificar el funcionamiento del servidor DNS. Algunas opciones pueden ser realizadas mediante la utilización de comandos *dig*, *ping* e *ping6* para verificar la conectividad, resolución inversa ,etc. Algunos ejemplos son:

```
# host 2001:db8:cafe::10
# ping www.example.com
# ping6 www.example.com
# nslookup -type=ANY example.com
```

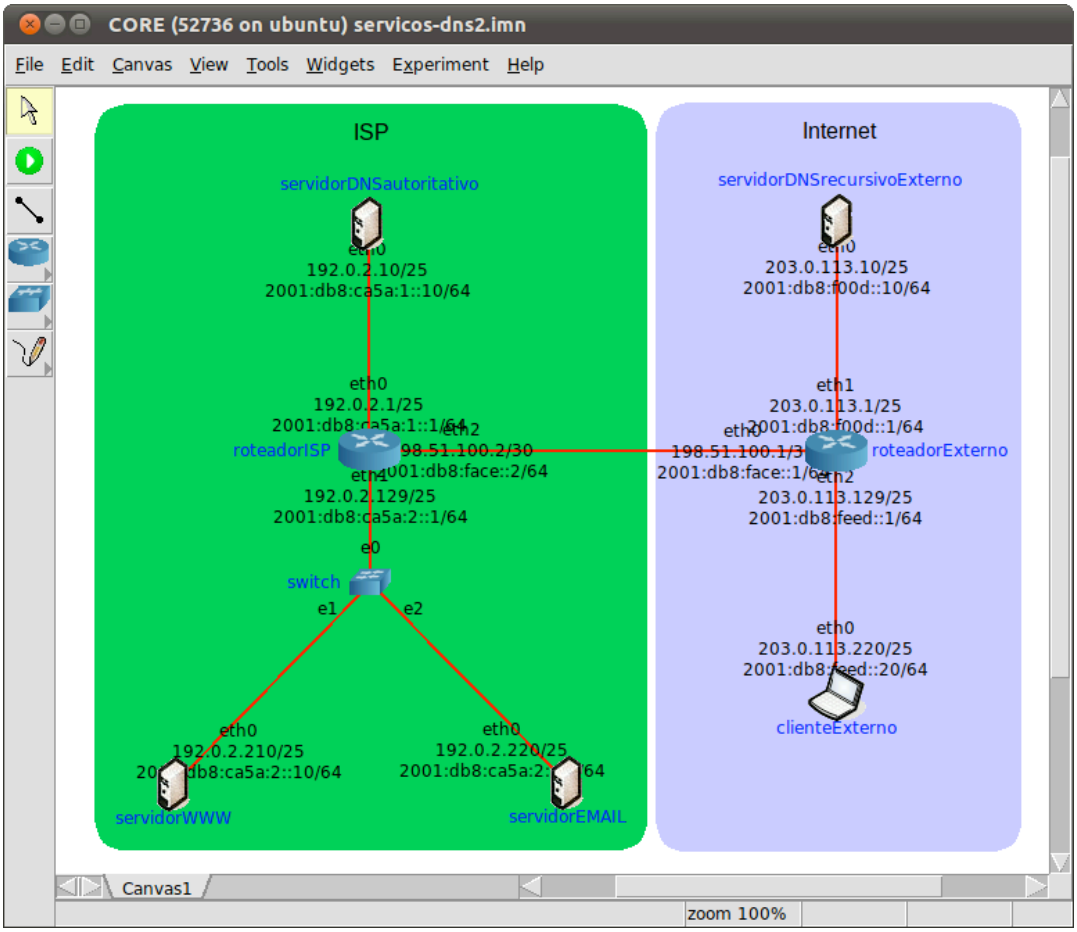
12. Detenga la simulación del CORE :

a. Pulse el botón  o;
b. Utilice el menú Experiment > Stop.

Experimento 2 - DNS: Configurando un Servidor Autoritativo

1. Para la realización de esta segunda experiencia, también es necesaria la instalación del BIND, tal cual fue descripta en el ítem 1 del ejercicio anterior.

2. Ahora, Inicie el CORE y abra el archivo "**servicios-dns2.imn**" ubicado en el directorio /home/core/Desktop/servicios/DNS, de la maquina virtual provista por LACNIC. La siguiente topología debe aparecer:



En esta topología tenemos, ubicados en la Internet, la representación de un servidor DNS recursivo (servidorDNSrecursivoExterno), responsable de recibir las consultas de nombres de sus clientes y re-encaminarlas para los servidores autoritativos, y la de un cliente (clienteExterno) que será utilizado para realizar las consultas DNS, testeando asi las configuraciones aplicadas. En el ISP, se encuentran dos servidores representando los servicios de e-mail y web, y un servidor DNS autoritativo (servidorDNSautoritativo) responsable por responder las consultas del dominio example.com.

3. Verifique las configuraciones de los nodos de la topología.

    a. Inicie la simulación realizando uno de los siguientes pasos:

        i. Pulse el botón  o;
        ii. Utilice el menú Experiment > Start.

4. En este laboratorio, las configuraciones serán realizadas solamente en el equipamiento del ISP. Inicialmente, analice los archivos de configuración de BIND ubicados en el servidor autoritativo del ISP. Este servidor ya esta configurado para responder por consultas de registros tipo A y de direccionamiento reverso IPv4.

    a. Para esto, acceda a una Terminal de la maquina 'servidorDNSautoritativo' (doble click sobre el icono) y visualice el archivo *named.conf* ubicado en el directorio /etc/named/ digitando el siguiente comando:

```
# cat /etc/named/named.conf
```

    El archivo *named.conf* deberá contener las líneas:

```
options {
 directory "/etc/named/";
 listen-on { any; };
 allow-query { any; };
 recursion no;
};

zone "." {
 type hint;
 file "named.root";
};

zone "example.com" {
 type master;
 file "example.com.zone";
};

zone "2.0.192.in-addr.arpa" {
 type master;
 file "192-0-2.db";
};
```

    Este archivo contiene las configuraciones básicas para el funcionamiento del servidor DNS autoritativo. En el primer bloque de comandos (*options)*, tenemos las especificaciones que controlan el comportamiento global del servidor. En este ejemplo, son listadas las siguientes opciones: *directory*, que indica en que directorio de encuentran los archivos utilizados por el BIND; *listen-on*, lista las direcciones IPv4 y puertos habilitados para responder a las consultas DNS, en este

ejemplo esta la configuración por defecto, responde en cualquiera de las interfaces y en el puerto 53; *allow-query*, lista desde cuales direcciones IP tiene permiso para recibir consultas, en este ejemplo estas consultas son aceptadas viniendo desde cualquier dirección IP; y *recursion*, indica si el servidor es capaz (yes) o no (no) de reencaminar consultas a otros servidores autoritativos.

Debajo de opciones, tenemos la lista de archivos con las zonas conocidas por el servidor y dos archivos con las respectivas informaciones. La zona "." Representa la zona raíz de Internet y el archivo *named.root* contiene las direcciones de los servidores raíz DNS (a.root-servers.net - m.root-servers.net) a donde el BIND irá a buscar la información sobre los dominios de primer nivel (por exemplo: .uy, .com, .net, .org....). La zona "example.com" indica el dominio sobre el cual el servidor DNS tiene autoridad para responder consultas (type master) y la "2.0.192.in-addr.arpa" indica cual es la zona de direccionamiento reverso IPv4 por la que el servidor responde. Ahora, analice cada uno de los archivos relacionados a estas dos zonas.

b. Primero analice el archivo example.com.zone localizado en el directorio /etc/named/, para eso digite el siguiente comando:

```
# cat /etc/named/example.com.zone
```

El archivo example.com.zone deberá contener las lineas:

```
;; Se recomienda utilizar un valor de TTL igual a 1 dia (86400 segundos),
;; pero para la demostración utilizaremos un valor menor
$TTL 1s
example.com.    IN    SOA ns.example.com.  root.example.com. (
                          15 ; serial
                          28800 ; refresh
                          7200 ; retry
                          604800 ; expire
                          1s ; ttl
                          )

;;Servidor que responde por el dominio
                    IN    NS       ns.example.com.
ns                  IN    A        192.0.2.10

;;Servidor de e-mail
example.com.        IN    MX   10  mail.example.com.
mail                IN    A        192.0.2.220

;;Politica de SPF
example.com.        IN    TXT      "v=spf1 mx ip4:192.0.2.0/24 -all"
example.com.        IN    SPF      "v=spf1 mx ip4:192.0.2.0/24 -all"

;;Servidor Web
example.com.        IN    A        192.0.2.210
www                 IN    CNAME    example.com.
```

Este archivo representa los registros y directivas relacionadas a la zona example.com.

La directiva $TTL (Time To Live) indica el tiempo que los registros deberán permanecer en el cache sin que sean actualizados, pudiendo ser expresado este teimpo en segundos, minutos, horas, días o semanas (en nuestro ejemplo este tiempo esta seteado en un segundo, solamente para que los ejercicios puedan ser demostrados. La recomendación para sistemas en produccion es que sea al menos de un dia).

c. Ahora, analice el archivo 192-0-2.db localizado en el directorio /etc/named/. Para eso, digite el siguiente comando:

```
# cat /etc/named/192-0-2.db
```

El archivo 192-0-2.db deberá contener las líneas:

```
$TTL 86400
2.0.192.in-addr.arpa. IN SOA ns.example.com.  root.example.com. (
                              15 ; serial
                              28800 ; refresh
                              7200 ; retry
                              604800 ; expire
                              86400 ; ttl
                              )

;; Servidor DNS que responde por esta zona reversa
                       IN   NS   ns.example.com.

;; Direcciones reversas
10                     IN   PTR   ns.example.com.
210                    IN   PTR   www.example.com.
220                    IN   PTR   mail.example.com.
```

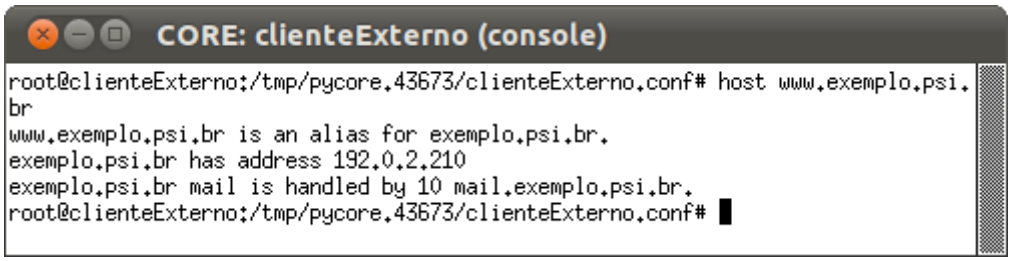
Este archivo presenta los registros y directivas relacionadas a la zona de direccionamiento reverso IPv4.

5. Haga ahora algunas consultas DNS para chequear las configuraciones del servidor DNS autoritativo de la red del ISP.

a. Para esto, acceda a la máquina 'clienteExterno' (doble click sobre el icono) y digite el siguiente comando:

```
# host www.example.com
```

El resultado debe ser:



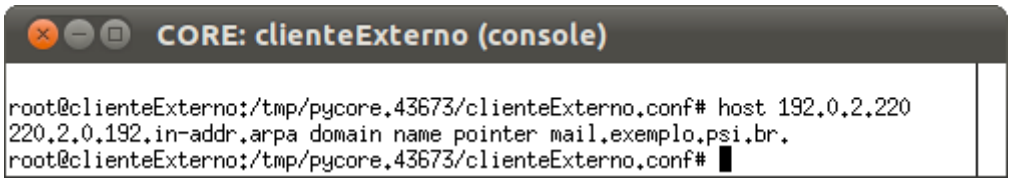
A partir de la respuesta obtenida se puede observar que:

- el nombre www.example.com es un alias para el dominio example.com;
- para el nombre consultado existe una dirección IPv4 asociada, la 192.0.2.210;
- y que existe un servidor de e-mail asociado al dominio example.com, el servidor mail.example.com.

b. Otra consulta que puede ser realizada es la de resolución de direccionamiento reverso. Acceda a la maquina 'clienteExterno' y digite el siguiente comando:

```
# host 192.0.2.220
```

El resultado debe ser:



El contenido de las respuestas esta basado en el contenido de los archivos 192-0-2.db y example.com.zone, existentes en 'servidorDNSrecursivo' y analizados en los ítem 4b y 4c de este ejercicio. Note que, a pesar que los servidores del ISP tienen direcciones IPv6 en sus interfaces de red, ninguna consulta DNS realizada devolvió una dirección IPv6 como respuesta. Esto ocurrio por que no hay esa información registrada en los archivos de zona del servidor DNS autoritativo del ISP.

6. De este modo, el próximo paso es configurar el Servidor Autoritativo para que sea capaz tanto de recibir consultas vía IPv6 como de devolver direcciones IPv6 a las consultas realizadas.

a. Primer paso, acceda a una Terminal en la maquina 'servidorDNSautoritativo' (doble click sobre el icono) y edite el archivo *named.conf* localizado en el directorio */etc/named/* digitando el siguiente comando:

```
# nano /etc/named/named.conf
```

b. Agregue a las opciones la línea listen-on-v6 { any; }; habilitando de esta forma al servidor a recibir consultas via IPv6. El campo *options* del archivo *named.conf* quedara de esta forma:

ATENCION: Solamente agregue la línea indicada, el resto del archivo no debe ser alterado.

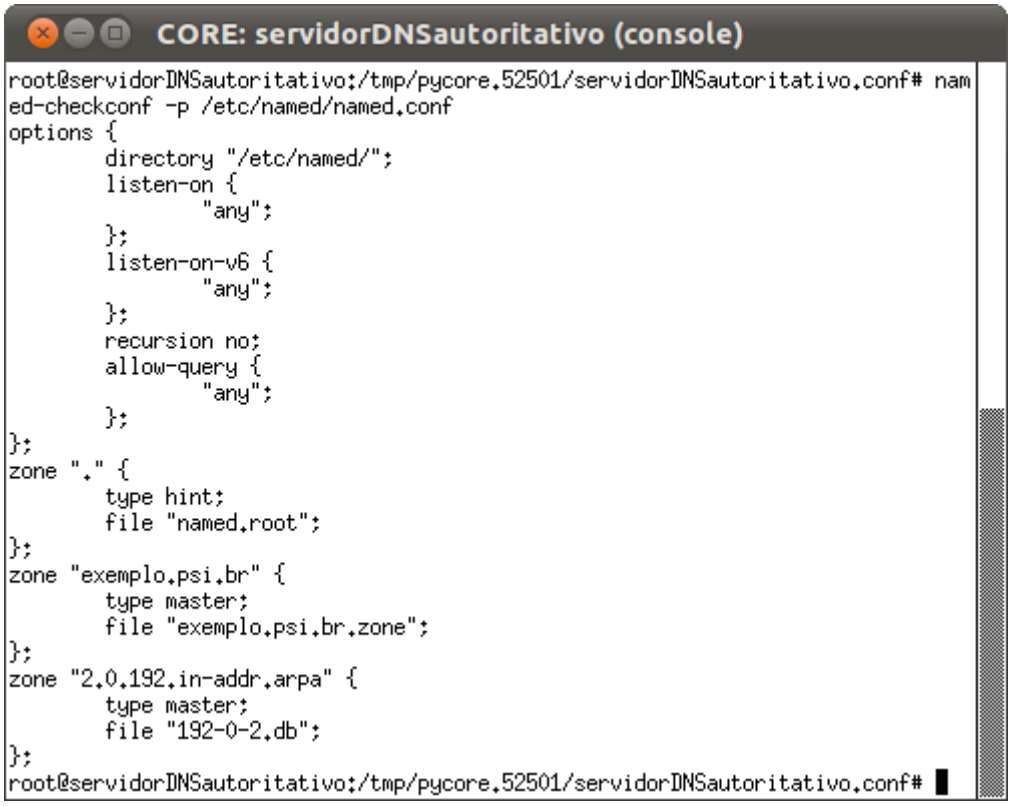
```
options {
 directory "/etc/named/";
 listen-on { any; };
 listen-on-v6 { any; };
 allow-query { any; };
 recursion no;
};
```

Pulse Ctrl+X para salir del 'nano' y luego 'Y' para confirmar la modificación del archivo.

c. Antes de reiniciar el proceso BIND, verifique si el archivo "named.conf" fue generado correctamente. Esto puede ser realizado a través del siguiente comando:

```
# named-checkconf -p /etc/named/named.conf
```

El resultado debe ser:



d. Edite también el archivo example.com.zone ubicado en el directorio /etc/named/, agregando las direcciones IPv6 a los nombres y registros ya configurados y modificando los parametros de las políticas SPF. Para esto, digite el siguiente comando:

```
# nano /etc/named/example.com.zone
```

El archivo example.com.zone deberá contener las líneas:

ATENCION: Las líneas que deben ser agregadas están destacadas abajo!

```
;; Se recomienda utilizar el valor de TTL igual a 1 dia
;; (86400 segundos),
;; para esta demostración utilizaremos un valor menor
$TTL 1s
example.com. IN   SOA ns.example.com.  root.example.com. (
                      15 ; serial
                      28800 ; refresh
                      7200 ; retry
                      604800 ; expire
                      1s ; ttl
                    )
;;Servidor que responde por el dominio
              IN   NS       ns.example.com.
ns            IN   A        192.0.2.10
ns            IN   AAAA     2001:db8:ca5a:1::10
```

```
;;Servidor de e-mail
example.com.     IN   MX   10  mail.example.com.
mail             IN   A        192.0.2.220
mail             IN   AAAA     2001:db8:ca5a:2::220

;;Politica de SPF
example.com.     IN  TXT   "v=spf1 mx ptr ip4:192.0.2.0/24 \
ip6:2001:db8:ca5a::/48 -all"
example.com.     IN  SPF   "v=spf1 mx ptr ip4:192.0.2.0/24 \
ip6:2001:db8:ca5a::/48 -all"

;;Servidor Web
example.com.      IN   A        192.0.2.210
example.com.      IN   AAAA     2001:db8:ca5a:2::210
www               IN   CNAME    example.com.
```

Pulse Ctrl+X para salir de 'nano' y luego 'Y' para confirmar la modificación del archivo.

Si esta utilizando la maquina virtual utilizada por LACNIC, el contenido de este archivo puede ser visto en :

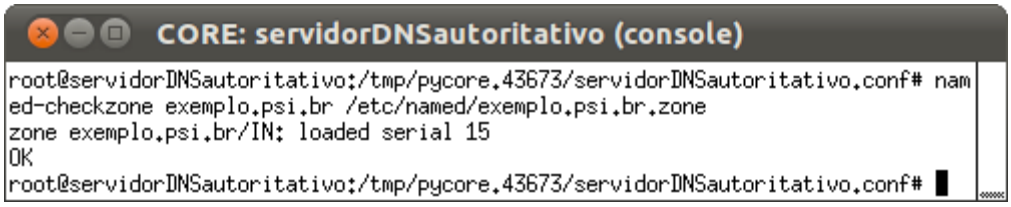
/home/core/Desktop/servicos/DNS/example.com.zone.

Observe que además de agregar los registros AAAA a los nombres de dominios previamente registrados, también fueron agregados parámetros a las políticas de SPF.

e. Para verificar que no existen errores en el archivo de zona generado, digite el siguiente comando en la Terminal de 'servidorDNSautoritativo':

```
# named-checkzone example.com /etc/named/example.com.zone
```

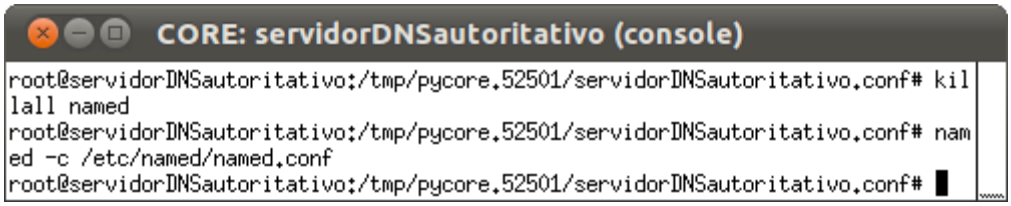
El resultado debe ser:



f. En caso que los pasos anteriores no hayan presentado erroes, reinicie el proceso de BIND para que las modificaciones sean aplicadas. Para eso, digite los siguientes comandos:

```
# killall named
# named -c /etc/named/named.conf
```

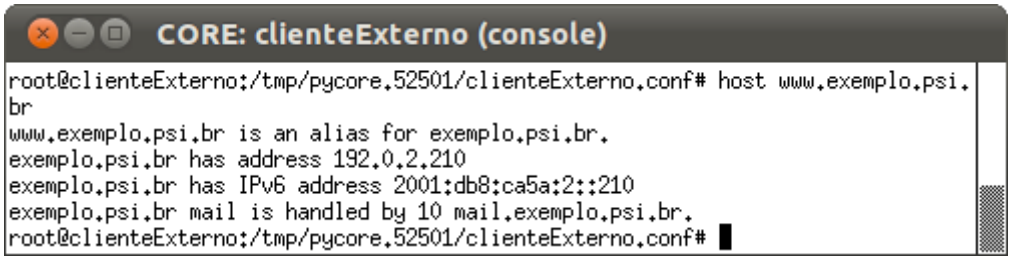
El resultado debe ser:



g. Para verificar si las modificaciones fueron realizadas correctamente, acceda a la maquina 'clienteExterno' (doble click en el icono) y realice algunas consultas DNS. Para eso, utilice el comando host digitando lo siguiente:

```
# host www.example.com
```

El resultado debe ser:

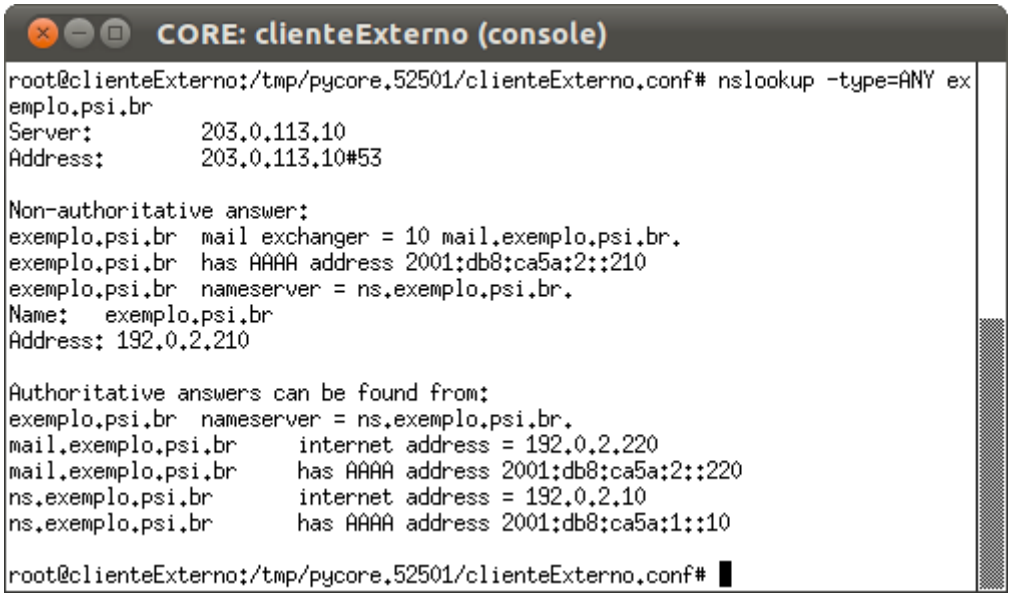


Ademas de la información obtenida en el punto 5, también tenemos ahora una dirección IPv6 asociada al nombre de dominio www.example.com.

h. Repita los chequeos para las otras direcciones y compare los resultados. Utilice por ejemplo el comando el comando nslookup para obtener una respuesta mas comleta digitando lo siguiente:

```
# nslookup -type=ANY example.com
```

El resultado debe ser:



7. Para finalizar el ejercici, configure el Servidor Autoritativo para responder a las consultas de direccionamiento reverso IPv6.

   a. Para esto, acceda a la máquina 'servidorDNSautoritativo' (doble click sobre el icono) y cree el archivo 2001-db8-ca5a.db dentro del diretorio /etc/named/, digitando el siguiente comando:

      ```
      # nano /etc/named/2001-db8-ca5a.db
      ```

      Agregue las líneas siguientes al archivo 2001-db8-ca5a.db:

      ```
      $TTL 86400
      a.5.a.c.8.b.d.0.1.0.0.2.ip6.arpa.    IN   SOA   ns.exemplo.psi.br. \
      root.example.com. (
                           15 ; serial
                           28800 ; refresh
                           7200 ; retry
                           604800 ; expire
                           86400 ; ttl
                           )

      ;; Servidor DNS que responde por esta zona revera
                            IN   NS   ns.exemplo.psi.br.

      ;; Direcciones reversas
      $ORIGIN      a.5.a.c.8.b.d.0.1.0.0.2.ip6.arpa.
      0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0  IN  PTR  ns.example.com.
      0.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0  IN  PTR  www.example.com.
      0.2.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0  IN  PTR  mail.example.com.
      ```

      Pulse Ctrl+X para salir de nano y luego 'Y' para confirmar la modificación del archivo.

En caso que este utilizando la maquina virtual provista por LACNIC, el contenido de este archivo puede ser visto en:

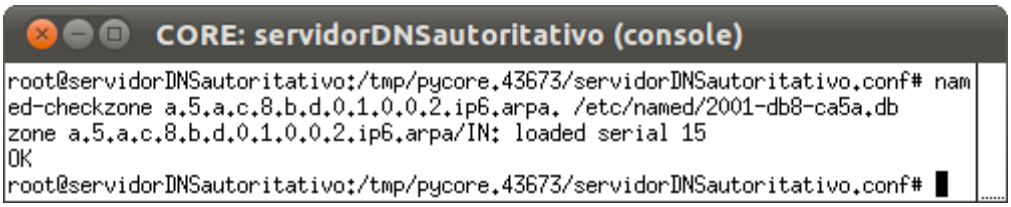
/home/core/Desktop/servicios/DNS/2001-db8-ca5a.db.

Este archivo presenta los registros y directivas relacionadas con la zona de direccionamiento reversa IPv6. Este posee las mismas funcionalidades y características del archivo 192-0-2.db analizado en el ítem 4c.

b. Para verificar si no existen errores en el archivo de zona generado, digite el siguiente comando en una Terminal de 'servidorDNSautoritativo':

```
# named-checkzone a.5.a.c.8.b.d.0.1.0.0.2.ip6.arpa \
                  /etc/named/2001-db8-ca5a.db
```

El resultado debe ser:



c. Ahora, registre esa zona en el archivo named.conf localizado en el directorio /etc/named/. Para eso dgite el siguiente comando en una terminal de la maquina 'servidorDNSautoritativo':

```
# nano /etc/named/named.conf
```

d. Agregue al final del archivo las siguientes lineas:

```
zone "a.5.a.c.8.b.d.0.1.0.0.2.ip6.arpa" {
  type master;
  file "2001-db8-ca5a.db";
};
```

Pulse Ctrl+X para salir del 'nano' y luego 'Y' para confirmar la modificación del archivo.

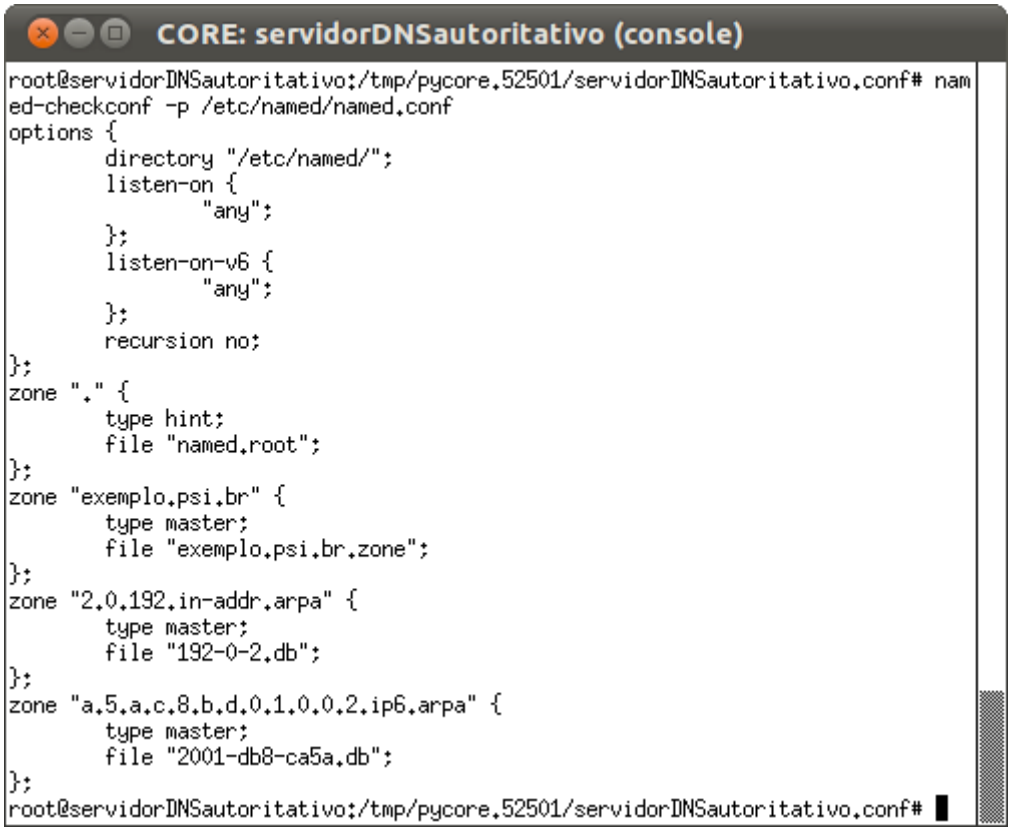
En caso que estén utilizando la maquina virtual provista por LACNIC pueden ver el contenido de este archivo en :

/home/core/Desktop/servicios/DNS/named.conf2.

e. Antes de reiniciar el proceso BIND, verifique si el archivo "named.conf" fue generado correctamente. Esto puede ser realizado con el siguiente comando:

```
# named-checkconf -p /etc/named/named.conf
```

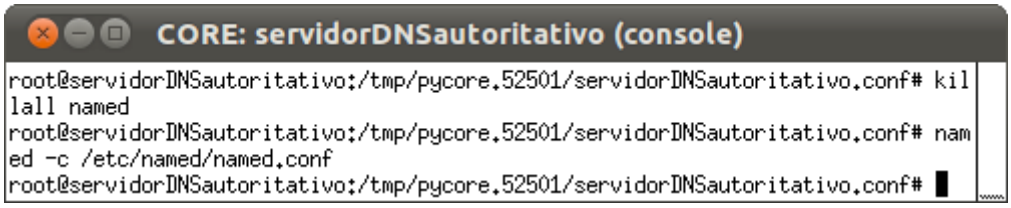
El resultado debe ser:



f. Caso que los pasos anteriores no hayan presentado errores de ejecución, reinicie el proceso BIND para que las alteraciones sean aplicadas. Para eso digite los siguientes comandos:

```
# killall named
# named -c /etc/named/named.conf
```

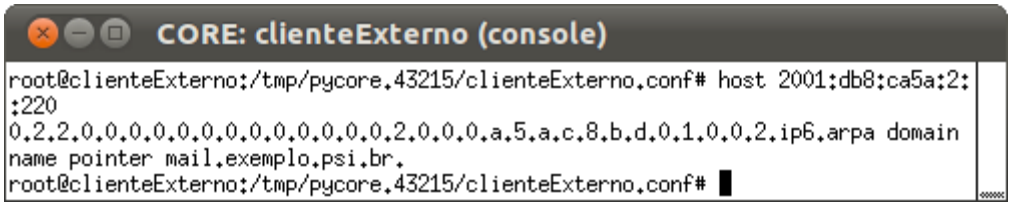
El resultado debe ser:



g. Para verificar si los cambios fueron realizados correctamente, acceda a la maquina virtual 'clienteExterno' (doble click sobre el icono) y realice algunas consultas DNS. Oara eso, utilice el comando host digitando lo siguiente:

```
# host 2001:db8:ca5a:2::220
```

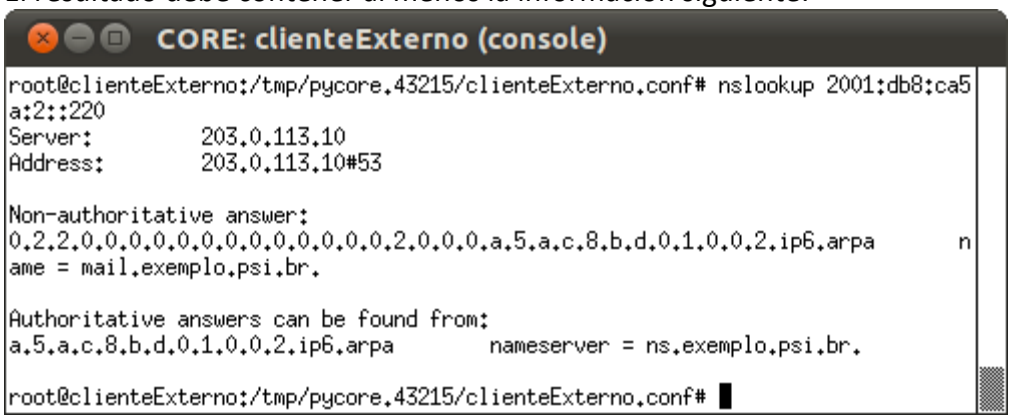
El resultado debe ser:



h. Repita estos chequeos para otras direcciones y compare los resultados. Utilice, por ejemplo, el comando nslookup para obtener una respuesta mas completa digitando lo siguiente:

```
# nslookup 2001:db8:ca5a:2::220
```

El resultado debe contener al menos la información siguiente:



9. Para terminar, es posible realizar un serie de chequeos de conectividad por el nombre de una maquina. Algunas opciones puede ser realizadas con la utilizacon del comando ping o *ping6*, *traceroute* o *traceroute6* y *mtr*. Algunos ejemplos son:

```
# ping www.example.com
# ping6 www.example.com
# mtr example.com
# traceroute6 mail.example.com
```

9. Detenga la simulación del CORE :

c. Pulse el botón  o;
d. Utilice el menú Experiment > Stop.