IPv6 – DHCPv6

Experimento: DHCPv6 Full - Solicit, Advertise, Request & Reply

Objetivo

Este experimento tiene como objetivo presentar el funcionamiento de DHCPv6 *stateful*, o sea el envío de datos de configuración opcionales, DNS, y dirección IPv6.

Para la realización de este ejercicio será utilizada la topología descripta en el archivo: **DHCPv6-E1.imn**.

Introducción Teórica

Dynamic Host Configuration Protocol (DHCP) es un protocolo de autoconfiguración stateful, utilizado para distribuir direcciones IP e información de red en forma dinámica. A pesar de esto las implementaciones IPv6 tienen significativas diferencias y particularidades con relación a su funcionamiento con IPv4, lo que hace de estas implementaciones incompatibles entre si. En esta experiencia solamente será observado DHCPv6 operando como un servicio stateful.

La arquitectura cliente-servidor es utilizada como base del funcionamiento de ese protocolo. En cada red debe haber un servidor capaz de decidir sobre la configuración de cada una de las interfaces de red presentes. En la práctica, entre el servidor DHCP y las maquinas cliente, se realiza un intercambio de 4 tipos de mensajes:

- **Solicit** es un mensaje enviado por el cliente, con dirección *Multicast Agent DHCP* (**FF02::1:2**), hacia la red y con intención de encontrar un servidor DHCP;
- **Advertise** es un mensaje enviado por el servidor DHCP, directamente a la dirección link-local del cliente, para indicar que él puede ofrecer la información de configuración necesaria;
- **Request** es un mensaje enviado por el cliente directamente al servidor DHCP para solicitar los datos de configuración;
- **Reply** es un mensaje enviado por el servidor DHCP a la dirección link-local del cliente como respuesta al mensaje de *Request*.

Existe un tipo de configuración para el cliente, llamada *rapid commit*, que permite el intercambio de información con apenas dos mensajes. Este tipo de configuración solamente es aconsejado cuando la red dispone solamente de un server o cuando existe una gran cantidad de direcciones a ser resueltas.

En caso de que existan routers en la red, ocurren algunas particularidades del mecanismo DHCPv6, por ejemplo el envío, a partir de routers, de información acerca de las características del servicio a través del envio de mensajes del tipo *Router Advertisement*. En ellas son activados dos flags: *AdvManagedFlag*, que define la autorización de recepción de direcciones

IPv6, por medio del server DHCPv6, y el flag *AdvOtherConfigFlag*, que habilita la recepción de otras configuraciones provenientes del servidor DHCPv6.

Hay dos formas de eliminar la influencia de los routers en la operación del DHCP, una realizada en el lado del cliente y otra en el Router mismo. En el lado del cliente, es preciso seleccionar la opción de no aceptar mensajes del tipo *Router Advertisement* y del lado del Router es necesario configurarlo para que no envíe mensajes *Router Advertisement*.

La otra particularidad, que ocurre en presencia de los routers de la red, ocurre en el caso de que se encuentre ubicado un Router entre el cliente y el server. En ella el Router también es responsable de traducir los mensajes *multicast* enviados por el cliente para encontrar el servidor DHCP.

Descripción del Experimento

1. En caso de que no este utilizando la máquina provista por LACNIC es preciso, antes de comenzar con la experiencia, instalar alguno software necesario (caso contrario vaya directamente al paso 2). Siga las siguientes instrucciones para realizar las instalaciones necesarias:

    - Para realizar algunas verificaciones durante el experimento será necesaria la instalación del programa **Wireshark** que facilita la visualización de paquetes en la red. En la máquina virtual, utilice una Terminal para ejecutar el comando:

      ```
      $ sudo apt-get install wireshark
      ```

      Antes de la instalación le será solicitada la contraseña del usuario *core*. Digite "core" para continuar con la instalación.

    - El **dhcpd**, que el servicio responsable por las tareas de servidor do DHCP. Para instalarlo descargue la ultima versión (4.2.4-P1 a Agosto/2012) desde http://www.isc.org/software/dhcp y utilice los siguientes comandos en una Terminal:

      ```
      $ cd <lugar_donde_descargo_el_archivo>
      $ tar xf dhcp-4.2.4-P1.tar.gz
      $ cd dhcp-4.2.4-P1/
      $ ./configure
      $ make
      $ sudo make install
      ```

    ***Obs**: Recuerde utilizar los números de versión correctos para extraer el paquete y acceder a la carpeta de instalación. Luego del comando 'sudo' le será solicitada una contraseña de usuario, digite "*core*" para continuar con la instalación.

El cliente **dibbler-client**, que realiza las funciones de cliente DHCP. Para instalarlo, descargue la ultima versión (0.8.3RC1 a Agosto/2012) del código fuente desde el sitio http://klub.com.pl/dhcpv6/ y utilice los siguientes comandos en una Terminal:

```
$ cd <lugar_donde_descargo_el_archivo>
$ tar xf dibbler-0.8.3RC1.tar.gz
$ cd dibbler-0.8.3RC1/
$ ./configure
$ make
$ sudo make install
```

***Obs**: Recuerde utilizar los números de versión correctos para extraer el paquete y acceder a la carpeta de instalación. Luego del comando 'sudo' le será solicitada una contraseña de usuario, digite "*core*" para continuar con la instalación.

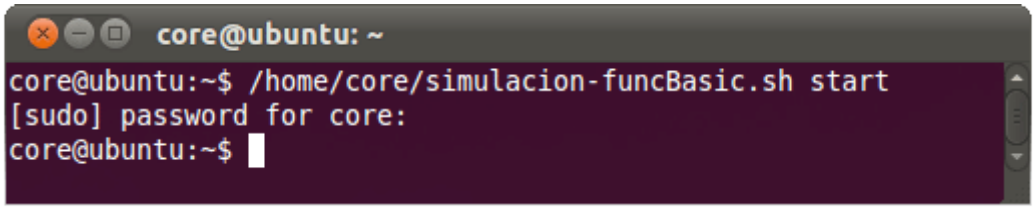
2. Inicie la configuración de la simulación:

En una terminal de la máquina virtual digite el siguiente comando:

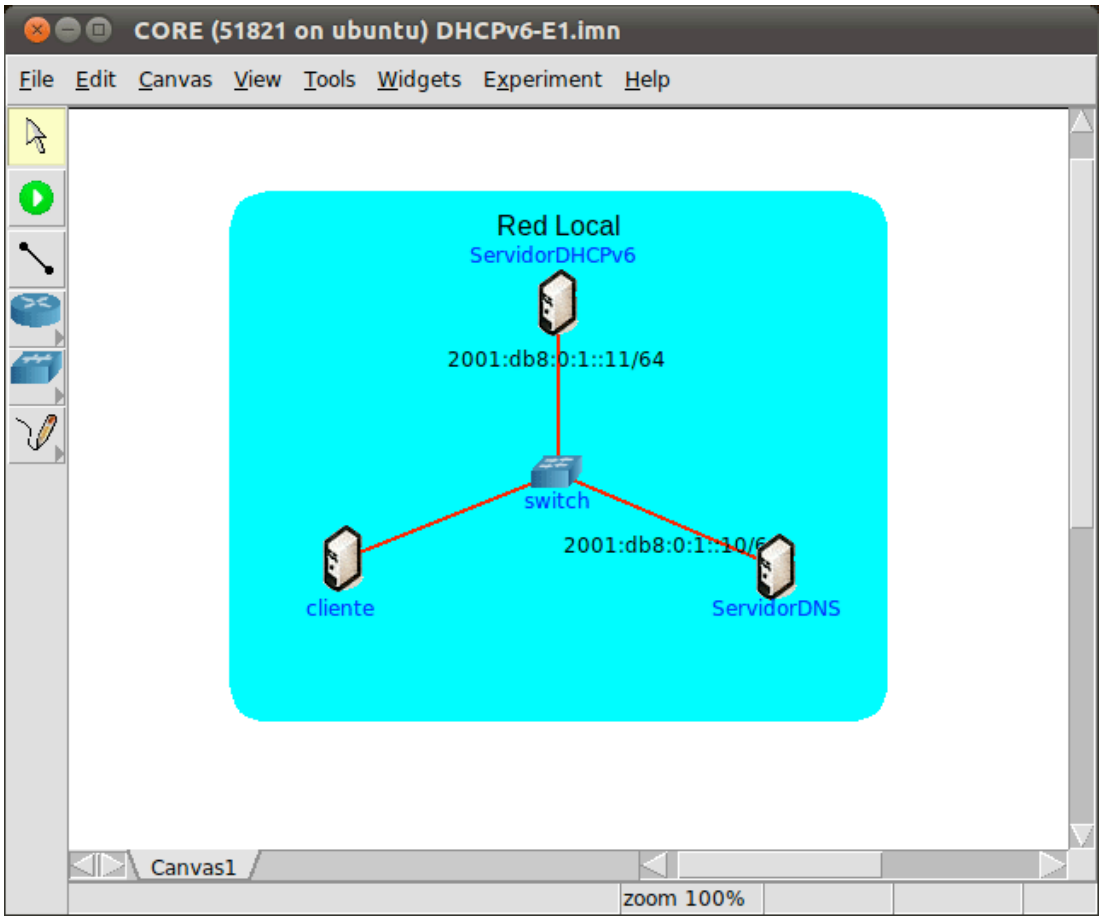
```
$ /home/core/simulacion-funcBasic.sh start
```

En caso que sea necesario, digite "core" para continuar con la configuración.

El resultado debe ser:



3. Inicie CORE y abra el archivo "**DHCPv6-E1.imn**" localizado en el directorio Desktop "Funcionalidades/DHCPv6", de la maquina de LACNIC. La siguiente topología debe aparecer:

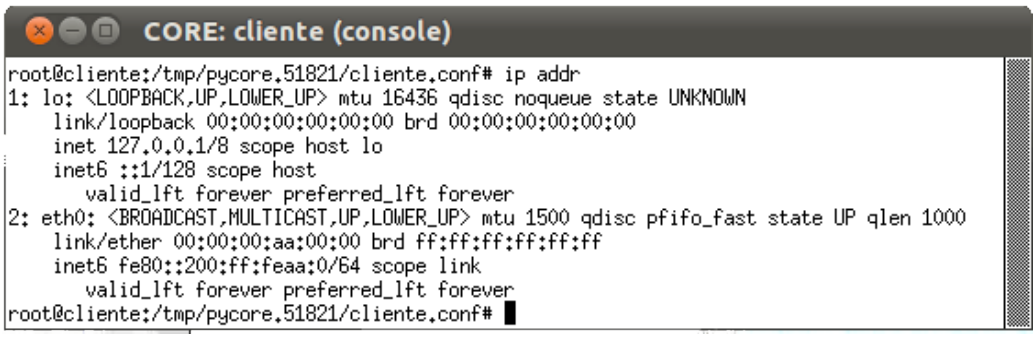


4. Verifique la configuración de los nodos de la topología.
   - Inicie la simulación realizando uno de los siguientes pasos:
     - Pulse el botón  ; o
     - Utilice el menú Experiment > Start.

   - Espere hasta que CORE termine de iniciar la simulación y abra una Terminal de la maquina cliente, con un doble-click sobre ella.
   - Observe la configuración de red de cliente a través del siguiente comando:

     ```
     # ip addr
     ```

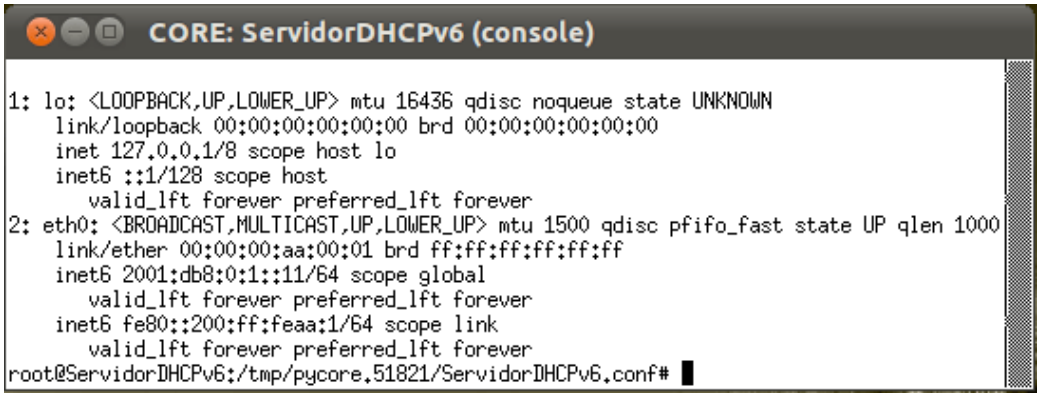
El resultado debe ser:



***Obs**: Con este comando es posible observar las direcciones de las interfaces.

- Observe la configuración del servidorDHCPv6 con el mismo comando.

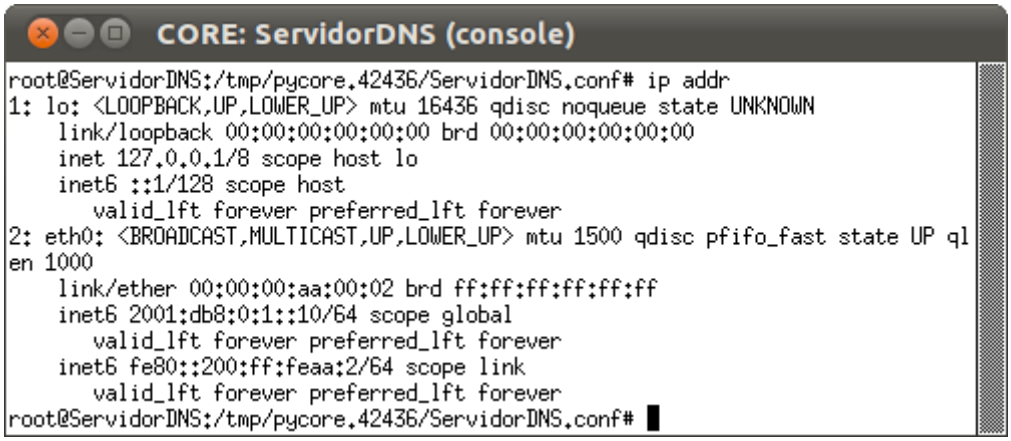
El resultado debe ser:



***Obs**: Con este comando es posible observar las direcciones de las interfaces.

- Observe la configuración de ServidorDNS con el mismo comando

El resultado debe ser:



***Obs**: Con este comando es posible observar las direcciones de las interfaces.

5. Inicie el servicio DNS en el ServidorDNS.

   - Abra una terminal en ServidorDNS con un doble-click
   - Utilice el siguiente comando para iniciar el servicio DNS:

     ```
     # dnsmasq -i eth0
     ```

     El resultado debe ser:

6. Configure el dhcp en el Servidor para enviar las configuraciones al cliente.
   - Abra una terminal en el ServidorDHCPv6;
   - Cree dos archivos nuevos con los siguientes nombres: *dhcpd.conf* y *dhcp.leases*. Para realizar esto digite los comandos:

     ```
     # touch dhcpd.conf
     # touch dhcpd.leases
     ```

     El resultado debe ser:

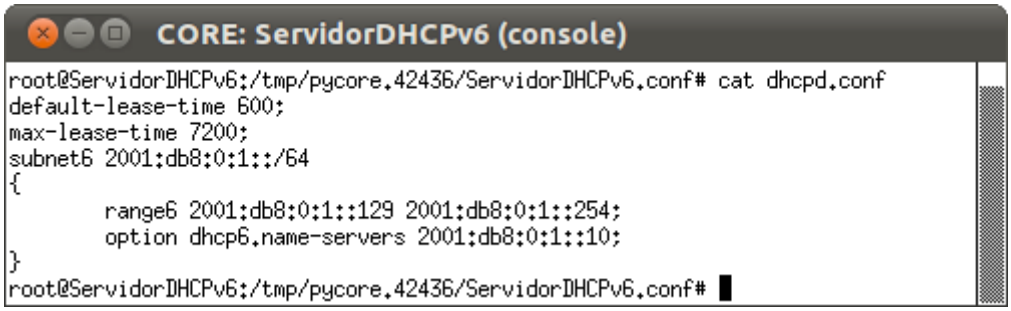
     

   - Edite el archivo dhcpd.conf, deberá contener las lineas:

     ```
     default-lease-time 600;
     max-lease-time 7200;
     subnet6 2001:db8:0:1::/64
     {
           range6 2001:db8:0:1::129 2001:db8:0:1::254;
           option dhcp6.name-servers 2001:db8:0:1::10;
     }
     ```

     ***Obs**: El campo name-servers contiene la dirección de la maquina que funcionara como servidor DNS y el campo range6 contiene el rango de direcciones dentro del prefijo de subred configurado que serán distribuidas entre los dispositivos clientes.

El resultado debe ser:



***Obs**: un editor de texto en la máquina virtual que puede ser utilizado es el **nano**.

Para utilizarlo digite en una terminal:

```
# nano dhcpd.conf
```

En el nano, la secuencia utilizada para salvar el archivo es CTRL-O y para salir es CTRL-X.

- Inicie el programa de dhcp a través del comando:

```
# dhcpd -6 -cf dhcpd.conf -lf dhcpd.leases
```

El resultado debe ser:

7. Configure dibbler-client en el cliente para recibir las configuraciones desde el servidor.
   - Abra una terminal en la maquina cliente.
   - Dentro de la carpeta '*/etc/dibbler*', cree un archivo nuevo llamado *client.conf* con el comando:

```
# touch /etc/dibbler/client.conf
```

El resultado debe ser:

- Incluya en ese archivo el texto:

```
iface eth0 {
      ia
      option dns-server
}
```

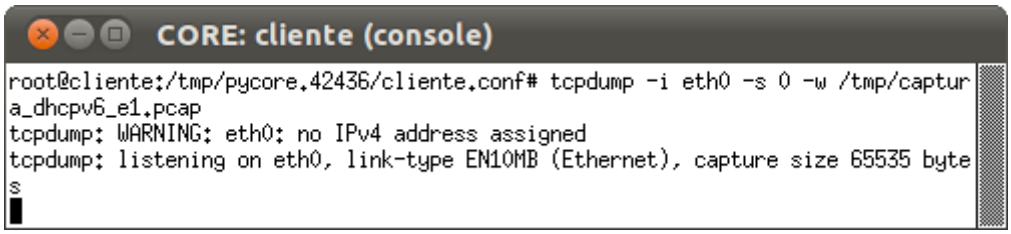
El resultado debe ser:

***Obs**: Para esta simulación, la carpeta de configuraciones de *dibbler* fue virtualizada para la maquina cliente, sino normalmente este programa es instalado con una configuración por defecto localizada en '*/etc/dibbler/client.conf*'.

8. Efectúe el intercambio de mensajes DHCP con el ServidorDHCP.
   - Abra un terminal de cliente;
   - Utilice el siguiente comando para comenzar la captura de paquetes en su interface:

```
# tcpdump -i eth0 -s 0 -w /tmp/captura_dhcpv6_e1.pcap
```

El resultado debe ser:



***Obs**: No cierre esta terminal hasta el final del experimento, una vez que haga eso terminara la ejecución del comando "tcpdump" y con ello la captura de paquetes.

   - Abra otro terminal en la máquina cliente;
   - Inicie el programa dibbler-client:

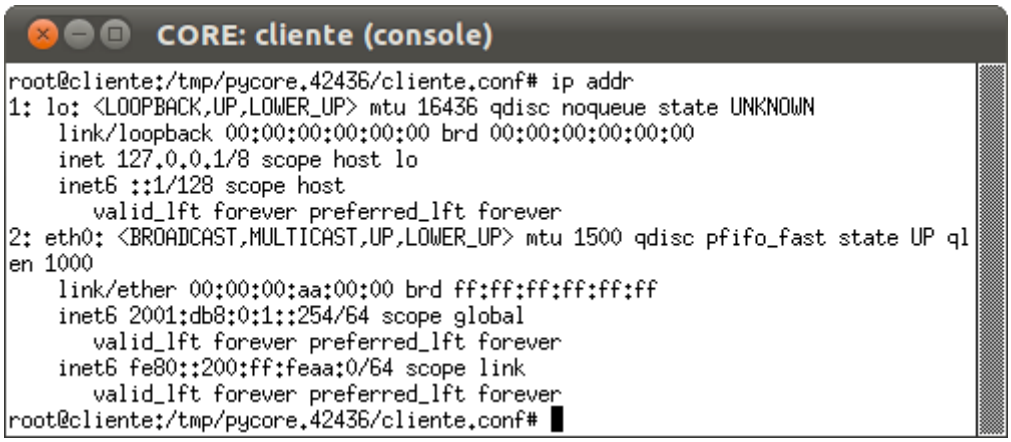
```
# dibbler-client start
```

El resultado debe ser:

- Espere algunos segundos y utilice el siguiente comando para verificar que la dirección IPv6 de alcance global fue obtenida en el cliente:

```
# ip addr
```

El resultado debe ser:



***Obs**: Note la dirección ipv6 adquirida vía DHCPv6.

- Para visualizar el dns obtenido vía dhcp, digite el comando:

```
# cat /etc/resolv.conf
```

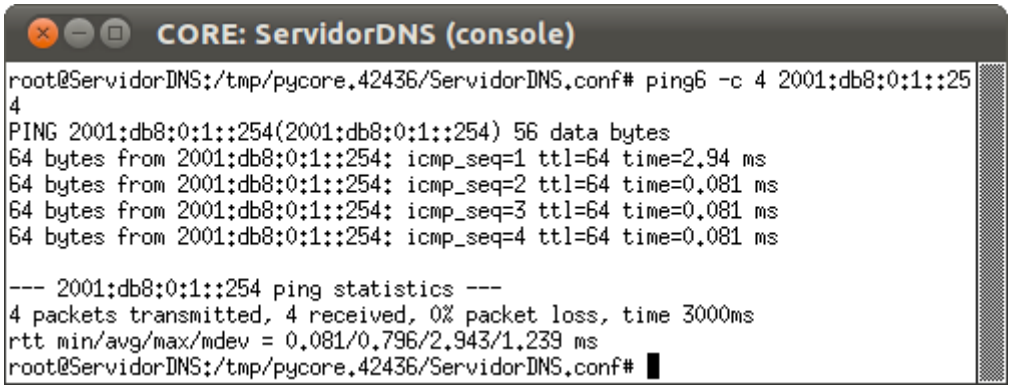
El resultado debe ser:

***Obs**: Observe la dirección IPv6 del DNS recibida vía DHCPv6.

9. Revise la conectividad IPv6 entre los nodos de la red:
    - En una Terminal de ServidorDNS, utilice el siguiente comando :

```
# ping6 -c 4 2001:db8:0:1::254
```

El resultado debe ser:

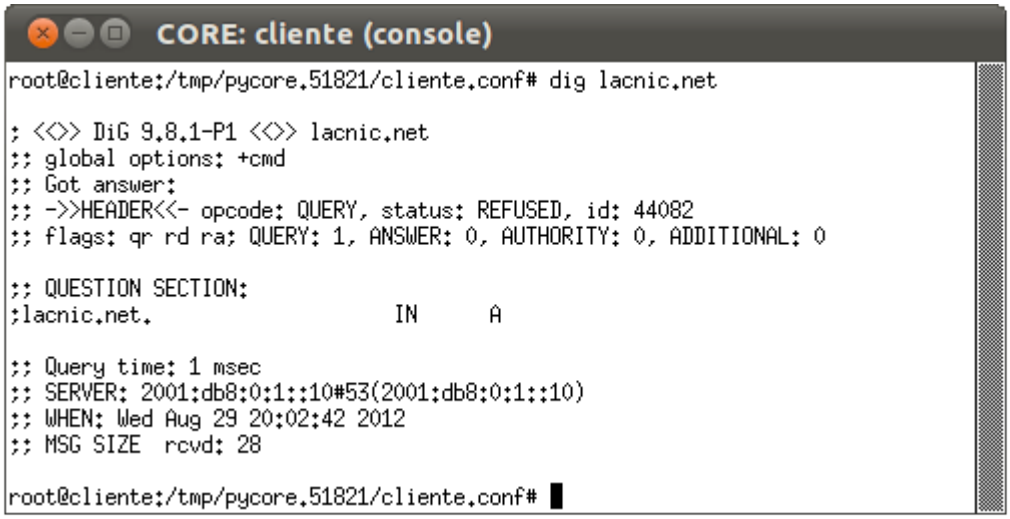


***Obs**: La dirección IPv6 debe ser la misma que obtuvo vía DHCPv6 en el paso 8

- En la Terminal del cliente revise el servicio DNS con el comando:

```
# dig lacnic.net
```

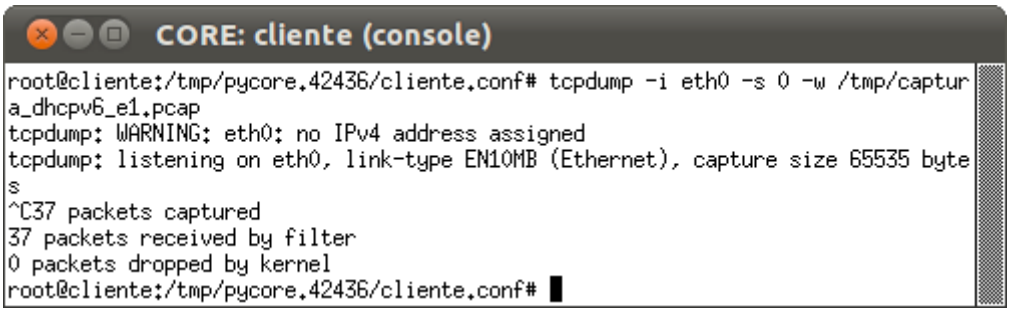
El resultado debe ser:



***Obs**: Observe que el servidor DNS responde a la solicitud del cliente.

- En la terminal del cliente, cierre la captura de paquetes a través de la secuencia Ctrl+C.

El resultado debe ser:



***Obs**: La cantidad de paquetes puede variar de acuerdo con el tiempo esperado hasta ejecutar el comando Ctrl+C.

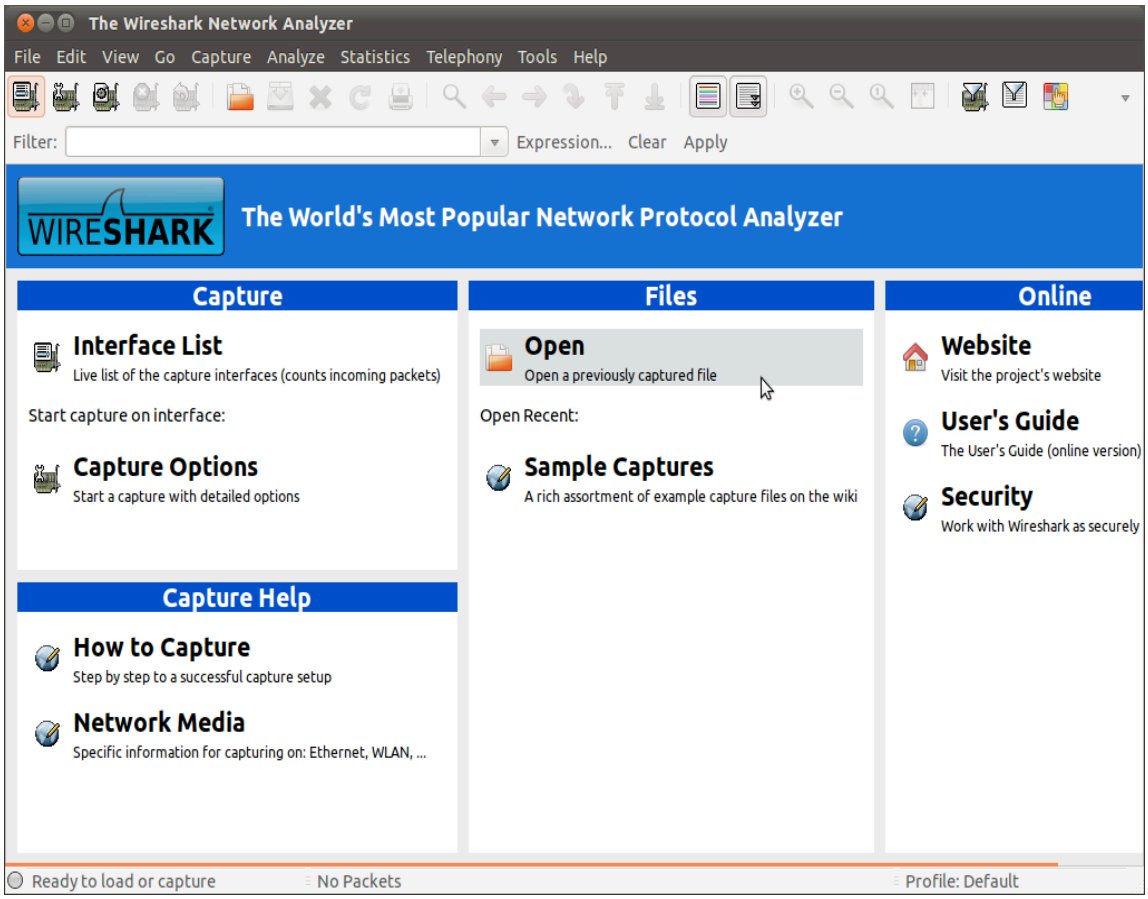
10. Cierre la simulación con una de las siguientes acciones:

    - Puse el botón  ; o
    - Utilice el menú Experiment > Stop.

11. La verificación de los paquetes capturados será realizada a través del programa **Wireshark**. Para iniciarlo ejecute el siguiente comando en una terminal de la maquina virtual:

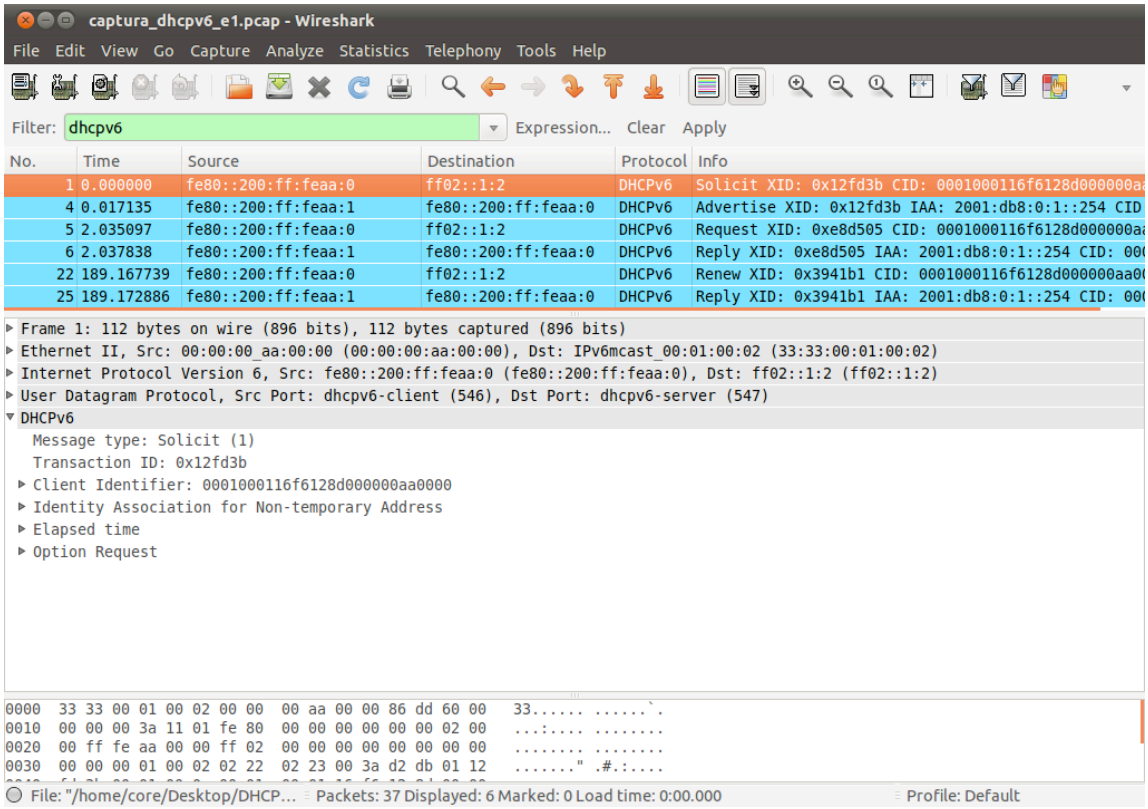
```
$ wireshark
```

    Si esta utilizando la máquina virtual provista por LACNIC puede iniciar esta aplicación haciendo doble-click sobre el icono correspondiente ubicado en el Escritorio.



- Abra el archivo **/tmp/captura_dhcpv6_e1.pcap** con el menú File>Open;
- Vea los paquetes *Solicit*, *Advertise*, *Request* y *Reply*. Analícelos y observe los datos contenidos en los mismos.

Solicit:



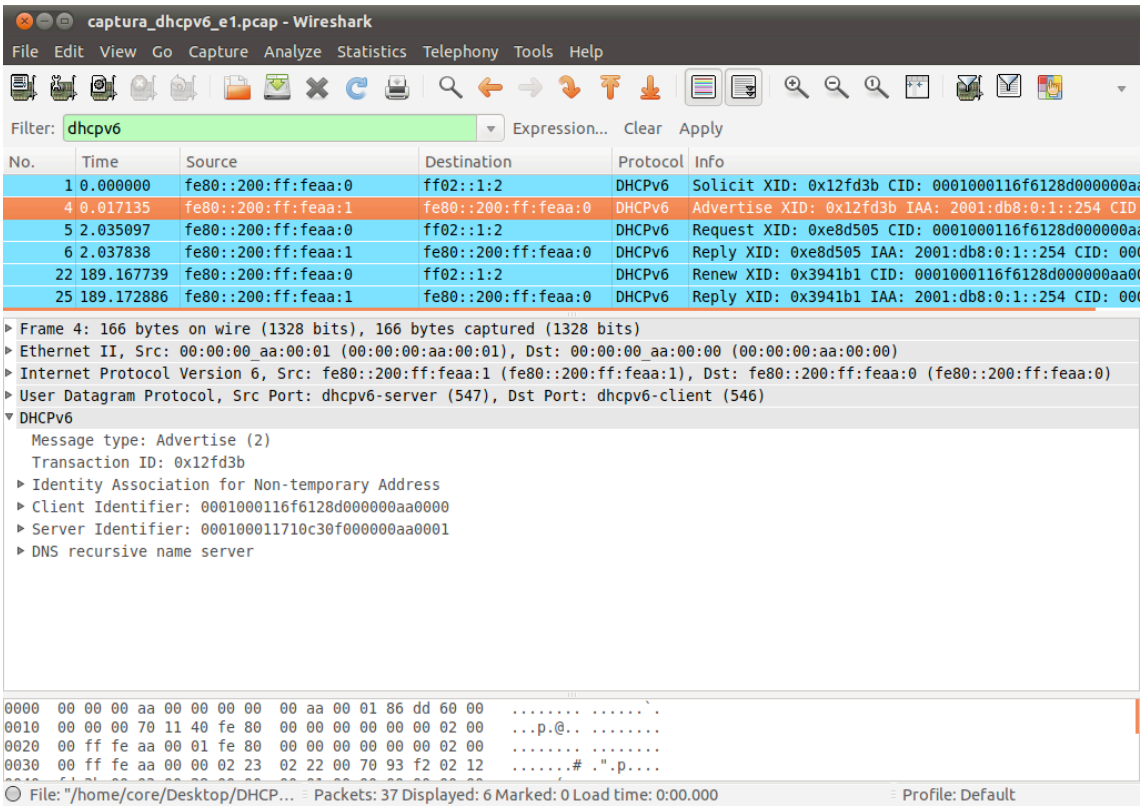
***Obs**: el filtro dhcpv6 puede ser usado para ayudar a filtrar los mensajes.

Campos importantes:

- **Destination (Ethernet)**: el destino es la dirección (33:33:00:01:00:02) siendo que el prefijo 33:33 indica que el mensaje es un multicast en la capa Ethernet y el sufijo 00:01:00:02 indica los últimos 32 bits de la dirección multicast IPv6 del mensaje.
- **Source (Ethernet)**: el origen es la dirección MAC de la interface de la maquina que envía la solicitud (00:00:00:aa:00:00).
- **Type (Ethernet)**: indica que el mensaje utiliza el protocolo IPv6 (x86dd).
- **Next Header (IPv6)**: indica cual es el próximo cabezal, en este caso, el valor 0x11 se refiere a un mensaje UDP.
- **Source (IPv6)**: el origen es la dirección IP del link-local de la interface directamente conectada al enlace al que se realizó la solicitud (fe80::200:ff:feaa:0).
- **Destination (IPv6)**: el destino es la dirección *Multicast Agent DHCP* (FF02::1:2).
- **Source port (UDP)**: indica el puerto donde se encuentra el servicio dhcpv6-client cuyo valor es 546.
- **Destination port (UDP)**: indica el puerto donde se encuentra el servicio dhcpv6-server en el servidor. Su valor es 547.
- **Message type (DHCPv6)**: indica a través del valor 1 que el tipo de mensaje es *Solicit*;

- **Client Identifier (DHCPv6)**: contiene datos de la identificación única del cliente basada en la dirección física.
- **Identity Association for Non-temporary Address (DHCPv6)**: sirve para solicitar la dirección IPv6 al servidor.
- **Option Request (DHCPv6)**: Requested Option Code: indica la información que el dispositivo está solicitando al servidor DHCP, en este caso, *DNS Recursive Name Server* con el valor 23;

Advertise:



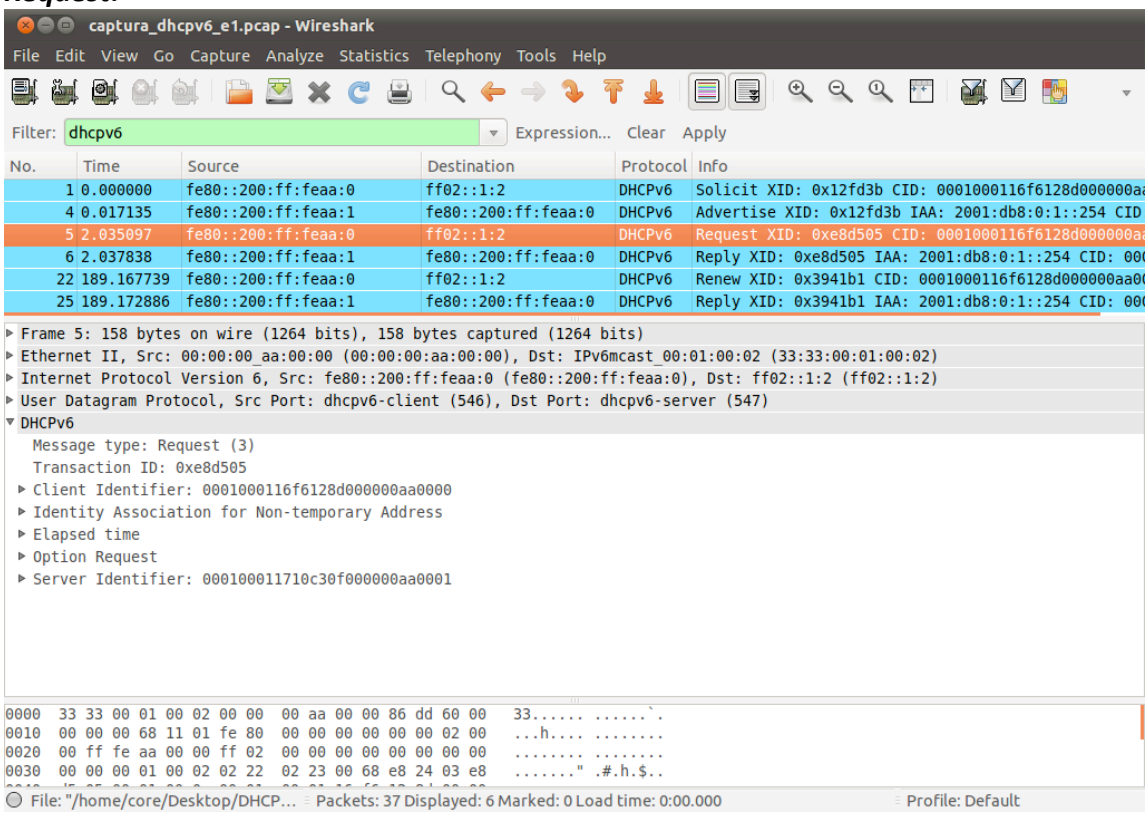
***Obs**: el filtro dhcpv6 puede ser usado para ayudar a filtrar los mensajes.

Campos importantes:

- **Destination (Ethernet)**: el destino es la dirección MAC de la interface de la maquina solicitante (00:00:00:aa:00:00).
- **Source (Ethernet)**: el origen es la dirección MAC de la interface de máquina que envió la respuesta (00:00:00:aa:00:01).
- **Type (Ethernet)**: indica que el mensaje utiliza el protocolo IPv6 (x86dd).
- **Next Header (IPv6)**: indica cual es el próximo cabezal, en este caso, el valor 0x11 se refiere a un mensaje UDP.
- **Source (IPv6)**: el origen es la dirección IP de link-local de la interface del dispositivo que envió el mensaje, o sea, del servidor DHCP6 (fe80::200:ff:feaa:1).
- **Destination (IPv6)**: el destino es la dirección unicast del link-local de la maquina solicitante (fe80::200:ff:feaa:0).

- **Source port (UDP)**: indica el puerto donde se encuentra el servicio dhcpv6-server cuyo valor es 547.
- **Destination port (UDP)**: indica el puerto donde se encuentra el servicio dhcpv6-client cuyo valor es 546.
- **Message type (DHCPv6)**: indica a través del valor 2 que el tipo de mensaje es *Advertise*;
- **Identity Association for non-temporary address (DHCPv6)**: sirve para cargar la dirección IPv6 para el cliente.
    - IA Address: contiene la dirección y las características que el cliente debe utilizar (2001:db8:0:1::254).
- **Client Identifier (DHCPv6)**: contiene datos de la identificación única del cliente basada en su dirección física.
- **Server Identifier (DHCPv6)**: contiene datos de identificación del servidor basada en su dirección física.
- **DNS recursive name server (DHCPv6)**: DNS servers address: indica la dirección ipv6 del servidor DNS solicitado: (2001:db8:0:1::10);

Request:

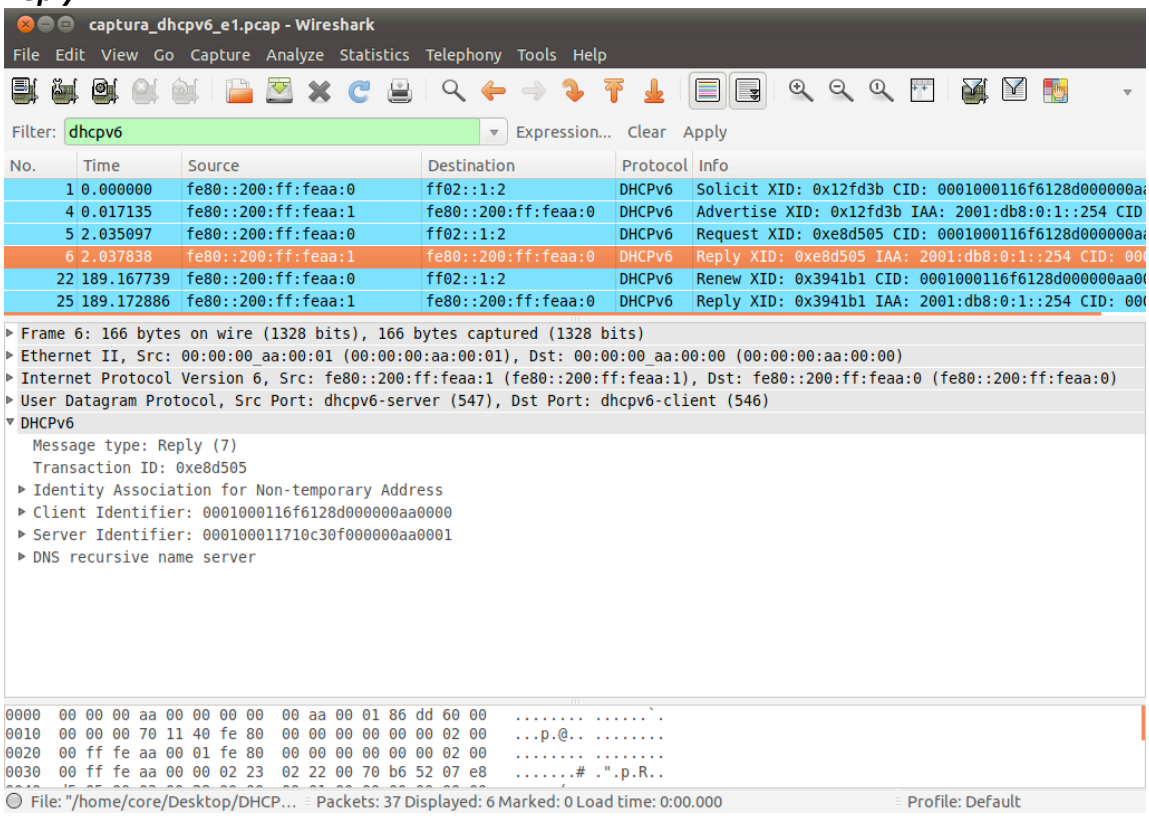


***Obs**: el filtro dhcpv6 puede ser usado para ayudar a filtrar los mensajes.

Campos importantes:

- **Destination (Ethernet)**: el destino es la dirección (33:33:00:01:00:02) siendo que el prefijo 33:33 indica que el mensaje es un multicast de capa Ethernet y el sufijo 00:01:00:02 indica los últimos 32 bits de la dirección multicast IPv6 del mensaje.
- **Source (Ethernet)**: el origen es la dirección MAC de la interface de la maquina del cliente (00:00:00:aa:00:00).
- **Type (Ethernet)**: indica que el mensaje utiliza el protocolo IPv6 (x86dd).
- **Next Header (IPv6)**: indica cual es el próximo cabezal, en este caso, el valor 0x11 se refiere a un mensaje UDP.
- **Source (IPv6)**: el origen es la dirección IP link-local de la interface del dispositivo que envió el mensaje, o sea del cliente (fe80::200:ff:feaa:0).
- **Destination (IPv6)**: el destino es la dirección *Multicast Agent DHCP* (**FF02::1:2**).
- **Source port (UDP)**: indica el puerto donde se encuentra el servicio *dhcpv6-client* cuyo valor es 546.
- **Destination port (UDP)**: indica el puerto donde se encuentra el servicio *dhcpv6-server* cuyo valor es 547.
- **Message type (DHCPv6)**: indica a través del valor 3 que el tipo de mensaje es un *Request*;
- **Client Identifier (DHCPv6)**: contiene datos de la identificación única del cliente basada en su dirección física
- **Identity Association for non-temporary address (DHCPv6)**: sirve para confirmar la dirección IPv6 recibida.
    - IA Address: contiene la dirección y las características que el cliente ira a utilizar (2001:db8:0:1::254).
- **Option Request (DHCPv6)**:
    - Requested Option Code: indica que información esta siendo solicitada al servidor DHCP. En este caso, *DNS recursive name server* con el valor 23;
- **Server Identifier (DHCPv6)**: contiene datos de identificación única del servidor basada en su dirección física.

Reply:



***Obs**: el filtro dhcpv6 puede ser usado para ayudar a filtrar los mensajes.

Campos importantes:

- **Destination (Ethernet)**: el destino es la dirección MAC de la interface de la maquina del cliente (00:00:00:aa:00:00).
- **Source (Ethernet)**: el origen es la dirección MAC de la maquina que esta enviando la respuesta (00:00:00:aa:00:01).
- **Type (Ethernet)**: indica que el mensaje utiliza el protocolo IPv6 (x86dd).
- **Next Header (IPv6)**: indica cual es el próximo cabezal, en este caso, el valor 0x11 se refiere a un mensaje UDP.
- **Source (IPv6)**: el origen es una dirección IP link-local de la interface del dispositivo que envió el mensaje, o sea, del servidor DHCPv6 (fe80::200:ff:feaa:1).
- **Destination (IPv6)**: el destino es la dirección IPv6 unicast del link-local del cliente (fe80::200:ff:feaa:0).
- **Source port (UDP)**: indica el puerto donde se encuentra el servicio *dhcpv6-server* cuyo valor es 547.
- **Destination port (UDP)**: indica el puerto donde se encuentra el servicio dhcpv6-client cuyo valor es 546.
- **Message type (DHCPv6)**: indica a través el valor 7 que el tipo de mensaje es Reply;

- **Identity Association for non-temporary address (DHCPv6)**: sirve para confirmar la dirección IPv6 ofrecida.
    - IA Address: contiene la dirección y las características que el cliente va a utilizar (2001:db8:0:1::254).
- **Client Identifier (DHCPv6)**: contiene datos de identificación única del cliente basada en su dirección física.
- **Server Identifier (DHCPv6)**: contiene datos de identificación única del servidor basados en su dirección física.
- **DNS recursive name server (DHCPv6)**:
    - DNS servers address: indica la dirección IPv6 del servidor DNS solicitado (2001:db8:0:1::10);