Universidad Nacional Autónoma de México

Facultad de Ciencias

Redes de Computadoras

Práctica 4

Instalación y configuración de un servidor DNS

Profesor: Paulo Contreras Flores

Ayudante Lab: José Daniel Campuzano Barajas

Objetivo

• El alumno conocerá la forma en que se realiza la resolución de nombres de dominio usando DNS.

• Aprenderá a instalar y configurar un servidor DNS utilizando el software Bind

Introducción

DNS (Domain Name System) se usa principalmente para asociar los nombres de host con su dirección IP. Es un sistema esquema jerárquico de nombres basado en dominios, es un sistema de bases de datos distribuido.

El espacio de nombres de dominio es una jerarquía de nombres administrada por la ICANN(Internet Corporation for Assigned Name and Numbers). En la que cada dominio se divide en subdominios, los que a su vez se dividen, y así en lo sucesivo. Los dominios se pueden representar mediante un árbol, las hojas del árbol representan los dominios que no tienen subdominios, pero que contienen host. Un dominio u hoja puede contener un solo host, o puede representar a una compañía y contener miles de host, Figura 1.

Los dominios de nivel superior se dividen en dos categorías:

• Genéricos, datan de 1980, pero a lo largo del tiempo se han introducido nuevos.

• Países, los dominios de país incluyen una entrada para cada país, de acuerdo a la ISO 3166.

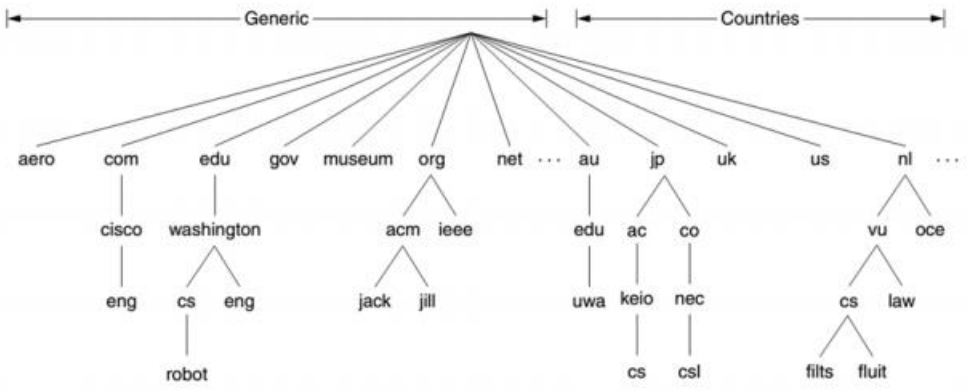


Figura 1. Espacio de nombres de dominio.

Los dominios de nivel superior son operados por registradores nombrados por la ICANN. Para solicitar un nombre de dominio de segundo nivel, se hace la solicitud al registrador correspondiente, si el registro está disponible y si la marca no está registrada se otorga el dominio y se paga una cuota. Cada dominio puede tener un grupo de registros de recursos asociados a él. Los registros son la base de datos del DNS. Para un host individual, el registro de recursos más común es la dirección IP. Por lo que la función principal del DNS es relacionar los nombres de dominio con los registros de recursos. Algunos de los registros son:

- A - Dirección IPv4 de un host.
- NS - Servidor de nombres.
- CNAME - Nombre canónico.
- MX - Intercambio de correo.

El espacio de nombres de DNS se divide en zonas, el lugar donde se colocan los limites dentro de una zona es responsabilidad del administrador de esa zona y cada zona se asocia con uno o más servidores de nombres. Una zona debe tener un DNS

primario, el cual obtiene su información de un archivo en su disco duro, y uno o más servidores secundarios, los cuales obtienen su información del DNS primario, Figura 2.

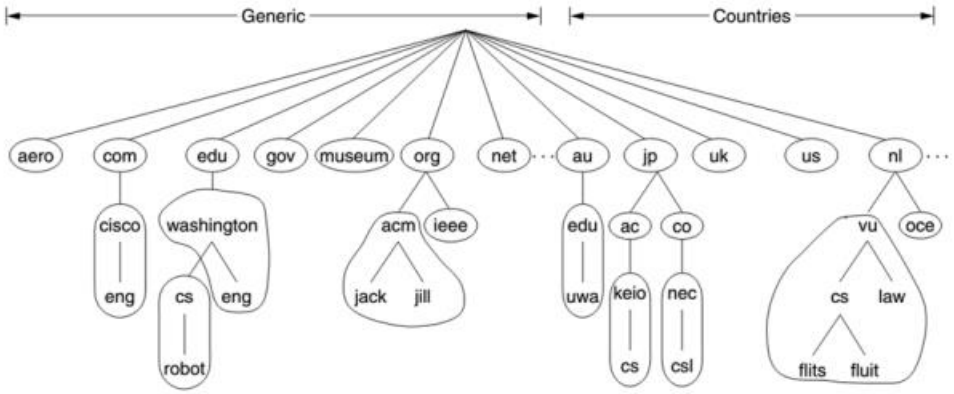


Figura 2. Espacio de DNS dividido en zonas.

Al proceso de buscar un nombre y encontrar una dirección se le conoce como resolución de nombres. Si un host hace una consulta, se la envía a uno de los servidores de nombres locales, si el dominio que se busca está bajo la jurisdicción del servidor de nombres, devuelve los registros de 2 recursos autorizados. Un registro autorizado es uno que proviene de la autoridad que administra ese registro, y siempre será correcto. También existen los registros en cache, almacenados en el DNS local, los cuales no siempre están actualizados. Si el dominio que se busca es remoto, si no hay información en la cache (en el DNS local) sobre el dominio buscado, el DNS local empezara una consulta remota.

En la Figura 3 de la diapositiva se muestra un ejemplo de una consulta remota del dominio robot.cs.washington.edu, y se asume el peor de los casos, es decir, que cada dispositivo no tiene registrada esta consulta en su memoria RAM (cache DNS) de alguna consulta realizada previamente.

Primero se realiza la consulta en el DNS Local (cs.vu.nl), esta consulta tiene el nombre del dominio buscado, el tipo A y la clase IN. El siguiente paso es empezar en la parte superior de la jerarquía de nombres y preguntar a cada uno de los servidores raíz. Estos servidores tienen información sobre cada dominio de nivel superior. Se le pregunta a uno de los servidores Root (a.root-servers.net), estos tienen solamente información de los dominios genéricos, para este caso tienen información sobre el servidor que contiene datos del dominio .edu, es decir información sobre el dominio del siguiente nivel. Después se le pregunta al servidor edu (a.edu-servers.net) sobre el dominio washington.edu, este servidor conoce que otro servidor contiene la información para este dominio. Así continua la búsqueda, cada servidor DNS de un nivel superior conoce al servidor DNS del siguiente nivel, la secuencia se repite hasta obtener el servidor DNS que conoce el registro buscado.

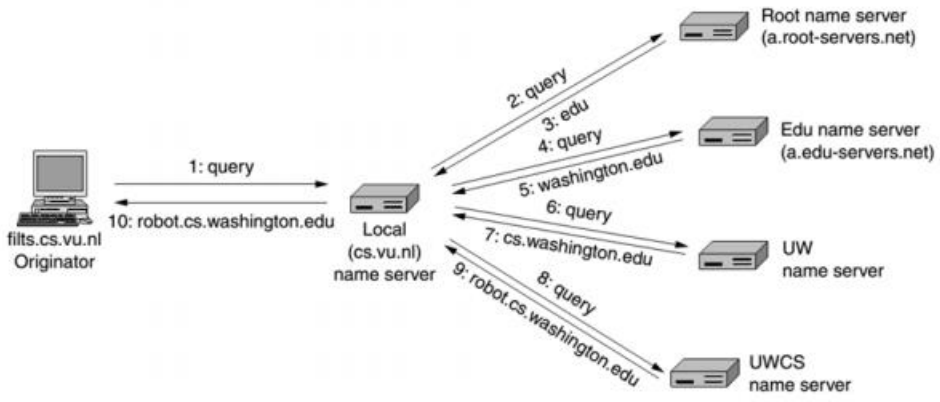


Figura 3. Consulta remota.

Existen 13 servidores raíz DNS, Figuras 4. Cada servidor raíz podría ser lógicamente una sola computadora. Sin embargo, como toda Internet depende de los servidores raíz, estos son computadoras de alto desempeño con un alto grado de replicación.

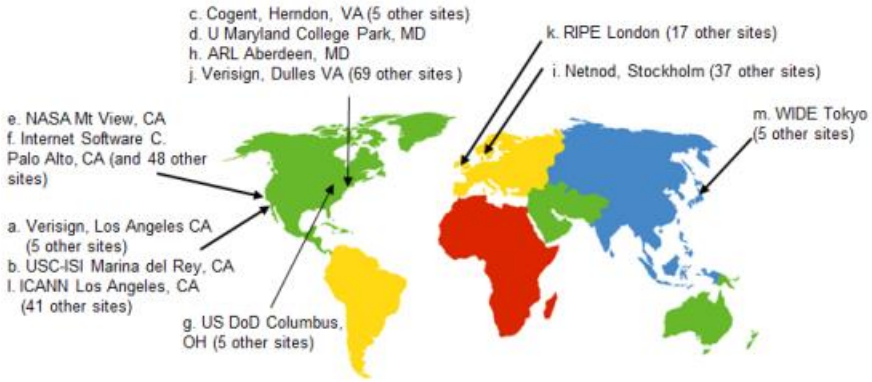


Figura 4. Servidores raíz.

Por ejemplo, es improbable que un servidor de nombres raíz conozca la dirección de un host en la UNAM, cuyo dominio es unam.mx, y tal vez tampoco conozca el servidor de nombres para la UNAM, pero debe conocer el servidor de nombres del dominio mx, este servidor que conoce el dominio mx debería de saber que servidor tiene la información del dominio unam.mx, es decir, cada servidor DNS de un nivel superior conoce al servidor DNS del siguiente nivel, la secuencia se repite hasta obtener el servidor DNS que conoce el registro buscado.

Desarrollo

Para esta práctica se utilizarán los servidores instalados en la Práctica 2 y Práctica 3. De manera general se requiere que un cliente de una red local (A) sea capaz de consultar el servidor web (B) de su misma red mediante un nombre de dominio. El cliente (A) primero realizará la consulta de nombre de dominio al servidor DNS (C) y después de obtener la dirección IP correspondiente al servidor web (B), dirigirá su petición a él para solicitar el formulario de inicio de sesión.

1. Configuración del entorno de virtualización

a. Agregar un nuevo adaptador de red virtual en el cual se conectarán todos los *equipos virtuales. Esto se logra desde el menú Edit -> Virtual Network Editor ... -> Add Network...*

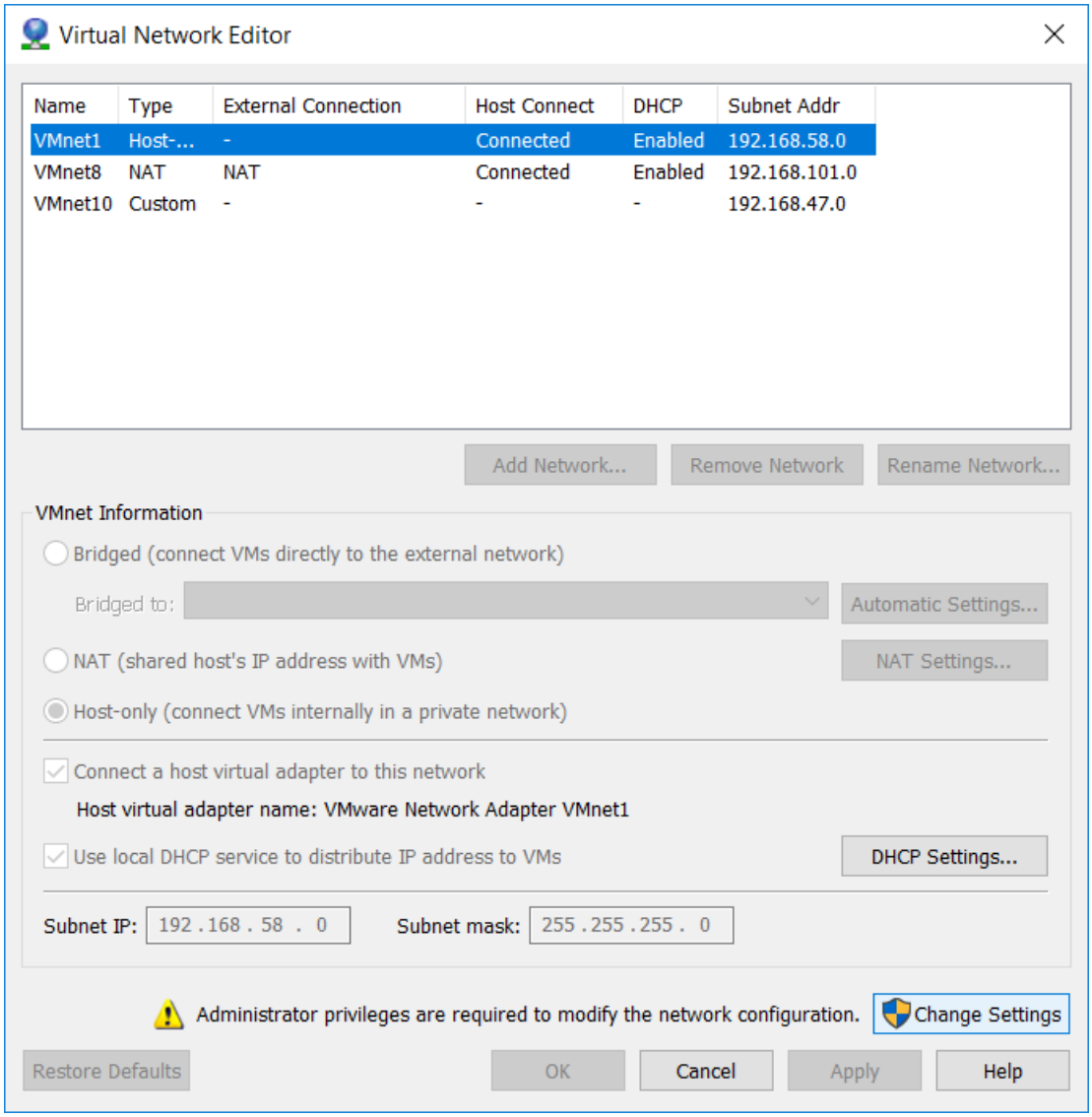


Figura 5. Virtual Network Editor

NOTA: Dar click en el botón *Change Setting* y aceptar la alerta de seguridad en caso de sistemas Windows.

b. Después de presionar sobre el botón Add Network... se mostrará un cuadro de diálogo donde se debe seleccionar el adaptador a agregar, en este caso seleccionar VMnet7 o cualquier otro adaptador disponible.

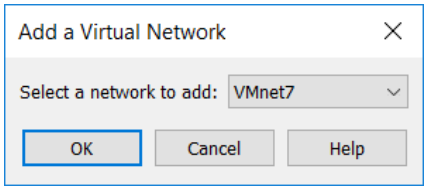


Figura 6. Agregar Adaptador Virtual VMnet7

c. Por último, configurar el adaptador para que se pueda utilizar el segmento de red 192.168.1.0 con máscara de red 255.255.255.0 tal como se muestra en la Figura 7.

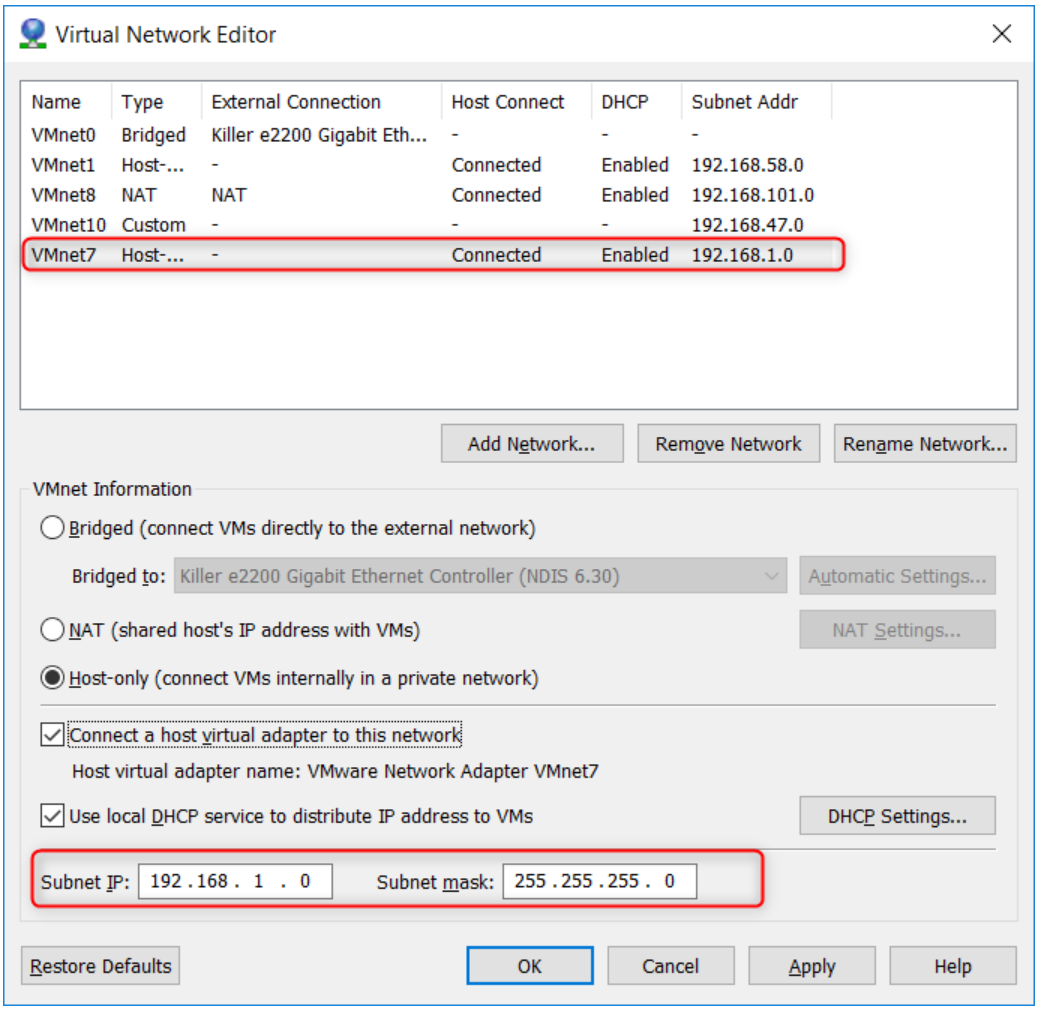


Figura 7. Configuración del adaptador virtual VMnet7.

d. Conectar los equipos al adaptador virtual VMnet1 para esto ingresar en el menú VM> Settings... se mostrará la pantalla de configuraciones de la máquina virtual. En la sección Network Adapter marcar en el panel derecho la opción Custom: Specific virtual network y seleccionar la opción VMnet1 tal como se muestra en la Figura 8. Repetir el procedimiento en los equipos A y B.

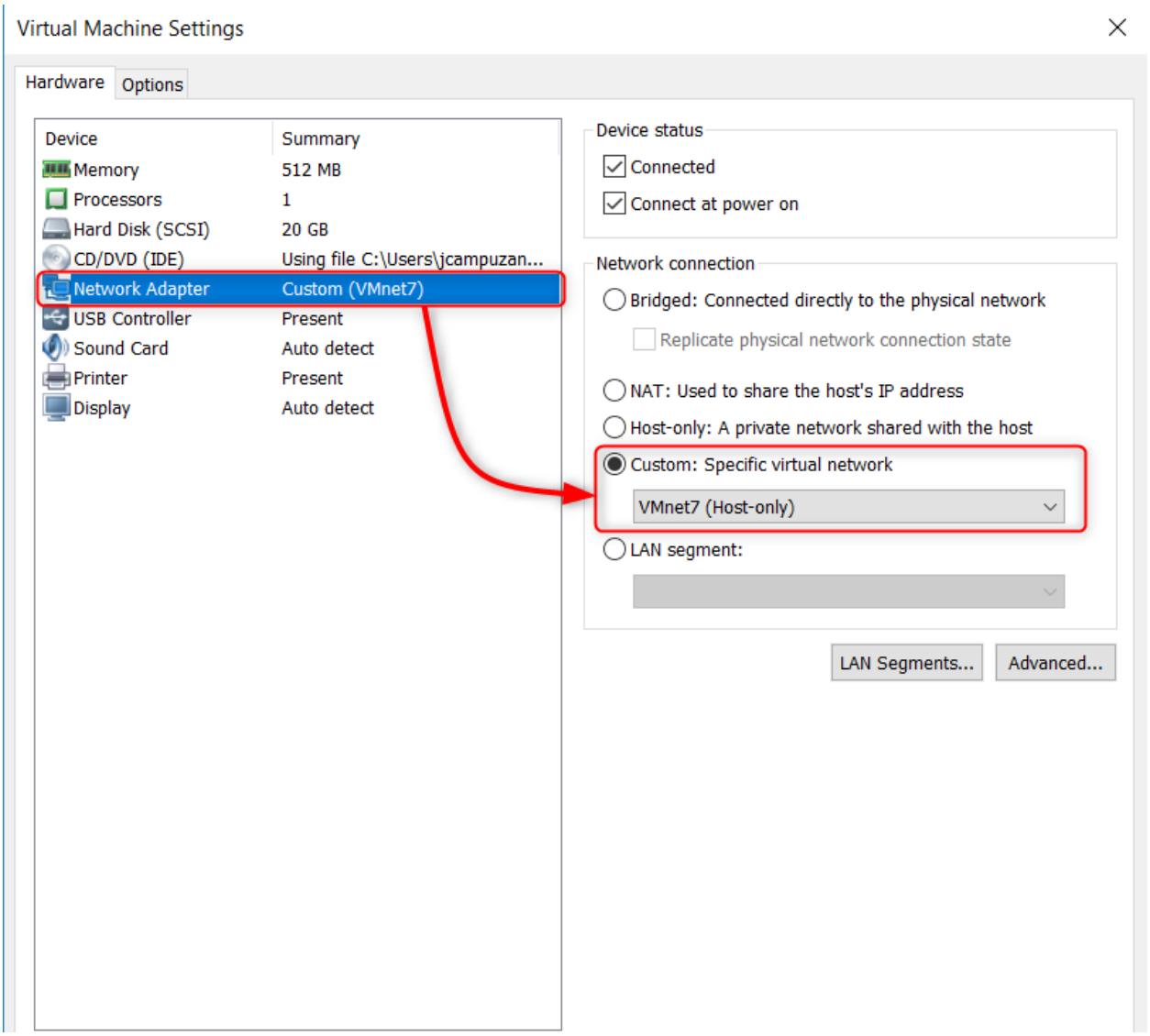


Figura 8. Conexión de la máquina virtual al adaptador VMnet1.

2. Instalación y configuración del servidor DNS

a. Configurar dirección IP estática en el equipo C. Para ello editar el archivo /etc/network/interfaces y hacer los cambios necesarios de manera que contenga la configuración mostrada en la Figura 9. Repetir el procedimiento en el equipo B cambiando la dirección IP por la 192.168.1.150 .

```
autho eth0
iface eth0 inet static
address 192.168.1.200
netmask 255.255.255.0
gateway 192.168.1.2
```

Figura 9. Configuracion de Red

b. Reiniciar el servicio de red con el comando service networking restart.

NOTA: Puede suceder que el comando no configure de manera correcta las interfaces, si eso sucede, reiniciar el equipo y verificar que la interface está encendida y con la configuración establecida en el archivo interfaces. c. Instalar la herramienta Bind, **apt-get install bind9 bind9utils bind9-doc**.

3. Configuración del manejador de Base de Datos

a. En la Tabla 1 se muestran los registros que se agregaran al DNS.

Host	Servicio	Nombre Canónico	Dirección IP
ns1	DNS Primario	ns1.redes.edu	192.168.1.200
www	Web	www.redes.edu	192.168.1.150
cliente	----------	kali.redes.edu	192.168.1.100

Tabla 1. Datos para servidor DNS

b. Para configurar correctamente el servidor DNS se requieren los siguientes archivos:

i. /etc/bind/named.conf.local # Archivo de configuraciones para consultas locales
ii. /etc/bind/named.conf.options # Archivo de configuraciones globales de Bind
iii. /etc/bind/zones/db.redes.edu # Archivo de resolución de nombres de dominio
iv. /etc/bind/zones/db.192.168.1 # Archivo de resolución inversa

c. A continuación, se muestra la configuración de cada uno de los archivos para el correcto funcionamiento de la práctica.

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "redes.edu"{
        type master;
        file "/etc/bind/zones/db.redes.edu";
};

zone "1.168.192.in-addr.arpa"{
        type master;
        file "/etc/bind/zones/db.192.168.1";
};
```

Figura 10. named.conf.local

```
acl "trusted"{
        192.168.1.200;  #Direccion IP de este servidor
        192.168.1.100;  #Direccion IP del cliente
};

options {
        directory "/var/cache/bind";
        recursion yes;
        allow-recursion {trusted;};
        listen-on {192.168.1.200;};
        allow-transfer {none;};

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                8.8.8.8;
                8.8.4.4;
        };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

Figura 11. named.conf.options

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.redes.edu. admin.redes.edu. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
; name servers - NS records
       IN      NS      ns1.redes.edu.

; name servers - A records
ns1.redes.edu.       IN      A       192.168.1.200

; 192.168.1.0/24 - A records
www.redes.edu.  IN      A       192.168.1.150
kali.redes.edu. IN      A       192.168.1.100
```

Figura 12. db.redes.edu

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.redes.edu. admin.redes.edu. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
; name servers - NS records
       IN      NS      ns1.redes.edu.

; PTR - records
68      IN PTR ns1.redes.edu.    ;.200
68      IN PTR www.redes.edu.    ;.150
68      IN PTR kali.redes.edu.   ;.100
```

Figura 13. db.192.168.1

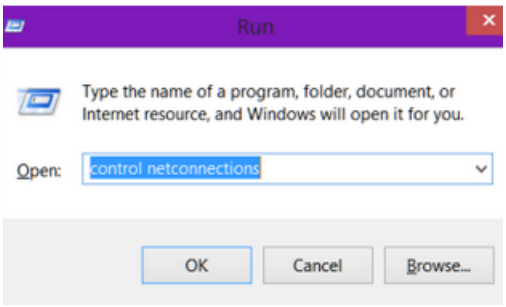
d. Una vez realizados los cambios reiniciar el servicio DNS. /etc/init.d/bind9 restart
e. Utilizar la herramienta netstat para verificar el estado del servicio

```
root@ns1:~# netstat -tpln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.1.200:53        0.0.0.0:*               LISTEN      3160/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1434/sshd
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      3160/named
```

4. Configuración del cliente

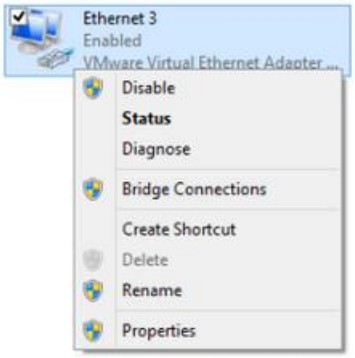
En equipos Windows:

• Presionar la combinación de teclado Windows + R



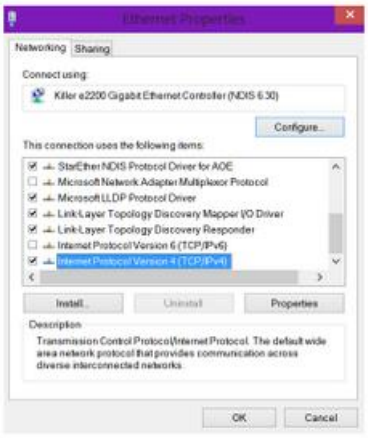
• En el cuadro de dialogo insertar el comando control netconnections. Se mostrarán las interfaces de red

• Presionar el botón secundario del ratón sobre el adaptador Ethernet 3 y seleccionar Propiedades.



NOTA: Existe la posibilidad de que el adaptador virtual tenga otro nombre, verificar que se esté configurando el adaptador correspondiente a la VMnet7.

• Seleccionar la opción Protocolo de Internet Versión 4 de la lista desplegable y posteriormente presionar el botón Propiedades.



• Modificar los parámetros de DNS e IP

En equipos GNU/Linux:

• Editar el archivo /etc/resolv.conf y agregar las siguientes directivas

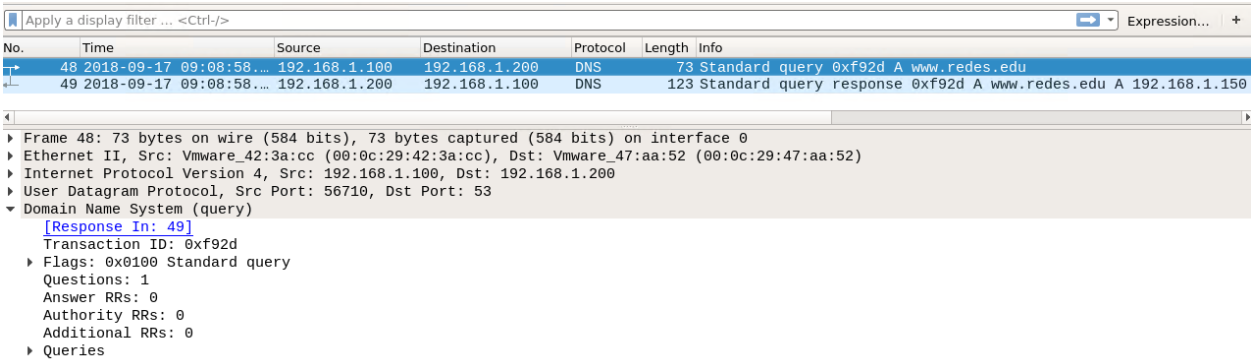
```
search redes.edu
nameserver 192.168.1.200
```

5. Captura de tráfico y verificación de la resolución de nombres

Iniciar una captura de tráfico con Wireshark.

Desde el equipo cliente conectarse a www.redes.edu/form.html

Verificar la resolución del domino en Wireshark



Cuestionario

¿Qué función tiene un servidor DNS autoritativo?

¿Qué función tiene un servidor DNS primario?

¿Qué función tiene un servidor DNS secundario?

¿Por cuál puerto se establecen las conexiones al servidor DNS?

Investigar el uso de los siguientes dominios, com, edu, gov, org, net, biz, xyz, mx, jp, tv.

Investigar sobre los registros DNS, A, AAAA, PTR, CNAME, TXT, MX.

¿En cuál RFC se especifica el protocolo DNS?

Consigne en el reporte una captura donde se muestre la resolución DNS seguida de la respuesta HTTP/S del servidor web.

Notas adicionales

• El reporte se entrega de forma individual.

• Se permite trabajar en equipo en caso de que sea complicado virtualizar las maquinas requeridas, corre por cuenta del equipo hacer las modificaciones en VMware para lograr la conectividad entre las maquinas (físicas o virtuales). El reporte se entrega de forma individual a pesar de haber trabajado en equipo

• Consigne en el reporte los pasos que considere necesarios para explicar cómo realizo la práctica, incluya capturas de pantalla que justifiquen su trabajo.

• Incluya las respuestas del Cuestionario en su reporte.

• Se pueden agregar posibles errores, complicaciones, opiniones, críticas de la práctica o del laboratorio, o cualquier comentario relativo a la práctica.

• La fecha de entrega será el día lunes 24 de septiembre de 2018 antes de las 11:59 a.m.