



TEMA DEL PROYECTO:

SERVIDOR DNS, MAESTRO Y ESCLAVO EN SISTEMA OPERATIVO DEBIAN

MATERIA:

REDES I

CATEDRATICO:

ING. MANUEL FLORES VILLATORO

HORARIO:

10:30 A.M. A 1:00 P.M.

INTEGRANTES DEL GRUPO # 7			
APELLIDO	NOMBRE	CARNET	NOTA
MARTINEZ HERNANDEZ	DENIS YOSILEY	MH01121153	
RAMIREZ ARIAS	WILLIAM GILBERTO	RA02110334	
FLORES TORRES	HENRY EDENILSON	FT02110600	
CORADO ESCOBAR	PABLO RODRIGO	CE02110289	
ALVARADO FUNES	ROBERTO VLADIMIR	AF02110290	

FECHA DE ENTREGA:

SABADO 24 DE MAYO DE 2014

Contenido

INTRODUCCION.....	3
OBJETIVOS DEL PROYECTO.....	4
Objetivo General:	4
Objetivo Especifico:.....	4
MARCO TEORICO.....	5
¿QUE ES UN DNS?	5
¿QUE ES BIND?.....	6
INSTALACIÓN DEL SERVIDOR DNS BIND.....	7
El servidor DNS bind admite tres modos de funcionamiento:.....	7
• Servidor DNS maestro	8
• Servidor DNS esclavo.....	8
• Servidor caché DNS	9
ARCHIVOS DE CONFIGURACION DEL DNS.....	10
CONFIGURACIÓN DNS MAESTRO.....	11
Archivo de zona de búsqueda directa.....	12
Los tipos de entradas que podemos crear en el DNS son:.....	13
Archivo de zona de búsqueda inversa	15
DIAGRAMA DE RED	17
DIAGRAMA DE GANTT.....	18
CONCLUSIONES.....	19
RECOMENDACIONES.....	20
BIBLIOGRAFIA.....	21

INTRODUCCION.

En el presente documento se hará una investigación de los programas que se necesitan en el desarrollo de una configuración de un sistema dns, maestro y esclavo, con el fin de poder contar con todos los conocimientos necesarios al momento de desarrollar la configuración del sistema antes mencionado ya que es de vital importancia que todos estos estén instalados para el correcto funcionamiento de dicho sistema.

Comenzando con la investigación de todas las tecnologías como lo es la instalación del sistema operativo Debian siendo esta una de las distribuciones de GNU/Linux y continuando con la instalación de un dns que nos permita configurar dos computadoras la cual una estará como maestro y la otra como esclavo todo con el propósito de traducir los nombres de dominio a direcciones IP y direcciones IP a nombres de dominio. Lo que se busca es hacer una conexión entre dos computadoras por medio de una red cableada.

La práctica se realizará cuando se comience a configurar el sistema bind9 que es donde se encuentran los archivos con los cuales se les asignará un nombre de dominio, una dirección IP, la computadora que tendrá el rol de maestro y la computadora que se ejecutará como esclavo, los cables serán utp45 todo esta configuración se realizará por medio de consola para aprender y practicar todos los comandos a utilizar. Uno de los puntos más importantes es conocer paso a paso la configuración de todos los archivos necesarios en el proceso.

OBJETIVOS DEL PROYECTO

Objetivo General:

- Configurar todos los archivos en el bind9 para la implementación del servidor dns maestro y esclavo.

Objetivo Especifico:

- Conocer toda la información sobre un dns.
- Investigar bind9 y las funciones que cumple en el proyecto.
- Adquirir todos los componentes físicos a utilizar.

MARCO TEORICO

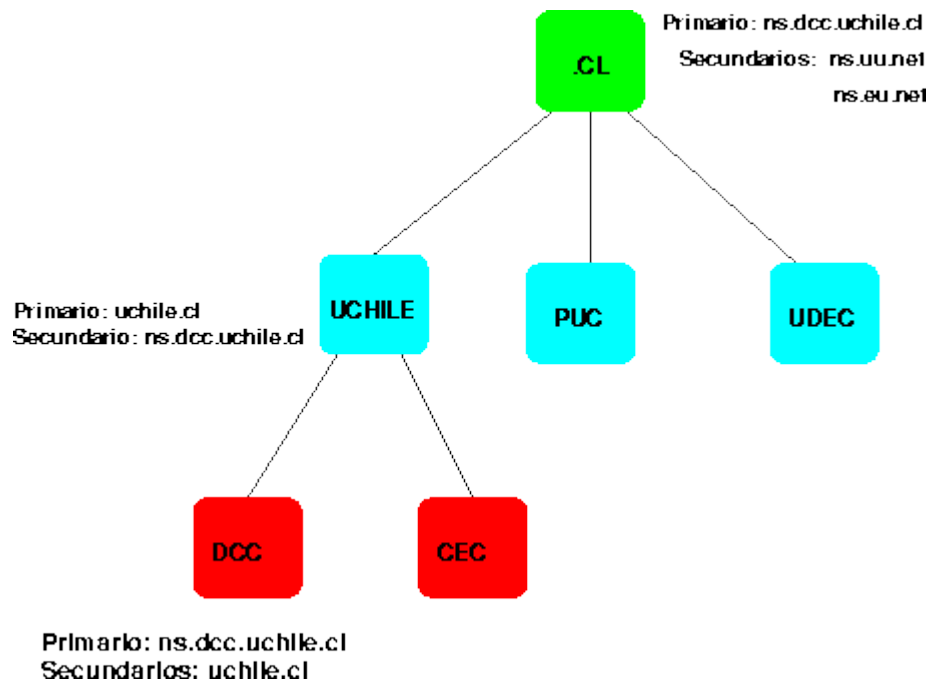
¿QUE ES UN DNS?

El dns (domain name service) es un sistema de nombres que permite traducir , el nombre de dominio IP y viceversa. Aunque internet solo funciona en base a direcciones IP, el dns permite a los humanos utilicen nombres de dominio que son mucho más fácil de recordar.

El sistema de nombres en el servicio de internet es un sistema distribuidos, jerárquicamente, replicado y tolerante a fallas. Aunque parece muy difícil lograr todos esos objetivos la solución no es tan compleja en realidad. El punto central se basa en un árbol que define la jerarquía entre los dominios y los subdominios. En un nombre de dominio, la jerarquía se lee de derecha a izquierda por ejemplo en dcc.uchile.cl, el dominio más alto es el cl. Para que exista una raíz del árbol, se puede ver como si existiera un punto al final del nombre dcc.uchile.cl y todos los dominios están bajo esa raíz (también llamado punto).

Cada componente del dominio (y también la raíz) tienen un servidor primario y varios servidores secundarios. Todos estos servidores tienen la misma autoridad para responder por ese dominio, pero el primero es el único con derecho para hacer modificaciones en el. Por ello el primario tiene la copia maestra y los secundarios copian la información desde el, el servidor de nombres es un programa que típicamente es una versión de bind (Berkeley internet name daemon) en general es mejor traer la última versión desde internet (www.isc.org) que usar la que vienen en el sistema operativo, por ser un servidor que ha cambiado mucho en los últimos tiempos.

La raíz de sistema del dominio es servida por algunos servidores “bien conocidos”. Todo servidor de nombre debe de ser configurado con la lista de los servidores raíz bien conocidos, estos servidores dicen de que dominios de primer nivel existen y cuáles son sus servidores de nombres .



Existe un conflicto de competencia entre el servidor de un dominio y el de un sub-dominio: ambos deben saber cuales son los servidores de nombres del sub-dominio. En un inicio, estarán de acuerdo, pero con el tiempo los servidores pueden ir cambiando, y las versiones de ambos pueden ser inconsistentes. Actualmente, el que manda es el servidor del sub-dominio, y su información es la más importante. Por ejemplo, si el servidor de .cl dice que uchile.cl es servido por los servidores A y B, y luego el servidor A dice que uchile.cl es servido por A y C, la información que se recibirá en el mundo es que los servidores son A y C. El único requisito es que por lo menos uno de los servidores de nombres que figuran en el dominio debe corresponder a uno de los que lista el sub-dominio. Si no es así, el dominio queda sin servidores y es inaccesible del resto del mundo

¿QUE ES BIND?

BIND (Berkeley Internet Name Domain, anteriormente: Berkeley Internet Name Daemon) es el servidor de DNS más comúnmente usado en Internet,^{3 4} especialmente en sistemas Unix, en los cuales es un Estándar de facto. Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley y liberado por primera vez en el 4.3BSD. Paul Vixie comenzó a mantenerlo en 1988 mientras trabajaba para la DEC.

Una nueva versión de BIND (BIND 9) fue escrita desde cero en parte para superar las dificultades arquitectónicas presentes anteriormente para auditar el código en las primeras versiones de BIND, y también para incorporar DNSSEC (DNS Security Extensions). BIND 9 incluye entre otras características importantes: TSIG, notificación DNS, nsupdate, IPv6, rndc flush, vistas, procesamiento en paralelo, y una arquitectura mejorada en cuanto a portabilidad. Es comúnmente usado en sistemas GNU/Linux.

INSTALACIÓN DEL SERVIDOR DNS BIND

Si con las posibilidades que nos ofrece dnsmasq no son suficientes para nuestra red y necesitamos un servidor DNS más completo, podemos utilizar el paquete bind9. Para instalarlo, podemos hacerlo con apt-get desde una consola de root:

```
// Instalación del servidor DNS bind
```

```
# apt-get install bind9
```

De esta forma instalaríamos los programas necesarios para disponer de un completo servidor DNS con bind. Tan solo será necesario configurarlo y ponerlo en marcha.

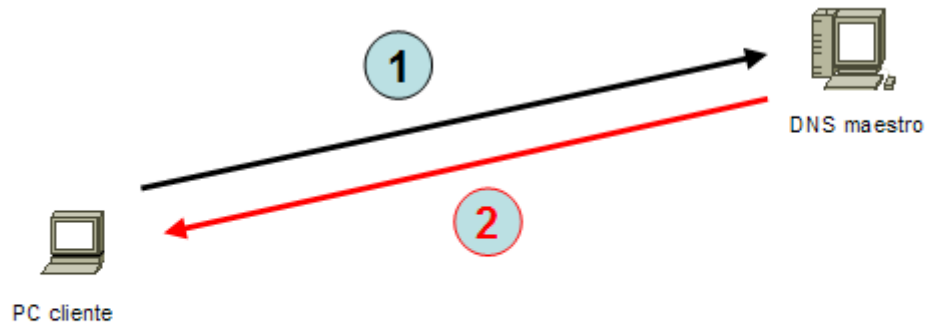
Configuración del servidor DNS

El servidor DNS bind admite tres modos de funcionamiento:

- Servidor DNS maestro
- Servidor DNS esclavo
- Servidor caché DNS

✚ Servidor DNS maestro

En este modo de funcionamiento, nuestro servidor se comporta como un auténtico servidor DNS para nuestra red local. Atenderá directamente a las peticiones de resolución de direcciones pertenecientes a la red local y reenviará a servidores DNS externos las peticiones del resto de direcciones de Internet.



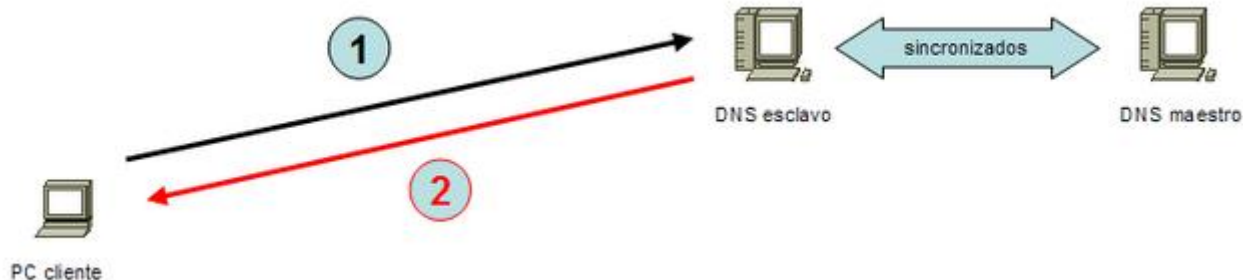
1 – Consulta DNS: ¿Cuál es la IP de aula5pc7.ieslapaloma.com?

2 – Respuesta DNS: La IP de aula5pc7.ieslapaloma.com es 192.168.0.107

- Consulta a un DNS maestro
- Consulta a un DNS maestro

✚ Servidor DNS esclavo

Un servidor esclavo actuará como un servidor espejo de un servidor DNS maestro. Permanecerá sincronizado con el maestro. Se utilizan para repartir las peticiones entre varios servidores aunque las modificaciones solo se realicen en el maestro. En redes locales salvo por razones de disponibilidad, es raro que exista la necesidad de tener dos servidores DNS ya que con uno será suficiente.



- Consulta a un DNS esclavo
- Consulta a un DNS esclavo

✚ Servidor caché DNS

En este modo de funcionamiento, nuestro servidor se comporta como si fuera un auténtico servidor DNS para nuestra red local aunque realmente no sea un servidor DNS propiamente dicho. Cuando recibe una petición de DNS por parte de un cliente de nuestra red, la trasladará a un DNS maestro que puede estar en nuestra red o fuera, almacenará en una memoria caché la respuesta y a la vez la comunicará a quien hizo la petición. Si un segundo cliente vuelve a realizar la misma petición, como nuestro servidor tiene la respuesta almacenada en su memoria caché, responderá inmediatamente sin tener que cursar la petición a ningún servidor DNS de Internet.

Disponer de un servidor caché DNS en nuestra red local aumenta la velocidad de la conexión a Internet pues cuando navegamos por diferentes lugares, continuamente se están realizando peticiones DNS. Si nuestro caché DNS almacena la gran mayoría de peticiones que se realizan desde la red local, las respuestas de los clientes se satisfarán prácticamente de forma instantánea proporcionando al usuario una sensación de velocidad en la conexión.

Es un modo de funcionamiento de sencilla configuración ya que prácticamente lo único que hay que configurar son las direcciones IP de un DNS primario y de un DNS secundario. Muchos routers ADSL ofrecen ya este servicio de caché, tan solo hay que activarlo y configurar una o dos IPs de servidores DNS en

Internet. En los PCs de nuestra red local podríamos poner como DNS primario la IP de nuestro router y como DNS secundario una IP de un DNS de Internet.

Consulta a un cache DNS. En caso de fallo, se redirecciona hacia un DNS maestro

Consulta a un cache DNS. En caso de fallo, se redirecciona hacia un DNS maestro

ARCHIVOS DE CONFIGURACION DEL DNS

El archivo de configuración del DNS es el archivo `/etc/bind/named.conf`, pero este hace referencia a otros cuantos archivos como por ejemplo:

- Archivo `named.conf`: Archivo principal de configuración
- Archivo `named.conf.options`: Opciones genéricas
- Archivo `named.conf.local`: Especificación particular de este servidor DNS
- Archivo `db.127`: Especificación dirección de retorno
- Archivo `db.root`: DNSs de nivel superior

Otros archivos: `db.0`, `db.255`, `db.empty`, `db.local`, `rndc.conf`, `rndc.key`, `zones.rfc1918`

Configuración como caché DNS

Por defecto, al instalar el paquete `bind` está preconfigurado como servidor caché DNS. Tan solo será necesario editar el archivo `/etc/bind/named.conf.options` y en la sección `forwarders` añadir las IPs de dos servidores DNS donde redirigir las peticiones DNS:

```
// Configuración como caché DNS
```

```
// Añadir IPs de los DNS de nuestro proveedor en /etc/bind/named.conf.options
```

```
options {
```

```
forwarders {  
80.58.0.33; 80.58.32.97;  
};  
};
```

CONFIGURACIÓN DNS MAESTRO

Por razones de accesibilidad y organizativas, deseamos asignar un nombre a todos los equipos de nuestra red, para lo que instalaremos un servidor DNS privado con un dominio ficticio, por ejemplo 'ieslapaloma.com'. Todos los PCs de nuestra red pertenecerán a dicho dominio ficticio que funcionará solo en nuestra red interna, no en Internet. En tal caso el nombre completo de los PCs terminará con 'ieslapaloma.com', por ejemplo: aula5pc2.ieslapaloma.com. Lo ideal en una situación así es disponer de un servidor DNS que sea maestro de nuestro dominio, es decir, maestro del dominio interno 'ieslapaloma.com'.

Nuestro servidor DNS maestro para nuestro dominio ficticio interno 'ieslapaloma.com' será capaz de resolver peticiones internas de nombres de este dominio, tanto de forma directa como de forma inversa, es decir, si recibe una consulta acerca de quién es aula5pc7.ieslapaloma.com deberá devolver su IP, pongamos por ejemplo 192.168.0.107. Si la consulta es una consulta DNS inversa acerca de quién es 192.168.0.107, deberá responder aula5pc7.ieslapaloma.com. Por ello deberemos añadir en el archivo /etc/bind/named.conf.local la especificación de maestro para el dominio y para la resolución inversa, por ejemplo:

```
// Añadir en /etc/bind/named.conf.local  
  
// Archivo para búsquedas directas  
zone "redesuno.com" {  
type master;  
file "/etc/bind/redesuno.db";  
};
```

```
// Archivo para búsquedas inversas
zone "11.254.168.in-addr.arpa" {
type master;
file "/etc/bind/192.rev";
};
```

Evidentemente será necesario crear los archivos `redesuno.db` y `192.rev` que especificarán la asociación entre nombres y direcciones IP de nuestra red en un sentido y en otro respectivamente.

Archivo de zona de búsqueda directa

Supongamos que en nuestra red local tenemos un aula llamada `aula5` con 12 PCs con IPs que van desde la `192.168.0.101` hasta `112` y cuyos nombres van desde `aula5pc1` hasta `aula5pc10`, luego un servidor web (`pc11`) y un servidor de correo electrónico que además es servidor DNS (`pc12`). El archivo de configuración DNS de nuestro dominio podría ser así:

```
// Archivo /etc/bind/redesuno.db
;
; BIND data file for redesuno.com
;
@ IN SOA ieslapaloma.com. root.redesuno.com. (
1 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Default TTL
IN NS dns.ieslapaloma.com.
IN MX 10 mail.ieslapaloma.com.
dns IN A 168.254.11.1
```

Serial: Indica la serie que lleva el Archivo de Zona" db ", este número es de suma importancia cada vez que sea alterado el archivo, ya que cuando un servidor "Slave" intenta actualizar sus datos es únicamente esta serie la que revisa, esto es, si al momento de comunicarse el servidor "Slave" con su servidor primario no detecta ningún cambio en este parámetro, asumirá que los datos no han cambiado

Refresh: Indica al servidor "Slave" el lapso de tiempo en segundos con que debe intentar comunicarse con el servidor primario para actualizar el Archivo de Zona.

Reintentar: En dado caso de fallar la comunicación con el servidor primario después de un intervalo Refresh (parámetro anterior) se debe intentar a razón de este valor.

Expirar: Si el servidor "Slave" no puede comunicarse con su servidor primario después del tiempo de este parámetro, el servidor "Slave" considerará el Archivo de Zona inválido.

TTL(Time to Live): Este valor es aplicable a todos los Resource Record del Archivo de Zona, cada resolución es enviada con este parámetro, a diferencia del parámetro anterior (expirar) que indica al servidor "Slave" cuando expirar los datos, este parámetro le indica a todos los servidores que han recibido información el tiempo de validez.

Los tipos de entradas que podemos crear en el DNS son:

Tipo de registro	Descripción
A	Traduce nombres a direcciones IP
PTR	Traduce direcciones a nombres
SOA	El primer registro de cualquier archivo de zona
SRV	Resuelve nombres de servidores que proveen servicios
NS	Identifica el servidor DNS de cada zona
MX	Para servidores de correo
CNAME	Resoluciones desde nombre de host a nombres de host

A (host o equipo): Contiene la información de asignaciones de nombre a dirección IP, es decir lo que ya sabemos que asignarle un nombre a una dirección IP. Los registros de recursos A también se conocen como registros de host.

NS (name server): Designa los nombres de dominio DNS de los servidores que tienen autoridad en una zona determinada o que contienen el archivo de zona de ese dominio.

CNAME (canonical name): Permite proporcionar nombres adicionales a un servidor que ya tiene un nombre en un registro de recursos A. Por ejemplo, si el servidor llamado "servidor1.ventas.miempresa" aloja el sitio web de "ventas.miempresa", debería tener también el nombre "www.ventas.miempresa. Los registros de recursos CNAME también se conocen como registros de alias.

MX (mail exchanger): Especifica el servidor en el que las aplicaciones de correo electrónico pueden entregar correo. Por ejemplo, si tiene un servidor de correo que se ejecuta en un equipo llamado mail1.ventas.miempresa y desea que todo el correo de nombreDeUsuario@ventas.miempresa se entregue en este servidor, necesitamos que el registro de recursos MX exista en la zona de "ventas.miempresa" y apunte al servidor de correo de ese dominio. A veces hay gente que se quiere poner un servidor de correo en casa, bien para aprender o por necesidad, si no le dice a su proveedor de Internet que le cree una entrada en el DNS de tipo MX ese servidor de correo nunca recibirá mensajes. ¡Vital para Exchange funcione desde el exterior!

SOA (Start Of Authority): Indica el punto de partida o el punto original de autoridad para la información almacenada en una zona. El registro de recursos SOA es el primero que se crea cuando se agrega una zona nueva. Contiene también varios parámetros que utilizan otros equipos que emplean DNS para determinar cuánto tiempo utilizarán la información de la zona y con cuánta frecuencia hay que realizar actualizaciones.

PTR (pointer): Se utiliza en una zona de búsqueda inversa creada en el dominio in-addr.arpa para designar una asignación inversa de una dirección IP de host a un nombre de dominio DNS de host.

SRV (service): Lo registran los servicios para que los clientes puedan encontrar un servicio mediante DNS. Los registros SRV se utilizan para identificar servicios en Active Directory y también se conocen como registros de ubicación de servicio.

Las primeras líneas son unos parámetros relacionados con la actualización del DNS (número de serie y periodos de actuación). Las dos siguientes líneas indican quién es el servidor primario (NS = Name Server) y quien procesa el

correo electrónico del dominio (MX = Mail eXchange). Las siguientes líneas especifican las IPs de los distintos PCs componentes del dominio (A = Address).

Si olvidamos algún punto y coma, dará errores y no funcionará correctamente. Para revisar los archivos disponemos de los comandos `named-checkconf` y `named-checkzone` que analizan que esté correcta la sintaxis de los mismos.

Por lo general, un registro de DNS contiene la siguiente información:

Nombre de dominio (FQDN)	TTL	Tipo	Clase	RData
es.redesuno.com	3600	A	IN	168.254.11.1

Archivo de zona de búsqueda inversa

Para poder realizar consultas inversas (de IP a nombre) será necesario crear el siguiente archivo:

```
// Archivo /etc/bind/192.rev
```

```
;
```

```
; BIND reverse data file for 168.254.11.1
```

```
;
```

```
@ IN SOA redesuno.com. root.redesuno.com. (
```

```
1 ; Serial
```

```
604800 ; Refresh //refrescar despues de un periodo de tiempo
```

```
86400 ; Retry // reintentar despues de una hora
```

```
2419200 ; Expire // Expirar despues de una semana
```

```
604800 ) ; Default TTL despues de u dia
```

```
IN NS dns.redesuno.com.
```

Una vez configurado nuestro servidor DNS, debemos indicar a nuestro servidor Linux que el servidor DNS es él mismo, lo cual se especifica en el archivo `/etc/resolv.conf`.

```
// Indicamos que nosotros mismos somos servidores DNS
```

```
// y por defecto buscamos en nuestro dominio
```

```
// Editar /etc/resolv.conf del servidor DNS
```

```
nameserver 127.0.0.1
```

```
search ieslapaloma.com
```

En el resto de PCs de la red, indicaremos que el servidor DNS es 168.254.11.1

```
// En el resto de PCs de la red indicamos quién es el DNS
```

```
// Editar /etc/resolv.conf del resto de PCs de la red
```

```
nameserver 168.254.11.1
```

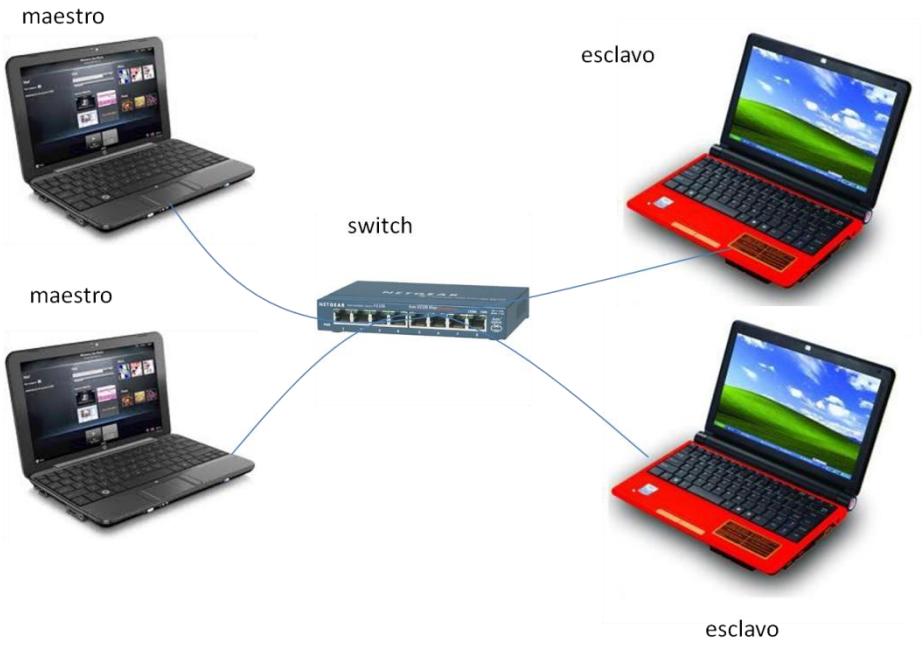
Tan solo nos faltará poner en marcha nuestro servidor de nombres ejecutando en el servidor el script de inicio correspondiente:

```
// Arranque del servidor DNS
```

```
# /etc/init.d/bind9 restart
```

y, mediante el comando `host`, el comando `dig` o el comando `nslookup` hacer alguna consulta de prueba:

DIAGRAMA DE RED



CONCLUSIONES.

- El programa bind es el encargado de enlazar las maquinas y configurarlas por medio de los archivos de configuración conf.local.
- Los dns sirven para distribuir las peticiones que se le hacen a un servidor y evitar el congestionamiento en la conversión de direcciones IP a nombres de dominio y viceversa.
- Con la configuración del dns nos aseguramos que las solicitudes que se le hacen a la zona estén siempre recibidas ya sea por el maestro y esclavo y si uno deja de funcionar el otro cubrirá con la demanda de las solicitudes.

RECOMENDACIONES.

- El servidor dns puede ser implementado de forma rápida y precisa en las empresas que quieran tener una red local.
- Para las pequeñas empresas o instituciones es una solución muy factible debido a que no se necesita invertir mucho solo contar con los conocimientos adecuados y las maquinas.
- Como estudiantes se puede emprender pequeños proyectos que serán de mucho beneficio en su implementación en lugares donde se pueden realizar horas sociales.

BIBLIOGRAFIA

[http://es.wikibooks.org/wiki/DNS_en_BIND/2-
_%C2%BFQu%C3%A9_es_BIND9](http://es.wikibooks.org/wiki/DNS_en_BIND/2-_%C2%BFQu%C3%A9_es_BIND9)

http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns_bind9.html

<http://users.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html>

<http://www.desarrolloweb.com/faq/50.php>

http://es.wikipedia.org/wiki/Domain_Name_System

<http://www.herramientasdns.com/registros-dns.aspx>