

Laboratorio de DNS y DHCP

CC50P, Taller de Redes de Datos

Profesor: Sebastián Castro A.

Introducción

El DNS es un servicio fundamental para el buen funcionamiento de una infraestructura de red basada en protocolos de Internet. Durante mucho tiempo también ha sido el servicio más descuidado desde el punto de vista de administración. Los esfuerzos se han concentrado en fortalecer la conectividad IP o la redundancia de los equipos y se han dejado de lado buscar su robustez y correcta administración.

Trabajaremos en este laboratorio en una configuración que les permita entender el mecanismo de funcionamiento, realizar las tareas más comunes (crear una zona, ser secundario de otra) y algunas tareas más avanzadas, como el uso de criptografía en el DNS.

Herramientas a utilizar

Linux

Comandos Necesarios

- **ifconfig**: permite configurar y chequear el estado de las interfaces de red, en particular la interfaz `eth0` es normalmente la interfaz real de red existente, algunos ejemplos:
 - `ifconfig -a`, despliega el estado y configuración de todas las interfaces existentes para el sistema.
 - `ifconfig eth0 inet 192.168.88.3 netmask 255.255.255.240 broadcast 192.168.88.15 up`, configura la interfaz `eth0` con el número IP 192.168.88.3 y activa la interfaz si ésta estuviera desactivada.
- **ping**: permite el envío de datagramas ICMP a un destino particular. Utilizado para verificar conectividad IP, y obtener muestras para medir latencia, RTT, tasa de pérdida.
 - `ping -c 100 192.168.88.4`: Envía 100 paquetes a la dirección 192.168.88.4
- **rndc** (Remote Named Controller): Es una herramienta que permite enviar comandos de control para el demonio de DNS, como iniciarlo, recargar archivos de configuración, recargar zonas, etc. Existe un archivo de configuración ubicado en `/ramdisk/bind/etc/rndc.conf`, por lo que deberá ejecutarlo como: `"rndc -c /ramdisk/bind/etc/rndc.conf <comando>"`.
- **named**: Corresponde al binario que da el servicio de DNS.
- **named-checkzone**: Programa utilizado para verificar la correcta sintaxis de un archivo de zona. Su invocación es `"named-checkzone <nombre-zona> <archivo-zona>"`.
- **named-checkconf**: Programa utilizado para verificar la correcta sintaxis de un archivo de configuración de BIND (`named.conf`). Su invocación típica es `"named-checkconf <archivo-named.conf>"`.
- **dig**: Es un programa que sirve para enviar consultas a un servidor DNS. Su estructura de ejecución normal es `"dig etiqueta RR @servidor"`. Acepta también algunas opciones útiles como `"+trace"`, que sirve para seguir el camino completo de resolución de una etiqueta (no especifique el servidor en esta opción); `"+tcp"` utiliza como transporte TCP en vez de UDP

(que es el transporte por defecto); “-k `archivo.llave`” utiliza la llave definida en el archivo para solicitar alguna operación (útil para la transferencia de zona). Existe además otra llamada que será de utilidad, usada para solicitar una zona completa: “`dig AXFR dominio @servidor`”.

- **pump:** Programa utilizado para solicitar y administrar la asignación dinámica de direcciones a nivel cliente. Es quien se encarga de pedir una dirección IP via DHCP a un servidor y luego renovar la dirección cuando corresponda.

Infraestructura de trabajo

Para realizar las diferentes experiencias de este laboratorio, contaremos con un switch, 10 computadores tipo PC corriendo Linux Knoppix, 1 notebook con Linux/Windows.

Experiencia 1

Objetivo: Conectar el computador a la red, obtener una dirección y bajar los archivos de configuración necesarios para operar con el DNS.

Datos:

- Red 192.168.0.0/25 (máscara 255.255.255.128)
- El computador del profesor se llama “profesor.lab” y su dirección será la 192.168.0.126.

Procedimiento

1. Inicie su computador. Automáticamente solicitará una dirección via DHCP al servidor de DHCP habilitado en la red. Ud obtendrá una dirección en el rango 192.168.0.110 y 192.168.0.120.
2. Verifique conectividad con el profesor, ejecutando “`ping 192.168.0.126`”
3. Verifique la correcta resolución de nombres, ejecutando “`ping profesor.lab`”.
4. Descargue el archivo de configuraciones para el DNS (<http://profesor.lab/dns/dns.tar>) y guárdelo en el directorio “/ramdisk”.
5. Descomprima el contenido del archivo usando `tar xvf dns.tar`.
6. Inicie su servidor de DNS con el comando “`named -c /ramdisk/bind/etc/named.conf -g`”. Esto dejará el servidor en modo depuración y podrá ver las líneas de log en la consola.
7. Verifique que su servidor de DNS funciona correctamente usando “`dig`”.
8. Solicite al profesor que verifique su configuración (NO OLVIDE ESTE PASO).

Experiencia 2

Objetivo: Configuración de un primario.

Datos:

- El profesor se asignará un nombre de dominio que utilizará de ahora en adelante, no lo olvide.

Instrucciones

1. Con el servidor de DNS andando, utilice el archivo “/ramdisk/bind/named/master/zona.base” para crear un archivo de zona para su dominio. No edite el archivo directamente, sino que haga una copia con el nombre de su archivo de zona, y luego edítelo.
2. Edite su archivo “/ramdisk/bind/etc/named.conf” para definir el primario para la zona que recién creó. Existe una estructura general en el archivo, que Ud. deberá ajustar para sus propias necesidades.

3. Antes de probar, verifique que su archivo de zona y su archivo de configuración son correctos. Para ello use “named-checkzone” y “named-checkconf” respectivamente.
4. Una vez que sus archivos sean correctos, recargue su configuración ejecutando “rndc -c /ramdisk/bind/etc/rndc.conf reload” y verifique los mensajes de error entregados por el proceso “named”.
5. Verifique con dig y consultando directamente a su servidor, el correcto funcionamiento de su dominio.
6. Solicite al profesor que verifique su trabajo.

Experiencia 3

Objetivo: Registrar su dirección MAC en el servidor DHCP del profesor.

Instrucciones

1. Utilizando el CGI ubicado en <http://profesor.lab/cgi-bin/dhcp.pl> registre la MAC de su equipo y su nombre asignado.
2. Una vez que todos hayan realizado este paso, procederemos a asignar una IP fija a cada computador (lo que nos permitirá expandir nuestra infraestructura de DNS).
3. Con la configuración obtenida y el servidor de DHCP reiniciado, deberá buscar el proceso en ejecución llamado “pump” y matarlo usando kill. Luego, ejecútelo de nuevo y obtendrá su dirección IP fija.

Experiencia 4

Objetivo: Configuración de un secundario.

Instrucciones

1. Configuraré su servidor como secundario de la zona “zona.test”, cuyo primario es el servidor del profesor.
2. Edite el archivo “named.conf” y siga las instrucciones. Ya existe un patrón para realizar esta tarea, sólo deberá actualizar algunos parámetros.
3. Una vez editado, verifique su archivo de configuración con “named-checkconf” y luego recárguelo usando “rndc reload” (no olvide el parámetro -c).
4. Verifique las líneas de log del proceso “named” y luego verifique utilizando DIG su propio servidor.
5. Solicite al profesor que verifique su trabajo.

Experiencia 5

Objetivo: Restringiendo la transferencia de zona, utilizando llaves TSIG.

Instrucciones

1. El profesor restringirá la transferencia de la zona “zona.test” sólo a aquellos hosts que tengan una llave habilitada.
2. Para ello, genere una llave ejecutando “dnssec-keygen -a HMAC-MD5 -b 128 -n HOST -r /dev/urandom <nombre-llave>”. El formato del nombre de llave será “<grupo>-test.key.” (ojo con el punto al final). El formato es convención de éste laboratorio. El comando generará dos archivos, de la forma K<nombre-llave>+<algo>+<llave-id>.(key|private), que contienen el nombre de la llave y el contenido.
3. Suba el archivo .key al servidor del profesor, usando “scp”. Para ello, ejecute “scp K*.key lab@profesor.lab:dnstest”.
4. Mientras el profesor incorpora su llave a la configuración del servidor principal, Ud. prepare su archivo de configuración, usando el molde ya disponible. Cabe notar que aparte de indicar la llave a usar y su contenido, deberá descomentar la sección donde se indica que llave usar para conectarse con la IP del servidor del profesor. **NOTA IMPORTANTE:** el nombre de la llave tiene que ser ingresado en el archivo de configuración tal como se generó, sino la transferencia no funcionará.
5. Verifique que puede transferir la zona utilizando “dig AXFR zona.test @profesor.lab -k K<llave>.key”. Si funciona, podrá ver los registros de la zona, si no, verá un mensaje de “Transfer failed”.

Experiencia 6

Objetivo: Verificación de la resolución usando DIG

Instrucciones

1. Probaremos que la delegación de dominios, definición de registros y resolución operan correctamente.
2. Para ello, tome registros de su dominio y de otros dominios y consúltelos usando “dig” con la opción +trace. Con ello podrá entender los pasos necesarios para poder resolver.
3. Probaremos también consulta los reversos para la red. Para ello, utilice su dirección IP y consulte por “dig -x IP”. Deberá obtener un registro PTR con el nombre de su máquina.