SRC. IES Haría
UT2. Actividad 3

Delegación de autoridad DNS en Linux

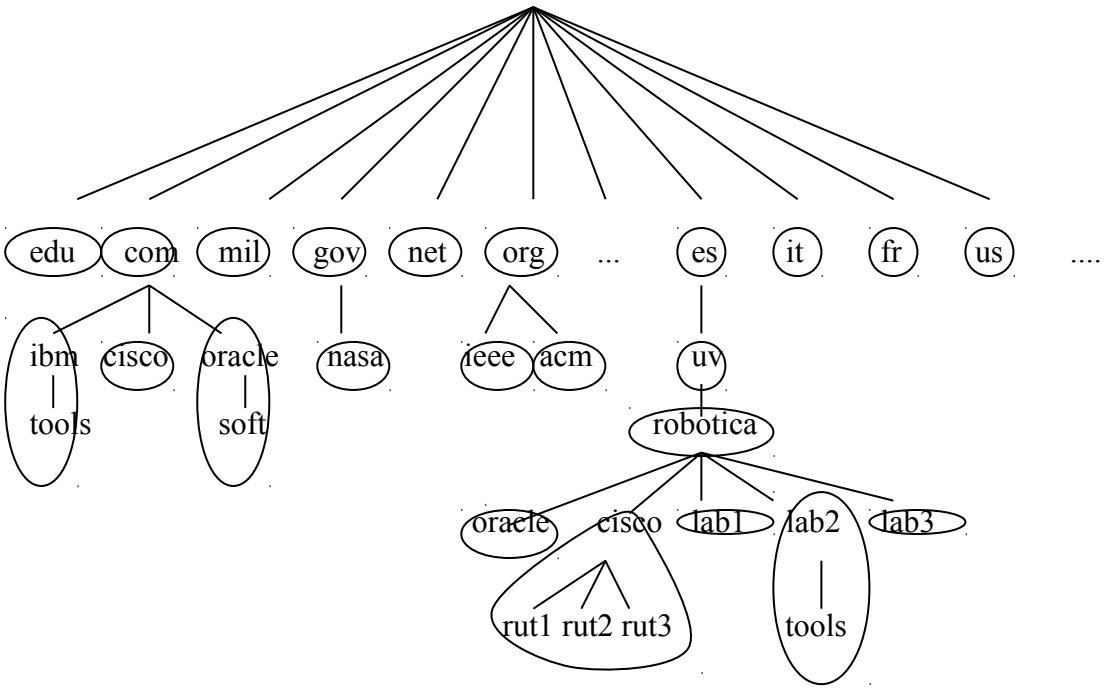
Teoría. Servidores de nombres y zonas de autoridad

Toda la información acerca de un espacio de dominio se guarda en una computadora que llamamos Servidor de Nombres. Esto es la implementación física del llamado programa servidor que antes hemos mencionado.

Generalmente, los servidores tienen información completa acerca de una parte del espacio de dominio de nombres, que llamamos *zona de autoridad*. Más exactamente una *zona* es la porción del espacio de nombres de dominio de la que es responsable un determinado servidor DNS. La zona de autoridad de estos servidores abarca al menos un dominio y también pueden incluir subdominios, aunque a veces los servidores de un dominio puede delegar sus dominios en otros servidores.

La diferencia entre una *zona* y un *dominio* es que la primera contiene los nombres de dominio y datos que representan a un dominio y un *dominio* es un nombre a que agrupa a otras máquinas o dominios inferiores.

Veamos a continuación una forma de dividir el espacio de nombres:



División en zonas de parte del Espacio de Dominio de Nombres.

Cada **zona** tendrá asignada un **servidor de nombres primario** que obtiene su información de su base de datos local y uno o más **servidores secundarios** que obtienen su información del servidor de nombres primario. Recordemos que el lugar donde se colocan los limites de una zona dentro de una zona es responsabilidad del administrador de esa zona.

Pasos de la actividad

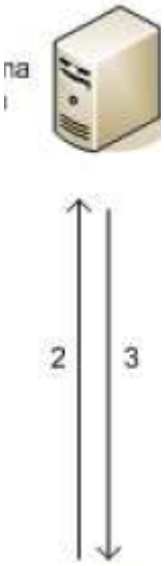
Realiza esta actividad en pareja o utilizando dos máquinas virtuales. En uno de los servidores se administra la zona principal y se va a delegar la administración de un subdominio. Por tanto, al otro servidor se le va a añadir un subdominio y vamos a crear el archivo de zonas para el mismo.

En la anterior actividad creamos el dominio (suponiendo que te llamas adrian) **adrian.edu** y configuramos un servidor maestro de DNS (172.16.110.1, por ejemplo) para dicha zona. Vamos a crear un subdominio, por ejemplo **delante.adrian.edu** y vamos a delegar la administración del mismo al servidor del compañero (172.16.110.2, por ejemplo).
Los pasos, **de forma genérica**, serían:

1) Creamos una nueva zona en otro equipo a la que puedes llamar, p. ej., **delante.adrian.edu**
2) Creamos en la zona **adrian.edu** un **registro** para indicar cuál es el servidor de nombres dónde se encuentra la zona delegada **delante.adrian.edu**. Pej: nsdelante IN A 172.16.110.2
3) Creamos el **enlace a la nueva zona** en la zona del dominio **adrian.edu** mediante el registro: delante IN NS nsdelante. Este es el registro que indica a los clientes a que servidor de DNS deben contactar para resolver direcciones del subdominio **delante.adrian.edu**

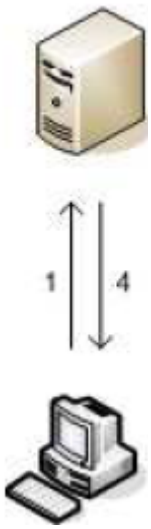
Gráficamente:

Servidor de DNS que administra la zona `delante.adrian.edu` (172.16.110.**2**)




```
@       IN SOA  ns.delante.adrian.edu
root(1 360000 3600 3600000 3600)
         IN NS    ns
ns       IN A     172.16.110.2
oliver   IN A     172.16.110.5
raul     IN A     172.16.110.7
… ← resto de hosts de la parte delante del
aula
```

Servidor de DNS que administra la zona `adrian.edu` (172.16.110.**1**)




```
@       IN SOA  ns.adrian.edu
root.adrian.edu(1360000 3600 3600000 3600)
            IN NS    ns
ns          IN A     172.16.110.1
delante     IN NS    nsdelante
nsdelante   IN A     172.16.110.2
israel      IN A     172.16.110.5
oscar       IN A     172.16.110.6
… ← resto hosts de la zona detrás del aula
```

Este servidor DNS contiene la zona **adrian.edu** y por tanto no conoce la dirección IP de **raul.delante.adrian.edu**, pero conoce donde se encuentra el servidor DNS que contiene la zona delante.adrian.edu

4) El software de DNS bind viene por defecto con DNSSEC activado, lo cual da problemas al realizar resoluciones de nombres, debido a que no lo tenemos configurado. Bind también, por defecto, configurado para escuchar peticiones por IPv6. Para deshabilitarlos, en ambos servidores, editamos el fichero **`/etc/bind/named.conf.options`**. En la parte final del mismo aparecen las siguientes líneas:

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

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

Cambiamos el contenido de forma que quede:

```
//========================================================================
// 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 no;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { none; };
```

Si además tuviésemos añadidos forwarders en el fichero debemos comentarlos, porque si no el servidor reenviaría las peticiones a los forwarders cuando le preguntáramos por registros de la zona delegada.

```
        //forwarders{
        //      172.16.0.1;
        //      8.8.8.8
        //};
```

Luego reiniciamos el servicio (`sudo service bind9 restart`) para que se apliquen los cambios.

Comprobaciones:

En un equipo cliente podremos ahora resolver los nombres de los equipos y servidores de la zona delegada, preguntándole tanto al servidor de la zona delegada como al servidor de la zona principal. Si por ejemplo, en un equipo de la red, ejecutamos:

```
dig @172.16.110.1  raul.delante.adrian.edu
dig @172.16.110.2  raul.delante.adrian.edu
```

Debemos obtener respuesta.

Sin embargo, si preguntamos al servidor de la zona delegada por nombres de la zona principal:

```
dig @172.16.110.2  router.adrian.edu
```

No vamos a obtener respuesta puesto que el servidor delegado no sabe como reenviar las peticiones al servidor principal. Para indicárselo, editamos, en el servidor delegado, el fichero **`/etc/bind/named.conf.local`** y añadimos lo siguiente:

```
zone "adrian.edu" {
        type forward;
        forwarders {172.16.110.1;};
};
```

Con ello estamos indicando al servidor secundario a quien debe reenviar las peticiones si le solicitan registros del servidor de la zona principal.

Ahora, después de reiniciar el servicio, deberíamos obtener respuesta al ejecutar:

```
dig @172.16.110.2  router.adrian.edu
```

Cuando hayas terminado, si estas haciendo la práctica con un compañero, realiza los mismos pasos cambiando los roles.

Comprueba el correcto funcionamiento y avisa al profesor para que corrija la actividad