Gestión e Implantación
de Redes de Computadores

Práctica 1

Prácticas GIRC

Configuración software de una red Linux con TCP/IP.

Objetivo

En esta práctica se pretende mostrar el proceso de instalación y configuración de TCP/IP sobre Linux, tanto del protocolo como de los servicios más representativos.

Al finalizar la sesión dispondremos de una red de área local con nodos configurados en Linux, utilizando el protocolo de red TCP/IP, nodos capaces de proporcionar y acceder a sistemas de archivos, páginas, formularios HTTP e Internet a través de un proxy, etc. En definitiva, al finalizar la práctica estaremos en disposición de crear nuestra propia **INTRANET** o de integrarnos sin problemas en **INTERNET** basándonos en el sistema operativo Linux.

Conocimientos previos

Dispositivo y protocolo de red (TCP/IP)

De igual forma que los manejadores de dispositivo, las rutinas que proporcionan la implementación de la pila de protocolos TCP/IP deben estar incluidos en el núcleo de linux. También, de igual forma que los manejadores, tenemos los mismos métodos para realizar esta tarea:

- Estáticamente, compilando el núcleo del sistema Operativo incluyendo el código necesario.
- Dinámicamente, añadiendo las rutinas ya compiladas al núcleo durante la inicialización del sistema o una vez ya inicializado.

De hecho, lo normal es que, tanto la tarea de instalación de los manejadores como la de instalación de los protocolos, se efectúe al mismo tiempo. Es decir, si optamos por compilar el núcleo, añadiremos las opciones de dispositivo y las de TCP/IP. Si, por el contrario, optamos por añadir módulos, incluiremos los módulos de los dispositivos y los de TCP/IP en el archivo de configuración.

A continuación describimos algunas de las opciones de compilación que nos encontraremos durante su configuración:

IP forwarding/gatewaying [n]
Determina si el equipo podrá o no realizar reenvío de paquetes destinados a sistemas diferentes. Si el equipo que estamos configurando va a actuar como "puerta de enlace" (o gateway).

IP multicasting [n]
Determina el soporte de operaciones que utilicen este protocolo. Este protocolo se utiliza para enviar paquetes a más de un equipo.

IP firewalling [n]
Determina si el núcleo tendrá o no capacidades para filtrado de paquetes y otras tareas similares para gestión de seguridad.

Configuración de TCP/IP

Para configurar el protocolo TCP/IP necesitamos configurar los siguientes apartados:

- Configuración del dispositivo adaptador de red
- Configuración de las rutas
- Configuración de los nombres de dominio (DNS)
- Configuración de los servicios y servidores

Configuración del dispositivo adaptador de red
Configurar el dispositivo de red consiste básicamente en asignarle una dirección IP junto con algunos parámetros adicionales como la máscara de red, la dirección de difusión (broadcast) y, finalmente, activar dicho dispositivo.

El comando utilizado para esta tarea es ip o bien ifconfig. A continuación mostramos una línea típica de configuración de dispositivo para el primer adaptador de red ethernet del equipo:

```
_# ip link set eth0 up

_# ip addr add 172.20.41.6/24 dev eth0
```

Para comprobar la configuración actual de un dispositivo, utilizaremos el mismo comando pero indicando tan sólo el adaptador deseado. Por ejemplo:

```
_# ip addr ls eth0

1: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:50:da:07:29:84 brd ff:ff:ff:ff:ff:ff
```

inet 172.20.44.224/24 scope global eth0

_# ip addr ls lo

1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/32 scope host lo
inet 127.0.0.1/8 scope host lo

Otra opción es ejecutar la orden *ifconfig* sin argumentos.

Encaminamiento (routing)
Una vez configurado nuestro dispositivo, el siguiente paso natural será indicar a nuestro equipo cómo y por dónde debe enviar los paquetes para que lleguen al resto de nodos de la red.

Podemos optar por la estrategia de enrutamiento dinámico activando alguno de los demonios disponibles para tal fin: **gated** y **routed**. Sin embargo, nosotros optaremos por la estrategia de configurar nuestras rutas explícitamente y de forma estática. Según esto, se trata de crear una serie de reglas que le indiquen al equipo cómo trabajar con los paquetes.

El comando utilizado para esta cuestión es el comando **route** (para obtener ayuda tendremos que utilizar las opciones "man route"), ahora incluido como *objeto* del comando **ip** (iproute2).

La primera ruta y fundamental es la que le indica al equipo cómo y por dónde enviar los paquetes dirigidos a equipos de la propia red, ésta ruta la crea el sistema automáticamente al asignar la dirección ip a una interfaz. No obstante, la orden para añadir nuevas rutas a la tabla de rutas del núcleo es:

_# ip route add <red_local>/<máscara> dev eth0 [table <tabla>]

Crearemos todas las rutas necesarias para alcanzar las redes que conocemos y dependen de nosotros

Puerta de enlace (Gateway)
Una de las diferencias del protocolo TCP/IP frente al protocolo NetBEUI es que TCP/IP sí es reencaminable, es decir, podemos enviar paquetes de una a otra red utilizando nodos especiales que funcionan como encaminadores de los paquetes. Estos nodos se denominan frecuentemente: puerta de enlace o gateway y deberán poseer la capacidad de reenvío de paquetes (IP forwarding) antes comentada..

Por lo tanto, si es necesario, generaremos la "ruta por defecto" que se utilizará siempre que no se encuentre otra regla para un determinado paquete y que utilizará una "puerta de enlace" para enviar paquetes al exterior de nuestra red:

_# ip route add default via <gateway> dev eth0

default está definido como la IP 0.0.0.0 y gateway suele tener la primera dirección de la red.

Para comprobar que la configuración de la red se ha realizado correctamente, se dispone de los comandos ping, traceroute y netstat. Con los dos primeros se comprueba la comunicación y el camino que se sigue para establecer una conexión con el host remoto. Con el tercero, se comprueba el estado de las interfeces de red (opción -i) y las rutas configuradas (opción -r).

¿Cómo comprobaríamos que nuestra red está bien configurada? ¿Qué comprobaciones deberíamos hacer

para comprobar que nuestro PC está conectado a la red?

Configuración del cliente de DNS
En multitud de ocasiones hemos visto que existe un mecanismo alternativo a las direcciones IP para nombrar un determinado nodo de nuestra red y que proporcione un mecanismo más sencillo para el usuario que la utilización de direcciones numéricas. Se trata, obviamente del sistema de nombres DNS (Domain Name Server). Este sistema está basado en una base de datos local o distribuida que contiene la relación existente entre una dirección IP y su nombre DNS. Un nombre dns está compuesto por

nombreHost.dominio

Para asignar un nombre a nuestro equipo, utilizaremos el siguiente comando:

_# hostname Nombre

Archivos importantes en la configuración básica de TCP/IP y DNS

- /etc/hosts
- /etc/networks
- /etc/resolv.conf
- /etc/host.conf

Archivo /etc/hosts
Se trata del principal archivo utilizado para la resolución de nombres local. Contiene una relación entre direcciones IP y nombres DNS. A continuación se muestra un ejemplo de archivo:

```
_# cat /etc/hosts
127.0.0.1        localhost
172.20.41.7    clL16-1   clL16-1.eps.ua.es
172.20.41.8    clL16-2   clL16-2.eps.ua.es
172.20.41.9    clL16-3   clL16-3.eps.ua.es
```

Archivo /etc/networks
Se trata de un archivo similar a /etc/hosts pero destinado a la resolución de IPs referidas a redes. A continuación se muestra un ejemplo típico:

```
_# cat /etc/networks
loopnet      127.0.0.0
L16      172.20.41.0
```

Archivo /etc/resolv.conf
Este archivo contiene una serie de directivas que permiten configurar la resolución de nombres DNS.

domain
Indica el dominio DNS al que pertenece el equipo

search
Permite especificar una lista de dominios que se utilizarán para completar un nombre DNS que no esté totalmente cualificado.

Según esto, si decidimos utilizar un nombre como `clL16-1` en vez de utilizar `clL16`.eps.ua.es y en la etiqueta "search" hemos incluido dtic.ua.es e inf.ua.es, el sistema añadirá estos

dominios a clL16-1 para intentar resolver el nombre apropiadamente.

> **Nota:** El primer dominio de la lista se utilizará como el dominio del equipo, de igual forma que la etiqueta "domain" antes descrita.

nameserver
Con esta directiva especificamos el servidor de nombres DNS que deseemos utilizar.

> **Nota:** La dirección del servidor de nombres se debe proporcionar indicando su dirección IP puesto que si diéramos su nombre DNS, no podría resolverlo.

A continuación mostraremos un pequeño ejemplo de archivo **/etc/resolv.conf**:

```
_# cat /etc/resolv.conf
domain eps.ua.es
search eps.ua.es
nameserver 172.25.40.81
nameserver 172.20.41.86
```

Archivo /etc/host.conf
Es perfectamente compatible utilizar los dos estrategias (archivo hosts y servidor DNS) al mismo tiempo. Para indicar qué estrategia y qué orden se utilizará para realizar la resolución de nombres utilizaremos la directiva "order" de este archivo.

Las opciones son: bind para indicar la resolución a través de servidor de nombres y hosts para indicar la resolución mediante el archivo /etc/hosts

A continuación podemos ver un sencillo ejemplo de este archivo en el que se indica que se utilice primero la resolución local a través del archivo **/etc/hosts** y, si no se ha podido resolver, utilizará el servidor o servidores de nombre definidos en el archivo **/etc/resolv.conf**:

```
_# cat /etc/host.conf
order hosts, bind
```

Herramientas de configuración y depuración en línea

Tenemos a nuestra disposición una serie de comandos que nos permiten efectuar tareas de depuración de la configuración. En ocasiones, encontraremos situaciones que sólo podremos resolver manualmente. Los comandos disponibles son:

nslookup
Permite depurar la resolución de nombres, cambiando el servidor que deseemos utilizar, configurándolo en modo depuración para que muestre todos los pasos seguidos en la obtención de un nombre, etc.

ping
Es una de las utilidades más básicas de TCP/IP utilizada para depurar redes. Esta utilidad simplemente envía un paquete TCP/IP y espera recibirlo, mostrando al final una estadística de los paquetes enviados y de los recibidos. Si nuestra red funciona correctamente, deberán

coincidir ambos números.

Con esta utilidad también podemos observar la velocidad de la comunicación puesto que nos indica el tiempo que ha tardado el equipo remoto en devolver el paquete enviado.

arp
Permite manipular la caché de direcciones del nodo de la RED. Con la opción -a, conseguimos que se muestre todas las direcciones que se han resuelto recientemente.

traceroute
Es otro de los clásicos para depurar redes TCP/IP. Su versión UNIX es el comando "traceroute". Se trata de una utilidad que nos muestra (dado un nombre de nodo), todos los nodos (gateways) por los que pasa la información hasta alcanzar su destino.

netstat
Muestra información diversa sobre las conexiones de red, servicios activos, estadísticas de los dispositivos (opción -i), tabla de rutas (opción -rn), etc.

VirtualBox + Ubuntu

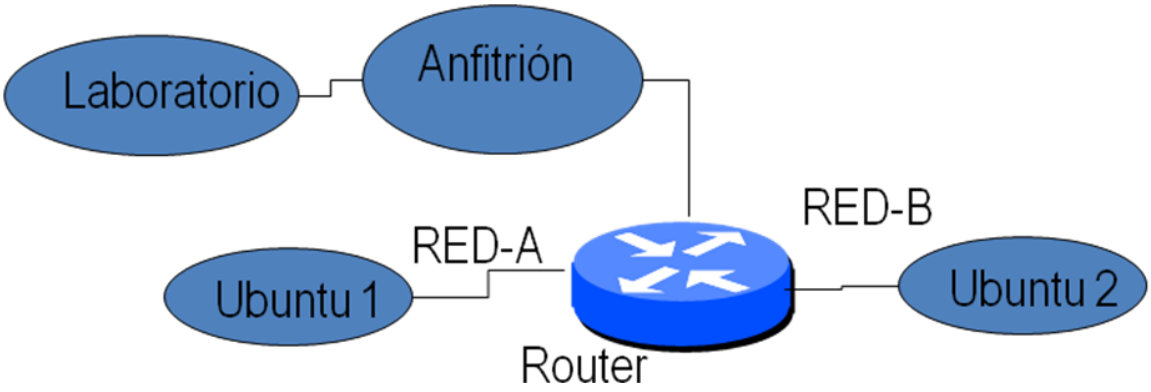
Para esta práctica emplearemos el sistema operativo disponible en los ordenadores del laboratorio. Simularemos una red de trabajo utilizando VirtualBox como software de virtualización y crearemos las máquinas virtuales necesarias utilizando como imagen del sistema una distribución Ubuntu, preferiblemente la UBUNTU 16.04.3, aunque puede ser cualquiera.

Enunciado de la práctica

Básicamente, las tareas a realizar en esta práctica son:

- Iniciar el equipo y comprobar que se ha cargado todo perfectamente y que tenemos salida a Internet.
- Empleando el software de virtualización VirtualBox, crear y configurar, en el equipo de laboratorio, una red simulada que siga el esquema del dibujo. Para ello, se dispone de la clase C 192.168.X.0, donde X es el número de PC. Los tres equipos deben tener la configuración mínima adecuada que le permita conectarse con cualquier equipo de las dos redes locales virtuales definidas (red A y red B) y con Internet (tarjetas y tablas de rutas). Además, se debe configurar el cliente de DNS en todos los equipos para que se pueda resolver los nombres de equipos.
  Para crear el router se debe añadir una máquina virtual con 3 interfaces. Una para la red A (red interna), otra para la Red B (red interna) y otra para la red de comunicación con el Anfitrión (NAT, ésta es el que nos comunica con el resto del laboratorio e Internet)
- Comprobar el funcionamiento de la red.

Para la corrección de la práctica se debe explicar al profesor cómo se han resuelto cada una de las cuestiones planteadas así como las pruebas realizadas para comprobar el funcionamiento de la red. Esta información se expondrá también en una breve memoria de la realización de la práctica.



DURACIÓN DE LA PRÁCTICA: 2 sesiones