

Prácticas

1. Configuración TCP/IP de Linux

Objetivo: configurar una agrupación de tarjetas de redes en una distribución usando Network Manager.

1. Se pueden crear agrupaciones de tarjetas de redes con Linux. En caso de que falle una, otra puede tomar el relevo, o incluso n tarjetas pueden funcionar de manera simultánea. Las tarjetas se llaman, generalmente, bond0, bond1, etc, pero pueden llamarse también de otra manera.

Cree una interfaz:

```
nmcli con add type bond ifname bond0
```

2. Crear agrupaciones de tarjetas (bonding) necesita la carga del módulo "bonding" y la definición de un modo de agrupación. Los parámetros de este módulo determinan el modo de funcionamiento de la agrupación. El modo 1, llamado activo-backup: si la primera tarjeta deja de funcionar, la segunda toma el relevo, y viceversa. También se puede definir un intervalo de comprobación, expresado en milisegundos. Modifique la configuración de la agrupación:

```
nmcli con modify bond0  
+bond.options "mode=active-backup,miimon=100"
```

3. Las dos tarjetas eth0 y eth1 formarán parte de la agrupación. Añádalas como esclavas de la agrupación:

```
nmcli con add type ethernet ifname eth0 master bond0  
nmcli con add type ethernet ifname eth1 master bond0
```

4. Active la agrupación con el comando ifup:

```
# ifup bond0
```

5. Verifique el estado del bonding:

```
# cat /proc/net/bonding/bond0
Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: eth0
...

Slave Interface: eth0
MII Status: up
Link Failure Count: 0
Permanent HW addr: xx:xx:xx:xx:xx:xx

Slave Interface: eth1
MII Status: up
Link Failure Count: 0
Permanent HW addr: xx:xx:xx:xx:xx:xx
```

2. Algunos comandos de red

Objetivo: manejar los comandos ping y traceroute para determinar el funcionamiento de la red.

1. Emita un solo ping hacia la dirección que elija; por ejemplo, linuxes.org, y verifique el retorno del comando.

```
# ping -c 1 linuxes.org
PING linuxes.org (172.67.213.170) 56(84) bytes of data.
64 bytes from linuxes4 (172.67.213.170): icmp_seq=1 ttl=59
time=6.43 ms

--- linuxes.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 6.833/6.833/6.833/0.000 ms
# echo $?
0
```

2. El código de retorno 0 indica que la máquina remota ha contestado. Escriba una línea de comandos que permita probar si un servidor contesta y que, en caso contrario, permita salir del programa con un mensaje de error:

```
# ping -c 1 linuxes.org >/dev/null 2>&1 || { echo "El servidor no
responde"; exit 1; }
```

3. Dos servidores de datos están en sitios diferentes. Un servidor cualquiera, esté donde esté, quiere determinar el servidor más cercano para limitar el tráfico de red y el número de pasarelas que debe pasar. Para ello, va a utilizar traceroute y las opciones `-q 1` (una petición por salto) y `-n` (visualización de los "hops" en formato simple).

```
# traceroute -q 1 -n server1
1 10.x.y.247 0.619 ms
2 10.x.y.2 0.956 ms
3 10.x.y.8 1.028 ms
4 172.x.y.101 1.979 ms
```

4. Para determinar el trayecto más corto, basta con contar el número de saltos:

```
S1=$(tracert -q 1 -n $SERVER1 2>/dev/null | wc -l)
S2=$(tracert -q 1 -n $SERVER2 2>/dev/null | wc -l)
```

5. Compare los dos valores y determine el servidor más cercano que hay que configurar en la variable SERVER; para optimizar los accesos habrá que utilizar el servidor en esta variable.

```
[ $SERVER1 -ge $SERVER2 ] && SERVER=$SERVER2 || SERVER=$SERVER1
```

3. El resolver

Objetivo: gestionar la resolución de nombre.

1. Su máquina forma parte de una gran red que dispone de dos servidores de nombres DNS y varios dominios y subdominios declarados. Pertenece al dominio subnet1.slynet.org. Las IP de los servidores DNS son 10.17.23.127 y 10.17.23.247. Construya el archivo /etc/resolv.conf:

```
domain subnet1.slynet.org
nameserver 10.17.23.127
nameserver 10.17.23.247
```

2. Su máquina se llama s14p23 (sala 14, puesto 23). Debe poder acceder mediante su nombre corto (hostname) a todas las máquinas, incluidas las de los otros subdominios. Por ejemplo, s19p01 está en el subdominio subnet2.slynet.org. Modifique /etc/resolv.conf en consecuencia:

```
domain subnet1.slynet.org
search subnet1.slynet.org subnet2.slynet.org
nameserver 10.17.23.127
nameserver 10.17.23.247
```

3. Algunos servicios recuperan el nombre de su máquina mediante una resolución local que pasa por /etc/hosts. Su IP es 10.17.35.168. Ahora bien: en Linux se suele asociar el nombre de anfitrión al localhost 127.0.0.1. Rectifique esto en /etc/hosts:

```
127.0.0.1    localhost
10.17.35.168 s14p23 s14p23.subnet1.slynet.org
```

4. La resolución local pasa primero por /etc/hosts y luego por el DNS. Pero el DNS suele estar más actualizado que /etc/hosts. Modifique el archivo /etc/nsswitch en consecuencia: modifique el orden de la línea hosts:

```
hosts: dns files
```

4. Servicios de red

Objetivo: controlar varios servicios de redes.

1. Quiere saber a qué servicio está asociado el puerto 137. Busque la información en el archivo `/etc/servicios`. Se utiliza este puerto para la resolución de nombres Netbios (Microsoft, Samba).

```
# grep "137/" /etc/servicios
netbios-ns 137/tcp    #NETBIOS Name Service
netbios-ns 137/udp
```

2. Para todas las distribuciones, sin distinción, desactive el servicio `xinetd` `telnet` si está presente. Diríjase a `/etc/xinetd.d`, abra el archivo `telnet` y modifique la línea siguiente:

```
disable = yes
```

Vuelva a iniciar `xinetd` para leer la configuración de nuevo.

3. El servicio `sshd` autoriza la conexión de `root` y quiere evitarlo. Modifique la configuración de `sshd` en consecuencia. El archivo de configuración es `/etc/ssh/sshd_config`.

Modifique el parámetro siguiente:

```
PermitRootLogin no
```

O comente la línea simplemente y vuelva a ejecutar `sshd`.

4. Su máquina dispone de varios programas arrancados que establecen conexiones en red. Una de ellas -no sabe cuál- está conectada al puerto remoto 1863. ¿Cómo encontrar el proceso asociado?

Un método consiste en utilizar netstat para listar las conexiones en curso y los procesos asociados:

```
# netstat -A inet -p -n | grep 1863
tcp    0    0 192.x.y.z 207.46.27.19:1863 ESTABLISHED
10505/kopete
```

Otra solución, que no se ha considerado en el capítulo, es la utilización de lsof con el parámetro `-i`. Ya que todo es archivo, las conexiones de red también:

```
# lsof -i : 1863
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
kopete 10505 seb 15u IPv4 132412 0t0 TCP slyserver:33097
...
```

5. El funcionamiento por defecto del cliente DHCP consiste en sobrescribir el archivo `/etc/resolv.conf` con cada renovación de dirección. El parámetro `-R` lo evita. Según la distribución, puede impedirlo.

Por ejemplo en OpenSUSE, el archivo `/etc/sysconfig/network/dhcp` acepta un parámetro `DHCLIENT_MODIFY_RESOLV_CONF="yes"` o `"no"` para resolver por defecto este caso. Busque en la ayuda de su distribución cómo modificar este tipo de parámetros.

6. La «artimaña» siguiente le explica cómo mandar un correo electrónico desde una conexión telnet hacia un servidor SMTP. Abra una conexión telnet y siga las instrucciones siguientes:

```
# telnet smtp.dominio.net 25
HELO hola
MAIL FROM:joe.dalton@lucky.net
RCPT TO: sheriff@daisytown.net
DATA
subject:Nunca me tendrás

Sherif, nunca cogerás a los Dalton.
.
QUIT
```

5. Archivos compartidos

Objetivo: compartir archivos y directorios mediante NFS y Samba. Se deben instalar e iniciar los servicios NFS y Samba.

1. En su máquina 192.168.1.25 cree un directorio /DATOS que va a compartir tanto mediante NFS como con Samba. Para NFS, modifique el archivo /etc/exports para exportar su contenido para todos los miembros de la subred 192.168.1.0/24 en modo de sólo lectura.

```
# mkdir /DATOS
# vi /etc/exports
```


Añada la línea siguiente:

```
/DATOS 192.168.1.0/255.255.255.0(ro)
```

2. Exporte su recurso. Verifique que el recurso compartido esté correctamente activo.

Ejecute el comando exportfs:

```
# exportfs -av
```

Verifique si el recurso compartido está presente:

```
# showmount -e localhost
```

3. En otra máquina de la subred, monte esta compartición NFS en el directorio /DATOS local y convierta esta modificación en permanente:

```
# mount -t nfs 192.168.1.25:/DATOS /DATOS
```

Añada una línea en /etc/fstab de la manera siguiente:

```
192.168.1.25:/DATOS/DATOSnfsdefaults00
```

4. Exporte /DATOS con Samba, en modo de sólo lectura, únicamente para el usuario joe, con el nombre DATOS. El recurso compartido está oculto. Modifique el archivo /etc/smb/smb.conf así:

```
[DATOS]
comment = Carpeta compartida DATOS
path = /DATOS
browseable = no
public = no
writable = no
printable = no
valid users = joe
```

Pruebe la sintaxis:

```
# testparm
```

Y vuelva a ejecutar Samba.

5. Cree el usuario Samba joe asociado:

```
# smbpasswd -a joe
```

6. Pruebe el recurso compartido con smbclient:

```
# smbclient //192.168.1.25/DATOS -U joe
```