

Laboratorio 7



Apellidos: Moreno Vera

Nombres: Felipe Adrian

Código: 20120354I

Asignatura: Administración de Redes (CC481)

2016 - I

Indice

Actividad 1	(4)
Actividad 2	(14)
Actividad 3	(20)
Actividad 4	(22)
Actividad 5	(24)
Actividad 6	(28)
Actividad 7	(32)

Preámbulo . . .

Debemos preparar nuestras 3 máquinas virtuales, una llamada Router, y otras 2 llamadas Server 1 y Server 2. Todas con interfaz gráfica.



Configuramos según el laboratorio indica ... y comenzamos :D

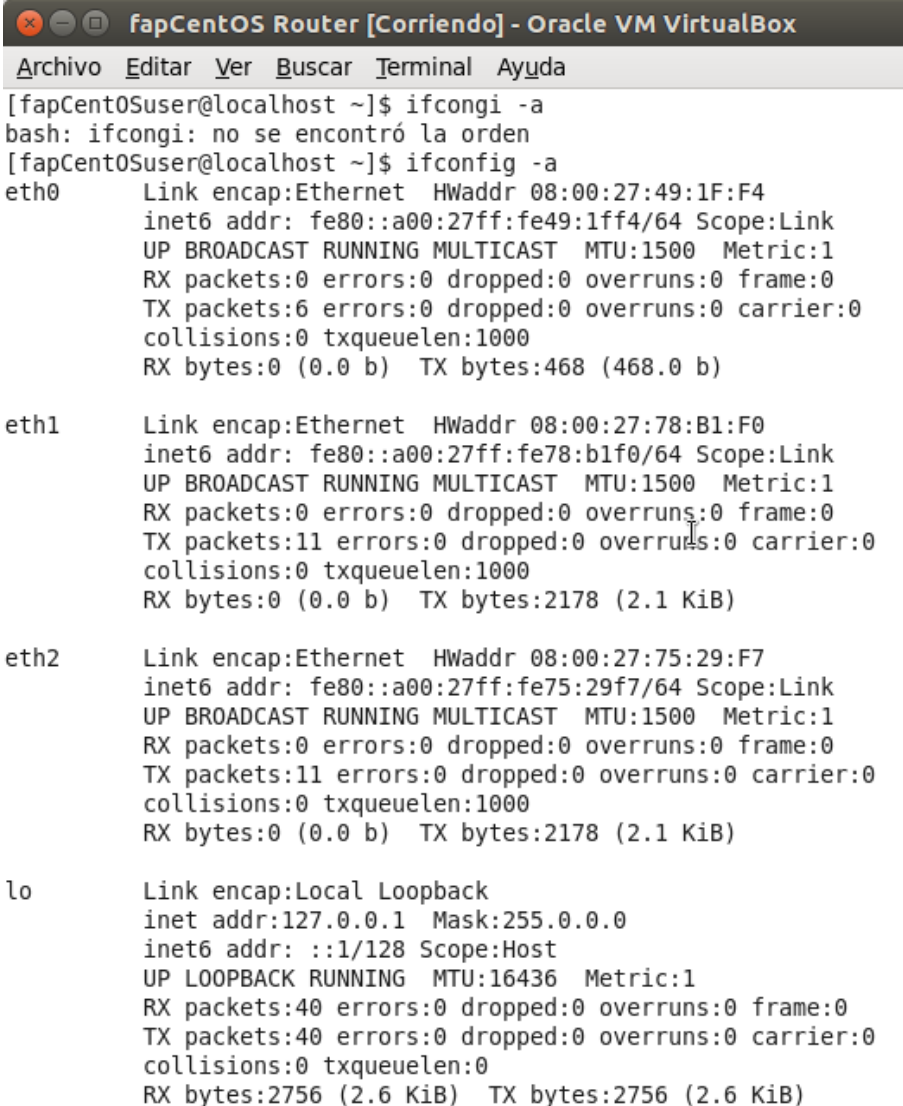
Actividad 1

1. [Router] Ejecutar el comando ifconfig para ver los interfaces del sistema. Este comando sólo muestra los interfaces que están activos (“levantados”-up). Todos los interfaces de red se pueden ver con la opción -a.

NOTA 1: Antes que nada tienes que desactivar conexión automática de cada interfaz si estas en CentOS con entorno gráfico.

NOTA 2: Hay que verificar la MAC desde Configuración de VirtualBox con la de la interfaz de red al hacer ifconfig, teniendo que coincidir el nombre de la red de VirtualBox con la IP asignada a la interfaz de red.

NOTA 3: Es recomendable reiniciar el servicio (sudo service network restart) primero en el servido y luego en las máquinas. Conectar el Router a System eth0



```
fapCentOS Router [Corriendo] - Oracle VM VirtualBox
Archivo Editar Ver Buscar Terminal Ayuda
[fapCentOSuser@localhost ~]$ ifconfigi -a
bash: ifconfigi: no se encontró la orden
[fapCentOSuser@localhost ~]$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:49:1F:F4
          inet6 addr: fe80::a00:27ff:fe49:1ff4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:468 (468.0 b)

eth1      Link encap:Ethernet  HWaddr 08:00:27:78:B1:F0
          inet6 addr: fe80::a00:27ff:fe78:b1f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:2178 (2.1 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:75:29:F7
          inet6 addr: fe80::a00:27ff:fe75:29f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:2178 (2.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2756 (2.6 KiB)  TX bytes:2756 (2.6 KiB)
```

2. [Server1 y Server2] Repetir el ejercicio 1 y comprobar la salida del comando. Desactivar el interfaz con 'ifconfig eth0 down' y comprobar la salida de ifconfig con y sin la opción -a.

```
[fapCent0Suser@localhost ~]$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:F8:D4:DC
          inet6 addr: fe80::a00:27ff:fe8:d4dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1710 (1.6 KiB)  TX bytes:468 (468.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2756 (2.6 KiB)  TX bytes:2756 (2.6 KiB)
```

```
[fapCent0Suser@localhost ~]$ Server 1
```

```
[fapCent0Suser@localhost ~]$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:C6:10:DD
          inet6 addr: fe80::a00:27ff:fec6:10dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:468 (468.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2756 (2.6 KiB)  TX bytes:2756 (2.6 KiB)
```

```
[fapCent0Suser@localhost ~]$ server 2
```

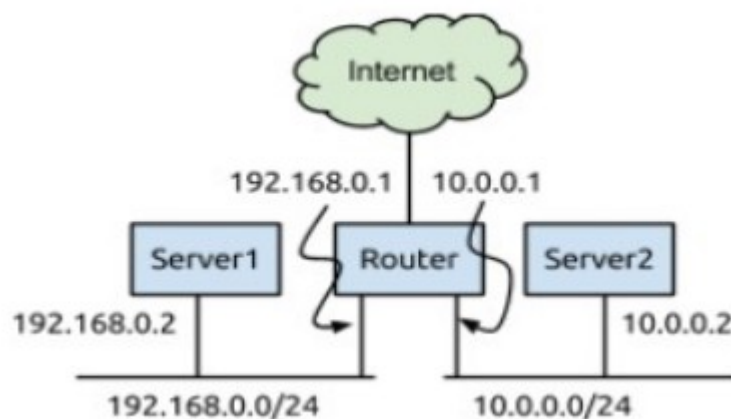
```
[root@localhost fapCent0Suser]# ifconfig eth0 down
[root@localhost fapCent0Suser]# ifconfig
lo                Link encap:Local Loopback
                  inet addr:127.0.0.1  Mask:255.0.0.0
                  inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING  MTU:16436  Metric:1
                  RX packets:40 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:2756 (2.6 KiB)  TX bytes:2756 (2.6 KiB)
```

```
[root@localhost fapCent0Suser]# server 1
```

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost fapCent0Suser]# ifconfig eth0 down
[root@localhost fapCent0Suser]# ifconfig
lo                Link encap:Local Loopback
                  inet addr:127.0.0.1  Mask:255.0.0.0
                  inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING  MTU:16436  Metric:1
                  RX packets:42 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:2860 (2.7 KiB)  TX bytes:2860 (2.7 KiB)
```

```
[root@localhost fapCent0Suser]# Server 2
```

3. [Router] Para configurar la red (asignar direcciones IP, y rutas) usaremos los comandos ifconfig y route. La configuración con los parámetros básicos con ifconfig será: # ifconfig <device> <dirección_ip> netmask <máscara> up



1. Configurar eth0 y eth1 según la topología mostrada en el esquema.

```
[root@localhost fapCent0Suser]# ifconfig eth1 192.168.0.1 netmask 255.255.255.0 up
[root@localhost fapCent0Suser]# ifconfig eth2 10.0.0.1 netmask 255.255.255.0 up
[root@localhost fapCent0Suser]# Router █
```

2. Comprobar los resultados con el comando ifconfig, observar la dirección de broadcast de cada interfaz.

```
[root@localhost fapCent0Suser]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:49:1F:F4
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe49:1ff4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13443 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7283 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10856424 (10.3 MiB)  TX bytes:398720 (389.3 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:78:B1:F0
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:b1f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:11899 (11.6 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:75:29:F7
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe75:29f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:5351 (5.2 KiB)
```


3. Consultar la página de manual para ver otras opciones de ifconfig.

- broadcast [direccion] : asigna la puerta de enlace
- multicast : es una bandera para asignar la puerta de enlace automáticamente
- arp : habilitar el uso del protocolo ARP en esta interface
- promisc : si es habilitado todos los paquetes de la puerta de enlace serán recibidos por el interface

4. [Server1 y Server2] Repetir el ejercicio 2 para cada servidor con las direcciones especificadas.

```
[root@localhost fapCent0Suser]# ifconfig eth0 192.168.0.2 netmask 255.255.255.0 up
[root@localhost fapCent0Suser]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:F8:D4:DC
          inet addr:192.168.0.2  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8:d4dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3420 (3.3 KiB)  TX bytes:2953 (2.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2756 (2.6 KiB)  TX bytes:2756 (2.6 KiB)

[root@localhost fapCent0Suser]# server 1
```

```
[root@localhost fapCent0Suser]# ifconfig eth0 10.0.0.2 netmask 255.255.255.0 up
[root@localhost fapCent0Suser]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:C6:10:DD
          inet addr:10.0.0.2  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:10dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60 (60.0 b)  TX bytes:3064 (2.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2860 (2.7 KiB)  TX bytes:2860 (2.7 KiB)

[root@localhost fapCent0Suser]# Server 2
```


5. [Router, Server1 y Server2] Al configurar la red en un interfaz, automáticamente se añade la ruta para esa red. Las rutas se pueden ver con el comando `route` o con `netstat` (opción `-r` ó `-nr`). Comprobar las rutas en todas las máquinas e interpretar las salidas dadas.

```
[root@localhost fapCentOSuser]# netstat -r
Kernel IP routing table
Destination      Gateway          Genmask          Flags      MSS Window  irtt Iface
10.0.0.0          *                255.255.255.0    U          0 0        0 eth2
10.0.2.0          *                255.255.255.0    U          0 0        0 eth0
192.168.0.0       *                255.255.255.0    U          0 0        0 eth1
default          10.0.2.2         0.0.0.0          UG         0 0        0 eth0
[root@localhost fapCentOSuser]# Router
```

```
[root@localhost fapCentOSuser]# route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.0.0      *                255.255.255.0    U        0      0      0 eth0
[root@localhost fapCentOSuser]# server 1
```

```
[root@localhost fapCentOSuser]# route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
10.0.0.0          *                255.255.255.0    U        0      0      0 eth0
[root@localhost fapCentOSuser]# server 2
```

6. [Router, Server1 y Server2] Una vez configurada la capa de red (nivel 3, IP) debería comprobarse la conectividad a ese nivel con el comando `ping`.

1. Comprobar la conectividad Server1-Router y Server2-Router en ambos extremos.

Server 1 hacia Router:

```
[root@localhost fapCentOSuser]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.441 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.317 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.299 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.320 ms
^C
--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3653ms
rtt min/avg/max/mdev = 0.299/0.344/0.441/0.057 ms
[root@localhost fapCentOSuser]# server1 -> Router
```

Server 2 hacia Router:

```
[root@localhost fapCent0Suser]# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.034 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.251 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.400 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.318 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3198ms
rtt min/avg/max/mdev = 0.034/0.250/0.400/0.137 ms
[root@localhost fapCent0Suser]# server 2 -> router
```

Del Router hacia los servers:

```
[root@localhost fapCent0Suser]# Router -> server 2
bash: Router: no se encontró la orden
[root@localhost fapCent0Suser]#
[root@localhost fapCent0Suser]# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.150 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.311 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.328 ms
^C
--- 10.0.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2796ms
rtt min/avg/max/mdev = 0.150/0.263/0.328/0.080 ms
[root@localhost fapCent0Suser]#
[root@localhost fapCent0Suser]# Router -> server 1
bash: Router: no se encontró la orden
[root@localhost fapCent0Suser]#
[root@localhost fapCent0Suser]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=0.091 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=64 time=0.320 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=64 time=0.320 ms
^C
--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2427ms
rtt min/avg/max/mdev = 0.091/0.243/0.320/0.109 ms
```

2. Estudiar las opciones de ping. Especialmente interesantes son el número de solicitudes echo, el tamaño de los datos enviados y ttl. Especifique dichas opciones.

- a : cada ping hace un sonido
- c [número] : número de veces que se hace solicitudes de ECHO.
- s [número] : especifica el tamaño en bytes de los datos a enviar, el número por defecto es 56 y combinado con la cabecera los datos ICMP hace 64 bytes
- t ttl : tiempo de vida del paquete

7. [Router, Server1] Para establecer la comunicación entre las dos máquinas es necesario disponer de las direcciones físicas. El protocolo ARP realiza esta resolución de direcciones.

1. Después del ping, Router debe tener las direcciones MAC de Server1 y Server2. Averiguar las MAC de ambas con el comando arp. Verificar con la información que muestra ifconfig en Server1 y Server2.

```
[root@localhost fapCentOSuser]# arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.2.2         ether   52:54:00:12:35:02 C              eth0
192.168.0.2      ether   08:00:27:f8:d4:dc C              eth1
10.0.0.2         ether   08:00:27:c6:10:dd C              eth2
[root@localhost fapCentOSuser]# router
```

Si ve los ifconfig del server 1 y server 2 de los ejercicios de arriba, se verificará que son los mostrados.

2. Consultar la página de manual de arp. Estudiar cómo añadir y eliminar entradas manualmente.

Para eliminar se usa: arp -d hostname y para agregar se usar arp -s hostname macAdres

```
[root@localhost fapCentOSuser]# arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.2.3         ether   52:54:00:12:35:03 C              eth0
10.0.2.2         ether   52:54:00:12:35:02 C              eth0
10.0.0.2         ether   08:00:27:c6:10:dd C              eth2
192.168.0.2      ether   08:00:27:f8:d4:dc CM             eth1
[root@localhost fapCentOSuser]# arp -d 192.168.0.2
[root@localhost fapCentOSuser]# arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.2.3         ether   52:54:00:12:35:03 C              eth0
10.0.2.2         ether   52:54:00:12:35:02 C              eth0
10.0.0.2         ether   08:00:27:c6:10:dd C              eth2
192.168.0.2      (incomplete)
[root@localhost fapCentOSuser]# arp -s 192.168.0.2 08:00:27:f8:d4:dc
[root@localhost fapCentOSuser]# arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.2.3         ether   52:54:00:12:35:03 C              eth0
10.0.2.2         ether   52:54:00:12:35:02 C              eth0
10.0.0.2         ether   08:00:27:c6:10:dd C              eth2
192.168.0.2      ether   08:00:27:f8:d4:dc CM             eth1
[root@localhost fapCentOSuser]#
```

8. [Router] Cuando hay problemas de red es necesario depurar la conexión y determinar en que capa se encuentra el problema. Las herramientas anteriores arp y ping son de gran utilidad para determinarlos. Además un monitor de red (sniffer) es de gran utilidad.

1. Eliminar las entradas arp de la tabla en Router.

```
[root@localhost fapCent0Suser]# arp -d 10.0.0.2
[root@localhost fapCent0Suser]# arp -d 192.168.0.2
[root@localhost fapCent0Suser]# arp
```

Address	HWtype	HWaddress	Flags	Mask	Iface
10.0.2.3	ether	52:54:00:12:35:03	C		eth0
10.0.2.2	ether	52:54:00:12:35:02	C		eth0
10.0.0.2		(incomplete)			eth2
192.168.0.2		(incomplete)			eth1

2. En un terminal monitorizar el tráfico del interfaz eth0 (tcpdump -i eth0).

```
[root@localhost fapCent0Suser]# tcpdump -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

No hay comunicación

3. Realizar un ping a Server1 y ver el tráfico (pregunta-respuesta ARP y solicitud-respuesta ICMP-ECHO).

```
[root@localhost fapCent0Suser]# ping 192.168.0.2 -c 4
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=0.109 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=64 time=0.301 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=64 time=0.327 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=64 time=0.275 ms

--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.109/0.253/0.327/0.085 ms
```

Y medimos mientras que desde el server 1 hacemos ping al router.

```
[root@localhost fapCentOSuser]# tcpdump -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
15:35:36.906433 ARP, Request who-has 192.168.0.2 tell 192.168.0.1, length 28
15:35:36.906689 ARP, Reply 192.168.0.2 is-at 08:00:27:f8:d4:dc (oui Unknown), length 46
15:35:36.908534 IP 192.168.0.2 > 192.168.0.1: ICMP echo request, id 40458, seq 6, length 64
15:35:36.908547 IP 192.168.0.1 > 192.168.0.2: ICMP echo reply, id 40458, seq 6, length 64
15:35:37.908346 IP 192.168.0.2 > 192.168.0.1: ICMP echo request, id 40458, seq 7, length 64
15:35:37.908369 IP 192.168.0.1 > 192.168.0.2: ICMP echo reply, id 40458, seq 7, length 64
..
```

4. Consultar la página de manual de tcpdump y estudiar algunas opciones de filtrado, especialmente por protocolo y direcciones de host destino y origen. Muestre y explique dichas salidas.

Capturar el tráfico al puerto telnet o ssh:

```
[root@localhost fapCentOSuser]# tcpdump tcp port 2 and \((port 22 or port 23\)
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
..
```

Capturar paquetes de tipo udp:

```
[root@localhost fapCentOSuser]# tcpdump ip proto \udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
..
```

Capturar paquetes que tengan como origen 192.168.0.2:

```
[root@localhost fapCentOSuser]# tcpdump src host 192.168.0.2 -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
..
```

Capturar paquetes que tengan como destino 10.0.0.2:

```
[root@localhost fapCentOSuser]# tcpdump dst host 10.0.0.2 -i eth2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 65535 bytes
..
```

Actividad 2

1. [Router, Server1 y Server2] La configuración global de la red se configura en `/etc/sysconf/network`, este archivo habilita la red (NETWORKING) y fija el nombre del host. El servicio `network` configura los interfaces de red definidos cuando arranca:

1. [REPASO] Comprobar el servicio `network` con los comandos `chkconfig` y `service` (opción `status`).

```
[root@localhost fapCent0Suser]# service network status
Dispositivos configurados:
lo eth0
Dispositivos activos en el momento:
lo eth0 eth1 eth2
[root@localhost fapCent0Suser]# chkconfig network
[root@localhost fapCent0Suser]# chkconfig --list network
network          0:desactivado  1:desactivado  2:activo        3:activo        4:activo
                  5:activo      6:desactivado
[root@localhost fapCent0Suser]#
[root@localhost fapCent0Suser]# router
```

```
[root@localhost fapCent0Suser]# chkconfig --list network
network          0:desactivado  1:desactivado  2:activo        3:activo        4:activo
                  5:activo      6:desactivado
[root@localhost fapCent0Suser]# service network status
Dispositivos configurados:
lo eth0
Dispositivos activos en el momento:
lo eth0
[root@localhost fapCent0Suser]# server 1
```

```
[root@localhost fapCent0Suser]# chkconfig --list network
network          0:desactivado  1:desactivado  2:activo        3:activo        4:
:activo 5:activo      6:desactivado
[root@localhost fapCent0Suser]# service network status
Dispositivos configurados:
lo eth0
Dispositivos activos en el momento:
lo eth0
[root@localhost fapCent0Suser]# server 2
```


2. El nombre del host no tiene que corresponder con el FQDN. Además se puede cambiar con hostname. Fijar los nombres router, server1, server2 tanto en el archivo /etc/sysconfig/network, como con el comando hostname.

Cambiando el nombre de router:

```
[root@localhost fapCent0Suser]# hostname
localhost.localdomain
[root@localhost fapCent0Suser]# hostname router
[root@localhost fapCent0Suser]# hostname
router
[root@localhost fapCent0Suser]# nano /etc/sysconfig/network
[root@localhost fapCent0Suser]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=router
```

Cambiando el nombre del server1:

```
[root@localhost fapCent0Suser]# hostname
localhost.localdomain
[root@localhost fapCent0Suser]# hostname server1
[root@localhost fapCent0Suser]# hostname
server1
[root@localhost fapCent0Suser]# nano /etc/sysconfig/net
netconsole      network      networking/    network-scripts/
[root@localhost fapCent0Suser]# nano /etc/sysconfig/network
[root@localhost fapCent0Suser]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=server1
[root@localhost fapCent0Suser]# █
```

Cambiando el nombre de server2:

```
[root@localhost fapCent0Suser]# hostname
localhost.localdomain
[root@localhost fapCent0Suser]# hostname server2
[root@localhost fapCent0Suser]# hostname
server2
[root@localhost fapCent0Suser]# nano /etc/sysconfig/network
[root@localhost fapCent0Suser]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=server2
[root@localhost fapCent0Suser]# █
```


2. [Router, Server1 y Server2] La configuración de los interfaces se guarda en /etc/sysconf/network-scripts/ifcfg-<dev>. Esto permite:

1. Usar los comandos ifup/ifdown. Por ejemplo, ifup eth0 aplicaría la configuración de /etc/sysconf/network-scripts/ifcfg-eth0

```
[root@localhost fapCentOSuser]# ifdown eth0
Estado de dispositivo: 3 (desconectado)
[root@localhost fapCentOSuser]# ifup eth0
Estado de conexión activa: activando
Ruta de conexión activa: /org/freedesktop/NetworkManager/ActiveConnection/3
estado: activada
Conexión activada
```

2. Hacer la configuración de red persistente.

La configuración de un interfaz de red en IPv4 puede ser básicamente de dos tipos: DHCP y estática. Ejemplos:

#Configuración DHCP		#Configuración estática
DEVICE=eth0		DEVICE=eth0
BOOTPROTO=dhcp		BOOTPROTO=none
ONBOOT=yes		ONBOOT=yes
		NETWORK=192.168.0.0
		NETMASK=255.255.255.0
		IPADDR=192.168.0.1

1. Configurar los archivos ifcfg-eth0, ifcfg-eth1, ifcfg-eth2 para las máquinas según la sección anterior.

```
[root@router fapCentOSuser]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO="dhcp"
HWADDR="08:00:27:49:1F:F4"
NM_CONTROLLED="yes"
ONBOOT="no"
TYPE="Ethernet"
UUID="10a4ce90-9d85-4f82-9bcc-985c38bc099d"
```

```
[root@router fapCentOSuser]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
NETWORK=192.168.0.0
NETMASK=255.255.255.0
IPADDR=192.168.0.1
HWADDR=08:00:27:78:B1:F0
```

```
[root@router fapCentOSuser]# cat /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.0.0
NETMASK=255.255.255.0
IPADDR=10.0.0.1
HWADDR=08:00:27:75:29:F7
```

server1:

```
[root@localhost fapCentOSuser]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO=none
ONBOOT=yes
NETWORK=192.168.0.0
NETMASK=255.255.255.0
IPADDR=192.168.0.2
HWADDR=08:00:27:F8:D4:DC
```

server2:

```
[root@localhost fapCentOSuser]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.0.0
NETMASK=255.255.255.0
IPADDR=10.0.0.2
HWADDR="08:00:27:C6:10:DD"
```

2. Comprobar la red (ifconfig eth0), “echar abajo” el interfaz (ifdown eth0), comparar la red (ifconfig), “levantar” el interfaz (ifup eth0). Verificar la conectividad en cada caso.

Router: Inicio

```
eth1  Link encap:Ethernet  HWaddr 08:00:27:78:B1:F0
      inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe78:b1f0/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:2098 errors:0 dropped:0 overruns:0 frame:0
      TX packets:2144 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:206930 (202.0 KiB)  TX bytes:213596 (208.5 KiB)

eth2  Link encap:Ethernet  HWaddr 08:00:27:75:29:F7
      inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe75:29f7/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:68 errors:0 dropped:0 overruns:0 frame:0
      TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:10256 (10.0 KiB)  TX bytes:19564 (19.1 KiB)
```

Desactivando las interfaces:

```
[root@router fapCent0Suser]# ifdown eth1
Estado de dispositivo: 3 (desconectado)
[root@router fapCent0Suser]# ifdown eth2
Estado de dispositivo: 3 (desconectado)
```

Verificando las interfaces

```
eth1      Link encap:Ethernet  HWaddr 08:00:27:78:B1:F0
          inet6 addr: fe80::a00:27ff:fe78:b1f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2098 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2145 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:206930 (202.0 KiB)  TX bytes:213650 (208.6 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:75:29:F7
          inet6 addr: fe80::a00:27ff:fe75:29f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:150 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10256 (10.0 KiB)  TX bytes:19672 (19.2 KiB)
```

Activando:

```
[root@router fapCent0Suser]# ifup eth1
Estado de conexión activa: activando
Ruta de conexión activa: /org/freedesktop/NetworkManager/ActiveConnection/19
estado: activada
Conexión activada
[root@router fapCent0Suser]# ifup eth2
Estado de conexión activa: activada
Ruta de conexión activa: /org/freedesktop/NetworkManager/ActiveConnection/20
```

Verificando:

```
eth1      Link encap:Ethernet  HWaddr 08:00:27:78:B1:F0
          inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:b1f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2098 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2144 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:206930 (202.0 KiB)  TX bytes:213596 (208.5 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:75:29:F7
          inet addr:10.0.0.1 Bcast:10.0.0.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe75:29f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10256 (10.0 KiB)  TX bytes:19564 (19.1 KiB)
```

Server1:

```
[root@localhost fapCentOSuser]# ifdown eth0
Estado de dispositivo: 3 (desconectado)
[root@localhost fapCentOSuser]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:F8:D4:DC
          inet6 addr: fe80::a00:27ff:fe8:d4dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2136 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:209382 (204.4 KiB)  TX bytes:210991 (206.0 KiB)

[root@localhost fapCentOSuser]# ifup eth0
Estado de conexión activa: activada
Ruta de conexión activa: /org/freedesktop/NetworkManager/ActiveConnection/3
[root@localhost fapCentOSuser]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:F8:D4:DC
          inet addr:192.168.0.2  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8:d4dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2147 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:209382 (204.4 KiB)  TX bytes:213604 (208.5 KiB)
```

Server2:

```
[root@localhost fapCentOSuser]# ipdown eth0
bash: ipdown: no se encontró la orden
[root@localhost fapCentOSuser]# ifdown eth0
Estado de dispositivo: 3 (desconectado)
[root@localhost fapCentOSuser]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:C6:10:DD
          inet6 addr: fe80::a00:27ff:fec6:10dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19299 (18.8 KiB)  TX bytes:11432 (11.1 KiB)

[root@localhost fapCentOSuser]# ifup eth0
Estado de conexión activa: activada
Ruta de conexión activa: /org/freedesktop/NetworkManager/ActiveConnection/2
[root@localhost fapCentOSuser]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:C6:10:DD
          inet addr:10.0.0.2  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:10dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19299 (18.8 KiB)  TX bytes:14092 (13.7 KiB)
```

3. Los ficheros admiten más opciones, estudiarlas.

DHCP_HOSTNAME: se usa esta opción si el servidor DHCP requiere del cliente su nombre host antes de darle un IP.

HWADDR=<MAC-address>: es la dirección MAC del dispositivo ethernet

MACADDR=<MAC-address>: es la dirección MAC que se sobrescribe al dispositivo

USERCTL=<respuesta> : uno de los siguientes

yes : Usuarios que no son root pueden controlar este dispositivo

no : Solo el usuario root puede controlar este dispositivo

Actividad 3

1. [Router] La resolución de nombres se configura en /etc/resolv.conf.

Este archivo contiene los servidores DNS (nameserver) y el dominio por defecto (search).

1. Consultar el contenido en router.

```
[root@router fapCent0Suser]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 10.0.2.3
```

2. Comprobar el funcionamiento con la orden host (consulta DNS).

Por ejemplo host www.google.com.

```
[root@router fapCent0Suser]# host www.google.com
www.google.com has address 179.6.255.29
www.google.com has address 179.6.255.59
www.google.com has address 179.6.255.54
www.google.com has address 179.6.255.35
www.google.com has address 179.6.255.30
www.google.com has address 179.6.255.50
www.google.com has address 179.6.255.39
www.google.com has address 179.6.255.20
www.google.com has address 179.6.255.34
www.google.com has address 179.6.255.49
www.google.com has address 179.6.255.44
www.google.com has address 179.6.255.55
www.google.com has address 179.6.255.45
www.google.com has address 179.6.255.25
www.google.com has address 179.6.255.24
www.google.com has address 179.6.255.40
www.google.com has IPv6 address 2800:3f0:4005:403::2004
[root@router fapCent0Suser]#
```

3. Añadir el servidor 8.8.8.8, y repetir la consulta.

```
[root@router fapCent0Suser]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 10.0.2.3
nameserver 8.8.8.8
```

Consultando:

```
[root@router fapCent0Suser]# host www.google.com
www.google.com has address 179.6.255.25
www.google.com has address 179.6.255.29
www.google.com has address 179.6.255.50
www.google.com has address 179.6.255.39
www.google.com has address 179.6.255.54
www.google.com has address 179.6.255.24
www.google.com has address 179.6.255.59
www.google.com has address 179.6.255.44
www.google.com has address 179.6.255.55
www.google.com has address 179.6.255.20
www.google.com has address 179.6.255.35
www.google.com has address 179.6.255.45
www.google.com has address 179.6.255.49
www.google.com has address 179.6.255.34
www.google.com has address 179.6.255.30
www.google.com has address 179.6.255.40
www.google.com has IPv6 address 2800:3f0:4005:403::2004
```

2. [Router] No siempre es necesario recurrir a un servidor DNS. El sistema guarda (opcionalmente) una traducción en /etc/hosts, con el formato “dirección nombre1 nombre2...”

1. Añadir al fichero /etc/hosts entradas para cada máquina, ej. 192.168.0.2 server1.

```
[root@router fapCent0Suser]# cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.0.2  server1
10.0.0.2     server2
```


2. Comprobar que ahora es posible hacer ping server1.

```
[root@router fapCent0Suser]# ping server1 -c 3
PING server1 (192.168.0.2) 56(84) bytes of data.
64 bytes from server1 (192.168.0.2): icmp_seq=1 ttl=64 time=0.532 ms
64 bytes from server1 (192.168.0.2): icmp_seq=2 ttl=64 time=0.289 ms
64 bytes from server1 (192.168.0.2): icmp_seq=3 ttl=64 time=0.337 ms

--- server1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.289/0.386/0.532/0.105 ms
[root@router fapCent0Suser]#
```

3. El fichero que determina que servicios usar (DNS o /etc/hosts) es /etc/nsswitch.conf. Examinar su contenido (entrada para hosts).

```
[root@router fapCent0Suser]# cat /etc/nsswitch.conf | grep host
#hosts:      db files nisplus nis dns
hosts:       files dns
```

Opciones:

- nisplus : Usa NIS version 3
- nis : Usa NIS
- dns : Usa DNS
- files : Usa los archivos locales
- db : Usa los archivos base de datos locales
- compat : Usa NIS en modo compatibilidad
- hesiod : usar Hesiod para revisión de usuarios

Actividad 4

1. [Router] La máquina Router tiene conectividad con las redes 10.0.0.0/24 y 192.168.0.0/24 y podría encaminar paquetes de una red a otra usando su tabla de rutas. Simplemente:

1. No debe haber ninguna regla que filtre el tráfico (tabla FORWARD)

iptables -F

```
[root@router fapCent0Suser]# iptables -F
[root@router fapCent0Suser]#
```

2. Activar forwarding para la pila ipv4. # sysctl net.ipv4.conf.all.forwarding=1

NOTA: La configuración puede hacerse permanente en /etc/sysctl.conf

```
[root@router fapCent0Suser]# sysctl net.ipv4.conf.all.forwarding=1
net.ipv4.conf.all.forwarding = 1
```


2. [Server1, Server2] Añadir las ruta para acceder a la otra red en cada uno de los servidores (ej. una ruta a la red 10.0.0.0/24 vía 192.168.0.1 en server1):

1. [Server1, Opción 1] Especificar la ruta explícitamente para esa red.

route add -net 10.0.0.0/24 gw 192.168.0.1

```
[root@server1 fapCentOSuser]# route add -net 10.0.0.0/24 gw 192.168.0.1
[root@server1 fapCentOSuser]# █
```

2. [Server2, Opción 2] Especificar el router como encaminador por defecto.

route add default gw 10.0.0.1

```
[root@server2 fapCentOSuser]# route add default gw 10.0.0.1
[root@server2 fapCentOSuser]# █
```

3. Consultar en ambos casos la tabla de rutas (route y netstat -nr).

```
[root@server1 fapCentOSuser]# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
10.0.0.0         192.168.0.1     255.255.255.0   UG      0      0      0 eth0
192.168.0.0      *               255.255.255.0   U        0      0      0 eth0
link-local       *               255.255.0.0     U       1002    0      0 eth0
[root@server1 fapCentOSuser]# netstat -nr
Kernel IP routing table
Destination      Gateway          Genmask         Flags  MSS Window  irtt Iface
10.0.0.0         192.168.0.1     255.255.255.0   UG      0  0      0 eth0
192.168.0.0      0.0.0.0         255.255.255.0   U        0  0      0 eth0
169.254.0.0      0.0.0.0         255.255.0.0     U        0  0      0 eth0

[root@server2 fapCentOSuser]# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
10.0.0.0         *               255.255.255.0   U      0      0      0 eth0
link-local       *               255.255.0.0     U     1002    0      0 eth0
default          10.0.0.1        0.0.0.0         UG      0      0      0 eth0
[root@server2 fapCentOSuser]# netstat -nr
Kernel IP routing table
Destination      Gateway          Genmask         Flags  MSS Window  irtt Iface
10.0.0.0         0.0.0.0         255.255.255.0   U      0  0      0 eth0
169.254.0.0      0.0.0.0         255.255.0.0     U      0  0      0 eth0
0.0.0.0          10.0.0.1        0.0.0.0         UG      0  0      0 eth0
[root@server2 fapCentOSuser]# █
```

4. Comprobar la conectividad haciendo ping entre los servidores.

Del server 1 al server 2:

```
[root@server1 fapCent0Suser]# ping 10.0.0.2 -c 3
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=63 time=1.23 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=63 time=0.584 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=63 time=0.556 ms

--- 10.0.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.556/0.791/1.234/0.314 ms
[root@server1 fapCent0Suser]# █
```

Del server 2 al server 1:

```
[root@server2 fapCent0Suser]# ping 192.168.0.2 -c 3
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=63 time=1.11 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=63 time=0.578 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=63 time=0.436 ms

--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.436/0.709/1.113/0.291 ms
[root@server2 fapCent0Suser]# █
```

Actividad 5

1. [Router] El protocolo DHCP permite configurar la red de un host, incluyendo direcciones IP o servidores DNS, entre otros parámetros. Vamos a configurar el servicio dnsmasq, que además de servidor DHCP implementa un proxy DNS.

1. El servicio se configura en /etc/dnsmasq.conf. Estudiar los comentarios referidos a dhcp.

no-dhcp-interface=* : deshabilita dhcp en la interface especificada

dhcp-range=[dir1],[dir2],[tiempo]: el servidor dns otorga una direccion entre dir1 y dir2, y la otorga por un tiempo especificado en [tiempo].

dhcp-host=[mac],[dir] : otorga a la maquina con [mac] la direccion [dir].

dhcp-host=[mac],ignore : no ofrece el servicio dhcp a la maquina con [mac]

dhcp-ignore=#known : ignora a los clientes especificados en dhcp-host

dhcp-vendorclass=red,Linux : envia opciones especiales con la etiqueta red a los host linux

dhcp-userclass=red,accounts :

dhcp-mac=red,11:22:33:*.:* : envia opciones especiales con la etiqueta red a los host con mac que corresponda al patron.

2. Configurar dhcp para las dos redes con dhcp-range. Escoger un rango y tiempo de lease para cada uno (ej. dhcp-range=192.168.0.100,192.168.0.150,12h).

```
# Uncomment this to enable the integrated DHCP server, you need to
# supply the range of addresses available for lease and optionally
# a lease time. If you have more than one network, you will need to
# repeat this for each network on which you want to supply DHCP
# service.
#dhcp-range=192.168.0.50,192.168.0.150,12h
dhcp-range=192.168.0.100,192.168.0.150,12h

# This is an example of a DHCP range where the netmask is given
# is needed for networks we reach the dnsmasq DHCP server via a
# agent. If you don't know what a DHCP relay agent is, you probably
# don't need to worry about this.
#dhcp-range=192.168.0.50,192.168.0.150,255.255.255.0,12h

# This is an example of a DHCP range with a network-id, so that the
# Nombre del fichero a escribir: /etc/dnsmasq.conf
```

3. Reiniciar el servicio dnsmasq (usando el comando service).

```
[root@router fapCent0Suser]# service dnsmasq restart
dnsdomainname: `Host' desconocido
dnsdomainname: `Host' desconocido
Shutting down dnsmasq: [ OK ]
dnsdomainname: `Host' desconocido
Starting dnsmasq: [ OK ]
[root@router fapCent0Suser]#
```

2. [Server1 y Server2] Desactivar los interfaces y configurarlos con la orden (dhclient -v eth0).

```
[root@server1 fapCentOSuser]# ifdown eth0
Estado de dispositivo: 3 (desconectado)
[root@server1 fapCentOSuser]# dhclient -v eth0
Internet Systems Consortium DHCP Client 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:f8:d4:dc
Sending on   LPF/eth0/08:00:27:f8:d4:dc
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5 (xid=0x23alce2a)
DHCPOFFER from 192.168.0.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67 (xid=0x23alce2a)
DHCPACK from 192.168.0.1 (xid=0x23alce2a)
bound to 192.168.0.82 -- renewal in 18521 seconds.
[root@server1 fapCentOSuser]# █
```

```
[root@server2 fapCentOSuser]# ifdown eth0
Estado de dispositivo: 3 (desconectado)
[root@server2 fapCentOSuser]# dhclient -v eth0
Internet Systems Consortium DHCP Client 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:c6:10:dd
Sending on   LPF/eth0/08:00:27:c6:10:dd
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6 (xid=0x7ba9acc1)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 14 (xid=0x7ba9acc1)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 14 (xid=0x7ba9acc1)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 9 (xid=0x7ba9acc1)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 15 (xid=0x7ba9acc1)
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3 (xid=0x7ba9acc1)
No DHCPOFFERS received.
No working leases in persistent database - sleeping.
```

3. [Server1] Cambiar la configuración ifcfg-eth0 para que use dhcp y probarla con ifdown/ifup.

```
[root@server1 fapCentOSuser]#  
[root@server1 fapCentOSuser]# cat /etc/sysconfig/network-scripts/ifcfg-eth0  
ad  
DEVICE="eth0"  
#BOOTPROTO=none  
BOOTPROTO=dhcp  
ONBOOT=yes  
#NETWORK=192.168.0.0  
#NETMASK=255.255.255.0  
#IPADDR=192.168.0.2  
HWADDR=08:00:27:F8:D4:DC  
  
[root@server1 fapCentOSuser]# ifdown eth0  
Estado de dispositivo: 3 (desconectado)  
[root@server1 fapCentOSuser]# ifup eth0  
Estado de conexión activa: activando  
Ruta de conexión activa: /org/freedesktop/NetworkManager/ActiveConnection/2  
estado: activando  
estado: activada  
Conexión activada  
[root@server1 fapCentOSuser]# ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:F8:D4:DC  
          inet addr:192.168.0.82  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fef8:d4dc/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:2120 (2.0 KiB)  TX bytes:17735 (17.3 KiB)
```

4. [Server2] También funcionará el proxy DNS, se puede ver la traducción con por ejemplo ping www.google.com, aunque no se recibirá respuesta.

```
[root@server2 fapCentOSuser]# ping 8.8.8.8 -c 5  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
  
--- 8.8.8.8 ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 14000ms  
  
[root@server2 fapCentOSuser]#
```

Se ve que no recibe paquetes de retorno.

Actividad 6

1. [Router] Comprobar las estadísticas de cada interfaz con ifconfig, comprobar los bytes transmitidos y recibidos en cada caso.

```
[root@router fapCentOSuser]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:49:1F:F4
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe49:1ff4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:386 errors:0 dropped:0 overruns:0 frame:0
          TX packets:294 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:111630 (109.0 KiB)  TX bytes:23727 (23.1 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:78:B1:F0
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:b1f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:267 errors:0 dropped:0 overruns:0 frame:0
          TX packets:178 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39819 (38.8 KiB)  TX bytes:16119 (15.7 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:75:29:F7
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe75:29f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:561 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:105963 (103.4 KiB)  TX bytes:17892 (17.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
```

En el server 1 (eth1) se recibieron 39819 Kb y se transmitió 16119 Kb.

En el server 2 (eth2) se recibieron 105963 Kb y se transmitió 17892 Kb.

2. [Router] Los procesos que están escuchando en el sistema se pueden ver con netstat (opción -ta para TCP o -ua para UCP) o con lsof -i. Establecer qué procesos en el sistema tienen puertos abiertos y las conexiones establecidas.

```
[root@router fapCentOSuser]# netstat -ta
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         Stat
e
tcp        0      0 *:sunrpc                *:*                     LIST
EN
tcp        0      0 *:domain                *:*                     LIST
EN
tcp        0      0 *:ssh                   *:*                     LIST
EN
tcp        0      0 localhost:ipp           *:*                     LIST
EN
tcp        0      0 localhost:smtp          *:*                     LIST
EN
tcp        0      0 *:35869                 *:*                     LIST
EN
tcp        0      0 10.0.2.15:49385         179.6.254.153:http      ESTA
BLISHED
tcp        0      0 *:48033                 *:*                     LIST
EN
tcp        0      0 *:sunrpc                *:*                     LIST
EN
tcp        0      0 *:domain                *:*                     LIST
EN
tcp        0      0 *:ssh                   *:*                     LIST
EN
tcp        0      0 localhost:ipp           *:*                     LIST
EN
tcp        0      0 localhost:smtp          *:*                     LIST
EN
```

Todo proceso TCP esta en estado de Listener


```
[root@router fapCent0Suser]# netstat -ua
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp      0      0 *:netconfsoapbeep      *:.*
udp      0      0 *:bootps                *:.*
udp      0      0 *:bootpc                *:.*
udp      0      0 *:mdns                  *:.*
udp      0      0 *:sunrpc                 *:.*
udp      0      0 *:ipp                   *:.*
udp      0      0 *:42105                 *:.*
udp      0      0 *:50354                 *:.*
udp      0      0 *:domain                *:.*
udp      0      0 *:connendp              *:.*
udp      0      0 *:sunrpc                 *:.*
udp      0      0 *:domain                *:.*
udp      0      0 *:connendp              *:.*
udp      0      0 *:57015                 *:.*
```

```
[root@router fapCent0Suser]# lsof -i | tail
sshd      1705      root    4u  IPv6  12820      0t0  TCP *:ssh (LISTEN)
master    1785      root    12u IPv4  13156      0t0  TCP localhost:smtp (LISTEN)
master    1785      root    13u IPv6  13158      0t0  TCP localhost:smtp (LISTEN)
clock-app 2457 fapCent0Suser 21u IPv4  28035      0t0  TCP 10.0.2.15:49385->179.6.254.153:http (ESTABLISHED)
dhclient  2672      root     6u  IPv4  25001      0t0  UDP *:bootpc
dnsmasq   3461     nobody   5u  IPv4  27845      0t0  UDP *:bootps
dnsmasq   3461     nobody   6u  IPv4  27854      0t0  UDP *:domain
dnsmasq   3461     nobody   7u  IPv4  27855      0t0  TCP *:domain (LISTEN)
dnsmasq   3461     nobody   8u  IPv6  27856      0t0  UDP *:domain
dnsmasq   3461     nobody   9u  IPv6  27857      0t0  TCP *:domain (LISTEN)
```

Se observa que el proceso(servicio) dnsmasq con pid 3461 esta activo.

3. [Router] Los números de puerto bien conocidos están definidos en /etc/services. Comprobar las correspondencia usando la opción -n de netstat (-tan).

```
[root@router fapCent0Suser]# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         Stat
e
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
EN
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN
EN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
EN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
EN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
EN
tcp        0      0 0.0.0.0:35869           0.0.0.0:*               LISTEN
EN
tcp        0      0 10.0.2.15:49385         179.6.254.153:80        ESTABLISHED
BLISHED
tcp        0      0 :::48033                 :::*                     LISTEN
EN
tcp        0      0 :::111                   :::*                     LISTEN
EN
tcp        0      0 :::53                    :::*                     LISTEN
EN
tcp        0      0 :::22                    :::*                     LISTEN
EN
tcp        0      0 :::1:631                 :::*                     LISTEN
EN
tcp        0      0 :::1:25                  :::*                     LISTEN
EN
-
[root@router fapCent0Suser]# cat /etc/services | grep 48033/tcp | head -n 1
[root@router fapCent0Suser]# cat /etc/services | grep 111/tcp | head -n 2
sunrpc      111/tcp          portmapper rpcbind    # RPC 4.0 portmapper TCP
lmsocialserver 1111/tcp        # LM Social Server
[root@router fapCent0Suser]# cat /etc/services | grep 53/tcp | head -n 2
domain      53/tcp           # name-domain server
knetd       2053/tcp         lot105-ds-upd         # Kerberos de-multiplexor
[root@router fapCent0Suser]# cat /etc/services | grep 22/tcp | head -n 2
ssh         22/tcp           # The Secure Shell (SSH) Protocol
l
bpjava-msvc 13722/tcp        # BP Java MSVC Protocol
[root@router fapCent0Suser]# cat /etc/services | grep 631/tcp | head -n 2
ipp         631/tcp          # Internet Printing Protocol
visitview   1631/tcp         # Visit view
[root@router fapCent0Suser]# cat /etc/services | grep 25/tcp | head -n 2
smtp        25/tcp           mail
timed       525/tcp          timeserver
[root@router fapCent0Suser]# █
```

El proceso dnsmasq está usando el puerto 53 como se puede observar en /etc/services que explica que el puerto 53 es usado por el servidor de nombre de dominios.

El puerto 22 de tcp indica que se usa para el servidor ssh y el puerto 25 de tcp es para el servidor de correos.

Actividad 7

1. [Router] Comprobar que está en ejecución sshd y determinar en qué puerto escucha el servicio.

En la actividad anterior ejercicio ultimo, se observa que el puerto 22 está siendo usado por el servidor ssh(sshd).

2. [Router] Acceder a Server1 como root (ssh root@server1).

Como server 1 esta como dhcp, ya no podemos hacer [root@server1](#), pues lo habiamos agregado como 192.168.0.2, pero ahora tiene ip 192.168.0.139.

```
[root@router fapCent0Suser]# ssh root@192.168.0.139
The authenticity of host '192.168.0.139 (192.168.0.139)' can't be established.
RSA key fingerprint is f1:35:fa:b5:93:0f:e4:54:15:ca:ad:31:4c:51:a4:ca.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.139' (RSA) to the list of known hosts.
root@192.168.0.139's password:
[root@server1 ~]# █
```

3. [Router] Copia segura de ficheros. Copiar el fichero /etc/passwd a Server1 (scp/etc/passwd root@server1:/tmp/copia_passwd). Observar la sintaxis y comprobar que la copia se ha realizado correctamente.

Haciendo copia de seguridad desde el router:

```
[root@router fapCent0Suser]# scp /etc/passwd root@192.168.0.139:/tmp/copia_passwd
root@192.168.0.139's password:
passwd                               100% 1720      1.7KB/s   00:00
[root@router fapCent0Suser]# █
```

Verificando la transferencia de datos en server 1:

```
[root@server1 fapCent0Suser]# cat /tmp/copia_passwd | head -n 5
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

4. [Router] Autenticación con par de claves pública/privada:

1. Generar el par de claves con ssh-keygen. (no encriptar la clave privada).

```
[root@router fapCentOSuser]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
48:d6:45:9e:53:e5:1d:06:4f:5f:f0:ff:31:08:c1 root@router
The key's randomart image is:
+--[ RSA 2048 ]-----+
|      .+.00+*0|
|      . + E..+0=|
|      0 . +. .|=|
|      0 . . . .|
|      . S . 0.|
|                  +|
|                  .|
+-----+

```

2. Copiar la clave pública a Server1 (ssh-copy-id -i .ssh/id_rsa.pub root@server1).

```
[root@router ~]# ssh-copy-id -i .ssh/id_rsa.pub root@192.168.0.139
root@192.168.0.139's password:
Now try logging into the machine, with "ssh 'root@192.168.0.139'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

3. Entrar en Server1 como root (no pedirá clave). Ver los contenidos de .ssh/authorized_keys en Server1, contiene los contenidos de id_rsa.pub.

Ya no pide clave de acceso.

```
[root@router ~]# ssh root@192.168.0.139
Last login: Sun Feb 14 19:39:24 2016 from 192.168.0.1
[root@server1 ~]# █
```

Verificando que sean iguales:

```
[root@server1 ~]# cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA1Djxst7S8SZdJ7BlJ0w9r47PX2gq61da0K/9Ty6HmkbRzvC
z+ewlwRQH1WwvXk+LnLYKeHdxQcYqYqLxhDf1ke00/D1Cifodea+JapRumafnlQ0ieluvlD0BU6/KVK6MQ7
lf/F4/FJCH0S7K/ek1ZBYe9L4n/SSsRo+t5smypWJSj9TQ3x40D55aUeQGAdUwkkUxyN0XntFa1D3wW0NgL
5ISbw74dnpNXmmUYqMXML54ndE4iVAjC93JTyGF62EQH29MaNmqr30qHuv09APN8q0cQuDNCg8ivggNubQV
9t1A+st4Yy1lTNJ9WR/fm8okT53j33aEJ05AEtBJxQTT6Q== root@router
[root@server1 ~]# exit
logout
Connection to 192.168.0.139 closed.
[root@router ~]# cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA1Djxst7S8SZdJ7BlJ0w9r47PX2gq61da0K/9Ty6HmkbRzvC
z+ewlwRQH1WwvXk+LnLYKeHdxQcYqYqLxhDf1ke00/D1Cifodea+JapRumafnlQ0ieluvlD0BU6/KVK6MQ7
lf/F4/FJCH0S7K/ek1ZBYe9L4n/SSsRo+t5smypWJSj9TQ3x40D55aUeQGAdUwkkUxyN0XntFa1D3wW0NgL
5ISbw74dnpNXmmUYqMXML54ndE4iVAjC93JTyGF62EQH29MaNmqr30qHuv09APN8q0cQuDNCg8ivggNubQV
9t1A+st4Yy1lTNJ9WR/fm8okT53j33aEJ05AEtBJxQTT6Q== root@router
[root@router ~]# █
```

4. Observar los permisos del directorio .ssh y sus contenidos.

```
[root@router ~]# ls -la .ssh
total 20
drwx-----. 2 root root 4096 feb 14 19:55 .
dr-xr-x---. 8 root root 4096 feb 14 19:42 ..
-rw-----. 1 root root 1675 feb 14 19:55 id_rsa
-rw-r--r--. 1 root root 393 feb 14 19:55 id_rsa.pub
-rw-r--r--. 1 root root 395 feb 14 19:42 known_hosts
[root@router ~]# █
```

id_rsa.pub

```
[root@router ~]# cat -v .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA1Djxst7S8SZdJ7BlJ0w9r47PX2gq61da0K/9Ty6HmkbRzvC
z+ewlwRQH1WwvXk+LnLYKeHdxQcYqYqLxhDf1ke00/D1Cifodea+JapRumafnlQ0ieluvlD0BU6/KVK6MQ7
lf/F4/FJCH0S7K/ek1ZBYe9L4n/SSsRo+t5smypWJSj9TQ3x40D55aUeQGAdUwkkUxyN0XntFa1D3wW0NgL
5ISbw74dnpNXmmUYqMXML54ndE4iVAjC93JTyGF62EQH29MaNmqr30qHuv09APN8q0cQuDNCg8ivggNubQV
9t1A+st4Yy1lTNJ9WR/fm8okT53j33aEJ05AEtBJxQTT6Q== root@router
[root@router ~]# █
```

known_hosts

```
192.168.0.139 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA3eA4Z5dVmtxFrN8QlZSBKGIexhYVeVHPY
rkJNGmY8cCanCbeYr2WQ3krFKpJQ+/Fap5YY5dfiUK7Wc5iE/YBaad6dR2qb25Z8w+1uzfs5nRpIm8kjWJ
3uJv17P0lgXRcLCnaHo8vxAmg2Uqr2a/C62lehr0YhIw+ZTr2IVfjztLYIMTmAYvcHQb5ePADTw/Fn0Trin
BRrtgQr7jESa+li+BqTXSPWJWZpXqkecVq0yixzdl+wj6nTzmvnq6pyGExabXpG+Gtz8TB2nd2lZZevJRYR
i1IXe+f6R20J8iqjgSu20jRSkyYyqzSFIIfQuPlw48xhrrsbMNRw0aQSl3m0w==
[root@router ~]# █
```

id_rsa.pub

```
[root@router ~]# cat -v .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA1Djxst7S8SZdJ7BlJ0w9r47PX2gq61da0K/9Ty6HmkbRzvCz
+ewlwRQH1WwvXk+LnLYKeHdxQcYqQyLxhDf1ke00/D1Cifodea+JapRumafnlQ0i
eluvlD0BU6/KVK6MQ7lf/F4/FJCH0S7K/ek1ZBYe9L4n/SSsRo+t5smyPwJSj9TQ
3x40D55aUeQGADuWkkUxyN0XntFa1D3wW0NgL5ISbW74dnpNXmmUYqMXML54ndE4
iVAjC93JTyGF62EQH29MaNmqr30qHuv09APN8q0cQuDNCg8ivggNubQV9t1A+st4
Yy1lTNJ9WR/fm8okT53j33aEJ05AEtBJxQTT6QIBIwKCAQEAyBhu29lnzW1QhIG+
dYJmC+0MqmmHjW+exMMwqb4oFR4ziJn0Q2mvBoCZq/hJ6zU0nJpEYvRGNrOG7tfn
xc5ckN3elg3fpgn+iKzSBWdg90aJ5EVBBa1Nxbj8wyz9YXniwIppjW2AEW54D1Fa/G
t0MyVw2K5sHrMIGpvt89kHUHJXWAW7MOAMyhtQcd/dawFJZJRA1pj6ZXpKorclDg
xz49vMWHuv94S0mP01h+TXoNTKzEE5530a7Lg5NWBf0YvDRhjp1VZQA+8gqQ0yXo
yuo3V6CKm40mk3+4jgXCd9QJPslQBd+0PlfHgQ0ySIUvXzTG0072h9uARfnrlpPA
timQuwKBgQDqqFKhQYD04Gx0vQWhNsFlur4dNJAZzVVX8eCBtMDGnwFhUzAz6bQ
LSmeKQuMnux1C5y1kGCqLuyVRsnMcDfw2kw9tnyoWa0/qBwa3DKAhS0e7LVuweU0
iPCLa6RAqK+kiNq9I/EF1dNGPMwRiNxdScYMVr0irolLak+tQA7LQKBgQDnhkBM
lQJGiCpZK04y0SV275firl5n1U0mQUW2iv+d51d1MVFTN/ITMhCmkhYXnZbmCQiP
hyaRf/AW2z4XfT8+aBYVGLIU6H7k4sVE8wdv0oBikjMh+U1ItbwRJE36C5Yoir3P
DKE2iVCgz2l1CwsfhfxCVFHJg0gqxSKUAURBLQKBgFcoK7g85sFaq/DYfm8UvNyx
ay9rS4D0fsjkz7sl4TPurLGX6U7uCsJZ6uL5TW6+r5kwMuRaMohakmNUzpxkMf9Y
YwvzUt9xwHpjALXcwKz+Q/WLHtFd9f4Vmyx4cDVF+BiKmmOCYNZIG0X5Uxx0qaAr
g4ykniBQyMhDjme/kl8fAoGAfa9HiCUBPDtKMGePBVI46Ms1Memg9om3Ans0eQmg
tm4K59jxojRQnk5gz3PgG3L0Qlys4DNstWK1iMapBW/ggPas5uGFPozXK8uPqRY3
PLQZzxwqYuZryGKn7Axk2DIs8W/jYcUHDvoV06PLiK45PP+Xkbi+rzdzdk3CUFh1
gncCgYEAirJNPlr7PSXEQIm1DviE0oMYC/teLJf4RdrVtJUSe+lvP5nIjUFRnfu+
l4K05EDk6t2HwGSvIMYU4LfsW3/r03BS9AXjTCmWx/Lsm0Y+KC0dAjH+1WUGCThD
5Mrkgba1PZE+BQGxkXyPlDay06QTHn3ZZvCEtBAvuuhJEQffF90=
-----END RSA PRIVATE KEY-----
```

5. Comprobar la conexiones con lsof o netstat.

```
[root@router ~]# lsof -i | tail -n 15
rpc.statd 1505      rpcuser  11u  IPv6  11908      0t0  TCP *:48033 (LISTEN)
cupsd    1580      root    6u   IPv6  12223      0t0  TCP localhost:ipp (LISTEN)
)
cupsd    1580      root    7u   IPv4  12224      0t0  TCP localhost:ipp (LISTEN)
)
cupsd    1580      root    9u   IPv4  12227      0t0  UDP *:ipp
sshd     1705      root    3u   IPv4  12818      0t0  TCP *:ssh (LISTEN)
sshd     1705      root    4u   IPv6  12820      0t0  TCP *:ssh (LISTEN)
master   1785      root    12u  IPv4  13156      0t0  TCP localhost:smtp (LISTEN)
)
master   1785      root    13u  IPv6  13158      0t0  TCP localhost:smtp (LISTEN)
)
clock-app 2457 fapCentOSuser 21u  IPv4  30179      0t0  TCP 10.0.2.15:49391->179.
6.254.153:http (ESTABLISHED)
dhclient 2672      root    6u   IPv4  25001      0t0  UDP *:bootpc
dnsmasq  3461      nobody  5u   IPv4  27845      0t0  UDP *:bootps
dnsmasq  3461      nobody  6u   IPv4  27854      0t0  UDP *:domain
dnsmasq  3461      nobody  7u   IPv4  27855      0t0  TCP *:domain (LISTEN)
dnsmasq  3461      nobody  8u   IPv6  27856      0t0  UDP *:domain
dnsmasq  3461      nobody  9u   IPv6  27857      0t0  TCP *:domain (LISTEN)
```


5. [Server1] El servidor ssh dispone de múltiples opciones para ajustar su funcionamiento.

1. Estudiar el fichero /etc/ssh/sshd_config

```
# Host *
# ForwardAgent no
# ForwardX11 no
# RhostsRSAAuthentication no
# RSAAuthentication yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/identity
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# Port 22
# Protocol 2,1
# Cipher 3des
# Ciphers aes128-ctr,aes192-ctr,aes256
cbc
# MACs hmac-md5,hmac-sha1,umac-64@open
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Port: es el puerto en el que escucha conexiones entrantes.

ListenAddress: son las direcciones de los host permitidos para realizar conexión.


```
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

MaxAuthTries: Es el número de intentos máximos para logear

MaxSessions: Es el número maximo de conexiones establecidas a la vez en el servidor.

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes
```

PasswordAuthenticacion: se asigna 'yes' si queremos que el servidor exija contraseñas. 'no' si no queremos.

2. Deshabilitar el login como root

```
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin yes
PermitRootLogin no

^G Ver ayuda ^O Guardar ^R !
^X Salir ^J Justificar ^W !
```

Basta darle no a PermitRootLogin

3. Reiniciar el servidor

```
[root@server1 ~]# nano /etc/ssh/sshd_config
[root@server1 ~]# service sshd restart
Parando sshd: [ OK ]
Iniciando sshd: [ OK ]
[root@server1 ~]# █
```

4. Verificar el funcionamiento de la nueva configuración

Vemos desde el router:

```
[root@router ~]# ssh root@192.168.0.139
root@192.168.0.139's password:
Permission denied, please try again.
```

Nos deniega el permiso, intentaremos con el usuario fapCentOSuser

```
[root@router ~]# ssh fapCentOSuser@192.168.0.139
fapCentOSuser@192.168.0.139's password:
[fapCentOSuser@server1 ~]$ █
```

Y observamos que podemos ingresar con el usuario, mas no como root.

Referencias:

https://es.wikipedia.org/wiki/Protocolo_de_resoluci%C3%B3n_de_direcciones
<http://www.tuxylinux.com/editar-la-tabla-arp/>
<http://www.rationallyparanoid.com/articles/tcpdump.html>
https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-networkscripts-interfaces.html
<http://man7.org/linux/man-pages/man5/nsswitch.conf.5.html>
<http://xmodulo.com/how-to-set-up-dhcp-server-using-dnsmasq.html>
http://www.techotopia.com/index.php/Configuring_CentOS_6_Remote_Access_using_SSH