

Práctica 1

Asignatura: Administración de sistemas 2

Fecha: 1/3/2020

Autor: Diego Marco Beisty, 755232

RESUMEN

En esta primera práctica de la asignatura se han puesto en marcha 2 máquinas virtuales sobre la red. Se les han asignado direcciones IPv6 públicas y se ha configurado una de ellas como router. Para administrar las VMs, se ha trabajado en el entorno libvirt haciendo uso de herramientas como virsh y virt-manager.

INTRODUCCIÓN

Como primera aproximación a la administración de máquinas virtuales en red, se van a configurar las MVs orouter1 y o1ff2 conectándolas a dos subredes IPv6.

La MV llamada orouter1 se va a configurar como router. Para ello se va a asociar su interfaz vio0 a la subred exterior `2001:470:736b:f000`, que conecta a internet mediante el encaminador Central.

Además se asociará una interfaz vlan (vlan199), creada sobre vio0 a una subred interior `2001:470:736b:1ff`.

La MV llamada o1ff2 se conectará a la subred `2001:470:736b:1ff` activando la tarjeta vio0 y asociando una tarjeta vlan a esta subred interior.

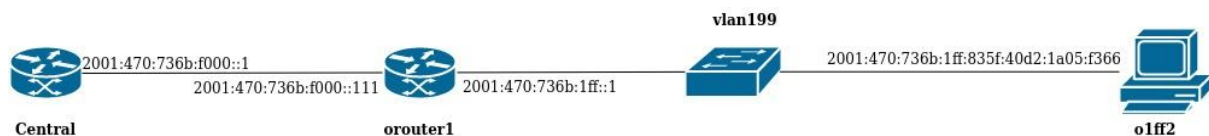
La configuración completa del sistema se detalla más adelante en el apartado [DESARROLLO DEL SISTEMA](#).

OBJETIVOS

Los principales objetivos de esta práctica son:

- 1) Configuración de entorno de virtualización distribuido (libvirt con kvm)
- 2) Conexión de máquinas a redes IPv6
- 3) Manejo de redes vlan
- 4) Configuración sobre S.O openBSD

ARQUITECTURA Y ELEMENTOS RELEVANTES



En el diagrama quedan representados de izquierda a derecha los siguientes elementos.

- El router Central que conecta las MVs a internet.
- Orouter1, que está conectado a la subred 2001:470:736b:f000 con Central, y a la subred 2001:470:736b:1ff con o1ff2 mediante la vlan199, reconocida por el switch que interconecta a ambas MVs.
- o1ff2 que está conectado a la vlan 199 en la subred interior 2001:470:736b:1ff

ELEMENTOS SIGNIFICATIVOS DE LA PRÁCTICA

Subredes IP implicadas:

- Subred exterior que comunica con internet mediante el encaminador Central:
2001:470:736b:f000::/64
- Subred interior vlan que comunica el router orouter1 con o1ff2:
2001:470:736b:1ff::/64

VLANS implicadas:

En orouter1 se define una interfaz virtual vlan (vlan 199) que conecta mediante un switch virtual con el interfaz virtual de la máquina o1ff2.

Una vlan es una solución software de la capa de enlace que permite segmentar varias redes lógicas sobre una misma red física. Esto es posible añadiendo un campo en la trama ethernet que indica el número de vlan al que está asociado el host origen de la trama y mediante el uso de switches inteligentes que son capaces

de recordar y dirigir el tráfico de tramas según la vlan asociada. Permitiendo así que por ejemplo un mensaje broadcast no llegue a todos los host conectados físicamente a la red mediante un switch si no que solo llegue a los host conectados lógicamente a la misma red vlan.

En la práctica y concretamente en openBSD, una vlan se configura activando una tarjeta física y creando una tarjeta virtual a partir de ella en la que se indica el número de vlan y la dirección IP asociada a la tarjeta.

Routers implicados:

- Router Central
`2001:470:736b:f000::1`
- Router orouter1
`2001:470:736b:f000::111`

Encaminadores por defecto utilizados:

- MV orouter1, por defecto router Central
`2001:470:736b:f000::1`
- MV o1ff2, por defecto router orouter1
`2001:470:736b:1ff::1`

¿Qué ocurre si introducimos “inet6 autoconf” en el fichero “hostname.vio0” de la máquina interna de prueba y por qué?

El interfaz vio0 de o1ff2 se autoconfigura con el prefijo de subred servido por orouter1 (rad), `2001:470:736b:f000::/64` correspondiente a la subred externa.

El interfaz vlan199 se queda sin poder autoconfigurar ninguna ip.

Esto se produce porque el servicio rad solo es atendido por el interfaz vio0 que consigue autoconfigurar una ip de la subred externa, (no la de subred interna puesto que no es una interfaz vlan). El interfaz vlan es generado a partir de vio0 y no tiene prioridad para atender el servicio rad.

DESARROLLO DEL SISTEMA

Configuración de la imagen base

Inicialmente se ha partido de una máquina virtual con imagen de disco o.qcow2 a la que se le ha aplicado la siguiente configuración inicial:

- 1) Se ha añadido un nuevo usuario llamado `a755232`.

- 2) Se ha añadido el usuario `a755232` al grupo `wheel`.
- 3) Se han concedido permisos de root sin contraseña a los usuarios del grupo `wheel`.

Para añadir el usuario se ha usado el comando: `sudo useradd -m -g wheel -s /bin/bash a755232.`

Para conceder permisos se ha creado el fichero de configuración del comando `doas` `/etc/doas.conf`, al que se ha añadido la línea: `permit nopass keepenv :wheel.`

Además se ha personalizado el entorno permitiendo autocompletar comandos con la tecla `tab` y se ha adoptado el estilo de edición de vi con el comando `set -o vi` añadiéndolo al fichero `~/.profile` para garantizar su persistencia.

Creación y configuración de router IPv6: orouter1

A partir de la imagen base `o.qcow2` que contiene el S.O openBSD junto con los cambios descritos en el apartado anterior, se ha creado una nueva imagen diferencial llamada `orouter1.qcow2` que se utilizará para arrancar y configurar la MV `orouter1` con capacidad para enrutar paquetes.

Para crear la imagen diferencial se ha usado el comando:

```
qemu-img create -f qcow2 -o backing_file=o.qcow2  
orouter1.qcow2
```

Posteriormente se ha copiado el fichero `o.xml` renombrándolo como `orouter1.xml` y se han modificado los siguientes cuatro campos:

- Nombre de máquina:
`<name>orouter1</name>`
- Dirección del fichero qcow2:
`<source file='/misc/alumnos/as2/as22019/a755232/orouter1.qcow2'/>`
- Identificador mac:
`<mac address='52:54:00:01:FF:01'/>`
- uuid:
`<uuid>667734dd-445c-42f8-aeb3-65f956261ff1</uuid>`

Después se ha definido la máquina en libvirt con el comando `virsh -c qemu:///system define orouter1.xml` y se ha arrancado con `virt-manager`.

Se le ha añadido una dirección IPv6 pública que lo conecta a la subred `2001:470:736b:f000` (subred exterior donde se encuentra Router central).

Para ello en el fichero `/etc/hostname.vio0`, se ha eliminado la IPV4 que venía configurada y se ha añadido:

```
up  
inet6 alias 2001:470:736b:f000::111 64
```

```
-autoconfprivacy
```

Donde la primera línea levanta la tarjeta física virtualizada de red vio0. La segunda define la tarjeta en la subred 2001:470:736b:f000 y la tercera línea permite desactivar la configuración de direcciones privadas en la interfaz.

A continuación se va a definir una interfaz vlan a partir de la tarjeta física virtualizada vio0 con IPv6 pública que lo conecta a la subred 2001:470:736b:1ff (subred interior donde se configurará posteriormente otra VM).

Para ello se ha creado el fichero /etc/hostname.vlan199 y se ha añadido:

```
inet6 alias 2001:470:736b:1ff::1 64 vlan 199 vlandev vio0  
-autoconfprivacy
```

Donde la primera línea define la subred asociada, el número de vlan que la identifica y el dispositivo físico del que está asociada la tarjeta virtual.

El encaminador por defecto de orouter1 es el router Central. Se añade su dirección IPv6 en el fichero /etc/mygate:

```
2001:470:736b:f000::1
```

Una vez conectado la VM orouter1 a las dos subredes y definido su encaminador por defecto, se ha activado el encaminamiento IPv6 mediante el comando
echo 'net.ipv6.ipv6.forwarding=1' > sysctl.conf

Se ha activado el servicio de anuncios de prefijos IPv6 en el dispositivo vlan199 para que cualquier máquina conectada a la vlan de número 199 reciba el prefijo de subred 2001:470:736b:1ff y sea capaz de agregarlo a su propia dirección de host autogenerada con su identificador mac.

En el fichero /etc/rc.conf.local se ha añadido:

```
rad_flags=""
```

En el fichero /etc/rad.conf se ha añadido:

```
interface vlan199
```

Por último se ha cambiado el nombre de la máquina en /etc/myname:

```
orouter1
```

Creación de otra VM: o1ff2

Se ha creado otra máquina virtual llamada o1ff2 a partir de la imagen base o.qcow2

En el fichero o1ff2.xml se han modificado los siguientes campos:

- Nombre de máquina:

```
<name>o1ff2</name>
```

- Dirección del fichero qcow2:

```
<source file='/misc/alumnos/as2/as22019/a755232/  
o1ff2.qcow2'/>
```

- Identificador mac:
`<mac address='52:54:00:01:FF:02' />`
- uuid:
`<uuid>667734dd-445c-42f8-aeb3-65f956261ff2</uuid>`

La tarjeta de red vio0 se ha dejado activada pero no se le ha asociado ninguna subred.

```
Fichero /etc/hostname.vio0
-inet6
up
-autoconfprivacy
```

Se ha configurado una tarjeta vlan a partir de vio0 editando en el fichero /etc/hostname.vlan199:

```
vlan 199 vlandev vio0 up
inet6 autoconf
-autoconfprivacy
```

Donde en la segunda línea podemos observar que se asocia dinámicamente una dirección IPv6 escuchando el servicio rad levantado en orouter1.

Por último se ha añadido el enrutador por defecto en /etc/mygate, que corresponde con la dirección IPv6 de orouter1 2001:470:736b:1ff::1. Se ha incluido también el nombre de la MV en /etc/myname, o1ff2.

PRUEBAS DE FUNCIONAMIENTO

Tras la terminar con la configuración de red en las respectivas máquinas orouter1 y o1ff2, se han reiniciado las tarjetas de red con el comando sh/etc/netstart.

Se ha comprobado la conectividad de las dos máquinas desde distintos puntos de la red mediante el comando ping:

Desde orouter1 hacia o1ff2:

```
orouter1$ ping6 $o1ff2
PING 2001:470:736b:1ff:835f:40d2:1a05:f366
(2001:470:736b:1ff:835f:40d2:1a05:f366): 56 data bytes
64 bytes from 2001:470:736b:1ff:835f:40d2:1a05:f366: icmp_seq=0 hlim=64
time=0.651 ms
64 bytes from 2001:470:736b:1ff:835f:40d2:1a05:f366: icmp_seq=1 hlim=64
time=0.546 ms
```

Desde o1ff2 hacia orouter1:

```
o1ff2$ ping6 $orouter1
PING 2001:470:736b:1ff::1 (2001:470:736b:1ff::1): 56 data bytes
64 bytes from 2001:470:736b:1ff::1: icmp_seq=0 hlim=64 time=0.412 ms
64 bytes from 2001:470:736b:1ff::1: icmp_seq=1 hlim=64 time=0.464 ms
64 bytes from 2001:470:736b:1ff::1: icmp_seq=2 hlim=64 time=0.522 ms
```

Desde el ordenador del laboratorio hacia orouter1:

```
~/ ping6 2001:470:736b:f000::111
PING 2001:470:736b:f000::111(2001:470:736b:f000::111) 56 data bytes
64 bytes from 2001:470:736b:f000::111: icmp_seq=1 ttl=63 time=0.446 ms
64 bytes from 2001:470:736b:f000::111: icmp_seq=2 ttl=63 time=0.646 ms
64 bytes from 2001:470:736b:f000::111: icmp_seq=3 ttl=63 time=0.762 ms
```

Desde el ordenador del laboratorio hacia o1ff2:

```
~/ ping6 2001:470:736b:1ff:835f:40d2:1a05:f366
PING
2001:470:736b:1ff:835f:40d2:1a05:f366(2001:470:736b:1ff:835f:40d2:1a05:f366
) 56 data bytes
64 bytes from 2001:470:736b:1ff:835f:40d2:1a05:f366: icmp_seq=1 ttl=62
time=0.744 ms
64 bytes from 2001:470:736b:1ff:835f:40d2:1a05:f366: icmp_seq=2 ttl=62
time=1.20 ms
```

Desde o1ff2 hacia la ipv6 del dominio ipv6.google.com:

```
o1ff2$ ping6 2a00:1450:4003:809::200e
PING 2a00:1450:4003:809::200e (2a00:1450:4003:809::200e): 56 data bytes
64 bytes from 2a00:1450:4003:809::200e: icmp_seq=0 hlim=54 time=74.720 ms
64 bytes from 2a00:1450:4003:809::200e: icmp_seq=1 hlim=54 time=74.867 ms
64 bytes from 2a00:1450:4003:809::200e: icmp_seq=2 hlim=54 time=74.160 ms
```

Tras la realización satisfactoria de todas las pruebas se ha comprobado que las dos máquinas están correctamente conectadas a la red.

PROBLEMAS ENCONTRADOS

Asignación incorrecta del encaminador por defecto de la MV o1ff2, asignándole la IPv6 de la interfaz vio0 de orouter1 en vez de la IPv6 de la interfaz vlan199 de orouter1.

Asignación de `inet6 alias 2001:470:736b:1ff::1 64 NONE vlan 199 vlandev vio0` a la interfaz vlan199 de orouter1 dejaba a la máquina no alcanzable en la red. Se solucionó eliminando NONE.

Cambié el nombre del usuario root, con usermod para hacer menos rastreable la cuenta ante barridos ssh, pero esto originó un fallo en el sistema de ficheros que dejaba inoperativa la VM. Lo solucioné haciendo uso del último backup que tenía guardado del sistema.