AS2 : Práctica Nº 1

Objetivo: Puesta en marcha de 2 VMs con OpenBSD sobre entorno libvirt, en red y configuración de uno de ellos como router en IPv6.

Entrega: La entrega de la Práctica 1 se realizará a través de la tarea habilitada para tal efecto en Moodle, siendo la **fecha límite** de entrega el **16 de febrero de 2023 y la evaluación el 17 de febrero**.

Se deberá **entregar** una **memoria** en la que, al menos, se incluya:

1.- Resumen
2.- Introducción y objetivos.
3.- Arquitectura de elementos relevantes
4.- Comprehensión de elementos significativos de la práctica (Subredes IP implicadas, VLANs implicados, routers implicados, encaminadores por defecto utilizados)
5.- Problemas encontrados y su solución.

Adicionalmente, en la sección 4 se deberá responder a la siguiente cuestión:
¿Qué ocurre si introducimos "inet6 autoconf" en el fichero "hostname.vio0" de la máquina interna de prueba y por qué?

Terminos a utilizar: vlans, Ipv6, subredes IP (y su prefijo correspondiente), routers (nuevos ? nueva subred ?), acceso a subredes IP, encaminadores implicados, tests de conectividad (ping6 y traceroute6/tracepath6).

Enunciado:

A. Datos globales de red y de sistemas para toda la asignatura

A lo largo de las prácticas, y para evitar conflictos, se utilizará un particionado de varios espacios de nombres compartidos por los alumnos : @ MAC, etiquetas VLAN, @IP, DNS, nombres de usuarios, etc.

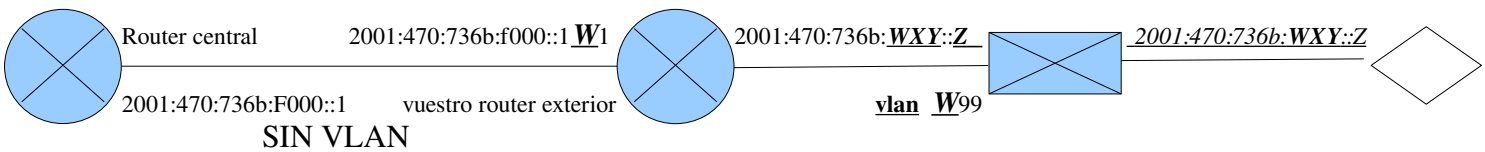
Algunos valores que se van a utilizar ya a partir de esta práctica son :

Contraseña usuario root	lojusto2
W	**nº grupo seleccionado en moodle** (hexadecimal **salvo VLAN**)
XY	Designación hexadecimal de subred para cada práctica
Z	Designación de máquina específica en subred
Nombre usuario	La misma disponible ya en CentOS

Cada alumno tiene **un prefijo de red global** "2001:470:736b:0***W00***::/56" IPv6 y **un rango de 100 valores vlan** comenzando por ***W***00. Estos elementos serán necesarios a lo largo de toda la asignatura.

B. Arquitectura inicial de red y sistemas

Subred exterior : 2001:470:736b:f000::/64 **VM1 = orouter*W*** **Subred :** 2001:470:736b:***WXY***::/64 **VM2= o*WXYZ***



SIN VLAN

- Valor de Variables para todos los alumnos :

XY = FF
Z=1 para VM1 - router-
Z=2 para VM2 – máquina interna

- Nombre libvirt y DNS de VMS : <ident SO>***WXYZ***

***** ident SO = o (OpenBSD), u (ubuntu), c (centos), etc

- Datos de redRed :

@ *MAC* VMs qemu **:** 52:54:00:0***W:XY:0Z***

Identificador VLAN **:** ***W*99 (W debe ser convertido a decimal si pasa de 9)**

@ IPv6 VMs en subred externa **:** 2001:470:736b:F000::1***W***1

Encaminador principal por defecto para VMS en subred exterior (central), IPv6 **:** 2001:470:736b:F000::1

Servidor DNS IPv6 : 2001:470:736b:F000::2

********** ***Prefijo subred global de cada alumno*** para sus VMs y ***para toda la asignatura*** (utilizado en encaminador principal, -central-) **:** 2001:470:736b:**W00**:/56

Servidor soporte **:** central.cps.unizar.es (2001:470:736b:F000::1)

Subred exterior con encaminador principal : 2001:470:736b:F000::/64

Subred primaria de máquinas físicas del laboratorio 1.02 (CentOS) **:** 2001:470:1f0b:19fb::/64

Se utilizan varias máquinas OpenBSD **sobre** el entorno de **libvirt** y **kvm** de **CentOS,** y red **IPv6.**

Utilizaremos **virt-manager** para preparar los dispositivos virtuales sobre los que se apoyara el fichero imagen del sistema operativo.

Si quereis disponer de IPv6 en vuestros portátiles, instalar (ubuntu/debian) el paquete **miredo** (crea, automáticamente, un túnel IPv6 sobre IPv4, detrás de NAT).

Notas :

- **Ctrl-Alt** quita el foco del ratón del terminal de la VM.
- En los ficheros de configuración de sistemas Unix (y Linux), por norma general, se pueden introducir líneas de **comentarios** con el carácter **#**

B. *Configuracíon de la imagen base (esencial hacer correctamente estos pasos para resto de práticas)*

1. Copiar ficheros o.qcow2 y o.xml (desde directorio /misc/usuarios/unai/vms/) a vuestro directorio /misc/alumnos/as2/as22021/<vuestro directorio con vuestro nombre usuario>. Renombrar vuestroo.qcow2 a **oW.qcow2**, y o.xml a **oW.xml** (W convertirlo a vuestro identificador)
2. Modificar el PATH de acceso a vuestro fichero oW.qcow2 (source) con vuestro camino de directorios, y también su nombre de fichero, **en oW.xml**. Verificar que el fichero **oW.qcow2 y el directorio que lo contiene** tenga como **grupo propietario "vmu"** y **permisos de grupo "rw"**.
3. Modificar el **campo "mac address"** en **o*W*.xml** al valor 52:54:00:***W:11:01***, donde W (debe tener 2 cifras), el **campo"name"** debe coincidir con el **nombre del fichero** (sin extensión xml) y el **campo "uuid"** de deben **cambiar últimas 4 o 5 cifras con W, 1, 1, Z.**
4. Definir la máquina en **libvirt/kvm** con "**virsh** -c qemu:///system define **o.xml**" y arrancar "virt-manager". Desde el virt-manager arrancar la VM. Conectaros como root con la contraseña indicada al inicio.
5. Eliminar configuracion actual de IP con "ifconfig vio0 -inet". Modificar el fichero /etc/hostname.vio0 para, solamente, activar la tarjeta de red mediante "up".

6. Crear cuenta usuario normal (adduser) con vuestro **nombre de cuenta de hendrix** y añadiéndole al grupo *wheel*. Configurar el comando **doas** para que los miembros del grupo *wheel* puedan ejecutar programas con privilegios de root sin contraseña.

7. Copiar, **desde esta VM con scp**, la clave pública de ssh de los hosts CentOS del laboratorio 1.02 al fichero ".ssh/authorized_keys" de este usuario en esta VM. Utilizar la direcciones link-local de ipv6 en la VM y en el interfaz "br1" de centos. A partir de aqui, ya teneis la posibilidad de conectaros y trabajar por ssh, desde el exterior, a esta VM mediante IPv6 con autentificación de clave pública (no se puede de otra forma debido a la configuración establecida a ssh en esta VM), por ahora con link-local. **Probarlo**.

8. **Parar la máquina con shutdown**, **y** cuando os indica que ya ha parado, **forzar su parada completa** desde el menu de virt-manager. Ejecutar un "undefine" de la VM mediante virsh para limpiar su presencia en la máquina física. **Esta VM no debería ser arrancada ni modificada en el futuro.** Sino puede introducir inconsistencia en futuras VMs diferenciales.

C. *Creación y configuración básica de un router IPv6*

1. Crear una imagen diferencial con imagen base *o.qcow2*, y de nombre **orouter*W*.qcow2**, según el método explicitado en el anexo A.

2. **Copiar** el fichero o.xml a **orouter*W*.xml,** y modificar su contenido para poner el camino completo de acceso a vuestro fichero orouter*W*.qcow2 **(source) y el nombre (name) de la VM a orouter*W***. Verificar que el fichero **orouter*W*.qcow2** tenga como grupo propietario "vmu" y permisos de grupo "rw".

3. Modificar "mac address" en **o*W*.xml** al valor 52:54:00:***W:XY:01***, donde W (debe tener 2 cifras), X, Y son las 3 o 4 cifras definidas en la sección inicial de variables. Y el campo "uuid" de ese mismo fichero, cambiar últimas 4 o 5 cifras con W, X, Y, Z.

4. Definir la máquina en **libvirt** con :

   "**virsh** -c qemu+ssh://<usuario>@155.210.154.210/system define **orouter*W*.xml**"

   Y arrancar "virt-manager", y desde el virt-manager arrancar la máquina virtual. Conectaros como root con la contraseña indicada al inicio de este guión.

5. Modificar el fichero /etc/hostname.vio0 para que funcione **sólo** con la @ 2001:470:736b:f000::1***W***1. Y modificar el fichero /etc/mygate para que **sólo** incluya el encaminador IPv6 principal por defecto de su subred, es decir, el router "central" según el gráfico anterior.

6. Copiar fichero /etc/hostname.vio0 a otro con nombre /etc/hostname.vlan***W***99. Modificar, este último, para poner @IPv6=2001:470:736b:***WXY***::**1** y la vlan =***W***99, indicando como dispositivo asociado **vio0**. **Habeis definido 2 tarjetas de red**, una fisica sin VLAN y una virtual con vlan, que están **conectadas a 2 subredes diferentes**, una exterior y otra interior.

   Además, OpenBSD, como el resto de sistemas en la actualidad, tiene activada la configuración de @ Ipv6 anónimas (o privadas) con la generacion aleatoria periódica de @Ipv6 públicas únicas. Y esto, además, en muchos casos, de la dirección IPv6 asignada automáticamente por composición de prefijo de subred Ipv6 anunciado por router y @MAC de la tarjeta de red.
   En nuesto caso, nos INTERESA **eliminar** esta @ anónima para simplificar el comportamiento de red. Para eliminarlo, añadir , a todos los ficheros de dispositivo de red con ipv6 activa (/etc/hostanme.vlan??? de todas las VMs y **vio0** de router exterior) , la línea :

   –autoconfprivacy

   Y aplicadlo a todas las VMs que creemos a partir de ahora.

7. Para activar encaminamiento ip6 y no contestación a anuncios de prefijo ip6, modificar /etc/**sysctl.conf** (teneis ejemplo de fichero en /etc/examples/) con :

net.inet6.ip6.forwarding=1

8. Hay que poner en funcionamiento el servicio de anuncio de prefijos IPv6 a la subred de la vlan :

   Poner en marcha el servicio ***rad*** *(mirar páginas man en internet)***,** mediante activación de servicio, en */etc/rc.conf.local*, incluyendo *rad_flags*="" o mediante comando **rcctl** *(mirar paginas man en internet)*. Adicionalmente, indicar la tarjeta, en la que se anuncia la información de prefijo y encaminador por defecto, en el fichero "/etc/rad.conf" con la nueva línea "interface <vuestro_interface>". Se pueden precisar aspecto adicionales de funcionamiento de este servicio en este fichero de configuración, pero, por ahora, no son necesarios.

9. Modificar el nombre de la máquina en /etc/myname a "**orouter*W***".

10. Rearrancar la VM con "shutdown -r now".

11. Comprobar conexión y creación de usuario conectandose por ssh desde CentOS a "nombreusuario@2001:470:736b:f000::1***W***1". Verificar que dicho usuario esta en grupo wheel con comando **id**.

12. Si no lo teneis creado, generar pareja clave-pública privada, para ssh en **CentOS**, con "ssh-keygen". Copiar la clave pública generada al fichero **authorized_keys** en ~/.ssh del directorio home de vuestra cuenta de usuario creada en la VM (En CentOS, "*ssh-copy-id nombreusuario@2001:470:736b:f000::1**W**1*") y también en CentOS. **Comprobar** que os funciona la conexión ssh sin contraseña tanto a la VM como a CentOS.

D. Creación de otra VM de prueba para red interior

13. Siguiendo los pasos de la sección C, efectuar otra imagen diferencial nueva sobre la misma base (o.qcow2) para una nueva VM de nombre "oWXYZ" (con Z=2). Adaptar todos los nombres explicitados (ficheros, nombre VM, etc) en la sección C a este nombre. También, adaptar @ MAC (ahora Z=2) y el campo "uuid" en ".xml" de forma similar a sección C (ahora Z=2) .

14. Definir la máquina en **libvirt** y arrancarlo en "virt-manager". Entrar en sesión con root.

15. Editar /etc/hostname.vio0 para que contenga solo las líneas (solo lo activamos, pero que no coja configuración automática de IPv6) :

    -inet6
    up

16. Crear fichero /etc/hostname.vlanW99 con el contenido (en este si que tiene que tomar la IPv6 automática) :

    vlan W99 vlandev vio0 up

    inet6 autoconf

17. Recordar completar ambos ficheros previos, de configuración de tarjetas de red, con la línea adicional :

    -soii -temporary

18. Poner el nombre DNS que corresponde a esta VM en /etc/myname.

19. Habilitar el servicio "slaacd" mediante "rcctl". ¿ Para qué es necesario ?

20. Reconfigurar ambas tarjetas con : # *sh /etc/netstart* . El comando ifconfig debería mostrar la @ IPv6 en la tarjeta vlanW99.

21. **Probar** que podeis conectaros con ssh a esta máquina, primero desde el router y, después, desde un host CentOS. Si funciona desde el router y no desde CentOS, vuestro router no encamina.

22. Copiar el authorized_keys del usuario desde el router a esta máquina de forma adecuada. Comprobar que podeis conectaros con ssh sin contraseña.

23. **Parar la máquina con shutdown**, **y** cuando indique que ya ha parado, **forzar su parada completa** desde el menu de virt-manager.

    Ya tenéis un router con una red interna con IPv6 global y una VM cliente.

E. Final

1. **Parar las máquinas con shutdown**, **y** cuando os indica que ya ha parado, **forzar su parada completa** desde el menu de virt-manager.
2. ***Haced buenas copias de seguridad de los ficheros (qcow2 y xml) de VM (incluida la base) .***

Esto es todo, por ahora. Recordad que **NO se debe apagar** vuestro sistema **sin** antes **ejecutar** el comando de apagado del sistema como **root** : ***shutdown -h now***.

Realizad una copia de seguridad de vuestra imagen de disco a vuestro dispositivo de almacenamiento usb.

AL TERMINO DE LAS PRACTICAS SALID DE SESIÓN DE TODOS LOS ORDENADORES CON LO QUE ESTEIS CONECTADOS, Y SI NADIE MAS LO UTILIZA, APAGARLO con "sudo shutdown -h now".

ANEXO A : Creación de imagenes diferenciales con comando "qemu-img"

En lugar de clonar el fichero de imagen entero, una imagen diferencial crea un fichero dónde sólo guarda las diferencias, mientras utiliza los datos no cambiados del fichero de imagen base . Para conseguirlo, se va a utilizar la herramienta "qemu-img" con la siguiente línea de comandos :

qemu-img create -f qcow2 -o backing_file=o.qcow2 orouter***W***.qcow2

orouter***W***.qcow2 es la imagen de la nueva máquina virtual a configurar. La **imagen base**, o.qcow2, **sólo** necesita estar con **permisos de lectura (suprimir** el permiso de escritura**)**. Para trabajar desde casa, hay que llevarse los 2 ficheros, la base y el diferencial (o diferenciales cuando haya más máquinas)

Recordad que la imagen base (o.qcow2) debe estar con mismo nombre e ubicación en directorios que cuando se ha ejecutado este comando qemu-img, para que la imagen diferencial funcione (algunas lecturas seguiran haciendose sobre la base en la misma ubicación registrada en esta operación) !!

Hay posibilidad de recuperar las 2 de nuevo en una sola imagen (parámetro *commit*) o cambiar el nombre y/o ubicación de la imagen base (parámetro *rebase*). Por ahora no lo necesitamos.

Referencias

- Diapositivas de la asignatura
- Páginas man de "intro", "hostname.if", "ifconfig", "route", "netstart", "rtadvd", etc ... de OpenBSD.

ANEXO B :

Para portátil con (letra)ubuntu, cambiar en el fichero xml :

1. emulator : /usr/bin/kvm???
2. machine : pc??
3. source file : camino completo a fichero imagen qcow2
4. En lugar de bridge configurar NAT en xml dado que utilizais wifi y es más complicada la configuración bridge con ella. Utilizareis portátil, no como servidor sino para pruebas locales y como cliente de conexión a libvirt.