Pràctica 1: Virtualització i xarxes

Aplicacions i serveis d'internet — iTIC

Francisco del Águila López Aleix Llusà Serra Alexis López Riera

18 de febrer de 2021

Índex

Resum

Protocols d'internet: IP, MAC, ARP, NAT, DHCP, ICMP (ping), SSH

1 Organització

1.1 Objectius

Els objectius d'aquesta pràctica són:

1. Com a previ de les pràctiques de l'assignatura, aprendre a utilitzar tècniques de virtualització per tal de poder establir un entorn de proves de serveis d'internet. La configuració de l'entorn descrit en aquest document s'utilitzarà a les pràctiques de l'assignatura.
2. Entendre la virtualització de xarxes amb *Linux Bridge* i `OpenVPN`.
3. Observar la transparència de la virtualització a l'usuari: aquest no pot distingir si l'entorn és virtualitzat o no.
4. Establir connexions remotes mitjançant SSH
5. Usar Wireshark per a analitzar les trames que circulen per la xarxa.

1.2 Condicions

- La pràctica està calibrada per a ésser treballada en equips de dues persones.
- La durada de la pràctica és de 2 setmanes.

1.3 Lliurables

Aquesta pràctica no comporta lliuraments. L'ús d'aquestes eines s'estendrà a la resta de pràctiques del curs i, per tant, s'avaluarà conjuntament amb aquestes futures pràctiques.

1.4 Material necessari

Per dur a terme la pràctica cal tenir instal·lat una eina de virtualització de màquines i una de xarxes, a més d'una eina d'anàlisi de xarxa. En el cas de GNU/Debian i equiparables cal que instal·leu els paquets `qemu-kvm`, `bridge-utils`, `openvpn` i `wireshark`.

> TASCA PRÈVIA 1 Instal·leu en el vostre computador els paquets anteriors. En els computadors de laboratori ja els trobareu instal·lats. En el cas que el vostre processador no tingui propietats de virtualització hardware, podeu utilitzar `qemu` en comptes de `qemu-kvm`.

Nota: en sistemes que tinguin versions velles de `qemu`, com és el cas de Ubuntu <= 12.04, si es vol usar només qemu s'ha d'instal·lar el paquet `qemu-system` i usar-lo amb l'ordre adequada p.ex. `qemu-system-i386`.

2 Introducció a la virtualització

La virtualització és una tècnica que consisteix en executar diverses màquines virtuals en una de física. És a dir, les màquines virtuals comparteixen, sense saber-ho, els recursos de la màquina física: disc, CPU, memòria, xarxa, etc. És més, mitjançant la virtualització es poden emular

recursos que realment la màquina física no té. Les màquines virtuals veuen els recursos com a propis i físics i no s'adonen que estan virtualitzades.

Hi ha diferents tipus de virtualització de màquines i en aquesta pràctica veurem l'eina de virtualització qemu/kvm que és de tipus virtualització completa. Per a la virtualització de xarxa veurem dues eines.

2.1 Escenari

A les pràctiques de l'assignatura necessitarem diverses màquines i una xarxa local per a poder tenir un entorn de proves. Per a simular aquest entorn utilitzarem tècniques de virtualització de manera que siguin transparents a l'usuari, és a dir, que externament no es podrà distingir que són màquines virtuals.

Cal entendre bé l'entorn descrit i les configuracions realitzades ja que seran necessàries per a les pràctiques següents.

Per a poder experimentar amb la xarxa no disposem d'adreces públiques. Per tant, crearem una xarxa local privada; és a dir amb adreces IP privades que són les que s'inclouen en els grups següents:

- 10.0.0.0/8 (255.0.0.0)
- 172.16.0.0/12 (255.240.0.0)
- 192.168.0.0/16 (255.255.0.0)

Escollim crear una xarxa privada en el rang `172.20.0.0/16`.

Cada grup de pràctiques tindrà assignada una subxarxa amb 256 adreces a on podrà fer i desfer segons el seu criteri. **No** podrà assignar adreces que no pertanyin a la seva subxarxa. Així doncs, cada grup tindrà una subxarxa en el rang `172.20.ng.0/24` a on *ng* és el número de grup. Amb el mateix efecte, cada grup tindrà disponibles les adreces MAC 52:54:00:99:ng:xx.

Noteu que el proveïdor OUI (*Organizationally unique identifier*) associat a les adreces 52:54:00: és qemu i aquestes adreces estan pensades per a ser assignades a màquines virtuals; una altre proveïdor similar és Xensource en el rang 00:16:3e:. Recordeu-ho en visualitzar les MAC a Wireshark ja que hi apareixen amb el nom de proveïdor, podeu consultar els OUI assignats a `http://standards.ieee.org/develop/regauth/oui/oui.txt` i a `http://anonsvn.wireshark.org/wireshark/trunk/manuf`.

Per a interconnectar les subxarxes dels grups haureu de seguir la tècnica descrita a l'apartat 5.3. Heu d'utilitzar una VPN de l'assignatura, a la qual us podreu connectar mitjançant un usuari i contrasenya que us proporcionarà el professor.

Tasca 2 **Agrupeu la configuració!** Un cop hagueu llegit la pràctica i hagueu entès el desplegament de màquines i xarxes virtuals que haureu de fer, escriviu les ordres que configuren l'entorn en un script per tal de poder-lo utilitzar en les pràctiques següents.

Tingueu una imatge de disc virtual preparada amb un sistema bàsic instal·lat. Així la podeu copiar per crear màquines noves i només us caldrà canviar el nom i l'adreça IP.

3 Virtualització de màquines amb qemu/KVM

En aquestes pràctiques utilitzarem `qemu` [Bel09] com a virtualitzador de màquines. En aquest context, s'anomena host a la màquina física i guest a cada màquina virtual que tingui.

Hi ha una extensió de kernel anomenada KVM (*Kernel Virtual Machine*) que permet utilitzar el suport de virtualització per part d'alguns processadors. Per saber si el vostre processador té tecnologia de virtualització, cerqueu si teniu la flag *vmx* o *svm* a `/proc/cpuinfo`. En cas afirmatiu mireu si teniu el dispositiu `/dev/kvm` i que estigui activat en el nucli `lsmod | grep kvm`; si no hi és pot ser que necessiteu activar la virtualització a la Bios. En el cas de no disposar de KVM, canvieu *kvm* per *qemu* en la documentació següent.

El primer pas és disposar de disc virtual:

```
qemu-img create -f qcow2 virtu.img 4G
```

Els segon pas és arrencar la màquina oferint-li el disc virtual com a disc dur:

```
kvm virtu.img
```

En aquest cas, el disc virtual és buit i per tant no hi ha cap unitat des d'on poder arrencar. Si la interfície us captura el ratolí, premeu CTRL+ALT per a alliberar-lo.

El tercer pas és instal·lar un sistema operatiu al disc. Per exemple oferim una unitat lectora amb una imatge de CD inserida:

```
kvm virtu.img -cdrom cd.iso
```

Si en el procés d'instal·lació apareix el missatge indicant que el sistema té poca memòria, podeu definir al màquina virtual amb la memòria desitjada amb el paràmetre -m:

```
kvm virtu.img -m 512M -cdrom cd.iso
```

Tasca 3 Instal·leu un Debian GNU/Linux en una màquina virtual. Utilitzarem Debian *testing*, en aquests moments Debian jessie, per a tenir eines actuals. Podeu trobar una imatge per al CD d'instal·lació a `http://www.debian.org/distrib/netinst`. Amb les *netinst*, les instal·lacions que es completen per xarxa, en tindreu prou.

Seguiu el procés d'instal·lació: escolliu la configuració automàtica de xarxa i escolliu no instal·lar paquets addicionals en la configuració del tasksel. El procés tarda uns 15 minuts (amb KVM).

Un cop acabada la instal·lació, arrenqueu la màquina i instal·leu els paquets que considereu imprescindibles: sudo, ssh, less, emacs, etc.

3.1 Xarxa user-mode

Per defecte, QEMU utilitza les opcions -nic i -user per a establir una xarxa user-mode. Amb això s'afegeix un adaptador simple de xarxa al guest i es dóna al host accés a la xarxa mitjançant NAT; fixeu-vos que l'ordre anterior `kvm virtu.img` és equivalent a:

```
kvm -hda virtu.img -net nic -net user
```

Des d'un guest normalment es pot trobar el host actuant com a passarel·la a l'adreça privada 10.0.2.2, un servidor de DHCP a la 10.0.2.2 i un servidor de noms a la 10.0.2.3. Al guest se li ofereix una adreça a partir de la 10.0.2.15.

Tasca 4 Des de la màquina virtual, trobeu la IP de la màquina virtual, quina xarxa li correspon i la IP que aquesta veu del host. Feu Pings a aquestes adreces i proveu de connectar-vos-hi mitjançant ssh.

Podeu consultar les IP amb `/sbin/ifconfig` i `/sbin/route`.

Nota: amb l'adaptador de xarxa de `qemu` els Ping a Internet no funcionen ja que només es permet tràfic TCP o UDP. A tall d'exemple, es pot fer Ping a la màquina host a l'adreça privada (10.0.2.2) però no a la IP pública.

La IP del guest s'assigna privada automàticament mitjançant DHCP de QEMU, així com la MAC també s'assigna automàticament a 52:54:00:12:34:56. Amb l'opció hostfwd es poden redireccionar ports del host cap a ports del guest:

```
kvm virtu.img -net nic -net user,hostfwd=tcp::5555-:22
```

això permet accedir al guest per ssh, connectant a la IP del host

```
ssh localhost -p 5555
```

Tasca 5

1. Comproveu que teniu el servidor de *ssh* funcionant a la màquina virtual.
2. Atureu la màquina virtual i arrenqueu-la amb una redirecció de ports per a ssh (port 22). Connecteu-vos mitjançant ssh des del host a la màquina virtual amb tres adreces diferents:
   - ssh localhost -p 5555
   - ssh <ipguest> a on *ipguest* és la IP de la màquina virtual, per comprovar que des del host no veiem al guest.
   - ssh <iphost> -p 5555 a on *iphost* és la IP de la vostra màquina host.
3. Demaneu a un altre grup la IP de la seva màquina i el port que tenen redirigit. Proveu de connectar-vos-hi amb ssh.

La redirecció de ports és incòmoda i no és transparent a l'usuari. Per a les pràctiques ens serà més útil virtualitzar la xarxa.

3.2 Virtualització del disc

La virtualització del disc és la part que s'encarrega de construir discs virtuals. Hi ha diferents mètodes de virtualització de disc; en el disc virtual creat anteriorment s'ha utilitzat el mètode de virtualització amb fitxer-imatge. Concretament, el fitxer-imatge s'ha creat amb format qcow2, el qual només emmagatzema els sectors on hi ha dades i a més permet crear fitxers-imatge derivats d'un altre.

Si no s'indica quin format es vol, per defecte qemu-img create utilitza el format raw. En el format raw el fitxer-imatge internament té tots els sectors del disc emmagatzemats. Cal recordar que els sistemes operatius solen gestionar eficientment els fitxers *sparse* (els fitxers amb blocs de valor zero). Tot i així quan es copien aquests fitxers cal tenir en compte la seva naturalesa especial.

Per a les pràctiques utilitzeu el format qcow2 com s'ha descrit. Per a treballar amb noves màquines virtuals simplement podeu copiar-ne el fitxer imatge de disc. Aleshores quan engegueu per primer cop aquesta màquina copiada canvieu-li la configuració que faci falta (nom, adreça IP, etc.) per a diferenciar-la de l'altra.

4 Virtualització de màquines amb LXC (a nivell de Sistema Operatiu)

Una alternativa a virtualitzar tot el maquinari d'una màquina fictícia, a la que se li hauria de ficar tot un programari (Sistema Operatiu) per a que funcioni, seria virtualitzar màquines a partir de la capa del kernel del sistema operatiu. En aquest cas, les màquines virtualitzades han de compartir (és únic) el kernel del sistema operatiu de la màquina real. A aquest tipus de virtualització consisteix en la creació i gestió de contenidors de màquines (*containers*). El nom de *contenidor* s'escau molt bé ja que una manera d'entendre aquest tipus de virtualització és considerar que certs processos del sistema operatiu quedin continguts dins un entorn que simula una màquina complerta.

Per crear *contenidors* es pot fer en funció de diferents privilegis.

- Un usuari del sistema sense privilegis crea un *contenidor* sense privilegis
- L'usuari *root* crea un *contenidor* sense privilegis
- L'usuari *root* crea un *contenidor* amb privilegis per gestionar la xarxa, muntar sistemes de fitxers, etc.

Pel cas que ens interessa crearem *contenidors* que tinguin tots els privilegis necessaris, per tant només els podrà crear *root*.

La comanda per crear un *contenidor* és

```
sudo lxc-create -t plantilla -n el-meu-container
```

Les plantilles disponibles poden ser distribucions disponibles com Ubuntu, Debian, Fedora, etc. Per obtenir més informació sobre *Linux Containers* disposeu de [Con18] on trobareu la descripció dels manuals de les comandes disponibles.

També una bona guia la trobareu a [Can18] on s'explica com fer que els *contenidors* puguin arrencar automàticament, o bé com configurar la xarxa, etc.

Cal fer notar que cadascun dels *contenidors* creats amb privilegis els trobarem dins del directori */var/lib/lxc* on per una banda es troba tant el fitxer de configuració que defineix el *contenidor*, com el sistema de fitxers associat a aquest *contenidor*. Els paràmetres del fitxer de configuració associat a cada *contenidor* els trobarem detallats al manual de *lxc.container.conf*.

Per a cada *contenidor* disposarem dels paquets que tinguem instal·lats dins del seu sistema de fitxers.

Algunes de les principals comandes de *lxc* són:

```
sudo lxc-ls --fancy
sudo lxc-start --name u1 --daemon
sudo lxc-info --name u1
sudo lxc-stop --name u1
sudo lxc-destroy --name u1
```

Els Linux Containers tracten la xarxa d'una manera còmode i automàtica per a que un cop s'haig creat el *contenidor* aquesta màquina virtual pugui disposar de xarxa. El mecanisme és similar a com ho fa *kvm*.

Durant la instal·lació dels *lxc* es crea automàticament una xarxa basada en un bridge. Això s'aconsegueix a través del servei *lxc-net*. Trobareu més informació a [deb17] i [blo18].

5 Virtualització de xarxes

Les eines disponibles ens permeten crear una xarxa virtual amb aparells de xarxa virtualitzats. Hi ha vàries tècniques de xarxa virtual que funcionen amb `qemu/KVM` [Qem12], ja hem vist el mètode de xarxa *user-mode* i ara veurem el *Linux bridge*. Per altra banda, per tal d'interconnectar les xarxes dels diferents grups de pràctiques usarem tècniques de xarxes virtuals privades (VPN, de l'anglès *virtual private network*).

La tècnica habitual per a establir una xarxa virtual permanent és la de *Linux bridge*. Amb aquest mètode la xarxa virtual s'integra a la xarxa del host i per tant es necessiten permisos de root. En el vostre propi computador no hi haurà cap problema, però per a les pràctiques al laboratori no teniu accés de root al sistema i en aquests computadors us haureu d'atendre a la configuració que trobeu.

5.1 OpenVPN

L'`OpenVPN` permet la interconnexió de xarxes privades TCP/IP a través de xarxes públiques també basades en TCP/IP com és Internet. La interconnexió d'aquestes xarxes privades pot mantenir la privacitat ja que es pot fer servir mecanismes de clau pública basades en certificats. La utilització de certificats assegura l'autenticació de les xarxes privades que s'interconnecten així com la protecció mitjançant xifrat de les dades que es comuniquen. Aquests aspectes de seguretat es veuran a la part final del curs.

Aquesta interconnexió de xarxes privades es pot dur a terme tant a nivell 2 com a nivell 3. Si es realitza a nivell 3 es necessita de dispositius que facin la feina d'encaminar els paquets (encaminadors / routers) i per tant cal definir correctament en aquests encaminadors les taules d'encaminament de totes les xarxes privades interconnectades. Per contra, si es realitza a nivell 2, l'`OpenVPN` es comporta com un gran commutador virtual on es connecten les xarxes privades. En aquest cas totes les xarxes privades interconnectades són equivalents a una única xarxa local virtual i per tant no cal definir ni configurar encaminadors. El mecanisme que farem servir a la pràctica serà aquest: interconnexió de les xarxes privades de cada grup de pràctiques a nivell 2.

Des del punt de vista d'aplicació, l'`OpenVPN` segueix el model de client / servidor d'Internet:

El servidor espera possibles connexions de clients i ha d'estar accessible públicament. Per aquest motiu el servidor serà una màquina disponible per part de l'Escola i la seva única feina serà la d'acceptar totes les connexions dels clients. Aquest servidor `OpenVPN` serà l'encarregat d'oferir aquest commutador virtual al que els diferents grups de pràctiques es connectaran per estar en xarxa local. Per tant proporcionarà interconnexió a nivell 2 entre les xarxes de cada grup de pràctiques.

Els clients estaran a les màquines de cada grup de pràctiques. Quan s'estableix una connexió `OpenVPN` des d'un client es crea una nova interfície de xarxa. Si la interconnexió `OpenVPN` es

realitza a nivell 2, aquesta interfície de xarxa que es crea es com si estigues connectada al commutador virtual creat pel servidor. Si la interfície creada per l'`OpenVPN` forma part d'un bridge local de la màquina, aquest bridge i totes les seves interfícies formaran també part de la xarxa local virtual formada pel servidor.

A Atenea hi ha disponible el fitxer de configuració tant de client com de servidor per fer tot aquest muntatge. Per crear la connexió `OpenVPN` simplement s'ha de cridar la comanda següent:

```
/usr/sbin/openvpn --config client.txt
```

S'ha de tenir en compte que si es crida la comanda amb privilegis de root fent sudo s'ha d'introduir la contrasenya de root de la màquina local, seguidament demanarà el nom d'usuari per autentificar-se al servidor `OpenVPN` (és el que teniu a l'Escola) i per últim la vostra contrasenya. Si la connexió s'estableix amb èxit, no sortirà cap missatge d'error i el terminal quedarà bloquejat amb la connexió establerta.

Recordeu que si es fa servir les màquines del laboratori no cal executar la comanda `openvpn` amb privilegis de root.

5.2 Linux bridge

El *Linux ethernet bridge* [Bö01] es pot utilitzar per connectar diversos aparells ethernet. En el nostre cas l'utilitzarem com a commutador virtual. Per evitar conflictes amb les interfícies físiques de la màquina real, que generalment estan controlades pel gestor de xarxa gràfic *network-manager*, no afegirem al bridge cap d'aquestes interfícies (eth0, wlan0). De la mateixa manera, les interfícies físiques generalment funcionen amb DHCP i això provocaria problemes amb les IP de les màquines virtuals si volem mantenir el rang `172.20.0.0/16`. Per tant es crearà aquest bridge només per connectar les interfícies de les màquines virtuals.

A continuació fem un resum de les instruccions bàsiques per a configurar un escenari com el de la figura 1. La informació de com s'ha de contigurar el fitxer `/etc/network/interfaces` quan es fa servir les utilitats de bridge es pot consultar a *man bridge-utils-interfaces*.

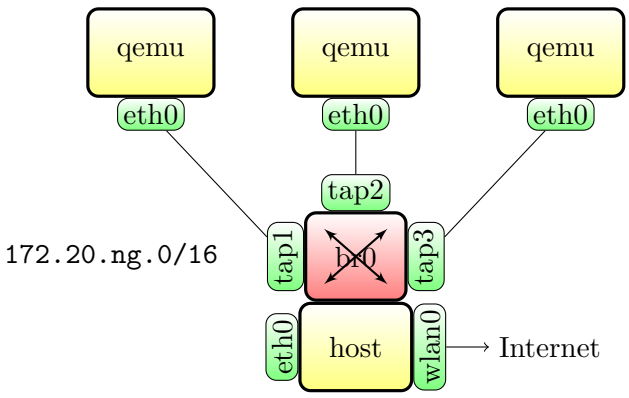

Figura 1: Esquema de xarxa bàsic amb bridge

Així a la vostra màquina i com a root configureu el fitxer `/etc/network/interfaces`:

```
auto br0
##bridge-utils
```

```
#br0 per a bridge amb connexió al host i taula de rutes
iface br0 inet static
      address 172.20.ng.xx
      netmask 255.255.0.0
      bridge_ports none
```

Ara cal reiniciar la màquina o engegar les interfícies de xarxa amb:

```
ifup br0
```

Ja podeu arrencar la màquina virtual amb una interfície de xarxa connectada al bridge (necessitareu permisos de root). En la majoria de casos s'executa un script que afegeix la nova interfície tap al bridge que s'ha creat, però l'script dóna per fet que el nom del bridge és aquella interficie per on està definit el default gateway. En el nostre cas no serà així per tant executarem la comanda sense l'execució del script. Posteriorment s'haurà d'afegir la nova interfície tap al bridge br0 de forma manual. En cas que la interfície de tapX no estigui activa, s'ha d'activar :

```
kvm virtu.img −net nic −net tap,script=no
brctl addif br0 tapX
ifconfig tapX up
```

Quan arrenqueu més d'una màquines virtual amb connexió al bridge, recordeu que no poden tenir les mateixes MAC:

```
kvm virtu.img −net nic,macaddr=52:54:00:99:34:57 −net tap,script=no

kvm virtu2.img −net nic,macaddr=52:54:00:99:34:58 −net tap,script=no
```

Tasca 6 Ara no hi ha servidor de DHCP que us ajudi, haureu de configurar manualment la xarxa de cada màquina a `/etc/network/interfaces`. Entrant al terminal de les màquines virtuals podeu accedir a la xarxa virtual amb les eines de xarxa de cada màquina. A tal efecte comproveu amb ping i connexions ssh la visibilitat entre les màquines virtuals i el host. Tampoc tindreu servidors de DNS.

Fins ara, la xarxa virtual que heu creat resta aïllada dels altres grups i d'Internet. A continuació explorem algunes tècniques per a trencar aquest aïllament.

- Connexió a Internet.
- Connexió del bridge amb els altres grups de pràctiques.
- Connexió a la xarxa virtual des del host: amb la configuració descrita fins aquest punt, la màquina host ja forma part del bridge on estan connectades les màquines virtuals. A més, quan el bridge es connecta remotament amb els altres bridge, la màquina host també està connectada a la mateixa xarxa.

5.2.1 Connexió externa a Internet

Per a alguns serveis, com per exemple instal·lar paquets, necessitem l'accés a l'exterior, és a dir a Internet.

Una possibilitat és arrencar la màquina virtual en mode -net user sense connectar al bridge, i així d'aquesta manera s'obté un accés amb NAT a través de la màquina host segons s'ha descrit a l'apartat 3.1.

També existeix la possibilita d'aprofitar que la màquina host pot estar connectada a Internet (a través de les seves altres interfícies eth0, wlan0) i permetre que faci d'encaminador per les màquines virtuals. En aquest cas s'hauria de configurar les màquines virtuals de manera que el seu default gateway a la taula de rutes sigui la màquina host. Recordeu que la comanda per manipular la taula de rutes és `route`. Per convertir la màquina host en un encaminador (router) heu de recuperar el treball fet a la última pràctica de l'assignatura de xarxes de comunicacions. Essencialment els passos a seguir són:

1. Activar el forwarding. Això s'aconsegueix:

   ```
   sysctl −w net.ipv4.ip_forward=1
   ```

   o bé

   ```
   echo 1 > /proc/sys/net/ipv4/ip_forward
   ```

2. En el cas que es vulgui fer NAT, fer servir la comanda `iptables`

   ```
   iptables -t nat -A POSTROUTING -s 172.20.ng.xx/16 -o eth0 -j MASQUERADE
   ```

   On -A POSTROUTING indica que és una regla que afecta a la cadena POSTROUTING, -s `172.20.ng.xx/16` indica que aquesta regla afectarà als paquets amb aquesta adreça d'origen, -o eth0 indica que s'aplicarà als paquets que surtin, -j MASQUERADE és l'acció de fer la traducció d'adreces.

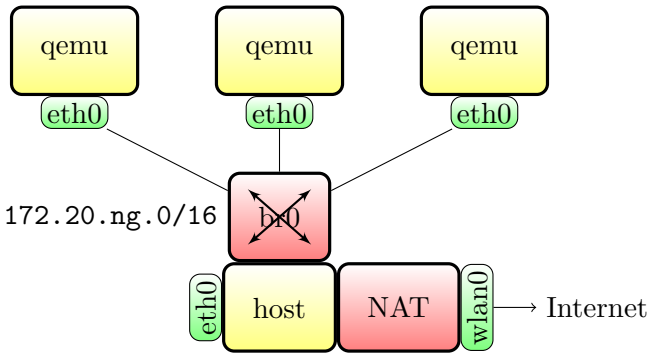

Figura 2: Xarxa bridge amb encaminador/NAT

5.3 Connexió entre commutadors amb openVPN

Per a connectar la vostra xarxa virtual a una altra, és a dir expandir la vostra xarxa, utilitzarem una VPN (Virtual Private Network). De manera que tots els grups de pràctiques quedareu interconnectats a la VPN en una xarxa virtual com a la figura 3.

Tingueu present que per a usar les connexions cal que la xarxa de cada màquina estigui ben configurada. Un cop connectats a la VPN trobareu el servidor internament a l'adreça `172.20.0.1`; podeu fer-li pings per a comprovar que esteu connectats correctament a la VPN.

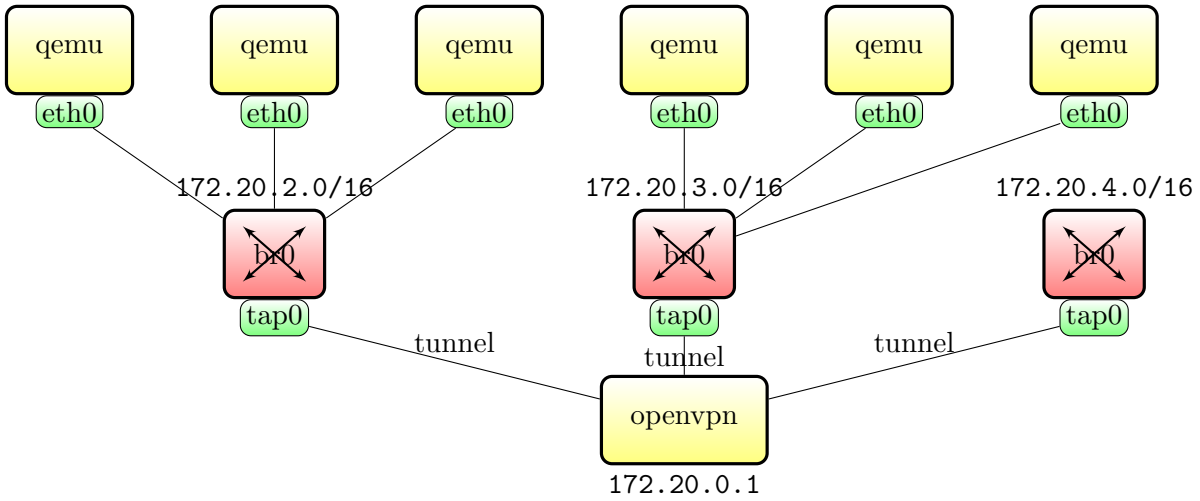

Figura 3: Xarxa amb servidor `OpenVPN` com a commutador

Tasca 7 Per tal que us pugueu comunicar entre els grups de pràctiques, configureu-vos a la mateixa xarxa local `172.20.0.0/16`; és a dir cada màquina virtual ha d'estar a la xarxa i amb la màscara de xarxa adequada. Alternativament, a la secció 7.1 us proposem una interconnexió millorada de les xarxes segmentant-les amb encaminadors.

5.4 Laboratori

A les màquines del laboratori no es té privilegis d'administració, per aquest motiu la configuració de xarxa està feta amb un esquema que permet la utilització de connexions `OpenVPN` i la creació de màquines virtuals sense la necessitat d'aquests permisos. Per aconseguir-ho s'ha predefinit un bidge amb un conjunt de possibles interfícies virtuals tipus tapX (interfícies virtuals creades per funcionar a nivell 2). La configuració del fitxer `/etc/network/interfaces` és la següent:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto kvm-br0
iface kvm-br0 inet manual
bridge_ports none

auto tap0 tap1 tap2 tap3 tap4 tap5 tap6 tap7
iface tap0 inet manual
      pre-up tunctl -t $IFACE -g Estudiants
      pre-up brctl addif kvm-br0 $IFACE
      up ifconfig $IFACE 0.0.0.0 up
      down ifconfig $IFACE down
      down brctl delif kvm-br0 $IFACE
      down tunctl -d $IFACE
```

```
iface tap1 inet manual
      pre-up tunctl -t $IFACE -g Estudiants
      pre-up brctl addif kvm-br0 $IFACE
      up ifconfig $IFACE 0.0.0.0 up
      down ifconfig $IFACE down
      down brctl delif kvm-br0 $IFACE
      down tunctl -d $IFACE
```

Amb aquesta configuració, hi ha predefinits fins a 8 tapX. Per conveni reservarem el tap0 per establir la connexió `OpenVPN` i la resta de tap1:tap7 quedaran reservats per les diferents màquines virtuals que volem connectar al bridge local *kvm-br0*.

En aquest cas tant per la connexió `OpenVPN` com per la activació de les màquines virtuals s'ha d'especificar un tap concret sense deixar-ho de manera genèrica sense índex.

6 Eines de xarxa

Podeu aplicar totes les eines de xarxa que ja coneixeu de l'assignatura de Xarxes de Comunicació. A continuació us mostrem com utilitzar-les per a les màquines i les xarxes virtuals.

6.1 Connexió remota

Per a l'administració de sistemes és vital la connexió remota. Cal conèixer i treballar còmodament amb l'eina `ssh`.

Ja heu vist com realitzar algunes connexions mitjançant ssh i durant les pràctiques següents n'anireu veient més. Consulteu el manual quan tingueu dubtes del seu funcionament: man ssh.

També hi ha altres tipus de connexions remotes. Per exemple es poden realitzar connexions de transferència de fitxers, consulteu scp i rsync; connexions remotes gràfiques, consulteu ssh −X i el protocol VNC; o bé Proxy Socks, consulteu ssh −D.

Aneu consultant els manuals quan ho necessiteu. Una referència és el Barrett i Silverman [BS01].

6.2 Wireshark

Wireshark [Wir04] és una eina per analitzar les trames que circulen per una interfície de xarxa. Per a poder explorar la xarxa virtual us proposem dues maneres:

1. Emmagatzemar la traça de xarxa de cada màquina en un fitxer amb format PCAP i llegir-lo amb Wireshark:

   kvm disc.img −net nic,macaddr=52:54:00:12:34:57 −net tap −net dump,file=tal.pcap
   wireshark tal.pcap

2. Connectar Wireshark a una interfície de xarxa virtual tap o al bridge.

   wireshark −i tap1

7 Extensions

7.1 Màquina virtual funcionant com un encaminador dins de xarxa virtual

Necessitem un encaminador per a poder segmentar les xarxes dels grups entre elles. Cada xarxa local de grup és `172.20.gg.0/24` i a cada una cal encaminar paquets cap a les xarxes locals dels altres grups. Crearem una màquina virtual i configurarem el sistema com un encaminador entre la xarxa virtual del grup i la VPN de l'assignatura. També ho podeu fer directament a la màquina host, on ja hi teniu la connexió `OpenVPN` establerta.

Configurarem l'escenari següent: els encaminadors tenen dues interfícies de xarxa: per una es connecten entre ells a la xarxa `172.20.200.0/24` i per l'altra es connecten a la xarxa del grup `172.20.ng.0/24`. Ho podeu veure a la figura 4. Si configureu l'encaminador directament al host en comptes de la màquina virtual *gw*, aleshores la interfície eth0 es correspondrà amb el br0.

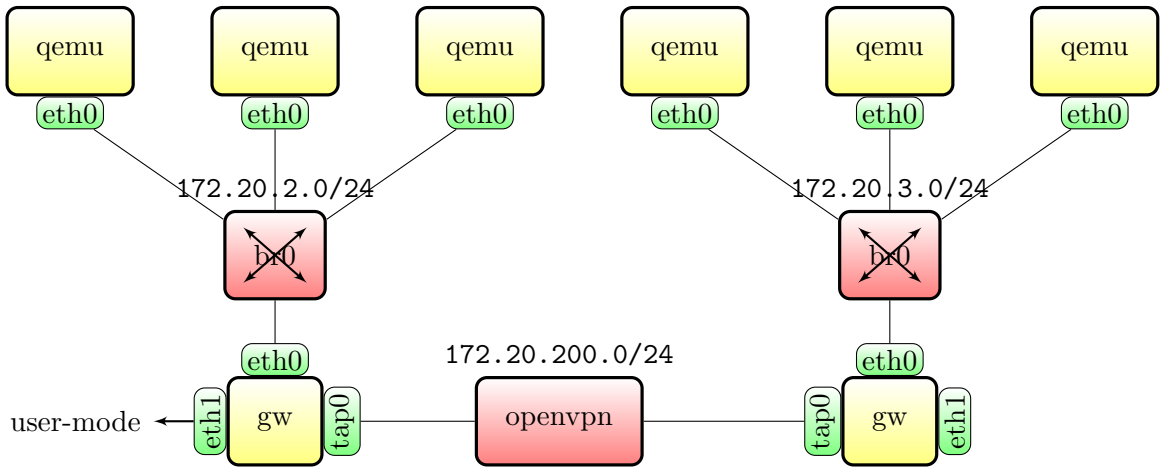

Figura 4: Xarxes segmentades per encaminadors

Per a configurar l'escenari seguiu els passos següents:

1. Configureu la xarxa virtual del grup amb el br0 com ja s'ha descrit.
2. Creeu una màquina virtual nova anomenada gw i doneu-li dues interfícies de xarxa, una connectada al br0 i l'altra amb xarxa user-mode.

   ```
   kvm gw.img \
     -net nic,vlan=0,macaddr=52:54:00:99:gg:01 -net tap,vlan=0,script=no \
     -net nic,vlan=1,macaddr=52:54:00:99:gg:0a -net user,vlan=1
   ```

3. Configureu la màquina gw amb l'adreça `172.20.gg.1` per la primera interfície i amb DHCP per a la segona (la xarxa user-mode proporcionarà automàticament la IP).
4. Estabiu una connexió amb `OpenVPN` configurada amb l'adreça `172.20.200.gg`. Fixeu-vos que el túnel VPN sortirà per la segona interfície del gw, en cas que ho feu directament al host el túnel sortirà per la interfície connectada a Internet (eth0, wlan0, etc.).
5. Per tal que els sistema operatiu s'avingui a gestionar i reenviar paquets d'altres màquines cal que activeu el forwarding, de manera permanent a `/etc/sysctl.conf`:

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

i executeu els canvis amb sysctl −p /etc/sysctl.conf.

6. Configureu les altres màquines virtuals de manera que tinguin la màquina gw com a encaminador.

7. Configureu la màquina gw de manera que conegui la xarxa local i les xarxes dels altres grups i pugui funcionar com a encaminador per a les altres màquines. Per tal que es faci l'encaminament heu de configurar la taula de rutes convenientment, a més recordeu d'activar el forwarding. La taula de rutes, substituint <gg> pel vostre grup, ha de ser semblant a:

```
Destination         Gateway      Genmask         Iface
default           10.0.2.2       0.0.0.0         eth1
10.0.2.0                *       255.255.255.0   eth1
172.20.gg.0             *       255.255.255.0   eth0
172.20.200.0            *       255.255.255.0   tap0
172.20.2.0     172.20.200.2       255.255.255.0   tap0
172.20.3.0     172.20.200.3       255.255.255.0   tap0
```

Per a les eines d'encaminament, consulteu documentació sobre el nivell de xarxa [Bro07].

Referències

[Bel09] Fabrice Bellard. *QEMU. Open source machine emulator and KVM (Kernel Virtual Machine)*. 2009–2012. URL: http://wiki.qemu.org/ (consultat 17 de des. de 2012).

[blo18] Stan's blog. *Bridge with lxc-net*. 1 de febr. de 2018. URL: https://stanislas.blog/2018/02/setup-network-bridge-lxc-net/ (consultat 18 de febr. de 2021).

[Bro07] Martin A. Brown. *Guide to IP Layer Network Administration with Linux*. Versió 0.4.5. linux-ip.net, març de 2007. URL: http://linux-ip.net/html/index.html (consultat 11 de gen. de 2013).

[BS01] Daniel J. Barrett i Richard E. Silverman. *SSH, The Secure Shell: The Definitive Guide*. 1a edició. Sebastopol (US–CA): O'Reilly, febr. de 2001. 560 pàgines. ISBN: 978-0-596-00011-0. URL: http://oreilly.com/catalog/sshtdg/chapter/.

[Bö01] Uwe Böhme. *Linux BRIDGE-STP-HOWTO*. Versió 0.04. The Linux Documentation Project. tldp.org, gen. de 2001. URL: http://tldp.org/HOWTO/BRIDGE-STP-HOWTO/index.html (consultat 11 de gen. de 2013).

[Can18] Canonical. *Linux Containers*. 1 de gen. de 2018. URL: https://help.ubuntu.com/lts/serverguide/lxc.html (consultat 1 de gen. de 2018).

[Con18] Linux Containers. *Linux Containers*. 1 de gen. de 2018. URL: https://linuxcontainers.org/lxc/getting-started/ (consultat 1 de gen. de 2018).

[deb17] debian. *Debian simple bridge*. 7 de set. de 2017. URL: https://wiki.debian.org/LXC/SimpleBridge (consultat 18 de febr. de 2021).

[Qem12] Qemu. *Documentation/Networking – QEMU*. 25 de jul. de 2012. URL: http://wiki.qemu.org/Documentation/Networking (consultat 11 de gen. de 2013).

[Wir04] Wireshark Foundation. *The Wireshark Wiki*. 2004–2013. URL: `http://wiki.wireshark.org` (consultat 11 de gen. de 2013).