## Práctica 3

**Apellidos:** Alcausa Luque

**Nombre:** Juan Carlos

**Titulación:** Grado de Ingeniería Informática y Matemáticas

**Grupo: D**

**PC de la práctica:** 528

**Lea el enunciado de la práctica para saber el contexto de cada ejercicio.**

**Recuerde configurar de forma adecuada la máquina virtual como primer paso.**

**Para editar fichero gedit /etc/resolv.conf**

**Ejercicio 1.** Los comandos **ipconfig** de Windows y **ip address** de Linux muestran información sobre las interfaces de red de la máquina. Ejecute esos comandos en una consola de Windows y en la máquina virtual Linux, busque la información de su interfaz física e identifique su IP, máscara y puerta de enlace asociada, y rellene la tabla de abajo.

|  |  |  |
| --- | --- | --- |
|  | Windows | Linux |
| IP | 192.168.164.188 | - |
| Máscara | 255.255.252.0 | - |
| Puerta de enlace | 192.168.167.254 | - |

* ¿Está el Linux de la máquina virtual en la misma red IPv4 que el Windows de la máquina huésped? ¿Por qué? No, no hay ninguna dirección IPv4 en Linux. En Linux por defecto se genera una dirección IPv6 con base en la dirección física
* ¿A qué se refiere el interfaz “lo” en la máquina virtual (busque información en Internet)? Es el loopback que se usa para pruebas dentro del propio dispositivo

**Ejercicio 2.** Si queremos que la máquina Linux tenga como IP, la misma que la de Windows, pero cambiando el segundo bit más significativo de la parte reservada para los hosts en sus direcciones, ¿cuál debería ser la IP de Linux? Configure la IP y la máscara de subred en Linux con el siguiente comando:

* ip address add <dirIP>/<prefijo> dev <dispositivo>

donde el valor de dispositivo será **enp0s3**, el valor de dirIP el que acaba de calcular; y la máscara la misma que en Windows.

* Comando: ip address add 192.168.165.188/22 dev enp0s3

Ejecute nuevamente el comando **ip address** (sin ningún parámetro adicional) para observar los cambios que se han producido y que todo sea correcto. Salida: inet: 192.168.165.188/22 pero inet6 sigue igual

**Ejercicio 3.** Intente ahora hacer desde Linux un ping[[1]](#footnote-1) a la IP de loopback (127.0.0.1), a las IPs de su máquina (la de Windows y la de Linux) y a una máquina externa a la red (intente tanto por nombre **www.lcc.uma.es** como por IP: **150.214.108.11**) ¿Cuáles funcionan y cuáles no?

* Ping a 127.0.0.1: sí
* Ping a su IP de Linux: sí
* Ping a su IP de Windows: sí
* Ping a la IP del profesor (Linux): sí
* Ping a la IP del profesor (Windows): sí
* Ping a [www.lcc.uma.es](http://www.lcc.uma.es): no (nombre o servicio desconocido)
* Ping a 150.214.108.11: no (red inaccesible)

**Ejercicio 4.** Observe la tabla de encaminamiento de su máquina virtual Linux con el comando **ip route**.

* ¿Cómo explica esta tabla por qué algunos pings de los anteriores funcionan y otros no? Como no tenemos una puerta de enlace predeterminada los paquetes no pueden salir de nuestra subred

**Ejercicio 5.** Además de consultar la tabla de encaminamiento, con el comando **ip route** podemos modificarla:

* Añada una entrada de encaminamiento por defecto usando el **ip route add default via <Gateway>** (como valor de gateway use **192.168.167.254**). Vuelva a probar los pings que fallaron en el ejercicio 3 y comente el motivo por el que ahora funcionan algunos que antes no: Funciona el 150.214.108.11 pero la URL no porque no sabe transformal las URL en IP’s todavía (no le hemos indicado el servidor DNS)
* Finalmente, cree el fichero **/etc/resolv.conf[[2]](#footnote-2)** con la línea **nameserver** 150.214.57.7. ¿Funcionan ahora todos los pings? Sí
* ¿Por qué funcionan los que antes fallaban? Porque no tenía un servidor DNS adecuado asociado

**Ejercicio 6.** Cuando se envía un mensaje al exterior de su red local se hacen dos consultas a su tabla de encaminamiento:

* Primero se busca la entrada que nos lleva al destino final. Al ser externa, se escogerá la entrada por defecto, que nos indica que debemos enviar a la puerta de enlace (su router).
* Luego buscamos la entrada para llegar a nuestro router (la entrada que nos permite comunicarnos con los equipos de nuestra red) que nos dirá que esta comunicación se puede hacer por entrega directa.

Observe la tabla de encaminamiento de Windows (comando route PRINT -4). ¿Qué filas de esa tabla representan las siguientes entradas?

1. Entrada que le permite comunicarse con un equipo su propia red física (diferente al suyo): son tres direcciones: la de nuestro equipo (192.168.164.188), la de otro equipo (192.168.164.188) y la de broadcast dentro de la subred (todos los bits del host a 1, 192.168.167.255)

Entrada por defecto: sería la primera entrada, la que tiene 0.0.0.0 y la dirección sería 192.168.167.254

**Ejercicio 7. Ejercicio 7.** Otro comando útil que nos aporta información sobre las comuniones es **netstat** (funciona tanto en Windows como Linux). Este comando nos ofrece información sobre las conexiones que tenemos en nuestro equipo e incluso qué programas las generan. Esto lo veremos en el Tema 4. También permite examinar estadísticas de los mensajes enviados y recibidos usando la opción **–s**. Ejecute en Windows el comando **netstat –s** y analizando las estadísticas de IPv4 e ICMPv4 (ICMP sobre IPv4), responda a las siguientes preguntas (una breve descripción de cada estadística puede ver en este [enlace](https://loicpefferkorn.net/2018/09/linux-network-statistics-reference/)). Se recomienda tomar una captura de pantalla y analizar los datos sobre ella ya que las estadísticas van cambiando sobre el tiempo:

1. [Estadísticas IPv4] ¿Qué estadística nos indica cuántos paquetes hemos descartado? ¿Qué porcentaje representa sobre el total de datagramas recibidos? Paquetes recibidos descartados: 5515. Sería un 3,47% sobre el total de paquetes recibidos
2. [Estadísticas IPv4] ¿Qué estadística recoge la detección de error en el CHECKSUM? ¿Cuántos potenciales paquetes tienen ese error? Errores de encabezado
3. [Estadísticas ICMPv4] ¿Qué tipo de mensajes ICMP que informan de error ha recibido? Destino inaccesible y ecos
4. [Estadísticas ICMPv4] Indique qué comandos podría utilizar en su equipo para forzar que se generasen más respuestas ICMP de al menos dos tipos diferentes: uno de tiempo agotado haciendo un ping con un TTL muy bajo (tiempo agotado) y otra de eco con un ping correcto

1. Haga los ping con la opción –c 2 para que solo envíe un mensaje ICMP. [↑](#footnote-ref-1)
2. Use nano /etc/resolv.conf [↑](#footnote-ref-2)