## Práctica 2 y 3

**Apellidos:** Camacho Marín

**Nombre:** Sergio

**Titulación:** Grado de Ingeniería informática

**Grupo: A**

**PC de la práctica:** PC 108 (aunque para la parte de Linux me fue necesario utilizar otro ordenador debido a problemas de tiempo)

**Lea el enunciado de la práctica para saber cómo generar el tráfico de cada ejercicio.**

**Ejercicio 1.** Observe la cabecera IP de los diferentes datagramas:

* ¿Qué protocolo se indica en el campo “protocolo” de los datagramas que transportan mensajes DNS, ICMP, FTP y HTTP? Rellene la tabla con dicha información.

|  |  |  |
| --- | --- | --- |
| Protocolo | Campo protocolo | Valor (HEX) |
| DNS | UDP(17) | 0X11 |
| ICMP | ICMP(1) | 0X1 |
| HTTP | TCP(6) | 0X6 |
| FTP | TCP(6) | 0X6 |

* ¿Qué indica este campo? **Este campo indica a qué protocolo hay que entregar el datagrama. Cada protocolo tiene un número asociado.**

**Ejercicio 2.** Seleccione una petición de ICMP (el *echo request*) y complete la siguiente tabla indicando la dirección IP destino (cabecera IP) y la dirección MAC destino (cabecera Ethernet). Repita el proceso con una petición DNS (la pregunta).

|  |  |  |
| --- | --- | --- |
|  | ICMP | DNS |
| Dirección IP destino (cab IP) | 150.214.54.251 | 192.168.164.8 |
| Dirección MAC destino (cab Ethernet) | 00:11:bc:50:00 | 8c:dc:d4:35:9b:15 |

* ¿Por qué en un caso son iguales los destinos y en el otro no? **Esto se debe a que uno de los enviados es recibido y otro es de respuesta a esa trama.**

**Ejercicio 3.** Responda las siguientes preguntas:

* ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)? **Su tipo es 8, y su código es 0**

Para el resto de preguntas y rellena la tabla considere solo las peticiones.

* ¿Qué filtro podría poner para que sólo aparezcan los fragmentos relacionados con un datagrama concreto? **ip.id == <número de identificación>**
* Completa la siguiente tabla, indicando los flags que tiene activo cada fragmento, su identificador y su desplazamiento (para cada tamaño escribe un valor por cada fragmento, separados por comas (,) cuando hay varios fragmentos).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tamaño | Fragmentos | Identificadores | Flags | Desplazamientos |
| 1400 | 1 | 0x4802 | 000 | 0 |
| 3200 | 3 | 0x85d8  0x85d8  0x85d8 | 1º001(MF)  2º001(MF)  3º000(DF) | 1º 0  2º 185  3º 370 |

**Ejercicio 4.** Realice dos pings a **eii.cv.uma.es** con tamaños MAX y MAX+1 y el bit DF activo (MAX es el tamaño máximo calculado). Añada una captura de pantalla.

* ¿Cuál es el valor máximo? **1472**
* ¿Por qué es ese tamaño? **Porque es el MTU(1500) quitando la cabecera IP y la de ICMP.**
* ¿En la traza de wireshark aparece el segundo ping? ¿Por qué?

**No aparece dentro de la traza wireshark debido a que excede el tamaño de envío y es necesario fragmentar, pero como se especifica no fragmentar, no es posible hacer un request, por lo tanto no aparece.**

**Ejercicio 5.** Haga un ping a **eii.cv.uma.es** usando un TTL creciente, empezando por 1 y deteniéndose cuando se empiece a recibir una respuesta del servidor. Observe en Wireshark el intercambio de paquetes que se produce.

* ¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)?**Tipo 11, código 0 y su significado es que el tiempo de vida del paquete ha sido excedido en el tránsito de respuesta.**
* ¿Qué incluye dicho mensaje ICMP como información adicional?

**Un encapsulado que contiene un datagrama IP, en el cual se muestran todos los datos del ping que se intenta hacer, con su consecuente protocolo ICMP que sería parte del datagrama original que ha provocado el error.**

**Ejercicio 6.** Responda a las siguientes preguntas:

* ¿Qué tipo de paquetes (protocolo de más alto nivel) usa **tracert** para hacer su función?

**UDP, TCP y ICMP**

* Además de los mensajes propios para obtener el camino, **tracert** puede provocar que se realicen otros envíos auxiliares para conseguir información o mostrar de forma más amistosa la información, ¿qué otros mensajes pueden ser necesarios? **El comando tracert te muestra la información del router destino, así como la ruta seguida por el enrutamiento hasta llegar a ese destino, con los tiempos de acceso a esos routers.**
* ¿Qué estrategia usa **tracert** para averiguar qué máquina hay en cada salto del paquete? **La estrategia de tracert es provocar un error por TTL en el router en el que accede por direccionamiento para que este le envíe una respuesta de error, con esto ya sabe que en ese salto se enruta por ese sitio.**

**Ejercicio 7.** Los comandos **ipconfig** de Windows y **/sbin/ifconfig** 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 (haga capturas y márquelas). **IP: 192.168.164.89, Máscara:255.255.252.0 y GateWay debido a que no ejecute route(en caso contrario, aparecería en default).**
* ¿Está el Linux de la máquina virtual en la misma red IPv4 que el Windows de la máquina huésped? ¿Por qué? **No, esto se debe a que tiene distinta red virtual que la máquina virtual.**
* ¿A qué se refiere el interfaz “lo” en la máquina virtual?**Es una interfaz de red virtual. Que le corresponden direcciones loopback, las cuales se suele utilizar cuando una transmisión de datos tiene como destino el propio host.**

**Ejercicio 8.** 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? **192.168.165.89**
* Configure la IP y la máscara de subred en Linux con el siguiente comando: /sbin/ifconfig <dispositivo> <dir IP> netmask <máscara> donde el valor de dispositivo será **eth0** y el valor de la dirIP que acaba de calcular y la máscara que sea igual que en Windows.**/sbin/ifconfig <dispositivo> <192.168.165.89> netmask <255.255.252.0>**

**Ejercicio 9.** Intenta ahora hacer desde Linux un ping a la IP de loopback (127.0.0.1), la IP del Windows de su propia máquina, a la IP de la máquina del profesor (Linux y Windows) y a una máquina externa a la red (intente tanto por nombre **eii.cv.uma.es** como por IP: **150.214.54.251**)

* ¿Cuáles funcionan y cuáles no?**Funcionan todos los pings menos (eii.cv.uma.es) y (150.214.54.251).**

**Ejercicio 10.** Observe la tabla de encaminamiento con el comando **/sbin/route**.

* ¿Cómo explica esta tabla por qué algunos pings de los anteriores funcionan y otros no?

**Porque falta la puerta de enlace(gateway) que sirve para interconectar redes, y siendo eii.cv.uma.es y su dirección ip, redes externas, no se puede acceder si no se dispone de una configuración.**

**Ejercicio 11.** Añada una entrada de encaminamiento por defecto (192.168.167.254 como gw).

* Vuelva a probar los pings que fallaron en el ejercicio 9 y comente el motivo por el que ahora funcionan algunos que antes no. **Funcionan todos menos eii.cv.uma.es, pero es porque está configurado la entrada de encaminamiento para el caso de su IP.**
* Edite el fichero /etc/resolv.conf y añada al final la línea **nameserver** 150.214.57.7. ¿Funcionan ahora todos los pings? ¿Por qué cree que funcionan los que antes fallaban?**Ahora funcionan todos los pings, esto se debe a que se tiene la entrada de encaminamiento que dispone el enlace a la IP de eii.cv.uma.es y, el caso especial, es que al introducir nameserver se obtiene de la dirección eii.cv.uma.es, su dirección IP, por lo que ahora sí funciona.**

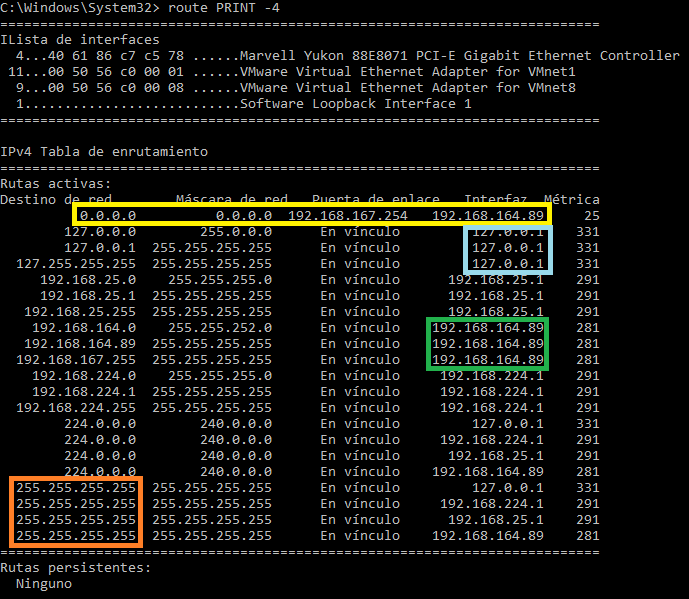
**Ejercicio 12.** Observe la tabla de encaminamiento de Windows (comando **route PRINT -4**). Haga una captura donde se vea todas las entradas de la tabla y sobre esa imagen **marque** los siguientes elementos:

a) Entradas referidas a la interfaz de loopback**(azul)**

b) Entradas de su interfaz física que le permite comunicarse con su propia red**(verde)**

c) Entrada por defecto**(amarilla)**

d) Entradas relacionadas con multicast**(naranja)**

****

**Ejercicio 13.** Explique los principales elementos del código desarrollado para este ejercicio.

**No he entendido estos ejercicios finales, debido a que no recuerdo haber escuchado nada en clase y no encuentro contexto de enlace entre estos dos ejercicios y los demás.**

**Ejercicio 14:** Pruebe su programa con la IP/máscara del equipo del laboratorio (en Windows).

* ¿Qué clase de dirección es?
* ¿Es coherente la máscara usada con la clase?
* En caso negativo, ¿qué nombre recibe el esquema que permite tal incoherencia?