PDI - TP 1 - B

Alumnos:
Alonso Facundo
Alvarez Poli Bautista
Kloster Agustin

El concepto básico de sockets a bajo nivel es enviar un solo paquete por vez con todos los encabezados de los protocolos completados dentro del programa en lugar de usar el kernel.

Unix provee dos tipo de sockets para el acceso directo a la red:

SOCK_PACKET, recibe y envía datos al dispositivo ubicado en la capa de enlace. Esto significa que el "header" de la placa de red incluido en los datos puede ser escrito o leído. En general es el header de Ethernet. Todos los encabezados de los protocolos subsecuentes también deben ser incluidos en los datos.

SOCK_RAW, es el que usaremos por ahora, que incluye los encabezados IP, protocolos y datos subsecuentes.

Desde el momento que lo creamos se puede enviar cualquier tipo de paquetes IP por este socket. También se pueden recibir cualquier tipo de paquetes que lleguen al host, después que el socket fue creado, si se hace un "read()" desde él. Se puede observar que aunque el socket es una interfaz al header IP, es tambiés específico para una capa de transporte. Esto significa que para escuchar tráfico TCP, UDP, ICMP hay que crear 3 raw sockets por separado, usando IPPROTO_TCP, IPPROTO_UDP y IPPROTO_ICMP (números de protocolo son 0 ó 6 para tcp, 17 para udp y 1 para icmp).

Con esta información es posible crear un simple "sniffer", que muestre todo el contenido de los paquetes TCP que se reciban. (En este ejemplo se evitan los headers IP y TCP, y se imprime solamente el "payload" con encabezados IP y TCP contenidos en el paquete).

- Utilizando el código raw.c como base escribir un "sniffer" que es un programa que muestra el contenido del tráfico que llega.

```
08 4B 92 32 82 24 01 00 00 14 F9 00 00 10 D9 00
00 00 05 05 00 00 08 63 01 00 00 14 FA 00 00 10
D9 00 00 00 05 07 00 00 08 63
Paquete TCP - Puerto de origen: 51500, Puerto de destino: 40435
Datos:
02 00 FE 28 00 00 01 01 08 0A 08 4B 92 34
08 4B 92 34
Paquete TCP - Puerto de origen: 51500, Puerto de destino: 40435
Datos:
02 00 FE 3B 00 00 01 01 08 0A 08 4B 92 79
08 4B 92 34 82 8D 1B E1 AC 4A 12 E1 AC 4A 1B E1
AC 5E E1 E1 AC 4A 1B
Paquete TCP - Puerto de origen: 40435, Puerto de destino: 51500
Datos:
4B F3 FE 28 00 00 01 01 08 0A 08 4B 92 A7
08 4B 92 79
Paquete TCP - Puerto de origen: 40435, Puerto de destino: 51500
Datos:
4B F3 FE 37 00 00 01 01 08 0A 08 4B 94 08
08 4B 92 79 82 0D 09 00 00 00 00 00 00 10 D9 00
00 00 00
Paquete TCP - Puerto de origen: 51500, Puerto de destino: 40435
Datos:
02 00 FE 28 00 00 01 01 08 0A 08 4B 94 08
08 4B 94 08
Paquete TCP - Puerto de origen: 40435, Puerto de destino: 33868
Datos:
02 00 FF 02 00 00 01 01 08 0A 08 4B 96 18
08 4B 92 30 82 7E 00 D6 01 00 00 07 9A 00 00 07
22 00 00 00 C9 04 02 06 CC 01 06 0A 04 01 05 BD
```

- Enviar tráfico al "sniffer" desde el cliente escrito en la parte A del TP1

```
6D 70 6F 3A 20 30 2E 30 30 30 30 38 35 0A
Paquete TCP - Puerto de origen: 35220, Puerto de destino: 8081
Datos:
02 00 FE 28 00 00 01 01 08 0A 08 4C 7C 23
08 4C 7C 23
Paquete TCP - Puerto de origen: 8081, Puerto de destino: 35220
Datos:
02 00 FE 28 00 00 01 01 08 0A 08 4C 7C 23
08 4C 7C 23
Paquete TCP - Puerto de origen: 40435, Puerto de destino: 51500
Datos:
4B F3 FE 4E 00 00 01 01 08 0A 08 4C 7C 24
08 4C 7C 22 82 24 01 00 00 15 F0 00 00 11 56 00
00 00 05 05 00 00 08 DE 01 00 00 15 F1 00 00 11
56 00 00 00 05 07 00 00 08 DE
Paquete TCP - Puerto de origen: 51500, Puerto de destino: 40435
Datos:
02 00 FE 28 00 00 01 01 08 0A 08 4C 7C 24
08 4C 7C 24
Paquete TCP - Puerto de origen: 40435, Puerto de destino: 33868
Datos:
02 00 FE 40 00 00 01 01 08 0A 08 4C 7C 24
08 4C 7C 22 82 16 01 00 00 08 55 00 00 07 D3 00
00 00 09 04 02 06 C9 01 06 F4 07 00
Paquete TCP - Puerto de origen: 33868, Puerto de destino: 40435
Datos:
5F FB FE 28 00 00 01 01 08 0A 08 4C 7C 25
08 4C 7C 24
Paquete TCP - Puerto de origen: 33868, Puerto de destino: 40435
Datos:
5F FB FE 43 00 00 01 01 08 0A 08 4C 7C 26
08 4C 7C 24 82 95 CF 94 8D 29 CE 94 8D 2E 1B 94
8D 21 9A 94 8D 29 C7 90 8F 2F AA 92 79 2E CF
Paquete TCP - Puerto de origen: 40435, Puerto de destino: 33868
Datos:
02 00 FF 1D 00 00 01 01 08 0A 08 4C 7C 2A
08 4C 7C 26 82 7E 00 F1 01 00 00 08 56 00 00 07
D4 00 00 00 82 04 02 06 CC 01 06 8B 01 05 78 7B
22 69 64 22 3A 36 2C 22 65 76 65 6E 74 22 3A 22
5C 72 5C 6E 53 65 72 76 69 64 6F 72 20 3A 20 46
61 63 74 6F 72 69 61 6C 3A 20 31 5C 72 5C 6E 50
69 64 20 68 69 6A 6F 3A 20 30 5C 72 5C 6E 50 69
64 20 70 61 64 72 65 3A 20 37 33 32 31 5C 72 5C
6E 54 69 65 6D 70 6F 3A 20 30 2E 30 30 30 30 38
35 5C 72 5C 6E 49 6E 67 72 65 73 65 20 74 65 78
74 6F 20 3A 20 22 7D 01 00 00 08 57 00 00 07 D4
00 00 00 55 04 02 06 CC 01 06 8B 01 05 4B 7B 22
69 64 22 3A 35 2C 22 65 76 65 6E 74 22 3A 22 4D
65 6E 73 61 6A 65 20 64 65 6C 20 63 6C 69 65 6E
74 65 3A 20 61 73 64 61 73 5C 72 5C 6E 5C 72 5C
6E 52 65 73 70 75 65 73 74 61 20 65 6E 76 69 61
64 61 2E 5C 72 5C 6E 22 7D
Paquete TCP - Puerto de origen: 35220, Puerto de destino: 8081
Datos:
02 00 FE 28 00 00 01 01 08 0A 08 4C 7C 53
08 4C 7C 23
```

- Enviar tráfico ICMP al "sniffer" y mostrar los resultados del LOG con comentarios.

```c
if ((sockfd = socket(AF_INET, SOCK_RAW, IPPROTO_ICMP)) < 0) {
    perror("socket");
    exit(EXIT_FAILURE);
}
```

El archivo icmp.c es un archivo que envía paquetes icmp

```
klos@DESKTOP-8JVJS4P:~$ sudo ./icmp 127.0.0.1
Packet 1 sent to 127.0.0.1
Packet 2 sent to 127.0.0.1
Packet 3 sent to 127.0.0.1
Packet 4 sent to 127.0.0.1
Packet 5 sent to 127.0.0.1
Packet 6 sent to 127.0.0.1
Packet 7 sent to 127.0.0.1
Packet 8 sent to 127.0.0.1
Packet 9 sent to 127.0.0.1
Packet 10 sent to 127.0.0.1
klos@DESKTOP-8JVJS4P:~$
```

```
klos@DESKTOP-8JVJS4P:~$ sudo ./raw
Paquete ICMP
Datos:
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 90 00 00 00 00 00 00 00 08 00 00 00
00 00 00 00 53 E5 74 64 04 00 00 00 50 03 00 00
00 00 00 00
Paquete ICMP
Datos:
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 90 00 00 00 00 00 00 00 08 00 00 00
00 00 00 00 53 E5 74 64 04 00 00 00 50 03 00 00
00 00 00 00
Paquete ICMP
Datos:
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 08 00 7F 6A C3 47 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
Paquete ICMP
Datos:
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 08 00 7F 6A C3 47 01 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
Paquete ICMP
Datos:
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 08 00 E7 05 C3 47 02 00 00 00 00 00
```