

PRÁCTICA 4

Viktor Yosava

`vikyosava@uma.es`

Redes y Sistemas Distribuidos. Ingeniería de la Salud

1 Análisis con Wireshark de los protocolos IP e ICMP

Tarea 1. Identificación IP de la máquina

Paso 1

Ejercicio 1.

Observe la salida ¿Qué incluye la información proporcionada? Captura la salida y detalla esta información. ¿cuántas interfaces aparecen? Indica las que te parezcan más relevantes

```
C:\Users\vikto>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : DESKTOP-S5U80TK
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Killer E2600 Gigabit Ethernet Controller
Dirección física. . . . . : 08-97-98-BA-05-FC
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Conexión de área local* 1:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Dirección física. . . . . : 9C-29-76-F8-39-6F
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Conexión de área local* 10:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Dirección física. . . . . : 9E-29-76-F8-39-6E
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Dirección física. . . . . : 9C-29-76-F8-39-6E
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::8541:a96f:817:11d6%12(Preferido)
Dirección IPv4. . . . . : 192.168.1.4(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : domingo, 22 de enero de 2023 10:19:24
La concesión expira . . . . . : lunes, 23 de enero de 2023 14:53:08
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 127674742
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2A-8D-83-6D-08-97-98-BA-05-FC
Servidores DNS. . . . . : 8.8.8.8
                        192.168.1.1
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Fig. 1. ipconfig /all

La información proporcionada me muestra la configuración IP de Windows seguida de la configuración completa de TCP/IP para todos los adaptadores de mi equipo.

Aparecen 4 interfaces, 2 físicas: *Adaptador de Ethernet Ethernet* y *Adaptador de LAN inalámbrica Wi-Fi*; y 2 lógicas: *Adaptador de LAN inalámbrica Conexión de área local* 1* y *Adaptador de LAN inalámbrica Conexión de área local* 10*.

Ejercicio 2.

Detalla la configuración de red de tu máquina (dirección IP, máscara, gateway/pasarela, dns) que puedas extraer de este comando.

```
Dirección IPv4. . . . . : 192.168.1.4(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidores DNS. . . . . : 8.8.8.8
                        192.168.1.1
```

Fig. 2. Configuración red

Dirección IP: 192.168.1.4

Máscara: 255.255.255.0

Gateway: 192.168.1.1

DNS: 8.8.8.8 y 192.168.1.1

Paso 2

La IP que aparece en la página (171.33.234.238) no coincide con la dada por el comando anterior. Esto se debe a que mi IPv4 pública debe ser única para mi router, y este se encarga de asignar una IP privada a cada uno de mis dispositivos gracias al protocolo NAT.

Tarea 2. Tabla de Encaminamiento

```
C:\Users\vikto>netstat -r

=====
Lista de interfaces
 8...08 97 98 ba 05 fc .....Killer E2600 Gigabit Ethernet Controller
17...9c 29 76 f8 39 6f .....Microsoft Wi-Fi Direct Virtual Adapter
13...9e 29 76 f8 39 6e .....Microsoft Wi-Fi Direct Virtual Adapter #2
12...9c 29 76 f8 39 6e .....Intel(R) Wi-Fi 6 AX201 160MHz
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz  Métrica
 0.0.0.0            0.0.0.0            192.168.1.1          192.168.1.4    35
 127.0.0.0          255.0.0.0          En vínculo           127.0.0.1    331
 127.0.0.1          255.255.255.255    En vínculo           127.0.0.1    331
127.255.255.255    255.255.255.255    En vínculo           127.0.0.1    331
192.168.1.0         255.255.255.0      En vínculo           192.168.1.4    291
192.168.1.4         255.255.255.255    En vínculo           192.168.1.4    291
192.168.1.255       255.255.255.255    En vínculo           192.168.1.4    291
224.0.0.0           240.0.0.0          En vínculo           127.0.0.1    331
224.0.0.0           240.0.0.0          En vínculo           192.168.1.4    291
255.255.255.255     255.255.255.255    En vínculo           127.0.0.1    331
255.255.255.255     255.255.255.255    En vínculo           192.168.1.4    291
=====
Rutas persistentes:
Ninguno

IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica      Puerta de enlace
 1  331 ::1/128                      En vínculo
12  291 fe80::/64                    En vínculo
12  291 fe80::8541:a96f:817:11d6/128
    En vínculo
 1  331 ff00::/8                      En vínculo
12  291 ff00::/8                      En vínculo
=====
Rutas persistentes:
Ninguno
```

Fig. 3. netstat -r

Ejercicio 3.

Observe la salida ¿Qué incluye la información proporcionada? Captura la salida y detalla esta información.

La información muestra la tabla de enrutamiento de mi dispositivo.

La lista de interfaces muestra el número de interfaz asignado a cada red.

Las tablas de enrutamiento IPv4 e IPv6 muestran respectivamente las rutas IPv4 e IPv6 conocidas.

Ejercicio 4.

¿Puedes completar la configuración de red con la información de la tabla de encaminamiento?

No es posible ya que no muestra la dirección DNS.

Tarea 3. Encapsulamiento en IP

Ejercicio 6.

¿Qué protocolo se indica en el campo “protocolo” de la cabecera de los datagramas IP que transportan mensajes DNS e ICMP? ¿Por qué no aparece ARP en el campo de protocolo en ningún datagrama?

Protocol		
DNS	Protocol: UDP (17)	Identification: 0x3128 (12584)
ICMP	Protocol: ICMP (1)	Identification: 0x4a1d (18973)

Fig. 4. Campos de la cabecera IP

En el caso de DNS aparece UDP en el campo ”protocolo”, en el caso de ICMP aparece ICMP (1).

ARP no aparece debido a que hace uso de direcciones MAC en lugar de IPv4.

Tarea 4. Fragmentación en IP

Ejercicio 7.

¿Cuál es el tipo de mensaje ICMP enviado como consecuencia del comando PING y su código en la cabecera ICMP? (Tipo y código son dos campos de la cabecera ICMP) ¿Cuántos fragmentos se observan que salen de la máquina? ¿Cuántos fragmentos de respuesta entran? ¿En qué fragmento muestra Wireshark la cabecera ICMP? ¿En cuál de ellos se ve realmente la cabecera de ICMP? Indica en la siguiente tabla los flags que tiene activo cada fragmento, su identificador y su desplazamiento (para cada tamaño escribe un valor por cada fragmento)

```

C:\Users\vikto>ping bing.com -l 1100

Haciendo ping a bing.com [13.107.21.200] con 1100 bytes de datos:
Respuesta desde 13.107.21.200: bytes=1100 tiempo=13ms TTL=121
Respuesta desde 13.107.21.200: bytes=1100 tiempo=14ms TTL=121
Respuesta desde 13.107.21.200: bytes=1100 tiempo=15ms TTL=121
Respuesta desde 13.107.21.200: bytes=1100 tiempo=13ms TTL=121

Estadísticas de ping para 13.107.21.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 13ms, Máximo = 15ms, Media = 13ms

C:\Users\vikto>ping bing.com -l 3100

Haciendo ping a bing.com [13.107.21.200] con 3100 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 13.107.21.200:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\vikto>ping bing.com -l 5200

Haciendo ping a bing.com [13.107.21.200] con 5200 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 13.107.21.200:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

```

Fig. 5. Resultados al hacer ping con distintos tamaños

```

▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0

```

Fig. 6. Tipo de mensaje ICMP enviado y código

ICMP	1142	Echo (ping)	request
ICMP	1142	Echo (ping)	reply
ICMP	1142	Echo (ping)	request
ICMP	1142	Echo (ping)	reply
ICMP	1142	Echo (ping)	request
ICMP	1142	Echo (ping)	reply
ICMP	1142	Echo (ping)	request
ICMP	1142	Echo (ping)	reply
ICMP	182	Echo (ping)	request
ICMP	182	Echo (ping)	request
ICMP	182	Echo (ping)	request
ICMP	182	Echo (ping)	request
ICMP	802	Echo (ping)	request
ICMP	802	Echo (ping)	request
ICMP	802	Echo (ping)	request
ICMP	802	Echo (ping)	request

Fig. 7. Paquetes que salen y entran

Como podemos observar en la imagen anterior, solo es necesario un fragmento para enviar 1100 bytes a la vez. También vemos que no es posible hacer ping con los mensajes de 3100 bytes y 5200 bytes, esto es debido a que la página se protege de ataques de denegación de servicio.

Wireshark muestra la cabecera ICMP en todos los fragmentos, pero realmente vemos la cabecera en los de respuesta.

Tamaño	Fragmentos	Identificadores	Flags	Desplazamientos
1100	1	0x076e (1902)	0x0	0
3100	1	0x0772 (1906)	0x0	2960
5200	1	0x0776 (1910)	0x0	4440

Fig. 8. Tabla de fragmentos

Como no llega a haber respuesta y los desplazamientos mantienen el mismo valor en los envíos de los paquetes, nunca llega a haber más de un fragmento.

Ejercicio 8.

Podemos activar el flag DF (don't fragment) usando la opción `-f` en el comando ping. Realice un ping a la página web de `bing.com` con tamaños 1000 y 3000 y el bit DF activo. ¿Funciona el ping en los dos casos? ¿Cuántos fragmentos hay ahora en cada caso? ¿Qué utilidad puede tener el pedir que no se fragmenten los paquetes para el administrador de una red?

```
C:\Users\vikto>ping bing.com -l 1000 -f

Haciendo ping a bing.com [13.107.21.200] con 1000 bytes de datos:
Respuesta desde 13.107.21.200: bytes=1000 tiempo=14ms TTL=121
Respuesta desde 13.107.21.200: bytes=1000 tiempo=15ms TTL=121
Respuesta desde 13.107.21.200: bytes=1000 tiempo=15ms TTL=121
Respuesta desde 13.107.21.200: bytes=1000 tiempo=15ms TTL=121

Estadísticas de ping para 13.107.21.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 14ms, Máximo = 15ms, Media = 14ms

C:\Users\vikto>ping bing.com -l 3000 -f

Haciendo ping a bing.com [13.107.21.200] con 3000 bytes de datos:
Es necesario fragmentar el paquete pero se especificó DF.
Es necesario fragmentar el paquete pero se especificó DF.
Es necesario fragmentar el paquete pero se especificó DF.
Es necesario fragmentar el paquete pero se especificó DF.

Estadísticas de ping para 13.107.21.200:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
        (100% perdidos),
```

Fig. 9. Resultados al hacer ping sin fragmentos

En el primer caso el ping funciona sin problemas, habiendo un único fragmento.

En el segundo caso el ping no funciona, esta vez debido a que es necesario fragmentar el mensaje de 3000 bytes.

Pedir que no se fragmenten los datos podría ser útil en caso de que queramos reducir el número de operaciones, ayudando al rendimiento global y de los routers.

2 Utilizar Wireshark para capturar y analizar tramas de Ethernet IP e ICMP

Tarea 1. Utilización de Wireshark para capturar y analizar tramas de Ethernet II

Ejercicio 1.

Haga una captura de pantalla de Wireshark donde se muestren únicamente las tramas de los protocolos indicados.

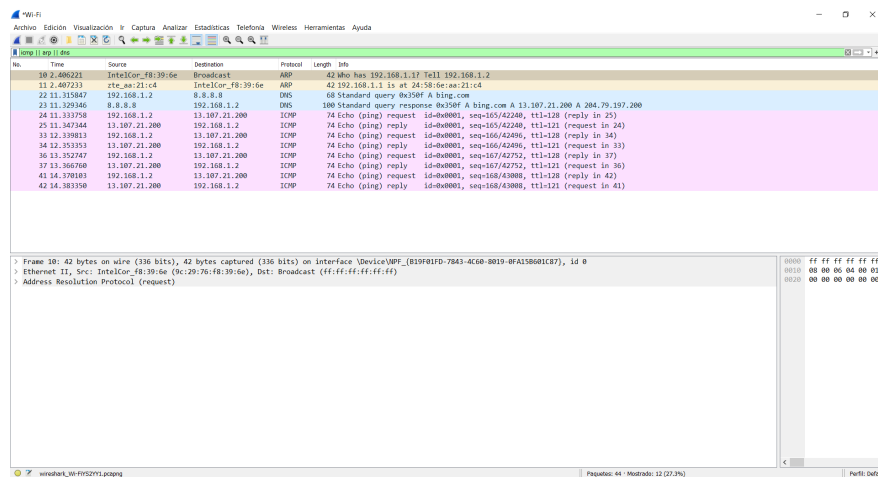


Fig. 10. Wireshark

Ejercicio 2.

Analizando la traza capturada de Wireshark del comando ping complete la información requerida.

Información de la dirección MAC de su computadora.

Dirección MAC: 9c:29:76:f8:39:6e

Fabricante de NIC: 9c:29:76

Número de serie de NIC: f8:39:6e

10	2.406221	IntelCor_f8:39:6e	Broadcast	ARP	42 Who has 192.1
11	2.407233	zte_aa:21:c4	IntelCor_f8:39:6e	ARP	42 192.168.1.1 i
22	11.315847	192.168.1.2	8.8.8.8	DNS	68 Standard quer
23	11.329346	8.8.8.8	192.168.1.2	DNS	100 Standard quer
24	11.333758	192.168.1.2	13.107.21.200	ICMP	74 Echo (ping) r
25	11.347344	13.107.21.200	192.168.1.2	ICMP	74 Echo (ping) r
33	12.339813	192.168.1.2	13.107.21.200	ICMP	74 Echo (ping) r
34	12.353353	13.107.21.200	192.168.1.2	ICMP	74 Echo (ping) r
36	13.352747	192.168.1.2	13.107.21.200	ICMP	74 Echo (ping) r
37	13.366760	13.107.21.200	192.168.1.2	ICMP	74 Echo (ping) r
41	14.370103	192.168.1.2	13.107.21.200	ICMP	74 Echo (ping) r
42	14.383350	13.107.21.200	192.168.1.2	ICMP	74 Echo (ping) r

```

<
> Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF{...}
> Ethernet II, Src: IntelCor_f8:39:6e (9c:29:76:f8:39:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_f8:39:6e (9c:29:76:f8:39:6e)
    Sender IP address: 192.168.1.2
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1

```

Fig. 11. Información de la dirección MAC de la computadora.

Información de la dirección MAC de Gateway/router:

Dirección MAC: 24:58:6e:aa:21:c4

Fabricante de NIC: 24:58:6e

Número de serie de NIC: aa:21:c4

10	2.406221	IntelCor_f8:39:6e	Broadcast	ARP	42	Who has 192.1
11	2.407233	zte_aa:21:c4	IntelCor_f8:39:6e	ARP	42	192.168.1.1 i
22	11.315847	192.168.1.2	8.8.8.8	DNS	68	Standard quer
23	11.329346	8.8.8.8	192.168.1.2	DNS	100	Standard quer
24	11.333758	192.168.1.2	13.107.21.200	ICMP	74	Echo (ping) r
25	11.347344	13.107.21.200	192.168.1.2	ICMP	74	Echo (ping) r
33	12.339813	192.168.1.2	13.107.21.200	ICMP	74	Echo (ping) r
34	12.353353	13.107.21.200	192.168.1.2	ICMP	74	Echo (ping) r
36	13.352747	192.168.1.2	13.107.21.200	ICMP	74	Echo (ping) r
37	13.366760	13.107.21.200	192.168.1.2	ICMP	74	Echo (ping) r
41	14.370103	192.168.1.2	13.107.21.200	ICMP	74	Echo (ping) r
42	14.383350	13.107.21.200	192.168.1.2	ICMP	74	Echo (ping) r

```

<
> Frame 11: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF...
> Ethernet II, Src: zte_aa:21:c4 (24:58:6e:aa:21:c4), Dst: IntelCor_f8:39:6e (9c:29:76:f8:39:6e)
  Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: zte_aa:21:c4 (24:58:6e:aa:21:c4)
    Sender IP address: 192.168.1.1
    Target MAC address: IntelCor_f8:39:6e (9c:29:76:f8:39:6e)
    Target IP address: 192.168.1.2

```

Fig. 12. Información de la dirección MAC de Gateway/router.

Ejercicio 3.

Si observa la traza obtenida, notará que en ningún momento aparece la dirección MAC para **www.bing.com**. ¿Sabría decir por qué? ¿Existiría alguna forma de obtenerla?

No es posible obtenerla porque **www.bing.com** es un dominio, mientras que las direcciones MAC son direcciones únicas que pertenecen a dispositivos. Para poder acceder a una MAC, el dispositivo debe estar conectado a la misma red que el mío.