

Memoria de las prácticas

A día 5 de mayo de 2021

Primer bloque de prácticas:

- Práctica 1. Tramas en Wireshark
- Práctica 2. Análisis protocolos IP e ICMP
- Práctica 3. Configuración de red

Marcos Hidalgo Baños

GRADO DE INGENIERÍA INFORMÁTICA - GRUPO D
SUBGRUPO DE PRÁCTICAS 3

Práctica 1

Apellidos: **Hidalgo Baños**

Nombre: **Marcos**

Titulación: **Grado de Ing. Informática D**

Grupo: **Grupo3**

PC de la práctica: **Ordenador Propio**

Ejercicio 1. Elija un mensaje http, y localice en la cabecera Ethernet II

- **Número de trama elegida:** 707
- **Información de la dirección MAC de su computadora:**
 - Dirección MAC (en hexadecimal): *88:b1:11:ac:91:62*
 - Fabricante de NIC (en hexadecimal): *88:b1:11*
 - Nombre: *Intel Corporate*
 - Número de serie de NIC (en hexadecimal): *ac:91:62*
- **Información de la dirección MAC de gateway/router:**
 - Dirección MAC (en hexadecimal): *d8:fb:5e:c2:87:c9*
 - Fabricante de NIC (en hexadecimal): *d8:fb:5e*
 - Nombre: *Askey Computer Corp*
 - Número de serie de NIC (en hexadecimal): *c2:87:c9*

No.	Time	Source	Destination	Protocol	Length	Info
94	22.354408	192.168.1.51	5.255.145.9	HTTP	334	GET /msdownload/update/v3/static/trustedr/en/a
97	22.375995	5.255.145.9	192.168.1.51	HTTP	320	HTTP/1.1 304 Not Modified
698	43.410694	192.168.1.51	150.214.57.91	HTTP	494	GET / HTTP/1.1
700	43.450437	150.214.57.91	192.168.1.51	HTTP	597	HTTP/1.1 301 Moved Permanently (text/html)
707	43.505652	192.168.1.51	150.214.40.97	HTTP	499	GET /etsi-informatica/ HTTP/1.1
709	43.539608	150.214.40.97	192.168.1.51	HTTP	155	HTTP/1.1 301 Moved Permanently
735	44.172328	192.168.1.51	88.221.52.56	HTTP	315	GET /connectiontest.html HTTP/1.1
737	44.189491	88.221.52.56	192.168.1.51	HTTP	302	HTTP/1.1 200 OK (text/html)

> Frame 707: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits) on interface \Device\NPF_{35E0075D-D5BA-4D73-8E00-...}

▼ Ethernet II, Src: IntelCor_ac:91:62 (88:b1:11:ac:91:62), Dst: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

> Destination: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

> Source: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

Type: IPv4 (0x0800)

Ejercicio 2. Indique qué filtro debe añadir para que se muestren las tramas donde no se utilice su dirección MAC.

- **¿Qué filtro usó?**
eth.src ne 88:b1:11:ac:91:62 and eth.dst ne 88:b1:11:ac:91:62
- **¿Cuántas tramas muestra Wireshark?**
36 tramas de 16320, lo que supone un 0.2 %
- **¿Por qué recibe esas tramas?**
Tal y como indica el filtro, se muestran aquellas tramas que no contienen la dirección MAC de mi ordenador. Que una trama no contenga esta dirección no quiere decir que no se envíe o reciba desde la red.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	224.0.0.1	IGMPv2	46	Membership Query, general
2	0.001238	fe80::dafb:5eff:fec::ff02::1	ff02::1	ICMPv6	90	Multicast Listener Query
9	2.762404	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
17	4.916373	192.168.1.56	255.255.255.255	UDP	71	9999 → 9999 Len=29
18	8.910758	fe80::dafb:5eff:fec::ff02::1	ff02::1	ICMPv6	78	Router Advertisement from d8:fb:5e:c2:87:c9
28	12.901297	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
51	15.051494	192.168.1.1	224.0.0.1	IGMPv2	46	Membership Query, general
52	15.051694	fe80::dafb:5eff:fec::ff02::1	ff02::1	ICMPv6	90	Multicast Listener Query
59	15.361285	192.168.1.56	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
100	24.577682	192.168.1.69	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
101	24.578154	192.168.1.69	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
251	29.796620	192.168.1.1	224.0.0.1	IGMPv2	46	Membership Query, general
252	29.797609	fe80::dafb:5eff:fec::ff02::1	ff02::1	ICMPv6	90	Multicast Listener Query
261	30.103882	192.168.1.73	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
262	30.108464	192.168.1.73	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
394	33.483745	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
395	33.489701	fe80::dafb:5eff:fec::ff02::1	ff02::1	ICMPv6	78	Router Advertisement from d8:fb:5e:c2:87:c9
715	43.621877	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
892	44.863015	192.168.1.1	224.0.0.1	IGMPv2	46	Membership Query, general
893	44.863015	fe80::dafb:5eff:fec::ff02::1	ff02::1	ICMPv6	90	Multicast Listener Query
1161	45.160137	192.168.1.73	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
1162	45.161925	192.168.1.73	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
6057	49.463927	192.168.1.69	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
6059	49.467820	192.168.1.69	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
6346	49.771170	192.168.1.56	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QN" question
6347	49.771170	192.168.1.56	224.0.0.251	MDNS	132	Standard query 0x0000 SRV google-nest-mini-0eb33069e3c9d02f815420b1645e0826._googlecast._tcp.local, "QN" qu...
6348	49.775263	192.168.1.56	224.0.0.251	MDNS	426	Standard query response 0x0000 PTR Google-Nest-Mini-0eb33069e3c9d02f815420b1645e0826._googlecast._tcp.local...
6349	49.777614	192.168.1.56	224.0.0.251	MDNS	199	Standard query response 0x0000 SRV, cache flush 0 0 8009 0eb33069e3c9-d02f-8154-20b1645e0826.local A, cach...

Frame 395: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{35E0075D-D58A-4073-8E00-61D525B148A5}, id 0

Ethernet II, Src: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9), Dst: IPv6cast_01 (33:33:00:00:00:01)

Destination: IPv6cast_01 (33:33:00:00:00:01)

Source: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

Type: IPv6 (0x86dd)

Internet Protocol Version 6, Src: fe80::dafb:5eff:fec2:87:c9, Dst: ff02::1

Internet Control Message Protocol v6

Source Hardware Address (eth.src), 6 bytes

Packets: 16320 · Displayed: 36 (0.2%) · Dropped: 0 (0.0%) · Profile: Default

Ejercicio 3. Dibuje la torre de protocolos (tal como se ha visto en clase, es decir, en la parte inferior los protocolos de más bajo nivel) de un paquete ARP, uno ICMP, uno DNS y uno HTTP.

- Torre de protocolos de un paquete ARP (número de trama seleccionada: 75)

Ethernet II
ARP

No.	Time	Source	Destination	Protocol	Length	Info
9	2.762404	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
19	8.968749	IntelCor_ac:91:62	Broadcast	ARP	42	Who has 192.168.1.56? Tell 192.168.1.51
21	9.317913	Google_3c:94:ee	IntelCor_ac:91:62	ARP	42	192.168.1.56 is at f0:ef:86:3c:94:ee
28	12.901297	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
30	13.226569	IntelCor_ac:91:62	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.51
31	13.229353	AskeyCom_c2:87:c9	IntelCor_ac:91:62	ARP	42	192.168.1.1 is at d8:fb:5e:c2:87:c9
74	18.925400	AskeyCom_c2:87:c9	IntelCor_ac:91:62	ARP	42	Who has 192.168.1.51? Tell 192.168.1.1
75	18.925462	IntelCor_ac:91:62	AskeyCom_c2:87:c9	ARP	42	192.168.1.51 is at 88:b1:11:ac:91:62
394	33.483745	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
715	43.621877	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
6046	49.443021	AskeyCom_c2:87:c9	IntelCor_ac:91:62	ARP	42	Who has 192.168.1.51? Tell 192.168.1.1
6047	49.443061	IntelCor_ac:91:62	AskeyCom_c2:87:c9	ARP	42	192.168.1.51 is at 88:b1:11:ac:91:62
11073	53.759995	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73
16319	63.895385	Tp-LinkT_09:5f:d6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.73

Frame 75: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{35E0075D-D58A-4073-8E00-61D525B148A5}, id 0

Ethernet II, Src: IntelCor_ac:91:62 (88:b1:11:ac:91:62), Dst: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

Destination: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

Source: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

Type: ARP (0x0806)

Address Resolution Protocol (reply)

*/*De ahora en adelante las torres de protocolos crecerán a lo ancho
(de izquierda a derecha) en lugar de en vertical (de arriba a abajo)*/*

- Torre de protocolos de un paquete ICMP (número de trama seleccionada: 85)

Ethernet II	IPv4	ICMP
-------------	------	------

No.	Time	Source	Destination	Protocol	Length	Info
37	13.785675	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3d8e, seq=0/0, ttl=64 (no response found!)
68	17.908750	192.168.1.51	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001, seq=1199/44804, ttl=128 (reply in 69)
69	17.938035	150.214.57.91	192.168.1.51	ICMP	74	Echo (ping) reply id=0x0001, seq=1199/44804, ttl=51 (request in 68)
73	18.921108	192.168.1.51	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001, seq=1200/45060, ttl=128 (reply in 76)
76	18.952168	150.214.57.91	192.168.1.51	ICMP	74	Echo (ping) reply id=0x0001, seq=1200/45060, ttl=51 (request in 73)
78	19.938605	192.168.1.51	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001, seq=1201/45316, ttl=128 (reply in 79)
79	19.970200	150.214.57.91	192.168.1.51	ICMP	74	Echo (ping) reply id=0x0001, seq=1201/45316, ttl=51 (request in 78)
84	20.953369	192.168.1.51	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001, seq=1202/45572, ttl=128 (reply in 85)
85	20.982120	150.214.57.91	192.168.1.51	ICMP	74	Echo (ping) reply id=0x0001, seq=1202/45572, ttl=51 (request in 84)
731	44.080168	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3d8e, seq=0/0, ttl=64 (no response found!)

> Frame 85: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{35E0075D-D58A-4D73-8E00-61D5258148A5}, id 0

> Ethernet II, Src: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9), Dst: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

> Destination: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

> Source: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

Type: IPv4 (0x0800)

- Torre de protocolos de un paquete DNS (número de trama seleccionada: 702)

Ethernet II	IPv4	UDP	DNS
-------------	------	-----	-----

No.	Time	Source	Destination	Protocol	Length	Info
421	33.568834	192.168.1.51	80.58.61.250	DNS	75	Standard query 0xb10 A apis.google.com
422	33.585957	80.58.61.250	192.168.1.51	DNS	91	Standard query response 0xc04 A www.gstatic.com A 142.250.200.131
423	33.586829	80.58.61.250	192.168.1.51	DNS	91	Standard query response 0xc04 A www.gstatic.com A 142.250.178.163
424	33.586829	80.58.61.250	192.168.1.51	DNS	112	Standard query response 0xb10 A apis.google.com CNAME plus.l.google.com A 142.250.200.78
464	34.031334	192.168.1.51	80.58.61.250	DNS	75	Standard query 0x7715 A play.google.com
468	34.077390	80.58.61.250	192.168.1.51	DNS	91	Standard query response 0x7715 A play.google.com A 142.250.184.174
693	43.328723	192.168.1.51	80.58.61.250	DNS	82	Standard query 0x2489 A www.informatica.uma.es
694	43.377393	80.58.61.250	192.168.1.51	DNS	124	Standard query response 0x2489 A www.informatica.uma.es CNAME informatica.informatica.uma.es A 150.214.57.91
701	43.453025	192.168.1.51	80.58.61.250	DNS	70	Standard query 0xc04 A www.uma.es
702	43.469326	80.58.61.250	192.168.1.51	DNS	112	Standard query response 0xc04 A www.uma.es CNAME ccumali.sci.uma.es A 150.214.40.97
845	44.742736	192.168.1.51	80.58.61.250	DNS	80	Standard query 0x87ec A fonts.googleapis.com A 142.250.200.138
849	44.762612	80.58.61.250	192.168.1.51	DNS	96	Standard query response 0x87ec A fonts.googleapis.com A 142.250.200.138
1586	45.564784	192.168.1.51	80.58.61.250	DNS	72	Standard query 0x5df3 A piwik.uma.es
1643	45.639102	80.58.61.250	192.168.1.51	DNS	348	Standard query response 0x5df3 A piwik.uma.es A 150.214.40.101 NS dns1.cica.es NS dns1.gssi.es NS chico.red.
1900	46.021636	192.168.1.51	80.58.61.250	DNS	74	Standard query 0xf2ab A cse.google.com
1991	46.086253	80.58.61.250	192.168.1.51	DNS	90	Standard query response 0xf2ab A cse.google.com A 172.217.168.174
2246	46.285292	192.168.1.51	80.58.61.250	DNS	83	Standard query 0xf8f1 A maps-api-ssl.google.com
2519	46.518300	80.58.61.250	192.168.1.51	DNS	123	Standard query response 0xf8f1 A maps-api-ssl.google.com CNAME clients1.google.com A 142.250.200.142
4118	48.038407	192.168.1.51	80.58.61.250	DNS	79	Standard query 0xab67 A clients1.google.com
4431	48.274279	192.168.1.51	80.58.61.250	DNS	91	Standard query 0x8440 A content-autofill.googleapis.com
4539	48.347326	80.58.61.250	192.168.1.51	DNS	119	Standard query response 0xab67 A clients1.google.com CNAME clients1.google.com A 142.250.200.142
4775	48.522601	192.168.1.51	80.58.61.250	DNS	107	Standard query response 0x8440 A content-autofill.googleapis.com A 142.250.184.170
7673	51.165289	192.168.1.51	80.58.61.250	DNS	77	Standard query 0xf65e A beacons3.gvt2.com
8103	51.523511	80.58.61.250	192.168.1.51	DNS	93	Standard query response 0xf65e A beacons3.gvt2.com A 172.217.168.163
12342	54.669921	192.168.1.51	80.58.61.250	DNS	79	Standard query 0x6244 A maps.googleapis.com
12703	54.911546	80.58.61.250	192.168.1.51	DNS	95	Standard query response 0x6244 A maps.googleapis.com A 142.250.178.170
16284	59.013109	192.168.1.51	80.58.61.250	DNS	75	Standard query 0x4e30 A docs.google.com
16285	59.036620	80.58.61.250	192.168.1.51	DNS	91	Standard query response 0x4e30 A docs.google.com A 216.58.215.142

> Frame 702: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{35E0075D-D58A-4D73-8E00-61D5258148A5}, id 0

> Ethernet II, Src: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9), Dst: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

> Destination: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

> Source: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

Type: IPv4 (0x0800)

- Torre de protocolos de un paquete HTTP (número de trama seleccionada: 707)

Ethernet II	IPv4	TCP	HTTP
-------------	------	-----	------

No.	Time	Source	Destination	Protocol	Length	Info
94	22.354408	192.168.1.51	5.255.145.9	HTTP	334	GET /msdownload/update/v3/static/trustedr/en/authrootst1.cab?228e6
97	22.375995	5.255.145.9	192.168.1.51	HTTP	320	HTTP/1.1 304 Not Modified
698	43.410694	192.168.1.51	150.214.57.91	HTTP	494	GET / HTTP/1.1
700	43.450437	150.214.57.91	192.168.1.51	HTTP	597	HTTP/1.1 301 Moved Permanently (text/html)
707	43.505652	192.168.1.51	150.214.40.97	HTTP	499	GET /etsi-informatica/ HTTP/1.1
709	43.539608	150.214.40.97	192.168.1.51	HTTP	155	HTTP/1.1 301 Moved Permanently
735	44.172328	192.168.1.51	88.221.52.56	HTTP	315	GET /connectiontest.html HTTP/1.1
737	44.189491	88.221.52.56	192.168.1.51	HTTP	302	HTTP/1.1 200 OK (text/html)

> Frame 707: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits) on interface \Device\NPF_{35E0075D-D58A-4D73-8E00-61D5258148A5}, id 0

> Ethernet II, Src: IntelCor_ac:91:62 (88:b1:11:ac:91:62), Dst: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

> Destination: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

> Source: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

Type: IPv4 (0x0800)

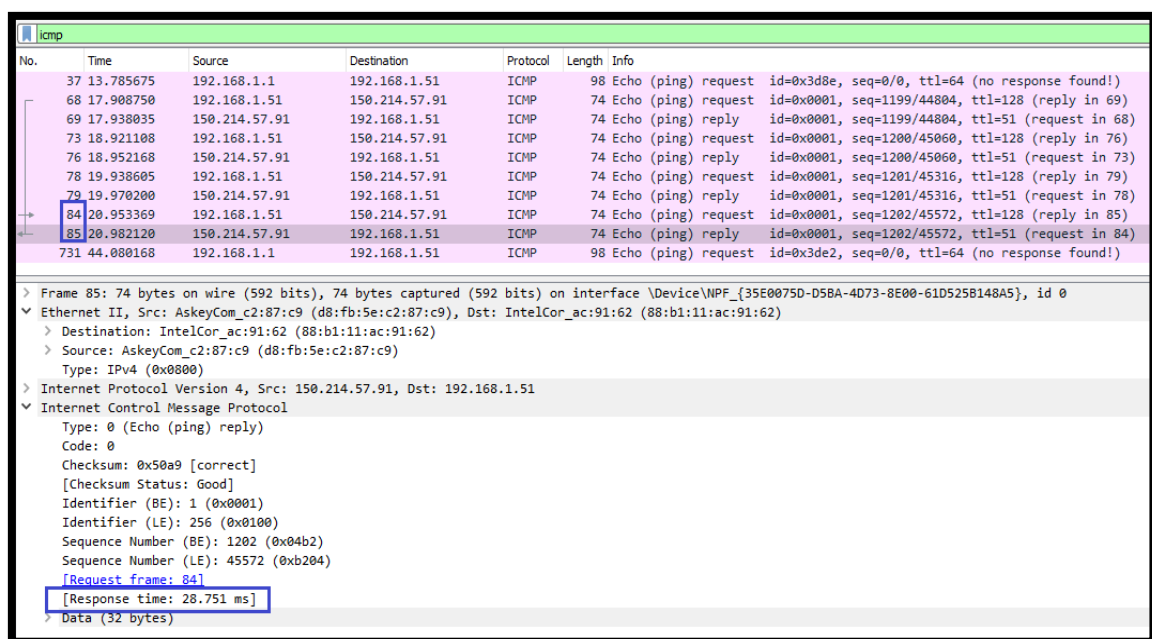
Ejercicio 4. Observe el campo tipo de la cabecera Ethernet II para cada uno de los mensajes anteriores. Rellene la siguiente tabla y luego responda a las preguntas.

Tipo en la cabecera Ethernet II		
	Hexadecimal	Texto
ARP	(0x806)	ARP
HTTP	(0x800)	IPv4
ICMP	(0x800)	IPv4
DNS	(0x800)	IPv4

- **¿Qué significa este campo?**
El campo tipo define la longitud exacta del campo de Datos de la trama. La manera en la que así lo hace es indicando qué protocolo se ha utilizado para implementarla.
- **¿Por qué en tramas diferentes es igual?**
Cada trama tiene un tipo de protocolo de conmutación asignado que expresa cómo ha sido transmitida. No es difícil entender que diferentes tramas puedan utilizar el mismo protocolo.

Ejercicio 5. En Wireshark observe la diferencia entre el tiempo de la primera petición icmp (Echo (ping) request) y su respuesta (Echo (ping) reply).

- **Números de las tramas seleccionadas:**
84 y 85
- **¿Cuánto tiempo es (en milisegundos)?**
28.751 ms
- **¿A qué concepto visto en la parte de teoría equivale dicho tiempo?**
Debido a que recibir una respuesta conlleva haber enviado una trama y haber esperado a recibir una confirmación, equivale al Round-Trip Time.



Ejercicio 6. Según la teoría vista en clase, las tramas Ethernet deben tener un tamaño mínimo de 64 bytes. Wireshark no muestra el campo FCS (ya que es tratado automáticamente por la tarjeta de red), por lo que la trama mostrada en Wireshark tendrá un tamaño de 60 bytes.

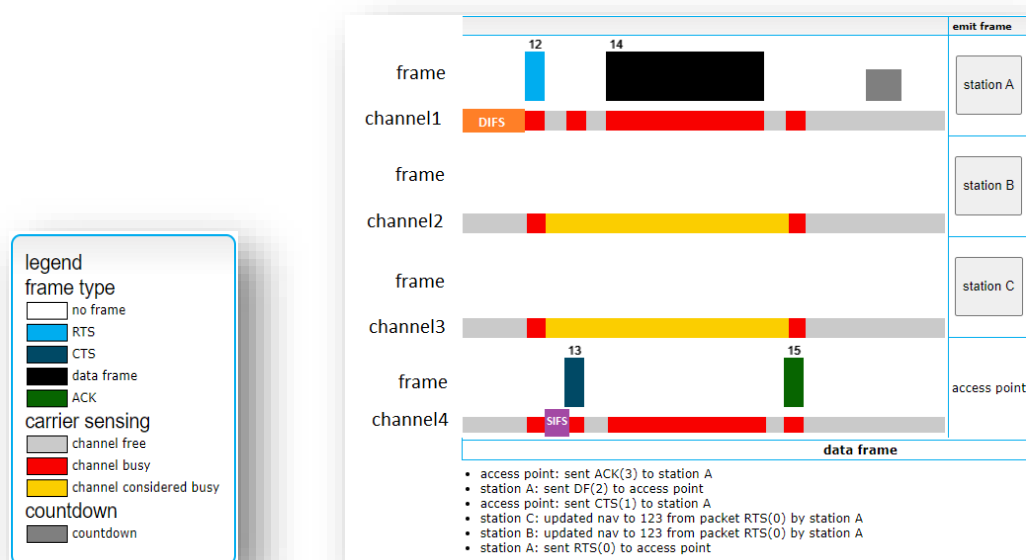
- **Busque una trama con tamaño 60 (filtro: `frame.len == 60`), Número de trama seleccionada:** *Mi traza en Wishark no muestra nada al aplicar el filtro :(*
- **¿Qué mecanismo se utiliza para completar el tamaño si los datos transmitidos son más pequeños de 46 bytes)?**
Se aplica una técnica conocida como Padding (Tráfico de Relleno), que como su nombre indica, consiste en generar tráfico artificial e de irrelevante contenido para alargar el tamaño de la trama.

Ejercicio 7. Simule que la estación A envía una trama al punto de acceso teniendo tanto las estaciones ocultas como no ocultas. Tras elegir el escenario, pulse botón de inicio (*start*), y observe las estaciones B y C.

- **¿Cuándo empieza el temporizador NAV en cada escenario?**
- **¿Por qué ocurre de ese modo?**
- **Tome una captura de pantalla de cada escenario donde se vea cuando se activa este temporizador y añádalas a la memoria marcando en una de ellas los tiempos DIFS y SIFS que observe.**

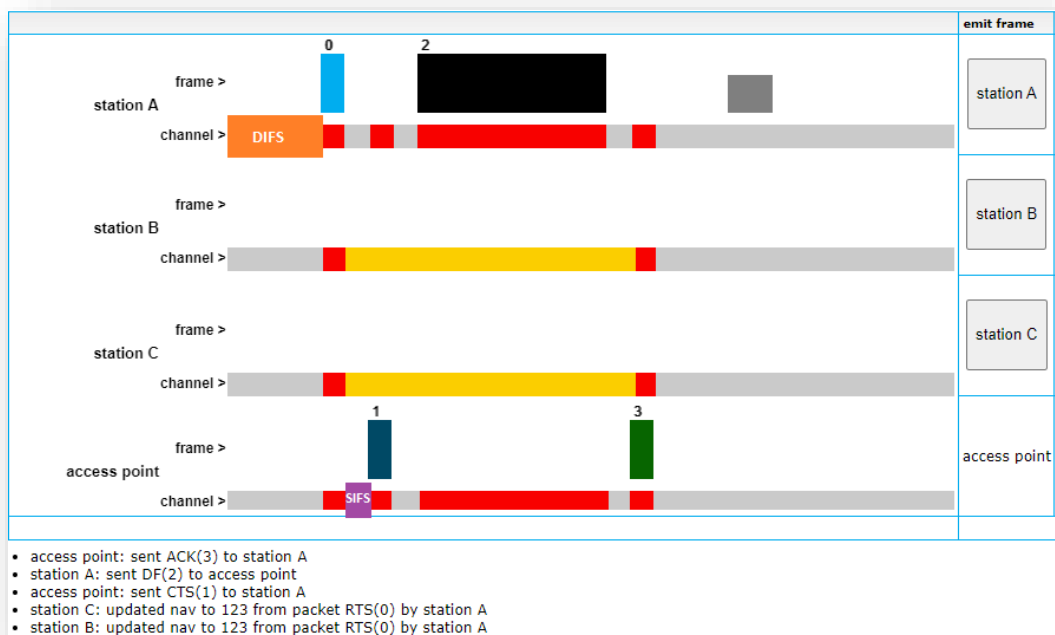
➤ Escenario 1. Sin estaciones ocultas

- *El NAV corresponde con la banda amarilla y comienza en las estaciones B y C (channel2 y channel3) cuando ambas reciben el RTS (banda cian) de la estación A.*
- *Esto es así porque todas las estaciones se escuchan entre sí y son capaces de escuchar su entorno para detectar mediante el RTS de A que dicha estación quiere empezar a transmitir. Por lo tanto, deben quedarse bloqueadas hasta que termine.*
- *El DIFS corresponde con el recuadro naranja y el SIFS con el morado para todos los escenarios.*

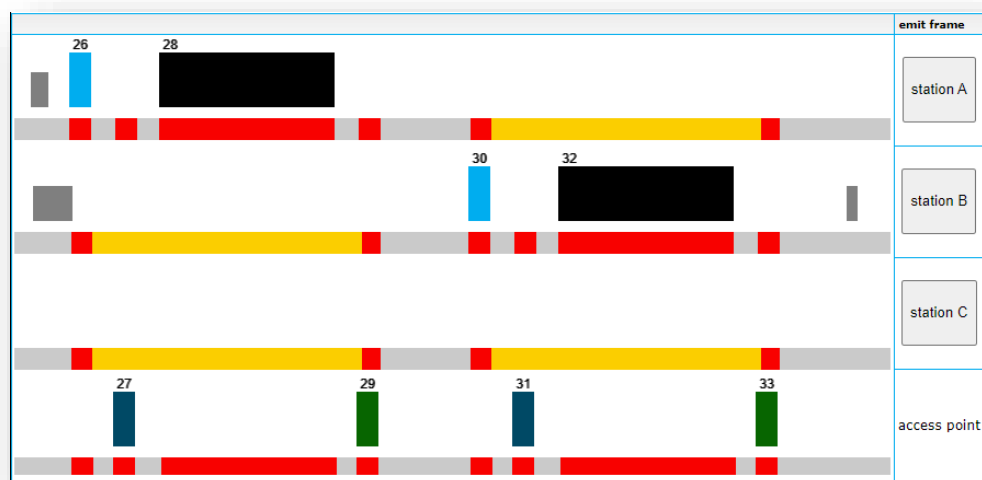


➤ Escenario 2. Estaciones ocultas

- El NAV corresponde con la banda amarilla y comienza en las estaciones B y C (channel2 y channel3) cuando ambas reciben el CTS (banda azulada) del access point.
- Esto es así porque todas las estaciones no se escuchan entre sí y no son capaces de escuchar completamente su entorno. Por lo tanto, requieren del Access point para que les indique mediante una señal CTS cuándo este está ocupado recibiendo información de otra estación desconocida para ellos (B y C). Así sabrán que no deben enviar nada hasta que el access point vuelva a enviar un ACK de confirmación.



Ejercicio 8. Sin terminal oculto, simule que tanto la estación A y la B intentan enviar una trama.



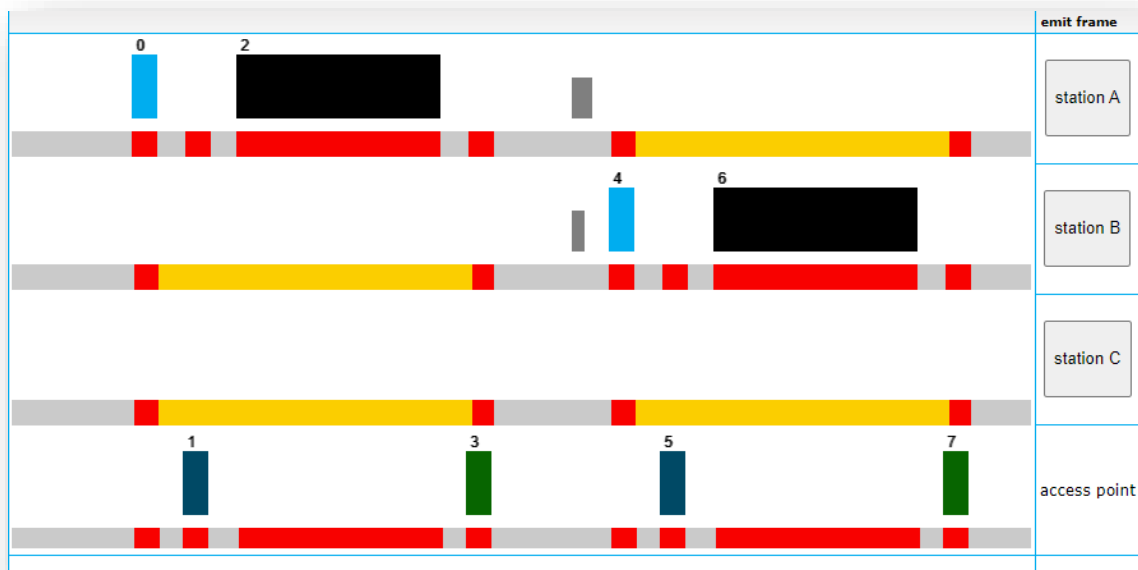
- **¿Cómo detecta el protocolo que se ha producido la colisión?**
Al haber dos canales intentando emitir, sus correspondientes RTS colisionan en el medio ya que se emiten a la vez. El protocolo sabe que esto no puede ocurrir y ninguna de las dos consigue avanzar.
- **¿Cómo consigue finalmente enviar uno de los nodos sin que se produzca colisión?**
Al principio de las colisiones, ambas estaciones se bloquean continuamente la una a la otra por consecuencia de sus RTS. Cuando el tiempo de intentos de una de las estaciones se agota (la que clicamos después) la primera es capaz de avanzar y emitir su RTS.

De ahora en adelante no se producirá ninguna otra colisión y el proceso seguirá como de costumbre, uno detrás de otro (B espera el ACK de A para mandar su propio RTS).

Ejercicio 9. Ahora use ambos escenarios (con y sin terminal oculto), y siga el siguiente esquema: pulse el botón de inicio, ahora pulse en A para que se produzca el envío, pero inmediatamente pulse también la B (antes de que se vea visualmente el envío de A):

➤ Escenario 1. Sin estación oculta

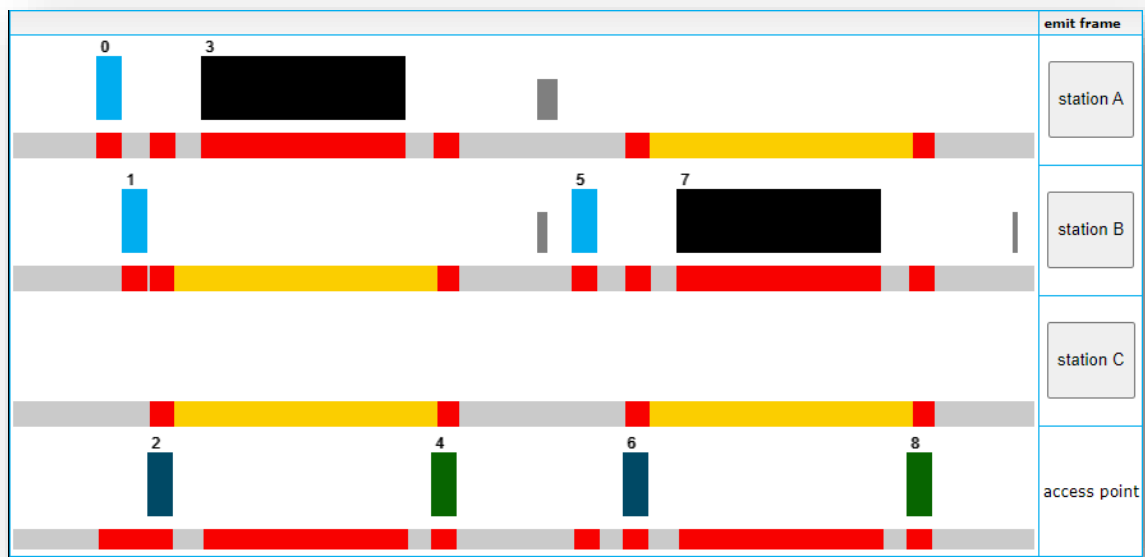
- **¿Por qué la estación B ni siquiera empieza su envío hasta que no acaba A?**
Si las no existe ninguna estación oculta, todas pueden oírse entre sí y si B sabe que A está comenzando una transmisión (mediante el CTS de A) no va a intentar mandar su propio CTS porque sabe que causará una colisión.



➤ Escenario 2. Estación oculta

- **¿Por qué A no detecta la colisión entre el RTS de B y el CTS del AP?**
Al haber estaciones ocultas, A no es capaz de detectar que B también ha mandado su propio RTS, solo puede detectar que el Access Point ha mandado su CTS y le da luz verde para comenzar a emitir.

- **¿Por qué si A está enviando la trama de datos, B envía el RTS?**
B desconoce de esta situación por el mismo motivo de antes, las estaciones ocultas. B intenta conectar con Access Point y como está ocupado nunca recibe su CTS y se bloquea por un tiempo NAV. Cuando detecte el APK volverá a intentarlo de nuevo, desconociendo que antes de él A ya ha mandado sus datos.
- **¿Cómo consigue finalmente A que llegue su trama correctamente al AP?**
Como A ha sido el primero en mandar su RTS, el Access Point está libre y accede a recibir lo que A tenga que decir. Esto se lo comunica mediante una señal CTS y comienza a recibir los datos. Una vez acabado, le devuelve un ACK de confirmación.



Práctica 2

Apellidos: **Hidalgo Baños**

Nombre: **Marcos**

Titulación: **Grado de Ing. Informática D**

Grupo: **Grupo de Prácticas 3**

PC de la práctica: **PC134**

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

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

Protocolo	Valor Campo protocolo (texto)	Valor Campo protocolo (HEX)	Número de trama
ICMP	ICMP(1)	01	18968
HTTP	TCP(6)	06	18777
DNS	UDP(17)	11	18768
FTP	TCP(6)	06	17729

1º) Hacemos el ping correspondiente que generará las tramas a analizar

```
Microsoft Windows [Versión 10.0.17134.1006]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 www.informatica.uma.es

Haciendo ping a informatica.informatica.uma.es [150.214.57.91] con 32 bytes de datos:
Respuesta desde 150.214.57.91: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 150.214.57.91:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

2º) Filtramos según el protocolo en Wireshark para obtener los datos para completar la tabla

Protocolo ICMP

No.	Time	Source	Destination	Protocol	Length	Info
572	17.770699	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3c50, seq=0/0, ttl=64 (no res...
17639	48.276930	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3c92, seq=0/0, ttl=64 (no res...
18762	78.937328	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3d04, seq=0/0, ttl=64 (no res...
18968	96.452936	192.168.1.51	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001, seq=2479/44809, ttl=128...
18975	96.485111	150.214.57.91	192.168.1.51	ICMP	74	Echo (ping) reply id=0x0001, seq=2479/44809, ttl=51 ...
19084	108.068244	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3d73, seq=0/0, ttl=64 (no res...

> Frame 18968: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{35E0075D-D5BA-4D73-8E00-61D525B148A5}

> Ethernet II, Src: IntelCor_ac:91:62 (88:b1:11:ac:91:62), Dst: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

> Internet Protocol Version 4, Src: 192.168.1.51, Dst: 150.214.57.91

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x1057 (4183)

> Flags: 0x00

Fragment Offset: 0

Time to Live: 128

Protocol: ICMP (1)

Header Checksum: 0x985d [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.51

Destination Address: 150.214.57.91

> Internet Control Message Protocol

<

```

0000  d8 fb 5e c2 87 c9 88 b1 11 ac 91 62 08 00 45 00  ..^.....b...E..
0010  00 3c 10 57 00 00 80 01 98 5d c0 a8 01 33 96 d6  <..W.....]...3..
0020  39 5b 08 00 43 ac 00 01 09 af 61 62 63 64 65 66  9[...C.....abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdfgh hi

```

Protocolo HTTP

No.	Time	Source	Destination	Protocol	Length	Info
11840	35.635865	93.184.220.29	192.168.1.51	OSCP	853	Response
18766	80.067838	192.168.1.51	34.107.221.82	HTTP	381	GET /success.txt HTTP/1.1
18777	80.179366	34.107.221.82	192.168.1.51	HTTP	274	HTTP/1.1 200 OK (text/plain)
18779	80.186890	192.168.1.51	34.107.221.82	HTTP	386	GET /success.txt?ipv4 HTTP/1.1
18782	80.223654	34.107.221.82	192.168.1.51	HTTP	274	HTTP/1.1 200 OK (text/plain)

> Frame 18777: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface \Device\NPF_{35E0075D-D5BA-4D73-8E00-61D525B148A5}

> Ethernet II, Src: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9), Dst: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

> Internet Protocol Version 4, Src: 34.107.221.82, Dst: 192.168.1.51

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 260

Identification: 0xd97a (55674)

> Flags: 0x00

Fragment Offset: 0

Time to Live: 58

Protocol: TCP (6)

Header Checksum: 0xe4e0 [validation disabled]

[Header checksum status: Unverified]

Source Address: 34.107.221.82

Destination Address: 192.168.1.51

> Transmission Control Protocol, Src Port: 80, Dst Port: 49616, Seq: 221, Ack: 655, Len: 220

> Hypertext Transfer Protocol

> Line-based text data: text/plain (1 lines)

<

```

0000  88 b1 11 ac 91 62 d8 fb 5e c2 87 c9 08 00 45 00  ....b...^.....E..
0010  01 04 d9 7a 00 00 3a 06 e4 e0 22 6b dd 52 c0 a8  <...z...[ ]...k.R...
0020  01 33 00 50 c1 d0 1c a6 29 e9 c5 ef a7 79 50 18  <3 P.....).....yP..
0030  01 09 d0 81 00 00 48 54 54 50 2f 31 2e 31 20 32  <.....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 6e  00 OK..S erver: n
0050  67 69 6e 78 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c  ginx..Da te: Mon,
0060  20 31 32 20 41 70 72 20 32 30 32 31 20 31 38 3a  12 Apr 2021 18:
0070  32 34 3a 34 34 20 47 4d 54 0d 0a 43 6f 6e 74 65  24:44 GM T..Conte
0080  6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c  nt-Type: text/pl

```

Protocolo DNS

No.	Time	Source	Destination	Protocol	Length	Info
18661	72.145672	80.58.61.250	192.168.1.51	DNS	168	Standard query response 0xea5a A roaming.officeap...
18765	80.067338	192.168.1.51	80.58.61.250	DNS	84	Standard query 0x0968 A detectportal.firefox.com
18768	80.099235	192.168.1.51	80.58.61.254	DNS	84	Standard query 0x0968 A detectportal.firefox.com
18769	80.159123	80.58.61.250	192.168.1.51	DNS	195	Standard query response 0x0968 A detectportal.fir...
18775	80.179218	80.58.61.254	192.168.1.51	DNS	195	Standard query response 0x0968 A detectportal.fir...

> Frame 18768: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{35E0075D-D58A-4D73-8E00-61D525B148A5}

> Ethernet II, Src: IntelCor_ac:91:62 (88:b1:11:ac:91:62), Dst: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

> Internet Protocol Version 4, Src: 192.168.1.51, Dst: 80.58.61.254

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 70
 Identification: 0x4bf0 (19440)
 > Flags: 0x00
 Fragment Offset: 0
 Time to Live: 128
Protocol: UDP (17)
 Header Checksum: 0xea3 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.51
 Destination Address: 80.58.61.254
 > User Datagram Protocol, Src Port: 54146, Dst Port: 53
 > Domain Name System (query)

0000 d8 fb 5e c2 87 c9 88 b1 11 ac 91 62 08 00 45 00 ...^.....b..E..
 0010 00 46 4b f0 00 00 80 11 9e a3 c0 a8 01 33 50 3a ..FK.....3P:
 0020 3d fe d3 82 00 35 00 32 ae 1a 09 68 01 00 00 01 =...5.2...h....
 0030 00 00 00 00 00 00 0c 64 65 74 65 63 74 70 6f 72detectpor
 0040 74 61 6c 07 66 69 72 65 66 6f 78 03 63 6f 6d 00 tal-fire fox.com
 0050 00 01 00 01

Protocolo FTP

No.	Time	Source	Destination	Protocol	Length	Info
17720	50.379951	150.214.40.67	192.168.1.51	FTP	88	Response: 257 "/" is the current directory
17721	50.380755	192.168.1.51	150.214.40.67	FTP	62	Request: TYPE I
17722	50.409990	150.214.40.67	192.168.1.51	FTP	73	Response: 200 Type set to I
17723	50.410740	192.168.1.51	150.214.40.67	FTP	60	Request: PASV
17724	50.441564	150.214.40.67	192.168.1.51	FTP	105	Response: 227 Entering Passive Mode (150,214,40,6...
17725	50.442724	192.168.1.51	150.214.40.67	FTP	61	Request: CWD /
17729	50.471850	150.214.40.67	192.168.1.51	FTP	82	Response: 250 CWD command successful
17730	50.472528	192.168.1.51	150.214.40.67	FTP	60	Request: LIST
17731	50.503425	150.214.40.67	192.168.1.51	FTP	109	Response: 150 Opening BINARY mode data connection...
17737	50.534509	150.214.40.67	192.168.1.51	FTP	77	Response: 226 Transfer complete

> Ethernet II, Src: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9), Dst: IntelCor_ac:91:62 (88:b1:11:ac:91:62)

> Internet Protocol Version 4, Src: 150.214.40.67, Dst: 192.168.1.51

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 68
 Identification: 0xa27b (41595)
 > Flags: 0x40, Don't fragment
 Fragment Offset: 0
 Time to Live: 53
Protocol: TCP (6)
 Header Checksum: 0x2244 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 150.214.40.67
 Destination Address: 192.168.1.51
 > Transmission Control Protocol, Src Port: 21, Dst Port: 49674, Seq: 1380, Ack: 81, Len: 28
 > File Transfer Protocol (FTP)
 [Current working directory: /]

0000 88 b1 11 ac 91 62 d8 fb 5e c2 87 c9 08 00 45 00b..^.....E..
 0010 00 44 a2 7b 40 00 35 06 22 44 96 d6 28 43 c0 a8 ..D.{@.5.."D..(..
 0020 01 33 00 15 c2 0a 8c 6a e0 c2 5c 5f be f8 50 18 ..3.....j...\\...P..
 0030 00 e5 30 d0 00 00 32 35 30 20 43 57 44 20 63 6f ..0...25.0 CWD co
 0040 6d 6d 61 6e 64 20 73 75 63 63 65 73 73 66 75 6c mmand su ccessful
 0050 0d 0a ..

- ¿Qué indica este campo?

Indica, como su nombre indica, el protocolo utilizado para enviar la trama en cuestión. Un detalle para destacar es que hay que tener cuidado con el numerito asociado entre paréntesis, que no indica lo parece indicar :)

Ejercicio 2. Seleccione una petición de ICMP de su equipo (el mensaje *Echo Request*) y complete la siguiente tabla indicando la dirección IP destino (en la cabecera IP) y la dirección MAC destino (en la cabecera Ethernet). Repita el proceso con una petición FTP (en la *Info pone Request*).

	ICMP	FTP
Dirección IP destino (cab IP)	150.214.57.91	150.214.40.67
Dirección MAC destino (cab Ethernet)	d8:fb:5e:c2:87:c9	d8:fb:5e:c2:87:c9
Número de trama	18968	17693

Protocolo ICMP

No.	Time	Source	Destination	Protocol	Length	Info
572	17.770699	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3c50, seq=0/0, ttl=64 (no res...
17639	48.276930	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3c92, seq=0/0, ttl=64 (no res...
18762	78.937328	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3d04, seq=0/0, ttl=64 (no res...
18968	96.452936	192.168.1.51	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001, seq=2479/44809, ttl=128...
18975	96.485111	150.214.57.91	192.168.1.51	ICMP	74	Echo (ping) reply id=0x0001, seq=2479/44809, ttl=51 ...
19084	108.068244	192.168.1.1	192.168.1.51	ICMP	98	Echo (ping) request id=0x3d73, seq=0/0, ttl=64 (no res...

> Frame 18968: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF {35E0075D-D58A-4D73-8E00-61D5258148A5}

> Ethernet II, Src: IntelCor_ac:91:62 (88:b1:11:ac:91:62), Dst: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

> Internet Protocol Version 4, Src: 192.168.1.51, Dst: 150.214.57.91

> Internet Control Message Protocol

Protocolo FTP

No.	Time	Source	Destination	Protocol	Length	Info
17692	50.183460	150.214.40.67	192.168.1.51	FTP	77	Response: 220 FTP Server ready.
17693	50.184116	192.168.1.51	150.214.40.67	FTP	70	Request: USER anonymous
17695	50.215962	150.214.40.67	192.168.1.51	FTP	129	Response: 331 Anonymous login ok, send your compl...
17696	50.220491	192.168.1.51	150.214.40.67	FTP	80	Request: PASS mozilla@example.com
17697	50.251907	150.214.40.67	192.168.1.51	FTP	113	Response: 230-Bienvenido al FTP anónimo de la Un...
17698	50.253212	150.214.40.67	192.168.1.51	FTP	57	Response:
17700	50.254302	150.214.40.67	192.168.1.51	FTP	57	Response:

> Frame 17693: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF {35E0075D-D58A-4D73-8E00-61D5258148A5}

> Ethernet II, Src: IntelCor_ac:91:62 (88:b1:11:ac:91:62), Dst: AskeyCom_c2:87:c9 (d8:fb:5e:c2:87:c9)

> Internet Protocol Version 4, Src: 192.168.1.51, Dst: 150.214.40.67

> Transmission Control Protocol, Src Port: 49674, Dst Port: 21, Seq: 1, Ack: 24, Len: 16

> File Transfer Protocol (FTP)

[Current working directory:]

- ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no?

Por definición, las direcciones MAC son inmutables ya que son direcciones físicas, mientras que la IP depende del protocolo con el que se ha mandado.

Ejercicio 3. Responda las siguientes preguntas:

- ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)?

En el caso de las respuestas ICMP, el tipo y el código son 0.

Por otro lado, las peticiones tienen tipo 8 y código 0.

- ¿Qué filtro podría poner para que sólo aparezcan los fragmentos relacionados con un datagrama concreto?

Como se muestra en las capturas, $ip.id == <identificador>$

A) Realizamos los dos pings a `ww.informatica.uma.es` con tamaños 1000 y 3000

```
C:\WINDOWS\system32 ping -n 1 www.informatica.uma.es -l 1000

Haciendo ping a informatica.informatica.uma.es [150.214.57.91] con 1000 bytes de datos:
Respuesta desde 150.214.57.91: bytes=1000 tiempo<1m TTL=63

Estadísticas de ping para 150.214.57.91:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\WINDOWS\system32 ping -n 1 www.informatica.uma.es -l 3000

Haciendo ping a informatica.informatica.uma.es [150.214.57.91] con 3000 bytes de datos:
Respuesta desde 150.214.57.91: bytes=3000 tiempo<1m TTL=63

Estadísticas de ping para 150.214.57.91:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

B) De igual manera, filtramos en WireShark para contestar a la primera pregunta

Protocolo ICMP (Reply)

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
743	58.137970	192.168.164.34	150.214.57.91	ICMP	1042	Echo (ping) request
744	58.138560	150.214.57.91	192.168.164.34	ICMP	1042	Echo (ping) reply
934	73.473134	192.168.164.34	150.214.57.91	ICMP	82	Echo (ping) request
937	73.473751	150.214.57.91	192.168.164.34	ICMP	82	Echo (ping) reply

> Frame 744: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits) on interface \Device\NPF...

> Ethernet II, Src: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75), Dst: HewlettP_34:e1:81 (8c:dc:d4:34:e1:81)

> Internet Protocol Version 4, Src: 150.214.57.91, Dst: 192.168.164.34

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x5a5d [correct]

[Checksum Status: Good]

Protocolo ICMP (Request)

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
743	58.137970	192.168.164.34	150.214.57.91	ICMP	1042	Echo (ping) request
744	58.138560	150.214.57.91	192.168.164.34	ICMP	1042	Echo (ping) reply
934	73.473134	192.168.164.34	150.214.57.91	ICMP	82	Echo (ping) request
937	73.473751	150.214.57.91	192.168.164.34	ICMP	82	Echo (ping) reply

> Frame 743: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits) on interface \Device\NPF...

> Ethernet II, Src: HewlettP_34:e1:81 (8c:dc:d4:34:e1:81), Dst: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75)

> Internet Protocol Version 4, Src: 192.168.164.34, Dst: 150.214.57.91

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x525d [correct]

[Checksum Status: Good]

- 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	Nº tramas	Ids	Flags	Desplazamientos
1000	744	33895	0x00	0
3000	932, 933, 934	23558	0x20, 0x20, 0x01	0, 1480, 2960

- C) Aplicamos el filtro correspondiente (explicados en la segunda pregunta)
D) Localizamos las tramas que actúan al hacer ambos pines

Tamaño de Trama = 1000

Wireshark packet capture showing packet 744, an ICMP Echo (ping) reply. The packet details pane shows:

- Total Length: 1028
- Identification: 0x8467 (33895)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 63
- Protocol: ICMP (1)

Tamaño de Trama = 3000

Wireshark packet capture showing packet 932, a Fragmented IP protocol (proto=ICMP 1, off=0, ID=5c06). The packet details pane shows:

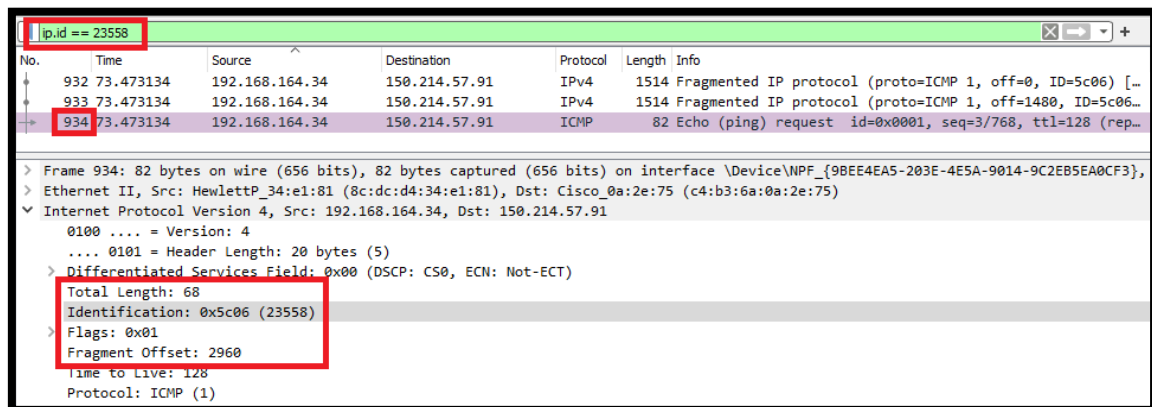
- Total Length: 1500
- Identification: 0x5c06 (23558)
- Flags: 0x20, More fragments
- Fragment Offset: 0
- Time to Live: 128
- Protocol: ICMP (1)

Tamaño de Trama = 3000

Wireshark packet capture showing packet 933, a Fragmented IP protocol (proto=ICMP 1, off=1480, ID=5c06). The packet details pane shows:

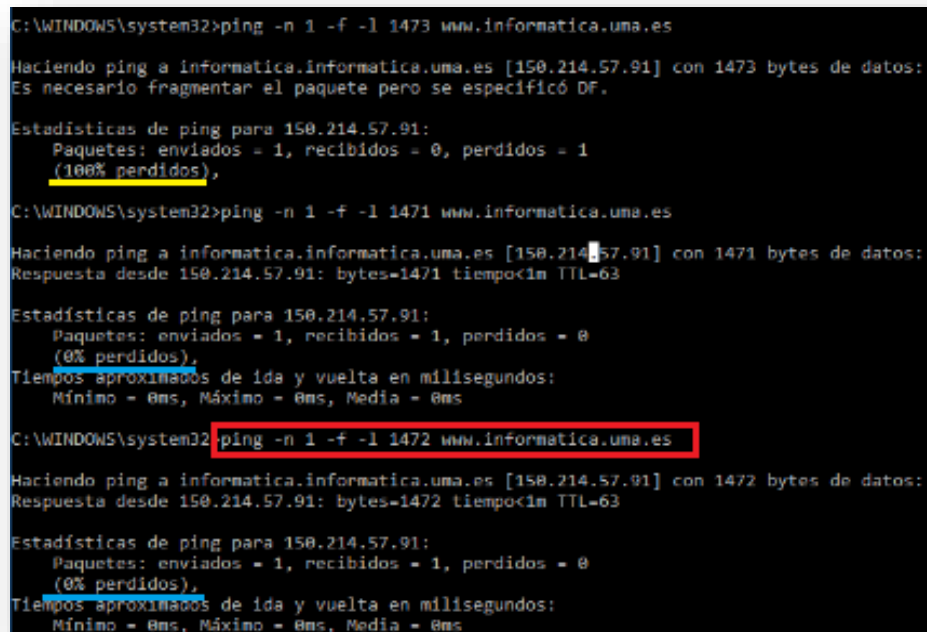
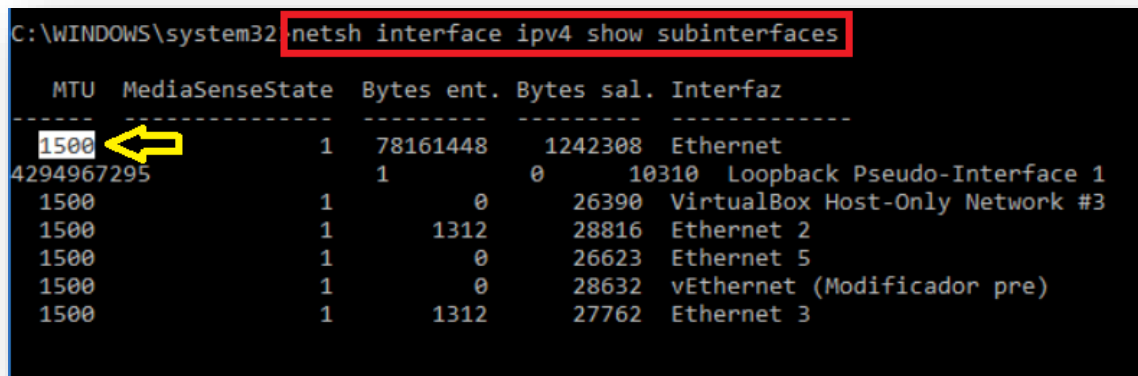
- Total Length: 1500
- Identification: 0x5c06 (23558)
- Flags: 0x20, More fragments
- Fragment Offset: 1480
- Time to Live: 128
- Protocol: ICMP (1)

Tamaño de Trama = 3000



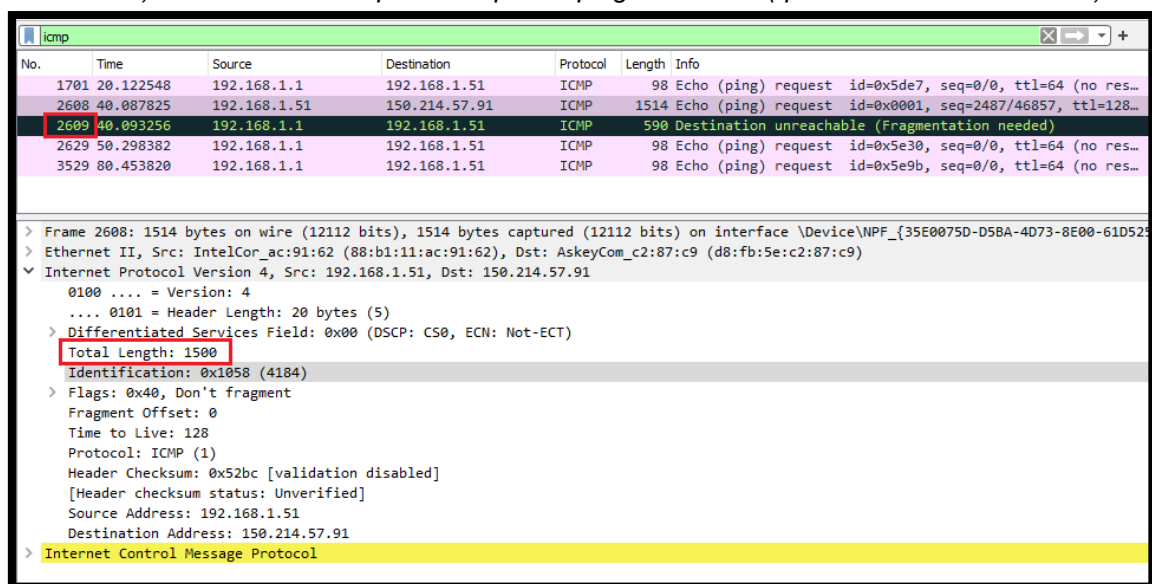
Ejercicio 4. Realice dos pings a **informatica.cv.uma.es** con tamaños MAX y MAX+1 y el bit DF activo (MAX es el tamaño máximo calculado). Añada una captura de pantalla del terminal.

A) Consultamos el valor MAX y probamos qué valor inferior es el verdadero máximo



- **¿Cuál es el valor máximo?**
El verdadero tamaño MAX resulta de $1500 - 20 - 8 = 1472$ bytes
- **¿Por qué es ese tamaño?**
 $MAX = MTU - (\text{tamaño cabecera IP}) - (\text{tamaño cabecera ICMP}) = 1472$ bytes
- **¿En la traza de wireshark aparece el primer ping? ¿Y el segundo?**
En la traza salen tres pings, tal y como indico en la captura de la consola, uno para los valores 1471 y 1472, que sí tienen éxito. Por otro lado, el marcado en la captura siguiente se muestra claramente que no se ha podido enviar.
 - **¿Por qué?**
Esto es debido a que el tamaño del paquete es mayor que el máximo permitido y, al decirle que no lo puede fragmentar, se bloquea y muestra esta trama de error.

B) Consultamos si aparece el primer ping en la traza (que vemos resulta en error)



Ejercicio 5. Haga un ping a **informatica.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.

```
C:\WINDOWS\system32 ping -n 1 -i 1 www.informatica.uma.es

Haciendo ping a informatica.informatica.uma.es [150.214.57.91] con 32 bytes de datos:
Respuesta desde 192.168.167.254: TTL expirado en tránsito.

Estadísticas de ping para 150.214.57.91:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),

C:\WINDOWS\system32 ping -n 1 -i 2 www.informatica.uma.es

Haciendo ping a informatica.informatica.uma.es [150.214.57.91] con 32 bytes de datos:
Respuesta desde 150.214.57.91: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 150.214.57.91:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
Tiempo aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

- **Número de trama analizada**
Trama número 772
- **¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)?**
Se recibe un mensaje tipo 11 con código 0. Esto indica que el paquete no ha llegado al destino porque el tiempo de vida a sido excedido durante el trayecto.
- **¿Qué incluye dicho mensaje ICMP como información adicional?**
Incluye información sobre los saltos que se han fijado para hacer el ping (último recuadro en la imagen) que en este caso es 1, tal y como se indica en la consola de comandos en el primer recuadro rojo.

No.	Time	Source	Destination	Protocol	Length	Info
771	65.795109	192.168.164.34	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001,
772	65.795566	192.168.167.254	192.168.164.34	ICMP	70	Time-to-live exceeded (Time to
925	78.635976	192.168.164.34	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001,
926	78.636472	150.214.57.91	192.168.164.34	ICMP	74	Echo (ping) reply id=0x0001,
1246	107.073915	192.168.164.34	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001,
1247	107.074410	150.214.57.91	192.168.164.34	ICMP	74	Echo (ping) reply id=0x0001,
1407	117.917778	192.168.164.34	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001,
1408	117.918106	150.214.57.91	192.168.164.34	ICMP	74	Echo (ping) reply id=0x0001,

> Frame 772: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{9BEE4EA5-203}

> Ethernet II, Src: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75), Dst: HewlettP_34:e1:81 (8c:dc:d4:34:e1:81)

> Internet Protocol Version 4, Src: 192.168.167.254, Dst: 192.168.164.34

▼ Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0x9fa3 [correct]
[Checksum Status: Good]
Unused: 00000000

▼ Internet Protocol Version 4, Src: 192.168.164.34, Dst: 150.214.57.91

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x5c2a (23594)
> Flags: 0x00
Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x289b [validation disabled]

Ejercicio 6. Responda a las siguientes preguntas:

```
Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32: tracert www.informatica.uma.es

Traza a la dirección informatica.informatica.uma.es [150.214.57.91]
sobre un máximo de 30 saltos:

 1    1 ms    <1 ms    <1 ms    192.168.167.254
 2    <1 ms    <1 ms    <1 ms    informatica.informatica.uma.es [150.214.57.91]

Traza completa.
```

- **Indique el número de las tramas utilizadas para responder estas preguntas**
Tramas número 1156, 1157, 1158, 1159, 1160 y 1161 (recuadro rojo) cuyo protocolo es ICMP y tramas número 1154, 1155, 1162, 1163 (recuadros amarillos) para el protocolo DNS.
- **¿Qué tipo de paquetes (protocolo de más alto nivel) usa tracer para hacer su función?**
Emplea paquetes cuyo protocolo es ICMP.
- **Además de los mensajes propios para obtener el camino, tracer 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?**
También produce otros paquetes DNS que traducen la dirección IP a la URL que le corresponda.
- **¿Qué estrategia usa tracer para averiguar qué máquina hay en cada salto del paquete?**
Emplea un envío continuado de mensajes ICMP a la dirección en cuestión de manera que podamos rastrear las direcciones IP de los nodos intermedios (routers) y así averiguar cuál es la dirección IP deseada.

No.	Time	Source	Destination	Protocol	Length	Info
1154	57.984125	192.168.164.34	150.214.57.7	DNS	82	Standard query 0x7a73 A www.informatica.uma.es
1155	57.984848	150.214.57.7	192.168.164.34	DNS	124	Standard query response 0x7a73 A www.informatica.uma.es
1156	57.993325	192.168.164.34	150.214.57.91	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=1 (no res
1157	57.994489	192.168.167.254	192.168.164.34	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1158	57.995735	192.168.164.34	150.214.57.91	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=1 (no res
1159	57.996120	192.168.167.254	192.168.164.34	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1160	57.996429	192.168.164.34	150.214.57.91	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=1 (no res
1161	57.996853	192.168.167.254	192.168.164.34	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1162	57.997533	192.168.164.34	150.214.57.7	DNS	88	Standard query 0x7973 PTR 254.167.168.192.in-addr.arpa
1163	57.998501	150.214.57.7	192.168.164.34	DNS	164	Standard query response 0x7973 No such name PTR 254.167.16

Additional RRs: 0

Queries

- www.informatica.uma.es: type A, class IN
 - Name: www.informatica.uma.es
 - [Name Length: 22]
 - [Label Count: 4]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

Answers

- www.informatica.uma.es: type CNAME, class IN, cname informatica.informatica.uma.es
 - Name: www.informatica.uma.es
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 86400 (1 day)
 - Data length: 14
 - CNAME: informatica.informatica.uma.es
- informatica.informatica.uma.es: type A, class IN, addr 150.214.57.91
 - Name: informatica.informatica.uma.es
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 86400 (1 day)
 - Data length: 4
 - Address: 150.214.57.91

[Request In: 1154]

[Time: 0.000723000 seconds]

Práctica 3

Apellidos: **Hidalgo Baños**

Nombre: **Marcos**

Titulación: Grado de **Ingeniería Informática D**

Grupo: **Grupo de Prácticas 3**

PC de la práctica: **xxxx (No me acordé de apuntarlo)**

Ejercicio 1. 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).

1) *Ejecutamos el comando ipconfig en la consola de Windows*

```
C:\WINDOWS\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet vEthernet (Modificador pre):

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . : fe80::8179:8dbb:65f5:c654%22
    Dirección IPv4. . . . . : 172.27.219.209
    Máscara de subred . . . . . : 255.255.255.240
    Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.168.164.24
    Máscara de subred . . . . . : 255.255.252.0
    Puerta de enlace predeterminada . . . . . : 192.168.167.254

Adaptador de Ethernet VirtualBox Host-Only Network #3:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . : fe80::fdac:a17f:8e89:a3b%25
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet 5:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . : fe80::7cdc:c0e:cd2a:18e7%18
    Dirección IPv4. . . . . : 192.168.99.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . : fe80::9dfe:b512:b564:a3c5%11
    Dirección IPv4. . . . . : 192.168.64.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet 3:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . : fe80::85bc:215e:b43f:b50f%12
    Dirección IPv4. . . . . : 192.168.44.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :
```

(No hay posible equivocación ya que es la única conexión que posee puerta de enlace predeterminada)

2) Ejecutamos el comando `/sbin/ifconfig` en el terminal de Linux

```

alumno@localhost:~$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D9:EA:65
          inet6 addr: fe80::20c:29ff:fed9:ea65/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2556 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:335018 (327.1 KiB)  TX bytes:9561 (9.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2904 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2904 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4455748 (4.2 MiB)  TX bytes:4455748 (4.2 MiB)
  
```

- ¿Está el Linux de la máquina virtual en la misma red IPv4 que el Windows de la máquina huésped? ¿Por qué?

Nos resulta imposible determinar si ambas máquinas están en la misma red porque el comando `/sbin/ifconfig` no nos muestra la misma información que su homólogo en Windows `ipconfig`. En Linux no sabemos ni la máscara de red ni el identificador de red.

- ¿A qué se refiere el interfaz “lo” en la máquina virtual?

lo stands for Loopback, que es una interfaz de red que, como su nombre indica, se dedica a realizar pruebas y diagnósticos entre la máquina local (Windows) y la máquina virtual (Linux) de forma que ambas se comuniquen entre sí.

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?

11111111.11111111.111111_00.00000000 → Máscara de Subred (255.255.252.0)

11000000.10101000.101001_00.00011000 → IP Windows (192.168.164.93)

11000000.10101000.101001_01.00011000 → IP Linux (**192.168.165.93**)

- 1) Configuramos la IP y la máscara de subred en Linux con el siguiente comando:

➤ `/sbin/ifconfig <dispositivo> <dirIP> netmask <máscara>`¹

donde el valor de dispositivo será **eth0**, el valor de dirIP el que acaba de calcular; y la máscara la misma que en Windows.

¹ También es posible usar la notación prefijo con `/sbin/ifconfig <dispositivo> <dir>/<prefijo>`

Tras ejecutar dicho comando, podemos comprobar que ahora sí se muestra la misma IPv4 que la máquina local, además de coincidir sus máscaras de red

```
[root@localhost alumno]# /sbin/ifconfig eth0 192.168.165.24 netmask 255.255.252.0
[root@localhost alumno]# /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D9:EA:65
          inet addr:192.168.165.24  Bcast:192.168.167.255  Mask:255.255.252.0
          inet6 addr: fe80::20c:29ff:fed9:ea65/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8022 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:998944 (975.5 KiB)  TX bytes:12717 (12.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2904 errors:0 dropped:0 overruns:0 frame:0
```

Ejercicio 3. Intente ahora hacer desde Linux un ping² 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 **www.informatica.uma.es** como por IP: **150.214.57.91**)

```
alumno@localhost:/home/alumno
File Edit View Terminal Tabs Help
[root@localhost alumno]# ping -c 1 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.018 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.018/0.018/0.018/0.000 ms
[root@localhost alumno]# ping -c 1 192.168.164.24
PING 192.168.164.24 (192.168.164.24) 56(84) bytes of data.
64 bytes from 192.168.164.24: icmp_seq=1 ttl=128 time=2.28 ms

--- 192.168.164.24 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.281/2.281/2.281/0.000 ms
[root@localhost alumno]# ping -c 1 www.informatica.uma.es
ping: unknown host www.informatica.uma.es
[root@localhost alumno]# ping -c 1 150.214.57.91
connect: Network is unreachable
[root@localhost alumno]# ping -c 1 192.168.164.9
PING 192.168.164.9 (192.168.164.9) 56(84) bytes of data.
64 bytes from 192.168.164.9: icmp_seq=1 ttl=128 time=1.74 ms

--- 192.168.164.9 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.745/1.745/1.745/0.000 ms
[root@localhost alumno]# --> profe windows
bash: --: command not found
[root@localhost alumno]# ping -c 1 192.168.165.9
PING 192.168.165.9 (192.168.165.9) 56(84) bytes of data.
64 bytes from 192.168.165.9: icmp_seq=1 ttl=64 time=2.17 ms

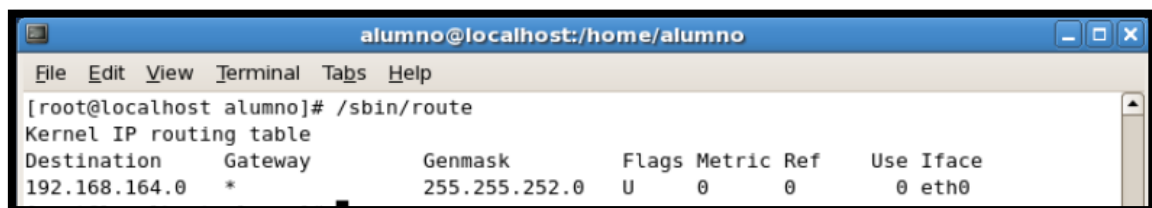
--- 192.168.165.9 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.172/2.172/2.172/0.000 ms
[root@localhost alumno]# --> profe linux
```


- **¿Cuáles funcionan y cuáles no?**

De los siete pings han funcionado los pings a la IP de loopback, la IP de Windows, la IP de Linux y los pings a las máquinas del profesor. Esto se debe a que en todos los casos se hacen referencia a direcciones que están incluidas en la tabla de encaminamiento.

Sin embargo, los pines a www.informatica.uma.es y a su dirección IP 150.214.57.91 no funcionan debido a que ninguna de sus direcciones está especificada en la tabla de encaminamiento.

Ejercicio 4. Observe la tabla de encaminamiento en Linux con el comando `/sbin/route`.



Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.164.0	*	255.255.252.0	U	0	0	0	eth0

- **¿Cómo explica la tabla que solo algunos pings de los anteriores funcionan?**

Aquellos pings que sí funcionaron tenían en común que se efectuaron a direcciones cuyos identificadores de red se encuentran en la tabla de encaminamiento (192.168.164.0)

Los otros dos pings, por otro lado, se efectuaron a direcciones que no se mostraban en dicha tabla. El caso particular de www.informatica.uma.es no se pudo realizar porque dicho dominio no tenía ninguna dirección asociada (el sistema no sabe qué IP tiene asociada ya que no se muestra en la tabla)

Ejercicio 5. Además de consultar la tabla de encaminamiento, con el comando `route` podemos modificarla (necesita ser root, use `sudo` delante del comando).

En concreto podemos (**R** = red, **M** = máscara y **G** = gateway).

- Añadir entrada (entrega directa):** `sudo route add -net R netmask M dev interfazReal`
- Añadir entrada (entrega indirecta):** `sudo route add -net R netmask M gw G`
- Añadir entrada (por defecto):** `sudo route add default gw G`
- Borrar entrada (red destino):** `sudo route del -net R netmask M`
- Borrar entrada (por defecto):** `sudo route del default`

Usando esos comandos realice las siguientes acciones:

- 1) Añada una entrada de encaminamiento por defecto usando el comando c (como valor de gateway use **192.168.167.254**).
- 2) Vuelva a probar los pings que fallaron en el ejercicio 3 comente el motivo por el que ahora funcionan algunos que antes no.

```

alumno@localhost:/home/alumno
File Edit View Terminal Tabs Help
[root@localhost alumno]# /sbin/route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.164.0 * 255.255.252.0 U 0 0 0 eth0
[root@localhost alumno]# sudo /sbin/route add default gw 192.168.167.254
[root@localhost alumno]# ping -c 1 www.informatica.uma.es
ping: unknown host www.informatica.uma.es
[root@localhost alumno]# ping -c 1 150.214.57.91
PING 150.214.57.91 (150.214.57.91) 56(84) bytes of data.

--- 150.214.57.91 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

```

- **¿Funcionan ahora todos los pings?**

Como era de esperar, los pings que antes funcionaron lo siguen haciendo. Sin embargo, esta vez el ping a 150.214.57.91 sí se ha realizado con éxito tal y como muestra la captura.

Esto es debido a que al ejecutar el comando indicado hemos añadido una nueva entrada (la de la red default) a la tabla de encaminamientos y todas aquellas redes que no se encuentren en la tabla se tratarán mediante dicha red

El ping a www.informatica.uma.es sigue sin funcionar porque el problema no se ha solucionado, hay que indicarle una dirección IP que aún no está asociada.

3) Edite el fichero **/etc/resolv.conf** y añada al final la línea **nameserver 150.214.57.7**

```

[root@localhost alumno]# gedit /etc/resolv.conf
(gedit:6559): GnomeUI-WARNING **: While connecting to session manager:
Authentication Rejected, reason : None of the authentication protocols specified are supported and host-based authentication failed.
[root@localhost alumno]# ping -c 1 www.informatica.uma.es
PING informatica.informatica.uma.es (150.214.57.91) 56(84) bytes of data.
64 bytes from informatica.informatica.uma.es (150.214.57.91): icmp_seq=1 ttl=63 time=0.606 ms

--- informatica.informatica.uma.es ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.606/0.606/0.606/0.000 ms

```

- **¿Por qué cree que funcionan los que antes fallaban?**

Tras modificar el fichero, hemos añadido una nueva funcionalidad que permite al sistema que ejecuta un comando ping asignar una dirección IP (150.214.57.91) para aquellas veces en las que se pasa como parámetro una URL. Este es el motivo por el que hasta ahora no funcionaba.

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 con el comando `route PRINT -4`. Haga una captura de pantalla donde se vean todas las entradas de la tabla marcando:

- Entrada que le permite comunicarse con un equipo su propia red física.
- Entrada por defecto.

```
C:\WINDOWS\system32\route PRINT -4
-----
Lista de interfaces
22...c6 15 37 37 9b da .....Hyper-V Virtual Ethernet Adapter
16...8c dc d4 35 9b 4f .....Realtek PCIe GBE Family Controller
25...0a 00 27 00 00 19 .....VirtualBox Host-Only Ethernet Adapter #3
18...0a 00 27 00 00 12 .....Npcap Loopback Adapter
11...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1 #2
12...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8 #2
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            192.168.167.254      192.168.164.24      25
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
172.27.219.208     255.255.255.240    En vínculo           172.27.219.209     271
172.27.219.209     255.255.255.255    En vínculo           172.27.219.209     271
172.27.219.223     255.255.255.255    En vínculo           172.27.219.209     271
192.168.44.0        255.255.255.0      En vínculo           192.168.44.1        291
192.168.44.1        255.255.255.255    En vínculo           192.168.44.1        291
192.168.44.255     255.255.255.255    En vínculo           192.168.44.1        291
192.168.56.0        255.255.255.0      En vínculo           192.168.56.1        281
192.168.56.1        255.255.255.255    En vínculo           192.168.56.1        281
192.168.56.255     255.255.255.255    En vínculo           192.168.56.1        281
192.168.64.0        255.255.255.0      En vínculo           192.168.64.1        291
192.168.64.1        255.255.255.255    En vínculo           192.168.64.1        291
192.168.64.255     255.255.255.255    En vínculo           192.168.64.1        291
192.168.99.0        255.255.255.0      En vínculo           192.168.99.1        281
192.168.99.1        255.255.255.255    En vínculo           192.168.99.1        281
192.168.99.255     255.255.255.255    En vínculo           192.168.99.1        281
192.168.164.0       255.255.252.0      En vínculo           192.168.164.24      281
192.168.164.24     255.255.255.255    En vínculo           192.168.164.24      281
192.168.167.255    255.255.255.255    En vínculo           192.168.164.24      281
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           192.168.56.1        281
224.0.0.0          240.0.0.0          En vínculo           192.168.64.1        291
224.0.0.0          240.0.0.0          En vínculo           192.168.44.1        291
224.0.0.0          240.0.0.0          En vínculo           192.168.99.1        281
224.0.0.0          240.0.0.0          En vínculo           192.168.164.24      281
224.0.0.0          240.0.0.0          En vínculo           172.27.219.209     271
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           192.168.56.1        281
255.255.255.255    255.255.255.255    En vínculo           192.168.64.1        291
255.255.255.255    255.255.255.255    En vínculo           192.168.44.1        291
255.255.255.255    255.255.255.255    En vínculo           192.168.99.1        281
255.255.255.255    255.255.255.255    En vínculo           192.168.164.24      281
255.255.255.255    255.255.255.255    En vínculo           172.27.219.209     271
-----
Rutas persistentes:
Ninguno
```

Ejercicio 7. Desarrolle un código Java que usando la clase previa **liste todos los interfaces de activos** mostrando su nombre, MAC, IP e identificador de la red a la que pertenece incluyendo su prefijo (use solo la primera IP si tiene varias).

Por ejemplo, la salida esperada tendría el siguiente aspecto:

lo: MAC = No disponible | IP = 127.0.0.1 (127.0.0.0/8)

eth3: MAC = D4:5D:64:54:D9:23 | IP = 192.168.1.142 (192.168.1.0/24)

eth20: MAC = 00:15:5D:B9:64:C9 | IP = 172.23.208.1 (172.23.208.0/20)