

### **EJERCICIO N° 1**

Teniendo en cuenta que una empresa tiene 5 sucursales distribuidas de la siguiente manera, todas las sucursales debe tener conexión a Internet:

- SUCURSAL 1 (SAN RAFAEL): 12 HOST y 2 SERVIDORES.
- SUCURSAL 2 (MENDOZA): 25 HOST y 3 SERVIDORES.
- SUCURSAL 3 (BUENOS AIRES): 51 HOST, 5 AP y 6 SERVIDORES.
- SUCURSAL 4 (CÓRDOBA): 10 HOST, 1 AP y 1 SERVIDOR.
- SUCURSAL 5 (SANTA FE): 12 HOST Y 1 SERVIDOR.

RESOLVER LO SIGUIENTE:

- 1) Realizar el direccionamiento utilizando una red /24 para cada una de las sucursales.
- 2) Realizar el direccionamiento óptimo utilizando solo una red /24.
- 3) Llenar las siguientes tablas para cada uno de los casos anteriores y analizar los resultados.

Sucursal	Dirección de Red	Mascara de Subred	Dirección de Broadcast	Rango de IP	N.º host totales	N.º host usados	N.º host libres
1	192.168.1.0	255.255.255.0	192.168.1.255	192.168.1.1 a 192.168.1.254	254	14	240
2	192.168.2.0	255.255.255.0	192.168.2.255	192.168.2.1 a 192.168.2.254	254	28	226
3	192.168.3.0	255.255.255.0	192.168.3.255	192.168.3.1 a 192.168.3.254	254	62	192
4	192.168.4.0	255.255.255.0	192.168.4.255	192.168.4.1 a 192.168.4.254	254	12	242
5	192.168.5.0	255.255.255.0	192.168.5.255	192.168.5.1 a 192.168.5.254	254	13	241

Sucursal	Dirección de Red	Mascara de Subred	Dirección de Broadcast	Rango de IP	N.º host totales	N.º host usados	N.º host libres
3	192.168.1.0 /25	255.255.255.128	192.168.1.127	192.168.1.1 a 192.168.1.126	126	63	63
2	192.168.1.128 /27	255.255.255.224	192.168.1.159	192.168.1.129 a 192.168.1.158	30	29	1
1	192.168.1.160 /27	255.255.255.224	192.168.1.191	192.168.1.161 a 192.168.1.190	30	15	15
5	192.168.1.192 /28	255.255.255.240	192.168.1.207	192.168.1.193 a 192.168.1.206	14	14	0
4	192.168.1.208 /28	255.255.255.240	192.168.1.223	192.168.1.209 a 192.168.1.222	14	13	1

## EJERCICIO N° 2

Indicar si las siguientes direcciones IP son de host, red o broadcast. Por qué?

- a. 192.168.1.16/29 → es una dirección de red (coincide con la dirección de red y la parte de host/broadcast se encuentra solo en bits 0)  
Dir. IP: 1 0 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 1 0 0 0 0  
Masc. de red: 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 0 0 0  
**Resultado:** 1 0 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 1 0 0 0 0
- b. 10.59.58.255/23 → es una dirección de host (se encuentra entre la dirección de red y la de broadcast y la parte de host/broadcast se encuentra intercalado de 0 y 1)  
Dir. IP: 0 0 0 0 1 0 1 0 . 0 0 1 1 1 0 1 1 . 0 0 1 1 1 0 1 0 . 1 1 1 1 1 1 1 1  
Masc. de red: 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 0 . 0 0 0 0 0 0 0 0  
**Resultado:** 0 0 0 0 1 0 1 0 . 0 0 1 1 1 0 1 1 . 0 0 1 1 1 0 1 1 . 0 0 0 0 0 0 0 0
- c. 126.255.255.255/16 → es una dirección de broadcast (es la última dirección)  
Dir. IP: 0 1 1 1 1 1 1 0 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1  
Masc. de red: 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0  
**Resultado:** 0 1 1 1 1 1 1 0 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0
- d. 172.16.0.0/16 → es una dirección de red (coincide con la dirección de red y la parte de host/broadcast se encuentra solo en bits 0)  
Dir. IP: 1 0 1 0 1 1 0 0 . 0 0 0 1 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0  
Masc. de red: 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0  
**Resultado:** 1 0 1 0 1 1 0 0 . 0 0 0 1 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0
- e. 192.168.1.18/28 → es una dirección de host (se encuentra entre la dirección de red y la de broadcast y la parte de host/broadcast se encuentra intercalado de 0 y 1)  
Dir. IP: 1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 1 0 0 1 0  
Masc. de red: 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 0 0 0 0  
**Resultado:** 1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 1 . 0 0 0 1 0 0 1 0
- f. 150.32.248.0/18 → es una dirección de host (se encuentra entre la dirección de red y la de broadcast y la parte de host/broadcast se encuentra intercalado de 0 y 1)  
Dir. IP: 1 0 0 1 0 1 1 0 . 0 0 1 0 0 0 0 0 . 1 1 1 1 1 0 0 0 . 0 0 0 0 0 0 0 0  
Masc. de red: 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0  
**Resultado:** 1 0 0 1 0 1 1 0 . 0 0 1 0 0 0 0 0 . 1 1 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0

## EJERCICIO N° 3

Para las siguientes redes indicar cuales con las primeras 5 direcciones IP disponibles para hosts y las últimas 5 direcciones IP disponibles para hosts:

- a) 159.22.21.0/25

Primeras:	Últimas:
159.22.21.1	159.22.21.122
159.22.21.2	159.22.21.123
159.22.21.3	159.22.21.124
159.22.21.4	159.22.21.125
159.22.21.5	159.22.21.126

**b) 52.168.0.0./16**

Primeras:	Últimas:
52.168.0.1	52.168.255.250
52.168.21.2	52.168.255.251
52.168.21.3	52.168.255.252
52.168.21.4	52.168.255.253
52.158.21.5	52.168.255.254

**c) 200.115.66.0/30**

Solamente se encuentran 2 direcciones disponibles:

200.115.66.1

200.115.66.2

#### **EJERCICIO N° 4**

Dada la red 192.168.0.0/24, desarrolle un esquema de direccionamiento que cumpla con los siguientes requerimientos. Optimice el espacio de direccionamiento tanto como sea posible.

1. Una subred de 30 hosts para Profesores.
2. Una subred de 90 hosts para Estudiantes.
3. Una subred de 20 hosts para Invitados.
4. Tres subredes de 2 hosts para enlaces entre enrutadores.

Subred	Direccion de red	Mascara de subred	Direccion de broadcast	Rango de IP	N.º host totales	N host usados	N host libres
Estudiantes /25	192.168.0.0	255.255.255.128	192.168.0.127	192.168.0.1 a 192.168.0.126	126	90	36
Profesores /27	192.168.0.128	255.255.255.224	192.168.0.159	192.168.0.129 a 192.168.0.158	30	30	0
Invitados /27	192.168.0.160	255.255.255.224	192.168.0.191	192.168.0.161 a 192.168.0.190	30	20	10
Enlace 1 /30	192.168.0.192	255.255.255.252	192.168.0.195	192.168.0.161 y 192.168.0.190	2	2	0
Enlace 2 /30	192.168.0.196	255.255.255.252	192.168.0.199	192.168.0.197 y 192.168.0.198	2	2	0
Enlace 3 /30	192.168.0.200	255.255.255.252	192.168.0.203	192.168.0.201 y 192.168.0.202	2	2	0

### **EJERCICIO N° 5**

En una red Ethernet, un host tiene configurada la dirección IP 150.10.10.12/26. Debe enviar un paquete a la dirección 150.10.10.58/26.

- Describe y muestre la operación que debe hacerse para saber si la IP destino pertenece a la misma red.
  - Realice la misma operación que “a” si ahora la dirección IP destino es 150.10.10.88/26.
  - Describe las diferencias.
- La dirección 150.10.10.58/26 está dentro de la misma red.  
Para comprobar si las ip de los hosts pertenecen a una misma red debemos convertir cada ip de host con su máscara a binario

Luego para saber a qué red pertenece el origen comparamos cada bit del host con cada bit de la máscara mediante la operación lógica AND, resultando en:

```
150.10.10.12/26 >>>> 1 0 0 1 0 1 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 1 1 0 0
                        and 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0
                        -----
                        1 0 0 1 0 1 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 0 0 0 0
```

150.10.10.0 Red

El siguiente paso consiste en realizar el mismo procedimiento para el host y máscara de destino:

```
150.10.10.58 >>>> 1 0 0 1 0 1 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 1 0 1 0 . 0 0 1 1 1 0 1 0
                        and 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0
                        -----
                        1 0 0 1 0 1 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 0 0 0 0
```

Red obtenida: 150.10.10.0

Rango de host: 150.10.10.0 hasta 150.10.10.62

Como podemos observar, las redes obtenidas son las mismas, denotando que la ip de origen, y la de destino pertenecen a la misma red.

- Realice la misma operación que “a” si ahora la dirección IP destino es 150.10.10.88/26  
150.10.10.88/26 >>>> 1 0 0 1 0 1 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 1 0 1 0 . 0 1 0 1 1 0 0 0  
 and 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0  
 -----  
 1 0 0 1 0 1 1 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 1 0 1 0 . 0 1 0 0 0 0 0 0  
150.10.10.64 Dirección red  
150.10.10.127 Dirección de broadcast  
La dirección 150.10.10.88 no se encuentra en la misma red

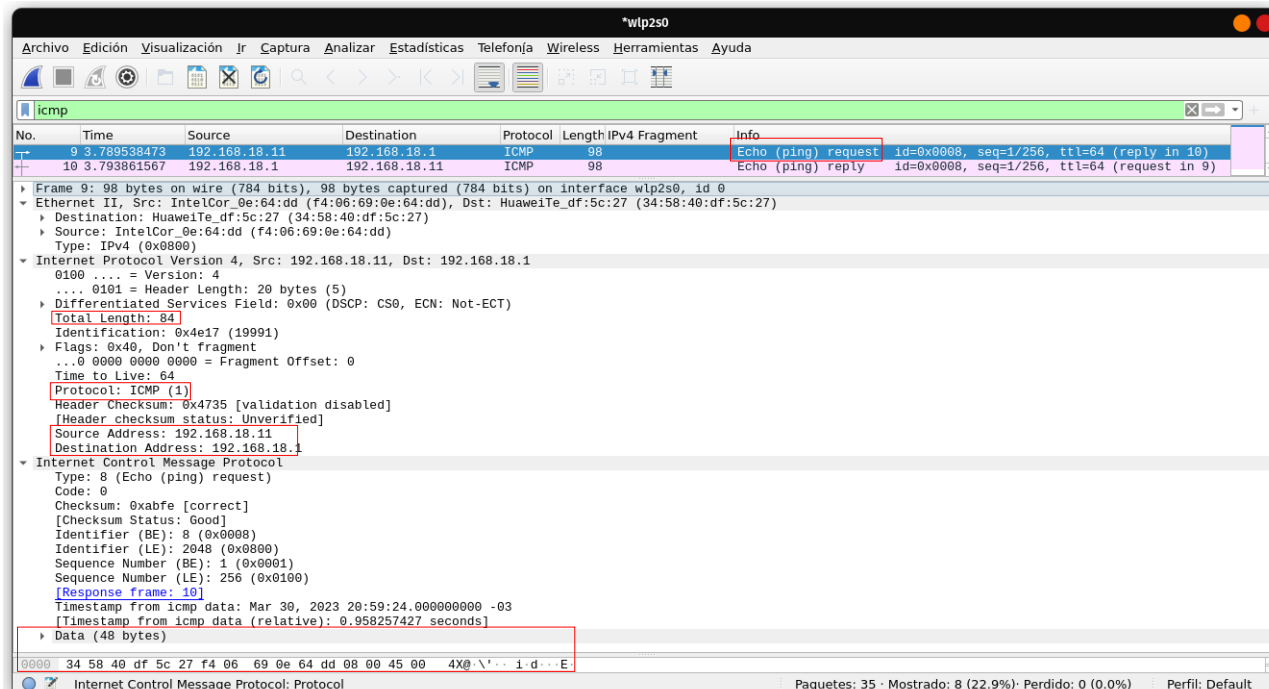
- Describe las diferencias.  
Si comparas la ip con la máscara está todo en 0 osea que está dentro de la misma red.  
La diferencia notable es que los factores que nos pueden indicar que dos hosts son distintos suelen ser la dirección de red y la máscara. Es importante de determinar si las direcciones ip pertenecen a una misma red o no, para saber con precisión hacia qué lugar serán enviados los datos.

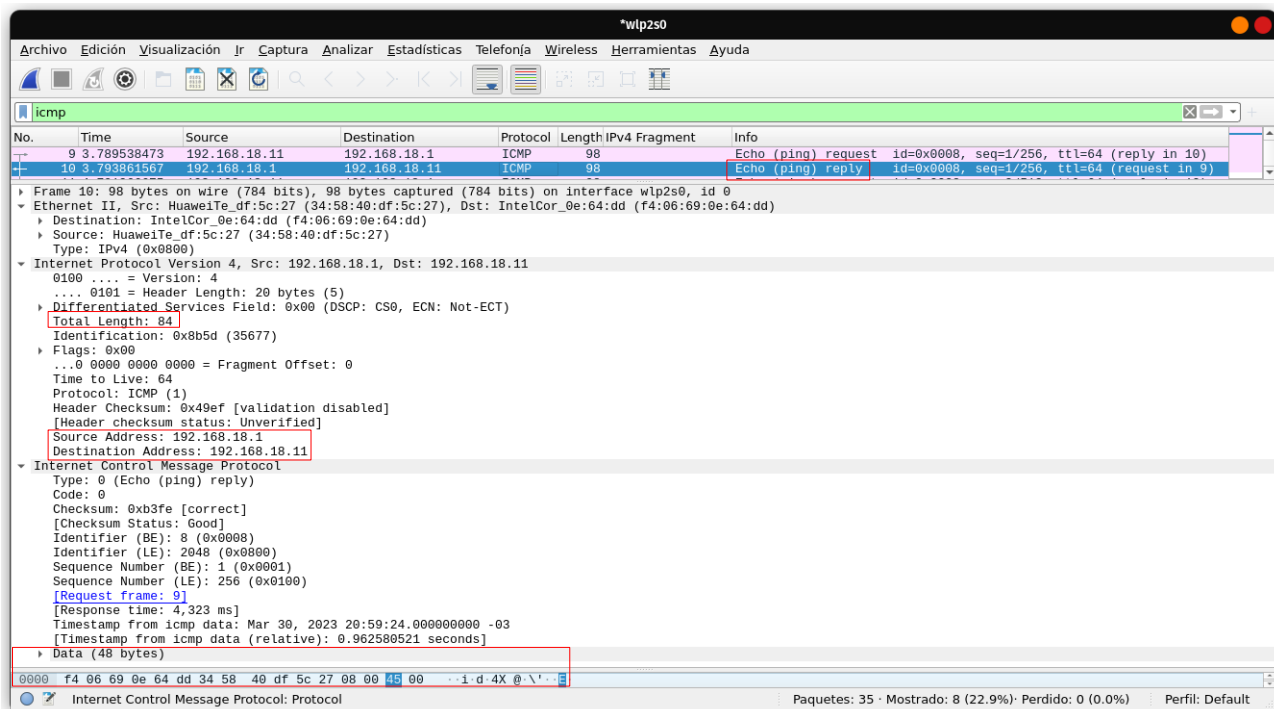
**EJERCICIO N° 6**

Dada la siguiente dirección de red: 19.13.0.0/8, dividirla en subredes de las siguientes capacidades:

1. 2 subredes de 1000 hosts
2. 2 subredes 2000 hosts
3. 2 subredes de 5000 host
4. 1 subred de 14000 host
5. 2 subred de 70 hosts
6. 2 subredes de 2 hosts

Subred	Dirección de red	Máscara de subred	Dirección de broadcast	Rango de IP	N.º host totales	N host usados	N host libres
1	19.0.0.0 /18	255.255.192.0	19.0.63.255	19.0.0.1 a 19.0.63.254	16382	14000	2382
2	19.0.64.0 /19	255.255.224.0	19.0.95.255	19.0.64.1 a 19.0.95.254	8190	5000	3190
3	19.0.96.0 /19	255.255.224.0	19.0.127.255	19.0.96.1 a 19.0.127.254	8190	5000	3190
4	19.0.128.0 /21	255.255.248.0	19.0.135.255	19.0.128.1 a 19.0.135.254	2046	2000	46
5	19.0.136.0 /21	255.255.248.0	19.0.143.255	19.0.136.1 a 19.0.143.254	2046	2000	46
6	19.0.144.0 /22	255.255.252.0	19.0.147.255	19.0.144.1 a 19.0.147.254	1022	1000	22
7	19.0.148.0 /22	255.255.252.0	19.0.151.255	19.0.148.1 a 19.0.151.254	1022	1000	22
8	19.0.152.0 /25	255.255.255.128	19.0.152.127	19.0.152.1 a 19.0.152.126	126	70	56
9	19.0.152.128 /25	255.255.255.128	19.0.152.255	19.0.152.129 a 19.0.152.254	126	70	56
10	19.0.153.0 /30	255.255.255.252	19.0.153.3	19.0.153.1 a 19.0.153.2	2	2	0
11	19.0.153.4 /30	255.255.255.252	19.0.153.7	19.0.153.5 a 19.0.153.6	2	2	0





## EJERCICIO N° 8

Deje el correr el analizador unos 5 minutos, mientras usa distintos accesos a su red (ya sea en forma local o a Internet). Por ejemplo, navegue en Internet, acceda a su correo, acceda a su servidor de archivos, etc.  
Analice ahora su captura e informe:

a) ¿Cuántos paquetes IP se enviaron y recibieron?

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	47769				0.1244	100%	5.3900	80,226
52.5.112.135	105				0.0003	0.22%	0.1100	157,271
35.161.224.95	3				0.0000	0.01%	0.0200	212,170
34.120.208.123	164				0.0004	0.34%	0.1700	6,496
34.117.237.239	10				0.0000	0.02%	0.0700	69,818
239.255.255.250	168				0.0004	0.35%	0.0200	62,933
224.0.0.251	22				0.0001	0.05%	0.0100	9,569
216.58.202.86	74				0.0002	0.15%	0.2800	63,303
216.58.202.74	56				0.0001	0.12%	0.2600	21,180
216.58.202.110	14				0.0000	0.03%	0.1300	9,295
200.51.41.141	530				0.0014	1.11%	0.6800	17,186
200.51.41.139	34				0.0001	0.07%	0.1200	15,381
200.115.94.211	3545				0.0092	7.42%	5.1500	363,291
20.201.28.151	303				0.0008	0.63%	1.2100	36,012
192.168.18.9	43				0.0001	0.09%	0.0100	2,268
192.168.18.255	13				0.0000	0.03%	0.0100	2,268
192.168.18.11	47566				0.1239	99.58%	5.3800	80,226
192.168.18.10	136				0.0004	0.28%	0.0100	2,659
192.168.18.1	314				0.0008	0.66%	0.1200	9,717
192.168.0.3	308				0.0008	0.64%	0.0400	0,000
192.168.0.16	154				0.0004	0.32%	0.0200	0,000

Se enviaron y recibieron 47769 paquetes



- b) ¿Cuál es la dirección IP con la que más paquetes se intercambiaron? ¿A quién pertenece dicha IP?

Wireshark - Conversations - wlp2s0

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.18.11	138.97.176.237	25,244	32 M	2,074	198 k	23,170	32 M	59.482543	154.2693	10 k	1.673 k
192.168.18.11	142.251.134.78	3,870	4,385 k	557	225 k	3,313	4,160 k	12.094964	362.1080	4.977	91 k
192.168.18.11	200.115.94.211	3,545	4,559 k	324	34 k	3,221	4,525 k	353.244837	20.8498	13 k	1.736 k
192.168.18.11	142.251.133.5	3,003	4,235 k	1,145	252 k	1,858	3,982 k	6.482428	375.1458	5,386	84 k
192.168.18.11	142.251.134.14	1,902	1,973 k	407	170 k	1,495	1,803 k	9.804062	70.4616	19 k	204 k
192.168.18.11	138.97.176.236	1,035	1,300 k	99	15 k	936	1,285 k	353.133135	18.4964	6,584	556 k
192.168.18.11	142.251.133.195	777	530 k	301	39 k	476	491 k	6.626210	179.2270	1,776	21 k
192.168.18.11	151.139.128.10	715	1,541 k	354	38 k	361	1,503 k	143.016786	187.4546	1,622	64 k
192.168.18.11	142.251.133.238	573	559 k	141	30 k	432	529 k	12.110842	170.7397	1,406	24 k
192.168.18.11	200.51.41.141	530	434 k	256	40 k	274	393 k	13.246579	137.4422	2,363	22 k
192.168.18.11	172.217.173.246	481	438 k	129	18 k	352	419 k	49.248245	304.4680	497	11 k
192.168.18.11	142.251.133.206	441	126 k	227	87 k	214	39 k	36.920469	345.2959	2,025	911
192.168.18.11	18.64.174.25	433	355 k	205	17 k	228	338 k	153.973177	195.0301	730	13 k
192.168.18.11	192.168.0.3	308	299 k	308	299 k	0	0	0.000345	379.9986	6,299	0
192.168.18.11	20.201.28.151	303	294 k	136	26 k	167	267 k	32.790114	124.5177	1,690	17 k
192.168.18.11	142.251.133.227	300	98 k	119	32 k	181	66 k	6.489193	357.2517	735	1,480
192.168.18.11	192.168.18.1	290	64 k	145	13 k	145	50 k	3.553734	367.0477	288	1,109
192.168.18.11	142.250.79.67	278	234 k	88	15 k	190	219 k	9.145185	148.8118	824	11 k
192.168.18.11	185.199.109.154	256	188 k	128	13 k	128	174 k	34.244614	173.6125	620	8,045
192.168.18.11	18.65.48.73	256	298 k	128	12 k	128	286 k	144.630793	172.2321	575	13 k
192.168.18.11	142.251.133.74	244	62 k	119	25 k	125	36 k	27.875855	352.0786	589	833
192.168.18.11	142.251.134.42	236	110 k	106	19 k	130	91 k	9.066317	179.7878	864	4,073
192.168.18.11	172.64.132.15	209	204 k	32	7,277	177	197 k	143.532239	0.7751	75 k	2,032 k

Resolución de nombre Limitar filtro de visualización Hora de inicio absoluta

Ayuda Copiar Seguir flujo... Gráfica... Cerrar

La dirección IP 138.97.176.237 fue con la que más paquetes se intercambiaron y pertenece a Cable Televisora Color.

## EJERCICIO N° 9

Uso del comando Ping:

- a) Ejecute el comando ping a su puerta de enlace predeterminada. Mostrar el resultado y comentar que significa cada campo de respuesta.

```
oltyxs@bangho:~
oltyxs@bangho:~ 64x19
> ping 10.51.0.2
PING 10.51.0.2 (10.51.0.2) 56(84) bytes of data.
64 bytes from 10.51.0.2: icmp_seq=1 ttl=64 time=1.39 ms
64 bytes from 10.51.0.2: icmp_seq=2 ttl=64 time=1.50 ms
64 bytes from 10.51.0.2: icmp_seq=3 ttl=64 time=1.81 ms
64 bytes from 10.51.0.2: icmp_seq=4 ttl=64 time=2.08 ms
64 bytes from 10.51.0.2: icmp_seq=5 ttl=64 time=2.33 ms
64 bytes from 10.51.0.2: icmp_seq=6 ttl=64 time=1.67 ms
64 bytes from 10.51.0.2: icmp_seq=7 ttl=64 time=4.29 ms
^C
--- 10.51.0.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 1.389/2.152/4.291/0.923 ms
took 7s base
```

**64 bytes:** tamaño del paquete que envía.  
**from 10.51.0.2:** es el destino al que hicimos ping, en este caso el gateway.  
**icmp\_seq:** es el número de secuencia de cada paquete ICMP. Aumenta en uno por cada solicitud.  
**ttl:** es el valor de tiempo de vida, representa el número de saltos de red que puede hacer un paquete antes de que un enrutador lo descarte.  
**time:** es el tiempo que tarda un paquete en llegar a destino y volver al origen.



- b) Ejecute el comando ping a la dirección IP 8.8.8.8. Mostrar resultado y verificar tiempo de respuesta.

```
ollyxs@bangho:~  
ollyxs@bangho:~ 80x24  
> ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=126 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=60.7 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=37.3 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=29.6 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=36.1 ms  
64 bytes from 8.8.8.8: icmp_seq=6 ttl=113 time=29.6 ms  
^C  
--- 8.8.8.8 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5008ms  
rtt min/avg/max/mdev = 29.586/53.270/126.414/34.341 ms  
took 5s base
```

- c) Investigue para qué sirve el parámetro -l (-s en Linux) con el comando ping y realice una prueba. Escriba sus comentarios.

```
ollyxs@bangho:~  
ollyxs@bangho:~ 80x24  
> ping -s 10 10.51.14.241  
PING 10.51.14.241 (10.51.14.241) 10(38) bytes of data.  
18 bytes from 10.51.14.241: icmp_seq=1 ttl=64  
18 bytes from 10.51.14.241: icmp_seq=2 ttl=64  
18 bytes from 10.51.14.241: icmp_seq=3 ttl=64  
18 bytes from 10.51.14.241: icmp_seq=4 ttl=64  
18 bytes from 10.51.14.241: icmp_seq=5 ttl=64  
18 bytes from 10.51.14.241: icmp_seq=6 ttl=64  
18 bytes from 10.51.14.241: icmp_seq=7 ttl=64  
18 bytes from 10.51.14.241: icmp_seq=8 ttl=64  
18 bytes from 10.51.14.241: icmp_seq=9 ttl=64  
^C  
--- 10.51.14.241 ping statistics ---  
9 packets transmitted, 9 received, 0% packet loss, time 8170ms  
took 9s base
```

El parámetro -s en Linux sirve para enviar un tamaño de buffer

- d) Ejecute el comando ping a 8.8.8.8 -i 3 (-t en Linux) . Mostrar el resultado y comentar que significa la respuesta, modifique el parámetro hasta que obtenga una respuesta positiva.

```
ollyxs@bangho:~  
ollyxs@bangho:~ 80x24  
> ping -t 3 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
From 209.13.176.201 icmp_seq=1 Time to live exceeded  
From 209.13.176.201 icmp_seq=2 Time to live exceeded  
From 209.13.176.201 icmp_seq=3 Time to live exceeded  
From 209.13.176.201 icmp_seq=4 Time to live exceeded  
From 209.13.176.201 icmp_seq=5 Time to live exceeded  
^C  
--- 8.8.8.8 ping statistics ---  
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4005ms  
  
> ping -t 15 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=31.0 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=30.4 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=30.9 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=29.6 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=30.0 ms  
^C  
--- 8.8.8.8 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 29.613/30.403/31.046/0.546 ms  
took 4s base
```

El parámetro -t establece el indicador de tiempo de vida, como podemos ver, si se agota el tiempo de espera se pierde el paquete.

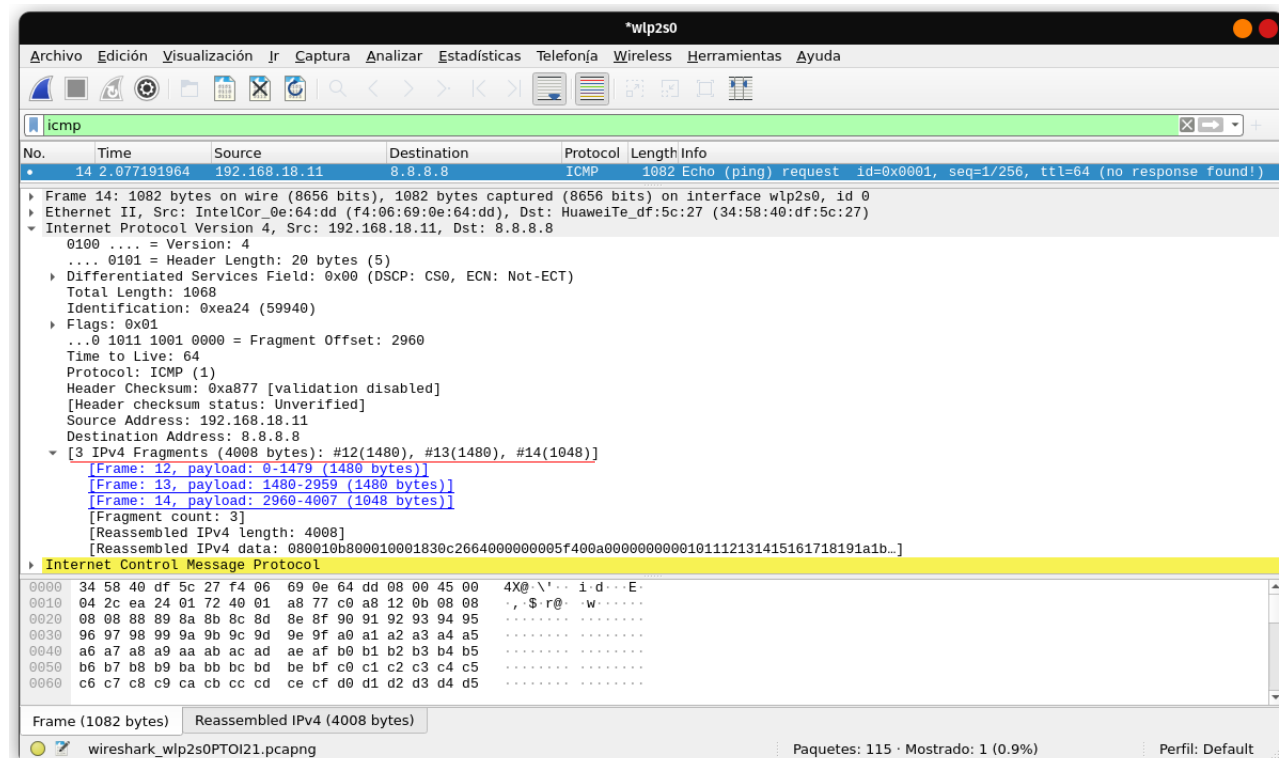
### EJERCICIO N° 10

Ejecute el comando ping a 8.8.8.8 -n 1 -l 4000.

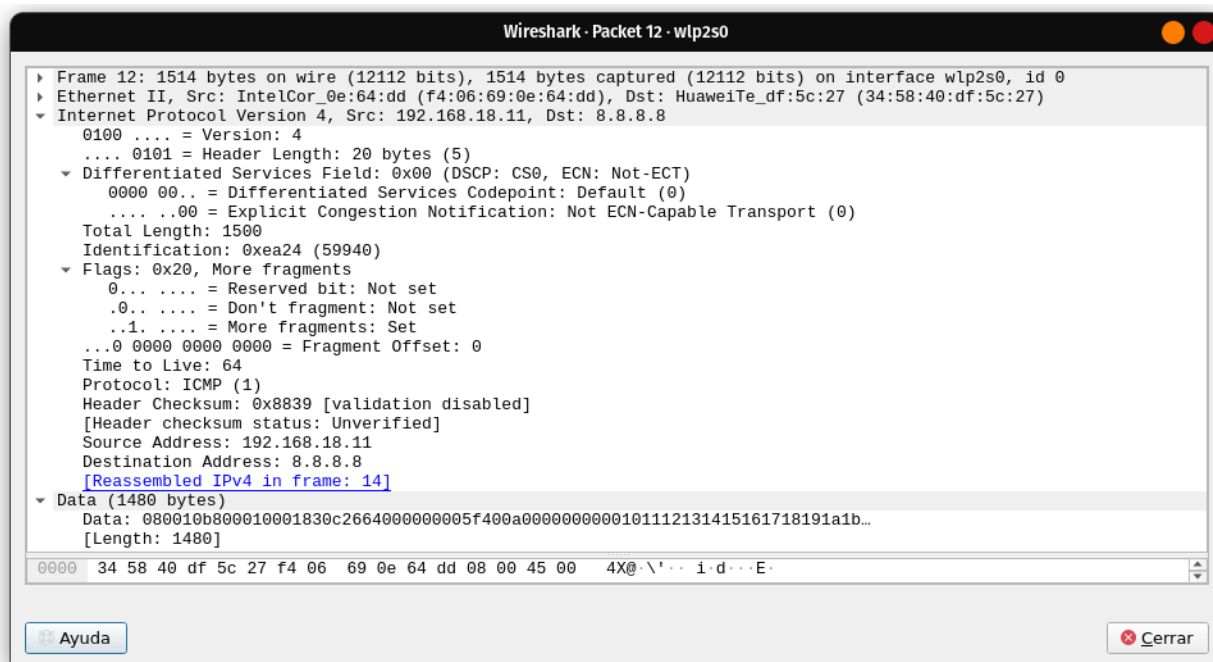
Si se obtuvo respuesta correcta, inicie el sniffer Wireshark, coloque el filtro ICMP y comience una captura, ejecute nuevamente el comando. Pare la captura e indique:

- Determine la cantidad de paquetes IP del envío.
- Represente y compare los campos de longitud total, flags y desplazamiento del fragmento para todos los paquetes.
- Indique el valor del campo protocolo de la cabecera de los fragmentos IP ¿es el mismo?
- Indique que tamaño de mensaje es necesario para generar un fragmento más.
- Indique la cantidad de bytes que viajan en cada paquete

```
ollyxs@bangho:~  
ollyxs@bangho:~ 64x9  
> ping -c 1 -s 4000 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 4000(4028) bytes of data.  
  
--- 8.8.8.8 ping statistics ---  
1 packets transmitted, 0 received, 100% packet loss, time 0ms  
  
took 10s base
```

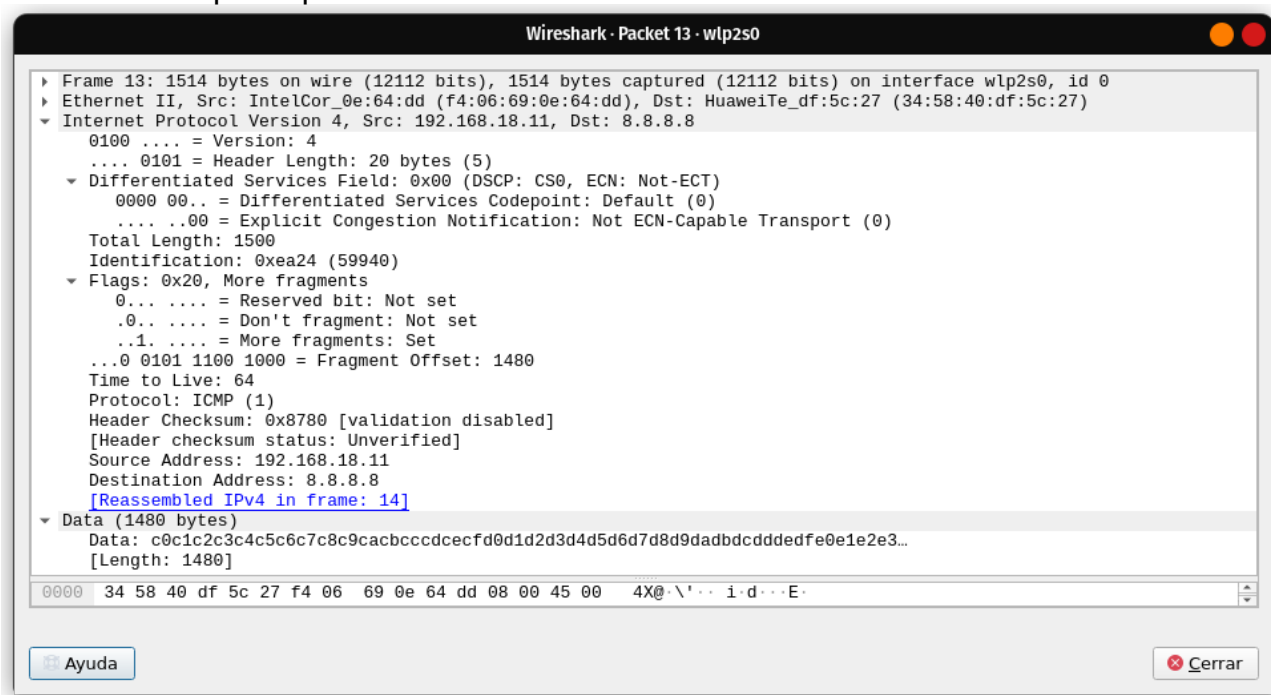


- Al hacer el ping obtuvimos una respuesta incorrecta porque es un paquete es muy grande para ser enviado pero al analizar con wireshark observamos que lo divide en 3 fragmentos.
- Al expandir cada fragmento del paquete podemos observar en detalle cada fragmento con los campos que se requieren, longitud total del fragmento, flags, fragments offset.



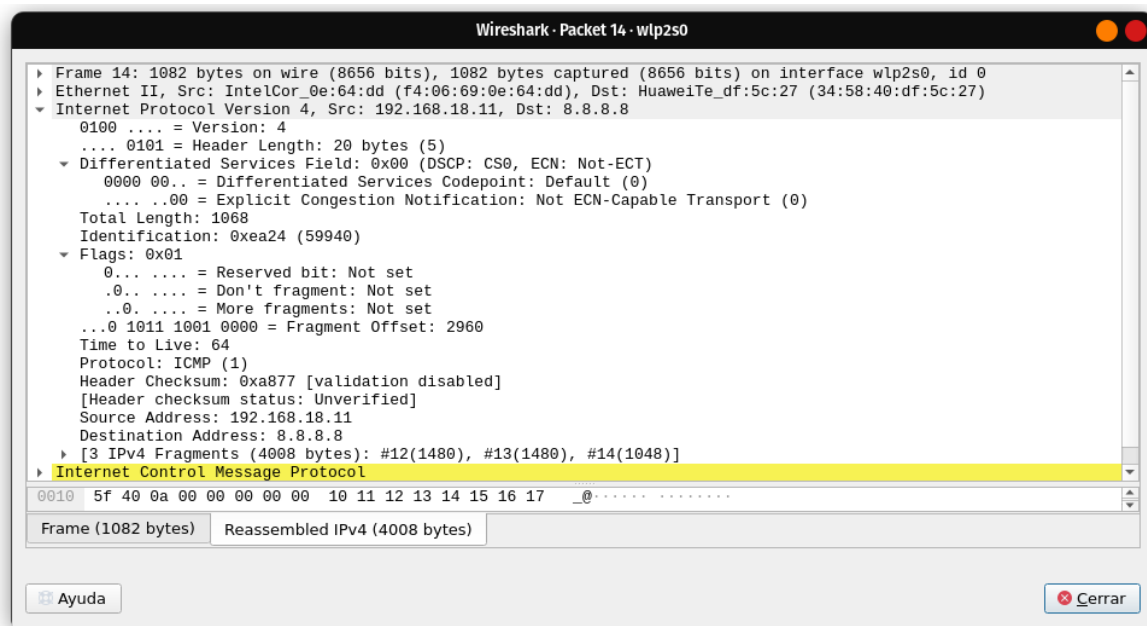
#### Fragmento 12:

- Longitud total del fragmento: 1500
- Flags: Al ser el primer fragmento, se activa el 1 de que vienen más paquete
- Desplazamiento del fragmento: Posición 0
- Campo de protocolo: ICMP 1



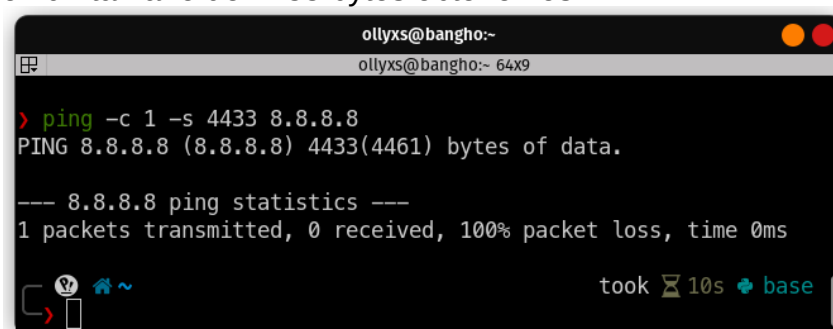
#### Fragmento 13:

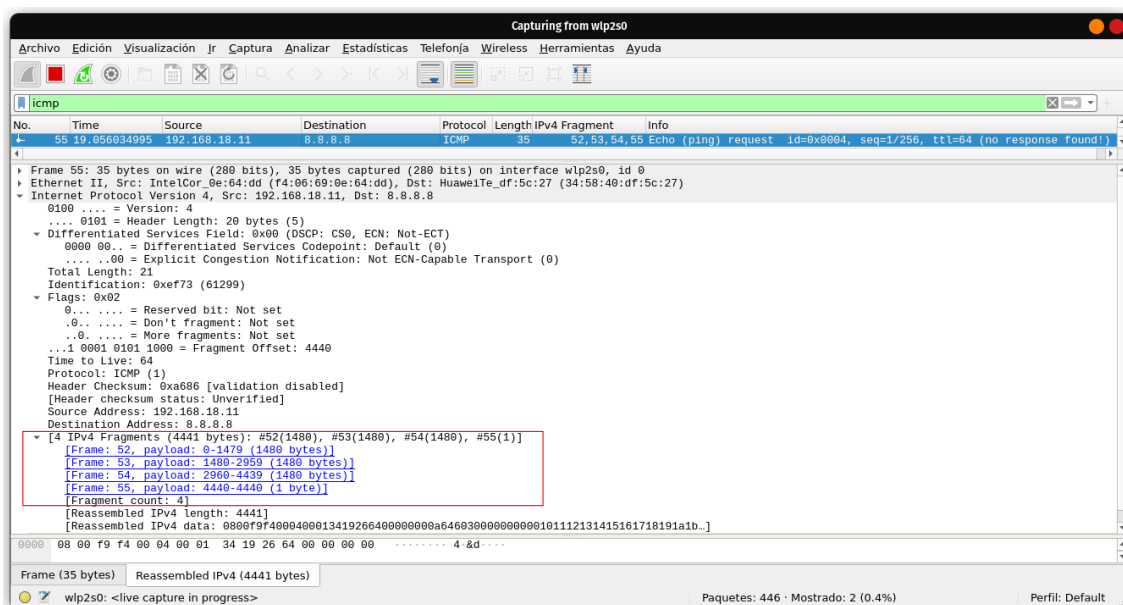
- Longitud total del fragmento: 1500
- Flags: Al ser el primer fragmento, se activa el 1 de que vienen más paquete
- Desplazamiento del fragmento: Posición 1480
- Campo de protocolo: ICMP 1



Fragmento 14:

- Longitud total del fragmento: 1068
  - Flags: Ningún bit de flag activado ya que se trata del último fragmento del paquete
  - Desplazamiento del fragmento: Posición 2960
  - Campo de protocolo: ICMP 1
- c) Teniendo como referencia las imágenes del punto anterior, podemos ver que el valor del campo protocolo en el encabezado de cada uno de los fragmentos es el mismo: ICMP 1.
- d) Para poder generar un nuevo fragmento en el paquete, el tamaño del mismo debe ser mayor a 4432, por lo que si realizamos una nueva petición ping a la puerta de enlace con un tamaño de 4433 bytes obtenemos.





e) Los tamaños de los fragmentos son:

▶ Frame 12:	1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlp2s0, id 0
▶ Frame 13:	1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlp2s0, id 0
▶ Frame 14:	1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits) on interface wlp2s0, id 0

### EJERCICIO N° 11

Repita el ejercicio 10, pero agregando el parámetro -f (-M en Linux). ¿Qué resultado obtuvo? ¿Por qué?

No es posible enviar el paquete porque el parámetro -M indica no fragmentar el paquete, pero el mismo requiere ser fragmentado, ya que su tamaño es de 4000 bytes y el MTU del receptor está limitado a 1500 bytes.

Es por esto que obtenemos el siguiente mensaje:

