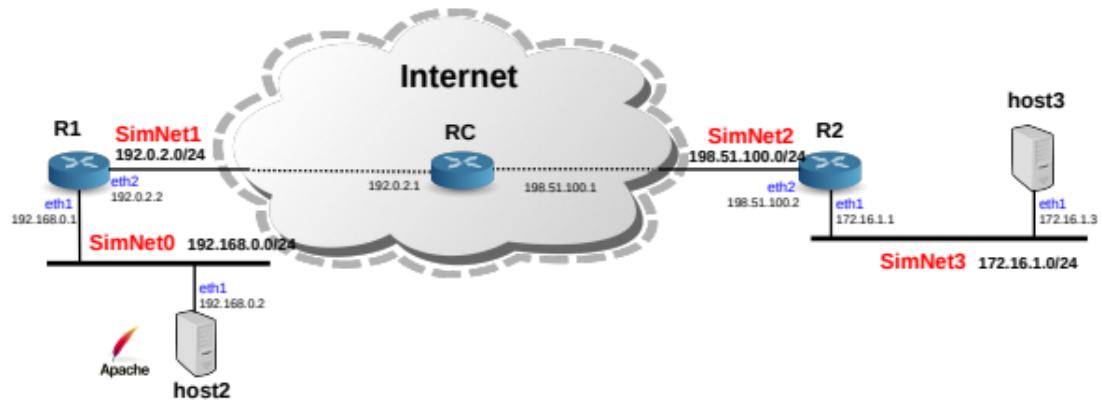


## P9: IP Tunnels



### 0.3 starting the scenario using simctl

```
//from terminal  
simctl iptunnel sh  
start
```

```
Virtual machines from iptunnel:  
num      vms      enabled  tty's  Id  
1        RC       0  
2        R2       0  
3        host3    0  
4        R1       0  
5        host2    0
```

### 0.4 Configuring IPIP tunnels

```
//from R2  
ip tunnel add tunnel0 mode ipip local 198.51.100.2 remote 192.0.2.2 ttl 0 nopmtudisc  
dev eth2                                     #configuring the tunnel  
ifconfig tunnel0 1.2.3.4                      #activando la nueva interfaz virtual  
route add -net 192.168.0.0/24 dev tunnel0      #actualizar tabla de ruta  
...  
R2:~# ip tunnel add tunnel0 mode ipip local 198.51.100.2 remote 192.0.2.2 ttl 0  
nopmtudisc dev eth2  
R2:~# ifconfig tunnel0 1.2.3.4  
R2:~# route add -net 192.168.0.0/24 dev tunnel0
```

```
//from R1
```

```
ip tunnel add tunnel0 mode ipip local 192.0.2.2 remote 198.51.100.2 ttl 0 nopmtudisc  
dev eth2  
ifconfig tunnel0 1.2.3.4  
route add -net 172.16.1.0/24 dev tunnel0
```

## 0.5 Testing the tunnels: protocol and TTL fields

1. Open FOUR wireshark network analyzers in the PHYSICAL HOST and capture traffic in each of these networks: SimNet0, SimNet1, SimNet2 and SimNet3.

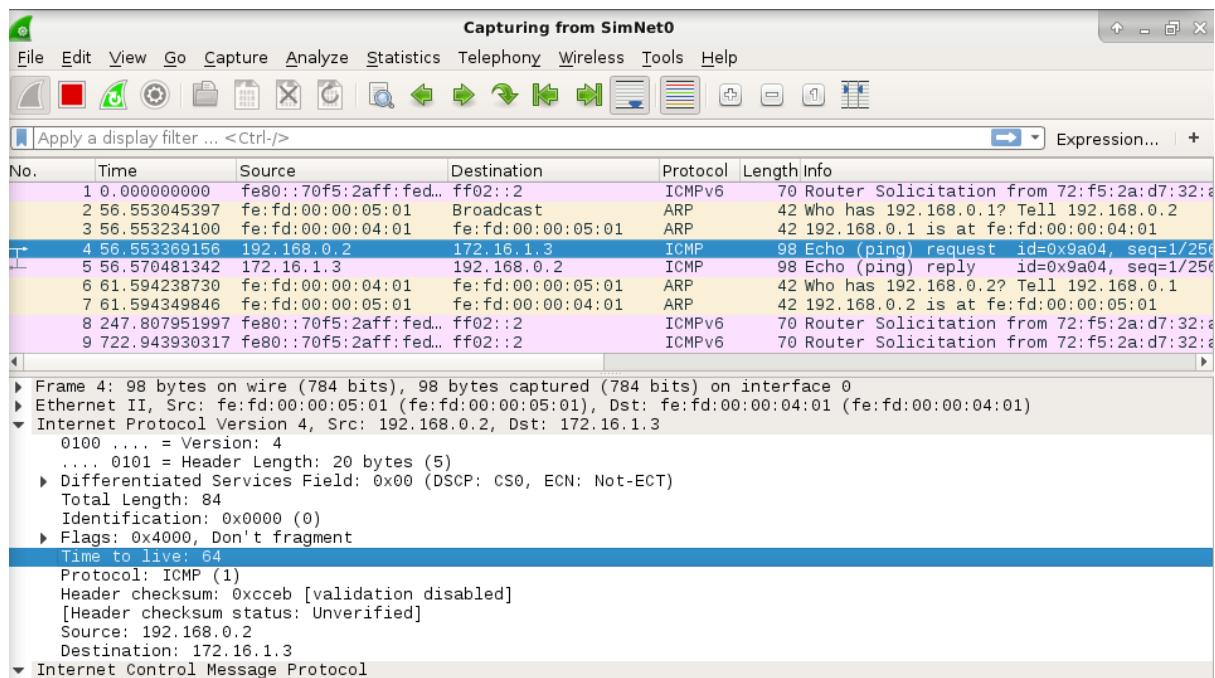
To properly see fragmented messages, DISABLE the following option in all these wiresharks:Edit-Preferences-Protocols-IPv4-Reassemble fragmented IPv4 datagrams.

2. Send the following ping from host2 to host3:

```
//from host2
ping -c1 172.16.1.3
```

```
host2:~# ping -c1 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 56(84) bytes of data.
64 bytes from 172.16.1.3: icmp_seq=1 ttl=62 time=38.1 ms

--- 172.16.1.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 38.183/38.183/38.183/0.000 ms
```



**Capturing from SimNet1**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
2	34.025632578	fe:fd:00:00:04:02	Broadcast	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2
3	34.026707413	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.1 is at fe:fd:00:00:01:01
4	34.026853518	192.168.0.2	172.16.1.3	ICMP	118	Echo (ping) request id=0x9a04, seq=1/2
5	34.042318685	172.16.1.3	192.168.0.2	ICMP	118	Echo (ping) reply id=0x9a04, seq=1/2
6	39.055557578	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
7	39.055711169	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:04:02
8	258.047914098	fe80::740d:17ff:fea.. ff02::2		ICMPv6	70	Router Solicitation from 76:0d:17:a6:11
9	765.951998819	fe80::740d:17ff:fea.. ff02::2		ICMPv6	70	Router Solicitation from 76:0d:17:a6:11

Frame 4: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0

Ethernet II, Src: fe:fd:00:00:04:02 (fe:fd:00:00:04:02), Dst: fe:fd:00:00:01:01 (fe:fd:00:00:01:01)

Internet Protocol Version 4, Src: 192.0.2.2, Dst: 198.51.100.2

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 104
- Identification: 0x0000 (0)
- Flags: 0x4000, Don't fragment
- Time to live: 63
- Protocol: IP (4)
- Header checksum: 0x4f5a [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.0.2.2
- Destination: 198.51.100.2

Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x0000 (0)
- Flags: 0x4000, Don't fragment
- Time to live: 63
- Protocol: ICMP (1)
- Header checksum: 0xcdeb [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.2
- Destination: 172.16.1.3

Internet Control Message Protocol

**Capturing from SimNet2**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
2	21.753250882	fe:fd:00:00:01:02	Broadcast	ARP	42	Who has 198.51.100.2? Tell 198.51.100.1
3	21.753452293	fe:fd:00:00:02:02	fe:fd:00:00:01:02	ARP	42	198.51.100.2 is at fe:fd:00:00:02:02
4	21.753563289	192.168.0.2	172.16.1.3	ICMP	118	Echo (ping) request id=0x9a04, seq=1/2
5	21.754279822	172.16.1.3	192.168.0.2	ICMP	118	Echo (ping) reply id=0x9a04, seq=1/2
6	26.772902422	fe:fd:00:00:02:02	fe:fd:00:00:01:02	ARP	42	Who has 198.51.100.1? Tell 198.51.100.2
7	26.773062684	fe:fd:00:00:01:02	fe:fd:00:00:02:02	ARP	42	198.51.100.1 is at fe:fd:00:00:01:02
8	278.528015268	fe80::e423:aff:fefc.. ff02::2		ICMPv6	70	Router Solicitation from e6:23:0a:fc:be
9	851.968044943	fe80::e423:aff:fefc.. ff02::2		ICMPv6	70	Router Solicitation from e6:23:0a:fc:be

Frame 4: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0

Ethernet II, Src: fe:fd:00:00:01:02 (fe:fd:00:00:01:02), Dst: fe:fd:00:00:02:02 (fe:fd:00:00:02:02)

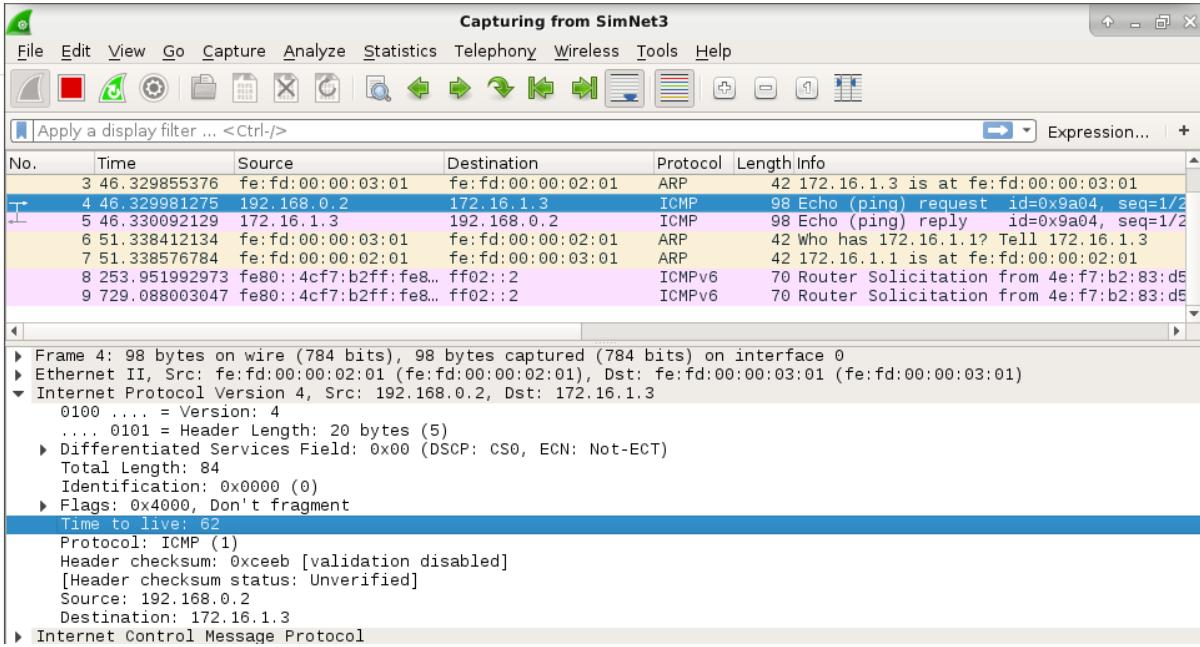
Internet Protocol Version 4, Src: 192.0.2.2, Dst: 198.51.100.2

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 104
- Identification: 0x0000 (0)
- Flags: 0x4000, Don't fragment
- Time to live: 62
- Protocol: IP (4)
- Header checksum: 0x505a [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.0.2.2
- Destination: 198.51.100.2

Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x0000 (0)
- Flags: 0x4000, Don't fragment
- Time to live: 63
- Protocol: ICMP (1)
- Header checksum: 0xcdeb [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.0.2
- Destination: 172.16.1.3

Internet Control Message Protocol



(a) What is the meaning of the -c option? (consult the man page of ping if necessary)

**para enviar pings finitos. -c 2 envias 2 pings.**

(b) Is the ping working? How many packets can you see?

**si, 1 pq hemos hecho ping de 1 paquete.**

3. Assuming that the ping is working, it is necessary to emphasize certain aspects related to tunneling issues:

(a) Verify that the IP packet in SimNet1 and SimNet2 is encapsulated using IPIP. How many IP headers can you see in these packets? Which is the value of the "Protocol" field in the Outer Header?

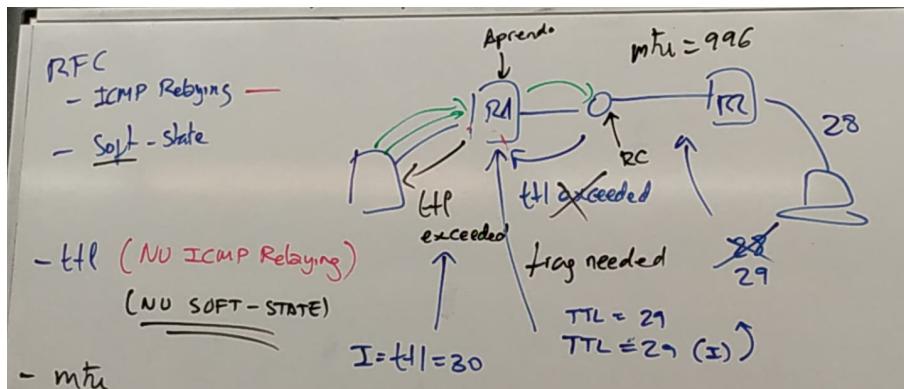
**Dentro del outer header de los paquetes de capturados en SimNet1 y 2 podemos ver un campo Protocol: IPIP. Dentro de estos paquetes hay dos headers IP, el outer y el inner header (exterior e interior). En las inner header el protocolo obviamente es ICMP ya que estamos encapsulando un echo-request/reply.**

**EL valor de protocolo es IPIP(4)**

(b) Determine the difference in size from the original IP packet (in SimNet0) and the encapsulated one (in SimNet1).

**El paquete IP original tiene un tamaño de 84 bytes mientras que el encapsulado es de 104 bytes, 20 bytes más correspondientes a la outer header.**

(c) Identify the value of the “TTL” field in the original IP packet and how this value evolve during the transmission, both in the inner and in the outer headers. Remind that we used the option ttl inherit during the creation of the tunnels.



Siguiendo este esquema(mirar lo azul), en nuestro caso, al inicio tenemos ttl 64, cuando pasa al R1 tenemos ttl= 63. Este decremento es debido a que el router ha de consultar su tabla de enrutamiento, entonces se decrementa 1 ttl, pq solo hace 1 salto. Y como ahí se empieza a hacer la encapsulacion, el protocolo IPIP copia el ttl con ese valor. Al llegar al R2, router destino, como ha de consultar tambien su tabla de enrutamiento de decrementa 1 , ttl=62. Pero solo se decrementa el de outer header, el inner header se queda igual, ttl=63, porque en los tunneles, el inner header no se modifica. y Despues como ha de ir de R2 al destino hace un salto mas, entonces se decrementa 1 ttl de inner head.

Al final, vemos que tenemos 2 saltos, empezamos con 64 y acabamos con 62.

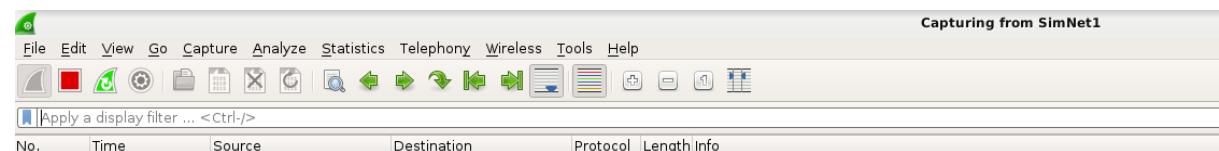
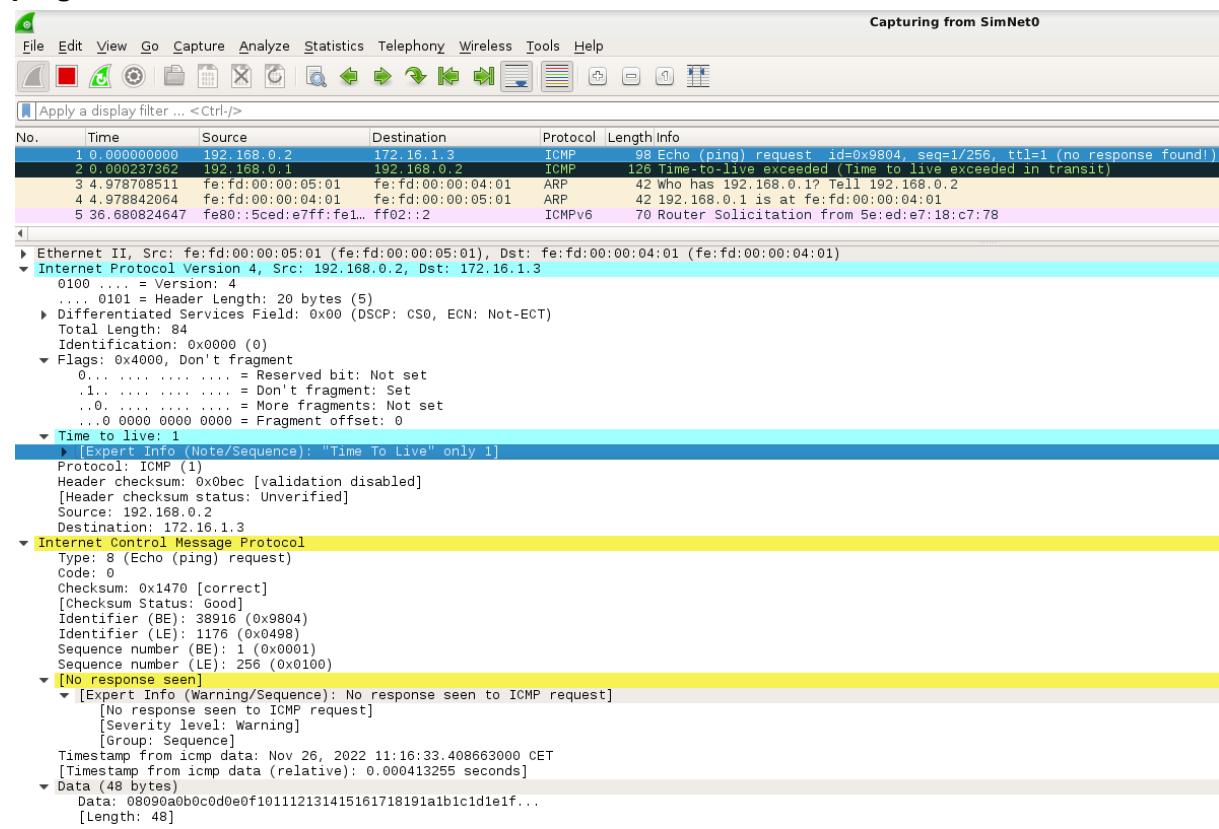
TTL	SimNet0	SimNet1	SimNet2	SimNet3
Outer header		63	62	
Inner header	64	63	63	62

4. To evaluate the behavior of the tunnel when the TTL expires, we will send IP packets from host2 (192.168.0.2) to host3 (172.16.1.3) increasing one by one the TTL. First, clear and start again the capture in the four wiresharks to perfectly monitor step by step the transmission of this packets in all the involved networks (SimNet0, SimNet1, SimNet2 and SimNet3). Next, send again one ICMP echo-request messages using the ping program and TTL=1.

(a) Can you see packets in all the networks? Did the packet reach the destination host? In which host the packet was lost?

**// from host2**

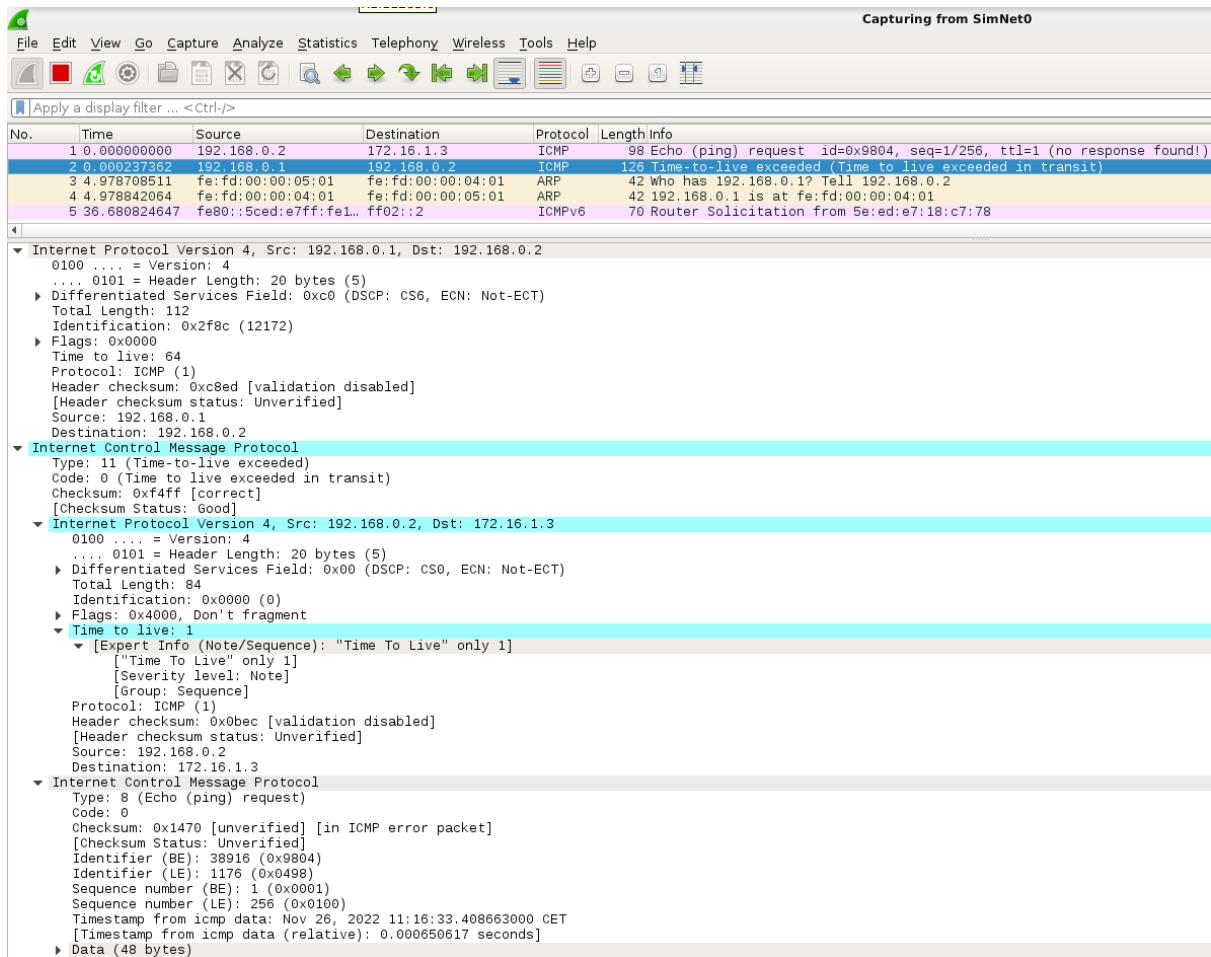
**ping -c1 -t1 172.16.1.3**



**El ping solo llega al R1 y se pierde, Como tiene solo 1 ttl, hace solo 1 salto. Cuando llega al R1 su ttl es 0, entonces no hace mas saltos y se descarta.**

(b) Can you see any ICMP error message? Which one? In which network?

Y el R1 le envia al host2 el error ICMP: TTL exceeded in transit) in SimNet0.



(c) Which are the origin and destination IP addresses of this error message?

ip.src = 192.168.0.1(R1 eth1)

ip.dst = 192.168.0.2 (host2)

Now clear all the wiresharks and send again another ping, but with TTL=2.

(a) Did the packet reach the destination host? In which machine the packet was lost?

//from host2

ping -c1 -t2 172.16.1.3

```
host2:~# ping -c1 -t2 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 56(84) bytes of data.

3
--- 172.16.1.3 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Capturing from SimNet0

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	fe:fd:00:00:05:01	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.0.2
2	0.000246672	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42 192.168.0.1 is at fe:fd:00:00:04:01
3	0.000364415	192.168.0.2	172.16.1.3	ICMP	98 Echo (ping) request id=0x9d04, seq=1/256, ttl=2 (no response found!)

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

- Ethernet II, Src: fe:fd:00:00:05:01 (fe:fd:00:00:05:01), Dst: fe:fd:00:00:04:01 (fe:fd:00:00:04:01)
  - Destination: fe:fd:00:00:04:01 (fe:fd:00:00:04:01)
  - Source: fe:fd:00:00:05:01 (fe:fd:00:00:05:01)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 84
  - Identification: 0x0000 (0)
  - Flags: 0x4000, Don't fragment
  - Time to live: 2
    - [Expert Info (Note/Sequence): "Time To Live" only 2]
      - "Time To Live" only 2
      - [Severity level: Note]
      - [Group: Sequence]
    - Protocol: ICMP (1)
    - Header checksum: 0x0a0c [validation disabled]
    - [Header checksum status: Unverified]
    - Source: 192.168.0.2
    - Destination: 172.16.1.3
  - Internet Control Message Protocol
    - Type: 8 (Echo (ping) request)
    - Code: 0
    - Checksum: 0x6c82 [correct]
    - [Checksum Status: Good]
    - Identifier (BE): 40196 (0x9d04)
    - Identifier (LE): 1181 (0x049d)
    - Sequence number (BE): 1 (0x0001)
    - Sequence number (LE): 256 (0x0100)
    - [No response seen]
      - [Expert Info (Warning/Sequence): No response seen to ICMP request]
        - [No response seen to ICMP request]
        - [Severity level: Warning]
        - [Group: Sequence]
      - Timestamp from icmp data: Nov 26, 2022 11:32:27.337473000 CET
      - [Timestamp from icmp data (relative): 0.020831167 seconds]
    - Data (48 bytes)

Capturing from SimNet1

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	fe:fd:00:00:04:02	Broadcast	ARP	42 Who has 192.0.2.1? Tell 192.0.2.2
2	0.001169082	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42 192.0.2.1 is at fe:fd:00:00:01:01
3	0.0013377445	192.168.0.2	172.16.1.3	ICMP	118 Echo (ping) request id=0x9d04, seq=1/256, ttl=1 (no response found!)
4	0.001472641	192.0.2.1	192.0.2.2	ICMP	146 Time-to-live exceeded (Time to live exceeded in transit)
5	0.001784715	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42 Who has 192.0.2.2? Tell 192.0.2.1
6	0.002013697	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42 192.0.2.2 is at fe:fd:00:00:04:02

Frame 3: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0

- Ethernet II, Src: fe:fd:00:00:04:02 (fe:fd:00:00:04:02), Dst: fe:fd:00:00:01:01 (fe:fd:00:00:01:01)
  - Destination: fe:fd:00:00:01:01 (fe:fd:00:00:01:01)
  - Source: fe:fd:00:00:04:02 (fe:fd:00:00:04:02)
  - Type: Internet Protocol Version 4, Src: 192.0.2.2, Dst: 198.51.100.2
    - 0100 .... = Version: 4
    - .... 0101 = Header Length: 20 bytes (5)
    - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    - Total Length: 104
    - Identification: 0x0000 (0)
    - Flags: 0x4000, Don't fragment
    - Time to live: 1
      - Protocol: IP/ICMP (4)
      - Header checksum: 0x8d5a [validation disabled]
      - [Header checksum status: Unverified]
      - Source: 192.0.2.2
      - Destination: 198.51.100.2
    - Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3
      - 0100 .... = Version: 4
      - .... 0101 = Header Length: 20 bytes (5)
      - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      - Total Length: 84
      - Identification: 0x0000 (0)
      - Flags: 0x4000, Don't fragment
      - Time to live: 1
        - Protocol: ICMP (1)
        - Header checksum: 0x0bec [validation disabled]
        - [Header checksum status: Unverified]
        - Source: 192.168.0.2
        - Destination: 172.16.1.3
      - Internet Control Message Protocol
        - Type: 8 (Echo (ping) request)
        - Code: 0
        - Checksum: 0x6c82 [correct]
        - [Checksum Status: Good]
        - Identifier (BE): 40196 (0x9d04)
        - Identifier (LE): 1181 (0x049d)
        - Sequence number (BE): 1 (0x0001)
        - Sequence number (LE): 256 (0x0100)
        - [No response seen]
          - [Expert Info (Warning/Sequence): No response seen to ICMP request]
            - Timestamp from icmp data: Nov 26, 2022 11:32:27.337473000 CET
            - [Timestamp from icmp data (relative): 0.022413076 seconds]
          - Data (48 bytes)

**El paquete se vuelve a perder, Pero ahora el RC.**

(b) Can you see any ICMP error message? Which one? In which network?

**Si, el mismo que antes, TTL exceeded, en la SimNet0.**

Capturing from SimNet1						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe:fd:00:00:04:02	Broadcast	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2
2	0.001169082	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.1 is at fe:fd:00:00:01:01
3	0.001337445	192.168.0.2	172.16.1.3	ICMP	118	Echo (ping) request id=0x9d04, seq=1/256, ttl=1 (no response found!)
4	0.001472641	192.0.2.1	192.0.2.2	ICMP	146	Time-to-live exceeded (Time to live exceeded in transit)
5	5.001784715	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
6	5.002013697	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:04:02

Internet Control Message Protocol  
Type: 11 (Time-to-live exceeded)  
Code: 0 (Time to live exceeded in transit)  
Checksum: 0xf4ff [correct]  
[Checksum Status: Good]  
Internet Protocol Version 4, Src: 192.0.2.2, Dst: 198.51.100.2  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 104  
Identification: 0x0000 (0)  
Flags: 0x4000, Don't fragment  
Time to live: 1  
► [Expert Info (Note/Sequence): "Time To Live" only 1]  
Protocol: IP/ICMP (4)  
Header checksum: 0x8d5a [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.0.2.2  
Destination: 198.51.100.2  
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 84  
Identification: 0x0000 (0)  
Flags: 0x4000, Don't fragment  
Time to live: 1  
► [Expert Info (Note/Sequence): "Time To Live" only 1]  
Protocol: ICMP (1)  
Header checksum: 0xb0ec [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.168.0.2  
Destination: 172.16.1.3  
Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0x6c82 [unverified] [in ICMP error packet]  
[Checksum Status: Unverified]  
Identifier (BE): 40196 (0x9d04)  
Identifier (LE): 1181 (0x049d)  
Sequence number (BE): 1 (0x0001)  
Sequence number (LE): 256 (0x0100)

(c) Which is the origin and destination IP addresses of this error message?

**ip.src = 192.0.2.1 (RC)**

**ip.dst = 192.0.0.2 (eht2 R1)**

(d) Can you see any ICMP relaying?

**No vemos ICMP relaying porque no el mensaje de error no va al host sino al R1.**

(e) Send again the same ping with TTL=2. Is there any soft state?

**No, ya que no se envia ningun mensaje desde R1 a host2.**

(f) Is this behavior compliant with RFC 2003 (see section 4.4)?

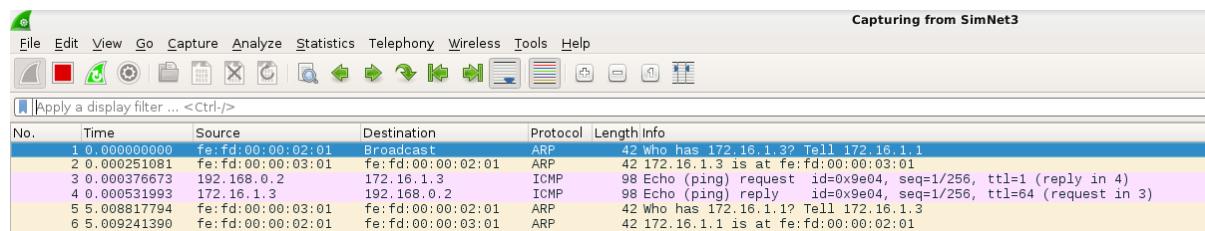
**Si, porque el host2 no ha recibido ningn mensaje.**

(mirar el 4.4 de la documentacion)

Now use TTL=3:

```
//from host2  
ping -c1 -t3 172.16.1.3
```

```
host2:~# ping -c1 -t3 172.16.1.3  
PING 172.16.1.3 (172.16.1.3) 56(84) bytes of data.  
64 bytes from 172.16.1.3: icmp_seq=1 ttl=62 time=34.8 ms  
  
--- 172.16.1.3 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 34.857/34.857/34.857/0.000 ms
```



(a) Did the packet reach the destination host?

**si, se envia correctamente**

(b) Can you see any ICMP reply message?

**Suuu**

## 0.6 Testing the tunnels: nopmtudisc

### 0.6.1 Limiting the MTU

1. Use ifconfig to see which is the value of the MTU in the tunnel interfaces both in R1 and R2.

-recordatorio:

- The maximum length of an IP datagram is 64KBytes
- The value of the MTU depends on the type of transmission link, for example, ethernet links have a MTU of 1500 bytes.
- The "Path MTU" is the smallest MTU of all the hops of the path between source and destination.

```
//from R2 & R1
```

```
ifconfig
```

R2:~# [ ]	tunnel0 Link encap:IPIP Tunnel Hwaddr inet addr:1.2.3.4 P-t-P:1.2.3.4 Mask: UP POINTOPOINT RUNNING NOARP MTU:1480 RX packets:2 errors:0 dropped:0 overruns: TX packets:2 errors:0 dropped:0 overruns: collisions:0 txqueuelen:0 RX bytes:168 (168.0 B) TX bytes:168 (168.0 B)	R1:~# [ ]	tunnel0 Link encap:IPIP Tunnel Hwaddr inet addr:1.2.3.4 P-t-P:1.2.3.4 Mask:255.255.255.255 UP POINTOPOINT RUNNING NOARP MTU:1480 Metric:1 RX packets:1 errors:0 dropped:0 overruns:0 frame:0 TX packets:1 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:84 (84.0 B) TX bytes:84 (84.0 B)
-----------	---	-----------	---

(a) Which is this value?

**La MTU de tunnel es 1480 Bytes.**

(b) Is there any relationship between the MTU assigned to the tunnel, and the MTU assigned to the physical interface?

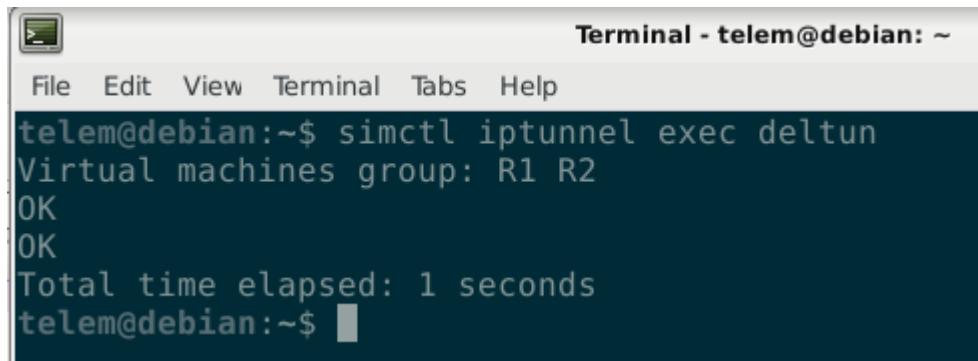
**La MTU de la interfaz física es 1500 Bytes (la estandar). La relación entre estas 2 MTU es de 20 Bytes.**

**Basicamente, es para que el el de tunnel pueda añadir la cabecera de outer header.**

2. Delete the previously configured tunnel in R2. Instead of doing it manually, you can use this script to do so. Go to the console of your HOST machine, and execute:

**//from terminal**

**simctl iptunnel exec deltun**



```
Terminal - telem@debian: ~
File Edit View Terminal Tabs Help
telem@debian:~$ simctl iptunnel exec deltun
Virtual machines group: R1 R2
OK
OK
Total time elapsed: 1 seconds
telem@debian:~$ █
```

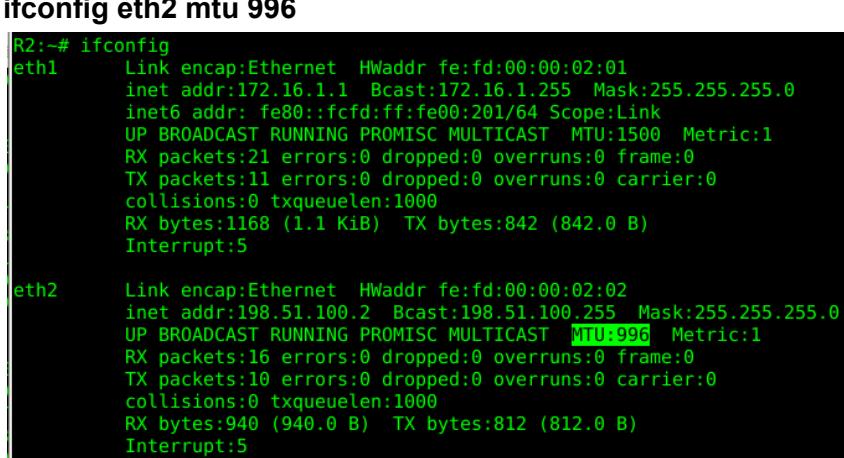
3. Change the MTU of SimNet2 to the value 996 bytes. So, get the consoles of R2 and RC and use the ifconfig command to do so. For instance, in R2 execute:

**//from R2**

**ifconfig eth2 mtu 996**

**//from RC**

**ifconfig eth2 mtu 996**



```
R2:~# ifconfig
eth1      Link encap:Ethernet HWaddr fe:fd:00:00:02:01
          inet addr:172.16.1.1 Bcast:172.16.1.255 Mask:255.255.255.0
          inet6 addr: fe80::fcfd:ff:fe00:201/64 Scope:Link
            UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
            RX packets:21 errors:0 dropped:0 overruns:0 frame:0
            TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1168 (1.1 KiB) TX bytes:842 (842.0 B)
            Interrupt:5

eth2      Link encap:Ethernet HWaddr fe:fd:00:00:02:02
          inet addr:198.51.100.2 Bcast:198.51.100.255 Mask:255.255.255.0
          inet6 addr: fe80::fcfd:ff:fe00:202/64 Scope:Link
            UP BROADCAST RUNNING PROMISC MULTICAST MTU:996 Metric:1
            RX packets:16 errors:0 dropped:0 overruns:0 frame:0
            TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:940 (940.0 B) TX bytes:812 (812.0 B)
            Interrupt:5
```

```

RC:~# ifconfig
eth1      Link encap:Ethernet HWaddr fe:fd:00:00:01:01
          inet addr:192.0.2.1 Bcast:192.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::fcfd:ff:fe00:101/64 Scope:Link
            UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
            RX packets:37 errors:0 dropped:0 overruns:0 frame:0
            TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:3096 (3.0 KiB) TX bytes:1202 (1.1 KiB)
            Interrupt:5

eth2      Link encap:Ethernet HWaddr fe:fd:00:00:01:02
          inet addr:198.51.100.1 Bcast:198.51.100.255 Mask:255.255.255.0
          inet6 addr: fe80::fcfd:ff:fe00:102/64 Scope:Link
            UP BROADCAST RUNNING PROMISC MULTICAST MTU:996 Metric:1
            RX packets:32 errors:0 dropped:0 overruns:0 frame:0
            TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:2852 (2.7 KiB) TX bytes:742 (742.0 B)
            Interrupt:5

```

4. Reestablish again the tunnel using the following script:

**//from terminal**

**simctl iptunnel exec addtun\_nopmtu**

```

telem@debian:~$ simctl iptunnel exec addtun_nopmtu
Virtual machines group: R1 R2
OK
OK
Total time elapsed: 1 seconds

```

(a) Which is now the MTU in both sides of the tunnel?

**//from R1 //from R2**

**ifconfig**

R1:~# [ ]	tunnel0  Link encap:IPIP Tunnel HWaddr UP POINTOPOINT RUNNING NOARP MTU:1480 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
-----------	--

**MTU tunnel R1= 1480**

R2:~# [ ]	tunnel0  Link encap:IPIP Tunnel HWaddr UP POINTOPOINT RUNNING NOARP MTU:976 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
-----------	---

**MTU tunnel R2= 976**

(b) Why this change in the MTU value?

**Para poder meter la cabecera (outer header) cuando se encapsulen los paquetes.**

## 0.6.2 Fragmentation fields and options

1. Put all wireshark's listening traffic in all SimNet interfaces.

2. Send the following ping from host2 to host3:

//from host2

**ping -c1 -s 500 -M want 172.16.1.3**

-s option is used to set the number of bytes in the "data".

-M option is used to manage fragmentation in the origin host.

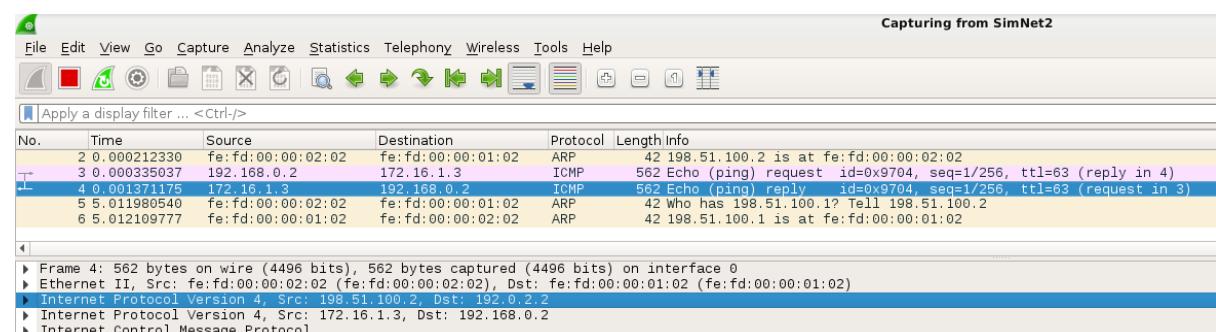
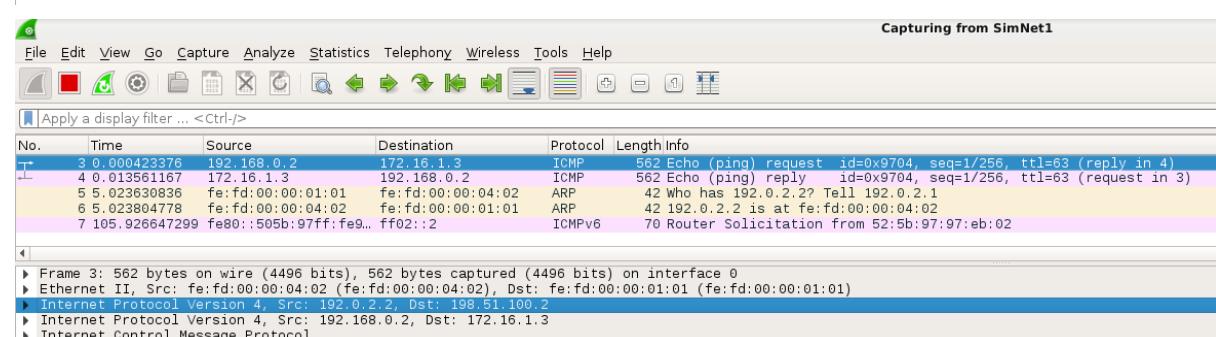
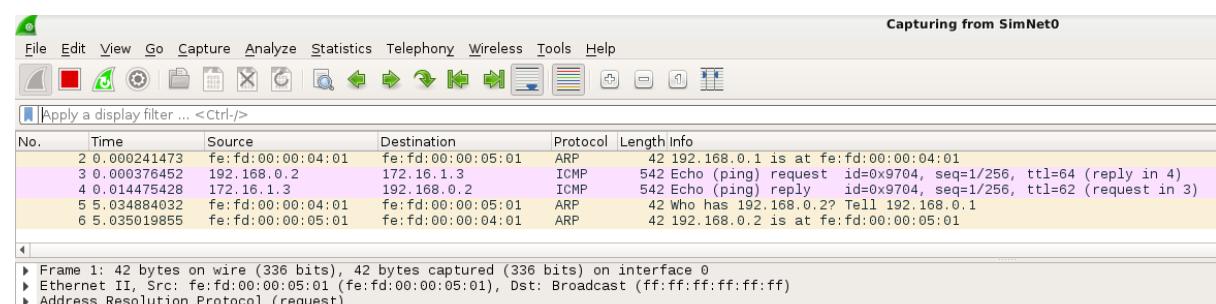
do (prohibit fragmentation, even local one).

want (do PMTU discovery, fragment locally when packet size is large).

dont (do not set DF flag).

```
host2:~# ping -c1 -s 500 -M want 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 500(528) bytes of data.
508 bytes from 172.16.1.3: icmp_seq=1 ttl=62 time=35.1 ms

--- 172.16.1.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 35.138/35.138/35.138/0.000 ms
host2:~#
```



Capturing from SimNet3						
No.	Time	Source	Destination	Protocol	Length Info	
3	0.000344755	192.168.0.2	172.16.1.3	ICMP	542 Echo (ping) request id=0x9704, seq=1/256, ttl=62 (reply in 4)	
4	0.000517240	172.16.1.3	192.168.0.2	ICMP	542 Echo (ping) reply id=0x9704, seq=1/256, ttl=64 (request in 3)	
5	0.000774787	fe:fd:00:00:03:01	fe:fd:00:00:02:01	ARP	42 Who has 172.16.1.1? Tell 172.16.1.3	
6	5.000920100	fe:fd:00:00:02:01	fe:fd:00:00:03:01	ARP	42 172.16.1.1 is at fe:fd:00:00:02:01	
7	105.913886998	fe80::f0ec:e6ff:fe0.. ff02::2		ICMPv6	70 Router Solicitation from f2:ec:e6:0a:02:e8	

Frame 3: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0  
 ▶ Ethernet II, Src: fe:fd:00:00:02:01 (fe:fd:00:00:02:01), Dst: fe:fd:00:00:03:01 (fe:fd:00:00:03:01)  
 ▶ Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3  
 ▶ Internet Control Message Protocol

(a) How many ICMP packets can you see? What kind of packets?

En cada SimNet tenemos un echo-request y un echo-reply. En SimNet0 y SimNet3 tenemos paquetes IP y en SimNet1 y SimNet2 (tunnel) tenemos paquetes IP encapsulados en paquetes IPIP.

(b) Which is the size of these packets? Describe the headers of these packets.

En SimNet0 y SimNet3 tenemos paquete=542 Bytes. En SimNet0 y SimNet3 tenemos paquete=562 Bytes (+20 de IPIP).

Capturing from SimNet0						
No.	Time	Source	Destination	Protocol	Length Info	
4	0.014475428	172.16.1.3	192.168.0.2	ICMP	542 Echo (ping) reply id=0x9704, seq=1/256, ttl=62 (request in 3)	
5	5.034884032	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42 Who has 192.168.0.2? Tell 192.168.0.1	
6	5.035019855	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42 192.168.0.2 is at fe:fd:00:00:05:01	
7	171.463403864	fe80::8082:c8ff:fe9.. ff02::2		ICMPv6	70 Router Solicitation from 82:82:c8:94:dc:08	
8	744.903415742	fe80::8082:c8ff:fe9.. ff02::2		ICMPv6	70 Router Solicitation from 82:82:c8:94:dc:08	

Frame 4: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0  
 ▶ Ethernet II, Src: fe:fd:00:00:04:01 (fe:fd:00:00:04:01), Dst: fe:fd:00:00:05:01 (fe:fd:00:00:05:01)  
 ▶ Destination: fe:fd:00:00:05:01 (fe:fd:00:00:05:01)  
 ▶ Source: fe:fd:00:00:04:01 (fe:fd:00:00:04:01)  
 ▶ Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 172.16.1.3, Dst: 192.168.0.2  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSOF: CS0, EON: Not-ECT)  
 Total Length: 528  
 Identification: 0x53bb (21435)  
 ▶ Flags: 0x0000  
 Time to live: 62  
 Protocol: ICMP (1)  
 Header checksum: 0xb974 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 172.16.1.3  
 Destination: 192.168.0.2  
 ▶ Internet Control Message Protocol  
 Type: 0 (Echo (ping) reply)  
 Code: 0  
 Checksum: 0xed4 [correct]  
 [Checksum Status: Good]  
 Identifier (BE): 38660 (0x9704)  
 Identifier (LE): 1175 (0x0497)  
 Sequence number (BE): 1 (0x0001)  
 Sequence number (LE): 256 (0x0100)  
 [Request frame: 3]  
 [Response time: 14.099 ms]  
 Timestamp from icmp data: Nov 26, 2022 13:08:10.733898000 CET  
 [Timestamp from icmp data (relative): 0.035098612 seconds]  
 ▶ Data (492 bytes)  
 Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...  
 [Length: 492]

TAMAÑO CABECERAS (8 icmp+20 ip +20 IPIP), pero hay mas. 14 ethernet

(c) Have these packets been fragmented? Why?

Los paquetes no han sido fragmentados porque no se supera la MTU mínima que hay entre host2 y host3 (que son 976 bytes teniendo en cuenta el túnel).

(d) Which is the value of the “don’t fragment” (DF) flag in the ICMP packets in SimNet0?

Echo repli→ ip.flags.df == 0

Echo request→ ip.flags.df == 1

(e) And in SimNet1, which is the value of DF in the Outer and Inner headers?

Echo reply → ip.flags.df == 0

Echo request → ip.flags.df == 1

**En los 2 casos, inner header y outer header. Outer header hereda la info de inner como pasaba con los ttl's.**

3. Now execute

//from host2

ping -c1 -s 500 -M dont 172.16.1.3

```
host2:~# ping -c1 -s 500 -M dont 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 500(528) bytes of data.
508 bytes from 172.16.1.3: icmp_seq=1 ttl=62 time=38.9 ms

--- 172.16.1.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 38.953/38.953/38.953/0.000 ms
```

(a) What is the difference compared to the previous test?

**Ahora todos los paquetes, tanto echo request como echo reply tienen DF= 0.** (don't permite fragmentacion).

4. Now execute:

//from host2

ping -c1 -s 500 -M do 172.16.1.3

(a) Can you see any difference in wireshark compared to the first case? Is there any difference at all?

**No hay diferencia con -M want, eso es porque no hemos necesitado fragmentar en ninguno de los casos.**

**La MTU mas pequena posible es la de 996 que viene condicionada por la R2, pero en el tunnel es de 976 visto anteriormente, entonces el tamaño maximo de datos es 976-20-8= 948 Bytes.(restando cabecera ip y icmp a la mtu del tunnel)**

Aqui no restamos cabecera ethernet, porque va aparte de la MTU.

Si enviamos mas de 948 Bytes de datos, el paquete se pierde.

```
host2:~# ping -c1 -s 1000 -M do 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 1000(1028) bytes of data.

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

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	fe:fd:00:00:04:02	Broadcast	ARP	42 Who has 192.0.2.1? Tell 192.0.2.2
2	0.000199826	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42 192.0.2.1 is at fe:fd:00:00:01:01
3	0.000365169	192.168.0.2	172.16.1.3	ICMP	1062 Echo (ping) request id=0x9f04, seq=1/256, ttl=63 (no response found!)
4	0.000588799	192.0.2.1	192.0.2.2	ICMP	590 Destination unreachable (Fragmentation needed)
5	0.010947231	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42 Who has 192.0.2.2? Tell 192.0.2.1
6	0.011247655	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42 192.0.2.2 is at fe:fd:00:00:04:02

**En este caso el router RC envia a R1 q necesita fragmentar.**

## The -M want option

-M want option is the default option used by ping, we only deactivate DF when needed. messages ICMP Datagram Too Big (Type 3, Code 4, also known as Fragmentation Needed), used in the PMTU Discovery mechanism, are able to modify the status of the dynamic routing table (kernel routing cache).

So, you are going to increment the size of packets to cause fragmentation:

1. Delete the kernel routing cache executing the label flushcache.

//from terminal

**sudo ip route flush cache**

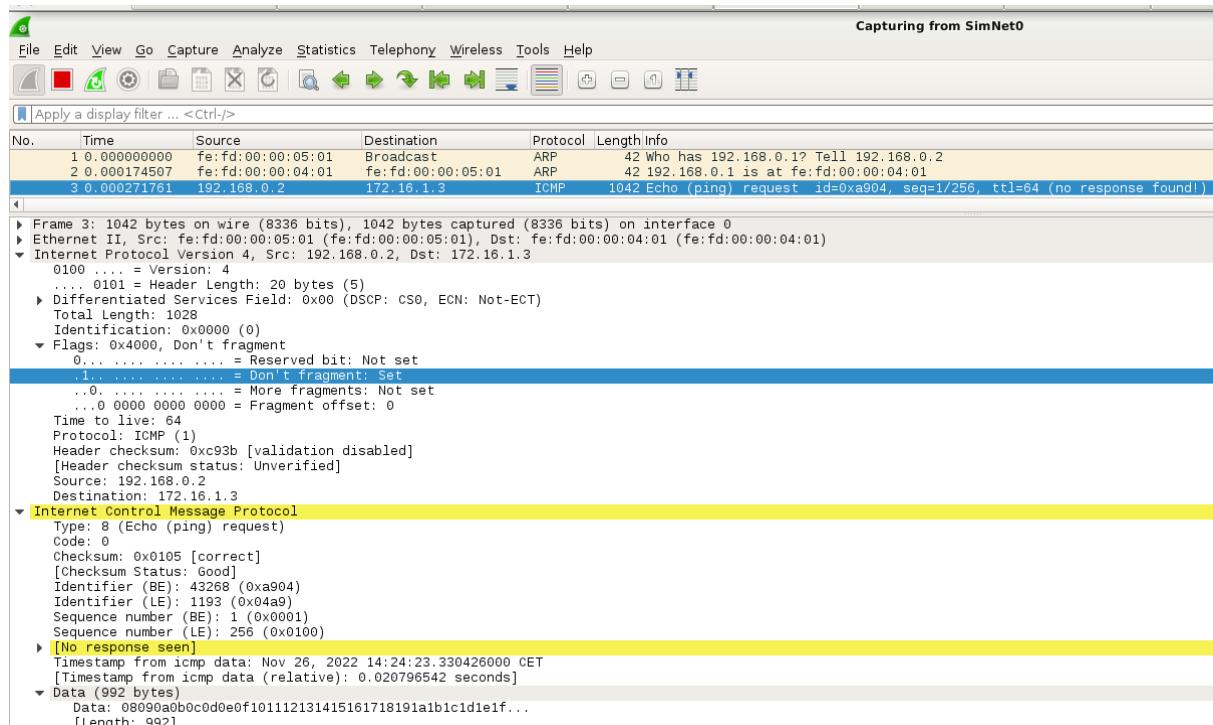
**simctl iptunnel exec flushcache #para el tunnel**

2. Put all wiresharks listening traffic in all SimNet interfaces.

3. Execute the following command in host2:

//from host2

**ping -c1 -s 1000 -M want 172.16.1.3**



Capturing from SimNet1						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe:fd:00:00:04:02	Broadcast	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2
2	0.000139007	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.1 is at fe:fd:00:00:01:01
3	0.000272033	192.168.0.2	172.16.1.3	ICMP	1062	Echo (ping) request id=0xa904, seq=1/256, ttl=63 (no response found!)
4	0.000404572	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
5	0.005302535	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
6	0.005494496	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:04:02

Frame 3: 1062 bytes on wire (8496 bits), 1062 bytes captured (8496 bits) on interface 0  
 ▶ Ethernet II, Src: fe:fd:00:00:04:02 (fe:fd:00:00:04:02), Dst: fe:fd:00:00:01:01 (fe:fd:00:00:01:01)  
 ▶ Internet Protocol Version 4, Src: 192.0.2.2, Dst: 198.51.100.2  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 1048  
 Identification: 0x0000 (0)  
 ▶ Flags: 0x4000, Don't fragment  
 0... .... .... .... = Reserved bit: Not set  
 .1. .... .... .... = Don't fragment: Set  
 ..0. .... .... .... = More fragments: Not set  
 ...0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 63  
 Protocol: IP/IPv4 (4)  
 Header checksum: 0x4baa [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.0.2.2  
 Destination: 198.51.100.2  
 ▶ Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 1028  
 Identification: 0x0000 (0)  
 ▶ Flags: 0x4000, Don't fragment  
 0... .... .... .... = Reserved bit: Not set  
 .1. .... .... .... = Don't fragment: Set  
 ..0. .... .... .... = More fragments: Not set  
 ...0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 63  
 Protocol: ICMP (1)  
 Header checksum: 0xca3b [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.168.0.2  
 Destination: 172.16.1.3  
 ▶ Internet Control Message Protocol  
 Type: 8 (Echo (ping) request)

Capturing from SimNet1						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe:fd:00:00:04:02	Broadcast	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2
2	0.000139007	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.1 is at fe:fd:00:00:01:01
3	0.000272033	192.168.0.2	172.16.1.3	ICMP	1062	Echo (ping) request id=0xa904, seq=1/256, ttl=63 (no response found!)
4	0.000404572	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
5	0.005302535	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
6	0.005494496	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:04:02

Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0  
 ▶ Ethernet II, Src: fe:fd:00:00:01:01 (fe:fd:00:00:01:01), Dst: fe:fd:00:00:04:02 (fe:fd:00:00:04:02)  
 ▶ Internet Protocol Version 4, Src: 192.0.2.1, Dst: 192.0.2.2  
 ▶ Internet Control Message Protocol  
 Type: 3 (Destination unreachable)  
 Code: 4 (Fragmentation needed)  
 Checksum: 0xe5fd [correct]  
 [Checksum Status: Good]  
 Unused: 0000  
 MTU of next hop: 996  
 ▶ Internet Protocol Version 4, Src: 192.0.2.2, Dst: 198.51.100.2  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 1048  
 Identification: 0x0000 (0)  
 ▶ Flags: 0x4000, Don't fragment  
 0... .... .... .... = Reserved bit: Not set  
 .1. .... .... .... = Don't fragment: Set  
 ..0. .... .... .... = More fragments: Not set  
 ...0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 62  
 Protocol: IP/IPv4 (4)  
 Header checksum: 0x4caa [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.0.2.2  
 Destination: 198.51.100.2  
 ▶ Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 1028  
 Identification: 0x0000 (0)  
 ▶ Flags: 0x4000, Don't fragment  
 0... .... .... .... = Reserved bit: Not set  
 .1. .... .... .... = Don't fragment: Set  
 ..0. .... .... .... = More fragments: Not set  
 ...0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 63  
 Protocol: ICMP (1)  
 Header checksum: 0xca3b [validation disabled]  
 [Header checksum status: Unverified]

(a) Is the ping working?

No, el paquete se pierde en R1, porque necesita fragmentar. R1 envia el error (Fragmentacion needed) al R1 porque R1 tiene DF=1. Pero R1 no lo envia al Host2 (no hay ICMP relying),

(b) How many ICMP packets can you see in SimNet0? What kind of packets? Is set the DF flag in the IP header of the ICMP echo-request?

Solo tenemos 1 echo-request. EL DF esta a 1, que por defecto arranca asi.

(c) And in SimNet1, what packets can you see? Is the DF flag set in the IP headers (inner and outer)?

Aqui tenemos el echo-request y tambien el ICMP error.

As you can see, there is an error produced by the MTU by means of a message ICMP fragmentation-needed. This error appears due to the DF flag is Set in the Outer IP header of the ICMP echo-request message.

(d) What device is the origin of the ICMP fragmentation-needed message? And the destination? Which is the maximum MTU notified in this message?

```
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 4 (Fragmentation needed)
  Checksum: 0xe5fd [correct]
  [Checksum Status: Good]
  Unused: 0000
  MTU of next hop: 996
```

RC es el dispositivo que envía el fragmentation-needed a R1, en el mensaje ICMP hay un campo "MTU of next hop: 996" que corresponde con la MTU de SimNet2.

(e) In your opinion, what entity should be the proper destination of this message?

host2

(f) According to RFC2003 (see Section 4.1), is R1 acting as relay of the message and what can you see? Describe sizes and headers.

```
Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 4 (Fragmentation needed)
```

entonces miro la documentacion la parte 4.1 y el codigo 4.

Datagram too big. (segun el documento).

the encapsulator is not performing ICMP Relaying. Instead, the encapsulator uses soft state to inform the origin host about the error.

(g) In SimNet3, how many ICMP echo-reply messages can you see? Describe sizes and headers.

<https://www.youtube.com/shorts/s8j6zW0SAyo>

1. Delete the kernel routing cache executing the label flushcache.

//from terminal

**simctl iptunnel exec flushcache**

2. Put all wiresharks listening traffic in all SimNet interfaces.

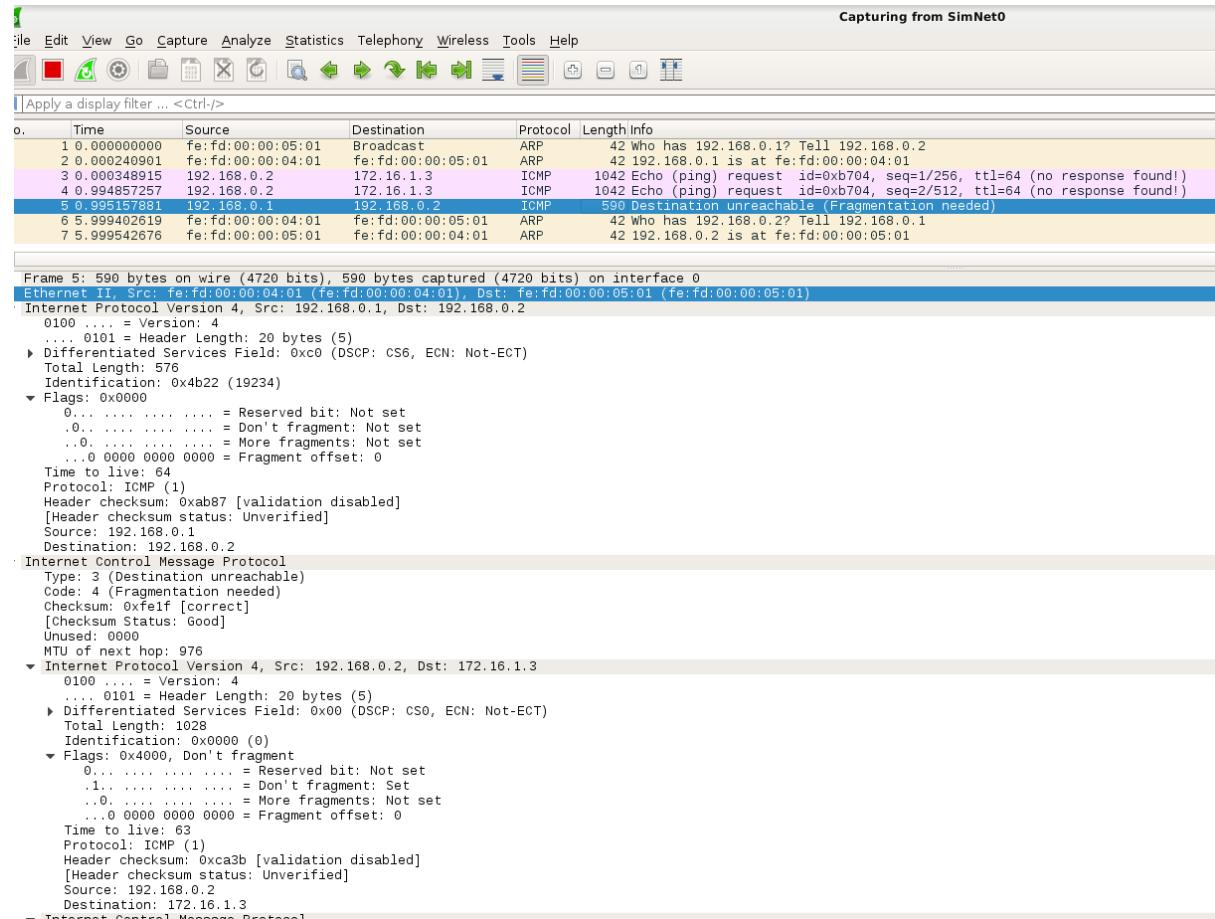
3. Execute the following command in host2:

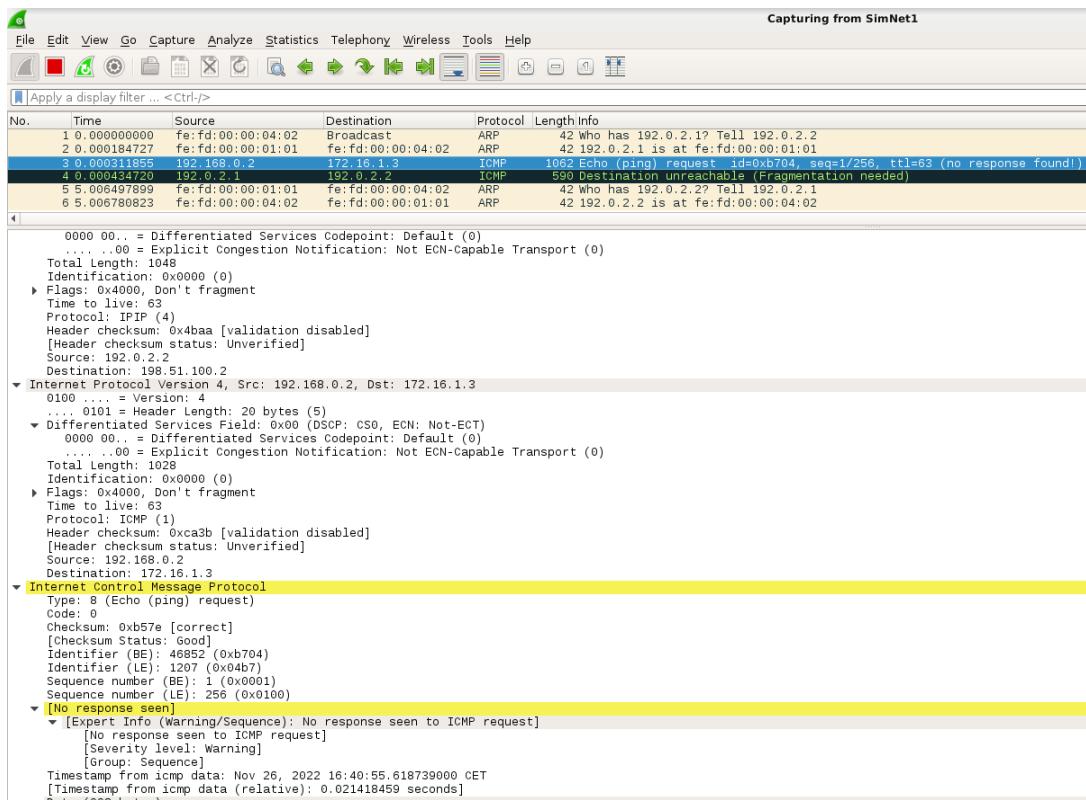
//from host2

**ping -c2 -s 1000 -M want -i1 172.16.1.3**

```
host2:~# ping -c2 -s 1000 -M want -i1 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 1000(1028) bytes of data.
From 192.168.0.1 icmp_seq=2 Frag needed and DF set (mtu = 976)

--- 172.16.1.3 ping statistics ---
2 packets transmitted, 0 received, +1 errors, 100% packet loss, time 1015ms
```





(a) Is the ping working? How many ICMP messages can you see in SimNet0? Is the DF flag set in the IP header of these messages?

**No, el ping no funciona. En SimNet0 tenemos 3 mensajes ICMP, 2 del echo request y 1 de error.**

**El DF de los echo request es 1, en cambio el DF de error es 1. Es logico, porque el error es debido a eso, RC necesita fragmentar el paquete porque supera su MTU, pero le llega como DF=1 entonces envia un error diciendo que DF tiene que ser 0 porque necesita fragmentar.**

(b) In SimNet1, how many ICMP echo-requests can you see? What about the DF flag?

**En SimNet1, tenemos 2 mensajes ICMP, 1 de echo-request y 1 de error.**

**Sucede lo mismo, RC necesita fragmentar pero le llegan con DF=1 (inner & outer).**

**Pero aqui solo tenemos 1 ping, porque el otro ha sido descartado en el R1.**

(c) Can you see an ICMP fragmentation-needed message in SimNet0? Which is the origin and destination of this message? Which is the maximum MTU notified in this message?

**ip.src == 192.0.2.1, ip.dst == 192.0.2.2. icmp.mtu == 996**

(d) Do you think that R1 maintains a soft state of the MTU of the tunnel?

```
host2:~# ping -c2 -s 1000 -M want -i1 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 1000(1028) bytes of data.
From 192.168.0.1 icmp seq=2 Frag needed and DF set (mtu = 976)

--- 172.16.1.3 ping statistics ---
2 packets transmitted, 0 received, +1 errors, 100% packet loss, time 1015ms
```

**Yes. because host get message of error.**

**soft state= hay memoria, porque R1 sabe que en RC se tendra que fragmentar, entonces R1 informa al host de eso.**

This soft state can be seen by executing the following command in R1:  
**ip route show cache ----- esto no me enseña nada.**

Now, we will send three ICMP echo-request messages:

1. Delete the kernel routing cache executing the label flushcache.

**//from terminal**

**simctl iptunnel exec flushcache**

2. Put all wiresharks listening traffic in all SimNet interfaces.

3. Execute the following command in host2:

**//from host2**

**ping -c3 -s 1000 -M want -i1 172.16.1.3 #i= intervalo (sec)**

```
host2:~# ping -c3 -s 1000 -M want -i1 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 1000(1028) bytes of data.
From 192.168.0.1 icmp_seq=2 Frag needed and DF set (mtu = 976)
1008 bytes from 172.16.1.3: icmp_seq=3 ttl=62 time=23.6 ms

--- 172.16.1.3 ping statistics ---
3 packets transmitted, 1 received, +1 errors, 66% packet loss, time 2018ms
rtt min/avg/max/mdev = 23.600/23.600/23.600/0.000 ms
```

Capturing from SimNet0						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:05:01	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
2	0.000321020	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	192.168.0.1 is at fe:fd:00:00:04:01
3	0.000426417	192.168.0.2	172.16.1.3	ICMP	1042	Echo (ping) request id=0xc604, seq=1/256, ttl=64 (no response found!)
4	0.981242976	192.168.0.2	172.16.1.3	ICMP	1042	Echo (ping) request id=0xc604, seq=2/512, ttl=64 (no response found!)
5	0.9981530433	192.168.0.1	192.168.0.2	ICMP	590	Destination unreachable (Fragmentation needed)
6	1.997630045	192.168.0.2	172.16.1.3	ICMP	986	Echo (ping) request id=0xc604, seq=3/768, ttl=64 (reply in 8)
7	1.998050812	192.168.0.2	172.16.1.3	IPv4	90	Fragmented IP protocol (proto=ICMP 1, offf=952, ID=938d)
8	2.020957037	172.16.1.3	192.168.0.2	ICMP	1042	Echo (ping) reply id=0xc604, seq=3/768, ttl=62 (request in 6)
9	5.991269525	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	Who has 192.168.0.2? Tell 192.168.0.1
10	5.991385675	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42	192.168.0.2 is at fe:fd:00:00:05:01
11	385.637187348	fe80::8082:c8ff:fe9... ff02::2		ICMPv6	70	Router Solicitation from 82:82:c8:94:dc:08

Capturing from SimNet1						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:04:02	Broadcast	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2
2	0.000176843	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.1 is at fe:fd:00:00:01:01
3	0.000385460	192.168.0.2	172.16.1.3	ICMP	1062	Echo (ping) request id=0xc604, seq=1/256, ttl=63 (no response found!)
4	0.000502855	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
5	1.997792258	192.168.0.2	172.16.1.3	ICMP	1010	Echo (ping) request id=0xc604, seq=3/768, ttl=63 (reply in 7)
6	1.998073193	192.0.2.2	198.51.100.2	IPv4	86	Fragmented IP protocol (proto=IP 4, offf=976, ID=6c68)
7	2.019799360	172.16.1.3	192.168.0.2	ICMP	1006	Echo (ping) reply id=0xc604, seq=3/768, ttl=63 (request in 5)
8	2.020114058	172.16.1.3	192.168.0.2	IPv4	110	Fragmented IP protocol (proto=ICMP 1, offf=952, ID=ffd1)
9	5.014545609	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
10	5.014804743	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:04:02

Capturing from SimNet2						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:01:02	Broadcast	ARP	42	Who has 198.51.100.2? Tell 198.51.100.1
2	0.000274195	fe:fd:00:00:02:02	fe:fd:00:00:01:02	ARP	42	198.51.100.2 is at fe:fd:00:00:02:02
3	0.000374249	192.168.0.2	172.16.1.3	ICMP	1010	Echo (ping) request id=0xc604, seq=3/768, ttl=63 (reply in 5)
4	0.000452774	192.0.2.2	198.51.100.2	IPv4	86	Fragmented IP protocol (proto=IP 4, offf=976, ID=6c68)
5	0.001366970	172.16.1.3	192.168.0.2	ICMP	1006	Echo (ping) reply id=0xc604, seq=3/768, ttl=63 (request in 3)
6	0.001826020	172.16.1.3	192.168.0.2	IPv4	110	Fragmented IP protocol (proto=ICMP 1, offf=952, ID=ffd1)
7	5.017297488	fe:fd:00:00:02:02	fe:fd:00:00:01:02	ARP	42	Who has 198.51.100.1? Tell 198.51.100.2
8	5.017421177	fe:fd:00:00:01:02	fe:fd:00:00:02:02	ARP	42	198.51.100.1 is at fe:fd:00:00:01:02

Capturing from SimNet3						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe:fd:00:00:02:01	Broadcast	ARP	42	Who has 172.16.1.3? Tell 172.16.1.1
2	0.000219715	fe:fd:00:00:03:01	fe:fd:00:00:02:01	ARP	42	172.16.1.3 is at fe:fd:00:00:03:01
3	0.000316269	192.168.0.2	172.16.1.3	ICMP	1042	Echo (ping) request id=0xc604, seq=3/768, ttl=62 (reply in 4)
4	0.000445548	172.16.1.3	192.168.0.2	ICMP	1042	Echo (ping) reply id=0xc604, seq=3/768, ttl=64 (request in 3)
5	5.006068160	fe:fd:00:00:03:01	fe:fd:00:00:02:01	ARP	42	Who has 172.16.1.1? Tell 172.16.1.3
6	5.006199175	fe:fd:00:00:02:01	fe:fd:00:00:03:01	ARP	42	172.16.1.1 is at fe:fd:00:00:02:01

Now let us analyze this test in detail:

(a) Is the ping working? How do you know that?

**Si que funciona, porque el host2 recibe un echo-reply. El ping exitoso es el 3ero ya que se ha enviado fragmentado. los primeros 2 pings son descartados en RC, pq su MTU es 996 y le llegan paquetes de 1000 con DF=1.**

(b) In SimNet0, have a look at the DF flag in all the ICMP echo-request messages. What can you deduce? Is there any difference in the third ICMP Echo request message?

**En SimNet0 los 2 pings tienen DF=1 (set) y el 3ero no, por tanto se fragmenta. Esta fragmentacion la hace el host2 que es el emisor.**

(c) In SimNet0, who is performing the fragmentation of the third ICMP echo-request? Which are the sizes of the packets that compose this third ICMP echo-request? Take notes of the existing headers.

**El host2 hace la fragmentacion, el tamaño de paquete es de 986, (936 datos + 14 eth+8 icmp+ 20 ip). falta 8 bytes.**

**los 8 bytes estos son los timestamps, que wireshark lo interpreta como cabecera.**

Capturing from SimNet0						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe:fd:00:00:05:01	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
2	0.000321020	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	192.168.0.1 is at fe:fd:00:00:04:01
3	0.000426417	192.168.0.2	172.16.1.3	ICMP	1042	Echo (ping) request id=0xc604, seq=1/256, ttl=64 (no response found!)
4	0.981242976	192.168.0.2	172.16.1.3	ICMP	1042	Echo (ping) request id=0xc604, seq=2/512, ttl=64 (no response found!)
5	0.981530433	192.168.0.2	192.168.0.2	ICMP	590	Destination unreachable (Fragmentation needed)
6	1.997630045	192.168.0.2	172.16.1.3	ICMP	986	Echo (ping) request id=0xc604, seq=3/768, ttl=64 (reply in 8)
7	1.998050812	192.168.0.2	172.16.1.3	IPV4	90	Fragmented IP protocol (proto:ICMP 1, off=952, Id=938d)
8	2.020957037	172.16.1.3	192.168.0.2	ICMP	1042	Echo (ping) reply id=0xc604, seq=3/768, ttl=62 (request in 6)
9	5.991269575	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	Who has 192.168.0.2? Tell 192.168.0.1
10	5.991385675	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42	192.168.0.2 is at fe:fd:00:00:05:01
11	385.637187348	fe80::8082:c8ff:fe0...ff02::2		ICMPv6	70	Router Solicitation from 82:82:c8:94:dc:08

Frame 6: 986 bytes on wire (7888 bits), 986 bytes captured (7888 bits) on interface 0  
**Ethernet II, Src: fe:fd:00:00:05:01 (fe:fd:00:00:05:01), Dst: fe:fd:00:00:04:01 (fe:fd:00:00:04:01)**  
 Destination: fe:fd:00:00:04:01 (fe:fd:00:00:04:01)  
 Source: fe:fd:00:00:05:01 (fe:fd:00:00:05:01)  
 Type: IPv4 (0x0800)  
**Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3**  
 0100 ... = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 972  
 Identification: 0x938d (37773)  
 Flags: 0x2000, More fragments  
 0... .... .... .... = Reserved bit: Not set  
 .0.. .... .... .... = Don't fragment: Not set  
 ..1.... .... .... = More fragments: Set  
 ...0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 64  
 Protocol: ICMP (1)  
 Header checksum: 0x55e6 [validation disabled]  
 Header checksum status: Unverified  
 Source: 192.168.0.2  
 Destination: 172.16.1.3  
**Internet Control Message Protocol**  
 Type: 8 (Echo (ping) request)  
 Code: 0  
 Checksum: 0x935b [unverified] [fragmented datagram]  
 [Checksum Status: Unverified]  
 Identifier (BE): 50692 (0xc604)  
 Identifier (LE): 1222 (0x04c6)  
 Sequence number (BE): 3 (0x0003)  
 Sequence number (LE): 768 (0x300)  
 [Response Frame: 8]  
 Timestamp from icmp data: Nov 26, 2022 17:22:08.690268000 CET  
 [Timestamp from icmp data (relative): 0.000169685 seconds]  
 Data (936 bytes)  
 Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...  
 [Length: 936]

en el examen si nos dicen q hagamos paquetes de x tamaño, allí incluimos cabecera ethernet.

Capturing from SimNet0

No. Time Source Destination Protocol Length Info

1	0.000000000	fe:fd:00:00:05:01	Broadcast	ARP	42 Who has 192.168.0.1? Tell 192.168.0.2
2	0.000321020	fe:fd:00:00:04:01	fe:fd:00:00:04:01	ARP	42 192.168.0.1 is at fe:fd:00:00:04:01
3	0.000426417	192.168.0.2	172.16.1.3	ICMP	1042 Echo (ping) request id=0xc604, seq=1/256, ttl=64 (no response found)
4	0.981242976	192.168.0.2	172.16.1.3	ICMP	1042 Echo (ping) request id=0xc604, seq=2/512, ttl=64 (no response found)
5	0.981530433	192.168.0.1	192.168.0.2	ICMP	590 Destination unreachable (Fragmentation needed)
6	1.997630045	192.168.0.2	172.16.1.3	ICMP	986 Echo (ping) request id=0xc604, seq=3/768, ttl=64 (reply in 8)
7	1.998050812	192.168.0.2	172.16.1.3	IPv4	90 Fragmented IP protocol (proto=ICMP 1, off=952, ID=93d8)
8	2.020957037	172.16.1.3	192.168.0.2	ICMP	1042 Echo (ping) reply id=0xc604, seq=3/768, ttl=62 (request in 6)
9	5.991269525	fe:fd:00:00:04:01	fe:fd:00:00:04:01	ARP	42 Who has 192.168.0.2? Tell 192.168.0.1
10	5.991385675	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42 192.168.0.2 is at fe:fd:00:00:05:01
11	385.637187348	fe80::8082:c0ff:fe00:ff02::2		ICMPv6	70 Router Solicitation from 82:82:c8:94:dc:08

Frame 7: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0

Ethernet II, Src: fe:fd:00:00:05:01 (fe:fd:00:00:05:01), Dst: fe:fd:00:00:04:01 (fe:fd:00:00:04:01)

Destination: fe:fd:00:00:04:01 (fe:fd:00:00:04:01)

Address: fe:fd:00:00:04:01 (fe:fd:00:00:04:01) = LG bit: Locally administered address (this is NOT the factory default)

.....0..... = IG bit: Individual address (unicast)

Source: fe:fd:00:00:05:01 (fe:fd:00:00:05:01)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3

0100 .... = Version: 4

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

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

Total Length: 76

Identification: 0x93d8 (37773)

Flags: 0x0077

0... .... .... = Reserved bit: Not set

.0.. .... .... = Don't fragment: Not set

..0.... .... = More fragments: Not set

...0 0000 0111 0111 = Fragment offset: 119

Time to live: 64

Protocol: ICMP (1)

Header checksum: 0x78ef [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.2

Destination: 172.16.1.3

Data (56 bytes)

Data: b0b1b2b3b4b5b6b7b8b9babbbcbdbefc0c1c2c3c4c5c6c7...

[Length: 56]

Este es el paquete fragmentado, 90B=56 data+20ip+14 eth.

Cada router recibe los paquetes fragmentados, los junta y lo fragmenta con su criterio /o no y lo envia.

(d) In SimNet1, how many fragmented packets can you see that correspond to this third ICMP echo-request? What about the DF flag in the Inner and Outer IP headers?

Capturing from SimNet1

No. Time Source Destination Protocol Length Info

1	0.000000000	fe:fd:00:00:04:02	Broadcast	ARP	42 Who has 192.0.2.1? Tell 192.0.2.2
2	0.000176843	fe:fd:00:00:01:01	fe:fd:00:00:01:01	ARP	42 192.0.2.1 is at fe:fd:00:00:01:01
3	0.000365460	192.168.0.2	172.16.1.3	ICMP	1062 Echo (ping) request id=0xc604, seq=1/256, ttl=63 (no response found)
4	0.000502855	192.0.2.1	192.0.2.2	ICMP	590 Destination unreachable (Fragmentation needed)
5	1.9977922258	192.168.0.2	172.16.1.3	ICMP	1010 Echo (ping) request id=0xc604, seq=3/768, ttl=63 (reply in 7)
6	1.998073193	192.0.2.2	192.51.100.2	IPv4	86 Fragmented IP protocol (proto=IP 4, off=976, ID=6c68)
7	2.019799360	172.16.1.3	192.168.0.2	ICMP	1006 Echo (ping) reply id=0xc604, seq=3/768, ttl=63 (request in 5)
8	2.020114058	172.16.1.3	192.168.0.2	IPv4	110 Fragmented IP protocol (proto=ICMP 1, off=952, ID=ffff)
9	5.014545609	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42 Who has 192.0.2.2? Tell 192.0.2.1
10	5.014804743	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42 192.0.2.2 is at fe:fd:00:00:04:02

Frame 6: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0

Ethernet II, Src: fe:fd:00:00:04:02 (fe:fd:00:00:04:02), Dst: fe:fd:00:00:01:01 (fe:fd:00:00:01:01)

Internet Protocol Version 4, Src: 192.0.2.2, Dst: 198.51.100.2

0100 .... = Version: 4

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

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

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 72

Identification: 0x6c68 (27752)

Flags: 0x007a

0... .... .... = Reserved bit: Not set

.0.. .... .... = Don't fragment: Not set

..0.... .... = More fragments: Not set

...0 0000 0111 1010 = Fragment offset: 122

Time to live: 63

Protocol: IP/PIP (4)

Header checksum: 0x2298 [validation disabled]

[Header checksum status: Unverified]

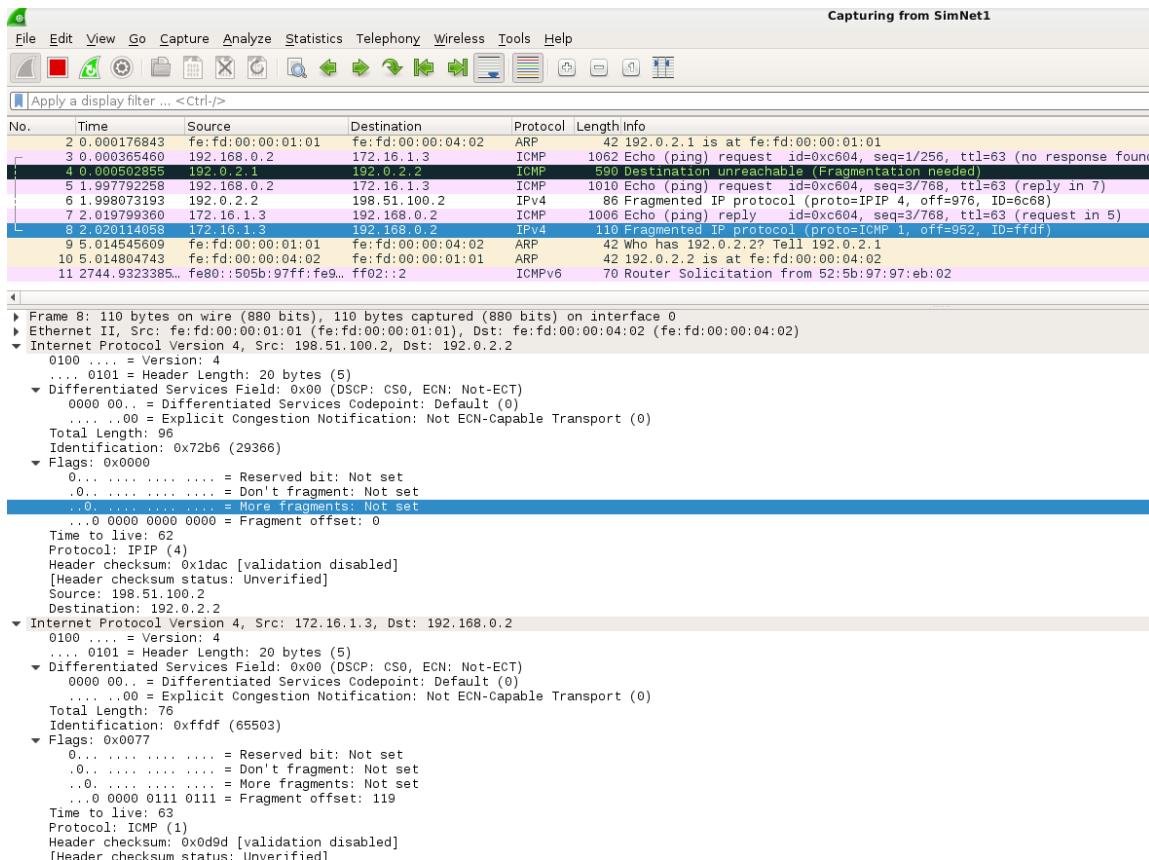
Source: 192.0.2.2

Destination: 198.51.100.2

Data (52 bytes)

Data: b4b5b6b7b8b9babbbcbdbefc0c1c2c3c4c5c6c7c8c9cacb...

[Length: 52]



**Hay 2 paquetes fragmentados. En las cuales el DF=0, tanto en inner header como en el outer header.**

(e) Describe in detail the sizes and headers of these packets. Is fragmentation performed in the same way than SimNet0? Why the difference? Notice that the Fragment Offset field in the IP header is measured in units of 8 bytes.

**No porque en el SimNet0 tenemos la MTU es un poco mas grande que en la SimNet1, aparte en la SimNet 1 se hace la encapsulacion y en el 0 no.**

(f) In SimNet3, how many ICMP echo-requests can you see? Describe sizes and headers.

**1 echo request, paquete (992 dato+8) + 8 +8+14+20 = 1042.**

(g) In SimNet3, how many ICMP echo-reply messages can you see? Describe sizes and headers.

**1 echo reply, paquete (992 dato+8)+8+14+20 = 1042.**

(h) In SimNet2, how many fragmented packets can you see that correspond to this third ICMP echo-reply? Describe in detail sizes of these packets and headers. Is fragmentation performed in the same way than for the ICMP Request message? Describe in detail sizes of these packets and headers.

**Hay 2 fragmentaciones, pero de tamaño diferente que el SimNet0 ya que ahora se ha de añadir 20 bytes de protocolo IPIP. Como las longitudes serán distintas y la fragmentación se hace con números múltiplos de 8 pues salen fragmentaciones distintas.**

Finally, we will send the latest ping of this series:

1. Delete the kernel routing cache executing the label flushcache.

//from terminal

**simctl iptunnel exec flushcache**

2. Put all wiresharks listening traffic in all SimNet interfaces.

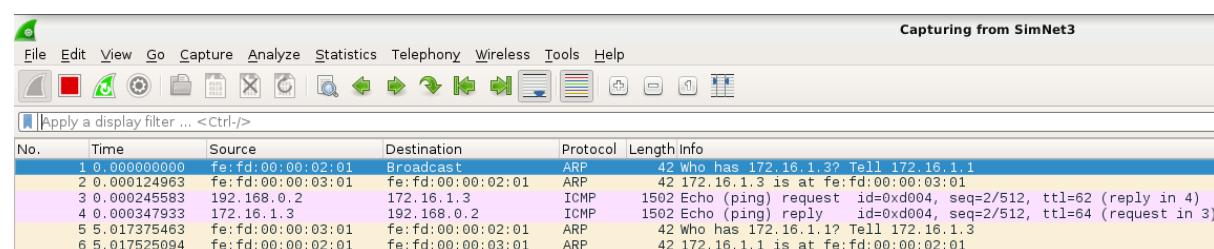
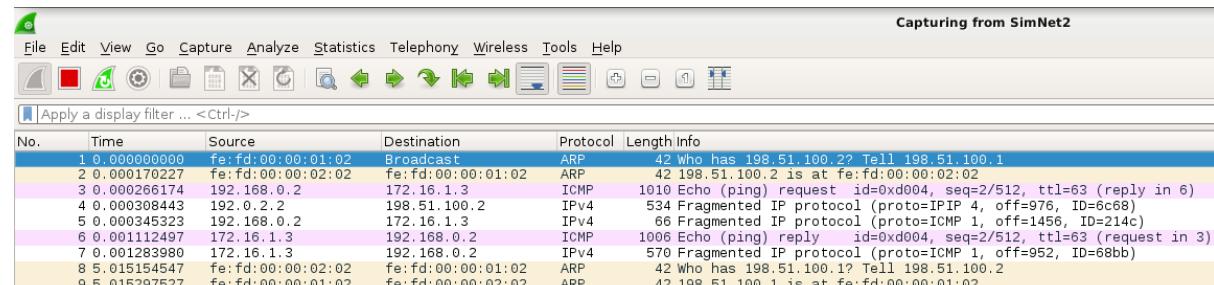
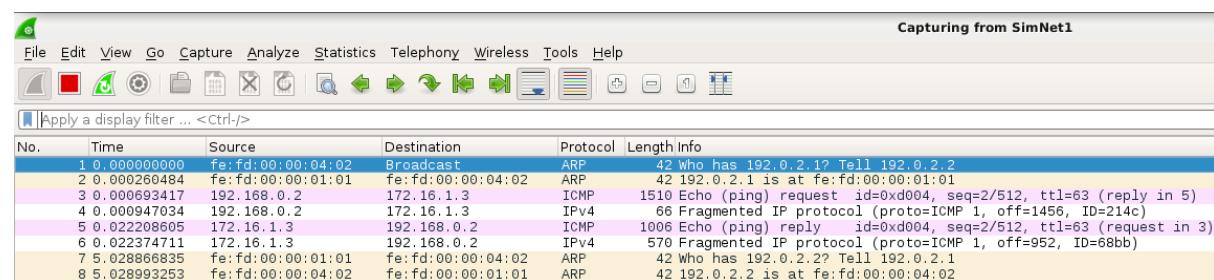
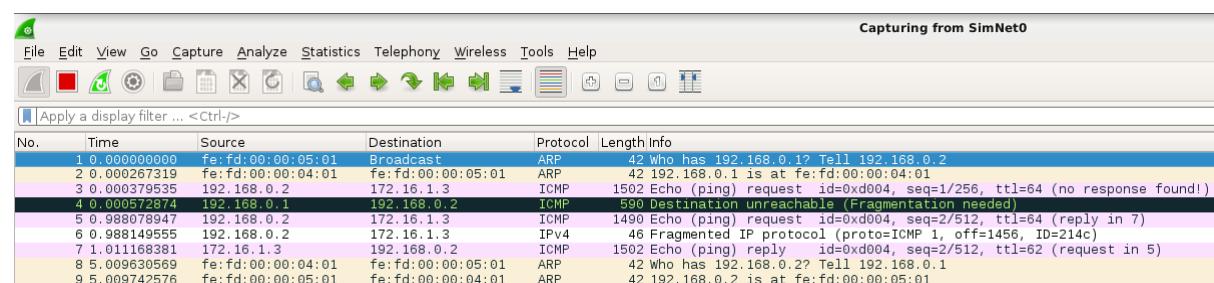
3. Execute the following command in host2:

//from host2

**ping -c2 -s 1460 -M want -i1 172.16.1.3**

```
host2:~# ping -c2 -s 1460 -M want -i1 172.16.1.3
PING 172.16.1.3 (172.16.1.3) 1460(1488) bytes of data.
From 192.168.0.1 icmp_seq=1 Frag needed and DF set (mtu = 1480)
1468 bytes from 172.16.1.3: icmp_seq=2 ttl=62 time=23.3 ms

--- 172.16.1.3 ping statistics ---
2 packets transmitted, 1 received, +1 errors, 50% packet loss, time 1008ms
rtt min/avg/max/mdev = 23.312/23.312/23.312/0.000 ms
```



(a) Is there any error message? Who is the sender of this error?

**Si, lo envia R1 a host2.**

(b) Which is the value of MTU that is reporting this error message? Is this value the real path MTU value? Why there are no more errors during the transmission? Have a look to the DF flag

**icmp.mtu == 1480**, es es lo que indica el error icmp. Si es el valor maximo de datos que puede pasar por el R1 ya que su MTU es 1500 (1480 datos + 20 cabecera).

En el primer ping tenemos DF=1, pero despues de recibir el error, el host2 pone en el segundo ping DF=0.

Por eso el segundo ping es exitoso, ya que viaja con el DF=0, entonces en routers que se tenga que fragmentar se fragmenta y se envia paquetes fragmentados.

---

### The -M do option (TO DO AT HOME)

### 0.7 Testing tunnels: pmtudisc (TO DO AT HOME)

---

### 0.8 Testing tunnels: TCP and MSS

Maximum Segment Size (MSS) is the maximum amount of data (in bytes) that TCP can receive in a TCP segment.

In the 3-way handshake (SYN, SYN/ACK, ACK) of TCP, each side informs its MSS value to the other side.

This is done by means of the “Options” field of the TCP headers in the SYN segments.

Each host calculates its MSS by deducting the minimum IP and TCP headers to the MTU value. In case of using Ethernet, a host will advertise a MSS of 1460 bytes (1500 bytes of MTU - 20 bytes of minimum IP header - 20 bytes of minimum TCP header).

Now you are going to test how the TCP protocol behaves when the connection go through a tunnel. First, reestablish the tunnel with the option nomptudisc. Leave the MTU=996 in SimNet2.

**//from terminal**

**simctl iptunnel exec deltun**

**simctl iptunnel exec addtun\_nopmtu**

**//from R1 and RC**

**ifconfig eth2 mtu 996**

## 0.8.1 Netcat and TCP

First, we will start doing a correct transmission (without filtering rules) using netcat:

1. Put all wiresharks listening traffic in all SimNet interfaces.
2. Start a netcat server in host3 listening in port 12345 (the -l option means listen, that is, this host is behaving as server):

//from host3

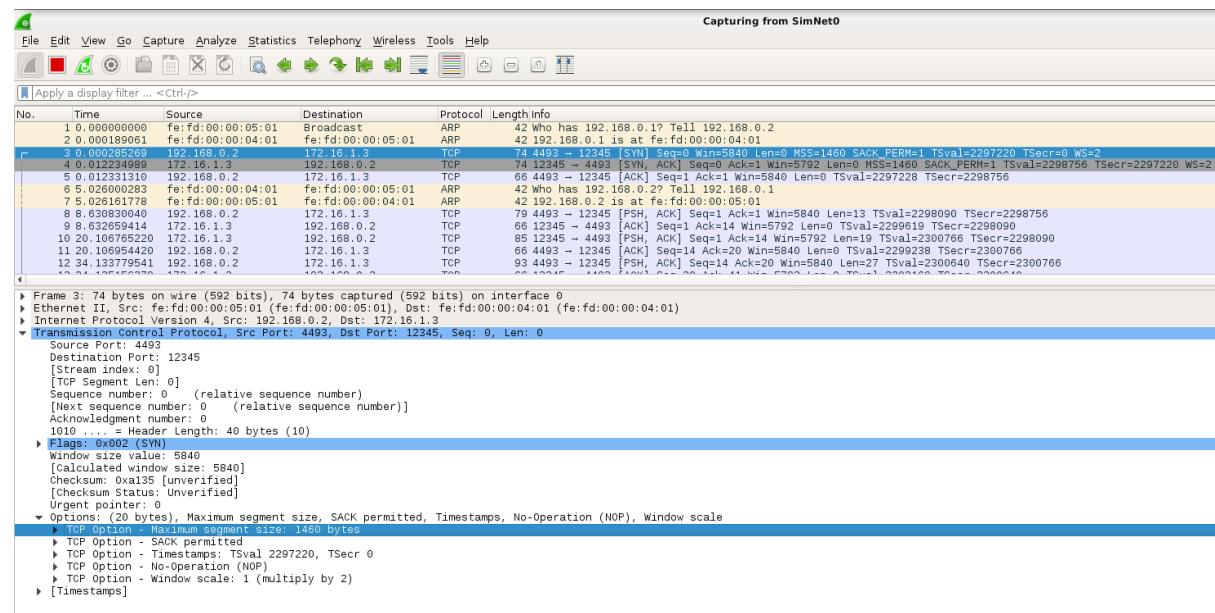
```
nc -l - p 12345
```

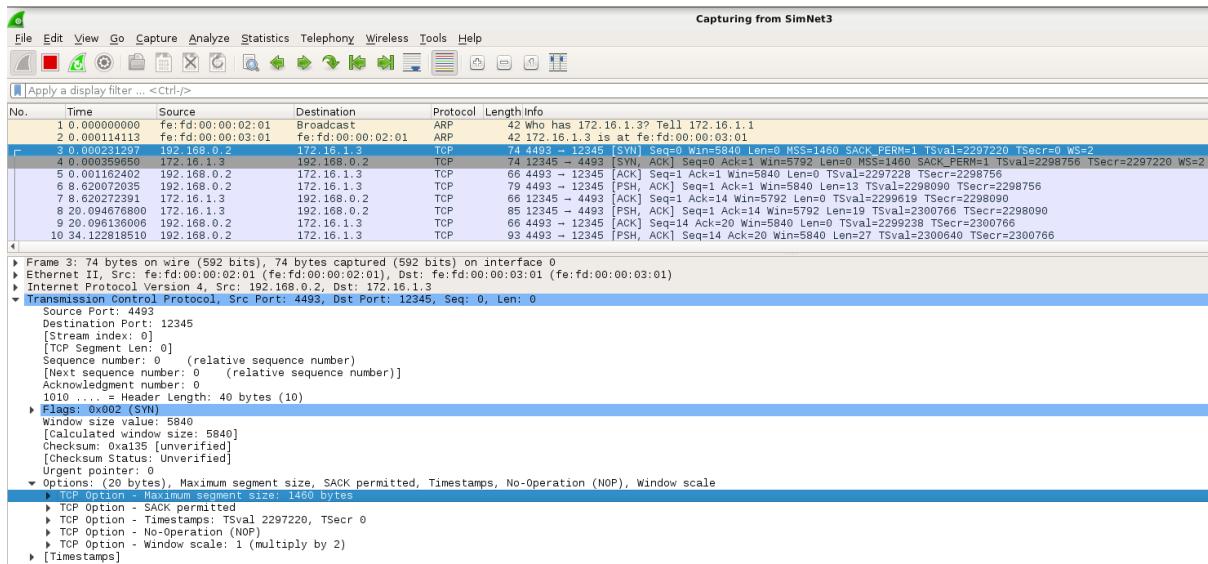
//from host2

```
nc 172.16.1.3
```

```
host2:~# nc 172.16.1.3 12345
Hola Mclovin
Hey james, que tal
bien Mc y tu como andas??

host3:~# nc -l - p 12345
Hola Mclovin
Hey james, que tal
bien Mc y tu como andas??
```





(a) Can you see the classical 3-way handshake of TCP?

**SIUUUU**

(b) Which is the value of the MSS (Maximum Segment Size) advertised in this handshake?

**1460 Bytes tanto el cliente como el servidor.**

(c) What is the meaning of this MSS? Can have the client a MSS different from the server?

**El MSS es el máximo número de bytes de datos que un host puede recibir a través de TCP en un segmento TCP. El cliente podría tener un MSS diferente al servidor ya que depende del MTU de la capa de enlace, de todas formas hay que recordar que no se negocia con el MSS sino que se informa de éste y el que envía los datos está obligado a usarlo.**

## **0.8.2 Netcat to transfer files**

Netcat can also be used to transfer files:

1. Delete the kernel routing cache executing the label flushcache.

**//from terminal**

**simctl iptunnel exec deltun**

**simctl iptunnel exec addtun\_nopmtu**

**//from R1 and RC**

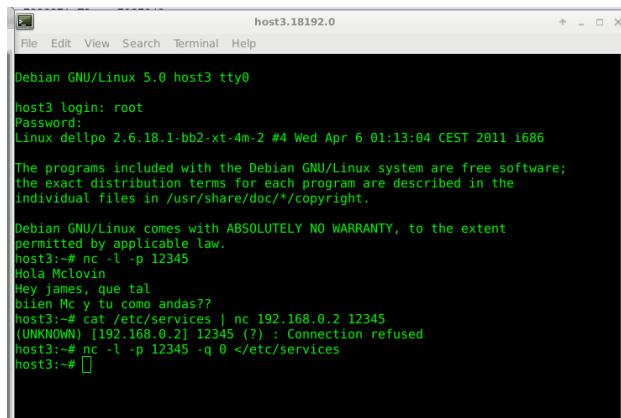
**ifconfig eth2 mtu 996**

2. Put all wiresharks listening traffic in all SimNet interfaces.

3. Start the netcat server in host3, that will send the file /etc/services towards the client when the connection has been established:

**//from host3**

**nc -l -p 12345 -q 0 </etc/services**



```
host3.18192.0
File Edit View Search Terminal Help
Debian GNU/Linux 5.0 host3 tty
host3 login: root
Password:
Linux dellpo 2.6.18.1-bb2-xt-4m-2 #4 Wed Apr 6 01:13:04 CEST 2011 i686
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
host3:# nc -l -p 12345
Hola Mclovin
Hey james, que tal
bien Mc y tu como andas?
host3:# cat /etc/services | nc 192.168.0.2 12345
(UNKNOWN) [192.168.0.2] 12345 (?) : Connection refused
host3:# nc -l -p 12345 -q 0 </etc/services
host3:#
```

4. Start the netcat client in host2, that will display in the screen the file /etc/services of the server.

**//from host2**

**nc 172.16.1.3 12345**

```

host2.19911.0
File Edit View Search Terminal Help
amixdttape 10083/tcp          # amanda backup services
smsp 11201/tcp          # Alamin SMS gateway
smsp 11201/udp
xpilot 15345/tcp          # XPilot Contact Port
xpilot 15345/udp
sgl-cmsd 17001/udp          # Cluster membership services daemon
sgl-crsd 17002/udp
sgl-gcd 17003/udp          # SGI Group membership daemo
n
sgl-cad 17004/tcp          # Cluster Admin daemon
isdnlog 2001/tcp          # isdn logging system
isdnlog 2001/udp
vboxd 20012/tcp          # voice box system
vboxd 20012/udp
binkp 24554/tcp          # binkp fidonet protocol
asp 27374/tcp          # Address Search Protocol
asp 27374/udp
csync2 30865/tcp          # cluster synchronization to
ol
ircproxy 57000/tcp          # Detachable IRC Proxy
tido 60177/tcp          # fidonet EMSI over telnet
tido 60179/tcp          # fidonet EMSI over TCP

# Local services
host2:~#

```

Capturing from SimNet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/>

Time	Source	Destination	Protocol	Length	Info
1 0.0000000000	fe:fd:00:00:05:01	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
2 0.0000000000	fe:fd:00:00:04:01	fe:fd:00:00:04:01	ARP	42	192.168.0.1 is at fe:fd:00:00:04:01
3 0.000369894	192.168.0.2	172.16.1.3	TCP	74	3183 - 12345 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=7935335 TSeqcr=0 WS=2
4 0.0332659478	172.16.1.3	192.168.0.2	TCP	74	12345 - 3183 [SYN, ACK] Seq=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSeqval=7936869 TSeqcr=7935335 WS=2
5 0.033709465	192.168.0.2	172.16.1.3	TCP	66	3183 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeqval=7935342 TSeqcr=7936869

Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
 ▶ Ethernet II, Src: fe:fd:00:00:05:01 (fe:fd:00:00:05:01), Dst: fe:fd:00:00:04:01 (fe:fd:00:00:04:01)  
 ▶ Internet Protocol Version 4, Src: 192.168.0.2, Dst: 172.16.1.3  
 ▶ Transmission Control Protocol, Src Port: 3183, Dst Port: 12345, Seq: 0, Len: 0  
 Source Port: 3183  
 Destination Port: 12345  
 [Stream index: 0]  
 [Sequence number: 0 (relative sequence number)]  
 [Next sequence number: 0 (relative sequence number)]  
 Acknowledgment number: 0  
 1010 ... = Header Length: 40 bytes (10)  
 ▶ Flags: 0x002 (SYN)  
 Window size value: 5840  
 [Calculated window size: 5840]  
 Checksum: 0x5f1f [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0  
 ▶ Options: (20 bytes). Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale  
 ▶ TCP Option Maximum segment size: 1460 bytes  
 ▶ TCP Option - SACK permitted  
 ▶ TCP Option - Timestamps: TSeqval 7935335, TSeqcr 0  
 ▶ TCP Option - No-Operation (NOP)  
 ▶ TCP Option - Window scale: 1 (multiply by 2)  
 ▶ [Timestamps]

Capturing from SimNet1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1 0.0000000000	fe:fd:00:00:04:02	Broadcast	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2	
2 0.000178632	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.1 is at fe:fd:00:00:01:01	
3 0.0003252598	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=7935335 TSeqcr=0 WS=2	
4 0.0332625789	172.16.1.3	192.168.0.2	TCP	86	12345 - 3183 [SYN, ACK] Seq=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSeqval=7936869 TSeqcr=7935335 WS=2	
5 0.033262887	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeqval=7935342 TSeqcr=7936869	
6 0.033187585	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=1 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
7 0.035211175	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [ACK] Seq=925 Ack=1 Win=5792 Len=524 TSeqval=7936871 TSeqcr=7935342	
8 0.039524966	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=1 Win=7689 Len=0 TSeqval=7935342 TSeqcr=7936871	
9 0.036435172	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=1449 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
10 0.036747940	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [ACK] Seq=2373 Ack=1 Win=5792 Len=524 TSeqval=7936871 TSeqcr=7935342	
11 0.037152442	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=1 Win=9536 Len=0 TSeqval=7935342 TSeqcr=7936871	
12 0.037152442	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=2881 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
13 0.039127574	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [PSH, ACK] Seq=3821 Ack=1 Win=5792 Len=524 TSeqval=7936871 TSeqcr=7935342	
14 0.038562140	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=2373 Win=11384 Len=0 TSeqval=7935342 TSeqcr=7936871	
15 0.039178280	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=4245 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
16 0.039471932	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [ACK] Seq=5269 Ack=1 Win=5792 Len=524 TSeqval=7936871 TSeqcr=7935342	
17 0.039855284	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=1 Win=13239 Len=0 TSeqval=7935342 TSeqcr=7936871	
18 0.040376124	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=5793 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
19 0.040531068	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [ACK] Seq=6717 Ack=1 Win=5792 Len=524 TSeqval=7936871 TSeqcr=7935342	
20 0.040531070	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=1 Win=9536 Len=0 TSeqval=7935342 TSeqcr=7936871	
21 0.041487708	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=7241 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
22 0.041737902	172.16.1.3	192.168.0.2	TCP	114	12345 - 3183 [PSH, ACK] Seq=8165 Ack=1 Win=5792 Len=28 TSeqval=7936871 TSeqcr=7935342	
23 0.042140335	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=4345 Win=16928 Len=0 TSeqval=7935342 TSeqcr=7936871	
24 0.042741821	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=8193 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
25 0.042903140	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=9117 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
26 0.043615854	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=5269 Win=18776 Len=0 TSeqval=7935342 TSeqcr=7936871	
27 0.044136712	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=10041 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
28 0.044245459	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=10465 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
29 0.044245462	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=10503 Ack=1 Win=5792 Len=0 TSeqval=7936871 TSeqcr=7935342	
30 0.046938056	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=11889 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
31 0.047216168	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=12813 Ack=1 Win=5792 Len=924 TSeqval=7936871 TSeqcr=7935342	
32 0.0490686700	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=6717 Win=20624 Len=0 TSeqval=7935342 TSeqcr=7936871	

Capturing from SimNet2							
No.	Time	Source	Destination	Protocol	Length	Info	
6	0.022980181	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=1 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
27	0.031990232	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=10041 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
30	0.034781031	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=11884 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
31	0.035068707	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=12813 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
33	0.037521000	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=13737 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
9	0.024270455	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=14491 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
30	0.038946309	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=14661 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
38	0.039913629	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=15581 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
40	0.040539317	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=16504 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
42	0.041680480	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=17433 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
50	0.135973503	172.16.1.3	192.168.0.2	TCP	86	12345 - 3183 [ACK] Seq=18481 Ack=2 Win=5792 Len=924 TSval=7936862 TSecr=7935342	
10	0.024583318	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [ACK] Seq=2373 Ack=1 Win=5792 Len=524 TSval=7936871 TSecr=7935342	
12	0.025567486	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=2891 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
15	0.027010926	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=3435 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
16	0.027266519	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [ACK] Seq=5269 Ack=1 Win=5792 Len=524 TSval=7936871 TSecr=7935342	
18	0.028215157	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=6211 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
19	0.028372262	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [ACK] Seq=6717 Ack=1 Win=5792 Len=524 TSval=7936871 TSecr=7935342	
21	0.030352512	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=7241 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
24	0.031992893	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=8193 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
25	0.030761467	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [ACK] Seq=9117 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
7	0.032004146	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [ACK] Seq=925 Ack=1 Win=5792 Len=524 TSval=7936871 TSecr=7935342	
44	0.042144262	172.16.1.3	192.168.0.2	TCP	210	12345 - 3183 [FIN, PSH, ACK] Seq=18357 Ack=1 Win=5792 Len=124 TSval=7936871 TSecr=7935342	
28	0.032154951	172.16.1.3	192.168.0.2	TCP	1010	12345 - 3183 [PSH, ACK] Seq=10965 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
10	0.025956158	172.16.1.3	192.168.0.2	TCP	610	12345 - 3183 [PSH, ACK] Seq=8211 Ack=1 Win=5792 Len=524 TSval=7936871 TSecr=7935342	
22	0.029577637	172.16.1.3	192.168.0.2	TCP	114	12345 - 3183 [PSH, ACK] Seq=8165 Ack=1 Win=5792 Len=29 TSval=7936871 TSecr=7935342	
4	0.020608521	172.16.1.3	192.168.0.2	TCP	94	12345 - 3183 [SWSN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7936865	
52	5.03094424	fe:fd:00:00:01:02	fe:fd:00:00:02:02	ARP	42	198.51.100.1 is at fe:fd:00:00:01:02	
2	0.000210488	fe:fd:00:00:01:02	fe:fd:00:00:02:02	ARP	42	198.51.100.2 is at fe:fd:00:00:02:02	
5	0.021343554	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=7935342 TSecr=7936869	
37	0.039643496	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=10041 Len=0 TSval=7936871 TSecr=7935342	
39	0.040210740	192.168.0.2	172.16.1.3	TCP	86	3183 - 12345 [ACK] Seq=10965 Len=0 TSval=28016 Len=0 TSval=7935342 TSecr=7936871	

Capturing from SimNet3							
No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000000	192.168.0.2	172.16.1.3	TCP	74	3183 - 12345 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=7935335 TSecr=0 WS=2	
2	0.019543148	fe:fd:00:00:03:01	Broadcast	ARP	42	Who has 172.16.1.1? Tell 172.16.1.3	
3	0.019770887	fe:fd:00:00:02:01	fe:fd:00:00:03:01	ARP	42	172.16.1.1 is at fe:fd:00:00:02:01	
4	0.019875019	192.168.0.2	192.168.0.2	TCP	74	12345 - 3183 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7936869 TSecr=7935335 WS=2	
5	0.020942524	192.168.0.2	172.16.1.3	TCP	66	3183 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=7935342 TSecr=7936869	
6	0.021719902	172.16.1.3	192.168.0.2	TCP	1514	12345 - 3183 [ACK] Seq=1 Ack=1 Win=5792 Len=1448 TSval=7936871 TSecr=7935342	
7	0.021745849	172.16.1.3	192.168.0.2	TCP	1514	12345 - 3183 [ACK] Seq=1449 Ack=1 Win=5792 Len=1448 TSval=7936871 TSecr=7935342	
8	0.022037601	172.16.1.1	172.16.1.3	ICMP	580	Destination unreachable (Fragmentation needed)	
9	0.022037601	172.16.1.1	172.16.1.3	ICMP	580	Destination unreachable (Fragmentation needed)	
10	0.022272072	172.16.1.3	192.168.0.2	TCP	990	[TCP Out-Of-Order] 12345 - 3183 [ACK] Seq=1 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
11	0.022256618	172.16.1.3	192.168.0.2	TCP	590	[TCP Out-of-order] 12345 - 3183 [ACK] Seq=925 Ack=1 Win=5792 Len=524 TSval=7936871 TSecr=7935342	
12	0.023465956	192.168.0.2	172.16.1.3	TCP	66	3183 - 12345 [ACK] Seq=1 Ack=925 Win=7688 Len=0 TSval=7935342 TSecr=7936871	
13	0.023594213	172.16.1.3	192.168.0.2	TCP	990	[TCP Out-Of-Order] 12345 - 3183 [ACK] Seq=1449 Ack=1 Win=5792 Len=924 TSval=7936871 TSecr=7935342	
14	0.023618038	172.16.1.3	192.168.0.2	TCP	590	[TCP Retransmission] 12345 - 3183 [ACK] Seq=2373 Ack=1 Win=5792 Len=524 TSval=7936871 TSecr=7935342	
15	0.023785810	172.16.1.2	172.16.1.2	TCP	66	3183 - 12345 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSval=7025249 TSecr=7936871	
Internet Control Message Protocol							
Type: 3 (Destination unreachable)							
Code: 4 (Fragmentation needed)							
Csum: 0x36f1 [correct]							
[Checksum Status: Good]							
Unreachable hop: 976							
Internet Protocol Version 4, Src: 172.16.1.3, Dst: 192.168.0.2							
0100 ... = Version: 4							
...0101 = Header Length: 20 bytes (5)							
... Differential Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)							
0000 0000 ... = Differentiated Services Codepoint: Default (0)							
...0000 0000 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)							
Total Length: 1860							
Identification: 0x21c9 (8649)							
Flags: 0x4000, Don't fragment							
0 ... = Reserved bit: Not set							
1 ... = Don't fragment: Set							
0 ... = More fragments: Not set							
...0 0000 0000 0000 = Fragment offset: 0							
Time to live: 64							
Protocol: 6 (TCP)							
Header checksum: 0xa595 [validation disabled]							
[Header checksum status: Unverified]							
Source: 172.16.1.3							
Destination: 192.168.0.2							
Transmission Control Protocol, Src Port: 12345, Dst Port: 3183, Seq: 3052354222, Ack: 3037289685							
Source Port: 12345							
Destination Port: 3183							
Sequence number: 3052354222 (relative sequence number)							
Acknowledgment number: 3037289685 (relative ack number)							
1000 ... = Header Length: 32 bytes (8)							
Flags: 0x10 (ACK)							
Window size value: 2896							
[Calculated window size: 2896], [Window size offset: 0], [Window size scale factor: 0]							

(a) In the 3-way handshake, which was the value of the MSS?

**Si, el valor de MSS es de 1460 Bytes para los 2 (cliente, servidor).**

(b) Did you notice any problem during the transmission according to the wiresharks?

**Si, en el SimNet3 hay mensaje de error ICMP (fragmentation-needed).**

(c) Can you see any ICMP message in SimNet3? Who is sending these error messages and why?

**El mensaje de error lo envia R2 al host3 avisando que se envie paquetes mas pequeños.(indicando en el mensaje ICMP que ponga DF=0).**

(d) Was the file transmitted properly? Who solved the problem?

**Si, pero con retransmision. R2 ha resuelto el problema, ya que ha avisado al host3 que envie paquetes pequeños.**

(e) Is this meaning that the MSS has changed during the transmission?.

**No cambia, solo se ve la principio al establecer la comunicación,**

As you can see from the previous example, TCP is a reliable protocol. This means that it will retransmit lost information until it is properly received (or after a certain number of unsuccessful retransmissions). TCP is able to change the lenght of the segments in case that the network reports problems of size, but this does not mean that the MSS changes, as it is a fixed value.

Obviously, files can be transmitted in both directions using netcat. In the previous example, we made a transmission in which the server transferred a file towards the client. Now we will test this same operation in the reverse direction.

1. Delete the kernel routing cache executing the label flushcache.

**//from terminal**

**simctl iptunnel exec flushcache**

2. Put all wiresharks listening traffic in all SimNet interfaces.

3. Start the netcat server in host3:

**//from host3**

**nc -l -p 12345**

4. Start the netcat client in host2, but in this case inject the file /etc/services of the client towards the server using the TCP connection.

**//from host2**

**nc 172.16.1.3 12345 -q 0 </etc/services**

```

host2.0                               host3.18192.0
File Edit View Search Terminal Help      File Edit View Search Terminal Help
amidxtape 10083/tcp # amanda backup services
smsgp 11201/tcp # Alamin SMS gateway
smsgp 11201/udp
xpilot 15345/tcp # XPilot Contact Port
xpilot 15345/udp
sgl-cmds 17001/udp # Cluster membership services daemon
sgl-crsd 17002/udp
sgl-gcd 17003/udp # SGI Group membership daemon
sgl-cad 17004/tcp # Cluster Admin daemon
isdnlog 20011/tcp # isdn logging system
isdnlog 20011/udp
vboxd 20012/tcp # voice box system
vboxd 20012/udp
binkp 24554/tcp # binkp fidonet protocol
asp 27374/tcp # Address Search Protocol
asp 27374/udp
csync2 30865/tcp # cluster synchronization tool
dircproxy 57000/tcp # Detachable IRC Proxy
tfido 60177/tcp # fidonet EMSI over telnet
fido 60179/tcp # fidonet EMSI over TCP
# Local services
host2:# nc 172.16.1.3 12345 -q 0 </etc/services
host2:# [REDACTED]

```

Capturing from SimNet0						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe:ff:00:00:05:01	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
2	0.000289741	fe:ff:00:00:04:01	fe:ff:00:00:05:01	ARP	42	192.168.0.1 is at fe:ff:00:00:04:01
3	0.000382873	192.168.0.2	172.16.1.3	TCP	74	2516 - 12345 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=8312522 TSeqcr=0 WS=2
4	0.019611098	192.168.1.3	192.168.0.2	TCP	74	12345 - 2516 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSeqval=8314059 TSeqcr=8312522 WS=2
5	0.019750499	192.168.0.2	172.16.1.3	TCP	66	2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeqval=8312530 TSeqcr=8314059
6	0.021291098	192.168.0.2	172.16.1.3	TCP	1514	2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1448 TSeqval=8312531 TSeqcr=8314059
7	0.021502004	192.168.0.1	192.168.0.2	ICMP	590	Destination unreachable (Fragmentation needed)
8	0.0218686096	192.168.0.2	172.16.1.3	TCP	1494	2516 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=1428 TSeqval=8312531 TSeqcr=8314059
9	0.022105029	192.168.0.2	172.16.1.3	TCP	1494	12345 - 2516 [ACK] Seq=1449 Ack=1 Win=5840 Len=1428 TSeqval=8312531 TSeqcr=8314059
10	0.311290742	192.168.0.1	192.168.0.2	ICMP	590	Destination unreachable (Fragmentation needed)
11	0.3688756137	192.168.0.2	172.16.1.3	TCP	990	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=924 TSeqval=8312615 TSeqcr=8314059
12	0.8699824237	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=25 Win=7640 Len=0 TSeqval=8314144 TSeqcr=8312615
13	0.869923975	192.168.0.2	172.16.1.3	TCP	570	[TCP Retransmission] 2516 - 12345 [ACK] Seq=25 Ack=1 Win=5840 Len=504 TSeqval=8312616 TSeqcr=8314059
14	0.869941316	192.168.0.2	172.16.1.3	TCP	66	[TCP Retransmission] 2516 - 12345 [ACK] Seq=25 Ack=1 Win=5840 Len=20 TSeqval=8312616 TSeqcr=8314144
15	0.872095322	192.168.0.2	172.16.1.3	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=1 Win=5840 Len=924 TSeqval=8314144 TSeqcr=8312616
16	0.872022502	192.168.0.2	172.16.1.3	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=1 Win=5840 Len=924 TSeqval=8314144 TSeqcr=8312616
17	0.872135510	192.168.0.2	172.16.1.3	TCP	990	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314059
18	0.872139582	192.168.0.2	172.16.1.3	TCP	570	[TCP Retransmission] 2516 - 12345 [ACK] Seq=273 Ack=1 Win=5840 Len=504 TSeqval=8312616 TSeqcr=8314144
19	0.872155426	192.168.0.2	172.16.1.3	TCP	66	2516 - 12345 [ACK] Seq=2877 Ack=1 Win=5840 Len=20 TSeqval=8312616 TSeqcr=8314144
20	0.872283520	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=273 Win=11336 Len=0 TSeqval=8314144 TSeqcr=8312616
21	0.8732299867	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=2877 Win=13184 Len=0 TSeqval=8314144 TSeqcr=8312616
22	0.873315022	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314059
23	0.873424471	192.168.0.2	172.16.1.3	TCP	990	2516 - 12345 [ACK] Seq=2897 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
24	0.873444144	192.168.0.2	172.16.1.3	TCP	590	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
25	0.873459594	192.168.0.2	172.16.1.3	TCP	990	2516 - 12345 [ACK] Seq=435 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
26	0.873486748	192.168.0.2	172.16.1.3	TCP	590	2516 - 12345 [ACK] Seq=5269 Ack=1 Win=5840 Len=524 TSeqval=8312616 TSeqcr=8314144

Capturing from SimNet1						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe:ff:00:00:04:02	Broadcast	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2
2	0.000200491	fe:ff:00:00:01:01	fe:ff:00:00:04:02	ARP	42	192.0.2.1 is at fe:ff:00:00:01:01
3	0.000339729	192.168.0.2	172.16.1.3	TCP	94	2516 - 12345 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=8312522 TSeqcr=0 WS=2
4	0.019611098	192.168.0.2	172.16.1.3	TCP	94	12345 - 2516 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=8312522 TSeqcr=0 WS=2
5	0.019750499	192.168.0.2	172.16.1.3	TCP	66	2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeqval=8312530 TSeqcr=8314059
6	0.021361670	192.168.0.2	172.16.1.3	TCP	1514	[TCP Previous segment capture] 2516 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=1428 TSeqval=8312531 TSeqcr=8314059
7	0.021500901	192.0.2.1	192.168.0.2	ICMP	590	Destination unreachable (Fragmentation needed)
8	0.866241980	192.168.0.2	172.16.1.3	TCP	1010	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=924 TSeqval=8312615 TSeqcr=8314059
9	0.866954687	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=925 Win=7640 Len=0 TSeqval=8314144 TSeqcr=8312616
10	0.870341139	192.168.0.2	172.16.1.3	TCP	590	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
11	0.870352671	192.168.0.2	172.16.1.3	TCP	100	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
12	0.871148307	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=1429 Win=9488 Len=924 TSeqval=8312616 TSeqcr=8314144
13	0.871165013	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=1449 Win=9488 Len=924 TSeqval=8312616 TSeqcr=8314144
14	0.871593641	192.168.0.2	172.16.1.3	TCP	1010	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
15	0.871610199	192.168.0.2	172.16.1.3	TCP	590	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=504 TSeqval=8312616 TSeqcr=8314144
16	0.872041979	192.168.0.2	172.16.1.3	TCP	100	[TCP Retransmission] 2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=504 TSeqval=8312616 TSeqcr=8314144
17	0.872419799	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=2372 Win=11336 Len=0 TSeqval=8314144 TSeqcr=8312616
18	0.872435089	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=2877 Win=13184 Len=0 TSeqval=8314144 TSeqcr=8312616
19	0.872437043	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=2877 Win=13184 Len=0 TSeqval=8314144 TSeqcr=8312616
20	0.873039311	192.168.0.2	172.16.1.3	TCP	1010	2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
21	0.873057781	192.168.0.2	172.16.1.3	TCP	610	2516 - 12345 [PSH, ACK] Seq=4345 Ack=1 Win=5840 Len=524 TSeqval=8312616 TSeqcr=8314144
22	0.873424740	192.168.0.2	172.16.1.3	TCP	1008	2516 - 12345 [PSH, ACK] Seq=4345 Ack=1 Win=5840 Len=524 TSeqval=8312616 TSeqcr=8314144
23	0.873807638	192.168.0.2	172.16.1.3	TCP	610	2516 - 12345 [PSH, ACK] Seq=524 Ack=1 Win=5840 Len=524 TSeqval=8312616 TSeqcr=8314144
24	0.874010201	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=3821 Win=15032 Len=0 TSeqval=8314144 TSeqcr=8312616
25	0.874043827	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=4345 Win=16880 Len=0 TSeqval=8314144 TSeqcr=8312616
26	0.874060118	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=5269 Win=18728 Len=0 TSeqval=8314144 TSeqcr=8312616
27	0.874576331	192.168.0.2	172.16.1.3	TCP	1010	2516 - 12345 [ACK] Seq=5793 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
28	0.874593846	192.168.0.2	172.16.1.3	TCP	610	2516 - 12345 [ACK] Seq=6717 Ack=1 Win=5840 Len=524 TSeqval=8312616 TSeqcr=8314144

Capturing from SimNet2						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe:ff:00:00:01:02	Broadcast	ARP	42	Who has 198.51.100.2? Tell 198.51.100.1
2	0.000291131	fe:ff:00:00:02:02	fe:ff:00:00:01:02	ARP	42	198.51.100.1 is at fe:ff:00:00:01:02
3	0.000339729	192.168.0.2	172.16.1.3	TCP	610	2516 - 12345 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=8312522 TSeqcr=0 WS=2
4	0.019611098	192.168.0.2	172.16.1.3	TCP	64	12345 - 2516 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=8312522 TSeqcr=0 WS=2
5	0.033110630	192.168.0.2	172.16.1.3	TCP	66	2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeqval=8312530 TSeqcr=8314059
6	0.052175822	192.168.0.2	172.16.1.3	TCP	1010	2516 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=924 TSeqval=8312615 TSeqcr=8314059
7	0.052613811	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=1 Ack=925 Win=7640 Len=0 TSeqval=8314144 TSeqcr=8312616
8	0.054262080	172.16.1.3	192.168.0.2	TCP	590	12345 - 2516 [ACK] Seq=925 Ack=1 Win=5840 Len=0 TSeqval=8314144 TSeqcr=8312616
9	0.054277793	192.168.0.2	172.16.1.3	TCP	1010	2516 - 12345 [ACK] Seq=1429 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
10	0.054321818	192.168.0.2	172.16.1.3	TCP	610	2516 - 12345 [ACK] Seq=1429 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
11	0.054601939	172.16.1.3	192.168.0.2	TCP	610	2516 - 12345 [ACK] Seq=1449 Win=9488 Len=924 TSeqval=8312616 TSeqcr=8314144
12	0.055512337	192.168.0.2	172.16.1.3	TCP	1010	2516 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
13	0.055530627	192.168.0.2	172.16.1.3	TCP	590	2516 - 12345 [ACK] Seq=2373 Ack=1 Win=5840 Len=504 TSeqval=8312616 TSeqcr=8314144
14	0.055559052	192.168.0.2	172.16.1.3	TCP	106	2516 - 12345 [ACK] Seq=2877 Win=11336 Len=0 TSeqval=8314144 TSeqcr=8312616
15	0.055603124	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=2373 Win=11336 Len=0 TSeqval=8314144 TSeqcr=8312616
16	0.0556080229	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=2877 Win=13184 Len=0 TSeqval=8314144 TSeqcr=8312616
17	0.0556095680	172.16.1.3	192.168.0.2	TCP	86	12345 - 2516 [ACK] Seq=2897 Win=13184 Len=0 TSeqval=8314144 TSeqcr=8312616
18	0.055610032	192.168.0.2	172.16.1.3	TCP	100	2516 - 12345 [ACK] Seq=2897 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
19	0.057018180	192.168.0.2	172.16.1.3	TCP	610	2516 - 12345 [ACK] Seq=2897 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
20	0.057032902	192.168.0.2	172.16.1.3	TCP	1010	2516 - 12345 [ACK] Seq=4345 Ack=1 Win=5840 Len=924 TSeqval=8312616 TSeqcr=8314144
21	0.057049370	192.168.0.2</				

Capturing from SimNet3						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:ff:00:00:02:01	Broadcast	ARP	42	Who has 172.16.1.3? Tell 172.16.1.1
2	0.000364435	fe:ff:00:00:03:01	Broadcast	ARP	42	172.16.1.3 is at fe:ff:00:00:03:01
3	0.000364435	fe:ff:00:00:02:01	172.16.1.3	TCP	64	SYN ACK Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSeq=8312522 TSeqr=0 WS=2
4	0.000364435	172.16.1.3	192.168.0.2	TCP	74	12345 - 2516 [SYN ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSeq=8312522 TSeqr=8314059 WS=2
5	0.002444402	192.168.0.2	172.16.1.3	TCP	66	2516 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeq=8312530 TSeqr=8314059
6	0.051503457	192.168.0.2	172.16.1.3	TCP	990	2516 - 12345 [ACK] Seq=1 Ack=1 Win=924 TSeq=8312615 TSeqr=8314059
7	0.851672953	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=925 Win=7640 Len=0 TSeq=8314144 TSeqr=8312615
8	0.853585968	192.168.0.2	172.16.1.3	TCP	570	2516 - 12345 [ACK] Seq=925 Ack=1 Win=5840 Len=504 TSeq=8312616 TSeqr=8314144
9	0.853603142	192.168.0.2	172.16.1.3	TCP	86	12345 - 2516 [ACK] Seq=1249 Ack=1 Win=5840 Len=20 TSeq=8312616 TSeqr=8314144
10	0.853795187	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1249 Ack=1 Win=5840 Len=0 TSeq=8312616 TSeqr=8314144
11	0.854174464	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1249 Ack=1 Win=5840 Len=0 TSeq=8312616 TSeqr=8314144
12	0.854976929	192.168.0.2	172.16.1.3	TCP	990	2516 - 12345 [ACK] Seq=1249 Ack=1 Win=5840 Len=924 TSeq=8312616 TSeqr=8314144
13	0.854984384	192.168.0.2	172.16.1.3	TCP	570	2516 - 12345 [ACK] Seq=2373 Ack=1 Win=5840 Len=504 TSeq=8312616 TSeqr=8314144
14	0.854917399	192.168.0.2	172.16.1.3	TCP	86	2516 - 12345 [ACK] Seq=2877 Ack=1 Win=5840 Len=20 TSeq=8312616 TSeqr=8314144
15	0.855069793	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=2373 Win=11330 Len=0 TSeq=8314144 TSeqr=8312616
16	0.855087293	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=2877 Win=13184 Len=0 TSeq=8314144 TSeqr=8312616
17	0.855102289	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=2897 Win=13184 Len=0 TSeq=8314144 TSeqr=8312616
18	0.8554391817	192.168.0.2	172.16.1.3	TCP	990	2516 - 12345 [ACK] Seq=2897 Ack=1 Win=5840 Len=504 TSeq=8312616 TSeqr=8314144
19	0.855441002	192.168.0.2	172.16.1.3	TCP	590	2516 - 12345 [PSH] Seq=3821 Ack=1 Win=5840 Len=504 TSeq=8312616 TSeqr=8314144
20	0.855442546	192.168.0.2	172.16.1.3	TCP	990	2516 - 12345 [ACK] Seq=4345 Ack=1 Win=5840 Len=924 TSeq=8312616 TSeqr=8314144
21	0.8556441002	192.168.0.2	172.16.1.3	TCP	590	2516 - 12345 [ACK] Seq=5269 Ack=1 Win=5840 Len=524 TSeq=8312616 TSeqr=8314144
22	0.856673161	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=3821 Win=15032 Len=0 TSeq=8314144 TSeqr=8312616
23	0.856691742	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=4345 Win=16880 Len=0 TSeq=8314144 TSeqr=8312616
24	0.856707323	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=5269 Win=18724 Len=0 TSeq=8314144 TSeqr=8312616
25	0.857878923	192.168.0.2	172.16.1.3	TCP	990	2516 - 12345 [ACK] Seq=5793 Ack=1 Win=5840 Len=924 TSeq=8312616 TSeqr=8314144
26	0.858106783	192.168.0.2	172.16.1.3	TCP	590	2516 - 12345 [ACK] Seq=6771 Ack=1 Win=5840 Len=224 TSeq=8312616 TSeqr=8314144
27	0.858106783	192.168.0.2	172.16.1.3	TCP	990	2516 - 12345 [ACK] Seq=6771 Ack=1 Win=5840 Len=924 TSeq=8312616 TSeqr=8314144
28	0.858106108	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=6717 Win=20576 Len=0 TSeq=8314144 TSeqr=8312616
29	0.858127163	172.16.1.3	192.168.0.2	TCP	66	12345 - 2516 [ACK] Seq=1 Ack=8165 Win=22424 Len=0 TSeq=8314144 TSeqr=8312616
30	0.860498219	192.168.0.2	172.16.1.3	TCP	570	2516 - 12345 [ACK] Seq=8165 Ack=1 Win=5840 Len=504 TSeq=8312616 TSeqr=8314144

(a) Which are the commands that you used to do the previous behavior?

**host3 como server y host2 como cliente con grep del fichero etc/services.**

(b) Did you notice any problem during the transmission according to the wiresharks?

**Hay acks duplicados, y en SimNet0 y SimNet1 hay mensajes de error ICMP ().**

(c) Can you see any ICMP message in SimNet0 and SimNet1? Who is sending these error messages and why?

**En SimNet0 hay 2 mensajes (fragmentation needed) que lo envia el R1 al host2.**

**En SimNet1 hay 1 mensaje que lo envia RC al R1.**

**Estos mensajes son enviados porque los paquetes necesitan ser fragmentados.**

(d) Was the file transmitted properly? Who solved the problem?

**Si, porque TCP retransmite hasta que los paquetes llegan correctamente al destino. RC informa al R1 y R1 avisa al host2, y host2 resuelve el problema, enviando paquetes fragmentados.**

(e) According to the transmission, who is the TCP client and who is the TCP server?

**host3 server, host2 cliente.**

Again, TCP solved the problem by adapting the length of the segments to the network conditions and retransmitting lost information. Notice that the TCP client is the host that started the TCP dialogue by sending the first message SYN, and the TCP server is the host that answered by sending the SYN-ACK message, no matter of the direction of the data transmission.

### **0.8.3 TCP, tunnels and filtering**

1. Let us imagine that the network administrator of R1 wants to protect this router against typical attacks that use ICMP. For this reason, it avoids sending ICMP messages to this router. So, execute the following command to filter the ICMP traffic whose destination is R1:

```
//from R1
iptables -A INPUT -p icmp -j DROP
```

2. Delete the kernel routing cache executing the label flushcache.

```
//from terminal
simctl iptunnel exec flushcache
```

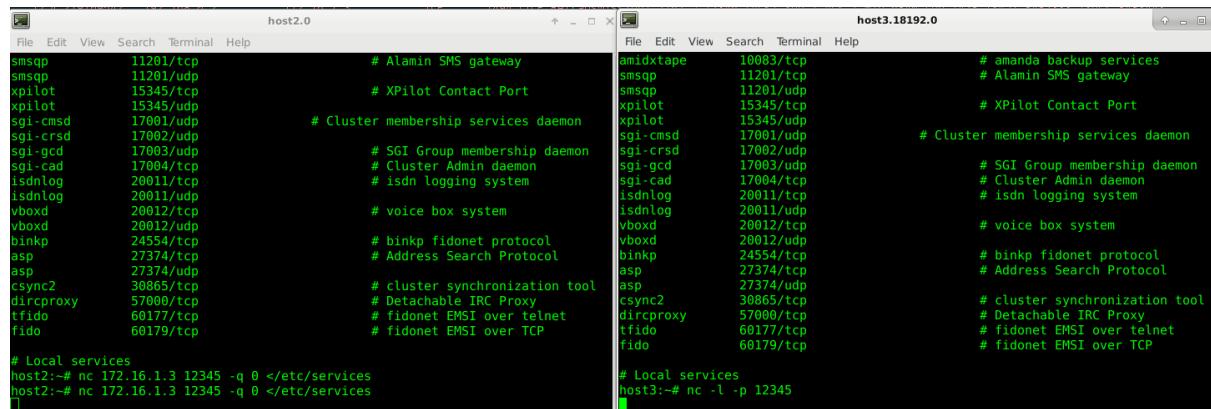
3. Put all wiresharks listening traffic in all SimNet interfaces.

4. Again using netcat, send the file /etc/services from host2 (acting as client) towards host3 (acting as server).

```
//from host3
nc -l -p 12345
```

**//from host2**

**nc 172.16.1.3 12345 -q 0 </etc/services**



Capturing from SimNet0						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:05:01	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
2	0.000187057	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	192.168.0.1 is at fe:fd:00:00:04:01
3	0.000200000	fe:fd:00:00:02:02	fe:fd:00:00:02:02	ARP	42	192.168.0.2 is at fe:fd:00:00:02:02
4	0.0180392166	172.16.1.3	192.168.0.2	TCP	74	12345 - 2152 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=8481905 Tscr=0 WS=2
5	0.018113028	192.168.0.2	172.16.1.3	TCP	66	2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 Tsvl=8483443 Tscr=8481905 WS=2
6	0.019259985	192.168.0.2	172.16.1.3	GTP	1514	Send routing information for GPRS request
7	0.019403836	192.168.0.1	192.168.0.2	ICMP	590	Destination unreachable (Fragmentation needed)
8	0.019643350	192.168.0.2	172.16.1.3	TCP	1494	2152 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=1428 Tsvl=8481913 Tscr=8483443
9	0.296024261	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8481941 Tscr=8483443
10	0.86077447	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8481997 Tscr=8483443
11	1.978088893	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8482109 Tscr=8483443
12	1.980088893	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8482109 Tscr=8483443
13	5.023576556	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	Who has 192.168.0.2? Tell 192.168.0.1
14	5.023718428	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42	192.168.0.2 is at fe:fd:00:00:05:01
15	8.701729524	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8482781 Tscr=8483443
16	17.661950690	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8483677 Tscr=8483443
17	35.580050967	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8485469 Tscr=8483443
18	40.580137752	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
19	40.580295266	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	192.168.0.1 is at fe:fd:00:00:04:01
20	71.00141737508	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8480053 Tscr=8482443
21	114.0014231028	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8482211 Tscr=8483443
22	148.093421268	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
23	148.093588269	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	192.168.0.1 is at fe:fd:00:00:04:01
24	263.112906495	fe:fd:00:00:05:01	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
25	263.113115668	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	192.168.0.1 is at fe:fd:00:00:04:01
26	263.113218800	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8480222 Tscr=8483443
27	383.104231028	192.168.0.2	172.16.1.3	TCP	1494	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8502222 Tscr=8483443
28	388.105765226	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
29	388.105945249	fe:fd:00:00:04:01	fe:fd:00:00:05:01	ARP	42	192.168.0.1 is at fe:fd:00:00:04:01
Capturing from SimNet1						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:04:02	Broadcast	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2
2	0.000134789	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.1 is at fe:fd:00:00:01:01
3	0.000134818	192.0.2.1	192.0.2.2	TCP	1494	2152 - 12345 [SYN, ACK] Seq=0 Win=0 MSS=1460 SACK_PERM=1 Tsvl=8481905 Tscr=0 WS=2
4	0.0174072702	172.16.1.3	192.168.0.2	TCP	94	12345 - 2152 [ACK] Seq=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=8483443 Tscr=8481905 WS=2
5	0.017724241	192.168.0.2	172.16.1.3	TCP	86	2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8481913 Tscr=8483443
6	0.019252889	192.168.0.2	172.16.1.3	TCP	1514	[TCP Previous segment not captured] 2152 - 12345 [ACK] Seq=1449 Ack=1 Win=5840 Len=1428 Tsvl=8481913 Tscr=8483443
7	0.019366798	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
8	0.295615798	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8481941 Tscr=8483443
9	0.299515798	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
10	0.300465572	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8481997 Tscr=8483443
11	0.860615307	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
12	1.977828101	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8482109 Tscr=8483443
13	1.977993800	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
14	2.194388978	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8482333 Tscr=8483443
15	2.195114145	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
16	5.026472539	fe:fd:00:00:01:01	fe:fd:00:00:02:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
17	5.026645630	fe:fd:00:00:02:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:02:02
18	8.701393059	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8492781 Tscr=8483443
19	8.701534915	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
20	10.681408452	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
21	17.661950690	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
23	35.579743199	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8485460 Tscr=8483443
24	71.417037632	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8489953 Tscr=8483443
25	71.417037632	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
26	76.122972598	fe:fd:00:00:04:02	fe:fd:00:00:04:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
27	76.125257776	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.2 is at fe:fd:00:00:01:01
28	143.093444636	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8496221 Tscr=8483443
29	143.0996164604	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
30	148.103110434	fe:fd:00:00:01:01	fe:fd:00:00:02:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
31	148.103222103	fe:fd:00:00:02:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:01:01
32	148.103222103	192.0.2.1	192.0.2.2	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8483443 Tscr=8483443
33	268.122972598	192.0.2.1	192.0.2.2	ICMP	590	Destination unreachable (Fragmentation needed)
34	268.122972598	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
35	268.123095119	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:01:01
36	388.103905884	192.168.0.2	172.16.1.3	TCP	1514	[TCP Retransmission] 2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8502222 Tscr=8483443
37	388.115447888	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
38	388.115554017	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42	192.0.2.2 is at fe:fd:00:00:04:02
Capturing from SimNet2						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:01:02	Broadcast	ARP	42	Who has 198.51.100.2? Tell 198.51.100.1
2	0.000120496	fe:fd:00:00:02:02	fe:fd:00:00:01:02	ARP	42	198.51.100.2 is at fe:fd:00:00:02:02
3	0.000165578	198.51.100.2	198.51.100.3	TCP	1514	2152 - 12345 [SYN, ACK] Seq=0 Win=0 MSS=1460 SACK_PERM=1 Tsvl=8481905 Tscr=0 WS=2
4	0.001072778	172.16.1.3	192.168.0.2	TCP	94	12345 - 2152 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=8483443 Tscr=8481905 WS=2
5	0.001565472	192.168.0.2	172.16.1.3	TCP	86	2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=1428 Tsvl=8481913 Tscr=8483443
6	5.017351291	fe:fd:00:00:02:02	fe:fd:00:00:01:02	ARP	42	Who has 198.51.100.1? Tell 198.51.100.2
7	5.017494541	fe:fd:00:00:01:02	fe:fd:00:00:02:02	ARP	42	198.51.100.1 is at fe:fd:00:00:01:02
8	39.373744189	fe:80::f0ec:e0ff:fe0.. ff02:2	ICMPv6	70	Router Solicitation from ea:e8:32:9e:5d:9e	
Capturing from SimNet3						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:02:01	Broadcast	ARP	42	Who has 172.16.1.3? Tell 172.16.1.1
2	0.000165568	fe:fd:00:00:03:01	fe:fd:00:00:02:01	ARP	42	172.16.1.3 is at fe:fd:00:00:03:01
3	0.000165568	198.51.100.2	198.51.100.3	TCP	1514	2152 - 12345 [SYN, ACK] Seq=0 Win=0 MSS=1460 SACK_PERM=1 Tsvl=8481905 Tscr=0 WS=2
4	0.000406583	172.16.1.3	192.168.0.2	TCP	74	12345 - 2152 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsvl=8483443 Tscr=8481905 WS=2
5	0.001179547	192.168.0.2	172.16.1.3	TCP	66	2152 - 12345 [ACK] Seq=1 Ack=1 Win=5840 Len=0 Tsvl=8481913 Tscr=8483443
6	39.373251534	fe:80::f0ec:e0ff:fe0.. ff02:2	ICMPv6	70	Router Solicitation from ea:e8:32:9e:5d:9e	

(a) Can you see the 3-way handshake? Did you notice problems with these 3 initial messages?

**Si, no hay ningun problema con el handshake, porque no superan la MTU.**

(b) Did you notice problems with data segments? Why? Which is the difference with the previous ones?

**Si, en la SimNet0 vemos que necesitan paquetes grandes y se necesita fragmentar. Pero ahora el host2 no soluciona el problema porque no le llegan los mensajes ICMP. porque se hemos indicado que las tramas icmp se tiren al llegar al R1.**

(c) Can you see any ICMP message in SimNet1? And in SimNet0?

**Si, en los 2 casos son mensajes ICMP de fragmentation needed porque se envian paquetes superior a la MTU de R1 y RC.**

(d) Was the file transmitted properly? Why?

**No porque los paquetes se pierden, como R1 ignora los mensajes ICMP, al host2 nunca le llegan ack y host2 las retransmite y no termina nunca porque nunca recibe un ack.**

(e) What will happen if instead of the INPUT chain, we use the FORWARD chain in the filtering rule?

**Si usaremos la chain FORWARD (filtra mensajes que tendría que “pasar” más adelante, pero en este caso RC envía directamente a R1) en lugar de la chain INPUT creo que funcionaría, porque realmente R1 no está “pasándole” los mensajes ICMP de RC a host2, sino que en base a los soft state que guarda, el propio R1 genera estos mensajes (pero ahora no tiene el soft state guardado porque rechaza los ICMP antes de procesarlos)**

As you can see, the client is not receiving feedback from the errors of the network due to the filtering rule, so it is unable to adapt the TCP transmission to the conditions of the network. TCP assumes that losses are due to congestion, so it will try to retransmit lost segments just waiting more and more time.

## **0.8.4 Changing the MSS**

the MSS counts only DATA octets in the segment, and it does not count the TCP header or the IP header.

**ip route add ROUTE advmss VALUE**

where ROUTE is the route we want to add (more information using ip route show), and VALUE is the "Advertised MSS" in bytes. In case the route exists, instead of add use change

### **Change the MSS in the host**

1. Delete the kernel routing cache executing the label flushcache.

**//from terminal**

**simctl iptunnel exec flushcache**

2. Put all wiresharks listening traffic in all SimNet interfaces.
3. Identify which are the proper parameters to change the mss properly:
  - Which is the value of the advertised MSS to avoid fragmentation in path?  
Notice that the MTU in SimNet2=996.  
**MSS = 996B (MTUrestrictiva) - 20B (HIPInner) - 20B (HPOuter) - 20B (Htcp) = 936B.**

- Which message of the 3-way handshake of TCP should be change? Why?  
**Hemos de cambiar el SYN/ACK porque es el que contiene el valor de MSS del servidor , que es el que genera problema.**

- If we are changing the MSS in a host, which is the host where we should execute the command?  
**el host3 porque es el que tiene la información del MSS del cliente.**

4. Now that you fully know all the parameters to properly change the MSS, use ip route to change it.

**//from host3**

**ip route add 192.168.0.0/24 via 172.16.1.1 advmss 936**

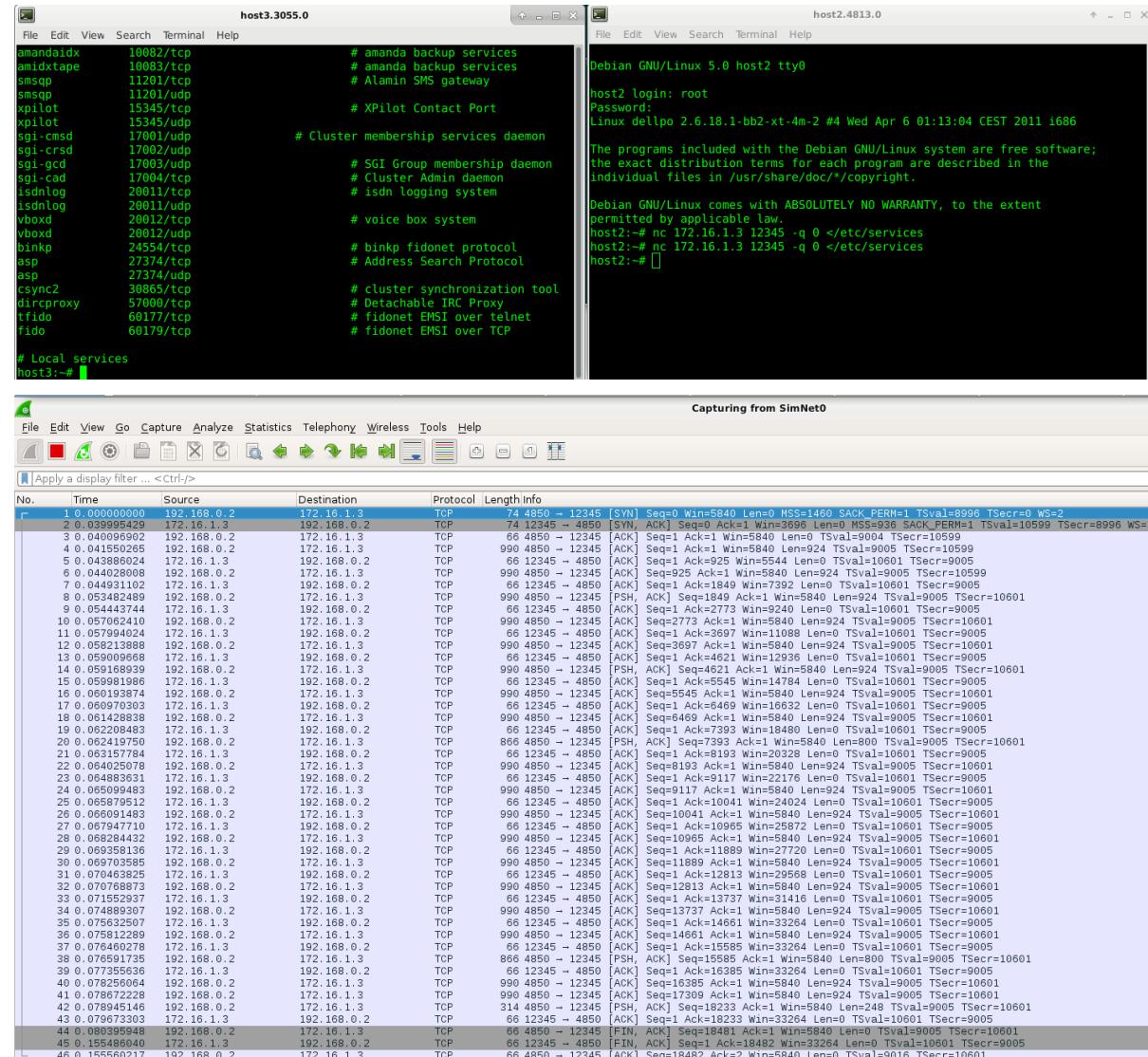
5. Using netcat again, send the file /etc/services from host2 (acting as client) towards host3 (acting as server).

//from host3

```
nc -l -p 12345
```

//from host2

```
nc 172.16.1.3 12345 -q 0 </etc/services
```



en todas las SimNetx vemos este flujo.

Salvo una diferencia, la MSS de SimNet3 es 936, que es lo que hemos cambiado.

(a) Did you notice problems with data segments?

No ha habido ningun problema.

(b) Can you see any ICMP message in SimNet1 and SimNet0?

**No porque no ha habido errores, porque no ha habido errores de transmission.**

(c) Was the file transmitted properly?

**Yes.**

Prior to continue with the following test, delete the route that you configured in the host to change the MSS.

**//from host3**

**ip route delete 192.168.0.0/24 via 172.16.1.1**

Change the MSS in the router

1. Delete the kernel routing cache executing the label flushcache.

**//from terminal**

**simctl iptunnel exec flushcache**

2. Put all wiresharks listening traffic in all SimNet interfaces.

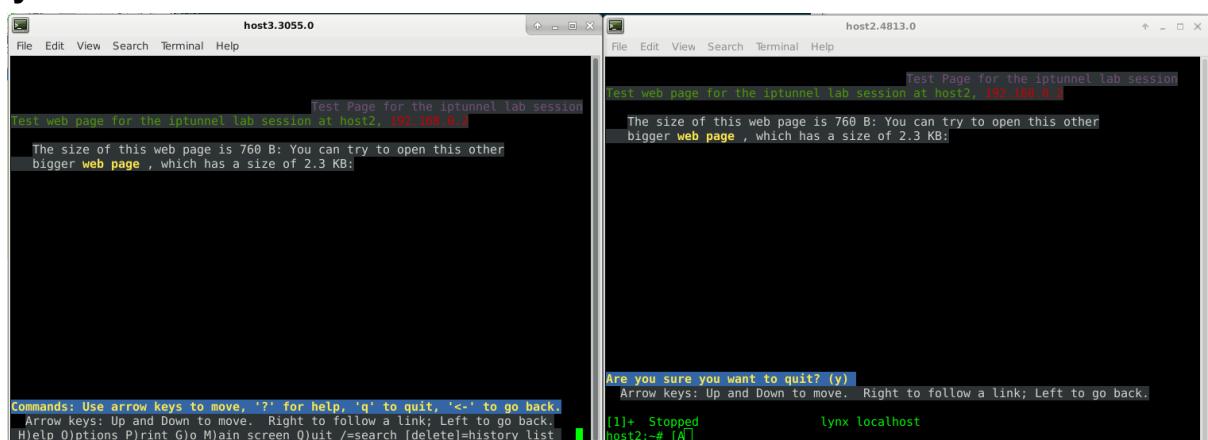
3. Connect to the web server of host2 using lynx from host3:

**//from host2**

**lynx localhost**

**//from host3**

**lynx 192.168.0.2**



Capturing from SimNet0						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	fe80::e434:4cff:fe..	ff02::2	ICMPv6	70	Router Solicitation from e6:34:4c:35:ff:01
2	340.415438102	fe:fd:00:00:04:01	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.1
3	340.415513944	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42	192.168.0.2 is at fe:fd:00:00:05:01
4	340.415513944	fe:fd:00:00:05:01	192.168.0.2	TCP	74	Syn=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeq=105592 TSecr=103999 WS=2
5	340.415649904	192.168.0.2	172.16.1.3	TCP	74	80 - 3124 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSeq=103999 TSecr=103999
6	340.416176809	172.16.1.3	192.168.0.2	TCP	66	3124 - 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeq=105595 TSecr=103999
7	340.437499185	172.16.1.3	192.168.0.2	HTTP	285	GET / HTTP/1.0
8	340.437609118	192.168.0.2	172.16.1.3	TCP	66	80 - 3124 [ACK] Seq=1 Ack=220 Win=6864 Len=0 TSeq=104001 TSecr=105598
9	340.450283656	192.168.0.2	172.16.1.3	HTTP	781	HTTP/1.1 200 OK (text/html)
10	340.450773695	172.16.1.3	192.168.0.2	TCP	66	3124 - 80 [ACK] Seq=220 Ack=716 Win=7270 Len=0 TSeq=105598 TSecr=104001
11	340.451210152	192.168.0.2	172.16.1.3	TCP	66	80 - 3124 [FIN, ACK] Seq=716 Ack=220 Win=6864 Len=0 TSeq=104001 TSecr=105598
12	340.499355113	172.16.1.3	192.168.0.2	TCP	66	3124 - 80 [ACK] Seq=220 Ack=717 Win=7270 Len=0 TSeq=105602 TSecr=104001
13	340.510118949	172.16.1.3	192.168.0.2	TCP	66	3124 - 80 [FIN, ACK] Seq=220 Ack=717 Win=7270 Len=0 TSeq=105605 TSecr=104001
14	340.511343867	192.168.0.2	172.16.1.3	TCP	66	80 - 3124 [ACK] Seq=717 Ack=221 Win=6864 Len=0 TSeq=104008 TSecr=105605

Capturing from SimNet1						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::547d:ddff:fe8... ff02::2		ICMPv6	70	Router Solicitation from 56.7d:dd:8e:d7:ed
2	389.567146562	fe:fd:00:00:01:01	Broadcast	ARP	42	Who has 192.0.2.2? Tell 192.0.2.1
3	389.567262329	fe:fd:00:00:04:02	192.168.0.2	ARP	42	192.0.2.2 is at fe:fd:00:00:04:02
4	389.567277783	172.16.1.3	192.168.0.2	TCP	94	3124 - 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=105592 TSecr=0 WS=2
5	389.568103263	172.16.1.3	192.168.0.2	TCP	94	3124 - 80 [ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=103999 TSecr=105592 WS=2
6	389.568103263	172.16.1.3	192.168.0.2	TCP	86	3124 - 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=105595 TSecr=103999
7	389.589410411	172.16.1.3	192.168.0.2	HTTP	305	GET / HTTP/1.0
8	389.590053053	192.168.0.2	172.16.1.3	TCP	86	80 - 3124 [ACK] Seq=1 Ack=220 Win=6864 Len=0 TSval=104001 TSecr=105598
9	389.602370666	192.168.0.2	172.16.1.3	HTTP	801	HTTP/1.1.200 OK (text/html)
10	389.602701245	172.16.1.3	192.168.0.2	TCP	86	3124 - 80 [ACK] Seq=220 Ack=716 Win=7270 Len=0 TSval=105598 TSecr=104001
11	389.603287570	192.168.0.2	172.16.1.3	TCP	86	80 - 3124 [FIN ACK] Seq=220 Ack=220 Win=6864 Len=0 TSval=104001 TSecr=105598
12	389.651204212	172.16.1.3	192.168.0.2	TCP	86	3124 - 80 [ACK] Seq=220 Ack=717 Win=7270 Len=0 TSval=105602 TSecr=104001
13	389.661967765	172.16.1.3	192.168.0.2	TCP	86	3124 - 80 [FIN, ACK] Seq=220 Ack=717 Win=7270 Len=0 TSval=105605 TSecr=104001
14	389.663496959	192.168.0.2	172.16.1.3	TCP	86	80 - 3124 [ACK] Seq=717 Ack=221 Win=6864 Len=0 TSval=104008 TSecr=105605
15	394.590915991	fe:fd:00:00:04:02	fe:fd:00:00:01:01	ARP	42	Who has 192.0.2.1? Tell 192.0.2.2
16	394.591219216	fe:fd:00:00:01:01	fe:fd:00:00:04:02	ARP	42	192.0.2.1 is at fe:fd:00:00:01:01

Capturing from SimNet2						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::cc39:8aff:fe8... ff02::2		ICMPv6	70	Router Solicitation from ce:39:84:98:fe:1d
2	373.170926602	fe:fd:00:00:02:02	Broadcast	ARP	42	Who has 198.51.100.1? Tell 198.51.100.2
3	373.171087230	fe:fd:00:00:01:02	192.168.0.2	ARP	42	198.51.100.1 is at fe:fd:00:00:01:02
4	373.171087230	172.16.1.3	192.168.0.2	TCP	94	3124 - 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=105592 TSecr=0 WS=2
5	373.183799539	182.168.0.2	172.16.1.3	TCP	94	80 - 3124 [SYN, ACK] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=103999 TSecr=105592 WS=2
6	373.184056673	172.16.1.3	192.168.0.2	TCP	86	3124 - 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=105595 TSecr=103999
7	373.205364970	172.16.1.3	192.168.0.2	HTTP	305	GET / HTTP/1.0
8	373.206125437	192.168.0.2	172.16.1.3	TCP	86	80 - 3124 [ACK] Seq=1 Ack=220 Win=6864 Len=0 TSval=104001 TSecr=105598
9	373.218634189	192.168.0.2	172.16.1.3	HTTP	801	HTTP/1.1.200 OK (text/html)
10	373.218635310	172.16.1.3	192.168.0.2	TCP	86	3124 - 80 [ACK] Seq=220 Ack=716 Win=7270 Len=0 TSval=105598 TSecr=104001
11	373.219347081	192.168.0.2	172.16.1.3	TCP	86	80 - 3124 [FIN ACK] Seq=716 Ack=220 Win=6864 Len=0 TSval=104001 TSecr=105598
12	373.267099600	172.16.1.3	192.168.0.2	TCP	86	3124 - 80 [ACK] Seq=220 Ack=717 Win=7270 Len=0 TSval=105602 TSecr=104001
13	373.277605777	172.16.1.3	192.168.0.2	TCP	86	3124 - 80 [FIN, ACK] Seq=716 Ack=717 Win=7270 Len=0 TSval=105605 TSecr=104001
14	373.2798605184	192.168.0.2	172.16.1.3	TCP	86	80 - 3124 [ACK] Seq=717 Ack=221 Win=6864 Len=0 TSval=104008 TSecr=105605
15	378.181111837	fe:fd:00:00:01:02	fe:fd:00:00:02:02	ARP	42	Who has 198.51.100.2? Tell 198.51.100.1
16	378.191300864	fe:fd:00:00:02:02	fe:fd:00:00:01:02	ARP	42	198.51.100.2 is at fe:fd:00:00:02:02

Capturing from SimNet3						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::b45b:7dff:fe8... ff02::2		ICMPv6	70	Router Solicitation from b6:5b:7d:f2:ce:dc
2	405.938465332	fe:fd:00:00:03:01	Broadcast	ARP	42	Who has 172.16.1.1? Tell 172.16.1.3
3	405.938465332	fe:fd:00:00:02:01	fe:fd:00:00:03:01	ARP	42	172.16.1.1 is at fe:fd:00:00:02:01
4	405.938806193	172.16.1.3	192.168.0.2	TCP	74	3124 - 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=105592 TSecr=0 WS=2
5	405.951891221	192.168.0.2	172.16.1.3	TCP	74	80 - 3124 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=103999 TSecr=105592 WS=2
6	405.951979438	172.16.1.3	192.168.0.2	TCP	66	3124 - 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=105595 TSecr=103999
7	405.973268131	172.16.1.3	192.168.0.2	HTTP	285	GET / HTTP/1.0
8	405.984316026	192.168.0.2	172.16.1.3	TCP	66	80 - 3124 [ACK] Seq=1 Ack=220 Win=6864 Len=0 TSval=104001 TSecr=105598
9	405.986514329	192.168.0.2	172.16.1.3	HTTP	781	HTTP/1.1.200 OK (text/html)
10	405.986564684	172.16.1.3	192.168.0.2	TCP	66	3124 - 80 [ACK] Seq=220 Ack=716 Win=7270 Len=0 TSval=105598 TSecr=104001
11	405.987420269	192.168.0.2	172.16.1.3	TCP	66	80 - 3124 [FIN ACK] Seq=716 Ack=220 Win=6864 Len=0 TSval=104001 TSecr=105598
12	405.987420269	172.16.1.3	192.168.0.2	TCP	66	3124 - 80 [ACK] Seq=717 Ack=717 Win=7270 Len=0 TSval=105602 TSecr=104001
13	406.045664011	172.16.1.3	192.168.0.2	TCP	66	3124 - 80 [FIN, ACK] Seq=716 Ack=717 Win=7270 Len=0 TSval=105605 TSecr=104001
14	406.047747686	192.168.0.2	172.16.1.3	TCP	66	80 - 3124 [ACK] Seq=717 Ack=221 Win=6864 Len=0 TSval=104008 TSecr=105605
15	410.074794156	fe:fd:00:00:02:01	fe:fd:00:00:03:01	ARP	42	Who has 172.16.1.3? Tell 172.16.1.1
16	410.075192631	fe:fd:00:00:03:01	fe:fd:00:00:02:01	ARP	42	172.16.1.3 is at fe:fd:00:00:03:01

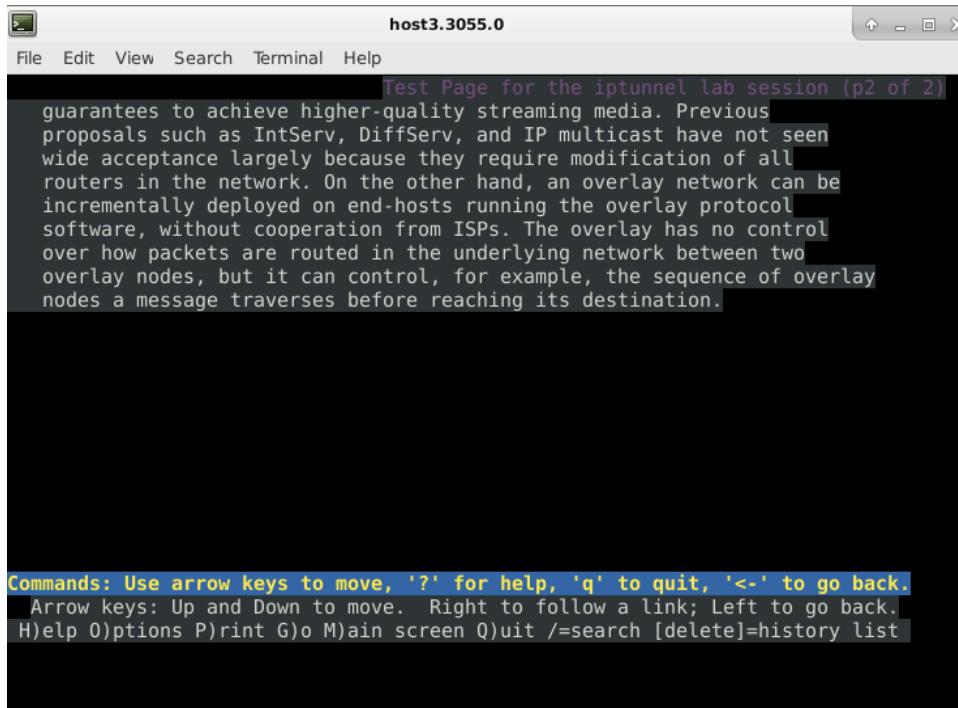
(a) Can you see the main web page of host2?

**Si**

(b) Can you see any error message in the wiresharks?

**No**

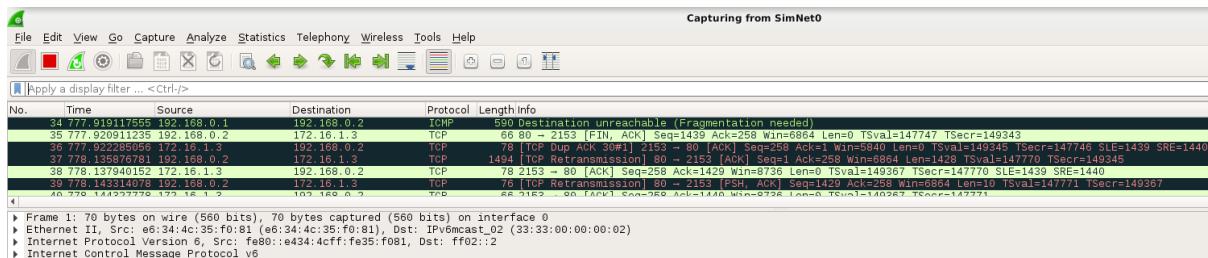
As you can see there is no problem to see the main web page of this host. However, browse the web in order to see the other local web page:



(a) Did you noticed any error?

**Si, podemos ver que no carga la segunda parte.**

(b) What do you see in the wiresharks?



Ahora vemos que hay mensajes ICMPs, enviado por R1 al host2.

Retransmisiones enviadas por host2 al host3.

Tambien tenemos Ack's, duplicados.

El problema es similar al de hace dos apartados, habría que fragmentar pero R1 descarta los mensajes ICMP así que host2 no sabe que tiene que fragmentar.

(c) Why do you think that the main web page is working, but the second one cannot be downloaded?

Por el tamaño de las paginas. La principal no tiene muchos datos (es mas ligera) que la pagina siguiente.(se puede ver en la length de los paquetes.)

(d) Try to solve the problem by changing the MSS in R2 using the MANGLE table of iptables. Remember that you have to change the MSS in the proper message of the 3-way handshake.

**el cambio de mms se hace como en el ejercicio anterior, pero ahora el cliente es el host3 .**

**(ya ta hecho)**

//from R2

**iptables -t mangle -A FORWARD -o tunnel0 -p tcp --syn -j TCPMSS --set-mss 936**

Capturing from SimNet0						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:04:01	Broadcast	ARP	42	who has 192.168.0.2? Tell 192.168.0.1
2	0.000135618	fe:fd:00:00:05:01	fe:fd:00:00:04:01	ARP	42	192.168.0.2 is at fe:fd:00:00:05:01
3	0.000135618	192.168.0.2	192.168.0.2	TCP	42	Syn=5792 Win=5820 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=936 SACK_PERM=1 TSeqval=396415 TSeqcr=0 WS=2
4	0.000403274	192.168.0.2	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeqval=396418 TSeqcr=394822
5	0.001374771	172.16.1.3	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSeqval=396418 TSeqcr=394822
6	0.023718592	172.16.1.3	192.168.0.2	HTTP	285	GET / HTTP/1.0
7	0.023958336	192.168.0.2	172.16.1.3	TCP	66	80 - 3968 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=936 SACK_PERM=1 TSeqval=396425 TSeqcr=396422
8	0.023958336	192.168.0.2	172.16.1.3	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSeqval=396425 TSeqcr=394825
9	0.023228576	192.168.0.2	172.16.1.3	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSeqval=396425 TSeqcr=394825
10	0.033521134	192.168.0.2	172.16.1.3	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSeqval=396425 TSeqcr=394825
11	0.075203403	172.16.1.3	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSeqval=396425 TSeqcr=394825
12	0.098976225	172.16.1.3	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSeqval=396425 TSeqcr=394825
13	0.098976225	192.168.0.2	172.16.1.3	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSeqval=396425 TSeqcr=394825
14	0.0989761713	172.16.1.3	192.168.0.2	TCP	74	3968 - 80 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=936 SACK_PERM=1 TSeqval=396425 TSeqcr=394825
15	14.4632981023	192.168.0.2	172.16.1.3	TCP	74	80 - 3969 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=936 SACK_PERM=1 TSeqval=396425 TSeqcr=394825
16	14.4632981023	172.16.1.3	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSeqval=396425 TSeqcr=394825
17	14.4632981023	192.168.0.2	172.16.1.3	HTTP	233	GET /big.html HTTP/1.0
18	14.4632981023	192.168.0.2	172.16.1.3	TCP	66	3969 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 TSeqval=397866 [TCP segment of a reassembled PDU]
19	14.4632981023	192.168.0.2	172.16.1.3	TCP	996	80 - 3969 [ACK] Seq=220 Ack=717 Win=7270 Len=0 MSS=936 SACK_PERM=1 TSeqval=396426 TSeqcr=394825
20	14.4632981023	192.168.0.2	172.16.1.3	TCP	66	3969 - 80 [ACK] Seq=220 Ack=717 Win=7270 Len=0 MSS=936 SACK_PERM=1 TSeqval=396426 TSeqcr=394825
21	14.495300198	192.168.0.2	172.16.1.3	HTTP	580	HTTP/1.1 200 OK
22	14.495913974	172.16.1.3	192.168.0.2	TCP	66	3969 - 80 [ACK] Seq=258 Ack=1439 Win=9536 Len=0 TSeqval=397866 TSeqcr=396268
23	14.495913974	192.168.0.2	172.16.1.3	TCP	66	80 - 3969 [FIN, ACK] Seq=1439 Ack=258 Win=6864 Len=0 TSeqval=396270 TSeqcr=397868
24	14.5049783491	172.16.1.3	192.168.0.2	TCP	66	3969 - 80 [ACK] Seq=258 Ack=1440 Win=9536 Len=0 TSeqval=397873 TSeqcr=396270
25	14.5049783491	172.16.1.3	192.168.0.2	TCP	66	3969 - 80 [FIN, ACK] Seq=258 Ack=1440 Win=9536 Len=0 TSeqval=397874 TSeqcr=396270
26	14.506012557	192.168.0.2	172.16.1.3	TCP	66	3969 - 80 [ACK] Seq=1440 Ack=259 Win=6864 Len=0 TSeqval=396278 TSeqcr=397874

**Ahora, no hay retransmisiones**

**En todas las SimNetx vemos este flujo. Salvo una diferencia, en SimNet3 MMS es 1452.**

Capturing from SimNet3						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe:fd:00:00:03:01	Broadcast	ARP	42	who has 172.16.1.1? Tell 172.16.1.3
2	0.000263201	fe:fd:00:00:02:01	fe:fd:00:00:03:01	ARP	42	172.16.1.1 is at fe:fd:00:00:02:01
3	0.000374901	172.16.1.3	192.168.0.2	TCP	74	3968 - 80 [SYN, ACK] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=396415 TSeqcr=0 WS=2
4	0.018646401	172.16.1.3	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=936 SACK_PERM=1 TSeqval=396418 TSeqcr=394822
5	0.018646401	172.16.1.3	192.168.0.2	HTTP	285	GET / HTTP/1.0
6	0.021626444	172.16.1.3	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=936 SACK_PERM=1 TSeqval=396425 TSeqcr=394825
7	0.043519015	192.168.0.2	172.16.1.3	TCP	66	80 - 3969 [SYN, ACK] Seq=1 Ack=220 Win=6864 Len=0 TSeqval=394825 TSeqcr=396422
8	0.051707395	192.168.0.2	172.16.1.3	HTTP	781	HTTP/1.1 200 OK
9	0.051786508	172.16.1.3	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=220 Ack=716 Win=7270 Len=0 TSeqval=396422 TSeqcr=394825
10	0.052816881	192.168.0.2	172.16.1.3	TCP	66	80 - 3969 [FIN, ACK] Seq=1439 Ack=220 Win=6864 Len=0 TSeqval=394825 TSeqcr=396422
11	0.053591813	172.16.1.3	192.168.0.2	TCP	66	3968 - 80 [ACK] Seq=220 Ack=717 Win=7270 Len=0 TSeqval=396426 TSeqcr=394826
12	0.118455597	192.168.0.2	172.16.1.3	TCP	66	3968 - 80 [ACK] Seq=1440 Ack=221 Win=6864 Len=0 TSeqval=396429 TSeqcr=394825
13	0.118455597	192.168.0.2	172.16.1.3	TCP	66	80 - 3968 [ACK] Seq=1440 Ack=221 Win=6864 Len=0 TSeqval=396429 TSeqcr=394825
14	0.024720764	fe:fd:00:00:02:01	fe:fd:00:00:03:01	ARP	42	Who has 172.16.1.3? Tell 172.16.1.1
15	0.024830936	fe:fd:00:00:03:01	fe:fd:00:00:02:01	ARP	42	172.16.1.3 is at fe:fd:00:00:02:01
16	14.482274947	172.16.1.3	192.168.0.2	TCP	74	3969 - 80 [SYN, ACK] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSeqval=397866 TSeqcr=0 WS=2
17	14.483188653	192.168.0.2	172.16.1.3	TCP	74	80 - 3969 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSeqval=396268 TSeqcr=397866 WS=2
18	14.504373312	172.16.1.3	192.168.0.2	HTTP	323	GET /big.html HTTP/1.0
20	14.511810102	192.168.0.2	172.16.1.3	TCP	66	80 - 3969 [ACK] Seq=1439 Ack=258 Win=6864 Len=0 TSeqval=396270 TSeqcr=397868
21	14.513377786	192.168.0.2	172.16.1.3	TCP	990	80 - 3969 [ACK] Seq=1 Ack=258 Win=6864 Len=0 TSeqval=396270 TSeqcr=397868 [TCP segment of a reassembled PDU]
22	14.513631434	172.16.1.3	192.168.0.2	TCP	66	3969 - 80 [ACK] Seq=258 Ack=259 Win=6864 Len=0 TSeqval=396270 TSeqcr=397868
23	14.5146466770	192.168.0.2	172.16.1.3	HTTP	580	HTTP/1.1 200 OK
24	14.514653933	172.16.1.3	192.168.0.2	TCP	66	3969 - 80 [ACK] Seq=258 Ack=259 Win=6864 Len=0 TSeqval=396270 TSeqcr=397868
25	14.515213567	192.168.0.2	172.16.1.3	TCP	66	80 - 3969 [SYN, ACK] Seq=1440 Ack=1440 Win=9536 Len=0 TSeqval=397873 TSeqcr=396270
26	14.516304337	172.16.1.3	192.168.0.2	TCP	66	3969 - 80 [ACK] Seq=258 Ack=259 Win=1440 Win=9536 Len=0 TSeqval=397874 TSeqcr=396270
27	14.569953899	172.16.1.3	192.168.0.2	TCP	66	3969 - 80 [FIN, ACK] Seq=1440 Ack=259 Win=1440 Win=9536 Len=0 TSeqval=397874 TSeqcr=396270

We hope that all these experiments helped you to understand how complicated is to solve problems of communication networks when using tunnels, even in the case of using the most simplistic IPIP tunnel. In following lab sessions, maybe you will be asked to create GRE tunnels, so try to remember all these concepts.