

Práctica 2: Formato del datagrama IP y configuración de direcciones IP

1. Campos de la cabecera IP

1- El origen del paquete es 101.0.0.1 y el destino es 103.0.0.2

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	101.0.0.1	103.0.0.2	ICMP	98	Echo (ping) request id=1

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: 2a:c7:f0:1c:03:3a (2a:c7:f0:1c:03:3a), Dst: 5a:3a:7d:81:6d:2b (5a:3a:7d:81:6d:2b)
 Destination: 5a:3a:7d:81:6d:2b (5a:3a:7d:81:6d:2b)
 Source: 2a:c7:f0:1c:03:3a (2a:c7:f0:1c:03:3a)
 Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 101.0.0.1, Dst: 103.0.0.2
Internet Control Message Protocol

2- La maquinas están conectadas a un router ya que tienen diferente dirección: 101 y 103

3- EL TTL (time to live) es de 62

4- Con el valor TTL podemos saber cuántos routers atraviesan ya que cada router vale como una unidad, y sabiendo que el TTL se inicializa con un valor de 64 y pone 62, sabemos que atraviesan dos routers.

```
Internet Protocol Version 4, Src: 101.0.0.1, Dst: 103.0.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCH: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0000 (0)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
    Header checksum: 0x70a6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 101.0.0.1
    Destination: 103.0.0.2
```

El Apartado TTL se encuentra en el protocolo IP

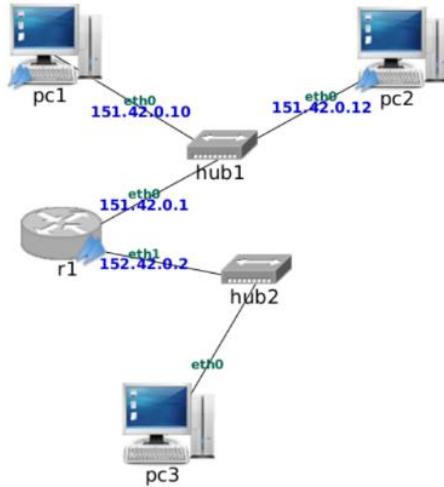
2. Configuración de direcciones IP

2.1. El comando ifconfig/ip

1- Todos los pcs tienen la misma dirección (Local loopback), la misma mascara de red y también el mismo inet addr.

```
pc1 login: root (automatic login)
Last login: Sat Mar 12 16:49:17 UTC 2022 on ttys1
pc1:~# ifconfig
lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:2 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:100 (100.0 B)  TX bytes:100 (100.0 B)
```

- 2- Direcciones ip configuradas mediante comando ifconfig eth0 11.0.0.1 netmask 255.255.255.0. Una vez que apagas un pc o un router su dirección asignada se pierde (La captura muestra que apago el router y lo vuelvo a arrancar, de forma que se pierde la dirección).



Explicación de las capturas:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	26:f7:9a:6d:f8:65	Broadcast	ARP	42	Who has 151.42.0.12? Tell 151.42.0.10
2	0.000268	c6:51:85:6a:72:36	26:f7:9a:6d:f8:65	ARP	42	151.42.0.12 is at c6:51:85:6a:72:36
3	0.000168	151.42.0.10	151.42.0.12	ICMP	98	Echo (ping) request id=0x0702, seq=1/256,
4	0.000218	151.42.0.12	151.42.0.10	ICMP	98	Echo (ping) reply id=0x0702, seq=1/256,

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 ▶ Ethernet II, Src: 26:f7:9a:6d:f8:65 (26:f7:9a:6d:f8:65), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)

Tras realizar el ping -c 1 de pc1 a pc2 se obtienen 2 tramas de tipo ICMP que son los mensajes enviados. Una trama de envío del pc1, otra de respuesta del pc2.

Podemos ver dos tramas con valor ARP que corresponden a averiguar la dirección del pc al que se le envía al ping. El primer arp nos muestra quien pregunta y quien responde y la segunda trama arp corresponde con la respuesta y se muestra la dirección Ethernet correspondiente.

Las dos primeras tramas no tienen protocolo IP

Trama 1: Origen Ethernet -26:f7:9a:6a:f8:65 Destino Ethernet- Broadcast (El destino broadcast es debido a que cualquier ordenador puede responder al arp que pregunta por la dirección)

Trama 2: Origen Ethernet- c6:51:85:6a:72:36 (es el pc que necesitamos saber para el ping) Destino Ethernet - 26:f7:9a:6d:f8:65 (es el pc que responde al arp)

Trama 3: Pestaña Ethernet y Pestaña IP con sus correspondientes direcciones. (IPv4 0x800)

3	0.000168	151.42.0.10	151.42.0.12	ICMP	98 Echo (ping) request id=
4	0.000218	151.42.0.12	151.42.0.10	ICMP	98 Echo (ping) reply id=

Trama 4: Pestaña Ethernet y Pestaña IP con sus correspondientes direcciones. (IPv4 0x800)

1	4	0.000218	151.42.0.12	151.42.0.10	ICMP	98 Echo (ping) reply id=0

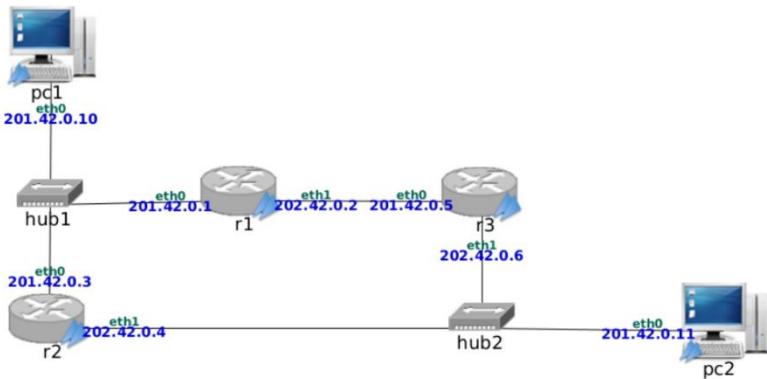
2.2. El fichero /etc/network/interfaces

1- Hay tres redes distintas, la primera es la que une el pc1, hub1, r1 y r2. La segunda une hub2, pc2, r2 y r3. Y la última une r3 y r1.

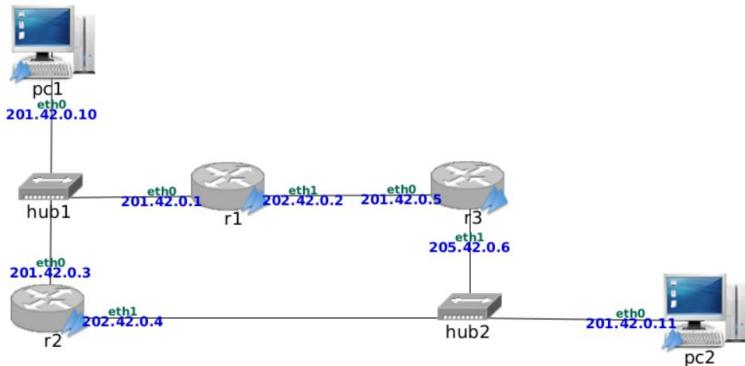
2- Comandos útiles para interfaces de dispositivos:

- **Para hacer a la interfaz del dispositivo:**
nano /etc/network/interfaces
- **Una vez añadidas o cambiado lo necesario, se asienta esa información con:**
/etc/init.d/networking restart
- **Para acceder al manual de interfaces:**
man interfaces
- **Para hacer caer esa dirección modificada usamos stop, y para volver a arrancarla usamos start.**
/etc/init.d/networking stop
/etc/init.d/networking start

Direcciones cambiadas ya mediante nano



Para modificar la dirección IP de r3 (eth1) debemos cambiarle todos los números de la red, el último número pertenece al router por lo que no es tan importante.



Ejemplo del r3 una vez modificado la interfaz y las direcciones de un router, tras realizarle /etc/init.d/networking restart y comprobar que si se han producido esos cambios con ifconfig.

```
r3:~# ifconfig
eth0      Link encap:Ethernet HWaddr 4e:96:50:ba:ed:51
          inet addr:201.42.0.5 Bcast:201.42.0.255 Mask:255.255.255.0
          inet6 addr: fe80::4c96:50ff:feba:ed51/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:384 (384.0 B) TX bytes:238 (238.0 B)
          Interrupt:5

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:200 (200.0 B) TX bytes:200 (200.0 B)

r3:~# /etc/init.d/networking restart
Reconfiguring network interfaces...
```

```
eth1      Link encap:Ethernet HWaddr f6:0c:9c:50:d4:b8
          inet addr:202.42.0.6 Bcast:202.42.0.255 Mask:255.255.255.0
          inet6 addr: fe80::f40c:9cff:fe50:d4b8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:768 (768.0 B) TX bytes:328 (328.0 B)
          Interrupt:5

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:500 (500.0 B) TX bytes:500 (500.0 B)
```

- Si usas el comando de stop para tirar abajo una dirección que anteriormente ha sido guardada mediante nano, una vez que la vuelvas a arrancar con el comando de start, las direcciones guardadas anteriormente se quedarán guardadas.

9- La captura obtiene 8 tramas, 4 de tipo ARP y otras 4 de tipo ICMP.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	e6:2f:4c:5c:35:17	Broadcast	ARP	42	Who has 201.42.0.1? Tell 201.42.0.10
2	0.000076	02:00:91:6c:9d:af	e6:2f:4c:5c:35:17	ARP	42	201.42.0.1 is at 02:00:91:6c:9d:af
3	0.000098	201.42.0.10	201.42.0.1	ICMP	98	Echo (ping) request id=0x2303, seq=1/256,
4	0.000116	201.42.0.1	201.42.0.10	ICMP	98	Echo (ping) reply id=0x2303, seq=1/256,
5	0.992246	201.42.0.10	201.42.0.1	ICMP	98	Echo (ping) request id=0x2303, seq=2/512,
6	0.992465	201.42.0.1	201.42.0.10	ICMP	98	Echo (ping) reply id=0x2303, seq=2/512,
7	4.989508	02:00:91:6c:9d:af	e6:2f:4c:5c:35:17	ARP	42	Who has 201.42.0.10? Tell 201.42.0.1
8	4.989760	e6:2f:4c:5c:35:17	02:00:91:6c:9d:af	ARP	42	201.42.0.10 is at e6:2f:4c:5c:35:17

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 ▶ Ethernet II, Src: e6:2f:4c:5c:35:17 (e6:2f:4c:5c:35:17), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)

Al realizar un ping -c 2 podemos encontrar 4 tramas ICMP que son los mensajes se envían y responden (reply y request). Mientras que los arp son los mensajes q un dispositivo envía a otro para poder saber su dirección y de esta forma en enviar el arping o ping.

Es decir, si un ordenador quiere enviar un ping a otro pc sin saber su dirección, primero debe saber esta dirección por lo que en la captura de las tramas saldría un arp correspondiente al ordenador que intenta averiguar la dirección del otro.

Protocol	Length	Info
ARP	42	Who has 201.42.0.1? Tell 201.42.0.10
ARP	42	201.42.0.1 is at 02:00:91:6c:9d:af
ICMP	98	Echo (ping) request id=0x2303, seq=1/256,
ICMP	98	Echo (ping) reply id=0x2303, seq=1/256,
ICMP	98	Echo (ping) request id=0x2303, seq=2/512,
ICMP	98	Echo (ping) reply id=0x2303, seq=2/512,
ARP	42	Who has 201.42.0.10? Tell 201.42.0.1
ARP	42	201.42.0.10 is at e6:2f:4c:5c:35:17

Who has es el ordenador por el que se pregunta y tell es el ordenador que pregunta sobre la dirección de dicho pc. La línea de abajo corresponde con que ese pc responde con la dirección Ethernet del pc preguntado anteriormente.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	e6:2f:4c:5c:35:17	Broadcast	ARP	42	Who has 201.42.0.1? Tell 201.42.0.10
2	0.000076	02:00:91:6c:9d:af	e6:2f:4c:5c:35:17	ARP	42	201.42.0.1 is at 02:00:91:6c:9d:af
3	0.000098	201.42.0.10	201.42.0.1	ICMP	98	Echo (ping) request id=0x2303, seq=1/256,
4	0.000116	201.42.0.1	201.42.0.10	ICMP	98	Echo (ping) reply id=0x2303, seq=1/256,
5	0.992246	201.42.0.10	201.42.0.1	ICMP	98	Echo (ping) request id=0x2303, seq=2/512,
6	0.992465	201.42.0.1	201.42.0.10	ICMP	98	Echo (ping) reply id=0x2303, seq=2/512,
7	4.989508	02:00:91:6c:9d:af	e6:2f:4c:5c:35:17	ARP	42	Who has 201.42.0.10? Tell 201.42.0.1
8	4.989760	e6:2f:4c:5c:35:17	02:00:91:6c:9d:af	ARP	42	201.42.0.10 is at e6:2f:4c:5c:35:17

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 ▶ Ethernet II, Src: e6:2f:4c:5c:35:17 (e6:2f:4c:5c:35:17), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)

Tenemos un pc y un router que son las encargadas de las diferentes tramas.

La dirección IP del pc es 201.42.0.10 y su dirección Ethernet es e6:2f:4c:5c:35:17.

La dirección IP del router es 201.42.0.1 y su dirección Ethernet es 02:00:91:6c:9d:af

Con saber esa información podemos ver cuál es el origen de cada trama y su respectiva dirección.

10- Si realizamos el ping del pc1 (eth0) a la dirección eth1 de r1, los paquetes hacen el intento de enviarse, pero como podemos observar pone que hay 0 recibidos y dos errores.

```
pc1:~# ping -c 2 201.42.0.2
PING 201.42.0.2 (201.42.0.2) 56(84) bytes of data.
From 201.42.0.10 icmp_seq=1 Destination Host Unreachable
From 201.42.0.10 icmp_seq=2 Destination Host Unreachable

--- 201.42.0.2 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1002ms
, pipe 2
pc1:~#
```

3. Fragmentación IP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	101.0.0.1	103.0.0.2	ICMP	1514	Echo (ping) request id=0xf314, seq=1/256, ttl=62 (no respons...
2	0.000096	101.0.0.1	103.0.0.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6e0a)
3	0.000161	101.0.0.1	103.0.0.2	IPv4	1082	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=6e0a)

Frame 3: 1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits)
Ethernet II, Src: 2a:c7:f0:1c:03:3a (2a:c7:f0:1c:03:3a), Dst: 5a:3a:7d:81:6d:2b (5a:3a:7d:81:6d:2b)
Internet Protocol Version 4, Src: 101.0.0.1, Dst: 103.0.0.2
Data (1048 bytes)

- 1- Si la dirección IP es la misma para ellos, en este caso si lo es por lo que pertenecen al mismo datagrama original.

No.	Time	Source	Destination
1	0.000000	101.0.0.1	103.0.0.2
2	0.000096	101.0.0.1	103.0.0.2
3	0.000161	101.0.0.1	103.0.0.2

- 2- Cada trama lleva 1500 bytes de datos del datagrama original.

Como el datagrama original supera la cantidad total de bytes (1500) se fragmenta en dos tramas de Ethernet (1500 bytes más 14 de origen, destino y protocolo, CRC no está contado). Así que las tramas 2 y 3 no podrían llevar más datos.

- 3- El datagrama original estaría formado por $1500 + (1082 - 14) = 2566$ (Los fragmentados), si sumamos las tres tramas seria $1500 + 1500 + 1068 = 4068$

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	101.0.0.1	103.0.0.2	ICMP	1514	Echo (ping) request id=0xf314, seq=1/256, ttl=62 (no response found!)
2	0.000096	101.0.0.1	103.0.0.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6e0a)
3	0.000161	101.0.0.1	103.0.0.2	IPv4	1082	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=6e0a)

Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: 2a:c7:f0:1c:03:3a (2a:c7:f0:1c:03:3a), Dst: 5a:3a:7d:81:6d:2b (5a:3a:7d:81:6d:2b)
Internet Protocol Version 4, Src: 101.0.0.1, Dst: 103.0.0.2
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x6e0a (28170)
Flags: 0x2000, More fragments
Time to live: 62
Protocol: ICMP (1)
Header checksum: 0x1d14 [validation disabled]
[Header checksum status: Unverified]
Source: 101.0.0.1
Destination: 103.0.0.2

Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xc6ef [unverified] [fragmented datagram]
[Checksum Status: Unverified]
Identifier (BE): 62228 (0xf314)
Identifier (LE): 5363 (0x14f3)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[No response seen]
Timestamp from icmp data: Feb 24, 2014 18:42:54.679305000 CET
[Timestamp from icmp data (relative): 0.000509000 seconds]
Data (1464 bytes)

Data (1464 bytes) -Esos datos son el contenido del mensaje ICMP, que en este caso está formado por 16 de cabecera del mensaje ICMP y 1464 de los datos del mensaje ICMP.

- 4- Si el datagrama se desordenase, se podría unificar y ordenar observando el identificador y el offset (número de bytes que lleva cada trama sumando la anterior, primero 1480, luego 2960 y así sucesivamente) del datagrama y de esta forma podría ordenarlo.
- 5- Lo sabemos porque pertenece al mismo identificador de datagrama (ID=6e0a)

Protocol	Length	Info
ICMP	1514	Echo (ping) request id=0xf314, seq=1/256, ttl=62 (no respons...
IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6e0a)
IPv4	1082	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=6e0a)

- 6- Porque al ser fragmentado pertenece al nivel Ethernet y al protocolo IPv4.
- 7- Una vez cambiada la opción de wireshark, los datos siguen siendo los mismos, pero vemos que la forma de mostrarlos es diferente.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	101.0.0.1	103.0.0.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0)
2	0.000096	101.0.0.1	103.0.0.2	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480)
3	0.000161	101.0.0.1	103.0.0.2	ICMP	1082	Echo (ping) request id=0xf314, seq=1/256,

```

Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: 2a:c7:f0:1c:03:3a (2a:c7:f0:1c:03:3a), Dst: 5a:3a:7d:81:6d:2b (5a:3a:7d:81:6d:2b)
Internet Protocol Version 4, Src: 101.0.0.1, Dst: 103.0.0.2
Data (1480 bytes)

```

Podemos ver que identifica al primer paquete como fragmento, y también el segundo, pero no lo marca en el último. Wireshark señala en el primer y segundo paquete que ha reensamblado los 3 fragmentos en el tercer paquete.

En el tercer paquete se mantiene la cabecera tal y como es, pero se detalla (al final de la cabecera IP) los campos de los 3 fragmentos: [3 IPv4 Fragments (4008 bytes): #1(1480), #2(1480), #3(1048)]. También se incluye en la parte de datos los datos agregados de los 3 fragmentos.

IMPORTANTE: Si en la captura una vez activada la opción de fragmentar no sale el offset (número de fragmentos), eso quiere decir que son tres datagramas diferentes, aunque tengan el mismo identificador de datagrama.

Origen: Si un switch tiene x direcciones aprendidas, solo aprende las direcciones de las tramas que se le envían con dirección origen y no destinó.

Si esa trama origen la tenía aprendida se reinicia su contador.

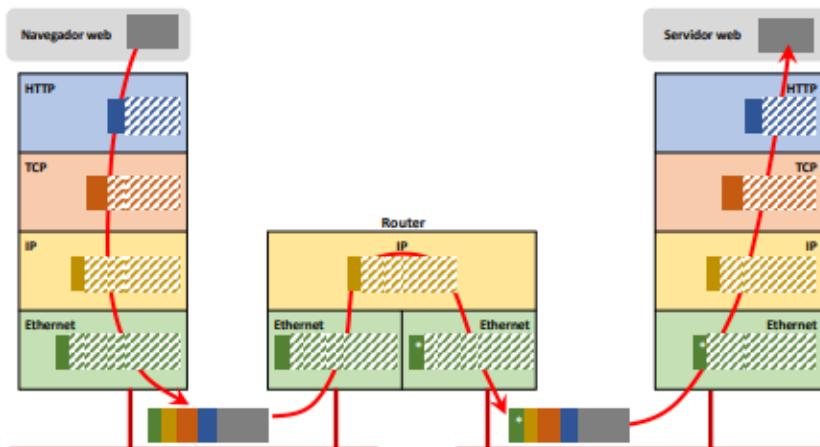
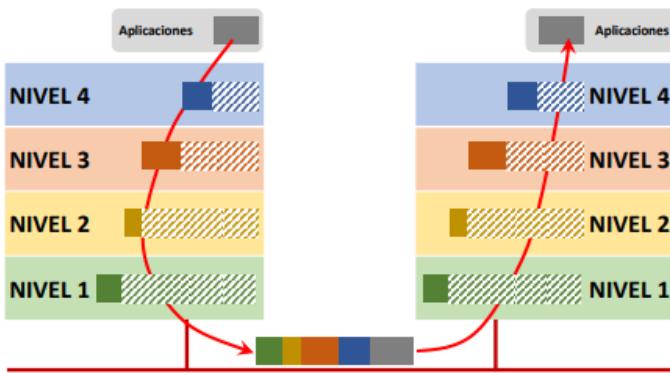
Si esa trama origen no la tenía aprendida, la aprende.

Destino: Si el destino de la trama que le llega no la tenía aprendida o es una dirección broadcast, la dirección que se coge para reenviar la trama es todas menos por donde ha llegado.

Si el destino de la trama que le llega si la tenía aprendida, se reenviara por el ethX de esa trama destino que ya tenía aprendida.

tipo	código	descripción
0	0	respuesta de eco
3	0	destino inalcanzable: red inalcanzable
3	1	destino inalcanzable: máquina inalcanzable
3	3	destino inalcanzable: puerto inalcanzable
8	0	solicitud de eco
11	0	tiempo excedido: TTL = 0
12	1	cabecera IP incorrecta: falta una opción
13	0	solicitud de marca de tiempo
14	0	respuesta de marca de tiempo

Mensajes informativos	
0	no se puede llegar a la red
1	no se puede llegar al host o aplicación de destino
2	el destino no dispone del protocolo solicitado
3	no se puede llegar al puerto destino o la aplicación destino no está libre
4	se necesita aplicar fragmentación, pero el flag correspondiente indica lo contrario
5	la ruta de origen no es correcta
6	no se conoce la red destino
7	no se conoce el host destino
8	el host origen está aislado
9	la comunicación con la red destino está prohibida por razones administrativas
10	la comunicación con el host destino está prohibida por razones administrativas
11	no se puede llegar a la red destino debido al Tipo de servicio
12	no se puede llegar al host destino debido al Tipo de servicio



Deber ir del nivel más bajo al más alto (red, trans, aplicación)

- **1** De red de x a aplicación de x (de red a aplicación)
- **2** Del nivel anterior hacia ese primer nivel que aparece (de enlace a red)
- En el router la 2 no puede ser de red a transporte porque no hay transporte y tampoco de transporte a aplicación, pero si puede ser de enlace a red.

Si es directamente a la red o al enlace, debe tener todo a partir de esa que dicen, incluyéndola.

Si va bajando el nivel al que baja no sale. Por ejemplo, bajar de transporte a red, estaría aplicación y transporte, pero no red. Tener muy en cuenta que los routers no tienen ni transporte ni aplicación, por lo que no podría bajar de transporte a red porque no tienen transporte. Solo podrían bajar de red a enlace.