

Homework Traffic Analysis

Nicola Alessandro Domingo - 177363

Esercizio 1

Vengono generati 4 frame: 2 per la risoluzione ARP (ARP Request e ARP Reply), 2 per il ping (Echo Request e Echo Reply).

In dettaglio si ha:

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
2	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	130.192.16.2 is at 00:00:00:22:22:22
3	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
4	00:00:00:22:22:22 --> 00:00:00:11:11:11 130.192.16.2 --> 130.192.16.1	ICMP	Echo (ping) reply

Per la precisione, vengono inviati altri due ping request e quindi altri due ping reply.

Esercizio 2

Supponendo che chi effettua il ping request, invia un solo pacchetto di questo tipo, sul link andranno trasmesse le seguenti 8 trame:

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
2	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	130.192.16.2 is at 00:00:00:22:22:22
3	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
4	00:00:00:22:22:22 --> 00:00:00:11:11:11 130.192.16.2 --> 130.192.16.1	ICMP	Echo (ping) reply
5	00:00:00:33:33:33 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.1? Tell 130.192.16.3
6	00:00:00:11:11:11 --> 00:00:00:33:33:33	ARP Reply	130.192.16.1 is at 00:00:00:11:11:11
7	00:00:00:33:33:33 --> 00:00:00:11:11:11 130.192.16.3 --> 130.192.16.1	ICMP	Echo (ping) request
8	00:00:00:11:11:11 --> 00:00:00:33:33:33 130.192.16.1 --> 130.192.16.3	ICMP	Echo (ping) reply

Esercizio 3

All'inizio H2 risponderà normalmente ai ping. Quando si disconnette, H1 continuerà ad inviargli gli echo request fin quando la entry nella cache ARP corrispondente al MAC di H2 non scade (anche se non riceverà alcun echo reply).

A questo punto per poterlo raggiungere, H1 deve reinviare l'ARP Request per conoscere il MAC Address di H2, ma non riceverà alcun ARP Reply come risposta.

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
2	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	130.192.16.2 is at 00:00:00:22:22:22
3	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
4	00:00:00:22:22:22 --> 00:00:00:11:11:11 130.192.16.2 --> 130.192.16.1	ICMP	Echo (ping) reply
H2 si disconnette			
...	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
...	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
...	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
Scade la entry nella cache ARP di H1			
...	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
...	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
...	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1

Esercizio 4

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.253? Tell 130.192.16.1
2	00:00:00:DD:DD:DD --> 00:00:00:11:11:11	ARP Reply	130.192.16.253 is at 00:00:00:DD:DD:DD
3	00:00:00:11:11:11 --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.16.253	Query DNS	Query DNS per www.polito.it
4	00:00:00:DD:DD:DD --> 00:00:00:11:11:11 130.192.16.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 130.192.16.2
5	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
6	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	130.192.16.2 is at 00:00:00:22:22:22
7	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
8	00:00:00:22:22:22 --> 00:00:00:11:11:11 130.192.16.2 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 5

- Frame ricevuti dalla scheda di rete dell'host H2: tutti.
- Frame ricevuti dal sistema operativo dell'host H2 quando la scheda di rete è in promiscuous mode: tutti.
- Frame ricevuti dal sistema operativo dell'host H2 quando la scheda di rete è in modalità standard (non promiscua): 1, 5, 7.

Esercizio 6

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.253? Tell 130.192.16.1
2	00:00:00:DD:DD:DD --> 00:00:00:11:11:11	ARP Reply	130.192.16.253 is at 00:00:00:DD:DD:DD
3	00:00:00:11:11:11 --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.16.253	Query DNS	Query DNS per www.polito.it
4	00:00:00:DD:DD:DD --> 00:00:00:11:11:11 130.192.16.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 130.192.16.2
5	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
6	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	130.192.16.2 is at 00:00:00:22:22:22
7	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
8	00:00:00:22:22:22 --> 00:00:00:11:11:11 130.192.16.2 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 7

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.254? Tell 130.192.16.1
2	00:00:00:EE:EE:EE --> 00:00:00:11:11:11	ARP Reply	130.192.16.254 is at 00:00:00:EE:EE:EE
3	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
4	00:00:00:EE:EE:EE --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.253? Tell 130.192.17.254
5	00:00:00:DD:DD:DD --> 00:00:00:EE:EE:EE	ARP Reply	130.192.17.253 is at 00:00:00:DD:DD:DD
6	00:00:00:EE:EE:EE --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
Il DNS ha già in cache il MAC di R, quindi non esegue il protocollo ARP			
7	00:00:00:DD:DD:DD --> 00:00:00:EE:EE:EE 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 130.192.16.2
Il router ha già in cache il MAC di H1, quindi non esegue il protocollo ARP			
8	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 130.192.16.2
9	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
10	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	130.192.16.2 is at 00:00:00:22:22:22
11	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
12	00:00:00:22:22:22 --> 00:00:00:11:11:11 130.192.16.2 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 8

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.253? Tell 130.192.16.1
2	00:00:00:DD:DD:DD --> 00:00:00:11:11:11	ARP Reply	130.192.16.253 is at 00:00:00:DD:DD:DD
3	00:00:00:11:11:11 --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.16.253	Query DNS	Query DNS per www.polito.it
4	00:00:00:DD:DD:DD --> 00:00:00:11:11:11 130.192.16.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 32.10.1.3
5	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.254? Tell 130.192.16.1
6	00:00:00:EE:EE:EE --> 00:00:00:11:11:11	ARP Reply	130.192.16.254 is at 00:00:00:EE:EE:EE
7	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 32.10.1.3	ICMP	Echo (ping) request
8	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 32.10.1.3 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 9

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.254? Tell 130.192.16.1
2	00:00:00:EE:EE:EE --> 00:00:00:11:11:11	ARP Reply	130.192.16.254 is at 00:00:00:EE:EE:EE
3	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
4	00:00:00:EE:EE:EE --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.253? Tell 130.192.17.1
5	00:00:00:DD:DD:DD --> 00:00:00:EE:EE:EE	ARP Reply	130.192.17.253 is at 00:00:00:DD:DD:DD
6	00:00:00:EE:EE:EE --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
7	00:00:00:DD:DD:DD --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.254? Tell 130.192.17.253
8	00:00:00:CC:CC:CC --> 00:00:00:DD:DD:DD	ARP Reply	130.192.17.254 is at 00:00:00:CC:CC:CC
9	00:00:00:DD:DD:DD --> 00:00:00:CC:CC:CC 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
Il router R2 "consiglia" al DNS di usare la scorciatoia per H1 passando attraverso R1, ed invia in ICMP Redirect			
10	00:00:00:CC:CC:CC --> 00:00:00:DD:DD:DD 130.192.17.254 --> 130.192.17.253	ICMP Redirect	Use 130.192.17.1 to reach 130.192.16.1
11	00:00:00:CC:CC:CC --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.1? Tell 130.192.17.254
12	00:00:00:EE:EE:EE --> 00:00:00:CC:CC:CC	ARP Reply	130.192.17.1 is at 00:00:00:EE:EE:EE
13	00:00:00:CC:CC:CC --> 00:00:00:EE:EE:EE 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
14	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
15	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 30.10.1.3	ICMP	Echo (ping) request
16	00:00:00:EE:EE:EE --> 00:00:00:CC:CC:CC 130.192.16.1 --> 30.10.1.3	ICMP	Echo (ping) request
17	00:00:00:CC:CC:CC --> 00:00:00:EE:EE:EE 30.10.1.3 --> 130.192.16.1	ICMP	Echo (ping) reply
18	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 30.10.1.3 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 10 (Sbagliato)

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.254? Tell 130.192.16.1
2	00:00:00:EE:EE:EE --> 00:00:00:11:11:11	ARP Reply	130.192.16.254 is at 00:00:00:EE:EE:EE
3	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
R1 dovrebbe sapere che per raggiungere la rete 130.192.17.0/24 deve passare da R2, di cui conosce l'IP (perché si suppone le tabelle di routing siano configurate correttamente) ma non il MAC			
4	00:00:00:EE:EE:EE --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.254? Tell 130.192.16.254
5	00:00:00:CC:CC:CC --> 00:00:00:EE:EE:EE	ARP Reply	130.192.17.254 is at 00:00:00:CC:CC:CC
6	00:00:00:EE:EE:EE --> 00:00:00:CC:CC:CC 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
7	00:00:00:CC:CC:CC --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.253? Tell 130.192.17.254
8	00:00:00:DD:DD:DD --> 00:00:00:CC:CC:CC	ARP Reply	130.192.17.253 is at 00:00:00:DD:DD:DD
9	00:00:00:CC:CC:CC --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
10	00:00:00:DD:DD:DD --> 00:00:00:CC:CC:CC 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
11	00:00:00:CC:CC:CC --> 00:00:00:EE:EE:EE 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
12	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
13	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 30.10.1.3	ICMP	Echo (ping) request
14	00:00:00:EE:EE:EE --> 00:00:00:CC:CC:CC 130.192.16.1 --> 30.10.1.3	ICMP	Echo (ping) request
15	00:00:00:CC:CC:CC --> 00:00:00:EE:EE:EE 30.10.1.3 --> 130.192.16.1	ICMP	Echo (ping) reply
16	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 30.10.1.3 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 10 (Corretto)

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.254? Tell 130.192.16.1
2	00:00:00:EE:EE:EE --> 00:00:00:11:11:11	ARP Reply	130.192.16.254 is at 00:00:00:EE:EE:EE
3	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
4	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 130.192.16.254 --> 130.192.16.1	ICMP	ICMP Destination unreachable: Network unreachable

Esercizio 11 (Sbagliato)

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.254? Tell 130.192.16.1
2	00:00:00:EE:EE:EE --> 00:00:00:11:11:11	ARP Reply	130.192.16.254 is at 00:00:00:EE:EE:EE
3	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
R1 dovrebbe sapere che per raggiungere la rete 130.192.17.0/24 deve passare da R2, di cui conosce l'IP (perché si suppone le tabelle di routing siano configurate correttamente) ma non il MAC			
4	00:00:00:EE:EE:EE --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.254? Tell 130.192.16.254
5	00:00:00:CC:CC:CC --> 00:00:00:EE:EE:EE	ARP Reply	130.192.17.254 is at 00:00:00:CC:CC:CC
6	00:00:00:EE:EE:EE --> 00:00:00:CC:CC:CC 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
7	00:00:00:CC:CC:CC --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.253? Tell 130.192.17.254
8	00:00:00:DD:DD:DD --> 00:00:00:CC:CC:CC	ARP Reply	130.192.17.253 is at 00:00:00:DD:DD:DD
9	00:00:00:CC:CC:CC --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
10	00:00:00:DD:DD:DD --> 00:00:00:CC:CC:CC 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
11	00:00:00:CC:CC:CC --> 00:00:00:EE:EE:EE 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
12	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
13	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 30.10.1.3	ICMP	Echo (ping) request
È ragionevole supporre che per andare verso Internet R1 sia configurato usare l'altra sua interfaccia e non inoltrare i pacchetti a R2			
14	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 30.10.1.3 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 11 (Corretto)

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.254? Tell 130.192.16.1
2	00:00:00:EE:EE:EE --> 00:00:00:11:11:11	ARP Reply	130.192.16.254 is at 00:00:00:EE:EE:EE
3	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
Il pacchetto è inoltrato su Internet e raggiungerà R2 prima o poi. Questi, poi, lo inoltrerà al DNS.			
4	00:00:00:CC:CC:CC --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.253? Tell 130.192.17.254
5	00:00:00:DD:DD:DD --> 00:00:00:CC:CC:CC	ARP Reply	130.192.17.253 is at 00:00:00:DD:DD:DD
6	00:00:00:CC:CC:CC --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.17.253	Query DNS	Query DNS per www.polito.it
7	00:00:00:DD:DD:DD --> 00:00:00:CC:CC:CC 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
8	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 130.192.17.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 30.10.1.3
9	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE 130.192.16.1 --> 30.10.1.3	ICMP	Echo (ping) request
10	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 30.10.1.3 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 12

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.253? Tell 130.192.16.1
2	00:00:00:DD:DD:DD --> 00:00:00:11:11:11	ARP Reply	130.192.16.253 is at 00:00:00:DD:DD:DD
3	00:00:00:11:11:11 --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.16.253	Query DNS	Query DNS per www.polito.it
Per il DNS, l'host H1 si trova in un'altra sottorete, pertanto deve inoltrare il pacchetto al suo default gateway R			
4	00:00:00:DD:DD:DD --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.254? Tell 130.192.16.253
<i>Non intercettati dalla scheda di rete di H1</i>	00:00:00:EE:EE:EE --> 00:00:00:DD:DD:DD	ARP Reply	130.192.16.254 is at 00:00:00:EE:EE:EE
	00:00:00:DD:DD:DD --> 00:00:00:EE:EE:EE 130.192.16.253 --> 130.192.16.1	Query DNS	Query DNS Response: www.polito.it is at 130.192.16.2
5	00:00:00:EE:EE:EE --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.1? Tell 130.192.16.254
6	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE	ARP Reply	130.192.16.1 is at 00:00:00:11:11:11
7	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 130.192.16.253 --> 130.192.16.1	Query DNS	Query DNS Response: www.polito.it is at 130.192.16.2
8	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
9	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	130.192.16.2 is at 00:00:00:22:22:22
10	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
11	00:00:00:22:22:22 --> 00:00:00:11:11:11 130.192.16.2 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 13

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.253? Tell 130.192.16.1
2	00:00:00:DD:DD:DD --> 00:00:00:11:11:11	ARP Reply	130.192.16.253 is at 00:00:00:DD:DD:DD
3	00:00:00:11:11:11 --> 00:00:00:DD:DD:DD 130.192.16.1 --> 130.192.16.253	Query DNS	Query DNS per www.polito.it
Per il DNS, l'host H1 si trova in un'altra sottorete, pertanto deve inoltrare il pacchetto al suo default gateway R			
4	00:00:00:DD:DD:DD --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.100? Tell 130.192.16.253
<i>Non intercettati dalla scheda di rete di H1</i>	00:00:00:EE:EE:EE --> 00:00:00:DD:DD:DD	ARP Reply	130.192.16.100 is at 00:00:00:EE:EE:EE
	00:00:00:DD:DD:DD --> 00:00:00:EE:EE:EE 130.192.16.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 130.192.16.2
5	00:00:00:EE:EE:EE --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.1? Tell 130.192.16.100
6	00:00:00:11:11:11 --> 00:00:00:EE:EE:EE	ARP Reply	130.192.16.1 is at 00:00:00:11:11:11
7	00:00:00:EE:EE:EE --> 00:00:00:11:11:11 130.192.16.253 --> 130.192.16.1	Response DNS	Query DNS Response: www.polito.it is at 130.192.16.2
8	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.2? Tell 130.192.16.1
9	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	130.192.16.2 is at 00:00:00:22:22:22
10	00:00:00:11:11:11 --> 00:00:00:22:22:22 130.192.16.1 --> 130.192.16.2	ICMP	Echo (ping) request
11	00:00:00:22:22:22 --> 00:00:00:11:11:11 130.192.16.2 --> 130.192.16.1	ICMP	Echo (ping) reply

Esercizio 14 (Sbagliato)

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.16.1? Tell 130.192.16.81
2	00:00:00:AA:AA:AA --> 00:00:00:11:11:11	ARP Reply	130.192.16.1 is at 00:00:00:AA:AA:AA
3	00:00:00:11:11:11 --> 00:00:00:AA:AA:AA 130.192.16.81 --> 130.192.17.2	Query DNS	Query DNS per www.google.com
4	00:00:00:AA:AA:AA --> 00:00:00:11:11:11 130.192.17.2 --> 130.192.16.81	Response DNS	Query DNS Response: www.google.com is at 180.112.4.3
5	00:00:00:11:11:11 --> 00:00:00:AA:AA:AA 130.192.16.81 --> 180.112.4.3	ICMP	Echo (ping) request
6	00:00:00:AA:AA:AA --> 00:00:00:11:11:11 180.112.4.3 --> 130.192.16.81	ICMP	Echo (ping) reply

Esercizio 14 (Corretto)

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 130.192.17.2? Tell 130.192.16.81
---	---	-------------	---

La netmask di H1 è sbagliata e crede che il DNS sia nella sua stessa sottorete quindi invia un'ARP Request in broadcast a cui nessuno risponderà.

Esercizio 15

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.64.1? Tell 172.16.64.11
2	00:00:00:CC:CC:CC --> 00:00:00:11:11:11	ARP Reply	172.16.64.1 is at 00:00:00:CC:CC:CC
3	00:00:00:11:11:11 --> 00:00:00:CC:CC:CC 172.16.64.11 --> 172.16.10.2	Query DNS	Query DNS per www.polito.it
R2 deve passare da R1 di cui sa l'IP per raggiungere il DNS. Invia anche un ICMP Redirect ad H1			
4	00:00:00:CC:CC:CC --> 00:00:00:11:11:11 172.16.64.1 --> 172.16.64.11	ICMP Redirect	Use 172.16.64.2 to reach 172.16.10.2
5	00:00:00:CC:CC:CC --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.64.2? Tell 172.16.64.1
6	00:00:00:AA:AA:AA --> 00:00:00:CC:CC:CC	ARP Reply	172.16.64.2 is at 00:00:00:AA:AA:AA
7	00:00:00:CC:CC:CC --> 00:00:00:AA:AA:AA 172.16.64.11 --> 172.16.10.2	Query DNS	Query DNS per www.polito.it
<i>Non intercettati dalla scheda di rete di H1</i>	00:00:00:BB:BB:BB --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.10.2? Tell 172.16.10.1
	00:00:00:DD:DD:DD --> 00:00:00:BB:BB:BB	ARP Reply	172.16.10.2 is at 00:00:00:DD:DD:DD
	00:00:00:BB:BB:BB --> 00:00:00:DD:DD:DD 172.16.64.11 --> 172.16.10.2	Query DNS	Query DNS per www.polito.it
	00:00:00:DD:DD:DD --> 00:00:00:BB:BB:BB 172.16.10.2 --> 172.16.64.11	Response DNS	Query DNS Response: www.polito is at 172.16.64.6
R1 inoltra la risposta DNS direttamente ad H1 di cui conosce l'IP ma non il MAC, infatti non è lui il suo DG.			
8	00:00:00:AA:AA:AA --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.64.11? Tell 172.16.64.2
9	00:00:00:11:11:11 --> 00:00:00:AA:AA:AA	ARP Reply	172.16.64.11 is at 00:00:00:11:11:11
10	00:00:00:AA:AA:AA --> 00:00:00:11:11:11 172.16.10.2 --> 172.16.64.11	Response DNS	Query DNS Response: www.polito is at 172.16.64.6
11	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.64.6? Tell 172.16.64.11
12	00:00:00:22:22:22 --> 00:00:00:11:11:11	ARP Reply	172.16.64.6 is at 00:00:00:22:22:22
13	00:00:00:11:11:11 --> 00:00:00:22:22:22 172.16.64.11 --> 172.16.64.6	ICMP	Echo (ping) request
14	00:00:00:22:22:22 --> 00:00:00:11:11:11 172.16.64.6 --> 172.16.64.11	ICMP	Echo (ping) reply

Esercizio 16 (Sbagliato)

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.64.1? Tell 172.16.64.11
2	00:00:00:CC:CC:CC --> 00:00:00:11:11:11	ARP Reply	172.16.64.1 is at 00:00:00:CC:CC:CC
3	00:00:00:11:11:11 --> 00:00:00:CC:CC:CC 172.16.64.11 --> 172.16.10.2	Query DNS	Query DNS per www.polito.it
R2 deve passare da R1 di cui sa l'IP per raggiungere il DNS. Invia anche un ICMP Redirect ad H1			
4	00:00:00:CC:CC:CC --> 00:00:00:11:11:11 172.16.64.1 --> 172.16.64.11	ICMP Redirect	Use 172.16.64.2 to reach 172.16.10.2
5	00:00:00:CC:CC:CC --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.64.2? Tell 172.16.64.1
6	00:00:00:AA:AA:AA --> 00:00:00:CC:CC:CC	ARP Reply	172.16.64.2 is at 00:00:00:AA:AA:AA
7	00:00:00:CC:CC:CC --> 00:00:00:AA:AA:AA 172.16.64.11 --> 172.16.10.2	Query DNS	Query DNS per www.polito.it
<i>Non intercettati dalla scheda di rete di H1</i>	00:00:00:BB:BB:BB --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.10.2? Tell 172.16.10.1
	00:00:00:DD:DD:DD --> 00:00:00:BB:BB:BB	ARP Reply	172.16.10.2 is at 00:00:00:DD:DD:DD
	00:00:00:BB:BB:BB --> 00:00:00:DD:DD:DD 172.16.64.11 --> 172.16.10.2	Query DNS	Query DNS per www.polito.it
	00:00:00:DD:DD:DD --> 00:00:00:BB:BB:BB 172.16.10.2 --> 172.16.64.11	Response DNS	Query DNS Response: www.polito is at 172.16.64.6
R1 inoltra la risposta DNS direttamente ad H1 di cui conosce l'IP ma non il MAC, infatti non è lui il suo DG.			
8	00:00:00:AA:AA:AA --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.64.11? Tell 172.16.64.2
9	00:00:00:11:11:11 --> 00:00:00:AA:AA:AA	ARP Reply	172.16.64.11 is at 00:00:00:11:11:11
10	00:00:00:AA:AA:AA --> 00:00:00:11:11:11 172.16.10.2 --> 172.16.64.11	Response DNS	Query DNS Response: www.polito is at 172.16.64.6
11	00:00:00:11:11:11 --> 00:00:00:CC:CC:CC 172.16.64.11 --> 172.16.15.3	HTTP	GET HTTP
12	00:00:00:CC:CC:CC --> 00:00:00:11:11:11 172.16.15.3 --> 172.16.64.11	HTTP	HTTP 200 OK

Esercizio 16 (Corretto)

1	00:00:00:11:11:11 --> FF:FF:FF:FF:FF:FF	ARP Request	Who has 172.16.64.1? Tell 172.16.64.11
2	00:00:00:CC:CC:CC --> 00:00:00:11:11:11	ARP Reply	172.16.64.1 is at 00:00:00:CC:CC:CC
3	00:00:00:11:11:11 --> 00:00:00:CC:CC:CC 172.16.64.11 --> 172.16.15.3	TCP SYN	
4	00:00:00:CC:CC:CC --> 00:00:00:11:11:11 172.16.15.3 --> 172.16.64.11	TCP SYN-ACK	
5	00:00:00:11:11:11 --> 00:00:00:CC:CC:CC 172.16.64.11 --> 172.16.15.3	TCP ACK	
6	00:00:00:11:11:11 --> 00:00:00:CC:CC:CC 172.16.64.11 --> 172.16.15.3	HTTP	GET HTTP
7	00:00:00:CC:CC:CC --> 00:00:00:11:11:11 172.16.15.3 --> 172.16.64.11	HTTP	HTTP 200 OK
8 - ...	Frame corrispondenti alla pagina HTTP richiesta		

Esercizio 17

In questo caso, l'host H1 ha una netmask errata, in quanto dovrebbe valere 24 e non 23.

Ciò porta all'errata considerazione che il server DNS si trovi nella sua stessa sottorete.

In dettaglio, usando una notazione mista binario-decimale puntato, si ha:

IP H1: 130.192.000100000.01010001
NETMASK 255.255.11111110.00000000
IP DNS: 130.192.00010001.00000010

H1 fa l'AND bitwise tra il suo IP e la netmask 255.255.254.0 ed ottiene l'indirizzo di rete 130.192.16.0/23; poi fa l'AND tra l'IP del DNS e la stessa netmask ed ottiene lo stesso indirizzo di rete, da qui, quindi, l'errore.

Se la netmask fosse stata 24, l'AND tra l'IP del DNS e la giusta netmask 255.255.255.0 avrebbe portato all'indirizzo di rete 130.192.17.0 per il DNS, ed H1 avrebbe proceduto correttamente (ARP per il MAC del DG, inoltro della query DNS al DG, ricezione del DNS Response, invio della richiesta HTTP attraverso il DG, ricezione della pagina).

Pensando erroneamente che il DNS fosse nella sua stessa sottorete, per poterlo raggiungere deve conoscere il suo MAC ed invia una ARP Request alla quale, però, non seguirà nessuna ARP Reply, in quanto in quella sottorete non c'è alcun host avente IP 130.192.17.2.

La risoluzione DNS quindi fallirà e da qui anche la visualizzazione della pagina.

Per diagnosticare questo tipo di problema si potrebbe usare `ifconfig` (in sistemi Unix-like) o `ipconfig` (in ambiente Windows) e verificare che la netmask impostata per l'host sia corretta, e porti alla corretta identificazione della sottorete in cui ci si trova.