

# 01QZD

## Laboratorio di Internet e Comunicazioni



### Internet - Laboratorio 1

#### 5. Connectivity check – Advanced ping

- 1) Cosa succede quando un terminale esegue un ping all'indirizzo di broadcast?

Quando si esegue il comando ping verso l'indirizzo di broadcast viene richiesto di aggiungere il parametro -b al comando.

```
ping 172.16.0.63 -b
```

Il terminale richiedente invia a tutti gli altri il pacchetto icmp request, gli altri terminali lo ricevono e, se configurati per la risposta ognuno risponde con un pacchetto icmp reply. Di default il SO non è configurato per la risposta al broadcast in quanto può essere utilizzato per attaccare una rete (o un host) sovraccaricandola.

All'interno della tabella arp del mittente non viene aggiunto alcun indirizzo mac in quanto il mittente non esegue alcuna arp request per un indirizzo IP che corrisponde a più host (indirizzo broadcast).

Gli altri host, prima di rispondere eseguono un'arp request per identificare l'indirizzo mac del mittente. Esso non era noto a priori perché l'indirizzo del pacchetto ricevuto in broadcast non viene salvato nell'arp del destinatario.

Una volta che il mittente avrà risposto all'arp request, il suo indirizzo mac sarà memorizzato nella tabella arp del destinatario ed esso provvederà a mandare un pacchetto di risposta. Il mittente iniziale calcola di conseguenza il RTT in base al primo pacchetto di risposta che riceve.

- 2) Cosa succede quando un terminale esegue un ping all'indirizzo di rete?

Quando si esegue un ping all'indirizzo di rete il comportamento è identico a quello osservato al punto precedente.

### Rete con indirizzo duplicato

Abbiamo configurato la rete per avere due host con lo stesso indirizzo IP (H1, H1')

- 1) Cosa succede quando H2 esegue un ping su H1?

Inizialmente H2 esegue una arp request. Sia H1 che H1' rispondono alla richiesta. Nella tabella arp di H2 sarà memorizzato l'indirizzo mac dell'host che risponde più velocemente (ad esempio H1'), e dunque H2 inizierà a pingare H1'.

Periodicamente H2 effettua un aggiornamento dei dati contenuti nella tabella arp. Nel caso in cui l'host H1 riesca a rispondere più velocemente di H1', nella tabella arp di H2 l'indirizzo

```
ale@xubuntu-macbook-pro:~$ ping 172.16.0.3
PING 172.16.0.3 (172.16.0.3) 56(84) bytes of data:
64 bytes from 172.16.0.3: icmp_seq=1 ttl=64 time=1.05 ms
64 bytes from 172.16.0.3: icmp_seq=2 ttl=64 time=0.523 ms
64 bytes from 172.16.0.3: icmp_seq=3 ttl=64 time=0.434 ms
64 bytes from 172.16.0.3: icmp_seq=4 ttl=64 time=0.527 ms
64 bytes from 172.16.0.3: icmp_seq=5 ttl=64 time=0.554 ms
64 bytes from 172.16.0.3: icmp_seq=6 ttl=64 time=0.525 ms
64 bytes from 172.16.0.3: icmp_seq=7 ttl=64 time=0.532 ms
64 bytes from 172.16.0.3: icmp_seq=8 ttl=64 time=0.463 ms
64 bytes from 172.16.0.3: icmp_seq=9 ttl=64 time=0.612 ms
64 bytes from 172.16.0.3: icmp_seq=10 ttl=64 time=0.549 ms
64 bytes from 172.16.0.3: icmp_seq=11 ttl=64 time=0.537 ms
64 bytes from 172.16.0.3: icmp_seq=12 ttl=64 time=0.525 ms
64 bytes from 172.16.0.3: icmp_seq=13 ttl=64 time=0.446 ms
64 bytes from 172.16.0.3: icmp_seq=14 ttl=64 time=0.542 ms
^C
--- 172.16.0.3 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13289ms
rtt min/avg/max/mdev = 0.434/0.559/1.057/0.145 ms
ale@xubuntu-macbook-pro:~$ arp
Indirizzo TipoHW IndirizzoHW Flag Maschera Interfaccia
172.16.0.3 ether b8:27:eb:b7:c5:a7 ens9
ale@xubuntu-macbook-pro:~$
```

mac di H1' sarà sostituito con quello di H1.

- 2) Cosa succede quando H1 e H1' incominciano a pingare H2 nello stesso momento? Controlla le tabelle di arp.

Inizialmente H1 e H1' inviano ognuno una arp request verso H2, e salvano nelle rispettive tabelle arp l'indirizzo mac di H2. Nella tabella arp di H2 viene associato all'IP di H1 e H1' l'indirizzo mac del primo host di cui riceve l'arp request.

Assumiamo che H2 memorizzi l'indirizzo mac di H1'. Per ogni ICMP request ricevuta da H2, qualunque sia il mittente (H1 o H1'), H2 risponderà sempre ad H1', che riceverà dunque anche le risposte alle richieste di H1. Le risposte alle richieste di H1' sono coerenti al numero di sequenza, al contrario di quelle riferite ad H1.

Durante un successivo aggiornamento della tabella arp di H2, potrebbe essere effettuata una modifica dell'indirizzo mac associato all'ip condiviso tra H1 e H1'. H1 diventerebbe dunque il destinatario di tutte le risposte alle ICMP request.

## Netmask sbagliate

Configuriamo H1 e H2 in modo tale che i rispettivi indirizzi IP abbiano netmask diverse. H1 risulta non appartenente alla stessa subnet di H2.

- 1) Cosa succede quando H1 esegue il comando di ping verso H2? Quali pacchetti invia H1? Quali pacchetti invia H2? Come cambiano le tabelle arp di H1 e di H2?

Quando H1 vuole eseguire un ping verso H2 manda inizialmente una arp request. H2 riceve la richiesta, senza tuttavia fornire una risposta. Questo perché, se H2 rispondesse, H1 comincerebbe a mandare pacchetti ad H2, a cui esso non potrebbe rispondere, in quanto H1 viene visto da H2 al di fuori della rete in cui è collocato. Si verrebbe dunque a creare un collegamento logico unidirezionale, per cui sarebbe impossibile instaurare una comunicazione reciproca.

Le tabelle arp di H1 e H2 rimangono dunque vuote.

354	967.098084	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.66
355	967.098115	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.66
356	968.121574	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.66
357	968.121632	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.66
358	969.145760	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.66
359	969.145817	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.66

- 2) Cosa succede quando H2 esegue il comando di ping verso H1? Quali pacchetti invia H2? Quali pacchetti invia H1? Come cambiano le tabelle arp di H1 e di H2?

H2 prova a mandare una ICMP request verso H1. Tuttavia, al livello IP di H2 il pacchetto viene bloccato poiché l'IP di H1 non appartiene alla stessa rete di H2, e non sono disponibili rotte per raggiungerlo. Il controllo viene effettuato confrontando l'and bit a bit dell'indirizzo IP di H2 associato alla propria Netmask con quello dell'indirizzo ip di H1.

```
ale@xbuntu-macbook-pro:~$ arp
Indirizzo TipoHW IndirizzoHW Flag Maschera Interfaccia
172.16.0.3 ether b8:27:eb:b7:c5:a7 C ens9
ale@xbuntu-macbook-pro:~$ ping 172.16.0.66
connect: Network is unreachable
ale@xbuntu-macbook-pro:~$ arp
Indirizzo TipoHW IndirizzoHW Flag Maschera Interfaccia
172.16.0.3 ether b8:27:eb:b7:c5:a7 C ens9
ale@xbuntu-macbook-pro:~$
```

## Conflitto con indirizzo di broadcast

Abbiamo configurato H1 e H2 in modo tale che H1 presenti l'indirizzo di broadcast della rete a cui appartiene H2:

- H1 con un indirizzo IP 172.16.0.127 con Netmask 255.255.255.0
- H2 con un indirizzo IP 172.16.0.1 con Netmask 255.255.255.128

- 1) Cosa succede quando H1 pinga H2? Quali pacchetti sta trasmettendo H1? Quali pacchetti sta trasmettendo H2? Come cambiano le tabelle arp?

Viene trasmessa una arp request da H1 a H2. L'arp di H2 dovrebbe fornire una risposta ad H1, tuttavia non lo fa perché H1 ha l'indirizzo IP di broadcast. Rispondere ad H1, dunque, significherebbe rispondere a tutti gli host appartenenti alla rete, cosa che non ha senso logico.

```
nunzio@nunzio:~/Scrivania$ ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data:
From 172.16.0.127 icmp_seq=1 Destination Host Unreachable
From 172.16.0.127 icmp_seq=2 Destination Host Unreachable
From 172.16.0.127 icmp_seq=3 Destination Host Unreachable
From 172.16.0.127 icmp_seq=4 Destination Host Unreachable
From 172.16.0.127 icmp_seq=5 Destination Host Unreachable
From 172.16.0.127 icmp_seq=6 Destination Host Unreachable
^C
--- 172.16.0.1 ping statistics ---
 7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6127ms
pipe 4
nunzio@nunzio:~/Scrivania$ arp
Indirizzo TipoHW IndirizzoHW Flag Maschera Interfaccia
172.16.0.1                               (incompleto)          enp0s8
nunzio@nunzio:~/Scrivania$
```

Nella tabella arp di H1 viene inserita una entry corrispondente ad H2. Poiché H1 non riceve una risposta, il campo riservato all'indirizzo mac di H2 rimane incompleto.

Per quanto riguarda invece la tabella arp di H2, essa rimane invariata.

703	1331.846004650	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1?	Tell 172.16.0.127
704	1332.869213521	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1?	Tell 172.16.0.127
705	1333.893413375	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1?	Tell 172.16.0.127
706	1334.917459182	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1?	Tell 172.16.0.127
707	1335.941780567	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1?	Tell 172.16.0.127
708	1336.964805302	PcsCompu_e5:92:80	Broadcast	ARP	60	Who has 172.16.0.1?	Tell 172.16.0.127

- 2) Cosa succede quando H2 pinga H1? Quali pacchetti sta trasmettendo H1? Quali pacchetti sta trasmettendo H2? Come cambiano le tabelle arp?

H2 manda una ICMP request, senza effettuare prima una arp request, poiché l'indirizzo IP di H1 è l'indirizzo di broadcast della rete. Prima di inviare una risposta, H1 trasmette una arp request ad H2. Tuttavia, H2 non fornirà mai una risposta per gli stessi motivi evidenziati al punto 1).

Anche in questo caso nella tabella arp di H1 viene inserita una entry relativa ad H2, e poiché H2 non fornisce una risposta alla arp request di H1, il campo riservato all'indirizzo mac di H2 rimane incompleto.

```
ale@xbuntu-macbook-pro:~$ arp
ale@xbuntu-macbook-pro:~$ ping 172.16.0.127
Do you want to ping broadcast? Then -b
ale@xbuntu-macbook-pro:~$ ping 172.16.0.127 -b
WARNING: pinging broadcast address
PING 172.16.0.127 (172.16.0.127) 56(84) bytes of data:
^C
--- 172.16.0.127 ping statistics ---
 20 packets transmitted, 0 received, 100% packet loss, time 19440ms
ale@xbuntu-macbook-pro:~$ arp
ale@xbuntu-macbook-pro:~$
```