Esercitazione di Laboratorio - NA02

Riccardo Persello

8 giugno 2021

Ricezione di pacchetti ARP

1. **Riuscite a individuare un pacchetto ARP rivolto al vostro elaboratore?**

   Si.

2. **Se no, perché?**

   -

3. **Se sì, qual è l'indirizzo MAC che il vostro elaboratore comunica in risposta?**

   `A0:78:17:83:57:03`.

4. **Individuate un pacchetto ARP inviato dal vostro elaboratore e descrivetene il contenuto:**

   Il pacchetto indica una interfaccia di tipo 1 (Ethernet). Il campo PTYPE (protocol type) ha un valore pari a `0x800`, corrispondente al protocollo IPv4. HLEN (hardware address length) è pari a 6, infatti gli indirizzi harware (MAC) hanno una dimensione di 6 otteti. PLEN (protocol address length) è pari a 4, essendo un indirizzo IPv4. Nel campo del codice operazione si trova un valore pari a 2, indicante che il pacchetto inviato è una risposta. Successivamente si trovano i 4 indirizzi (due MAC e due IP) del mittente e del destinatario della risposta.

- Mittente: 192.168.43.12 (`A0:78:17:83:57:03`)
- Destinatario: 192.168.43.1, gateway (`DA:33:F3:CD:E2:7E`)

5. **Che pacchetti di ARP reply riuscite a osservare? Perché?**

   Oltre ai pacchetti inviati in quanto risposte alle ARP request effettuate dal default gateway (circa ogni 30 secondi), si notano dei pacchetti di ARP reply da parte del default gateway esattamente ogni 90 secondi, indirizzati al calcolatore in uso, ma senza una corrispondente ARP request.

Ping

Basandovi sui nomi di rete di server a voi conosciuti (esempio: www.ieee.org), cercate di trovarne uno che risponda al ping. Verificate anche (collegandovi per esempio mediante un browser, se si tratta di server web) se i server che non rispondono sono effettivamente irraggiungibili o se semplicemente il ping è stato disattivato per ragioni di sicurezza. (esempio: www.uniud.it).

Server	Indirizzo IP	Risponde al ping?	È raggiungibile?
google.com	216.58.206.78	Si	Si
localhost	127.0.0.1	Si	Si
uniud.it	158.110.3.47	No	Si
sd1.persello.tk	157.90.151.101	Si	Si

Ping 2

1. **Che indirizzo MAC ha la porta del router definito come default gateway per il vostro computer?**

   `DA:33:F3:CD:E2:7E`

2. **A chi corrisponde l'indirizzo IP di destinazione contenuto nel messaggio "echo request" relativo al comando ping verso l'esterno della rete locale?**

   L'indirizzo IP di destinazione della *echo request* è quello del server remoto.

3. **A chi corrisponde l'indirizzo MAC?**

   L'indirizzo MAC di destinazione della *echo request* è quello del default gateway.

Trace route

Basandovi inizialmente sui nomi di rete di server a voi conosciuti, e successivamente sugli indirizzi che avrete individuato durante lo svolgimento dell'esercizio, cercate l'indirizzo più "lontano" (in termini di numero di hop) che riuscite a trovare.

> Server più lontano: **sd1.persello.tk**, indirizzo IP: **157.90.151.101**, numero di hop: **18**. Si sono provati numerosi nomi di server conosciuti, ma la maggior parte non rispondono né al ping, né al traceroute (il quale non riesce a comunicare con il server di destinazione e arriva al numero massimo di hop senza fornire un risultato).

Trace route 2

Riuscite a individuare i pacchetti utilizzati dal programma tracert?

Si. Se non si effettuano altre operazioni riguardanti l'indirizzo per cui si sta effettuando il traceroute, è possibile filtrare i pacchetti inviati verso quel server per visualizzare ciò che la nostra macchina fa per portare a termine questa operazione. Questo è possibile in quanto i pacchetti inviati da `traceroute` sono diretti all'indirizzo passato come parametro.

Applicando il filtro `ip.addr == 157.90.151.101` si mantengono in lista tutti i pacchetti inviati e ricevuti dall'indirizzo specificato (in questo caso un server personale), ma non solo. Anche i pacchetti di errore ICMP ricevuti dal calcolatore e provenienti da altri nodi (in questo caso, intermedi tra la nostra macchina ed il server di destinazione) che contengano riferimenti all'indirizzo filtrato, vengono mantenuti nell'elenco.

Che protocollo utilizza?

I protocolli utilizzati sono UDP e ICMP.

Come fa ad ottenere un messaggio da ogni router attraversato?

Vengono inviati dei pacchetti UDP, a gruppi di tre, con TTL (a livello IP) iniziale pari a 1 e via via crescente, con destinazione l'indirizzo specificato. In questo modo, ogni serie di pacchetti riesce ad "esplorare" la rete con un percorso di lunghezza pari ad un *hop* in più rispetto a quello della serie precedente. Quando un nodo incontra un pacchetto con un TTL pari a 1, non lo inoltra al nodo successivo, in quanto otterrebbe un TTL pari a zero. Il nodo invia quindi al mittente un messaggio ICMP di errore, specificando il motivo (*Time to live exceeded in transit*), e quindi rivelando il proprio indirizzo IP.

In questo modo, ogni router presente sul percorso che collega la macchina in uso al server con l'indirizzo specificato riceverà un pacchetto con TTL pari ad 1, e manderà un messaggio di errore al mittente, il quale può quindi costruire un elenco ordinato di nodi, rappresentanti il percorso preso da un pacchetto che deve raggiungere una macchina remota. Alcuni nodi non rispondono a questo tipo di pacchetti, causando la presentazione di una riga di tre asterischi nell'output del comando `traceroute`. È necessario che il nodo di destinazione risponda con un messaggio ICMP (e che questo non venga bloccato) per far sì che il comando termini prima del numero massimo di tentativi.

Il comando termina quando riceve un messaggio ICMP dal nodo di destinazione. Nel caso in cui si passi come argomento al comando un

URL, viene effettuata una query al DNS per trovare l'indirizzo IP corrispondente.

La sorgente del documento è disponibile al seguente indirizzo: https://github.com/persello/esercizi-rdc. Documento generato con pandoc.