ICMP: comando TRACE

Il comando IOS **trace** si basa sia sul messaggio Time Exceeded, sia sul campo TTL nella impostazione IP.

A seguito di invio di pacchetti IP con protocollo di trasporto UDP (traceroute) con TTL = 1 impostato volutamente, si riceve un messaggio ICMP Time Exceeded dal primo router nel percorso; questo perché il primo router decrementa il TTL a zero, di conseguenza scarta il pacchetto ed invia il messaggio Time Exceeded alla sorgente del traffico (ad esempio un qualsiasi host della rete).

Il comando **trace** prende nota dell'indirizzo IP del primo router quando invia il messaggio Time Exceeded (in realtà trace invia tre pacchetti con TTL = 1 in successione).

A questo punto il comando **trace** invia un ulteriore insieme di tre pacchetti con TTL = 2; questi pacchetti attraversano il primo router (il quale decrementa il valore TTL = 1), e poi vengono scartati dal secondo router poiché il TTL viene decrementato = 0.

I pacchetti originali inviati dal comando **trace** utilizzano un numero di porta di destinazione UDP che difficilmente viene usato; in questo modo l'host di destinazione restituirà un messaggio di "Port Unreachable".

Questo messaggio significa che i pacchetti hanno raggiunto il vero host di destinazione senza aver superato il tempo massimo: pertanto il comando **trace** è utile per capire se i pacchetti stanno arrivando a destinazione