1.Environment:Run Ubuntu ova with VirtualBox on macOS

2. 1)detect:假設短時間內收到大量同一個IP送出的ICMP packets且TTL如果都偏低的話, 表示該IP可能正在進行traceroute

2)defend:在防火牆上做設定, 也可以藉由路由器的Access Control List 來辨識網路封包並應如何處置, 例如不允許ICMP封包經過, 避免DoS等網路攻擊

3.有時traceroute會遇到三個星號, 導致無法得知完整的路徑, 可能的原因有兩者:
1)中間經過的device可能有防火牆block了ICMP packet
2)當下的網路可能繁忙, 導致router沒有辦法送出ICMP packet

4.
1)會影響RTT的因素非常的多, 最主要的原因就是網路或各種因素造成的延遲, 都會影響RTT的值，甚至封包到達router和返回的路經都有可能不相同。
2)封包通過IP網絡的路徑由網絡配置決定, 封包通過網絡的路徑可能並不總是相同。實際上, 封包實際通過網絡所經過的路徑可能和traceroute所顯示的不同。
3)若路徑中的某個router發生問題的話, 則將不會收到該router的RTT值或IP地址信息。

5.國內的網站 64 hops 以內會trace完，而國外的網站可能需要超過 64 hops, 並且國外網站的RTT會在某次顯著增大, 這可能是因為需要跨海, 再來, trace國外的網站也更容易time out

6.ICMP:發送ICMP Echo Request後會因為TTL歸0而收到router回送的ICMP Time Exceed, 到final idestination後會回送ICMP Echo Reply(final reply)

UDP:發送UDP packet出去，在送的過程跟ICMP一樣會收到router回送的ICMP Time Exceed，但到final destination後會回送ICMP Destination Unreachable(final reply)而不是ICMP Echo Reply
TCP:跟ICMP和UDP一樣是利用TTL做traceroute，但發送的是SYN(handshake過程中嘗試建立連線的packet)，在送的過程跟ICMP和UDP一樣會收到router回送的ICMP Time Exceed，但到final destination後會回送SYN+ACK跟ICMP和UDP不同

Reference:
https://zhuanlan.zhihu.com/p/101810847
https://blog.paessler.com/4-vital-tips-for-getting-the-most-out-of-traceroute
https://networkengineering.stackexchange.com/questions/16530/traceroute-doesnt-print-entire-route-sometimes