Discussion2 Feedback

###### Post by [Beran Necat](https://www.my-course.co.uk/user/view.php?id=12095&course=7516)

[**76 days ago**](https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289122#p1009966)

*Re: Initial Post*

Hi Ying,

There are several reasons why a “Request timed out” message may appear at the end of a trace route. It could be because a device isn’t programmed to respond to the Internet Control Message Protocol (ICMP) or traceroute requests, it could also be due to the presence of a firewall or other security device which may be blocking the request.

Regards, Beran

###### Post by [Austin Mundy](https://www.my-course.co.uk/user/view.php?id=16068&course=7516)

[**69 days ago**](https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289122#p1013104)

*Peer Response*

Thank you for your post, you provided some insightful information. Your hop count was 25 hops, which seems to be slightly longer than other results. Two of the hops had dropped due to exceeding the TTL of the packets (Parziale et al, 2006). As well the latency increased rather drastically from hop eight to nine. They consisted though and there were no drops towards the end, so it reached the destination with no problem. The name server and mail server results also were consistent with other user tests. Dig in particular is a powerful tool that provides a lot of built-in functionality. It can be a bit more complicated than nslookup in everyday use, however. As well, nslookup is technically deprecated, meaning it is good to learn other alternatives.

It is interesting to bring up how there are several name servers for redundancy. As you stated this would help against Denial of service(Dos) attacks, by providing redundancy. However, as shown in the work above, it is rather easy to find the IP addresses of these servers. A DDoS attack would be rather effective against this site (cisa, 2019). The scans show that other alternatives are needed to secure them such as the use of proxy or a NAT firewall.

References:

CISA.(2010) Understanding Denial-of-Service Attacks. Available from: <https://www.cisa.gov/uscert/ncas/tips/ST04-015> [Accessed 11 December 2021].

Parziale et al.(2006) *TCP/IP Tutorial and Technical Overview.* 8th ed. New York: IBM Redbooks. Available from: <https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf> [Accessed 11 December 2021].

###### Post by [Muhammad Qasim](https://www.my-course.co.uk/user/view.php?id=16177&course=7516)

[**67 days ago**](https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289122#p1014155)

*Peer Response*

You were able to obtain route information as well as the time required for each hop, router by router, from the source computer to the destination IP by using the traceroute command. The three group members' data showed inconsistencies in locations and timings, with up to 25 hops and a maximum delay of 307 milliseconds. Some routes, however, included asterisks or the message "Request timed out" in their responses. It's possible that the packets arrived at a router with a firewall that prevents traceroute requests from being broadcast online, or that the router did not respond before the timeout occurred (Parziale et al., 2006). Nslookup is a sophisticated command-line utility for network management, according to PEYCHEV (2021). It may be used to obtain information such as domain names, IP addresses, and mail exchange (MX), and name servers records (Nslookup.io, 2021). It is available as software as a command line and as an online tool.

References

Nslookup.io (2021). Available from: [**https://www.nslookup.io/dns-records/allmytype.co.uk**](https://www.nslookup.io/dns-records/allmytype.co.uk) [Accessed 14 December 2021].

Peychev, B. (2021) 10 most used Nslookup commands. Available from: [**https://www.cloudns.net/blog/10-most-used-nslookup-commands/**](https://www.cloudns.net/blog/10-most-used-nslookup-commands/) [Accessed 14 December 2021].

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006). TCP/IP Tutorial And Technical Overview. 8th ed. New York, IBM.