

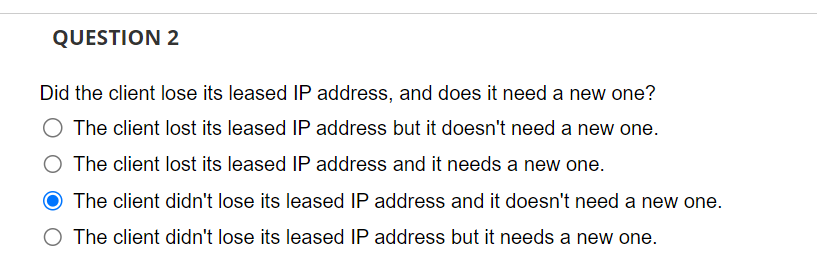
Search “icmp” which shows icmp packets being sent with increasing TTLs in sets of 3.

OR

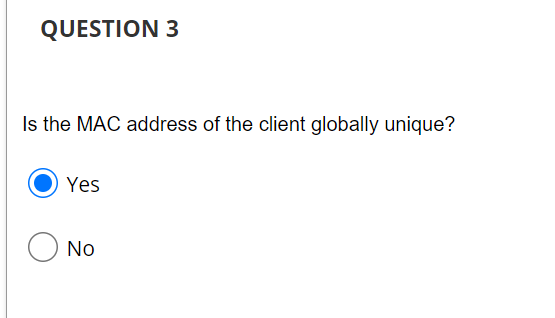
A screenshot of a computer

Description automatically generated with low confidence

DNS response in packet 84 shows coms3200.uqcloud.net type A record of 130.102.71.30



If you search ‘dhcp’ you see that the client received its ip (192.168.0.103) with a lease time of 7200s = 2hrs, and the total packet capture time is for 80 secs so it still has the address and doesn’t need a new one



Mac of client 192.168.0.103 is Netgear\_2b:41:66 (9c:c9:eb:2b:41:66)

A screenshot of a computer

Description automatically generated with low confidence

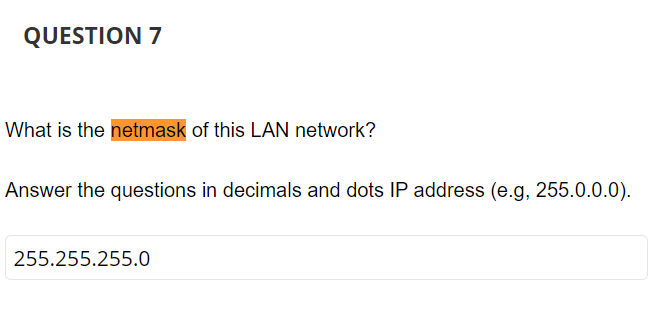
Search arp and see how many arp requests are sent from host to client???

A white background with black text

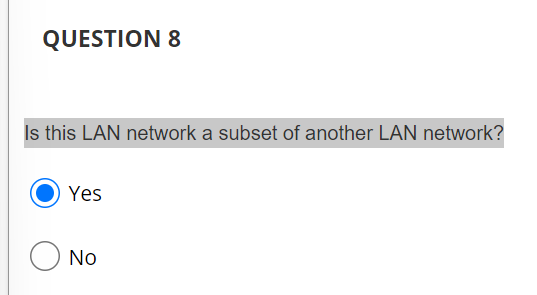
Description automatically generated with low confidence

A screenshot of a question

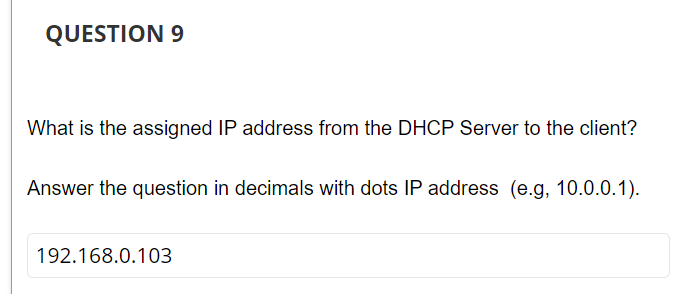
Description automatically generated with low confidence



DHCP offer packet



Second response from the trace route icmp packets is from 192.168.1.0 which is the second router outside our immediate one at 192.168.0.0

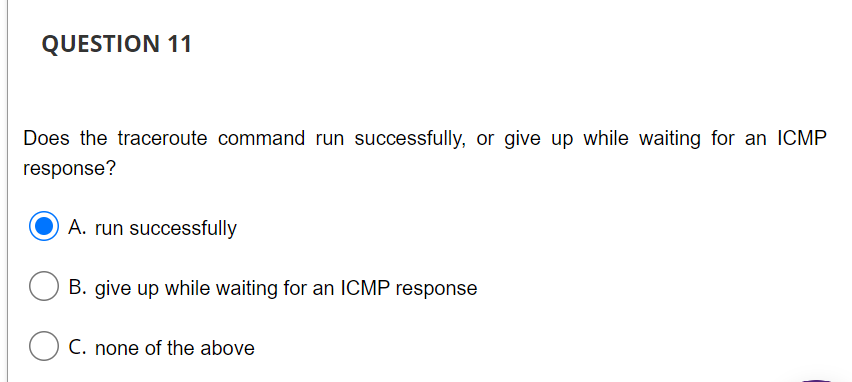


Look up dhcp and check

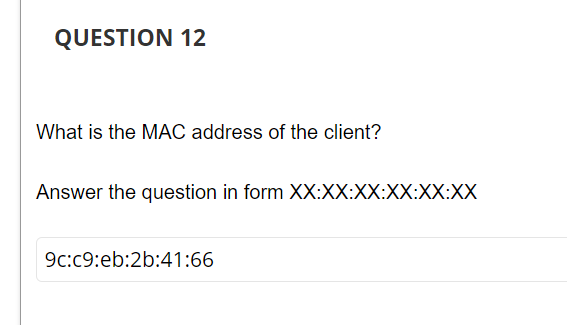
A screenshot of a computer

Description automatically generated with low confidence

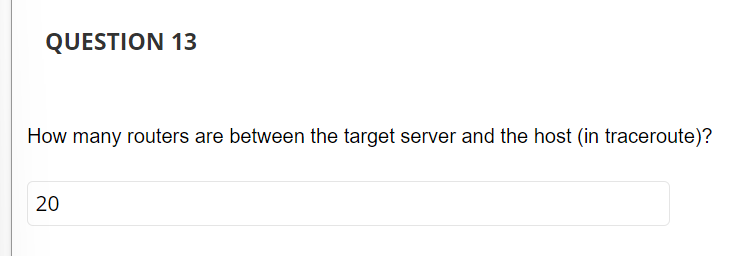
Look up dhcp



Final trace route icmp packets get responses from the target server



Look up first dhcp packet



Final traceroute packet has ttl of 21. Ttl starts at 0 so therefore there are 20 routers between

A screenshot of a computer

Description automatically generated with low confidence

Look up icmp

A screenshot of a computer

Description automatically generated with low confidence

<https://osqa-ask.wireshark.org/questions/41152/how-to-check-if-fragmentation-is-happening/>

ip.flags.mf ==1 or ip.frag\_offset gt 0