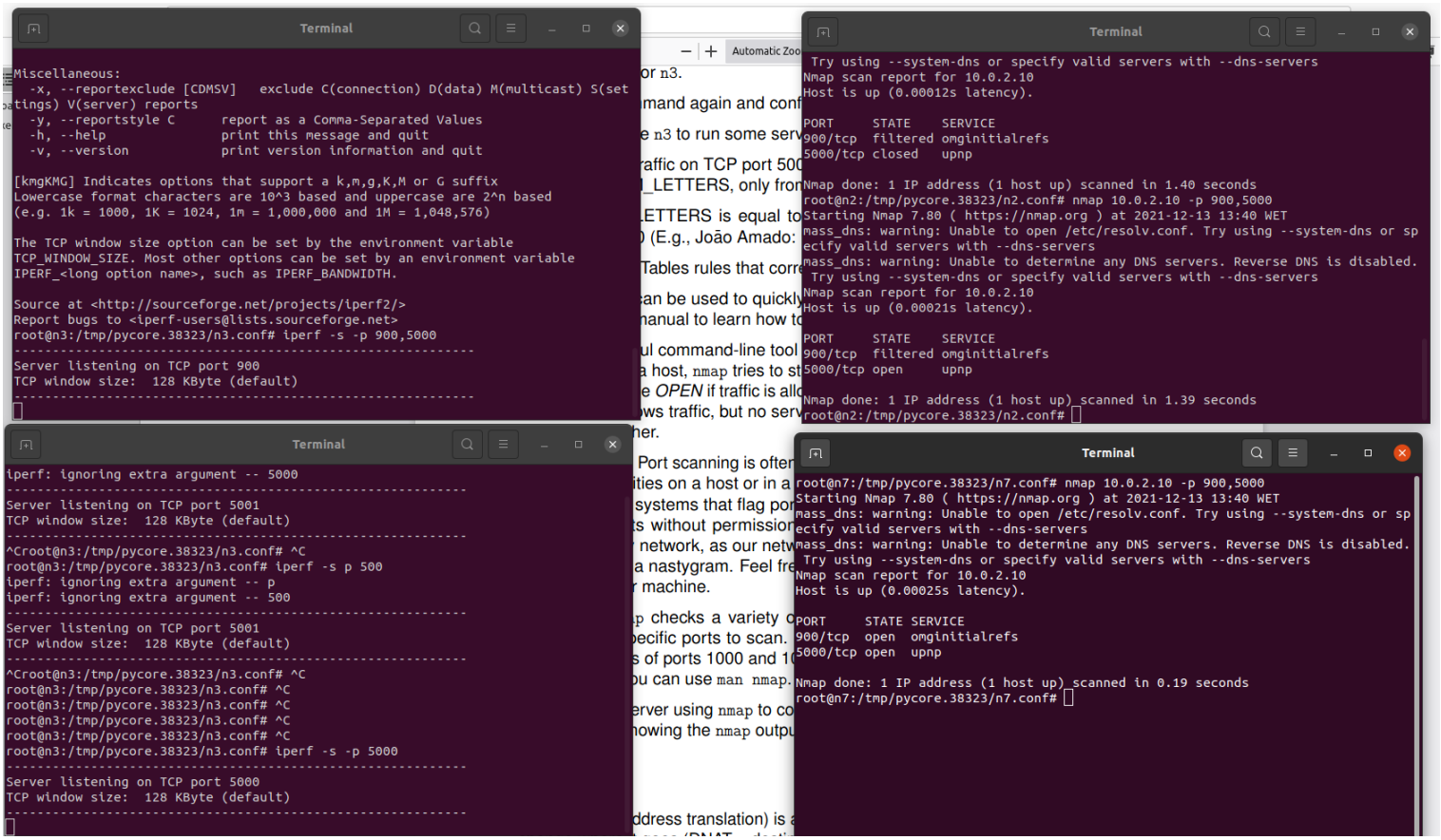
q1:
iptables -I INPUT -j DROP

q2:
iptables -I INPUT -p icmp -j ACCEPT

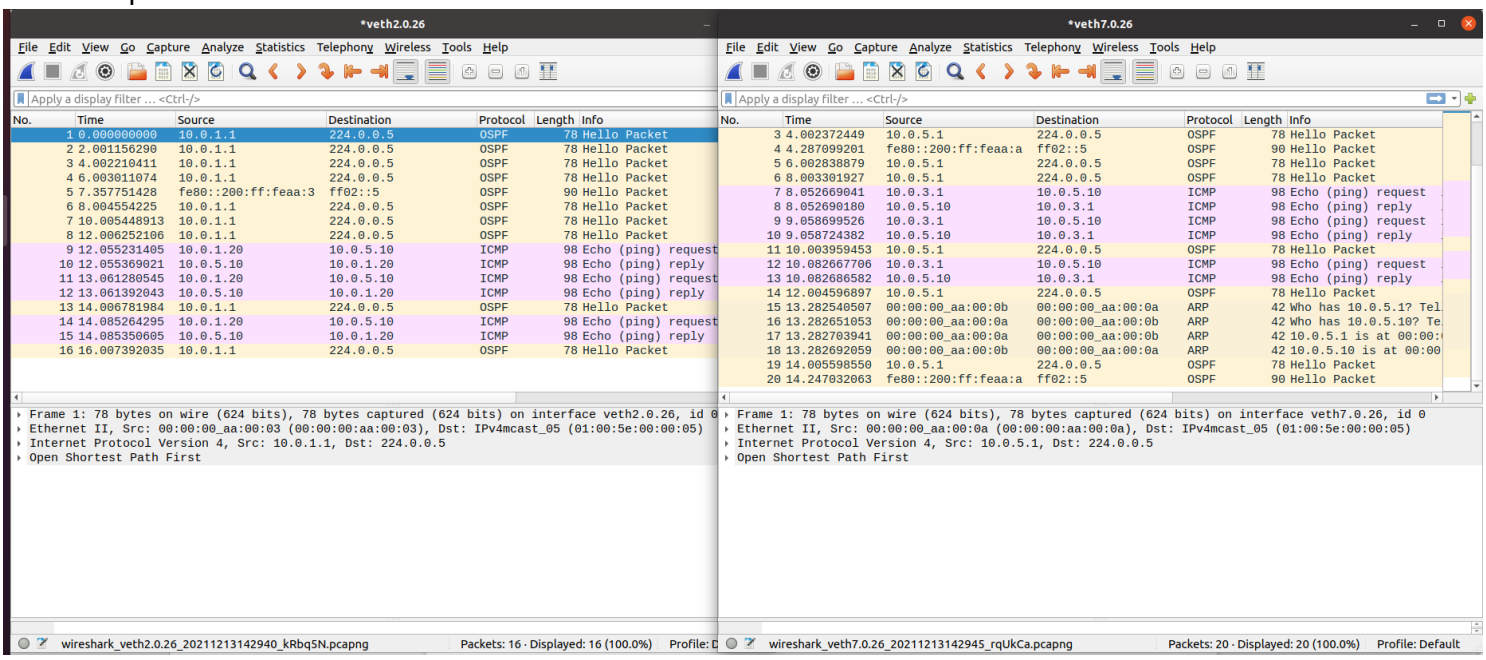
q3:
iptables -I INPUT -p TCP --dport 5000 -j ACCEPT
iptables -I INPUT -p TCP --dport 900 -s 10.0.5.10 -j ACCEPT

q4:



q5:
iptables -t NAT -A POSTROUTING -o eth3 -j MASQUERADE

q6:



Using ping, n7 thinks it is talking to n4, because there's a masket connection to n7 (right Wireshark window in screenshot). On the other side, n2 thinks it is talking directly to n7 (left Wireshark window in screenshot).

q7:
Temos de configurar as chains de PREROUTING e FORWARDING para o n4 saber de que forma tratar o packet que neste caso iria ser redirecionado da port 80 do n4 para a port 80 do n3.

q8:
iptables -A PREROUTING -t nat -i eth3 -p TCP --dport 80 -j DNAT --to 10.0.2.10:80
iptables -A FORWARD -p TCP -d 10.0.2.10 --dport 80 -j ACCEPT

q9:
No, port-forwarding is transparent, so n3 doesn't realize it is happening. It just sees the packets comming from n7.