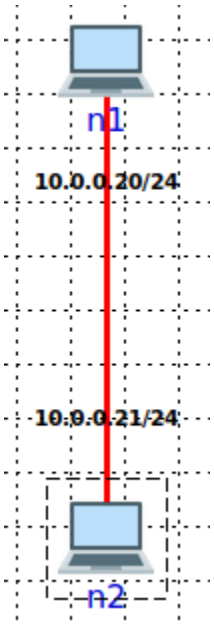
TLS Assignment

References:

- https://www.openssl.org/docs/man1.0.2/man1/openssl-s_client.html
- https://www.openssl.org/docs/man1.0.2/man1/openssl-s_server.html

Part 1: TLS (10 points)

Create the topology shown below in CORE:



1. Use openssl s_client and s_server to create the following configurations
   1.1. Use the script provided to generate X.509 certs.
   1.2. (1pts) Run a TLS1.2 server and a TLS1.2 client. Show the command you used on both and a screenshot of the TLS full handshake in Wireshark
   1.3. (1pts) Run a TLS1.3 server and a TLS1.2 client. Describe what happened. What Alert message type and what Level are generated?
   1.4. (1pts) Run a DTLS1.2 server and a DTLS1.2 client. Show a screenshot of the Hello Verify Request message with the cookie value.
   1.5. (2pts) Run a TLS1.2 server and a TLS1.2 client. Configure the server to request a certificate from the client. Configure the client with a cert and a private key.
      1.5.1. Show a screenshot of the certificate request from server, certificate from client, and certificate verify from the client.

1.6. Run a TLS1.2 server configured to use the cipher: ECDHE-RSA-AES256-GCM-SHA384 and a TLS1.2 client configured to use the cipher: DHE-RSA-AES256-GCM-SHA384.
    1.6.1. Hint: look at the output of openssl ciphers
    1.6.2. (1pt) Show the command you used
    1.6.3. (1pt) Describe what happened. What Alert message type and what Level are generated?
1.7. (1.5pts) Repeat 1.2 (do not show screenshot of handshake) but add a 10% packet loss to the link between the two nodes beforehand.
    1.7.1. Send 10 messages from client to server: “message 1“, “message 2”, …etc. Show a screenshot of the server terminal after 2 minutes of sending the last message showing the list of messages received.
1.8. (1.5pts) Repeat 1.4 (do not show screenshot of handshake) but add a 10% packet loss to the link between the two nodes beforehand.
    1.8.1. Send 10 messages from client to server: “message 1“, “message 2”, …etc. Show a screenshot of the server terminal after 2 minutes of sending the last message showing the list of messages received.