PA #4: TLS Chat Server

CST 311

Team 9

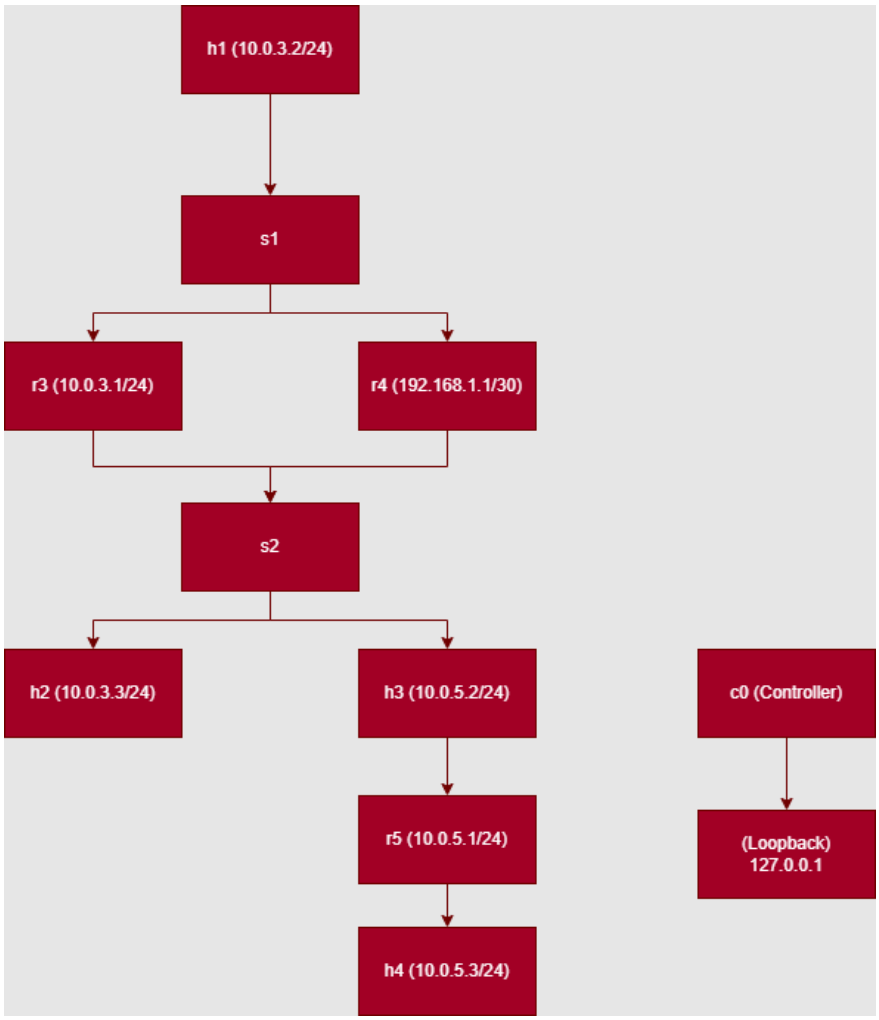
Dawn Petersen(Team Lead)
Nima Mahanloo
Armondo Lopez
Christopher Loi

October 21, 2023

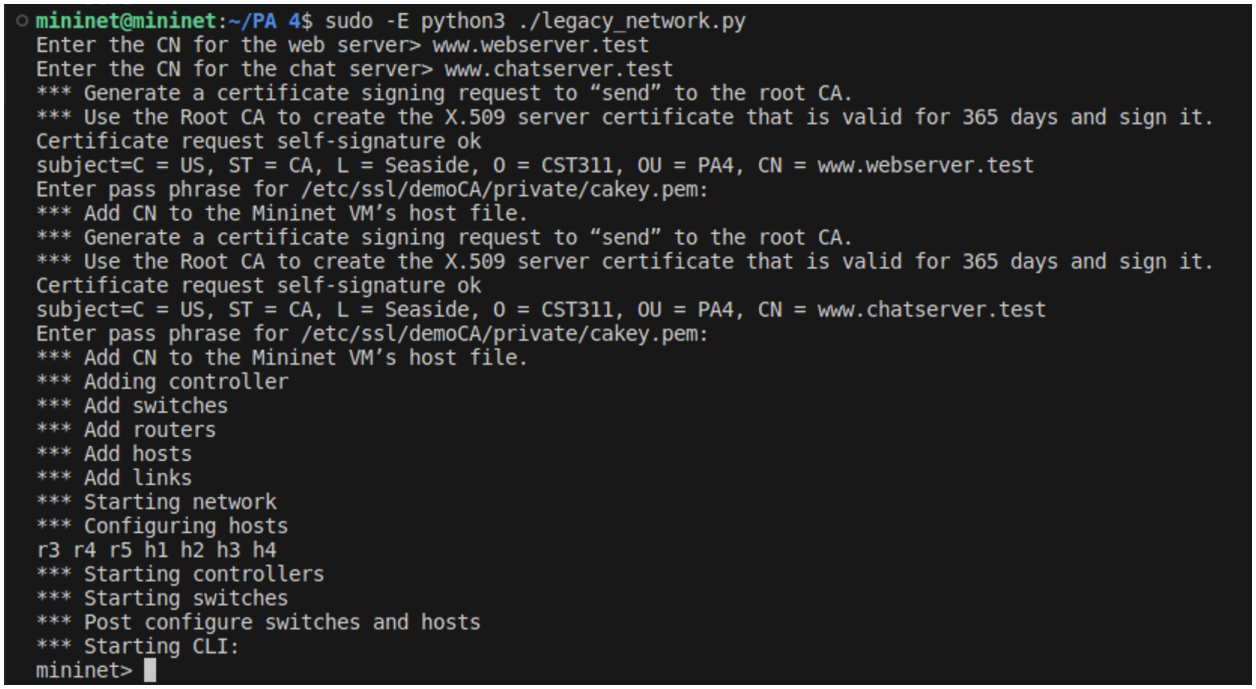
One Minute Meeting:

Nima was assigned to modify the legacy_network.py to create the network and be sure all nodes are pinging each other successfully. He also developed the certificate_issuer.py to automate the process of CA certificate creation entirely for both the simple webserver and the chat server. Dawn was assigned to modify legacy_network.py to create and run a simple TLS web server on Host 2. She also modified the PA3 project files to run a TLS-enabled chat server on Host 4 and two chat clients on Host 1 and 3 successfully. Armondo and Chris have been assigned to test everything, including the network, certificate issuer, certificates, web server, chatting process, and chat server and clients. They created all necessary screenshots and all required materials for the project report and made and handled that report document completely.

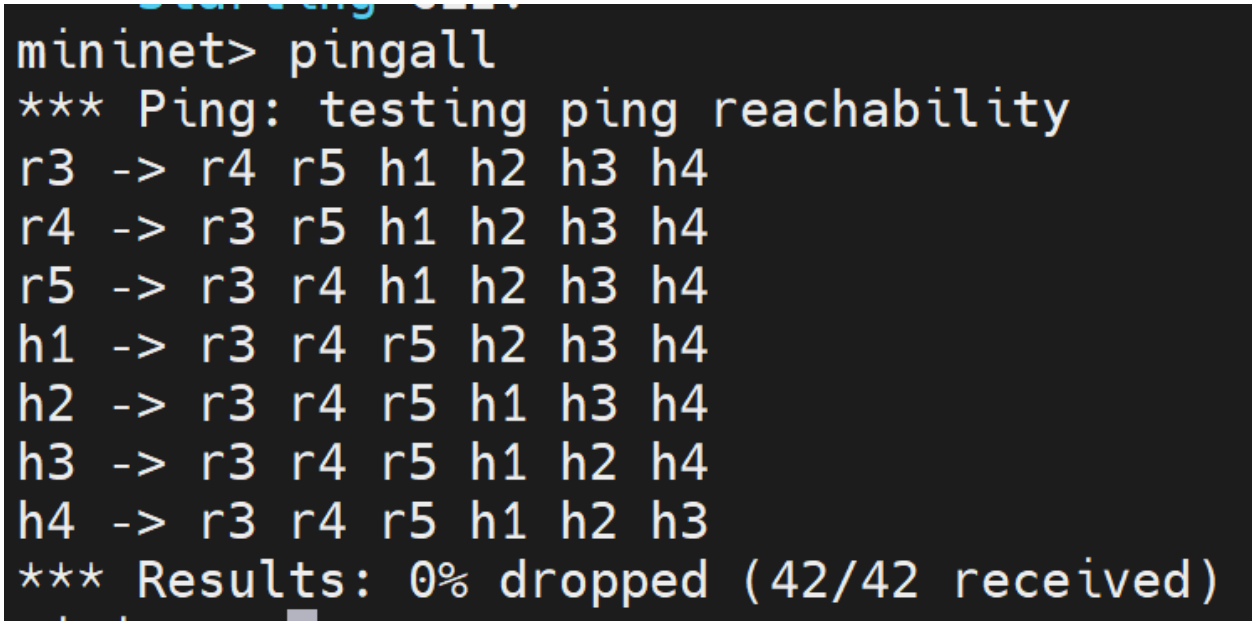
Draw and submit the network design with all interfaces labeled with interface names (e.g., s1-eth1) and interface IP addresses:



Screen capture of the program that runs with no Python errors.



Screen capture of successful pingall at the mininet> prompt:



A list of lines that were changed and why

- *h1 = net.addHost('h1', cls=Host, ip='10.0.0.1', defaultRoute=None)* to
  h1 = net.addHost('h1', ip='10.0.3.2/24', defaultRoute='via 10.0.3.1')
  REASON: We changed the subnet that h1 was in to better suit our needs for the assignment.
- *h2 = net.addHost('h2', cls=Host, ip='10.0.0.2', defaultRoute=None)* to
  h2 = net.addHost('h2', ip='10.0.3.3/24', defaultRoute='via 10.0.3.1')
  REASON: We changed the subnet that h2 was in to better suit our needs for the assignment.
- *h3 = net.addHost('h1', cls=Host, ip='10.0.0.3', defaultRoute=None)* to
  h3 = net.addHost('h3', ip='10.0.5.2/24', defaultRoute='via 10.0.5.1')
  REASON: We changed the subnet that h3 was in to better suit our needs for the assignment.
- *h4 = net.addHost('h2', cls=Host, ip='10.0.0.4', defaultRoute=None)* to
  h4 = net.addHost('h4', ip='10.0.5.3/24', defaultRoute='via 10.0.5.1')
  REASON: We changed the subnet that h4 was in to better suit our needs for the assignment.
- *net.addLink(r3, r4)* to
  net.addLink(r3, r4, intfName1='r3-eth2', intfName2='r4-eth1', params1={'ip':'192.168.1.2/30'}, params2={'ip':'192.168.1.3/30'})
  REASON: We were having trouble connecting these two routers together, so we tried to be as specific as we could in our code in order to connect them.
- *net.addLink(r4, r5)* to

net.addLink(r4, r5, intfName1='r4-eth2', intfName2='r5-eth2', params1={'ip':'192.168.2.1/30'}, params2={'ip':'192.168.2.2/30'})
REASON: We were having trouble connecting these two routers together, so we tried to be as specific as we could in our code in order to connect them.

What were any interesting findings and lessons learned?

Something that we had a lot of trouble with was that we could get r3 to connect with r4 and r4 to connect with r5, but we couldn't get r3 to connect to r5. We saw Professor Ogden about this issue and he was able to help us through it!

Why didn't the original program forward packets between the hosts?

The original program didn't forward packets between the hosts because the connections between the separate hosts hadn't been set up yet. We had to add the code in order for those packets to be sent between hosts.

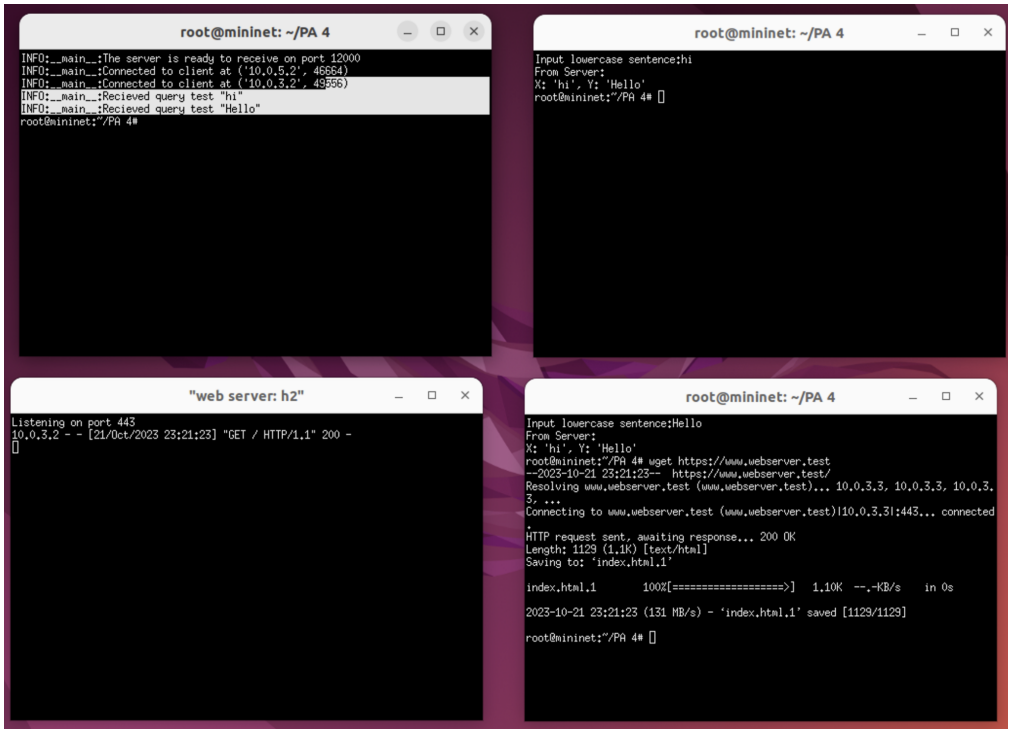
Is the line ' r3.cmd('sysctl -w net.ipv4.ip_forward=1') ' required?

Yes, this line is required because it sets up IP forwarding for r3, which is an essential task for routers.

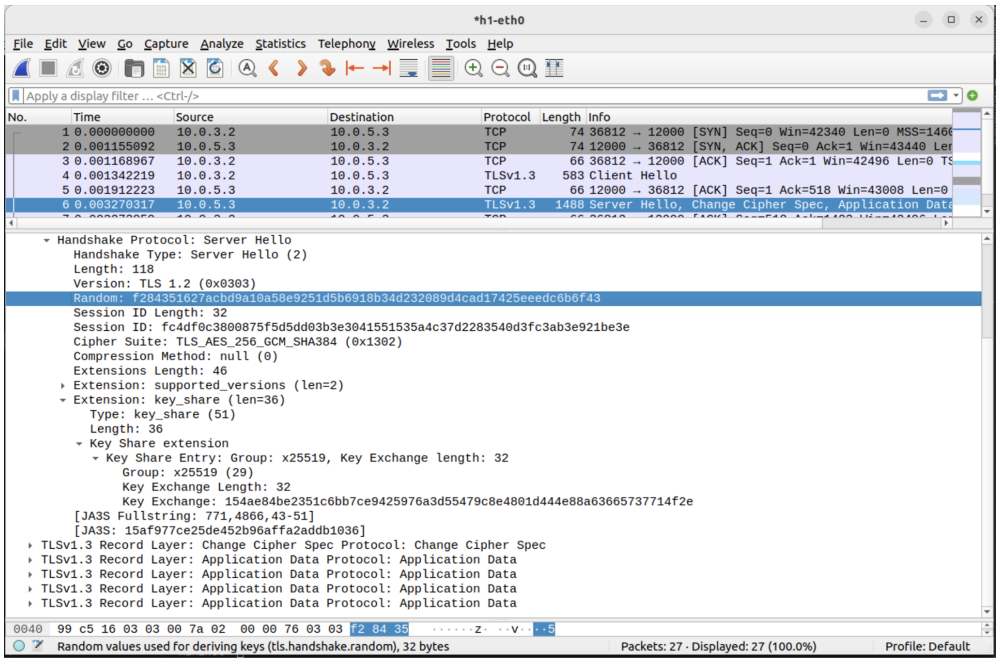
Intentionally break your working program, e.g.: change a subnet length, IP address, or default route for a host. Explain why your change caused the network to break.

This change caused the network to break because it caused two hosts to be in different subnets. This means that there wouldn't be a way for information to pass between hosts.

Screen capture of a successful chat session between the two chat clients



Screen capture of a Wireshark trace of the communication between a chat client and the chat server.



Screen capture of the successful wget (or curl) of the web server index file.

```
mininet> h1 wget h2
--2023-10-20 20:58:29--  http://10.0.3.3/
Connecting to 10.0.3.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 628 [text/html]
Saving to: 'index.html.2'

index.html.2        100%[===================>]     628  --.-KB/s    in 0s

2023-10-20 20:58:29 (1.45 MB/s) - 'index.html.2' saved [628/628]
```

Screenshot of decrypted server web certificates.

```
mininet@mininet:~/PA 4$ sudo cat webserver.test-cert.pem
-----BEGIN CERTIFICATE-----
MIIDXTCCAkUCFA/+jiDFv5qK4F3NwtuNhye5QZaAMA0GCSqGSIb3DQEBCwUAMG4x
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRMwEQYDVQQHDApTYWNy
YW1lbnRvMQwwCgYDVQQKDANTQ0QxDzANBgNVBAsMBkNTVDMxMTEWMBQGA1UEAwwN
Y2EuY3N1bWIudGVzdDAeFw0yMzEwMjIwMTUyMjNaFw0yNDEwMjEwMTUyMjNaMGgx
CzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTEQMA4GA1UEBwwHU2Vhc2lkZTEPMA0G
A1UECgwGQ1NUMzExMQwwCgYDVQQLDANQQTQxGzAZBgNVBAMMEnd3dy53ZWJzZXJ2
ZXIudGVzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJT4rE8d5y7C
L8d0X61B1U2uJZorOasovYsTiW0arrMlSQw41vXNnKVKPgXZHH0AQab7xI9JZQRl
Z0KlB4avzD8Czwc2RPe94uW1OyUkiwRLlaxtAwwgjo8Dgr4XonDQMQl3lXIBOy5F
+H8PAZd2mBFhEQ/LpavPu/velG5BV08mREt7dxPQ2jHgAu5JLummP4/zW4bibQVB
CAvZijcgXshTsMM8Igc/LlQuW9eZYhxBc75VipKgeNrlrix7MbG5JVKxOYhxt79u
A0KEnrvgmvF4Fp5pAOds0i6kjriggiQ0wJ0X0KMYZmWIf4aQ9HQyCw5RZOiSpjkG
Fuf9A+EoLfsCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEASQSQxKV6esO7Up7PWcS/
y2CAMEpsRrcC6W4CZbWRDVZm6Rzn6D5+ysj7ykFBS3BAatFkLy7qaoz7aGog9acG
1rUo+bcFdeTPJYwt+4yxYuIr3yQHNefri0XdQ5rHHqAJ9YtmmAdpdFjy+tpGk4+X
4ilnBMumb58fbE8y5jPerirWZmUyqeo+neLmrj2f61CcP/HcucAKlfT0cTtztdeA
d6YV7+wsepAPX/NcgL11U1HG/+xHdgkmQnbCmDOGSlHwCjSp+Z3n3z/CWScAiZ+Y
VxW9R8V/I/0AHnDR00NhX8Oh6V32s4svHO3FZnuiKJuaAqVT0pIQif6K+bPMaNva
QA==
-----END CERTIFICATE-----
mininet@mininet:~/PA 4$
```

Screenshot of decrypted server chat certificates.