

## **PA #4: TLS Chat Server**

CST 311

### **Team 9**

Dawn Petersen(Team Lead)

Nima Mahanloo

Armondo Lopez

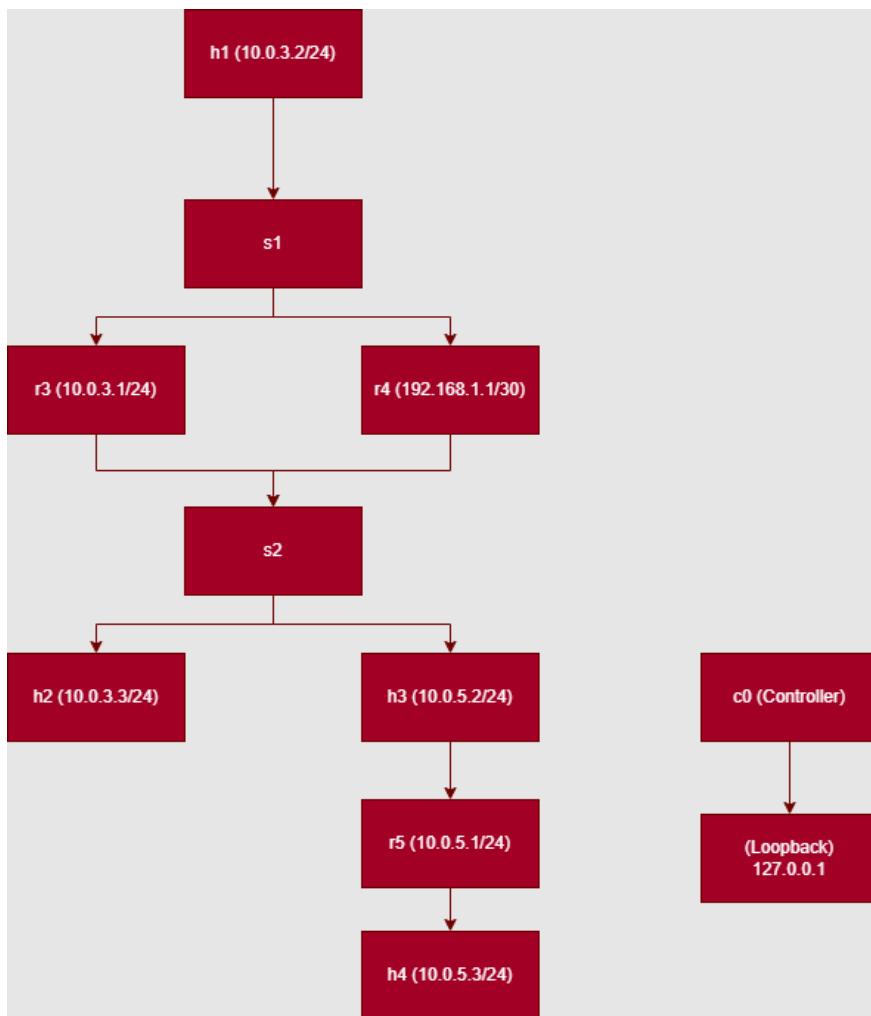
Christopher Loi

**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.

```
○ mininet@mininet:~/PA 4$ sudo -E python3 ./legacy_network.py
Enter the CN for the web server> www.webserver.test
Enter the CN for the chat server> www.chatserver.test
*** Generate a certificate signing request to "send" to the root CA.
*** Use the Root CA to create the X.509 server certificate that is valid for 365 days and sign it.
Certificate request self-signature ok
subject=C = US, ST = CA, L = Seaside, O = CST311, OU = PA4, CN = www.webserver.test
Enter pass phrase for /etc/ssl/demoCA/private/cakey.pem:
*** Add CN to the Mininet VM's host file.
*** Generate a certificate signing request to "send" to the root CA.
*** Use the Root CA to create the X.509 server certificate that is valid for 365 days and sign it.
Certificate request self-signature ok
subject=C = US, ST = CA, L = Seaside, O = CST311, OU = PA4, CN = www.chatserver.test
Enter pass phrase for /etc/ssl/demoCA/private/cakey.pem:
*** Add CN to the Mininet VM's host file.
*** Adding controller
*** Add switches
*** Add routers
*** Add hosts
*** Add links
*** Starting network
*** Configuring hosts
r3 r4 r5 h1 h2 h3 h4
*** Starting controllers
*** Starting switches
*** Post configure switches and hosts
*** Starting CLI:
mininet> █
```

Screen capture of successful pingall at the mininet> prompt:

```
mininet> pingall
*** Ping: testing ping reachability
r3 -> r4 r5 h1 h2 h3 h4
r4 -> r3 r5 h1 h2 h3 h4
r5 -> r3 r4 h1 h2 h3 h4
h1 -> r3 r4 r5 h2 h3 h4
h2 -> r3 r4 r5 h1 h3 h4
h3 -> r3 r4 r5 h1 h2 h4
h4 -> r3 r4 r5 h1 h2 h3
*** Results: 0% dropped (42/42 received)
```

### 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.

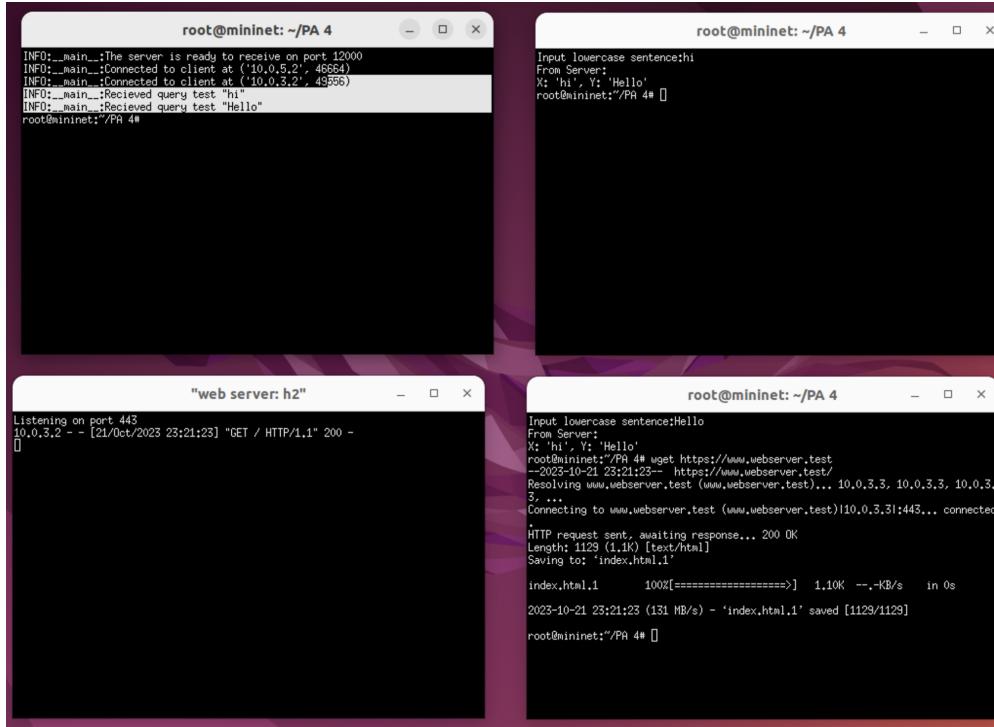
### **Is the line ' r3.cmd('sysctl -w net.ipv4.ip\_forward=1') ' required?**

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

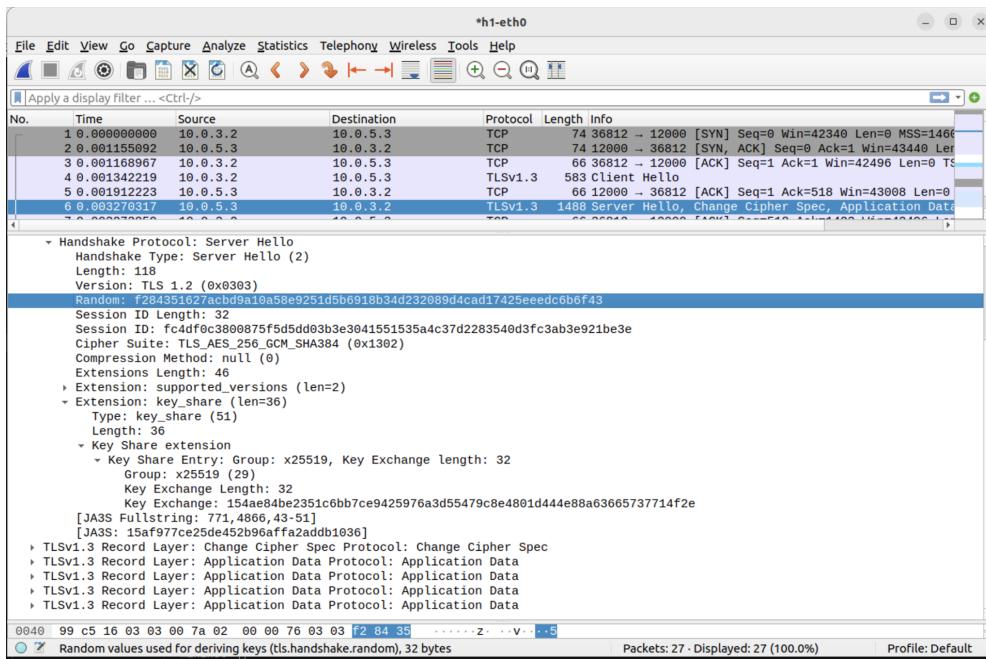
### **Intentionally break your working program, e.g.: change a subnet length, IP address, or default route for a host. Explain why your change caused the network to break.**

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
CzAJBgNVBAYTA1VTMRMwEQYDVQQIDAoDYWxpZm9ybmlhMRMwEQYDVQQHDApTYWNy
YW1lbRvMQwwCgYDVQQKDANTQ0QxDzANBgNVBAsMBkNTVDMxMTEWMBQGA1UEAwwN
Y2EuY3N1bWIudGVzdDAeFw0yMzEwMjIwMTUyMjNaFw0yNDEwMjEwMTUyMjNaMGgx
CzAJBgNVBAYTA1VTMQswCQYDVQQIDAJDQTEQMA4GA1UEBwwHU2Vhc2lkZTEPMA0G
A1UECgwGQ1NUMzExMQwwCgYDVQQLDANQQTQxGzAZBgNVBAMMEnd3dy53ZWJzzXJ2
ZXIudGVzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJT4rE8d5y7C
L8d0X61B1U2uJZorOasovYsTiW0arrMlsQw41vXNnKVKPgXZHH0AQab7xI9JZQRl
Z0Klb4avzD8CzwC2RPe94uW10yUkiwRllaxtAwwgjo8Dgr4XonDQMql3lXIB0y5F
+H8PAZd2mBFhEQ/LpavPu/velG5BV08mREt7dxPQ2jHgAu5JLummP4/zW4bibQVB
CAvZjcgXshTsMM8Igc/LlQuW9eZYhxBc75VipKgeNrlrix7MbG5JVKx0Yhxt79u
A0KEEnrvgmvF4Fp5pA0ds0i6kjriggiQ0wJ0X0KMYZmWIf4aQ9HQyCw5RZ0iSpjkG
Fuf9A+EoLfsCAwEAATANBgkqhkiG9w0BAQsFAA0CAQEASQSxKV6es07Up7PWcS/
y2CAMEpsRrcC6W4CzbWRDVZm6Rzn6D5+ysj7ykFBS3BAatFkLy7qaoz7aGog9acG
1rUo+bcFdeTPJYwt+4yxYuIr3yQHNeFri0XdQ5rHHqAJ9YtmmAdpdFjy+tpGk4+X
4ilnBMumb58fbE8y5jPerirWZmUyqeo+neLmrj2f61CcP/HcucAKlfT0cTtztdmA
d6YV7+wsepAPX/NcgL11U1HG/+xHdgkmQnbCmD0GSlHwCjSp+Z3n3z/CWSAiZ+Y
VxW9R8V/I/0AHnDR00NhX80h6V32s4svH03FZnuiKJuaAqVT0pIQif6K+bPMaNva
QA==
-----END CERTIFICATE-----
• mininet@mininet:~/PA 4$
```

### Screenshot of decrypted server chat certificates.

```
mininet@mininet:~/PA 4$ cat chatserver-cert.pem
-----BEGIN CERTIFICATE-----
MIIDVTCCAj0CFEXAh4hCr389P7cQNO2wQ2sC6fPBMA0GCSqGSIb3DQEBCwUAMG4x
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDAjDYWxpZm9ybmlhMRMwEQYDVQQHDApTYWNy
YW1lbnnRvMQwwCgYDVQQKDANTQ0QxDzANBAsMBkNTVDMxMTEWMBQGA1UEAwN
Y2EuY3N1bWIudGVzdDAeFw0yMzEwMjIwNDUxMTZaFw0yNDEwMjEwNDUxMTZaMGAx
CzAJBgNVBAYTAlVTMQswCQYDVQQIDAjDQTEQMA4GA1UEBwwHU2Vhc2lkZTEPMA0G
A1UECgwGQ1NUMzExMQwwCgYDVQQLDANQQTQxEzARBgNVBAMMCmNoYXRzzXJ2ZXiW
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCC226DjRzCnnxFssB7AvpG
B7kXl5A7LXc80chSwx0W2rVOWGpDqm1ISfIsyJgwS+kpl8oArymRgxLlySiEJPQV
3J0Tc0OpftnURC0m3zqsCsYXvs/KlkBMso70vT/dKbaxFxLYlsr0yK942kDcEvIl
guDsPbQUdoL8Ed5YpbbU7P7IXinybSKrmGtLXRd76Ds/wEyE/fFQcc781WrzB0i0
938QByoJQ1arXg0W0JN7KcCTITo0cdjZ5VCpwDSJb1mQeXUDIq4nPAcEEevK46+7
ZPg5YDfi45j9bMDWuIQD4hJ6FsnrCWLu49E8PHQtuhbBRB10ubhxpnWX8d9opaD
AgMBAAEwDQYJKoZIhvcNAQELBQADggEBAGiGtyV3VQ2b3MmhiqxZPdIeUjbvSAED
tGbhr7BQzVHhmaajKzrizsghlS7F5WuZ2jBHLLXKw9HYb+19UQCiu/2jPMvjnn0
B0dWIViis1xxWgmcW+aFojc6sJ0RqsLwAEYRFB05fvIcjXwE5GbfpVcYUz7NOS6bc
EWa8xF9WfVfaqJ8WoZSVsBvkxJhGcXFkdpYn3YmtZAp8LtiwWL4N5D84fEYH03EP
EN1I2kf3YDdqy5B2fS6Ch4ykNkt5ZcgGBEzl4DcEmbnnksZfin5jjzXQhjTDkW48
lGoJJBjuBP0MUAjsB3Rg3Kaq6Ey8CfHJheEBaytyPVA0zLIPGCWwe5Y=
-----END CERTIFICATE-----
mininet@mininet:~/PA 4$
```