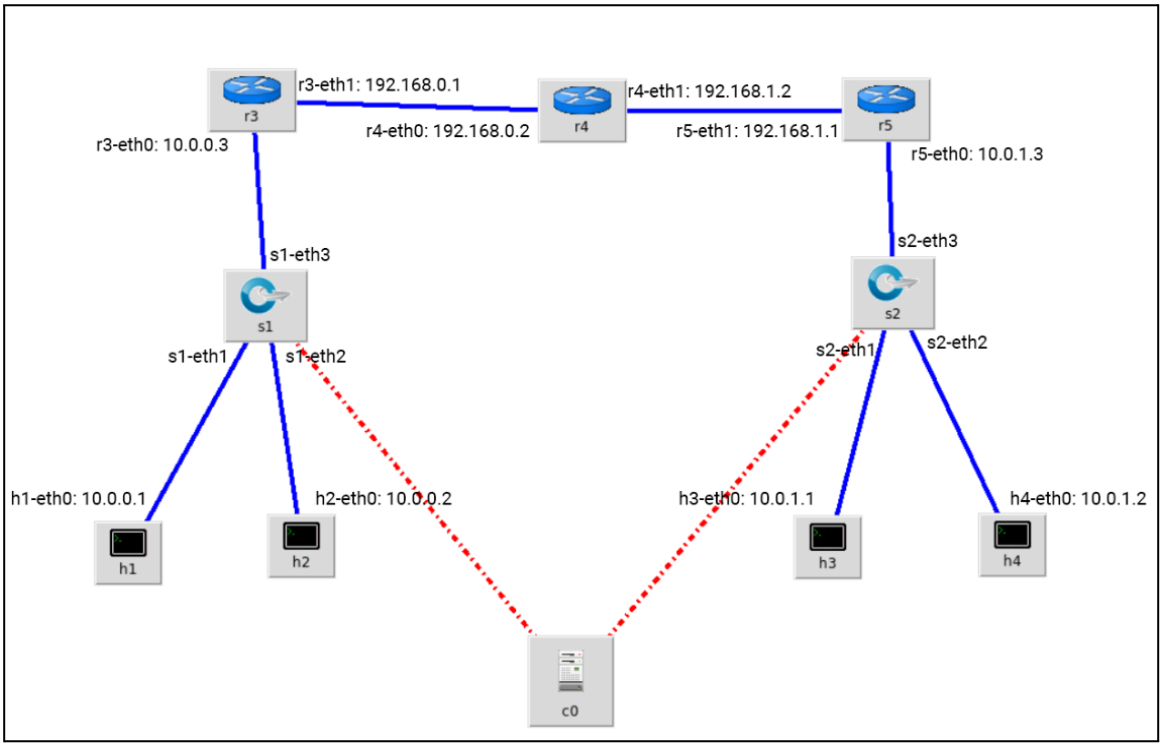
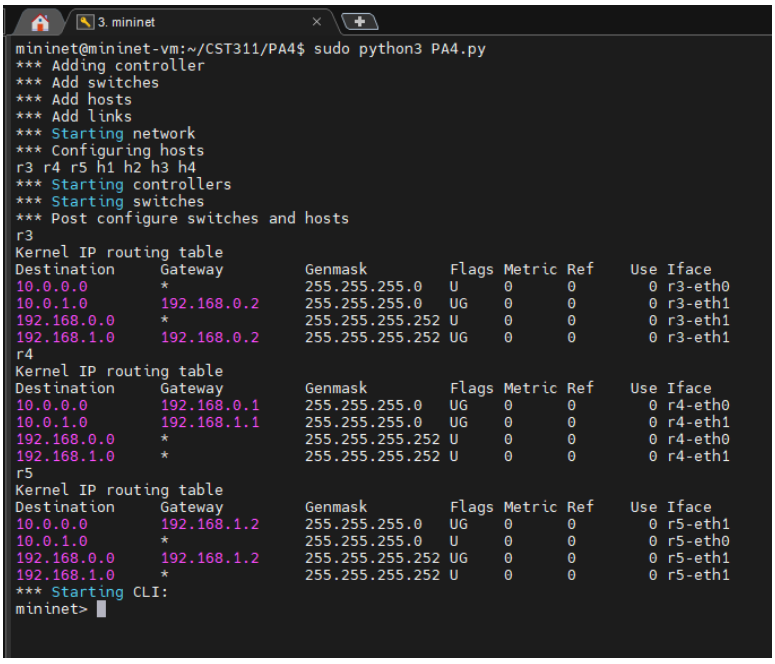
Pacific Analytics
Anna Bellizzi, David Debow, Justin Johnson, Ryan Parker

1. Network Design



2. Network Creation Script Run - No Errors



3. Successful pingall at the mininet› prompt

```
192.168.0.0     192.168.1.2     255.255.255.252 UG    0      0        0 r5-eth1
192.168.1.0     *               255.255.255.252 U     0      0        0 r5-eth1
*** Starting CLI:
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)
mininet>
```

4. Line changes in code

There are nine general line changes in the code, with six adjustments and three new additions.

In the import section, we added two new imports. For time.sleep we add import time. For the makeTerm pop-up window add import makeTerm. These imports are needed for sleep and makeTerm to work.

Adjusted values in the net declaration. Switch the CIDR number from 8 to 24 for ipBase = '10.0.0.0/8' to '10.0.0.0/24' Different subnets. To meet specifications.

We moved the add switches to above add host routers. Switch s1 and s2 need to be initialized before the add router host. Otherwise, errors are produced.

In the add host for router nodes. For r3, r4, r5. We gave the routers IP addresses besides 0.0.0.0. IP addresses match the topography of rX-eth0. Where x is 1,2, or 3, it is changed because it's not physically possible for those to have the same IP address of 0.0.0.0 and be three separate routers with different interfaces.

In the add host section we made changes for h1, h2, h3, h4. Rather than 10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.0.4, we split hosts on to two different subnets. Different routers connect them on different networks. Therefore two different subnets for h1, h2, and h3, h4 match the topography of these hosts being physically separated.

In the addlink section, we added arguments for some of the addlinks. Expand addlink for r3,s1 r5,s2 r3,r4 r5,r4. This is to define the links r3,s1 = r3-eth0, r5,s2 = r5-eth0, r3, r4 = r3-eth1, r4-eth0 and r5, r4 = r5-eth1, r4-eth1. This allows for travel across subnets.

Added a new line with router commands. Added trace IP routes for r3, r4, and r5. A total of six lines or two traceroutes for each router. The traceroutes make forwarding packets between the hosts possible. A sample command is r3.cmd('sudo ip route add 10.0.1.0/24 via 192.168.0.2 dev r3-eth1').

Added another new section to display traceroute information on r3, r4, and r5. It lists the destination, gateway, genmask, and interface. Trace route information is for debugging and quality of life.

Added a new section to call xterm to pop up three windows with one chat server and two chat clients running. This call reduces the interaction needed by the user.

5. Questions

a. *What were any interesting findings and lessons learned?*

   We learned that the xterm host terminal windows will not open, or will close if there is an error in the script.

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

   The original program did not forward packets between the hosts because there were no static routes, there were not two separate subnets, and all hosts were set to default IP addresses.

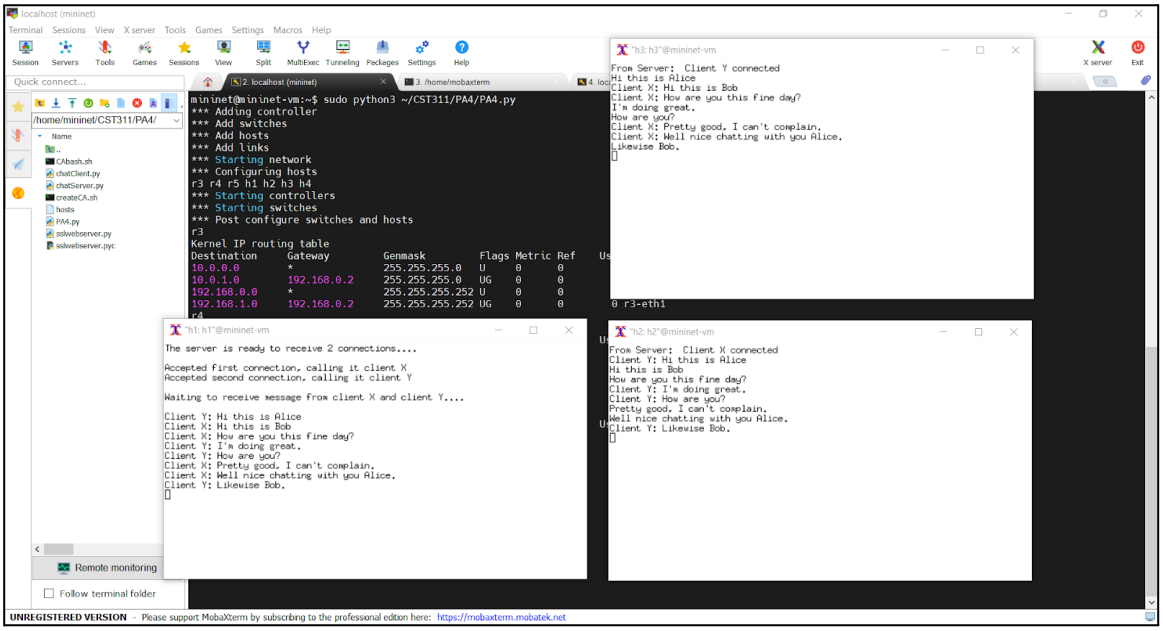
c. *Is the line ' r3.cmd('sysctl -w net.ipv4.ip_forward=1') ' required?*

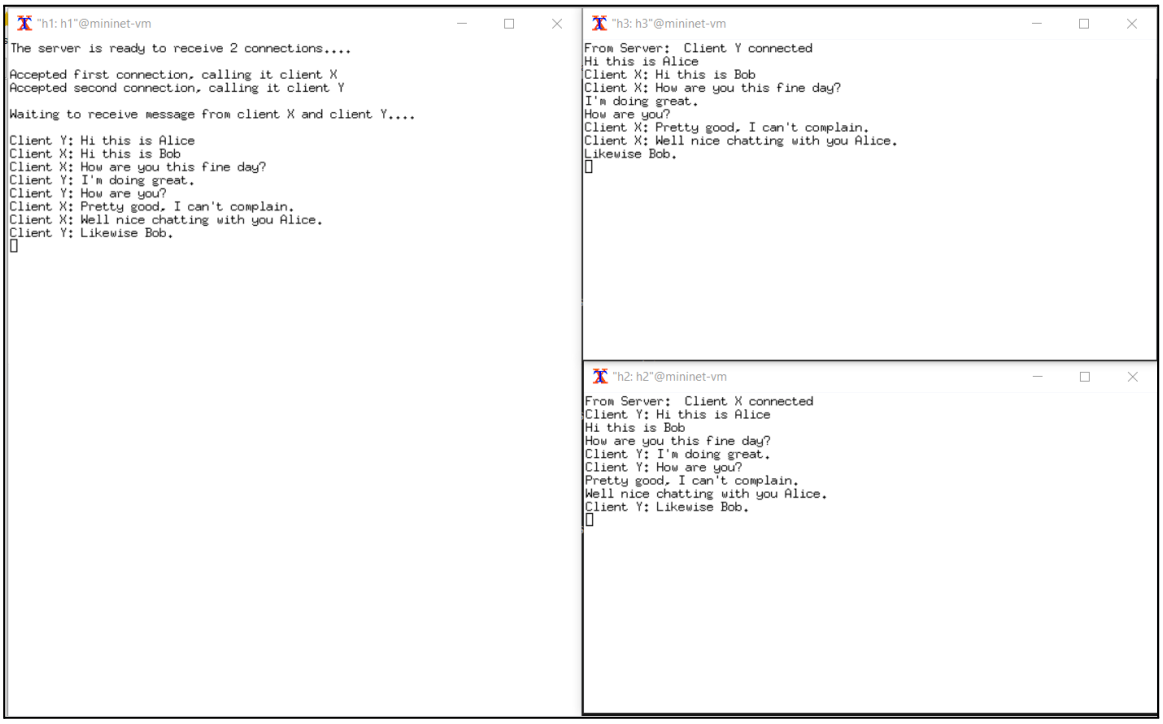
   Yes, it is required.

d. *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.*

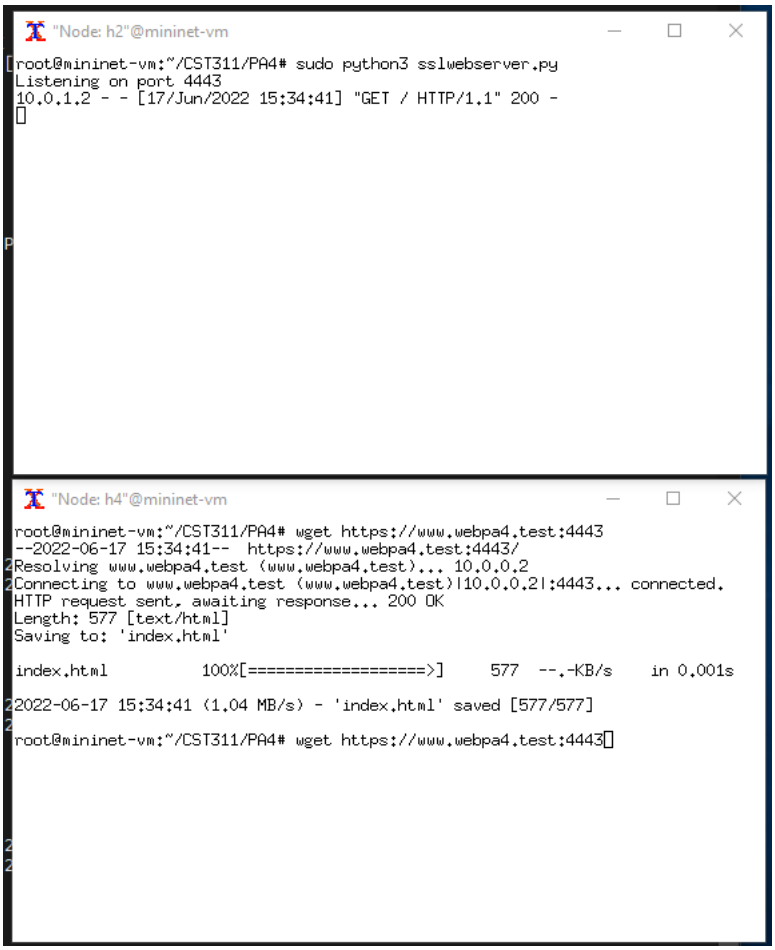
   If eth0 and eth1 of r4 are assigned 10.0.x.x addresses, the two subnets can not communicate.

6. Successful Chat Session





7. Successful wget of webserver index file



8. Decrypted Web Certificates

```
DECRYPTED  ROOT CERT
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d9:26:12:9e:ab:b6:8c:46
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=ca.cst311.test
        Validity
            Not Before: Jun 17 03:10:02 2022 GMT
            Not After : Jun 16 03:10:02 2027 GMT
        Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=ca.cst311.test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9f:b5:f2:89:6c:a2:ad:d5:a0:06:88:16:4a:f4:
                    41:87:c1:01:b1:4d:f2:45:7a:51:83:ca:da:32:c7:
                    06:ed:25:cb:d1:b2:fc:1c:08:f9:63:a5:91:4d:03:
                    97:0d:6e:97:9f:4c:a8:c9:b5:68:74:9a:c5:63:5b:
                    de:e7:bd:f9:4d:ad:7f:31:24:ac:fb:58:72:60:e5:
                    74:4c:43:19:e7:f9:30:5a:63:20:23:bf:d3:2d:58:
                    5c:24:e7:ea:b6:17:70:98:9a:a2:b0:15:8b:24:fd:
                    84:85:74:ee:78:cd:ed:24:6e:a7:9b:b2:58:e6:6d:
                    9a:cc:4e:51:51:93:a3:1f:f7:3f:01:d2:ed:a3:df:
                    08:fd:0c:9a:4c:fe:20:4f:dd:b6:6d:a9:2a:38:47:
                    23:1f:c3:12:14:0e:a7:b0:ba:91:63:c4:f8:0b:94:
                    30:53:a9:a0:c6:f6:9e:a7:c8:63:be:52:a1:55:fd:
                    19:82:5b:3c:2a:89:f3:34:83:3a:ad:2a:08:92:5a:
                    51:e9:33:52:a0:72:d9:e9:5e:7e:5c:6e:c1:8e:bd:
                    83:6e:a0:ed:ec:28:41:8f:1d:68:42:6c:9a:91:39:
                    65:e3:80:be:f1:d3:18:66:f8:4d:a3:95:71:03:c3:
                    d1:cb:4b:1a:b4:87:9c:0b:1d:04:e3:51:c2:37:30:
                    fe:db
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                96:6F:64:17:F3:2F:7F:81:3C:61:05:96:9B:31:9C:86:4A:04:88:6C
            X509v3 Authority Key Identifier:
                keyid:96:6F:64:17:F3:2F:7F:81:3C:61:05:96:9B:31:9C:86:4A:04:88:6C

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         9a:ef:48:5d:f6:21:f7:8b:8d:66:77:ec:83:bf:06:d8:51:b9:
         97:de:3f:93:5d:6c:5b:b4:9a:66:f6:30:d1:6b:af:65:f3:38:
         80:ef:31:48:f5:f9:e1:ac:f5:a6:35:2e:47:70:43:c0:d6:bb:
         1c:2b:6d:3a:b9:53:31:d4:33:1e:b6:1e:9c:68:83:aa:36:c5:
         45:96:56:57:9a:37:09:db:36:89:a5:e5:f8:3e:38:19:5b:9a:
         b2:c4:58:ca:dc:5a:23:a7:ec:c6:82:ce:79:b5:ce:74:45:39:
         04:53:34:6a:e9:ea:31:aa:14:62:ce:46:f5:49:55:18:27:0c:
         07:96:63:8c:57:1d:4c:51:3b:ec:52:ec:2f:04:83:3f:36:9a:
         26:ee:0e:44:70:a9:0e:f2:76:b8:91:de:ea:02:7a:04:ca:e2:
         bf:5e:99:48:05:2f:cc:4d:6e:19:81:bb:1b:1b:17:1f:bd:42:
         a6:32:42:b3:e9:df:c8:64:57:0b:4a:73:0c:8f:6b:a8:bc:44:
         c2:35:bb:52:cc:82:9f:e8:12:f5:84:e4:de:30:a1:c8:94:a4:
         2b:25:12:83:5e:c2:61:56:98:0e:10:37:6e:8f:42:e3:06:17:
         2c:b7:ac:4d:0a:5f:3e:4d:e2:39:90:18:ee:07:11:e0:29:8e:
         ac:6c:8b:a2
moved cakey.pem to private directory
```

```
You have created a server certificate, that is valid for one year, and signed it with your CA certific
ate
Decrypted Server Cert
GET A SCREEN SHOT FOR SUBMISSION
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            d5:6b:e1:bd:fc:5b:a7:0b
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=ca.cst311.test
        Validity
            Not Before: Jun 17 03:10:04 2022 GMT
            Not After : Jun 17 03:10:04 2023 GMT
        Subject: C=US, ST=CA, L=Seaside, O=CST311, OU=Networking, CN=www.webpa4.test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9c:42:c0:c5:23:65:9e:3c:89:3c:67:a2:24:31:
                    8a:b3:02:ae:df:ac:33:50:99:c5:36:a1:2e:57:8c:
                    67:33:df:6f:77:f6:a2:4d:34:e3:23:e7:07:97:2f:
                    c3:ea:30:ff:2b:c6:8b:19:6f:5e:86:0b:f2:f7:37:
                    5d:4f:56:e1:ac:bb:ca:18:50:d8:e3:e5:1f:5a:3d:
                    06:a9:7e:f1:a6:0a:87:0b:bf:21:d8:9e:e2:cc:b5:
                    42:94:47:e0:03:20:36:cc:ce:a7:8c:f6:ec:07:1f:
                    48:e2:b7:81:d9:11:e0:df:8d:2b:a0:93:12:16:88:
                    cc:cc:33:ac:ba:e5:2f:69:64:3c:9c:8c:38:9f:9c:
                    01:ea:7a:e0:56:3b:d6:04:e8:77:ac:45:62:09:ed:
                    84:1d:d9:fd:78:21:93:c7:46:6f:40:6d:af:70:95:
                    1a:48:b5:07:83:76:d9:43:08:cf:e4:f2:5a:d4:1f:
                    7a:4a:f6:fc:0f:b0:eb:48:38:93:39:c3:5a:ad:11:
                    a9:cb:64:66:94:e7:9d:6d:de:8e:93:58:e5:11:7d:
                    df:3d:db:96:3d:d9:b4:0a:78:15:77:e7:de:49:c2:
                    68:28:6d:6e:5a:86:93:34:5f:15:c2:d5:a9:cd:90:
                    92:c2:8f:77:56:89:25:b8:9b:4c:4e:0c:95:2c:bd:
                    bf:29
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         43:d9:fa:32:e5:4f:cd:f4:44:87:7b:4a:44:a5:fe:6e:78:38:
         6b:d7:5c:54:9e:41:50:4e:ab:72:e4:33:64:9b:62:30:51:01:
         31:a9:f0:3f:a9:bb:66:eb:38:0d:f2:59:1c:25:2e:73:df:4c:
         0f:93:dc:ed:47:54:b4:5a:ab:28:4a:a9:65:cd:d5:5d:c9:0a:
         c4:be:72:d7:a9:ec:76:62:28:65:0a:3c:d8:c4:2a:0b:98:03:
         c5:da:46:9a:71:5e:93:04:ce:f3:c6:18:76:db:35:93:a5:2b:
         ee:82:b4:f5:64:77:49:e4:26:bb:1e:6a:44:e1:0e:11:9f:83:
         6b:8c:76:b8:16:ca:b0:97:47:91:65:32:77:c0:e7:73:87:2e:
         44:8f:83:49:77:3e:4a:fb:3b:b6:1c:df:c2:1e:b5:5b:b8:2d:
         49:b2:99:17:a6:b5:34:f4:15:01:f4:a5:d4:ae:bb:32:51:24:
         dc:7c:ce:3f:d5:ec:b6:dc:cc:4d:07:fa:f2:88:d8:9e:b7:bc:
         bb:07:d5:4f:43:30:ff:d4:05:ce:54:8b:fe:8a:9f:fb:4f:df:
         94:1b:d5:ca:48:81:2b:c4:e3:5a:ea:20:76:c4:0c:5a:fe:7f:
         05:b0:64:09:6d:68:bd:ab:bc:f1:ed:1c:0c:7d:3f:21:72:ac:
         82:55:f1:d3
mininet@mininet-vm:~/CST311$ host www.webpa4.test
```