RIT | جامعة روتشستر الأمريكية للتكنولوجيا في دبي
A Global American University in Dubai

NSSA Lab - 04

Suhaila Alfalasi

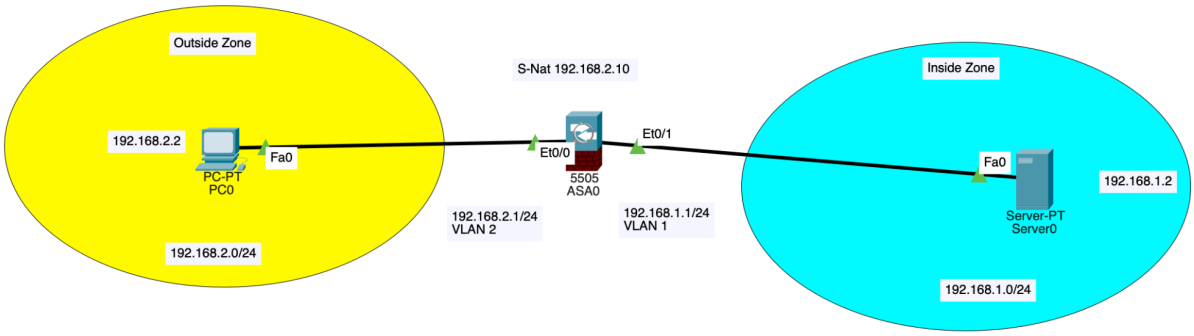
Rania Kanaan

RIT Dubai

Professor Muhammad Haseeb Jalalzai

April 18, 2024

1. (2pts) Submit a screenshot of the Packet Tracer network topology. Each network interface should be labelled with port number and IP address.



This displays the configuration of the network, complete with the web server, PC, and Cisco ASA 5505 firewall.

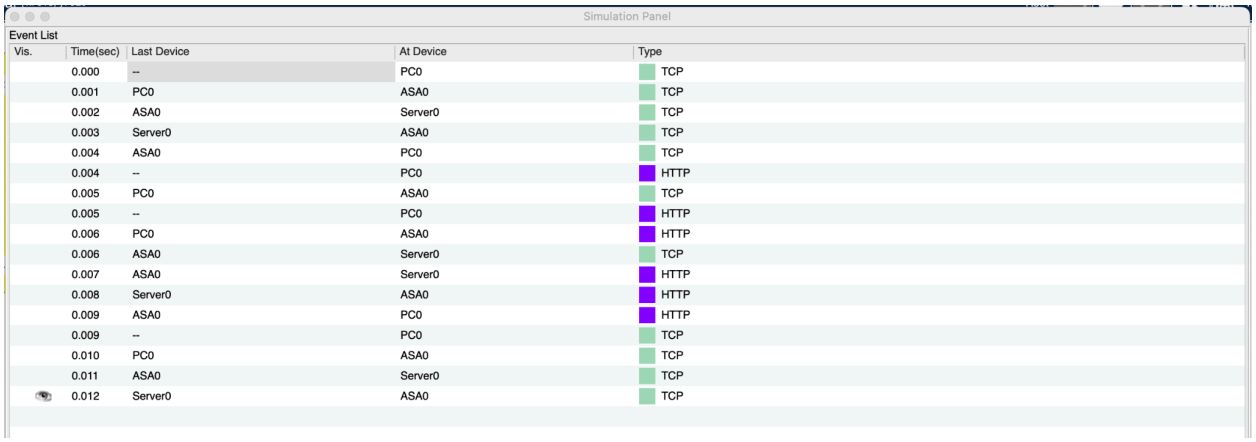
2. (2pts) Submit screenshots showing (i) PC0 can ping and traceroute to the web server, and (ii) PC0's web browser can successfully download a web page from web server.

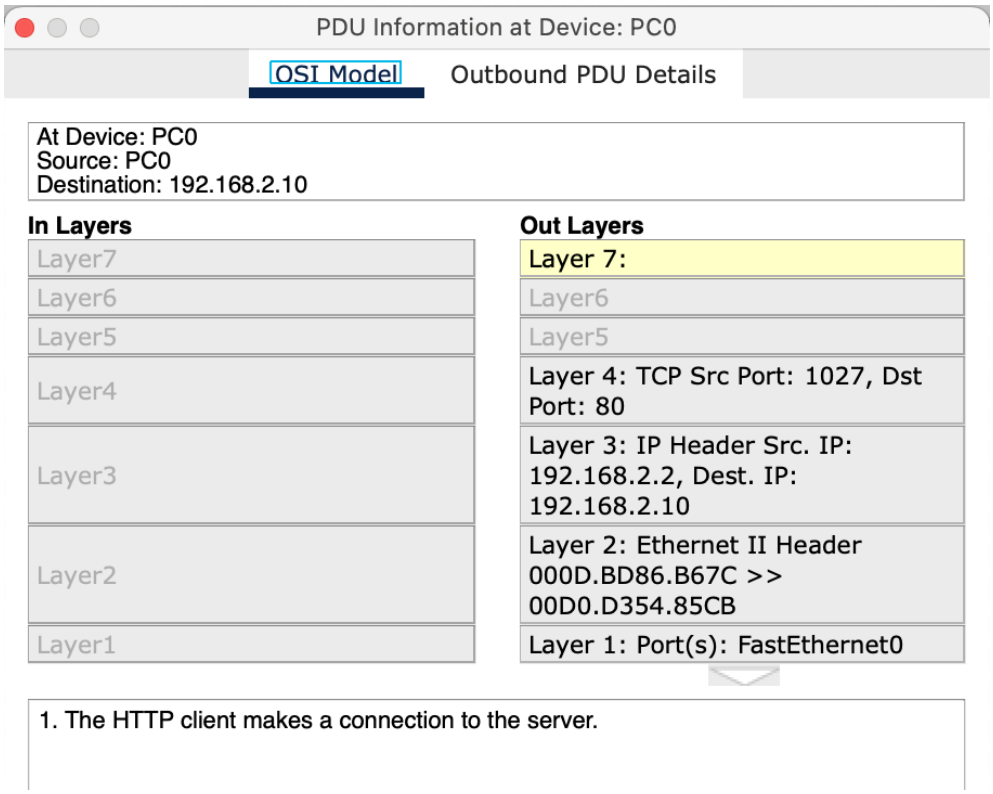
```
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time=32ms TTL=127
Reply from 192.168.2.10: bytes=32 time=37ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 37ms, Average = 17ms
```

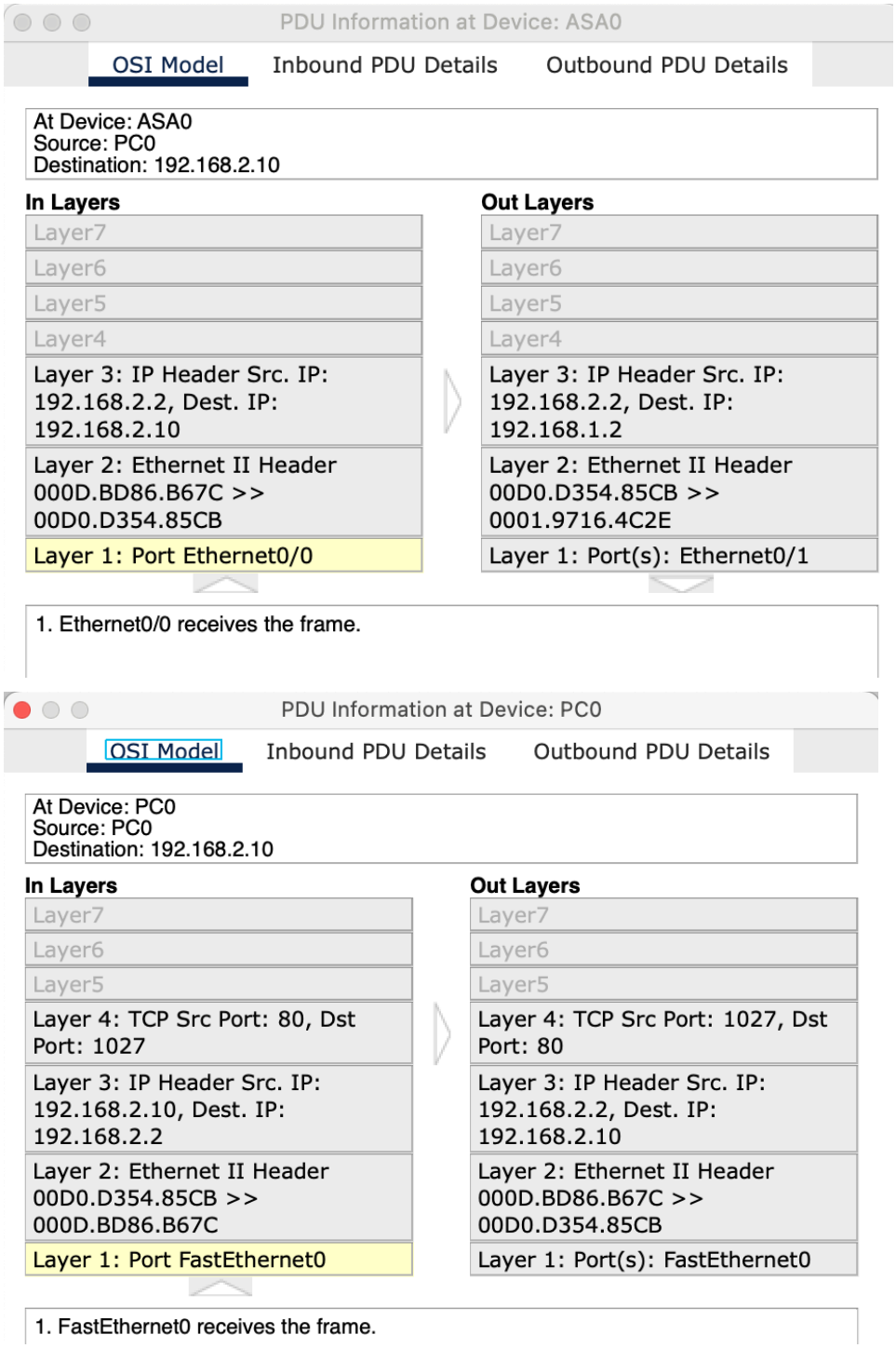
These pictures show that the network is set up correctly, enabling PC0 to use HTTP (web browser) and ICMP (ping and traceroute) to connect with the web server.

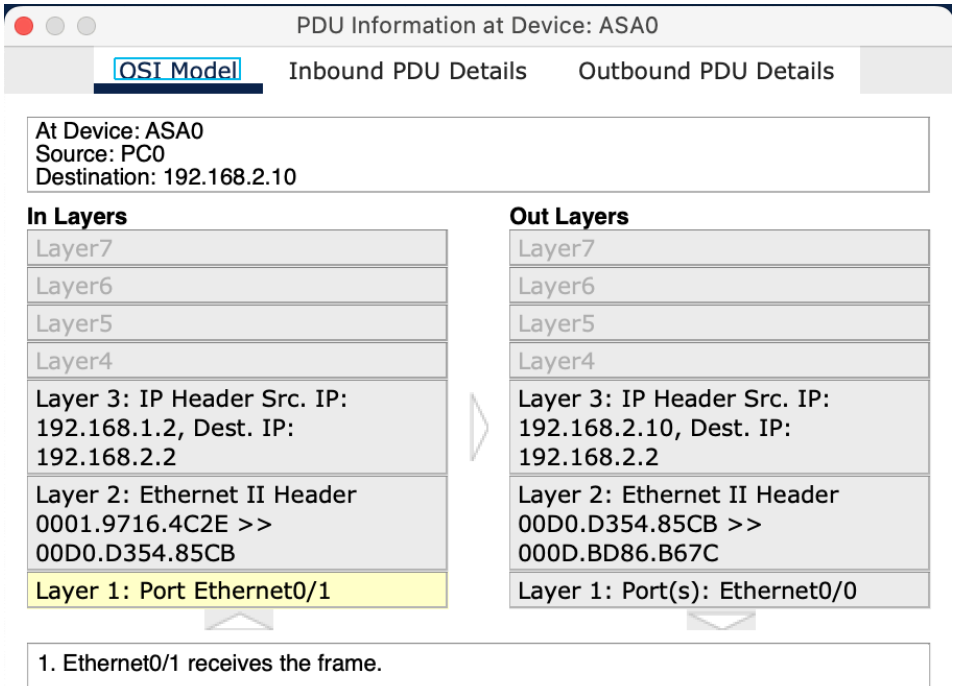
3. (2pts) In Simulation mode, capture and decode web traffic (i) from PC0 to ASA5505 firewall, and (ii) from ASA5505 firewall to web server. Submit screenshots of the decoded

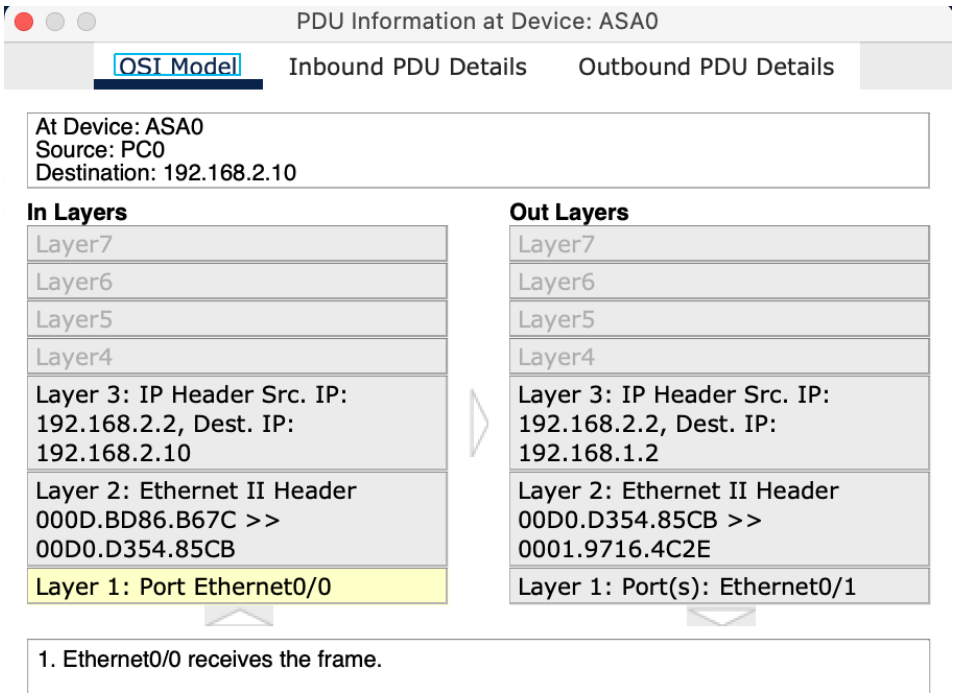
IP and TCP header fields within the packets and circle the field in the two packets that shows the IP address prior to and after NAT translation.






PDU Information at Device: ASA0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: ASA0
Source: PC0
Destination: 192.168.2.10
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.2.10
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.1.2
Layer 2: Ethernet II Header 000D.BD86.B67C >> 00D0.D354.85CB
Layer 2: Ethernet II Header 00D0.D354.85CB >> 0001.9716.4C2E
Layer 1: Port Ethernet0/0
Layer 1: Port(s): Ethernet0/1
1. Ethernet0/0 receives the frame.
PDU Information at Device: PC0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: PC0
Source: PC0
Destination: 192.168.2.10
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 80, Dst Port: 1027
Layer 4: TCP Src Port: 1027, Dst Port: 80
Layer 3: IP Header Src. IP: 192.168.2.10, Dest. IP: 192.168.2.2
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.2.10
Layer 2: Ethernet II Header 00D0.D354.85CB >> 000D.BD86.B67C
Layer 2: Ethernet II Header 000D.BD86.B67C >> 00D0.D354.85CB
Layer 1: Port FastEthernet0
Layer 1: Port(s): FastEthernet0
1. FastEthernet0 receives the frame.


PDU Information at Device: ASA0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: ASA0
Source: PC0
Destination: 192.168.2.10
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.2.2
Layer 3: IP Header Src. IP: 192.168.2.10, Dest. IP: 192.168.2.2
Layer 2: Ethernet II Header 0001.9716.4C2E >> 00D0.D354.85CB
Layer 2: Ethernet II Header 00D0.D354.85CB >> 000D.BD86.B67C
Layer 1: Port Ethernet0/1
Layer 1: Port(s): Ethernet0/0
1. Ethernet0/1 receives the frame.


PDU Information at Device: ASA0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: ASA0
Source: PC0
Destination: 192.168.2.10
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.2.10
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.1.2
Layer 2: Ethernet II Header 000D.BD86.B67C >> 00D0.D354.85CB
Layer 2: Ethernet II Header 00D0.D354.85CB >> 0001.9716.4C2E
Layer 1: Port Ethernet0/0
Layer 1: Port(s): Ethernet0/1
1. Ethernet0/0 receives the frame.

PDU Information at Device: PC0

OSI Model | Outbound PDU Details

At Device: PC0
Source: PC0
Destination: HTTP CLIENT

In Layers	Out Layers
Layer7	Layer 7: HTTP
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1027, Dst Port: 80
Layer3	Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.2.10
Layer2	Layer 2: Ethernet II Header 000D.BD86.B67C >> 00D0.D354.85CB
Layer1	Layer 1: Port(s):

1. The HTTP client sends a HTTP request to the server.

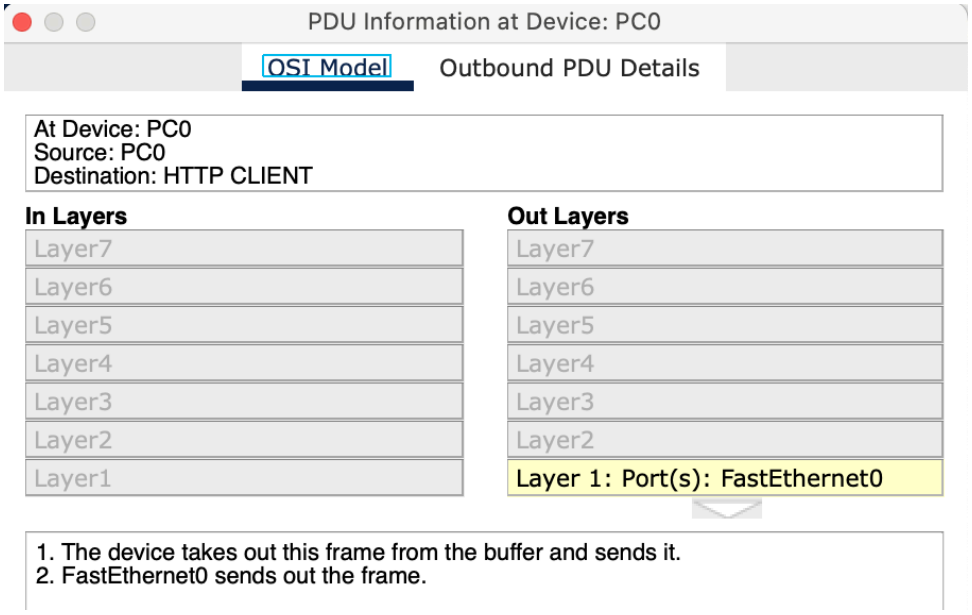
PDU Information at Device: ASA0

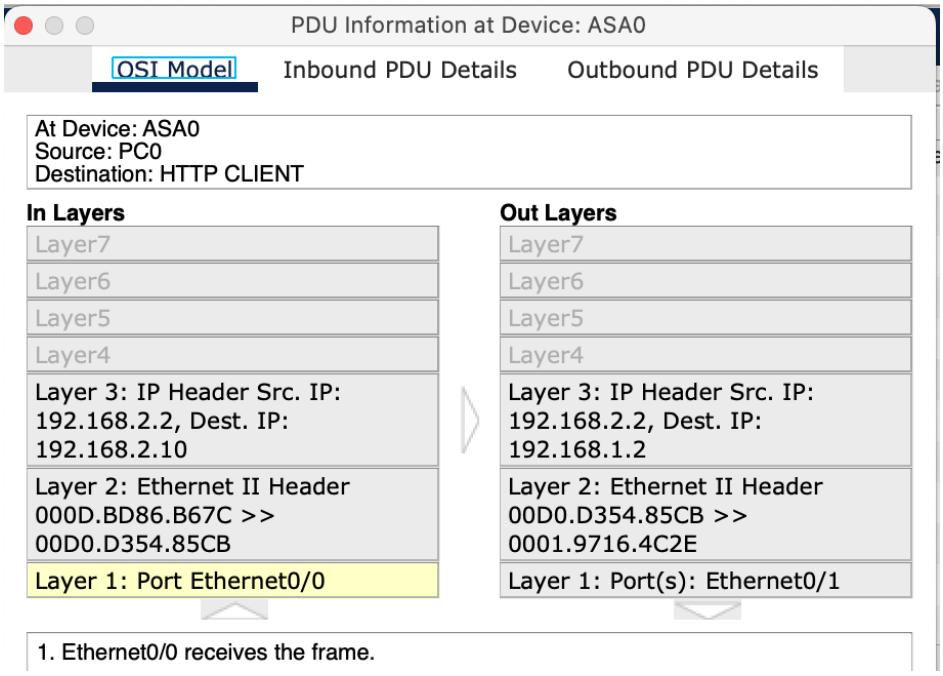
OSI Model | Inbound PDU Details | Outbound PDU Details

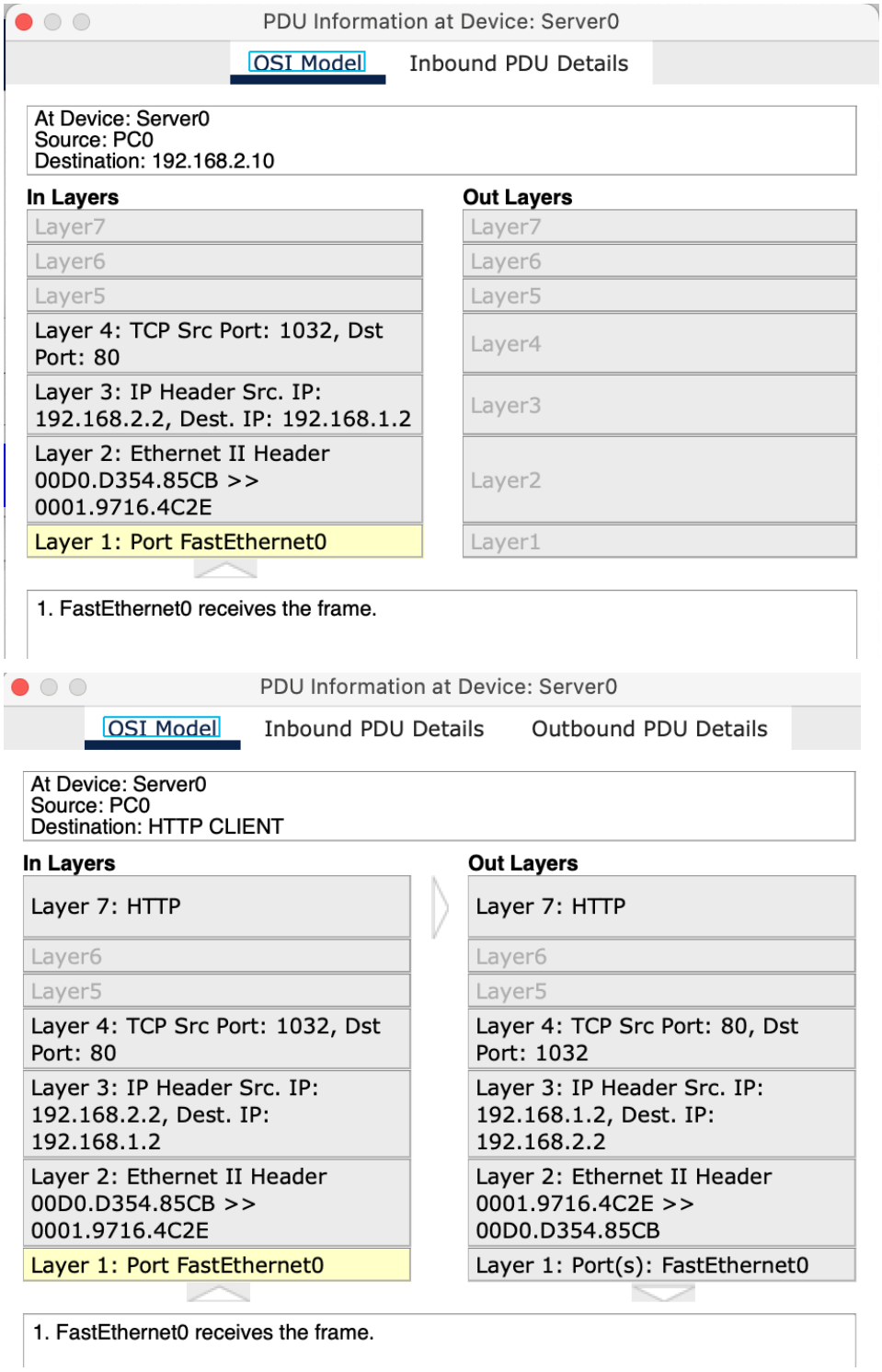
At Device: ASA0
Source: PC0
Destination: 192.168.2.10

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.2.10	Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.1.2
Layer 2: Ethernet II Header 000D.BD86.B67C >> 00D0.D354.85CB	Layer 2: Ethernet II Header 00D0.D354.85CB >> 0001.9716.4C2E
Layer 1: Port Ethernet0/0	Layer 1: Port(s): Ethernet0/1

1. Ethernet0/0 receives the frame.


PDU Information at Device: PC0
OSI Model
Outbound PDU Details
At Device: PC0
Source: PC0
Destination: HTTP CLIENT
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1
Layer 1: Port(s): FastEthernet0
1. The device takes out this frame from the buffer and sends it.
2. FastEthernet0 sends out the frame.


PDU Information at Device: ASA0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: ASA0
Source: PC0
Destination: HTTP CLIENT
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.2.10
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.1.2
Layer 2: Ethernet II Header 000D.BD86.B67C >> 00D0.D354.85CB
Layer 2: Ethernet II Header 00D0.D354.85CB >> 0001.9716.4C2E
Layer 1: Port Ethernet0/0
Layer 1: Port(s): Ethernet0/1
1. Ethernet0/0 receives the frame.


PDU Information at Device: Server0
OSI Model
Inbound PDU Details
At Device: Server0
Source: PC0
Destination: 192.168.2.10
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 1032, Dst Port: 80
Layer4
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.1.2
Layer3
Layer 2: Ethernet II Header 00D0.D354.85CB >> 0001.9716.4C2E
Layer2
Layer 1: Port FastEthernet0
Layer1
1. FastEthernet0 receives the frame.
PDU Information at Device: Server0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Server0
Source: PC0
Destination: HTTP CLIENT
In Layers
Out Layers
Layer 7: HTTP
Layer 7: HTTP
Layer6
Layer5
Layer 4: TCP Src Port: 1032, Dst Port: 80
Layer 4: TCP Src Port: 80, Dst Port: 1032
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.1.2
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.2.2
Layer 2: Ethernet II Header 00D0.D354.85CB >> 0001.9716.4C2E
Layer 2: Ethernet II Header 0001.9716.4C2E >> 00D0.D354.85CB
Layer 1: Port FastEthernet0
Layer 1: Port(s): FastEthernet0
1. FastEthernet0 receives the frame.

PDU Information at Device: Server0

OSI Model | Inbound PDU Details

At Device: Server0
Source: PC0
Destination: 192.168.2.10

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 1032, Dst Port: 80	Layer4
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.1.2	Layer3
Layer 2: Ethernet II Header 00D0.D354.85CB >> 0001.9716.4C2E	Layer2
Layer 1: Port FastEthernet0	Layer1

1. FastEthernet0 receives the frame.

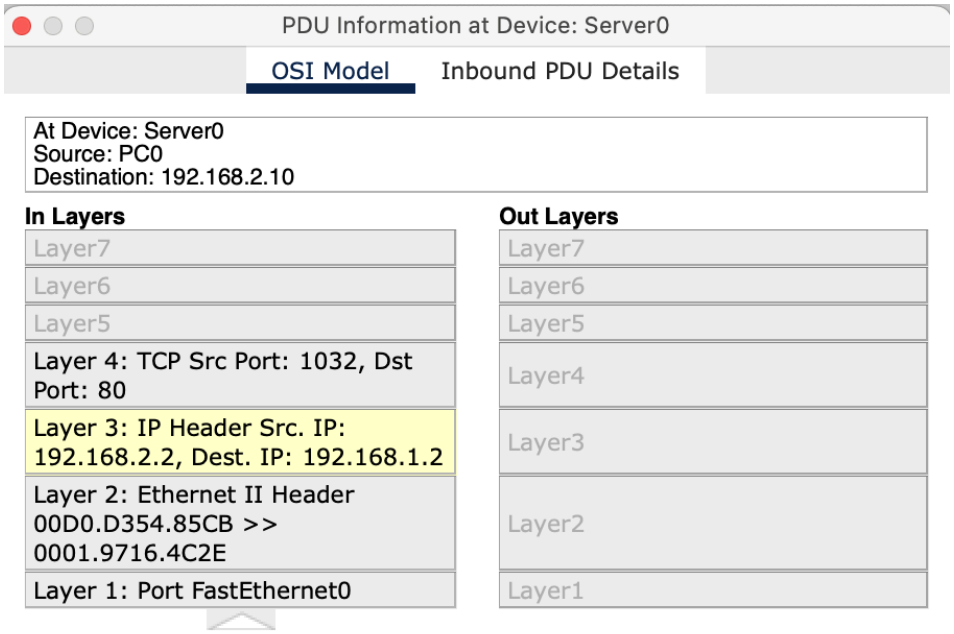
PDU Information at Device: Server0

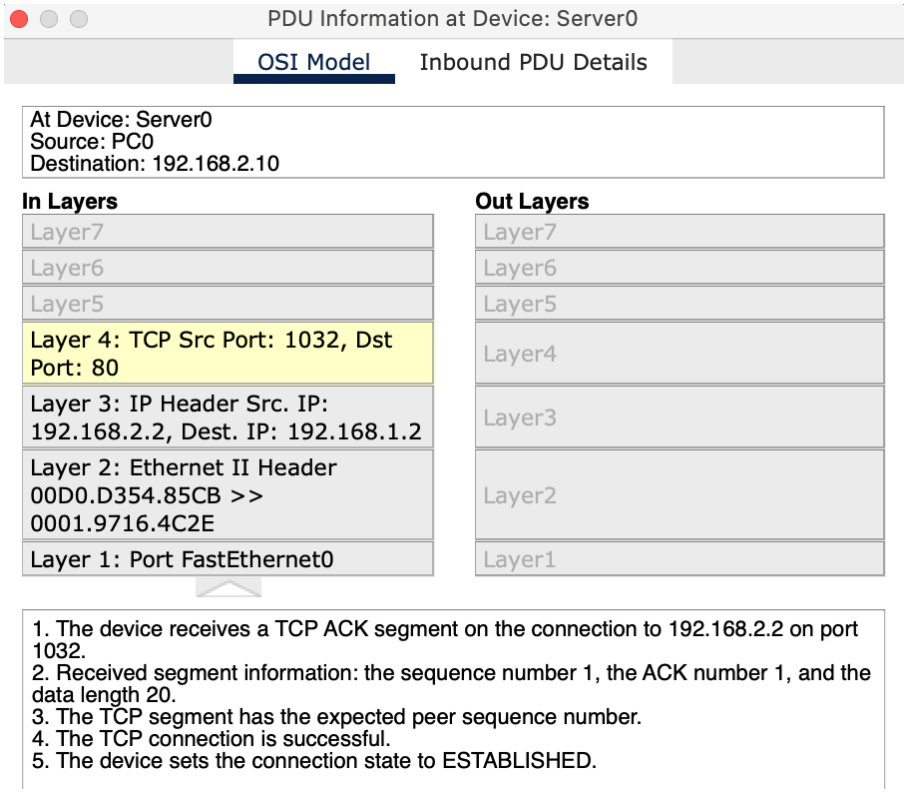
OSI Model | Inbound PDU Details

At Device: Server0
Source: PC0
Destination: 192.168.2.10

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 1032, Dst Port: 80	Layer4
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.1.2	Layer3
Layer 2: Ethernet II Header 00D0.D354.85CB >> 0001.9716.4C2E	Layer2
Layer 1: Port FastEthernet0	Layer1

1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.





We captured and decoded web traffic from PC0 to the ASA5505 firewall and from the firewall to the web server while it was in simulation mode. This stage is examining the packets' IP and TCP header information to see how the firewall manages traffic and carries out NAT translation.

4. (2pts) Submit outputs of “show switch vlan” , “show nat”, “show xlate”, “show access-list” as evidence that firewall is properly configured and is blocking all traffic initiated from outside except for icmp and http traffic.

```
:
ciscoasa#show switch vlan

VLAN Name                            Status    Ports
---- ------------------------------- --------- -------------------------------
1    inside                          up        Et0/1, Et0/2, Et0/3, Et0/4
                                               Et0/5, Et0/6, Et0/7
2    outside                         up        Et0/0
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static www 192.168.2.10
    translate_hits = 0, untranslate_hits = 0

ciscoasa#show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N - net-to-net
NAT from inside:192.168.1.2/32 to outside:192.168.2.10/32 flags s idle 00:17:15,  timeout 0:00:00

ciscoasa#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list www; 4 elements; name hash: 0x6970e38d
access-list www line 1 extended permit tcp any host 192.168.2.10 eq www(hitcnt=2) 0x874756c8
access-list www line 2 extended permit icmp any host 192.168.2.10(hitcnt=8) 0x89647b5a
access-list www line 3 extended deny ip any any(hitcnt=101) 0xe87ad954
access-list www line 4 extended deny icmp any any(hitcnt=0) 0x803a3340
```

these outputs show that the firewall is properly configured and is blocking all traffic from outside except for ICMP and HTTP traffic. The commands show the VLAN configuration, NAT translation settings, translation table, and access list rules.

5. (2pts) Submit a copy of the entire Cisco ASA 5505 firewall configuration file (copy and paste to Word document the entire output of “show running-config” from enable mode of CLI). Also submit a copy of the Cisco Packet Tracer file.

ciscoasa#show running-conf
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5

```
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.2.1 255.255.255.0
!
object network www
host 192.168.1.2
nat (inside,outside) static 192.168.2.10
!
!
access-list www extended permit tcp any host 192.168.2.10 eq www
access-list www extended permit icmp any host 192.168.2.10
access-list www extended deny ip any any
access-list www extended deny icmp any any
!
!
access-group www in interface outside
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
!
```

This contains the results of the CLI's "show running-config" command while in enable mode. It shows the firewall's whole setup, including access list rules, NAT settings, and interface settings.