EXAM BELT 3 SCADA

NAJD FARIS ALEID

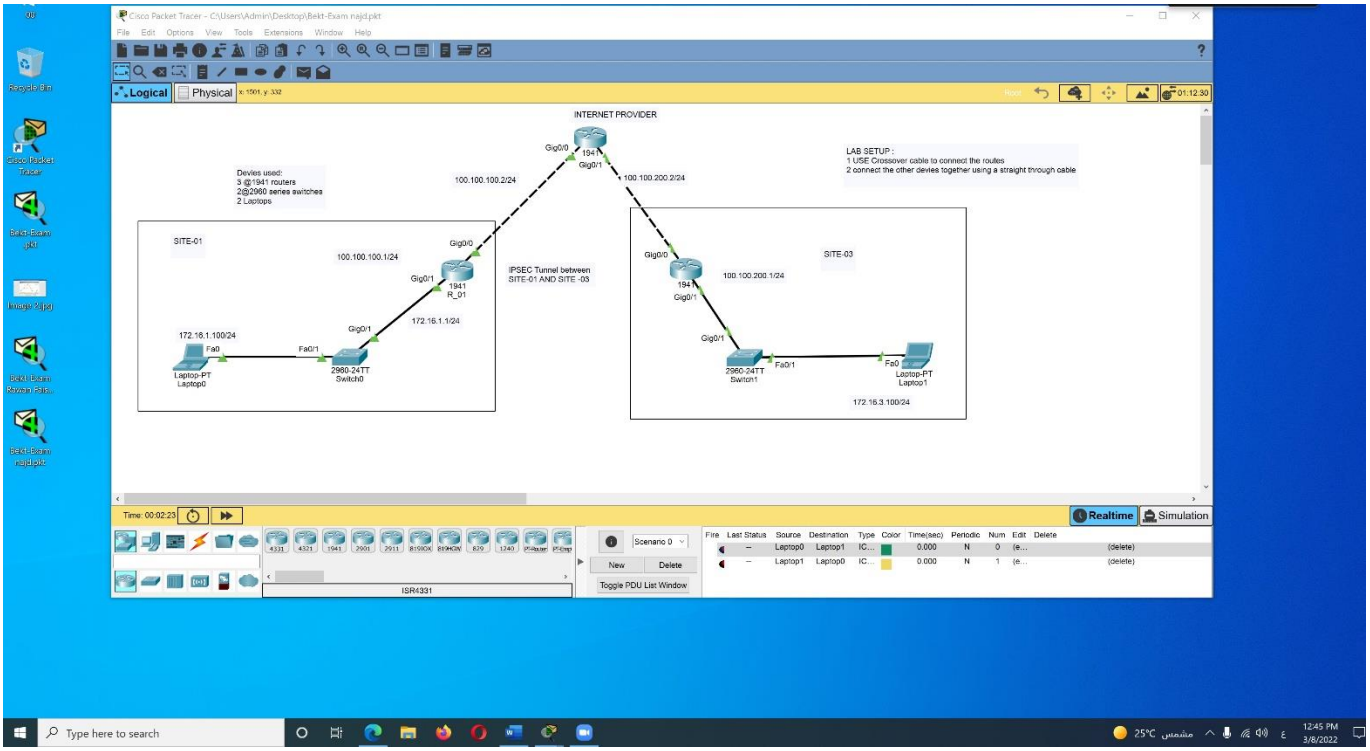
Question 1

Consider the topology below. You have been tasked to secure the communication between site 1 and site 2 using IPsec.

Initial Setup

1/ Use a crossover cable to connect the routers together.

ANSWERS



We are using the 1941 Routers for this topology.

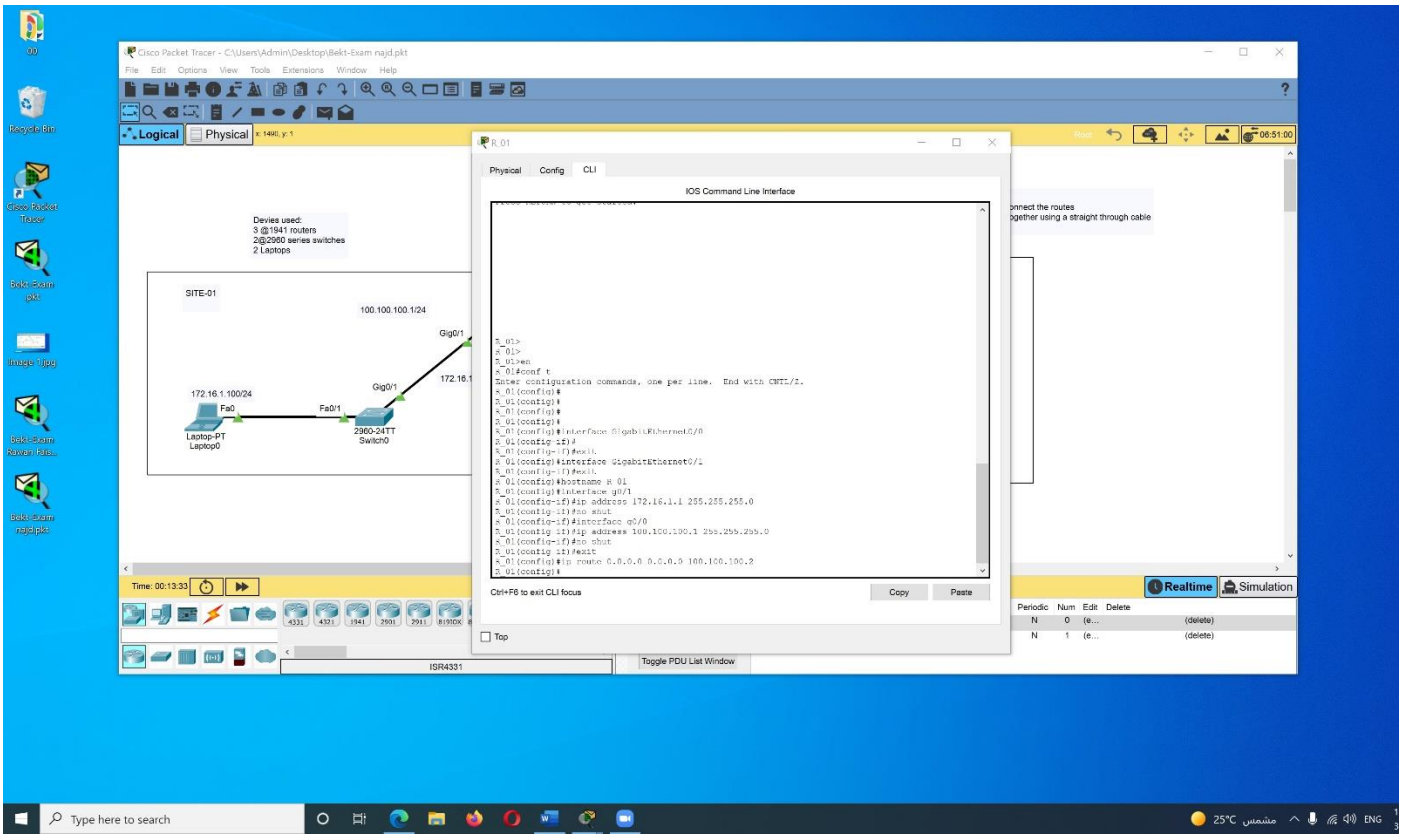
2/ Connect the other devices together using a straight through cable connection.

3/ Perform initial router configuration.

Configure the interface IP addresses on the routers and a default route on R_01 and R_03 pointing to the R_02 router. The R_02 router acts as an internet provider and has no knowledge of other networks except its directly connected network.

Configure the interface IP addresses on the routers and a default route on R_01

```
R_01(config)#hostname R_01
R_01(config)#interface g0/1
R_01(config-if)#ip address 172.16.1.1 255.255.255.0
R_01(config-if)#no shut
R_01(config-if)#interface g0/0
R_01(config-if)#ip address 100.100.100.1 255.255.255.0
R_01(config-if)#no shut
R_01(config-if)#exit
R_01(config)#ip route 0.0.0.0 0.0.0.0 100.100.100.2
```



Configure the interface IP addresses on the routers and a default route on R_02

R_02>en

R_02#

R_02#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R_02(config)#hostname R_02

R_02(config)#interface g0/1

R_02(config-if)#ip address 100.100.200.2 255.255.255.0

R_02(config-if)#no shut

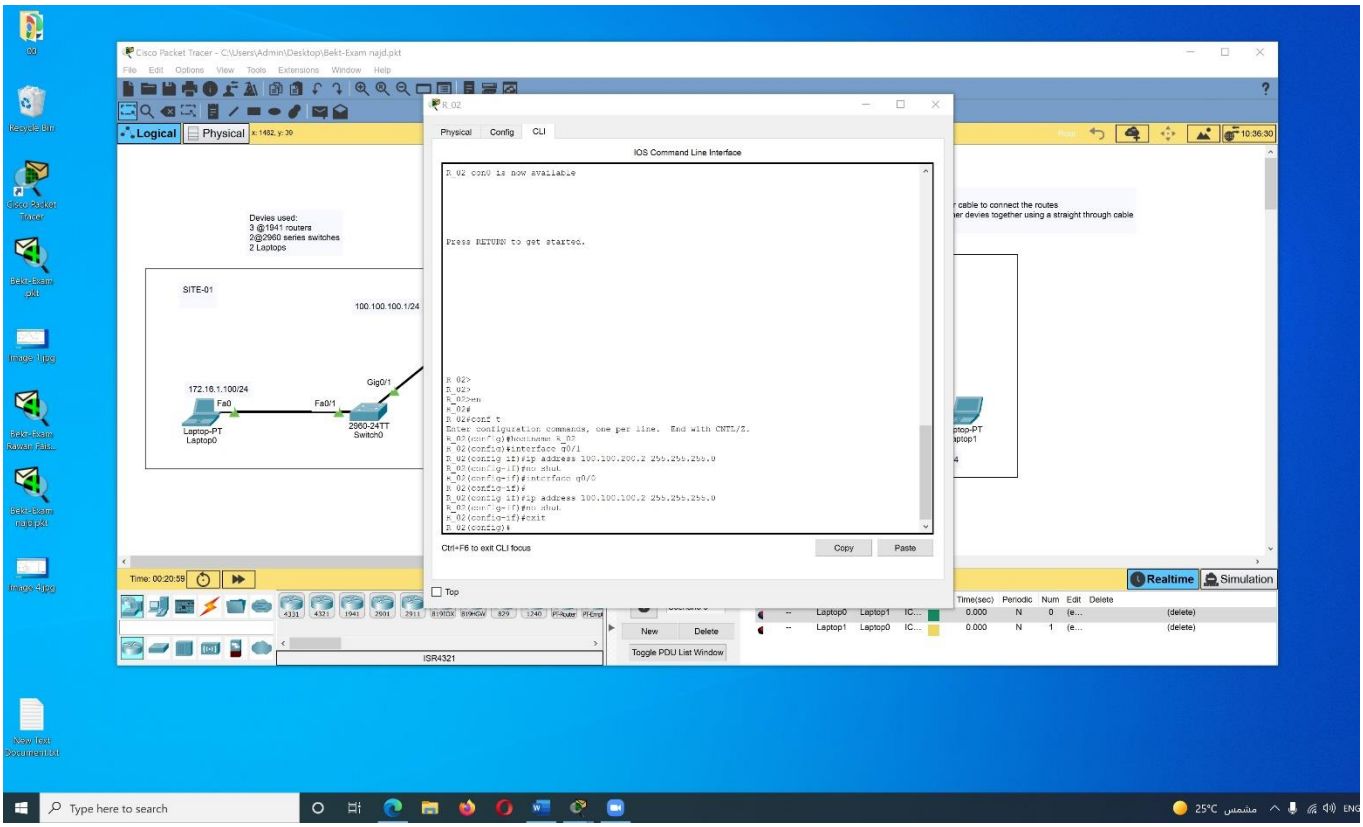
R_02(config-if)#interface g0/0

R_02(config-if)#

R_02(config-if)#ip address 100.100.100.2 255.255.255.0

R_02(config-if)#no shut

R_02(config-if)#exit



Configure the interface IP addresses on the routers and a default route on R_03

R_03>

R_03>en

R_03#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R_03(config)#hostname R_03

R_03(config)#interface g0/1

R_03(config-if)#ip address 172.16.3.1 255.255.255.0

R_03(config-if)#no shut

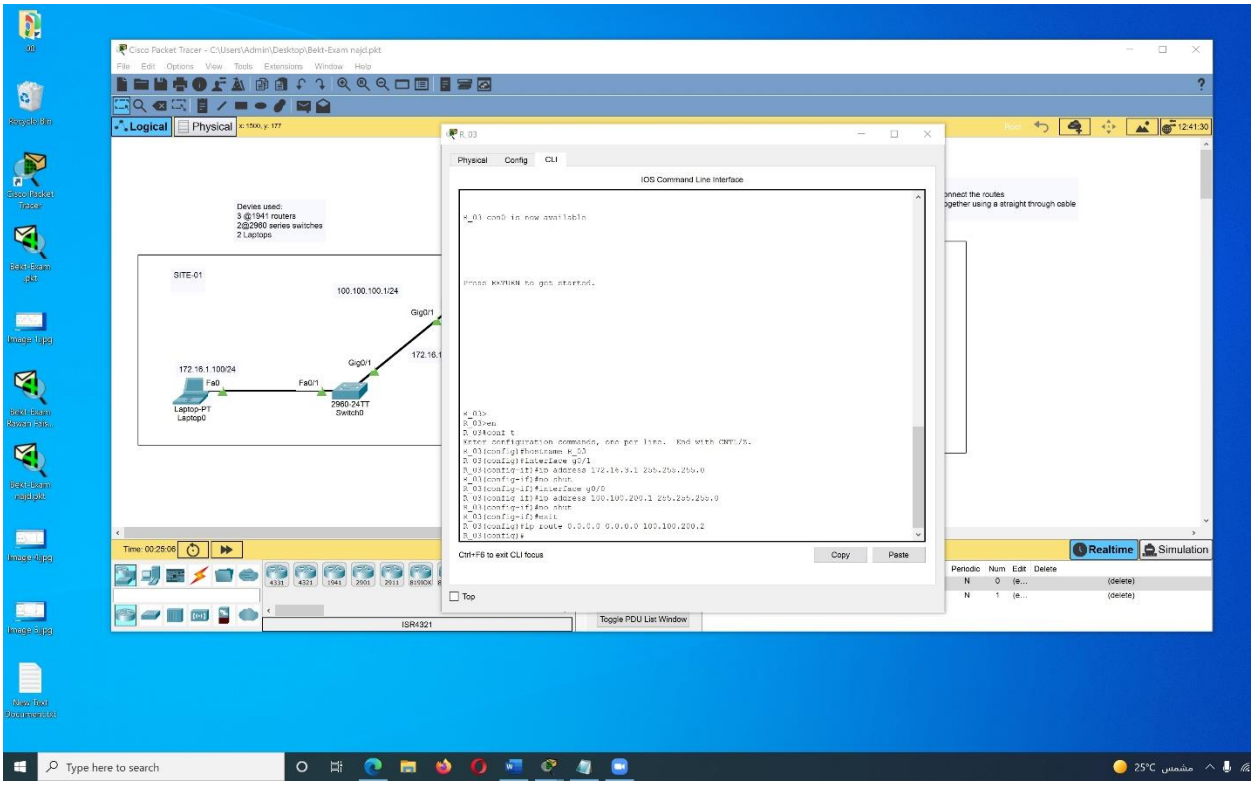
R_03(config-if)#interface g0/0

R_03(config-if)#ip address 100.100.200.1 255.255.255.0

R_03(config-if)#no shut

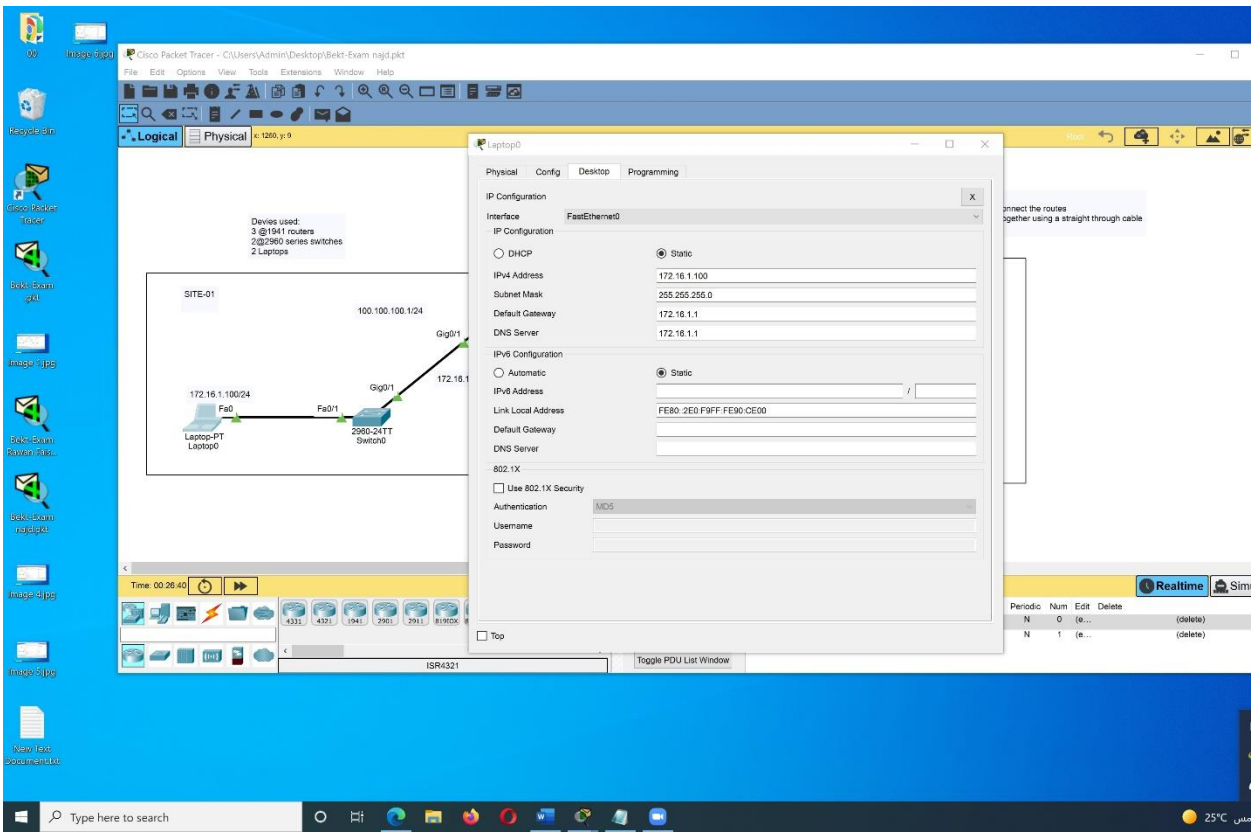
R_03(config-if)#exit

R_03(config)#ip route 0.0.0.0 0.0.0.0 100.100.200.2

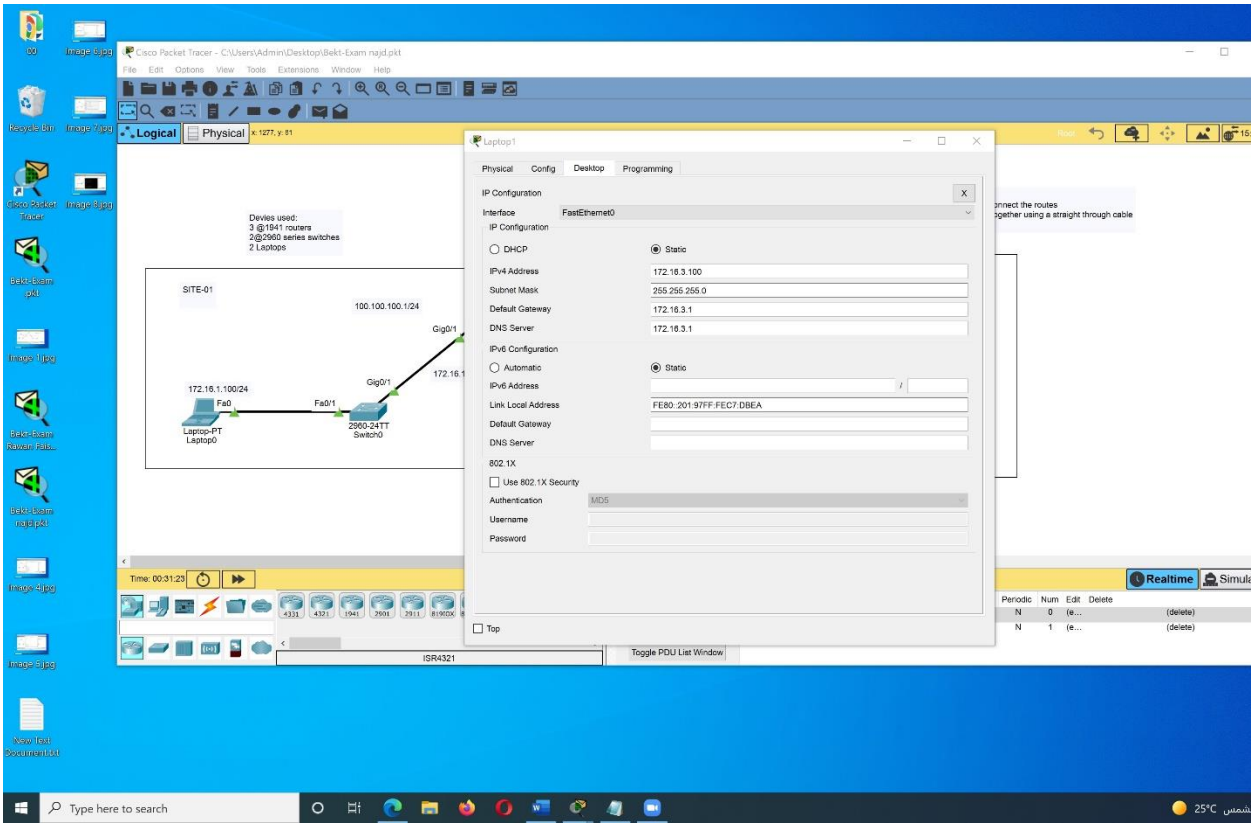


4/ Ensure that the laptops have static IP addresses configured. Laptop0 should have IP 172.16.1.100/24. Laptop1 should have 172.16.3.100/24. Attempt pinging across from Laptop0 to Laptop1. This should fail as R_02 does not know how to route this traffic.

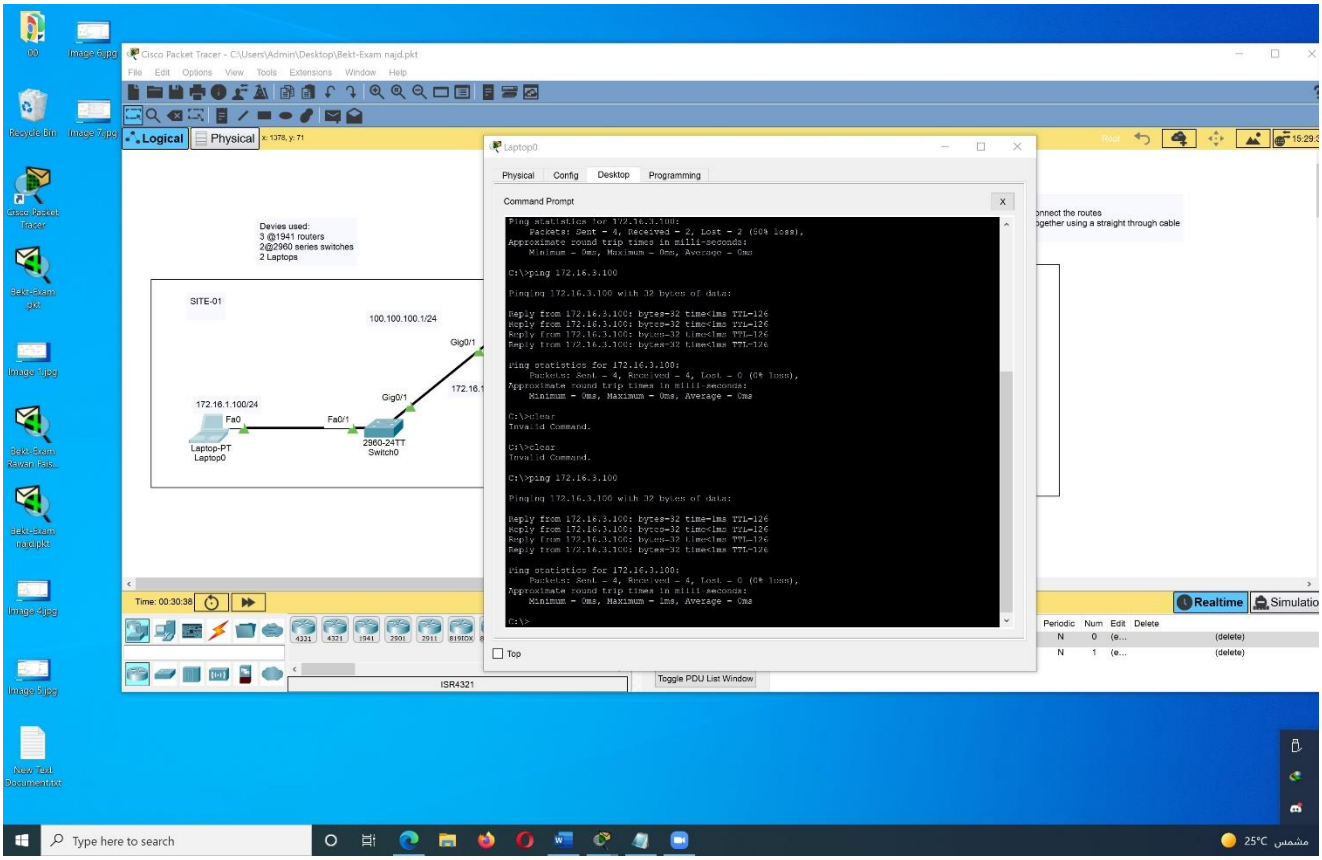
Laptop0



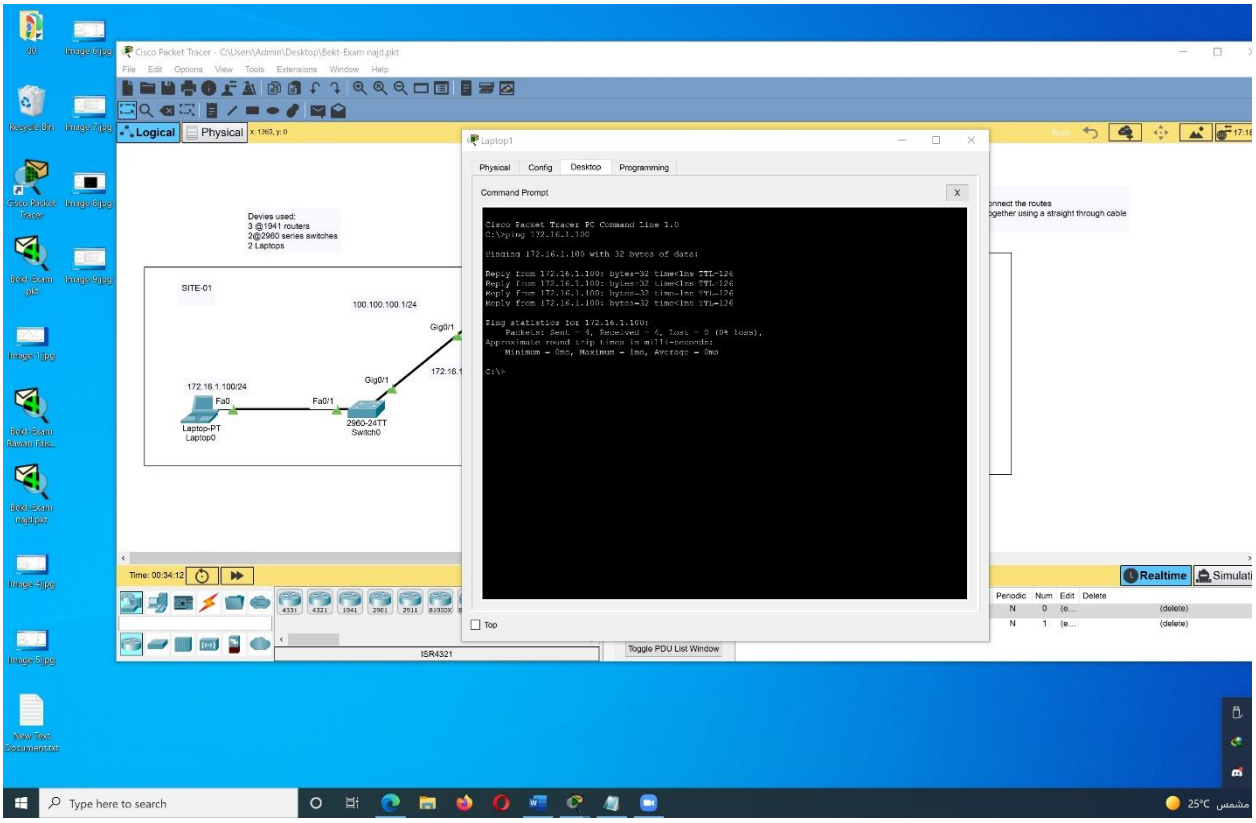
Laptop1




```
!Laptop0
Ping 172.16.3.100
```



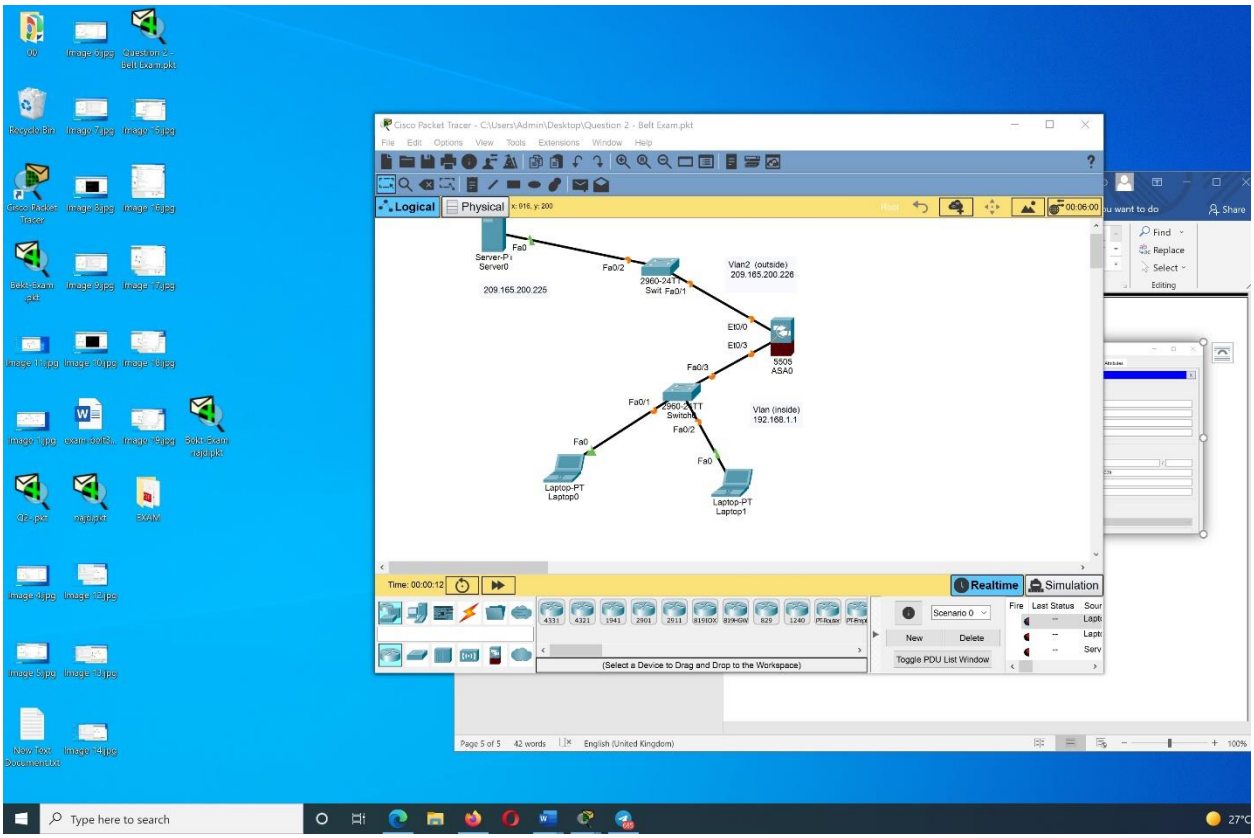

```
!Laptop1
ping 172.16.1.100
```

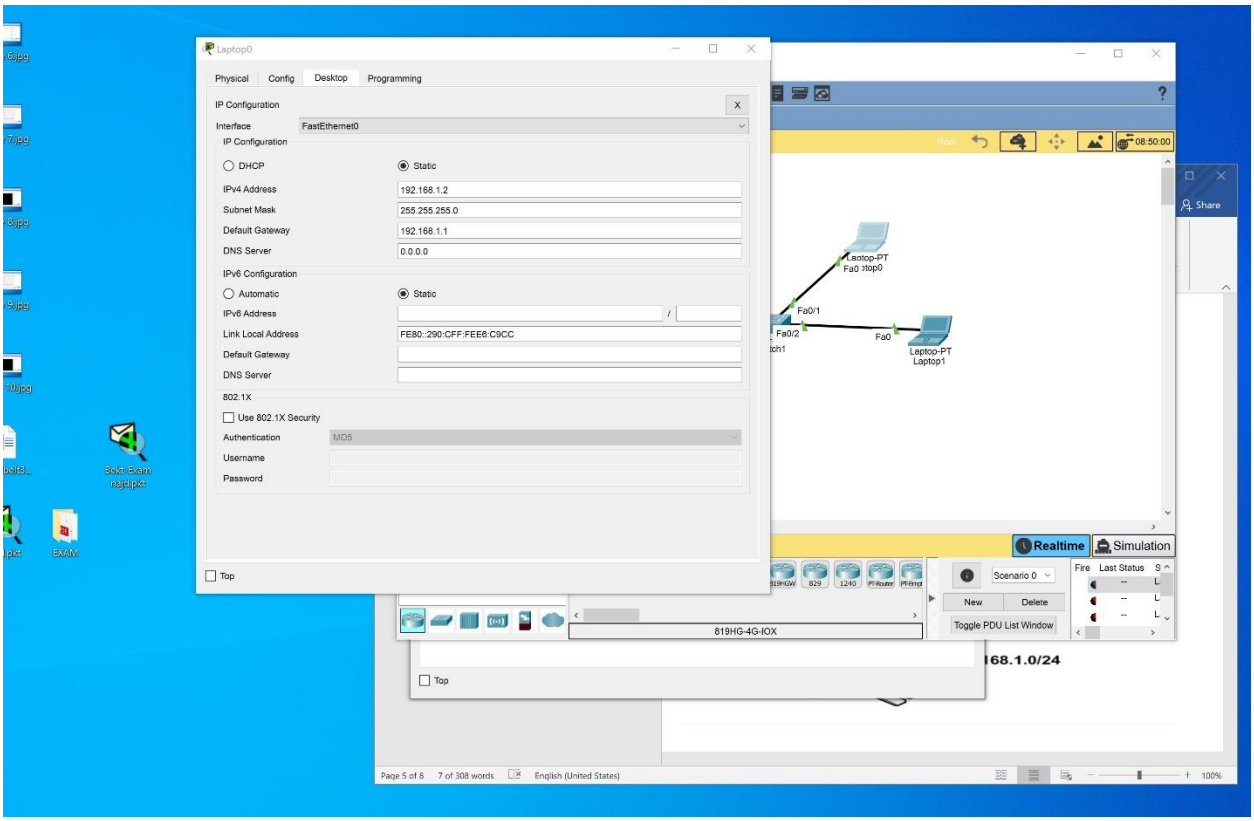

Cisco Packet Tracer - C:\Users\Admin\Desktop\Bekt-Exam najd.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
Devies used:
3 @1941 routers
2@2960 series switches
2 Laptops
SITE-01
100.100.100.1/24
Gig0/1
172.16.1.100/24
Fa0
Fa0/1
Laptop-PT
Laptop0
2960-24TT
Switch0
Laptop1
Physical
Config
Desktop
Programming
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time<1ms TTL=126
Reply from 172.16.1.100: bytes=32 time<1ms TTL=126
Reply from 172.16.1.100: bytes=32 time=1ms TTL=126
Reply from 172.16.1.100: bytes=32 time<1ms TTL=126
Ping statistics for 172.16.1.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top
Time: 00:34:12
Realtime
Simulati
ISR4321
Toggle PDU List Window
Type here to search
25°C مشمس

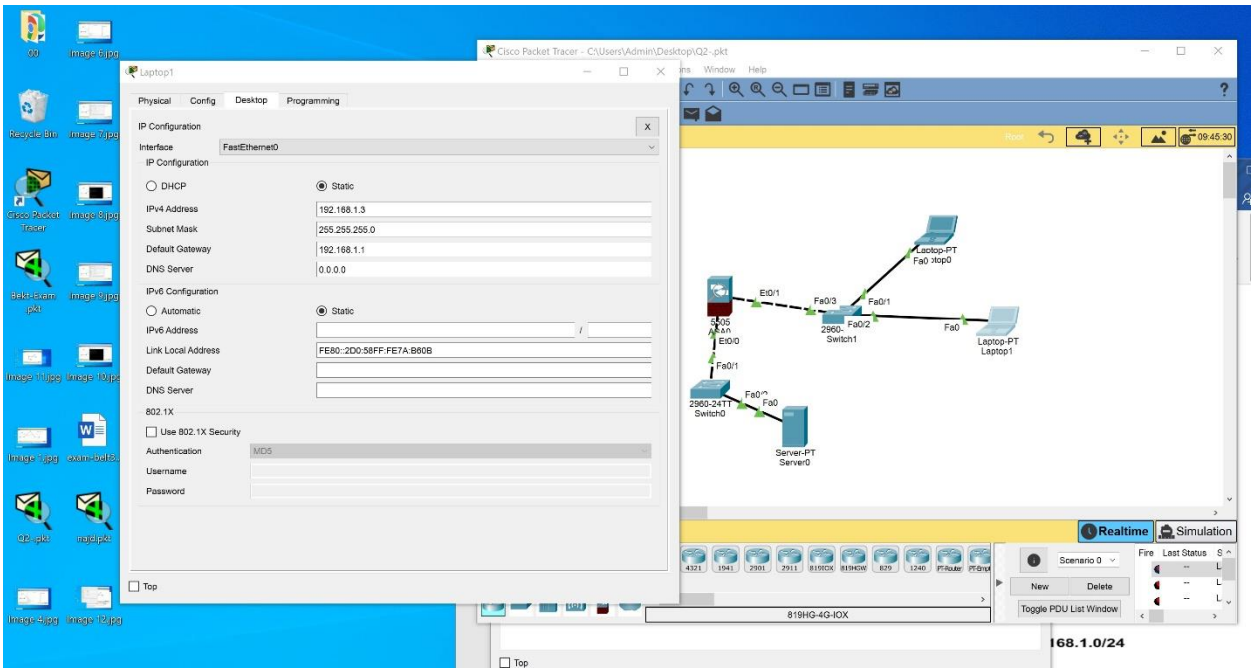
Question 2

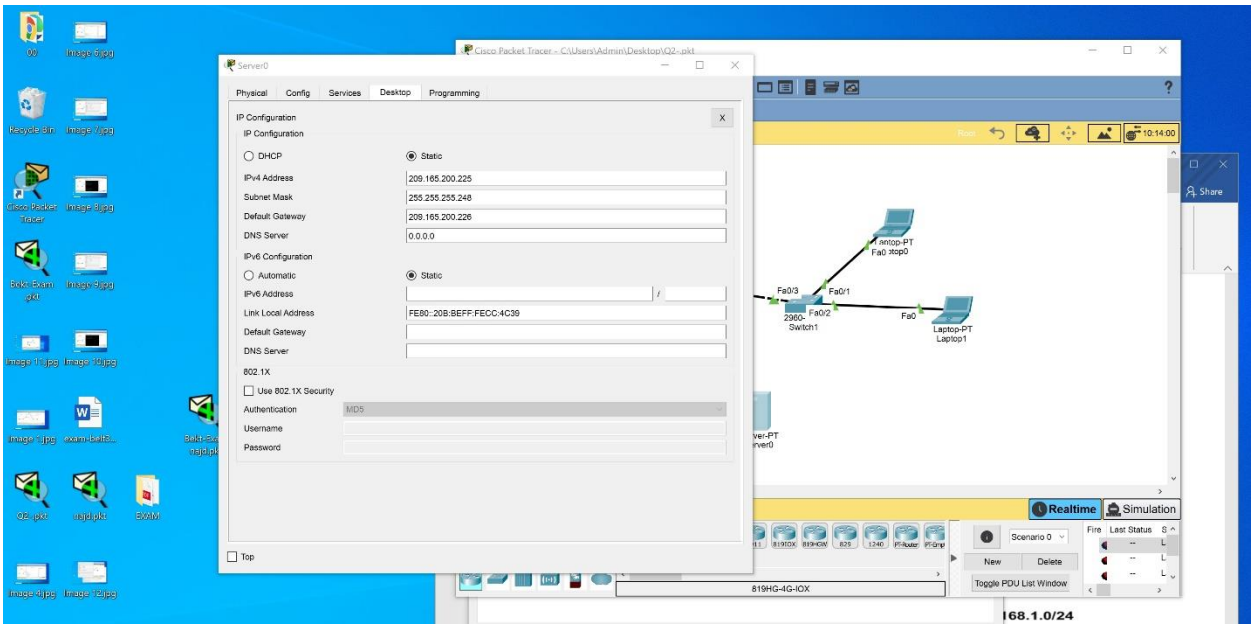
Answers

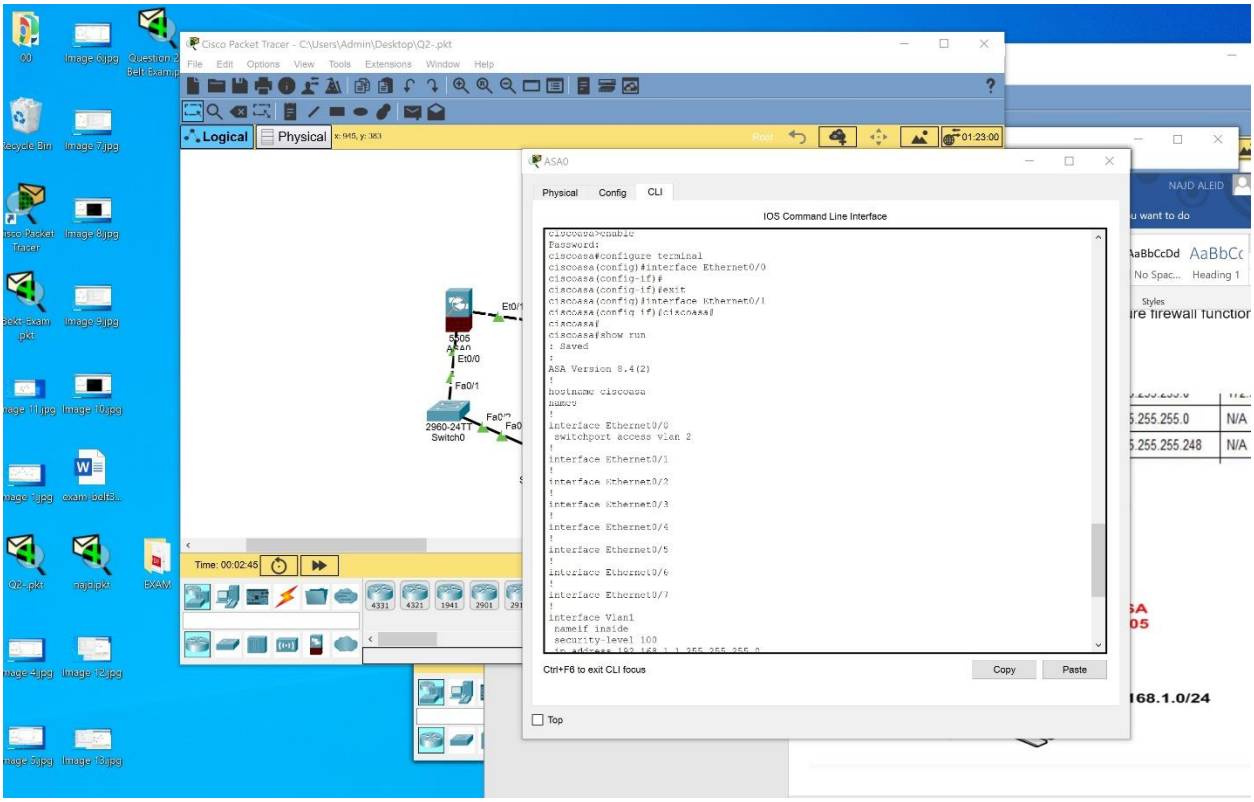
Configure ASA basic security and firewall settings.

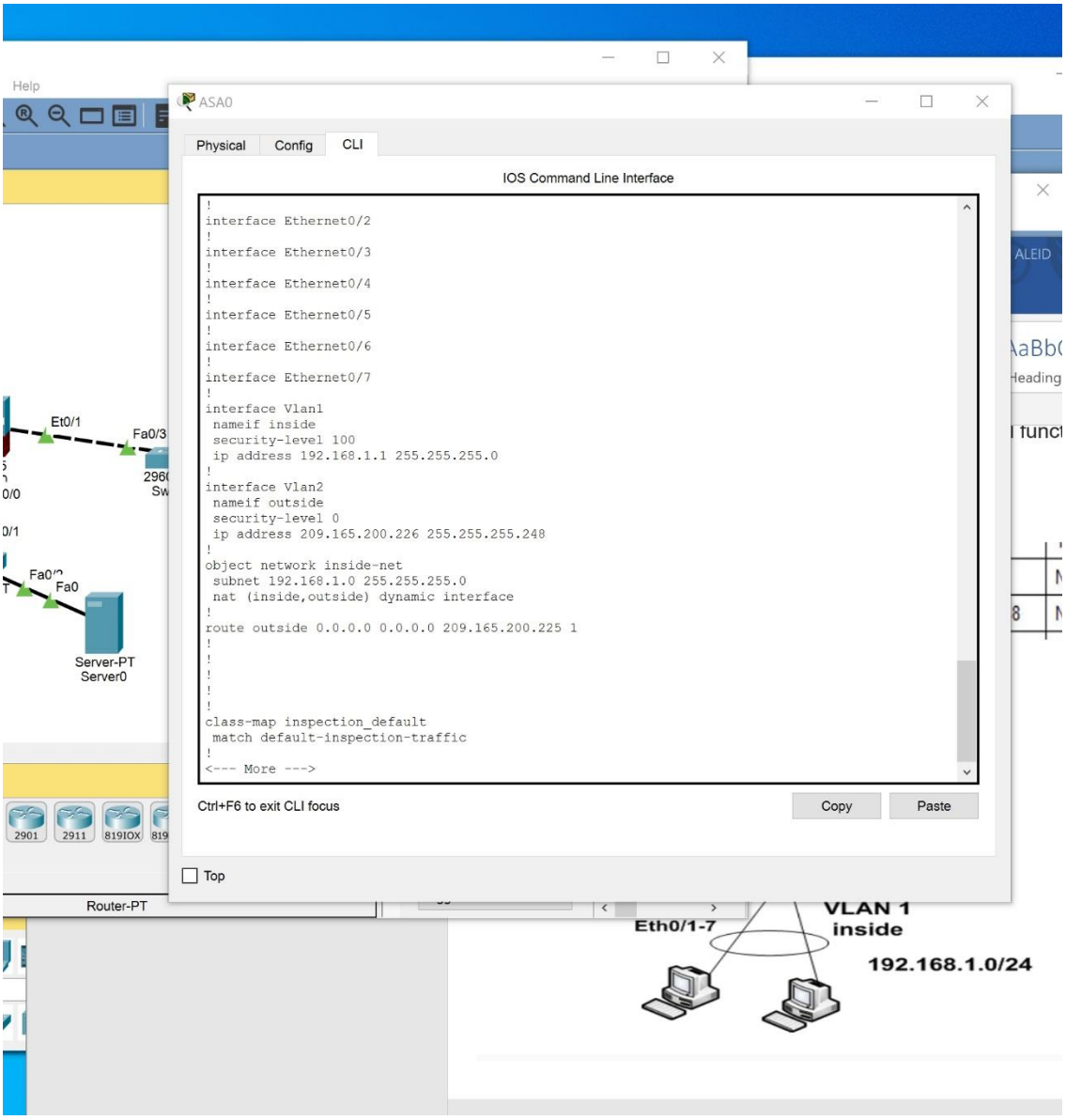


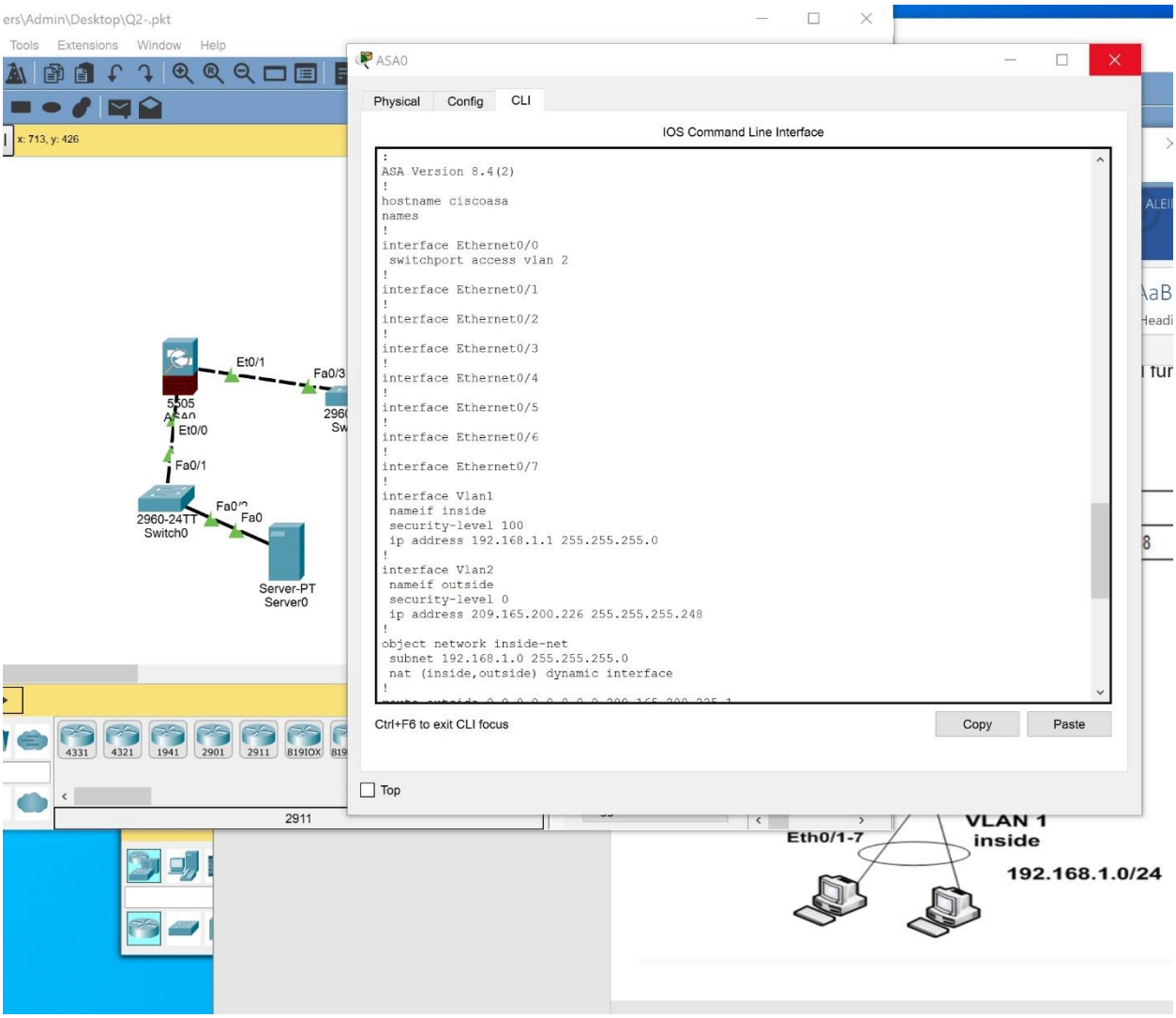

Laptop0
Physical
Config
Desktop
Programming
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::290:CFF:FEE6:C9CC
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top
Laptop-PT
Fa0/1
Fa0/2
Fa0
Laptop-PT
Laptop1
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
819HG-4G-IOX
Page 5 of 8
7 of 308 words
English (United States)

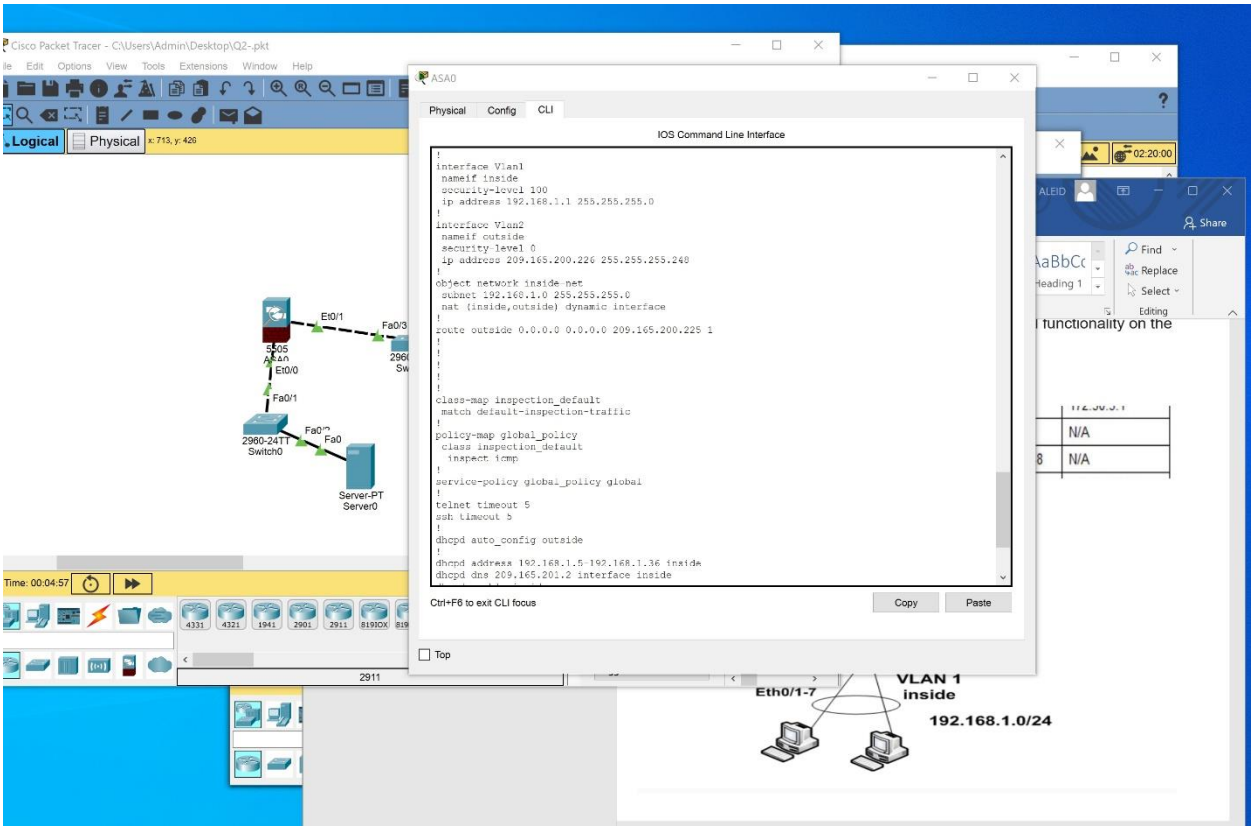

Cisco Packet Tracer - C:\Users\Admin\Desktop\Q2-.pkt
Laptop1
Physical
Config
Desktop
Programming
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2D0:58FF:FE7A:B60B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top
Laptop-PT
Fa0/1
Fa0/3
Fa0/2
Fa0
2960-
Switch1
Laptop-PT
Laptop1
Fa0/1
2960-24TT
Switch0
Server-PT
Server0
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
819HG-4G-IOX

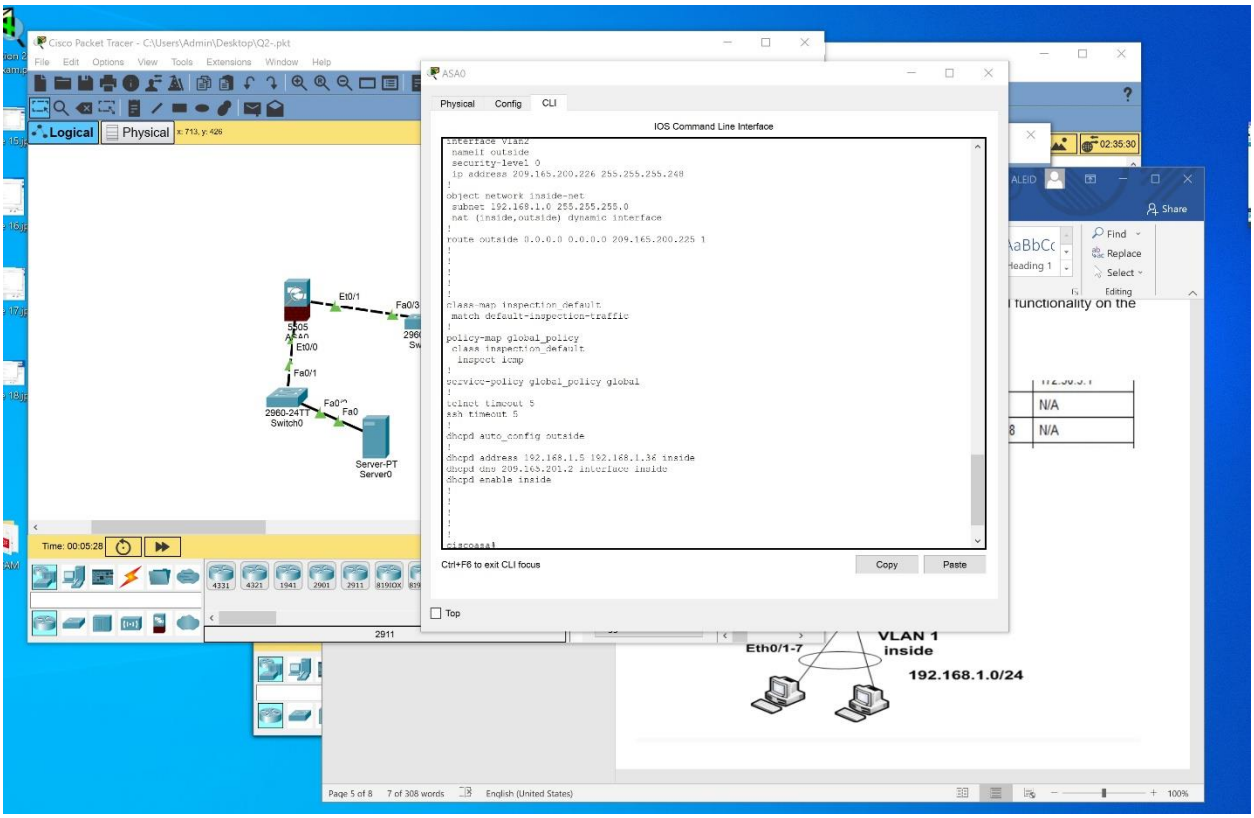

Server0
Physical
Config
Services
Desktop
Programming
IP Configuration
DHCP
Static
IPv4 Address
209.165.200.225
Subnet Mask
255.255.255.248
Default Gateway
209.165.200.226
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20B:BEFF:FECC:4C39
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top
Cisco Packet Tracer - C:\Users\Admin\Desktop\Q2-.pkt
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
819HG-4G-IOX
168.1.0/24


Cisco Packet Tracer - C:\Users\Admin\Desktop\Q2-.pkt
File
Edit
Options
View
Tools
Extensions
Window
Help
Logical
Physical
ASA0
Physical
Config
CLI
IOS Command Line Interface
ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#interface Ethernet0/0
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface Ethernet0/1
ciscoasa(config-if)#ciscoasa#
ciscoasa#show run
: Saved
ASA Version 8.4(2)
hostname ciscoasa
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
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Time: 00:02:45
168.1.0/24


ASA0
Physical
Config
CLI
IOS Command Line Interface
!
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 209.165.200.226 255.255.255.248
!
object network inside-net
subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
!
!
!
!
class-map inspection_default
match default-inspection-traffic
!
<--- More --->
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Et0/1
Fa0/3
Fa0
Server-PT
Server0
Router-PT
Eth0/1-7
VLAN 1
inside
192.168.1.0/24


ers\Admin\Desktop\Q2-.pkt
Tools Extensions Window Help
x: 713, y: 426
ASA0
Physical Config CLI
IOS Command Line Interface
:
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 209.165.200.226 255.255.255.248
!
object network inside-net
 subnet 192.168.1.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Et0/1
Et0/0
Fa0/1
Fa0
2960-24TT
Switch0
Server-PT
Server0
4331
4321
1941
2901
2911
2911
Eth0/1-7
VLAN 1
inside
192.168.1.0/24


Cisco Packet Tracer - C:\Users\Admin\Desktop\Q2-.pkt
ASA0
Physical
Config
CLI
IOS Command Line Interface
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 209.165.200.226 255.255.255.248
object network inside-net
subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect icmp
service-policy global_policy global
telnet timeout 5
ssh timeout 5
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd dns 209.165.201.2 interface inside
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Et0/1
Et0/0
Fa0/1
Fa0
Server-PT
Server0
2960-24TT
Switch0
Time: 00:04:57
Eth0/1-7
VLAN 1
inside
192.168.1.0/24
N/A
N/A


Cisco Packet Tracer - C:\Users\Admin\Desktop\Q2-.pkt
ASA0
Physical
Config
CLI
IOS Command Line Interface
interface Vlan2
nameif outside
security-level 0
ip address 209.165.200.226 255.255.255.248
object network inside-net
subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect icmp
service-policy global_policy global
telnet timeout 5
ssh timeout 5
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd dns 209.165.201.2 interface inside
dhcpd enable inside
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Time: 00:05:28
Eth0/1-7
VLAN 1
inside
192.168.1.0/24
N/A
N/A
Page 5 of 8
7 of 308 words
English (United States)

Laptop0

Physical Config Desktop Programming

Command Prompt

```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time<1ms TTL=127
Reply from 209.165.200.225: bytes=32 time<1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=2ms TTL=127

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=4ms TTL=127
Reply from 209.165.200.225: bytes=32 time<1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=10ms TTL=127

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:
```

Top

Laptop1

Physical Config Desktop Programming

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=62ms TTL=127
Reply from 209.165.200.225: bytes=32 time<1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=2ms TTL=127
Reply from 209.165.200.225: bytes=32 time<1ms TTL=127

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 62ms, Average = 16ms

C:\>
```

Configure vlans:

```
Type help or '?' for a list of available commands.

ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#hostname ASA
ASA(config)#interface Vlan 1
ASA(config-if)#nameif inside
ASA(config-if)#security-level 100
ASA(config-if)#ip address 192.168.1.1 255.255.255.0
ASA(config-if)#no shutdown
ASA(config-if)#exit
ASA(config)#interface Vlan 2
ASA(config-if)#nameif outside
ASA(config-if)#security-level 0
ASA(config-if)#ip address 209.165.200.226 255.255.255.248
ASA(config-if)#no shutdown
ASA(config-if)#
```

Assign and enable:

```
ASA(config-if)#exit
ASA(config)#interface Ethernet0/0
ASA(config-if)#switchport access vlan 2
ASA(config-if)#no shutdown
ASA(config-if)#interface Ethernet0/1
ASA(config-if)#no shutdown
ASA(config-if)#interface Ethernet0/2
ASA(config-if)#no shutdown
ASA(config-if)#interface Ethernet0/3
ASA(config-if)#no shutdown
ASA(config-if)#interface Ethernet0/4
ASA(config-if)#no shutdown
ASA(config-if)#interface Ethernet0/5
ASA(config-if)#no shutdown
ASA(config-if)#interface Ethernet0/6
ASA(config-if)#no shutdown
ASA(config-if)#interface Ethernet0/7
ASA(config-if)#no shutdown
ASA(config-if)#
```

Configure PAT:

```
ASA(config-if)#exit
ASA(config)#object network inside-net
ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)#nat (inside,outside) dynamic interface
ASA(config-network-object)#exit
ASA#conf t
ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
ASA(config)#
```

Modify the default MPF application inspection global service policy:

```
ASA(config)#class-map inspection_default
ASA(config-cmap)#match default-inspection-traffic
ASA(config-cmap)#exit
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect icmp
ASA(config-pmap-c)#exit
ASA(config)#service-policy global_policy global
ASA(config)#
```

Configure dhcp:

```
ASA(config)#telnet timeout 5
ASA(config)#ssh timeout 5
ASA(config)#dhcpd auto_config outside
ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 inside
ASA(config)#dhcpd dns 209.165.201.2 interface inside
ASA(config)#dhcpd enable inside
ASA(config)#
```

Check successful connectivity from laptop to server:

Laptop0

Physical Config Desktop Programming

Command Prompt

```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time<1ms TTL=127
Reply from 209.165.200.225: bytes=32 time<1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=2ms TTL=127

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=4ms TTL=127
Reply from 209.165.200.225: bytes=32 time<1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=10ms TTL=127

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:
```

Top

Laptop1

Physical Config Desktop Programming

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=62ms TTL=127
Reply from 209.165.200.225: bytes=32 time<1ms TTL=127
Reply from 209.165.200.225: bytes=32 time=2ms TTL=127
Reply from 209.165.200.225: bytes=32 time<1ms TTL=127

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 62ms, Average = 16ms

C:\>
```

Question 3

You been tasked to come up with information security controls which can satisfy the following requirement

1. End user accounts create in devices or centralized authentication server
   Software and devices authenticate using certificates.
2. Mobile devices and network infrastructure authenticates users.
3. Firewalls monitor traffic from untrusted networks.
4. EPO server can restrict interactions with mobile devices.
5. Audit records/logs generated by equipment.
6. Equipment supports encrypted protocols, robust check sums/hashing.
7. Application whitelisting enabled on end devices.
8. Equipment supports user names and passwords for authorization
9. Firewalls segment networks and protect boundaries.
10. Firewall can filter messages from external networks.