Department of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Lab Final Exam

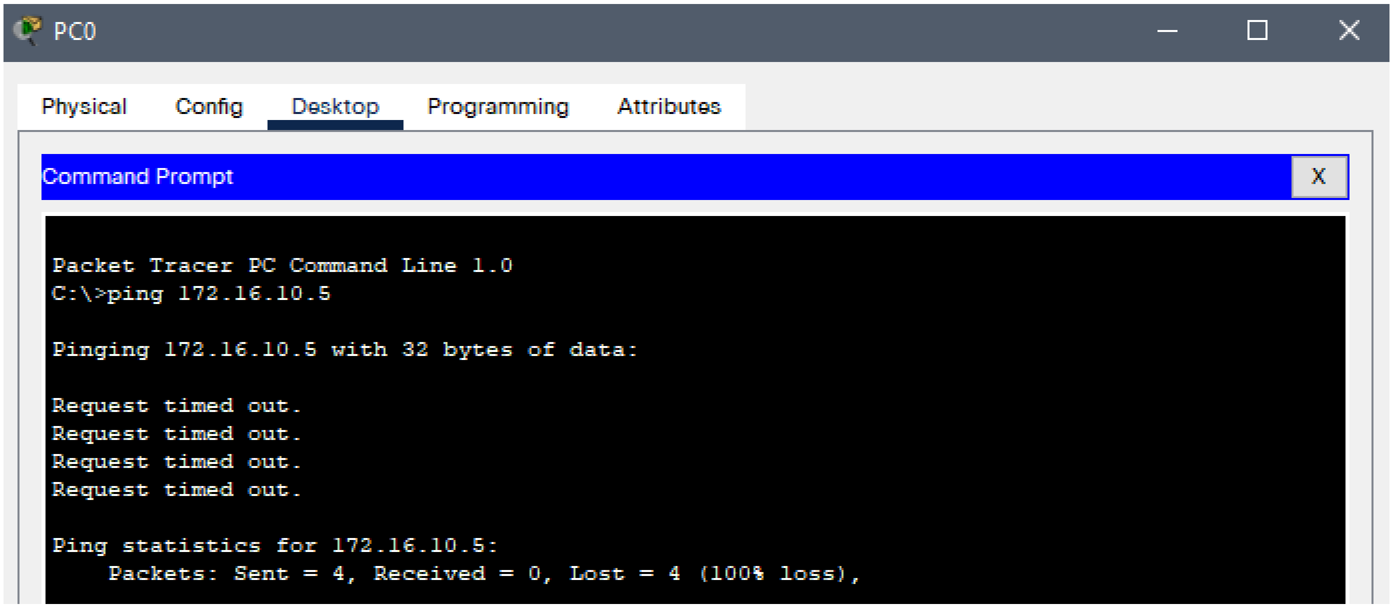
CSE 4512: Computer Networks Lab

Name: Md Farhan Ishmam
Student ID: 180041120
Section: CSE-1
Semester: Fifth
Academic Year: 2021

[Just attach appropriate screenshots as mentioned in Exam task description in their proper place.]

Step 0:

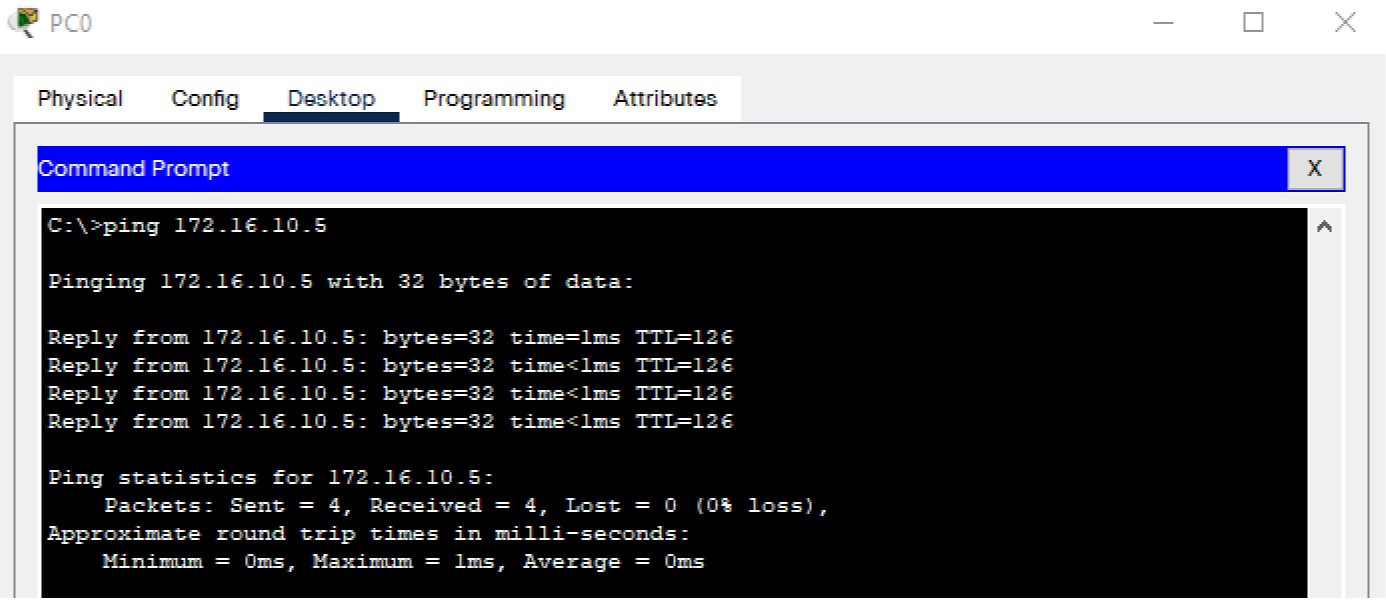
1. Ping result (from *PC0* to *Web Server*)



```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.5

Pinging 172.16.10.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.10.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

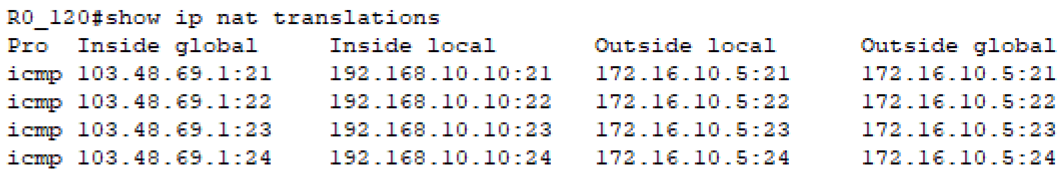
Step 1 (NAT):

1. Ping result after NAT configuration (from *PC0* to *Web Server*)



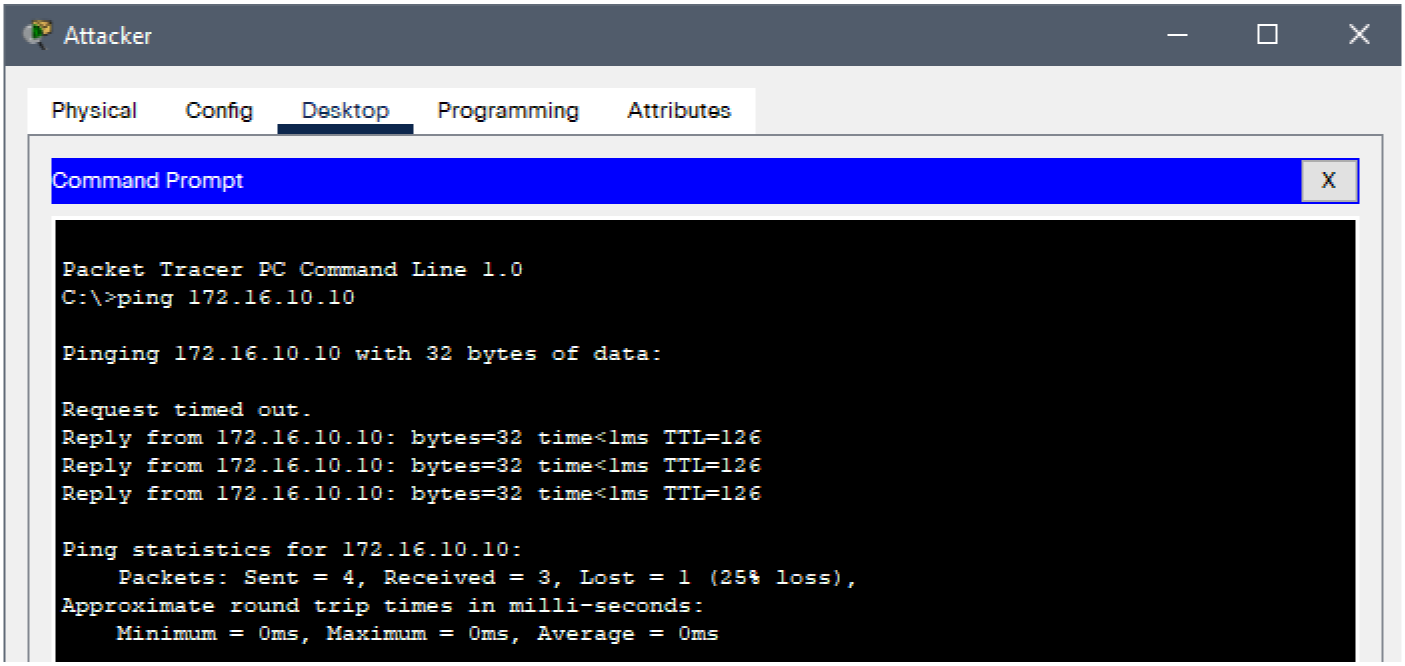
```
C:\>ping 172.16.10.5

Pinging 172.16.10.5 with 32 bytes of data:

Reply from 172.16.10.5: bytes=32 time=1ms TTL=126
Reply from 172.16.10.5: bytes=32 time<1ms TTL=126
Reply from 172.16.10.5: bytes=32 time<1ms TTL=126
Reply from 172.16.10.5: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2. Command output after above ping (**`show ip nat translations`**)



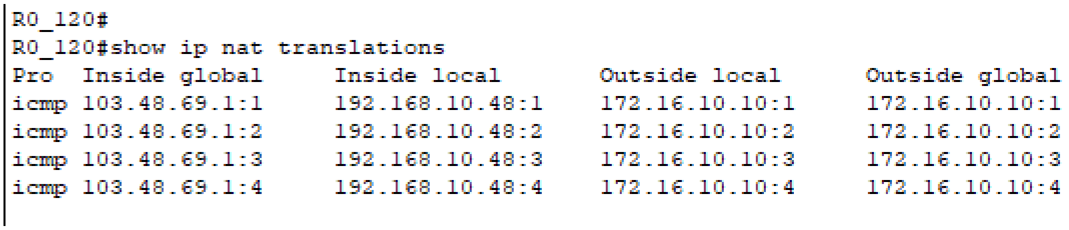
```
R0_120#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 103.48.69.1:21    192.168.10.10:21   172.16.10.5:21     172.16.10.5:21
icmp 103.48.69.1:22    192.168.10.10:22   172.16.10.5:22     172.16.10.5:22
icmp 103.48.69.1:23    192.168.10.10:23   172.16.10.5:23     172.16.10.5:23
icmp 103.48.69.1:24    192.168.10.10:24   172.16.10.5:24     172.16.10.5:24
```

3. Ping result after NAT configuration (from *Attacker* laptop to *Mail Server*)



```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:

Request timed out.
Reply from 172.16.10.10: bytes=32 time<1ms TTL=126
Reply from 172.16.10.10: bytes=32 time<1ms TTL=126
Reply from 172.16.10.10: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.10.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

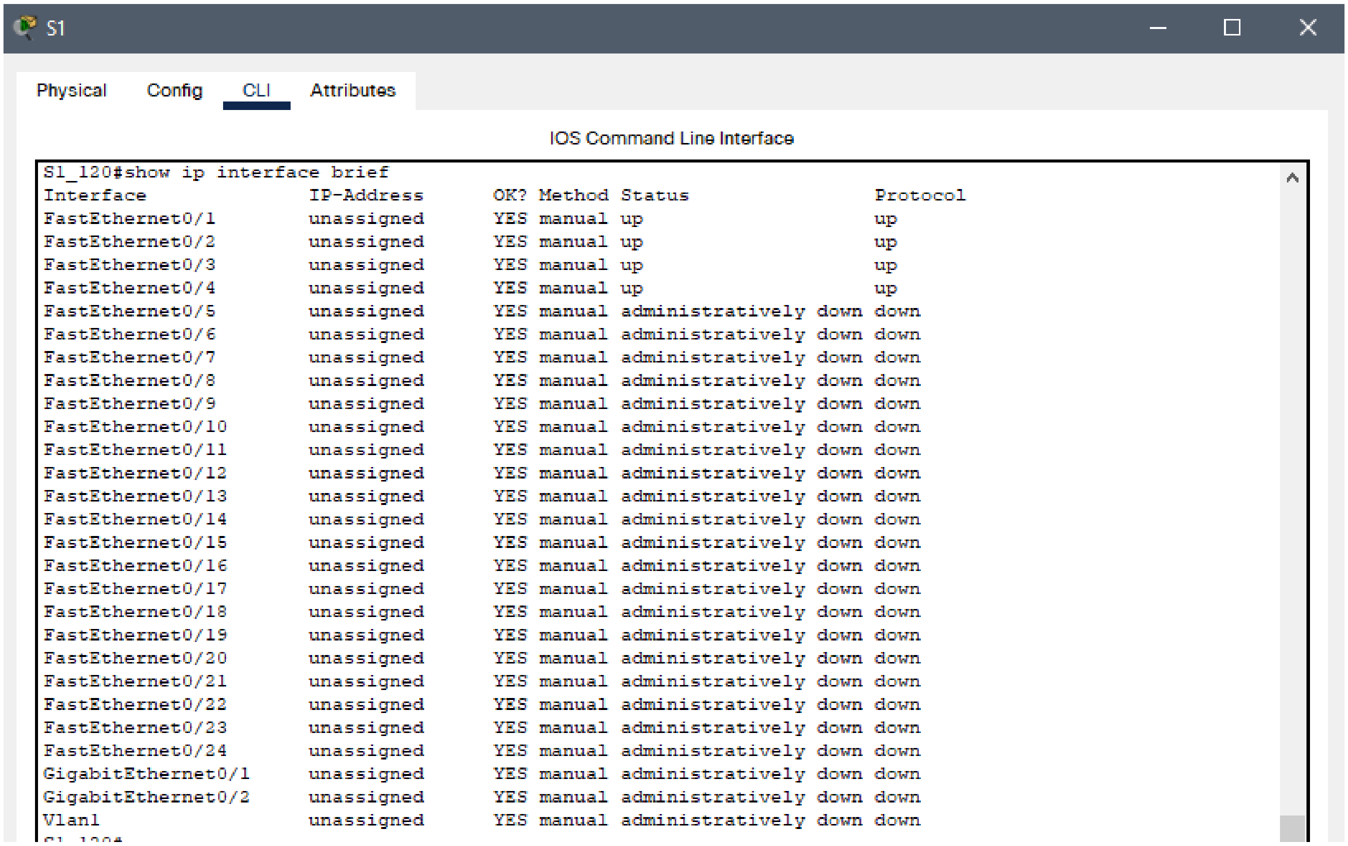
4. Command output after above ping (**`show ip nat translations`**)



```
R0_120#
R0_120#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 103.48.69.1:1     192.168.10.48:1    172.16.10.10:1     172.16.10.10:1
icmp 103.48.69.1:2     192.168.10.48:2    172.16.10.10:2     172.16.10.10:2
icmp 103.48.69.1:3     192.168.10.48:3    172.16.10.10:3     172.16.10.10:3
icmp 103.48.69.1:4     192.168.10.48:4    172.16.10.10:4     172.16.10.10:4
```

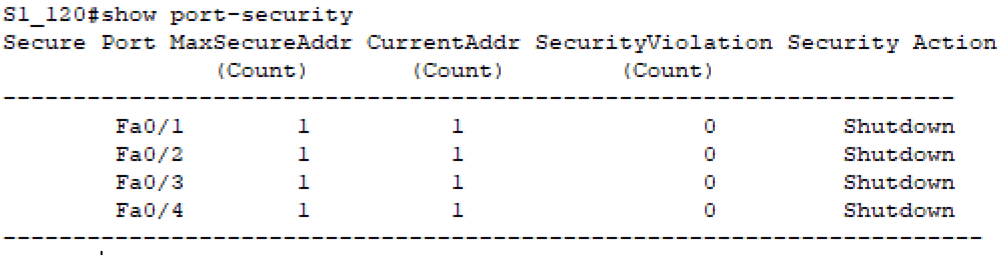
Step 2 (Switch Port Security):

1. Command output after disabling all unused ports (**`show ip interface brief`**)



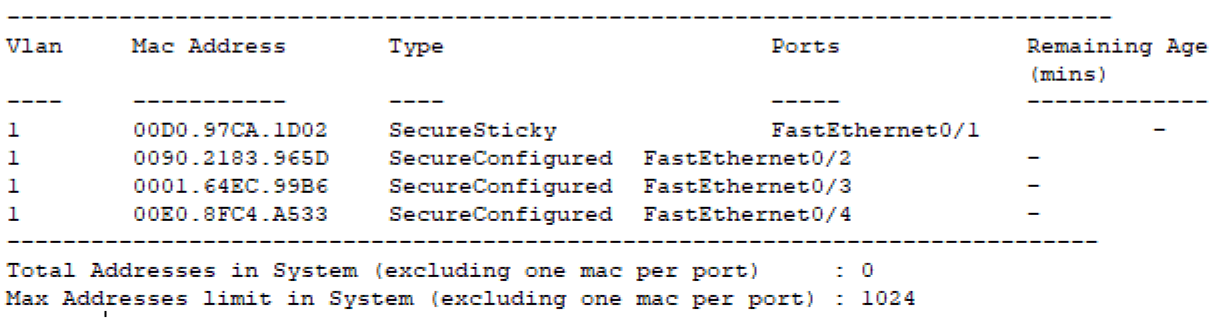
```
S1_120#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual up                    up
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
S1_120#
```

2. Command output after configuring switch port security (**`show port-security`**)



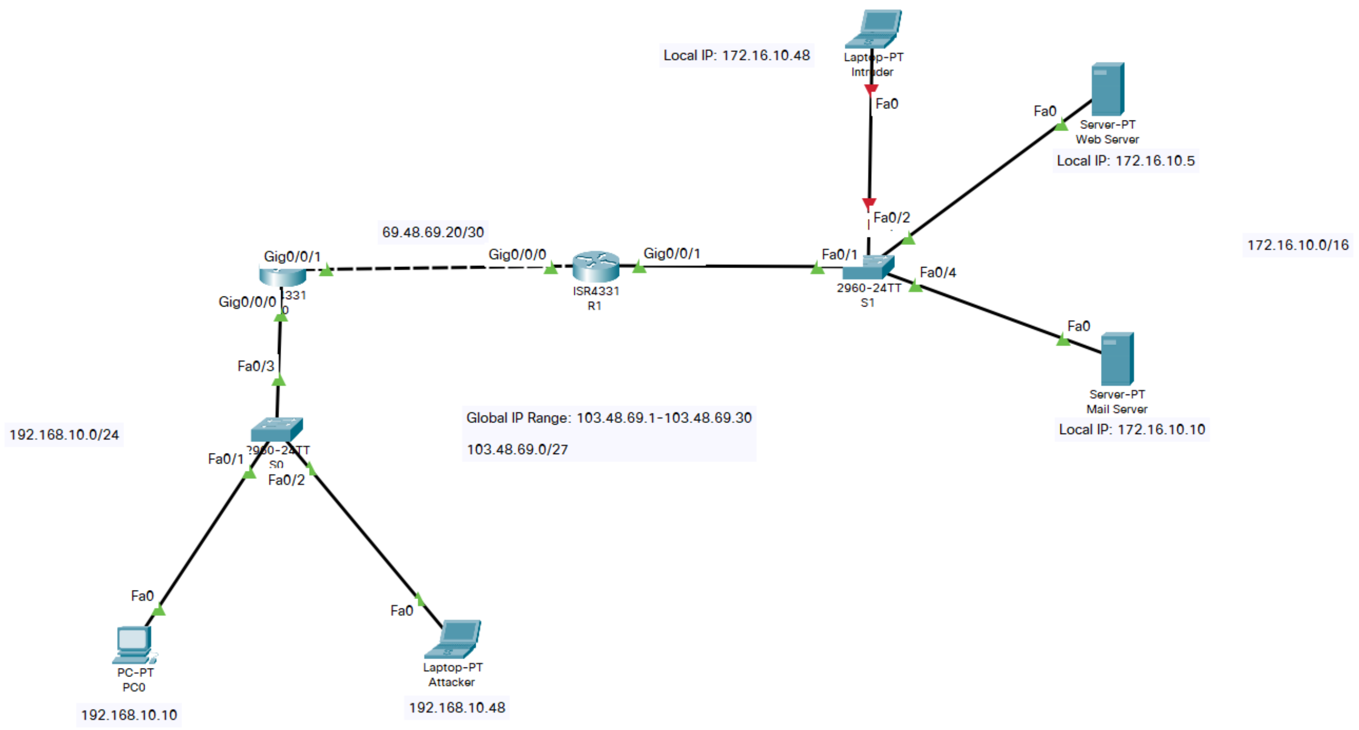
```
S1_120#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 0         Shutdown
        Fa0/2        1          1                 0         Shutdown
        Fa0/3        1          1                 0         Shutdown
        Fa0/4        1          1                 0         Shutdown
----------------------------------------------------------------------
```

3. Command output after configuring switch port security (**`show port-security address`**)

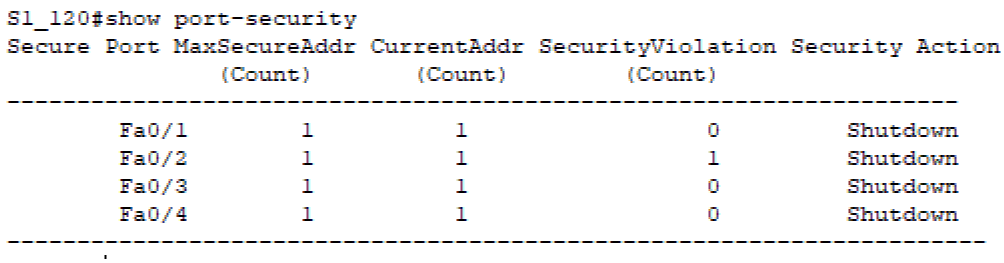


```
-------------------------------------------------------------------------------
Vlan     Mac Address       Type                        Ports            Remaining Age
                                                                         (mins)
----     -----------       ----                        -----            -------------
1        00D0.97CA.1D02    SecureSticky                FastEthernet0/1           -
1        0090.2183.965D    SecureConfigured  FastEthernet0/2             -
1        0001.64EC.99B6    SecureConfigured  FastEthernet0/3             -
1        00E0.8FC4.A533    SecureConfigured  FastEthernet0/4             -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

4. Screenshot of the whole topology after ping (from *Intruder* laptop to *Web Server*)



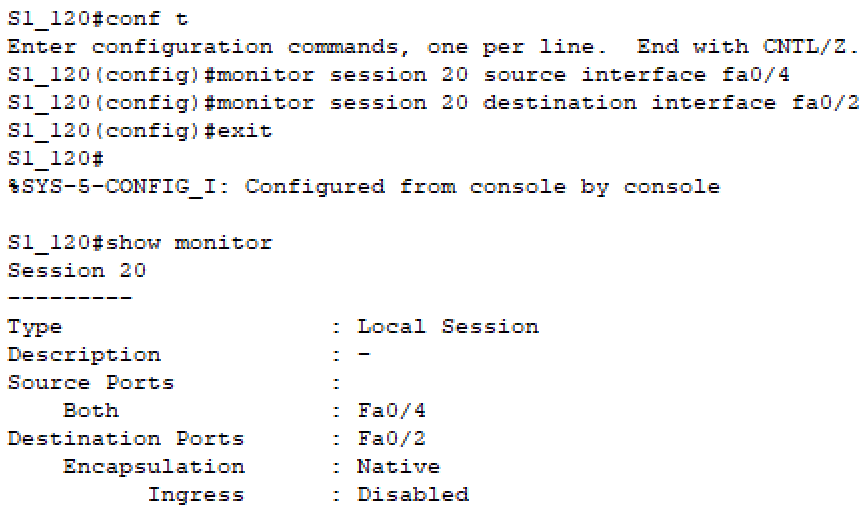
5. Command output after security violation from *Intruder* laptop (**`show port-security`**)



```
S1_120#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                  0        Shutdown
        Fa0/2        1          1                  1        Shutdown
        Fa0/3        1          1                  0        Shutdown
        Fa0/4        1          1                  0        Shutdown
----------------------------------------------------------------------
```

Step 3 (SPAN):

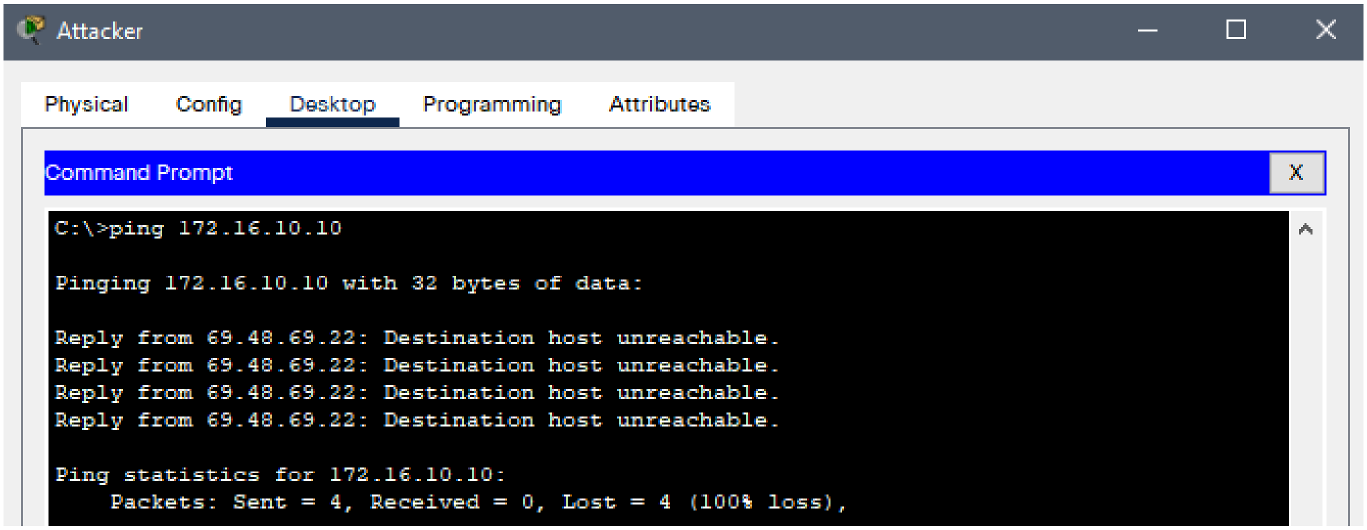
1. Command output after configuring SPAN (**`show monitor`**)



```
S1_120#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1_120(config)#monitor session 20 source interface fa0/4
S1_120(config)#monitor session 20 destination interface fa0/2
S1_120(config)#exit
S1_120#
%SYS-5-CONFIG_I: Configured from console by console

S1_120#show monitor
Session 20
---------
Type                       : Local Session
Description                : -
Source Ports               :
    Both                   : Fa0/4
Destination Ports          : Fa0/2
    Encapsulation          : Native
          Ingress          : Disabled
```

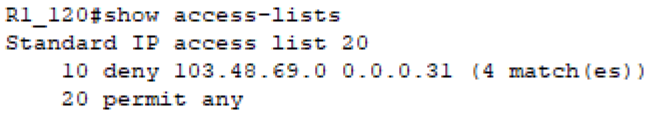
Step 4 (ACL):

1. Ping result after configuring ACL (from *Attacker* laptop to *Mail Server*)



```
C:\>ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:

Reply from 69.48.69.22: Destination host unreachable.
Reply from 69.48.69.22: Destination host unreachable.
Reply from 69.48.69.22: Destination host unreachable.
Reply from 69.48.69.22: Destination host unreachable.

Ping statistics for 172.16.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2. Command output after configuring ACL (**`show access-lists`**)



```
R1_120#show access-lists
Standard IP access list 20
    10 deny 103.48.69.0 0.0.0.31 (4 match(es))
    20 permit any
```