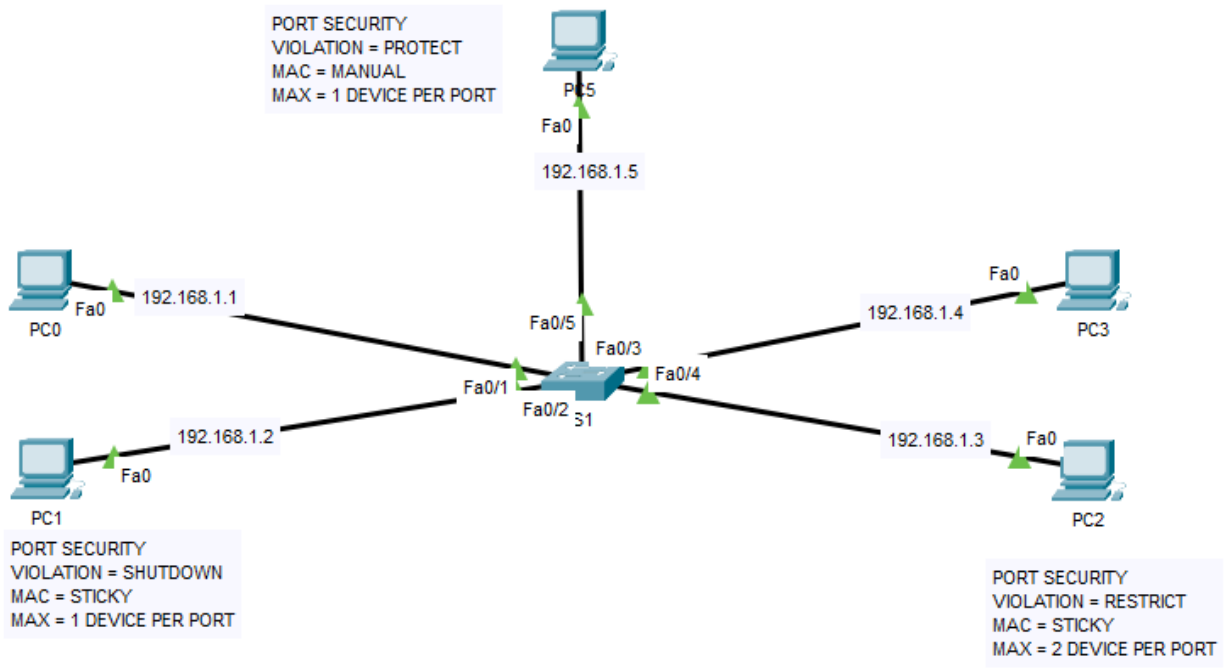
2024

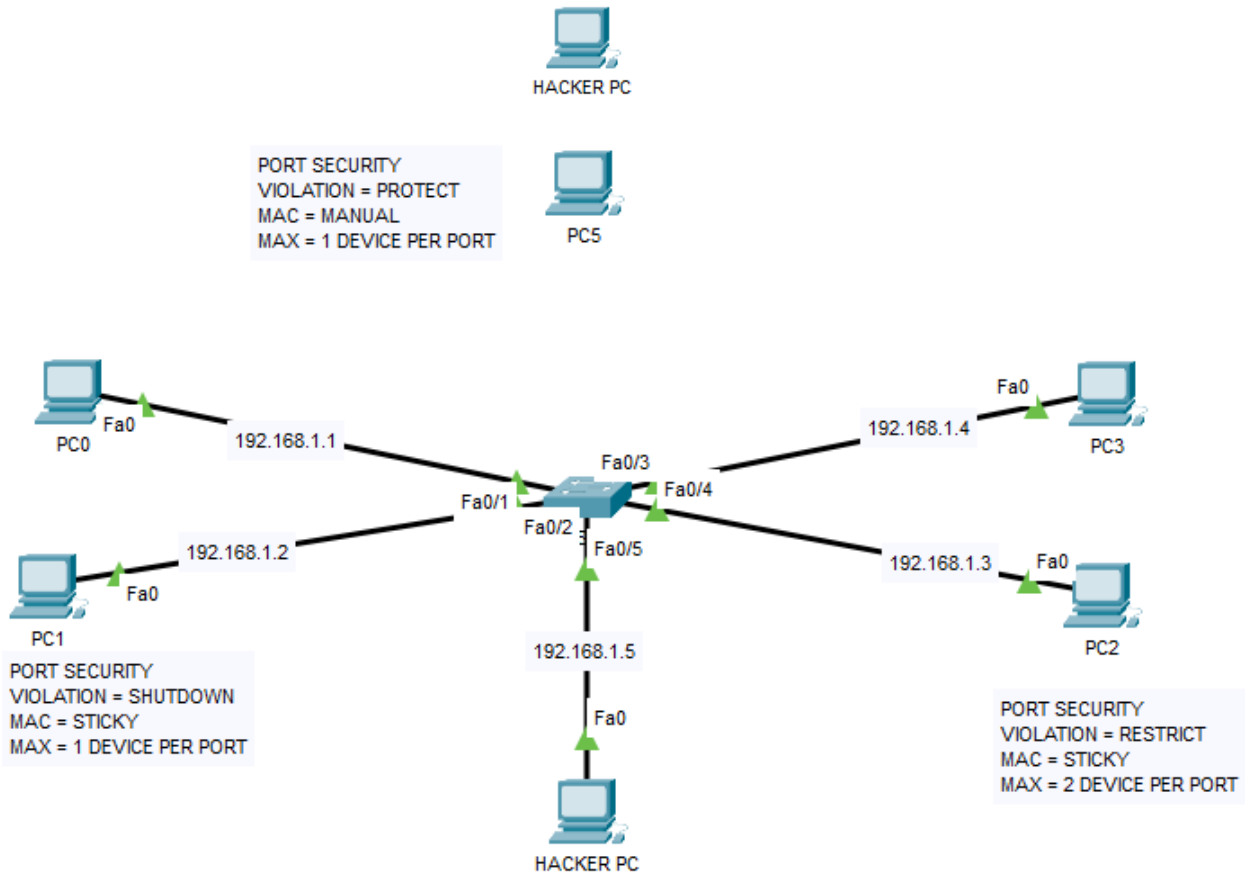
Port Security

CONFIGURING PORT SECURITY & SWITCHPORT SECURITY CONFIGURATION

INACIO ANDRE

- By default, all interfaces on a Cisco switch are turned on. That means that an attacker could connect to your network through a wall socket and potentially threaten your network. If you know which devices will be connected to which ports, you can use the Cisco security feature called **port security**. By using port security, a network administrator can associate specific MAC addresses with the interface, which can prevent an attacker to connect his device. This way you can restrict access to an interface so that only the authorized devices can use it. If an unauthorized device is connected, you can decide what action the switch will take, for example discarding the traffic and shutting down the port.


PORT SECURITY
VIOLATION = PROTECT
MAC = MANUAL
MAX = 1 DEVICE PER PORT
PC5
Fa0
192.168.1.5
Fa0/5
Fa0/3
Fa0/4
Fa0/1
Fa0/2
S1
PC0
Fa0
192.168.1.1
192.168.1.4
Fa0
PC3
192.168.1.2
Fa0
PC1
192.168.1.3
Fa0
PC2
PORT SECURITY
VIOLATION = SHUTDOWN
MAC = STICKY
MAX = 1 DEVICE PER PORT
PORT SECURITY
VIOLATION = RESTRICT
MAC = STICKY
MAX = 2 DEVICE PER PORT


HACKER PC
PORT SECURITY
VIOLATION = PROTECT
MAC = MANUAL
MAX = 1 DEVICE PER PORT
PC5
PC0
Fa0
192.168.1.1
192.168.1.4
Fa0
PC3
Fa0/3
Fa0/1
Fa0/4
Fa0/2
Fa0/5
192.168.1.2
Fa0
PC1
192.168.1.3
Fa0
PC2
192.168.1.5
Fa0
HACKER PC
PORT SECURITY
VIOLATION = SHUTDOWN
MAC = STICKY
MAX = 1 DEVICE PER PORT
PORT SECURITY
VIOLATION = RESTRICT
MAC = STICKY
MAX = 2 DEVICE PER PORT

S1

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#int range f0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation shutdown
```

```
S1(config)#int range f0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum 2
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation restrict
```

```
S1(config)#int f0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport port-security mac-address 0003.E499.2D94
S1(config-if)#switchport port-security violation protect
```

```
S1(config)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)         (Count)
------------------------------------------------------------------------
        Fa0/1         1           0                0          Shutdown
        Fa0/2         1           0                0          Shutdown
        Fa0/3         2           0                0          Restrict
        Fa0/4         2           0                0          Restrict
        Fa0/5         1           1                0           Protect
------------------------------------------------------------------------
```

From PC0 TO PC2

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

From PC0 TO PC3

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

From HACKER PC TO PC3, Using fa0/5

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

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

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```