Port Security Violation

OSI Layer Layer 2 - Data Link Layer

Cause of Issue: If a port on the switch is configured with the Port Security feature and a device is connected to this port with a MAC address that is not predefined, the switch considers this as a security violation. In this case, depending on the configured violation behaviour (violation mode) of the port: The port can be completely closed (shutdown mode), it can only stop traffic but the port remains open (restrict mode), or it can only silently block incoming traffic (protect mode). This is an access control mechanism at Layer 2 level and is used to prevent malicious people with physical access from connecting to the network without authorisation.

Admin Guide - Port Security Application Steps

Step 1: Enabling Port Security: The port security feature is activated on the relevant switch port.

```
Switch(config-if)# switchport port-security
```

Step 2: Defining a Fixed MAC Address (Optional): It is used to allow access only to a specific MAC address.

```
Switch(config-if)# switchport port-security mac-address 0011.2233.4455
```

Step 3: Maximum Allowed MAC Number**:** The maximum number of MAC addresses that can be learnt on the port is limited.

```
Switch(config-if)# switchport port-security maximum 1
```

Step 4: Setting the Security Violation Mode**:** Determines how the port behaves in case of a violation:

protect: The traffic of the violating device is blocked, the port is not closed.

restrict: Traffic is blocked, also syslog/snmp notification is made.

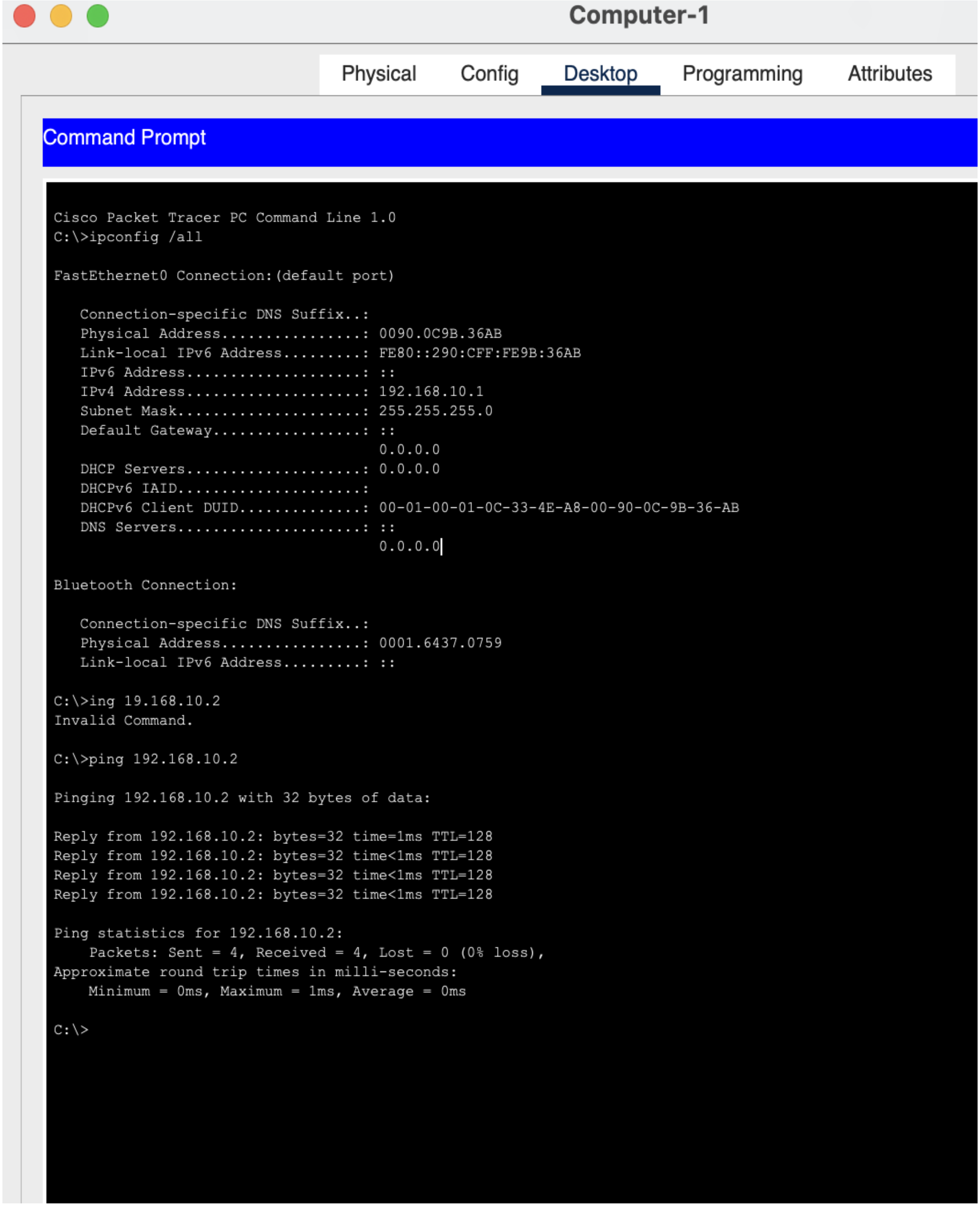
shutdown: The port is completely closed (default behaviour).

```
Switch(config-if)# switchport port-security violation shutdown
```

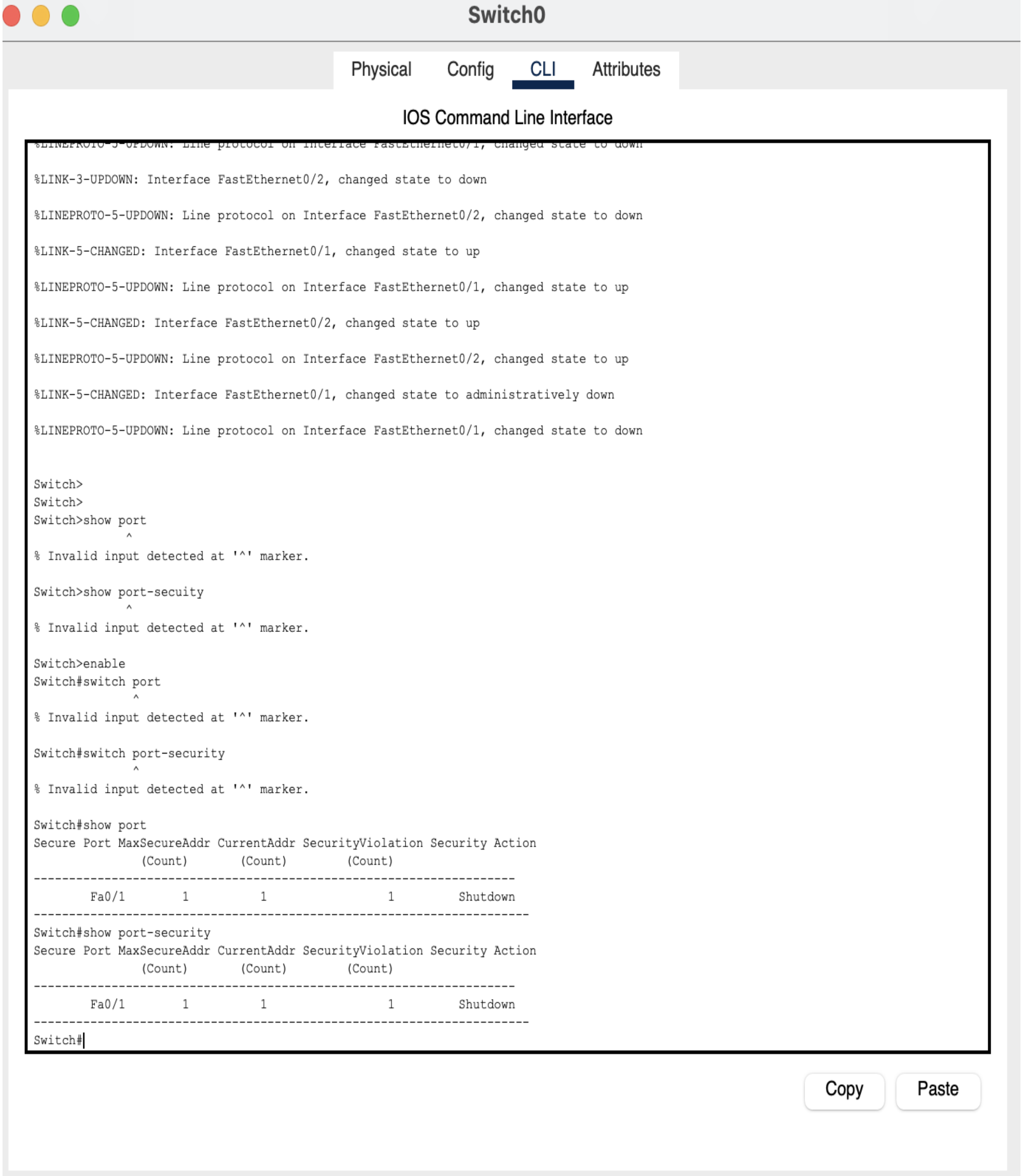
Step 5: Log and Monitoring**:** Syslog and/or SNMP support must be configured for centralised monitoring of port security events.

logging, snmp-server enable traps port-security)

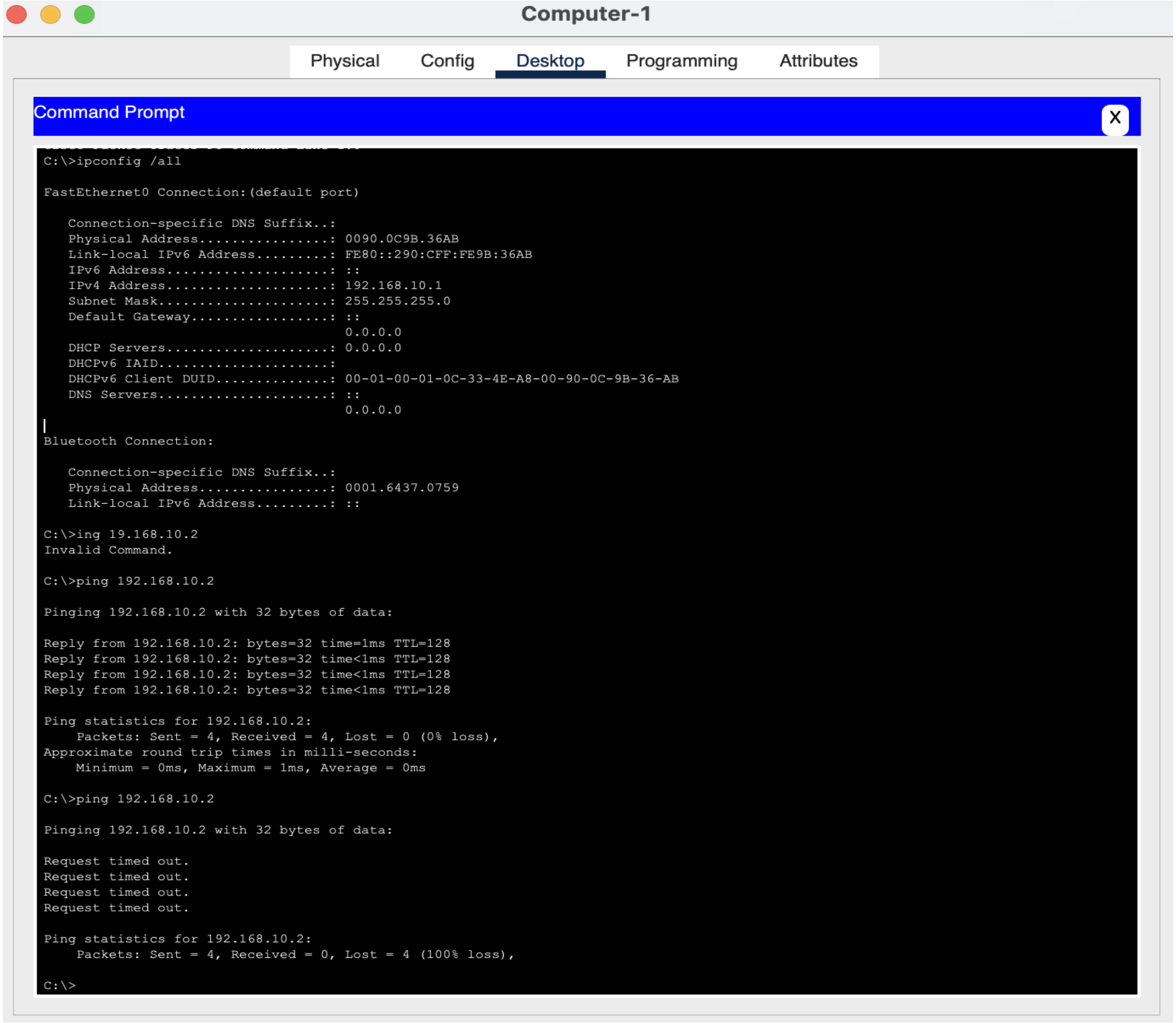
Simulation:



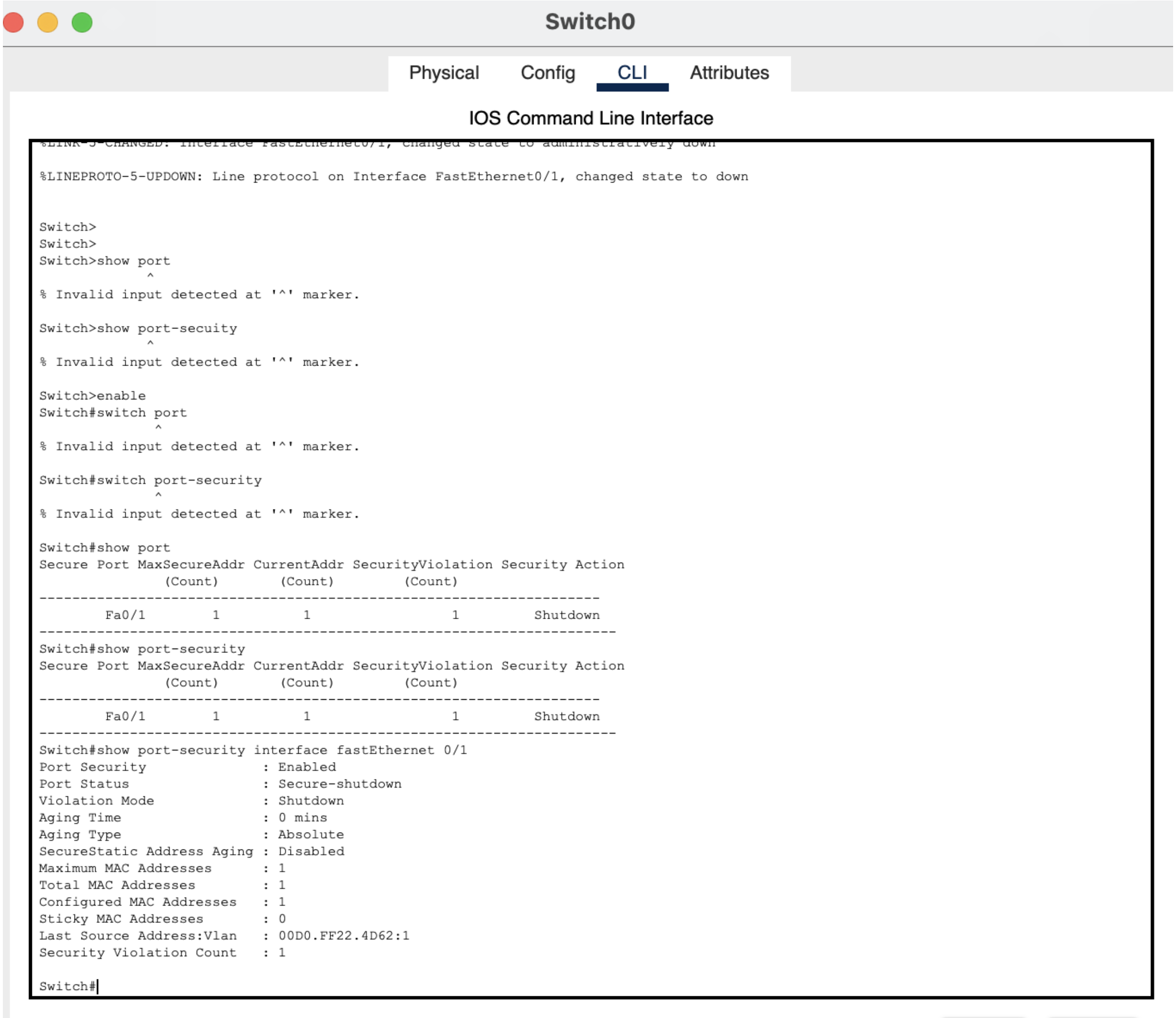
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0090.0C9B.36AB
   Link-local IPv6 Address.........: FE80::290:CFF:FE9B:36AB
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.10.1
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-0C-33-4E-A8-00-90-0C-9B-36-AB
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.6437.0759
   Link-local IPv6 Address.........: ::

C:\>ing 19.168.10.2
Invalid Command.

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down


Switch>
Switch>
Switch>show port
             ^
% Invalid input detected at '^' marker.

Switch>show port-secuity
             ^
% Invalid input detected at '^' marker.

Switch>enable
Switch#switch port
              ^
% Invalid input detected at '^' marker.

Switch#switch port-security
              ^
% Invalid input detected at '^' marker.

Switch#show port
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 1         Shutdown
----------------------------------------------------------------------
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 1         Shutdown
----------------------------------------------------------------------
Switch#
```



```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0090.0C9B.36AB
   Link-local IPv6 Address.........: FE80::290:CFF:FE9B:36AB
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.10.1
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-0C-33-4E-A8-00-90-0C-9B-36-AB
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.6437.0759
   Link-local IPv6 Address.........: ::

C:\>ing 19.168.10.2
Invalid Command.

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

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

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down


Switch>
Switch>
Switch>show port
             ^
% Invalid input detected at '^' marker.

Switch>show port-secuity
             ^
% Invalid input detected at '^' marker.

Switch>enable
Switch#switch port
              ^
% Invalid input detected at '^' marker.

Switch#switch port-security
              ^
% Invalid input detected at '^' marker.

Switch#show port
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 1         Shutdown
----------------------------------------------------------------------
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 1         Shutdown
----------------------------------------------------------------------
Switch#show port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00D0.FF22.4D62:1
Security Violation Count   : 1

Switch#
```

Initially, the MAC address of Computer-1 connected to the switch is assigned as secure MAC. Later, when Computer-2 with a different MAC address was connected to the same port, the port went into "shutdown" state due to security policy. Therefore, ping traffic between PC1 and PC2 was interrupted and logged as Violation Count: 1

Switch Message Comment:

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

Fa0/1 1 1 1 1 1 Shutdown

Switch#show port-security

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
            (Count) (Count) (Count)
------------------------------------------------------------------
      Fa0/1 1 1 1 1 1        Shutdown
--------------------------------------------------------------------
Switch#show port-security interface fastEthernet 0/1
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 00D0.FF22.4D62:1
Security Violation Count : 1
```

Description:

Only 1 MAC address defined on Fa0/1 port

MaxSecureAddr: 1

However, an unauthorised MAC address is connected through this port

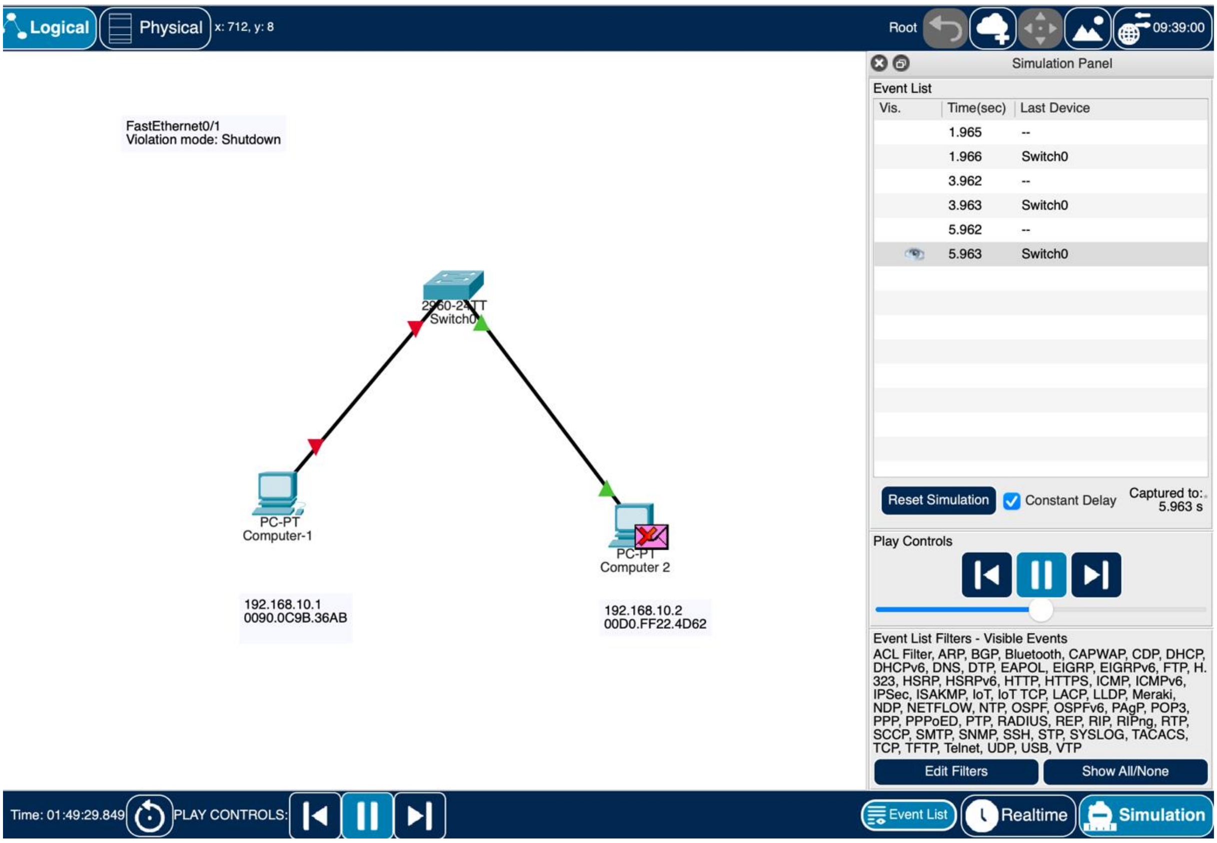
SecurityViolation: 1

As a result, it went into "Shutdown" mode and the port closed automatically.

The state of the port: Secure shutdown: closed for security reasons

Violation Mode: Shutdown: in this mode the port is completely shut down (traffic proof) when there is a violation.

Last violator MAC address: 00D0.FF22.4D62 → This device was seen as unauthorised by the port.



FastEthernet0/1
Violation mode: Shutdown

192.168.10.1
0090.0C9B.36AB

192.168.10.2
00D0.FF22.4D62

Event List

Vis.	Time(sec)	Last Device
	1.965	--
	1.966	Switch0
	3.962	--
	3.963	Switch0
	5.962	--
👁	5.963	Switch0

☑ Constant Delay

Captured to: 5.963 s

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Port traffic is interrupted. The port is in "Secure-shutdown" mode.

This means that this port can no longer send or receive any data packets. The device connected to that port loses network connection (cannot get IP, cannot go to the Internet, cannot access the LAN).

Security Breach Counter Increases

Security Violation: This was triggered when an unauthorised MAC address was connected. Each new violation increases this counter.

The port does not open automatically; administrator intervention is required. It must be manually up-down (shutdown / no shutdown). Or the MAC address causing the violation must be added to the list of authorised addresses.

Syslog/SNMP Warning: If there is a log server or SNMP monitoring in the system, it will be logged as a security violation.

For example, when an unauthorised laptop is connected to a computer network and the MAC address of this laptop is not defined in the port, the port is automatically closed.

The user says "I cannot go online" but there is no physical problem in the hardware. In fact, the switch has closed the port for security reasons.

Simulation File Name: P10_210316084_BinnurSöztutar_Port_Security_Violation.pkt