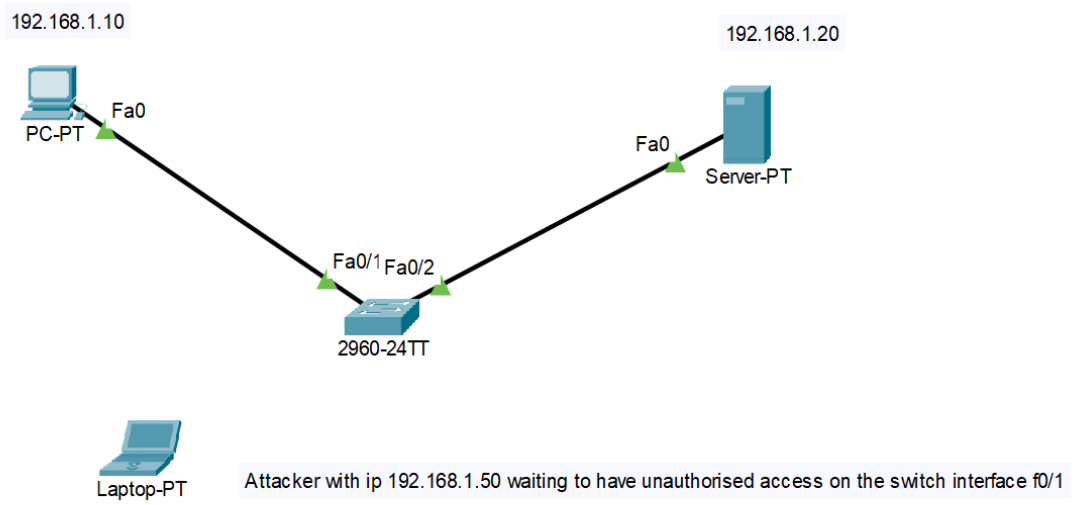
Port Security Implementation Guide

Notes prepared by: **Baba Shaheer**
Email: b.shaheer@ulster.ac.uk

Network Overview



Network Diagram

- **PC-PT**: 192.168.1.10 (Connected to switch port Fa0/1)
- **Laptop-PT**: Any IP (e.g., 192.168.1.50) - Used to demonstrate security violation
- **Server-PT**: 192.168.1.20
- **Switch**: Cisco Catalyst 2960-24TT

Introduction

This guide provides detailed instructions for implementing port security on a Cisco Catalyst switch. Port security limits the number of valid MAC addresses allowed on a port and can shut down ports when violations occur, protecting the network from unauthorized access attempts.

What is Port Security?

Port security is a Layer 2 security feature that allows you to restrict which MAC addresses can use a specific switch port. This helps prevent several common network attacks:

1. **MAC Flooding Attacks**: Attackers flood switches with fake MAC addresses to overflow the CAM table

2. **Rogue Device Prevention**: Unauthorized devices can't connect to network ports
3. **MAC Spoofing Protection**: Prevents devices from impersonating authorized devices

In our scenario, we'll implement the most common use case: restricting a port to a single authorized device (PC-PT) and automatically shutting down the port if an unauthorized device (Laptop-PT) attempts to connect.

Step-by-Step Implementation

1. Basic Switch Configuration

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname Switch2960
Switch2960(config)# enable secret cisco
Switch2960(config)# line console 0
Switch2960(config-line)# password cisco
Switch2960(config-line)# login
Switch2960(config-line)# exit
Switch2960(config)# line vty 0 15
Switch2960(config-line)# password cisco
Switch2960(config-line)# login
Switch2960(config-line)# exit
Switch2960(config)# service password-encryption
```

2. Configure Port Security on Fa0/1

```
Switch2960(config)# interface fastEthernet 0/1
Switch2960(config-if)# switchport mode access         # Sets the port to
access mode (required for port security)
Switch2960(config-if)# switchport port-security       # Enables port security
on the interface
```

> **What's happening**: Before enabling port security, the interface must be configured as an access port. Port security cannot be enabled on dynamic ports (those set to "dynamic auto" or "dynamic desirable"). Once port security is enabled, the port will begin monitoring MAC addresses.

3. Configure Port Security Parameters

```
Switch2960(config-if)# switchport port-security maximum 1        # Allows
only 1 MAC address on this port
Switch2960(config-if)# switchport port-security mac-address sticky    #
Dynamically learns and saves MAC addresses
Switch2960(config-if)# switchport port-security violation shutdown     #
Shuts down port if violation occurs
Switch2960(config-if)# exit
```

> **What's happening**: - `maximum 1` restricts the port to only allowing a single MAC address. This is perfect for end-user ports where only one device should be connected. - `mac-address sticky` tells the switch to automatically learn the MAC

address of the first connected device (PC-PT in our case) and add it to the running-config. This MAC address becomes the only authorized device for this port. - `violation shutdown` configures the switch to completely disable the port if any unauthorized device (different MAC address) attempts to connect. This is the most secure violation mode.

4. Verify Port Security Configuration

```
Switch2960# show port-security interface fastEthernet 0/1
```

Expected output:

```
Port Security              : Enabled
Port Status                : Secure-up
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   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : XXXX.XXXX.XXXX:1
Security Violation Count   : 0
```

5. Test Port Security - Initial Connection

1. Connect PC-PT (192.168.1.10) to Fa0/1
2. The switch will automatically learn and "stick" the MAC address of PC-PT
3. Verify connectivity by pinging Server-PT (192.168.1.20)

```
PC-PT> ping 192.168.1.20
```

What's happening: When you connect the PC to the port for the first time after enabling sticky learning, the switch detects the PC's MAC address and adds it to its secure address table. This MAC address is now considered the only legitimate device for this port. The switch will also add this MAC address to the running configuration (but not the startup configuration unless you save it with "copy running-config startup-config").

You can verify that the MAC address was learned with the following command:

```
Switch2960# show port-security address
```

At this point, normal network communication is possible, and the PC can successfully communicate with the server.

6. Testing Violation Scenario

1. Disconnect PC-PT from Fa0/1
2. Connect Laptop-PT with IP 192.168.1.50 to Fa0/1

3. The port should shut down automatically due to MAC address violation
4. Verify port status:

   `Switch2960# show interface fastEthernet 0/1 status`

   Expected output: `fastEthernet0/1 err-disabled`

What's happening: When you disconnect PC-PT and connect Laptop-PT, the switch detects a new MAC address attempting to use the port. Since we configured: - Maximum of 1 MAC address allowed - Sticky learning already recorded PC-PT's MAC address - Violation mode set to "shutdown"

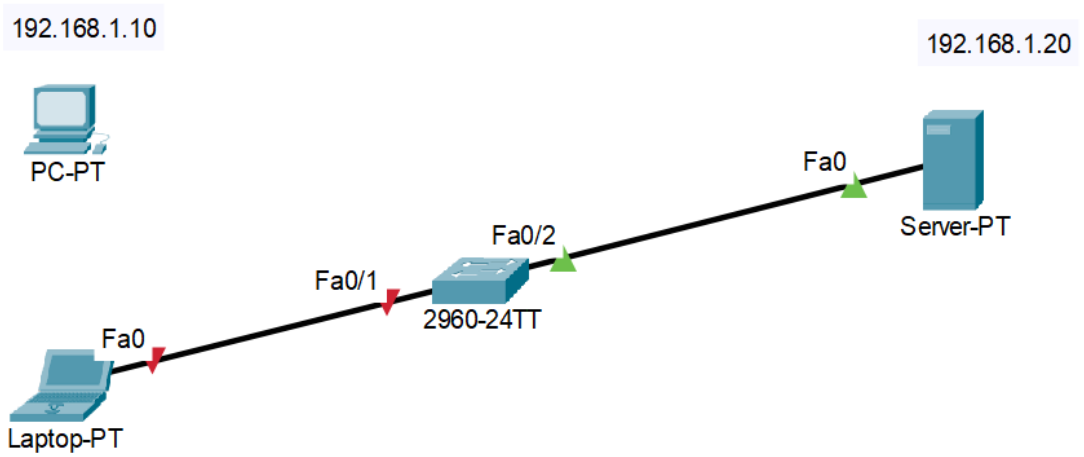
The switch immediately places the port in "err-disabled" state (administratively shutdown). This completely blocks all traffic, effectively preventing the unauthorized laptop from accessing the network. The switch also generates a log message about the security violation.

This is exactly the "BOOM" moment described in your scenario - the unauthorized device cannot establish communication with the server because the switch port immediately shuts down when it detects the violation.

You can check the violation counter with:

```
Switch2960# show port-security interface fastEthernet 0/1
```

The "Security Violation Count" will have increased by 1.



7. Recovering from Port Security Violation

```
Switch2960# configure terminal
Switch2960(config)# interface fastEthernet 0/1
Switch2960(config-if)# shutdown          # Manually shut down the already
```

```
err-disabled port
Switch2960(config-if)# no shutdown       # Re-enable the port
Switch2960(config-if)# exit
```

What's happening: When a port is in err-disabled state due to a security violation, you must manually recover it. This two-step process (shutdown/no shutdown) resets the port and allows it to become operational again. However, the port security features remain active, so:

1. If you reconnect the original PC-PT (with the authorized MAC address), the port will work normally.
2. If you connect the unauthorized Laptop-PT again, the port will immediately go back into err-disabled state.

This manual recovery requirement ensures that a network administrator is aware of the security violation and takes deliberate action to restore connectivity.

8. Optional: Configure Auto-Recovery from Violations

```
Switch2960(config)# errdisable recovery cause psecure-violation    # Enable
auto-recovery for port security violations
Switch2960(config)# errdisable recovery interval 300               # Set
recovery time to 300 seconds (5 minutes)
```

What's happening: In production environments, having to manually recover ports can create significant administrative overhead. The auto-recovery feature automatically brings ports back online after a specified timeout period (300 seconds in this example).

This is useful because: 1. It reduces the need for administrator intervention for temporary issues 2. It prevents extended outages for legitimate users if a violation was accidental 3. It still provides security by keeping the port disabled during the timeout period

However, be aware that if an attacker is persistent, they might see the port reactivate and continue attempting to access it. Monitoring systems should be configured to alert administrators of repeated violations.

9. Verify Learned MAC Addresses

```
Switch2960# show port-security address
```

Port Security Configuration Options

Violation Modes:

- **Shutdown** (Default): The interface is error-disabled, traffic is dropped, and no notifications are sent

  ```
  Switch2960(config-if)# switchport port-security violation shutdown
  ```

  This is the most secure option and was used in our demonstration. When violated, the port is completely disabled until manually reset or auto-recovery occurs.

- **Restrict**: Drops packets with unknown source addresses, increments violation counter, and sends SNMP traps

  ```
  Switch2960(config-if)# switchport port-security violation restrict
  ```

  This mode allows the port to remain operational but drops unauthorized traffic. It's useful when you want to track violations without disabling the port completely.
- **Protect**: Silently drops packets with unknown source addresses but keeps the port operational

  ```
  Switch2960(config-if)# switchport port-security violation protect
  ```

  This is the least secure mode as it doesn't log or notify about violations. It simply drops unauthorized traffic without alerting administrators.

MAC Address Learning Methods:

- **Static**: Manually configure specific MAC address(es)

  ```
  Switch2960(config-if)# switchport port-security mac-address
  XXXX.XXXX.XXXX
  ```

- **Sticky**: Dynamically learns and adds MAC addresses to the running configuration

  ```
  Switch2960(config-if)# switchport port-security mac-address sticky
  ```

- **Dynamic**: Learns MAC addresses but removes them when the switch restarts or the interface shuts down

Security Considerations

- Port security helps prevent unauthorized access to the network
- "Sticky" learning simplifies configuration by automatically learning MAC addresses
- Shutdown violation mode provides the highest security but requires manual intervention
- Consider implementing SNMP traps to alert administrators of security violations

Troubleshooting Commands

```
Switch2960# show port-security                          # Shows global port
security statistics
Switch2960# show port-security address                  # Lists all secure
MAC addresses on all ports
Switch2960# show port-security interface fastEthernet 0/1    # Detailed port
security info for a specific interface
Switch2960# show errdisable recovery                    # Shows which error
causes will auto-recover
Switch2960# show interfaces status err-disabled         # Lists all
interfaces in err-disabled state
```

Monitoring and Maintenance Notes: - Check port security violations regularly as they indicate potential security incidents - After setting up port security, save the configuration to preserve learned sticky addresses `Switch2960# copy running-config startup-config` - If legitimate device replacement is needed, you'll need to update the secure MAC address by: 1. Clearing the current MAC address: `Switch2960(config-if)# no switchport port-security mac-address sticky` 2. Reconnecting the new device (the switch will learn its MAC address) 3. Saving the configuration

Common Issues and Solutions

Issue	Possible Cause	Solution
Port unexpectedly in err-disabled state	Security violation occurred	Check violation count and recover port
MAC address not learning	Port not in access mode	Configure interface as access port
Multiple devices needed on single port	Maximum addresses set too low	Increase maximum addresses limit
Port doesn't auto-recover	Auto-recovery not configured	Configure errdisable recovery

---