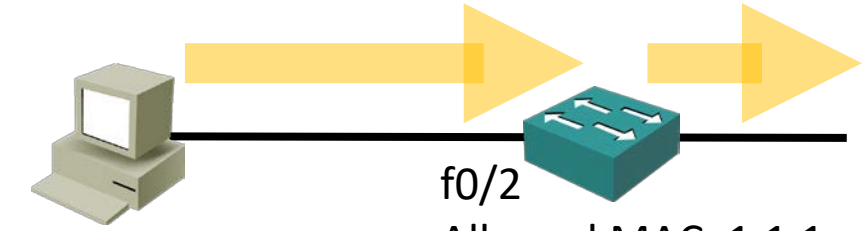
Shut Down Unused Interfaces

- Best practice is to administratively shut down unused switch ports
- This stops somebody getting access to the network if they physically connect to the port

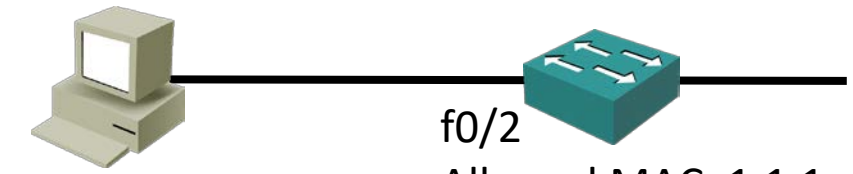
```
SW1(config)#int f0/2
SW1(config-if)#shutdown
```

Port Security

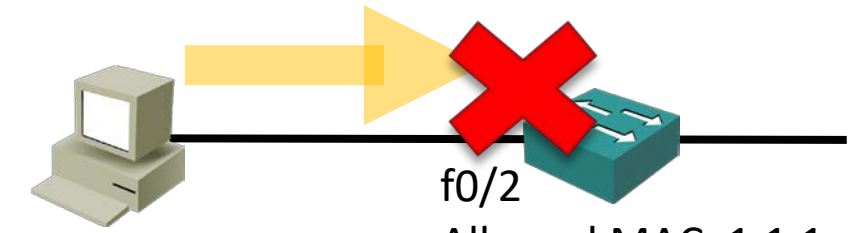
- Port Security enables an administrator to specify which MAC address or addresses can send traffic in to an individual switch port.
- This can be used to lock a port down to a particular host or hosts



Port Security

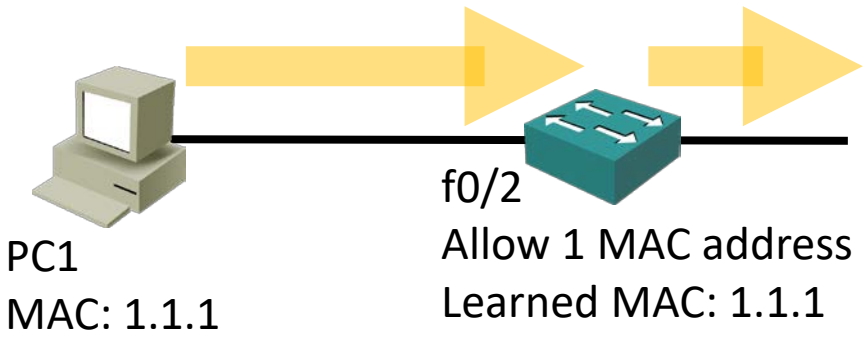


Port Security



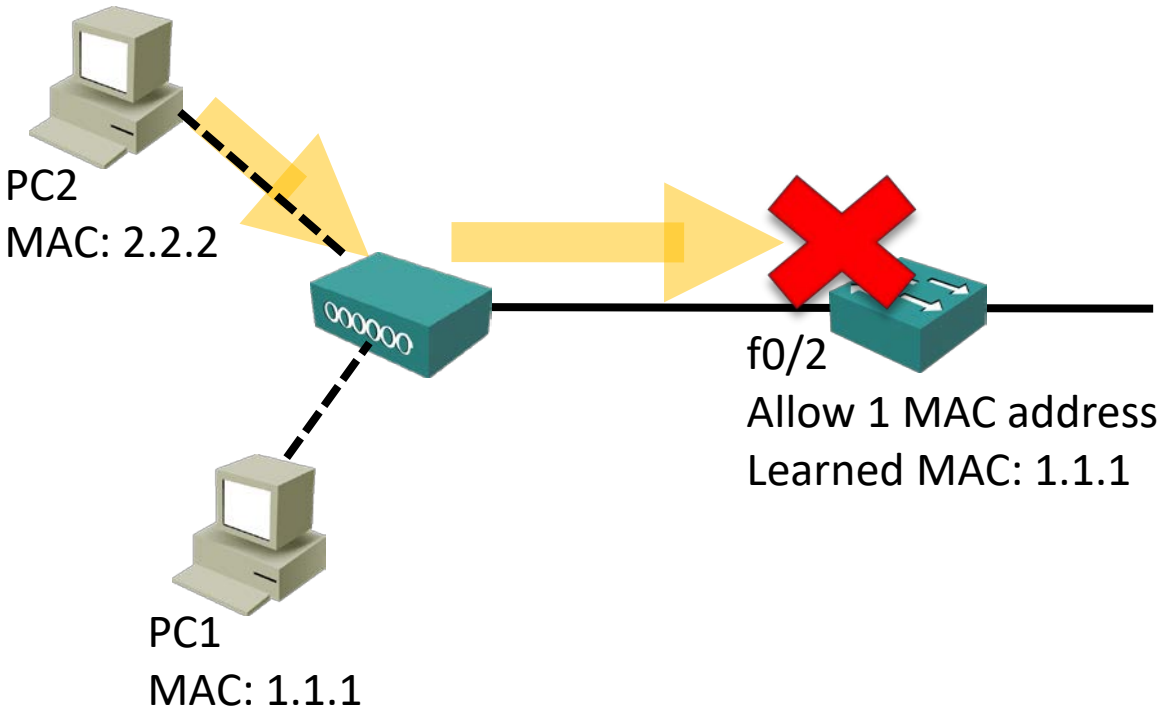
Port Security

- It is easy to spoof a MAC address, so locking ports down to a specific host is not usually Port Security's main role in production networks
- Port Security can also configure individual switch ports to allow only a specified number of source MAC addresses to send traffic in to the port
- It can learn connected MAC addresses



Port Security

- This is useful to prevent users from adding Wireless Access Points or other shared devices



Port Security Configuration

```
SW1(config)#int f0/2
SW1(config-if)#switchport port-security
```

Port Security Default Behaviour

- If you configure Port Security with no additional parameters then only one MAC address is allowed to transmit on the port
- The current MAC address can be disconnected and replaced. The port is not locked down to a particular MAC address
- If a shared device is connected and multiple hosts try to transmit the port will be shut down

Port Security Verification - Defaults

```
SW1#show port-security interface f0/2
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 : 0
Last Source Address:Vlan : 0000.0CA0.A359:1
Security Violation Count : 0
```

Security Violation Actions

- You have three options when an unauthorised MAC address sends traffic in to the port:
  - **Shutdown (Default):** The interface is placed into the error-disabled state, blocking all traffic
  - **Protect:** Traffic from unauthorised addresses is dropped. Traffic from allowed addresses is forwarded
  - **Restrict:** Traffic from unauthorised addresses is dropped, logged and the violation counter incremented. Traffic from allowed addresses is forwarded

Violation Action Configuration

```
SW1(config)#int f0/2
SW1(config-if)# switchport port-security violation protect

SW1(config-if)# switchport port-security violation restrict
```

Error-Disabled Interfaces

- If the Violation Action is set to Shutdown and a violation occurs, the port will move to an error-disabled state
- To bring an error-disabled interface back into service:
  - Physically remove the host with the offending MAC address
  - Manually shutdown then no shutdown the interface

Auto-Recovery

- You can bring error disabled ports back into service automatically after they have been disabled for a configurable period of time (in seconds)

```
SW1(config)# errdisable recovery cause psecure-violation
SW1(config)# errdisable recovery interval 600
```