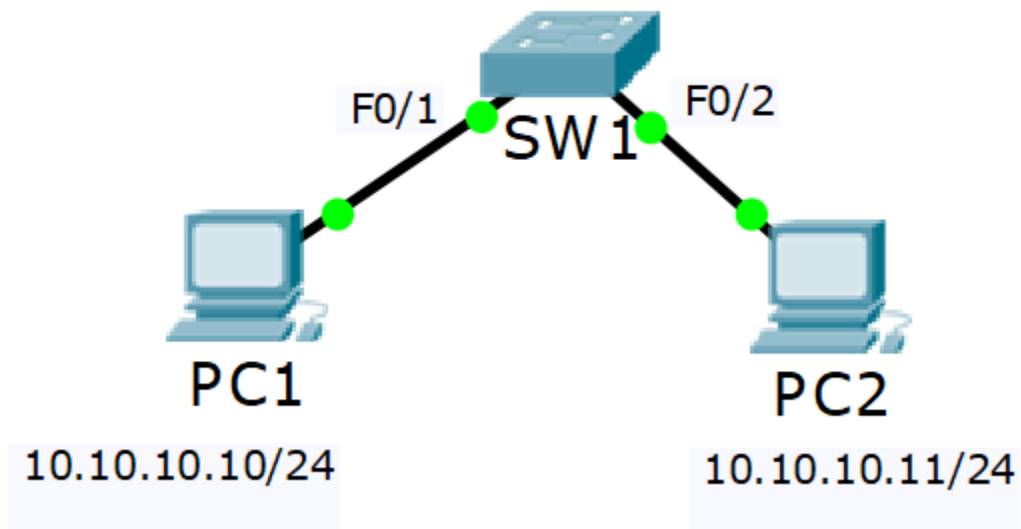


## **27-1 Port Security Configuration Lab** **Exercise**

In this lab you will configure Port Security on a small campus network.

### **Lab Topology**



### **Load the Startup Configurations**

Open the '27-1 Port Security Configuration.pkt' file in Packet Tracer to load the lab.

## Disable Unused Ports

- 1) Disable all unused ports on SW1. This prevents unauthorised hosts plugging in to them to gain access to the network.

## Port Security Configuration

- 2) Configure Port Security on interface FastEthernet 0/1. Allow a maximum of two MAC addresses and manually add PC1's MAC address to the configuration.

**Important:** After enabling Port Security, do not send traffic between the PCs (for example 'ping') until you have manually added PC1's MAC address to the configuration. If you do, Port Security will learn PC1's MAC address dynamically and Packet Tracer has no function to remove it.

This results in the error "Found duplicate mac-address". In this case you have to shutdown interface Fa0/1, save the configuration, reload then add PC1's MAC address before enabling interface Fa0/1 again.

Shutting down the interface is necessary because PC1 sends gratuitous ARPs when its interface comes up.

- 3) Enable Port Security on interface FastEthernet 0/2 with the default settings.
- 4) From PC1 or PC2, generate some traffic between the PCs.
- 5) On SW1, use a 'show port-security' command to verify if the MAC address of PC2 has been learned by Port Security.
- 6) Verify the full Port Security configuration on both interfaces. Do not use the 'show running-config' command in this task.