ISLAMIC UNIVERSITY OF TECHNOLOGY

Organization of Islamic Cooperation

Board Bazar, Gazipur

Laboratory Report

CSE 4512

**Title**: Configuring Switch Port Security in Cisco Devices

**Objective**:

* Describe the concept of Switch Port Security
* Explain importance of Switch Port Security in securing an organization
* Configure Switch Port Security in CISCO devices
* Use Switch Port Security feature to achieve varying degrees of protection

**Devices/Software Used**: Cisco Packet Tracer

**Theory**:

Ways of Learning and limiting MAC addresses on a secure port:

The maximum number of MAC address on a secure port can be limited using the switchport port-security maximum value command.

There are three ways in which we can tell the switch to learn MAC addresses:

Manual Configuration – We manually enter the valid MAC addresses.

Dynamic Learning – The MAC addresses are automatically learnt by the switch when a device is connected to the port but are forgotten upon restart.

Dynamic Learning (Sticky) – The dynamically learnt MAC addresses are added to the running configuration, from where they can be saved to the NVRAM and thus not forgotten upon restart.

Port security aging:

This option allows us to specify a time after which the MAC addresses that are allowed on the port are removed. We can also set the aging type, which can be either absolute, which simply removes the devices after the specified time, or inactivity, which removes the devices only if they are inactive for the specified amount of time.

Port security violations:

This option allows us to specify what action to take if there is a violation. The action can be of one of three types:

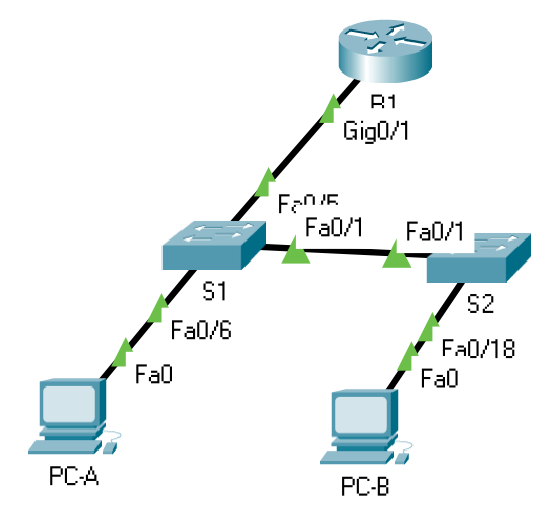
Protect – Drop all traffic from the offending device.

Restrict – Drop all traffic from the offending device, log the violation and increment the violation counter.

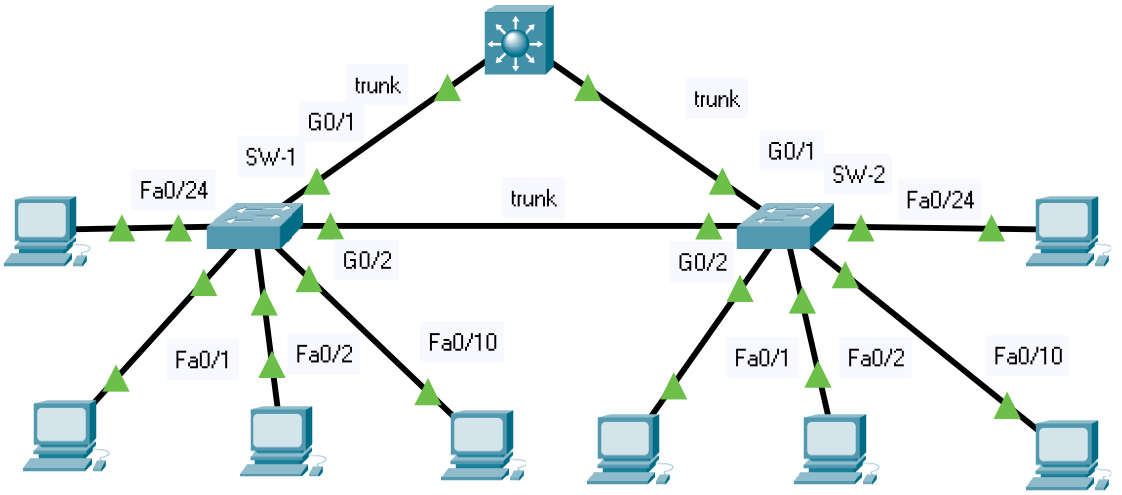
Shutdown – Send the switchport into error disabled mode, where no further traffic is forwarded. This is the default mode. It can be reset by disabling and re-enabling the switchport. The violation is also logged and the violation counter is incremented.

**Diagram of the experiment**:

Task 1:



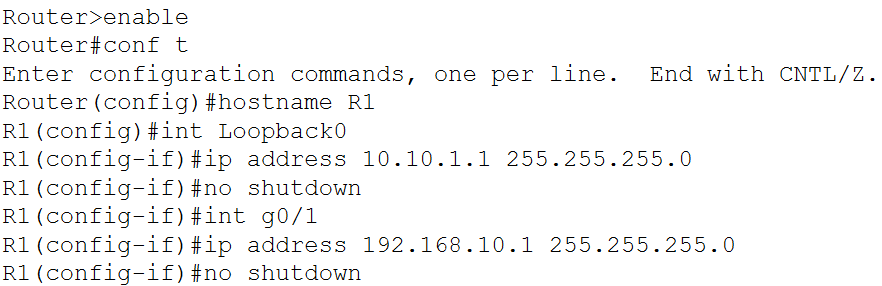
Task 2:



**Working Procedure**:

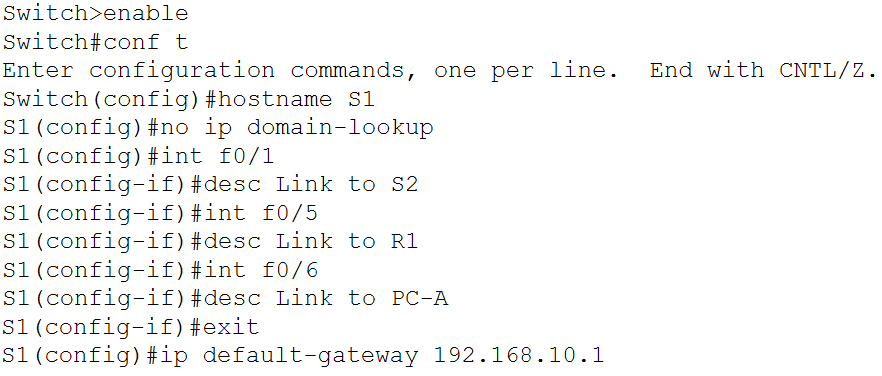
Task 1

1. The network was cabled as shown in the diagram above.
2. R1 was configured:

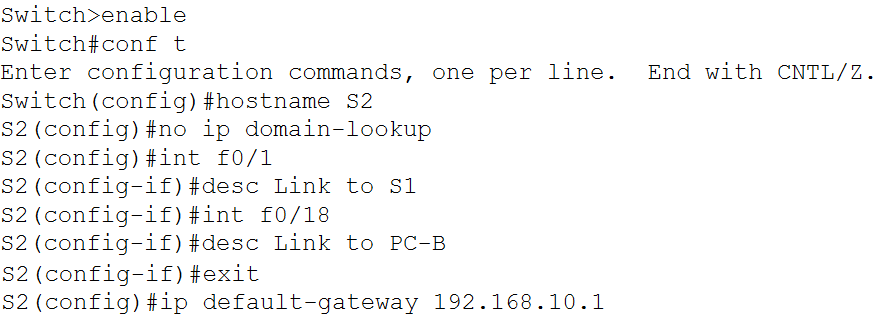


1. Basic switch settings were configured:

S1:

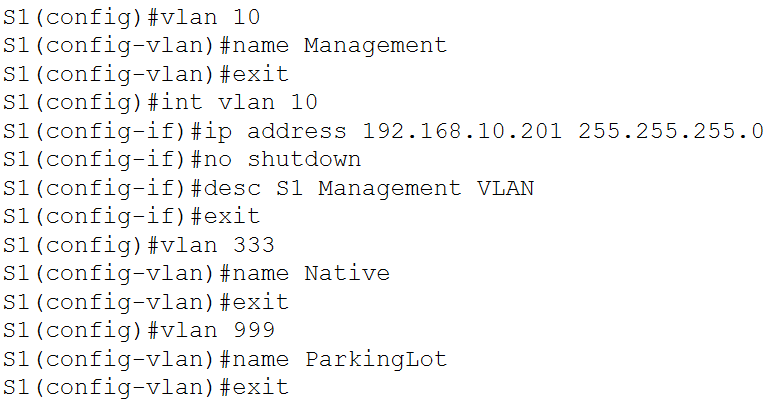


S2:

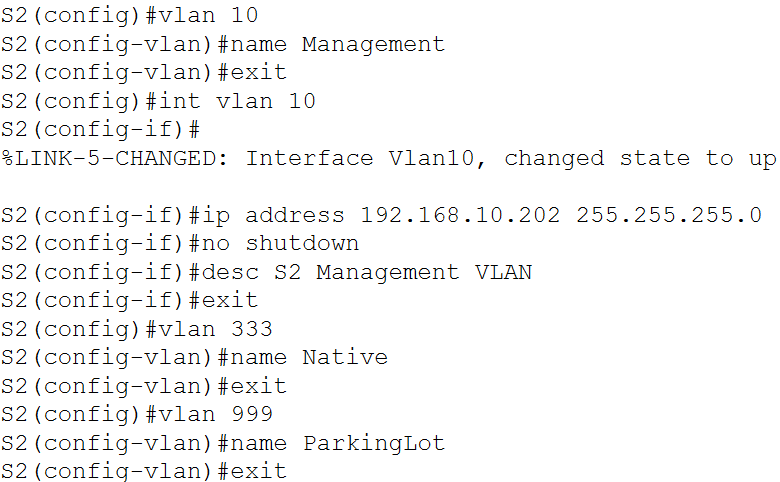


1. VLAN was configured on switches:

S1:

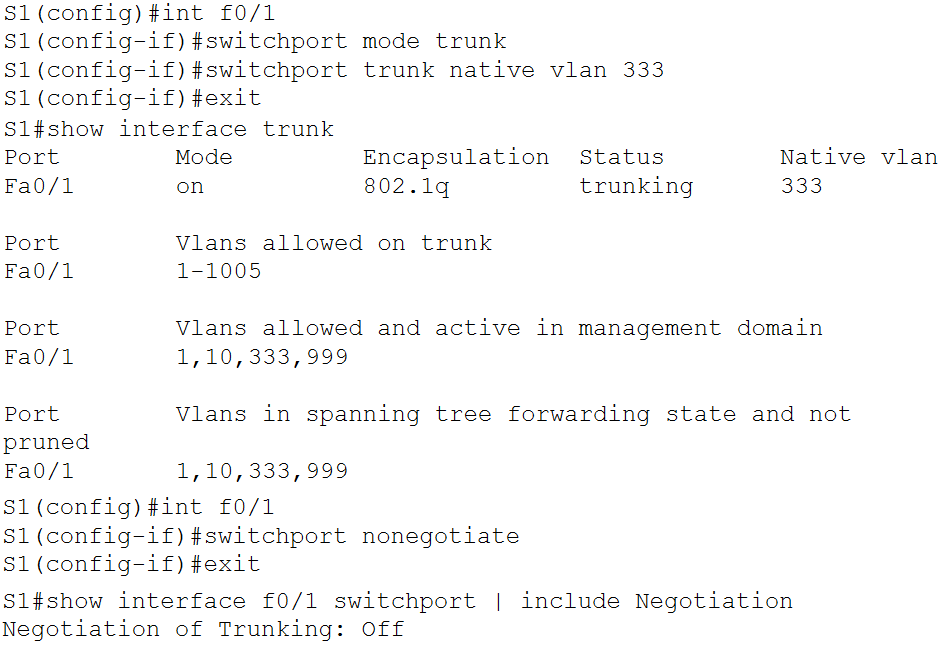


S2:

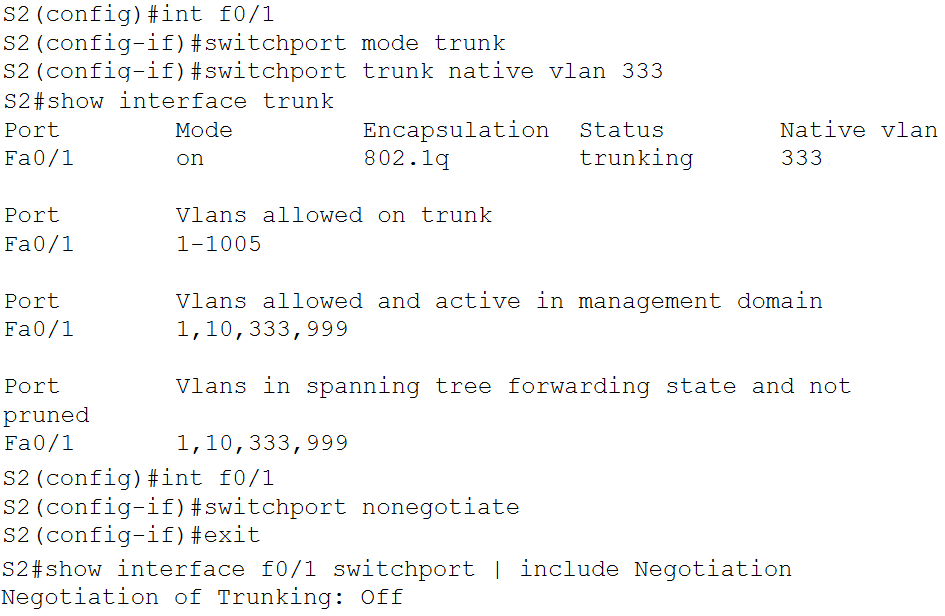


1. Trunking was implemented on each of the switches:

S1:

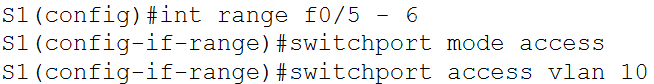


S2:

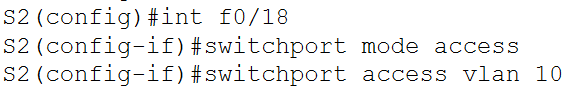


1. Configured access ports on switches:

S1:

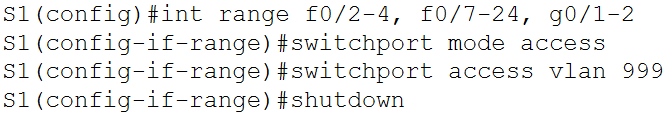


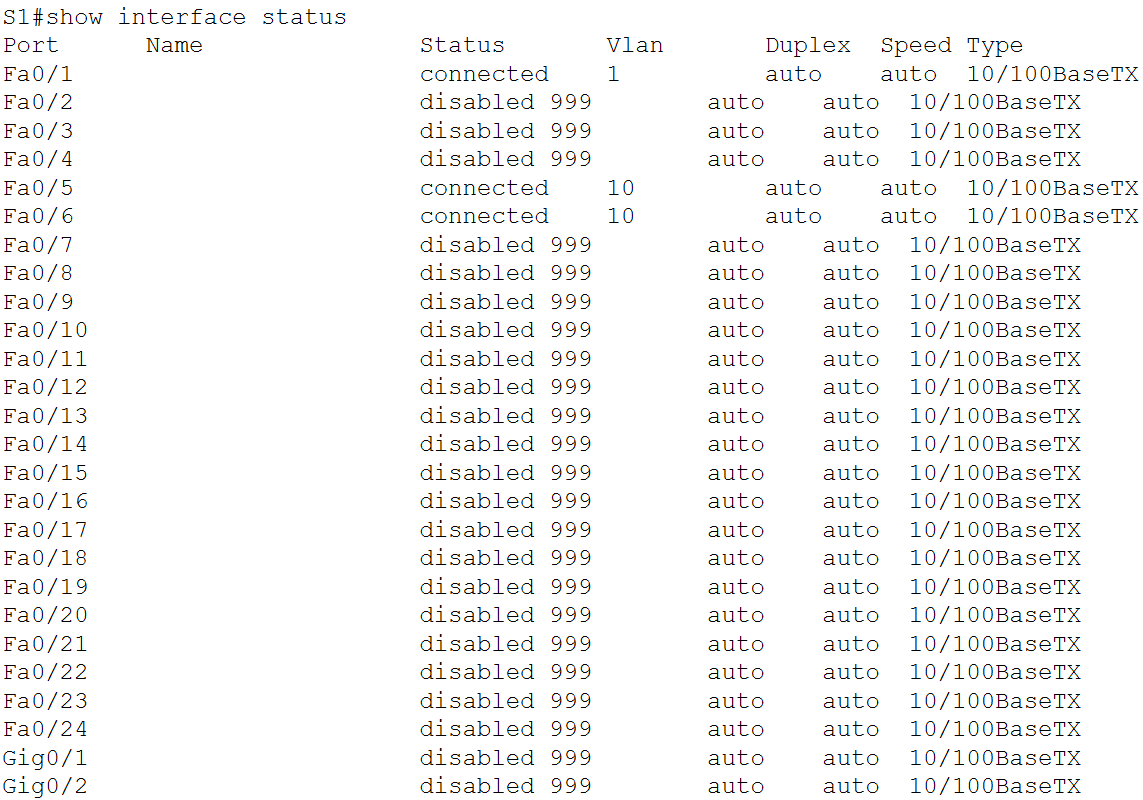
S2:



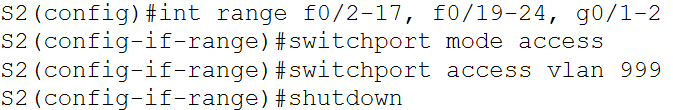
1. Secured and disabled unused switchports:

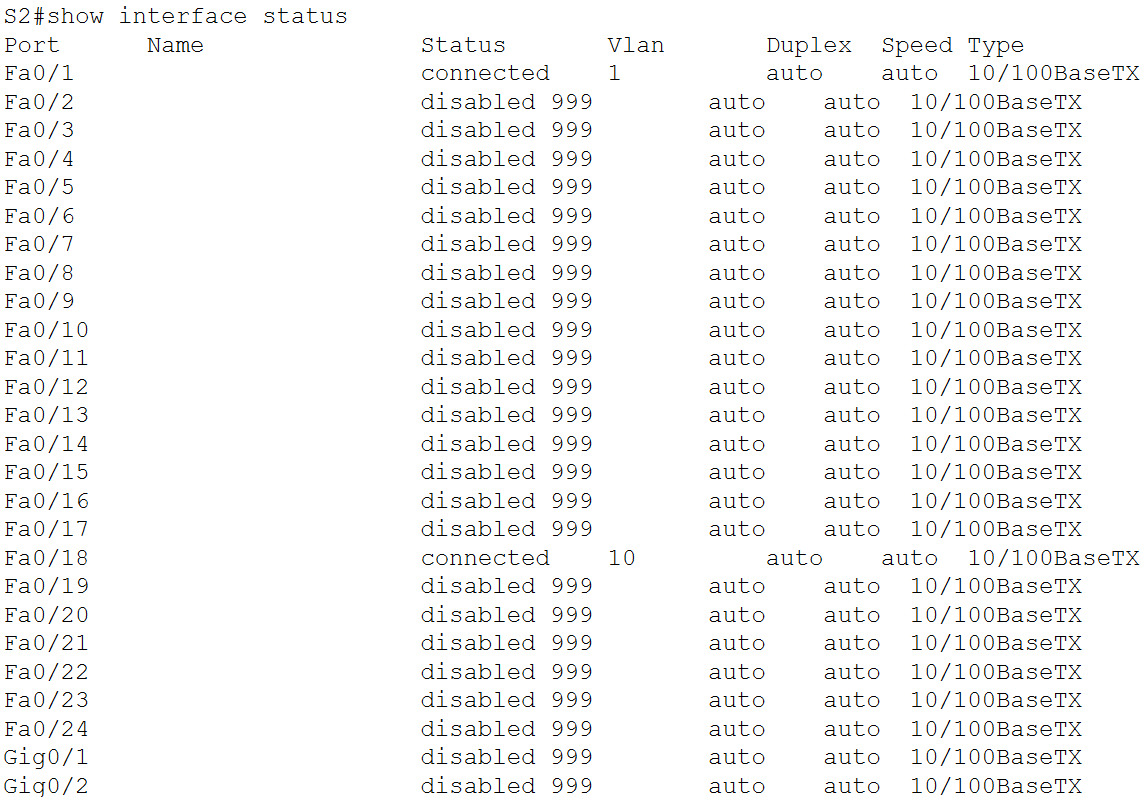
S1:

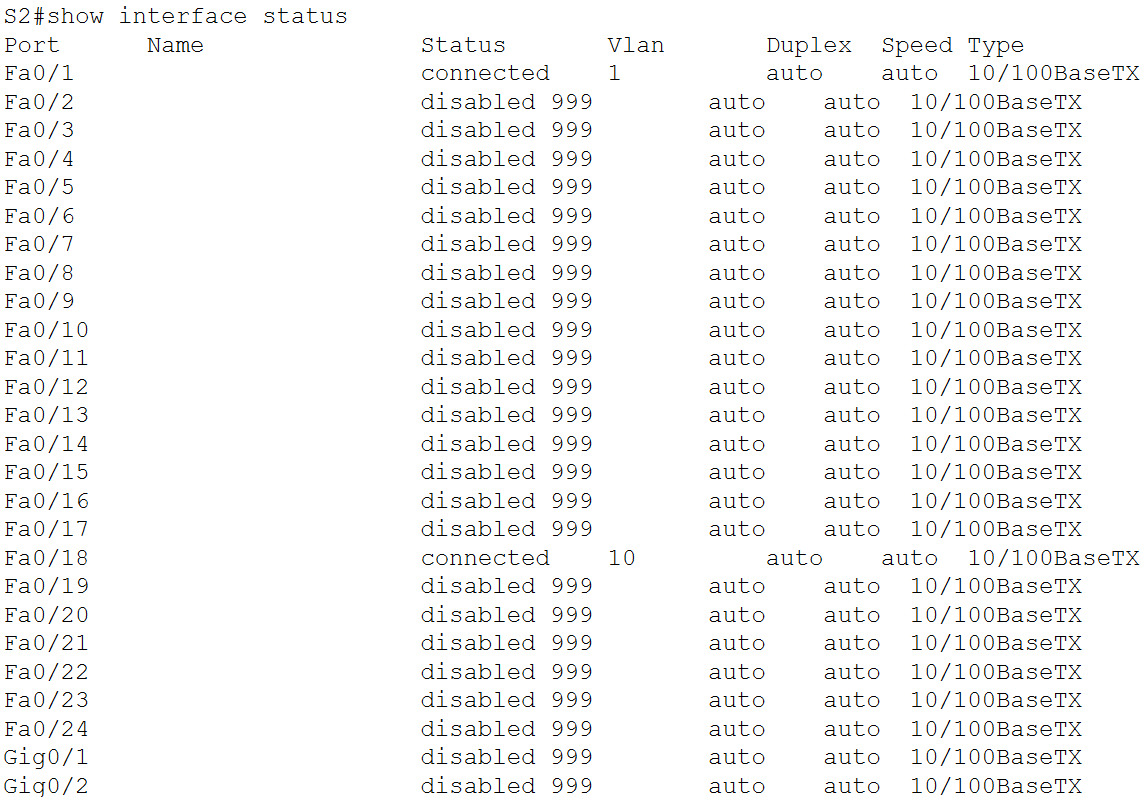




S2:

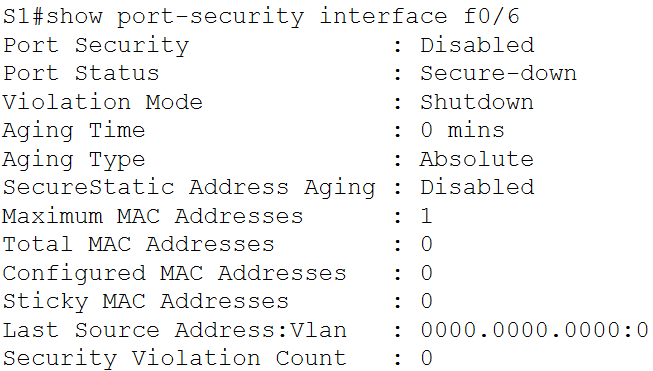


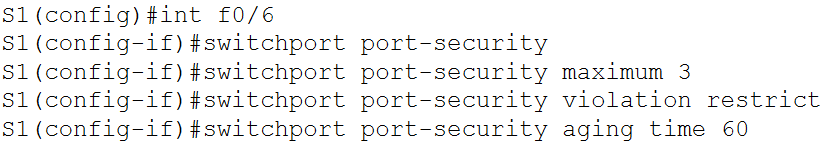




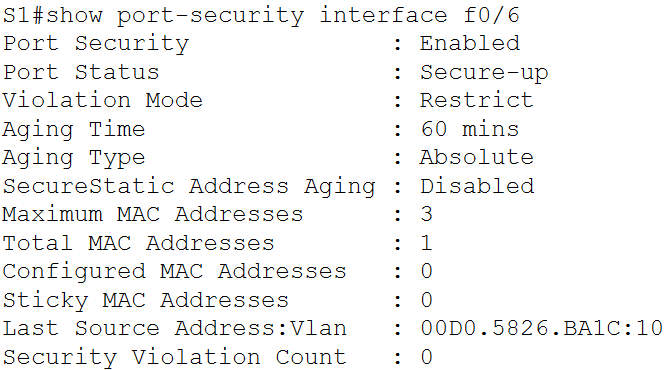
1. Documented and implemented port security features:

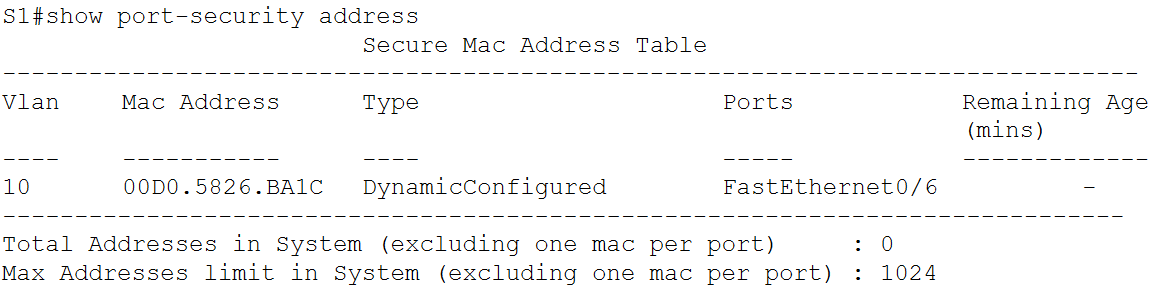
S1:



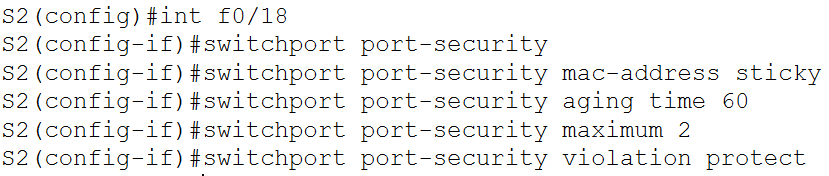


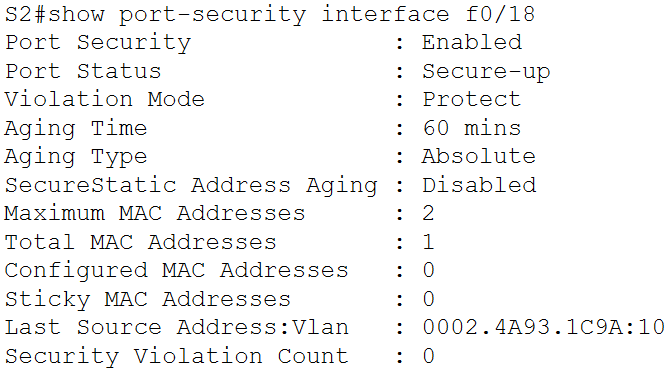
Note that the aging type could not be set. The command is not available on Cisco Packet Tracer.

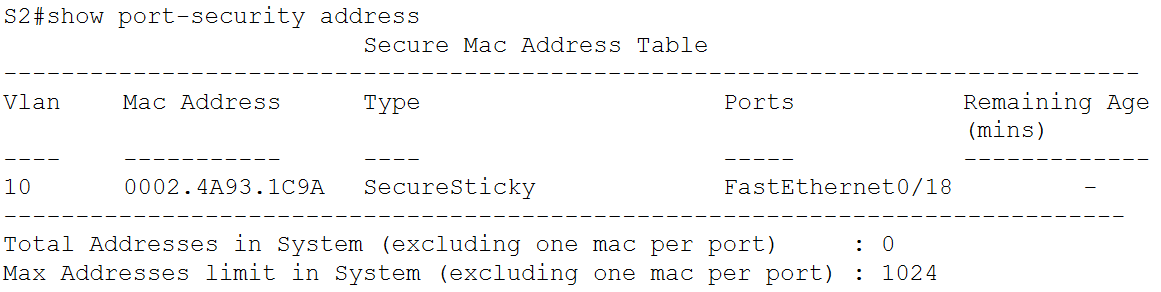




S2:

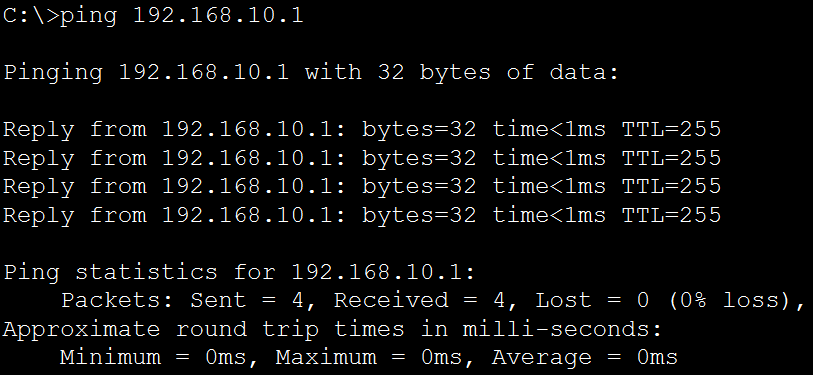




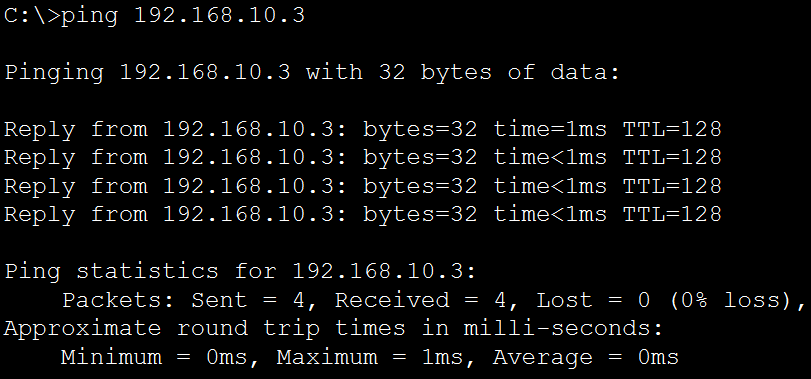


1. Pings were performed between the different devices. Note that this required setting the IP addresses of the PCs statically. Using DHCP causes an error which prevents the pings.

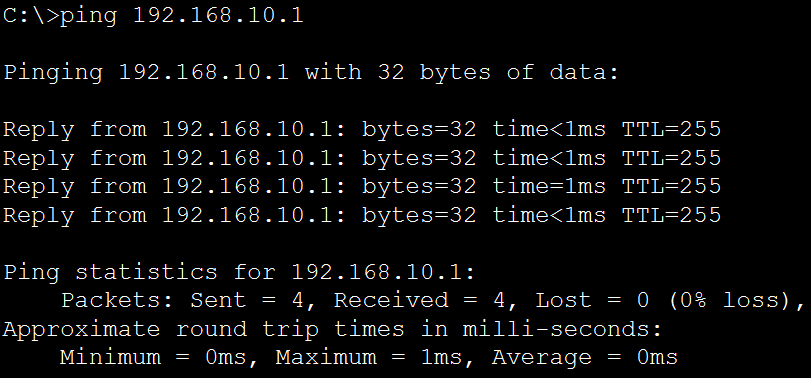
Ping from PC-A to R1:



Ping from PC-A to PC-B:



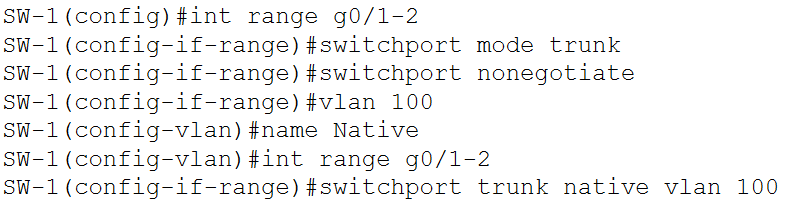
From PC-B to R1:



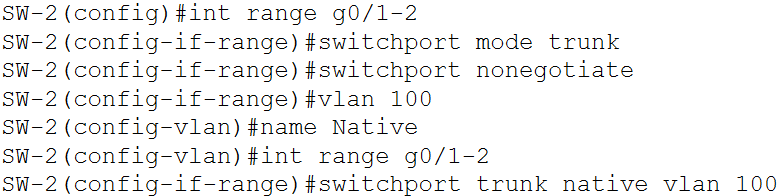
Task 2

1. Created a secure trunk:

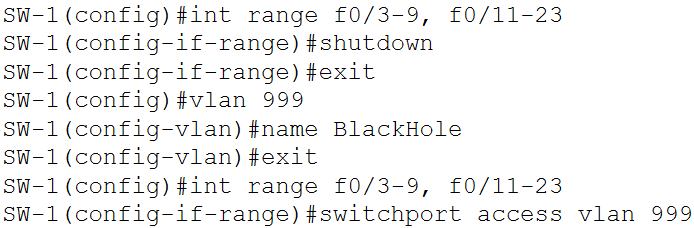
SW1:



SW2:

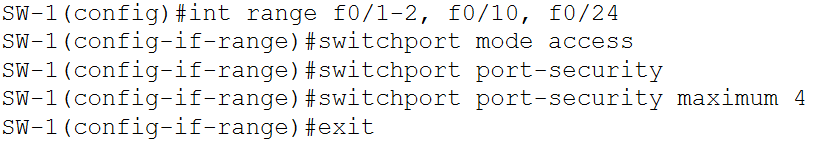


1. Secured unused switchports on SW1:

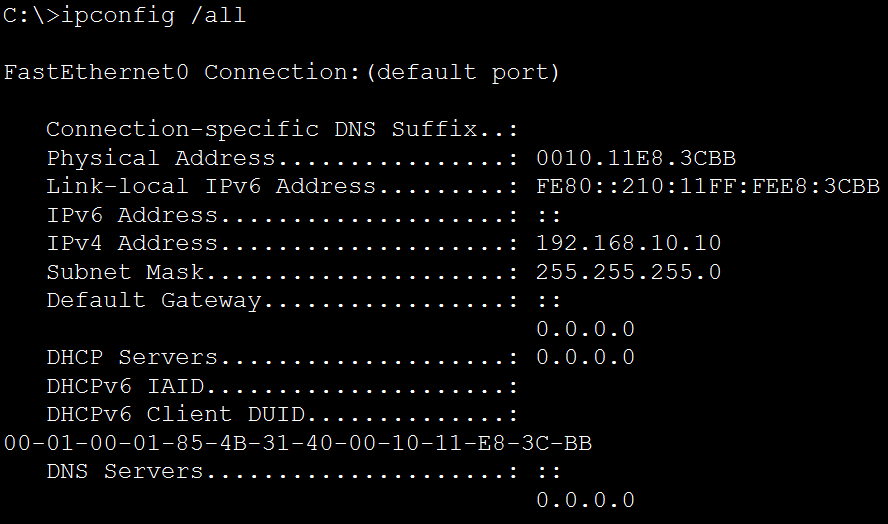


1. Implemented port security:

SW1:

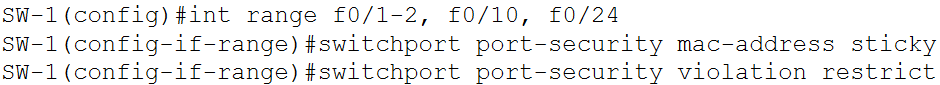


PC1:



SW1:





**Reflection Questions**:

Task # 01:

Question: In reference to Port Security on S2, why is there no timer value for the remaining age in minutes when sticky learning was configured?

Answer: There is no aging for sticky MAC addresses.

Question: In reference to Port Security, what is the difference between the absolute aging type and inactivity aging type?

Answer: Under absolute aging, the MAC address is no longer allowed after the specified amount of time. Under inactivity aging, the MAC address is no longer allowed if it does not transfer any data for the specified amount of time.

**Challenges**:

In task 1, it is not possible to ping between the devices unless the IP address of the PCs are set statically.