Title: Configure switch port security by limiting the specific MAC addresses to access particular switch port.

Objective: To create a network and simulate switch port security by restricting MAC addresses that can access the network through a switch port.

Mode Used: Cisco Packet Tracer

Theory:

Switch port security is a security feature in network switches that allow administrators to control access to a network by limiting the number of devices i.e. MAC addresses, that can connect to a specific switch port. This feature helps in mitigating security risks associated with unauthorized access to the network.

MAC Address Learning: Switch port security can dynamically learn the MAC addresses of devices connected to the port and maintain a secure MAC address table. This can be done by manually configuring static MAC addresses or dynamically using sticky MAC addresses.

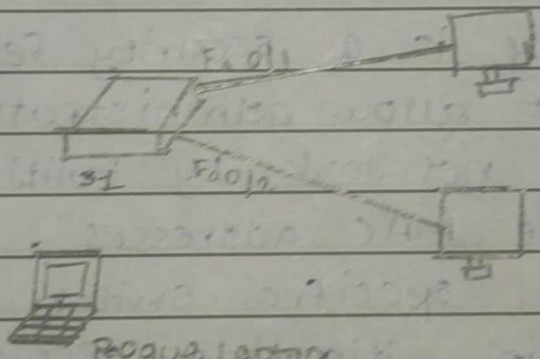
Violation Actions: When a violation of port security occurs, following actions can be taken:

Protect: Packets are dropped from unauthorized MAC addresses without notification

Restrict: Packets are dropped, and log message is genesated to notify administrators

Shutdown: Shuts down all communication on the port.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC 2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Procedure :

1) Setup the network and end devices as given in the diagram.

2) For each device, assign IP Address & subnet Mask according to the addressing Table

3) Access command line for S1 and enter
- en
- conf t
- interface range f0/1 - 2
- switchport port-security

4) Run the following to set maximum devices to one:
- switchport port-security maximum 1

5) Setup the port security to dynamically learn MAC addresses:
- switchport port-security mac-address sticky

6) Set the violation mode to restrict
- switchport portsecurity violation restrict

7) Disable all unused ports:
- interface range f0/3 - 24, g0/1 - 2
- shutdown

8) Verify PC2 can ping PC1
- ping 10.10.10.10

9) Now disconnect PC2 from interface fa0/2 and connect the rogue laptop to the same interface

10) Try to ping PC1 from Rogue laptop
- ping 10.10.10.10

11) Run port-security to check for violations
- show port-security interface fa 0/2

Observations:

1) When using dynamic configuration (stick) the switch automatically collects and stores the MAC address of PC1 and PC2.

2) Pinging PC1 from PC2 works normally; but when we connect a rogue laptop to the same port the switch automatically drops the packets.

3) When using restrict mode, the switch drops unauthorized packets and tracks the number of packets that are dropped.

Conclusion:

Port security is a critical feature in network switches that controlls access by limiting the number of devices can be connected to one port. It provides various violation actions and features like sticky MAC addresses to effectively manage network security.

Questions:

Q1) Explain the concept of switch port security and its significance in network security.

→ Switch port security is a security feature on network switches that restrict which and how many devices can connect to a specific port by identify a device based on its MAC Addreses. By only allowing authorized devices to transmit data, it prevents unauthorized access and improves network security.

Q2) Describe the different violation modes and their impliation

→ There are three violation modes:

Protect: Packets are dropped from unauthorized MAC address without notification

Restrict: Packets are dropped and log message is genesated to notify administrators

Shutdown: shuts down all communications on a port unlike other two.

Q3) Walk through the steps to configure switch port security on Cisco switch using command line interface.

→ a. Select all interfaces/ports for saurity:
- interface range f 0/1 - 5

b. Set maximum MAC addresses for a port
- switchport port-security maximum 2

c. Setup Sticky addresses
- switchport port-security mac-address sticky

d. Set violation mode
- switchport port-security violation shutdown

Q4) Discuss the role of MAC addresses in switch port security and how they are utilized to control access to switch ports.

→ MAC address are crucial in port security because unlike IP addresses, they are fixed and can be used ~~for~~ to uniquely identify a device.

The switch maintains a MAC address table that maps one or many MAC addresses to a specific port on the switch, and uses this MAC address table to filter network traffic based on violation rules.

Q5) Demonstrate a scenario where unauthorized access attempts are made to a switch port with port security enabled and explain how switch responds based on configured violation mode.

→ Consider a network consisting of a switch and two PCs, with port security enabled. The PCs are connected on ports 0/0 and 0/1 and other ports are disabled.

Another PC attempts to connect to port 0/1, using a Hub with second PC. Then, if the security mode is -

Protect : Communications between first two PCs are unaffected, while packets from third PC are dropped.

Restricted : Similias to protect, but the switch also records all violations and logs it internally.

Shutdown : The switch, on detection of violation shuts down interface 0/1, so neither second nor third PC can send packets to first PC.