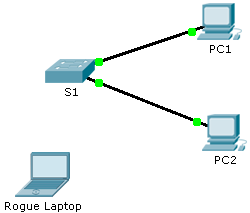
Packet Tracer - Configuring Switch Port Security

.

1. Topology



1. 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 |
| PC2 | NIC | 10.10.10.11 | 255.255.255.0 |
| Rogue Laptop | NIC | 10.10.10.12 | 255.255.255.0 |

1. Objective

Part 1: Configure Port Security

Part 2: Verify Port Security

1. Background

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port’s ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

1. Configure Port Security
   * 1. Access the command line for **S1** and enable port security on Fast Ethernet ports 0/1 and 0/2.

S1(config)# **interface range fa0/1 - 2**

S1(config-if-range)# **switchport port-security (mở trên các cổng Fast Ethernet 0/1 và 0/2)**

* + 1. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

S1(config-if-range)# **switchport port-security maximum 1 (tối đa để chỉ một thiết bị có thể truy cập các cổng Fast Ethernet 0/1 và 0/2)**

* + 1. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

S1(config-if-range)# **switchport port-security mac-address sticky**

(Bảo vệ các cổng sao cho địa chỉ MAC của một thiết bị được tự động và thêm vào cấu hình đang chạy)

* + 1. Set the violation so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.

S1(config-if-range)# **switchport port-security violation restrict**

(Đặt vi phạm sao cho các cổng Fast Ethernet 0/1 và 0/2 không bị tắt khi xảy ra vi phạm, nhưng thông báo về vi phạm bảo mật được tạo và các gói từ nguồn không xác định bị loại bỏ)

* + 1. Disable all the remaining unused ports. Hint: Use the **range** keyword to apply this configuration to all the ports simultaneously.

S1(config-if-range)# **interface range fa0/3 - 24 , gi1/1 - 2**

S1(config-if-range)# **shutdown**

(Vô hiệu hóa tất cả các cổng chưa sử dụng còn lại)

1. Verify Port Security
   * 1. From **PC1**, ping **PC2**.
     2. Verify port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration.
     3. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.
     4. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**
     5. Disconnect **PC2** and connect **Rogue Laptop** to **PC2’s** port. Verify that **Rogue Laptop** is unable to ping **PC1**.
     6. Display the port security violations for the port **Rogue Laptop** is connected to.

S1# show port-security interface fa0/2

(Hiển thị các vi phạm bảo mật cổng cho cổng Rogue Laptop khi được kết nối)

* + 1. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.
    2. Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not?