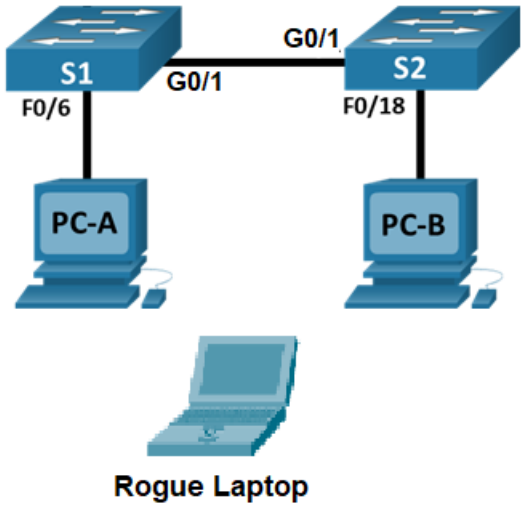
Shaun Lim
Aldrich Go
Dave Bolima
Amienz Arago

Lab 7.1 – VLAN and MAC Table Security

Topology



Addressing Table

Device	Interface / VLAN	IP Address	Subnet Mask
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	NIC	192.168.10.11	255.255.255.0
PC – B	NIC	192.168.10.12	255.255.255.0
Rogue Device (Laptop or PC)	NIC	192.168.10.200	255.255.255.0

Objectives

Part 1: Configure the Network Devices.

Part 2: Configure VLANs on Switches.

Part 3: Configure VLAN Security.

Part 3: Configure Port Security Features.

Background / Scenario

It is quite common to lock down access and install strong security features on PCs and servers. It is important that your network infrastructure devices, such as switches and routers, are also configured with security features.

In this lab, you will follow some best practices for securing a switch against VLAN hopping attacks. You will also configure and verify port security to lock out any device with a MAC address not recognized by the switch.

Required Resources

- 2 Switches
- 2 PCs, 1 laptop (or PC)
- Cabling as shown in the topology

Instructions

Part 1: Configure the Network Devices.

Step 1: Cable the network.

a. Set up the test topology in Packet Tracer as illustrated in the diagram

b. Initialize the devices.

Step 2: Configure and verify basic switch settings.

a. Configure the hostname for switches S1 and S2.

b. Prevent unwanted DNS lookups on both switches.

c. Configure interface descriptions for the ports that are in use in S1 and S2.

d. Set the default-gateway for the Management VLAN to 192.168.10.1 on both switches.

Step 3: Configure end devices.

a. Configure the PC and loptop hosts according to the IP addressing table

Part 2: Configure VLANs on Switches.

Step 1: Configure VLAN 10.

Add VLAN 10 to S1 and S2 and name the VLAN **Management.**

Step 2: Configure the SVI for VLAN 10.

Configure the IP address according to the Addressing Table for SVI for VLAN 10 on S1 and S2. Enable the SVI interfaces and provide a description for the interface.

Step 3: Configure VLAN 333 with the name Native on S1 and S2.

Step 4: Configure VLAN 999 with the name ParkingLot on S1 and S2.

Part 3: Configure Switch VLAN Security.

Step 1: Implement 802.1Q trunking.

a. On both switches, configure trunking on G0/1 and set the port to use VLAN 333 as the native VLAN.

What command/s is needed to do so?

```
Int g0/1
Switchport mode trunk
Switchport trunk native vlan 333
```

b. Verify that trunking is configured on both switches.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gig0/1       on              802.1q         trunking      333

Port        Vlans allowed on trunk
Gig0/1       1-4094

Port        Vlans allowed and active in management domain
Gig0/1       1,10,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1       1,10,333,999

S2# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gig0/1       on              802.1q         trunking      333

Port        Vlans allowed on trunk
Gig0/1       1-4094

Port        Vlans allowed and active in management domain
Gig0/1       1,10,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1       1,10,333,999
```

c. Disable DTP negotiation on G0/1 on S1 and S2.

What command is needed to do so?

Switchport nonegotiate

d. Verify with the **show interfaces** command.

```
S1# show interfaces g0/1 switchport | include Negotiation
Negotiation of Trunking: Off

S2# show interfaces g0/1 switchport | include Negotiation
Negotiation of Trunking: Off
```

Step 2: Configure access ports.

a. On S1, configure F0/6 as access ports that are associated with VLAN 10.

b. On S2, configure F0/18 as an access port that is associated with VLAN 10.

c. Verify the status of unused ports by issuing the **show** command.

```
S1# show interfaces status
```

What is the status and VLAN assignment of unused ports as indicated in the show command output?

Status: notconnect VLAN Assignment: 1

Step 3: Secure and disable unused switchports.

a. On S1 and S2, move ALL unused ports from VLAN 1 to VLAN 999 and disable the unused ports.

On which ports does this step need to be done for S1 and S2?

S1: fa0/1-5, fa0/7-24, g0/2, S2: : fa0/1-17, fa0/19-24, g0/2

b. Verify that unused ports are disabled and associated with VLAN 999 by issuing the **show** command.

```
S1# show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        disabled     999          auto   auto 10/100BaseTX
Fa0/2                        disabled     999          auto   auto 10/100BaseTX
Fa0/3                        disabled     999          auto   auto 10/100BaseTX
Fa0/4                        disabled     999          auto   auto 10/100BaseTX
Fa0/5                        disabled     999          auto   auto 10/100BaseTX
Fa0/6     Link to PC-A       connected    10         a-full  a-100 10/100BaseTX
Fa0/7                        disabled     999          auto   auto 10/100BaseTX
Fa0/8                        disabled     999          auto   auto 10/100BaseTX
Fa0/9                        disabled     999          auto   auto 10/100BaseTX
Fa0/10                       disabled     999          auto   auto 10/100BaseTX
<output omitted>
S2# show interfaces status
```

```
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        disabled     999          auto   auto 10/100BaseTX
Fa0/2                        disabled     999          auto   auto 10/100BaseTX
Fa0/3                        disabled     999          auto   auto 10/100BaseTX
<output omitted>
Fa0/14                       disabled     999          auto   auto 10/100BaseTX
Fa0/15                       disabled     999          auto   auto 10/100BaseTX
Fa0/16                       disabled     999          auto   auto 10/100BaseTX
Fa0/17                       disabled     999          auto   auto 10/100BaseTX
Fa0/18    Link to PC-B       connected    10         a-full  a-100 10/100BaseTX
Fa0/19                       disabled     999          auto   auto 10/100BaseTX
Fa0/20                       disabled     999          auto   auto 10/100BaseTX
Fa0/21                       disabled     999          auto   auto 10/100BaseTX
Fa0/22                       disabled     999          auto   auto 10/100BaseTX
Fa0/23                       disabled     999          auto   auto 10/100BaseTX
Fa0/24                       disabled     999          auto   auto 10/100BaseTX
Gi0/1     Link to S1         connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi0/2                        disabled     999          auto   auto 10/100/1000BaseTX
```

Part 4: Configure Port Security Features

Step 1: Verify port security features.

The interfaces F0/6 on S1 and F0/18 on S2 are configured as access ports.

On S1, issue the **show port-security interface f0/6** command to display the default port security settings for interface F0/6. Record your answers in the table below.

Default Port Security Configuration	
Feature	**Default Setting**
Port Security	**Disabled**
Maximum number of MAC addresses	**1**
Violation Mode	**Shutdown**
Aging Time	**0 mins**
Aging Type	**Absolute**
Secure Static Address Aging	**Disabled**
Sticky MAC Address	**0**

Step 2: Configure and verify port security with static secure address.

a. Note the MAC addresses of PC-A as recorded by S1 by issuing a **show mac address-table** command from privileged EXEC mode. Find the dynamic entries for ports F0/6 and record them below. If there is no entry yet, you may issue a ping between PC-A and PC-B in order to allow S1 to learn the address.

PC-A MAC Address	**0000.0c2e.3cb9**

b. Access the command line for S1 and enable port security on Fa0/6.

```
S1(config)# interface f0/6
S1(config-if)# switchport port-security
```

c. Set the maximum so that only one device can access the port.

```
S1(config-if)# switchport port-security maximum 1
```

d. Secure the ports so that only the MAC address of PC-A is allowed on the port. Use the address recorded in Step 2a in place of xxxx.xxxx.xxxx in the command sample below.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

e. Set the violation mode so that the Fa0/6 is disabled when a violation occurs and a notification of the security violation is generated

```
S1(config-if)# switchport port-security violation shutdown
```

f. Verify port security on S1 F0/6 by issuing a **show port-security interface** command.

```
S1# show port-security interface f0/6
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

What is the port status of F0/6?	**Secure-up**

g. Generate some traffic by using PC-A to ping S1 and verify that PC-A is allowed to communicate while connected to Fa0/6.

h. You will now violate security by attaching a different host to the switchport. Disconnect PC-A from S1 Fa0/6 and connect the Rogue Device in its place.

From the Rogue Device, ping S1. You will eventually see messages displayed on the CLI of S1 indicating a security violation.

Was the ping successful? Why or why not?

No, because the instructions earlier made it so only the mac-address of PCA is allowed on the port, any other pings from a device other than PCA would shutdown the port.

i. On the switch, verify port security with the following commands.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
      Fa0/6            1           1                1         Shutdown
```

```
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-shutdown
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   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:10
Security Violation Count   : 1

S1# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                  Ports      Remaining Age
                                                             (mins)
----     -----------       ----                  -----    -------------
  10     30f7.0da3.1821    SecureConfigured      Fa0/6        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

j. Disconnect the Rogue Device from S1 and reconnect PC-A.

k. From PC-A, ping S1 again

Was the ping successful?	**No**

l. On the switch, issue the **show interface f0/6** command to determine the cause of ping failure. Record your findings.

FastEthernet0/6 is down, line protocol is down (err-disabled)

Hardware is Lance, address is 0090.0cb6.cb06 (bia 0090.0cb6.cb06)

Description: Connection to PCA

BW 100000 Kbit, DLY 1000 usec,

```
   reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

Full-duplex, 100Mb/s

input flow-control is off, output flow-control is off

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:00:08, output 00:00:05, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

   956 packets input, 193351 bytes, 0 no buffer

   Received 956 broadcasts, 0 runts, 0 giants, 0 throttles

   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

   0 watchdog, 0 multicast, 0 pause input

   0 input packets with dribble condition detected
```

2357 packets output, 263570 bytes, 0 underruns

0 output errors, 0 collisions, 10 interface resets

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out

m. Clear the S1 F0/6 error disabled status.

```
S1# config t
S1(config)# interface f0/6
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Note: There may be a delay while the port states converge.

n. Issue the **show interface f0/6** command on S1 to verify F0/6 is no longer in error disabled mode.

```
S1# show interface f0/6
FastEthernet0/6 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

o. From the PC-A ping S1 again. The ping should be successful.

Step 3: Configure and verify port security with sticky learning.

a. Access the command line for S2, enable port security on Fa0/18 and set the maximum addresses to 1.

What are the commands to do so?

switchport port-security

switchport port-security maximum 1

b. Secure the port so that the MAC address of a device is dynamically learned and added to the running configuration.

```
S2(config-if)# switchport port-security mac-address sticky
```

c. Set the violation mode so that the Fa0/6 are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.

```
S2(config-if)# switchport port-security violation restrict
```

d. Generate some traffic by using PC-B to ping S2 then verify that the address of PC-B was learned.

```
S2# show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
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       : 1
Last Source Address:Vlan   : 0022.5646.3411:10
Security Violation Count   : 0

S2# show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
  10    0022.5646.3411    SecureSticky                  Fa0/18        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

e. Verify that the Sticky Secure MAC address was also recorded in the running configuration of S2.

```
S2# show running-config
```

Is the address of PC-B recorded under the configurations of Fa0/18?	**Yes**

f. Disconnect PC-B and connect the Rogue Device to S2 F0/18, which is the port to which PC-B was originally connected. Using the Laptop's command line, ping S2.

What is the result of the ping?

It failed.

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.202:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

g. Display the port security violations for the port to which the Rogue Device is connected.

```
S2# show port-security interface f0/18
```

How many violations have occurred?	4

h. Disconnect the Rogue Device and reconnect PC-B. Verify PC-B can ping S2.

Why is PC-B able to ping S2 when it was reconnected, but the Rogue Device is not?

Its because the sticky mac address in port security was set to PCB's mac-address since it is PCB's mac address that was learned first, meaning if PCB is connected to S2, it will be able to ping it. However, if another device tries to ping S2, it will not work because the port security is already set to PC-B's mac address.

Reflection Questions

1. Why is it important that unused ports be reassigned to an unused VLAN and disabled especially on access layer switches? Discuss your answer by describing what type of attack/s can be performed and their consequences on the network if these practices are not implemented.

Reassigning unused ports to an unused VLAN and disabling them on access layer switches is crucial for preventing unauthorized access, network disruptions, and security breaches. Failing to implement these practices can lead to attacks like MAC spoofing, leading to unauthorized access, broadcast storms, network instability, and non-compliance with security standards.

2. Should port security be enabled on ports connected by trunk links? Why or why not?

Port security should not be enabled on ports connected by trunk links, since trunks are used to carry traffic between switches and connect different VLANS. Port security is more of a feature used to control and restrict access to individual switch ports based on the MAC address of connected devices, which is better for enhancing security on access ports.

3. What is the difference between static secure and sticky secure addresses; and if you were to design a network, why would you choose 1 method over the other?

Static secure addresses involve manually configuring a list of allowed MAC addresses for a switch port, while sticky secure addresses automatically record and allow devices with the same MAC address on a port after an initial connection. If I were to design a network, I would choose sticky over static if I have to configure plenty of devices, where it would be tiring to manually configure port security with plenty of mac addresses and if the network has high device mobility (plenty and frequent connections). However, if the network is closely monitored and connections are few and infrequent, I would go with static.

4. What is the difference between the reaction of a switch to a port security violation when using shutdown mode compared to restrict mode; and if you were to design a network, why would you choose 1 mode over the other?

In shutdown, the port is shutdown if there would be a security violation. In restrict, the port will not be shut down when there is a security violation, but there will be logs showing that a violation happened. I would choose one over the other depending on the network. If the network requires high security and is not particularly strict about downtime, I would go with shutdown mode since it provides a stronger security response by shutting down the port, meaning it is obvious that an attack happens, with the only downside

being shutting down the port can be disruptive and might lead to network downtime if not closely monitored. On the other hand, I would choose restrict mode if the network requires continuous operation and is strict about downtime. The only downside is, if an attack happens, its far more difficult to know if it happened unless one checks the logs.