Lab 8 - Switch Security Configuration

**Name/ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Topology

Diagram

Description automatically generated

# VLAN Table

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN | Name | IPv4 Subnet Address | Interface Assigned |
| 10 | Management | 192.168.10.0 /24 | S1: VLAN 10 interface  S2: VLAN 10 interface  S1: F0/6  S2: F0/18 |
| 333 | Native | N/A | N/A |
| 999 | ParkingLot | N/A | S1: F0/2-4, F0/7-24, G0/1-2  S2: F0/2-17, F0/19-24, G0/1-2 |

# Objectives

Part 1: Configure the Network Devices.

* Cable the network.
* Configure R1.
* Configure and verify basic switch settings.

Part 2: Configure VLANs on Switches.

* Configure VLAN 10.
* Configure the SVI for VLAN 10.
* Configure VLAN 333 with the name Native on S1 and S2.
* Configure VLAN 999 with the name ParkingLot on S1 and S2.

Part 3: Configure Switch Security.

* Implement 802.1Q trunking.
* Configure access ports.
* Secure and disable unused switchports.
* Document and implement port security features.
* Verify end-to-end-connectivity.

Lab Report General Instructions

1. Lab report should include your names and IDs.
2. Lab report should include answers to all questions highlighted in grey.
3. Lab report should include all required screenshots.
4. Screenshots should include your names at the command prompt.
5. Lab report should include answers to all reflection questions. This part is individual work even if the lab is group work. Pls use your own words to answer the questions. Copy answers will receive zero.
6. Reflection questions should be answered clearly with enough elaboration.

# Background / Scenario

This is a comprehensive lab to review previously covered Layer 2 security features.

**Note**: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.3 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

**Note**: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

# Required Resources

* 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.3 universal image or comparable)
* 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
* 2 PCs (Windows with a terminal emulation program, such as Tera Term)
* Console cables to configure the Cisco IOS devices via the console ports
* Ethernet cables as shown in the topology

# Instructions

## Configure the Network Devices.

### Cable the network.

Cable the network as shown in the topology.

### Configure an IP address on PC-A and PC-B

1. Select **DHCP** option from the PC IP Configuration settings. Both PCs will obtain the IP address configuration dynamically.

### Configure R1.

* + - 1. **Copy and paste** the following configuration script on R1.

enable

configure terminal

hostname R1

no ip domain lookup

ip dhcp excluded-address 192.168.10.1 192.168.10.9

ip dhcp excluded-address 192.168.10.201 192.168.10.202

ip dhcp relay information trust-all

ip dhcp pool Students

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

domain-name CCNA2.Lab-11.6.1

exit

interface Loopback0

ip address 10.10.1.1 255.255.255.0

exit

interface GigabitEthernet0/0/1

description Link to S1 Port 5

ip address 192.168.10.1 255.255.255.0

no shutdown

exit

line con 0

logging synchronous

exec-timeout 0 0

end

* + - 1. Verify the running-configuration on R1 using the following command:

R1# **show ip interface brief**

1. Verify IP addressing and interfaces are in an up / up state (troubleshoot as necessary).

Close configuration window

### Configure and verify basic switch settings.

* + - 1. Configure the hostname for switches S1 and S2.

Open configuration window

Open configuration window

* + - 1. Prevent unwanted DNS lookups on both switches.
      2. Set the default-gateway for the Management VLAN to 192.168.10.1 on both switches.

## Configure VLANs on Switches.

### Configure VLAN 10 on S1 and S2.

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

### Configure VLAN 333 with the name Native on S1 and S2.

### Configure VLAN 999 with the name ParkingLot on S1 and S2.

### Configure the SVI for VLAN 10 on S1 and S2.

* + - 1. Configure the IP address according to the topology for SVI for VLAN 10 on S1 and S2.
      2. Provide a description for the interface.
      3. Enable the SVI interfaces.

## Configure Switch Security.

### Implement 802.1Q trunking.

* + - 1. On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.
      2. Use the command **show interface trunk** to verify that trunking is configured on both switches.

S1# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 333

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,333,999

S2# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 333

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,333,999

**Screenshot the command output on both switches S1 and S2 and paste them here. Add your name and ID at the command prompt.**

* + - 1. Disable DTP negotiation on F0/1 on S1 and S2.

S1(config)# **interface f0/1**

S1(config-if)# **switchport nonegotiate**

S2(config)# **interface f0/1**

S2(config-if)# **switchport nonegotiate**

* + - 1. Verify with the **show interfaces** command.

S1# **show interfaces f0/1 switchport | include Negotiation**

Negotiation of Trunking: Off

S2# **show interfaces f0/1 switchport | include Negotiation**

Negotiation of Trunking: Off

**Screenshot the command output on both switches S1 and S2 and paste them here. Add your name and ID at the command prompt.**

### Configure access ports.

* + - 1. On S1, configure F0/5 and F0/6 as access ports that are associated with VLAN 10.
      2. On S2, configure F0/18 as an access port that is associated with VLAN 10.
      3. Issue the **show vlan brief** command and verify that VLAN 10 is assigned to the correct interfaces on both switches.

**Screenshot the command output on both switches S1 and S2 and paste them here. Add your name and ID at the command prompt.**

### Secure and disable unused switchports.

* + - 1. On S1 and S2, assign the unused ports as access ports, move them from VLAN 1 to VLAN 999 and disable them. User the **interface range** command to identify the unused ports.
      2. 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 Link to S2 connected trunk a-full a-100 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 Link to R1 connected 10 a-full a-100 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

S2# **show interfaces status**

Port Name Status Vlan Duplex Speed Type

Fa0/1 Link to S1 connected trunk a-full a-100 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 disabled 999 auto auto 10/100/1000BaseTX

Gi0/2 disabled 999 auto auto 10/100/1000BaseTX

**Screenshot the command output on both switches S1 and S2 and paste them here. Add your name and ID at the command prompt.**

### Document and implement port security features.

In this step, you **will configure port security based on MAC addresses.** Switches can be subject to MAC address table overflow attacks, MAC spoofing attacks, and unauthorized connections to switch ports. You will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

The interfaces F0/6 on S1 and F0/18 on S2 are configured as access ports. In this step, you will also configure port security on these two access ports.

* + - 1. 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** |  |
| **Maximum number of MAC addresses** |  |
| **Violation Mode** |  |
| **Aging Time** |  |
| **Aging Type** |  |
| **Secure Static Address Aging** |  |
| **Sticky MAC Address** |  |

* + - 1. On S1, enable port security on F0/6 with the following settings:
* Enable port security

S1 (config) # **interface f0/6**

S1 (config-if) # **switchport port-security**

* Set the maximum number of MAC addresses to **3**

S1 (config-if) # **switchport port-security maximum 3**

* Set the violation type to **restrict**

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

* Set the aging time to **60 min**

S1 (config-if) # **switchport port-security aging time 60**

* Set the aging type to **inactivity**

S1 (config-if) # **switchport port-security aging type inactivity**

(this command not supported on Packet Tracer)

* + - 1. From PC-A ping S1.
      2. Verify port security on S1 F0/6.

S1# **show port-security interface f0/6**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Restrict

Aging Time : 60 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 3

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0022.5646.3411:10

Security Violation Count : 0

**Screenshot your result and paste it here. Add your name and ID at the command prompt.**

S1# **show port-security address**

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

10 0022.5646.3411 SecureDynamic Fa0/6 60 (I)

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

* + - 1. Enable port security for F0/18 on S2. Configure the port to add MAC addresses learned on the port automatically to the running configuration.

S2(config)# **interface f0/18**

S2(config-if)# **switchport port-security**

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

* + - 1. Configure the following port security settings on S2 F/18:
* Maximum number of MAC addresses: **2**

S2(config-if)# **switchport port-security maximum 2**

* Violation type: **Protect**

S2(config-if)# **switchport port-security violation protect**

* Aging time: **60 min**

S2(config-if)# **switchport port-security aging time 60**

* + - 1. **From PC-B ping S2.**
      2. Verify port security on S2 F0/18.

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

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Protect

Aging Time : 60 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 0022.5646.3413:10

Security Violation Count : 0

**Screenshot your result and paste it here. Add your name and ID at the command prompt.**

S2# **show port-security address**

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

10 0022.5646.3413 SecureSticky Fa0/18 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

### Verify end-to-end connectivity.

Verify PING connectivity between all devices. If the pings fail, you may need to disable the firewall on the PC hosts.

**Screenshot the following ping results and paste them here. Add your name and ID at the command prompt.**

**Ping from PC-A to PC-B**

**Ping from PC-A to Lo0**

**Ping from PC-A to S2**

# Reflection Questions

* 1. **What is a recommended best practice when dealing with the native VLAN? Explain.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. **Why would you enable port security on a switch?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. **Why should unused ports on a switch be disabled?**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_