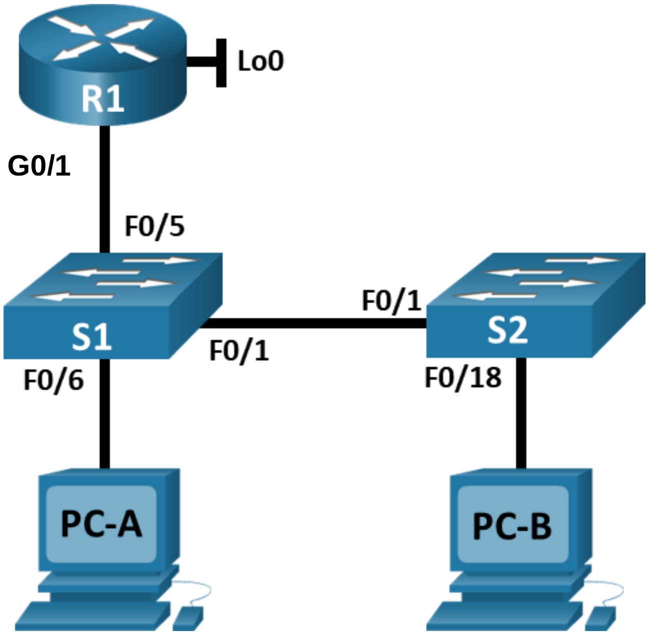
Hardware Lab 4 - Switch Security Configuration

Topology



Addressing Table

Device	Interface / VLAN	IP Address	Subnet Mask
R1	G0/1	192.168.10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
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	DHCP	255.255.255.0
PC – B	NIC	DHCP	255.255.255.0

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.
- Implement DHCP snooping security.
- Implement PortFast and BPDU guard.
- Verify end-to-end-connectivity.

Background / Scenario

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

Instructions

Part 1: Configure the Network Devices.

Step 1: Cable the network.

a. Cable the network as shown in the topology.

b. Initialize the devices.

Step 2: Configure R1.

a. Load the following configuration script on R1.

Step 3:

```
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 pool Students
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 domain-name CCNA2.Lab-11.6.1
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.0
```

```
!
interface GigabitEthernet0/1
 description Link to S1 Port 5
 ip dhcp relay information trusted
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 exec-timeout 0 0
```

a. Verify the running-configuration on R1 using the following command:

```
R1# show ip interface brief
```

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

Step 4: Configure and verify basic switch settings.

a. **Configure** the hostname for switches S1 and S2.

b. **Configure** the default-gateway for the Management VLAN to 192.168.10.1 on both switches.

Part 2: Configure VLANs on Switches (Hardware VLAN lab can help with this).

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 using no shutdown.

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 Security (Lecture 5 slide 17 can help with this section).

Step 1: Implement 802.1Q trunking.

a. On both switches, **configure trunking** on F0/1 to use VLAN 333 as the native VLAN.

b. 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
```

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

d. 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
```

Step 2: Configure access ports.

a. On S1, **configure** F0/5 and 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.

Step 3: Secure and disable unused switchports.

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

- Note: On S1 ports int fa0/2-4, fa0/7-24 and G0/1-2 and S2 ports are fa0/2-17, fa0/19-24 and G0/1-2.

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     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
<output omitted>
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
<output omitted>
```

c. **Change** your workstations adapter settings (IPv4 properties) to automatic and verify if they have received an IP address dynamically from **R1**, who is the **DHCP server**.

d. **Verify** the settings in the command prompt using **ipconfig**.

```
C:\Users\student> ipconfig
```

e. **Ping** from PC-A to PC-B, were the pings successful?

f. **Ping** from S1 to S2 from the `S1#` prompt – were the pings successful?

g. Troubleshoot if pings are not working and disable software firewalls.

Before moving on to **Step 4: Port Security**, please test for connectivity and **answer Q1 – Q5 on Moodle**.

Step 4: Document and implement port security features (Lecture 4 – Slide 30 Can help with this section)

The interface **F0/6** on S1 is configured as an **access** port. In this step, you will also configure port security on this access port on S1.

a. 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	

b. On S1, **enable** port security on F0/6 with the following settings:

- Configure port-security first and then:
- Increase the maximum number of MAC addresses to: **3**
- Violation type: **restrict**
- Aging time: **60 min**
- Aging type: **inactivity**

c. 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
```

```
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
```

Before moving on to **Step 5: DHCP Snooping**, please **answer Q6 on Moodle.**

Step 5: Implement DHCP snooping security (Lecture 5 - Slide

a. On **S2**, enable DHCP snooping and configure DHCP snooping on VLAN 10.

b. Configure the trunk port on S2 as a trusted port.

c. Limit the untrusted port, F18 on S2, to five DHCP packets per second.

d. Verify DHCP Snooping on S2.

```
S2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/18           no         no              5
  Custom circuit-ids:
```

e. From the command prompt on PC-B, release and then renew the IP address.

```
C:\Users\Student> ipconfig /release
C:\Users\Student> ipconfig /renew
```

f. Verify the DHCP snooping binding using the **show ip dhcp snooping binding** command.

```
S2# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
```

```
------------------  ---------------  ----------  -------------  ----  ----------------
----
00:50:56:90:D0:8E   192.168.10.11    86213       dhcp-snooping   10   FastEthernet0/18
Total number of bindings: 1
```

Before moving on to **Step 6: Port Fast**, please test for connectivity and **answer Q7 on Moodle.**

Step 6: Implement PortFast and BPDU guard.

a. Configure PortFast on all the access ports that are in use on both switches.

b. Enable BPDU guard on S1 and S2 VLAN 10 access ports connected to PC-A and PC-B.

c. Verify that BPDU guard and PortFast are enabled on the appropriate ports.

```
S1# show spanning-tree interface f0/6 detail
 Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   <output omitted for brevity>
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 128, received 0
```

Before moving on to **Step 7: Testing for Connectivity**, please test for connectivity and **answer Q8 on Moodle.**

Step 7: Verify end-to-end connectivity.

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

2. Each student must show their configuration of either S1 port-security or S2 DHCP Snooping to their lecturer.

3. Students should have the relevant show commands ready for grading.

Before leaving the lab space, please test for connectivity and **provide your unique code to Moodle for this section of the lab.**