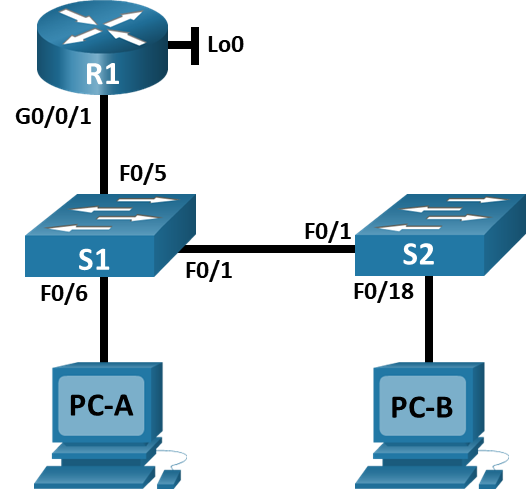
Lab - Configuración de Seguridad en el Switch

# Topología



# Tabla de Asignación de Direcciones

| Dispositivos | Interface / VLAN | Dirección IP | Máscara de Subred |
| --- | --- | --- | --- |
| R1 | G0/0/1 | 192.168.10.1 | 255.255.255.0 |
| R1 | Bucle invertido 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 |

# Objetivos

Parte 1: Configurar los dispositivos de red.

* Conectar la red
* Configurar R1
* Configurar y verificar los parámetros básicos del switch

Parte 2: Configurar las VLAN en los Switches.

* Configurar la VLAN 10.
* Configurar el SVI para VLAN 10.
* Configurar la VLAN 333 con el nombre Native en S1 y S2.
* Configurar la VLAN 999 con el nombre ParkingLot en S1 y S2.

Parte 3: Configurar la seguridad del Switch.

* Implemente el enlace troncal 802.1Q.
* Configure los puertos de acceso.
* Asegure y deshabilite los puertos del switch no utilizados.
* Documentar e implementar funciones de seguridad de los puertos.
* Implemente la seguridad de DHCP snooping.
* Implemente PortFast y la protección BPDU.
* Verifique la conectividad de extremo a extremo.

# Aspectos básicos/Situación

Este es un laboratorio completo para revisar las características de seguridad de Capa 2 cubiertas anteriormente.

**Nota**: Los routers que se utilizan en los laboratorios prácticos de CCNA son Cisco 4221 con Cisco IOS XE versión 16.9.3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota**: Asegúrese de que los interruptores se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

# Recursos Necesarios

* 1 Router (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.3 o comparable)
* 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
* 2 PC (Windows con un programa de emulación de terminal, como Tera Term)
* Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
* Cables Ethernet, como se muestra en la topología

# Instrucciones

## Configurar los dispositivos de red.

### Conecte la red.

1. Realice el cableado de red tal como se muestra en la topología.
2. Inicializar los dispositivos.

### Configurar R1

* + - 1. Cargue el siguiente script de configuración en R1.

Abrir la ventana de configuración

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 GigabitEthernet0/0/1

description Link to S1 Port 5

ip dhcp relay information trusted

ip address 192.168.10.1 255.255.255.0

no shutdown

!

línea con 0

logging synchronous

exec-timeout 0 0

* + - 1. Verifique la configuración en ejecución en R1 con el siguiente comando:

R1# **show ip interface brief**

1. Verifique que el direccionamiento IP y las interfaces estén en un estado activo / activo (solucione los problemas según sea necesario).

Cerrar la ventana de configuración

### Configure y verifique los parámetros básicos del switch.

* + - 1. Configure el nombre de host para los switches S1 y S2.

Abrir la ventana de configuración

* + - 1. Evite búsquedas DNS no deseadas en ambos switches.
      2. Configure las descripciones de interfaz para los puertos que están en uso en S1 y S2.
      3. Establezca la puerta de enlace predeterminada para la VLAN de administración en 192.168.10.1 en ambos switches.

## Configure las VLAN en los Switches.

### Configure la VLAN 10.

Agregue la VLAN 10 a S1 y S2 y asigne un nombre a la VLAN de administración **Management.**

### Configure el SVI para VLAN 10.

Configure la dirección IP de acuerdo con la Tabla de Direccionamiento para SVI para VLAN 10 en S1 y S2. Habilite las interfaces SVI y proporcione una descripción para la interfaz.

### Configure la VLAN 333 con el nombre Native en S1 y S2.

### Configure la VLAN 999 con el nombre ParkingLot en S1 y S2.

### Implemente el enlace 802.1Q.

* + - 1. En ambos switches, configure el enlace troncal en F0/1 para usar la VLAN 333 como la VLAN nativa.
      2. Verifique que el enlace troncal esté configurado en ambos switches.

S1# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 en 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 en 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

* + - 1. Deshabilite la negociación DTP en F0/1 en S1 y S2.
      2. Verifique con el comando **show interfaces** .

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

Negotiation of Trunking: Off

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

Negotiation of Trunking: Off

### Configure los puertos de acceso.

* + - 1. En S1, configure F0/5 y F0/6 como puertos de acceso asociados con la VLAN 10.
      2. En S2, configure F0/18 como un puerto de acceso asociado con la VLAN 10.

### Asegure y deshabilite los puertos de conmutación no utilizados.

* + - 1. En S1 y S2, mueva los puertos no utilizados de la VLAN 1 a la VLAN 999 y desactive los puertos no utilizados.
      2. Verifique que los puertos no utilizados estén deshabilitados y asociados con la VLAN 999 emitiendo el comando **show interfaces status** .

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

<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

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

### Documentar e implementar funciones de seguridad portuaria.

Las interfaces F0/6 en S1 y F0/18 en S2 están configuradas como puertos de acceso. En este paso, también configurará la seguridad del puerto en estos dos puertos de acceso.

* + - 1. En S1, haga el comando**show port-security interface f0/6** para mostrar la configuración de seguridad de puerto predeterminada para la interfaz F0/6. Registre sus respuestas en la tabla a continuación.

| Configuración de seguridad de puerto predeterminada | |
| --- | --- |
| Característica | Configuración Predeterminada |
| Seguridad de puertos |  |
| Número máximo de direcciones MAC |  |
| Modo de Violación |  |
| Tiempo de Vencimiento |  |
| Tipo de Vencimiento |  |
| Vencimiento seguro de la dirección estática |  |
| Dirección MAC Sticky |  |

* + - 1. En S1, habilite la seguridad del puerto en F0/6 con la siguiente configuración:
* Número máximo de direcciones MAC: **3**
* Tipo de violación: **restrict**
* Tiempo de vencimiento: **60 min**
* Tipo de vencimiento: **inactivity**
  + - 1. Verifique la seguridad del puerto en 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

* + - 1. Habilite la seguridad del puerto para F0/18 en S2. Configure el puerto para agregar direcciones MAC aprendidas en el puerto automáticamente a la configuración en ejecución.
      2. Configure las siguientes configuraciones de seguridad de puerto en S2 F 0/18:
* Número máximo de direcciones MAC: **2**
* Violation type: **Protect**
* Tiempo de vencimiento: **60 min**
  + - 1. Verifique la seguridad del puerto en 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 : 0

Last Source Address:Vlan : 0022.5646.3413:10

Security Violation Count : 0

S2# **show port-security address**

Secure Mac Address Table

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

Vlan Mac Address Type Ports Remaining Age

(mins)

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

10 0022.5646.3413 SecureSticky Fa0/18 -

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

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

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

### Implemente la seguridad de DHCP snooping.

* + - 1. En S2, habilite la inspección DHCP y configure la inspección DHCP en la VLAN 10.
      2. Configure el puerto troncal en S2 como un puerto confiable.
      3. Limite el puerto no confiable, F18 en S2, a cinco paquetes DHCP por segundo.
      4. Verifique la inspección DHCP en S2.

S2# **show ip dhcp snooping**

Switch DHCP snooping is enabled

DHCP snooping está configurado en las siguientes VLANs;

10

DHCP snooping es operacional en las siguientes VLANs;

10

DHCP snooping está configurado en las siguientes interfaces L3

Inserción de opción 82 habilitada

circuit-id default format: vlan-mod-port

remote-id: 0cd9.96d2.3f80 (MAC)

La Opción 82 en puertos no confiables no es permitida.

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping está configurado en las siguientes interfaces L3

Interface Trusted Allow option Rate limit (pps)

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

FastEthernet0/1 yes yes unlimited

Custom circuit-ids:

FastEthernet0/18 no no 5

Custom circuit-ids:

* + - 1. Desde el símbolo del sistema en la PC-B, suelte y luego renueve la dirección IP.

C:\Users\Student> **ipconfig /release**

C:\Users\Student> **ipconfig /renew**

* + - 1. Verifique el enlace de iDHCP snooping utilizando el comando **show ip dhcp snooping binding**.

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

### Implemente PortFast y la protección BPDU.

* + - 1. Configure PortFast en todos los puertos de acceso que están en uso en ambos switches.
      2. Habilite la protección BPDU en los puertos de acceso VLAN 10 S1 y S2 conectados a la PC-A y PC-B.
      3. Verifique que la protección BPDU y PortFast estén habilitados en los puertos apropiados.

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

### Verifique la conectividad de extremo a extremo.

Verifique la conectividad PING entre todos los dispositivos en la Tabla de Direccionamiento IP. Si los ping fallan, es posible que deba deshabilitar el firewall en los hosts de la PC.

Cerrar la ventana de configuración

# Preguntas de Reflexión

* 1. En referencia a Port Security en S2, ¿por qué no hay un valor de temporizador para la edad restante en minutos cuando se configuró el aprendizaje permanente?
  2. En referencia a Port Security en S2, si carga el script de configuración en ejecución en S2, ¿por qué la PC-B en el puerto 18 nunca obtendrá una dirección IP a través de DHCP?
  3. En referencia a Port Security, ¿cuál es la diferencia entre el tipo de envejecimiento absoluto y el tipo de envejecimiento por inactividad?