Lab - Configuración de Seguridad en el Switch

Topología

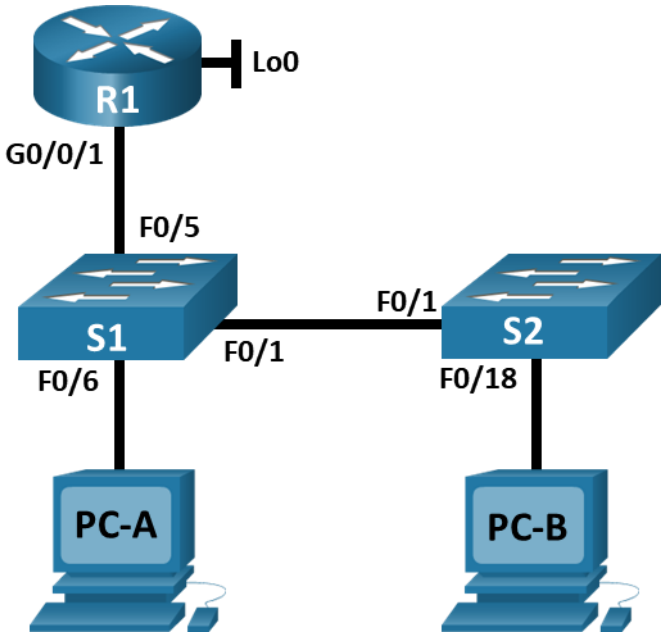

Tabla de asignación de direcciones

de red	Interface / VLAN	Dirección IP	Máscara de subred
R1	G0/0/1	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

Objetivos

Part 1: Configurar los dispositivos de red.

- Conecte la red.
- Configurar R1
- Configurar y verificar los parámetros básicos del switch **Part 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.
- Configurar 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.

Antecedentes/Escenario

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 (universalk9 imagen). 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 al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los switches 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 Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 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

Parte 1: Configurar los dispositivos de red.

Paso 1: Conecte la red.

a. Realice el cableado de red tal como se muestra en la topología.

b. Inicializar los dispositivos.

Paso 2: Configurar R1

a. Verifique la configuración en ejecución en R1 con el siguiente comando:

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

Paso 3: Configure y verifique os parámetros básicos del switch

a. Configure el nombre de host para los switches S1 y S2.

b. Evite búsquedas DNS no deseadas en ambos switches.

c. Configure las descripciones de interfaz para los puertos que están en uso en S1 y S2.

d. Establezca la puerta de enlace predeterminada para la VLAN de administración en 192.168.10.1 en ambos switches.

Parte 2: Configure las VLAN en los Switches.

Paso 1: Configure la VLAN 10.

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

Paso 2: 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.

Paso 3: Configure la VLAN 333 con el nombre Native en S1 y S2.

Paso 4: Configure la VLAN 999 con el nombre ParkingLot en S1 y S2.

Parte 3: Configure la seguridad del Switch.

Paso 1: Implemente el enlace 802.1Q.

a. En ambos switches, configure el enlace troncal en F0/1 para usar la VLAN 333 como la VLAN nativa.

b. Verifique que el enlace troncal esté configurado en ambos

c. Deshabilite la negociación DTP en F0/1 en S1 y S2.

d. Verifique con el comando **show interfaces** .

Paso 2: Configure puertos de acceso.

a. En S1, configure F0/5 y F0/6 como puertos de acceso asociados con la VLAN 10.

b. En S2, configure F0/18 como un puerto de acceso asociado con la VLAN 10.

Paso 3: Asegure y deshabilite los puertos del switch no utilizados.

a. En S1 y S2, mueva los puertos no utilizados de la VLAN 1 a la VLAN 999 y desactive los puertos no utilizados.

b. Verifique que los puertos no utilizados estén deshabilitados y asociados con la VLAN 999 emitiendo el comando **show interfaces status** .

Paso 4: Documente e implemente seguridad de puertos (port security).

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.

a. En S1, ejecute 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 predeterminada de puertos	
Característica (Feature)	**Configuración predeterminada (Default Setting)**
Seguridad de Puertos(Port Security)	
Número máximo de direcciones MAC (Maximum number of MAC addresses)	
Modo de Violacion (Violation Mode)	
Tiempo de Vencimiento (Aging Time)	
Tipo de Vencimiento (Aging Type)	
Antigüedad segura de direcciones estáticas (Secure Static Address Aging)	
Dirección MAC segura persistente (Sticky MAC Address)	

b. En S1, habilite la seguridad de puerto (port security) en F0/6 con la siguiente configuración:

- Número máximo de direcciones MAC: **3**
- Tipo de violación (Violation type):

restrict ○ Tiempo de vencimiento (Aging

time): **60 min** ○ Tipo de vencimiento

(Aging type): **inactivity**

c. Verifique la seguridad de puerto (port security) en S1 F0/6.

d. Habilite la seguridad de puerto (port security) para F0/18 en S2. Configure el puerto para agregar direcciones MAC, aprendidas automáticamente, a la configuración.

e. Configure las siguientes la seguridad de puerto (port security) en S2 F 0/18:

- Número máximo de direcciones MAC: **2**
- Tipo de Violación (Violation type):

Protect ○ Tiempo de vencimiento (Aging

time): **60 min**

f. Verifique la seguridad de puerto (port security) en S2 F0/18.

Paso 5: Implemente DHCP snooping.

a. En S2, habilite DHCP snooping y configúrelo para la VLAN 10.

b. Configure el puerto troncal en S2 como un puerto confiable (trusted ported).

c. Limite el puerto no confiable, F18 en S2, a cinco paquetes DHCP por segundo.

d. Verifique DHCP snooping en S2.

Paso 6: BPDU.

a. Configure PortFast en todos los puertos de acceso que están en uso en ambos switches.

b. Habilite BPDU guard, en los puertos de acceso de VLAN 10 conectados a la PC-A y PC-B.

c. Verifique que BPDU guard y PortFast estén habilitados en los puertos apropiados.

Paso 7: Verifique la conectividad de extremo a extremo

Verifique la conectividad PING entre todos los dispositivos en la tabla de direccionamiento IP. Verifique la conectividad PING entre todos los dispositivos en la tabla de direccionamiento IP.

Preguntas de reflexión

1. En referencia a Port Security en S2, ¿por qué cuando se configuró el aprendizaje permanente, no se establecio un temporizador para darle seguimiento al timempo de vencimiento restante?

   Este conmutador no es compatible con el envejecimiento de la seguridad del puerto de las direcciones seguras persistentes.

2. En referencia a Port Security en S2, si carga el archivo de configuración en S2, ¿por qué la PC-B en el puerto 18 nunca obtendrá una dirección IP a través de DHCP?

   La seguridad del puerto está configurada para solo dos direcciones MAC y el puerto 18 tiene dos direcciones MAC "permanentes" vinculadas al puerto

3. En referencia a Port Security, ¿cuál es la diferencia entre el tipo de envejecimiento absoluto y el tipo de envejecimiento por inactividad?

Si se establece el tipo de inactividad, las direcciones seguras en el puerto se eliminarán solo si no hay tráfico de datos desde las direcciones de origen seguras durante el período de tiempo especificado.