Packet Tracer: Configuración de la seguridad de puertos de un switch

Topología

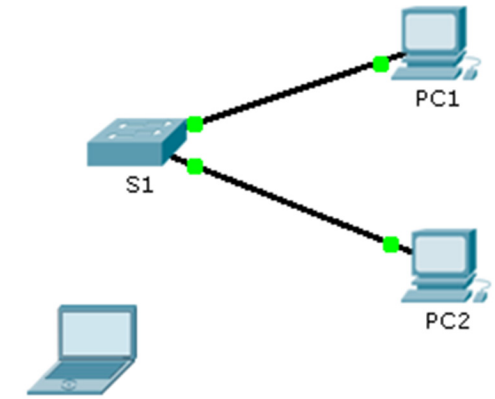

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Computadora portátil maliciosa	NIC	10.10.10.12	255.255.255.0

Objetivo

Parte 1: Configurar la seguridad de los puertos

Parte 2: Verificar la seguridad de los puertos

Aspectos básicos

En esta actividad, configurará y verificará la seguridad de puertos de un switch. La seguridad de puertos permite restringir el tráfico de entrada de un puerto mediante la limitación de las direcciones MAC que tienen permitido enviar tráfico al puerto.

Parte 1: Configurar la seguridad del puerto

a. Acceda a la línea de comandos del **S1** y habilite la seguridad de puertos en Fast Ethernet 0/1 y 0/2.

b. Establezca la seguridad máxima, de modo que solo un dispositivo pueda acceder a los puertos Fast Ethernet 0/1 y 0/2.

c. Proteja los puertos de modo que la dirección MAC de un dispositivo se detecte de forma dinámica y se agregue a la configuración en ejecución.

d. Establezca la violación para que los puertos Fast Ethernet 0/1 y 0/2 no se desactiven cuando se produzca una violación, pero se genere una notificación de la violación de seguridad y se eliminen los paquetes de la fuente desconocida.

e. Deshabilite todos los demás puertos sin utilizar. Sugerencia: utilice la palabra clave **range** para aplicar esta configuración a todos los puertos de forma simultánea.

Parte 2: Verificar la seguridad del puerto

a. En la **PC1**, haga ping a la **PC2**.

b. Verifique que la seguridad de puertos esté habilitada y que las direcciones MAC de la **PC1** y la **PC2** se hayan agregado a la configuración en ejecución.

c. Conecte la **Computadora portátil maliciosa** a cualquier puerto de switch no utilizado y observe que las luces de enlace estén rojas.

d. Habilite el puerto y verifique que la **Computadora portátil maliciosa** pueda hacer ping a la **PC1** y la **PC2**. Después de la verificación, desactive el puerto conectado a la **Computadora portátil maliciosa.**

e. Desconecte la **PC2** y conecte la **Computadora portátil maliciosa** al puerto de la **PC2**. Verifique que la **Computadora portátil maliciosa** no pueda hacer ping a la **PC1**.

f. Muestre las infracciones de seguridad de puertos correspondientes al puerto al que está conectada la **Computadora portátil maliciosa**.

g. Desconecte la **Computadora portátil maliciosa** y vuelva a conectar la **PC2**. Verifique que la **PC2** pueda hacer ping a la **PC1**.

h. ¿Por qué la **PC2** puede hacer ping a la **PC1**, pero la **Computadora portátil maliciosa** no puede?

p

