

Configuración de seguridad de puerto en el switch

Resultados de Aprendizaje	
RdA1	Comprender La Estructura de la red.
RdA2	Aplicar los conocimientos de interconexión de redes.
RdA3	Efectuar medidas de seguridad básicas

INTRODUCCIÓN

En esta práctica de laboratorio, examinará y configurará un switch de LAN independiente. Pese a que el switch realiza funciones básicas en su estado predeterminado de manera no convencional, existe una cantidad de parámetros que un administrador de red debe modificar para garantizar una LAN segura y optimizada. Esta práctica de laboratorio presenta los conceptos básicos de la configuración del switch.

Diagrama de topología

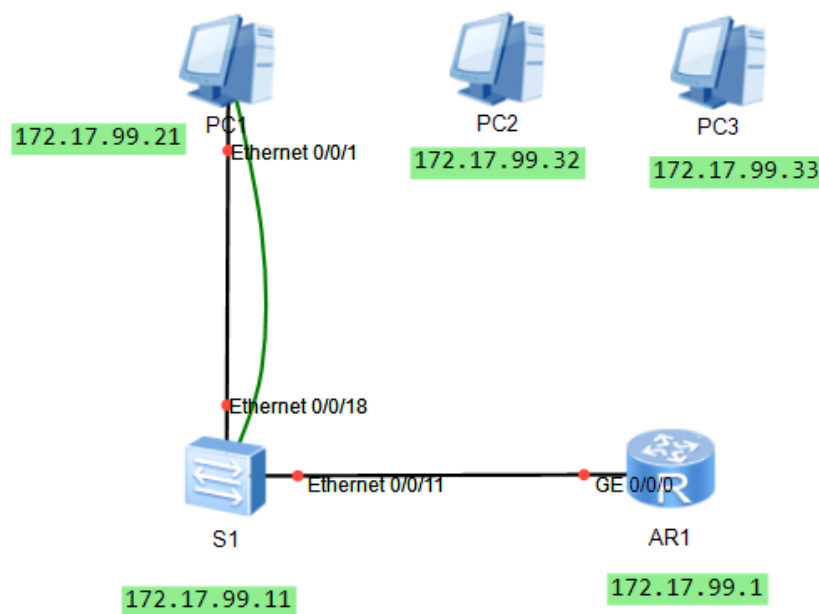


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway (puerta de salida) predeterminada
PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.11
PC2	NIC	172.17.99.32	255.255.255.0	172.17.99.11
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

I.- Realizar la configuración básica del switch

1.1: Entrar al modo privilegiado.

Puede acceder a todos los comandos del switch en modo privilegiado. Sin embargo, debido a que muchos comandos privilegiados configuran parámetros de operación, el acceso privilegiado debe estar protegido por contraseña a fin de evitar el uso no autorizado.

1.2: Examinar la configuración actual del switch.

Examine el archivo de configuración activa actual.

<Switch> **display current-configuration**

2.1: Configurar un segundo host.

Para esta tarea es necesario un segundo host. Establezca la dirección IP de la PC2 en 172.17.99.32 con una máscara de subred 255.255.255.0 y una gateway predeterminada en 172.17.99.11. No conecte aún esta PC al switch.

2.2: Verificar la conectividad.

Verifique que la PC1 y el switch aún están correctamente configurados haciendo ping a la dirección IP de la VLAN 99 del switch desde el host.

2.3: Copiar las direcciones MAC del host.

Anote las direcciones MAC de los host

Recuerde utilizar en cmd el comando ipconfig /all para saber mac del host.

PC1 _____

PC2 _____

2.4: Determinar qué direcciones MAC ha aprendido el switch.

Muestre las direcciones MAC aprendidas utilizando el comando **display mac-address dynamic**

```
.
<S1>display mac-address dynamic
```

¿Las direcciones MAC concuerdan con las direcciones MAC del host?

2.5: Enumerar las opciones de seguridad de puerto.

Explore las opciones para configurar la seguridad de puerto en la interfaz Fast Ethernet 0/18.

```
<S1> system-view
[S1]interface ethernet 0/0/18
[S1 interface ethernet 0/0/18] port-security enable
```

2.6: Configurar la seguridad de puerto en un puerto de acceso.

Configure el puerto del switch Giga Ethernet 0/18 para que acepte sólo dos dispositivos, para que aprenda las direcciones MAC de dichos dispositivos dinámicamente y para que bloquee el tráfico de hosts inválidos en caso de violación.

```
[S1 interface ethernet 0/0/18]port link-type access
[S1 interface ethernet 0/0/18]port-security enable
```

```
[S1 interface ethernet 0/0/18] port-security max-mac-num 2
[S1 interface ethernet 0/0/18]port-security mac-address sticky
[S1 interface ethernet 0/0/18]port-security protect-action
```

2.7: Verificar los resultados.

Muestre la configuración de seguridad de puerto.

<S1> display mac-address sticky

<S1> display current-configuration interface ethernet 0/0/18

2.8: Examinar el archivo de configuración activo.

<S1> display current-configuration

¿Hay sentencias enumeradas que reflejan directamente la implementación de seguridad de la configuración activa? _____

2.9: Modificar la configuración de post seguridad en un puerto.

En la interfaz Giga ethernet 0/18, establezca la dirección MAC de seguridad máxima del puerto en 1 y que se desactive en caso de violación.

```
[S1 interface ethernet 0/0/18] port-security max-mac-num 1
[S1 interface ethernet 0/0/18] port-security protect-action shutdown.
```

Haga ping a la dirección de la VLAN 99 del switch desde la PC1 para verificar la conectividad y actualizar la tabla de direcciones MAC. En este momento debe ver la dirección MAC para la PC1 “insertada” en la configuración activa.

2.11: Introducir un host no autorizado.

Desconecte la PC1 y conecte la PC2 al puerto Fast Ethernet 0/18. Haga ping a la dirección 172.17.99.11 de la VLAN 99 desde el nuevo host. Espere a que la luz de enlace color ámbar se torne verde. Una vez que se torna verde, debe apagarse casi inmediatamente.

Anote cualquier observación:

2.12: Mostrar la información sobre la configuración del puerto.

Para ver la información de configuración sólo para el puerto Fast Ethernet 0/18, ejecute el siguiente comando:

<S1> display interface ethernet 0/0/18

¿Cuál es el estado de esta interfaz?

2.13: Reactivar el puerto.

Si se produce una violación de seguridad y el puerto se desconecta, puede utilizar el comando **undo shutdown** para reactivarlo. Sin embargo, mientras el host no autorizado se encuentre conectado a Giga ethernet 0/18, cualquier tráfico desde el host desactivará el puerto. Vuelva a conectar la PC1 a Giga ethernet 0/18 e ingrese los siguientes comandos en el switch:

```
<S1> system-view
[S1] interface ethernet 0/0/18
[S1 interface ethernet 0/0/18]undo shutdown
```

2.14: Limpieza

Eliminar el archivo de configuración de inicio del switch de la NVRAM.

```
<Switch>reset saved-configuration
```

Como respuesta, aparecerá la siguiente petición de entrada:

```
<Huawei>reset saved-configuration
Warning: The action will delete the saved configuration in the
device.
The configuration will be erased to reconfigure. Continue? [Y/N]:y
Warning: Now clearing the configuration in the device.
Apr 10 2013 14:43:13-08:00 Huawei %01CFM/4/RST_CFG(1)[2]:The user
chose Y when
deciding whether to reset the saved configuration.
Info: Succeeded in clearing the configuration in the device.
```

COMENTARIOS

_____A continuación exprese sus dificultades, problemas o percepción general con respecto a la guía.
