Configuración de ACL extendidas

Topología

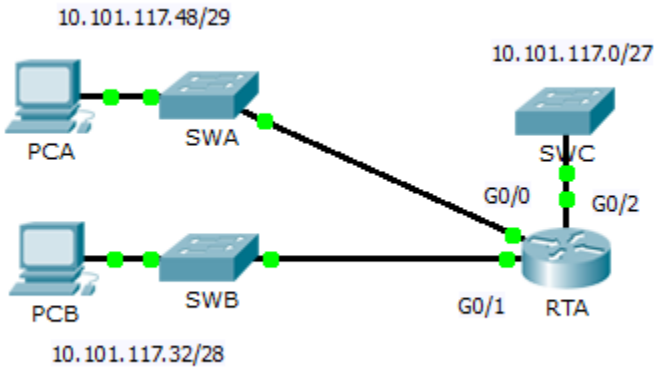

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RTA	G0/0	10.101.117.49	255.255.255.248	N/D
	G0/1	10.101.117.33	255.255.255.240	N/D
	G0/2	10.101.117.1	255.255.255.224	N/D
PCA	NIC	10.101.117.51	255.255.255.248	10.101.117.49
PCB	NIC	10.101.117.35	255.255.255.240	10.101.117.33
SWC	VLAN1	10.101.117.2	255.255.255.224	10.101.117.1

Objetivos

Parte 1: configurar, aplicar y verificar una ACL extendida numerada

Parte 2: preguntas de reflexión

Aspectos básicos/situación

En esta situación, los dispositivos de una LAN pueden acceder de forma remota a los dispositivos de otra LAN mediante el protocolo Telnet. Aparte de ICMP, se deniega todo el tráfico de otras redes.

Parte 1: configurar, aplicar y verificar una ACL extendida numerada

Configure, aplique y verifique una ACL para que cumpla con la siguiente política:

- Se permite el tráfico de Telnet desde los dispositivos de la red 10.101.117.32/28 hasta los dispositivos en las redes 10.101.117.0/27.
- Se permite el tráfico ICMP desde cualquier origen hasta cualquier destino.
- El resto del tráfico a 10.101.117.0/27 está bloqueado.

Paso 1: configurar la ACL extendida.

a. Desde el modo de configuración adecuado en el **RTA**, utilice el último número válido de lista de acceso extendida para configurar la ACL. Utilice los siguientes pasos para crear la primera instrucción de ACL:

   1) El último número de lista para ACL extendidas es 199.

   2) El protocolo es TCP.

   3) La red de origen es 10.101.117.32.

   4) La máscara wildcard se puede determinar si se resta 255.255.255.240 a 255.255.255.255.

   5) La red de destino es 10.101.117.0.

   6) La máscara wildcard se puede determinar si se resta 255.255.255.224 a 255.255.255.255.

   7) El protocolo es Telnet.

   ¿Cuál es la primera instrucción de ACL?

   _____

   _____

b. Se permite ICMP, y se necesita una segunda instrucción de ACL. Utilice el mismo número de lista de acceso para permitir todo el tráfico ICMP, independientemente de la dirección de origen o de destino. ¿Cuál es la segunda instrucción de ACL? (Sugerencia: utilice las palabras clave any).

   _____

c. El resto del tráfico IP se deniega de manera predeterminada.

Paso 2: aplicar el ACL extendida.

La regla general es colocar las ACL extendidas cerca del origen. Sin embargo, dado que la lista de acceso 199 afecta el tráfico que se origina de las dos redes, 10.101.117.48/29 y 10.101.117.32/28, la mejor ubicación de esta ACL podría ser en la interfaz gigabit Ethernet 0/2 en dirección saliente. ¿Cuál es el comando para aplicar la ACL 199 a la interfaz Gigabit Ethernet 0/2?

_____

Paso 3: verificar la implementación de la ACL extendida.

a. Haga ping de la **PCB** a todas las otras direcciones IP en la red. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.

b. Desde la **PCB**, acceda al **SWC** mediante Telnet. La contraseña es **cisco**.

c. Salga del servicio de Telnet del **SWC**.

d. Haga ping de la **PCA** a todas las otras direcciones IP en la red. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.

e. Desde la **PCA**, acceda al **SWC** mediante Telnet. La lista de acceso ocasiona que el router rechace la conexión.

f. Desde la **PCA**, acceda al **SWB** mediante Telnet. La lista de acceso está colocada en **G0/2** y no afecta esta conexión.

g. Una vez que inicie sesión en el **SWB**, no salga. Acceda al **SWC** mediante Telnet.