Taller configuración de ACL IPv4 estándar numeradas Topología

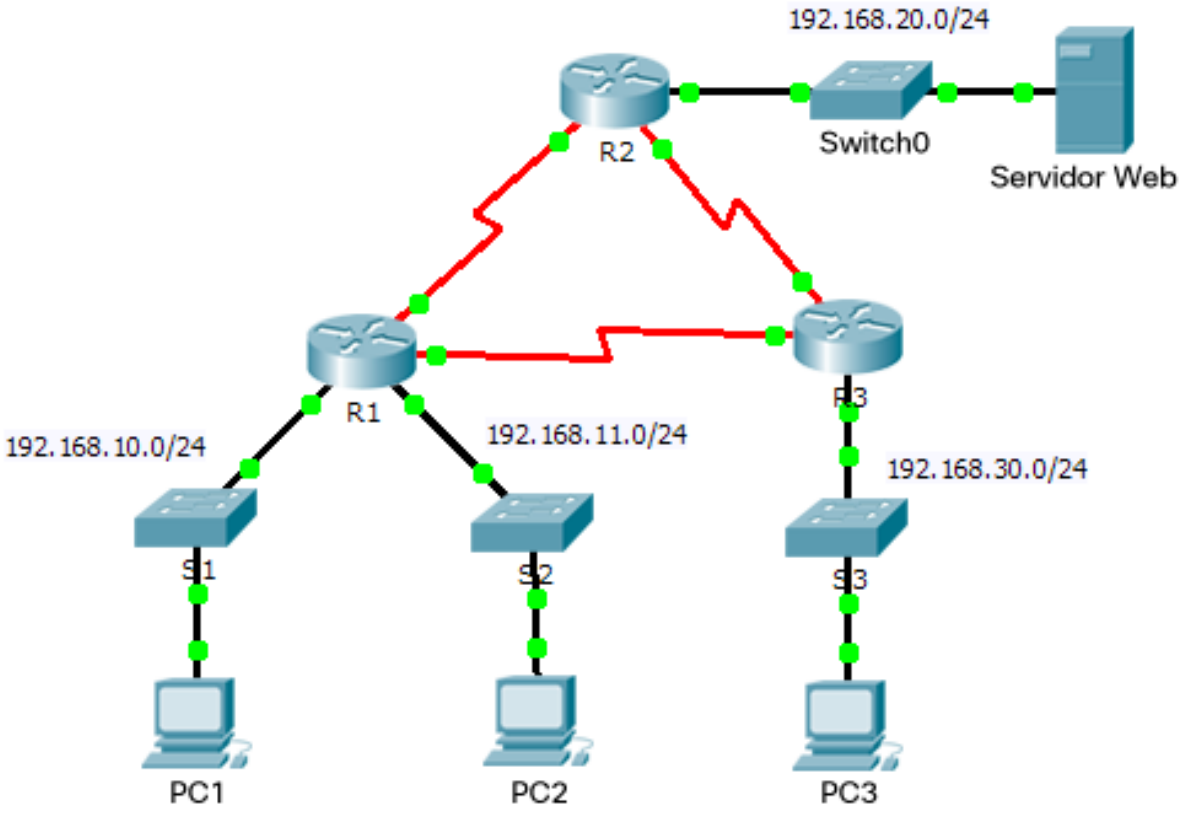

Tabla de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	N/D
	G0/1	192.168.11.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
	S0/0/1	10.3.3.1	255.255.255.252	N/D
R2	G0/0	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
R3	G0/0	192.168.30.1	255.255.255.0	N/D
	S0/0/0	10.3.3.2	255.255.255.252	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
Servidor Web	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos

Parte 1: planificar una implementación de ACL

Parte 2: configurar, aplicar y verificar una ACL estándar

Aspectos básicos/situación

Las listas de control de acceso (ACL) estándar son scripts de configuración del router que controlan si un router permite o deniega paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, incluidas las direcciones IP y el routing del protocolo de routing de gateway interior mejorado (EIGRP).

Parte 1: planificar una implementación de ACL

Paso 1: investigar la configuración actual de red.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tenga conectividad completa. Elija una computadora y haga ping a otros dispositivos en la red para verificar que la red tenga plena conectividad. Debería poder hacer ping correctamente a todos los dispositivos.

Paso 2: evaluar dos políticas de red y planificar las implementaciones de ACL.

a. En el **R2** están implementadas las siguientes políticas de red:

- La red 192.168.11.0/24 no tiene permiso para acceder al **servidor web** en la red 192.168.20.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.11.0/24 al **servidor web** en 192.168.20.254 sin interferir con otro tráfico, se debe crear una ACL en el **R2**. La lista de acceso se debe colocar en la interfaz de salida hacia el **servidor web**. Se debe crear una segunda regla en el **R2** para permitir el resto del tráfico.

b. En el **R3** están implementadas las siguientes políticas de red:

- La red 192.168.10.0/24 no tiene permiso para comunicarse con la red 192.168.30.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.10.0/24 a la red 192.168.30/24 sin interferir con otro tráfico, se debe crear una lista de acceso en el **R3**. La ACL se debe colocar en la interfaz de salida hacia la **PC3**. Se debe crear una segunda regla en el **R3** para permitir el resto del tráfico.

- Un ping de 192.168.30.10 a 192.168.20.254 se realiza correctamente.