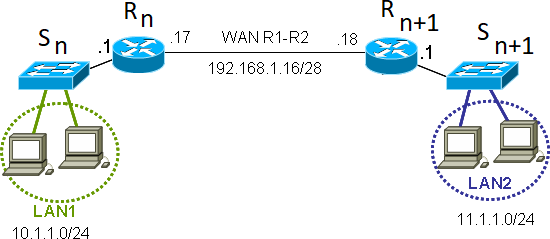


## Objetivos

Identificar los componentes principales de las ACLs y se configuran lista de Acceso en los Routers de la marca Cisco.

## Desarrollo

1. De acuerdo con el siguiente diagrama el instructor le asignara el grupo al que pertenece:



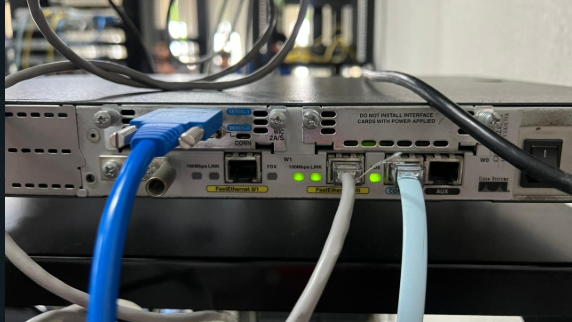


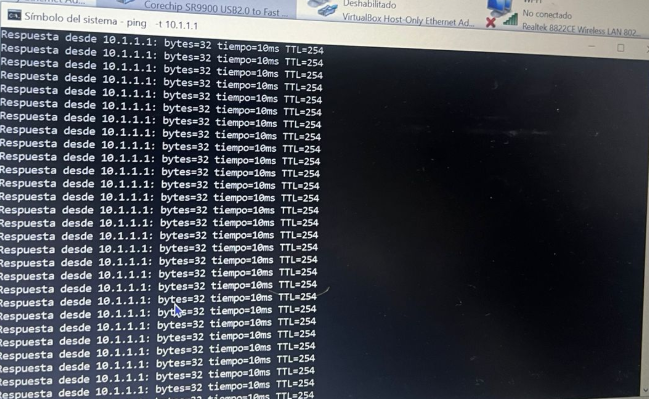


Diagrama de ingeniería de red

El direccionamiento IP que se muestra es para el equipo de trabajo no.1, para los siguientes se deberá sumar un digito al primer numero de cada dirección (ejemplo equipo no. 2 (LAN1 = 20.1.1.0. LAN2= 21.1.1.0 …WANR1-R2 = 193.168.1.16 ..etc)

El protocolo de enrutamiento que se usa para este laboratorio es RIP.

1. Antes de crear las listas de acceso usted deberá probar toda la conectividad de la red utilizando el comando ping hacia todos los hosts vecinos.
2. ¿Fue exitoso el acceso a todos los hosts de la red?, en caso contrario realice troubleshooting con sus compañeros de equipo. Si todos los pings respondonden exitosamente



1. Utilizando la configuración del diagrama anterior proceda a crear las siguientes listas de acceso
   * Configurar una Lista de Acceso que evite que la PC1 en la LAN 1 pueda tener comunicación con el router 2
   * Evitar que la LAN del Router 3 pueda tener comunicación con las LANs del Router 1
2. Para realizar la primera lista de acceso ingrese al router R2 y cree la ACL correspondiente:

# R2(config)# access-list 1 deny A.B.C.D

Donde: A.B.C.D es la ip de la PC1

1. ¿Qué significa el número uno de la access-list?

El número "1" en la access-list identifica una lista de acceso estándar específica en el router.

1. Para permitir que todos los demás miembros de la red tengan acceso R2, utilice:

# R2(config)# access-list 1 permit any

1. ¿Cual es la última instrucción que el IOS coloca en todas access list creadas?

La última instrucción es "deny any", que deniega todo el tráfico que no esté explícitamente permitido.

1. Ahora aplique esta access-list a la interfaz correspondiente del Router 2 con el comando:

# R2(config-if)# ip access-group 1 in

9. ¿Cuál interfase selecciono? ¿Explique por qué?

La interfaz seleccionada es la interfaz que conecta el router R2 con la LAN1, porque es la interfaz que recibe el tráfico de la PC1.

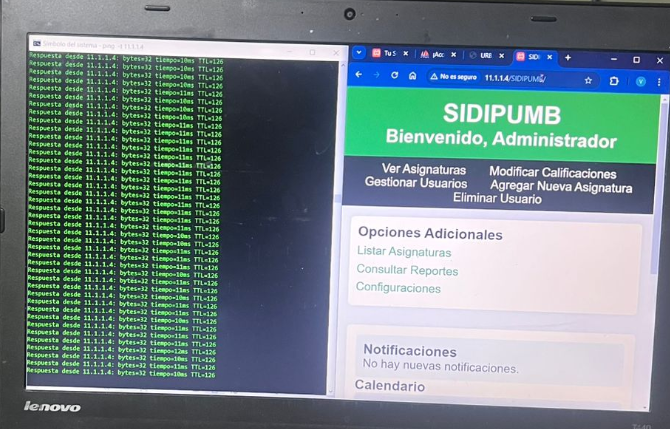
1. ¿Qué significa la opción in?

La opción "in" se refiere al tráfico que ingresa a la interfaz

1. ¿Qué significa el número uno después de la instrucción access-group?

El número uno se refiere al número de la lista de acceso que se está aplicando.

1. Para probar el funcionamiento de esta lista de acceso intente mandar un ping desde la PC1 al router 2.
2. ¿Cual debería ser el resultado del punto anterior?



1. Para la segunda lista de acceso vaya al router R1 y cree la lista de acceso, utilice: **R1(config)#access-list 1 deny 200.30.30.0 0.0.0.15 (ejemplo) R1(config)#access-list 1 permit any**
2. Qué significa la instrucción 0.0.0.15 después de la dirección de IP del identificador de red.

La instrucción 0.0.0.15 se refiere a la máscara de subred.

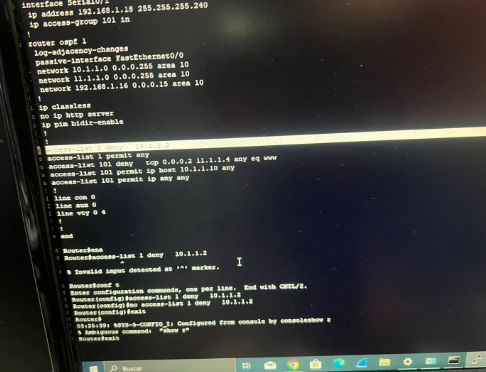
1. ¿En qué interfaces debe aplicar esta lista de acceso?

La lista de acceso debe aplicarse a las interfaces que conectan el router R1 con las LANs.

1. Para aplicar esta lista de acceso nuevamente utilice el comando:

# R1(config)#ip access-group 1 in

1. Compruebe el funcionamiento de esta lista de acceso



1. Ahora trate de bloquear todo el trafico de la aplicación FTP de red LAN 3 a la red LAN 4, para lo anterior solicite a su vecino implementar un servidor de FTP y realizar algunas pruebas exitosas de transferencia de archivos antes de realizar la lista de acceso y aplicarla a la interfase correspondiente.

Recuerde que debe permitir todo el demás tráfico entre las redes LAN 3 y LAN 4.

1. Anote los comandos para realizar lo anterior:

access-list 101 deny tcp 192.168.1.17 0.0.0.15 area 1

access-list 101 permit ip any any

interface FastEthernet 0/0

ip access-group 101 in

show running-config (Verificar la configuración)

show access-lists (Verificar el estado de la lista de acceso)

1. ¿En qué interfaces aplico esta lista de acceso? ¿Explique por qué?

interface fa0/1

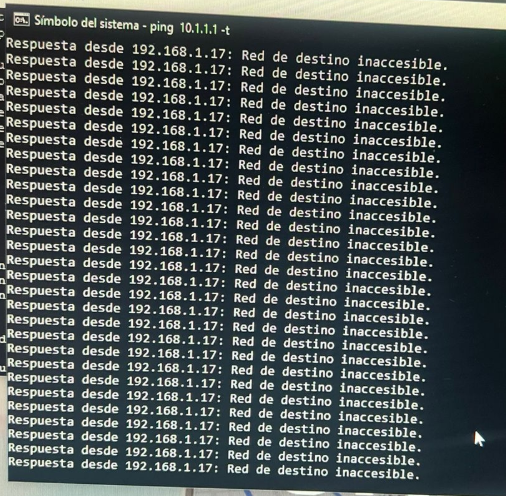
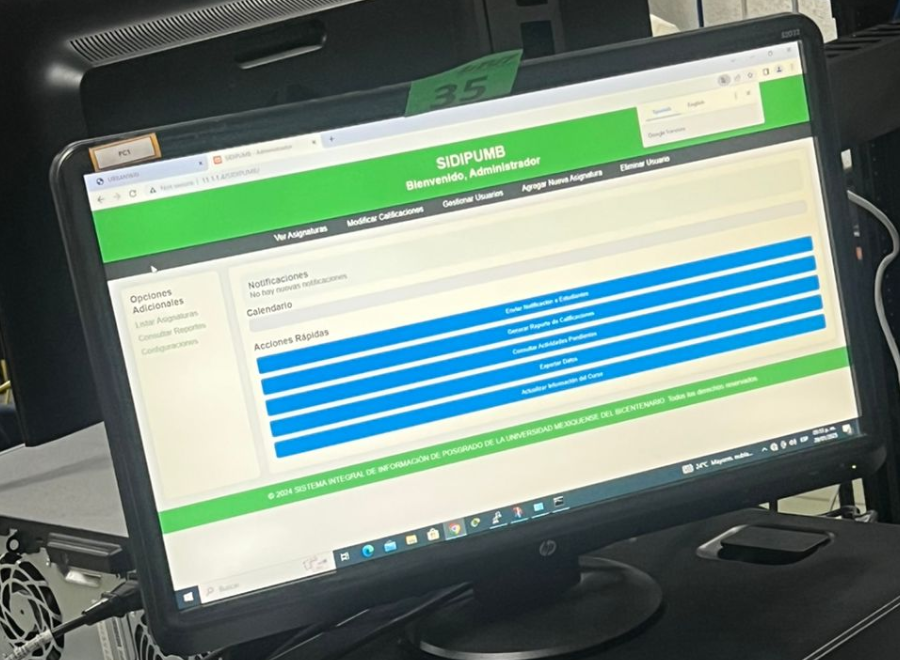
ip access-group 100 out

Por la topologia, donde sea mas fácil o de tu preferencia de realizar el filtrado

1. Cual comando utilizo para permitir el flujo de tráfico diferente a FTP.

access-list 100 permit ip any any

1. Compruebe el funcionamiento de esta lista de acceso

1. Como se llama este tipo de lista donde se utilizan las direcciones IP fuente y destino y el protocolo de la aplicación IP

Este tipo de lista se llama "Lista de Acceso Extendida".

## Conclusiones

Se demostró cómo las ACLs son esenciales para mantener la integridad y seguridad de una red, mostrando su capacidad para bloquear servicios específicos como el FTP mientras se permite el resto del tráfico, y cómo aplicarlas de manera efectiva en distintas interfaces para lograr el control deseado. Esta experiencia nos ha proporcionado una comprensión de las herramientas disponibles para la administración de redes y cómo implementarlas correctamente para asegurar la protección y eficiencia de nuestros sistemas de comunicación