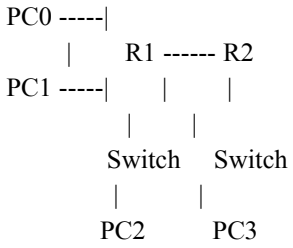
Práctica de Laboratorio: Configuración de Listas de Acceso Estándar y Extendidas en Cisco

1. Objetivos

- Comprender el propósito y funcionamiento de las listas de control de acceso (ACLs).
- Configurar ACLs estándar para controlar el tráfico por dirección IP de origen.
- Configurar ACLs extendidas para filtrar tráfico por dirección IP, protocolo y puertos.
- Verificar el funcionamiento y efecto de las ACLs aplicadas.

2. Topología de Red Sugerida



3. Equipamiento

- 2 Routers Cisco (R1 y R2)
- 2 Switches
- 4 PCs (PC0 a PC3)
- Cables de red
- Cisco Packet Tracer / GNS 3, o dispositivos físicos

4. Direccionamiento IP Sugerido

Dispositivo	Interfaz	Dirección IP	Subred
PC0	NIC	192.168.1.2	255.255.255.0
PC1	NIC	192.168.1.3	255.255.255.0
PC2	NIC	192.168.2.2	255.255.255.0
PC3	NIC	192.168.3.2	255.255.255.0
R1	Fa0/0	192.168.1.1	255.255.255.0
R1	Fa0/1	10.0.0.1	255.255.255.252
R2	Fa0/0	10.0.0.2	255.255.255.252
R2	Fa0/1	192.168.2.1	255.255.255.0
R2	Fa0/2	192.168.3.1	255.255.255.0

5. Actividades

Parte A: Configuración Básica

1. Configura el direccionamiento IP en todos los dispositivos.
2. Verifica la conectividad con ping entre todas las PCs.

Parte B: Lista de Acceso Estándar

Objetivo: Bloquear el acceso de PC0 (192.168.1.2) a cualquier red más allá de R1.

1. En R1, crea una ACL estándar:

```
R1(config)# access-list 10 deny 192.168.1.2
R1(config)# access-list 10 permit any
```

2. Aplica la ACL en la interfaz Fa0/0 (de entrada):

```
R1(config)# interface Fa0/0
R1(config-if)# ip access-group 10 in
```

3. Verifica que PC0 no puede hacer ping a PC2 ni PC3, pero PC1 sí.

Parte C: Lista de Acceso Extendida

Objetivo: Permitir únicamente tráfico web (HTTP) desde PC2 (192.168.2.2) hacia PC3 (192.168.3.2). Bloquear todo lo demás.

1. En R2, crea la ACL extendida:

```
R2(config)# access-list 100 permit tcp host 192.168.2.2 host 192.168.3.2 eq 80
R2(config)# access-list 100 deny ip any any
```

2. Aplica la ACL en la interfaz Fa0/2 (de entrada o salida según pruebas):

```
R2(config)# interface Fa0/2
R2(config-if)# ip access-group 100 in
```

3. Simula una conexión HTTP (web) desde PC2 a PC3. Asegúrate de que ICMP (ping) esté bloqueado y solo HTTP funcione.

6. Verificación

Utiliza los siguientes comandos para verificar:

```
show access-lists
show ip interface Fa0/0
show ip access-lists
debug ip packet
```

7. Preguntas de Análisis

1. ¿Cuál es la diferencia entre una ACL estándar y una extendida?
2. ¿Qué efecto tiene el orden de las instrucciones en una ACL?
3. ¿Por qué es importante tener una instrucción permit any al final de las ACLs?

8. Conclusiones