UNIVERSIDAD NACIONAL DE JUJUY

Facultad de Ingeniería
Analista Programador Universitario
Cátedra Redes II

Trabajo práctico Nº 5

Seguridad · Listas de control de acceso ACL

Datos de entrega	Completar
Nombre del grupo	
Comisión	
Integrantes	
Año	2026

Objetivo general

Aplicar listas de control de acceso para comprender cómo un router permite o bloquea tráfico según reglas definidas y verificar su efecto en Cisco Packet Tracer.

Objetivos específicos

- Definir ACL y diferenciar ACL estándar de ACL extendida.
- Interpretar wildcard masks, sentidos in y out y deny implícito.
- Configurar y verificar una ACL estándar en Cisco Packet Tracer.
- Analizar ACL extendidas respetando el orden de procesamiento.

Presentación

Responder cada consigna respetando su numeración. Incluir las capturas solicitadas junto al punto correspondiente, con texto y resultados legibles.

Parte 1 Conceptos básicos de ACL

Responder con palabras propias. Cuando resulte necesario, acompañar la explicación con un ejemplo breve de configuración.

1. ¿Qué es una ACL?

Respuesta del grupo:

2. ¿Qué tipos de ACL conoce?

Respuesta del grupo:

3. Explique la sintaxis de una ACL estándar y de una ACL extendida. Indique también cómo se crea una ACL y cómo se aplica a una interfaz de un router.

Respuesta del grupo:

Parte 2 Configuración de ACL estándar en Packet Tracer

Material de trabajo. Utilizar exclusivamente el archivo EJERCICIO 1 PACKET TRACER ACL.pka provisto para esta actividad. No modificar la topología ni el direccionamiento ya configurados.

4. Reconozca la topología del archivo de Packet Tracer e identifique las redes involucradas en la práctica.

Equipo o red	Identificación en la topología	Dato a verificar
LAN de PC1	192.168.10.0/24	Red conectada a R1 mediante S1.
LAN de PC2	192.168.11.0/24	Red conectada a R1 mediante S2.
LAN del servidor web	192.168.20.0/24	Red conectada a R2 mediante S0.
LAN de PC3	192.168.30.0/24	Red conectada a R3 mediante S3.

Evidencia 1. Incorpore una captura de la topología completa. Deben distinguirse R1, R2, R3, PC1, PC2, PC3, el servidor web y las cuatro redes.

5. Antes de configurar las ACL, compruebe la conectividad solicitada y registre el resultado.

Prueba inicial	Origen	Destino	Resultado antes de la ACL
A	PC2, red 192.168.11.0/24	Servidor web, red 192.168.20.0/24	
B	PC1, red 192.168.10.0/24	PC3, red 192.168.30.0/24	

Evidencia 2. Incorpore una captura de las pruebas previas. Debe verse el equipo de origen, el destino y que la comunicación inicialmente funciona.

6. En R2, configure y aplique la ACL estándar numerada 1 para impedir que la red 192.168.11.0/24 acceda a la red 192.168.20.0/24.

La ACL estándar solo evalúa la dirección de origen. Por ese motivo se aplica en R2, sobre la interfaz GigabitEthernet 0/0 y en sentido saliente: así filtra el tráfico cuando intenta salir hacia la red 192.168.20.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)# access-list 1 permit any
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Evidencia 3. Incorpore una captura de la configuración en R2 y otra de show access-lists 1 o show ip interface gigabitEthernet 0/0. Deben verse la ACL y el sentido out.

7. En R3, configure y aplique la ACL estándar numerada 1 para impedir que la red 192.168.10.0/24 acceda a la red 192.168.30.0/24.

En este caso la ACL se aplica en R3, sobre GigabitEthernet 0/0 y en sentido saliente, porque el tráfico que se desea restringir tiene como destino la red 192.168.30.0/24.

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit any
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

Evidencia 4. Incorpore una captura de la configuración en R3 y otra de show access-lists 1 o show ip interface gigabitEthernet 0/0. Deben verse la ACL y el sentido out.

8. Verifique el efecto de las ACL aplicadas. Complete la tabla e incorpore las capturas de las pruebas finales.

Prueba final	Origen	Destino	Resultado esperado	Resultado obtenido
A	PC2, red 192.168.11.0/24	Servidor web, red 192.168.20.0/24	Denegado	
B	PC1, red 192.168.10.0/24	PC3, red 192.168.30.0/24	Denegado	
C	PC2, red 192.168.11.0/24	PC3, red 192.168.30.0/24	Permitido	
D	PC1, red 192.168.10.0/24	Servidor web, red 192.168.20.0/24	Permitido	

Evidencia 5. Incorpore las capturas de las cuatro pruebas finales. Ubique cada captura inmediatamente debajo de la fila o respuesta que permite justificar.

9. Explique brevemente por qué las ACL se aplican en sentido out en R2 y R3. Indique qué alcance tendría una ACL estándar aplicada in sobre R1 para las redes de origen.

Respuesta del grupo:

Parte 3 Evaluación de ACL extendidas

5. Lea las ACL 103 y 104 de arriba hacia abajo. Para cada caso, indique si el acceso queda permitido o denegado. Si no coincide con ninguna ACE, tenga en cuenta el deny implícito.

ACL 103

```
access-list 103 permit ip host 192.168.1.66 host 192.168.3.75
access-list 103 permit ip host 192.168.1.77 host 192.168.3.75
access-list 103 deny ip 192.168.1.0 0.0.0.255 host 192.168.3.75
access-list 103 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 103 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Origen	Destino	Permitir o denegar
192.168.1.66	192.168.3.51	
192.168.1.66	192.168.3.75	
192.168.1.88	192.168.3.51	
192.168.1.88	192.168.3.75	
192.168.1.77	192.168.3.75	
192.168.1.33	192.168.2.34	

ACL 104

```
access-list 104 deny tcp host 192.168.1.66 host 192.168.3.200 eq 80
access-list 104 permit tcp host 192.168.1.77 host 192.168.3.75 eq 22
access-list 104 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 104 permit ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
```

Origen	Destino	Protocolo	Permitir o denegar
192.168.1.66	192.168.1.88	HTTP	
192.168.1.66	192.168.4.75	SSH	
192.168.1.77	192.168.3.75	HTTP	
192.168.1.88	192.168.2.75	HTTP	
192.168.1.77	192.168.3.75	SSH	
192.168.1.66	192.168.3.200	HTTP	