Guía de Laboratorio

GL-3

Configuración de Routers Cisco Packet Tracer

ACL Estándar y ACL Extendida

Elaborado por:

Santiago Aguilar Cárdenas

Facultad de Ingeniería Electrónica

Universidad Santo Tomás

Seccional Tunja

Información Académica

Guía de Laboratorio

GL-3

Elaborado por:

Santiago Aguilar Cárdenas

Director del Trabajo de Grado:
Ph.D. William Fabián Chaparro Becerra

Codirectores del Trabajo de Grado:
M.Sc. Angélica María Salazar Madrigal
M.Sc. Cristian David Parra Camacho

Facultad de Ingeniería Electrónica
Universidad Santo Tomás
Seccional Tunja

Información del Documento

Ficha técnica

Guía:	GL-3 – ACL estándar y ACL extendida en Cisco Packet Tracer.
Modalidad:	Simulación.
Duración sugerida:	2 horas (según el avance del grupo).
Público objetivo:	Estudiantes de pregrado.
Requisitos:	Direccionamiento IPv4 configurado, conectividad base verificada con `ping`.
Producto esperado:	Políticas de filtrado con ACL estándar y extendida, verificadas con pruebas (`ping`, acceso HTTP y `show access-lists`).

Facultad de Ingeniería Electrónica
Universidad Santo Tomás
Seccional Tunja

PREÁMBULO

Propósito

Esta guía presenta un procedimiento **paso a paso y verificable** para implementar **Listas de Control de Acceso (ACL)** en simulación. Se trabaja con la misma topología base de la guía GL-1 (cuatro routers y cuatro LAN) y se aplican dos casos:

- **ACL estándar:** bloqueo por **origen** (subred) y aplicación sobre una interfaz.
- **ACL extendida:** bloqueo por **protocolo/puerto** (HTTP) entre un host cliente y un servidor web.

Nota Importante

En los ejemplos se utilizan direcciones del tipo **192.168.XX.0**. Ajuste **XX** según el valor asignado por el docente (por ejemplo, **XX=13**). Mantenga consistencia entre PCs, routers y servidores.

Criterios de trabajo

- Antes de aplicar ACL, confirme conectividad base (`ping`) y rutas.
- Recuerde que toda ACL termina con un **deny any** implícito. Incluya la línea `permit` requerida.
- Aplique ACL en la interfaz correcta y en la dirección adecuada: **in** (entrada) o **out** (salida).
- Guarde evidencias: `show access-lists`, `show ip interface`, capturas del navegador (HTTP) y resultados de `ping`.

Competencias

- Interpretación de *wildcard masks* en ACL estándar.
- Filtrado por protocolo, origen/destino y puertos en ACL extendida.

Objetivos

- Reconocer el propósito y funcionamiento de **ACL estándar** y **ACL extendida**.
- Implementar una **ACL estándar** para bloquear una red de origen específica, manteniendo el resto del tráfico permitido.
- Implementar una **ACL extendida** para bloquear **HTTP (puerto 80)** entre un host cliente y un servidor web, permitiendo otros servicios.
- Aplicar ACL en la interfaz y dirección correctas (`in`/`out`) y validar con comandos `show`.
- Documentar evidencias de funcionamiento (`ping`, acceso web, contadores de coincidencias en ACL).

Resultados esperados

Al finalizar, el estudiante entregará:

1. Evidencias (capturas o transcripción) de los comandos ejecutados.
2. Evidencias de conectividad **antes y después** de aplicar ACL (`ping` y navegación HTTP).
3. Salidas de verificación: `show access-lists` y `show ip interface` (o `show running-config | section access-list`).

Índice general

Índice de figuras

1

Unidad 1: Escenario, topología y preparación

1.1 Escenario de trabajo

En esta práctica se utiliza una topología de **cuatro routers** interconectados en forma de rectángulo y **cuatro redes LAN** (una por extremo). Sobre esta base se implementan políticas de filtrado usando **ACL estándar** y **ACL extendida** en **routers Cisco 1841** de Cisco Packet Tracer.

Idea clave

ACL estándar filtra principalmente por **dirección IP de origen**.

ACL extendida filtra por **origen, destino, protocolo y puertos** (por ejemplo, HTTP/80).

1.2 Topología y redes

La topología base (misma referencia de GL-1) se muestra en la Figura 1.1. Para el laboratorio físico, los equipos Cisco 1841 se conectan por consola y por interfaces FastEthernet/Serial según el montaje disponible.

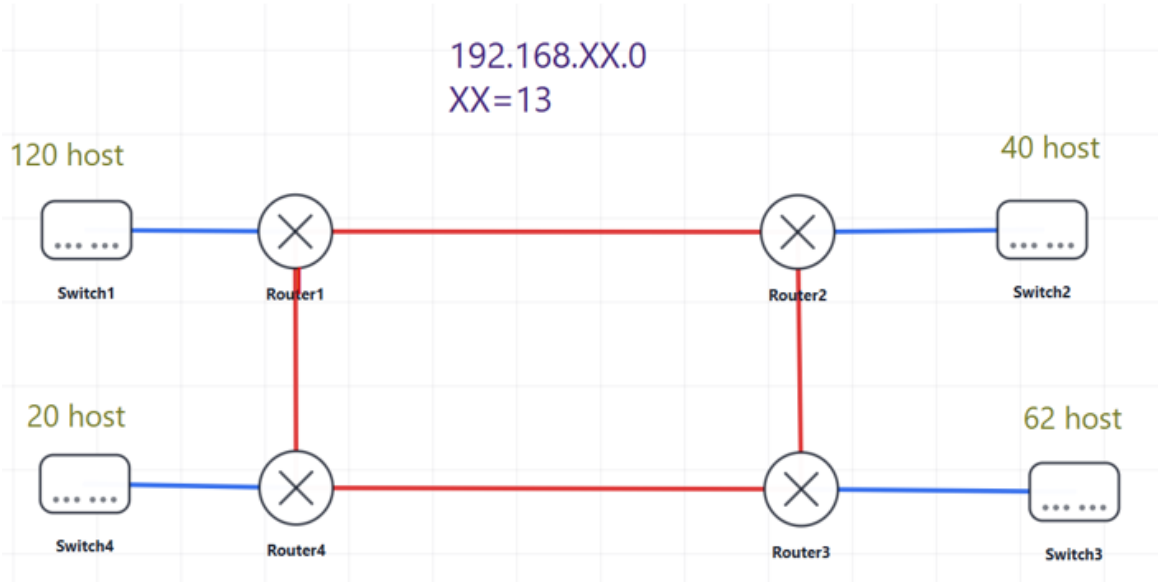

Figura 1.1: Topología base con 4 routers y 4 LAN (referencia de laboratorio).

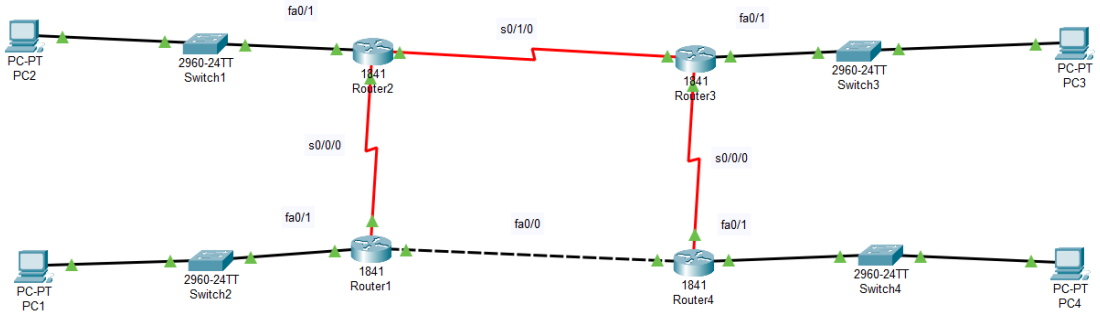

Figura 1.2: Configuración Cisco Packet Tracer.

1.3 Requisitos previos

1. Conectividad base establecida (direccionamiento y rutas configuradas).
2. Identificar **qué red se desea bloquear** y **desde dónde se desea bloquear**.

Nota Importante

Antes de crear ACL, valide conectividad con `ping` entre redes. Así podrá comprobar el efecto del filtrado **después** de aplicar la ACL.

2

Unidad 2: ACL estándar (filtrado por origen)

2.1 Objetivo de la unidad

Implementar una **ACL estándar** para impedir conectividad desde una red de origen específica, manteniendo permitido el resto del tráfico.

2.2 Prueba inicial (antes de ACL)

Siguiendo la misma topología, verifique primero que existe conectividad con `ping`. En el escenario de referencia, se realizan pruebas hacia el host **192.168.14.2** (PC) desde el origen indicado por el docente. Si las respuestas son exitosas, continúe.

Evidencia esperada

`ping` exitoso: **0 % perdidos**. Esta evidencia se compara con el resultado **después** de aplicar la ACL.

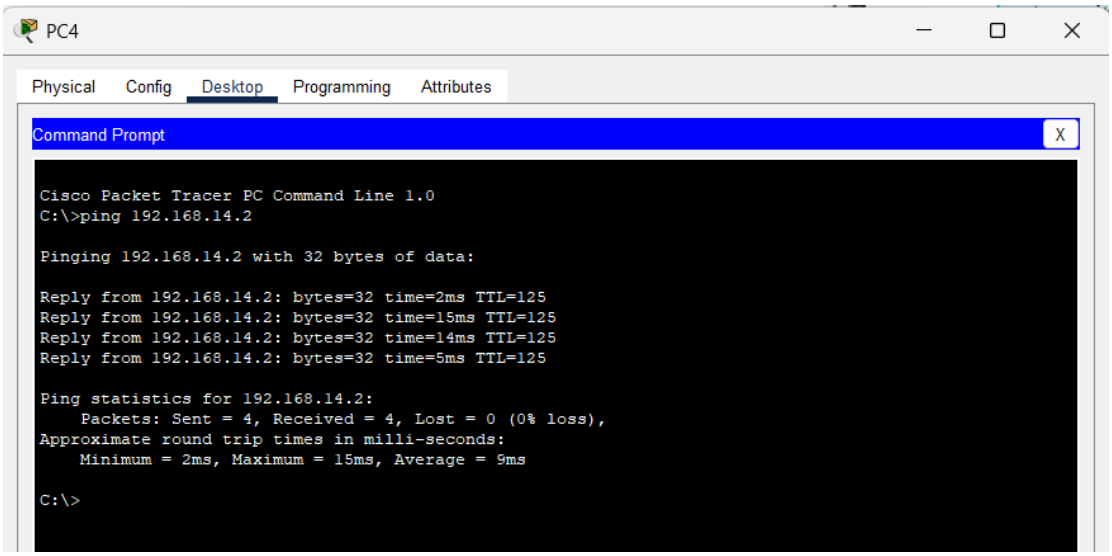

Figura 2.1: Evidencia del `ping` exitoso desde PC4 (antes de aplicar la ACL).

2.3 Configuración de la ACL estándar (Router R4)

En Cisco IOS, las ACL estándar se numeran típicamente entre **1–99** o **1300–1999**. En este laboratorio se usa la ACL **10**.

2.3.1 Crear reglas (deny/permit)

En el router **R4**, ingrese:

```
R4(config)# access-list 10 deny 192.168.14.0 0.0.0.63
R4(config)# access-list 10 permit any
```

Nota Importante

La máscara **0.0.0.63** corresponde a un bloque de **64 direcciones** (típicamente /26). Ajuste el origen y wildcard según la red que su práctica requiera.

2.3.2 Aplicar ACL a la interfaz

Luego aplique la ACL en la interfaz indicada (en este caso **FastEthernet0/1**) y en la dirección correspondiente (**out**):

```
R4(config)# interface f0/1
R4(config-if)# ip access-group 10 out
```

2.4 Prueba posterior (después de ACL)

Repita la prueba con `ping` hacia **192.168.14.2**. Si la ACL se aplicó correctamente, se observará **tiempo de espera agotado** y **100 % perdidos**.

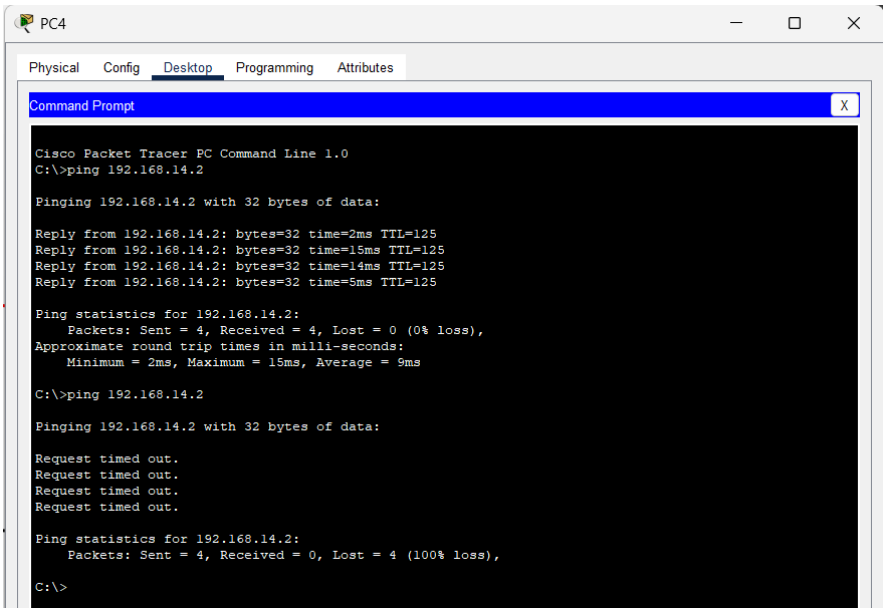

Figura 2.2: Evidencia de `ping` fallido (después de aplicar la ACL): tiempo de espera agotado y 100 % de pérdida.

2.5 Verificación en el router (Cisco Packet Tracer)

Use `show access-lists` para observar la lista y sus contadores:

```
R4# show access-lists
Standard IP access list 10
 10 deny   192.168.14.0, wildcard bits 0.0.0.63
 20 permit any
```

Evidencia solicitada

Tome una captura de pantalla del resultado de `show access-lists` como evidencia de verificación en el router (Cisoc Packet Tracer). Asegúrese de que en la imagen se observen claramente las líneas `deny` y `permit`, junto con sus coincidencias (matches).

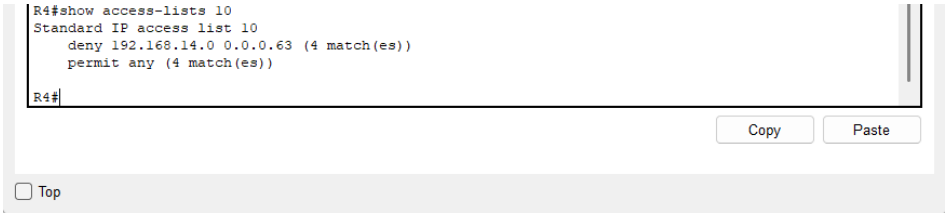

Figura 2.3: Evidencia de verificación con `show access-lists` en ACL estándar.

Interpretación

El número de **matches** indica cuántos paquetes coincidieron con cada línea. Si el `ping` fue bloqueado, la línea `deny` aumentará sus coincidencias.

3

Unidad 3: ACL extendida (filtrado por protocolo y puerto)

3.1 Objetivo de la unidad

Implementar una **ACL extendida** que bloquee **HTTP (TCP/80)** desde un host cliente específico hacia un servidor web, manteniendo permitido el resto del tráfico.

En esta práctica se agregó un servidor en **Cisco Packet Tracer** para realizar las pruebas del servicio web.

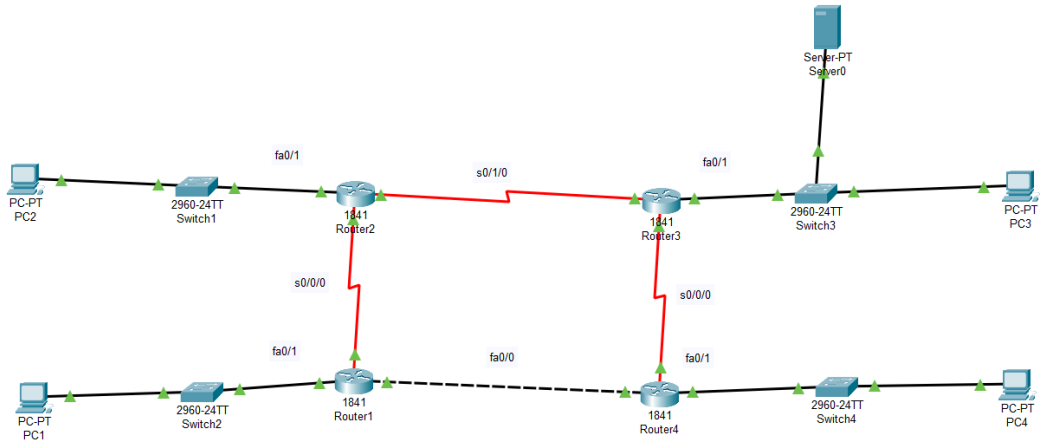

Figura 3.1: Servidor agregado en Cisco Packet Tracer para las pruebas de ACL extendida.

3.2 Escenario: servidor web (Server PT)

En la red de prueba se utiliza un servidor de **Cisco Packet Tracer (Server PT)** para publicar el servicio HTTP. Para esta práctica, se **modificó la IP del servidor a** `192.168.13.130`.

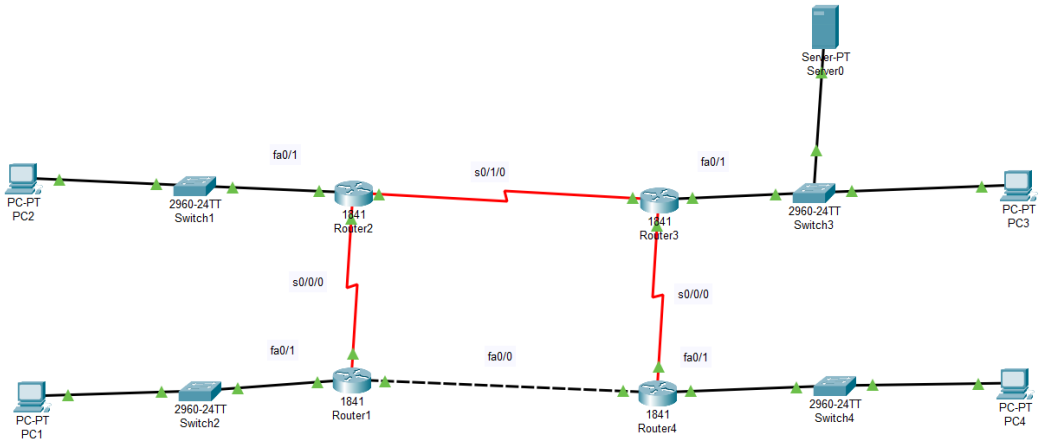

Figura 3.2: Configuración del Server PT en Packet Tracer con IP `192.168.13.130`.

Para el caso de referencia:

- **Cliente bloqueado:** `192.168.13.2`
- **Servidor web:** `192.168.13.130`

3.3 Prueba inicial (antes de ACL)

Antes de aplicar la ACL, confirme que el cliente puede alcanzar al servidor:

- `ping 192.168.13.130` debe responder.
- En el navegador, acceder a `http://192.168.13.130` debe cargar el sitio.

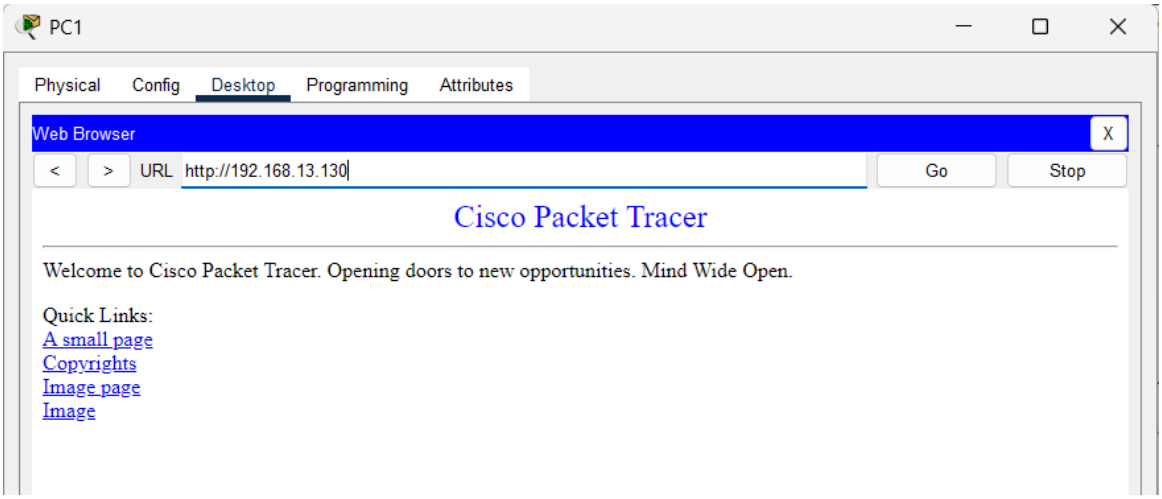

Figura 3.3: Prueba inicial: acceso HTTP exitoso antes de aplicar la ACL.

3.4 Crear la ACL extendida (Router R1)

Las ACL extendidas pueden numerarse típicamente entre **100–199** o **2000–2699**. En este laboratorio se usa la **101**.

3.4.1 Reglas de filtrado

En **R1**, configure:

```
R1(config)# access-list 101 deny tcp host 192.168.13.2 host
   192.168.13.130 eq 80
R1(config)# access-list 101 permit ip any any
```

Nota Importante

La línea `permit ip any any` es necesaria para evitar que el **deny implícito** bloquee todo el tráfico no especificado.

3.4.2 Aplicación de la ACL en la interfaz

Aplique la ACL en la interfaz indicada (en el caso de referencia **FastEthernet0/1**) y en dirección **in**:

```
R1(config)# interface f0/1
R1(config-if)# ip access-group 101 in
```

3.5 Prueba posterior: HTTP bloqueado

Con la ACL aplicada:

- El `ping` puede seguir respondiendo (depende de la política aplicada).
- El acceso HTTP desde `192.168.13.2` hacia `192.168.13.130` debe fallar.

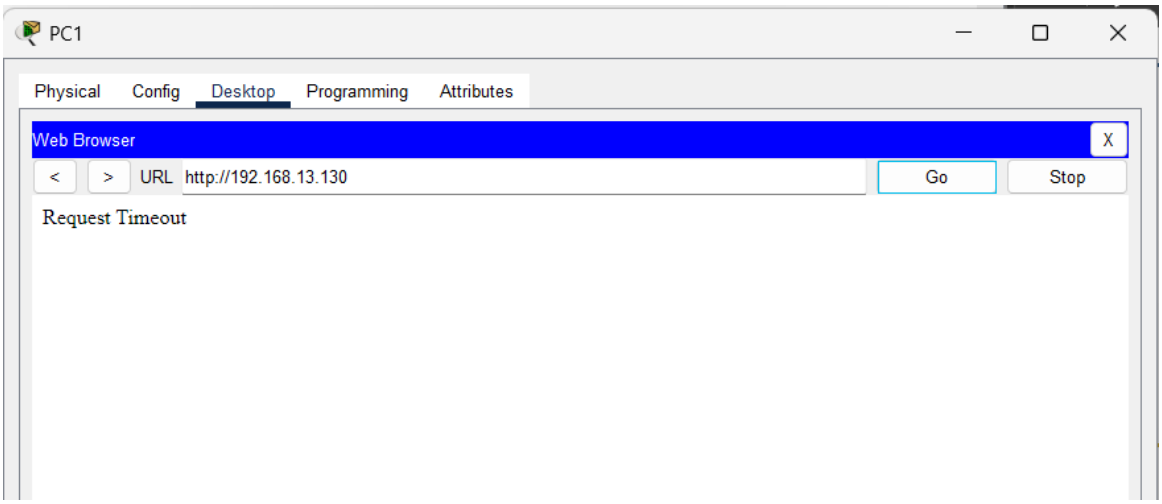

Figura 3.4: Evidencia de HTTP bloqueado (el navegador no obtiene respuesta).

3.6 Comprobación con otra IP (permitido)

Cambie el cliente a otra IP dentro de la misma red (por ejemplo `192.168.13.3`) y repita el acceso HTTP. En el escenario de referencia, el sitio vuelve a ser accesible desde la IP permitida.

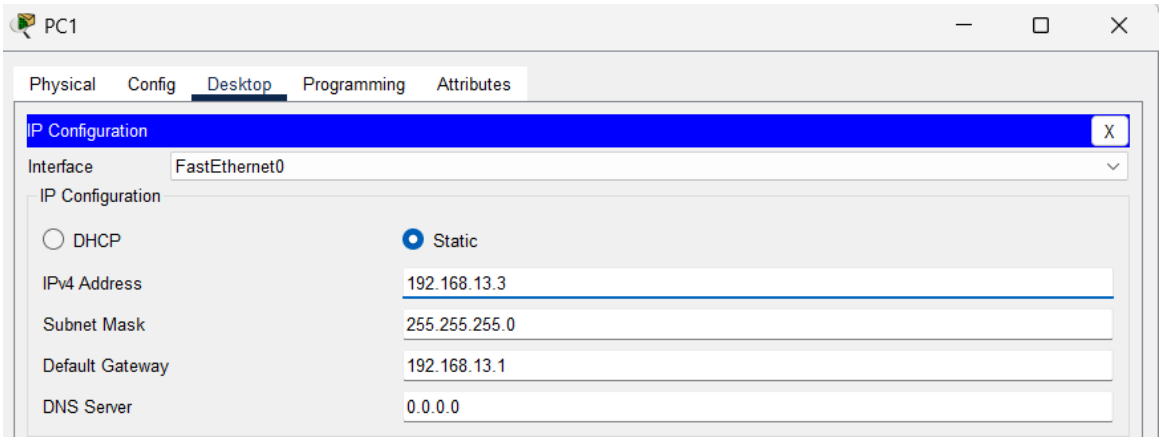

Figura 3.5: Evidencia del cambio de IP del cliente para validar acceso permitido.

Breve descripción: al cambiar la IP del cliente a `192.168.13.3`, el acceso HTTP vuelve a permitirse porque la regla `deny` estaba aplicada solo al host `192.168.13.2`.

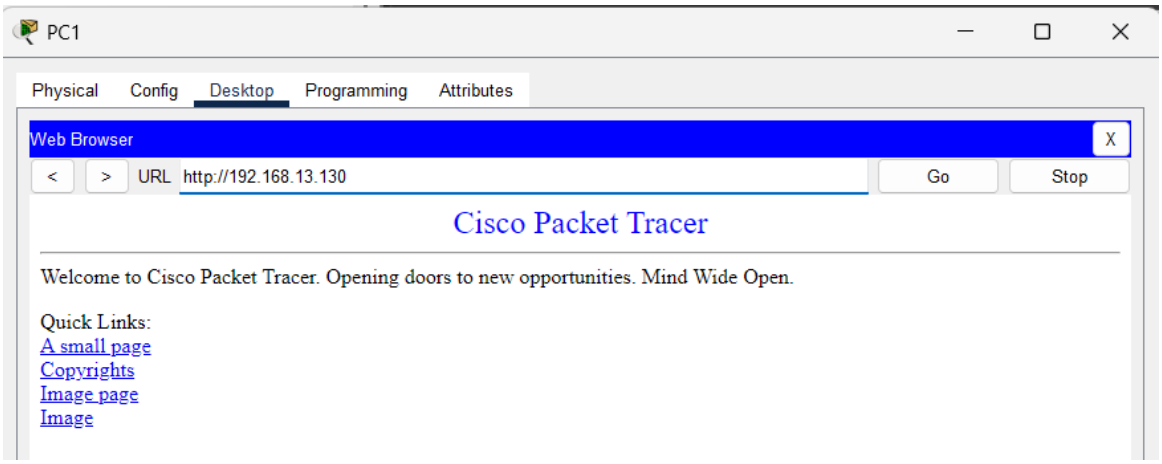

Figura 3.6: Evidencia: el sitio vuelve a ser accesible después del cambio de IP del cliente.

3.7 Verificación en el router

Use `show access-lists` para validar las líneas y observar los contadores de coincidencia:

```
R1# show access-lists
Extended IP access list 101
 10 deny tcp host 192.168.13.2 host 192.168.13.130 eq www
 20 permit ip any any
```

Evidencia solicitada

Tome una captura de pantalla del resultado de `show access-lists` como evidencia de la verificación de ACL extendida. Asegúrese de que en la imagen se observen claramente las líneas `deny` y `permit`, junto con sus coincidencias (matches).

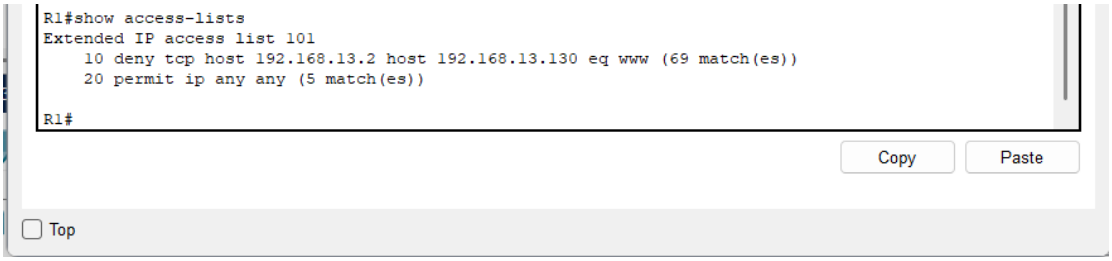

Figura 3.7: Evidencia de verificación con `show access-lists` para ACL extendida.

4

Unidad 4: Pruebas, verificación y entrega

4.1 Checklist de verificación

Complete la siguiente lista para asegurar que la práctica quedó funcional:

1. **Antes de ACL:** `ping` exitoso entre el origen y el destino del caso.
2. **ACL estándar:**
   - ACL creada con `deny` + `permit any`.
   - ACL aplicada en interfaz correcta con `ip access-group <num> in|out`.
   - `show access-lists` muestra contadores aumentando en la línea `deny`.
3. **ACL extendida (HTTP):**
   - ACL 101 creada con `deny tcp host <cliente> host <servidor> eq 80`.
   - `permit ip any any` presente.
   - HTTP bloqueado para el host indicado y permitido para otra IP.

4.2 Evidencias mínimas para entregar

Resultados esperados

1. Captura o transcripción de `show access-lists` en R4 (ACL 10) y en R1 (ACL 101).
2. Captura de `ping` **antes** y **después** del ACL estándar.
3. Captura del navegador mostrando **HTTP bloqueado** desde la IP restringida.
4. Captura del navegador mostrando **HTTP permitido** desde una IP distinta.

4.3 Actividades propuestas

1. Modifique la ACL extendida para bloquear también **HTTPS (443)** y compruebe el efecto.
2. Cambie la ACL estándar para bloquear una subred diferente (use wildcard correcto).