UCUENCA

UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

COMPUTACIÓN

Práctica 13 - Listas de Control de Acceso

Integrantes:

Ledesma Fabián

Macas Kelly

Mendoza Bryan

Quizhpi Luis

Romero David

Asignatura: Redes de Computadoras

Docente: Ing. Raúl Ortiz, Ing. Andrea Mory

Fecha de entrega: 15/07/2025

Jefe de laboratorio	Ing. Raúl Ortiz Gaona PhD
Técnico de Laboratorio	Ing. Andrea Mory
Práctica # 13	Listas de Control de Acceso

1. ANTECEDENTES

Muchas veces se necesita negar a permitir el acceso a ciertos recursos que existen en una red. Una forma de hacerlo es utilizando listas de control de acceso ACL (Access Control List).

2. OBJETIVOS

El objetivo de la práctica es el siguiente:
1. Impedir que una red tenga acceso a otra red.

3. EQUIPO Y MATERIALES

2 ruteadores
2 switches
4 PCs
9 cables directos
1 cable cruzado
1 cable de consola

4. DISEÑO DE LA RED CON MÁSCARA DE SUBRED DE LONGITUD FIJA

Datos:
Se desea que la red con dirección 192.168.0.0 no pueda acceder a la red con dirección 172.16.0.0, y que la red con dirección 192.168.1.0 sí pueda acceder a la red 172.16.0.0

5. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS

1. Conectar los equipos como se indica en la Figura 1.
2. Configurar las PCs.
3. Configurar las interfaces de red de los enrutadores.
4. Configurar enrutamiento dinámico RIP en los enrutadores
5. Impedir que la red 192.168.0.0 no pued acceder a la red 172.16.0.0
   Router(config)# access-list 101 deny ip 192.168.0.0 0.0.0.255 172.16.0.0 0.0.0.0
   Router(config)# interface gigabitEthernet 0/0
   Router(config-if)# ip access-group 101 out
6. Comprobar conectividad
7. Permitir que la red 192.168.1.0 sí pueda acceder a la red 172.16.0.0

Router(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.0.0 0.0.255.255

8. Volver a probar la conectividad

Luego, los estudiantes configurarán NAT con dos redes LAN conectadas al enrutador R1, con direcciones de red privadas clase A y B respectivamente.

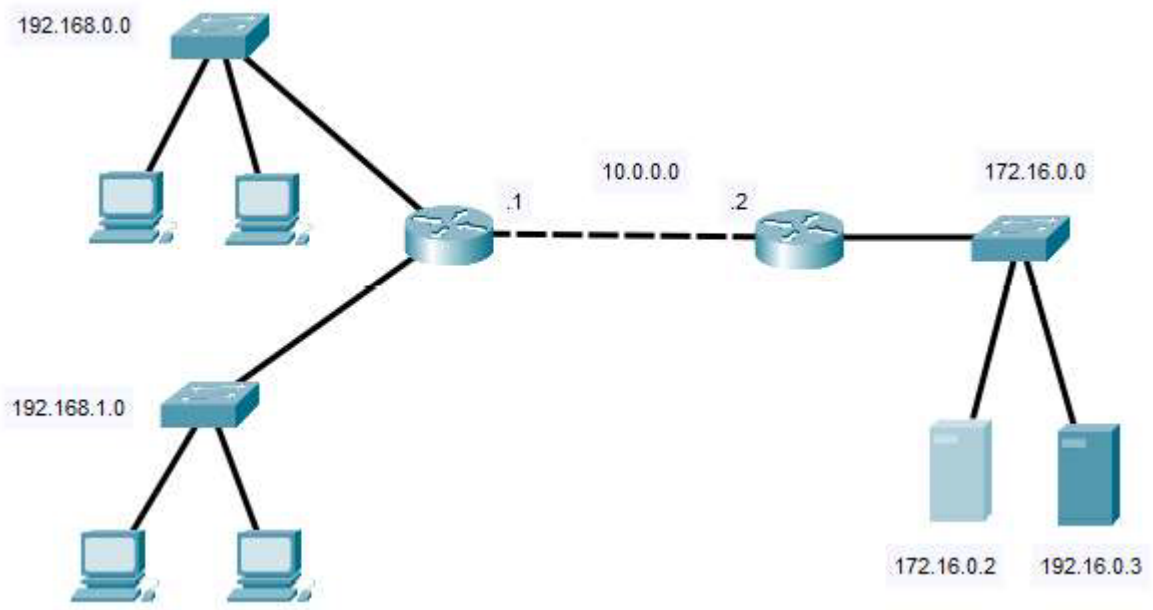

Figura 1. Topología de red

6. RESULTADOS OBTENIDOS

Esta práctica se realizó únicamente en el software Cisco Packet Tracer.

Primero, se armó la topología de la Figura 1, para posteriormente, configurar las interfaces de red de los router, mediante los siguientes comandos:

Primer router

- Configuración de la 1ra interfaz - switch
  Router>enable
  Router#configure terminal
  Router(config)#interface g 0/0
  Router(config-if)#ip address 192.168.0.1 255.255.255.0
  Router(config-if)#no shutdown
  Router(config-if)#exit
- Configuración de la 2da interfaz - switch
  Router(config)#interface g 0/1
  Router(config-if)#ip address 192.168.1.1 255.255.255.0
  Router(config-if)#no shutdown
  Router(config-if)#exit
- Configuración de la 3ra interfaz - router
  Router(config)#interface g 0/2

```
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Segundo router

- Configuración de la 1ra interfaz - switch

```
Router>enable
Router#configure terminal
Router(config)#interface g 0/0
Router(config-if)#ip address  10.0.0.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

- Configuración de la 2da interfaz - switch

```
Router(config)#interface g 0/1
Router(config-if)#ip address 172.16.0.1 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

A continuación, se configuró el enrutamiento de los router, mediante los siguientes comandos:

Primer router

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#network 10.0.0.0
Router(config-router)#exit
```

Segundo router

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 172.16.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#exit
```

Por último, y como parte principal de la práctica, se configuró la lista de control de acceso, donde se busca impedir que la red 192.168.0.0 no pueda acceder a la red 172.16.0.0. Se lo realizó mediante los siguientes comandos:

```
Router(config)#access-list 101 deny ip 192.168.0.0 0.0.0.255 172.16.0.0 0.0.0.0
Router(config)#interface g 0/2
Router(config-if)#ip access-group 101 out
Router(config-if)#exit.
Router(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.0.0 0.0.255.255
```

A continuación, se realizó la configuración de las IP's respectivas por cada una de las computadoras y servidores.

- Computadoras correspondientes a la red 192.168.0.0

  IP: 192.168.0.2
  Máscara: 255.255.255.0
  Gateway: 192.168.0.1

  IP: 192.168.0.3
  Máscara: 255.255.255.0
  Gateway: 192.168.0.1

- Computadoras correspondientes a la red 192.168.1.0

  IP: 192.168.1.2
  Máscara: 255.255.255.0
  Gateway: 192.168.0.1

  IP: 192.168.1.3
  Máscara: 255.255.255.0
  Gateway: 192.168.0.1

- Servidores correspondientes a la red 172.16.0.0

  IP: 172.16.0.2
  Máscara: 255.255.0.0
  Gateway: 172.16.0.1

  IP: 172.16.0.3
  Máscara: 255.255.0.0
  Gateway: 172.16.0.1

Para verificar las conexiones y configuraciones realizadas se realizó un ping entre las computadoras de la misma red, para las 3 redes existentes en la topología, los resultados se pueden verificar en las Figuras 2, 3 y 4.

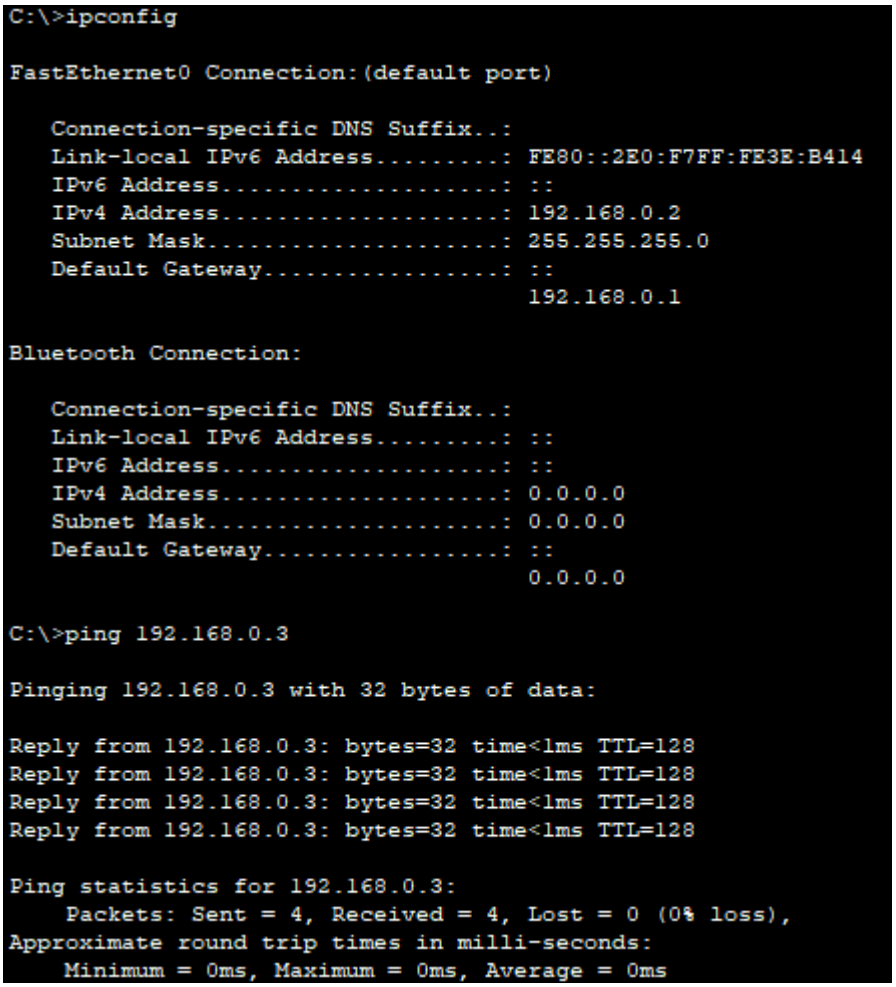

Figura 2. Comprobación de la conexión entre host de la red 192.168.0.0

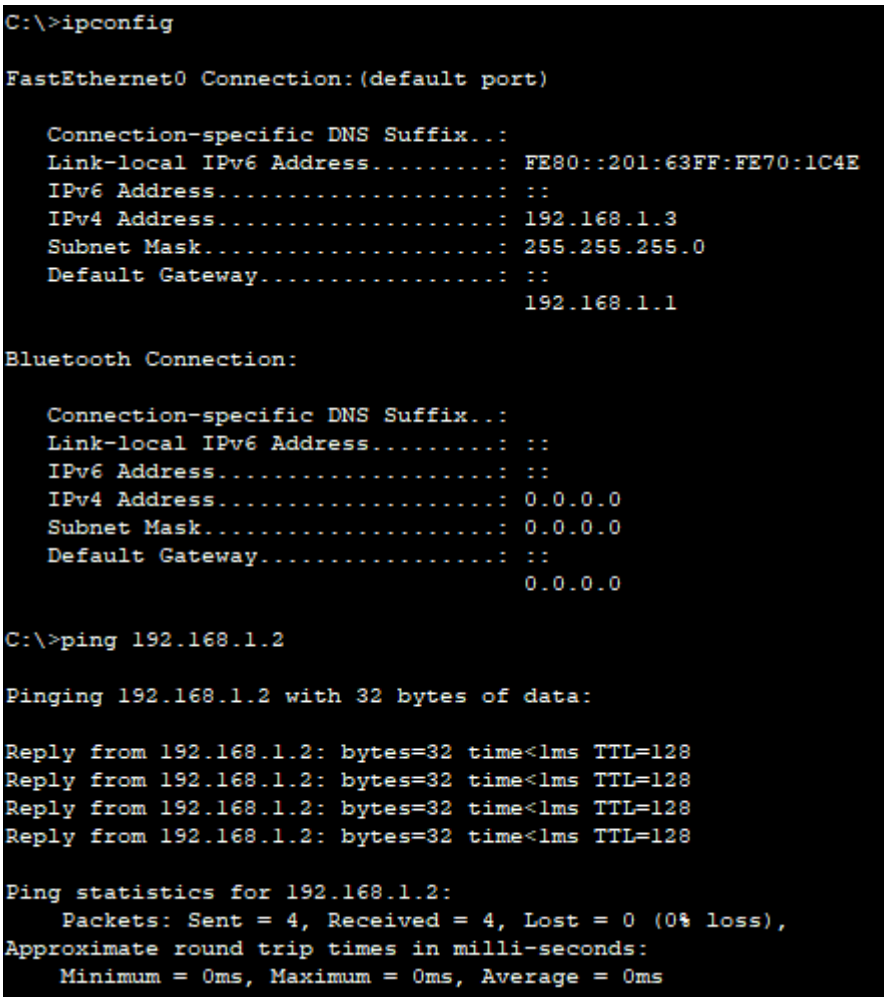

Figura 3. Comprobación de la conexión entre host de la red 192.168.1.0

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:42FF:FE9A:900B
   IPv6 Address.....: ::
   IPv4 Address.....: 172.16.0.2
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 172.16.0.1

C:\>ping 172.16.0.3

Pinging 172.16.0.3 with 32 bytes of data:

Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 4. Comprobación de la conexión entre host de la red 172.16.0.0

Finalmente, se realizó un ping para comprobar la conexión entre las redes que tienen permitido la comunicación, es decir, la red 172.16.0.0 con la red 192.168.1.0. En la Figura 5 se aprecia como la conexión es exitosa entre el host 192.168.1.3 con el servidor 172.16.0.2.

De igual forma, se comprobó, si efectivamente la configuración del control de lista de acceso fue exitosa, realizando un ping entre el host 192.168.0.2 con el servidor 172.16.0.3. En la Figura 6 se comprueba como el ping no tuvo éxito, es decir la red 192.168.0.0 no puede acceder a la red 172.16.0.0.

```
C:\>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time<1ms TTL=126
Reply from 172.16.0.2: bytes=32 time<1ms TTL=126
Reply from 172.16.0.2: bytes=32 time<1ms TTL=126
Reply from 172.16.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 5. Comprobación de la conexión entre la red 192.168.1.0 con la red 172.16.1.0

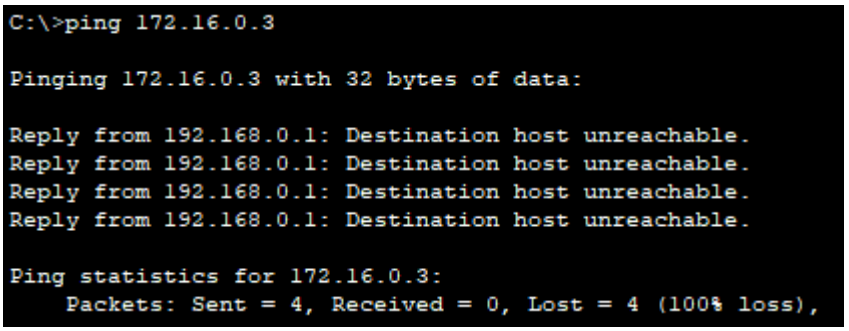

Figura 4. Comprobación de la conexión entre la red 192.168.1.0 con la red 172.16.0.0

7. CONCLUSIONES

- Se completó la práctica logrando el objetivo de impedir que una red específica acceda a contra red mientras se permite el acceso desde una tercera red.
- El software Cisco Packet Tracer demostró ser una herramienta útil para simular redes y probar configuraciones de seguridad sin necesidad de equipos físicos.
- La práctica ayudó a entender cómo aplicar políticas de seguridad en redes empresariales donde es necesario restringir el acceso a ciertos recursos.

8. RECOMENDACIONES

- Antes de configurar las listas de acceso, es importante planificar qué redes deben comunicarse y cuáles no, para evitar bloquear comunicaciones necesarias.
- Mantener un registro de todas las configuraciones realizadas para poder revisar o modificar las reglas más adelante.
- Siempre comprobar que las redes que sí deben comunicarse puedan hacerlo después de aplicar las restricciones.

9. FUENTES DE INFORMACIÓN