Cajiga Gutiérrez Edgar Uriel
Zepeda Flores Alejandro de Jesús

Packet Tracer: resolución de problemas de las ACL

Topología

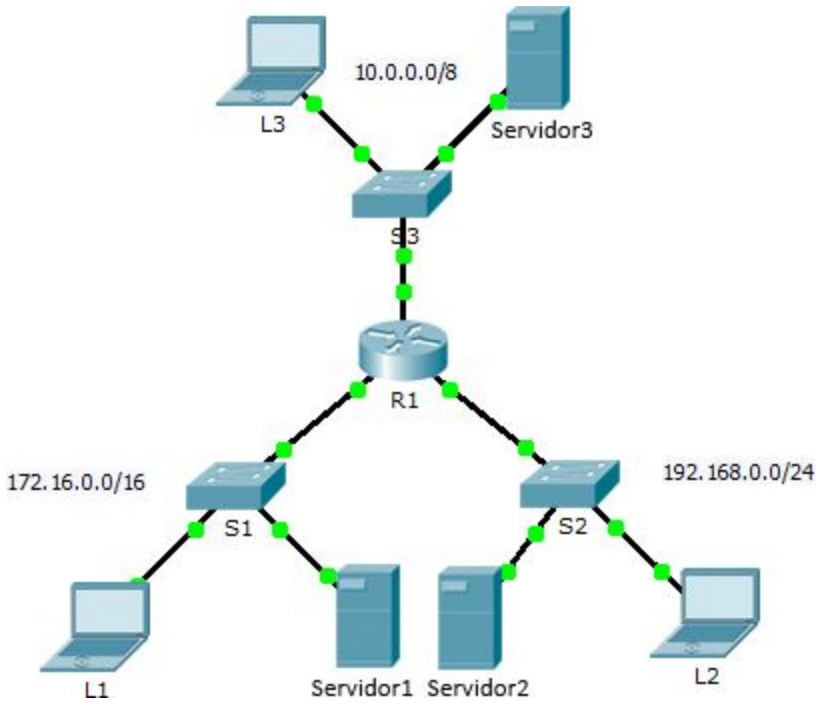


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
	G0/0	10.0.0.1	255.0.0.0	N/A
R1	G0/1	172.16.0.1	255.255.0.0	N/A
	G0/2	192.168.0.1	255.255.255.0	N/A
Server1	NIC	172.16.255.254	255.255.0.0	172.16.0.1
Server2	NIC	192.168.0.254	255.255.255.0	192.168.0.1
Server3	NIC	10.255.255.254	255.0.0.0	10.0.0.1
L1	NIC	172.16.0.2	255.255.0.0	172.16.0.1
L2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
L3	NIC	10.0.0.2	255.0.0.0	10.0.0.1

Cajiga Gutiérrez Edgar Uriel
Zepeda Flores Alejandro de Jesús

Packet Tracer: resolución de problemas de ACL

Objetivos

Parte 1: resolver el problema 1 de la ACL
Parte 2: resolver el problema 2 de la ACL
Parte 3: resolver el problema 3 de la ACL

Situación

En esta red, deberían estar implementadas las tres políticas siguientes:

- Los hosts de la red 192.168.0.0/24 no pueden acceder a ningún servicio TCP del Servidor 3.
- Los hosts de la red 10.0.0.0/8 no pueden acceder al servicio HTTP del Servidor 1.
- Los hosts de la red 172.16.0.0/16 no pueden acceder al servicio FTP del Servidor 2.

Nota: todos los nombres de usuario y las contraseñas del FTP son “cisco”. No debe haber otras restricciones. Lamentablemente, las reglas implementadas no funcionan de manera correcta. Su tarea es buscar y corregir los errores relacionados con las listas de acceso en el R1.

Parte 1: resolver el problema 1 de la ACL

Los hosts de la red 192.168.0.0/24 no pueden acceder (intencionalmente) a ningún servicio TCP del Servidor 3, pero no deberían tener ningún tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

1) Con la L2, intente acceder a los servicios FTP y HTTP de Servidor1, Servidor2, y Servidor3.
2) Desde la L2, haga ping a Servidor1, Servidor2 y Servidor3.
3) Desde la L2, haga ping a G0/2 del R1.
4) Vea la configuración en ejecución en el R1. Examine la lista de acceso 192_to_10 y su ubicación en las interfaces. ¿La lista de acceso se colocó en la interfaz apropiada y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?
5) Realice otras pruebas, según sea necesario.

```
ip access-list extended 192_to_10
 deny tcp 192.168.0.0 0.0.0.255 host 10.255.255.254
```

Paso 2: implementar una solución.

Realice un ajuste a la lista de acceso 192_to_10 para solucionar el problema.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list extended 192_to_10
R1(config-ext-nacl)#20 permit ip any any
R1(config-ext-nacl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
ip access-list extended 192_to_10
 deny tcp 192.168.0.0 0.0.0.255 host 10.255.255.254
 permit ip any any
```

Packet Tracer: resolución de problemas de ACL

Parte 2: resolver el problema 2 de la ACL

Los hosts de la red 10.0.0.0/8 no pueden acceder (intencionalmente) al servicio HTTP del Servidor 1, pero no deberían tener ningún tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

1) Con la L3, intente acceder a los servicios FTP y HTTP de Servidor 1, Servidor 2, y Servidor 3.
2) Desde la L3, haga ping a Servidor1, Servidor2 y Servidor3.
3) Vea la configuración en ejecución en el R1. Examine la lista de acceso 10_to_172 y su ubicación en las interfaces. ¿La lista de acceso se colocó en la interfaz apropiada y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?
4) Realice otras pruebas, según sea necesario.

```
ip access-list extended 10_to_172
 deny tcp 10.0.0.0 0.255.255.255 host 172.16.255.254 eq www
 permit ip any any
```

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip access-group 10_to_172 out
 duplex auto
 speed auto
```

Paso 2: implementar una solución.

Realice un ajuste a la lista de acceso 10_to_172 para solucionar el problema.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/0
R1(config-if)#no ip access-group 10_to_192 out
R1(config-if)#ip access-group 10_to_192 in
R1(config-if)#no ip access-group 10_to_172 out
R1(config-if)#ip access-group 10_to_172 in
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip access-group 10_to_172 in
 duplex auto
 speed auto
```


Packet Tracer: resolución de problemas de ACL

Parte 3: resolver el problema 3 de la ACL

Los hosts de la red 172.16.0.0/16 no pueden acceder (intencionalmente) al servicio FTP del Servidor 2, pero no deberían tener ningún tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

1) Con la L1, intente acceder a los servicios FTP y HTTP de Servidor 1, Servidor 2, y Servidor 3.
2) Desde la L1, haga ping a Servidor1, Servidor2 y Servidor3.
3) Vea la configuración en ejecución en el R1. Examine la lista de acceso 172_to_192 y su ubicación en las interfaces. ¿La lista de acceso se colocó en el puerto apropiado y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?
4) Realice otras pruebas, según sea necesario.

```
ip access-list extended 172_to_192
 permit ip any any
 deny tcp 172.16.0.0 0.0.255.255 host 192.168.0.254 eq ftp
```

Paso 2: implementar una solución.

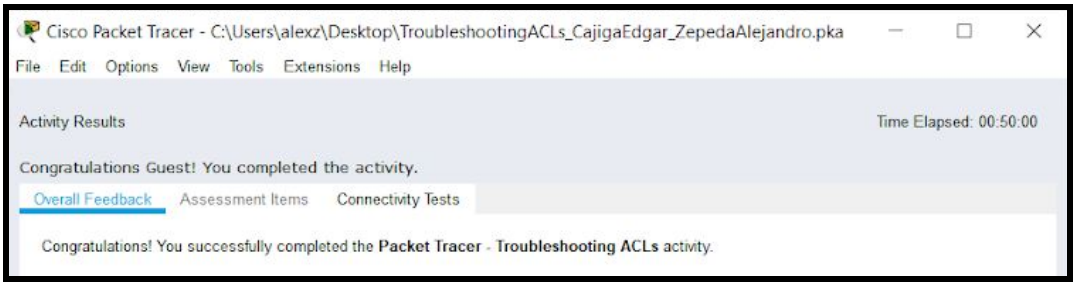
Realice un ajuste a la lista de acceso 172_to_192 para solucionar el problema.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list extended 172_to_192
R1(config-ext-nacl)#no 10
R1(config-ext-nacl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list extended 172_to_192
R1(config-ext-nacl)#30 permit ip any any
R1(config-ext-nacl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Packet Tracer: resolución de problemas de ACL

Resultados



Ping de L1 a S1, S2 y S3

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time<1ms TTL=128
Reply from 172.16.255.254: bytes=32 time<1ms TTL=128
Reply from 172.16.255.254: bytes=32 time<1ms TTL=128
Reply from 172.16.255.254: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time=1ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127
Reply from 192.168.0.254: bytes=32 time=3ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

```
Pinging 10.255.255.254 with 32 bytes of data:

Reply from 10.255.255.254: bytes=32 time=1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127

Ping statistics for 10.255.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Packet Tracer: resolución de problemas de ACL

Ping de L2 a S1, S2 y S3

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time=1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time=3ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Pinging 10.255.255.254 with 32 bytes of data:

Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127

Ping statistics for 10.255.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping de L3 a S1, S2 y S3

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time=1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Packet Tracer: resolución de problemas de ACL

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time=1ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 10.255.255.254

Pinging 10.255.255.254 with 32 bytes of data:

Reply from 10.255.255.254: bytes=32 time=1ms TTL=128
Reply from 10.255.255.254: bytes=32 time=3ms TTL=128
Reply from 10.255.255.254: bytes=32 time<1ms TTL=128
Reply from 10.255.255.254: bytes=32 time<1ms TTL=128

Ping statistics for 10.255.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Conclusiones

- ### Edgar Uriel Cajiga Gutiérrez

  Con esta práctica, pudimos aprender como realizar diferentes configuraciones de permisos de servicios para los diferentes Routers de una topología dada, notamos que se debe tomar en cuenta el orden y la forma de denegar un permiso ya que en esto radica si el problema planteado será solucionado o no. Otra cosa que pudimos reforzar a lo largo de esta práctica fue analizar las tablas de las ACL, en estas pudimos detectar en qué sentido se encuentran y determinar si se encuentran configuradas correctamente o es necesario hacer algún cambio.

- ### Alejandro de Jesús Zepeda Flores

  Al dar solución a esta práctica, se reforzaron los temas vistos en clase permitiendo aplicar una correcta configuración a las ACL.Por otro lado pudimos notar la importancia de mantener un buen orden al aplicar las configuraciones, ya que de estas dependerá que la tarea se cumple de una forma correcta. También aprendimos cuál es el proceso para eliminar una ACL y como reemplazar esta con una nueva, además de comprobar que la configuración fue aplicada exitosamente al hacer uso de las PC's para intentar acceder a los servicios que fueron bloqueados por las listas.

