

Packet Tracer: configuración de ACL extendidas, situación 1

Topología

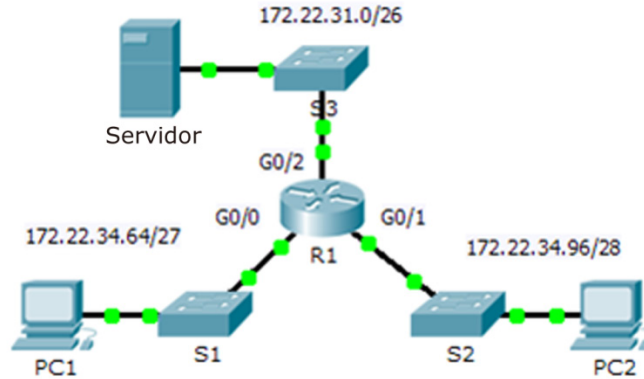


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.22.34.65	255.255.255.224	N/D
	G0/1	172.22.34.97	255.255.255.240	N/D
	G0/2	172.22.34.1	255.255.255.192	N/D
Servidor	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Objetivos

Parte 1: configurar, aplicar y verificar una ACL extendida numerada

Parte 2: configurar, aplicar y verificar una ACL extendida con nombre

Aspectos básicos/situación

Dos empleados necesitan acceder a los servicios que proporciona el servidor. La **PC1** solo necesita acceso FTP, mientras que la **PC2** solo necesita acceso web. Ambas computadoras pueden hacer ping al servidor, pero no entre sí.

Parte 1: configurar, aplicar y verificar una ACL extendida numerada

Paso 1: configurar una ACL para que permita tráfico FTP e ICMP.

- Desde el modo de configuración global en el **R1**, introduzca el siguiente comando para determinar el primer número válido para una lista de acceso extendida.

```
R1 (config)# access-list ?
  <1-99>      IP standard access list
  <100-199>  IP extended access list
```

- b. Agregue **100** al comando, seguido de un signo de interrogación.

```
R1(config)# access-list 100 ?  
deny    Specify packets to reject  
permit  Specify packets to forward  
remark  Access list entry comment
```

- c. Para permitir el tráfico FTP, introduzca **permit**, seguido de un signo de interrogación.

```
R1(config)# access-list 100 permit ?  
ahp     Authentication Header Protocol  
eigrp   Cisco's EIGRP routing protocol  
esp     Encapsulation Security Payload  
gre     Cisco's GRE tunneling  
icmp    Internet Control Message Protocol  
ip      Any Internet Protocol  
ospf    OSPF routing protocol  
tcp     Transmission Control Protocol  
udp     User Datagram Protocol
```

- d. Esta ACL permite tráfico FTP e ICMP. ICMP se indica más arriba, pero FTP no, porque FTP utiliza TCP. Entonces, se introduce TCP. Introduzca **tcp** para refinar aún más la ayuda de la ACL.

```
R1(config)# access-list 100 permit tcp ?  
A.B.C.D Source address  
any      Any source host  
host     A single source host
```

- e. Observe que se podría filtrar por **PC1** por medio de la palabra clave **host** o bien se podría permitir cualquier (**any**) host. En este caso, se permite cualquier dispositivo que tenga una dirección que pertenezca a la red 172.22.34.64/27. Introduzca la dirección de red, seguida de un signo de interrogación.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?  
A.B.C.D Source wildcard bits
```

- f. Para calcular la máscara wildcard, determine el número binario opuesto a una máscara de subred.

```
11111111.11111111.11111111.111 = 00000 255.255.255.224  
00000000.00000000.00000000.000 = 11111 0.0.0.31
```

- g. Introduzca la máscara wildcard, seguida de un signo de interrogación.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?  
A.B.C.D Destination address  
any      Any destination host  
eq       Match only packets on a given port number  
gt       Match only packets with a greater port number  
host     A single destination host  
lt       Match only packets with a lower port number  
neq     Match only packets not on a given port number  
range    Match only packets in the range of port numbers
```

- h. Configure la dirección de destino. En esta situación, se filtra el tráfico hacia un único destino: el servidor. Introduzca la palabra clave **host** seguida de la dirección IP del servidor.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host  
172.22.34.62 ?
```

```
dscp      Match packets with given dscp value
eq        Match only packets on a given port number
established established
gt        Match only packets with a greater port number
lt        Match only packets with a lower port number
neq       Match only packets not on a given port number
precedence Match packets with given precedence value
range     Match only packets in the range of port numbers
<cr>
```

- i. Observe que una de las opciones es **<cr>** (retorno de carro). Es decir, puede presionar la tecla **Enter**, y la instrucción permitiría todo el tráfico TCP. Sin embargo, solo se permite el tráfico FTP. Por lo tanto, introduzca la palabra clave **eq**, seguida de un signo de interrogación para mostrar las opciones disponibles. Luego, introduzca **ftp** y presione la tecla **Enter**.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
```

```
<0-65535> Port number
ftp        File Transfer Protocol (21)
pop3       Post Office Protocol v3 (110)
smtp       Simple Mail Transport Protocol (25)
telnet     Telnet (23)
www        World Wide Web (HTTP, 80)
```

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

- j. Cree una segunda instrucción de lista de acceso para permitir el tráfico ICMP (ping, etcétera) desde la **PC1** al **Servidor**. Observe que el número de la lista de acceso es el mismo y que no es necesario detallar un tipo específico de tráfico ICMP.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

- k. El resto del tráfico se deniega de manera predeterminada.

Paso 2: aplicar la ACL a la interfaz correcta para filtrar el tráfico.

Desde la perspectiva del **R1**, el tráfico al cual se aplica la ACL 100 ingresa desde la red conectada a la interfaz Gigabit Ethernet 0/0. Ingrese al modo de configuración de interfaz y aplique la ACL.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Paso 3: verificar la implementación de la ACL.

- a. Haga ping de la **PC1** al **Servidor**. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.
- b. Desde la **PC1**, acceda mediante FTP al **Servidor**. Tanto el nombre de usuario como la contraseña son **cisco**.
- ```
PC> ftp 172.22.34.62
```
- c. Salga del servicio FTP del **Servidor**.
- ```
ftp> quit
```
- d. Haga ping de la **PC1** a la **PC2**. El host de destino debe ser inalcanzable, debido a que el tráfico no está permitido de manera explícita.

Parte 2: configurar, aplicar y verificar una ACL extendida con nombre

Paso 1: configurar una ACL para que permita acceso HTTP y tráfico ICMP.

- Las ACL con nombre comienzan con la palabra clave **ip**. Desde el modo de configuración global del **R1**, introduzca el siguiente comando, seguido por un signo de interrogación.

```
R1(config)# ip access-list ?
    extended  Extended Access List
    standard  Standard Access List
```

- Puede configurar ACL estándar y extendidas con nombre. Esta lista de acceso filtra tanto las direcciones IP de origen como de destino, por lo tanto, debe ser extendida. Introduzca **HTTP_ONLY** como nombre. (A los fines de la puntuación de Packet Tracer, el nombre distingue mayúsculas de minúsculas).

```
R1(config)# ip access-list extended HTTP_ONLY
```

- El indicador de comandos cambia. Ahora está en el modo de configuración de ACL extendida con nombre. Todos los dispositivos en la LAN de la **PC2** necesitan acceso TCP. Introduzca la dirección de red, seguida de un signo de interrogación.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 ?
    A.B.C.D  Source wildcard bits
```

- Otra manera de calcular el valor de una wildcard es restar la máscara de subred a 255.255.255.255.

```
    255.255.255.255
  - 255.255.255.240
  -----
  = 0.  0.  0. 15
```

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?
```

- Para finalizar la instrucción, especifique la dirección del servidor como hizo en la parte 1 y filtre el tráfico **www**.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
```

- Cree una segunda instrucción de lista de acceso para permitir el tráfico ICMP (ping, etcétera) desde la **PC2** al **Servidor**. Nota: la petición de entrada se mantiene igual, y no es necesario detallar un tipo específico de tráfico ICMP.

```
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

- El resto del tráfico se deniega de manera predeterminada. Salga del modo de configuración de ACL extendida con nombre.

Paso 2: aplicar la ACL a la interfaz correcta para filtrar el tráfico.

Desde la perspectiva del **R1**, el tráfico al cual se aplica la lista de acceso **HTTP_ONLY** ingresa desde la red conectada a la interfaz Gigabit Ethernet 0/1. Ingrese al modo de configuración de interfaz y aplique la ACL.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Paso 3: verificar la implementación de la ACL.

- Haga ping de la **PC2** al **Servidor**. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.
- Desde la **PC2**, acceda mediante FTP al **Servidor**. La conexión debería fallar.
- Abra el navegador web en **PC2** e introduzca la dirección IP de **Server** como URL. La conexión debería establecerse correctamente.