# Packet Tracer: configure y modifique las ACL IPv4 estándar

## Tabla de asignación de direcciones

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
|---|---|---|---|---|
| R1 | G0/0/0 | 192.168.10.1 | 255.255.255.0 | N/D |
| | G0/0/1 | 192.168.20.1 | 255.255.255.0 | |
| | S0/1/0 (DCE) | 10.1.1.1 | 255.255.255.252 | |
| empresarial | S0/1/0 | 10.1.1.2 | 255.255.255.252 | N/D |
| | S0/1/1 (DCE) | 10.2.2.2 | 255.255.255.252 | |
| | S0/2/1 | 209.165.200.225 | 255.255.255.224 | |
| R3 | G0/0/0 | 192.168.30.1 | 255.255.255.0 | N/D |
| | G0/0/1 | 192.168.40.1 | 255.255.255.0 | |
| | /1/1 | 10.2.2.1 | 255.255.255.252 | |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S2 | VLAN 1 | 192.168.20.11 | 255.255.255.0 | 192.168.20.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| S4 | VLAN 1 | 192.168.40.11 | 255.255.255.0 | 192.168.40.1 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-B | NIC | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |
| PC-D | NIC | 192.168.40.3 | 255.255.255.0 | 192.168.40.1 |

## Objetivos

**Parte 1. Verificar la conectividad**

**Parte 2: Configurar y verificar las ACL estándar numeradas y nombradas Parte 3: Modificar una ACL estándar**

## Antecedentes / Escenario

La seguridad de la red y el control del flujo de tráfico son cuestiones importantes al diseñar y administrar redes IP. La capacidad para configurar reglas apropiadas para filtrar los paquetes, sobre la base de las políticas de seguridad establecidas, es una aptitud valiosa.

En este laboratorio, configurará reglas de filtrado para dos ubicaciones comerciales que están representadas por R1 y R3. La administración estableció algunas políticas de acceso entre las redes LAN ubicadas en el R1 y el R3, que usted debe implementar. El router Edge que se encuentra entre R1 y R3 ha sido proporcionado



por el ISP no tendrá ninguna ACL colocada en él. No se le permitiría ningún acceso administrativo al enrutador Edge porque solo puede controlar y administrar su propio equipo.

## Instrucciones Parte 1: Verificar la conectividad

En la parte 1, se comprueba la conectividad entre dispositivos.

**Nota:** Es muy importante probar si la conectividad funciona **antes** de configurar y aplicar listas de acceso. Desea asegurarse de que su red funciona correctamente antes de comenzar a filtrar el tráfico.

Desde PC-A, ping PC-C y PC-D. ¿Tus ping fueron exitosos?aquí. SI

Desde R1, ping PC-C y PC-D. ¿Tus ping fueron exitosos? SI

Desde PC-C, ping PC-A y PC-B. ¿Tus ping fueron exitosos? SI

Desde R3, ping PC-A y PC-B. ¿Tus ping fueron exitosos? SI

¿Todos los equipos pueden hacer ping al servidor en 209.165.200.254? SI, TODAS LAS PC´S HACEN PING

## Parte 2: Configurar y verificar ACL estándar numeradas y con nombre

### Paso 1: Configurar una ACL estándar numerada

Las ACL estándar filtran el tráfico únicamente sobre la base de la dirección IP de origen. Una práctica recomendada típica para las ACL estándar es configurar y aplicar la ACL lo más cerca posible del destino. Para la primera lista de acceso en esta actividad, cree una ACL numerada estándar que permita el tráfico de todos los hosts en la red 192.168.10.0/24 y todos los hosts en la red 192.168.20.0/24 para acceder a todos los hosts en 192.168.30.0/24 red. La política de seguridad también establece que debe existir una **denegación explícita de cualquier entrada de control de acceso (ACE)**, también conocida como una declaración de ACL, al final de todas las ACL.

¿Qué máscara wildcard usaría para permitir que todos los hosts en la red 192.168.10.0/24 accedan a la red 192.168.30.0/24? USARIA 0.0.0.255

Según las mejores prácticas recomendadas por Cisco, ¿en qué router colocaría esta ACL? R3

¿En qué interfaz colocaría esta ACL? ¿En qué sentido la aplicaría? G0/0/0. LA ACL DEBE APLICARSE EN SENTIDO DE SALIDA

a. Configure la ACL en el R3. Use 1 como el número de lista de acceso.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. Aplique la ACL a la interfaz apropiada en el sentido correcto.

```
R3 (config) # interface g0/0/0
R3(config-if)# ip access-group 1 out
```

c. Verifique una ACL numerada.

El uso de varios comandos **show** puede ayudarlo a verificar tanto la sintaxis como la ubicación de sus ACL en su router.

¿Qué comando usaría para ver la lista de acceso 1 en su totalidad, con todas las ACE? DO SHOW ACCESS-LIST O SHOW ACCESS-LIST 1

¿Qué comando usaría para ver dónde se aplicó la lista de acceso y en qué sentido? **SHOW IP INTERFACE G0/0/0 O SHOW IP INTERFACE**

1) En R3, emita el comando **show access-lists 1**.

```
R3# show access-list 1
Standard IP access list 1
    permit 192.168.10.0, wildcard bits 0.0.0.255
permit 192.168.20.0, wildcard bits 0.0.0.255     deny
any
```

2) En R3, emita el comando **show ip interface g0/0/0**.

```
R3# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound access list is not set
<Output omitted>
```

3) Pruebe la ACL para ver si permite que el tráfico de la red 192.168.10.0/24 acceda a la red 192.168.30.0/24.

Desde el símbolo del sistema en la PC-A, haga ping a la dirección IP de la PC-C. ¿Fueron correctos los pings?. SI

4) Pruebe la ACL para ver si permite que el tráfico de la red 192.168.20.0/24 acceda a la red 192.168.30.0/24.

Desde la consola del sistema de la PC-B, haga ping a la dirección IP de la PC-C. ¿Fueron correctos los pings? SI

5) ¿Deben tener éxito los pings de PC-D a PC-C? Ping de PC-D a PC-C para verificar su respuesta.

NO, LOS PINGS NO DEBERÍAN TENER ÉXITO. AL INTENTAR EL PING SE COMPRUEBA QUE LA ACL FUNCIONA SEGÚN LO PREVISTO.

d. Desde la petición de entrada del R1, vuelva a hacer ping a la dirección IP de la PC-C.

```
R1# ping 192.168.30.3
```

¿El ping se realizó correctamente? Explique. NO, LOS PING FALLARON CUANDO HACE PING DESDE EL ROUTER, ESTE USA LA INTERFAZ MÁS CERCANA AL DESTINO COMO LA DIRECCIÓN DE ORIGEN. LA DIRECCIÓN DE ORIGEN DE LOS PINGS ERA 10.1.1.1. LA LISTA DE ACCESO EN EL R3 SOLO PERMITE EL ACCESO DE LAS REDES 192.168.10.0/24 Y 192.168.20.0/24.

e. Emita el comando **show access-lists 1** nuevamente. Tenga en cuenta que el resultado del comando muestra información sobre el número de veces que cada ACE ha coincidido con el tráfico que alcanzó la interfaz Gigabit Ethernet 0/0/0.

```
R3# show access list 1
Standard IP access list 1

    permit 192.168.10.0 0.0.0.255 (4
match(es))     permit 192.168.20.0 0.0.0.255
(4 match(es))     deny any (4 match(es))
```

## Paso 2: Configurar una ACL estándar con nombre

Cree una ACL estándar con nombre que se ajuste a la siguiente política: permitir que el tráfico de todos los hosts en la red 192.168.40.0/24 tenga acceso a todos los hosts en la red 192.168.10.0/24. Además, solo debe permitir el acceso del host PC-C a la red 192.168.10.0/24. El nombre de esta lista de acceso debe ser BRANCH-OFFICE-POLICY.

Según las mejores prácticas recomendadas por Cisco, ¿en qué router colocaría esta ACL? R1

¿En qué interfaz colocaría esta ACL? ¿En qué sentido la aplicaría? G0/0/0. LA ACL DEBE APLICARSE EN SENTIDO DE SALIDA. LOS ESTUDIANTES PUEDEN RESPONDER COLOCANDO LA ACL EN LA INTERFAZ S0/0/0 EN R1 EN LA DIRECCIÓN DE ENTRADA. DESTAQUE QUE ESTO TAMBIÉN IMPEDIRÍA CON EFICACIA QUE TODO EL TRÁFICO DE LAS LAN EN R3 LLEGUEN A LA RED 192.168.20.0/24.

a. Cree la ACL estándar con nombre BRANCH-OFFICE-POLICY en el R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Mira el primer ACE en la lista de acceso. ¿Cuál es otra forma de escribir esto? PERMIT 192.168.30.3 0.0.0.0

b. Aplique la ACL a la interfaz apropiada en el sentido correcto.

```
R1# config t
R1(config)# interface g0/0/0
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c. Verifique una ACL con nombre.

1) En el R1, emita el comando show access-lists.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit host 192.168.30.3
    20 permit 192.168.40.0 0.0.0.255
```

¿Hay alguna diferencia entre esta ACL en R1 y la ACL en R3? Si es así, ¿cuál es? LA INSTRUCCIÓN "DENY ANY" EN EL R1 NO SE MUESTRA DE MANERA EXPLÍCITA, PERO ESTÁ IMPLÍCITA. ES IMPORTANTE ENFATIZAR QUE CONFIGURAR LA DENEGACIÓN DE ACE DE FORMA EXPLÍCITA ES UNA BUENA PRÁCTICA. ESTO AYUDA A RECORDAR Y VISUALIZAR LA DENEGACIÓN IMPLÍCITA EN LA SALIDA DEL COMANDO "SHOW ACCESS-LISTS". NO HACERLO PODRÍA RESULTAR EN LA DENEGACIÓN DE TRÁFICO QUE DEBERÍA HABERSE PERMITIDO. ADEMÁS, CUANDO SE USA UN RECHAZO EXPLÍCITO DE "ANY" ACE, SE PUEDE REGISTRAR Y VERIFICAR EL NÚMERO DE COINCIDENCIAS PARA ESA CONDICIÓN ACE CON "SHOW ACCESS-LISTS".

2) En R1, emita el comando **show ip interface g0/0/0** para verificar que la ACL esté configurada en la interfaz.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set

<Output omitted>
```

Probar la ACL. Desde la consola del sistema en la PC-C, haga ping a la dirección IP de la PC-A. ¿Fueron exitosos los pings? SI

3) Pruebe la ACL para asegurarse de que solo el host PC-C tenga acceso a la red 192.168.10.0/24. Debe hacer un ping extendido y utilizar la dirección G0/0/0 en R3 como su fuente. Haga ping a la dirección IP de la PC-A.

```
R3# ping
Protocol [ip]:
Target IP address: 192.168.10.3 Repeat
count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

```
Extended commands [n]: y Source address
or interface: 192.168.30.1 Type of
service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.1
U.U.U
```

¿Fueron correctos los pings? NO

4) Pruebe la ACL para ver si permite que el tráfico de la red 192.168.40.0/24 acceda a la red 192.168.10.0/24. Desde la consola del sistema de la PC-D, haga ping a la dirección IP de la PC-A.

¿Fueron correctos los pings?

SI

## Parte 3: Modificar una ACL estándar

En el ámbito empresarial, es común que las políticas de seguridad cambien. Por este motivo, quizá sea necesario modificar las ACL. En la Parte 3, cambiará una de las ACL que configuró anteriormente para que coincida con una nueva política de administración que se está implementando.

Intente hacer ping al servidor en 209.165.200.254 desde PC-A. Observe que el ping no se realiza correctamente. La ACL en R1 está bloqueando el tráfico de Internet para que regrese a PC-A. Esto se debe a que la dirección de origen de los paquetes que se devuelven no está en el intervalo de direcciones permitidas.

La gerencia ha decidido que el tráfico que regresa de la red 209.165.200.224/27 debe tener acceso completo a la red 192.168.10.0/24. La administración también quiere que las ACL en todos los enrutadores sigan reglas consistentes. Se debe colocar una ACE **deny any** al final de todas las ACL. Debe modificar la ACL BRANCH-OFFICE-POLICY.

Agregará dos líneas adicionales a esta ACL. Hay dos formas de hacer esto:

**OPCIÓN 1:** Emita un comando **no ip access-list standard BRANCH-OFFICE-POLICY** en el modo de configuración global. Esto eliminaría la ACL del router. Dependiendo del IOS del enrutador, ocurriría uno de los siguientes escenarios: se cancelaría todo el filtrado de paquetes y se permitirían todos los paquetes a través del enrutador; o, debido a que no eliminó el comando **ip access-group** de la interfaz G0 / 1, el filtrado todavía está en su lugar. Independientemente de lo que suceda, una vez que la ACL ya no esté, puede volver a escribir toda la ACL o cortarla y pegarla con un editor de texto.

**OPCIÓN 2**: Puede modificar las ACL en su lugar agregando o eliminando líneas específicas dentro de la propia ACL. Esto puede ser útil, especialmente con las ACL que son largas. Al volver a escribir toda la ACL, o al cortarla y pegarla, se pueden producir errores con facilidad. La modificación de las líneas específicas dentro de la ACL se logra fácilmente.

Para esta actividad, use la Opción 2.

## Paso 1: Modificar una ACL estándar con nombre

a. Desde R1, emita el comando **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0 0.0.0.255 (5 matches)
```

b. Agregue dos líneas adicionales al final de la ACL. En el modo de configuración global, modifique la ACL BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1 (config-std-nacl) # 40 deny any
R1(config-std-nacl)# end
```

c. Verifique la ACL.

1) En el R1, emita el comando **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 209.165.200.224, wildcard bits 0.0.0.31
    40 deny any:
```

¿Debe aplicar la ACL BRANCH-OFFICE-POLICY a la interfaz G0/1 en el R1? NO, EL COMANDO IP ACCESS-GROUP BRANCH-OFFICE-POLICY OUT TODAVÍA ESTÁ IMPLEMENTADO EN G0/1

2) Pruebe la ACL para ver si permite que el tráfico del acceso a la red 209.165.200.224/27 regrese a la red 192.168.10.0/24. Desde PC-A, realice un ping al servidor en 209.165.200.254.

¿Fueron correctos los pings? SI

## Preguntas de reflexión

1. Como puede observar, las ACL estándar son muy eficaces y funcionan muy bien. ¿Por qué tendría la necesidad de usar ACL extendidas?

LAS ACL ESTÁNDAR FILTRAN SEGÚN LA DIRECCIÓN DE ORIGEN Y CARECEN DE GRANULARIDAD, LO QUE SIGNIFICA QUE PERMITEN O NIEGAN TODO TIPO DE TRÁFICO. POR OTRO LADO, LAS ACL EXTENDIDAS SON MÁS COMPLEJAS DE CONFIGURAR PERO SON IDEALES PARA REDES COMPLICADAS DONDE SE REQUIERE PERMITIR CIERTOS PUERTOS DE CAPA 4 Y BLOQUEAR OTROS. PARA LAS ACL ESTÁNDAR, ES CRUCIAL APLICARLAS CERCA DEL DESTINO PARA EVITAR QUE EL TRÁFICO INNECESARIO UTILICE EL ANCHO DE BANDA DE LA RED. EN CAMBIO, LAS ACL EXTENDIDAS PUEDEN BLOQUEAR EL TRÁFICO CERCA DE SU ORIGEN, EVITANDO ASÍ QUE LLEGUE AL DESTINO DONDE SE BLOQUEARÍA.

2. Normalmente se requiere más tipeo cuando se usa una ACL con nombre en lugar de una ACL numerada. ¿Por qué elegiría ACL con nombre en vez de ACL numeradas?

HAY DOS RAZONES PARA USAR ACL CON NOMBRE. PRIMERO, PERMITEN MODIFICAR LÍNEAS ESPECÍFICAS DENTRO DE LA ACL SIN TENER QUE REESCRIBIR TODA LA LISTA. SEGUNDO, PROPORCIONAN UN NOMBRE

DESCRIPTIVO QUE AYUDA A REGISTRAR EL PROPÓSITO DE LA ACL. LAS VERSIONES MÁS RECIENTES DEL IOS TAMBIÉN PERMITEN MODIFICAR LAS ACL NUMERADAS DE MANERA SIMILAR.