Práctica de laboratorio: configuración y verificación de ACL estándar

Topología

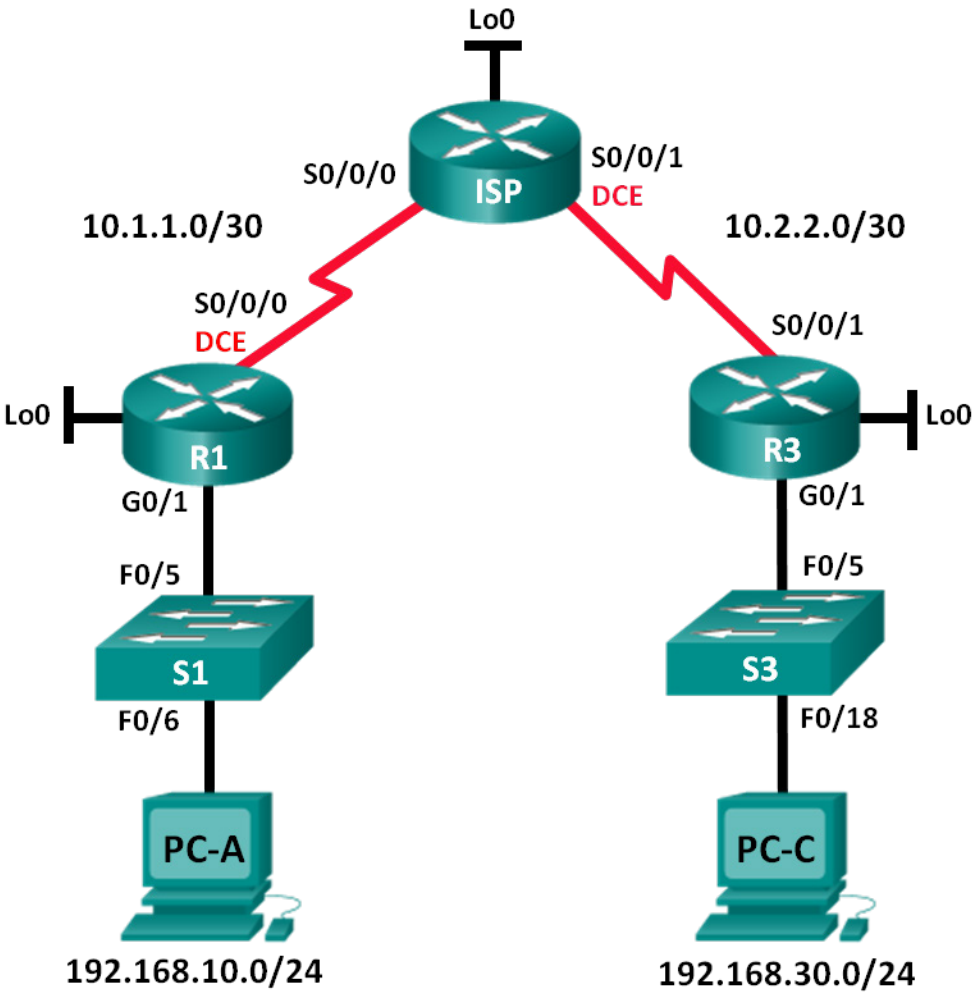

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

- Configurar los equipos para que coincidan con la topología de la red.
- Inicializar y volver a cargar los routers y los switches.

Parte 2: configurar los dispositivos y verificar la conectividad

- Asignar una dirección IP estática a las computadoras.
- Configurar los parámetros básicos en los routers.
- Configurar los parámetros básicos en los switches.
- Configurar los procesos de routing EIGRP en el R1, el ISP y el R3.
- Verificar la conectividad entre los dispositivos.

Parte 3: configurar y verificar ACL estándar numeradas y con nombre

- Configurar, aplicar y verificar una ACL estándar numerada.
- Configurar, aplicar y verificar una ACL con nombre.

Parte 4: modificar una ACL estándar

- Modificar y verificar una ACL estándar con nombre.
- Probar la ACL.

Información básica/situación

La seguridad de red es una cuestión importante 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 esta práctica de laboratorio, establecerá reglas de filtrado para dos oficinas representadas por el R1 y el 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 ISP que se ubica entre el R1 y el R3 no tendrá ninguna ACL. Usted no tiene permitido el acceso administrativo al router ISP, debido a que solo puede controlar y administrar sus propios equipos.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red y borrará cualquier configuración, en caso de ser necesario.

Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar los routers y los switches.

Parte 2: Configurar dispositivos y verificar la conectividad

En la parte 2, configurará los parámetros básicos en los routers, los switches y las computadoras. Consulte la topología y la tabla de direccionamiento para conocer los nombres de los dispositivos y obtener información de direcciones.

Paso 1: configurar las direcciones IP en la PC-A y en la PC-C.

Paso 2: configurar los parámetros básicos de los routers.

a. Desactive la búsqueda del DNS.

b. Configure los nombres de los dispositivos como se muestra en la topología.

c. Cree interfaces loopback en cada router como se muestra en la tabla de direccionamiento.

d. Configure las direcciones IP de interfaz, como se muestra en la topología y en la tabla de direccionamiento.

e. Configure **class** como la contraseña del modo EXEC privilegiado.

f. Asigne la frecuencia de reloj **128000** a las interfaces seriales DCE.

g. Asigne **cisco** como la contraseña de consola.

h. Asigne **cisco** como la contraseña de vty y habilite acceso por Telnet.

Paso 3: (optativo) configurar los parámetros básicos en los switches.

a. Desactive la búsqueda del DNS.

b. Configure los nombres de los dispositivos como se muestra en la topología.

c. Configure la dirección IP de la interfaz de administración, como se muestra en la topología y en la tabla de direccionamiento.

d. Configure **class** como la contraseña del modo EXEC privilegiado.

e. Configure un gateway predeterminado.

f. Asigne **cisco** como la contraseña de consola.

g. Asigne **cisco** como la contraseña de vty y habilite acceso por Telnet.

Paso 4: Configure los procesos de routing de EIGRP en el R1, el ISP y el R3.

a. Configure el sistema autónomo (AS) número 10 y anuncie todas las redes en el R1, el ISP y el R3. Desactivar la sumarización automática.

b. Después de configurar EIGRP en el R1, el ISP y el R3, verifique que todos los routers tengan tablas de routing completas con todas las redes. De lo contrario, resuelva el problema.

Paso 5: verificar la conectividad entre los dispositivos.

Nota: es muy importante probar si la conectividad funciona **antes** de configurar y aplicar listas de acceso. Tiene que asegurarse de que la red funcione adecuadamente antes de empezar a filtrar el tráfico.

a. Desde la PC-A, haga ping a la PC-C y a la interfaz loopback en el R3. ¿Los pings se realizaron correctamente?

b. Desde el R1, haga ping a la PC-C y a la interfaz loopback en el R3. ¿Los pings se realizaron correctamente?

c. Desde la PC-C, haga ping a la PC-A y a la interfaz loopback en el R1. ¿Los pings se realizaron correctamente?

d. Desde el R3, haga ping a la PC-A y a la interfaz loopback en el R1. ¿Los pings se realizaron correctamente?

Parte 3: 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 configurarlas y aplicarlas lo más cerca posible del destino. Para la primera lista de acceso, cree una ACL estándar numerada que permita que el tráfico proveniente de todos los hosts en la red 192.168.10.0/24 y de todos los hosts en la red 192.168.20.0/24 acceda a todos los hosts en la red 192.168.30.0/24. La política de seguridad también indica que debe haber una entrada de control de acceso (ACE) **deny any**, también conocida como “instrucción 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?

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

¿En qué interfaz colocaría esta ACL? ¿En qué sentido la aplicaría?

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

c. Verifique una ACL numerada.

El uso de diversos comandos **show** puede ayudarle a verificar la sintaxis y la colocación de las ACL en el router.

¿Qué comando usaría para ver la lista de acceso 1 en su totalidad, con todas las ACE?

¿Qué comando usaría para ver dónde se aplicó la lista de acceso y en qué sentido?

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

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

2) En el R3, emita el comando **show ip interface g0/1**.

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  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. ¿Tuvieron éxito los pings?

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. Debe hacer un ping extendido y usar la dirección loopback 0 en el R1 como origen. Haga ping a la dirección IP de la PC-C. ¿Tuvieron éxito los pings?

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
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 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

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

```
R1# ping 192.168.3.3
```

¿El ping se realizó correctamente? ¿Por qué o por qué no?

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?

¿En qué interfaz colocaría esta ACL? ¿En qué sentido la aplicaría?

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
```


Observe la primera ACE permit en la lista de acceso. ¿Cuál sería otra forma de escribir esto?

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

```
R1# config t
R1(config)# interface g0/1
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 192.168.30.3
    20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

¿Hay alguna diferencia entre esta ACL en el R1 y la ACL en el R3? Si es así, ¿cuál es?

2) En el R1, emita el comando **show ip interface g0/1**.

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<Output Omitted>
```

3) Pruebe la ACL. Desde el símbolo del sistema en la PC-C, haga ping a la dirección IP de la PC-A. ¿Tuvieron éxito los pings?

4) 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 usar la dirección G0/1 en el R3 como origen. Haga ping a la dirección IP de la PC-A. ¿Tuvieron éxito los pings?

5) 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. Debe hacer un ping extendido y usar la dirección loopback 0 en el R3 como origen. Haga ping a la dirección IP de la PC-A. ¿Tuvieron éxito los pings?

Parte 4: 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 4, cambiará una de las ACL que configuró anteriormente para que coincida con una nueva política de administración que se debe implementar.

La administración decidió que los usuarios de la red 209.165.200.224/27 no deben tener acceso total a la red 192.168.10.0/24. La administración también desea que las ACL en todos sus routers se ajusten a reglas coherentes. 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 quitaría la ACL completa del router. Según el IOS del router, ocurriría una de las siguientes situaciones: se cancelaría todo el filtrado de paquetes y se permitiría el acceso de todos los paquetes al router o bien, debido a que no quitó el comando **ip access-group** de la interfaz G0/1, el filtrado se sigue implementando. 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 implementadas y agregar o eliminar líneas específicas dentro de las ACL. Esto puede ser práctico, especialmente con las ACL que tienen muchas líneas de código. 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.

Nota: para esta práctica de laboratorio, utilice la opción 2.

Paso 1: modificar una ACL estándar con nombre.

a. En el modo EXEC privilegiado 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)
```

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?

2) Desde la entrada de comandos del ISP, emita un ping extendido. Pruebe la ACL para ver si permite que el tráfico de la red 209.165.200.224/27 acceda a la red 192.168.10.0/24. Debe hacer un ping extendido y usar la dirección loopback 0 en el ISP como origen. Haga ping a la dirección IP de la PC-A. ¿Tuvieron éxito los pings?

Reflexión

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

2. Generalmente, se requiere escribir más al usar una ACL con nombre que una ACL numerada. ¿Por qué elegiría ACL con nombre en vez de ACL numeradas?

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.