Práctica de laboratorio: configuración y verificación de ACL extendidas

Topología

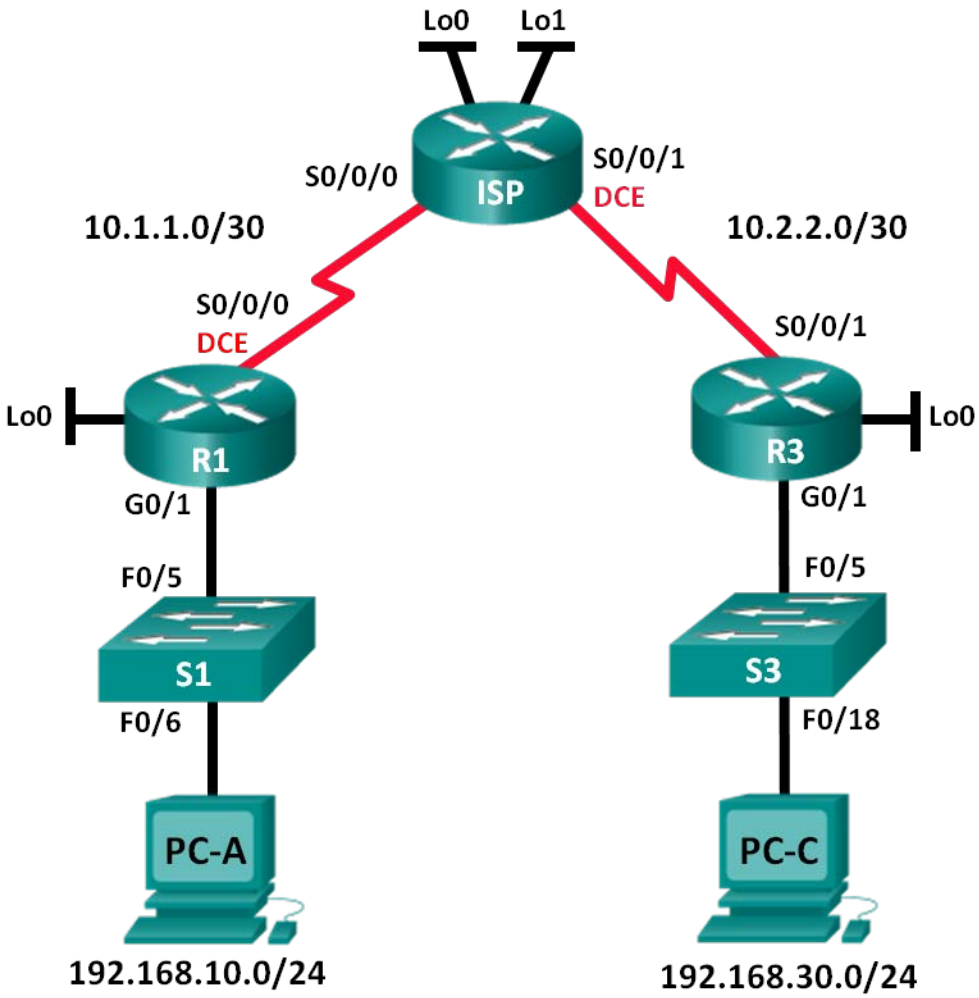

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.10.1	255.255.255.0	N/D
	Lo0	192.168.20.1	255.255.255.0	N/D
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/D
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/D
	Lo0	209.165.200.225	255.255.255.224	N/D
	Lo1	209.165.201.1	255.255.255.224	N/D
R3	G0/1	192.168.30.1	255.255.255.0	N/D
	Lo0	192.168.40.1	255.255.255.0	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
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

Parte 2: configurar los dispositivos y verificar la conectividad

- Configurar los parámetros básicos de las computadoras, los routers y los switches.
- Configurar routing OSPF en R1, ISP y R3.

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

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

Parte 4: modificar y verificar ACL extendidas

Aspectos básicos/situación

Las listas de control de acceso (ACL) extendidas son sumamente eficaces. Ofrecen un mayor grado de control que las ACL estándar en cuanto a los tipos de tráfico que se pueden filtrar y también en cuanto al lugar de origen y el destino del tráfico.

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 tiene ninguna ACL. Usted no tiene permitido el acceso administrativo al router ISP, dado 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 de la serie 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, 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 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 al instructor.

Recursos necesarios

- 3 routers (Cisco 1941 con Cisco IOS versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con Cisco IOS 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, si fuera 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 los 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 en el R1

a. Desactive la búsqueda de DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

c. Cree una interfaz loopback en el R1.

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 la interfaz S0/0/0.

g. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el acceso por Telnet. Configure **logging synchronous** para las líneas de consola y las líneas vty.

h. Habilite el acceso web en el R1 para simular un servidor web con autenticación local para el usuario **admin**.

```
R1(config)# ip http server
```



```
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

Paso 3: configurar los parámetros básicos en el ISP.

a. Configure el nombre del dispositivo como se muestra en la topología.

b. Cree las interfaces loopback en el ISP.

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

d. Desactive la búsqueda de DNS.

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

f. Asigne la frecuencia de reloj **128000** a la interfaz S0/0/1.

g. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el acceso por Telnet. Configure **logging synchronous** para las líneas de consola y las líneas vty.

h. Habilite el acceso web en el ISP. Utilice los mismos parámetros que en el paso 2h.

Paso 4: configurar los parámetros básicos en el R3.

a. Configure el nombre del dispositivo como se muestra en la topología.

b. Cree una interfaz loopback en el R3.

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

d. Desactive la búsqueda de DNS.

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

f. Asigne **cisco** como la contraseña de consola y configure **logging synchronous** en la línea de consola.

g. Habilite SSH en el R3.

```
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa modulus 1024
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

h. Habilite el acceso web en el R3. Utilice los mismos parámetros que en el paso 2h.

Paso 5: (optativo) configurar los parámetros básicos en el S1 y el S3.

a. Configure los nombres de host como se muestra en la topología.

b. Configure las direcciones IP de las interfaces de administración como se muestra en la topología y en la tabla de direccionamiento.

c. Desactive la búsqueda de DNS.

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

e. Configure la dirección de gateway predeterminado.

Paso 6: Configurar routing OSPF en R1, ISP y R3.

a. Asigne 1 como ID del proceso OSPF y publique todas las redes de R1, el ISP, y R3. La configuración de OSPF del R1 se incluye como referencia.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# network 192.168.20.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

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

Paso 7: verificar la conectividad entre los dispositivos.

Nota: es muy importante verificar la conectividad **antes** de configurar y aplicar ACL. Asegúrese 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 las interfaces loopback y de serie en el R3.

¿Los pings se realizaron correctamente?

b. Desde el R1, haga ping a la PC-C y a las interfaces loopback y serial en el R3.

¿Los pings se realizaron correctamente?

c. Desde la PC-C, haga ping a la PC-A y a las interfaces loopback y serial en el R1.

¿Los pings se realizaron correctamente?

d. Desde el R3, haga ping a la PC-A y a las interfaces loopback y serial en el R1.

¿Los pings se realizaron correctamente?

e. Desde la PC-A, haga ping a las interfaces loopback en el router ISP.

¿Los pings se realizaron correctamente?

f. Desde la PC-C, haga ping a las interfaces loopback en el router ISP.

¿Los pings se realizaron correctamente?

g. Abra un navegador web en la PC-A y vaya a http://209.165.200.225 en el ISP. Se le pedirá que introduzca un nombre de usuario y contraseña. Utilice **admin** como el nombre de usuario y **class** como la contraseña. Si se le solicita que acepte una firma, acéptela. El router cargará Cisco Configuration Professional (CCP) Express en una ventana diferente. Es posible que se le solicite un nombre de usuario y una contraseña. Use **admin** como nombre de usuario y **class** como contraseña.

h. Abra un navegador web en la PC-C y vaya a http://10.1.1.1 en el R1. Se le pedirá que introduzca un nombre de usuario y contraseña. Utilice **admin** como el nombre de usuario y **class** como la contraseña. Si se le solicita que acepte una firma, acéptela. El router cargará CCP Express en una ventana diferente. Es posible que se le solicite un nombre de usuario y una contraseña. Use **admin** como nombre de usuario y **class** como contraseña.

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

Las ACL extendidas filtran el tráfico de diferentes formas. Las ACL extendidas pueden realizar el filtrado según direcciones IP de origen, puertos de origen, dirección IP de destino y puertos de destino, así como según varios protocolos y servicios.

Las políticas de seguridad son las siguientes:

1. Permitir que el tráfico web que se origina en la red 192.168.10.0/24 vaya a cualquier red.

2. Permitir una conexión SSH a la interfaz serial del R3 desde la PC-A.
3. Permitir que los usuarios en la red 192.168.10.0/24 accedan a la red 192.168.20.0/24.
4. Permitir que el tráfico web que se origina en la red 192.168.30.0/24 acceda al R1 mediante la interfaz web y la red 209.165.200.224/27 en el ISP. NO se debe permitir que la red 192.168.30.0/24 tenga acceso a cualquier otra red a través de la web.

Al observar las políticas de seguridad mencionadas anteriormente, sabe que necesitará al menos dos ACL para cumplir con ellas. Una práctica recomendada es colocar ACL extendidas lo más cerca posible del origen. Para estas políticas, respetaremos esta práctica.

Paso 1: configurar una ACL extendida numerada en el R1 para las políticas de seguridad 1 y 2.

Usará una ACL extendida numerada en el R1. ¿Cuáles son los rangos de las ACL extendidas?

a. Configure la ACL en el R1. Use 100 como el número de la ACL.

```
R1(config)# access-list 100 remark Allow Web & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

¿Qué indica el 80 que aparece en el resultado del comando anterior?

¿A qué interfaz debe aplicarse la ACL 100?

¿En qué sentido se debería aplicar la ACL 100?

b. Aplique la ACL 100 a la interfaz S0/0/0.

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 100 out
```

c. Verifique la ACL 100.

1) Abra un navegador web en la PC-A y vaya a http://209.165.200.225 (el router ISP). La conexión debería realizarse correctamente; de lo contrario, resuelva el problema.

2) Establezca una conexión SSH de la PC-A al R3 con 10.2.2.1 como dirección IP. Inicie sesión con las credenciales **admin** y **class**. La conexión debería realizarse correctamente; de lo contrario, resuelva el problema.

3) En la petición de entrada del modo EXEC privilegiado en el R1, emita el comando **show access-lists**.

```
R1# show access-lists
Extended IP access list 100
    10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)
    20 permit tcp any any eq www (111 matches)
```

4) Desde el símbolo del sistema de la PC-A, emita un ping a 10.2.2.1. Explique los resultados.

Paso 2: configurar una ACL extendida con nombre en el R3 para la política de seguridad 3.

a. Configure la política en el R3. Asigne el nombre WEB-POLICY a la ACL.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80
```

b. Aplique la ACL WEB-POLICY a la interfaz S0/0/1.

```
R3(config-ext-nacl)# interface S0/0/1
R3(config-if)# ip access-group WEB-POLICY out
```

c. Verifique la ACL WEB-POLICY.

1) En la petición de entrada del modo EXEC privilegiado en el R3, emita el comando **show ip interface s0/0/1**.

¿Cuál es el nombre de la ACL, si tiene un nombre?

¿En qué sentido se aplicó la ACL?

2) Abra un navegador web en la PC-C y vaya a http://209.165.200.225 (el router ISP). La conexión debería realizarse correctamente; de lo contrario, resuelva el problema.

3) Desde la PC-C, inicie una sesión web en http://10.1.1.1 (R1). La conexión debería realizarse correctamente; de lo contrario, resuelva el problema.

4) Desde la PC-C, inicie una sesión web en http://209.165.201.1 (router ISP). La conexión debería fallar; de lo contrario, resuelva el problema.

5) Desde el símbolo del sistema de la PC-C, haga ping a la PC-A. ¿Cuál fue el resultado y por qué?

Parte 4: modificar y verificar ACL extendidas

Debido a las ACL aplicadas en el R1 y el R3, no se permiten pings ni ningún otro tipo de tráfico entre las redes LAN en el R1 y el R3. La administración decidió que debe permitirse todo el tráfico entre las redes 192.168.10.0/24 y 192.168.30.0/24. Debe modificar las ACL en el R1 y el R3.

Paso 1: modificar la ACL 100 en el R1.

a. En el modo EXEC privilegiado en el R1, emita el comando **show access-lists**.

¿Cuántas líneas hay en esta lista de acceso?

b. Ingrese al modo de configuración global y modifique la ACL en el R1.

```
R1(config)# ip access-list extended 100
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
R1(config-ext-nacl)# end
```


c. Emita el comando **show access-lists**.

¿En qué lugar de la ACL 100 apareció la línea nueva que acaba de agregar?

Paso 2: modificar la ACL WEB-POLICY en el R3.

a. En el modo EXEC privilegiado en el R3, emita el comando **show access-lists**.

¿Cuántas líneas hay en esta lista de acceso?

b. Ingrese al modo de configuración global y modifique la ACL en el R3.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
R3(config-ext-nacl)# end
```

c. Emita el comando **show access-lists** para verificar que la línea nueva se haya agregado al final de la ACL.

Paso 3: verificar las ACL modificadas.

a. Desde la PC-A, emita un comando ping a la dirección IP de la PC-C. ¿Produjo un resultado correcto?

b. En la PC-C, haga ping a la dirección IP de la PC-A. ¿Fueron correctos los pings?

¿Por qué las ACL funcionaron inmediatamente para los pings después de que las cambió?

Reflexión

1. ¿Por qué es necesario planificar y probar meticulosamente las ACL?

2. Qué tipo de ACL es mejor: ¿estándar o extendida?

3. ¿Por qué la entrada de control de acceso (ACE) o la instrucción de ACL **deny any** implícita de las ACL aplicadas al R1 y al R3 no bloquea los paquetes de saludo ni las actualizaciones de routing OSPF?

Tabla de resumen de interfaces de router

Resumen de interfaces de router				
Modelo de router	**Interfaz Ethernet 1**	**Interfaz Ethernet 2**	**Interfaz serial 1**	**Interfaz serial 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 hacer 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 un comando de Cisco IOS para representar la interfaz.