Cisco | Networking Academy®
Mind Wide Open™

Práctica de laboratorio 5.5.1: Listas de control de acceso básicas

Diagrama de topología

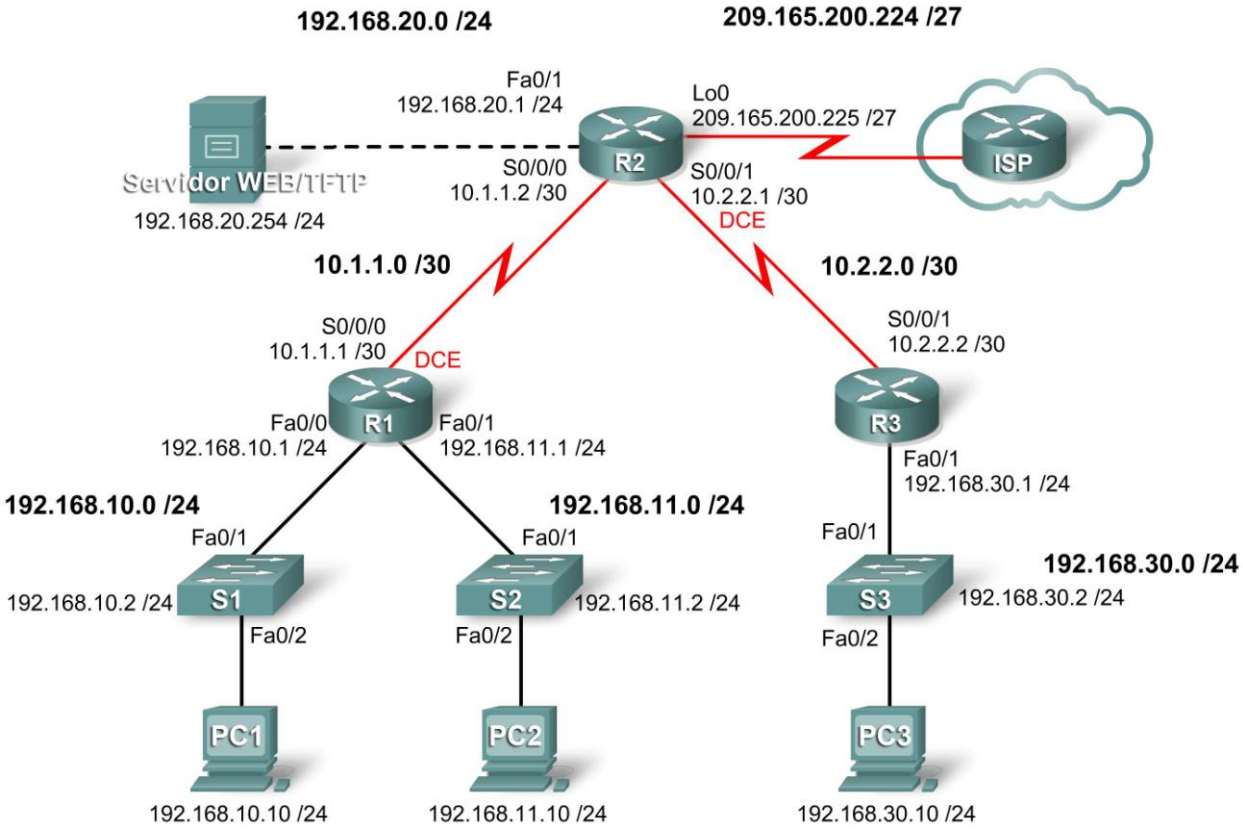

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**Fa0/0**	192.168.10.1	255.255.255.0	
	Fa0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
R2	**Fa0/1**	192.168.20.1	255.255.255.0	
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
	Lo0	209.165.200.225	255.255.255.224	
R3	**Fa0/1**	192.168.30.1	255.255.255.0	
	S0/0/1	10.2.2.2	255.255.255.252	
S1	**Vlan1**	192.168.10.2	255.255.255.0	192.168.10.1

S2	**Vlan1**	192.168.11.2	255.255.255.0	192.168.11.1
S3	**Vlan1**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Web Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, el usuario podrá:

- Diseñar ACL nombradas estándar y nombradas ampliadas
- Aplicar ACL nombradas estándar y nombradas ampliadas
- Probar ACL nombradas estándar y nombradas ampliadas
- Realizar la resolución de problemas relacionados con ACL nombradas estándar y nombradas ampliadas

Escenario

En esta práctica de laboratorio, se aprenderá a configurar la seguridad básica de red mediante listas de control de acceso. Se aplicarán ACL estándar y ampliadas.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Se puede utilizar cualquier router del laboratorio, siempre y cuando éste disponga de las interfaces necesarias que se muestran en el diagrama de topología.

Nota: Esta práctica de laboratorio se desarrolló y probó mediante routers 1841. Si se utilizan routers serie 1700, 2500 ó 2600, los resultados y las descripciones del router pueden ser diferentes. En routers más antiguos o en versiones de IOS anteriores a la 12.4, es posible que algunos comandos sean diferentes o que no existan.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar las configuraciones básicas del router

Configure los routers R1, R2, R3 y los switches S1, S2 y S3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router de modo que coincida con el diagrama de topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de **class** en el Modo EXEC.
- Configure un mensaje del día.
- Configure una contraseña de cisco para las conexiones de consola.
- Configure una contraseña para las conexiones de vty.
- Configure máscaras y direcciones IP en todos los dispositivos.
- Habilite OSPF área 0 en todos los routers para todas las redes.

- Configure una interfaz loopback en R2 para simular el ISP.
- Configure direcciones IP para la interfaz VLAN 1 en cada switch.
- Configure cada switch con la gateway por defecto apropiada.
- Verifique que la conectividad IP sea total mediante el comando **ping**.

Tarea 3: Configurar una ACL estándar

Las ACL estándar pueden filtrar tráfico sólo según la dirección IP de origen. Una práctica recomendada típica es configurar una ACL estándar tan cerca del destino como sea posible. En esta tarea, se configurará una ACL estándar. La ACL está diseñada para impedir que el tráfico desde la red 192.168.11.0/24, ubicada en un laboratorio de estudiantes, acceda a cualquiera de las redes locales de R3.

Esta ACL se aplicará en dirección entrante en la interfaz serial de R3. Se debe recordar que cada ACL tiene un comando “deny all” implícito que hace que se bloquee todo el tráfico que no coincida con una sentencia de la ACL. Por esta razón, se debe agregar la sentencia **permit any** al final de la ACL.

Antes de configurar y aplicar esta ACL, asegúrese de probar la conectividad desde PC1 (o la interfaz Fa0/1 de R1) a PC3 (o la interfaz Fa0/1del R3). Las pruebas de conectividad deberían realizarse correctamente antes de aplicar la ACL.

Paso 1: Crear la ACL en el router R3.

En el modo de configuración global, cree una ACL nombrada estándar denominada **STND-1**.

```
R3(config)#ip access-list standard STND-1
```

En el modo de configuración de ACL estándar, agregue una sentencia que deniegue cualquier paquete con una dirección de origen de 192.168.11.0 /24 e imprima un mensaje a la consola por cada paquete coincidente.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255 log
```

Permita todo el tráfico restante.

```
R3(config-std-nacl)#permit any
```

Paso 2: Aplicar la ACL.

Aplique la ACL **STND-1** como filtro en los paquetes que ingresan a R3 a través de la interfaz serial 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 in
R3(config-if)#end
R3#copy run start
```

Paso 3: Probar la ACL.

Antes de probar la ACL, asegúrese de que la consola de R3 esté visible. De este modo, se podrán ver los mensajes de registro de la lista de acceso cuando se deniegue el acceso al paquete.

Pruebe la ACL haciendo ping de PC2 a PC3. Debido a que la ACL está diseñada para bloquear el tráfico con direcciones de origen de la red 192.168.11.0 /24, PC2 (192.168.11.10) no debería poder hacer ping a PC3.

También se puede utilizar un ping ampliado desde la interfaz Fa0/1 del R1 a la interfaz Fa0/1 del R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
```

```
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.11.1
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 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
U.U.U
Success rate is 0 percent (0/5)
```

Se debería poder ver el siguiente mensaje en la consola de R3:

```
*Sep  4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0
0.0.0.0 -> 192.168.11.1, 1 packet
```

En el modo EXEC privilegiado de R3, ejecute el comando **show access-lists**. El resultado debe ser similar al siguiente. Cada línea de una ACL tiene un contador asociado que muestra cuántos paquetes coinciden con la regla.

```
Standard IP access list STND-1
    10 deny   192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)
    20 permit any (25 matches)
```

El objetivo de esta ACL era bloquear los hosts de la red 192.168.11.0/24. Cualquier otro host, como por ejemplo, los de la red 192.168.10.0/24, debería tener acceso a las redes de R3. Realice otra prueba de PC1 a PC3 para asegurarse de que este tráfico no se bloquee.

También se puede utilizar un ping ampliado desde la interfaz Fa0/0 del R1 a la interfaz Fa0/1 del R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.10.1
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 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms
```

Tarea 4: Configurar una ACL ampliada

Cuando se requiere un mayor nivel de detalle, se debe usar una ACL ampliada. Las ACL ampliadas pueden filtrar el tráfico teniendo en cuenta otros aspectos, además de la dirección de origen. Las ACL ampliadas pueden filtrar según el protocolo, las direcciones IP de origen y destino y los números de

puerto de origen y destino.

Una política adicional para esta red establece que los dispositivos de la LAN 192.168.10.0/24 sólo pueden alcanzar las redes internas. Los equipos de esta LAN no pueden acceder a Internet. Por lo tanto, estos usuarios deben bloquearse para que no alcancen la dirección IP 209.165.200.225. Debido a que este requisito debe cumplirse tanto en el origen como en el destino, se necesita una ACL ampliada.

En esta tarea, se configurará una ACL ampliada en R1 que impide que el tráfico que se origina en cualquier dispositivo de la red 192.168.10.0/24 acceda al host 209.165.200.255 (el ISP simulado). Esta ACL se aplicará en dirección saliente en la interfaz Serial 0/0/0 de R1. Una práctica recomendada típica para la aplicación de ACL ampliada es ubicarlas tan cerca del origen como sea posible.

Antes de comenzar, verifique que se pueda hacer ping a 209.165.200.225 desde PC1.

Paso 1: Configurar una ACL ampliada y nombrada.

En el modo de configuración global, cree una ACL nombrada y ampliada, denominada **EXTEND-1**.

```
R1(config)#ip access-list extended EXTEND-1
```

Observe que el indicador del router cambia para señalar que ahora se encuentra en el modo de configuración de ACL ampliada. Desde este indicador, agregue las sentencias necesarias para bloquear el tráfico desde la red 192.168.10.0 /24 al host. Utilice la palabra clave **host** cuando defina el destino.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Recuerde que el comando “deny all” implícito bloquea cualquier otro tráfico sin la sentencia adicional **permit**. Agregue la sentencia **permit** para asegurarse de que no se bloquee el tráfico restante.

```
R1(config-ext-nacl)#permit ip any any
```

Paso 2: Aplicar la ACL.

Con las ACL estándar, lo más conveniente es ubicar a la ACL lo más cerca posible del destino. Las ACL ampliadas generalmente se ubican cerca del origen. La ACL **EXTEND-1** se ubicará en la interfaz serial y filtrará el tráfico saliente.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group EXTEND-1 out log
R1(config-if)#end
R1#copy run start
```

Paso 3: Probar la ACL.

Desde PC1, haga ping a la interfaz loopback de R2. Estos ping deberían fallar porque todo el tráfico proveniente de la red 192.168.10.0/24 se filtra cuando el destino es 209.165.200.225. Si el destino es cualquier otra dirección, los pings deberían realizarse correctamente. Confirme esto haciendo ping al R3 desde el dispositivo de red 192.168.10.0/24.

Nota: La función de ping ampliado de R1 no puede utilizarse para probar esta ACL, ya que el tráfico se originará dentro de R1 y no volverá probarse con la ACL aplicada a la interfaz serial de R1.

Es posible verificarlo nuevamente al ejecutar **show ip access-list** en R1 después de hacer ping.

```
R1#show ip access-list
Extended IP access list EXTEND-1
    10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)
    20 permit ip any any
```

Tarea 5: Controlar el acceso a las líneas VTY con una ACL estándar

Es conveniente restringir el acceso a las líneas VTY del router para la administración remota. Puede aplicarse una ACL a las líneas VTY, lo que permite restringir el acceso a hosts o redes específicos. En esta tarea, se configurará una ACL estándar para permitir que los hosts de dos redes accedan a las líneas VTY. Se le negará el acceso a todos los demás hosts.

Verifique que pueda establecer una conexión telnet a R2 desde R1 y R3.

Paso 1: Configurar la ACL.

Configure una ACL estándar nombrada en R2 que permita el tráfico desde 10.2.2.0/30 y 192.168.30.0/24. Debe denegarse todo el tráfico restante. Denomine la ACL **TASK-5**.

```
R2(config)#ip access-list standard TASK-5
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Paso 2: Aplicar la ACL.

Entre al modo de configuración de línea para las líneas VTY de 0 a 4.

```
R2(config)#line vty 0 4
```

Utilice el comando **access-class** para aplicar la ACL a las líneas vty en dirección entrante. Observe que esto difiere del comando que se utiliza para aplicar las ACL a otras interfaces.

```
R2(config-line)#access-class TASK-5 in
R2(config-line)#end
R2#copy run start
```

Paso 3: Probar la ACL.

Establezca una conexión telnet a R2 desde R1. Observe que R1 no tiene direcciones IP en su rango de direcciones que aparece en las sentencias de permiso de la ACL TASK-5. Los intentos de conexión deberían fallar.

```
R1# telnet 10.1.1.2
Trying 10.1.1.2 …
% Connection refused by remote host
```

Desde R3, establezca una conexión telnet a R2. Aparece una petición de entrada para la contraseña de la línea VTY.

```
R3# telnet 10.1.1.2
Trying 10.1.1.2 … Open
CUnauthorized access strictly prohibited, violators will be prosecuted
to the full extent of the law.

User Access Verification

Password:
```

¿Por qué los intentos de conexión desde otras redes fallan aunque no se enumeren específicamente en la ACL?

_____

_____

Tarea 6: Resolución de problemas en las ACL

Cuando se configura incorrectamente una ACL o se la aplica a la interfaz incorrecta o en la dirección incorrecta, el tráfico de red puede verse afectado de manera no deseada.

Paso 1: Eliminar la ACL STND-1 de S0/0/1 de R3.

En una tarea anterior, se creó y aplicó una ACL nombrada y estándar en R3. Utilice el comando **show running-config** para visualizar la ACL y su ubicación. Se debería ver que una ACL llamada **STND-1** se configuró y aplicó en dirección entrante en Serial 0/0/1. Recuerde que esta ACL se diseñó para impedir que todo el tráfico de red con una dirección de origen de la red 192.168.11.0/24 acceda a la LAN del R3.

Para eliminar la ACL, entre al modo de configuración de la interfaz para Serial 0/0/1 de R3. Utilice el comando **no ip access-group STND-1** para eliminar la ACL de la interfaz.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 in
```

Use el comando **show running-config** para confirmar que la ACL se haya eliminado de la Serial 0/0/1.

Paso 2: Aplicar la ACL STND-1 en S0/0/1 saliente.

Para probar la importancia de la dirección de filtrado de la ACL, aplique nuevamente la ACL **STND-1** a la interfaz Serial 0/0/1. Esta vez, la ACL filtrará el tráfico saliente en lugar del tráfico entrante. Recuerde utilizar la palabra clave **out** cuando aplique la ACL.

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

Paso 3: Probar la ACL.

Pruebe la ACL haciendo ping de PC2 a PC3. Como alternativa, utilice un ping ampliado desde R1. Observe que esta vez los pings se realizan correctamente y que los contadores de la ACL no aumentan. Confirme esto mediante el comando **show ip access-list** en R3.

Paso 4: Restablecer la configuración original de la ACL.

Elimine la ACL de la dirección saliente y aplíquela nuevamente a la dirección entrante.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 out
R3(config-if)#ip access-group STND-1 in
```

Paso 5: Aplicar TASK-5 a la interfaz serial 0/0/0 entrante de R2.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group TASK-5 in
```

Paso 6: Probar la ACL.

Intente comunicarse con cualquier dispositivo conectado a R2 o R3 desde R1 o sus redes conectadas. Observe que toda la comunicación está bloqueada. Sin embargo, los contadores de la ACL no aumentan. Esto se debe al comando “deny all” implícito al final de todas las ACL. Esta sentencia deny impide todo el tráfico entrante a la serial 0/0/0 desde cualquier origen que no sea R3. Básicamente, esto hará que las rutas de R1 se eliminen de la tabla de enrutamiento.

Se deberían ver mensajes similares a los que aparecen a continuación impresos en las consolas de R1 y R2 (debe transcurrir un tiempo para que la relación vecina OSPF se desactive, por lo que deberá ser paciente):

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
```

```
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Una vez recibido este mensaje, ejecute el comando **show ip route** tanto en R1 como en R2 para determinar qué rutas se eliminaron de la tabla de enrutamiento.

Elimine la ACL TASK-5 de la interfaz y guarde las configuraciones.

```
R2(config)#interface serial 0/0/0
R2(config-if)#no ip access-group TASK-5 in
R2(config)#exit
R2#copy run start
```

Tarea 7: Documentar las configuraciones del router

Configuraciones

Router 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group EXTEND-1 out
 clockrate 64000
 no shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip access-list extended EXTEND-1
 deny   ip 192.168.10.0 0.0.0.255 host 209.165.200.225
 permit ip any any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
```

```
 login
!
```

Router 2

```
hostname R2
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clockrate 125000
 no shutdown
!
router ospf 1
 no auto-cost
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.31 area 0
!
ip access-list standard TASK-5
 permit 10.2.2.0 0.0.0.3
 permit 192.168.30.0 0.0.0.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class TASK-5 in
 password cisco
 login
!
```

Router 3

```
hostname R3
!
```

```
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip access-group STND-1 out
 no shutdown
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip access-list standard STND-1
 deny   192.168.11.0 0.0.0.255 log
 permit any
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
end
```

Tarea 8: Limpiar

Borre las configuraciones y recargue los routers. Desconecte y guarde los cables. Para los equipos PC host que normalmente se conectan a otras redes (tal como la LAN de la escuela o Internet), reconecte los cables correspondientes y restablezca las configuraciones TCP/IP.