Práctica de laboratorio: resolución de problemas de configuración y colocación de ACL

Topología

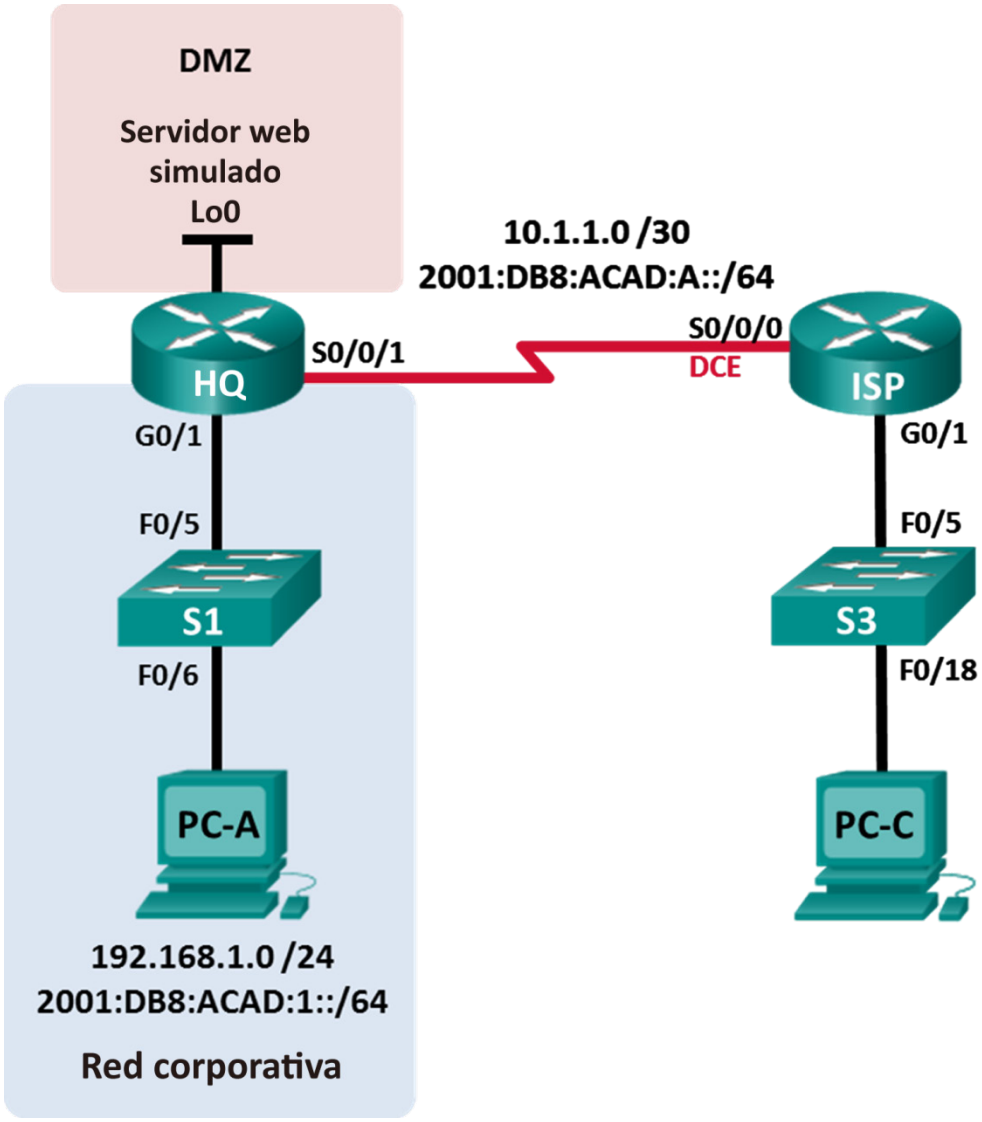

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
		Dirección/prefijo IPv6		
		Dirección local de enlace		
HQ	G0/1	192.168.1.1	255.255.255.0	N/D
		2001:DB8:ACAD:1::1/64		
		FE80::1		
	S0/0/1	10.1.1.2	255.255.255.252	N/D
		2001:DB8:ACAD:A::2/64		
		FE80::2		
	Lo0	192.168.4.1	255.255.255.0	N/D
		2001:DB8:ACAD:4::1/64		
		FE80::1		
ISP	G0/1	192.168.3.1	255.255.255.0	N/D
		2001:DB8:ACAD:3::1/64		
		FE80::1		
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/D
		2001:DB8:ACAD:A::1/64		
		FE80::1		
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
		2001:DB8:ACAD:1::3/64		FE80::1
		FE80::3		
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1
		2001:DB8:ACAD:3::3/64		FE80::1
		FE80::3		

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: resolver problemas de acceso interno

Parte 3: resolver problemas de acceso remoto

Aspectos básicos/situación

Una lista de control de acceso (ACL) es una serie de comandos IOS que proporcionan filtrado de tráfico básico en un router Cisco. Las ACL se usan para seleccionar los tipos de tráfico que se deben procesar.

Una instrucción de ACL individual se conoce como entrada de control de acceso (ACE). Las ACE en la ACL se evalúan de arriba abajo, y al final de la lista hay una ACE deny all implícita. Las ACL también controlan los tipos de tráfico entrante y saliente de una red según los hosts o las redes de origen y destino. Para procesar el tráfico deseado correctamente, la ubicación de las ACL es fundamental.

En esta práctica de laboratorio, una pequeña empresa acaba de agregar un servidor web a la red para permitir que los clientes tengan acceso a información confidencial. La red IPv4 e IPv6 de la empresa se divide en dos zonas: zona de red corporativa y zona perimetral (DMZ). La zona de red corporativa aloja los servidores privados y los clientes internos. La DMZ aloja el servidor web al que se puede acceder de forma externa (simulado por Lo0 en HQ).

Al acceso seguro a corporativo y a las redes de DMZ, varias ACL se configuró en el router HQ. Sin embargo, existen problemas con las ACL configuradas. En esta práctica de laboratorio, examinará lo que están haciendo y toman las ACL acciones correctivas para implementarlas correctamente.

Al resolver las ACL, es importante que su propósito y resultado deseado se entienda bien. Por este motivo, a continuación se describen las ACL configuradas en HQ:

- **ACL 101** se implementa para limitar el tráfico que abandona la zona de la red corporativa. Esta zona se conoce generalmente como el privados o la red interna porque contiene los servidores privados y clientes internos. En esta topología, esta zona es la dirección de red asignada 192.168.1.0/24. Por lo tanto, sólo el tráfico de esa red se debe permitir para salir de la red interna.
- **ACL 102** se utiliza para limitar el tráfico que ingresa a la red corporativa. A esa red solo pueden acceder las respuestas a las solicitudes que se originaron dentro de la red corporativa. Esto incluye solicitudes basadas en TCP de los hosts internos, como web y FTP. Se permite el acceso de ICMP a la red para fines de resolución de problemas, de forma que los hosts internos pueden recibir mensajes ICMP entrantes generados en respuesta a pings. Ninguna otra red debería poder acceder a la zona corporativa.
- **ACL 121** controla el tráfico saliente a la DMZ y a la red corporativa. Solo se permite tráfico HTTP al servidor web DMZ (simulado por Lo0 en HQ). Se permite cualquier otro tráfico relacionado con la red, como EIGRP, desde redes externas. Además, se deniega el acceso a la red corporativa a las direcciones privadas internas válidas, como 192.168.1.0, las direcciones de loopback, como 127.0.0.1, y las direcciones de multidifusión, con el fin de impedir ataques malintencionados de usuarios externos a la red.
- **IPv6 ACL** nombrada NO-ICMP deniega el tráfico ICMP a la DMZ y a la red corporativa originados desde el exterior. La respuesta de ICMP puede en la red que responde a las solicitudes de los hosts de Internet. Se permite cualquier otro tráfico relacionado con la red, como EIGRP, desde redes externas. Además, la red externa tiene permitido el acceso al servidor web DMZ (simulado por Lo0 en HQ).

Nota: Los routers que se usan en las actividades prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con Cisco IOS versión 15.4(3) (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

- 2 routers (Cisco 1941 con Cisco IOS versión 15.4(3), imagen universal o equivalente)
- 2 switches (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 2 PC (Windows 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: Armar la red y configurar los ajustes básicos de los dispositivos

En la parte 1, elaborará la topología de red y configurará los routers y switches con ajustes básicos, como contraseñas y direcciones IP. También se proporcionan configuraciones predefinidas para la configuración inicial del router. Además, configurará los parámetros de IP de las computadoras en la topología.

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

Paso 2: Configurar hosts de PC según la tabla de asignación de direcciones

Paso 3: inicializar y volver a cargar los routers y los switches según sea necesario.

Paso 4: (optativo) configurar los parámetros básicos de cada switch.

a. Desactive la búsqueda de DNS.

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

c. Configure las direcciones IP y los gateways predeterminados, tal como se muestra en la tabla de asignación de direcciones.

d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

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

f. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.

Paso 5: Configure los parámetros básicos para cada router.

a. Desactive la búsqueda de DNS.

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

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

d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

e. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.

Paso 6: Configure el acceso HTTP y las credenciales de usuario en el router HQ.

Las credenciales de usuario local se configuran para acceder al servidor web simulado (192.168.4.1).

```
HQ(config)# ip http server
HQ(config)# username admin privilege 15 secret adminpass
HQ(config)# ip http authentication local
```


Paso 7: Cargar las configuraciones de los routers

Se le proporcionan las configuraciones de los routers ISP y HQ. Existen errores dentro de estas configuraciones, y es su tarea corregirlas.

Router ISP

```
hostname ISP
ipv6 unicast-routing
ipv6 router eigrp 1
 eigrp router-id 10.1.1.1
 no shutdown
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:3::1/64
 ipv6 eigrp 1
 no shutdown
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
 ipv6 eigrp 1
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 no auto-summary
end
```

Router HQ

```
hostname HQ
ipv6 unicast-routing
ipv6 router eigrp 1
 eigrp router-id 10.1.1.2
 no shutdown
interface Loopback0
 ip address 192.168.4.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:4::1/64
 ipv6 eigrp 1
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:1::1/64
 ip access-group 101 out
ip access-group 102 in
ipv6 eigrp 1
 no shutdown
interface Serial0/0/1
```



```
 ip address 10.1.1.2 255.255.255.252
 ip access-group 121 in
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:A::2/64
 ipv6 eigrp 1
ipv6 traffic-filter NO-ICMP out
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 red 192.168.1.0
 network 192.168.4.0
 no auto-summary
ip http server
access-list 101 permit ip 192.168.11.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny ip any any
access-list 121 permit tcp any host 192.168.4.1 eq 89
access-list 121 deny icmp any host 192.168.4.11
access-list 121 deny ip 192.168.1.0 0.0.0.255 any
access-list 121 deny   ip 127.0.0.0 0.255.255.255 any
access-list 121 deny   ip 224.0.0.0 31.255.255.255 any
access-list 121 permit ip any any
access-list 121 deny ip any any
ipv6 access-list NO-ICMP
 deny icmp any any echo-request
 permit ipv6 any any
end
```

Parte 2: resolver problemas de acceso interno

En la parte 2, se examinan las ACL en el router HQ para determinar si se configuraron correctamente.

Paso 1: resolver problemas en la ACL 101.

ACL 101 se implementa para limitar el tráfico que abandona la zona de la red corporativa. Esta zona solo aloja clientes internos y servidores privados. Solo la red 192.168.1.0/24 puede salir de esta zona de red corporativa.

a. ¿Se puede hacer ping de la PC-A a su gateway predeterminado?

b. Después de verificar que PC-A se configuró correctamente, examine el router HQ para encontrar posibles errores de configuración; para ello, mire el resumen de ACL 101. Introduzca el comando **show access-lists 101**.

```
HQ# show access-lists 101
Extended IP access list 101
    10 permit ip 192.168.11.0 0.0.0.255 any
    20 deny ip any any
```


c. ¿Existe algún problema en la ACL 101?

d. Corrija ACL 101. Registre los comandos usados para corregir los errores.

e. ¿Se puede hacer ping de la PC-A a su gateway predeterminado?

f. La PC-A aún no puede hacer ping a su gateway predeterminado, por lo tanto Verifique que la ACL 101 se aplica en la dirección correcta en la interfaz G0/1. Introduzca el comando **show ip interface g0/1**.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  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
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 101
  Inbound  access list is 102
```

¿El sentido de la ACL 101 en la interfaz G0/1 está configurado correctamente?

g. Edite la dirección de la ACL 101 en la interfaz G0/1. Registre los comandos usados para corregir los errores.

h. Verifique que el tráfico de la red 192.168.1.0 /24 puede salir de la red corporativa. Ahora PC-A debería poder emitir un ping a la interfaz de su gateway predeterminado.

Paso 2: resolver problemas en la ACL 102.

ACL 102 se implementa para limitar el tráfico que ingresa a la red corporativa. No se permite el acceso de tráfico que se origina en redes externas a la red corporativa. Se permite el acceso de tráfico remoto a la red corporativa si el tráfico establecido se originó en la red interna. Se permiten mensajes de respuesta ICMP para fines de resolución de problemas.

a. ¿Se puede hacer ping de la PC-A a la PC-C?

b. Examine el router HQ y vea el resumen de la ACL 102 para encontrar posibles errores de configuración. Introduzca el comando **show access-lists 102**.

```
HQ# show access-lists 102
Extended IP access list 102
    10 permit tcp any any established
```



```
    20 permit icmp any any echo-reply
    30 permit icmp any any unreachable
    40 deny ip any any (57 matches)
```

c. ¿Existe algún problema en la ACL 102?

d. Verifique que la ACL 102 esté aplicada en el sentido correcto en la interfaz G0/1. Introduzca el comando **show ip interface g0/1**.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  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
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 101
  Inbound  access list is 101
```

e. ¿Existe algún problema con la aplicación de la ACL 102 a la interfaz G0/1?

f. Corrija los errores encontrados con respecto a la ACL 102. Registre los comandos usados para corregir los errores.

g. ¿Se puede hacer ping de la PC-A a la PC-C ahora?

Parte 3: resolver problemas de acceso remoto

En la parte 3, ACL 121 está configurada para impedir ataques de suplantación (spoofing) provenientes de redes externas y para permitir solo acceso HTTP remoto al servidor web (192.168.4.1) en la DMZ.

a. Verifique que la ACL 121 esté configurada correctamente. Introduzca el comando **show ip access-list 121**.

```
HQ# show ip access-lists 121
Extended IP access list 121
    10 permit tcp any host 192.168.4.1 eq 89
    20 deny icmp any host 192.168.4.11
    30 deny ip 192.168.1.0 0.0.0.255 any
    40 deny   ip 127.0.0.0 0.255.255.255 any
    50 deny   ip 224.0.0.0 31.255.255.255 any
    60 permit ip any any (354 matches)
    70 deny ip any any
```

¿Existe algún problema en esta ACL?

b. Realizar y registre los cambios de configuración necesarios a la ACL 121.

c. Verifique que la ACL 121 se aplique en la dirección correcta en la interfaz HQ S0/0/1. Introduzca el comando **show ip interface s0/0/1**.

```
HQ# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.1.2/30
  Broadcast address is 255.255.255.255
<se omitió el resultado>
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is 121
```

¿Existe algún problema con la aplicación de esta ACL?

d. Verifique que la PC-C solo pueda acceder al servidor web simulado en el HQ mediante el navegador web. Para acceder al servidor web (192.168.4.1), proporcione el nombre de usuario **admin** y la contraseña **adminpass**.

Parte 4: Solucionar problemas en ACL de IPv6

En la parte 4, una ACL de IPv6 llamado NO-ICMP deniega el tráfico ICMP a la DMZ y a la red corporativa que se originan en el exterior. La respuesta del ICMP a los hosts internos, los paquetes EIGRP, y el tráfico relacionado red se permiten en redes externas. Además, la red externa tiene permitido el acceso al servidor web DMZ (simulado por Lo0 en HQ).

a. Verifique que la ACL **NO-ICMP** se haya configurado correctamente. Introduzca el comando **show ipv6 access-list NO-ICMP**.

```
Access-list NO-ICMP show ipv6 de HQ#
IPv6 access list NO-ICMP
    deny icmp any any secuencia 10 de solicitud de eco
permit ipv6 any any sequence 20
```

¿Existe algún problema en esta ACL?

b. Verifique que la ACL NO-ICMP se aplique en la dirección correcta en la interfaz HQ S0/0/1. Introduzca el comando **show ipv6 interface s0/0/1**.

```
HQ# show ipv6 interface s0/0/1
Serial0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::2
```



```
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::A
  FF02::1:FF00:1
  FF02::1:FF00:2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
Funciones de resultados: Lista de acceso
Outgoing access list NO-ICMP
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND RAs are suppressed (periodic)
Hosts use stateless autoconfig for addresses.
```

¿Existe algún problema con la aplicación de esta ACL?

c. Realizar y registre los cambios de configuración necesarios a ACL NO-ICMP.

Reflexión

1. ¿Cómo se debería ordenar la instrucción de ACL, de lo general a lo específico o viceversa?

2. Si elimina una ACL con el comando **no access-list** y la ACL sigue aplicada a la interfaz, ¿qué sucede?

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.

