Práctica de laboratorio: configuración y verificación de restricciones de VTY

Topología

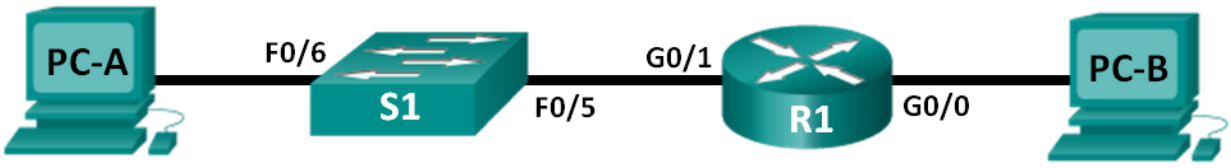

Tabla de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/D
	G0/1	192.168.1.1	255.255.255.0	N/D
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objetivos

Parte 1: Configurar los parámetros básicos de los dispositivos

Parte 2: configurar y aplicar la lista de control de acceso en el R1

Parte 3: verificar la lista de control de acceso mediante Telnet

Parte 4: configurar y aplicar la lista de control de acceso en el S1 (desafío)

Aspectos básicos/situación

Es aconsejable restringir el acceso a las interfaces de administración del router, como las líneas de consola y las líneas vty. Se puede utilizar una lista de control de acceso (ACL) para permitir el acceso de direcciones IP específicas, lo que asegura que solo la computadora del administrador tenga permiso para acceder al router mediante telnet o SSH.

Nota: En los resultados de los dispositivos Cisco, ACL se abrevia como access-list (lista de acceso).

En esta práctica de laboratorio, creará y aplicará una ACL estándar con nombre para restringir el acceso remoto a las líneas vty del router.

Después de crear y aplicar la ACL, probará y verificará la ACL intentando acceder al router desde diferentes direcciones IP mediante Telnet.

En esta práctica de laboratorio se le proporcionarán los comandos necesarios para crear y aplicar la ACL.

Nota: Los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 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

- 1 router (Cisco 1941 con Cisco IOS versión 15.2(4)M3, imagen universal o similar)
- 1 switch (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, como se muestra en la topología

Nota: las interfaces Gigabit Ethernet en los routers Cisco de la serie 1941 tienen detección automática, y se puede utilizar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable Ethernet cruzado.

Parte 1. Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y configurará las direcciones IP de las interfaces, el acceso a los dispositivos y las contraseñas del router.

Paso 1. Realice el cableado de red tal como se muestra en el diagrama de topología.

Paso 2. configurar los parámetros de red de la PC-A y la PC-A, según la tabla de direccionamiento.

Paso 3. Inicializar y volver a cargar el router y el switch.

a. Acceda al router e ingrese al modo de configuración global.

b. Copie la siguiente configuración básica y péguela en la configuración en ejecución en el router.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. Configure las direcciones IP en las interfaces que se indican en la tabla de direccionamiento.

d. Guarde la configuración en ejecución en el archivo de configuración de inicio.

e. Acceda al switch mediante el puerto de consola e ingrese al modo de configuración global.

f. Copie la siguiente configuración básica y péguela en la configuración en ejecución en el switch.

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

g. Configure las direcciones IP en la interfaz de VLAN1 que se indican en la tabla de direcciones.

h. Configure el gateway predeterminado para el switch.

i. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Parte 2. configurar y aplicar la lista de control de acceso en el R1

En la parte 2, configurará una ACL estándar con nombre y la aplicará a las líneas de terminal virtual del router para restringir el acceso remoto al router.

Paso 1. configurar y aplicar una ACL estándar con nombre.

a. Acceda al router R1 mediante el puerto de consola y habilite el modo EXEC privilegiado.

b. En el modo de configuración global, use un espacio y un signo de interrogación para ver las opciones de comandos de **ip access-list**.

```
R1(config)# ip access-list ?
  extended    Extended Access List
  helper      Access List acts on helper-address
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence Access List
  standard    Standard Access List
```

c. Use un espacio y un signo de interrogación para ver las opciones de comandos de **ip access-list standard**.

```
R1(config)# ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
```

d. Agregue **ADMIN-MGT** al final del comando **ip access-list standard** y presione Enter. Ahora se encuentra en el modo de configuración de listas de acceso estándar con nombre (config-std-nacl).

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)#
```


e. Introduzca la entrada de control de acceso (ACE) permit o deny de su ACL, también conocida como "instrucción de ACL", de a una línea por vez. Recuerde que al final de la ACL hay una instrucción implícita **deny any**, que deniega todo el tráfico. Introduzca un signo de interrogación para ver las opciones de comandos.

```
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
```

f. Cree una ACE permit para la PC-A de Administrador en 192.168.1.3 y una ACE permit adicional para admitir otras direcciones IP administrativas reservadas desde 192.168.1.4 hasta 192.168.1.7. Observe que la primera ACE permit indica un único host pues usa la palabra clave **host**. Se podría haber usado la ACE **permit 192.168.1.3 0.0.0.0** en lugar de esta. La segunda ACE permit admite los hosts 192.168.1.4 a 192.168.1.7 debido a que se usa el carácter comodín 0.0.0.3, que es lo inverso de la máscara de subred 255.255.255.252.

```
R1(config-std-nacl)# permit host 192.168.1.3
R1(config-std-nacl)# permit 192.168.1.4 0.0.0.3
R1(config-std-nacl)# exit
```

No es necesario introducir una ACE deny, porque hay una ACE **deny any** implícita al final de la ACL.

g. Ahora que creó una ACL con nombre, aplíquela a las líneas vty.

```
R1(config)# line vty 0 15
R1(config-line)# access-class ADMIN-MGT in
R1(config-line)# exit
```

Parte 3. verificar la lista de control de acceso mediante Telnet

En la parte 3, usará Telnet para acceder al router y verificar que la ACL con nombre funcione correctamente.

Nota: SSH es más seguro que Telnet; sin embargo, SSH requiere que el dispositivo de red esté configurado para aceptar conexiones SSH. En esta práctica de laboratorio, se usa Telnet por cuestiones de facilidad.

a. Abra un símbolo del sistema en la PC-A y verifique que pueda comunicarse con el router mediante el comando **ping**.

```
C:\Users\user1> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\Users\user1>
```

b. Use el símbolo del sistema de la PC-A para iniciar el programa cliente de Telnet y acceda al router mediante telnet. Introduzca los datos de inicio de sesión y luego las contraseñas de enable. Debería haber iniciado sesión correctamente, visto el mensaje de aviso y recibido una petición de entrada de comandos del R1.

```
C:\Users\user1> telnet 192.168.1.1

Unauthorized access is prohibited!

User Access Verification

Password:
R1>enable
Contraseña:
R1#
```

¿La conexión Telnet se realizó correctamente?

_____

c. Escriba **exit** en el símbolo del sistema y presione Enter para salir de la sesión de Telnet.

d. Cambie la dirección IP para comprobar si la ACL con nombre bloquea direcciones IP no permitidas. Cambie la dirección IPv4 a 192.168.1.100 en la PC-A.

e. Intente acceder al R1 mediante telnet en 192.168.1.1 otra vez. ¿La sesión de Telnet se estableció correctamente?

_____

¿Qué mensaje recibió? _____

f. Cambie la dirección IP de la PC-A para comprobar si la ACL con nombre permite que un host con una dirección IP en el rango de 192.168.1.4 a 192.168.1.7 acceda al router mediante telnet. Después de cambiar la dirección IP de la PC-A, abra el símbolo del sistema de Windows e intente acceder al router R1 mediante telnet.

¿La sesión de Telnet se estableció correctamente?

_____

_____

g. En el modo EXEC privilegiado en el R1, escriba el comando **show ip access-lists** y presione Enter. En el resultado del comando, observe la forma en que el IOS de Cisco asigna automáticamente los números de línea a las ACE de la ACL en incrementos de 10 y muestra la cantidad de veces que se encontraron coincidencias para cada ACE permit (entre paréntesis).

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
```

Debido a que se establecieron correctamente dos conexiones Telnet al router y cada sesión de Telnet se inició desde una dirección IP que coincide con una de las ACE permit, hay coincidencias para cada ACE permit.

¿Por qué piensa que hay dos coincidencias para cada ACE permit cuando se inició solo una conexión desde cada dirección IP?

_____

_____

_____

_____

¿De qué forma determinaría el momento en el que el protocolo Telnet ocasiona las dos coincidencias durante la conexión Telnet?

_____

_____

_____

h. En el R1, ingrese al modo de configuración global.

i. Ingrese al modo de configuración de lista de acceso para la lista de acceso con nombre ADMIN-MGT y agregue una ACE **deny any** al final de la lista de acceso.

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
```

Nota: Dado que hay una ACE **deny any** implícita al final de todas las ACL, agregar una ACE **deny any** explícita es innecesario. Sin embargo, el deny any explícito al final de la ACL puede ser útil para que el administrador de red registre o, simplemente, conozca la cantidad de veces que coincidió la ACE de lista de acceso **deny any**.

j. Intente acceder al R1 mediante telnet desde la PC-B. Esto crea una coincidencia con la ACE **deny any** en la lista de acceso con nombre ADMIN-MGT.

k. En el modo EXEC privilegiado, escriba el comando **show ip access-lists** y presione Enter. Ahora debería ver varias coincidencias con la ACE **deny any**.

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
    30 deny any (3 matches)
```

La conexión Telnet fallida produce más coincidencias con la ACE deny explícita que una conexión correcta. ¿Por qué cree que sucede esto?

_____

_____

Parte 4. configurar y aplicar la lista de control de acceso en el S1 (desafío)

Paso 1. configurar y aplicar una ACL estándar con nombre para las líneas vty en el S1.

a. Sin consultar los comandos de configuración del R1, intente configurar la ACL en el S1 y permita solo la dirección IP de la PC-A.

b. Aplique la ACL a las líneas vty del S1. Recuerde que hay más líneas vty en un switch que en un router.

Paso 2. probar la ACL de vty en el S1.

Acceda mediante Telnet desde cada una de las computadoras para verificar que la ACL de vty funcione correctamente. Debería poder acceder al S1 mediante telnet desde la PC-A, pero no desde la PC-B.

Reflexión

1. Como lo demuestra el acceso remoto a vty, las ACL son filtros de contenido eficaces que tienen una aplicación más allá de las interfaces de red de entrada y de salida. ¿De qué otras formas se pueden aplicar las ACL?

   _____

   _____

2. ¿La aplicación de una ACL a una interfaz de administración remota de vty mejora la seguridad de una conexión Telnet? ¿Esto convierte a Telnet en una herramienta de administración de acceso remoto más viable?

   _____

   _____

   _____

3. ¿Por qué tiene sentido aplicar una ACL a las líneas vty, en vez de a interfaces específicas?

   _____

   _____

   _____

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 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 un comando de Cisco IOS para representar la interfaz.