**Actividad 5.2.8:   
Configuración de las ACL estándar**

**NOTA PARA EL USUARIO:** Si bien puede completar esta actividad sin instrucciones impresas, se ofrece una versión en PDF en la sección de texto de la misma página desde la que inició esta actividad.

**Tabla de direccionamiento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dispositivo** | **Interfaz** | **Dirección IP** | **Máscara de subred** |
| **R1** | **S0/0/0** | 10.1.1.1 | 255.255.255.252 |
| **Fa0/0** | 192.168.10.1 | 255.255.255.0 |
| **Fa0/1** | 192.168.11.1 | 255.255.255.0 |
| **R2** | **S0/0/0** | 10.1.1.2 | 255.255.255.252 |
| **S0/0/1** | 10.2.2.1 | 255.255.255.252 |
| **S0/1/0** | 209.165.200.225 | 255.255.255.224 |
| **Fa0/0** | 192.168.20.1 | 255.255.255.0 |
| **R3** | **S0/0/1** | 10.2.2.2 | 255.255.255.252 |
| **Fa0/0** | 192.168.30.1 | 255.255.255.0 |
| **ISP** | **S0/0/1** | 209.165.200.226 | 255.255.255.224 |
| **Fa0/0** | 209.165.201.1 | 255.255.255.224 |
| **Fa0/1** | 209.165.202.129 | 255.255.255.224 |
| **PC1** | **NIC** | 192.168.10.10 | 255.255.255.0 |
| **PC2** | **NIC** | 192.168.11.10 | 255.255.255.0 |
| **PC3** | **NIC** | 192.168.30.10 | 255.255.255.0 |
| **PC4** | **NIC** | 192.168.30.128 | 255.255.255.0 |
| **Servidor WEB/TFTP** | **NIC** | 192.168.20.254 | 255.255.255.0 |
| **Servidor WEB** | **NIC** | 209.165.201.30 | 255.255.255.224 |
| **Host externo** | **NIC** | 209.165.202.158 | 255.255.255.224 |

**Objetivos de aprendizaje**

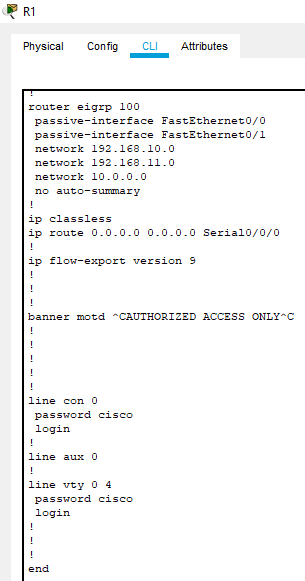
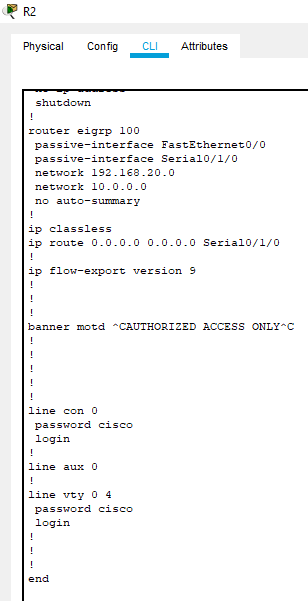
* Investigar la configuración actual de la red
* Evaluar una política de red y planificar una implementación de ACL
* Configurar ACL estándar numeradas
* Configurar ACL estándar nombradas

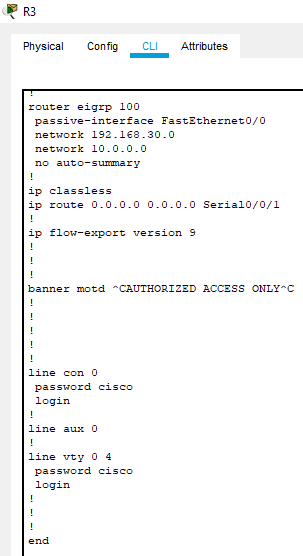
**Introducción**

Las ACL estándar son guiones de configuración del router que controlan si un router acepta o rechaza paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, lo que incluye direcciones IP y enrutamiento EIGRP. La contraseña EXEC del usuario es **cisco** y la contraseña EXEC privilegiada es**class**.

**Tarea 1: Investigar la configuración actual de la red**

Se puede observar que los Routers tienen una configuración eigrp 100, esto se pudo observar por el comando **show run**

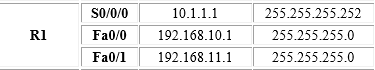




**Paso 1. Visualizar la configuración en ejecución en los routers.**

Visualice las configuraciones en ejecución en los tres routers por medio del comando **show running-config** mientras está en el modo EXEC privilegiado. Observe que las interfaces y el enrutamiento están totalmente configurados. Compare las configuraciones de la dirección IP con la tabla de direccionamiento que se muestra más arriba. En este momento, no debe haber ninguna ACL configurada en los routers.

El router ISP no requiere ninguna configuración durante este ejercicio. Supongamos que el router ISP no está bajo su administración y el administrador del ISP se ocupa de su configuración y mantenimiento.

**Router 1**

**Comparación:**

Tabla Show run

S0/0/0 S0/0/0

10.1.1.1 255.255.255.252 10.1.1.1 255.255.255.252

Fa0/0 Fa0/0

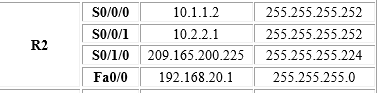
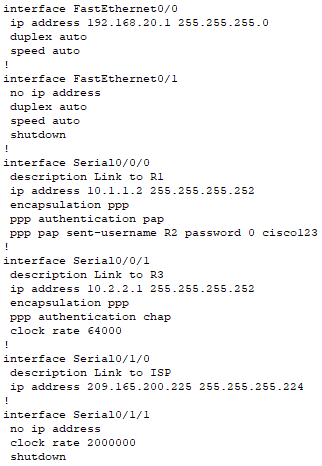
192.168.10.1 255.255.255.0 192.168.10.1 255.255.255.0

Fa0/1 Fa0/1

192.168.11.1 255.255.255.0 192.168.11.1 255.255.255.0

S0/0/1

clock rate 2000000

**Router 2**

**Comparación:**

Tabla Show run

S0/0/0 S0/0/0

10.1.1.2 255.255.255.252 10.1.1.2 255.255.255.252

S0/0/1 S0/0/1

10.2.2.1 255.255.255.252 10.2.2.1 255.255.255.252

S0/1/0 S0/1/0

209.165.200.225 255.255.255.224 209.165.200.225 255.255.255.224

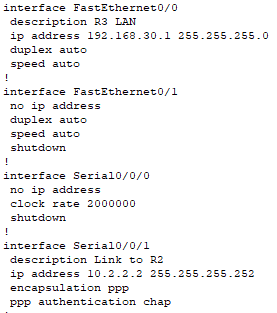
Fa0/0 Fa0/0

192.168.20.1 255.255.255.0 192.168.20.1 255.255.255.0

S0/1/1

clock rate 2000000

**Router 3**



**Comparación:**

Tabla Show run

S0/0/01 S0/0/1

10.2.2.2 255.255.255.252 10.2.2.2 255.255.255.252

Fa0/0 Fa0/0

192.168.30.1 255.255.255.0 192.168.30.1 255.255.255.0

S0/0/0

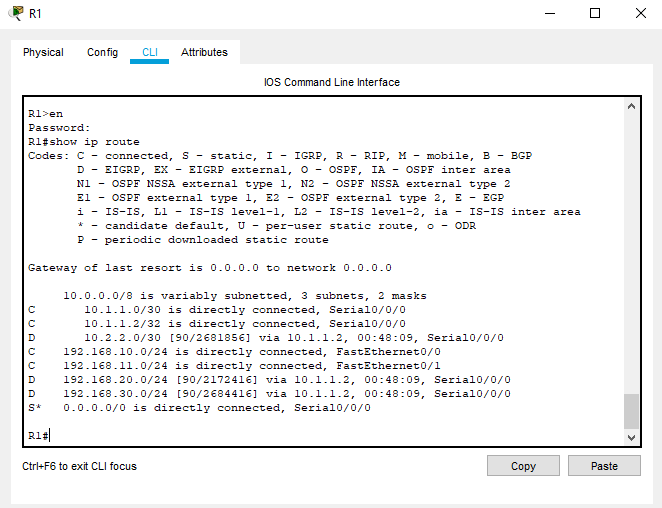
clock rate 2000000

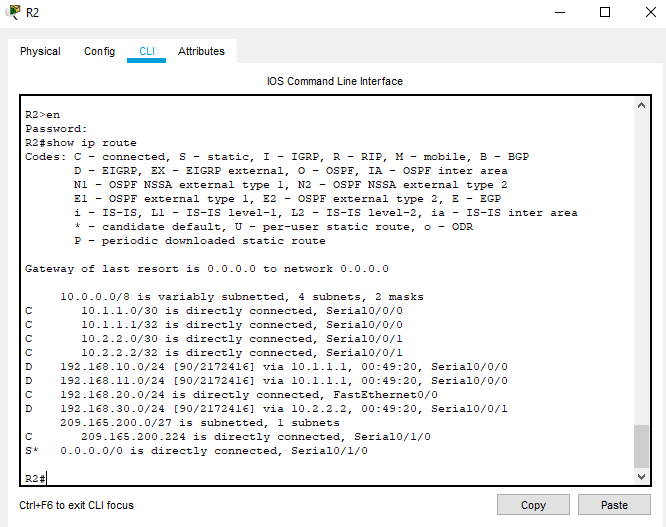
**Paso 2. Confirmar que todos los dispositivos puedan acceder a todas las demás ubicaciones.**

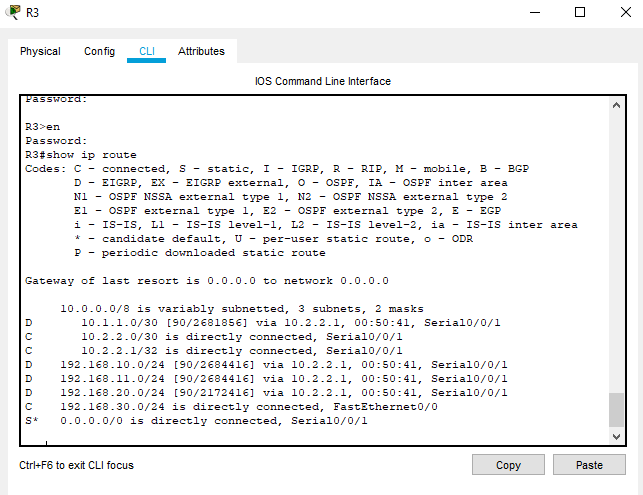
Antes de aplicar cualquier ACL a una red, es importante confirmar que exista conectividad completa. Si no prueba la conectividad en su red antes de aplicar una ACL, probablemente la resolución de problemas sea más difícil.

Un paso útil en la prueba de conectividad es visualizar las tablas de enrutamiento en cada dispositivo para asegurarse de que cada red figure en éstas. En R1, R2 y R3 ejecute el comando **show ip route**. Debe ver que cada dispositivo tiene rutas conectadas para redes conectadas y rutas dinámicas a todas las demás redes remotas. Todos los dispositivos pueden acceder a todas las demás ubicaciones.

**Comando show ip route**

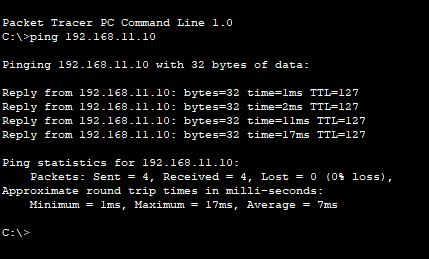




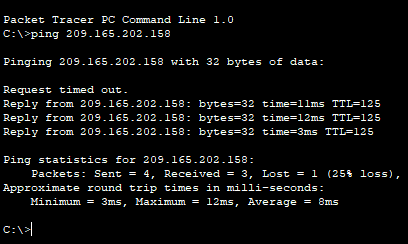


Aunque la tabla de enrutamiento puede ser útil para evaluar el estado de la red, la conectividad aún debe probarse al hacer **ping**. Realice las siguientes pruebas:

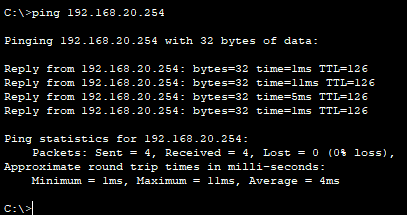
 Desde la PC1, haga ping a la PC2.



 Desde la PC2, haga ping al host externo.



 Desde la PC4, haga ping al servidor Web/TFTP.



Cada una de estas pruebas de conectividad debe tener éxito.

**Tarea 2: Evaluar una política de red y planificar una implementación de ACL**

**Paso 1. Evaluar la política para las LAN del R1.**

* La red 192.168.10.0/24 puede acceder a todas las ubicaciones, excepto a la red 192.168.11.0/24.
* La red 192.168.11.0/24 puede acceder a todos los demás destinos, excepto a cualquier red conectada al ISP.

**Paso 2. Planificar la implementación de ACL para las LAN del R1.**

* Dos ACL implementan completamente la política de seguridad para las LAN del R1.
* La primera ACL en el R1 deniega el tráfico desde la red 192.168.10.0/24 a la red 192.168.11.0/24, pero permite el resto del tráfico.
* Esta primera ACL, aplicada en dirección de salida en la interfaz Fa0/1, monitorea el tráfico  que se envía a la red 192.168.11.0.
* La segunda ACL, ubicada en el R2, deniega a la red 192.168.11.0/24 el acceso al ISP, pero permite el resto del tráfico.
* El trafico saliente desde la interfaz S0/1/0 en R2 está controlado.
* Coloque las sentencias ACL en orden, desde la más específica a la menos específica. Primero se deniega el acceso del tráfico de la red a otra red antes de permitir el acceso del resto del tráfico.

**Paso 3. Evaluar la política para la LAN del R3.**

* La red 192.168.30.0/10 puede acceder a todos los destinos.
* El host 192.168.30.128 no tiene permitido el acceso fuera de la LAN.

**Paso 4. Planificar la implementación de ACL para la LAN del R3.**

* Una ACL implementa completamente la política de seguridad para la LAN del R3.
* La ACL se coloca en el R3 y deniega al host 192.168.30.128 el acceso fuera de la LAN, pero permite el tráfico desde todos los demás hosts de la LAN.
* Al aplicar una ACL entrante en la interfaz Fa0/0, esta ACL monitoreará todo el tráfico que intente salir de la red 192.168.30.0/10.
* Coloque las sentencias ACL en orden, desde la más específica a la menos específica. Primero se deniega el acceso al host 192.168.30.128 antes que permitir el acceso al resto del tráfico.

**Tarea 3: Configurar ACL estándar numeradas**

**Paso 1. Determinar la máscara wildcard.**

La máscara wildcard en una sentencia ACL determina cuánto se debe verificar en una dirección IP de origen o destino. Un bit 0 implica hacer coincidir ese valor en la dirección, mientras que un bit 1 ignora ese valor en la dirección. Recuerde que las ACL estándar sólo pueden verificar direcciones de origen.

* Debido a que la ACL en el R1 deniega todo el tráfico de la red 192.168.10.0/24, se rechazará toda dirección IP de origen que comience con 192.168.10. Dado que el último octeto de la dirección IP puede ignorarse, la máscara wildcard correcta es 0.0.0.255. Cada octeto en esta máscara puede interpretarse como “verificar, verificar, verificar, ignorar”.
* La ACL en el R2 también deniega el tráfico de la red 192.168.11.0/24. Puede aplicarse la misma máscara wildcard, 0.0.0.255.

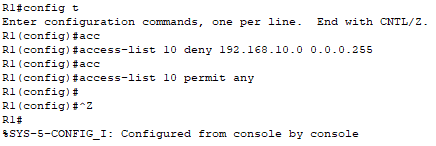
**Paso 2. Determinar las sentencias.**

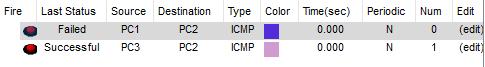
* Las ACL se configuran en el modo de configuración global.
* Para las ACL estándar, use un número entre 1 y 99. El número **10** se usa para esta lista en el R1 para ayudar a recordar que esta ACL monitorea la red 192.168.**10**.0.
* En el R2, la lista de acceso **11** deniega el tráfico de la red 192.168.**11**.0 a cualquier red ISP; por lo tanto, la opción deny está configurada con la red **192.168.11.0** y la máscara wildcard **0.0.0.255**.
* Debe permitirse el resto del tráfico con la opción **permit** debido a la sentencia implícita “deny any” al final de las ACL. La opción **any** especifica a todo host de origen.

Configure lo siguiente en R1:

R1(config)#**access-list 10 deny 192.168.10.0 0.0.0.255**

R1(config)#**access-list 10 permit any**



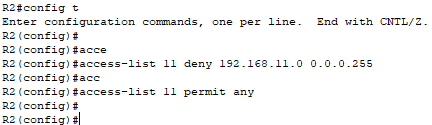


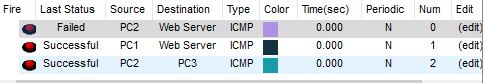
Nota: Packet Tracer no calificará una configuración de ACL hasta que todas las sentencias se ingresen en el orden correcto.

Ahora cree una ACL en el R2 para denegar la red 192.168.11.0 y permitir las demás redes. Para esta ACL, use el número 11. Configure lo siguiente en R2:

R2(config)#**access-list 11 deny 192.168.11.0 0.0.0.255**

R2(config)#**access-list 11 permit any**





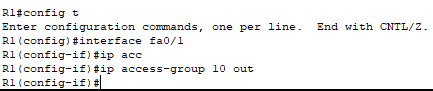
**Paso 3. Aplicar las sentencias a las interfaces.**

En R1, ingrese al modo de configuración para la interfaz Fa0/1.

Ejecute el comando **ip access-group 10 out** para aplicar la ACL estándar saliente en la interfaz.

R1(config)#**interface fa0/1**

R1(config-if)#**ip access-group 10 out**



En R2, ingrese al modo de configuración para la interfaz S0/1/0.

Ejecute el comando **ip access-group 11 out** para aplicar la ACL estándar saliente en la interfaz

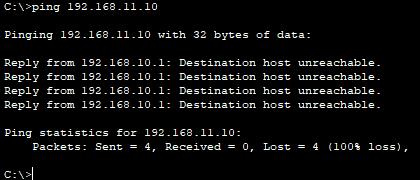
R2(config)#**interface s0/1/0**

R2(config-if)#**ip access-group 11 out**

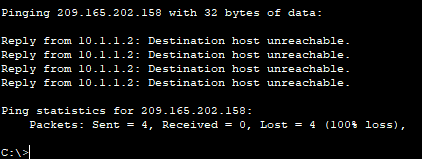


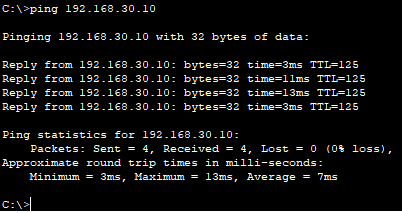
**Paso 4. Verificar y probar las ACL.**

Con las ACL configuradas y aplicadas, la PC1 (192.168.10.10) no debe poder hacer ping a la PC2 (192.168.11.10), ya que la ACL 10 se aplica con dirección de salida en la Fa0/1 en R1.

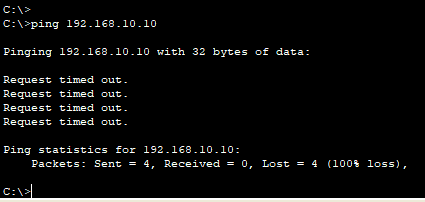


La PC2 (192.168.11.10) no debe poder hacer ping al servidor Web (209.165.201.30) ni al host externo (209.165.202.158), pero sí debe poder hacer ping a cualquier otra ubicación, ya que la ACL 11 se aplica en dirección de salida en la S0/1/0 en R2.





Sin embargo, la PC2 no puede hacer ping a la PC1 porque la ACL 10 en R1 impide la respuesta de eco desde la PC1 a la PC2.



**Paso 5. Verificar los resultados.**

Su porcentaje de finalización debe ser del 67%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

**Tarea 4: Configurar una ACL estándar nombrada**

**Paso 1. Determinar la máscara wildcard.**

* La política de acceso para R3 indica que el host en 192.168.30.128 no debe tener permitido ningún acceso fuera de la LAN local. El resto de los hosts de la red 192.168.30.0 deben tener permitido el acceso a las demás ubicaciones.
* Para verificar un único host, debe verificarse la dirección IP completa mediante la palabra clave host.
* Se permiten todos los paquetes que no coinciden con la sentencia host.

**Paso 2. Determinar las sentencias.**

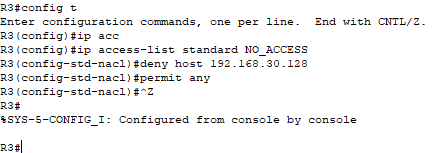
* En R3, entre al modo de configuración global.
* Cree una ACL nombrada con la denominación NO\_ACCESS mediante el comando ip access-list standard NO\_ACCESS. Ingresará al modo de configuración de ACL. Todas las sentencias permit y deny se configuran desde este modo de configuración.
* Deniegue el tráfico desde el host 192.168.30.128 con la opción host.
* Permita todo el tráfico restante con permit any.

Configure la siguiente ACL nombrada en R3:

R3(config)#**ip access-list standard NO\_ACCESS**

R3(config-std-nacl)#**deny host 192.168.30.128**

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

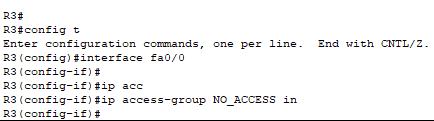


**Paso 3. Aplicar las sentencias a la interfaz correcta.**

Ejecute el comando **ip access-group NO\_ACCESS in** para aplicar la ACL nombrada entrante en la interfaz. Este comando hace que todo el tráfico que ingresa a la interfaz Fa0/0 desde la LAN 192.168.30.0/24 se compare con la ACL.

R3(config)#**interface fa0/0**

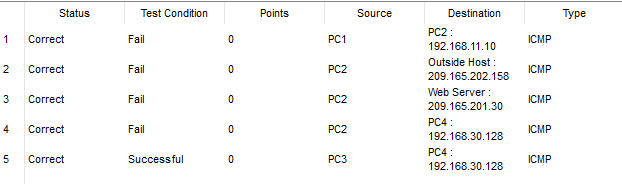
R3(config-if)#**ip access-group NO\_ACCESS in**



**Paso 4. Verificar y probar las ACL.**

Haga clic en **Verificar resultados** y luego en**Pruebas de conectividad**. Las siguientes pruebas deben fallar:

* PC1 a PC2
* PC2 a host externo
* PC2 a Servidor Web
* Todos los pings desde la PC4 y hacia ésta, excepto entre la PC3 y la PC4



**Paso 5. Verificar los resultados.**

Su porcentaje de finalización debe ser del 100%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

