**Actividad 5.3.4:   
Configuración de las ACL extendidas**

**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** | 10.2.2.2 | 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** | 10.2.2.1 | 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 las ACL extendidas numeradas
* Configurar las ACL extendidas nombradas

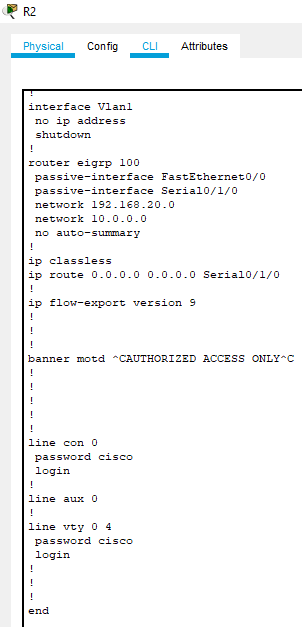
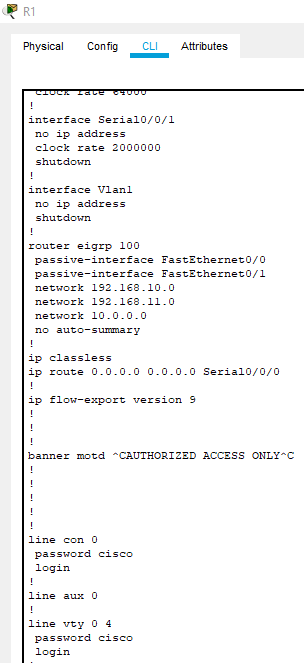
**Introducción**

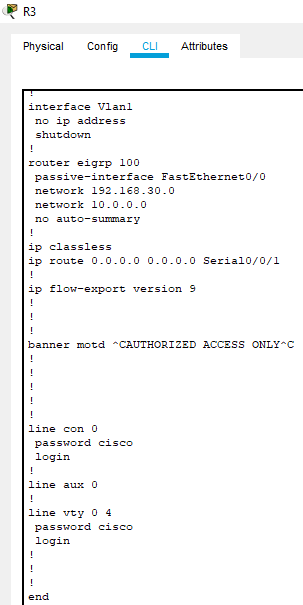
Las ACL extendidas son guiones de configuración del router que controlan si un router acepta o rechaza paquetes según la dirección de origen o destino y protocolos o puertos. Las ACL extendidas proporcionan mayor flexibilidad y especificidad que las ACL estándar. Esta actividad se concentra en definir criterios de filtrado, configurar ACL extendidas, 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**

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

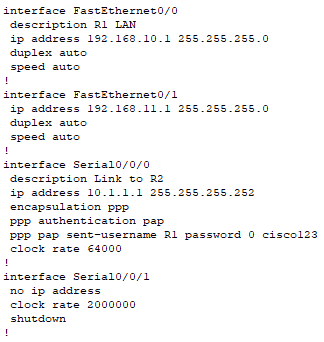
Visualice las configuraciones en ejecución en los tres routers por medio del comando **show running-config**mientras está en el modo EXEC privilegiado. Observe que las interfaces y el enrutamiento están totalmente configurados. Compare las configuraciones de la dirección IP con la tabla de direccionamiento 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. Se supone 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

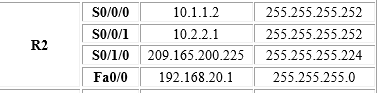
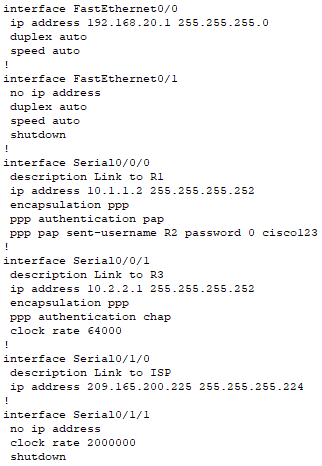
192.168.10.1 255.255.255.0 192.168.10.1 255.255.255.0

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

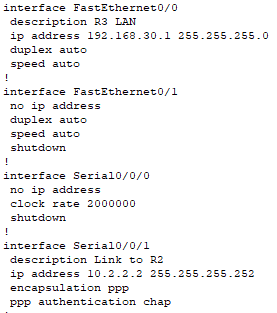
Fa0/0 Fa0/0

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

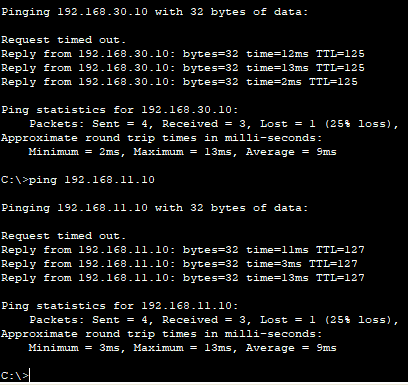
S0/0/0

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, la resolución de problemas será muy difícil.

A fin de asegurar la conectividad a lo largo de toda la red, utilice los comandos **ping** y **tracert** entre diferentes dispositivos de red para verificar las conexiones.



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

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

* Para la red 192.168.10.0/24, bloquee el acceso Telnet a todas las ubicaciones y el acceso TFTP al servidor Web/TFTP corporativo en 192.168.20.254. Se permite todo el acceso restante.
* Para la red 192.168.11.0/24, permita el acceso TFTP y el acceso Web al servidor Web/TFTP corporativo en 192.168.20.254. Bloquee el resto del tráfico de la red 192.168.11.0/24 a la red 192.168.20.0/24. Se permite todo el acceso restante.

**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 mantiene la primera parte de la política, se configura en R1 y se aplica con dirección de entrada a la interfaz Fast Ethernet 0/0.
* La segunda ACL mantiene la segunda parte de la política, se configura en R1 y se aplica con dirección de entrada a la interfaz Fast Ethernet 0/1.

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

* Todas las direcciones IP de la red 192.168.30.0/24 tienen bloqueado el acceso a todas las direcciones IP de la red 192.168.20.0/24.
* La primera mitad de 192.168.30.0/24 puede acceder a todos los demás destinos.
* La segunda mitad de 192.168.30.0/24 puede acceder a las redes 192.168.10.0/24 y 192.168.11.0/24.
* La segunda mitad de 192.168.30.0/24 tiene permitido el acceso Web e ICMP a todos los demás destinos.
* El resto del acceso está implícitamente denegado.

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

Este paso requiere una ACL configurada en R3 y aplicada con dirección de entrada a la interfaz Fast Ethernet 0/0.

**Paso 5. Evaluar la política para el tráfico proveniente de Internet a través del ISP.**

* Los hosts externos pueden establecer una sesión de Web con el servidor Web interno únicamente en el puerto 80.
* Se permiten únicamente las sesiones TCP establecidas.
* A través del R2 solamente se permiten respuestas de ping.

**Paso 6. Planificar las implementaciones de ACL para el tráfico proveniente de Internet a través del ISP.**

Este paso requiere una ACL configurada en R2 y aplicada con dirección de entrada a la interfaz Serial 0/1/0.

**Tarea 3: Configurar ACL extendidas numeradas**

**Paso 1. Determinar las máscaras wildcard.**

Se necesitan dos ACL para implementar la política de control de acceso en R1. Ambas ACL se diseñarán para denegar una red de clase C completa. Se configurará una máscara wildcard que coincide con todos los hosts en cada una de estas redes de clase C.

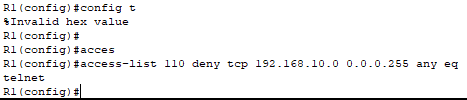
Por ejemplo: para que la subred completa de 192.168.10.0/24 coincida, la máscara wildcard es 0.0.0.255. Esto puede interpretarse como “verificar, verificar, verificar, ignorar” y, básicamente, coincide con la red 192.168.10.0/24 completa.

**Paso 2. Configurar la primera ACL extendida para R1.**

Desde el modo de configuración global, configure la primera ACL con el número 110. En primer lugar, se debe bloquear Telnet a cualquier ubicación para todas las direcciones IP en la red 192.168.10.0/24.

Al escribir la sentencia, asegúrese de estar actualmente en el modo de configuración global.

R1(config)#**access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet**



A continuación, bloquee todas las direcciones IP en la red 192.168.10.0/24 del acceso TFTP al host en 192.168.20.254.

R1(config)#**access-list 110 deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp**



Por último, permita el resto del tráfico.

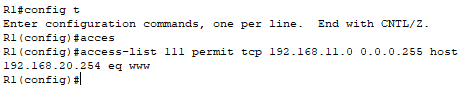
R1(config)#**access-list 110 permit ip any any**



**Paso 3. Configurar la segunda ACL extendida para R1.**

Configure la segunda ACL con el número 111. Permita WWW al host en 192.168.20.254 para cualquier dirección IP en la red 192.168.11.0/24.

R1(config)#**access-list 111 permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www**



A continuación, permita TFTP al host en 192.168.20.254 para cualquier dirección IP en la red 192.168.11.0/24.

R1(config)#**access-list 111 permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp**



Bloquee el resto del tráfico de la red 192.168.11.0/24 a la red 192.168.20.0/24.

R1(config)#**access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255**



Por último, permita cualquier otro tráfico. Esta sentencia garantiza que no se bloquee el tráfico proveniente de otras redes.

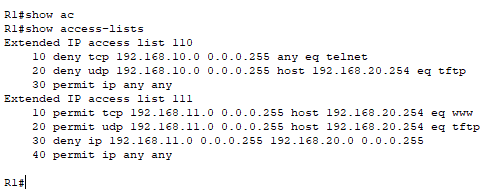
R1(config)#**access-list 111 permit ip any any**



**Paso 4. Verificar las configuraciones de ACL.**

Confirme sus configuraciones en R1 mediante el comando show access-lists. Los resultados serán similares a los siguientes:

R1#**show access-lists** Extended IP access list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp permit ip any any Extended IP access list 111 permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255 permit ip any any



**Paso 5. Aplicar las sentencias a las interfaces.**

Para aplicar una ACL a una interfaz, ingrese al modo de configuración de interfaz para esa interfaz. Configure el comando **ip access-group** *access-list-number* **{in | out}** para aplicar la ACL a la interfaz.

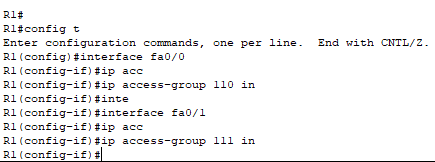
Cada ACL filtra el tráfico entrante. Aplique la ACL 110 a Fast Ethernet 0/0 y la ACL 111 a Fast Ethernet 0/1.

R1(config)#**interface fa0/0**

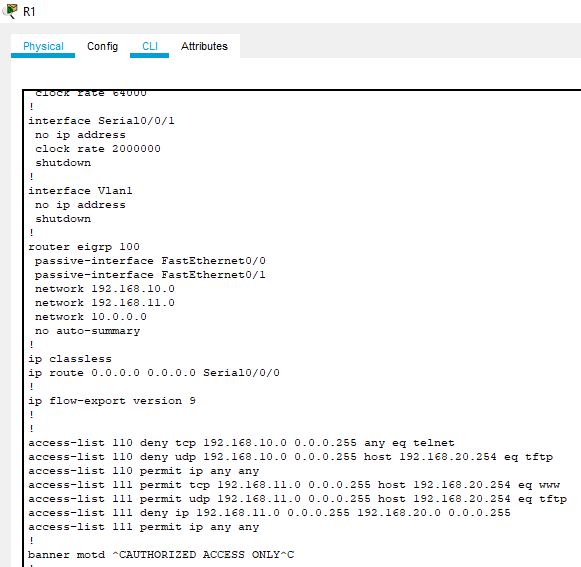
R1(config-if)#**ip access-group 110 in**

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

R1(config-if)#**ip access-group 111 in**



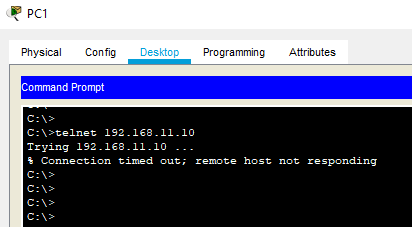
Confirme que las ACL aparezcan en la configuración en ejecución del R1 y que se hayan aplicado a las interfaces correctas.



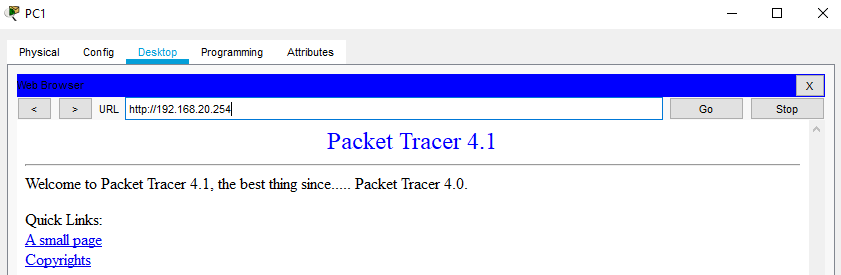
**Paso 6. Probar las ACL configuradas en R1.**

Ahora que las ACL se han configurado y aplicado, es muy importante comprobar que el tráfico esté bloqueado o permitido según lo previsto.

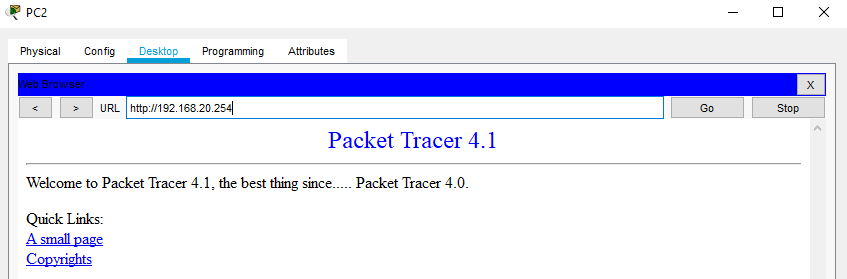
* Desde la PC1, intente obtener acceso Telnet a cualquier dispositivo. Esto debe estar bloqueado.



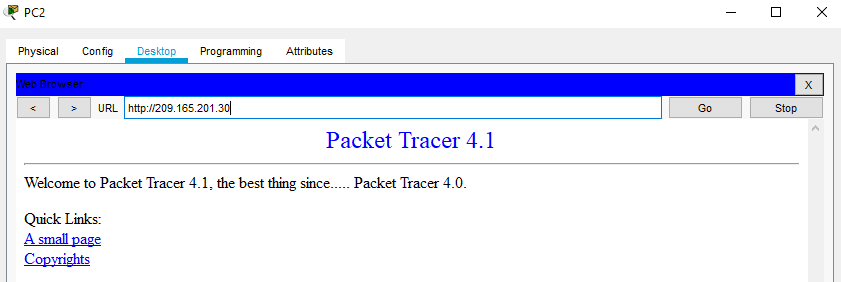
* Desde la PC1, intente acceder al servidor Web/TFTP corporativo a través de HTTP. Esto debe estar permitido.



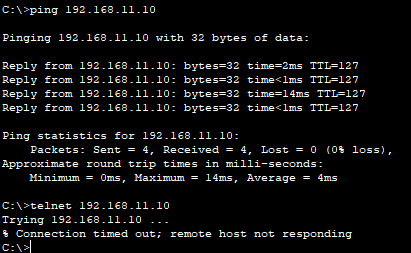
* Desde la PC2, intente acceder al servidor Web/TFTP a través de HTTP. Esto debe estar permitido.



* Desde la PC2, intente acceder al servidor Web externo a través de HTTP. Esto debe estar permitido.



Según su conocimiento sobre ACL, intente algunas otras pruebas de conectividad desde la PC1 y la PC2.



**Paso 7. Verificar los resultados.**

Packet Tracer no admite la prueba del acceso TFTP; por lo tanto, no podrá verificar esa política. Sin embargo, su porcentaje de finalización debe ser del 50%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

**Tarea 4: Configurar una ACL extendida numerada para R3**

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

La política de acceso para la mitad inferior de las direcciones IP en la red 192.168.30.0/24 requiere:

* Denegar el acceso a la red 192.168.20.0/24
* Permitir el acceso a todos los demás destinos.

La mitad superior de las direcciones IP en la red 192.168.30.0/24 tiene las siguientes restricciones:

* Permitir el acceso a 192.168.10.0 y 192.168.11.0
* Denegar el acceso a 192.168.20.0
* Permitir el acceso Web e ICMP a todas las demás ubicaciones.

Para determinar la máscara wildcard, considere qué bits deben verificarse para que la ACL coincida con las direcciones IP 0–127 (mitad inferior) o 128–255 (mitad superior).

Recuerde que una manera de determinar la máscara wildcard es restar la máscara de red normal de 255.255.255.255. La máscara normal para las direcciones IP 0–127 y 128–255 para una dirección de clase C es 255.255.255.128. Mediante el método de sustracción, a continuación se muestra la máscara wildcard correcta:

255.255.255.255 – 255.255.255.128 ------------------ 0. 0. 0.127

**Paso 2. Configurar la ACL extendida en R3.**

En R3, ingrese al modo de configuración global y configure la ACL con 130 como número de lista de acceso.

La primera sentencia bloquea el acceso de la 192.168.30.0/24 a todas las direcciones en la red 192.168.30.0/24.

R3(config)#**access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255**



La segunda sentencia permite que la mitad inferior de la red 192.168.30.0/24 acceda a cualquier otro destino.

R3(config)#**access-list 130 permit ip 192.168.30.0 0.0.0.127 any**

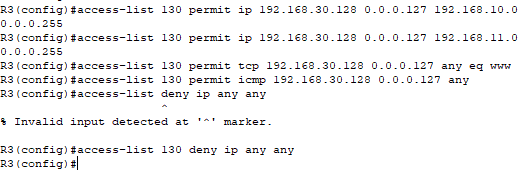


Las sentencias restantes permiten explícitamente que la mitad superior de la red 192.168.30.0/24 acceda a las redes y los servicios que permite la política de red.

R3(config)#**access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0 0.0.0.255**

R3(config)#**access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0 0.0.0.255**

R3(config)#**access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www** R3(config)#**access-list 130 permit icmp 192.168.30.128 0.0.0.127 any** R3(config)#**access-list 130 deny ip any any**

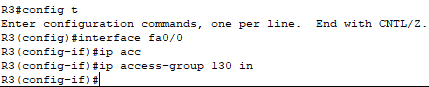


**Paso 3. Aplicar las sentencias a la interfaz.**

Para aplicar una ACL a una interfaz, ingrese al modo de configuración de interfaz para esa interfaz. Configure el comando **ip access-group** *access-list-number* **{in | out}** para aplicar la ACL a la interfaz.

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

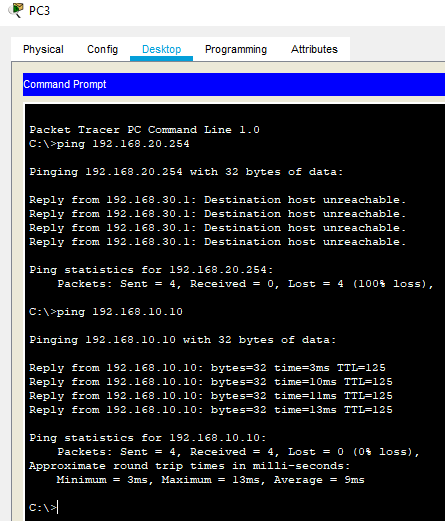
R3(config-if)#**ip access-group 130 in**



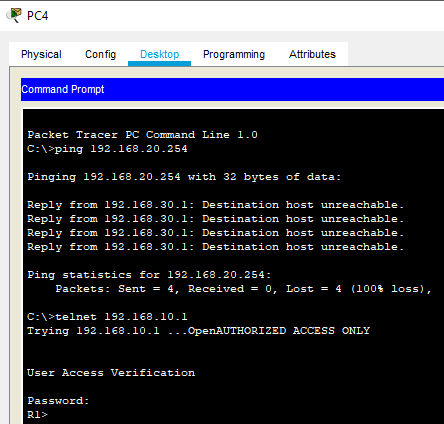
**Paso 4. Verificar y probar las ACL.**

Ahora que la ACL se ha configurado y aplicado, es muy importante comprobar que el tráfico esté bloqueado o permitido según lo previsto.

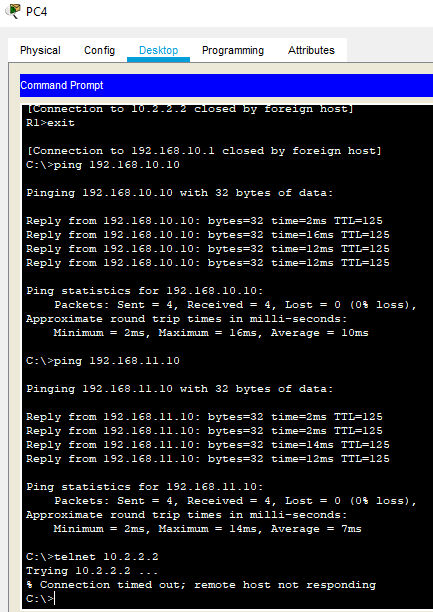
* Desde la PC3, haga ping al servidor Web/TFTP. Esto debe estar bloqueado.
* Desde la PC3, haga ping a cualquier otro dispositivo. Esto debe estar permitido.



* Desde la PC4, haga ping al servidor Web/TFTP. Esto debe estar bloqueado.
* Desde la PC4, haga telnet a R1 en 192.168.10.1 ó 192.168.11.1. Esto debe estar permitido.

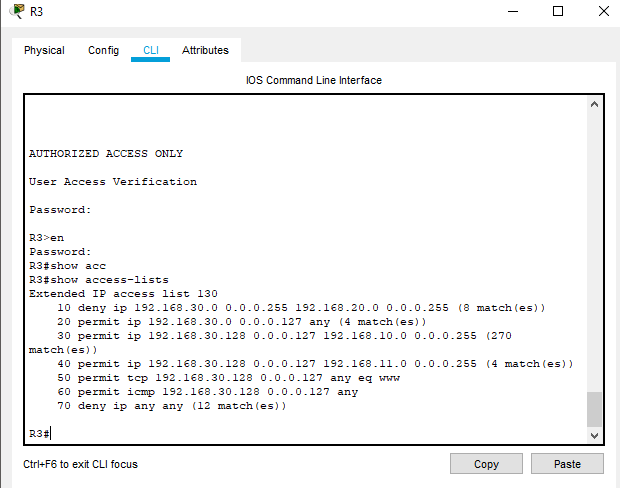


* Desde la PC4, haga ping a la PC1 y la PC2. Esto debe estar permitido.
* Desde la PC4, haga telnet a R2 en 10.2.2.2. Esto debe estar bloqueado.



Después de haber realizado estas pruebas y haber obtenido los resultados correctos, utilice el comando EXEC privilegiado show access-lists en R3 para verificar que las sentencias ACL coincidan.

Según su conocimiento sobre ACL, realice otras pruebas para verificar que cada sentencia coincida con el tráfico correcto.



**Paso 5. Verificar los resultados.**

Su porcentaje de finalización debe ser del 75%. De lo contrario, haga clic en **Verificar resultados** para ver qué componentes requeridos aún no se han completado.

**Tarea 5: Configurar una ACL extendida nombrada**

**Paso 1. Configurar una ACL extendida y nombrada en R2.**

Recuerde que la política en R2 se diseñará para filtrar el tráfico de Internet. Debido a que R2 tiene la conexión al ISP, ésta es la mejor ubicación para la ACL.

Configure una ACL nombrada con la denominación FIREWALL en R2 mediante el comando **ip access-list extended** *name*. Este comando coloca al router en modo de configuración de ACL extendida y nombrada. Observe el indicador del router cambiado.

R2(config)#**ip access-list extended FIREWALL**

R2(config-ext-nacl)#



En el modo de configuración de ACL, agregue las sentencias para filtrar el tráfico tal como se describe en la política:

* Los hosts externos pueden establecer una sesión de Web con el servidor Web interno únicamente en el puerto 80.
* Se permiten únicamente las sesiones TCP establecidas.
* Las respuestas de ping se permiten a través de R2

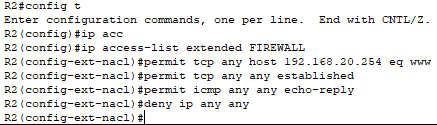
.

R2(config-ext-nacl)#**permit tcp any host 192.168.20.254 eq www**

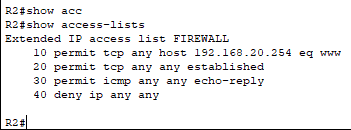
R2(config-ext-nacl)#**permit tcp any any established**

R2(config-ext-nacl)#**permit icmp any any echo-reply**

R2(config-ext-nacl)#**deny ip any any**



Después de configurar la ACL en R2, utilice el comando **show access-lists** para confirmar que la ACL tenga las sentencias correctas.

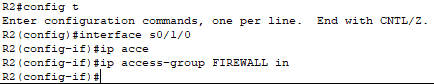


**Paso 2. Aplicar la ACL a la interfaz.**

Utilice el comando **ip access-group** *name* **{in | out}** para aplicar la ACL entrante en la interfaz opuesta al ISP del R2.

R3(config)#**interface s0/1/0**

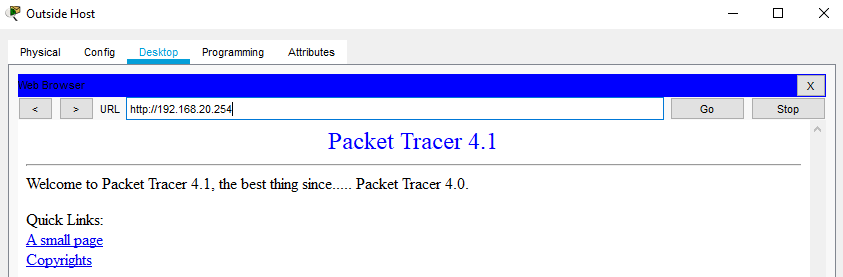
R3(config-if)#**ip access-group FIREWALL in**



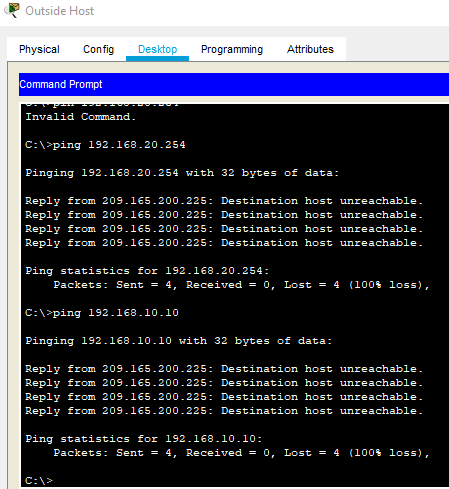
**Paso 3. Verificar y probar las ACL.**

Realice las siguientes pruebas para asegurarse de que la ACL esté funcionando según lo previsto.

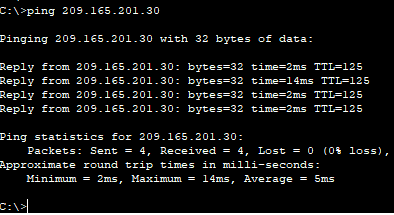
* Desde el host externo, abra una página Web en el servidor Web/TFTP interno. Esto debe estar permitido.



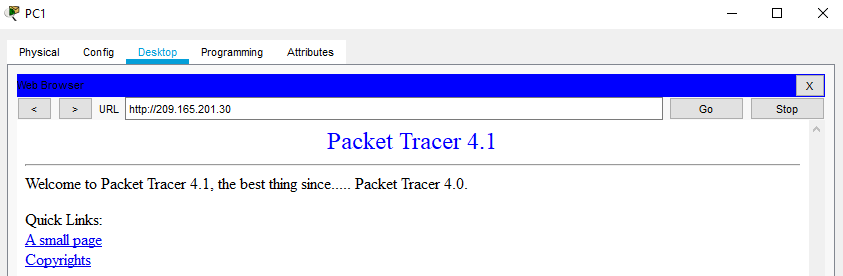
* Desde el host externo, haga ping al servidor Web/TFTP interno. Esto debe estar bloqueado.
* Desde el host externo, haga ping a la PC1. Esto debe estar bloqueado.



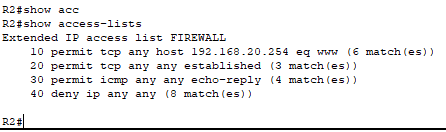
* Desde la PC1, haga ping al servidor Web externo en 209.165.201.30. Esto debe estar permitido.



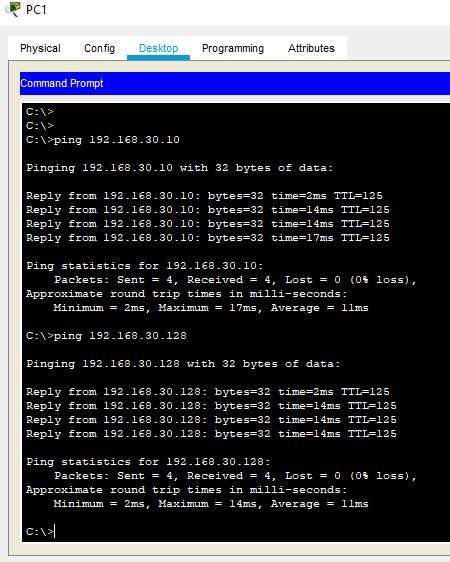
* Desde la PC1, abra una página Web en el servidor Web externo. Esto debe estar permitido.



Después de haber realizado estas pruebas y haber obtenido los resultados correctos, utilice el comando EXEC privilegiado **show access-lists** en R2 para verificar que las sentencias ACL coincidan.



Según su conocimiento sobre ACL, realice otras pruebas para verificar que cada sentencia coincida con el tráfico correcto.



**Paso 4. 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.

