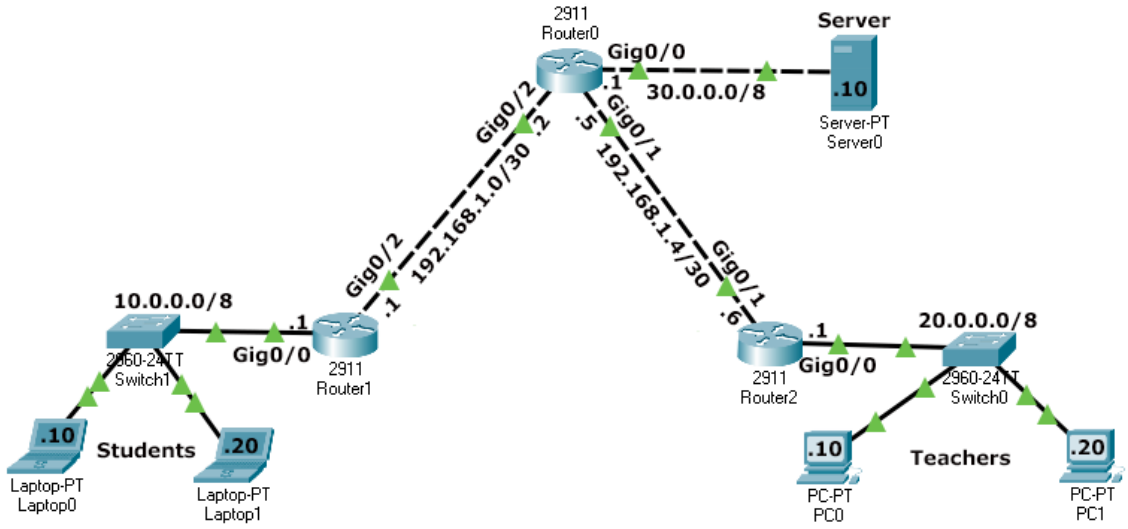
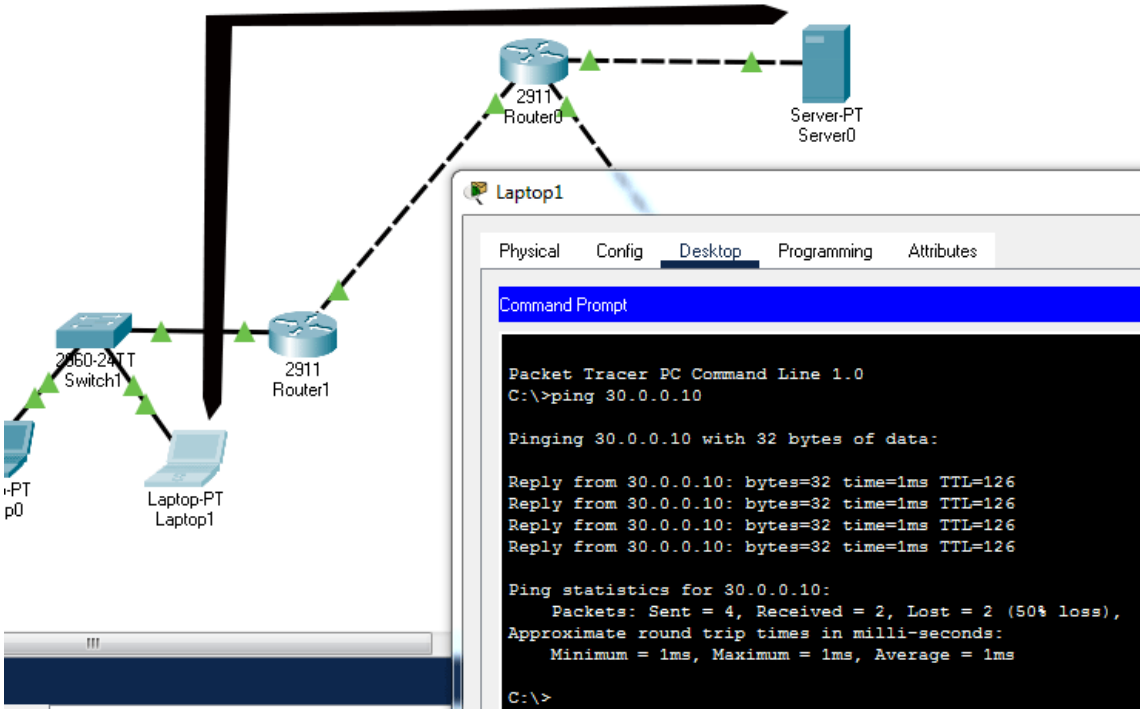
Creamos un laboratorio de Packet Tracert como se muestra en la siguiente imagen.



Configure las direcciones IP como se muestra en la imagen anterior y active el protocolo RIPv2 para el enrutamiento y pruebe la conectividad entre las secciones. Para probar la conectividad entre las secciones, puede utilizar el comando ping.

La siguiente imagen muestra cómo utilizar el comando ping para probar la conectividad entre Laptop1 y Server0.



Si todos los dispositivos finales pueden acceder entre sí, el laboratorio está listo para la práctica.

Objetivos/requisitos

Crear e implementar una lista de acceso estándar que bloquee el acceso de la sección Estudiantes a la sección Servidor.

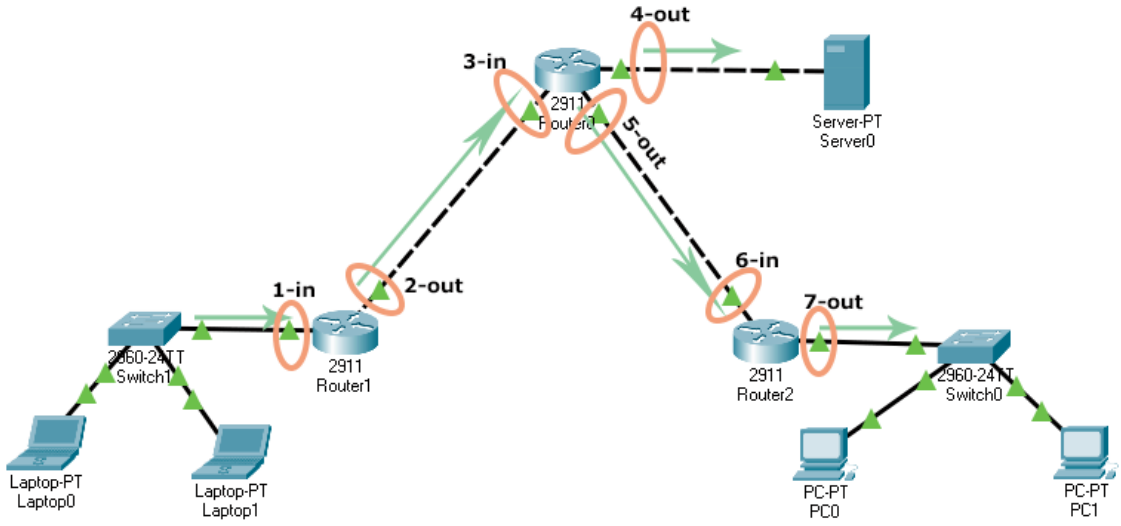
Comprensión de los requisitos

La sección Estudiantes utiliza la subred IP 10.0.0.0/8. Todos los paquetes que se originan en esta sección tienen una dirección IP de esta subred. Si creamos una ACL estándar con una declaración de denegación para esta subred, todos los paquetes que tengan una dirección IP de esta subred en su dirección de origen serán descartados.

Seleccionando la ubicación y la dirección de la ACL

La interfaz de un router utiliza la ACL para filtrar el tráfico que pasa por ella. Una ACL mal implementada puede bloquear todo el tráfico que pasa por ella. Antes de crear e implementar una ACL, tenemos que seleccionar la interfaz correcta y la dirección correcta para la ACL.

En nuestra red, tenemos siete ubicaciones donde podemos implementar la ACL. La siguiente imagen muestra estas ubicaciones y la dirección en la que se pueden utilizar para filtrar el tráfico.



La siguiente tabla enumera las ubicaciones anteriores y el efecto de la ACL en cada una de ellas.

Localización	Interface	Dirección	Efecto
1	Router1 Gig0/0	In	La sección de estudiantes no podrá acceder al servidor ni a la sección de profesores.

2	Router1 Gig0/2	Out	La sección de Estudiantes no podrá acceder a la sección de Servidores y Profesores.
3	Router0 Gig0/2	In	La sección de Estudiantes no podrá acceder a la sección de Servidores y Profesores.
4	**Router0 Gig0/0**	**Out**	**La sección Estudiantes no podrá acceder a la sección Servidores, pero sí a la sección Profesores.**
5	Router0 Gig0/1	Out	La sección Estudiantes no podrá acceder a la sección Profesores pero sí a la sección Servidores.
6	Router1 Gig0/1	In	La sección Estudiantes no podrá acceder a la sección Profesores pero sí a la sección Servidores.
7	Router1 Gig0/0	Out	La sección Estudiantes no podrá acceder a la sección Profesores pero sí a la sección Servidores.

Como puede ver en la tabla anterior, la ubicación correcta para nuestra ACL es el Gig0/0 del Router0 y la dirección correcta es la de salida.

Comandos de configuración de ACL estándar

Tenemos dos comandos para crear una lista de acceso estándar. Estos comandos son 'access-list' y 'ip access-list'. El comando 'ip access-list' tiene una ventaja sobre el comando 'access-list'. Nos permite actualizar o modificar declaraciones. Ya hemos aprendido a utilizar el comando 'access-list' para crear una lista de acceso estándar en la parte anterior de este tutorial. En esta parte, vamos a utilizar el comando 'ip access-list'.

El comando 'ip access-list' es un comando del modo de configuración global. Para crear una lista de acceso estándar, utiliza la siguiente sintaxis.

```
Router(config)# ip access-list standard ACL_#
```

En la sintaxis anterior, ACL_# es el nombre o número de la ACL estándar. Cuando se pulsa la tecla enter después de introducir este comando, el prompt de comando cambia y se entra en el modo de configuración de ACL estándar.

```
Router(config-std-acl)#
```

En el modo de configuración de ACL estándar, puede utilizar la siguiente sintaxis para crear declaraciones.

```
Router(config)# ip access-list standard ACL_name
Router(config-std-acl)# permit|deny source_IP_address
[wildcard_mask]
```

Una ACL no hace nada hasta que se aplica a una interfaz. Para aplicar una ACL estándar a una interfaz, entre en el modo de configuración de la interfaz y utilice el siguiente comando.

```
Router(config)# tipo de interfaz [slot_#]puerto_#
Router(config-if)# ip access-group ACL_# in|out
```

Una vez que se activa una ACL en una interfaz, la interfaz procesa todos los paquetes a través de ella.

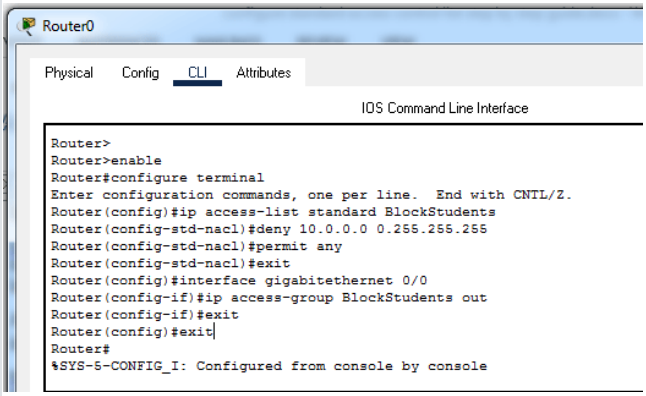
Creación de una ACL estándar

Acceda al prompt de comandos del Router0 y ejecute los siguientes comandos.

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list standard BlockStudents
Router(config-std-nacl)#deny 10.0.0.0 0.255.255.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip access-group BlockStudents out
Router(config-if)#exit
Router(config)#exit
Router#
```

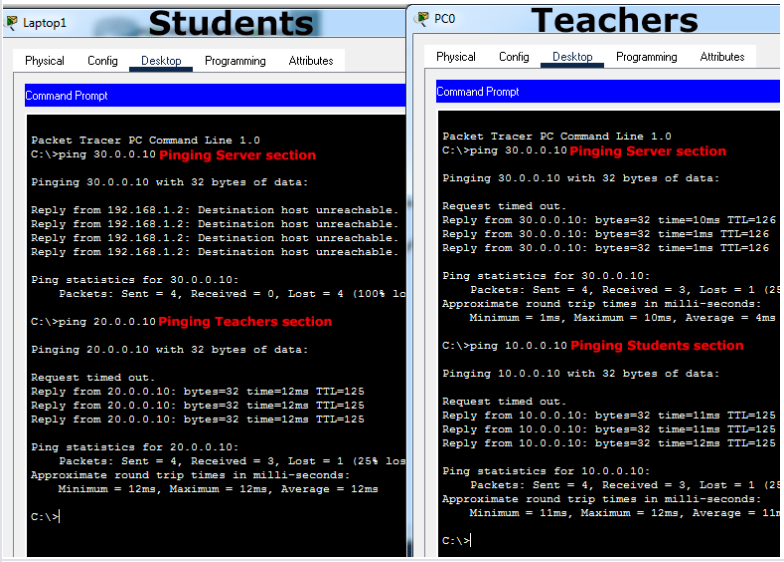
Vamos a discutir los comandos anteriores. Utilizamos los dos primeros comandos para entrar en el modo de configuración global. El siguiente comando crea una ACL estándar llamada BlockStudents. En el modo de configuración de la ACL, añadimos dos declaraciones. La primera declaración deniega todo el tráfico procedente de la subred 10.0.0.0/8. La segunda declaración permite todo el resto del tráfico. Utilizamos los siguientes comandos para salir del modo de configuración ACL y entrar en el modo de configuración de la interfaz. El siguiente comando aplica la ACL BlockStudents en la dirección de salida. Los dos últimos comandos salen del modo de configuración de la interfaz y del modo de configuración global, respectivamente.

La siguiente imagen muestra cómo ejecutar los comandos anteriores en el prompt de comandos del router.



Verificación

Para verificar la ACL, podemos probar la conectividad entre las secciones. La sección Estudiantes no debería poder acceder a la sección Servidor, pero sí a la sección Profesores. La sección Profesores debería poder acceder tanto a la sección Servidor como a la sección Alumnos. Puede utilizar el comando ping para probar la conectividad. La siguiente imagen muestra esta prueba.



Modificación/actualización de una sentencia ACL estándar

Para modificar o actualizar una sentencia ACL estándar, siga los siguientes pasos.

Utilice el comando 'show access-lists' para ver el número de secuencia de la sentencia.
Entre en el modo de configuración de ACL estándar
Elimine la sentencia existente con el comando 'no [número de secuencia]'

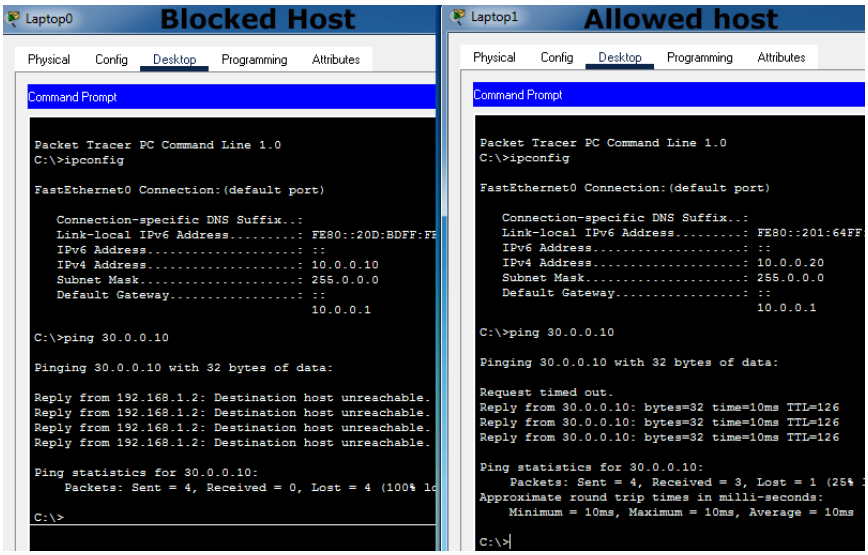
Inserte la sentencia modificada, actualizada o la nueva con el número de secuencia de la antigua sentencia Pongamos un ejemplo. Supongamos que, en lugar de bloquear toda la subred, sólo queremos bloquear un único host (10.0.0.10/8) de la sección Students. Para esto, acceda al prompt CLI del Router0 y ejecute los siguientes comandos.		

```
Router>
Router#show access-lists
Standard IP access list BlockStudents
10 deny 10.0.0.0 0.255.255.255
20 permit any
Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#ip access-list standard BlockStudents
Router(config-std-nacl)#no 10
Router(config-std-nacl)#10 deny 10.0.0.10 0.0.0.0
Router(config-std-nacl)#exit
Router(config)#exit
Router#
Router#show access-lists
Standard IP access list BlockStudents
10 deny host 10.0.0.10
20 permit any
Router#
```

Entendamos los comandos anteriores.

En primer lugar, comprobamos el número de secuencia de la sentencia que hemos utilizado para bloquear toda la sección de Estudiantes. Como podemos en la salida anterior, el número de secuencia de la sentencia es 10. Después, entramos en el modo de configuración ACL de la ACL. En el modo de configuración de la ACL, eliminamos la sentencia actual con el comando 'no sequence_number_of_statement'. Al final, insertamos la nueva sentencia en el lugar de la sentencia existente.

Como la ACL ya está activa en la interfaz, ésta empieza a utilizar la nueva sentencia en cuanto se añade. Para verificar el cambio, vuelva a enviar solicitudes de ping desde el host bloqueado y el host permitido. La siguiente imagen muestra esta prueba.



Para eliminar una ACL estándar, utilice el siguiente comando en el modo de configuración global.

```
Router(config)no ip access-list standard ACL_#
```

Reemplace ACL_# con el nombre o número de la ACL.

El siguiente comando borra la ACL BlockStudents.

```
Router(config)no ip access-list standard BlockStudents
```