



Instituto Politécnico Nacional



Escuela Superior de Cómputo

Practica 6. ACL

Materia:

Administración de servicios en red

Grupo:

4CV13

Profesor:

Henestrosa Carrasco Leticia

Integrantes: (*Equipo 1*)

Arévalo Andrade Miguel Ángel
Castro Cruces Jorge Eduardo
López Mares Irene Elizabeth
Pedroza García Rodolfo

Fecha:

martes, 22 de marzo de 2022

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

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.

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.

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 tráfico 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.

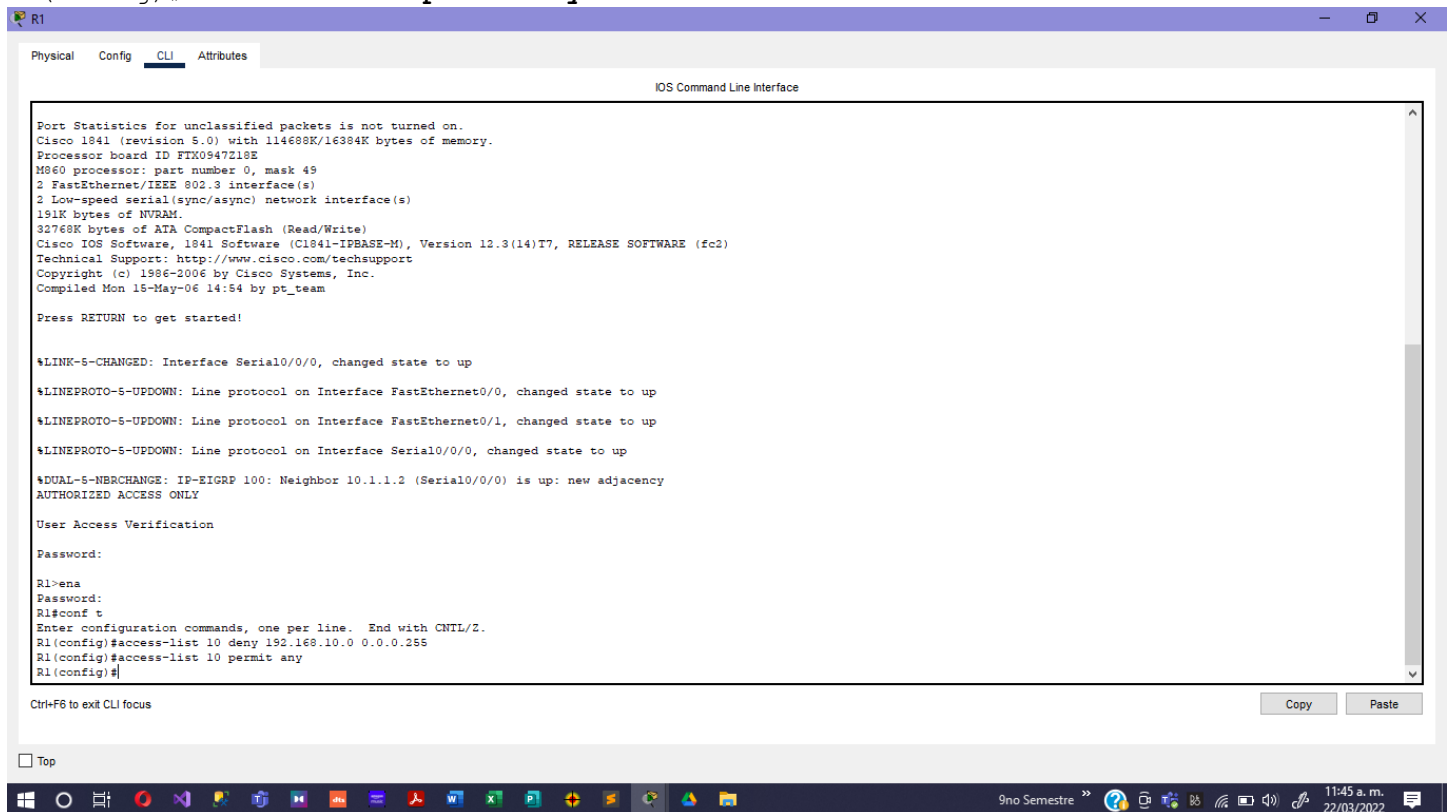
Paso 2. Determinar las sentencias.

- 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
```

R2

Physical

Config

CLI

Attributes

IOS Command Line Interface

32768K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.2.2.2 (Serial0/0/1) is up: new adjacency

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

AUTHORIZED ACCESS ONLY

User Access Verification

Password:

R2>ena

Password:

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

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

R2(config)#access-list 11 permit any

R2(config)#

Ctrl+F6 to exit CLI focus

CopyPaste

☐ Top

9no Semestre 11:47 a.m.
22/03/2022

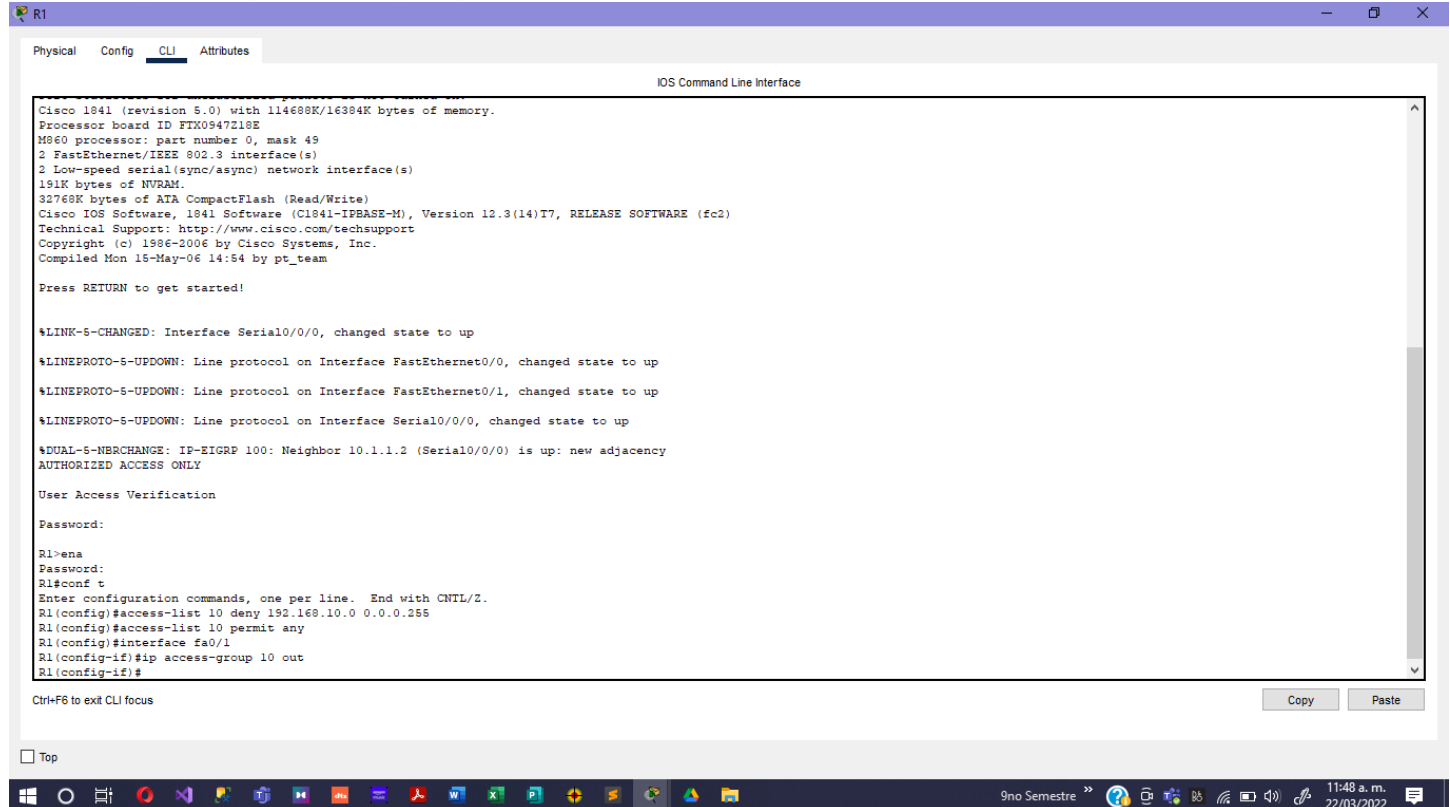
Paso 3. Aplicar las sentencias a las interfaces.

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
```

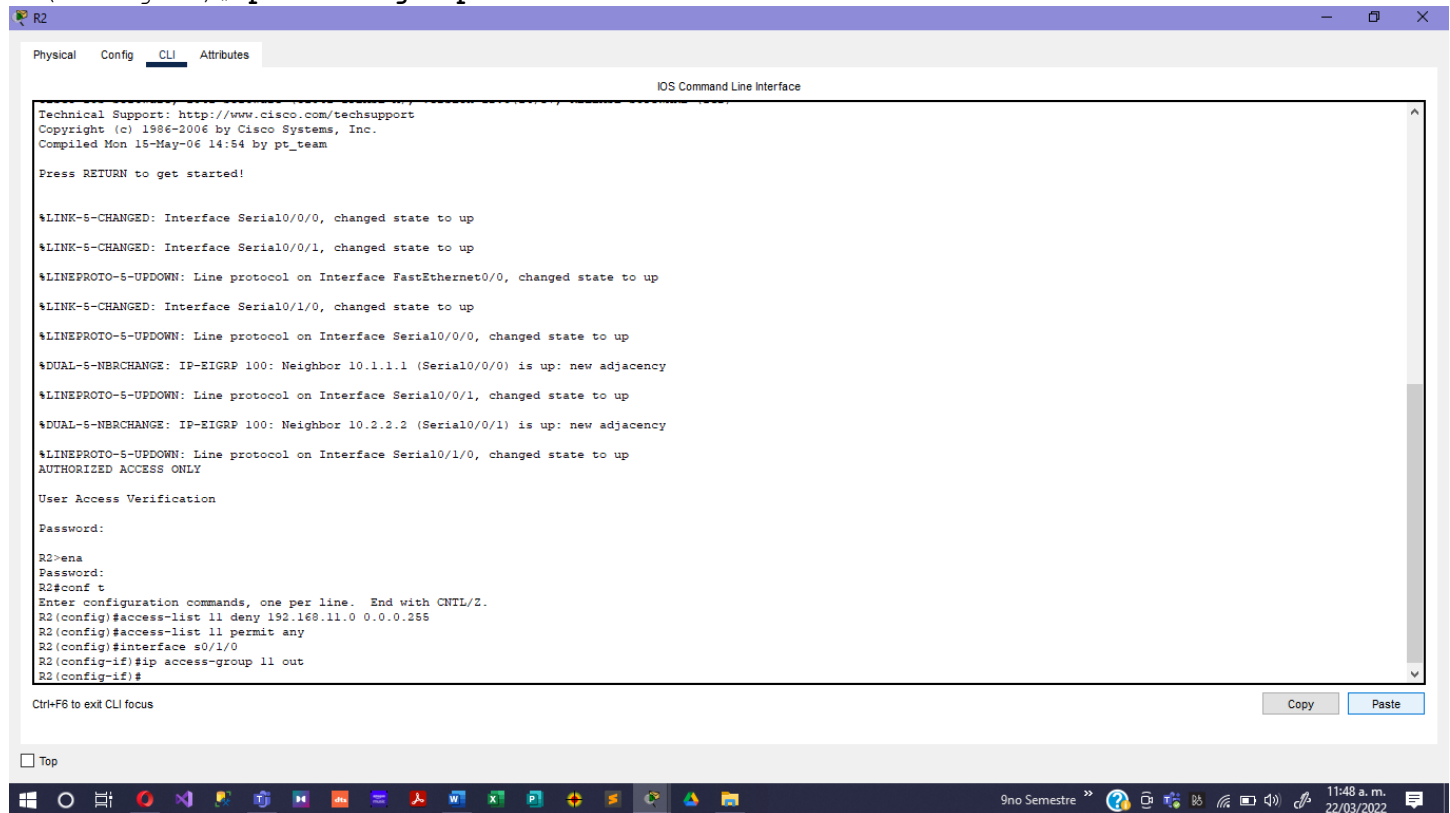


En R2, ingrese al modo de configuración para la interfaz S0/1/0.

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

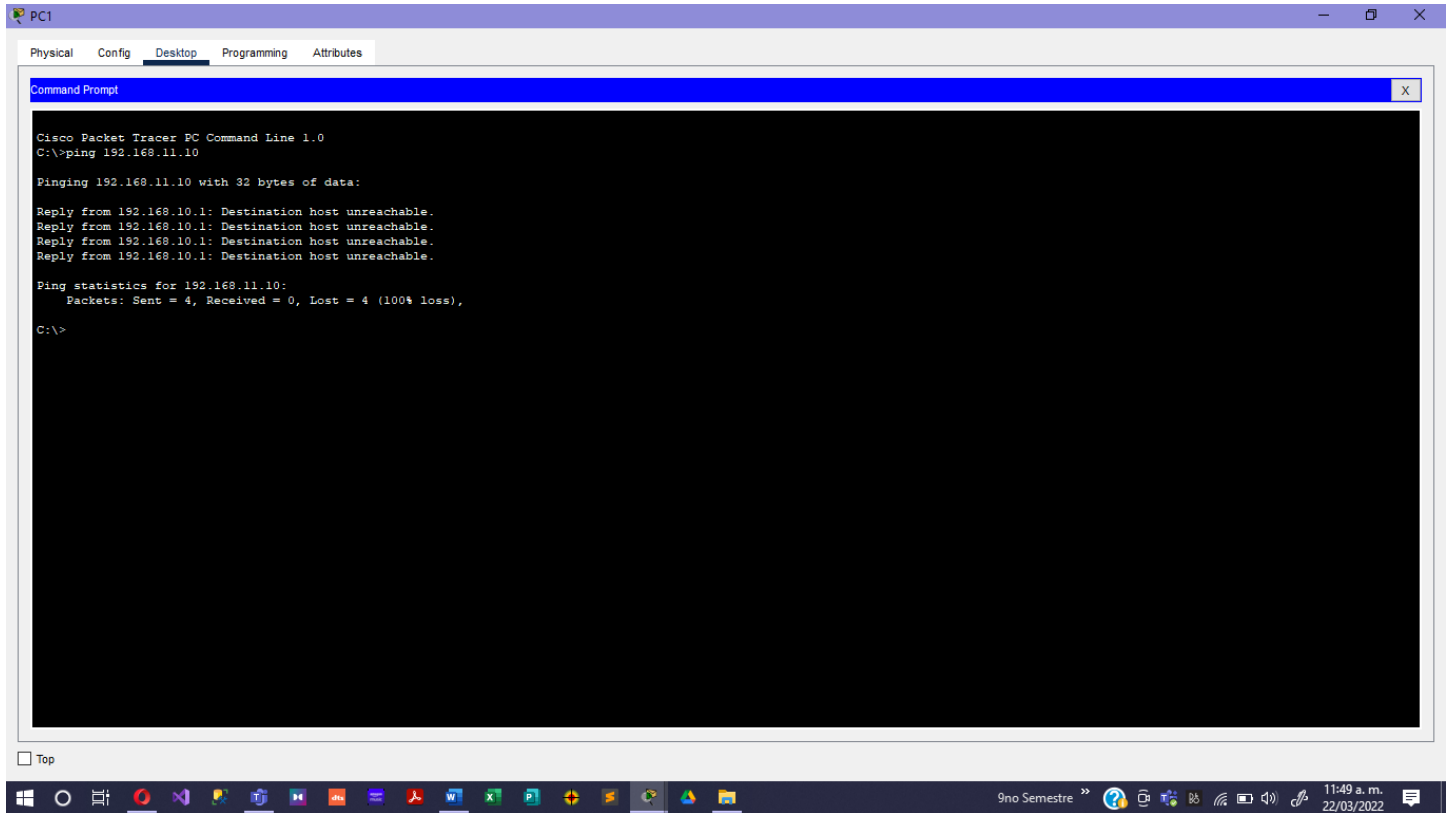
```
R2 (config)#interface s0/1/0
```

```
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.

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.30

Pinging 209.165.201.30 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 209.165.201.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.202.158

Pinging 209.165.202.158 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 209.165.202.158:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192
Ping request could not find host 192. Please check the name and try again.
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.10: bytes=32 time=19ms TTL=125
Reply from 192.168.30.10: bytes=32 time=29ms TTL=125
Reply from 192.168.30.10: bytes=32 time=10ms TTL=125

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 29ms, Average = 19ms
```

Top

9no Semestre 11:52 a.m. 22/03/2022

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.

PT Activity: 04:37:16

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
R3	Fa0/0	192.168.20.1	255.255.255.0
	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

Time Elapsed: 04:37:16

Top Dock Check Results

Back 1/1 Next

Completion: 66%

9no Semestre 11:53 a.m. 22/03/2022

Tarea 4: Configurar una ACL estándar nombrada

Paso 1. Determinar la máscara wildcard.

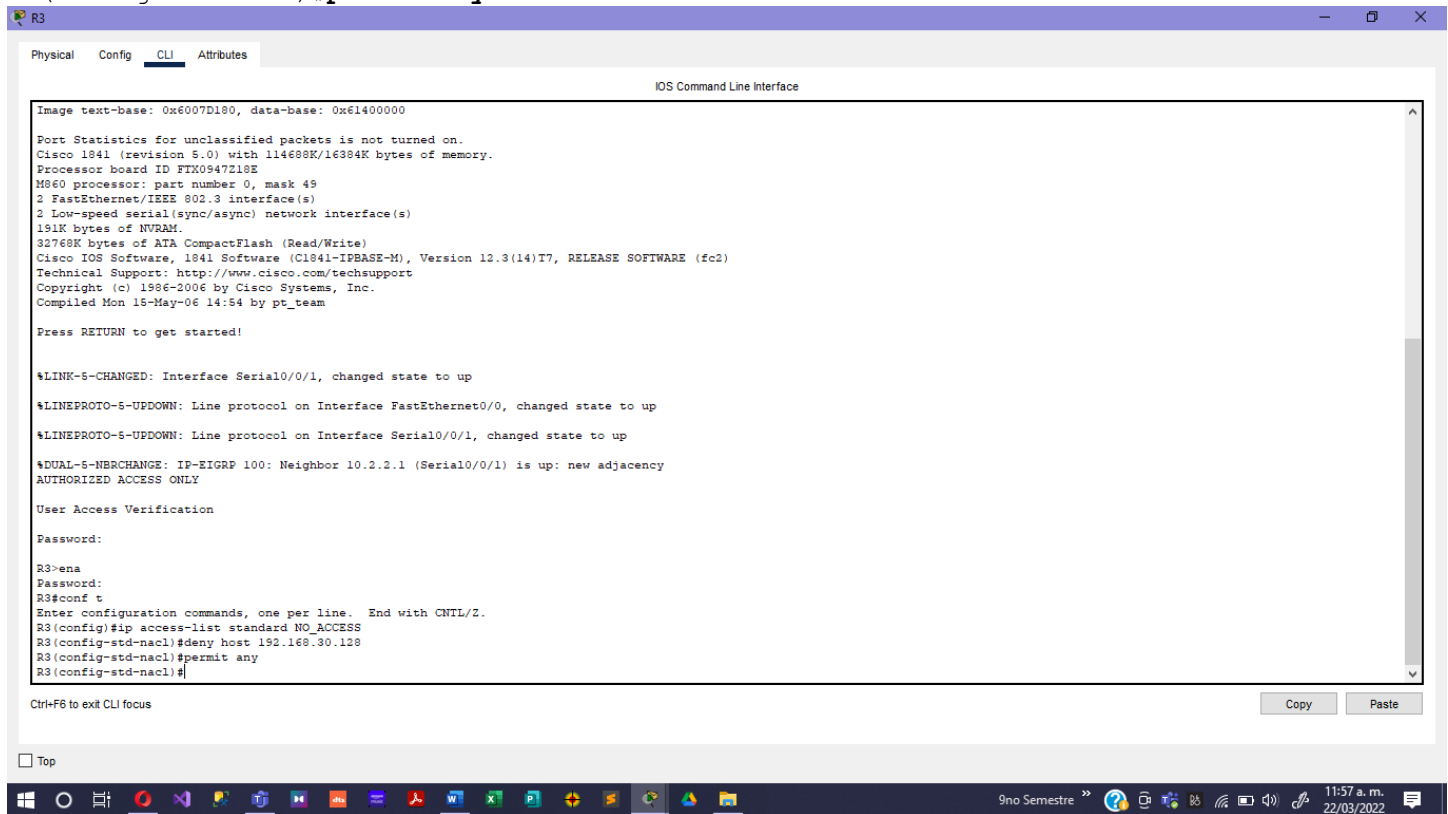
- La política de acceso para R3 indica que el host en 192.168.30.128 no debe tener permitido ningún acceso fuera de la LAN local. El resto de los hosts de la red 192.168.30.0 deben tener permitido el acceso a las demás ubicaciones.
- Para verificar un único host, debe verificarse la dirección IP completa 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
```

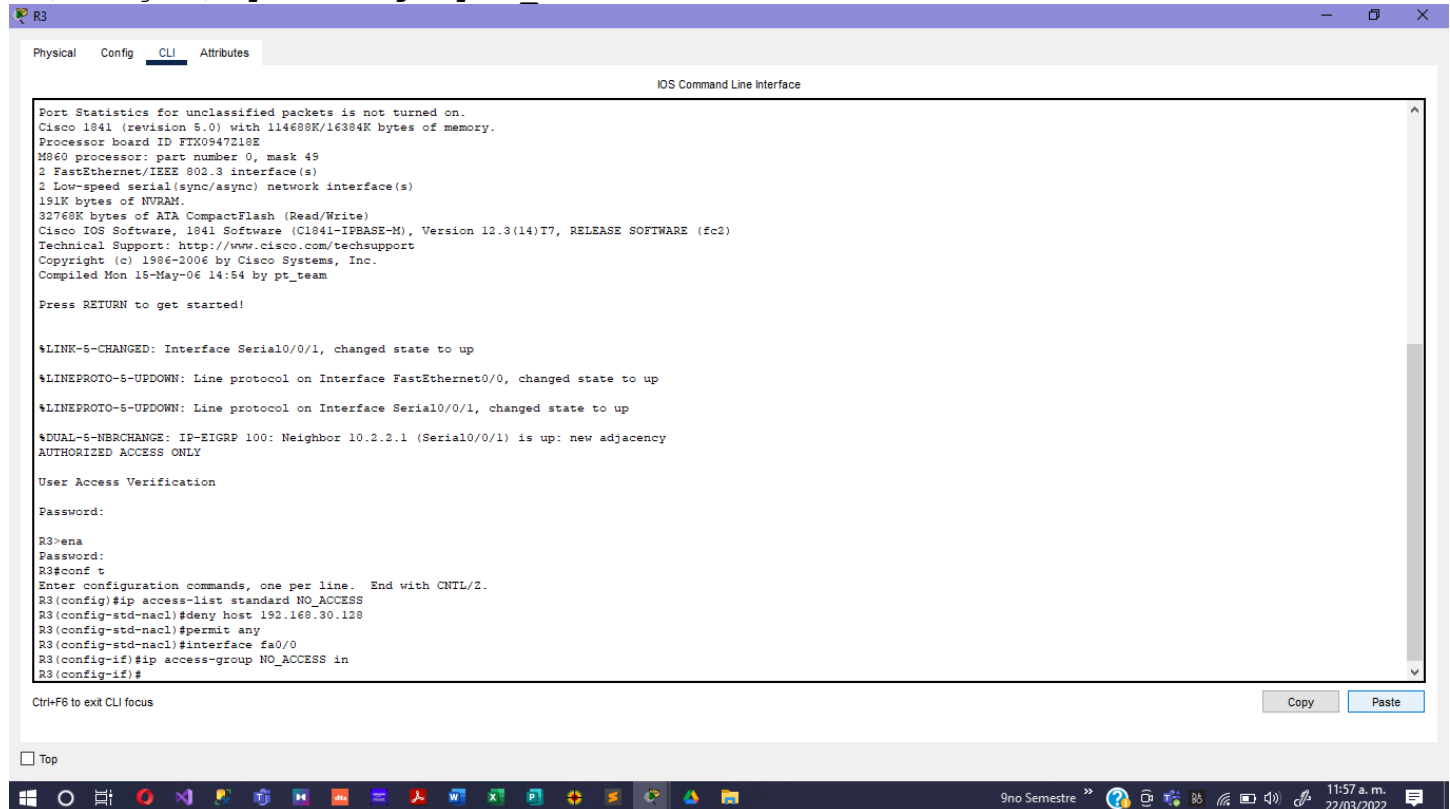


Paso 3. Aplicar las sentencias a la interfaz correcta.

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
```

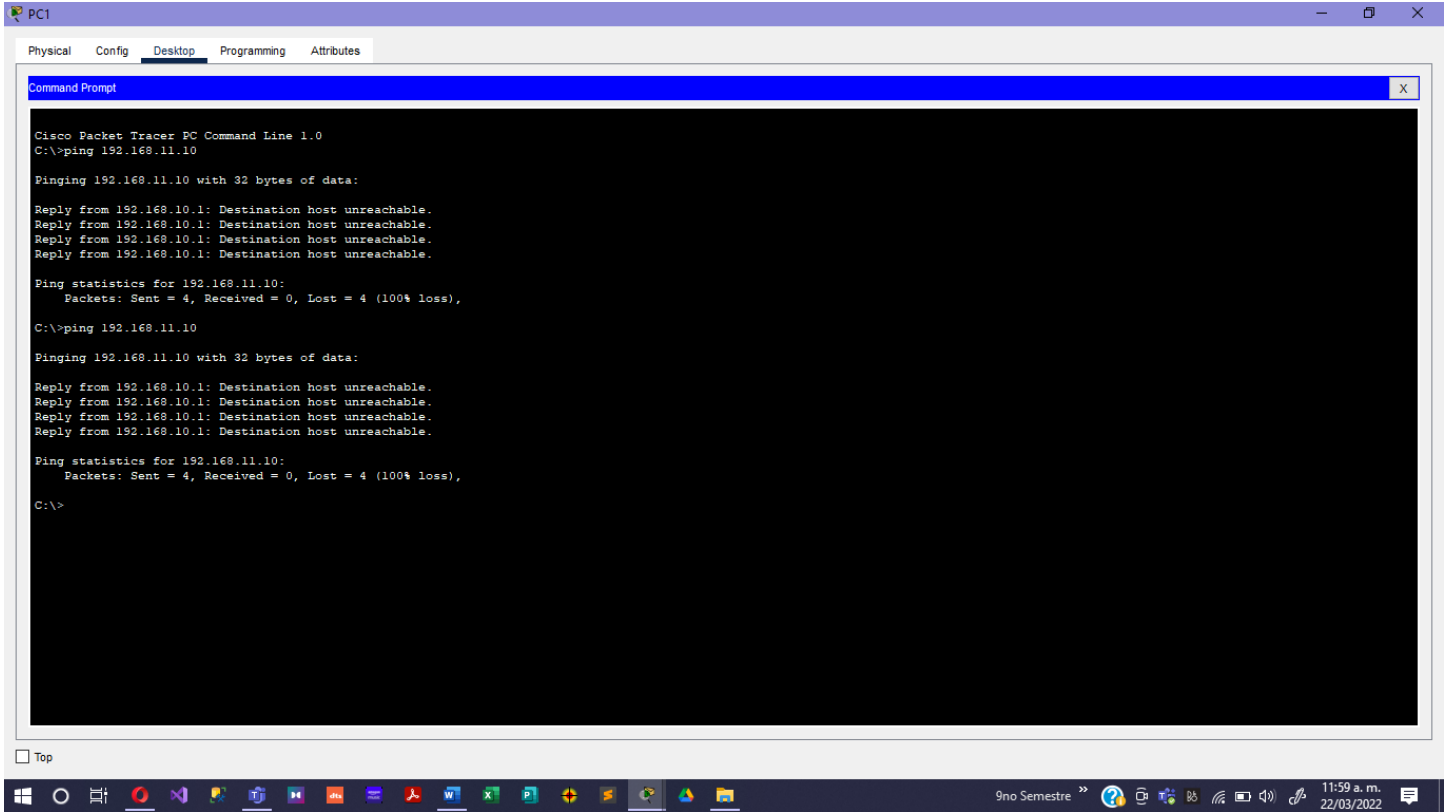
```
R3(config-if)#ip access-group NO_ACCESS in
```



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



The screenshot shows the PC1 configuration window in Cisco Packet Tracer. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows two failed ping attempts to the IP address 192.168.11.10. Each attempt consists of four 'Destination host unreachable' replies and a summary showing 100% packet loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

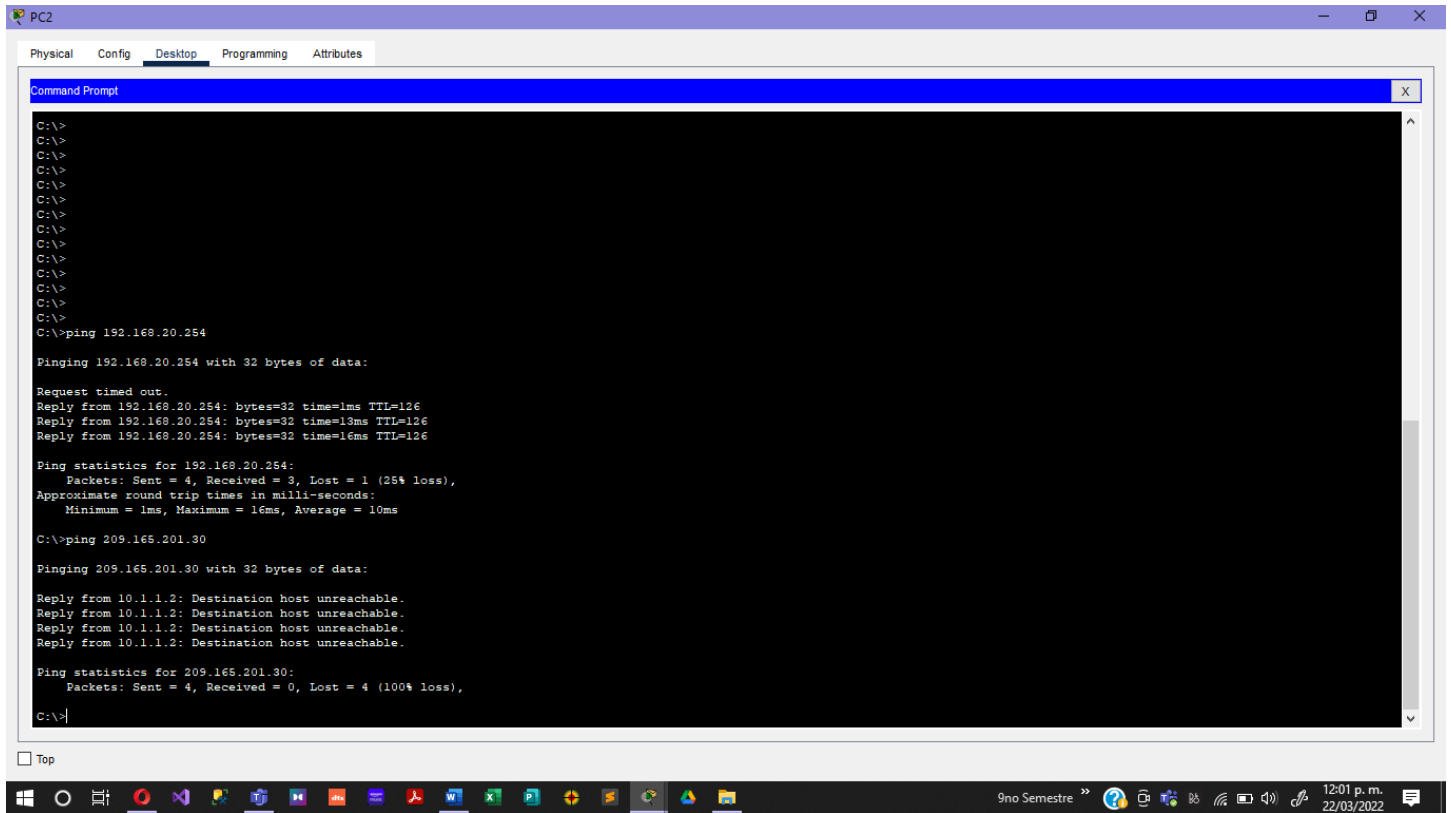
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

The taskbar at the bottom shows the system clock as 11:59 a.m. on 22/03/2022, and the user is logged in as '9no Semestre'.

- PC2 a host externo
- PC2 a Servidor Web



The screenshot shows a Windows desktop environment. At the top, there is a window titled "PC2" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active. Below the tabs is a "Command Prompt" window. The Command Prompt displays the following text:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=13ms TTL=126
Reply from 192.168.20.254: bytes=32 time=16ms TTL=126

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 10ms

C:\>ping 209.165.201.30

Pinging 209.165.201.30 with 32 bytes of data:

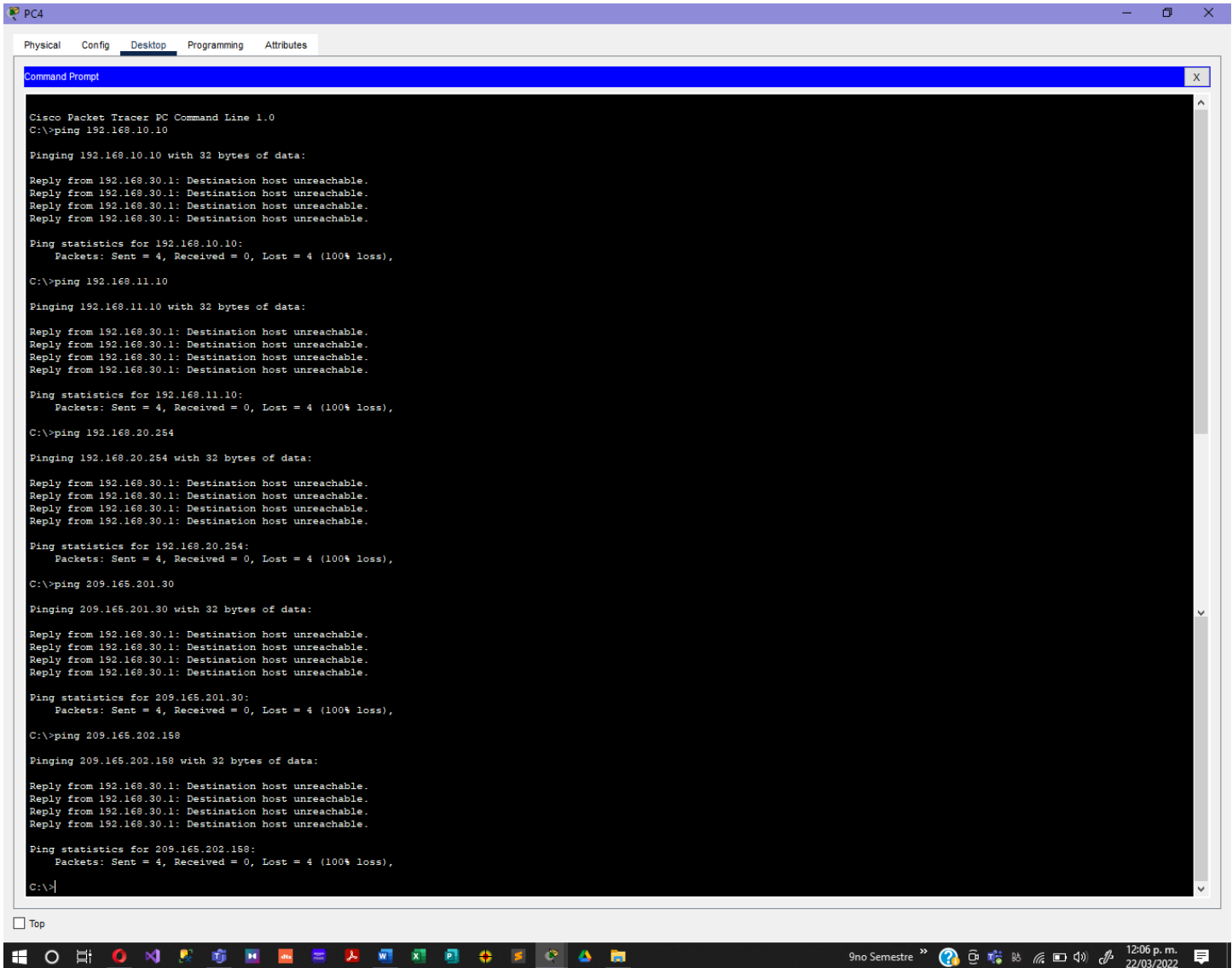
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 209.165.201.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

At the bottom of the screen, there is a taskbar with various application icons. The system tray on the right shows the date and time: "12:01 p.m. 22/03/2022".

- Todos los pings desde la PC4 y hacia ésta, excepto entre la PC3 y la PC4



```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.201.30

Pinging 209.165.201.30 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 209.165.201.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.202.158

Pinging 209.165.202.158 with 32 bytes of data:

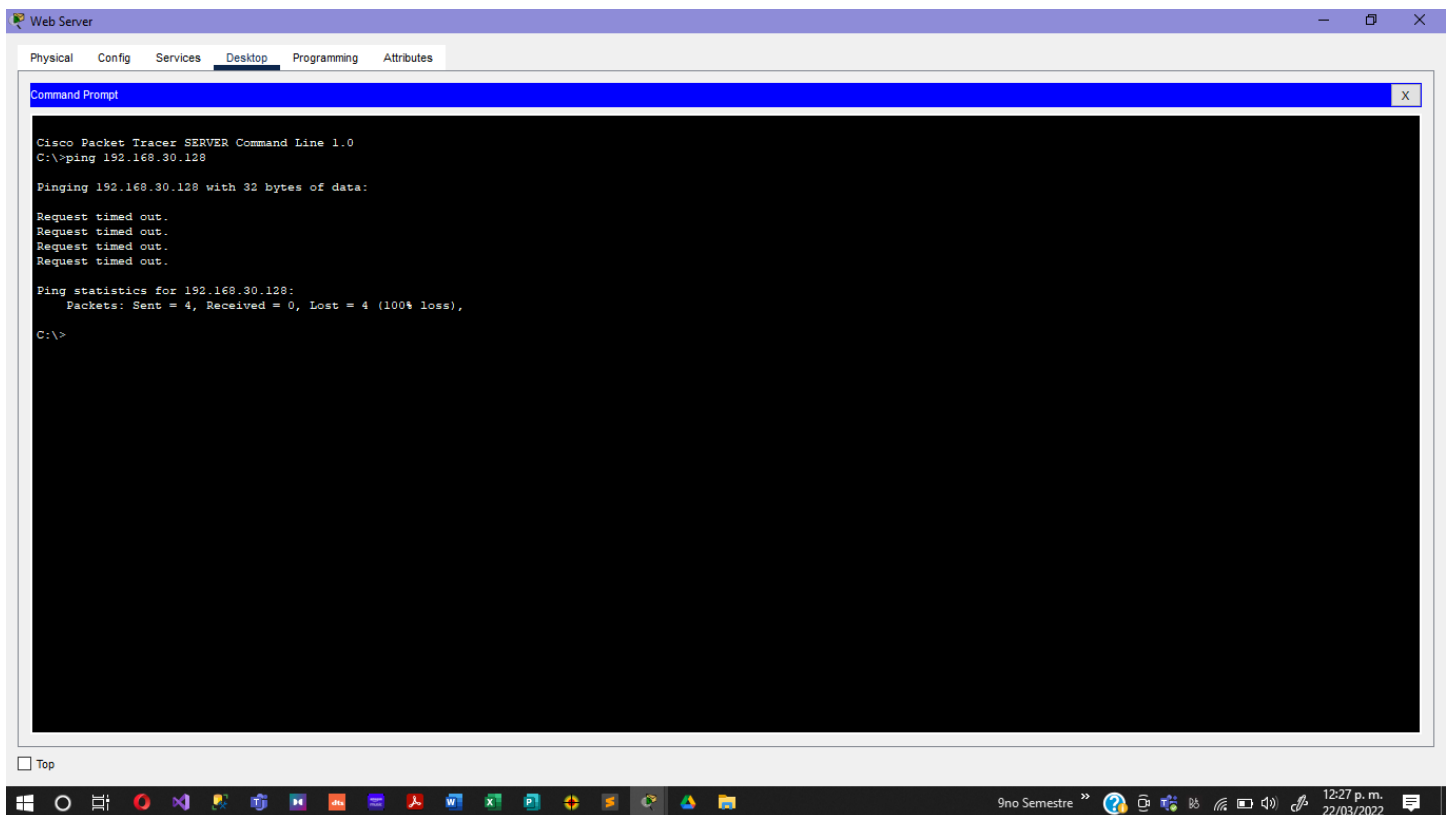
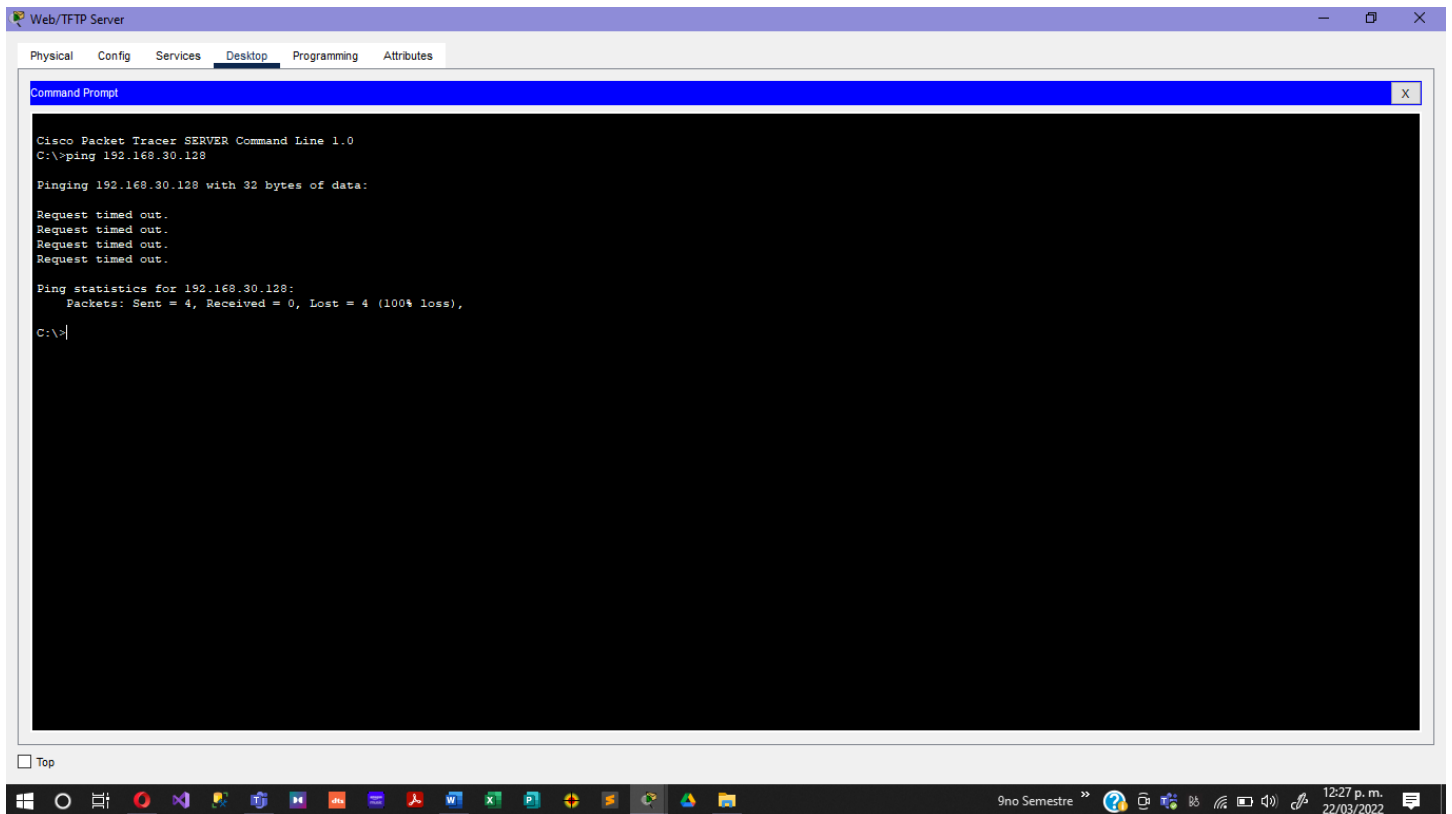
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

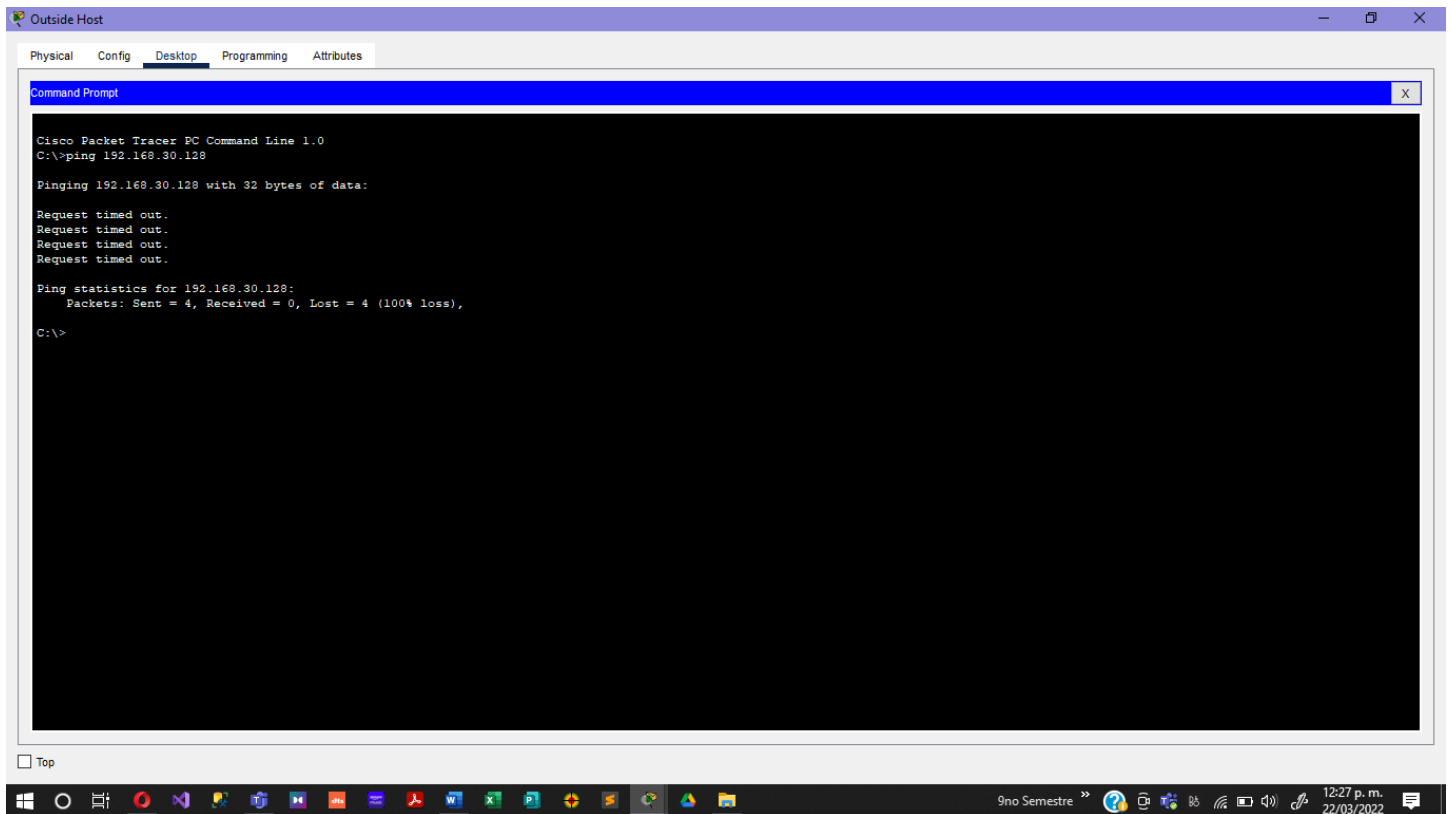
Ping statistics for 209.165.202.158:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

9no Semestre 12:06 p.m. 22/03/2022





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.

PT Activity: 05:11:53

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
R3	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
ISP	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/1	209.165.200.226	255.255.255.224
	Fa0/1	209.165.201.1	255.255.255.224
PC1	NIC	209.165.202.129	255.255.255.224
PC2	NIC	192.168.10.10	255.255.255.0
PC3	NIC	192.168.11.10	255.255.255.0
PC4	NIC	192.168.30.10	255.255.255.0
Servidor WEB/FTP	NIC	192.168.30.128	255.255.255.0
Servidor WEB	NIC	192.168.20.254	255.255.255.0
Servidor WEB	NIC	209.165.201.30	255.255.255.224

Time Elapsed: 05:11:53

Top Dock Check Results

Back 1/1

Completion: 100%*

9no Semestre 12:28 p. m. 22/03/2022

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Congratulations on completing this activity!

Close

Packet Tracer: demostración de listas de control de acceso

Objetivos

Parte 1: verificar la conectividad local y probar la lista de control de acceso

Parte 2: eliminar la lista de control de acceso y repetir la prueba

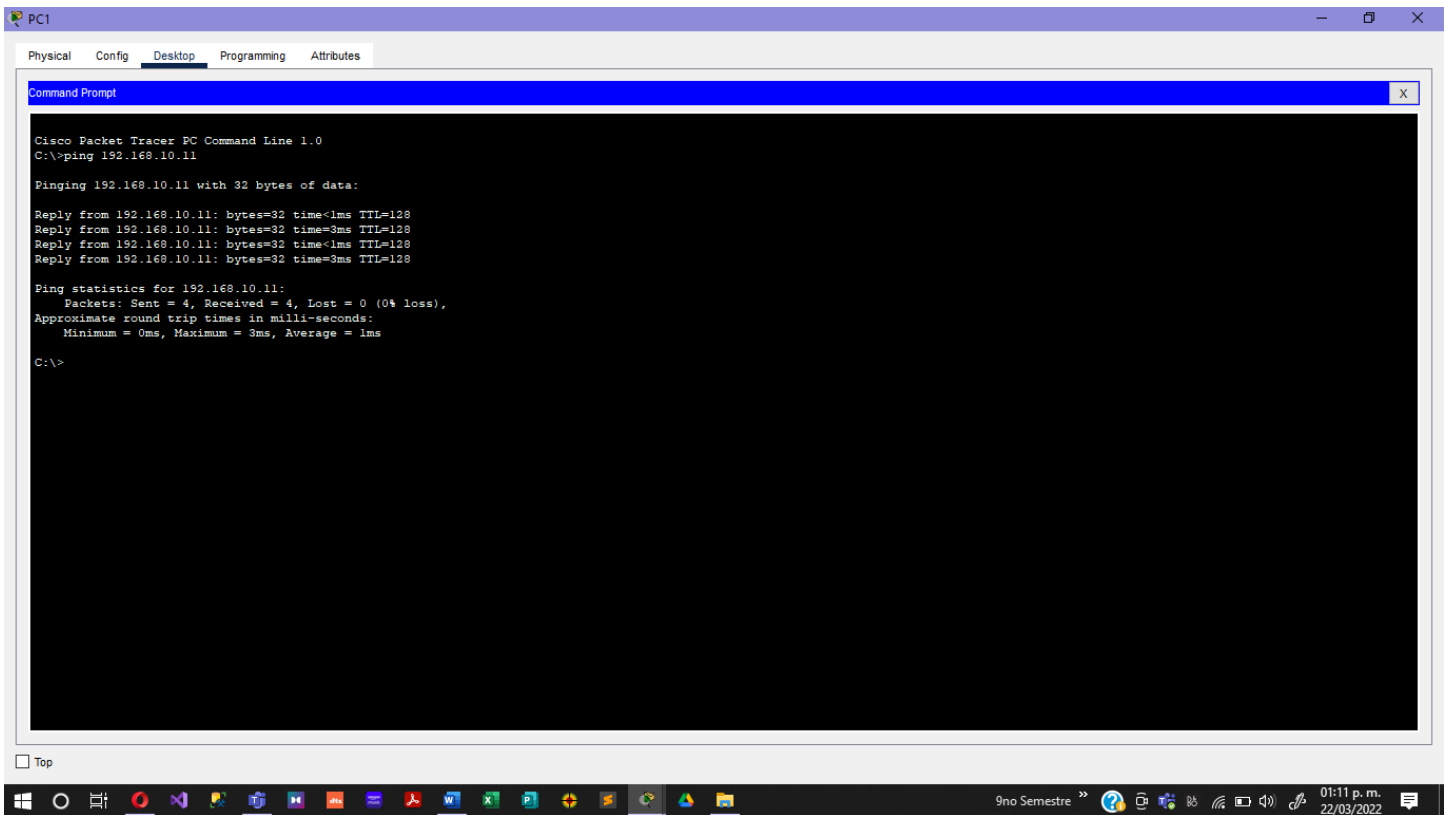
Aspectos básicos

En esta actividad, observará cómo se puede utilizar una lista de control de acceso (ACL) para evitar que un ping llegue a hosts en redes remotas. Después de eliminar la ACL de la configuración, los pings se realizarán correctamente.

Parte 1: Verificar la conectividad local y probar la lista de control de acceso

Paso 1: Hacer ping a los dispositivos de la red local para verificar la conectividad.

a. Desde la petición de ingreso de comando de la **PC1**, haga ping a la **PC2**.



The screenshot shows the Cisco Packet Tracer interface with the PC1 configuration window open. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```

The taskbar at the bottom shows the Windows 10 interface with various application icons and a system clock indicating 01:11 p.m. on 22/03/2022.

b. Desde la petición de ingreso de comando de la **PC1**, haga ping a la **PC3**.

The screenshot shows a Cisco Packet Tracer PC Command Line window for PC1. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.11.10: bytes=32 time=24ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 24ms, Average = 8ms

C:\>
```

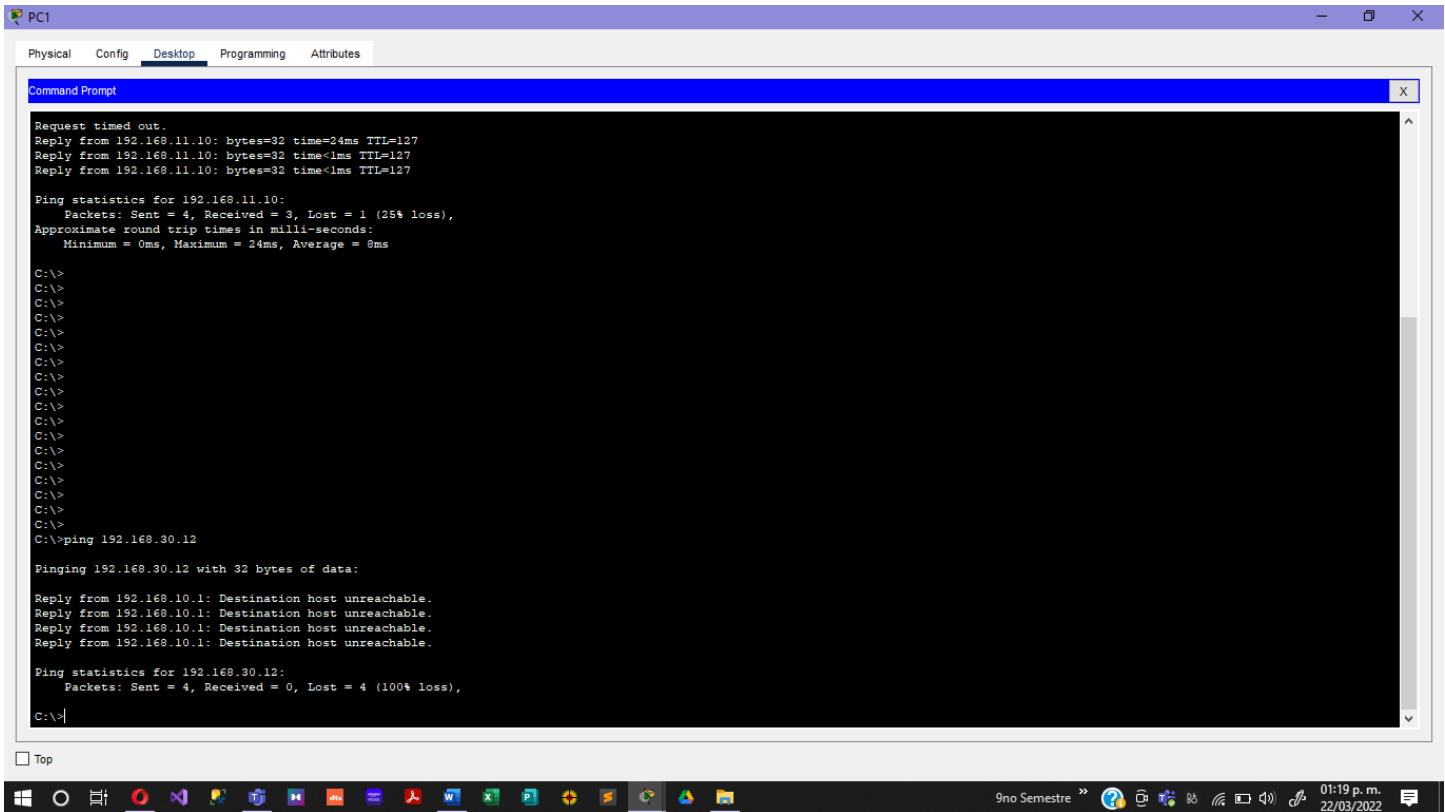
At the bottom of the window, there is a "Top" button and a taskbar showing various application icons, the text "9no Semestre", and the system clock "01:12 p.m. 22/03/2022".

¿Por qué se realizaron de forma correcta los pings?

Esto se debe a que no hay ninguna ACL que restrinja sus conexión.

Paso 2: Hacer ping a los dispositivos en las redes remotas para probar la funcionalidad de la ACL.

- Desde la petición de ingreso de comando de la **PC1**, haga ping a la **PC4**.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Reply from 192.168.11.10: bytes=32 time=24ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 24ms, Average = 8ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.30.12

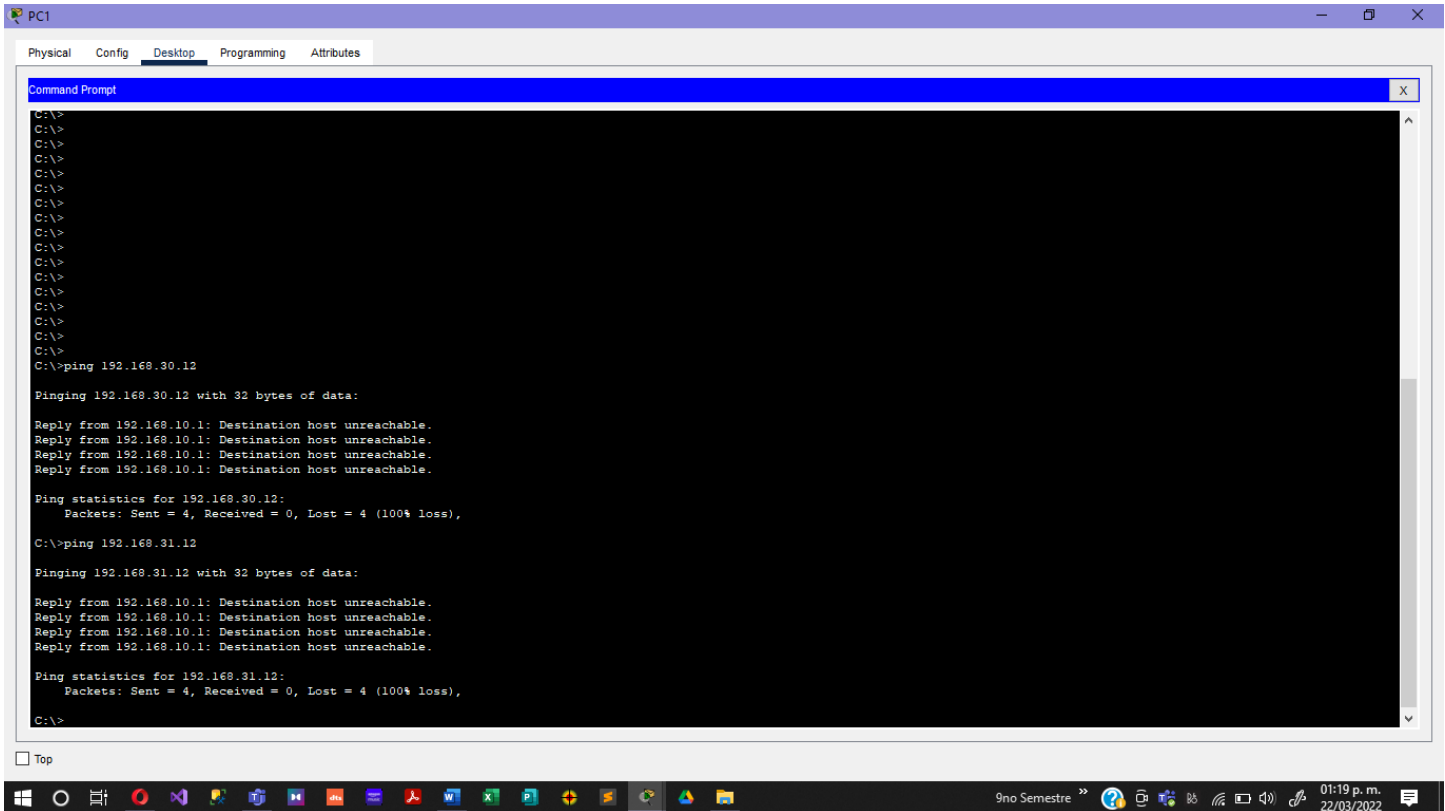
Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

- Desde la petición de ingreso de comando de la **PC1**, haga ping al **servidor DNS**.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.31.12

Pinging 192.168.31.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.31.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

¿Por qué fallaron los pings? (Sugerencia: utilice el modo de simulación o vea las configuraciones del router para investigar).

Cisco Packet Tracer - C:\Users\georg\Desktop\ESCOM\9no Semestre\ASR\Praticas\6.2 ACL Demonstration.pka

File Edit Options View Tools Extensions Window Help

Logical Physical x: 783, y: 293

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device
	0.000	--	PC1
	0.001	PC1	S1
	0.002	S1	R1
	0.002	--	R1

Reset Simulation ☒ Constant Delay Captured to: 0.002 s

Play Controls

Event List Filters - Visible Events

ICMP

Edit Filters Show All/None

Time: 00:51:13.113 PLAY CONTROLS

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	In Progress	PC1	PC4	ICMP		0.000	N	0	(edit)

9no Semestre 01:24 p.m. 22/03/2022

Cisco Packet Tracer - C:\Users\georg\Desktop\ESCOM\9no Semestre\ASR\Praticas\6.2 ACL Demonstration.pka

File Edit Options View Tools Extensions Window Help

Logical Physical x: 786, y: 309

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device
	0.000	--	PC1
	0.001	PC1	S1
	0.002	S1	R1
	0.002	--	R1

Reset Simulation ☒ Constant Delay Captured to: 0.002 s

Play Controls

Event List Filters - Visible Events

ICMP

Edit Filters Show All/None

Time: 00:51:33.107 PLAY CONTROLS

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	In Progress	PC1	Server D...	ICMP		0.000	N	0	(edit)

9no Semestre 01:24 p.m. 22/03/2022


```
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.10.0 0.0.0.255 area 10
network 192.168.11.0 0.0.0.255 area 11
network 10.10.1.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
end
R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9no Semestre 01:27 p. m. 22/03/2022

Esto se debe a que existe una ACL en el R1 que impide que la LAN 192.168.10.0/24 salga.

Parte 2: Eliminar la ACL y repetir la prueba

Paso 1: Utilizar los comandos show para investigar la configuración de la ACL.

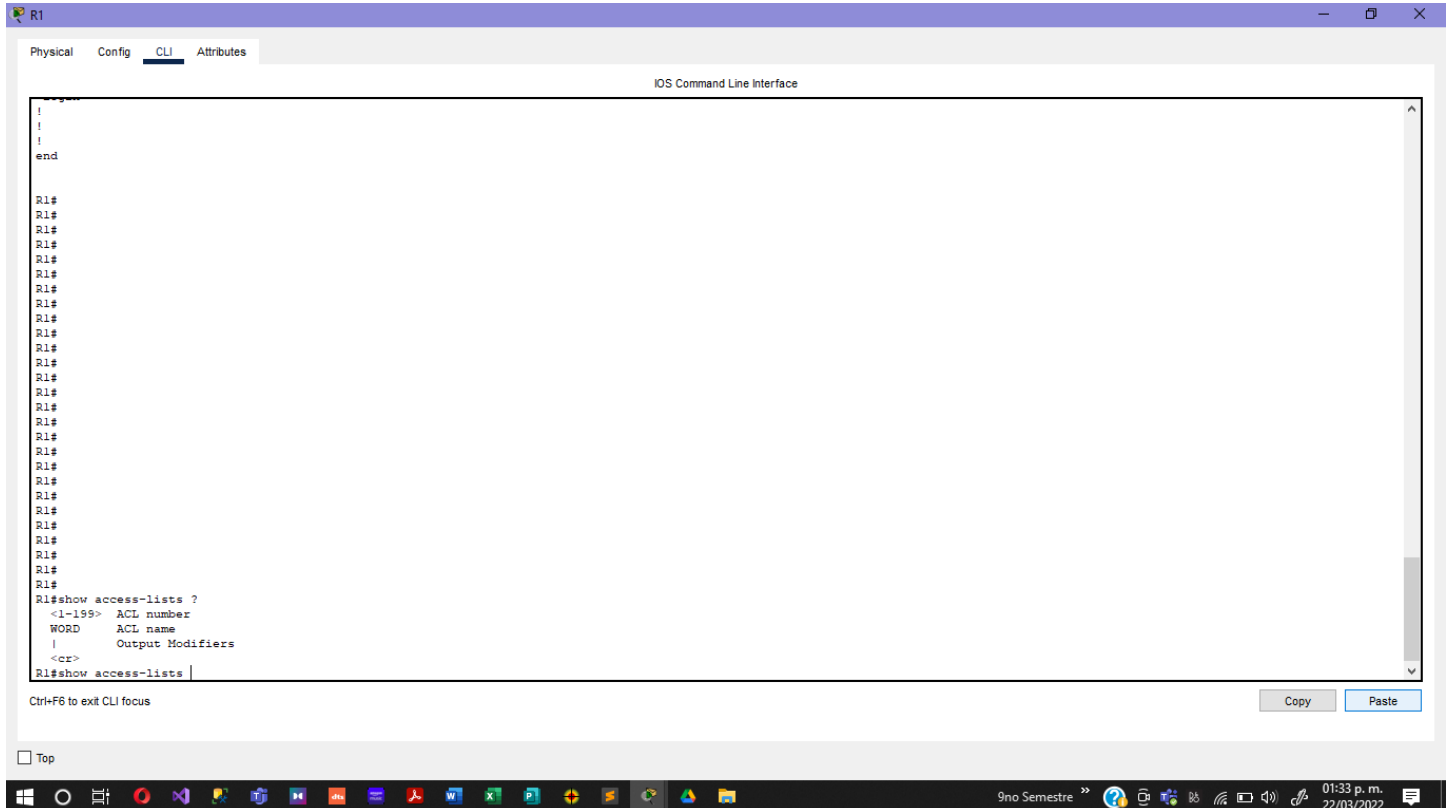
- Utilice los comandos **show run** y **show access-lists** para ver las ACL configuradas actualmente. Para obtener una vista rápida de las ACL vigentes, utilice **show access-lists**. Introduzca el comando **show access-lists** seguido de un espacio y un signo de interrogación (?) para ver las opciones disponibles:

```
R1#show access-lists ?
```

```
<1-199> ACL number
```

```
WORD ACL name
```

```
<cr>
```



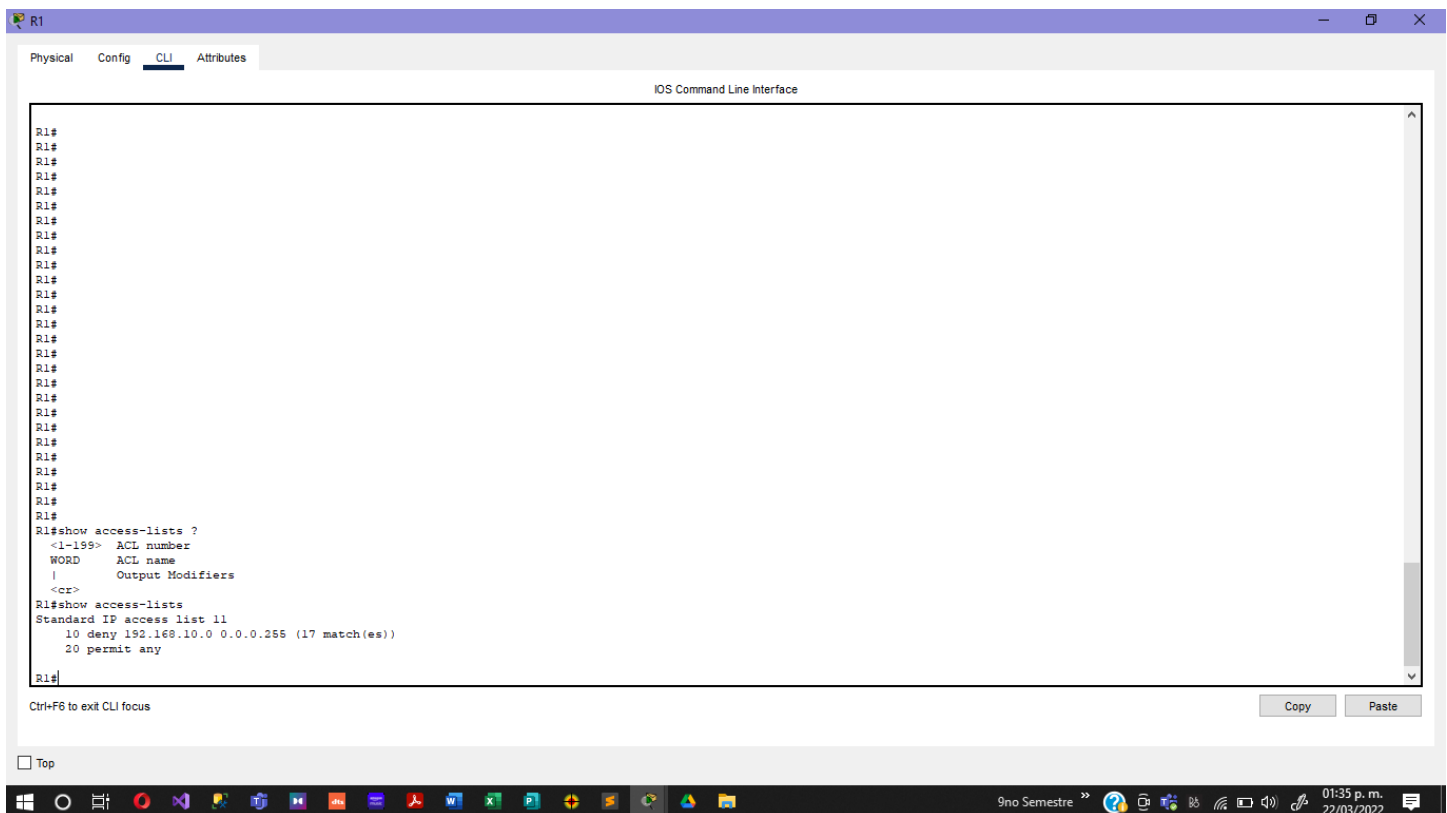
Si conoce el número o el nombre de la ACL, puede filtrar aún más el resultado del comando **show**. Sin embargo, el **R1** tiene solo una ACL, por lo que basta con el comando **show access-lists**.

```
R1#show access-lists
```

Lista de acceso IP estándar 11

```
10 deny 192.168.10.0 0.0.0.255
```

```
20 permit any
```



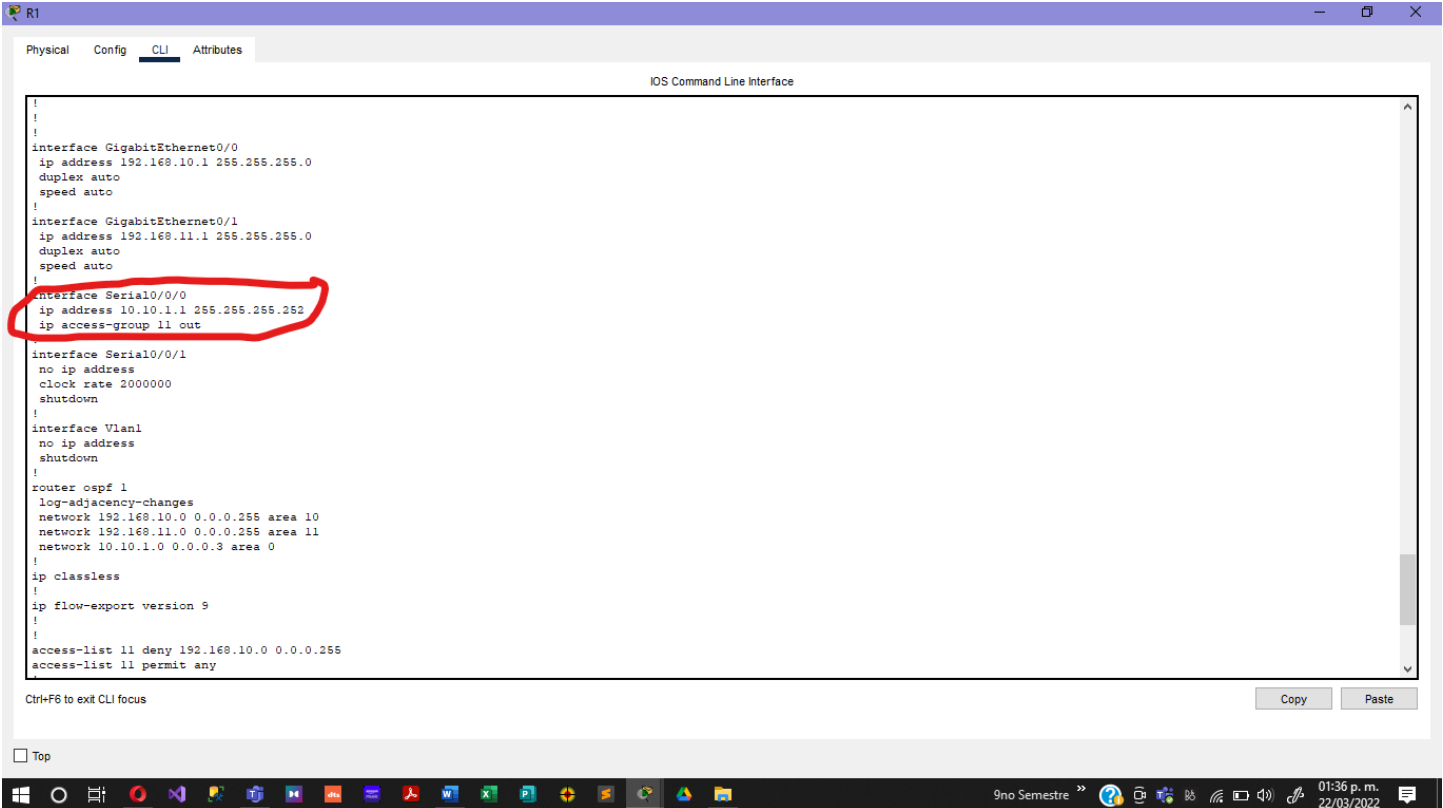
La primera línea de la ACL impide cualquier paquete que se origine en la red **192.168.10.0/24**, lo que incluye los ecos del protocolo de mensajería de control de Internet (ICMP) (solicitudes de ping). La segunda línea de la ACL permite que todo el resto del tráfico **ip** de **cualquier** origen atravesase el router.

- b. Para que una ACL tenga efecto en el funcionamiento del router, debe aplicarse a una interfaz en una dirección específica. En esta situación, la ACL se utiliza para filtrar el tráfico que sale de una interfaz. Por lo tanto, todo el tráfico que sale de la interfaz especificada de R1 se examinará contra la ACL 11.

Aunque pueda ver la información de IP con el comando **show ip interface**, en algunos casos puede ser más eficaz utilizar solo el comando **show run**.

Usando uno o los dos comandos, ¿a qué interfaz y dirección se aplica la ACL?

Salida



```
!
!
!
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.11.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.10.1.1 255.255.255.252
ip access-group 11 out
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.10.0 0.0.0.255 area 10
network 192.168.11.0 0.0.0.255 area 11
network 10.10.1.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 5
!
!
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9no Semestre 01:36 p. m. 22/03/2022

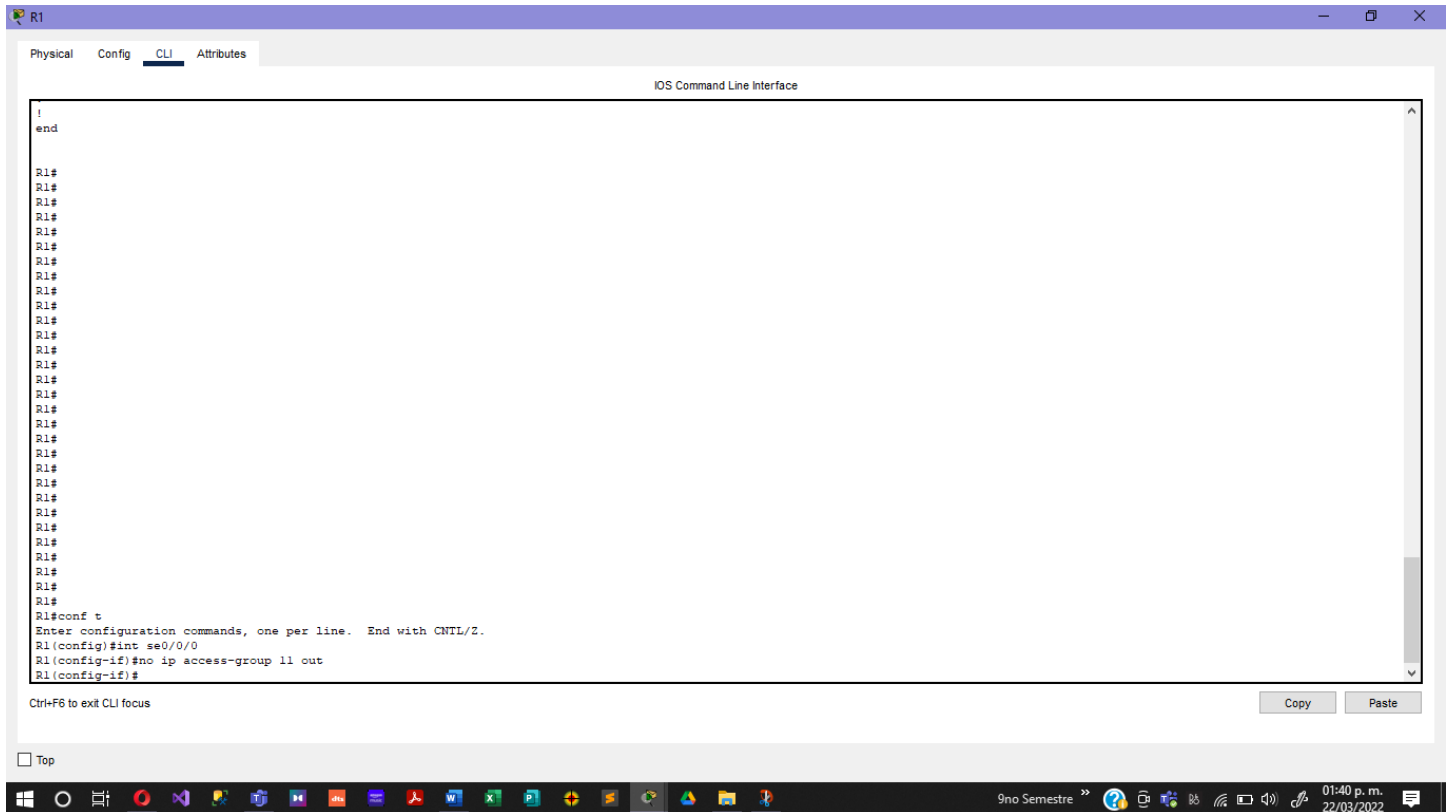
Paso 2: Eliminar la lista de acceso 11 de la configuración.

Es posible eliminar las ACL de la configuración por medio de la emisión del comando **no access list** [número de ACL]. El comando **no access-list** elimina todas las ACL configuradas en el router. El comando **no access-list** [número de ACL] solo elimina una ACL específica.

- a. En la interfaz Serial0/0/0, elimine la lista de acceso 11 aplicada antes a la interfaz como filtro de **salida**:

```
R1 (config)# int se0/0/0
```

```
R1(config-if)#no ip access-group 11 out
```



- b. En el modo de configuración global, elimine la ACL por medio del siguiente comando:

```
R1 (config)# no access-list 11
```

c. Verifique que la **PC1** ahora pueda hacer ping al **servidor DNS** y a **PC4**.

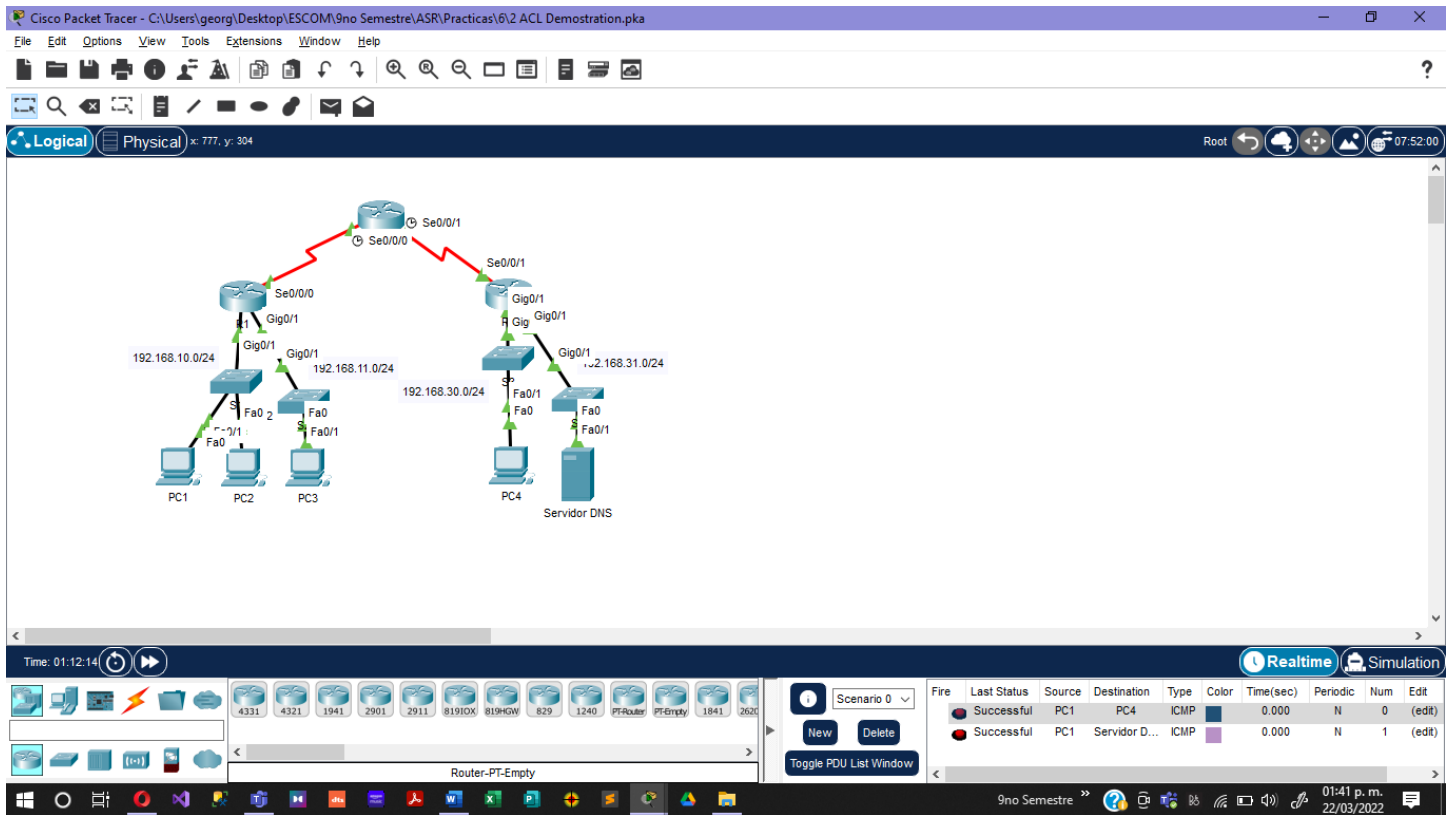


Tabla de calificación sugerida

Ubicación de la consulta	Puntos posibles	Puntos obtenidos
Parte 1, paso 1 b.	50	
Parte 1, paso 2 b.	40	
Parte 2, paso 2 b.	10	
Puntuación total	100	