



INSTITUTO POLITÉCNICO
NACIONAL



ESCUELA SUPERIOR DE CÓMPUTO

ADMINISTRACIÓN DE SERVICIOS EN RED

Práctica 6 - ACL estándar

Autor:
Hernández Castellanos César Uriel

Docente:
Henestrosa Carrasco Leticia

Ingeniería en Sistemas Computacionales

13 de Septiembre de 2019

Índice

.2 Índice de figurā	3	Introducción.	4
2. Objetivo general.	4		
3. Objetivos específicos.	4		
4. Topología.	4		
5. Desarrollo.	4		
5.1. Investigar la configuración actual de la red	4		
5.1.1. Visualizar la configuración en ejecución en los router	4		
5.1.2. Confirmar que todos los dispositivos puedan acceder a todas las demás ubicaciones	8		
6. Evaluar una política de red y planificar una implementación de ACL	10		
7. Resultados	15		
8. Conclusión	15		
9. Referencias	15		

Índice de figuras

1.	Topología	4
2.	Configuración en ejecución del router R1 (P1)	5
3.	Configuración en ejecución del router R1 (P2)	5
4.	Configuración en ejecución del router R1 (P3)	6
5.	Configuración en ejecución del router R2	6
6.	Configuración en ejecución del router R3	7
7.	Tabla de enrutamiento de R1	7
8.	Tabla de enrutamiento de R2	8
9.	Tabla de enrutamiento de R3	8
10.	Ping desde PC1 a PC2	9
11.	Ping desde PC2 a un host externo	9
12.	Ping desde PC4 a un servidor Web/TFTP	10
13.	Configuración de ACL 1	10
14.	Ping desde PC1 a PC2	11
15.	Ping desde PC2 a PC1	11
16.	Configuración de ACL2	12
17.	Ping desde PC2 a los dispositivos que pertenecen a ISP	12
18.	Restringiendo al host 192.168.30.128	13
19.	Denegando el acceso	13
20.	Ping desde Web/TFTP Server a PC4	13
21.	Ping de PC4 a Web/FTPServer	14
22.	Ping de PC3 a PC1	14
23.	Resultado final de la actividad	15

1. Introducción.

La ACL estándar son guiones de configuración del router que controlan si un router acepta o rechaza paquetes según la dirección de origen. Esta práctica 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 se encuentran configurados, lo que incluye direcciones IP y enrutamiento EIGRP.

2. Objetivo general.

Aprender a configurar ACL estándar

3. Objetivos específicos.

1. Investigar la configuración actual de la red
2. Evaluar una política de red y planificar una implementación de ACL
3. Configurar ACL estándar numeradas.
4. Configurar ACL estándar nombradas

4. Topología.

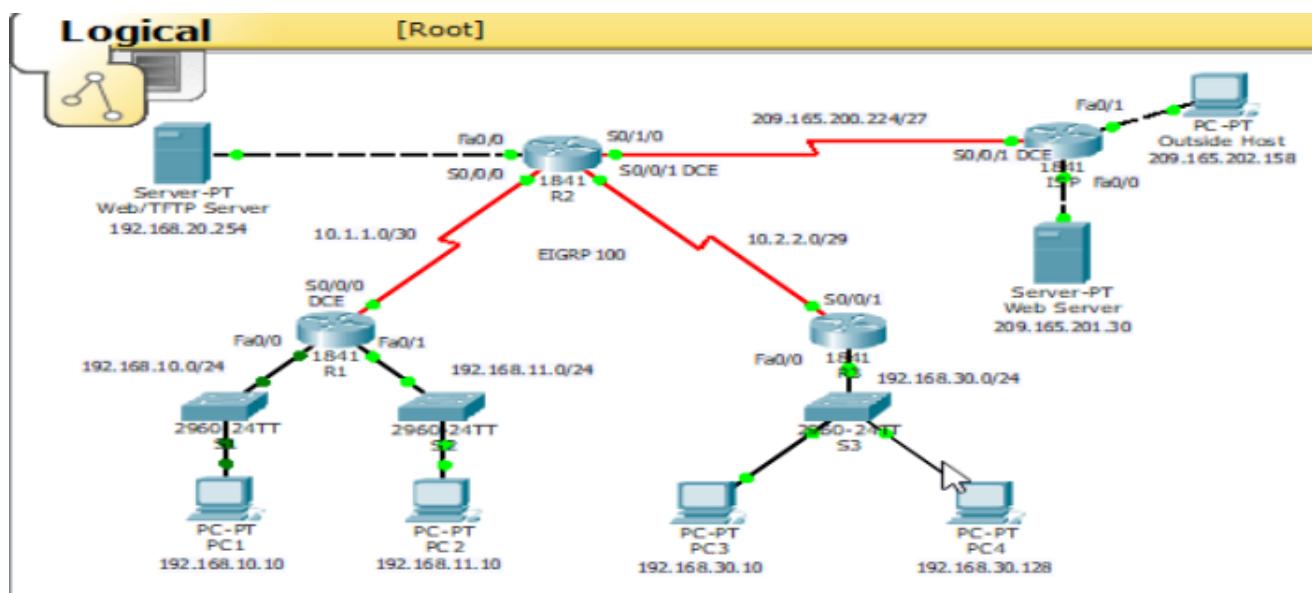


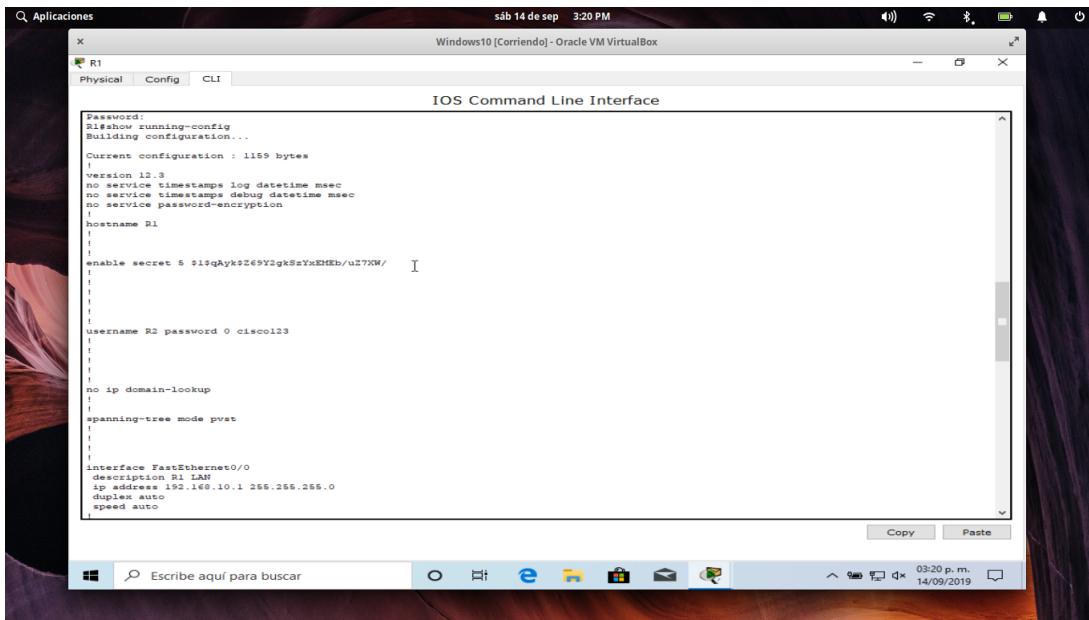
Figura 1: Topología

5. Desarrollo.

5.1. Investigar la configuración actual de la red

5.1.1. Visualizar la configuración en ejecución en los router

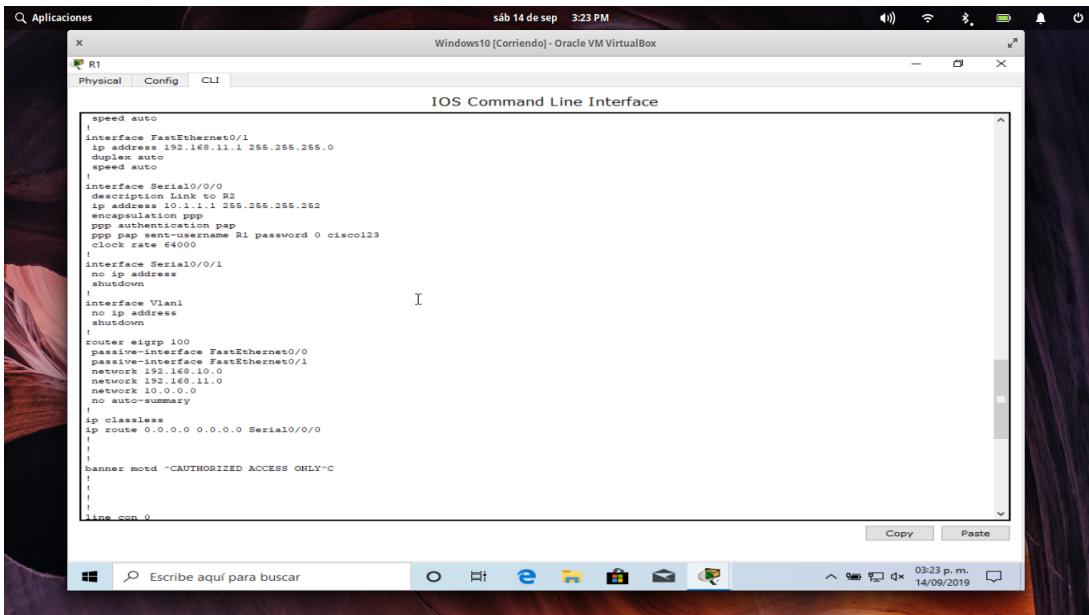
Visualice las configuraciones en ejecución en los tres routers por medio del comando `show running config` mientras está en el modo EXEC privilegiado. Observar que las interfaes y el enrutamiento están totalmente configurados.



```

Password:
R1#show running-config
Building configuration...
Current configuration : 1159 bytes
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
!
!
!
!
!
!
username R2 password 0 cisco123
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/0
description R1 LAN
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
```

Figura 2: Configuración en ejecución del router R1 (P1)



```

speed auto
interface FastEthernet0/1
ip address 192.168.11.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
description Link to R2
ip address 10.1.1.1 255.255.255.252
ppp authentication pap
ppp pap sent-username R1 password 0 cisco123
clock rate 64000
!
interface Serial0/0/1
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 192.168.11.0
network 10.0.0.0
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
!
banner motd ^CAUTHORIZED ACCESS ONLY^C
!
!
line con 0
!
```

Figura 3: Configuración en ejecución del router R1 (P2)

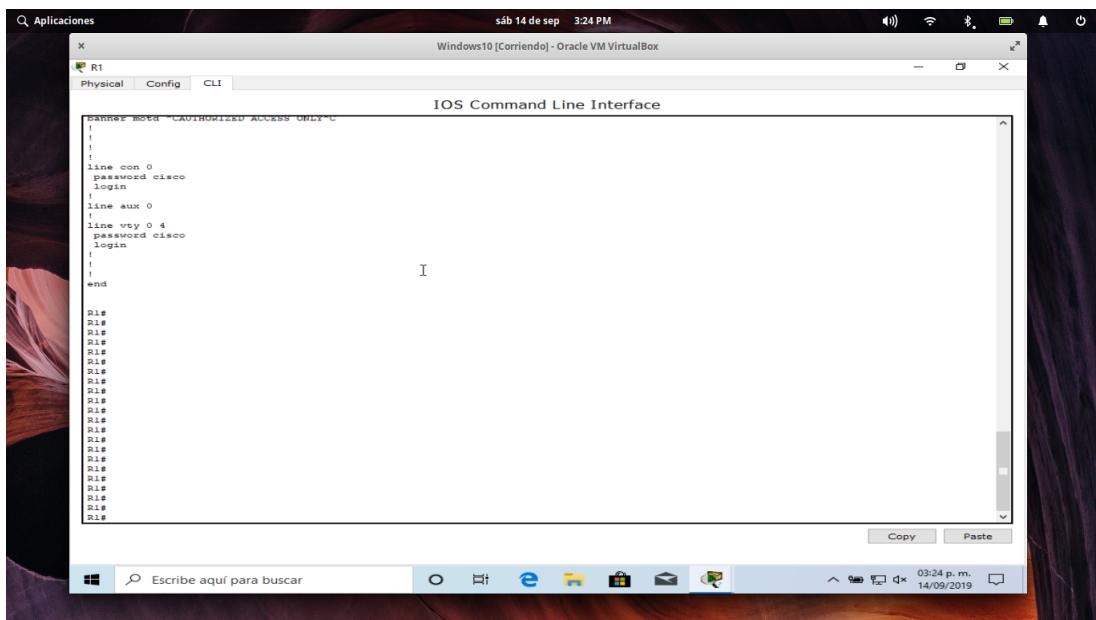


Figura 4: Configuración en ejecución del router R1 (P3)

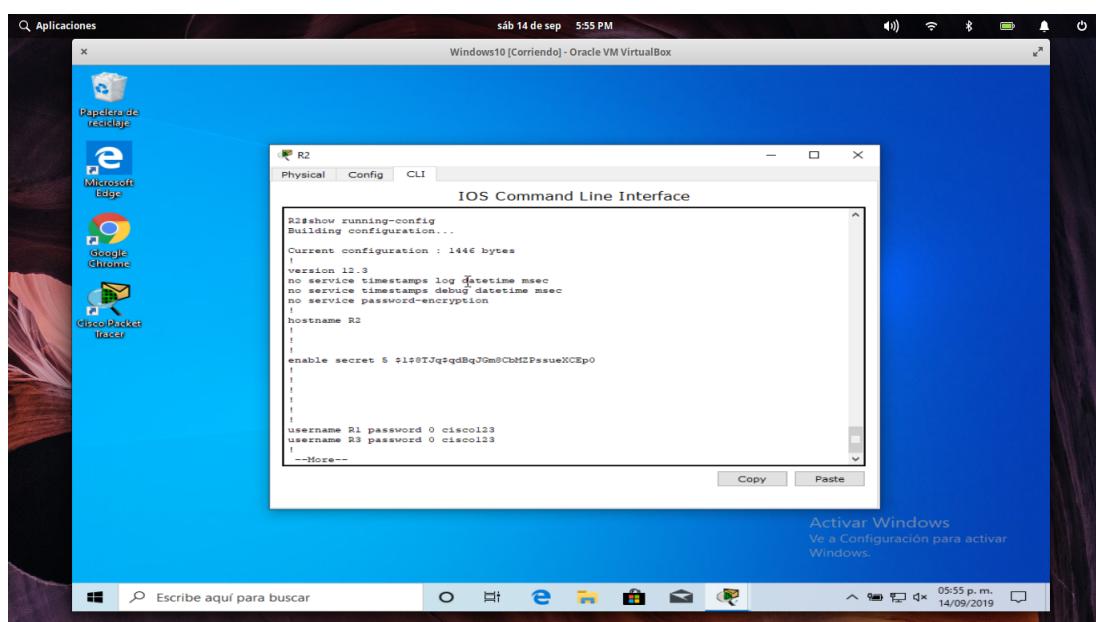


Figura 5: Configuración en ejecución del router R2

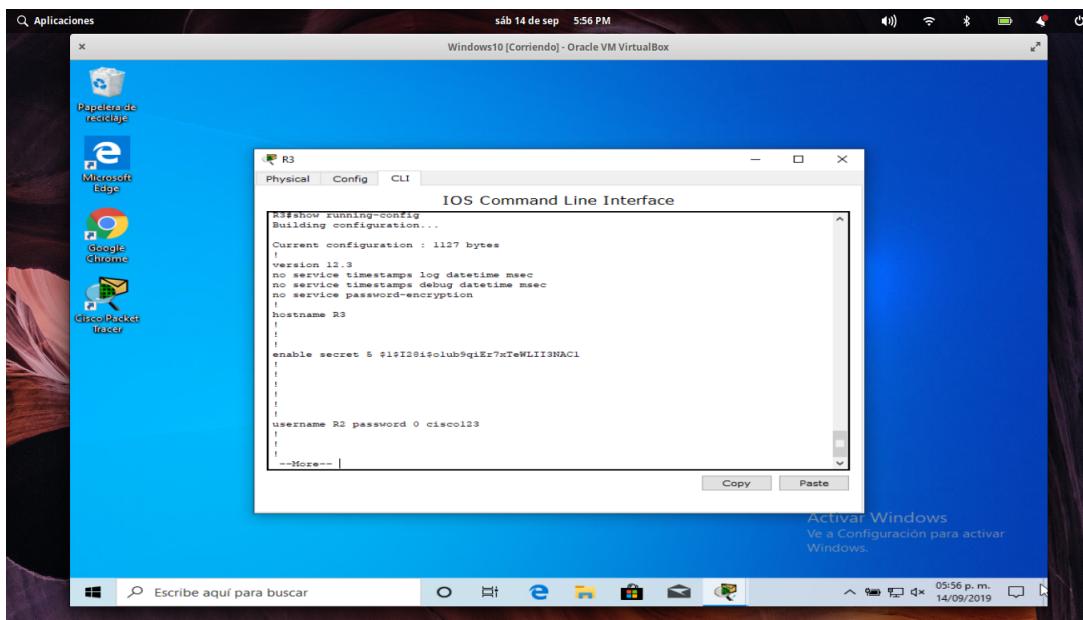


Figura 6: Configuración en ejecución del router R3

Antes de aplicar cualquier ACL en una red, es importante confirmar que exista conectividad completa.

A continuación se mostraran las tablas de enrutamiento en cada dispositivo esto con el fin de asegurar de que cada red figure.

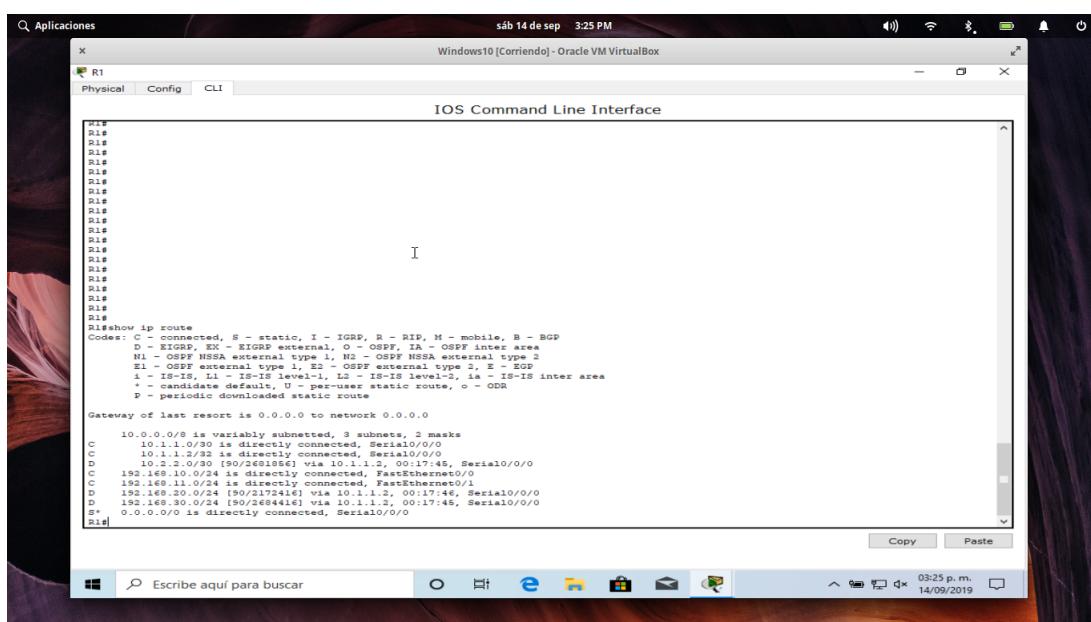


Figura 7: Tabla de enrutamiento de R1

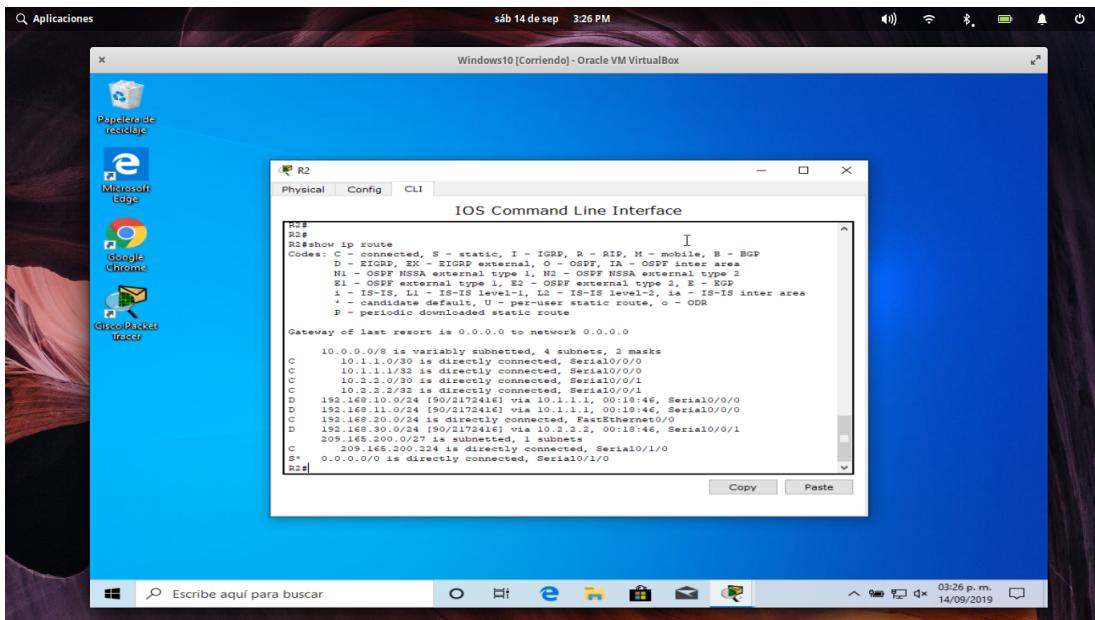


Figura 8: Tabla de enrutamiento de R2

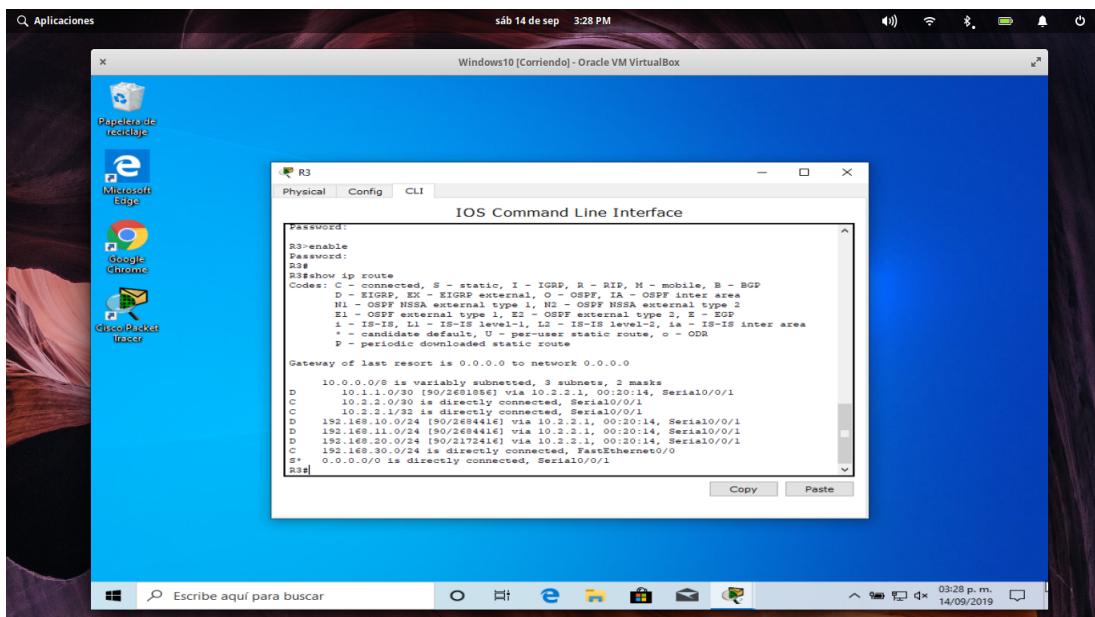


Figura 9: Tabla de enrutamiento de R3

5.1.2. Confirmar que todos los dispositivos puedan acceder a todas las demás ubicaciones

Aunque la tabla de enrutamiento puede ser de utilidad, la conectividad aún debe probarse haciendo ping.

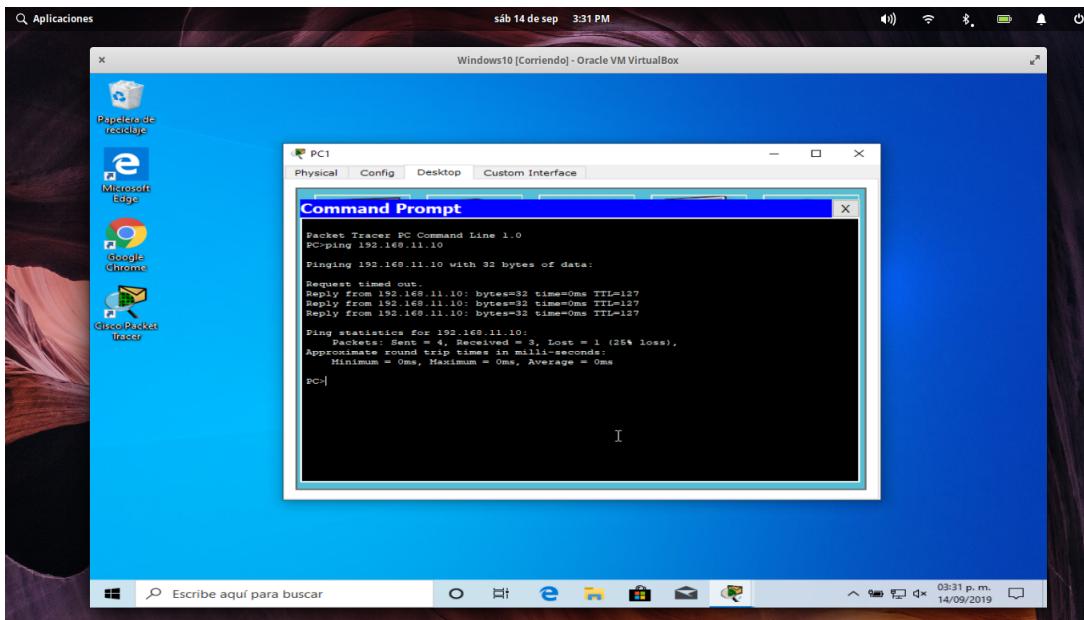


Figura 10: Ping desde PC1 a PC2

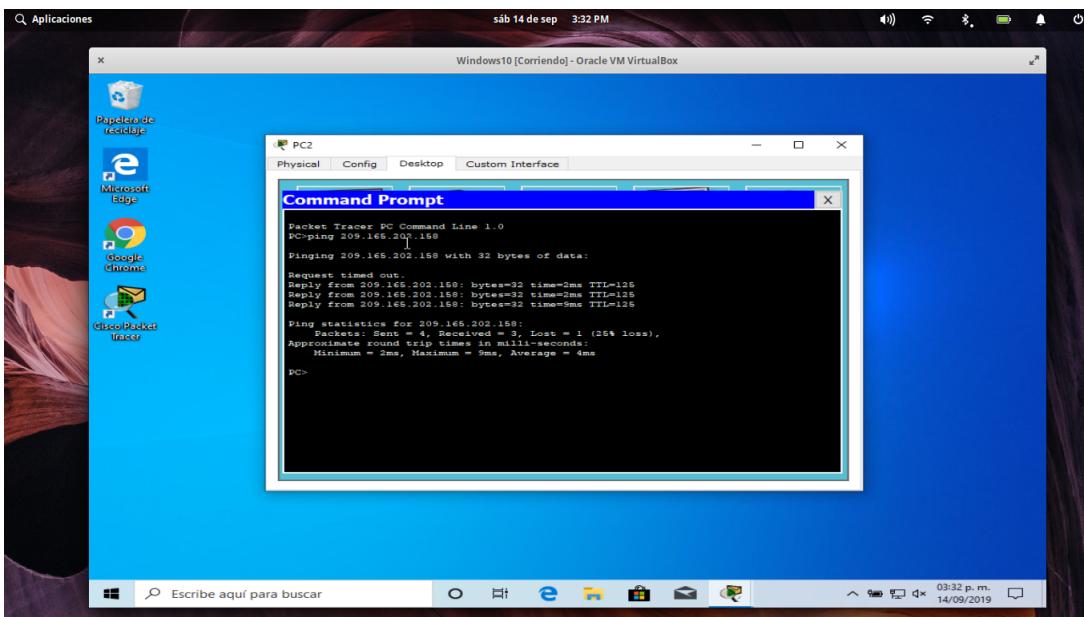


Figura 11: Ping desde PC2 a un host externo

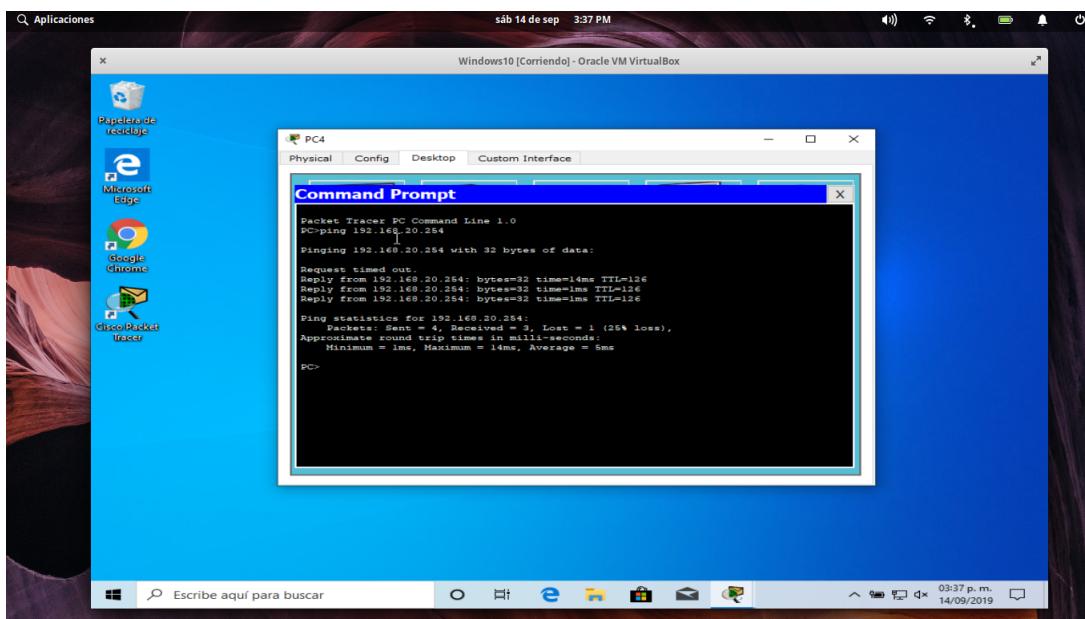


Figura 12: Ping desde PC4 a un servidor Web/TFPT

Con esto finalizamos nuestras pruebas de conectividad

6. Evaluar una política de red y planificar una implementación de ACL

La red 192.168.10.0/24 puede acceder a todas las ubicaciones, excepto a la red 192.168.11.0/24

```

R1
Physical Config CLI
IOS Command Line Interface

Password:
R1#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)#ac
R1(config)#access-list 10 de
R1(config)#access-list 10 deny 192.168.11.0
0.0.0.255
R1(config)#ac
R1(config)#access-list 10 pe
R1(config)#access-list 10 permit a
R1(config)#access-list 10 permit any
R1(config)#int f0/1
R1(config-if)#ip
R1(config-if)#ip a
R1(config-if)#ip ac
R1(config-if)#ip access-group 10 |

```

Figura 13: Configuración de ACL 1

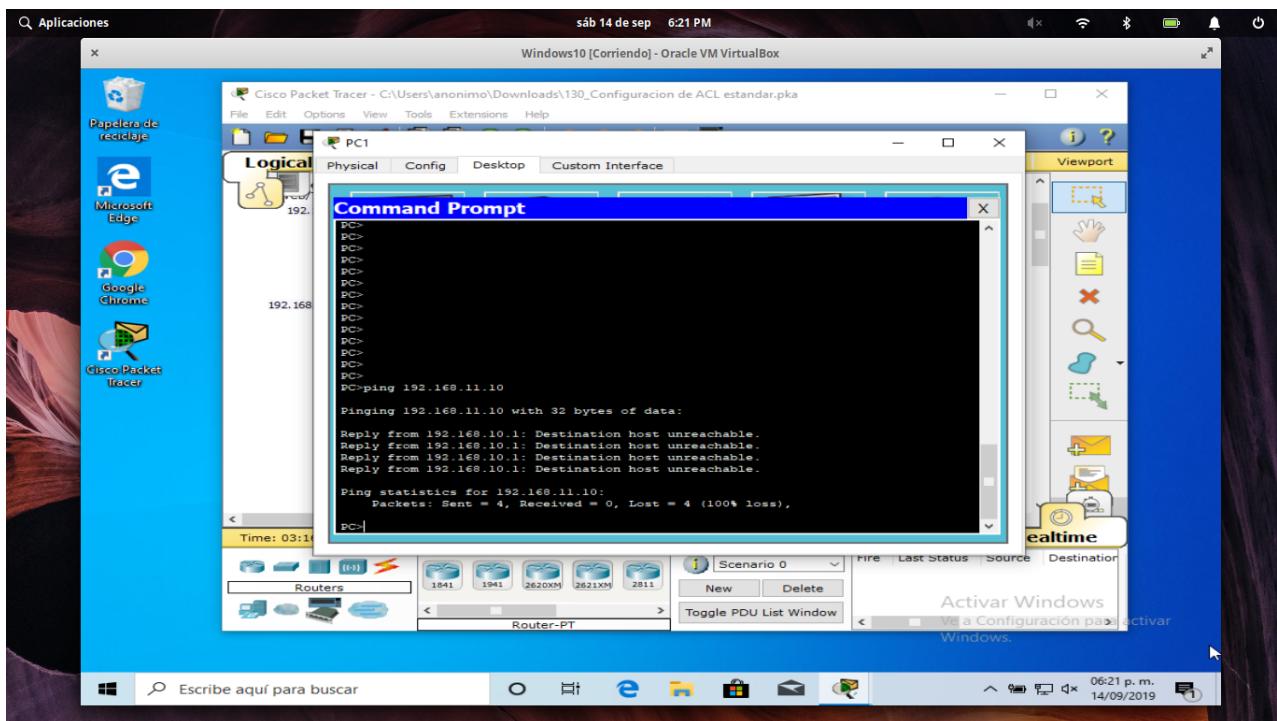


Figura 14: Ping desde PC1 a PC2

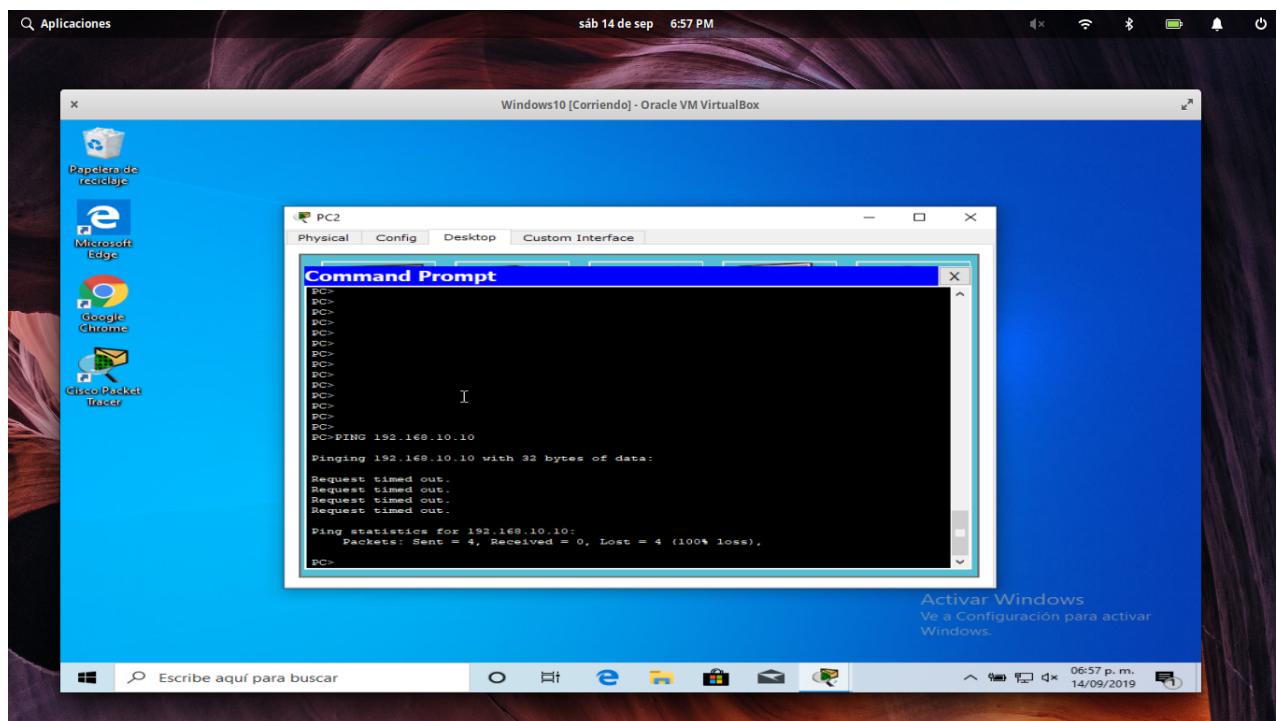
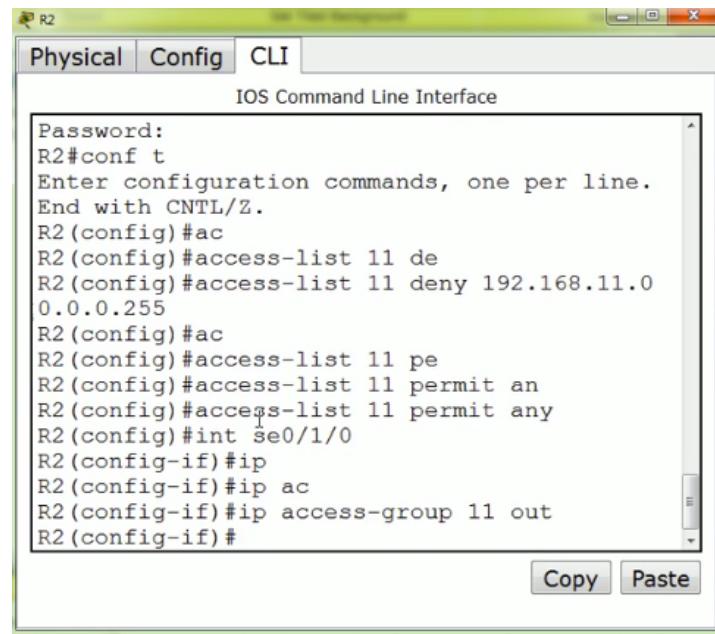


Figura 15: Ping desde PC2 a PC1

La red 192.168.11.0/24 puede acceder a todos los demás destinos, excepto a cualquier red conectada al ISP



```

R2
Physical Config CLI
IOS Command Line Interface
Password:
R2#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
R2(config)#ac
R2(config)#access-list 11 de
R2(config)#access-list 11 deny 192.168.11.0
0.0.0.255
R2(config)#ac
R2(config)#access-list 11 pe
R2(config)#access-list 11 permit an
R2(config)#access-list 11 permit any
R2(config)#int se0/1/0
R2(config-if)#ip
R2(config-if)#ip ac
R2(config-if)#ip access-group 11 out
R2(config-if)#

```

Figura 16: Configuración de ACL2

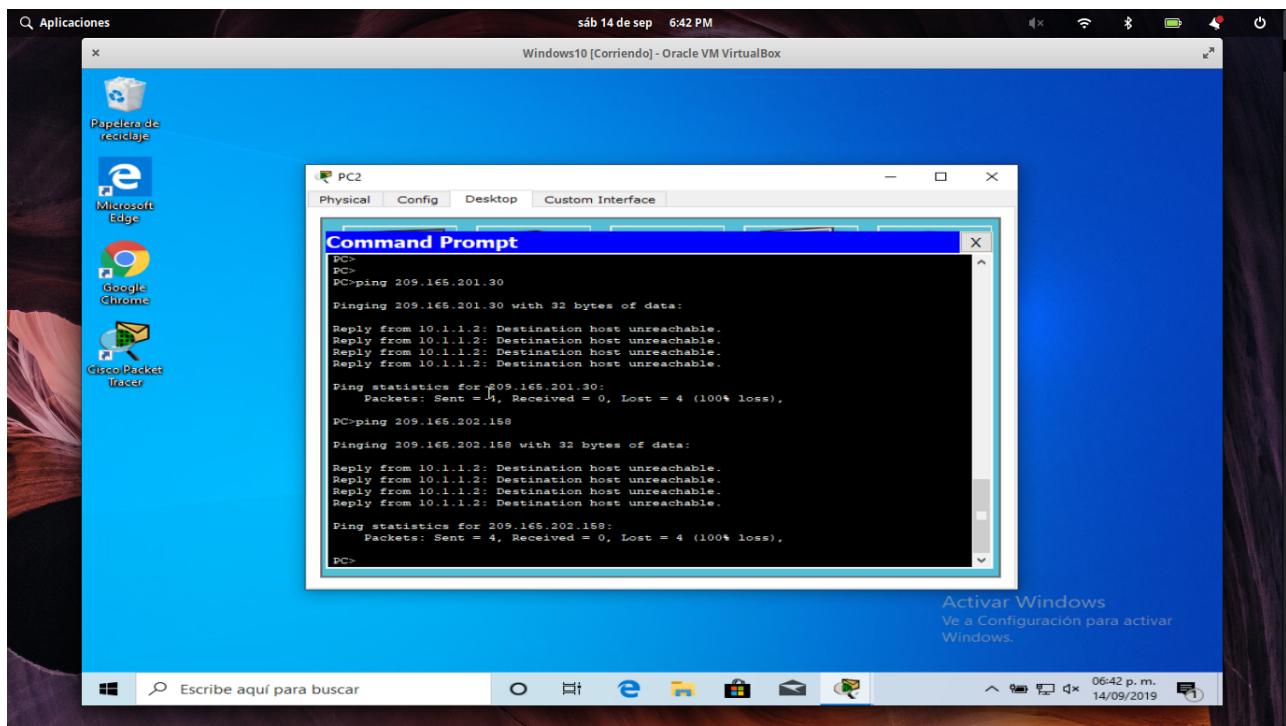
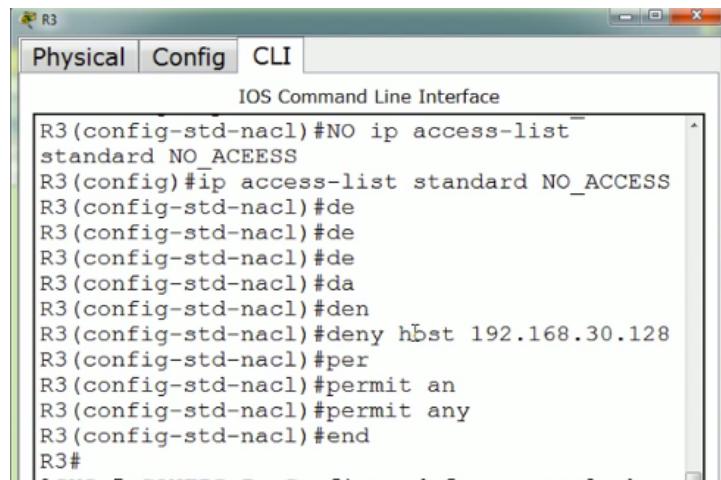


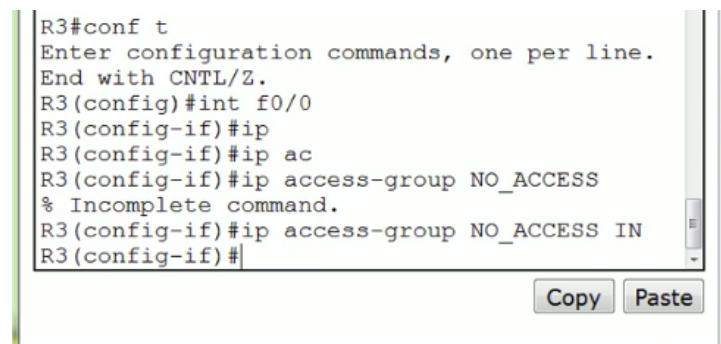
Figura 17: Ping desde PC2 a los dispositivos que pertenecen a ISP

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



```
R3(config-std-nacl)#NO ip access-list
standard NO_ACESS
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#de
R3(config-std-nacl)#de
R3(config-std-nacl)#da
R3(config-std-nacl)#den
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#per
R3(config-std-nacl)#permit any
R3(config-std-nacl)#end
R3#
```

Figura 18: Restringiendo al host 192.168.30.128



```
R3#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
R3(config)#int f0/0
R3(config-if)#ip
R3(config-if)#ip ac
R3(config-if)#ip access-group NO_ACCESS
% Incomplete command.
R3(config-if)#ip access-group NO_ACCESS IN
R3(config-if)#

```

Figura 19: Denegando el acceso

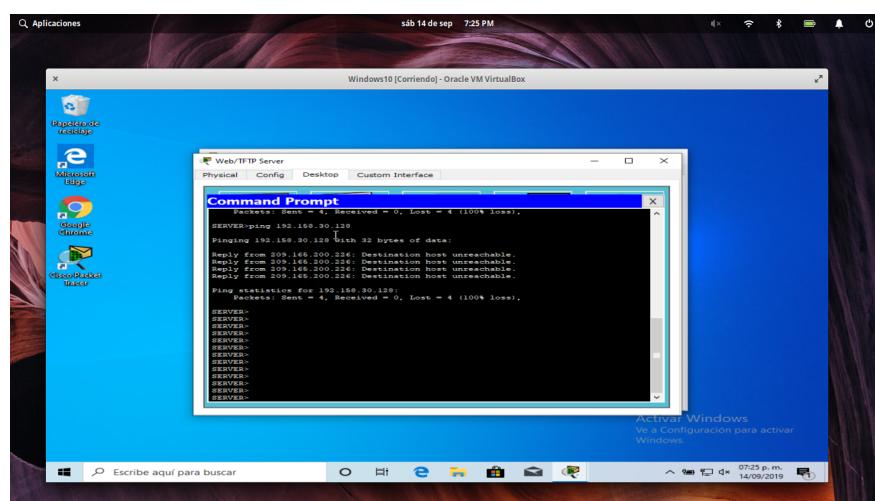


Figura 20: Ping desde Web/TFTP Server a PC4

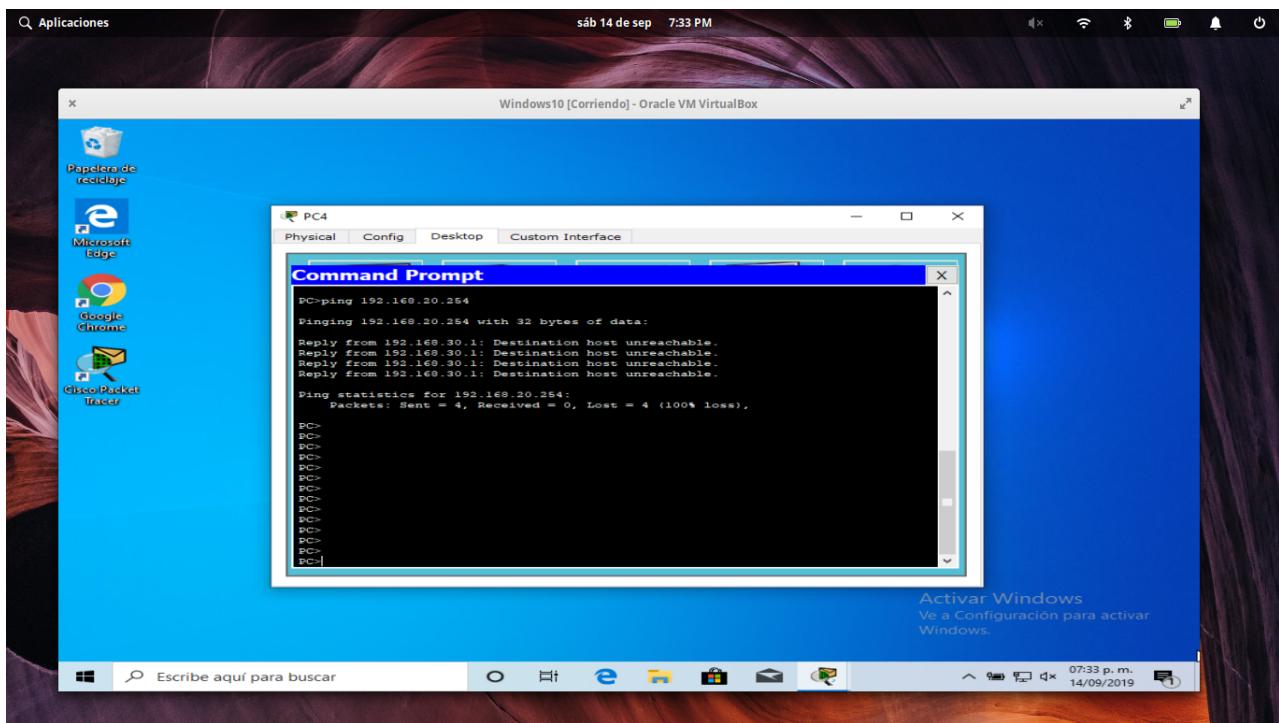


Figura 21: Ping de PC4 a Web/FTPServer

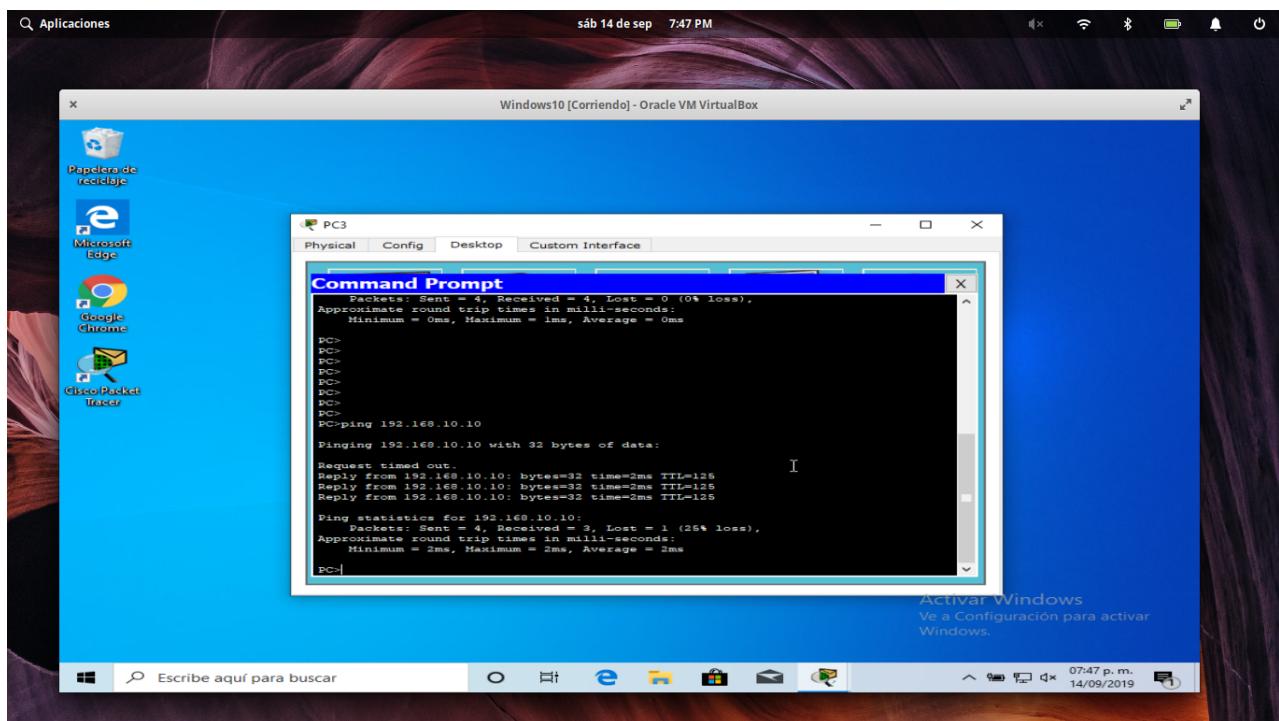


Figura 22: Ping de PC3 a PC1

7. Resultados

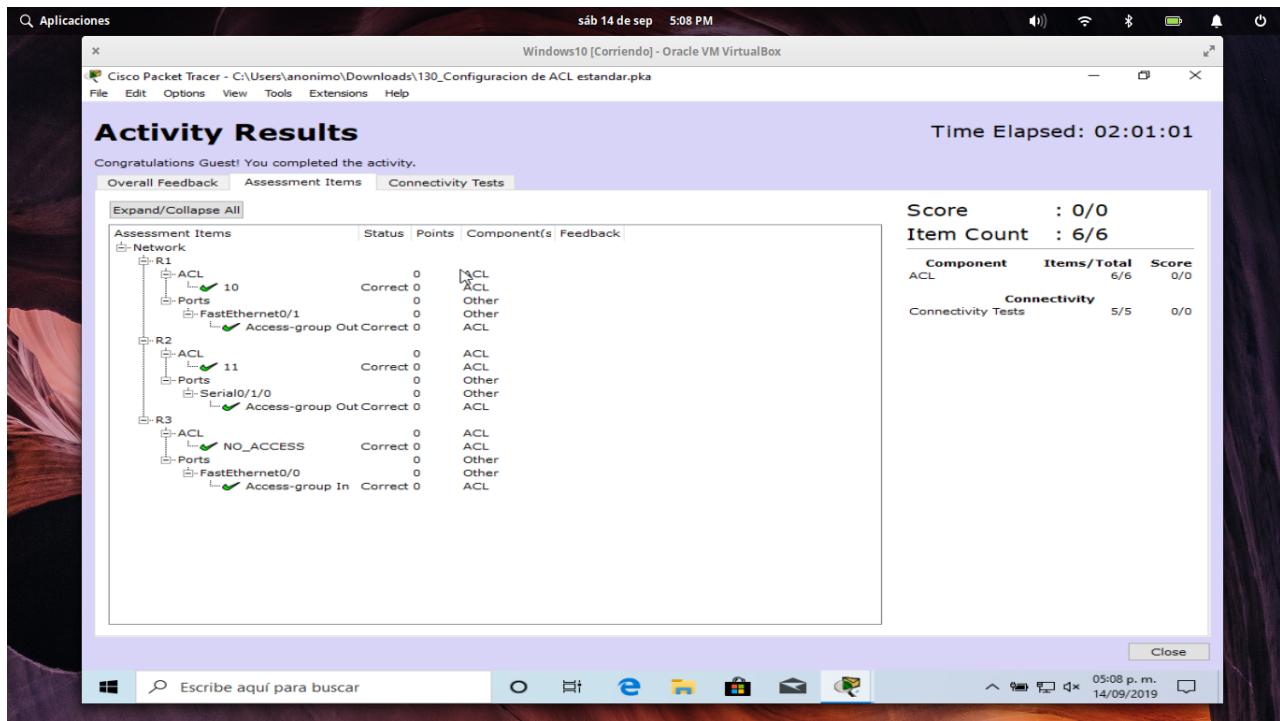


Figura 23: Resultado final de la actividad

8. Conclusión

Las ACL nos sirven como mecanismo para extender/reducir los privilegios de diferentes dispositivos y como mecanismo de tráfico entrante y saliente en dispositivos router. Pero en ambos casos el objetivo es la separación de privilegios y así establecer los permisos idóneos para cada caso.

9. Referencias

[1] Cisco Networking Academy Builds IT Skills Education For Future Careers”, Netacad.com, 2019. [Online]. Available: <https://www.netacad.com/es>. [Accessed: 13- Sep- 2019].