



INSTITUTO POLITÉCNICO  
NACIONAL



ESCUELA SUPERIOR DE CÓMPUTO

ADMINISTRACIÓN DE SERVICIOS EN RED

---

## Práctica 7 - ACL extendidas

---

*Autor:*

Hernández Castellanos César Uriel

*Docente:*

Henestrosa Carrasco Leticia

**Ingeniería en Sistemas Computacionales**

13 de Septiembre de 2019

# Índice

.2 Índice de figuras	4
<b>3. Introducción.</b>	
<b>2. Objetivo general.</b>	4
<b>3. Objetivos específicos.</b>	4
<b>4. Desarrollo.</b>	4
4.1. Investigar la configuración actual de la red . . . . .	4
4.1.1. Visualizar la configuración en ejecución en los routers . . . . .	4
4.1.2. Confirmar que todos los dispositivos puedan acceder a todas las demás ubicaciones . . . . .	5
4.2. Evaluar una política de red y planificar una implementación de ACL en R1 . . . . .	6
4.3. Configurar una ACL extendida numerada para R3 . . . . .	11
4.4. Configurar una ACL extendida nombrada en R2 . . . . .	16
4.4.1. Verificando resultados . . . . .	19
<b>5. Comandos</b>	20
<b>6. Conclusiones</b>	21
<b>7. Referencias</b>	21

## Índice de figuras

1.	Configuración en R1 . . . . .	4
2.	Configuración en R2 . . . . .	5
3.	Configuración en R3 . . . . .	5
4.	Pruebas de conectividad a diferentes dispositivos desde R1 . . . . .	6
5.	Configurando la lista de acceso 110 . . . . .	6
6.	Configurando la lista de acceso 111 y 110 . . . . .	7
7.	Visualizando las listas de acceso configuradas . . . . .	7
8.	Configurando la lista de acceso 111 . . . . .	8
9.	Configuración del grupo 110 y 111 . . . . .	8
10.	Pruebas de conexión telnet desde PC1 . . . . .	9
11.	Intentando acceder desde PC1 al servidor Web/TFTP corporativo . . . . .	9
12.	Intentando acceder desde PC2 al servidor Web/TFTP a través de HTTP . . . . .	10
13.	Intentando acceder desde PC1 al servidor Web/TFTP a través de HTTP . . . . .	10
14.	Intentando acceder desde PC1 al servidor Web externo a través de HTTP . . . . .	11
15.	Intentando acceder desde PC2 al servidor Web externo a través de HTTP . . . . .	11
16.	Configurando la lista de acceso 130 . . . . .	12
17.	Configurando la lista de acceso 130 . . . . .	12
18.	Intentando acceder desde R3 al servidor Web/TFTP . . . . .	13
19.	Intentando acceder desde R3 a cualquier dispositivo . . . . .	13
20.	Intentando acceder desde R4 al servidor Web/TFTP . . . . .	14
21.	Realizando una conexión telnet desde PC4 a 192.168.10.1 . . . . .	14
22.	Realizando una conexión telnet desde PC4 a 192.168.11.1 . . . . .	15
23.	Intentando acceder desde PC4 a PC1 Y PC2 . . . . .	15
24.	Realizando conexión telnet de PC4 a R2 en 10.2.2.2 . . . . .	16
25.	Configurando una ACL extendida nombrada en R2 . . . . .	16
26.	Intentando acceder desde el host externo a una página Web en el servidor Web/TFTP interno . . . . .	17
27.	Intentando acceder desde el host externo al servidor Web/TFTP interno . . . . .	17
28.	Realizando un ping desde el host externo a PC1 . . . . .	18
29.	Realizando un ping desde PC1 al servidor Web externo en 209.165.201.30 . . . . .	18
30.	Abriendo una página Web desde PC1 al servidor Web externo . . . . .	19
31.	Resultados finales . . . . .	19
32.	Comandos utilizados en la práctica . . . . .	20

## 1. Introducción.

Las ACL extendidas son guiones de configuración del router que controlan si un router acepta o rechaza paquetes según la dirección origen o destino y protocolos o puertos. Las ACL extendidas proporcionan mayor flexibilidad y especialidad que las ACL estándar. Esta práctica 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.

## 2. Objetivo general.

Aprender a configurar las ACL extendidas.

## 3. Objetivos específicos.

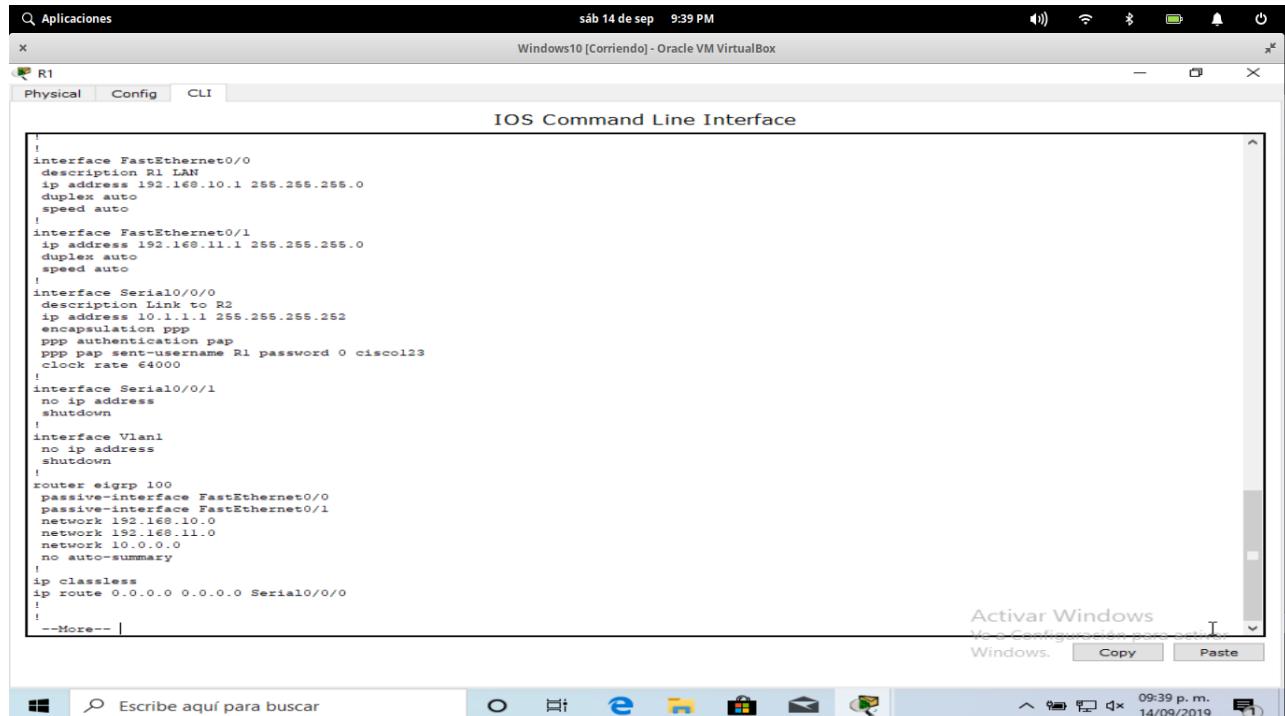
1. Investigar la configuración actual de la red.
2. Evaluar una política de red y planificar una implementación de ACL.
3. Configurar las ACL extendidas numeradas.
4. Configurar ACL extendidas nombradas.

## 4. Desarrollo.

### 4.1. Investigar la configuración actual de la red

#### 4.1.1. 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.



```

! 
interface FastEthernet0/0
description R1 LAN
ip address 192.168.10.1 255.255.255.0
duplex auto
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
encapsulation ppp
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 192.168.10.0
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
!
--More-- |

```

Figura 1: Configuración en R1



Figura 2: Configuración en R2

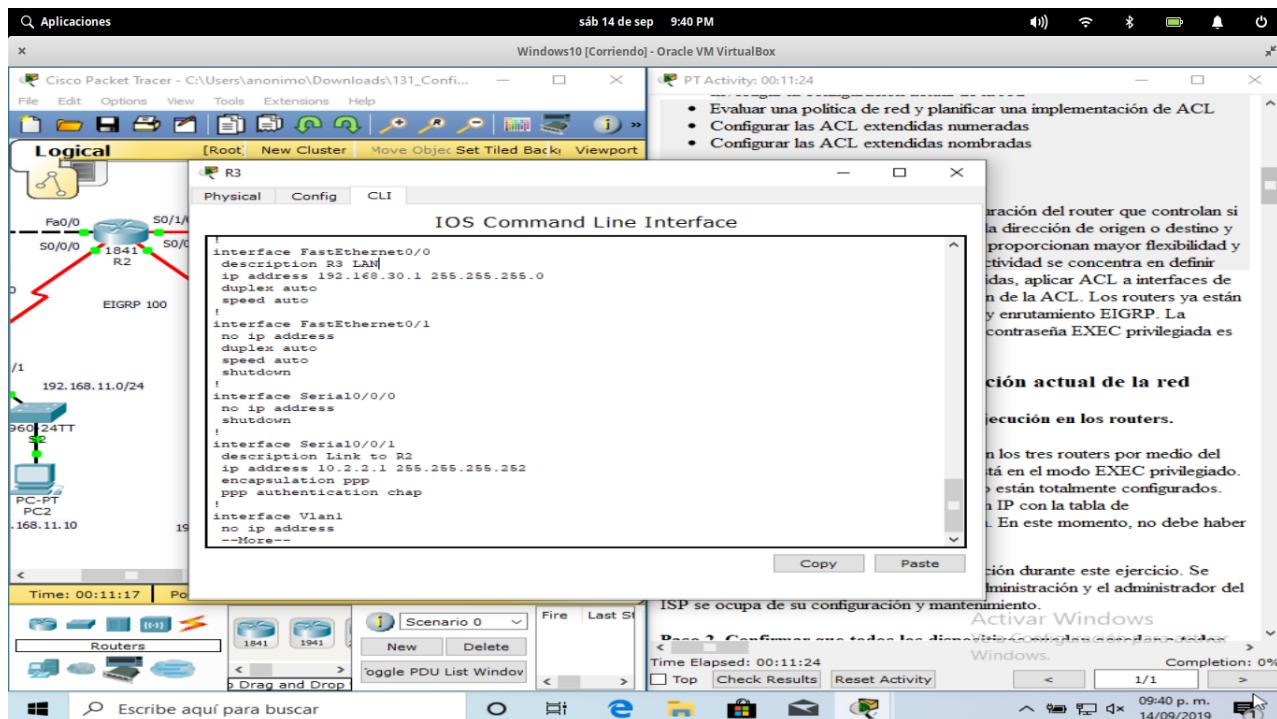


Figura 3: Configuración en R3

#### 4.1.2. 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

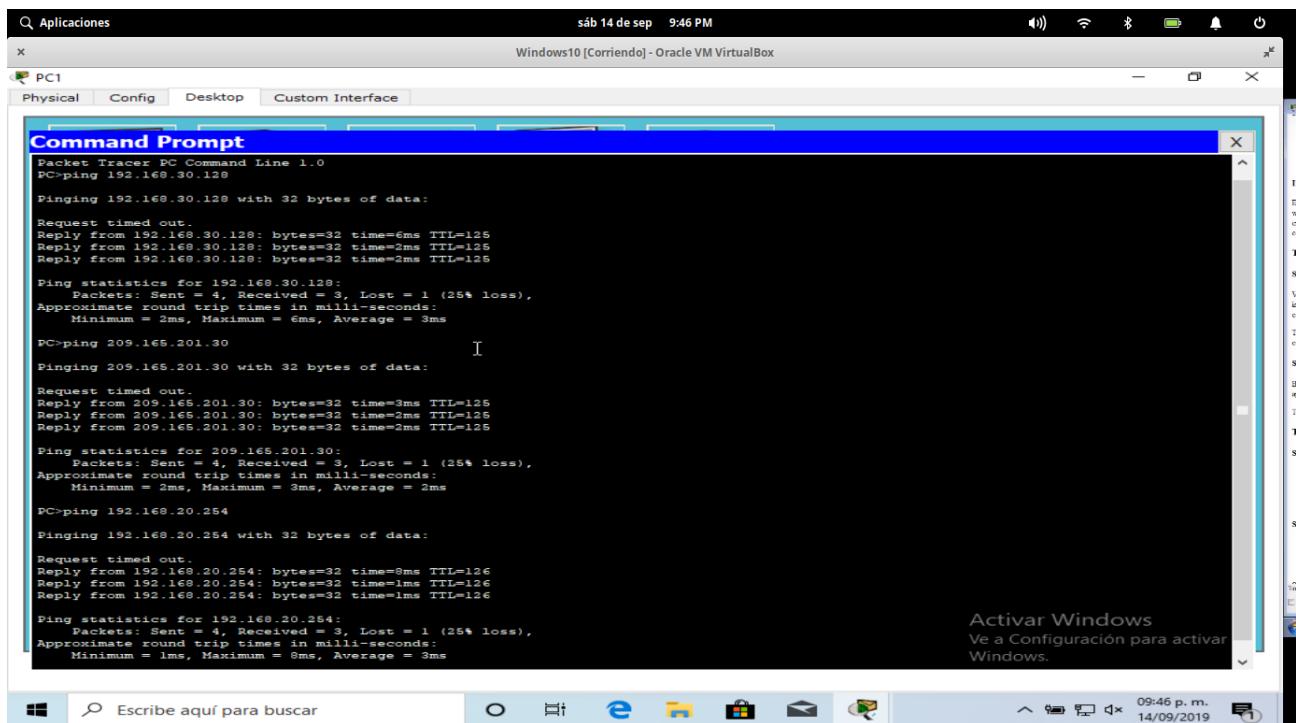


Figura 4: Pruebas de conectividad a diferentes dispositivos desde R1

#### 4.2. Evaluar una política de red y planificar una implementación de ACL en R1

Evaluar la política para las LAN del R1

1. 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 tráfico restante
2. Para la red 192.168.11.0/2, 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

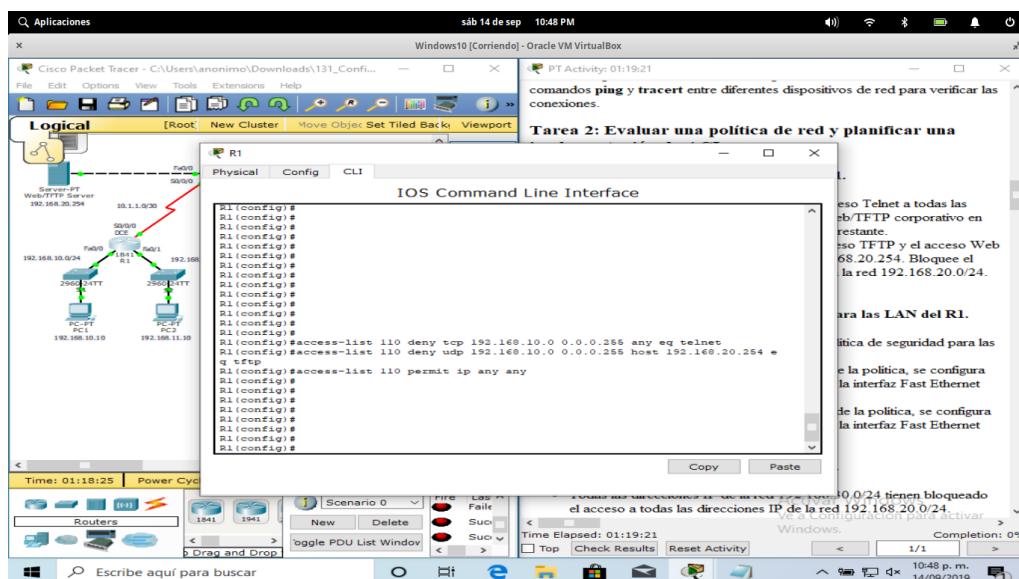


Figura 5: Configurando la lista de acceso 110

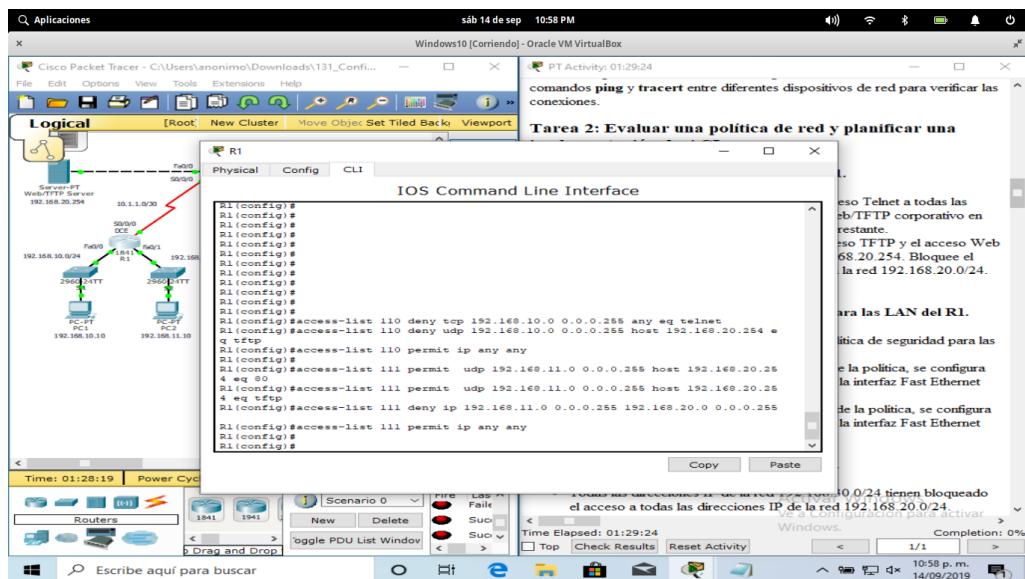


Figura 6: Configurando la lista de acceso 111 y 110

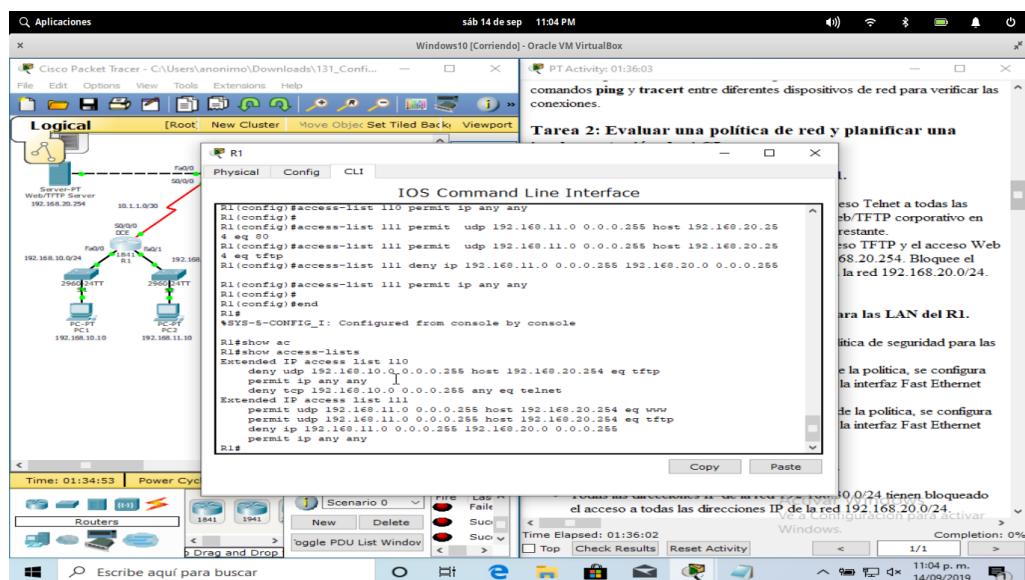


Figura 7: Visualizando las listas de acceso configuradas

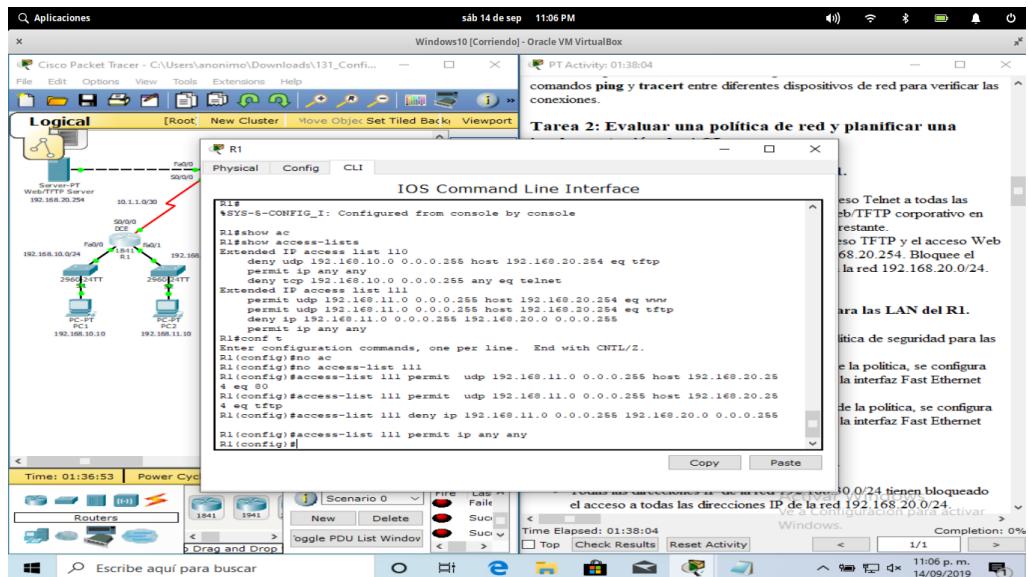


Figura 8: Configurando la lista de acceso 111

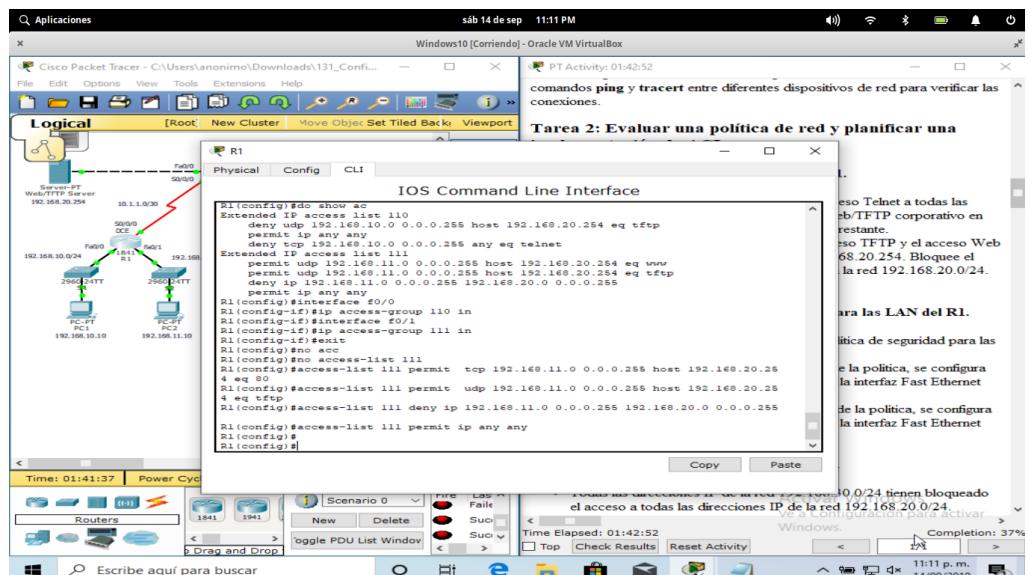


Figura 9: Configuración del grupo 110 y 111

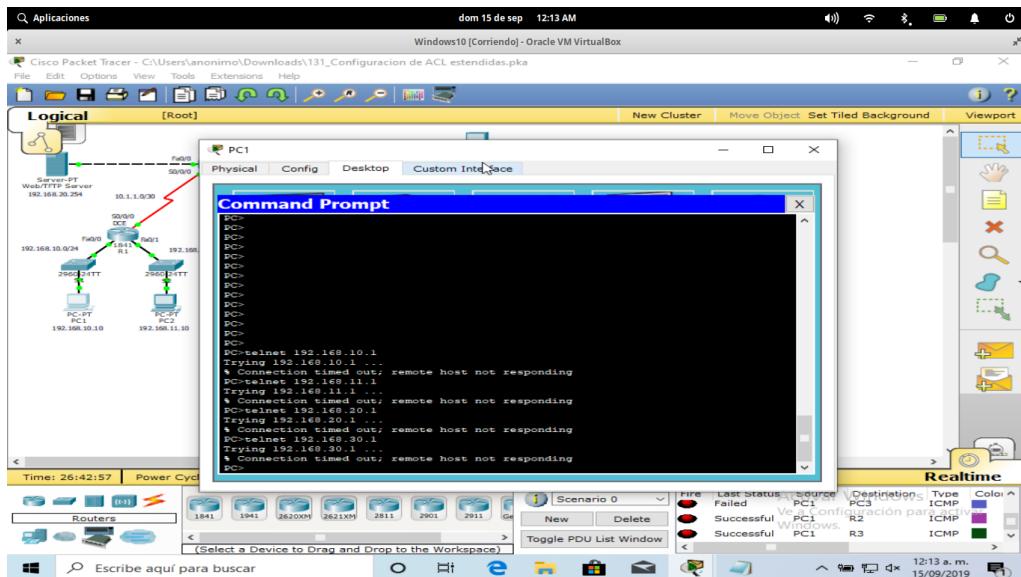


Figura 10: Pruebas de conexión telnet desde PC1

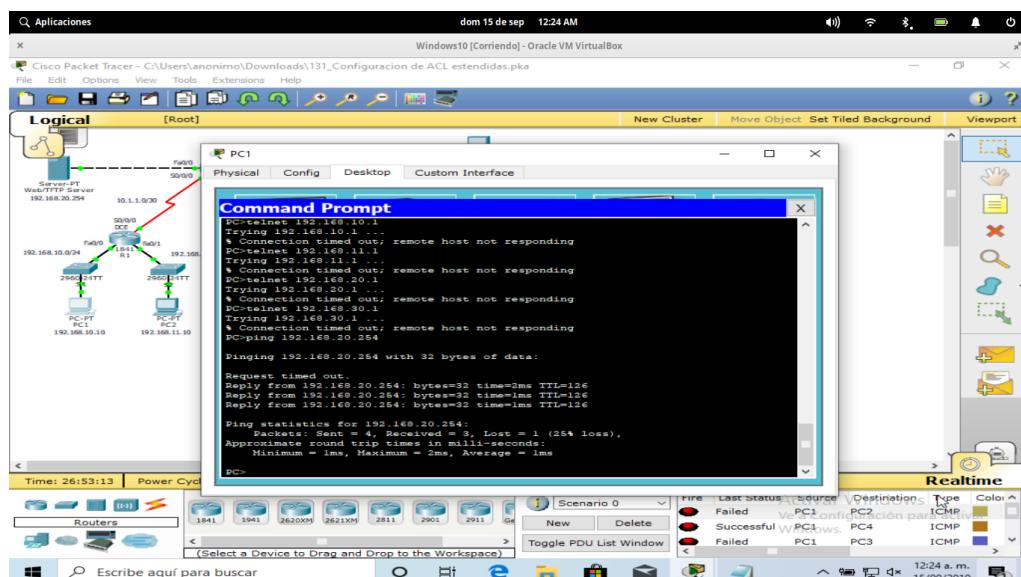


Figura 11: Intentando acceder desde PC1 al servidor Web/TFTP corporativo

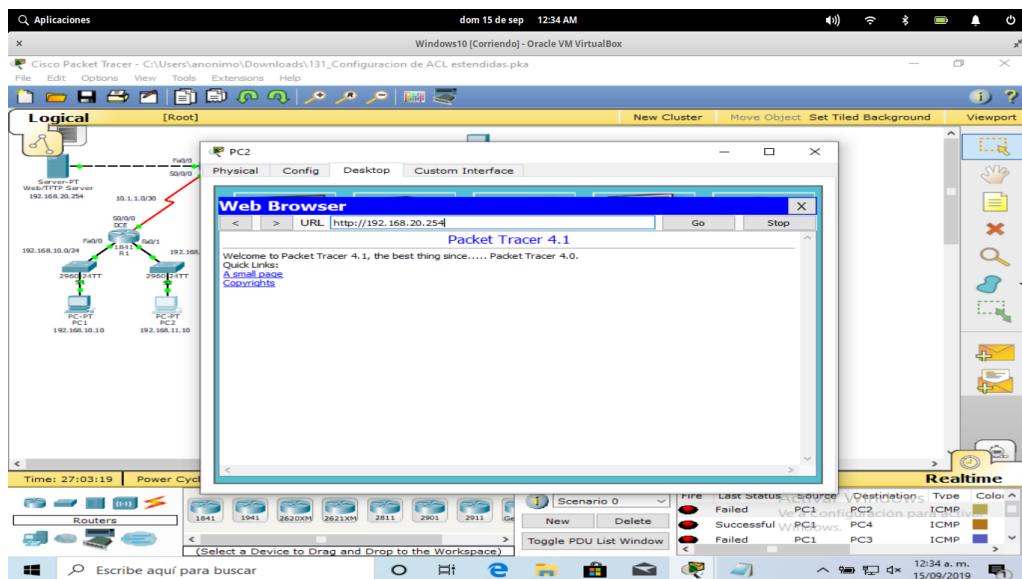


Figura 12: Intentando acceder desde PC2 al servidor Web/TFTP a través de HTTP

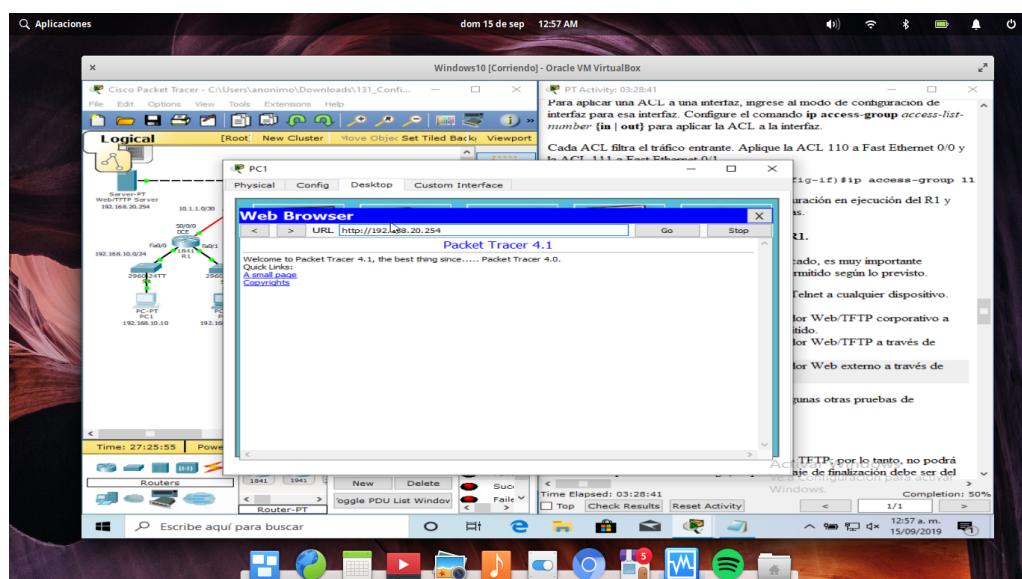


Figura 13: Intentando acceder desde PC1 al servidor Web/TFTP a través de HTTP

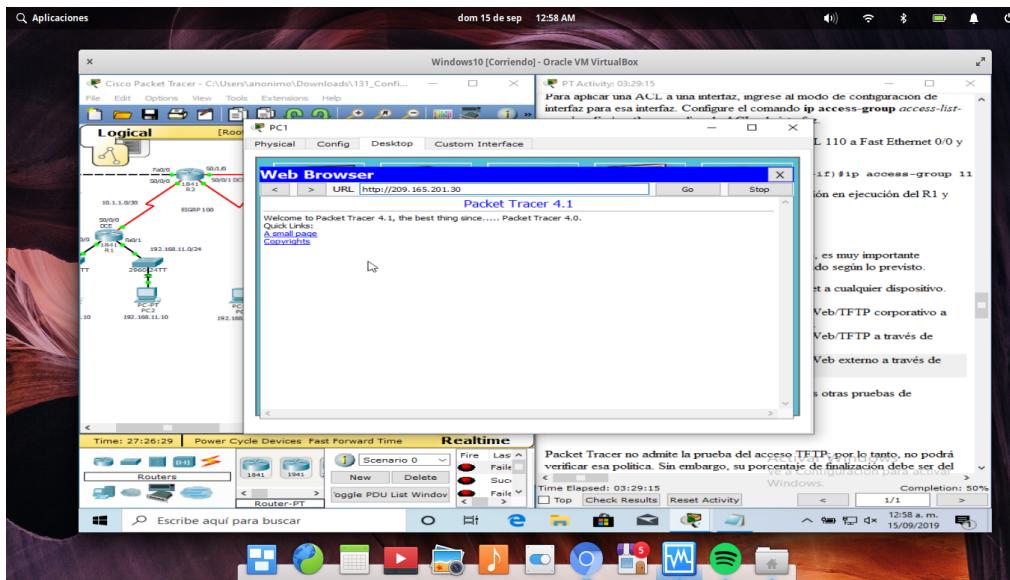


Figura 14: Intentando acceder desde PC1 al servidor Web externo a través de HTTP

#### 4.3. Configurar una ACL extendida numerada para R3

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

1. Denegar el acceso a la red 192.168.20.0/24
2. 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

1. Permitir el acceso a 192.168.10.0 y 192.168.11.0
2. Denegar el acceso a 192.168.20.0
3. Permitir el acceso Web e ICPM a todas las demás ubicaciones

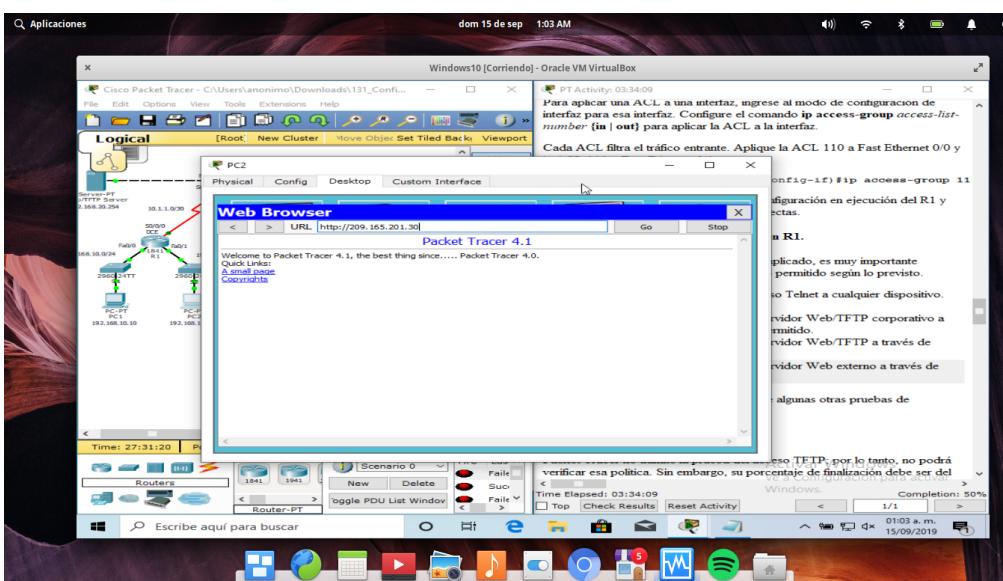


Figura 15: Intentando acceder desde PC2 al servidor Web externo a través de HTTP

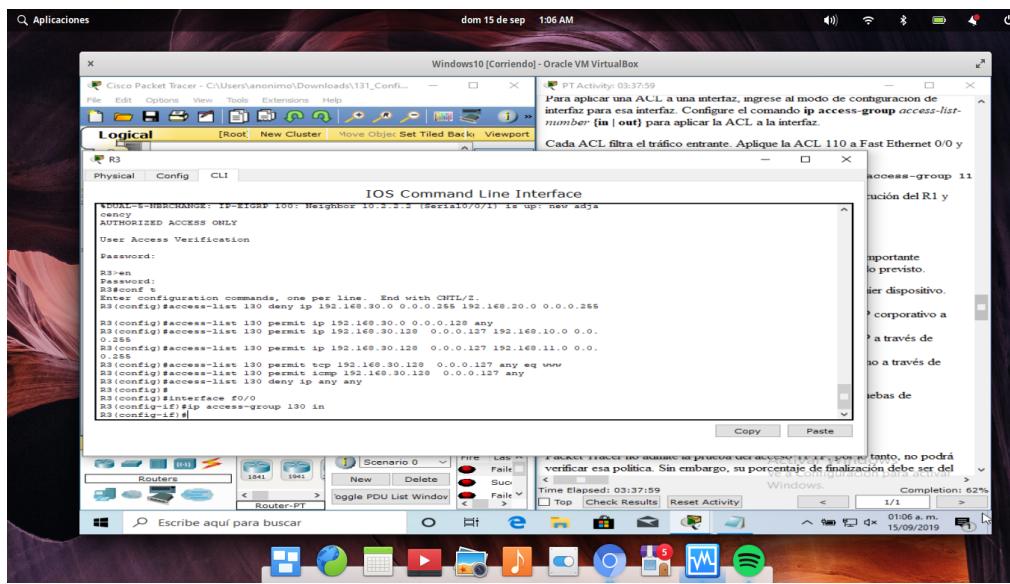


Figura 16: Configurando la lista de acceso 130

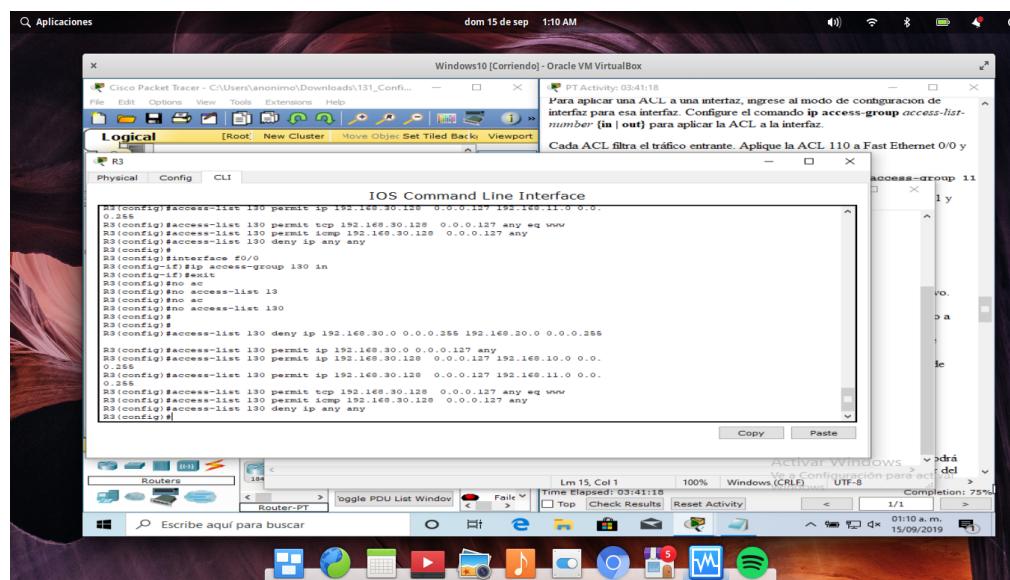


Figura 17: Configurando la lista de acceso 130

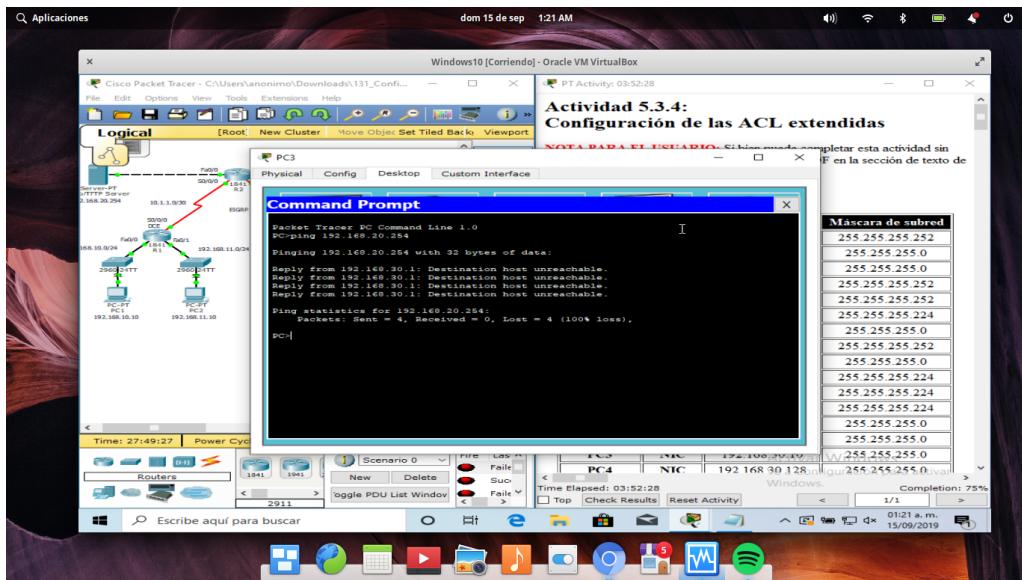


Figura 18: Intentando acceder desde R3 al servidor Web/TFTP

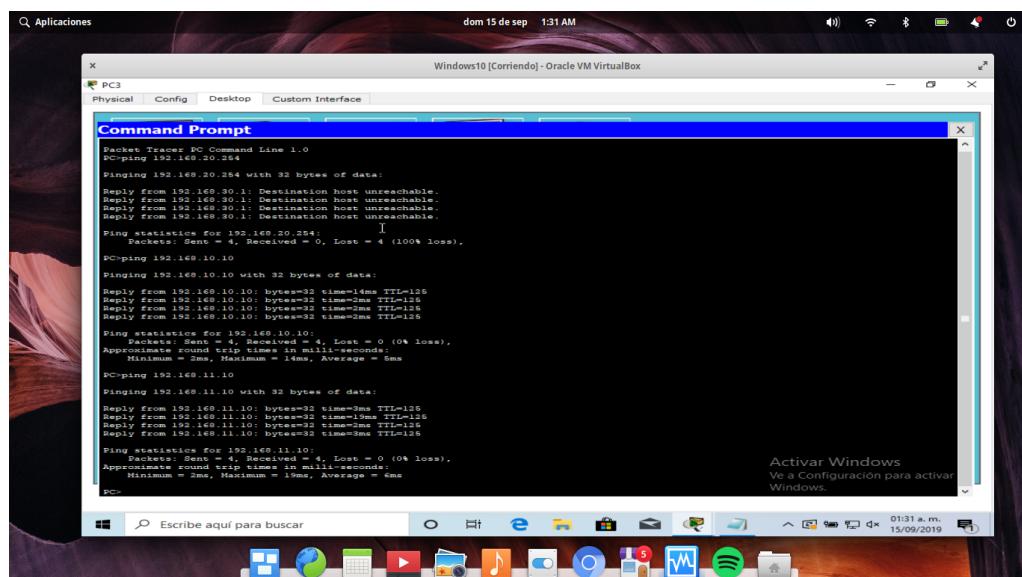


Figura 19: Intentando acceder desde R3 a cualquier dispositivo

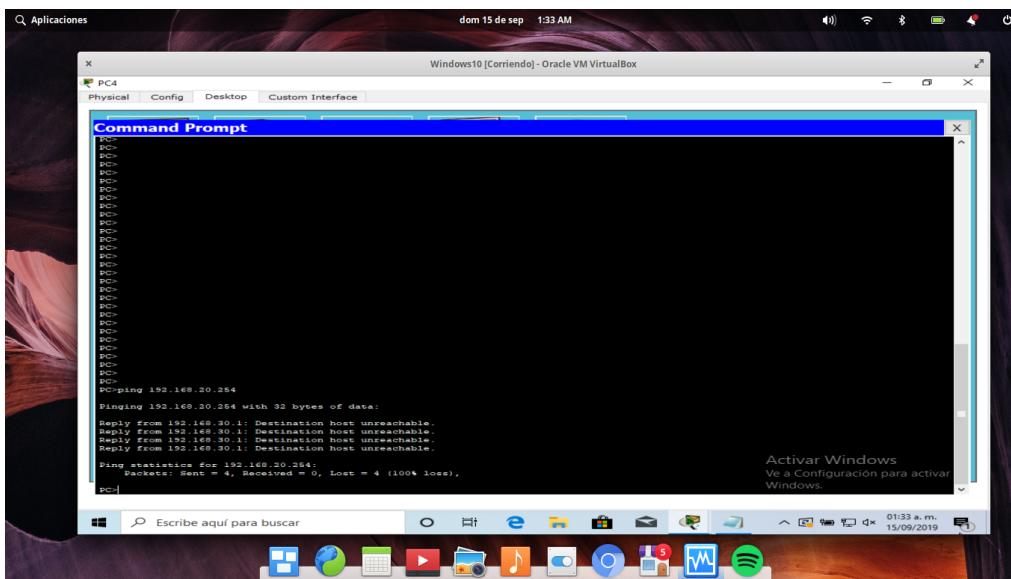


Figura 20: Intentando acceder desde R4 al servidor Web/TFTP

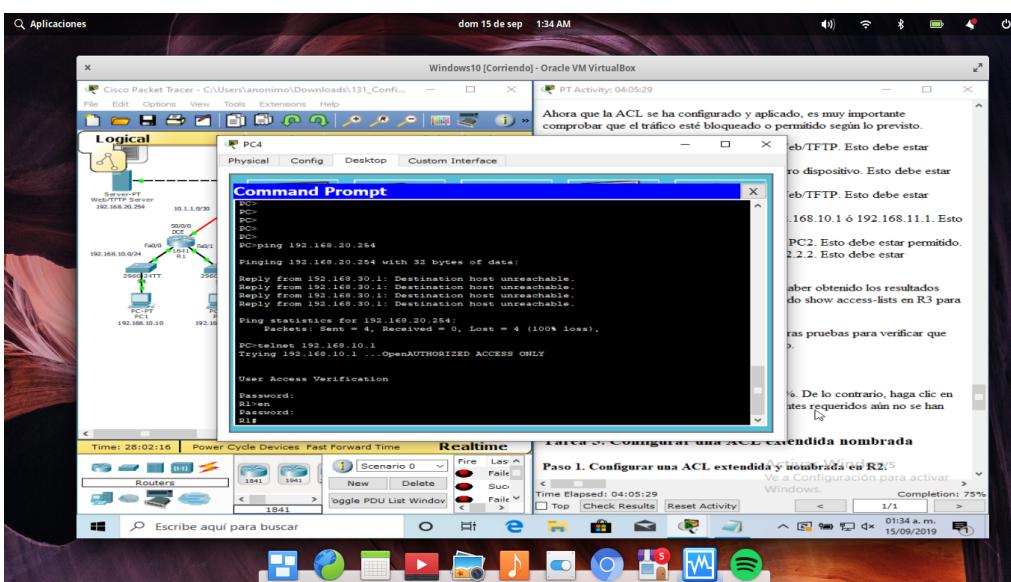


Figura 21: Realizando una conexión telnet desde PC4 a 192.168.10.1

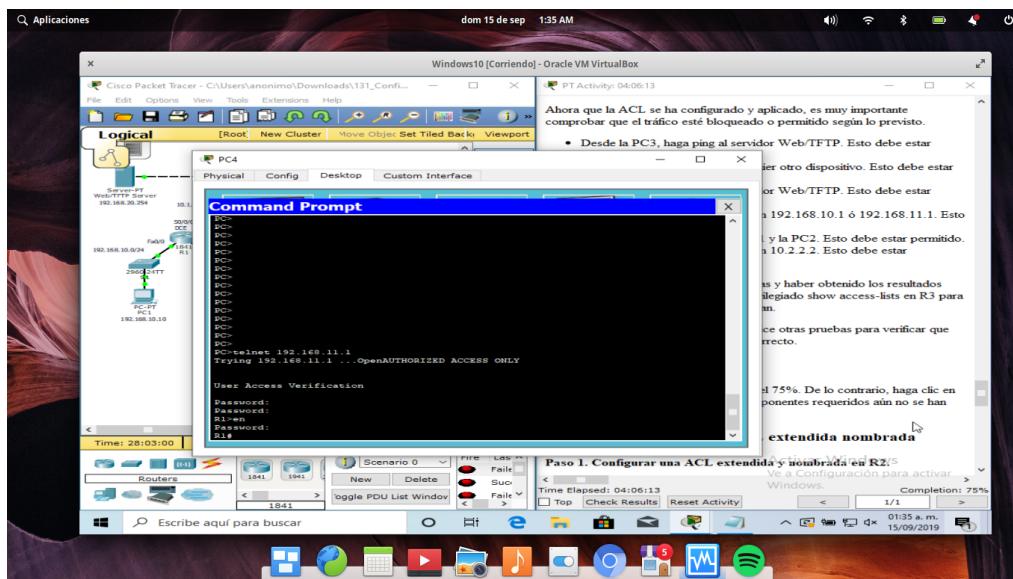


Figura 22: Realizando una conexión telnet desde PC4 a 192.168.11.1

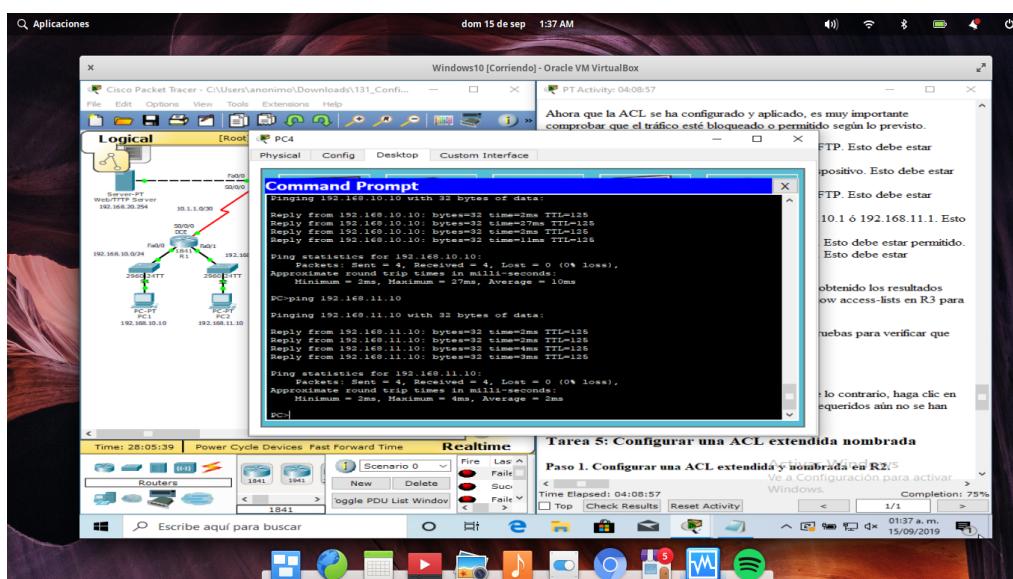


Figura 23: Intentando acceder desde PC4 a PC1 Y PC2

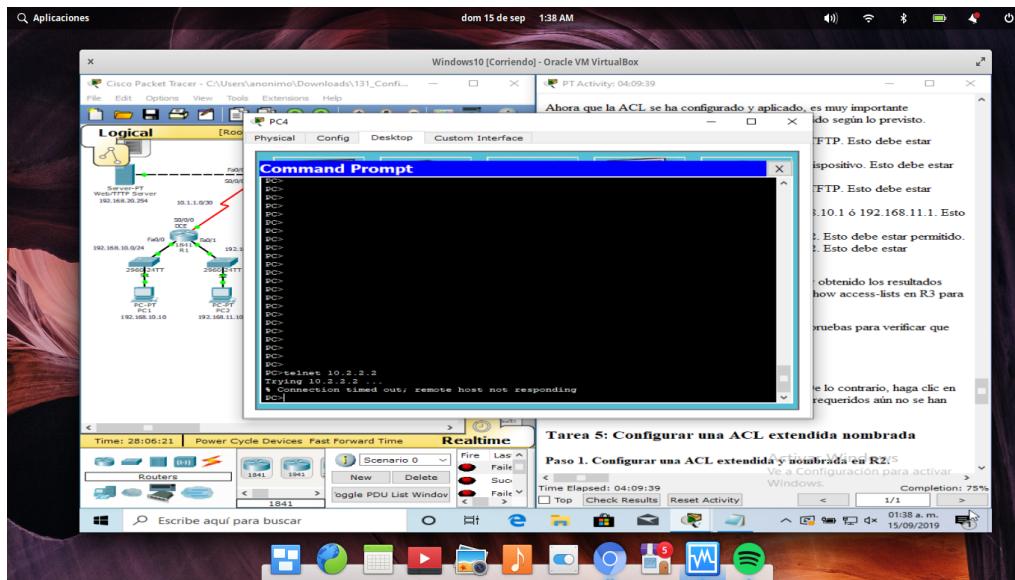


Figura 24: Realizando conexión telnet de PC4 a R2 en 10.2.2.2

#### 4.4. Configurar una ACL extendida nombrada en R2

La política en R2 se diseñará para filtrar el tráfico de Internet. Debido a que R2 tiene la conexión al ISP.

Se configurará una ACL nombrada con la denominación FIREWALL en R2 mediante el comando ip access-list extend FIREWALL

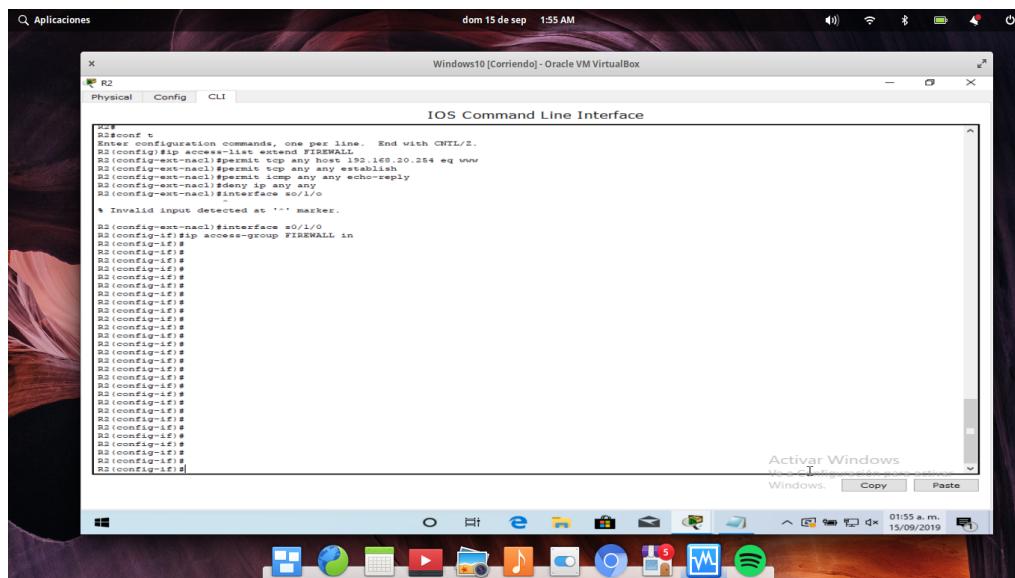


Figura 25: Configurando una ACL extendida nombrada en R2

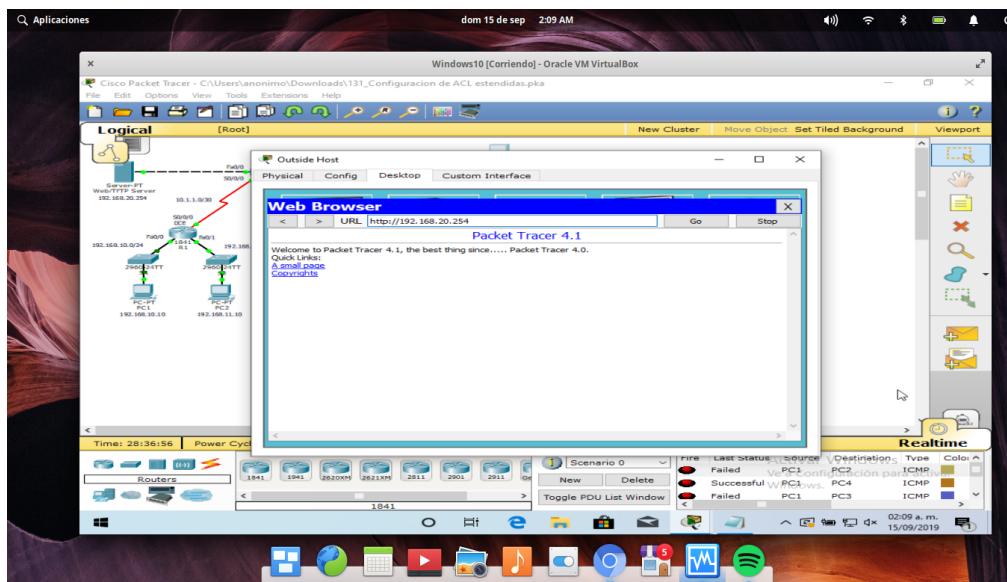


Figura 26: Intentando acceder desde el host externo a una página Web en el servidor Web/TFTP interno

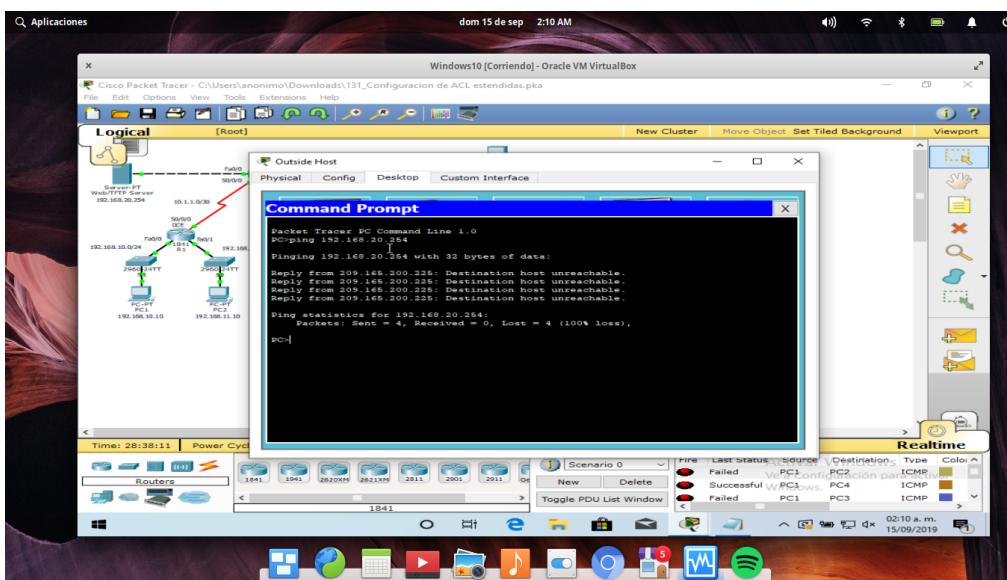


Figura 27: Intentando acceder desde el host externo al servidor Web/TFTP interno

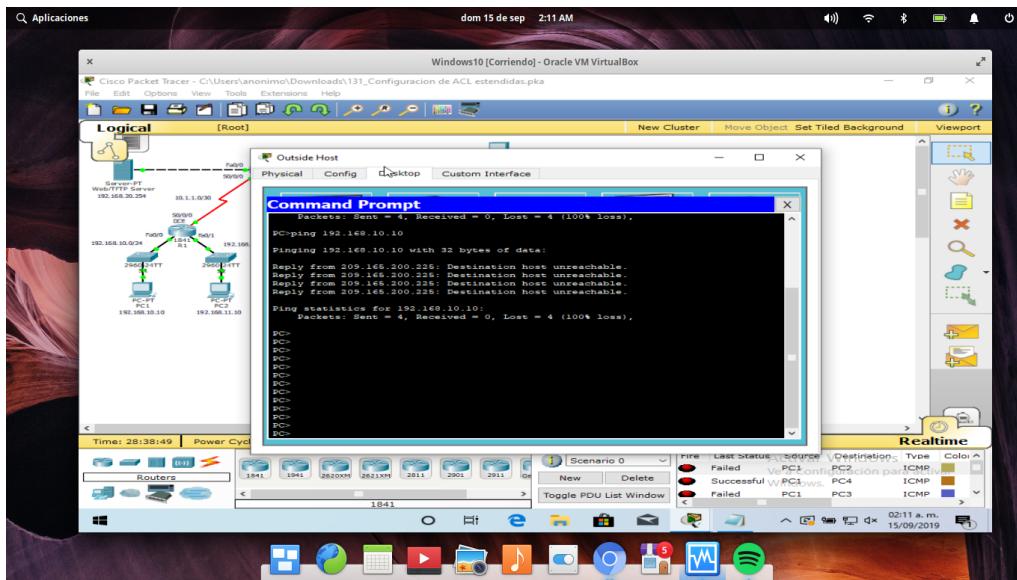


Figura 28: Realizando un ping desde el host externo a PC1

```

C:\>ping 209.165.201.30

Pinging 209.165.201.30 with 32 bytes of data:
Request timed out.
Reply from 209.165.201.30: bytes=32 time=1ms TTL=125
Reply from 209.165.201.30: bytes=32 time=2ms TTL=125
Reply from 209.165.201.30: bytes=32 time=3ms TTL=125
Reply from 209.165.201.30: bytes=32 time=2ms TTL=125

Ping statistics for 209.165.201.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>

```

Figura 29: Realizando un ping desde PC1 al servidor Web externo en 209.165.201.30

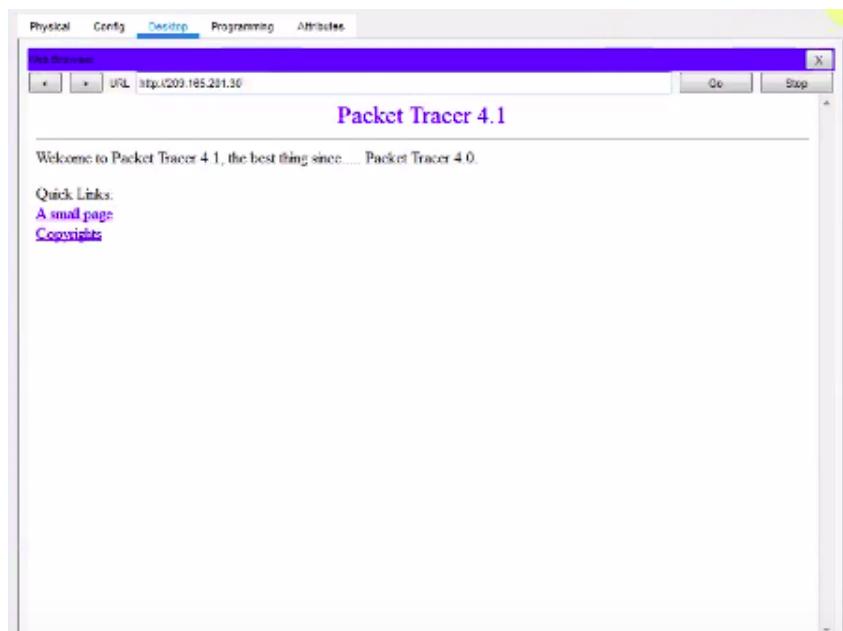


Figura 30: Abriendo una página Web desde PC1 al servidor Web externo

#### 4.4.1. Verificando resultados

Assessment Items		Status	Points	Component(s)	Feedback
Network					
R1					
ACL					
110	Correct	0		ACL	
111	Correct	0		ACL	
Ports					
FastEthernet0/0		0		Other	
Access-group In Correct		0		ACL	
FastEthernet0/1		0		Other	
Access-group In Correct		0		ACL	
R2					
ACL		0		ACL	
Ports		0		Other	
Serial0/1/0		0		Other	
Access-group In Correct		0		ACL	
R3					
ACL		0		ACL	
130	Correct	0		ACL	
Ports		0		Other	
FastEthernet0/0		0		Other	
Access-group In Correct		0		ACL	

Figura 31: Resultados finales

## 5. Comandos

```
access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
access-list 110 deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
access-list 110 permit ip any any

access-list 111 permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
access-list 111 permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 111 permit ip any any

interface f0/0
ip access-group 110 in
interface f0/1
ip access-group 111 in

access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 130 permit ip 192.168.30.0 0.0.0.127 any
access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0 0.0.0.255
access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0 0.0.0.255
access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
access-list 130 deny ip any any

interface f0/0
ip access-group 130 in

ip access-list extend FIREWALL
permit tcp any host 192.168.20.254 eq www
permit tcp any any established
permit icmp any any echo-reply
deny ip any any
interface s0/1/0
ip access-group FIREWALL in
```

Figura 32: Comandos utilizados en la práctica

## 6. Conclusiones

A diferencia de las ACL estándar, las ACL extendidas permiten obtener una mayor granulidad, siendo posible el filtrar el tráfico de la red ya sea por protocolo, puerto, host, etc.

En conclusión las ACL son de gran ayuda cuando no se cuenta con un gran presupuesto para nuestra red y con éste mecanismo es posible controlar nuestro tráfico de red.

## 7. 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].