



Instituto Politécnico Nacional

Escuela Superior de Cómputo



Práctica ACL Ext.

Administración de Servicios en Red

Grupo: 4CV13

Alumnos:

Cazares Martínez Maximiliano

Lemus Milian Armando.

Morales Pascual Daniela Angélica.

Ramos Nieves Adrian

Profesora.

Leticia Henestrosa Carrasco

Introducción

Las ACL extendidas se utilizan con más frecuencia que las ACL estándar, porque proporcionan un mayor grado de control. Pueden filtrar por dirección de origen, dirección de destino, protocolo (es decir, IP, TCP, UDP, ICMP) y número de puerto. Esto proporciona una gama de criterios más amplia sobre la cual basar la ACL. Por ejemplo, una ACL extendida puede permitir el tráfico de correo electrónico de una red a un destino específico y, simultáneamente, denegar la transferencia de archivos y la navegación web. Las ACL ampliadas se introdujeron en la Versión 8.3 del software de Cisco IOS. Las ACL extendidas controlan el tráfico por la comparación de las direcciones de origen y de destino de los paquetes IP a las direcciones configuradas en la ACL. Las ACL extendidas se crean en el modo de configuración global.

Los comandos para las ACL se abordan en los siguientes temas.

Al igual que las ACL estándar, las ACL extendidas se pueden crear como:

- ACL Extendida Numerada – Creado con el comando de configuración global `access-list access-list-number`
- ACL Extendida Nombrada – Creado con el comando `ip access-list extended access-list-name`.

En el ejemplo que se muestra en la figura 1, se deniega el tráfico FTP de la subred 192.168.11.0 que va a la subred 192.168.10.0, pero se permite el resto del tráfico. Observe el uso de las máscaras wildcard y de la instrucción `deny any` explícita. Recuerde que FTP utiliza los puertos TCP 20 y 21, por lo tanto, la ACL requiere ambas palabras claves de nombre de puerto `ftp` y `ftp-data` o `eq 20` y `eq 21` para denegar el tráfico FTP. Los pasos de procedimiento para configurar las ACL extendidos son los mismos que para las ACL estándar. Primero se configura la ACL extendida y luego se activa en una interfaz. Sin embargo, la sintaxis y los parámetros del comando son más complejos para soportar las características adicionales que proporcionan las ACLs extendidas. Utiliza el comando de configuración global `no access-list` para eliminar un ACL extendido. Aunque hay muchas palabras clave y parámetros para las ACLs extendidas, no es necesario usarlos todos cuando se configura una ACL extendida.

Si se utilizan números de puerto en vez de nombres de puerto, los comandos se deben escribir de la siguiente forma:

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
```

Para evitar que la instrucción deny any implícita al final de la ACL bloquee todo el tráfico, se agrega la instrucción permit ip any any. Si no hay por lo menos una instrucción permit en una ACL, todo el tráfico en la interfaz donde se aplicó esa ACL se descarta. La ACL se debe aplicar en sentido de entrada en la interfaz G0/1 para filtrar el tráfico de la LAN 192.168.11.0/24 cuando ingresa a la interfaz del router.

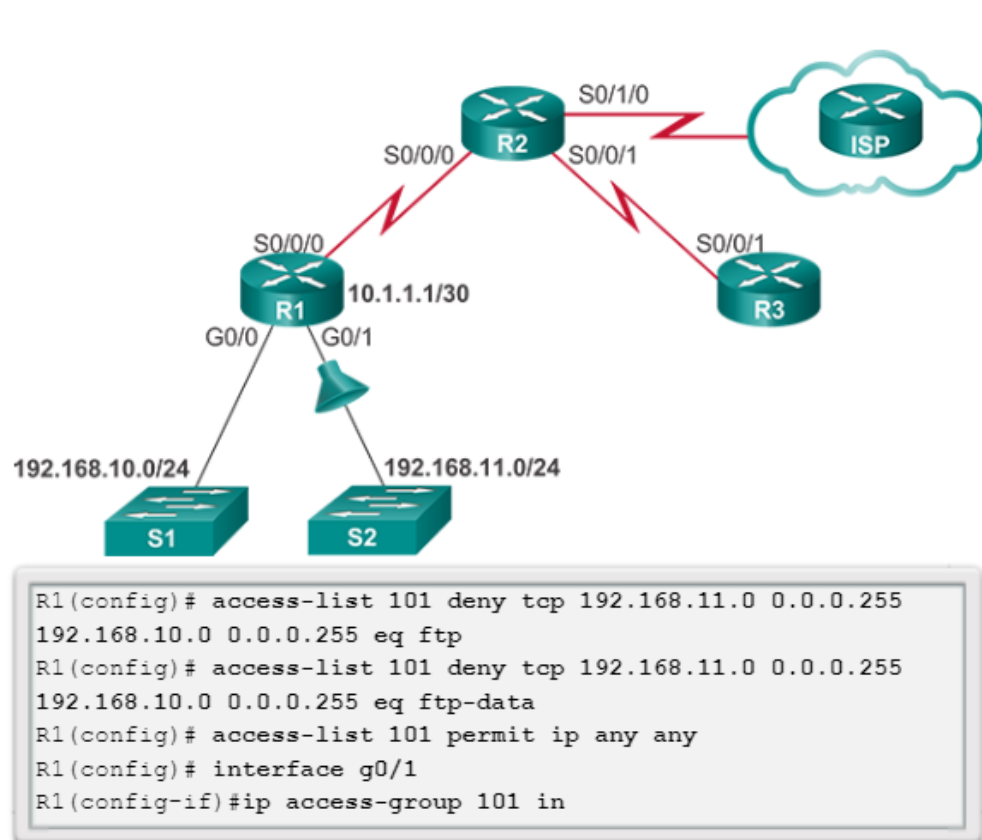


Figura 1 Ejemplo para denegar FTP1

En el ejemplo que se muestra en la figura 2, se deniega el tráfico de Telnet de cualquier origen a la LAN 192.168.11.0/24, pero se permite el resto del tráfico IP. Debido a que el tráfico destinado a la LAN 192.168.11.0/24 sale de la interfaz G0/1, la ACL se aplica a G0/1 con la palabra clave out. Observe el uso de las palabras clave any en la instrucción permit. Esta instrucción permit se agrega para asegurar que no se bloquee ningún otro tipo de tráfico.

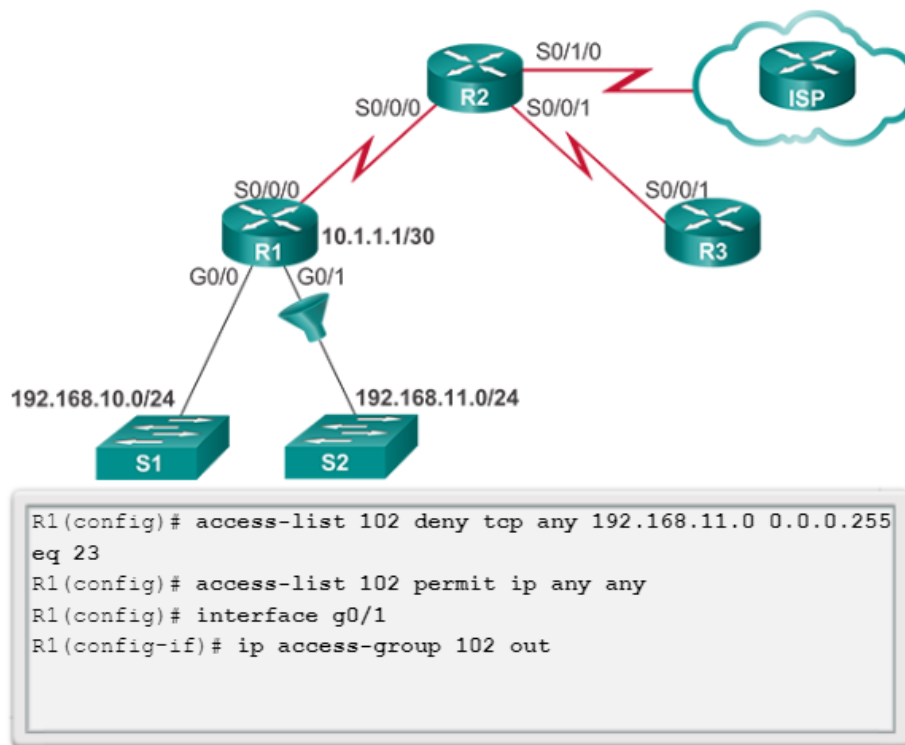



Figura 2 Ejemplo para denegar FTP2

Desarrollo

En la siguiente imagen podemos observar la configuración general del R1 después de haber aplicado las ACL indicadas en el ejercicio guiado.



```
.
interface FastEthernet0/0
  description R1 LAN
  ip address 192.168.10.1 255.255.255.0
  ip access-group 101 in
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 192.168.11.1 255.255.255.0
  ip access-group 102 in
  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
  clock rate 2000000
  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
!
ip flow-export version 9
!
!
access-list 101 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
access-list 101 deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
access-list 101 permit ip any any
access-list 102 permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
access-list 102 permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
access-list 102 deny ip 190.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 102 permit ip any any
```

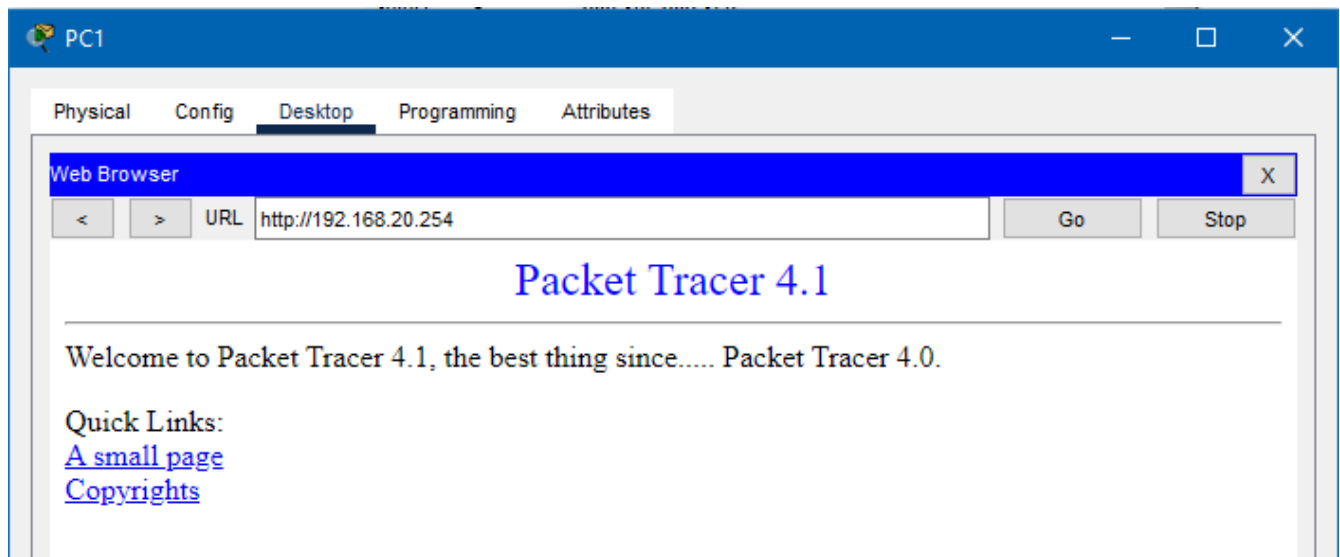
A continuación, se muestran las ACL de R1 mediante el comando “show access-lists”.

```
R1#show acc
R1#show access-lists
Extended IP access list 101
 10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
 20 deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
 30 permit ip any any
Extended IP access list 102
 10 permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
 20 permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
 30 deny ip 190.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
 40 permit ip any any
```

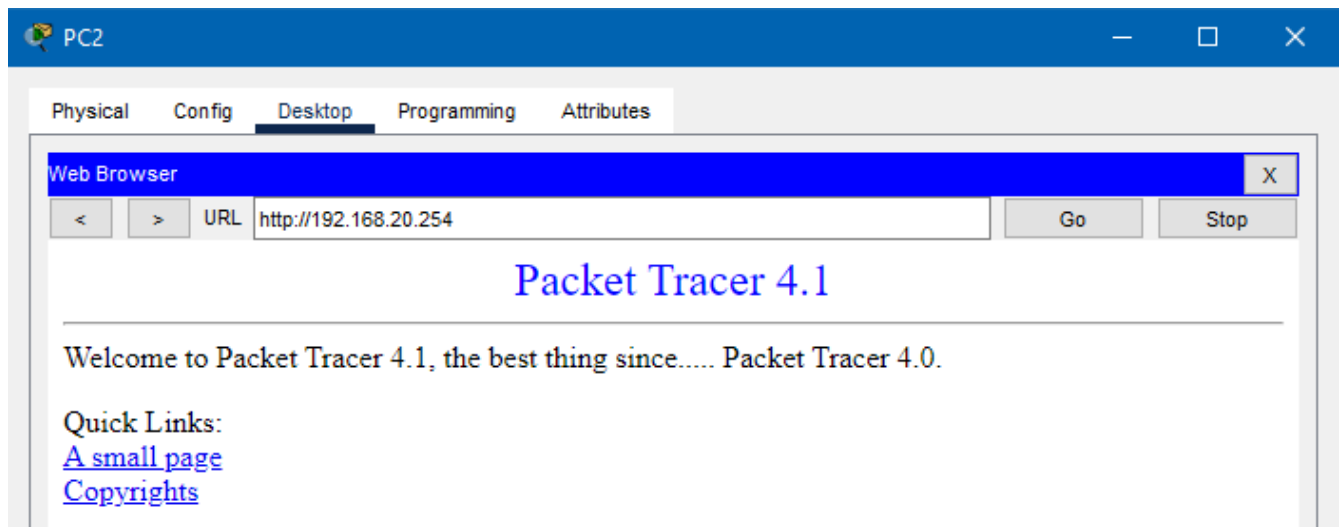
Desde PC1 intentamos hacer Telnet a cualquier host, en este caso al 192.168.11.10 y la conexión es negada.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.11.10
Trying 192.168.11.10 ...
% Connection timed out; remote host not responding
```

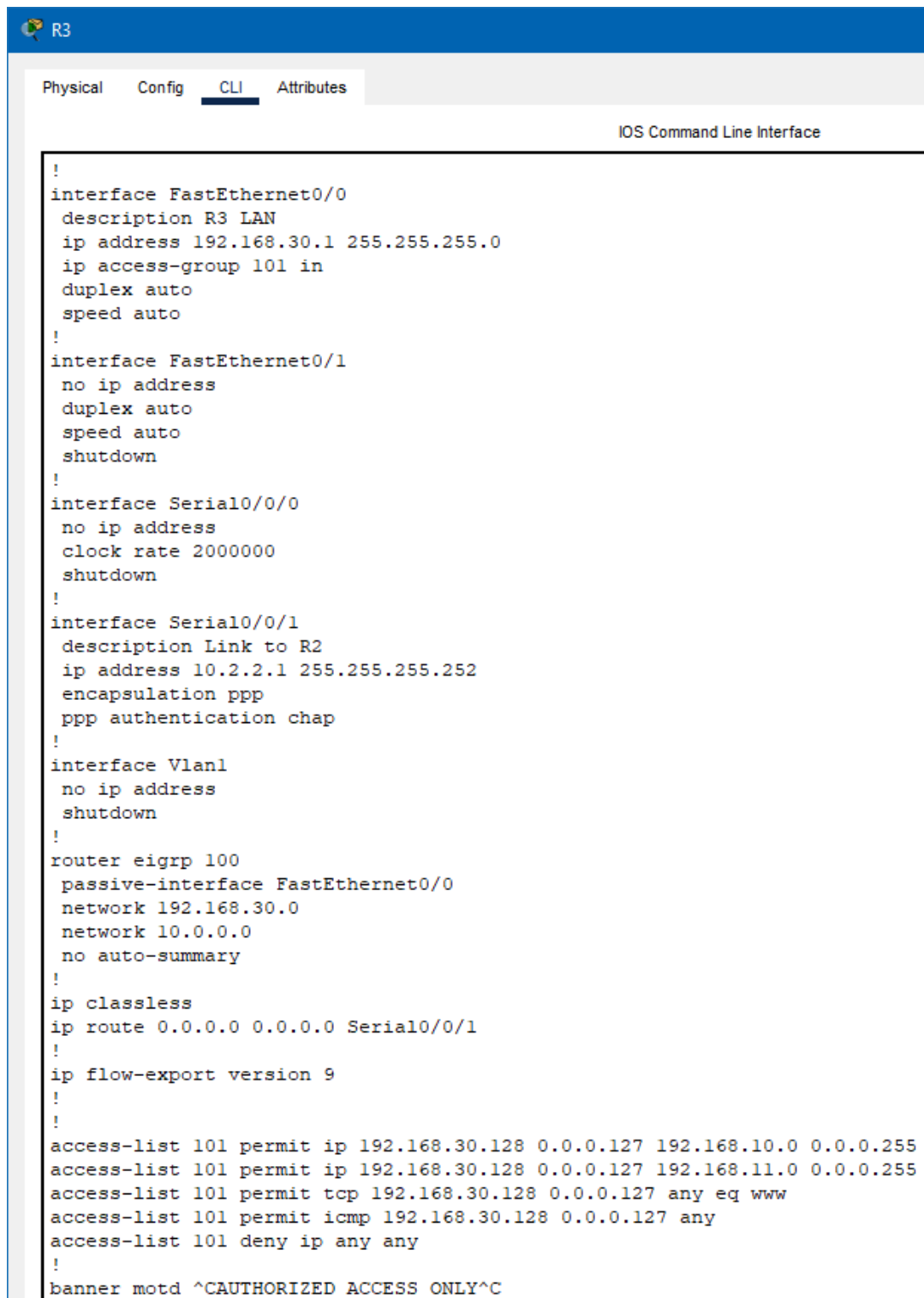
Ahora, intentamos hacer una conexión HTTP al servidor Web/TFTP desde PC1.



Y finalmente, hacemos lo mismo pero ahora desde PC2.



En R3 tenemos la siguiente configuración general después de aplicar la ACL.



```
!
interface FastEthernet0/0
  description R3 LAN
  ip address 192.168.30.1 255.255.255.0
  ip access-group 101 in
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface Serial0/0/0
  no ip address
  clock rate 2000000
  shutdown
!
interface Serial0/0/1
  description Link to R2
  ip address 10.2.2.1 255.255.255.252
  encapsulation ppp
  ppp authentication chap
!
interface Vlan1
  no ip address
  shutdown
!
router eigrp 100
  passive-interface FastEthernet0/0
  network 192.168.30.0
  network 10.0.0.0
  no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
ip flow-export version 9
!
!
access-list 101 permit ip 192.168.30.128 0.0.0.127 192.168.10.0 0.0.0.255
access-list 101 permit ip 192.168.30.128 0.0.0.127 192.168.11.0 0.0.0.255
access-list 101 permit tcp 192.168.30.128 0.0.0.127 any eq www
access-list 101 permit icmp 192.168.30.128 0.0.0.127 any
access-list 101 deny ip any any
!
banner motd ^CAUTHORIZED ACCESS ONLY^C
```


y la siguiente lista de acceso.

```
R3#show access-lists
Extended IP access list 101
 10 permit ip 192.168.30.128 0.0.0.127 192.168.10.0 0.0.0.255
 20 permit ip 192.168.30.128 0.0.0.127 192.168.11.0 0.0.0.255
 30 permit tcp 192.168.30.128 0.0.0.127 any eq www
 40 permit icmp 192.168.30.128 0.0.0.127 any
 50 deny ip any any
```

Ahora, la primera prueba es un ping al servidor Web/TFTP desde PC3, la cual es negada.

```
Cisco Packet Tracer PC Command Line 1.0
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),
```

En la siguiente imagen podemos ver una petición de telnet a la ip 192.168.10.1 la cual es permitida.

```
C:\>telnet 192.168.10.1
Trying 192.168.10.1 ...OpenAUTHORIZED ACCESS ONLY

User Access Verification

Password: |
```

Por último, tenemos ping tanto a PC1 y PC2 desde PC4.

```
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=20ms TTL=125
Reply from 192.168.10.10: bytes=32 time=11ms TTL=125
Reply from 192.168.10.10: bytes=32 time=3ms TTL=125
Reply from 192.168.10.10: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 20ms, Average = 9ms


C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time=2ms TTL=125
Reply from 192.168.11.10: bytes=32 time=15ms TTL=125
Reply from 192.168.11.10: bytes=32 time=14ms TTL=125
Reply from 192.168.11.10: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 15ms, Average = 8ms
```

Finalmente, tenemos la configuración general de R2 y su lista de acceso.



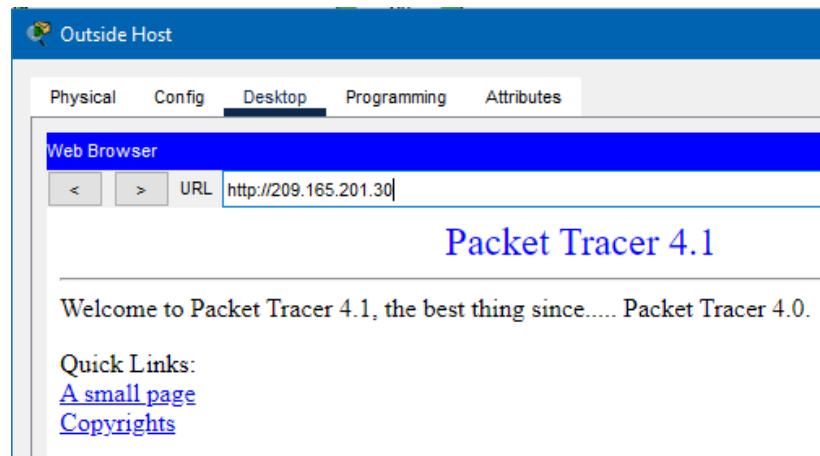
```

:
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description Link to R1
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password 0 cisco123
!
interface Serial0/0/1
 description Link to R3
 ip address 10.2.2.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 64000
!
interface Serial0/1/0
 description Link to ISP
 ip address 209.165.200.225 255.255.255.224
 ip access-group FIREWALL in
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 passive-interface FastEthernet0/0
 passive-interface Serial0/1/0
 network 192.168.20.0
 network 10.0.0.0
 no auto-summary
:

```

```
Extended IP access list FIREWALL
 10 permit tcp any host 192.168.20.254 eq www
 20 permit tcp any any established
 30 permit icmp any any echo-reply
 40 deny ip any any
```

La primera prueba consiste en un ping al servidor Web/TFTP desde Outside Host.



La siguiente prueba es un ping a PC1, el cual será negado.

```
Pinging 192.168.10.10 with 32 bytes of data:

Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.

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

Finalmente, la última prueba es un ping a la ip 209.165.201.30.

```
C:\>ping 209.165.201.30

Pinging 209.165.201.30 with 32 bytes of data:

Reply from 209.165.201.30: bytes=32 time=2ms TTL=125
Reply from 209.165.201.30: bytes=32 time=2ms TTL=125
Reply from 209.165.201.30: bytes=32 time=2ms 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 = 2ms, Average = 2ms
```

Conclusiones

Cazares Martínez Maximiliano

Las ACL extendidas son de mucha ayuda cuando se necesita controlar el tráfico en una red y poder negar o permitir ciertos protocolos como Telnet o HTTP desde cierta subred a otra. Esta práctica me ayudó mucho a entender mejor las ACL extendidas, no fue demasiado complicada gracias a que la guía nos dice paso a paso que es lo que hay que hacer y en cual interfaz aplicarla.

Lemus Milian Armando

Morales Pascual Daniela Angélica

En la práctica pudimos aplicar lo aprendido referente a las ACL extendidas, su concepto y beneficios que nos otorgan, así controlando el tráfico de manera que aumente el rendimiento y dando seguridad básica para el acceso a la red. Además que pudimos aplicar los comandos que nos ayudaron a realizar todo el control y configuración de las listas de acceso de los router para manejar el tráfico de cada red y subred que estaban permitiendo o no el intercambio de información.

Ramos Nieves Adrian

Como vimos en clase acerca de las ACL estándar, ahora las ACL extendidas siguen el mismo concepto sobre el control de tráfico en una red. en la cual mediante los protocolos para el paso de paquetes tales como son TCP,HTTP, etc podemos dar acceso a ciertas partes de nuestra topología. Con los conocimientos obtenidos con base en la información proporcionada se configuró con la ayuda de Cisco packet tracer la topología vista durante la práctica para el entendimiento de cómo se permite o deniega los diferentes paquetes en los routers.

Bibliografías

- [1] Configuración de Listas de Acceso IP. (2022, 16 marzo). Cisco.
https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html#extaclds
- [2] Walton, A. (2020, 3 septiembre). ▷ Configuración de ACL Extendidas IPv4 ». CCNA desde Cero.
<https://ccnadesdecero.es/configurar-acl-extendidas/#:%7E:text=Las%20ACL%20extendidas%20se%20utilizan,la%20cual%20basar%20la%20ACL.>
- [3] Documento sin título. (s. f.). ACL. https://www.reuter.com.ar/CCNA/CCNA2/mod9_ccna2/