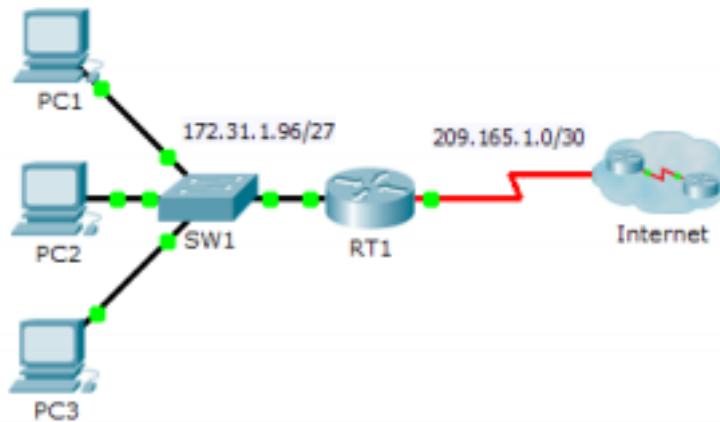




Packet Tracer: configuración de ACL extendidas, situación 3

## Packet Tracer: configuración de ACL extendidas, situación 3

### Topología



### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RT1	G0/0	172.31.1.126	255.255.255.221	N/A
	S0/0/0	209.165.1.2	255.255.255.252	N/A
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server1	NIC	64.101.255.254		
Server2	NIC	64.103.255.254		



## Packet Tracer: configuración de ACL extendidas, situación 3

### Objetivos

Parte 1: configurar una ACL extendida con nombre

Parte 2: aplicar y verificar la ACL extendida

### Información básica/situación

En esta situación, se permite que determinados dispositivos de la LAN tengan acceso a varios servicios en servidores ubicados en Internet.

## Parte 1: Configurar una ACL extendida y nombrada

Utilice una ACL con nombre para implementar la política siguiente:

- 1) Bloquee el acceso HTTP y HTTPS desde la **PC1** hasta el **Servidor 1** y el **Servidor 2**. Los servidores están dentro de la nube, y solo conoce sus direcciones IP.
- 2) Bloquee el acceso FTP desde la **PC2** hasta el **Servidor1** y el **Servidor2**.
- 3) Bloquee el acceso ICMP desde la **PC3** hasta el **Servidor1** y el **Servidor2**.

### Paso 1: denegar a la PC1 el acceso a los servicios HTTP y HTTPS en el Servidor1 y el Servidor2.

Cree una ACL de IP extendida con nombre que le deniegue a la **PC1** el acceso a los servicios HTTP y HTTPS del **Servidor1** y el **Servidor2**. Ya que no es posible observar directamente la subred de servidores en Internet, se necesitan cuatro reglas.

1. ¿Cuál es el comando para iniciar la ACL con nombre?

```
RT1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RT1(config)#ip access-list extended ACL
RT1(config-ext-nacl) #
```

2. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor1** solo para HTTP (puerto 80).
3. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor1** solo para HTTPS (puerto 443).
4. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor2** solo para HTTP.
5. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor2** solo para HTTPS.

```
RT1(config-ext-nacl) #deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
RT1(config-ext-nacl) #deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
RT1(config-ext-nacl) #deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
RT1(config-ext-nacl) #deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
```

### Paso 2: denegar a la PC2 el acceso a los servicios FTP en el Servidor1 y el Servidor2.

1. Registre la instrucción que deniega el acceso de la **PC2** al **Servidor1** solo para FTP (puerto 21 únicamente).
2. Registre la instrucción que deniega el acceso de la **PC2** al **Servidor2** solo para FTP (puerto 21 únicamente).

```
RT1(config-ext-nacl) #deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
RT1(config-ext-nacl) #deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
```



### Packet Tracer: configuración de ACL extendidas, situación 3

#### Paso 3: denegar a la PC3 que haga ping al Servidor1 y al Servidor2.

1. Registre la instrucción que deniega el acceso ICMP de la PC3 al Servidor1.
2. Registre la instrucción que deniega el acceso ICMP de la PC3 al Servidor2.

```
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.101.255.254
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.103.255.254
```

#### Paso 4: permitir todo el tráfico IP restante.

1. De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con alguna regla de la lista. ¿Qué comando permite el resto del tráfico?

```
RT1(config-ext-nacl)#permit ip any any
RT1(config-ext-nacl)#End
```

## Parte 2: aplicar y verificar la ACL extendida

El tráfico que se filtrará proviene de la red 172.31.1.96/27 y tiene como destino las redes remotas. La ubicación adecuada de la ACL también depende de la relación del tráfico con respecto al **RT1**.

#### Paso 1: aplicar la ACL a la interfaz apropiada en el sentido correcto.

- 1) ¿Cuáles son los comandos que necesita para aplicar la ACL a la interfaz apropiada en el sentido correcto?

```
RT1(config)#interface g0/0
RT1(config-if)#ip access-group ACL in
RT1(config-if)#End
```

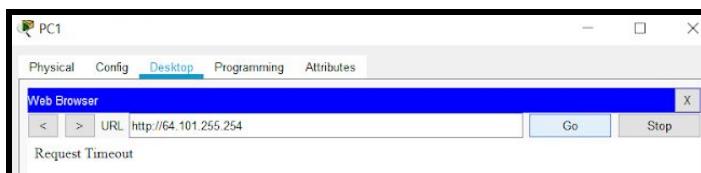
#### Paso 2: implementar una solución.

- 1) Acceda a los sitios web del **Servidor1** y **Servidor2** mediante el navegador web de la **PC1** con los protocolos **HTTP** y **HTTPS**

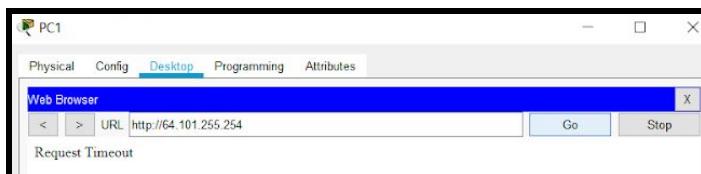
→ PC1

◆ Servidor 1

• HTTP



• HTTPS

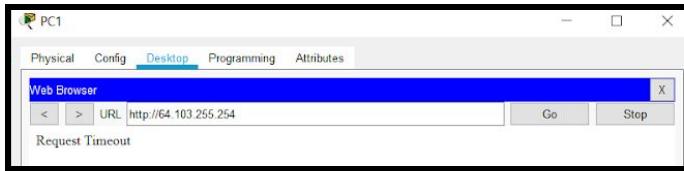




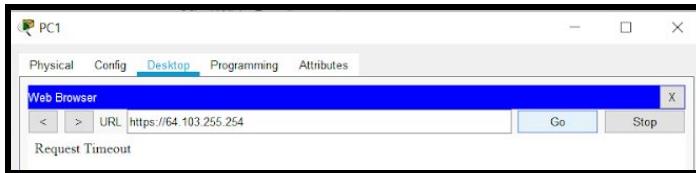
### Packet Tracer: configuración de ACL extendidas, situación 3

#### ◆ Servidor 2

- HTTP



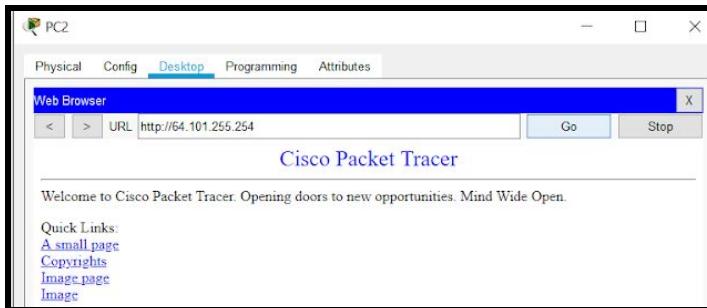
- HTTPS



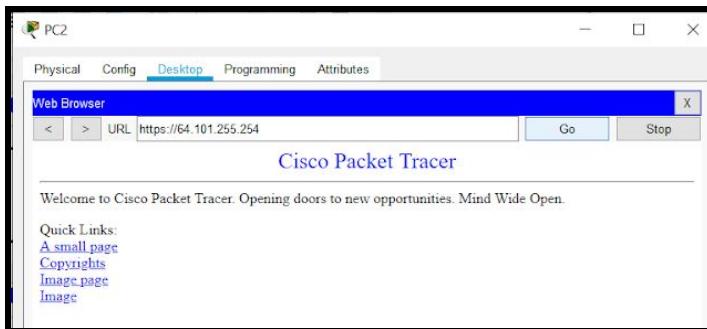
→ PC2

#### ◆ Servidor 1

- HTTP



- HTTPS

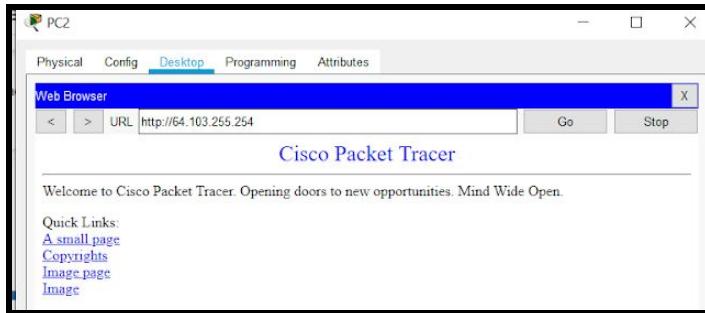




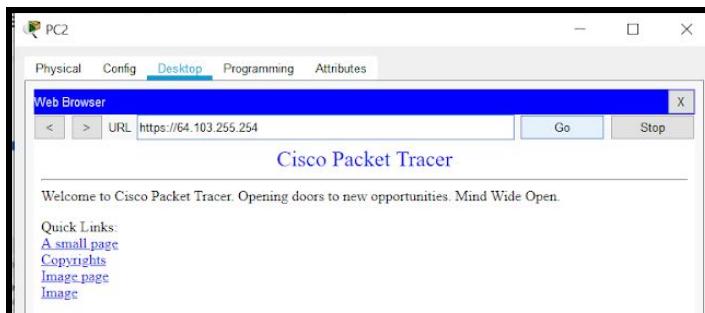
### Packet Tracer: configuración de ACL extendidas, situación 3

#### ◆ Servidor 2

- HTTP



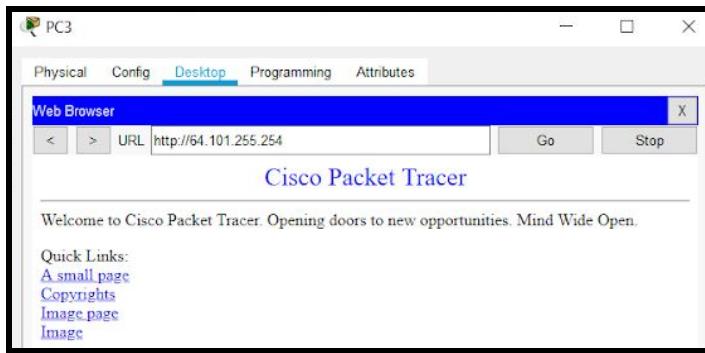
- HTTPS



→ PC3

#### ◆ Servidor 1

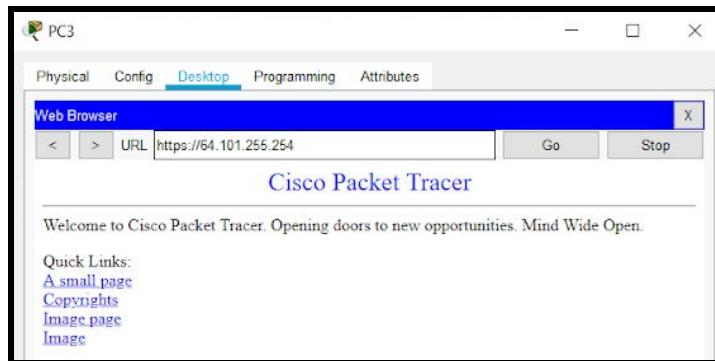
- HTTP





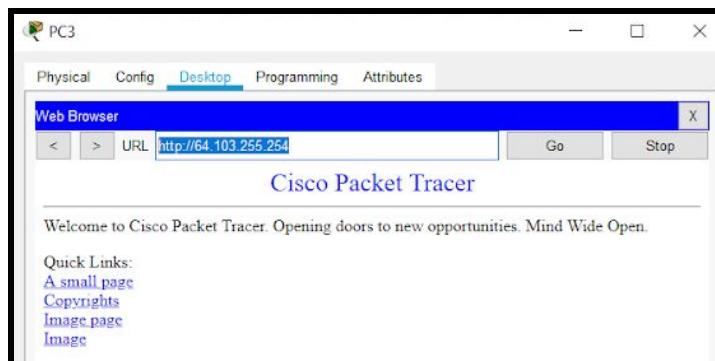
### Packet Tracer: configuración de ACL extendidas, situación 3

- **HTTPS**

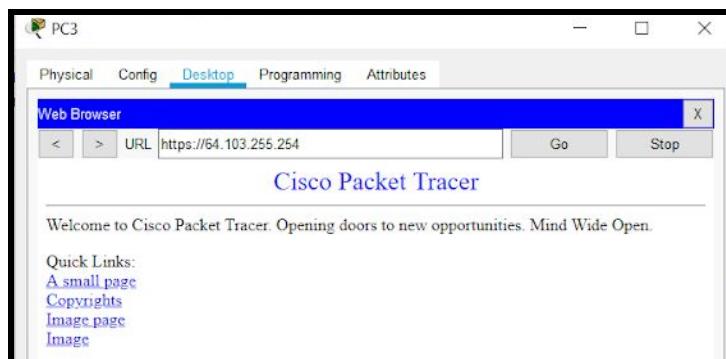


### ◆ Servidor 2

- **HTTP**



- **HTTPS**





### Packet Tracer: configuración de ACL extendidas, situación 3

- 2) Acceda al **Servidor1** y el **Servidor2** mediante FTP con la **PC1**.

→ PC1

#### ◆ Servidor 1

```
C:\>ftp 64.101.255.254
Trying to connect...64.101.255.254
Connected to 64.101.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

#### ◆ Servidor 2

```
C:\>ftp 64.103.255.254
Trying to connect...64.103.255.254
Connected to 64.103.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

→ PC2

#### ◆ Servidor 1

```
C:\>ftp 64.101.255.254
Trying to connect...64.101.255.254

%Error opening ftp://64.101.255.254/ (Timed out)

.

(Disconnecting from ftp server)
```

#### ◆ Servidor 2

```
C:\>ftp 64.103.255.254
Trying to connect...64.103.255.254

%Error opening ftp://64.103.255.254/ (Timed out)

.

(Disconnecting from ftp server)
```



### Packet Tracer: configuración de ACL extendidas, situación 3

→ PC3

#### ◆ Servidor 1

```
Packet Tracer PC Command Line 1.0
C:\>ftp 64.101.255.254
Trying to connect...64.101.255.254
Connected to 64.101.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

#### ◆ Servidor 2

```
C:\>ftp 64.103.255.254
Trying to connect...64.103.255.254
Connected to 64.103.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

- 3) Haga ping al **Servidor1** y al **Servidor2** desde la **PC1**.

→ PC1

```
C:\>ping 64.101.255.254
Pinging 64.101.255.254 with 32 bytes of data:
Reply from 64.101.255.254: bytes=32 time=2ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=4ms TTL=126
Reply from 64.101.255.254: bytes=32 time=11ms TTL=126

Ping statistics for 64.101.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 4ms

C:\>ping 64.103.255.254
Pinging 64.103.255.254 with 32 bytes of data:
Reply from 64.103.255.254: bytes=32 time=2ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=14ms TTL=126
Reply from 64.103.255.254: bytes=32 time=8ms TTL=126

Ping statistics for 64.103.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 6ms
```



### Packet Tracer: configuración de ACL extendidas, situación 3

→ PC2

```
C:\>ping 64.101.255.254

Pinging 64.101.255.254 with 32 bytes of data:

Reply from 64.101.255.254: bytes=32 time=2ms TTL=126
Reply from 64.101.255.254: bytes=32 time=11ms TTL=126
Reply from 64.101.255.254: bytes=32 time=2ms TTL=126
Reply from 64.101.255.254: bytes=32 time=10ms TTL=126

Ping statistics for 64.101.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 6ms

C:\>ping 64.103.255.254

Pinging 64.103.255.254 with 32 bytes of data:

Reply from 64.103.255.254: bytes=32 time=2ms TTL=126
Reply from 64.103.255.254: bytes=32 time=4ms TTL=126
Reply from 64.103.255.254: bytes=32 time=12ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126

Ping statistics for 64.103.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms

C:\>
```

→ PC3

```
----- C:\>ping 64.101.255.254

Pinging 64.101.255.254 with 32 bytes of data:

Reply from 172.31.1.126: Destination host unreachable.

Ping statistics for 64.101.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.103.255.254

Pinging 64.103.255.254 with 32 bytes of data:

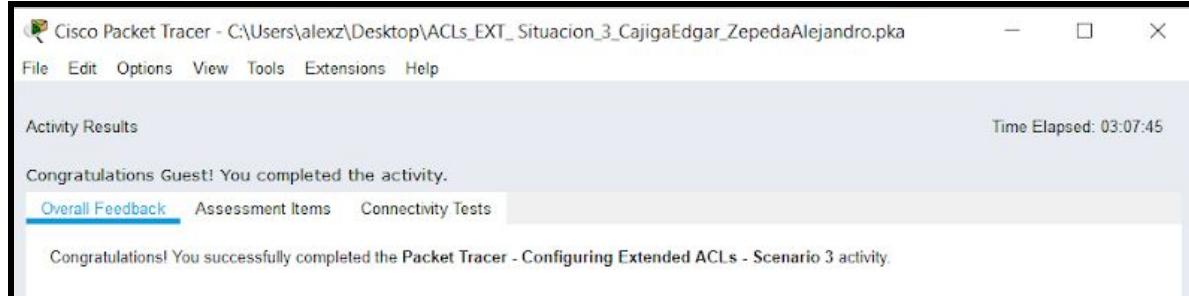
Reply from 172.31.1.126: Destination host unreachable.

Ping statistics for 64.103.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
.
```



## Packet Tracer: configuración de ACL extendidas, situación 3

### Resultados



### Conclusiones

- **Edgar Uriel Cajiga Gutiérrez**

Con esta práctica aplicamos conceptos vistos en clase tales como ACL extendida y las diferentes configuraciones que son posibles asignarles según el problema planteado. También vimos como es importante analizar el lugar donde se coloca al ACL ya que de esta forma podemos facilitar las tareas para los routers. Por último vimos de primera mano como al hacer las configuraciones correspondientes es posible denegar diferentes servicios a un host al intentar acceder a este por medio de las PC's.

- **Alejandro de Jesús Zepeda Flores**

Al dar solución a esta práctica, tuvimos la oportunidad de configurar una ACL extendida, además de esto le dimos un nombre a la ACL y configuramos los diferentes permisos en función de lo solicitado, tales como denegar el acceso de cierta PC a un determinado servidor por medio de un protocolo definido (http y https), ademas de posteriormente comprobar que las denegaciones de servicio fueron aplicadas correctamente intentando acceder desde la PC al servidor denegado.