



# Configuración de ACL IP V6

**Nombre del Alumno:**

**Jireh Hernández Castillo**

**Matricula:**

**1717110620**

**Nombre del Docente:**

**MTI. Oscar Lira Uribe**

**Materia:**

**Aplicación de las Telecomunicaciones**

**Universidad:**

**Universidad Tecnológica de Tulancingo**

**Carrera:**

**ING. En Tecnologías de la Información y Comunicación**

**Grupo:**

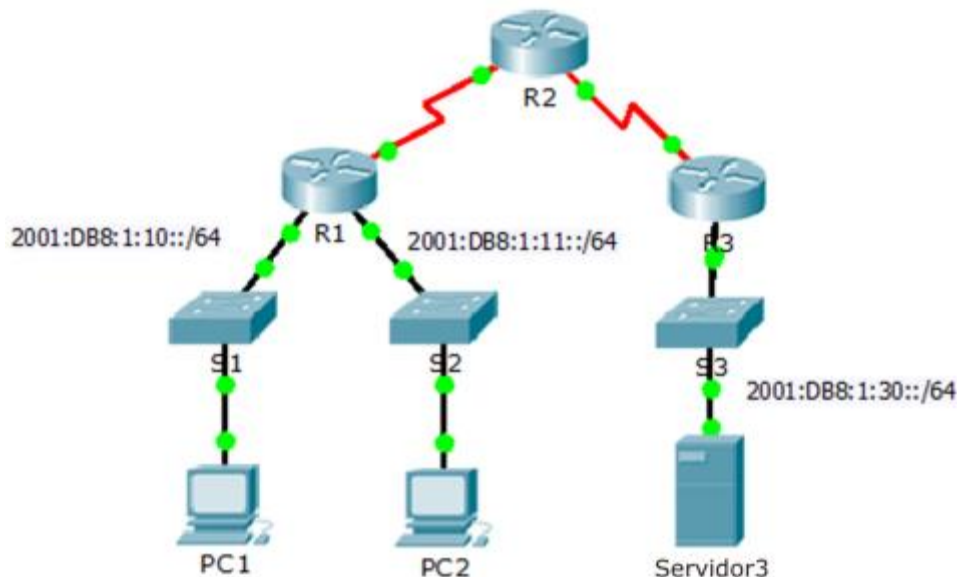
**ITI91**

**Fecha:**

**28 de julio de 2020**

# Packet Tracer: Configuración de ACL IPV6

## Topología



## Tabla de Direcccionamiento

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

## Objetivos

**Parte 1:** configurar, aplicar y verificar una ACL de IPv6

**Parte 2:** configurar, aplicar y verificar una segunda ACL de IPv6

### Parte 1: configurar, aplicar y verificar una ACL de IPv6

Según los registros, una computadora en la red 2001:DB8:1:11::0/64 actualiza repetidamente su página web, lo que ocasiona un ataque por negación de servicio (DoS) contra el Servidor3. Hasta que se pueda identificar y limpiar el cliente, debe bloquear el acceso HTTP y HTTPS a esa red mediante una lista de acceso.

#### Paso 1: configurar una ACL que bloquee el acceso HTTP y HTTPS.

Configure una ACL con el nombre BLOCK\_HTTP en el R1 con las siguientes instrucciones.

- Bloquear el tráfico HTTP y HTTPS para que no llegue al Servidor3.
  - R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
  - R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
- Permitir el paso del resto del tráfico IPv6.

```

R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ip any any

```

## Paso 2: aplicar la ACL a la interfaz correcta.

Aplique la ACL a la interfaz más cercana al origen del tráfico que se desea bloquear.

- R1(config-if) # ipv6 traffic-filter BLOCK\_HTTP in

```

R1(config)#int g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1(config-if)#

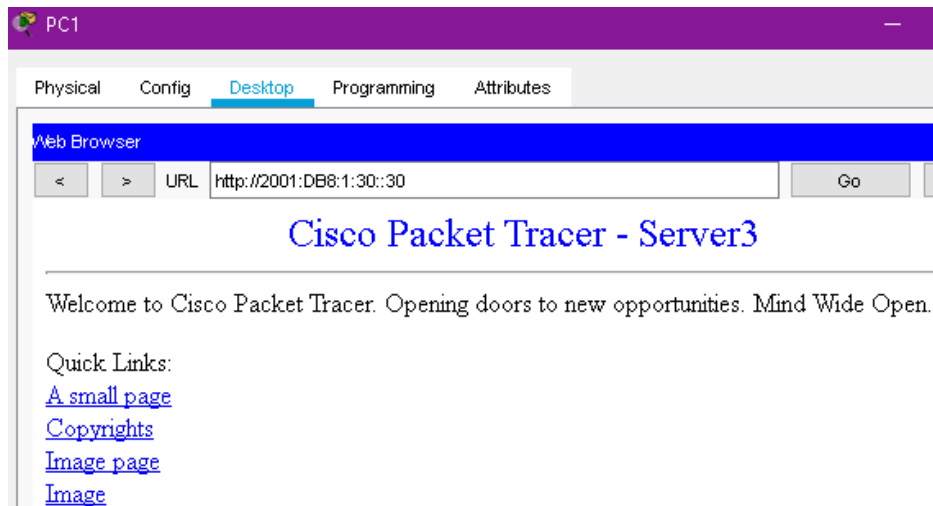
```

## Paso 3: verificar la implementación de la ACL.

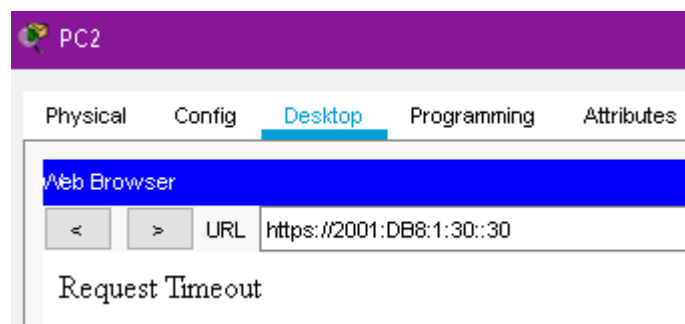
Realice las siguientes pruebas para verificar que la ACL funcione de manera correcta:

- Abra el Web Browser PC1 en <http://2001:DB8:1:30::30> o <https://2001:DB8:1:30::30>. Debería aparecer el sitio web.
- Abra el Web Browser PC2 en <http://2001:DB8:1:30::30> o <https://2001:DB8:1:30::30>. El sitio web debería estar bloqueado.
- Haga ping de la PC2 a 2001:DB8:1:30::30. El ping debería realizarse correctamente.

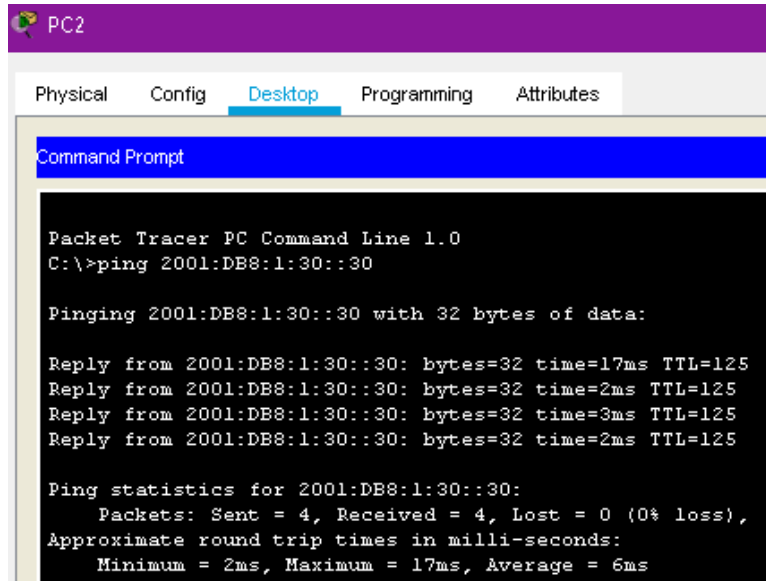
### PC1



### PC2



### Ping PC2



The screenshot shows a Packet Tracer PC named PC2. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The text in the window is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:30::30: bytes=32 time=17ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 17ms, Average = 6ms
```

## Parte 2: configurar, aplicar y verificar una segunda ACL de IPv6

Ahora, en los registros se indica que su servidor recibe pings de diversas direcciones IPv6 en un ataque por negación de servicio distribuido (DDoS).

### Paso 1: crear una lista de acceso para bloquear ICMP.

Configure una ACL con el nombre BLOCK\_ICMP en el R3 con las siguientes instrucciones:

- Bloquear todo el tráfico ICMP desde cualquier host hasta cualquier destino.
- Permitir el paso del resto del tráfico IPv6.

```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
```

### Paso 2: aplicar la ACL a la interfaz correcta.

En este caso, el tráfico ICMP puede provenir de cualquier origen. Para asegurar que el tráfico ICMP esté bloqueado, independientemente de su origen o de los cambios que se produzcan en la topología de la red, aplique la ACL lo más cerca posible del destino.

```
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address FE80::3 link-local
ipv6 address 2001:DB8:1:30::1/64
ipv6 eigrp 1
R3(config-if)#int g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
```

### Paso 3: verificar que la lista de acceso adecuada funcione.

- Haga ping de la PC2 a 2001:DB8:1:30::30. El ping debe fallar.
- Haga ping de la PC1 a 2001:DB8:1:30::30. El ping debe fallar.

Abra el Web Browser PC1 en <http://2001:DB8:1:30::30> o <https://2001:DB8:1:30::30>. Debería aparecer el sitio web.

## PC2

```
C:\>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

## PC1

```
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

