
Instituto Politécnico Nacional

Escuela Superior de Computo

Unidad de aprendizaje: Administración de servicios de red [4CV5]

Profesor: Henestrosa Carrasco Leticia

---

# Actividad #8: Configuración y resolución de problemas con ACL's

---

*Alumnos: García González Aarón Antonio & Villalba Gil Ángel*

Noviembre, 2020

# Índice

## Objetivos

- Configurar una ACL extendida con nombre
- Configurar una ACL estándar numerada
- Aplicar y verificar la ACL extendida
- Aplicar y verificar ACL estándar

## Introducción

La seguridad de red es un tema muy amplio, y gran parte de este tema se encuentra más allá del ámbito de este curso. Sin embargo, una de las habilidades más importantes que necesita un administrador de red es el dominio de las listas de control de acceso (ACL). [1]

En un router Cisco, puede configurar un firewall simple que proporcione capacidades básicas de filtrado de tráfico mediante ACL. Los administradores utilizan las ACL para detener el tráfico o para permitir solamente tráfico específico en sus redes. Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar) que se aplican a los protocolos de capa superior o a las direcciones. Las ACL son una herramienta potente para controlar el tráfico hacia y desde la red. Se pueden configurar ACL para todos los protocolos de red enrutada.

Los routers no tienes ACL configuradas de manera predeterminada, por lo que no filtran el tráfico de manera predeterminada. El tráfico que ingresa al router se enruta solamente en función de la información de la tabla de routing. Sin embargo, cuando se aplica una ACL a una interfaz, el router realiza la tarea adicional de evaluar todos los paquetes de red a medida que pasan a través de la interfaz para determinar si el paquete se puede reenviar.

Las ACL definen el conjunto de reglas que proporcionan un control adicional para los paquetes que ingresan por las interfaces de entrada, para los que retransmiten a través del router y para los que salen por las interfaces de salida del router. Las ACL no operan sobre paquetes que se originan en el router mismo.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente, como se muestra en la ilustración.

- ACL de entrada: los paquetes entrantes se procesan antes de enrutarse a la interfaz de salida. Las ACL de entrada son eficaces, porque ahorran la sobrecarga de enrutar búsquedas si el paquete se descarta. Si las pruebas permiten el paquete, este se procesa para el routing. Las ACL de entrada son ideales para filtrar los paquetes cuando la red conectada a una interfaz de entrada es el único origen de los paquetes que se deben examinar.
- ACL de salida: los paquetes entrantes se enrutan a la interfaz de salida y después se procesan mediante la ACL de salida. Las ACL de salida son ideales cuando se aplica el mismo filtro a los paquetes que provienen de varias interfaces de entrada antes de salir por la misma interfaz de salida.

La última sentencia de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Debido a esta denegación implícita, una ACL que no tiene, por lo menos, una instrucción permit bloqueará todo el tráfico.

Los dos tipos de ACL de IPv4 de Cisco son estándar y extendida.

ACL estándar

Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan. En el ejemplo de la figura 1, se permite todo el tráfico de la red 192.168.30.0/24. Debido al "deny any" (denegar todo) implícito al final, todo el resto del tráfico se bloquea con esta ACL. Las ACL estándar se crean en el modo de configuración global.

ACL extendidas

Las ACL extendidas filtran paquetes IPv4 según varios atributos:

- Tipo de protocolo
- Dirección IPv4 de origen
- Dirección IPv4 de destino
- Puertos TCP o UDP de origen
- Puertos TCP o UDP de destino
- Información optativa de tipo de protocolo para un control más preciso

Las ACL estándar y extendidas se pueden crear con un número o un nombre para identificar la ACL y su lista de instrucciones.

El uso de ACL numeradas es un método eficaz para determinar el tipo de ACL en redes más pequeñas con tráfico definido de forma más homogénea. Sin embargo, un número no proporciona información sobre el propósito de la ACL. Por este motivo, a partir de la versión 11.2 del IOS de Cisco, se puede utilizar un nombre para identificar una ACL de Cisco.

Las ACL no deben configurarse en ambos sentidos. La cantidad de ACL y el sentido aplicado a la interfaz dependen de los requisitos que se implementen.

Las siguientes son algunas pautas para el uso de ACL:

- Utilice las ACL en los routers de firewall ubicados entre su red interna y una red externa, como Internet.
- Utilice las ACL en un router ubicado entre dos partes de la red para controlar el tráfico que entra a una parte específica de su red interna o que sale de esta.
- Configure las ACL en los routers de frontera, es decir, los routers ubicados en los límites de las redes. Esto proporciona una separación muy básica de la red externa o entre un área menos controlada y un área más importante de su propia red.
- Configure las ACL para cada protocolo de red configurado en las interfaces del router de frontera.

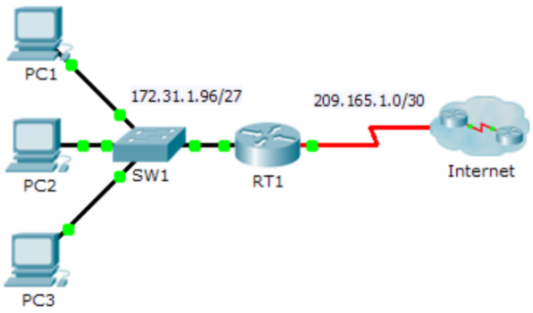
Las tres P, Para recordar una regla general de aplicación de ACL en un router, puede pensar en "las tres P". Se puede configurar una ACL por protocolo, por sentido y por interfaz:

- Una ACL por protocolo: para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.
- Una ACL por sentido: las ACL controlan el tráfico en una interfaz de a un sentido por vez. Se deben crear dos ACL diferentes para controlar el tráfico entrante y saliente.
- Una ACL por interfaz: las ACL controlan el tráfico para una interfaz, por ejemplo, GigabitEthernet 0/0.

# Desarrollo

## Práctica a - 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 | 255.255.255.224 | 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 | | |

### Parte 1: Configurar una ACL extendida y nombrada

Utilice una ACL con nombre para implementar la política siguiente:

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

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

```
ip access-list extended ACL
```

b. Registre la instrucción que deniega el acceso de la PC1 al Servidor1 solo para HTTP (puerto 80).

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

c. Registre la instrucción que deniega el acceso de la PC1 al Servidor1 solo para HTTPS (puerto 443).

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

d. Registre la instrucción que deniega el acceso de la PC1 al Servidor2 solo para HTTP.

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

e. 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 64.103.255.254 eq 443
```

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

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

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

b. 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 64.103.255.254 eq 21
```

*Paso 3: Denegar a la PC3 que haga ping al Servidor1 y al Servidor2.*

a. Registre la instrucción que deniega el acceso ICMP de la PC3 al Servidor1.

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

b. 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 64.103.255.254
permit ip any any
```

*Paso 4: Permitir todo el tráfico IP restante.*

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?

```
permit ip any any
```

## 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.*

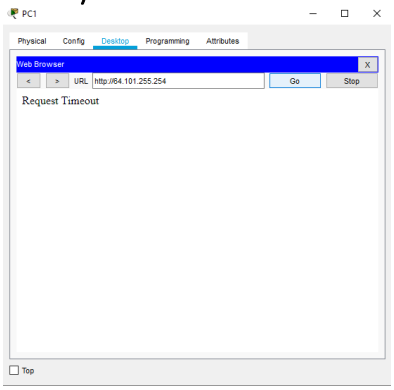
a. ¿Cuáles son los comandos que necesita para aplicar la ACL a la interfaz apropiada en el sentido correcto?

```
interface g0/0
ip access-group ACL in
```

*Paso 2: probar el acceso de cada computadora.*

- PC1

HTTP y HTTPS




FTP

```
C:\>ftp 64.101.255.254
```

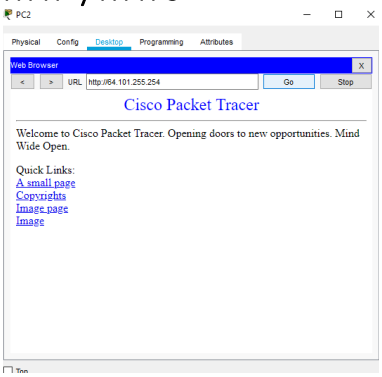
```
Trying to connect...64.101.255.254
Connected to 64.101.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)

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)
```

Ping

```
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=8ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms 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 = 5ms

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=11ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=10ms 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 = 11ms, Average = 6ms
```

- PC2

HTTP y HTTPS




FTP

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

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

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

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

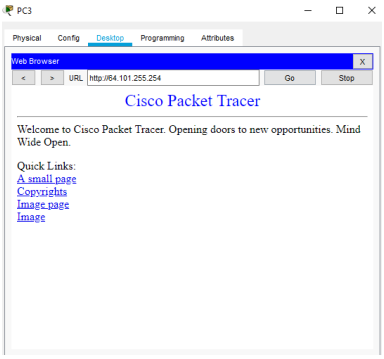
Ping

```
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=6ms TTL=126
Reply from 64.101.255.254: bytes=32 time=14ms TTL=126
Reply from 64.101.255.254: bytes=32 time=2ms 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 = 14ms, 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=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=12ms TTL=126
Reply from 64.103.255.254: bytes=32 time=2ms 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
```

- PC3

HTTP y HTTPS




FTP

```
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)

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)
```

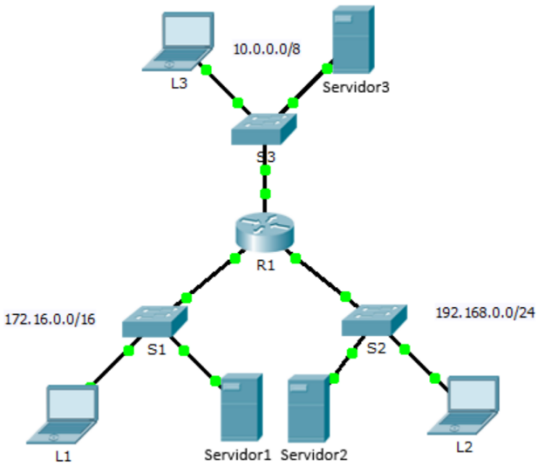
Ping

```
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.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
```

```
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.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
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)
```

## Práctica b - Resolución de problemas de las ACL

### Topología




### Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
|---|---|---|---|---|
| R1 | G0/0 | 10.0.0.1 | 255.0.0.0 | N/A |
| | G0/1 | 172.16.0.1 | 255.255.0.0 | N/A |
| | G0/2 | 192.168.0.1 | 255.255.255.0 | N/A |
| Server1 | NIC | 172.16.255.254 | 255.255.0.0 | 172.16.0.1 |
| Server2 | NIC | 192.168.0.254 | 255.255.255.0 | 192.168.0.1 |
| Server3 | NIC | 10.255.255.254 | 255.0.0.0 | 10.0.0.1 |
| L1 | NIC | 172.16.0.2 | 255.255.0.0 | 172.16.0.1 |
| L2 | NIC | 192.168.0.2 | 255.255.255.0 | 192.168.0.1 |
| L3 | NIC | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |

### Situación

En esta red, deberían estar implementadas las tres políticas siguientes:

- Los hosts de la red 192.168.0.0/24 no pueden acceder a ningún servicio TCP del Servidor3.
- Los hosts de la red 10.0.0.0/8 no pueden acceder al servicio HTTP del Servidor1.
- Los hosts de la red 172.16.0.0/16 no pueden acceder al servicio FTP del Servidor2.

Nota: todos los nombres de usuario y las contraseñas del FTP son “cisco”. No debe haber otras restricciones. Lamentablemente, las reglas implementadas no funcionan de manera correcta. Su tarea es buscar y corregir los errores relacionados con las listas de acceso en el R1.

## Parte 1 - Los hosts de la red 192.168.0.0/24 no pueden acceder a ningún servicio TCP del Servidor3.

Los hosts de la red 192.168.0.0/24 no pueden acceder (intencionalmente) a ningún servicio TCP del Servidor3, pero no deberían tener otro tipo de restricción.

### *Paso 1: determinar el problema de la ACL.*

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

- Con la L2, intente acceder a los servicios FTP y HTTP de Servidor1, Servidor2, y Servidor3.

```
Servidor #1
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254

%Error opening ftp://172.16.255.254/ (Timed out)
(Disconnecting from ftp server)
```

```
Servidor #2
C:\>ftp 192.168.0.254
Trying to connect...192.168.0.254
Connected to 192.168.0.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

```
Servidor #3
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254

%Error opening ftp://10.255.255.254/ (Timed out)
(Disconnecting from ftp server)
```

- Desde la L2, haga ping a Servidor1, Servidor2 y Servidor3.

```
Servidor #1
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 172.16.255.254:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Servidor #2

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time=1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Servidor #3

```
C:\>ping 10.255.255.254

Pinging 10.255.255.254 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 10.255.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Desde la L2, haga ping a G0/2 del R1.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Vea la configuración en ejecución en el R1. Examine la lista de acceso 192_to_10 y su ubicación en las interfaces. ¿La lista de acceso se colocó en la interfaz apropiada y en el sentido correcto? ¿Existe alguna

instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

```
R1#show access-list 192_to_10
Extended IP access list 192_to_10
deny tcp 192.168.0.0 0.0.0.255 host 10.255.255.254 (12 match(es))
```

Considero que la lista de acceso extendida 192_to_10 está en la interfaz apropiada y en el sentido correcto, dado que únicamente deniega un segmento de red al servidor, y por defecto esta implicitico "deny any any", es por lo que todo está denegado y solo está la instrucción deny, no hay orden que revisar.

- Realice otras pruebas, según sea necesario.

### *Paso 2: implementar una solución*

Realice un ajuste a la lista de acceso 192_to_10 para solucionar el problema.

Vamos a agregar un permiso de todos a todos en el router #1

```
R1(config)#ip access-list extended 192_to_10
R1(config-ext-nacl)#20 permit ip any any
R1(config-ext-nacl)#end
```

```
R1#sh running-config
ip access-list extended 192_to_10
deny tcp 192.168.0.0 0.0.0.255 host 10.255.255.254
permit ip any any
```

O bien:

```
R1#show access-list 192_to_10
Extended IP access list 192_to_10
deny tcp 192.168.0.0 0.0.0.255 host 10.255.255.254 (12 match(es))
permit ip any any
```

### *Paso 3: verificar que el problema se haya resuelto y registrar la solución*

- Con la L2, intente acceder a los servicios FTP y HTTP de Servidor1, Servidor2, y Servidor3.

Por lo que volveremos a realizar las primeras pruebas del paso #1.

```
Servidor #1
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254
Connected to 172.16.255.254
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 192.168.0.254
Trying to connect...192.168.0.254
Connected to 192.168.0.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Servidor #3

```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254

%Error opening ftp://10.255.255.254/ (Timed out)
(Disconnecting from ftp server)
```

Dado que el enunciado especifica que los hosts de la red 192.168.0.0/24 no pueden acceder a ningún servicio TCP del Servidor #3, y ftp pertenece a la familia TCP, todo correcto.

- Desde la L2, haga ping a Servidor1, Servidor2 y Servidor3.

Servidor #1

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time=1ms TTL=127
Reply from 172.16.255.254: bytes=32 time=2ms TTL=127
Reply from 172.16.255.254: bytes=32 time=1ms TTL=127
Reply from 172.16.255.254: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Servidor #2

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:
```

```
Reply from 192.168.0.254: bytes=32 time=24ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 24ms, Average = 6ms
```

Servidor #3

```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254

%Error opening ftp://10.255.255.254/ (Timed out)
(Disconnecting from ftp server)
```

- Desde la L2, haga ping a G0/2 del R1.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

## Parte 2 - Los hosts de la red 10.0.0.0/8 no pueden acceder (intencionalmente) al servicio HTTP del Servidor1, pero no deberían tener otro tipo de restricción.

### *Paso 1: determinar el problema de la ACL.*

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

- Con la L3, intente acceder a los servicios FTP y HTTP de Servidor1, Servidor2, y Servidor3.

  Servicios FTP

  Servidor #1

```
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254
Connected to 172.16.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

  Servidor #2

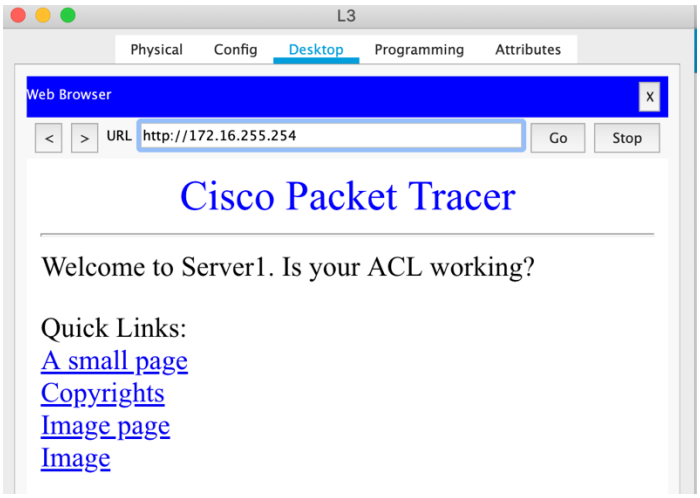
```
C:\>ftp 192.168.0.254
Trying to connect...192.168.0.254
Connected to 192.168.0.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

  Servidor #3

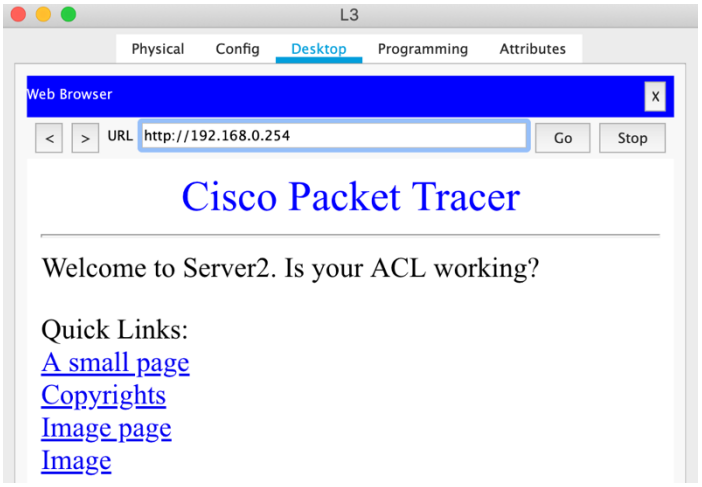
```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254
Connected to 10.255.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Servicios HTTP

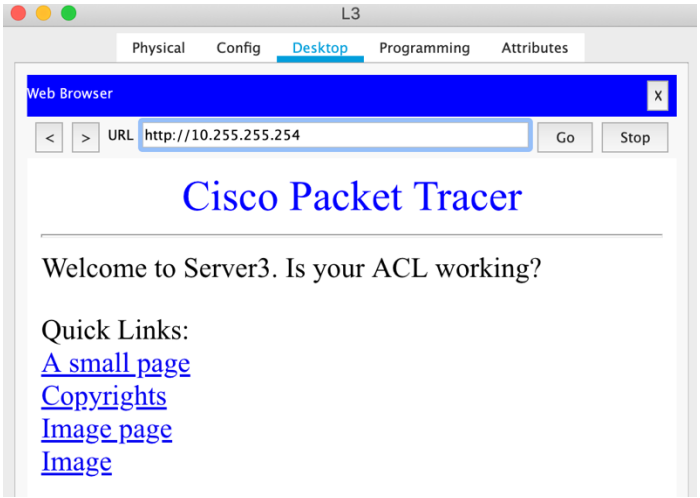
Servidor #1




Servidor #2




Servidor #3



- Desde la L3, haga ping a Servidor1, Servidor2 y Servidor3.

Servidor #1

```
C:\>ping 172.16.255.254
Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time=1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.255.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Servidor #2

```
C:\>ping 192.168.0.254
Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time=5ms TTL=127
Reply from 192.168.0.254: bytes=32 time=1ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 5ms, Average = 1ms
```

Servidor #3

```
C:\>ping 10.255.255.254
Pinging 10.255.255.254 with 32 bytes of data:

Reply from 10.255.255.254: bytes=32 time<1ms TTL=128
Reply from 10.255.255.254: bytes=32 time<1ms TTL=128
Reply from 10.255.255.254: bytes=32 time<1ms TTL=128
Reply from 10.255.255.254: bytes=32 time=1ms TTL=128

Ping statistics for 10.255.255.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- Vea la configuración en ejecución en el R1. Examine la lista de acceso 10_to_172 y su ubicación en las interfaces. ¿La lista de acceso se colocó en la interfaz apropiada y en el sentido correcto? ¿Existe alguna

instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

Parece que no hubiese lista de acceso, ya que se hay acceso libre del segmento a cualquiera de los 3 servidores, y el enunciado solicita que el segmento de red 10.0.0.0/8 no se le de acceso a servicio HTTP en el servidor #1.

Vamos a revisar la lista de acceso existente en el router #1:

- Realice otras pruebas, según sea necesario.

```
R1#show access-lists
Extended IP access list 10_to_172
10 deny tcp 10.0.0.0 0.255.255.255 host 172.16.255.254 eq www
20 permit ip any any (29 match(es))
Extended IP access list 172_to_192
10 permit ip any any (26 match(es))
20 deny tcp 172.16.0.0 0.0.255.255 host 192.168.0.254 eq ftp
Extended IP access list 192_to_10
10 deny tcp 192.168.0.0 0.0.0.255 host 10.255.255.254 (36 match(es))
20 permit ip any any (30 match(es))
```

```
R1#show running-config
hostname R1
interface GigabitEthernet0/0
ip address 10.0.0.1 255.0.0.0
ip access-group 10_to_172 out
duplex auto
speed auto
!
```

*Paso 2: implementar una solución.*

Realice un ajuste a la lista de acceso 10_to_172 para solucionar el problema.

Considero que la ACL es correcta pero la aplicación de esta no lo es, debería de estar de entrada y no salida, entonces vamos a intentar corregirlo:

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int
R1(config)#interface g
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#no ip ac
R1(config-if)#no ip access-group 10_to_172 out
R1(config-if)#ip ac
R1(config-if)#ip access-group 10_to_172 in
R1(config-if)#end
```

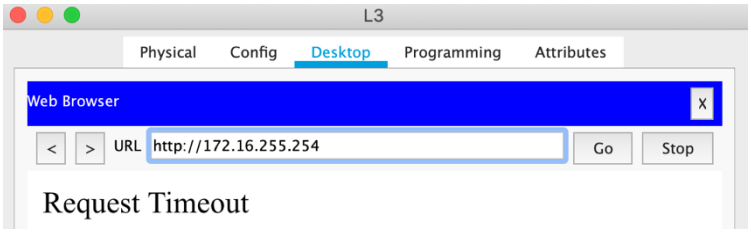
*Paso 3: verificar que el problema se haya resuelto y registrar la solución.*

Si el problema se resuelve, registre la solución. De lo contrario, vuelva al paso 1.

Se nos solicita que el segmento 10.0.0.0/8 no tenga acceso al servicio http del servidor #1, vamos a revisar:

Comprobamos la configuración

```
R1#show running-config
interface GigabitEthernet0/0
ip address 10.0.0.1 255.0.0.0
ip access-group 10_to_172 in
duplex auto
speed auto
```




Vamos a revisar que los servicios de ftp y ping siguen funcionando:

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time=22ms TTL=127
Reply from 172.16.255.254: bytes=32 time=1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.255.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 22ms, Average = 5ms

C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254
Connected to 172.16.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Parte 3 – Los hosts de la red 172.16.0.0/16 no pueden acceder (intencionalmente) al servicio FTP del Servidor2, pero no deberían tener otro tipo de restricción.

*Paso 1: determinar el problema de la ACL.*

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

- Con la L1, intente acceder a los servicios FTP y HTTP de Servidor1, Servidor2, y Servidor3.

Servicio FTP

Servidor #1

```
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254
Connected to 172.16.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Servidor #2

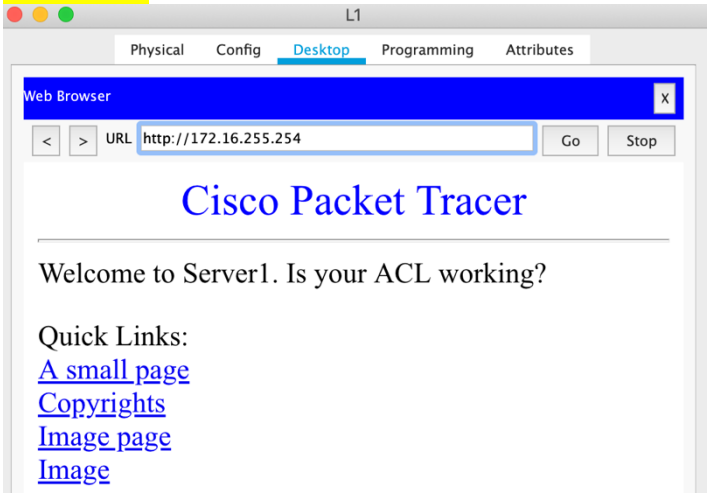
```
C:\>ftp 192.168.0.254
Trying to connect...192.168.0.254
Connected to 192.168.0.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Servidor #3

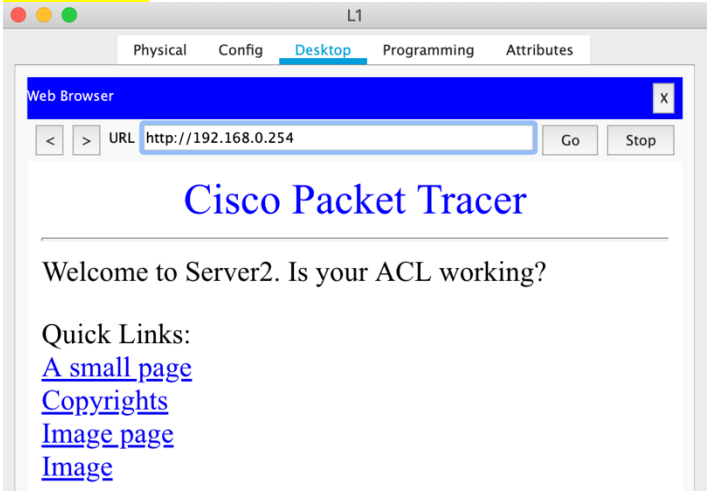
```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254
Connected to 10.255.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Servicio HTTP

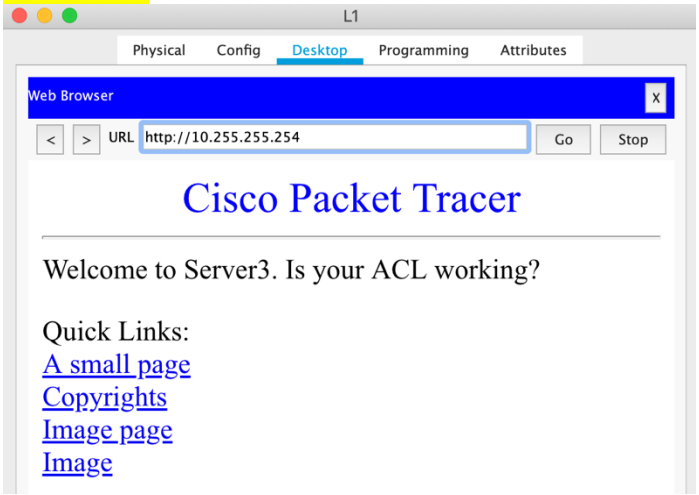
Servidor #1




Servidor #2




Servidor #3



- Desde la L1, haga ping a Servidor1, Servidor2 y Servidor3.

Servidor #1

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time=1ms TTL=128
Reply from 172.16.255.254: bytes=32 time<1ms TTL=128
Reply from 172.16.255.254: bytes=32 time<1ms TTL=128
Reply from 172.16.255.254: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.255.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Servidor #2

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time=1ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127
Reply from 192.168.0.254: bytes=32 time=2ms TTL=127
Reply from 192.168.0.254: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.0.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Servidor #3

```
C:\>ping 10.255.255.254

Pinging 10.255.255.254 with 32 bytes of data:

Reply from 10.255.255.254: bytes=32 time=1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127

Ping statistics for 10.255.255.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- Vea la configuración en ejecución en el R1. Examine la lista de acceso 172_to_192 y su ubicación en las interfaces. ¿La lista de acceso se colocó en el puerto apropiado y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

Parece que no hubiese lista de acceso, ya que se hay acceso libre del segmento a cualquiera de los 3 servidores, y el enunciado solicita que el segmento de red 172.16.0.0/16 no se le de acceso a servicio FTP en el servidor #2.

- Realice otras pruebas, según sea necesario.

Vamos a revisar la lista de acceso existente en el router #1:

```
R1#show running-config
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
ip access-group 172_to_192 in
duplex auto
speed auto
!

R1#show access-list 172_to_192
Extended IP access list 172_to_192
permit ip any any (87 match(es))
deny tcp 172.16.0.0 0.0.255.255 host 192.168.0.254 eq ftp
```

Este caso es muy similar al anterior, ya que no se está aplicando la condición de restricción de la instrucción deny, entonces de acuerdo con los cuestionamientos anteriores, la lista de acceso está en el puerto y sentido correcto, dado que primero se permite y luego se deniega, esa es la instrucción que no permite que se ejecute como se solicita, es decir el orden no es el correcto.

*Paso 2: implementar una solución.*

Realice un ajuste a la lista de acceso 172_to_192 para solucionar el problema.

```
R1#show access-list 172_to_192
Extended IP access list 172_to_192
permit ip any any (87 match(es))
deny tcp 172.16.0.0 0.0.255.255 host 192.168.0.254 eq ftp

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip a
R1(config)#ip access-listext
R1(config)#ip access-list ex
R1(config)#ip access-list extended 172_to_192
R1(config-ext-nacl)#no 10
R1(config-ext-nacl)#30 permit ip any any
```

```
R1#show access-list 172_to_192
Extended IP access list 172_to_192
permit ip any any (87 match(es))
deny tcp 172.16.0.0 0.0.255.255 host 192.168.0.254 eq ftp
```

```
R1#show access-lists 172_to_192
Extended IP access list 172_to_192
deny tcp 172.16.0.0 0.0.255.255 host 192.168.0.254 eq ftp
permit ip any any
```

*Paso 3: verificar que el problema se haya resuelto y registrar la solución.*

Si el problema se resuelve, registre la solución. De lo contrario, vuelva al paso 1.

Verificamos que el segmento 172.16.0.0/16 no tiene servicio de FTP en el servidor #2

```
C:\>FTP 192.168.0.254
Trying to connect...192.168.0.254

%Error opening ftp://192.168.0.254/ (Timed out)
(Disconnecting from ftp server)
```

# Conclusiones

## García González Aarón Antonio

Esta practica estuvo sencilla, hasta cierto punto fue “bonita” ya que se pudo ver de primera mano como permitir y denegar servicios tales como http, ftp y de ping.
El uso de las key words me quedo mucho más claro al aplicarlas, para el caso del sentido de entrada o salida de una ACL suponía que el ponerla en la entrada o en la salida era indiferente, solo se pondría a trabajar al router de más, pero al hacer la práctica pude observar que, si no está en donde debe de estar, no se aplica bien la lista de acceso.
Detalles tan simples como el orden, el sentido u el omitir que siempre hay un deny any any implícito y no permitir después de denegar, hará que todo este denegado para todos.

## Villalba Gil Angel

Con la realización de esta práctica me quedo más clara las operaciones de “denegar” y “permitir”, el realizar la practica fue algo sencillo pues todo iba paso a paso por lo que para ser sincero no me confundí, además de que las palabras clave son muy fáciles de entender.
Cuando la había leído aun no comprendía como hacer lo que se nos pedía sin embargo poco a poco al ver esas palabras clave y sentencias fue muy sencillo el aplicarlos y resolver lo que se pedía en la práctica.
Espero así sean las siguientes practicas pues me han ayudado a aprender cosas que no sabía con anterioridad.

## Referencias

[1]. "Principios básicos de routing y switching", Itesa.edu.mx, 2020. [Online]. Available: https://www.itesa.edu.mx/netacad/switching/course/module9/index.html#9.0.1.1. [Accessed: 15- Nov- 2020].