Control de Tráfico Firewall y QoS con MikroTik RouterOS

v6.33.5.01

Manual de Laboratorio

ABC Xperts ®
Network Xperts ®
Academy Xperts ®

Tabla de Contenido

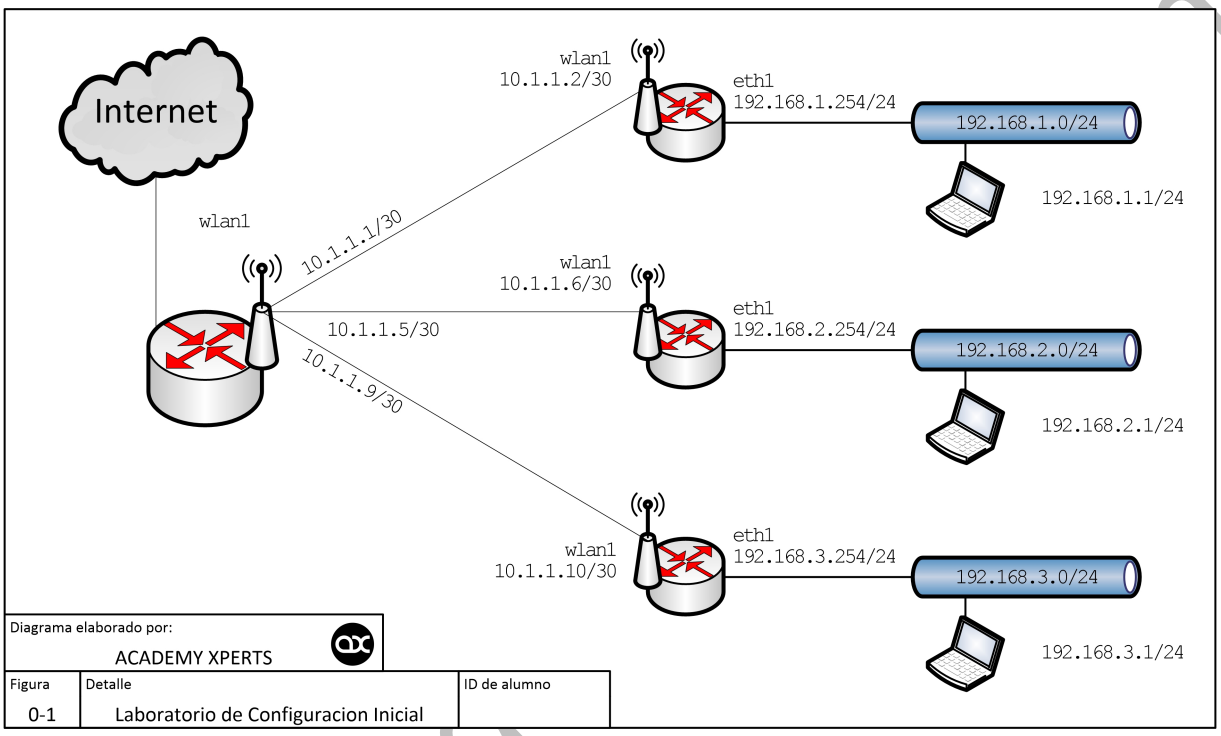
Laboratorio 0-1: Configuración Inicial

Objetivo:

- Cada estudiante debe configurar su equipo de trabajo (router) para poder dar acceso a internet a su laptop.
- Se debe contar con los conocimientos necesarios de NAT, Ruteo, Wireless y DNS para ejecutar esta práctica, los mismos que fueron aprendidos en el curso inicial de RouterOS.

Escenario:

- La Figura 0-1 (Laboratorio de Configuración Inicial) muestra la configuración que deberán conseguir cada uno de los estudiantes



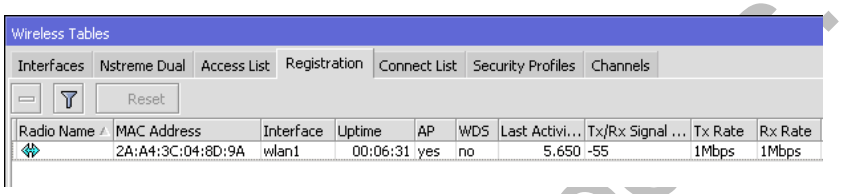
Asignación de direcciones IP

- Cada participante deberá trabajar con un grupo de direcciones específicas para las interfaces Wireless y LAN.
- El instructor debe asignar un número a cada estudiante con el cual deberá validar las subredes entregadas en base a la siguiente tabla (**Tabla L0-1.1**)

	LAN			IP wlan1	IP wlan1			
ID	ID de red	IP ether1	IP Laptop	(estudiante)	(trainer)	Gateway	DNS1	DNS2
1	192.168.1.0/24	192.168.1.254/24	192.168.1.1/24	10.1.1.2/30	10.1.1.1/30	10.1.1.1	10.1.1.1	8.8.8.8
2	192.168.2.0/24	192.168.2.254/24	192.168.2.1/24	10.1.1.6/30	10.1.1.5/30	10.1.1.5	10.1.1.5	8.8.8.8
3	192.168.3.0/24	192.168.3.254/24	192.168.3.1/24	10.1.1.10/30	10.1.1.9/30	10.1.1.9	10.1.1.9	8.8.8.8
4	192.168.4.0/24	192.168.4.254/24	192.168.4.1/24	10.1.1.14/30	10.1.1.13/30	10.1.1.13	10.1.1.13	8.8.8.8
5	192.168.5.0/24	192.168.5.254/24	192.168.5.1/24	10.1.1.18/30	10.1.1.17/30	10.1.1.17	10.1.1.17	8.8.8.8
6	192.168.6.0/24	192.168.6.254/24	192.168.6.1/24	10.1.1.22/30	10.1.1.21/30	10.1.1.21	10.1.1.21	8.8.8.8
7	192.168.7.0/24	192.168.7.254/24	192.168.7.1/24	10.1.1.26/30	10.1.1.25/30	10.1.1.25	10.1.1.25	8.8.8.8
8	192.168.8.0/24	192.168.8.254/24	192.168.8.1/24	10.1.1.30/30	10.1.1.29/30	10.1.1.29	10.1.1.29	8.8.8.8
9	192.168.9.0/24	192.168.9.254/24	192.168.9.1/24	10.1.1.34/30	10.1.1.33/30	10.1.1.33	10.1.1.33	8.8.8.8
10	192.168.10.0/24	192.168.10.254/24	192.168.10.1/24	10.1.1.38/30	10.1.1.37/30	10.1.1.37	10.1.1.37	8.8.8.8
11	192.168.11.0/24	192.168.11.254/24	192.168.11.1/24	10.1.1.42/30	10.1.1.41/30	10.1.1.41	10.1.1.41	8.8.8.8
12	192.168.12.0/24	192.168.12.254/24	192.168.12.1/24	10.1.1.46/30	10.1.1.45/30	10.1.1.45	10.1.1.45	8.8.8.8
13	192.168.13.0/24	192.168.13.254/24	192.168.13.1/24	10.1.1.50/30	10.1.1.49/30	10.1.1.49	10.1.1.49	8.8.8.8
14	192.168.14.0/24	192.168.14.254/24	192.168.14.1/24	10.1.1.54/30	10.1.1.53/30	10.1.1.53	10.1.1.53	8.8.8.8
15	192.168.15.0/24	192.168.15.254/24	192.168.15.1/24	10.1.1.58/30	10.1.1.57/30	10.1.1.57	10.1.1.57	8.8.8.8
16	192.168.16.0/24	192.168.16.254/24	192.168.16.1/24	10.1.1.62/30	10.1.1.61/30	10.1.1.61	10.1.1.61	8.8.8.8
17	192.168.17.0/24	192.168.17.254/24	192.168.17.1/24	10.1.1.66/30	10.1.1.65/30	10.1.1.65	10.1.1.65	8.8.8.8
18	192.168.18.0/24	192.168.18.254/24	192.168.18.1/24	10.1.1.70/30	10.1.1.69/30	10.1.1.69	10.1.1.69	8.8.8.8
19	192.168.19.0/24	192.168.19.254/24	192.168.19.1/24	10.1.1.74/30	10.1.1.73/30	10.1.1.73	10.1.1.73	8.8.8.8
20	192.168.20.0/24	192.168.20.254/24	192.168.20.1/24	10.1.1.78/30	10.1.1.77/30	10.1.1.77	10.1.1.77	8.8.8.8

Tarea 1: Configuración Wlan (Estudiante)

1. Hacer un reset a toda la configuración del router
```
/system reset-configuration no-defaults=yes
```
2. Verificar que el instructor ha configurado una red Wireless con los correspondientes parámetros de autenticación y encriptación.
   - SSID: `MTCTCE_AcademyXperts`
   - Autenticación: `WPA PSK` y/o `WPA2 PSK`
   - Cifrado: `AES`
   - WPA1 y/o WPA2 Pre-Shared key: `mikrotik`
3. Configurar la tarjeta Wireless del Estudiante
```
/interface wireless security-profiles add authentication-types=wpa-psk,wpa2-psk \
    mode=dynamic-keys name=profile1 wpa-pre-shared-key=mikrotik \
    wpa2-pre-shared-key=mikrotik
/interface wireless set wlan1 band=2ghz-b/g/n disabled=no mode=station-bridge \
    security-profile=profile1 ssid=MTCTCE_AcademyXperts
```
4. El estudiante debe estar conectado al AP del instructor. Debe verificar revisando en la tabla de registro y obtener un resultado similar al siguiente:
```
/interface wireless registration-table print
 # INTERFACE    RADIO-NAME       MAC-ADDRESS               AP  SIGNAL... TX-RATE UPTIME
 0 wlan1                         2A:A4:3C:04:8D:9A         yes -50dBm... 1Mbps   1m9s
```



Tarea 2: Asignar IP a interface wlan

1. El estudiante debe configurar la dirección IP correspondiente a la `wlan1` de acuerdo a la **Tabla L0-1.1** y basado en la asignación entregada por el instructor.
```
/ip address add address=10.1.1.2/30 interface=wlan1
```
2. Verificar por medio de `ping` que puede llegar al AP (interface `wlan`) del Instructor. Para esto deberá hacer `ping` a la IP de la subred `/30` correspondiente.
```
/ping 10.1.1.1
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 10.1.1.1                                   56  64 0ms
    1 10.1.1.1                                   56  64 0ms
    2 10.1.1.1                                   56  64 0ms
    3 10.1.1.1                                   56  64 0ms
    4 10.1.1.1                                   56  64 0ms
    sent=5 received=5 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Tarea 3: Configurar la ruta por default

1. El estudiante debe configurar la ruta por default (`0.0.0.0/0`) para poder salir a Internet. Para esto deberá especificar la IP del Gateway correspondiente según la **Tabla L0-1.1**
```
/ip route add dst-address=0.0.0.0/0 gateway=10.1.1.1
```
2. Verificar por medio de `ping` que puede llegar a una dirección IP pública, por ejemplo, a la IP `8.8.8.8`.
```
/ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56  48 125ms
    1 8.8.8.8                                    56  48 76ms
    2 8.8.8.8                                    56  48 77ms
    sent=3 received=3 packet-loss=0% min-rtt=76ms avg-rtt=92ms max-rtt=125ms
```

Tarea 4: Configurar el DNS

1. El estudiante debe configurar las direcciones de los DNS servers para poder resolver los nombres de dominio. Para esto deberá especificar la IP de los servidores DNS1 y DNS2 correspondientes según la **Tabla L0-1.1**. Es importante también configurar el router para que actúe como caché DNS (`allow-remote-requests`).
```
/ip dns set servers=10.1.1.1,8.8.8.8 allow-remote-requests=yes
```
2. Verificar por medio de `ping` que puede resolver un nombre de dominio, por ejemplo `google.com`
```
/ping google.com
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 190.57.158.234                             56  57 6ms
    1 190.57.158.234                             56  57 6ms
    2 190.57.158.234                             56  57 5ms
    sent=3 received=3 packet-loss=0% min-rtt=5ms avg-rtt=5ms max-rtt=6ms
```

Tarea 5: Configurar interface Ether1 del router e Interface Ethernet de Laptop Estudiante

1. El estudiante debe configurar la interface Ether1 en base la dirección asignada según la **Tabla L0-1.1**.

```
/ip address add address=192.168.1.1/24 interface=ether1
```

2. El estudiante debe configurar los parámetros de la tarjeta de red Ethernet de su laptop

3. Verificar por medio de `ping` que puede llegar desde la laptop a la dirección IP de la interface `Ether1` de su router

```
MacBook-Pro:~ academy$ ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254): 56 data bytes
64 bytes from 192.168.1.254: icmp_seq=0 ttl=64 time=0.481 ms
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.462 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.388 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.433 ms

--- 192.168.1.254 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.388/0.441/0.481/0.035 ms
```

Tarea 6: Configurar interface Ether1 del router e Interface Ethernet de Laptop Estudiante

1. El estudiante debe configurar la regla de `src-nat` para poder permitir que su laptop salga a internet.

```
/ip firewall nat add chain=srcnat out-interface=wlan1 action=masquerade
```

2. El estudiante debe verificar que puede navegar a internet desde su laptop

Tarea 7: Configurar dirección IP de servidores NTP y la fecha/hora actual del sistema

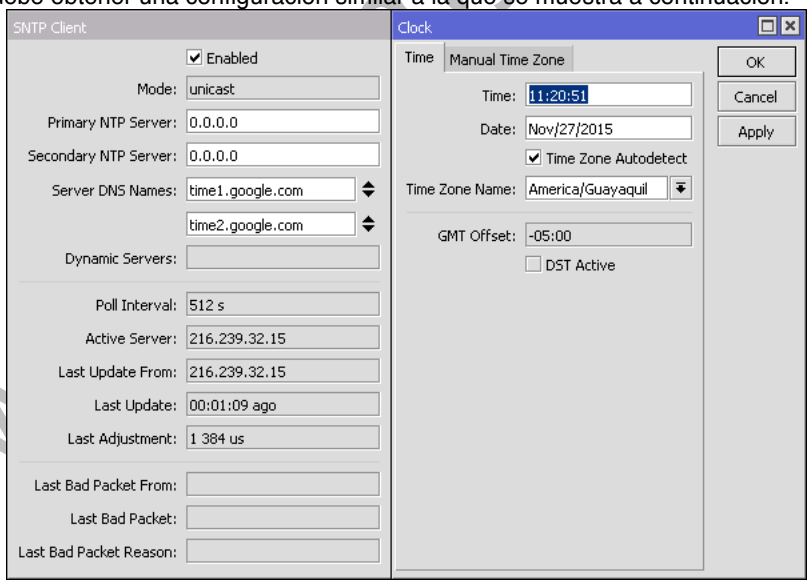
1. El estudiante debe configurar las direcciones IP de los servidores NTP.

```
/system ntp client set enabled=yes server-dns-names=time1.google.com,time2.google.com
```

2. El estudiante debe configurar fecha/hora actual del sistema basado en la información obtenida de los servidores NTP.

```
/system clock set time-zone-name=America/Guayaquil
```

3. El estudiante debe obtener una configuración similar a la que se muestra a continuación.

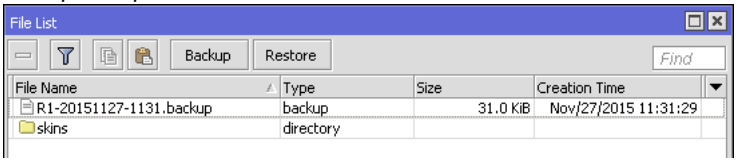


Tarea 8: Generar respaldo de la configuración de su router

1. El estudiante debe configurar las direcciones IP de los servidores NTP.

```
/system backup save
Saving system configuration
Configuration backup saved
```

2. El estudiante debe verificar que el respaldo se generó satisfactoriamente en su router. Para esto debe chequear que el archivo de backup está presente en `/file`. Puede obtener un resultado similar al siguiente:



Lista de tareas a completar (Laboratorio 0-1)
El estudiante debe verificar que se han cumplido los siguientes pasos antes de pasar a los próximos laboratorios. Es sumamente importante completar todos los procesos y ejecutar el respaldo ya que será necesario utilizar dicho backup en ejercicios posteriores

	Marque con √ los pasos que ha podido completar	√
Tarea 1	Verificar que el router está conectado al AP del Instructor	
Tarea 2	Ejecutar un ping satisfactorio al AP del Instructor	
Tarea 3	Ejecutar un ping satisfactorio a `8.8.8.8`	
Tarea 4	Ejecutar un ping satisfactorio a `google.com`	
Tarea 5	Ejecutar un ping satisfactorio a la interface `Ether1` de su router	
Tarea 6	Estudiante debe navegar satisfactoriamente en Internet	
Tarea 7	Estudiante debe obtener la fecha y hora actual en su router	
Tarea 8	Estudiante debe verificar que ha generado el respaldo de su router	
Tarea 9	Estudiante debe copiar el archivo de `backup` a su computador	

Capítulo 1: DNS

Domain Name System

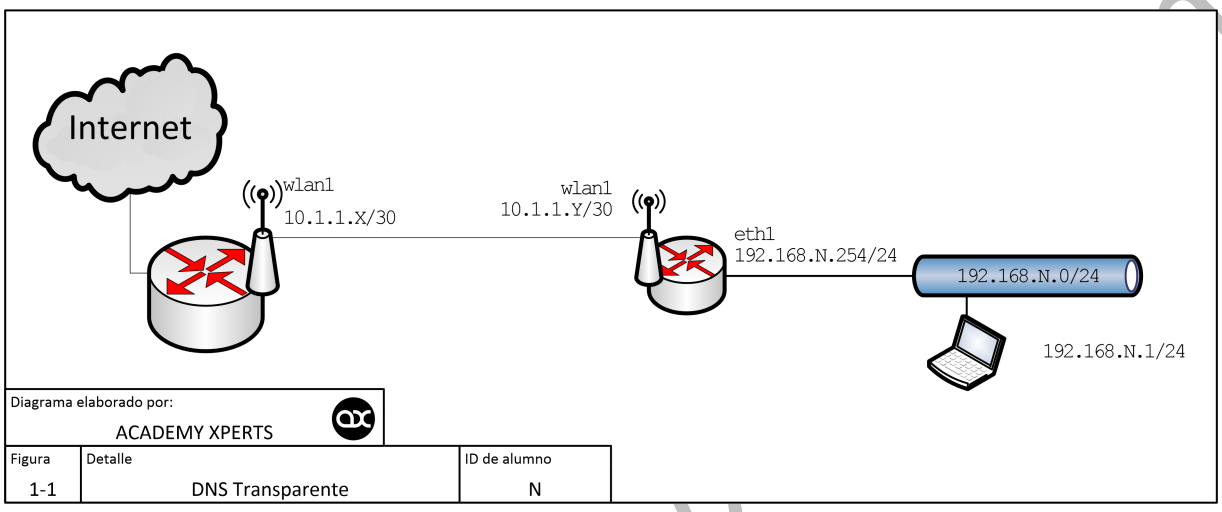
Laboratorio 1-1: DNS transparente

Objetivo:

- Activar el DNS caché
- Capturar el tráfico DNS y re direccionarlo a su propio router
- Comprobar el funcionamiento del DNS transparente

Escenario:

- La Figura 1-1 (Laboratorio de DNS transparente) muestra la configuración que deberán conseguir cada uno de los estudiantes



Tarea 1: Habilitar el servicio DNS Caché

1. En el Laboratorio 0-1 se activó el DNS caché en el router a través de la opción `allow-remote-requests`. Para esto deberá especificar la IP de los servidores DNS1 y DNS2 correspondientes según la **Tabla L0-1.1**

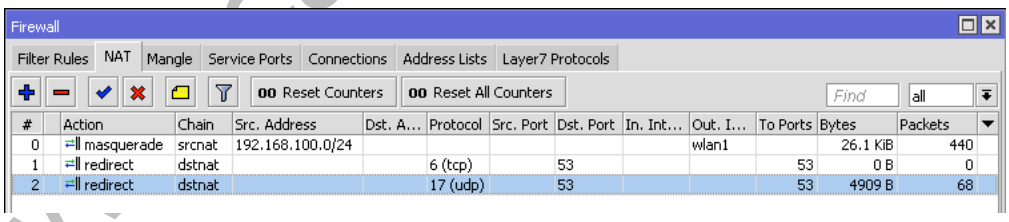
```
/ip dns set servers=10.1.1.2,8.8.8.8 allow-remote-requests=yes
```

Tarea 2: Reglas de dstnat

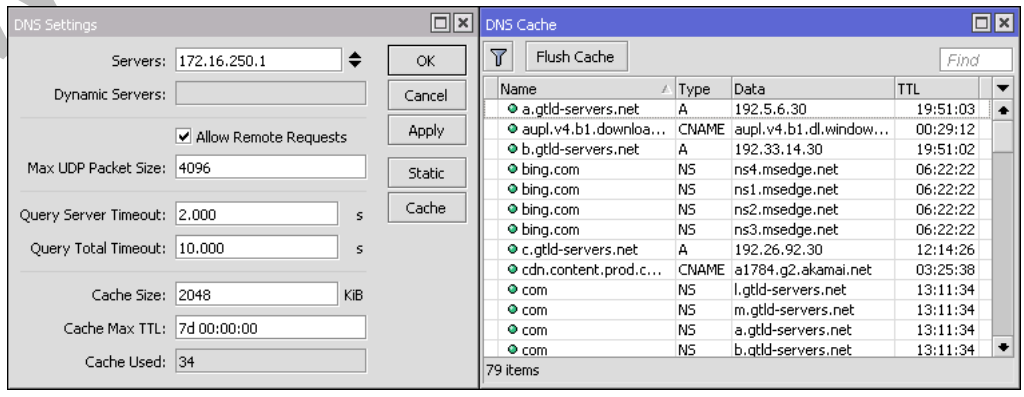
1. Crear las reglas de dstnat para capturar el tráfico TCP 53 y UDP 53

```
/ip firewall nat add chain=dstnat protocol=tcp dst-port=53 action=redirect to-ports=53
/ip firewall nat add chain=dstnat protocol=udp dst-port=53 action=redirect to-ports=53
```

2. Verificar que las reglas de proxy DNS están trabajando. Para esto debe generara tráfico a través del browser de su laptop y observar en `/firewall nat` que por lo menos la regla de UDP presente tráfico de `bytes` y `packets`. Debe obtener un comportamiento similar a la siguiente gráfica:

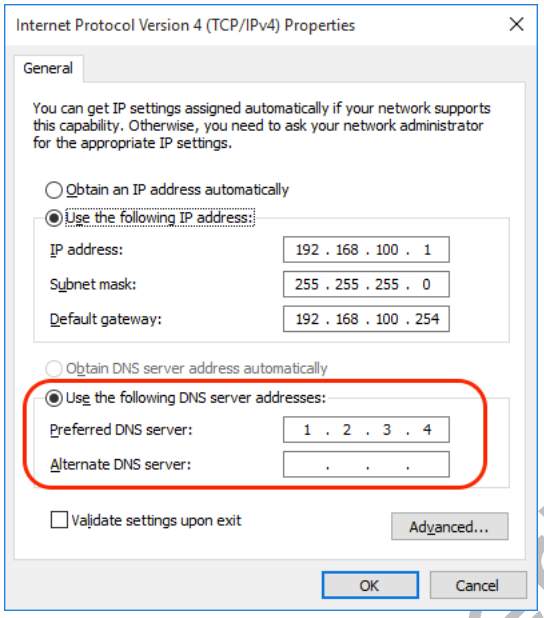


3. Verificar que se está alimentando la tabla DNS Caché. Debe obtener un comportamiento similar a la siguiente gráfica:



Tarea 3: Verificar la efectividad del DNS transparente

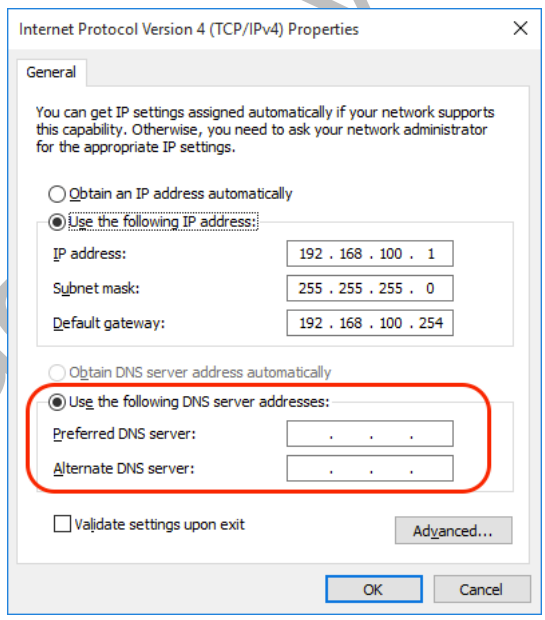
1. El estudiante debe cambiar la dirección IP del DNS Server de su laptop por la dirección IP de un DNS que no exista, por ejemplo `1.2.3.4`



2. Verificar que se sigue manteniendo la resolución de nombres en la laptop a pesar de haber puesto la IP de un DNS Server que no existe. El estudiante debe generara tráfico a través del browser de su laptop.

Tarea 4: Verificar comportamiento cuando no se configura DNS

1. En este ejercicio el estudiante NO configurará ninguna dirección IP en la sección de servidores DNS de su laptop. Debe dejar en blanco este campo.



2. Verificar que YA NO existe resolución de nombres en la laptop cuando no se configura la dirección IP de un DNS Server. El estudiante debe generara tráfico a través del browser de su laptop.

Pregunta 1-1: Por qué en la Tarea 4 no se puede navegar vía browser (resolución de nombres de dominio) a pesar que está activa la configuración de DNS Transparente?

Lista de tareas a completar (Laboratorio 1-1)
El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1	Confirmar que desde su laptop (conectado al router) puede navegar a internet con la configuración del Laboratorio 0-1	
Tarea 2.1	Confirmar que existe tráfico en las reglas dstnat especialmente en UDP 53 (bytes/packets)	
Tarea 2.2	Confirmar que se está alimentando la tabla DNS Caché	
Tarea 3	Confirmar que se sigue teniendo navegación a pesar de haber configurado la dirección IP de un DNS que no existe	
Tarea 4	Confirmar que NO se tiene navegación cuando el campo de configuración de DNS Server en la laptop queda vacío (en blanco)	
Tarea 5	Responder Pregunta 1-1	

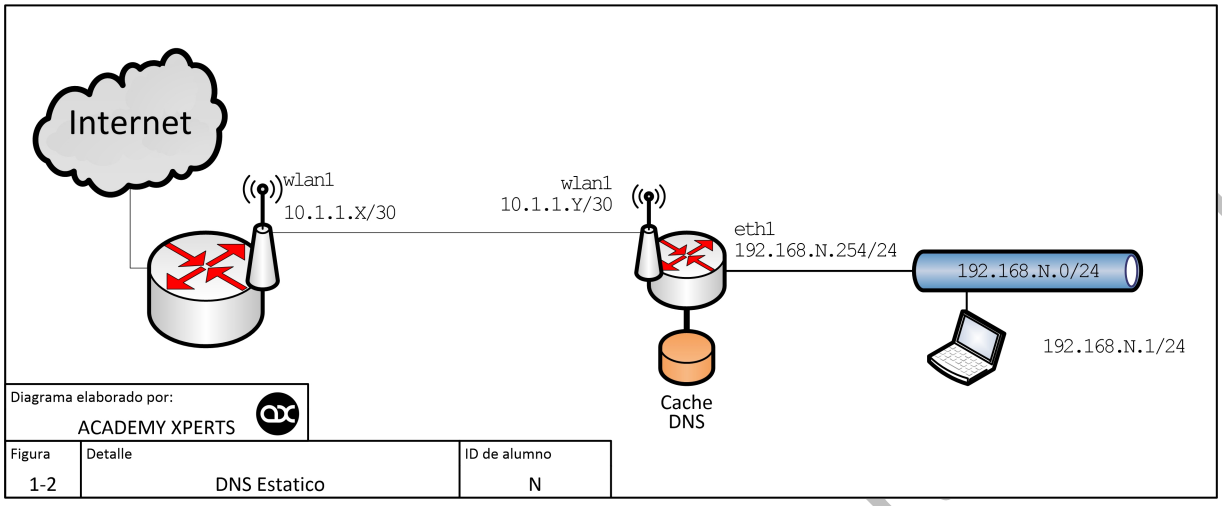
Laboratorio 1-2: DNS Estático

Objetivo:

- Comprobar el funcionamiento de las entradas estáticas DNS

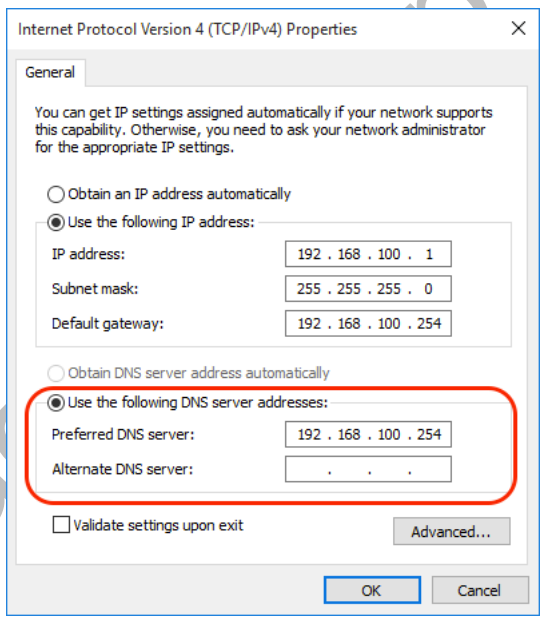
Escenario:

- La Figura 1-2 (Laboratorio de DNS Estático) muestra la configuración que deberán tener cada uno de los estudiantes



Tarea 1: Verificar funcionamiento del DNS Transparente

1. Con la configuración vigente del Laboratorio 1-1 se creará una entrada estática. Recuerde restablecer la dirección IP del servidor DNS primario en la laptop del estudiante



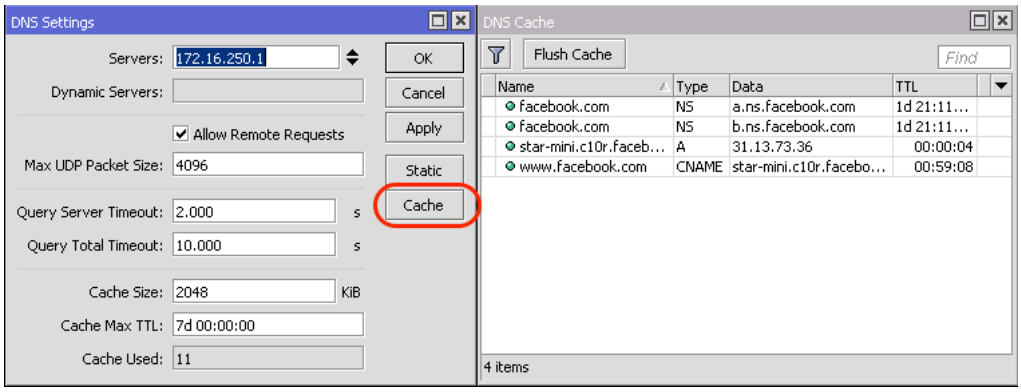
2. Ejecutar un ping a *www.facebook.com* o navegar usando el browser. Cuando ejecute el ping obtendrá una dirección IP similar a la que se muestra continuación:

```
C:\WINDOWS\system32>ping www.facebook.com

Pinging star-mini.c10r.facebook.com [31.13.73.36] with 32 bytes of data:
Reply from 31.13.73.36: bytes=32 time=136ms TTL=81
Reply from 31.13.73.36: bytes=32 time=135ms TTL=81
Reply from 31.13.73.36: bytes=32 time=127ms TTL=81
Reply from 31.13.73.36: bytes=32 time=127ms TTL=81

Ping statistics for 31.13.73.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 127ms, Maximum = 136ms, Average = 131ms
```

3. Verificar en el router la entrada generada en el caché producto del ping o la navegación a *www.facebook.com* . Deberá obtener un resultado similar al siguiente:

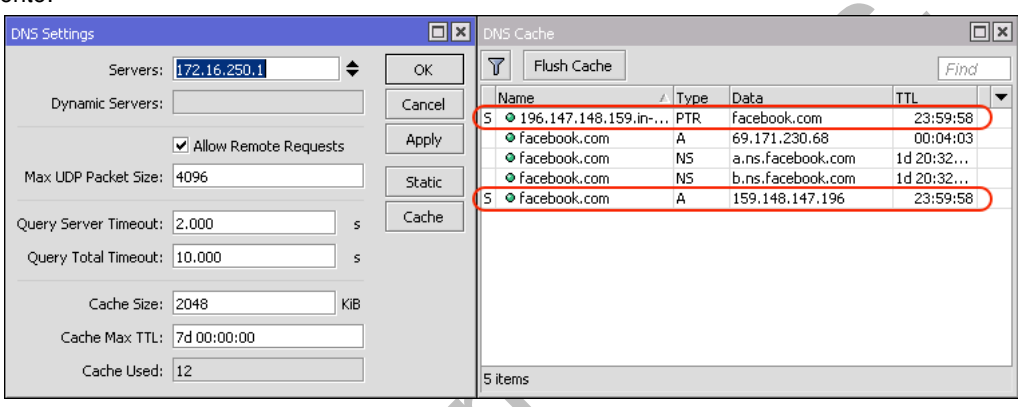


Tarea 2: Crear una entrada de DNS Estática

1. Generar una entrada estática DNS para *www.facebook.com* donde se pondrá una dirección IP diferente a la obtenida en la Tarea 1. En este ejercicio usaremos la IP 159.148.147.196 que corresponde a la IP de *www.mikrotik.com*

```
/ip dns static add name=www.facebook.com address=159.148.147.196
```

2. Verificar en el router que se ha creado la entrada estática en el caché. Deberá obtener un resultado similar al siguiente:



3. Ejecutar un ping a *www.facebook.com*. Se obtendrá la dirección IP de *www.mikrotik.com* (159.148.147.196) que es la que se definió en la entrada estática:

```
C:\WINDOWS\system32>ping www.facebook.com

Pinging star-mini.c10r.facebook.com [159.148.147.196] with 32 bytes of data:
Reply from 159.148.147.196: bytes=32 time=136ms TTL=81
Reply from 159.148.147.196: bytes=32 time=135ms TTL=81
Reply from 159.148.147.196: bytes=32 time=127ms TTL=81
Reply from 159.148.147.196: bytes=32 time=127ms TTL=81

Ping statistics for 159.148.147.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 127ms, Maximum = 136ms, Average = 131ms
```

Pregunta 1-2: Que registro tiene preferencia, Estático o Dinámico, en el Caché DNS?

Lista de tareas a completar (Laboratorio 1-2)

El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1.1	Verificar el ping o navegación a *www.facebook.com*	
Tarea 1.2	Verificar la presencia de la entrada estática en el router	
Tarea 2	Verificar la IP generada como resultado del ping a *www.facebook.com*	
Tarea 5	Responder Pregunta 1-2	

Capítulo 2: DHCP

Dynamic Host Configuration Protocol

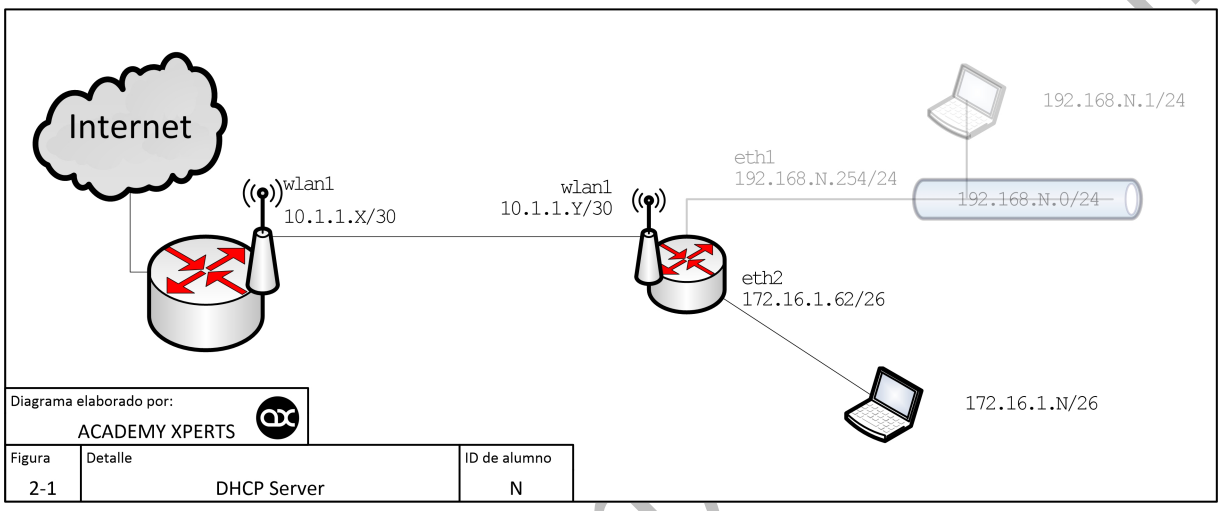
Laboratorio 2-1: DHCP Server

Objetivo:

- Configurar manualmente el DHCP Server.
- Asignar automáticamente la dirección IP a la laptop del cliente
- Confirmar que la laptop sigue teniendo salida a Internet

Escenario:

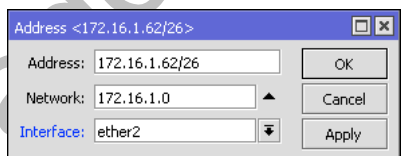
- La Figura 2-1 (DHCP Server) muestra la configuración que deberán conseguir cada uno de los estudiantes
- La configuración de Ether1 se deja intacta.
- Se trabajará en la interface Ether2



Tarea 1: Proceso de creación de DHCP Server manual

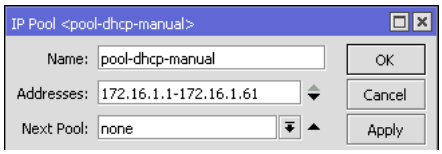
1. Asignar la dirección 172.16.1.62/26 a la interface Ether2

```
/ip address add address=172.16.1.62/26 interface=ether2
```



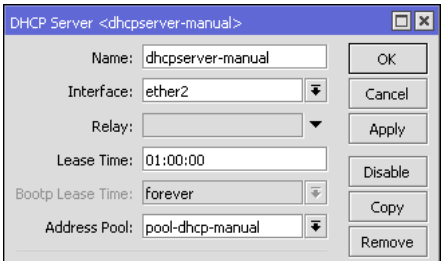
2. Crear un pool de direcciones basados en el rango de IPs del segmento de Ether2. Debe tener en cuidado en excluir del rango la dirección IP de la interface del router, al igual que cualquier IP que se desee asignar estáticamente a cualquier dispositivo.

```
/ip pool add name=pool-dhcp-manual ranges=172.16.1.1-172.16.1.61
```



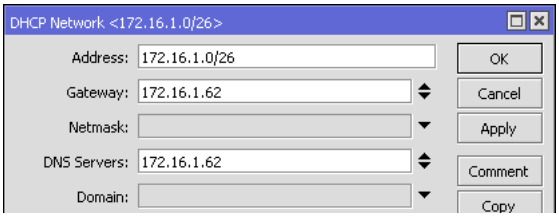
3. Crear el DHCP Server manualmente.

```
/ip dhcp-server add name=dhcpserver-manual interface=ether2 address-pool=pool-dhcp-manual lease-time=1h
disabled=no
```



4. Crear el Network.

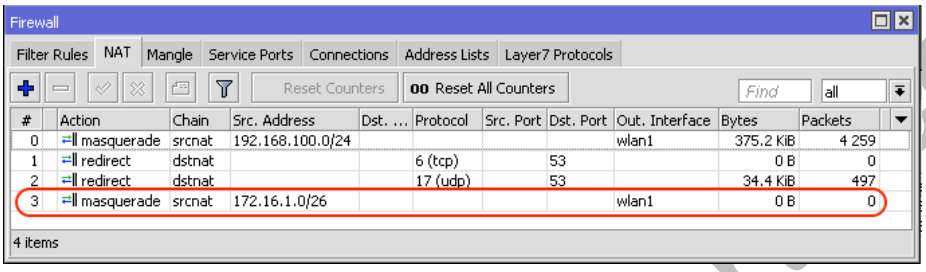
```
/ip dhcp-server network add address=172.16.1.0/26 gateway=172.16.1.62 dns-server=172.16.1.62
```



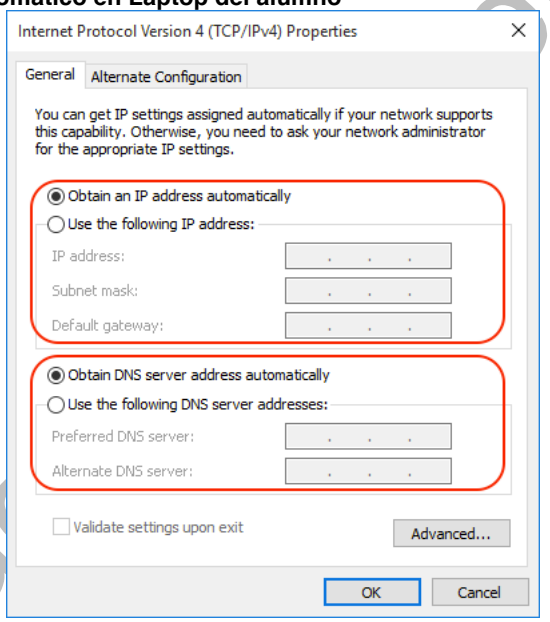
Tarea 2: Agregar la regla de NAT correspondiente

1. Crear una nueva regla de NAT que haga el NATeo de la subred 172.16.1.0/26

```
/ip firewall nat add chain=srcnat src-address=172.16.1.0/26 out-interface=wlan1
action=masquerade
```



Tarea 3: Configuración DHCP automático en Laptop del alumno

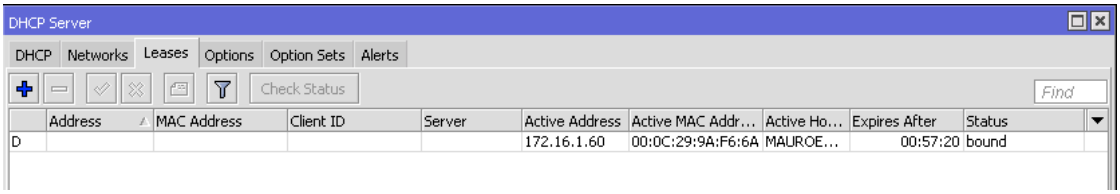


1. El alumno debe confirmar que ha recibido la dirección IP asignada por el router (DHCP Server). Debe verificar que se le ha asignado los diferentes parámetros: Dirección IP, Gateway, Subnet Mask, DNS, etc. Para esto debe ejecutar el comando `ipconfig` en su consola de DOS

```
C:\WINDOWS\system32>ipconfig /renew
Windows IP Configuration
Ethernet adapter Local Area Connection 1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.1.60
   Subnet Mask . . . . . . . . . . . : 255.255.255.192
   Default Gateway . . . . . . . . . : 172.16.1.1
```

2. Verificar que en el router se ha asignado la dirección IP a la laptop del estudiante



Tarea 4: Salida a internet

1. Luego de completar los pasos anteriores, el estudiante debe navegar en Internet

Lista de tareas a completar (Laboratorio 2-1)

El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1.1	Verificar que se asignó la dirección IP a la Ether2	
Tarea 1.2	Verificar que se creó el Pool de direcciones	
Tarea 1.3	Verificar que se creó el DHCP Server	
Tarea 1.4	Verificar que se creó el Network correspondiente	
Tarea 2	Verificar regla de NAT en router	
Tarea 3.1	Verificar que el alumno recibe la dirección IP	
Tarea 3.2	Verificar en el router que se ha asignado la dirección IP a la laptop	
Tarea 4	Verificar la navegación en Internet desde la Laptop	

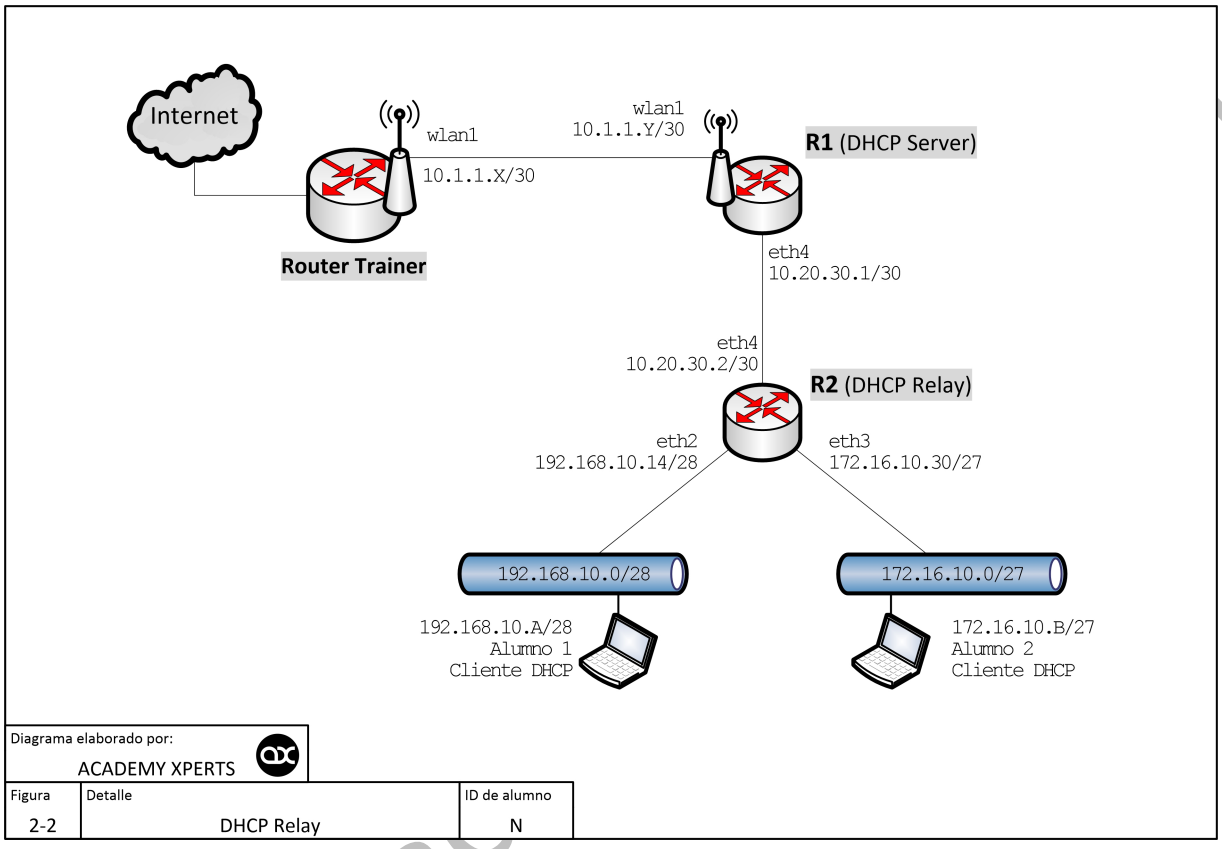
Laboratorio 2-2: DHCP Relay

Objetivo:

- Configurar un DHCP Relay para que entregue direcciones IP dinámicamente a los clientes DHCP a través de una red ruteada
- Los clientes DHCP deben poder navegar en Internet

Escenario:

- La Figura 2-2 (DHCP Relay) muestra la configuración que deberán conseguir cada uno de los estudiantes



Tarea 1: Configurar en R1 salida a Internet, DNS, reglas de NAT

1. El estudiante que tenga a su cargo la configuración de R1 deberá restaurar el back-up que se generó en el Laboratorio 0-1 (Laboratorio de Configuración Inicial).

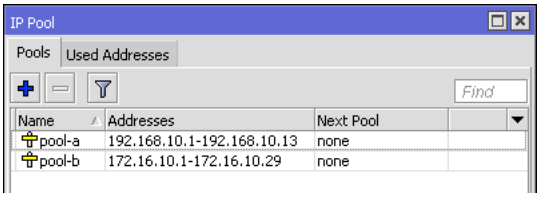
Tarea 2: Configurar en R1 parámetros de Pool, DHCP Server/Relay, Network y Rutas

1. Asignar dirección IP a Ether4

```
/ip address add address=10.20.30.1/30 interface=ether4
```

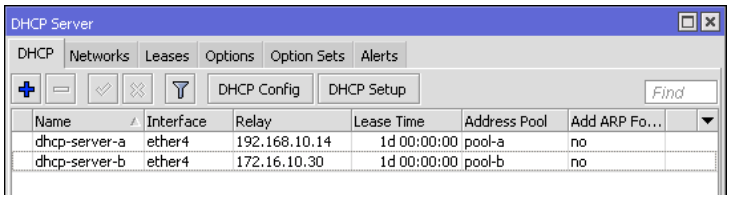
2. Crear los pool de direcciones (a y b) que serán usadas por el DHCP Server

```
/ip pool add name=pool-a ranges=192.168.10.1-192.168.10.13
/ip pool add name=pool-b ranges=172.16.10.1-172.16.10.29
```



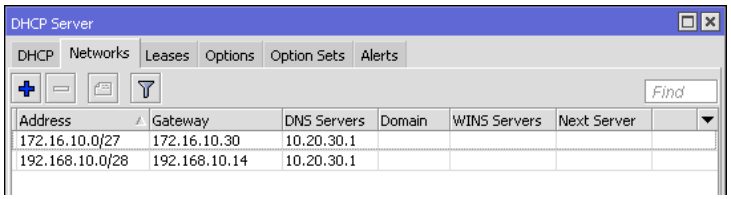
3. Crear los DHCP Server con las respectivas referencias al DHCP-Relay

```
/ip dhcp-server add name=dhcp-server-a interface=ether4 relay=192.168.10.14 lease-time=1d \
 address-pool=pool-a disabled=no
/ip dhcp-server add name=dhcp-server-b interface=ether4 relay=172.16.10.30 lease-time=1d \
 address-pool=pool-b disabled=no
```



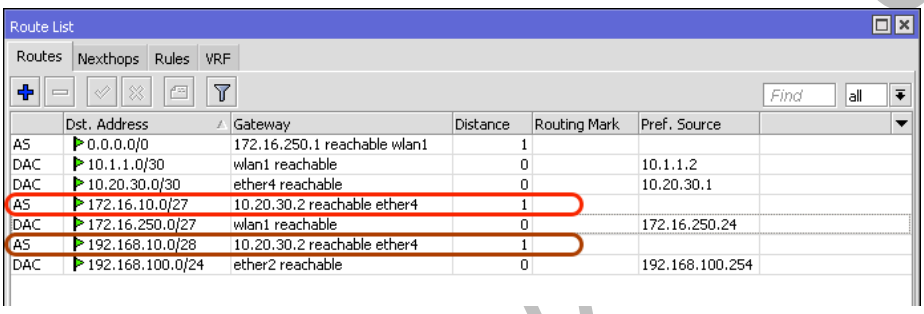
4. Crear los Network correspondientes

```
/ip dhcp-server network add address=192.168.10.0/28 gateway=192.168.10.14 dns-server=10.20.30.1
/ip dhcp-server network add address=172.16.10.0/27 gateway=172.16.10.30 dns-server=10.20.30.1
```



5. Crear las rutas hacia las redes remotas locales

```
/ip route add dst-address=192.168.10.0/28 gateway=10.20.30.2
/ip route add dst-address=172.16.10.0/27 gateway=10.20.30.2
```



Tarea 3: Configurar en R2 parámetros de Interfaces, DHCP Relay, y Rutas

1. Asignar dirección IP a Ether4

```
/ip address add address=10.20.30.2/30 interface=ether4
```

2. Asignar direcciones IP a Ether2 (red-a) y Ether3 (red-b)

```
/ip address add address=192.168.10.14/28 interface=ether2
/ip address add address=172.16.10.30/27 interface=ether3
```

3. Configurar el DHCP-Relay en R2

```
/ip dhcp-relay add name=relay-dhcp-a interface=ether2 dhcp-server=10.20.30.1 \
 local-address=192.168.10.14 disabled=no
/ip dhcp-relay add name=relay-dhcp-b interface=ether3 dhcp-server=10.20.30.1 \
 local-address=172.16.10.30 disabled=no
```

4. Configurar la ruta por default en R2

```
/ip route add dst-address=0.0.0.0/0 gateway=10.20.30.1
```

Tarea 4: Asignación dinámica de direcciones a clientes DHCP (laptops) a través de R2

1. Un estudiante debe conectarse a Ether2 y el otro a Ether3. Cada uno debe obtener automáticamente la dirección IP a la subred correspondiente. Finalmente ambos deben tener salida a Internet

Pregunta 2-2: Por qué es necesario configurar un DHCP-Relay para que un DHCP-Server pueda entregar direcciones a través de una red ruteada?

Lista de tareas a completar (Laboratorio 2-2)

El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1	Verificar que R1 tiene acceso a Internet y correctamente configuradas las reglas de DNS y NAT	
Tarea 2	Verificar las configuraciones de Pool, DHCP Server/Relay, Network y Rutas en R1	
Tarea 3	Verificar las configuraciones de Interfaces, DHCP Relay, y Rutas en R2	
Tarea 4	Verificar la asignación dinámicas a ambos estudiantes, y la salida a Internet de cada uno	
Tarea 5	Responder Pregunta 2-2	

Capítulo 4: Firewall Filter – Chain Input

/ip firewall filter

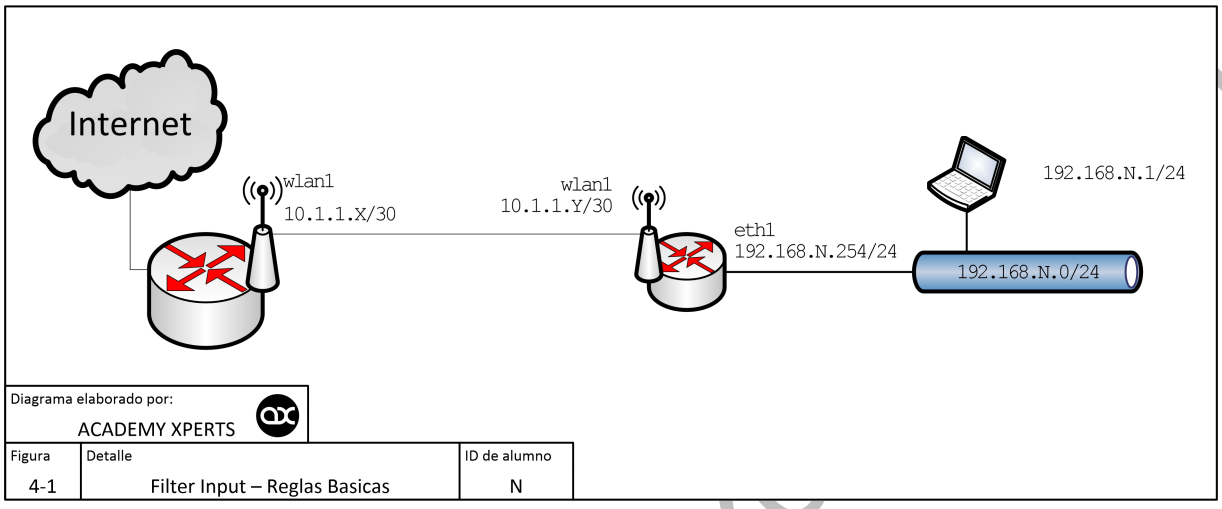
Laboratorio 4-1: Filter Input – Reglas Básicas

Objetivo:

- Configurar las 4 reglas básicas de Firewall INPUT

Escenario:

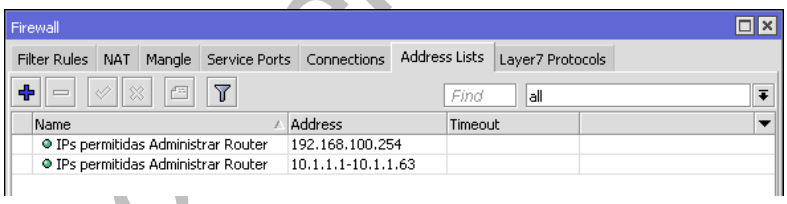
- La Figura 4-1 (Filter Input – Reglas Básicas) muestra la configuración que deberán conseguir cada uno de los estudiantes



Tarea 1: Reglas Básicas de Filter Input

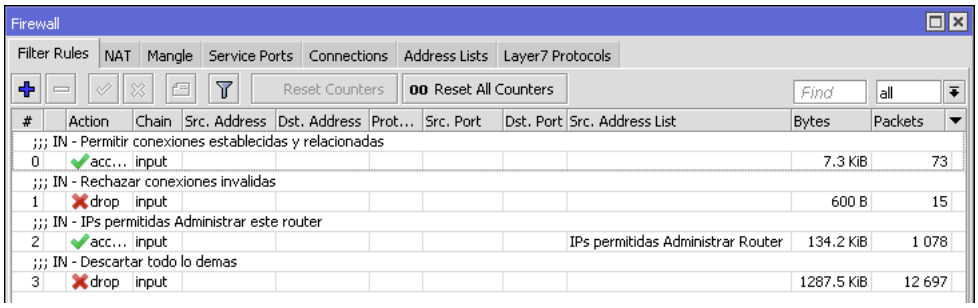
1. Cada estudiante debe crear un `address-list` donde debe especificar las direcciones IP que estarán permitidas que administren su router. En el caso de este ejercicio las direcciones serán: la IP de su laptop (la IP del comando a continuación es solo un ejemplo), y la red WAN Wireless

```
/ip firewall address-list
add address=192.168.100.254 list="IPs permitidas Administrar Router"
add address=10.1.1.1-10.1.1.63 list="IPs permitidas Administrar Router"
```



2. Crear las 4 reglas básicas en INPUT

```
/ip firewall filter
add chain=input comment="IN - Permitir conexiones establecidas y relacionadas" connection-
state=\
    established,related
add action=drop chain=input comment="IN - Rechazar conexiones invalidas" connection-
state=invalid
add chain=input comment="IN - IPs permitidas Administrar este router" src-address-list=\
    "IPs permitidas Administrar Router"
add action=drop chain=input comment="IN - Descartar todo lo demas"
```



Tarea 2: Pruebas de validación de reglas

1. Cada estudiante debe poder ingresar vía Winbox al router de su vecino. Caso contrario el vecino debe validar su `address-list`

2. El estudiante debe cambiar la dirección IP de su laptop y probar el acceso a su propio router. Puesto que la nueva IP no está definida en el `address-list` no debe poder ingresar

Tarea 3: Acceso vía por Capa 2

1. Puesto que en la Tarea 2.2 no se puede ingresar, el estudiante debe tratar de ingresar por Capa 2
2. Abrir un Winbox y verificar si puede visualizar la `MAC` de la interface del rute a la cual está conectado
3. Escribir la `MAC-address` de la interface del router e intentar ingresar

Pregunta 4-1.1: Por qué en la Tarea 3 no apareció la dirección MAC del router?

Pregunta 4-1.2: Por qué se puede ingresar por Capa 2?

Lista de tareas a completar (Laboratorio 4-1)

El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1.1	Verificar creación del address-list y asignación de IPs correspondientes	
Tarea 1.2	Verificar creación de 4 reglas básicas de INPUT	
Tarea 2.1	Prueba de acceso Winbox a routers de vecinos	
Tarea 2.2	Cambio de IP en Laptop y verificación de restricción	
Tarea 3	Comprobar el acceso por Capa 2	
Tarea 4.1	Responder Pregunta 4-1.1	
Tarea 4.2	Responder Pregunta 4-1.2	

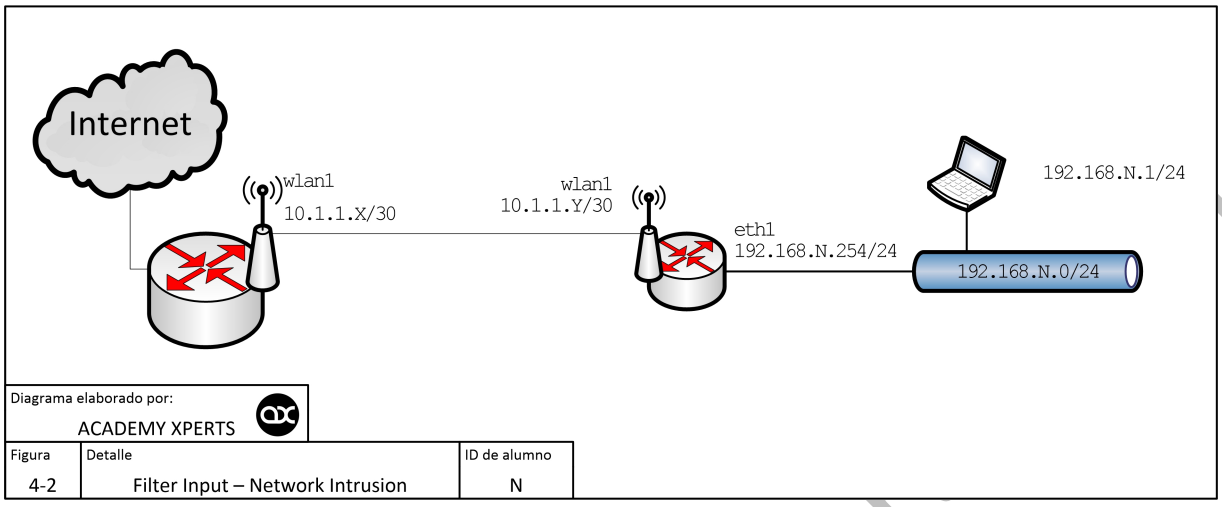
Laboratorio 4-2: Filter Input – Network Intrusion

Objetivo:

- Configurar las reglas fundamentales para proteger al router de las Intrusiones de Red más conocidas

Escenario:

- La Figura 4-2 (Filter Input – Network Intrusion) muestra la configuración que se debe seguir



Tarea 1: Protección contra el Port Scan (escaneo de puertos)

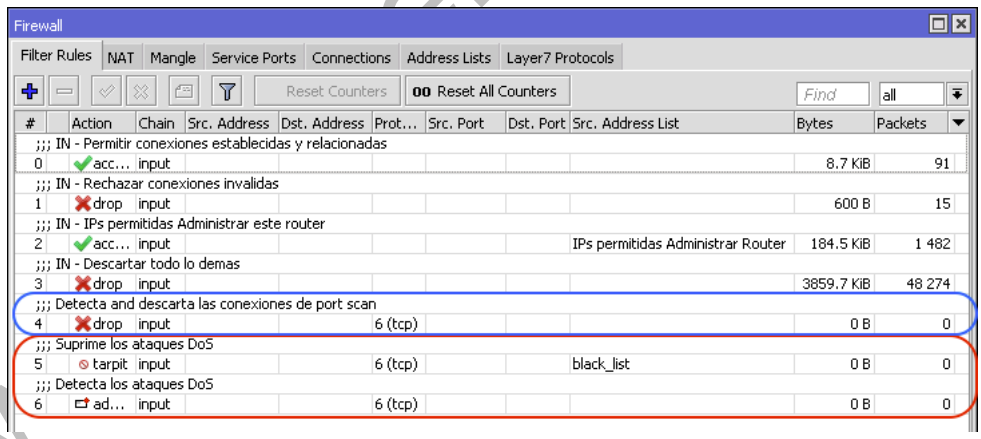
1. Se debe crear la regla

```
/ip firewall filter
add chain=input protocol=tcp psd=10,3s,3,1 action=drop \
comment="Detecta and descarta las conexiones de port scan" disabled=no
```

Tarea 2: Protección contra el DoS (Denial of Service)

1. Se deben crear las reglas

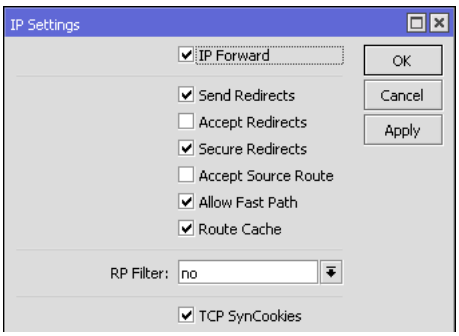
```
/ip firewall filter
add chain=input protocol=tcp connection-limit=3,32 src-address-list=black_list \
action=tarpit comment="Suprime los ataques DoS" disabled=no
add chain=input protocol=tcp connection-limit=10,32 action= add-src-to-address-list \
address-list=black_list address-list-timeout=1d comment="Detecta los ataques DoS" disabled=no
```



Tarea 3: Protección contra el DDoS (Distributed Denial of Service)

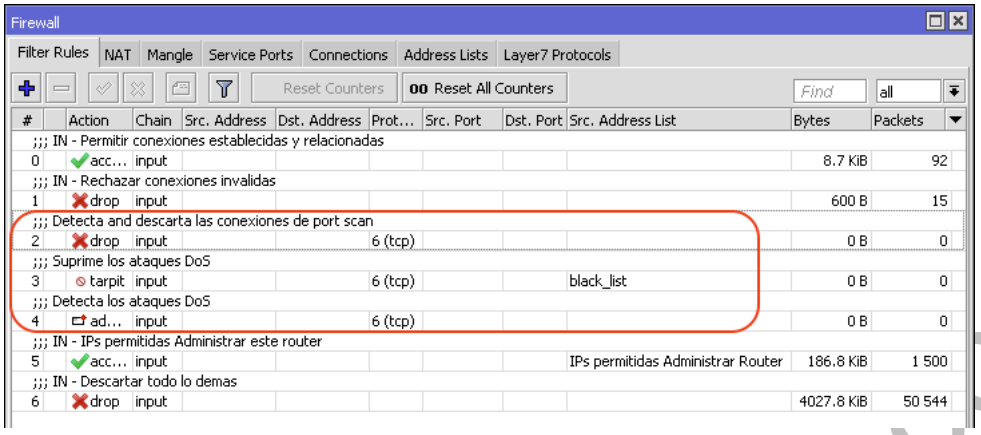
1. Se debe crear la regla

```
/ip settings set tcp-syncookies=yes
```



Tarea 4: Reubicación adecuada de las reglas de Network Intrusion

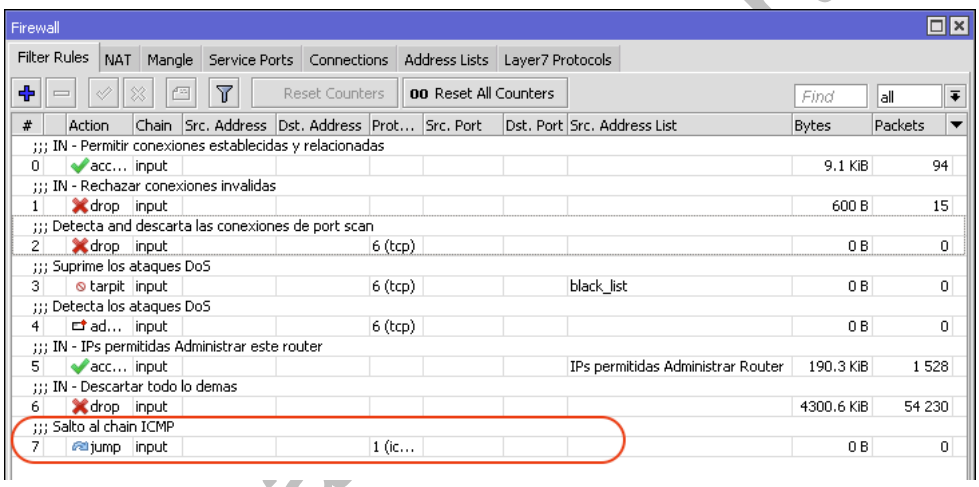
1. Se debe ubicar adecuadamente las reglas. Se sugiere que las mismas estén antes de la regla que acepta las IPs que pueden administrar el router. De esta forma se previene que cualquiera de los equipos que tenga acceso al router, pudiera estar infectado y de esta forma comprometer la integridad del dispositivo.



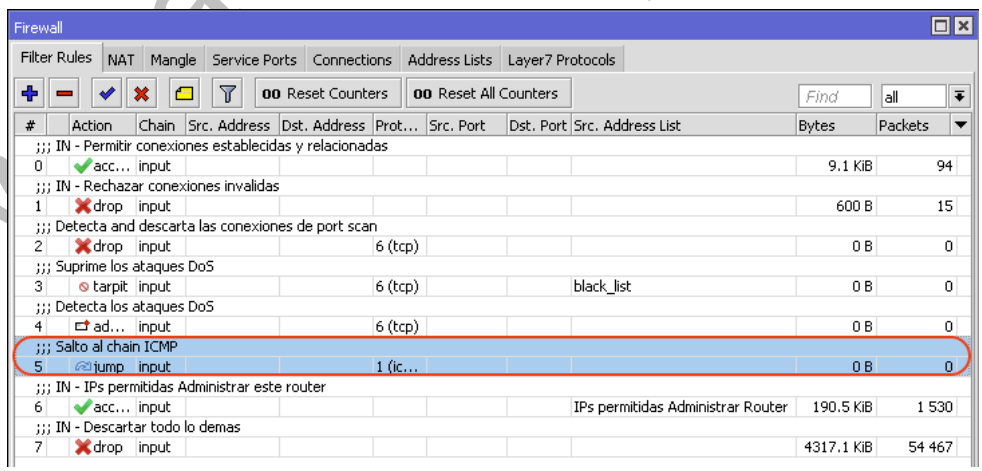
Tarea 5: Protección contra el Ping Flooding (Inundación de Paquetes ICMP)

1. Se debe crear una regla de jump para generar un chain personalizado

```
/ip firewall filter
add chain=input protocol=icmp action=jump jump-target=ICMP \
comment="Salto al chain ICMP" disabled=no
```



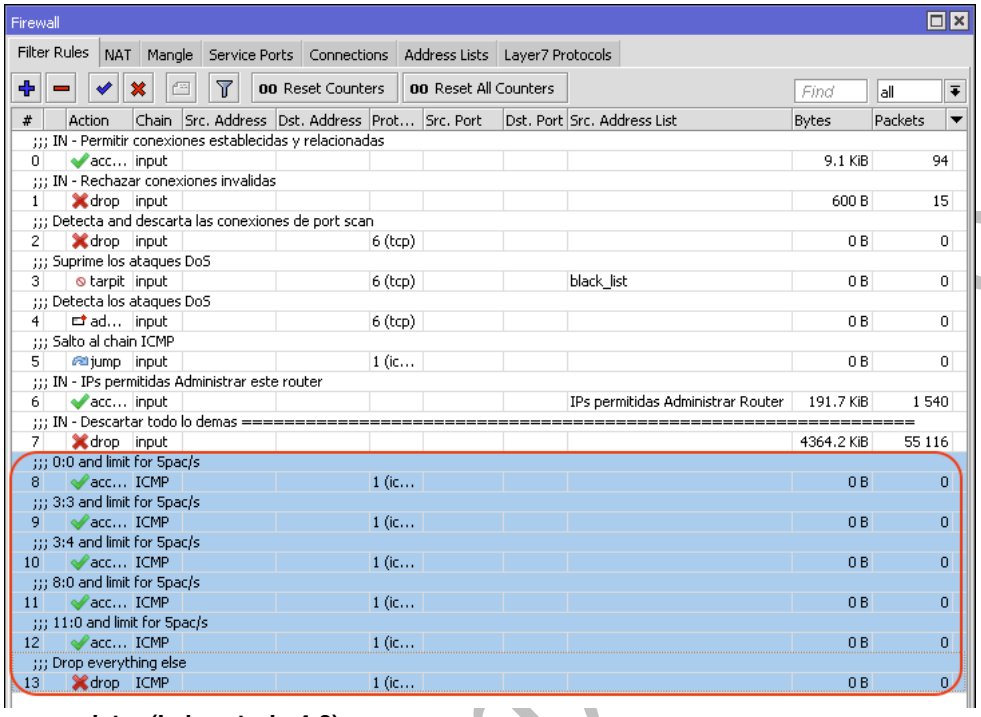
2. Se debe ubicar adecuadamente esta regla. Se sugiere que la mismas esté antes de la regla que acepta las IPs que pueden administrar el router. De esta forma se previene que cualquiera de los equipos que tenga acceso al router, pudiera estar infectado y de esta forma comprometer la integridad del dispositivo.



3. Se deben crear las reglas de control de mensajería ICMP. Estas reglas pueden quedar ubicadas al final de todas las reglas ya que serán llamadas cuando se invoque el chain ICMP.

```
/ip firewall filter
add chain=ICMP protocol=icmp icmp-options=0:0-255 limit=5,5 action=accept \
comment="0:0 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp icmp-options=3:3 limit=5,5 action=accept \
```

```
comment="3:3 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp icmp-options=3:4 limit=5,5 action=accept \
comment="3:4 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp icmp-options=8:0-255 limit=5,5 action=accept \
comment="8:0 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp icmp-options=11:0-255 limit=5,5 action=accept \
comment="11:0 and limit for 5pac/s" disabled=no
add chain=ICMP protocol=icmp action=drop comment="Drop everything else" disabled=no
```



Lista de tareas a completar (Laboratorio 4-2)

El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1	Verificar creación reglas contra Port Scan	
Tarea 2	Verificar creación reglas contra DoS	
Tarea 3	Verificar creación regla contra DDoS	
Tarea 4	Reubicación de las reglas creadas en las tareas 1, 2 y 3	
Tarea 5	Verificar creación regla de salto a ICMP y reglas contra Ping Flooding	

Capítulo 5: Firewall Filter – Chain Forward

/ip firewall filter

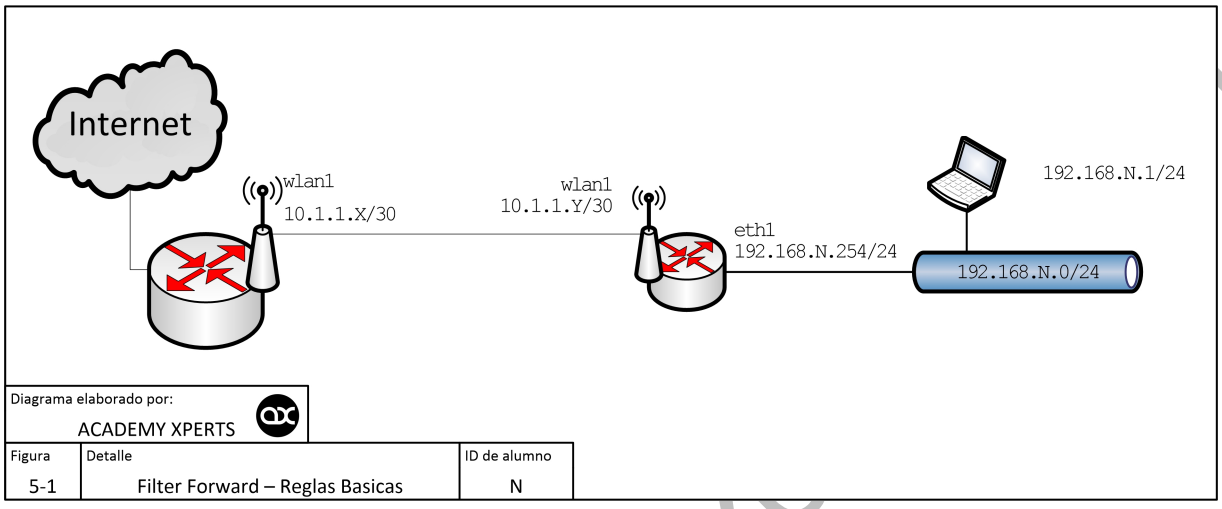
Laboratorio 5-1: Filter Forward – Reglas Básicas

Objetivo:

- Configurar las 4 reglas básicas de Firewall FORWARD

Escenario:

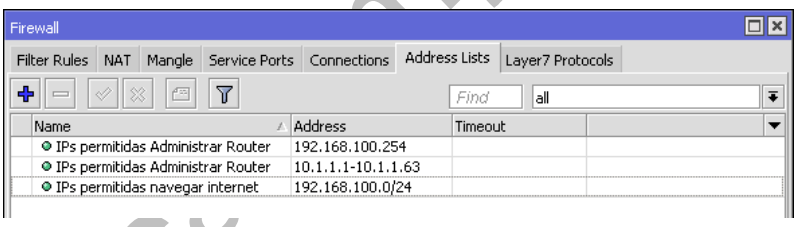
- La Figura 5-1 (Filter Forward – Reglas Básicas) muestra la configuración que deberán conseguir cada uno de los estudiantes



Tarea 1: Reglas Básicas de Filter Forward

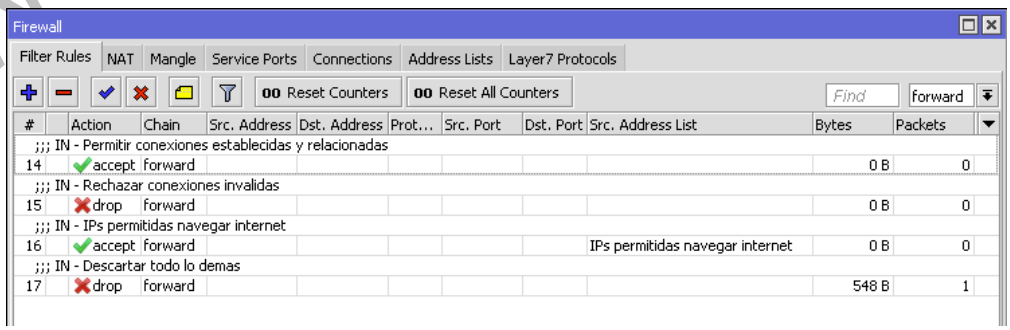
1. Cada estudiante debe crear un `address-list` donde debe especificar las direcciones IP que estarán permitidas navegar a Internet. En el caso de este ejercicio las direcciones serán el segmento de la red LAN (local)

```
/ip firewall address-list
add address=192.168.100.0/24 list="IPs permitidas navegar internet"
```



2. Crear las 4 reglas básicas en FORWARD

```
/ip firewall filter
add chain=forward comment="IN - Permitir conexiones establecidas y relacionadas" connection-
state=\
    established,related
add action=drop chain=forward comment="IN - Rechazar conexiones invalidas" connection-
state=invalid
add chain=forward comment="IN - IPs permitidas navegar internet" src-address-list=\
    "IPs permitidas navegar internet"
add action=drop chain=forward comment="IN - Descartar todo lo demas"
```



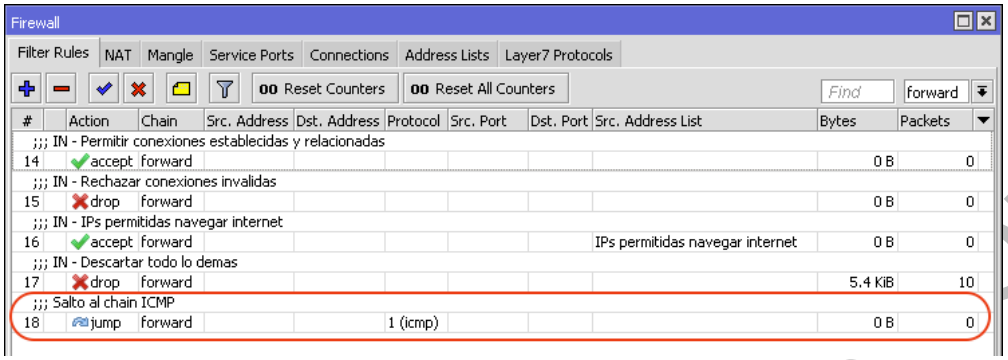
Tarea 2: Pruebas de validación de reglas

1. Cada estudiante debe poder navegar a Internet. Caso contrario debe revisar su `address-list`

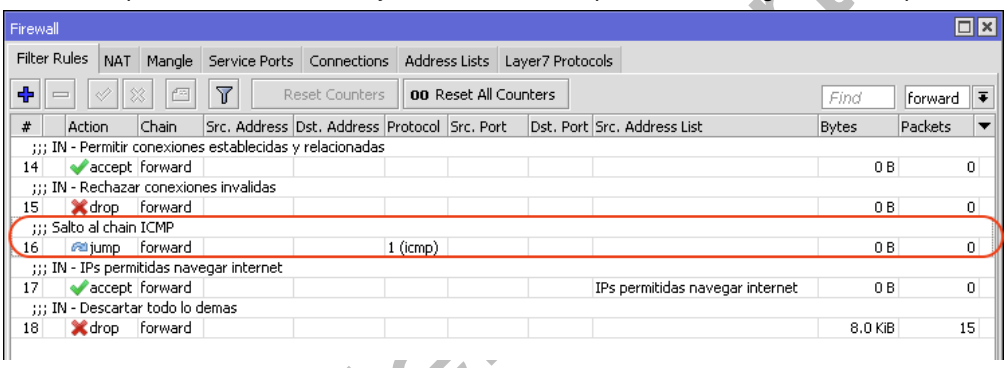
Tarea 3: Salto a control ICMP

1. Se aprovechará las definiciones de control de mensajería ICMP que se generaron en la Tarea 5.3 del Laboratorio 4-2. Para esto se debe crear una regla de jump para saltar al chain personalizado ICMP

```
/ip firewall filter
add chain=forward protocol=icmp action=jump jump-target=ICMP \
comment="Salto al chain ICMP" disabled=no
```



2. Se debe ubicar adecuadamente esta regla. Se sugiere que la mismas esté antes de la regla que acepta las IPs que tienen permitido el acceso a Internet. De esta forma se previene que cualquiera de los equipos que tenga acceso al router, pudiera estar infectado y de esta forma comprometer la integridad del dispositivo.



Lista de tareas a completar (Laboratorio 5-1)

El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1.1	Verificar creación del address-list y asignación de IPs correspondientes	
Tarea 1.2	Verificar creación de 4 reglas básicas de INPUT	
Tarea 2	Prueba de salida a internet	
Tarea 3	Verificar creación regla de salto a ICMP y correcta reubicación	

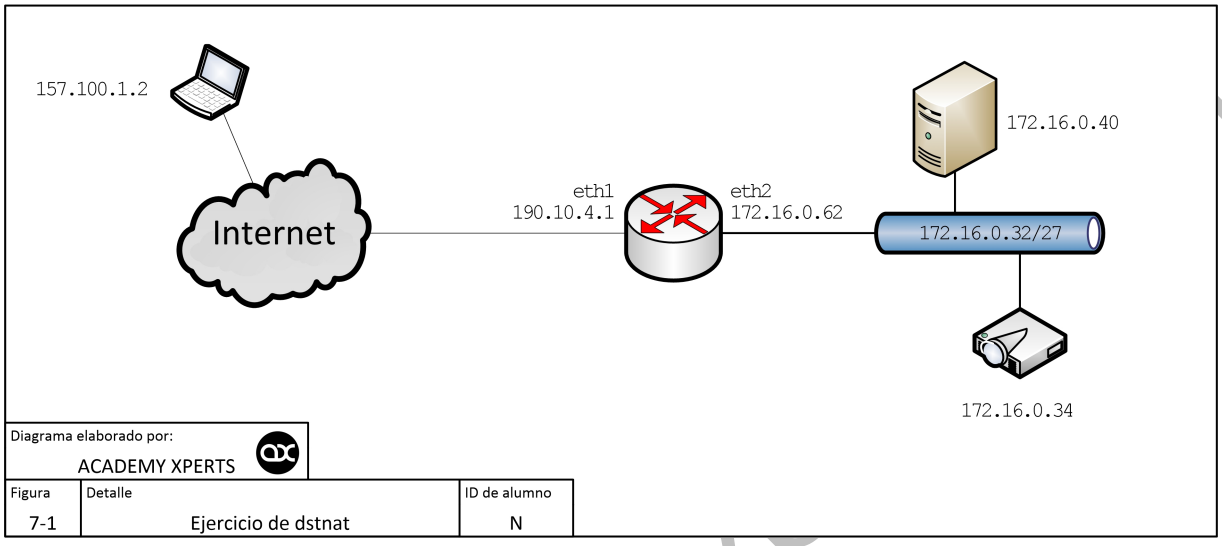
Laboratorio 7-1: Ejercicio de dstnat

Objetivo:

- El estudiante debe comprender el funcionamiento del firewall basado en el Diagrama de Flujo

Escenario:

La Figura 7-1 (Ejercicio de dstnat) muestra la disposición de los dispositivos para la pregunta a continuación



Tema:

- Según el diagrama de la Figura 7-1, existe una cámara IP (`172.16.0.34`) y un Servidor Web (`172.16.0.40`) en la red LAN
- El router tiene configuradas la regla de NAT (srcnat) correspondiente para realizar el enmascaramiento y los dispositivos de la LAN pueden navegar sin problemas en Internet

Pregunta 7-1.1:

Cuáles de las siguientes sentencias son correctas para que se pueda ejecutar correctamente el enmascaramiento y los dispositivos de LAN puedan salir a internet? Asuma que todas las reglas son generadas en `/ip firewall nat`

a) `add action=masquerade chain=srcnat out-interface=ether1 src-address=172.16.0.0/27`
b) `add action=masquerade chain=srcnat in-interface=ether2 out-interface=ether1 src-address=172.16.0.32/27`
c) `add action=masquerade chain=srcnat out-interface=ether1 src-address=172.16.0.32/27`
d) `add action=masquerade chain=dstnat out-interface=ether1 src-address=172.16.0.32/27`
e) `add action=src-nat chain=srcnat out-interface=ether1 src-address=172.16.0.32/27 to-address=190.10.4.1`
f) `add action=masquerade chain=srcnat out-interface=ether1`
g) `add action=masquerade chain=srcnat out-interface=ether1 src-address=0.0.0.0`
h) `add action=masquerade chain=srcnat out-interface=ether1 src-address=0.0.0.0/0`
i) `add action=masquerade chain=srcnat out-interface=ether1 src-address=255.255.255.255`

Pregunta 7-1.2: Se puede utilizar in-interface cuando action=srcnat?

Pregunta 7-1.3:

Se desea bloquear específicamente el tráfico http hacia el Web Server (172.16.0.40) que proviene de 157.100.1.2

Cual de las siguientes sentencias identificaría a la regla que se debe armar?

a) `src-address=172.16.0.0/27, dst-address=172.16.0.40`
b) `src-address=190.10.4.1, dst-address=172.16.0.40`
c) `src-address=190.10.4.1, dst-address=157.100.1.2`
d) `src-address=172.16.0.40, dst-address=157.100.1.2`
e) `src-address=157.100.1.2, dst-address=172.16.0.40`
f) `src-address=157.100.1.2, dst-address=190.10.4.1`

Pregunta 7-1.4:

En la pregunta 7-1.3 que chain se debe utilizar en `/ip firewall filter` para poner limitantes al tráfico? Por qué?

a) `Input`
b) `Output`
c) `Forward`

Lista de tareas a completar (Laboratorio 7-1)
El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1	Responder Pregunta 7-1.1	
Tarea 2	Responder Pregunta 7-1.2	
Tarea 3	Responder Pregunta 7-1.3	
Tarea 4	Responder Pregunta 7-1.4	

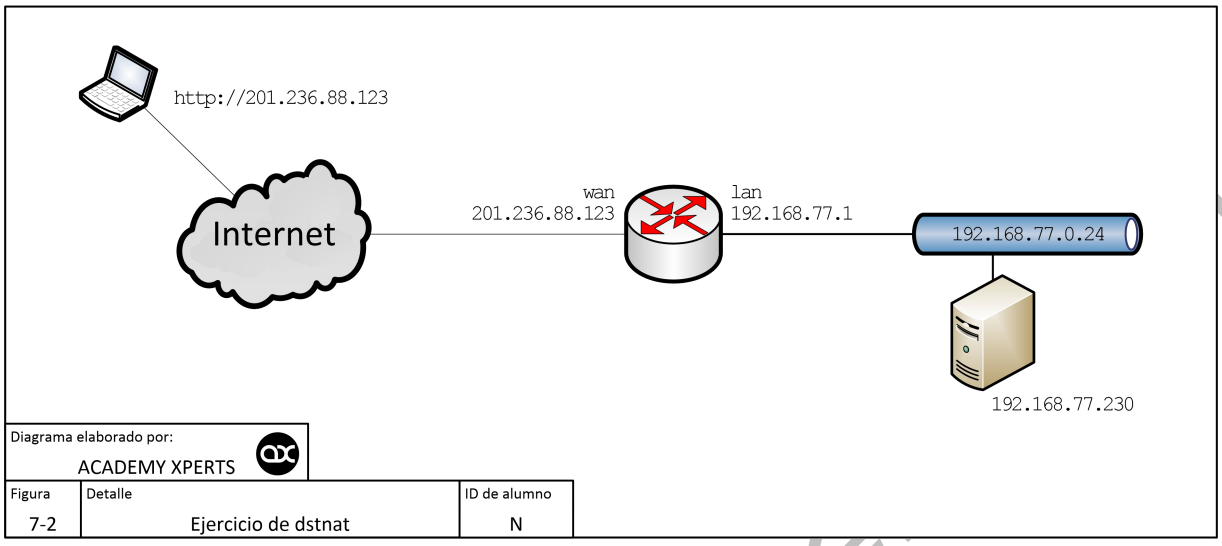
Laboratorio 7-2: Ejercicio de dstnat

Objetivo:

- El estudiante debe comprender el funcionamiento del firewall basado en el Diagrama de Flujo

Escenario:

La Figura 7-2 (Ejercicio de dstnat) muestra la disposición de los dispositivos para la pregunta a continuación



Tema:

Se tiene un servidor web correctamente configurado dentro de la red LAN. La dirección IP del servidor es `192.168.77.230/24` y su gateway (puerta de enlace) es `192.168.77.1`. El router tiene la siguiente dirección IP en la interface wan: `201.236.88.123`, la cual se puede alcanzar desde internet.

El router tiene la siguiente configuración en el firewall:

```
/ip firewall filter
add chain=input connection-state=established action=accept
add chain=input protocol=tcp dst-port=80 action=accept
add chain=input action=drop
add chain=forward connection-state=established action=accept
add chain=forward in-interface=lan action=accept
add chain=forward action=drop

/ip firewall nat
add action=masquerade chain=srcnat out-interface=wan
add action=dst-nat chain=dstnat dst-port=80 in-interface=wan protocol=tcp to-addresses=192.168.77.230 to-
ports=80
```

Pregunta 7-2.1:

Si se coloca en el navegador web del equipo que está en Internet la siguiente dirección `http://201.236.88.123`, ¿cuál página deberá abrir?

a) Página web del RouterOS
b) Página web de MikroTik (*www.mikrotik.com)*
c) Página web del servidor interno
d) Ninguna

Lista de tareas a completar (Laboratorio 7-2)

El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1	Responder Pregunta 7-2.1	

Capítulo 8: Firewall Mangle

connection-mark & packet-mark

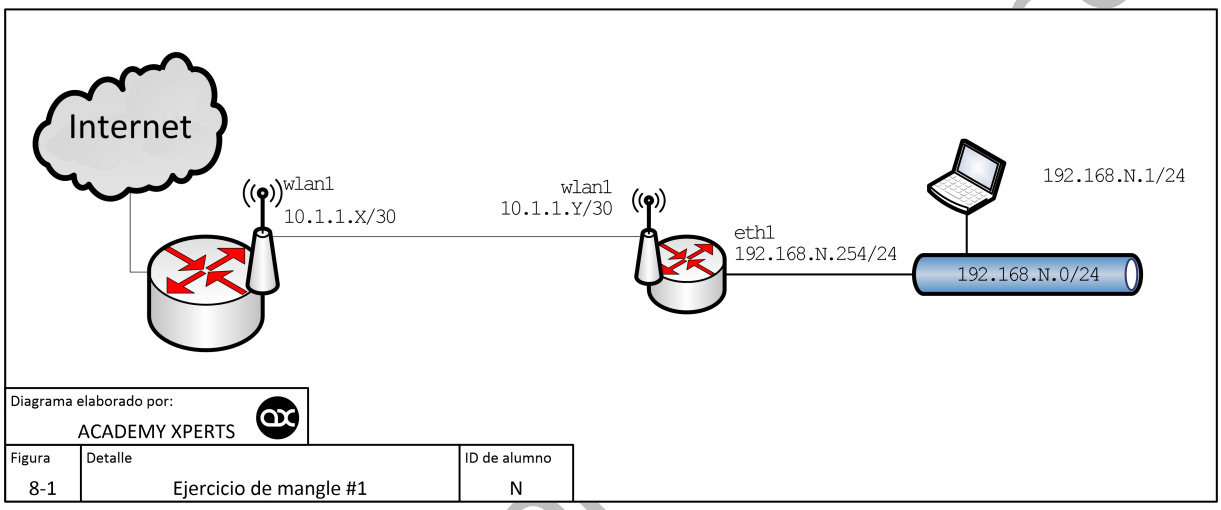
Laboratorio 8-1: Ejercicio de mangle #1

Objetivo:

- Configurar las reglas de mangle (conexión y paquetes) para realizar QoS
- Este grupo de reglas se realizará por cada servicio, aprovechando cada marca de paquete la marca de conexión previa
- Los servicios sobre los que se desea hacer `connection-mark` y `packet-mark` son los siguientes:
  - Mail (TCP: POP 110, POP SSL 995, IMAP 143, IMAP SSL 993, SMTP 25, 465, 587)
  - VoIP (UDP: 10000 al 20000)
  - http/https (80, 443)
  - P2P
  - Resto del tráfico

Escenario:

La Figura 8-1 (Ejercicio de mangle #1) muestra la disposición de los dispositivos para la pregunta a continuación



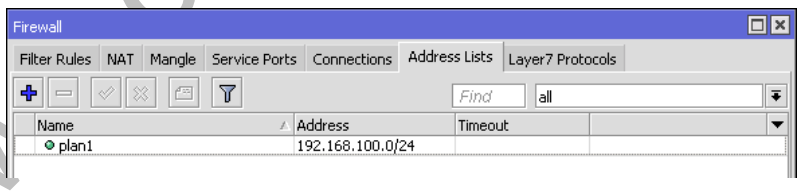
Tarea 1: Restaurar el back-up inicial

1. El estudiante debe restaurar el back-up que se generó en el Laboratorio 0-1 (Laboratorio de Configuración Inicial).

Tarea 2: Crear un address-list para este ejercicio

1. Cada estudiante debe crear un `address-list` donde debe especificar las direcciones IP que estarán permitidas navegar a Internet. En el caso de este ejercicio las direcciones serán el segmento de la red LAN (local)

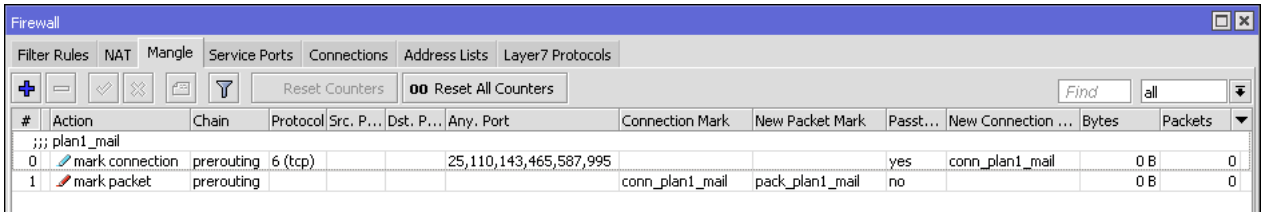
```
/ip firewall address-list
add address=192.168.100.0/24 list="plan1"
```



Tarea 3: Marcas de conexión & paquetes para tráfico Mail

1. Primero realizar la marca de conexión y luego la marca de paquete basado en la marca de conexión anterior

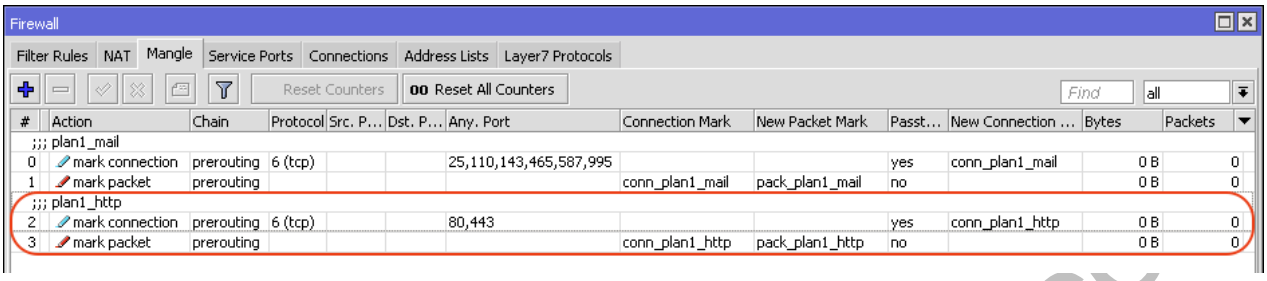
```
/ip firewall mangle
add action=mark-connection chain=prerouting comment=plan1_mail new-connection-mark=conn_plan1_mail port=\
    25,110,143,465,587,995 protocol=tcp src-address-list=plan1
add action=mark-packet chain=prerouting connection-mark=conn_plan1_mail new-packet-mark=pack_plan1_mail \
    passthrough=no
```



Tarea 4: Marcas de conexión & paquetes para tráfico http/https

1. Primero realizar la marca de conexión y luego la marca de paquete basado en la marca de conexión anterior

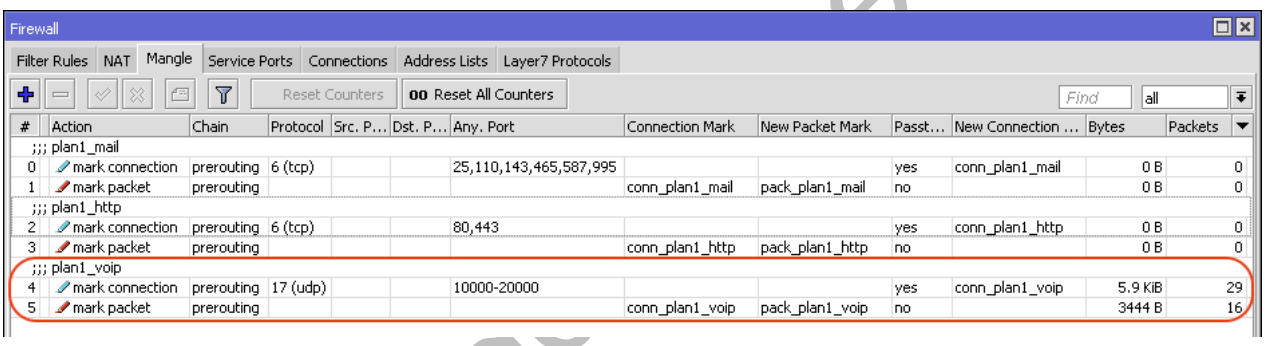
```
/ip firewall mangle
add action=mark-connection chain=prerouting comment=plan1_http new-connection-mark=conn_plan1_http port=\
    80,443 protocol=tcp src-address-list=plan1
add action=mark-packet chain=prerouting connection-mark=conn_plan1_http new-packet-mark=pack_plan1_http \
    passthrough=no
```



Tarea 5: Marcas de conexión & paquetes para tráfico VoIP

1. Primero realizar la marca de conexión y luego la marca de paquete basado en la marca de conexión anterior

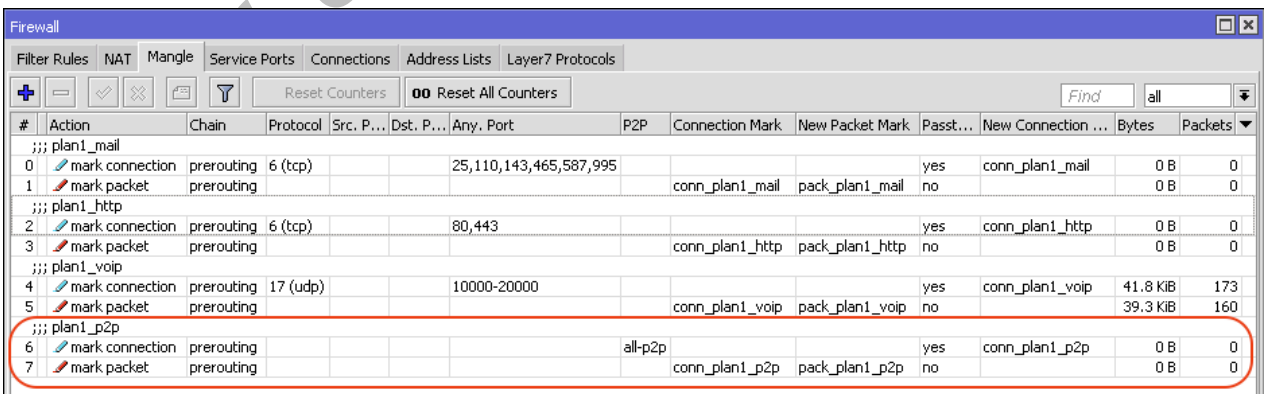
```
/ip firewall mangle
add action=mark-connection chain=prerouting comment=plan1_voip new-connection-mark=conn_plan1_voip port=\
    10000-20000 protocol=udp
add action=mark-packet chain=prerouting connection-mark=conn_plan1_voip new-packet-mark=pack_plan1_voip \
    passthrough=no
```



Tarea 6: Marcas de conexión & paquetes para tráfico P2P

1. Primero realizar la marca de conexión y luego la marca de paquete basado en la marca de conexión anterior

```
/ip firewall mangle
add action=mark-connection chain=prerouting comment=plan1_p2p new-connection-mark=conn_plan1_p2p p2p=\
    all-p2p src-address-list=plan1
add action=mark-packet chain=prerouting connection-mark=conn_plan1_p2p new-packet-mark=pack_plan1_p2p \
    passthrough=no
```

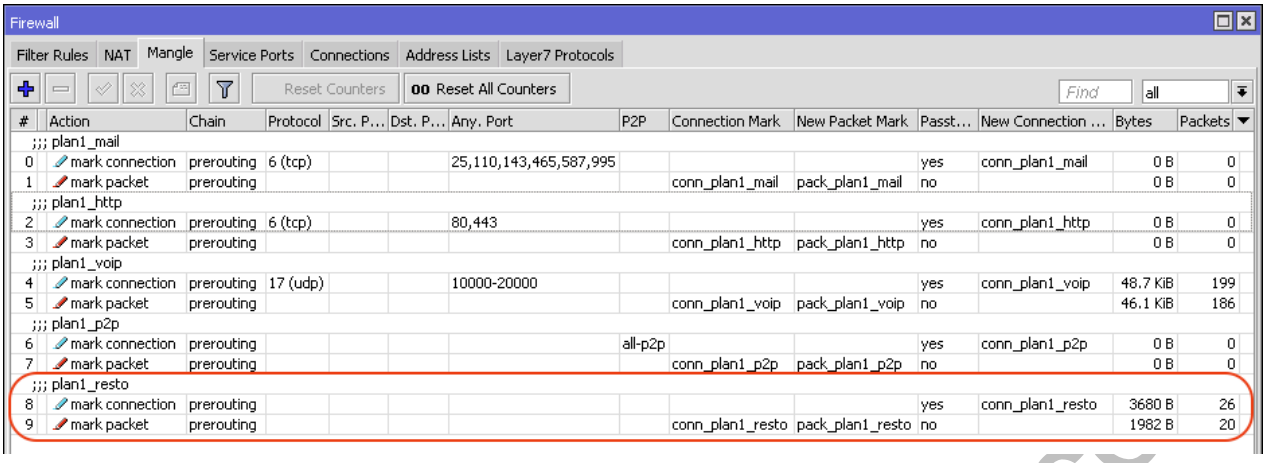


Tarea 7: Marcas de conexión & paquetes para tráfico Resto (restante)

1. Primero realizar la marca de conexión y luego la marca de paquete basado en la marca de conexión anterior

```
/ip firewall mangle
add action=mark-connection chain=prerouting comment=plan1_resto new-connection-mark=conn_plan1_resto \
    src-address-list=plan1
```

```
add action=mark-packet chain=prerouting connection-mark=conn_plan1_resto new-packet-mark=pack_plan1_resto \
    passthrough=no
```



#	Action	Chain	Protocol	Src. P...	Dst. P...	Any. Port	P2P	Connection Mark	New Packet Mark	Passt...	New Connection ...	Bytes	Packets
;;; plan1_mail													
0	mark connection	prerouting	6 (tcp)			25,110,143,465,587,995				yes	conn_plan1_mail	0 B	0
1	mark packet	prerouting						conn_plan1_mail	pack_plan1_mail	no		0 B	0
;;; plan1_http													
2	mark connection	prerouting	6 (tcp)			80,443				yes	conn_plan1_http	0 B	0
3	mark packet	prerouting						conn_plan1_http	pack_plan1_http	no		0 B	0
;;; plan1_voip													
4	mark connection	prerouting	17 (udp)			10000-20000				yes	conn_plan1_voip	48.7 KiB	199
5	mark packet	prerouting						conn_plan1_voip	pack_plan1_voip	no		46.1 KiB	186
;;; plan1_p2p													
6	mark connection	prerouting					all-p2p			yes	conn_plan1_p2p	0 B	0
7	mark packet	prerouting						conn_plan1_p2p	pack_plan1_p2p	no		0 B	0
;;; plan1_resto													
8	mark connection	prerouting								yes	conn_plan1_resto	3680 B	26
9	mark packet	prerouting						conn_plan1_resto	pack_plan1_resto	no		1982 B	20

Lista de tareas a completar (Laboratorio 8-1)
El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1	Verificar que se ha restaurado el backup del Laboratorio 0-1 y que se tiene salida a Internet	
Tarea 2	Verificar la creación del address-list	
Tarea 3	Verificar las marcas de conexión & paquetes para tráfico Mail	
Tarea 4	Verificar las marcas de conexión & paquetes para tráfico http/https	
Tarea 5	Verificar las marcas de conexión & paquetes para tráfico VoIP	
Tarea 6	Verificar las marcas de conexión & paquetes para tráfico P2P	
Tarea 7	Verificar las marcas de conexión & paquetes para tráfico Resto (restante)	

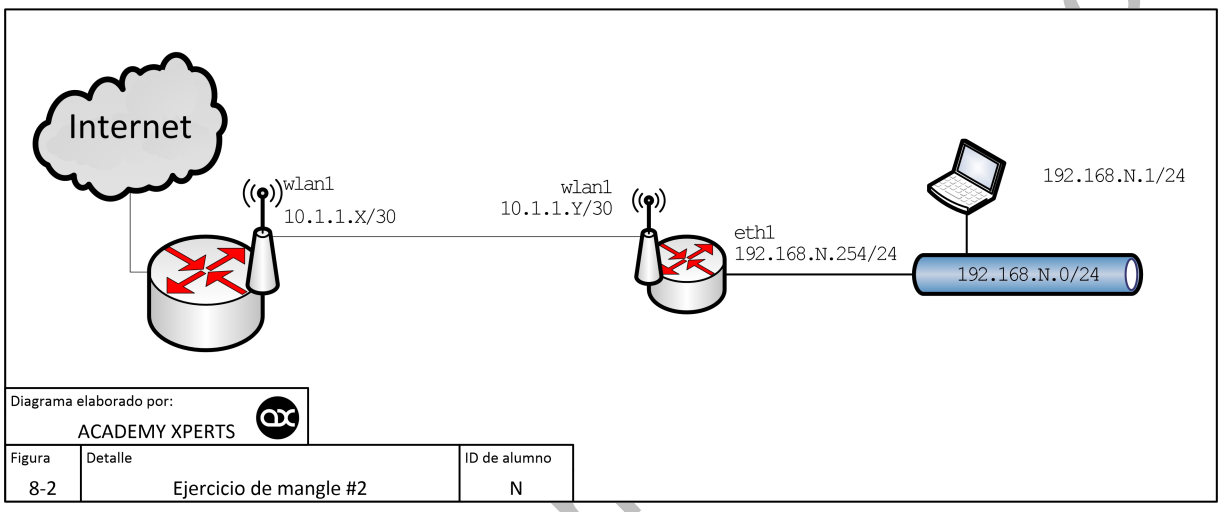
Laboratorio 8-2: Ejercicio de mangle #2

Objetivo:

- Configurar las reglas de mangle (conexión y paquetes) para realizar QoS
- Este grupo de reglas se realizará haciendo una sola marca de conexión. Las demás reglas de marcado de paquetes se armarán basados en la marca de conexión principal
- Se utilizará el mismo `address-list` del Laboratorio 8-1
- Los servicios sobre los que se desea hacer `connection-mark` y `packet-mark` son los siguientes:
    - Mail (TCP: POP 110, POP SSL 995, IMAP 143, IMAP SSL 993, SMTP 25, 465, 587)
    - VoIP (UDP: 10000 al 20000)
    - http/https (80, 443)
    - P2P
    - Resto del tráfico

Escenario:

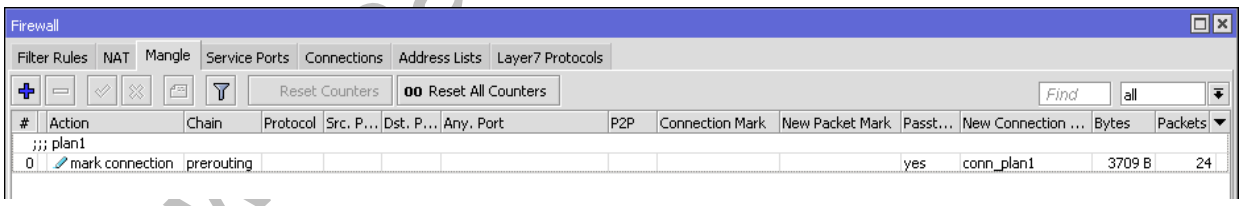
La Figura 8-2 (Ejercicio de mangle #2) muestra la disposición de los dispositivos para la pregunta a continuación



Tarea 1: Marcas de conexión general

1. Primero realizar la marca de conexión cuyo único filtro será el `src-address-list=plan1`

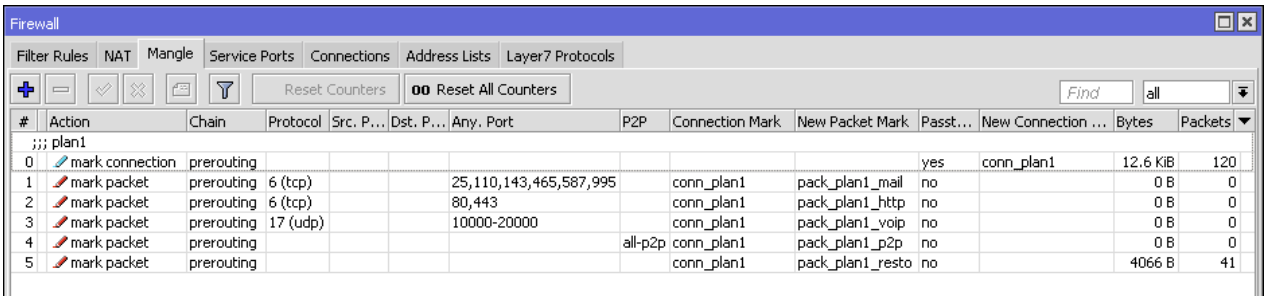
```
/ip firewall mangle
add action=mark-connection chain=prerouting comment=plan1 new-connection-mark=conn_plan1 \
    src-address-list=plan1
```



Tarea 2: Marcas de conexión & paquetes para los demás servicios

1. Las marcas de paquete se realizarán basadas en la marca de conexión general (con_plan1)

```
/ip firewall mangle
add action=mark-packet chain=prerouting connection-mark=conn_plan1 new-packet-mark=pack_plan1_mail \
    passthrough=no port=25,110,143,465,587,995 protocol=tcp
add action=mark-packet chain=prerouting connection-mark=conn_plan1 new-packet-mark=pack_plan1_http \
    passthrough=no port=80,443 protocol=tcp
add action=mark-packet chain=prerouting connection-mark=conn_plan1 new-packet-mark=pack_plan1_voip \
    passthrough=no port=10000-20000 protocol=udp
add action=mark-packet chain=prerouting connection-mark=conn_plan1 new-packet-mark=pack_plan1_p2p p2p=\
    all-p2p passthrough=no
add action=mark-packet chain=prerouting connection-mark=conn_plan1 new-packet-mark=pack_plan1_resto \
    passthrough=no
```



#	Action	Chain	Protocol	Src. P...	Dst. P...	Any. Port	P2P	Connection Mark	New Packet Mark	Passt...	New Connection ...	Bytes	Packets
;;; plan1													
0	mark connection	prerouting								yes	conn_plan1	12.6 KiB	120
1	mark packet	prerouting	6 (tcp)			25,110,143,465,587,995		conn_plan1	pack_plan1_mail	no		0 B	0
2	mark packet	prerouting	6 (tcp)			80,443		conn_plan1	pack_plan1_http	no		0 B	0
3	mark packet	prerouting	17 (udp)			10000-20000		conn_plan1	pack_plan1_voip	no		0 B	0
4	mark packet	prerouting					all-p2p	conn_plan1	pack_plan1_p2p	no		0 B	0
5	mark packet	prerouting						conn_plan1	pack_plan1_resto	no		4066 B	41

Lista de tareas a completar (Laboratorio 8-2)
El estudiante debe verificar que se han cumplido los siguientes pasos para confirmar el seguimiento correcto a este laboratorio.

	Marque con √ los pasos que ha podido completar	√
Tarea 1	Verificar la marca de conexión general basado en el address-list del Laboratorio 8-1	
Tarea 2	Verificar las marcas de paquetes para los servicios de mail, http/https, VoIP, P2P y Resto	

Capítulo 9: HTB

Hierarchical Token Bucket

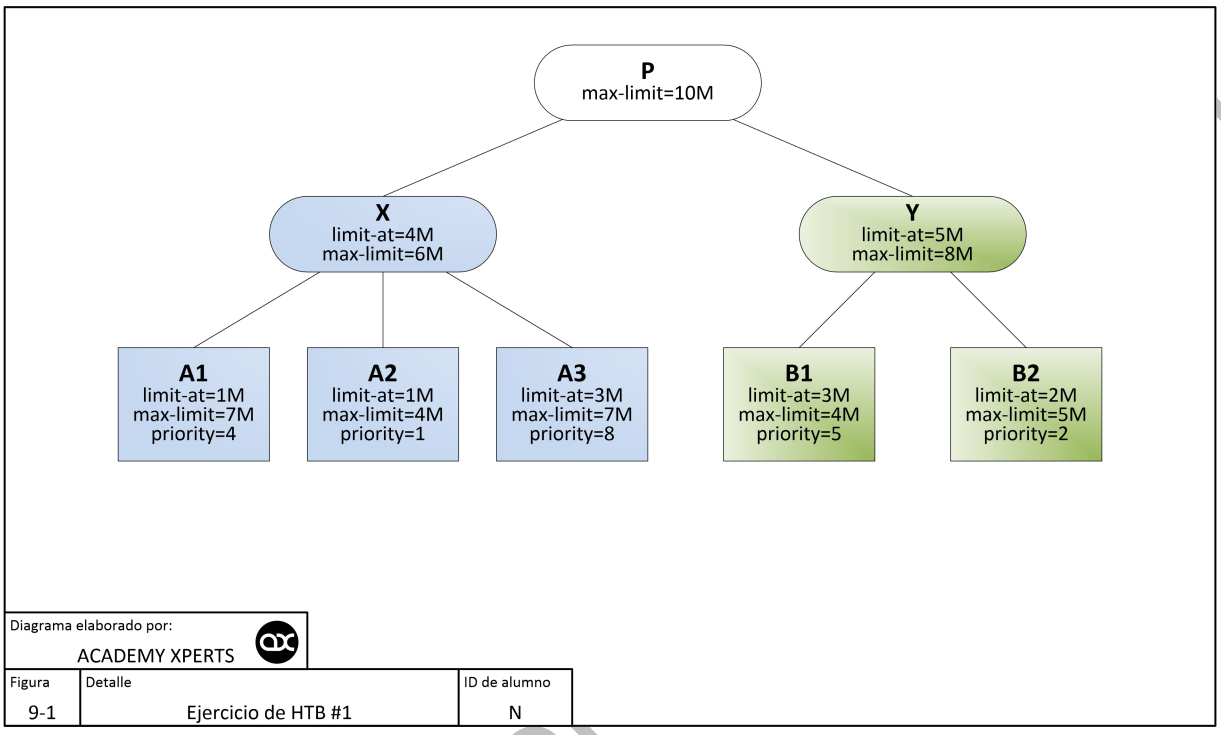
Laboratorio 9-1: Ejercicio de HTB #1

Objetivo:

- Comprender el funcionamiento de HTB en RouterOS

Escenario:

La Figura 9-1 (Ejercicio de HTB #1) muestra la disposición de los padres-hijos en la estructura HTB



Tema:

Se tiene la siguiente estructura:

```
queue "P" max-limit=10M
   queue "X" parent="P" limit-at=4M max-limit=6M
        queue "A1" parent="X" limit-at=1M max-limit=7M priority=4
        queue "A2" parent="X" limit-at=1M max-limit=4M priority=1
        queue "A3" parent="X" limit-at=3M max-limit=7M priority=8
   queue "Y" parent="P" limit-at=5M max-limit=8M
        queue "B1" parent="Y" limit-at=3M max-limit=4M priority=5
        queue "B2" parent="Y" limit-at=2M max-limit=5M priority=2
```

Pregunta:

En caso de que todas colas (queues) hijos requiera 2Mbps cada uno al mismo tiempo, lo van a conseguir?

- Verdadero
- Falso

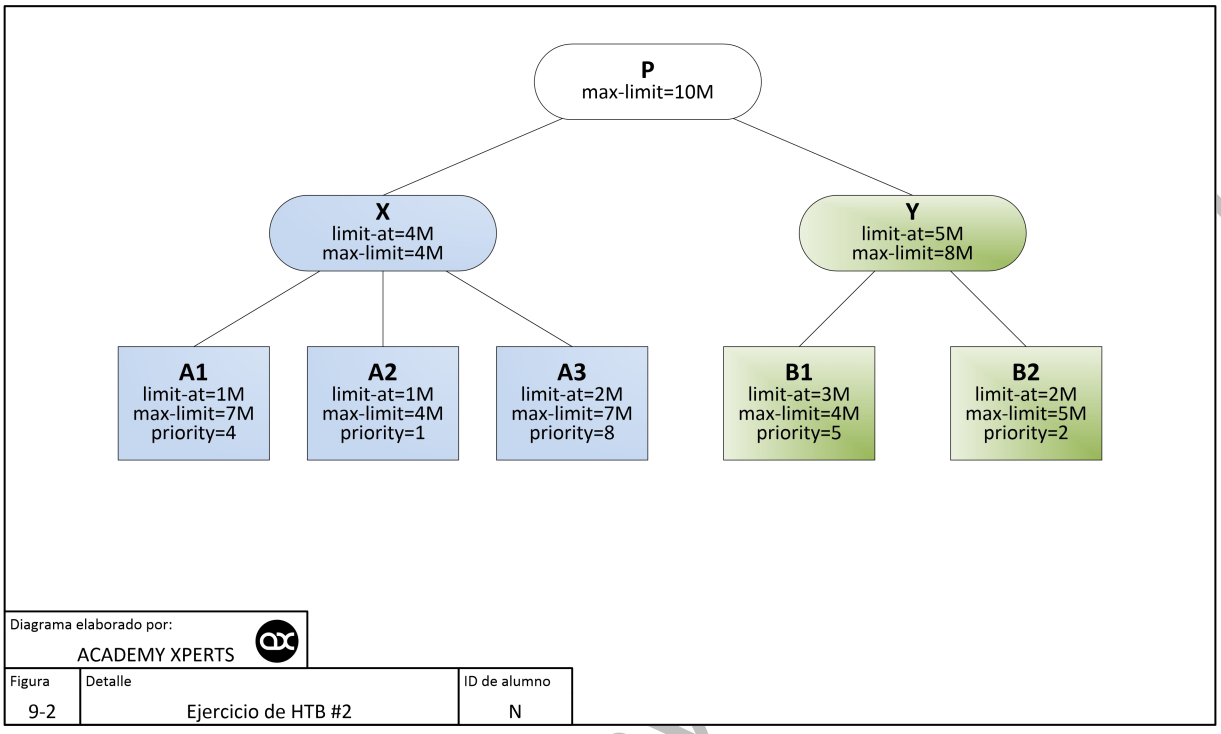
Laboratorio 9-2: Ejercicio de HTB #2

Objetivo:

- Comprender el funcionamiento de HTB en RouterOS

Escenario:

La Figura 9-2 (Ejercicio de HTB #2) muestra la disposición de los padres-hijos en la estructura HTB



Tema:

Se tiene la siguiente estructura:

```
queue "P" max-limit=10M
   queue "X" parent="P" limit-at=4M max-limit=4M
        queue "A1" parent="X" limit-at=1M max-limit=7M priority=4
        queue "A2" parent="X" limit-at=1M max-limit=4M priority=1
        queue "A3" parent="X" limit-at=2M max-limit=7M priority=8
   queue "Y" parent="P" limit-at=5M max-limit=8M
        queue "B1" parent="Y" limit-at=3M max-limit=4M priority=5
        queue "B2" parent="Y" limit-at=2M max-limit=5M priority=2
```

Pregunta:

Cuál cola (queue) obtendrá más de su `limit-at` en el peor escenario posible?

a) B1
b) A1
c) B2
d) A3
e) A2

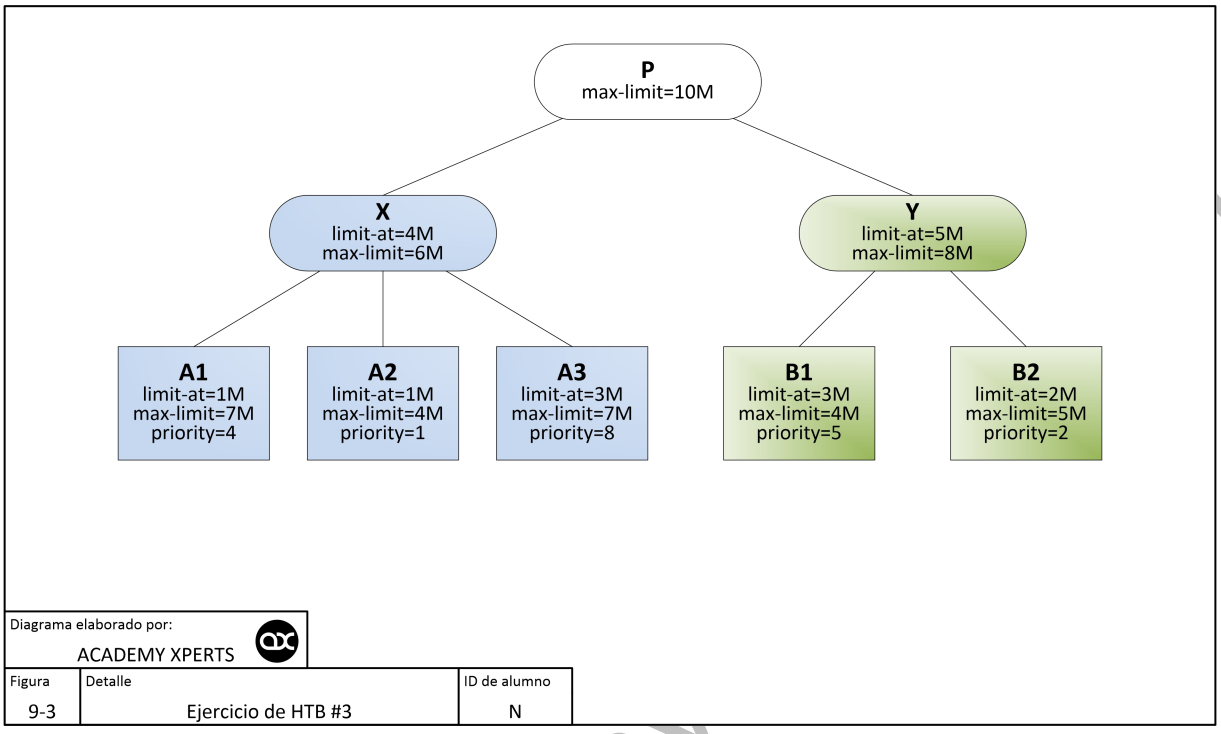
Laboratorio 9-3: Ejercicio de HTB #3

Objetivo:

- Comprender el funcionamiento de HTB en RouterOS

Escenario:

La Figura 9-3 (Ejercicio de HTB #3) muestra la disposición de los padres-hijos en la estructura HTB



Tema:

Se tiene la siguiente estructura:

```
queue "P" max-limit=10M
   queue "X" parent="P" limit-at=4M max-limit=6M
        queue "A1" parent="X" limit-at=1M max-limit=7M priority=4
        queue "A2" parent="X" limit-at=1M max-limit=4M priority=1
        queue "A3" parent="X" limit-at=3M max-limit=7M priority=8
   queue "Y" parent="P" limit-at=5M max-limit=8M
        queue "B1" parent="Y" limit-at=3M max-limit=4M priority=5
        queue "B2" parent="Y" limit-at=2M max-limit=5M priority=2
```

Pregunta:

Si las colas (queues) A2 y A3 no requieren tráfico, cómo se distribuirá el ancho de banda en el peor escenario posible?

a) queue "A1" 3M, "B2" 3M, "B1" 5M
b) queue "A1" 5M, "B2" 2M, "B1" 3M
c) queue "A1" 4M, "B2" 2M, "B1" 4M
d) queue "A1" 4M, "B2" 3M, "B1" 3M
e) queue "A1" 4M, "B2" 7M, "B1" 4M

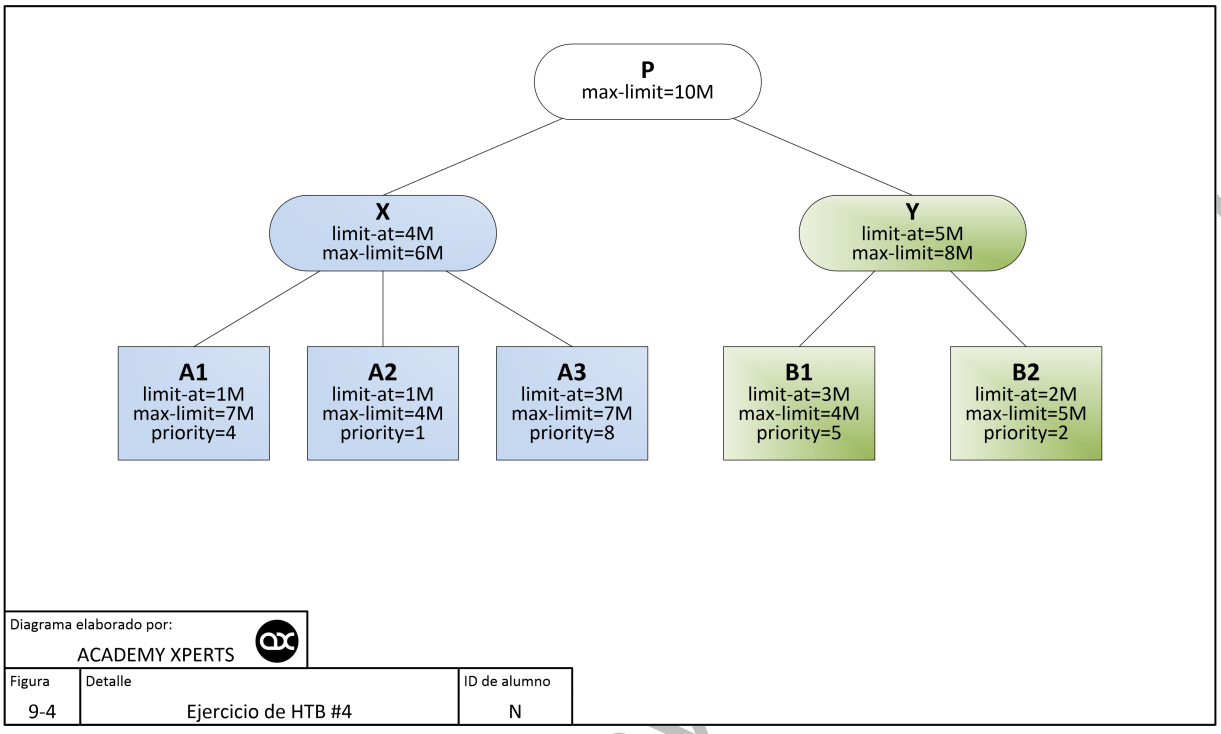
Laboratorio 9-4: Ejercicio de HTB #4

Objetivo:

- Comprender el funcionamiento de HTB en RouterOS

Escenario:

La Figura 9-4 (Ejercicio de HTB #4) muestra la disposición de los padres-hijos en la estructura HTB



Tema:

Se tiene la siguiente estructura:

```
queue "P" max-limit=10M
   queue "X" parent="P" limit-at=4M max-limit=6M
        queue "A1" parent="X" limit-at=1M max-limit=7M priority=4
        queue "A2" parent="X" limit-at=1M max-limit=4M priority=1
        queue "A3" parent="X" limit-at=3M max-limit=7M priority=8
   queue "Y" parent="P" limit-at=5M max-limit=8M
        queue "B1" parent="Y" limit-at=3M max-limit=4M priority=5
        queue "B2" parent="Y" limit-at=2M max-limit=5M priority=2
```

Pregunta:

Si las colas (queues) A1 y B2 no requieren tráfico, cómo se distribuirá el ancho de banda en el peor escenario posible?

a) "A2" 3M, "A3" 3M, "B1" 4M
b) "A2" 2M, "A3" 5M, "B1" 3M
c) "A2" 4M, "A3" 2M, "B1" 4M
d) "A2" 4M, "A3" 2M, "B1" 4M
e) "A2" 4M, "A3" 7M, "B1" 4M