

# Pruebas y securización con Mikrotik

José Manuel Román

# Exención de responsabilidad:

Cualquier acción o actividad relacionada con el material que se expone a continuación es tu responsabilidad. El maluso de la información proporcionada en esta presentación puede causar acciones legales. El autor no será responsable en ningún caso de cualquier acción que se lleve a cabo para infringir la ley utilizando esta presentación.

## Acerca de mi

- 16 años de experiencia en T.I.
- 7 años enseñando redes
- 6 años como analista de seguridad
- Socio de Cloud Networking Spain (Wisp). Consultoría y enseñanza.
- Ingeniero Técnico de Sistemas.
- Master ITIL.
- Certificaciones de seguridad: Cisa and Cispp
- Certificaciones Mikrotik: MTCINE, MTCNA, MTCRE, MTCTCE, MTCWE, MTCUME. Trainer.

## Acerca de Cloud Networking

- WISP con redes en Castilla la Mancha y Extremadura
- Montaje y mantenimiento de Wisp, con redes desplegadas en Andalucía, Castilla la Mancha, Extremadura y Logroño.
- Clases mensuales de Certificaciones Mikrotik
  - Próxima edición MTCNA 19,20,21 de octubre en Alcazar de San Juan
- Consultoria de Redes.
- Consultoria de seguridad.

## Objetivo

El objetivo de esta presentación es mostrar las herramientas que proporciona Mikrotik para probar y auditar configuraciones de firewall y QoS.

Principalmente Traffic Generator.

## Agenda

- Duración: 30 minutos
- Introducción: 5 minutos
- Escenario 1 Pruebas de reglas contra Synflood: 12 minutos
- Escenario 2 Pruebas de Queue tree para VoIP: 12 minutos

## Problema

No sé qué hacer cuando necesito probar o auditar si un router está cumpliendo con unas políticas de seguridad o de QoS en entornos complejos.

¿Qué hacer cuando necesitamos enseñar QoS y reglas de firewall complejas?

## Síntomas

Tenemos configuraciones complejas y no tenemos ni idea de como probar esa configuración.

Los clientes o nuestros estudiantes nos exigen que las configuraciones funcionen.



## Solución

Necesitamos herramientas para  
enseñanza y pruebas

## Tools

En RoS hay un gran número de herramientas comúnmente utilizadas para probar y enseñar:

- Ping, Traceroute.
- Monitorización en tiempo real y sniffer.
- Generador de tráfico.

## Herramientas externas

Similares a otras que no están presentes en Mikrotik:

- Hping3
- Scapy
- Wireshark

## Primer Escenario

En este escenario vamos a probar el funcionamiento de tres políticas de seguridad que intentan limitar un ataque Synflood.

El ataque lo vamos a generar utilizando la herramienta Traffic Generator.

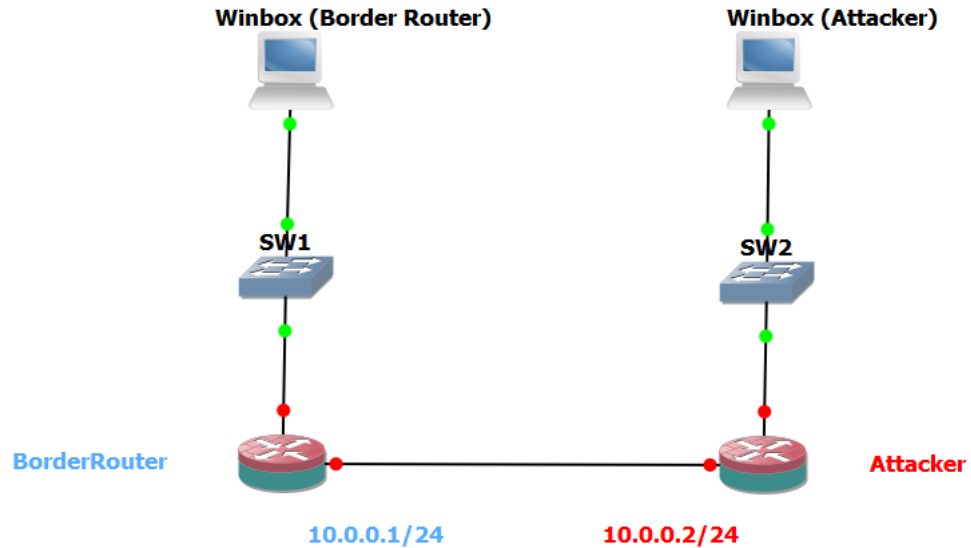
## Primer escenario

Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.



## Escenario 1



## TCP handshake

Normalmente cuando un cliente intenta comenzar una conexión TCP a un servidor, se intercambian una serie de mensajes que normalmente se ejecutan de la siguiente manera:

- Un cliente manda una petición SYN (synchronize) al servidor.
- El servidor acknowledges esta petición mandando SYN-ACK de vuelta al cliente.
- El cliente responde con un ack y la conexión se establece.



## Flags TCP en el firewall

¿Dónde podemos encontrar los flags tcp en Mikrotik?

The screenshot shows the 'New Firewall Rule' dialog box in Mikrotik WinBox. The 'TCP Flags' section is highlighted with a blue box. The 'TCP Flags' list includes:  fin,  ack,  cwr,  ece,  fin,  psh,  rst,  syn,  urg. The 'enabled' checkbox is checked at the bottom left.



## Ataque(syn flood)

SYN flood es una forma de ataque de denegación de servicio en el que un atacante manda una sucesión de peticiones SYN a un sistema objetivo para intentar consumir todos los recursos del servidor y de esta forma el servidor no pueda atender peticiones legítimas.

## Primer escenario

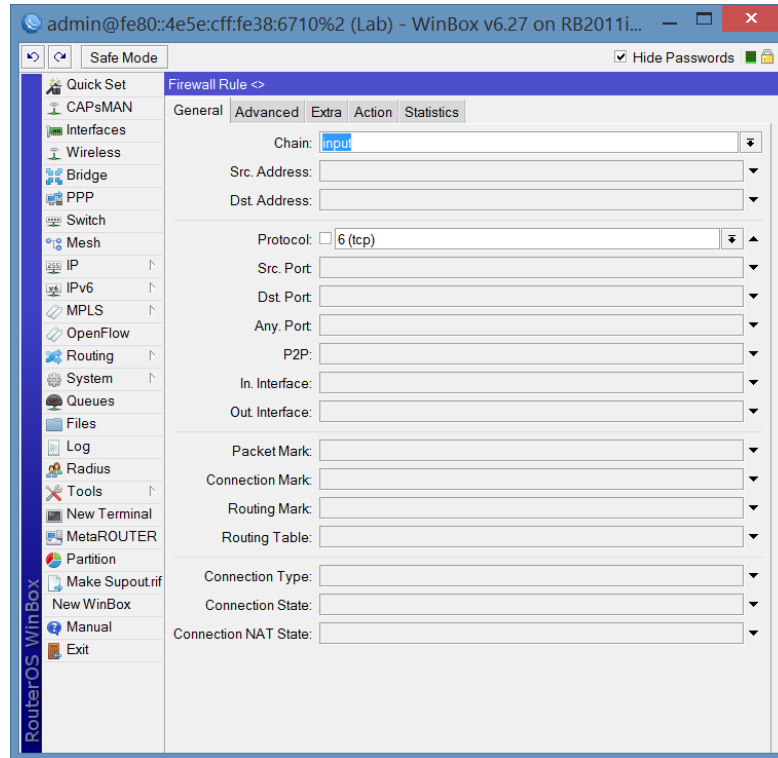
Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

## Primera regla (Política 1)

Vamos a configurar una regla para intentar parar el ataque:

```
/ip firewall filter add chain=input comment="synflood policy1"  
connection-limit=20,32 disabled=no protocol=tcp action=drop
```



The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The window title is "admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...". The interface is in "Safe Mode" and has "Hide Passwords" checked. The left sidebar shows a navigation tree with categories like "Quick Set", "CAPsMAN", "Interfaces", "Wireless", "Bridge", "PPP", "Switch", "Mesh", "IP", "IPv6", "MPLS", "OpenFlow", "Routing", "System", "Queues", "Files", "Log", "Radius", "Tools", "New Terminal", "MetaROUTER", "Partition", "Make Supout.rif", "New WinBox", "Manual", and "Exit". The main area is titled "Firewall Rule" and has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "General" tab is active, showing the following configuration fields:

- Chain:
- Src. Address:
- Dst. Address:
- Protocol:  6 (tcp)
- Src. Port:
- Dst. Port:
- Any. Port:
- P2P:
- In. Interface:
- Out. Interface:
- Packet Mark:
- Connection Mark:
- Routing Mark:
- Routing Table:
- Connection Type:
- Connection State:
- Connection NAT State:



The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The 'General' tab is selected. The 'Connection Limit' section is expanded, showing a 'Limit' field with the value '20' and a 'Netmask' field with the value '32'. The left sidebar contains a tree view of system components including CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, IPv6, MPLS, OpenFlow, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rif, New WinBox, Manual, and Exit.

The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule, now on the 'Action' tab. The 'Action' dropdown menu is set to 'drop'. The 'Log' checkbox is checked, and the 'Log Prefix' field contains the text 'policy|'. The left sidebar is identical to the previous screenshot.

## Encuesta online

¿Funcionará la regla?

```
/ip firewall filter add chain=input comment="synflood policy1" connection-  
limit=20,32 disabled=no protocol=tcp action=drop
```

- No, esta regla no dropea paquetes
- La regla funciona pero no para el ataque
- Sí, funciona y limita el ataque synflood.



<https://survey.zohopublic.com/zs/f3ip30>

## Primer escenario

Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

## Tool to test the policy

- El generador de tráfico es una herramienta que permite evaluar rendimiento de DUT (Device Under Test) o SUT (System Under Test).
- La herramienta puede generar y enviar paquetes en bruto por unos puertos determinados. También es capaz de recopilar valores de latencia, jitter, ratios de tx/rx, contadores de paquetes perdidos y detectar paquetes fuera de orden.

<https://survey.zohopublic.com/zs/f3ip3O>





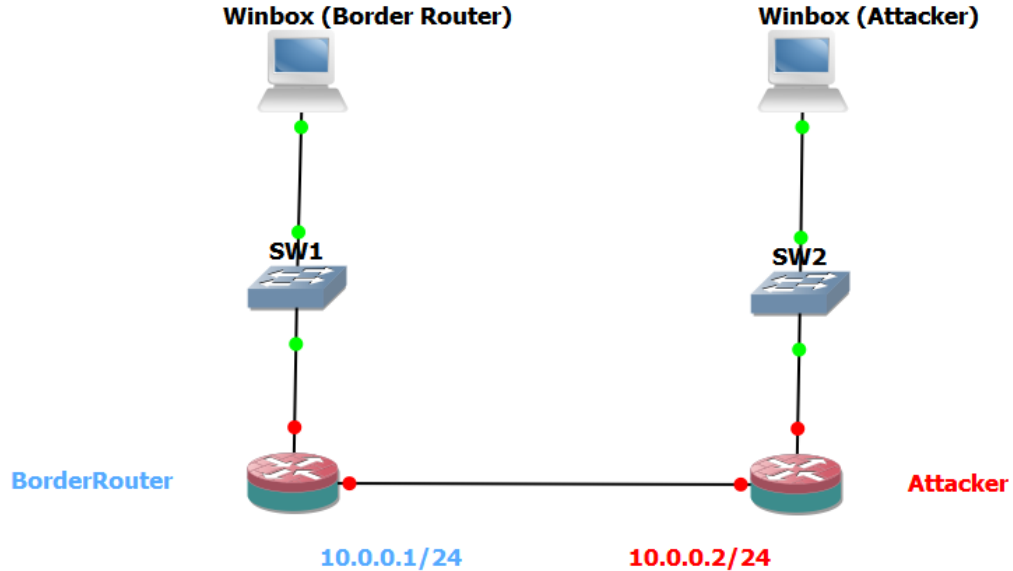
# Artesanía con el generador de tráfico

## Flujo de trabajo de las pruebas





## Escenario 1

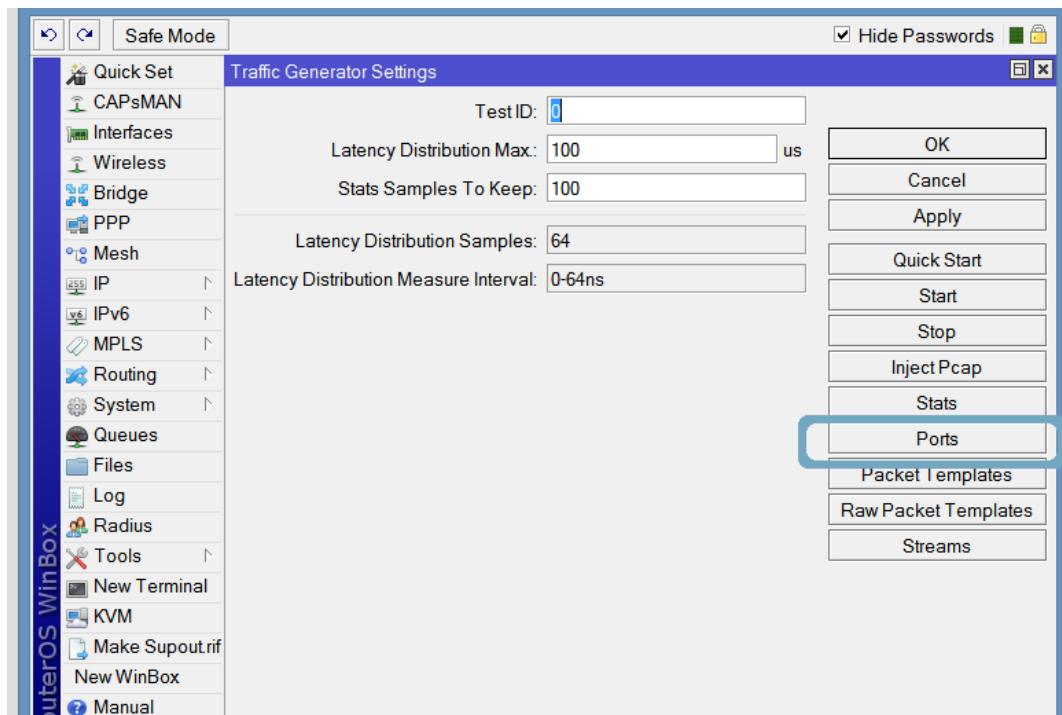


## Primer escenario

Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

## Traffic Generator (Port)





# Traffic Generator (Port)

The screenshot shows the Mikrotik WinBox interface. The main window is titled "Traffic Generator Settings" and contains the following fields:

- Test ID: 0
- Latency Distribution Max: 100 us
- Stats Samples To Keep: 100

Buttons for "OK", "Cancel", and "Apply" are visible. Below this is the "Traffic Generator Ports" window, which displays a table with the following data:

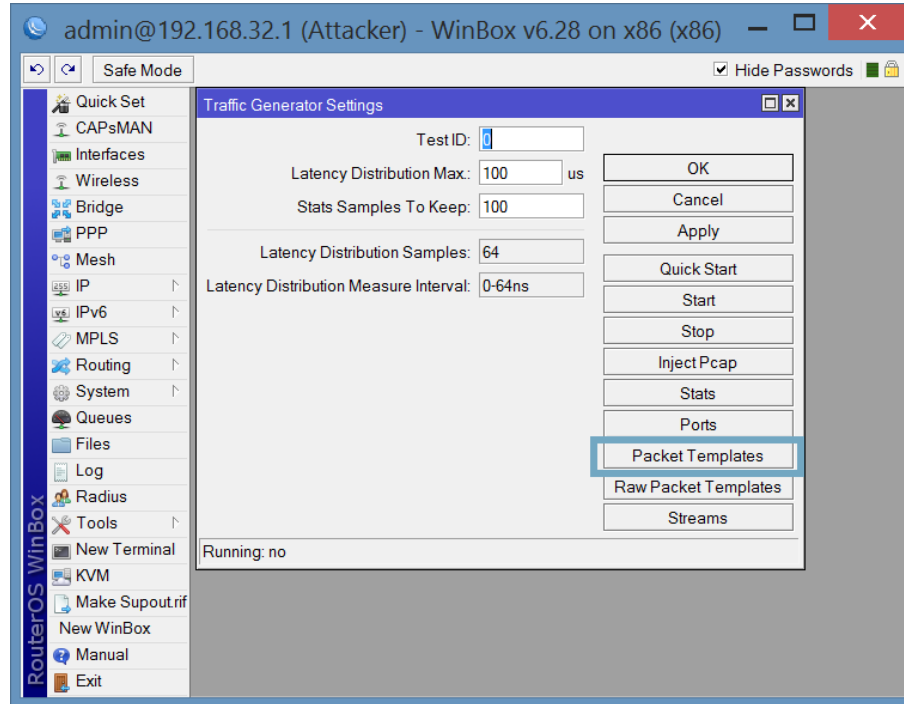
Name	Interface	First Header
port1	ether1	mac

A dialog box titled "Traffic Generator Port <port1>" is open, showing the configuration for the selected port:

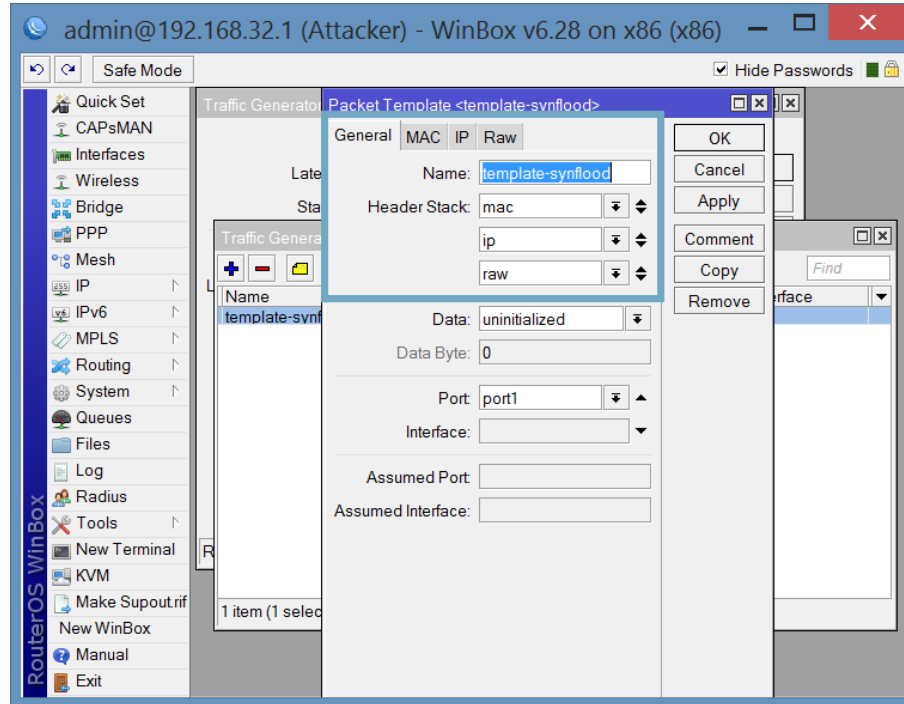
- Name: port1
- Interface: ether1
- First Header: mac

Buttons for "OK", "Cancel", "Apply", "Disable", "Copy", and "Remove" are present. The status "1 item (1 selected)" and "enabled" are shown at the bottom of the dialog.

## Traffic Generator (Packet Template)



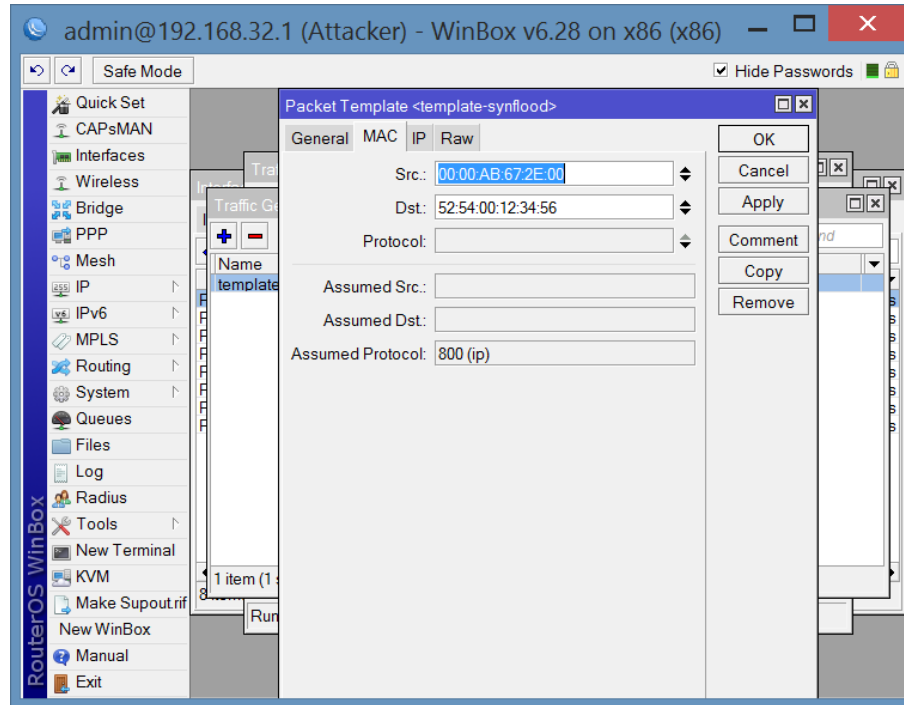
# Traffic Generator (Packet Template)







## Traffic Generator(Packet Template)





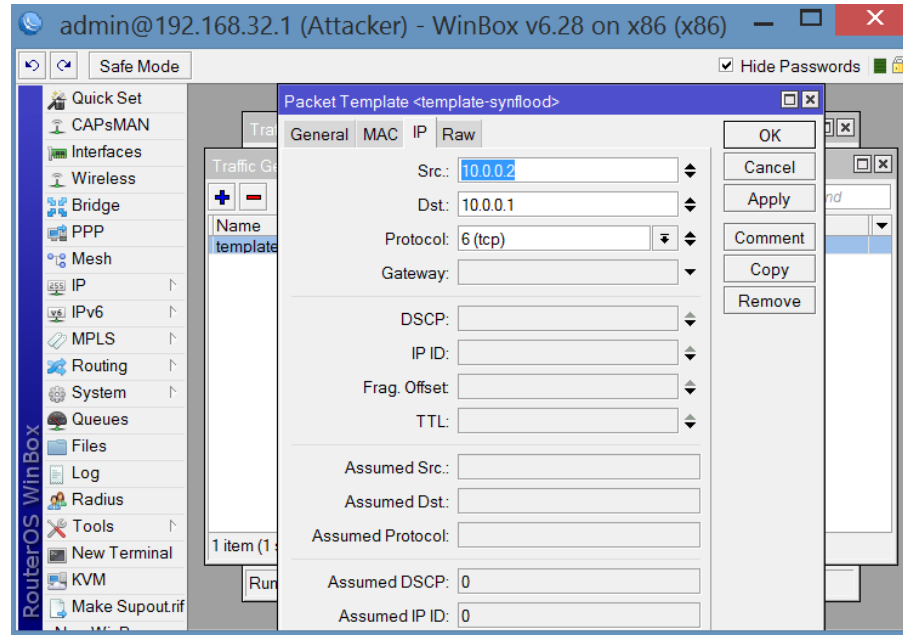
## Traffic Generator(Packet Template)

The screenshot shows the Mikrotik WinBox interface for configuring an interface. The main window is titled "Interface <ether1>" and has tabs for "General", "Ethernet", "Status", and "Traffic". The "General" tab is active, showing fields for Name (ether1), Type (Ethernet), MTU (1500), L2 MTU, Max L2 MTU, and MAC Address (00:00:AB:67:2E:00). The ARP checkbox is checked and labeled "enabled". A "Neighbor List" dialog box is open in the foreground, displaying a table of neighbors.

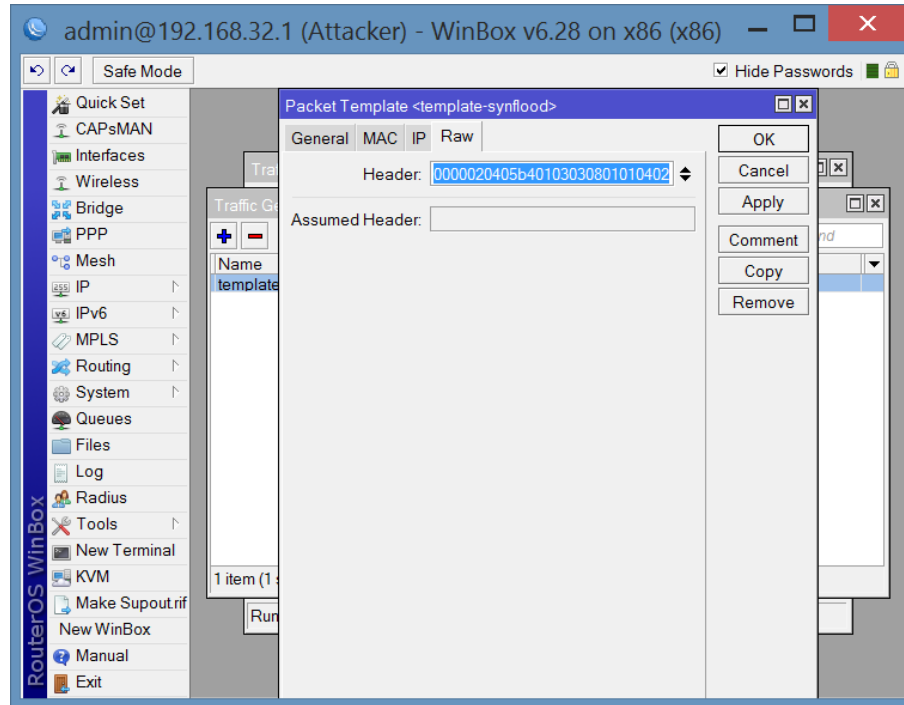
Interface	IP Address	MAC Address	Identity	Platform	Version	Board ...	IPv6
ether1	10.0.0.1	52:54:00:12:34:56	Border...	MikroTik	6.28	x86	yes



## Traffic Generator(Packet Template)



## Traffic Generator(Packet Template)





# Traffic Generator(Stream)

The screenshot shows the Mikrotik WinBox interface. The main window is titled "admin@192.168.32.1 (Attacker) - WinBox v6.28 on x86 (x86)". The left sidebar contains a navigation menu with items like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, KVM, Make Supout.rif, New WinBox, Manual, and Exit. The main area displays the "Traffic Generator Settings" window, which is open to the "Traffic Generator Streams" tab. A "Packet Stream <synflood>" dialog box is open, showing the following configuration:

- Name: synflood
- Default Port: dynamic0
- Port: port1
- ID: 0
- Packet Size: 1500
- MBPS: 10
- PPS: (empty)
- Tx Template: template-synflood
- enabled

Buttons for OK, Cancel, Apply, Disable, Copy, and Remove are visible. Below the dialog, a table shows "1 item (1 selected)" with a status of "Running: no".

## Primer escenario

Probando las reglas anti synflood:

- Configuración de las reglas.
- Preparación del generador de tráfico para generar un tráfico con determinadas características.
- Probar las reglas con el tráfico creado anteriormente.

## Traffic Generator(Quick start)

admin@192.168.32.1 (Attacker) - WinBox v6.28 on x86 (x86)

Safe Mode  Hide Passwords

**Quick Start**

Test ID:

Stream:

Port:

Interface:

Packet Size:

PPS:

MBPS:

Tx Template:

Start Stop Close New Window

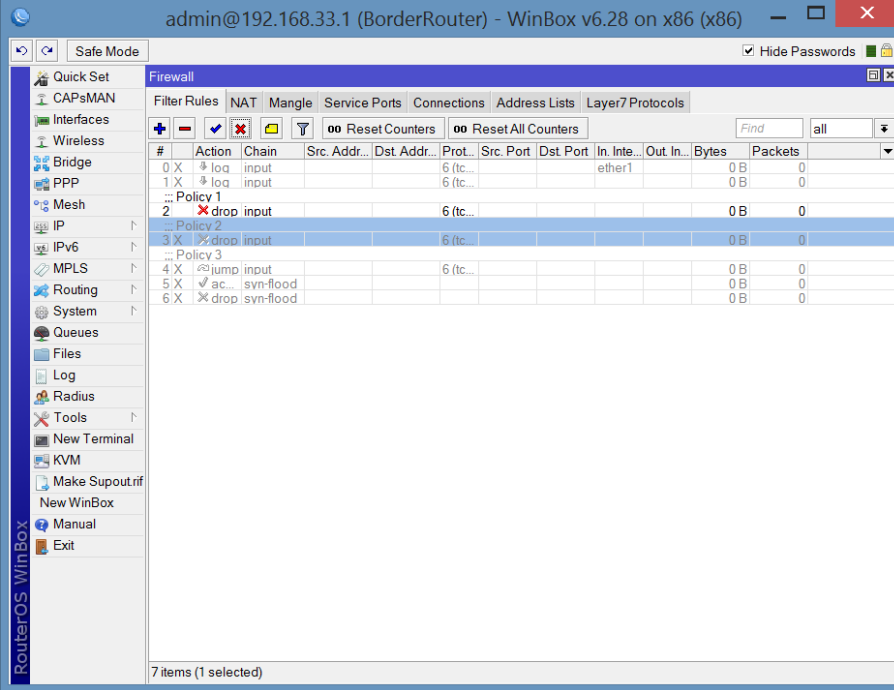
Seq	ID	Tx Packets	Tx Rate	Rx Packets	Rx Rate	Lost Packe...	Lost Rate
1	0	10	120.0 kbps	0	0 bps	10	120.0 kbps
2	0	10	120.0 kbps	0	0 bps	10	120.0 kbps
3	0	10	120.0 kbps	0	0 bps	10	120.0 kbps
4	0	10	120.0 kbps	0	0 bps	10	120.0 kbps
5	0	10	120.0 kbps	0	0 bps	10	120.0 kbps
TOT	0	50	120.0 kbps	0	0 bps	50	120.0 kbps

RouterOS WinBox

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP
- IPv6
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- KVM
- Make Supout.tif
- New WinBox
- Manual
- Exit



## Contadores de Border Router (política 1)



The screenshot shows the Mikrotik WinBox interface for Firewall Filter Rules. The window title is 'admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 (x86)'. The 'Filter Rules' tab is active. The table below shows the configuration for 7 items, with 'Policy 1' selected.

#	Action	Chain	Src. Addr...	Dst. Addr...	Prot...	Src. Port	Dst. Port	In. Inte...	Out In...	Bytes	Packets
0	X	loa	input		6 (tc...			ether1		0 B	0
1	X	loa	input		6 (tc...					0 B	0
...											
2	X	drop	input		6 (tc...					0 B	0
...											
3	X	drop	input		6 (tc...					0 B	0
...											
4	X	connp	input		6 (tc...					0 B	0
...											
5	X	ac	syn-flood							0 B	0
...											
6	X	drop	syn-flood							0 B	0



## Encuesta online

¿Funcionará la regla?

```
/ip firewall filter add chain=input comment="synflood policy1"  
connection-limit=20,32 disabled=no protocol=tcp action=drop
```

- No, esta regla no dropea paquetes
- La regla funciona pero no para el ataque
- Sí, funciona y limita el ataque synflood.

<https://survey.zohopublic.com/zs/f3ip30>

## Política 1

No, esta regla no dropea paquetes

El atacante nunca llega a establecer conexiones y entonces hay un límite de conexiones que no aplica.

<https://survey.zohopublic.com/zs/f3ip3O>

## Política 2

```
/ip firewall filter add chain=input limit=20,1 protocol=tcp tcp-flags=syn  
action=drop
```

<https://survey.zohopublic.com/zs/f3ip3O>





The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The window title is "admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...". The "General" tab is selected. The "Chain" is set to "input". The "Protocol" is set to "6 (tcp)". The "In. Interface" and "Out. Interface" fields are empty. The "Connection Type", "Connection State", and "Connection NAT State" are also empty. The left sidebar shows various system components like CAPsMAN, Interfaces, Bridge, PPP, Switch, Mesh, IP, IPv6, MPLS, OpenFlow, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rif, New WinBox, Manual, and Exit.

The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule, with the "Advanced" tab selected. The "Src. Address List" and "Dst. Address List" are empty. The "Layer7 Protocol" is empty. The "Content" is empty. The "Connection Bytes" and "Connection Rate" are empty. The "Per Connection Classifier" is empty. The "Src. MAC Address" is empty. The "Out. Bridge Port" and "In. Bridge Port" are empty. The "Ingress Priority" is empty. The "Priority" is empty. The "DSCP (TOS)" is empty. The "TCP MSS" is empty. The "Packet Size" is empty. The "Random" is empty. The "TCP Flags" section shows "TCP Flags" set to "syn" and "Invert" unchecked. The "ICMP Options" section shows "IPv4 Options" empty. The left sidebar is identical to the previous screenshot.



The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The window title is "admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 (x86)". The "Firewall Rule" configuration window is open, with the "Limit" tab selected. The "Limit" section is expanded, showing "Rate" set to 20 and "Burst" set to 1. The "Action" tab is also visible, showing buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", "Reset Counters", and "Reset All Counters". The left sidebar contains a tree view of system components like CAPsMAN, Interfaces, Bridge, PPP, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, KVM, Make Supoutnif, New WinBox, Manual, and Ext.

The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The window title is "admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 (x86)". The "Firewall Rule" configuration window is open, with the "Action" tab selected. The "Action" dropdown menu is set to "drop". The "Log" checkbox is checked, and the "Log Prefix" is set to "policy 2". The "Action" tab is also visible, showing buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", "Reset Counters", and "Reset All Counters". The left sidebar contains a tree view of system components like CAPsMAN, Interfaces, Bridge, PPP, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, KVM, Make Supoutnif, New WinBox, Manual, and Ext.

## Encuesta online

¿Funcionará la política 2?

```
/ip firewall filter add chain=input limit=20,1 protocol=tcp tcp-flags=syn  
action=drop
```

- No, esta regla no dropea paquetes
- La regla funciona pero no para el ataque
- Sí, funciona y limita el ataque synflood.

<https://survey.zohopublic.com/zs/f3ip3O>



¿Por qué los contadores se incrementan de 40 en 40?

The screenshot shows the Mikrotik WinBox interface for Firewall Filter Rules. The table below is a representation of the data shown in the interface:

#	Action	Chain	Src. Addr...	Dst. Addr...	Prot...	Src. Port	Dst. Port	In. Inte...	Out. In...	Bytes	Packets
0	X log	input			6 (tc...			ether1		0 B	0
1	X log	input			6 (tc...					0 B	0
2	X drop	input			6 (tc...					0 B	0
3	X drop	input			6 (tc...			ether1		512.3 KiB	353

## Encuesta online

¿Funciona la política 2?

La regla dropea paquetes pero no limita el ataque.  
Dropea 20 paquetes cada segundo.

<https://survey.zohopublic.com/zs/f3ip30>



## Política 3

```
/ip firewall filter
```

```
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
```

```
add chain=syn-flood limit=100,5
```

```
add action=drop chain=syn-flood
```

<https://survey.zohopublic.com/zs/f3ip30>

## Encuesta online

¿Funciona la política 3?

```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
add chain=syn-flood limit=100,5
add action=drop chain=syn-flood
```

- No, esta regla no dropea paquetes
- La regla dropea paquetes pero no limita el ataque
- Sí, la regla limita el ataque.

<https://survey.zohopublic.com/zs/f3ip3O>

## Política 3 (Primera regla)

/ip firewall filter

```
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
```

<https://survey.zohopublic.com/zs/f3ip3O>





The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The window title is "admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...". The "General" tab is selected, showing the following fields:

- Chain:
- Src. Address:
- Dst. Address:
- Protocol:  6 (tcp)
- Src. Port:
- Dst. Port:
- Any. Port:
- P2P:
- In. Interface:
- Out. Interface:
- Packet Mark:
- Connection Mark:
- Routing Mark:
- Routing Table:
- Connection Type:
- Connection State:
- Connection NAT State:

The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule, with the "Advanced" tab selected. The window title is "admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...". The "Advanced" tab shows the following fields:

- Src. Address List:
- Dst. Address List:
- Layer7 Protocol:
- Content:
- Connection Bytes:
- Connection Rate:
- Per Connection Classifier:
- Src. MAC Address:
- Out. Bridge Port:
- In. Bridge Port:
- Ingress Priority:
- Priority:
- DSCP (TOS):
- TCP MSS:
- Packet Size:
- Random:
- TCP Flags:  syn  invert
- ICMP Options:
- IPv4 Options:



admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...

Safe Mode  Hide Passwords

### Firewall Rule <>

General Advanced Extra Action Statistics

Action: **jump**

Log

Log Prefix:

Jump Target: **syn-flood**

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Reset Counters  
Reset All Counters

enabled

RouterOS WinBox

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP
- IPv6
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- KVM
- Make Supout.tif
- New WinBox
- Manual
- Exit

## Política 3 (Segunda regla)

```
/ip firewall filter
```

```
add chain=syn-flood limit=100,5
```



admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...

Safe Mode  Hide Passwords

RouterOS WinBox

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP
- IPv6
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- KVM
- Make Supout.rif
- New WinBox
- Manual
- Exit

### Firewall Rule <>

General | **Advanced** | Extra | Action | Statistics

Chain: **syn-flood**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...

Safe Mode  Hide Passwords

RouterOS WinBox

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP
- IPv6
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- KVM
- Make Supout.rif
- New WinBox
- Manual
- Exit

### Firewall Rule <>

General | **Advanced** | Extra | Action | Statistics

Action: **accept**

Log

Log Prefix:



The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The window title is "admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...". The interface includes a sidebar with navigation options such as Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, KVM, Make Supout.rif, New WinBox, Manual, and Exit. The main area is titled "Firewall Rule <>" and has tabs for General, Advanced, Extra, Action, and Statistics. The "General" tab is active, showing configuration options for Connection Limit, Limit (Rate: 100 / sec, Burst: 5), Dst Limit, Nth, Time, Src. Address Type, Dst. Address Type, PSD, Hotspot, and IP Fragment.





## Política 3 (Tercera Regla)

```
/ip firewall filter  
add action=drop chain=syn-flood
```

<https://survey.zohopublic.com/zs/onCNRc>



admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...

Safe Mode  Hide Passwords

RouterOS WinBox

Firewall Rule <>

General | **Advanced** | Extra | Action | Statistics

Chain: **syn-flood**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

admin@192.168.33.1 (BorderRouter) - WinBox v6.28 on x86 ...

Safe Mode  Hide Passwords

RouterOS WinBox

Firewall Rule <>

General | **Advanced** | Extra | Action | Statistics

Action: **drop**

Log

Log Prefix:

## Encuesta online

¿Funcionará la política 3?

```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
add chain=syn-flood limit=100,5
add action=drop chain=syn-flood
```

- No, esta regla no dropea paquetes
- La regla dropea paquetes pero no limita el ataque
- Sí, la regla limita el ataque.

<https://survey.zohopublic.com/zs/f3ip3O>

## Encuesta online

¿Funcionará la política 3?

```
/ip firewall filter
add action=jump chain=input comment="Policy 3" jump-target=syn-flood protocol=tcp tcp-flags=syn
add chain=syn-flood limit=100,5
add action=drop chain=syn-flood
```

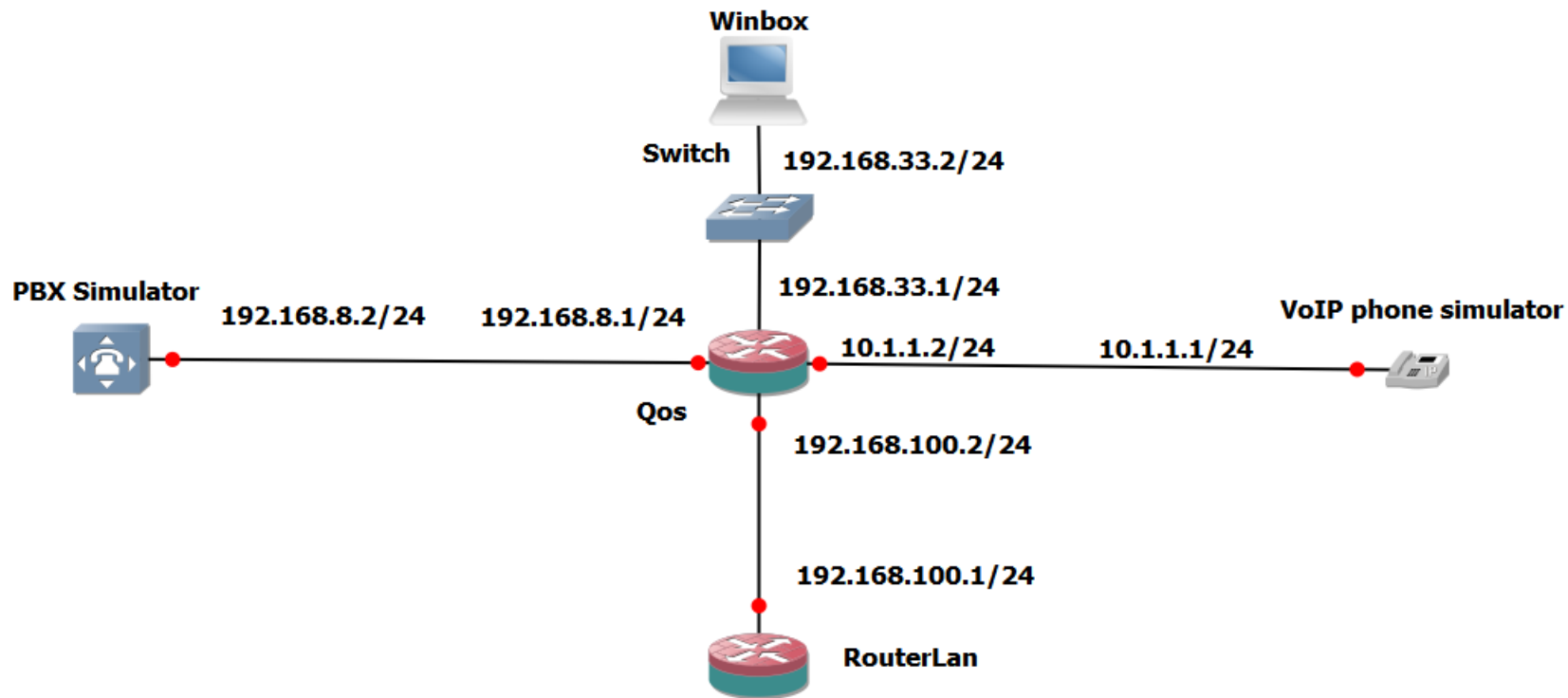
Sí, limita el ataque synflood.

<https://survey.zohopublic.com/zs/f3ip3O>



## Escenario 2 (Probando QoS)

En este lab vamos a probar un marcado  
de paquetes y un queue tree

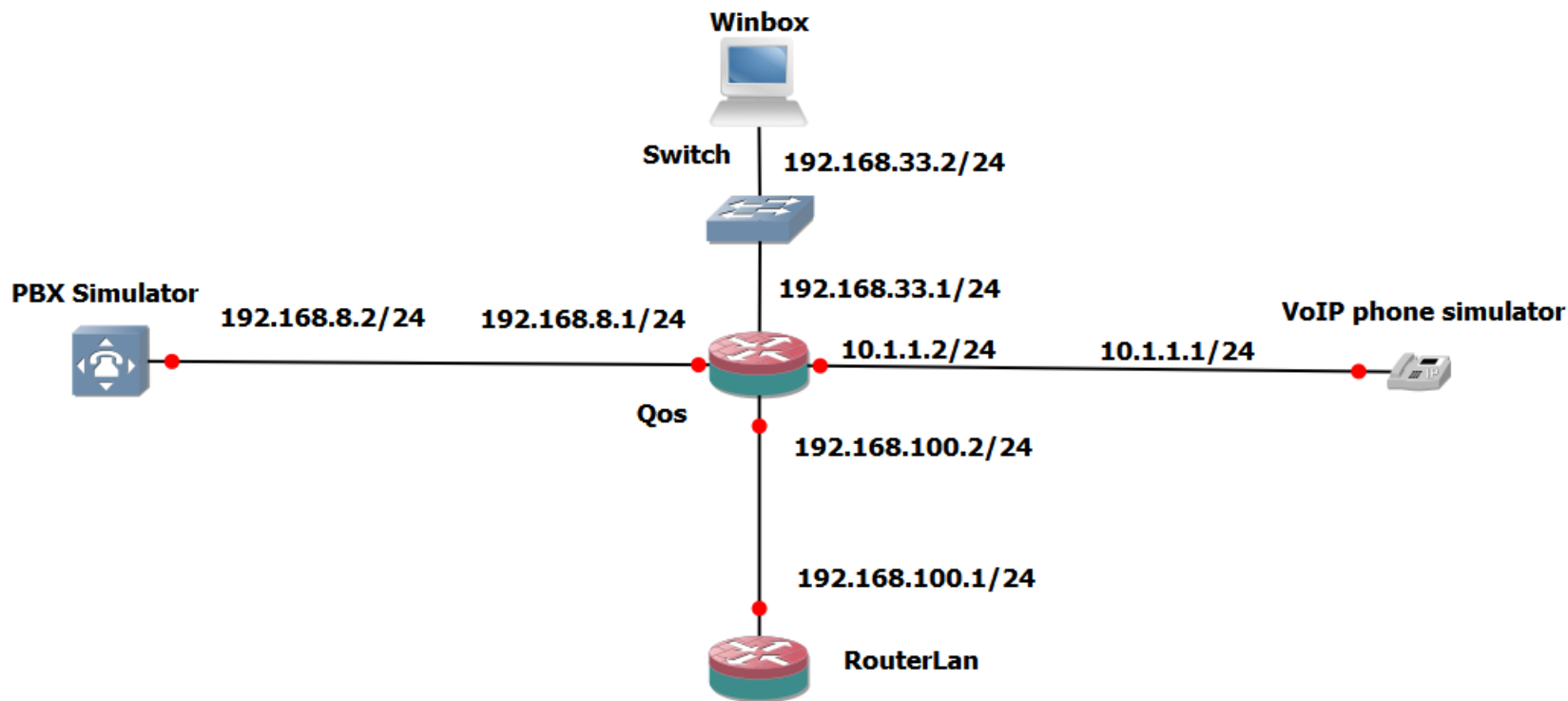


## Configuración de Router

```
[admin@Qos] > ip address print
```

Flags: X - disabled, I - invalid, D - dynamic

#	ADDRESS	NETWORK	INTERFACE
0	192.168.33.1/24	192.168.33.0	ether3
1	192.168.8.1/24	192.168.8.0	ether1
2	10.1.1.2/24	10.1.1.0	ether2
3	192.168.100.2/24	192.168.100.0	ether4





## Configuración de Router

```
[admin@VoIPPhoneSimulator] > ip address print
```

Flags: X - disabled, I - invalid, D - dynamic

#	ADDRESS	NETWORK	INTERFACE
0	10.1.1.1/24	10.1.1.0	ether1

## Configuración de Router

```
[admin@RouterLan] > ip address print
```

Flags: X - disabled, I - invalid, D - dynamic

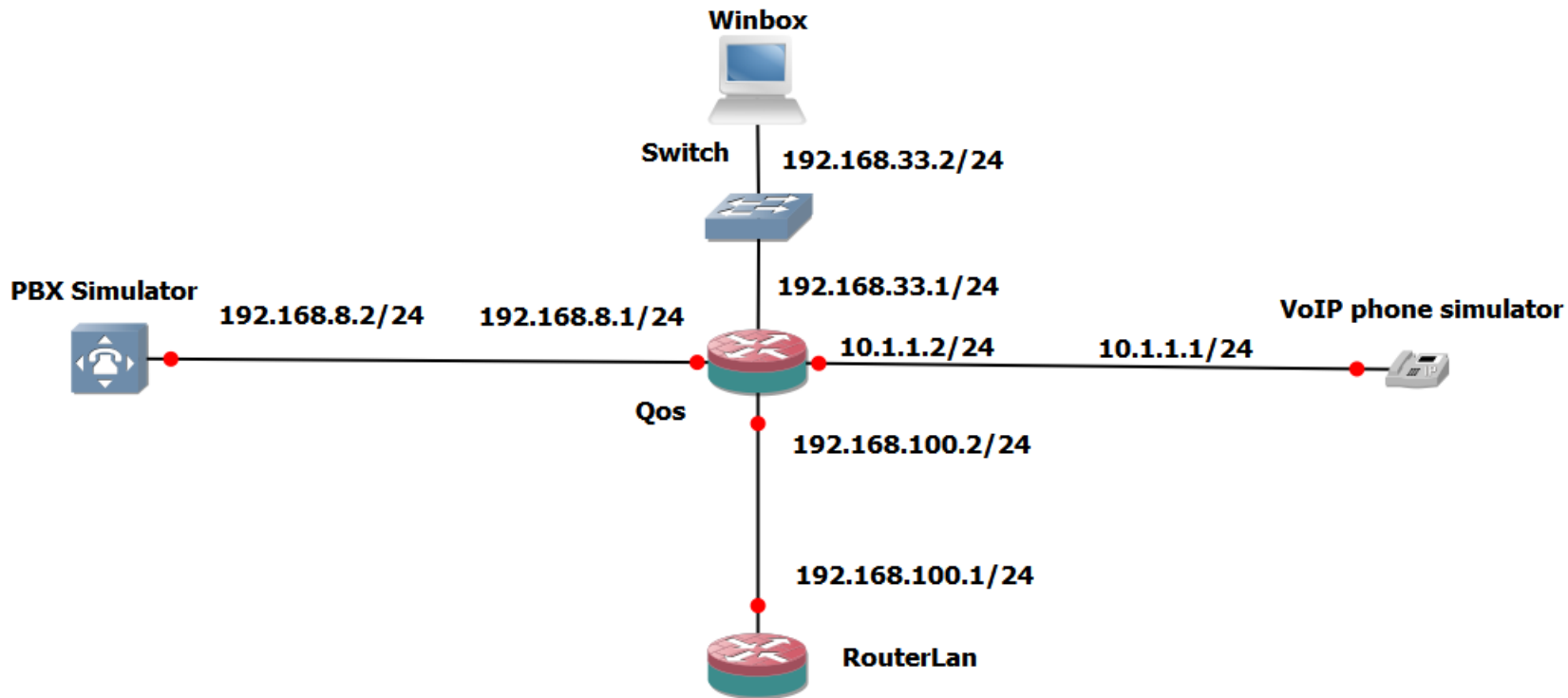
#	ADDRESS	NETWORK	INTERFACE
0	192.168.100.1/24	192.168.100.0	ether1

## Configuración de Router

```
[admin@PbxSimulator] > ip address print
```

```
Flags: X - disabled, I - invalid, D - dynamic
```

#	ADDRESS	NETWORK	INTERFACE
0	192.168.8.2/24	192.168.8.0	ether1



## Escenario 2

En este caso vamos a probar una configuración de queue tree que prioriza el tráfico de voz. El router con nombre QoS tiene reglas de marcado y limitaciones con queue tree.

## Mangle rules

```
[admin@Qos] > ip firewall mangle print
```

```
Flags: X - disabled, I - invalid, D - dynamic
```

```
0   ;;; Normal traffic
```

```
chain=prerouting action=mark-packet new-packet-mark=Rest passthrough=yes src-  
address=192.168.100.1
```

```
dst-address=192.168.8.2 log=no log-prefix=""
```

```
1   ;;; RTP traffic
```

```
chain=prerouting action=mark-packet new-packet-mark=VoipPhones passthrough=no dscp=46 log=no  
log-prefix=""
```

```
2   ;;; SIP traffic
```

```
chain=prerouting action=mark-packet new-packet-mark=VoipPhones passthrough=no dscp=26 log=no  
log-prefix=""
```

## Valores de Dscp en las llamadas Voip

Los mensajes RTP del audio de la conversación se marcan con DSCP EF=0xB8 (=184) . Un valor DSCP de 184 para el traffic generator se convierte en un valor de 46 para la regla de mangle.

1 ::: RTP traffic

```
chain=prerouting action=mark-packet new-packet-  
mark=VoipPhones passthrough=no dscp=46 log=no  
log-prefix=""
```

## Valores de Dscp en las llamadas Voip

Los mensajes de señalización SIP se marcan con el DSCP, AF31=0x68 =104 para el traffic generator. Un valor DSCP de 104 se convierte en un valor de 26 para la regla de mangle

```
2   ::: SIP traffic
```

```
chain=prerouting action=mark-packet new-packet-ark=VoipPhones  
passthrough=no dscp=26 log=no log-prefix=""
```



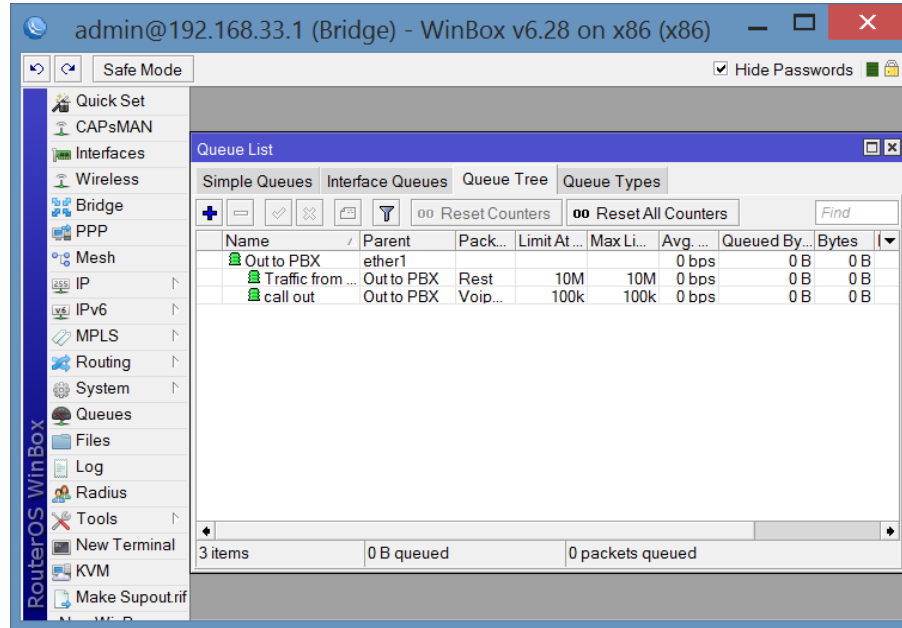
## Queue tree

```
[admin@Qos] > queue tree print
```

```
Flags: X - disabled, I - invalid
```

- ```
0  name="Out to PBX" parent=ether1 packet-mark="" limit-at=0 queue=default priority=8  
    max-limit=0  
    burst-limit=0 burst-threshold=0 burst-time=0s
```
- ```
1  name="call out" parent=Out to PBX packet-mark=VoipPhones limit-at=100k queue=default  
    priority=1  
    max-limit=100k burst-limit=100k burst-threshold=100k burst-time=10s
```
- ```
2  name="Traffic from Router Lan" parent=Out to PBX packet-mark=Rest limit-at=10M  
    queue=default priority=8  
    max-limit=10M burst-limit=10M burst-threshold=10M burst-time=10s
```

# Queue tree



admin@192.168.33.1 (Bridge) - WinBox v6.28 on x86 (x86)

Safe Mode  Hide Passwords

Queue List

Simple Queues | Interface Queues | **Queue Tree** | Queue Types

+ - ✓ ✕ 📄 🔍 Reset Counters Reset All Counters Find

| Name             | Parent     | Pack... | Limit At ... | Max Li... | Avg ... | Queued By... | Bytes |
|------------------|------------|---------|--------------|-----------|---------|--------------|-------|
| Out to PBX       | ether1     |         |              |           | 0 bps   | 0 B          | 0 B   |
| Traffic from ... | Out to PBX | Rest    | 10M          | 10M       | 0 bps   | 0 B          | 0 B   |
| call out         | Out to PBX | Voip... | 100k         | 100k      | 0 bps   | 0 B          | 0 B   |

3 items | 0 B queued | 0 packets queued

## Workflow del test



## Testing steps

Vamos a preparar 3 paquetes diferentes con Traffic Generator en el VoIPPhoneSimulator:

- Dos paquetes van a simular tráfico VoIP (Rtp y SIP)
- El otro paquete simulará tráfico desde RouterLan (con spoofing)
- Crearemos un stream con los paquetes anteriores.



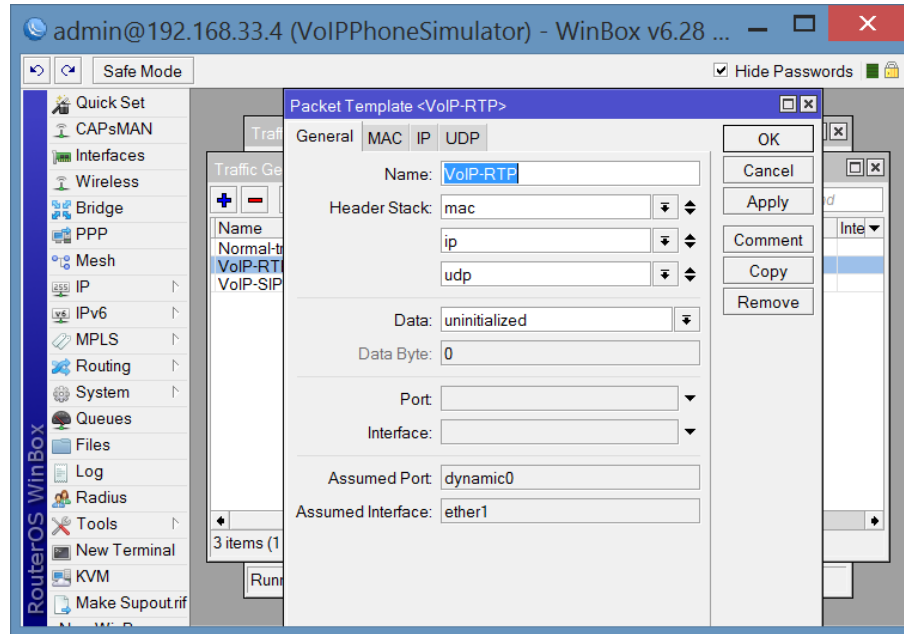
# Rtp packet

The screenshot shows the WinBox interface for RouterOS. The main window is titled "Traffic Generator Settings" and contains a sub-window titled "Traffic Generator Packet Templates". This sub-window displays a table of "Raw Packet Templates".

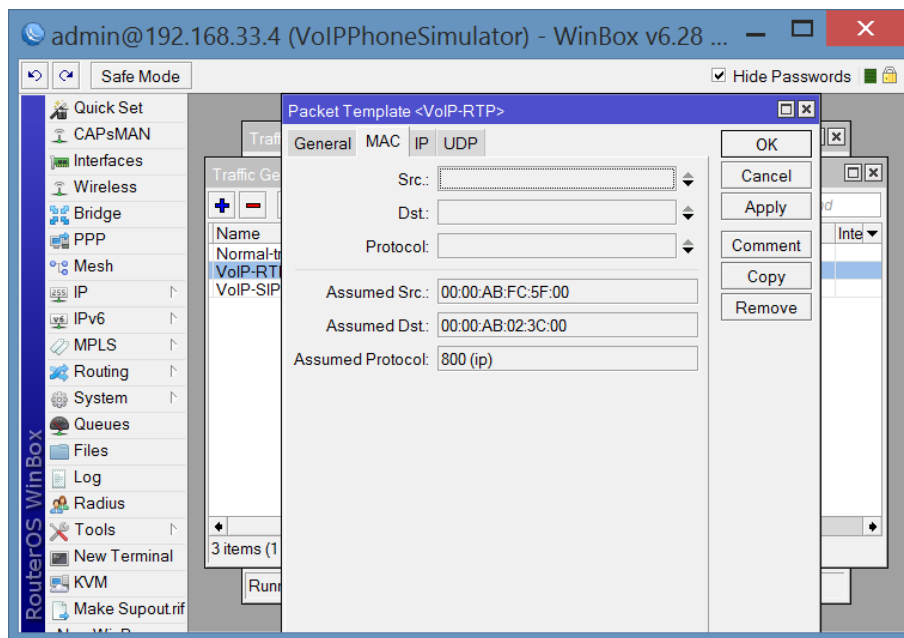
| Name                     | Header Stack | Data          | Data B... | Port | Inte |
|--------------------------|--------------|---------------|-----------|------|------|
| Normal-Traffic-RouterLan | mac, ip      | uninitialized |           |      |      |
| VoIP-RTP                 | mac, ip, udp | uninitialized |           |      |      |
| VoIP-SIP                 | mac, ip, udp | uninitialized |           |      |      |

At the bottom of the sub-window, it indicates "3 items (1 selected)" and "Running: no".

# Rtp packet

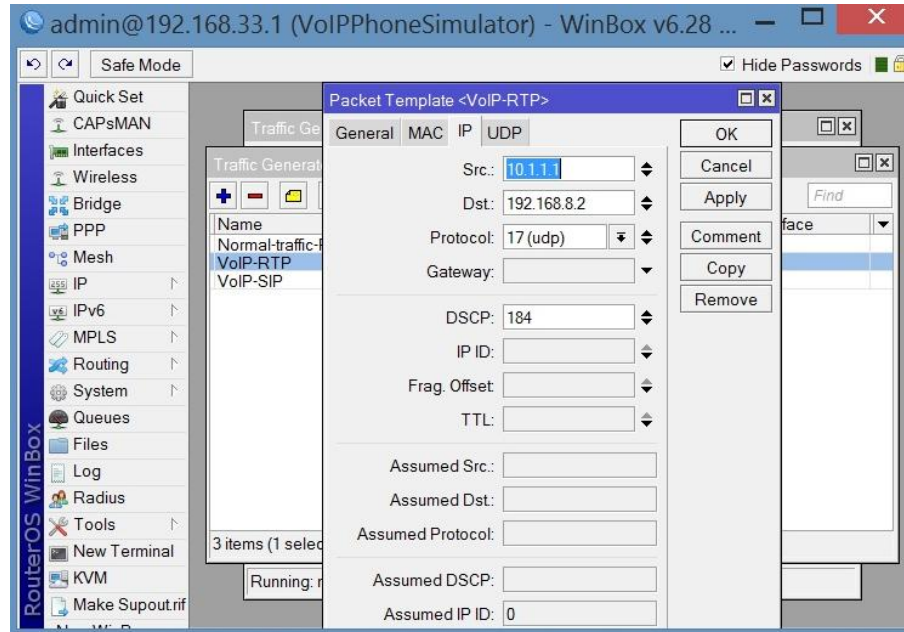


# Rtp packet



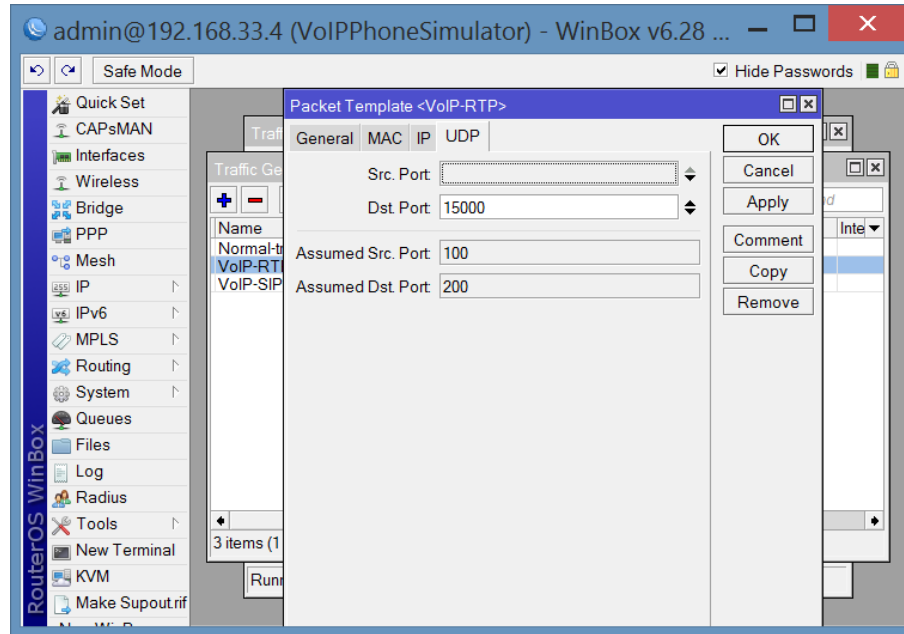


# Rtp packet



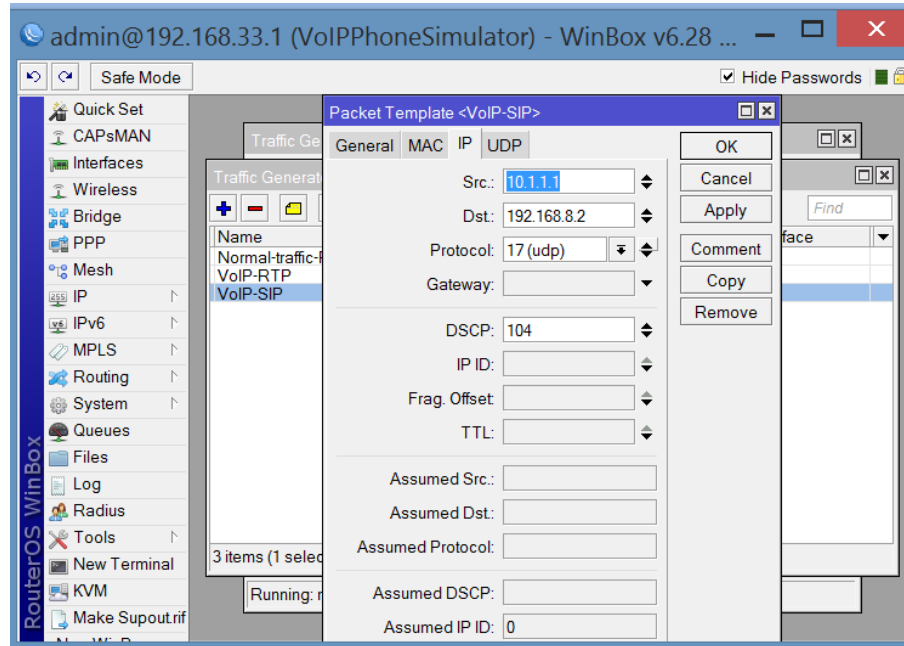


# Paquete Rtp

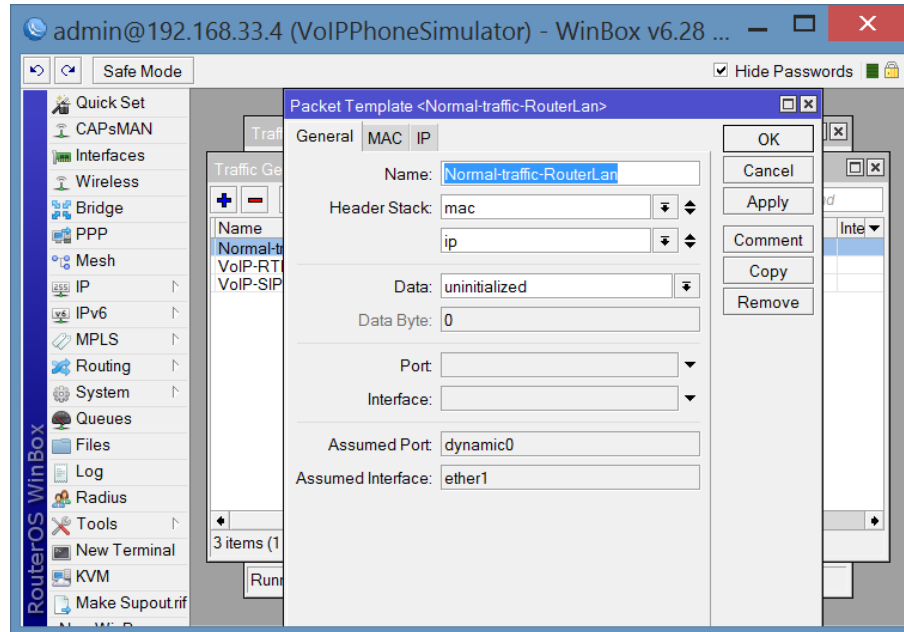




# Paquete SIP

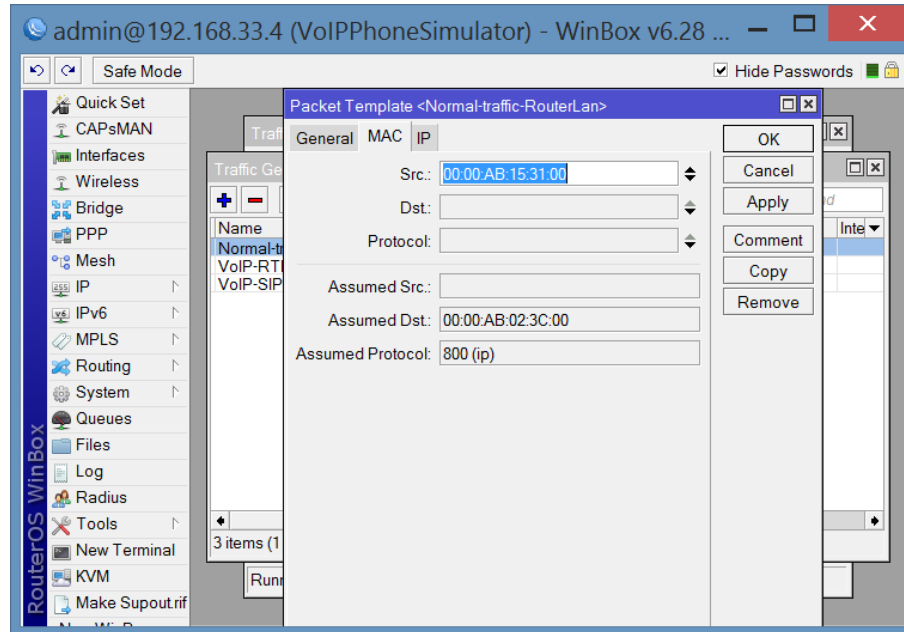


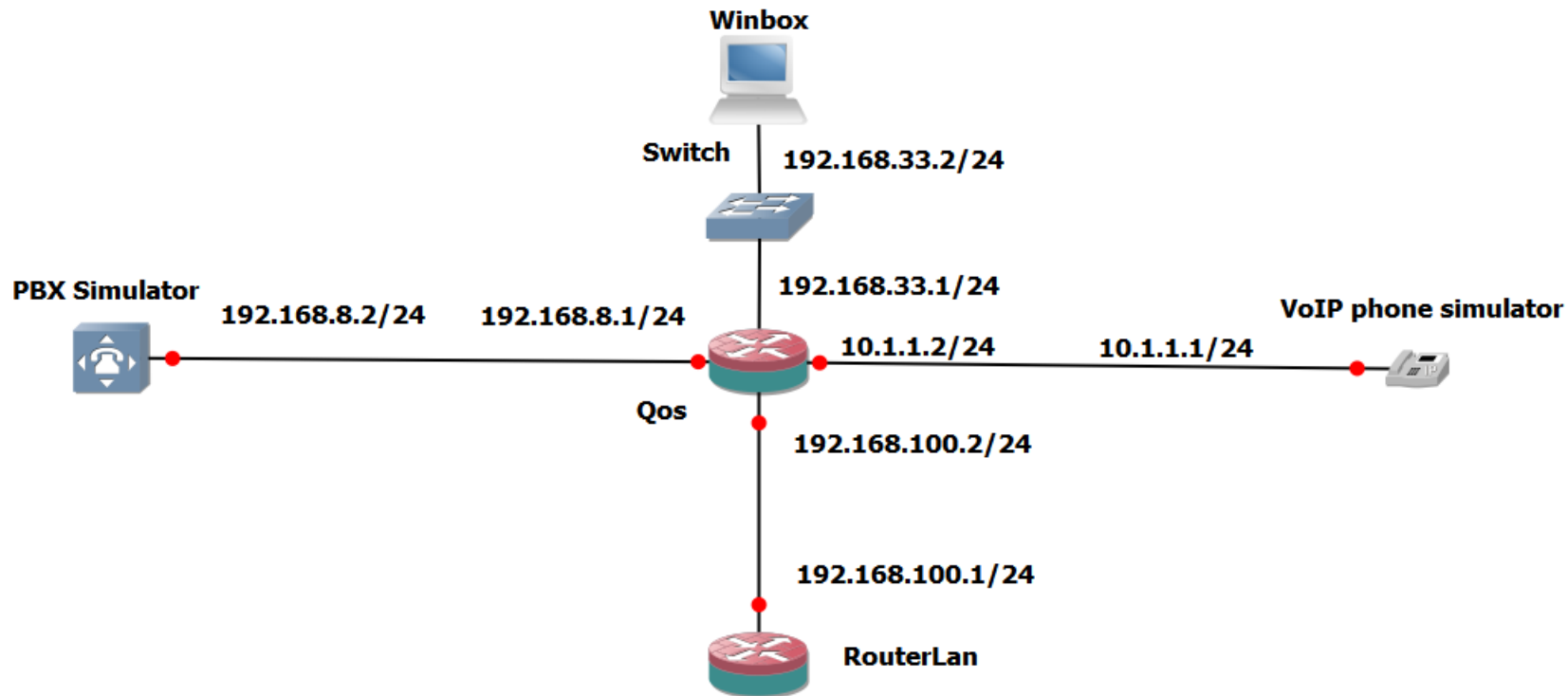
## Packet from RouterLan (Spoofing)



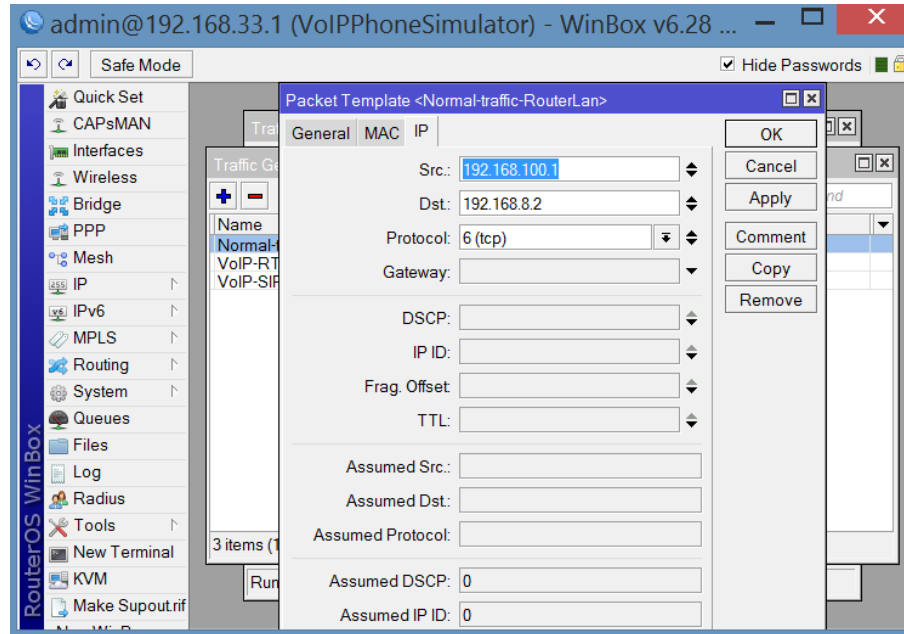


## Packet from RouterLan (Spoofing)





## Paquetes con RouterLan (Spoofing)





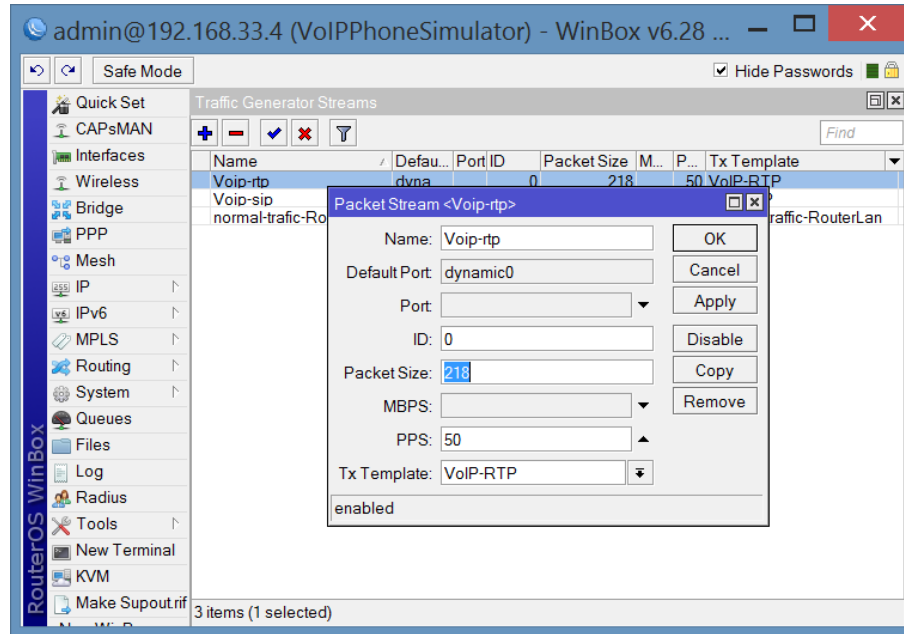
# Stream

The screenshot shows the WinBox v6.28 interface for a Mikrotik device. The title bar indicates the user is 'admin@192.168.33.4 (VoIPPhoneSimulator)'. The main window is titled 'Traffic Generator Streams' and contains a table with the following data:

| Name                     | Defau...     | Port ID | Packet Size | M... | P... | Tx Template              |
|--------------------------|--------------|---------|-------------|------|------|--------------------------|
| Voip-rtp                 | dyna...      | 0       | 218         |      | 50   | VoIP-RTP                 |
| Voip-sip                 | Default Port | 1       | 1500        |      | 1    | VoIP-SIP                 |
| normal-traffic-RouterLan | dyna...      | 2       | 1500        | 20   |      | Normal-traffic-RouterLan |

The interface also shows a sidebar with various configuration categories like CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, KVM, and Make Supoutrif. The status bar at the bottom indicates '3 items'.

# Stream



The screenshot shows the WinBox interface for a RouterOS instance. The main window is titled 'admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...'. The 'Traffic Generator Streams' window is open, displaying a table of streams. A dialog box titled 'Packet Stream <Voip-rtp>' is overlaid on the table, showing the configuration for the selected 'Voip-rtp' stream.

| Name              | Defau... | Port ID | Packet Size | M... | P... | Tx Template |
|-------------------|----------|---------|-------------|------|------|-------------|
| Voip-rtp          | dyna...  | 0       | 218         |      | 50   | VoIP-RTP    |
| Voip-sip          |          |         |             |      |      |             |
| normal-traffic-Ro |          |         |             |      |      |             |

The 'Packet Stream <Voip-rtp>' dialog box contains the following configuration:

- Name: Voip-rtp
- Default Port: dynamic0
- Port: [Dropdown]
- ID: 0
- Packet Size: 218
- MBPS: [Dropdown]
- PPS: 50
- Tx Template: VoIP-RTP
- enabled





# Stream

The screenshot shows the WinBox interface for a RouterOS device. The main window is titled "admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...". The "Traffic Generator Streams" window is open, displaying a table of streams. A "Packet Stream <Voip-sip>" dialog box is overlaid on top, showing configuration details for the selected stream.

| Name              | Default | Port ID | Packet Size | M... | P... | Tx Template |
|-------------------|---------|---------|-------------|------|------|-------------|
| Voip-tp           | dyna    | 0       | 218         |      | 50   | VoIP-RTP    |
| Voip-sip          |         |         |             |      |      |             |
| normal-traffic-Ro |         |         |             |      |      |             |

**Packet Stream <Voip-sip>**

Name: Voip-sip  
Default Port: dynamic0  
Port: [dropdown]  
ID: 1  
Packet Size: 1500  
MBPS: [dropdown]  
PPS: 1  
Tx Template: VoIP-SIP  
enabled



# Stream

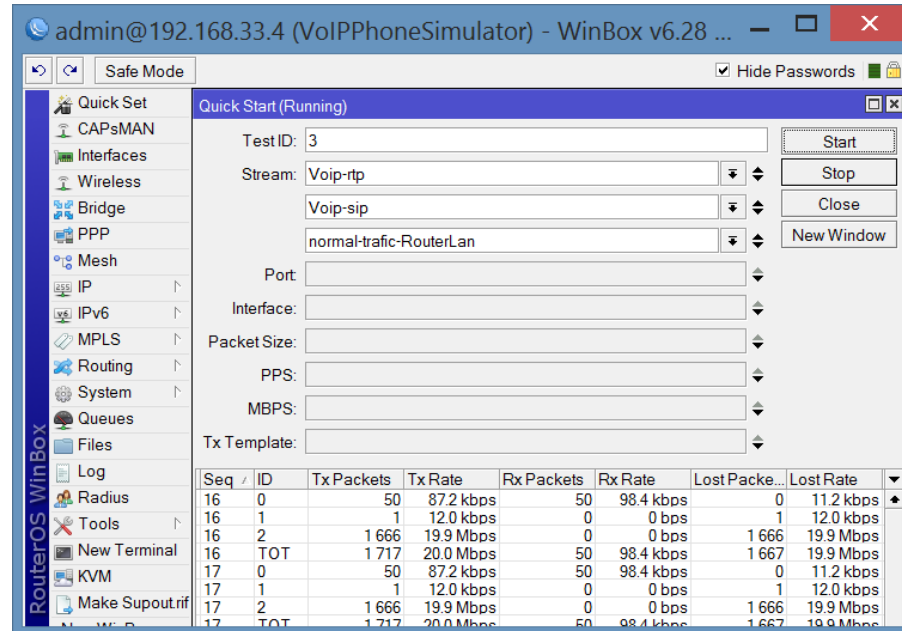
The screenshot shows the WinBox interface for a RouterOS device. The main window is titled "admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...". The "Traffic Generator Streams" window is open, displaying a table of streams. A dialog box for editing a stream named "normal-traffic-RouterLan" is overlaid on top.

| Name              | Defau... | Port ID | Packet Size | M... | P... | Tx Template |
|-------------------|----------|---------|-------------|------|------|-------------|
| Voip-rtp          | dyna     | 0       | 218         |      | 50   | VoIP-RTP    |
| Voip-sip          |          |         |             |      |      |             |
| normal-traffic-Ro |          |         |             |      |      |             |

**Packet Stream <normal-traffic-RouterLan>**

Name: normal-traffic-RouterLan  
Default Port: dynamic0  
Port: [dropdown]  
ID: 2  
Packet Size: 1500  
MBPS: 20  
PPS: [dropdown]  
Tx Template: Normal-traffic-RouterLan  
enabled

## Running the test



admin@192.168.33.4 (VoIPPhoneSimulator) - WinBox v6.28 ...

Safe Mode  Hide Passwords

Quick Start (Running)

Test ID: 3

Stream: Voip-rtsp

Voip-sip

normal-traffic-RouterLan

Port:

Interface:

Packet Size:

PPS:

MBPS:

Tx Template:

| Seq | ID  | Tx Packets | Tx Rate   | Rx Packets | Rx Rate   | Lost Packets | Lost Rate |
|-----|-----|------------|-----------|------------|-----------|--------------|-----------|
| 16  | 0   | 50         | 87.2 kbps | 50         | 98.4 kbps | 0            | 11.2 kbps |
| 16  | 1   | 1          | 12.0 kbps | 0          | 0 bps     | 1            | 12.0 kbps |
| 16  | 2   | 1666       | 19.9 Mbps | 0          | 0 bps     | 1666         | 19.9 Mbps |
| 16  | TOT | 1717       | 20.0 Mbps | 50         | 98.4 kbps | 1667         | 19.9 Mbps |
| 17  | 0   | 50         | 87.2 kbps | 50         | 98.4 kbps | 0            | 11.2 kbps |
| 17  | 1   | 1          | 12.0 kbps | 0          | 0 bps     | 1            | 12.0 kbps |
| 17  | 2   | 1666       | 19.9 Mbps | 0          | 0 bps     | 1666         | 19.9 Mbps |
| 17  | TOT | 1717       | 20.0 Mbps | 50         | 98.4 kbps | 1667         | 19.9 Mbps |



# Comprobando los resultados (Router QoS)

The screenshot shows the Mikrotik WinBox interface with the Firewall Filter Rules configuration page. The table displays the following data:

| #              | Action | Chain      | Src. Addr... | Dst. Addr... | Prot... | Src. Port | Dst. Port | In. Inte... | Out. In... | Bytes     | Packets |
|----------------|--------|------------|--------------|--------------|---------|-----------|-----------|-------------|------------|-----------|---------|
| Normal traffic |        |            |              |              |         |           |           |             |            |           |         |
| 0              | ma...  | prerouting | 192.168.1... | 192.168.8.2  |         |           |           |             |            | 70.6 MiB  | 49 835  |
| RTP traffic    |        |            |              |              |         |           |           |             |            |           |         |
| 1              | ma...  | prerouting |              |              |         |           |           |             |            | 297.8 KiB | 1 495   |
| SIP traffic    |        |            |              |              |         |           |           |             |            |           |         |
| 2              | ma...  | prerouting |              |              |         |           |           |             |            | 43.5 KiB  | 30      |



# Comprobando los resultados (Router QoS)

The screenshot shows the Mikrotik WinBox interface. The main window is titled "admin@192.168.33.1 (Qos) - WinBox v6.28 on x86 (x86)". The left sidebar shows the RouterOS menu with "Queues" selected. The main panel displays the "Queue List" configuration window, which is currently showing the "Simple Queues" tab. The configuration table is as follows:

| # | Name        | Parent     | Pack... | Limit At ... | Max Li... | Avg ...   | Queued By... | Bytes     | Pack... |
|---|-------------|------------|---------|--------------|-----------|-----------|--------------|-----------|---------|
| 0 | Out to P... | ether1     |         |              |           | 10.1 ...  | 0 B          | 131.7 ... | 96 707  |
| 1 | Traffi...   | Out to PBX | Rest    | 10M          | 10M       | 100 ...   | 70.3 KiB     | 130.4 ... | 91 191  |
| 2 | call out    | Out to PBX | Voip... | 100k         | 100k      | 99.2 k... | 0 B          | 1322...   | 5 564   |

At the bottom of the Queue List window, the summary statistics are:

- 3 items
- 70.3 KiB queued
- 48 packets queued



## Comprobando los resultados (Router QoS)

The screenshot shows the Mikrotik WinBox interface. The main window is titled "admin@192.168.33.1 (Qos) - WinBox v6.28 on x86 (x86)". The left sidebar shows the RouterOS menu with "Queues" selected. The main area displays the "Queue List" window, which is open to the "Statistics" tab for a queue named "call". The statistics are as follows:

| Statistic        | Value      |
|------------------|------------|
| Avg. Rate        | 99.2 kbps  |
| Avg. Packet Rate | 51         |
| Queued Bytes     | 0 B        |
| Queued Packets   | 0          |
| Bytes            | 2328.6 KiB |
| Packets          | 9 803      |
| Dropped          | 0          |
| PCQ Queues       |            |

The "Queue List" window also shows a table with 3 items (1 selected). The "Queue <call out>" window has buttons for "OK", "Cancel", "Apply", "Disable", "Comment", "Copy", "Remove", "Reset Counters", and "Reset All Counters".



# Muchas gracias

Contact: [jose.roman@cloudnetworking.es](mailto:jose.roman@cloudnetworking.es)