

# Securing and testing with Mikrotik

José Manuel Román

## About me

- 16 years' I.T. experience
- 7 years teaching networking
- 6 years security analyst
- CEO at Cloud Networking Spain (Wisp Provider)
- Network architect at Ipink.
- Bachelor of Computer Science.
- Master ITIL.
- Security Certifications: Cisa and Cispp
- Mikrotik Certifications: MTCINE, MTCNA, MTCRE, MTCTCE, MTCWE, MTCUME
- Mikrotik Certified Trainer
- Security consultant

## Objective

The objective of this presentation is to show the Mikrotik *tools* that help to *test* and *audit firewall* and Qos policies.

## Schedule

- Duration: 30 minutes
- Introduction: 5 minutes
- Scenario 1 Testing Synflood rules: 15 minutes
- Scenario 2 Testing VoIP queue tree: 10 minutes

## Problem

What to do when I need to test or audit if a router was enforcing QoS marking policies on incoming frames or was embracing complex security policies?

What to do when I need to teach QoS and complex firewall rules?



```

13 #my public addressing
14 add address=X.X.X.X comment="" disabled=no list=public-add
15
16 #my private addressing
17 add address=S.S.S.S/SS comment="" disabled=no list=internal-nets
18
19 #any port knock exclusions
20 add address=Y.Y.Y.Y comment="" disabled=no list=port-knock-3
21
22 #any SMTP exclusions
23 add address=Z.Z.Z.Z comment="" disabled=no list=smtp-bypass
24
25 /ip firewall filter
26 #match more than 5 pings in 5 seconds. Then drop the traffic inbound and forw
27 add action=accept chain=input comment="start of greg rules up to 5 pings in 5
28 add action=add-src-to-address-list address-list=icmp-attack address-list-timeo
29 disabled=no protocol=icmp
30 add action=drop chain=input comment="drop excessive icmp traffic for 12 hours"
31 add action=drop chain=forward comment="drop excessive icmp traffic for 12 hour
32 #drop 1918 inbound
33 add action=drop chain=forward comment="block rfc 1918 and multicast inbound" d
34 add action=drop chain=forward comment="block our addressing inbound - spoofed"
35 add action=drop chain=input comment="block rfc 1918 and multicast inbound" dis
36 add action=drop chain=input comment="block our addressing inbound - spoofed" d
37 #start port knocking
38 add action=add-src-to-address-list address-list=port-knock-1 address-list-time
39 dst-port=444 protocol=udp
40 add action=add-src-to-address-list address-list=port-knock-2 address-list-time
41 dst-port=117 protocol=udp src-address-list=port-knock-1
42 add action=add-src-to-address-list address-list=port-knock-3 address-list-time
43 dst-port=600 protocol=tcp src-address-list=port-knock-2
44 add action=accept chain=input comment="allow winbox in via port knock" disable
45 add action=drop chain=input comment="allow winbox in via port knock" disabled=
46 #port scans and DOS
47 add action=add-src-to-address-list address-list=port-scan address-list-timeout
48 in-interface=ether1 protocol=tcp psd=21,3s,3.1 src-address-list=!internal-
49 add action=add-src-to-address-list address-list=port-scan address-list-timeout
50 tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
51 add action=add-src-to-address-list address-list=port-scan address-list-timeout
52 fin,syn
53 add action=add-src-to-address-list address-list=port-scan address-list-timeout
54 syn,rst
55 add action=add-src-to-address-list address-list=port-scan address-list-timeout
56 fin,psh,urg,!syn,!rst,!ack
57 add action=add-src-to-address-list address-list=port-scan address-list-timeout
58 fin,svn,rst,psh,ack,urg

```

- August 2013
- July 2013
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012
- July 2012
- June 2012
- May 2012
- April 2012
- March 2012
- February 2012
- January 2012
- December 2011
- November 2011
- October 2011
- September 2011
- August 2011

## Firewall rules from Grew Sowel blog

## Symptoms

We have a complex configuration and we have no idea how to test it.

Students or clients asking us to demonstrate that setting works.

## Solution

# We need tools to test and teach



## Tools

There are a number of tools commonly used for testing or teaching networking that are present in mikrotik:

- Ping, Traceroute
- Real-time traffic monitoring and sniffer
- Traffic generator

## External tools

Similar to others that are not present in mikrotik:

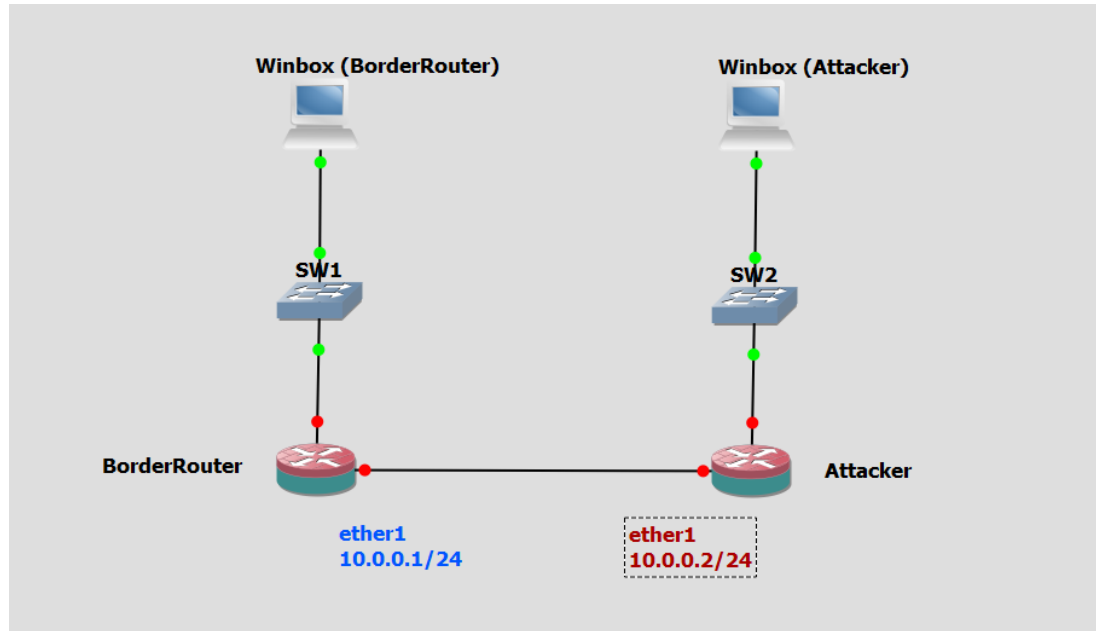
- Nmap and nping
- Hping3
- Scapy
- Wireshark

## First scenario

In this scenario we will test three sets of firewall rules to limit a synflood attack.



## Scenario 1



## TCP handshake

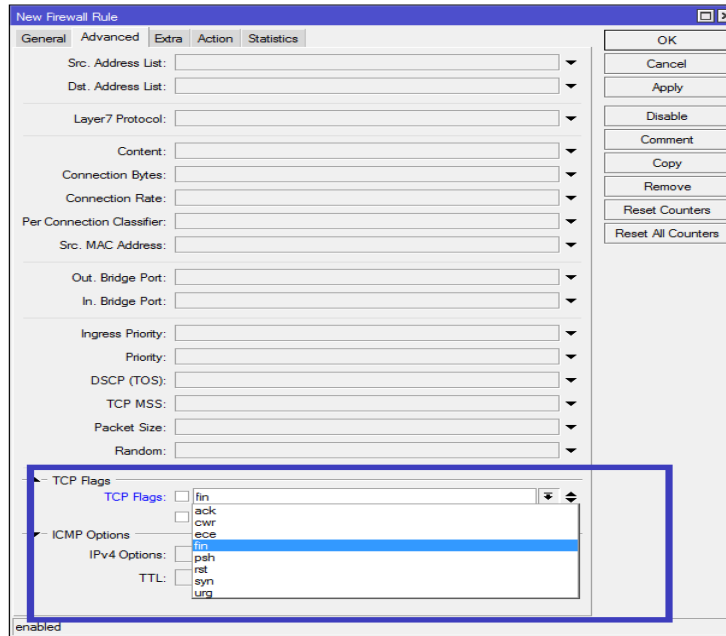
Normally when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

- Client requests a connection by sending a SYN (synchronize) message to the server.
- The server acknowledges this request by sending SYN-ACK back to the client.
- The client responds with an ACK, and the connection is established.



# TCP flags in Mikrotik firewall

## Where can I find the tcp flags in Mikrotik router?



## Attack(syn flood)

SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

## First scenario

### Testing synflood rules

- [Rules configuration.](#)
- Preparing the traffic generator to generate traffic with certain characteristics.
- Testing the rules with the previous traffic.



## First rule (Policy 1)

We configure a rule to try to stop or mitigate the attack:

```
/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:

- 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 window title is "admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...". 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". Other sections like "Dst. Limit", "Nth", "Time", "Src. Address Type", "Dst. Address Type", "PSD", "Hotspot", and "IP Fragment" are collapsed. The left sidebar contains various system and network configuration options.

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 "General" tab is also visible in the background.

## Survey online

Does policy 1 work?

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

- No, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the sinflood attack.

<http://freeonlinesurveys.com/s/JZxVzhiO>



## First scenario

### Testing synflood rules

- Rules configuration.
- Preparing the traffic generator to generate traffic with certain characteristics.
- Testing the rules with the previous traffic.

## Tool to test the policy

- Traffic Generator is a tool that allows to evaluate performance of DUT (Device Under Test) or SUT (System Under Test).
- Tool can generate and send RAW packets over specific ports. It also collects latency and jitter values, tx/rx rates, counts lost packets and detects Out-of-Order (OOO) packets.

<http://freeonlinesurveys.com/s/JZxVzhiO>



## Crafting with traffic generator



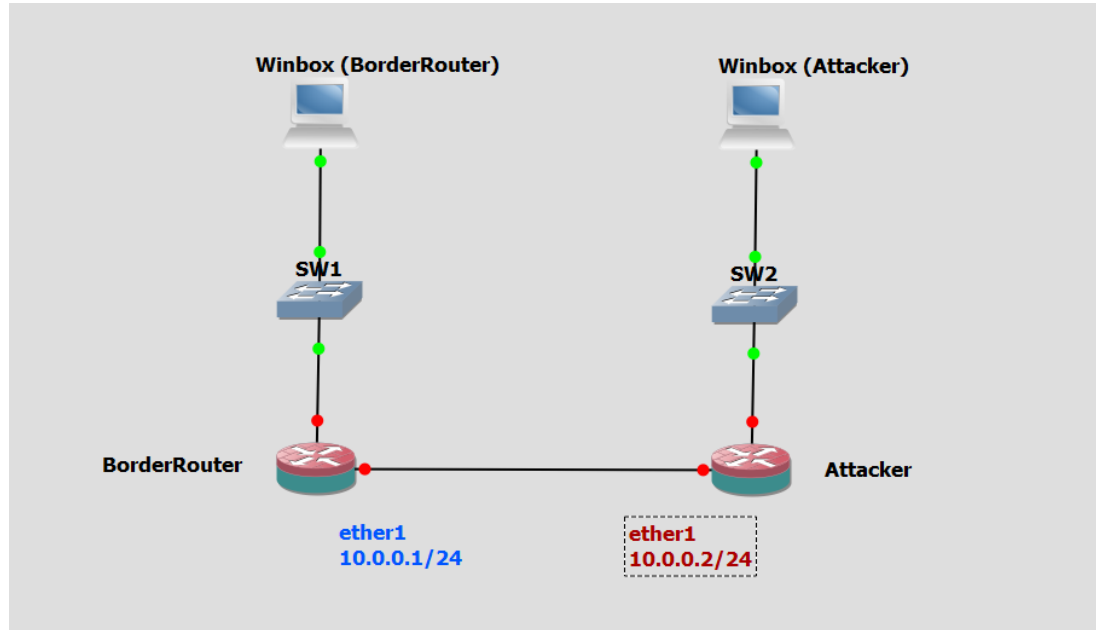
## Testing workflow







## Scenario 1



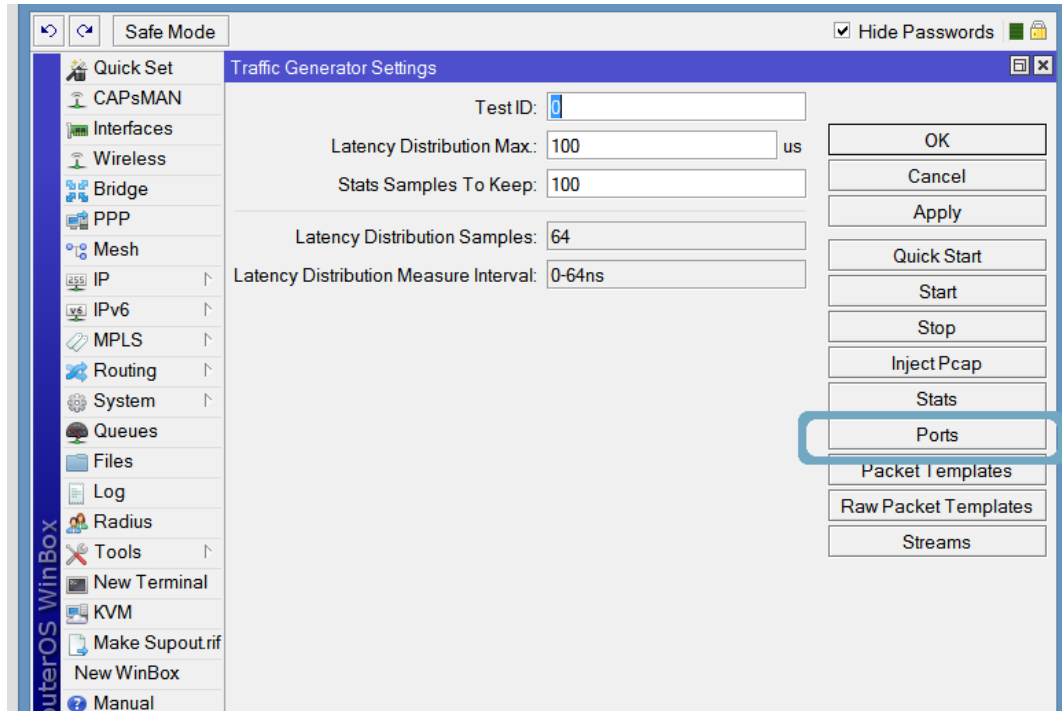
## First scenario

### Testing ynflood rules

- Rules configuration.
- Preparing the traffic generator to generate traffic with certain characteristics.
- Testing the rules with the previous traffic.



## Traffic Generator (Port)





# Traffic Generator (Port)

The screenshot shows the RouterOS 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 "Traffic Generator Port <port1>" dialog box 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)

The screenshot shows the WinBox interface for a RouterOS user. The main window is titled "Traffic Generator Settings" and contains the following fields and buttons:

- Test ID:
- Latency Distribution Max:  us
- Stats Samples To Keep:
- Latency Distribution Samples:
- Latency Distribution Measure Interval:

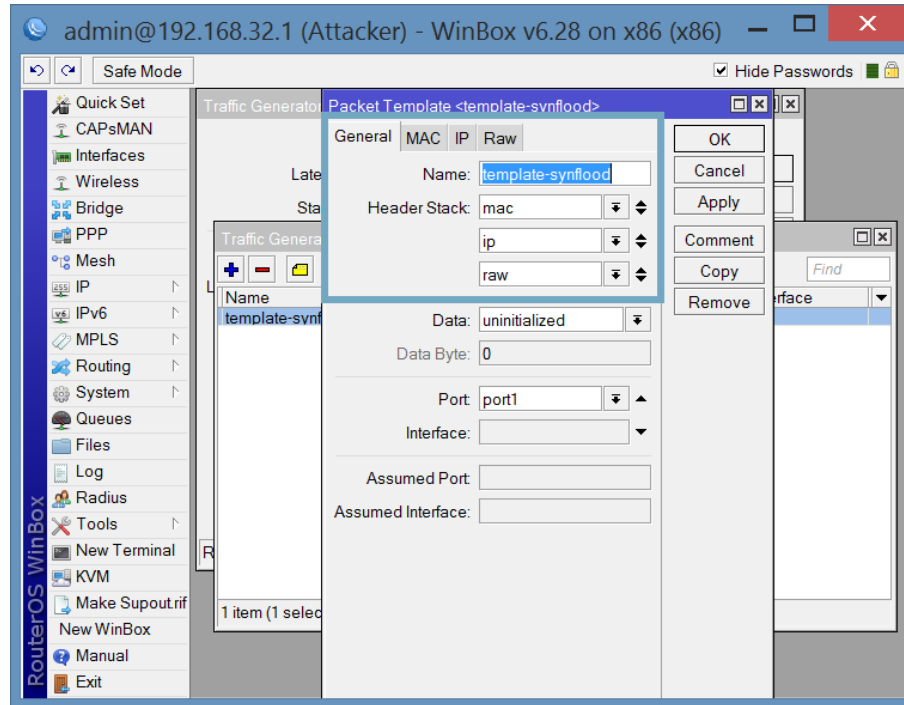
Buttons on the right side of the window:

- OK
- Cancel
- Apply
- Quick Start
- Start
- Stop
- Inject Pcap
- Stats
- Ports
- Packet Templates** (highlighted with a blue box)
- Raw Packet Templates
- Streams

At the bottom of the window, it says "Running: no".

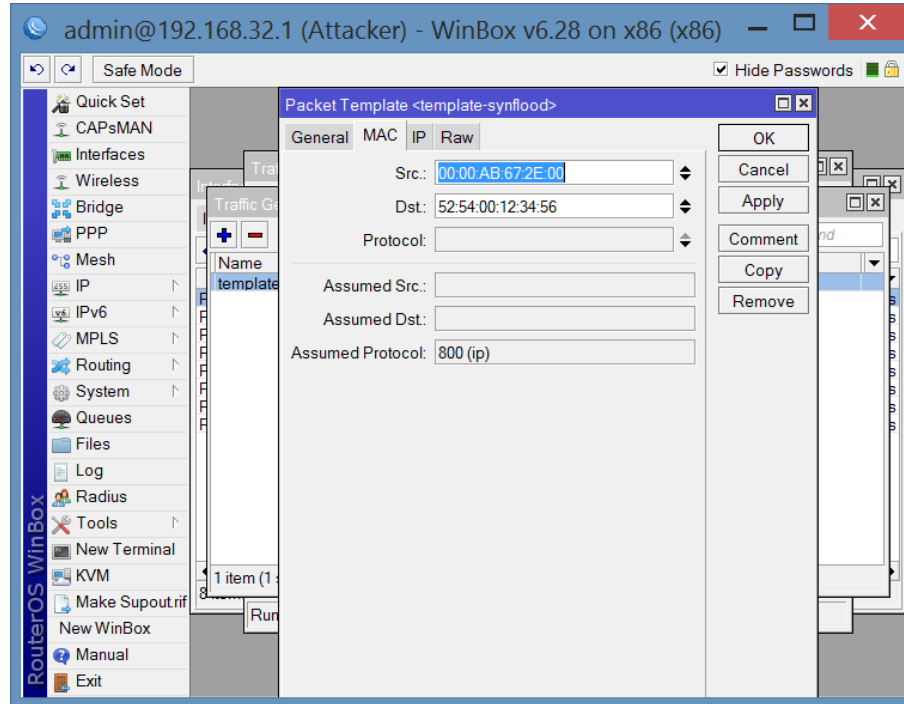


## Traffic Generator (Packet Template)





## Traffic Generator(Packet Template)





## Traffic Generator(Packet Template)

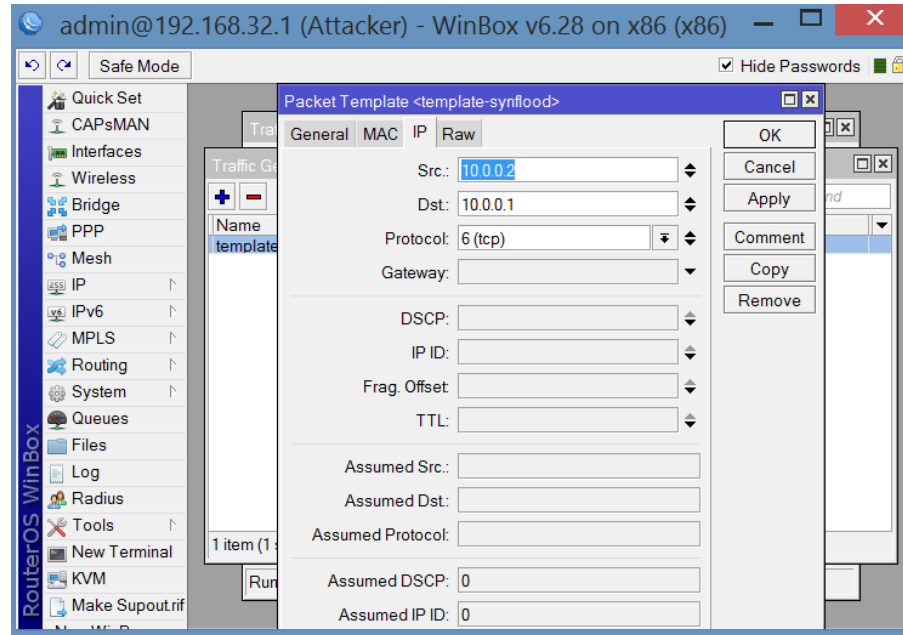
The screenshot shows the Mikrotik WinBox interface for configuring an interface. The 'Interface <ether1>' dialog box is open, showing the 'General' tab. The 'MAC Address' field is highlighted with a blue box and contains the value '00:00:AB:67:2E:00'. Below this, a 'Neighbor List' dialog box is also open, showing a table of neighbors. The 'MAC Address' column in the table is also highlighted with a blue box, and the value '52:54:00:12:34:56' is visible in the row for interface 'ether1'.

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



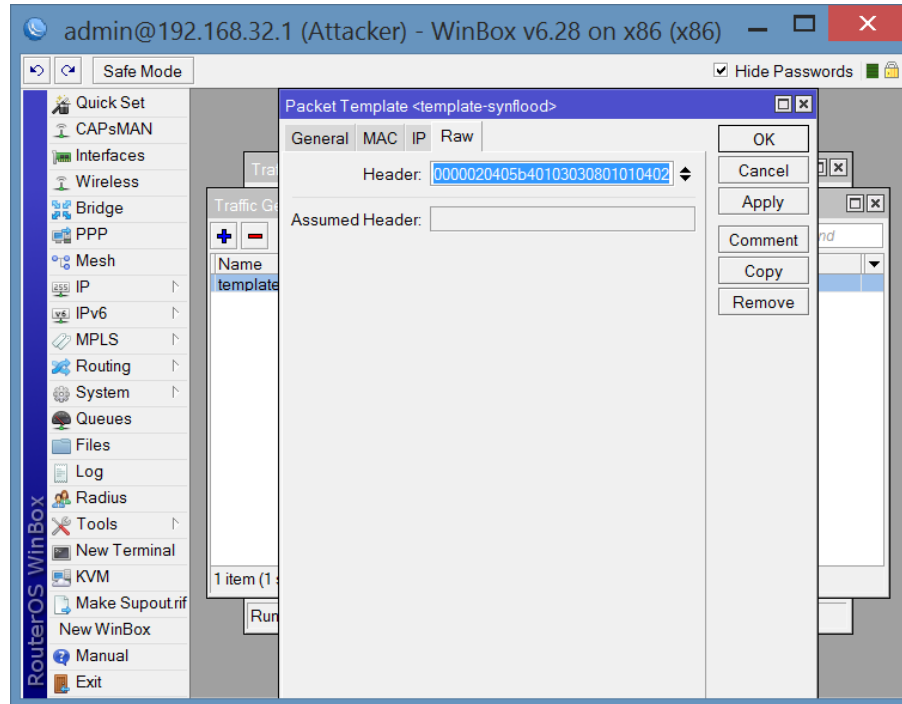


## Traffic Generator(Packet Template)

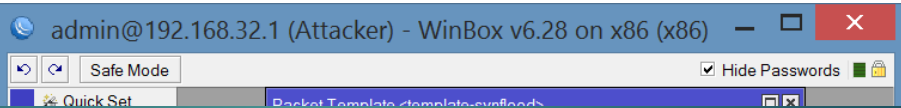


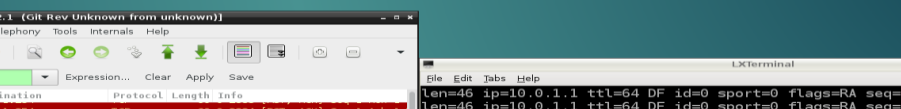


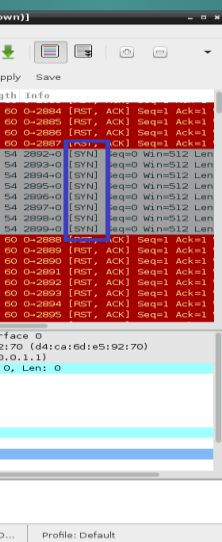
## Traffic Generator(Packet Template)

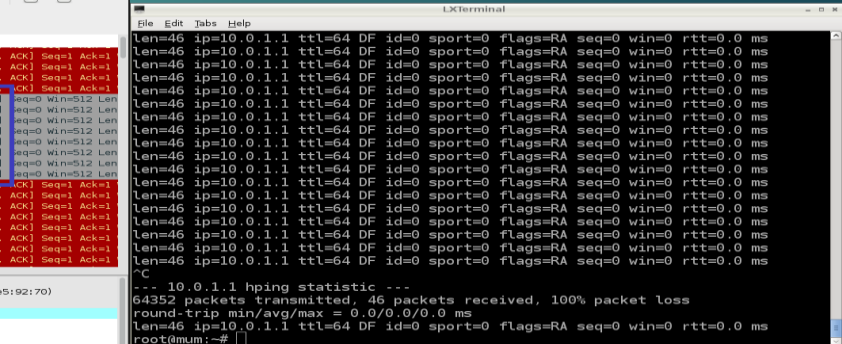


# Traffic Generator(Packet Template)











# Traffic Generator(Stream)

The screenshot shows the WinBox interface for a MikroTik router. The main window is titled "admin@192.168.32.1 (Attacker) - WinBox v6.28 on x86 (x86)". The left sidebar contains a menu with options 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 "Traffic Generator Settings" and "Traffic Generator Streams". 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".

## First scenario

### Testing ynflood rules

- Rules configuration.
- Preparing the traffic generator to generate traffic with certain characteristics.
- Testing the rules with the previous traffic.



# Traffic Generator(Quick start)

The screenshot shows the WinBox interface with the 'Quick Start' window open. The configuration is as follows:

- Test ID: 0
- Stream: synflood
- Port: port1
- Interface: (empty)
- Packet Size: (empty)
- PPS: (empty)
- MBPS: (empty)
- Tx Template: (empty)

Buttons on the right: 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



# Border Router Counters (policy 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 "Firewall" tab is active, and the "Filter Rules" sub-tab is selected. The "Reset Counters" and "Reset All Counters" buttons are visible. A table lists the filter rules, with "Policy 1" selected. The table has columns for #, Action, Chain, Src. Addr., Dst. Addr., Prot., Src. Port, Dst. Port, In. Inte..., Out In..., Bytes, and Packets. The status of each rule is shown in the first column: 0 (X), 1 (X), 2 (X), 3 (X), 4 (X), 5 (X), and 6 (X). The "Action" column shows "loa" for rules 0-1, "drop" for rule 2, and "drop" for rules 3-6. The "Chain" column shows "input" for all rules. The "Prot." column shows "6 (tc...)" for rules 0-3 and "6 (tc...)" for rules 4-6. The "Bytes" and "Packets" columns show "0 B" and "0" for all rules. The status bar at the bottom indicates "7 items (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 drop	input			6 (tc...					0 B	0
5	X ac. sym-flood									0 B	0
6	X drop sym-flood									0 B	0

## Survey online

Does policy 1 work?

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

- No, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the sinflood attack.



## Policy 1

No, this rule doesn't drop packets  
Because the attacker never established connections and there is a  
connection limit that doesn't apply

## Policy 2

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

<http://freeonlinesurveys.com/s/JZxVzhiO>



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 configuration:

- 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 "Extra" tab selected. The window title is "admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...". The configuration includes:

- 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 (x86)

Safe Mode  Hide Passwords

Firewall Rule <>

General Advanced Extra Action Statistics

Connection Limit

Limit

Rate: 20 /sec

Burst: 1

Dst. Limit

Nth

Time

Src. Address Type

Dst. Address Type

PSD

Hotspot

IP Fragment

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

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

Safe Mode  Hide Passwords

Firewall Rule <>

General Advanced Extra Action Statistics

Action: drop

Log

Log Prefx: policy 2

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

## Survey online

Does policy 2 work?

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

- No, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the sinflood attack.

<http://freeonlinesurveys.com/s/JZxVzhiO>



# Why the counters are incremented 40 every 2 seconds?

The screenshot shows the Mikrotik WinBox interface for Firewall Filter Rules. The table below represents 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

## Survey online

Does policy 2 work?

The rule works but doesn't limit the attack  
In this case only drops 20 packets every second

<http://freeonlinesurveys.com/s/JZxVzhiO>

## Policy 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
```

<http://freeonlinesurveys.com/s/JZxVzhiO>



## Survey online

Does policy 3 work?

```
/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, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the synflood attack.



<http://freeonlinesurveys.com/s/JZxVzhiO>

## Policy 3 (First rule)

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

<http://freeonlinesurveys.com/s/JZxVzhiO>



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 "Extra" tab selected. The window title is "admin@fe80::4e5e:cff:fe38:6710%2 (Lab) - WinBox v6.27 on RB2011i...". The "Extra" 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**

enabled

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

## Policy 3 (Second rule)

```
/ip firewall filter  
add chain=syn-flood limit=100,5
```



<http://freeonlinesurveys.com/s/JZxVzhiO>



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: **accept**

Log

Log Prefix:



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

- Connection Limit
- Limit
  - Rate: 100 / sec
  - Burst: 5
- Dst Limit
- Nth
- Time
- Src. Address Type
- Dst. Address Type
- PSD
- Hotspot
- IP Fragment

## Policy 3 (Third rule)

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



<http://freeonlinesurveys.com/s/JZxVzhiO>





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:

## Survey online

Does policy 3 work?

```
/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, this rule doesn't drop packets
- The rule works but doesn't limit the attack
- Yes, it limits the synflood attack.

<http://freeonlinesurveys.com/s/JZxVzhiO>

## Survey online

Does policy 3 work?

```
/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
```

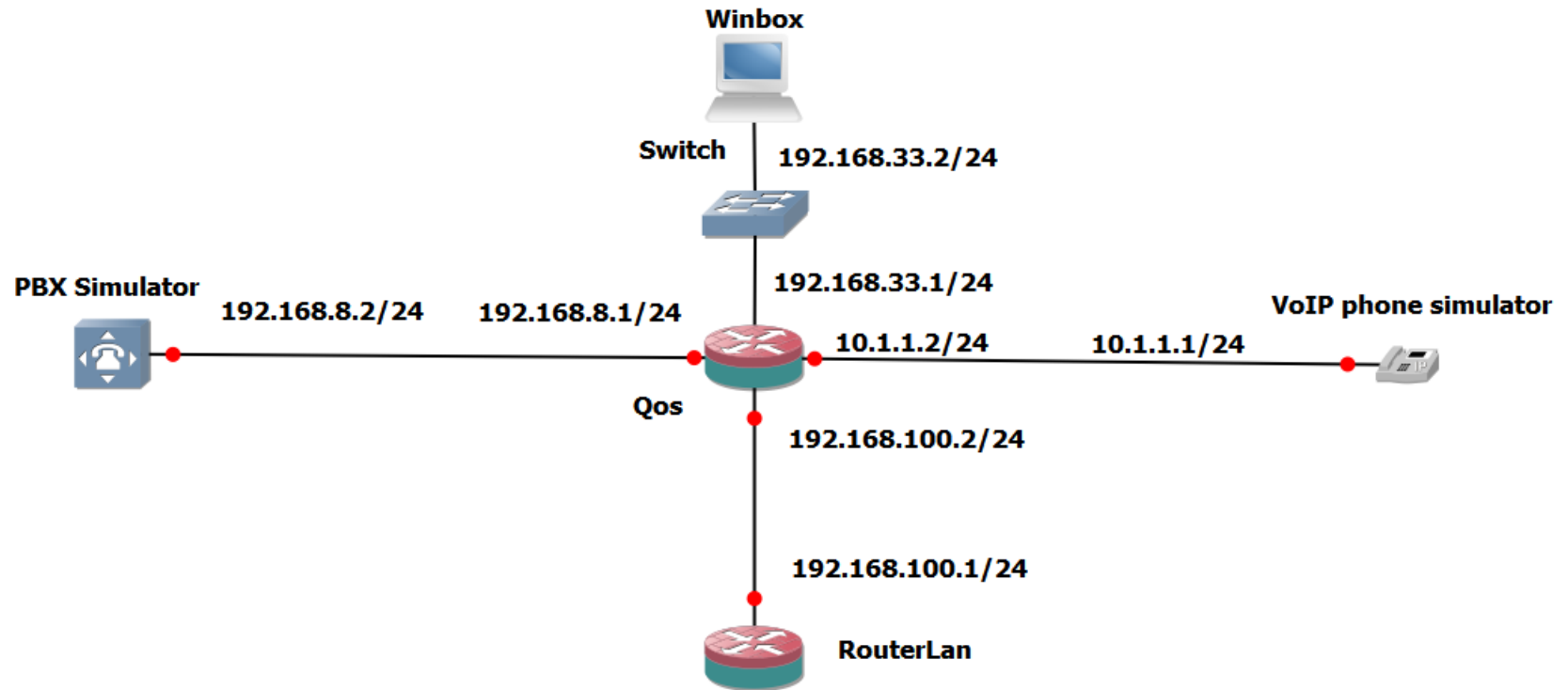
Yes, it limits the synflood attack.

<http://freeonlinesurveys.com/s/JZxVzhiO>



## Scenario 2 (Testing QoS)

In this laboratory we will test  
packet marking configuration and queue tree



## Router Configuration

```
[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

## Router Configuration

```
[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

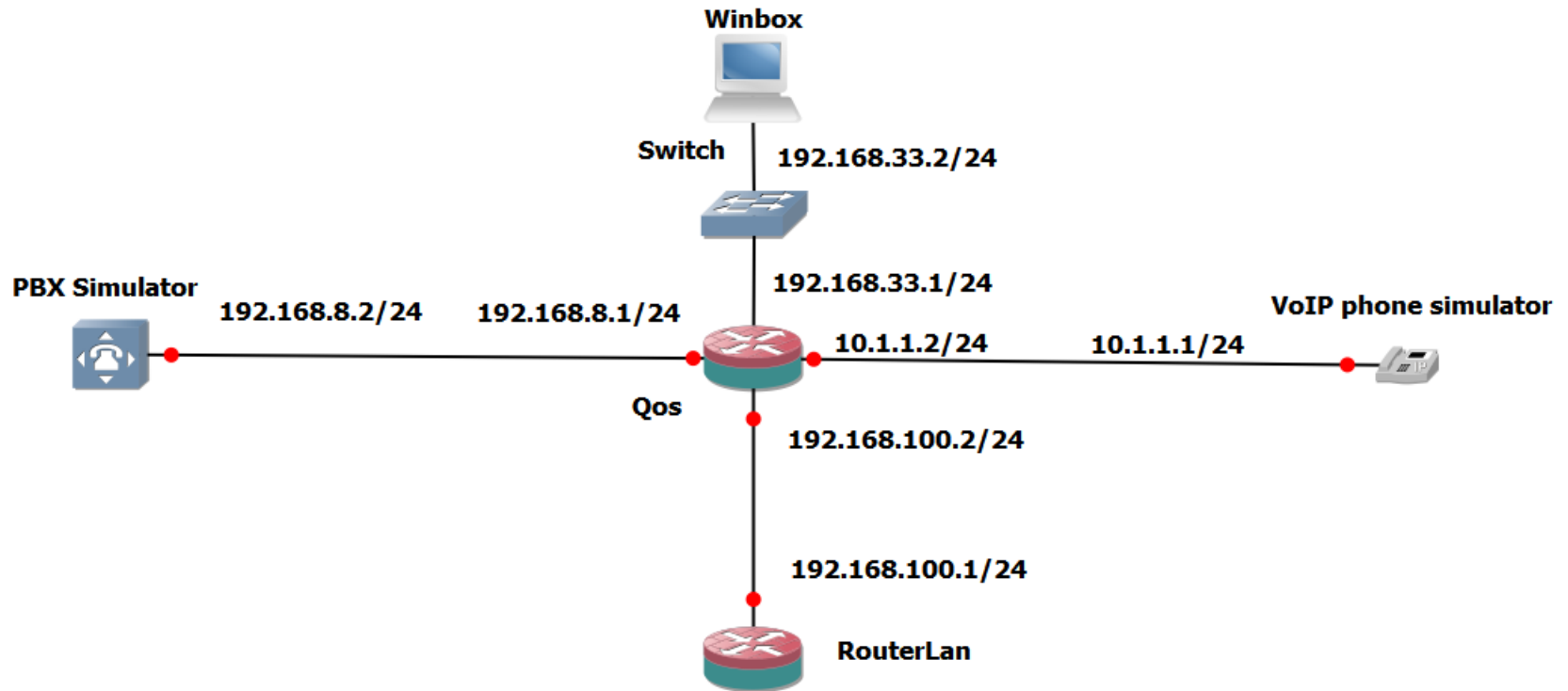
## Router Configuration

```
[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





## Scenario 2

in this case we will try a queue tree configuration that prioritizes voice traffic. QoS router has mangle rules and queue tree limitations.

## 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=""
```

## Dscp values Voip calls

SIP signaling messages will be marked by DSCP value of 26

## Dscp values Voip calls

RTP voice audio data will be marked by DSCP value of 46

## 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=""
```

## 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

The screenshot shows the WinBox interface for RouterOS. The 'Queue List' window is open, displaying a table of queues. The 'Queue Tree' tab is selected, showing a hierarchical structure of queues. The table has columns for Name, Parent, Pack..., Limit At..., Max Li..., Avg..., Queued By..., and Bytes. The data shows three queues: 'Out to PBX' (parent: ether1), 'Traffic from ...' (parent: Out to PBX), and 'call out' (parent: Out to PBX). The status bar at the bottom indicates 3 items, 0 B queued, and 0 packets queued.

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



## Testing workflow



## Testing steps

We will prepare 3 different packets with Traffic Generator in VoIPPhoneSimulator Router:

- Two packets will simulate VoIP traffic (Rtp and SIP)
- The other packet we'll simulate traffic from RouterLan (with spoofing)
- We create a stream with the three previous packets

## Dscp values Voip calls

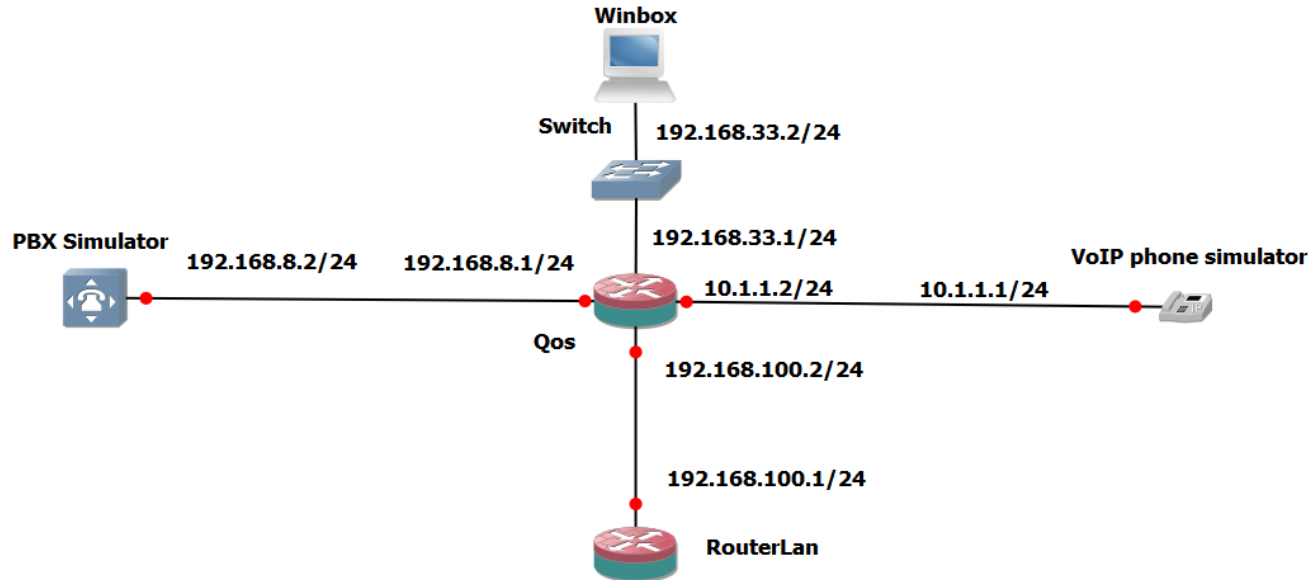
SIP signaling messages will be marked by DSCP value of 26  
A DSCP value of 26 results in a ToS byte value of 104  $AF31=0x68$   
(=104)

## Dscp values Voip calls

RTP voice audio data will be marked by DSCP value of 46  
A DSCP value of 46 results in a ToS byte value of 184 EF=0xB8



# Scenario 2





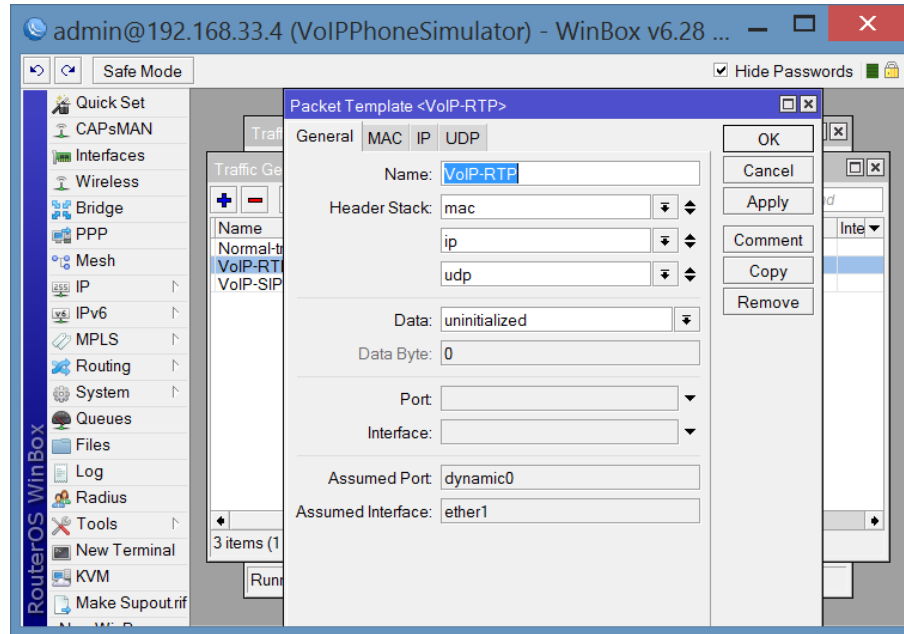
# Rtp packet

The screenshot shows the WinBox interface for RouterOS. The main window is titled "Traffic Generator Packet Templates" and displays a table of raw packet templates. The table has columns for Name, Header Stack, Data, Data B..., Port, and Inte. Three templates are listed: Normal-traffic-RouterLan, VoIP-RTP (which is selected), and VoIP-SIP. Below the table, it indicates "3 items (1 selected)" and "Running: no".

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			

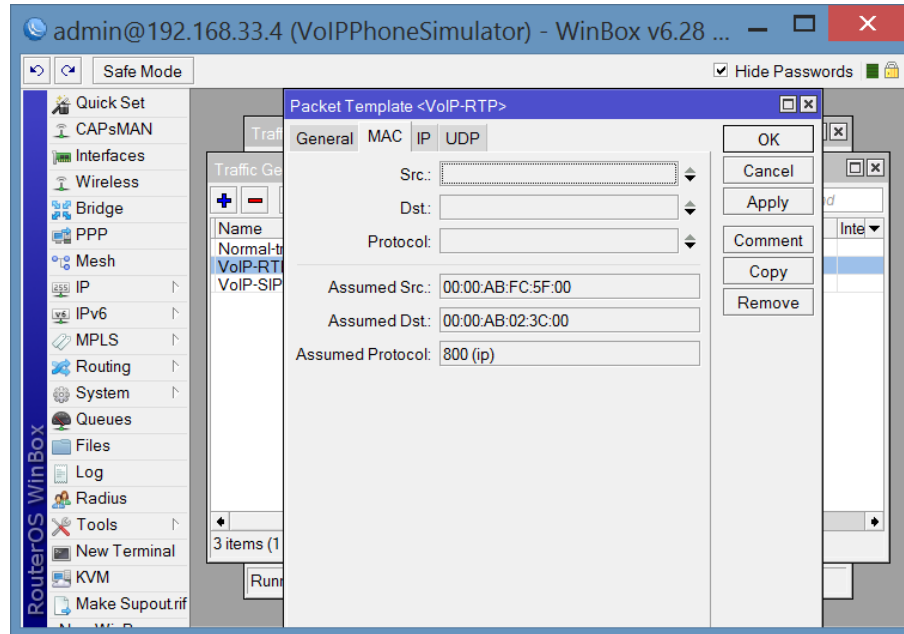


# Rtp packet





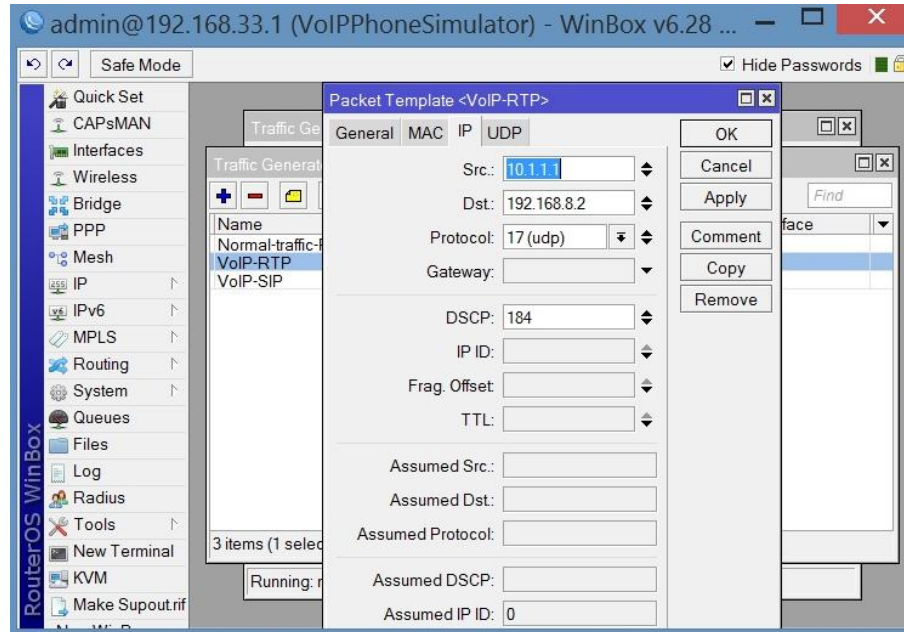
# Rtp packet





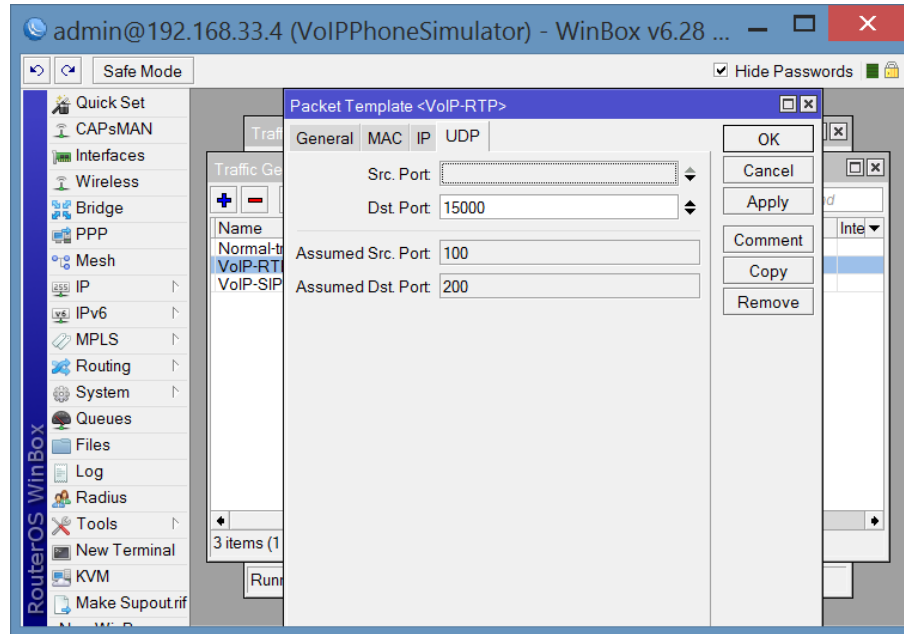


## Rtp packet



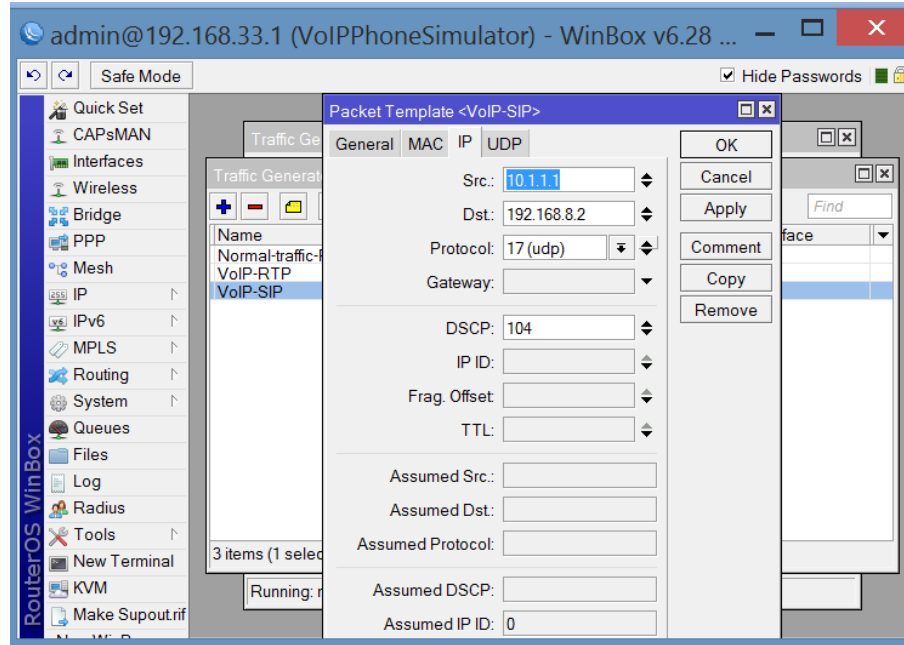


# Rtp packet



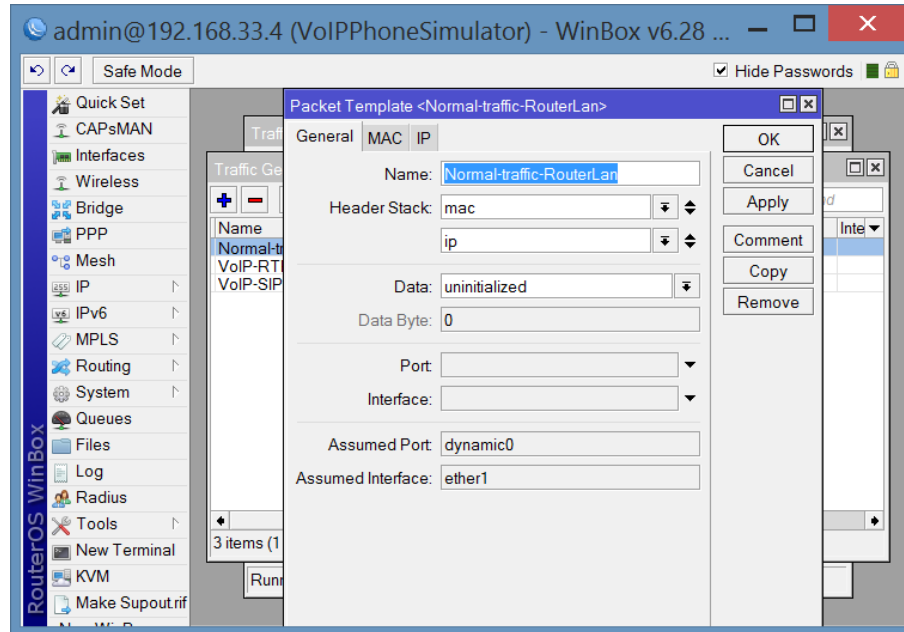


# SIP Packet



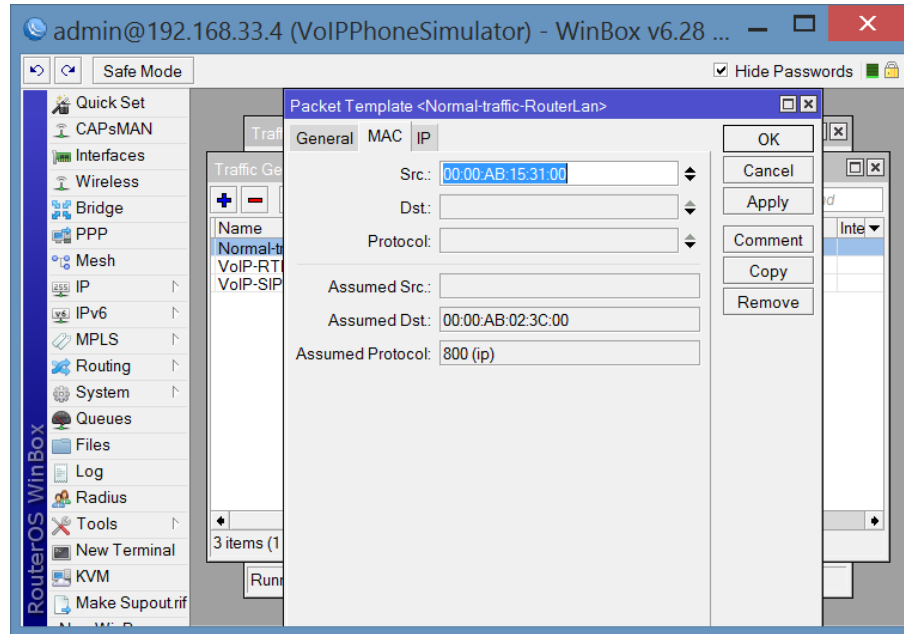


## Packet from RouterLan (Spoofing)



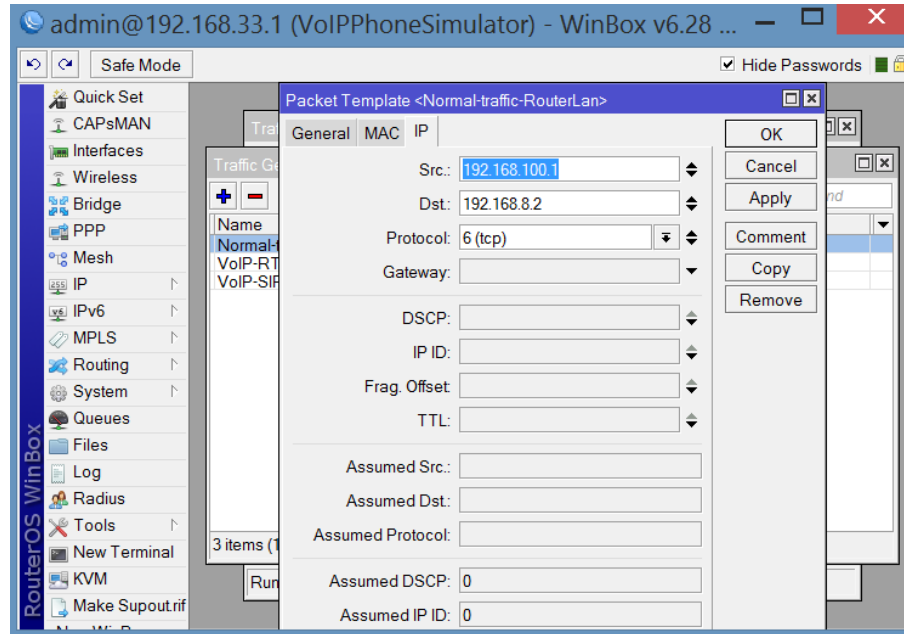


## Packet from RouterLan (Spoofing)





## Packets from RouterLan (Spoofing)





# Stream

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



# Stream

The screenshot shows the WinBox interface for RouterOS. 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 stream. The configuration includes:

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

The dialog box "Packet Stream <Voip-rtp>" contains the following fields and controls:

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

Buttons: OK, Cancel, Apply, Disable, Copy, Remove.





# Stream

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

- Name: Voip-sip
- Default Port: dynamic0
- Port: (dropdown menu)
- ID: 1
- Packet Size: 1500
- MBPS: (dropdown menu)
- PPS: 1
- Tx Template: VoIP-SIP

Buttons: OK, Cancel, Apply, Disable, Copy, Remove. Status: enabled



# 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 left sidebar contains a tree view of system components, with 'RouterOS WinBox' highlighted. The main area displays the 'Traffic Generator Streams' configuration page. A table lists several streams, with 'normal-traffic-RouterLan' selected. A dialog box is open over this stream, showing the following configuration:

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

Stream: Voip-rtsp [Stop]

Voip-sip [Close]

normal-traffic-RouterLan [New Window]

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



## Checking the results (Router QoS)

The screenshot shows the WinBox interface for a MikroTik router. The 'Firewall' tab is active, and the 'Filter Rules' sub-tab is selected. The table below displays the configuration and statistics for three filter rules:

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



## Checking the results (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 "Queues" menu item is selected in the left sidebar. The "Queue List" dialog box is open, showing a table of queue configurations. The table has columns for Name, Parent, Pack., Limit At..., Max Li..., Avg..., Queued By..., Bytes, and Pack... The data rows are:

Name	Parent	Pack.	Limit At...	Max Li...	Avg...	Queued By...	Bytes	Pack...
Out to P...	ether1				10.1...		0 B 131.7...	96 707
Traffi...	Out to PBX	Rest	10M	10M	100.0...		70.3 KiB 130.4...	91 191
call out	Out to PBX	Voip...	100k	100k	99.2 k...		0 B 1322...	5 564

At the bottom of the dialog box, it shows "3 items", "70.3 KiB queued", and "48 packets queued".



# Checking the results (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 "Queue List" configuration window is open, showing 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 list of queues with columns for Name, Out to, Traffic, and Call. The "call" queue is selected.

## Disclaimer

The information provided on this presentation are for educational purposes only. The author is no way responsible for any misuse of the information.



# Thanks a lot Hvala!

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

Thanks a lot to Fajar Nugroho

<https://freeonlinesurveys.com/app#/795807/analyze/-1>



## References

- <http://mum.mikrotik.com/presentations/HR13/legend.pdf>
- <http://mum.mikrotik.com/presentations/HR13/maia.pdf>
- <http://mum.mikrotik.com/presentations/HR13/kirnak.pdf>
- [http://mum.mikrotik.com/presentations/BR11/1\\_Maia.pdf](http://mum.mikrotik.com/presentations/BR11/1_Maia.pdf)
- [http://mum.mikrotik.com/presentations/CY15/Denial\\_of\\_Service\\_Attack.pdf](http://mum.mikrotik.com/presentations/CY15/Denial_of_Service_Attack.pdf)
- <https://tools.ietf.org/html/bcp38>
- [http://www.mikrotikbrasil.com.br/artigos/Layer2\\_Security\\_Poland\\_2010\\_Maia.pdf](http://www.mikrotikbrasil.com.br/artigos/Layer2_Security_Poland_2010_Maia.pdf)

The labs are available for gns3