

# Mikrotik User Meeting 2018

Dusit Thani Hotel

Makati, Philippines

January 16 2018



# Introduction.



## **CYGNAL TECHNOLOGIES**

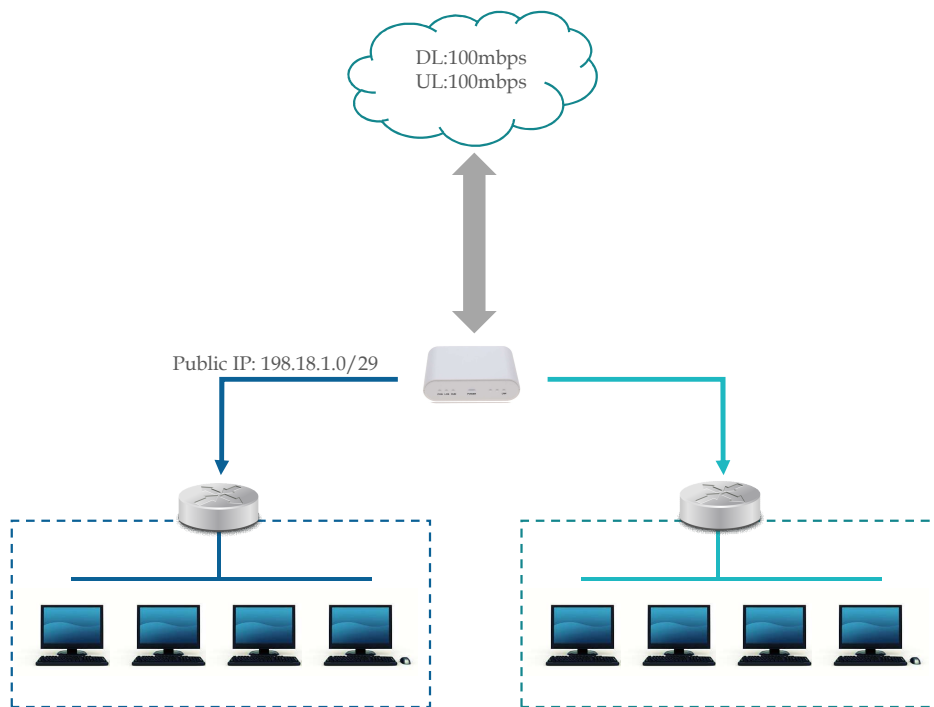
- ❖ Cygnal Technologies was established in the Middle East since 1997-2013 (under the name Cygnal and PCTek)
  - Internet Dial-up and VSAT Provider for military service contractors.
- ❖ Established in the Philippines since 2013
- ❖ Registered Internet Provider
- ❖ Been using and implementing Mikrotik RouterOS since late 1999-Present
- ❖ IT Solution provider
  - Network Infrastructure consultation and commissioning
  - Mikrotik consultation and deployment
  - Cloud Hosting Provider
  - Software Development
  - Wireless and Hotspot solution provider
  - Public Hotspot operator.



**CYGNALTECHNOLOGIES**

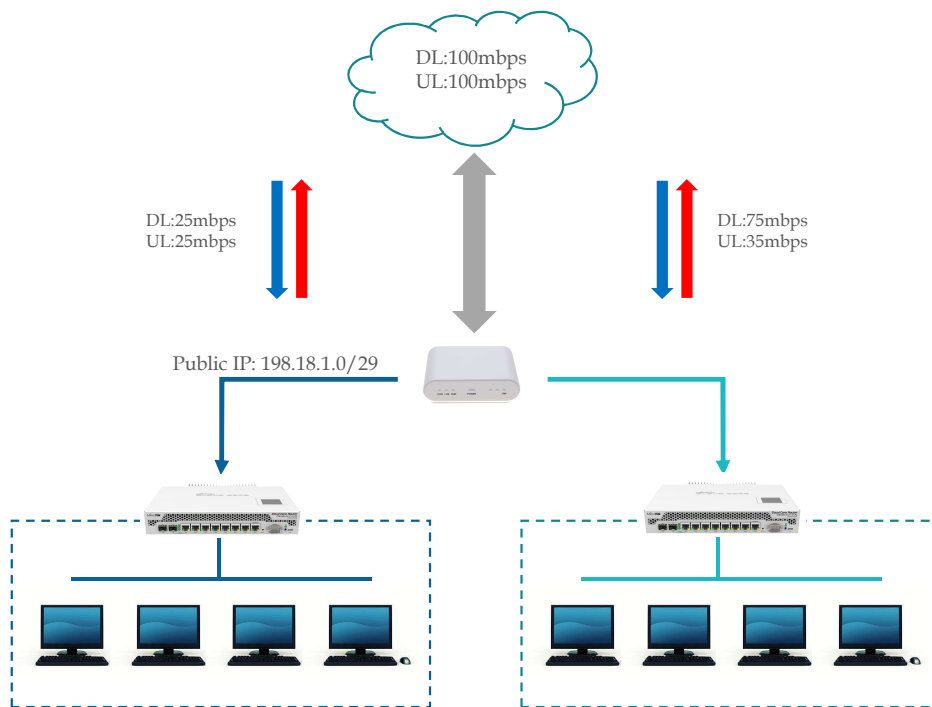


# The Current setup:



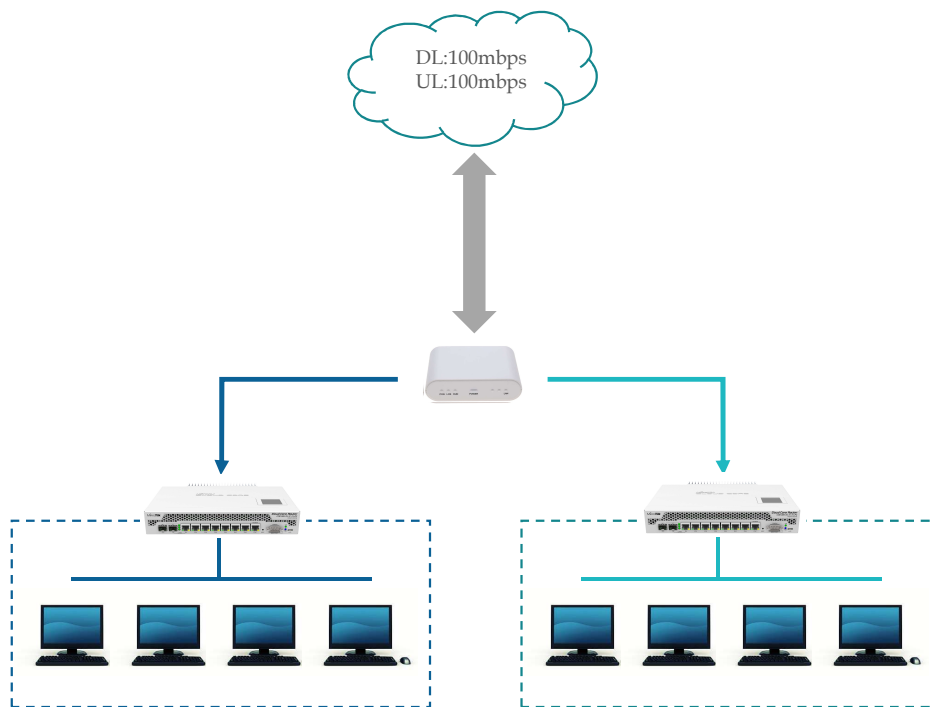
- The ISP allocated the network with small public ip-block of /29, all public IP must be assigned to the routers, and clients should NOT be natted.
- The network router is a non-mikrotik router with its own proprietary services and security protocols and is connected to the remote router located overseas.
- Workstations has a specific route provided by the non-mikrotik router to reach other devices on the remote side.

# The Task (and considerations):



- Provide a scalable Bandwidth management for each network.
- Not to replace the existing core router
- Not to make any changes to current infrastructure (e.g. IP addressing, Routing, Firewall, VPN, Security, etc.)
- Minimal Downtime < 1~2 mins.
- Provide Hotspot.
- And a provision for a NATTED LAN.

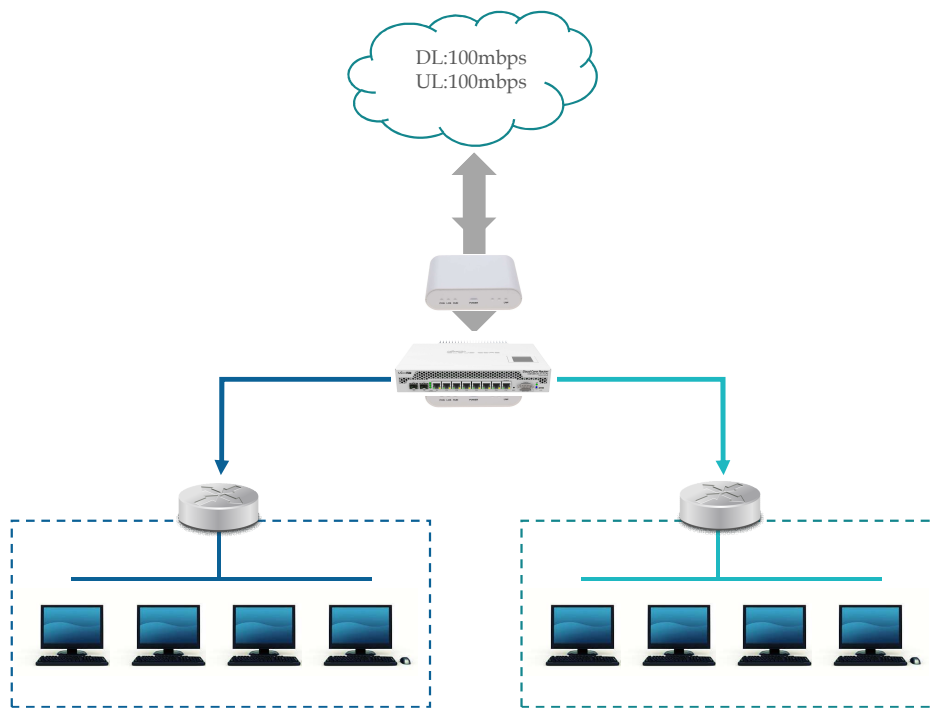
# Possible Solution



- X** Replace the current router with Mikrotik?
- It breaks all proprietary connectivity and security.

**CYGNAL TECHNOLOGIES**

## Solution:

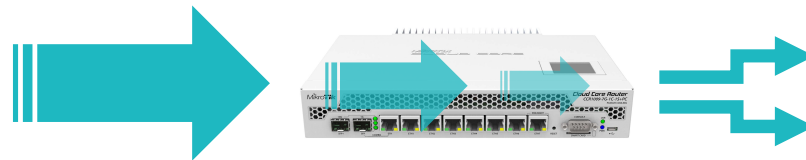


- Add a Mikrotik router just right after the fiber modem.
- And make it transparent.

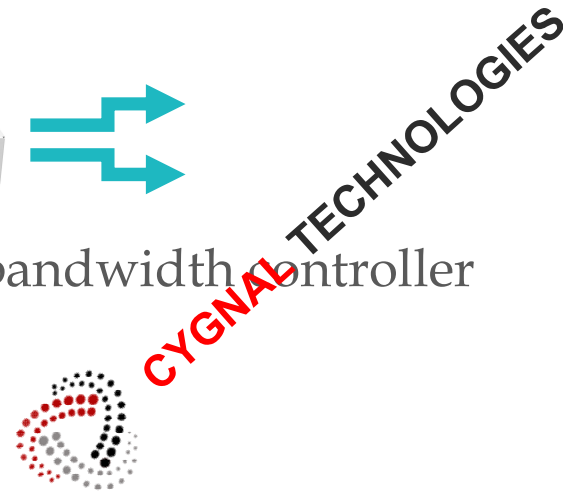
What mode should we use?



Router mode?  
-or-  
Bridged mode?



Mikrotik as IN-LINE transparent bandwidth controller



# In-Line Devices

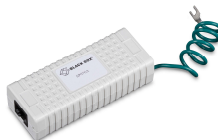
## ■ What is an inline network device?

- A device that can be installed between two or more network devices that can perform specific function, it receives the packets and forwards them to intended destination, it can enhance or alter the data in transit.
- It operates at Layer-2 (data link) and some operates at L2 and L3
- It is transparent and end devices are not aware of its presence.

### Non-Intrusive in-line devices



Coupler  
To extend  
Cable length



Surge  
Protector



PoE

These taps does not alter the data in transit

### Intrusive in-line devices



Network Sniffer  
Tap



Appliance bandwidth  
Controller

These taps can alter the data in transit





Exinda Appliance

It's a WAN optimization appliance

- It controls the traffic (Layer 2 and above)
- Application accelerator
- Application Visibility
- Cache Server
- Monitoring and reporting
- Can be set as in-line network device

Effectively used in a slow network such as the VSAT systems.

Price is based on the WAN bandwidth,

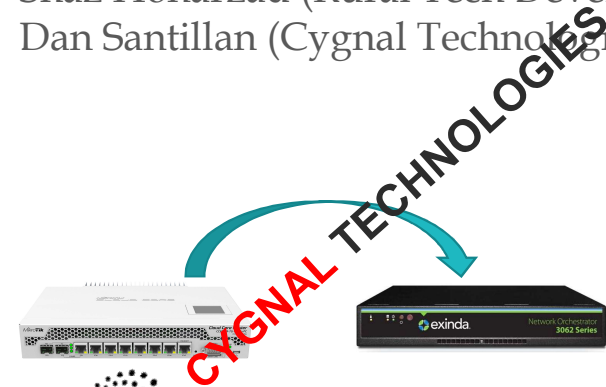
A 2mbps wan costs US\$1,000 and for 100mbps WAN priced at US\$6,500

**CYGNAL TECHNOLOGIES**

# Rural Tech Development (Papua New Guinea)



- Shaz Honarzad (Rural Tech Development)
- Dan Santillan (Cygnal Technologies)



Make Mikrotik to function similar to Exinda

By the way.. They are hiring now!

Need 2 Mikrotik engineers

# Lets make Mikrotik to function like Exinda!



## 3 Steps Configuration

1. Attach the ports to a bridge.
2. Create a Bridge Filter
3. Create the bandwidth limit

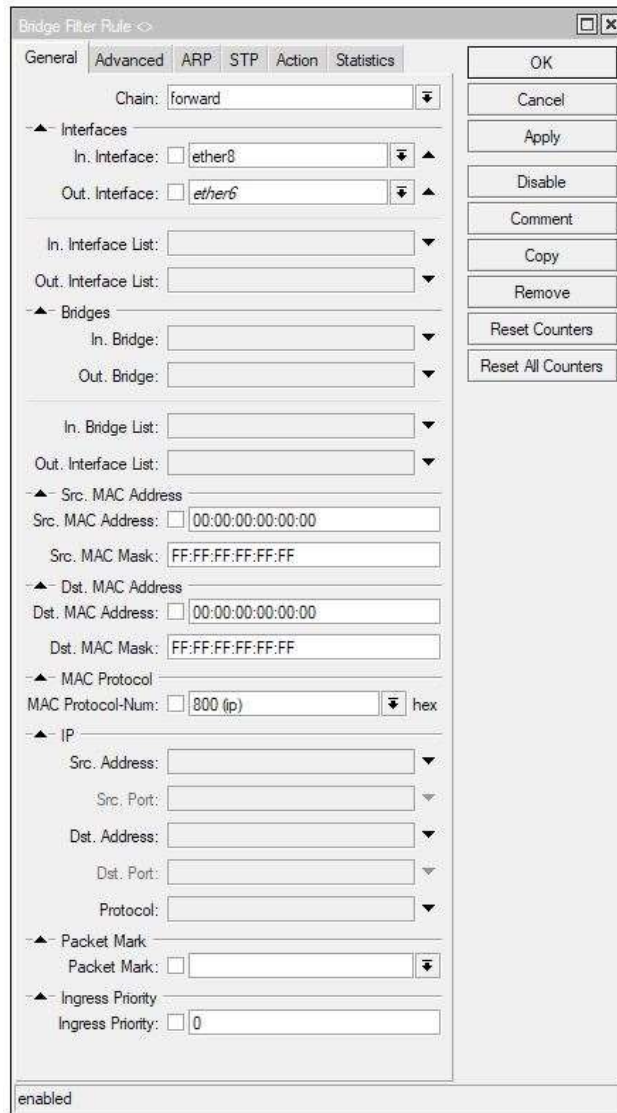


**CYGNAL TECHNOLOGIES**

***Note:** There's already a Transparent Traffic Shaper entry at mikrotik wiki using a simple method.*

I used a different approach here and you can see the difference.

I separated the **ingress** and **egress** traffic by identifying the physical IN and OUT port, and by doing so, it gives more flexibility to further use of Layer 2 fields through the bridge filter. I did not use the mangle to mark the necessary packets due to its lacking of layer-2 fields.



Bridge Filter Rule <>

General | Advanced | ARP | STP | Action | Statistics

Chain: forward

Interfaces

In. Interface: ether8

Out. Interface: ether6

In. Interface List:

Out. Interface List:

Bridges

In. Bridge:

Out. Bridge:

In. Bridge List:

Out. Interface List:

Src. MAC Address

Src. MAC Address: 00:00:00:00:00:00

Src. MAC Mask: FF:FF:FF:FF:FF:FF

Dst. MAC Address

Dst. MAC Address: 00:00:00:00:00:00

Dst. MAC Mask: FF:FF:FF:FF:FF:FF

MAC Protocol

MAC Protocol-Num: 800 (ip)

IP

Src. Address:

Src. Port:

Dst. Address:

Dst. Port:

Protocol:

Packet Mark

Packet Mark:

Ingress Priority

Ingress Priority: 0

enabled

OK

Cancel

Apply

Disable

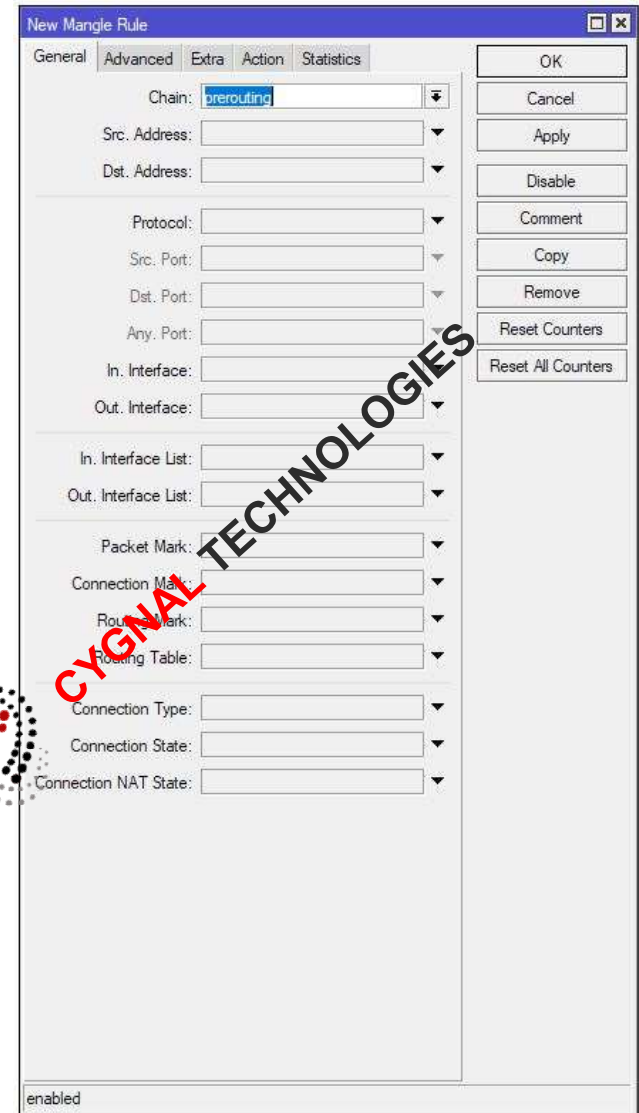
Comment

Copy

Remove

Reset Counters

Reset All Counters



New Mangle Rule

General | Advanced | Extra | Action | Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

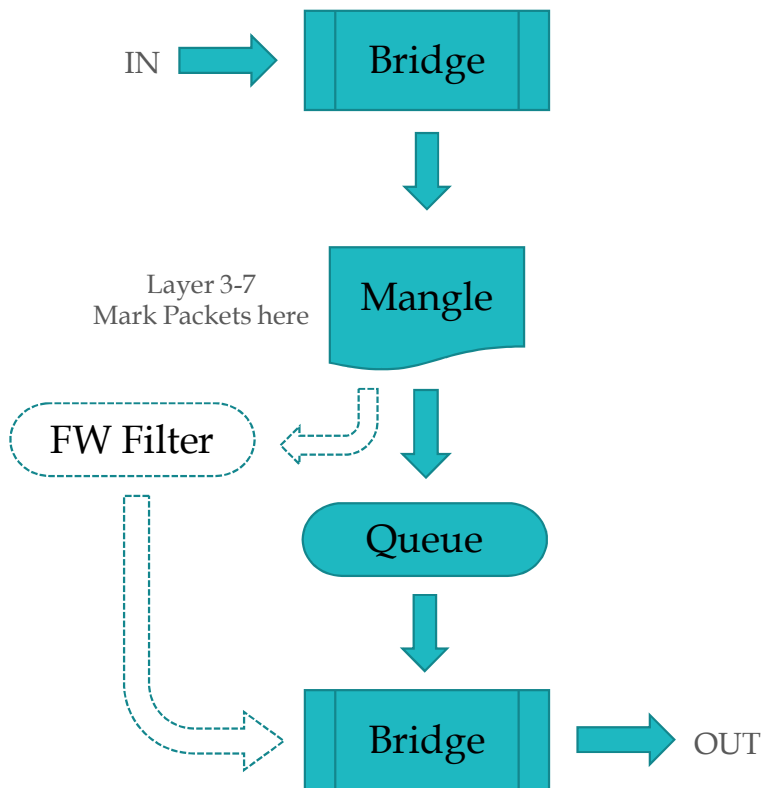
Remove

Reset Counters

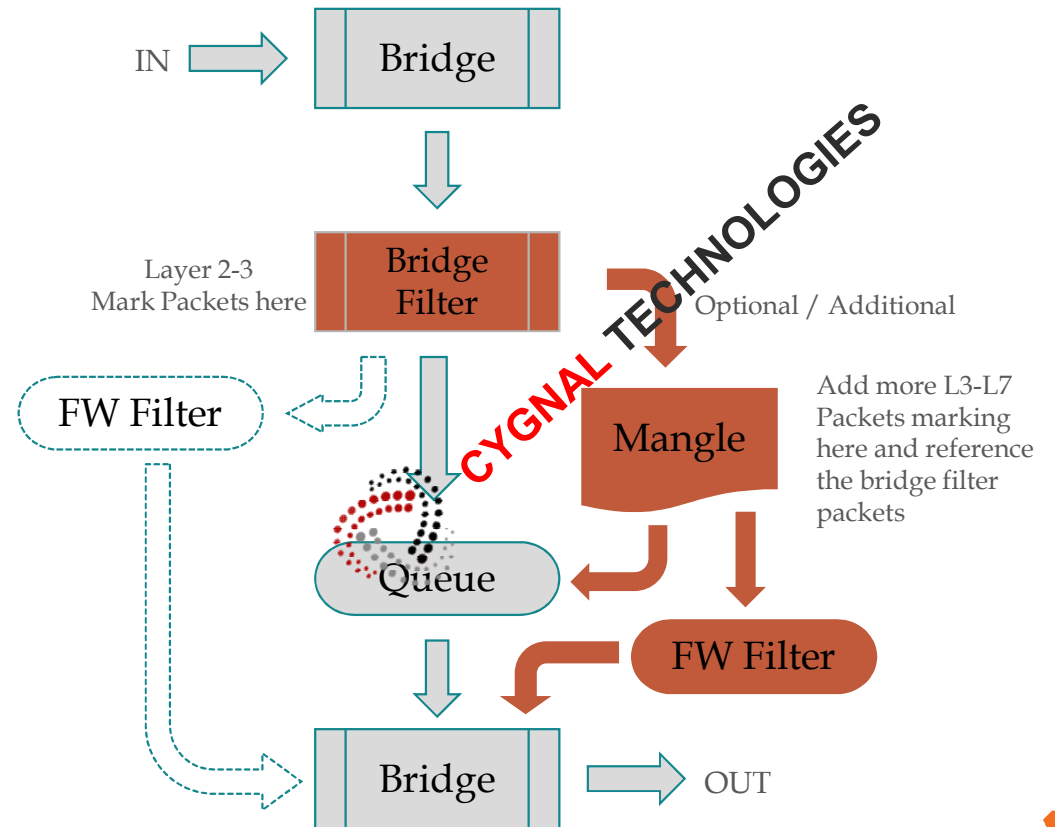
Reset All Counters

## Visualization Comparison

Wiki Method



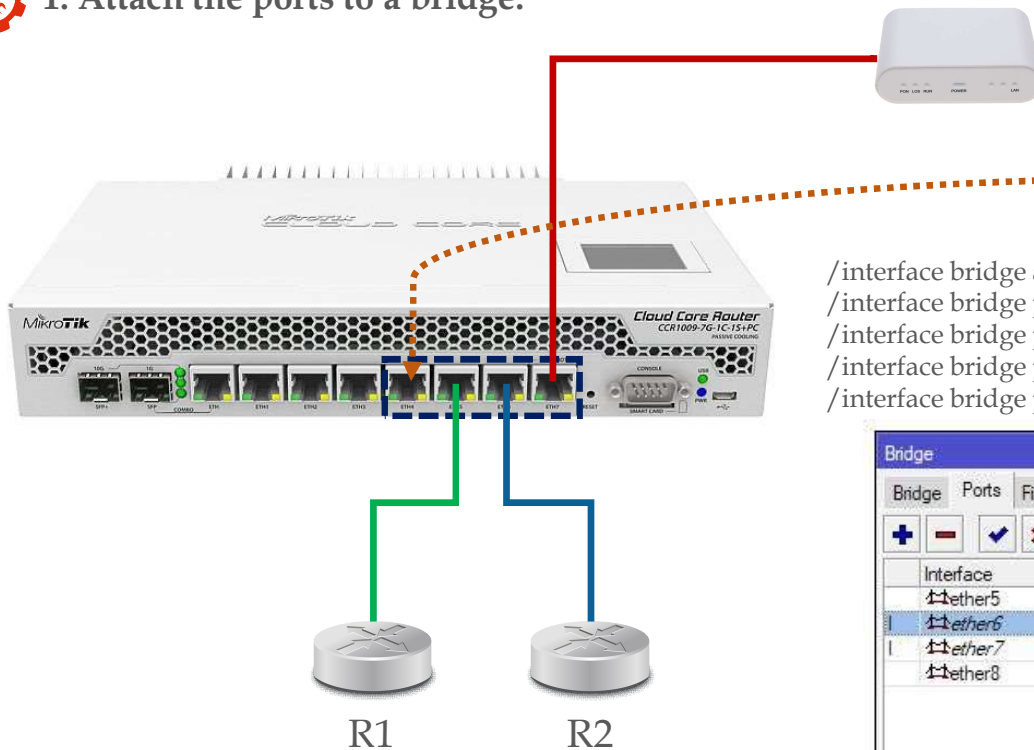
Layer 2-7 support Method



# Configuration: Setting up the bridge



## 1. Attach the ports to a bridge.



- Bridged 4 ports.
  - ISP Port
  - 2 ports for the routers.
  - 1 port reserved for later use

```
/interface bridge add name=in-line-bridge
/interface bridge port add interface=ether5 bridge=in-line-bridge comment="Reserved"
/interface bridge port add interface=ether6 bridge=in-line-bridge comment="R1"
/interface bridge port add interface=ether7 bridge=in-line-bridge comment="R2"
/interface bridge port add interface=ether8 bridge=in-line-bridge comment="ISP Uplink"
```

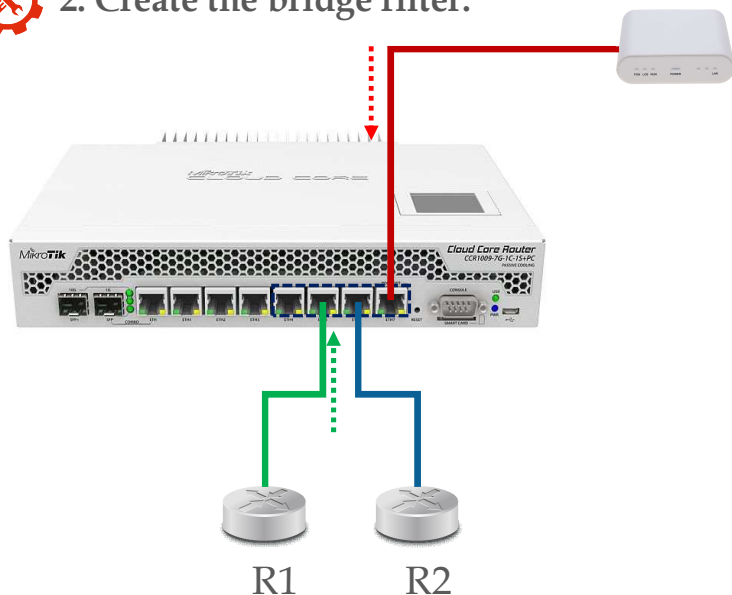
Interface	Bridge	Path Cost	Role	Root Pat...	Comment
ether5	in-line-bridge	10	designated port		Reserved
ether6	in-line-bridge	10	disabled port		R1
ether7	in-line-bridge	10	disabled port		R2
ether8	in-line-bridge	10	designated port		ISP Uplink

4 items (1 selected)

# Configuration: Setting up Bridge Filter



## 2. Create the bridge filter.



Identify the interface port for IN and OUT and mark the packets accordingly.

**Direction: ISP → R1 (router #1 download)**

```
/interface bridge filter add chain=forward in-interface=ether8 out-interface=ether6 \
action=mark-packet new-packet-mark="wan-to-R1-pkt" comment="R1 download"
```

**Direction: ISP ← R1 (router #1 upload)**

```
/interface bridge filter add chain=forward in-interface=ether6 out-interface=ether8 \
action=mark-packet new-packet-mark="R1-to-wan-pkt" comment="R1 Upload"
```

**Direction: ISP → R2 (router #2 download)**

```
/interface bridge filter add chain=forward in-interface=ether8 out-interface=ether7 \
action=mark-packet new-packet-mark="wan-to-R2-pkt" comment="R2 download"
```

**Direction: ISP ← R2 (router #2 upload)**

```
/interface bridge filter add chain=forward in-interface=ether7 out-interface=ether8 \
action=mark-packet new-packet-mark="R2-to-wan-pkt" comment="R2 Upload"
```

**Enable Bridge Firewall**

```
/interface bridge settings set use-ip-firewall=yes
```

Bridge						
Bridge Ports Filters NAT Hosts						
#	Action	Chain	Interfaces/In. Interface	Interfaces/Out. Interface	Packets	Comment
0	mark packet	forward	ether8	ether6	0	R1 download
1	mark packet	forward	ether6	ether8	0	R1 upload
2	mark packet	forward	ether8	ether7	0	R2 download
3	mark packet	forward	ether7	ether8	0	R2 upload

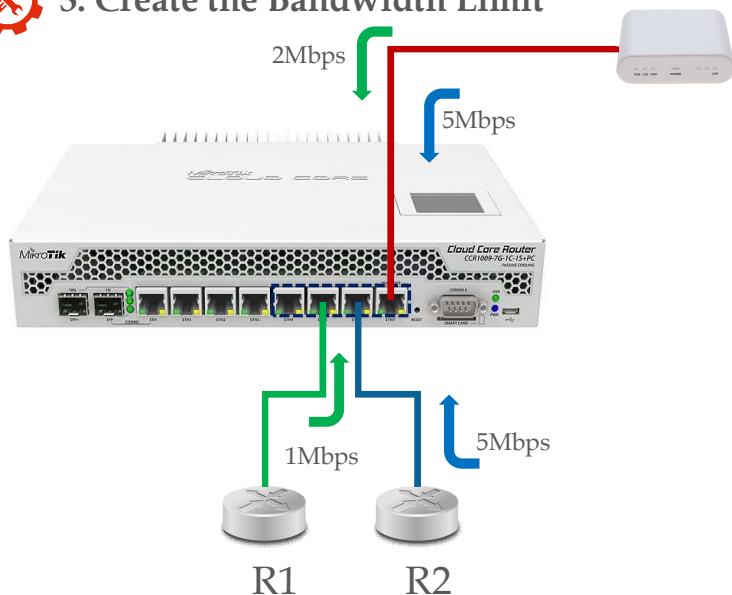




# Configuration: Setting up Bandwidth Limit



## 3. Create the Bandwidth Limit



Use Simple Queue or the Queue Tree facility

### R1 Limit Download

```
/queue simple add name=R1-download packet-marks=wan-to-R1-pkt limit-at=0/2M \
max-limit=0/2M target="0.0.0.0/0"
```

### R1 Limit Upload

```
/queue simple add name=R1-upload packet-marks=R1-to-wan-pkt limit-at=1M/0 \
max-limit=1M/0 target="0.0.0.0/0"
```

### R2 Limit Download

```
/queue simple add name=R2-download packet-marks=wan-to-R2-pkt limit-at=0/5M \
max-limit=0/5M target="0.0.0.0/0"
```

### R2 Limit Upload

```
/queue simple add name=R2-upload packet-marks=R2-to-wan-pkt limit-at=5M/0 \
max-limit=5M/0 target="0.0.0.0/0"
```

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Upload Avg. Rate	Download Avg. Rate	Comment
0	R1-download	0.0.0.0/0	unlimited	2M	wan-to-R1-pkt			
1	R1-upload	0.0.0.0/0	1M	unlimited	R1-to-wan-pkt			
2	R2-download	0.0.0.0/0	unlimited	5M	wan-to-R2-pkt			
3	R2-upload	0.0.0.0/0	5M	unlimited	R2-to-wan-pkt			

4 items (1 selected) | 0 B queued | 0 packets queued



CYGNAL TECHNOLOGIES

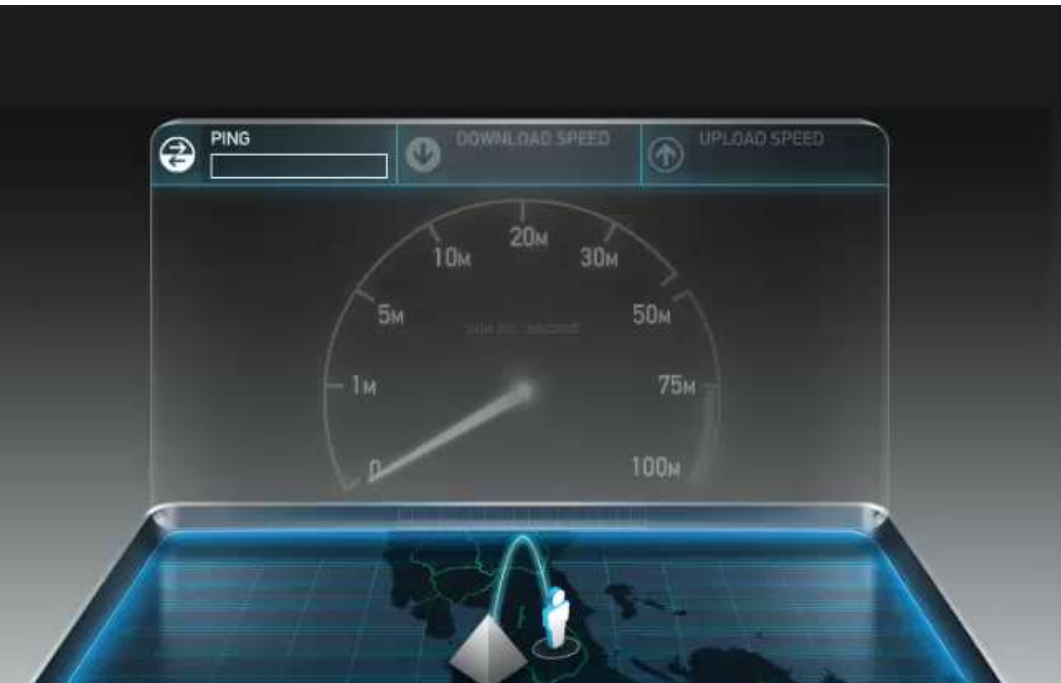


CYGNAL  
Technologies



# Speed Test

(video edited to cut playback time)



The screenshot displays a network configuration interface with three main sections: Queue List, Address List, and Route List. The Queue List table is the primary focus, showing four items with their respective targets, upload/download limits, and packet counts. A red watermark "CYGNAL TECHNOLOGIES" is overlaid diagonally across the interface.

#	Name	Target	Upload Max Limit	Download Max Limit	Packets	Upload Avg...	Download Avg...
0	R1-download	0.0.0.0/0	unlimited	2M			
1	R1-upload	0.0.0.0/0	1M	unlimited			
2	R2-download	0.0.0.0/0	unlimited	5M			30.5 kbps
3	R2-upload	0.0.0.0/0	5M	unlimited		42.3 kbps	

4 items 0 B queued 0 packets queued

Address List: 0 items

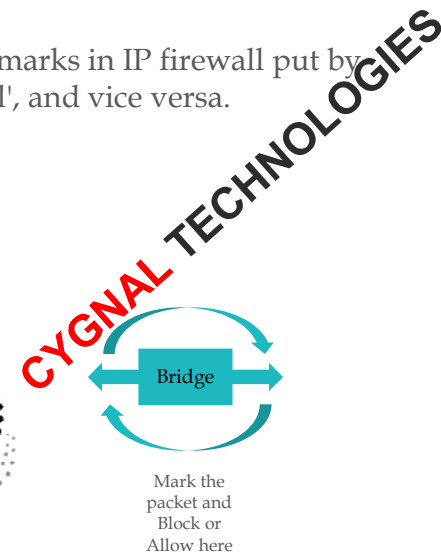
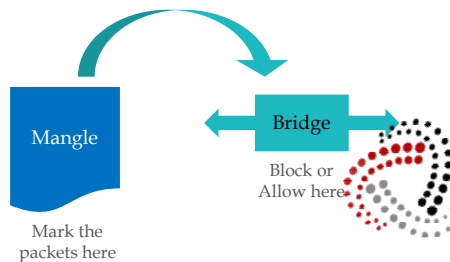
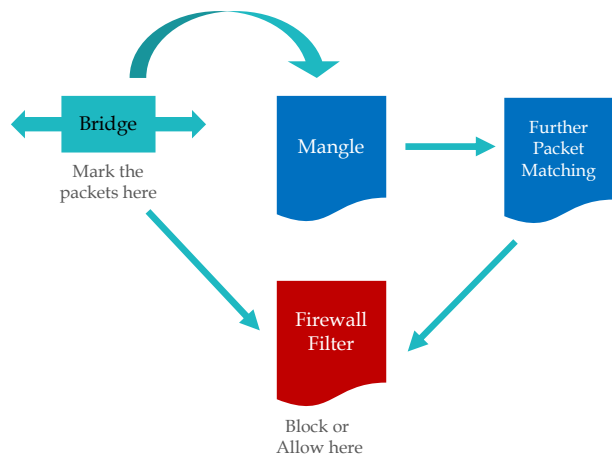
Route List: 0 items

# Firewall on the Bridge

The bridge firewall implements packet filtering and thereby provides security functions that are used to manage data flow to, from and through bridge.

You can put packet marks in bridge firewall (filter and NAT), which are the same as the packet marks in IP firewall put by '/ip firewall mangle'. In this way, packet marks put by bridge firewall can be used in 'IP firewall', and vice versa.

Source: ([https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#Bridge\\_Firewall](https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge#Bridge_Firewall))



# Firewall on Mikrotik

- IP Firewall Filter
- Protocol based filtering (Mangle / Firewall Filter).
- DNS or Web Proxy redirection.
- Layer 7 matcher.
- Etc..etc.

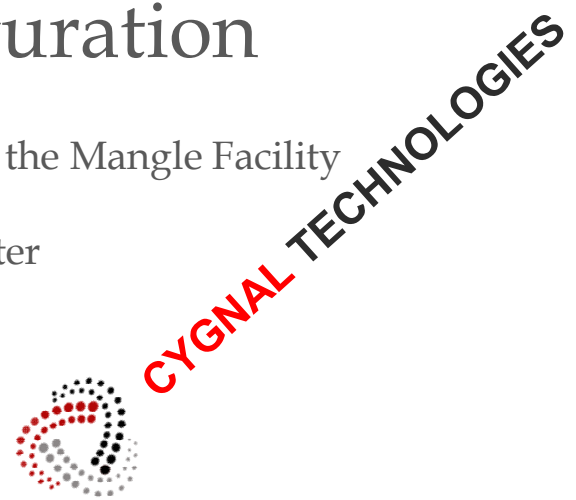
These approach are mostly based on Layer-3 and above (and a very little portion of layer 2), it requires that mikrotik device MUST be the gateway in order for the filter to work.

Our mikrotik in-line shaper/filter does NOT act as the gateway, therefore, it doesn't need to have an assigned IP address or any running services like DNS or Web Proxy.

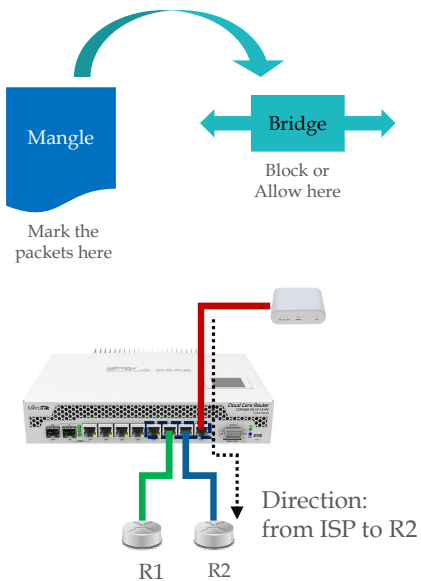


## 2 Steps Configuration

1. Mark the packet at the Mangle Facility
2. Create a Bridge Filter



# Demonstration:



Important: Be mindful of the direction.

A demonstration of filtering packets on bridge interface (L2) and the mangle facility.

Mark a packet containing the word "ESMTP" for mail transfer session.

```
/ip firewall mangle add chain=prerouting content="ESMTP" action=mark-packet new-packet-mark=esmtmp-pkt
```

Create the bridge filter rule and attach the esmtmp-pkt mark.

```
/interface bridge filter add chain=forward in-interface=ether8 out-interface=ether7 packet-mark=esmtmp-pkt action=drop
```

#	Action	Chain	Interfaces/In. Interface	Interfaces/Out. Interface	Packet Mark	Packets	Bytes
0	drop	forward	ether8	ether7	esmtmp-pkt	0	0
1	mark packet	forward	ether8	ether6		0	0
2	mark packet	forward	ether6	ether8		0	0
3	mark packet	forward	ether8	ether7		0	0
4	mark packet	forward	ether7	ether8		0	0

#	Action	Chain	Proto...	Src. Port	Dst. Port	Connection Mark	Out. Bridge Port	In. Bridge Port	New Packet Mark	Bytes	Packets
0	mark packet	prerouting							esmtmp-pkt	847 B	11

# Filter Turned-Off

admin@E4:8D:8C:6B:47:F4 (Cygnaltech) - WinBox v6.40.3 on hAP ac (mipsbe)

Session Settings Dashboard

Safe Mode Session: E4:8D:8C:6B:47:F4

Bridge

Bridge Ports Filters NAT Hosts

00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Interfaces/In...	Interfaces/Out...	Packet Mark	Packets	Comment
0	drop	forward	ether3	ether7	sentto.pkt	10	
1	mark packet	forward	ether8	ether6		0	R1 download
2	mark packet	forward	ether6	ether8		0	R1 upload
3	mark packet	forward	ether8	ether7		6 052	R2 download
4	mark packet	forward	ether7	ether8		13 388	R2 upload

5 items (1 selected)

Address List

Address	Network	Interface
---------	---------	-----------

0 items

Route List

Routes	Nexthops	Rules	VRF
--------	----------	-------	-----

0 items

outerOS WinBox

New Terminal

MetaROUTER

Partition

Make Supout.tif

Manual

New WinBox

```
[root@ds ~]# tailf -n 5 /var/log/maillog
Jan 12 23:39:44 ds postfix/smtpd[4218]: disconnect from unknown[10.124.124.112]
Jan 12 23:43:55 ds clamd[1187]: SelfCheck: Database status OK.
Jan 12 23:53:55 ds clamd[1187]: SelfCheck: Database modification detected. Forcing reload.
Jan 12 23:53:55 ds clamd[1187]: Reading databases from /var/lib/clamav
Jan 12 23:54:04 ds clamd[1187]: Database correctly reloaded (6528056 signatures)
Jan 12 23:56:03 ds postfix/smtpd[4451]: connect from unknown[10.124.124.112]
Jan 12 23:56:21 ds postfix/smtpd[4451]: lost connection after CONNECT from unknown[10.124.124.112]
Jan 12 23:56:21 ds postfix/smtpd[4451]: disconnect from unknown[10.124.124.112]
```

Write: Test Email - Thunderbird

File Edit View Options Tools Help

Send Spelling Attach Security Save

From: Administrator <admin@cygnaltech.com> admin@cygnaltech.com

To: Dan Santillan <santillan.dans.mt@gmail.com>

Subject: Test Email

This is an email test.

CYGNAL TECHNOLOGIES

# Filter Turned-On

admin@E4:8D:8C:6B:47:F4 (Cygnaltech) - WinBox v6.40.3 on hAP ac (mipsbe)

Session Settings Dashboard

Safe Mode Session: E4:8D:8C:6B:47:F4

Bridge

Bridge Ports Filters NAT Hosts

00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Interfaces/In...	Interfaces/Out...	Packet Mark	Packets	Comment
0	drop	forward	ether8	ether7	smtp-pkt	0	
1	mark packet	forward	ether8	ether6		0	R1 download
2	mark packet	forward	ether6	ether8		0	R1 upload
3	mark packet	forward	ether8	ether7		1 573	R2 download
4	mark packet	forward	ether7	ether8		3 692	R2 upload

5 items (1 selected)

Address List

Address	Network	Interface
---------	---------	-----------

0 items

Route List

Routes	Nexthops	Rules	VRF
--------	----------	-------	-----

0 items

outerOS WinBox

New Terminal

MetaROUTER

Partition

Make Suptout.tif

Manual

New WinBox

```
root@ds:~  
[root@ds ~]# tailf -n 5 /var/log/maillog  
Jan 12 23:39:44 ds postfix/smtpd[4218]: disconnect from unknown[10.124.124.112]  
Jan 12 23:43:55 ds clamd[1187]: SelfCheck: Database status OK.  
Jan 12 23:53:55 ds clamd[1187]: SelfCheck: Database modification detected. Forcing reload.  
Jan 12 23:53:55 ds clamd[1187]: Reading databases from /var/lib/clamav  
Jan 12 23:54:04 ds clamd[1187]: Database correctly reloaded (6528056 signatures)
```

Write: Test Email - Thunderbird

File Edit View Options Tools Help

Send Spelling Attach Security Save

From: Administrator <admin@cygnaltech.com> admin@cygnaltech.com

To: Dan Santillan <santillan.dans.mt@gmail.com>

Subject: Test Email

This is an email test.

CYGNAL TECHNOLOGIES

So what L2 fields that can be used for packet matcher under the bridge filter?

<b>1. General</b> <ul style="list-style-type: none"> <li>• Interfaces IN/OUT</li> <li>• Bridges IN/OUT</li> <li>• SRC/DST addresses</li> <li>• MAC Protocols</li> <li>• IP Src/Dst Addresses and Protocols (L3)</li> </ul>	<b>2. VLAN</b> <ul style="list-style-type: none"> <li>• Vlan ID</li> <li>• VLAN Encapsulation</li> <li>• 802.3 Type and SAP</li> <li>• Packet Types</li> </ul>
<b>3. ARP</b> <ul style="list-style-type: none"> <li>• Opcodes</li> <li>• Hardware Type</li> <li>• Packet Type</li> <li>• Addresses</li> <li>• SRC and DST MAC Address</li> <li>• Gratuitous</li> </ul>	<b>4. STP</b> <ul style="list-style-type: none"> <li>• STP Types</li> <li>• STP Flags</li> <li>• STP Root Addresses</li> <li>• STP Root Cost</li> <li>• STP Sender-Address</li> <li>• STP Port</li> <li>• STP Priorities</li> <li>• STP Ages / STP Time</li> </ul>

2,3 and 4 are not available at the mangle



**Mangle Rule**

To cover Layer 3 to Layer 7

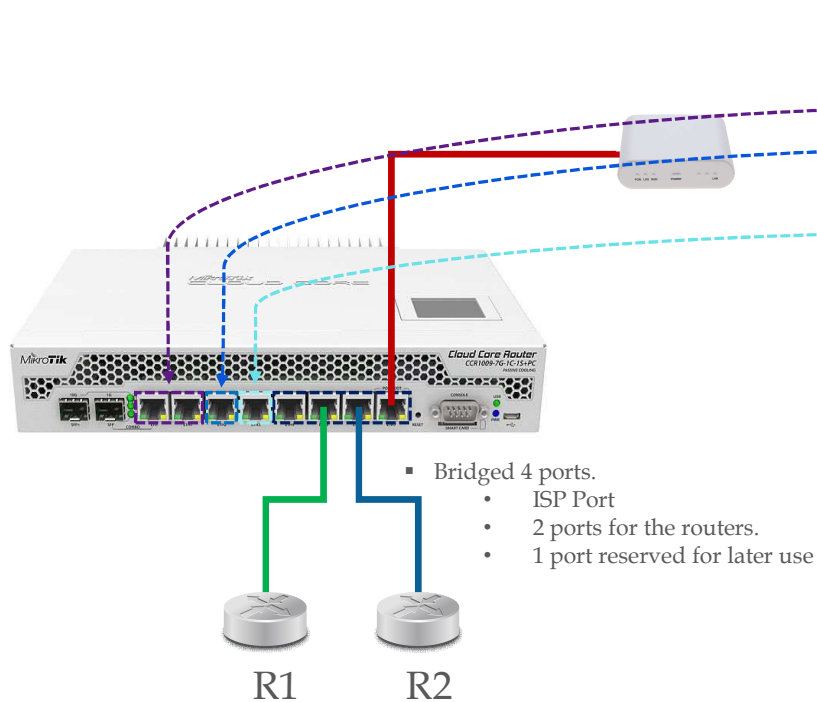


A better chance to hit a specific packets

**CYGNAL TECHNOLOGIES**



# Expansion

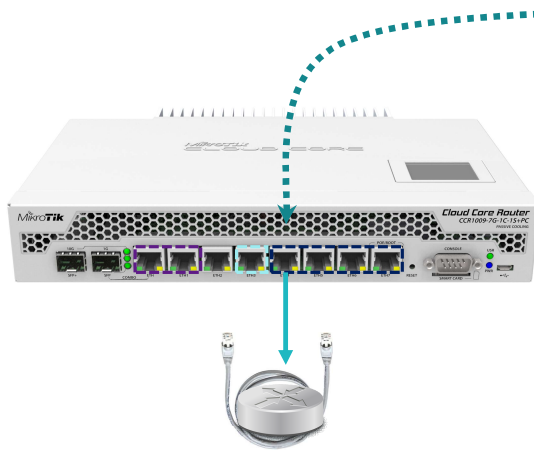


What to do with the unused ports?

- Use it for the natted LAN and...
- Hotspot access port.
- Use this port for the "WAN" port of the natted LAN and hotspot

The hotspot port and the WAN port MUST not be a member of the LAN bridge

# Almost done...



Remember the reserved port?

This port is a member of the **in-line-bridge** interface and it should not have a public ip address, the port can be used for expansion by connecting another device or router to it.

*(although, it is ok to assign it with an ip address, we are trying to avoid for the interface to listen on any protocols on this port and just make it a managed switch)*

The simple solution is just to connect the “wan” port and the “in-line-bridge” port with a patch cable.



## LAN Configuration

### Create the bridge for natted LAN

```
/interface bridge add name=lan-bridge comment="LAN"
```

### Add the ports to the lan-bridge

```
/interface bridge port add interface=ether1 bridge=lan-bridge  
/interface bridge port add interface=ether2 bridge=lan-bridge
```

### Add the IP address to the lan-bridge

```
/ip address add address=192.168.1.1/24 interface=lan-bridge
```

### NAT the LAN subnet

```
/ip firewall nat add chain=srcnat src-address=192.168.1.0/24 action=masquerade \  
out-interface=wan-bridge
```



## WAN Configuration

### Create the bridge for WAN

```
/interface bridge add name=wan-bridge comment="WAN"
```

### Add the ports to the wan-bridge

```
/interface bridge port add interface=ether4 bridge=wan-bridge
```

### Add the Public IP to the wan-bridge

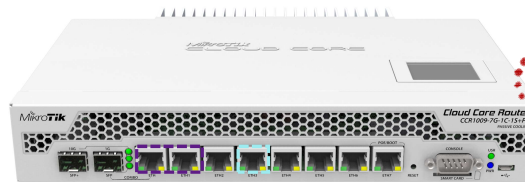
```
/ip address add address=198.18.1.4/29 interface=wan-bridge
```

### Add the Public IP gateway

```
/ip route add dst-address=0.0.0.0/0 gateway=198.18.1.1 distance=1
```

### Enable DNS server

```
/ip dns set server="8.8.8.8, 8.8.4.4" allow-remote-requests=yes
```



LAN WAN

CYGNAL TECHNOLOGIES



**CYGNAL**TECHNOLOGIES

[www.cygnaltech.com](http://www.cygnaltech.com)

- E N D -



**CYGNAL** TECHNOLOGIES