Securing Networks with MikroTik Router OS

Zagreb,Croatia,
March 14th 2013

Presenter
Tom Smyth
CTO Wireless Connect Ltd.

Wireless Connect Ltd.

- ✓Irish Company Incorporated in 2006
- ✓Operate an ISP in the centre of Ireland.
- ✓Good Infrastructure Expertise.
- ✓ Certified MikroTik Partners
- ✓Training
- ✓Certified OEM Integrators
- ✓Consultants
- ✓Value Added Reseller

Speaker Profile:

- ✓Studied BEng. Mechanical & Electronic Engineering, DCU,Ireland
- ✓Has been working in Industry since 2000
- ✓Server Infrastructure Engineer
- ✓Systems / Network Administrator
- ✓Internet Security Consultant
- ✓1st MikroTik Certified Trainer in June 2007 in Ireland

Security Information sources

✓ENISA –http://www.enisa.europa.eu/

✓OWASP http://owasp.org

✓Rits Group – http://www.ritsgroup.com/

✓ISAS – http://www.isas.ie/

✓SANS Institute – http://sans.org

✓CIS Centre for Internet Security – http://cisecurity.org/

✓NIST Computer Security http://csrc.nist.gov/

✓Open BSD – http://OpenBSD.org/

✓Spamhaus.org – http://spamhaus.org

✓nmap.org – http://nmap.org

✓ha.ckers.org – http://ha.ckers.org/

Router OS

- Highly Versatile
- Highly Customisable
- Highly Cost Effective
- Allows one to manage Security Threats in many Ways

What Can MikroTik Router OS Do ?

- It is a Stateful Firewall
- It is a Web Proxy
- It is a Socks Proxy
- It is a DNS Cache / Proxy
- It is a Router
- It is an IPSEC Concentrator
- It is an IDS – Intrusion Detection System
- It is an IPS – Intrusion Prevention System

Ways to Contact Tom

- Email Info /a+/ wirelessconnect.eu
- Phone
  - +353876193172
  - +35312916265
- Skype
  - Tomwirelessconnecteu

Previous MUM Presentations

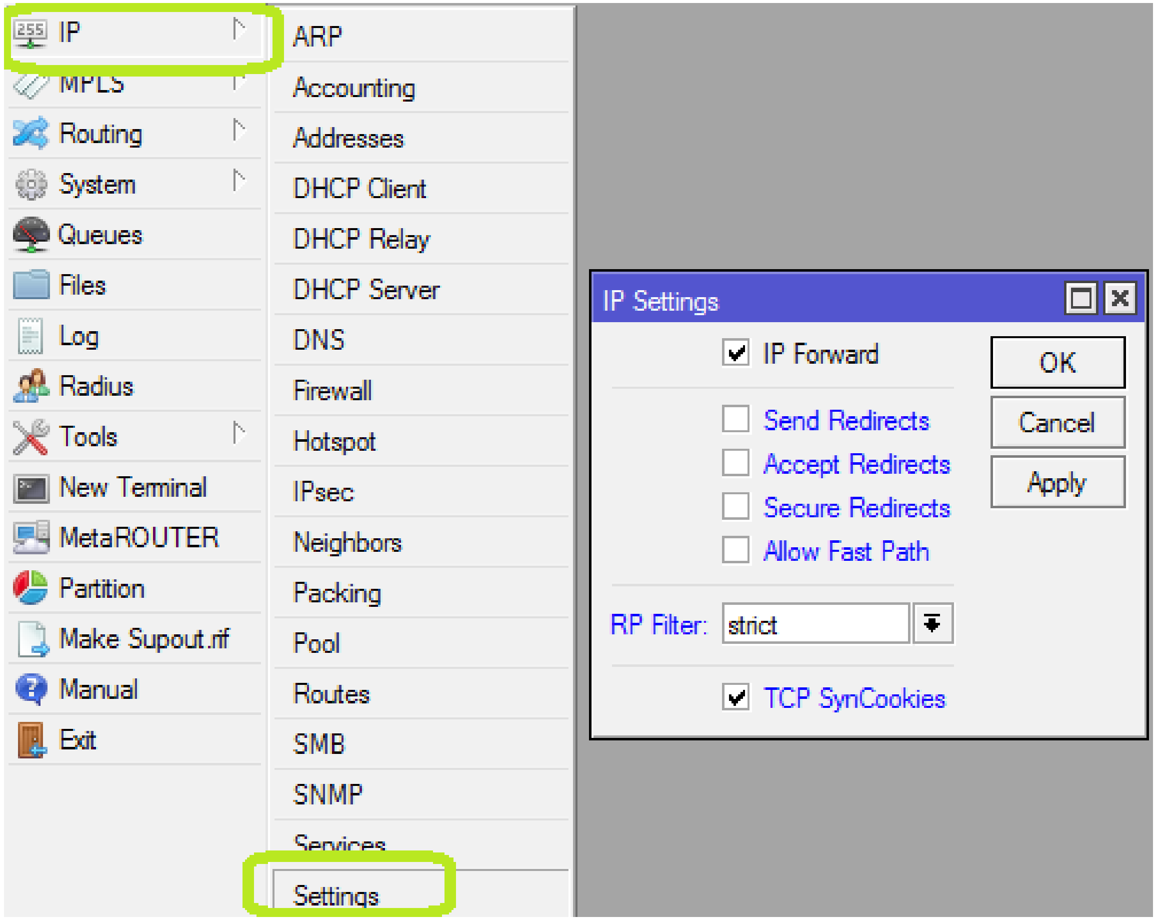
- See my presentations from previous mums for more information
  - MUM New Orleans 2012 -> MikroTik Advanced Security
  - MUM Dubai 2012 --> Blackhole Routing Techniques
  - MUM Budapest 2011 --> Advanced Firewall Strategies
  - MUM Poland 2010 --> Web Proxy as a Web application firewall
- Check out My good friend Maia Wardner of MD Brazil's Many Presentations on Network Security lots of examples and brilliant illustrations

Overview

- New IP Kernel hardening settings available in Mikrotik
- Implementing Port isolation in Bridges to acheve private vlan Functionality

IP Security Settings

- New Security Hardening settings are available in Mikrotik Router OS v6
- They set various fundamental Linux Kernel parameters to reduce security risks to your router and your networks
- The Settings Include:
  - IP Forward
  - Send Redirects
  - Accept Secure Redirects
  - Accept Redirects
  - Allow Fastpath
  - Reverse Path filtering
  - TCP Syn Cookie



IP Settings

☑ IP Forward

☐ Send Redirects

☐ Accept Redirects

☐ Secure Redirects

☐ Allow Fast Path

RP Filter: strict

☑ TCP SynCookies

IP Forward

- According to Industry best practice (NSA/ CIS) that systems that do not have router functionality should have IP forwarding disabled.
- Examples of Dedicated Systems that dont Require IP forwarding Capability
  - Usermanager
  - Proxy
  - NTP
  - DNS Servers
- Linux Kernel Parameter = net.ipv4.ip forward = 0
  - Disable the ability of the router to route packets from one interface to another based on IP

Why Disable IP Forward

- Prevents Servers / Appliances becomming unauthorised routers
- Prevents circumvention of firewall rules that block traffic based on incomming interface.

Send Redirects

- A Router can send redirects to request that a computer with a sub optimal routing table can be temporarly corrected to allow traffic to flow.
- Redirects are Expensive computationally for the Router and the Device Receiving them
- End Devices do not require Send Redirects
- Linux Kernel Parameters
  - net.ipv4.conf.all.send redirects = 0
  - net.ipv4.conf.default.send redirects = 0

Why Disable Send Redirects

- A Router could in advertently give an attacker information about the topology of the network
- “The Database Subnet” is reachable via 10.1.2.3, not me.

Accept Redirects

- Redirects inbound allow suboptimal routing tables on the router to be temporarly overridden to allow communications to occur
- They are computationally expensive redirected traffic increases load on the router dramatically

Why Disable Accept Redirects

- Accepting Redirects allows your Routing Table to be temporarly over ridden
  - Denial of Service
  - Vastly Increased Resource Usage
  - Potential for Redirecting Traffic through unauthorised devices (Man in the Middle)

Secure Redirects

- Accepting secure_redirects setting linux network interfaces to accept ICMP redirect messages only from default gateways in the routing table
- Kernel Parameters that control this setting
  - net.ipv4.conf.default.secure_redirects = 0
  - net.ipv4.conf.all.secure_redirects = 0

Why Disable Secure Redirects

- Accepting even secure redirects allows your Routing Table to be temporarly over ridden by ICMP traffic comming from Gateways in your routing table
  - Denial of Service
  - Vastly Increased Resource Usage
  - Potential for Redirecting Traffic through unauthorised devices (Man in the Middle)

Allow Fastpath

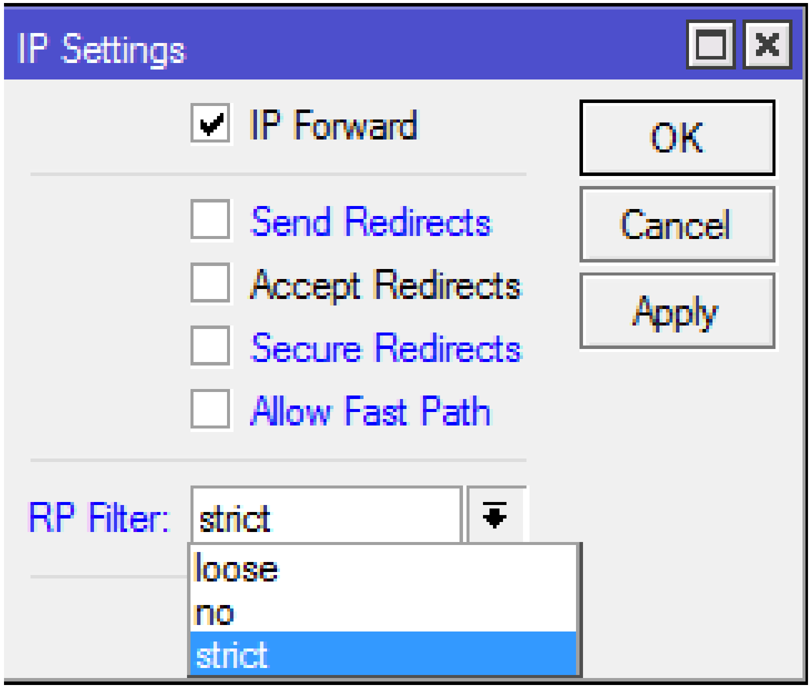
- Fastpath is a software optimisation of the kernel to allow significantly increased forwarding speed
- Fastpath optimises Throughput on a number of layers
  - Layer3 (Ipv4 and Ipv6)
  - Layer 2.5 (MPLS)
  - Layer 2 (Bridging)

Why not enable Fastpath?

- The Dramatic increase in throughput is achieved at the expense of firewall inspection and control
- If Traffic control and security is your priority, one may have to sacrifice some throughput.

Reverse Path Filter / Verification

- Kernel level check of ingress traffic against IP Routing Table
- Strict RPF -> Only accept traffic entering on the interface that the Best / most specific route matching the packet uses
- Loose RPF -> Accept traffic entering on any interface that has a route that could be used to route to the IP
- Can be combined with Blackhole routes to allow bi-directional Enforcement of policy



IP Settings

☑ IP Forward

□ Send Redirects

□ Accept Redirects

□ Secure Redirects

□ Allow Fast Path

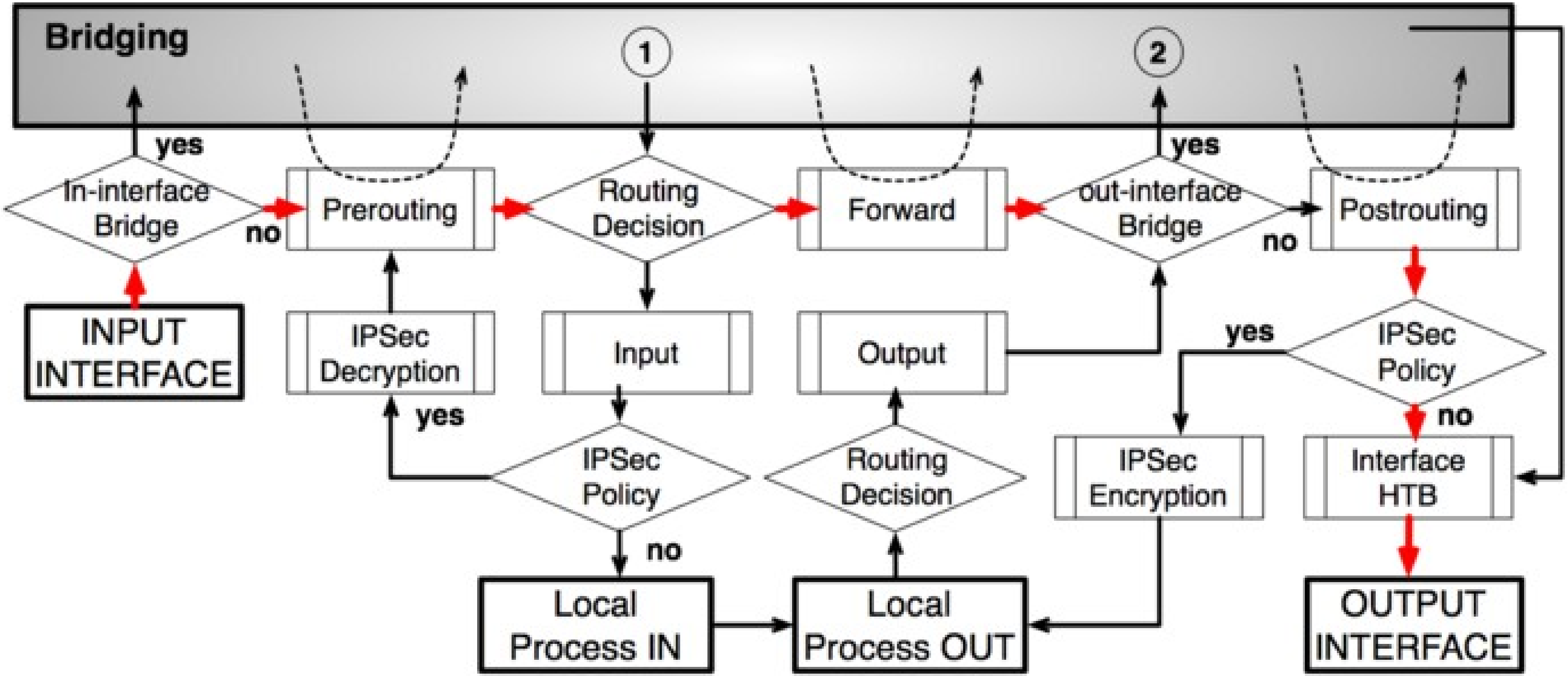
RP Filter: strict

loose
no
strict

Alternatives to Firewall Filtering

- If we want to filter traffic going towards a destination for example
- Let us take a look at the Kernel where, MikroTik Router OS Does its Magic

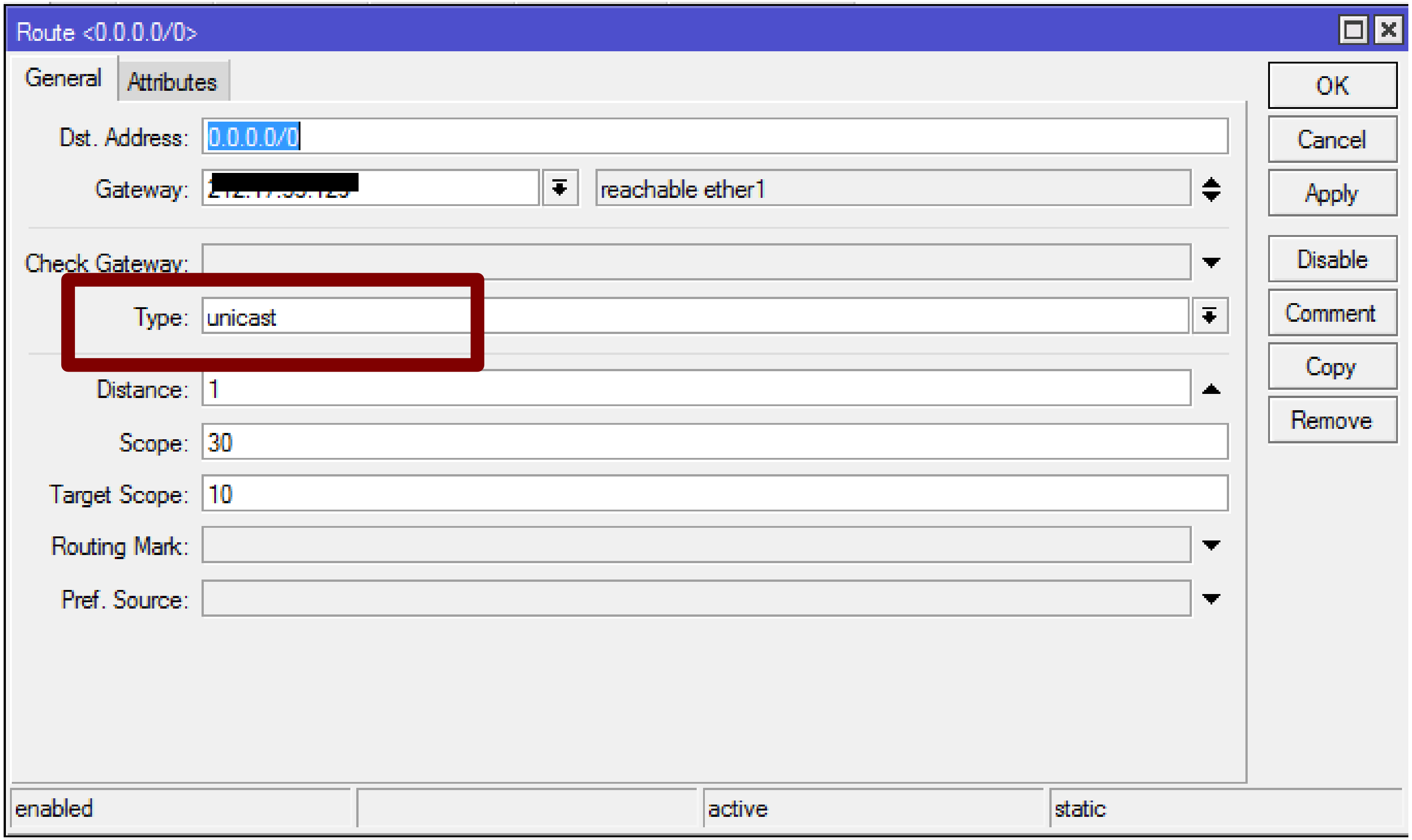
MikroTik Kernel -Packet Flow



- It Seems all packets flowing to / through the router are processed using the routing table

Filtering Using Routes

- Most people are familiar with Routing as a tool to help traffic reach its destination,
- These “Normal” routes are called Unicast routes



Route <0.0.0.0/0>

General | Attributes

Dst. Address: 0.0.0.0/0

Gateway: [redacted] reachable ether1

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

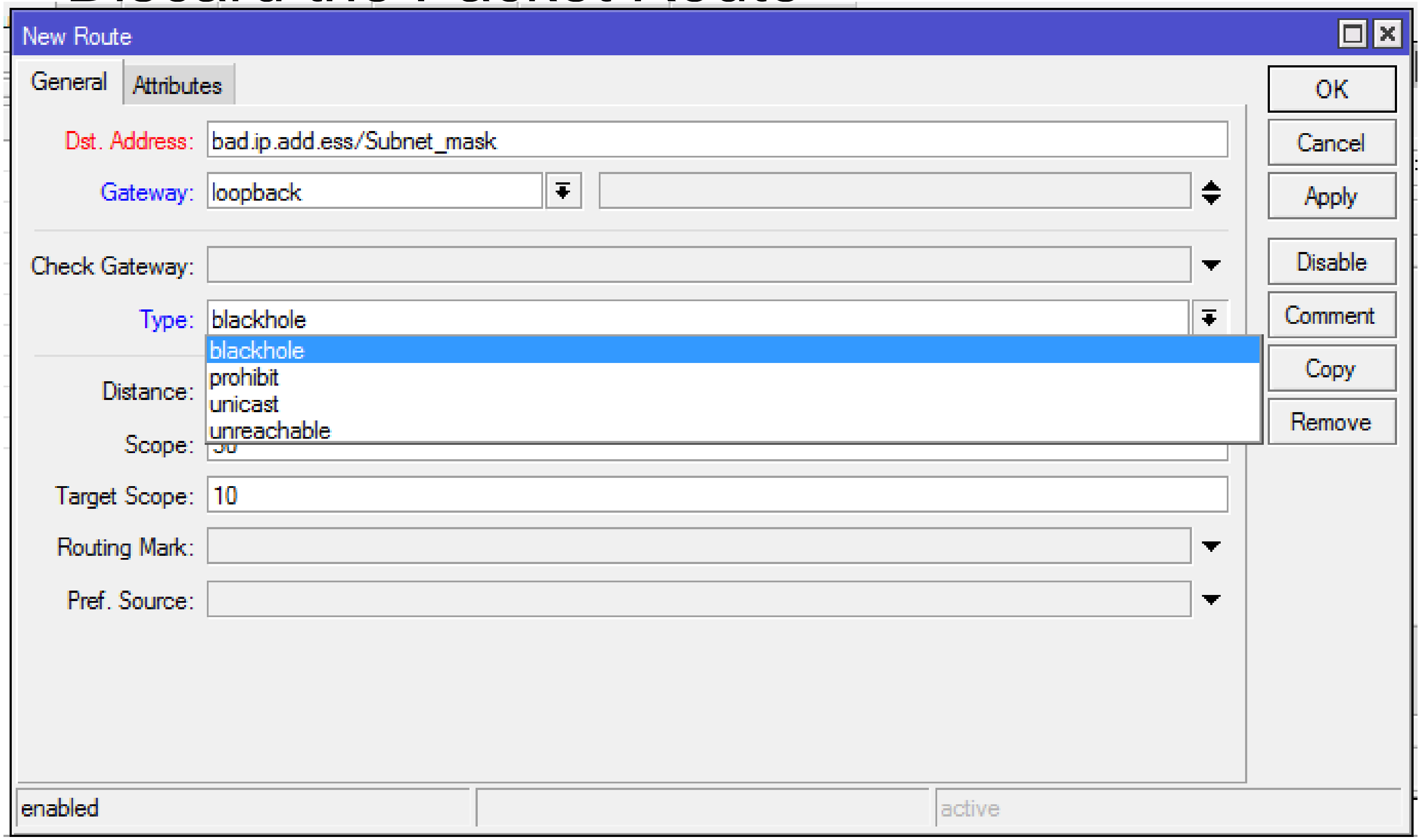
Routing Mark:

Pref. Source:

enabled | active | static

Enter the BlackHole Route

- BlackHole – the name from the astronomical phenomena where any object placed into the BlackHole will never leave.
- BlackHole – Discard the Packet Route



Dst. Address: bad.ip.add.ess/Subnet_mask

Gateway: loopback

Check Gateway:

Type: blackhole

blackhole
prohibit
unicast
unreachable

Distance:

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

enabled

active

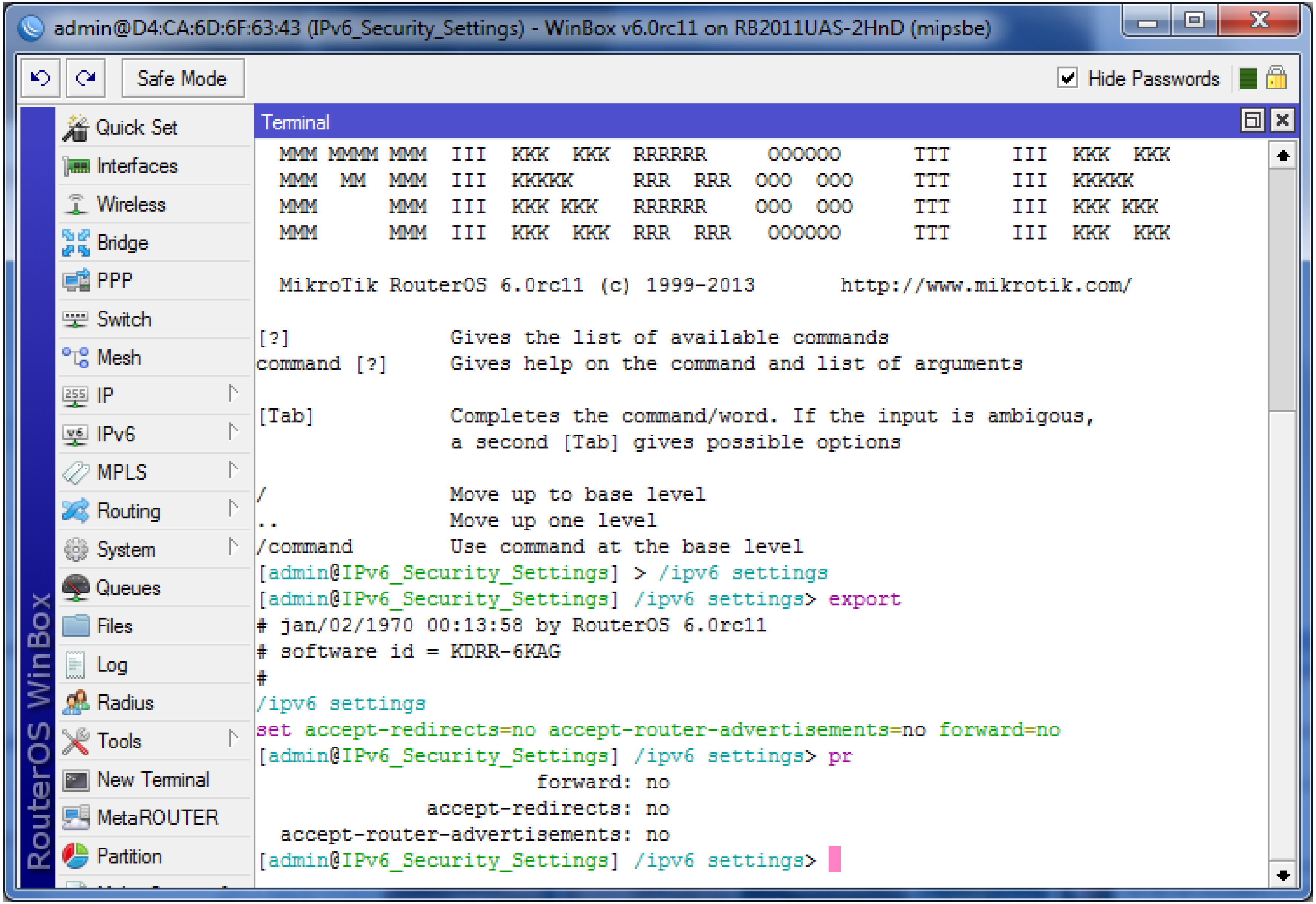
Why Enable Fastpath

- RPF + Black Hole Routes + Fastpath = Could mean Accelerated Filtering :)
- As long as RPF does not affect fastpath

TCP Syn Cookies

- Enabling Syn Cookies prevents the Age old Syn attack Denial of Service Attack

IP v6 Kernel Parameters



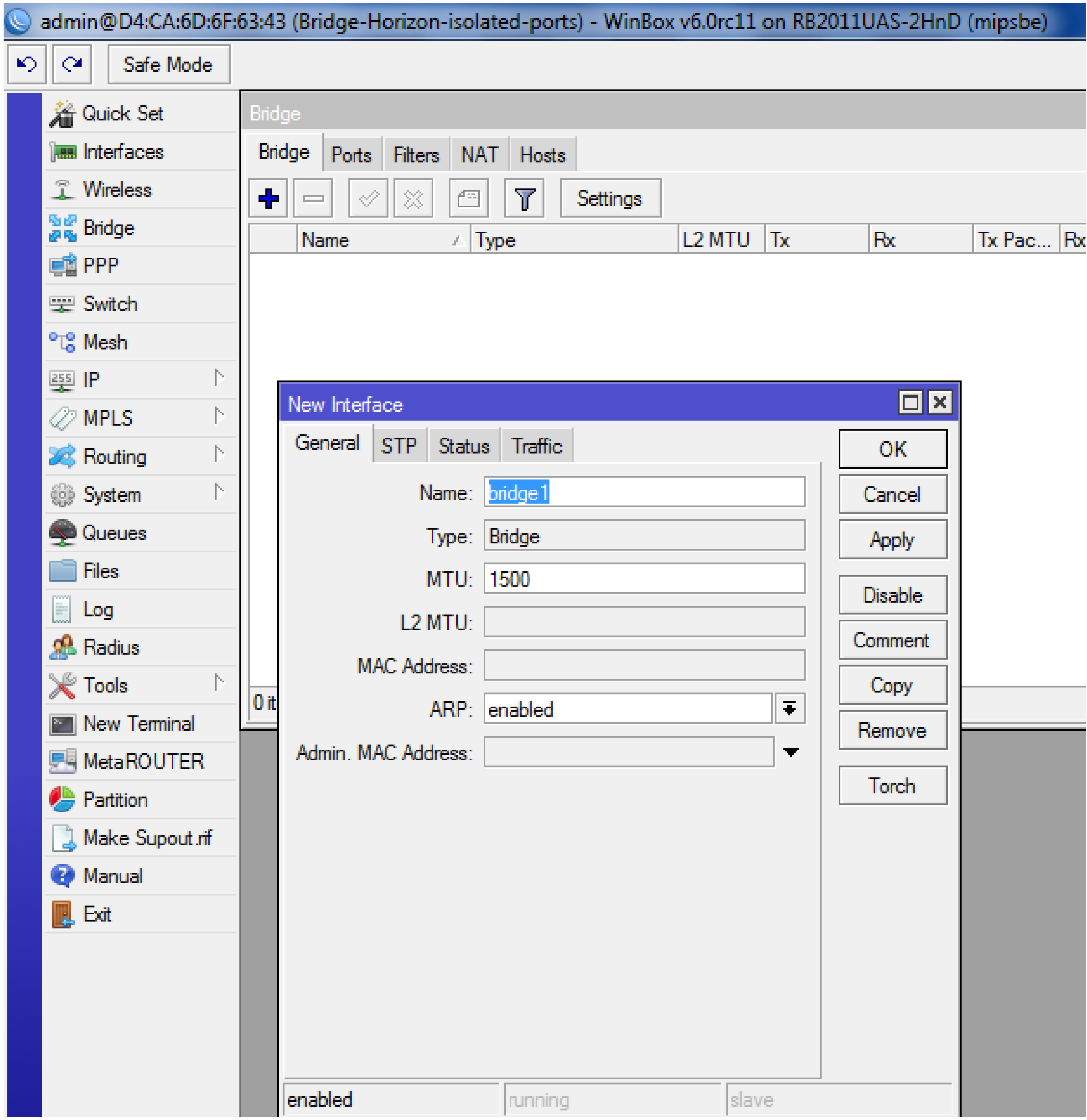
```
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.0rc11 (c) 1999-2013       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambigous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level
[admin@IPv6_Security_Settings] > /ipv6 settings
[admin@IPv6_Security_Settings] /ipv6 settings> export
# jan/02/1970 00:13:58 by RouterOS 6.0rc11
# software id = KDRR-6KAG
#
/ipv6 settings
set accept-redirects=no accept-router-advertisements=no forward=no
[admin@IPv6_Security_Settings] /ipv6 settings> pr
                       forward: no
              accept-redirects: no
  accept-router-advertisements: no
[admin@IPv6_Security_Settings] /ipv6 settings>
```

Bridge Horizon & Protected ports

Bridge Split Horizon

- Bridge Port Split Horizon is a feature that allows the effecient management of Traffic flow between ports
- Bridge Port Split Horizon was primarly developed as a loop avoidance Technology on VPLS meshed Layer 2 Networks
- Horizon values are only significant locally
- Horizons must be configured to avoid loops manually!
- Split Horizon allows or disallows communication according to the following rules
  - Frames are allowed flow between ports with different Horizon Values
  - Frames cannot Flow between ports with the same Horizon

Create the Bridge



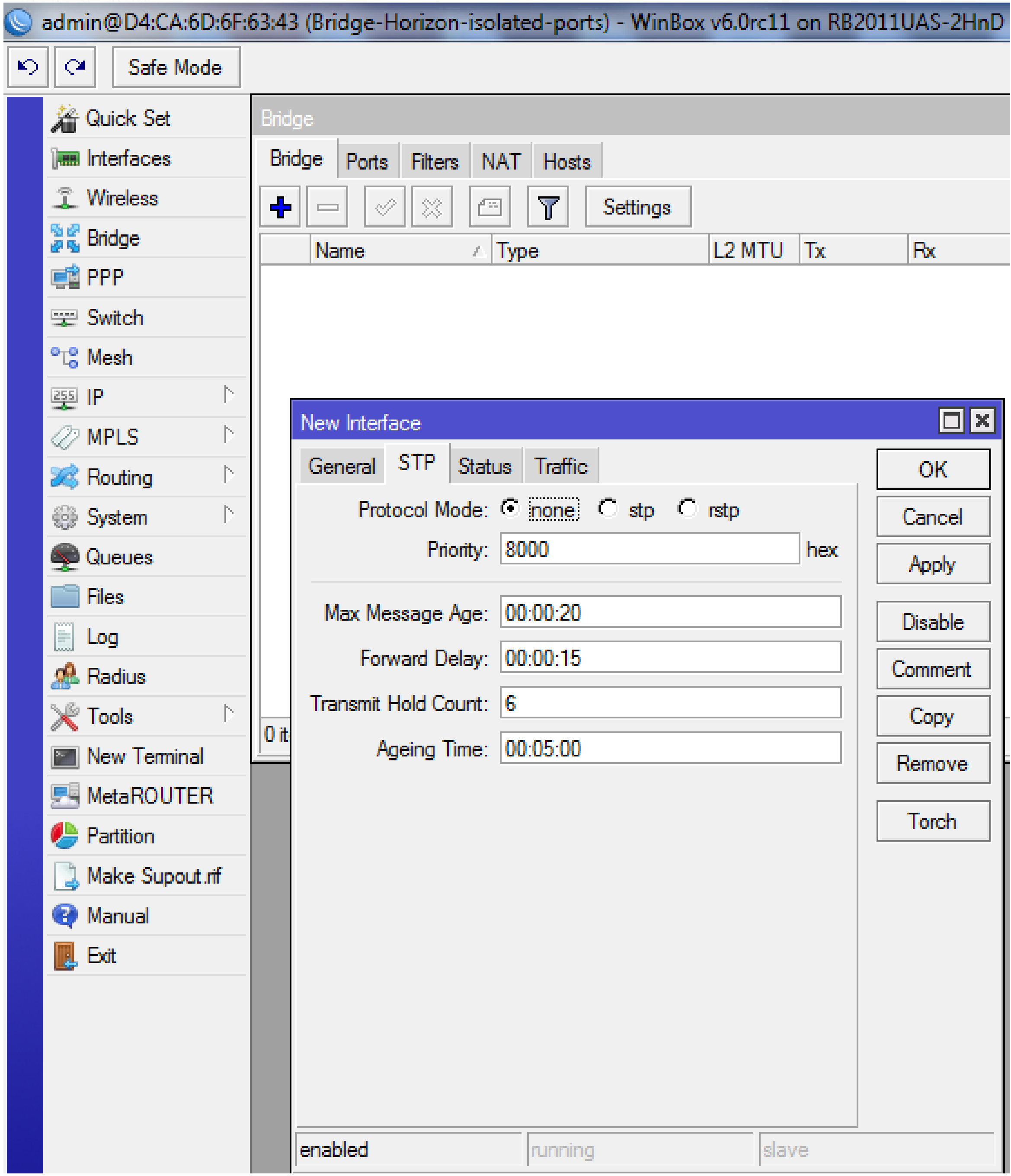
admin@D4:CA:6D:6F:63:43 (Bridge-Horizon-isolated-ports) - WinBox v6.0rc11 on RB2011UAS-2HnD (mipsbe)

New Interface

Name: bridge1
Type: Bridge
MTU: 1500
L2 MTU:
MAC Address:
ARP: enabled
Admin. MAC Address:

enabled | running | slave

Disable STP


admin@D4:CA:6D:6F:63:43 (Bridge-Horizon-isolated-ports) - WinBox v6.0rc11 on RB2011UAS-2HnD

New Interface — STP

Protocol Mode: ● none ○ stp ○ rstp

Priority: 8000 hex

Max Message Age: 00:00:20

Forward Delay: 00:00:15

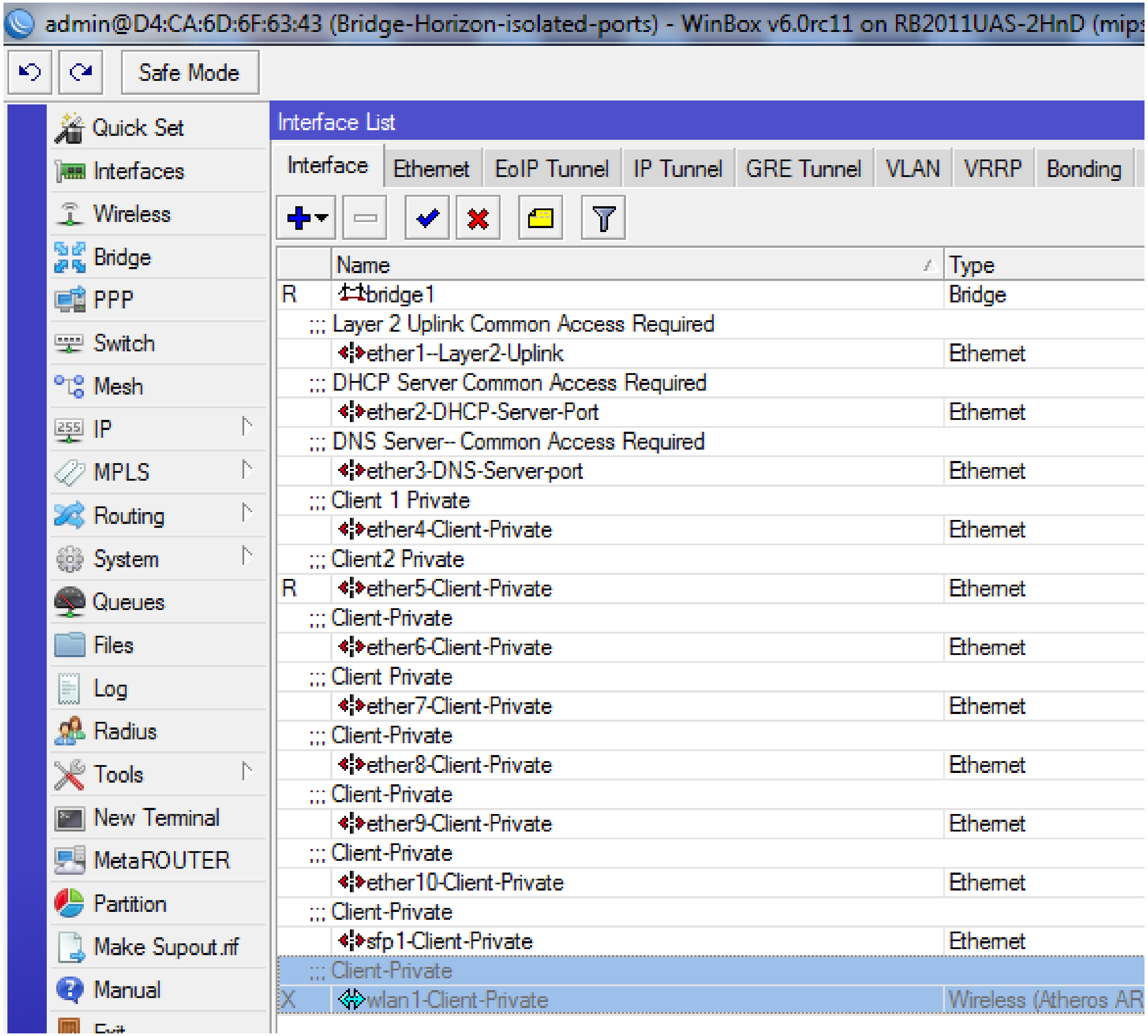
Transmit Hold Count: 6

Ageing Time: 00:05:00

enabled | running | slave

Identify Ports physical and their Policy

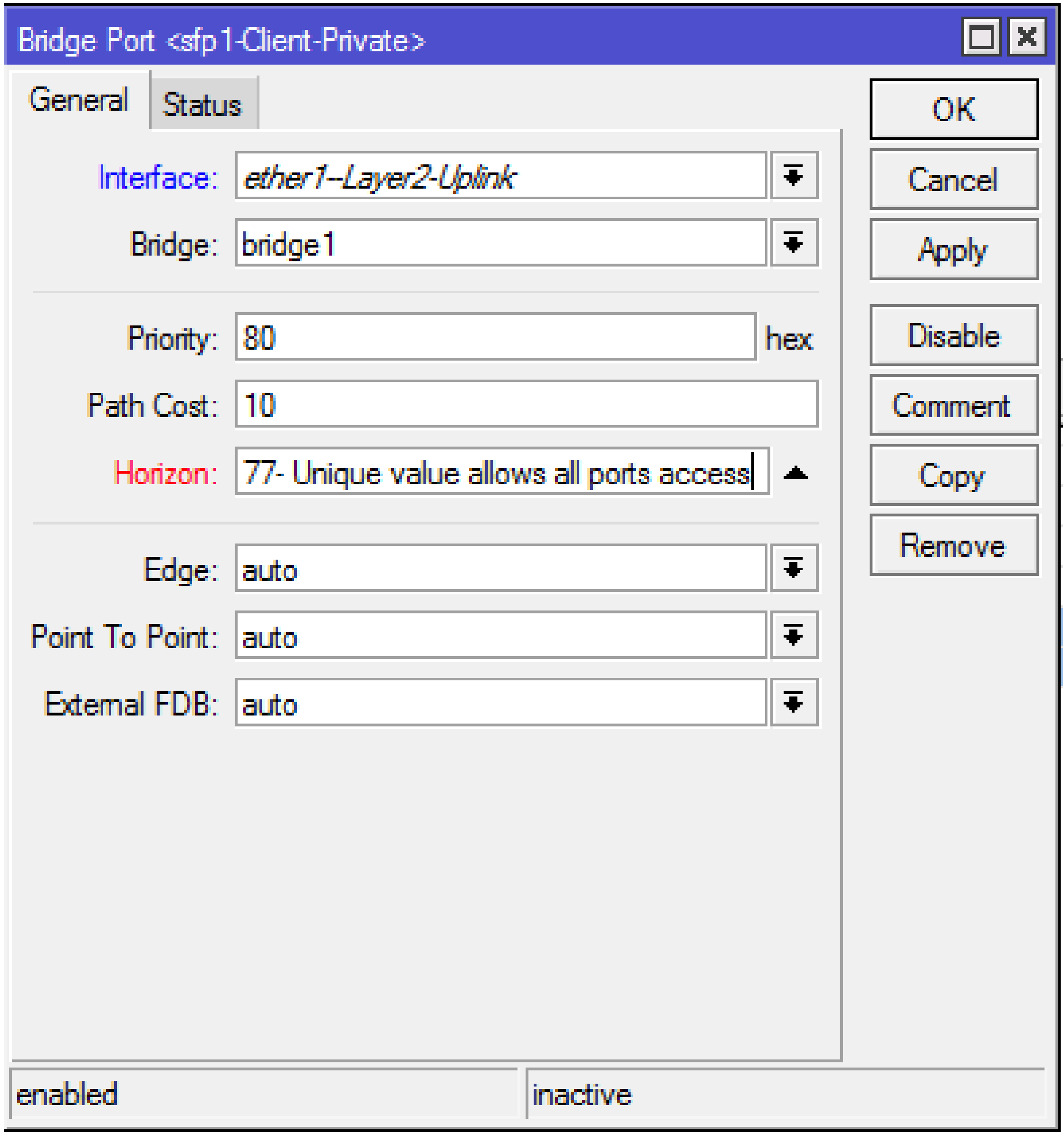
- Clients cant talk to each other
- Clients can talk to servers
- Servers can talk to each other



admin@D4:CA:6D:6F:63:43 (Bridge-Horizon-isolated-ports) - WinBox v6.0rc11 on RB2011UAS-2HnD (mips

	Name	Type
R	bridge1	Bridge
	;;; Layer 2 Uplink Common Access Required	
	ether1--Layer2-Uplink	Ethernet
	;;; DHCP Server Common Access Required	
	ether2-DHCP-Server-Port	Ethernet
	;;; DNS Server-- Common Access Required	
	ether3-DNS-Server-port	Ethernet
	;;; Client 1 Private	
	ether4-Client-Private	Ethernet
	;;; Client2 Private	
R	ether5-Client-Private	Ethernet
	;;; Client-Private	
	ether6-Client-Private	Ethernet
	;;; Client Private	
	ether7-Client-Private	Ethernet
	;;; Client-Private	
	ether8-Client-Private	Ethernet
	;;; Client-Private	
	ether9-Client-Private	Ethernet
	;;; Client-Private	
	ether10-Client-Private	Ethernet
	;;; Client-Private	
	sfp1-Client-Private	Ethernet
	;;; Client-Private	
X	wlan1-Client-Private	Wireless (Atheros AR

Set Port Horizon Value according to policy for servers



Bridge Port <sfp1-Client-Private>

General | Status

Interface: ether1--Layer2-Uplink

Bridge: bridge1

Priority: 80 hex

Path Cost: 10

Horizon: 77- Unique value allows all ports access

Edge: auto

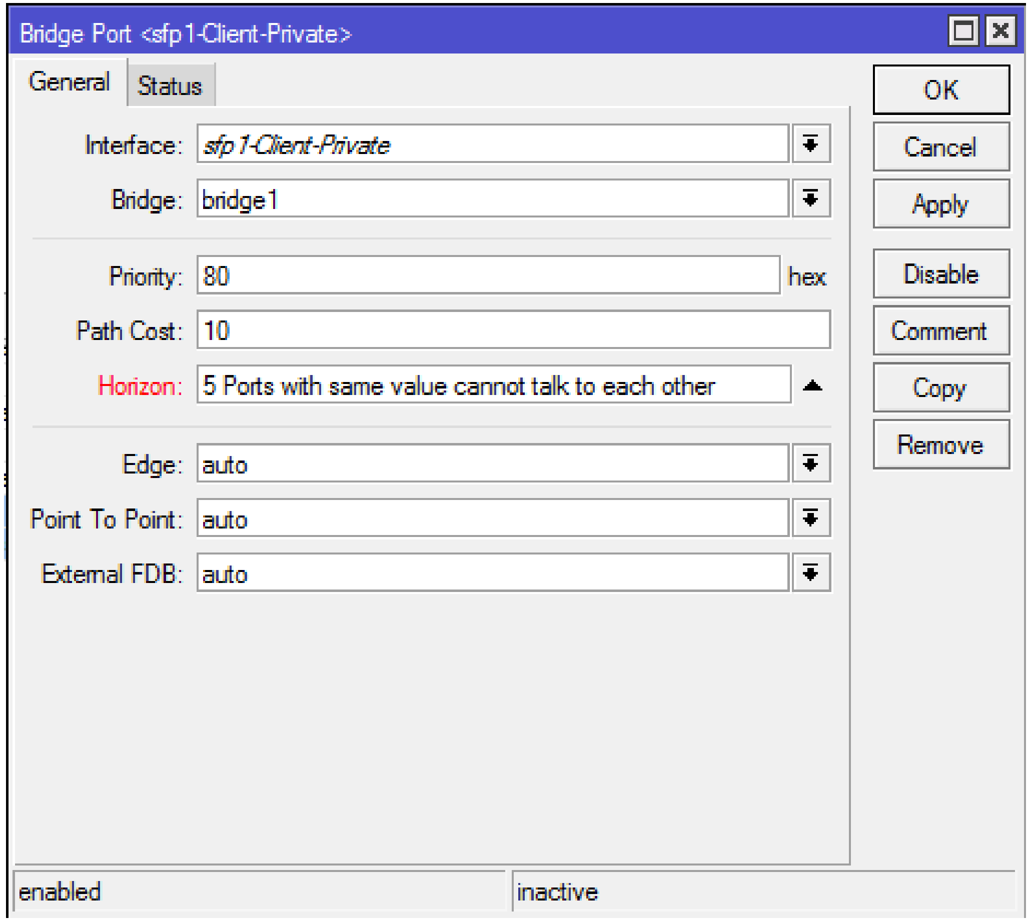
Point To Point: auto

External FDB: auto

enabled

inactive

Set Bridge port Horizon value for Clients



Bridge Port <sfp1-Client-Private>

Interface: *sfp1-Client-Private*

Bridge: bridge1

Priority: 80 hex

Path Cost: 10

Horizon: 5 Ports with same value cannot talk to each other

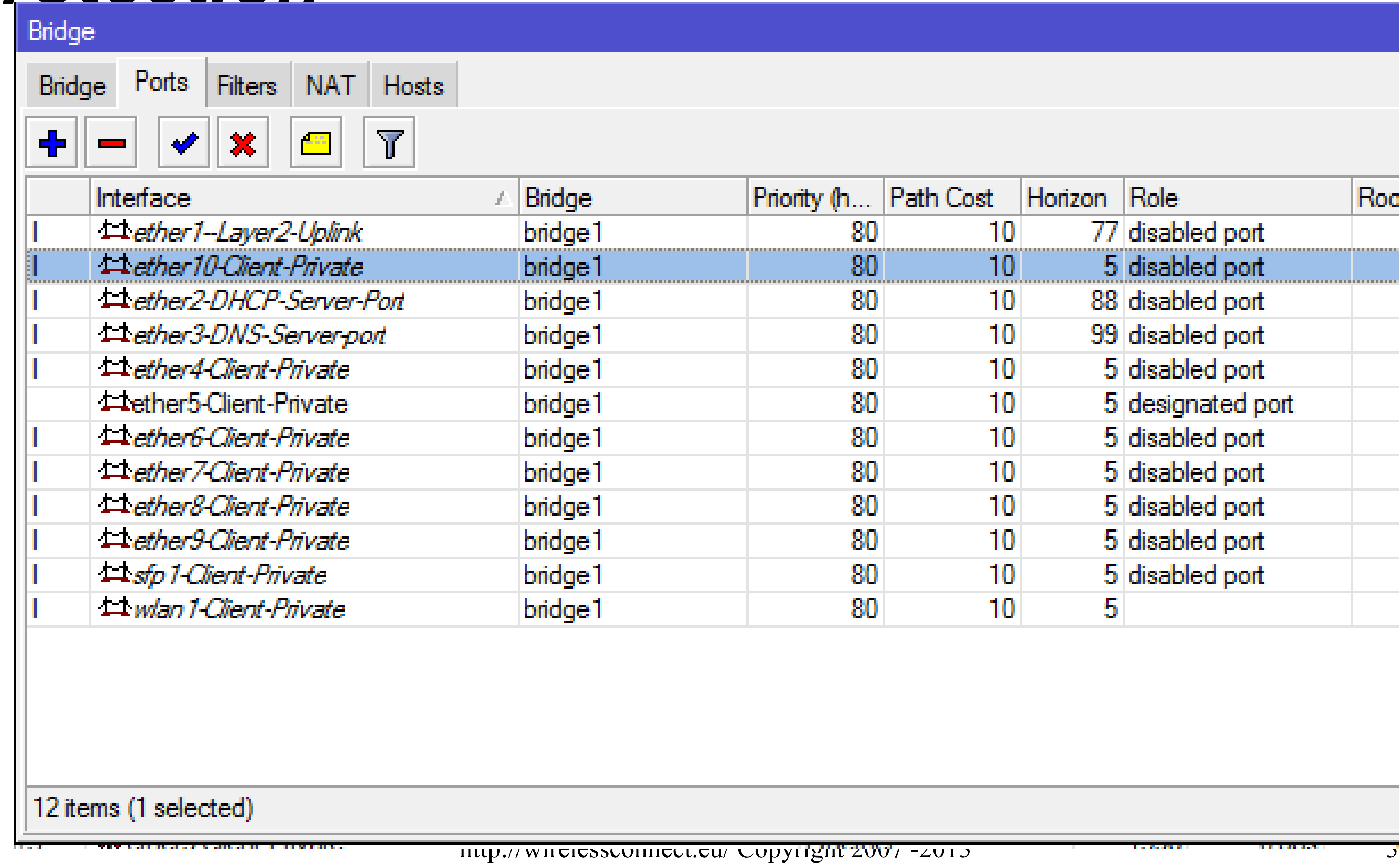
Edge: auto

Point To Point: auto

External FDB: auto

enabled   inactive

Configured Bridge / Switch with Pvlan Protection



Bridge

Bridge | Ports | Filters | NAT | Hosts

	Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Roo
I	ether1--Layer2-Uplink	bridge1	80	10	77	disabled port	
I	ether10-Client-Private	bridge1	80	10	5	disabled port	
I	ether2-DHCP-Server-Port	bridge1	80	10	88	disabled port	
I	ether3-DNS-Server-port	bridge1	80	10	99	disabled port	
I	ether4-Client-Private	bridge1	80	10	5	disabled port	
	ether5-Client-Private	bridge1	80	10	5	designated port	
I	ether6-Client-Private	bridge1	80	10	5	disabled port	
I	ether7-Client-Private	bridge1	80	10	5	disabled port	
I	ether8-Client-Private	bridge1	80	10	5	disabled port	
I	ether9-Client-Private	bridge1	80	10	5	disabled port	
I	sfp1-Client-Private	bridge1	80	10	5	disabled port	
I	wlan1-Client-Private	bridge1	80	10	5		

12 items (1 selected)

Thank You

- I hope you enjoyed the Presentation as Much As I Did :)
- Come over and Chat with me about security, networking and other exciting technologies, over a cup of tea!
- Thanks to Mikrotik Support Staff for dealing with so many of my requests... and keep pushing the developers!