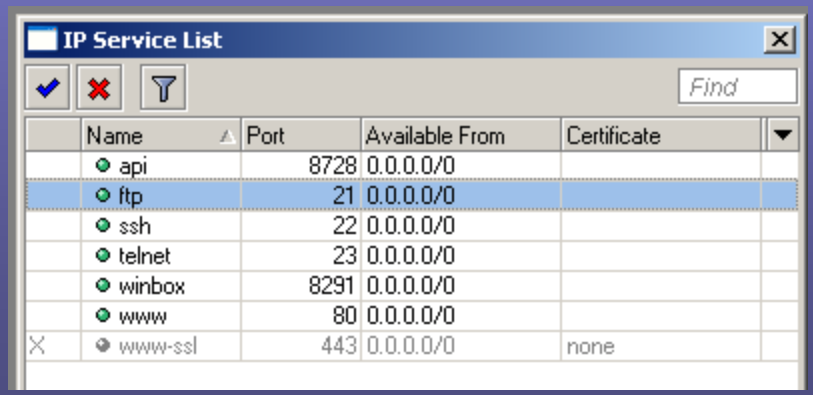
<3G Networks>

Mikrotik Security

IP -> Services

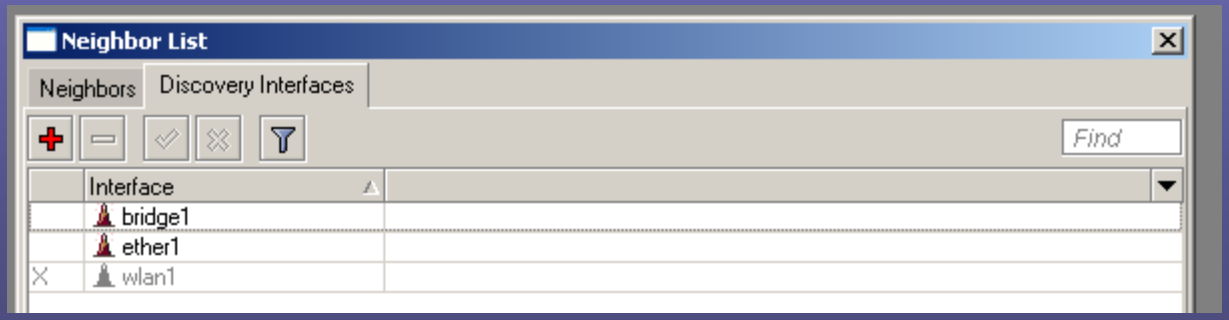
- Disable unused services
- Set Available From for appropriate hosts
- Secure protocols are preferred (Winbox/SSH)



	Name	Port	Available From	Certificate
	api	8728	0.0.0.0/0	
	ftp	21	0.0.0.0/0	
	ssh	22	0.0.0.0/0	
	telnet	23	0.0.0.0/0	
	winbox	8291	0.0.0.0/0	
	www	80	0.0.0.0/0	
X	www-ssl	443	0.0.0.0/0	none

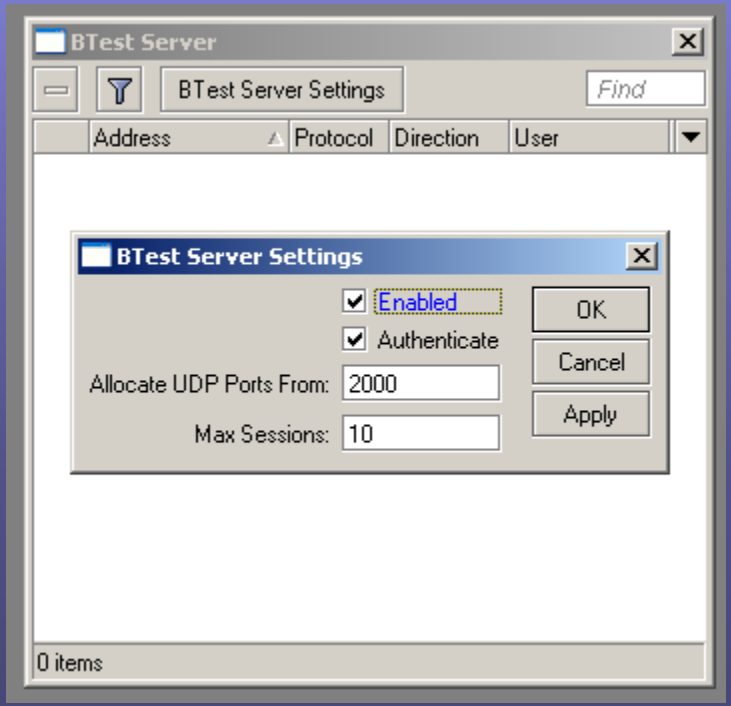
IP -> Neighbors

- Disable Discovery Interfaces where not necessary. All interfaces that don't directly connect to your own infrastructure.
- Note: Winbox discovery won't work if you disable neighbor discovery.



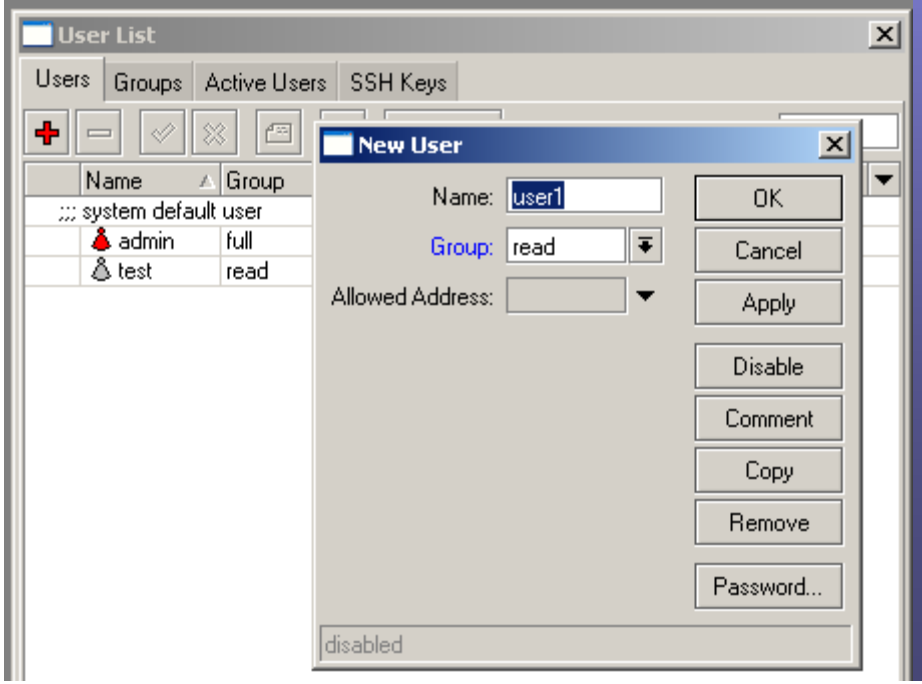
Tools -> Btest Server

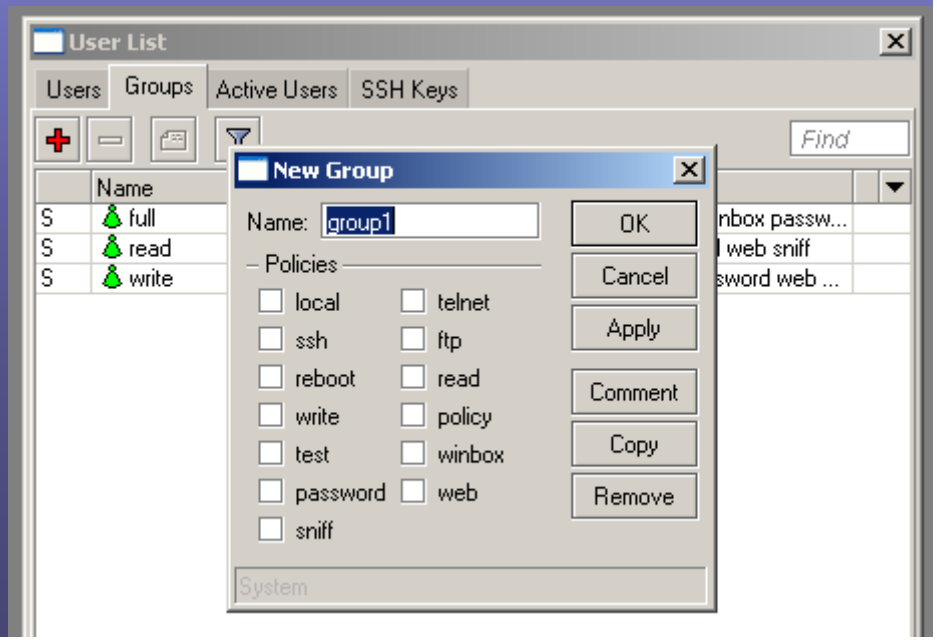
- By default the bandwidth test server is enabled. Be sure to only activate this when necessary.



System -> Users

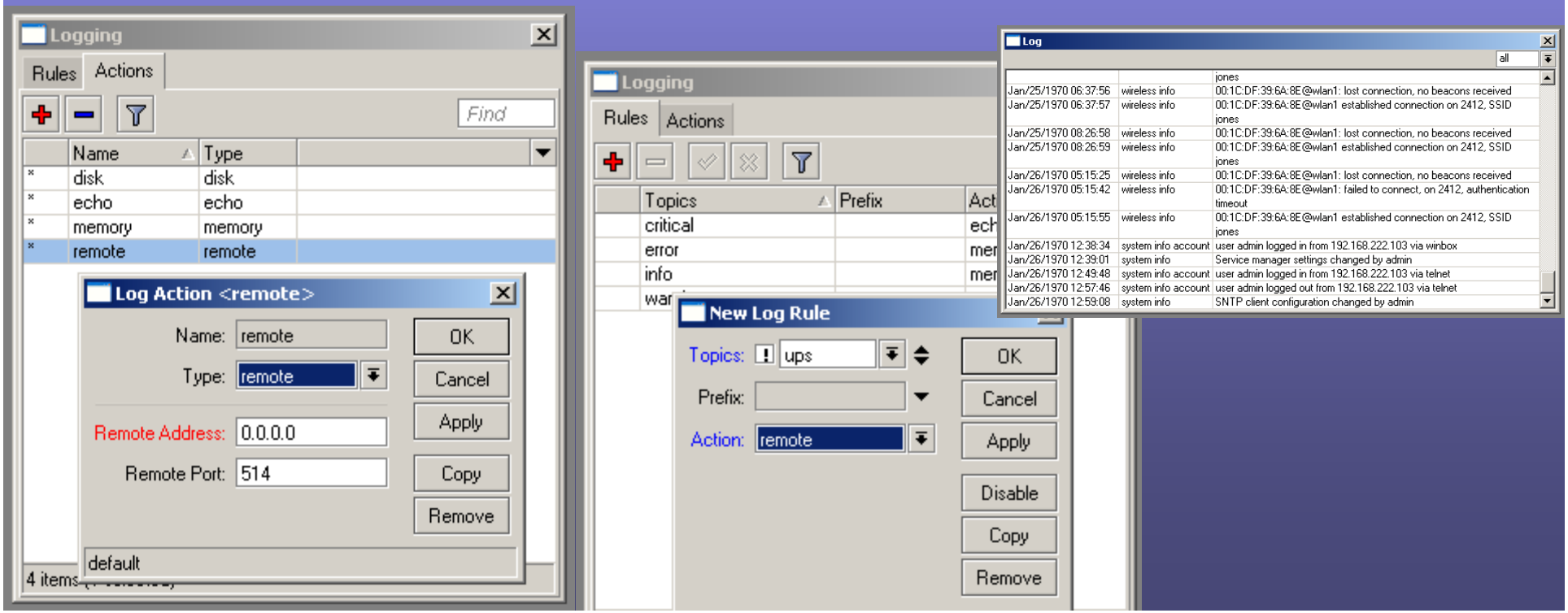
- Users are assigned to groups.
- Groups specify what access you get.
- User section allows password changes.



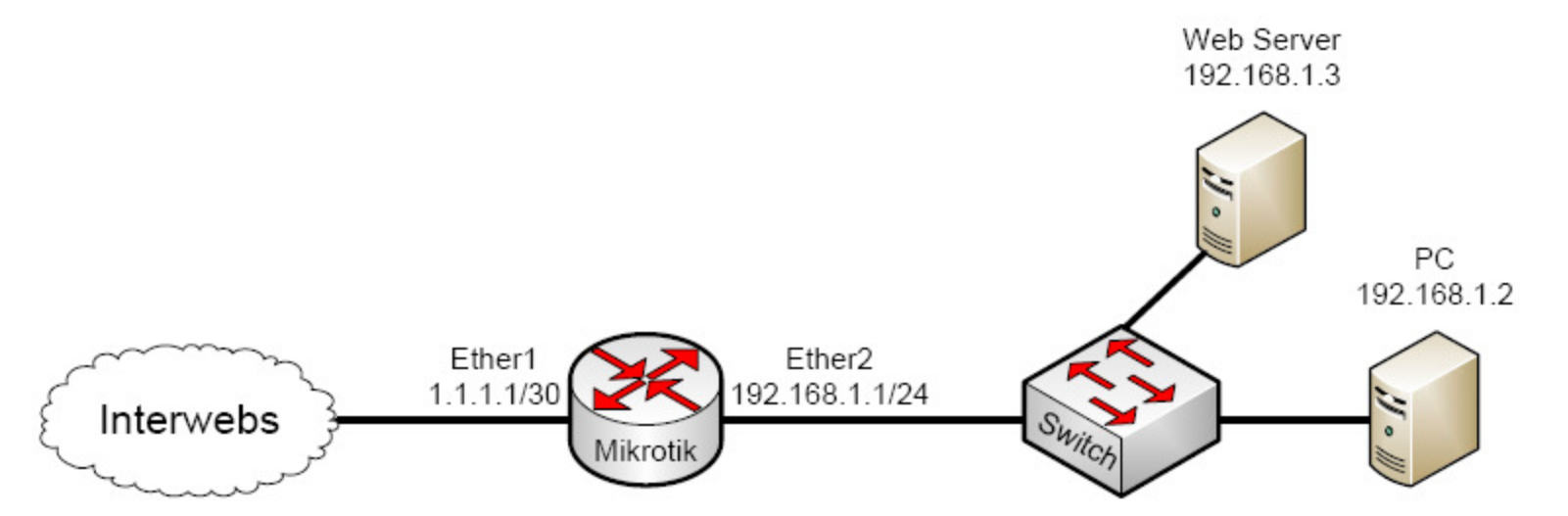


System -> Logging and Log

- Setup special actions to get more detail on a specific subject.
- Send to syslog server (CactiEZ).

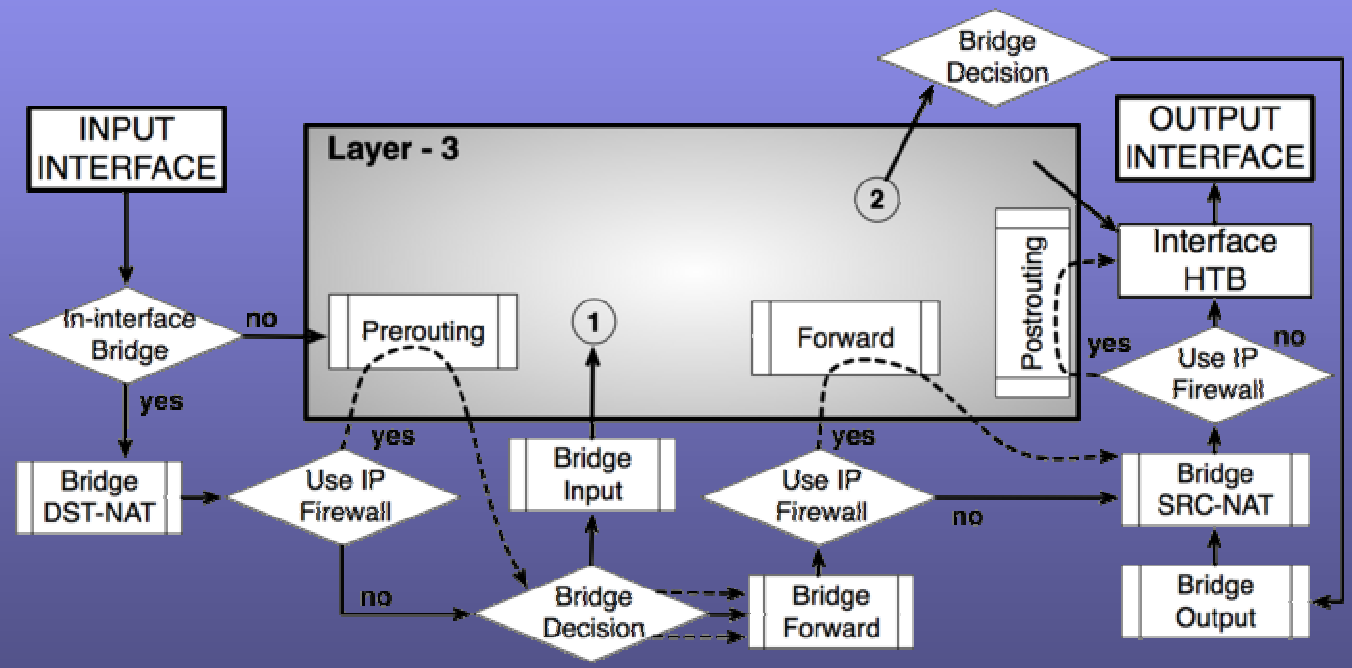


Basic Diagram



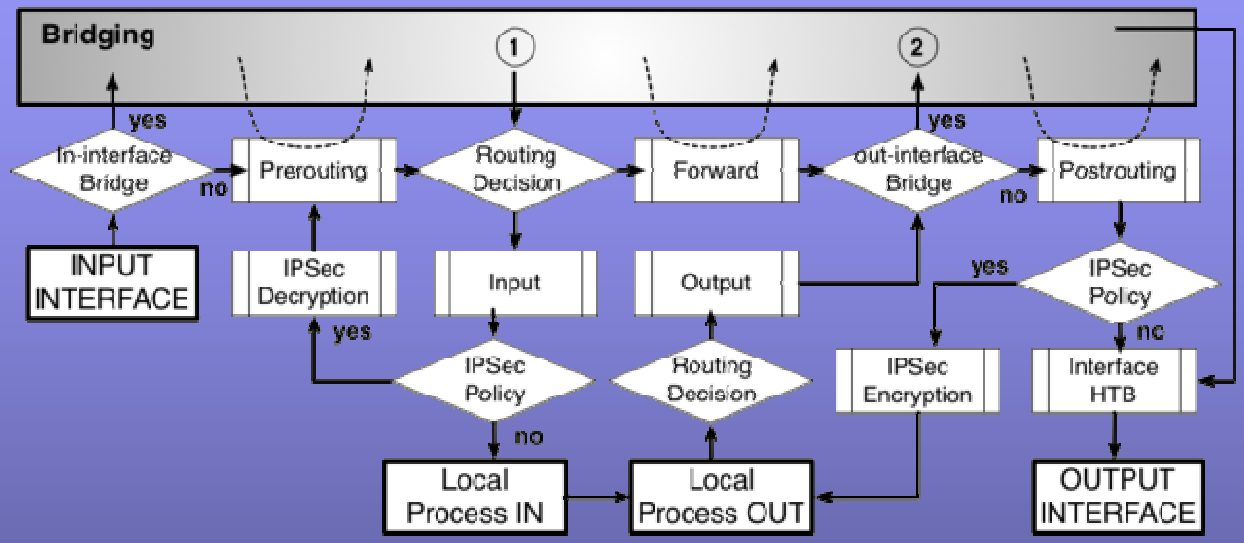
Packet Flow - Bridging

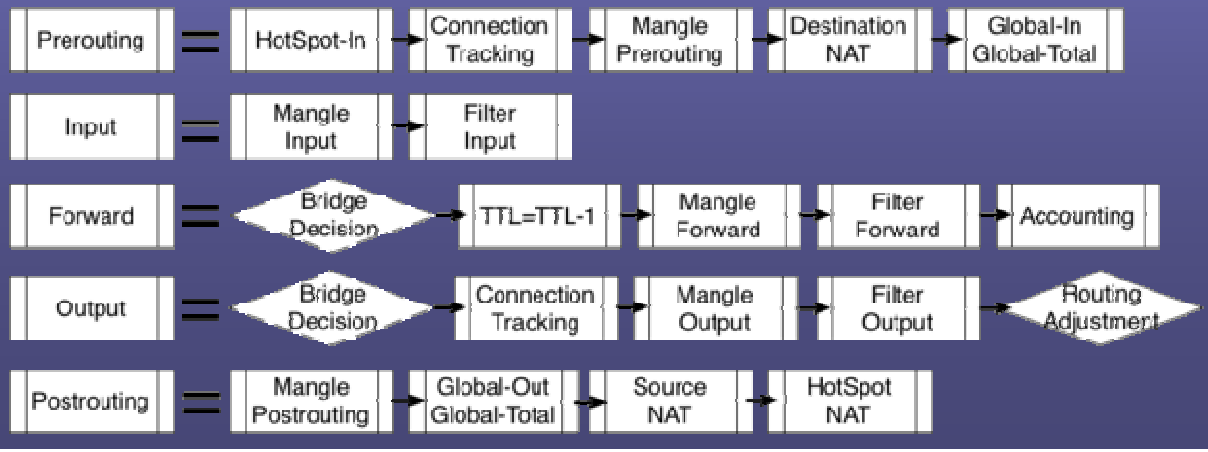
- Via http://wiki.mikrotik.com/wiki/Packet_Flow



Packet Flow - Routing

- Via http://wiki.mikrotik.com/wiki/Packet_Flow





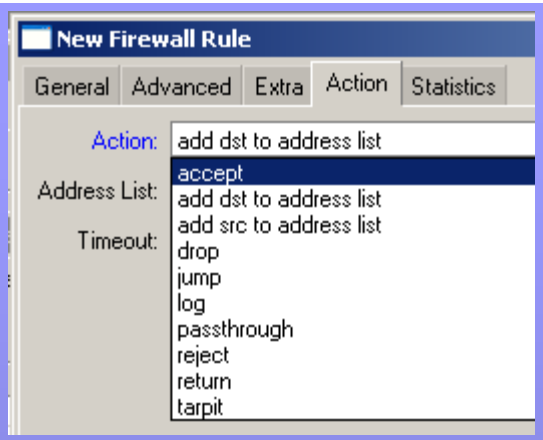
PAT Protection

- PAT(Port Address Translation) “NAT Overload”
- This gives you some protection because connections can’t be sourced from outside of your network.
- The easiest method is to IP -> firewall -> NAT. Then create a source nat with action of masquerade.

IP -> Firewall -> Filter

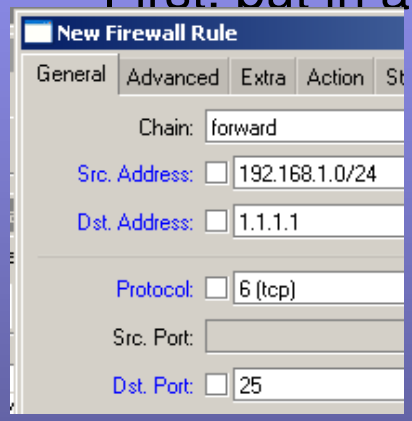
- Lets get down to the nitty gritty, firewall filtering.
- There are 3 chain options:
  - Input – The input chain is traffic destined TO the router. This would be someone trying to ping the router or IPSec traffic destined for the router.
  - Output – The output chain is traffic sourced from the router heading OUT. This would be an ICMP reply or the router initiating a ping out.
  - Forward – The forward chain is traffic moving through the router. This is where most all of our rules will be made.

- There are 10 action options (here are the most used):
  - Accept – This stops processing the rule and does nothing.
  - Add dst to address list – This will add the destination address to a specified address list. You can even specify an amount of time for the address to timeout of the list.
  - Add src to address list – Opposite of dst version.
  - Drop – This will discard packets that match this rule.
  - Log – This will put an entry in the log file every time this rule is matched. It will also include the src/dst IP address.
  - Tarpit – Used with botnet attacks. This will reply to the attack with a SYN/ACK packet and holds open the TCP session. This fools the attacker into thinking he hit the actual server when it is really just the router.

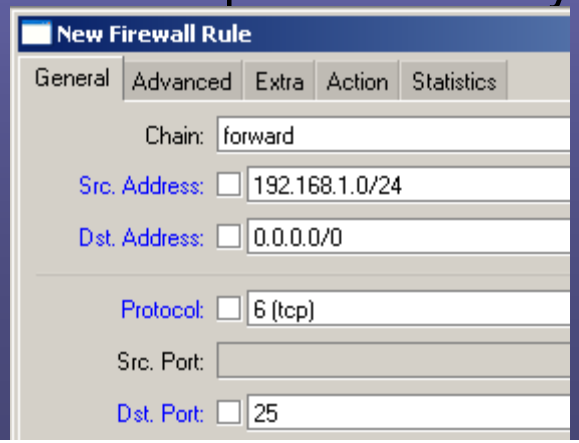


Allowing Specific SMTP Outbound

- Often you want to allow your users to only use your specific SMTP server. This will prevent users infected with viruses from spamming.
- First, put in an allow for a specific SMTP server.



- Now put in the deny for anyone trying to reach any other SMTP.

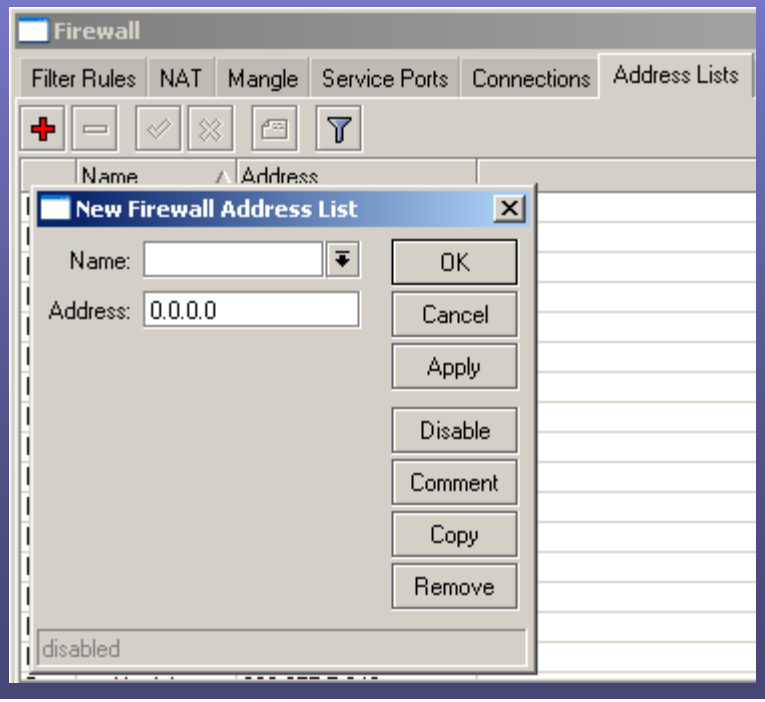


Arranging Rules

- The order of operation is very important. Rules are processed top down. A packet starts at the top of the firewall rules list. It keeps passing down the rules until it finds a match. Once it finds a match, processing is stopped.
- Rules can be dragged and dropped to change the order.

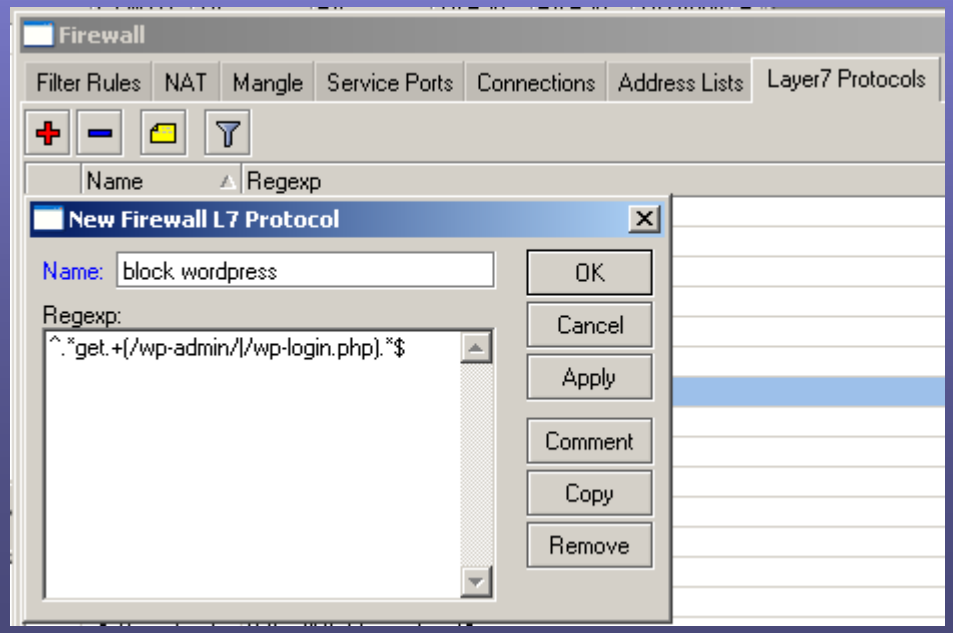
Address Lists

- Address lists can be lists of individual IP address or subnets. These can be used in filter rules or in mangle rules. These can be built manually or automatically.



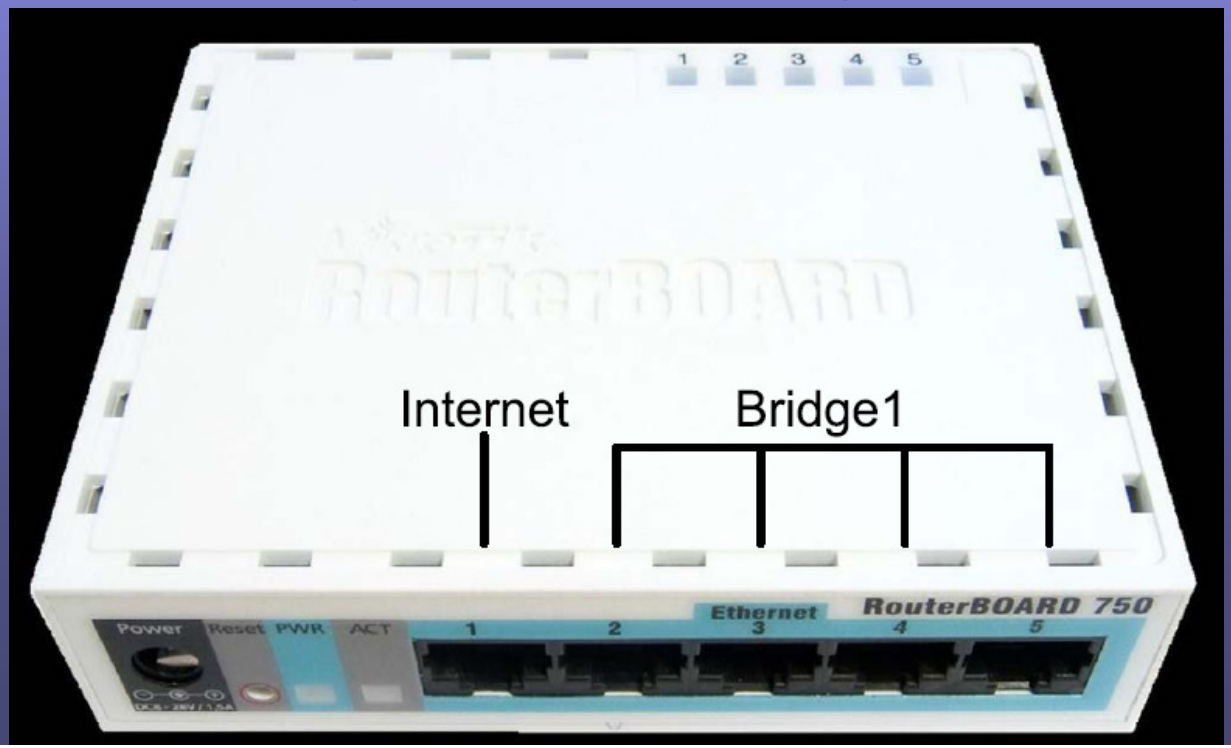
Layer 7 Matching

- L7 matching checks the data portion of the packet. This means the traffic can't be encrypted to be matched.
- The L7 matches in regex (regular expression) format.
- L7 can be used in firewall and mangle rules.



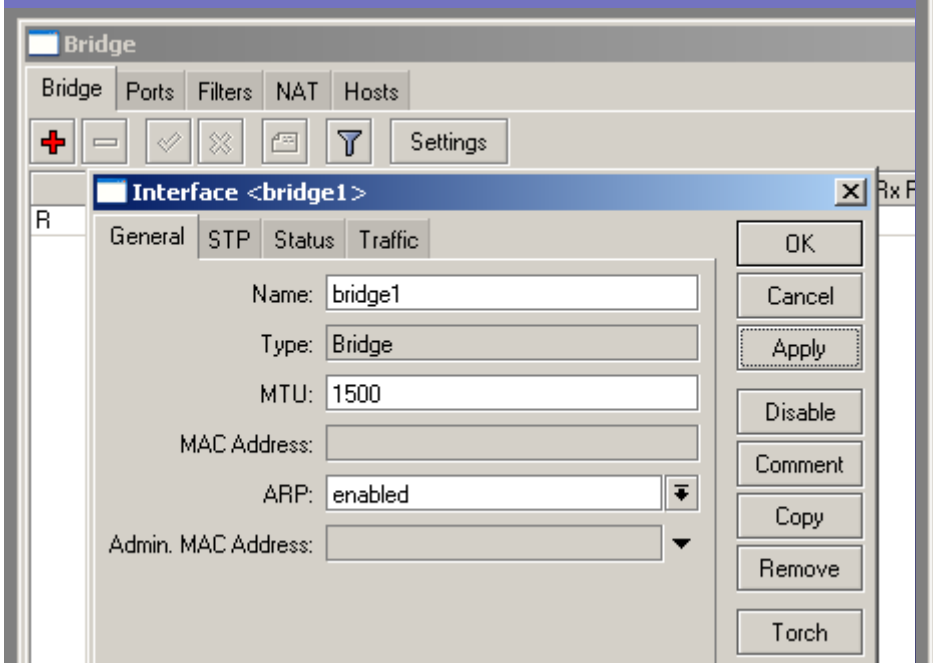
Bridging Interfaces

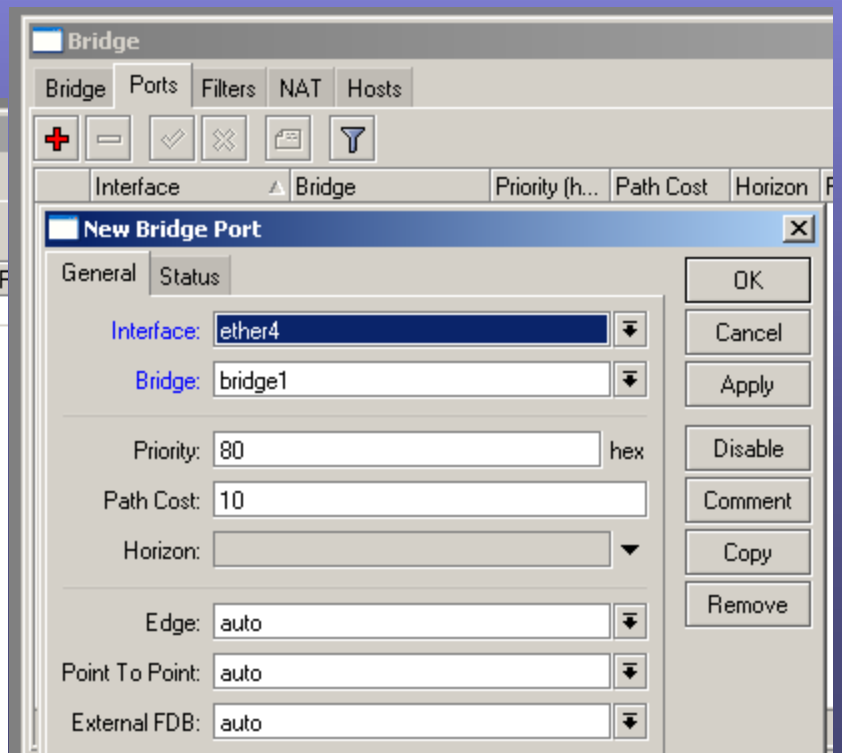
- For a 5 port RB, it is common to have a single internet interface and bridge the remaining interfaces together.
- An IP will be assigned to the Bridge interface.



Bridging Configuration

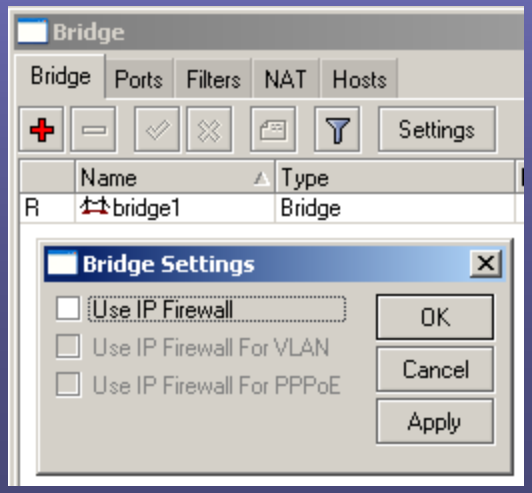
- Create the bridge
- Add ports to the bridge.





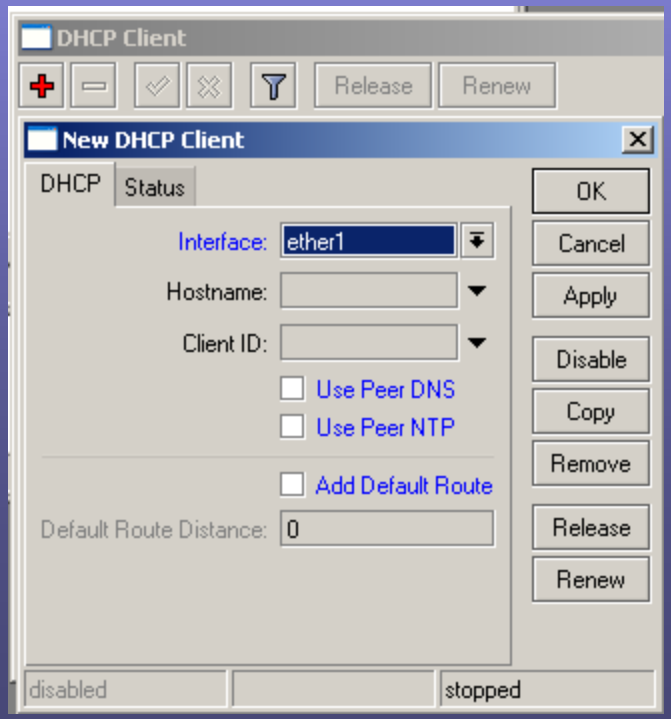
Enabling Bridging Firewall

- From bridge, click settings and then choose “Use IP Firewall”.



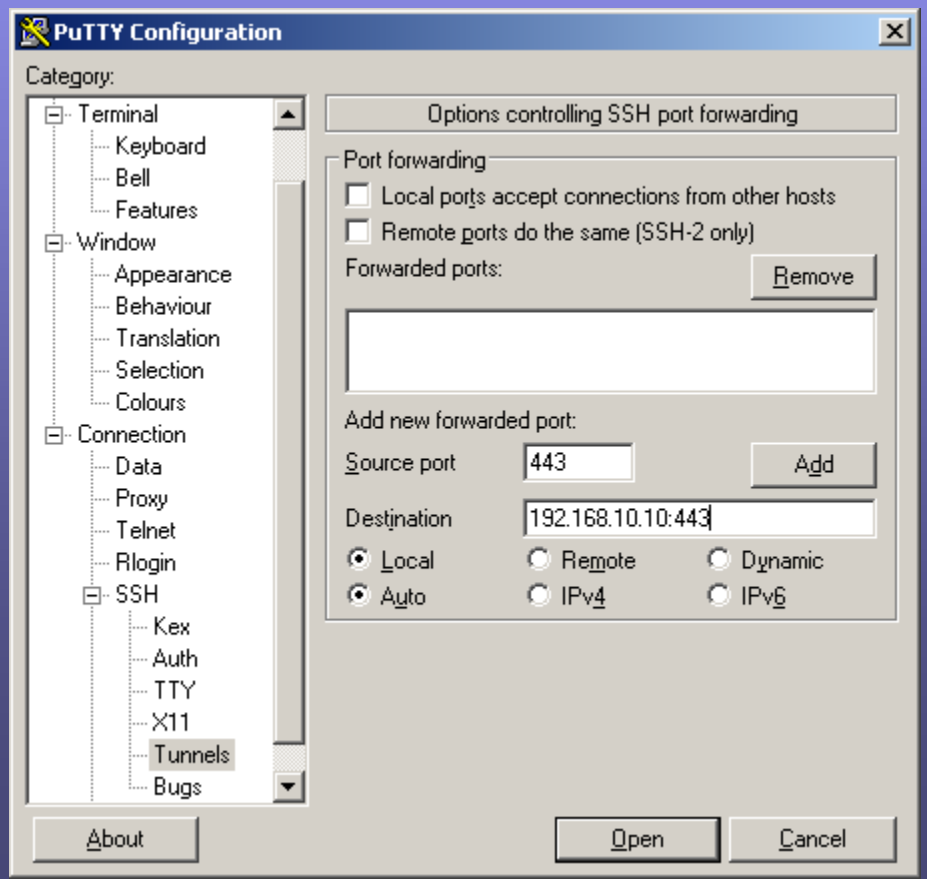
Rogue DHCP Detection

- There is a built in rogue detection program, though it gives false positives.
- I prefer to use IP -> DHCP Client, the DHCP Client.
- Be sure you uncheck DNS, NTP and Default route, otherwise a rogue can introduce new routes into your routing table.



SSH Tunnel

- Allows you to tunnel any traffic through the MTK into a network.



Resources

- Awesome Site – http://GregSowell.com
- Mikrotik Video Tutorials - http://gregsowell.com/?page_id=304
- Mikrotik Support Docs- http://www.mikrotik.com/testdocs/ros/3.0/
- CactiEZ - http://cactiez.cactiusers.org/download/
- Cacti Video Tutorials - http://gregsowell.com/?page_id=86
- Great Consultant ;)- http://gregsowell.com/?page_id=245