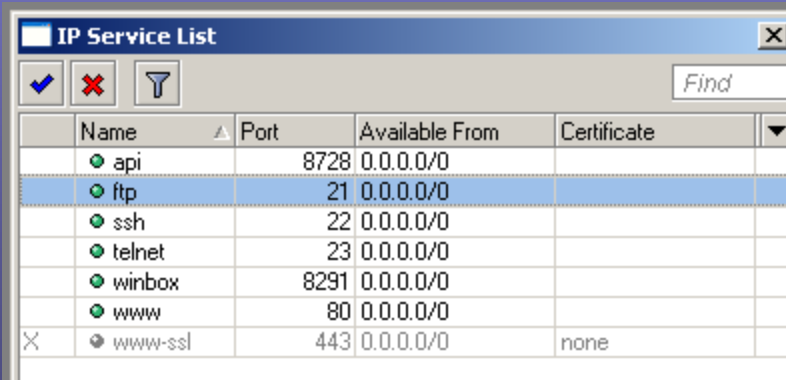


« 3G Networks »

Mikrotik Security

IP -> Services

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

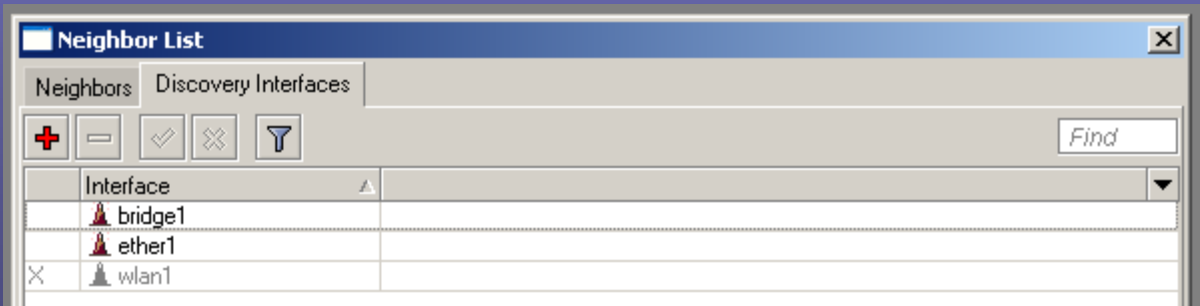


The screenshot shows a window titled "IP Service List" with a table of services. The table has columns for Name, Port, Available From, and Certificate. The services listed are api, ftp, ssh, telnet, winbox, www, and www-ssl. The ftp service is highlighted in blue.

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	
www-ssl	443	0.0.0.0/0	none

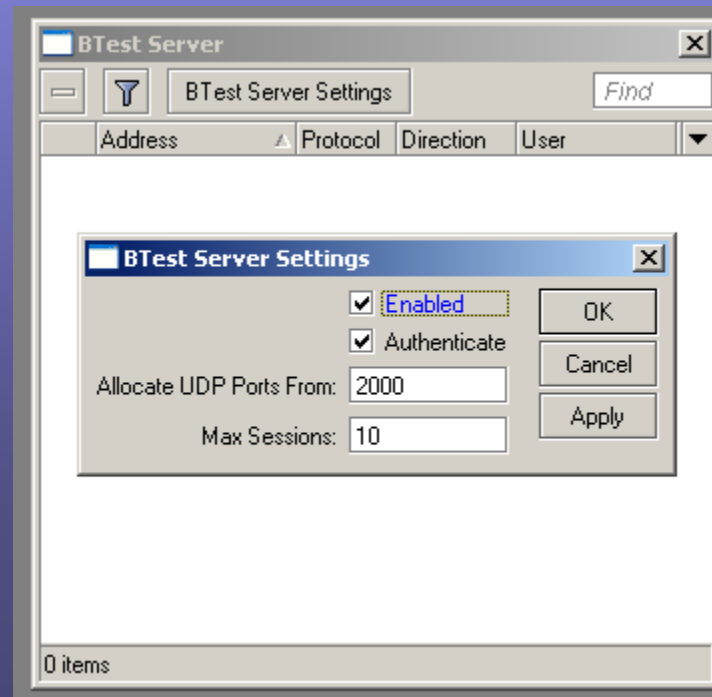
IP -> Neighbors

- 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.



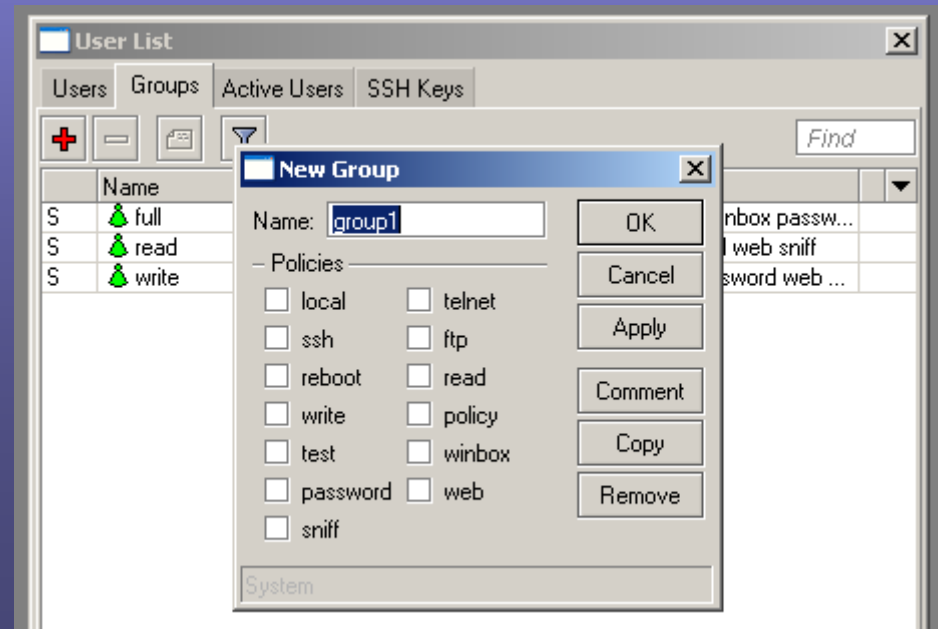
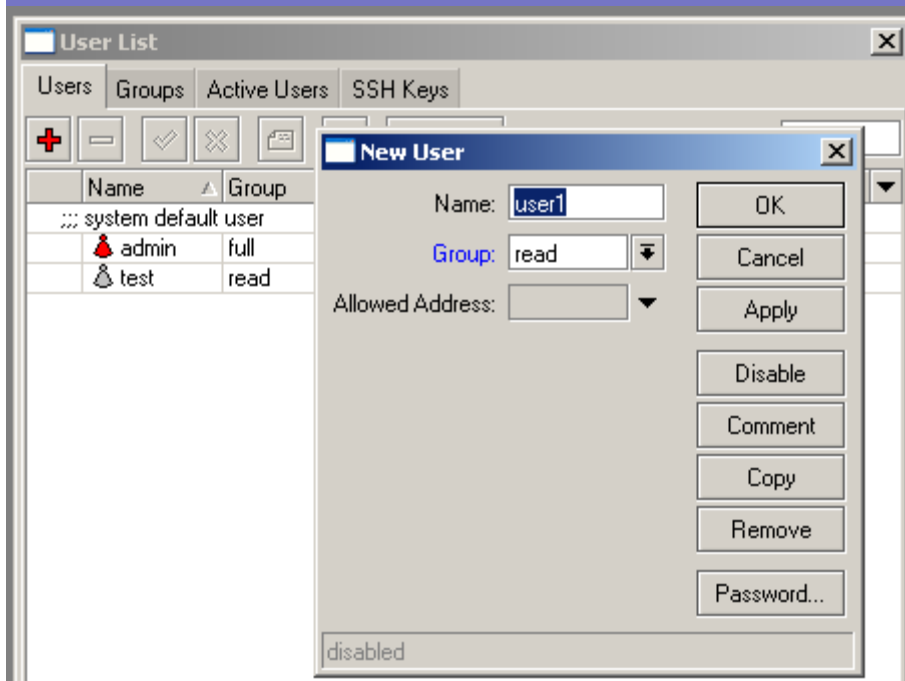
Tools -> Btest Server

- 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).

The screenshot displays the Mikrotik WinBox interface for configuring logging. It shows three overlapping windows:

- Logging (Rules tab):** A table listing logging rules. The 'remote' rule is selected.
- Log Action <remote>:** A configuration dialog for the 'remote' action, showing fields for Name, Type, Remote Address, and Remote Port.
- Log (Log tab):** A window showing a list of log entries with columns for Date/Time, Topic, Prefix, and Action.
- New Log Rule:** A dialog for creating a new rule, with 'ups' selected for Topics and 'remote' for Action.

Name	Type
* disk	disk
* echo	echo
* memory	memory
* remote	remote

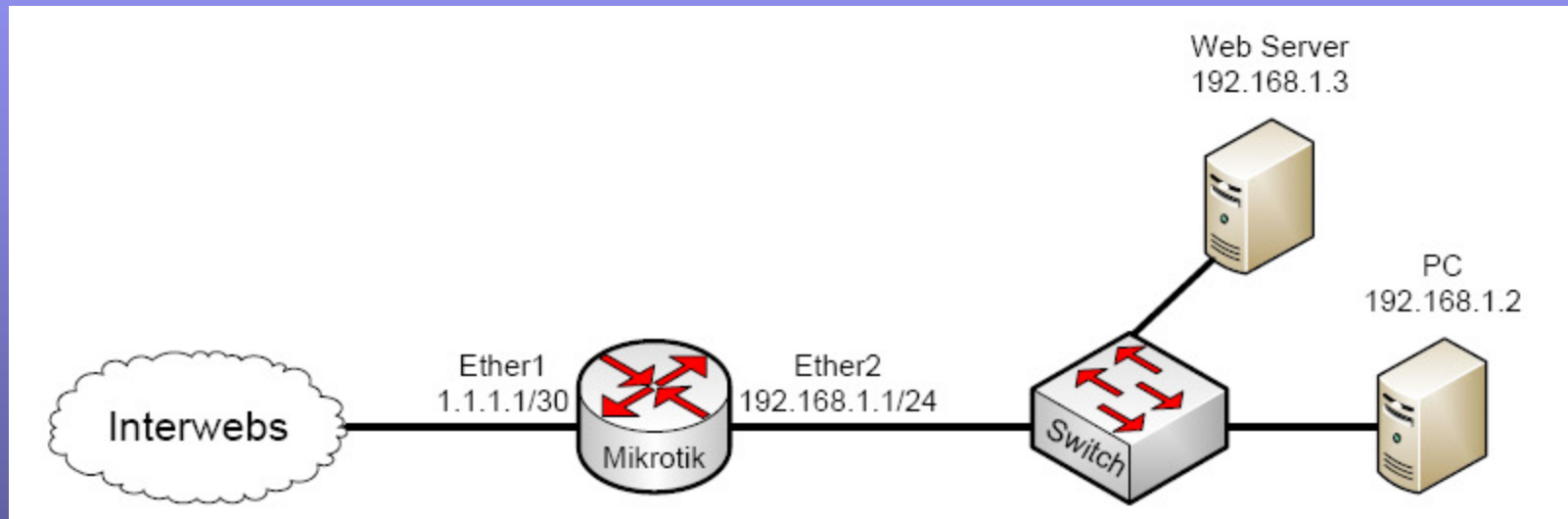
Name	Type
remote	remote

Topics	Prefix	Action
critical		echo
error		mer
info		mer
war		

Date/Time	Topic	Prefix	Action
Jan/25/1970 06:37:56	wireless info	00:1C:DF:39:6A:8E@wlan1:	lost connection, no beacons received
Jan/25/1970 06:37:57	wireless info	00:1C:DF:39:6A:8E@wlan1:	established connection on 2412, SSID jones
Jan/25/1970 08:26:58	wireless info	00:1C:DF:39:6A:8E@wlan1:	lost connection, no beacons received
Jan/25/1970 08:26:59	wireless info	00:1C:DF:39:6A:8E@wlan1:	established connection on 2412, SSID jones
Jan/26/1970 05:15:25	wireless info	00:1C:DF:39:6A:8E@wlan1:	lost connection, no beacons received
Jan/26/1970 05:15:42	wireless info	00:1C:DF:39:6A:8E@wlan1:	failed to connect, on 2412, authentication timeout
Jan/26/1970 05:15:55	wireless info	00:1C:DF:39:6A:8E@wlan1:	established connection on 2412, SSID jones
Jan/26/1970 12:38:34	system info account		user admin logged in from 192.168.222.103 via winbox
Jan/26/1970 12:39:01	system info		Service manager settings changed by admin
Jan/26/1970 12:49:48	system info account		user admin logged in from 192.168.222.103 via telnet
Jan/26/1970 12:57:46	system info account		user admin logged out from 192.168.222.103 via telnet
Jan/26/1970 12:59:08	system info		SNTP client configuration changed by admin

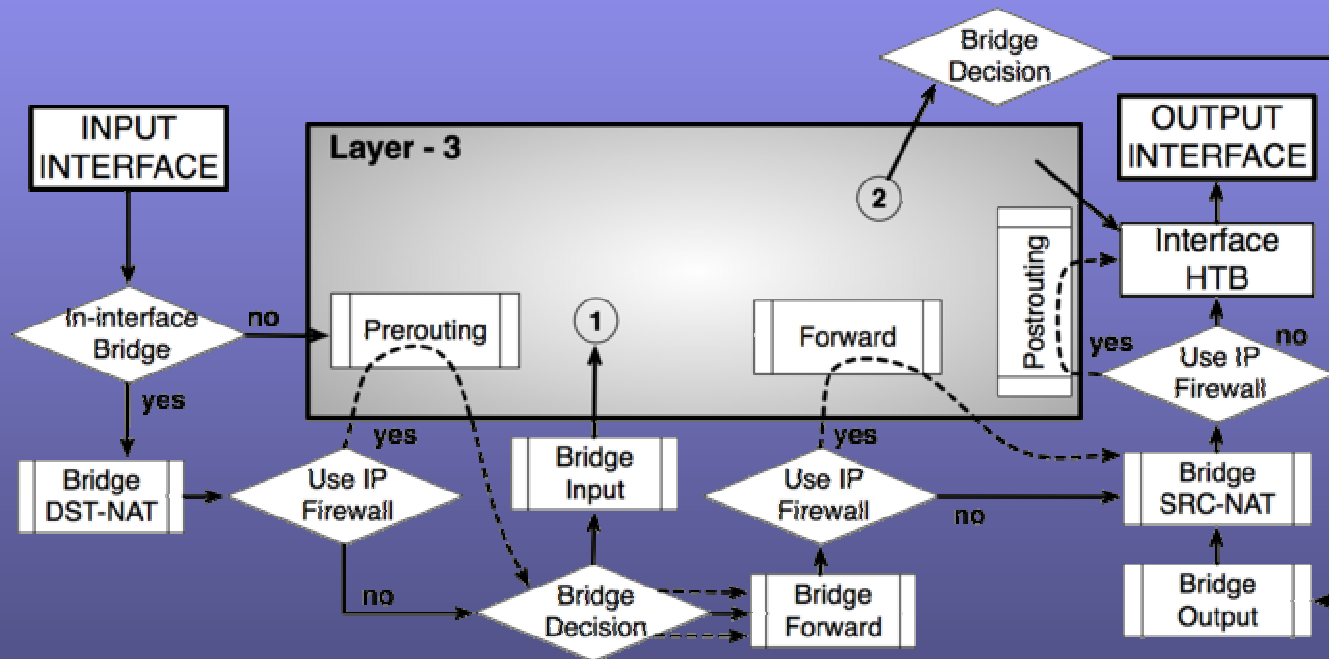
Topics	Action
ups	remote

Basic Diagram



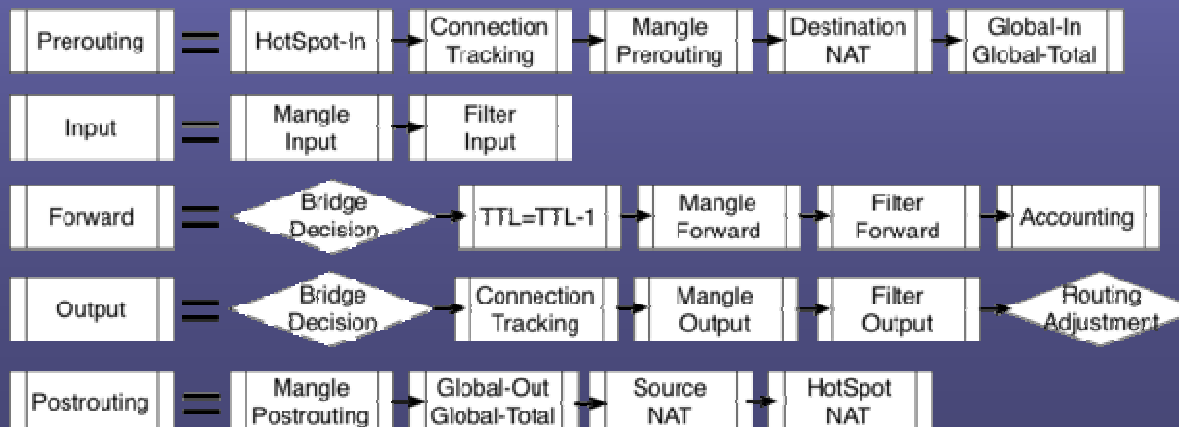
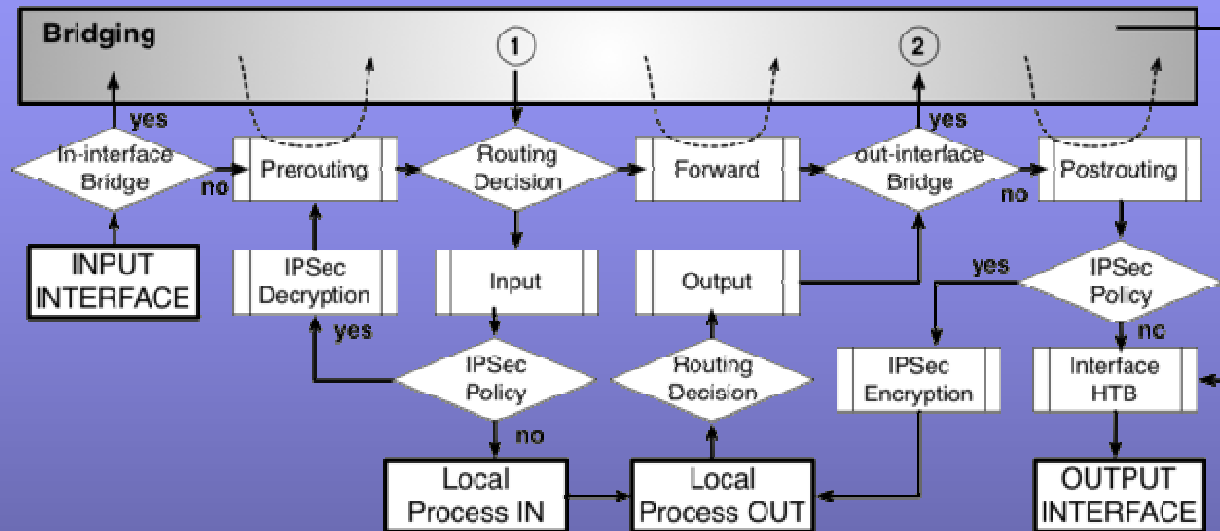
Packet Flow - Bridging

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



Packet Flow - Routing

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



PAT Protection

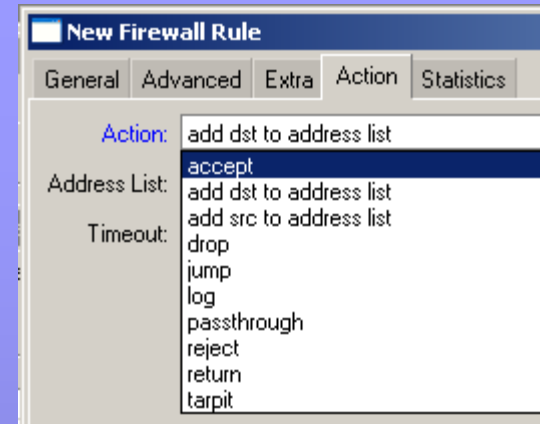
- PAT(Port Address Translation) “NAT Overload”
- This gives you some protection because connections can't be sourced from outside of your network.
- The easiest method is to IP -> firewall -> NAT. Then create a source nat with action of masquerade.

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.

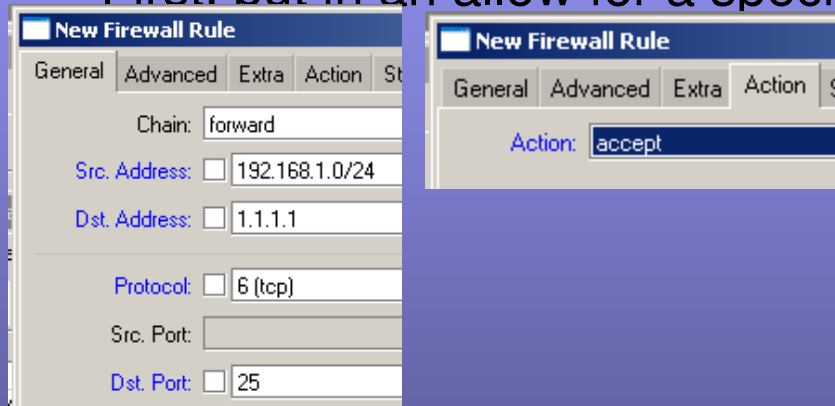
- There are 10 action options (here are the most used):

- 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

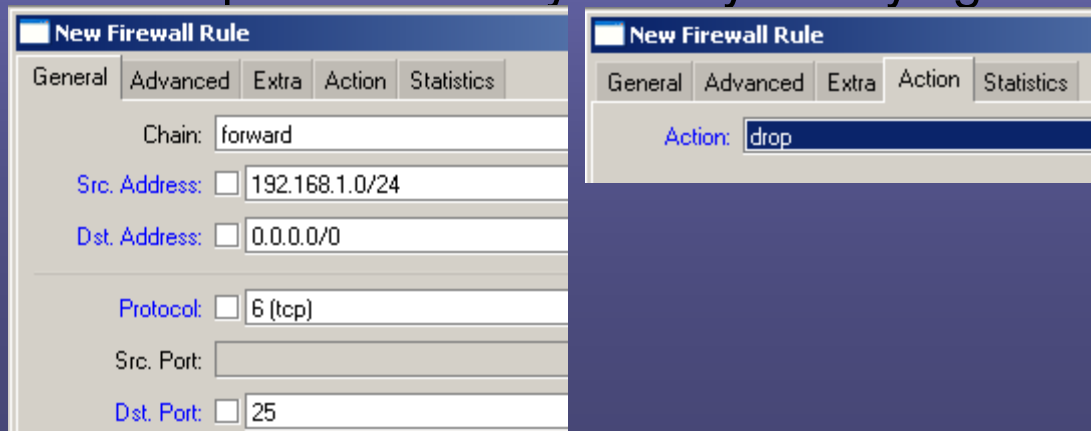
- Often you want to allow your users to only use your specific SMTP server. This will prevent users infected with viruses from spamming.
- First, put in an allow for a specific SMTP server.



The screenshot shows the 'New Firewall Rule' dialog box with the following configuration:

- Chain: forward
- Src. Address: 192.168.1.0/24
- Dst. Address: 1.1.1.1
- Protocol: 6 (tcp)
- Src. Port: (empty)
- Dst. Port: 25
- Action: accept

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



The screenshot shows the 'New Firewall Rule' dialog box with the following configuration:

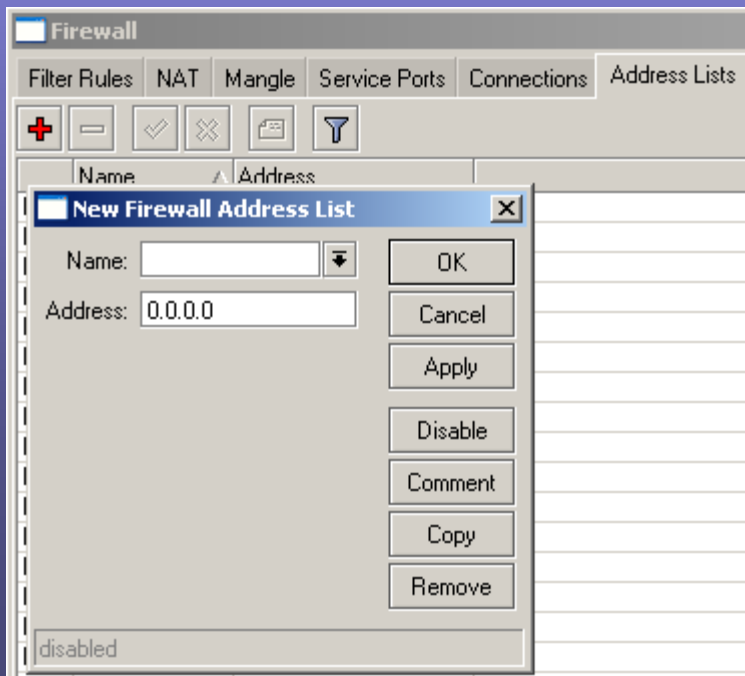
- Chain: forward
- Src. Address: 192.168.1.0/24
- Dst. Address: 0.0.0.0/0
- Protocol: 6 (tcp)
- Src. Port: (empty)
- Dst. Port: 25
- Action: drop

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.

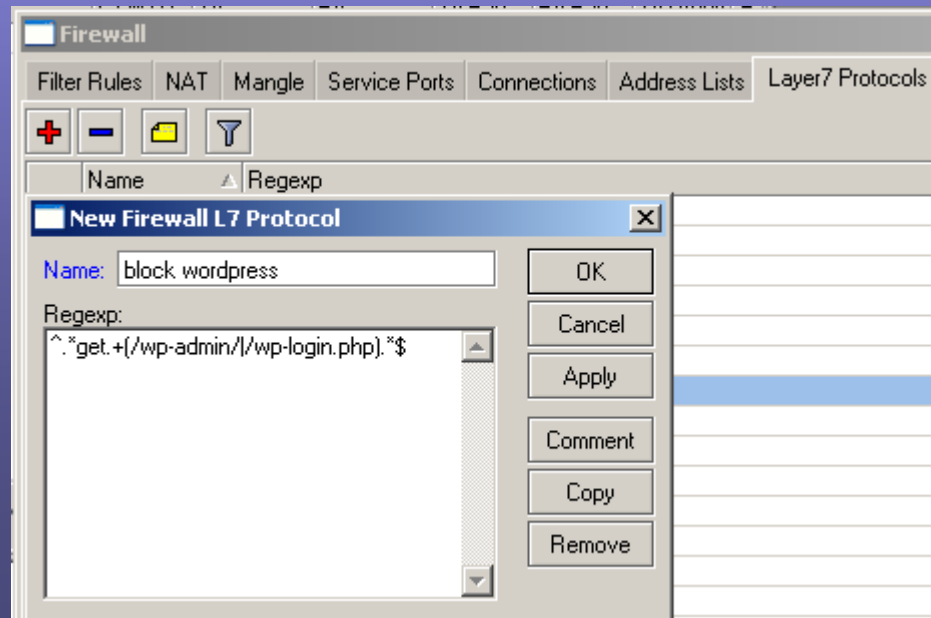
Address Lists

- 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.



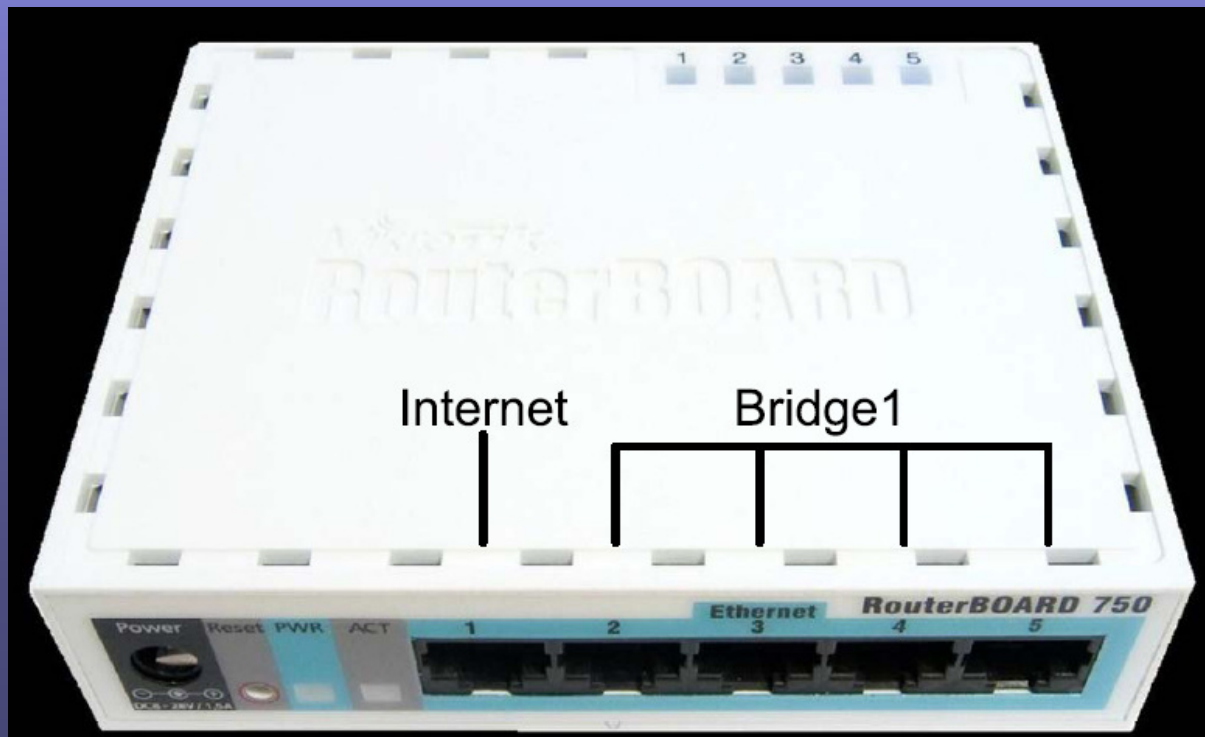
Layer 7 Matching

- 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.



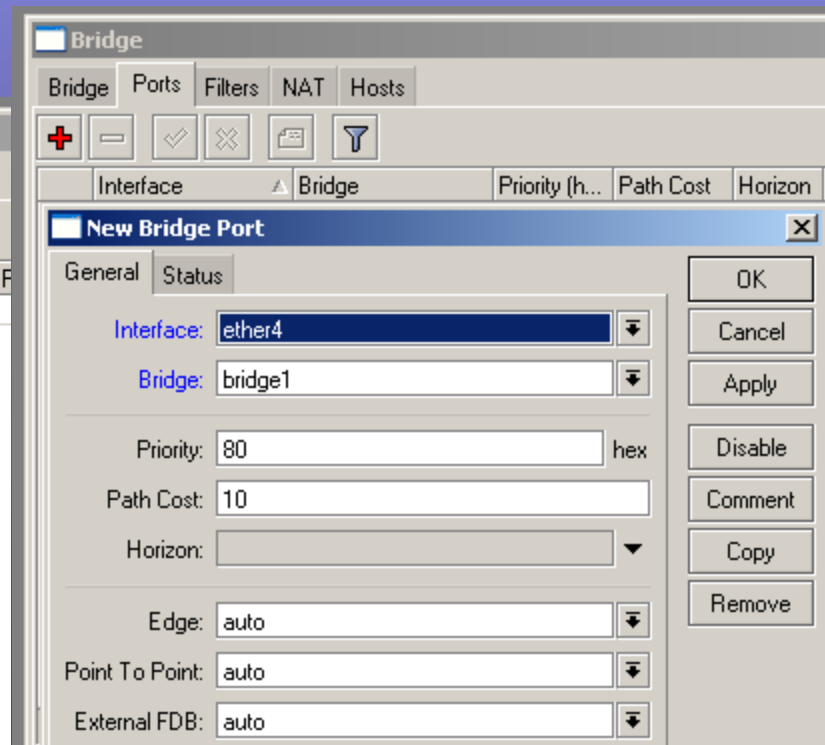
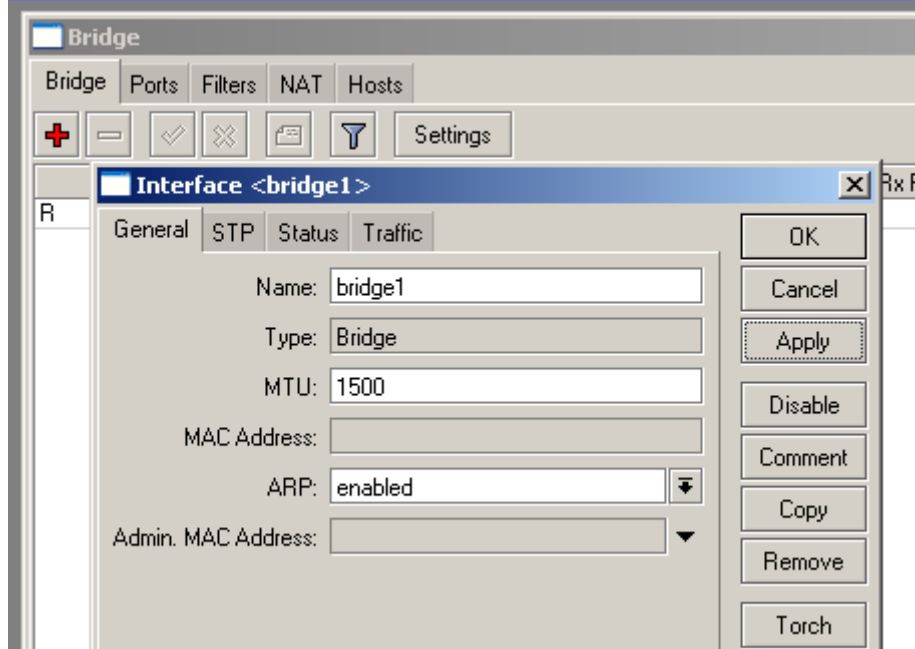
Bridging Interfaces

- 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.



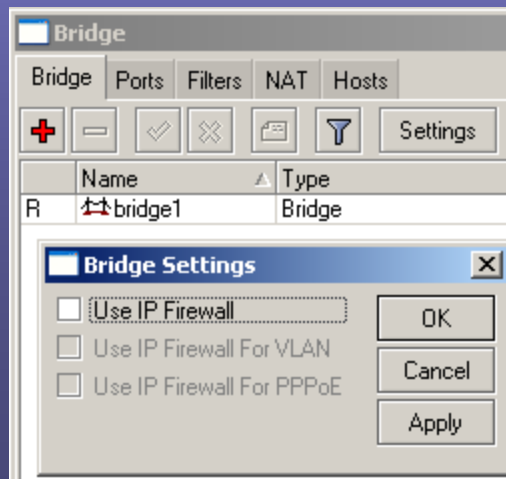
Bridging Configuration

- Create the bridge
- Add ports to the bridge.



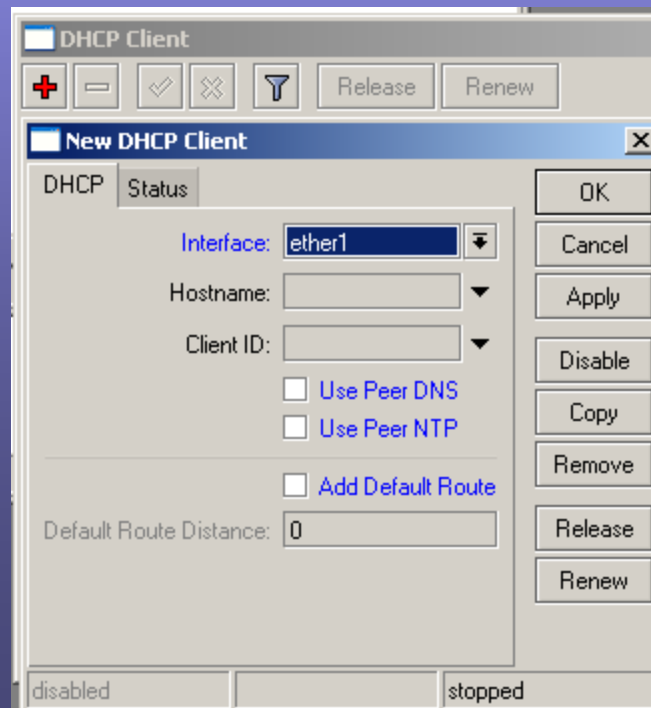
Enabling Bridging Firewall

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



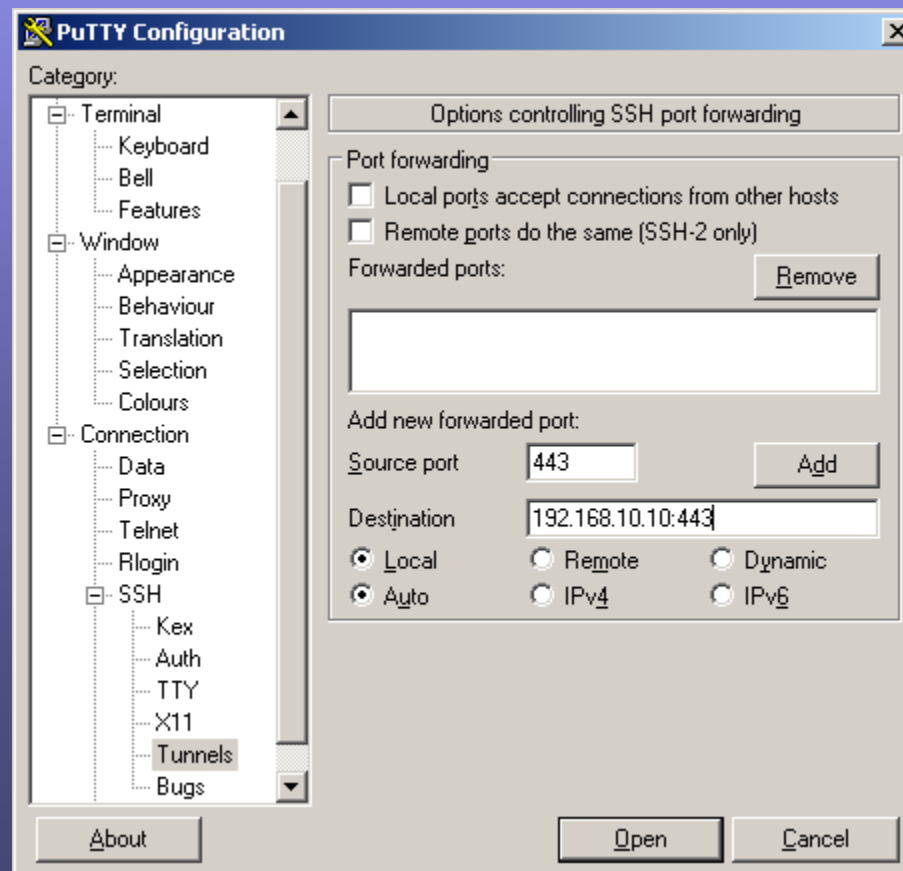
Rogue DHCP Detection

- 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