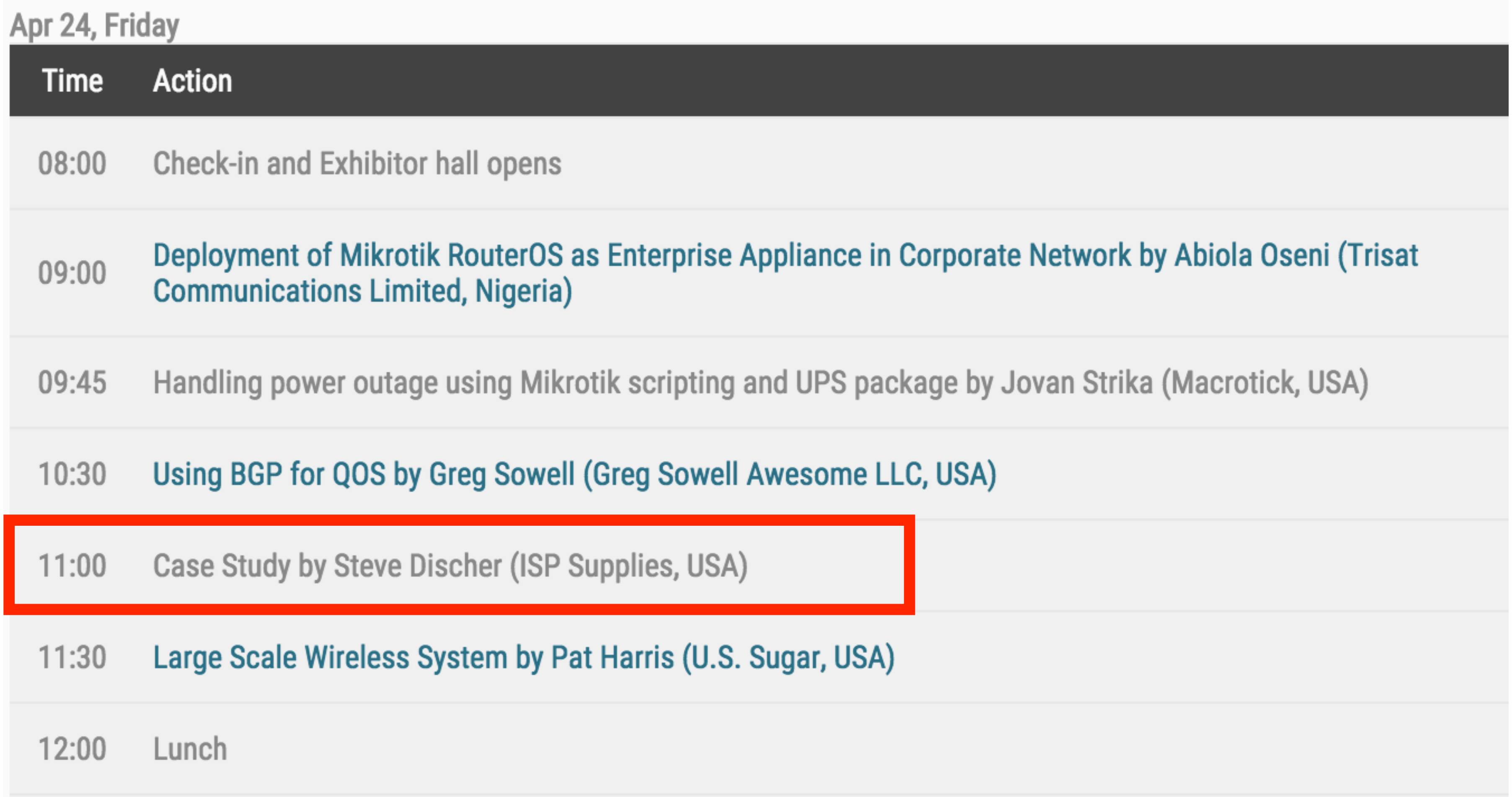
About Me

- Steve Discher, from College Station, Texas, USA
- MikroTik Certified Trainer since 2008 and teach RouterOS classes, LearnMikroTik.com and blog at SteveDischer.com
- Operate a wireless distribution company, ISPSupplies.com

Congratulations to 13 New MTCNA's



Apr 24, Friday

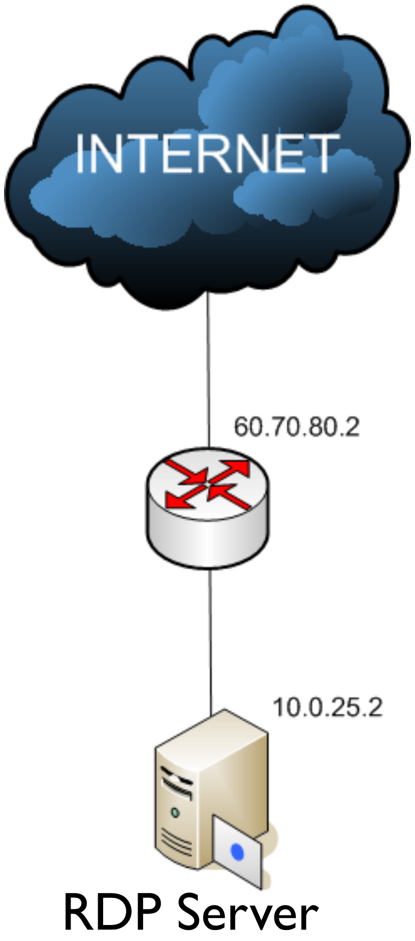
Time	Action
08:00	Check-in and Exhibitor hall opens
09:00	Deployment of Mikrotik RouterOS as Enterprise Appliance in Corporate Network by Abiola Oseni (Trisat Communications Limited, Nigeria)
09:45	Handling power outage using Mikrotik scripting and UPS package by Jovan Strika (Macrotick, USA)
10:30	Using BGP for QOS by Greg Sowell (Greg Sowell Awesome LLC, USA)
11:00	Case Study by Steve Discher (ISP Supplies, USA)
11:30	Large Scale Wireless System by Pat Harris (U.S. Sugar, USA)
12:00	Lunch

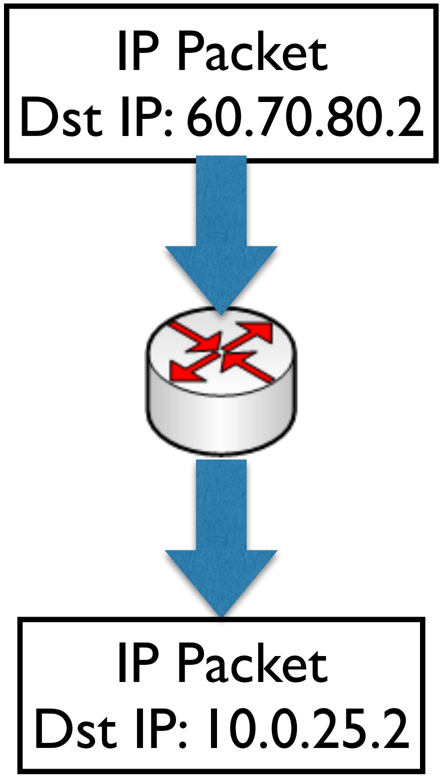
Look at nine different RouterOS forgotten features, configuration calamities and some sweet solutions to simple problems

Inbound NAT with a Dynamic IP

PROBLEM: I have a dynamic WAN IP but want to allow inbound services

Destination NAT With a Dynamic IP

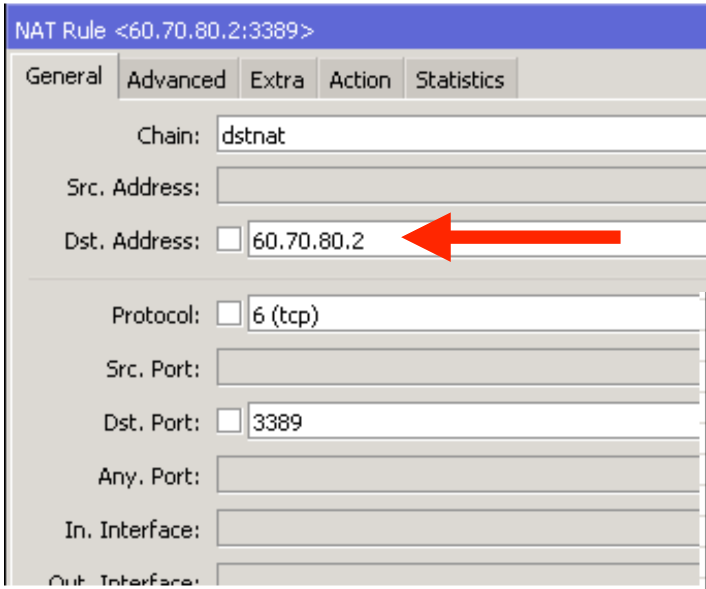




IP Packet
Dst IP: 60.70.80.2

IP Packet
Dst IP: 10.0.25.2

Destination NAT With a Dynamic IP



NAT Rule <60.70.80.2:3389>

Chain: dstnat

Src. Address:

Dst. Address: □ 60.70.80.2

Protocol: □ 6 (tcp)

Src. Port:

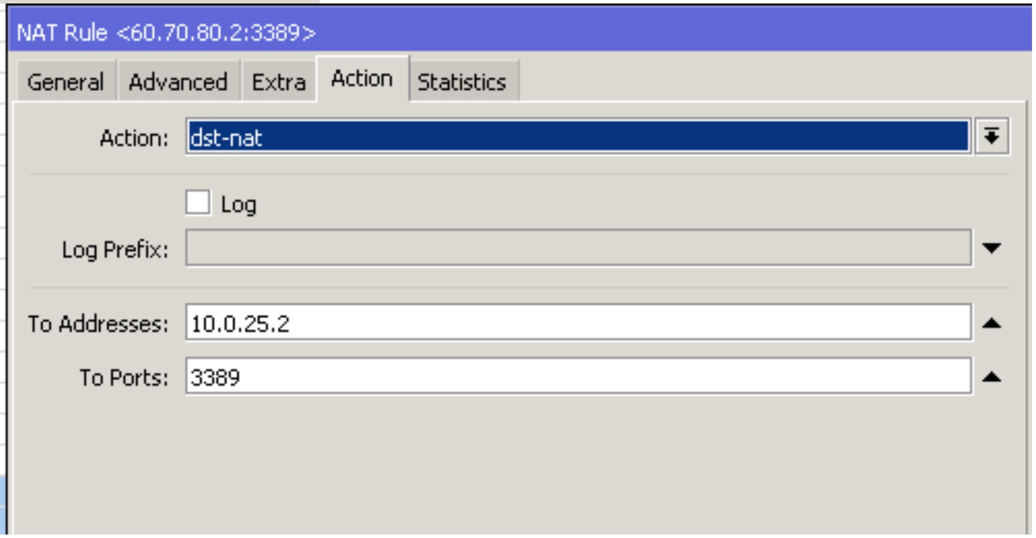
Dst. Port: □ 3389

Any. Port:

In. Interface:

Out. Interface:

With a static IP, it is simple…



NAT Rule <60.70.80.2:3389>

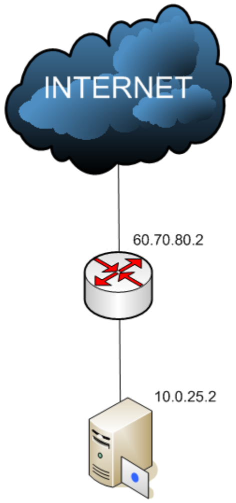
Action: dst-nat

□ Log

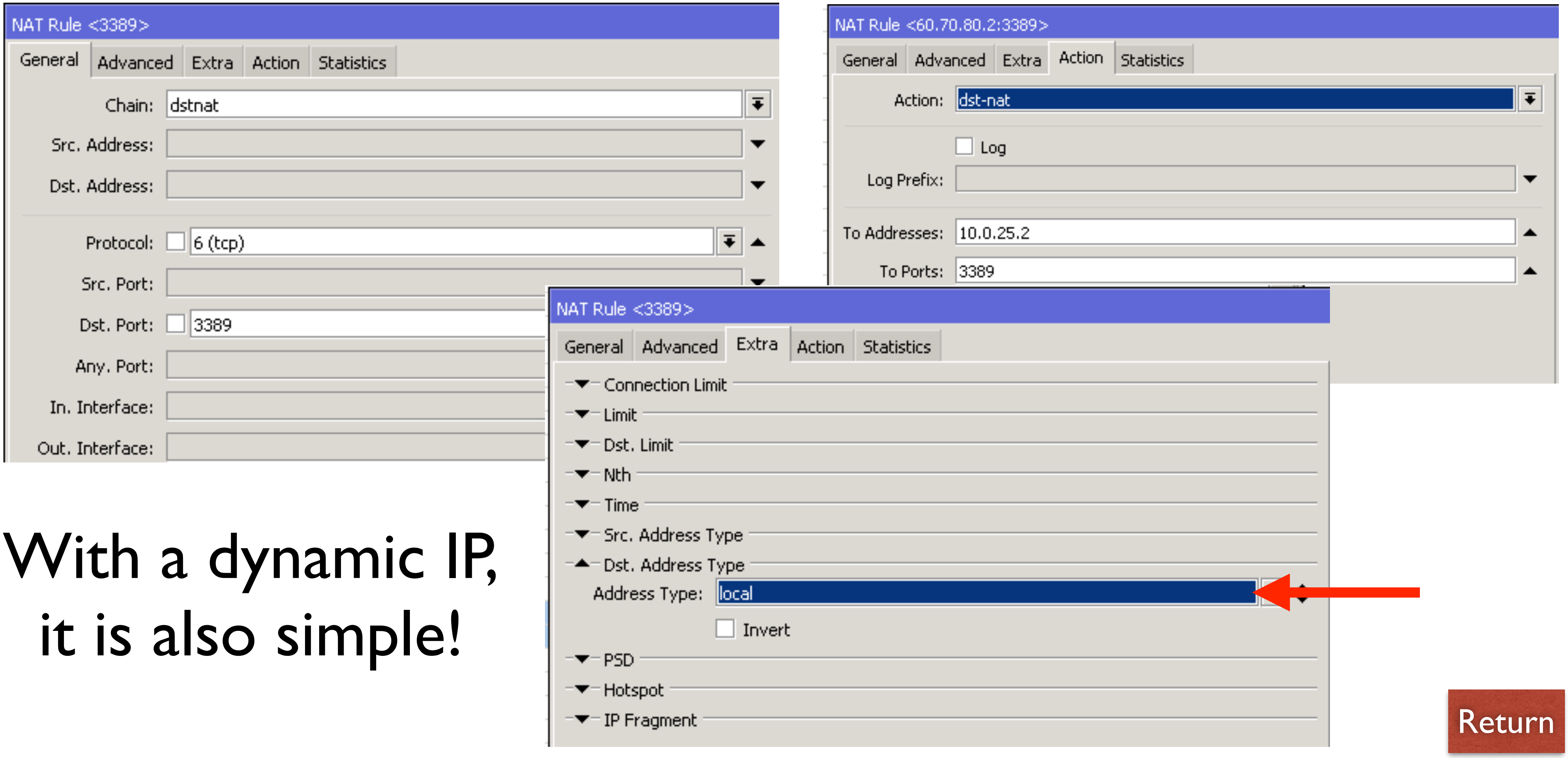
Log Prefix:

To Addresses: 10.0.25.2

To Ports: 3389



Destination NAT With a Dynamic IP



NAT Rule <3389>

Chain: dstnat

Src. Address:

Dst. Address:

Protocol: □ 6 (tcp)

Src. Port:

Dst. Port: □ 3389

Any. Port:

In. Interface:

Out. Interface:

NAT Rule <60.70.80.2:3389>

Action: dst-nat

□ Log

Log Prefix:

To Addresses: 10.0.25.2

To Ports: 3389

NAT Rule <3389>

Address Type: local

□ Invert

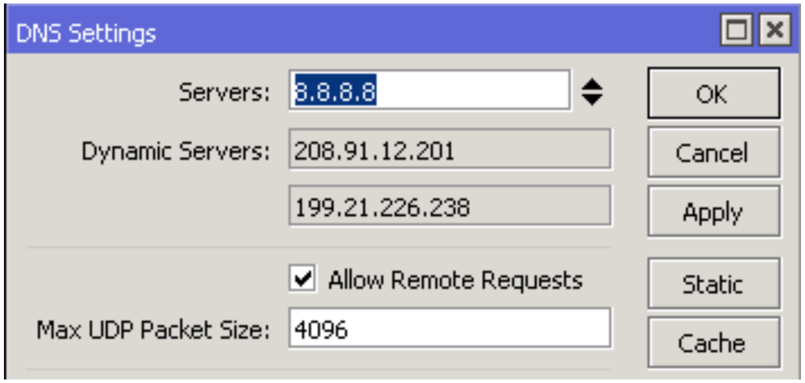
With a dynamic IP, it is also simple!

Return

How to Not be a Participant In a DNS Attack

DNS Allow Remote Requests

PROBLEM: Open DNS servers can be used to launch Distributed Denial of Service (DDoS) attacks



Servers: 8.8.8.8

Dynamic Servers: 208.91.12.201

199.21.226.238

☑ Allow Remote Requests

Max UDP Packet Size: 4096

DNS Allow Remote Requests

SOLUTION: Create a firewall rule to block everything on the WAN port or specifically to block port 53 UDP and TCP.

```
/ip firewall filter

add chain=input protocol=tcp dst-port=53 in-interface=ether1-gateway
action=drop

add chain=input protocol=udp dst-port=53 in-interface=ether1-gateway
action=drop
```

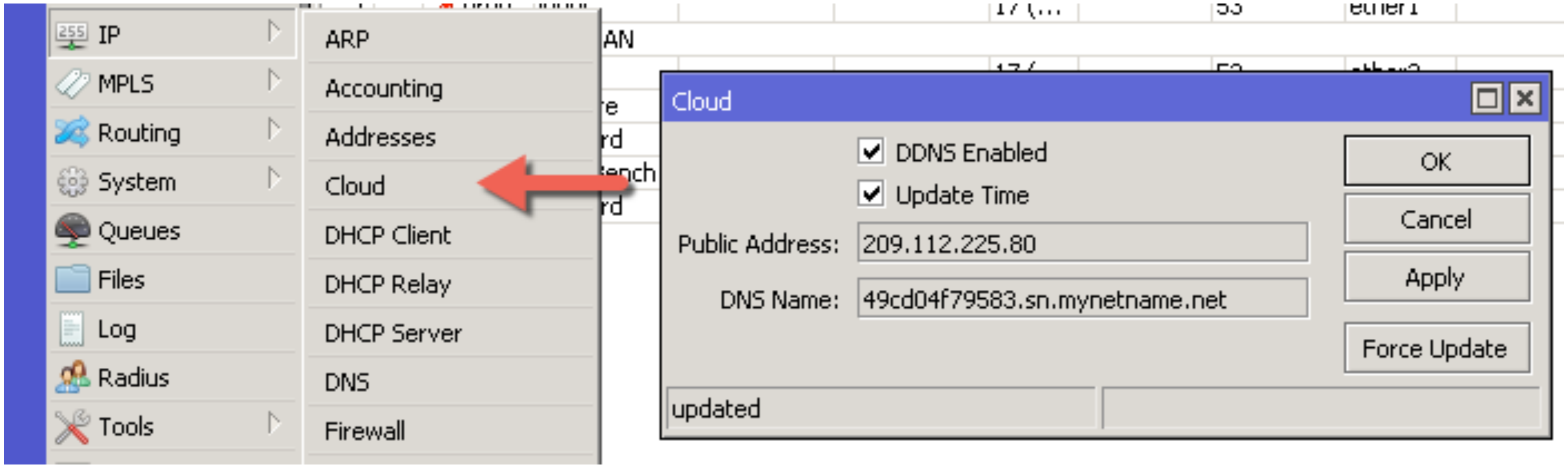
Return

Where's That Firewall?

IP Cloud Feature

- Starting with RouterOS v6.14 MikroTik offers a Dynamic DNS name service for RouterBOARD devices.
- This means that your device can automatically get a working domain name, this is useful if your IP address changes.
- Prior to this feature, you had to use problematic DynDNS Scripts

IP Cloud Feature



Cloud

☑ DDNS Enabled

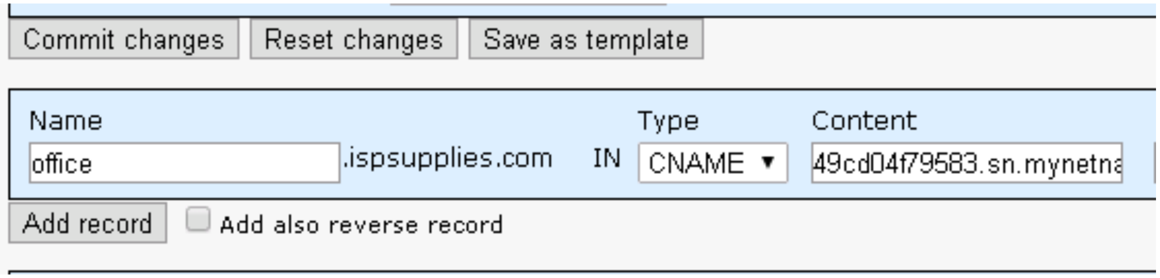
☑ Update Time

Public Address: 209.112.225.80

DNS Name: 49cd04f79583.sn.mynetname.net

updated

Create a CNAME in your DNS server for the MyNetName.net host name



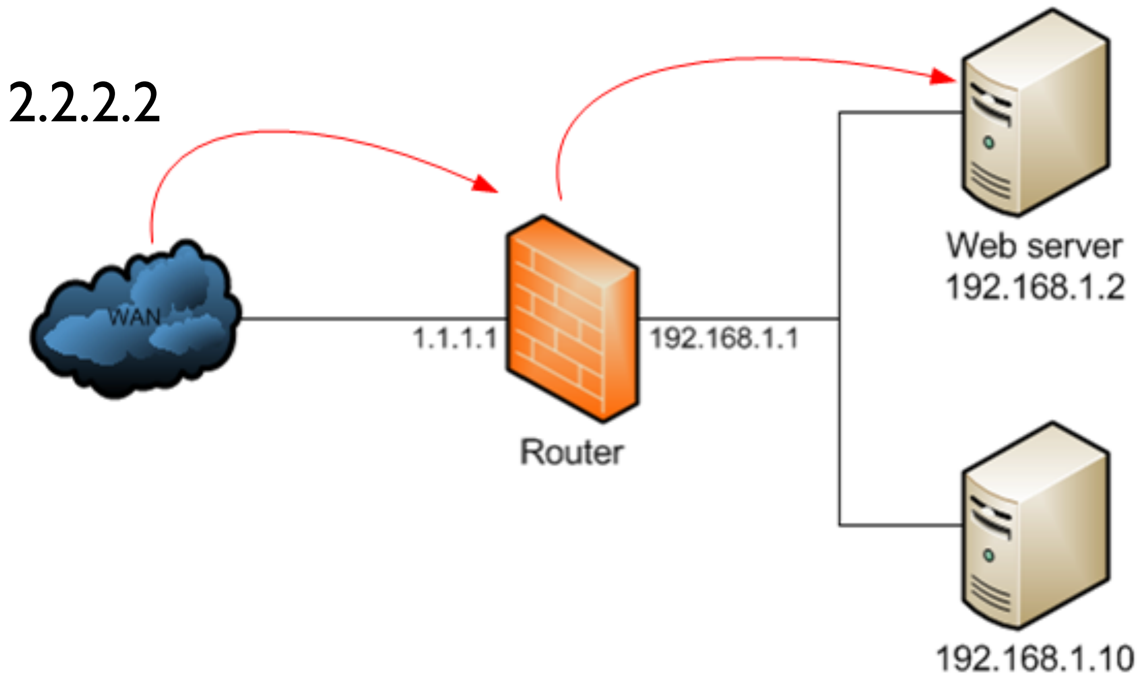
Name		Type	Content
office .ispsupplies.com	IN	CNAME ▾	49cd04f79583.sn.mynetna

☐ Add also reverse record

Return

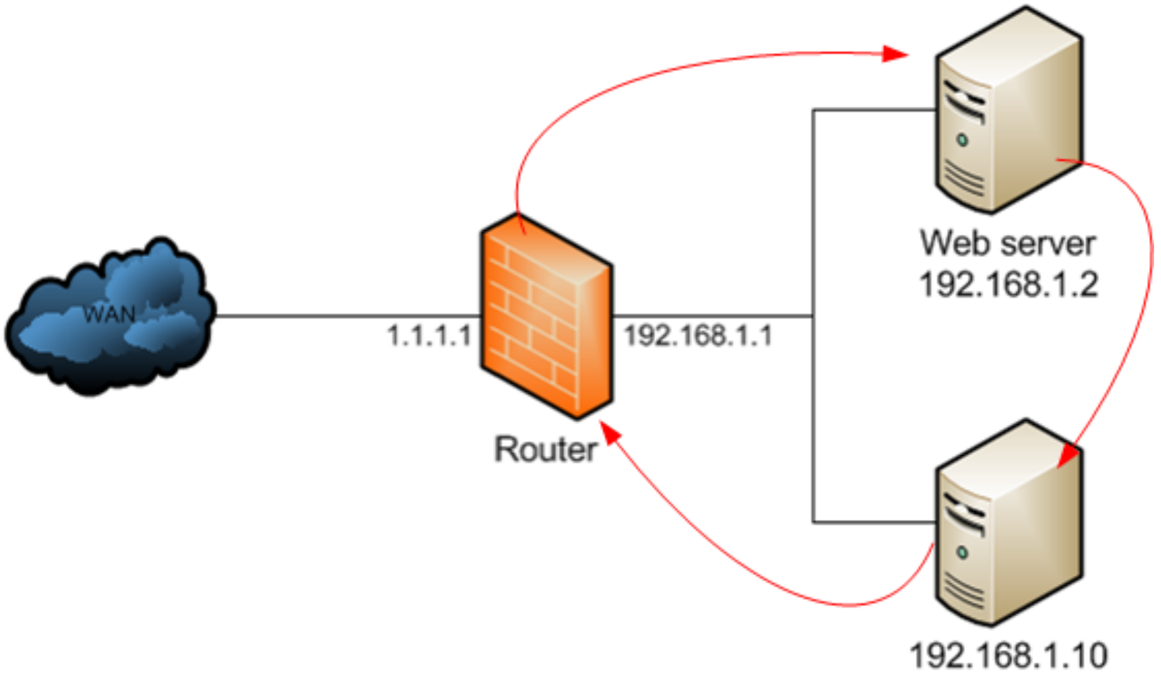
Hairpin NAT

Hairpin NAT



	Source IP	Destination IP
Step 1	2.2.2.2	1.1.1.1
Step 2	2.2.2.2	192.168.1.2
Step 3	192.168.1.2	2.2.2.2
Step 4	1.1.1.1	2.2.2.2

Hairpin NAT



Step 1	Source IP 192.168.1.10	Destination IP 1.1.1.1
Step 2	Source IP 192.168.1.10	Destination IP 192.168.1.2
Step 3	Source IP 192.168.1.2	Destination IP 192.168.1.10

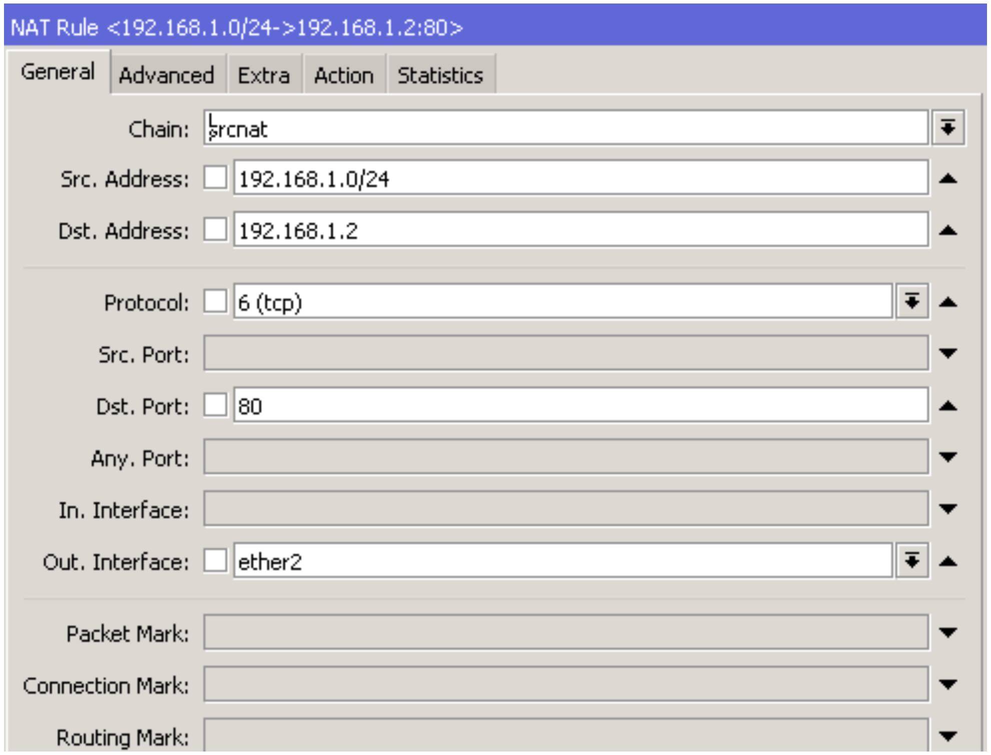
Hairpin NAT

- Server replies but source IP address of the request is on the same subnet as the web server.

- Server does not send the reply back to the router, but sends it back directly to 192.168.1.10 with a source IP address in the reply of 192.168.1.2.

- The client receives the reply packet, but it discards it because it expects a packet back from 1.1.1.1, and not from 192.168.1.2. As far as the client is concerned the packet is invalid and not related to any connection the client previously attempted to establish.

Hairpin NAT



NAT Rule <192.168.1.0/24->192.168.1.2:80>

Chain: srcnat

Src. Address: □ 192.168.1.0/24

Dst. Address: □ 192.168.1.2

Protocol: □ 6 (tcp)

Src. Port:

Dst. Port: □ 80

Any. Port:

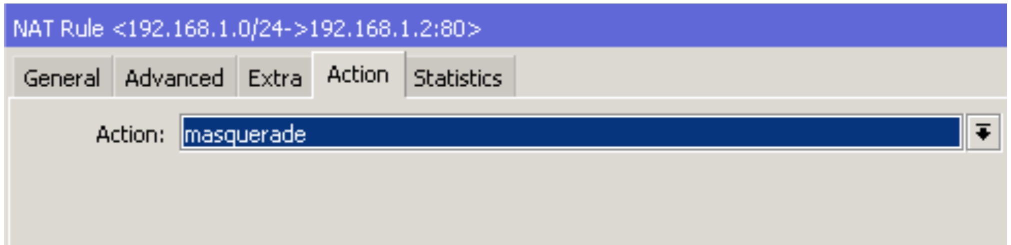
In. Interface:

Out. Interface: □ ether2

Packet Mark:

Connection Mark:

Routing Mark:



NAT Rule <192.168.1.0/24->192.168.1.2:80>

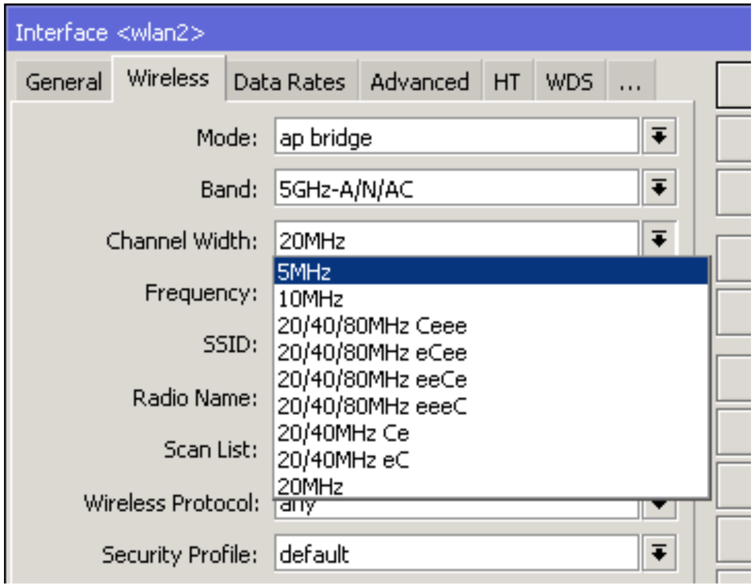
Action: masquerade

```
/ip firewall nat
add chain=srcnat src-address=192.168.1.0/24 dst-address=192.168.1.2\
protocol=tcp dst-port=80 out-interface=ether2 action=masquerade
```

Return

802.11ac Center/ Extension Channels

802.11ac Control Channel Nomenclature



Interface <wlan2>

General | Wireless | Data Rates | Advanced | HT | WDS | ...

Mode: ap bridge

Band: 5GHz-A/N/AC

Channel Width: 20MHz

- 5MHz
- 10MHz
- 20/40/80MHz Ceee
- 20/40/80MHz eCee
- 20/40/80MHz eeCe
- 20/40/80MHz eeeC
- 20/40MHz Ce
- 20/40MHz eC
- 20MHz

Frequency:

SSID:

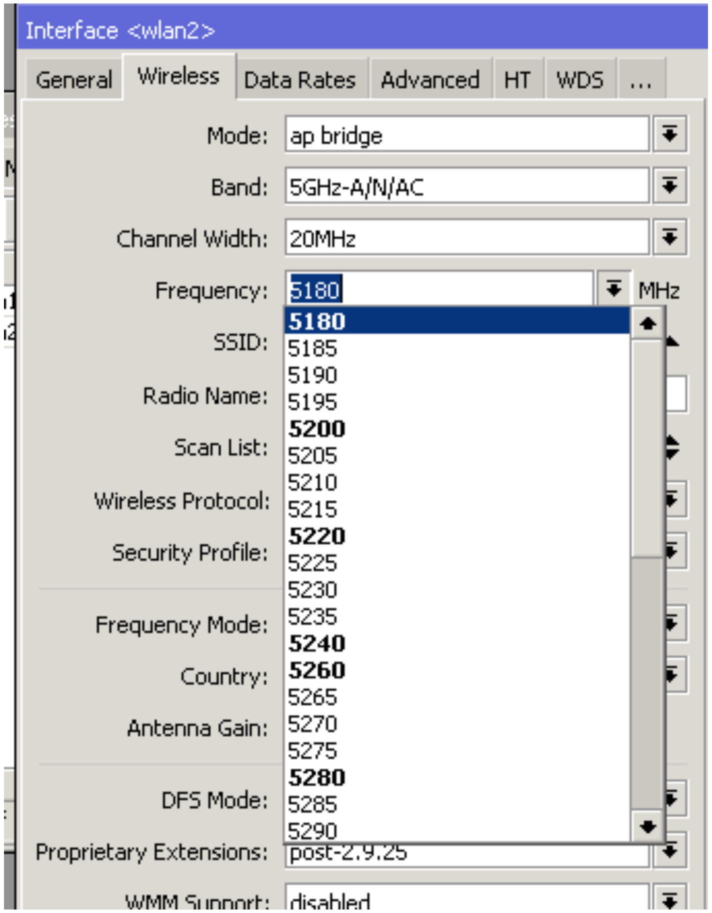
Radio Name:

Scan List:

Wireless Protocol: any

Security Profile: default

Ceee…what?



Interface <wlan2>

General | Wireless | Data Rates | Advanced | HT | WDS | ...

Mode: ap bridge

Band: 5GHz-A/N/AC

Channel Width: 20MHz

Frequency: 5180 MHz

- **5180**
- 5185
- 5190
- 5195
- **5200**
- 5205
- 5210
- 5215
- **5220**
- 5225
- 5230
- 5235
- **5240**
- **5260**
- 5265
- 5270
- 5275
- **5280**
- 5285
- 5290

SSID:

Radio Name:

Scan List:

Wireless Protocol:

Security Profile:

Frequency Mode:

Country:

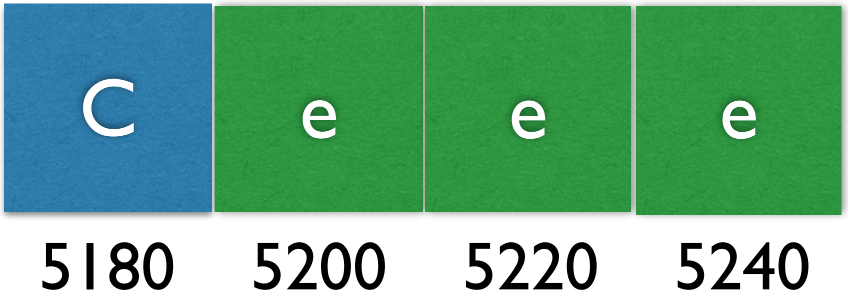
Antenna Gain:

DFS Mode:

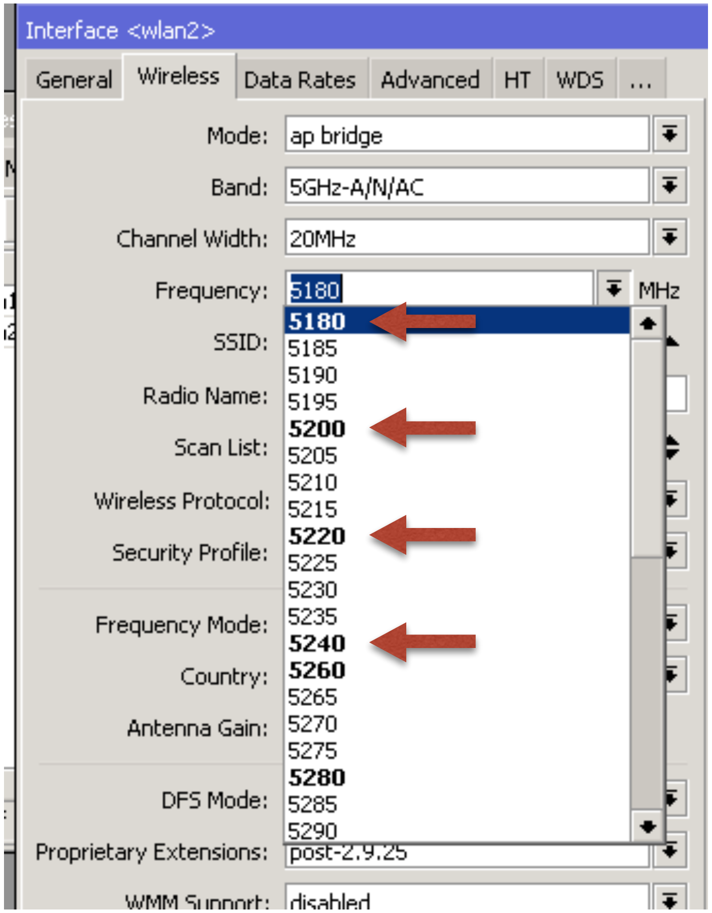
Proprietary Extensions: post-2.9.25

WMM Support: disabled

802.11ac Control Channel Nomenclature



Remember not to put extension below/above Control if no valid frequencies exist there!



Mode: ap bridge

Band: 5GHz-A/N/AC

Channel Width: 20MHz

Frequency: 5180 MHz

SSID:

Radio Name:

Scan List:

Wireless Protocol:

Security Profile:

Frequency Mode:

Country:

Antenna Gain:

DFS Mode:

Proprietary Extensions: post-2.9.25

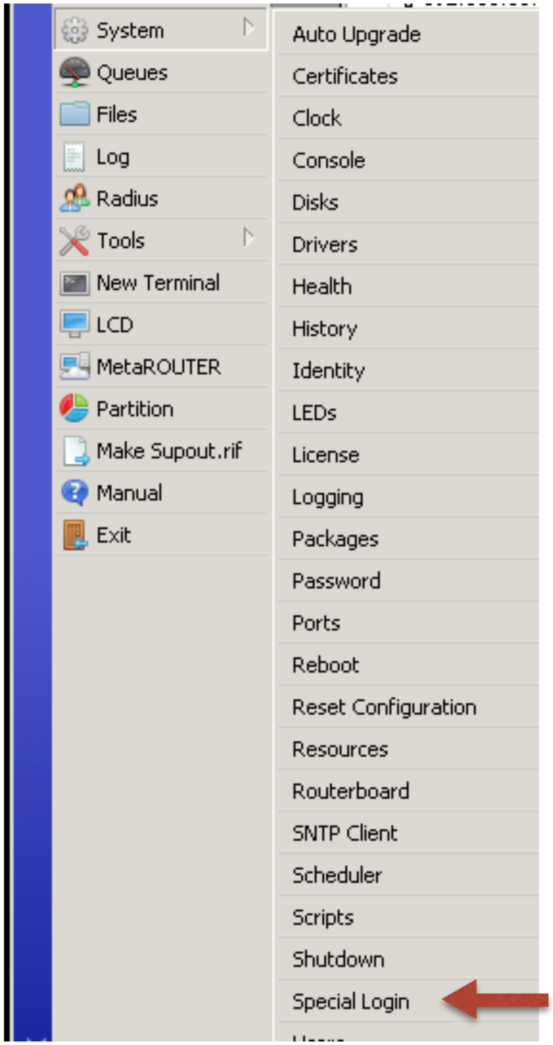
WMM Support: disabled

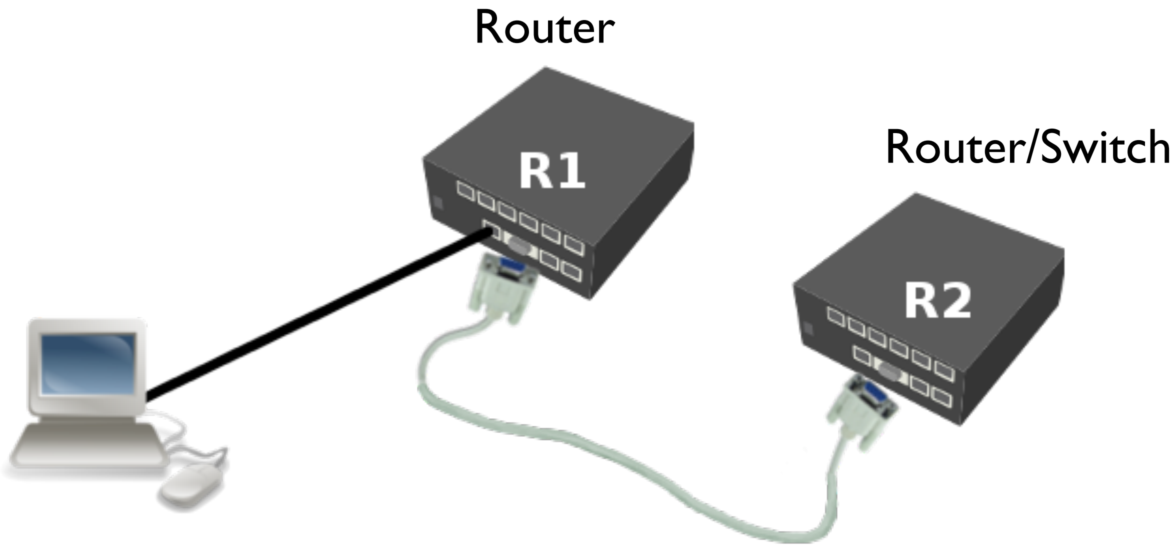
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5260
5265
5270
5275
5280
5285
5290

Return

Special Login

Special Login



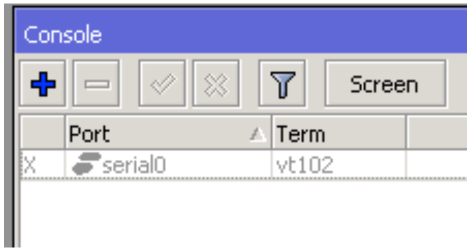


SSH/Telnet to an IP on a router, and be redirected to a serial port based on user name.

Special Login

Router:

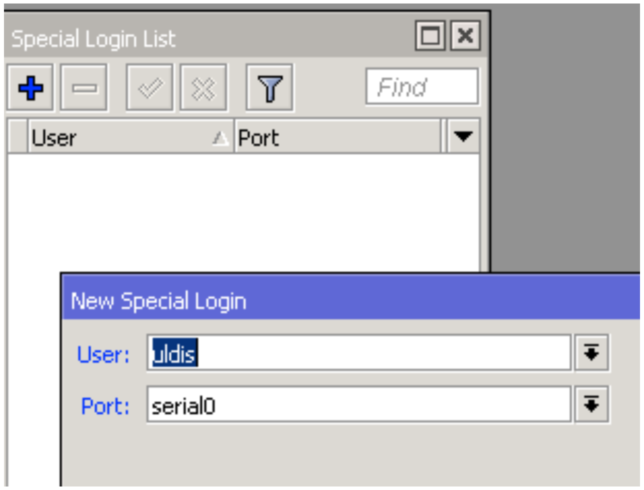
1. Disable serial console



Console

	Port	Term
X	serial0	vt102

2. Add new user with port in Special login



Special Login List

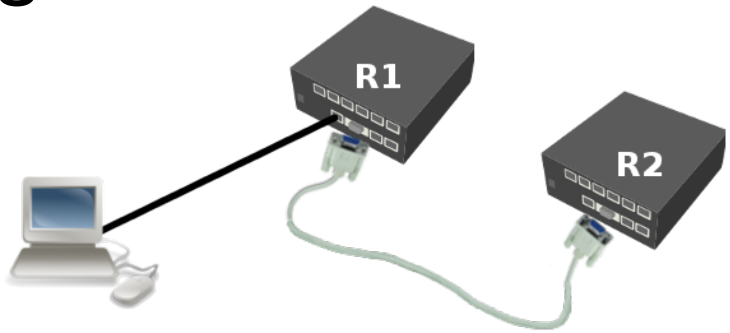
User	Port

New Special Login

User: uldis

Port: serial0

```
ssh serial@R1
```



is redirected to serial port of R2

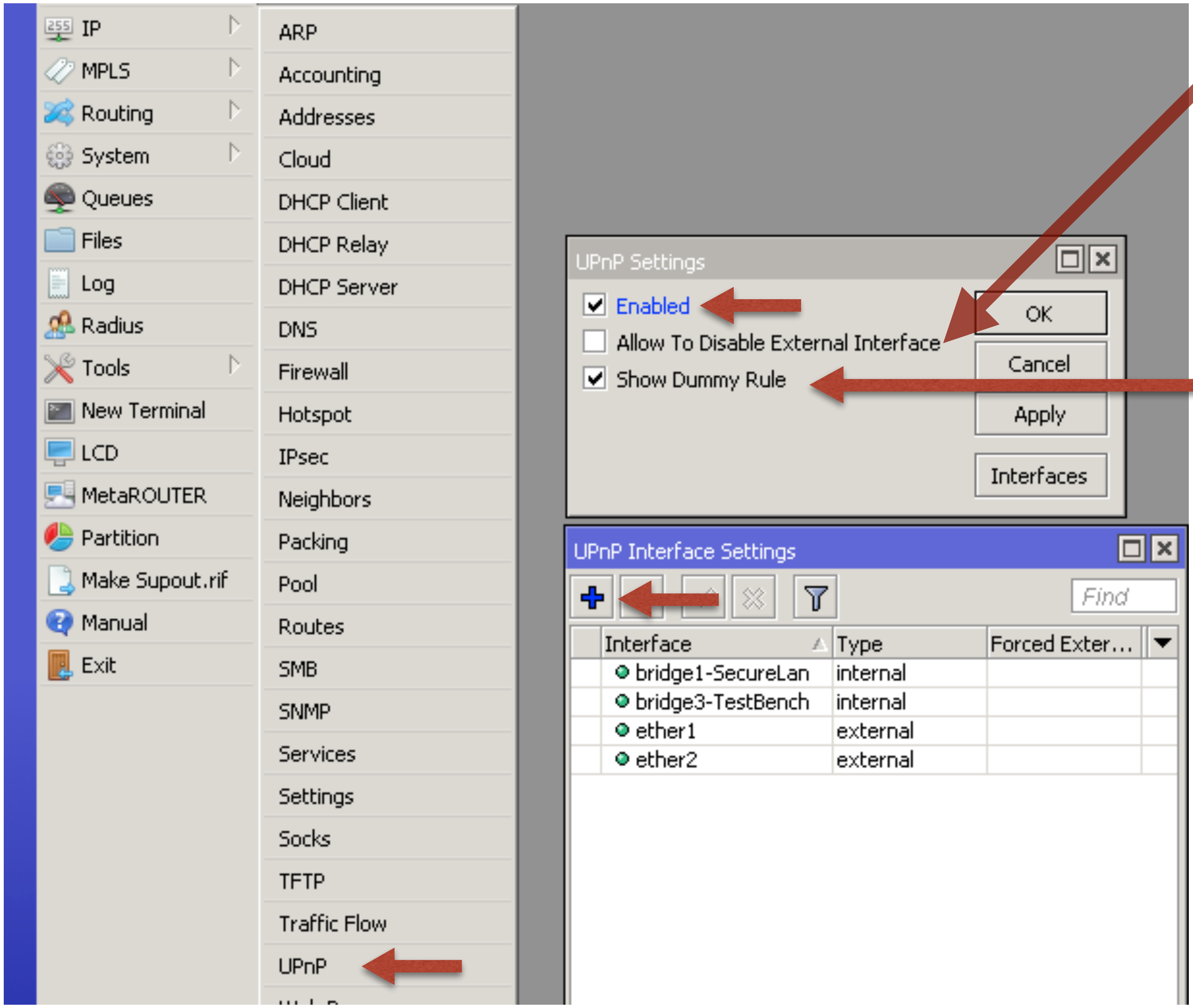
Return

UPnP

UPnP

Universal Plug and Play architecture for transparent peer-to-peer network connectivity of personal computers and network-enabled intelligent devices or appliances, typically game consoles.

UPnP



UPnP Settings

☑ Enabled

□ Allow To Disable External Interface

☑ Show Dummy Rule

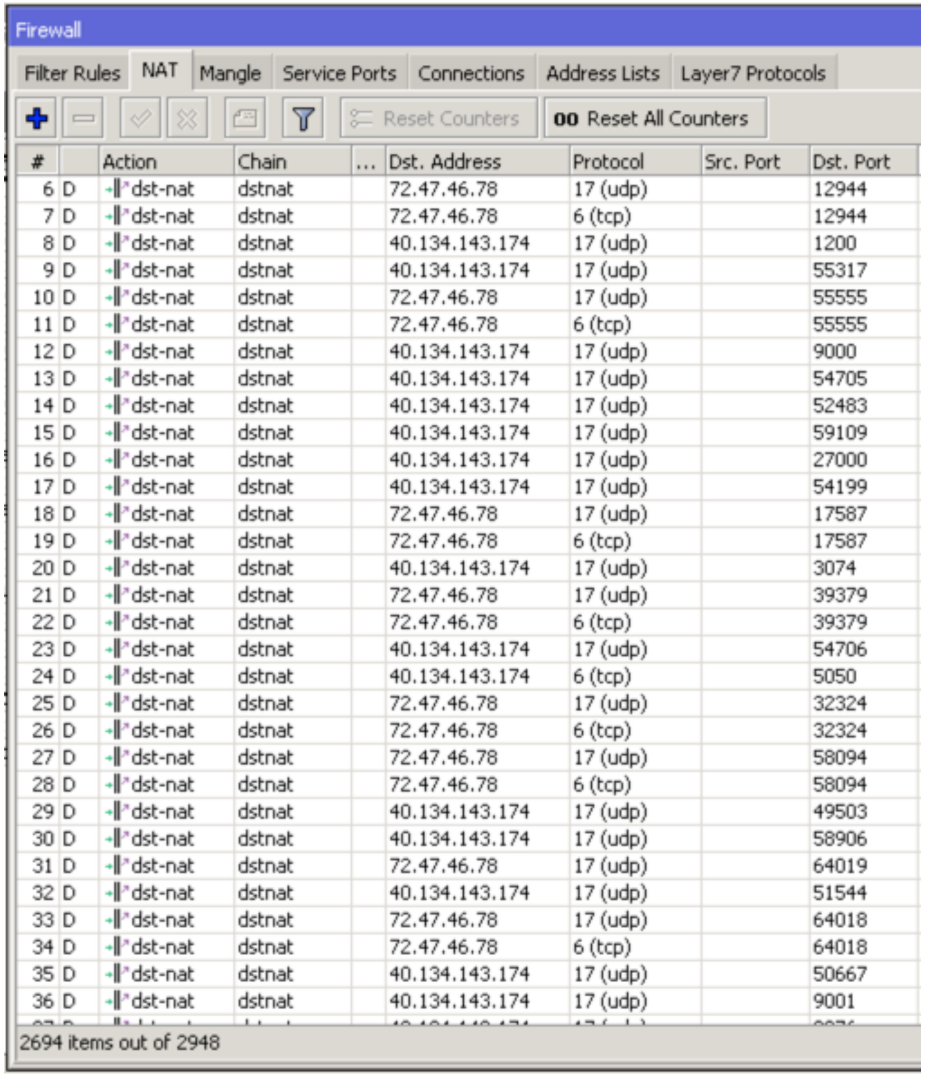
UPnP Interface Settings

Interface	Type	Forced Exter...
bridge1-SecureLan	internal	
bridge3-TestBench	internal	
ether1	external	
ether2	external	

Required by standard, but don’t enable!

Enables a workaround for some broken implementations

UPnP



#		Action	Chain	...	Dst. Address	Protocol	Src. Port	Dst. Port
6	D	dst-nat	dstnat		72.47.46.78	17 (udp)		12944
7	D	dst-nat	dstnat		72.47.46.78	6 (tcp)		12944
8	D	dst-nat	dstnat		40.134.143.174	17 (udp)		1200
9	D	dst-nat	dstnat		40.134.143.174	17 (udp)		55317
10	D	dst-nat	dstnat		72.47.46.78	17 (udp)		55555
11	D	dst-nat	dstnat		72.47.46.78	6 (tcp)		55555
12	D	dst-nat	dstnat		40.134.143.174	17 (udp)		9000
13	D	dst-nat	dstnat		40.134.143.174	17 (udp)		54705
14	D	dst-nat	dstnat		40.134.143.174	17 (udp)		52483
15	D	dst-nat	dstnat		40.134.143.174	17 (udp)		59109
16	D	dst-nat	dstnat		40.134.143.174	17 (udp)		27000
17	D	dst-nat	dstnat		40.134.143.174	17 (udp)		54199
18	D	dst-nat	dstnat		72.47.46.78	17 (udp)		17587
19	D	dst-nat	dstnat		72.47.46.78	6 (tcp)		17587
20	D	dst-nat	dstnat		40.134.143.174	17 (udp)		3074
21	D	dst-nat	dstnat		72.47.46.78	17 (udp)		39379
22	D	dst-nat	dstnat		72.47.46.78	6 (tcp)		39379
23	D	dst-nat	dstnat		40.134.143.174	17 (udp)		54706
24	D	dst-nat	dstnat		40.134.143.174	6 (tcp)		5050
25	D	dst-nat	dstnat		72.47.46.78	17 (udp)		32324
26	D	dst-nat	dstnat		72.47.46.78	6 (tcp)		32324
27	D	dst-nat	dstnat		72.47.46.78	17 (udp)		58094
28	D	dst-nat	dstnat		72.47.46.78	6 (tcp)		58094
29	D	dst-nat	dstnat		40.134.143.174	17 (udp)		49503
30	D	dst-nat	dstnat		40.134.143.174	17 (udp)		58906
31	D	dst-nat	dstnat		72.47.46.78	17 (udp)		64019
32	D	dst-nat	dstnat		40.134.143.174	17 (udp)		51544
33	D	dst-nat	dstnat		72.47.46.78	17 (udp)		64018
34	D	dst-nat	dstnat		72.47.46.78	6 (tcp)		64018
35	D	dst-nat	dstnat		40.134.143.174	17 (udp)		50667
36	D	dst-nat	dstnat		40.134.143.174	17 (udp)		9001

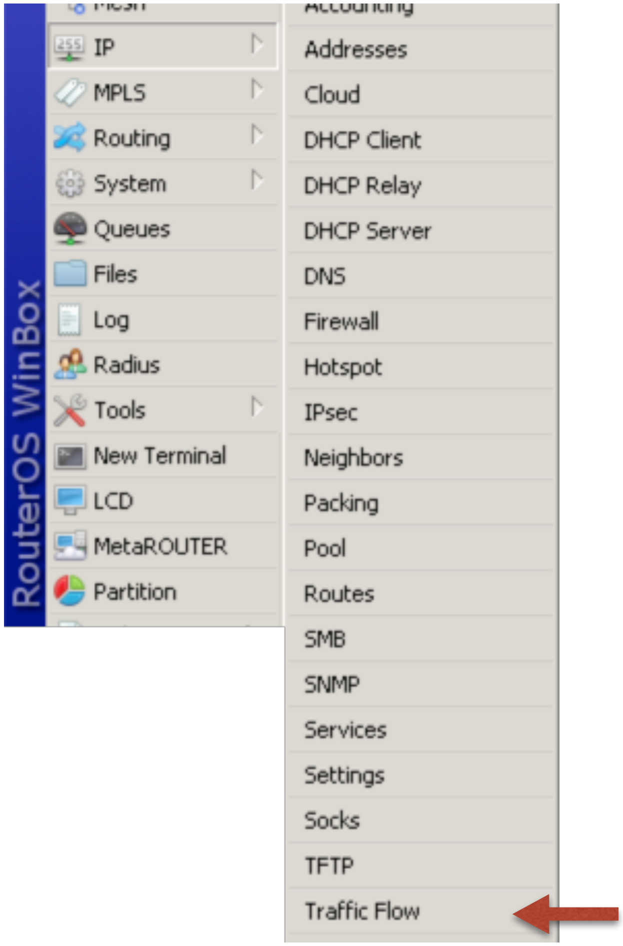
2694 items out of 2948

2300 active hosts producing 2694 dynamic NAT rules

Return

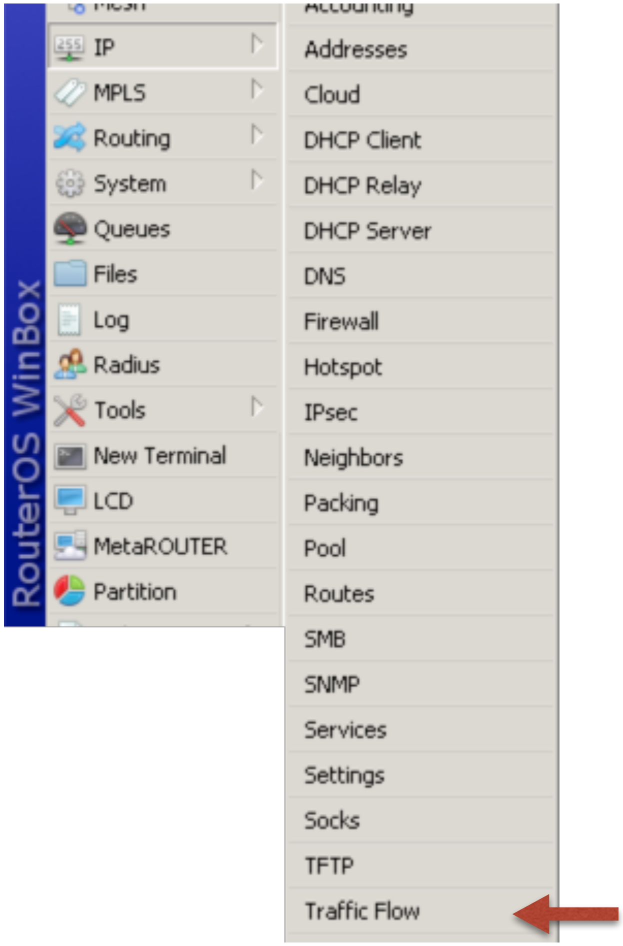
IP Flows

IP Traffic Flow



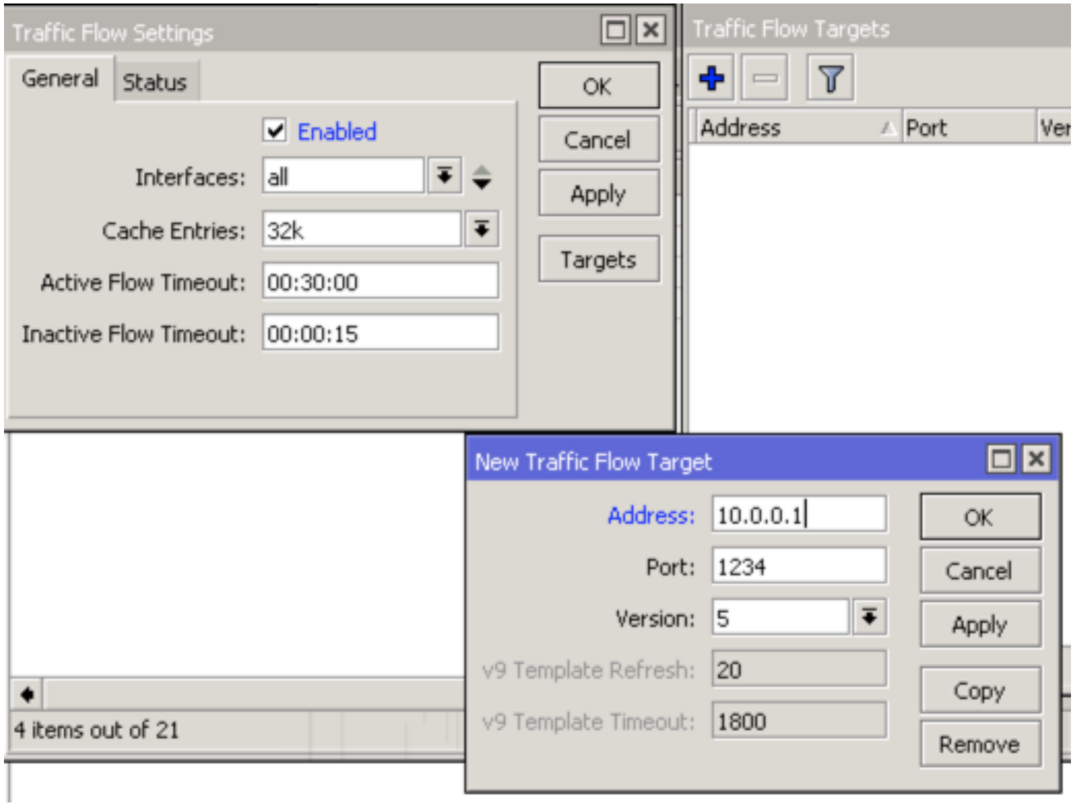
- MikroTik Traffic-Flow is a system that provides statistic information about packets which pass through the router.
- Besides network monitoring and accounting, system administrators can identify various problems that may occur in the network.

IP Traffic Flow



- With help of Traffic-Flow, it is possible to analyze and optimize the overall network performance.
- As Traffic-Flow is compatible with Cisco NetFlow, it can be used with various utilities which are designed for Cisco's NetFlow.

IP Traffic Flow



Traffic Flow Settings

General | Status

☑ Enabled

Interfaces: all

Cache Entries: 32k

Active Flow Timeout: 00:30:00

Inactive Flow Timeout: 00:00:15

4 items out of 21

New Traffic Flow Target

Address: 10.0.0.1

Port: 1234

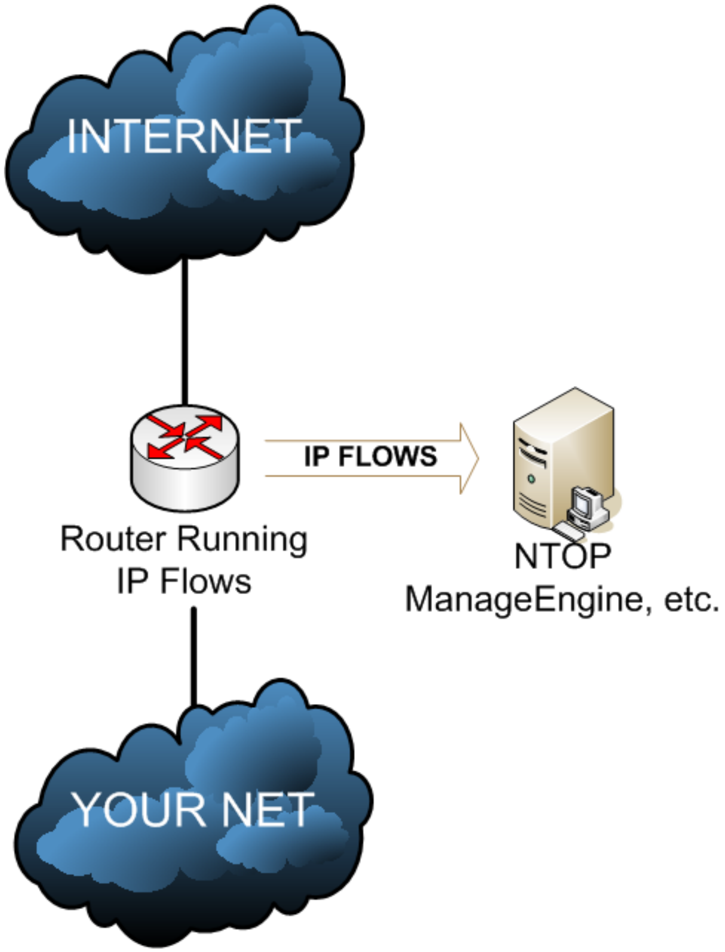
Version: 5

v9 Template Refresh: 20

v9 Template Timeout: 1800

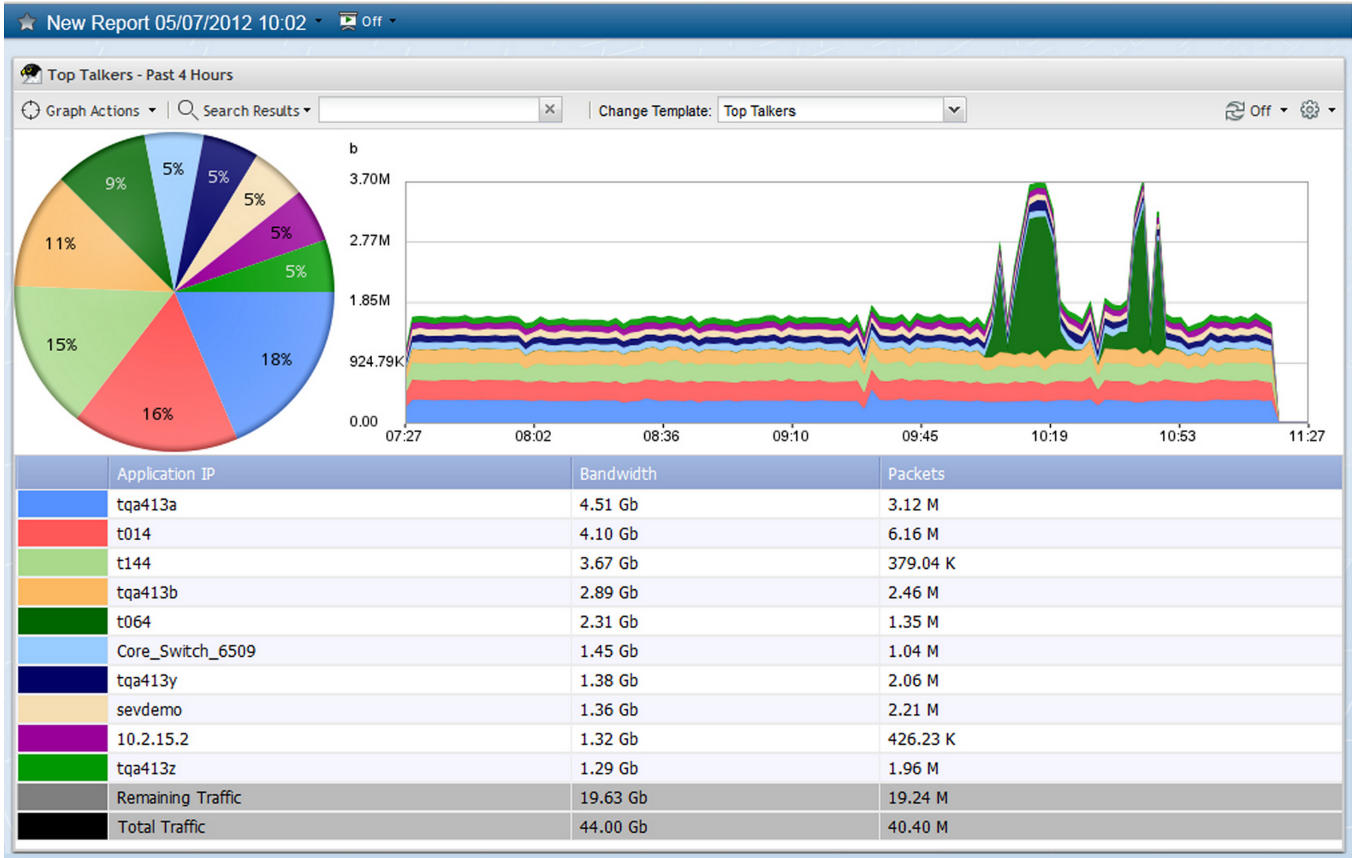
Enable flows and create a target. The target is a NetFlows server such as ManageEngine, or NTOP.

IP Traffic Flow



IP Traffic Flow

This data can then be analyzed and charted to determine the types of traffic flowing through your router, source IP's destination IP's, top talkers , etc. statistically over time.



	Application IP	Bandwidth	Packets
🟦	tqa413a	4.51 Gb	3.12 M
🟥	t014	4.10 Gb	6.16 M
🟩	t144	3.67 Gb	379.04 K
🟧	tqa413b	2.89 Gb	2.46 M
🟩	t064	2.31 Gb	1.35 M
🟦	Core_Switch_6509	1.45 Gb	1.04 M
🟦	tqa413y	1.38 Gb	2.06 M
🟨	sevdemo	1.36 Gb	2.21 M
🟪	10.2.15.2	1.32 Gb	426.23 K
🟩	tqa413z	1.29 Gb	1.96 M
⬜	Remaining Traffic	19.63 Gb	19.24 M
⬛	Total Traffic	44.00 Gb	40.40 M

Return

MikroTikConfig.com

Updated!

2013 St. Louis MUM

- Java based, limited functionality

2014 Pittsburgh MUM

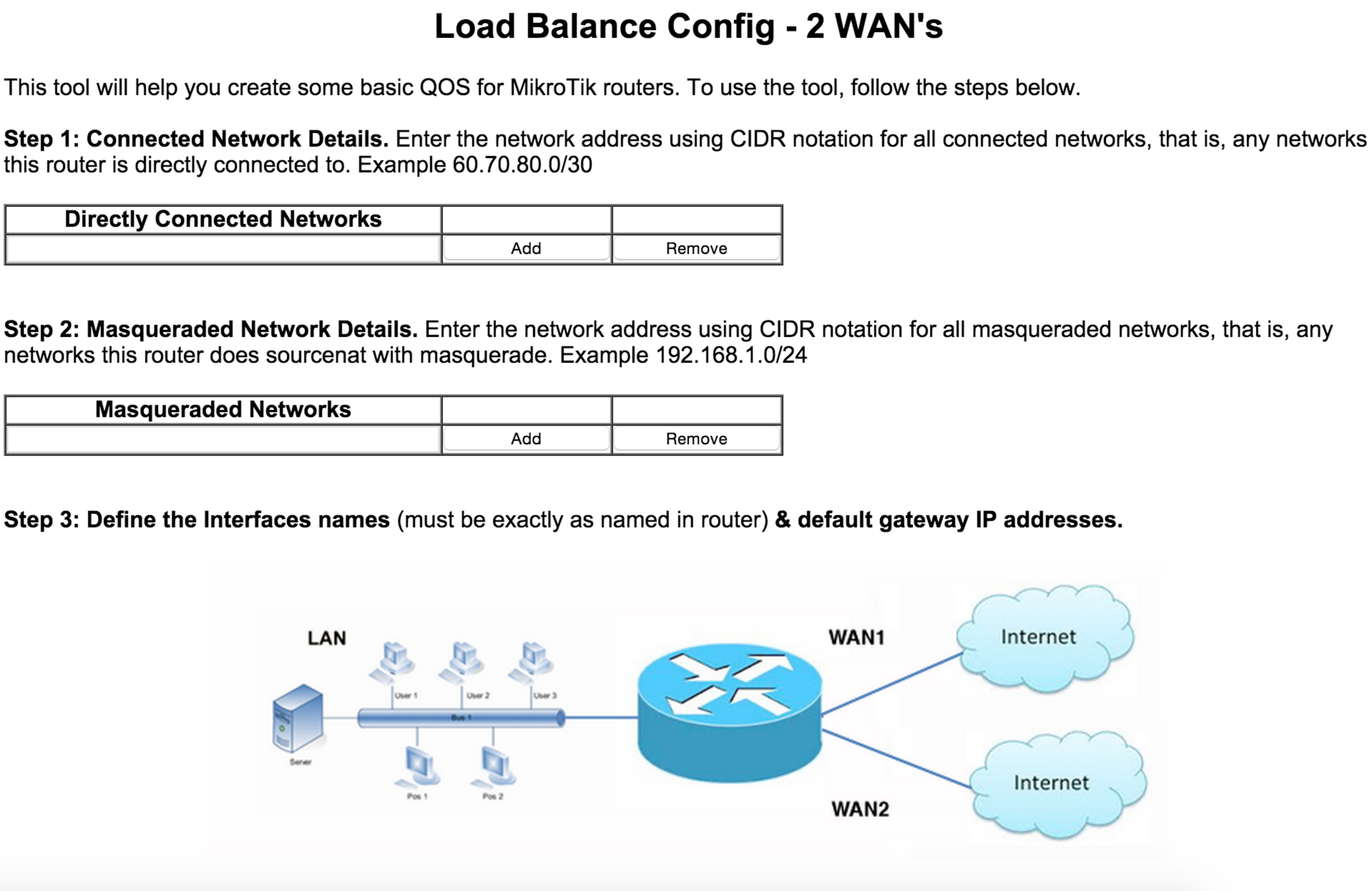
- Web based, added firewall, QOS and country based address lists

2015

- Add PCC based load balancing for 2 or 3 WAN connections

MikroTikConfig.com

Fill in the blanks, download a text file, import.



Load Balance Config - 2 WAN's

This tool will help you create some basic QOS for MikroTik routers. To use the tool, follow the steps below.

Step 1: Connected Network Details. Enter the network address using CIDR notation for all connected networks, that is, any networks this router is directly connected to. Example 60.70.80.0/30

Directly Connected Networks		
	Add	Remove

Step 2: Masqueraded Network Details. Enter the network address using CIDR notation for all masqueraded networks, that is, any networks this router does sourcenat with masquerade. Example 192.168.1.0/24

Masqueraded Networks		
	Add	Remove

Step 3: Define the Interfaces names (must be exactly as named in router) **& default gateway IP addresses.**

Demo

Questions?

Thank You For Playing!

- Training: MyWISPTraining.com & LearnMikroTik.com
- Store: ISPSupplies.com
- Blog: SteveDischer.com
- "RouterOS by Example" available from distributors, Amazon.com, Kindle, iTunes
- Configurator: MikroTikConfig.com