YouTube

Embracing Netflix

Managing Streaming Content on Your Wireless Network

NETFLIX

hulu

About Me

- Steve Discher, from College Station, Texas, USA
- Class of '87 Texas A&M University
- Using MikroTik since early 2004 when I started my first WISP
- Author of the book "RouterOS by Example"
- MikroTik Certified Trainer and teach RouterOS classes, MyWISPTraining.com
- Operate a wireless distribution company, ISPSupplies.com

Who Needs This?

- WISP's
- Entertainment or resort venues with WiFi
- Any other fixed wireless operator

Streaming

Assumption 1

Your users are going to stream movies. Netflix for example currently has 33 million subscribers!

State of the Network

plug into
free Wi-Fi*
during your stay.

*Free actually means $9.99 per hour or an incredibly annoying Wi-Fi experience.

Sorry, it is what it is.

No Signal
Horrible Wi-Fi HOTEL

Streaming

Assumption 2

You have been telling your customers "Streaming content is not supported on our network."

Relax, you won't have to say that too many more times.

OFFICIAL DISCLAIMER

1. Steve Discher is not an attorney nor does he play one on TV.

2. For all matters of law, please consult an attorney and do not rely on any advice I give you here today.

3. Question everything I tell you if it sounds like legal advice!

OFFICIAL DISCLAIMER

FCC 2010 Ruling on “Net Neutrality”

Open Internet Rules

The FCC has adopted three basic open Internet rules:

- Transparency. Broadband providers must disclose information regarding their network management practices, performance, and the commercial terms of their broadband services.
- No blocking. Fixed broadband providers (such as DSL, cable modem, or fixed wireless providers) may not block lawful content, applications, services, or non-harmful devices. Mobile broadband providers may not block lawful websites, or applications that compete with their voice or video telephony services.
- No unreasonable discrimination. Fixed broadband providers may not unreasonably discriminate in transmitting lawful network traffic over a consumer’s broadband Internet access service. Unreasonable discrimination of network traffic could take the form of particular services or websites appearing slower or degraded in quality.

Navigating Through the Gray Area

- Entertainment network operators, hotels, RV Parks, etc. can likely shape traffic however they wish.
- Fixed wireless operators, WISPS, etc. should use caution.

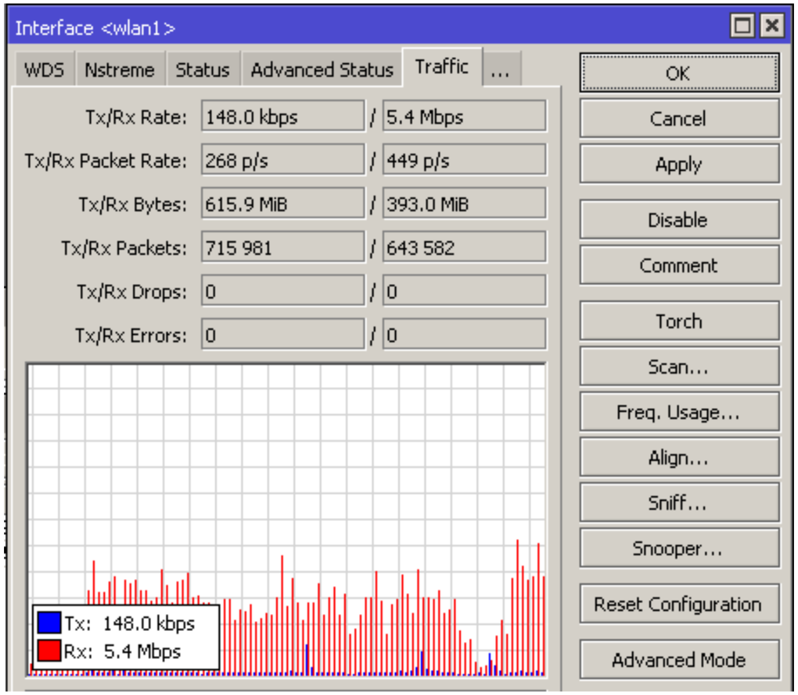
Navigating Through the Gray Area

- My presentation will be based on the assumption that you are trying to help your customer.
- Purpose of traffic shaping is to enhance their streaming experience.
- Although these methods are applicable to the entire network, we will assume you will apply rate limits applicable for the level of service the customer is buying.
  - For Example:

    If a customer buys the 3 Mb/s download package, they should be able to stream Netflix at 3Mb/s, not be limited to 512k for Netflix and 3 Mb/s for everything else.

How Much Bandwidth?

- Netflix SuperHD requires a minimum of 5Mb/s download speed, not able to test in my area because my ISP not a member of the Netflix open connect network
- Non-HD, requires an average of 3-5Mb/s download speed
- Decent quality all the way down to 512k download, Netflix, Hulu and YouTube, likely others



Interface <wlan1>

Tx/Rx Rate: 148.0 kbps / 5.4 Mbps
Tx/Rx Packet Rate: 268 p/s / 449 p/s
Tx/Rx Bytes: 615.9 MiB / 393.0 MiB
Tx/Rx Packets: 715 981 / 643 582
Tx/Rx Drops: 0 / 0
Tx/Rx Errors: 0 / 0

🟦 Tx: 148.0 kbps
🟥 Rx: 5.4 Mbps

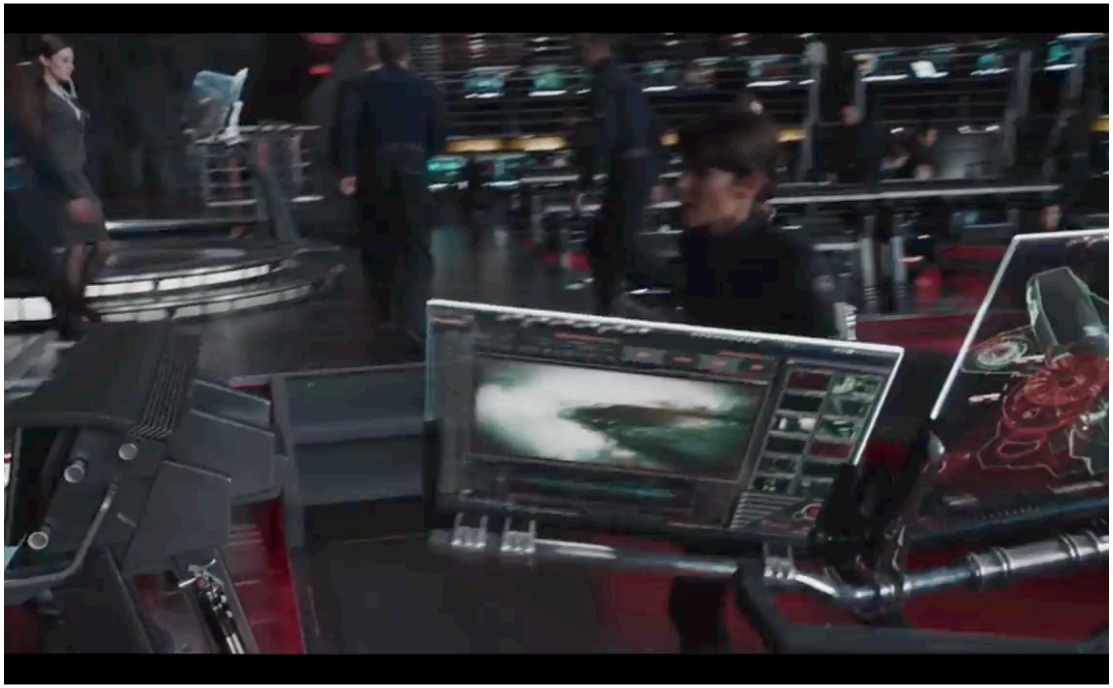
Traffic through WAN interface, no shaping, watching an SD movie

Side by Side Comparison

5Mb/s

512k

512k Customer Rate Limit With One Other User Browsing Web



What is the Solution?

Ensure that streaming traffic always has access to sufficient bandwidth even if that means starving bandwidth from all other types of traffic.

How is that Done?

1. Identify the most popular sources of streaming traffic and mark those packets.

2. Create queues, sort traffic into those queues and ensure that the streaming queue is allowed to fill their queues first.

Background

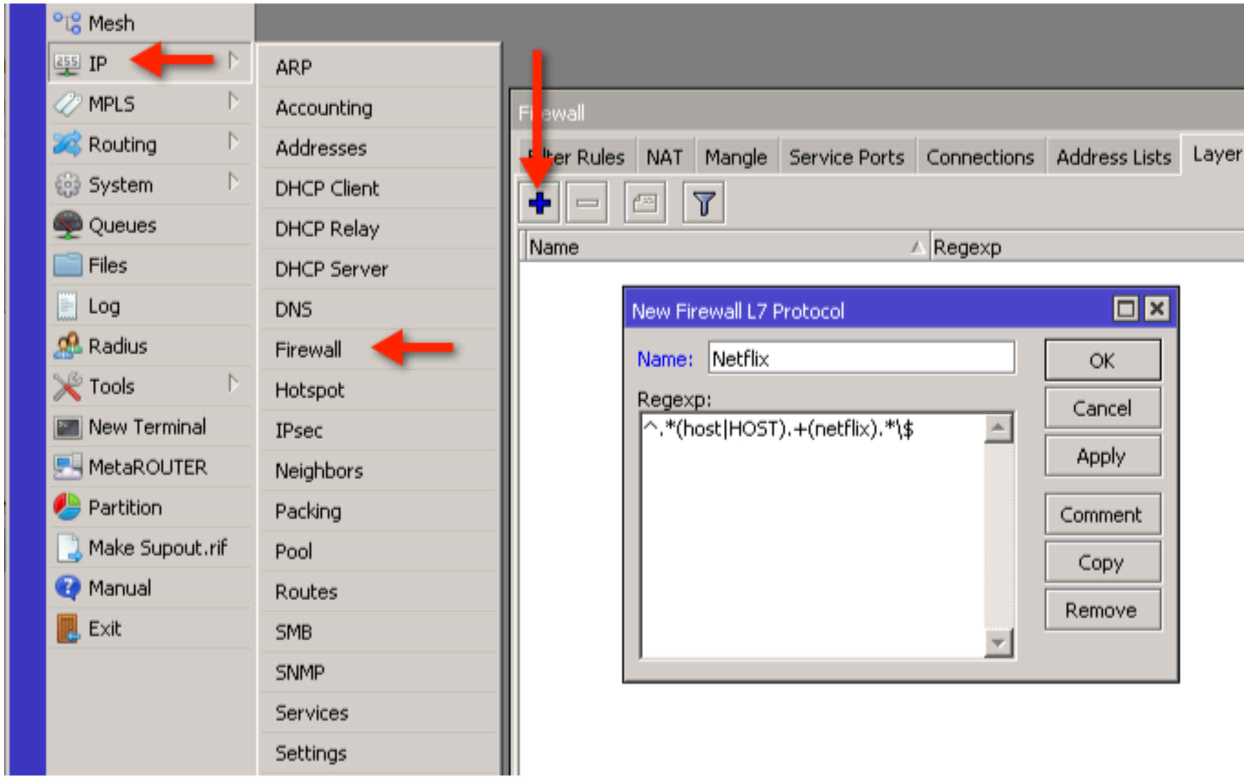
We will use two main facilities of RouterOS, mangling using **Mangling** and queueing using **Queues** in the Queue tree and custom queue types.

Can I do the same thing with simple queues? Absolutely but I urge you to be a man and use the queue tree.

And, you will make Janis (technical not sales) smile!

Quick Start For The Impatient

Mangle Process Step by Step



Name: Netflix

Regexp:
```
^.*(host|HOST).+(netflix).*\$
```

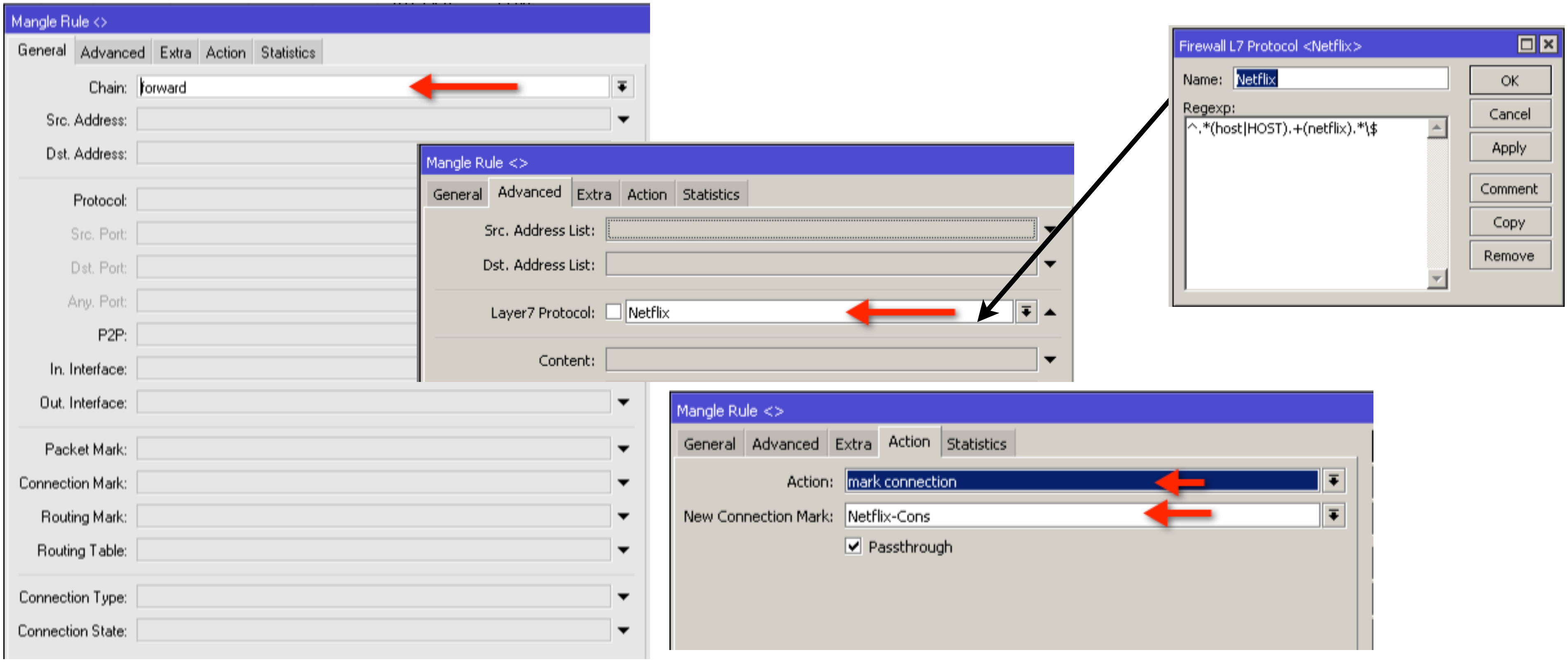
```
^.*(host|HOST).+(netflix).*\$
```

- We first need a Regex matcher

- The Regex is the heart of the config so it has to be right!

- This example is for Netflix

Mangle Process Step by Step



Mangle Rule <>

Chain: forward

Mangle Rule <>

Layer7 Protocol: □ Netflix

Firewall L7 Protocol <Netflix>

Name: Netflix

Regexp:

```
^.*(host|HOST).+(netflix).*\$
```

Mangle Rule <>

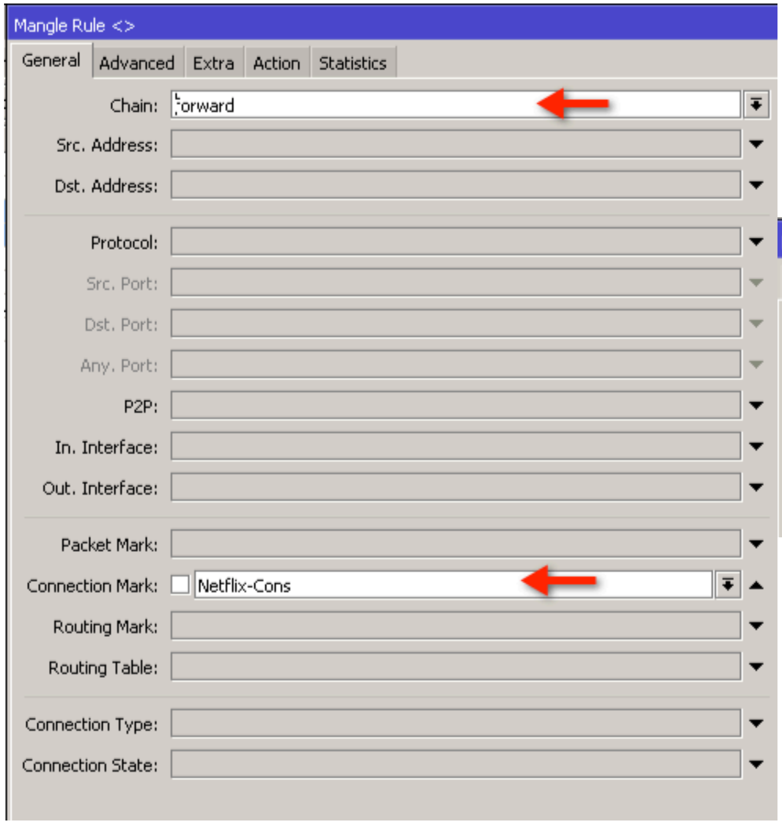
Action: mark connection

New Connection Mark: Netflix-Cons

☑ Passthrough

- Next we create a mangle rule in the forward chain, matching all packets and use the L7 matcher

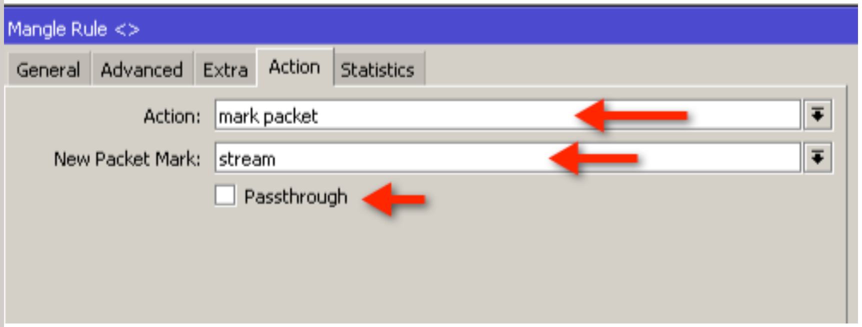
Mangle Process Step by Step



Mangle Rule <>

Chain: forward

Connection Mark: □ Netflix-Cons



Mangle Rule <>

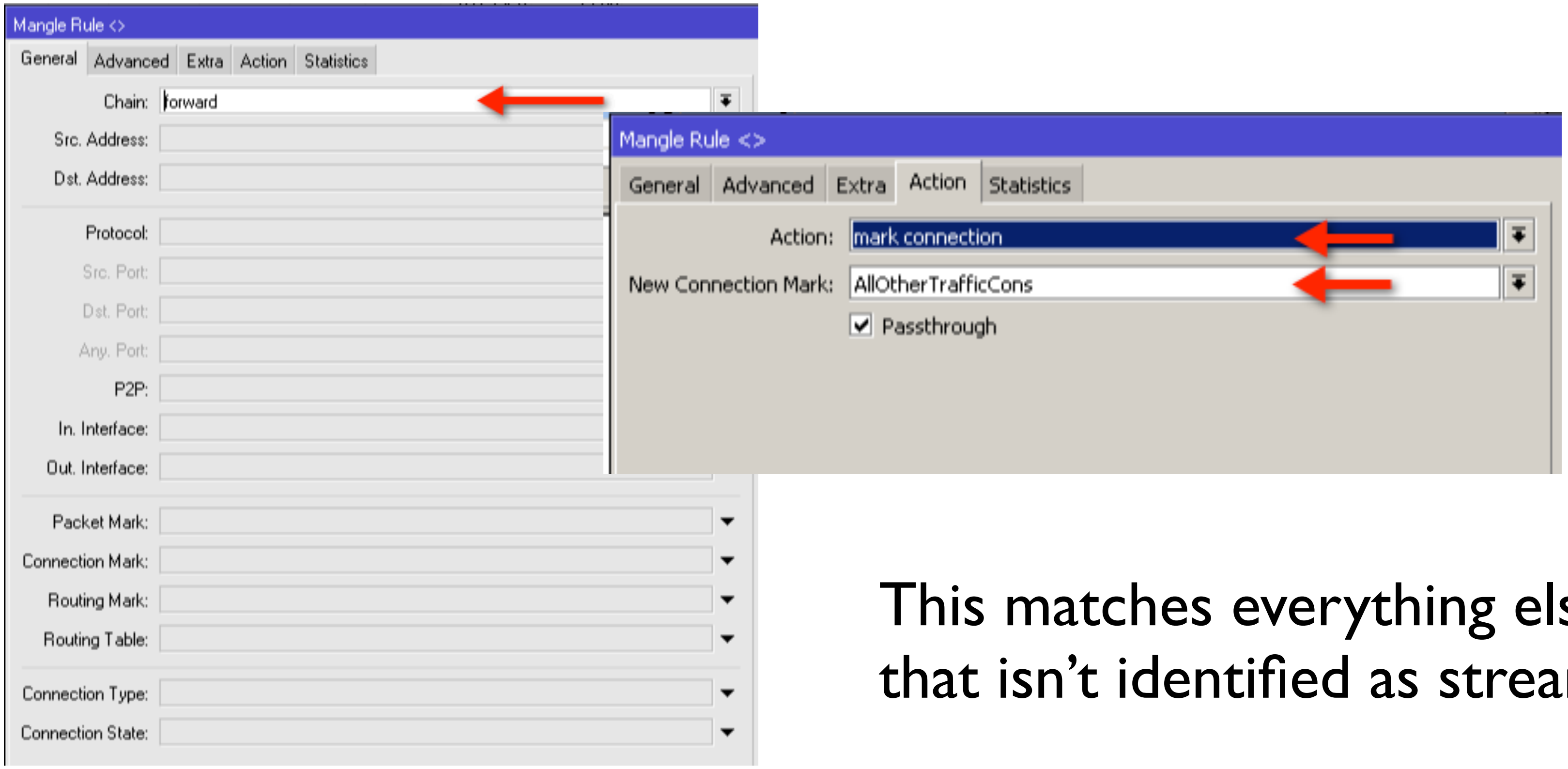
Action: mark packet

New Packet Mark: stream

□ Passthrough

- Next we create a mangle rule in the forward chain, matching connection mark Netflix-Cons and mark the packets

Mangle Process Step by Step



Mangle Rule <>

Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Mangle Rule <>

Action: mark connection

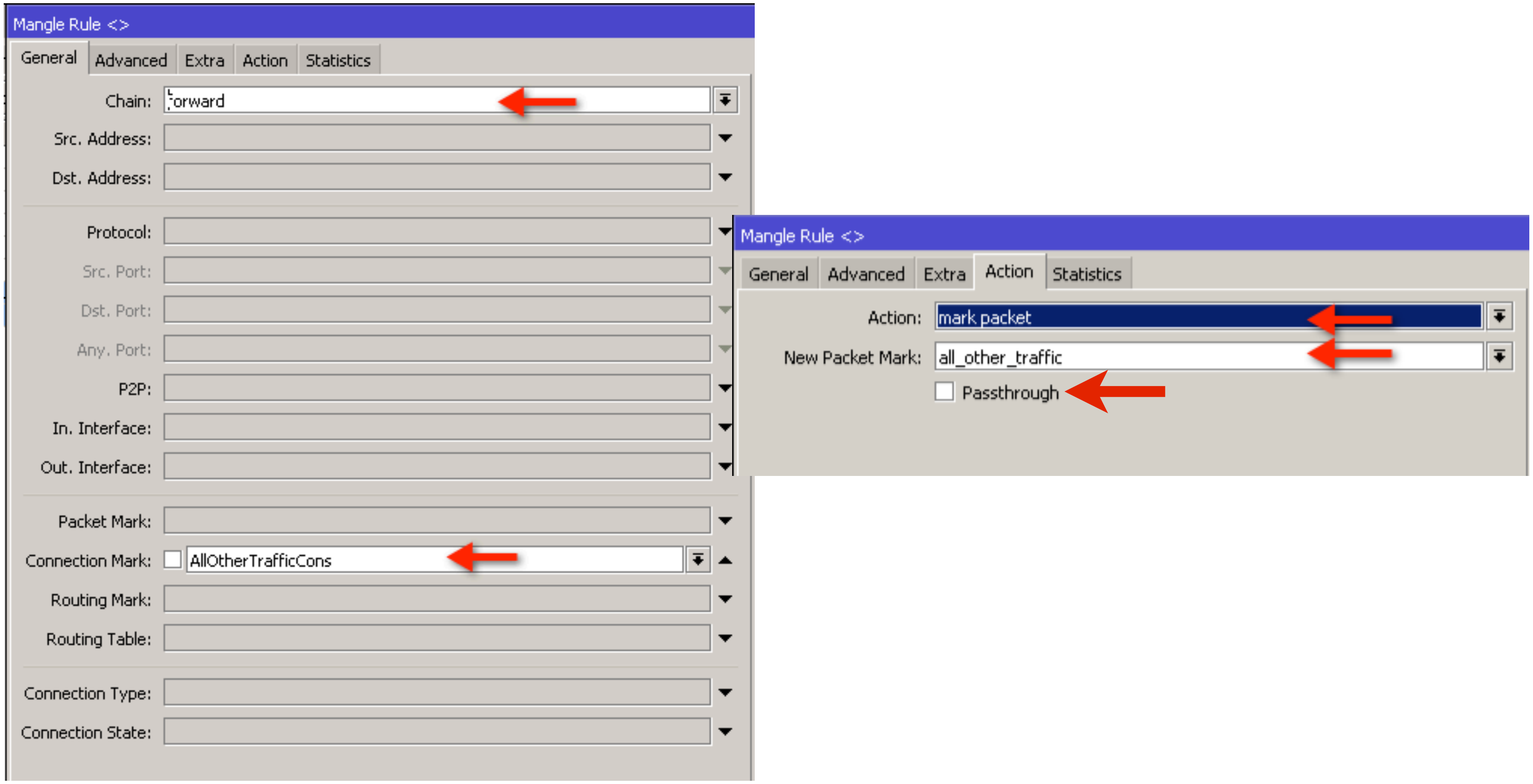
New Connection Mark: AllOtherTrafficCons

☑ Passthrough

This matches everything else that isn’t identified as streaming

- Next we create a mangle rule in the forward chain, matching all packets

Mangle Process Step by Step



Chain: forward

Connection Mark: □ AllOtherTrafficCons

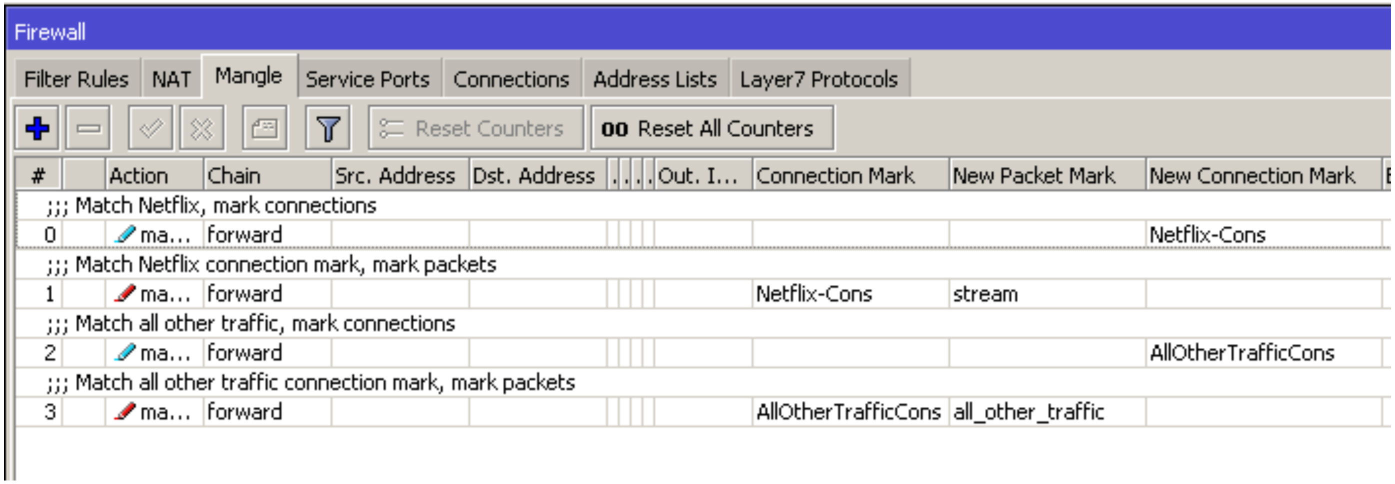
Action: mark packet

New Packet Mark: all_other_traffic

□ Passthrough

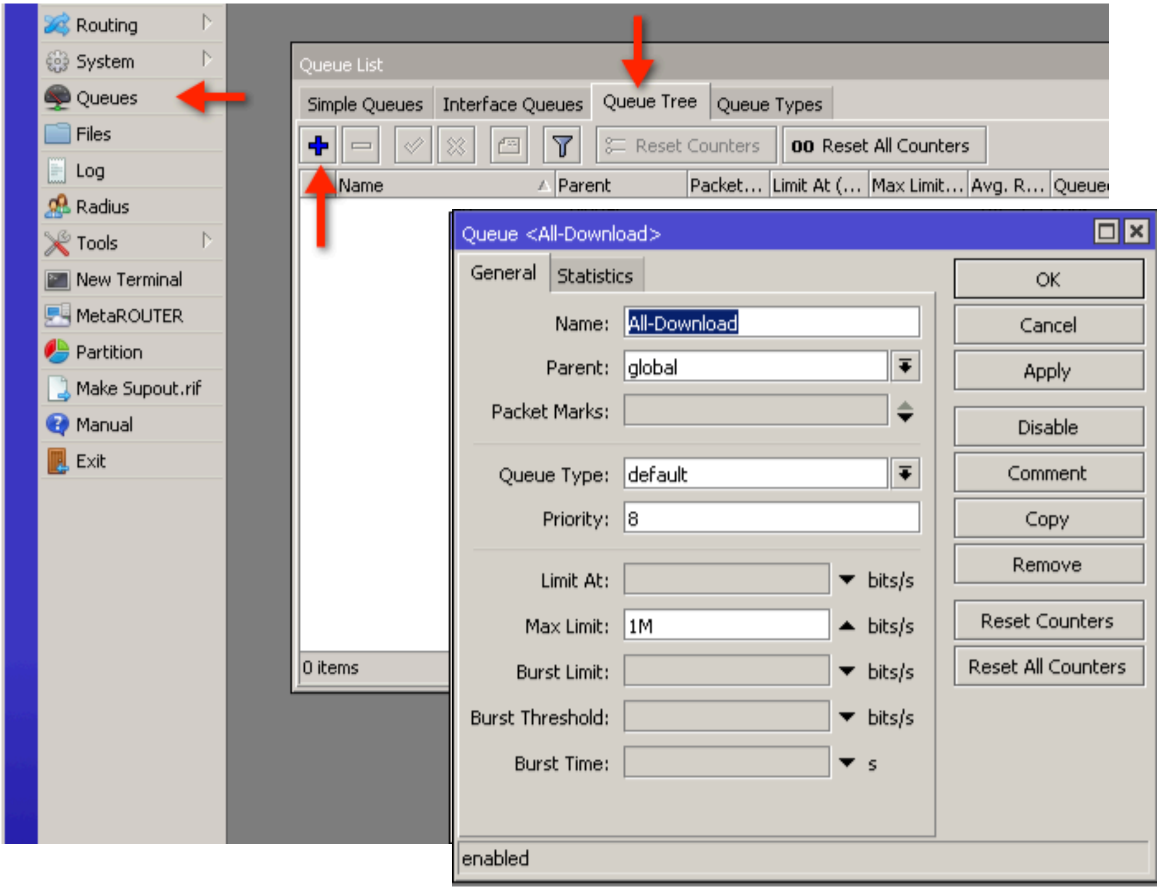
- Finally we create a mangle rule in the forward chain, matching connection mark AllOtherTrafficCons and mark the packets

Mangle Process Result



#		Action	Chain	Src. Address	Dst. Address	.	.	.	Out. I...	Connection Mark	New Packet Mark	New Connection Mark	B
;;; Match Netflix, mark connections													
0		ma...	forward									Netflix-Cons	
;;; Match Netflix connection mark, mark packets													
1		ma...	forward							Netflix-Cons	stream		
;;; Match all other traffic, mark connections													
2		ma...	forward									AllOtherTrafficCons	
;;; Match all other traffic connection mark, mark packets													
3		ma...	forward							AllOtherTrafficCons	all_other_traffic		

Queue Process Step by Step



Name: All-Download

Parent: global

Packet Marks:

Queue Type: default

Priority: 8

Limit At: bits/s

Max Limit: 1M bits/s

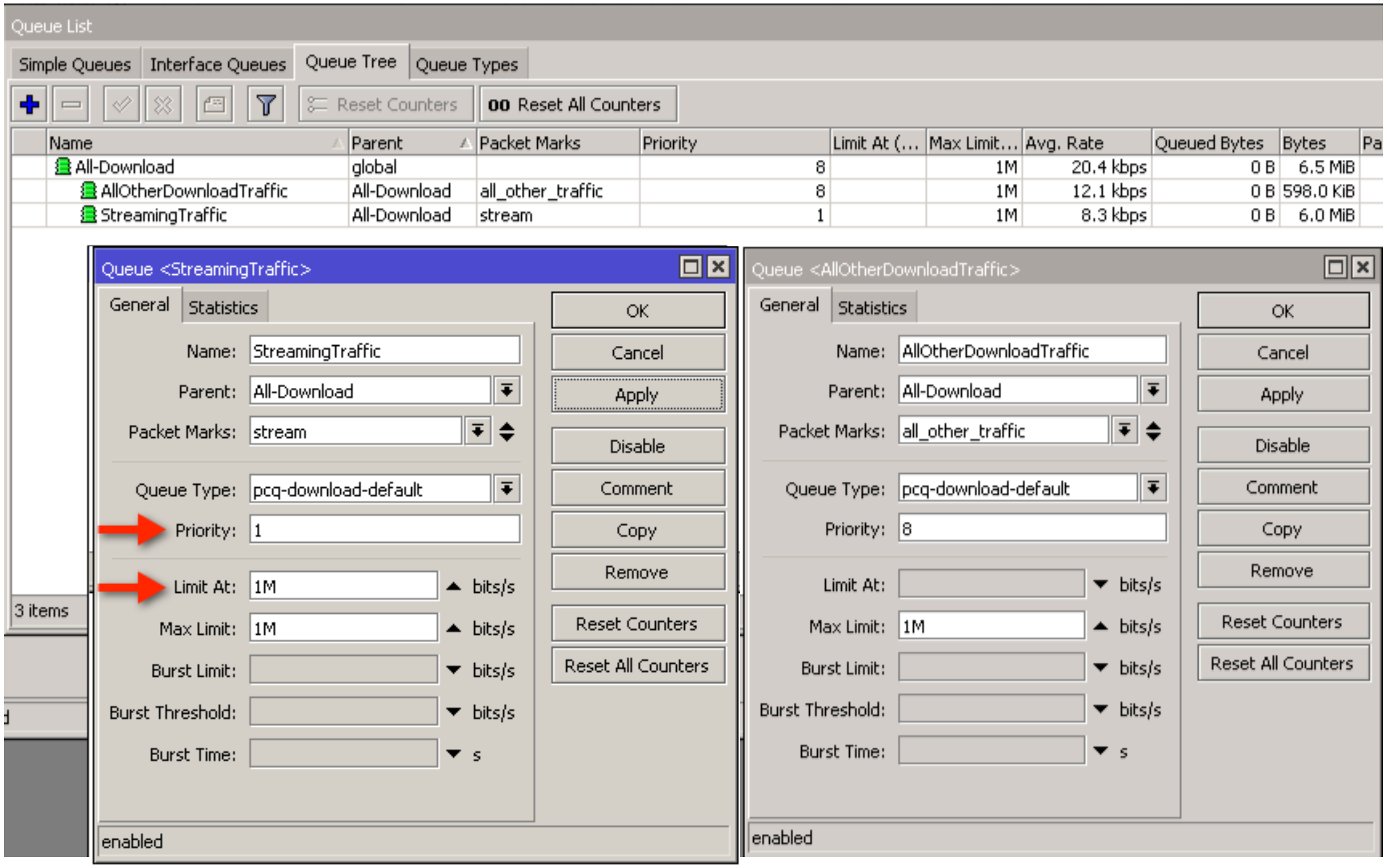
Burst Limit: bits/s

Burst Threshold: bits/s

Burst Time: s

- Start by creating the top level queue, the parent.
- We should set the max limit, in this case the internet connection speed

Queue Process Step by Step



Name	Parent	Packet Marks	Priority	Limit At (...	Max Limit...	Avg. Rate	Queued Bytes	Bytes	Pa
All-Download	global		8		1M	20.4 kbps	0 B	6.5 MiB	
AllOtherDownloadTraffic	All-Download	all_other_traffic	8		1M	12.1 kbps	0 B	598.0 KiB	
StreamingTraffic	All-Download	stream	1		1M	8.3 kbps	0 B	6.0 MiB	

Queue <StreamingTraffic>

Name: StreamingTraffic
Parent: All-Download
Packet Marks: stream
Queue Type: pcq-download-default
Priority: 1
Limit At: 1M bits/s
Max Limit: 1M bits/s
Burst Limit: bits/s
Burst Threshold: bits/s
Burst Time: s

enabled

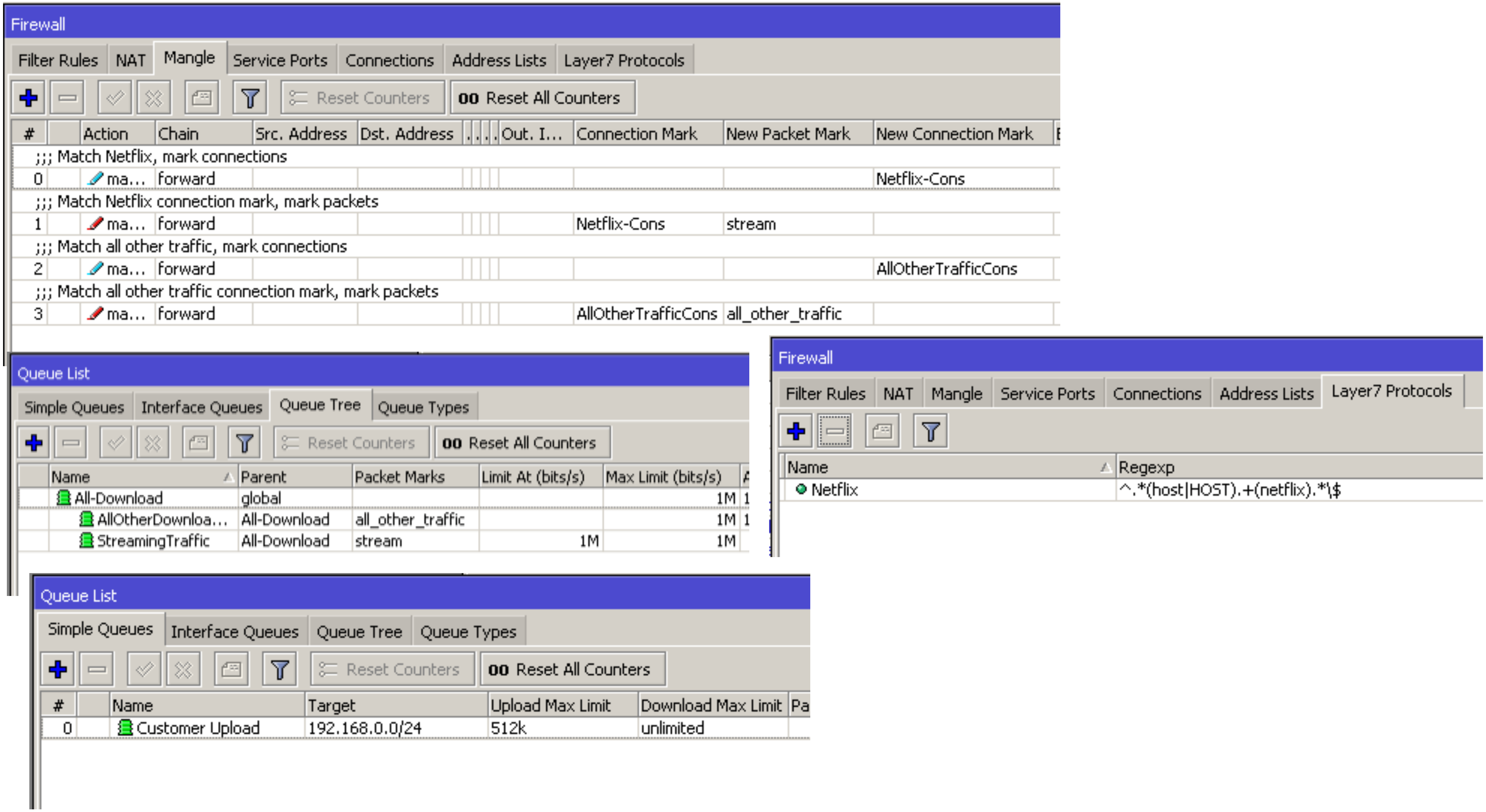
Queue <AllOtherDownloadTraffic>

Name: AllOtherDownloadTraffic
Parent: All-Download
Packet Marks: all_other_traffic
Queue Type: pcq-download-default
Priority: 8
Limit At: bits/s
Max Limit: 1M bits/s
Burst Limit: bits/s
Burst Threshold: bits/s
Burst Time: s

enabled

- Next we create two child queues, one for streams and one for everything else.

Final Config - Winbox



#		Action	Chain	Src. Address	Dst. Address	Out. I...	Connection Mark	New Packet Mark	New Connection Mark
;;; Match Netflix, mark connections									
0		ma...	forward						Netflix-Cons
;;; Match Netflix connection mark, mark packets									
1		ma...	forward				Netflix-Cons	stream	
;;; Match all other traffic, mark connections									
2		ma...	forward						AllOtherTrafficCons
;;; Match all other traffic connection mark, mark packets									
3		ma...	forward				AllOtherTrafficCons	all_other_traffic	

Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)
All-Download	global			1M
AllOtherDownloa...	All-Download	all_other_traffic		1M
StreamingTraffic	All-Download	stream	1M	1M

Name	Regexp
Netflix	^.*(host|HOST).+(netflix).*\$

#		Name	Target	Upload Max Limit	Download Max Limit	Pa
0		Customer Upload	192.168.0.0/24	512k	unlimited	

Final Config - CLI

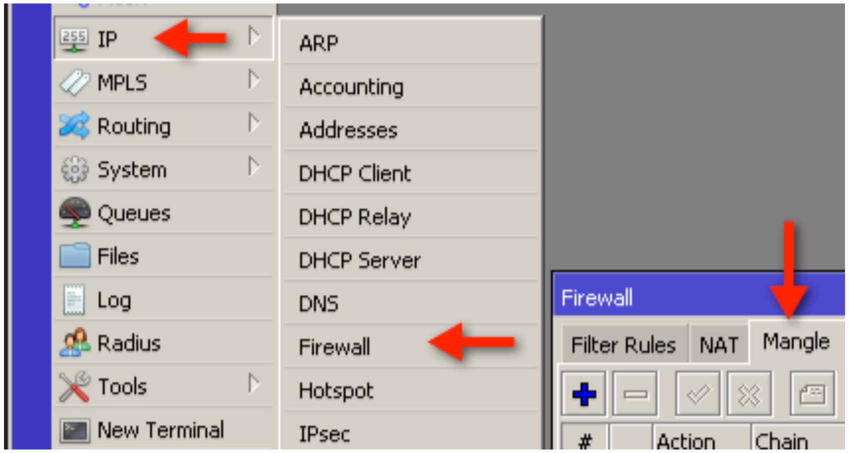
Config does not include standard setup items like DHCP, masquerade, etc.

```
/ip firewall layer7-protocol
add name=Netflix regexp="^.*(host|HOST).+(netflix).*\$"
/queue simple
add disabled=no max-limit=512k/0 name="Customer Upload" target=\
    192.168.0.0/24
/queue tree
add max-limit=1M name=All-Download parent=global queue=default
add limit-at=1M max-limit=1M name=StreamingTraffic packet-mark=stream parent=\
    All-Download priority=1 queue=pcq-download-default
add max-limit=1M name=AllOtherDownloadTraffic packet-mark=all_other_traffic \
    parent=All-Download queue=pcq-download-default
/queue type
set pcq-download-default pcq-rate=512k
/ip firewall mangle
add action=mark-connection chain=forward comment="Match Netflix, mark connections" disabled=no layer7-protocol=Netflix \
    new-connection-mark=Netflix-Cons passthrough=yes
add action=mark-connection chain=forward comment="Match all other traffic, mark connections" disabled=no new-connection-mark=\
    AllOtherTrafficCons passthrough=yes
add action=mark-packet chain=forward comment="Match Netflix connection mark, mark packets" connection-mark=Netflix-Cons \
    disabled=no new-packet-mark=stream passthrough=no
add action=mark-packet chain=forward comment="Match all other traffic connection mark, mark packets" connection-mark=\
    Netflix-Cons disabled=no new-packet-mark=all_other_traffic passthrough=no
```

Time To Dig In

I like to teach the why's rather than just the how.

Mangling



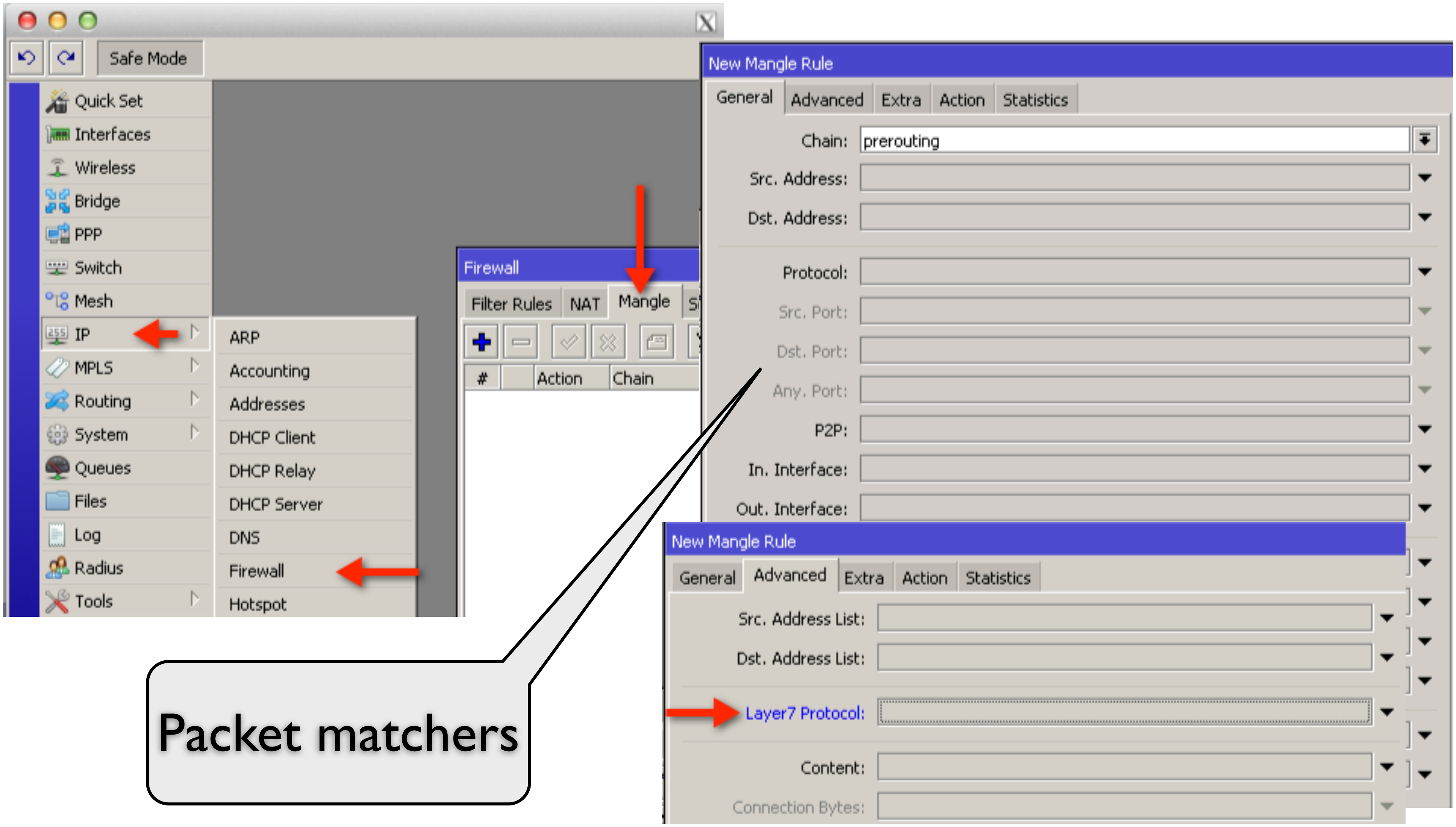
- The purpose of the mangle facility is to identify traffic and then do something meaningful to, like marking it so we can manage it later.

- Mangles can identify traffic based on source port, destination port, protocol, etc.,

OR

- By using Layer7 matcher expressions, better choice for streaming traffic since protocols like RTMP use port 80

Mangle Rules



Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

New Mangle Rule

Src. Address List:

Dst. Address List:

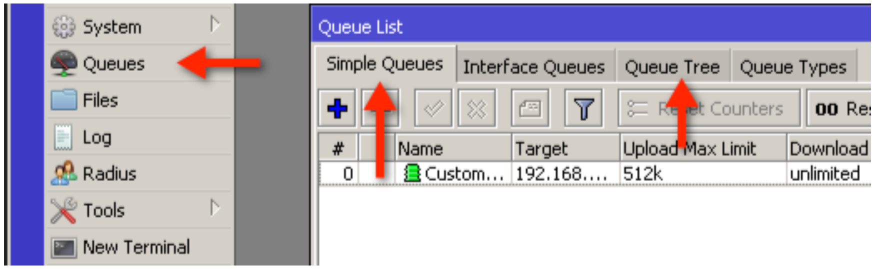
Layer7 Protocol:

Content:

Connection Bytes:

Packet matchers

Queues

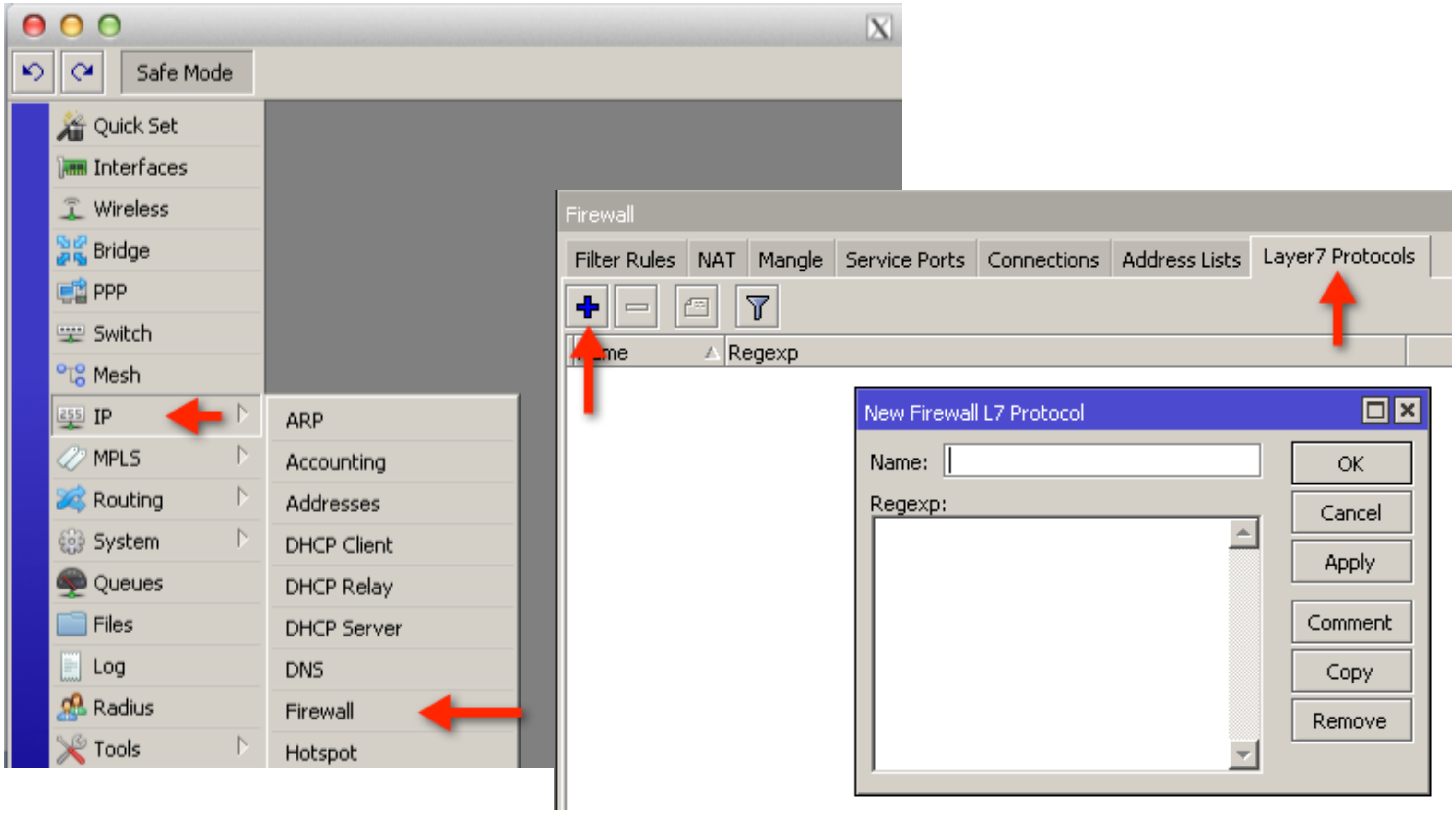


#	Name	Target	Upload Max Limit	Download
0	Custom...	192.168....	512k	unlimited

Queues allow you to allocate bandwidth based on some criteria. In our case we will use packet marks as our criteria.

We can create hierarchal relationships between the queues such that some queues are allowed to fill before other queues. This is often called “traffic prioritization” which can be a misnomer.

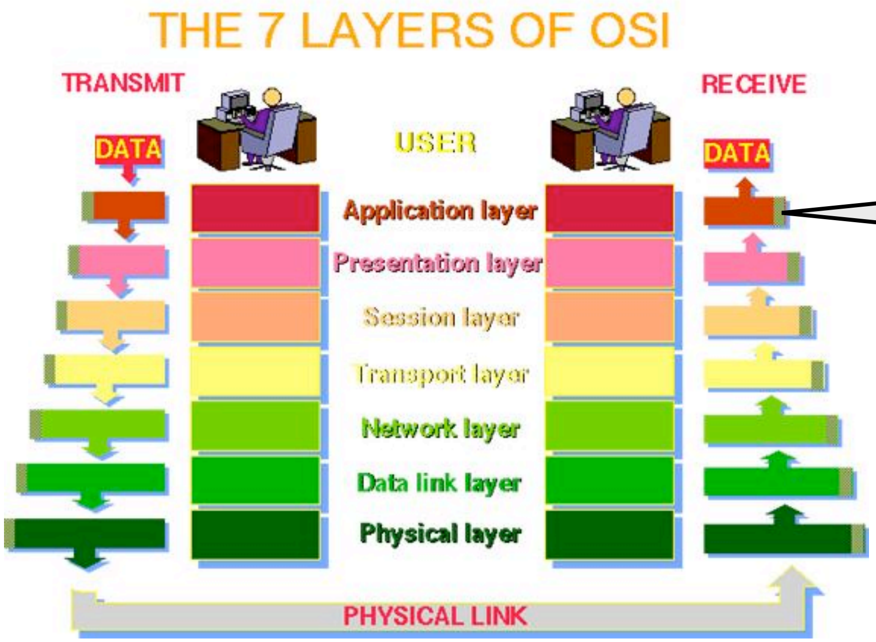
L7 Matchers



Name:

Regexp:

Remember Layer 7?



Layer 7 - Application Layer

- Remember the OSI Model?
- OSI - Open System Interconnection
- Seven tiered model for network communication

Remember Layer 7?

- In Layer 7 we can see the "flavor" of IP traffic.
- This layer provides application services for file transfers, e-mail, and other network software services. For example, Telnet and FTP are applications that exist entirely in the application level.

Layer 7 in ROS

- The L7 matcher collects the first 10 packets of a connection or the first 2KB of a connection and searches for a pattern. If pattern is not found in collected data, matcher does not inspect further.
- You should take into account that a lot of connections will significantly increase memory usage. To avoid it add regular firewall matchers to reduce amount of data passed to layer-7 filters.

Layer 7 in ROS

- An additional requirement is that the Layer7 matcher must see both directions of traffic (incoming and outgoing). To satisfy this requirement L7 rules should be set in the forward chain.
- If the rule is set in the input/prerouting chain then the same rule also must be set in the output/ postrouting chain, otherwise the collected data may not be complete resulting in incorrectly matched patterns.

Layer 7 Uses Regex

- Regex, the abbreviation for Regular Expressions is a sequence of characters that forms a search pattern.
- For example, if I told you I was doing a search for “*” you would know that I meant “everything”.
- Likewise, if I searched for “*.exe” you would already know I was probably looking for an executable file with any file name.
- Regex is like search patterns on steroids!

Layer 7 Uses Regex

- This presentation is not on Regex.
- Examples:

^	matches the beginning of a string
.	matches any character
*	matches 0 or more of the preceding character, so .* matches one or an unlimited number of any character

- Regex has different flavors but the one used by ROS is the same as the L-7 Filter Project found on Sourceforge.net (http://l7-filter.sourceforge.net/protocols)

Sources of Regex Expressions

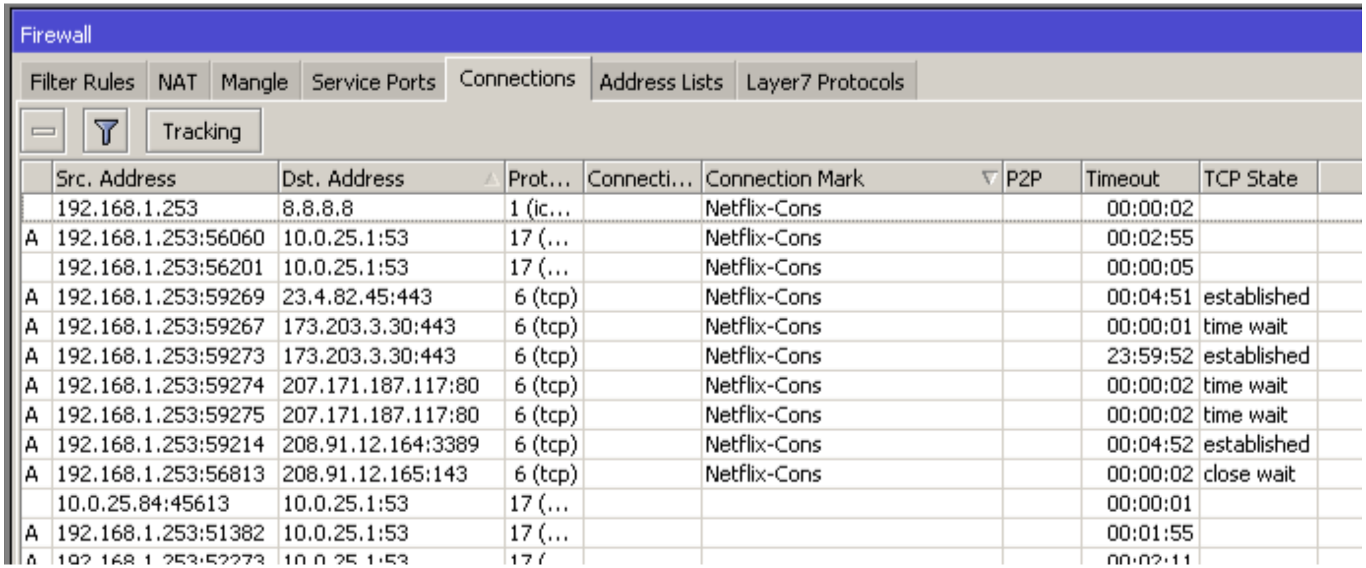
- MikroTik Wiki http://www.mikrotik.com/download/l7-protos.rsc
- My Web Site http://MyWISPTraining.com

Understanding Mangle Process

- **Optimal mangle** - match connections, passthrough and then mark packets
- Least resource intensive
- Wiki suggests we match connections/packets in the forward chain, that way we get to look at the upload and download streams

Why Mark connections Then Packets?

- Lease resource intensive.
- Makes troubleshooting easier.
- Remember, mangle order is important!



	Src. Address	Dst. Address	Prot...	Connecti...	Connection Mark	P2P	Timeout	TCP State
	192.168.1.253	8.8.8.8	1 (ic...		Netflix-Cons		00:00:02	
A	192.168.1.253:56060	10.0.25.1:53	17 (...		Netflix-Cons		00:02:55	
	192.168.1.253:56201	10.0.25.1:53	17 (...		Netflix-Cons		00:00:05	
A	192.168.1.253:59269	23.4.82.45:443	6 (tcp)		Netflix-Cons		00:04:51	established
A	192.168.1.253:59267	173.203.3.30:443	6 (tcp)		Netflix-Cons		00:00:01	time wait
A	192.168.1.253:59273	173.203.3.30:443	6 (tcp)		Netflix-Cons		23:59:52	established
A	192.168.1.253:59274	207.171.187.117:80	6 (tcp)		Netflix-Cons		00:00:02	time wait
A	192.168.1.253:59275	207.171.187.117:80	6 (tcp)		Netflix-Cons		00:00:02	time wait
A	192.168.1.253:59214	208.91.12.164:3389	6 (tcp)		Netflix-Cons		00:04:52	established
A	192.168.1.253:56813	208.91.12.165:143	6 (tcp)		Netflix-Cons		00:00:02	close wait
	10.0.25.84:45613	10.0.25.1:53	17 (...				00:00:01	
A	192.168.1.253:51382	10.0.25.1:53	17 (...				00:01:55	
A	192.168.1.253:52273	10.0.25.1:53	17 (...				00:02:11	

Queue Process Step by Step

- Next we will create the queues.
- Queues are the basis of QOS or Quality of Service.
- In ROS, all queues are based on HTB
- The ability to prioritize queues, allowing some queues to fill before others is the key to ensuring service levels.
- Remember that prioritizing traffic does not "re-order" packets, they will still come and go in whatever order they are transmitted but we will help ensure network congestion is minimized for certain traffic types

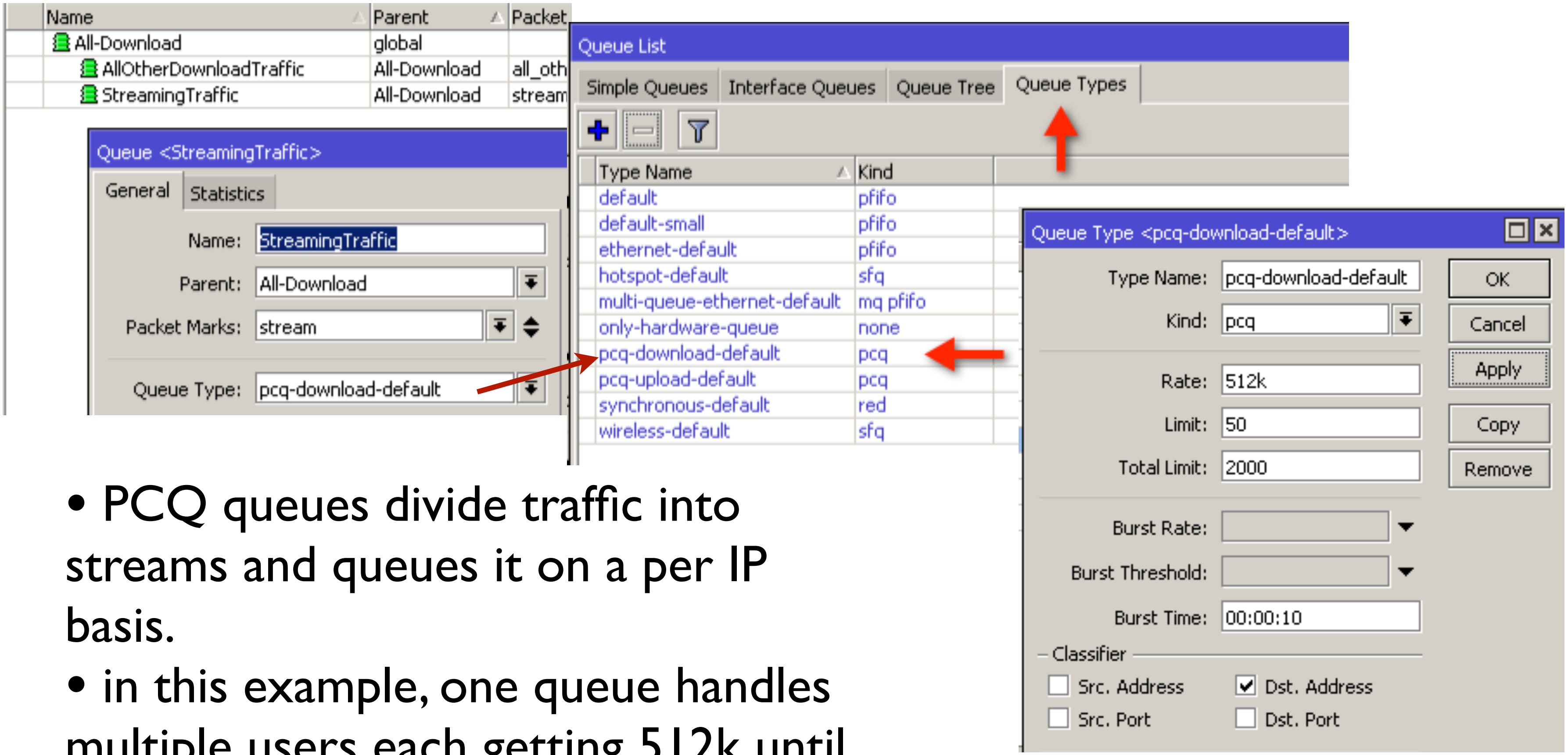
Queue Process Step by Step

- In Version 6, the queue tree was revamped. We now have only 1 global queue called "global", not global-in, out, total, etc.
- This greatly simplifies the queue tree but also pushes us toward simple queues.
- I like the hierarchal nature of the queue tree so we will use it for this configuration.

Queue Process Step by Step

- Queue trees are most effective when we break them down into upload and download queues. Since streaming traffic in this example is primarily download, we will only create download queues for simplicity.

Note We Are Using PCC Queue Type



Name	Parent	Packet
All-Download	global	
AllOtherDownloadTraffic	All-Download	all_oth
StreamingTraffic	All-Download	stream

Queue <StreamingTraffic>

Name: StreamingTraffic

Parent: All-Download

Packet Marks: stream

Queue Type: pcq-download-default

Queue List

Type Name	Kind
default	pfifo
default-small	pfifo
ethernet-default	pfifo
hotspot-default	sfq
multi-queue-ethernet-default	mq pfifo
only-hardware-queue	none
pcq-download-default	pcq
pcq-upload-default	pcq
synchronous-default	red
wireless-default	sfq

Queue Type <pcq-download-default>

Type Name: pcq-download-default

Kind: pcq

Rate: 512k

Limit: 50

Total Limit: 2000

Burst Rate:

Burst Threshold:

Burst Time: 00:00:10

Classifier

□ Src. Address ☑ Dst. Address

□ Src. Port □ Dst. Port

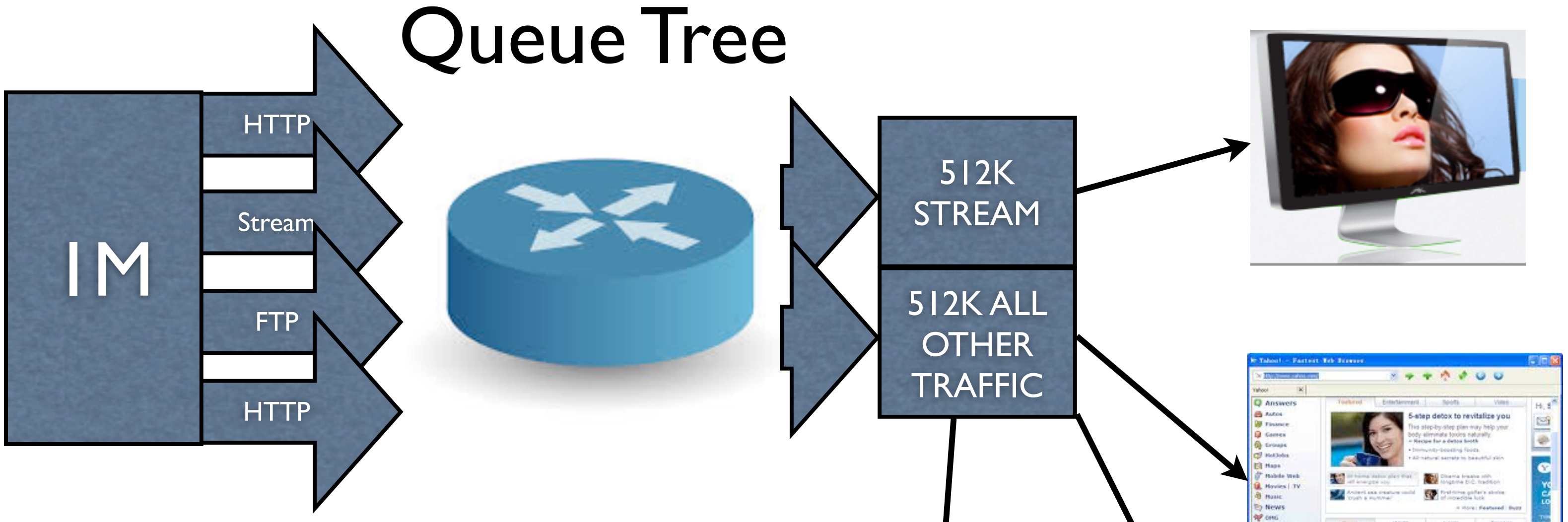
- PCQ queues divide traffic into streams and queues it on a per IP basis.
- in this example, one queue handles multiple users each getting 512k until exhausted

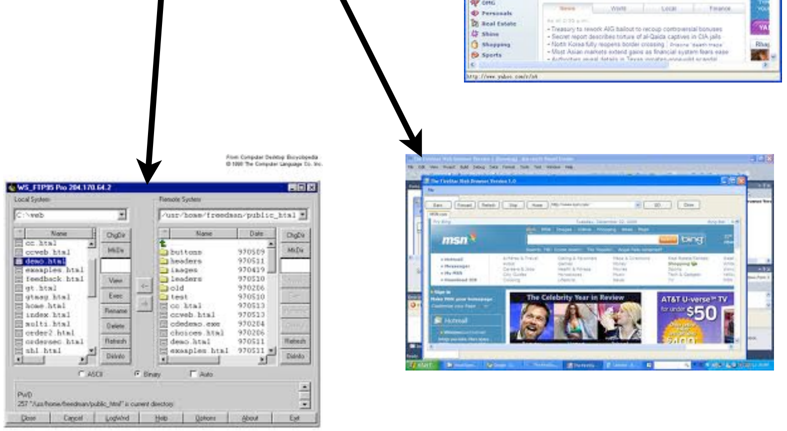
MikroTik BOOT CAMP

About the Queue Tree

- Remember that the top level queues (parents) will always try to satisfy the leaf queues' (children) limit-at setting first, then the max-limit setting if they have enough bandwidth to distribute to the leaf queues
- Think of limit-at as a committed rate, use it sparingly

How Will This Configuration Behave?

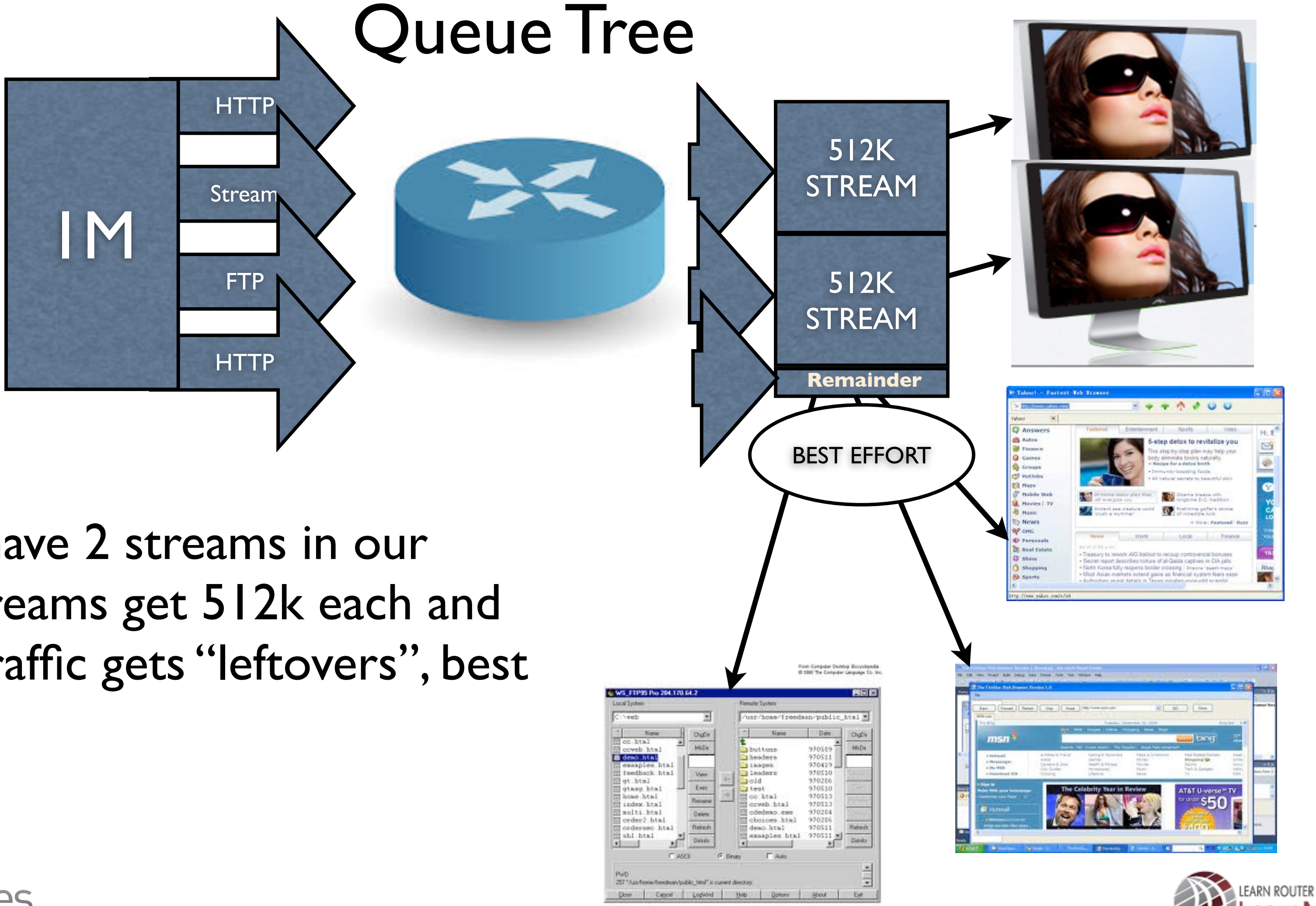




We have multiple types of traffic entering the router, yet our stream gets entire 512k allocation, all other traffic share remaining bandwidth

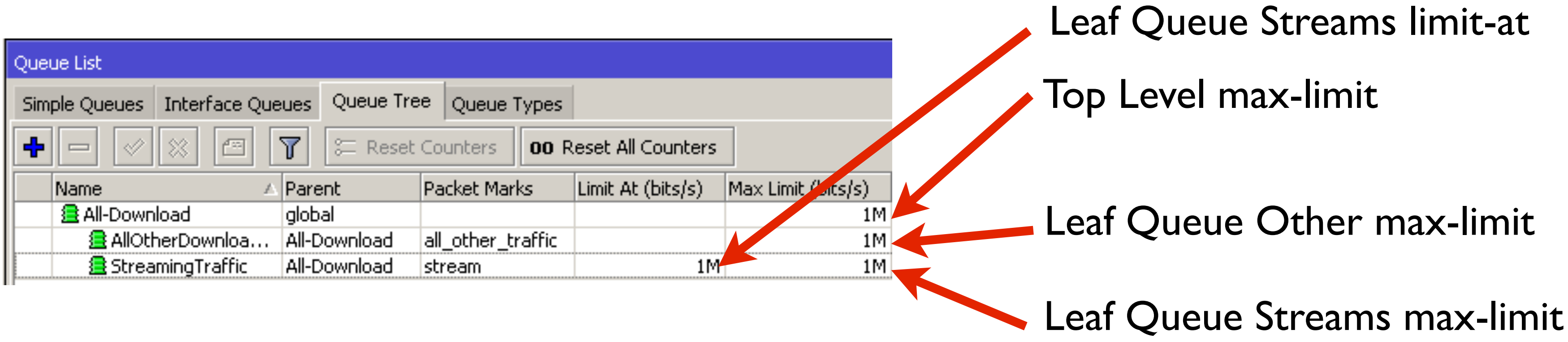
How Will This Configuration Behave?

Queue Tree



When we have 2 streams in our example, streams get 512k each and remaining traffic gets “leftovers”, best effort

How Do You Set The Queues?



Queue List

Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)
All-Download	global			1M
AllOtherDownloa...	All-Download	all_other_traffic		1M
StreamingTraffic	All-Download	stream	1M	1M

Leaf Queue Streams limit-at

Top Level max-limit

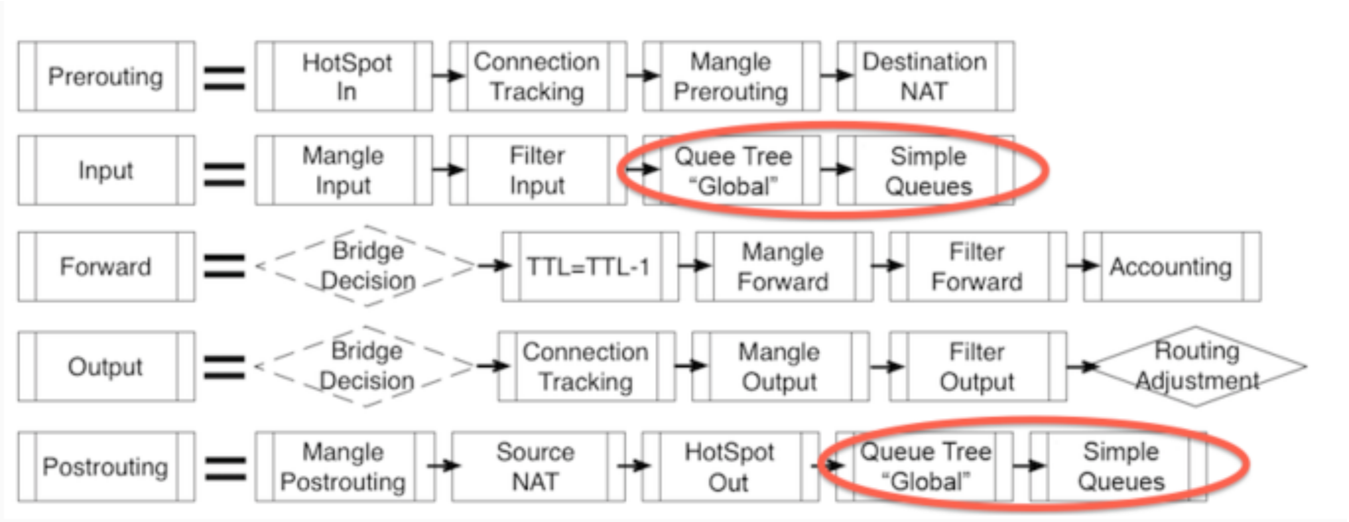
Leaf Queue Other max-limit

Leaf Queue Streams max-limit

Download Speed	# of Simultaneous Streams	Top Level max-limit	Leaf Queue Streams limit-at	Leaf Queue Streams max-limit	Leaf Queue Other max-limit
512k	1	512k	512k	512k	512k
1M	2	1M	1M	1M	1M
1.5M	3	1500k	1500k	1500k	1500k
2M	4	2M	2M	2M	2M

What About Upload Rate Limiting?

- A major change in version 6 is the packet flow diagram.
- In previous versions simple queues were slow and would rob bandwidth from the queue tree
- Simple queues are now AFTER the global HTB



Prerouting = HotSpot In → Connection Tracking → Mangle Prerouting → Destination NAT

Input = Mangle Input → Filter Input → Quee Tree "Global" → Simple Queues

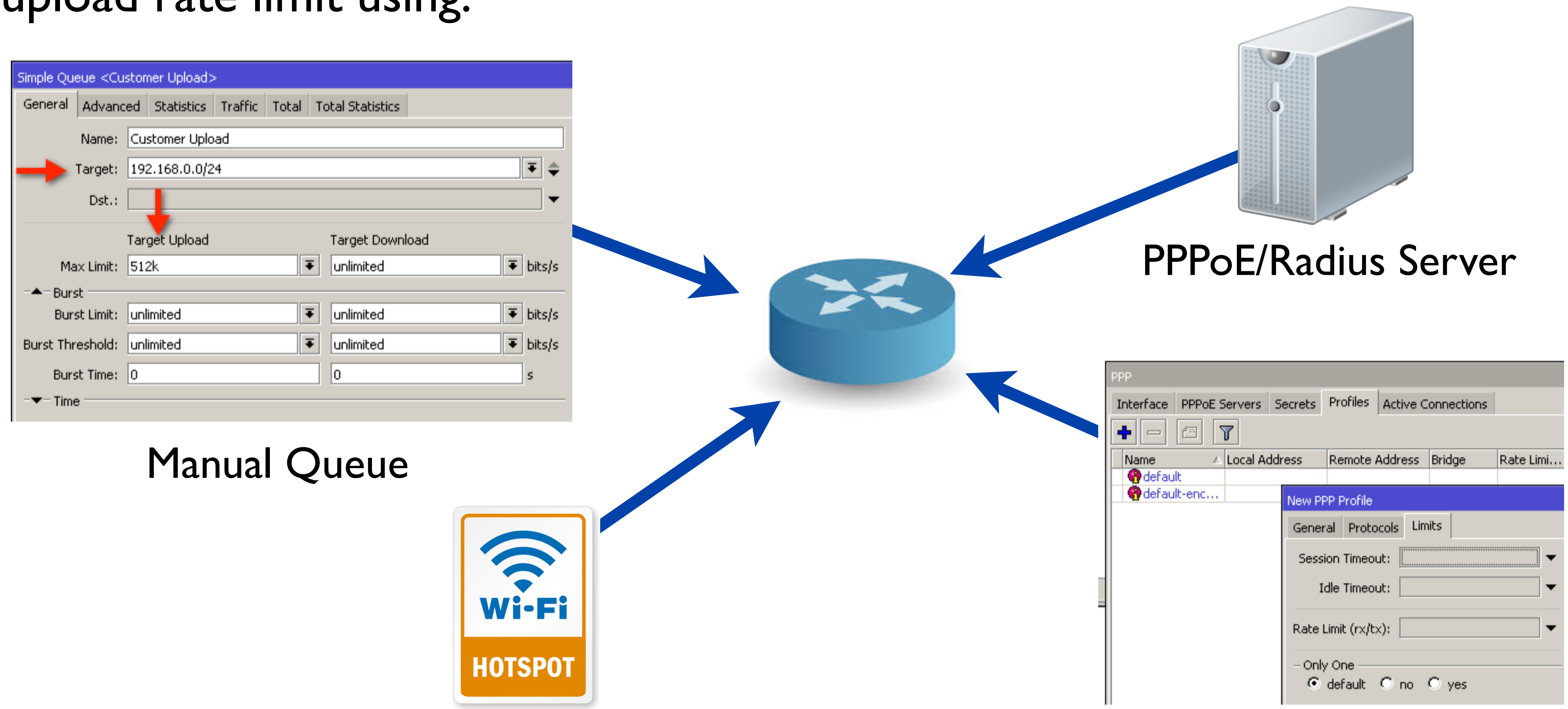
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting

Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment

Postrouting = Mangle Postrouting → Source NAT → HotSpot Out → Queue Tree "Global" → Simple Queues

What About Upload Rate Limiting?

With the queue tree in place, create a simple queue for customer upload rate limit using:



Simple Queue <Customer Upload>

Name: Customer Upload

Target: 192.168.0.0/24

Dst.:

	Target Upload	Target Download	
Max Limit:	512k	unlimited	bits/s
Burst			
Burst Limit:	unlimited	unlimited	bits/s
Burst Threshold:	unlimited	unlimited	bits/s
Burst Time:	0	0	s

Time

Manual Queue

PPPoE/Radius Server

Hotspot User Profile

PPP

Name	Local Address	Remote Address	Bridge	Rate Limi...
default				
default-enc...				

New PPP Profile

Session Timeout:

Idle Timeout:

Rate Limit (rx/tx):

Only One

● default ○ no ○ yes

PPPoE Profile

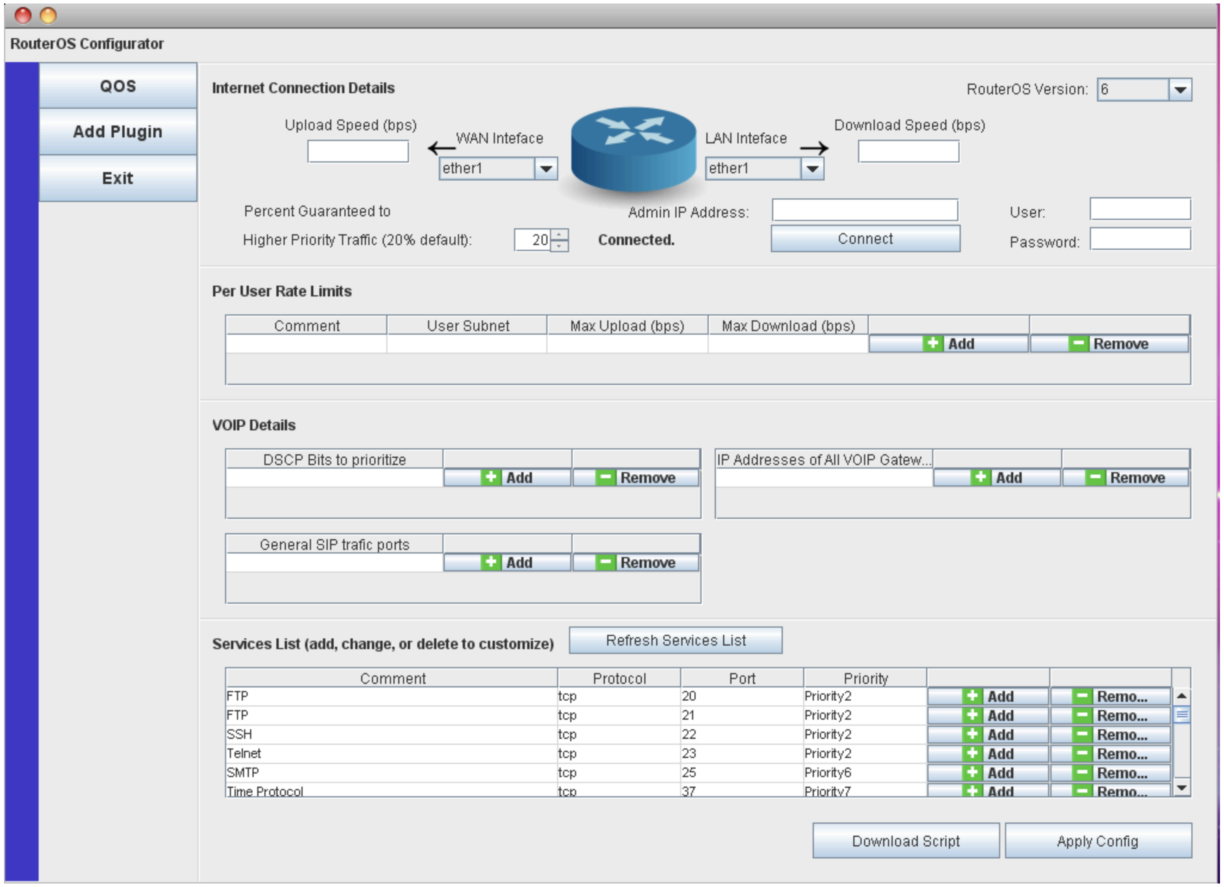
Suggestions

- Reduce router load by making the packet matchers more selective

- Packet-mark = no-mark or connection-mark = no-mark are good ways to do this

ISPSupplies

New Product!



Internet Connection Details

RouterOS Version: 6

Upload Speed (bps)

WAN Inteface ← ether1

LAN Inteface → ether1

Download Speed (bps)

Percent Guaranteed to Higher Priority Traffic (20% default): 20

Admin IP Address:

Connected.

User:

Password:

Per User Rate Limits

Comment	User Subnet	Max Upload (bps)	Max Download (bps)

VOIP Details

DSCP Bits to prioritize

IP Addresses of All VOIP Gatew...

General SIP trafic ports

Services List (add, change, or delete to customize)

Comment	Protocol	Port	Priority		
FTP	tcp	20	Priority2	Add	Remo...
FTP	tcp	21	Priority2	Add	Remo...
SSH	tcp	22	Priority2	Add	Remo...
Telnet	tcp	23	Priority2	Add	Remo...
SMTP	tcp	25	Priority6	Add	Remo...
Time Protocol	tcp	37	Priority7	Add	Remo...

MikroTik Configurator

- Concept is similar to QuickSet but for more complex configurations
- Container app with plugin architecture
- Java - works on Windows/Mac
- QOS Plugin
- Load Balance Plugin
- Firewall plugin
- Other plugins available soon
- Join the email notification list at MikroTikConfig.com

Thank You!

- MyWISPTraining.com
- LearnMikroTik.com
- ISPSupplies.com
- "RouterOS by Example" available from distributors, Amazon.com, Kindle, iTunes