ENHANCED CACHING FOR SERVICE

Presented by:
Sunday A. Idajili
ITClick Networx Limited
http://www.itclick.net
sonny@itclick.net

Abstract

- ISPs are constantly seeking ways to improve web http service delivery to end users.
- To achieve Quality of Service, ISPs deploy Bandwidth Managers to shape customer traffic based on several policies.
- To accelerate http delivery, ISPs deploy web caches to cache frequently accessed web sites.
- Though bandwidth is saved using a web cache and bandwidth manager, the accelerated performance is not felt by the end user because they are still penalized by the bandwidth manager even when content is cached and residing on the web cache.
- This presentation will show you how to use the TOS (RouterOS v2.9) or DSCP (RouterOS v3.0) mangle feature on your RouterOS bandwidth manager together with a squid-2.6 external cache to manage the delivery of cache contents with or without penalty to your end users, making them experience the true performance of caching.

About ITClick Networx

- A subsidiary of ITClick Solutions Limited - Nigeria
- Established in 2002 to provide Telecommunication services
- Core business areas: Telecommunications, Consulting, Network design and integration services.

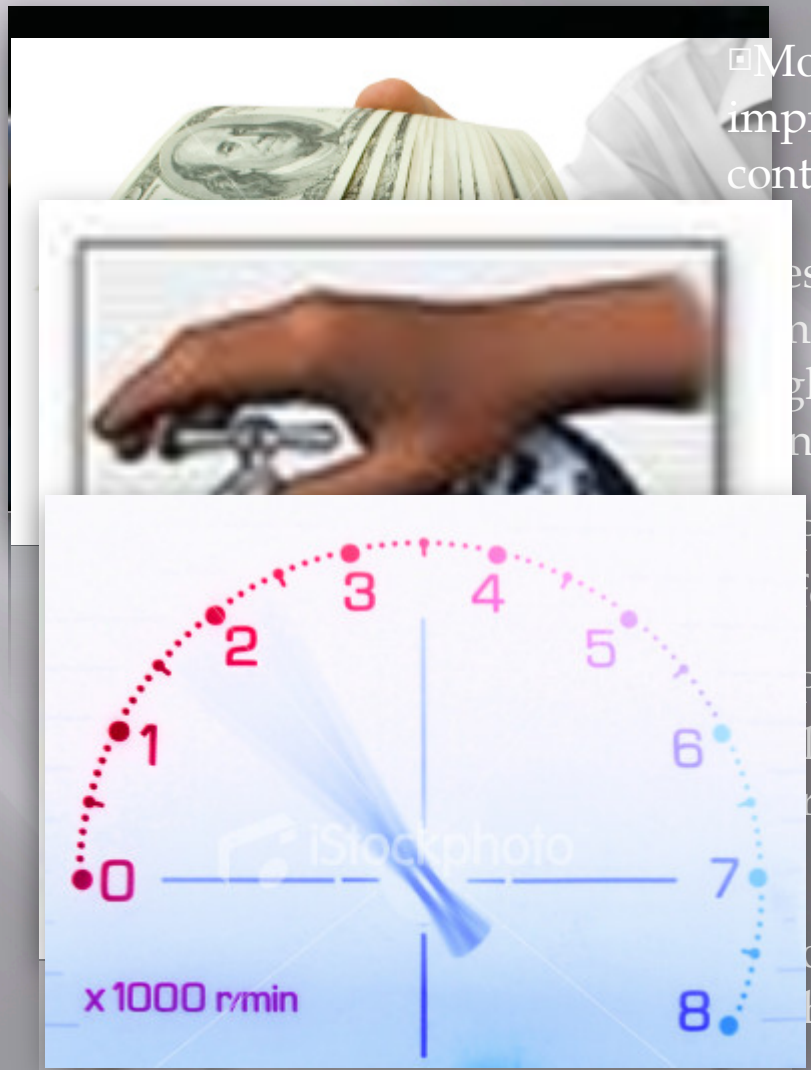
More information about us can be found at
http://www.itclick.net

Mikrotik Experience

- Using Mikrotik since 2004
- Currently running ISP with 16 active base stations

Mikrotik specific Expertise:
- Radius , Billing and Caching techniques
- Centralized Hotspot, Advanced Queue Tree based QoS,
- Advanced firewall and Routing (Policy based, OSPF and BGP), scripting
- RF planning for city wide and long distance wireless Networks, PTP, PTMP, Mesh, Nstreme.
- Dude Network monitoring with SMS alerts,
- Virtual networking (VLAN, IPSec, PPTP, IP and Tunnels).

Overview: Bandwidth and QoS



- Most ISPs upgrade bandwidth in an attempt to improve quality, when actually the problem is lack of control.
- esides financial implications, bandwidth upgrade can netimes not be a near option. Upstream provider ght be out of capacity, as it is today for most ISPs ng VSAT in Africa.
- Ps implement QoS policies to optimize network formance and keep critical applications running.
- Ps deploy transparent Web Caches to improves lity, accelerates http access and significantly reduces rall bandwidth requirements. Statistics show that of typical ISP traffic is web based.
- oS combined with Zero Penalty Hits (ZPH) Web hing results in a high byte hits rate

Benefits: ZPH Caching and QoS

ncreased value for customers

ncreased satisfaction for customers

creased profit for ISP

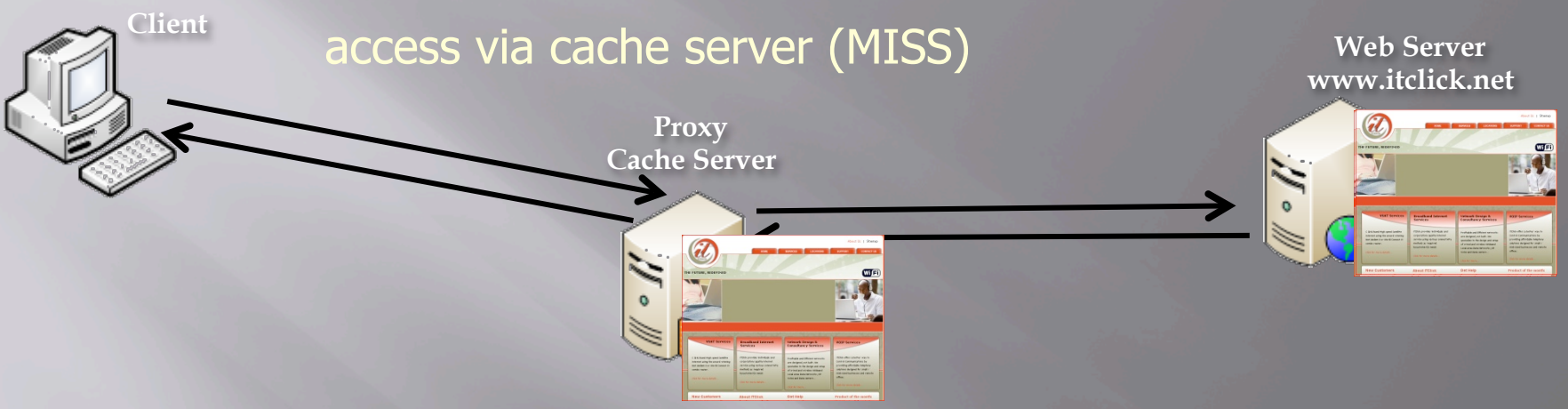
GETTING IT DONE

The basic Web Cache

The basic Web Cache

- Client requests page from http://www.itclick.net from browser
  - TCP: CONNECT www.itclick.net
  - HTTP: GET index.html
- Web server responds back with the page index.html

The basic Web Cache

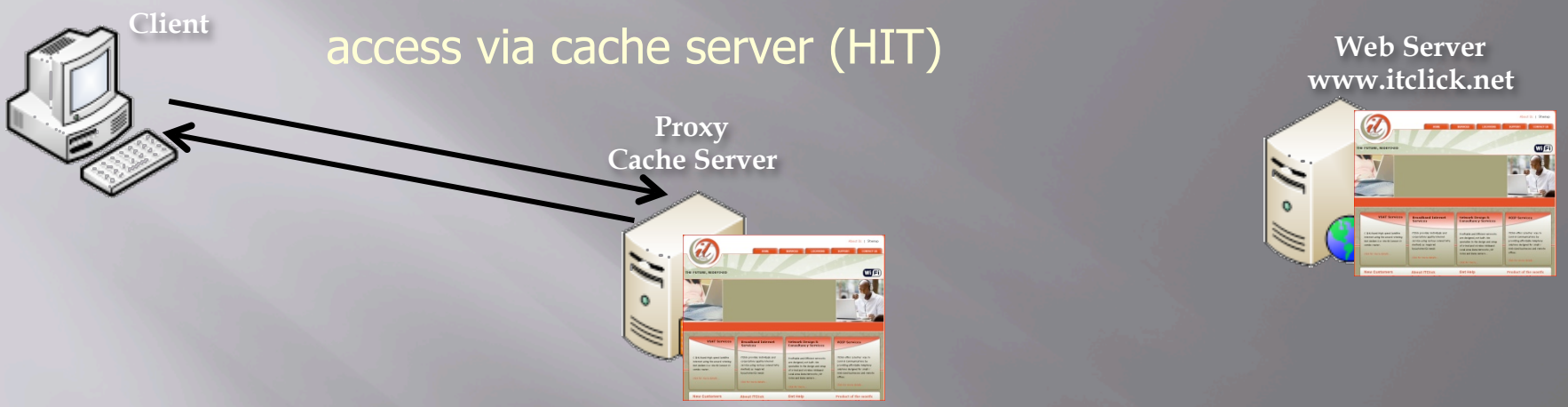


- Client requests page from http://www.itclick.net from browser via cache server
  - TCP: CONNECT cache-server.isp.com.ng
  - HTTP: GET www.itclick.net/index.html

- Cache processes request for www.itclick.net/index.html

- Cache MISS causes proxy fetch from web server
  - TCP: CONNECT www.itclick.net
  - HTTP: GET index.html

The basic Web Cache



- Client requests page from http://www.itclick.net from browser via cache server
  - TCP: CONNECT cache-server.isp.com.ng
  - HTTP: GET www.itclick.net/index.html

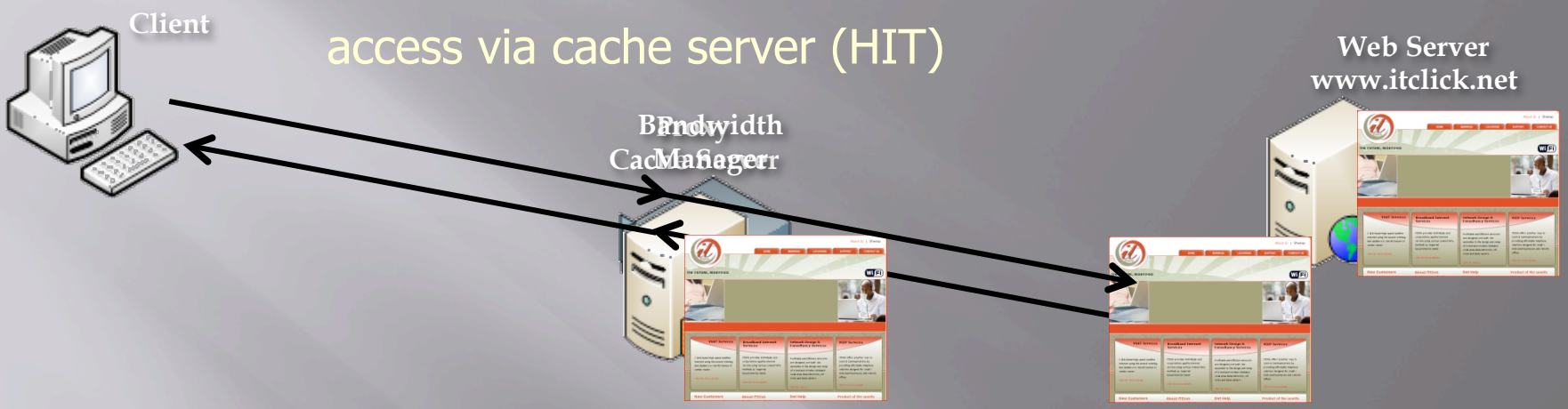
- Cache processes request for www.itclick.net/index.html

- Cache HIT causes proxy fetch from disk
  - TCP: CONNECT www.itclick.net
  - HTTP: GET index.html

THE CHALLENGE

Caching with QoS Management

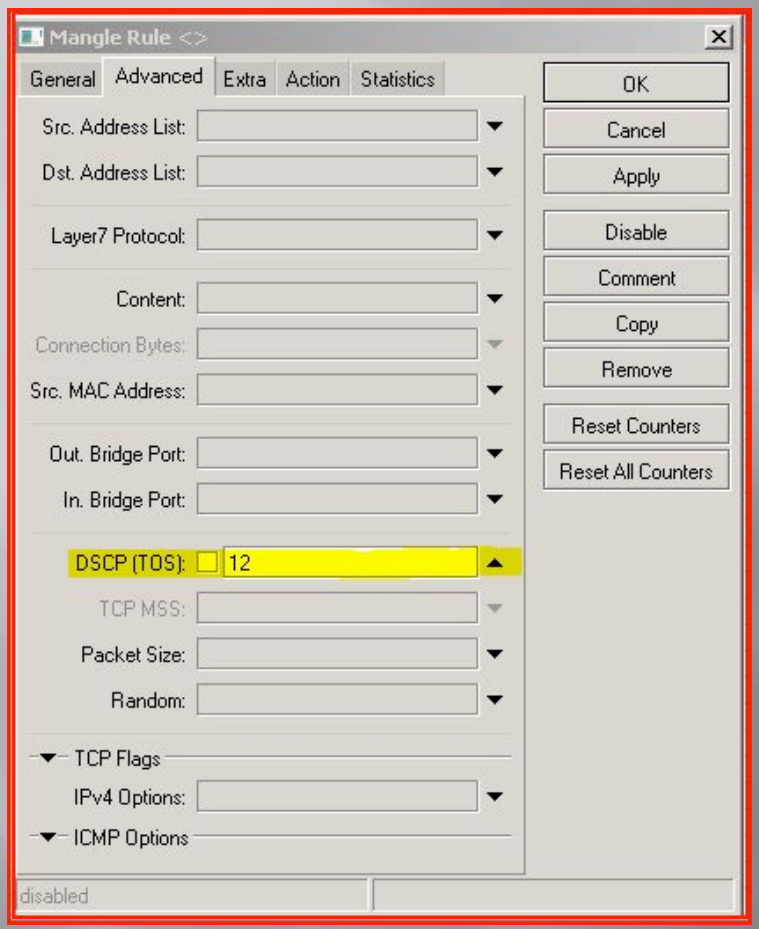
QoS between Cache and Client



- Client requests web page from internet via cache server. Cache HIT causes proxy fetch from disk
- QoS shapes all traffic flows including the cache server's response to client. Bandwidth is saved for Cache HITS, but overall client experience is limited by the QoS policies in place.
- We need to find a way to classify client side traffic based on whether the response from the cache is a HIT (contents fetched from objects saved on the cache disk) or a MISS (contents fetched from web server on the Internet) and pass this information to the Bandwidth Manager.
- The Bandwidth Manager can then allow client access HITS from the Cache without penalty based on such classifications.

The Zero Penalty Hit Solutions

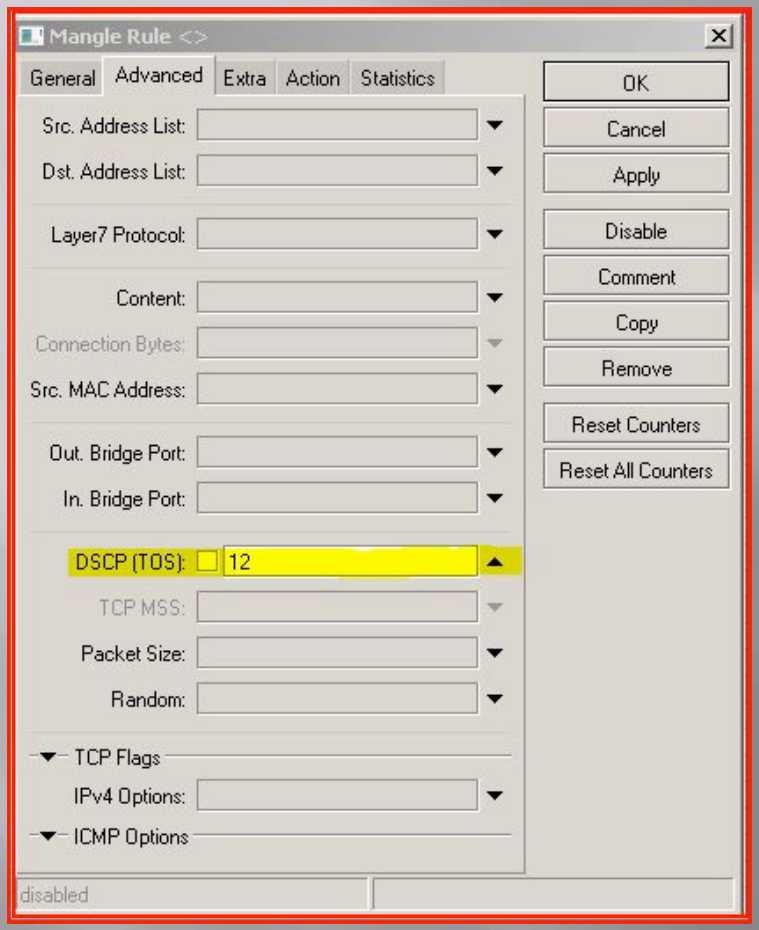
Mikrotik RouterOS v3



- Only very few Web Caches can classify client side traffic based on a HIT or MISS.
- Mikrotik Proxy in RouterOS v3 supports DSCP (TOS) Cache HITS marking option, which can be later used in mangle.
- Mikrotik mangle can be used to match HITS based on the chosen DSCP (TOS) value and mark the packets for use in either queue trees or simple queues

The Zero Penalty Hit Solutions

Mikrotik RouterOS v3



Visit the wiki to know more on deploying this exciting RouterOS V3 feature at http://wiki.mikrotik.com/wiki/Queue_with_Masquerading_and_Internal_Web-Proxy

The Zero Penalty Hit Solutions

Squid 2.6 with ZPH patch

- The second solution is Marin Stavrev's patch for squid – http://zph.bratcheda.org

- If you follow Marin's instructions with some common sense, you should be able to get your squid up and running with some new ZPH directives added to squid's configuration. I have used this patch on squid-2.6-SATBLE16.

- I will provide tips on how to make squid 2.6 patched with Marin's ZPH TOS work with Mikrotik RouterOS 2.9 and 3.x.

- I will also provide tips to make this work in a Mikrotik hotspot server, with dynamic simple queues.

```
zph_tos_local
zph_tos_peer
zph_tos_parent
zph_preserve_miss_tos
zph_preserve_miss_tos_mask
```

Things you must know

Squid 2.6 with ZPH patch

TOS Byte							
P2	P1	P0	T2	T1	T0	CU	CU

- IP precedence—three bits (P2 to P0)
- Delay, Throughput and Reliability—three bits (T2 to T0)
- CU (Currently Unused)—two bits(CU1–CU0)

DiffServ Field							
DS	DS	DS	DS	DS	DS	EC	EC

- DSCP – six bits (DS5–DS0)
- ECN – two bits

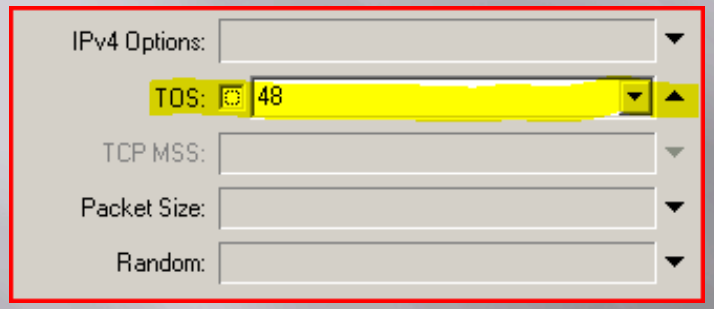
- **TOS - Type of Service is** 8 bits in the IP packet header. It may be utilized by networks to define the handling of the datagram during transport.

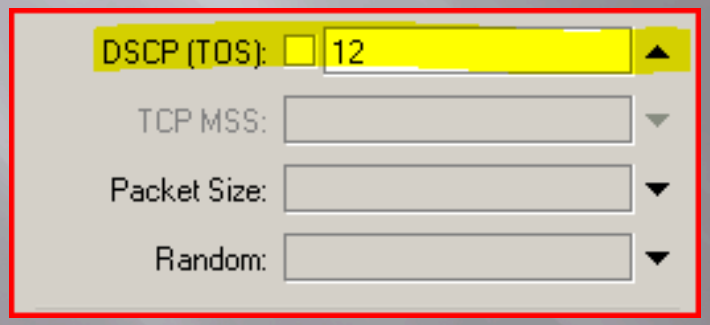
- DSCP - **Differentiated Services Code Point** is the most significant 6 bits of the 8 bit TOS header. Differentiated Services (DiffServ) is a new model which supersedes the original specification for defining packet priority described in RFC791. DiffServ increases the number of definable priority levels by reallocating bits of an IP packet for priority marking. See RFC 2474 and RFC 2475.

Things you must know

Squid 2.6 with ZPH patch

```
zph_tos_local 0x30
```





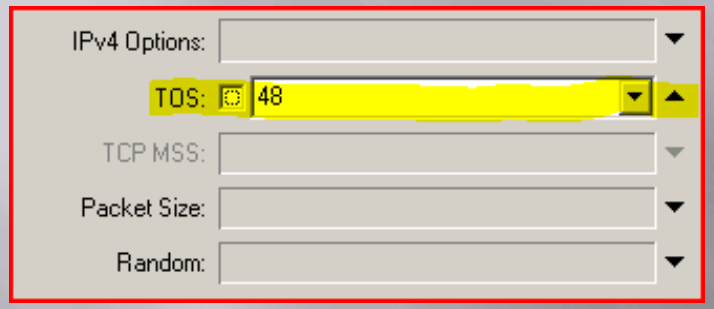
- The ZPH directives added to squid.conf by the latest ZPH squid patch (squid-2.6.STABLE2-ToS_Hit_ToS_Preserve.patch as of writing) accepts TOS values only in hexadecimal (hex).
- Mikrotik RouterOS v2.9.x accepts TOS values only in decimal (dec)
- Mikrotik RouterOS v3.x adopts the new DSCP model and accepts values only in decimal (dec)

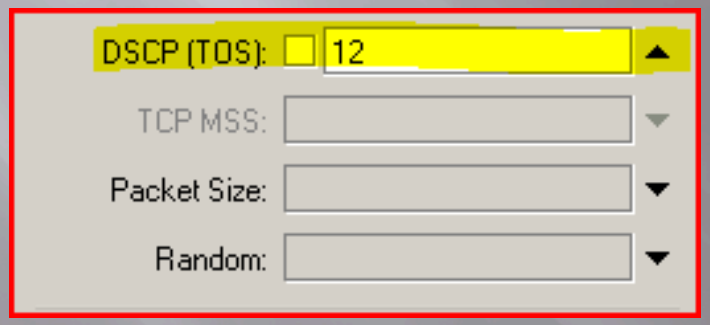
Things you must know

Squid 2.6 with ZPH patch

zph_tos_local 0x30

TOS 0x30 (hex) = TOS 48 (dec)





- When using an external ZPH Squid with RouterOS v2.6.x bandwidth manager, squid.conf file will have hex TOS while RouterOS mangle will have dec TOS value.

- When using an external ZPH Squid with RouterOS v3.x bandwidth manager, squid.conf file will have HEX TOS and you must make two step conversions for RouterOS v3.x.

1. First Convert hex TOS to hex DSCP value
2. Then convert this hex DSCP to dec DSCP for use in RouterOS v3.x mangle

TOS 0x30 (hex) = TOS 00110000 (bin)

TOS 00110000 (bin) = DSCP 001100 (bin)

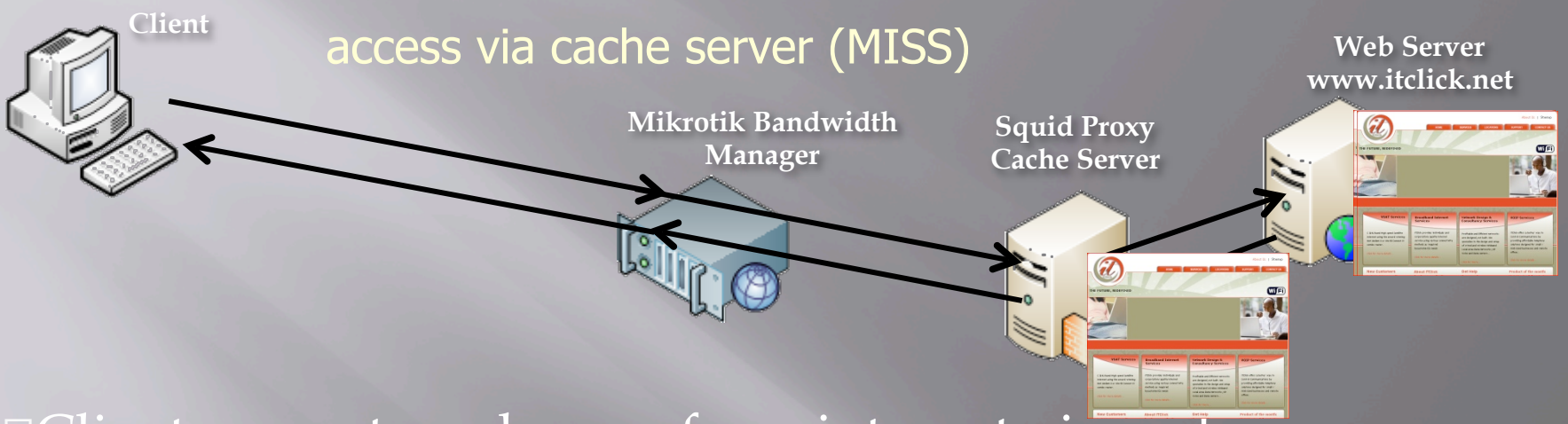
DSCP 001100 (bin) = C (hex) = DSCP 12 (dec)

TOS 0x30 (hex) = DSCP 12 (dec)

PUTTING IT TOGETHER

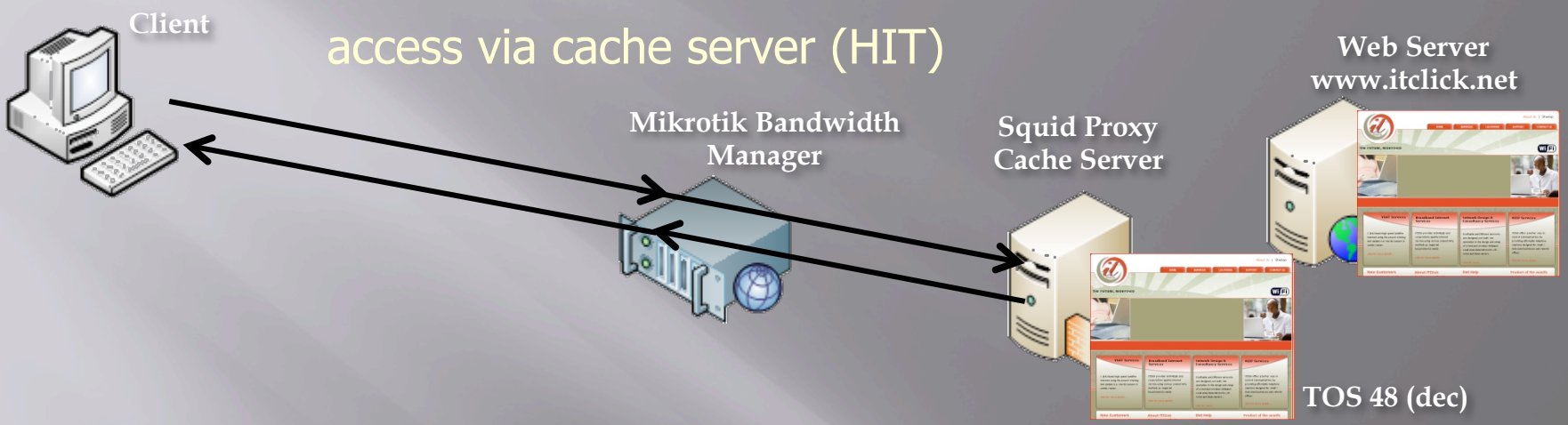
Squid Zero Penalty Caching with RouterOS QoS Management

Mikrotik, Squid Cache and Client



- Client requests web page from internet via cache server.
- Cache MISS causes proxy fetch from Web Server on the Internet.
- Because response is a cache MISS, IP TOS header is not classified. Mikrotik QoS shapes the traffic flow in accordance to the limit set for client. Client CANNOT get fresh internet object beyond set limit.

Mikrotik, Squid Cache and Client

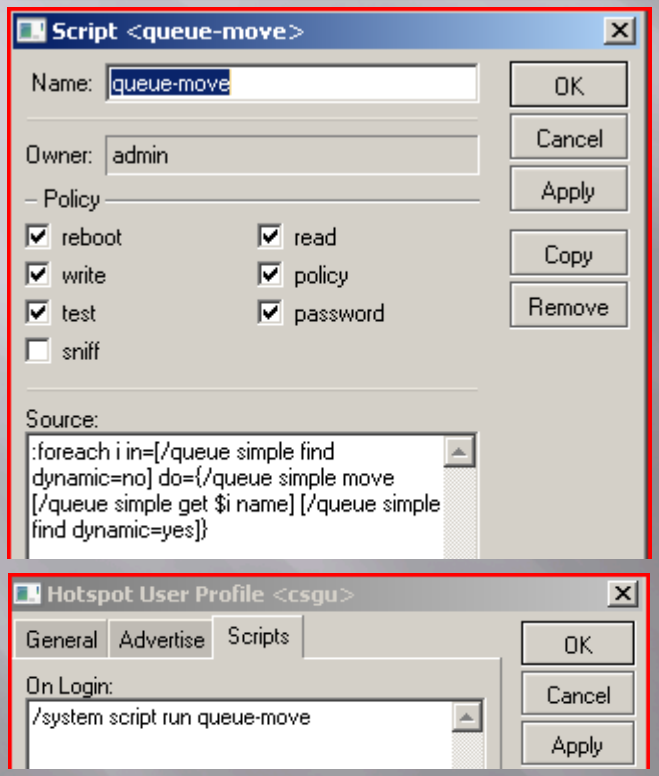


- Client requests web page from internet via cache server.
- Cache HIT causes proxy fetch from disk.
- Because response is a cache HIT, IP TOS header is modified to 0x30h (48 dec) by the Cache Server.
- Mikrotik mangle matches TOS 48 (dec) [v2.9.x] or DSCP 12 (dec) [v3.x], then marks this flow which is then bypassed by the queues and not shaped or penalized.
- Client gets the web page at maximum speed possible.

Mikrotik, Squid Cache and Client

Hotspot Dynamic simple Queue workaround

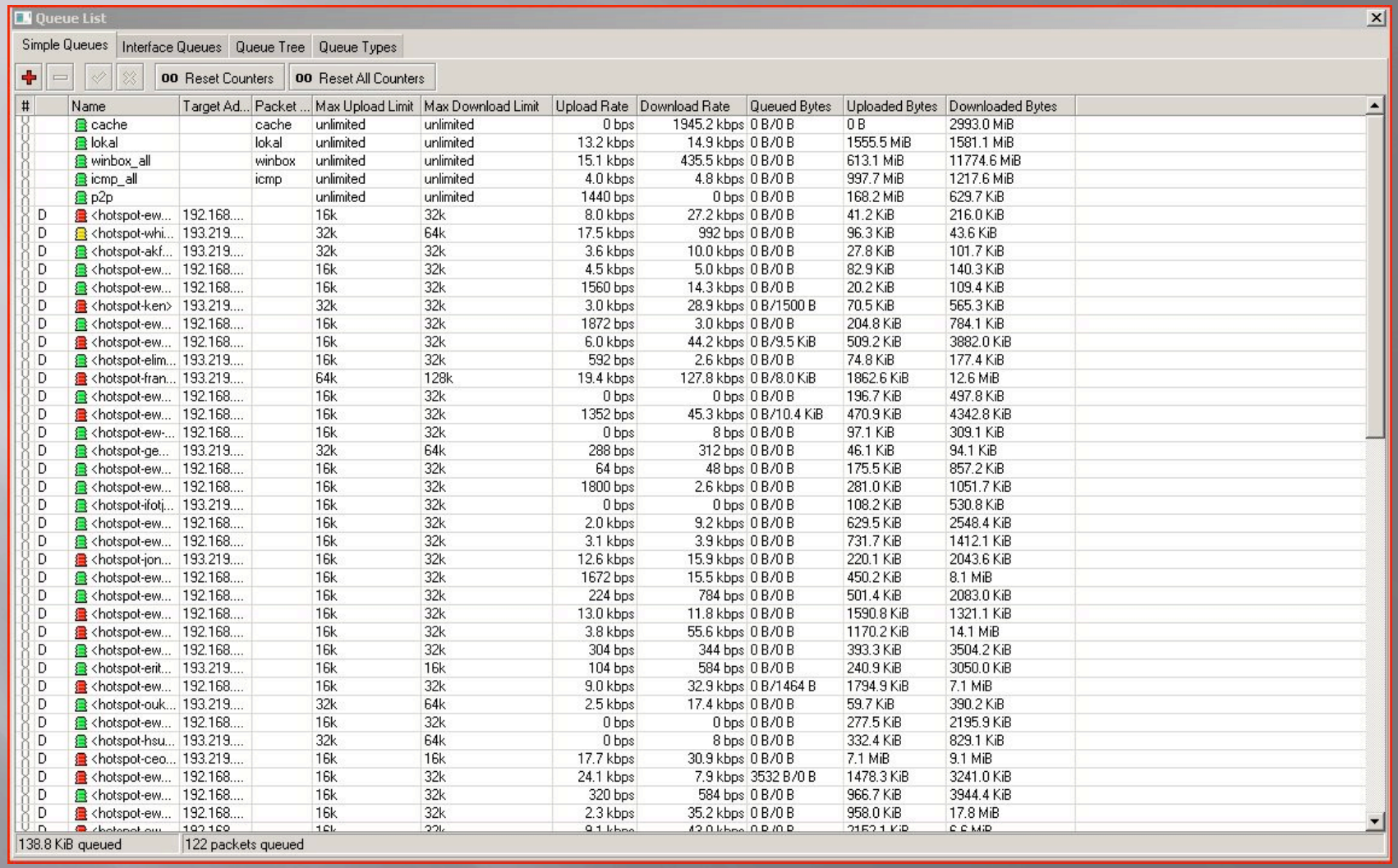
```
:foreach i in=[/queue simple find dynamic=no] do={/queue simple move [/queue simple get $i name] [/queue simple find dynamic=yes]}
```



- Mikrotik Simple queues are processed in order. Unlimited queue for cache hits must stay above all other queues
- Simple queues are dynamically assigned by radius or hotspot user profiles in a hotspot environment.
- Dynamic queues always stays above static queues
- Work around is to use scripts option in hotspot profile to automatically move static queues above dynamic queues on every login

Mikrotik, Squid Cache and Client

Hotspot Dynamic simple Queue workaround

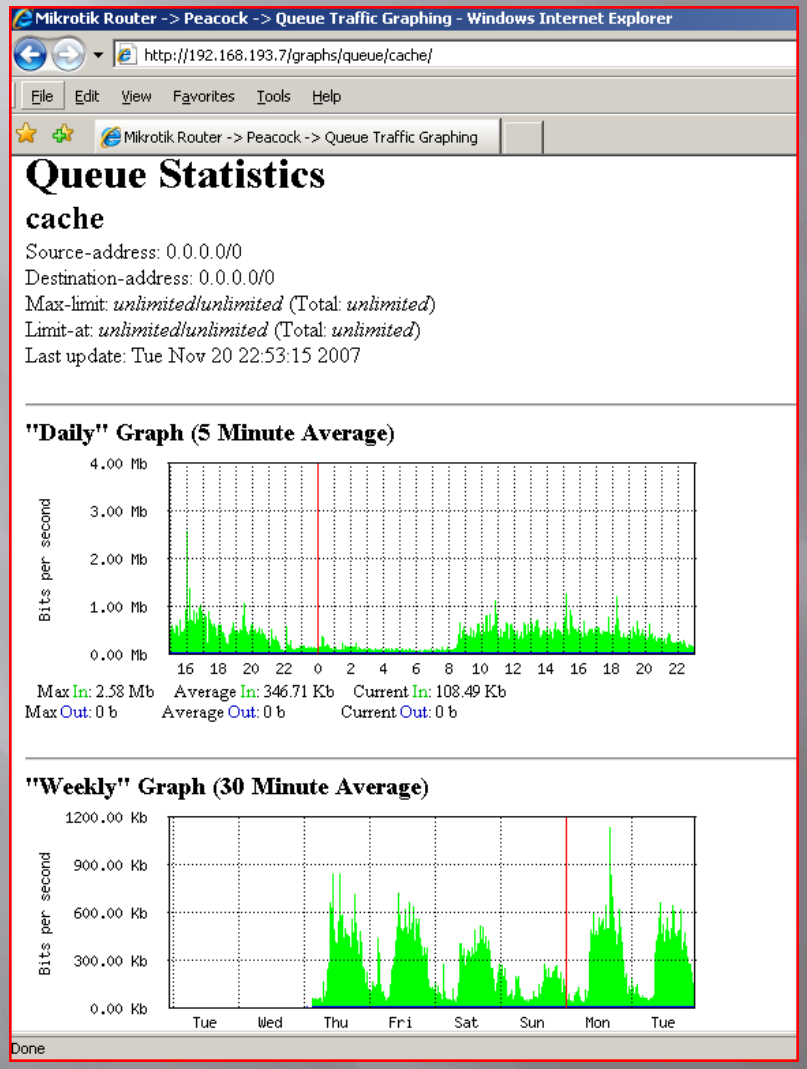


#		Name	Target Ad...	Packet ...	Max Upload Limit	Max Download Limit	Upload Rate	Download Rate	Queued Bytes	Uploaded Bytes	Downloaded Bytes
		cache		cache	unlimited	unlimited	0 bps	1945.2 kbps	0 B/0 B	0 B	2993.0 MiB
		lokal		lokal	unlimited	unlimited	13.2 kbps	14.9 kbps	0 B/0 B	1555.5 MiB	1581.1 MiB
		winbox_all		winbox	unlimited	unlimited	15.1 kbps	435.5 kbps	0 B/0 B	613.1 MiB	11774.6 MiB
		icmp_all		icmp	unlimited	unlimited	4.0 kbps	4.8 kbps	0 B/0 B	997.7 MiB	1217.6 MiB
		p2p			unlimited	unlimited	1440 bps	0 bps	0 B/0 B	168.2 MiB	629.7 KiB
	D	<hotspot-ew...	192.168....		16k	32k	8.0 kbps	27.2 kbps	0 B/0 B	41.2 KiB	216.0 KiB
	D	<hotspot-whi...	193.219....		32k	64k	17.5 kbps	992 bps	0 B/0 B	96.3 KiB	43.6 KiB
	D	<hotspot-akf...	193.219....		32k	32k	3.6 kbps	10.0 kbps	0 B/0 B	27.8 KiB	101.7 KiB
	D	<hotspot-ew...	192.168....		16k	32k	4.5 kbps	5.0 kbps	0 B/0 B	82.9 KiB	140.3 KiB
	D	<hotspot-ew...	192.168....		16k	32k	1560 bps	14.3 kbps	0 B/0 B	20.2 KiB	109.4 KiB
	D	<hotspot-ken>	193.219....		32k	32k	3.0 kbps	28.9 kbps	0 B/1500 B	70.5 KiB	565.3 KiB
	D	<hotspot-ew...	192.168....		16k	32k	1872 bps	3.0 kbps	0 B/0 B	204.8 KiB	784.1 KiB
	D	<hotspot-ew...	192.168....		16k	32k	6.0 kbps	44.2 kbps	0 B/9.5 KiB	509.2 KiB	3882.0 KiB
	D	<hotspot-elim...	193.219....		16k	32k	592 bps	2.6 kbps	0 B/0 B	74.8 KiB	177.4 KiB
	D	<hotspot-fran...	193.219....		64k	128k	19.4 kbps	127.8 kbps	0 B/8.0 KiB	1862.6 KiB	12.6 MiB
	D	<hotspot-ew...	192.168....		16k	32k	0 bps	0 bps	0 B/0 B	196.7 KiB	497.8 KiB
	D	<hotspot-ew...	192.168....		16k	32k	1352 bps	45.3 kbps	0 B/10.4 KiB	470.9 KiB	4342.8 KiB
	D	<hotspot-ew-...	192.168....		16k	32k	0 bps	8 bps	0 B/0 B	97.1 KiB	309.1 KiB
	D	<hotspot-ge...	193.219....		32k	64k	288 bps	312 bps	0 B/0 B	46.1 KiB	94.1 KiB
	D	<hotspot-ew...	192.168....		16k	32k	64 bps	48 bps	0 B/0 B	175.5 KiB	857.2 KiB
	D	<hotspot-ew...	192.168....		16k	32k	1800 bps	2.6 kbps	0 B/0 B	281.0 KiB	1051.7 KiB
	D	<hotspot-ifotj...	193.219....		16k	32k	0 bps	0 bps	0 B/0 B	108.2 KiB	530.8 KiB
	D	<hotspot-ew...	192.168....		16k	32k	2.0 kbps	9.2 kbps	0 B/0 B	629.5 KiB	2548.4 KiB
	D	<hotspot-ew...	192.168....		16k	32k	3.1 kbps	3.9 kbps	0 B/0 B	731.7 KiB	1412.1 KiB
	D	<hotspot-jon...	193.219....		16k	32k	12.6 kbps	15.9 kbps	0 B/0 B	220.1 KiB	2043.6 KiB
	D	<hotspot-ew...	192.168....		16k	32k	1672 bps	15.5 kbps	0 B/0 B	450.2 KiB	8.1 MiB
	D	<hotspot-ew...	192.168....		16k	32k	224 bps	784 bps	0 B/0 B	501.4 KiB	2083.0 KiB
	D	<hotspot-ew...	192.168....		16k	32k	13.0 kbps	11.8 kbps	0 B/0 B	1590.8 KiB	1321.1 KiB
	D	<hotspot-ew...	192.168....		16k	32k	3.8 kbps	55.6 kbps	0 B/0 B	1170.2 KiB	14.1 MiB
	D	<hotspot-ew...	192.168....		16k	32k	304 bps	344 bps	0 B/0 B	393.3 KiB	3504.2 KiB
	D	<hotspot-erit...	193.219....		16k	16k	104 bps	584 bps	0 B/0 B	240.9 KiB	3050.0 KiB
	D	<hotspot-ew...	192.168....		16k	32k	9.0 kbps	32.9 kbps	0 B/1464 B	1794.9 KiB	7.1 MiB
	D	<hotspot-ouk...	193.219....		32k	64k	2.5 kbps	17.4 kbps	0 B/0 B	59.7 KiB	390.2 KiB
	D	<hotspot-ew...	192.168....		16k	32k	0 bps	0 bps	0 B/0 B	277.5 KiB	2195.9 KiB
	D	<hotspot-hsu...	193.219....		32k	64k	0 bps	8 bps	0 B/0 B	332.4 KiB	829.1 KiB
	D	<hotspot-ceo...	193.219....		16k	16k	17.7 kbps	30.9 kbps	0 B/0 B	7.1 MiB	9.1 MiB
	D	<hotspot-ew...	192.168....		16k	32k	24.1 kbps	7.9 kbps	3532 B/0 B	1478.3 KiB	3241.0 KiB
	D	<hotspot-ew...	192.168....		16k	32k	320 bps	584 bps	0 B/0 B	966.7 KiB	3944.4 KiB
	D	<hotspot-ew...	192.168....		16k	32k	2.3 kbps	35.2 kbps	0 B/0 B	958.0 KiB	17.8 MiB

138.8 KiB queued | 122 packets queued

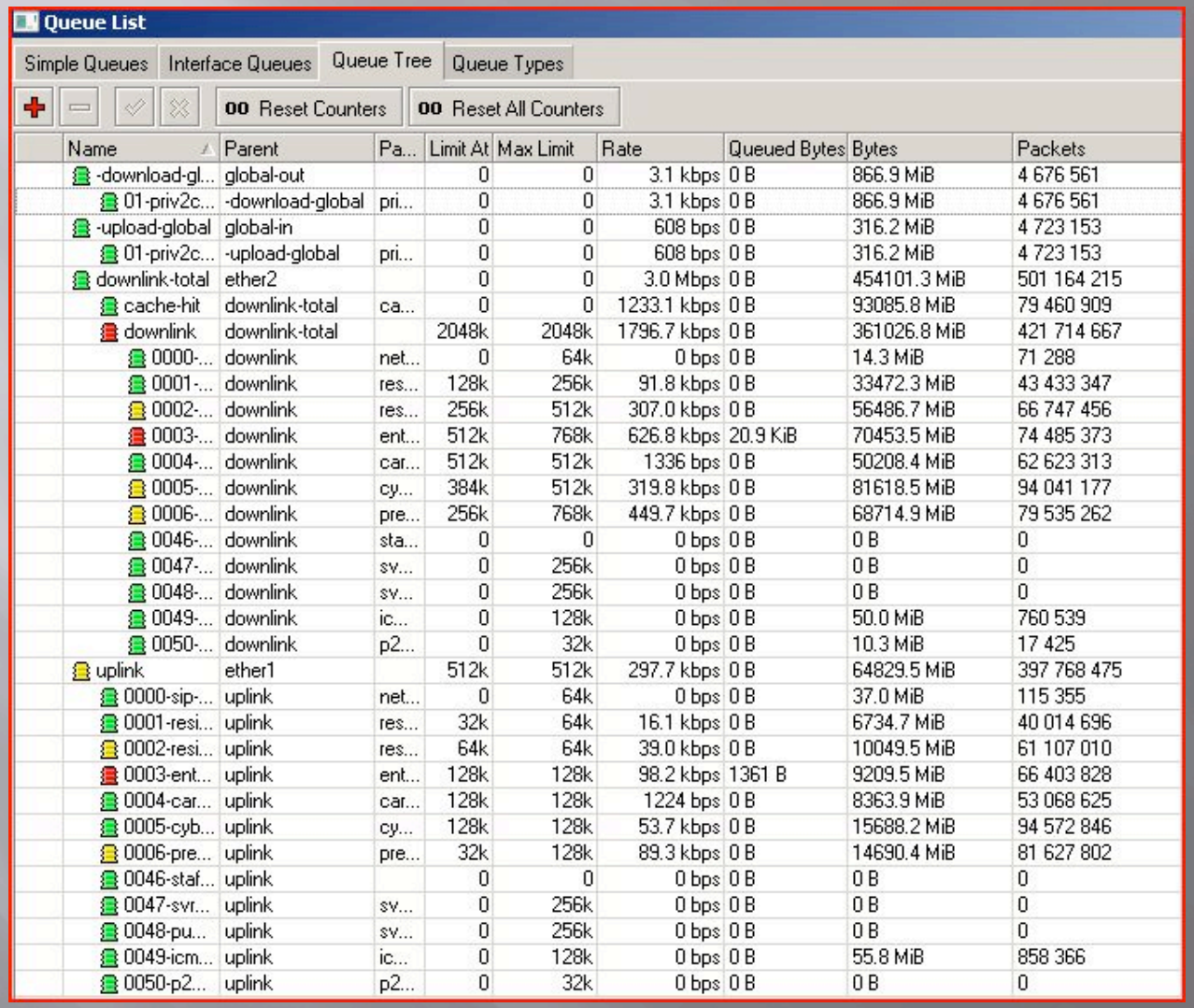
Mikrotik, Squid Cache and Client

Simple Queue graph



Mikrotik, Squid Cache and Client

Queue Trees



Name	Parent	Pa...	Limit At	Max Limit	Rate	Queued Bytes	Bytes	Packets
-download-gl...	global-out		0	0	3.1 kbps	0 B	866.9 MiB	4 676 561
01-priv2c...	-download-global	pri...	0	0	3.1 kbps	0 B	866.9 MiB	4 676 561
-upload-global	global-in		0	0	608 bps	0 B	316.2 MiB	4 723 153
01-priv2c...	-upload-global	pri...	0	0	608 bps	0 B	316.2 MiB	4 723 153
downlink-total	ether2		0	0	3.0 Mbps	0 B	454101.3 MiB	501 164 215
cache-hit	downlink-total	ca...	0	0	1233.1 kbps	0 B	93085.8 MiB	79 460 909
downlink	downlink-total		2048k	2048k	1796.7 kbps	0 B	361026.8 MiB	421 714 667
0000-...	downlink	net...	0	64k	0 bps	0 B	14.3 MiB	71 288
0001-...	downlink	res...	128k	256k	91.8 kbps	0 B	33472.3 MiB	43 433 347
0002-...	downlink	res...	256k	512k	307.0 kbps	0 B	56486.7 MiB	66 747 456
0003-...	downlink	ent...	512k	768k	626.8 kbps	20.9 KiB	70453.5 MiB	74 485 373
0004-...	downlink	car...	512k	512k	1336 bps	0 B	50208.4 MiB	62 623 313
0005-...	downlink	cy...	384k	512k	319.8 kbps	0 B	81618.5 MiB	94 041 177
0006-...	downlink	pre...	256k	768k	449.7 kbps	0 B	68714.9 MiB	79 535 262
0046-...	downlink	sta...	0	0	0 bps	0 B	0 B	0
0047-...	downlink	sv...	0	256k	0 bps	0 B	0 B	0
0048-...	downlink	sv...	0	256k	0 bps	0 B	0 B	0
0049-...	downlink	ic...	0	128k	0 bps	0 B	50.0 MiB	760 539
0050-...	downlink	p2...	0	32k	0 bps	0 B	10.3 MiB	17 425
uplink	ether1		512k	512k	297.7 kbps	0 B	64829.5 MiB	397 768 475
0000-sip-...	uplink	net...	0	64k	0 bps	0 B	37.0 MiB	115 355
0001-resi...	uplink	res...	32k	64k	16.1 kbps	0 B	6734.7 MiB	40 014 696
0002-resi...	uplink	res...	64k	64k	39.0 kbps	0 B	10049.5 MiB	61 107 010
0003-ent...	uplink	ent...	128k	128k	98.2 kbps	1361 B	9209.5 MiB	66 403 828
0004-car...	uplink	car...	128k	128k	1224 bps	0 B	8363.9 MiB	53 068 625
0005-cyb...	uplink	cy...	128k	128k	53.7 kbps	0 B	15688.2 MiB	94 572 846
0006-pre...	uplink	pre...	32k	128k	89.3 kbps	0 B	14690.4 MiB	81 627 802
0046-staf...	uplink		0	0	0 bps	0 B	0 B	0
0047-svr...	uplink	sv...	0	256k	0 bps	0 B	0 B	0
0048-pu...	uplink	sv...	0	256k	0 bps	0 B	0 B	0
0049-icm...	uplink	ic...	0	128k	0 bps	0 B	55.8 MiB	858 366
0050-p2...	uplink	p2...	0	32k	0 bps	0 B	0 B	0

Feature Request

RouterOS v3 proxy

- Transparency with IP spoofing – For us in a country with so much fraud, there is need to be able to track abuse (credit card and scam) based on client's source IP address. Proxying replaces client's IP with Cache's own. NOT all web servers are configured to log x-forwarded-for headers, even when enabled. This is the main reason why we run a custom squid, with kernel level IP spoofing using the help of TPROXY patch from Balabit – http://www.balabit.com/support/community/products/tproxy

- Ability to specify cache refresh patterns for specific objects

- Some form of analysis and report generator for the logs

THANK YOU

?