

Connection load balancing with mikrotik [workshop]

Mikrotik User Meeting Jakarta, 13 october 2016

Achmad Mardiansyah

achmad@glcnetworks.com

GLC Networks, Indonesia

Agenda

- Introduction
- The basics: connection and routing
- Load Balancing (LB) techniques (PCC)
- Some issues and recommendations
- Q & A

What is GLC?

- Garda Lintas Cakrawala (www.glcnetworks.com)
- An Indonesian company
- Located in Bandung
- Areas: Training, IT Consulting
- Mikrotik Certified Training Partner
- Mikrotik Certified Consultant
- Mikrotik distributor

Trainer Introduction



- Name: Achmad Mardiansyah
- Base: bandung, Indonesia
- Linux user since '99
- Certified Trainer (MTCNA/RE/WE/UME/INE/TCE)
- Mikrotik Certified Consultant
- Work: Telco engineer, Sysadmin, PHP programmer, and Lecturer
- Personal website: <http://achmad.glcnetworks.com>
- More info: <http://au.linkedin.com/in/achmadmardiansyah>

About Telkom University



- Located in Bandung, Indonesia
- 7 Faculties, 27 schools
- Areas: Engineering, Communications, Computing, Business and management, Arts
- 650+ Academic staff, 400+ Administration staff, 20000+ students
- An exchange program
- Runs mikrotik academy program

Mikrotik academy @ TEL-U

- Started in 2013
- Embedded into schools curricula
- 100% hands-on
- Get MTCNA certification



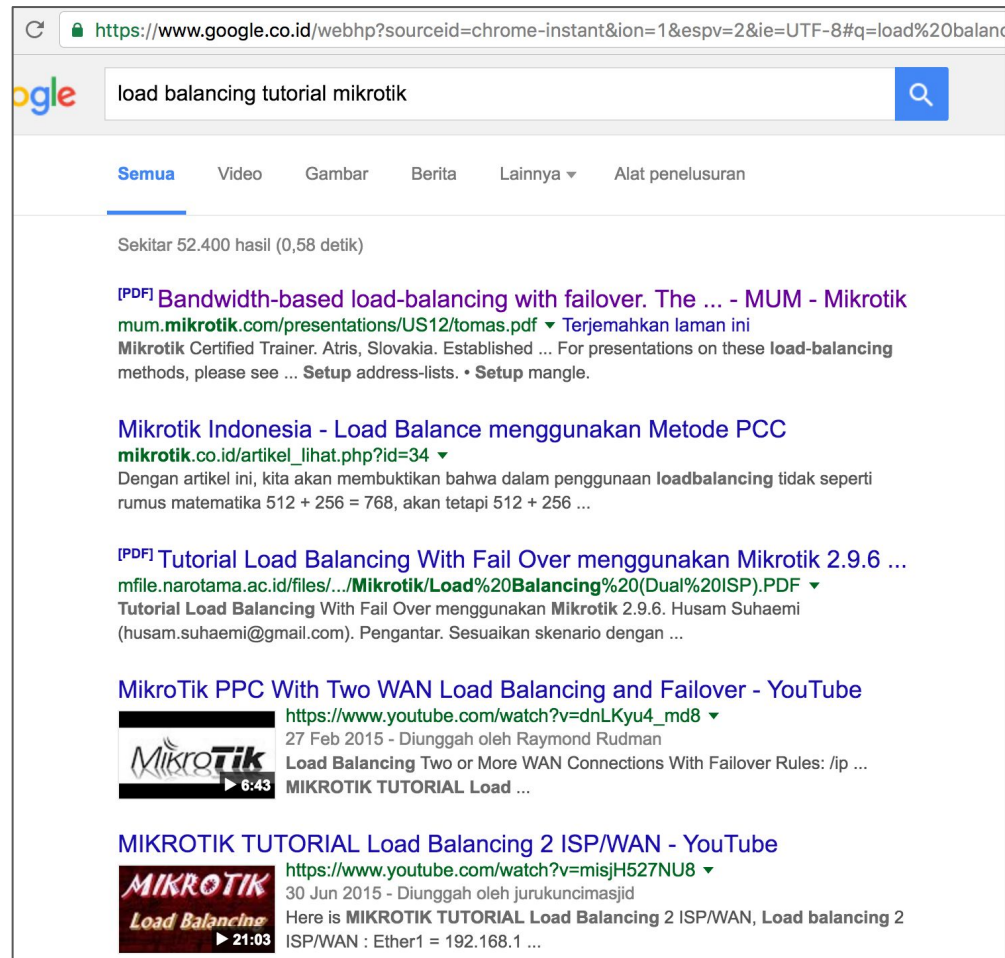
The basics: Connection and Routing

Why should i care?

- Lots of tutorials in internet!!!
- Tons of pages, tutorial, videos

Questions for reader:

- Do you really understand that?
- Did the writer understand that?
- Is it really works as expected?



Are those webpages really works on you?

- Information overloaded... which one suits you?
- Perhaps they have different environment on their network
- You need to understand how it works...

Subject: Configure PCC load balancing for multiple WAN on Mikrotik

Hi Achmad,

We have have two Upstream ISPs, and we want to apply load balancing on them. We followed tutorial from [https://\[redacted\]wordpress.com/2\[redacted\]mikrotik-dual-wan-load-b\[redacted\]](https://[redacted]wordpress.com/2[redacted]mikrotik-dual-wan-load-b[redacted]) but its not working well. We need this configured and fully working.

OTHER DETAILS

Client: [redacted]ISP)
Consultant: Achmad Mardiansyah
Estimated Budget: [redacted]

> 3. Saya mau coba Load Balance Ethernet+Bolt LTE ZTE MF90

> [http://mikrotik\[redacted\]?id=76](http://mikrotik[redacted]?id=76)

> [http://\[redacted\]isp-load-balancing-pcc-dengan-failover-tanpa-script](http://[redacted]isp-load-balancing-pcc-dengan-failover-tanpa-script)

> tapi belum berhasil

> Apa trainernya dah pernah coba

—
dulu pernah diimplementasikan disini:

<http://www.glcnetworks.com/main/maret-2014-optimasi-jaringan-pada-sebuah-kantor-di-jakarta/>

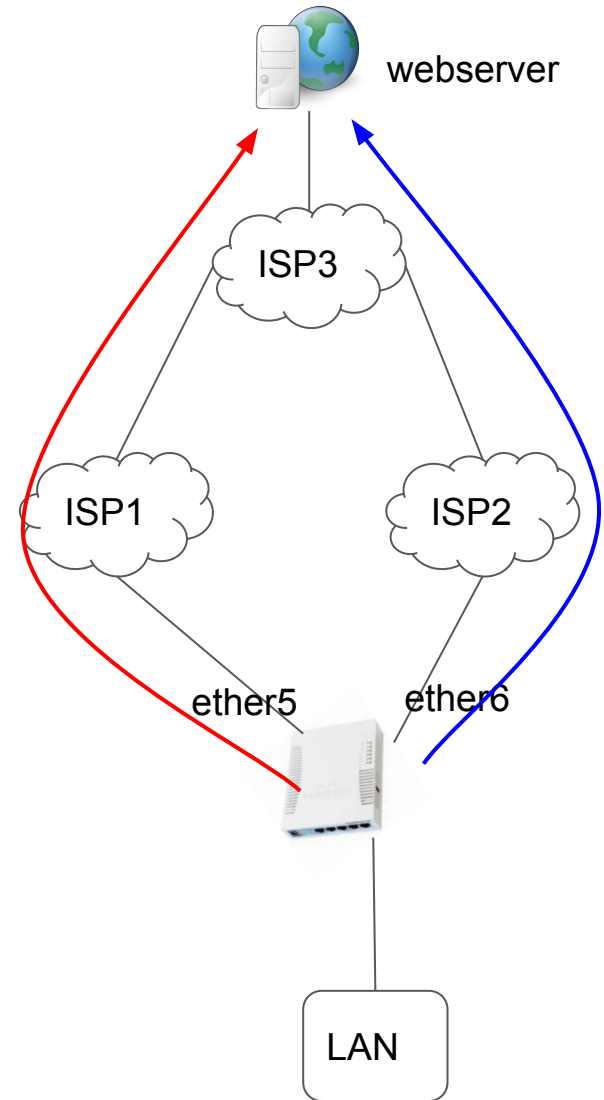
mudah2an membantu ya

What is (traffic) load balancing?

- Is a process to forward traffic on several links
- Applied on router
- != failover

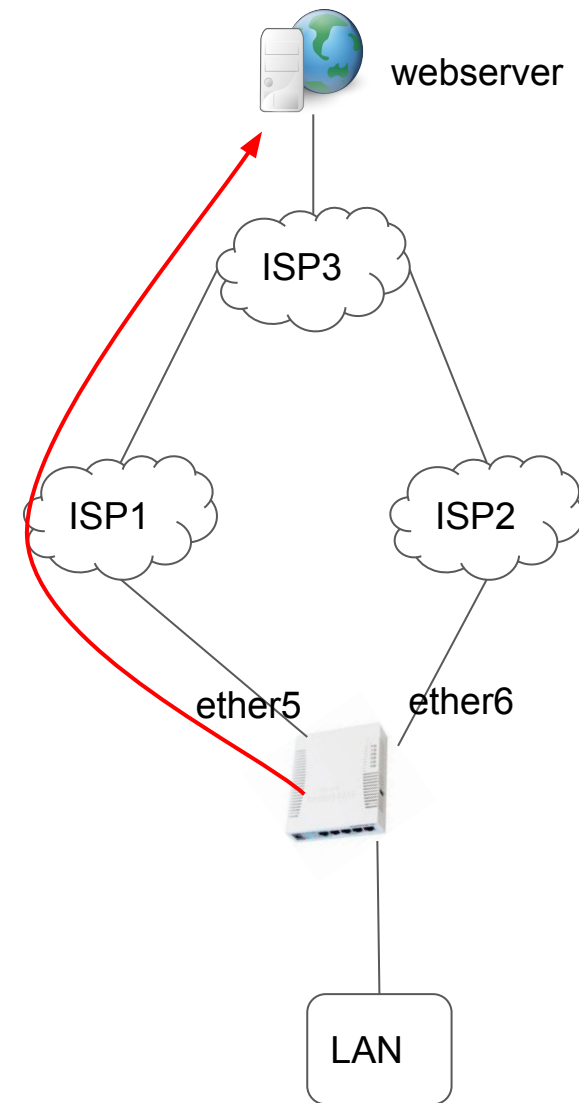
Benefits:

- Increase utilisation of upstream links



What is connection?

- When you access a server you will create a connection
- **Connection** is identified by a set of IP addresses (source and destination) and ports (source and destination)
- See connection tracking below



Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Tracking Find

	Src. Address	Dst. Address	Protocol	Connecti...	Timeout	TCP State	Or
C	192.168.2.1	224.0.0.1	2 (igmp)		00:08:25	0 t	+
SC	192.168.2.18:47248	8.8.8.8:53	17 (udp)		00:00:08	0 t	
C	192.168.98.99	192.168.98.2	47 (gre)		00:00:25	0 t	
C	192.168.98.99	192.168.98.4	47 (gre)		00:00:25	0 t	
C	192.168.98.99	192.168.98.3	47 (gre)		00:00:25	0 t	
C	192.168.98.99	192.168.98.1	47 (gre)		00:00:25	0 t	
C	192.168.98.99	224.0.0.9	2 (igmp)		00:08:32	0 t	
SACs	192.168.99.254:13765	157.56.52.27:40022	17 (udp)		00:00:07	0 t	
SACs	192.168.99.254:13765	157.55.130.149:40003	17 (udp)		00:01:33	0 t	
SACs	192.168.99.254:13765	157.55.235.145:40018	17 (udp)		00:02:24	0 t	
SACs	192.168.99.254:13765	157.55.130.175:40024	17 (udp)		00:02:24	0 t	
SACs	192.168.99.254:49155	17.188.157.40:5223	6 (tcp)		23:50:11	established 0 t	
SACs	192.168.99.254:49155	17.188.157.40:5223	6 (tcp)		23:50:36	established 0 t	

60 items Max Entries: 218040

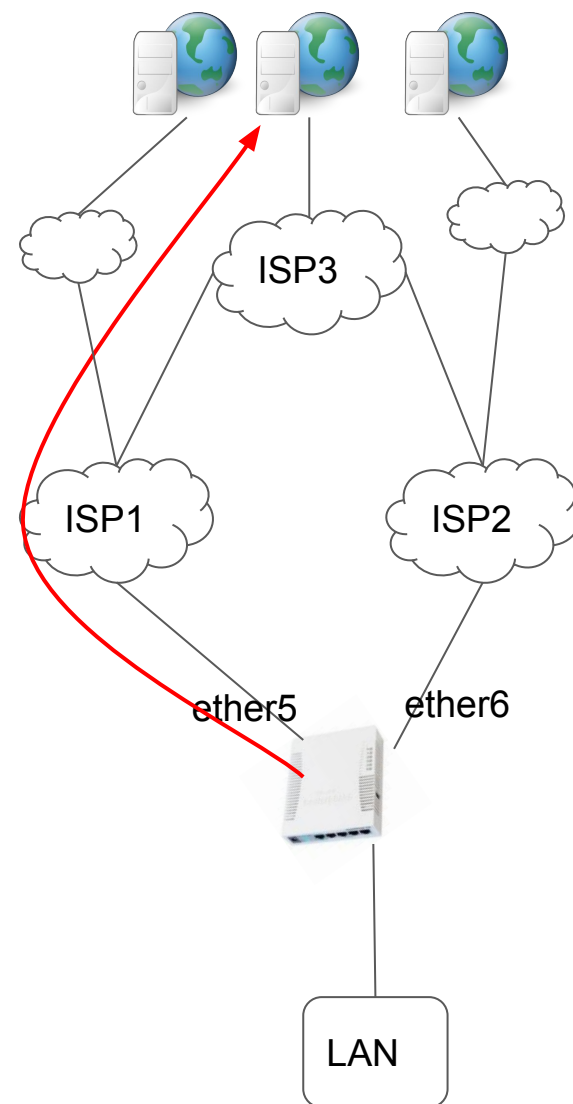
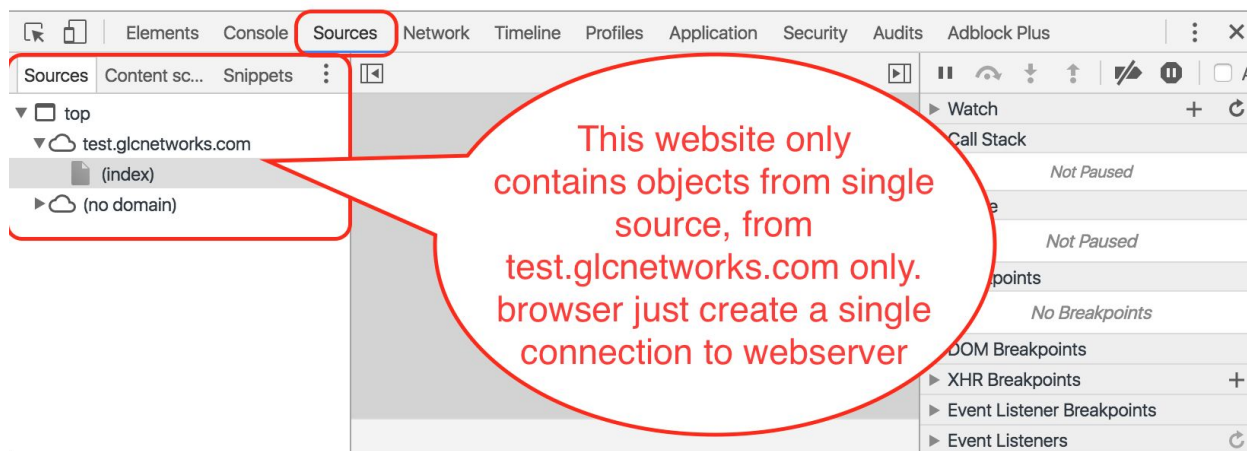
Single connection to a website

Website with single connection:

<http://test.glcnetworks.com>

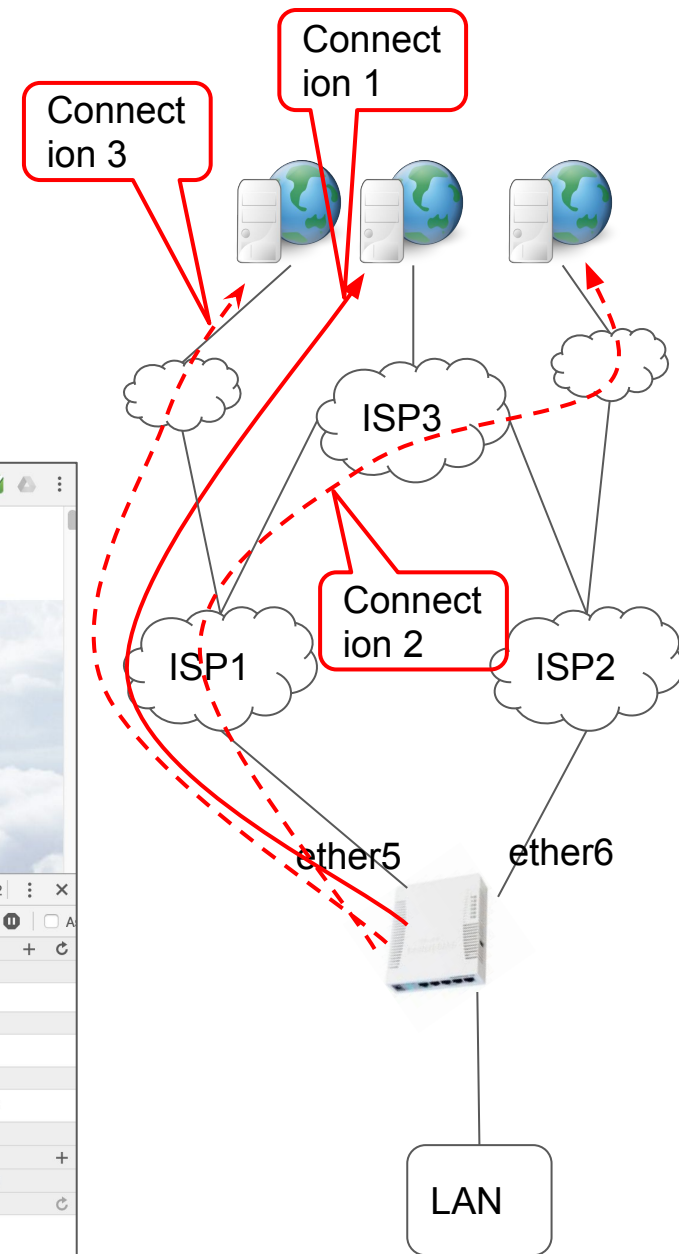
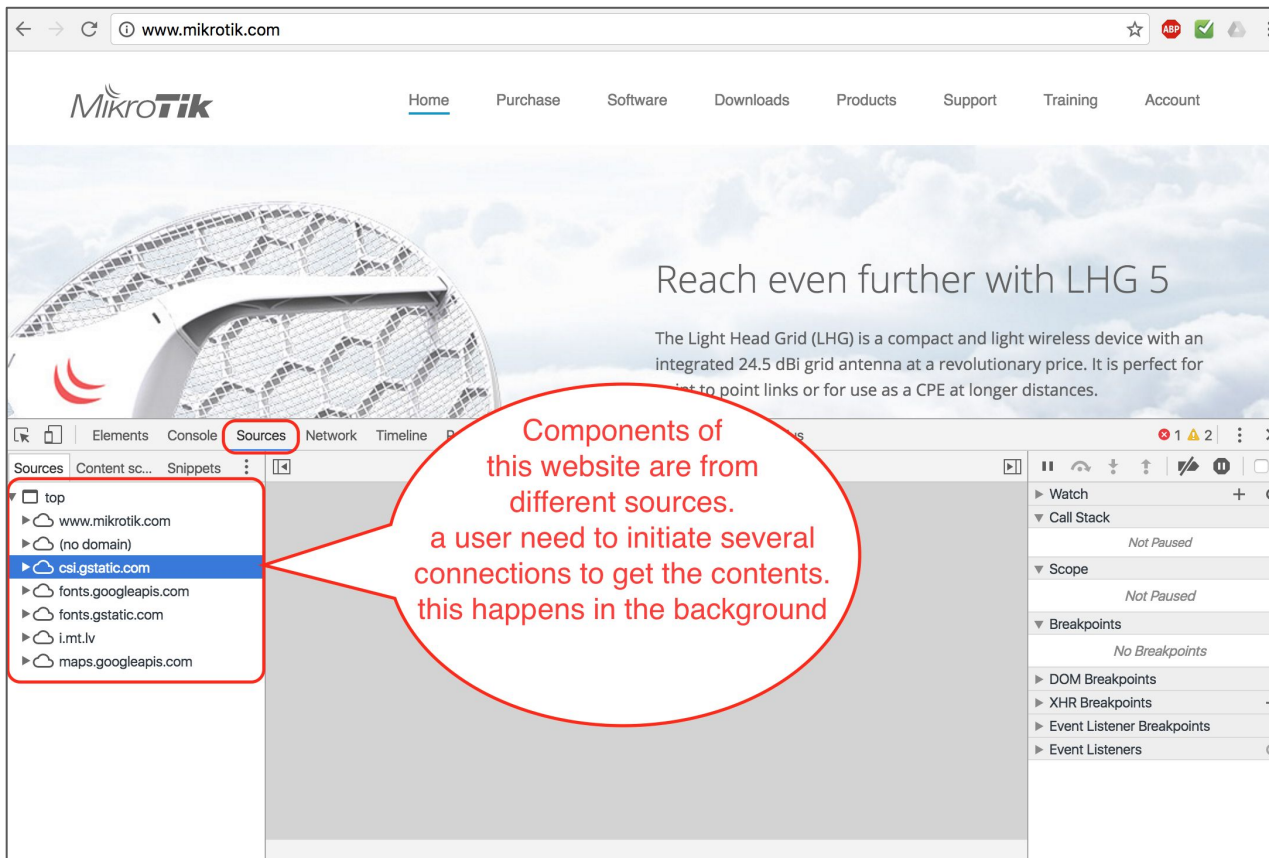


This is GLC test page
Your IP address is: 66.96.239.53



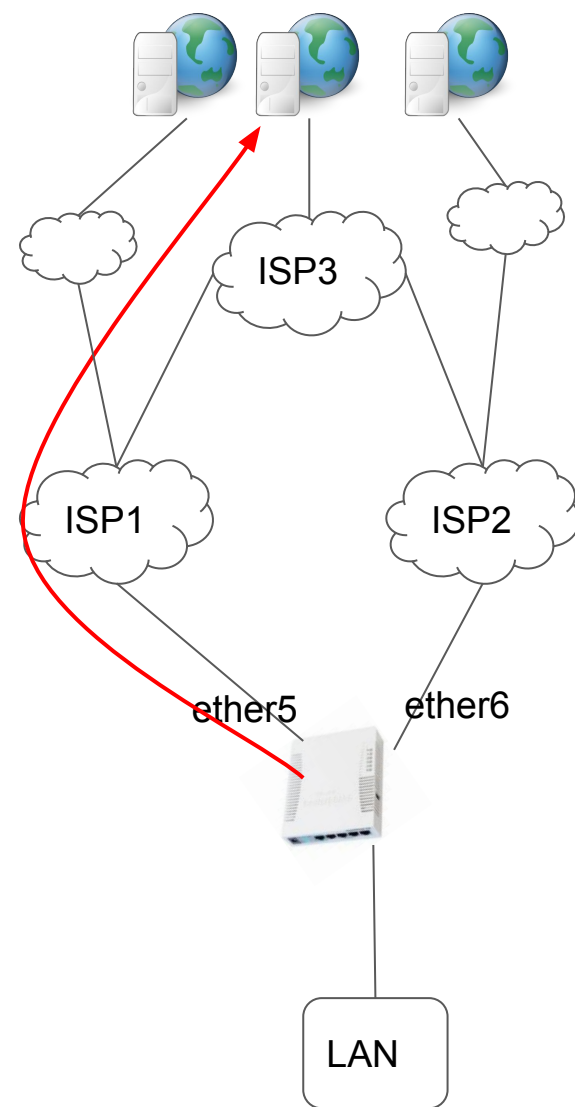
Website with multiple objects

- Client will open multiple connections to get website components



Routing and Forwarding

- A process to forward a packet from input interface to output interface, based on information on routing table.
- As we use private IP address, there will be a NAT process before sending out to exit interface
- To check our public IP address, go to <http://test.glcnetworks.com>



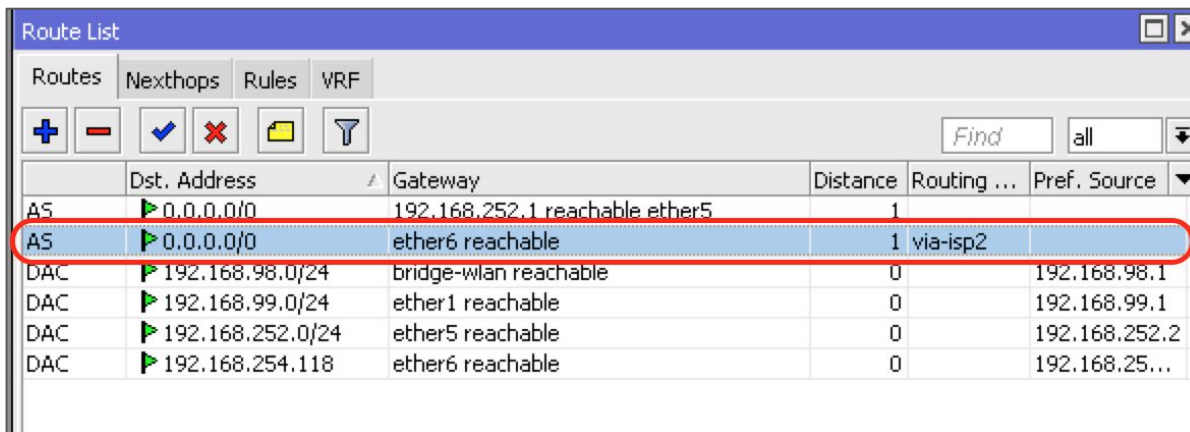
Route List

	Dst. Address	Gateway	Distance	Rou...	Pref. Source	OS
AS	0.0.0.0/0	192.168.252.1 reachable ether5	1			
DAC	192.168.99.0/24	ether1 reachable	0		192.168.99.1	
DAC	192.168.252.0/24	ether5 reachable	0		192.168.252.2	

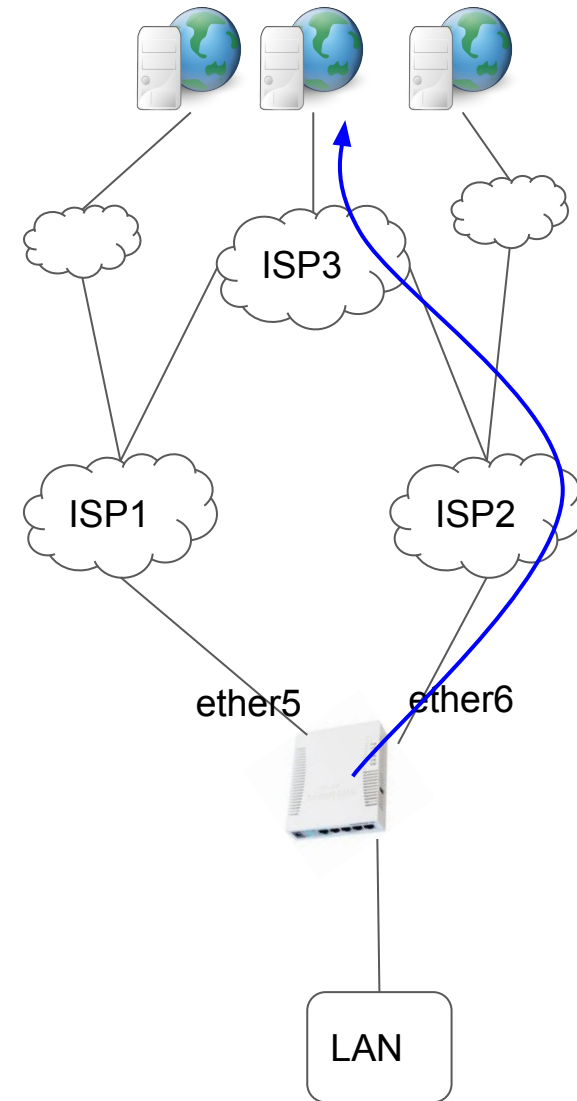
3 items

Adjust routing (mangle: mark-routing)

- Process to mark a packet to for routing purpose
- Steps:
 - Create firewall mangle with action mark-routing
 - Create routing entry with defined-mark
 - Create NAT rule if we use private IP address
- To check our public IP address, go to <http://test.glcnetworks.com>



	Dst. Address	Gateway	Distance	Routing ...	Pref. Source
AS	0.0.0.0/0	192.168.252.1 reachable ether5	1		
AS	0.0.0.0/0	ether6 reachable	1	via-isp2	
DAC	192.168.98.0/24	bridge-wlan reachable	0		192.168.98.1
DAC	192.168.99.0/24	ether1 reachable	0		192.168.99.1
DAC	192.168.252.0/24	ether5 reachable	0		192.168.252.2
DAC	192.168.254.118	ether6 reachable	0		192.168.25...



Forward traffic via ISP2 using mangle

The screenshot displays the Mikrotik WinBox interface for configuring network settings. The top section shows the Firewall configuration, with the 'Mangle' tab selected. A table lists the configured mangle rules, with rule 2 highlighted in red. Rule 2 is named 'mark routing', has an action of 'mark routing', and is applied to the 'prerouting' chain on the 'ether1' interface. The bottom section shows the Route List configuration, with the 'Routes' tab selected. A table lists the configured routes, with the route for '0.0.0.0/0' via 'ether6' highlighted in red. The 'Routing Mark' for this route is set to 'via-isp2'.

Firewall Configuration

#	Action	Chain	Src. A...	Dst. ...	Prot...	Sr...	D...	In. Interface
1	change MSS	forward			6 (tcp)			all ppp
0	change MSS	forward			6 (tcp)			
2	mark routing	prerouting						ether1

Route List Configuration

Routes	Nexthops	Rules	VRF
AS	0.0.0.0/0	192.168.252.1 reachable ether5	1
AS	0.0.0.0/0	ether6 reachable	1 via-isp2
DAC	192.168.98.0/24	bridge-wlan reachable	0
DAC	192.168.99.0/24	ether1 reachable	0
DAC	192.168.252.0/24	ether5 reachable	0
DAC	192.168.254.118	ether6 reachable	0

New Route Configuration

General	Attributes
Dst. Address: 0.0.0.0/0	Gateway: ether6
Check Gateway: ping	Type: unicast
Distance: 1	Scope: 30
Target Scope: 10	Routing Mark: via-isp2
Pref. Source:	

Forward traffic via ISP1 using mangle

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists

Filter Rules

#	Action	Chain	Src. A...	Dst. ...	Prot...	Sr...	D...
1	change MSS	forward			6 (tcp)		
0	change MSS	forward			6 (tcp)		
2	mark routing	prerouting					

Route List

Routes

	Dst. Address	Gateway	Distance
AS	0.0.0.0/0	192.168.252.1 reachable ether5	1
AS	0.0.0.0/0	ether6 reachable	1
AS	0.0.0.0/0	192.168.252.1 reachable ether5	1
DAC	192.168.98.0/24	bridge-wlan reachable	0
DAC	192.168.99.0/24	ether1 reachable	0
DAC	192.168.252.0/24	ether5 reachable	0
DAC	192.168.254.118	ether6 reachable	0

New Route

General

Dst. Address: 0.0.0.0/0

Gateway: 192.168.252.1

Check Gateway: ping

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark: via-isp1

Pref. Source:

OK Cancel Apply Disable Comment Copy Remove

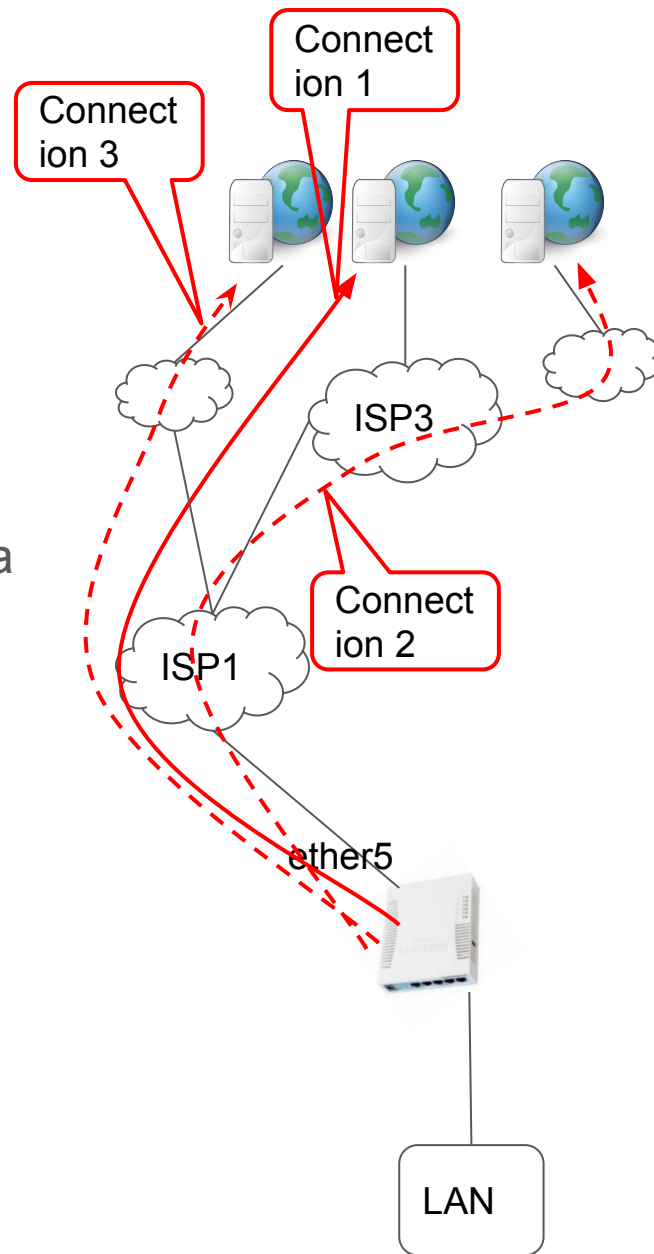
Load Balancing techniques

Load balancing techniques

Method	Per-connection	per-packet
Firewall marking	YES	YES
ECMP	YES	NO
PCC	YES	NO
Nth	YES	YES
Bonding	NO	YES
OSPF	YES	NO
BGP	YES	NO

How PCC works?

- PCC = Per Connection Classifier
- PCC can identify the connection and mark them for further processing
- Example: a client opens a multi-object website via single ISP. both addresses (src-address and dst-address) are used to identify connection
- PCC can identify each connection made from client



Applying PCC

- You need to understand the concept of connection
- Applied on firewall mangle
- Need to define classifier. Can be based on:
 - Source or destination address only
 - Both addresses
 - Etc
- Define connection number and total connection

Total
connection

Connection
identifier

Per Connection Classifier: ☐ src address : 1 / 0

Src. MAC Address: ☐ both addresses
both addresses and ports
both ports

Out. Bridge Port: ☐ dst address
dst address and port

In. Bridge Port: ☐ dst port
src address
src address and port

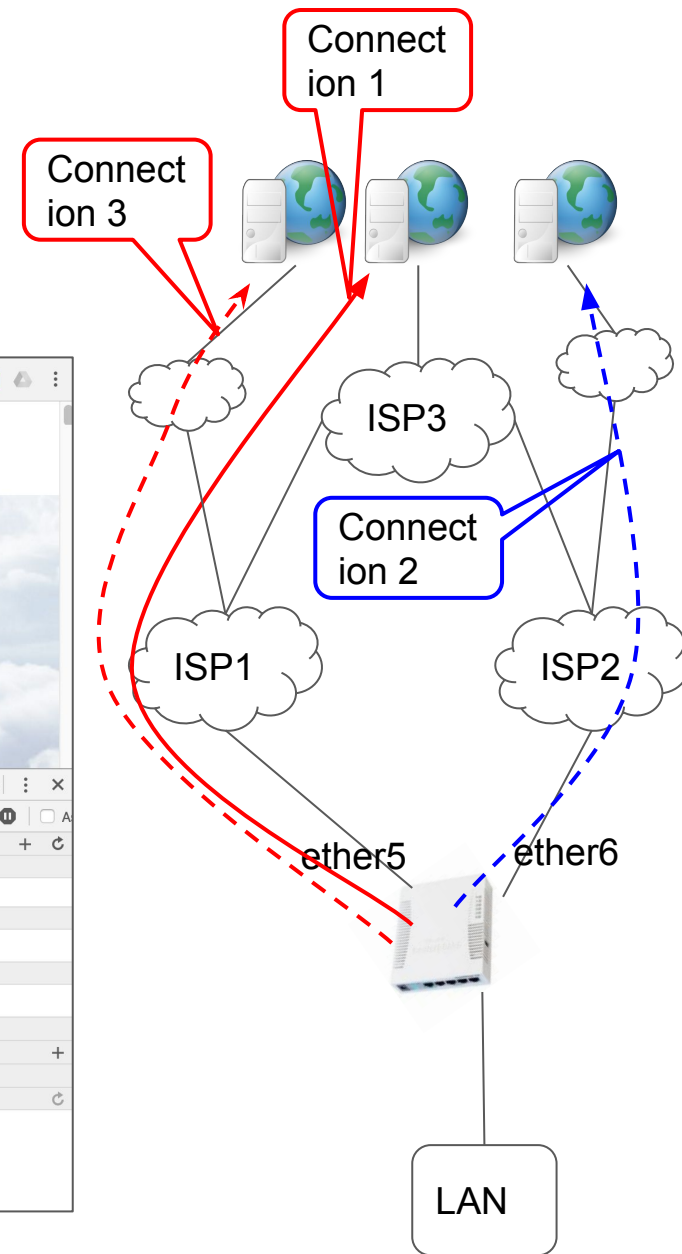
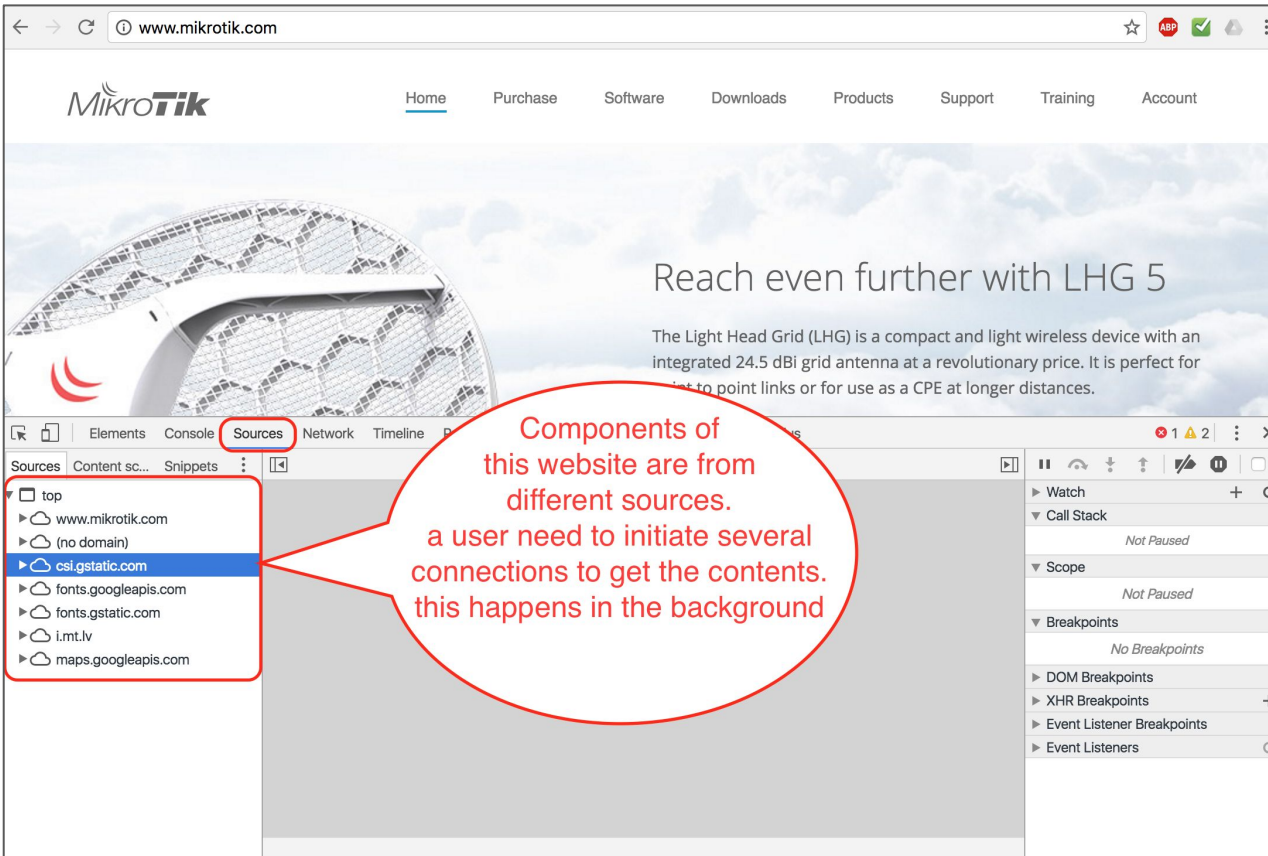
In. Bridge Port List: ☐ src port

Lets play with PCC classifier...

- Apply different classifier and check the result

Per Connection Classifier:	☐	src address	⌵	:	1	/	0	▲	
Src. MAC Address:	☐	both addresses both addresses and ports both ports							▼
Out. Bridge Port:	☐	dst address dst address and port							▼
In. Bridge Port:	☐	dst port src address src address and port							▼
In. Bridge Port List:	☐	src port							▼

Website with multiple objects, LB with classifier: both address



Some issues & recommendations

Some issues & recommendations

Issues:

- **Beware of NATed connection** -> webserver will see inbound connection from 2 ip public addresses -> page will not displayed correctly (as it is considered illegal session)
- **Beware of NATed connection** -> webserver will see inbound connection from 2 ip public addresses -> banking / https pages will not allow you to access their website

Recommendations

- **If you use NAT**, Better to use classifier based on **source IP address** only -> will give client consistent path to the destination
- **Avoid NAT if possible** -> using public IP address end-to-end -> use BGP -> better performance

QA

Some info

- Hope you are more curious now
- These materials are part of Mikrotik Certified Traffic Control Engineer (MTCTCE) course
- If you are interested, you can sign up to our website

www.glcnetworks.com/main/

GLC Networks Mikrotik, Ubiquity, Radius manager

Class Topology

Home Product Schedule Payment Gallery Jobs Contact Post

Home

Welcome to GLC Networks

Here's Our Upcomming Event!

Linux System Administration (RHCSA)

Bandung (3-6 October 2016)

Location: Jl. Batik Kumell No. 7 Bandung

Training Investment: General IDR 4 Juta Academic IDR 2 Juta

Don't Miss It !!

Include: Printed Module Lunch Certificate Access to GLC Cloud

Note: *Membawa laptop yang support with

for free

Come and Join GLCNetworks Webinar Event

Thursday 6th October 2016, Starts 19.00 Jakarta Time (GMT+7)

This Webinar will discuss about BGP on Mikrotik

Agenda:

1. Introduction
2. Topic Discussions**
3. Questions & Answers

**Note: You may request the discussion topic to admin

Info & Registration Pls Visit :

www.glcnetworks.com/main/schedule/

The Search Box

Search ... Search

Recent Posts

- September 2016, MTCNA training, Bandung
- September 2016, MTCNA training, Bandung
- September 2016, MTCUME training, Bandung
- September 2016, MTCNA + MTCRE training, Bandung
- September 2016, MTCWE training, Bandung

Recent Comments

www.glcnetworks.com

End of slides

- Thank you for your attention
- Please submit your feedback: <http://bit.ly/glcfeedback>
- Like our facebook page: “GLC networks”
- Stay tune with our schedule