

# Troubleshooting load balancing

Mikrotik User Meeting  
Malaysia, 12 june 2019

Achmad Mardiansyah  
[achmad@glcnetworks.com](mailto:achmad@glcnetworks.com)  
GLC Networks



# Agenda

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

# What is GLC?

- Garda Lintas Cakrawala ([www.glcnetworks.com](http://www.glcnetworks.com))
- Based in Bandung, Indonesia
- Areas: Training, IT Consulting
- Certified partner for: Mikrotik, Ubiquity, Linux foundation
- Product: GLC radius manager
- Regular event: webinar (every 2 weeks, see our schedule on website)



# About me



- Name: Achmad Mardiansyah
- Base: bandung, Indonesia
- Linux user since 1999, mikrotik user since 2007,
- Mikrotik Certified Trainer  
(MTCNA/RE/WE/UME/INE/TCE/IPv6)
- Mikrotik Certified Consultant
- Teacher at Telkom University (Bandung, Indonesia)
- Website contributor: [achmadjournal.com](http://achmadjournal.com),  
[mikrotik.tips](http://mikrotik.tips), [asysadmin.tips](http://asysadmin.tips)
- More info:  
<http://au.linkedin.com/in/achmadmardiansyah>



# Past experiences



- 2019, **Congo (DRC)**: build a wireless ISP from ground-up
- 2018, **Malaysia**: network revamp, develop billing solution and integration, setup dynamic routing
- 2017, **Libya (north africa)**: remote wireless migration for a new Wireless ISP
- 2016, **United Kingdom**: facilitates workshop for a wireless ISP, migrating a bridged to routed network
- 2015, **West Borneo**: supporting wireless infrastructure project
- 2014, **Senegal (west africa)**: TAC2 engineer for HLR migration from NOKIA to ERICSSON



# About Telkom University



- Located in Bandung, Indonesia
- 7 Faculties, 27 schools
- Areas: Engineering, Communications, Computing, Bussiness 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 curriculum
- 100% hands-on
- Get MTCNA certification



# About load balancing

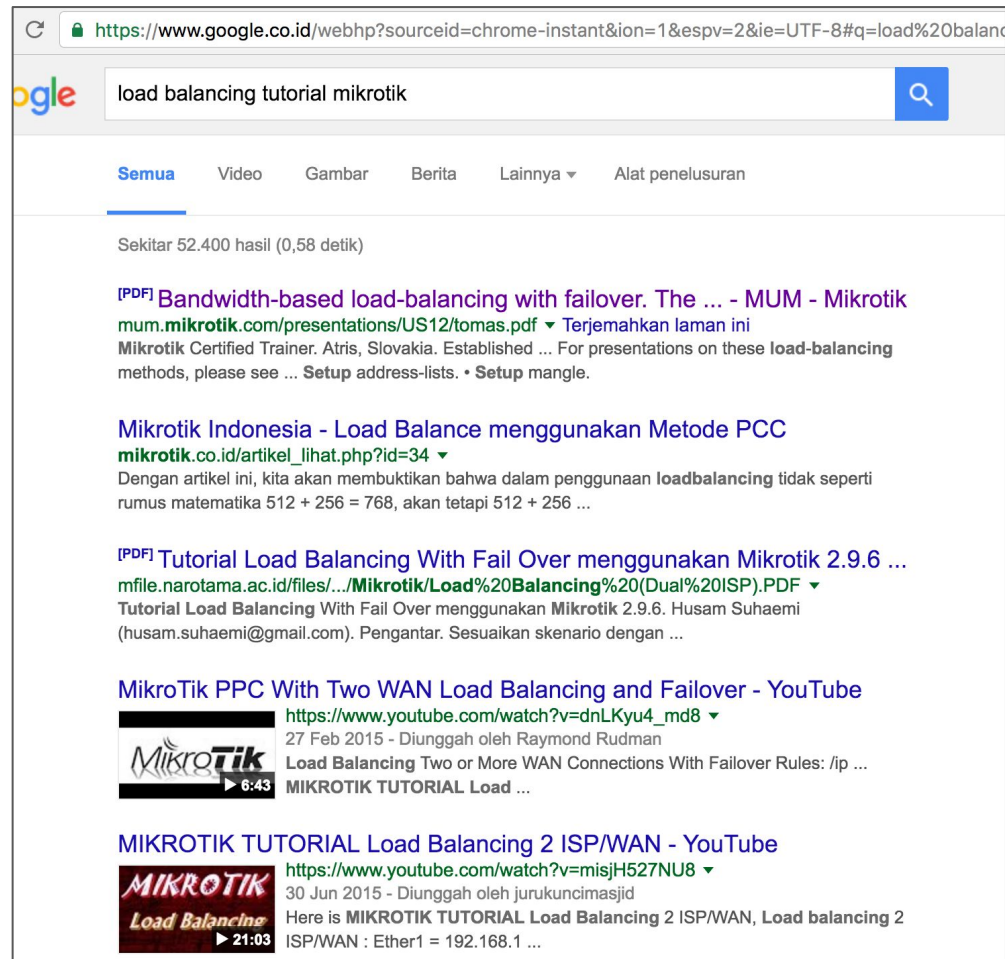


# Why should i care?

- 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 work on you?

- Information overloaded... which one suits you?
- Perhaps their network environment is different than yours
- 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/\[redacted\]mikrotik-dual-wan-load-b](https://[redacted]wordpress.com/[redacted]mikrotik-dual-wan-load-b) 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:

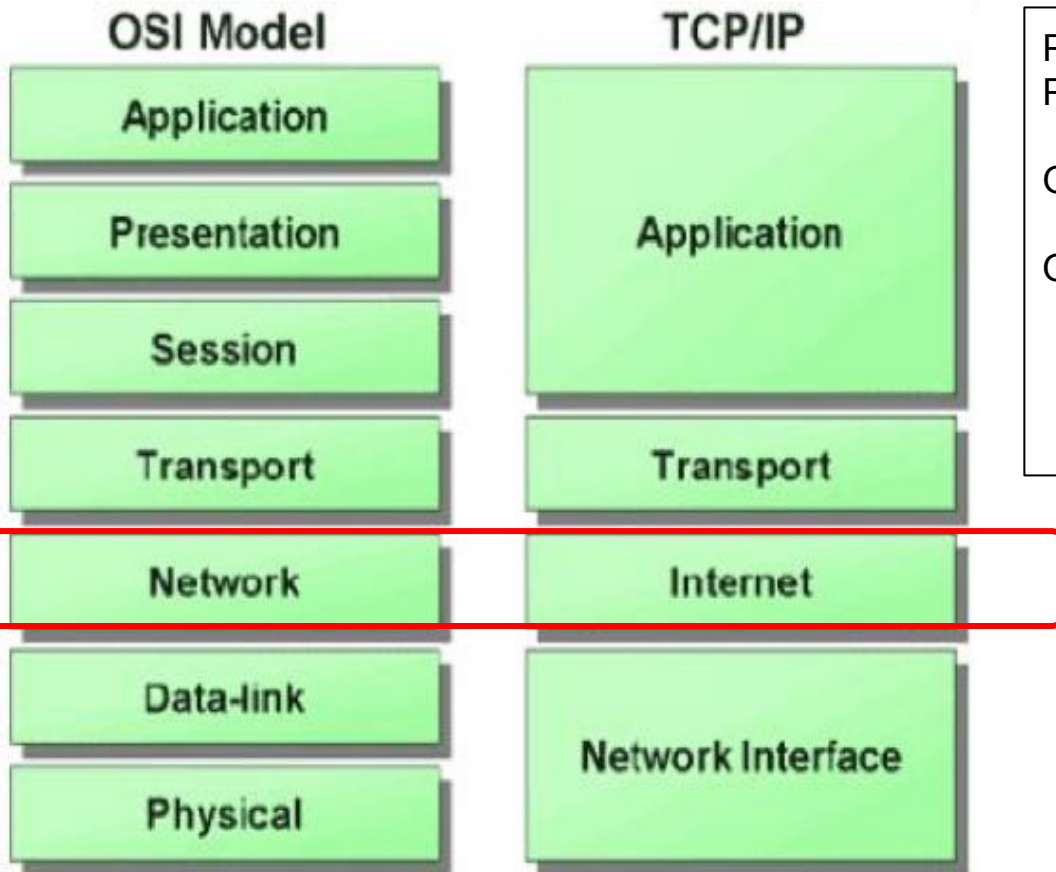
<http://www.glcnetworks.com/main/maret-2014-optimasi-jaringan-pada-sebuah-kantor-di-jakarta/>

mudah2an membantu ya

# The basics: packet, connection, routing



# What is packets?



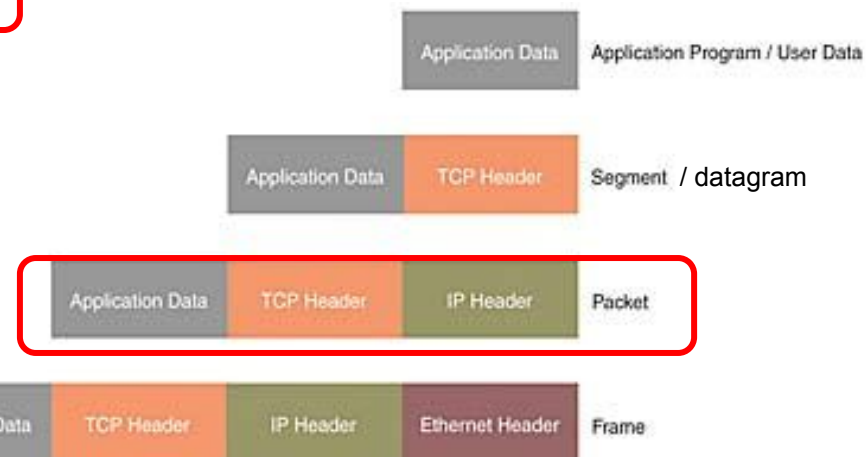
TCP/IP and the OSI model

Packet is a unit of data transmission (layer 3 PDU)

Other units: segment, datagram, frame

Questions:

- Is there any packet in a frame?
- Is there any packet in a segment?
- How to measure mbps of packets



# How do you know packet's statistics?

Measured in pps (packet per second) -> part of router performance

Interface List									
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
<div> <span>+</span> <span>-</span> <span>✓</span> <span>✗</span> <span>📄</span> <span>🔍</span> <span>Detect Internet</span> </div>									
	Name	Type	Actu...	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (...)	Comme...
R	ether1	Ethernet	1500	1580	3.1 Mbps	165.3 kbps	405	244	to ISP1
R	ether2	Ethernet	1500	1580	140.4 kbps	2.3 Mbps	191	345	
R	vlan3200	VLAN	1500	1576	2.5 Mbps	784.7 kbps	293	153	to inter-
R	vlan3216	VLAN	1500	1576	0 bps	0 bps	0	0	to IDS (
R	ether3	Ethernet	1500	1580	21.4 kbps	5.4 kbps	10	5	to ISP2
R	ether4	Ethernet	1500	1580	25.5 kbps	47.2 kbps	36	72	to SERV
R	ether5	Ethernet	1500	1580	60.6 kbps	51.1 kbps	81	84	to mana
	ether6	Ethernet	1500	1580	0 bps	0 bps	0	0	
	ether7	Ethernet	1500	1580	0 bps	0 bps	0	0	

# Layer 3 header (which one is IPv4?)

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP				ECN				Total Length															
4	32	Identification																Flags				Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length															Next Header								Hop Limit								
8	64	Source Address																															
12	96																																
16	128																																
20	160																																
24	192	Destination Address																															
28	224																																
32	256																																
36	288																																



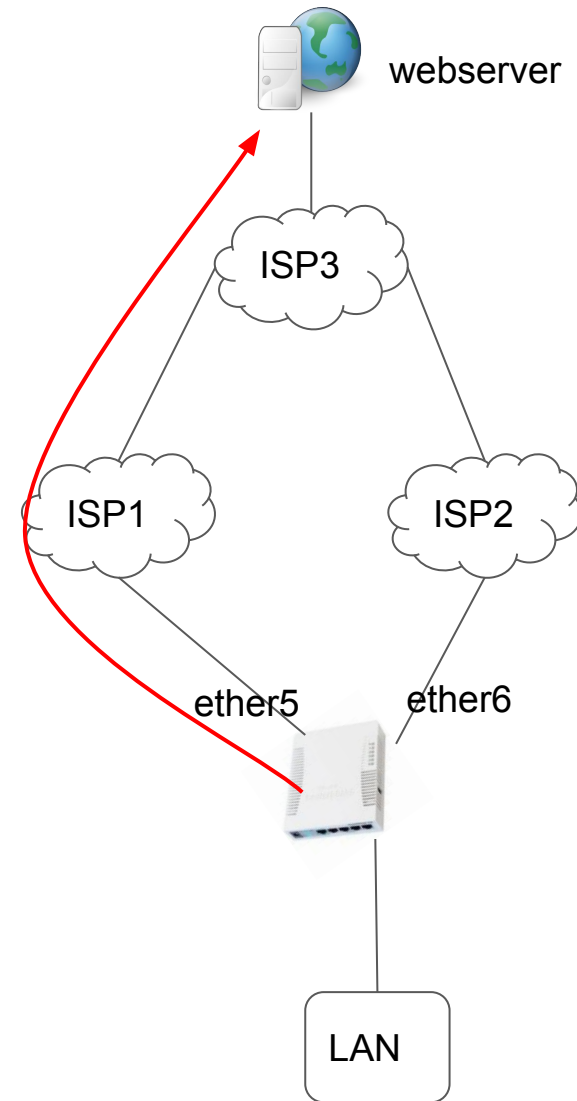
# Layer 4 header (which one is TCP?)

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset	Reserved 0 0 0			N S	C W R	E C E	U R G	A C K	P R E	S S E	F Y N	Window Size																			
16	128	Checksum																Urgent pointer (if URG set)															
20	160	Options (if <i>data offset</i> > 5. Padded at the end with "0" bytes if necessary.)																															
...	...	...																															

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																Checksum															

# What is connection?

- **A Connection** is identified by a set of IP addresses (source and destination) and ports (if necessary. E.g. source and destination port)
- When you access a remote computer, you will create a connection



# Questions:

- Is packet part of connection?
- Is connection part of packet?
- Can 1 connection have more than one packets?
- Do packets have mechanism between them so that they know their arrangement or connection between them?
- Can router identify relation between packet? E.g. keep track the relations between packet?



# Mikrotik supports connection tracking

Mikrotik conn-track supports protocol: TCP, UDP, ICMP and others

The image shows two screenshots from the Mikrotik WinBox interface. The left screenshot displays the 'Firewall' configuration window, specifically the 'Connections' tab. A red circle highlights a list of active connections. The right screenshot shows the configuration for a firewall rule, with a red circle highlighting the 'Connection State' options.

**Firewall Connections Table:**

	Src. Address	Dst. Address	Protocol	Connecti...	Time...
C	192.168.2.1	224.0.0.1	2 (igmp)		00:
SC	192.168.2.18:47248	8.8.8.8:53	17 (udp)		00:
C	192.168.98.99	192.168.98.2	47 (gre)		00:
C	192.168.98.99	192.168.98.4	47 (gre)		00:
C	192.168.98.99	192.168.98.3	47 (gre)		00:
C	192.168.98.99	192.168.98.1	47 (gre)		00:
C	192.168.98.99	224.0.0.9	2 (igmp)		00:
SACs	192.168.99.254:13765	157.56.52.27:40022	17 (udp)		00:
SACs	192.168.99.254:13765	157.55.130.149:40003	17 (udp)		00:
SACs	192.168.99.254:13765	157.55.235.145:40018	17 (udp)		00:
SACs	192.168.99.254:13765	157.55.130.175:40024	17 (udp)		00:
SACs	192.168.99.254:49155	17.188.157.40:5223	6 (tcp)		23:
SACs	192.168.99.254:49155	74.125.130.188:5228	6 (tcp)		23:

60 items | Max Entries: 218040

**Firewall Rule Configuration (Connection State):**

Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☒ invalid ☐ established ☐ related ☐ new ☐ untracked

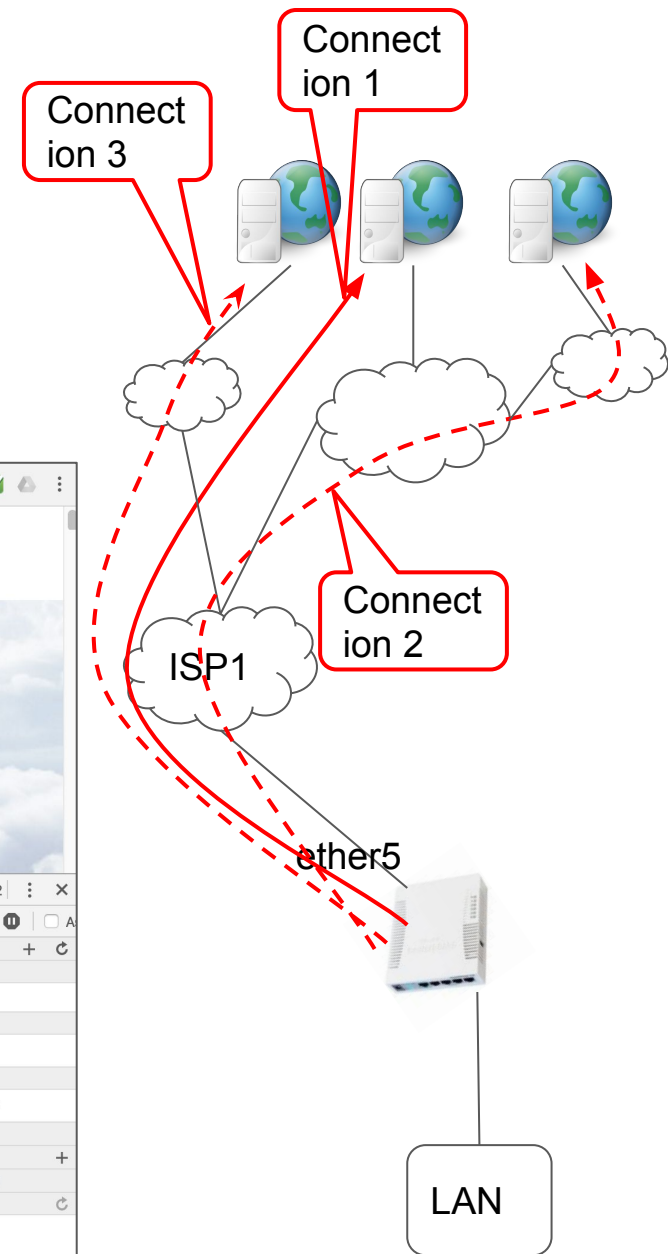
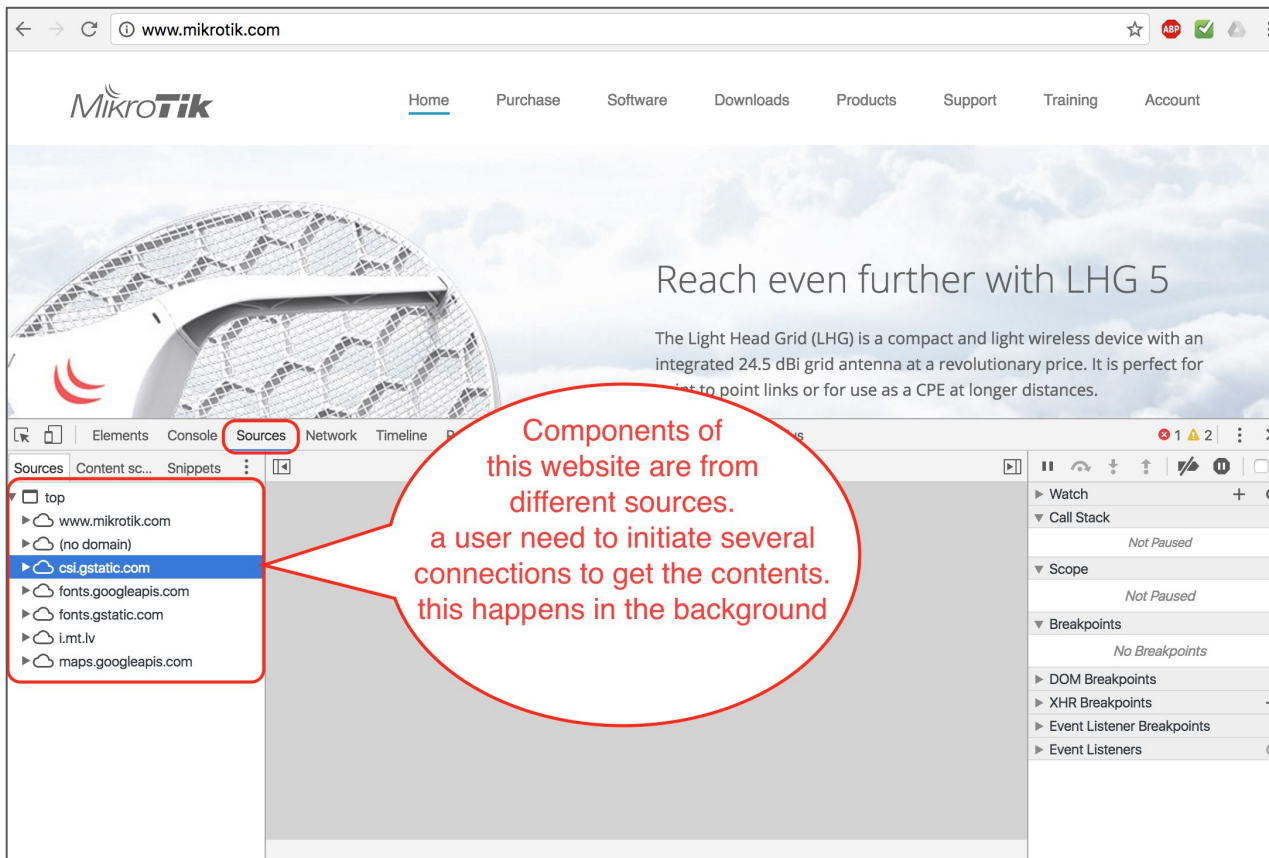
Connection NAT State:

## QUESTION

**HOW MANY CONNECTION(S)  
YOUR BROWSER CREATE  
WHEN YOU OPEN A WEBSITE?**

# Answer: inspect the web elements

- Client can open **multiple connections** to get website components

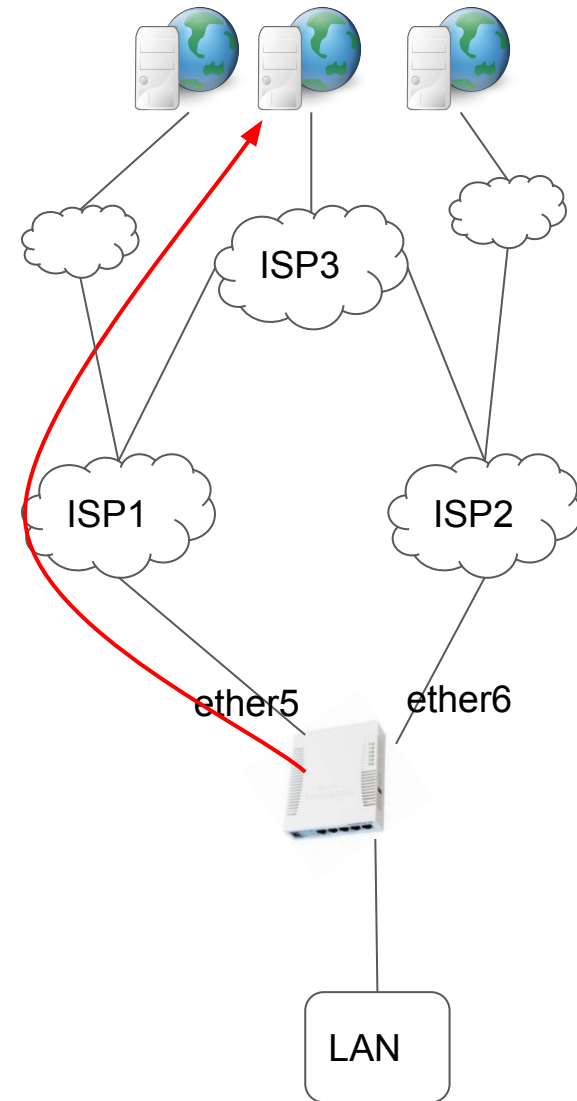
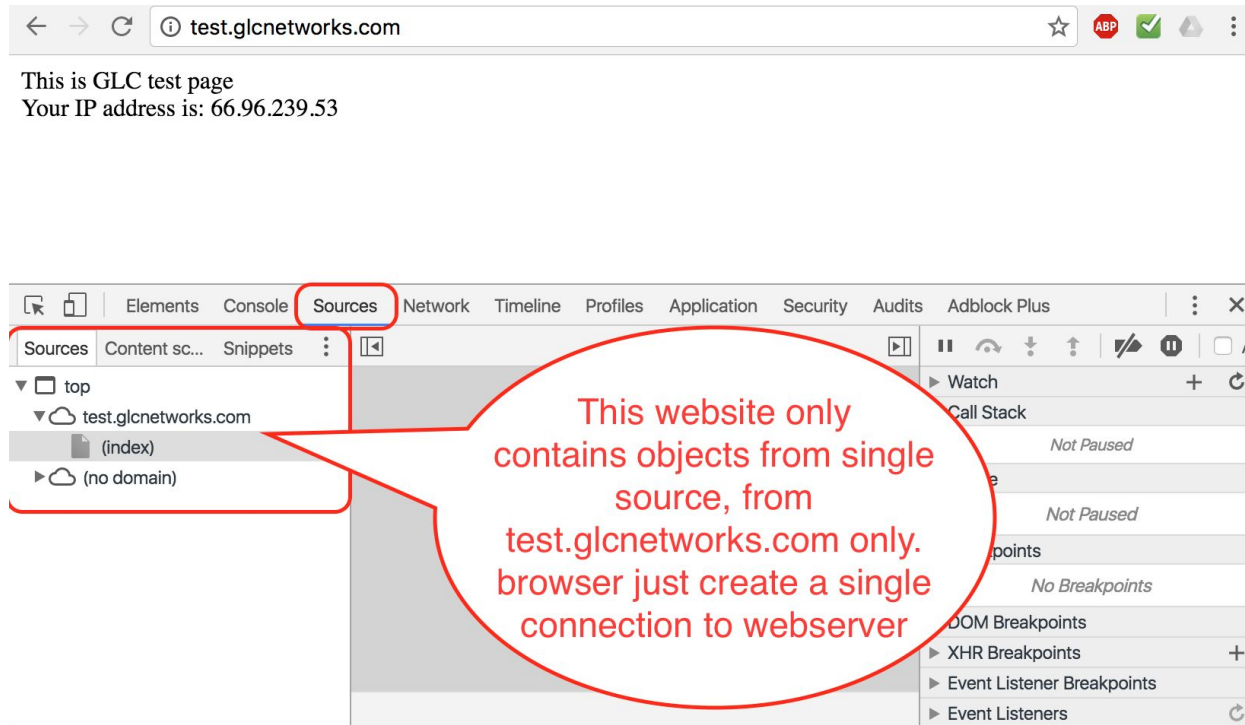




# Example: Single connection to a website

Website with single connection:

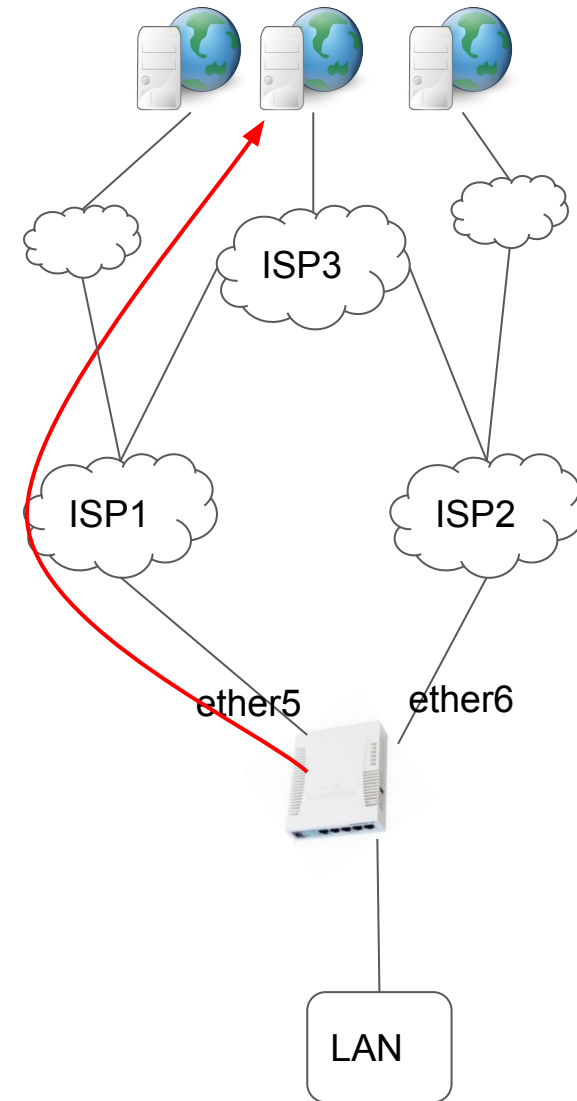
<http://test.glcnetworks.com>



# Routing and forwarding

# 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 your public IP address, go to <http://test.glcnetworks.com>



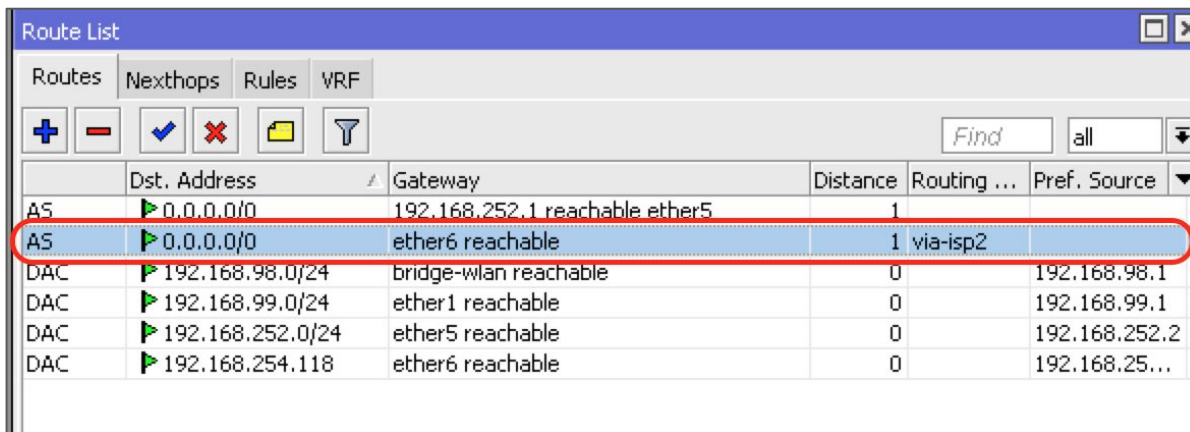
Route List

Routes	Nexthops	Rules	VRF
AS	0.0.0.0/0	192.168.252.1 reachable ether5	1
DAC	192.168.99.0/24	ether1 reachable	0
DAC	192.168.252.0/24	ether5 reachable	0

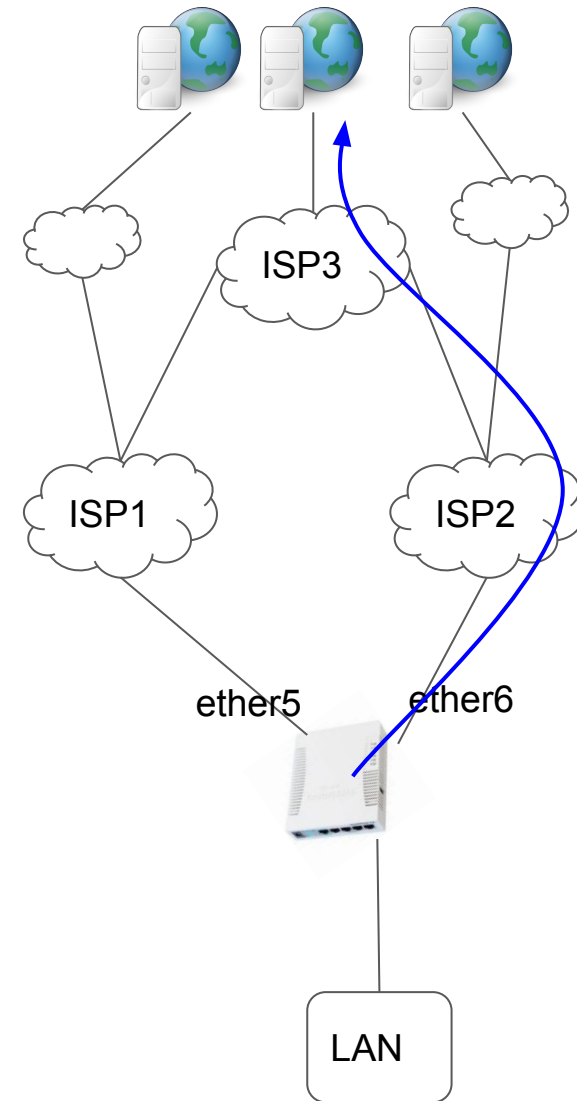
3 items

# 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

Firewall

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

+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters

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

Route List

Routes Nexthops Rules VRF

+ - ✓ ✗ 📁 🔍 Find all

	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...

New Route

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:

enabled active



# Forward traffic via ISP1 using mangle

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists

+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters

#	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 Nexthops Rules VRF

+ - ✓ ✗ 📁 🔍

	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

7 items (1 selected)

New Route

General Attributes

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

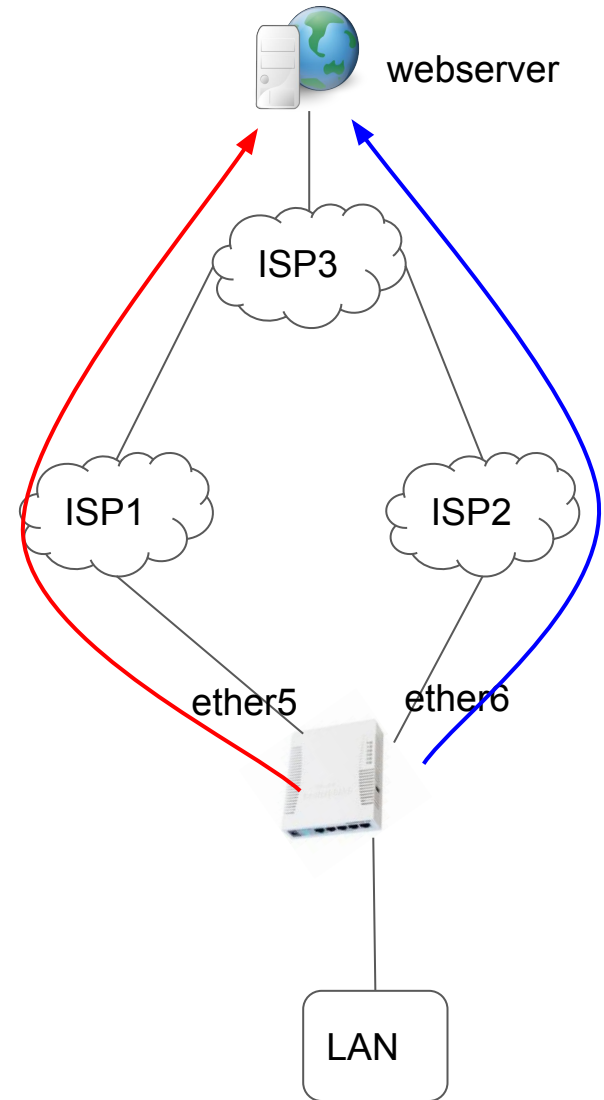
# Load Balancing

# What is (traffic) load balancing?

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

## Benefits:

- Increase utilisation of upstream links

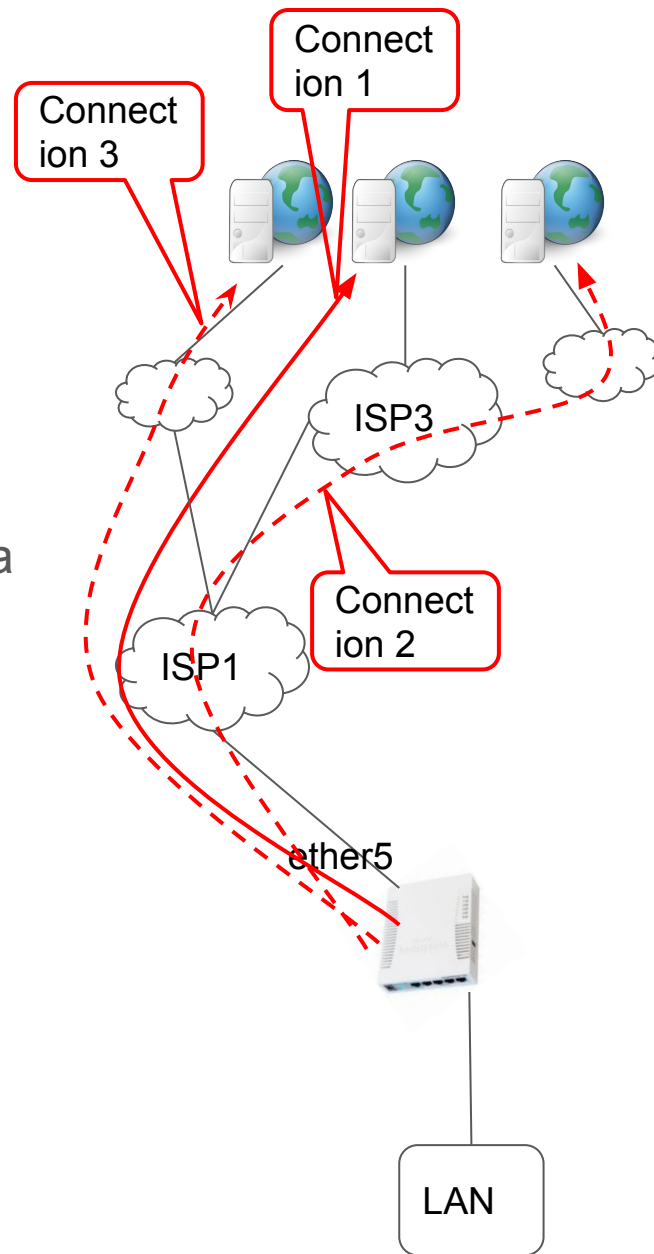


# Load balancing techniques

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 (conn-track=active)
- 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  
you want to  
create

Connection  
identifier

Per Connection Classifier: ☐ src address : 1 / 0

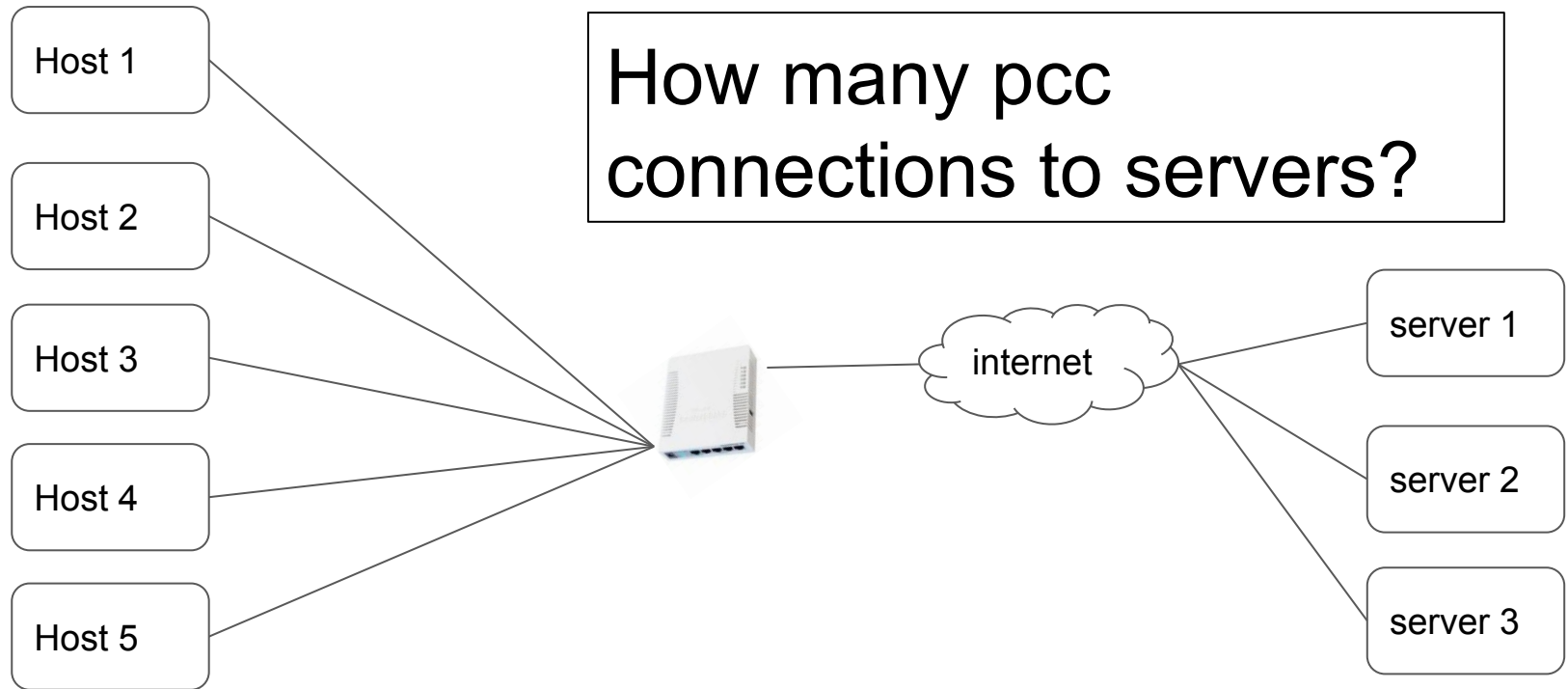
Src. MAC Address: ☐ both addresses  
both addresses and ports  
both ports

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

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

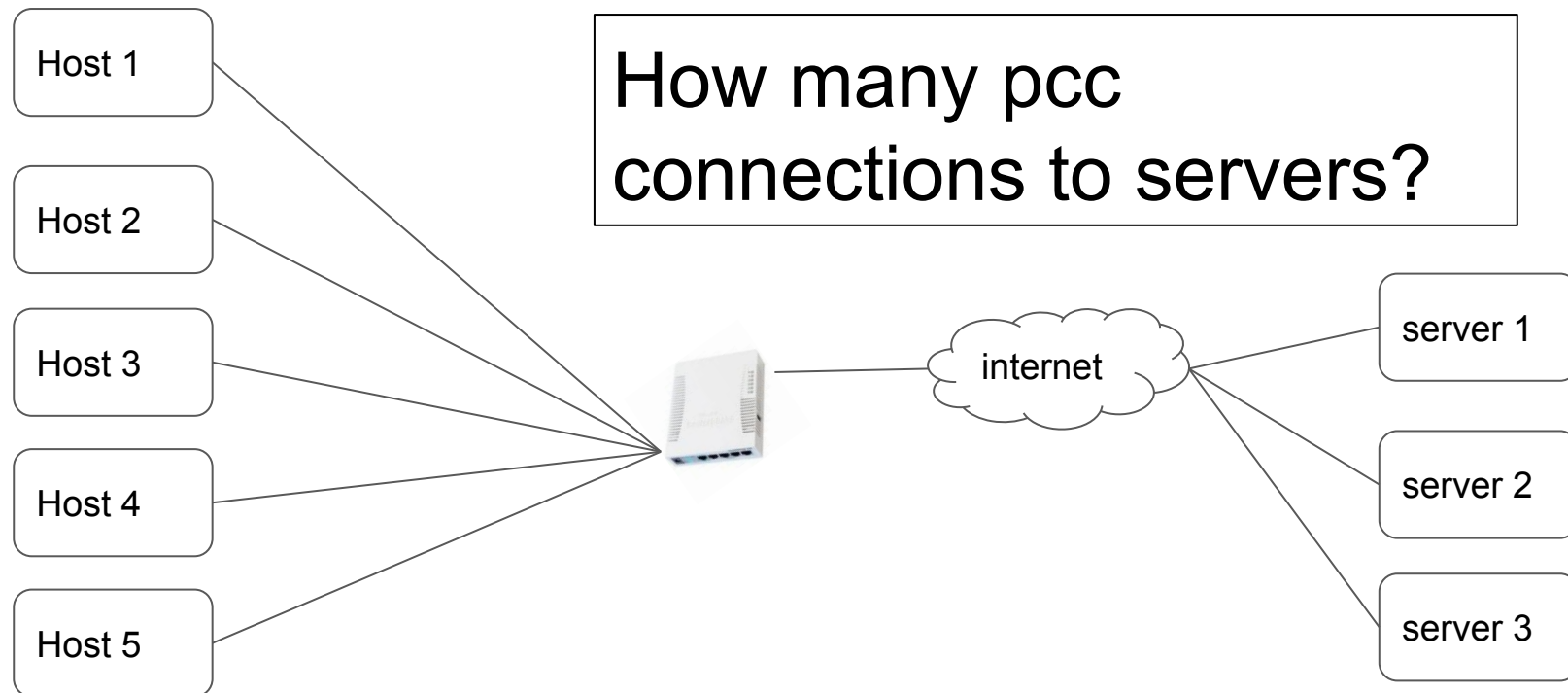
In. Bridge Port List: ☐ src port

## Exercise: Classifier=src-addr



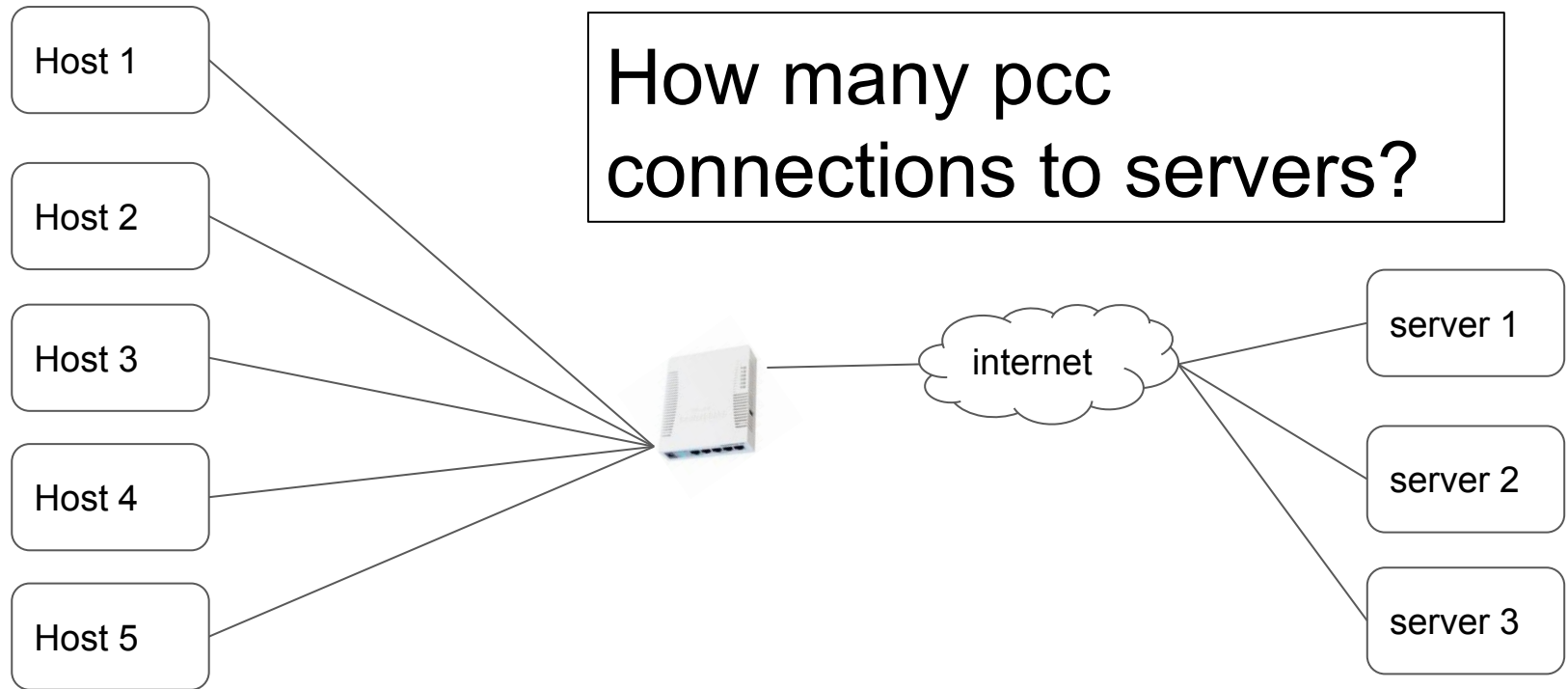
Each host connects to 3 servers

## Exercise: Classifier=dst-addr



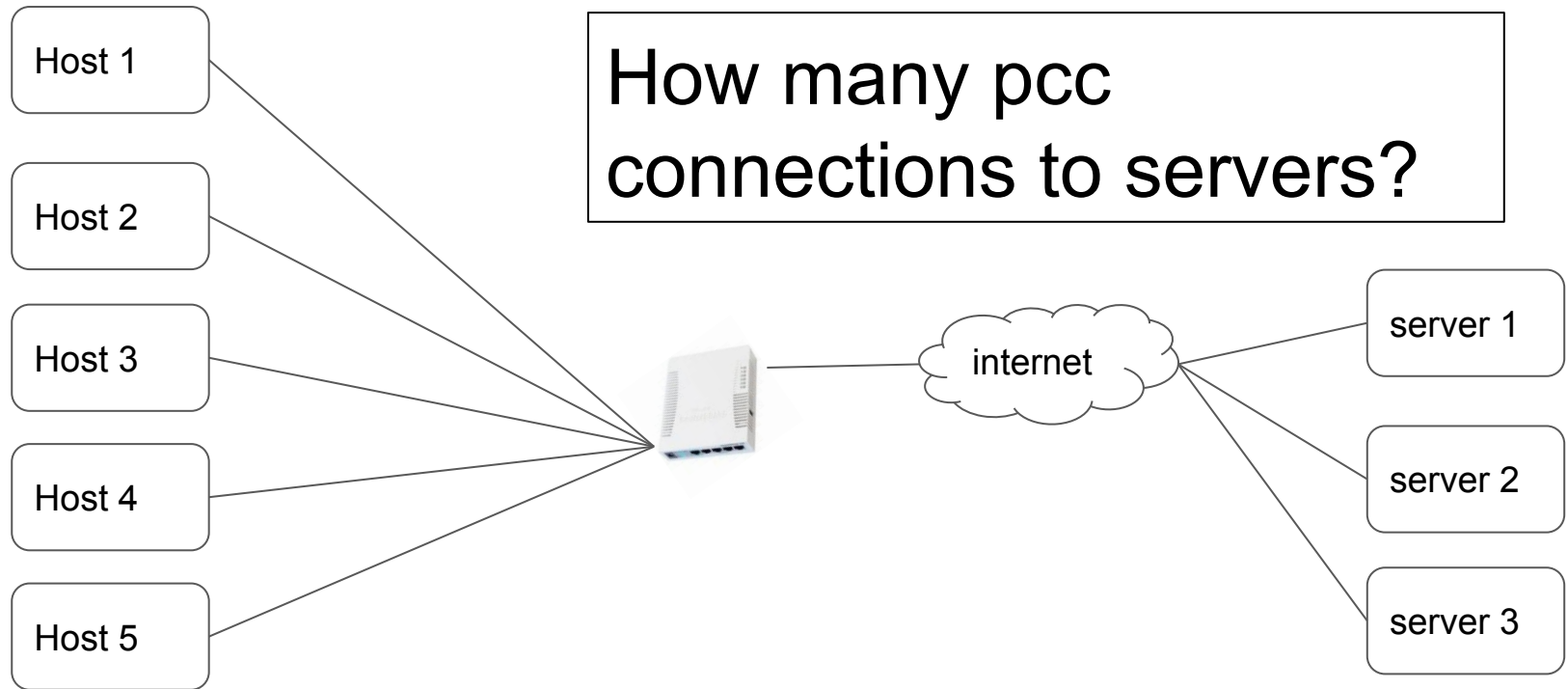
Each host connects to 3 servers

# Exercise: Classifier=both-address



Each host connects to 3 servers

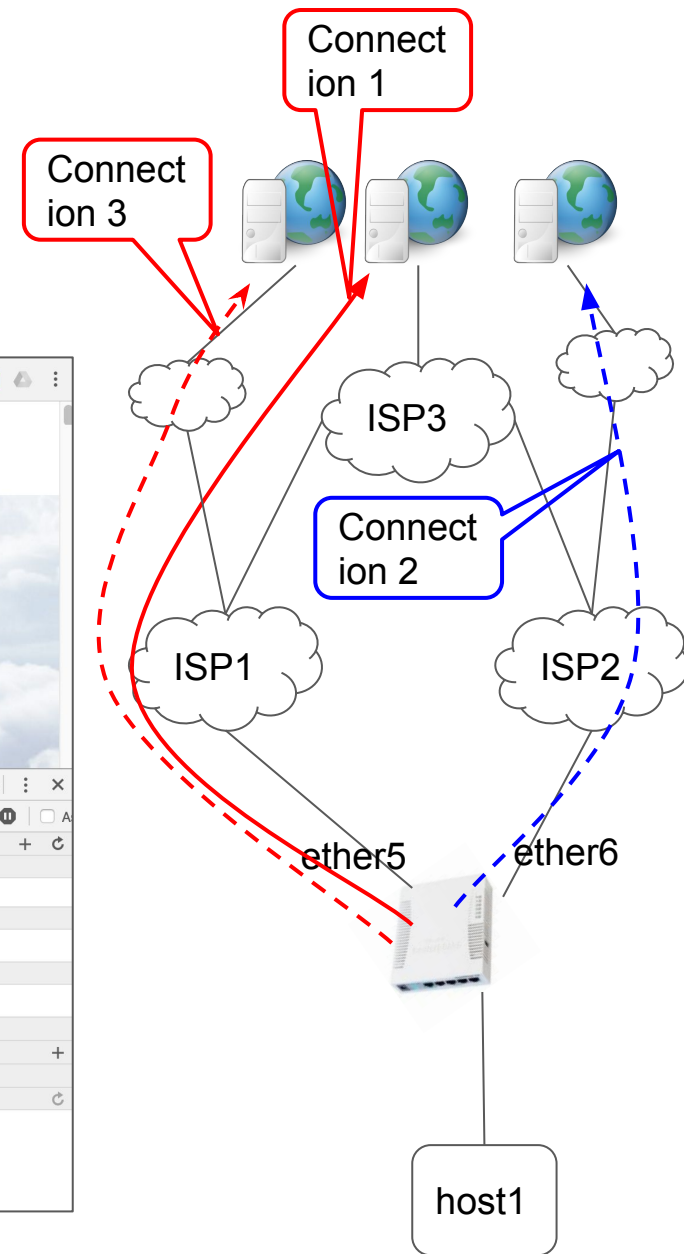
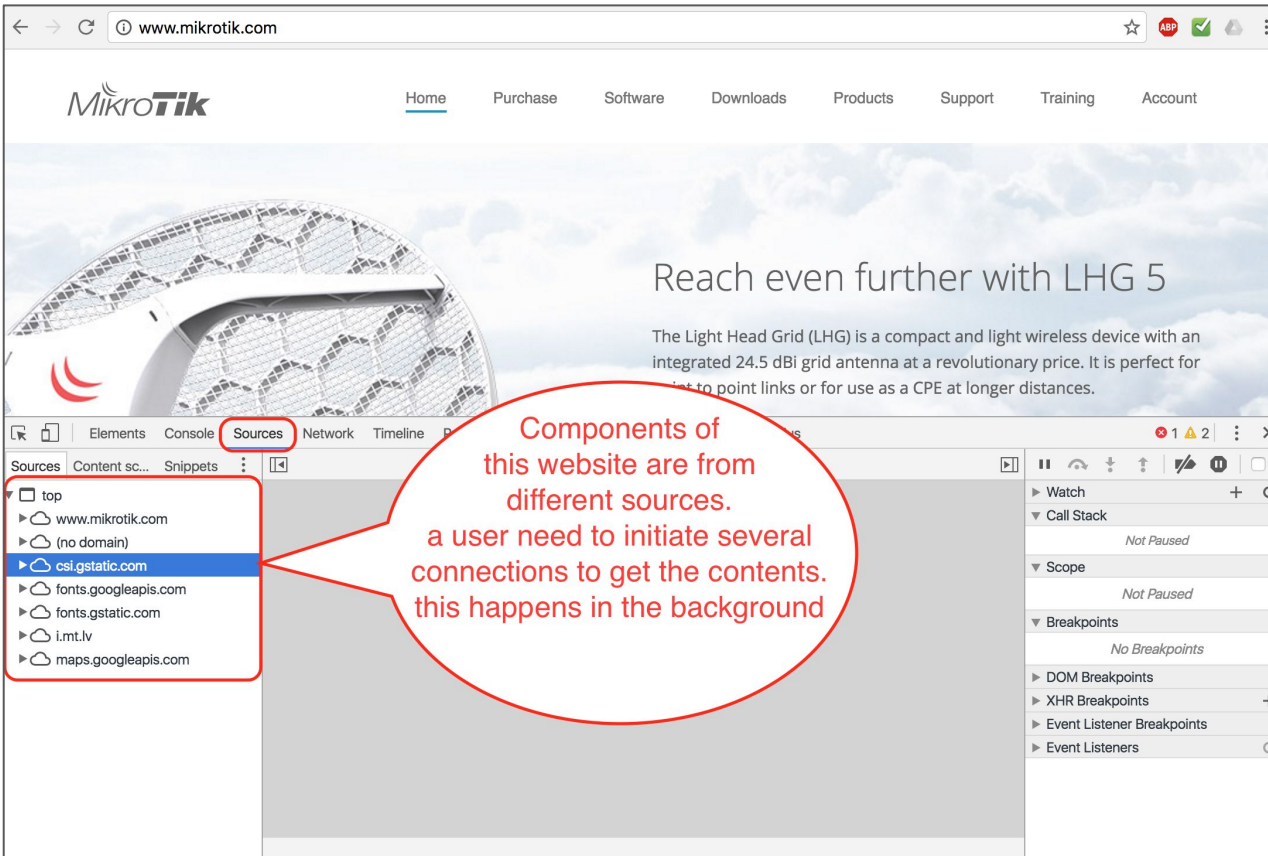
# Exercise: Classifier=both-address-and-ports



Each host connects to 3 servers



# Example: 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)
  - 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



# 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