PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

Improving Network Reliability with Traffic Steering Using Two ISP Links on Mikrotik Routers

Herdian Saputra[1*], Fawaidul Badri[2], Nanda Saputri[3], Erwinsyah Sipahutar [4], Oktrison[5]
[1]Akademi Komunitas Negeri Aceh Barat, Indonesia, [2]Universitas Islam Malang, Indonesia, [3]Politeknik Negeri Lhokseumawe, Indonesia, [4,5]Politeknik ATI Padang, Indonesia
[1]herdian.saputra@aknacehbarat.ac.id, [2]fawaidulbadri@unisma.ac.id, [3]nandasaputri@pnl.ac.id, [4]erwin.metro@gmail.com, [5]oktrison88@gmail.com

open access

***Corresponding Author**

Article History:
Submitted: 23-09-2024
Accepted: 25-09-2024
Published: 01-10-2024

Keywords:
Traffic Steering; NAT; RAW.

ABSTRACT

Traffic Steering is an additional technique applied to network traffic especially when filtering, modification, or optimization is required. Network operators usually use traffic steering to expand the value of VAS or value-added service (value-added service that refers to additional services (content) based on existing telecommunication networks). This technique is applied so that the use of traffic from a link can be directed according to the client's needs and further maximize the functional use of the link itself. In general, the implementation of traffic steering is built based on three concepts, namely: NAT (Network Address Translation), Firewall RAW, and IP Routes. In this Traffic Steering implementation, the DSTNAT chain feature on the NAT firewall is used to direct access with the destination that has been set to a specific web server.

INTRODUCTION

Along with the development of the modern era, the development of science and technology also develops. The use of computer network technology as a data communication medium is increasing to date, especially in the internet network (interconnection networking) which is a complex network. The need for the shared use of resources in the network, both software and hardware, has resulted in the emergence of various network technology developments themselves. Along with the increasing level of need and the increasing number of network users who want a form of network that provides maximum results both in terms of efficiency and improving the security of the network itself (Putra & Anton, 2024). The high need for access results in an unbalanced traffic load and a decrease in access speed. This is certainly a challenge for internet service providers to provide fast and reliable internet access services to customers (Susafa'ati et al., 2024).

To help customers with high internet access services, the development of network system infrastructure must be assisted using Internet Service Providers (ISPs). One of the important parameters for building a good internet infrastructure is the availability of large bandwidth. The availability of bandwidth capacity does not rely on just one backbone line. For this reason, a minimum of two lines are needed so that the bandwidth capacity can be maximized, which can ease the traffic load and speed up response time. One solution is to use the Traffic Steering system or traffic control on the application (Anton & Irman, 2024).

An agency certainly wants to provide the best internet connection and minimize the costs incurred. Whether the internet connection is fast or slow. To meet these needs, of course, you must be wise in choosing an existing ISP. Some ISPs provide high-speed connections, but the operational costs also need to be taken into account. Subscribing to two or more lines in one ISP is one solution that can be taken to meet large internet needs.

The Traffic Steering method on the Mikrotik router is used to set the search destination path by the interface link (ISP) that is accessed to be able to reduce and maximize the use of existing link bandwidth. Mikrotik is one way to be able to develop internet service packages so that they can be used in various available computer devices(Rahmat, 2022). In addition, the application of Traffic Steering on this Mikrotik router can prevent the occurrence of Over Load Traffic on a link so that the link connection speed can be maintained and stable. This concept is very necessary to be applied to an agency.

The above factors are the background for the author to take the topic of the final project with the title "Improving Network Reliability with Traffic Steering Using Two ISP Links on Mikrotik Routers".

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

LITERATURE REVIEW

Research that has been conducted by previous researchers related to Improving Network Reliability with Traffic Directing Using Two ISP Links on Mikrotik Routers, includes the following: Analysis and Implementation of Data Traffic Redirection (Failover) of Internet Access on Two ISPs (Taufan et al., 2023). Study Of Using Two Isps With Load Balancing And Failover To Improve Network Performance Based On Mikrotik Routers (Azmi & Razi, 2022). Implementasi Load Balancing Metode Per Connection Classifier Dan Failover Recursive Menggunakan Mikrotik (Rahmat, 2022). Implementation of Load Balancing Two ISPs Using Mikrotik (Utomo, 2011). Analysis of 4G Network Load Balancing Performance on Mikrotik PC Router Using PCC Method (Nasir, 2020). Load Balancing On Mikrotik at Karang Jaya Health Center Using NTH Method (Syahrani & Yuliadi, 2023).

METHOD

The stages of these stages are explained as follows the method stages used in this research are as follows:

1. Two ISP Traffic Steering Design
2. Implementation of Traffic Steering for Two ISPs on the Mikrotik Router.

Network Topology

The topology created in implementing traffic steering for two ISPs consists of 3 clients, one router and two ISP links. Figure 1 shows the implementation of traffic steering topology on a Mikrotik router using two ISP (Internet Service Provider) links.

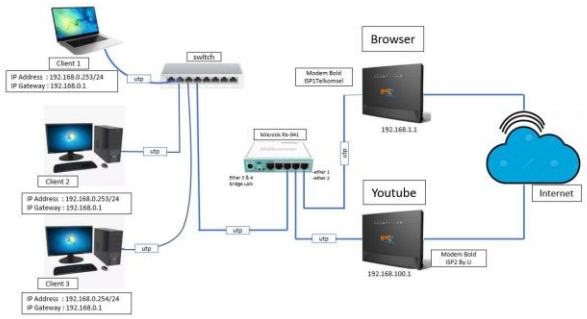


Figure 1. Topologi Traffic Steering

In designing traffic steering using two ISP links on the Mikrotik router, there are three clients, one switch, one router and two modems. Routers are used as hardware to steer traffic on certain ISPs, where the steering takes place on the Mikrotik router which is set on the Firewell feature.

Firewalls operate using certain rules. These rules determine the condition expressions that tell the router what the router should do with the IP packets that pass through it. Each rule is based on conditions and actions to be carried out. When an IP packet passes, the firewall will match it with the conditions that have been created and then determine what action the router will take according to those conditions.

Device Specifications

In implementing traffic steering there are software and hardware specifications which will be explained as follows.

Software Specifications

This software specification aims to choose exactly what software is used to configure traffic steering using two ISPs so that it can operate correctly. The software used to configure traffic steering on the two ISPs will be shown in table 1.

Table 1. Software Specifications

No	Software	Description
1	Microsoft Windows 10	As an operating system for clients
2	Mikrotik winbox v.3.32	Utility for Remote GUI to Mikrotik router

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

Hardware Specifications

The hardware requirements used to design traffic steering for two ISPs on the Mikrotik router are in Table 2.

Table 2. Hardware Specifications

No	Hardware	Quantity
1	Mikrotik router versi RB941	1
2	Modem Bold 4G	2
3	LAPTOP	1
4	Switch Tp-Link	1
5	*Provider*	2

IP Address Addressing

Table 3 IP Address Addressing

Interface	IP Address	Gateway	Network
ISP 1	192.168.1.2/24	192.168.1.1	192.168.1.0
ISP 2	192.168.100.2/24	192.168.100.1	192.168.3.0
Local	192.168.0.1/24		192.169.0.0

In Table 3 is a table regarding IP Address addressing and the interfaces on the router side, namely with the following explanation:

1. ISP-1 interface: is the interface connected to the network leading to modem A or ISP-1 gateway.
2. ISP-2 interface: is the interface connected to the network that goes to modem B or ISP-2 gateway.
3. Local Interface: is an interface connected to a local network that connects the client to the router.

In implementing traffic steering, first set the IP address that will be used for the interface address. For creating the IP on the interface used, you can see the table above.

System Implementation Steps

The following are the steps for implementing traffic steering for two ISPs on a Mikrotik router. Seen in Figure 2 System Implementation Process Flow Diagram.

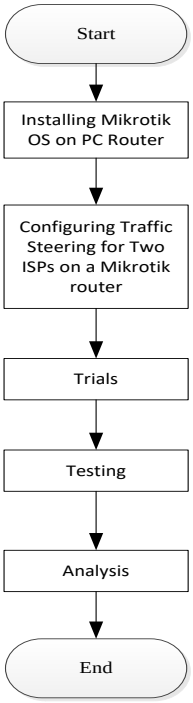


Figure 2. System Implementation Process Flow Diagram

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

Implementation of Two ISP Traffic Steering on Mikrotik Routers

In this configuration, testing was only carried out on four applications which will be traffic steering to two different interfaces. This application can be seen in Table. There are several steps in implementing Traffic Steering, where these steps will be discussed in more detail in this sub-chapter.

Table 4. Traffic Steering Application

Aplikasi	Interface
Browser	ISP1
Youtube	ISP2

In Table 4 there is a list of applications that will be traffic steered using two ISP links with a Mikrotik router.

Basic Mikrotik Configuration

In the basic configuration of a Mikrotik router, there are several things that must be done so that each device can connect so that it can access the server and the internet. What is done in this configuration is IP address configuration, internet gateway configuration, and DHCP server and client configuration. There are several stages for the router to connect to the internet, namely configuring the IP address, NAT, and DHCP server.

IP DHCP Client

The next configuration is the IP DHCP Client configuration, where this configuration activates the DHCP Client function on the ISP1 interface and ISP2 interface so that the proxy can connect to the internet. At this stage, configuration is carried out by default via Winbox software in Graphical User Interface (GUI) mode.

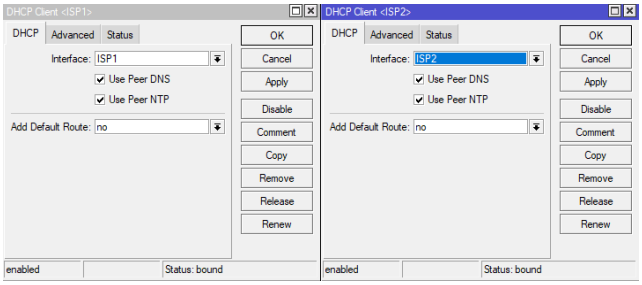


Figure 3. IP DHCP Client

This default configuration is complete where the router has got a gateway IP address and also a DNS IP so that the router can be directly implemented into the network. The results of this configuration are shown in Figure 3.3. The DHCP Client IP on router 1 is 192.168.1.254/24 and the DHCP Client IP on router 2 is 192.168.100.254/24. The status information on the DHCP client must be bound, which means that both routers have received IP address, gateway, and also DNS, DHCP client, namely DHCP on the client side whose purpose is to request an IP address from the DHCP server.

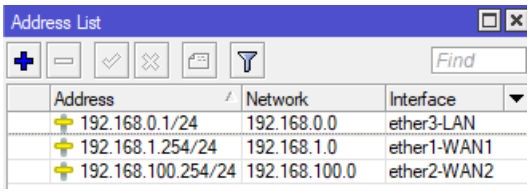


Figure 4. IP Address

The IP address obtained from the DHCP server can be seen in the address list tool as in Figure 4.

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

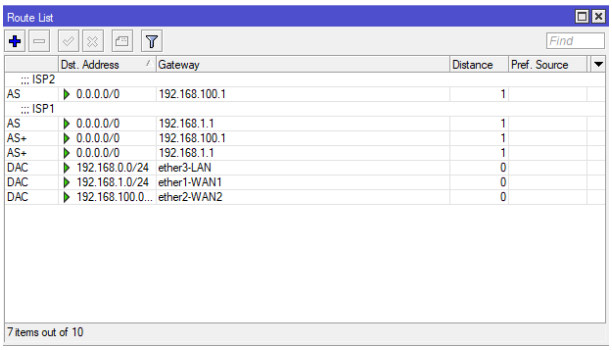


Figure 5. IP Route List

In Figure 5 shows the IP route, in this section make sure that the router device has received a gateway IP, where the gateway IP obtained on router one is 192.168.1.1 and on router two is 192.168.100.1 during the simulation.

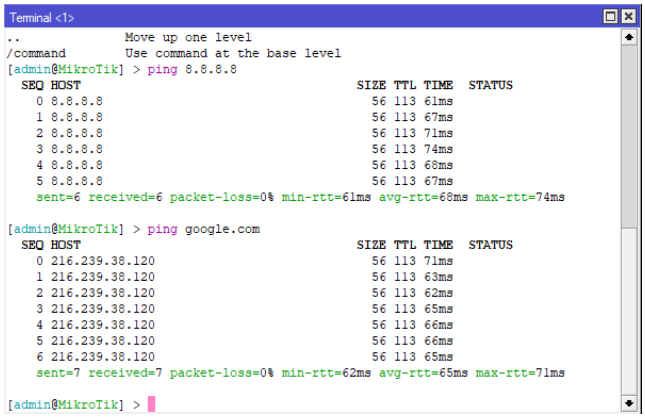


Figure 6. Test Internet Connection on Router

To ensure that the router is connected to the internet, you can test it using the terminal tools in the Winbox feature, then run the ping DNS server command to 8.8.8.8 and also google.com as shown in Figure 6.

IP Address

Next, configure the IP address on each interface of the router device. Address List is one of the Mikrotik features that is used to make certain IPs into names. This makes it easier to mark an address configuration.

In this address list configuration there are several interfaces, where on the LAN interface there is an IP address 10.10.1.1/24 which leads to the local network, ISP1 with an IP address 192.168.1.254/24 and on the ISP2 interface there is an IP address 192.168.100.254/24. The ISP1 and ISP2 IP interfaces will be used as gateways for clients to connect to the computer network in that area. The steps for creating an IP address can be seen in Figure 7.

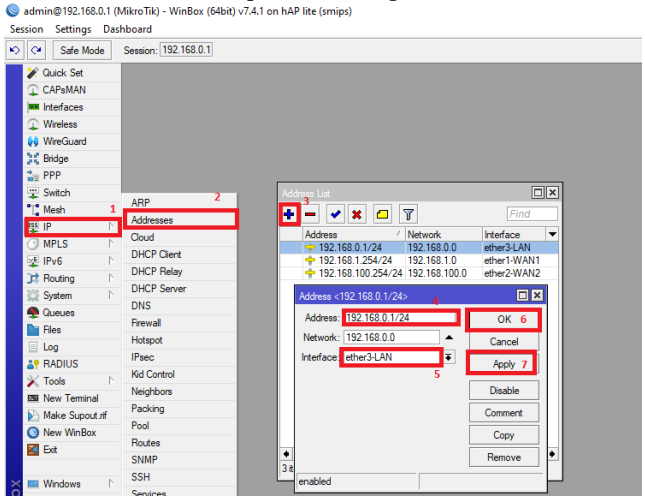


Figure 7. IP Address Configuration

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

Network Address Translation (NAT) configuration

Table 5. NAT Chain Out Configuration Planning.

Chain	Out. Interface	Action
srcnat	ISP1	Masquerade
srcnat	ISP2	Masquerade

In table 5 there is a NAT configuration plan carried out for traffic steering for two ISPs on the Mikrotik router. Network Address Translation (NAT) is a function in a firewall that is used to change the IP address of the sender and recipient of a data packet. In Figure 8 there are basic steps in configuring NAT on a firewall.

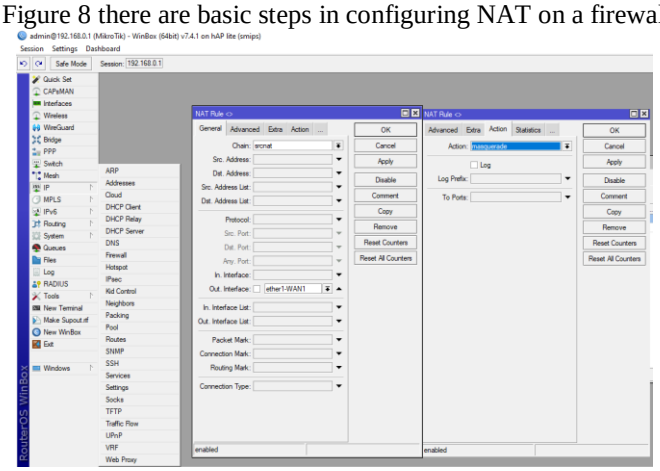


Figure 8. NAT configuration

In this step, the purpose of the scrnat chain is to determine what part of a packet will be changed. When it passes through a router, the desired requirement in this simulation is for the client computer to be connected to the internet.

In using scrnat, it functions when a packet sent from the client computer to the internet network must be changed in the source address section, where the source IP flag of the packet is changed to the IP address on ISP1 or ISP2 so that the packet can be sent to the internet network. Therefore, the out interfaces used are ISP1 and ISP2, their function is to go to the internet network and in the action section masquerade is used which means that when the chain used is a scrnat chain, the router takes action to change the source IP flag of a packet originating from the client computer to IP address used on ether1 so that the packet can be recognized by the public network.

DHCP Server

The purpose of setting the DHCP server is so that the router can distribute IP addresses to client computers dynamically or automatically so that connected devices do not need to manually configure IP addresses anymore.

Raw Configuration

RAW is a firewall table that is similar to a filter table in that it handles packet filtering. However, raw has the advantage of not consuming as many CPU resources as a firewall filter (it is lighter). This is because raw is able to bypass or drop packets before the connection tracking process occurs.

Connection tracking is a feature or ability to view information on current connections. Examples are source address, destination address, source and destination port, protocol type, and so on [14]. In the RAU firewall configuration, there are four applications that will be set in RAU to implement traffic steering, namely:

Youtube configuration

The next configuration is the YouTube configuration on the raw firewall. This is done to get the server address from Youtube. The steps for configuring YouTube in the .youtube.com context can be seen in Figure 9.

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

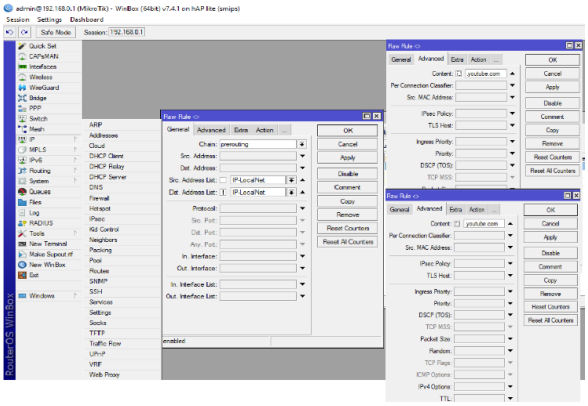


Figure 9. Configure youtube.com content in RAW

The next YouTube configuration is the y.tmg.com content configuration, where the context includes content from the YouTube application itself. The configuration can be seen in Figure 10.

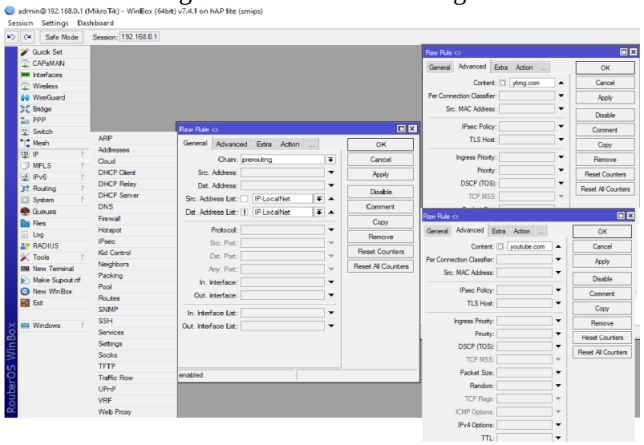


Figure 10. Configuring ytmg.com content in RAW

The final step in configuring raw YouTube content is .googlevideo.com. The configuration can be seen in Figure 11.

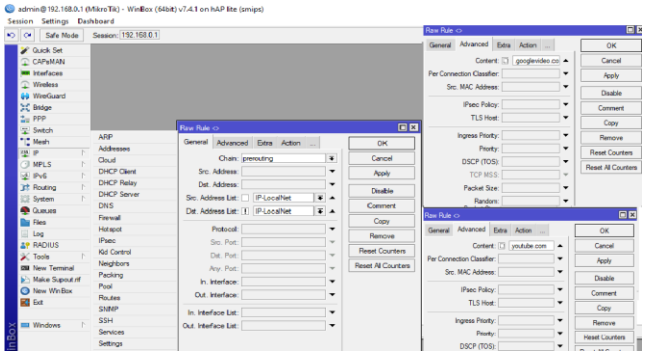


Figure 11. Configure youtube.com content in RAW

Configure Address List

Address list is one of the MikroTik features whose function is to make it easier to mark an address configuration. so with the address list you can create a list of addresses you want to mark without having to interfere with important configurations in other features. Another function of the address list is as an action on the firewall so that the admin can determine what addresses he wants to mark and enter into the address list. The address list for applications can automatically be obtained from accessing content that has been set in RAW. It can be seen in Figure 12.

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

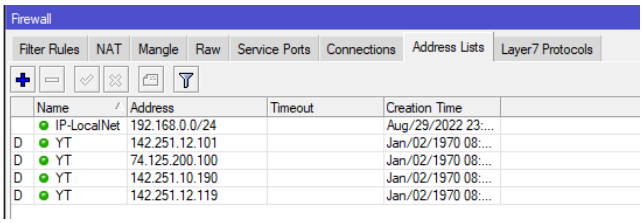


Figure 12. Address List configuration

Mangle Configuration

Mangle is one of the features found in the firewall menu. Mangle is the stage where data packets coming from a particular interface will be processed. The function of the rules in the dimangle is to mark packets so that they can be directed according to the existing routing rules.

In the mangle there are 3 types of marking that can be used by MikroTik RouterOS, namely:

1. Connection-mark, used to mark 1 CONNECTION, both request and response. This mark will mark the "new" packet or the first packet to pass, then all packets that have the same connection as the first packet will receive the same marking.
2. Packet-mark, is a marking used to mark each packet that passes through the router, just like the Connection Mark, this marking also marks Request and Response traffic. Packet-mark is also used to mark each packet that passes through the Router.
3. Route-mark, Route-Mark is used for selecting routing paths.

Bydefault the mangle parameters are divided into several chains, namely:

1. Chain Input is used to mark incoming traffic to the Mikrotik router and you can only select In. Interface only.
2. Chain Output is used to mark traffic that goes out through the Mikrotik router and can only select Out. Interface only.
3. Chain Forward is used to mark incoming and outgoing traffic through the router and can select In and Out Interfaces.
4. Chain Prerouting is used to mark incoming traffic to and through the router (download traffic). This chain can only select Out. Interface only.
5. xChain Postrouting is used to mark traffic that goes out and through the router (upload traffic) and can only select In. Interface only.

Application Routing Settings

Routing is a process carried out by a router to determine the destination route that a packet will take. At the destination address stage (IP Address) is a single IP or destination subnet network that connects with IP 0.0.0.0/0, where all destinations will be redirected to a certain gateway. Next is the gateway (exit), which is a single IP from the router that must be addressed (next hop). Where the gateway IP address must be an IP address whose subnet is the same as one of the IP addresses installed on the router, for example on ISP1 there is a gateway IP 192.168.1.1, and the gateway IP on ISP2 is 192.168.100.1. Figure 13 shows the stages of routing settings.

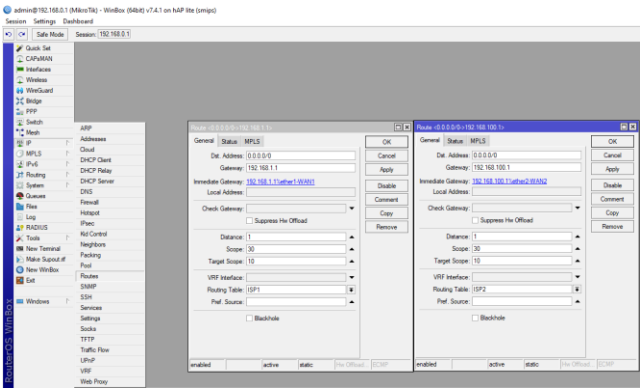


Figure 13. Application Routing Configuration

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

RESULT AND DISCUSSION

In this section, data analysis is carried out on the results obtained in implementing Traffic Steering on a Mikrotik router using two ISP (Internet Service Provider) links. To find out whether the application of the steeringc application method on certain ISPs, namely ether1 and ether2, was successful. This chapter explains how to collect data and analyze the traffic steering method for two ISPs on the Mikrotik router.

Data Testing

Data testing and analysis in traffic steering for two ISPs on the Mikrotik router will be carried out using traceroute on the Mikrotik feature in Winbox, command prompt and the Winmtr application. The following are the various tests carried out to see the implementation of the configuration results carried out.

Testing Connections in a Network

Before observing the traffic steering method on the Mikrotik router using two ISP links, a connection test was carried out leading to the router gateway and the IP address of the web server to be addressed. This test is carried out by pinging the router's gateway and the web server's IP address. In Figure 15 there are ping results to the web server.

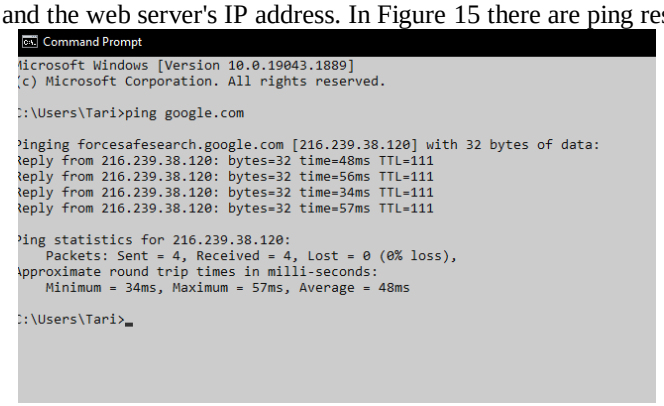


Figure 14. PING process on the web server

Testing Using Mikrotik Traceroute

Traceroute or tracert on this proxy is a tool for measuring the speed and routes that data takes when it goes to the server. This speed is measured in milliseconds (ms). The results of the traceroute will be displayed in a row of numbers on the computer screen. Tracerroute works by sending a series of messages called an ICMP Echo Request to the destination server.

In the process of using Traceroute on the Mikrotik feature, testing will be carried out on YouTube, Google and Twitter. This test was carried out to display results using the traffic steering method, where the user uses two available internet connection lines, namely ISP1 and ISP2. This test will show whether the traffic steering process on youtube.com was successful or not. It can be seen in Figure 15.

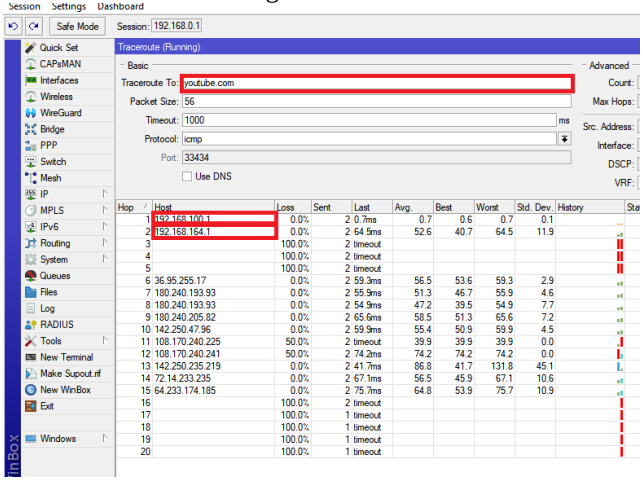


Figure 15. Implementation of YouTube traffic steering to ISP2 on Mikrotik Tracert

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

In Figure 15, the implementation of traffic steering in the YouTube application was successfully carried out with the initial process of accessing the IP being two ISP IPs with IP 192.168.100.1 and there was a loss of 0.0%, sent 2 packets, last or time the packet was received by the server was 0.7 ms, Average or average The average time received by the server is 0.7, Best or what can also be called the best time for a packet to be received by the server is 0.6, Wost or the longest time for the server to receive a packet is 0.7, with Std Dev 0.1.

Next, test the implementation of traffic steering on Mikrotik traceroute using twitter.com. It can be seen in Figure 16.

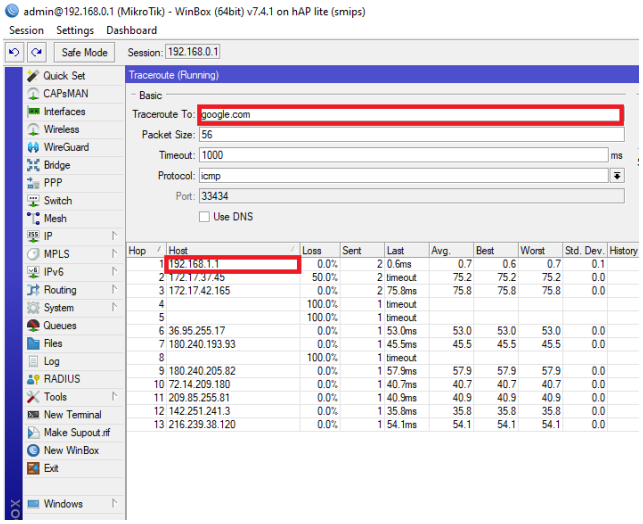


Figure 16. Implementation of Google traffic steering to ISP1 on Mikrotik Tracert

In the picture above, you can see that google.com is directed to ISP one with IP 192.168.1.1, and there is a loss of 0.0%, sent 2 packets, with the last or time received 0.6 ms, average or average time received by the server 0.7 , best or the best time for a packet to be received by the server is 0.6, wost or the longest time for a packet to be received by the server is 0.7 with a dev standard of 0.1.

Testing Using Tracert Command Prompt

The second test in implementing traffic steering is using Tracert Common Prompt from Windows with the youtube.com, facebook.com and instagram.com websites.

Tracerroute works by sending a series of messages called an ICMP Echo Request to the destination server. During the first request, the TTL duration is at number one. TTL (Time to Live) is the length of time data can stay on the network. When data arrives on the first route, its TTL number will be reduced from one to zero. Then, there will be a notification to the device that the time is up. The device will look at the IP address of the route and calculate how long the response time will be, then display it on the screen. After that, traceroute will repeat the above process with a larger TTL number (a multiple of one), until the data reaches the destination server.

In each traceroute process, the route with the IP address will be displayed on the PC. This is what is called a hop, namely the "point" that data passes through on its way to the server. Generally, the division of hops is:

a. The first hop is the device
b. The second hop is the ISP
c. The hop at the end of the traceroute is the destination server

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

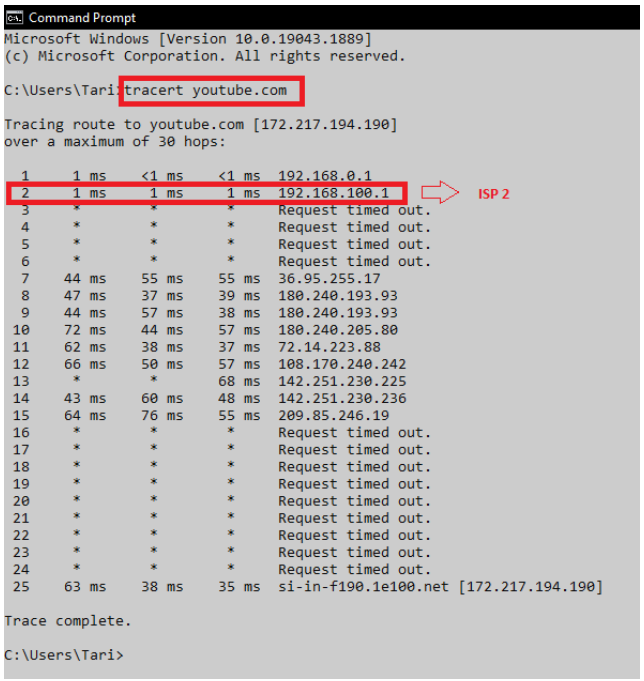


Figure 17. Implementation of YouTube traffic steering to ISP2 on Tracert CMD

In Figure 17 is an example of a tracert command to youtube.com going to ISP2 with IP 192.168.100.1. You can see that tracert to the YouTube server requires 25 hops from the device used. The response of each hop was recorded under 100 ms. This means it is quite fast because the network is smooth.

There were requests timed out 14 times on the YouTube server test, rto occurred because the server at that hop did not receive the ICMP Echo Request message. This often happens if the server is busy. Meanwhile, if an asterisk occurs because the server at that hop does not respond to tracert requests. If it only appears once, wait for a response at the next hop. However, if several lines of asterisks appear, it is likely that the server is having problems.

The next test was carried out on the facebook.com server with traffic steering towards ISP1 with IP 192.168.1.1, seen in Figure 18.

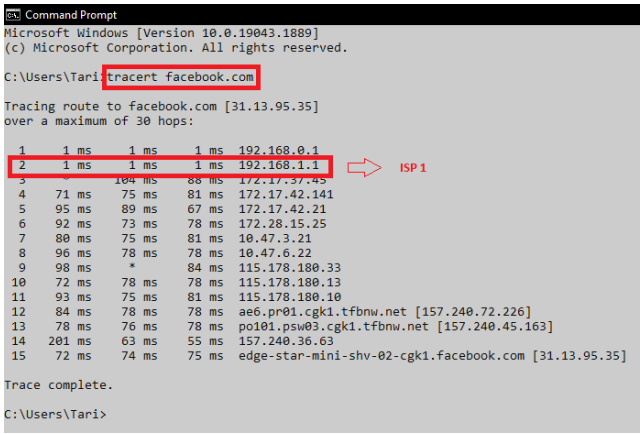


Figure 18. Implementation of Facebook traffic steering to ISP1 on Tracert CMD

It can be seen in the tracert image that going to the Facebook server requires 18 hops from the device used. The response of each hop was recorded under 100 ms. This means that it is quite fast because the network is smooth and there is 1 RTO.

Next, in testing using Tracert Command Prompt with the Instagram.com web server it will be steered via ISP1 with IP 192.168.1.1. It can be seen in Figure 19.

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

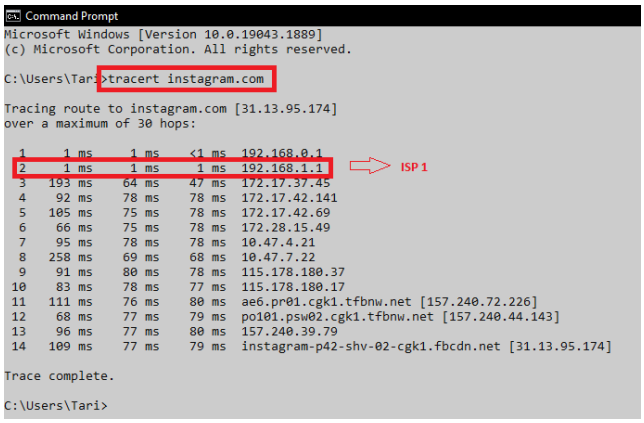


Figure 19. Implementation of Instagram.com traffic steering to ISP1 on tracert CMD

In testing the instagram.com server using tracert CMD it requires 13 hops from the device used. The response of each hop is recorded over 100 ms. This means that it is quite slow because the network is not smooth and rto occurred 3 times.

Testing Using WinMTR

WinMTR is a network diagnostic tool that is open code and very easy to use. How to use it is to run the software then enter the host name or destination IP address. In testing using WinMTR, there are three applications, namely YouTube. Gmail, and Yahoo.

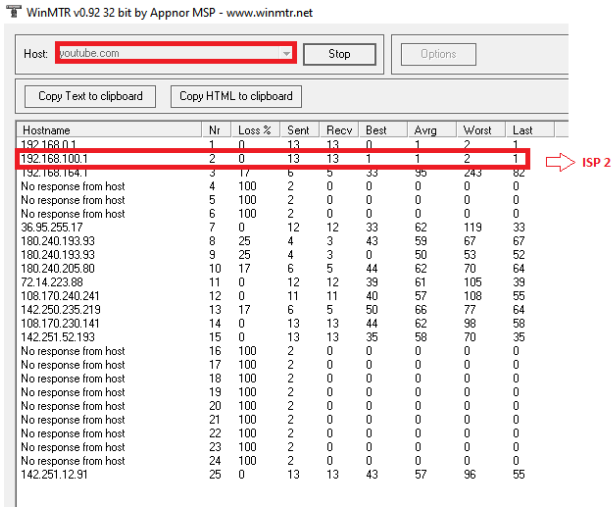
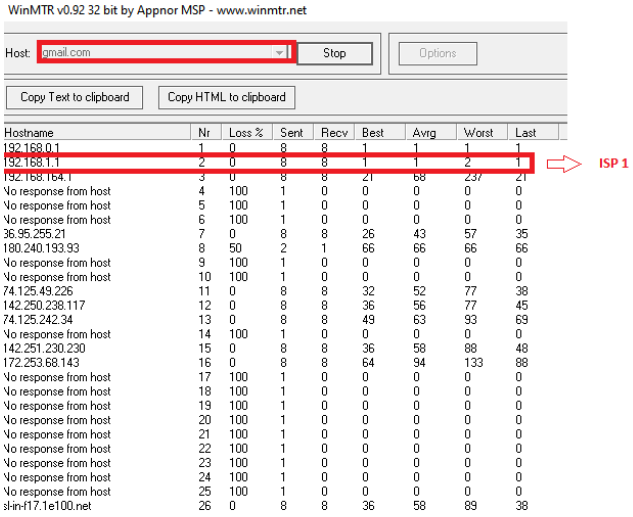


Figure 20. Implementation of YouTube traffic steering to ISP2 on the Win MTR application

In Figure 20 there is a YouTube host display in the Win MTR application. Where it can diagnose that there is a problem with the quality of the internet network connection, namely Loss%, where packet loss occurs with varying values. The higher the Loss value, the slower the connection will be. The Loss% column informs you of the percentage of connections that are lost at each hop. As for the Snt column, it calculates the number of packet numbers sent, for example on the client IP, namely 192.168.0.1, there are 25 packets sent to the server. The next four columns, namely Last, Avg, Best and Wrst, use lantency measurement units in milliseconds (for example: ms). Last is the last latency sent, Avg is the average latency of all packets, while Best and Wrst describe the fastest and longest times during which packets are sent to the host.

PERFECT
JOURNAL OF SMART ALGORITHMS

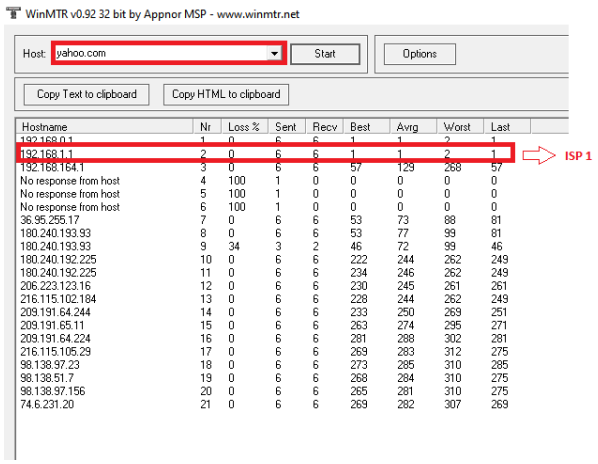
E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10



Hostname	Nr	Loss %	Sent	Recv	Best	Avrg	Worst	Last
192.168.0.1	1	0	8	8	1	1	1	1
192.168.1.1	2	0	8	8	1	1	2	1
192.168.164.1	3	0	8	8	21	68	237	21
No response from host	4	100	1	0	0	0	0	0
No response from host	5	100	1	0	0	0	0	0
No response from host	6	100	1	0	0	0	0	0
36.95.255.21	7	0	8	8	26	43	57	35
180.240.193.93	8	50	2	1	66	66	66	66
No response from host	9	100	1	0	0	0	0	0
No response from host	10	100	1	0	0	0	0	0
74.125.49.226	11	0	8	8	32	52	77	38
142.250.238.117	12	0	8	8	36	56	77	45
74.125.242.34	13	0	8	8	49	63	93	69
No response from host	14	100	1	0	0	0	0	0
142.251.230.230	15	0	8	8	36	58	88	48
172.253.68.143	16	0	8	8	64	94	133	88
No response from host	17	100	1	0	0	0	0	0
No response from host	18	100	1	0	0	0	0	0
No response from host	19	100	1	0	0	0	0	0
No response from host	20	100	1	0	0	0	0	0
No response from host	21	100	1	0	0	0	0	0
No response from host	22	100	1	0	0	0	0	0
No response from host	23	100	1	0	0	0	0	0
No response from host	24	100	1	0	0	0	0	0
No response from host	25	100	1	0	0	0	0	0
sl-in-f17.1e100.net	26	0	8	8	36	58	89	38

Figure 21. Implementation of Gmail traffic steering to ISP1 on the WinMTR apk

Furthermore, on Gmail.com, it can be seen in Figure 21 that Gmail's steering traffic successfully leads to ISP1 with IP 192.168.1.1 and there are 26 hops sent with different navigation standards for each hop that is passed, for example on IP 192.168.164 there is 1 8 packets are sent with an 8 packet receiver and the best time or fastest time for sending the packet is 1 ms with the average or average latency of all packets being 1 ms with the worst or longest time for the packet sent to the host being 1 ms .



Hostname	Nr	Loss %	Sent	Recv	Best	Avrg	Worst	Last
192.168.0.1	1	0	6	6	1	1	2	1
192.168.1.1	2	0	6	6	1	1	2	1
192.168.164.1	3	0	6	6	57	129	268	57
No response from host	4	100	1	0	0	0	0	0
No response from host	5	100	1	0	0	0	0	0
No response from host	6	100	1	0	0	0	0	0
36.95.255.17	7	0	6	6	53	73	88	81
180.240.193.93	8	0	6	6	53	77	99	81
180.240.193.93	9	34	3	2	46	72	99	46
180.240.192.225	10	0	6	6	222	244	262	249
180.240.192.225	11	0	6	6	234	246	262	249
206.223.123.16	12	0	6	6	230	245	261	261
216.115.102.184	13	0	6	6	228	244	262	249
209.191.64.244	14	0	6	6	233	250	269	251
209.191.65.11	15	0	6	6	263	274	295	271
209.191.64.224	16	0	6	6	281	288	302	281
216.115.105.29	17	0	6	6	269	283	312	275
98.138.97.23	18	0	6	6	273	285	310	285
98.138.51.7	19	0	6	6	268	284	310	275
98.138.97.156	20	0	6	6	265	281	310	275
74.6.231.20	21	0	6	6	269	282	307	269

Figure 22. Implementation of Yahoo traffic steering to ISP1 on the Win MTR application

In Figure 22 there is a test on yahoo.com with 21 hops, where the first IP hop is the client IP 192.168.1.1 and the second hop is the ISP1 IP 192.168.1.1. It can be seen in the yahoo.com test that it succeeded in steering the application to ISP1 with the final destination being 74.6.231.20 which is the Yahoo server itself.

Disable Enable Testing ISP 1 and ISP 2

In this testing process, ISP1 nat will be disabled, its function is to see whether access to the browser is successful or not and also access to YouTube. The traffic steering success test can be seen in this process if only YouTube can be accessed when the ISP1 NAT is off. As seen in Figure 25, ISP1's NAT is disabled and the browser cannot be accessed.

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

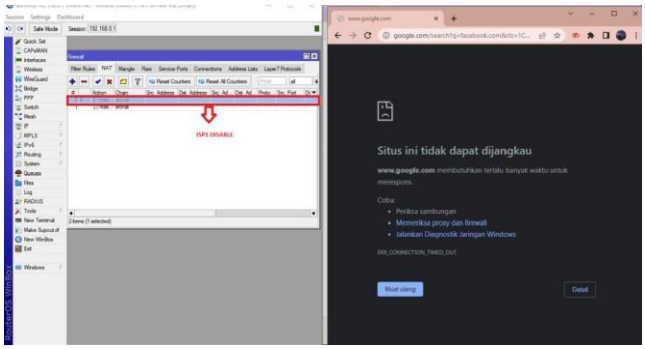


Figure 23. Disable NAT ISP 1

After testing disable the NAT for ISP1, then set it back to enable on ISP1 to prove that access to the browser was successful. It can be seen in Figure 24.

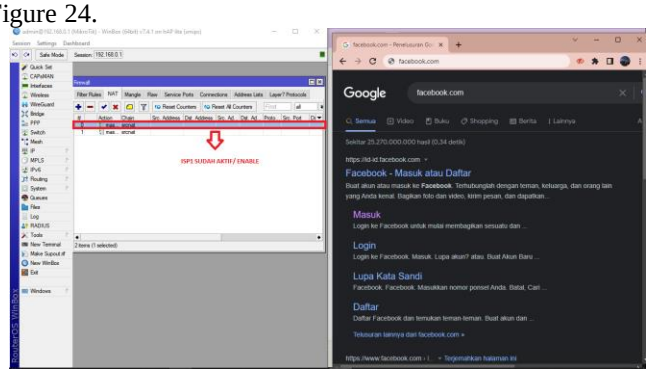


Figure 24. Enable NAT ISP 1

The next test is disabling ISP2 to prove whether YouTube can be accessed or not if ISP2 is turned off. It can be seen in Figure 25.

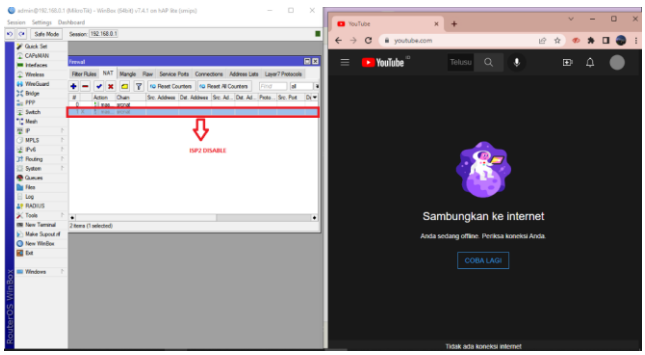


Figure 25. Disable NAT ISP 2

The image above is proof that traffic steering for the YouTube application can only be done via ISP2, and if ISP2 is off, YouTube will not get an internet connection even though ISP1 is still on. Next, test enable on ISP2 to regain internet connection on YouTube. Seen in Figure 26, the enable process on ISP2.

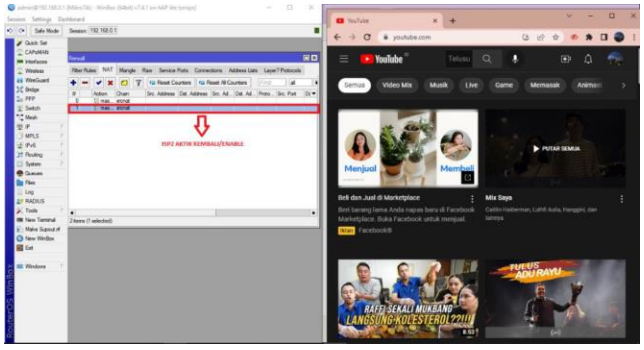


Figure 26. Enable NAT ISP2

PERFECT
JOURNAL OF SMART ALGORITHMS

E-ISSN: 3064-0377
Volume 1, **Number** 2, July 2024
https://doi.org/10.62671/perfect.v1i2.10

Testing ISP1 and ISP2 Traffic

In the traffic testing process between the two ISPs, the process of activating video streaming on YouTube will be carried out to get the results of which traffic runs if YouTube is activated. It can be seen in Figure 27.

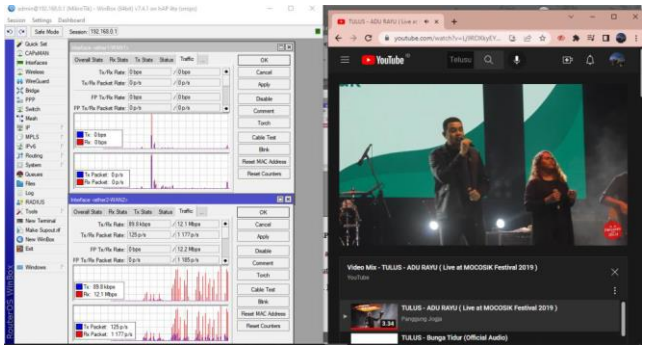


Figure 27. YouTube Traffic Testing

It can be seen from the picture above that the traffic that is running is ISP2 traffic because the access process carried out is YouTube which is steered via ISP2. Meanwhile, on ISP1, traffic only runs at the beginning, which is because before direct access to YouTube you have to go through a browser first.

CONCLUSION

1. Based on the results of this preparation and discussion, conclusions can be drawn in accordance with the research objectives.
2. Traffic Steering is an additional technique applied to network traffic, especially when filtering, modification or optimization is required. Network operators usually use Traffic Steering to expand the value of VAS or value added service (Value Added Service which refers to additional services (content) based on existing telecommunications networks).
3. The implementation of traffic steering in this final project report takes two examples of web servers being tested, namely browser steering on ISP1 and YouTube steering on ISP2.
4. Traffic steering on two web servers has been tested. When one of the ISPs goes down, the web server that is being steered by that ISP cannot be accessed or vice versa. Disabling the ISP is found in Firewell NAT (Network Address Tranlation).

REFERENCES

Anton, A., & Irman, A. (2024). Implementasi Load Balance Mikrotik Dual ISP Dengan PCC dan Metode Failover Pada PT. Wahana Ciptasinatria. *Jurnal Teknologi Informasi*, *10*(1), 9–16. https://doi.org/10.52643/jti.v10i1.4318

Azmi, K., & Razi, F. (2022). Studi Penggunaan Dua Isp Dengan Load Balancing Dan Failover Untuk Meningkatkan Kinerja Jaringan Berbasis. *Jurnal Tektro*, *06*(02), 176–183.

Nasir, F. (2020). Analisis Kinerja Load Balancing Jaringan 4G Pada Pc Router Mikrotik Menggunakan Metode PCC. *Tugas Akhir, Universitas Semarang*.

Putra, A., & Anton, A. (2024). Implementation of Load Balancing With PCC Method And Failover Using Mikrotik At PT. Maxpower Indonesia. *JISA(Jurnal Informatika Dan Sains)*, *7*(1), 78–82. https://doi.org/10.31326/jisa.v7i1.2022

Rahmat, B. M. R. (2022). Implementasi Load Balancing Metode Per Connection Classifier Dan Failover Recursive Menggunakan Mikrotik. *JSR : Jaringan Sistem Informasi Robotik*, *6*(2), 284–289. https://doi.org/10.58486/jsr.v6i2.163

Susafa'ati, S., Raharjo, M., & Aldori, R. (2024). Per Connection Classifer Load Balancing dengan Mikrotik pada SMK Tunas Harapan Jakarta. *Jurnal Teknik Komputer*, *10*(1), 7–12. https://doi.org/10.31294/jtk.v10i1.15183

Syahrani, A. H., & Yuliadi, B. (2023). Load Balancing On Mikrotik at Karang Jaya Health Center Using NTH Method. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, *11*(2), 267–282. https://doi.org/10.33558/piksel.v11i2.7107

Taufan, M., Zaen, A., & Tantoni, A. (2023). Analisis dan Implementasi Pengalihan Trafik Data (Failover) Akses Internet Pada Dua ISP. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *4*(3), 1726–1736. https://doi.org/10.30865/klik.v4i3.1336

Utomo, A. D. (2011). Implementasi Load Balancing Dua ISP Menggunakan Mikrotik. *Skripsi, Universitas Islam Negeri Syarif Hidayatullah*.