

# Captive Portal Development for Hotspot Services using Simple Queue Method

Saputra Bahrul Ilmi  
Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

Imam Riadi  
Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

## ABSTRACT

Hotspot as a Wireless Local Area Network (WLAN) based network has become a commonly used place to fulfill internet needs. Uneven bandwidth sharing is often a problem in providing hotspot services. The purpose of this research is to build an internet network. This research uses a proxy router with a simple queue method as a user regulator. This research collects data from literature studies, field studies, design, implementation, and performance evaluation of captive portal development on hotspot services using a proxy router with the simple queue method. Based on the data collection results, this report compares the results of ping, downloading, and uploading before and after the captive portal application with the simple queue method. Based on the results of captive portal research as a performance evaluation in this study, the results obtained before the application of bandwidth restrictions using the simple queue method get a ping value of 10 ms, download 23.2 Mbps, and upload 64.1 Mbps. The research results after implementing bandwidth restrictions using the simple queue method obtained a ping value of 8 ms, download of 1.7 Mbps, and upload of 1.8 Mbps. The results of this study can be concluded that users get internet access with more even speeds.

## Keywords

Network, Bandwidth, Simple Queue.

## 1. INTRODUCTION

Hotspot is a collection of networks based on a Wireless Local Area Network (WLAN) with the 802.11a/b/g Standard, which serves signal limitations where users, when wanting to connect to the network, must be within the vicinity of the hotspot location [1]. The IP address is a term used to designate an address that distinguishes one computer from another, and numbers are used to distinguish these addresses. This numbering system consists of IP Version 4 and IP Version 6 [2]. Bandwidth is a measurement of data or information that can flow from one place to another within a network at a specific time [3]. In using hotspot-based internet services, we often encounter internet users who only enter the password of the SSID or WiFi address available without any authentication and monitoring of users. As a result, network administrators need clear information about the identity of connected users. Mikrotik routerOS is an operating system that transforms computer systems into network routers with various features, including Firewall and NAT, Routing, Hotspot, Point Tunneling Protocol, DNS Server, DHCP Server, and other functionalities [4]. Mikrotik provides network management through a software package called user manager. The User Manager package is designed to regulate bandwidth and usage time for hotspot users [5]. Simple queue is a feature in mikrotik routerOS that enables bandwidth management in network scenarios [6]. The Simple queue method is capable of

performing bandwidth management on packets that have been marked.

In using hotspot-based internet services, we often encounter internet users who only enter the password of the SSID or WiFi address available without any authentication and monitoring of users. As a result, network administrators do not have clear information about the identity of connected users. This research develops a hotspot-based network using the simple queue method as an internet user management tool. With user management, hotspot-based internet services are expected to help network administrators manage and monitor users connected to the hotspot.

## 2. LITERATURE STUDY

### 2.1 Computer Network

Computer network is a series of systems consisting of a computer to another computer and from one device to another connected as one unit. Computer Network can generally be categorized into:

1. Local Area Network (LAN)  
A local Area Network is a network concept that connects network devices within the scope of a close distance. This network range is used in schools, universities, home offices, and others [7].
2. Metropolitan Area Network (MAN)  
Metropolitan Area Network is a concept that connects devices from one city to another with a relatively broad scope. This network range is used in one city with another district with another district [8].
3. Wide Area Network (WAN)  
Wide Area Network is a concept that connects network devices between one country and another with a broad scope. Network coverage is used in one country with another country [9].

### 2.2 Internet Protocol Address

Internet Protocol Address or IP address is an address that distinguishes one computer from another [10]. To distinguish these addresses, IP addresses use numbers consisting of Internet Protocol Version 4 and Internet Protocol Version 6 [11]. Subnet Mask aims to break or divide the network on a computer so that it can become smaller subnet. Network ID is used to identify a network from other networks, and then Host ID serves to identify hosts in a network [12]. IP addresses are divided into several classes;

1. IP Class A  
The first Class A starts from the numbers 0000 0000 (0) has an Internet Protocol range of 0 – 127 and has a maximum number of hosts of 16,777,214.[13].

2. IP Class B  
The first class B starts at 1000 0000 (128) with an Internet Protocol range of 128 – 191 and has a maximum host of 65,534.
3. IP Class C  
The first class C starts at 1100 0000 (192) with a total Internet Protocol range of 192 – 223 and has a maximum number of hosts of 254.

## 2.3 Network Topology

There are types of networks that are grouped based on network topology, namely;

1. Star Network Topology  
The Star network topology is a network architecture with a link as a center using a HUB or switch device as the center point. The function of the HUB or switch is the central point for connecting one computer device to another. The Star topology is commonly used in offices, homes, schools and other institutions in local area networks. Star topology can be seen in Figure 1 [14].

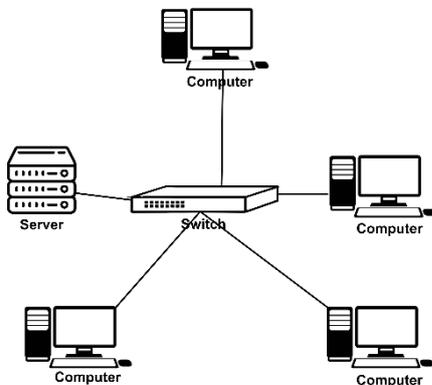


Figure 1. Star Topology

2. Mesh Network Topology  
Mesh network topology is a network topology that can connect one computer device to another randomly or irregularly. The mesh topology, when sending data goes directly to the destination device. In contrast, other topologies, when sending data, must pass through another device before arriving at the destination device. The mesh topology can be seen in Figure 2.

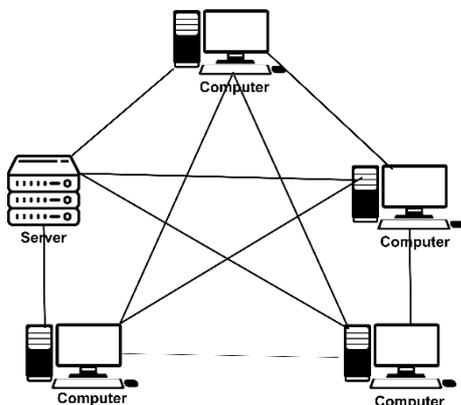


Figure 2. Mesh Topology

3. Tree Network Topology  
The Tree network topology is a topology that branches or branches like a tree. Making connections between devices requires a HUB or Switch as a data transfer medium. Tree topology (tree), also called hierarchical topology, is a type of network topology often used in large organizations, such as companies or universities. The Tree topology can be seen in Figure 3.

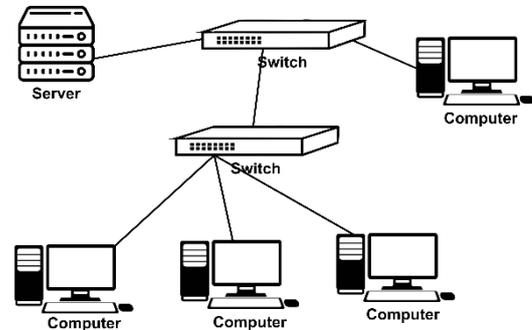


Figure 3. Tree Topology

## 2.4 Bandwidth Management

Bandwidth management is a feature in mikrotik that can be used to manage and optimize the performance of various types of networks by implementing Quality Of Service (QoS) services to determine the type of traffic on a network [15]. QoS is the ability to describe the efficiency level in a telecommunication system [16]. Bandwidth management mechanism to prevent bandwidth usage monopoly so that all customers get their bandwidth ratio [17]. Simple queue is one of the features on mikrotik routerOS to perform bandwidth management in network scenarios [18], and the simple queue method is capable of managing bandwidth for packets that have been marked. The simple queue method is a feature method for sharing or queuing internet bandwidth on a proxy, which is usually used for small and medium networks because the bandwidth distribution system is per user [19]. Simple queue can manage download and upload traffic to each user [20].

## 3. METHODOLOGY

### 3.1 Research Scenario

This scenario is made to explain how the difference is before applying a bandwidth limitation and after applying a bandwidth limitation. This research scenario was conducted by conducting network diagnostics and designing computer networks using the research topology to carry out measurements. This research measurement uses three parameters: ping, download, and upload. Ping is used to test whether a computer can connect with other computers. Download is used to test requests from local to internet servers. Upload is used to test delivery from local to internet servers [21]. This research uses the Research and Development method, which is a research method that can produce a product that has products by the area of expertise and has an effectiveness of a product. This research aims to realize a hotspot network using the simple queue method on a voucher-based internet network. The research phase that will be carried out in the research and development of a voucher-based internet product using the simple queue method can be seen in Figure 4.

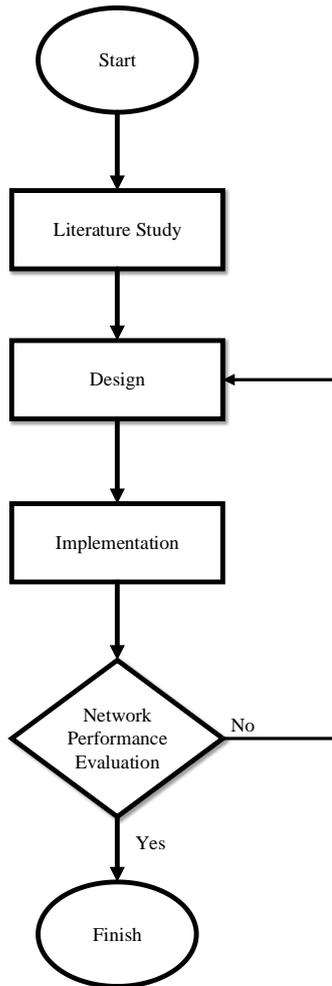


Figure 4. Flowchart Research Stage

### 3.2 Design

1. Internet Provider  
ISP is an Internet Server Provider as an Internet service provider; an ISP has an IP of 192.168.0.1/24 with a Subnet Mask of 255.255.255.0. Then, the ISP distributes IP to its partners as an IP DHCP Server from the ISP.
2. Mikrotik Router  
This mikrotik router is located at BinbunNet. BinbunNet, as an ISP partner, gets an IP of 192.168.0.2/24 with a Subnet Mask of 255.255.255.0 and a gateway of 192.168.0.1 with ether1 as the recipient of the IP from the ISP. Thus, the mikrotik router can already connect to the ISP. To send an internet connection, the proxy router provides a DHCP Server IP by providing ether3 and ether4 ports as bridge ports that are continuous with each other. The proxy router provides a DHCP Server IP of 192.168.1.1/24 with a subnet mask of 255.255.255.0 gateway 192.168.1.1. To connect the Admin PC to the router, the router offers an IP on ether2 with IP 192.168.88.1/24 subnet mask 255.255.255.0 and gateway 192.168 .88.1
3. Access Point  
The access point plays a role in spreading internet signals to devices connected via radio waves [22]. To receive as a liaison for mikrotik routers that are propagated via a radio wave-based network, the access point provides IP Local Area Network configuration 192.168.1.2/24 with a subnet

mask of 255.255.255.0 and gateway 192.168.1.1. It turns off the design on the DHCP Server menu with an access point. So that when the user connects to the access point, the user gets an IP from the proxy IP DHCP router.

4. User 1, User 2, User 3, User 4  
Users participate as hotspot service users; each gets a DHCP IP from the proxy router. User 1 Gets IP 192.168.1.3/24 subnet mask with 255.255.255.0 and Gateway 192.168.1.1, Then User 2 Gets IP 192.168.1.4/24 subnet mask 255.255.255.0 and gateway 192.168.1.1/24. User 3 gets IP 192.168.1.5/24 by having subnet mask 255.255.255.0 and gateway 192.168.1.1. To see the design results can be seen in Figure 5.

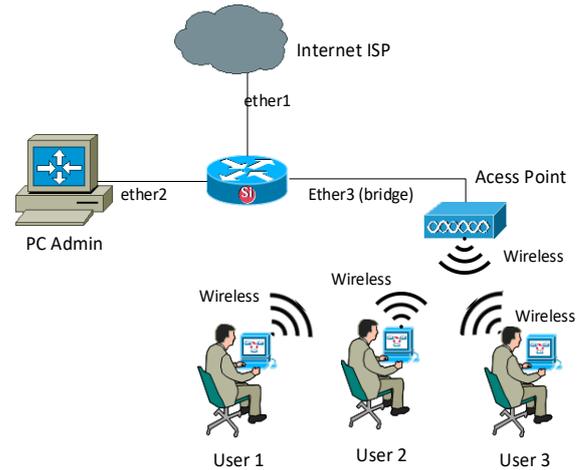


Figure 5. BinbunNet Local Area Network Design

5. Hardware  
The use of hardware in the tools and materials of this study can be seen in Table 1.

Table 1. Hardware used In The Research

No	Hardware		Quantity
	Name	Specification	
1	Laptops	Brand : HP Probook 430 G2 Processor : Core i5 gen 5 Memory RAM : 16 GB Storage : SSD 256 GB	1
2	Router Mikrotik	Router Mikrotik HaP Lite RB941-2nD CPU : 650MHz RAM : 32 MB Wireless : dual chain 2.4GHz	1
3	UTP and RJ 45 cables	UTP Cable Brand CAT 5E	1
4	Access Point	Access Point TP-Link	1

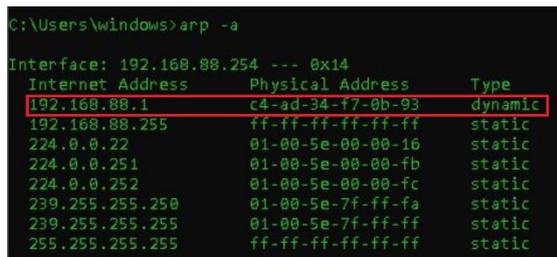
6. Software  
The use of software in the tools and materials of this study can be seen in Table 2.

**Table 2. Software used In the Research**

No	Software	Description
1	Putty	Putty is software that is used to control proxy hardware remotely. Using Putty software, you can configure the proxy.
2	Microsoft Visio	Microsoft Visio is a computer tool that functions to create network topologies or draw network schematics.
3	Google Chrome	It is a web browser tool that functions to browse the internet. As shown in the picture

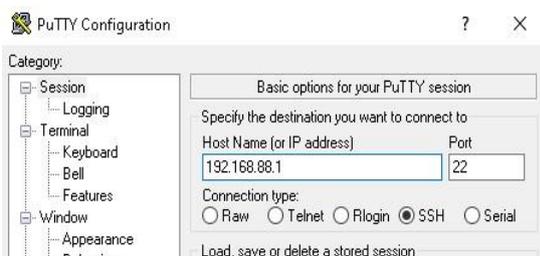
### 3.3 Implementation

- Internet Provider Login Router Mikrotik  
To log into the mikrotik router, the administrator must know the IP of the mikrotik router. To find out the IP of the mikrotik router, open a command prompt in windows by pressing the windows icon + r simultaneously, then typing the command "cmd" to open the command prompt. After opening the command prompt, type "arp-a" to see how many IP routers are the proxy. This can be seen in Figure 6.



**Figure 6. Show the IP address of the Proxy Router**

The "arp -a" command displays the address resolution protocol table, which displays the IP address connected to the computer. After executing the arp -a command, the IP address appears; it can be seen that the proxy IP is 192.168.88.1. After knowing that the mikrotik router IP is 192.168.88.1, we will log in to the mikrotik router. If logging in using the putty application, we must open it to configure it. After opening the putty application, provide the Host Name table column with IP 192.168.88.1 with port 22. The configuration can be seen in Figure 7.



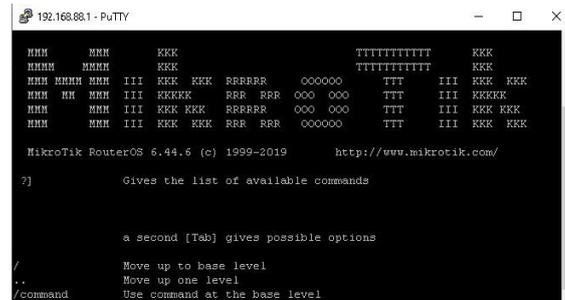
**Figure 7. Putty Configuration**

After filling in the Hostname and Port click Menu. Then it will open a login window. Enter login as: admin. Then press enter on the keyboard. These steps can be seen in Figure 8.



**Figure 8. Display Login using Putty**

After logging in, a text that says mikrotik will appear, as shown in Figure 9.



**Figure 9. Display after Logging in to the Router using Putty**

In Figure 9, it can be concluded that logging in via the putty application has been successful.

- DHCP Client Configuration  
For the proxy router to get internet access rights from the ISP, the router must be configured with a DHCP Client to get an internet connection. Configuration via putty can be seen in Code 1.

#### Code 1. DHCP Client

```
/ip dhcp-client
```

Code 1 explains that to enter the DHCP Client menu, enter the IP menu and then the DHCP Client menu. After entering the DHCP Client menu, add ether1 as a DHCP Client IP recipient from the ISP. To configure adding ether1 as DHCP Client can be seen in Code 2.

#### Code 2. Added DHCP Client on ether1

```
add interface=ether1
```

Code 2 explains that port ether1 is added as DHCP Client.

- NAT Firewall Configuration  
After the IP DHCP Client configuration provided by the ISP, the router must configure Network Address Translation, commonly known as NAT [23]. The function of NAT is to translate the local IP to the public IP address the ISP has provided. To configure NAT on a proxy router. To configure NAT on a proxy router, see Code 3.

#### Code 3. Enter the NAT menu

```
/ ip Firewall nat
```

The code 3 explains that to enter the NAT menu, enter the menu "IP", → "Firewall", → and "NAT". After entering the NAT menu, to configure NAT, see code 4.

#### Code 4. NAT Configuration

```
/ add chain=srcnat  
action=masquerade out-  
interface=ether1
```

Add NAT rules by specifying packets that have left the router or the term is outgoing. Then "action=masquerade" explains that the IP address of the local network packet will be replaced by the public IP address provided by the ISP. "out-interface=ether1" specifies that the ether1 port performs a masquerade action.

4. Bridge port Configuration on the proxy router  
For the proxy router to get internet access rights from the ISP, the router must be configured with a DHCP Client to get an internet connection. Configuration via putty can be seen in Code 5.

#### Code 5. Bridge Configuration

```
/ interface bridge add  
name=bridge1
```

The code 5 explains entering the bridge menu and adding a bridge by name bridge1. Then, after making the bridge name, add the ether3 and ether4 ports to the bridge port. To configure the port combination on the bridge can be seen in the code 6.

#### Code 6. Port Configuration for bridge

```
/interface bridge port add  
bridge=bridge1 interface=ether3  
/interface bridge port add  
bridge=bridge1 interface=ether4
```

Code 6 explains that the bridge port interface adds ether3 as bridge1, and the bridge port interface adds ether4 as bridge1. So that ether3 and ether4 become one unit, then it can be concluded that the bridge configuration has been completed.

5. IP Address configuration on the bridge  
So that the bridge can be recognized, the bridge must be configured with an IP address to configure the IP address on the proxy via text mode, which can be seen in Code 7.

#### Code 7. IP Address Configuration On Bridge port

```
/ ip address add  
address=192.168.1.1/24  
interface=bridge1
```

Code 7 explains that enter the IP Address menu and then add IP Address 192.168.1.1/24 with bridge1 interface. Then bridge1 has been configured with IP address 192.168.1.1/24, bridge1 includes ether3 and ether4. So that ether3 and ether4 become one unit.

6. Configuration of DHCP Server Router  
In the mikrotik DHCP Server configuration, the aim is for the client to get an IP automatically from the router so that the client does not need to configure the IP manually [24]. To do this configuration can be seen in the code 8.

#### Code 8. Pool Configuration on DHCP Server

```
/ip pool add name=my-pool  
ranges=192.168.1.2-192.168.1.254
```

Code 8 explains that entering the IP menu creates a pool by adding the pool name my-pool with the IP range 192.168.1.2 – 192.168.1.254. After configuring the pool create a DHCP Server configuration, which can be seen in the code 9.

#### Code 9. Pool Configuration on DHCP Server

```
/ip dhcp-server add name=my-dhcp  
interface=bridge1 address-pool=my-  
pool
```

Code 9 explains how to enter the IP menu and then the DHCP Server menu; then, add DHCP with the name my-DHCP and interface bridge1 and the address from my-pool. The meaning of my-pool is the IP range of the 9 code. After the configuration, create a network on the DHCP Server. The command can be seen in the code 10.

#### Code 10. Pool Configuration on DHCP Server

```
/ip dhcp-server network add  
address=192.168.1.0/24 gateway=192.1  
68.1.1 dns-server=8.8.8.8,1.1.1.1
```

The code 10 explains how to configure the network on the DHCP Server by entering the IP menu, then DHCP Server after that to the network menu, and adding the network address 192.168.1.0/24 and the gateway 192.168.1.1 with the IP DNS Server 8.8.8.8, and 1.1.1.1. DNS Server 8.8.8.8 belongs to Google company, and DNS Server 1.1.1.1 belongs to Cloudflare company.

7. Hotspot Configuration on Mikrotik Router  
Hotspot configuration aims to provide authentication services to clients so that when accessing the internet, the client must authenticate before surfing the internet [25]. To configure the hotspot can be seen in the code 11.

#### Code 11. Hotspot Configuration

```
/ip hotspot setup
```

The code 11 explains how to enter the menu, go to the hotspot, and set up a hotspot. After carrying out the command in code 11, when the command is running. After the command runs, a display will appear to select the hotspot interface. On the hotspot interface menu, select bridge1; the function of this hotspot interface is to select the target where the hotspot originates. Then, for the local address of the network, enter IP 192.168.1.1/24; the function of the local address of the network is to determine the default IP from bridge 1. On the masquerade network menu, enter yes; on the masquerade network, it allows traffic from users connected to the hotspot to be NAT. Then, for the address pool of the network, enter the IP 192.168.1.2-192.168.1.254. The address pool of the network functions to set the client's IP range. On the select certificate menu, enter none because it does not have an SLL certificate, then select none. Next, on the IP address of the SMTP server menu, enter 0.0.0.0. After that, on the DNS servers, enter the mikrotik router IP and Google IP 192.168.1.1, 8.8.8.8. On the DNS name menu, enter binbun.co.id on the name of the local hotspot menu. The user enters adminbibun and the password for the user binbunadmin, so when the user will login, use the username and password that has been created. To see the configuration of the hotspot can be seen in Figure 10.

```
[admin@MikroTik] > /ip hotspot setup
Select interface to run HotSpot on

 hotspot interface: bridge1
Set HotSpot address for interface

 local address of network: 192.168.1.1/24
masquerade network: yes
Set pool for HotSpot addresses

 address pool of network: 192.168.1.2-192.168.1.254
Select hotspot SSL certificate

 Select certificate: none
Select SMTP server

 ip address of smtp server: 0.0.0.0
Setup DNS configuration

 dns servers: 192.168.1.1,8.8.8.8
DNS name of local hotspot server

 dns name: binbun.co.id
Create local hotspot user

 name of local hotspot user: adminbinbun
password for the user: binbunadmin
```

Figure 10. Configuration Hotspot Router Mikrotik

Before creating a user profile hotspot, it would be nice to create a simple queue script so that hotspots can automatically appear in the simple queue. Can be seen in the code 12.

**Code 12. Simple Queue Script Configuration with Hotspot**

```
/system script add name=script1
source=" :local username [/ip hotspot
active get [find user=\$user] user];
:local limit [/ip hotspot user profile
get [find name=\$username] rate-
limit]; :local maxLimit [/ip hotspot
user profile get [find name=\$username]
rate-limit-ceil]; /queue simple add
name=\$username target-
addresses=\$username parent=global-in
packet-marks="" priority=8/8 limit-
at=0/0
```

Code 12 aims for a simple queue to display clients connected to hotspots. The explanation for code 12 is to enter the system menu. In the script sub-menu, add a script with the name script1 by loading the source code, taking the user from the hotspot user, then taking the speed limit from the user profile, creating a simple queue rule with the hotspot username, and setting limit-at and max-limit from the hotspot user profile. The proxy router must be configured according to each user profile for the user to connect to the hotspot according to the voucher purchase. Configure user profiles can be seen in the Code 13.

**Code 13. Hotspot Configuration Simple Queue**

```
/ip hotspot user profile add
name=1day shared-users=1 rate-
limit=2M/2M session-timeout=1d
on-login=" :global user
```

The code 13 above explains that it aims to create a user profile on the proxy hotspot. The function of the user profile is to set internet usage access policies for clients connected to the proxy router. The script above explains that entering the IP menu. Hotspot goes to the user profile menu tab, then adds a user profile with a one-day name and only one device can be connected, and the session is only one day with a download speed of two Mbps and an upload speed of two Mbps. To create a user or client name

on the hotspot can be done with the command as in code 14.

**Code 14. Create User Hotspot**

```
/ip hotspot user add name=bahru1
profile=1day password=bahru122
```

Code 14 explains that to create a hotspot user by going to the "IP" menu → "hotspot," → entering the "user" menu tab → , adding the name bahru1 with a one-day profile and the password bahru122. To see connected users can be done using Code 15.

**Code 15. Simple Queue**

```
/queue simple print detail
```

The results of Code 15 can be seen in Figure 11.

```
[admin@MikroTik] > /queue simple print detail
Flags: X - disabled, I - invalid, D - dynamic
0 D name="<hotspot-aj1"> target=192.168.1.2/32 parent=none packet-marks=""
priority=8/8 queue=default-small/default-small limit-at=2M/2M
max-limit=2M/2M burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s
bucket-size=0.1/0.1
1 D name="hs-<hotspot1"> target=bridge1 parent=none packet-marks=""
priority=8/8 queue=hotspot-default/hotspot-default limit-at=0/0
max-limit=0/0 burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s
bucket-size=0.1/0.1
```

Figure 11. Simple Queue View User

8. Access Point Configuration

In the access point configuration, there is no need for a password name, only applying the SSID replacement shown in Figure 12.

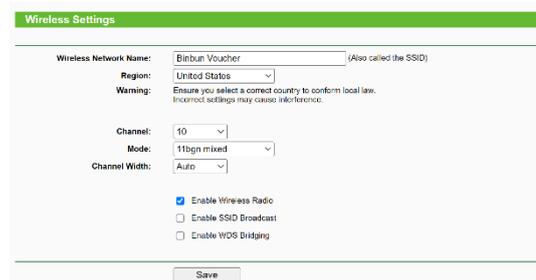


Figure 12. Access Point SSID Configuration

Figure 12 illustrates the configuration of the wireless network name with the name Binbun Voucher, with channel 10, which means radio frequency channel 10, and 11bgn mixed mode. As well as activating wireless radio and activating SSID broadcast. Then, when the user accesses the device to the access point and gets an IP from mikrotik, the DHCP access point is switched to disable mode, as shown in Figure 13.

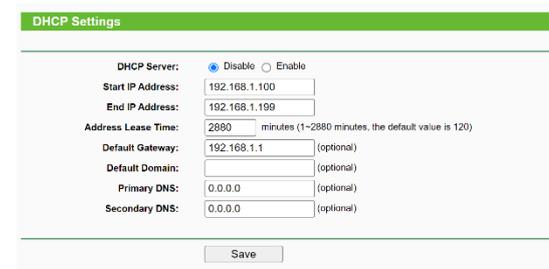


Figure 13. DHCP Access Point Configuration

Figure 13 explains that the IP DHCP Server from the access point is disabled because the client, when

connected to the access point, gets a DHCP IP from the proxy router, not from the access point. In this case, the access point only acts as a spreader of radio signal access.

#### 4. RESULT AND DISCUSSION

This chapter shows the evaluation stage. The first evaluation step is that the client connects to the WiFi hotspot. Then, after the client is successfully connected, the client gets the mikrotik router IP address. Figure 14 can be used as a reference to find out the results of the first evaluation.

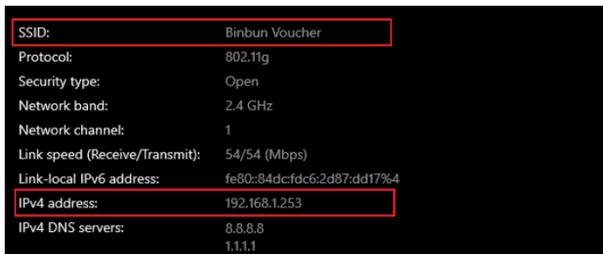


Figure 14. Client has DHCP IP from Router

Figure 14 explains that after connecting to the access point, the user gets an IP from the router with IP 192.168.1.253 and the user is already connected to the SSID Wifi Binbun Voucher. After getting the IP, the user will be directed to a web page containing the username and password. To be able to see hotspot login authentication can be seen in Figure 15.



Figure 15. User Interface When Login Hotspot

The result of the second test is to check the internet network connection using the speedtest.cbn.id website. This application displays three results types: ping, download, and upload. The following is an image showing the state of the hotspot network before and after implementing the captive portal using the simple queue method. Figure 16 shows the test results before implementing the captive portal.

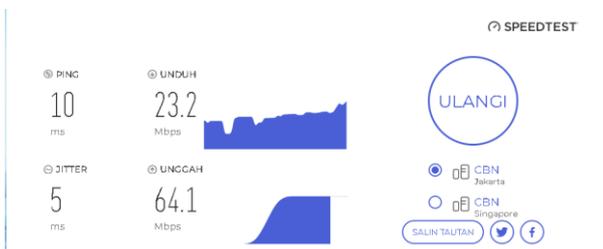


Figure 16. Test Results before implement

Based on Figure 16 above, it can be seen that the internet connection is running. The ping value obtained is 10 ms, the jitter gets a value of 5 ms, the download gets a value of 23.2 Mbps, and the upload gets a value of 64.1 Mbps. Then, in Figure 17 are the test results after implementing the captive portal using the simple queue method.

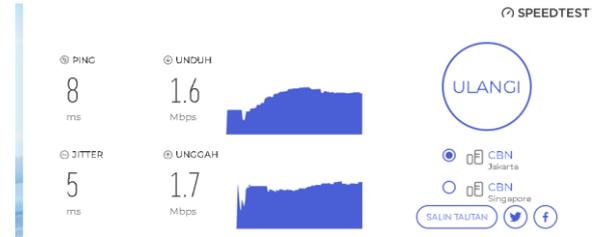


Figure 17. Test Results after implement

Based on figure 17 it can be seen that the internet network connection is running, and has a ping value of 8 ms, Jitter 5 ms, download 1.6 Mbps and upload 1.7 Mbps. In Table 6 it can be seen that the results of the comparison of the ping, download, upload values before and after implementing captive portal. To see a comparison before and after the application of bandwidth limitations can be seen in table 3.

Table 3. Recapitulation Before and after measurement Hotspot using Captive Portal

Test Category	Result Before Limitation	Result After Limitation
Ping	10 ms	8 ms
Download	23.2 Mbps	1.6 Mbps
Upload	64.1 Mbps	1.7 Mbps

Table 3 explains that the ping table gets a ping value of 10 ms before applying the bandwidth limitation method. After applying the bandwidth limitation method, it gets a ping value of 8 ms, which means a faster speed. In the download table, before applying the bandwidth limitation, get 23.2 Mbps, but after applying the bandwidth limit, get a bandwidth speed of 1.6 Mbps. Then, the upload table explains that before applying the bandwidth limitation, get a speed of 64.1 Mbps. After applying the bandwidth limit, get a bandwidth capacity of 1.7 Mbps. Upload and download are limited to 2 Mbps / 2 Mbps, which means the internet speed per client cannot exceed 2 Mbps. This study's results show that bandwidth distribution per client is evenly distributed and obtains a download and upload limit speed of 2 Mbps.

#### 5. CONCLUSION

The design in this study aims to efficiently meet the needs of network design so that the architecture includes software and hardware according to the needs of internet voucher services. This study aims to design and implement a bandwidth-sharing system according to needs, using the simple queue method on mikrotik routers. Internet network traffic on the router is carried out by dividing groups based on user profiles to ensure that the bandwidth allocation for each client gets according to needs. Implementation on a hotspot network with the simple queue method obtains the difference in data before and after applying the bandwidth limit before applying the ping limit of 10 ms, download 23.2 Mbps and upload 64.1 Mbps. After applying the simple queue method to bandwidth limitations, the known results from users are 8 ms ping, 1.7 Mbps download and 1.8 Mbps upload. It can be concluded that the captive portal on the hotspot service has been successfully created.

#### 6. REFERENCES

[1] D. A. Riefi, T. Y. Arif, and Syahrial, "Evaluation of the Effect of TIM Parameters Based on Multirate on Energy Consumption of IEEE 802.11ah Network," J. RESTI (Journal of Information Systems Engineering and Technology), vol. 5, no. 4, pp. 713–720, 2021, doi: 10.29207/resti.v5i4.3224

- [2] B. K. Simpony, "Simple Queue for User and Bandwidth Management in Hotspot Networks Using Mikrotik," *J. Informatics*, vol. 8, no. 1, pp. 87–92, 2021, doi: 10.31294/ji.v8i1.9385.
- [3] D. Al Kautsar and L. Nulhakim, "Bandwidth Management Using Simple Queue Method at Subur Graphic Store, Central Jakarta," *J. Informatics Technological College*, vol. VI, no. 2, pp. 63–70, 2020.
- [4] D. S. Tampubolon, Hanifah Aprilyani, and R. W. Pulungan, "Network Design and Bandwidth Management for Users Using Mikrotik in the Communication and Information Office of North Sumatra Province," *J. Computer Science and Informatics Engineering*, vol. 01, no. 1, pp. 26–37, 2022, doi: 10.55537/cosie.v1i1.28.
- [5] R. R. D. Marcus, H. E. Rosyadi, and F. Y. Pamuji, "Prototype of Computer Network Administration and Security System Based on Mikrotik DHCP Server," *Briliant Journal of Research and Conceptual Studies*, vol. 6, no. 3, p. 685, 2021, doi: 10.28926/briliant.v6i3.630.
- [6] S. Agung and H. Harafani, "Bandwidth Management Implementation Using Simple Queue Method at PT BPR Depo Mitra Mandiri," *JISN (Journal of Information Systems and Network)*, vol. 03, no. 01, pp. 2–5, 2022.
- [7] A. Dzulfiqri and A. Hidayat, "Bandwidth Management and Content Filtering Implementation Using Mikrotik Router at SMP Muhammadiyah 3 Metro," *J. Student Computer Science*, vol. 3, no. 2, 2022.
- [8] M. Gustiawan and R. J. Yudianto, "Hotspot Network Implementation in Offices to Improve Network Security," vol. 4, no. 4, pp. 244–247, 2021.
- [9] I. K. Astuti, "Computer Faculty INDAH KUSUMA ASTUTI Section 01," *Computer Journal*, p. 8, 2018, [Online]. Available: <https://id.scribd.com/document/503304719/computer-network>
- [10] F. M. Sinaga, S. J. Pipin, and H. Kurniawan, "Computer Network Installation Training Using Cisco Simulation at SMK Methodist Tanjung Morawa," vol. 4, no. 1, pp. 45–50, 2023, doi: 10.47065/jrespro.v4i1.3633.
- [11] S. Sikarti, "Simulation of Metro Ethernet Transport Network Planning Using Cisco Packet Tracer Application Version 6.2.0," vol. 1, no. 2, 2023..
- [12] B. Ahmad and T. Difa, "Computer Network Security System Using Proxy Server with Assessment & Hardening Method," 2020.
- [13] A. isador Harsapranata, "Analysis of DNS Utilized in Domain Filtering in WAN Networks Using Open Source," *J. IKRA-ITH Informatics*, vol. 3, no. 88, pp. 20–29, 2019, [Online]. Available: <https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/287>
- [14] R. Mujiastuti and I. Prasetyo, "Building an Integrated VPN-Based Network Security System with DNS Filtering PIHOLE," no. November 2021, 1846..
- [15] G. Feoh, P. W. Gunawan, T. Informatics, and U. D. Pura, "Implementation of Bandwidth Management with Hierarchical Token Bucket (Htb), Per Connection Queue (Pcq) and Layer 7 Protocol Methods Using a Mikrotik Router," vol. 1, no. 1, pp. 65–84, 2022, [Online]. Available: <https://jurnal.undhirabali.ac.id/index.php/jakasakti/index>
- [16] W. Setyanto and E. R. Nainggolan, "Simple Queue Using Mikrotik" vol. 10, no. 2, pp. 114–126, 2022.
- [17] M. Purwahid, J. Triloka, and S. M. K. N. Sukadana, "Quality of Service (QOS) Analysis of Internet Network to Support Computer Network Infrastructure Strategic Plan in SMK N I Sukadana," vol. 02, no. 03, 2019.
- [18] J. D. Santoso, "Comparison Analysis of Queue Methods," vol. VII, 2020.
- [19] R. Sopandi, H. Priyandaru, A. Taufik, and U. Saputra, "Bandwidth Management Implementation at SMK Darul Mu 'In," vol. 14, no. 2, 2023..
- [20] S. Agung et al., "Bandwidth Management Using Simple Queue Method at the Department of Communication and," *Molecular Biology*, vol. 03, no. 01, pp. 2–5, 2022.
- [21] B. Saputro, *Research and Development Management for Thesis and Dissertation Writers*, vol. 53, no. 9, 2017.
- [22] D. S. Lubis.Mhd, D. Hasannudin, J. Efendi, L. Wiljono, and M. Sufiani, "Building a Router in Computer Networks Using Ubuntu OS," *Kaputama Informatics Journal*, vol. 4, no. 2, pp. 111–125, 2020.
- [23] H. Rahmatullah and S. Nadenggan, "Analysis of Local Area Network Performance using Quality of Service," vol. 183, no. 46, pp. 43–51, 2022..
- [24] A. Wicaksana and T. Rachman, "Design of Internet PC Router with Network Address Translation (NAT) Using Windows 2003 Server Case Study: DEPARTEMEN AGAMA KAYUAGUNG," vol. 3, no. 1, pp. 10–27, 2018,[Online]. Available: <https://medium.com/@arifwicaksana/use-casedefinition-a7e576e1b6bf>
- [25] F. Ardianto, B. Alfaresi, and R. A. Yuansyah, "Mikrotik-Based Hotspot Network Using User Authentication Method," *J. Surya Energy*, vol. 2, no. 2, p. 167, 2018.