JAIIT (Journal of Advances in Information and Industrial Technology)
Vol. 7, No. 1 May 2025, ISSN 2716-1935, E-ISSN 2716-1927

The Model of Sharing Public IP Address Using Tunneling Protocol

Tomi Defisa[*1)], Thomas Budiman[2)], Anton Zulkarnain Sianipar[3)]
[1)]Department of Computing, University Malaysia of Computer Science & Engineering, Selangor, Malaysia
[2,3)]Department of Informatic Engineering, STMIK Jayakarta, Jakarta, Indonesia
[1*]P09220003@student.unimy.edu.my, [2]thomas@stmik.jayakarta.ac.id, [3]antonz.jayakarta@gmail.com

ARTICLEINFO

Article history:
Received 14 May 2025
Revised 30 May 2025
Accepted 31 May 2025
Available online 31 May 2025

Keywords:
Digital Transformation
EoIP
Internet Service Provider
PPTP
Tunneling

ABSTRACT

Digital Transformation cannot be separated from the support of Internet connections. The Global Internet Network only recognizes Public IP Address. The Internet Service Provider (ISP) will provide a Public IP Address to customers who subscribe to a business or Enterprise service. Companies with branch offices that subscribe to broadband internet services typically receive private IP addresses, which limits the availability of public IP addresses for systems or other purposes. This paper aims to utilize the Point-to-Point Tunneling Protocol (PPTP) and Ethernet over IP (EoIP) tunnel protocol features on MikroTik Routers for sharing a Public IP address, with a special focus on public IP Address version 4 (IPv4). Point-to-Point Tunneling Protocol (PPTP) is used to establish a Virtual Private Network (VPN) between the Head Office and Branch Office. Then, Ethernet over Internet Protocol (EoIP) is utilized to create a bridge network. Based on the test results, the Public IP Address was successfully detected on the internet network during bandwidth testing, and the route to the internet network was seen passing through the gateway from the Public IP address prefix of the Head Office. To demonstrate that Public IP Addresses can be used in Branch Offices. This model can be a solution for companies to share Public IP addresses between the head office and the Branch Office.

1. Introduction

In the era of Industry 4.0, all sectors are transitioning from local (offline) to Public (online) access systems. This aims to provide user convenience. The Internet network plays a crucial role in the digital transformation process; for a system to be accessed via the Internet network, a Public IP Address is needed. Currently, the average system on the internet network is still dominated by using IPv4. The limited number of IPv4 is a problem for companies during the migration process to IPv6 by all countries. An IP address is a unique identifier assigned to a computer for communication on a computer network. There are two types of IP Address, namely IP Address version 4 (IPv4) and IP Address version 6 (IPv6). IP addresses are unique; therefore, it is not allowed to use the same IP address within a single network [1]. Internet Service Providers (ISPs) provide increasingly widespread internet access to remote villages, as seen in the case of ISP [2]. Many Internet Service Providers (ISPs) offer various products with different features that customers receive, especially on Public IP Addresses, but subscription fees are more expensive compared to Broadband Internet services. Today's technologies are pushed to provide high-quality solutions with minimal operational costs, especially in terms of network and architecture. The tunneling method is a technology that handles and provides point-to-point connections from source to destination [3].

VPN solutions are used as one of the measures to accelerate company performance in terms of data transfer without having to spend more money [4]. In this study, the concept of sharing Public IP Addresses from the Head Office to the Branch office is applied via the internet network by building a Virtual Private Network (VPN). This concept requires the head office to have a Public IP Address. Virtual Private Network (VPN) is a method of utilizing an internet network that functions to create a relatively secure private network. Virtual Private Network (VPN) networks can be said to be safe

because the transmitted data packets will be encrypted to prevent eavesdropping by unauthorized parties [5]. Several protocols can be used to build a Virtual Private Network (VPN) network, including PPTP, L2TP/IPSec, OpenVPN, and IKEv2/IPSec [6]. The implementation of a virtual private network using the L2tp/IPsec protocol method was successful so that the VPN process remains safe from external attacks [7]. Virtual Private Network (VPN) allows you to help connect local networks between companies using an internet connection [8]. VPN network can be a solution for remote access to intranet networks via the internet [9]. The Point-to-Point Tunneling Protocol (PPTP) method is used to connect one location to another branch to make data exchange faster and safer [10]. The result of data encryption depends on the protocol used. Encryption on the Point-to-Point Tunneling Protocol (PPTP) protocol uses the Microsoft-Point-to-Point Encryption (MPPE) method with a 128-bit key.

Basically, for computers to communicate with each other, they must be connected to a computer network. A computer network is a communication system that allows computers to communicate with each other and exchange data [8]. Point-to-Point Tunneling Protocol (PPTP) was chosen because it supports multiple platforms and is easy to configure and maintain [11]. PPTP uses TCP port 1723; if the router blocks the port, then the router cannot communicate. Building a computer network cannot be separated from the function of hardware, namely the router. A router is a hardware device that is specifically designed to build a network so that computers can be connected to each other [12]. MikroTik Router is one of the routers that is widely used because it is affordable but has many features that can be utilized by users, such as building a Virtual Private Network (VPN). One of the benefits of Ethernet over Internet Protocol (EoIP) on MikroTik Routers is that it can build a direct and secure network path between the head office and the branch office [13]. Ethernet over Internet Protocol (EoIP) Tunnel is a feature on MikroTik RouterOS that builds a tunnel network between MikroTik RouterOS over a TCP/IP connection [13]. Designing a VPN using access built by EOIP can make it easier for employees to access company data and systems remotely by connecting computers between branches via the network [10]. The use of Ethernet over IP (EoIP) tunnel technology can solve the problem of automatic data backup between servers in the cyber data center and servers in the XYZ apartment [14]. Bridge interfaces are used to combine multiple physical interfaces into a single logical interface. On the other hand, virtual Private Networks (VPNs) play a crucial role in ensuring secure communication over public networks [15].

2. Methods

This study uses the research & development (R&D) method. This research is based on problems that often occur in several companies that have limitations on Public IP Addresses. Public IP Addresses are not only used for systems but are also used for remote device management or the use of Voice over Internet Protocol (VoIP). Each of these designs has its own architecture and method, depending on its needs and use cases [9]. This study also uses internet connections from 2 different companies and services. At the Head Office, the Dedicated Internet Access network from PT Trans Indonesia Superkoridor is used. While at the Branch Office, the Broadband Internet network is used by PT Telekomunikasi Indonesia Tbk. At the Head Office, already the Public IP Address is Static, while the Branch Office gets a Private IP after the Network Address Translation (NAT) process from the Internet Service Provider (ISP) gateway. This effort is made so that the Public IP from the Head Office can be used at the Branch Office. The global configuration steps are 1) Activation of Point-to-Point Tunneling Protocol (PPTP) server protocol, 2) Creation of Virtual Private Network (VPN) authentication, 3) Creation of EoIP Tunnel, and 4) Creation of Bridge Interface.

Then, after the Virtual Private Network (VPN) is connected between the Head Office and the Branch Office, a test is carried out on the use of a Static Public IP Address on the laptop that is directly connected to the Router. If successful, the laptop can connect to the internet. Next, a speed test tool is carried out to see the results of the Public IP Address used.

 DOI: https://doi.org/10.52435/jaiit.v7i1.691

3. Results and Discussions

3.1. Network Topology Design and Resources Allocation

a. Network Topology Design

In this study, the MikroTik Router is used to build network communication from the Head Office to the Branch Office. There are two types used, namely MikroTik RouterBoard RB3011 devices at the Head Office and RB750Gr2 at the Branch Office. Also, use one laptop for testing. Figure 1. is a network topology design, where the Head Office is a Virtual Private Network (VPN) server and the Branch Office is a client. On the Head Office router, Point-to-Point Tunneling Protocol (PPTP) Server and Ethernet over Internet Protocol (EoIP) configurations are activated. The basic concept of the Ethernet over Internet Protocol (EoIP) protocol requires a Remote Address to be addressed. In this study, the Branch Office as a Remote Address uses a Private IP Address that cannot be recognized from the Internet network, so the Ethernet over Internet Protocol (EoIP) protocol cannot be implemented. The solution to this problem is to first build a Virtual Private Network (VPN) using the Point-to-Point Tunneling Protocol (PPTP). The result of the Point-to-Point Tunneling Protocol (PPTP) connection is that it gets a Private IP Address allocation from the Head Office router, and after that, an Ethernet over Internet Protocol (EoIP) protocol network is built. Then, a bridge network is established between the interfaces. After the Virtual Private Network (VPN) is established, the next step is to test the Internet connection on a laptop directly connected to the router using the Public IP Address from the Head Office.

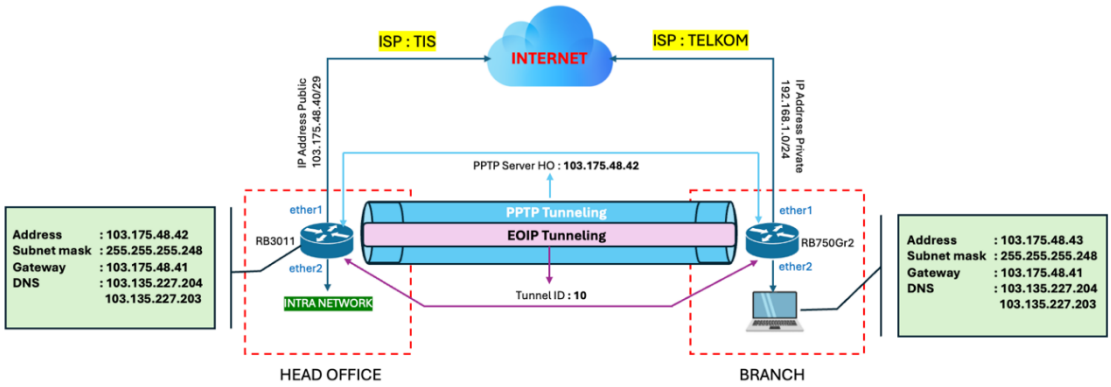

Figure 1. Network Topology Design

b. Resources Allocation

At this stage, an explanation is given regarding the technical requirements for building a tunnel network to be able to communicate between the Head Office and Branch Office.

Table 1. IP Address Mapping

Site	IP Address	Gateway	Interface	Internet Connection
Head Office	103.175.48.42/29	103.175.48.41	Bridge-EOIP	Dedicated
Branch Office	192.168.1.2/24	192.168.1.1	ether1	Broadband
Laptop	103.175.48.43/29	103.175.48.41	ether2	Broadband

Table 1 shows the allocation of IP Address for each router and Laptop. The public IP Address at the head office is given space from the Internet Service Provider (ISP) with a /29 subnet that gets 5 Public IP Addresses that can be used. In this study, 1 IP is used on the router as an internet gateway, and the 4 IPs are still available. This available IP will be used for testing on the Branch Office side. Specifically for the Head Office, the IP Address is used on the Bridge interface. Before the IP Address is directed to the bridge interface, a Bridge domain is first created on the Head Office router. On this bridge interface, the interface connected to the Internet Service Provider (ISP) as an Internet gateway and the Ethernet over Internet Protocol (EoIP) tunnel interface are registered as bridge members. On the Branch Office router, a domain bridge is also created with members of the ether2 interface and the

Ethernet over Internet Protocol (EoIP) interface. This aims to combine networks in one logic interface so that laptops in the Branch Office can use the Public IP Address. At the same time, the IP for the Branch Office router gets a Private IP Address from the Optical Network Terminal (ONT). Then, the Laptop in the Branch Office directly connects to the interface ether2 router using a LAN cable and the Public IP Address.

Table 2. PPTP Server Configuration

Site	Server	Enable	Profile	Authentication
Head Office	103.175.48.42/29	yes	default	mschap2 mschap1 chap pap

Table 2 is the PPTP Server configuration on the Head Office router. In the authentication option, all authentication methods are enabled to make it easier for clients to connect.

Table 3. PPTP Secret Configuration

Site	Name	Password	Service	Local Address	Remote Address
Head Office	eoip-branch	eoip-branch	any	192.168.20.65	192.168.20.65

Table 3 is a secret configuration that will be used by the client on the branch office router. The IP Local Address and Remote Address will be used for the EoIP Tunnel. The determination of the IP Local Address and Remote Address is adjusted to the network needs. However, it must be ensured that the prefix that will be used for VPN has not been used on other networks to avoid conflict.

Table 4. PPTP Client Configuration

Site	Server	Type	User	Password	Profile
Branch Office	103.175.48.42/29	PPTP-Client	eoip-branch	eoip-branch	default-encryption

Table 4 is the PPTP Client configuration on the Branch Office router. The client will perform the configuration on the Dial Out menu with the server Connection to 103.175.48.42. The Server IP must be adjusted on the Head Office router.

Table 5. Tunnel EoIP Mapping

Site	IP Address	Tunnel ID	Local Address	Remote Address
Head Office	EOIP-TO-BRANCH	10	192.168.20.65	192.168.20.68
Branch Office	EOIP-TO-HO	10	192.168.20.68	192.168.20.65

For Ethernet over Internet Protocol (EoIP) configuration, it must be configured on the Head Office router and Branch Office router. This is very different from the PPTP configuration, where neither is a server. In building an EoIP Tunnel, it is mandatory to pay attention to the Tunnel ID, Local Address, and Remote Address parameters. The Tunnel ID must be the same between the Head Office and the Branch Office. Tunnel ID is an identity when building a tunnel and must not be the same for other EoIP Tunnel. In this study, the configuration requirements are presented in Table 5. Tunnel ID uses a value of 10. There is no standard for setting a value of 10; it only adjusts to needs. Then, the Local Address configuration on the Head Office router will become the Remote Address on the Branch Office router and vice versa.

Table 6. Public IP Address Laptop

Site	IP Address	Subnet mask	Gateway	DNS Server
Branch Office	103.175.48.43	255.255.255.248	103.175.48.41	103.135.227.204 103.135.227.203

 DOI: https://doi.org/10.52435/jaiit.v7i1.691

Table 6 is the Public IP Address that will be used on laptops in branch offices for testing. The DNS server used is adjusted from the Internet Service Provider (ISP).

3.2. Test Result

This study used the Virtual Private Network (VPN) method, which is Site-to-Site, where communication is tunneled will be done between routers. In this test, the results of the Virtual Private Network (VPN) connection using Point-to-Point Tunneling Protocol (PPTP) between the Head Office router and the Branch Office successfully. Figure 2 shows that the Branch Office router has successfully connected to the Point-to-Point Tunneling Protocol (PPTP) Server VPN network on the Head Office router.

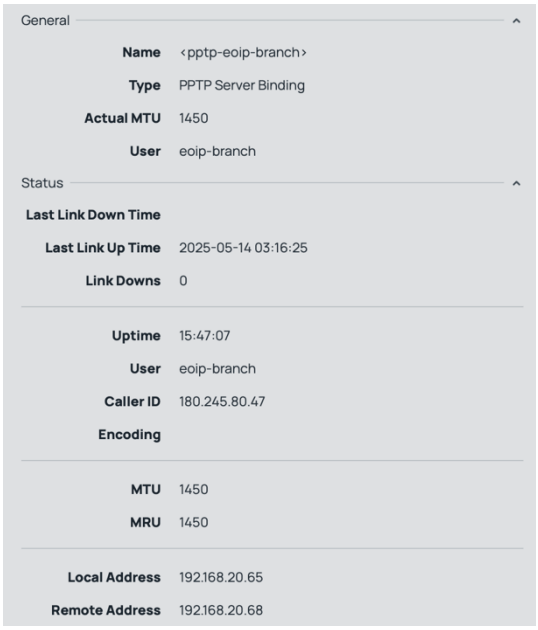

Figure 2. PPTP Client Connection Status

Figure 2 displays the status information of the branch office client connection on the head office router. In the figure, the Local Address and Remote Address match the secret configuration on the Head Office router. The IP obtained from the Virtual Private Network (VPN) Point-to-Point Tunneling Protocol (PPTP) will be used by the EoIP Tunnel. Basically, to build an EoIP Tunnel network through the Internet network, there must be a Public IP Address between the routers so that they can recognize each other. In this study, the Branch Office has limitations related to the Public IP Address. To implement the EoIP Tunnel, a Virtual Private Network (VPN) network must first be built using one of the protocols, namely the Point-to-Point Tunneling Protocol (PPTP).

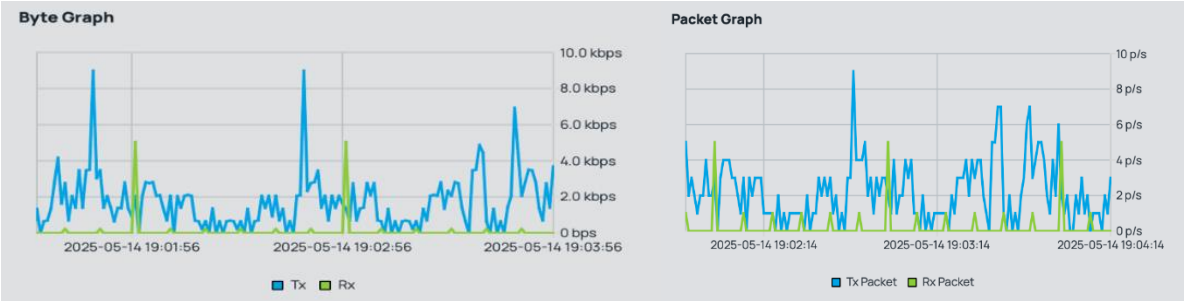

Figure 3. Traffic & Packet Graph PPTP Client

Figure 3 shows a graph for traffic and packets from a Virtual Private Network (VPN) connection. The Tx parameter in the Byte Graph shows the Transmit traffic to the client, which can be interpreted as the client download traffic. While Rx shows the Receive traffic from the client, which can be

interpreted as the client upload traffic. This also applies to the Tx and Rx Packets. After successfully establishing a Virtual Private Network (VPN) connection then, a new session for EoIP Tunnel starts.

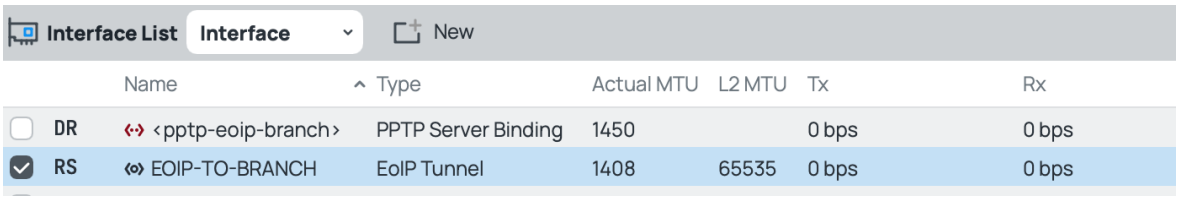

Figure 4. EoIP Connection Status

Figure 4 shows that the Branch Office router has successfully connected to Ethernet over Internet Protocol (EoIP) on the Head Office router. The RS flag sign has a meaning where R is Running while S is Slave. It can be interpreted that the Branch Office can communicate with the Head Office. For detailed connection information, we can see Figure 4.

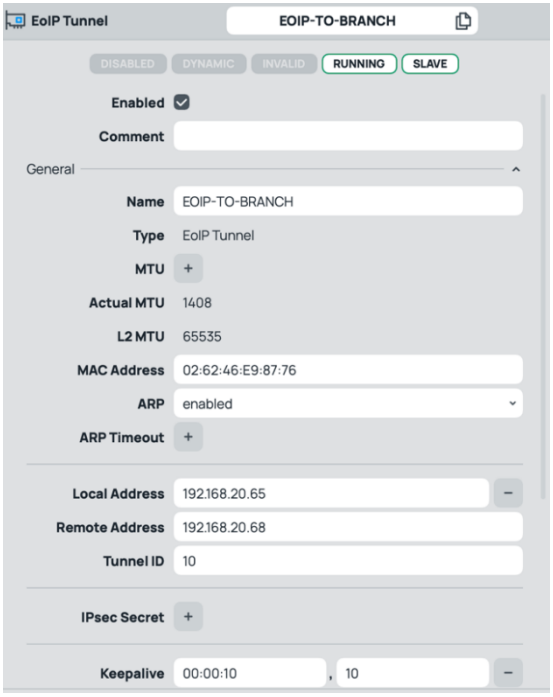

Figure 4. EoIP Connection Status Detail

After the Virtual Private Network (VPN) is active and the EoIP is connected, the next step is to test it using a laptop. The laptop configuration can be seen in Figure 5.

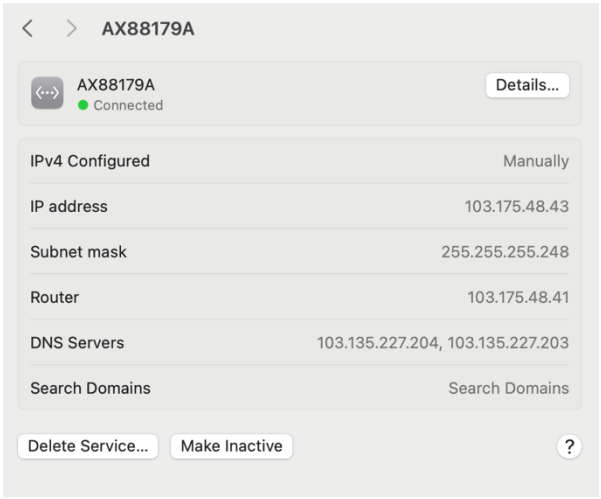

Figure 5. Network Configuration

 DOI: https://doi.org/10.52435/jaiit.v7i1.691

The last test conducted was using the Public IP Address from the Head Office office on a laptop at the Branch Office. To ensure that the Public IP Address is successfully used on the laptop can be seen from 1) The laptop can be connected to the Internet Network, 2) Bandwidth Testing, and 3) Viewing the network route using the traceroute function.

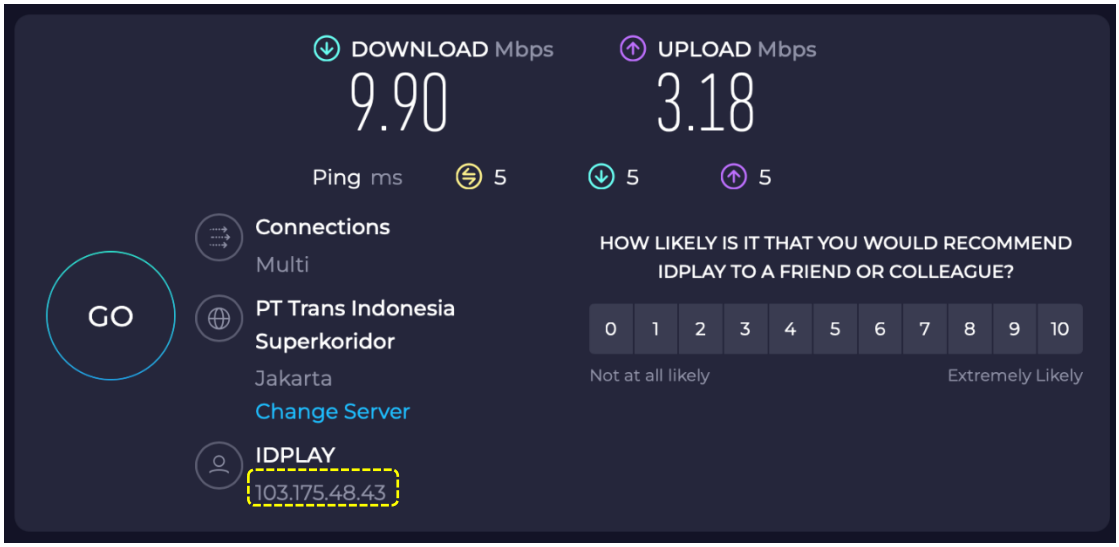

Figure 6. Bandwidth Testing

Figure 6 shows the results of the bandwidth test. This bandwidth test can be used as a reference that the laptop can connect to the internet. Another thing that can be done is to access one of the websites available on the internet. Information on mark the yellow line shows the Public IP Address detected from the laptop. The results of this test, the laptop has successfully used the Public IP Address from the Head Office. In practice, the difference in services between Internet Service Providers (ISPs) between Broadband Internet and Dedicated Internet lies in the priority of routes and quality assurance. Dedicated Internet routes are shorter and can be given the best path authority compared to Broadband Internet. With the difference in routes, it will affect the speed of access. However, the amount of bandwidth obtained still depends on the Broadband Internet service. The use of tunneling will also reduce the Maximum Transfer Unit (MTU) value, where the default for Ethernet is 1500 Bytes, while using Point-to-Point Tunneling Protocol (PPTP) is 1450 Bytes. MTU determines the amount of data packet size that can be transmitted on a network connection. The larger the MTU size, the larger the packet size that is passed. This will reduce the fragmentation process in data packets.

```
(base) tomidefisa@Tomis-MacBook-Air ~ % traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 40 byte packets
 1  103.175.48.41 (103.175.48.41)  4.854 ms  5.006 ms  4.599 ms
 2  ip33-224-135-103.tis.net.id (103.135.224.33)  9.029 ms  5.363 ms  4.286 ms
 3  119.235.217.1 (119.235.217.1)  5.361 ms  5.982 ms  5.202 ms
 4  74.125.118.221 (74.125.118.221)  17.210 ms
    72.14.194.83 (72.14.194.83)  19.297 ms  19.203 ms
 5  72.14.194.82 (72.14.194.82)  17.231 ms
    74.125.118.220 (74.125.118.220)  18.493 ms  19.411 ms
 6  * * *
 7  dns.google (8.8.8.8)  16.520 ms  16.657 ms  16.377 ms
(base) tomidefisa@Tomis-MacBook-Air ~ %
```

Figure 7. Traceroute DNS Google

To ensure the gateway route that passes through the internet on the laptop, the traceroute function is used. Route testing is carried out on one of Google DNS with IP 8.8.8.8. From the traceroute results in Figure 7, the Gateway passed at hop one is already using the Head Office Public IP Address. It can

be concluded that the Public IP Address from the Head Office can be used from the branch office via a Virtual Private Network (VPN) connection.

4. Conclusion

Based on the tests conducted, The Branch Office router successfully connected to the Head Office router via the internet network with Virtual Private Network (VPN) support using the Point-to-Point Tunneling Protocol (PPTP) protocol. The results of the bandwidth test conducted showed that the detected Public IP Address was the Head Office Public IP Address, and this proved that the Ethernet over Internet Protocol (EoIP) function and the bridge interface used between routers were running well as a switching interface. Network route testing performed using traceroute shows the internet connection from the laptop to the internet passing through the Head Office network gateway. The function of the Virtual Private Network (VPN), in addition to being able to connect to the central network via the internet, can also be used to create network clusters. From the test results, it can be concluded that the Sharing Public IP Address model can be implemented in the problem of limited Public IP Addresses. This model can be adopted to help organizations in sharing Public IP Addresses. For further research, other Virtual Private Network (VPN) protocols such as L2TP, SSTP, or OVPN server can be used, and the performance of routers with different bandwidth capacities can be compared.

Acknowledgement

Thank you for the support of all the PT Trans Indonesia Superkoridor network teams. Hopefully, this research can be used as a solution for customers.

References

[1] R. Febrianti, E. Rikardo Nainggolan, U. Radiyah, "Implementasi VPN Berbasis Point To Point Tunneling Protocol (PPTP) Menggunakan Mikrotik Router Board." *Jurnal Infortech*, vol. 3, no. 1, pp. 46–51, 2021, doi: 10.31294/infortech.v3i1.10400.

[2] D. Setiawan, A. Bode, and W. Yunus, "Implementasi EOIP Tunnel Dan Bonding pada Routerboad Mikrotik Untuk Menambah Kapasitas Wireless Link," *Jurnal Ilmiah Ilkom Balok*, vol. 2, no. 1, 2023, doi: 10.37195/balok.v2i1.397.

[3] B. Arifwidodo, "Performansi EOIP-PPTP dengan EOIP-L2TP Pada Router Mikrotik," *Journal of Telecommunication, Electronics, and Control Engineering (JTECE)*, vol. 2, no. 1, pp. 01–07, Jan. 2020, doi: 10.20895/jtece.v2i1.104.

[4] R. Fauziah, R., and R. Yusuf, "Implementasi Jaringan VPN untuk Mengurangi Biaya Komunikasi Menggunakan Metode EoIP Over PPTP: Studi Kasus House Printing," *Jurnal Edukasi dan Penelitian*, vol. 7, no. 3, pp. 390-399, Dec. 2021.

[5] M. A. Wardana, A. Z. Nusri, and J. Juliandika, "Jaringan Virtual Private Network (Vpn) Berbasis Mikrotik Pada Kantor Kecamatan Marioriawa Kabupaten Soppeng," *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI)*, vol. 5, no. 2, pp. 107–116, Oct. 2022, doi: 10.57093/jisti.v5i2.135.

[6] E. O. Akinsanya and P. D. Okeke, "Virtual Private Networks (VPN): A Conceptual Review of Security Protocols and Their Application in Modern Networks," *Engineering Science & Technology Journal*, vol. 5, no. 4, pp. 1452–1472, 2024, doi: 10.51594/estj/v5i4.1076.

[7] E. Syah Putra Siahaan and C. Eko Suharyanto, "Perancangan dan Implementasi Virtual Private Network dengan Mikrotik," *Jurnal Comasie*, 2021.

[8] A. Purnama Sari and N. Kemala, "Perancangan Jaringan Virtual Private Network Berbasis IP Security Menggunakan Router Mikrotik," vol. 7, no. 2, 2020.

[9] V. Phang and E. Setyaningsih, "Perancangan Virtual Private Network Dengan Protokol PPTP Menggunakan MikroTik Untuk Kebutuhan Remote Access," *Jurnal POLEKTRO: Jurnal Power Elektronik*, vol. 10, no. 2, 2021.

[10] R. A. Putra, H. Supendar, and R. Fahlapi, "Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik," *Jurnal Komputer Antartika*, vol. 1, no. 3, pp. 108-116, 2023.

[11] L. Oktaviana Sari and T. Dwi Kharisma, "Implementation Of VPN using the PPTP Method to Access CCTV Monitoring Data at the Bukit Raya District Office Penerapan VPN Menggunakan Metode PPTP untuk Mengakses Data Monitoring CCTV di Kantor Kecamatan Bukit Raya," *Jurnal Inovtek Polbeng*, vol. 9, no. 2, 2024.

[12] Y. Kuspandi Putra and M. Sadali, "Penerapan Mikrotik Dalam Mengembangkan Infrastruktur Jaringan Pada Kantor Desa Rumbuk Kecamatan Sakra," *Jurnal Informatika dan Teknologi*, vol. 3, no. 2, pp. 182–193, 2020.

[13] Sidik, A. Sudaryana, and R. Santoso, "Implementasi Virtual Interface Menggunakan Metode EOIP Tunnel Pada Jaringan WAN PT. Indo Matra Lestari", *Jurnal Teknik Komputer AMIK BSI*, vol. 6, no.1, 2020, doi: 10.31294/jtk.v4i2.

[14] D. Verian Nugroho and H. Noprisson, "Rancang Bangun Interkoneksi Jaringan Berbasis VPN Menggunakan Metode EOIP Tunnel," *JSAI: Journal Scientific and Applied Informatics*, vol. 7, no. 3, 2024, doi: 10.36085.

[15] A. Purwana, "Analysis of Ethernet Over Internet Protocol (EOIP) VPN Performance," *Journal of Computer Science and Information Technology*, vol. 7, issue. 3, 2021.

This page is intentionally left blank

 DOI: https://doi.org/10.52435/jaiit.v7i1.691