

IMPLEMENTASI INTERCITY BERBASIS TUNNELING MIKROTIK MENGUNAKAN METODE EOIP TUNNEL

Rizky Agung Ferdiana Adam¹⁾, Syarif Hidayatulloh²⁾

^{1,2}Teknik Informatika, Universitas BSI Bandung

^{1,2}Jalan Sekolah Internasional No.1-6 Antapani, Bandung

Email: ¹rizky.ferdiana@gmail.com, ²syarif.sfq@gmail.com

Abstrak

Kehandalan jaringan komputer berbasis WAN menjadi sangat penting terutama bagi perusahaan atau organisasi yang memiliki kantor cabang dengan jarak yang berjauhan. Untuk membuat media transmisi WAN berbasis fiber optik dapat dilakukan tetapi apabila kantor cabang berada di kota atau provinsi lain akan menghabiskan biaya yang mahal terlebih lagi waktu yang dibutuhkan untuk membangun jaringan tetap antar kota akan memakan waktu yang lama. Media interkoneksi antar kota diharapkan dapat menggunakan sumber daya yang mudah didapat dan juga memanfaatkan koneksi internet yang sudah ada. Model intercity berbasis Tunneling EOIP (Ethernet Over IP) menggunakan router Mikrotik dapat membuat koneksi WAN intercity memungkinkan jaringan pada suatu LAN terhubung secara virtual dan privat dengan jaringan LAN lain menggunakan koneksi internet yang sudah tersedia.

Kata Kunci: Tunnel, EOIP, Mikrotik, VPN

1. Pendahuluan

Jaringan Komputer pada dasarnya adalah mekanisme yang menghubungkan antar komputer ke komputer lain secara any to any. Jika di masa lalu perusahaan menghubungkan cabang-cabang kantornya untuk berkomunikasi dalam jaringan dengan cara membangun interkoneksi sendiri yang sesuai dengan budget dan kemampuan perusahaan, untuk interkoneksi sendiri dapat menggunakan bermacam-macam media transmisi seperti kabel fiber optik, radio atau VSAT. Namun pengadaan jalur khusus seperti ini akan menghabiskan biaya yang sangat mahal, terlebih apabila perusahaan memiliki cabang yang terpisah geografis sangat jauh seperti antar kota, provinsi bahkan negara [1] Solusi lainnya adalah dengan menggunakan saluran sewa secara point to point dengan menggunakan media transmisi yang disebutkan diatas tentunya juga menghabiskan biaya yang mahal[2].

Komunikasi jaringan komputer secara point to point pada dasarnya memiliki banyak cara, salah satunya adalah menggunakan Metronet Fiber Optik, namun permasalahan yang sering terjadi adalah putusnya koneksi yang disebabkan gangguan eksternal

[3]. Begitu pula dengan penggunaan VSAT sebagai media untuk membangun koneksi point to point antar cabang, masalah yang sering terjadi umumnya adalah kondisi cuaca dan juga rintangan yang akan menghalangi sinyal koneksi VSAT [4]

Maka saat ini pemanfaatan jaringan WAN dan Internet menjadi penting untuk memberikan solusi yang efektif dan efisien serta lebih murah untuk diimplementasikan. Modern ini pemanfaatan jaringan WAN dan internet menjadi solusi yang umum digunakan untuk membangun jaringan yang lebih privat diatas jaringan publik. Proses membangun sebuah jaringan privat diatas jaringan publik biasa disebut juga dengan Tunneling. Ada beragam jenis metode Tunneling yang dapat diimplementasikan dan memiliki ragam karakteristik maupun kelebihan dan kekurangan yang dapat digunakan sesuai kebutuhan, salah satunya dengan menggunakan perangkat Router Mikrotik. Untuk membuat suatu Tunnel, kedua kantor cabang harus terkoneksi ke internet dan memiliki IP Publik Static, lalu mikrotik akan membuat jalur pribadi diatas koneksi TCP/IP[5].

Jaringan komputer memberi kemampuan sebagai media komunikasi dan berbagi informasi yang mempercepat proses kerja baik dari segi waktu maupun ruang, sehingga perkembangan teknologi informasi mempengaruhi segala aspek kehidupan manusia. Sebagai salah satu aspek yang paling mempengaruhi kehidupan tersebut lah internet menjadi kian diminati, selain sangat bermanfaat namun internet juga tetap memiliki kelemahan dalam keamanannya, maka penerapan internet sebagai media komunikasi perlu diperhatikan juga aspek keamanannya. Unit Ecosystem Service Assurance PT Telekomunikasi Indonesia yang merupakan salah satu unit yang menguji coba, menangani beberapa gangguan dan layanan baru di Telkom untuk dikembangkan dan dijual, dimana semua proses aktifitas pengelolaan dan penanganan gangguan aplikasi harus menggunakan jaringan intranet kantor pusat. Para pegawai juga sering mendapat tugas rapat dan pelatihan ke luar kota, maka dibutuhkan aplikasi yang memungkinkan pegawai untuk tetap terhubung ke jaringan intranet kantor walau sedang berada di luar jaringan kantor. Pada penelitian ini berfokus pada aplikasi penyedia VPN yang bersifat opensource, yaitu OpenVPN Access Server. Implementasi penggunaan

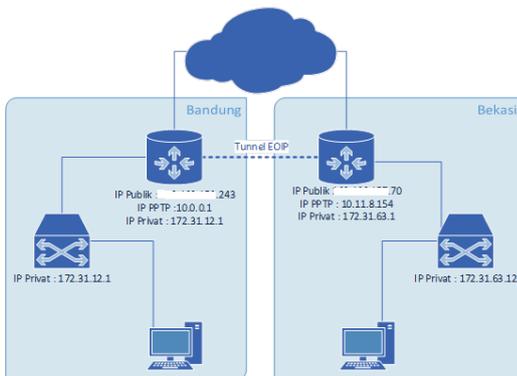
aplikasi ini relatif mudah karena sudah menggunakan Graphical User *Interface* (GUI) berbasis WEB. Sebuah aplikasi OpenVPN dibuat diantara 2 buah akses internet dengan firewall dan aplikasi OpenVPN. Aplikasi tersebut kemudian disetting agar dapat melewati firewall dan tidak diblokir oleh firewall[6].

Tidak terkecuali PT Sarana Integrasi Prima, perusahaan yang bergerak di bidang penyediaan Jartaplok (Jaringan Tetap Lokal) berbasis fiber optik yang mempunyai rekan dan pelanggan dari kalangan *Internet Service Provider* dan mempunyai cabang di beberapa kota besar di Indonesia. Untuk menyediakan interkoneksi tiap cabang untuk kebutuhan internal dan mitra perusahaan, PT Sarana Integrasi Prima juga membutuhkan sebuah mekanisme *Tunneling* yang efektif dan efisien untuk menunjang operasional dan proses bisnisnya. Di setiap cabang saat ini masing-masing sudah terkoneksi dengan internet untuk kebutuhan operasional di masing-masing divisi regional.

Penelitian ini akan berfokus untuk membuat jalur *Tunnel* menggunakan salah satu protocol *Tunnel* pada perangkat mikrotik yaitu *EOIP* (Ethernet Over IP). *EOIP* adalah Mikrotik *RouterOS* protocol yang memanfaatkan jalur koneksi internet untuk membangun koneksi bridging ethernet antar *router* (Mikrotik, 2017). Hal ini memungkinkan kedua jaringan yang berbeda dapat diperlakukan seolah-olah berada pada satu lingkup geografis yang dekat dan juga privat. Hasil yang diharapkan agar perusahaan mempunyai teknologi jaringan pribadi dengan memanfaatkan jaringan publik.

2. Metode

Metode penelitian ini membuat teknologi *Tunneling* menggunakan perangkat Mikrotik dengan metode *EOIP Tunnel*. Kedua sisi *router* yang akan dihubungkan akan menggunakan perangkat Mikrotik *Router* yang memiliki IP Publik statis dan terkoneksi ke internet.



Gambar 1. Skema Jaringan

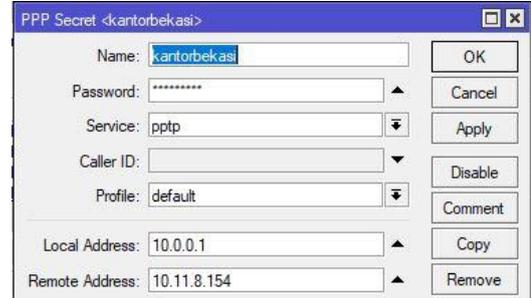
3. Hasil dan Pembahasan

Konfigurasi *EOIP Tunnel* meliputi pembuatan PPTP VPN, *EOIP Tunnel* dan konfigurasi *Switch* di sisi

Bekasi.

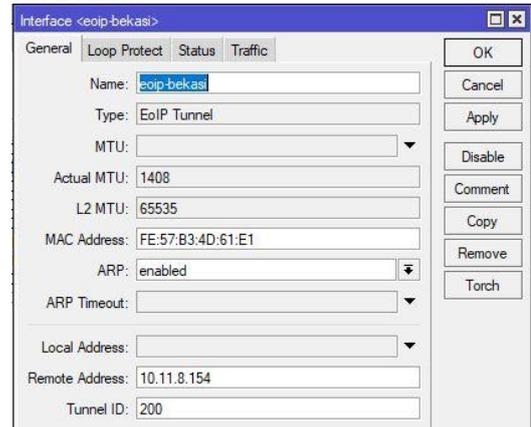
3.1. Konfigurasi Router Bandung

Pertama adalah membuat PPTP Server untuk menyediakan IP Privat yang akan menghubungkan *EOIP Tunnel*.



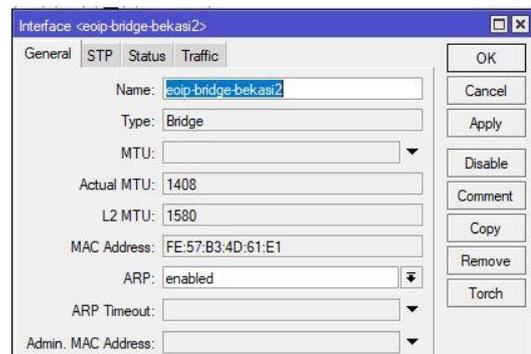
Gambar 2. Konfigurasi PPTP Server

Kemudian melakukan pembuatan *interface EOIP Tunnel* dengan memanggil IP Privat *Router* Bekasi yang terhubung dengan PPTP VPN. *Tunnel ID* yang diberikan juga harus bersifat unik dan sama dengan *Tunnel ID* di sisi Bekasi.



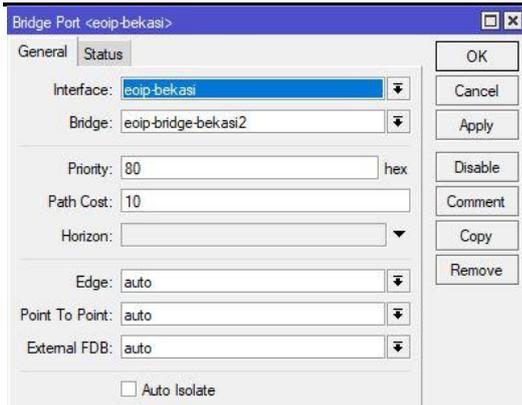
Gambar 3. Konfigurasi EOIP Interface

Lalu buat *interface bridge* untuk menghubungkan *EOIP Tunnel* dengan jaringan lokal.



Gambar 4. Konfigurasi Bridge Router Bandung

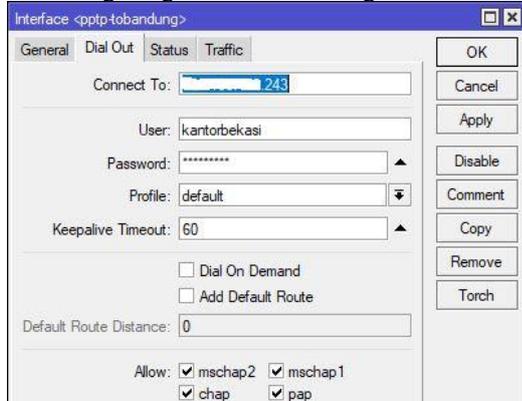
Kemudian definisikan *interface* yang akan disertakan pada *interface bridge*, yaitu *interface EOIP Tunnel*



Gambar 5. Konfigurasi EOIP Tunnel pada Bridge di router Bandung

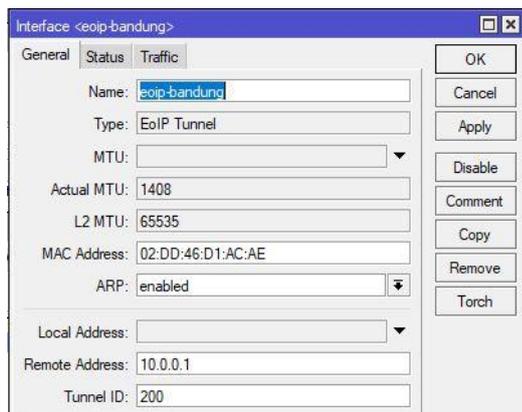
3.2. Konfigurasi Router Bekasi

Pertama adalah membuat VPN PPTP agar terhubung dengan router Bandung melalui IP Privat



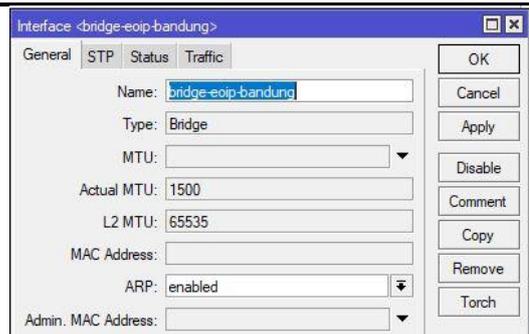
Gambar 6. Konfigurasi PPTP Client

Kemudian membuat interface EOIP yang memiliki Tunnel ID yang sama dengan router Bandung, dan memanggil IP Privat router Bandung yang diperoleh dari PPTP Server.



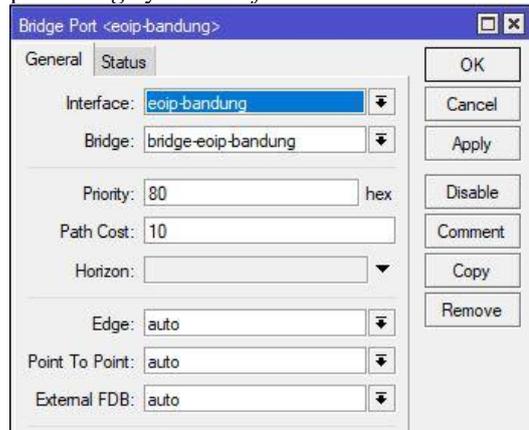
Gambar 7. Konfigurasi EOIP Tunnel Bekasi

Lalu buat interface bridge untuk menghubungkan EOIP dengan jaringan lokal.

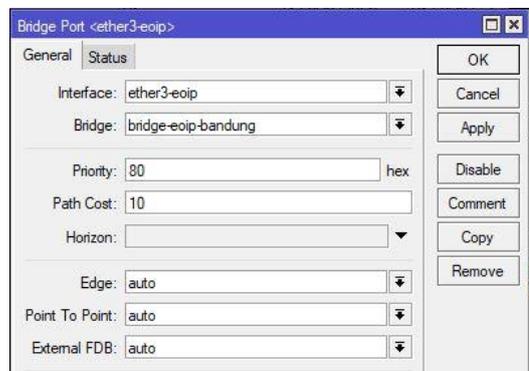


Gambar 8. Konfigurasi Bridge Router Bekasi

Kemudian definisikan interface yang akan disertakan pada bridge yaitu interface EOIP Tunnel.



Gambar 9. Konfigurasi EOIP Tunnel pada Bridge Router Bekasi



Gambar 10. Konfigurasi Interface baru pada router yang disertakan pada bridge router Bekasi

3.3. Konfigurasi Switch Bekasi

Pada Switch Bekasi, buatlah VLAN Baru yang akan terhubung dengan jaringan di Bandung.

```
SWITCH-BEKASI>ena
SWITCH-BEKASI#conf
SWITCH-BEKASI_config#int g0/3
SWITCH-BEKASI_config_g0/3#description TO-TUNNEL_EOIP
SWITCH-BEKASI_config_g0/3#switchport mode trunk
SWITCH-BEKASI_config_g0/3#switchport trunk vlan-allowed add 4
SWITCH-BEKASI_config_g0/3#ex
SWITCH-BEKASI_config#int g0/5
SWITCH-BEKASI_config_g0/5#description PC_ADMIN
SWITCH-BEKASI_config_g0/5#switchport mode access
SWITCH-BEKASI_config_g0/5#switchport pvid 4
SWITCH-BEKASI_config_g0/5#ex
SWITCH-BEKASI_config#vlan 4
SWITCH-BEKASI_config_vlan4#name VLAN_Operasional_to_Bandung
SWITCH-BEKASI_config_vlan4#ex
```

Gambar 11. Konfigurasi VLAN

3.4. Hasil Penelitian

Pada Aplikasi winbox akan terlihat *interface EOIP Tunnel* sudah terlewati traffic.

Name	Type	L2 MTU	Tx	Rx
bridge-eoip-bandung	Bridge	1598	0 bps	4.2 kbps
bridge-eoip-psec	Bridge		0 bps	0 bps
bridge	Bridge		0 bps	0 bps
eoip-bandung	EOIP Tunnel	65535	14.5 kbps	17.8 kbps
eoip-psec	EOIP Tunnel	65535	0 bps	0 bps
ether1	Ethernet	1598	147.7 kbps	31.3 kbps
ether2	Ethernet	1598	0 bps	5.6 kbps
ether3	Ethernet	1598	18.7 kbps	12.8 kbps
3112-MGMT	VLAN	1594	0 bps	0 bps
ether4	Ethernet	1598	0 bps	0 bps
ether5	Ethernet	1598	0 bps	0 bps
ether6	Ethernet	1598	0 bps	0 bps
ether7	Ethernet	1598	0 bps	0 bps
ether8	Ethernet	1598	0 bps	0 bps
ether9	Ethernet	1598	0 bps	0 bps
ether10	Ethernet	1598	0 bps	0 bps
internet	PPTP Client		133.0 kbps	2.1 kbps
pptp-tobandung	PPTP Client		14.0 kbps	19.8 kbps

Gambar 12. Interface Status

Apabila dilakukan penelusuran, akan terlihat bahwa dari komputer Bekasi ke *File Server* yang berada di Bandung hanya melewati IP Privat saja.

```

C:\Users\noc>tracert 172.15.16.41
Tracing route to 172.15.16.41 [172.15.16.41]
over a maximum of 30 hops:
 0  20 ms  9 ms  13 ms  172.15.16.41.lightspeed.brhmal.sbcglobal.net [172.15.16.41]
Trace complete.

C:\Users\noc>tracert 172.31.12.149
Tracing route to mail.connectivist.co.id [172.31.12.149]
over a maximum of 30 hops:
 0  8 ms  7 ms  7 ms  172.15.16.1.lightspeed.brhmal.sbcglobal.net [172.15.16.1]
 1  8 ms  8 ms  8 ms  mail.connectivist.co.id [172.31.12.149]
Trace complete.

C:\Users\noc>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . . . :
    Link-local IPv6 Address . . . . . : fe80::c36:e1d9:2015:d85b%12
    IPv4 Address. . . . . : 172.15.16.54
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.15.16.1
    
```

Gambar 13. Hasil Traceroute

Apabila melakukan pengecekan pada *Switch*, akan terlihat bahwa VPN bekerja pada layer 2 Datalink sehingga mac address dari VLAN yang sama di sisi Bandung akan terdeteksi juga di jaringan lokal Bekasi.

```

SWITCH-BEKASI#show mac address-table vlan 4
Mac Address Table (Total 22)
-----
Vlan  Mac Address      Type      Ports
----  -
4     7077.8116.1823    DYNAMIC  g0/3
4     c83d.d47e.e383    DYNAMIC  g0/3
4     c83d.d47e.e3c5    DYNAMIC  g0/3
4     e4be.edac.90da    DYNAMIC  g0/3
4     48db.503f.148a    DYNAMIC  g0/3
4     e4be.ed7f.2850    DYNAMIC  g0/3
4     0c38.3e1a.b69d    DYNAMIC  g0/3
4     0c38.3e1a.b699    DYNAMIC  g0/3
4     4ced.fb23.39b6    DYNAMIC  g0/3
4     dc85.dea4.81d5    DYNAMIC  g0/3
4     9cae.d3f6.6ce6    DYNAMIC  g0/3
4     02dd.46d1.acae    DYNAMIC  g0/3
4     c83d.d47e.5807    DYNAMIC  g0/3
4     c087.eb8f.8e73    DYNAMIC  g0/3
4     a8a7.9505.be97    DYNAMIC  g0/3
4     fe57.b34d.61e1    DYNAMIC  g0/3
4     e48d.8c34.db24    DYNAMIC  g0/3
4     acb5.7ad2.8338    DYNAMIC  g0/3
4     044b.ed32.6fa9    DYNAMIC  g0/3
4     40f0.2f64.3f8c    DYNAMIC  g0/3
4     9801.a7c7.4227    DYNAMIC  g0/3
4     c85b.76cd.d776    DYNAMIC  g0/5
    
```

Mac address dari jaringan Bandung (lines 1-16)
Mac address komputer Bekasi (lines 17-22)

Gambar 14. Hasil pengecekan mac-address

Kita dapat memantau paket apa saja yang sedang melewati VPN *EOIP Tunnel* juga menggunakan fitur Torch yang ada pada MikrotikOS.

Eth. Protocol	Prot.	Src.	Dest.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack.	Rx Pack.
800 (ip)		172.15.16.1	172.15.16.54			0 bps	0 bps	0	0
800 (ip)		172.15.16.222	224.0.1.75			0 bps	0 bps	0	0
800 (ip)		239.255.255.250	172.15.16.54			1432 bps	0 bps	1	0
800 (ip)		172.217.194.100	172.15.16.54			0 bps	0 bps	0	0
800 (ip)		103.66.70.12	172.15.16.54			0 bps	0 bps	0	0
800 (ip)		103.66.70.13	172.15.16.54			3046 kbps	6.0 Mbps	432	0
800 (ip)		172.15.16.56	255.255.255.255			0 bps	0 bps	0	0
800 (ip)		172.15.16.56	172.15.16.255			0 bps	736 bps	0	0
800 (ip)		172.15.16.56	224.0.0.251			0 bps	0 bps	0	0
800 (ip)		172.15.16.56	224.0.0.252			0 bps	600 bps	0	0
800 (ip)		172.15.16.48	239.255.255.250			0 bps	0 bps	0	0

Gambar 15. Hasil Torch

EOIP Tunnel tidak terlalu membebani perangkat *router* sehingga tidak mengganggu kinerja *router* secara keseluruhan.

Uptime: 6d 22:45:50

Free Memory: 37.5 MiB

Total Memory: 64.0 MiB

CPU: MIPS 74Kc V4.12

CPU Count: 1

CPU Frequency: 600 MHz

CPU Load: 2 %

Free HDD Space: 109.1 MiB

Total HDD Size: 128.0 MiB

Sector Writes Since Reboot: 1 211

Total Sector Writes: 2 464

Bad Blocks: 0.0 %

Architecture Name: mipsbe

Board Name: RB2011iL

Version: 6.30.4

Build Time: Aug/25/2015 12:59:46

Gambar 16. CPU Load

4. Kesimpulan

1. Pembuatan *intercity* berbasis *EOIP Tunnel* antara kota Bandung dan Bekasi dapat dilakukan dengan baik karena kedua *router* di sisi Kota Bandung dan Bekasi menggunakan Static IP Public dan bandwidth internet yang cukup.
2. Kualitas koneksi *Tunnel EOIP* amat bergantung pada kualitas internet dari kedua sisi *router*, apabila salah satu *router* mengalami gangguan atau degradasi kualitas bandwidth maka akan mempengaruhi kecepatan dan kapasitas *EOIP Tunnel*.
3. MikrotikOS memperlakukan *interface EOIP Tunnel* sebagai bagian dari *interface* lokalnya, sehingga link dibuat seolah-olah berada pada satu LAN (*Local Area*

Network) yang sama. Hal ini menjadi kelebihan karena apabila bandwidth internet yang tersedia berkualitas baik, akan terjadi koneksi WAN berkapasitas LAN.

4. Implementasi *EOIP Tunnel* tidak begitu membebani prosesor *router* sehingga sangat mudah dan ringan.

5. *Interface* yang dilakukan *bridge* akan terpisah secara virtual dengan jaringan lokal, sehingga diperlukan mekanisme lain untuk menghubungkan jaringan yang masuk ke *EOIP Tunnel* dengan jaringan yang secara fisik terhubung ditempat yang sama

6. Autentikasi yang digunakan pada penelitian ini menggunakan 2 kali metode autentikasi, pertama menggunakan PPTP VPN yaitu autentikasi berdasarkan metode username dan password, yang kedua menggunakan autentikasi berdasarkan *IP Address*, karena untuk membangun *EOIP Tunnel*, kedua *IP address* harus saling men-dial.

Daftar Pustaka

- [1] V. D. Septriadi dan A. Prihanto, "Membangun Jaringan Intranet dengan melewati VLAN diatas VPN menggunakan Metode PPTP BCP," *Manaj. Inform.*, vol. 7, no. 2, hal. 109–116, 2017.
- [2] Suryanto dan S. Dewi, "IMPLEMENTASI JARINGAN VPN BERBASIS IP-MPLS PADA PT. MHE DEMAG INDONESIA," vol. XV, no. 1, hal. 98–105, 2013.
- [3] S. N. Khasanah dan L. A. Utami, "Implementasi Failover Pada Jaringan WAN Berbasis VPN," vol. IV, no. 1, hal. 62–66, 2018.
- [4] PT Space Net Indonesia, "Vsat Part 2: Komponen, Kelebihan Dan Kekurangan Vsat - Qilat," 2016. .
- [5] PT Citraweb Solusi Teknologi, "Mikrotik.ID: Interkoneksi Jaringan dengan Tunnel," 2013. .
- [6] F. Firmansyah dan M. Badrul, "PENERAPAN METODE OPEN VPN-ACCESS SERVER SEBAGAI RANCANGAN JARINGAN WIDE AREA NETWORK," vol. XII, no. 1, hal. 40–52, 2015.