

Implementasi *Virtual Interface* Menggunakan Metode *EOIP Tunnel* Pada Jaringan WAN PT. Indo Matra Lestari

Sidik¹, Ade Sudaryana², Rame Santoso³

^{1,2}Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri

³Universitas Bina Sarana Informatika

¹sidik.sdk@nusamandiri.ac.id

²ade_sudaryana@yahoo.co.id

³rame.rms@bsi.ac.id

Diterima	Direvisi	Disetujui
07-11-2019	02-01-2020	02-02-2020

Abstrak - Jaringan komputer menjadi poin penting dalam perusahaan yang mempunyai banyak kantor cabang untuk proses koordinasi transfer data. Koneksi PT Indo Matra Lestari menggunakan sistem VPN dengan metode PPTP. Data Center dijadikan sebagai VPN server, clientnya adalah Kantor Pusat dan Kantor Cabang Citereup. Diantara Kantor Pusat dengan Kantor Cabang Citereup tidak ada koneksi secara langsung sehingga dalam mengakses data yang dilakukan antara Kantor pusat dengan Kantor Cabang Citereup menjadi lambat, sebab data harus melewati Data Center sebelum sampai ketujuan. Terlebih lagi data yang di akses bersifat pribadi bagi perusahaan dan hanya diakses pada jaringan lokal. Solusi yang digunakan untuk membuat jalur jaringan langsung dan aman antara Kantor Pusat dengan Kantor Cabang adalah menggunakan EoIP Tunnel pada router mikrotik. Metode tunneling pada EoIP dapat membuat bridging jaringan antar perangkat mikrotik, EoIP Tunnel akan berubah menjadi Virtual Interface pada router mikrotik sehingga seolah-olah antar router mikrotik terhubung secara lokal. Tunnel ID pada EoIP Tunnel berfungsi sebagai keamanan jalur tunneling. Penerapan EoIP Tunnel membuat jalur koneksi point to point antar perangkat Mikrotik menjadi lebih cepat dalam akses data karena akses data tersebut langsung ketujuan. Agar koneksi EoIP Tunnel ini dapat berjalan optimal dan baik maka dibutuhkan juga sebuah manajemen jaringan dalam mengatur pemakaian bandwidth internet.

Kata Kunci: *virtual interface, EOIP Tunnel*

Abstract - Computer networks have become an important point in companies that have many branch offices to coordinate the transfer of data. PT Indo Matra Lestari's connection uses a VPN system using the PPTP method. Data Center is used as a VPN server, the client is the Head Office and Citereup Branch Offices. Between the Head Office and the Citereup Branch Office there is no direct connection so access to data made between the Head Office and the Citereup Branch Office is slow, because the data must pass through the Data Center before reaching its destination. Moreover, the data accessed is private to the company and only accessed on the local network. The solution used to create a direct and secure network path between the Head Office and Branch Offices is to use the EoIP Tunnel on the proxy router. Tunneling method in EoIP can make network bridging between proxy devices, EoIP Tunnel will change to Virtual Interface on the proxy router so that it is as if the proxy router is connected locally. Tunnel ID on the EoIP Tunnel functions as a tunneling path security. The application of the EoIP Tunnel makes the point to point connection point between Mikrotik devices faster in data access because the data access is directed to the destination. In order for this EoIP Tunnel connection to run optimally and well, a network management is needed in managing internet bandwidth usage

Keywords: *virtual interface, EOIP Tunnel*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini mengalami kemajuan yang sangat pesat. Dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat. Oleh karena itu dibutuhkan suatu sarana yang dapat mendukung hal tersebut. Salah satunya adalah

jaringan komputer dengan koneksi internet yang cepat dan stabil (Sumarno & Probo Hasmoro, 2013). Menurut (Kurniawan, 2007) menjelaskan bahwa "jaringan komputer adalah kumpulan sejumlah *peripheral* yang terdiri dari beberapa komputer, printer, LAN Card, dan peralatan lain yang saling terintegrasi satu sama lain". Namun permasalahan yang sering timbul adalah faktor

keamanan yang saat ini menjadi hal yang sangat penting untuk diperhatikan. Maka dibutuhkan suatu cara agar dapat memperoleh suatu informasi data, tukar menukar data, dilakukan dengan aman, stabil dan terhindar dari lamanya proses pengiriman data dari satu kantor ke kantor lainnya.

PT Indo Matra Lestari merupakan perusahaan yang mempunyai beberapa kantor cabang. Saat ini sistem yang dipakai oleh PT Indo Matra Lestari untuk koneksi jaringan antar kantor cabang menggunakan VPN (*Virtual Private Network*) dengan metode PPTP. VPN (*virtual private network*) adalah sebuah proses dimana jaringan umum (*public network* atau *internet*) diamankan kemudian difungsikan menjadi sebuah jaringan privat (*private network*) (Pramana, Widyastuti, & Triyono, 2014). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengizinkan penggunaannya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya. Pemilihan penggunaan VPN-PPTP tidak begitu maksimal pada PT Indo Matra Lestari, karena sistem koneksi jaringan yang ada di PT Indo Matra Lestari, yaitu kantor pusat – *data center* – kantor cabang. Antara kantor pusat terlebih dahulu terkoneksi ke *data center* lalu baru diteruskan ke kantor cabang. Permasalahan yang muncul saat ini yaitu jika kantor cabang ingin membuka data-data yang ada di *file server* tidak bisa *direct* menuju ke kantor pusat, tetapi terlebih dahulu harus melewati data center sehingga waktu untuk *copy*, *write*, *read*, dan eksekusi file menjadi lambat. Di data center sendiri ada beberapa server lain, yaitu server aplikasi, mail server, database server, dan *domain controller server*. Selain itu VPN yang diterapkan antara router di data center dengan router yang ada di kantor cabang gudang Citereup tidak terkoneksi dengan baik karena koneksi yang tidak stabil pada gudang Citereup sehingga menimbulkan load pada *traffic* jaringan. Sering terjadinya *flooding* dan FO CUT pada ISP Arsen yang pakai di data center juga menjadi faktor lain yang menghambat karyawan yang ada di kantor cabang gudang Citereup untuk mengakses File Server. Dalam pemanfaatan fitur tunneling menggunakan virtual interface EoIP di mikrotik router OS untuk koneksi bridging antar kantor melalui jaringan ADSL Telkom Speedy menunjukkan bahwa untuk aplikasi-aplikasi yang masih memerlukan model *local/ private network* maka internet masih bisa dimanfaatkan dengan melakukan proses tunneling berbasis protokol IP misalkan menggunakan fitur EoIP di Mikrotik RouterOS. EoIP Tunnel merupakan fitur pada Mikrotik RouterOS yang membangun sebuah network tunnel antar Mikrotik RouterOS di atas sebuah koneksi TCP/IP. Pemanfaatan EoIP Tunnel dapat membuat virtual ethernet antar perangkat Mikrotik RouterOS sehingga seolah-olah jaringan yang bersifat public network menjadi jaringan yang

bersifat *local network* (Cahyadi, 2010). Tunneling merupakan data yang dienkapsulasi (dibungkus) dengan header yang berisi informasi routing untuk mendapatkan kon-eksi point to point sehingga data melewati jaringan publik dan dapat mencapai akhir tujuan (Meyatmaja & Syafrizal, 2012). Sedangkan tunnel adalah jalur yang dilewati melalui internet. VPN-PPTP mempunyai stabilitas kecepatan yang lebih baik dan layak digunakan untuk kepentingan home small corporate yang tidak membutuhkan enkripsi yang terlalu rumit tetapi tetap secure (Triyono, Rachmawati, & Dhimas Irnawan, 2014). Mikrotik router adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mempunyai berbagai fitur yang lengkap untuk jaringan dan wireless. Selain itu MikroTik dapat juga berfungsi sebagai firewall bagi komputer lain dan memberikan prioritas bagi komputer lain agar bisa mengakses data internet maupun data lokal. Mikrotik bertujuan untuk mengatur bandwidth serta melakukan manajemen jaringan komputer. Penempatan router MikroTik ditempatkan pada sebuah komputer yang dijadikan sebagai gateway suatu jaringan. menjelaskan secara singkat metode atau algoritma yang diusulkan (Riadi, 2011).

METODOLOGI PENELITIAN

Metode penelitian yang digunakan penulis pada penelitian ini terdiri dari dua metode yaitu:

1. Metode Pengembangan Sistem

Untuk menunjang tercapainya jaringan usulan yang dapat menyelesaikan masalah yang ada pada PT Indo Matra Lestari maka penulis melakukan penelitian langsung pada jaringan yang sudah ada pada PT Indo Matra Lestari. Penelitian tersebut meliputi:

a. Analisa Kebutuhan

Membangun sebuah EoIP Tunnel dibutuhkan perangkat hardware RB450 dengan sistem operasi Mikrotik RouterOS level 4 atau di atasnya. EoIP Tunnel merupakan fitur dari Mikrotik RouterOS sehingga pemanfaatan EoIP ini hanya bisa digunakan antar perangkat Mikrotik RouterOS.

b. Desain

Pada tahapan ini, penulis merancang jaringan yang akan di usulkan pada PT. Indo Matra Lestari. Desain jaringan usulan akan dibuat menggunakan aplikasi GNS3 sebagai simulasi sistem jaringan EoIP Tunnel Mikrotik RouterOS.

c. Testing

Pada tahap ini, penulis membuat sebuah simulasi jaringan dengan menggunakan aplikasi GNS3 dan melakukan pengujian jaringan (*testing*) menggunakan perintah

PING pada aplikasi *Command Prompt* Microsoft Windows.

d. Implementasi

Pada tahap implementasi terdiri atas penginstalan hardware dan software yang membentuk sistem jaringan yang memanfaatkan EoIP Tunnel. Pada tahap ini dapat dibagi menjadi konfigurasi perangkat, instalasi fisik, pengujian, dan dokumentasi.

2. Metode Pengumpulan Data

a. Observasi

Penulis mengumpulkan data yang diperoleh dengan cara melakukan pengamatan langsung di PT Indo Matra Lestari.

b. Wawancara

Penulis melakukan wawancara langsung dengan nara sumber yaitu Bapak Angga Rahma Putra selaku Supervisor IT di PT Indo Matra Lestari untuk memperoleh informasi secara jelas dan detail.

c. Studi Kepustakaan

Pada metode pengumpulan ini, penulis mengumpulkan data-data teoritis dan mempelajari buku-buku atau literature, jurnal-jurnal dan artikel internet yang berkaitan dengan masalah diatas.

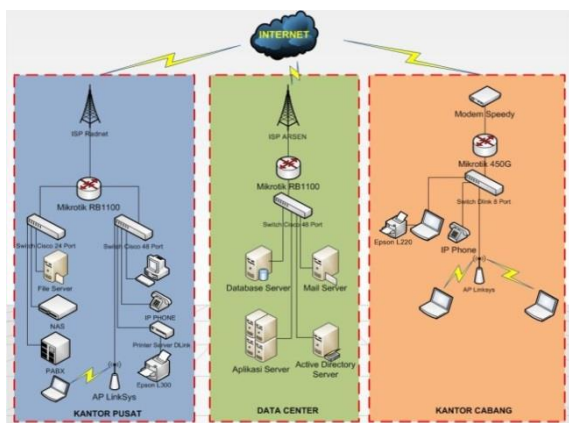
HASIL DAN PEMBAHASAN

Pada bagian ini, penulis menjelaskan tentang jaringan yang sedang diterapkan di perusahaan dan usulan jaringan yang penulis usulkan.

A. Jaringan yang sudah diterapkan

1. Topologi Jaringan

Topologi yang digunakan oleh PT Indo Matra Lestari terlihat sebagai berikut:



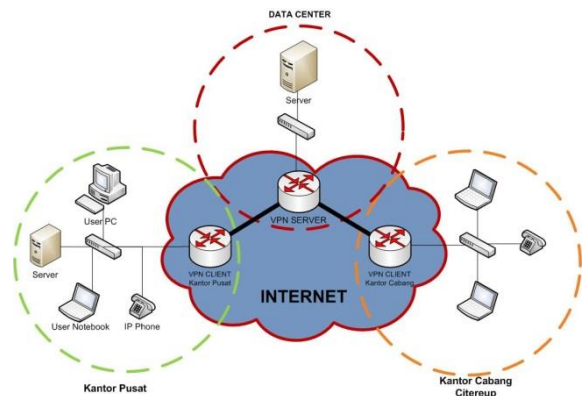
sumber: PT. Indo Matra Lestari (2016)

Gambar.1 Topologi jaringan berjalan PT. Indo Matra Lestari

Topologi jaringan yang digunakan pada masing-masing kantor pada PT Indo Matra Lestari menggunakan topologi star, switch digunakan sebagai *centralized* jaringan. Untuk user kantor pusat dan kantor cabang Citereup dikoneksikan dengan wifi metode *insfracture access point*. Pada data center semua server dikoneksikan dengan menggunakan kabel LAN.

2. Arsitektur Jaringan

PT Indo Matra Lestari menggunakan tipe jaringan client – server dengan topologi star pada jaringan LAN setiap kantor. Server digunakan sebagai pemberi fasilitas kepada komputer client. Server yang ada pada PT Indo Matra Lestari yaitu application server, mail server, file server, active directory server, PABX server, *Network Attached*



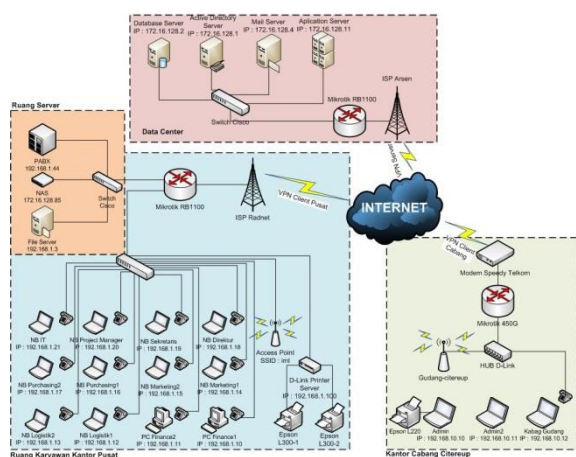
sumber: PT. Indo Matra Lestari (2016)

Gambar 2. Arsitektur jaringan WAN PT. Indo Matra Lestari

IP Address yang digunakan di PT Indo Matra Lestari menggunakan kelas IP A, B dan C. untuk IP kelas A digunakan untuk jalur VPN, IP kelas B digunakan di server, dan untuk kelas C digunakan untuk LAN PT. Indo Matra Lestari. Arsitektur jaringan merupakan aturan dalam membangun komunikasi komputer.

3. Skema Jaringan

PT Indo Matra Lestari menggunakan VPN-PPTP sebagai jalur interkoneksi antara kantor pusat, data center, dan kantor cabang. VPN Server terdapat pada router mikrotik yang ada di data center. Jalur VPN – PPTP pada PT Indo Matra Lestari yaitu kantor pusat – data center – kantor cabang. Data center menjadi *centralized* dalam menghubungkan kantor pusat dan kantor cabang. Selain itu pada data center terdapat empat server, yaitu *mail server*, *active directory server*, *application server*, dan *database server* semua server yang ada di Data Center menggunakan IP address kelas B yaitu 172.16.128.0/24.



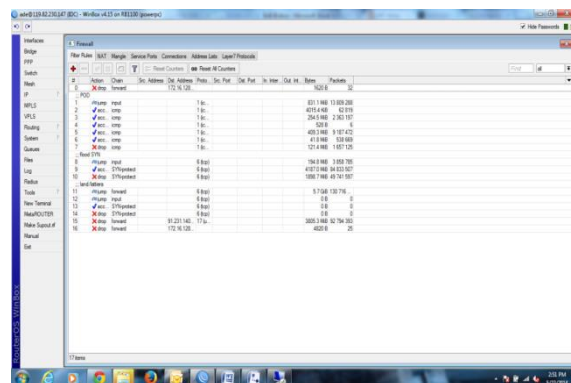
sumber: PT. Indo Matra Lestari (2016)
Gambar 3. Skema jaringan WAN PT. Indo Matra Lestari

Jaringan LAN pada kantor pusat menggunakan topologi star, IP address yang digunakan kelas C yaitu 192.168.1.0/24. User yang ada di kantor pusat berjumlah 12 user, 10 user menggunakan notebook dan 2 user menggunakan PC. terdapat tiga server pada kantor pusat, yaitu file server, Network Attached Storage (NAS), dan PABX Server. Pada kantor cabang Citeureup terdapat 3 user, menggunakan IP address kelas C yaitu 192.168.10.0/24 topologi yang digunakan adalah topologi star.

4. Keamanan Jaringan

Sistem keamanan jaringan di PT Indo Matra Lestari cukup kompleks, dimulai dari *joint access point* hingga akses internet semua menggunakan security. Untuk *joint access point*, user diharuskan mengisi WPA/WPA 2 sebagai *security key joint access point*. Penggunaan VPN (*Virtual Private Network*) dengan metode PPTP (*Point to Point Tunneling Protocol*) mempunyai sistem keamanan handal, pada protokol PPTP beroperasi pada layer 2 pada model OSI. Pada proses enkapsulasi, PPTP mengenkapsulasi PPP frames pada IP datagrams untuk ditransmisikan pada jaringan. PPTP juga menggunakan koneksi TCP untuk mengelola tunnel dan GRE (*Generic Routing Encapsulation*). Proses tunneling pada PPTP terjadi dengan cara membungkus paket informasi untuk kemudian ditransmisikan melalui jaringan internet. Pada proses ini PPTP menggunakan koneksi TCP yang dikenal sebagai PPTP control 4 *connection* untuk menciptakan, merawat dan mengakhiri tunnel serta *Generic Routing Encapsulation* (GRE). Dalam hal enkripsi, PPTP menggunakan mekanisme otentikasi yang sama dengan PPP seperti *Extensible Authentication Protocol* (EAP), *Challenge Handshake Protocol* (CHAP), *Shiva Password Authentication Protocol* (SPAP) dan *Password Authentication Protocol* (PAP). Selain itu untuk menghindari serangan dari luar, seperti DDOS, virus, dan lain-lain, jaringan PT Indo Matra Lestari menggunakan *mangle* di router mikrotik guna

mencegah serangan DDOS dari pihak luar. Sedangkan untuk melindungi perangkat komputer dari virus seperti *malware*, *worm*, *trojan*, dan lainnya menggunakan software anti virus Bit Defender dan MS Essential.

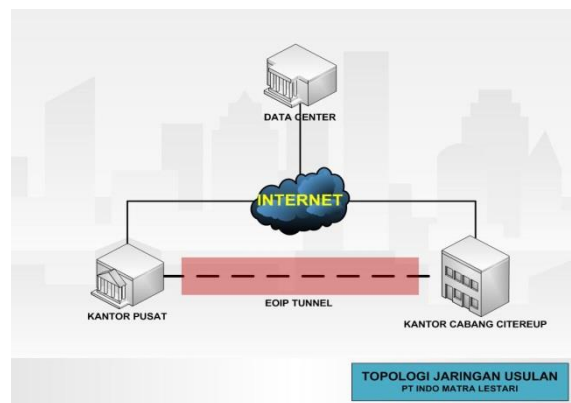


sumber: PT. Indo Matra Lestari (2016)
Gambar 4. Mangle Mikrotik anti DDOS

B. Jaringan yang di usulkan

Tidak adanya akses secara langsung antara kantor pusat dengan kantor cabang Citeureup mengakibatkan akses menuju ke *file server* menjadi lama dan mengganggu kinerja karyawan.

1. Topologi Jaringan usulan



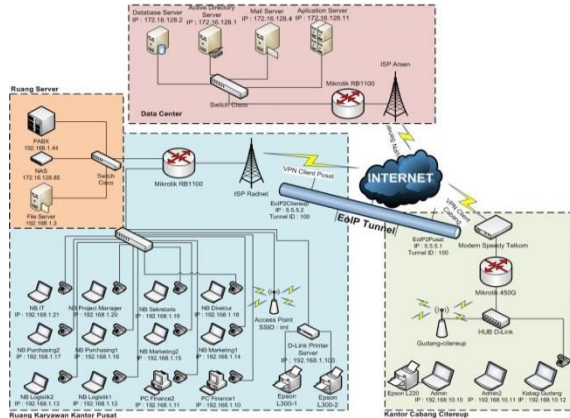
sumber: Sidik, Ade Sudaryana (2019)
Gambar 5. Topologi jaringan usulan PT. Indo Matra Lestari

Pada gambar topologi usulan dapat dilihat bahwa EoIP Tunnel dibuat pada kantor Pusat dengan kantor cabang Citeureup PT Indo Matra Lestari. EoIP Tunnel ini diharapkan dapat meningkatkan kinerja karyawan pada kantor cabang Citeureup karena tidak lagi kesulitan dalam mengakses ke File Server yang ada di kantor Pusat.

2. Skema Jaringan usulan

Pemanfaatan VPN-PPTP pada jaringan PT Indo Matra Lestari tidak dirubah, data center IDC masih digunakan sebagai centralize jaringan. Pembuatan EoIP Tunnel ini bertujuan agar ada jalur bypass

antar kantor pusat dan kantor cabang Citereup. Kantor cabang Citereup bisa secara langsung mengakses file server ke kantor pusat tanpa harus melalui data center terlebih dahulu. Skema jaringan setelah ada penambahan EoIP Tunnel:



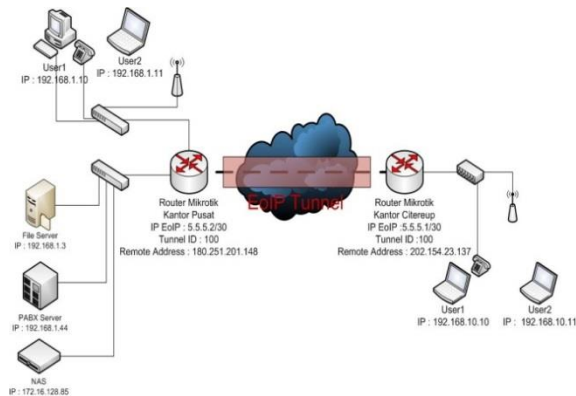
sumber: Sidik, Ade Sudaryana (2019)
Gambar 6. Skema jaringan usulan PT. Indo Matra Lestari

3. Keamanan Jaringan Usulan

EoIP Tunnel menggunakan protokol GRE (*Generic Routing Encapsulation*) dalam mengenkapsulasi paket yang akan dilewatkan dalam tunnel. Pada tunneling paket data dienskripsi dan dienkapsulasi. Keamanan jaringan EoIP Tunnel yang diterapkan pada PT Indo Matra Lestari, yaitu membuat rule pada firewall mikrotik, memfilter dari interface/MAC Address, dan membuat TUNNEL ID yang unik. Untuk menghindari serangan dari luar, seperti DDOS pada jalur EoIP Tunnel jaringan PT Indo Matra Lestari juga menggunakan mangle di router mikrotik guna mencegah serangan DDOS tersebut.

4. Rancangan Aplikasi EOIP Tunneling

Berikut Konfigurasi EoIP Tunnel dilakukan pada router mikrotik PT Indo Matra Lestari, yaitu:



sumber: Sidik, Ade Sudaryana (2019)
Gambar 7. Konfigurasi jaringan usulan menggunakan EoIP Tunneling

Pada gambar konfigurasi jaringan EoIP Tunnel, IP address untuk EoIP Tunnel yaitu 5.5.5.0/30. IP EoIP

Tunnel kantor pusat 5.5.5.2/30, kantor cabang Citereup IP EoIP Tunnel 5.5.5.1/30. Remote Address untuk kantor pusat 180.251.201.148 yang merupakan IP Publik dari ISP Speedy kantor cabang Citereup, sedangkan untuk remote address kantor cabang Citereup yaitu 202.154.23.137 yang merupakan IP Publik dari ISP Radnet kantor pusat. Tunnel ID untuk EoIP Tunnel PT Indo Matra Lestari yaitu 100. Alokasi IP Address untuk LAN kantor pusat yaitu 192.168.1.0/24, untuk kantor cabang Citereup yaitu 192.168.10.0/24.

5. Manajemen Jaringan Usulan

Manajemen jaringan yang diusulkan untuk PT Indo Matra Lestari adalah dengan manajemen bandwidth yang digunakan, yaitu dengan metode memisahkan paket data yang digunakan untuk keperluan kerja dan paket data untuk keperluan internet, setelah dipisahkan lalu dilakukan pembatasan pemakaian bandwidth yang digunakan. Konfigurasi pemisahan dan pembatasan bandwidth dapat dilakukan pada router mikrotik dengan memanfaatkan fitur *firewall*, *mangle*, dan *queues*.

6. Pengujian Jaringan Usulan

Pengujian jaringan ini bertujuan untuk mengkomparasi hasil jaringan sebelumnya dengan hasil jaringan usulan yang telah dibuat.

a. Pengujian Jaringan Awal

Pengujian jaringan awal ini dilakukan di kantor cabang Citereup PT Indo Matra Lestari, pengujian yang dilakukan yaitu, PING ke ip file-server, melakukan copy file dari file-server ke PC user, melakukan copy file dari PC user ke file-server, open file secara langsung dari file-server, dan melakukan traceroute ke file-server. Pengujian pertama melakukan PING ke IP Address File Server: 192.168.1.3.

```
C:\Windows\System32\cmd.exe - ping 192.168.1.3 -t
C:\WINDOWS\system32>ping 192.168.1.3 -t
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1730ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1260ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1837ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1269ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1271ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1633ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1089ms TTL=124
Reply from 192.168.1.3: bytes=32 time=905ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1177ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1273ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1450ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1633ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1635ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1635ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1817ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1892ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1892ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1269ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1215ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1309ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1894ms TTL=124
Reply from 192.168.1.3: bytes=32 time=728ms TTL=124
Rep
```

sumber: Sidik, Ade Sudaryana (2019)
Gambar 8. Pengujian awal jaringan usulan

PING tes dari PC user Citereup ke IP Address File Server. Hasilnya yaitu time to live paket data 124 bit, dan time untuk menuju file server yaitu rata-rata 1000 ms.

Eksekusi	Nama File	Size	Waktu
Buka Folder dari simpan data – share	-	-	8 detik
Buka Folder dari share - dokumen iml	-	-	10 detik
buka dokumen dari file server	pengalaman kerja iml.pptx	79 KB	20 detik
Copy file pdf dari file server ke komputer citereup	po genset 50 kva area kalimantan.pdf	2-MB	95 detik
buka dokumen pdf dari file server	po genset 50 kva area jateng.pdf	1.3 MB	195 detik
Copy folder dari file server ke komputer citereup	po sewa daya iml	70.8 MB	40 menit
Copy file rar dari komputer citereup ke file server	laporan bulanan.rar	58 MB	28 menit

sumber: Sidik, Ade Sudaryana (2019)
Gambar 9. Load traffic pada jalur VPN Citereup

Pengujian kedua dengan *copy file* dari *file server* ke PC user Citereup dengan ukuran file 70.8 MB.

Sumber: Sidik, Ade Sudaryana (2019)

Gambar 10. Copy file dari file server ke komputer Citereup

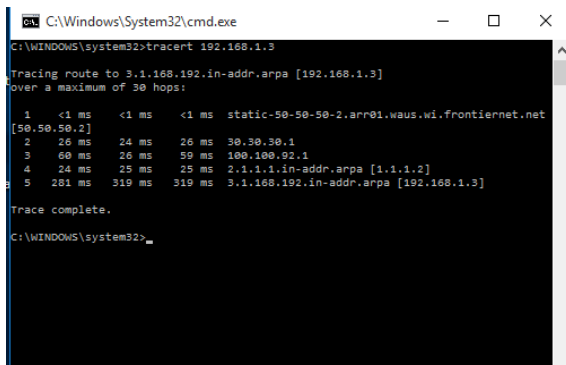
Berikut tabel dari hasil pengujian jaringan awal yang dilakukan di kantor cabang Citereup PT Indo Matra Lestari dalam membuka akses *file server*.

Tabel 1

Proses *write*, *copy* dan *buka file* pada komputer server Cabang Citeureup

sumber: Sidik, Ade Sudaryana (2019)

Pengujian terakhir yaitu melakukan *traceroute* ke *file-server* dari PC user kantor cabang Citereup.

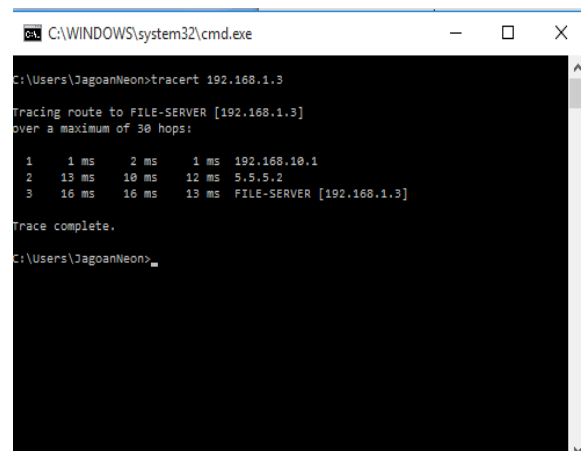


sumber: Sidik, Ade Sudaryana (2019)

Gambar 11. Traceroute file server dari komputer Citereup

b. Pengujian Jaringan Akhir

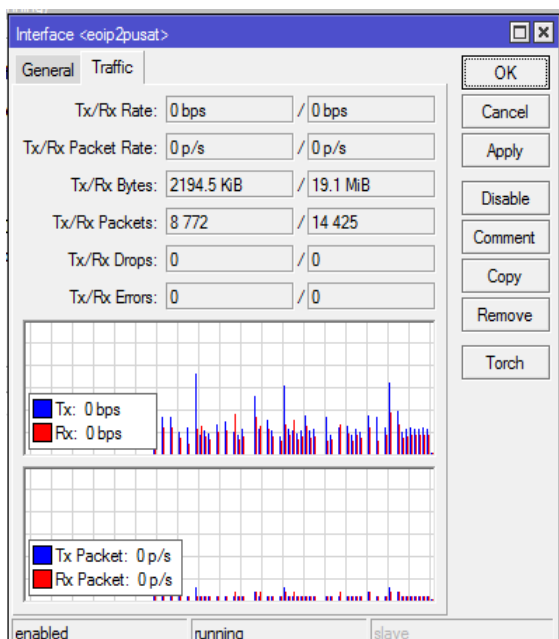
Pengujian jaringan usulan ini dilakukan dengan cara yang sama pada pengujian jaringan awal, yaitu PING ke ip file-server, melakukan copy file dari file-server ke PC user, melakukan copy file dari PC user ke file-server, open file secara langsung dari file-server, dan melakukan traceroute ke file-server. Pengujian dilakukan setelah EoIP Tunnel diimplementasikan pada jaringan PT Indo Matra Lestari. Pengujian pertama PING ke file server dari PC user Citereup, IP Address: 192.168.1.3. Perubahan setelah ada EoIP Tunnel yaitu time to live paket data 126 bit, dan time untuk menuju file server yaitu rata-rata 200 ms. *Traceroute* ke *file-server* dari PC user kantor cabang Citereup.



sumber: Sidik, Ade Sudaryana (2019)

Gambar 12. Traceroute file server dari komputer Citereup setelah EoIP Tunnel

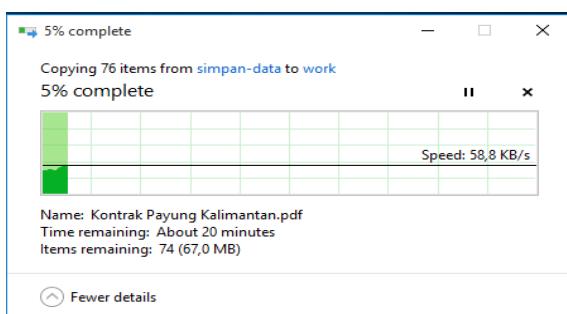
Dari gambar diatas terdapat 3 hops untuk mencapai file server dari PC user kantor cabang Citereup setelah ada EoIP Tunnel.



Sumber: Sidik, Ade Sudaryana (2019)

Gambar 13. Traffic data EoIP Tunnel pada mikrotik router kantor cabang Citereup

Pengujian kedua dengan copy file dari file server ke PC user Citereup dengan ukuran file 70.8 MB.



sumber: Sidik, Ade Sudaryana (2019)

Gambar 14. Copy file dari file server ke komputer Citereup setelah ada EoIP Tunnel

Setelah melakukan tes pada jaringan awal dan jaringan usulan maka didapatkan hasil tabel perbandingannya adalah sebagai berikut:

Tabel 2

Perbandingan hasil pengujian awal jaringan berjalan dengan pengujian akhir jaringan usulan

Eksekusi	Nama File	Size	Waktu Jaringan Awal	Waktu Jaringan Usulan
Buka Folder dari simpan data – share	-	-	8 detik	3 detik
Buka Folder dari share - dokumen iml	-	-	10 detik	5 detik
buka dokumen dari file server	pengalaman kerja iml.pptx	79 KB	20 detik	26 detik

Copy file pdf dari file server ke komputer citereup	po genset 50 kva area kalimantan.pdf	1.2 MB	95 detik	30 detik
buka dokumen pdf dari file server	po genset 50 kva area jateng.pdf	1.3 MB	195 detik	17 detik
Copy folder dari file server ke komputer citereup	po sewa daya iml	70.8 MB	40 menit	20 menit
Copy file rar dari komputer citereup ke file server	laporan bulanan.rar	58 MB	28 menit	15 menit

Berdasarkan proses pengujian jaringan usulan dengan membuat *link bypass* menggunakan metode EoIP Tunnel antara kantor cabang Citereup dan kantor pusat, didapatkan hasil bahwa untuk *copy*, *write*, dan *open file* akses ke *file server* menjadi lebih baik daripada pada saat pengujian jaringan awal. Secara umum terdapat kenaikan yang sangat signifikan dari tahapan pengujian diatas, dimana setelah menggunakan metode EoIP Tunnel terdapat peningkatan kecepatan rata-rata sebesar 48% dalam pengiriman data dari kantor cabang Citereup dan kantor pusat maupun sebaliknya.

KESIMPULAN

Setelah melakukan riset dan analisis pada jaringan internet yang ada di PT Indo Matra Lestari penulis menarik kesimpulan, bahwa:

1. EoIP Tunnel yang memanfaatkan fitur *tunneling* untuk *bridging* antar router mikrotik dapat membuat akses *point to point* menjadi lebih cepat.
2. Akses ke file server baik eksekusi file, *write*, *copy*, dan membuka file yang dilakukan dari kantor cabang Citereup menjadi lebih cepat setelah adanya jalur *bypass* ke kantor pusat dengan memanfaatkan fitur *tunneling* dari EoIP Tunnel. Terdapat peningkatan kecepatan sebesar 48% dalam proses pengiriman data (*data transfer*)
3. Dari segi keamanan, walau EoIP Tunnel tidak melakukan enkripsi seperti VPN (*Virtual Private Network*) namun EoIP masih bisa *secure* dengan mengaktifkan fitur firewall, *filtering* dan monitoring pada interface-interface EoIP.
4. Pembuatan EoIP Tunnel tidak memerlukan biaya tambahan karena EoIP Tunnel merupakan salah satu fitur dari router mikrotik.
5. Untuk durasi waktu saat *open file* yang ada di file server secara langsung dari PC user kantor Citereup bervariasi tergantung dari spesifikasi PC user tersebut.

REFERENSI

- Cahyadi, D. (2010). Pemanfaatan Fitur Tunneling Menggunakan Virtual Interface EoIP di MikrotikRouterOS Untuk Koneksi Bridging Antar Kantor Melalui Jaringan ADSL Telkom Speedy. *Jurnal Informatika Mulawarman*, 5(2), 50–54.
- Kurniawan, W. (2007). *Jaringan Komputer*. Yogyakarta: Penerbit ANDI.
- Meyatmaja, E., & Syafrizal, M. (2012). PERANCANGAN VIRTUAL PRIVATE NETWORK PADA PIKA MEDIA KOMUNIKA. *Jurnal DASI*, 13(4), 11–16.
- Pramana, I. J., Widyastuti, N., & Triyono, J. (2014). IMPLEMENTASI RADIUS SERVER PADA JARINGAN VIRTUAL PRIVATE NETWORK. *Jurnal JARKOM*, 1(2), 122–130.
- Riadi, I. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. *Jurnal Sistem Informasi Indonesia*, 1(1), 71–80.
- Sumarno, E., & Probo Hasgoro, H. (2013). Implementasi metode load balancing dengan dua jalur. *Indonesian Journal on Networking and Security*, 2(1), 28–34.
- Triyono, J., Rachmawati, Y., & Dhimas Irnawan, F. (2014). ANALISIS PERBANDINGAN KINERJA JARINGAN VPN BERBASIS MIKROTIK MENGGUNAKAN PROTOKOL PPTP DAN L2TP SEBAGAI MEDIA TRANSFER DATA. *Jurnal JARKOM*, 1(2), 112–121.