

Perancangan Jaringan VPN Menggunakan Metode Point To Point Tunneling Protocol

Bambang Supriyanto¹, Suharyanto²

¹STMIK Nusa Mandiri

e-mail: Bambangupriyanto1911@gmail.com

²Universitas Bina Sarana Informatika

e-mail: suharyanto@bsi.ac.id

Abstract - PT. Hail Otis Logistics is a Forwarding and Expedition Company that provides Custom Clearance Export and Import services as well as Shipping or Delivery from Partner Companies to Tanjung Priuk Port and vice versa. Currently PT. Hail Otis Logistics is sending company data using e-mail, so the company cannot yet ensure the security of the data sent. Due to the company's problems, designing a VPN is a means of communicating and transferring data securely and maintaining data validity. In this study VPN was built using the PPTP (Point To Point Tunneling Protocol) method to build a VPN network at PT. Hail Otis Logistics. Use PPTP because this method uses a protocol that allows point to point relationships that pass through the IP network. Results obtained in VPN development at PT. Hail Otis Logistics are VPN networks that can connect between headquarters and branch offices to transfer data safely. VPN development can provide security with encryption in every data communication.

Keywords: PPTP, Network, VPN

PENDAHULUAN

Semakin berkembangnya teknologi informasi sekarang ini, maka kebutuhan akan informasi semakin meningkat. 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 koneksi internet yang cepat dan stabil. 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 dan stabil. Oleh karena itu VPN diciptakan untuk menyelesaikan permasalahan dalam jaringan yang tidak aman.

Menurut Mufida, Irawan, & Chrisnawati, (2017:3) "VPN adalah sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antar jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur privacy dalam komunikasinya. Sifat pribadi VPN berarti bahwa traffic data VPN yang pada umumnya tidak terlihat, atau di enkapsulasi oleh lalu lintas jaringan yang mendasarinya. Dalam istilah yang lebih teknis, di link lapisan protokol jaringan virtual dikatakan terowongan atau tunnel yang melewati jaringan transportasi yang mendasarinya. Istilah VPN dapat

digunakan untuk menggambarkan berbagai macam konfigurasi jaringan dan protocol".

Sedangkan menurut Supendar, (2016:2) "Virtual Private Network (VPN) adalah sebuah teknologi komunikasi jaringan yang memungkinkan untuk dapat terkoneksi ke jaringan public dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan di dapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik public".

Sedangkan dari sisi perusahaan PT.Hail Otis Logistik yang memiliki beberapa kantor pusat dan kantor cabang sangat diperlukan untuk memudahkan komunikasi dan FILE SHARING antara user dan server maupun sesama user sehingga waktu yang terpakai menjadi lebih Efisien.

Permasalahan yang ada pada PT.Hail Otis Logistik yaitu belum terkoneksi antara kantor pusat yang berada di Jakarta Barat dengan kantor cabang yang berada di Jakarta Utara hal ini menyebabkan sulitnya transfer data atau sharing data dan juga dalam transfer data ini user masih menggunakan media internet seperti email karena banyak data-data penting yang terdapat didalamnya yang sangat rentan jika email itu sendiri diretas oleh pihak yang tidak bertanggung jawab.

II. METODE PENELITIAN

Metode Penelitian adalah salah satu cara bagaimana memahami suatu pembahasan, permasalahan dan pemecahannya. Metode penelitian yang penulis gunakan adalah:

Metode Pengumpulan Data

Dalam melakukan pengumpulan data untuk penulisan skripsi ini maka diperlukan data yang baik dan akurat sehingga penulis menggunakan beberapa metode pengumpulan data sebagai berikut:

a. Observasi

Metode Observasi adalah metode pengumpulan data dengan terjun langsung ke kantor PT. Hail Otis Logistik untuk melakukan pengamatan, pencatatan informasi mengenai penggunaan VPN dengan metode PPTP pada PT. Hail Otis Logistik

b. Wawancara

Metode wawancara yakni suatu metode pengumpulan data yang penulis menggunakan untuk berinteraksi dengan IT dan Direktur PT. Hail Otis Logistik.

c. Studi Pustaka

Penulis mendapatkan banyak tambahan penulisan dengan membaca banyak buku- buku, jurnal dan referensi yang berkaitan dengan jaringan komputer.

Analisa Penelitian

Sebelum melakukan perancangan VPN, penulis melakukan analisa yang terbagi menjadi beberapa bagian yaitu :

a. Analisa Kebutuhan.

Dalam tahap ini penulis melakukan analisis kebutuhan apa saja yang digunakan untuk merancang Jaringan private untuk transfer data yang lebih aman, maka dari itu diperlukan jaringan VPN dengan metode PPTP.

b. Desain

Pada tahap ini penulis memulai merancang skema jaringan VPN dengan metode PPTP.

c. Testing

Untuk mengetahui proses transfer data jaringan private berjalan dengan lancar dan aman, maka penulis melakukan perancangan jaringan VPN dengan metode PPTP.

d. Implementasi

Di tahap ini akan diterapkan semua yang telah di rencanakan dan di rancang sebelumnya. Tahap penerapan implementasi ini merupakan tahap yang sangat menentukan dari berhasil atau gagal project yang akan di bangun.

Virtual Private Network (VPN)

Menurut (Supendar, 2016:2) “Virtual Private Network (VPN) adalah sebuah teknologi komunikasi jaringan yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan di dapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik”.

Menurut (Mufida, Irawan, & Chrisnawati, 2017:3) “VPN adalah sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antar jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur privasi dalam komunikasinya”.

Menurut (Seta, Ridwan, & Wati, 2015:1) “VPN merupakan suatu jaringan private yang mempergunakan sarana jaringan komunikasi public yaitu internet dengan memakai tunneling protocol sebagai prosedur pengamanannya. VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik, infrastruktur publik yang paling banyak digunakan adalah jaringan internet. Didalam VPN terdapat perpaduan teknologi tunneling dan enkripsi yang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan”.

Menurut Triyono, Rachmawati K., & Irnawan, (2014:1) “Virtual Private Network (VPN) adalah sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antar jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur privacy dalam komunikasinya”.

Menurut sofana dalam (Burhanuddin & Badrul, 2014:3) “VPN atau Virtual Private Network adalah teknologi jaringan komputer yang memanfaatkan media komunikasi publik (open connection atau virtual circuits), seperti internet, untuk menghubungkan beberapa jaringan lokal. Informasi yang berasal dari node-node VPN akan “dibungkus” (tunneled) dan kemudian mengalir melalui jaringan public”. Sehingga

informasi menjadi aman dan tidak mudah dibaca oleh yang lain.

Menurut (Akhirianto & Wandanaya, 2016:2) “Virtual Private Network (VPN) berfungsi untuk menghubungkan kantor pusat dengan kantor cabang melalui jaringan publik dengan membuat suatu jalur pribadi yang diumpamakan sebagai terowongan (tunnel) dengan menggunakan fasilitas jalur yang sudah tersedia (internet) yang memungkinkan dua cabang kantor untuk melakukan komunikasi secara aman”. Dengan adanya teknologi ini, penekanan biaya dapat dilakukan pada proses penambahan infrastruktur yang ada di dalam perusahaan karena perusahaan tidak perlu membangun suatu jaringan fisik baru. Contoh

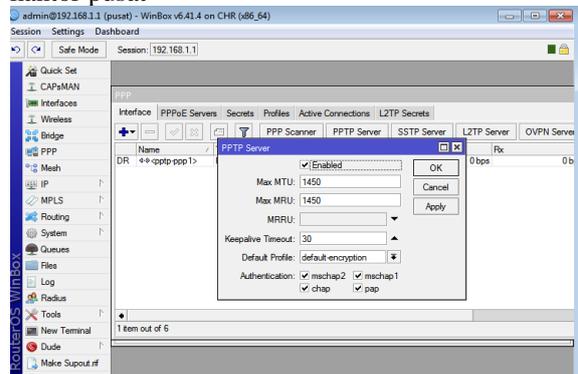
Protokol yang paling sering digunakan adalah PPTP, L2TP, SSTP dan OVPN. Setiap protokol memiliki karakteristik dan kelebihan dan cara kerja masing-masing.

HASIL DAN PEMBAHASAN

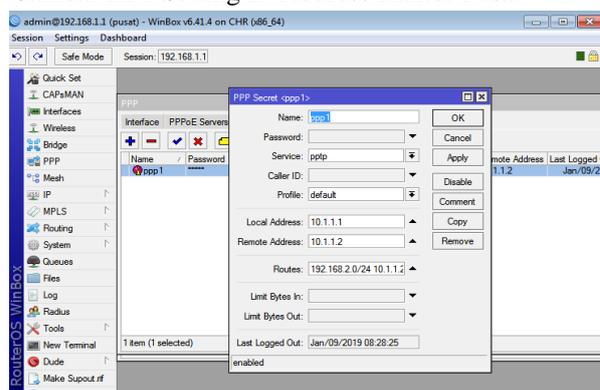
Rancangan Jaringan

Rancangan aplikasi ini penulis menggunakan software simulasi untuk melakukan perancangan jaringan VPN dengan metode PPTP tersebut antara kantor pusat PT. Hail Otis Logistik dengan kantor cabang. Adapun software simulasi yang digunakan adalah GNS3 (Graphic Network Simulation).

1. Konfigurasi PPTP server pada router kantor pusat



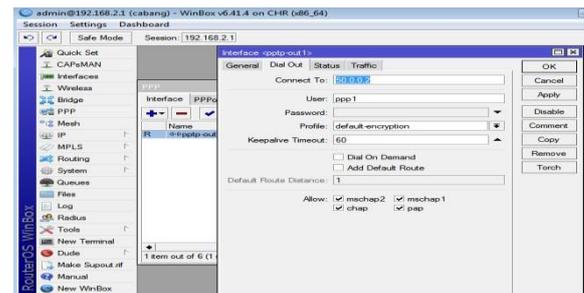
Gambar III.1 Setting IP Address Kantor Pusat



Gambar III.1a Setting IP Address Kantor Pusat

Langkah awal yang harus dilakukan adalah mengaktifkan PPTP Server. Masuk pada menu PPP->interface->PPTP Server. Gunakan profile “default- encryption” agar jalur VPN terenkripsi. Secret disini kita menentukan username dan password untuk proses autentikasi client yang akan terkoneksi ke PPTP server. Penggunaan huruf besar dan kecil berpengaruh. Local address adalah alamat ip yang akan terpasang pada router itu sendiri (router pusat/PPTP Server) setelah link terbentuk, remote address adalah ip yang akan diberikan ke client setelah link PPTP terbentuk. Perintah diatas berfungsi agar router kantor pusat dapat mengenali ipmana yang diperbolehkan melakukan komunikasi dengan router pusat. Dalam kondisi ini ip local kantor cabang yang akan di daftarkan di dalam routing table kantor pusat, karena ip local tersebut yang dibutuhkan untuk melakukan akses ke kantor pusat.

2. Konfigurasi PPTP Client pada router kantor cabang



Gambar III.3 Setting PPTP Kantor Cabang

Langkah untuk melakukan konfigurasi Client PPTP pada Router Mikrotik adalah tambahan interface baru PPTP Client lakukan dial ke IP Public Router pusat (PPTP Server) lalu masukkan username dan password sesuai pengaturan PPTP server. 50.0.0.2 adalah IP Public dari Server yang sesuai dengan kantor pusat.

Sesuai koneksi PPTP terbentuk, akan muncul IP Address baru di kedua Router dengan Flag yang menempel di interface PPTP sesuai dengan pengaturan Sectar pada PPTP Server.

Perintah diatas berguna untuk memberikan akses pada IP Address mana yg dapat berkomunikasi dengan kantor cabang. Hal ini dilakukan agar komunikasi antara kantor cabang dan kantor pusat berjalan dengan baik sehingga proses kirim dan terima file berjalan dengan efisien.

Manajemen Jaringan

Manajemen yang dilakukan penulis dalam VPN dengan metode PPTP ini adalah menambahkan sebuah administrator dapat memilah IP address mana yang berasal dari kantor cabang yang

diperbolehkan melakukan komunikasi dengan kantor pusat, begitu pula sebaliknya. Hal ini sangat memudahkan administrator dalam melakukan manajemen jaringan sehingga apabila PT. Hail Otis Logistik berkembang dan menjadi besar maka proses manajemen nya sudah terstruktur dan siap untuk dikembangkan lebih kompleks lagi.

Pengujian Jaringan

Pada tahap ini penulis melakukan uji coba terhadap jaringan komputer yang berada pada PT Hail Otis Logistik. Hal ini perlu dilakukan karena pengujian ini dilakukan untuk mengetahui apakah jaringan komputer PT Hail Otis Logistik sudah berjalan dengan optimal seperti yang diharapkan.

Pengujian Jaringan Awal

a. Ping dari PC pusat (192.168.1.2) kearah Router dan Internet pusat (192.168.1.1 & 50.0.0.1)

```
PC-1> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=1.516 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.018 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=3.513 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=2.283 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=2.585 ms
```

```
PC-1> ping 50.0.0.1
84 bytes from 50.0.0.1 icmp_seq=1 ttl=63 time=2.485 ms
84 bytes from 50.0.0.1 icmp_seq=2 ttl=63 time=5.200 ms
84 bytes from 50.0.0.1 icmp_seq=3 ttl=63 time=2.864 ms
84 bytes from 50.0.0.1 icmp_seq=4 ttl=63 time=4.856 ms
84 bytes from 50.0.0.1 icmp_seq=5 ttl=63 time=2.476 ms
```

Gambar III.4 Test Ping dari Pc ke Router Pusat dan Gateway ISP

Ping dari router pusat (192.168.1.1) ke arah gateway internet (50.0.0.1)

```
[admin@pusat] > ping 50.0.0.1
SEQ HOST                SIZE TTL TIME STATUS
0 50.0.0.1              56 64 1ms
1 50.0.0.1              56 64 1ms
2 50.0.0.1              56 64 2ms
3 50.0.0.1              56 64 3ms
4 50.0.0.1              56 64 1ms
5 50.0.0.1              56 64 1ms
6 50.0.0.1              56 64 3ms
7 50.0.0.1              56 64 1ms
8 50.0.0.1              56 64 1ms
sent=9 received=9 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=3ms
```

Gambar III.5 Test Ping dari Router Pusat ke Gateway Internet Servis Provider

b. Ping dari router pusat (50.0.0.1) kearah ip public router kantor cabang (60.0.0.1)

```
[admin@pusat] > ping 60.0.0.1
SEQ HOST                SIZE TTL TIME STATUS
0 60.0.0.1              56 64 3ms
1 60.0.0.1              56 64 3ms
2 60.0.0.1              56 64 1ms
3 60.0.0.1              56 64 1ms
4 60.0.0.1              56 64 1ms
5 60.0.0.1              56 64 2ms
6 60.0.0.1              56 64 1ms
7 60.0.0.1              56 64 1ms
sent=8 received=8 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=3ms
```

Gambar III.6 Test Ping dari Router Pusat ke Ip Public Cabang

c. Ping dari router pusat (50.0.0.2) kearah ip local client kantor cabang (192.168.2.2)

```
[admin@pusat] > ping 192.168.2.2
SEQ HOST                SIZE TTL TIME STATUS
0 192.168.2.2          56 63 3ms
1 192.168.2.2          56 63 5ms
2 192.168.2.2          56 63 4ms
3 192.168.2.2          56 63 4ms
4 192.168.2.2          56 63 11ms
5 192.168.2.2          56 63 5ms
6 192.168.2.2          56 63 4ms
7 192.168.2.2          56 63 6ms
8 192.168.2.2          56 63 4ms
9 192.168.2.2          56 63 4ms
10 192.168.2.2         56 63 7ms
sent=11 received=11 packet-loss=0% min-rtt=3ms avg-rtt=5ms max-rtt=11ms
```

Gambar III.7 Test Ping dari Router Pusat ke Ip Lokal Cabang

d. Ping dari router kantor cabang (60.0.0.2) menuju ip pubic kantor pusat (192.168.1.1)

```
[admin@cabang] > ping 192.168.1.1
SEQ HOST                SIZE TTL TIME STATUS
0 192.168.1.1          56 64 2ms
1 192.168.1.1          56 64 5ms
2 192.168.1.1          56 64 3ms
3 192.168.1.1          56 64 4ms
4 192.168.1.1          56 64 4ms
5 192.168.1.1          56 64 4ms
6 192.168.1.1          56 64 3ms
7 192.168.1.1          56 64 3ms
sent=8 received=8 packet-loss=0% min-rtt=2ms avg-rtt=3ms max-rtt=5ms
```

Gambar III.8 Test Ping dari Router Cabang ke Ip Public pusat

e. Ping dari router cabang (60.0.0.2) kearah ip public router kantor pusat (50.0.0.2)

```
[admin@cabang] > ping 50.0.0.2
SEQ HOST                SIZE TTL TIME STATUS
0 50.0.0.2              56 63 1ms
1 50.0.0.2              56 63 3ms
2 50.0.0.2              56 63 6ms
3 50.0.0.2              56 63 3ms
4 50.0.0.2              56 63 3ms
5 50.0.0.2              56 63 3ms
6 50.0.0.2              56 63 3ms
7 50.0.0.2              56 63 3ms
sent=8 received=8 packet-loss=0% min-rtt=1ms avg-rtt=3ms max-rtt=6ms
```

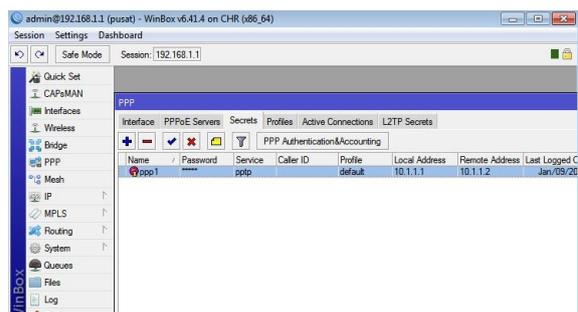
Gambar III.9 Test Ping dari Router Cabang ke Ip Router Pusat

Hasil pengetesan sebelum dilakukan konfigurasi VPN dengan metode PPTP dapat disimpulkan bahwa komunikasi jaringan public antara kantor pusat dan kantor cabang dapat berkomunikasi. Hal ini memang wajar karena jaringan tersebut bersifat public dan dapat diakses siapapun. Tetapi untuk jaringan local antara router pusat dan router cabang belum bisa berkomunikasi (tidak dapat dijangkau). Hal ini dikarenakan tidak adanya protocol yang dapat menghubungkan jaringan tersebut secara private.

Pengujian Jaringan Akhir

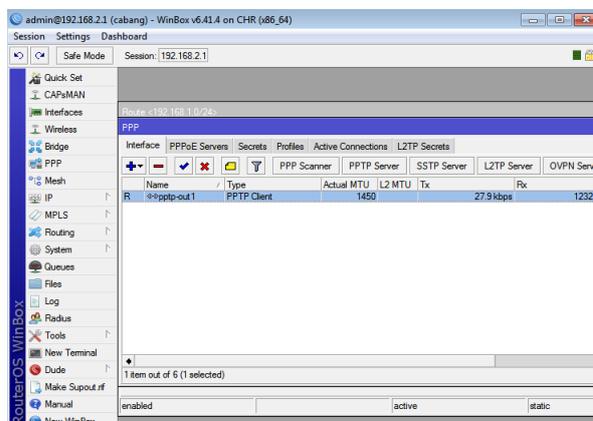
Pada pengujian akhir ini penulis melakukan test jaringan VPN dengan metode PPTP dan memastikan jaringan tersebut berjalan dengan baik.

a. Memastikan PPTP server aktif dan sudah berhasil digunakan (dilihat dari router pusat)



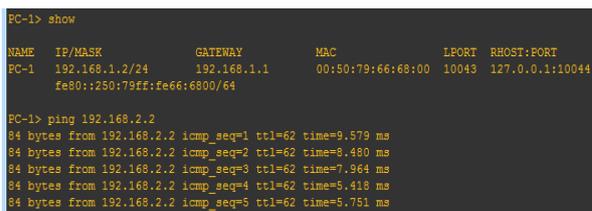
Gambar III.10 PPTP Server Aktif

b. Memastikan router kantor cabang terkoneksi dengan router kantor pusat



Gambar III.11 PPTP Client Aktif

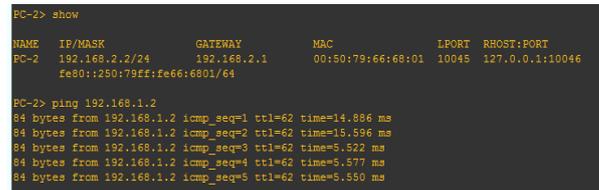
c. Melakukan test koneksi dengan melakukan ping dari jaringan lokal pada kantor pusat (192.168.1.2) menuju jaringan local pada kantor cabang (192.168.2.2)



Gambar III.12 Test Ping Jaringan Local Client Pusat ke Client Kantor Cabang.

d. Melakukan test koneksi dengan melakukan ping

dari jaringan local kantor cabang (192.168.2.2) menuju jaringan local pada kantor pusat (192.168.1.2)



Gambar III.13 Test Ping Jaringan Client Local Cabang ke Client Kantor Pusat

Dari hasil pengujian diatas dapat disimpulkan bahwa penggunaan VPN dengan metode PPTP sudah berjalan dengan baik, dan data yang dikirim dan di terima langsung end to end menuju ip yang dituju.

KESIMPULAN

Berdasarkan hasil analisa, perancangan dan pembahasan yang telah di sampaikan dalam bab-bab sebelumnya, maka di ambil kesimpulan sebagai berikut

1. Topologi jaringan komputer yang terpada antara kantor pusat dan kantor cabang akan meningkatkan proses komunikasi data yang efektif .
2. Adanya autentikasi dan enkripsi dalam VPN mendukung keamanan dan pertukaran data sehingga kerahasiaan data lebih terjamin.
3. Hasil penelitian ini membuktikan bahwa VPN dengan PPTP dapat digunakan untuk mendukung rancangan infrastruktur jaringan komputer antar kantor pusat berada di Jakarta barat dan kantor cabang yang berada di Jakarta utara. Proses tunneling dengan PPTP akan membuat jalur dan komunikasi data yang lebih aman dengan proses enkripsi pada setiap pengiriman paket datanya.

Berdasarkan hasil analisis dan penjelasan di atas, dapat diusulkan beberapa saran sebagai berikut:

1. Dibutuhkan sumber daya manusia yang mampu mengelola system jaringan komputer dalam lingkungan PT. Hail Otis Logistik.
2. Perlu ada penelitian yang lebih mendalam dalam hal system keamanan data yang di transmisikan melalui system jaringan private.

REFERENSI

Akhirianto, P. M., & Wandanaya, A. B. (2016). Perancangan Data Transmisi Jaringan

- Komputer Berbasis Open VPN Dengan Metode Pptp Pada CV. Margo Jaya Jakarta (September), 62–69.
- Ginta, P. W., Kusuma, G. P., & Negara, E. K. (2013). Implementasi Tools Network Mapper Pada Lokal Area Network (LAN) , 9(2).
- Halawa, S. (2016). Perancangan Aplikasi Pembelajaran Topologi Jaringan Komputer Untuk Sekolah Menengah Kejuruan (Smk) Teknik Komputer Dan Jaringan (Tkj) Dengan Metode Computer Based Instruction, 66– 71.
- Juliharta, K. (2013). Distribusi Konten Web Server Menggunakan Motode Content Delivery Network, 159–169.
- Khadijah, Y. H. (2014). Analisi Perbandingan Manajemen Jaringan Berbasis Mikrotik Dengan Cisco, 1–6.
- Mufida, E., Irawan, D., & Chrisnawati, G. (2017). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal Matrik*, 16(2), 9. <https://doi.org/10.30812/matrik.v16i2.7>
- Seta, H. B., Ridwan, M., & Wati, T. (2015). Perbandingan Virtual Private Network Protokol Menggunakan Point to Point Tunnel Protocol dan OpenVPN. *Konferensi Nasional Sistem & Informatika, (Perbandingan Vpn)*, 1–6.
- Supendar, H. (2016). Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik. *Bina Insani Ict Journal*, 3(1), 85–98. <https://doi.org/10.1016/j.toxicon.2013.12.002>
- Triyono, J., Rachmawati K., R. Y., & Irnawan, F. D. (2014). Analisis Perbandingan Kinerja Jaringan Vpn Berbasis Mikrotik Menggunakan Protokol Pptp Dan L2tp Sebagai Media Transfer Data, 1(2), 20–29.
- Warsito, & Astuti, B. R. T. (2013). Perancangan dan instalasi jaringan Local Area Network Sekolah Menengah Kejuruan Muhammadiyah Enam Gemolong Sragen. *Indonesian Journal on Networking and Security*, 2(2), 1–7.

PROFIL PENULIS

Bambang Supriyanto, Lulus Sekolah Tinggi Manajemen Informatika Komputer Nusa Mandiri Jakarta dengan program studi tehnik informatika. Suharyanto, Lahir di Jakarta, tahun 1974, Staff pengajar pada Universitas BSI Jakarta. Sampai saat ini masih aktif mengajar, sangat menyukai bidang ecommerce banyak memberikan bimbingan kepada mahasiswa terkait aplikasi bisnis ecommerce.