

# Simulasi Penggunaan L2TP VPN pada Komunikasi Satelit *Male Kombatan* Menggunakan GNS3

Iwan Nofi Yono Putro, Irma Rismayanti, Yanuar Prabowo,  
Rudi Choirul Anwar

iwan.nofi@lapan.go.id  
(29 Desember 2020)

---

## ABSTRAK

MALE (*Medium Altitude Long Endurance*) *Kombatan* merupakan sebuah produk hasil kerjasama dari beberapa lembaga, yaitu Kementerian Pertahanan Republik Indonesia (Ditjen Potan dan Balitbang), TNI Angkatan Udara, Badan Pengkajian dan Penerapan Teknologi (BPPT), Lembaga Penerbangan dan Antariksa Nasional (LAPAN), PT Dirgantara Indonesia, PT Lembaga Elektronik Nasional (PT LEN), dan Institut Teknologi Bandung (ITB). Pusat Teknologi Penerbangan (Pustekbang) merupakan salah satu bagian dari LAPAN yang bergerak dalam teknologi penerbangan. Tim Pustekbang telah mendesain sebuah topologi jaringan yang nantinya akan digunakan untuk sistem komunikasi MALE *Kombatan* dengan metode komunikasi BLOS (*Beyond Line of Sight*) yang memungkinkan pesawat dapat berkomunikasi dengan server dan GCS melalui satelit tanpa adanya *obstacle* yang mengganggu. Untuk memastikan desain topologi jaringan yang dibuat oleh tim Pustekbang dapat diaplikasi dengan baik pada MALE *Kombatan*, maka tim melakukan simulasi komunikasi menggunakan *software*. Simulasi ini dilakukan karena dianggap lebih hemat biaya dan dapat dilakukan berkali-kali tanpa adanya potensi kerusakan pada *hardware* di MALE *Kombatan*. Perangkat lunak yang digunakan untuk simulasi ini adalah GNS3, karena dianggap lebih baik digunakan untuk simulasi ini. Selain itu GNS3 telah berlisensi GNU dan dapat mendukung

banyak jenis perangkat jaringan serta dapat terkoneksi dengan *hardware* lain. Simulasi dilakukan dengan uji komunikasi dengan menggunakan VPN L2TP. Uji komunikasi yang dilakukan adalah dengan mencatat waktu yang dibutuhkan untuk melakukan *ping* dari UAV ke Server dan dari Server ke UAV.

**Kata kunci:** MALE, Simulasi, GNS3, Topologi jaringan, VPN.

### *ABSTRACT*

*Combatants MALE (Medium Altitude Long Endurance) is a product of cooperation from several institutions, namely the Ministry of Defense of the Republic of Indonesia (Ditjen Pothan and Balitbang), TNI Air Force, Agency for the Assessment and Application of Technology (BPPT), National Aeronautics and Space Agency (LAPAN), PT Dirgantara Indonesia, PT National Electronic Institute (PT LEN), and the Bandung Institute of Technology (ITB). The Aviation Technology Center (Pustekbang) is one part of LAPAN which is engaged in aviation technology. The Pustekbang team has designed a network topology which will later be used for the MALE Combatant communication system with the BLOS (Beyond Line of Sight) communication method which allows the aircraft to communicate with the server and GCS via satellite without any obstructions. To ensure that the network topology design created by the Pustekbang team can be applied properly to MALE Combatants, the team simulated communication using software. This simulation is carried out because it is considered more cost-effective and can be done multiple times without any potential damage to the hardware in MALE Combatants. The software used for this simulation is GNS3, because it is considered better to use for this simulation. In addition, GNS3 has GNU license and can support many types of network devices and can be connected to other hardware. The simulation is carried out by means of a communication test using L2TP VPN. The communication test is done by recording the time needed to ping from UAV to Server and from Server to UAV.*

**Keywords:** MALE, Simulation, GNS3, Network topology, VPN.

# 1. Pendahuluan

## 1.1. Latar belakang

MALE (*Medium Altitude Long Endurance*) Kombatant merupakan sebuah produk hasil kerjasama dari beberapa lembaga, yaitu Kementerian Pertahanan Republik Indonesia (Ditjen Pothan dan Balitbang), TNI Angkatan Udara, Badan Pengkajian dan Penerapan Teknologi (BPPT), Lembaga Penerbangan dan Antariksa Nasional (LAPAN), PT Dirgantara Indonesia, PT Lembaga Elektronik Nasional (PT LEN), dan Institut Teknologi Bandung (ITB). Pusat Teknologi Penerbangan (Pustekbang) merupakan salah satu bagian dari LAPAN yang bergerak dalam teknologi penerbangan. Saat ini, Pustekbang memiliki tim yang terlibat untuk mengembangkan sistem komunikasi pada MALE Kombatant. Sistem komunikasi ini merupakan salah satu fitur penting pada MALE Kombatant, agar pesawat tersebut dapat dikendalikan oleh GCS (*Ground Control Station*). Selain itu, dengan adanya sistem komunikasi pada MALE Kombatant, *engineer* akan mudah untuk mengirimkan dan menerima data yang dibutuhkan.

Tim Pustekbang telah mendesain sebuah topologi jaringan yang nantinya akan digunakan untuk sistem komunikasi MALE Kombatant. Topologi tersebut menggunakan metode komunikasi BLOS (*Beyond Line of Sight*) yang memungkinkan pesawat dapat berkomunikasi dengan server dan GCS melalui satelit tanpa adanya *obstacle* yang mengganggu. Dalam komunikasi BLOS, digunakanlah VPN (*Virtual Private Network*) dengan protokol L2TP (*Layer 2 Tunnel Protocol*). Hal ini memungkinkan setiap komunikasi yang dilakukan UAV dengan GCS dan Server melalui satelit bersifat aman. L2TP memberikan privasi dan keamanan bagi pengguna dengan enkripsi, sehingga komunikasi dengan L2TP dinilai lebih aman.

Untuk memastikan desain topologi jaringan yang dibuat oleh tim Pustekbang dapat diaplikasi dengan baik pada MALE Kombatant, maka tim melakukan simulasi komunikasi menggunakan *software*. Simulasi ini dilakukan karena

dianggap lebih hemat biaya dan dapat dilakukan berkali-kali tanpa adanya potensi kerusakan pada *hardware* di MALE Kombat. Beberapa *software* populer yang dapat digunakan untuk simulasi topologi jaringan, yaitu GNS3 dan Cisco Packet Tracer. Kedua *software* ini bersifat gratis. Namun, berdasarkan hasil perbandingan yang telah dilakukan oleh tim, GNS3 dianggap lebih baik digunakan untuk simulasi ini. Selain itu GNS3 telah berlisensi GNU dan dapat mendukung banyak jenis perangkat jaringan serta dapat terkoneksi dengan *hardware* lain. Dengan menggunakan GNS3 ini, memungkinkan *engineer* untuk melakukan *capture* data menggunakan *software* Wireshark. Dibandingkan dengan GNS3, Cisco Packet Tracer merupakan simulator yang dibuat oleh Cisco dan didedikasikan untuk perangkat Cisco. Meski bersifat gratis, namun simulator ini belum mendukung banyak jenis perangkat jaringan.

## 1.2. Masalah penelitian

Penelitian ini berawal dari permasalahan yang ada dibawah ini:

1. MALE Kombat perlu memiliki sistem komunikasi yang stabil dan baik untuk menerima dan mengirimkan data.
2. Desain topologi jaringan yang telah dibuat, perlu dilakukan uji komunikasi untuk mengetahui kinerjanya.
3. Belum diketahuinya kinerja tipe VPN L2TP pada topologi jaringan yang telah dibuat.
4. Uji komunikasi tidak dapat langsung dilakukan pada MALE Kombat, karena adanya keterbatasan biaya dan tim perlu mengurangi potensi kerusakan pada MALE Kombat.

### 1.3. Tujuan penelitian

Tujuan penelitian dirumuskan sebagai berikut:

1. Mendapatkan desain topologi jaringan yang mendukung sistem komunikasi yang stabil dan baik untuk menerima dan mengirimkan data.
2. Mengetahui kualitas topologi jaringan dengan menggunakan VPN L2TP.
3. Dengan dilakukan uji pada desain topologi jaringan yang telah dibuat, diharapkan tim akan terus melakukan pengembangan terhadap desain topologi jaringan. Sehingga desain topologi jaringan akan jauh lebih optimal ketika diimplementasikan dan diaplikasi di MALE Kombat.
4. Simulasi ini dilakukan sebagai usaha tim Pustekbang untuk mendapatkan desain topologi yang baik tanpa terikat oleh keterbatasan biaya dan juga tidak berpotensi merusak *hardware* MALE Kombat.

### 1.4. Manfaat penelitian

Penelitian ini diharapkan memiliki manfaat:

1. Masing-masing *engineer* dapat mengembangkan ilmu mengenai sistem komunikasi, meski adanya keterbatasan biaya.
2. *Engineer* dapat melakukan simulasi berkali-kali sehingga topologi jaringan dapat diperbaharui untuk mendapatkan topologi jaringan yang lebih optimal.

## 2. Metodologi

Metode yang digunakan dalam penelitian ini adalah *black box* dan studi kasus. Metode *black box testing* dengan tujuan untuk mengetahui apakah fungsionalitas tiap fitur pada aplikasi sistem berjalan seperti perencanaan<sup>[1]</sup>. *Black-Box Testing* merupakan teknik pengujian perangkat lunak yang berfokus pada spesifikasi fungsional dari perangkat lunak<sup>[6]</sup>. *Blackbox Testing* memungkinkan pengembang *software* untuk membuat himpunan kondisi input yang akan melatih seluruh syarat-syarat fungsional suatu program<sup>[6]</sup>.

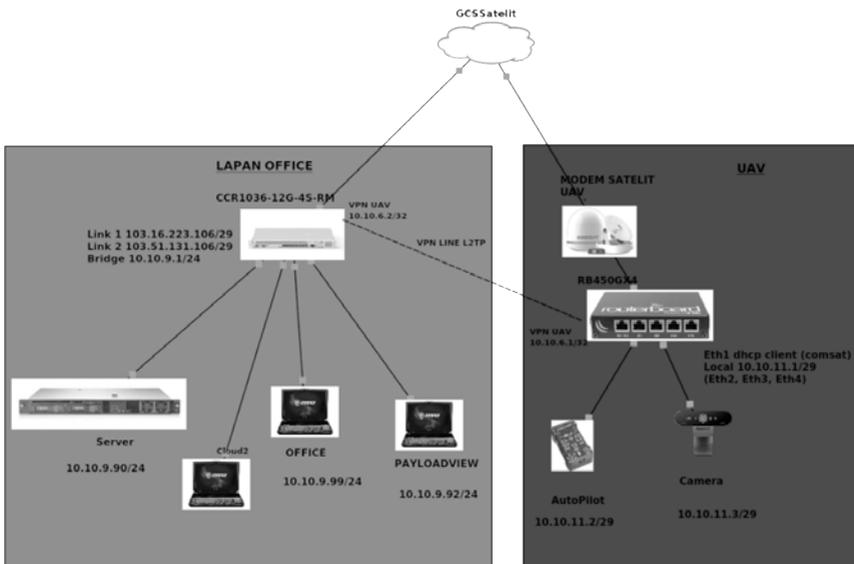
Penggunaan metode *blackbox testing* pada penelitian ini digunakan untuk mengetahui fungsionalitas fitur VPN L2TP pada topologi jaringan yang telah dibuat oleh tim Pustekbang dengan menggunakan GNS3. Topologi jaringan ini merupakan topologi yang nantinya akan diimplementasikan untuk sistem komunikasi MALE Kombat. Dengan mengetahui fungsionalitas fitur VPN L2TP yang disimulasikan pada GNS3, diharapkan tim Pustekbang dapat mengembangkan dan memperbaharui fitur VPN yang akan digunakan agar lebih optimal.

## 3. Hasil dan Pembahasan

### 3.1. Topologi jaringan

Untuk menggambarkan sistem komunikasi MALE Kombat, tim Pustekbang telah membuat topologi jaringan. Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk pola hubungan antar terminal dalam suatu sistem jaringan yang dapat mempengaruhi tingkat efektivitas kinerja jaringan<sup>[4]</sup>. Jaringan komputer adalah sekumpulan satu atau lebih perangkat yang saling terhubung dengan lain melalui media perantara seperti media kabel ataupun media tanpa kabel (nirkabel) sehingga dapat berkomunikasi dengan protokol internet<sup>[3]</sup>. Topologi jaringan tidak bisa dilepaskan dari kinerja sebuah jaringan. Topologi terdiri dari banyak aspek, beberapa

diantaranya adalah *type routing*, VPN (*Virtual Private Network*) dan jenis topologi. Jenis topologi yang sering digunakan adalah *bus*, *ring*, *star*, *mesh* dan *tree*. Dengan adanya gambaran sistem jaringan komputer, memudahkan *engineer* untuk mengetahui alur komunikasi dari sistem komunikasi yang dibuat. Selain itu, topologi jaringan ini dapat diubah-ubah sesuai dengan kebutuhan. Berikut ini adalah topologi jaringan yang telah dibuat oleh tim Pustekbang.



**Gambar 1.** Topologi jaringan L2TP komunikasi satelit MALE

Topologi jaringan yang dibuat menggunakan sistem komunikasi BLOS (*Beyond Line of Sight*). Berdasarkan topologi jaringan pada Gambar 1 dapat diketahui ada 3 titik utama, yaitu UAV (*Unmanned Aerial Vehicle*), GCS (*Ground Control Station*), dan Server. UAV terdiri dari perangkat-perangkat yang lokasinya berpindah-pindah. Sedangkan GCS dan Server merupakan perangkat-perangkat yang lokasinya tetap dan tidak berpindah tempat. Perangkat utama di UAV adalah MikroTik router board yang terhubung

juga dengan Autopilot dan Kamera sebagai payload. Sedangkan perangkat utama di GCS yaitu mikrotik *cloud router* yang terhubung dengan Server dan jaringan di Pusat Teknologi Penerbangan.

Agar UAV dapat dimonitoring serta dapat mengirimkan dan menerima data yang dibutuhkan, maka UAV dan GCS perlu memiliki sistem komunikasi yang stabil dan aman. Dengan menggunakan metode BLOS, memungkinkan UAV dapat dimonitoring oleh GCS dengan menggunakan komunikasi satelit. Selain itu, komunikasi dengan menggunakan satelit tidak terbatas untuk jarak tertentu saja, sehingga memungkinkan UAV dikontrol dari jarak jauh. Untuk komunikasi satelit, digunakan modem satelit Ku Band.

### 3.2. VPN L2TP

Komunikasi satelit mengharuskan perangkat memiliki IP *Public*. Namun, UAV tidak memiliki IP *Public*. Maka dari itu diperlukan koneksi khusus dan *private* agar UAV dapat melakukan komunikasi melalui satelit. Komunikasi *private* dapat dilakukan dengan menggunakan VPN (*Virtual Private Network*). Terdapat beberapa tipe VPN yang dapat digunakan sesuai dengan kebutuhan. Secara umum semua tipe tersebut memiliki fungsi yang sama. Yang membedakan adalah autentikasi dan enkripsi yang digunakan. Topologi jaringan pada Gambar 1 menggunakan tipe VPN L2TP (*Layer 2 Tunnel Protocol*). VPN L2TP memungkinkan komunikasi yang lebih aman karena dilakukan autentikasi tambahan, yaitu Pre-Shared key atau *secret*.

Kelebihan VPN L2TP:

- a. Menggunakan enkripsi IPSec, dan algoritme 3DES/AES dengan kunci 256 bit.
- b. Dapat langsung dipasang dalam sistem operasi Anda. Selain itu, L2TP/IPSec juga terintegrasi dalam banyak perangkat lunak (banyak penyedia VPN menyediakan protokol ini).

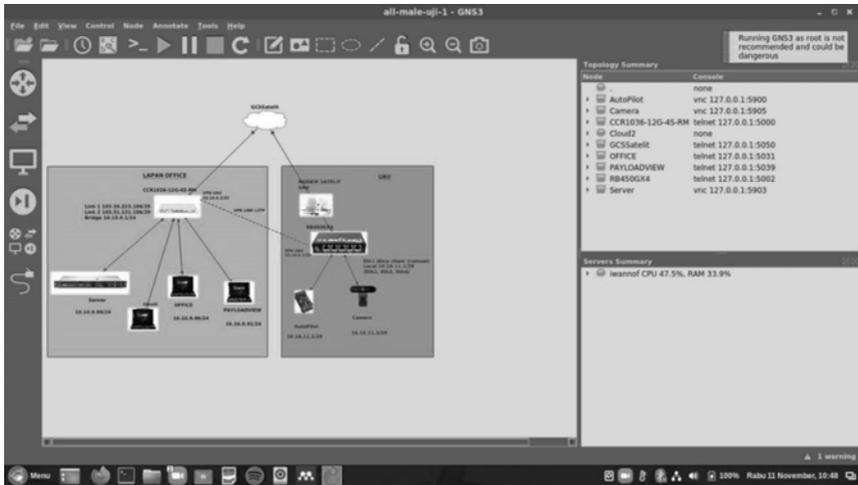
- c. L2TP saat digabungkan dengan IPSec, dikenal sebagai protokol yang sangat aman. Namun, menurut Edward Snowden, L2TP-IPSec telah dieksploitasi oleh NSA (Agen Keamanan Nasional) sebelumnya.
- d. Mudah untuk proses konfigurasi.
- e. Dapat melampaui batas kebanyakan firewall, restriksi jaringan dan ISP<sup>[5]</sup>.

Kekurangan VPN L2TP:

- a. Secara relatif lamban dan diblokir oleh firewall karena menggunakan port yang biasanya diblokir UDP 500.
- b. Stabilitas dan tingkat kehandalan dapat dibandingkan dengan OpenVPN, namun kadang bergantung pada stabilitasi jaringan<sup>[5]</sup>.
- c. Waktu inisiasi lebih lambat dari PPTP<sup>[7]</sup>.

### 3.3. GNS3

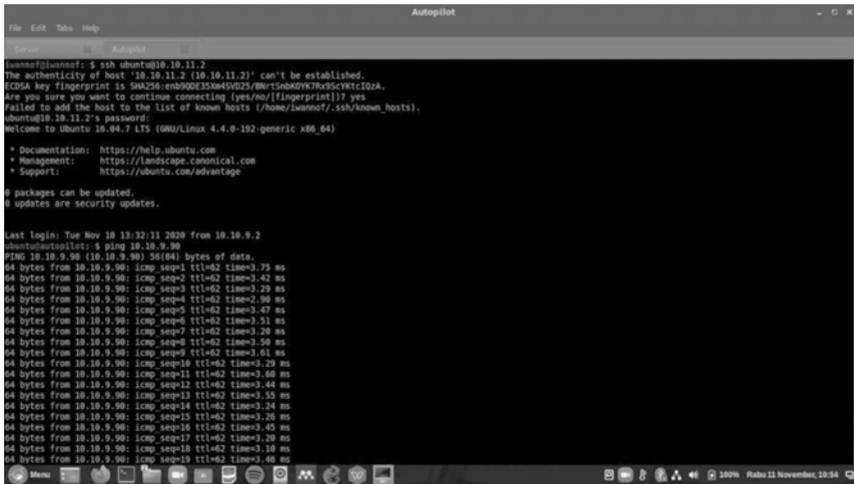
Untuk mengetahui seberapa optimal topologi jaringan yang telah dibuat oleh tim Pustekbang, tim melakukan simulasi dengan menggunakan *software*. *Software* yang digunakan adalah GNS3 (*Graphic Network Simulator-3*) yang bersifat gratis dan telah berlisensi GNU serta dapat mendukung banyak jenis perangkat jaringan serta dapat terkoneksi dengan *hardware* lain. Dengan menggunakan GNS3 ini, memungkinkan *engineer* untuk melakukan *capture* data menggunakan *software* Wireshark. GNS3 adalah *software* simulasi jaringan komputer berbasis GUI yang memungkinkan simulasi jaringan yang kompleks, karena menggunakan *operating system* asli dari perangkat jaringan seperti Cisco, MikroTik dan Juniper bahkan Linux<sup>[2]</sup>. Implementasi topologi jaringan ke simulator GNS3 dapat dilihat pada Gambar 2.



**Gambar 2.** Implementasi topologi jaringan di simulator GNS3

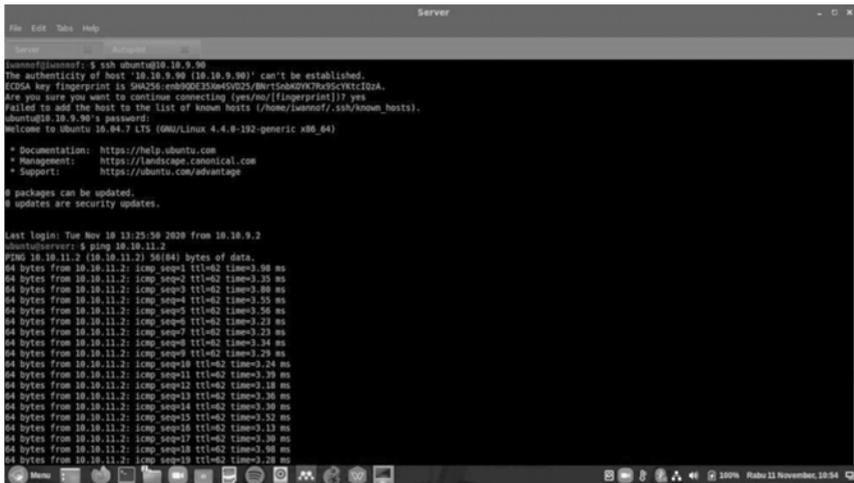
### 3.4. Pengujian

Setelah melakukan implementasi topologi jaringan pada GNS3, maka selanjutnya akan dilakukan uji komunikasi dengan menggunakan VPN L2TP. Uji komunikasi yang dilakukan adalah dengan mencatat waktu yang dibutuhkan untuk melakukan *ping* dari UAV ke Server dan dari Server ke UAV. Pencatatan waktu yang dibutuhkan untuk melakukan *ping* ini berguna untuk mengetahui kualitas topologi jaringan. Ping yang dilakukan dari UAV ke Server digambarkan pada Gambar 3.



Gambar 3. Ping dari UAV ke Server

Sedangkan ping yang dilakukan dari Server ke UAV digambarkan pada Gambar 4.



Gambar 4. Ping dari Server ke UAV

Hasil kegiatan Ping yang dilakukan, dicatatkan pada Tabel 1 di bawah ini.

**Tabel 1.** Hasil pengujian ping

Pengujian	UAV ke server (ms)	Server ke UAV (ms)
1	4,16	3,3
2	4,04	4,31
3	4,64	3,83
4	3,52	3,27
5	3,35	3,58
6	3,47	3,44
7	4,52	3,95
8	3,91	4,79
9	3,54	5
10	4,58	4,83
11	5,11	4,16
12	4,75	3,95
13	4,71	3,63
14	5,32	4,26
15	4,47	3,7
16	3,87	3,8
17	3,45	3,58
18	3,31	3,65
19	3,05	3,65
20	3,21	4,44
21	4,31	4,29
22	3,5	5,27
23	3,2	4,05
24	3,9	3,89
25	3,92	3,6
26	4,11	4,72
27	3,96	4,22
28	4,59	4,88
29	4,13	3,54

**Tabel 1.** Hasil pengujian ping (lanjutan)

Pengujian	UAV ke server (ms)	Server ke UAV (ms)
30	3,53	3,68
31	3,54	3,63
32	3,62	3,42
33	3,94	3,71
34	4,13	4,52
35	4,53	4,31
36	3,84	3,91
37	4,84	3,64
38	4,32	4,97
39	4,21	4
40	4,93	4,03
41	4,04	3,57
42	3,42	3,64
43	3,86	4,44
44	5,2	4,97
45	3,65	3,89
46	4,18	4,03
47	3,98	4,07
48	3,98	3,61
49	4,04	3,36
50	4,65	3,64
51	4,17	3,69
52	4,81	4,59
53	4,34	4,61
54	4,02	3,52
55	3,83	5,22
56	3,68	4,25
57	4,13	4,94
58	3,91	3,97
59	3,76	3,96
60	3,76	3,64

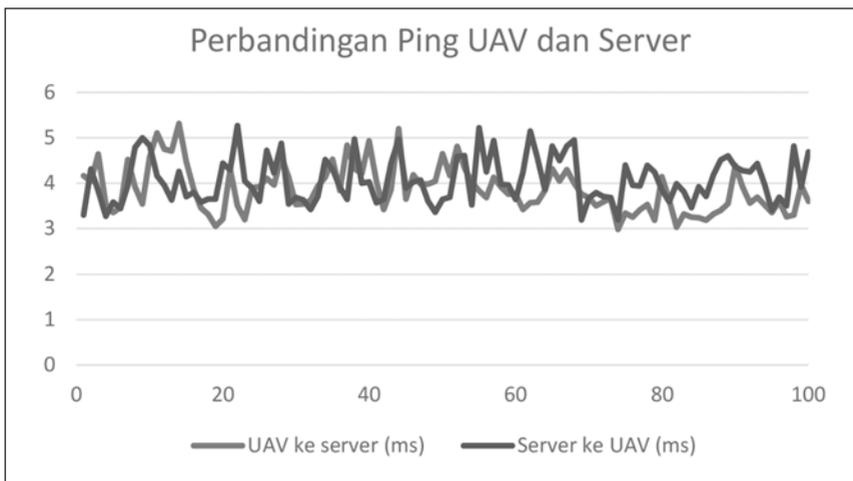
**Tabel 1.** Hasil pengujian ping (lanjutan)

Pengujian	UAV ke server (ms)	Server ke UAV (ms)
61	3,42	4,24
62	3,57	5,15
63	3,58	4,54
64	3,84	3,86
65	4,32	4,82
66	4,05	4,5
67	4,3	4,82
68	4	4,95
69	3,76	3,19
70	3,68	3,67
71	3,5	3,79
72	3,59	3,7
73	3,66	3,68
74	2,98	3,19
75	3,34	4,4
76	3,25	3,95
77	3,41	3,94
78	3,53	4,39
79	3,18	4,24
80	4,14	3,85
81	3,63	3,59
82	3,03	3,99
83	3,32	3,81
84	3,25	3,46
85	3,24	3,92
86	3,18	3,71
87	3,32	4,18
88	3,4	4,51
89	3,55	4,6
90	4,39	4,36
91	3,91	4,28

**Tabel 1.** Hasil pengujian ping (lanjutan)

Pengujian	UAV ke server (ms)	Server ke UAV (ms)
92	3,56	4,25
93	3,69	4,43
94	3,52	3,97
95	3,35	3,4
96	3,6	3,69
97	3,26	3,5
98	3,3	4,82
99	3,96	3,91
100	3,6	4,69
<b>Rata- rata</b>	<b>3,866</b>	<b>4,0695</b>
<b>Max</b>	<b>5,32</b>	<b>5,27</b>
<b>Min</b>	<b>2,98</b>	<b>3,19</b>

Dari data tabel di atas maka dibuat sebuah grafik perbandingan kinerja dari sisi ping antara dari server dibandingkan dari UAV seperti gambar di bawah ini.

**Gambar 5.** Grafik Perbandingan Data Uji Ping

## 4. Penutup

### 4.1. Kesimpulan

Berdasarkan hasil simulasi uji komunikasi VPN L2TP dengan melakukan ping, dapat disimpulkan bahwa:

- a. Dengan mengetahui kelebihan dan kelemahan VPN L2TP, tingkat kehandalan komunikasi menggunakan VPN L2TP dinilai baik, namun kadang tergantung pada kestabilan jaringan.
- b. Berdasarkan grafik hasil ping, uji ping dari UAV ke Server dan Server ke UAV dapat disimpulkan stabil. Hal ini terlibat dari waktu yang dibutuhkan untuk ping dari UAV ke Server dan Server ke UAV hampir sama.
- c. Kinerja VPN L2TP yang dianggap lebih aman dapat diimplementasikan pada topologi jaringan.

### 4.2. Saran

Saran dan perbaikan untuk penelitian selanjutnya:

- a. Melakukan pengujian dengan menggunakan VPN tipe lain untuk mengetahui kinerjanya.
- b. Untuk menguji kinerjanya lebih jauh, perlu dilakukan uji perbandingan dengan VPN tipe lain. Hal ini penting untuk memvalidasi hasil uji komunikasi yang telah dilakukan.

## Ucapan Terima Kasih

Terima kasih penulis ucapkan kepada Kepala Pusat Teknologi Penerbangan, Koordinator Program dan Fasilitas Pusat Teknologi Penerbangan, dan Majelis Peneliti Utama Pusat Teknologi Penerbangan atas fasilitas dan dukungan dalam kajian peran pustekbang dalam penguasaan Teknologi aeronautika serta segenap tim Program Sistem Komunikasi - MALE yang telah banyak berpartisipasi untuk berdiskusi dan menyusun paper ini.

## Daftar Pustaka

- [1] Ginting, E. S., & Hadi, I. (2020). Pengujian Konfigurasi Otomatis Penambahan Gateway Pada Virtual Router Menggunakan Aplikasi Otomatisasi Jaringan Berbasis Web. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 4(4), 1126–1131.
- [2] Nurdiansyah, Y., Pratama, N., Putra, M. I., & Sya'roni, M. A. (2020). Analisis Perbandingan Metode Interior Gateway Protocol RIP Dengan OSPF Pada Jaringan MPLS-VPLS. *INFORMAL: Informatics Journal*, 5(2), 49
- [3] Khadapi, M., & Rasmila. (2020). REDESAIN JARINGAN KOMPUTER PADA KANTOR PEMERINTAHAN KOTA PRABUMULIH. *Seminar Hasil Penelitian Vokasi (SEMHAVOK) Universitas Bina Darma*, 145–152.
- [4] Prama Wira Ginta<sup>1</sup>, Galih Putra Kusuma<sup>2</sup>, Edi Kusuma Negara<sup>3</sup> | Jurnal Media Informatika, Vol.9, No.2, September 2013 | 118 – 139 | ISSN : 1858-2680 | IMPLEMENTASI TOOLS NETWORK MAPPER PADA LOKAL AREA NETWORK (LAN)
- [5] Tove Marks, “Perbandingan protokol VPN Apa itu protokol VPN ?” 16 Mei 2020 [Online]. Tersedia: <https://Vpnoverview.Com/Id/Info-Vpn/Perbandingan-Protokol-Vpn/> [Diakses: 10 November 2020]
- [6] Jaya, T. S. (2018). Pengujian Aplikasi dengan Metode Blackbox Testing Boundary Value Analysis (Studi Kasus: Kantor Digital Politeknik Negeri Lampung). *Jurnal Informatika Pengembangan IT (JPIT)*, 3(2), 45–46.
- [7] RACHMAWAN, A. (2018). Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN. *Jurnal Manajemen Informatika*, 8(2), 53–57.