Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 6 No. 5 (2022) 824 - 831 ISSN Media Electronic: 2580-0760

Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area

Bita Parga Zen[1], Anggi Zafia[2], Iwan Nofi Yono Putro[3]
[1.2] Informatics Engineering, Faculty of Informatics, Telkom Purwokerto Institute of Technology
[3] National Research and Innovation Agency
[1] bita@ittelkom-pwt.ac.id , [2]zafia@ittelkom-pwt.ac.id, [3] iwan.nofi.yono.putro@brin.go.id

Abstract

An unmanned Combat Aerial Vehicle (UCAV) is an unmanned aircraft that has a serial control communication device that can be seen directly in real-time. In carrying out UCAV flights, it requires good and stable data transmission security so that signal loss does not occur during the communication process. Researchers create a concept of a security scheme in communication at the Ground Control Station (GCS) that can be used for the use of UCAV communication at long distances, using the Quality of Service (QoS) method from OPEN VPN with parameters Throughput, Packet Loss, Delay (Latency) and Jitter can determine the reliability of a UCAV communication network. Based on the results of Quality of Service (QoS) testing with OpenVPN Autopilot UCAV objects on the ICMP protocol have the smallest packet loss value of 0%, the delay parameter is 5.2ms, the jitter parameter gets a high value of 4.68 ms higher than the TCP protocol and UDP. The TCP protocol has a relatively small packet loss value of 0.3% and ranks second to the ICMP protocol, then the delay value is 8.48 ms greater than the ICMP and UDP protocols, and the jitter parameter value is 0.0013 ms smaller than the ICMP and UDP protocols. The use of VPN OVPN is a good recommendation. Still, researchers suggest that should use not only OPEN VPN but also L2TP VPN and PPTP VPN for security at the Ground Control Station at UCAV as a comparison.

Keywords: *Unmanned Combat Aerial Vehicle; Quality of Service; Defense; Ground Control Station; OPEN VPN*

1. Introduction

The Republic of Indonesia has maritime and land borders with ten countries in the region (Thailand, Malaysia, Vietnam, the Philippines, East Leste, Papua New Guinea, Australia, and the Republic of Palau) [1] is the 7th largest country in the world based on geographical location and has waters as one of the trades. which makes Indonesia vulnerable to border problems related to regional border issues which have always been a problem for the beneficiary parties, the real threat of armed criminal groups and separatism currently has the potential to disrupt the country's defense and security system.[2]. entering the industrial revolution 4.0 where all have used technology as the main component in various fields, especially industrial production, information, and communication technology [3]. anticipating national defense to maintain the sovereignty of the nation [4], this certainly cannot be separated from the modern defense equipment owned by developed countries, one of which is the development of unmanned aircraft technology Unmanned Combat Aerial Vehicle (UCAV). UCAV aims to be a control serial communication tool that can be seen directly in real-time [5] and can monitor if there is a threat in the defense area. UCAV is controlled by the Ground Control Station (GCS) which can be used for the use of UCAV communications at long distances [6], but the obstacle is that it is vulnerable to interference, both from damage to the device and from security factors. In GCS, a computer network is needed for stability and security when sending and receiving data to ensure that the data sent reaches its destination [7], and the data sent is confidential.

For this reason, it is necessary to test network quality and data security on the network at GCS using Quality of Service (QoS) analysis [8]. The quality of data delivery services is the key to the attack area that affects the operational performance of the Unmanned Combat Aerial Vehicle (UCAV). Data transmission service area refers to the distance at which a missile on a UCAV, if this is neglected, can hit and damage a target with a certain probability under specific environmental parameters, including altitude, missile and target speed,

Accepted: 09-08-2022 | Received in revised: 27-09-2022 | Published: 31-10-2022

ballistic tilt angle, entry angle, and off-axis angle, in an air combat environment [9]

One way to test network quality is to perform a QoS analysis. Quality of Service (QOS) is a technology that allows network administrators to deal with the effects of congestion on packet flow traffic from various services to make optimal use of network resources, rather than increasing the physical capacity of the network. [10]. defines that QoS is a technique for managing bandwidth, delay, jitter, and packet loss for packet flow in a network [10]. The purpose of the QoS mechanism is to influence at least one of the four basic QoS parameters that have been determined. In addition to testing network stability using QoS, data transmission security needs to be implemented to ensure data safety from unauthorized parties [11]. One way to secure data on a network is to implement a Virtual Private Network (VPN) which can make a network private and secure using a public network or the internet.

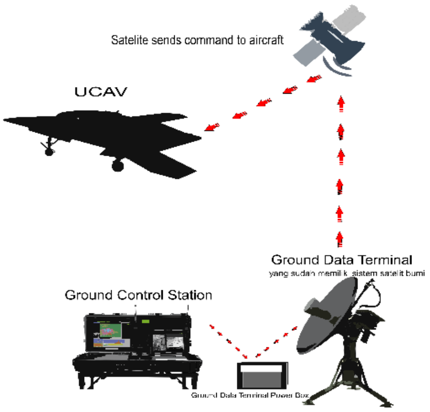

Satelite sends command to aircraft
UCAV
Ground Data Terminal
yang sudah memilik sistem satelit bumi
Ground Control Station
Ground Data Terminal Power Box

Figure 1. GCS to UCAV Communication Scheme

This is one of the basics of making simulations and analyses of QOS (Quality Of Service) throughput, delay, jitter, and packet loss stages. [12] with the addition of data security using VPN OpenVPN using the GNS3 network simulator application with the Hardware In The Loop Simulations technique which is a simulation involving some external hardware as support that will be applied to the Ground Control Station to control UCAV.

2. Research Method

This research will build a simulation and analysis of the Quality of Service on Unmanned Combat Aerial Vehicle Communication Networks for Data Security by explaining the levels or sequences starting from Throughput, delay, jitter, and packet loss at Ground Control Station Using OPENVPN with Hardware In The Loop Technique, Design This simulation will be a study that will be used for testing. and identify needs by providing detailed and accurate research figures. Figure 2 below are the stages of the process carried out by the researcher

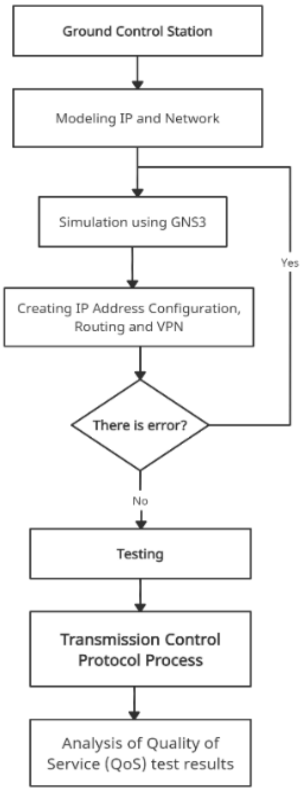

Ground Control Station
Modeling IP and Network
Simulation using GNS3
Creating IP Address Configuration, Routing and VPN
There is error?
Yes
No
Testing
Transmission Control Protocol Process
Analysis of Quality of Service (QoS) test results

Figure 2 Research Process Flow

2.1 Modeling IP and Network

In the IP address classification stage Configure all router interfaces connected to multiple ports by assigning an IP address to each port connected to the router. [13]. regarding the IP address to be used, there are several public IPs used for certain routers and private IPs. The following table classifier IP Address used.

Table 1. IP Address Classification

Device	Interfaces	IP Adress
Router Pustekbang BRIN	ether1	103.16.223.107/29
	ether1	10.10.5.136/27
	local VPN	10.11.6.1/32
Router1	ether1	103.16.223.108/29
	ether2	103.51.131.107/29
Router 2	ether1	103.51.131.108/29
	ether2	10.0.0.1/30
Router 3	ether1	10.0.0.2/30
	ether2	10.0.0.5/30
GCS Sat	ether1	10.0.0.6/30
	ether2	10.0.0.9/30
Satellite	ether1	10.0.0.10/30
	ether2	10.0.0.13/30
Modern Sat UCAV	ether1	10.0.0.14/30
	ether2	10.0.0.17/3
Router Client	ether1	10.0.0.18/30
	ether2	10.11.12.1/29
	remote VPN	10.11.6.2/32

In Figure 2 there are 8 device routers, where the

DOI: https://doi.org/10.29207/resti.v6i5.4412

Pustekbang BRIN router is marked with a yellow background, while the client router side is marked with a green background. for public routers or routers outside the server and client are marked with a gray background (gray). Furthermore, for the Server and Client in this simulation, Cloud2 is the Pustekbang Server and Cloud3 is the Client. Each device is external hardware connected to the GNS3 simulation software with the concept of Hardware in The Loop System. This topology design is implemented in the GNS3 software by adding a Mikrotik Router to the Qemu system contained in the GNS3. Then each router is connected and configured as needed.

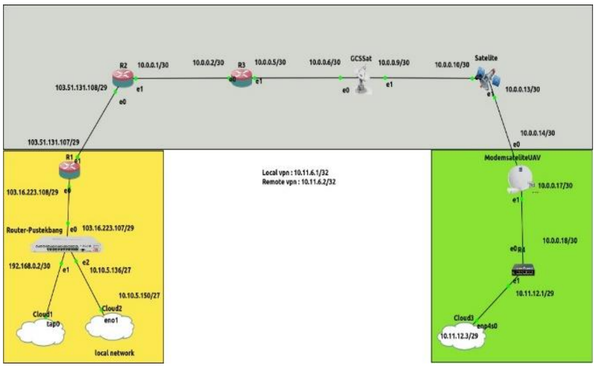


Figure 2. Communication Network Topology Design

2.2 *Quality of Service (QoS)*

Quality of Service (QoS) is an attempt to define the characteristics of a network quality by measuring how good the network quality of service is using certain parameters [14]. The International Telecommunication Union-Telecommunication (ITU-T) G.1010 standards are discussed in this paper as they relate to the quality of service (QoS) performance from telemetry data utilizing UDP protocols both with and without VPN on Ground Control Station (GCS) communication with UCAV [15]. G.1010 is an ITU-T standard. [16] .

A guarantee for zero information loss or the absence of packet loss is a parameter that must be taken into account for data transfer. Then, the delay that happens must be less than 1 second and the fluctuation of the delay (jitter) that occurs must adhere to certain guidelines [15]. It is anticipated that the reliability performance of satellite communications that are intended and may be beneficial for long-range UCAV communication applications would be known from the findings of testing and analysis [17].

There are 3 levels of QoS that are often used, namely Best-effort service, which is a service model where each application for each data transmission is required without asking permission from the computer network. a service that can meet all the requirements of different QoS rules [18]. The ultimate goal of QoS is to provide a better and more planned network service with controlled dedicated bandwidth, jitter, and latency and increase loss characteristics centered on network characteristics. [19]

a. Throughput

The total number of successful packet arrivals seen at the destination over the course of a certain time interval divided by the length of that time interval is known as throughput. A network's real capacity for data transmission is known as throughput [20]. Because throughput can be referred to as bandwidth under actual circumstances, throughput is typically always associated with bandwidth.

$$Throughput = \frac{Datapacketreceived}{observationtime}$$

Table 2. Category Throughput

Throughput	***Throughput***	***Index***
Very good	76%-100%	4
Good	51% s/d 75%	3
Fair	26% s/d 50%	2
Poor	<25%	1

b. Delay

Delay (Latency) is the time it takes for data to travel the distance from the sender to the receiver. delay can be affected by long distances, physical media, data congestion, or also long processing times [18]. The equation to calculate the delay is:

$$Avaragedelay = \frac{Totaldelay}{Totalpacketsreceived} \tag{1}$$

Table 1. Category Delay

Category Delay	*Delay*	*Index*
Very good	< 150 ms	4
Good	150 s/d 300 ms	3
Fair	301 s/d 450 ms	2
Poor	> 450 ms	1

[21]

c. Jitter

Jitter is a delay that varies over time. Jitter is referred to as a change in delay variation or the difference between the initial delay and the next delay in the data transmission period [22]. The equation for calculating the jitter is:

$$Jitter = \frac{Totalvariationdelay}{Totalpacketsreceived} \tag{2}$$

The total variation of the delay is obtained from:

$$Total\ \ Variation\ Delay = Delay – (Average\ Delay) \tag{3}$$

Table 2. Category Jitter

Kategori *Jitter*	*Peak Jitter*	*Index*
Very good	0 ms	4
Good	1 s/d 75 ms	3
Fair	76 s/d 225 ms	2
Poor	> 225 ms	1

[21]

DOI: https://doi.org/10.29207/resti.v6i5.4412

d. Packet Loss

Packet loss is a parameter that shows the condition of a data packet that is lost from the total number of packets that can occur due to collision and congestion on a network [23]. The equation to calculate packet loss is:

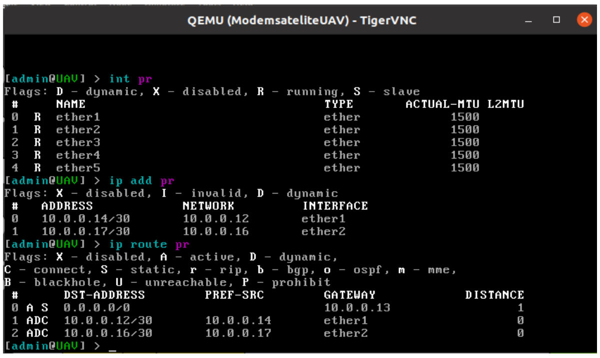
$$PacketLoss = \frac{Packagesent - Packagereceived}{Receivedpackage} x100\% \quad (4)$$

Table 3. Category Packet Loss

Kategori *Packet Loss*	*Packet Loss*	*Index*
Very good	0% - 2%	*4*
Good	3% - 14%	*3*
Fair	15% - 25%	*2*
Poor	> 25 %	*1*

2.3 Open VPN type VPN configuration

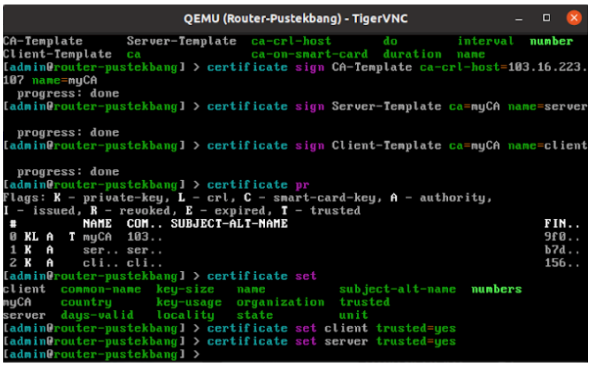
VPN configuration is carried out on the BRIN pustekbang router as a VPN Open VPN Server. VPN Open VPN Server is made using the default settings on the Pustekbang router so that it can be accessed by the client side as a tunnel that connects the network. The security used only uses default encryption to be able to connect to the network without using additional security such as IPsec or certificates. The following is the VPN Server OVPN configuration that has been created on the Pustekbang router. First, to increase the security of this OpenVPN connection, we will add certificates to the server as well as the client. After we create the certificate, we will first activate the OpenVPN Server on the main gateway router at 'Server-Pustekbang'. Type in SSL Linux PPP → on the Interface Tab of the OVPN Server Command. Then to enable OpenVPN Server check the Enabled option. Also, add a certificate for OpenVPN connection in 'Router-Pustekbang' as OVPN Server in parameter 'Certificate' as shown below.


QEMU (ModemsateliteUAV) - TigerVNC

```
[admin@UAV] > int pr
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                     TYPE       ACTUAL-MTU L2MTU
 0  R  ether1                                   ether            1500
 1  R  ether2                                   ether            1500
 2  R  ether3                                   ether            1500
 3  R  ether4                                   ether            1500
 4  R  ether5                                   ether            1500
[admin@UAV] > ip add pr
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.14/30       10.0.0.12       ether1
 1   10.0.0.17/30       10.0.0.16       ether2
[admin@UAV] > ip route pr
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          10.0.0.13                 1
 1 ADC  10.0.0.12/30       10.0.0.14       ether1                    0
 2 ADC  10.0.0.16/30       10.0.0.17       ether2                    0
[admin@UAV] > _
```

Figure 3 OPENVPN Server Configuration

Routing configuration is also carried out on the UCAV Satellite Modem router to connect to other router networks to be connected. The following is a picture of the routing configuration used on the UCAV Satellite Modem router, As with other VPN connections, we will also create a 'PPP secret' to dial a connection from the OVPN Client

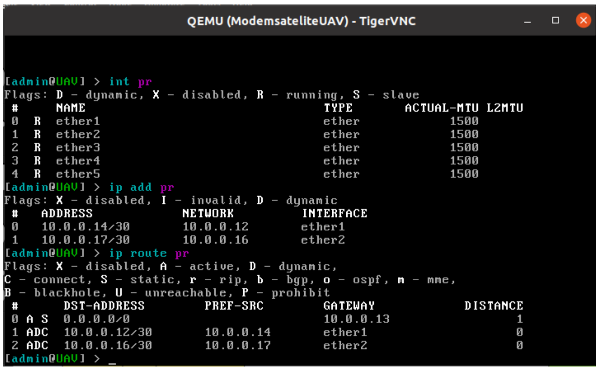

QEMU (Router-Pustekbang) - TigerVNC

```
CA-Template      Server-Template  ca-crl-host       do          interval   number
Client-Template  ca               ca-on-smart-card  duration    name
[admin@router-pustekbang] > certificate sign CA-Template ca-crl-host=103.16.223.
107 name=myCA
  progress: done
[admin@router-pustekbang] > certificate sign Server-Template ca=myCA name=server

  progress: done
[admin@router-pustekbang] > certificate sign Client-Template ca=myCA name=client

  progress: done
[admin@router-pustekbang] > certificate pr
Flags: K - private-key, L - crl, C - smart-card-key, A - authority,
I - issued, R - revoked, E - expired, T - trusted
 #          NAME  COM.. SUBJECT-ALT-NAME                                   FIN..
 0 KL A  T myCA  103..                                                     9f0..
 1 K  A    ser.. ser..                                                     b7d..
 2 K  A    cli.. cli..                                                     156..
[admin@router-pustekbang] > certificate set
client  common-name  key-size   name          subject-alt-name  numbers
myCA    country      key-usage  organization  trusted
server  days-valid   locality   state         unit
[admin@router-pustekbang] > certificate set client trusted=yes
[admin@router-pustekbang] > certificate set server trusted=yes
[admin@router-pustekbang] >
```

Figure 4 OPENVPN Authentication Configuration

Next, do the configuration for the 'Client' as an OpenVPN Client. Because we use the terminal, we go to the PPP menu → Interfaces → Add [+] → OVPN Client. Then fill in each parameter, If OpenVPN is successfully connected then we can see the OpenVPN Server router in the PPP → Active Connections menu. There will be displayed information from client devices that have successfully connected to OpenVPN Server.

Schematic on the Ground Control Station as the main link to the Unmanned Combat Aerial Vehicle (UCAV) which functions as reconnaissance and helps map out areas [24] at the time of combined operation which has 3 main components: 1. UCAV as the main component that can be flown for monitoring by air; 2. Ground Control Station as a computer for the control room in the UCAV remote control which can be viewed with a monitor in real-time both for taking pictures and for video, then the routing configuration is carried out on the UCAV Satellite Modem router to connect other router networks to be connected. The following figure shows the routing configuration used on the UCAV Satellite Modem router. 3. Ground Data Terminal as a distance determinant, namely the antenna for connecting the Ground Control Station to UCAV


QEMU (ModemsateliteUAV) - TigerVNC

```
[admin@UAV] > int pr
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                     TYPE       ACTUAL-MTU L2MTU
 0  R  ether1                                   ether            1500
 1  R  ether2                                   ether            1500
 2  R  ether3                                   ether            1500
 3  R  ether4                                   ether            1500
 4  R  ether5                                   ether            1500
[admin@UAV] > ip add pr
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.14/30       10.0.0.12       ether1
 1   10.0.0.17/30       10.0.0.16       ether2
[admin@UAV] > ip route pr
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          10.0.0.13                 1
 1 ADC  10.0.0.12/30       10.0.0.14       ether1                    0
 2 ADC  10.0.0.16/30       10.0.0.17       ether2                    0
[admin@UAV] > _
```

Figure 5 UCAV satellite modem router configuration.

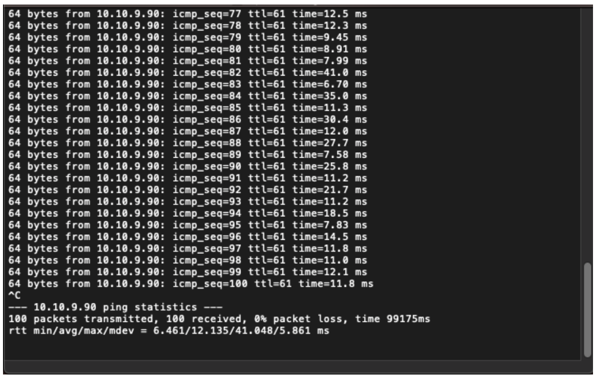
This research focuses on simulating the network design on GNS3 simulation software. In QoS, there are 3 main parameters used to analyze the quality of the service, namely, parameters of delay, jitter, and packet loss in the UCAV satellite modem router. In the analysis stage

DOI: https://doi.org/10.29207/resti.v6i5.4412

of the results of the Quality of Service (QoS) test the parameters used are the parameters of delay, jitter, and packet loss in each of the tested protocols, namely the routing configuration protocol is also carried out on the UCAV Satellite Modem router to connect other router networks so that they are connected. The following figure is the routing configuration used on the UCAV Satellite Modem router.

3. Result and Discussion

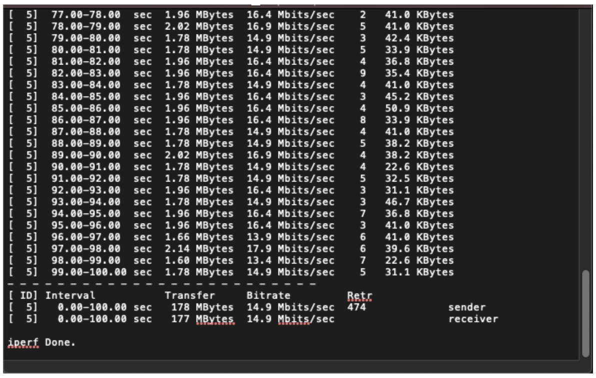
ICMP testing is done by sending a ping test packet to the server using the command: "ping 10.10.10.90" for a time interval of 100 seconds and is carried out 10 times. This test aims to maximize the data later in processing QoS. Parameters



```
64 bytes from 10.10.9.90: icmp_seq=77 ttl=61 time=12.5 ms
64 bytes from 10.10.9.90: icmp_seq=78 ttl=61 time=12.3 ms
64 bytes from 10.10.9.90: icmp_seq=79 ttl=61 time=9.45 ms
64 bytes from 10.10.9.90: icmp_seq=80 ttl=61 time=8.91 ms
64 bytes from 10.10.9.90: icmp_seq=81 ttl=61 time=7.99 ms
64 bytes from 10.10.9.90: icmp_seq=82 ttl=61 time=41.0 ms
64 bytes from 10.10.9.90: icmp_seq=83 ttl=61 time=6.70 ms
64 bytes from 10.10.9.90: icmp_seq=84 ttl=61 time=35.0 ms
64 bytes from 10.10.9.90: icmp_seq=85 ttl=61 time=11.3 ms
64 bytes from 10.10.9.90: icmp_seq=86 ttl=61 time=30.4 ms
64 bytes from 10.10.9.90: icmp_seq=87 ttl=61 time=12.0 ms
64 bytes from 10.10.9.90: icmp_seq=88 ttl=61 time=27.7 ms
64 bytes from 10.10.9.90: icmp_seq=89 ttl=61 time=7.58 ms
64 bytes from 10.10.9.90: icmp_seq=90 ttl=61 time=25.8 ms
64 bytes from 10.10.9.90: icmp_seq=91 ttl=61 time=11.2 ms
64 bytes from 10.10.9.90: icmp_seq=92 ttl=61 time=21.7 ms
64 bytes from 10.10.9.90: icmp_seq=93 ttl=61 time=11.2 ms
64 bytes from 10.10.9.90: icmp_seq=94 ttl=61 time=18.5 ms
64 bytes from 10.10.9.90: icmp_seq=95 ttl=61 time=7.83 ms
64 bytes from 10.10.9.90: icmp_seq=96 ttl=61 time=14.5 ms
64 bytes from 10.10.9.90: icmp_seq=97 ttl=61 time=11.8 ms
64 bytes from 10.10.9.90: icmp_seq=98 ttl=61 time=11.0 ms
64 bytes from 10.10.9.90: icmp_seq=99 ttl=61 time=12.1 ms
64 bytes from 10.10.9.90: icmp_seq=100 ttl=61 time=11.8 ms
^C
--- 10.10.9.90 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99175ms
rtt min/avg/max/mdev = 6.461/12.135/41.048/5.861 ms
```

Figure 6 ICMP Protocol Test

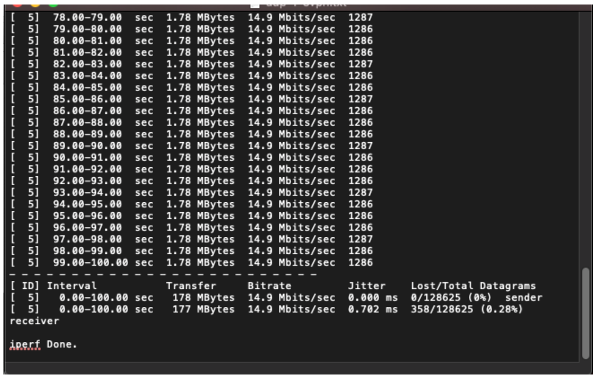
TCP testing is done by sending packets via port 5000 using the iperf3 application to the server using the command “iperf3 –c 10.10.9.90 –p 5000 –t 100 > filename.txt”. This test is carried out with a time interval of 100 seconds and is carried out ten times to get maximum data on QoS processing.



```
[  5]  77.00-78.00   sec  1.96 MBytes  16.4 Mbits/sec    2   41.0 KBytes
[  5]  78.00-79.00   sec  2.02 MBytes  16.9 Mbits/sec    5   41.0 KBytes
[  5]  79.00-80.00   sec  1.78 MBytes  14.9 Mbits/sec    3   42.4 KBytes
[  5]  80.00-81.00   sec  1.78 MBytes  14.9 Mbits/sec    5   33.9 KBytes
[  5]  81.00-82.00   sec  1.96 MBytes  16.4 Mbits/sec    4   36.8 KBytes
[  5]  82.00-83.00   sec  1.96 MBytes  16.4 Mbits/sec    9   35.4 KBytes
[  5]  83.00-84.00   sec  1.78 MBytes  14.9 Mbits/sec    4   41.0 KBytes
[  5]  84.00-85.00   sec  1.96 MBytes  16.4 Mbits/sec    3   45.2 KBytes
[  5]  85.00-86.00   sec  1.96 MBytes  16.4 Mbits/sec    4   50.9 KBytes
[  5]  86.00-87.00   sec  1.96 MBytes  16.4 Mbits/sec    8   33.9 KBytes
[  5]  87.00-88.00   sec  1.78 MBytes  14.9 Mbits/sec    4   41.0 KBytes
[  5]  88.00-89.00   sec  1.78 MBytes  14.9 Mbits/sec    5   38.2 KBytes
[  5]  89.00-90.00   sec  2.02 MBytes  16.9 Mbits/sec    4   38.2 KBytes
[  5]  90.00-91.00   sec  1.78 MBytes  14.9 Mbits/sec    4   22.6 KBytes
[  5]  91.00-92.00   sec  1.78 MBytes  14.9 Mbits/sec    5   32.5 KBytes
[  5]  92.00-93.00   sec  1.96 MBytes  16.4 Mbits/sec    3   31.1 KBytes
[  5]  93.00-94.00   sec  1.78 MBytes  14.9 Mbits/sec    3   46.7 KBytes
[  5]  94.00-95.00   sec  1.96 MBytes  16.4 Mbits/sec    7   36.8 KBytes
[  5]  95.00-96.00   sec  1.96 MBytes  16.4 Mbits/sec    3   41.0 KBytes
[  5]  96.00-97.00   sec  1.66 MBytes  13.9 Mbits/sec    6   41.0 KBytes
[  5]  97.00-98.00   sec  2.14 MBytes  17.9 Mbits/sec    6   39.6 KBytes
[  5]  98.00-99.00   sec  1.60 MBytes  13.4 Mbits/sec    7   22.6 KBytes
[  5]  99.00-100.00  sec  1.78 MBytes  14.9 Mbits/sec    5   31.1 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-100.00 sec   178 MBytes  14.9 Mbits/sec  474             sender
[  5]   0.00-100.00 sec   177 MBytes  14.9 Mbits/sec                  receiver

iperf Done.
```

Figure 7 TCP Protocol Test

UDP testing is done by sending packets via port 5000 using the iperf3 application to the server using the bandwidth obtained from the TCP protocol testing. This test is carried out with a time interval of 100 seconds and is carried out ten times to get maximum data on QoS processing.



```
[  5]  78.00-79.00   sec  1.78 MBytes  14.9 Mbits/sec  1287
[  5]  79.00-80.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  80.00-81.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  81.00-82.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  82.00-83.00   sec  1.78 MBytes  14.9 Mbits/sec  1287
[  5]  83.00-84.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  84.00-85.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  85.00-86.00   sec  1.78 MBytes  14.9 Mbits/sec  1287
[  5]  86.00-87.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  87.00-88.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  88.00-89.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  89.00-90.00   sec  1.78 MBytes  14.9 Mbits/sec  1287
[  5]  90.00-91.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  91.00-92.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  92.00-93.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  93.00-94.00   sec  1.78 MBytes  14.9 Mbits/sec  1287
[  5]  94.00-95.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  95.00-96.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  96.00-97.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  97.00-98.00   sec  1.78 MBytes  14.9 Mbits/sec  1287
[  5]  98.00-99.00   sec  1.78 MBytes  14.9 Mbits/sec  1286
[  5]  99.00-100.00  sec  1.78 MBytes  14.9 Mbits/sec  1286
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-100.00 sec   178 MBytes  14.9 Mbits/sec  0.000 ms  0/128625 (0%)  sender
[  5]   0.00-100.00 sec   177 MBytes  14.9 Mbits/sec  0.702 ms  358/128625 (0.28%)
receiver

iperf Done.
```

Figure 8 UDP Protocol Test

In the analysis phase of the Quality of Service (QoS) test results, the parameters used are the delay, jitter, and packet loss parameters in each of the tested protocols, namely the Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP) and User Data Protocol. (UDP). The following are the results of the test graph for each protocol obtained:

a. Throughput is the bandwidth obtained in each trial of the TCP and UDP protocols

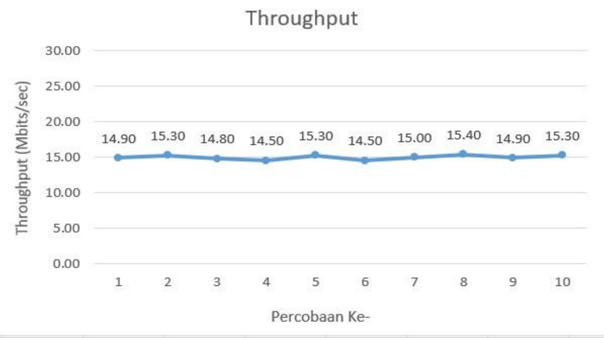


Figure 9 TCP and UDP Throughput Graph

b. Protocol ICMP
Delay ICMP
The following is the result of measuring the QoS parameters of the ICMP protocol delay based on a predetermined test scheme, the test results above the resulting graph show that the maximum average delay is 7.75 ms, the minimum average delay is 2.81 ms, and the average delay is 2.81 ms. total delay is 5.20 ms

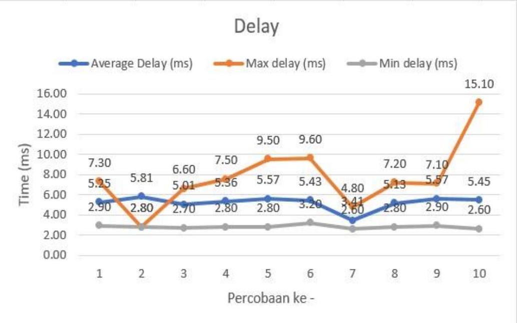


Figure 10. ICMP Delay Graph

DOI: https://doi.org/10.29207/resti.v6i5.4412

Jitter ICMP

The following are the results of the ICMP protocol jitter parameter QoS measurements based on a predetermined test scheme. In the parameters of the jitter, the maximum average jitter is 12.75 ms, the minimum average jitter is 0 ms, and the overall average jitter is 4.68 ms.

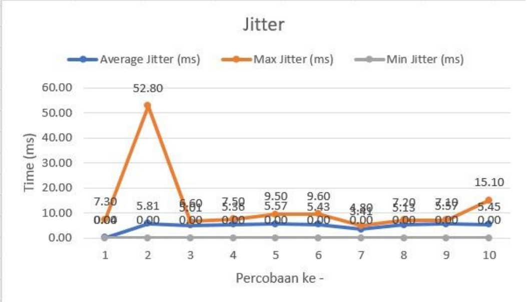


Figure 11. ICMP Jitter Graph

Packet Loss

The following is the result of measuring the QoS parameters of the ICMP packet loss protocol based on the test scheme that has been determined based on the graph below, in the ICMP packet loss protocol parameter, no packet loss was found at 0%.

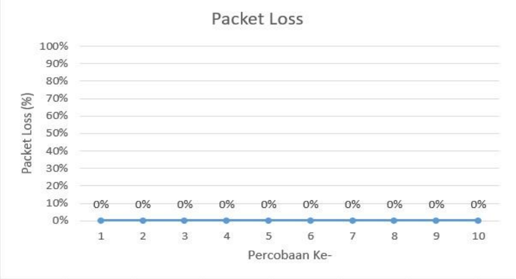
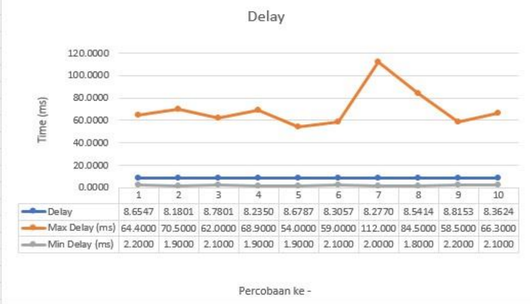


Figure 12. Grafik Packet Loss ICMP

c. Protocol TCP

Delay TCP

The following is the result of measuring the QoS parameters of the TCP protocol delay based on the test scheme that has been determined from the graph above, the delay results from the TCP protocol obtained the maximum delay on the 7th experiment with a value of 112.00 ms, the minimum delay on the 8th experiment with a value of 1.8000 ms, the maximum average delay on the 9th experiment with a value of 8.8153 ms, and the minimum average delay on the 2nd experiment with a value of 8.1801.

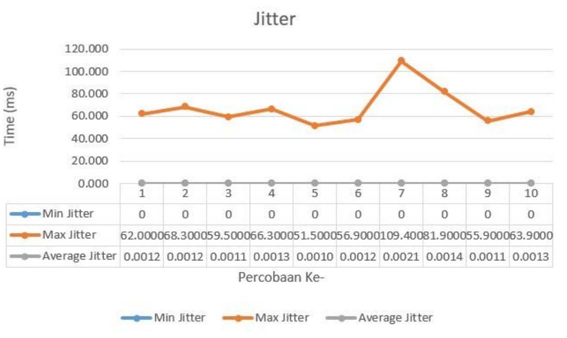


	1	2	3	4	5	6	7	8	9	10
Delay	8.6547	8.1801	8.7801	8.2350	8.6787	8.3057	8.2770	8.5414	8.8153	8.3624
Max Delay (ms)	64.4000	70.5000	62.0000	68.9000	54.0000	59.0000	112.000	84.5000	58.5000	66.3000
Min Delay (ms)	2.2000	1.9000	2.1000	1.9000	1.9000	2.1000	2.0000	1.8000	2.2000	2.1000

Figure 13. Grafik Delay TCP

Jitter TCP

The following is the result of measuring the QoS parameters of the TCP protocol jitter based on a predetermined test scheme. Based on the graph above, the results of the jitter of the TCP protocol obtained the maximum jitter on the 7th experiment with a value of 109,400 ms, the minimum jitter of all tests got a value of 0.0000 ms, the maximum average jitter on the 7th experiment with a value of 0.0021 ms and the minimum average jitter on the 5th experiment with a value of 0.0010.

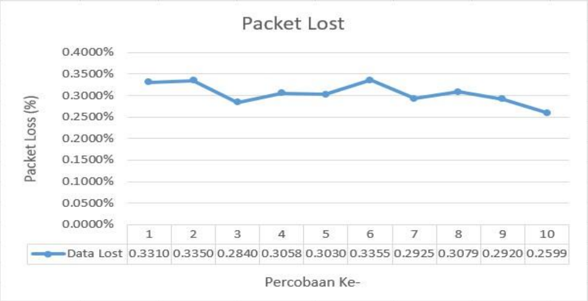


	1	2	3	4	5	6	7	8	9	10
Min Jitter	0	0	0	0	0	0	0	0	0	0
Max Jitter	62.0000	68.3000	59.5000	66.3000	51.5000	56.9000	109.400	81.9000	55.9000	63.9000
Average Jitter	0.0012	0.0012	0.0011	0.0013	0.0010	0.0012	0.0021	0.0014	0.0011	0.0013

Figure 14. TCP Jitter Graph

Packet Loss

The following is the result of measuring the QoS parameters of the TCP protocol packet loss based on the test scheme that has been determined in the graph above, the packet loss results from the TCP protocol obtained the maximum packet loss on the 6th experiment ith a value of 0.3355% and the minimum packet loss on the 10th experiment. with a value of 0.2599 ms.



	1	2	3	4	5	6	7	8	9	10
Data Lost	0.3310	0.3350	0.2840	0.3058	0.3030	0.3355	0.2925	0.3079	0.2920	0.2599

Figure 15. TCP Packet Loss Graph

DOI: https://doi.org/10.29207/resti.v6i5.4412

d. Protocol UDP

Delay UDP

The following is the result of measuring the QoS parameters of the UDP protocol delay. Based on the graph of the delay results from the UDP protocol, the maximum delay in the 3rd experiment with a value of 95,600 ms, the minimum delay in the 5th and 10th experiments with a value of 2,5000 ms, and the maximum average delay in the 10th experiment with a value of 4.9558 ms, and the minimum average delay on the 3rd experiment with a value of 4.6412 ms.

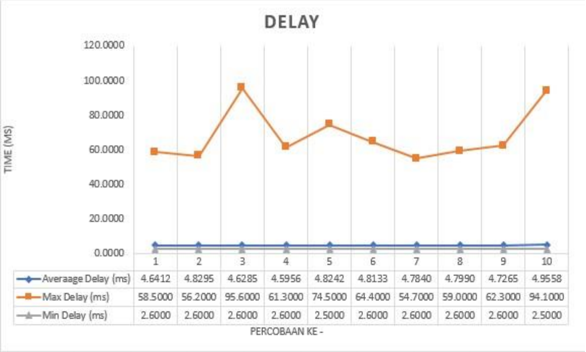


Figure 16. UDP Delay Graph

Jitter UDP

The following is the result of measuring the QoS parameters of the UDP protocol jitter. Based on the graph above, the jitter results of the UDP protocol obtained the maximum jitter on the 10th experiment with a value of 91.40 ms, the minimum jitter of all tests got a value of 0.0000 ms, the average maximum jitter in the 4th experiment with a value of 0.5781 ms, and the minimum average jitter in the 1st and 2nd experiments with a value of 0.0004 ms.

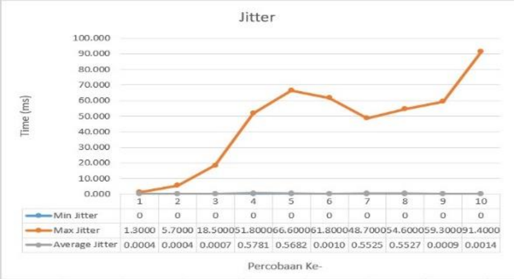


Figure 17 UDP Jitter Graph

Packet Loss

The following is the result of measuring the QoS parameter of the UDP protocol packet loss. Based on the graph above, the packet loss results from the UDP protocol obtained the maximum packet loss on the 10th experiment with a value of 0.2559% and the minimum packet loss on the 1st experiment with a value of 0.0000 %

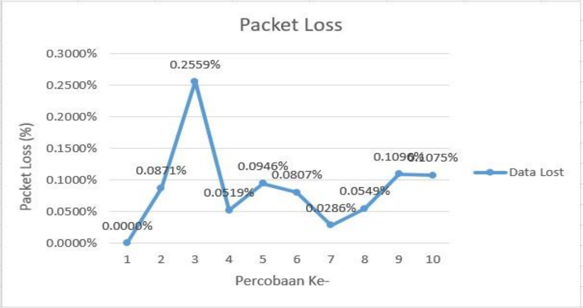


Figure 18. UDP Packet Loss Graph

QoS Recapitulation

By testing on each protocol with a predetermined scenario using QOS calculations (delay, jitter, and packet loss), the protocol used (ICMP, TCP, and UDP) in testing using VPN OVPN Has an excellent value based on the values taken from the overall average of the number of tests of each QoS parameter. The ICMP protocol has the smallest packet loss value (0%). Still, the delay parameter (5.2ms) is greater than the UDP protocol and smaller than the TCP protocol, and the jitter parameter gets a high value (4.68 ms). Higher than the TCP and UDP protocols. The TCP protocol has a relatively small packet loss value (0.3%) which ranks second to the ICMP protocol. The delay value is more excellent (8.48 ms) than the ICMP and UDP protocols, and the jitter parameter value is more minor (0.0013). of the ICMP protocol and more significant than the UDP protocol. While the TCP protocol itself has the highest packet loss value (0.3%) of the other two protocols, both the delay parameter (4.75 ms) and jitter (0.22 ms) have a relatively more nominal value than the other protocols

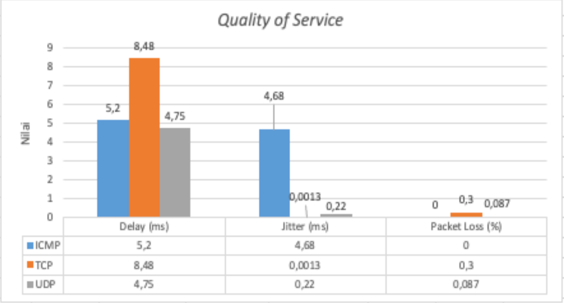


Figure 19. QoS Recapitulation Reports

Conclusion

The Ground Control Station security system using OPEN VPN has an excellent Quality of Service (QoS) value based on experiments using ICMP, TCP, and UDP protocols. This value is taken from the overall average number of tests for each QoS parameter; from the results of the QoS recapitulation above, UDP is more suitable for use on VPN OVPN. Then when viewed from the 4.75 ms delay and 0.22 ms jitter, the UDP protocol repositions its performance on the use of

DOI: https://doi.org/10.29207/resti.v6i5.4412

VPN OVPN so that this is a good recommendation for security at the Ground Control Station in the Unmanned Combat Aerial Vehicle (UCAV).

References

[1] B. J. Silalahi, A. M. Panjaitan, F. Tinus, and H. Feryandi, "Implementing Remote Sensing and Drone Mapping Technology for Land Management in Indonesia ' s Boundary Zone Implementing Remote Sensing and Drone Mapping Technology for Land Management in Indonesia ' s Boundary Zone Budi Jaya Silalahi , Albert Midian Panj," no. 8321, 2016.

[2] M. Zulkifli, Moeljadi, M. Fadli, and Nurjanah, "Strengthening Indonesia Naval Base As a Aircraft Carrier At the Frontier To Increase Power of Deterrence and State Defense At Sea," *Russ. J. Agric. Socio-Economic Sci.*, vol. 117, no. 9, pp. 3–13, 2021.

[3] V. Alcácer and V. Cruz-machado, "Engineering Science and Technology , an International Journal Scanning the Industry 4 . 0 : A Literature Review on Technologies for Manufacturing Systems," vol. 22, pp. 899–919, 2019.

[4] B. P. Zen, R. A. G. Gultom, and A. H. S. Reksoprodjo, "Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara," *J. Teknol. Penginderaan*, vol. 2, no. 1, pp. 105–122, 2020.

[5] S. Luo *et al.*, "Network for hypersonic UCAV swarms," *Sci. China Inf. Sci.*, vol. 63, no. 4, pp. 1–28, 2020.

[6] M. Mahardika, G. Nugroho, and E. Y. Prasetyo, "UAV long range surveillance system based on BiQuad antenna for the Ground Control Station," *Proc. - 14th IEEE Student Conf. Res. Dev. Adv. Technol. Humanit. SCOReD 2016*, pp. 3–7, 2017.

[7] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, mobility models and security issues," *Comput. Networks*, vol. 163, p. 106877, 2019.

[8] P. Dybiec, "Mobile Networks' Support for Large-Scale UAV Services 1,2," pp. 1–19, 2022.

[9] L. Yue, Q. Xiaohui, L. Xiaodong, and X. Qunli, "Deep reinforcement learning and its application in autonomous fitting optimization for attack areas of UCAVs," *J. Syst. Eng. Electron.*, vol. 31, no. 4, pp. 734–742, 2020.

[10] N. F. Puspitasari and A. Dahlan, "Analisa Trafik dan Quality of Service (QoS) Untuk Optimalisasi Manajemen Bandwith (Studi Kasus : Universitas AMIKOM Yogyakarta)," *J. Ilm. Data Manaj. dan Teknol. Inf.*, vol. 148, pp. 148–162, 2017.

[11] I. Nurrobi, K. Kusnadi, and R. Adam, "Penerapan Metode QoS (Quality of Service) untuk Menganalisa Kualitas Kinerja Jaringan Wireless," *J. Digit*, vol. 10, no. 1, p. 47, 2020.

[12] R. Syahputra, Rahmadi Kurnia, and Rian Ferdian, "Analysis of FHRP Design and Implementation in RIPv2 and OSPF Routing Protocols," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 1, pp. 102–108, 2020.

[13] M. Yannuzzi, X. Masip-Bruin, R. Serral-Gracia, E. Marin-Tordera, A. Sprintson, and A. Orda, "Maximum Coverage at Minimum Cost for Multi-Domain IP/MPLS Networks," no. May, pp. 1831–1839, 2008.

[14] M. Karakus and A. Durresi, "Quality of Service (QoS) in Software Defined Networking (SDN): A survey," *J. Netw. Comput. Appl.*, vol. 80, pp. 200–218, 2017.

[15] Y. Firmansyah, N. Rahayu, Y. Prabowo, I. N. Y. Putro, and F. Kurniawan, "Quality of Service (QoS) Analysis for Real-Time Telemetry by IP Satellite Communication," *Proceeding - 2020 Int. Conf. Radar, Antenna, Microwave, Electron. Telecommun. ICRAMET 2020*, pp. 18–21, 2020.

[16] ITU-T, "G.1010: End-user multimedia QoS categories," *Int. Telecommun. Union*, vol. 1010, 2001.

[17] F. G. Becker *et al.*, "Standard Interfaces of UAV Control System (UCS) For NATO UAV Interoperability," *Syria Stud.*, vol. 7, no. 1, pp. 37–72, 2015.

[18] R. Azhar, H. Santoso, and F. Faisal, "Analisa Quality Of Service Menggunakan Aplikasi Gnump3d sebagai Server Media Streaming," *J. Bumigora Inf. Technol.*, vol. 3, no. 1, pp. 45–55, 2021.

[19] A. Ahad, M. Tahir, and K. L. A. Yau, "5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions," *IEEE Access*, vol. 7, pp. 100747–100762, 2019.

[20] M. S. Bahbahani and E. Alsusa, "A Cooperative Clustering Protocol with Duty Cycling for Energy Harvesting Enabled Wireless Sensor Networks," *IEEE Trans. Wirel. Commun.*, vol. 17, no. 1, pp. 101–111, 2018.

[21] ETSI, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS)," *Etsi Tr 101 329 V2.1.1*, vol. 1, pp. 1–37, 1999.

[22] A. Budiman, A. Sucipto, and A. R. Dian, "Analisis Quality of Service Routing MPLS OSPF Terhadap Gangguan Link Failure," *Techno.Com*, vol. 20, no. 1, pp. 28–37, 2021.

[23] I. Suryani, L. Lindawati, and I. Salamah, "Analisa QOS (Quality Of Service) Jaringan Internet Di Teknik Elektro Politeknik Negeri Sriwijaya," *It J. Res. Dev.*, vol. 3, no. 1, pp. 32–42, 2018.

[24] D. Hartono and S. Darmawan, "Pemanfaatan Unmanned Aerial Vehicle (UAV) Jenis Quadcopter untuk Percepatan Pemetaan Bidang Tanah (Studi Kasus: Desa Solokan Jeruk Kabupaten Bandung)," *Reka Geomatika*, vol. 2018, no. 1, pp. 30–40, 2019.

DOI: https://doi.org/10.29207/resti.v6i5.4412