Analysis of Local Area Network Performance using Quality of Service

Holan Rahmatullah Suhut Nadenggan
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
The development of information technology is currently very rapid, especially in computer networks which have become fundamental in all aspects. Analysis of the performance of computer networks, especially network LAN (Local Area Networks) is an effort to assess the quality of the internet network provided. Organizations or agencies that use LAN (Local Area Network) should use a good standard of service quality. Quality of Service (QoS) is one way to determine the performance quality of a network. Quality of Service uses 4 parameters to determine the quality of a network, namely throughput, packet loss, delay, and jitter with good service quality standardization, namely the TIPHON standardization (Telecommunication Internet Protocol Harmonization Over Networks). This research was conducted by assessing the Quality of Service (QoS) in the laboratory computer network before and after a Distributed Denial of Service (DDoS) attack. The process of attacking computer networks using tools LOIC (Low Orbit Ion Cannon)and simultaneously measuring network quality using 4lparameters Quality of Service (QoS). This study aims to determine the quality of a LAN(Local Area Network) network will deteriorate if there is a Distributed Denial of Service (DDoS) attack. The results of theresearch were conducted in accordance with the scenarios and objectives desired. The measurementLAN (Local Area Network)performance, before the attack resulted in a value throughput of 80%, packet loss of 0%, delay of 194.5 ms, and jitter of 0 ms. After the attack resulted in a value throughput of 45%, packet loss of 77.5%, delay of 208.25 ms, and Jitter of 0.75 ms. With a QoS parameter index of 3.75 before an attack, and a QoS parameter index of 2.50 after an attack. The Conclusion is that network attacks can affect the quality of network services and even cause disruption to the network system when the traffic is very high, it is necessary to build Local Area Network security against attacks.

Keywords
Quality of Service,Throughput, Delay, Jitter,Packet Loss, DDoS, LOIC

1. INTRODUCTION
The development of information technology is currently growing rapidly[1], especially in computer networks which have become fundamental in all aspects. It is difficult to imagine in the current era of information technology without using a computer network topology. Due to a large number of needs for access and communication, the performance of computer networks must be in good condition, so it is necessary to solve problems in providing good computer network performance [2]. Measuring the performance of computer networks, especially LAN (Local Area Networks)networks can use the method Quality of Service (QoS)[3], which is designed to help end-users be more productive by ensuring that users get reliable performance from network-based applications [4]. Quality of Service (QoS) uses 4 parameters to determine the quality of a network, namely throughput, packet loss, delay, and jitter [5]. The implementation of these 4 parameters will use the standardization of Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) [6]. This study will use a Distributed Denial of Service (DDoS) attack [7], with tools LOIC (Low Orbit Ion Cannon)to test the quality of a network when it is flooded by an attack [8]. Comparison of Quality of Service in measurements before and after an attack is a benchmark of whether the quality of the network is in accordance with good service standards, namely standardizationTIPHON [9].

1.1 Study Literature

1.1.1 Previous Study
The first previous research is entitled "Study on Quality of Service Mikrotik Router Board Network Wifi in Multimedia Study Program SMK Negeri 2 Kupang". The researchon the performance of the Mikrotik Router Board RB750 seen from the parameters, Quality of Service namely Throughput, Delay, and Packet Loss on a network WiFi. The research method used action research method. The results of this study get a value Throughput "Good" and a value Delay "Medium"[10].

The second previous research is entitled "Analysis of the Quality of Service (QoS) of the network Internet to Support the Strategic Plan of Computer Network Infrastructure at SMK NI Sukadana". This research is to find out how well the performance of the network internet for learning media in SMK NI Sukadana. The parameters Quality of Service (QoS)used are Delay, Jitter, Packet Loss, and Throughput through tools Wireshark. The results of the study showed that the Throughput "not good"valueof 754 Kbps with an index of 2 according to the TIPHON standard [11].

The third previous research is entitled "Application of QoS (Quality of Service) Methods to Analyze Wireless Network Performance Quality" which discusses the performance of WLAN, using Quality of Service (QoS). This study produces values that do not match the TIPHON standard and getresults not compatible with the comparison between bandwidth the requiredand the simulation results [12].

The fourth previous study, entitled "Analysis of Wireless LAN Network Performance Using the Quality of Service (QoS) Method" in the study discussed the quality of theinternet WirelessLANnetwork on the UAD campus by using the parameters of throughput, delay, jitter, and packet loss at the Campus III Network Laboratory UAD. The results showed that the WirelessLAN network in the campus network

laboratory III UAD was good enough to be used in terms of the access process in the form of downloading and uploading[13].

The last previous research is entitled "Analysis of Interference Measurements on Access Point (AP) To Determine Quality of Quality of Service (QoS)" which discusses the analysis of measurementInterferenceon AccessPoint(AP) using parameters of throughput, delay, jitter, and packet loss. The results of the research on network quality during rainy weather, the distance that exceeds 10 meters with the device AccessPointand also the user or the user is too crowded, then this is very affected for the quality of Service(QoS) Analisa Pengukuran Interferensi Pada Acces Point (Ap) Untuk Mengetahui Kualitas Quality of Service (Qos)[14].

1.1.2 Computer Network

A computer network is a system consisting of computers designed to be able to share resources and access information (web browser)[15].A computer network can be interpreted as a collection of a number of communication terminals located in various locations consisting of more than one interconnected computer and access information simultaneously[16].

1.1.3 Quality of Service (QoS)

Quality of Service(QoS) is the ability of a network to provide better services for traffic services that pass through it[17]. Quality of Service(QoS) uses four parameters, namely throughput, delay, packet loss, and jitter[18] to determine whether a network is good or bad[9].Table 1 shows the value of QoS index parameter.

Table 1. QoS index parameter

Value	Persentase (%)	Index
3,8 – 4	100 %	Excellent
3 – 3,79	75 – 94,75 %	Good
2 – 2,99	50 – 74,75 %	Sufficient
1 – 1,99	25 – 49,75 %	Poor

This research investigates Quality of Service (QoS) parameters used include:

1. *Throughput*
   Table 2 shows the value throughput category. Throughputis the total number of successful packet arrivals observed at the destination during that time interval[9].Throughput is the actual ability of a network to transmit data. Usually, throughput is always associated with bandwidth. Because throughput can indeed be called bandwidth in actual conditions[8].

Table 2. Throughput Category

Category	Index	Throughput
Excellent	76 – 100%	4
Good	51 – 75%	3
Medium	26 – 50%	2
Poor	25%	1

2. *Delay*
   Table 3 shows the value delay category. Delay (Latency)is the time it takes the data to travel a distance from origin to destination. Delay can be affected by distance, physical media, as well as long processing [10].Delay is the delay in a packet caused by the transmission process from one point to another which is its destination [8].

Table 3. Delay Category

Category	Delay	Index
Excellent	> 150 m/s	4
Good	150 s/d 300 m/s	3
Medium	300 s/d 450 m/s	2
Poor	> 450 m/s	1

3. *Packet Loss*
   Table 4 shows the value of Packet Loss Category. Packet Loss is a parameter that describes a condition indicating the total number of packet lost. This lost packet can occur due to collisionand congestion on the network[11].

Table 4. Packet Loss Category

Category	Packet Loss	Index
Excellent	0 – 2%	4
Good	3 – 14%	3
Medium	15 – 24%	2
Poor	> 25%	1

4. *Jitter*
   Table 5 shows the value of jitter. Jitter is thevariation delay between packets that occurs on IP networks. The greater the jitter value, the lower the QoS value. To get a good network QoS, thevalue jitter must be kept to a minimum[9].

Table 5. Jitter Category

Category	Jitter	Index
Excellent	0 m/s	4
Good	1 s/d 75 m/s	3
Medium	76 s/d 125 m/s	2
Poor	> 225 m/s	1

1.1.4 Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) is an attack that occurs because the number of packets sent to the target server is very large, exceeding the server's ability to make the system slow or even crash [19]. Distribute Denial of Service (DDoS) is a type of structured attack, a DDoS attack is an attack that we may often encounter among other attacks [20].DDoS attacks are capable of crippling servers by flooding network traffic and causing downs[21].

Distributed Denial of Service (DDoS) is a type of Denial of Service (DoS) attack where attacks can be generated and shared resources, this can cause disruption or unavailability of services for authorized users [22].

1.1.5 Low Orbit Ion Cannon (LOIC)

Figure 1 shows the LOIC software interface. Low Orbit Ion Cannon (LOIC) is an application open-source for network stress testing, LOIC retrieves the IP address of the target system to flood the server with TCP, UDP, and HTTP packets on the network[23]. This software has several features in carrying out the simulation process, such as the IP Address input box, Method, and others, Low Orbit Ion Cannon (LOIC) is an application that is used to attack the network with SYN

Flood[7], by selecting the port to be attacked and which IP address to attack so that it can turn off the system when performing the "IMMA CHARGIN MAH LAZER" action [24].

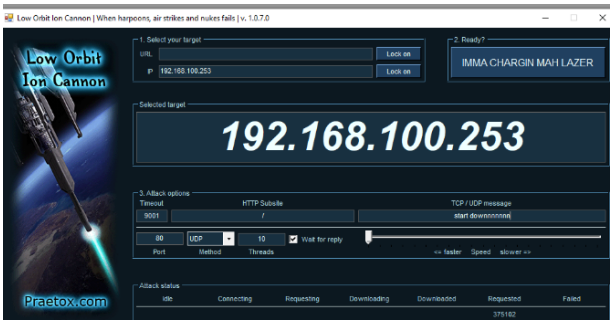

Figure1. LOIC Tool

1.1.6 Network Topology

Figure 2 shows the network topology is a way of connecting several computers to create a computer network. Network topology has various forms of computer arrangement with various types of cables, connectors, and different specifications. There are three types of network topology, namely bus, star, ring topology[25].

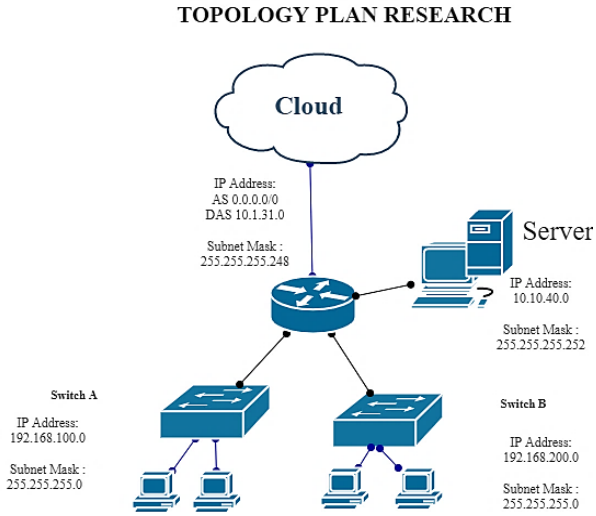

Figure 2. Network Topology

2. METHODOLOGY

2.1 Research Scenario

This scenario is made to explain how the stages of performance analysis of the Local Area Network (LAN) network will be made. This research scenario is carried out by conducting laboratory network diagnostics and designing computer networks according to the research topology to carry out measurements. Measurement of computer network quality in the laboratory, using 4 Quality of Service (QoS) parameters, namely Delay, Jitter, Throughput, and Packet Loss. The first measurement will get the real value of quality before the attack is carried out, the second measurement will get the value after the attack is carried out. Testing attacks on networks using LOIC tools as a DDOS attack concept[26].

The results of the LAN (Local Area Network) performance quality analysis will be compared according to the network quality standard, namely the TIPHON (Telecommunication and Internet Harmonization Over Network) standard. The results of the comparison will determine the solution to improve the quality of the network (Local Area Network) in the computer laboratory.Figure 3 shows the research scenario.

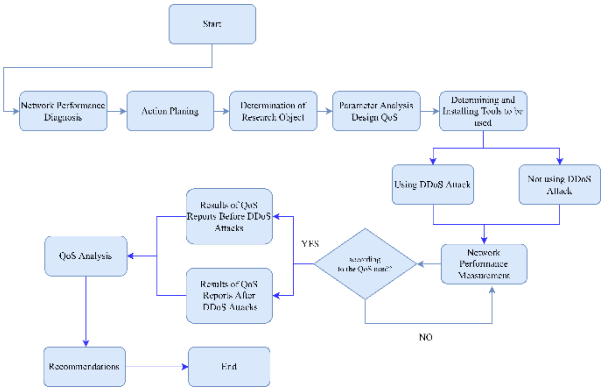

Figure 3. Research Scenario on Flowchart

2.2 Research Stages

At the implementation stage, is the stage where the stage of measuring network performance Quality of Service (QoS). The network performance measurement uses 4 parameters which are measured by the tool Network Speed meter to measure throughput, the tool Ping-test.net to measure Delay, the tool Speedtest measure Packet Loss, and Jitter. Measurements are made on the IP Client located on 2 switches in one network. The computer network used in this study is connected to the IP Public (which is used as the internet), namely IP 10.1.31.0/24 on the computer network in the Laboratory as internet. The LAN topology in the study will be connected with the NAT (Network Address Translation) method [27], with the network UAD, and make it 2 different networks. The server used in this study uses a server on the Ahmad Dahlan University (UAD) server, the concept of NAT (Network Address Translation) in the study, namely IP 0.0.0.0/0 as Active Static and 10.1.31.0 as DAS (Dynamic Active Static), with switch port 3 uses IP 192.168.100.0/24 and switch port 4 uses IP 192.168.200.0/24. The attack was carried out using IP 10.10.40.0/30 which was directly connected to port 2 of the router Table6 is a list of IP Clients for research in computer laboratory.

Table 6.List of IP AddressClients

NO	IP Address*Client*	Description
1	192.168.100.252	Computer 1 A
2	192.168.100.253	Computer 2 A
3	192.168.200.253	Computer 1 B
4	192.168.200.254	Computer 2 B

2.2.1 QoS Measurement BeforeDDoS Attack

The first measurement process in this study requires access in the form of download and upload by doing simple browsing on Google Chrome, then checks 4 parameters (Throughput, PacketLoss, Delay, and Jitter) on Quality of Service(QoS) [28], to get the results of measuring LAN (Local Area Network) network performance. The measurement results will be adjusted to the TIPHON (Telecommunications and Internet Harmonization Over Network) to see the quality of the network.

2.2.1.1 Throughput Measurement

Figure 4 shows the measurement of throughput using a LAN network (Local Area Network) using a Speed Meter Software in a Computer Laboratory. The throughput value was taken before the attack is carried out using Distributed Denial of Service (DDoS) on a test network topology in the Computer Laboratory, the value is obtained average upload and maximum upload. These two values can be used to obtain the value of throughput, taking the throughput value also done on 3 other computers.

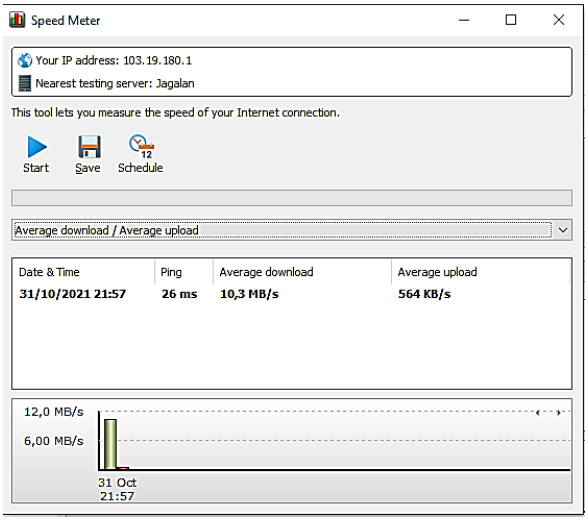

Figure 4.Throughput Parameter Measurement

Table 7 shows the testing used network speed meter, the parameter value is obtained throughput. The value obtained can also produce an average value. Average throughput in the first measurement gets a value 0.80 MB/s, including aexcellent category.

Table 7.Throughput Parameter before Attack

NO	IP Address	Average	Maximum	Throughput
1	192.168.100.252	1,31	1,69	0,78
2	192.168.100.253	1,68	2,00	0,84
3	192.168.200.253	1,90	2,20	0,86
4	192.168.200.254	1,12	1,58	0,71
Average (MB/s)				**0,80**

2.2.1.2 Packet Loss Measurement

Table 8 and figure 5 show the measurement Packet Loss by using a LAN(Local Area Network) prior to the attack using a Distributed Denial of Service (DDoS), the value of the speed of download (download) and upload speeds (upload).Both values can be used to obtain values packet loss.

Table 8. Packet Loss Parameter before Attack

NO	IP Address	Download (MB/s)	Upload (MB/s)	Packet Loss (%)
1	192.168.100.252	94.11	93.37	0
2	192.168.100.253	93.37	94.73	0
3	192.168.200.253	92.39	93.53	0
4	192.168.200.254	93.34	93.15	0
Average (%)				**0**

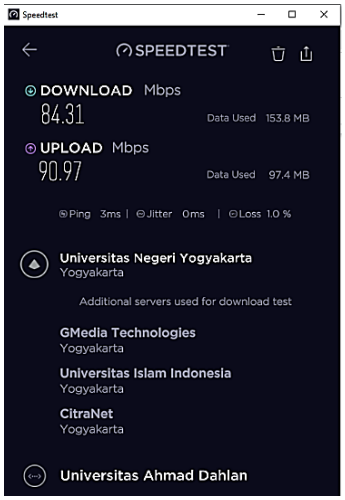

Figure 5. Packet Loss Measurement

2.2.1.3 Delay Measurement

Figure 6 shows the measurement Delay by using a LAN (Local Area Network) prior to the attack using a Distributed Denial of Service (DDoS), the value of the speed of download (download) and upload speeds(upload).Both of these values can be used to obtain the value delay. The delay value is also taken on 3 other computer pada research plan.

Figure 6. Delay Measurement

Table 9 show the test result using Ping-Test.Net, the parameter value is obtaineddelay. The value obtained can also produce an average delay value of 194.5ms. The first measurement of the QoS value still gets a good category value.

Table 9. Delay Parameterbefore Attack

NO	IP Address	Download (MB/s)	Upload (MB/s)	Delay (ms)
1	192.168.100.252	8.55	6.30	191
4	192.168.100.253	4.55	6.30	196
3	192.168.200.253	4.98	7.54	196
4	192.168.200.254	6.04	6.26	195
Average (ms)				**194,5**

2.2.1.4 Jitter Measurement

Figure 7 shows the measurement of Packet Loss using a LAN (Local Area Network) network before carrying out an attack using Distributed Denial of Service (DDoS) on a network topology test in the Computer Laboratory (Information

System Study Program), the results of the study obtained a ping value, where the ping value can be used to get jitter value

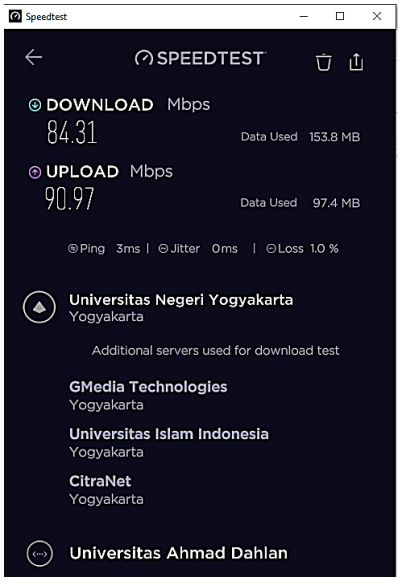

Figure 7.JitterParameterMeasurement

Table 10 shows the test result usingSpeedtest, the parameter value is obtained delay jitter. The value obtained can also produce an average value. Jitter on this measurement get an average value of 0 ms.

Table 10. Jitter Parameterbefore Attack

NO	IP Address	PING (ms)	Jitter (ms)
1	192.168.100.252	3	0
2	192.168.100.253	3	0
3	192.168.200.253	2	0
4	192.168.200.254	2	0
Average(ms)			**0**

.

2.2.2 QoS Measurement in DDoS Attack

Figure 8 shows the process of measuring Quality of Service (QoS) on a LAN Network int the Computer Laboratory by carrying out network attacks using tools LOIC (LowOrbit Ion Cannon), when the network attack is successful, it will measure 4parameters Quality of Service (QoS). This is a comparison of LAN network performance measurement (Local Area Network).

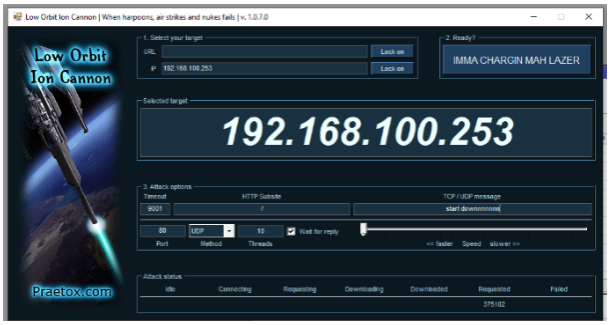

Figure 8. Low Orbit Ion Cannon

Attacking Distributed Denial of Service (DDoS) [29] using the Low Orbit Ion Cannon (LOIC), will be targeted to oneIP client in the network, a LAN(Local Area Network), with Method UDP, Threads 10, TCP/UDP "start downnnnnn",and with the value of speed (Speed) Faster 9. IP Client thatattacked is 192.168.100.253, which was located on switch A in the research plan in the Computer Laboratory.

2.2.2.1 Throughput Measurement

Figure 9 shows the measurement of throughput using a LAN (Local Area Network) after an attack using Distributed Denial of Service (DDoS) on the test network topology in the Computer Laboratoryobtained the average upload value (upload average) and maximum upload. Both values can be used to obtain the value throughput.

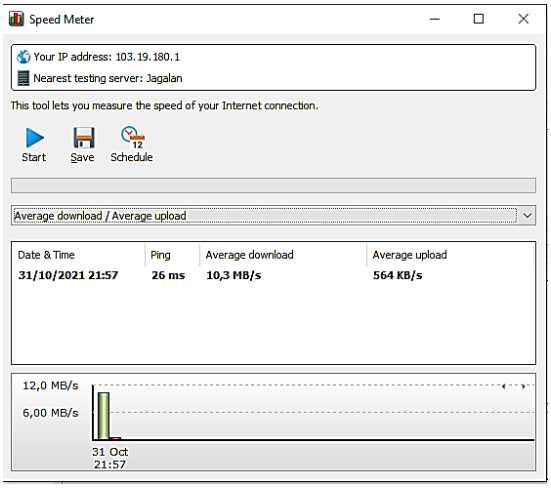

Figure9. ThroughputMeasurement

Table 11 shows the test result using network speed motor, the parameter value is obtained throughput. The value obtained can also produce an average value. The average throughput in the second measurement gets a value of 0.45, including a medium category after the attack on the LANnetwork.

Table 11. Throughput Parameter after Attack

NO	IP Address	Average Upload (MB/s)	Maximum Upload (MB/s)	Throughput (MB/s)
1	192.168.100.252	0.48	1.69	0.28
2	192.168.100.253	0.42	0.83	0.51
3	192.168.200.253	0.38	0.83	0.46
4	192.168.200.254	0.31	0.57	0.54
Average(MB/s)				**0,45**

2.2.2.2 Packet Loss Measurement

Measurement of packet loss using a LAN network (Local Area Network), after an attack using Distributed Denial of Service (DDoS) on the network topology testing in the Computer Laboratory, obtained the valuespeed download (download) and upload speeds(upload).Both values can be used to obtain values packet loss.

The average Packet Loss in the second measurement gets a value of 0.77%. The value obtained for this parameter packet loss uses a speedtest as shown in Figure 10. Table 12is the value of the parameter packet loss after the attack.

Table 12. Packet Loss Parameterafter Attack

NO	IP Address	Download (MB/s)	Upload (MB/s)	Packet Loss (%)
1	192.168.100.252	57.71	77.13	0.70
2	192.168.100.253	84.31	90.97	1.00
3	192.168.200.253	85.44	90.1	0.70
4	192.168.200.254	82.98	89.73	0.70
Average (%)				0,77

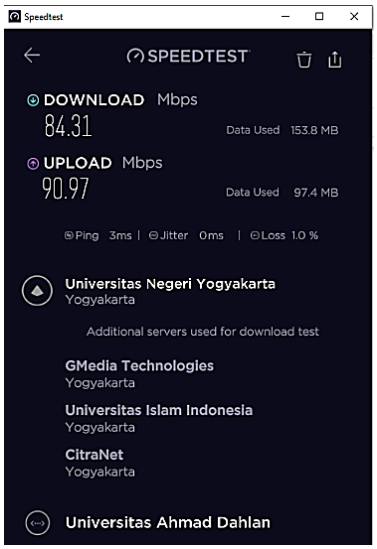

Figure10.Packet Loss Parameter Measurement

2.2.2.3 Delay Measurement

Figure 11 shows the measurements delay by using a LAN(Local Area Network), after an attack was launched using a Distributed Denial of Service (DDoS) on the network topology testing in the Computer Laboratory, obtained the value ofspeed download (download) and upload speeds(upload). Both of these values can be used to obtain the value delay.

Figure 11.Delay Parameter Measurement

Table 11 shows the test result using Ping-Test.Net, the parameter value is obtained delay. The value obtained can also produce an average value. Delay in this measurement gets an average value 208.25

Table 13. Delay Parameterafter Attack

NO	IP Address	Download (MB/s)	Upload (MB/s)	Delay (ms)
1	192.168.100.252	4.14	4.34	208
4	192.168.100.253	2.44	2.78	205
3	192.168.200.253	4.27	7.38	208
4	192.168.200.254	1.13	4.67	212
Average(ms)				**208,25**

2.2.2.4 Jitter Measurement

Figure 12 shows the measurement of jitter by using a LAN(Local Area Network), after an attack was launched using a Distributed Denial of Service (DDoS) on the test network topology in the Computer Laboratory, the valueping, where the ping value can be used to obtain the value jitter.

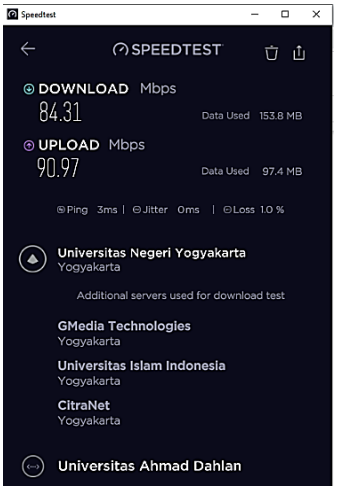

Figure 12. Jitter ParameterMeasurement

Table 14 shows the test result using network speed motorSpeedtest, the parameter value is obtained jitter. The value obtained can also produce an average value.

Table 14. Jitter ParameterafterAttack

NO	IP Address	PING (ms)	Jitter (ms)
1	192.168.100.252	6	1
2	192.168.100.253	4	1
3	192.168.200.253	5	1
4	192.168.200.254	3	0
Average (ms)			**0,75**

2.2.3 Analysis

Analysis of LAN network performance (Local Area Network) using the method Quality of Service (QoS)where this measurement is carried out in the Computer Laboratory, it is necessary to compare between the results of measuring network performance before and after a Distributed Denial of Service attack with standardization TIPHON (Telecommunications and Internet Protocol Harmonization Networks).The result of the measurement values will determine the QoS index parameter. Table 15 shows the result average of QoS measurement comparison before and after DDoS Attacks.

Table 15. The average of QoS measurements Comparison before and after DDoS Attacks

QoS Parameter		Measurement		Category
Name	Range	Average I	Average II	
Delay (ms)	< 150			
	< 250	194,50	208,25	Good
	< 350			
	< 450			
Jitter (ms)	0	0	0,75	Excellent
	< 75			
	< 125			
	< 225			
Packet Loss	0	0		Excellent
	< 3			
	< 15			
	< 25		77,5	Poor
Throughput	100	80		Excellent
	< 75			
	< 50		45	Medium
	< 25			

2.2.4 Result of LAN Network Performance Recapitulation

Recapitulation process LAN, comparing the Quality of Service (QoS) measurements, before and after a Distribute attack d Denial of Service (DDoS).Measurement network quality using LOIC tools greatly affects the LAN network, which gets a Throughput value of 45 Mb/s and a Packet Loss value of 0.77%. QoS Comparison values between parameters as in figure 13, figure 14, figure 15 dan figure 16.

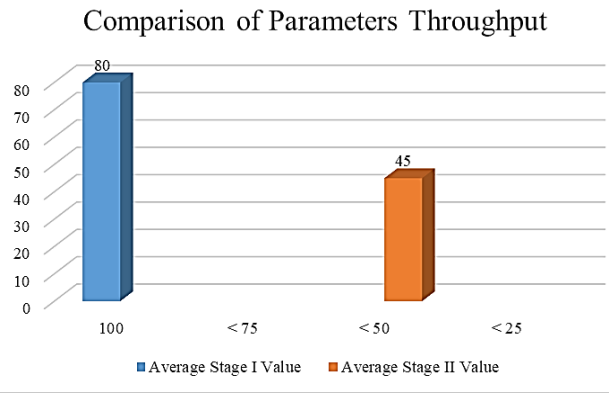

Figure 13. Comparisonof ParametersThroughput

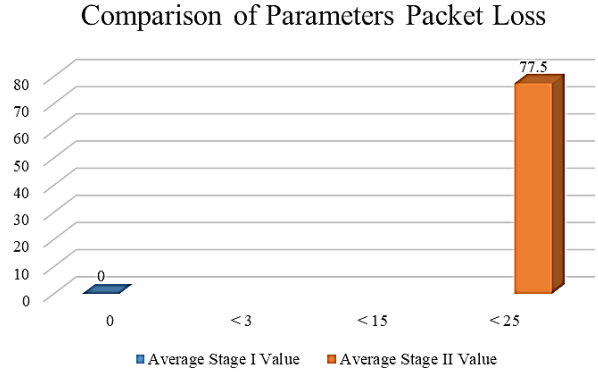

Figure 14. Comparison of ParametersPacket Loss

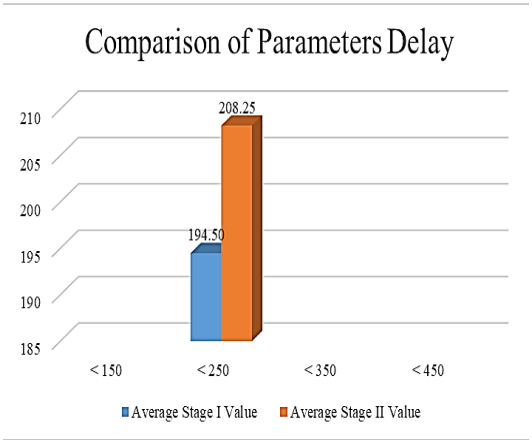

Figure 15. Comparison of Parameters Delay

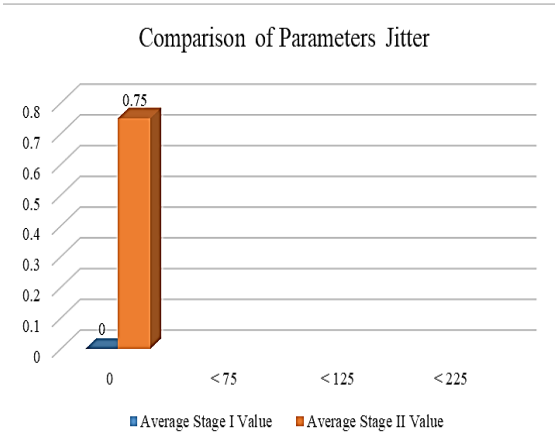

Figure 16.Comparison of Parameters Jitter

Table 16 shows the stage I measurements have an average Quality of Service (QoS) index of 3.75 with a percentage of 94 % belongs to the "Satisfactory" category. The Tabel 16 also shows stage II measurement using an attack using LOIC, as a Distributed Denial of Service attack, it has an average Quality of Service (QoS) index value of 2.50 with a percentage of 62.5% including the category "Poor"

Table 16. Recapitulationbefore and after measurement Local Area Network using Quality of Service

No.	Measurement	QoS Parameter	Average	Index
1	Stage I	Throughput (%)	0,80	4
		Packet Loss (%)	0	4
		Delay (ms)	194,5	3
		Jitter (ms)	0	4
Average index Quality of Service Value				**3,75**
2	Stage II	Throughput (%)	0,45	2
		Packet Loss (%)	77,5	1
		Delay (ms)	208,25	3
		Jitter (ms)	0,75	4
Average index Quality of Service Value				2,50

3. CONCLUSION

The process of analyzing computer network performance using Quality of Service (QoS) on a LAN (Local Area Network), to see network quality by comparing before and after aDDoS attack using tools LOIC, resulting in aQoSindexbefore the attack of 3.75. with a percentage of 94% including the "Satisfactory" category, and theQoSindex after the attack of 2.50 with a percentage of 2.50% including the "Poor" category. Attacks were conducted by using methods of traffic 10 faster, causing trouble for the network system.The Conclusion is that network attacks can affect the quality of network services and even cause disruption to the network system when the traffic is very high, it is necessary to build LAN security against attacks in Computer Laboratory. Future research is expected to measure the quality of the WLAN in Computer Laboratory.

4. REFERENCES

[1] M. R. Hidayat dan I. Riadi, "Investigation of Botnet Attacks using Network Forensic Development Life Cycle Method," *Int. J. Comput. Appl.*, vol. 183, no. 25, hal. 30–36, 2021, doi: 10.5120/ijca2021921632.

[2] M. Iqbal Ichwan, L. Sugiyanta, dan P. Wibowo Yunanto, "Analysis of Hierarchical Token Bucket (HTB) Bandwidth Management with Mikrotik on the SMK Negeri 22 Network," *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 3, no. 2, hal. 122–126, 2019, doi: 10.21009/pinter.3.2.6.

[3] T. N. Hidayat dan I. Riadi, "Optimation Wireless Security IEEE 802.1X using the Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP)," *Int. J. Comput. Appl.*, vol. 174, no. 11, hal. 25–30, 2021, doi: 10.5120/ijca2021920988.

[4] I. Riadi, W. P. Wicaksono, P. Studi, S. Informasi, dan U. A. Dahlan, "Implementation of Quality of Service Using the Hierarchical Token Bucket Method for Theory," *JUSI Vol. 1, No. 2 Sept. 2011*, vol. 1, no. 2, hal. 93–104, 2011.

[5] S. Ahdan, O. Firmanto, dan S. Ramadona, "Design and Analysis of QoS (Quality of Service) Using the HTB (Hierarchical Token Bucket) Method in RT/RW Net Housing Prasanti 2," *J. Teknoinfo*, vol. 12, no. 2, hal. 49, 2018, doi: 10.33365/jti.v12i2.89.

[6] M. Ulfah dan A. S. Irtawaty, "Measurement and Analysis of Internet Network Quality of Service (QoS) in the Balikpapan State Polytechnic Integrated Building," hal. 351–357, 2020.

[7] R. Indraguna, "Web Server Security Analysis from DDoS Attack using Information Systems Security Assessment Framework Method," vol. 183, no. 30, hal. 38–46, 2020.

[8] H. Shah, P. Shah, dan S. Naik, "DDOS Protection by Dividing and Limiting," *Int. J. Comput. Appl.*, vol. 155, no. 11, hal. 12–14, 2016, doi: 10.5120/ijca2016912251.

[9] Aprianto Budiman, M. Ficky Duskarnaen, dan Hamidillah Ajie, "Analysis of Quality of Service (Qos) on the Internet Network of Smk Negeri 7 Jakarta," *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 4, no. 2, hal. 32–36, 2020, doi: 10.21009/pinter.4.2.6.

[10] N. J. Meok, A. Atok, dan G. E. M. S, "A Study on Quality ff Service Mikrotik Routerboard Wifi Network in Multimedia Study Program SMK Negeri 2 Kupang," vol. 2, no. 1, 2019.

[11] M. Purwahid dan J. Triloka, "Analysis of Internet Network Quality of Service (QOS) to Support the Strategic Plan of Computer Network Infrastructure at SMK NI Sukadana," vol. 02, no. 03, hal. 100–109, 2019.

[12] I. Nurrobi, K. Kusnadi, dan R. Adam, "Application Of Quality of Service) Methods to Analyze The Performance Quality of Wireless Networks," *J. Digit*, vol. 10, no. 1, hal. 47, 2020, doi: 10.51920/jd.v10i1.155.

[13] B. N. Azura dan Nurharifah, "Performance Analysis of Wireless Lan Network using Quality Of Service (QoS) Method," *J. Teknol. Terap. Sains*, vol. 4, hal. 2, 2019.

[14] Y. Yanti, N. Pramita, dan Maulizar, "Analysis of Interference Measurements at Access Points (Ap) to Determine Quality of Service (Qos)," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 1, no. 1, hal. 17–21, 2018.

[15] M. J. N. Yudianto, Computer Networks and Its Definitions, vol. Vol.1. 2014.

[16] A. H. Suyanto, Introduction to Computer Networks, no. 45. 2004.

[17] I. K. S. Satwika, "Analysis of the Quality of Service of a Virtual Private Network (Vpn) at Stmik STIKOM Indonesia," *J. Ilm. Inform.*, vol. 7, no. 01, hal. 60, 2019, doi: 10.33884/jif.v7i01.1016.

[18] ETSI, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS)," 1999.

[19] O. R. Prayogo dan I. Riadi, "Router Forensic Analysis against Distributed Denial of Service (DDoS) Attacks," *Int. J. Comput. Appl.*, vol. 175, no. 39, hal. 19–25, 2020, doi: 10.5120/ijca2020920944.

[20] S. Geges dan W. Wibisono, "Development of Prevention of Distributed Denial of Service (Ddos) Attacks on Network Resources With Integration of Network Behavior Analysis and Client Puzzles," *JUTI J. Ilm. Teknol. Inf.*, vol. 13, no. 1, hal. 53, 2015, doi: 10.12962/j24068535.v13i1.a388.

[21] M. A. Ridho dan M. Arman, "Analysis of DDoS Attacks Using Artificial Neural Network Methods," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, hal. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.

[22] N. Athavale, S. Deshpande, V. Chaudhary, J. Chavan, dan S. S. Barde, "Framework for Threat Analysis and Attack Modelling of Network Security Protocols," *Int. J. Synth. Emot.*, vol. 8, no. 2, hal. 62–75, 2017, doi: 10.4018/ijse.2017070105.

[23] R. Arunadevi, "Experimentation Of Denial Of Service Attack In Wireless Local Area Infrastructure Network Using Loic Tool," vol. 8, no. 8, hal. 51–55, 2018, doi: 10.9790/9622-0808035155.

[24] Karmadenur dan R. Yusuf, "Analysis of Snort Rules to Prevent Synflood Attacks on Network Security," *Int. J. Comput. Appl.*, vol. 178, no. 40, hal. 14–19, 2019, doi: 10.5120/ijca2019919283.

[25] M. A. Anas, Y. Soepriyanto, dan Susilaningsih, "Development of Network Topology Multimedia

Tutorials for Class X Vocational School of Computer and Network Engineering," Muchammad Azwar Anas, Yerry Soepriyanto, Susilaningsih," *Multimed. Tutor.*, vol. 1, no. 4, hal. 307–314, 2018.

[26] H. A. Alamri, V. Thayananthan, dan J. Yazdani, "Machine Learning for Securing SDN based 5G Network," *Int. J. Comput. Appl.*, vol. 174, no. 14, hal. 9–16, 2021, doi: 10.5120/ijca2021921027.

[27] F. Chowdhury, "NAT Traversal Techniques: A Survey," *Int. J. Comput. Appl.*, vol. 175, no. 32, hal. 9–19, 2020, doi: 10.5120/ijca2020920885.

[28] K. A. Sadiq, J. K. Ayeni, dan F. S. Oyedepo, "An Optimized Kwara State Polytechnic Campus Networks using VLAN," *Int. J. Comput. Appl.*, vol. 175, no. 17, hal. 1–3, 2020, doi: 10.5120/ijca2020920671.

[29] A. Alhasan dan S. Wei, "Predicting DDoS Anomaly Patterns in SDN Controller using Hidden Markov Model," *Int. J. Comput. Appl.*, vol. 175, no. 39, hal. 33–41, 2020, doi: 10.5120/ijca2020920961.