



Article

Quality of Service (QoS) Management for Local Area Network (LAN) Using Traffic Policy Technique to Secure Congestion

Wan Muhd Hazwan Azamuddin , Rosilah Hassan *, Azana Hafizah Mohd Aman, Muhammad Kamrul Hasan and Ahmed Salih Al-Khaleefa *

Network and Communication Technology (NCT) Lab, Centre for Cyber Security, Fakulti Teknologi & Sains Maklumat (FTSM), Universiti Kebangsaan Malaysia (UKM), 43600 UKM, Bangi 43600, Selangor, Malaysia; p101964@siswa.ukm.edu.my (W.M.H.A.); azana@ukm.edu.my (A.H.M.A.); mkhasan@ukm.edu.my (M.K.H.)

* Correspondence: rosilah@ukm.edu.my (R.H.); ahmed.salih89@siswa.ukm.edu.my (A.S.A.-K.); Tel.: +60-13-388-7738 (R.H.); Tel.: +60-11-2122-2077 (A.S.A.-K.)

Received: 12 April 2020; Accepted: 25 April 2020; Published: 12 May 2020



Abstract: This study presents the proposed testbed implementation for the Advanced Technology Training Center (ADTEC) Batu Pahat, one of Malaysia's industrial training institutes. The objectives of this study are to discover the issues regarding network congestion, propose a suitable method to overcome such issues, and generate output data for the comparison of the results before and after the proposed implementation. The internet is directly connected to internet service providers (ISPs), which neither impose any rule nor filter the traffic components; all connections comply on the basis of the base effort services provided by the ISP. The congestion problem has been raised several times and the information technology (IT) department has been receiving complaints about poor and sometimes intermittent internet connection. Such issues provide some ideas for a possible solution because the end client is a human resource core business. In addition, budget constraints contribute to this problem. After a comprehensive review of related literature and discussion with experts, the implementation of quality of service through add-on rules, such as traffic policing on network traffic, was proposed. The proposed testbed also classified the traffic. Results show that the proposed testbed is stable. After the implementation of the generated solution, the IT department no longer receives any complaints, and thus fulfills the goal of having zero internet connection issues.

Keywords: best-effort service; classification; traffic policing; QoS; LAN

1. Introduction

Network technology users practice a variety of methods for searching for information, such as reading books from the library or reading an online article through internet access. Users need a unique id called an internet protocol (IP) address when they gather data from the internet. However, when billions of users try to gain simultaneous internet access to the same data, congestion traffic occurs. This phenomenon also happened in our training institute, which experiences congested internet connectivity during peak or non-peak hours. P.K. Dey et al. mentioned that the solution for increasing network traffic without it becoming congested is increasing the amount of bandwidth [1]. However, increasing the amount of bandwidth would increase our monthly cost. M. Marcon et al. mentioned that using a method that will yield a traffic-shaping network can resolve traffic congestion issues [2]. This proposal, however, will affect voice and video transmissions because real-time communication is necessary for such processes [3]. After comparing related works and considering the institutional budget constraints, this study has

generated the solution of applying traffic policing. This method is suitable for various data and prevents lagging issues in the internet connection.

With the growth of computer networking, data can be easily obtained by accessing the internet without any constraint. Before this technology, users needed to gather data by reading a book from the library and other sources. Internet services are provided by the internet service providers (ISPs) of each country. ISPs are the main proprietors of all internet-related services, which issue service level agreements (SLAs) that must be obeyed by customers. The current SLAs offer technology in accordance to customer demand and allocate bandwidth to provide stable internet access [1]. To ensure the stability of the network performance, ISPs apply a quality of service (QoS) approach on network access. Customers complain that resources are hardly accessible because of the bottleneck in the traffic. IP was developed as a new mechanism through the implementation of type of service (ToS), which was embedded with QoS technology in various operations in network technologies [4]. QoS is more ideal to apply on the customer side rather than on the provider side [5]. Customers directly connect to the local area network (LAN) using data packet communication to transmit large quantities of data using high bandwidth over the physical medium. Topology LAN is the best medium for low-range packet-based data communication. QoS standards are used to maintain transmission quality and diagnose errors that occur in the traffic network. The main function of QoS is to provide good service accessibility to the end user. To apply QoS, each network user must reach the network infrastructure that contains the applications. I. Zakariyya et al. stated that by applying QoS, the goal of providing high accessibility can be reached at least 99% per second and fails to do so no more than 5 min per year [6]. Various parameters of network transmissions, such as throughput, delay, jitter, loss, and noise loss (i.e., The number of packets that cannot reach the destination), can be determined. Loss occurs when the quantity of data is excessively big to be transferred. Zero loss can be achieved when the network traffic experiences zero congestion. M. Kassim et al. mentioned that when the network is congested, QoS will take part in the transmission to ensure zero communication loss [7]. Delay measurement can be defined as the total number of times that the data have been transmitted from the sender to receiver. Another network performance that can be measured is jitter, which is also known as delay variation. Jitter can be defined as the time consumed by the communication of the transmission data packet from the sender to its destination.

O Slavata and J. Holub stated that QoS for LANs can be assessed through software- and hardware-based approaches [8]. QoS can be applied to monitor network traffic and convergence using various techniques. This ensures the clear transmission of converging data, such as videos and voices. A.H.M. Aman et al. proposed a technique that may vary in terms of implementation on the basis of traffic or class services [9]. The QoS will assign a high priority to the transmission of data that contain video or voice, which therefore requires a traffic-based method. QoS technology can prevent any disruption in the network performance. Although QoS can solve bottleneck traffic, for congestion that happens all of a sudden, A.S. Ahmed et al. stated that in the case of sudden congestion, a misconfiguration setting for the queuing discipline can enable attacks, such as denial-of-service and worm [10]. This issue can be addressed using a suitable QoS mechanism.

2. Related Works

Many solutions have been proposed to evaluate network system performance, including an implementation of QoS using throughput, which is a QoS based on the bandwidth utilization. The assessment of the performance of this QoS is managed by the ISP. F. Amato et al. established some guidelines for processing large quantities of data from multimedia applications on social media and developed a technique that is based on a user-centered approach [11]. F. Amato et al. proposed a new solution by using the Flickr technique to generate multimedia stories [12]. However, this method focuses on visual analytics. The details of each QoS element will be discussed in the following subsection.

2.1. QoS and Network Convergence through Throughput

Network convergence involves different types of traffic that has specific requirements. Given that multiple traffics react based on their own behaviors, I. Zakariyya and M.N. A Rahman developed a new scheme for controlling the internet on the ingress router to measure the throughput, utilization in an IP-based network by considering traffic flows, and the corresponding processing times by using the adaptive throughput policy (ATP) algorithm [6]. This new algorithm has overcome several issues, such as congested hyper text transfer protocol (HTTP) and bandwidth performance under bursty traffic. The results showed that the ATP algorithm led to high bandwidth savings and fast traffic processing time under the threshold (P1). Bursty traffic throughput can be resolved by managing the network performance on the basis of the implementation policies on the ATP algorithm. In conclusion, this technique can control such throughput using the implementation policy in the development system.

Another objective of QoS-related studies is to assess the network performance with respect to voice delivery applications. The specific goal of such studies is to ensure that the packet loss will be discarded because the amount of packet delay will affect the transmission [13]. Voice applications use voice channels for transmission at a specific time. Voice-based applications achieve a satisfactory performance when they operate on a time-division multiplexing network application; such applications have run on best-effort service network as voice over IP. Best-effort service networks have numerous packets and large amounts of delays. Service network providers that use such networks do not have the required performance for voice applications. Therefore, G. Mojib et al. suggested that QoS technologies can be used to ensure that applications can be properly supported by using network multiservice IP [14].

2.2. QoS Based on Bandwidth Utilization

A previous study emphasized that the deployment of QoS is not necessary because increasing the bandwidth can resolve the network performance issues. The author argued that implementing QoS is complicated and adding bandwidth is relatively simple. However, we must look closely at the QoS problems to verify the above inference. I. Zakariyya et al. enforced a class-based weighted fair queue (CBWFQ) queuing discipline for fairness in sharing bandwidth among different traffic classes in the network, as well as a CBWFQ algorithm to control network congestion [6]. This technique is similar to the weighted round robin queuing discipline. Congestion occurs when all network connections have large bandwidths; thus, applying QoS technologies is appropriate. Researchers stated that the current carrier networks have large amounts of bandwidth and are designed to minimize traffic congestion. Moreover, adding minimum bandwidth will guarantee that each traffic's bandwidth requirement is met and the traffic classes are shaped based on their services.

Another related research conclusion is that aggressively adding bandwidth to IP networks will exploit the demand of the internet [9]. The carrier network may offer low latency connections across metropolitan area networks. The traffic that goes through a network should therefore be classified to achieve QoS. If congestion happens in the ingress router, the QoS level will be rated poorly even if the network providers offer excellent QoS performance.

2.3. Online Sequential Extreme Learning Machine

Z. Ali et al. stated that service providers have embedded QoS technologies in their services. Malaysian ISPs, such as Telekom Malaysia, own the network connection's copper, fiber, and wireless technologies [13]. Adding bandwidth will render QoS attractive to customer demands that require this technology to achieve the highest-quality transmission. ISP technologies are using dense wavelength division multiplexing in fiber optic connections to ensure that additional bandwidth can be immediately provided at an affordable cost when a customer requests a bandwidth upgrade. In comparison, other ISP technologies, such as mobile wireless and satellite communication, are highly constrained by the limited frequency spectrum.

Another researcher mentioned that another simple and cost-effective way to increase bandwidth is to increase the wavelengths. In addition, they suggested that service providers merge with another operator network technology (e.g., Maxis Communications) to provide best-effort services. By merging with an operator telco network, service providers can offer premium data services with performance guarantees. As applications that use QoS as their performance index, telco networks differentiate services on the basis of the classes between premium data service and best-effort subscribers. For a minimal user that does not use maximum bandwidth, the network can accomplish required throughput without throttling bandwidth. For those who need more bandwidth to reach their QoS satisfaction, the network can offer additional bandwidths at an additional price.

Measuring the QoS parameter with constraining bandwidth must be performed using a real traffic environment [15] to improve the performance of real-time traffic in a constrained bandwidth network. Among the queuing disciplines, such as round robin (RR), priority-based, and token bucket (TB), TB has the most satisfactory ability to receive the packets smoothly, and RR exhibited better performance than the other approaches [16]. However, these queuing disciplines were not compared simultaneously. Moreover, no policy or classification packet was applied to deploy the QoS technologies to obtain a comprehensive comparison of network performances under different queuing scenarios. Applying multiple techniques, such as first-in, first-out (FIFO), CBWFQ, low-latency queuing, class-based weighted random early detection, explicit congestion notification, and link fragmentation and interleaving (LFI), can result in high network performance levels [17]. The more advanced the method, the better the quality of the transmission [18]. The issues in using advanced methods include packet delay in transmission.

3. Methodology

The implementation of QoS via traffic policing involves four phases. This study utilized quantitative analysis to evaluate the network performance in our institution (i.e., Advanced Technology Training Center (ADTEC) Batu Pahat).

3.1. Phase 1—Data Collection and Survey

For phase 1, the necessary data and information is gathered by conducting a survey among the end users regarding their complaints. Some concepts and methodologies from previous literature are adjusted to achieve the research objectives. This phase is crucial in identifying the issues that happen in the current network communication. The questionnaire used in the survey is shown in Figure 1. The inputs that can be gathered from the questionnaire include the number of internet users during daytime, purpose of using the internet, and the number of times that connection issues happen in a week. A software is also used to obtain and analyze end user data.

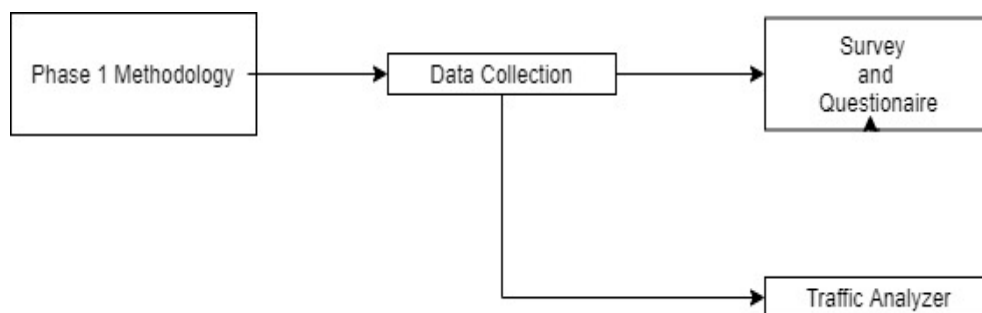
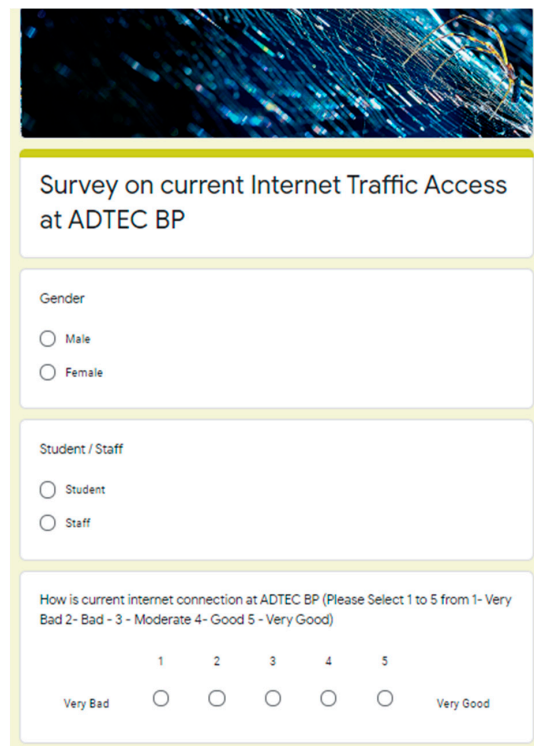


Figure 1. Data collection phase.

A survey form has been distributed among students and staff as it is shown in Figure 2. A total of 149 respondents participated (Figure 3), where 70.5% are male and the remaining 29.5% are female. Figure 4 shows that students comprise the majority of the respondents (31.5%). Approximately 53.7%

of the respondents (80) specified that their main issue is the poor internet service, 31.5% (47) stated that the internet connection is bad, and 13.4% (20) and 1.3% (2) stated that the internet connection is in moderate and in good condition, respectively. Figure 5 suggests that almost 85% experienced poor internet connection, which must be addressed. These data are inputted to the next phase to generate the solution to the connection issues in the current interconnection in ADTEC BP.



Survey on current Internet Traffic Access at ADTEC BP

Gender

Male

Female

Student / Staff

Student

Staff

How is current internet connection at ADTEC BP (Please Select 1 to 5 from 1- Very Bad 2- Bad - 3 - Moderate 4- Good 5 - Very Good)

Very Bad 1 2 3 4 5 Very Good

Figure 2. Advanced Technology Training Center (ADTEC) BP internet connection survey form.

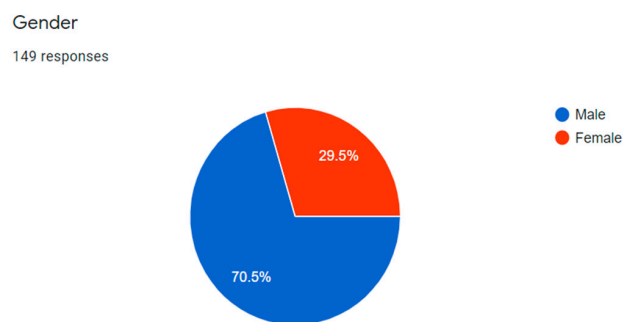


Figure 3. Demography by gender.

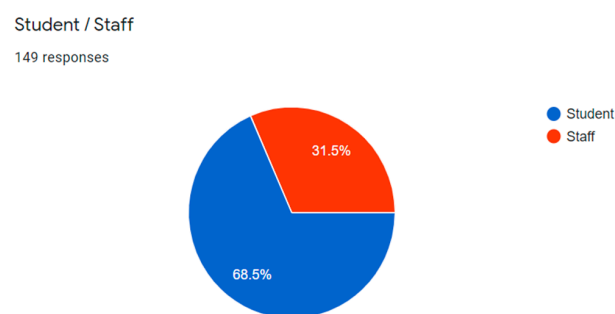


Figure 4. Demography by occupation.

How is current internet connection at ADTEC BP (Please Select 1 to 5 from 1- Very Bad 2- Bad - 3 - Moderate 4- Good 5 - Very Good)

149 responses

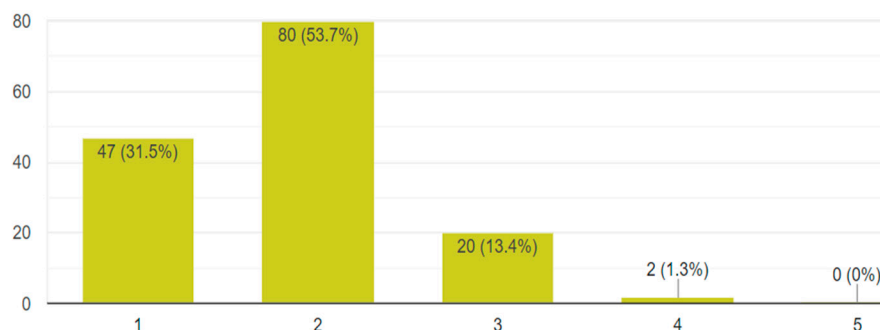


Figure 5. Statistics of the internet connection issues in ADTEC BP.

3.2. Phase 2—CISCO Router-on-a-stick Cross-Origin Resource Sharing (CORS) Development

The development in this phase is supported by the concepts from phase 1. As shown in Figure 6, the testbed setup is implemented on an initial network, which requires upgrade through the application of the QoS mechanism. Several modifications are applied to this testbed, such as applying virtual LAN and CROS for measuring the network performance at the egress router. The testbed started by designing a network diagram that must be upgraded and selecting suitable equipment for the hardware and software. Several routers and switches are used to set up the experimental QoS in our network infrastructure. No policy and rules are implemented before the testbed setup, which, according to the collected data, is the main cause of network congestion.

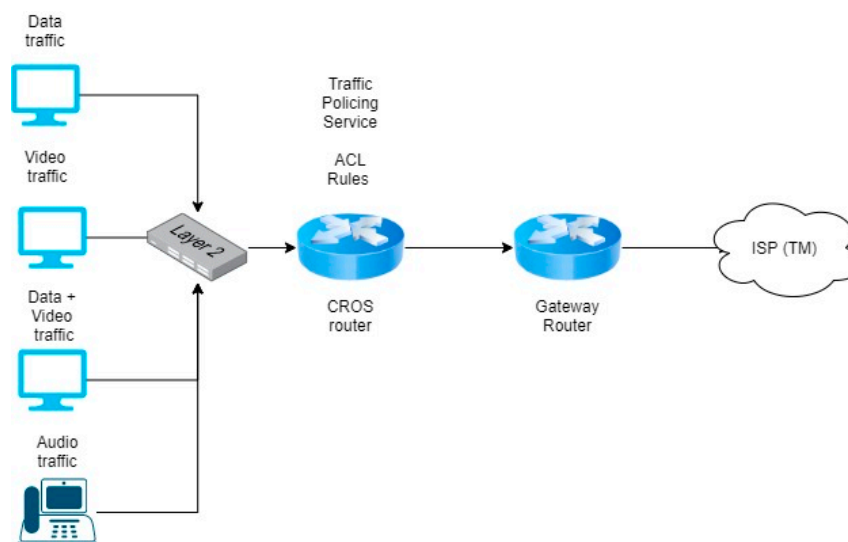


Figure 6. Testbed for CORS development.

The testbed utilizes several approaches through classification and remarking and traffic policing, which are configured on a testbed setup by applying a new approach to the current traffic network. Table 1 lists the three types of testing that must be generated for CORS development.

Table 1. Type of testing on CROS development.

Test	Description
Test 1	No classification and policy
Test 2	With classification but no policy
Test 3	With classification and policy

- (a) **Test 1: No classification and policy.** The FIFO queuing discipline without any rules on the router configuration is used for all incoming packet data. This discipline is the baseline for comparing transmission control protocol (TCP) and user datagram protocol (UDP) testing. None of the traffic is classified or remarked with any policy.
- (b) **Test 2: Traffic classification method.** This second methodology is based on the classification of the packets at the ingress router, which are categorized on the basis of their service classes. After grouping, the packets are differentiated depending on their values; packets that contain streaming data after the classification received high priority transmission. This testing, which mainly focuses on the classification of the packet, can be applied only by using a single TCP stream of a packet.
- (c) **Test 3: Traffic policing method.** This step aims to inspect, classify, and categorize the packets that arrive at the incoming port of the router to ensure that they will have unique differentiated services code point values. The remarking process is executed after the categorization at the egress router and each packet obtained is assigned its corresponding ToS value. Although the packet has been remarked, it can still obtain an agreement to enter the neighboring router. After exiting the egress router, all packets are remarked on the basis of the information that has been previously agreed on.

3.3. CROS Analysis

The results are compared with the theoretical concepts discussed in the literature review. The output measurements are collected through multi-testing on the basis of the various scenarios. Subsequently, the throughput, delay, and jitter are measured. Two protocols, namely TCP and UDP, are used as the standard for the experiment. The two tests are compared to obtain the best solution and to determine which protocol is suitable for QoS mechanism implementation. The analysis is conducted using simulation software, including Cisco Packet Tracer, jperf, and GNS3.

4. Results and Discussion

Three tests have been performed in the testbed to compare the differences in the network performances. Before the implementation of QoS in the ADTEC BP network, the network systems are often interrupted during peak hours and the network always goes offline. After the three improvement tests, many positive implications were observed. The detailed discussions of the results are presented in the subsequent subsections.

4.1. Test 1: Benchmark Testing

4.1.1. Test 1: Single Parallel Stream Implementation

Figure 3 shows the graph of the traffic load in packets per second versus time of the unclassified and unremarked traffic that passed through the router. The result shows that all frame sizes in the graph are linear and the single-stream transmission produced a constant throughput within the network. The maximum number of packets per second obtained through the single-stream transmission is 4200; a linear packet transmission of 3500 packets per second is maintained.

Figure 7 shows that 4000 packets have been traced at a gateway router without any control mechanism. The variety of input that has been inserted at the gateway router can substantially influence

the current network traffic. At 20 s, the traffic is linearly sustained for at most 2 min and then collapses due to congestion. Hence, an improved solution will be developed in the next testing process.

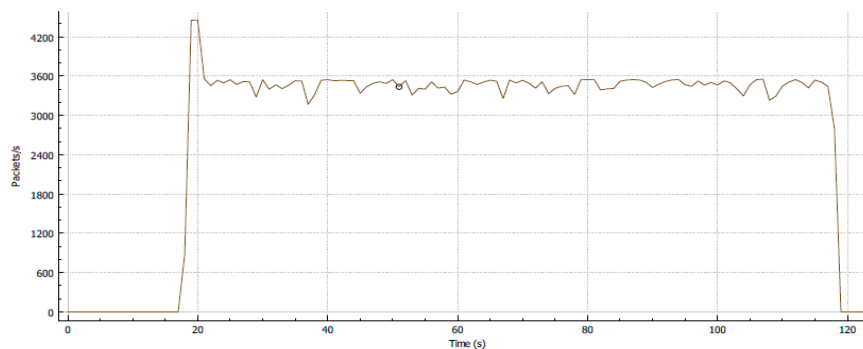


Figure 7. Single-stream throughput with no classification and no policy.

Table 2 presents the data transfer per packet of the 4000 packets that reached the egress router (gateway router). A packet is analyzed every 10 s; the transfer rate for each packet is around 69 MB and all packets produce throughput at 58 Mbps. Sampling data are analyzed for 100 s and will be continued for another 100 s for the second testing.

Table 2. Single-stream TCP testing.

Interval (sec)	Transfer (Mbytes)	Throughput (Mbps)
0.0–10.0	69.40	58.10
10.0–20.0	69.20	58.00
20.0–30.0	69.50	58.20
30.0–40.0	69.30	58.10
40.0–50.0	69.10	58.10
50.0–60.0	69.70	58.30
60.0–70.0	69.30	58.00
70.0–80.0	69.60	58.20
80.0–90.0	69.50	58.50
90.0–100	69.40	58.10

The results presented in Table 2 are plotted as packet size (MB) versus time (s) in Figure 8. The illustration shows that the minimum and maximum values for the packet size on a single TCP stream are 58 and 58.5 MB, respectively. The average packet size is 58 MB and the communication is linear in the TCP testing using single-stream transmission. This value can serve as a benchmark for this testbed because the data possess high bandwidth and high packet size during the single TCP transmission.

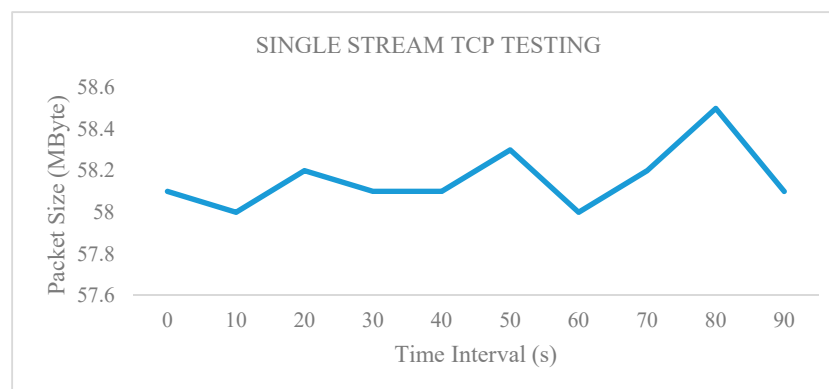


Figure 8. Single-stream TCP testing.

4.1.2. Two Parallel Stream Implementation

Figure 9 shows the simultaneous run of two parallel streams on the TCP test to measure the network performance; the stated transmission of the TCP protocol has a value. The two streams have their corresponding bandwidth transmission. Stream 1 (red line) has transmitted at most 5000 packets, whereas Stream 2 used approximately 2000 packets. The former is for video transmission, whereas the latter is for normal data transmission; video produces more packets compared to Stream 2 transmission and the graph is still linear.

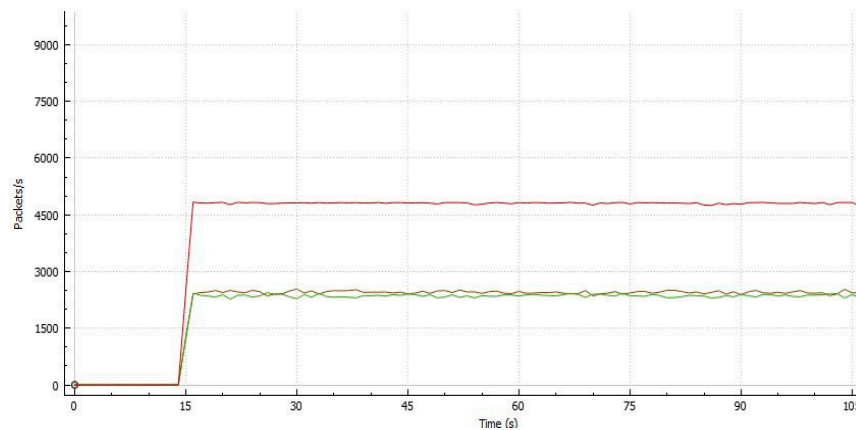


Figure 9. Two-stream throughput without classification and policing.

Table 3 shows that two input TCP transmissions have been analyzed at the egress router; each traffic has its bandwidth. For TCP Stream 1, the transfer rate starts at 52.70 MB and the bandwidth usage is at 46.40 MB. For TCP Stream 2, the transfer rate and bandwidth usage are 58.4 and 47.80 MB, respectively. The findings indicate that higher transfer consumes higher bandwidth. The transfer rate is higher in the previous test than in this test, which might be because the latter involves both streams that have to share the total throughput to obtain an effective success.

Table 3. Results of the TCP testing using two parallel streams.

Interval (sec.)	Stream 1 (Mbytes)	Stream 2 (Mbytes)	Throughput 1 (Mbps)	Throughput 2 (Mbps)
0.0–10.0	52.70	58.40	46.30	47.80
10.0–20.0	52.80	58.50	45.50	48.50
20.0–30.0	52.60	58.20	44.60	47.60
30.0–40.0	52.90	58.30	45.40	49.00
40.0–50.0	52.90	58.40	46.70	48.80
50.0–60.0	52.60	58.70	45.80	45.60
60.0–70.0	52.90	58.40	45.90	49.70
70.0–80.0	52.90	58.30	46.50	47.80
80.0–90.0	52.80	58.40	44.70	49.20
90.0–100	52.90	58.40	44.10	49.10
Total		1112.0		93.3

Figure 10 shows that two-stream traffic has been generated on the testbed testing. From time 0, Stream 1 produces 32 MB of packet size, whereas Stream 2 produces 31.5 MB. The results indicate that the value of the production packet size in this transmission is less than that in the single-stream TCP transmission. This phenomenon occurred as the traffics of Streams 1 and 2 share major bandwidth to communicate; both streams involve data and video transmission. In conclusion, implementing the QoS mechanism can support more traffic transmission compared with the single-stream transmission. Although the packet size of the former is less than that of the latter, no communication issue occurred.

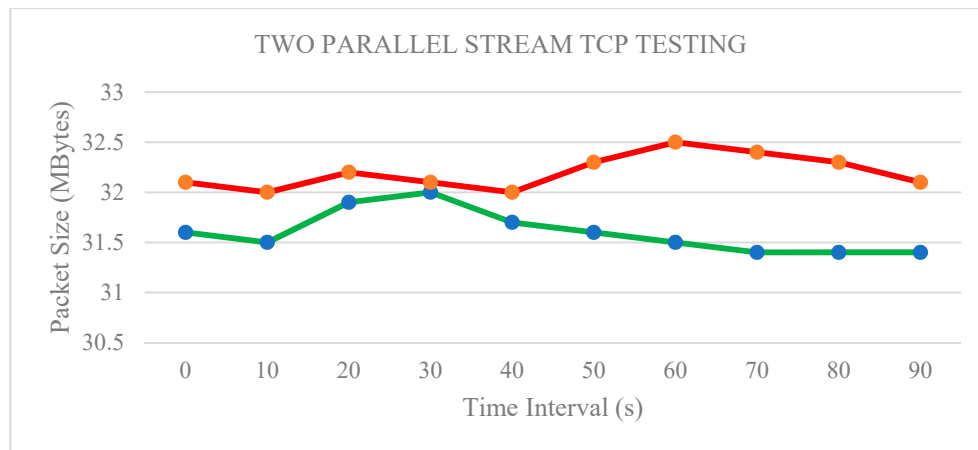


Figure 10. TCP testing using two parallel streams

4.1.3. Three Parallel Stream Implementation

Figure 11 illustrates the simultaneous run of three parallel streams in the TCP test to measure the network performance; the stated transmission of TCP protocol has a value. Similar to using two streams, the three streams will have their corresponding bandwidth transmission. Streams 1, 2, and 3 transmitted at 1700, 1600, and 1500 packets, respectively. Each stream represents data, audio, and video, respectively. From Figure 7, the more stream accessed by the traffic, the less packet size will be produced for network transmission.

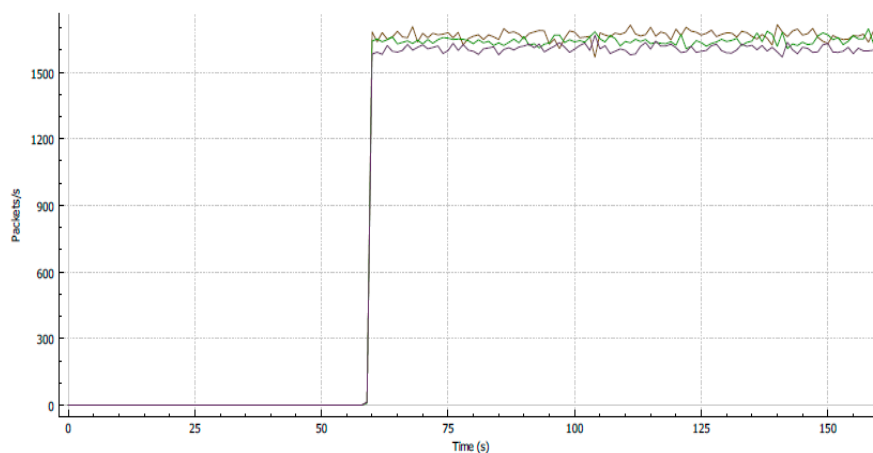


Figure 11. Throughput for three streams with no classification and policing.

Figure 12 shows that each stream is still a linear graph, but has its corresponding transmission value. Stream 1 (red line) used approximately 31.40 Mbps bandwidth, Stream 2 (yellow line) used 32.10 Mbps, and Stream 3 (green line) used approximately 30.50 Mbps. The total TCP packet size transferred using the three parallel streams is 1122 MB, with a corresponding bandwidth utilization of 94.2 Mbps. A small gap in the packet size is produced during the three-stream transmission. The traffic performance is clear but the number of productions decreased compared with the previous cases. Therefore, this methodology, even without using the traffic policing method, still exhibits satisfactory performance, despite the reduced packet size.

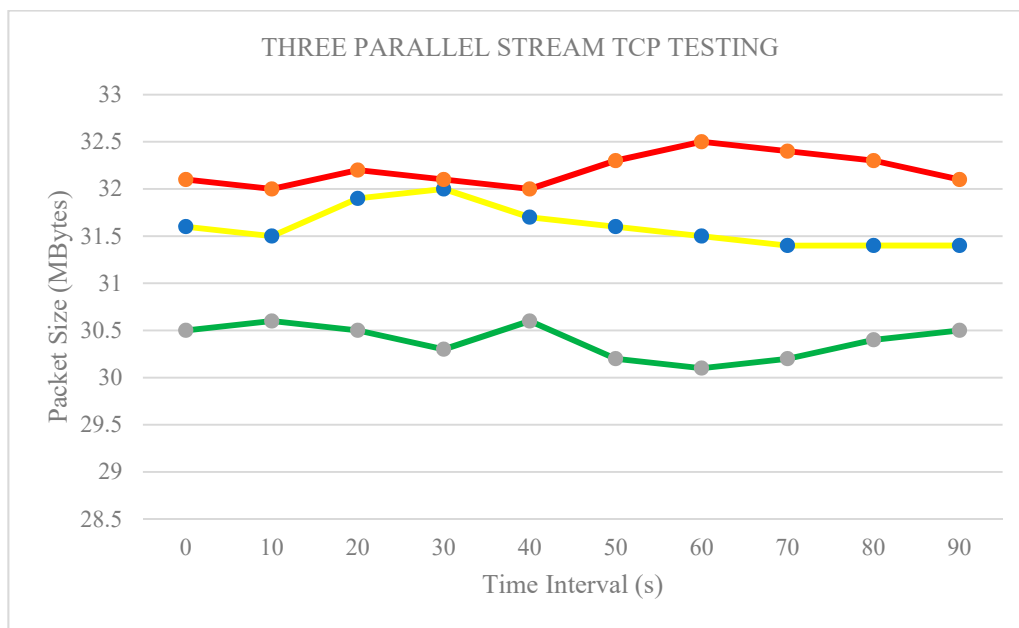


Figure 12. CP testing using three parallel streams.

4.2. Test 2: Traffic Classification Method

The next testbed used the second approach to classify the traffic that enters the ingress router. Table 4 presents the configurations that will be set up at a QoS router to perform the classification and categorization of traffic, namely, internet control message protocol (ICMP), HTTP, and VOICE packets. These configurations are adopted to ensure that each packet will have its own channel and bandwidth usage in the ADTEC BP infrastructure. Each traffic will be class mapped on each category and VOICE will match precedence 3.

Table 4. Traffic classification configurations

Traffic classification	class map	Setting	class map	Match-all	ICMP
	match	access-group	101		
	class-map	match-all	HTTP		
	match	access-group	105		
	class-map	match-all	VOICE		
	match	precedence	3		

The packet has been classified after entering the QoS_router (Figure 13). The different streams represent their packet markings. For example, the single-stream ICMP packet has been marked for 373 packets, which is equivalent to 72614 bytes, whereas HTTP packets have been marked for 1246 packets, which represent 304502 bytes. For the two and three parallel streams, the bar has doubled compared with the single-stream transmission. In conclusion, the second classification process is effective in ensuring that each traffic will not share the main bandwidth to achieve stable transmission.

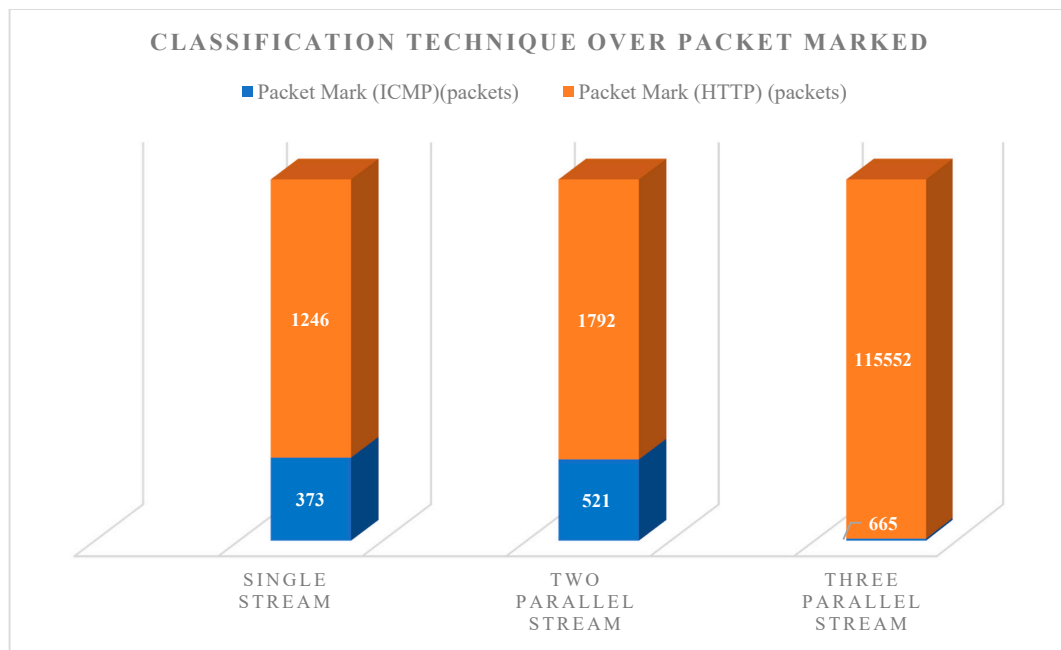


Figure 13. Packets marked by the classification technique.

4.3. Test 3: Traffic Policing Method

As shown in Figure 14, the output has collected an egress router. Packets that have bursty data more than 1.0 GB will be dropped off and the spike of traffic has been cut off. After the throughput of the traffic has been assigned, a packet for TCP testing that passed the access rule will be used in the transmission (Figure 15). This rule is useful in blocking big data communication, which is the common cause of network congestion. Figure 16 shows that the two parallel communications in one traffic, which have more bursty data than the previous test. In addition, many packets displayed numerous spikes. Figure 17 shows the output of the packet size after it was filtered using traffic policing. As shown in Figure 18, when numerous parallel TCP communications transmit in the network infrastructure, many packets dropped because the bulky data are removed. As an example of the three parallel streams, a total of 10840 packets are inserted at the egress router, which is equivalent to 1580609 bytes. After the process, almost 30% of the packets exceeded the limit and were dropped, whereas the remaining 70% passed through. In conclusion, this approach is suitable for TCP communication but is not recommended for handling UDP traffic (e.g., voice communication) because of substantial delays and losses.

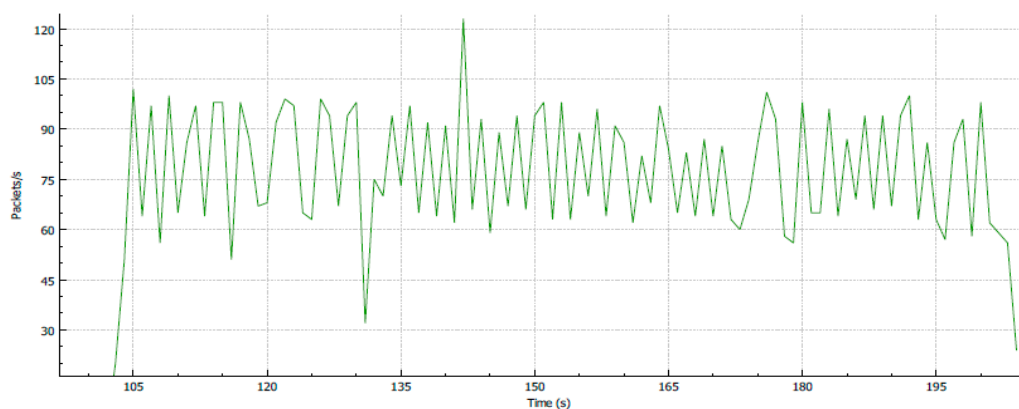


Figure 14. Throughput of the single-stream technique policing methodology.

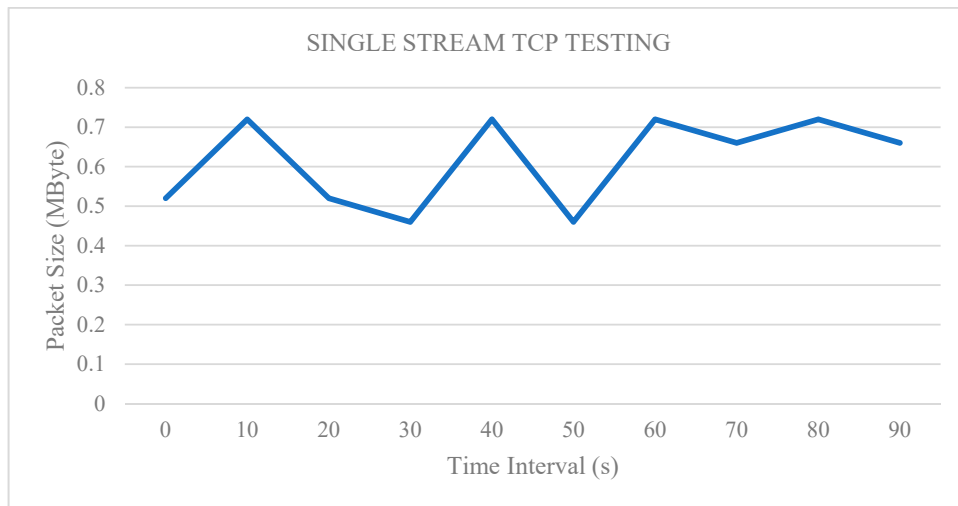


Figure 15. Packet size output of the single-stream technique policing.

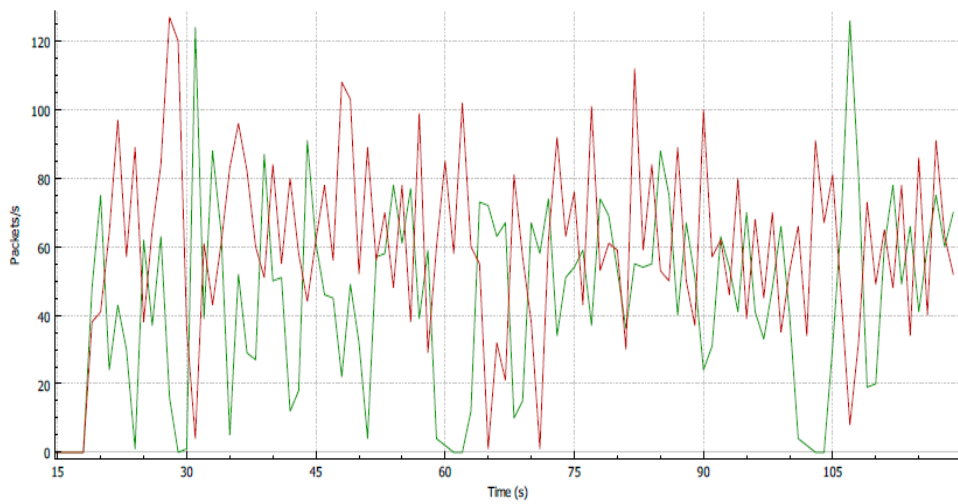


Figure 16. Throughput of the two-stream technique policing methodology.

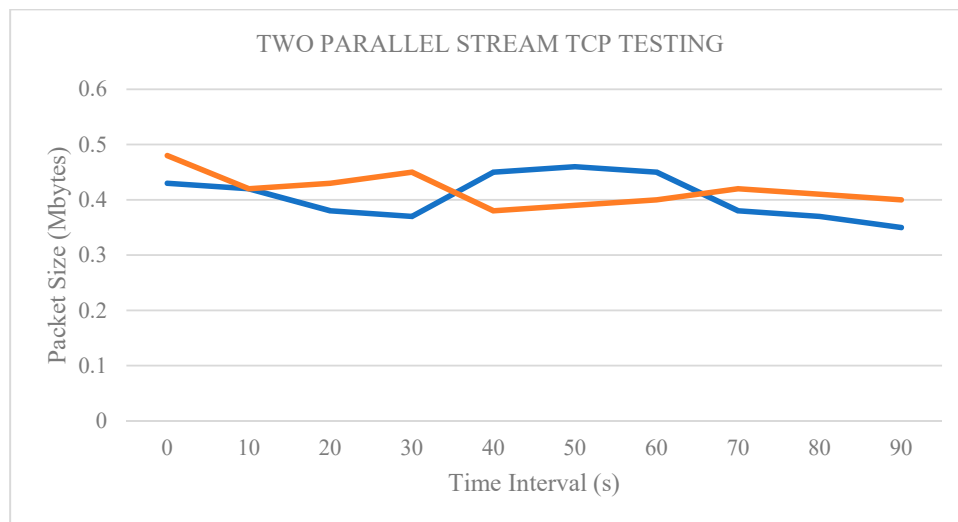


Figure 17. Packet size output of the two parallel TCPs after technique policing.

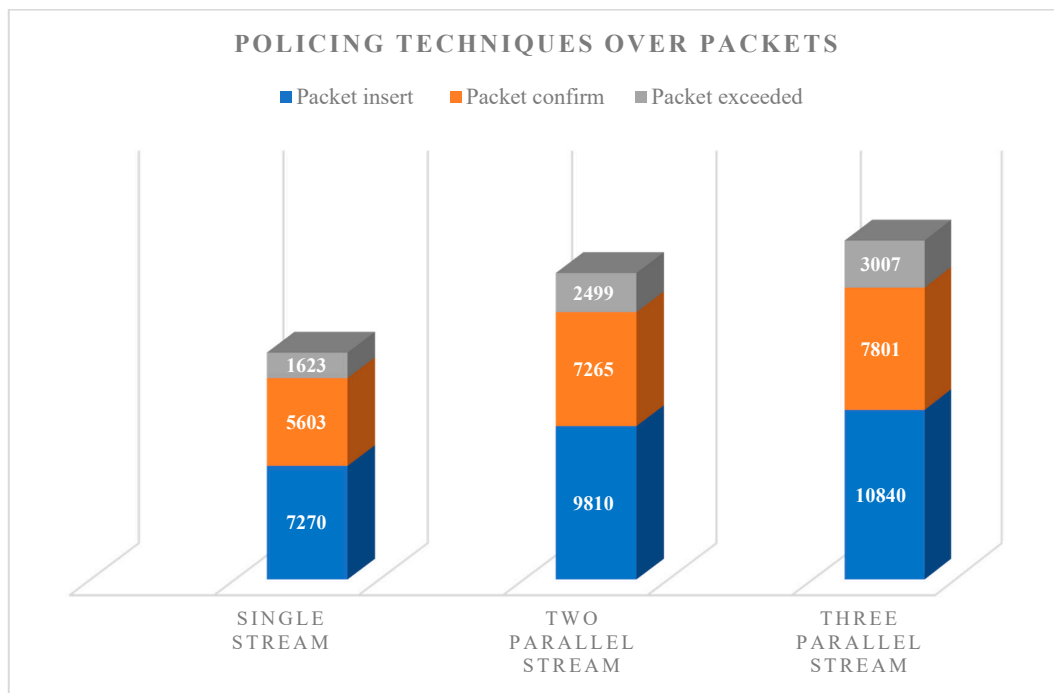


Figure 18. TCP packet filtering after traffic policing.

5. Conclusions

This study presents the functionality of QoS with traffic policing in overcoming network congestion. End users indicated that the networks have always been intermittent and congested during peak hours. Positive outcomes have been obtained during the implementation of QoS in the testbed. QoS not only resolves network congestion, but also stabilizes the LAN. Furthermore, CROS was added on the configuration, which allowed the network to achieve high performance utilization.

Author Contributions: Data curation, W.M.H.A.; formal analysis, A.S.A.-K.; funding acquisition, R.H. and A.H.M.A.; methodology, W.M.H.A.; project administration, W.M.H.A. and R.H.; resources, W.M.H.A., and A.S.A.-K.; software, A.S.A.-K.; supervision, R.H. and A.H.M.A.; visualization, W.M.H.A. and M.K.H.; writing – original draft, W.M.H.A.; writing – review and editing, R.H., A.H.M.A., M.K.H., and A.S.A.-K. All authors have read and agreed to the published version of the manuscript.

Funding: The research was funded by Universiti Kebangsaan Malaysia under grant code FRGS/1/2018/TK04/UKM/02/07 and GGPM-2019-030. The research is conducting at Network and Communication Technology Laboratory (NCT), Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM).

Conflicts of Interest: The authors declare no conflict of interest regarding this paper.

References

1. Dey, P.K.; Canbaz, M.A.; Yuksel, M.; Gunes, M.H. On correlating ISP topologies to their businesses. In Proceedings of the IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–7.
2. Marcon, M.; Dischinger, M.; Gummadi, K.P.; Vahdat, A. The local and global effects of traffic shaping in the internet. In Proceedings of the Third International Conference on Communication Systems and Networks (COMSNETS 2011), Bangalore, India, 4–8 January 2011; pp. 1–10.
3. AL-Khaleefa, A.S.; Ahmad, M.R.; Muniyandi, R.C.; Malik, R.F.; Isa, A.A.M. Optimized authentication for wireless body area network. *J. Telecommun. Electron. Comput. Eng.* **2018**, *10*, 137–142.
4. Jubair, M.A.; Mostafa, S.A.; Muniyandi, R.C.; Mahdin, H.; Mustapha, A.; Hassan, M.H.; Mahmoud, M.; Al-Jawhar, Y.; Salih, A.; Mahmood, A. Bat optimized link state routing protocol for energy-aware mobile ad-hoc networks. *Symmetry* **2019**, *11*, 1409. [[CrossRef](#)]

5. Bolla, R.; Carrega, A.; Repetto, M.; Robino, G. Improving efficiency of edge computing infrastructures through orchestration models †. *Computers* **2018**, *7*, 36. [[CrossRef](#)]
6. Zakariyya, I.; A Rahman, M.N. Bandwidth guarantee using Class Based Weighted Fair Queue (CBWFQ) scheduling algorithm. *Int. J. Digit. Inf. Wirel. Commun.* **2015**, *5*, 152–157. [[CrossRef](#)]
7. Kassim, M.; Ismail, M.; Yusof, M.I. A new adaptive throughput policy algorithm on campus ip-based network internet traffic. *J. Theor. Appl. Inf. Technol.* **2015**, *71*, 205–214.
8. Slavata, O.; Holub, J. Impact of the codec and various QoS methods on the final quality of the transferred voice in an IP network. *J. Phys. Conf. Ser.* **2015**, *588*, 012011. [[CrossRef](#)]
9. Aman, A.H.M.; Hassan, R.; Hashim, A.-H.A.; Ramli, H.A.M. Investigation of internet of things handover process for information centric networking and proxy mobile internet protocol. *Res. J. Eng. Technol.* **2019**, *38*, 867–874. [[CrossRef](#)]
10. Ahmed, A.S.; Hassan, R.; Othman, N.E.; Ahmad, N.I.; Kenish, Y. Impacts evaluation of DoS attacks over ipv6 neighbor discovery protocol. *J. Comput. Sci.* **2019**, *15*, 702–727. [[CrossRef](#)]
11. Amato, F.; Moscato, V.; Picariello, A.; Sperli, G. Recommendation in social media networks. In Proceedings of the IEEE Third International Conference on Multimedia Big Data (BigMM), Laguna Hills, CA, USA, 19–21 April 2017; pp. 213–216.
12. Amato, F.; Castiglione, A.; Mercurio, F.; Mezzanzanica, M.; Moscato, V.; Picariello, A.; Sperli, G. Multimedia story creation on social networks. *Future Gener. Comput. Syst.* **2018**, *86*, 412–420. [[CrossRef](#)]
13. Ali, Z.; Aman, A.H.B.M.; Hassan, R. Cloud Query Processing Analysis: Encryption and Decryption. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Special Issue* **2019**, 65–75. [[CrossRef](#)]
14. Mojib, G.; Aman, A.H.M.; Khalaf, M.; Hassan, R. Simulation Analysis for QoS in Internet of Things Wireless Network. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Special Issue* **2019**, 77–83. [[CrossRef](#)]
15. Kaur, S. Implementation of differential services based on priority, token bucket, round robin algorithms. *Int. J. Comput. Sci. Mob. Comput.* **2015**, *4*, 810–818.
16. AL-Khaleefa, A.S.; Ahmad, M.R.; Isa, A.A.M.; AL-Saffar, A.; Esa, M.R.M.; Malik, R.F. MFA-OSELM Algorithm for WiFi-Based Indoor Positioning System. *Information* **2019**, *10*, 146. [[CrossRef](#)]
17. AL-Saiagh, W.; Tiun, S.; AL-Saffar, A.; Awang, S.; Al-khaleefa, A.S. Word sense disambiguation using hybrid swarm intelligence approach. *PLoS ONE* **2018**, *13*, e0208695. [[CrossRef](#)] [[PubMed](#)]
18. AL-Khaleefa, A.S.; Ahmad, M.R.; Isa, A.A.M.; Esa, M.R.M.; Aljeroudi, Y.; Jubair, M.A.; Malik, R.F. Knowledge Preserving OSELM Model for Wi-Fi-Based Indoor Localization. *Sensors* **2019**, *19*, 2397. [[CrossRef](#)] [[PubMed](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).