Penerbit
Akademia Baru

Enhancement Quality of Service at ADTECBP LAN Using Traffic Policing

W. M. H. Ahmad Azamuddin[*], *Z. A. M. Noh, A. S. H. Basari and A. S. H. Shibghatullah*

Department of Computer System and Communication, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, 76100 Durian Tunggal Melaka, Malaysia.

[*]*hazwan@jtm.gov.my*

Abstract – *Internet service provider (ISP) provides best-effort service to all customers that subscribe to it and Quality of Service (QoS) is only given by provider if it being request. While traffic become congested, initial setting of configuration doesn't resolve this issue. Current trending on network nowadays with convergence of data, voice and video it is important for network to administrator to classify the traffic by using QoS mechanism. In applying differentiated QoS, router will classify and remarked the traffic to utilize the network. Regarding the Service Level Agreement (SLA), classification the traffic will make router to use more resources. Outcome from the result is very important by implementing these methods by using for network system administration, network engineer and others. In order study effectiveness by applying QoS on network, appropriate methodology need to be applied. Objective for this setup is to categorize network performance metrics such as throughput, jitter and packet loss based on multiple traffic accessing the router. Remarking and classify traffic will make router will do more work. Certain devices, performance become dropped when enabling this method. Another method is by make combination of classification, remarking and apply traffic policing. This method will deteriorate throughput at the egress router. Other than that, jitter and packet loss also will be increased by implementing traffic policing. Jitter, throughput and packet loss will be measured by using network performance tools such as IPERF. Regarding from previous review of literature, ISP or network provider need to concern about their SLA and providing service of network to avoid issue.*

Keywords: best-effort service, classification, quality of service (QoS), traffic policing

1.0 INTRODUCTION

In the emphasizing of the computer network, primary concern is send information to reach their destination. Internet Service Providers (ISP) nowadays we're more ramified in customer growth that need more demand for bandwidth to make sure the networking is running efficiently [1].

By the deployment QoS mechanism, all traffic was always fully utilizing the network than to overcome bottlenecks. Dispute resources are the factors for QoS to be expanded. IP's introductory design inclusive with the field of the Type of Service (TOS) predetermined for contributing various categories of operations. Nonetheless, it was not a preference for an ISP.

Bizarre, QoS has a small growth was the minimal factor measured as complexity of the billing. Formerly, providers charging user based on the package that they subscribe also on time usage and access size. In order to vary service plans and what customers' needs as immensely onerous, given that it administrator has to highlight into packet level prioritize.

Typically, Local Area Network (LAN) using packet data communication for providing communication that using high-bandwidth over networking media. LAN is a data communication network, typically a packet data communication network, limited in geographic scope [2].

Since, in the last two decades the technology and the technology of computing were merged from a huge resources mainframe computer with terminals into tiny more distributed resources personal computers. As the outcome, these merging resources are becoming obsolete and not fully used. On the other side, communication is becoming more useful and meaningful for all business, scientific, and other tasks. [3] The previous evolution network, the need for resource sharing and communication are not seriously important. LANs can be categorized by limitation of range, privatization usage and high speed of the network. LAN can be categorized either wired or wireless network depending on the connection.

High speed wired networks will be provided through wired networks, but due to the drawbacks like extensive cabling and immobility etc., the WLAN gained momentum. [3] Current computer networking today, they're not solely wired however wireless conjointly, looking at the variety of incidence like quality, rough terrains, or network security.

All 802.1x protocol either wireless or wired is mainly specified by LLC layer. 802.1x normal like IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring), IEEE 802.11 (WLANs) chiefly focuses between 2 layers. Our study has centered on improvement, Quality of Service (QoS) by enhance network performance on Wired and Wireless LANs by implements traffic policing technique.

QoS is outlined as activity of transmission quality and repair accessibility of an area network or internet works. Service accessibility is a major downside component of QoS. [4] So as to implement QoS, computer user ought to style the network infrastructure extremely obtainable. Main purpose to implement QoS is to succeed in High accessibility for ninety nine percentile the concerns period of time, and solely 5 minutes of time period happened annually. The standard of network transmission is determined by multiple issues like loss, delay and noise. [5] Loss chiefly will live variety of packets that have not found the destination compared to packet that has been transmitted. Loss is synchronous operate of accessibility. Once the network has been rated as extremely obtainable on non-congestion amount, loss is calculated primarily to zero. Whereas on congestion amount, QoS can take a task by electing packet that extremely exacting and born packet that's not appropriate for the transmission. [6] To delay, it is determined by quantity of your time that has to reach at the receiver once been transmitted from the sender. In voice state of affairs, delay is measured from speaker mouth's travel listener's ear. Another component of QoS parameter is delay variation (jitter), is measured by packet transmission within source and destination in terms of times. Given scenario, a packet needs 50 ms to transmits to the destination while next packet needs 75 ms to form an same way transmission, then the jitter is 25 ms. Voice over IP (VoIP) transmission using a noise buffer locally to change within the arrival times of voice knowledge packets become discarded [7].

Our achievable goal will be our milestone be achieved has been set up as our objective. The objective of our project is to enforce traffic policing on a local area network (LAN) to make sure current traffic will be stabilized and been avoided from DOS attack. This project would be very useful for to make sure there are no more traffic congestion happen during on operational hour.

Specific Objective:

1) To categorized network performance such as throughput, jitter and packet loss on current network ADTEC BP LAN.
2) To propose new network design with development traffic policing for ensure better performance.
3) To analyze QoS network performance after deployment new methodology inclusive VLAN implementation.

A backbone of productivity, organization can be measured by their communication network. By using transparent on networks, all applications such as voice, video encryption of date sending to the network. To make sure network is in good performance, service warranty need to be done in order to measure delay, jitter and losses of the packets [8].

QoS technologies can be applied by using a variety of tools and techniques, hardware and software to monitor network performance and technology of network convergence. The main objective of deploying QoS is to make sure data, video and voice quality convergence receive to end users clearly. The other advantageous using QoS is they may different any kind of traffic based on their class of services. [9] For higher priority packet such as video, voice and importance information applications will be processed first rather than traffic or packet that has lower priority. So that, QoS technology was an important technique, to make sure our network totally convergence.

QoS tools don't seem to be solely helpful in protective fascinating traffic, however conjointly in unmanageable congestion and misconfigured queuing discipline will propagate for DOS attack and worms. By using QoS all of these threats can be observed, monitored and discarded [10].

2.0 METHODOLOGY

In phase 1, establishing objective and methods to develop this project to deliver expected result accordance to technique that will be employed such as traffic policing. The target has been set after data gathering and information collection has been culled from user that using ADTECBP LAN. Other than that, reviewing previous literature that have the same concept and methodology will be benchmarked and some of amendment been applied to get this project objective will be reached. In that respect are three goals to be achieved to fulfil this project that has been stated in Research Objective.

In phase 2, by doing this project and applied a suitable method that has been chosen from phase 1. A testbed setup has been made from the current initial network and upgrade to appropriate network design, including VLAN implementation and traffic policing as a case control mechanism.

In phase 3, comparison result with expected that has been learned from the literature will be dissected. Data that will pile up from different case and scenario will be compared and chosen as the best solution. Two cases will be compared in this testbed by using the transport layer protocol as variants such as TCP and UDP protocol. This protocol will be tested in multiple stream to measure their network performance along the egress router.

In phase 4, after completing the experiment output will be gathered to be measured as network performance parameter. This testbed will specially make a comparison between throughput, delay and jitter based on application layer testing with multiple stream

2.1 Categorization QoS mechanism

Thither are many techniques to categorize QoS parameter. Either can use software or hardware based. In order to categorize QoS mechanism is we should bare aspect they will react to our network performance such as differentiation, classification, admission control, remarking and queuing. While doing above techniques such as admission control, packet can be marked on the router either can be dropped or discard after policy has been set up on it. Previous years ago data just only submitted on their channel only, then there no issues with quality of service. Nowadays, data to be sent required more bandwidth and need to be kept. That's means QoS need to be carried out either using queuing discipline or classification. When transmission of packet happens on the network, the response time could occur because of the time taken to arrive at ingress router. Throughput of the packet may be varied regarding of classification has been merged with queuing discipline. Throughput can be specified as the transmission from ingress to egress router and how long time taken to process the data. Another parameter that can be found is jitter or knows as a variation of delay. Jitter happen when there is different on packet latency.

The foremost measure is needed to measure all of this parameter on current network at the ADTEC BP network. Below is the current network diagram at ADTEC Batu Pahat.

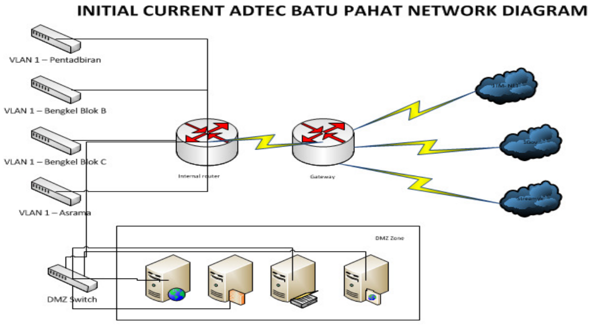


Figure 1: Initial Current ADTEC BP Network Diagram.

2.2 Testbed Setup

In this project sooner rather than using classification and remarking, another parameter that needs to see the effect on the QoS parameter is traffic policy configuration. Three tests need to be made for make comparison effectiveness of QoS.

2.2.1 Test 1: No classification and no policy applied

In this testing, all packet data while using FIFO queuing discipline and will flow without any restriction of policy. This testing will baseline for other testing. All the traffic flow will pass without any classification and policy applied.

2.2.2 Test 2: Classification and no policy apply applied

A packet that has arrived at ingress router will be classify and categorize on their own service class. After the packet has been grouped in class, complexity thing is to differentiate each packet. Streaming of this class will be specified them in higher priority packets. This test have just only merely have single stream to transmit. The main targets not in the streaming packet, but its only focus on classifying the packet.

2.2.3 Test 3: Classification and policy applied

In this test packet that arrive at ingress router will be classify and categorize to make sure each packet in group of service class will deliver their own DSCP value. Remarking process will happen at gateway router or an egress network node.

Packet transmission will have their own ToS values, so that after the packet has been remarked, it's easy for the packet to enter neighbouring router based on an agreement that has been achieved on both routers. Subsequently getting into egress router, a packet will be remarked with using information on the agreement.

3.0 TESTBED IMPLEMENTATION

From actual setup on ADTEC BP LAN, they use a default setting without applying any rules or policing mechanism to filter traffic. So we will upgrade the networking topology by enhancement certain rules to meet our objective.

Equipment that will be implemented on this testbed is:

Table 1: List Equipment applied in the testbed

No	Item	Model	Number of units
1	Router	Cisco 2911 Integrated Services Router	2
2	Router	Cisco 3600 Series Multifunction Platforms (3620 and 3640/3640A)	2
3	Switch	Cisco Catalyst 3560 Series Switches	1
4	VoIP Phone	Cisco Unified IP Phone 7940G	2
5	IP Communicator	Cisco IP Communicator	2

3.1 Experimental Setup

Aspects to be highlighted in this setup are queueing that will give big contribution on having best QoS solution. Priority traffic will have different queues to have effect of prioritization. In order to have traffic in specific queue, firstly need to classify the traffic. Basic function if classification has been made on packet when the router has enabled the QoS services. After classify has been made, the packet will be remarked. By doing this, There will be application layer testing to measure their performance on the network. The testing that will be made is TCP and UDP test. Each test will be based on 3 cases and each case will have a variety of streams to differentiate their outcome.

3.3.1 Case 1: No classification and no policy applied

In this case, multiple stream TCP connection will be tested to measure each network performance result. The test will start will start with single stream TCP test, continue with multiple stream, then triple stream and last test by using fourth stream. Variety of stream to be tested for checking the consistency of network will be maintained successfully.

For UDP testing, multiple stream also being tested to measure the network performance. But other technique has been set as parameter in UDP testing, variety of stream has being used. Bandwidth also has been set as varies for each stream. For example, for application UDP testing for 1.0 Mb bandwidth, there will have four testing inclusive 1 parallel stream, 2 parallel stream, 3 parallel stream and last but not least 4 parallel stream.

Table 2: Experimental testing on Case 1

Experimental Testing	**Bandwidth**	**Parallel Stream**	**Transmission**	**Interval per packet**	**Classification and remarking applied**	**Policy applied**
TCP	1.0 Mbps	1 2 3 4	100 s	1s	No	No
UDP	1.0 Mbps	1 2 3 4	100 s	1s	No	No
	2.0 Mbps	1 2 3 4	100 s	1s	No	No
	3.0 Mbps	1 2 3 4	100 s	1s	No	No
	4.0 Mbps	1 2 3 4	100 s	1s	No	No

3.3.2 Case 2: Classification and no policy applied

In this setup, TCP and UDP traffic packet is bent transmitted from client to be analysed on the router by using certain configuration. Classification of each packet has been done on cisco router 2911. As an example, router will look into packet a categorize them by class-map that has been defined on router configuration. This will make router work on extra basis per packet. To create a class of traffic, firstly is to different the packet either it TCP or UDP. This process in router can be done by applying rules by using access-list command to differentiate packet per basis. On this testbed, multiple of stream has been made to see when classify has been made, how it will affect the network performance. Extra work to made by enable multiple stream by enabling classification. For this classification, only TCP packet classification has been made such as HTTP and ICMP to check their outcome on network.

3.3.3 Case 3: Classification and policy applied

In this testbed, multiple stream of TCP or UDP packet has been transmitted to check either it meets the SLA agreement or not. This case will apply traffic policing on cisco router 2911. If the packet either TCP or UDP meet the rules or policing, the packet will be accepted otherwise the packet will be drop. This test has set 1.0 Mbps as the Committed Information Rate (CIR) value for 1Mbps for usage for data only. Table 3 show that experiment that will setup on this case 2.

Table 3: Experimental on Case 2

Experimenta l Testing	Bandwidth	Parallel Stream	Transmission	Interval per packet	Classification and remarking applied	Policy applied
TCP	1.0 Mbps	1 2 3 4	100 s	1s	Yes	Yes
UDP	1.0 Mbps	1 2 3 4	100 s	1s	Yes	Yes
	2.0 Mbps	1 2 3 4	100 s	1s	Yes	Yes
	3.0 Mbps	1 2 3 4	100 s	1s	Yes	Yes
	4.0 Mbps	1 2 3 4	100 s	1s	Yes	Yes

Table 4: Four parallel stream TCP testing

Interval (sec)	Stream 1 (Mbytes)	Stream 2 (Mbytes)	Stream 3 (Mbytes)	Stream 4 (Mbytes)	Band1 (Mbps)	Band2 (Mbps)	Band3 (Mbps)	Band4 (Mbps)
0.0 - 10 .0	27.50	28.00	28.30	28.30	23.50	23.40	23.70	23.70
10.0 - 20.0	27.30	28.00	28.50	28.50	23.50	23.50	23.80	23.80
20.0 - 30.0	27.40	28.20	28.40	28.40	23.40	23.60	23.90	23.90
30.0 - 40.0	27.60	28.20	28.20	28.20	23.60	23.40	23.40	23.40
40.0 - 50.0	27.50	28.40	28.40	28.40	23.50	23.60	23.80	23.80
50.0 - 60.0	27.50	27.90	28.30	28.30	23.40	23.40	23.40	23.40
60.0 - 70.0	27.60	27.60	28.20	28.20	23.60	23.30	23.90	23.90
70.0 - 80.0	27.50	28.30	28.40	28.40	23.20	23.10	23.40	23.40
80.0 - 90.0	27.40	28.30	28.20	28.20	23.50	23.50	23.50	23.50
90.0 - 100	27.70	28.10	28.10	28.10	23.10	23.60	23.70	23.70
0.0 - 100.0	275.00	281.00	283.00	283.00	23.10	23.60	23.70	23.70
Total		1122.00				94.10		

4.0 RESULTS

Table 4 shows that four parallel stream simultaneously run on TCP test to measure the performance. From the graph, its stated transmission of TCP protocol has their own value. When use four parallel streams, each stream will have their own bandwidth transmission. For stream one in have transmit at most 2380 packets while for stream two have transmit 2420 packets, third stream have transmitted 2440 packets and last stream transmit 2460 packets.

So for summary we can see that from this case without any marking, classification and policing being applied, the more streams we sent on the network, the more bandwidth has been utilized. But for combination of transmission stream such as 2 parallel streams, they will share the bandwidth to transmit packet along the networks.

Table 5: Four parallel stream (4.0 Mbytes)

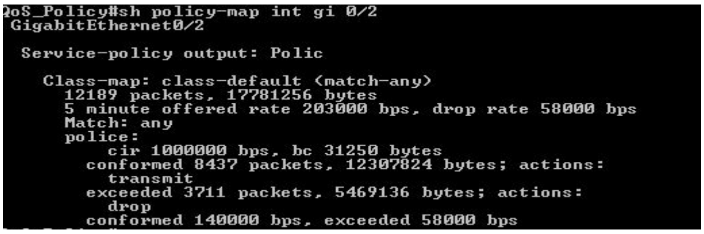
Interval (s)	Transfer (Mbytes)	Bandwidth (Mbps)	Jitter (ms)	% Loss
0.0 - 1.0	0.48	3.99	2.924	0 %
1.0 - 2.0	0.48	4.00	0.011	0 %
2.0 - 3.0	0.48	4.06	0.000	0 %
3.0 - 4.0	0.48	3.99	0.008	0 %
4.0 - 5.0	0.48	3.96	0.000	0 %
5.0 - 6.0	0.48	3.99	0.000	0 %
6.0 - 7.0	0.48	4.00	0.000	0 %
7.0 - 8.0	0.48	4.00	0.000	0 %
8.0 - 9.0	0.48	3.99	0.000	0 %
9.0 - 10.0	0.48	4.00	0.000	0 %
0.0 - 10.0	4.80	4.00	0.000	0.088 %

Table 6 shows that when make an UDP test for four parallel stream of 4.80 Mbytes, the bandwidth usage also use for 4.0 Mbps. Jitter occurs at t=1 (2.924 ms), t=2 (0.011 ms), t=4 (0.008 ms), and total jitter is 0.000 ms. Average percentage for packet loss is 0.088%.

Table 6: Four parallel streams implementation

Interval (sec)	Stream 1 (Mbytes)	Stream 2 (Mbytes)	Stream 3 (Mbytes)	Stream 4 (Mbytes)	Band1 (Mbps)	Band2 (Mbps)	Band3 (Mbps)	Band4 (Mbps)
0.0 - 10 .0	0.40	0.20	0.40	0.60	0.22	0.20	0.21	0.22
10.0 - 20.0	0.30	0.30	0.20	0.20	0.21	0.22	0.20	0.21
20.0 - 30.0	0.33	0.42	0.24	0.20	0.20	0.23	0.26	0.20
30.0 - 40.0	0.20	0.40	0.22	0.23	0.23	0.25	0.23	0.23
40.0 - 50.0	0.20	0.30	0.42	0.30	0.22	0.24	0.25	0.22
50.0 - 60.0	0.50	0.20	0.30	0.20	0.21	0.23	0.24	0.21
60.0 - 70.0	0.20	0.40	0.20	0.30	0.22	0.22	0.21	0.22
70.0 - 80.0	0.30	0.30	0.10	0.30	0.23	0.26	0.20	0.23
80.0 - 90.0	0.10	0.10	0.20	0.20	0.25	0.24	0.23	0.25
90.0 - 100	0.20	0.30	0.20	0.20	0.22	0.23	0.20	0.22
0.0 - 100.0	2.73	2.92	2.48	2.73	0.23	0.24	0.21	0.23
Total		10.86				0.91		

Table 6 shows that's each stream has drop issue occur but they have their own value for transmission. Total TCP packet has been transferred using 0.91 Mbps. Total TCP packet that has been transferred in four parallel stream is 10.86 Mbytes and bandwidth utilization is 0.91 Mbps.



```
QoS_Policy#sh policy-map int gi 0/2
 GigabitEthernet0/2

  Service-policy output: Polic

    Class-map: class-default (match-any)
      12189 packets, 17781256 bytes
      5 minute offered rate 203000 bps, drop rate 58000 bps
      Match: any
      police:
          cir 1000000 bps, bc 31250 bytes
        conformed 8437 packets, 12307824 bytes; actions:
          transmit
        exceeded 3711 packets, 5469136 bytes; actions:
          drop
        conformed 140000 bps, exceeded 58000 bps
```

Figure 2: Packet drops statistics on 4 parallel streams

Table 7: Four parallel streams UDP (4.0 Mbps)

Interval (s)	Transfer (Mbytes)	Bandwidth (Mbps)	Jitter (ms)	% Loss
0.0 - 1.0	0.03	0.28	0.974	0 %
1.0 - 2.0	0.04	0.32	0.171	92 %
2.0 - 3.0	0.03	0.26	0.041	94 %
3.0 - 4.0	0.04	0.32	0.998	92 %
4.0 - 5.0	0.03	0.24	0.275	94 %
5.0 - 6.0	0.04	0.32	0.048	92%
6.0 - 7.0	0.03	0.24	0.098	94%
7.0 - 8.0	0.04	0.31	5.255	92 %
8.0 - 9.0	0.04	0.31	7.622	92 %
9.0 - 10.0	0.03	0.25	7.476	94 %
0.0 - 10.0	0.35	0.28	23.583	93 %

Table 7 shows that when make an UDP test for 4 parallel stream of 0.35 Mbytes, the bandwidth drop to 0.28 Mbps because of policy-map applied. Total jitter for this transmission is 23.583 ms. Average percentage for packet loss is 93 %, so this the highest jitter from other cases.

4.1 Throughput test based on TCP

By using multiple streams of testing, bandwidth allocation for each stream allocated for 100 Mbps for transmission internal. For case 1, throughput for single steam allocated for 50 Mbps, for 2 parallel streams for 46 Mbps each, 3 parallel streams for 33 Mbps each and for 4 parallel streams is 23 Mbps each. So we conclude that for transmission bandwidth will divide equally to each stream to make them transmit successfully. While for comparison after applying policy-map and class-map on case 4, there are major impacts on network performance. By applying CIR 1.0 Mbps at egress router, throughput for single stream just reach 0.60 Mbps, for 2 parallel streams reach 0.39 Mbps each, for 3 parallel streams reach 0.29 Mbps each and for 4 parallel streams reach 0.23 Mbps each. Case 4 has to limit their bandwidth because network always congested and after applying this policy it's become more smooth and convenient.

4.2 Throughput test based on UDP

For this testing, variety of bandwidth per stream for each transmission has been set to measure the jitter and packet loss. For case 2, without applying any policy-map one UDP packet transfer 1.0 Mbps, throughput also remains 1Mbps. And the bet result is no jitter and packet loss occur in this scenario. Same result happen in case with bandwidth 2.0 Mbps, 3.0 Mbps and 4.0 Mbps. After applying class-map and policy on case 5, result changes immediately. While growing bandwidth tremendously, jitter of UDP packet increase highly and also the packet loss. So conclusion can be made, traffic policing is not suitable for UDP communication such as VoIP conference but highly applicable on TCP traffic implementation.

5.0 CONCLUSION

Network congestion always raise issued from client that always have intermittent connection to internet and the worst thing request to the network has been time out. Many possible factors that will make the network become congested. Alternative has been made in order to reduce this networking issue.

QoS is our approach to overcome this problem. In order to apply QoS, there are two method can be deployed, traffic policing and traffic shaping. We proposed to apply traffic policing methodology to be implemented on the current network infrastructure. Other than that, segmented the network also will reduce network traffic issue, by controlling the broadcast domain. Appling VLAN is the best solution.

5.1 Multiple bandwidth for TCP testing

Experimental has been tested with multiple streams but have single constant bandwidth. The bandwidth is pre-defined based on interface of network card that has been used that support up to 100 Mbps. So if variety of bandwidth can be tested, the result of throughput may differ from each case. Result also may vary their queuing scheme that be implemented on device. Besides of that network performance can be compared clearly.

5.2 Multiple classification and remarking

Current setup just monitors HTTP and ICMP traffic, while UDP is testing based on VoIP implementation. Maybe other traffic such as DNS, FTP and other security services can be classified and remark to check their performance while applying QoS.

5.3 Study of other aspect QoS

Other QoS criteria such as queuing and congestion management can be type of study on next topic to be implemented. Implementation congestion management technique will compare with this setup. It’s also important to know that queuing play active role in congestion management.

5.4 Applying QoE on testing

Quality of Experience (QoE) is a testing to measure the satisfaction of end user on using the network services such as web browsing, video conferencing and TV broadcast. While QoS implemented on network to measure the performance, QoE can be derive from user perspective.

REFERENCES

[1] Ratha, B. "Local Area Network" 2002.

[2] Bansal, R. K., Vikas Gupta, and Rahul Malhotra. "Performance analysis of wired and

wireless lan using soft computing techniques-a review." Global Journal of Computer Science and Technology 10, no. 8 (2010).

[3] Kassim, Murizah, Mahamod Ismail, and Mat Ikram Yusof. "A NEW ADAPTIVE THROUGHPUT POLICY ALGORITHM ON CAMPUS IP-BASED NETWORK INTERNET TRAFFIC." Journal of Theoretical & Applied Information Technology 71, no. 2 (2015).

[4] Zakariyya, Idris, and M. Nordin A. Rahman. "Bandwidth Guarantee using Class Based Weighted Fair Queue (CBWFQ) Scheduling Algorithm."International Journal of Digital Information and Wireless Communication (IJDIWC) 5, no. 3: 152-157.

[5] Kaur, Satinder, and Gurpreet Singh. "Implementation of Differential Services Based on Priority, Token Bucket, Round Robin Algorithms." (2015).

[6] Slavata, Oldřich, and Jan Holub. "Impact of the codec and various QoS methods on the final quality of the transferred voice in an IP network." InJournal of Physics: Conference Series, vol. 588, no. 1, p. 012011. IOP Publishing, 2015.

[7] Rani, Monu, and V. K. Pandey. "Study of Analysis and Controlling Network Management System." International Journal 3, no. 4 (2015).

[8] Song, Qingyang, and Abbas Jamalipour. "Network selection in an integrated wireless LAN and UMTS environment using mathematical modeling and computing techniques." IEEE wireless communications 12, no. 3 (2005): 42-48.

[9] Jung, Bokrae, JungYul Choi, Young-Tae Han, Min-Gon Kim, and Minho Kang. "Centralized scheduling mechanism for enhanced end-to-end delay and QoS support in integrated architecture of EPON and WiMAX." Journal of Lightwave Technology 28, no. 16 (2010): 2277-2288.

[10] Li, Frank Yong, and Norvald Stol. "QoS provisioning using traffic shaping and policing in 3rd-generation wireless networks." In Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE, vol. 1, pp. 139-143. IEEE, 2002.