INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2025, VOL. 71, NO. 1, PP. 285–292
Manuscript received August 10, 2024; revised March, 2025. doi:10.24425/ijet.2025.153572

Differentiated service quality analysis based on QoS traffic prioritisation

Dariusz Strzęciwilk

***Abstract*—This paper presents the results of a transmission quality study in a network with a DiffServ architecture. The impact of differentiated services based on traffic prioritisation was studied. A carrier network model in a differentiated services architecture with traffic prioritisation was designed and tested. The operator network used the OSPF protocol, while the client networks communicated using the EIGRP protocol. Different traffic classes in the queueing systems were studied, influencing delay and delay variation. Traffic generated with Exfo FTB-860 test equipment was introduced into the designed network. The measurement equipment used supported the ITUT Y.1564 measurement methodologies. The transmission quality was tested according to the EtherSAM methodology and carried out in bidirectional mode. The tests carried out showed the influence of different data lengths on the quality of transmission in the test network. The results proved that the correct implementation of QoS mechanisms in the network makes it possible to ensure the required quality of service. It was shown that for delay-sensitive traffic which fluctuates beyond its nominal speed, queuing systems allow transmission quality to be achieved with guaranteed bandwidth and delay.**

***Keywords*—DiffServ, Quality of Service, transmission quality, QoS, ITU-T methodology Y.1564, EtherSAM**

I. Introduction

TODAY'S packet-based Internet now provides many complex services and technologies that have revolutionised telecommunications systems. Examples include VoIP (*Voice over IP*) telephony [1], IPTV (*Internet Protocol Television*) [2], video conferencing, P2P exchange of files containing multimedia content, VoD (*Video on Demand*) [3] and IoT (*Internet of Things*) [4] technologies. The benefits of using these technologies are manifold. According to the authors [5], if VoIP technology is applied to improve organisational communication, it can impact the business environment. Effective communication in collaboration with employee satisfaction is a prerequisite for improving organisational performance. On the other hand, research by Yang et al. [6], points to the benefits of using IoT technology to manage emergencies such as fires, floods, earthquakes, terrorist attacks, etc. However, such emergencies require immediate access to real-time information so that appropriate decisions can be taken. The technologies above are, however, susceptible to delays and latency variability. Therefore, the QoS (*Quality of Service*) requirements for modern operator networks providing such services are stringent, as a drop in transmission quality is immediately perceived by the end user. Hence, in order to implement an operator network with a full QoS guarantee, the data transmission technologies used must be thoroughly investigated. QoS transmission and security mechanisms are among the most important challenges arising during the design and maintenance of modern computer networks and NG (*Next-Genaration*) networks [7], [8]. Guaranteeing adequate quality of service is particularly important for real-time applications, as these services are particularly delay-sensitive and require guaranteed bandwidth [9]. Today's IP networks are based on BE (*Best Effort*) services, where queuing of traffic and lack of QoS control can cause packet loss, delay and increased delay variation (jitter). A network architecture based on BE services needs to be enriched with mechanisms that guarantee QoS in particular for real-time applications. Hence, the aim of this study was to analyse the impact of data transmission quality in networks with DiffServ differentiated service architecture on traffic prioritisation. An analysis was made of the impact of QoS in the provider network for different DiffServ aggregates. In addition, available QoS methods for data transmission were analysed, and a corporate backbone network was designed and tested. Data streams belonging to the VoIP class, the business class requiring traffic prioritisation and the BE default class were studied.

D. Strzęciwilk is with Institute of Information Technology, University of Life Sciences, Warsaw, Poland (e-mail: dariusz_strzeciwilk@sggw.pl).

II. QoS specification

QoS (*Quality of Service*) is a set of parameters and mechanisms that allow the management and control of the quality of data transmission in communication networks. QoS makes it possible to ensure that the parameters for a given service are as constant as possible. Data packets transmitted over IP networks are subject to certain transmission problems, such as packet delay, packet delay variation (jitter) or packet loss. Hence, the provision of desirable QoS parameters for packets along the entire path from sender to receiver is the subject of much research [10], [11]. Many studies and projects have been conducted in the area of QoS performance, computer network modelling, and simulation and verification [12], [13]. However, the analysis and results of the work in this area show that this is not a simple task. To ensure an adequate level of service, QoS technology shapes and limits bandwidth to ensure fair access to network resources. Depending on the service requirements, it prioritises packets and manages their

delay. Today's QoS architectures on the Internet include a variety of mechanisms and protocols to manage the quality of service in networks. However, it is important to note that supporting end-to-end QoS in existing network architectures is an ongoing problem [14]. Since the core of Internet is owned and managed by a number of different providers of the network services, Internet's behaviour is much more unpredictable than in the case of single owner networks. At the current stage of research by the IETF on QoS architectures in IP networks, two architectures have been defined that allow traffic to be divided into classes with varying quality of service. The first class is IntServ (*Integrated Services*) which is described in RFC 1633 [15] and the second class is DiffServ (*Differentiated Services*) described in RFC 2475 [16]. These architectures allow extending the default BE (*Best Effort*) model [17] that is used in the current Internet.

III. Best-effort model

The BE (*Best Effort*) service model is widely used in public Internet networks. The service delivery model of the Internet based on the BE architecture cannot handle all services, especially critical and real-time services. The BE service model is a simple and essential quality of service (QoS) model for IP networks. Under this model, the network tries to transfer data between devices with the maximum performance and bandwidth available at any given time. However, it does not guarantee any particular QoS parameters or priorities for different types of traffic. The main features of the BE service model include:

- No guarantee of quality of service: In the BE model, there is no guarantee of delay, throughput, packet loss or other quality parameters,
- Availability of maximum bandwidth: The network tries to transmit data with the maximum bandwidth available (during periods of congestion, the network may be more heavily loaded),
- Non-recoverable packet loss: In the BE model, if a packet is lost due to congestion or other network problems, it is not retransmitted, it is lost forever,
- Delay and jitter: Delay and jitter in a BE network can be unstable and challenging to predict,
- Lack of prioritisation: There are no traffic prioritisation mechanisms in the BE model. All packets are treated equally. The BE model may not be sufficient for applications that require quality.

The BE model may not be sufficient for applications that require quality of service guarantees or low latency. The Best Effort model is the dominant model in all IP networks connecting to the largest network such as the Internet. In the Best Effort service model, there is no guarantee of reliability, throughput, and delay. It uses FIFO (*First-In-First Out*) as queuing scheduling (See Fig. 1.).

If the packet arrival process exceeds the ability to handle packets immediately, a queue is created. FIFO queuing does not work well in terms of providing good quality of service for data transmission, because when packets come from different traffic streams, then an aggressive stream can easily disrupt the flow in other streams. Processing packets in the order in which they arrive means that an aggressive stream can hijack more of the router's queue capacity. In fact, FIFO does not consider the QoS parameters of each packet, it just sends the packets according to the order of their arrival time. The result can be a sudden increase in latency or loss of transmitted packets. Several of packet scheduling algorithms have been developed, demonstrating better memory isolation between flows [18].

Fig. 1. FIFO queuing.

IV. Integrated Services Model

The IntServ model is one of the QoS management models for IP networks. IntServ is more advanced than the BE model and seeks to provide QoS guarantees for individual data streams in IP networks. This model provides the highest possible level of service for IP packets but requires all network elements, including user applications, to be able to use the RSVP signalling protocol. This limits both the flexibility of the network and its scalability. The key features of the IntServ model are:

- Quality of Service Guarantees (*QoS Guarantees*). One of the key features of the IntServ model is the ability to provide QoS guarantees for specific data streams,
- RSVP (*Resource Reservation Protocol*): The IntServ model uses the RSVP protocol to reserve network resources for specific data streams,
- Complexity and scalability: The IntServ model is relatively complex and can be difficult to implement and manage in large networks. Each data stream requires resource reservation,
- Prioritisation: IntServ allows priorities to be set for different data streams,
- Applications requiring QoS guarantees: The IntServ model is particularly useful for applications and services that require quality of service guarantees,
- Resource reservation: In the IntServ model, each application must reserve network resources before data transmission begins,
- Implementation requires router support: To successfully implement the IntServ model, network routers must support the RSVP protocol and be capable of reserving and maintaining the state of network resources for different data streams,
- Traffic conforming to the IntServ model: The IntServ model is designed to work best when traffic conforms to resource reservation and priority requirements,
- Not widely used: The IntServ model is not widely used in public networks due to its complexity and scalability limitations.

In summary, the IntServ model aims to provide QoS guarantees in communication networks but is relatively complex

and requires resource reservation for each data stream. It is mainly used in situations where QoS guarantees are crucial, and the network is smaller and more controllable.

V. Differentiated Services Model

The DiffServ model is a more scalable and flexible model than the IntServ model and is based on packet labelling at the IP layer level. The scalability problem present in the IntServ model has been eliminated in the DiffServ architecture. The DiffServ architecture model provides the most extensive and appealing solution for QoS support in current IP networks. The handling of individual data streams takes place at the network edge, while inside the service provider's network the data streams are allocated to DiffServ aggregates. The designation of the aggregates is done using the six-bit DSCP (*Differentiated Services Code Poin*) field in the IP header (See Fig. 2.).

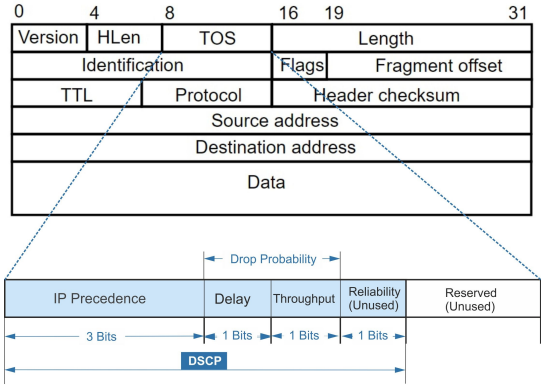

Fig. 2. DSCP field in the IP packet header [19].

The DiffServ architecture provides a means for network devices to classify traffic based on the DSCP codepoint and to map the traffic to a specific QoS forwarding treatment [20]. In the context of the Differentiated Services model, 'DiffServ aggregates' refer to the grouping or classification of traffic streams based on their QoS requirements and DSCP labels. The DiffServ field controls admission to QoS classes when the DSCPs are mapped to a BA (*Behaviour Aggregate*) [21]. This causes the packet to enter a queue served by one of a set of specified forwarding treatments, known as PHBs (*Per-Hop Behaviours*).

DiffServ aggregates are treated in an approximate or similar manner in the provider's network based on the value of the DSCP code. DiffServ aggregates allow different types of traffic to be prioritised and managed in the network, which helps to ensure a certain quality of service. Traffic is therefore divided into different groups based on the value of the DSCP code found in the headers of IP packets. Each aggregate can be assigned a specific priority or level of service, which means that packets in that group are assigned a specific way of being processed on the network. DiffServ aggregates allow quality of service to be managed more generally by grouping similar traffic streams into a single aggregate and applying appropriate PHB traffic behaviour to that group. Two basic types of PHB services are defined:

- EF PHB (*Expedited Forwarding PHB*) [22],
- AF PHB (*Assured Forwarding PHB*) [23].

Fig. 3 displays the DiffServ field and the DSCP settings for the class selector, default, AF, and EF PHBs. The DiffServ model is widely used in public Internet networks because it is more flexible and scalable than the IntServ model. DSCP allows packets to be tagged in a way that matches the requirements of applications and services, enabling effective QoS management of diverse network traffic. Using the 6-bit DSCP field, 64 classes can be defined for marking traffic. Whereby the DSCP field `000000` indicates the default packet class, which are supported by the BE forwarding model. Packets are forwarded in the order in which they are received. Packets with higher DSCP classes have a higher priority and are forwarded in other classes. The document RFC 1812 [24] specifies requirements for routers and recommendations for packet queuing disciplines.

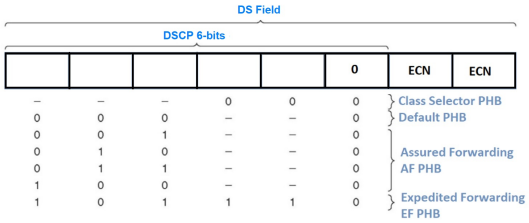

Fig. 3. DS and DSCP PHB fields.

The DiffServ model defines various PHBs or behaviours for a network node (router or switch), which determine what actions are taken against packets with specific DSCPs. The main features of DiffServ aggregates are summarised below:

- The EF PHB aggregate is often used to mark packets that require very low delay and packet loss, for example, in VoIP services. Packets in the EF aggregate are treated with the highest priority. However, the bandwidth dedicated to EF must be limited so that other classes of traffic are not 'starved'. The queue dedicated to the EF must be the highest priority queue,
- The AF PHB aggregate can include different traffic classes, with each class having a different priority. This allows the traffic behaviour to be adapted according to the application requirements. According to the standards specification, the AF PHB provides four queues for four traffic classes (AFxy): AF1y, AF2y, AF3y and AF4y. A specific bandwidth is reserved for each queue,
- The BE aggregate is labelled 'Best Effort,' meaning that the data is treated as standard traffic with no guarantee of quality of service,
- Application-specific aggregates - In some networks, there may be specific aggregates for specific applications or services, such as video conferencing, real-time streaming or Video-on-Demand.

RFC 3248 [25] defines the behaviour of the EF PHB aggregation, which specifies that, regardless of the network

conditions, the maximum packet handling time difference when passing through a network node must be limited according to the equation:

$$D_j - E_j \leq Z\frac{MTU}{R} \tag{1}$$

where:
D_j, E_j - handling times for the same packet j when the node is under traffic load and in the unloaded state,
Z - link-specific constant depending on the serial mechanisms and router configuration ,
MTU - Maximum Transmission Unit,
R - rate of EF PHB aggregate service.

DiffServ aggregators allow more efficient management of network traffic, especially for networks with heavy loads and diverse application needs. By classifying traffic and prioritising aggregates, the network can adapt its behaviour to the requirements of different types of traffic.

VI. Network topology

In order to carry out the tests, a sample ISP network supporting MPLS (*Multiprotocol Label Switching*) transmission was designed. The use of the MPLS protocol in ISP networks allows the separation of routing and traffic forwarding. The MPLS protocol is highly scalable and allows ISPs to serve large numbers of customers and manage traffic between multiple points in the network [26]. This makes it ideal for use in large and extensive ISP networks. In addition, MPLS enables traffic prioritisation at the label level. This ensures that QoS can be guaranteed for different types of traffic, such as VoIP, Video streaming, Real-time services and critical traffic. The topology of the investigated network consisting of two client locations connected to the ISP is shown schematically in Fig. 4.

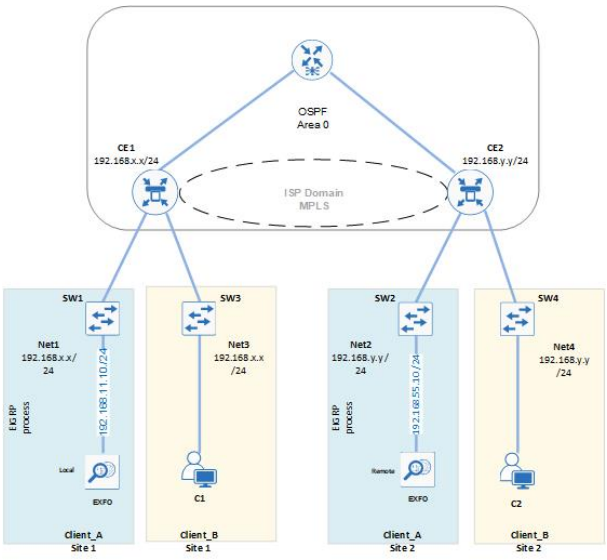

Fig. 4. Research network topology.

Cisco switches and routers were used in the studied network. The PE (*Provider Edge*) routers were connected to the client networks via CE (*Customer Edge*) devices. A hybrid routing protocol, EIGRP (*Enhanced Interior Gateway Routing Protocol*), was used on all client devices, which uses the DUAL (*Diffusing Update Algorithm*) to enable fast convergence and reduce potential routing loops. On the other hand, the single-area OSPF (*Open Shortest Path First*) protocol was used on the ISP's equipment. Customer networks with internal addresses `192.168.x.x/24`, `192.168.y.y/24` were connected to the ISP's network by sharing the EIGRP process on CE routers. On the ISP's edge nodes, redistribution of the EIGRP and OSPF protocols was enabled. In the network prepared in this way, two FTB-860 NetBlazer research testers were connected on the SW1 and SW2 client network switches to configure the tested services. For such a prepared configuration, the first test was performed without queuing enabled and without QoS mechanisms. This provided a baseline image of the network under test, which served as a reference network. Subsequently, the configuration was changed, and LLQ (*Low Latency Queue*) queuing mechanisms were added, thereby enforcing traffic prioritisation for the tested VoIP and Business classes. LLQ queueing is a QoS mechanism that allows prioritisation and low latency assurance for certain types of traffic in communication networks. This is particularly important for applications that require real-time data access, such as VoIP or videoconferencing, where low latency is crucial to quality of service. In the network under study, two traffic classes were programmed, class EF PHB and class AF PHB, with the remaining traffic assigned to the default class BE. An example of the defined traffic classes is shown in Fig. 5. To test the transmission quality, a test according to the EtherSAM methodology [27] was used, which performs SLA (*Service Level Agreement*) validation, measures jitter values, examines latency values in detail, frame loss and supports multiple traffic classes. SLA validation is the process by which it is verified that the service provider is providing the service according to the agreed terms. SLA validation is important to monitor and evaluate the quality of the services provided and to ensure that the service provider meets its obligations. Note that the EtherSAM methodology allows each test to be performed independently in both directions. Three traffic classes AF (*Assured Forwarding*), EF (*Expedited Forwarding*) and BE (*Best Effort*) were configured on the FTB-860 NetBlazer tester, which served in a further stage of the study. In addition, a service transmitting VoIP-type data using the G.729 audio codec was defined and assigned to the EF class. The business service was assigned to class AF11 and the third BE service was assigned a DSCP parameter of 0. The network thus prepared was tested and measured for transmission quality.

VII. Measurement results and discussion

To carry out the tests, two configurations of network devices were created, and measurements were made for each of them according to the EtherSAM (ITU-T Y.1564) methodology. In the first stage of testing, network measurements were performed without queuing mechanism and QoS parameters enabled. The research and testing were performed independently

```
class-map match-any EF
 match  dscp ef
 match mpls experimental topmost 5
class-map match-any AF11
 match  dscp af11
 match mpls experimental topmost 1
```

Fig. 5. Traffic classes defined.

according to Bidirectional EtherSAM methodologies for each tested service. Prior to the measurements, a local and a remote FTB-860 NetBlazer tester were configured and connected to the test network. The local tester was configured with the IP address `192.168.11.10/24` and the remote tester was configured with the fixed IP address `192.168.55.10/24`. The three test traffic aggregates EF, AF and BE were then set up on the local tester and assigned to the test services (See Table I). Tests were performed for the services to which VoIP, Business and BE services were assigned. Two different network equipment configurations were made, and transmission quality measurements were carried out using the EtherSAM methodology. The tests carried out were labelled Test 1 and Test 2, respectively. During Test 1, traffic was generated that was introduced into a network in which no QoS parameters were configured. The lack of queuing mechanisms in the MPLS domain meant that all traffic was treated as default traffic and was assigned to the BE class. The results of the measurements without active QoS mechanisms were labelled as Test 1 in the graphs.

TABLE I
TRAFFIC CLASSES TESTED.

Service 1	Service 2	Service 3
VoIP G.729	Business	Deafult BE
Class EF	Class AF11	DSCP 0

Measurement results labelled as Test 2 were performed with quality of service mechanisms enabled in the MPLS domain. The configuration of the devices was changed so that LLQ (*Low Latency Queuing*) was added, thus enforcing traffic prioritisation for the VoIP and business classes tested. Using the `class map` and `match any` functionality, two traffic classes were set, i.e. class EF and class AF. Traffic that did not belong to the defined classes EF and AF was directed to the default class BE with a DSCP code value of 0. The results obtained during the measurements with active quality of service mechanisms were marked in the diagrams as Test 2. The test results for Test 1 and Test 2 are summarised in diagrams Fig. 6-9. This allowed a comparison of the behaviour of the baseline network and the network with active quality of service mechanisms. In addition, the diagrams use the labels L (*Local*) and R (*Remote*) indicate the direction of traffic generated by testers located in the local network and the tester located in the remote network. The L-R designation thus indicates traffic generated from the local network to the remote network, and the R-L designation refers to traffic generated by the tester located in the remote network sent to the local network. In addition, incremental load tests were carried out during the tests. Such tests were denoted by the step parameter with a step size of 1 to step 5. During such tests, the devices incrementally generated traffic. Traffic was generated in five steps: 10, 25, 50, 75, and 100 per cent of the link capacity, respectively. This made it possible to simulate real-world conditions when the link is not saturated, but its load builds up gradually until the link is saturated. The tests carried out showed that the values of the Max jitter parameter obtained for configurations without active QoS parameters (See Fig. 6) and for configurations with active QoS parameters (See Fig. 7) have different values. The test results of Service 1 (class EF), which was used to carry VoIP G.729 data, showed that this service in the test with active QoS parameters have a significantly lower value of the Max Jitter parameter. It was found that at maximum link load, the value of the Max jitter parameter was reduced from a value of 5.7 ms to 3.1 ms and from a value of 14.58 ms to 4.32 ms.

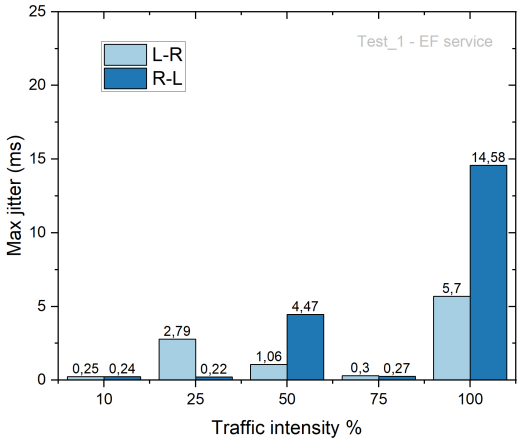

Fig. 6. Max jitter parameter for Service-1 tested under incremental load without active QoS parameters.

Similar results were observed for the service designated as Service 2 (class AF11), which was used to transmit Business data. The tests showed that as the traffic intensity parameter increases, the value of the Max Jitter parameter increases. Tests conducted for configurations without active QoS parameters showed significant fluctuations in the value of the Max jitter parameter. The highest value was observed at a link load of 75%, where the Max jitter parameter reached a value of 18.55 ms (See Fig. 8). In contrast, the results obtained in Test 2, i.e. for configurations with active QoS parameters, showed that the Max jitter parameter for Service 2 (class AF11), reached a maximum value of 4.84 ms at a link load of 100 % (See Fig. 9).

A change in the value of the Max Jitter parameter was also observed for the last Service 3 service, i.e. for the default class

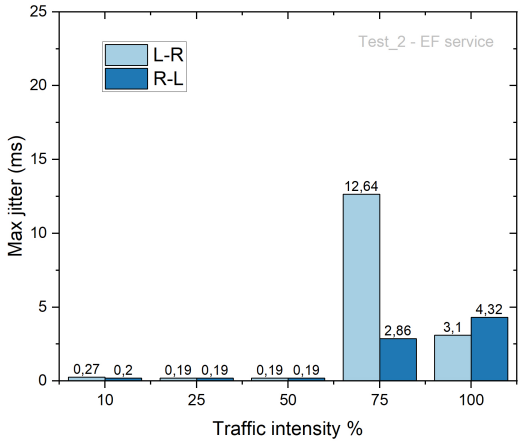

Fig. 7. Max jitter parameter measurements for Service-1 tested with incremental load and with QoS parameters active.

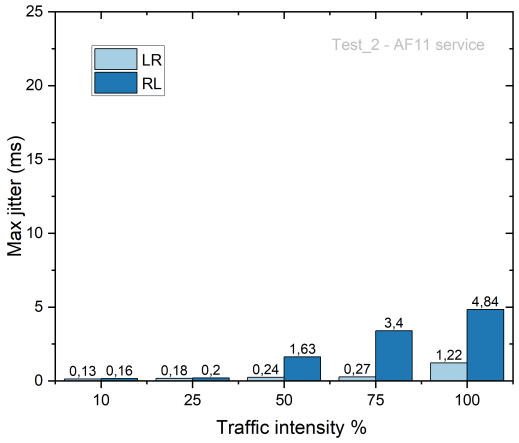

Fig. 9. Max jitter parameter measurements for Service 2 tested with incremental load and with QoS parameters active.

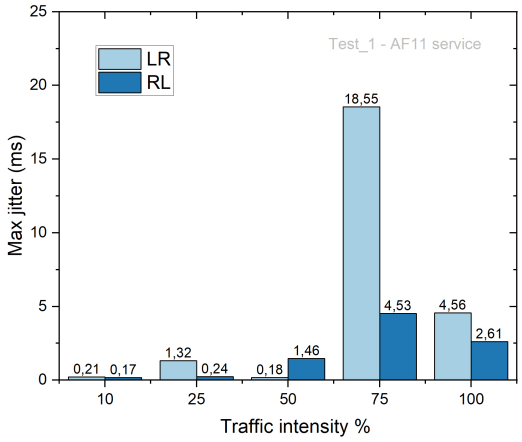

Fig. 8. Max jitter parameter for Service 2 tested with incremental load and without active QoS parameters.

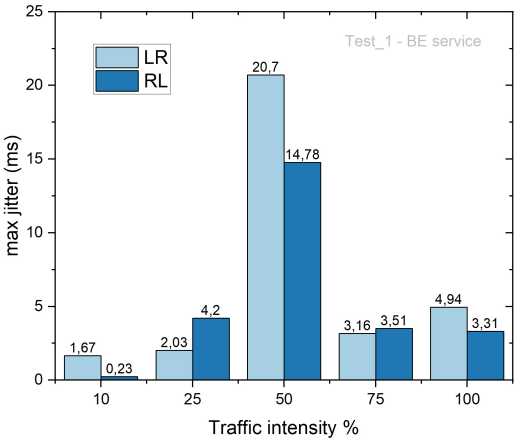

Fig. 10. Max jitter parameter for Service 3 tested with incremental load and without active QoS parameters.

that carries data in BE *(Best Effort)* mode. In this case, the value of the Max Jitter parameter also changes as the link load increases (See Fig. 10). In Test 2, the Max Jitter parameter for Service 3 (class BE) increases as the link load increases (See Fig. 11). This is due to the fact that during Test 2, QoS mechanisms are activated, which handle the higher priority data first, i.e. data from class AF11 and class EF. In contrast, the data carried in class BE is the lowest priority data and is handled last. This therefore has the effect of increasing the handling time of this data and increasing parameters such as max jitter and latency.

In the final step, a study of the impact of the delay parameter on the quality of service quality of service of data transmitted in the three traffic classes AF11, EF and BE was carried out. Delay is a critical parameter for many data types, especially for data requiring real-time handling. According to ITU-T recommendation G.114 [28], the delay in one direction for VoIP data must not exceed 150 ms. In the topology studied, Service 1 uses class EF, which was used to transport G.729 VoIP data. The results of the tests carried out showed that for the Test 1 configuration, i.e. for the configuration without active QoS parameters, the delay value remains at a similar level for all three traffic classes and varies between 631.42 ms and 636.31 ms (See Fig. 12). This means that none of the traffic classes meet the ITU-T G.114 recommendations. In contrast, the results obtained for Test 2, i.e. for configurations with active QoS parameters, showed a significant improvement in the delay parameter for data carried in traffic classes AF11 and EF. A significant decrease in the delay value was observed in these classes. In class AF11, the delay value decreased by 77.04 %, while in class EF, the delay value decreased by 75.77 %. As can be expected, the decrease in the value of the delay parameter in classes AF11 and EF is at the expense of the data transmitted in class BE. Data transmitted in the

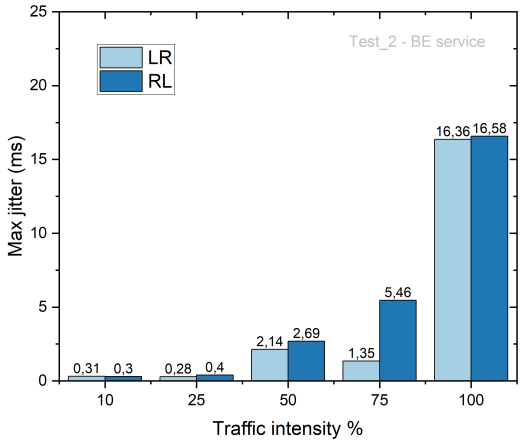

Fig. 11. Max jitter parameter for Service 3 tested with incremental load and with active QoS parameters.

BE class is treated as standard traffic with no guarantee of QoS. The tests carried out showed that the activation of the QoS parameters caused a very high increase in the delay of data transmitted in class BE. In the BE class, the delay value increases from 636.31 ms to 3205.93 ms. Such a change represents an increase in delay value of 503.99 %. The study, therefore, showed that the proper implementation of QoS parameters makes it possible to control and ensure quality of service guarantees for classes AF11 and EF.

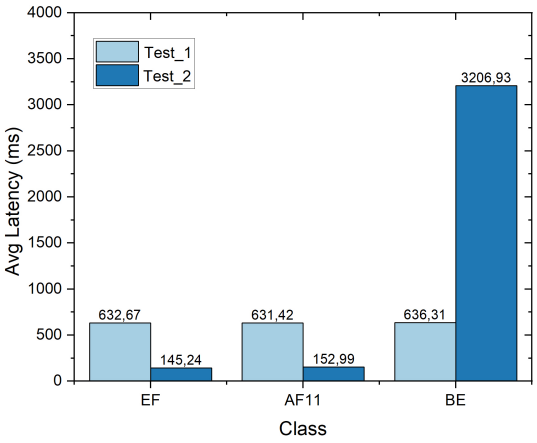

Fig. 12. Measurements of the Avg Latency parameter.

VIII. Conclusions

The vast volumes of data now being transmitted over network devices require a quality of service. The QoS requirements for IP-based networks used for real-time data transmission are stringent. This issue is all the more important as the share of multimedia, voice transmission, and sensitive applications in IP networks is increasing, and the demand for guaranteed services will grow. The development of high-speed data transmission standards forces the design and implementation of systems with the capacity of the system components necessary to ensure complex QoS quality parameters. Calculating the data transmission time from node to node is relatively easy, but the time and nature of waiting at the node remain unknown. Over-intensive use of network resources can lead to a deterioration of QoS services, resulting in increased queues in nodes or an increase in the probability of their overcrowding, causing an increase in waiting times. Carried out studies of selected AF11, EF and BE traffic classes showed that correct implementation of QoS mechanisms ensures adequate quality of service, which is in line with ITU-T recommendations. The conducted tests showed that properly implementing the QoS parameters makes it possible to provide guaranteed quality of service even under network congestion conditions.

References

[1] M. M. Abualhaj, S. N. Al-Khatib, M. Kolhar, A. Munther, and Y. Alraba'nah, "Effective voice frame pruning method to increase voip call capacity." *TEM Journal*, vol. 9, no. 1, 2020. [Online]. Available: https://doi.org/10.18421/TEM91âĂŘ08

[2] H. J. Kim and S. G. Choi, "A study on a qos/qoe correlation model for qoe evaluation on iptv service," in *2010 The 12th International Conference on Advanced Communication Technology (ICACT)*, vol. 2. IEEE, 2010, pp. 1377–1382. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5440288

[3] G. Miranda, D. F. Macedo, and J. M. Marquez-Barja, "Estimating video on demand qoe from network qos through icmp probes," *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 1890–1902, 2021. [Online]. Available: https://doi.org/10.1109/TNSM.2021.3129610

[4] R. Duan, X. Chen, and T. Xing, "A qos architecture for iot," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, 2011, pp. 717–720. [Online]. Available: https://doi.org/10.1109/iThings/CPSCom.2011.125

[5] H. Rojas, R. Renteria, E. N. Luque, M. Peralta, and J. L. Merma, "Proposal to implement low cost digital communication using voip technology, a case study," *International Journal of Future Computer and Communication*, vol. 7, no. 3, pp. 68–73, 2018. [Online]. Available: https://doi.org/doi:10.18178/ijfcc.2018.7.3.523

[6] L. Yang, S.-H. Yang, and L. Plotnick, "How the internet of things technology enhances emergency response operations," *Technological Forecasting and Social Change*, vol. 80, no. 9, pp. 1854–1867, 2013. [Online]. Available: https://doi.org/10.1016/j.techfore.2012.07.011

[7] F. M. Puspita, K. Seman, B. M. Taib, and Z. Shafii, "Improved models of internet charging scheme of single bottleneck link in multi qos networks," *Journal of Applied Sciences*, vol. 13, no. 4, pp. 572–579, 2013. [Online]. Available: https://doi.org/10.3923/jas.2013.572.579

[8] X. Yuan, H. Yao, J. Wang, T. Mai, and M. Guizani, "Artificial intelligence empowered qos-oriented network association for next-generation mobile networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 3, pp. 856–870, 2021. [Online]. Available: https://doi.org/10.1109/TCCN.2021.3065463

[9] D. Strzęciwilk, "Examination of transmission quality in the ip multi-protocol label switching corporate networks," *International Journal of Electronics and Telecommunications*, vol. 58, no. 3, pp. 267–272, 2012. [Online]. Available: https://doi.org/10.2478/v10177-012-0037-z

[10] Y. Deng, H. Lin, A. G. Phadke, S. Shukla, J. S. Thorp, and L. Mili, "Communication network modeling and simulation for wide area measurement applications," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*. IEEE, 2012, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ISGT.2012.6175664

[11] T. Mazhar, M. A. Malik, S. A. H. Mohsan, Y. Li, I. Haq, S. Ghorashi, F. K. Karim, and S. M. Mostafa, "Quality of service (qos) performance analysis in a traffic engineering model for next-generation wireless sensor networks," *Symmetry*, vol. 15, no. 2, p. 513, 2023. [Online]. Available: https://doi.org/10.3390/sym15020513

[12] X. Ji, B. Han, C. Xu, C. Song, and J. Su, "Adaptive qos-aware multipath congestion control for live streaming," *Computer Networks*, vol. 220, p. 109470, 2023. [Online]. Available: https://doi.org/10.1016/j.comnet.2022.109470

[13] D. Strzęciwilk, "Timed petri nets for modeling and performance evaluation of a priority queueing system," *Energies*, vol. 16, no. 23, p. 7690, 2023. [Online]. Available: https://doi.org/10.3390/en16237690

[14] M. Karakus and A. Durresi, "Quality of service (qos) in software defined networking (sdn): A survey," *Journal of Network and Computer Applications*, vol. 80, pp. 200–218, 2017. [Online]. Available: https://doi.org/10.1016/j.jnca.2016.12.019

[15] R. Braden, D. Clark, and S. Shenker, "Integrated services in the internet architecture: an overview," 1994. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1633

[16] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "Rfc2475: An architecture for differentiated service," 1998. [Online]. Available: https://doi.org/10.17487/RFC2475

[17] P. Gevros, J. Crowcroft, P. Kirstein, and S. Bhatti, "Congestion control mechanisms and the best effort service model," *IEEE network*, vol. 15, no. 3, pp. 16–26, 2001. [Online]. Available: https://doi.org/10.1109/65.923937

[18] J. Peng, *Communications and Networking*. Rijeka: IntechOpen, Sep 2010. [Online]. Available: https://doi.org/10.5772/262

[19] D. Strzęciwilk, R. Nafkha, and R. Zawiślak, "Performance analysis of a qos system with wfq queuing using temporal petri nets," in *Computer Information Systems and Industrial Management: 20th International Conference, CISIM 2021, Ełk, Poland, September 24–26, 2021, Proceedings 20*. Springer, 2021, pp. 462–476. [Online]. Available: https://doi.org/10.1007/978-3-030-84340-3_38

[20] A. Custura, R. Secchi, and G. Fairhurst, "Exploring dscp modification pathologies in the internet," *Computer Communications*, vol. 127, pp. 86–94, 2018. [Online]. Available: https://doi.org/10.1016/j.comcom.2018.05.016

[21] K. Nichols, S. Blake, F. Baker, and D. Black, "Definition of the differentiated services field (ds field) in the ipv4 and ipv6 headers," Tech. Rep., 1998. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2474

[22] B. Davie, A. Charny, J. Bennet, K. Benson, J.-Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis, "An expedited forwarding phb (per-hop behavior)," Tech. Rep., 2002. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3246

[23] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski, "Assured forwarding phb group," Tech. Rep., 1999. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2597

[24] F. Baker, "Rfc1812: Requirements for ip version 4 routers," 1995. [Online]. Available: https://dl.acm.org/doi/pdf/10.17487/RFC1812

[25] G. Armitage, B. Carpenter, A. Casati, J. Crowcroft, J. Halpern, B. Kumar, and J. Schnizlein, "Rfc3248: A delay bound alternative revision of rfc 2598," 2002. [Online]. Available: https://doi.org/10.17487/RFC3248

[26] L. De Ghein, *MPLS fundamentals*. Cisco Press, 2016. [Online]. Available: https://elhacker.info/manuales/Redes/Cisco/MPLS/MPLS%20Fundamentals.pdf

[27] T. Diallo and M. Dorais, "Ethersam: The new standard in ethernet service testing," *EXFO assessing next-gen networks*, pp. 1–12, 2011.

[28] T. ITU, "Recommendation g. 114, one-way transmission time," *Series G: Transmission Systems and Media, Digital Systems and Networks, Telecommunication Standardization Sector of ITU*, 2000. [Online]. Available: https://www.itu.int/rec/T-REC-G.114