INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2012, VOL. 58, NO. 3, PP. 267–272
Manuscript received December 3, 2011; revised February, 2012. DOI: 10.2478/v10177-012-0037-z

Examination of Transmission Quality in the IP Multi-Protocol Label Switching Corporate Networks

Dariusz Strzęciwilk

***Abstract*—The paper presents the examination of quality of transmission designed and built based on IP/MPLS technology as well as BGP and OSPF routing protocols of corporate network. It indicates the factors forming and affecting the service quality in IP network, including QoS support network architecture, particularly the architecture of DiffServ differentiated services. Main problems occurring in these architectures have been discussed. The analysis of data and voice transmission via IP network of Best Effort architecture and in Differentiated Service architecture of differentiated transmission quality have been conducted. It has been presented that the MPLS technology may be effectively applied in building corporate networks requiring network services of highest quality parameters with lossless packet transmission and maximum delay guarantee.**

***Keywords*—IP/MPLS network, DiffServ architecture, VoIP, transmission quality, quality of service.**

I. Introduction

THE Internet network consists of many heterogenic networks built by means of different data link techniques. Communication between applications in such a network is based mainly on the IP protocol (*Internet Protocol*) which does not use the properties of lower layers protocol and offers unreliable, connectionless network service exposed to packets loss, change in their order or duplication. This arises from the fact that there are no implemented mechanisms responsible for the quality of the realised network service that could be effectively applied to operate the application [1].

Data transmission technologies used in the building of wide area corporate networks must, however, fulfil the specified quality and quantity requirements. Apart from disadvantageous features of IP protocols, the quality of transmission may be affected by delays in data transmission, connected with packet queuing in the buffers of network devices, developing along with the increase in network load. The mere IP protocol, constructed in such a manner so as to obtain maximal simplicity and scalability, even at the cost of network quality and performance, does not allow for highly efficient corporate networks to be developed. The emergence of real time application brought attention to certain network parameters that used to be ignored. Networks using the IP protocol operate effectively only in traditional data transmission and the increase of demand for broadband services as well as use of multimedia renders providing the quality of services indispensible, especially for real time applications which require efficient transport algorithms via network, offered by the MPLS protocol (*Multi-Protocol Label Switching*), along with its virtual version VPN (*Virtual Private Networks*) [2]. MPLS plays a vital role, contributing efficient TE (*Traffic Engineering*), high speed, QoS (*Quality of Service*) and optimized resource allocation by balancing the load. The QoS architecture in IP networks is required to provide the resource reservation guarantees that allow differentiation and prioritization of flows. Application of algorithms and QoS mechanisms [3] in the IP network supports providing a strict guarantee of packet transfer quality for the selected traffic flows belonging to the so-called traffic/service classes, which allow the operators to render advanced telecommunication services. Voice and picture transmission cannot be exposed to any packet damage or loss, as retransmission or excessive delays of IP packets transferring voice data make such a transmission useless [4]. In order to prevent such situations from happening, the guaranteed quality of such services as voice or picture transmission is introduced, called QoS methods [3], [5]. ITU-T (*International Telecommunication Union*) [6], [7] and IETF (*Internet Engineering Task Force*) [8] indications point out that IP QoS networks should fulfil the strict QoS guarantees for such applications as voice, video, video-conferences or transfer of longer data sets. Currently, a developed telecommunication infrastructure of an organisation must no longer provide only phone calls and regular access to the Internet network, but it also requires 'custom-made' business solutions prepared regarding specific needs of the enterprise, such as VoIP voice services with band and delay guaranty or safe information exchange in the IP/VPN channels.

The objective of this paper is to analyse the transmission quality in IP/MPLS corporate networks. The transmission quality has been examined in a network built with application of data transmission technologies, used in building wide area corporate networks. The analysis of data and voice transmission via IP network of BE (*Best Effort*) architecture and in the DiffServ (*Differentiated Services*) architecture of differentiated transmission quality supporting QoS have been conducted. Performance tests for a designed and built network that may be used in building a wide area corporate network based on IP/MPLS technology as well as BGP (*Border Gateway Protocol*) and OSPF (*Open Shortest Path First*) routing protocols have been presented.

II. Transmission Quality in IP Multi-Protocol Label Switching Corporate Networks

The IP protocol has been optimised with regard to select the shortest route in the network ant not the control mechanisms

D. Strzęciwilk is with the Department of Application of Informatics, Warsaw Univeristy of Life Sciences (SGGW), Warsaw, Poland (e-mail: dariusz_strzeciwilk@sggw.pl).

of the packet flow which may cause network overload in adverse situations. In the late 90's of the previous century, there were attempts made aiming at upgrading the mechanisms of IP packet transfer in order to achieve a speed that would at least be close to the one offered by ATM switches. A variety of solutions has been introduced, constituting an attempt to combine the best features of the IP protocol with the switching speed in the data layer. Ipsilon proposed the IP Switching technique, Cisco introduced Tag Switching and other solutions were advanced by IBM and Cascade. Further on, the working group of IETF (*Internet Engineering Task Force*) introduced the unified standard known as the MLPS protocol [9] to be used with any other protocol of the network layer, although most implementations is based on the mere IP protocol. The idea of MPLS operation consists in adding an extra portion of information on the constant length of the so-called label to each packet entering the MPLS network [10], [11]. The path of the packet via the network is determined at the moment of reaching the edge of the network. The intermediate routers do not make any decisions in this matter anymore. Their operation is limited only to transferring the packet to the proper interface on the basis of the label value. At the output of the MPLS network, the label is taken off and the packet is ready for operation by regular IP routers. It is possible to ensure the quality of transmission in the IP network by means of advanced mechanisms provided by the MPLS protocol.

A. *Forwarding Equivalence Classes*

When the packets are entering the network, they are allocated to the FEC (*forwarding equivalence classes*). FECs allow to divide all packets into groups forming flows and the packets without the given group are treated equally by the routers, as regards both the path of transfer in the network and the mechanisms of queuing or rejection strategies. Allocation in an FEC may be conducted on:

- the asis of the source and destination address of the packet,
- source and destination port,
- source and destination port or the TOS (*Type of Service*) field of the IP packet.

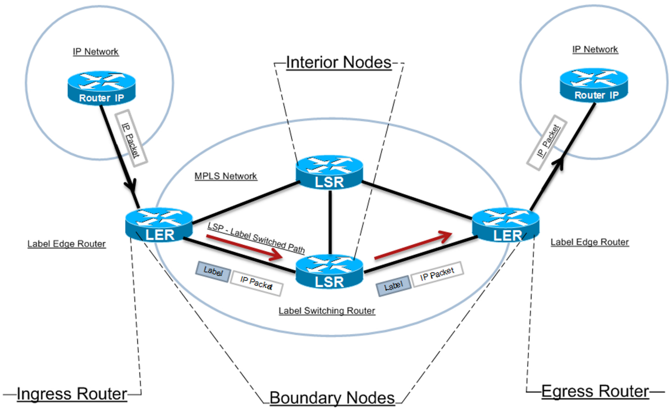

Fig. 1. The path of the IP packet in the MPLS domain.

The packets from the specified FEC flow through an unambiguously defined path – LSP (*Label Switched Path*). The path is determined by the edge router of the MPLS domain – LER router (*Label Edge Router*) (see Fig. 1), by means of information on the accessibility of the remaining routers provided by other routing protocols, e.g. OSPF, BGP. Specified resources may be allocated to each LSP, which guarantees the required bit rate as well as packet queuing and rejection policy, which ensures favouring of sensitive applications. It is assumed that the labels are only locally significant and they identify the FEC, and indirectly LSP, only in the nearest surrounding of the given network node. It is LDP (*Label Distribution Protocol*) that ensures the consistency of combination of FECs with local labels. Packets with added labels are switched inside the MPLS domain by LSR routers (*Label Switching Routers*) which does not have to process the whole IP heading and make the decision on the choice of path on the basis of the specified algorithm of routing and packet destination address. The decision is made solely on the basis of the label and routing table built by means of LDP. The router sends the packet to the appropriate interface, adding the new label assigned to the given FEC between the LSR in question and the following router on LDP. The first router in MPLS domain is called as ingress router and the last router in MPLS domain is called egress router [12]. The path of the IP packet in the exemplary MPLS domain has been presented in Fig. 1.

B. *Service Quality Problems*

The main cause of problems regarding the service quality in the networks is the fact that the IP protocol is connectionless. Each packet is treated individually which results in the lack of 'rigid' connection between the source and destination host. MPLS solves this problem by the use of LSP which makes it the connection protocol and the packets are not processed as isolated from FEC flows to which they belong. The building in of the IP protocol into the oriented connection frames makes the transmission between the final nodes to follow a strictly determined, previously defined LSP, which, among other things, improves the important QoS parameter constituted by the changeability of the packet transfer delay (*Jitter*). Therefore, in order to provide the appropriate standard of services in the IP networks, one may use the MPLS protocol which in the MPLS VPN version supports, despite advanced Traffic Engineering services and connection quality, the safety and separation of the traffic within various VPNs. Y. Bernet at al. in the paper [13] presents a description of the mechanisms indicated for the IP networks based on the DiffServ architecture [13]. The document defines the QoS mechanisms for the edge and core router in the DiffServ architecture. It has to be noted that the mechanisms supporting the DiffServ architecture described therein are implemented in the Cisco routers which were used to carry out the tests for the purpose of this paper.

III. DiffServ Architecture

Within the research of the IETF (*Internet Engineering Task Force*) organisation on the transmission quality in the

IP network the network architecture classes allowing for the distribution of traffic into classes with differentiated service quality have been defined, i.e. IntServ (*Integrated Services*) [14] RSVP (*Resource ReSerVation Protocol*) [15] and Differentiated Services [16]. The classes with differentiated quality constitute the development of the traditional model of the BE services for the network with the demanded service quality. The classes in the differentiated service model allow the operation of temporarily critical services (of real time) the guaranteed network service is intended for [17]. IntServ/RSVP and DiffServ architectures do not depend on each other, however they may be combined in the Modified Harvard Architecture in order to ensure a reliable e2e (*end to end*) communication [18]. The resultant architecture is considered one of the most promising architectures to deliver QoS guarantees in the future Internet [19]. Detailed information on the mentioned architectures have been presented in the papers of the authors [20], [21], [22].

A. *Soft Quality of Service*

In case of IntServ, there may occur some problems with scalability in the large backbone networks. The data flow generated by the application requires each router the packet passes through to store the information regarding the subject of the reserved resources. This consists in guaranteeing the band and determining the maximal level of delays in the given network node. The reservation of resources in such a case may consist in the guarantee of the lack of packet rejection or in the probability of packet rejection on the specified level. The DiffServ model has been developed in a manner allowing to evade the limitations resulting from both the Best Effort model and the IntServ model. It provides an 'almost' guaranteed QoS, concurrently being a scalable and elastic solution, also called *soft QoS*. In this model, the network traffic is divided into classes in compliance with the business assumptions. Each class is allocated to a different level of services and the packets are treated by the network devices according to the priority of the class. In the DiffServ architecture the identification of particular traffic flows takes place in the edge routers where the amount of these flows is usually not large. On the other hand, the core routers identify only the collective flows, defined by the allocation of the traffic to the given network service.

B. *Quality of Service Mechanism*

The set of QoS mechanisms has been defined within the framework of DiffServ architecture specification, to be used depending on the location of the given router within the network (edge or core) and in accordance with the adopted rules for the operation of particular traffic classes. The edge router identifies the particular traffic flows, monitors their conformity with the traffic contracts and is responsible for attributing the packets with proper DSCP field value [23] in compliance with the demanded type of service. Depending on the router type (core, edge), the DiffServ architecture provides the set of mechanisms to operate appropriate traffic classes. This results in the identification of particular traffic flows, monitoring of their conformity eith the traffic contracts and assigning proper DSCP field value (see Fig. 2) to the packets belonging to them taking place on the inbound router. The inbound interface of the router in the DiffServ architecture operates the packets through the following implemented mechanisms:

- MF (Multi-Field Type Classifier that identifies the particular traffic flows on the basis of the content of particular fields of the packet headings (source and destination addresses and port numbers)
- Traffic Conditioning Block includes the devices the task of which is to control the conformity of the flow with the profile specified by the traffic descriptor connected with it

The assumed monitoring device (meter) is the Token Bucket [24] mechanism. The packets consistent with the contract are marked by the marker device with the appropriate DSCP value. Depending on the principles of execution of the given service, the packets deemed inconsistent may be rejected by the dropper, marked with different DSCP code by the marker, or delayed by the shaper (see Fig. 2). There is no such functionality implemented on the core routers, because they do not identify the particular data flows.

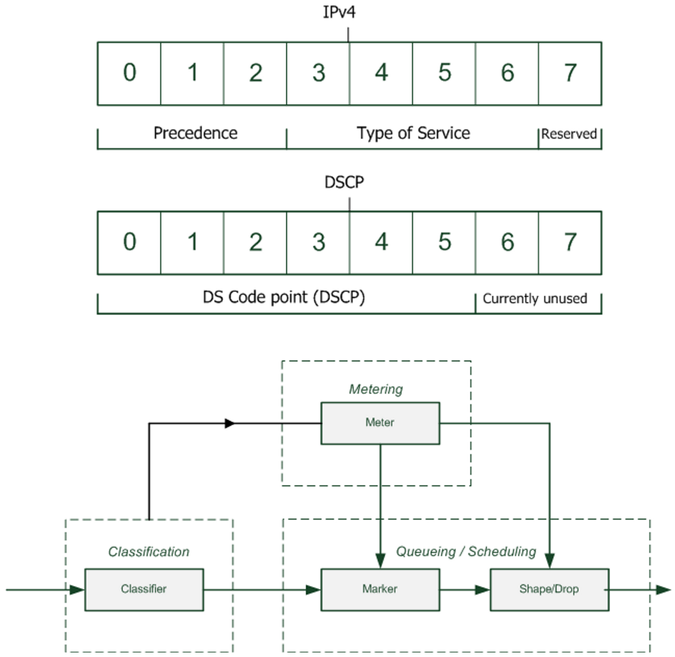

Fig. 2. DiffServ packet operation chart.

The packet operation mechanisms on the output port of the router are not dependent on its function and the manner of packet operation is specified by the set of packet transfer principles, the so-called PHB (*Per Hop Behaviour*). Each node in domain treats the packet in a specified way according to classifier or DSCP value. This forwarding behavior is called just PHB. It allocates resources to behavior aggregates and with the help of this basic hop-by-hop resource mechanism that uses differentiated services may be constructed.

To date, two main types of PHB have been defined, i.e. the Expedited Forwarding PHB [25], [26], [27] and the Assured Forwarding PHB Group [28].

IV. Network Design and Measurements

The IP/MPLS protocol supporting the mechanisms of providing the service quality were used to build the corporate network. The backbone network was built by means of Cisco router of 7200 series, including two LSR (P) routers and two LER (PE) routers (see Fig. 3). All routers of 7200 series had the IOS system in 12.4(11)T5 Advanced Services version. At the location of the client there have been access routers (CE). Between the routers forming the backbone of the network there have been the OSPFv4 dynamic routing protocol implemented which provided all core routers with the transfer of information on the accessible networks and interfaces within the backbone of the network and supported the exchange of information for the LDP protocol. In addition, on the PE routers there have been the BGPv4 external dynamic routing protocol launched in order to exchange the information on the VPN virtual networks, since the coexistence of two or more networks possessing the same addresses is impossible in the traditional IPv4 network addressing.

A. Network Ambiguity

The ambiguity in the routing may cause interference in the routing and incorrect packet routing. The IOS operation system allowed for application of the extended 96-bit addressing and elimination of the routing ambiguity. This is possible due to application of VRF (*Virtual Routing and Forwarding*) as well as RD (*Route Distinguisher*) markers, resulting in creation of expanded VPNv4 address space (See show ip bgp command).

```
PE0# show ip bgp vpn4 all
BGP table version is 25, local router
ID is 81.210.2.1
Status codes: s suppressed, d damped,
h history,* valid, > best, i-internal,
r RIB-failure, S Stale
Origin codes: i-IGP, e-EGP, ?-incomplete
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 1:101
(default for vrf VPN-CUST_A)
*> 10.0.0.0 77.252.10.2 0 32768 i
*>i11.0.0.0 81.210.2.2 0 100 0 i
*> 77.252.10.0/30 0.0.0.0 0 32768 i
*>i77.252.11.0/30 81.210.2.2 0 100 0 i
Route Distinguisher: 1:102
(default for vrf VPN-CUST_B)
*> 10.0.0.0 77.252.10.6 0 32768 i
*>i11.0.0.0 81.210.2.2 0 100 0 i
*> 77.252.10.4/30 0.0.0.0 0 32768 i
*>i77.252.11.4/30 81.210.2.2 0 100 0 i}
```

The expanded addressing allowed, despite the employment of identical address classes for both VPN-CUST_A and VPN-CUST_B virtual networks, for the proper separation and routing of the packets of both netwroks. Despite the main table, in the BGP routing table there were two VRF virtual tables created to store the information on the routes in VPNs.

The same address classes, depending on the VRF they belong to, were directed to different final devices. For the PE0 router the 10.0.0.0/8 of VRF VPN-CUST_A class is directed to the address of 77.252.10.2, whereas the one in VRF VPN-CUST_B to the address of 77.252.10.6. An analogous situation is found in case of PE1 with the 11.0.0.0/8 class. It has to be noted that the OSPF routing table and the BGP global table did not have the information on the created private networks, due to which neither of them was accessible from any location other than the CE and PE routers which had the information on the existence of the private networks. Due to such a solution the private networks were isolated both from each other as well as from the 'external world' (See show ip route command).

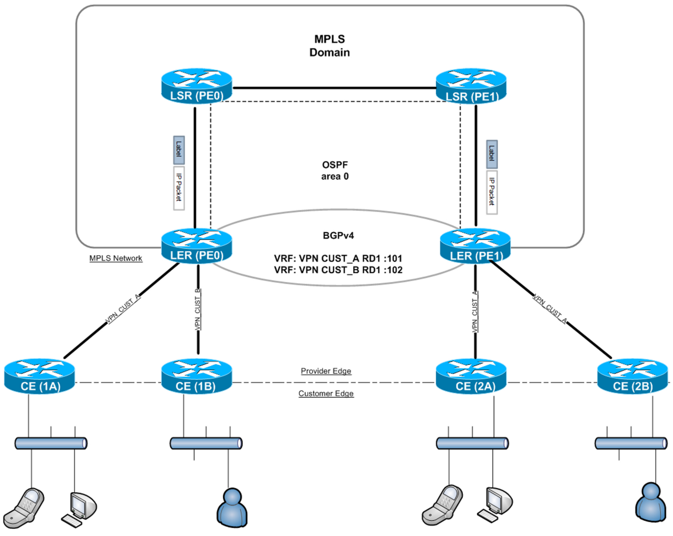

Fig. 3. Chart of the examined network.

```
PE0# show ip route
81.0.0.0/32 is subnetted, 4 subnets
C 81.210.2.1 is directly connected,
Loopback0
O 81.210.1.2 [110/3] via 83.238.0.5,
00:47:35, FastEthernet1/0
O 81.210.2.2 [110/4] via 83.238.0.5,
00:47:35, FastEthernet1/0
O 81.210.1.1 [110/2] via 83.238.0.5,
00:47:35, FastEthernet1/0
83.0.0.0/30 is subnetted, 3 subnets
O 83.238.0.16 [110/3] via 83.238.0.5,
00:47:35, FastEthernet1/0
C 83.238.0.4 is directly connected,
FastEthernet1/0
O 83.238.0.0 [110/2] via 83.238.0.5,
00:47:35, FastEthernet1/0
```

B. Network Measurements

The CE routers were connected to the network by means of V35 serial interface of the speed of 2 Mbps. The Px (LSR) and PEx (LER) routers were connected with each other by means of FastEthernet 100 Mbps interfaces, whereas the P0 and P1 routers by means of optical Gigabit Ethernet interfaces, with the use of optic fibre patchcords and mufflers -3 dBm to secure the SFP, due to the small distance between the devices located at the laboratory. All network performance tests were conducted at the laboratory site. The measurements were carried out with the use of JDSU HST-3000 and MST-8000 measuring devices. The applied devices support the measurement methods compliant with the RFC 2544 specification [29]. The HST-3000 device was used as the source of the data flow, whereas MST-8000 was the receiver of the flows and conducted the analysis of the received data. The first stage covered the generation of two flows, i.e. of data and voice. Both flows were generated by the HST-3000 device in a manner allowing the voice flow to possess a constant speed of 256 kbps with tolerance of 2% whereas the data flow was generated from the speed of 0 kbps which was increased by 100 kbps every 5 seconds, also with the tolerance of 2%, until the full link saturation (see Fig. 4). Both flows contained only the UDP datagrams and were generated as the so-called Flood. The conducted tests indicated that at the moment of obtaining approximately 70% of link saturation by the DATA flow speed, the packet losses and longer response times begin to generate in the VOICE flow (see Fig. 5). The analysis of the generated voice and data flows indicates that a significant alternation of the voice flow characteristics occurs upon the lapse of about 80 sec. This arises from the characteristics of both flows. The Voice flow is constituted by small packets of 60-100 bytes, the Data flow was generated as full 1500 byte packets. At 80% of the link saturation, the losses in the Voice flow reach as much as 40% and the times of over 200 ms, which, with the requirements of the Voice flow – losses less then 1% and time less than 150 ms, renders this service completely useless. It was concluded that at over 90% link saturation by the generated Data flow, in principal only single packets of the Voice flow are able to reach their destination.

C. Data and Voice Flows

The next stage of examination covered the generation of further data and voice flows. Both flows were generated by HST-3000 in the same manner as before. The voice flow was modified to simulate the VoIP connection, so as to define its highest priority belonging to the priority class called the priority aggregate. The data flow, however, possessed the lowest priority and simulated the remaining network traffic in the Best Effort class. As may be seen in the Fig. 5, the voice flow reached its assumed speed throughout the whole examined time slot, i.e. 256 kbps and times below 20 ms (see Fig. 6) as well as lack of packet loss. The results indicate that it fulfils all the requirements of proper operation of the voice service in the packet network with transmission quality.

V. Conclusion

The examined typology of the IP/MPLS corporate network indicated that at the output implementing the queuing algorithm of FIFO (*First In First Out*) type for the data and voice type traffic classes (marked with the same DSCP code) it is indispensible to assign the priority class. The fact the voice flow was not allocated to the priority class resulted in the link overload of greater than 70%, significant packet loss and increase in the response time being observed. The

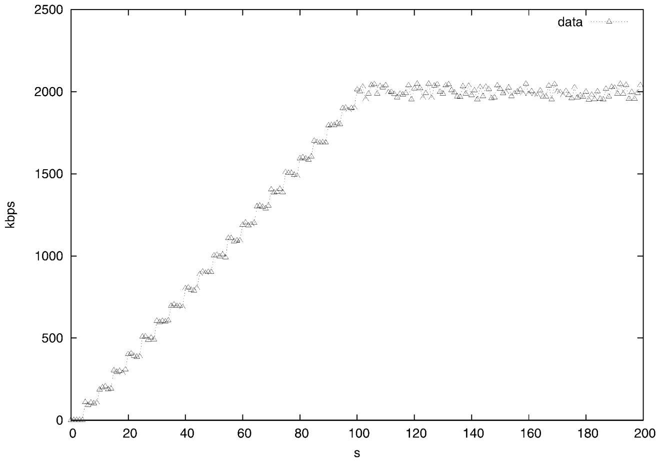

Fig. 4. Generated data flow.

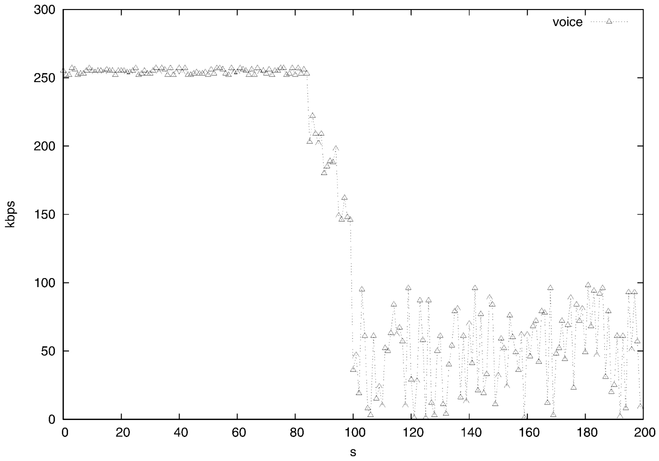

Fig. 5. Generated voice flow.

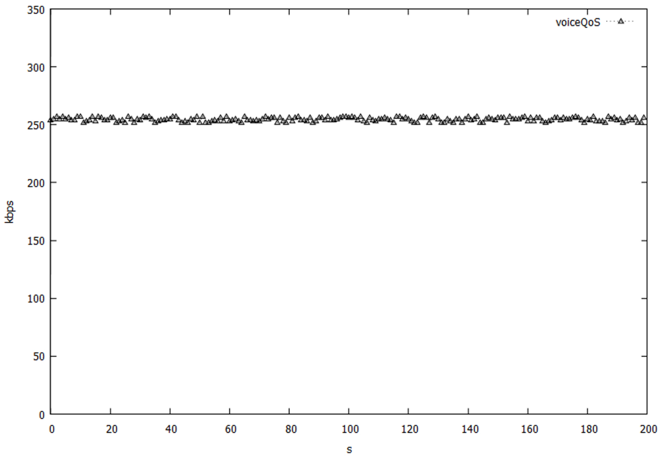

Fig. 6. Voice flow upon the application of QoS.

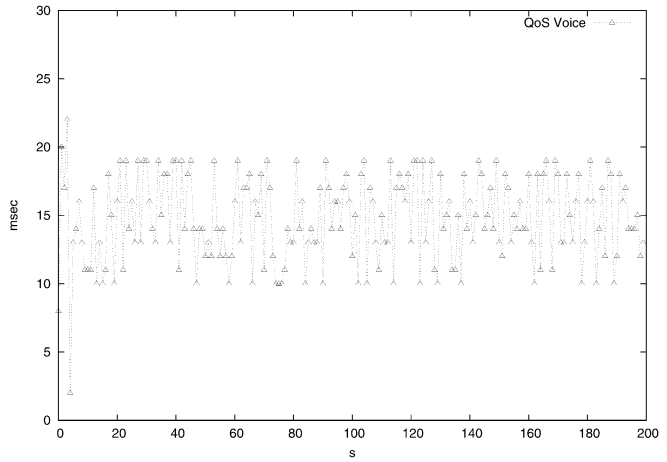

Fig. 7. The response times for the voice flow upon the application of QoS.

data flow may occupy the entire load of the accessible band, resulting in almost total loss of the voice packets. Therefore, the traffic operation on the link without the designated priority classes possess a direct influence on the quality of sensitive voice services. The data flows should be operated in a manner not influencing the quality of the critical flow transmissions. The traffic entering the network and classified in accordance with the traffic contract with higher priority marked as voice, allowed for effective traffic control, guaranteeing efficient operation of services belonging to the critical voice flows. Upon the alternation of the class priority for the voice flow, it reached its assumed speed and times lower that 20 ms with no packet loss throughout the whole examined time slot. On this basis it was concluded that it fulfilled the conditions of proper operation of critical voice flows in the packet network with service quality guarantee. The development of convergent services indicates that the works on providing service quality in the IP and IPv6 packet networks, especially in those based on the QoS and IP/MPLS protocol, will remain a fast growing area of technology and the subject of intensive research, being driven by the growth of real-time applications such as voice over IP.

REFERENCES

[1] L. D. Ghein, *MPLS Fundamentals*. Indianapolis, USA: Cisco Press, 2007.

[2] J. Postel (ed.), *Internet protocol – DARPA Internet Program Protocol Specification*, USC/Information Science Institute RFC 791, September 1981.

[3] A. Grenville, *Quality of Service in IP Networks*. Pearson Higher Education, 2000.

[4] D. Hucaby, *CCNP BCMSN exam certification guide: CCNP self-study*. Indianapolis, USA: Cisco Press, 2006.

[5] K. Ahlin, *Quality of Service Over IP Networks*. Linköping: Linköping University, 2003.

[6] *IP Packet Transfer and Availability Performance Parameters*, ITU-T Rec. Y.1540, December 2002.

[7] *Network Performance objectives for IP-based services*, ITU-T Rec. Y.1541, May 2002.

[8] J. Babiarz, K. Chan, and F. Baker, *Configuration Guidelines for DiffServ Service Classes*, Working Group of the IETF RFC 4594, August 2006.

[9] E. Rosen, A. Viswanathan, and R. Callon, *Multiprotocol Label Switching Architecture*, The Internet Society RFC 3031, January 2001.

[10] U. Black, *MPLS and Label Switching Networks*, 2nd ed. Singapore: Pearson Education (Singapore) Pte. Ltd, Indian Branch, 2002.

[11] G. Armitage, "MPLS the magic behind the myths," *IEEE Commun. Mag*, vol. 38, p. 124, 2000.

[12] G. Murugesan, A. M. Natarajan, and C. Venkatesh, "Enhanced Variable Splitting Ratio Algorithm for Effective Load Balancing in MPLS Networks," *Journal of Computer Science*, no. 4(3), pp. 232–238, 2008.

[13] Y. Bernet, S. Blake, D. Grossman, and A. Smith, *An Informal Management Model for Diffserv Routers*, IETF RFC 3290, May 2002.

[14] R. Braden, D. Clark, and S. Shenker, *Integrated Services in the Internet Architecture: an Overview*, IETF RFC 1633, June 1994.

[15] W. Stalling, *Computer networking and internet protocols and technology*. New Jersey, USA: Pearson Education, 2004.

[16] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, *An Architecture for Architecture for Differentiated Services*, IETF RFC 2475, December 1998.

[17] S. Shenker, C. Partridge, and R. Guerin, *Specification of guaranteed quality of service*, IETF RFC 2212, September 1997.

[18] Y. Bernet, et al., *A Framework for Integrated Services Operation over DiffServ Networks*, IETF RFC 2998, November 2000.

[19] Z. Mammeri, "Framework for parameter mapping to provide end-to-end QoS guarantees in IntServ/DiffServ architectures," *Computer Communications*, vol. 28 issue 9, pp. 1074–1092, June 2005.

[20] Y. C. Chang, R. C. Wang, J. L. Chen, and C. Kuo, "Scheduling Mechanism for IntServ/DiffServ Network Services," in *Proceedings of the 4th International Multi-Conference on Wireless and Optical Communications*, Banff, Canada, July 2004, pp. 184–189.

[21] Z. Mammeri, "End-to-End QoS Mapping in IntServ-over-DiffServ Architectures," in *High-Speed Networks and Multimedia Communications*, ser. Lecture Notes in Computer Science, M. Freire, P. Lorenz, and M.-O. Lee, Eds. Springer Berlin Heidelberg, 2003, vol. 2720, pp. 31–40, DOI: 10.1007/978-3-540-45076-4_4.

[22] H. Bai, M. Atiquzzaman, and W. A. Ivancic, "Running integrated services over differentiated service networks: quantitative performance measurements," M. Atiquzzaman and M. Hassan, Eds., vol. 4866, no. 1. Boston, MA, USA: SPIE, 2002, pp. 11–22, DOI: 10.1117/12.473015.

[23] K. Nichols, S. Blake, F. Baker, and D. Black, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, IETF RFC 2474, December 1998.

[24] W. Zhao, D. Olshefski, and H. Schulzrinne, "Internet Quality of Service: an overview," Columbia University, Computer Science Dept., Tech. Rep. Technical Report CUCS-003-00, February 2000.

[25] V. Jacobson, K. Nicholas, and I. Poduri, *An expedited forwarding PHB*, IETF RFC 2598, June 1999.

[26] G. Armitage, B. Carpenter, A. Casati, J. Crowcroft, J. Halpern, B. Kumar, and J. Schnizlein, *A delay bound alternative revision of RFC 2598*, IETF RFC 3246, March 2002.

[27] B. Davie, et al., *An Expedited Forwarding PHB (Per-Hop Behavior)*, IETF RFC 3246, March 2002.

[28] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski, *Assured Forwarding PHB Group*, IETF RFC 2597, June 1999.

[29] S. Bradner, *Benchmarking Methodology for Network Interconnect Device*, IETF RFC 2544, March 1999.