End-to-End QoS Provisioning by Flow Label in IPv6

Chuan-Neng Lin, Pei-Chen Tseng, and Wen-Shyang Hwang

Department of Electrical Engineering, National Kaohsiung University of Applied Sciences

Abstract

IPv6 as IP next generation is the successor to IPv4. IPv6 not only solves the shortcomings problem of IPv4 address, but also benefits the QoS especially during network congestion. Flow label field in IPv6 packet header provides an efficient way for packet marking, flow identification, and flow state lookup. This paper proposes the end-to-end QoS provisioning mechanism by utilizing 3-tuple instead of 5-tuple in IPv6 header, i.e. using flow label and traffic class to reserve resources to achieve customized QoS provision. This is also simulated in ns-2 network simulator, and results show the performance of the proposed mechanism is maintained during network congestion.

Keywords: Traffic Class, Flow Label, End-to-End QoS

1. Introduction

With the evolving rapidly of various multimedia applications, such as video telephonic systems, MoD, e-commerce, and real-time service, the existing IPv4 with best-effort service provided by today's Internet has been not sufficient. For deal with this requirement, IETF (Internet Engineering Task Force) proposed IPv6 as the successor to IPv4, and two types of QoS (Quality of Service): Integrated Service (IntServ) and Differentiated Service (DiffServ) [4].

IntServ reserves network resources along the entire path for per-flow end-to-end guarantee, but this leads to scalability problems which become more serious with increasing requests for various network applications. DiffServ makes a distinction between operations performed in the network core, and operations performed at the edges of the network. Core router only forwards the packets by different Per-Hop Behavior (PHB) treatment on the mapping policy of a DiffServ CodePoint (DSCP) in each packet's IP header. Edge router uses classifier to classify packets and performs traffic conditioning functions, including meter, marker, shaper, and dropper. Each packet must be set to an appropriate DSCP value. Depending on the actual queuing and forwarding implementation, there are three types of PHB, namely BE, EF (Expedited Forwarding) and AF (Assured Forwarding). The EF class, typically DSCP value 46, minimizes delay and jitter and provides the highest level of aggregate QoS. The AF class assigns preset Dropping Probability (DP) to different DiffServ class traffic to provide relative services [1].

In addition to solve the existing IPv4 address problem, IPv6 increases the IP address size from 32 bits to 128 bits [3], the current application for world-wide IPv6 implementation in [2]. IPv6 support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. Especially in QoS, there is a new added field (flow label) in IPv6 packet header to enhance QoS provisioning. Flow label field in IPv6 packet header provides an efficient way for packet marking, flow identification, and flow state lookup, but how to use this field in a specific architecture to provide QoS support is still an open issue [6]. This paper proposes the end-to-end QoS provisioning mechanism by utilizing 3-tuple instead of 5-tuple in IPv6 header, i.e. using flow label and traffic class to reserve resources to achieve customized QoS provision.

The remainder of this paper is organized as follows. In section 2 some related work of flow label is presented. The detailed scenarios of proposed end-to-end QoS mechanism are stated in section 3. In section 4 the simulation results are discussed, while section 5 concludes our work.

2. Related work

Figure 1 shows the packet header differences between IPv4 and IPv6. The traffic class field inherits the Type of Service (TOS) in IPv4 packet header. Hence DiffServ can be transferred seamlessly in IPv4 network to IPv6 network [4].

Traditionally, flow classifiers have been based on the 5-tuple of the source and destination addresses, ports, and the transport protocol type. However, some of these fields may be unavailable due to either fragmentation or encryption, or locating them past a chain of IPv6 option headers may be inefficient. Additionally, if classifiers depend only on IP layer headers, later introduction of alternative transport layer protocols will be easier. The usage of the 3-tuple

of the flow label and the source and destination address fields enables efficient IPv6 flow classification, where only IPv6 main header fields in fixed positions are used [7].

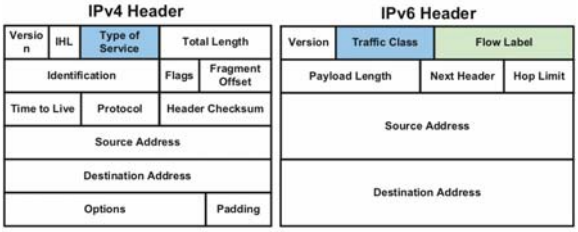


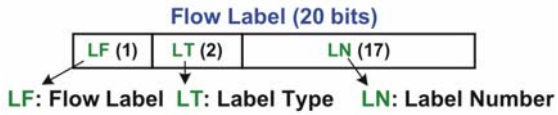
Fig. 1: Packet header differences between IPv4 and IPv6

The 20-bit flow label field in IPv6 packet header provides an efficient way for packet marking, flow identification, and flow state lookup, but how to use this field efficiently is still an open issue [5-7]. In [5] proposed a hybrid approach, which is using first three bits of flow label to define the rest 17 bits which is applicable to InterServ and DiffServ model. RFC3697 [7] describes the specification as follows:

- The 20-bit flow label field is used by a source to label packets of a flow.
- A flow label of zero is used to indicate that packets are not part of any flow.
- Packet classifiers use the triplet of flow label, source address, and destination address fields to identify which flow a particular packet belongs to.
- Packets are processed in a flow-specific manner by the nodes that have been set up with flow-specific state.
- The value flow label set by source must be delivered unchanged to the destination node(s).
- The same pair of source and destination must not use the same flow label values within 120 seconds.

3. End-to-End QoS Mechanism

There are four scenarios to achieve the proposed end-to-end QoS mechanism. Some routers supporting flow label and DiffServ function (with Flow-Label-and-DiffServ capable) have assumed according to the network topology. Firstly, 20-bit flow label field in the IPv6 packet header is divided into three parts detailed list as shown in figure 2. The first bit Label Flag (LF) set to 1 if flow label used. The 2-bit Label Type (LT) is the type of flow label. The rest of 17-bit Label Number (LN) is randomly generated by source for flow identification. Figure 3 shows Flow Label Marking Table (FLMT) and Flow Label Forwarding Table (FLFT), respectively. FLMT records Permit, 3-tuple of the flow label and the source and destination address, and TOS data for different kind of flow classification. FLFT lists its Next Hop for each flow. There are four scenarios for the proposed end-to-end provisioning mechanism: request scenario ① - ④, response scenario ⑤, delivery scenario ⑥, and termination scenario ⑦ as shown in Figure 4, 5, 6, and 7, respectively.



LF	0	Disable
	1	Enable
LT	00	The flow label is requested by source
	01	The flow label is responsed by destination
	10	The flow label is for data delivering
	11	The flow label is used to terminate connection
LN	A random number is created by source	

Fig. 2: The proposed flow label field in IPv6 packet header

Flow Label Marking Table (FLMT)

Permit	Label Number	Source	Destination	TOS
1 (yes)	0110010101101011	3FFE:3600:S::XX	3FFE:3600:D::XX	0xb8
⋮	⋮	⋮	⋮	⋮
0 (no)	0110101101100101	3FFE:3600:A::XX	3FFE:3600:C::XX	0x28

Flow Label Forwarding Table (FLFT)

Permit	Label Number	Next Hop
1 (yes)	0110010101101011	⋯
⋮	⋮	⋮
0 (no)	0110101101100101	⋯

Fig. 3: FLMT and FLFT

① The Host1 as shown in Figure 4, generates the Flow Label Number randomly. Here lists as (LF=1, LT=00, LN=Ran.Num.A) which regards as the request message for IPv6 packet.

② After gateway receives packets, it checks the Flow Label value. It check LN is unique or not if LF=1 and LT=00. If the number of LN is unique, it will record 3-tuple and TOS into FLMT. The value of TOS depends on the current situation of outgoing link. If not, it reply ICMP message to inform Host1 for requesting new LN for request message. Finally the Permit bit of FLMT set to 0, and this request packet are sent to the next (edge router).

③ Edge router checks LF, LT and LN of Flow Label field like gateway does after receiving packets. It selects the next hop (with Flow-Label-and-DiffServ capable) from the routing table. And the value of LN (Ran.Num.A) and next hop is recorded into FLFT. Finally the Permit bit of FLFT set to 0, and this request packet are sent to the next (core router). Core router did like edge router does.

④ Finally the request message is send to the destination node Host4.

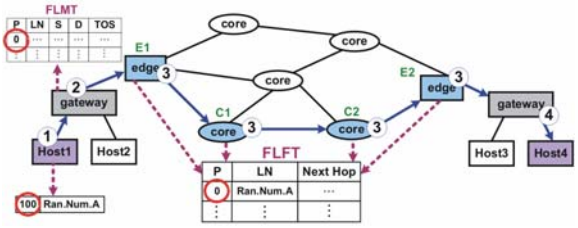


Fig. 4: Request Scenario

⑤ After receiving request message, Host4 does totally check. Host4 replies permit response message on Flow Label with LF=1, LT=01 and LN=Ran.Num.A along the same path (using the routing header) to Host1 if check OK. Routers and gateway along the path will change the related permit bit from 0 to 1 if same LN value in FLFT and FLMT while receiving response message (LT=01) for permitting the request message. Otherwise the ICMP message to inform reject message is instead.

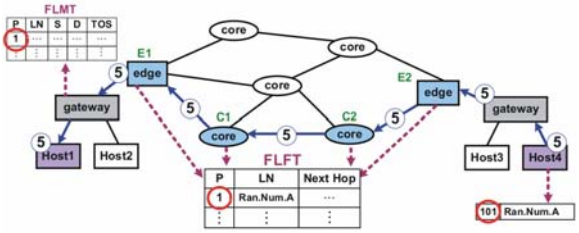


Fig. 5: Response Scenario

⑥ The data connection path establishes after permitting the request message. Host1 start using flow label (LF=1, LT=10, LN=Ran.Num.A) to deliver data and insert the related TOS to the traffic class fields in IPv6 packet header. Host1 must not use the same LN within 120 seconds after the LN expired [7].

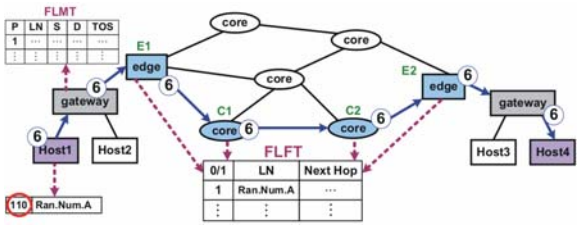


Fig. 6: Delivery Scenario

⑦ Host1 sends out the termination message by Flow Label with LF=1, LT=11, LN=Ran.Num.A if connection terminated. Gateway and routers delete the matching LN entry in FLMT and FLFT respectively after receiving the termination message (LT=11).

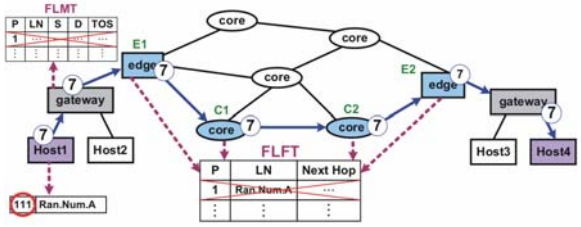


Fig. 7: Termination Scenario

This mechanism uses FLMT and FLFT respectively in gateway and router. This is because the bottleneck easily occurs in gateway link. The proposed mechanism not only improves the end-to-end QoS provisioning, but also eliminates the impact of bottleneck and reduces the load of edge router. FLMT and FLFT can use at the same time in edge router.

4. Simulation Results

The proposed mechanism is simulated in ns-2 network simulator. There are two cases in the different three (Best Effort, DiffServ, and Flow Label & DiffServ) mechanisms for the simulation as shown in Figure 8. There are only E1, E2, E3, C1, C2, C3 routers DiffServ-capable. The link between routers is 2 Mbps while host-to-gateway is 1.5 Mbps. S1 generates TCP traffic to D1, while S2 generates UDP traffic to D2. Each of S3-S10 generates 0.5 Mbps background traffic to D3-D10 to make network congestion occur.

Figure 9 shows the TCP results of throughput in the different three mechanisms, while Figure 10 is for UDP results. TCP uses sliding window to deliver more packets at once for TCP-Friendly. The half sliding window will be set by sender if sender detected network congestion occur. The TCP throughput fell down quickly during network congestion. This is why the TCP throughput in figure 9 is less than UDP

throughput in figure 10. Because of not all routers DiffServ-capable, the throughput will fell down quickly because of the packets even with high priority (DiffServ) have to contention the bandwidth as the Best Effort way at DiffServ-disable router during network congestion. The simulation results show the performance of the proposed end-to-end QoS provisioning by Flow Label & DiffServ mechanism is maintained during network congestion.

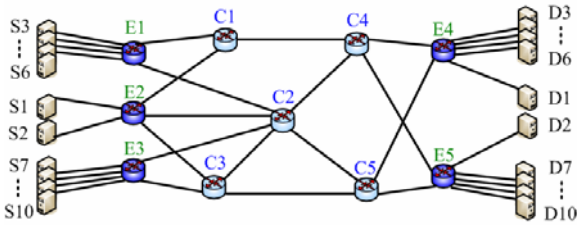


Fig. 8: The Simulated Network Topology

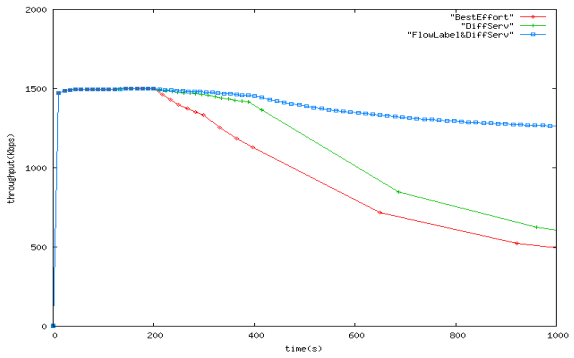


Fig. 9: The TCP Flow (throughput v.s. time)

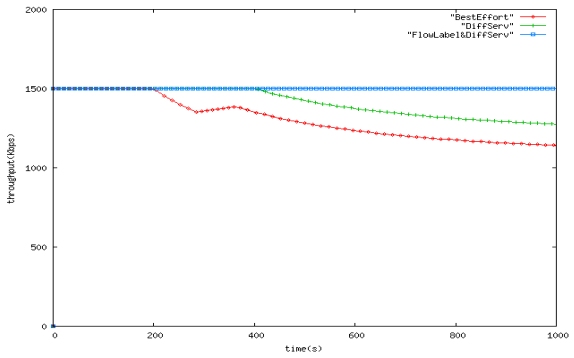


Fig. 10: The UDP Flow (throughput v.s. time)

5. Conclusions and Future Works

This paper proposes the end-to-end QoS provisioning mechanism by utilizing 3-tuple instead of 5-tuple in IPv6 header, i.e. using flow label and traffic class to reserve resources to achieve customized QoS provision. This proposes a solution for not all routers DiffServ-capable network to achieve end-to-end QoS provisioning. The mechanism can improve flow classification efficiently from 5-tuple in IPv4 header to 3-tuple in IPv6 header to lighten the load of edge router to make packet delivery faster. This is also simulated in ns-2 network simulator, and results show the performance of the proposed end-to-end QoS provisioning by Flow Label & DiffServ mechanism is maintained during network congestion. Our future works will focus on how to eliminate the packet loss during router or link failure, and how to make the bandwidth management to meet the user demand. Nowadays IPv4 activate since 1970s. How to utilize flow label for flow classification in the IPv4/IPv6 during IPv4/IPv6 transition time is a challenge [8].

6. References

[1] Wen-Shyang Hwang and Pei-Chen Tseng, “A QoS-aware Residential Gateway with Bandwidth Management,” IEEE Transactions on Consumer Electronics, pp. 840-848, Aug. 2005.

[2] Shu-Fen Tseng, His-Chieh Lee, Te-Ching Kung, Shou-Lien Chou, and Jing-Yi Chen, “The Development of Global IPv6 Products,” Proc. of the 19th International Conference on Advanced Information Networking and Applications, pp. 845-850, 2005.

[3] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6)”, IETF Network Working Group RFC 2460, 1998.

[4] K. Nichols, S. Blake, F. Baker, and D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, IETF Network Working Group RFC 2474, 1998.

[5] R. Banerjee, S. P. Malhotra, and M. Mahaveer, “A Modified Specification for Use of The IPv6 Flow Label for Providing An Efficient Quality of Service Using A Hybrid Approach”, IETF IPv6 Working Group Internet Draft, 2002.

[6] Guozhen Tan, Hengwei Yao, Yi Liu, and Ningning Han, “QoS Provision for IPv6 Traffic Using Dynamic Packet State”, Proc. of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services, pp. 23-28, Oct. 2005.

[7] J. Rajahalme, A. Conta, B. Carpenter, and S. Deering, “IPv6 Flow Label Specification”, IETF Network Working Group RFC 3697, 2004.

[8] T. Dreibholz, “An IPv4 Flow Label Option”, Network Working Group Internet Draft, 2005.