

# Implicit Admission Control for a Differentiated Services Network

Yuming Jiang, Anne Nevin, Peder J. Emstad  
Centre for Quantifiable Quality of Service in Communication Systems (Q2S)  
Department of Telematics  
Norwegian University of Science and Technology

Admission control is a crucial network element for providing quality of service (QoS) guarantees to multimedia and real time applications in the Internet. Most existing admission control approaches require the use of a signaling protocol to convey traffic information and service requirement of a flow to routers along its path (e.g. in Integrated Services networks) or to some central controllers (e.g. Bandwidth Brokers in Differentiated Services networks). This requirement has imposed significant constraints to customers and the network, and consequently limited its use [1].

This paper presents a framework approach, called implicit admission control (iAC), for admission control in a Differentiated Services (DiffServ) network. In this approach, no explicit signaling is used. Traffic information and service requirement of a flow are carried by each packet of the flow using the DiffServ field in the IP header. At each router, when the first packet of the flow is detected, the admission decision is made based on the traffic information and service requirement carried by the DiffServ field. The router rejects the flow simply by dropping its packets or the router may downgrade the flow to a lower priority level. In addition, to further simplify admission control procedure and make it scalable, two novel flow aggregation methods are adopted, which are link-based fair aggregation (LBFA) for deterministic QoS guarantee [2] and dynamic priority scheduling (DPS) for stochastic QoS guarantee [3]. Analytical results show that with these flow aggregation approaches, a newly admitted flow does not adversely affect QoS performance of existing flows. Consequently, with implicit admission control, the admission test is needed only for the new flow.

In this extended abstract, we focus on introducing the ideas of iAC and how it works. We shall include the detailed descriptions of LBFA and DPS and the detailed analysis in the full version.

The following introduces the requirements by the proposed iAC approach and the various operations involved in the approach. It is worth highlighting that their requirements are mostly supported by DiffServ.

First, the network under consideration is an access network supporting DiffServ. Under DiffServ, each packet is marked or remarked at the ingress router. The marking is based on the service level agreement between the user and the network. In the access network, an application of the user may mark its IP packets before sending them. This making at the user side can facilitate the network to differentiate packets that are from the same user but belong to different applications having different QoS requirements.

The marking information is carried by the DiffServ field in the IP header. The DiffServ field consists of a six-bit DiffServ codepoint (DSCP) and a two-bit currently unused (CU) field. The DSCP specifies the service class that the flow belongs to. To date, DiffServ has defined several service classes including the Expedited Forwarding (EF) class and the Assured Forwarding (AF) class groups in addition to the traditional Best Effort (BE) class. For iAC, we propose to use the two-bit CU field to represent four levels of (packet scale) peak rates:  $R$ ;  $R/n$ ;  $R/n^{**2}$ ;  $R/n^{**3}$ . Here  $R$  and  $n$  are two parameters made known to all the routers in the network, which determine how the four rate levels are chosen. They could be set by the network administrator or based on some empirical values. As an example, suppose all the input links of an ingress router have capacities less than  $10Mbps$ .  $R$  may be set to be  $8Mbps$  and  $n$  be 4. Under this setting, the four rate levels are respectively  $8Mbps$ ,  $2Mbps$ ,  $500Kbps$  and  $125Kbps$ .

Second, every ingress edge router knows the maximum total service rate that the network agrees to provide to the user. Also, it knows the allocation of this rate among the various DiffServ classes i.e. EF, AF and BE. In

addition, the edge router adopts a traffic conditioner for EF traffic from each user. The traffic conditioner uses a leaky bucket (LB) to enforce that the amount of EF traffic entering the network from the user does not exceed what the user has requested and is provided by the network. For this, the leaking rate of the LB is upper-bounded by the agreed maximum EF guaranteed rate that may be provided to the user. For example, suppose the link for a user connecting to the network has capacity *10Mbps* and the rate allocation among EF, AF and BE traffic from this user is 2:6:2. Then, the maximum total service rate that can be provided to the user is *10Mbps* and the maximum amount of EF traffic that may be sent by the user should be limited to *2Mbps* and is controlled by a leaky bucket having leaking rate of *2Mbps* at the ingress router.

Third, at each router, priority scheduling is adopted between EF, AF and BE traffic classes. In addition, link-based fair aggregation (LBFA) [2] is used to aggregate EF traffic and dynamic priority scheduling (DPS) [3] is used to aggregate AF traffic. The main idea of LBFA is to treat flows sharing the same edge-to-edge path as an aggregate, and merge such paths using a fair aggregator at each router if they share the same part of downstream path. The idea of DPS is to put the newly admitted flow at the lowest priority level. When a flow has been detected inactive for some time-out time, it is removed from the priority list. Implicitly, this increases by one priority level every flow admitted after the removed flow. Detailed introduction and analysis of LBFA and DPS can be found from [2] and [3] respectively. The analyses in [2][3] imply that a newly admitted flow does not adversely affect QoS performance of existing flows.

Fourth, admission test is performed at each router. The admission criterion used for EF traffic is the rate (and implicitly the delay). If the router has no enough unallocated rate for the EF class, the incoming request is rejected. Or, if agreed between the user and the network, the request is downgraded to the AF class, and an additional admission test for the downgraded AF flow is conducted. The admission criteria for AF traffic are stochastic delay and stochastic loss guarantees. If the incoming flow belongs to AF, the stochastic delay and loss guarantees provided to it are analyzed assuming the flow is admitted. The analysis is based on on-line measurements of existing EF and AF traffic. If these guarantees meet the service requirement implied by the DiffServ field in the IP header, the flow is admitted. Otherwise, the flow is rejected or downgraded to the BE class based on the agreement between the user and the network.

In summary, iAC is a simple framework for admission control. No requirement on signaling makes it easy to implement and scalable. This framework is built upon the following ideas.

- Adopt DiffServ as the service architecture for providing QoS guarantees. The service requirement of a flow is implied by the DSCP field.
- Use the CU field to support multiple rate levels that are further used as implicit traffic descriptors.
- Adopt priority scheduling between EF, AF and BE.
- Use LBFA to aggregate EF flows.
- Use DPS to aggregate AF flows.
- Admission test is performed at each router or may be performed only at the bottleneck router.

The differences between iAC and the existing AC approaches are two folds. Comparing with Bandwidth Broker approaches, iAC conducts admission control node-by-node, lets packets implicitly carry their QoS requirements and their corresponding flows' traffic information, and does not need any signaling. Comparing with the flow-aware networking approach, iAC supports multiple service levels, allows multiple rates used as implicit traffic descriptors, and is simpler to implement.

[1] J. W. Roberts. Internet Traffic, QoS, and Pricing. Proceedings of the IEEE, vol. 92, no. 9, Sept 2004.

[2] Y. Jiang. Link Based Fair Aggregation: A Simple Approach to Scalable Support of Per-Flow Service Guarantees. IFIP Networking 2004.

[3] Y. Jiang, P. J. Emstad, A. Nevin, et al. Measurement-Based Admission Control for a Flow-Aware Network. EuroNGI Conference on Next Generation Internet (NGI), 2005.