ELSEVIER

Computer Communications 24 (2001) 1626–1636

computer communications

www.elsevier.com/locate/comcom

Modeling and performance analysis for IPv6 traffic with multiple QoS classes

Liren Zhang*, Li Zheng

Network Technology Research Centre, School of Electrical and Electronic Engineering, Nanyang Technological University, Block S2, Singapore, Singapore 639798

Received 5 September 2000; revised 10 January 2001; accepted 10 January 2001

Abstract

This paper focuses on the modeling and performance analysis for IPv6 traffic with multi-class QoS in virtual private networks (VPN). The multi-class QoS is implemented on differentiated service basis using priority scheme of 4 bits defined in the packet header of IPv6. A VPN-enabled IP router is modeled as a tandem queuing system in which each output link consists of two parallel priority output queues. The high-priority queue is used to carry the delay sensitive traffic while the low-priority queue is used to carry the delay insensitive traffic. On the other hand, multiple thresholds are implemented in each queue, respectively, for packet loss priority control. The performance analysis is done using fluid flow techniques. The numerical results obtained from the analysis show that the differentiated service based on the priority schemes defined in IPv6 is able to effectively satisfy the multi-class QoS requirement for supporting multimedia services in VPN. The performance trade-off between the delay sensitive traffic and delay insensitive traffic in terms of traffic throughput, packet loss probability and end-to-end delay in VPN networks is presented. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Virtual private network; Quality of service; IPv6; Multimedia networking

1. Introduction

Currently, there is a significant interest in the development of virtual private network (VPN) over IP backbone. VPN is an enterprise network based on shared public network infrastructure but employing the same security, management and throughput policies as applied in a private network [13]. Comparing with the existing private networks, VPN is a more cost-effective mean of building and deploying private communication networks for multi-site communication, especially when IPv6 over broadband Internet is implemented. VPN is also able to support multimedia services such as voice, video, data and image transfer applications. For an IP-based VPN [16], the service provider connects multiple IP addresses located at geographically dispersed sites as appearing to be within a private network. As shown in Fig. 1, VPN can be implemented using VPN-enabled router [13] which plays the network layer functions in the TCP/IP protocol suite to support network security, network routing connectivity and QoS parameters.

One of the typical problems with the implementation of VPN over Internet is the difficulty of QoS guarantee. The Internet Engineering Task Force (IETF) has recommended a differentiated service mechanism for the traffic with different QoS requirement on priority basis [17,18]. IPv6 [2] is ideally designed for supporting such differentiated services [17]. However, in current IP-based networks, when the data are encrypted, it may be difficult for the network to determine the class-of-service based on packet content in the network layer, especially when a multiple class of QoS is involved. By contrast, this can be done in IP-based VPN which has the advantage that the class of service can be stated outside the VPN envelop of the IP packets [15]. Current QoS issues involved in VPN mainly focus on call admission control level [20,21] to determine the network ability for assigning network resources to mission-critical or delay-sensitive services while limiting resources committed to low-priority traffic as an essential component of VPN solution. According to service level agreements (SLA), IP traffic with multi-class of QoS from different users are classified and stored in separate buffers before they are transmitted in the network. The disadvantages of such mechanism are that (1) it complicates the implementation using separate buffers for different QoS classes, (2) the buffer utilization is inferior and (3) the re-sequencing is required at the destination which is highly undesirable for the traffic with different QoS classes but from the same user source.

* Corresponding author. Tel: +65-790-4508; fax: +65-792-0415.
E-mail address: elzhang@ntu.edu.sg (L. Zhang).

PII: S0140-3664(01)00313-9

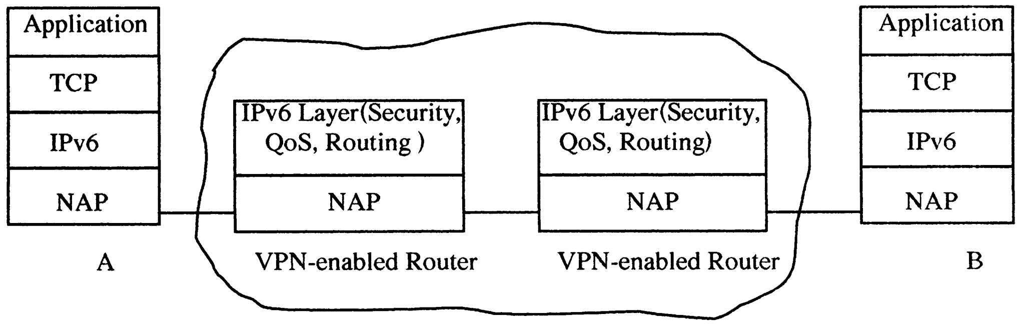

Fig. 1. VPN over IP backbone.

This paper focuses on the issues to improve QoS at IP packet level. The multi-class QoS is implemented on differentiated service basis using priority scheme of 4 bits defined in the packet header of IPv6. A VPN-enabled IP router is modeled as a tandem queuing system in which each output link consists of two space-priority output queues. The high priority queue is used to carry the delay sensitive traffic while the low priority queue for the delay insensitive traffic. On the other hand, multiple thresholds are implemented in each queue, respectively, for packet loss priority control [7]. The performance analysis is done using fluid flow technique [10,11]. The evaluation focuses on the performance trade-off between the delay sensitive traffic and delay insensitive traffic in terms of traffic throughput, packet loss probability and end-to-end delay in VPN networks are also presented.

2. Multi-class QoS support in IP-based VPN

Since QoS control on call admission basis in VPN is enable to provide services with multi-class QoS by assigning the network resources on service application basis such as IP telephony, e-commerce, IP video, and other multimedia offerings. However, in mega-scale VPNs, when IP traffic flows increase in carrier-sized networks, QoS guarantee on flow-by-flow basis only at the call admission level is impractical [14]. One of the key alternative solutions is to implement multiple QoS classes at IP level. The IP-level QoS mechanism is to provide variable grade of service with performance guarantees to the heterogeneous mixture of the traffic flows. Currently, although IPv4 traffic has already run over Internet, however, it is still not able to fully and efficiently support the critical application traffics with different QoS requirements. As a natural increment to IPv4 [19], IPv6 is not only able to inter-operate with the current IPv4 but also able to run well in broadband networks to provide a

Table 1
Recommended priority values in IPv6 for application categories

Priority	Application category
0	Uncharacterized traffic
1	‘Filler’ traffic (e.g. netnews)
2	Unattended data transfer (e.g. email)
3	(Reserved)
4	Attended bulk transfer (e.g. FTP, HTTP, NFS)
5	(Reserved)
6	Interactive traffic (e.g. telnet, X)
7	Internet control traffic (e.g. routing protocols, SNMP)

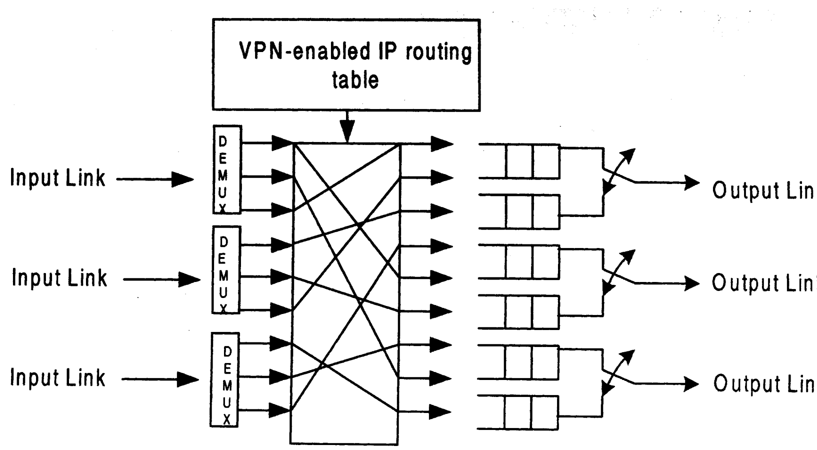

Fig. 2. Modeling of a VPN-enabled IP Router.