QoS for Aggregated Flows in VPNs

Authors: Pratik Bose, Dan Voce and Dilip Gokhale
Lockheed Martin Integrated Systems & Solutions,
22300 Comsat Drive, Clarksburg, MD USA, 20871

Abstract.: Aggregation of flows is a natural consequence of the transition of flows across multiple network domains. The quality of service that is provided to an aggregated flow is dependent on a sufficient set of individual flow characteristics correctly transformed in to the aggregated flow characteristics. VPN routers at the boundary of the private networks encrypt information within the data packets of a flow and flow characteristics are no longer visible to the interface domain. This document describes the challenges faced by QoS mechanisms to provide quality of service to secure aggregated flows.

INTRODUCTION

A simplified view of heterogeneous networks being designed today consists of high data rate (in Gbps) user networks which connect to backbone network service providers. The user networks are expected to consist of both wireless and optical infrastructure. A typical characteristic of the user networks is the presence of Virtual Private Network (VPN) routers which encrypt data intended for authenticated user network peers prior to injecting it into the backbone network. The backbone networks provide transport to these encrypted and encapsulated data packets to other user networks where peer VPN routers decrypt the information for end hosts.

The Quality of Service (QoS) is provided to the user network for typical parameters such as delay, delay variation, packet loss, throughput and service Availability. At the edge of the user network and backbone network microflows are aggregated based on flows which share similar parameters. The key issue is offering network service guarantees for one or more elevated classes of traffic for these encrypted flows. As evident, the user network must provide sufficient information to the backbone network about the QoS desired for the encrypted flow. Another key issue is to preempt lower priority flows to accommodate higher priority flows.

Shortcomings in Current Architectures

Differentiated Services

The DiffServ architecture naturally aggregates different application data into an IP flow with a single DSCP (for ex, voice data is typically marked with the Expedited Forwarding DSCP). The aggregate of say, all voice flows in the backbone

network using the DSCP does not provide sufficient information to distinguish between different application data types and the priority of a microflow within an aggregate.

Different recommendations have been made to provide higher QoS fidelity in the DiffServ architecture. These primarily have been based on traffic conditioning using additional parameters such as the source and the destination address of the flow; assigning additional DSCPs to distinguish between applications and flow priorities; congestion notification and bandwidth management

These methods however, do not provide sufficient guarantees that may be required by the user network for certain critical flows.

IntServ, RSVP and Aggregate RSVP

The IntServ framework was developed to provide QoS guarantees on a per-microflow basis. The key building blocks to an IntServ architecture are (a) admission control and (b) a resource reservation protocol that performs resource reservation once a flow is admitted. This model is extended to support the mapping of QoS classes to a DSCP in Aggregate RSVP

Aggregation with RSVP combining the aggregation of DiffServ is described in RFC 3175 which proposes a scheme to aggregate multiple RSVP reservations across a transit region (called an aggregation region) into a single reservation request.

Flow Based Networking

[1] proposes a new QoS signaling standard for use within IPv6 to permit the complete specification of the Quality of Service of a flow (or a group of flows) in-band in a hop-by-hop option field. This permits the QoS to be setup in real time by router hardware without a separate signaling message structure like RSVP. The QoS request and response are incorporated into the data flow packet headers so that the QoS can be setup during the first round trip.

QoS Challenges for Secure Aggregated Flows

The key challenges in providing QoS for secure aggregate flows using any of the architectures described in section 2 are as follows:

1. Signaling mechanisms between networks should sufficiently describe the desired QoS parameters without compromising the security of the flow.
2. Sufficient information must be provided to each network to enable the following QoS functions: Packet classification; Metering and shaping; Queue scheduling and management; and Priority and preemption.
3. The capability of VPN routers should be expanded such that these routers can participate in the QoS functions described in 2 above. The current capabilities of VPN routers are limited in this arena and secure flows are implemented as tunneled aggregates between VPN sites.
4. MLPP [2] defines a prioritized flow handling service where the relative importance of flows allows higher priority flows at the expense of lower

priority flows. RSVP provides a capability to signal priority preemption elements as defined in [20]. Preemption is applicable to emergency services as required by civilian and military networks.

5. The trust model of secure aggregation deems the network edge as an appropriate place to condition traffic. Traffic conditioning in the backbone may provide greater DiffServ QoS fidelity. However traffic conditioning in the backbone suffers from scalability issues.
6. QoS integration with the security model that is implemented by networks is necessary. Changes in VPN routing, authentication and encryption may affect the QoS of related flows. QoS functions must be capable of adapting to such changes emanating from the security function.
7. Scalability of an integrated QoS-security model also offers challenges that need to be addressed. As an example ARSVP can provide a combination of QoS aggregation and secure flow aggregation at VPN boundaries.

Emerging solutions

[3], [4] and [6] are examples of emerging solutions that address some of the requirements outlined in Section 3. [3] presents an architectural framework for nested VPN routers which participate in QoS signaling. [4] defines RSVP signaling at an IPSec router which can aggregate flows based on DSCP and security associations at the router. Further work is required to meet or exceed the requirements of QoS aggregation in secure networks.

CONCLUSION

A key consideration for heterogeneous networks of today and tomorrow is to support for QoS for secure aggregated flows. The applicability of different QoS approaches to the secure aggregate flows was described and their relative strengths and weaknesses with respect to meeting the functional requirements were evaluated. The optimal QoS solution must meet the challenges described in this paper and address the issues and constraints highlighted in this paper.

REFERENCES

[1] Lawrence G. Roberts, “QoS Signaling for IPv6 QoS Support”, TR-34.1.7/04.03.25.04, March 2004.

[2] International Telecommunications Union, “Multilevel Precedence and Preemption (MLPP)”, ITU-T Recommendation I.255.3, 1990.

[3] Fred Baker and Pratik Bose “QoS Signaling in a Nested Virtual Private Network” draft-baker-signaled-preemption-01.txt

[4] F Le, Faucheur et. al “Aggregate RSVP reservations for IPSec tunnels”

[5] Herzog – RFC 3181 - Signaled Preemption Priority Policy Element, October 2001

[6] James Polk et. al – “A Resource Reservation Extension for the Reduction of Bandwidth of A Reservation Flow” – draft-polk-tsvwg-rsvp-bw-reduction-00.txt.