INTERNET DRAFT
RSVP Working Group
draft-ietf-rsvp-tunnels-interop-00.txt

John J. Krawczyk
Bay Networks, Inc.

March 11, 1997
Expires: September, 1997

Designing Tunnels for Interoperability with RSVP

1. Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

2. Abstract

This memo provides information for designers of tunneling protocols that use IP-in-IP encapsulation. It describes how to design a tunnel header so that RSVP [RSVPv1] can be used to signal the Quality of Service requirements for individual flows within an IP-in-IP tunnel.

3. Introduction

There are many issues concerning the use of RSVP when data is encapsulated within IP-in-IP tunnels. This memo discusses the problem of classifying flows within a tunnel. It is hoped that this will aid those designing new tunneling mechanisms to make their proposals "RSVP friendly".

A problem with most of the existing IP-in-IP tunneling mechanisms is the inability to distinguish between flows within a tunnel based upon the tunnel "wrapper", or outer header. Therefore, while it is possible to make a reservation for the tunnel itself, all traffic in the tunnel is then treated in the same manner.

Performing classification based upon the tunnel payload is undesirable. Two major reasons are:

Examing additional fields in a packet can have severe performance penalties.

The payload may be encrypted.

Therefore, it is desirable to be able to distinguish flows based on fields in the encapsulating header. This memo explains how to design a tunnel header to meet this goal.

4. Requirements for an RSVP-Friendly Tunnel Header

We will assume here that any simplex IP-in-IP tunnel, unicast or multicast, can, at a minimum, be identified by the source and destination IP addresses and an IP protocol number [e.g., RFC2003]. In order to classify individual flows within a tunnel, at least one additional field is needed. To be compliant with RSVP version 1, the following alternatives can be considered:

UDP/TCP ports, or fields in the same location in the packet for protocols other than UDP and TCP.

For IPv6, the Flow ID.

Any mechanism compliant with the Generalized Port

Identifier as described in [RSVPIPSEC].

If classification on any other fields is desired, new RSVP SESSION and/or FILTER_SPEC / SENDER_TEMPLATE C-Types have to be defined.

5. An Example: UDP Encapsulation

A UDP encapsulation scheme would be compatible with RSVP version 1. A well-known port number is necessary for the UDP destination port field. Up to 65534 individual flows could then be multiplexed over the tunnel by using a different value for the UDP source port for each flow.

6. Security Considerations

Using a tunnel header as described in this document allows for a type of traffic pattern analysis. The required level of exposure may be acceptable in many situations because the actual source and destination of the traffic will not be visible if the end-to-end packet format does not make it so. If this exposure is unacceptable, per-flow classification is not possible.

7. References

[RSVPv1] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", Internet Draft draft-ietf-rsvp-spec-14.txt, November, 1996.

[RFC2003] C. Perkins, "IP Encapsulation within IP", IETF RFC 2003, October, 1996.

[RSVPIPSEC] L. Berger, T. O'Malley, "RSVP Extensions for IPSEC Data Flows", Internet Draft draft-berger-rsvp-ext-06.txt, Jan, 1997.

8. Author's Address

John J. Krawczyk
Bay Networks, Inc.
2 Federal Street
Billerica, MA 01821
+1-508-916-3811
jj@baynetworks.com