Network Working Group
Request for Comments: 2208
Category: Informational

A. Mankin, Ed.
USC/ISI
F. Baker
Cisco Systems
B. Braden
USC/ISI
S. Bradner
Harvard
M. O'Dell
UUNET Technologies
A. Romanow
Sun Microsystems
A. Weinrib
Intel Corporation
L. Zhang
UCLA

September 1997

Resource ReSerVation Protocol (RSVP) Version 1 Applicability Statement Some Guidelines on Deployment

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document describes the applicability of RSVP along with the Integrated Services protocols and other components of resource reservation and offers guidelines for deployment of resource reservation at this time. This document accompanies the first submission of RSVP and integrated services specifications onto the Internet standards track.

1. Introduction

RSVP [RFC 2205] is a unicast and multicast signalling protocol, designed to install and maintain reservation state information at each router along the path of a stream of data. The state handled by RSVP is defined by services [RFC 2211] and [RFC 2212] specified by the Integrated Services WG. These services and RSVP are being introduced to the IETF's standards track jointly. From henceforth, the acronym RSVP on its own is used as a shorthand for the signalling protocol combined with the integrated service specifications.

RSVP must be used in conjunction with several additional components, described in Table 1.

Table 1 Additional Components of Resource Reservation

1. Message formats in which parameters for desired services can be expressed. A proposed standard set of these formats is specified in [RFC 2210].

2. Router and host mechanisms (e.g. packet classification and scheduling, admission control algorithms) to implement one or both of the models [RFC 2211] and [RFC 2212], which are also in the standards track.

3. Message formats in which parameters for desired policies for admission control and resource use can be expressed. A small common subset of these formats for standards track is in the RSVP WG's charter. The Policy objects in the RSVP Protocol Specification are optional only at this time.

4. Diversely located mechanisms implementing desired admission control policy functions, including authorization and other security mechanisms.

In the presence of some form of each component in Table 1, RSVP-enabled applications can achieve differentiated qualities of service across IP networks. Networked multimedia applications, many of which require (or will benefit from) a predictable end-user experience, are likely to be initial users of RSVP-signalled services.

Because RSVP and the integrated services and other components listed in Table 1 mark a significant change to the service model of IP networks, RSVP has received considerable interest and press in advance of its release as a standards track RFC. At present, many vendors of operating systems and routers are incorporating RSVP and integrated services into their products for near-future availability. The goal of this applicability statement is to describe those uses of

the current RSVP specification that are known to be feasible, and to identify areas of limitation and ongoing chartered work addressing some of these limitations.

2. Issues Affecting Deployment of RSVP

Wide scale deployment of RSVP must be approached with care, as there remains a number of outstanding issues that may affect the success of deployment.

2.1. Scalability

The resource requirements (processing and storage) for running RSVP on a router increase proportionally with the number of separate sessions (i.e., RSVP reservations). Thus, supporting numerous small reservations on a high-bandwidth link may easily overly tax the routers and is inadvisable. Furthermore, implementing the packet classification and scheduling capabilities currently used to provide differentiated services for reserved flows may be very difficult for some router products or on some of their high-speed interfaces (e.g. OC-3 and above).

These scaling issues imply that it will generally not be appropriate to deploy RSVP on high-bandwidth backbones at the present time. Looking forward, the operators of such backbones will probably not choose to naively implement RSVP for each separate stream. Rather, techniques are being developed that will, at the "edge" of the backbone, aggregate together the streams that require special treatment. Within the backbone, various less costly approaches would then be used to set aside resources for the aggregate as a whole, as a way of meeting end-to-end requirements of individual flows.

In the near term, various vendors are likely to use diverse approaches to the aggregation of reservations. There is not currently chartered work in the IETF for development of standards in this space. A BOF, Future Directions of Differential Services, on April 7, 1997, at the Memphis IETF, is to consider the IETF’s next steps on this, among other issues. Public documentation of aggregation techniques and experience is encouraged.

2.2. Security Considerations

The RSVP WG submission for Proposed Standard includes two security-related documents [Baker96, RFC 2207]. [Baker96] addresses denial and hijacking or theft of service attacks. [RFC 2207] addresses RSVP mechanisms for data flows that themselves use IPSEC.

The first document is proposed to protect against spoofed reservation requests arriving at RSVP routers; such requests might be used to obtain service to unauthorized parties or to lock up network resources in a denial of service attack. Modified and spoofed reservation requests are detected by use of hop-by-hop MD5 checksums (in an Integrity Object) between RSVP neighbor routers. As described, RSVP hop-by-hop authentication assumes that key management and distribution for routers is resolved and deployed. Until an effective key infrastructure is in place, manually keyed session integrity might be used. In addition, [Baker96] may be updated with RFC 2085.

That RSVP needs an effective key infrastructure among routers is not unique to RSVP: it is widely acknowledged that there are numerous denial of service attacks on the routing infrastructure (quite independent of RSVP) that will only be resolved by deployment of a key infrastructure.

Theft of service risks will require the user to deploy with caution. An elementary precaution is to configure management logging of new and changed filter specifications in RSVP-enabled infrastructure, e.g. the newFlow trap [RFC 2206].

The Integrity object defined by [Baker96] may also play a role in policy control, as will be described in 2.3.

The second security-related document provides a mechanism for carrying flows in which the transport and user octets have been encrypted (RFC 1827). Although such encryption is highly beneficial to certain applications, it is not relevant to the functional security of RSVP or reservations.

The following section on Policy Control includes additional discussion of RSVP authorization security.

2.3. Policy Control

Policy control addresses the issue of who can, or cannot, make reservations once a reservation protocol can be used to set up unequal services.

Currently, the RSVP specification defines a mechanism for transporting policy information along with reservations. However, the specification does not define policies themselves. At present, vendors have stated that they will use the RSVP-defined mechanism to implement proprietary policies.

The RSVP WG is chartered to specify a simple standardized policy object and complete simple mechanisms for session use of the Integrity object in the near future. This applicability statement may be updated at the completion of the WG's charter.

Before any decision to deploy RSVP, it would be wise to ensure that the policy control available from a vendor is adequate for the intended usage. In addition to the lack of documented policy mechanisms in any of the policy areas (such as access control, authorization, and accounting), the community has little experience with describing, setting and controlling policies that limit Internet service. Therefore it is likely that vendor solutions will be revised often, particularly before the IETF has developed any policy specification.

3. Recommendations

Given the current form of the RSVP specifications, multimedia applications to be run within an intranet are likely to be the first to benefit from RSVP. SNA/DLSW is another "application" considered likely to benefit. Within the single or small number of related administrative domains of an intranet, scalability, security and access policy will be more manageable than in the global Internet, and risk will be more controllable. Use of RSVP and supporting components for small numbers of flows within a single Internet Service Provider is similar to an intranet use.

Current experience with RSVP has been collected only from test runs in limited testbeds and intranet deployment. We recommend that people begin to use RSVP in production intranet or limited ISP environments (as mentioned above), in which benefits can be realized without having to resolve some of the issues described in Section 2. To quote RFC 2026 about the use of Proposed Standard technology:

> Implementors should treat Proposed Standards as immature specifications. It is desirable to implement them in order to gain experience and to validate, test, and clarify the specification. However, since the content of Proposed Standards may be changed if problems are found or better solutions are identified, deploying implementations of such standards into a disruption-sensitive environment is not recommended.

General issues of scalability, security and policy control as outlined in Section 2 are the subjects of active research and development, as are a number of topics beyond this applicability statement, such as third-party setup of either reservations or differentiated service.

4. References

[Baker96] Baker, F., "RSVP Cryptographic Authentication", Work in Progress.

[RFC 2206], Baker, F. and J. Krawczyk, "RSVP Management Information Base", RFC 2206, September 1997.

[RFC 2207] Berger, L. and T. O'Malley, "RSVP Extensions for IPSEC Data Flows", RFC 2207, September 1997.

[RFC 2211] Wroclawski, J., "Specification of Controlled-Load Network Element Service", RFC 2211, September 1997.

[RFC 2212] Shenker, S., C. Partridge and R. Guerin, "Specification of Guaranteed Quality of Service", RFC 2212, September 1997.

[RFC 2205] Braden, R. Ed. et al, "Resource ReserVation Protocol -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC 2210] Wroclawski, J., "The Use of RSVP with IETF Integrated Services", RFC 2210, September 1997.

5. Authors' Addresses

Fred Baker
Cisco Systems
Phone: 408-526-4257
EMail: fred@cisco.com

Abel Weinrib
Intel Corporation
Phone: 503-264-8972
EMail: aweinrib@ibeam.intel.com

Bob Braden
USC/ISI
4676 Admiralty Way
Marina Del Rey, CA 90292
Phone: 310-822-1511
EMail: braden@isi.edu

Lixia Zhang
UCLA Computer Science Department
4531G Boelter Hall
Los Angeles, CA 90095-1596 USA
Phone: 310-825-2695
EMail: lixia@cs.ucla.edu

Scott Bradner
Harvard University
Phone: 617-495-3864
EMail: sob@harvard.edu

Allyn Romanow
Sun Microsystems
Phone: 415-786-5179
EMail: allyn@eng.sun.com

Michael O'Dell
UUNET Technologies
Phone: 703-206-5471
EMail: mo@uu.net

Allison Mankin
mankin@east.isi.edu