Network Working Group
Request for Comments: 3210
Category: Informational

D. Awduche
Movaz Networks
A. Hannan
Routingloop
X. Xiao
Photuris

December 2001

Applicability Statement for Extensions to RSVP for LSP-Tunnels

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.

Copyright Notice

Abstract

This memo discusses the applicability of "Extensions to RSVP (Resource ReSerVation Protocol) for LSP Tunnels". It highlights the protocol's principles of operation and describes the network context for which it was designed. Guidelines for deployment are offered and known protocol limitations are indicated. This document is intended to accompany the submission of "Extensions to RSVP for LSP Tunnels" onto the Internet standards track.

1.0 Introduction

Service providers and users have indicated that there is a great need for traffic engineering capabilities in IP networks. These traffic engineering capabilities can be based on Multiprotocol Label Switching (MPLS) and can be implemented on label switching routers (LSRs) from different vendors that interoperate using a common signaling and label distribution protocol. A description of the requirements for traffic engineering in MPLS based IP networks can be found in [2]. There is, therefore, a requirement for an open, non-proprietary, standards based signaling and label distribution protocol for the MPLS traffic engineering application that will allow label switching routers from different vendors to interoperate.

The "Extensions to RSVP for LSP tunnels" (RSVP-TE) specification [1] was developed by the IETF MPLS working group to address this requirement. RSVP-TE is a composition of several related proposals submitted to the IETF MPLS working group. It contains all the necessary objects, packet formats, and procedures required to establish and maintain explicit label switched paths (LSPs). Explicit LSPs are foundational to the traffic engineering application in MPLS based IP networks. Besides the traffic engineering application, the RSVP-TE specification may have other uses within the Internet.

This memo describes the applicability of the RSVP-TE specifications [1]. The protocol's principles of operation are highlighted, the network context for which it was developed is described, guidelines for deployment are offered, and known protocol limitations are indicated.

This applicability statement concerns only the use of RSVP to set up unicast LSP-tunnels. It is noted that not all of the features described in RFC2205 [3] are required to support the instantiation and maintenance of LSP-tunnels. Aspects related to the support of other features and capabilities of RSVP by an implementation that also supports LSP-tunnels are beyond the scope of this document. However, support of such additional features and capabilities should not introduce new security vulnerabilities in environments that only use RSVP to set up LSP-tunnels.

This applicability statement does not preclude the use of other signaling and label distribution protocols for the traffic engineering application in MPLS based networks. Service providers are free to deploy whatever signaling protocol that meets their needs.

In particular, CR-LDP [6] and RSVP-TE [1] are two signaling protocols that perform similar functions in MPLS networks. There is currently no consensus on which protocol is technically superior. Therefore, network administrators should make a choice between the two based upon their needs and particular situation.

2.0 Technical Overview of Extensions to RSVP for LSP Tunnels

The RSVP-TE specification extends the original RSVP protocol by giving it new capabilities that support the following functions in an MPLS domain:

(1) downstream-on-demand label distribution
(2) instantiation of explicit label switched paths
(3) allocation of network resources (e.g., bandwidth) to explicit LSPs
(4) rerouting of established LSP-tunnels in a smooth fashion using the concept of make-before-break

(5) tracking of the actual route traversed by an LSP-tunnel
(6) diagnostics on LSP-tunnels
(7) the concept of nodal abstraction
(8) preemption options that are administratively controllable

The RSVP-TE specification introduces several new RSVP objects, including the LABEL-REQUEST object, the RECORD-ROUTE object, the LABEL object, the EXPLICIT-ROUTE object, and new SESSION objects. New error messages are defined to provide notification of exception conditions. All of the new objects defined in RSVP-TE are optional with respect to the RSVP protocol, except the LABEL-REQUEST and LABEL objects, which are both mandatory for the establishment of LSP-tunnels.

Two fundamental aspects distinguish the RSVP-TE specification [1] from the original RSVP protocol [3].

The first distinguishing aspect is the fact that the RSVP-TE specification [1] is intended for use by label switching routers (as well as hosts) to establish and maintain LSP-tunnels and to reserve network resources for such LSP-tunnels. The original RSVP specification [3], on the other hand, was intended for use by hosts to request and reserve network resources for micro-flows.

The second distinguishing aspect is the fact that the RSVP-TE specification generalizes the concept of "RSVP flow." The RSVP-TE specification essentially allows an RSVP session to consist of an arbitrary aggregation of traffic (based on local policies) between the originating node of an LSP-tunnel and the egress node of the tunnel. To be definite, in the original RSVP protocol [3], a session was defined as a data flow with a particular destination and transport layer protocol. In the RSVP-TE specification, however, a session is implicitly defined as the set of packets that are assigned the same MPLS label value at the originating node of an LSP-tunnel. The assignment of labels to packets can be based on various criteria, and may even encompass all packets (or subsets thereof) between the endpoints of the LSP-tunnel. Because traffic is aggregated, the number of LSP-tunnels (hence the number of RSVP sessions) does not increase proportionally with the number of flows in the network. Therefore, the RSVP-TE specification [1] addresses a major scaling issue with the original RSVP protocol [3], namely the large amount of system resources that would otherwise be required to manage reservations and maintain state for potentially thousands or even millions of RSVP sessions at the micro-flow granularity.

The reader is referred to [1] for a technical description of the RSVP-TE protocol specification.

3.0 Applicability of Extensions to RSVP for LSP Tunnels

Use of RSVP-TE is appropriate in contexts where it is useful to establish and maintain explicit label switched paths in an MPLS network. LSP-tunnels may be instantiated for measurement purposes and/or for routing control purposes. They may also be instantiated for other administrative reasons.

For the measurement application, an LSP-tunnel can be used to capture various path statistics between its endpoints. This can be accomplished by associating various performance management and fault management functions with an LSP-tunnel, such as packet and byte counters. For example, an LSP-tunnel can be instantiated, with or without bandwidth allocation, solely for the purpose of monitoring traffic flow statistics between two label switching routers.

For the routing control application, LSP-tunnels can be used to forward subsets of traffic through paths that are independent of routes computed by conventional Interior Gateway Protocol (IGP) Shortest Path First (SPF) algorithms. This feature introduces significant flexibility into the routing function and allows policies to be implemented that can result in the performance optimization of operational networks. For example, using LSP-tunnels, traffic can be routed away from congested network resources onto relatively underutilized ones. More generally, load balancing policies can be actualized that increase the effective capacity of the network.

To further enhance the control application, RSVP-TE may be augmented with an ancillary constraint-based routing entity. This entity may compute explicit routes based on certain traffic attributes, while taking network constraints into account. Additionally, IGP link state advertisements may be extended to propagate new topology state information. This information can be used by the constraint-based routing entity to compute feasible routes. Furthermore, the IGP routing algorithm may itself be enhanced to take pre-established LSP-tunnels into consideration while building the routing table. All these augmentations are useful, but not mandatory. In fact, the RSVP-TE specification may be deployed in certain contexts without any of these additional components.

The capability to monitor point to point traffic statistics between two routers and the capability to control the forwarding paths of subsets of traffic through a given network topology together make the RSVP-TE specifications applicable and useful for traffic engineering within service provider networks.

These capabilities also make the RSVP-TE applicable, in some contexts, as a component of an MPLS based VPN provisioning framework.

It is significant that the MPLS architecture [4] states clearly that no single label distribution protocol is assumed for the MPLS technology. Therefore, as noted in the introduction, this applicability statement does not (and should not be construed to) prevent a label switching router from implementing other signaling and label distribution protocols that also support establishment of explicit LSPs and traffic engineering in MPLS networks.

4.0 Deployment and Policy Considerations

When deploying RSVP-TE, there should be well defined administrative policies governing the selection of nodes that will serve as endpoints for LSP-tunnels. Furthermore, when devising a virtual topology for LSP-tunnels, special consideration should be given to the tradeoff between the operational complexity associated with a large number of LSP-tunnels and the control granularity that large numbers of LSP-tunnels allow. Stated otherwise, a large number of LSP-tunnels allows greater control over the distribution of traffic across the network, but increases network operational complexity. In large networks, it may be advisable to start with a simple LSP-tunnel virtual topology and then introduce additional complexity based on observed or anticipated traffic flow patterns.

Administrative policies may also guide the amount of bandwidth to be allocated (if any) to each LSP-tunnel. Policies of this type may take into consideration empirical traffic statistics derived from the operational network in addition to other factors.

5.0 Limitations

The RSVP-TE specification supports only unicast LSP-tunnels. Multicast LSP-tunnels are not supported.

The RSVP-TE specification supports only unidirectional LSP-tunnels. Bidirectional LSP-tunnels are not supported.

The soft state nature of RSVP remains a source of concern because of the need to generate refresh messages periodically to maintain the state of established LSP-tunnels. This issue is addressed in several proposals that have been submitted to the RSVP working group (see e.g. [5]).

6.0 Conclusion

The applicability of the "Extensions to RSVP for LSP Tunnels" specification has been discussed in this document. The specification introduced several enhancements to the RSVP protocol, which make it applicable in contexts in which the original RSVP protocol would have been inappropriate. One context in which the RSVP-TE specification is particularly applicable is in traffic engineering in MPLS based IP networks.

7.0 Security Considerations

This document does not introduce new security issues. The RSVP-TE specification adds new opaque objects to RSVP. Therefore, the security considerations pertaining to the original RSVP protocol remain relevant. When deployed in service provider networks, it is mandatory to ensure that only authorized entities are permitted to initiate establishment of LSP-tunnels.

8.0 Acknowledgments

The authors gratefully acknowledge the useful comments received from the following individuals during initial review of this memo in the MPLS WG mailing list: Eric Gray, John Renwick, and George Swallow.

9.0 References

[1] Awduche, D., Berger, L., Gan, D., Li, T., Swallow, G. and V. Srinivasan, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC 3209, December 2001.

[2] Awduche, D., Malcolm, J., Agogbua, J., O'Dell, M. and J. McManus, "Requirements for Traffic Engineering Over MPLS," RFC 2702, September 1999.

[3] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1, Functional Specification", RFC 2205, September 1997.

[4] Rosen, E., Viswanathan, A. and R. Callon, "A Proposed Architecture for MPLS", RFC 3031, January 2001.

[5] Berger, L., Gan, D., Swallow, G., Pan, P., Tommasi, F. and S. Molendini, "RSVP Refresh Overhead Reduction Extensions", RFC 2961, April 2001.

[6] Jamoussi, B. et al, "Constraint-Based LSP Setup using LDP," Work in Progress.

10.0 Authors' Addresses

Daniel O. Awduche
Movaz Networks
7926 Jones Branch Drive, Suite 615
McLean, VA 22102

EMail: awduche@movaz.com
Voice: +1 703-298-5291

Alan Hannan
RoutingLoop
112 Falkirk Court
Sunnyvale, CA 94087

EMail: alan@routingloop.com
Voice: +1 408 666-2326

XiPeng Xiao
Photuris Inc.
2025 Stierlin Ct.
Mountain View, CA 94043

EMail: xxiao@photuris.com
Voice: +1 650-919-3215

11.0 Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.