Internet Draft
Updates: 3209
Category: Standards Track
Expiration Date: March 2, 2009

Lou Berger (LabN)
Dimitri Papadimitriou (Alcatel Lucent)
JP. Vasseur (Cisco)

**September 2, 2008**

# PathErr Message Triggered MPLS and GMPLS LSP Reroute

draft-ietf-mpls-gmpls-lsp-reroute-01.txt

## Status of this Memo



## Copyright Notice



## Abstract

This document describes how Resource ReserVation Protocol (RSVP) PathErr Messages may be used to trigger rerouting of Multi-Protocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Traffic Engineering (TE) Label Switched Paths (LSPs) without first removing LSP state or resources. Such LSP rerouting may be desirable in a number of cases including, for example, soft-preemption and graceful shutdown. This document describes the usage of existing Standards Track mechanisms to support LSP rerouting. In this case, it relies on mechanisms already defined as part of RSVP-TE and simply describes a sequence of actions to be executed. While existing protocol

definition can be used to support reroute applications, this document also defines a new reroute-specific error code to allow for the

future definition of reroute application-specific error values.

Table of Contents

## 1. Introduction

Resource ReserVation Protocol (RSVP), see [RFC2205], has been extended to support the control of Traffic Engineering (TE) Label Switched Paths (LSPs) for both Multi-Protocol Label Switching (MPLS) and Generalized MPLS (GMPLS) in, respectively, [RFC3209] and [RFC3473]. In all cases, a PathErr message is used to report errors to nodes upstream of the error detecting node. As defined in [RFC2205], and left unmodified by [RFC3209], PathErr messages "do not change path state in the nodes through which they pass". Notwithstanding this definition, PathErr messages are most commonly used to report errors during LSP establishment, i.e. the RSVP-TE processing that occurs prior to the ingress receiving a Resv message. (See [PATHERR] for a broader discussion on PathErr message handling.) Support for such usage was enhanced via the introduction of the Path_State_Removed flag in [RFC3473], which enables a processing node to free related LSP state and resources. The usage of PathErr messages during LSP establishment was further covered in [RFC4920] which describes in detail how a node may indicate that the node or one of its associated resources should be avoided, i.e., routed around, during LSP establishment.

PathErr messages can also be used to support a number of other cases that can occur after an LSP is established. This document focuses on the cases where PathErr messages can be used for a node to indicate that it desires an upstream node to reroute an LSP around the indicating node or a resources associated with the indicating node. Some examples of such cases are soft-preemption and graceful shutdown. (See [PREEMPTION] and [GRACEFUL]).

This document uses the terminology "reroute request" to refer to the indication by a node that an upstream reroute should take place. This document how a node can initiate a reroute request without disrupting LSP data traffic or, when so desired, with the disruption of data traffic and removal of LSP associated state and resources.

The mechanisms used to indicate reroute requests are derived from the mechanisms described in [RFC4920], and the error codes defined in [RFC4736]. This document describes (1) how a non-disruptive reroute request may be issued and, (2) based on an optional "timeout" period, how rerouting may be forced by removing LSP state and associated resources and signaling such removal. While this document describes how existing protocol definitions can be used to support rerouting, it also defines a new reroute-specific error code to allow for the future definition of reroute application-specific error values.

### 1.1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 2. Reroute Requests

This section describes how a downstream node can indicate that it desires a node upstream (along the LSP path) to initiate the re-routing of an LSP, and how the upstream nodes can respond to such a request. Initiating nodes, transit nodes, and ingress nodes are described separately.

### 2.1. Processing at Requesting Node

When a transit or egress node desires to request the rerouting of an established LSP, it first determines if it can act on the reroute request locally. A reroute request SHOULD be acted on locally if the ERO received in the LSP's incoming Path message does not precluded the reroute and the node's policy allows local repair. Examples of reroute requests that may be permissible are reroutes avoiding outgoing interface, component, label resource, or next hops not explicitly listed in the ERO. When the reroute request can be processed locally, standard local repair processing MUST be followed. The node SHOULD limit the number of local repair attempts. The expected norm is for local repair and, thereby, this case to be precluded by policy.

When the requesting node cannot act on a reroute request locally, it MUST issue a PathErr message indicating a reroute request. A reroute request MUST be indicated via one of the following combinations of error codes and error values:

1. "Notify/Local node maintenance required" to support backwards compatibility and to reroute around the local node.

2. "Notify/Local link maintenance required" to support backwards compatibility and to reroute around a local interface.

3. "Reroute/<any Reroute error value>" for future compatibility and when backwards compatibility is not a concern.

The rest of the ERROR_SPEC object is constructed based on the local reroute request. When the local reroute request directs a reroute around the local node, the local node MUST be indicated in the

ERROR_SPEC object. When the local request does not direct to reroute around the local node, the impacted interface MUST be indicated in the ERROR_SPEC object. The IF_ID ERROR_SPEC SHOULD also be used when supported. The TLVs defined in [RFC4920] MAY also be used when supported and when they can provide specific additional reroute request information, e.g., reroute around a specific label. The principles related to ERROR_SPEC object construction defined in section 6.3.1. of [RFC4920] SHOULD be followed.

### 2.1.1. Reroute Request Timeouts

Reroute request timeouts are used to remove an LSP when there is no response to a reroute request. Reroute request timeouts MUST NOT be used, when the LSP is not to be removed at the expiration of the Reroute request timeout period. When such LSP removal is desired and after initiating a reroute request, the initiating node MUST initiate a timeout during which it expects to receive a response to the reroute request. Valid responses are a PathTear message or a trigger Path message with an ERO avoiding the resource that was indicated in the reroute request. If either type of message is received, the timeout period MUST be canceled and no further action is needed. Note, normal refresh processing is not modified by the introduction of reroute request timeouts. Such processing may result in Path state being removed during the timeout period, in which case the timeout period MUST also be canceled.

If the reroute request timeout is reached, the initiating node MUST remove the LSP and its associated state and resources. Removal of LSP state is indicated downstream via a corresponding PathTear message. Removal is indicated upstream via a PathErr message with the error code of "Service preempted". The Path_State_Removed flag MUST be set if supported. When the Path_State_Removed flag is not supported, a corresponding ResvTear MUST also be sent.

## 2.2. Processing at Upstream Node

When a transit node's policy permits it to support reroute request processing and local repair, the node MUST examine incoming PathErr messages to see it the node can perform a requested reroute. A reroute request is indicated in a received PathErr message which carries one of the error code and value combinations listed above in Section 2.1. Note that a conformant implementation MUST check for any of the the three combinations listed in Section 2.1.

A transit node MAY act on a reroute request locally when the ERO received in the LSP's incoming Path message does not precluded the

reroute. As before, examples include loosely routed LSP next hops. When the reroute request can be processed locally, standard local repair processing MUST be followed. The node SHOULD limit the number of local repair attempts. Again, the expected norm is for local repair and, thereby, this case to be precluded due to policy.

When the transit node supports [RFC4920], is a boundary node and Boundary Re-routing is allowed, it SHOULD use a route request as a trigger to reroute the LSP. (Per [RFC4920], the Flags field of the LSP_ATTRIBUTES object of the initial Path message indicate "Boundary re-routing".) In the case the node triggers rerouting, it first MUST identify an alternate path within the domain. When such a path is available, the node MUST terminate the PathErr message and issue a Path message reflecting the identified alternate path. Processing then continues per [RFC4920]. When an alternate path is note available, the node cannot act on the reroute request.

When a transit node node cannot act on a reroute request locally, per standard processing, it MUST propagate the received PathErr message to the previous hop.

## 2.3. Processing at Ingress

When reroute processing is supported, an ingress node MUST check received PathErr messages to identify them as indicating reroute requests. A reroute request is indicated in a received PathErr message which carries one of the error code and value combinations listed above in Section 2.1. Note that a conformant implementation MUST check for any of the the three combinations listed in Section 2.1.

Upon receiving a reroute request, the ingress MUST attempt to identify an alternate path, avoiding the node, interface, resource, etc. identified within the ERROR_SPEC object. When an alternate path cannot be identified the reroute request MUST be discarded. When an alternate path is identified, a corresponding make-before-break LSP SHOULD be initiated, and standard make-before-break procedures MUST be followed.

# 3. IANA Considerations

IANA is requested to administer assignment of new values for namespaces defined in this document and reviewed in this section.

Upon approval of this document, the IANA will make the assignment in the "Error Codes and Globally-Defined Error Value Sub-Codes" section

of the "RSVP Parameters" registry located at http://www.iana.org/assignments/rsvp-parameters:

34* Reroute [This document]

This Error Code has the following defined Error Value sub-code:

0 = Generic LSP reroute request

Reroute error values should be allocated based on the following allocation policy as defined in [RFC5226].

| Range | Registration Procedures |
|---|---|
| 0-32767 | IETF Consensus |
| 32768-65535 | Private Use |

(*) Suggested value.

## 4. Security Considerations

This document introduces no new security considerations as this document describes usage of existing formats and mechanisms. This document does introduce a new error code value, but this value is functionally equivalent to existing semantics. The Section 9 of [RFC4920] and [RFC4736] should be used as the starting point for reviewing the security considerations related to the formats and mechanisms discussed in this document.

## 5. References

### 5.1. Normative References

[RFC2205] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1, Functional Specification", RFC 2205, September 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V. and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3473] Berger, L., Editor, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling - Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC4920] Farrel, A., Ed., "Crankback Signaling Extensions for MPLS and GMPLS RSVP-TE", RFC 4920, July 2007.

[RFC5226] Narten, T., Alvestrand, H., "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

### 5.2. Informative References

[RFC4736] Vasseur, JP., et al, "Reoptimization of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Loosely Routed Label Switched Path (LSP)", RFC 4736, November 2006.

[GRACEFUL] Ali, Z., et al., "Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks", draft-ietf-ccamp-mpls-graceful-shutdown-06.txt, Work in Progress, July 2008

[PATHERR] Vasseur, JP., Ed. "Node behavior upon originating and receiving Resource ReserVation Protocol (RSVP) Path Error message", draft-ietf-mpls-3209-patherr-03.txt, Work in Progress, August 2008.

[PREEMPTION] Meyer, M., Ed. "MPLS Traffic Engineering Soft Preemption", draft-ietf-mpls-soft-preemption-12.txt, Work in Progress, September 2008.

## 6. Acknowledgments

This document was conceived along with Matthew Meyer.

## 7. Author's Addresses

Lou Berger
LabN Consulting, L.L.C.
Phone: +1-301-468-9228
Email: lberger@labn.net

Dimitri Papadimitriou
Alcatel Lucent
Francis Wellesplein 1,
B-2018 Antwerpen, Belgium
Phone: +32 3 240-8491
Email: Dimitri.Papadimitriou@alcatel-lucent.be

JP Vasseur
Cisco Systems, Inc
1414 Massachusetts Avenue
Boxborough, MA 01719
USA
Email: jpv@cisco.com

## 8. Full Copyright Statement



## 9. Intellectual Property

## Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

Generated on: Tue Sep 2 13:05:25 EDT 2008