

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: February 27, 2015

F. Zhang, Ed.  
Huawei  
O. Gonzalez de Dios, Ed.  
Telefonica Global CTO  
D. Li  
Huawei  
C. Margaria

M. Hartley  
Z. Ali  
Cisco  
August 26, 2014

**RSVP-TE Extensions for Collecting SRLG Information**  
**draft-ietf-ccamp-rsvp-te-srlg-collect-07**

Abstract

This document provides extensions for the Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) to support automatic collection of Shared Risk Link Group (SRLG) Information for the TE link formed by a LSP.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on February 27, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">2</a>
<a href="#">2.</a>	<a href="#">Requirements Language . . . . .</a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">RSVP-TE Requirements . . . . .</a>	<a href="#">3</a>
<a href="#">3.1.</a>	<a href="#">SRLG Collection Indication . . . . .</a>	<a href="#">3</a>
<a href="#">3.2.</a>	<a href="#">SRLG Collection . . . . .</a>	<a href="#">3</a>
<a href="#">3.3.</a>	<a href="#">SRLG Update . . . . .</a>	<a href="#">3</a>
<a href="#">4.</a>	<a href="#">Encodings . . . . .</a>	<a href="#">3</a>
<a href="#">4.1.</a>	<a href="#">SRLG Collection Flag . . . . .</a>	<a href="#">3</a>
<a href="#">4.2.</a>	<a href="#">SRLG sub-object . . . . .</a>	<a href="#">4</a>
<a href="#">5.</a>	<a href="#">Signaling Procedures . . . . .</a>	<a href="#">5</a>
<a href="#">5.1.</a>	<a href="#">SRLG Collection . . . . .</a>	<a href="#">5</a>
<a href="#">5.2.</a>	<a href="#">SRLG Update . . . . .</a>	<a href="#">7</a>
<a href="#">5.3.</a>	<a href="#">Compatibility . . . . .</a>	<a href="#">7</a>
<a href="#">6.</a>	<a href="#">Manageability Considerations . . . . .</a>	<a href="#">7</a>
<a href="#">6.1.</a>	<a href="#">Policy Configuration . . . . .</a>	<a href="#">7</a>
<a href="#">6.2.</a>	<a href="#">Coherent SRLG IDs . . . . .</a>	<a href="#">8</a>
<a href="#">7.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">8</a>
<a href="#">8.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">8</a>
<a href="#">8.1.</a>	<a href="#">RSVP Attribute Bit Flags . . . . .</a>	<a href="#">8</a>
<a href="#">8.2.</a>	<a href="#">ROUTE_RECORD Object . . . . .</a>	<a href="#">9</a>
<a href="#">8.3.</a>	<a href="#">Policy Control Failure Error subcodes . . . . .</a>	<a href="#">9</a>
<a href="#">9.</a>	<a href="#">Acknowledgements . . . . .</a>	<a href="#">9</a>
<a href="#">10.</a>	<a href="#">References . . . . .</a>	<a href="#">10</a>
<a href="#">10.1.</a>	<a href="#">Normative References . . . . .</a>	<a href="#">10</a>
<a href="#">10.2.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">10</a>
	<a href="#">Authors' Addresses . . . . .</a>	<a href="#">10</a>

## [1.](#) Introduction

It is important to understand which TE links in the network might be at risk from the same failures. In this sense, a set of links may constitute a 'shared risk link group' (SRLG) if they share a resource whose failure may affect all links in the set [[RFC4202](#)].

On the other hand, as described in [[RFC4206](#)] and [[RFC6107](#)], H-LSP (Hierarchical LSP) or S-LSP (stitched LSP) can be used for carrying one or more other LSPs. Both of the H-LSP and S-LSP can be formed as



a TE link. In such cases, it is important to know the SRLG information of the LSPs that will be used to carry further LSPs.

This document provides an automatic mechanism to collect the SRLG for the TE link formed by a LSP. Note that how to use the collected SRLG information is out of scope of this document

## **2. Requirements Language**

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 [RFC 2119](#) [[RFC2119](#)].

## **3. RSVP-TE Requirements**

### **3.1. SRLG Collection Indication**

The ingress nodes of the LSP must be capable of indicating whether the SRLG information of the LSP should be collected during the signaling procedure of setting up an LSP. SRLG information SHOULD NOT be collected without an explicit request for it being made by the ingress node.

### **3.2. SRLG Collection**

If requested, the SRLG information should be collected during the setup of an LSP. The endpoints of the LSP may use the collected SRLG information and use it for routing, sharing and TE link configuration purposes.

### **3.3. SRLG Update**

When the SRLG information of an existing LSP for which SRLG information was collected during signaling changes, the relevant nodes of the LSP must be capable of updating the SRLG information of the LSP. This means that the signaling procedure must be capable of updating the new SRLG information.

## **4. Encodings**

### **4.1. SRLG Collection Flag**

In order to indicate nodes that SRLG collection is desired, this document defines a new flag in the Attribute Flags TLV, which is carried in an LSP\_REQUIRED\_ATTRIBUTES or LSP\_ATTRIBUTE Object:

- o Bit Number (to be assigned by IANA, early allocation requested, see [Section 8.1](#) for more details): SRLG Collection flag







As described in [RFC 3209](#) [[RFC3209](#)], the RECORD\_ROUTE object is managed as a stack. The SRLG sub-object SHOULD be pushed by the node before the node IP address or link identifier. The SRLG-sub-object SHOULD be pushed after the Attribute subobject, if present, and after the LABEL subobject, if requested.

[RFC 5553](#) [[RFC5553](#)] describes mechanisms to carry a PKS (Path Key Sub-object) in the RRO so as to facilitate confidentiality in the signaling of inter-domain TE LSPs, and allows the path segment that needs to be hidden (that is, a Confidential Path Segment (CPS)) to be replaced in the RRO with a PKS. If the CPS contains SRLG Sub-objects, these MAY be retained in the RRO by adding them again after the PKS Sub-object in the RRO.

A node MUST NOT push a SRLG sub-object in the RECORD\_ROUTE without also pushing either a IPv4 sub-object, a IPv6 sub-object, a Unnumbered Interface ID sub-object or a Path Key sub-object.

The rules of the processing of the LSP\_REQUIRED\_ATTRIBUTES, LSP\_ATTRIBUTE and ROUTE\_RECORD Objects are not changed.

## **5. Signaling Procedures**

### **5.1. SRLG Collection**

Per [RFC 3209](#) [[RFC3209](#)], an ingress node initiates the recording of the route information of an LSP by adding a RRO to a Path message. If an ingress node also desires SRLG recording, it MUST set the SRLG Collection Flag in the Attribute Flags TLV which MAY be carried either in an LSP\_REQUIRED\_ATTRIBUTES Object when the collection is mandatory, or in an LSP\_ATTRIBUTES Object when the collection is desired, but not mandatory

When a node receives a Path message which carries an LSP\_REQUIRED\_ATTRIBUTES Object and the SRLG Collection Flag set, if local policy determines that the SRLG information is not to be provided to the endpoints, it MUST return a PathErr message with Error Code 2 (policy) and Error subcode "SRLG Recording Rejected" (value to be assigned by IANA, early allocation of the value requested, see [Section 8.3](#) for more details) to reject the Path message.

When a node receives a Path message which carries an LSP\_ATTRIBUTES Object and the SRLG Collection Flag set, if local policy determines that the SRLG information is not to be provided to the endpoints, the Path message SHOULD NOT be rejected due to SRLG recording restriction and the Path message SHOULD be forwarded without any SRLG sub-object(s) in the RRO of the corresponding outgoing Path message.





If local policy permits the recording of the SRLG information, the processing node SHOULD add local SRLG information, as defined below, to the RRO of the corresponding outgoing Path message. It then forwards the Path message to the next node in the downstream direction.

Following the steps described above, the intermediate nodes of the LSP can collect the SRLG information in the RRO during the processing of the Path message hop by hop. When the Path message arrives at the egress node, the egress node receives SRLG information in the RRO.

Per [RFC 3209](#) [[RFC3209](#)], when issuing a Resv message for a Path message which contains an RRO, an egress node initiates the RRO process by adding an RRO to the outgoing Resv message. The processing for RROs contained in Resv messages then mirrors that of the Path messages.

When a node receives a Resv message for an LSP for which SRLG Collection is specified, if local policy determines that the SRLG information is not to be provided to the endpoints, if the SRLG-recording request was in a LSP\_REQUIRED\_ATTRIBUTES object, then a ResvErr with Error code 2 (policy) and Error subcode "SRLG Recording Rejected" (value to be assigned by IANA, early allocation of the value requested, see [Section 8.3](#) for more details) MUST be sent. If the request was in a LSP\_ATTRIBUTES object, then a ResvErr SHOULD NOT be generated, but SRLG information MUST NOT be added in the RRO. When local policy allows recording SRLG information, the node SHOULD add SRLG information, as defined below, to the RRO of the corresponding outgoing Resv message. When the Resv message arrives at the ingress node, the ingress node can get the SRLG information from the RRO in the same way as the egress node.

Note that a link's SRLG information for the upstream direction cannot be assumed to be the same as that in the downstream.

- o For Path and Resv messages for a unidirectional LSP, a node SHOULD include SRLG sub-objects in the RRO for the downstream data link only.
- o For Path and Resv messages for a bidirectional LSP, a node SHOULD include SRLG sub-objects in the RRO for both the upstream data link and the downstream data link from the local node. In this case, the node MUST include the information in the same order for both Path messages and Resv messages. That is, the SRLG sub-object for the upstream link is added to the RRO before the SRLG sub-object for the downstream link.



Based on the above procedure, the endpoints can get the SRLG information automatically. Then the endpoints can for instance advertise it as a TE link to the routing instance based on the procedure described in [\[RFC6107\]](#) and configure the SRLG information of the FA automatically.

## **[5.2.](#) SRLG Update**

When the SRLG information of a link is changed, the LSPs using that link should be aware of the changes. The procedures defined in [Section 4.4.3 of RFC 3209](#) [\[RFC3209\]](#) MUST be used to refresh the SRLG information if the SRLG change is to be communicated to other nodes according to the local node's policy. If local policy is that the SRLG change should be suppressed or would result in no change to the previously signaled SRLG-list, the node SHOULD NOT send an update.

## **[5.3.](#) Compatibility**

A node that does not recognize the SRLG Collection Flag in the Attribute Flags TLV is expected to proceed as specified in [RFC 5420](#) [\[RFC5420\]](#). It is expected to pass the TLV on unaltered if it appears in a LSP\_ATTRIBUTES object, or reject the Path message with the appropriate Error Code and Value if it appears in a LSP\_REQUIRED\_ATTRIBUTES object.

A node that does not recognize the SRLG RRO sub-object is expected to behave as specified in [RFC 3209](#) [\[RFC3209\]](#): unrecognized subobjects are to be ignored and passed on unchanged.

## **[6.](#) Manageability Considerations**

### **[6.1.](#) Policy Configuration**

In a border node of inter-domain or inter-layer network, the following SRLG processing policy should be capable of being configured:

- o Whether the SRLG IDs of the domain or specific layer network can be exposed to the nodes outside the domain or layer network, or whether they should be summarized, mapped to values that are comprehensible to nodes outside the domain or layer network, or removed entirely.

A node using [RFC 5553](#) [\[RFC5553\]](#) and PKS may apply the same policy.



## **6.2. Coherent SRLG IDs**

In a multi-layer multi-domain scenario, SRLG ids may be configured by different management entities in each layer/domain. In such scenarios, maintaining a coherent set of SRLG IDs is a key requirement in order to be able to use the SRLG information properly. Thus, SRLG IDs must be unique. Note that current procedure is targeted towards a scenario where the different layers and domains belong to the same operator, or to several coordinated administrative groups. Ensuring the aforementioned coherence of SRLG IDs is beyond the scope of this document.

Further scenarios, where coherence in the SRLG IDs cannot be guaranteed are out of the scope of the present document and are left for further study.

## **7. Security Considerations**

This document builds on the mechanisms defined in [RFC3473], which also discusses related security measures. In addition, [RFC5920] provides an overview of security vulnerabilities and protection mechanisms for the GMPLS control plane. The procedures defined in this document permit the transfer of SRLG data between layers or domains during the signaling of LSPs, subject to policy at the layer or domain boundary. It is recommended that domain/layer boundary policies take the implications of releasing SRLG information into consideration and behave accordingly during LSP signaling.

## **8. IANA Considerations**

### **8.1. RSVP Attribute Bit Flags**

IANA has created a registry and manages the space of the Attribute bit flags of the Attribute Flags TLV, as described in [section 11.3 of RFC 5420](#) [RFC5420], in the "Attribute Flags" section of the "Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Parameters" registry located in <https://www.iana.org/assignments/rsvp-te-parameters/rsvp-te-parameters.xhtml>. It is requested that IANA makes an early allocation in the "Attribute Flags" section of the mentioned registry.

This document introduces a new Attribute Bit Flag:



Bit No	Name	Attribute Flags Path	Attribute Flags Resv	RRO	Reference
-----	-----	-----	-----	---	-----
TBD(early allocation requested)	SRLG collection Flag	Yes	Yes	Yes	This I-D

### 8.2. ROUTE\_RECORD Object

IANA manages the "RSVP PARAMETERS" registry located at <http://www.iana.org/assignments/rsvp-parameters>. We request IANA to make an early allocation in the Sub-object type 21 ROUTE\_RECORD - Type 1 Route Record registry

This document introduces a new RRO sub-object:

Value	Description	Reference
-----	-----	-----
TBD (early allocation requested, suggested value 34)	SRLG sub-object	This I-D

### 8.3. Policy Control Failure Error subcodes

IANA manages the assignments 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>. We request IANA to make an early allocation in the "Sub-Codes - 2 Policy Control Failure" subsection of the the "Error Codes and Globally-Defined Error Value Sub-Codes" section of the "RSVP PARAMETERS" registry.

This document introduces a new Policy Control Failure Error sub-code:

Value	Description	Reference
-----	-----	-----
TBD (early allocation requested)	SRLG Recording Rejected	This I-D

## 9. Acknowledgements

The authors would like to thank Igor Bryskin, Ramon Casellas, Lou Berger, Alan Davey and Dhruv Dhody for their useful comments and improvements to the document.





## **10. References**

### **10.1. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [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., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", [RFC 3473](#), January 2003.
- [RFC5420] Farrel, A., Papadimitriou, D., Vasseur, JP., and A. Ayyangarps, "Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)", [RFC 5420](#), February 2009.
- [RFC5553] Farrel, A., Bradford, R., and JP. Vasseur, "Resource Reservation Protocol (RSVP) Extensions for Path Key Support", [RFC 5553](#), May 2009.

### **10.2. Informative References**

- [RFC4202] Kompella, K. and Y. Rekhter, "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", [RFC 4202](#), October 2005.
- [RFC4206] Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", [RFC 4206](#), October 2005.
- [RFC5920] Fang, L., "Security Framework for MPLS and GMPLS Networks", [RFC 5920](#), July 2010.
- [RFC6107] Shiomoto, K. and A. Farrel, "Procedures for Dynamically Signaled Hierarchical Label Switched Paths", [RFC 6107](#), February 2011.

Authors' Addresses



Fatai Zhang (editor)  
Huawei  
F3-5-B RD Center  
Bantian, Longgang District, Shenzhen 518129  
P.R.China

Email: zhangfatai@huawei.com

Oscar Gonzalez de Dios (editor)  
Telefonica Global CTO  
Distrito Telefonica, edificio sur, Ronda de la Comunicacion 28045  
Madrid 28050  
Spain

Phone: +34 913129647  
Email: oscar.gonzalezdedios@telefonica.com

Dan Li  
Huawei  
F3-5-B RD Center  
Bantian, Longgang District, Shenzhen 518129  
P.R.China

Email: danli@huawei.com

Cyril Margaria  
Suite 4001, 200 Somerset Corporate Blvd.  
Bridgewater, NJ 08807  
US

Email: cyril.margaria@gmail.com

Matt Hartley  
Cisco

Email: mhartley@cisco.com

Zafar Ali  
Cisco

Email: zali@cisco.com

