IS-IS WG
Internet-Draft
Intended status: Standards Track
Expires: February 17, 2017

S. Hegde
C. Bowers
Juniper Networks
P. Mattes
M. Nanduri
Microsoft
I. Mohammad
Arista Networks
August 16, 2016

Advertising TE protocols in IS-IS
draft-hegde-isis-advertising-te-protocols-00

Abstract

This document defines a mechanism to indicate which traffic engineering protocols are enabled on a link in IS-IS. It does so by introducing a new traffic-engineering protocol sub-TLV for TLV-22. This document also describes mechanisms to address backward compatibility issues for implementations that have not yet been upgraded to software that understands this new sub-TLV.

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].

Copyright Notice

Table of Contents

1. Introduction

IS-IS extensions for traffic engineering are specified in [RFC5305]. [RFC5305] defines several link attributes such as administrative group, maximum link bandwidth, and shared risk link groups (SRLGs) which can be used by traffic engineering applications. Additional link attributes for traffic engineering have subsequently been defined in other documents as well. Most recently [RFC7810] defined link attributes for delay, loss, and measured bandwidth utilization.

The primary consumers of these traffic engineering link attributes have been RSVP-based applications that use the advertised link attributes to compute paths which will subsequently be signalled

using RSVP-TE. However, these traffic engineering link attributes have also been used by other applications, such as IP/LDP fast-reroute using loop-free alternates as described in [RFC7916]. In the future, it is likely that traffic engineering applications based on

Segment Routing [I-D.ietf-spring-segment-routing] will also use these link attributes.

Existing IS-IS standards do not provide a mechanism to explicitly indicate whether or not RSVP has been enabled on a link. Instead, different RSVP-TE implementations have used the presence of certain traffic engineering sub-TLVs in IS-IS to infer that RSVP signalling is enabled on a given link. A study was conducted with various vendor implementations to determine which traffic engineering sub-TLVs cause an implementation to infer that RSVP signalling is enabled on a link. The results are shown in Figure 1.

TLV/ sub-TLV	Sub-TLV name	X	Y	Z
22	Extended IS Reachability TLV	N	N	N
22/3	Administrative group (color)	N	Y	Y
22/4	Link Local/Remote ID	N	N	N
22/6	IPV4 Interface Address	N	N	N
22/8	IPV4 Neighbor Address	N	N	N
22/9	Max Link Bandwidth	N	Y	Y
22/10	Max Reservable Link Bandwidth	N	Y	Y
22/11	Unreserved Bandwidth	Y	Y	Y
22/14	Extended Admin Group	N	Y	N
22/18	TE Default Metric	N	N	N
22/20	Link Protection Type	N	Y	Y
22/21	Interface Switching Capability	N	Y	Y
22/22	TE Bandwidth Constraints	N	Y	Y
22/33-39	TE Metric Extensions(RFC7180)	N	N	N
138	SRLG TLV	N	Y	Y

Figure 1: Traffic engineering Sub-TLVs that cause implementation X, Y, or Z to infer that RSVP signalling is enabled on a link

The study indicates that the different implementations use the presence of different sub-TLVs under TLV 22 (or the presence of TLV 138) to infer that RSVP signalling is enabled on a link. It is possible that other implementations may use other sub-TLVs to infer that RSVP is enabled on a link.

This document defines a standard way to indicate whether or not RSVP, segment routing, or another future protocol is enabled on a link. In this way, implementations will not have to infer whether or not RSVP is enabled based on the presence of different sub-TLVs, but can use the explicit indication. When network operators want to use a non-

RSVP traffic engineering application (such as IP/LDP FRR or segment routing), they will be able to advertise traffic engineer sub-TLVs and explicitly indicate what traffic engineering protocols are enabled on a link.

2. Motivation

The motivation of this document is to provide a mechanism to advertise TE attributes for current and future applications without ambiguity. The following objectives help to accomplish this in a range of deployment scenarios.

1. Advertise TE attributes for the link for variety of applications.

2. Allow the solution to be backward compatible so that nodes that do not understand the new advertisement do not cause issues for existing RSVP deployment.

3. Allow the solution to be extensible for any new applications that need to look at TE attributes.

3. Solution

3.1. Traffic-engineering protocol sub-TLV

A new sub-TLV Traffic-engineering protocol sub-TLV is added in the TLV 22 [RFC5305] or TLV 222 to indicate the protocols enabled on the link. The sub-TLV has flags in the value field to indicate the protocol enabled on the link. The length field is variable to allow

the flags field to grow for future requirements.

```
 Type  : TBD suggested value 40
 Length: Variable
 Value :
   0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                             Flags                             |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Traffic-Engineering Protocol sub-TLV

Type : TBA (suggested value 40)

Length: variable (in bytes)

Value: The value field consists of bits indicating the protocols enabled on the link. This document defines the two protocol values below.

Value	Protocol Name
0x01	RSVP
0x02	Segment Routing

Figure 3: Flags for the protocols

The RSVP flag is set to one to indicate that RSVP-TE is enabled on a link. The RSVP flag is set to zero to indicate that RSVP-TE is not enabled on a link.

The Segment Routing flag is set to one to indicate that Segment Routing is enabled on a link. The Segment Routing flag is set to zero to indicate that Segment Routing is not enabled on a link.

All undefined flags MUST be set to zero on transmit and ignored on receipt.

An implementation that supports the TE protocol sub-TLV and sends TLV 22 MUST advertise the TE protocol sub-TLV in TLV 22 for that link, even when both the RSVP and SR flags are set to zero. This allows a receiving router to determine whether or not the sending router is capable of sending the TE protocol sub-TLV. It is used for backward compatibility as described in Section 4.

4. Backward compatibility

Routers running older software that do not understand the new Traffic-Engineering protocol sub-TLV will continue to interpret the presence of some sub-TLVs in TLV 22 or the presence of TLV 138 as meaning that RSVP is enabled a link. A network operator may not want to or be able to upgrade all routers in the domain at the same time. There are two backward compatibility scenarios to consider depending on whether the router that doesn't understand the new TE protocol sub-TLV is an RSVP-TE ingress router or an RSVP-TE transit router.

Suppose we have an upgraded transit router that explicitly indicates that RSVP is not enabled on a link by advertising the TE protocol sub-TLV with the RSVP flag set to zero. An RSVP-TE ingress router that has not been upgraded to understand the new TE protocol sub-TLV

will not understand that RSVP-TE is not enabled on the link, and may include the link on a path computed for RSVP-TE. When the network tries to signal an explicit path LSP using RSVP-TE through that link, it will fail. In order to avoid this scenario, an operator can use the mechanism described below.

For this scenario, the basic idea is to use the existing administrative group link attribute as a means of preventing existing RSVP implementations from using a link. The network operator defines an administrative group to mean that RSVP is not enabled on a link. We call this admin group the RSVP-not-enabled admin group. If the operator needs to advertise a TE sub-TLV (maximum link bandwidth, for example) on a link, but doesn't want to enable RSVP on that link, then the operator also advertises the RSVP-not-enabled admin group on that link. The operator can then use existing mechanisms to exclude

links advertising the RSVP-not-enabled admin group from the constrained shortest path first (CSPF) computation used by RSVP. This will prevent RSVP implementations from attempting to signal RSVP-TE LSPs across links that do not have RSVP enabled. Once the entire network domain is upgraded to understand the TE protocol sub-TLV in this draft, the configuration involving the RSVP-not-enabled admin group is no longer needed for this network.

The other scenario to consider is when the RSVP-TE ingress router has been upgraded to understand the TE protocol sub-TLV, but an RSVP-TE transit router has not. In this case, the transit router is not capable of sending the TE protocol sub-TLV. If the RSVP-TE ingress router understands that the transit router is not capable of sending the TE protocol sub-TLV, then it can continue inferring whether or not RSVP-TE is enabled on the transit router links based on the presence of TE sub-TLVs, as it does today. We require an upgraded router to send the TE protocol sub-TLV if it sends TLV 22, even when both the RSVP and SR flags are set to zero. This allows the receiving router to interpret the absence of the TE-protocol sub-TLV together with presence of TLV 22 to mean that the sending router has not been upgraded. This allows the upgraded RSVP-TE ingress router to distingish between transit routers that have been upgraded and those that haven't, and behave accordingly.

5. Security Considerations

This document does not introduce any further security issues other than those discussed in [RFC1195] and [RFC5305].

6. IANA Considerations

This specification updates one IS-IS registry:

The extended IS reachability TLV Registry

i) Traffic-engineering Protocol sub-tlv = Suggested value 40

7. Acknowledgements

The authors thank Alia Atlas and Les Ginsberg for helpful discissions on the topic of this draft.

8. References

8.1. Normative References

[I-D.ietf-spring-segment-routing]
Filsfils, C., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", draft-ietf-spring-segment-routing-09 (work in progress), July 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, DOI 10.17487/RFC5305, October 2008, <http://www.rfc-editor.org/info/rfc5305>.

[RFC7810] Previdi, S., Ed., Giacalone, S., Ward, D., Drake, J., and Q. Wu, "IS-IS Traffic Engineering (TE) Metric Extensions", RFC 7810, DOI 10.17487/RFC7810, May 2016, <http://www.rfc-editor.org/info/rfc7810>.

8.2. Informative References

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, DOI 10.17487/RFC1195, December 1990, <http://www.rfc-editor.org/info/rfc1195>.

[RFC7916] Litkowski, S., Ed., Decraene, B., Filsfils, C., Raza, K., Horneffer, M., and P. Sarkar, "Operational Management of Loop-Free Alternates", RFC 7916, DOI 10.17487/RFC7916, July 2016, <http://www.rfc-editor.org/info/rfc7916>.

Authors' Addresses

Shraddha Hegde
Juniper Networks
Embassy Business Park
Bangalore, KA 560093
India

Email: shraddha@juniper.net

Chris Bowers
Juniper Networks
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
US

Email: cbowers@juniper.net

Paul Mattes
Microsoft
One Microsoft Way
Redmond, WA 98052
US

Email: pamattes@microsoft.com

Mohan Nanduri
Microsoft
One Microsoft Way
Redmond, WA 98052
US

Email: mnanduri@microsoft.com

Imtiyaz Mohammad
Arista Networks
Global Tech Park
Bangalore, KA 560103
India

Email: imtiyaz@arista.com