Support for RSVP-TE in L3VPNs

draft-kumaki-murai-l3vpn-rsvp-te-02.txt

Abstract

IP Virtual Private Networks (VPNs) provide connectivity between sites across an IP backbone. These VPNs can be supported using BGP/MPLS and the connections can be created by using MPLS Traffic Engineered (TE) Label Switched Paths (LSPs).

In order to support multiple MPLS-TE based BGP/MPLS IP-VPNs that are interconnected via the same Provider Edge (PE) routers, new RSVP extensions are required. This document outlines the requirements and proposes a solution for interconnecting multiple BGP/IP-VPNs via the same Provider Edge router.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on January 4, 2012.
Copyright Notice

Copyright (c) 2011 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

1. Introduction
2. Motivation
   2.1 Network Example
3. Protocol Extensions and Procedures
   3.1 Object Definitions
      3.1.1 LSP_TUNNEL_VPN-IPv4 and LSP_TUNNEL_VPN-IPv6 SESSION Object
      3.1.2 LSP_TUNNEL_VPN-IPv4 and LSP_TUNNEL_VPN-IPv6 SENDER_TEMPLATE Objects
      3.1.3 LSP_TUNNEL_VPN-IPv4 and LSP_TUNNEL_VPN-IPv6 FILTER_SPEC Objects
      3.1.4 VPN-IPv4 and VPN-IPv6 RSVP_HOP Objects
   3.2 Handling
      3.2.1 Path Message Processing at Ingress PE
      3.2.2 Path Message Processing at Egress PE
      3.2.3 Resv Processing at Egress PE
      3.2.4 Resv Processing at Ingress PE
      3.2.5 Other RSVP Messages
4. Management Considerations
   4.1 Impact on Network Operation
5. Security Considerations
6. IANA Considerations
7. References
   7.1 Normative References
   7.2 Informative References
8. Acknowledgments
9. Author’s Addresses

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].
1. Introduction

Some Service Providers would like to use BGP/MPLS IP-VPNs to support connections between Customer Edge (CE) sites. These connections can be established using MPLS Traffic Engineered (TE) Label Switched Paths (LSPs). [RFC3209] defines extensions to RSVP for establishing a customer LSP using MPLS. In order to establish a customer MPLS-TE LSP over BGP/MPLS IP-VPNs, it is necessary for the RSVP control messages, including Path messages and Resv messages described in [RFC3209], to be appropriately handled by the Provider Edge (PE) routers. The requirements for supporting BGP/MPLS RSVP-TE based IP-VPNs are documented in [RFC5824].

[RFC6016] defines the new types of existing objects (i.e. SESSION, SENDER_TEMPLATE, FILTERSPEC and RSVP_HOP) described in [RFC2205] to establish reservations for customer flows in the context of a BGP/MPLS IP-VPNs. Section 7.4 (Support for CE-CE RSVP-TE) of [RFC6016], describes the procedure used in this draft.

In order to support multiple MPLS-TE based BGP/MPLS IP-VPNs that are interconnected via the same Provider Edge (PE) routers, new RSVP extensions are required. This document outlines the requirements and proposes a solution for interconnecting multiple BGP/IP-VPNs via the same Provider Edge router.

2. Motivation

If multiple MPLS-TE based BGP/MPLS IP-VPNs are interconnected via the same Provider Edge (PE) router, new RSVP extensions are required. These extensions are necessary so that RSVP control messages from the Customer Edge (CE) equipment, such as Path messages and Resv messages, are appropriately handled by the PE routers.

2.1 Network Example

Customer MPLS TE LSPs in the context of BGP/MPLS IP-VPNs are shown in Figure 1 (Customer MPLS TE LSPs in the context of BGP/MPLS IP-VPNs).

Here, we make the following set of assumptions.

1. VPN1 and VPN2 are completely different customers.
2. CE1 and CE3 are head-end routers.
3. CE2 and CE4 are tail-end routers.
4. A same address (e.g., 192.0.2.1) is assigned at CE2 and CE4.

K.Kumaki, et al. [Page 3]
Consider that customers in VPN1 and VPN2 would like to establish a customer MPLS TE LSP between their sites (i.e., between CE1 and CE2, between CE3 and CE4). In this situation the following RSVP-TE Path messages would be sent:

1. CE1 would send a Path message to PE1 to establish the MPLS TE LSP (VPN1) between CE1 and CE2.

2. CE3 would also send a Path message to PE1 to establish the MPLS TE LSP (VPN2) between CE1 and CE2.

After receiving each Path messages, PE1 can identify each Path message from each incoming interface. Afterwards, PE1 forwards the messages to PE2 by routing information described in [RFC4364] and [RFC4659]. However, the current RSVP control message specification [RFC3209] does not specify how PE2 is able to identify each Path message (i.e., the Path message for VPN1 and VPN2). Additionally, Resv messages per VPN sent from PE2 cannot be identified at PE1.
3. Protocol Extensions and Procedures

In order to distinguish between the VPN1 Path/Resv messages and the
VPN2 Path/Resv messages described in Section 2.3. (Network Example),
an identifier in Path/Resv messages is required.

This section provides the additional objects that extend RSVP
to meet the requirements defined in Section 2.2 (Requirements).
These new object types are SESSION, SENDER_TEMPLATE and FILTERSPEC
object. These new objects will act as identifiers and allow PEs to
distinguish Path/Resv messages per VPN in the context of BGP/MPLS
IP-VPNs. The new object types are defined in Section 3.1
(Object Definitions) and the specific procedure is described in
Section 3.2 (Handling).

3.1 Object Definitions

3.1.1 LSP_TUNNEL_VPN-IPv4 and LSP_TUNNEL_VPN-IPv6 SESSION Object

The LSP_TUNNEL_VPN-IPv4 (or VPN-IPv6) SESSION object appears in RSVP
messages that ordinarily contain a SESSION object and are sent
between ingress PE and egress PE in either direction. The object MUST
NOT be included in any RSVP messages that are sent outside of the
provider’s backbone.

The LSP_TUNNEL_VPN-IPv6 SESSION object is analogous to the
LSP_TUNNEL_VPN-IPv4 SESSION object, using a VPN-IPv6 address
([RFC4659]) instead of a VPN-IPv4 address ([RFC4364]).

The formats of the objects are as follows:

Class = SESSION, LSP_TUNNEL_VPN-IPv4 C-Type = TBA
Class = SESSION, LSP_TUNNEL_VPN-IPv6 C-Type = TBA

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            VPN-IPv6 tunnel end point address                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| (24 bytes)                                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  MUST be zero            |      Tunnel ID                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Extended Tunnel ID                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      (16 bytes)                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The VPN-IPv4 tunnel end point address (respectively, VPN-IPv6 tunnel end point address) field contains an address of the VPN-IPv4 (respectively, VPN-IPv6) address family encoded as specified in [RFC4364](respectively, [RFC4659]).

The Tunnel ID and Extended Tunnel ID are identical to the same fields in the LSP_TUNNEL_IPv4 and LSP_TUNNEL_IPv6 SESSION objects as per [RFC3209].
3.1.2 LSP_TUNNEL_VPN-IPv4 and LSP_TUNNEL_VPN-IPv6 SENDER_TEMPLATE Objects

The LSP_TUNNEL_VPN-IPv4 (or VPN-IPv6) SENDER_TEMPLATE object appears in RSVP messages that ordinarily contain a SENDER_TEMPLATE object and are sent between ingress PE and egress PE in either direction (such as Path, PathError, and PathTear). The object MUST NOT be included in any RSVP messages that are sent outside of the provider’s backbone. The format of the object is as follows:

Class = SENDER_TEMPLATE, LSP_TUNNEL_VPN-IPv4 C-Type = TBA

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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   VPN-IPv4 tunnel sender address (12 bytes)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  MUST be zero                 |            LSP ID             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Class = SENDER_TEMPLATE, LSP_TUNNEL_VPN-IPv6 C-Type = TBA

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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            VPN-IPv6 tunnel sender address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            (24 bytes)                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  MUST be zero                 |            LSP ID             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

The VPN-IPv4 tunnel sender address (respectively, VPN-IPv6 tunnel sender address) field contains an address of the VPN-IPv4 (respectively, VPN-IPv6) address family encoded as specified in [RFC4364] (respectively, [RFC4659]).

The LSP ID is identical to the LSP ID field in the LSP_TUNNEL_IPv4 and LSP_TUNNEL_IPv6 SENDER_TEMPLATE objects as per [RFC3209].
3.1.3 LSP_TUNNEL_VPN-IPv4 and LSP_TUNNEL_VPN-IPv6 FILTER_SPEC Objects

The LSP_TUNNEL_VPN-IPv4 (or VPN-IPv6) FILTER_SPEC object appears in RSVP messages that ordinarily contain a FILTER_SPEC object and are sent between ingress PE and egress PE in either direction (such as Resv, ResvError, and ResvTear). The object MUST NOT be included in any RSVP messages that are sent outside of the provider’s backbone.

Class = FILTER SPECIFICATION, LSP_TUNNEL_VPN-IPv4 C-Type = TBA

The format of the LSP_TUNNEL_VPN-IPv4 FILTER_SPEC object is identical to the LSP_TUNNEL_VPN-IPv4 SENDER_TEMPLATE object.

Class = FILTER SPECIFICATION, LSP_TUNNEL_VPN-IPv6 C-Type = TBA

The format of the LSP_TUNNEL_VPN-IPv6 FILTER_SPEC object is identical to the LSP_TUNNEL_VPN-IPv6 SENDER TEMPLATE object.

3.1.4 VPN-IPv4 and VPN-IPv6 RSVP_HOP Objects

The format of the VPN-IPv4 and VPN-IPv6 RSVP_HOP objects are identical to objects described in [RFC6016].

3.2 Handling

It assumes that ingress PEs and egress PEs in the context of BGP/MPLS IP-VPNs have RSVP capabilities.

3.2.1 Path Message Processing at Ingress PE

When a Path message arrives at the ingress PE (PE1 in Figure 1), the PE needs to establish suitable Path state and forward the Path message on to the egress PE (PE2 in Figure 1). In this section we described the message handling process at the ingress PE.

1. CE1 would send a Path message to PE1 to establish the MPLS TE LSP (VPN1) between CE1 and CE2. The Path message is addressed to the eventual destination (the receiver at the remote customer site) and carries the IP Router Alert option, in accordance with [RFC2205]. The ingress PE must recognize the router alert, intercept these messages and process them as RSVP signalling messages.

2. When the ingress PE receives a Path message from a CE that is addressed to the receiver, the VRF that is associated with the incoming interface can be identified (this step does not deviate from current behavior).

3. The tunnel end point address of the receiver is looked up in the appropriate VRF, and the BGP Next-Hop for that tunnel end point address is identified. The next-hop is the egress PE.
4. A new LSP_TUNNEL_VPN-IPv4/VPN-IPv6 SESSION object is constructed, containing the Route Distinguisher (RD) that is part of the VPN-IPv4/VPN-IPv6 route prefix for this tunnel end point address, and the IPv4/IPv6 tunnel end point address from the original SESSION object.

5. A new LSP_TUNNEL_VPN-Pv4/IPv6 SENDER_TEMPLATE object is constructed, with the original IPv4/IPv6 tunnel sender address from the incoming SENDER_TEMPLATE plus the RD that is used by the PE to advertise the prefix for the customers VPN.

6. A new Path message is sent containing all the objects from the original Path message, replacing the original SESSION and SENDER_TEMPLATE objects with the new LSP_TUNNEL_VPN-IPv4/VPN-IPv6 type objects. This Path message is sent directly to the egress PE (the next hop as being looked up in step 3 above) without IP Router Alert.

3.2.2 Path Message Processing at Egress PE

In this section we described the message handling process at the egress PE.

1. When a Path message arrives at the egress PE (PE2 in Figure 1), it is addressed to the PE itself, and is handed to RSVP for processing.

2. The router extracts the RD and IPv4/IPv6 address from the LSP_TUNNEL_VPN-IPv4/VPN-IPv6 SESSION object, and determines the local VRF context by finding a matching VPN-IPv4 prefix with the specified RD that has been advertised by this router into BGP.

3. The entire incoming RSVP message, including the VRF information, is stored as part of the Path state.

4. The egress PE can now construct a Path message which differs from the Path message it received in the following ways:
   a. Its tunnel end point address is the IP address extracted from the SESSION object;
   b. The SESSION and SENDER_TEMPLATE objects are converted back to IPv4-type/IPv6-type by discarding the attached RD;
   c. The RSVP_HOP object contains the IP address of the outgoing interface of the egress PE and an LIH, as per normal RSVP processing.

5. The egress PE then sends the Path message on towards its tunnel end point address over the interface identified above. This Path message carries the IP Router-Alert option as required by [RFC2205].
3.2.3 Resv Processing at Egress PE

When a receiver at the customer site originates a Resv message for the session, normal RSVP procedures apply until the Resv, making its way back towards the sender, arrives at the "egress" PE (it is "egress" with respect to the direction of data flow, i.e. PE2 in figure 1). On arriving at PE2, the SESSION and FILTER_SPEC objects in the Resv, and the VRF in which the Resv was received, are used to find the matching Path state stored previously.

The PE constructs a Resv message to send to the RSVP HOP stored in the Path state, i.e., the ingress PE (PE1 in Figure 1). The LSP TUNNEL IPv4/IPv6 SESSION object is replaced with the same LSP_TUNNEL_VPN-IPv4/VPN-IPv6 SESSION object received in the Path. The LSP TUNNEL IPv4/IPv6 FILTER_SPEC object is replaced with a LSP_TUNNEL_VPN-IPv4/VPN-IPv6 FILTER_SPEC object, which copies the VPN-IPv4/VPN-IPv6 address from the LSP TUNNEL SENDER_TEMPLATE received in the matching Path message.

The Resv message MUST be addressed to the IP address contained within the RSVP_HOP object in the Path message.

3.2.4 Resv Processing at Ingress PE

Upon receiving a Resv message at the ingress PE (with respect to data flow, i.e. PE1 in Figure 1), the PE determines the local VRF context and associated Path state for this Resv by decoding the received SESSION and FILTER_SPEC objects. It is now possible to generate a Resv message to send to the appropriate CE. The Resv message sent to the ingress CE will contain LSP TUNNEL IPv4/IPv6 SESSION and LSP TUNNEL FILTER_SPEC objects, derived from the appropriate Path state.

3.2.5 Other RSVP Messages

Processing of other RSVP messages, i.e., PathError, PathTear, ResvError, ResvTear, and ResvConf message in general follows the rules defined in [RFC2205], with additional rules that MUST be observed for messages transmitted within the VPN, i.e., between the PEs as follows:

- The SESSION, SENDER_TEMPLATE, and FILTER_SPEC objects MUST be converted from LSP_TUNNEL_IPv4/LSP_TUNNEL_IPv6 [RFC3209] to LSP_TUNNEL_VPN_IPv4/LSP_TUNNEL_VPN_IPv6 form, respectively, and back in the same manner as described above for Path and Resv messages.
The appropriate type of RSVP_HOP object (VPN-IPv4 or VPN-IPv6) MUST be used as described in Section 8.4 of [RFC6016].

Depending on the type of RSVP_HOP object received from the neighbor, the message MUST be MPLS encapsulated or IP encapsulated.

The matching state and VRF MUST be determined by decoding the corresponding RD and IPv4 (respectively, IPv6) address in the SESSION and FILTER_SPEC objects.

The message MUST be directly addressed to the appropriate PE, without using the Router Alert Option.

4. Management Considerations

MPLS-TE based BGP/MPLS IP-VPNs are based on a peer model. If an operator would like to configure a new site to an existing VPN configuration of both the CE router and the attached PE router is required. The operator is not required to modify the configuration of PE routers connected to other sites or modify the configuration of other VPNs.

4.1 Impact on Network Operation

It is expected that the use of the extensions specified in this document will not significantly increase the level of operational traffic.

Furthermore, the additional extensions described in this document will have no impact on the operation of existing MPLS-TE resiliency mechanisms available within MPLS-TE.

5. Security Considerations

This document defines RSVP-TE extensions for BGP/MPLS IP-VPNs. Hence the security of the RSVP-TE extensions relies on the security of RSVP-TE extensions for LSP tunnels.

The security issues are described in the existing RSVP-TE extensions for LSP tunnels. [RFC3209]
6. IANA Considerations

IANA maintains a registry of RSVP parameters. As described in Section 3 (Protocol Extensions and Procedures) six new Class Types (C-types) have been defined. IANA is requested to make the following allocations from the "RSVP C-Types" sub-registry:

Class = SESSION, LSP_TUNNEL VPN-IPv4 C-Type = TBA
Class = SESSION, LSP_TUNNEL VPN-IPv6 C-Type = TBA
Class = SENDER TEMPLATE, LSP_TUNNEL VPN-IPv4 C-Type = TBA
Class = SENDER TEMPLATE, LSP_TUNNEL VPN-IPv6 C-Type = TBA
Class = FILTER SPECIFICATION, LSP_TUNNEL VPN-IPv4 C-Type = TBA
Class = FILTER SPECIFICATION, LSP_TUNNEL VPN-IPv6 C-Type = TBA
7. References

7.1 Normative References


7.2 Informative References


8. Acknowledgments

The authors would like to express thanks to Makoto Nakamura for his helpful and useful comments and feedback.

9. Author’s Addresses

Kenji Kumaki
KDDI Corporation
Garden Air Tower
Iidabashi, Chiyoda-ku,
Tokyo 102-8460, JAPAN
Email: ke-kumaki@kddi.com

Tomoki Murai
Furukawa Network Solutions Corp.
5-1-9, Higashi-Yawata, Hiratsuka
Kanagawa 254-0016, JAPAN
Email: murai@fnsc.co.jp

Dean Cheng
Huawei Technologies
2330 Central Expressway
Santa Clara CA 95050, U.S.A.
Email: dean.cheng@huawei.com

Peng Jiang
KDDI R&D Laboratories, Inc.
2-1-15 Ohara Fujimino
Saitama 356-8502, JAPAN
Email: pe-jiang@kddilabs.jp

Chikara Sasaki
KDDI R&D Laboratories, Inc.
2-1-15 Ohara Fujimino
Saitama 356-8502, JAPAN
Email: ch-sasaki@kddilabs.jp

Daisuke Tatsumi
KDDI Corporation
Garden Air Tower
Iidabashi, Chiyoda-ku,
Tokyo 102-8460, JAPAN
Email: da-tatsumi@kddi.com