TEAS Working Group   Zafar Ali, Ed.
Internet Draft   George Swallow, Ed.
Intended status: Standard Track   Cisco Systems
Expires: September 22, 2016   F. Zhang, Ed.
                                                             Huawei
                                                      D. Beller, Ed.
                                                              Nokia
                                                     March 21, 2016

**Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Path
Diversity using Exclude Route**

draft-ietf-teas-lsp-diversity-04.txt

Status of this Memo

Internet Draft   draft-ietf-teas-lsp-diversity-04.txt

Abstract

RFC 4874 specifies methods by which path exclusions can be
communicated during RSVP-TE signaling in networks where precise
explicit paths are not computed by the LSP source node. This
document specifies procedures for additional route exclusion
subobject based on Paths currently existing or expected to exist
within the network.

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 RFC 2119 [RFC2119].

Table of Contents

1. Introduction

   Path diversity for multiple connections is a well-known Service
   Provider requirement. Diversity constraints ensure that Label-
   Switched Paths (LSPs) can be established without sharing network
   resources, thus greatly reducing the probability of simultaneous
   connection failures.

   The source node can compute diverse paths for LSPs when it has
   full knowledge of the network topology and is permitted to signal
   an Explicit Route Object. However, there are scenarios where
   different nodes perform path computations, and therefore there is

a need for relevant diversity constraints to be signaled to those
nodes. These include (but are not limited to):

. LSPs with loose hops in the Explicit Route Object (ERO), e.g.
   inter-domain LSPs.

. Generalized Multi-Protocol Label Switching (GMPLS) User-
   Network Interface (UNI), where the core node may perform path
   computation [RFC4208].

[RFC4874] introduced a means of specifying nodes and resources to
be excluded from a route, using the eXclude Route Object (XRO) and
Explicit Exclusion Route Subobject (EXRS). It facilitates the
calculation of diverse paths for LSPs based on known properties of
those paths including addresses of links and nodes traversed, and
Shared Risk Link Groups (SRLGs) of traversed links. Employing
these mechanisms requires that the source node that initiates
signaling knows the relevant properties of the path(s) from which
diversity is desired. However, there are circumstances under which
this may not be possible or desirable, including (but not limited
to):

. Exclusion of a path which does not originate, terminate or
   traverse the source node of the diverse LSP, in which case the
   addresses of links and SRLGs of the path from which diversity
   is required are unknown to the source node.

. Exclusion of a path which is known to the source node of the
   diverse LSP for which the node has incomplete or no path
   information, e.g. due to operator policy. In this case, the
   source node is aware of the existence of the reference path but
   the information required to construct an XRO object to
   guarantee diversity from the reference path is not fully known.
   Inter-domain and GMPLS overlay networks can impose such
   restrictions.

This is exemplified in the Figure 1, where the overlay reference
model from [RFC4208] is shown.

```
   Overlay                                                  Overlay
   Network       +----------------------------------+       Network
+---------+      |                                  |      +---------+
|  +----+ |      |  +-----+    +-----+    +-----+    |      | +----+  |
|  |    | | UNI  |  |     |    |     |    |     |    | UNI  | |    |  |
|  -+ EN1+-+-----+--+ CN1 +----+ CN2 +----+ CN3 +---+-----+-+ EN3+- |
|  |    | | |    +--+--+         |         |        |   | +---+-|    |  |
|  +----+ | |    |  +--+--+    +--+--+    +--+--+   | |   | +----+  |
+---------+ |    |     |          |          |      | |   +---------+
            |    |     |          |          |      | |
+---------+ |    |  +--+--+       |       +--+--+   | |   +---------+
|  +----+ | |    |  |     |       |       +-------+   +-----+    | +----+  |
|  |    +-+--+  |  | CN4 +---------------+ CN5 |    |    | |    |  |
|  -+ EN2+-+-----+--+       |                 |    +---+-----+-+ EN4+- |
|  |    | | | UNI  |  +-----+                 +-----+    | UNI | |    |  |
|  +----+ | |    |                                  |      | +----+  |
+---------+ |    +----------------------------------+      +---------+
   Overlay              Core Network                        Overlay
   Network                                                  Network


            Legend:    EN  -  Edge Node
                       CN  -  Core Node
```
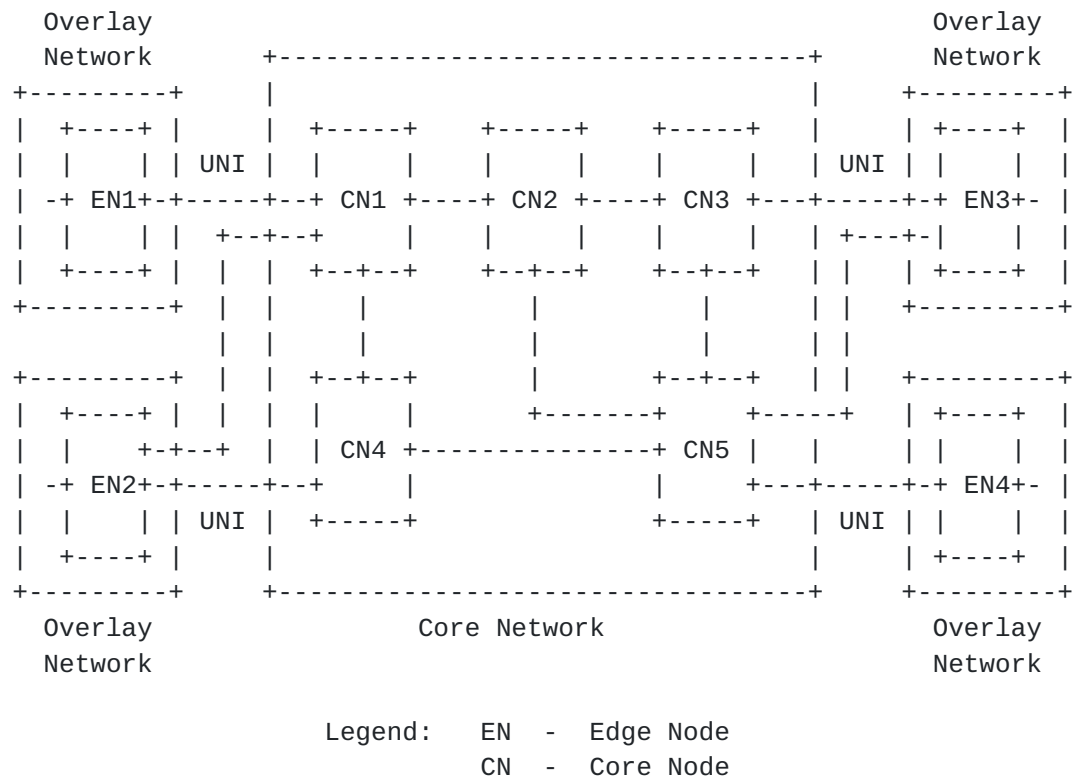
                 Figure 1: Overlay Reference Model [RFC4208]

   Figure 1 depicts two types of UNI connectivity: single-homed and
   dual-homed ENs (which also applies to higher order multi-homed
   connectivity.). Single-homed EN devices are connected to a single
   CN device via a single UNI link. This single UNI link may
   constitute a single point of failure. UNI connection between EN1
   and CN1 is an example of singled-homed UNI connectivity.

   A single point of failure caused by a single-homed UNI can be
   avoided when the EN device is connected to two different CN
   devices, as depicted for EN2 in Figure 1. For the dual-homing
   case, it is possible to establish two different UNI connections
   from the same source EN device to the same destination EN device.
   For example, two connections from EN2 to EN3 may use the two UNI
   links EN2-CN1 and EN2-CN4. To avoid single points of failure
   within the provider network, it is necessary to also ensure path
   (LSP) diversity within the core network.

   In a UNI network such as that shown in Figure 1, the CNs
   typically perform path computation. Information sharing across

the UNI boundary is restricted based on the policy rules imposed
by the core network. Typically, the core network topology
information is not exposed to the ENs. In the network shown in
Figure 1, consider a use case where an LSP from EN2 to EN4 needs
to be SRLG diverse from an LSP from EN1 to EN3. In this case, EN2
may not know SRLG attributes of the EN1- EN3 LSP and hence cannot
construct an XRO to exclude these SRLGs. In this example EN2
cannot use the procedures described in [RFC4874]. Similarly, an
LSP from EN2 to EN3 traversing CN1 needs to be diverse from an
LSP from EN2 to EN3 going via CN4. Again in this case, exclusions
based on [RFC4874] cannot be used.

This document addresses these diversity requirements by
introducing the notion of excluding the path taken by particular
LSP(s). The reference LSP(s) or route(s) from which diversity is
required is/are identified by an "identifier". The type of
identifier to use is highly dependent on the networking
deployment scenario; it could be client-initiated, allocated by
the (core) network or managed by a PCE. This document defines
three different types of identifiers corresponding to these three
cases: a client initiated identifier, a PCE allocated Identifier
and CN ingress node (UNI-N) allocated Identifier.

1.1. Client-Initiated Identifier

There are scenarios in which the ENs have the following
requirements for the diversity identifier:

- The identifier is controlled by the client side and is
  specified as part of the service request.

- Both client and server understand the identifier.

- It is necessary to be able to reference the identifier even if
  the LSP referenced by it is not yet signaled.

- The identifier is to be stable for a long period of time.

- The identifier is to be stable even when the referenced LSP is
  rerouted.

- The identifier is to be human-readable.

These requirements are met by using the LSP identifier. The LSP
identifier uniquely identifies an LSP in the network and
comprises of the following fields: IPv4/IPv6 tunnel sender
address, IPv4/IPv6 tunnel end point address, Tunnel ID, LSP ID,

and Extended Tunnel ID. These fields are defined in [RFC3209], sections 4.6.1.1 and 4.6.2.1.

The usage of the client-initiated identifier is illustrated by Figure 1. Suppose a LSP from EN2 to EN4 needs to be diverse with respect to a LSP from EN1 to EN3. The LSP identifier of the EN1-EN3 LSP is LSP-IDENTIFIER1, where LSP-IDENTIFIER1 is defined by the tuple (tunnel-id = T1, LSP ID = L1, source address = EN1.ROUTE Identifier (RID), destination address = EN3.RID, extended tunnel-id = EN1.RID). Similarly, LSP identifier of the EN2-EN3 LSP is LSP-IDENTIFIER2, where LSP-IDENTIFIER12 is defined by the tuple (tunnel-id = T2, LSP IS = L1, source address = EN2.RID, destination address = EN4.RID, extended tunnel-id = EN2.RID). The EN1-EN3 LSP is signaled with an exclusion requirement from LSP-IDENTIFIER2, and the EN2-EN3 LSP is signaled with an exclusion requirement from LSP-IDENTIFIER1. In order to maintain diversity between these two connections within the core network, it is assumed that the core network implements Crankback Signaling [RFC4920]. Note that crankback signaling is known to lead to slower setup times and sub-optimal paths under some circumstances as described by [RFC4920].

1.2. PCE-allocated Identifier

In scenarios where a PCE is deployed and used to perform path computation, the core edge node (e.g., node CN1 in Figure 1) could consult a PCE to allocate identifiers, which are used to signal path diversity constraints. In other scenarios a PCE is deployed at network node(s) or a PCE is part of a Network Management System (NMS). In all these cases, the Path Key as defined in [RFC5520] can be used in RSVP signaling as the identifier to ensure diversity.

An example of specifying LSP diversity using a Path Key is shown in Figure 2, where a simple network with two domains is shown. It is desired to set up a pair of path-disjoint LSPs from the source in Domain 1 to the destination in Domain 2, but the domains keep strict confidentiality about all path and topology information.

The first LSP is signaled by the source with ERO {A, B, loose Dst} and is set up with the path {Src, A, B, U, V, W, Dst}. However, when sending the RRO out of Domain 2, node U would normally strip the path and replace it with a loose hop to the destination. With this limited information, the source is unable to include enough detail in the ERO of the second LSP to avoid it taking, for example, the path {Src, C, D, X, V, W, Dst} for path-disjointness.

```
       --------------------     ----------------------------
      | Domain 1           |   |                  Domain 2 |
      |                    |   |                           |
      |     ---     ---    |   |   ---     ---     ---      |
      |    | A |--| B |--+--+--| U |--| V |---| W |        |
      |    / ---     ---   |   |   ---     ---     --- \    |
      |  ---/              |   |          /       /    \--- |
      | |Src|             |   |         /       /     |Dst| |
      |   ---\             |   |        /       /      /--- |
      |     \ ---     ---  |   |   --- /   --- /  --- /     |
      |      | C |--| D |--+--+--| X |---| Y |--| Z |       |
      |       ---     ---  |   |   ---     ---     ---      |
      |                    |   |                           |
       --------------------     ----------------------------
```
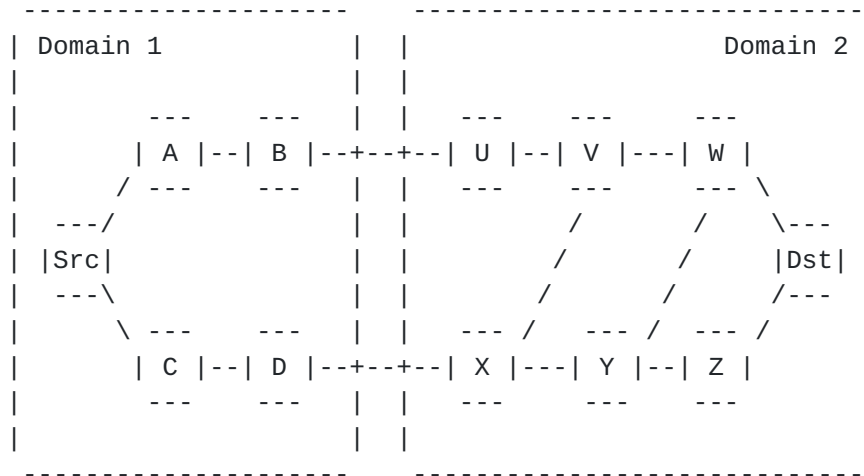
              Figure 2: A Simple Multi-Domain Network

   In order to improve the situation, node U performs the PCE
   function and replaces the path segment {U, V, W} in the RRO with
   a Path Key Subobject. The Path Key Subobject assigns an
   "identifier" to the key. The PCE ID in the message indicates that
   it was node U that made the replacement.

   With this additional information, the source is able to signal
   the subsequent LSPs with the ERO set to {C, D, exclude Path
   Key(EXRS), loose Dst}. When the signaling message reaches node X,
   it can consult node U to expand the Path Key and know how to
   avoid the path of the first LSP. Alternatively, the source could
   use an ERO of {C, D, loose Dst} and include an XRO containing the
   Path Key.

   This mechanism can work with all the Path-Key resolution
   mechanisms, as detailed in [RFC5553] section 3.1. A PCE, co-
   located or not, may be used to resolve the Path-Key, but the node
   (i.e., a Label Switching Router (LSR)) can also use the Path Key
   information to index a Path Segment previously supplied to it by
   the entity that originated the Path-Key, for example the LSR that
   inserted the Path-Key in the RRO or a management system.

1.3. Network-Assigned Identifier

   There are scenarios in which the network provides diversity-
   related information for a service that allows the client device
   to include this information in the signaling message. If the
   Shared Resource Link Group (SRLG) identifier information is both
   available and shareable (by policy) with the ENs, the procedure

defined in [DRAFT-SRLG-RECORDING] can be used to collect SRLG identifiers associated with an LSP (LSP1). When a second LSP (LSP2) needs to be diverse with respect to LSP1, the EN constructing the RSVP signaling message for setting up LSP2 can insert the SRLG identifiers associated with LSP1 as diversity constraints into the XRO using the procedure described in [RFC4874]. However, if the core network SRLG identifiers are either not available or not shareable with the ENs based on policies enforced by core network, existing mechanisms cannot be used.

In this draft, a signaling mechanism is defined where information signaled to the CN via the UNI does not require shared knowledge of core network SRLG information. For this purpose, the concept of a Path Affinity Set (PAS) is used for abstracting SRLG information. The motive behind the introduction of the PAS is to minimize the exchange of diversity information between the core network (CNs) and the client devices (ENs). The PAS contains an abstract SRLG identifier associated with a given path rather than a detailed SRLG list. The PAS is a single identifier that can be used to request diversity and associate diversity. The means by which the processing node determines the path corresponding to the PAS is beyond the scope of this document.

A CN on the core network boundary interprets the specific PAS identifier (e.g. "123") as meaning to exclude the core network SRLG information (or equivalent) that has been allocated by LSPs associated with this PAS identifier value. For example, if a Path exists for the LSP with the identifier "123", the CN would use local knowledge of the core network SRLGs associated with the "123" LSPs and use those SRLGs as constraints for path computation. If a PAS identifier is included for exclusion in the connection request, the CN (UNI-N) in the core network is assumed to be able to determine the existing core network SRLG information and calculate a path that meets the determined diversity constraints.

When a CN satisfies a connection setup for a (SRLG) diverse signaled path, the CN may optionally record the core network SRLG information for that connection in terms of CN based parameters and associates that with the EN addresses in the Path message. Specifically for Layer-1 Virtual Private Networks (L1VPNs), Port Information Tables (PIT) [RFC5251] can be leveraged to translate between client (EN) addresses and core network addresses.

The means to distribute the PAS information within the core network is beyond the scope of this document. The PAS and the

associated SRLG information can be distributed within the core
network by an Interior Gateway Protocol (IGP) or by other means
such as configuration. Regardless of means used to distribute the
PAS information, the information is kept inside core network and
is not shared with the overlay network (see Figure 1).

2. RSVP-TE signaling extensions

This section describes the signaling extensions required to
address the aforementioned requirements and use cases.

2.1. Diversity XRO Subobject

New Diversity XRO subobjects are defined below for the IPv4 and
IPv6 address families. Most of the fields in the IPv4 and IPv6
Diversity XRO subobjects are common and are described following
the definition of the two subobjects.

IPv4 Diversity XRO Subobject is defined as follows:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|  XRO Type   |    Length   |DI Type|A-Flags|E-Flags| Resvd |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          IPv4 Diversity Identifier Source Address           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Diversity Identifier Value                    |
//                         ...                                //
|                                                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Similarly, the IPv6 Diversity XRO Subobject is defined as
follows:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|  XRO Type   |    Length     |DI Type|A-Flags|E-Flags| Resvd |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         IPv6 Diversity Identifier source address             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        IPv6 Diversity Identifier source address (cont.)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        IPv6 Diversity Identifier source address (cont.)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        IPv6 Diversity Identifier source address (cont.)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Diversity Identifier Value                   |
//                           ...                               //
|                                                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

  L:

        The L-flag is used as for the XRO subobjects defined in
        [RFC4874], i.e.,

        0 indicates that the attribute specified MUST be excluded.

        1 indicates that the attribute specified SHOULD be avoided.

  XRO Type

        The value is set to for IPv4 diversity XRO subobject
        (value to be assigned by IANA). Similarly, The value is
        set to for IPv6 diversity XRO Subobject (value to be
        assigned by IANA).

  Length

        The Length contains the total length of the IPv4/ IPv6
        subobject in bytes, including the Type and Length fields.
        The Length is variable, depending on the diversity
        identifier value.

Diversity Identifier Type (DI Type)

   Diversity Identifier Type (DI Type) indicates the way the
   reference LSP(s) or route(s) with which diversity is
   required is identified in the IPv4/ IPv6 Diversity
   subobjects. The following three DI type values are defined
   in this document:

      DI Type value   Definition
      -------------   -------------------------------
            1   Client Initiated Identifier
            2   PCE Allocated Identifier
            3   Network Assigned Identifier

Attribute Flags (A-Flags):

   The Attribute Flags (A-Flags) are used to communicate
   desirable attributes of the LSP being signaled in the IPv4/
   IPv6 Diversity subobjects. The following flags are defined.
   Each flag acts independently. Any combination of flags is
   permitted.

   0x01 = Destination node exception

      Indicates that the exclusion does not apply to the
      destination node of the LSP being signaled.

   0x02 = Processing node exception

      Indicates that the exclusion does not apply to the
      node(s) performing ERO expansion for the LSP being
      signaled. An ingress UNI-N node is an example of such a
      node.

   0x04 = Penultimate node exception

      Indicates that the penultimate node of the LSP being
      signaled MAY be shared with the excluded path even when
      this violates the exclusion flags.

   0x08 = LSP ID to be ignored

      This flag is used to indicate tunnel level exclusion.
      Specifically, this flag is used to indicate that if
      diversity identifier contains lsp-id field, the lsp-id

           is to be ignored and the exclusion applies to any LSP
           matching the rest of the diversity identifier.

     Exclusion Flags (E-Flags):

           The Exclusion-Flags are used to communicate the desired
           type(s) of exclusion requested in the IPv4/ IPv6 diversity
           subobjects. The following flags are defined. Any
           combination of these flags is permitted. Please note that
           the exclusion specified by these flags may be modified by
           the value of the Attribute-flags. For example, node
           exclusion flag is ignored for the "Penultimate node" if the
           "Penultimate node exception" flag of the Attribute-flags is
           set.

           0x01 = SRLG exclusion

                Indicates that the path of the LSP being signaled is
                requested to be SRLG-diverse from the excluded path
                specified by the IPv4/ IPv6 Diversity XRO subobject.

           0x02 = Node exclusion

                Indicates that the path of the LSP being signaled is
                requested to be node-diverse from the excluded path
                specified by the IPv4/ IPv6 Diversity XRO subobject.

           0x04 = Link exclusion

                Indicates that the path of the LSP being signaled is
                requested to be link-diverse from the path specified
                by the IPv4/ IPv6 Diversity XRO subobject.
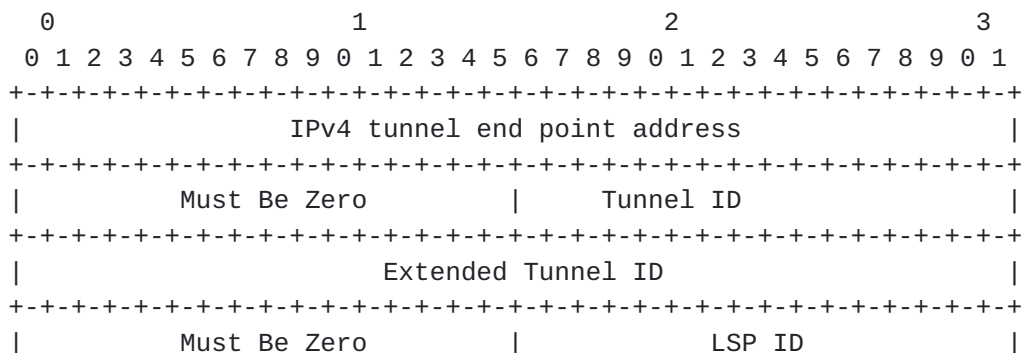

     Resvd

           This field is reserved. It SHOULD be set to zero on
           transmission, and MUST be ignored on receipt for both
           IPv4/ IPv6 Diversity XRO subobjects.

     IPv4 / IPv6 Diversity Identifier source address:

This field is set to the IPv4/ IPv6 address of the node
that assigns the diversity identifier. Depending on the
diversity identifier type, the diversity identifier source
may be a client node, PCE entity or network node.
Specifically:

o When the diversity identifier type is set to "IPv4/ IPv6
   Client Initiated Identifier", the value is set to IPv4/
   IPv6 tunnel sender address of the reference LSP against
   which diversity is desired. IPv4/ IPv6 tunnel sender
   address is as defined in [RFC3209].

o When the diversity identifier type is set to "IPv4/ IPv6
   PCE Allocated Identifier", the value indicates the IPv4/
   IPv6 address of the node that assigned the Path Key
   identifier and that can return an expansion of the Path
   Key or use the Path Key as exclusion in a path
   computation. The Path Key is defined in [RFC5553].

o When the diversity identifier type is set to "IPv4/ IPv6
   Network Assigned Identifier", the value indicates the
   IPv4/ IPv6 address of the node publishing the Path
   Affinity Set (PAS).

Diversity Identifier Value:

Encoding for this field depends on the diversity identifier
type, as defined in the following.

When the diversity identifier type is set to "Client
Initiated Identifier" in IPv4 Diversity XRO subobject, the
diversity identifier value MUST be encoded as follows:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 IPv4 tunnel end point address                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Must Be Zero          |           Tunnel ID          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Extended Tunnel ID                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Must Be Zero          |             LSP ID           |
```

```
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

        The IPv4 tunnel end point address, Tunnel ID, Extended
        Tunnel ID and LSP ID are as defined in [RFC3209].

        When the diversity identifier type is set to "IPv6 Client
        Initiated Identifier" in IPv6 Diversity XRO subobject, the
        diversity identifier value MUST be encoded as follows:

```
 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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                 IPv6 tunnel end point address                 |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |             IPv6 tunnel end point address (cont.)             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |             IPv6 tunnel end point address (cont.)             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |             IPv6 tunnel end point address (cont.)             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |        Must Be Zero         |           Tunnel ID             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                      Extended Tunnel ID                       |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                   Extended Tunnel ID (cont.)                  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                   Extended Tunnel ID (cont.)                  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                   Extended Tunnel ID (cont.)                  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |        Must Be Zero         |              LSP ID             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

        The IPv6 tunnel end point address, Tunnel ID, IPv6 Extended
        Tunnel ID and LSP ID are as defined in [RFC3209].

        When the diversity identifier type is set to "PCE Allocated
        Identifier" in IPv4 or IPv6 Diversity XRO subobject, the
        diversity identifier value MUST be encoded as follows:

```
 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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|        Must Be Zero          |           Path Key            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Path Key is defined in [RFC5553].

When the diversity identifier type is set to "Network
Assigned Identifier" in IPv4 or IPv6 Diversity XRO
subobject, the diversity identifier value MUST be encoded
as follows:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Path Affinity Set (PAS) identifier                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Path affinity Set (PAS) identifier field is a 32-bit
value that is scoped by, i.e., is only meaningful when
used in combination with, the Diversity Identifier source
address field. There are no restrictions on how a node
selects a PAS identifier value. Section 1.3. defines the
PAS term and provides context on how values may be
selected.

2.2. Diversity EXRS Subobject

[RFC4874] defines the EXRS ERO subobject. An EXRS is used to
identify abstract nodes or resources that must not or should not
be used on the path between two inclusive abstract nodes or
resources in the explicit route. An EXRS contains one or more
subobjects of its own, called EXRS subobjects [RFC4874].

An EXRS MAY include Diversity subobject as specified in this
document. In this case, the IPv4 EXRS format is as follows:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|   Type      |    Length     |            Reserved           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|  XRO Type   |    Length     |DI Type|A-Flags|E-Flags| Resvd |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|             IPv4 Diversity Identifier source address        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Diversity Identifier Value                  |
//                          ...                              //
|                                                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Similarly, the IPv6 EXRS format is as follows:

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|   Type    |    Length     |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|  XRO Type  |    Length    |DI Type|A-Flags|E-Flags| Resvd |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         IPv6 Diversity Identifier source address            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      IPv6 Diversity Identifier source address (cont.)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      IPv6 Diversity Identifier source address (cont.)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      IPv6 Diversity Identifier source address (cont.)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Diversity Identifier Value                  |
//                          ...                              //
|                                                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The meanings of respective fields in EXRS header are as defined
in [RFC4874]. The meanings of respective fields in the Diversity
subobject are as defined earlier in this document for the XRO
Diversity subobject.

2.3. Processing rules for the Diversity XRO and EXRS subobjects

The procedure defined in [RFC4874] for processing the XRO and
EXRS is not changed by this document. The processing rules for
the Diversity XRO and EXRS subobjects are similar unless the
differences are explicitly described. Similarly, IPv4 and IPv6
Diversity XRO subobjects and IPv4 and IPv6 Diversity EXRS
subobjects follow the same processing rules.

If the processing node cannot recognize the Diversity XRO/ EXRS
subobject, the node is expected to follow the procedure defined
in [RFC4874].

An XRO/ EXRS object MAY contain multiple Diversity subobjects of
the same DI Type. E.g., in order to exclude multiple Path Keys, a
node may include multiple Diversity XRO subobjects each with a
different Path Key. Similarly, in order to exclude the routes
taken by multiple LSPs, a node may include multiple Diversity
XRO/ EXRS subobjects each with a different LSP identifier.
Likewise, to exclude multiple PAS identifiers, a node may include
multiple Diversity XRO/ EXRS subobjects each with a different PAS
identifier. However, all Diversity subobjects in an XRO/ EXRS
MUST contain the same Diversity Identifier Type. If a Path
message contains an XRO/ EXRS with multiple Diversity subobjects
of different DI Types, the processing node MUST return a PathErr
with the error code "Routing Problem" (24) and error sub-code
"XRO/ EXRS Too Complex" (68/ 69).

If the processing node recognize the Diversity XRO/ EXRS
subobject but does not support the DI type, it MUST return a
PathErr with the error code "Routing Problem" and error value of
"Unsupported Diversity Identifier Type".

The nodes in the domain that perform path computation SHOULD
process the diversity information signaled in the XRO/ EXRS
Diversity subobjects. The transit nodes in a domain and the
domain egress node MAY ignore it. While processing EXRS object,
if a loose-hop expansion results in the creation of another
loose-hop in the outgoing ERO, the processing node MAY include
the EXRS in the newly created loose hop for further processing by
downstream nodes.

The attribute-flags affect the processing of the Diversity XRO/
EXRS subobject as follows:

    o When the "processing node exception" flag is set, the
       exclusion MUST be ignored for the node processing the XRO
       or EXRS subobject.

    o When the "destination node exception" flag is set, the
       exclusion MUST be ignored for the destination node in
       processing the XRO subobject. The destination node
       exception for the EXRS subobject applies to the explicit
       node identified by the ERO subobject that identifies the
       next abstract node. This flag is only processed if the L

bit is set in the ERO subobject that identifies the next
abstract node.

o When the "penultimate node exception" flag is set in the
   XRO subobject, the exclusion MUST be ignored for the
   penultimate node on the path of the LSP being established.
   The penultimate node exception for the EXRS subobject
   applies to the node before the explicit node identified by
   the ERO subobject that identifies the next abstract node.
   This flag is only processed if the L bit is set in the ERO
   subobject that identifies the next abstract node.

If the L-flag of the diversity XRO subobject or diversity EXRS
subobject is not set, the processing node proceeds as follows.

- If the Diversity Identifier Type is set to "IPv4/IPv6 Client
  Initiated Identifiers", the processing node MUST ensure that
  the path calculated/ expended for the signaled LSP is diverse
  from the route taken by the LSP identified in the Diversity
  Identifier Value field.

- If the Diversity Identifier Type is set to "IPv4/IPv6 PCE
  Allocated Identifiers", the processing node MUST ensure that
  any path calculated for the signaled LSP is diverse from the
  route identified by the Path-Key. The processing node MAY use
  the PCE identified by the IPv4/IPv6 Diversity Identifier Source
  Address in the subobject for route computation. The processing
  node MAY use the Path-Key resolution mechanisms described in
  [RFC5553].

- If the Diversity Identifier Type is set to "IPv4/IPv6 Network
  Assigned Identifiers", the processing node MUST ensure that the
  path calculated for the signaled LSP is diverse with respect to
  the values associated with the PAS identifier and Diversity
  Identifier source address fields.

- Regardless of whether the path computation is performed
  locally or at a remote node (e.g., PCE), the processing node
  MUST ensure that any path calculated for the signaled LSP is
  diverse from the requested Exclusion Flags.

- If the excluded path referenced in the XRO subobject is
  unknown to the processing node, the processing node SHOULD
  ignore the diversity XRO subobject and SHOULD proceed with the
  signaling request. After sending the Resv for the signaled LSP,
  the processing node MUST return a PathErr with the error code
  "Notify Error" (25) and error sub-code "Route reference in

diversity XRO identifier unknown" (value to be assigned by IANA) for the signaled LSP.

- If the processing node fails to find a path that meets the requested constraint, the processing node MUST return a PathErr with the error code "Routing Problem" (24) and error sub-code "Route blocked by Exclude Route" (67).

If the L-flag of the XRO diversity subobject or EXRS diversity subobject is set, the processing node proceeds as follows:

- If the Diversity Identifier Type is set to "IPv4/IPv6 Client Initiated Identifiers", the processing node SHOULD ensure that the path calculated/ expended for the signaled LSP is diverse from the route taken by the LSP identified in the Diversity Identifier Value field.

- If the Diversity Identifier Type is set to "IPv4/IPv6 PCE Allocated Identifiers", the processing node SHOULD ensure that the path calculated for the signaled LSP is diverse from the route identified by the Path-Key.

- If the Diversity Identifier Type is set to "IPv4/IPv6 Network Assigned Identifiers", the processing node SHOULD ensure that the path calculated for the signaled LSP is diverse with respect to the values associated with the PAS identifier and Diversity Identifier source address fields.

- If the processing node fails to find a path that meets the requested constraint, it SHOULD proceed with signaling using a suitable path that meets the constraint as far as possible. After sending the Resv for the signaled LSP, it MUST return a PathErr message with error code "Notify Error" (25) and error sub-code "Failed to satisfy Exclude Route" (value: to be assigned by IANA) to the source node.

If, subsequent to the initial signaling of a diverse LSP, an excluded path referenced in the XRO subobject becomes known to the processing node, or a change in the excluded path becomes known to the processing node, the processing node MUST re-evaluate the exclusion and diversity constraints requested by the diverse LSP to determine whether they are still satisfied.

If, subsequent to the initial signaling of a diverse LSP, the requested exclusion constraints for the diverse LSP are no longer satisfied and an alternative path for the diverse LSP that can satisfy those constraints exists, then:

- If the L-flag was not set in the original exclusion, the
  processing node MUST send a PathErr message for the diverse LSP
  with the error code "Routing Problem" (24) and error sub-code
  "Route blocked by Exclude Route" (67). The Path_State_Removed
  flag (PSR) [RFC3473] MUST NOT be set. A source node receiving a
  PathErr message with this error code and sub-code combination
  SHOULD take appropriate actions to migrate to a compliant path.

- If the L-flag was set in the original exclusion, the
  processing node MUST send a PathErr message for the diverse LSP
  with the error code "Notify Error" (25) and a new error sub-
  code "compliant path exists" (value: to be assigned by IANA).
  The PSR flag MUST NOT be set. A source node receiving a PathErr
  message with this error code and sub-code combination MAY
  signal a new LSP to migrate the compliant path.

If, subsequent to the initial signaling of a diverse LSP, the
requested exclusion constraints for the diverse LSP are no longer
satisfied and no alternative path for the diverse LSP that can
satisfy those constraints exists, then:

- If the L-flag was not set in the original exclusion, the
  processing node MUST send a PathErr message for the diverse LSP
  with the error code "Routing Problem" (24) and error sub-code
  "Route blocked by Exclude Route" (67). The PSR flag MUST be
  set.

- If the L-flag was set in the original exclusion, the
  processing node MUST send a PathErr message for the diverse LSP
  with the error code error code "Notify Error" (25) and error
  sub-code "Failed to satisfy Exclude Route" (value: to be
  assigned by IANA). The PSR flag MUST NOT be set. The source
  node MAY take no action and keep the LSP along the non-
  compliant path.

3. Security Considerations

This document does not introduce any additional security issues
above those identified in [RFC5920], [RFC2205], [RFC3209],
[RFC3473] and [RFC4874].

4. IANA Considerations

IANA is requested to administer the assignment of new values
defined in this document and summarized in this section.

4.1. New XRO subobject types

IANA registry: RSVP PARAMETERS
Subsection: Class Names, Class Numbers, and Class Types

This document defines two new subobjects for the EXCLUDE_ROUTE
object [RFC4874], C-Type 1. (see:
http://www.iana.org/assignments/rsvp-parameters/rsvp-
parameters.xhtml#rsvp-parameters-94)

```
Subobject Description          Subobject Type
------------------------       --------------
IPv4 Diversity subobject          TBA1
IPv6 Diversity subobject          TBA2
```

4.2. New EXRS subobject types

The diversity XRO subobjects are also defined as new EXRS
subobjects. (see: http://www.iana.org/assignments/rsvp-
parameters/rsvp-parameters.xhtml#rsvp-parameters-24)

4.3. New RSVP error sub-codes

IANA registry: RSVP PARAMETERS
Subsection: Error Codes and Globally Defined Error Value Sub-
Codes.
For Error Code "Routing Problem" (24) (see [RFC3209]) the
following sub-codes are defined. (see:
http://www.iana.org/assignments/rsvp-parameters/rsvp-
parameters.xhtml#rsvp-parameters-105)

```
+-------------+---------------------------+---------------+
| Error Value | Description               | Reference     |
| Sub-codes   |                           |               |
+-------------+---------------------------+---------------+
| TBA3        | Unsupported Diversity     | This document |
|             | Identifier Type           |               |
+-------------+---------------------------+---------------+
```

For Error Code "Notify Error" (25) (see [RFC3209]) the following
sub-codes are defined. (see:
http://www.iana.org/assignments/rsvp-parameters/rsvp-
parameters.xhtml#rsvp-parameters-105)

```
+-------------+---------------------------+---------------+
| Error Value | Description               | Reference     |
| Sub-codes   |                           |               |
+-------------+---------------------------+---------------+
| TBA4        | Route of XRO LSP          | This document |
|             | identifier unknown        |               |
| TBA5        | Failed to satisfy         | This document |
|             | Exclude Route             |               |
| TBA6        | Compliant path exists     | This document |
+-------------+---------------------------+---------------+
```

5. Acknowledgements

The authors would like to thank Luyuan Fang and Walid Wakim for
their review comments.

6. References

6.1. 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.

[RFC4874] Lee, CY., Farrel, A., and S. De Cnodder, "Exclude
          Routes - Extension to Resource ReserVation Protocol-
          Traffic Engineering (RSVP-TE)", RFC 4874, April 2007.

[RFC5553]   Farrel, A., Ed., Bradford, R., and JP. Vasseur,
"Resource Reservation Protocol (RSVP) Extensions for Path Key
Support", RFC 5553, May 2009.

6.2. Informative References

[RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and Y. Rekhter,
          "Generalized Multiprotocol Label Switching (GMPLS)
          User-Network Interface (UNI): Resource ReserVation
          Protocol-Traffic Engineering (RSVP-TE) Support for the
          Overlay Model", RFC 4208, October 2005.

[RFC4920] Farrel, A., Ed., Satyanarayana, A., Iwata, A., Fujita,
          N., and G. Ash, "Crankback Signaling Extensions for
          MPLS and GMPLS RSVP-TE", RFC 4920, July 2007.

[RFC5520]   Bradford, R., Ed., Vasseur, JP., and A. Farrel,
          "Preserving Topology Confidentiality in Inter-Domain
          Path Computation Using a Path-Key-Based Mechanism", RFC
          5520, April 2009.

[DRAFT-SRLG-RECORDING] F. Zhang, D. Li, O. Gonzalez de Dios, C.
          Margaria, "RSVP-TE Extensions for Collecting SRLG
          Information", draft-ietf-teas-rsvp-te-srlg-collect-04,
          in expert review.

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

[RFC5251] D. Fedyk, Ed., Y. Rekhter, Ed., D. Papadimitriou,
          R. Rabbat, L. Berger, "Layer 1 VPN Basic Mode",
          RFC 5251, July 2008.

[RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS
          Networks", RFC 5920, July 2010.

Contributors' Addresses

   Igor Bryskin
   ADVA Optical Networking
   Email: ibryskin@advaoptical.com

   Daniele Ceccarelli
   Ericsson
   Email: Daniele.Ceccarelli@ericsson.com

   Dhruv Dhody
   Huawei Technologies
   Email: dhruv.ietf@gmail.com

   Oscar Gonzalez de Dios
   Telefonica I+D
   Email: ogondio@tid.es

   Don Fedyk
   Hewlett-Packard
   Email: don.fedyk@hp.com

   Clarence Filsfils
   Cisco Systems, Inc.
   Email: cfilsfil@cisco.com

   Xihua Fu
   ZTE
   Email: fu.xihua@zte.com.cn

Gabriele Maria Galimberti
Cisco Systems
Email: ggalimbe@cisco.com

Ori Gerstel
SDN Solutions Ltd.
Email: origerstel@gmail.com

Matt Hartley
Cisco Systems
Email: mhartley@cisco.com

Kenji Kumaki
KDDI Corporation
Email: ke-kumaki@kddi.com

Ruediger Kunze
Deutsche Telekom AG
Email: Ruediger.Kunze@telekom.de

Lieven Levrau
Nokia
Email: Lieven.Levrau@nokia.com

Cyril Margaria
cyril.margaria@gmail.com

Julien Meuric
France Telecom Orange
Email: julien.meuric@orange.com

Yuji Tochio
Fujitsu
Email: tochio@jp.fujitsu.com

Xian Zhang
Huawei Technologies
Email: zhang.xian@huawei.com

Authors' Addresses

   Zafar Ali
   Cisco Systems.
   Email: zali@cisco.com

   Dieter Beller
   Nokia
   Email: Dieter.Beller@nokia.com

   George Swallow
   Cisco Systems
   Email: swallow@cisco.com

   Fatai Zhang
   Huawei Technologies
   Email: zhangfatai@huawei.com