Network Working Group S. De Cnodder
Internet Draft C. Pelsser
Expiration Date: January 2005

July 2004

Protection for inter-AS MPLS tunnels
draft-decnodder-ccamp-interas-protection-00.txt

Status of this Memo

Abstract

This document describes a solution for link protection, node protection, Shared Risk Link Group (SRLG) protection and fast recovery of inter-AS packet based LSPs. These problems are highlighted in [ASREQ]. The proposed solution is based on RSVP-TE [RFC3209] as recommended by [ASREQ]. Only the protection of links between 2 ASs, the protection of their SRLGs and of the nodes at the border of an AS are in the scope of this document.

1. Introduction

This document describes a solution for the following requirements from [ASREQ]:

1) link protection

2) node protection

3) SRLG protection

4) fast recovery

5) based on RSVP-TE [RFC3209]

MPLS Fast-Reroute techniques based on [FRR] together with the RSVP objects eXclude Route Object (XRO) and Explicit eXclude Route Subobject (EXRS), as defined in [XRO], will be used to fulfill the above requirements. Only the protection of links between 2 ASs, the protection of their SRLGs and of the nodes at the border of an AS are in the scope of this document.

Section 2 proposes to tunnel inter-AS LSPs through intra-AS LSPs inside an AS, as described in [HIER]. This tunneling favors the confidentiality requirement concerning intra-AS topologies [ASREQ] as well as the establishment of inter-AS LSPs. The establishment of inter-AS LSPs will not be studied further in this draft. In this document it is assumed that ASes define their SRLGs independently from the SRLGs in other ASes.

Section 3 shows that an end-to-end recovery LSP, crossing multiple ASs, can only provide link and node protection. For SRLG protection and fast recovery, the methods in [FRR] have to be used. Section 5 and section 6 describe how these methods can be used for the protection of inter-AS LSPs with detour LSPs and bypass tunnels. Nodes other than those mentioned in this document must use the methods in [FRR] to establish detour LSPs or bypass tunnels. Moreover, these nodes establish detour LSPs that merge with the working LSP in the same AS where they are originated, or these nodes establish/use bypass tunnels that terminate in the same AS as where they originate.

2. Inter-AS LSP tunneled through an intra-AS LSP

To improve scalability and confidentiality (which is outside the scope of this document), an inter-AS LSP can be tunneled through an intra-AS LSP [HIER]. For instance, in Figure 2 of Section 4, the link between R21 and R22 could be an LSP passing multiple core routers. And, the inter-AS LSP is tunneled through this LSP. Whether an inter-AS LSP is tunneled or not through an intra-AS LSP is not relevant for this document since this intra-AS LSP behaves as any other link in the network.

The procedures described in the following sections apply for inter-AS link, node and SRLG protection of inter-AS LSPs whether they are tunneled or not.

3. Problems in SRLG protection with disjoint end-to-end LSPs

The motivation to support fast-reroute techniques as described in [FRR] is twofold: first of all, it supports fast recovery, and, second, it provides SRLG protection, which is not the case for a disjoint end-to-end LSP. The problem to support SRLG protection, with the latter method, is described in this section.

There are different ways to provide end-to-end protection of inter-AS LSPs. A first possibility is to establish a secondary path that crosses different ASs than the working LSP. An alternative is to establish an LSP that follows the same AS path to the destination as the working LSP, i.e. it crosses the same ASs in the same order, but is link or node disjoint from the working LSP. However, these two solutions do not permit to establish an LSP that is disjoint from the SRLGs of the working LSP. That is, it is not possible to protect the working inter-AS LSP against SRLGs failures with a single end-to-end link or node disjoint LSP. This is due to the fact that ASs may possess links belonging to the same SRLG even if these ASs do not have the same convention to designate this SRLG. The allocation of SRLGs is not consistent among the ASs.

To explain this, we introduce the concepts of SRLG scope and SRLG ID scope. The SRLG scope of a particular SRLG is the collection of nodes that have a consistent understanding of that particular SRLG. This means that all nodes in the SRLG scope see the same set of links belonging to that SRLG. The nodes in an SRLG scope will not be aware of links outside the SRLG scope that may share for instance physical resources with links in the SRLG scope that are in the SRLG, and hence could fail at the same time.

Not all nodes in a particular SRLG scope must use the same SRLG ID to identify that particular SRLG. An SRLG scope can consist of different non-overlapping sections and each such section can use a different SRLG ID to refer to the SRLG. At the boundaries of these sections, there exists a one-to-one mapping of the corresponding SRLG IDs that identify the same SRLG. Such section of an SRLG scope where a particular SRLG ID is used to identify the SRLG, is called the SRLG ID scope.

Example 1: If a particular SRLG groups all the links of AS 1 and AS 2 that use a particular physical resource, and hence could fail at the same time, then the SRLG scope consists of AS 1 and AS 2. If AS 1 uses SRLG ID x to identify that SRLG and AS 2 uses SRLG ID y, then there are two SRLG IDs and their corresponding SRLG ID scopes are AS 1 and AS 2, and there is a one-to-one mapping of the SRLG IDs between

these SRLG ID scopes, i.e. x in AS 1 translates to y in AS 2.

Example 2: Suppose that a particular SRLG groups links in AS 1 that could fail at the same time and that another SRLG groups links in AS 2, i.e. the SRLG scope of the SRLGs are their corresponding ASs. AS 1 and AS 2 may use the same SRLG ID. Using the same SRLG ID does not mean that the 2 SRLGs are linked to each other is some way.

```
      AS1              AS2              AS3
 /----------\  /-------------- \  /------------\


        R12 ---- R21 ---- R23 ---- R31
       /           \                 \
      /             \                 \
 R11                 R25                R33
      \               \               /
       \               \             /
        R13 ---- R22 ---- R24 ---- R32
```

Figure 1: end-to-end SRLG protection

When SRLGs whose corresponding SRLG scope does not contain all ASs crossed by the inter-AS LSP, an end-to-end recovery LSP may fail to provide SRLG protection as explained by the example that follows. Suppose we have a working LSP going from R11 in AS1 to R33 in AS3 through R13, R22, R24 and R32. It is not possible to protect this LSP against SRLG failures with a recovery LSP crossing for instance R12, R21, R23 and R31 when there are SRLGs with SRLG scopes corresponding to a single AS (AS1, AS2, or AS3) or only 2 ASs. Suppose the SRLG scopes consists of only 1 AS, then AS3 could have links which can fail together with links in AS1 and neither AS1 nor AS3 will be aware of it. For example, link R11-R13 and link R31-R33 may share a physical resource but in case there are no SRLGs defined with SRLG scope containing AS1 and AS3, this will not be known by any of the ASs. This example relies on the fact that different ASs may use the same resources to join different nodes in their respective domain. A similar situation occurs when the working and the recovery LSP do not share the same AS path but instead partially cross different ASs.

In this document we consider SRLG scopes consisting of an AS. Therefore, this document only focuses on local protection, as defined in [FRR], because it is not possible to provide full protection of SRLGs with such SRLG scopes, along an inter-AS LSP, with a single end-to-end LSP. The solution proposed in this document enables the provision of link, node and SRLG protection of inter-AS LSPs.

4. Network model and terminology

To illustrate the procedures described in the next sections, the following network model is used:

```
              AS1                 AS2
        /-------------\    /------------\


         +---+   +---+      +---+   +---+
   ------|R11|---|R12|------|R21|---|R22|------
         +---+   +---+      +---+   +---+
           |       |          |       |
           |       |          |       |
           |       |          |       |
         +---+   +---+      +---+   +---+
   ------|R13|---|R14|------|R23|---|R24|------
         +---+   +---+      +---+   +---+
           |       |          |       |
           |       |          |       |
           |       |          |       |
         +---+   +---+      +---+   +---+
   ------|R15|---|R16|------|R25|---|R26|------
         +---+   +---+      +---+   +---+
```

Figure 2: a reference network model

The working LSP is established from a certain node (not shown on the figure) and goes over routers R13, R14, R23, and R24 towards the destination (also not shown on the figure). AS1 is referred to as the upstream AS of AS2, and AS2 is referred to as the downstream AS of AS1.

An "egress AS-BR" or a "primary egress AS-BR" is an Autonomous System Border Router (AS-BR) at which the working LSP leaves an AS. In the network example, in figure 2, this is router R14, inside AS1.

An "ingress AS-BR" or a "primary ingress AS-BR" is an AS-BR at which the working LSP enters an AS. In the network example, this is router R23, inside AS2.

A "secondary egress AS-BR" is an AS-BR at which the bypass tunnel or the detour LSP leaves an AS. In the network example, this could be router R12 or R16, in AS1.

A "secondary ingress AS-BR" is an AS-BR at which the bypass tunnel or the detour LSP enters an AS. In the network example, this could be router R21 or R25, in AS2.

"Inter-AS link protection" is the protection of an LSP against a failure of the link connecting two ASs on the path of the LSP. In the network example, the inter-AS link R14-R23 is to be protected.

"Inter-AS node protection" is the protection of an LSP against an AS-BR failure. This can be the egress AS-BR, R14, or the ingress AS-BR, R23, for the considered example.

"Inter-AS SRLG protection" is the protection of an LSP against a simultaneous failure of all links that belong to certain SRLGs which also contain the inter-AS link (R14-R23 in figure 2).

Other terminology and abbreviations are taken from [FRR].

5. Protection with detour LSPs

5.1 Link protection with detour LSPs

5.1.1 Procedures for the egress AS-BR

The primary egress AS-BR has to establish a detour LSP to protect the inter-AS link. The destination of the detour LSP will be the same as the destination of the working LSP. The detour LSP may merge with the working LSP at any downstream node or with other detour LSPs of the same working LSP, established by nodes downstream of the link to be protected. The egress AS-BR has to determine a secondary egress AS-BR and then it can perform a path calculation towards this AS-BR.

The primary egress AS-BR can select any other AS-BR as secondary egress AS-BR but it is recommended to select an AS-BR that is connected to the downstream AS of the working LSP (i.e. the AS where the primary ingress AS-BR is located). In case this condition is not met, it could be for instance possible that the downstream AS of the detour LSP chooses a path that goes through the AS where the detour LSP was originated causing loops. This is illustrated in Figure 3. Suppose the working LSP crosses the domains AS1, AS2, AS3 and AS4 in that order. The detour LSP protecting the link between AS2 and AS3 does not take the alternative link between AS2 and AS3 but it takes AS6, then AS6 could take AS5 as next AS and then at the end the detour LSP arrives at AS1 where it merges with the working LSP. It is clear that such detour does not protect the link that it is supposed to protect. Note that it is only recommended and not a must to take the same downstream AS because there are ways to solve this problem by excluding ASs [XRO] but this would be a rather complex solution.

```
      ________     ________     ________     ________
     (        )   (        )-----(        )-----(        )
     (  AS1   )-----(  AS2   )   (  AS3   )   (  AS4   )
     (________)   (________)-----(________)-----(________)
         |             |             |             |
         |             |             |             |
         |             |             |             |
      ___|___       ___|___       ___|___       ___|___
     (        )   (        )   (        )   (        )
     (  AS5   )-----(  AS6   )-----(  AS7   )-----(  AS8   )
     (________)   (________)   (________)   (________)
```

Figure 3: a detour LSP merging at a wrong place

In addition, it is recommended that the detour LSP merges in the AS where this downstream ingress AS-BR is located (the merging node could be the ingress AS-BR itself) if the destination of the working LSP is not in the downstream AS. For example, in figure 3, the detour LSP protecting the link of the working LSP between AS2 and AS3 should merge with the working LSP in AS3. If this does not happen, AS3 could select AS7 as next AS for the detour LSP and from then on A7 could select AS6, which further goes to AS5 and AS1 where the detour LSP merges with the working LSP upstream from the failure to protect. This recommendation also improves the scalability of the solution since merging LSPs diminishes the number of states to be maintained, the bandwidth to be reserved, and so on.

Therefore, the ERO for the detour LSP starting at the egress AS-BR should contain several path’s segments. It should first contain a strict or a loose path towards the secondary egress AS-BR followed by a segment of the RRO of the working LSP. The latter segment begins at the last hop in the downstream AS (the egress AS-BR in the downstream AS) of the working LSP and contains all hops thereafter up until the destination. For instance, in Figure 3, with a working LSP crossing AS1-AS2-AS3-AS4, the ERO of the detour LSP protecting the link of the working LSP between AS2 and AS3, should at least contain the routers of the working LSP in AS4 and the egress AS-BR of AS3 recorded in the RRO. That is, the ERO of the detour LSP at least contains: (1) A strict or loose path toward the secondary egress ASBR (2) The path of the working LSP starting at the last hop inside the downstream AS and ending at the destination of the working LSP. In the example network of Figure 2, we have a working LSP crossing the routers R13, R14, R23, R24, etc. Suppose that the selected egress AS-BR is R16 and the calculated path towards R16 is R14-R13-R15-R16 (R14 is originator of detour LSP) assuming that R14-R16 does not match the constraints of the detour LSP. The ERO of the detour LSP protecting link R14-R23 should therefore be composed of routers R13-R15-R16 (all strict)

followed by R24 (with loose flag set) and the following routers after R24 of the working LSP in the downstream AS of AS2, which is not shown in Figure 2. The path between R16 and R24 has to be calculated by R16 and R25.

There are two possible methods to determine the secondary egress AS-BR at the primary egress AS-BR. (1) The egress AS-BR can be manually configured with other AS-BRs that peer to the same AS or (2) it can lookup in its BGP table to find an other entry such that the AS-path has the same AS next hop as the currently selected entry. Option (1) is feasible because the number of links between 2 ASs is usually limited to only a small number of links.

It could be possible that the primary egress AS-BR is the same router as the secondary egress AS-BR and that the primary ingress AS-BR is the same router as the secondary ingress AS-BR. In this particular case when there are multiple links between the AS-BRs, the detour LSP must simply use an inter-AS link that is not the one used by the working LSP, and no path computation has to be done at the egress AS-BR.

The use of the LSP-Merge subobject, defined in Appendix A, is optional to provide link protection. This is an ERO subobject that forces the merging at the next node in the ERO and it makes sure that this merging node can switch traffic coming from the merging detour LSP to the originating detour LSP. See Appendix A for a description and see Section 5.3.1 for more details on where this subobject is mandatory to use (in case of SRLG protection).

5.1.2 Procedures for the ingress AS-BR

No extra procedures are required.

The detour LSP may merge with the working LSP at this node.

5.1.3 Procedures for the secondary egress AS-BR

The secondary egress AS-BR completes the path in the ERO by selecting a secondary ingress AS-BR in the downstream AS. If there is no ERO present, then the tunnel end point address in the Session object has to be used to route the Path message.

5.1.4 Procedures for the secondary ingress AS-BR

The secondary ingress AS-BR completes the ERO with a path towards the next subobject in the ERO. The LSP should merge with the working LSP at the node that processes the LSP-Merge subobject (if that subobject is present), if it was not yet merged at this point. If no ERO is present inside the Path message of the detour LSP, the path is computed based on the tunnel end point address.

5.2 Node protection with detour LSPs

The procedures and recommendations are the same for the protection of an ingress AS-BR failure as for link protection, with the exception that the egress AS-BR has to include an XRO object or an EXRS subobject [XRO] with the ingress AS-BR to exclude.

For the protection of the egress AS-BR, the same holds except that the procedure applies to the router on the path of the working LSP preceding the egress AS-BR. The method to determine a secondary egress AS-BR is the same as for link protection: either manual configuration or by using BGP routing information, if it is available. Note that the first solution requires more configuration as for link protection in case this router peers with more than one AS-BR.

5.3 SRLG protection with detour LSPs

Similar procedures as for link protection apply for SRLG protection. In addition, the secondary egress AS-BR must be an AS-BR that peers with the downstream AS of the working LSP. And, the detour LSP must merge in that AS. The former condition is necessary because only the two peering ASs know the SRLGs of the inter-AS link and the latter condition implies that the LSP-Merge subobject must be used. This subobject is inserted inside the ERO to indicate the node where merging needs to be done (see appendix A). The next subsections describe in more details the procedures to be performed at the nodes involved in the establishment of such detour LSP.

5.3.1 Procedures for the egress AS-BR

The egress AS-BR has to include an XRO object or an EXRS subobject to exclude the SRLGs of the inter-AS link. The XRO or the EXRS must include a list of SRLGs (defined for the AS containing the PLR) corresponding to the inter-AS link as well as a reference to this link. If the egress AS-BR can calculate a strict path to reach the secondary egress AS-BR, then the list of SRLGs may be removed. Only the reference to the link for which the detour LSP has to be SRLG disjoint is then required (see section 5.3.2). The secondary ingress AS-BR has to use the information in the XRO or EXRS to further calculate a path for the detour LSP.

To ensure merging inside the downstream AS, the LSP-Merge subobject (see Appendix A) has to be included in the ERO by the egress AS-BR. The LSR where the detour LSP is merged with the working LSP has to

ensure that it can perform a switch-over from the incoming detour LSP containing the LSP-Merge subobject to its originating detour LSP in case the next link has an SRLG in common with the inter-AS link. This is because in this case, both links can fail at the same time such that both detour LSPs will be activated at the same time. In other words, the PLR has to send the traffic from the main LSP or the incoming detour LSP on the departing detour LSP protecting the failure of the downstream resources, when protection is in use.

5.3.2 Procedures for the secondary egress AS-BR

The secondary egress AS-BR selects a next hop and the XRO or EXRS contains a reference to the link for which the detour LSP has to be SRLG disjoint. No list of SRLGs should be included because the SRLG IDs are local to an AS, which means that if a list of SRLG IDs would be sent to the next hop, then this node would not understand the IDs. Therefore only the reference to the inter-AS link is useful. This link is referenced by means of its IP address, see [XRO]. The secondary egress AS-BR thus removes the list of SRLGs related to the inter-AS link, if such a list of SRLGs was present.

5.3.3 Procedures for the ingress AS-BR

No extra procedures required.

5.3.4 Procedures for the secondary ingress AS-BR

If the secondary ingress AS-BR cannot compute a full path towards the node immediately preceeding the LSP-merge subobject, then the secondary ingress AS-BR adds the list of SRLGs of the inter-AS link to the received XRO object or EXRS subobject, respectively, if not already present. These SRLGs are known by the nodes inside this AS. This is required because the LSP can cross nodes inside the AS which do not know the SRLGs of the inter-AS link, but only the SRLGs of intra-area links, hence just a reference to a link whose SRLGs have to be excluded is not sufficient. An alternative would be to distribute inter-AS links and their SRLGs inside the IGP.

5.3.5 Path calculation

To allow the egress AS-BR and the secondary ingress AS-BR to calculate a path, the SRLGs of the inter-AS links towards the same downstream AS (upstream AS, respectively) as the working LSP have to be known. This could be achieved through manual configuration of the SRLGs of other inter-AS links to the same downstream/upstream AS at each AS-BR. For instance, in Figure 2, at R14 and R23, the SRLGs of R12-R21 can be configured such that they are known for the path calculation, and at R12, R16, R21 and R25, the SRLGs of R14-R23 can

be configured. An other option is to flood this information via BGP extensions to be defined or to distribute these links and their SRLGs inside the IGP. It is not assumed that nodes other than AS-BRs having a link to the same downstream/upstream AS know the SRLGs of these inter-AS links. If this would be the case, then the procedures above can be simplified, e.g., the egress AS-BR in Section 5.3.1 does not have to include a list of SRLGs anymore when only a partial path can be computed.

Also the secondary egress AS-BR has to know the SRLGs of the inter-AS link used by the working LSP. This is to allow the egress AS-BR to select a link in case there are multiple links towards the downstream AS, and to check if the link is indeed SRLG disjoint from the inter-AS link used by the working LSP.

5.3.6 SRLG and node protection

In this section we consider the protection of the egress AS-BR and of the SRLGs of the link preceding this AS-BR. The SRLG protection of the other intra-domain links and their downstream node is solved by [FRR]. Protection of the egress AS-BR and SRLG protection of the link preceding the egress AS-BR is best solved by using two detour LSPs at the node on the path of the working LSP preceding the egress AS-BR: a detour to protect against the SRLGs of the intra-AS link and a second detour LSP that is established using the procedures for node protection as described in the previous section. The detour protecting against the SRLGs has to merge in the same AS, i.e. it has to merge with the working LSP at the egress AS-BR. This is because other ASs do not know this intra-AS link, nor its SRLGs. To ensure that merging occurs at the egress AS-BR, the RRO of the working LSP should be fully included in the ERO of the detour LSP together with the LSP-Merge subobject. The ERO should be further prepended by a path, which is SRLG disjoint with the downstream link of the PLR on the working LSP (i.e. the intra-AS link), computed towards the egress AS-BR. This could only be a partial path towards the egress AS-BR in which case an XRO object or an EXRS subobject, containing the SRLGs to avoid, has to be added. It has to be ensured that these 2 detour LSPs do not merge, which means that at least one of the detour LSP should be a sender-template specific detour LSP.

The egress AS-BR must ensure that it can do a switch-over from the incoming detour LSP protecting against a failure of the preceding link to its originating detour LSP. This is because the preceding link and the inter-AS link can belong to the same SRLG, hence they can fail at the same time. For this reason, the LSP-Merge subobject must be used in this case.

If protection of the ingress AS-BR is requested, in addition to SRLG

protection, the egress AS-BR also has to put the ingress AS-BR in the XRO or EXRS like it was done for node protection.

The use of 2 detour LSPs (one for SRLG protection and the other for node protection) is also recommended when the ingress AS-BR is to be protected. In this case, if only 1 detour LSP is used, and the LSP only crosses 1 hop in the downstream AS (i.e. ingress AS-BR and egress AS-BR in the downstream AS are the same router), the detour LSP setup would not be able to provide SRLG protection. This is because the detour LSP crosses 3 ASs in this case: the AS where it originates, the single-hop AS (the hop to be protected), and the AS where it merges again, and the latter AS is not anymore aware of the SRLGs of the link to be protected because that link is between the first two ASs. This is illustrated in Figure 4. The working LSP traverses R12-R22-R32-R24 and node R22 together with the SRLGs of R12-R22 has to be protected. A single detour LSP protecting the SRLGs and R22 would traverse R12-R11-R21-R31 but R31 in AS3 cannot further expand the ERO of the detour LSP because it does not know the SRLGs or the SRLG IDs of R12-R22 between AS1 and AS2 (assuming local SRLGs). Therefore, 2 detour LSPs must be used: a detour LSP traversing R12-R11-R21-R22 for SRLG protection, and a detour LSP traversing for instance R12-R11-R21-R31-R32 to protect R22.

```
          AS1       AS2          AS3
        /-----\  /-----\  /--------------\


         +---+    +---+    +---+    +---+
   ------|R11|----|R21|----|R31|----|R33|------
         +---+    +---+    +---+    +---+
           |        |        |        |
           |        |        |        |
           |        |        |        |
         +---+    +---+    +---+    +---+
   ------|R12|----|R22|----|R32|----|R24|------
         +---+    +---+    +---+    +---+
```

Figure 4: a single-hop AS

In case of node and SRLG protection or in case of SRLG protection only, it is required to use sender-template specific detour LSPs to avoid that detour LSPs merge with each other.

6. Protection with bypass tunnels

The problem of protection by means of bypass tunnels can be split into two parts:

a) The bypass tunnel has to be signaled over a path that is disjoint with the network resources that it protects.

b) After the bypass tunnels are established, an appropriate bypass tunnel has to be selected for each particular working LSP such that the protection requirements for that LSP are met.

The first part is very similar to the establishement of detour LSPs: an XRO object or an EXRS subobject can be used to signal the bypass tunnel such that it is disjoint from the network resources used by the working LSP. The same recommendations as for detour LSPs apply, i.e. it is recommended that the downstream AS of the bypass tunnel and the working LSP are the same AS. Additionally, as two detour LSPs are required for SRLG protection of the upstream link of an egress ASBR and the egress ASBR itself, two bypass tunnels are also required to protect these resources. Note that the LSP-Merge subobject is not used for bypass tunnels as it was the case for detour LSPs because bypass tunnels do not merge with the working LSP at the far-end of the bypass tunnel, but they are terminated at that node.

The difficulty in providing protection with bypass tunnels lies in the selection of appropriate bypasses for the protection of given resources.

To select a bypass tunnel, the PLR has to take a bypass tunnel that it originates and that fulfills the following requirements:

a) The bypass tunnel must fulfill the appropriate constraints (bandwidth, link affinities, ...).

b) The bypass tunnel must be disjoint with the link/node/SRLGs to be protected.

c) The destination of the bypass tunnel must be the next-hop node (resp. next-next-hop node) of the working LSP, or a node further downstream on the path of the working LSP, in case of link protection (resp. node protection).

The first two requirements can be achieved since all required information is locally available in the PLR. This is because the PLR has established the candidate bypass tunnels, hence it knows the bandwidth and the resources protected by the bypass tunnel. Complying with the third requirement is more difficult. Generally, the PLR must check if the destination of the bypass tunnel belongs to one of the nodes listed in the RRO of the Resv message of the working LSP. Usually the RRO contains interface addresses and the destination of a bypass tunnel may be a different interface address or the node-id of

a router. This means that the PLR has to map the addresses listed in the RRO of the working LSP to the destination address of the bypass tunnel. In an intra-area environment this is possible since this information is available in the IGP topology, but in the inter-AS case, this information is not anymore available locally in the PLR. There are multiple methods to solve this problem:

Solution A: use [NODEID] where the node-id of the routers are put in the RRO of the Resv message of the working LSP and the node-id is also put in the RRO of the Resv message of the bypass tunnel if the destination was not the node-id. In this way, the PLR simply has to compare the node-ids in the RRO of the working LSP with the destination of the bypass tunnel or with the node-id in the RRO of the bypass tunnel.

Solution B: use the interface address that would be recorded in the RRO of the working LSP as destination of the bypass tunnel. For instance, when the link between ASBR1 and ASBR2 is to be protected, the destination address would be the address of the interface on ASBR2 towards ASBR1. If this link is unnumbered, the destination address used is the node-id that is mentioned in the RRO of the working LSP. This is sufficient to identify the common node on the working LSP and the bypass tunnel. When node protection is to be provided and the destination of the Bypass Tunnel is the next-hop of the protected node (next-next hop from the PLR point of view), the destination of the bypass tunnel should be the address of the interface on the next-next-hop router that goes towards the node being protected. Multiple bypass tunnels must be used in case of parallel links. Although the interface is used as destination, the bypass tunnel enters the node via another link and a failure of the interface used as destination of the bypass tunnel must not lead to the failure of the bypass tunnel itself (this is in particular important for link protection).

Until now, we supposed that the bypass tunnels were manually configured, with the destination being part of the configuration. But, bypass tunnels can also be signaled automatically when the first working LSP is established. Therefore, we have to determine the destination of these dynamically established bypass tunnels. In case of solution B, the information about the interface addresses in the RRO of the working LSP can be used as a destination address. In case the node-id is put in the RRO, then this node-id can be used.

7. Security Considerations

TBD

Acknowledgments

This work was partially supported by the DGTRE in the framework of the TOTEM project. The authors would like to thank Olivier Bonaventure, Adrian Farrel, Cheng-Yin Lee, Dimitri Papadimitriou, and Vishal Sharma for their useful comments and interesting discussions.

References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

[ASREQ] Zhang, R., Vasseur, JP., (Editors), "MPLS Inter-AS Traffic Engineering requirements", draft-ietf-tewg-interas-mpls-te-req-07.txt, work in progress.

[FRR] Pan, P., Atlas, A. (Editors), "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", draft-ietf-mpls-rsvp-lsp-fastreroute-03.txt, work in progress.

[XRO] Lee, CY., Farrel, A., De Cnodder, S., "Exclude Routes - Extension to RSVP-TE", draft-ietf-ccamp-rsvp-te-exclude-route-00.txt, work in progress.

[HIER] Kompella, K., Rekhter, Y., "LSP Hierarchy with Generalized MPLS TE", draft-ietf-mpls-lsp-hierarchy-08.txt, work in progress.

[NODEID] Vasseur, J.-P., Ali, Z., Sivabalan, S., "Definition of an RRO node-id subobject", draft-ietf-mpls-nodeid-subobject-01.txt, work in progress.

Authors Addresses

Stefaan De Cnodder
Alcatel
Francis Wellesplein 1
B-2018 Antwerpen
Belgium

Email: stefaan.de_cnodder@alcatel.be

Cristel Pelsser

INGI
Place Sainte Barbe, 2
B-1348, Louvain-La-Neuve
Belgium

Email: cpe@info.ucl.ac.be

Appendix A: LSP-Merge subobject

The LSP-Merge subobject is a new subobject in the Explicit Route Object (ERO). The procedures defined in [RFC3209] section 4.3.4.1 to select the next hop are modified as follows: if after step 3 of the next hop selection process the node finds an LSP-Merge subobject in front of the ERO, i.e. the LSP-Merge subobject is the first subobject in the ERO after removing the subobjects belonging to the local abstract node, then the LSP has to merge with an LSP with the same Session object and LSP ID at the current node, if such an LSP exists. If no such LSP exists, then the detour LSP is rejected and a ResvErr with errorcode TBD is sent to the originating node.

The LSP with which the LSP containing the LSP-Merge subobject merges must be a working LSP, i.e. it may not contain a DETOUR object. In addition the abstract node where the merging occurs must ensure that in case of a failure, the traffic can be switched from the LSP containing the LSP-Merge subobject to a recovery LSP that was established by the merging node to protect the working LSP. If these merging conditions cannot be met, the "SRLG protection available" flag inside RRO subobjects, of appendix B, is set to zero. This indicates to the source that SRLG protection is not provided for the working LSP.

```
 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      |            Resvd              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

L

Set to zero.

Type

TBD.

Length

The length field is set to 4.

Resvd

Set to zero on transmission and ignored on reception.

Appendix B: SRLG protection desired

Currently [FRR] does not specify how SRLG protection can be requested by the Head-End LSR. One way to do this is to define an "SRLG protection desired" flag in session attribute object. We will not further investigate this since it is outside the scope of this document.

In case two detours or bypass tunnels are available to provide SRLG and node protection, then the "local protection available" flag is set in the corresponding RRO subobject. Similarly, the "bandwidth protection" flag of the RRO subobject is set when both detours or bypass tunnels provide the requested bandwidth. Note that in case of SRLG protection, it is required to use sender-template specific detour LSP to avoid merging with other detour LSPs of the working LSP.

Intellectual Property Considerations

Full Copyright Statement