Internet Engineering Task Force
Internet Draft
draft-guo-rsvp-te-extensions-00.txt
July 2001

Expiration Date Jan 2002

Dan Guo, Jibin Zhan,
Nanda Ravindran, Prakash Siva
Wenjing Chu, Robert Cooper
(Turin Networks)

Raymond Cheung, James Fu
(Sorrento Networks)

Extensions to RSVP-TE for Supporting Diverse Path Protection
<draft-guo-rsvp-te-extensions.txt>

Status of this Memo

1. Abstract

This draft describes two specific extensions to RSVP-TE. The first extension is concerned about the scalability of RSVP-TE. It proposes expanding the length of tunnel ID in RSVP-TE session object, from 16 bits to 32 bits, in order to increase the upper limit of LSPs originated from one node. The second extension is to propose a new object for representing a protection group. A protection group can tie two or more diverse LSPs between a source-destination pair of nodes. This extension is warranted due to the importance and wide-spread applications of LSP protection switching mechanisms. With this extension, protection group information no longer is embedded into vendor-specific opaque objects. These two extensions only require minor changes to RSVP-TE protocol. When adopted into RSVP-TE, they will improve the scalability of RSVP-TE and simplify the support of diverse LSP protection mechanisms.

2. 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.

3. Introduction

The Generalized MPLS (GMPLS) extends MPLS to encompass TDM (e.g., SONET /SDH), Lambda Switch (LSC) and Fiber-Switching (FSC) [GMPLS-ARCH]. RSVP-TE, a GMPLS-based signaling protocol, is required to handle the signaling for provisioning of Label Switched Paths (LSPs) at a wide range of granularities [RSVP-TE][GMPLS-RSVP]. For example, SONET and SDH are two TDM standards widely used by operators to transport signals multiplexed over optical links. They possess a multiplexing hierarchy that includes a coarse circuit such as STS-48 and a fine-granularity circuit such as VT 1.5 [SONET]. As a result, it is of importance for RSVP-TE to be scalable in supporting a variety of switching technologies.

Additionally, there have been considerable efforts towards devising the mechanism for supporting LSP protection and restoration. In the case of optical transport networks (OTN), protection and restoration of transport circuits is a capability universally required [BMS][RECOV]. With the consideration of shared risk link group (SRLG) properties (see [SRLG]), two or more diverse circuits can be provisioned between a pair of nodes, to support various protection switching schemes (e.g., 1+1, 1:1, 1:n, m:n).

The goal of this draft is to describe two specific extensions to RSVP-TE. The first extension is concerned about the scalability of RSVP-TE. It proposes expanding the length of tunnel ID in RSVP-TE session object, from 16 bits to 32 bits, in order to increase the upper limit of LSPs originated from one node. In the latest RSVP-TE draft, tunnel ID occupies 32 bits but the higher 16 bits is mandated to be 0. This extension will greatly extend the addressing space for tunnel ID.

The second extension is to propose a new object for representing a protection group. The protection group is a concept for tying two or more diverse LSPs between a source-destination pair of nodes. This extension is warranted due to the importance and wide-spread applications of the LSP protection capability. For 1+1 or 1:1 protection switching schemes, one LSP is a working LSP and the other LSP is the protection LSP. For 1:N (or M:N) protection switching scheme, one LSP (or M LPSs) is the protection LSP shared by N working LSPs. Without this extension, the current approach is to have each vendor create private (opaque) objects for representing this information. This approach impairs the interoperability, since different nodes may be from different vendors using different coding schemes.

These two extensions only require minor changes to RSVP-TE protocol. Their implementation is straight-forward. When adopted into RSVP-TE, they will improve the scalability of RSVP-TE and simplify the support of diverse LSP protection mechanisms.

4. Extension 1: 32 Bits for Tunnel ID

An RSVP session is uniquely identified by a destination IP address, a tunnel ID, an LSP ID, and an extended tunnel ID. An extended tunnel ID is usually set to the source node IP address. An LSP ID is commonly used for supporting the "make-before-break" feature.

Currently, RSVP-TE uses 16 bits to represent a tunnel ID while the 16 bits immediate to its left are mandated to be 0 [RSVP-TE].

LSP_TUNNEL_IPv4 Session Object

Class = SESSION, LSP_TUNNEL_IPv4 C-Type = 7

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

IPv4 tunnel end point address

IPv4 address of the egress node for the tunnel.

Tunnel ID

A 16-bit identifier used in the SESSION that remains constant over the life of the tunnel.

For SONET/SDH, 16 bits are not enough. For example, at the VT 1.5 level, under current specifications, a node can have at most 1.5Mps*2**16, which is 96 Gbps. If a SONET node has more than 100 Gbps of combined throughput, we may run out of the available tunnel IDs.

We propose a simple modification that allows tunnel ID to occupy 32 bits:

Class = SESSION, LSP_TUNNEL_IPv4 C-Type = 7

```
    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                |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Tunnel ID  (32 bits)                                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      Extended Tunnel ID                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Tunnel ID
A 32-bit identifier used in the SESSION that remains constant over the life of the tunnel.

5. Extension 2: Protection Group object

As discussed in section 3, two or more diverse paths are often provisioned between a node-pair. Diverse paths are obtained by applying the SRLG constraint criteria to the constraint-based path computation. They take into account resource and logical structure disjointness that implies a lower probability of simultaneous lightpath failure. Diverse paths can form a protection group for providing various protection switching schemes (including 1+1, 1:1, 1:N, M:N). A protection path in a protection group can carry traffic identical to working traffic, or carry extra traffic, or simply stand by.

When a protection group is formed and provisioned, it is assigned an identifier (ID) by the traffic engineering (TE) manager. A protection group is uniquely defined by <source ID, destination ID, protection group ID>.

A protection group contains a collection of LSPs. For example, one primary LSP and one protection LSP for 1:1 or 1+1 protection schemes, or N working LSPs and one protection LSP for 1:N protection.

We propose to add a new object for representing a protection group (PG). The protection group provides a way to bond a number of LSPs together. It is an optional object at the path level.

```
<Path Message> ::=  <Common Header> [ <INTEGRITY> ]
                      <SESSION> <RSVP_HOP>
                      [ <TIME_VALUES> ]
                      [ <EXPLICIT_ROUTE> ]
                      [ PROTECTION_GROUP_OBJ ]
                      <LABEL_REQUEST>
                      [ <SESSION_ATTRIBUTE> ]
                      [ <POLICY_DATA> ... ]
                      <sender descriptor>
```

Class: TBD; C-type: TBD;

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |F| Type| Index | reserved      |    M           |      N        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                 PROTECTION GROUP ID                            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

F: 1 bit Flag to indicate whether this path is protection or working;

F=0: working path;
F=1: protection path;

Type: 3-bit field, to indicate protection type;
0: 1+1;
1: 1:1;
2: 1:N;
3: M:N
Index: 4-bit field to indicate the rank of this path.

For example, when F=0 (i.e., working path), Type is 2 (i.e.,1:N) and index =2, it means this path is the 2nd working.

Reserved: 8-bit field for future usage.

M: 8-bit field.
N: 8-bit field.

When type=0 (i.e., 1+1) or type=1 (i.e., 1:1), M and N must be 0;
When type=2 (i.e., 1:N), M must be 0 and N can be 0 to 255;
When type=3 (i.e., M:N), M and N can be 0 to 255.

Protection Group ID: 32-bit field to identify a protection group together with source ID and destination ID.

Additional information regarding traffic types, such as extra traffic or Non-preemptible Unprotected Traffic (NUT), can be added into this object. This is left for future study.

When a node receives a path message which contains the protection group object, it can extract the protection information regarding this path and pass it to the traffic engineering (TE) manager. It is up to the TE manager to match all the diverse paths belonging to the same protection group.

6. Security Considerations

The extensions specified here do not raise any security issues that are not already present in the RSVP-TE architecture.

7. References

[ANSI-T1.105] "Synchronous Optical Network (SONET): Basic Description Including Multiplex Structure, Rates, and Formats," ANSI T1.105, 2000.

[RSVP-TE] Awduche, D, et al, "RSVP-TE: Extensions to RSVP for LSP Tunnels", Internet Draft, Work in Progress, draft-ietf-mpls-revp-lsp-tunnel-08.txt, May 2001.

[GMPLS-ARCH] E. Mannie et al., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", Internet Draft, Work in progress, draft-many-gmpls-architecture-00.txt, February 2001.

[GMPLS-SONET/SDH] E. Mannie Editor, "GMPLS Extensions for SONET and SDH Control," Internet Draft, draft-ietf-ccamp-gmpls-sonet-sdh-01.txt, June 2001.

[GMPLS-RSVP] P. Ashwood-Smith et al., "Generalized MPLS Signaling - RSVP-TE Extensions", Internet Draft, Work in progress, draft-ietf-mpls-generalized-rsvp-te-03.txt, May 2001.

[BMS] G. Bernstein et al, "Framework for MPLS-based Control of Optical SDH/SONET Networks", Internet Draft, draft-bms-optical-sdhsonet-mpls-control-frmwrk-00.txt, November 2000

[RECOV] V. Sharma, et al, "Framework for MPLS-based Recovery," Internet Draft, draft-ietf-mpls-recovery-frmwrk-02.txt, March 2001.

[SRLG] D. Papadimitriou, et al, "Inference of Shared Risk LInk Groups," Internet Draft, draft-many-inference-srlg-00.txt, Aug 2001.

8. Author's Addresses

Dan Guo, Jibin Zhan, N. Ravindran, P. Siva, Wenjing Chu, R. Cooper
Turin Networks, Inc.
1415 N. McDowell Blvd, Petaluma, CA 95454
Phone: +1 707-665-4357
Email: {dguo,jzhan,nravindran, psiva,wchu,rcooper}@turinnetworks.com

Raymond Cheung, James Fu
Sorrento Networks, Inc.
9990 Mesa Rim Road,
San Diego, CA 92121
Email: {rcheung,jfu}@sorrentonet.com

9. Full Copyright Notice