1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

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

2. Abstract

This document discusses the shared mesh protection concept. Its aim is to provide fast, guaranteed recovery of service at significantly less cost of protection capacity compared to other schemes. In companion documents [1,2], extensions to RSVP-TE and OSPF-TE protocols are proposed that enable shared mesh protection. Those extensions, together with this document, first address global repair with path-based protection switching, as opposed to local repair of LSP failures and reroute. However, the concept can be extended straightforwardly to the local repair techniques being considered in the MPLS working group.

3. Purpose of This Document

The purpose of this document is to introduce and discuss the concept of path-based shared mesh protection. The document discusses this specific protection switching recovery scheme with shared-resource in terms of recovery path resource usage as outlined in the MPLS WG
draft on the framework for MPLS-based recovery [3]. It provides input to the MPLS Working Group for making recommendations to respective working groups for protocol extensions in supporting shared mesh protection [1],[2].

4. Introduction

In [3], the framework for MPLS-based recovery was presented, including outlines of principles, methods, and comparison criteria for evaluating different recovery schemes. Some form of protection bandwidth sharing and signaling support have been previously discussed in [4],[5].

In this document, the shared mesh protection concept is discussed which is applicable to the global repair topologically and to the 1-to-1, n-to-1 and n-to-m protections from path mapping perspective discussed in [3].

To guarantee the recovery and to maintain the performance of the service, sufficient resource needs to be available at the setup time of the protection LSPs. However it may or may not require reservation for additional protection bandwidth.

Indeed the key observation is that the need for reservation of protection bandwidth depends on whether there is already sufficient protection capacity set aside to protect other connections which do not belong to the same shared risk groups (SRGs) with the new primary connection. Thus the shared mesh protection scheme can significantly reduce the required network protection capacity.

Once a failure of a primary path (in the path-based case), is identified, the protection LSP for the affected working LSP is activated with just enough reserved protection bandwidth to guarantee failure recovery. Speed of recovery is supported by using fast failure notification schemes (which are beyond the scope of this document).

5. Shared Mesh Protection

Path-based protection schemes such as 1-to-1 or n-to-1 consider the protection of service traffic between two particular nodes. To provide protection of a working connection, guaranteed recovery with similar grade of service and sufficient amount of bandwidth must be set aside in the network. This can be achieved by computing and reserving required protection capacity at the same time that computation and activation of the working connection is performed. For path-based schemes, arrival of a request to establish shared mesh protection service between two nodes can prompt computation of a pair...
of disjoint connections between them. The primary and protection connections would be set up, meeting the following two necessary requirements. First, sufficient bandwidth should be available along the route of the working connection to accommodate the requested load. Second, either of the following two conditions must hold: either whatever bandwidth for protection had previously been reserved along the protection path is already sufficient to guarantee recovery from any single link or node failure along the new working path, or there must be enough available bandwidth along the protection path to accommodate the additional reservation.

From the point of view of the network, the degree to which the additional bandwidth for protection should be shared in this manner depends on the failure coverage objective for the particular LSP: whether the objective for the LSP is protection against failure of any single node, of any single link, or of an SRG.

6. Need for RSVP-TE Extensions

The computation of the protection path can be done in several ways depending on the available information. The simplest way is to calculate a disjoint path using the same link weights as the ones used for calculation of the primary path. In this case each router along the protection path needs to know about the primary path for which it is requested to protect. Further, knowing the primary path along each node of the protection path allows the admission controller of that node to determine, using locally maintained sharing information, the exact amount of bandwidth required and that which can be shared. Outgoing interface ID’s are required to be communicated in addition to the router ID’s. Details regarding the proposed RSVP-TE extensions to support sharing of protection resources can be found in [1] which addresses the requirements brought forth first in [5].

7. Need for OSPF-TE Extensions

While some sharing of protection bandwidth may be realized with the proposed extensions of RSVP-TE [1], the amount of bandwidth reserved for restoration is "best effort" and usually not minimized since the sharing potential on each of the links is not known before the protection path choice is made at the source router. Additional protection resource and sharing information of the network would be required for the source router to compute more intelligently the desired protection path which was first discussed in [5]. The proposed extensions to OSPF-TE [2] addresses this need and allow the source router compute the primary and protection path combination that utilizes the network resources efficiently with minimum signaling/crankback load.
8.0. References


9. Author Information

Akber Qureshi  
Lucent Technologies  
101 Crawfords Corner Rd.  
Holmdel, NJ 07733  
e-mail: mqureshi@lucent.com  
phone: +1 732 949 4791

Ramesh Nagarajan  
Lucent Technologies  
101 Crawfords Corner Rd.  
Holmdel, NJ 07733  
e-mail: rameshn@lucent.com  
phone: +1 732 949 2761

Y.T. Wang  
Lucent Technologies  
101 Crawfords Corner Rd.  
Holmdel, NJ 07733  
e-mail: ytwang@lucent.com  
phone: +1 732 949 0676

Sandy Goldfless  
Lucent Technologies  
1 Robbins Rd.  
Westford, MA 10886

shared-mesh-protection-Goldfless October 2002