Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: December 03, 2013

B. Wright, Ed.
J. Hardwick
Metaswitch Networks
V. Shukla
Verizon
J. Li
China Telecom Beijing Research Institute

June 2013

# Requirements for operator policy in GMPLS networks consisting of protected links
## draft-wright-ccamp-op-policy-prot-links-00

Abstract

This document describes policy options required by network operators in networks including APS links or links with an inherent protection capability. It also identifies gaps in the current GMPLS standards which may prevent these policy options from being implemented.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 03, 2013.

Table of Contents



## 1. Introduction

As described in [RFC4202], GMPLS networks frequently contain links which have an inherent protection capability, for example SONET APS links or abstract links which represent a bundle of lower layer LSPs. An operator may wish to configure different policies which, in the event of a failure that causes a change in the available protection capability of a link, affect both path computation and provisioned services. This draft describes some of these policy behaviors, and identifies where these behaviours cannot be implemented using existing GMPLS standards.

### 1.1. Requirements Language

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].

## 2. Protected Links

A link can be said to have an inherent protection capability if, in the event of a data plane failure affecting some part of the link, the link can continue to carry data. We call links which have an inherent protection capability "Protected Links". Figure 1 below shows an example of a Protected Link.

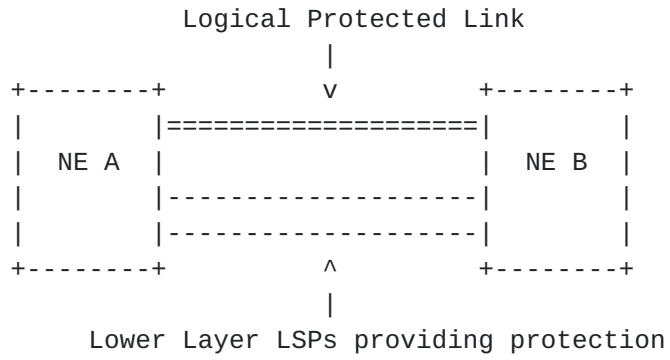


Figure 1: Diagram showing an example of a protected link

In this example, a bundle of LSPs transport data between the two network elements, as described in [RFC4201]. These LSPs are advertised as a single link into the client layer IGP. A protection scheme (such as 1+1, as described in [RFC4427]) can be configured for the link bundle to ensure that if one link in the bundle fails, traffic will be unaffected because other links in the bundle carry the data. Hence the link in the client layer has its own protection capabilities, which it can advertise as per [RFC4202]. However, failures of lower-layer LSPs can mean that, whilst the overall link bundle is still able to carry traffic, the protection capabilities that are still configured, are no longer present. Such links are referred to as "Protection Impaired".

## 3. Operator requirements

Operators have the following requirements which SHOULD be met in networks containing Protection Impaired links.

R1. It SHOULD be possible to include or exclude a Protection Impaired link from a path computed for an LSP, depending on the type of service that will use the LSP. For example, an operator's policy may allow LSPs corresponding to high priority unprotected services to be provisioned over the Protection-Impaired Link, but prevent lower priority LSPs from using it (because once the failure has been repaired, bandwidth on a high-value protected link would be used for low-priority LSPs).

R2. Depending on the service-level of a given LSP, it SHOULD be possible to configure a policy to reroute an existing LSP when a link it traverses becomes Protection Impaired (for example, if there are other links available which still have currently active protection capabilities). If the fault is repaired, then it SHOULD be possible to automatically revert the LSP to the original path.

### 3.1. Operational considerations

It is often advantageous to centralize policy configuration on as few network elements as possible. This makes network-wide policy changes easier to implement for operators. For example, in networks where Path Computation is performed by only a subset of the network elements (e.g. PCEs), it is preferable that the policy configuration relating to Path Computation is applied solely to those network elements.

## 4. Gap Analysis

An analysis of the current GMPLS protocols against the above requirements is as follows.

R1. As per [RFC4202], the current link protection type can be advertised by the OSPF-TE or ISIS-TE protocols so elements performing Path Computation can understand the currently available protection type. Per-Network Element level policy can determine the how the protection type is set when the link is advertised. However, there is no way currently to advertise both the configured link protection type and the current link protection type. Therefore, it is not possible to implement the Path Computation behavior described above if a different policy is required for different LSPs.

R2. A node which detects a failure MAY use the procedures defined in [RFC5712] to inform the head-end LSR. The head-end LSR MAY then elect to use this as a trigger to perform Path Computation to determine whether an alternative route exists and possibly re-route the LSP. However, there is no similar mechanism to inform the head-end LSR when a failure has been cleared.

## 5. Contributors

## 6. IANA Considerations

This memo includes no request to IANA.

## 7. Security Considerations

TBD

## 8. References

### 8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4201] Kompella, K., Rekhter, Y., and L. Berger, "Link Bundling in MPLS Traffic Engineering (TE)", RFC 4201, October 2005.

[RFC4202] Kompella, K. and Y. Rekhter, "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4202, October 2005.

[RFC4427] Mannie, E. and D. Papadimitriou, "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4427, March 2006.

[RFC5712] Meyer, M. and JP. Vasseur, "MPLS Traffic Engineering Soft Preemption", RFC 5712, January 2010.

## 8.2. Informative References

[G.808.1] ITU-T, "Generic Protection Switching - Linear trail and subnetwork protection", Recommendation G.808.1, December 2003.

[I-D.narten-iana-considerations-rfc2434bis] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", draft-narten-iana-considerations-rfc2434bis-09 (work in progress), March 2008.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

Authors' Addresses

Ben Wright (editor)
Metaswitch Networks
100 Church Street
Enfield, Middlesex
UK

Phone: +44 2083661177
Email: ben.wright@metaswitch.com

Jon Hardwick
Metaswitch Networks
100 Church Street
Enfield, Middlesex
UK

Phone: +44 2083661177
Email: jon.hardwick@metaswitch.com

Vishnu Shukla
Verizon
60 Sylvan Road
Waltham, MA 02451
USA

Email: vishnu.shukla@verizon.com

Junjie Li
China Telecom Beijing Research Institute
118 Xizhimenneidajie
Xicheng, Beijing
China

Email: lijj@ctbri.com.cn