Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2015

Z. Cui
R. Winter
NEC
H. Shah
Ciena
S. Aldrin
Huawei Technologies
M. Daikoku
KDDI

October 27, 2014

Use Cases and Requirements for MPLS-TP multi-failure protection
draft-cui-mpls-tp-mfp-use-case-and-requirements-03

Abstract

The basic survivability technique has been defined in Multiprotocol Label Switching Transport Profile (MPLS-TP) network [RFC6378]. That protocol however is limited to 1+1 and 1:1 protection, not designed to handle multi-failure protection.

This document introduces some use cases and requirements for multi-failure protection functionality.

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 April 30, 2015.

Table of Contents

1. Introduction

Today's packet optical transport networks are able to concentrate large volumes of traffic onto a relatively small number of nodes and links. As a result, the failure of a single network element can potentially interrupt a large amount of traffic. For this reason, ensuring survivability through network design is an important network design objective.

The basic survivability technique has been defined in MPLS-TP network [RFC6378]. That protocol however is limited to 1+1 and 1:1 protection, not designed to handle multi-failure protection.

The multi-failure protection is required for disaster recovery, e.g., even during natural disasters and other catastrophic events such as earthquake or tsunami, the network availability must be provided especially for high-priority services such as emergency telephone calls. Existing 1+1 or 1:n protection however is limited to cover single failure and no sufficient to maintain disaster recovery.

The multi-failure protection is also required for hazardous contion, e.g., when a working path or protection path was closed by network operator for construction work, the network service will become a hazardous condition. During this condition time, if another failure (e.g. a human-error or network entities failure) is occurred on the protection path, than the operator can't meet service level agreements (SLA). Thus, the multi-failure condition could put pressure on network operations.

On the other hand, many network operators have a very limited budget for improving network survivability. This requires a design approach, which takes budget limitations into consideration.

To increase the service availability and to reduce the backup network costs, we propose extend the 1+1 and 1:1 protection protocol to support the m:1 and m:n architecture type.

1.1. Document scope

This document describes the use cases and requirements for multi-failure protection in MPLS-TP networks without the use of control plane protocols. Existing solutions based on control plane such as GMPLS may be able to restore user traffic when multiple failures occur. Some networks however do not use full control plane operation for reasons such as service provider preferences, certain limitations or the requirement for fast service restoration (faster than achievable with control plane mechanisms). These networks are the focus of this document which defines a set of requirements for multi-failure protection not based on control plane support.

1.2. Requirements notation

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 [RFC2119].

2. m:n protection architecture

The following Figure 1 shows a protection domain with n working paths and m protection paths between ingress node LER-A and egress node LER-Z.

At the ingress node LER-A, the normal traffic is either permanently connected to its working path and may be connected to one of the protection paths (case of broadcast bridge), or is connected to either its working path or one of the protection paths (case of selector bridge). At the egress node LER-Z, the normal traffic is selected from either its working or one of the protection paths.

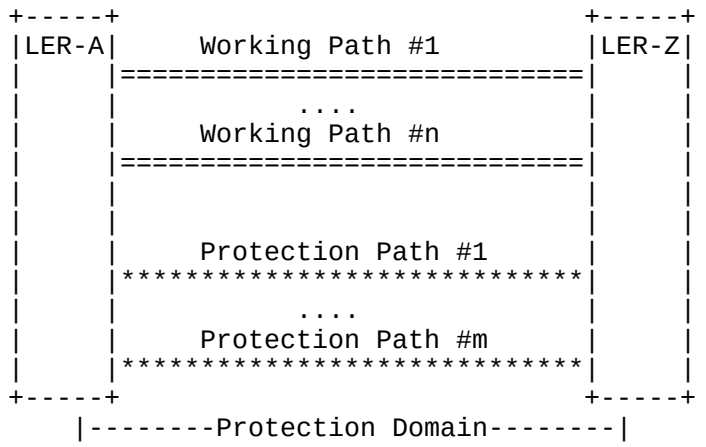

Figure 1: m:n protection domain

3. Use cases

3.1. m:1 (m > 1) protection

In the MPLS-TP linear protection such as 1+1/1:1 MPLS-TP protection, when a single failure is detected on the working path, the normal traffic can be restored to a protection path. The normal traffic however into a unprotected condition until the working path is completely repaired, that could put pressure on network operations.

The m:1 protection can increase service availability and reduce operator’s pressure, because it take multiple protection paths to ensuring high-priority services continue to operate on the 2nd, 3rd or N th alternate backup, at least one of m protection paths is an available.

The 2nd, 3rd or N th alternate backup paths may be provided in following cases.

3.1.1. pre-configuration

Before failure detection and/or notification, the protection relationship between the working and two or more protection paths SHOULD be configured and the protection path MUST be identified prior to use of the protection paths.

The unprotected extra traffic can be transported over the M protection path whenever the protection paths are not used to carry a normal traffic.

3.1.2. on-demand configuration

The protection relationship between a working path and a protection path are configured in the normal condition.

Other protection path such as 2nd, 3rd or N th alternate backup path is configured by either a control protocol or static configuration by the management system, only after failure detection and/or notification of either the working path or the protection path.

However, even when the configuration is performed by a control protocol, e.g. Generalized MPLS (GMPLS), the control protocol SHALL NOT be used as the primary mechanism for detecting or reporting network failures, or for initiating or coordinating protection switch-over. That is, it SHALL NOT be used as the primary resilience mechanism.

3.1.3. on-demand activation

Before failure detection and/or notification, two or more protection paths are instantiated between the same ingress-egress node pair as the working path, but note that the resources of m (m > 1) protection path may not be allocated.

The resource allocation on the m th protection path occurs only after failure detection and/or notification of either the working path or the protection path.

Therefore, this mechanism can against multiple failures but requires activation of the resource of m th protection path at ingress node and egress node after failure occurrence. After activated the m th protection path, the ingress node and egress node can carry the normal traffic.

3.2. m:n (m, n > 1) protection

In order to reduce backup costs, in the m:n architecture type, m dedicated protection transport paths are sharing backup resources for n working transport paths.

The bandwidth of each protection path should be allocated in such a way that it may be possible to protect any of the n working paths in case at least one of the m protection paths is available. When a working path is determined to be impaired, its normal user traffic signal first must be assigned to an available protection transport path followed by transition from the working to the assigned protection path at both the ingress node and egress node of the

protected domain. It is noted that when more than m working paths are impaired, only m working paths can be protected

On the other hand, the normal traffic is either permanently connected to its working path and may be connected to one of the protection paths. It is noted that when at least one of the m protection paths is available, than the working path can be protected.

4. Requirements

Some recovery requirements are defined [RFC5654]. That however is limited to cover single failure and is not able to care that the multiple failures. This Section 4 extends the requirements to support the multiple failures scenarios.

MPLS-TP MUST support m:1 protection with the following requirements:

R1 The m:1 protection MUST protects against multiple failures that are detected on both of working path and protection path.

R2 The backup paths pre-configuration SHOULD be supported.

R3 On-demand backup paths configuration MAY be supported.

R4 On-demand backup resource activation MAY be supported.

R5 Some priority schemes MUST be provided, because a protection path has to choose between two or more backup resources.

MPLS-TP MUST support m:n protection with the following requirements:

R6 The m:n protection MUST protects against multiple failures that are simultaneously-detected on both of working path and protection path or more than one multiple working paths.

R7 Some priority schemes MUST be provided, because the backup resources are shared by multiple working paths dynamically.

5. Security Considerations

TBD

6. IANA Considerations

TBD

7. Normative References

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

[RFC5654] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[RFC6378] Weingarten, Y., Bryant, S., Osborne, E., Sprecher, N., and A. Fulignoli, "MPLS Transport Profile (MPLS-TP) Linear Protection", RFC 6378, October 2011.

Authors' Addresses

Zhenlong Cui
NEC

Email: c-sai@bx.jp.nec.com

Rolf Winter
NEC

Email: Rolf.Winter@neclab.eu

Himanshu Shah
Ciena

Email: hshah@ciena.com

Sam Aldrin
Huawei Technologies

Email: aldrin.ietf@gmail.com

Masahiro Daikoku
KDDI

Email: ms-daikoku@kddi.com