Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 5, 2015

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

July 4, 2014

Use Cases and Requirements for MPLS-TP multi-failure protection
draft-cui-mpls-tp-mfp-use-case-and-requirements-02

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.

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 fault-tolerant 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 case of multi-failure condition is very rare, but not unheard of. For example, when a working path was closed by network operator for construction work, the network service will become a hazardous condition. During this 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).

A network must be able to handle multiple failures even that are a rare case, because especially some high-priority services such as emergency telephone calls request to network service provider

guarantee their service connections in a timely manner in any situation.

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: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. when a working path is determined to impaired, its normal traffic must be assigned to a protection path if a protection path is available. To reduce the backup network costs, m protection paths are sharing backup resource for n working paths, where m <= n typically. The bandwidth of each protection paths should be allocated enough to protect any of the n working paths.

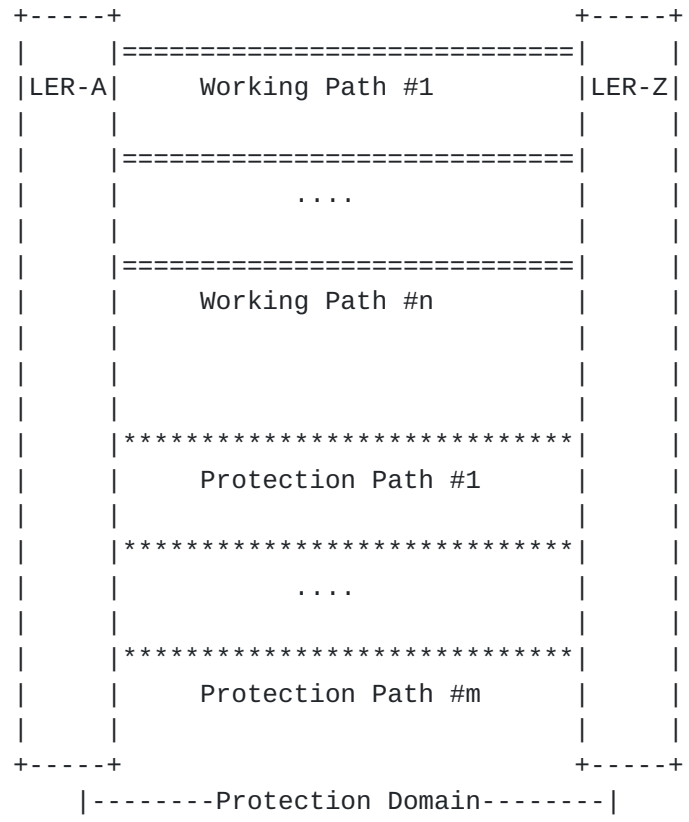

Figure 1: m:n ptorection domain

3. Use cases

3.1. Increase service availability

With technological advancement of mobile services or data center services, dependencies and business impact of network services have been increased phenomenally. End-users expectations of service availability also are increasing, which is driving service providers enhance their network's availability.

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

The m:n protection can increase service availability because it take multiple protection paths to ensuring high-priority services continue to operate on the 2nd, 3rd or Nth alternate backup, at least one of m protection paths is a available.

3.2. Reduce the backup costs

Network costs driven by high traffic growth rates are rising steadily, but revenues are no increased in direct proportion to traffic growth rates. This requires a design approach, which takes budget limitations into consideration.

Existing protection schemes such as 1+1 protection meet the sub 50 ms performance requirement but only protect against a single failure and are too costly.

The m:n protection is a useful solution, that can reduce the backup costs because m dedicated protection paths are sharing backup paths for n working paths, where m =< n typically.

The shared Mesh Protection (SMP) also can reduce the backup costs as described in [I-D.ietf-mpls-smp-requirements]. SMP however is based the 1:1 protection and does not able to care that the multiple failures are occurred on both working and protection paths. However, combine use of SMP and a set of m:1 protections to make a m:n protection likely, may be better able to recovers the multiple failures.

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:n protection with the following requirements:

R1 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.

R2 Some priority schemes MUST be provided, because the backup resources are shared by multiple working paths dynamically.

R3 TBD

5. Security Considerations

TBD

6. IANA Considerations

TBD

7. Normative References

[I-D.ietf-mpls-smp-requirements]
Weingarten, Y., Aldrin, S., Pan, P., Ryoo, J., and G. Mirsky, "Requirements for MPLS-TP Shared Mesh Protection", draft-ietf-mpls-smp-requirements-06 (work in progress), June 2014.

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

[RFC3945] Mannie, E., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, October 2004.

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

[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