Network Working Group
Internet Draft
Category: Informational
Expires: April 24, 2007

Kenji Kumaki, Ed
KDDI Corporation
Tomohiro Otani
KDDI R&D Labs
Shuichi Okamoto
NICT
Kazuhiro Fujihara
Yuichi Ikejiri
NTT
Communications
October 23, 2006

Interworking Requirements to Support operation of MPLS-TE over GMPLS networks

draft-kumaki-ccamp-mpls-gmpls-interwork-reqts-02.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a framework and Service Provider requirements for operating Multiprotocol Label Switching (MPLS) traffic engineering (TE) networks over Generalized MPLS (GMPLS) networks.

Operation of an MPLS-TE network as a client network to a GMPLS network has enhanced operational capabilities than provided by a co-existent protocol model (ships in the night).

The GMPLS network may be a packet or a non-packet network, and may itself be a multi-layer network supporting both packet and non-packet technologies. A MPLS-TE Label Switched Path (LSP) originates and terminates on an MPLS Label Switching Router (LSR). The GMPLS network provides transparent transport for the end-to-end MPLS-TE LSP.

Specification of solutions is out of scope for this document.

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.

Table of Contents

1. Introduction

Multiprotocol Label Switching traffic engineering (MPLS-TE) networks are often deployed over transport networks such that the transport networks provide connectivity between the Label Switching Routers (LSRs) in the MPLS-TE network. Increasingly, these transport networks are operated using a Generalized Multiprotocol Label Switching (GMPLS) control plane and label Switched Paths (LSPs) in the GMPLS network provide connectivity in the MPLS-TE network.

Generalized Multiprotocol Label Switching (GMPLS) protocols were developed as extensions to Multiprotocol Label Switching traffic engineering (MPLS-TE) protocols. MPLS-TE is limited to the control of packet switching networks, but GMPLS can also control sub-packet technologies at layers one and two.

The GMPLS network may be managed by an operator as a separate network (as it was when it was under management plane control before the use of GMPLS as a control plane), but optimizations of management and operation may be achieved by coordinating the use of the MPLS-TE and GMPLS networks and operating the two networks with a close client/server relationship.

GMPLS LSP setup may triggered by the signaling of MPLS-TE LSPs in the MPLS-TE network so that the GMPLS network is reactive to the needs of the MPLS-TE network. The triggering process can be under the control of operator policies without needing direct intervention by an operator.

The client/server configuration just described can also apply in migration scenarios for MPLS-TE packet switching networks that are being migrated to be under GMPLS control. [MIGRATE] describes a migration scenario called the Island Model. In this scenario, groups of nodes (islands) are migrated from the MPLS-TE protocols to the GMPLS protocols and operate entirely surrounded by MPLS-TE nodes (the sea). This scenario can be effectively managed as a client/server network relationship using the framework described in this document.

In order to correctly manage the dynamic interaction between the MPLS and GMPLS networks, it is necessary to understand the operational requirements and the control that the operator can impose. Although this problem is very similar to the multi-layer networks described in [MLN], it must be noted that those networks operate GMPLS protocols

in both the client and server networks which facilitates smoother interworking. Where the client network uses MPLS-TE protocols over the GMPLS server network there is a need to study the interworking of the two protocol sets.

This document examines the protocol requirements for protocol interworking to operate an MPLS-TE network as a client network over a GMPLS server network, and provides a framework for such operations.

2. Reference model

The reference model used in this document is shown in Figure 1. It can easily be seen that the interworking between MPLS-TE and GMPLS protocols must occur on a node and not on a link. Nodes on the interface between the MPLS-TE and GMPLS networks must be responsible for handling both protocol sets and for providing any protocol interworking that is required. We call these nodes Border Routers.

```
       --------------    -------------------------    --------------
      | MPLS Client  |  |   GMPLS Server Network  |  |  MPLS Client |
      |   Network    |  |                         |  |    Network   |
      |              |  |                         |  |              |
      |     ----   --+--+--    -----   -----    --+--+--   ----     |
      |    |    | |        |  |     | |     |  |        | |    |    |
      |    |MPLS|_| Border |__|GMPLS|_|GMPLS|__| Border |_|MPLS|    |
      |    |LSR | | Router |  | LSR | | LSR |  | Router | |LSR |    |
      |    |    | |        |  |     | |     |  |        | |    |    |
      |     ----   --+--+--    -----   -----    --+--+--   ----     |
      |              |  |                         |  |              |
      |              |  |                         |  |              |
       --------------    -------------------------    --------------

             |         |         GMPLS LSP        |         |
             |         |<------------------------>|         |
             |                                              |
             |<-------------------------------------------->|
                           End-to-End MPLS-TE LSP
```

Figure 1. Reference model of MPLS-TE/GMPLS interworking

MPLS-TE network connectivity is provided through a GMPLS LSP which is created between Border Routers. End-to-end connectivity between MPLS LSRs in the client MPLS-TE networks is provided by an MPLS-TE LSP that is carried across the MPLS-TE network by the GMPLS LSP using hierarchical LSP techniques [RFC4206], LSP stitching segments [STITCH] or a contiguous LSP. LSP stitching segments and contiguous

LSPs are only available where the GMPLS network is a packet switching network.

3. Detailed Requirements

This section describes detailed requirements for MPLS-TE/GMPLS interworking in support of the reference model shown in figure 1.

3.1 End-to-End Signaling

The solution MUST be able to preserve MPLS signaling information signaled within the MPLS-TE client network at the start of the MPLS-TE LSP, and deliver it on the other side of the GMPLS server network for use within the MPLS-TE client network at the end of the MPLS-TE LSP. This may require protocol mapping (and re-mapping), protocol tunneling, or the use of remote protocol adjacencies.

3.2 Triggered Establishment of GMPLS LSPs

The solution MUST provide the ability to establish end-to-end MPLS-TE LSPs over a GMPLS server network. It SHOULD be possible for GMPLS LSPs across the core network to be set up between Border Routers triggered by the signaling of MPLS-TE LSPs in the client network. GMPLS LSPs MAY also be pre-established as the result of management plane control.

3.3 Diverse Paths for End-to-End MPLS-TE LSPs

The solution SHOULD provide the ability to establish end-to-end MPLS-TE LSPs having diverse paths for protection of the LSP traffic. This means that MPLS-TE LSPs SHOULD be kept diverse both within the client MPLS-TE network and as they cross the server GMPLS network. This means that there SHOULD be a mechanism to request the provision of diverse GMPLS LSPs between a pair of Border Routers to provide protection of the GMPLS span, but also that there SHOULD be a way to keep GMPLS LSPs between different Border Routers disjoint.

3.4 Advertisement of MPLS-TE Information via the GMPLS Network

The solution SHOULD provide the ability to advertise of TE information from MPLS-TE client networks across the GMPLS server network.

The advertisement of TE information from within an MPLS-TE client network to all LSRs in the client network enables a head end LSR to compute an optimal path for an LSP to a tail end LSR that is reached over the GMPLS server network.

Where there is more than one client MPLS-TE network, the TE information from separate MPLS-TE networks MUST be kept private, confidential and secure.

3.5 Selective Advertisement of MPLS-TE Information via a Border Node

The solution SHOULD provide the ability to distribute TE reachability information from the GMPLS server network to MPLS-TE networks selectively. This information is useful for the LSRs in the MPLS-TE networks to compute paths that cross the GMPLS server network and to select the correct Border Routers to provide connectivity.

The solution MUST NOT distribute TE information from within a non-PSC GMPLS server network to any client MPLS-TE network as that information may cause confusion and selection of inappropriate paths.

3.6 Interworking of MPLS-TE and GMPLS protection

If an MPLS-TE LSPs is protected using MPLS Fast Reroute (FRR) [RFC4090], then similar PROTECTION MUST be provided over the GMPLS island. Operator and policy controls SHOULD be made available at the Border Router to determine how suitable protection is provided in the GMPLS island.

3.7 Independent Failure Recovery and Reoptimization

The solution SHOULD provide failure recovery and reoptimization in the GMPLS server network without impacting MPLS-TE client network and vice versa. That is, it SHOULD be possible to recover from a fault within the GMPLS island or to reoptimize the path across the GMPLS island without requiring signaling activity within the MPLS-TE client network. Similarly, it SHOULD be possible to perform recovery or reoptimization within the MPLS-TE client network without requiring signaling activity within the GMPLS server networks.

In case that failure in the GMPLS server network can not be repaired transparently, some kind of notification of the failure SHOULD be transmitted to MPLS-TE network.

3.8 Complexity and Risks

The solution SHOULD NOT introduce unnecessary complexity to the current operating network to such a degree that it would affect the stability and diminish the benefits of deploying such a solution in service provider networks.

3.9 Scalability consideration

The solution MUST scale well with consideration to at least the following considerations.

- The number of GMPLS-capable nodes (i.e., the size of the GMPLS server network).

- The number of MPLS-TE-capable nodes (i.e., the size of the MPLS-TE client network).
- The number of MPLS-TE client networks.
- The number of GMPLS LSPs.
- The number of MPLS-TE LSPs.

3.10 Performance Consideration

The solution SHOULD be evaluated with regard to the following criteria.

- Failure and restoration time.
- Impact and scalability of the control plane due to added overheads.
- Impact and scalability of the data/forwarding plane due to added overheads.

3.11 Management Considerations

Manageability of deployment of an MPLS-TE client network over GMPLS server network MUST addresses the following considerations.

- Need for coordination of MIB modules used for control plane management and monitoring in the client and server networks.
- Need for diagnostic tools that can discover and isolate faults across the border between the MPLS-TE client and GMPLS server networks.

4. Security Considerations

We will write security considerations in next version.

5. Recommended Solution Architecture

The recommended solution architecture to meet the requirements set out in the previous sections is known as the Border Peer Model. This architecture is a variant of the Augmented Model described in [RFC3945]. The remainder of this document presents an overview of this architecture. Details of protocol solutions are described in [BORDER-PEER].

In the Augmented Model, routing information from the lower layer (server) network is filtered at the interface to the higher layer (client) network and is distributed within the higher layer network. In the Border Peer Model, the interface between the client and server networks is the Border Router. This router has visibility of the routing information in the server network yet also participates as a peer in the client network. However, the Border Router does not distribute server routing information into the client network.

The Border Peer Model may also be contrasted with the Overlay Model [RFC3945]. In this model there is a protocol request/response interface (the user network interface - UNI) between the client and server networks. [RFC4208] shows how this interface may be supported by GMPLS protocols operated between client edge and server edge routers while retaining the routing information within the server network. The Border Peer Model can be viewed as placing the UNI within the Border Router thus giving the Border Router peer capabilities in both the client and server network.

5.1 Use of Contiguous, Hierarchical, and Stitched LSPs

All three LSP types MAY be supported in the Border Peer Model, but contiguous LSPs are the hardest to support because they require protocol mapping between the MPLS-TE client network and the GMPLS server network. Such protocol mapping can currently be achieved since MPLS-TE signaling protocols are a subset of GMPLS, but this mechanism is not future-proofed.

Contiguous and stitched LSPs can only be supported where the GMPLS server network has the same switching type (that is, packet switching) as the MPLS-TE network. Requirements for independent failure recovery within the GMPLS island require the use of loose path reoptimization techniques [LOOSE-REOPT] and end-to-end make-before-break [RFC3209] which will not provide rapid recovery.

For these reasons, the use of hierarchical LSPs across the server network is RECOMMENDED for the Border Peer Model, but see the discussion of Fast Reroute protection in section 5.3.

5.2 MPLS-TE Control Plane Connectivity

Control plane connectivity between MPLS-TE LSRs connected by a GMPLS island in the Border Peer Model MAY be provided by the control channels of the GMPLS network. If this is done, a tunneling mechanism (such as GRE [RFC2784]) SHOULD be used to ensure that MPLS-TE information is not consumed by the GMPLS LSRs. But care is required to avoid swamping the control plane of the GMPLS network with MPLS-TE control plane (particularly routing) messages.

In order to ensure scalability, control plane messages for the MPLS-TE client network MAY be carried between Border Routers in a single hop MPLS-TE LSP routed through the data plane of the GMPLS server network.

5.3 Fast Reroute Protection

If the GMPLS network is packet switching, Fast Reroute protection can be offered on all hops of a contiguous LSP. If the GMPLS network is packet switching then all hops of a hierarchical GMPLS LSP or GMPLS stitching segment can be protected using Fast Reroute. If the end-to-end MPLS-TE LSP requests Fast Reroute protection, the GMPLS packet switching network SHOULD provide such protection.

However, note that it is not possible to provide FRR node protection of the upstream Border Router without careful consideration of available paths, and protection of the downstream Border Router is not possible where hierarchical LSPs or stitching segments are used.

Note further that Fast Reroute is not available in non-packet technologies. However, other protection techniques are supported by GMPLS for non-packet networks and are likely to provide similar levels of protection.

The limitations of FRR need careful consideration by the operator and may lead to the decision to provide end-to-end protection for the MPLS-TE LSP.

6. IANA Considerations

This requirement document makes no requests for IANA action.

7. Normative References

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

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V. and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

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

[RFC4090] Pan, P., Swallow, G. and A. Atlas, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, May 2005.

[RFC4206] Kompella, K., and Rekhter, Y., "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", RFC 4206, October 2005.

[RFC4208] Swallow, G., et al., "Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", RFC 4208, October 2005.

[STITCH] Ayyangar, A., Vasseur, JP. "Label Switched Path Stitching with Generalized MPLS Traffic Engineering", draft-ietf-ccamp-lsp-stitching, work in progress.

8. Informative References

[RFC2784] Farinacci, D., et al., "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[BORDER-PEER] Kumaki, K. et al. "Operational, Deployment and Interworking Considerations for GMPLS", draft-kumaki-ccamp-mpls-gmpls-interworking, work in progress.

[LOOSE-REOPT] Vasseur, JP., Ikejiri, Y., and Zhang, R., "Reoptimization of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) loosely routed Label Switch Path (LSP)", draft-ietf-ccamp-loose-path-reopt, work in progress.

[MIGRATE] Shiomoto, K., et al., "Framework for MPLS-TE to GMPLS migration", draft-ietf-ccamp-mpls-gmpls-interwork-fmwk, work in progress.

[MLN] Shiomoto, K., Papadimitriou, D., Le Roux, J.L., Vigoureux, M., Brungard, D., "Requirements for GMPLS-based multi-region and multi-layer networks (MRN/MLN)", draft-ietf-ccamp-gmpls-mln-reqs, work in progress.

9. Acknowledgments

The author would like to express the thanks to Raymond Zhang, Adrian Farrel, and Deborah Brungard for their helpful and useful comments and feedback.

10.Author's Addresses

Kenji Kumaki (Editor)
KDDI Corporation
Garden Air Tower
Iidabashi, Chiyoda-ku,
Tokyo 102-8460, JAPAN
Email: ke-kumaki@kddi.com

Tomohiro Otani
KDDI R&D Laboratories, Inc.
2-1-15 Ohara Kamifukuoka   Phone: +81-49-278-7357
Saitama, 356-8502. Japan   Email: otani@kddilabs.jp

Shuichi Okamoto

NICT JGN II Tsukuba Reserach Center
1-8-1, Otemachi Chiyoda-ku,   Phone : +81-3-5200-2117
Tokyo, 100-0004, Japan   E-mail :okamoto-s@nict.go.jp

Kazuhiro Fujihara
NTT Communications Corporation
Tokyo Opera City Tower 3-20-2 Nishi Shinjuku, Shinjuku-ku
Tokyo 163-1421, Japan
EMail: kazuhiro.fujihara@ntt.com

Yuichi Ikejiri
NTT Communications Corporation
Tokyo Opera City Tower 3-20-2 Nishi Shinjuku, Shinjuku-ku
Tokyo 163-1421, Japan
EMail: y.ikejiri@ntt.com

11.Intellectual Property Statement

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.