Internet Engineering Task Force (IETF)
Request for Comments: 9730
Category: Informational
ISSN: 2070-1721

H. Zheng
Y. Lin
Huawei Technologies
Y. Zhao
China Mobile
Y. Xu
CAICT
D. Beller
Nokia

March 2025

Interworking of GMPLS Control and Centralized Controller Systems

Abstract

Generalized Multiprotocol Label Switching (GMPLS) control allows each network element (NE) to perform local resource discovery, routing, and signaling in a distributed manner.

The advancement of software-defined transport networking technology enables a group of NEs to be managed through centralized controller hierarchies. This helps to tackle challenges arising from multiple domains, vendors, and technologies. An example of such a centralized architecture is the Abstraction and Control of Traffic-Engineered Networks (ACTN) controller hierarchy, as described in RFC 8453.

Both the distributed and centralized control planes have their respective advantages and should complement each other in the system, rather than compete. This document outlines how the GMPLS distributed control plane can work together with a centralized controller system in a transport network.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9730.

in the Revised BSD License.

Table of Contents

1. Introduction

Generalized Multiprotocol Label Switching (GMPLS) [RFC3945] extends MPLS to support different classes of interfaces and switching capabilities such as Time-Division Multiplex Capable (TDM), Lambda Switch Capable (LSC), and Fiber-Switch Capable (FSC). Each network element (NE) running a GMPLS control plane collects network information from other NEs and supports service provisioning through signaling in a distributed manner. A more generic description of traffic-engineering networking information exchange can be found in [RFC7926].

On the other hand, Software-Defined Networking (SDN) technologies have been introduced to control the transport network centrally. Centralized controllers can collect network information from each node and provision services on corresponding nodes. One example is the Abstraction and Control of Traffic-Engineered Networks (ACTN) [RFC8453], which defines a hierarchical architecture with the Provisioning Network Controller (PNC), Multi-Domain Service

Coordinator (MDSC), and Customer Network Controller (CNC) as centralized controllers for different network abstraction levels. A PCE-based approach has been proposed in [RFC7491]: Application-Based Network Operations (ABNO).

GMPLS can be used to control network elements (NEs) in such centralized controller architectures. A centralized controller may support GMPLS-enabled domains and communicate with a GMPLS-enabled domain where the GMPLS control plane handles service provisioning from ingress to egress. In this scenario, the centralized controller sends a request to the entry node and does not need to configure all NEs along the path within the domain from ingress to egress, thus leveraging the GMPLS control plane. This document describes how the GMPLS control plane interworks with a centralized controller system in a transport network.

2. Abbreviations

The following abbreviations are used in this document.

ACTN: Abstraction and Control of Traffic-Engineered Networks [RFC8453]

APS: Automatic Protection Switching [G.808.1]

BRPC: Backward Recursive PCE-Based Computation [RFC5441]

CSPF: Constrained Shortest Path First

DoS: Denial of Service

E2E: end to end

ERO: Explicit Route Object

FA: Forwarding Adjacency

FRR: Fast Reroute

GMPLS: Generalized Multiprotocol Label Switching [RFC3945]

H-PCE: Hierarchical PCE [RFC8685]

IDS: Intrusion Detection System

IGP: Interior Gateway Protocol

IoCs: Indicators of Compromise [RFC9424]

IPS: Intrusion Prevention System

IS-IS: Intermediate System to Intermediate System

LMP: Link Management Protocol [RFC4204]

LSP: Label Switched Path

LSP-DB: LSP Database

MD: multi-domain

MDSC: Multi-Domain Service Coordinator [RFC8453]

MITM: Man in the Middle

ML: multi-layer

MPI: MDSC to PNC Interface [RFC8453]

NE: network element

NETCONF: Network Configuration Protocol [RFC6241]

NMS: Network Management System

OSPF: Open Shortest Path First

PCC: Path Computation Client [RFC4655]

PCE: Path Computation Element [RFC4655]

PCEP: PCE Communication Protocol [RFC5440]

PCEP-LS: Link State PCEP [PCEP-LS]

PLR: Point of Local Repair

PNC: Provisioning Network Controller [RFC8453]

RSVP: Resource Reservation Protocol

SBI: Southbound Interface

SDN: Software-Defined Networking

TE: Traffic Engineering

TED: Traffic Engineering Database

TLS: Transport Layer Security [RFC8446]

VNTM: Virtual Network Topology Manager [RFC5623]

3. Overview

This section provides an overview of the GMPLS control plane, centralized controller systems, and their interactions in transport networks.

A transport network [RFC5654] is a server-layer network designed to provide connectivity services for client-layer connectivity. This setup allows client traffic to be carried seamlessly across the server-layer network resources.

3.1. Overview of GMPLS Control Plane

GMPLS separates the control plane and the data plane to support time-division, wavelength, and spatial switching, which are significant in transport networks. For the NE level control in GMPLS, each node runs a GMPLS control plane instance. Functionalities such as service provisioning, protection, and restoration can be performed via GMPLS communication among multiple NEs. At the same time, the GMPLS control plane instance can also collect information about node and link resources in the network to construct the network topology and compute routing paths for serving service requests.

Several protocols have been designed for the GMPLS control plane [RFC3945], including link management [RFC4204], signaling [RFC3471], and routing [RFC4202] protocols. The GMPLS control plane instances applying these protocols communicate with each other to exchange resource information and establish LSPs. In this way, GMPLS control plane instances in different nodes in the network have the same view

of the network topology and provision services based on local policies.

3.2. Overview of Centralized Controller System

With the development of SDN technologies, a centralized controller architecture has been introduced to transport networks. One example architecture can be found in ACTN [RFC8453]. In such systems, a controller is aware of the network topology and is responsible for provisioning incoming service requests.

Multiple hierarchies of controllers are designed at different levels to implement different functions. This kind of architecture enables multi-vendor, multi-domain, and multi-technology control. For example, a higher-level controller coordinates several lower-level controllers controlling different domains for topology collection and service provisioning. Vendor-specific features can be abstracted between controllers, and a standard API (e.g., generated from RESTCONF [RFC8040] / YANG [RFC7950]) may be used.

3.3. GMPLS Control Interworking with a Centralized Controller System

Besides GMPLS and the interactions among the controller hierarchies, it is also necessary for the controllers to communicate with the network elements. Within each domain, GMPLS control can be applied to each NE. The bottom-level centralized controller can act as an NE to collect network information and initiate LSPs. Figure 1 shows an example of GMPLS interworking with centralized controllers (ACTN terminologies are used in the figure).

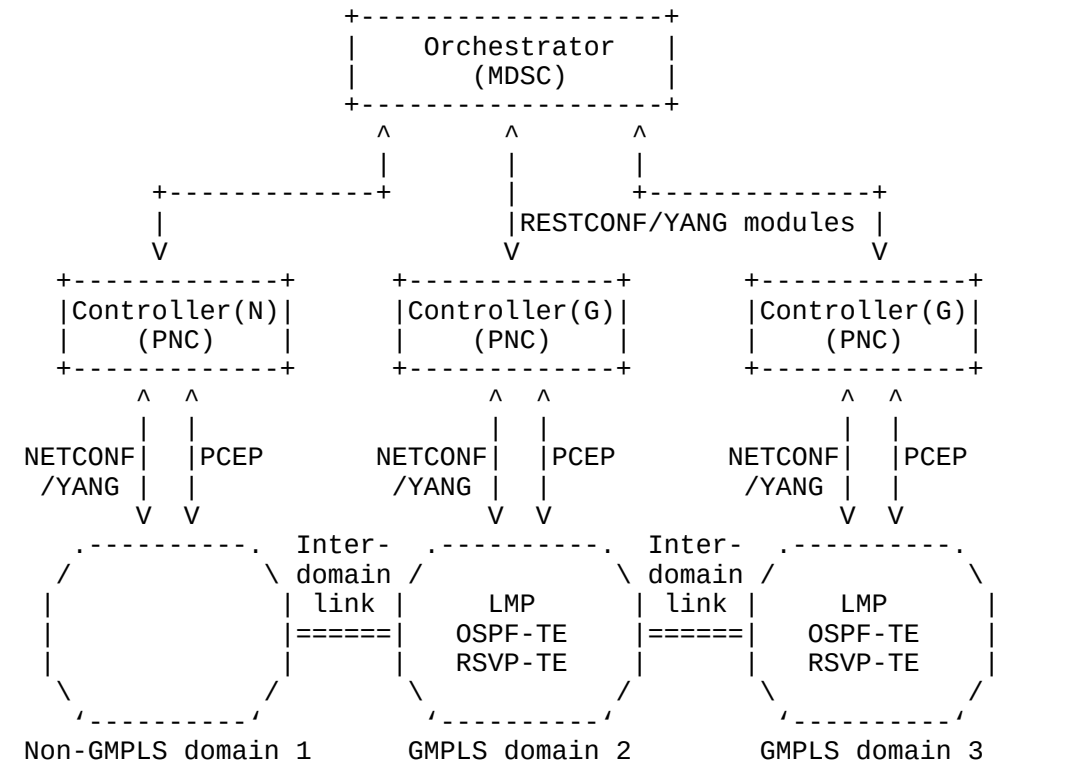


Figure 1: Example of GMPLS/non-GMPLS Interworking with Controllers

Controller(N): A domain controller controlling a non-GMPLS domain

Controller(G): A domain controller controlling a GMPLS domain

Figure 1 shows the scenario with two GMPLS domains and one non-GMPLS domain. This system supports the interworking among non-GMPLS domains, GMPLS domains, and the controller hierarchies.

For domain 1, the network elements were not enabled with GMPLS, so the control is purely from the controller, via Network Configuration Protocol (NETCONF) [RFC6241] with a YANG data model [RFC7950] and/or PCE Communication Protocol (PCEP) [RFC5440].

For domains 2 and 3:

* Each domain has the GMPLS control plane enabled at the physical network level. The Provisioning Network Controller (PNC) can exploit GMPLS capabilities implemented in the domain to listen to the IGP routing protocol messages (for example, OSPF Link State Advertisements (LSAs)) that the GMPLS control plane instances are disseminating into the network and thus learn the network topology. For path computation in the domain with the PNC implementing a PCE, Path Computation Clients (PCCs) (e.g., NEs, other controllers/PCEs) use PCEP to ask the PNC for a path and get replies. The Multi-Domain Service Coordinator (MDSC) communicates with PNCs using, for example, Representational State Transfer (REST) / RESTCONF based on YANG data models. As a PNC has learned its domain topology, it can report the topology to the MDSC. When a service arrives, the MDSC computes the path and coordinates PNCs to establish the corresponding LSP segment.

* Alternatively, the NETCONF protocol can be used to retrieve topology information utilizing the YANG module in [RFC8795] and the technology-specific YANG module augmentations required for the specific network technology. The PNC can retrieve topology information from any NE (the GMPLS control plane instance of each NE in the domain has the same topological view), construct the topology of the domain, and export an abstract view to the MDSC. Based on the topology retrieved from multiple PNCs, the MDSC can create a topology graph of the multi-domain network and can use it for path computation. To set up a service, the MDSC can exploit the YANG module in [YANG-TE] together with the technology-specific YANG module augmentations.

This document focuses on the interworking between GMPLS and the centralized controller system, including:

* the interworking between the GMPLS domains and the centralized controllers (including the orchestrator, if it exists) controlling the GMPLS domains and

* the interworking between a non-GMPLS domain (which is controlled by a centralized controller system) and a GMPLS domain, through the controller hierarchy architecture.

For convenience, this document uses the following terminologies for the controller and the orchestrator:

Controller(G): A domain controller controlling a GMPLS domain (the Controller(G) of the GMPLS domains 2 and 3 in Figure 1)

Controller(N): A domain controller controlling a non-GMPLS domain (the Controller(N) of the non-GMPLS domain 1 in Figure 1)

H-Controller(G): A domain controller controlling the higher-layer GMPLS domain, in the context of multi-layer networks

L-Controller(G): A domain controller controlling the lower-layer GMPLS domain, in the context of multi-layer networks

H-Controller(N): A domain controller controlling the higher-layer non-GMPLS domain, in the context of multi-layer networks

L-Controller(N): A domain controller controlling the lower-layer non-GMPLS domain, in the context of multi-layer networks

Orchestrator(MD): An orchestrator used to orchestrate the multi-domain networks

Orchestrator(ML): An orchestrator used to orchestrate the multi-layer networks

4. Discovery Options

In GMPLS control, the link connectivity must be verified between each pair of nodes. In this way, link resources, which are fundamental resources in the network, are discovered by both ends of the link.

4.1. LMP

The Link Management Protocol (LMP) [RFC4204] runs between nodes and manages TE links. In addition to the setup and maintenance of control channels, LMP can be used to verify the data link connectivity and correlate the link properties.

5. Routing Options

In GMPLS control, link state information is flooded within the network as defined in [RFC4202]. Each node in the network can build the network topology according to the flooded link state information. Routing protocols such as OSPF-TE [RFC4203] and IS-IS-TE [RFC5307] have been extended to support different interfaces in GMPLS.

In a centralized controller system, the centralized controller can be placed in the GMPLS network and passively receives the IGP information flooded in the network. In this way, the centralized controller can construct and update the network topology.

5.1. OSPF-TE

OSPF-TE is introduced for TE networks in [RFC3630]. OSPF extensions have been defined in [RFC4203] to enable the capability of link state information for the GMPLS network. Based on this work, OSPF has been extended to support technology-specific routing. The routing protocols for the Optical Transport Network (OTN), Wavelength Switched Optical Network (WSON), and optical flexi-grid networks are defined in [RFC7138], [RFC7688], and [RFC8363], respectively.

5.2. IS-IS-TE

IS-IS-TE is introduced for TE networks in [RFC5305], is extended to support GMPLS routing functions [RFC5307], and has been updated [RFC7074] to support the latest GMPLS switching capability and Types fields.

5.3. NETCONF/RESTCONF

NETCONF [RFC6241] and RESTCONF [RFC8040] protocols are originally used for network configuration. These protocols can also utilize topology-related YANG modules, such as those in [RFC8345] and [RFC8795]. These protocols provide a powerful mechanism for the notification (in addition to the provisioning and monitoring) of topology changes to the client.

6. Path Computation

6.1. Controller-Based Path Computation

Once a controller learns the network topology, it can utilize the

available resources to serve service requests by performing path computation. Due to abstraction, the controllers may not have sufficient information to compute the optimal path. In this case, the controller can interact with other controllers by sending, for example, YANG-based path computation requests [PATH-COMP] or PCEP to compute a set of potential optimal paths; and then, based on its constraints, policy, and specific knowledge (e.g., cost of access link), the controller can choose the more feasible path for end-to-end (E2E) service path setup.

Path computation is one of the key objectives in various types of controllers. In the given architecture, it is possible for different components that have the capability to compute the path.

6.2. Constraint-Based Path Computing in GMPLS Control

In GMPLS control, a routing path may be computed by the ingress node [RFC3473] based on the ingress node Traffic Engineering Database (TED). In this case, constraint-based path computation is performed according to the local policy of the ingress node.

6.3. Path Computation Element (PCE)

The PCE was first introduced in [RFC4655] as a functional component that offers services for computing paths within a network. In [RFC5440], path computation is achieved using the TED, which maintains a view of the link resources in the network. The introduction of the PCE has significantly improved the quality of network planning and offline computation. However, there is a potential risk that the computed path may be infeasible when there is a diversity requirement, as a stateless PCE lacks knowledge about previously computed paths.

To address this issue, a stateful PCE has been proposed in [RFC8231]. Besides the TED, an additional LSP Database (LSP-DB) is introduced to archive each LSP computed by the PCE. This way, the PCE can easily determine the relationship between the computing path and former computed paths. In this approach, the PCE provides computed paths to the PCC, and then the PCC decides which path is deployed and when it is to be established.

With PCE-initiated LSPs [RFC8281], the PCE can trigger the PCC to perform setup, maintenance, and teardown of the PCE-initiated LSP under the stateful PCE model. This would allow a dynamic network that is centrally controlled and deployed.

In a centralized controller system, the PCE can be implemented within the centralized controller. The centralized controller then calculates paths based on its local policies. Alternatively, the PCE can be located outside of the centralized controller. In this scenario, the centralized controller functions as a PCC and sends a path computation request to the PCE using the PCEP. A reference architecture for this can be found in [RFC7491].

7. Signaling Options

Signaling mechanisms are used to set up LSPs in GMPLS control. Messages are sent hop by hop between the ingress node and the egress node of the LSP to allocate labels. Once the labels are allocated along the path, the LSP setup is accomplished. Signaling protocols such as Resource Reservation Protocol - Traffic Engineering (RSVP-TE) [RFC3473] have been extended to support different interfaces in GMPLS.

7.1. RSVP-TE

RSVP-TE is introduced in [RFC3209] and extended to support GMPLS signaling in [RFC3473]. Several label formats are defined for a generalized label request, a generalized label, a suggested label, and label sets. Based on [RFC3473], RSVP-TE has been extended to support technology-specific signaling. The RSVP-TE extensions for the OTN, WSON, and optical flexi-grid network are defined in [RFC7139], [RFC7689], and [RFC7792], respectively.

8. Interworking Scenarios

8.1. Topology Collection and Synchronization

Topology information is necessary on both network elements and controllers. The topology on a network element is usually raw information, while the topology used by the controller can be either raw, reduced, or abstracted. Three different abstraction methods have been described in [RFC8453], and different controllers can select the corresponding method depending on the application.

When there are changes in the network topology, the impacted network elements need to report changes to all the other network elements, together with the controller, to sync up the topology information. The inter-NE synchronization can be achieved via protocols mentioned in Sections 4 and 5. The topology synchronization between NEs and controllers can either be achieved by routing protocols OSPF-TE/PCEP-LS in [PCEP-LS] or NETCONF protocol notifications with a YANG module.

8.2. Multi-Domain Service Provisioning

Service provisioning can be deployed based on the topology information on controllers and network elements. Many methods have been specified for single-domain service provisioning, such as the PCEP and RSVP-TE methods.

Multi-domain service provisioning would require coordination among the controller hierarchies. Given the service request, the end-to-end delivery procedure may include interactions at any level (i.e., interface) in the hierarchy of the controllers (e.g., MPI and SBI for ACTN). The computation for a cross-domain path is usually completed by controllers who have a global view of the topologies. Then the configuration is decomposed into lower-level controllers to configure the network elements to set up the path.

A combination of centralized and distributed protocols may be necessary to interact between network elements and controllers. Several methods can be used to create the inter-domain path:

1) With an end-to-end RSVP-TE session:

   In this method, all the domains need to support the RSVP-TE protocol and thus need to be GMPLS domains. The Controller(G) of the source domain triggers the source node to create the end-to-end RSVP-TE session; and the assignment and distribution of the labels on the inter-domain links are done by the border nodes of each domain, using RSVP-TE protocol. Therefore, this method requires the interworking of RSVP-TE protocols between different domains.

   There are two possible methods:

   1.1) One single end-to-end RSVP-TE session:

      In this method, an end-to-end RSVP-TE session from the source node to the destination node will be used to create the inter-domain path. A typical example would be the PCE initiation scenario, in which a PCE message (PCInitiate) is

sent from the Controller(G) to the source node, triggering an RSVP procedure along the path. Similarly, the interaction between the controller and the source node of the source domain can be achieved by using the NETCONF protocol with corresponding YANG modules, and then it can be completed by running RSVP among the network elements.

1.2) LSP Stitching:

The LSP stitching method defined in [RFC5150] can also create the E2E LSP. That is, when the source node receives an end-to-end path creation request (e.g., using PCEP or NETCONF protocol), the source node starts an end-to-end RSVP-TE session along the endpoints of each LSP segment (S-LSP) (refers to S-LSP in [RFC5150]) of each domain, to assign the labels on the inter-domain links between each pair of neighbor S-LSPs and to stitch the end-to-end LSP to each S-LSP. See Figure 2 as an example.

Note that the S-LSP in each domain can be either created by its Controller(G) in advance or created dynamically triggered by the end-to-end RSVP-TE session.

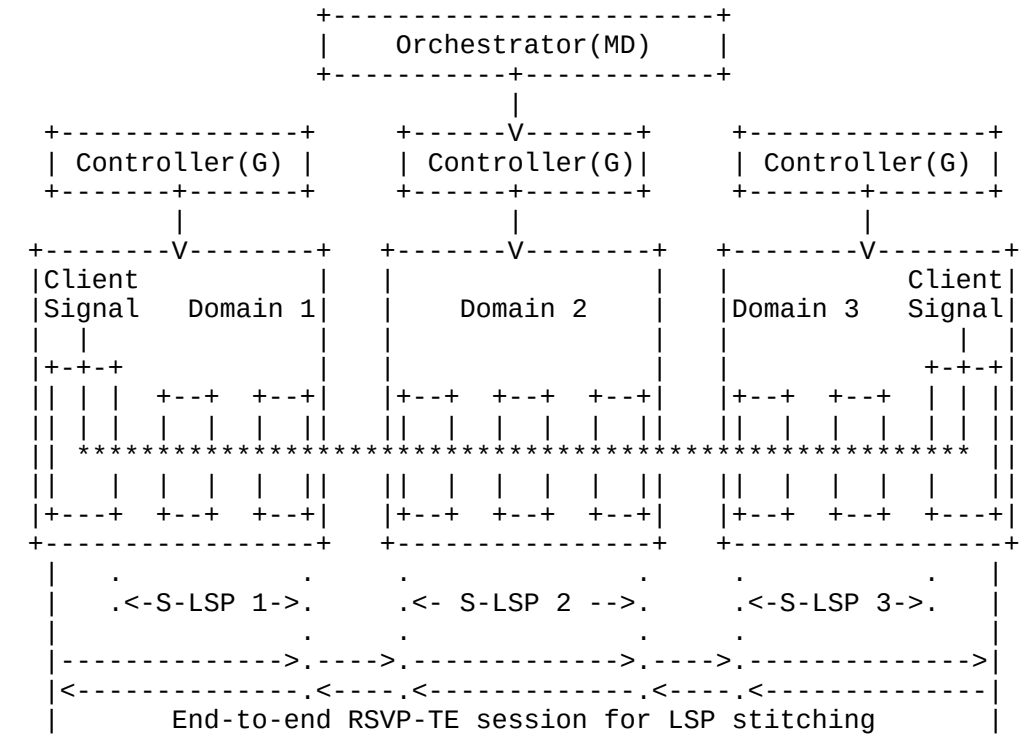


Figure 2: LSP Stitching

2) Without an end-to-end RSVP-TE session:

In this method, each domain can be a GMPLS domain or a non-GMPLS domain. Each controller (which may be a Controller(G) or a Controller(N)) is responsible for creating the path segment within its domain. The border node does not need to communicate with other border nodes in other domains for the distribution of labels on inter-domain links, so an end-to-end RSVP-TE session through multiple domains is not required, and the interworking of the RSVP-TE protocol between different domains is not needed.

Note that path segments in the source domain and the destination domain are "asymmetrical" segments, because the configuration of client signal mapping into the server-layer tunnel is needed at only one end of the segment, while configuration of the server-

layer cross-connect is needed at the other end of the segment. See the example in Figure 3.

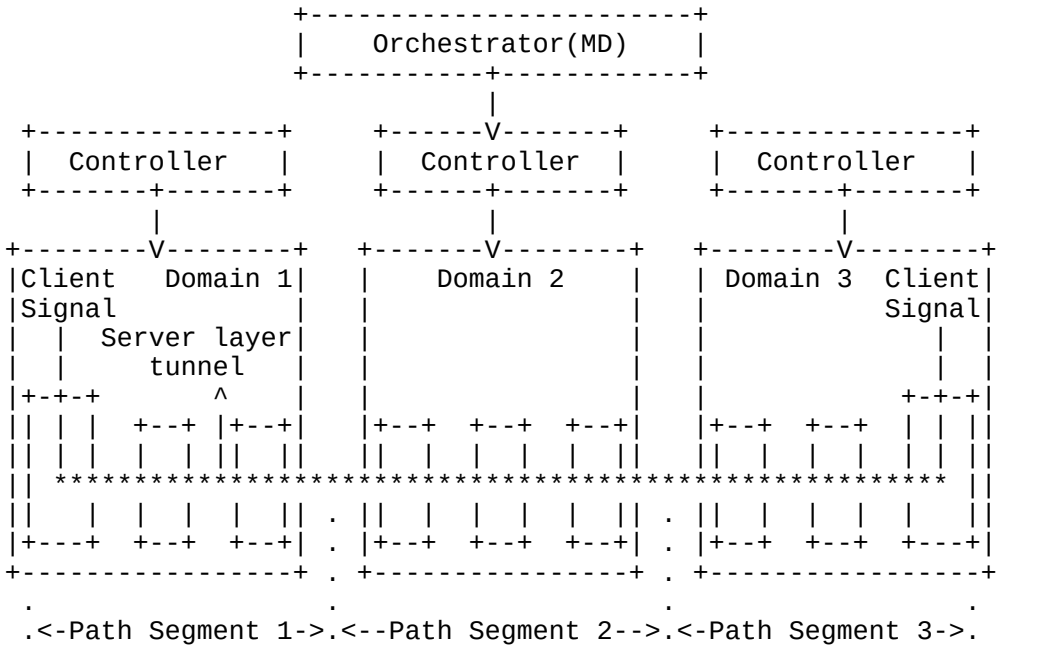


Figure 3: Example of an Asymmetrical Path Segment

The PCEP / GMPLS protocols should support the creation of such asymmetrical segments.

Note also that mechanisms to assign the labels in the inter-domain links also need to be considered. There are two possible methods:

2.1) Inter-domain labels assigned by NEs:

The concept of a stitching label that allows stitching local path segments was introduced in [RFC5150] and [SPCE-ID], in order to form the inter-domain path crossing several different domains. It also describes the Backward Recursive PCE-Based Computation (BRPC) [RFC5441] and Hierarchical PCE (H-PCE) [RFC8685] PCInitiate procedure, i.e., the ingress node of each downstream domain assigns the stitching label for the inter-domain link between the downstream domain and its upstream neighbor domain; and this stitching label will be passed to the upstream neighbor domain by PCE protocol, which will be used for the path segment creation in the upstream neighbor domain.

2.2) Inter-domain labels assigned by the controller:

If the resources of inter-domain links are managed by the Orchestrator(MD), each domain controller can provide to the Orchestrator(MD) the list of available labels (e.g., time slots if the OTN is the scenario) using topology-related YANG modules and specific technology-related extensions. Once the orchestrator(MD) has computed the E2E path, RSVP-TE or PCEP can be used in the different domains to set up the related segment tunnel consisting of information about inter-domain labels; for example, for PCEP, the label Explicit Route Object (ERO) can be included in the PCInitiate message to indicate the inter-domain labels so that each border node of each domain can configure the correct cross-connect within itself.

8.3. Multi-Layer Service Provisioning

GMPLS can interwork with centralized controller systems in multi-layer networks.

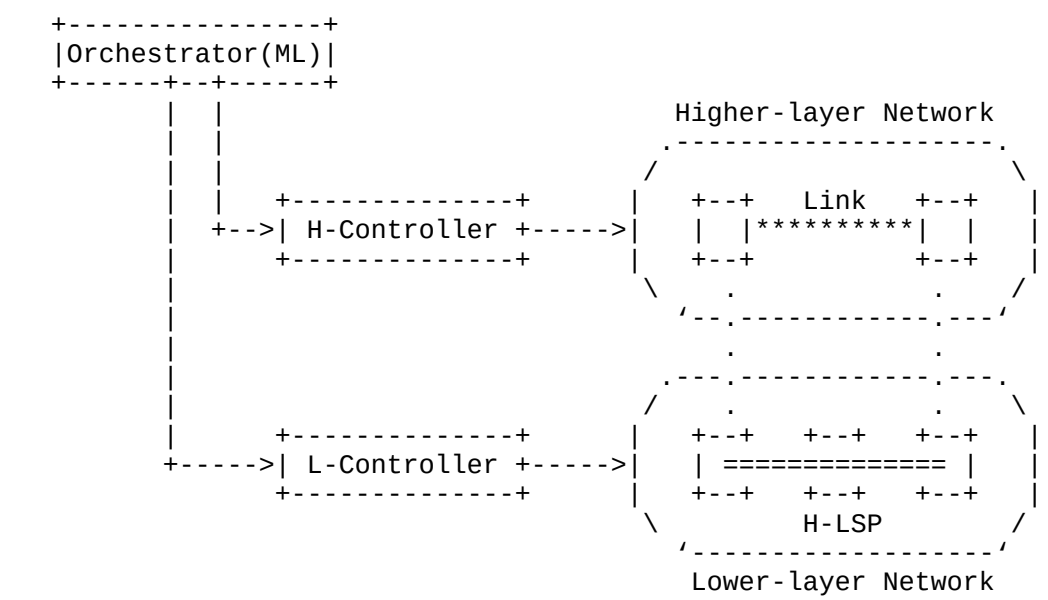


Figure 4: GMPLS-controller Interworking in Multi-Layer Networks

An example with two layers of network is shown in Figure 4. In this example, the GMPLS control plane is enabled in at least one layer network (otherwise, it is out of the scope of this document) and interworks with the controller of its domain (H-Controller and L-Controller, respectively). The Orchestrator(ML) is used to coordinate the control of the multi-layer network.

8.3.1. Multi-Layer Path Computation

[RFC5623] describes three inter-layer path computation models and four inter-layer path control models:

* 3 path computation models:
  - Single PCE path computation model
  - Multiple PCE path computation with inter-PCE communication model
  - Multiple PCE path computation without inter-PCE communication model
* 4 path control models:
  - PCE Virtual Network Topology Manager (PCE-VNTM) cooperation model
  - Higher-layer signaling trigger model
  - Network Management System VNTM (NMS-VNTM) cooperation model (integrated flavor)
  - NMS-VNTM cooperation model (separate flavor)

Section 4.2.4 of [RFC5623] also provides all the possible combinations of inter-layer path computation and inter-layer path control models.

To apply [RFC5623] in a multi-layer network with GMPLS-controller interworking, the H-Controller and the L-Controller can act as the PCE Hi and PCE Lo, respectively; and typically, the Orchestrator(ML) can act as a VNTM because it has the abstracted view of both the higher-layer and lower-layer networks.

Table 1 shows all possible combinations of path computation and path control models in multi-layer network with GMPLS-controller interworking:

Path computation / Path control	Single PCE	Multiple PCE with inter-PCE	Multiple PCE w/o inter-PCE
PCE-VNTM cooperation	N/A	Yes	Yes
Higher-layer signaling trigger	N/A	Yes	Yes
NMS-VNTM cooperation (integrated flavor)	N/A	Yes (1)	No (1)
NMS-VNTM cooperation (separate flavor)	N/A	No (1)	Yes (1)

Table 1: Combinations of Path Computation and Path Control Models

Note that:

* Since there is one PCE in each layer network, the path computation model "Single PCE path computation" is not applicable (N/A).

* For the other two path computation models "Multiple PCE with inter-PCE" and "Multiple PCE w/o inter-PCE", the possible combinations are the same as defined in [RFC5623]. More specifically:

  - (1) The path control models "NMS-VNTM cooperation (integrated flavor)" and "NMS-VNTM cooperation (separate flavor)" are the typical models to be used in a multi-layer network with GMPLS-controller interworking. This is because, in these two models, the path computation is triggered by the NMS or VNTM. And in the centralized controller system, the path computation requests are typically from the Orchestrator(ML) (acts as VNTM).

  - For the other two path control models "PCE-VNTM cooperation" and "Higher-layer signaling trigger", the path computation is triggered by the NEs, i.e., the NE performs PCC functions. It is still possible to use these two models, although they are not the main methods.

8.3.2. Cross-Layer Path Creation

In a multi-layer network, a lower-layer LSP in the lower-layer network can be created, which will construct a new link in the higher-layer network. Such a lower-layer LSP is called Hierarchical LSP, or H-LSP for short; see [RFC6107].

The new link constructed by the H-LSP can then be used by the higher-layer network to create new LSPs.

As described in [RFC5212], two methods are introduced to create the H-LSP: the static (pre-provisioned) method and the dynamic (triggered) method.

1) Static (pre-provisioned) method:

In this method, the H-LSP in the lower-layer network is created in advance. After that, the higher-layer network can create LSPs using the resource of the link constructed by the H-LSP.

The Orchestrator(ML) is responsible to decide the creation of H-LSP in the lower-layer network if it acts as a VNTM. Then it requests the L-Controller to create the H-LSP via, for example, an MPI under the ACTN architecture.

If the lower-layer network is a GMPLS domain, the L-Controller(G) can trigger the GMPLS control plane to create the H-LSP. As a typical example, the PCInitiate message can be used for the communication between the L-Controller and the source node of the H-LSP. And the source node of the H-LSP can trigger the RSVP-TE signaling procedure to create the H-LSP, as described in [RFC6107].

If the lower-layer network is a non-GMPLS domain, other methods may be used by the L-Controller(N) to create the H-LSP, which is out of scope of this document.

2) Dynamic (triggered) method:

In this method, the signaling of LSP creation in the higher-layer network will trigger the creation of H-LSP in the lower-layer network dynamically, if it is necessary. Therefore, both the higher-layer and lower-layer networks need to support the RSVP-TE protocol and thus need to be GMPLS domains.

In this case, after the cross-layer path is computed, the Orchestrator(ML) requests the H-Controller(G) for the cross-layer LSP creation. As a typical example, the MPI under the ACTN architecture could be used.

The H-Controller(G) can trigger the GMPLS control plane to create the LSP in the higher-layer network. As a typical example, the PCInitiate message can be used for the communication between the H-Controller(G) and the source node of the higher-layer LSP, as described in Section 4.3 of [RFC8282]. At least two sets of ERO information should be included to indicate the routes of higher-layer LSP and lower-layer H-LSP.

The source node of the higher-layer LSP follows the procedure defined in Section 4 of [RFC6001] to trigger the GMPLS control plane in both the higher-layer network and the lower-layer network to create the higher-layer LSP and the lower-layer H-LSP.

On success, the source node of the H-LSP should report the information of the H-LSP to the L-Controller(G) via, for example, the PCRpt message.

8.3.3. Link Discovery

If the higher-layer network and the lower-layer network are under the same GMPLS control plane instance, the H-LSP can be a Forwarding Adjacency LSP (FA-LSP). Then the information of the link constructed by this FA-LSP can be advertised in the routing instance, so that the H-Controller can be aware of this new FA. [RFC4206] and the following updates to it (including [RFC6001] and [RFC6107]) describe the detailed extensions to support advertisement of an FA.

If the higher-layer network and the lower-layer network are under separate GMPLS control plane instances or if one of the layer

networks is a non-GMPLS domain, after an H-LSP is created in the lower-layer network, the link discovery procedure will be triggered in the higher-layer network to discover the information of the link constructed by the H-LSP. The LMP defined in [RFC4204] can be used if the higher-layer network supports GMPLS. The information of this new link will be advertised to the H-Controller.

8.4. Recovery

The GMPLS recovery functions are described in [RFC4426]. Span protection and end-to-end protection and restoration are discussed with different protection schemes and message exchange requirements. Related RSVP-TE extensions to support end-to-end recovery are described in [RFC4872]. The extensions in [RFC4872] include protection, restoration, preemption, and rerouting mechanisms for an end-to-end LSP. Besides end-to-end recovery, a GMPLS segment recovery mechanism is defined in [RFC4873], which also intends to be compatible with Fast Reroute (FRR) (see [RFC4090], which defines RSVP-TE extensions for the FRR mechanism, and [RFC8271], which describes the updates of the GMPLS RSVP-TE protocol for FRR of GMPLS TE-LSPs).

8.4.1. Span Protection

Span protection refers to the protection of the link between two neighboring switches. The main protocol requirements include:

* Link management: Link property correlation on the link protection type

* Routing: Announcement of the link protection type

* Signaling: Indication of link protection requirement for that LSP

GMPLS already supports the above requirements, and there are no new requirements in the scenario of interworking between GMPLS and a centralized controller system.

8.4.2. LSP Protection

The LSP protection includes end-to-end and segment LSP protection. For both cases:

* In the provisioning phase:

  In both single-domain and multi-domain scenarios, the disjoint path computation can be done by the centralized controller system, as it has the global topology and resource view. And the path creation can be done by the procedure described in Section 8.2.

* In the protection switchover phase:

  In both single-domain and multi-domain scenarios, the existing standards provide the distributed way to trigger the protection switchover, for example, the data plane Automatic Protection Switching (APS) mechanism described in [G.808.1], [RFC7271], and [RFC8234] or the GMPLS Notify mechanism described in [RFC4872] and [RFC4873]. In the scenario of interworking between GMPLS and a centralized controller system, using these distributed mechanisms rather than a centralized mechanism (i.e., the controller triggers the protection switchover) can significantly shorten the protection switching time.

8.4.3. Single-Domain LSP Restoration

* Pre-planned LSP protection (including shared-mesh restoration):

In pre-planned protection, the protecting LSP is established only in the control plane in the provisioning phase and will be activated in the data plane once failure occurs.

In the scenario of interworking between GMPLS and a centralized controller system, the route of protecting LSP can be computed by the centralized controller system. This takes the advantage of making better use of network resources, especially for the resource-sharing in shared-mesh restoration.

* Full LSP rerouting:

In full LSP rerouting, the normal traffic will be switched to an alternate LSP that is fully established only after a failure occurrence.

As described in [RFC4872] and [RFC4873], the alternate route can be computed on demand when there is a failure occurrence or can be pre-computed and stored before a failure occurrence.

In a fully distributed scenario, the pre-computation method offers a faster restoration time but has the risk that the pre-computed alternate route may become out-of-date due to the changes of the network.

In the scenario of interworking between GMPLS and a centralized controller system, the pre-computation of the alternate route could take place in the centralized controller (and may be stored in the controller or the head-end node of the LSP). In this way, any changes in the network can trigger the refreshment of the alternate route by the centralized controller. This makes sure that the alternate route will not become out-of-date.

8.4.4. Multi-Domain LSP Restoration

A working LSP may traverse multiple domains, each of which may or may not support a GMPLS distributed control plane.

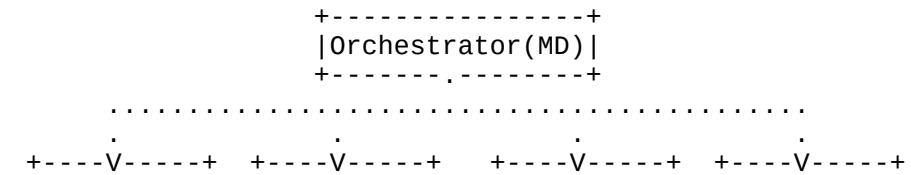
If all the domains support GMPLS, both the end-to-end rerouting method and the domain segment rerouting method could be used.

If only some domains support GMPLS, the domain segment rerouting method could be used in those GMPLS domains. For other domains that do not support GMPLS, other mechanisms may be used to protect the LSP segments, which are out of scope of this document.

1) End-to-end rerouting:

In this scenario, a failure on the working LSP inside any domain or on the inter-domain links will trigger the end-to-end restoration.

In both pre-planned and full LSP rerouting, the end-to-end protecting LSP could be computed by the centralized controller system and could be created by the procedure described in Section 8.2. Note that the end-to-end protecting LSP may traverse different domains from the working LSP, depending on the result of multi-domain path computation for the protecting LSP.



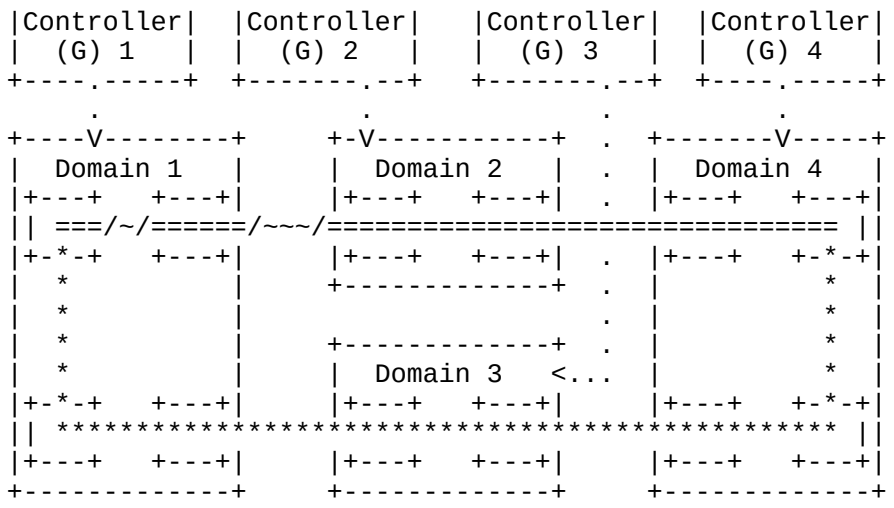


Figure 5: End-to-End Restoration

2) Domain segment rerouting:

2.1) Intra-domain rerouting:

If failure occurs on the working LSP segment in a GMPLS domain, the segment rerouting [RFC4873] could be used for the working LSP segment in that GMPLS domain. Figure 6 shows an example of intra-domain rerouting.

The intra-domain rerouting of a non-GMPLS domain is out of scope of this document.

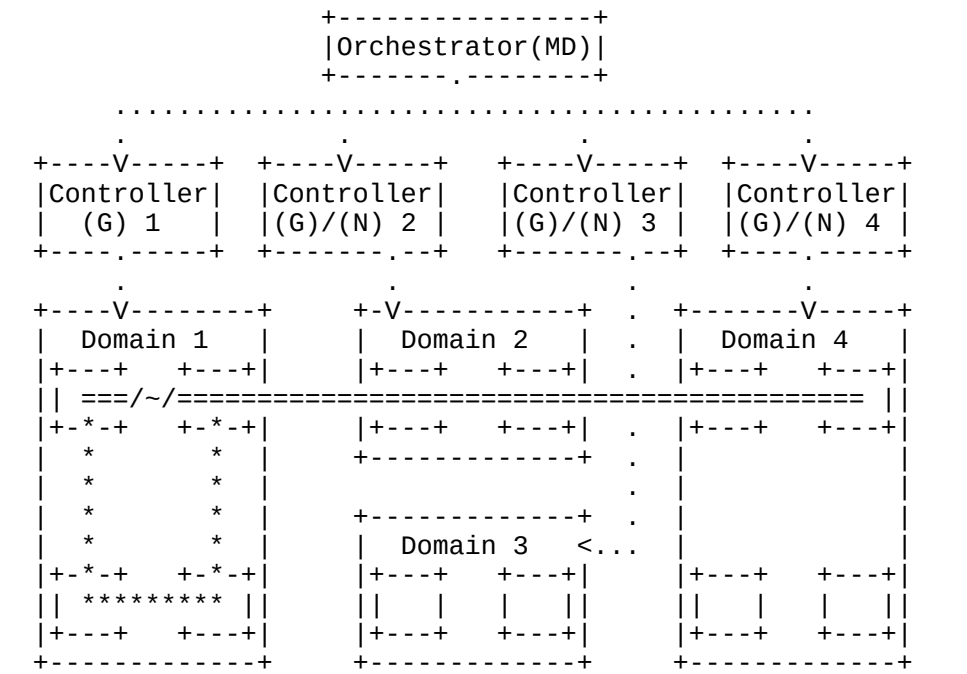


Figure 6: Intra-Domain Segment Rerouting

2.2) Inter-domain rerouting:

If intra-domain segment rerouting failed (e.g., due to lack of resource in that domain), or if failure occurs on the

working LSP on an inter-domain link, the centralized controller system may coordinate with other domain(s) to find an alternative path or path segment to bypass the failure and then trigger the inter-domain rerouting procedure. Note that the rerouting path or path segment may traverse different domains from the working LSP.

The domains involved in the inter-domain rerouting procedure need to be GMPLS domains, which support the RSVP-TE signaling for the creation of a rerouting LSP segment.

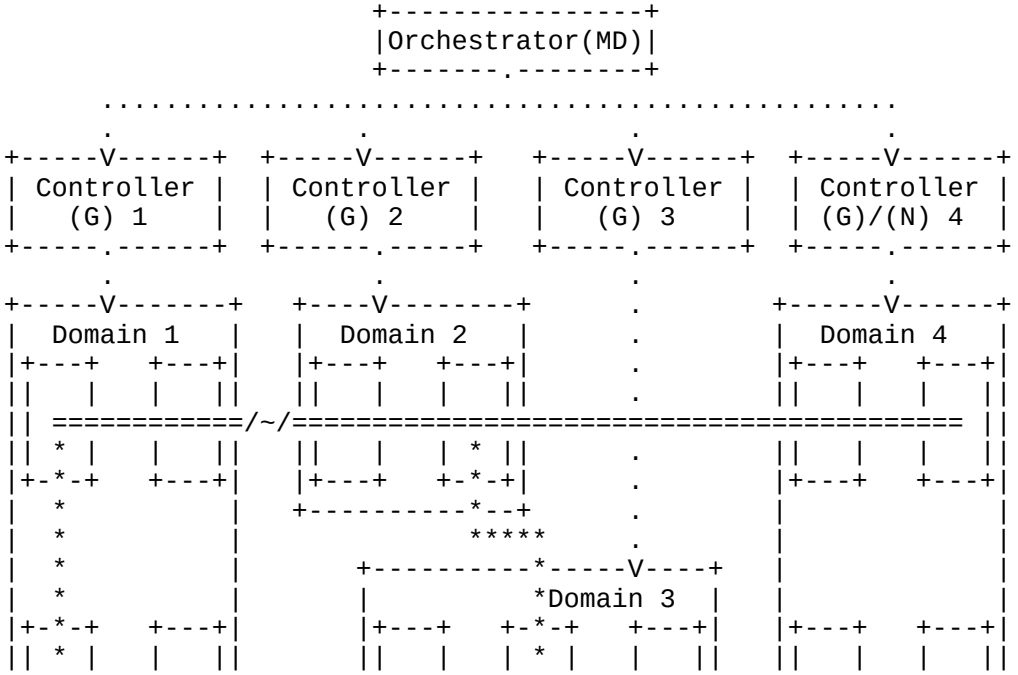
For inter-domain rerouting, the interaction between GMPLS and a centralized controller system is needed:

* A report of the result of intra-domain segment rerouting to its Controller(G) and then to the Orchestrator(MD). The former could be supported by the PCRpt message in [RFC8231], while the latter could be supported by the MPI of ACTN.

* A report of inter-domain link failure to the two Controllers (e.g., Controller(G) 1 and Controller(G) 2 in Figure 7) by which the two ends of the inter-domain link are controlled, respectively, and then to the Orchestrator(MD). The former could be done as described in Section 8.1, while the latter could be supported by the MPI of ACTN.

* The computation of a rerouting path or path segment crossing multi-domains by the centralized controller system (see [PATH-COMP]);

* The creation of a rerouting LSP segment in each related domain. The Orchestrator(MD) can send the LSP segment rerouting request to the source Controller(G) (e.g., Controller(G) 1 in Figure 7) via MPI interface, and then the Controller(G) can trigger the creation of a rerouting LSP segment through multiple GMPLS domains using GMPLS rerouting signaling. Note that the rerouting LSP segment may traverse a new domain that the working LSP does not traverse (e.g., Domain 3 in Figure 7).



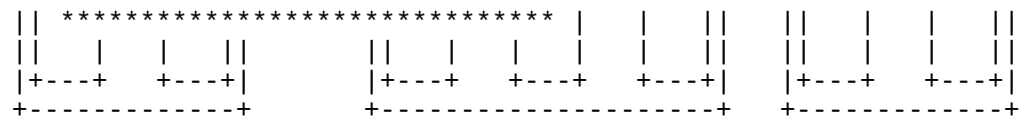


Figure 7: Inter-Domain Segment Rerouting

8.4.5. Fast Reroute

[RFC4090] defines two methods of fast reroute: the one-to-one backup method and the facility backup method. For both methods:

1) Path computation of protecting LSP:

   In Section 6.2 of [RFC4090], the protecting LSP (detour LSP in one-to-one backup or bypass tunnel in facility backup) could be computed by the Point of Local Repair (PLR) using, for example, a Constrained Shortest Path First (CSPF) computation. In the scenario of interworking between GMPLS and a centralized controller system, the protecting LSP could also be computed by the centralized controller system, as it has the global view of the network topology, resources, and information of LSPs.

2) Protecting LSP creation:

   In the scenario of interworking between GMPLS and a centralized controller system, the protecting LSP could still be created by the RSVP-TE signaling protocol as described in [RFC4090] and [RFC8271].

   In addition, if the protecting LSP is computed by the centralized controller system, the Secondary Explicit Route Object defined in [RFC4873] could be used to explicitly indicate the route of the protecting LSP.

3) Failure detection and traffic switchover:

   If a PLR detects that failure occurs, it may significantly shorten the protection switching time by using the distributed mechanisms described in [RFC4090] to switch the traffic to the related detour LSP or bypass tunnel rather than doing so in a centralized way.

8.5. Controller Reliability

The reliability of the controller is crucial due to its important role in the network. It is essential that if the controller is shut down or disconnected from the network, all currently provisioned services in the network continue to function and carry traffic. In addition, protection switching to pre-established paths should also work. It is desirable to have protection mechanisms, such as redundancy, to maintain full operational control even if one instance of the controller fails. This can be achieved through controller backup or functionality backup. There are several controller backup or federation mechanisms in the literature. It is also more reliable to have function backup in the network element to guarantee performance in the network.

9. Manageability Considerations

Each network entity, including controllers and network elements, should be managed properly and with the relevant trust and security policies applied (see Section 10), as they will interact with other entities. The manageability considerations in controller hierarchies

and network elements still apply, respectively. The overall manageability of the protocols applied in the network should also be a key consideration.

The responsibility of each entity should be clarified. The control of function and policy among different controllers should be consistent via a proper negotiation process.

10. Security Considerations

This document outlines the interworking between GMPLS and controller hierarchies. The security requirements specific to both systems remain applicable. Protocols referenced herein possess security considerations, which must be adhered to, with their core specifications and identified risks detailed earlier in this document.

Security is a critical aspect in both GMPLS and controller-based networks. Ensuring robust security mechanisms in these environments is paramount to safeguard against potential threats and vulnerabilities. Below are expanded security considerations and some relevant IETF RFC references.

* Authentication and Authorization: It is essential to implement strong authentication and authorization mechanisms to control access to the controller from multiple network elements. This ensures that only authorized devices and users can interact with the controller, preventing unauthorized access that could lead to network disruptions or data breaches. "The Transport Layer Security (TLS) Protocol Version 1.3" [RFC8446] and "Enrollment over Secure Transport" [RFC7030] provide guidelines on secure communication and certificate-based authentication that can be leveraged for these purposes.

* Controller Security: The controller’s security is crucial as it serves as the central control point for the network elements. The controller must be protected against various attacks, such as Denial of Service (DoS), Man in the Middle (MITM), and unauthorized access. Security mechanisms should include regular security audits, application of security patches, firewalls, and Intrusion Detection Systems (IDSs) / Intrusion Prevention Systems (IPSs).

* Data Transport Security: Security mechanisms on the controller should also safeguard the underlying network elements against unauthorized usage of data transport resources. This includes encryption of data in transit to prevent eavesdropping and tampering as well as ensuring data integrity and confidentiality.

* Secure Protocol Implementation: Protocols used within the GMPLS and controller frameworks must be implemented with security in mind. Known vulnerabilities should be addressed, and secure versions of protocols should be used wherever possible.

Finally, robust network security often depends on Indicators of Compromise (IoCs) to detect, trace, and prevent malicious activities in networks or endpoints. These are described in [RFC9424] along with the fundamentals, opportunities, operational limitations, and recommendations for IoC use.

11. IANA Considerations

This document has no IANA actions.

12. References

12.1. Normative References

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[RFC3473] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, DOI 10.17487/RFC3473, January 2003, <https://www.rfc-editor.org/info/rfc3473>.

[RFC3630] Katz, D., Kompella, K., and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, DOI 10.17487/RFC3630, September 2003, <https://www.rfc-editor.org/info/rfc3630>.

[RFC3945] Mannie, E., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, DOI 10.17487/RFC3945, October 2004, <https://www.rfc-editor.org/info/rfc3945>.

[RFC4090] Pan, P., Ed., Swallow, G., Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, DOI 10.17487/RFC4090, May 2005, <https://www.rfc-editor.org/info/rfc4090>.

[RFC4203] Kompella, K., Ed. and Y. Rekhter, Ed., "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4203, DOI 10.17487/RFC4203, October 2005, <https://www.rfc-editor.org/info/rfc4203>.

[RFC4206] Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", RFC 4206, DOI 10.17487/RFC4206, October 2005, <https://www.rfc-editor.org/info/rfc4206>.

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

[RFC4872] Lang, J.P., Ed., Rekhter, Y., Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, DOI 10.17487/RFC4872, May 2007, <https://www.rfc-editor.org/info/rfc4872>.

[RFC4873] Berger, L., Bryskin, I., Papadimitriou, D., and A. Farrel, "GMPLS Segment Recovery", RFC 4873, DOI 10.17487/RFC4873, May 2007, <https://www.rfc-editor.org/info/rfc4873>.

[RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, DOI 10.17487/RFC5305, October 2008, <https://www.rfc-editor.org/info/rfc5305>.

[RFC5307] Kompella, K., Ed. and Y. Rekhter, Ed., "IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 5307, DOI 10.17487/RFC5307, October 2008, <https://www.rfc-editor.org/info/rfc5307>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009,

<https://www.rfc-editor.org/info/rfc5440>.

[RFC6001] Papadimitriou, D., Vigoureux, M., Shiomoto, K., Brungard, D., and JL. Le Roux, "Generalized MPLS (GMPLS) Protocol Extensions for Multi-Layer and Multi-Region Networks (MLN/MRN)", RFC 6001, DOI 10.17487/RFC6001, October 2010, <https://www.rfc-editor.org/info/rfc6001>.

[RFC6107] Shiomoto, K., Ed. and A. Farrel, Ed., "Procedures for Dynamically Signaled Hierarchical Label Switched Paths", RFC 6107, DOI 10.17487/RFC6107, February 2011, <https://www.rfc-editor.org/info/rfc6107>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC7074] Berger, L. and J. Meuric, "Revised Definition of the GMPLS Switching Capability and Type Fields", RFC 7074, DOI 10.17487/RFC7074, November 2013, <https://www.rfc-editor.org/info/rfc7074>.

[RFC7491] King, D. and A. Farrel, "A PCE-Based Architecture for Application-Based Network Operations", RFC 7491, DOI 10.17487/RFC7491, March 2015, <https://www.rfc-editor.org/info/rfc7491>.

[RFC7926] Farrel, A., Ed., Drake, J., Bitar, N., Swallow, G., Ceccarelli, D., and X. Zhang, "Problem Statement and Architecture for Information Exchange between Interconnected Traffic-Engineered Networks", BCP 206, RFC 7926, DOI 10.17487/RFC7926, July 2016, <https://www.rfc-editor.org/info/rfc7926>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8271] Taillon, M., Saad, T., Ed., Gandhi, R., Ed., Ali, Z., and M. Bhatia, "Updates to the Resource Reservation Protocol for Fast Reroute of Traffic Engineering GMPLS Label Switched Paths (LSPs)", RFC 8271, DOI 10.17487/RFC8271, October 2017, <https://www.rfc-editor.org/info/rfc8271>.

[RFC8282] Oki, E., Takeda, T., Farrel, A., and F. Zhang, "Extensions to the Path Computation Element Communication Protocol (PCEP) for Inter-Layer MPLS and GMPLS Traffic Engineering", RFC 8282, DOI 10.17487/RFC8282, December 2017, <https://www.rfc-editor.org/info/rfc8282>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8453] Ceccarelli, D., Ed. and Y. Lee, Ed., "Framework for Abstraction and Control of TE Networks (ACTN)", RFC 8453,

DOI 10.17487/RFC8453, August 2018,
<https://www.rfc-editor.org/info/rfc8453>.

[RFC8685] Zhang, F., Zhao, Q., Gonzalez de Dios, O., Casellas, R., and D. King, "Path Computation Element Communication Protocol (PCEP) Extensions for the Hierarchical Path Computation Element (H-PCE) Architecture", RFC 8685, DOI 10.17487/RFC8685, December 2019, <https://www.rfc-editor.org/info/rfc8685>.

[RFC8795] Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and O. Gonzalez de Dios, "YANG Data Model for Traffic Engineering (TE) Topologies", RFC 8795, DOI 10.17487/RFC8795, August 2020, <https://www.rfc-editor.org/info/rfc8795>.

[RFC9424] Paine, K., Whitehouse, O., Sellwood, J., and A. Shaw, "Indicators of Compromise (IoCs) and Their Role in Attack Defence", RFC 9424, DOI 10.17487/RFC9424, August 2023, <https://www.rfc-editor.org/info/rfc9424>.

12.2. Informative References

[G.808.1] ITU-T, "Generic protection switching - Linear trail and subnetwork protection", ITU-T Recommendation G.808.1, May 2014, <https://www.itu.int/rec/T-REC-G.808.1-201405-I/en>.

[PATH-COMP] Busi, I., Belotti, S., de Dios, O. G., Sharma, A., and Y. Shi, "A YANG Data Model for requesting path computation", Work in Progress, Internet-Draft, draft-ietf-teas-yang-path-computation-24, 13 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-yang-path-computation-24>.

[PCEP-LS] Dhody, D., Peng, S., Lee, Y., Ceccarelli, D., Wang, A., and G. S. Mishra, "PCEP extensions for Distribution of Link-State and TE Information", Work in Progress, Internet-Draft, draft-ietf-pce-pcep-ls-02, 20 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-pcep-ls-02>.

[RFC3471] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, DOI 10.17487/RFC3471, January 2003, <https://www.rfc-editor.org/info/rfc3471>.

[RFC4202] Kompella, K., Ed. and Y. Rekhter, Ed., "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4202, DOI 10.17487/RFC4202, October 2005, <https://www.rfc-editor.org/info/rfc4202>.

[RFC4204] Lang, J., Ed., "Link Management Protocol (LMP)", RFC 4204, DOI 10.17487/RFC4204, October 2005, <https://www.rfc-editor.org/info/rfc4204>.

[RFC4426] Lang, J., Ed., Rajagopalan, B., Ed., and D. Papadimitriou, Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Recovery Functional Specification", RFC 4426, DOI 10.17487/RFC4426, March 2006, <https://www.rfc-editor.org/info/rfc4426>.

[RFC5150] Ayyangar, A., Kompella, K., Vasseur, JP., and A. Farrel, "Label Switched Path Stitching with Generalized Multiprotocol Label Switching Traffic Engineering (GMPLS TE)", RFC 5150, DOI 10.17487/RFC5150, February 2008,

<https://www.rfc-editor.org/info/rfc5150>.

[RFC5212] Shiomoto, K., Papadimitriou, D., Le Roux, JL., Vigoureux, M., and D. Brungard, "Requirements for GMPLS-Based Multi-Region and Multi-Layer Networks (MRN/MLN)", RFC 5212, DOI 10.17487/RFC5212, July 2008, <https://www.rfc-editor.org/info/rfc5212>.

[RFC5441] Vasseur, JP., Ed., Zhang, R., Bitar, N., and JL. Le Roux, "A Backward-Recursive PCE-Based Computation (BRPC) Procedure to Compute Shortest Constrained Inter-Domain Traffic Engineering Label Switched Paths", RFC 5441, DOI 10.17487/RFC5441, April 2009, <https://www.rfc-editor.org/info/rfc5441>.

[RFC5623] Oki, E., Takeda, T., Le Roux, JL., and A. Farrel, "Framework for PCE-Based Inter-Layer MPLS and GMPLS Traffic Engineering", RFC 5623, DOI 10.17487/RFC5623, September 2009, <https://www.rfc-editor.org/info/rfc5623>.

[RFC5654] Niven-Jenkins, B., Ed., Brungard, D., Ed., Betts, M., Ed., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, DOI 10.17487/RFC5654, September 2009, <https://www.rfc-editor.org/info/rfc5654>.

[RFC7138] Ceccarelli, D., Ed., Zhang, F., Belotti, S., Rao, R., and J. Drake, "Traffic Engineering Extensions to OSPF for GMPLS Control of Evolving G.709 Optical Transport Networks", RFC 7138, DOI 10.17487/RFC7138, March 2014, <https://www.rfc-editor.org/info/rfc7138>.

[RFC7139] Zhang, F., Ed., Zhang, G., Belotti, S., Ceccarelli, D., and K. Pithewan, "GMPLS Signaling Extensions for Control of Evolving G.709 Optical Transport Networks", RFC 7139, DOI 10.17487/RFC7139, March 2014, <https://www.rfc-editor.org/info/rfc7139>.

[RFC7271] Ryoo, J., Ed., Gray, E., Ed., van Helvoort, H., D'Alessandro, A., Cheung, T., and E. Osborne, "MPLS Transport Profile (MPLS-TP) Linear Protection to Match the Operational Expectations of Synchronous Digital Hierarchy, Optical Transport Network, and Ethernet Transport Network Operators", RFC 7271, DOI 10.17487/RFC7271, June 2014, <https://www.rfc-editor.org/info/rfc7271>.

[RFC7688] Lee, Y., Ed. and G. Bernstein, Ed., "GMPLS OSPF Enhancement for Signal and Network Element Compatibility for Wavelength Switched Optical Networks", RFC 7688, DOI 10.17487/RFC7688, November 2015, <https://www.rfc-editor.org/info/rfc7688>.

[RFC7689] Bernstein, G., Ed., Xu, S., Lee, Y., Ed., Martinelli, G., and H. Harai, "Signaling Extensions for Wavelength Switched Optical Networks", RFC 7689, DOI 10.17487/RFC7689, November 2015, <https://www.rfc-editor.org/info/rfc7689>.

[RFC7792] Zhang, F., Zhang, X., Farrel, A., Gonzalez de Dios, O., and D. Ceccarelli, "RSVP-TE Signaling Extensions in Support of Flexi-Grid Dense Wavelength Division Multiplexing (DWDM) Networks", RFC 7792, DOI 10.17487/RFC7792, March 2016, <https://www.rfc-editor.org/info/rfc7792>.

[RFC8231] Crabbe, E., Minei, I., Medved, J., and R. Varga, "Path Computation Element Communication Protocol (PCEP)

Extensions for Stateful PCE", RFC 8231,
DOI 10.17487/RFC8231, September 2017,
<https://www.rfc-editor.org/info/rfc8231>.

[RFC8234] Ryoo, J., Cheung, T., van Helvoort, H., Busi, I., and G. Wen, "Updates to MPLS Transport Profile (MPLS-TP) Linear Protection in Automatic Protection Switching (APS) Mode", RFC 8234, DOI 10.17487/RFC8234, August 2017, <https://www.rfc-editor.org/info/rfc8234>.

[RFC8281] Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for PCE-Initiated LSP Setup in a Stateful PCE Model", RFC 8281, DOI 10.17487/RFC8281, December 2017, <https://www.rfc-editor.org/info/rfc8281>.

[RFC8345] Clemm, A., Medved, J., Varga, R., Bahadur, N., Ananthakrishnan, H., and X. Liu, "A YANG Data Model for Network Topologies", RFC 8345, DOI 10.17487/RFC8345, March 2018, <https://www.rfc-editor.org/info/rfc8345>.

[RFC8363] Zhang, X., Zheng, H., Casellas, R., Gonzalez de Dios, O., and D. Ceccarelli, "GMPLS OSPF-TE Extensions in Support of Flexi-Grid Dense Wavelength Division Multiplexing (DWDM) Networks", RFC 8363, DOI 10.17487/RFC8363, May 2018, <https://www.rfc-editor.org/info/rfc8363>.

[SPCE-ID] Dugeon, O., Meuric, J., Lee, Y., and D. Ceccarelli, "PCEP Extension for Stateful Inter-Domain Tunnels", Work in Progress, Internet-Draft, draft-ietf-pce-stateful-interdomain-07, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-stateful-interdomain-07>.

[YANG-TE] Saad, T., Gandhi, R., Liu, X., Beeram, V. P., and I. Bryskin, "A YANG Data Model for Traffic Engineering Tunnels, Label Switched Paths and Interfaces", Work in Progress, Internet-Draft, draft-ietf-teas-yang-te-37, 9 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-yang-te-37>.

Acknowledgements

The authors would like to thank Jim Guichard, Area Director of IETF Routing Area; Vishnu Pavan Beeram, Chair of TEAS WG; Jia He and Stewart Bryant, RTGDIR reviewers; Thomas Fossati, Gen-ART reviewer; Yingzhen Qu, OPSDIR reviewer; David Mandelberg, SECDIR reviewer; David Dong, IANA Services Sr. Specialist; and ric Vyncke and Murray Kucherawy, IESG reviewers for their reviews and comments on this document.

Contributors

Xianlong Luo
Huawei Technologies
G1, Huawei Xiliu Beipo Village, Songshan Lake
Dongguan
Guangdong, 523808
China
Email: luoxianlong@huawei.com

Sergio Belotti
Nokia
Email: sergio.belotti@nokia.com

Authors’ Addresses

Haomian Zheng
Huawei Technologies
H1, Huawei Xiliu Beipo Village, Songshan Lake
Dongguan
Guangdong, 523808
China
Email: zhenghaomian@huawei.com

Yi Lin
Huawei Technologies
H1, Huawei Xiliu Beipo Village, Songshan Lake
Dongguan
Guangdong, 523808
China
Email: yi.lin@huawei.com

Yang Zhao
China Mobile
Email: zhaoyangyjy@chinamobile.com

Yunbin Xu
CAICT
Email: xuyunbin@caict.ac.cn

Dieter Beller
Nokia
Email: Dieter.Beller@nokia.com