**Contribution Number: OIF2001.227.2**

**Working Group: Architecture & Signaling Working Groups**

**Title: Inter-domain routing with Shared Risk Groups**

**Date: July 12th , 2001**

**Source:**


Sudheer Dharanikota
Raj Jain
**Nayna Networks**

Curtis Brownmiller
Yong Xue
**WorldCom**

Dimitri Papadimitriou
**Alcatel**

Greg Bernstein
**Ciena**

Riad Hartani
**Caspian Networks Inc.**

Vishal Sharma
**Metanoia**

John Strand
**AT&T**



**ABSTRACT: This document discusses how inter-domain routing using Shared Risk Group (SRG) may be used for computing diverse paths, and also discusses the extensions that we propose for routing (and eventually signaling) protocols. The concepts proposed in this document are useful to provide the requested intelligent control plane for multi-layered networks.**





For additional information contact:
The Optical Internetworking Forum, 39355 California Street,
Suite 307, Fremont, CA 94538
510-608-5990 phone ✥ info@oiforum.com

## 1. Introduction

For many years in the telecommunications industry, the concept of SRLG (Shared Risk Link Group) has been used for computing a path that is disjoint from a set of links sharing the same risk. For this purpose, links sharing the same risk are grouped together to have the same SRLG value. When two links (or more) share the same risk, it means that when one link fails the other(s) can fail simultaneously. Reference [IETF-DIMITRI-SRLG] provides enhancements to the concept of SRLGs thereby streamlining its meaning.

Networks are planned to recover from failures due to a risk (represented by an SRLG) using different mechanisms, which we call capabilities. So if we look at SRLG on a positive note we may want to intentionally use the capabilities supported in the network due to an SRLG. For example one may provide a 1:1 shared link protection (link capability) for many connections using the link that has an SRLG value of X.

A risk sharing, however, is not limited to links, which has been the case until now in a majority of the IETF proposals (e.g., [IETF-KIREETI-OSPF]). In this document, we extend the applicability of SRLGs to path (or connections) included in a *domain*, where we define a *domain* to be a group of resources (nodes and links) that provide similar capabilities and that share the same set of risk(s). For example a domain can be consecutive set of links that has 1:1 link level protection or a set of links that form a ring. Note that in such a scenario (for example in ring topology), a failure will affect all the other resources in the domain. This observation parallels the notion of what SRLG for a link to an SRG (Shared Risk Group) for a domain. One can visualize the similar capabilities of a domain to be the same protection capabilities, the same link encoding type, same multiplexing capability, same resource class and same Traffic-Engineering Metric etc.

The “shared risk concept” can also be viewed as a mechanism to hide or reduce the amount of topology information propagated in a multi-layered network. Consider a multi-layered network with fiber, optical (for instance G.709 OTN), SONET/SDH and router topology in the ascending order of encompassing the previous topology. Here the upper layer (which encompasses the lower layers) is called the client layer and the lower layer is called the server layer. In such a topology a link at the client layer (for example, router level) can mean many nodes and links in the server layer (for example, SONET/SDH, optical and fiber level). Hence to provide diversity at the client layer link level one should consider failures in the server layer topology. Thus, to provide diverse links or paths (sequences of links) at the client layer requires some means of abstracting the diversity at the server layer, so that this abstraction can be used by path computation at the client layer. At present the only way to provide this abstraction of the server layer topology in the client layers is to use SRLG. With the adoption of GMPLS (Generalized Multi-Protocol Label Switching) control plane in the packet and circuit based networks it is now possible to compute diverse paths in multiple layers. The notion of diversity can be abstracted and dynamically computed at many layers. In this document, we concentrate on the risk associated with a sequence of disjoint elements (unlike in case of SRLG). The procedures of doing such a complex task is provided in this document.

The following observations serve as a basis for considering the extension of the “Shared risk” concept to more than just a link:

- The number of nodes or links that are affected by a failure is dependent on the physical topology of the network (or the server layer(s) topology in a multi-layered network).
    - A typical node failure may also represent the failure of set of links, or multiple link failures or SRLGs.
    - On the other hand, a failure of a fiber (or a group of fibers) may result in the failure of multiple logical links, which topologically could be forming a ring or point-to-multipoint mesh network.
- The abstraction of the capability of a domain can be useful in
    - Summarizing (so reducing) the amount of information propagated in the routing protocols,
    - Hiding the topology of the domain for the sake of loose path specification (and hence loose path computation) Computing diverse paths by concatenating the capabilities of the domains.
    - Hiding the topology details of the server layers in a multi-layered network (if needed).
- Sharing risk is opposite to capability of a domain, which is a required parameter for service provisioning by ISPs.
    - Establishing a primary path disjoint from the secondary one at the same layer reduces the chances of losing traffic or dropping traffic for longer time. This can be logically concatenated by the notion of domains and domain capabilities. These domains can belong to a single level to multiple levels (as in multi-layered networks).
    - Such a notion enables more factual based risk assessment and hence helps in achieving risk reduction by improving incremental topological design.

This document is organized as follows:

Section 2 specifies the applicability of the SRG concept aligned with the carrier requirements detailed in Section 3. Then, the definition and the scope of the “risk Domain” concept are proposed in Section 4. The corresponding TE-Routing protocol extensions are detailed in Section 5 and a preliminary version of potential encoding of these extensions are suggested in Section 6. In the appendices we discuss the motivation and usage of this work for computing diversity and risk.

## 2. Applicability

The mechanisms proposed in this draft are applicable to the following operational areas:

- To achieve constraint based path computation in a multi-layered network with integrated control plane and reduction in the amount of TE (Traffic Engineering) parameters.
- To hide the topology in a tiered network (whether control planes overlay or peer-to-peer) with a single or multiple administrators to the domain(s).
- To reduce the amount of TE information propagated by localizing the scope of information propagation and hence distribution of the path computation.
- To propose mechanisms that are applicable to packet and non-packet oriented networks (multi-service networks) in the scope of GMPLS architecture independently of the path provisioning state.

## 3. Carrier requirements

As mentioned in [OIF-CARRIER-REQ] and [IPO-JOHN-IMP], the diversity compromises between two links being used for routing should be defined in terms of Shared Risk Link Groups (SRLGs), a group of links which share some resource, such as a specific sequence of fiber ducts or a specific office. A SRLG is a relationship between the resources that should be characterized by two parameters:

- Type of Compromise: Examples would be shared fiber cable, shared conduit, shared ROW, shared link on an optical ring, shared office - no power sharing, etc.)
    - Support for hierarchical SRLG allocation
    - Support for logical level and physical level diversity
    - Support for computing diverse path computation over multi-layered networks
    - Support for hiding lower-layer capability in the upper layers

Extent of Compromise: For compromised outside plant, this would be the length of the sharing.

## 4. Definitions and scope

### 4.1. Definition of risk domain

Definition: A “risk domain” is a group of arbitrarily connected nodes and links that together can provide certain like-capabilities (such as a chain of dedicated/shared protected links and nodes, or a ring forming nodes and links).

This is advertised in the routing protocols as “risk domain link”, an abstract point-to-multipoint link. It is rather advisable not advertising this as NBMA link to avoid the complexity of the designated router. This solution does not, however, preclude handling of the risk domain concept via a representation as a NBMA link.

Another way to see the risk domain link is as a Forwarding Adjacency (FA – refer to [IETF-KIREETI-FA]) if and only if source and destination are located within the same area and can have a pre-established path between them with the same capabilities in all the links through which this FA is passing through.

This concept of risk domain in parallel to the assumptions made about the MPLS domain or DiffServ domain till now. This differs in the previous definition of the domains in the sense that it is represented in the routing protocols and signaling protocols with domain-related values.

In the current document, we assume a risk domain is part of a routing (OSPF or ISIS) area. From now on, we use the term domain interchangeably with risk domain.

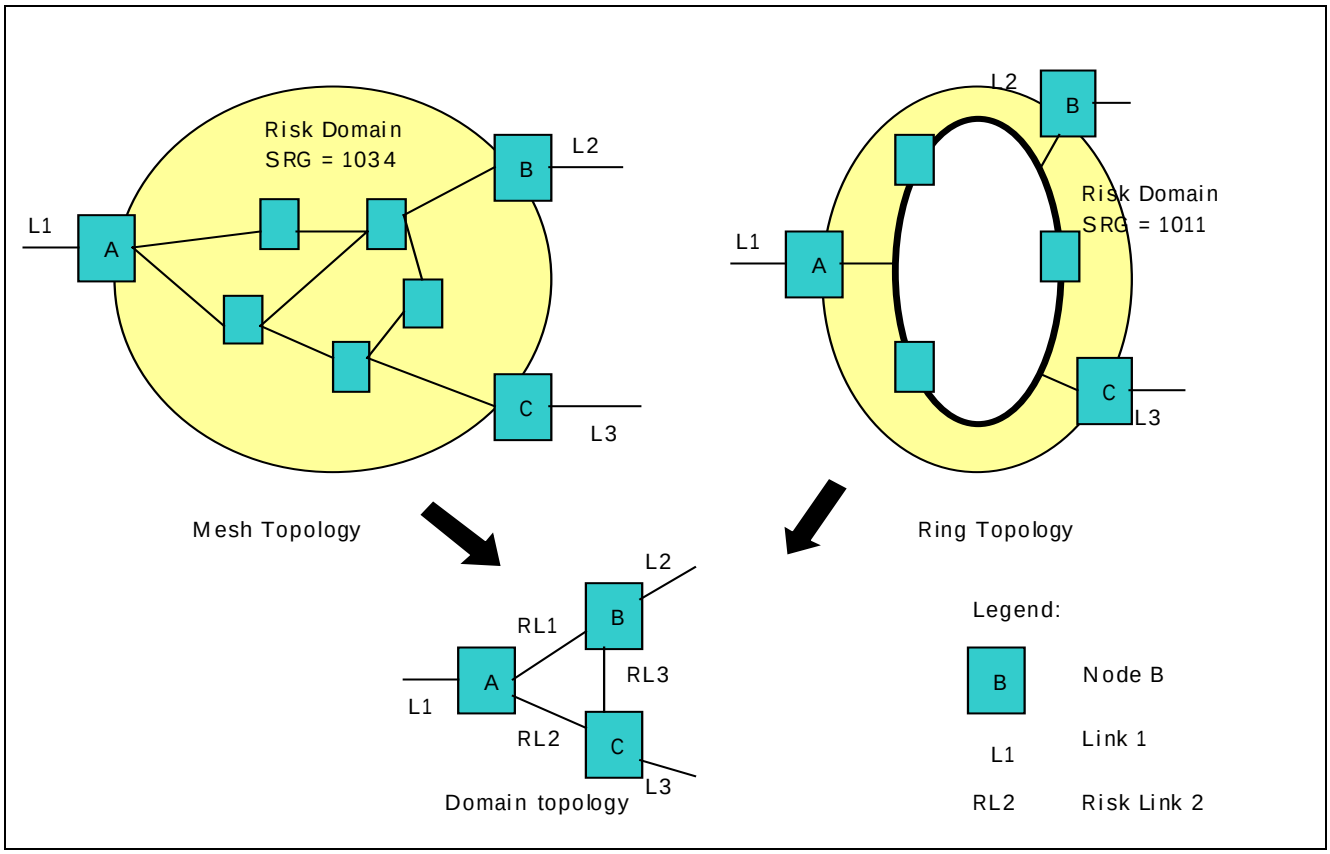



**Figure 1 Risk domain representation of a mesh and a ring topology**

Figure 1, depicts the notion of a risk domain and a risk link representation for both a meshed network and a ring network. More details on the risk domain usage will follow in the rest of the document.

## 4.2. Definition of SRG

Definition: An SRG (a 32 bit integer), as shown in Figure 1, represents the risk domains' capabilities and other parameters, which assist in computing diverse paths through the domain and in assessing the risk associated with the risk domain.

With the observations made in section 1 and the introduction of the concept of a risk domain, we define the notion of a "Shared Risk Group" (SRG) per risk domain.

Note that the SRLGs of this risk domain are a subset of the SRGs. SRLGs address only risks associated with the links (physical and logical) and locations within the risk domain, whereas SRGs contains nodes and other topological information in addition to links. The key difference between an SRLG and an SRG is that an SRLG translates to only one link share risk with respect to server layer topology (even FA and virtual links) while an SRG translates a sequence of SRLGs (including nodes) over the same layer from one source to one or more than one destination located within the same area.

### 4.3. Scope

The following are the goals of this work:

- Diversity:
  - To capture link, node and domain-level diversity with minimal TE information.
  - Summarizable SRG notation, which decreases the complexity of computing disjoint paths.
  - Propose a mechanism that works for both single and multi-layered networks, which use Generalized MPLS distributed control plane. In the first version of the document we consider only intra-AS networks with single layer topology. In the future version we will generalize the mechanism to inter-AS and multi-layered architectures.
- Risk:
  - Assign capabilities to the SRGs such Resource Class, TE Metric, etc.
  - Assign failure probability to the SRGs, which, in turn, enable the “evaluation” of the probabilities corresponding to the risk assessment.
  - Facilitate path computation against a given risk type. This case will be handled in the future versions of the document.
- Other:
  - SRLG is currently a flat 32 bit number in a given autonomous system. The notion of SRG will help in localization of SRLG allocation and hence helps in summarization.
  - Deployment (i.e., operational aspects) of a SRLG or SRG capable network.

## 5. Protocol requirements

The following are the protocol related requirements (mainly related to traffic-engineering routing protocol extensions), which are elaborated in this document:

- Configuration:
  - To enable the SRG mechanism the following configuration parameters may be required.
    - Domain boundary configuration
    - Hierarchical SRLG configuration
    - Domain to SRG allocation
    - Per SRG capabilities and risk factor allocation
    - Preferred path allocation parameters
    - Other link related parameters that can be extended to SRG such as TE Metric (additive metric), Resource Class (ON/OFF), etc.
- Encoding (refer to [IETF-DIMITRI-SRLG]):
  - Logical and physical structure: A logical and physical encoding of SRLGs should be proposed to reduce the number of SRLGs with scalability in mind. This also helps in hiding the actual underlying network topology in many cases, and allows for loose path computation. Refer to [IETF-DIMITRI-SRLG] for more information on this subject. In addition an encoding mechanism should be devised to derive the capabilities of a domain (which is represented by an SRG).
- Capability assignment
  - Domain, node, and link capability: Domain capability such as transport network level diversity (node, link, SRLG, path) provided by the domain can be associated with the SRG. This helps in deciding the logical and physical topologies of choice for the path. Other

capabilities such as TE Metric and Resource Class can also be considered.
    - Risk assessment parameters: Risks can be associated with both the SRGs to assess the possible risk associated with a path.
    - Preferential route selection: By associating weights to the SRGs, one can make the path selection algorithms choose certain SRG path(s).
- Routing protocol extensions to propagate them (distinction should be done between inter and intra-domain routing)
    - Given the domain-level decomposition of the physical topology of the optical network, the link semantics should be extended to accommodate the inter-domain links. Moreover, this concept helps in constructing logical- topologies at the domain-level abstraction, which in turn can be used in the SRG summarization and loose-path computation.
    - Propagate these additional links using the IGP routing protocols for intra- and inter-area routing purposes [probably that the “domain” is something that could be mapped to an IGP area so that inter-area routing would be more easy to achieve].
    - To reduce the amount of the flooded information and hence lightpath route computation complexity, the flooding scope of the information propagation is extended to accommodate domain-level.
    - Propagate the capability, risk assessment, and preferential route selection parameters per SRG.
- CSPF to use this path
    - Extend constraint-based path computation to accommodate the above extensions.

In the following sections we will elaborate each of these topics individually.

## 6. Extensions

### 6.1. Configuration

The configuration parameters considered are the following:

Domain boundary configuration: This is the configuration of domain to provide a boundary for summarization or hiding the capability information, as will be elaborated in the next few sections. This is in parallel to the concept of an area boundary in the existing IGPs.

Hierarchical SRLG configuration: The hierarchical SRLG configuration is provided by the SRLG encoding itself. In [IETF-DIMITRI-SRLG], the SRLG are encoded as a Resource Location and a Resource Identifier. The latter includes a list of type – SRLG identifier fields. This concept helps in localizing SRLG allocation, hiding the server layer link level topology and in reducing amount of server layer TE information propagation.

Domain to SRG allocation: Grouping of nodes and links that provide certain capability will have an SRG allocated to it. The SRG value can be a flat 32-bit number or can represent some of the domain capabilities. The SRG encoding will be discussed in the future versions of the document. The node ID from which the point-to-multipoint virtual link starts identifies the SRG allocation. This means that the root of the virtual point-to-multipoint link defines the SRG allocation.

Per SRG capability allocation: The capabilities of the domain such as protection and restoration can be assigned per domain. Please note that the likeness of these capabilities across the domain is a requirement for a link or a node to be part of the domain. Other link related parameters that can be extended to SRG such as TE Metric (additive metric), Resource Class (ON/OFF), etc could be also allocated per SRG.

Capability to risk factor parameters: Risk associate with a domain depends on the protection and restoration mechanisms inherent to the domain and that can be achieved through the capabilities of the domain. Since the risk domain belongs to a single operator, we can assign these parameters per mechanism per domain. This can be assigned per type of failure per SRG.

Preferred path allocation parameters: This is the weight associated to the SRG. This weight can be assigned statically configured once at the initial stage or dynamically determined since it can be defined as additive metric whose individual values are the link TE metrics.

## 6.2. Encoding

A hierarchical encoding mechanism is the key to the summarization process of the SRLGs of a given server layer link. This encoding can be performed on the physical and logical resources as elaborated in [IETF-DIMITRI-SRLG]. SRG on the other hand represents a both the nodes and the links, which can take the same hierarchical encoding as in SRLG, but in the current version of the document we assume it to be a 32-bit flat number with the capabilities being specified as TLVs.

## 6.3. Capability assignment

Refer to [IETF-GMPLS-ARCH] to get the complete list of the link capabilities that can be propagated. Here we envision at least the protection related capabilities can be extended to the domain level, in addition we have few more parameters, which assist in the risk assessment, as discussed below.

- Capability assignment (will be elaborated further in the later versions of the document): This is assigned to each of the SRG, which is propagated in the opaque LSA in the routing protocols and assists in the diverse path computation and risk assessment.
  - o Domain capability: Extensions similar to link capabilities as noted by [IETF-GMPLS-ARCH]. These include shared or dedicated protection capabilities of the links in the domain.
  - o Node capability: Extensions similar to link capabilities as noted by [IETF-GMPLS-ARCH].
  - o Link capability: Extensions as discussed by [IETF-GMPLS-ARCH].
  - o Conditional probability for risk: This provides the operator assigned risk factor for a given SRG. This can be carried per type of failure.

## 6.4. Routing protocol extensions

### 6.4.1. Propagation of a domain link

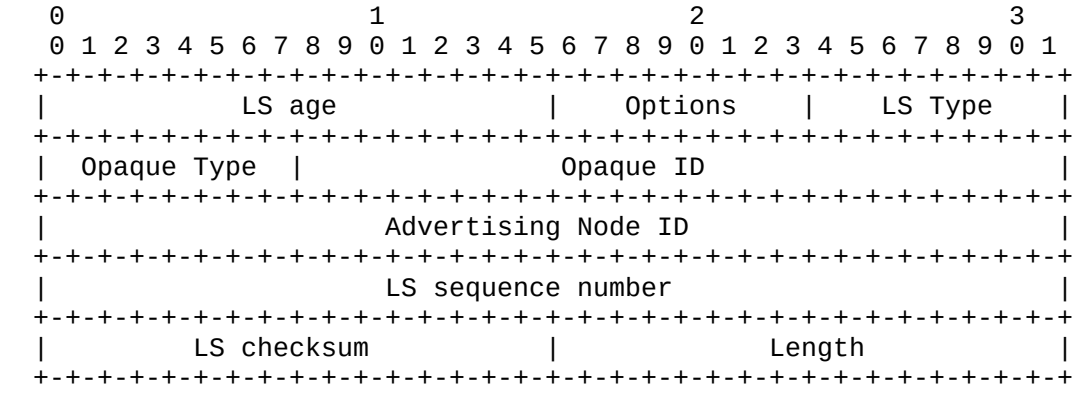
A network administrator groups a set of links and nodes of similar capabilities into a domain and assigns an SRG to the domain. A physical topology can have overlapping domains if links and/or nodes participating in the domain notion support multiple capabilities.

A domain is represented as an abstract point-to-multipoint link for the sake of representation, and for path computation in the routing protocols. As discussed before, this can represent any type of physical topology represented under the abstract notion of domain.

The exact semantics of the domain link opaque LSA (defined as an opaque LSA of Type 10) is presented in below. The scope of this opaque LSA can be link, area or AS specific.

#### 6.4.1.1. Opaque LSA Header

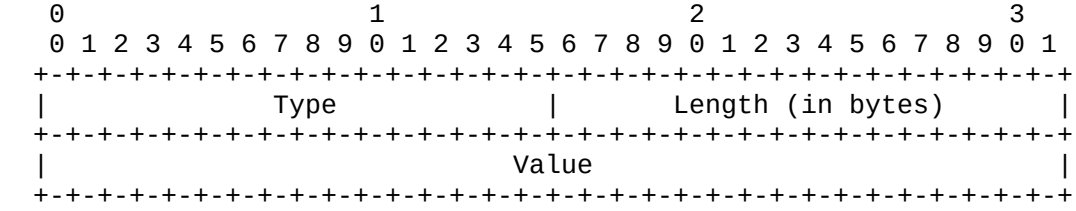
The Opaque Type-specific ID (i.e. Opaque ID) is a 24-bit sub-field sub-divided in a reserved sub-field (8 MSB) and a Source specific sub-field (16 LSB).




where LS Type value = 9, 10 or 11

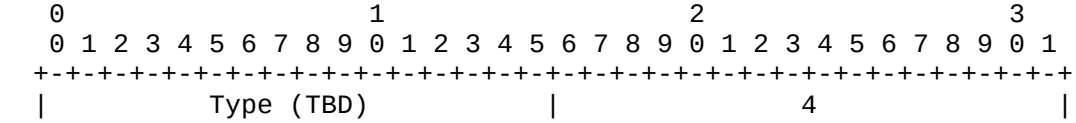
#### 6.4.1.2. Opaque LSA Payload

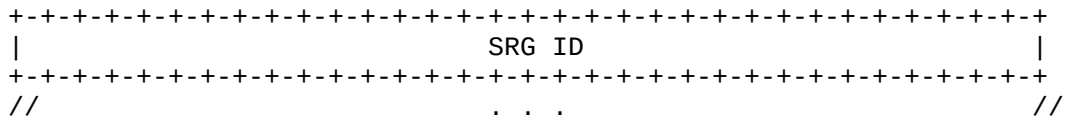
The Opaque LSA payload consists of one or more nested Type/Length/Value (TLV) structures. The format of the Opaque LSA TLV structure is defined as:




#### 6.4.1.3. SRG TLV

The SRG TLV includes the SRG ID (32 bits identifier).






Note that the TLVs other than the risk factor TLV is available in the IGP extensions as available now in the IETF drafts such as [IETF-GMPLS-OSPF], [IETF-GMPLS-ISIS]. In the future versions of this document we will elaborate on the other required TLVs specific to this document. Note that even the protection related TLVs would be specified per SRG (unlike per link in the case of regular networks).

6.4.2. Path computation

Path computation becomes very rich with this concept with the concept of the loose nodes and links being represented by the risk domain concept. A dynamic path computation mechanism can use the concatenation of the domains to compute the loose explicit path, leaving the expansion of the loose segments to the domain border nodes.

First we start with one domain “computation” and then expand it. Here below some guidelines:

- Pruning of SRG that do not belong to the same resource class
- Exclude all the resources already selected for other LSP using that SRG for the same VPN ID, same source node ID, etc.
- Exclude all the resources already selected for the same restoration group of LSP (case of edge-to-edge protection)
- Take the explicit inclusive and exclusive requirements into consideration

## 7. Conclusions

In this document we presented the concept of a risk domain abstracting nodes and links with like-capabilities. This notion can be used very effectively for inter-domain routing by reducing the amount of TE information to be carried. We proposed a mechanism called SRG to capture this information and assist in diverse path computation and risk assessment in single and multi-layered networks.

## 8. References

[IETF-KIREETI-TE] K. Kompella et al., “OSPF Extensions in Support of Generalized MPLS,” draft-kompella-ospf-gmpls-extensions-01.txt, IETF draft (work in progress).

[IETF-DIMITRI-SRLG] D. Papadimitriou et al., “Inference of Shared Risk Link Groups,” draft-many-inference-srlg-00.txt, IETF draft (work in progress).

[IETF-JOHN-IMP] J. Strand et al., “Impairments and other constraints on optical Layer routing,” draft-ietf-impairments-00.txt, IETF draft (work in progress).

[IETF-SRLG-PROTO-EXT] S. Dharanikota et al., “Inter domain routing with SRGs – Protocol extensions,” draft-many-ccamp-srg-00.txt, IETF draft (work in progress).

[IETF-GMPLS-ARCH] E. Mannie et al., “Generalized Multi-Protocol Label Switching (GMPLS) Architecture,” draft-many-gmpls-architecture-00.txt, IETF draft (work in progress).

[OIF-CARRIER-REQ] J. Strand et al., “Carrier Optical Services Framework and Associated Requirements for UNI,” OIF2000.155, OIF carrier group document.

[IETF-KIREETI-FA] K. Kompella, Y. Rekhter, “LSP Hierarchy with MPLS TE,” draft-ietf-mpls-lsp-hierarchy-02.txt, IETF Working group document.

---

[IETF-GMPLS-OSPF] [IETF-OPT-OSPF] Kireeti Kompella et al., “OSPF Extensions in Support of Generalized MPLS,” draft-kompella-ospf-gmpls-extensions-01.txt, IETF working group draft.

[IETF-GMPLS-ISIS] Kireeti Kompella et al., “IS-IS Extensions in Support of Generalized MPLS,” draft-ietf-isis-gmpls-extensions-02.txt, IETF working group draft.

## Appendix A: Diversity and SRG

A brief introduction is provided to the need for diversity to set the stage for the rest of the discussion. Traffic engineering in IP (Internet Protocol) networks is achieved using MPLS technology as an overlay on the IP networks. The success of the MPLS TE concept has lead to its application in the optical domain as well. The “pinned” or connection-oriented nature of LSPs reduces the capability of IP traffic to recover automatically from failures in the data path. To achieve path resiliency, therefore, diverse paths must be established between the source and destination MPLS nodes through the use of explicit routing (loose or strict). By introducing the connection-orientedness (LSPs) in the IP technology, we loose the automatic hop-by-hop recovery of the data paths in case of failures. Hence, diverse paths are established between the source and destination MPLS nodes for achieving path resiliency.

The diversity requirements of transport networks have some differences with those of router (Layer 3 and Layer 2 switching) networks. They are mainly:

- Transport networks provide elaborate protection and restoration mechanisms,
- Transport topologies are not always structured in mesh topologies (agreed but in fact an OCh on top of an OMS SPRing for instance appears as a point-to-point connection at the OCh level so that Ring topology does not necessarily mean ringed connection, as assumed by the router networks, and
- Transport-level protection and restoration mechanisms are not considered in the diverse path computation by the MPLS technology (at least till now) dynamic path computation constructs.

Diversity in the router world is achieved as follows:

- Request: Given the (physical and logical) topology, link capabilities, and constraints to calculate 1 to N diverse path between two points in the network.
- Input:
  - Topology:
    - Physical topology is always meshed and multiplexed (fiber, cables, segments etc.).

        - Areas and autonomous systems achieve logical topology.
    - Capability:
        - Only link capabilities are propagated.
    - Constraints:
        - Inclusive requirements: Such as a preferred links (color).
        - Exclusive requirements: Such as avoiding a node (node-level diversity, link-level diversity).
        - Limiting requirements: Such as bandwidth.
- Output:
    - Paths available or not.
    - If paths are available then provide the strict or loose paths.
        - Strict paths can be provided if the physical topology is known between the source and destination.
        - Loose paths are provided if the end-to-end physical topology is not known.

Diversity in the router + transport world may be achieved as follows:

- Request: Given the (physical and logical) topology, link capabilities, **domain capabilities** and constraints to calculate 1 to N diverse paths between two points in the network.
- Input:
    - Topology:
        - Physical topology is flexible **(Rings, Meshes, Ring-Mesh inter connected)**.
        - **Domains** (or islands) are used to achieve logical topology.
    - Capability:
        - Both link (or span) and domain capabilities need to be propagated.
    - Constraints:
        - Inclusive requirements: Such as preferred links and preferred link, node and **domain** capabilities.
        - Exclusive requirements: Such as avoiding a link, node or **domain**.
        - Limiting requirements: Such as bandwidth.
- Output:
    - Paths available or not.
    - If paths are available then provide the strict or loose paths.
        - Strict paths can be provided if the physical topology is known between the source and destination – not necessarily I can provide an strict routed SDH L-LSP while being aware of the lambda topology but not on the fiber or duct topology.
        - Loose paths are provided if the end-to-end physical topology is not known or cannot be interpreted such as in ring topologies or would like to leave to the risk domain to decide (for local optimization or due to lack of information or to reduce TE information flooding) – not necessarily for instance inter-area routing can be loose even if the local source area physical topology is known.

Discussion:

The following observations can be made between the diverse path setup mechanisms in the router world and in the transport world:

- Sharing risk is not only a property of the links, but it can be extended to nodes and domains. Thus, an SRG can be associated with the links, nodes, and even domains.
- Also, for example, domain capabilities can be associated with the domain SRG to achieve inclusive constraints. For example, a BLSR ring can have an SRG with ring capabilities associated with it.

As a precursor to achieving such constraints we propose to extend the SRLG notion to represent logical topologies. By assigning SRGs in a hierarchical fashion (to a region, a zone/domain and a node), we can capture the capabilities, and risks, associated with them. An extensive discussion on this subject is provided in [IETF-DIMITRI-SRLG].

Considering the above practical knowledge of real world scenarios, it is essential (to reduce the computation time) to reduce the number of SRLGs by means of some encoding. We observe that the amount of configuration can also be reduced (for example, from 100s of SRLGs on a Trans-Atlantic link). This poses the following requirements:

- Need a mechanism to encode (and hence summarizable) SRLG to group represent a link or node or domain wide individual SRGs.
- Need to modify the path computation algorithms (such as CSPF) for accommodating the new encoding scheme.
- Need to enhance the path computation mechanisms to work with the logical topologies (or domains).
- Need to propagate the logical topologies (or domains) via the routing protocols.

## Appendix B: Risk assessment and SRG

Risk (the complementary of availability) assessment is defined as the evaluation of the potential risk associated with the inclusion of a given resource (this resource belongs to a given resource type located within a given logical structure such as a geographical location) in a given path.

A brief discussion for the motivation of the risk assessment capabilities of SRLG is provided here. Consider the following example, where the client device makes the following requests to the optical network:

- Request (either through signaling protocols or using an SLA) for a persistent connection with 99.999 % (widely known 5 9s) of availability or equally a down time less than X minutes per year.
- Request a high-protection for a portion of the traffic (at the expense of paying a higher charge) compared to other low-priority traffic.

Such requirements will be translated into constraints in path computation. Such constraints can be grouped into path selection constraints and path characterization constraints.

- Path selection constraints:
    - These typically dictate which physical path should be taken to achieve the client’s availability requirements. These requirements are typically the logical and physical diversity.
- Path characterization constraints:

- Path characterization requirements typically dictate the protection mechanisms as requested by the client. This can be achieved in the form of optical rings, meshed protection mechanisms, etc. These constraints can be used in using the link, node, and domain capabilities as discussed in the previous section on diversity.

The components that need formalization in this example are:

- Step 1. Specification of the user requirements (such as the example above), which need to be translated into “network constraints”.
- Step 2. Configuring the network in a way that helps in assessing its features, such as the availability
- Step 3. Propagating the information thus configured.
- Step 4. Using information thus propagated in path computation.

Step 1 of specifying the requirements is not in the scope of this document. Steps 2 - 4 are discussed below.

Discussion:

A convenient way to achieve risk assessment is by associating a conditional risk value with each of the SRLGs and SRGs, as discussed in [IETF-DIMITRI-SRLG]. Also, by associating a weight factor with the SRG, we can increase the choice of selecting specific SRGs. This calls for configuring:

- A Risk factor per SRG
- A Weight factor per SRG

In addition to the SRG capabilities, discussed before, the above values can also be propagated via routing protocols. These routing requirements are discussed in the following section.

With the help of the above two configuration parameters, the use of typical CSPF algorithms to compute a path can be extended to assess the risk associated with the path. For example, if a path traverses SRGs 1, 3, 5, then one may infer that the risk associated with this path is (Risk 1 x Risk 3 x Risk 5).