Network Working Group
IETF Internet Draft
Proposed Status: Informational
Expires: January 2004

Adrian Farrel
Olddog Consulting

Jean-Philippe Vasseur
Cisco Systems, Inc.

Arthi Ayyangar
Juniper Networks

July 2004

draft-farrel-ccamp-inter-domain-framework-01.txt

A Framework for Inter-Domain MPLS Traffic Engineering

Status of this Memo

Copyright Notice

Abstract

This document provides a framework for establishing and controlling Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Label Switched Paths (LSPs) in multi-domain networks.

For the purposes of this document, a domain is considered to be any collection of network elements within a common sphere of address management or path computational responsibility. Examples of such domains include IGP areas and Autonomous Systems.

1. Introduction

The Traffic Engineering Working Group has developed requirements for inter-area and inter-AS MPLS Traffic Engineering in [INTER-AREA] and [INTER-AS].

Various proposals have subsequently been made to address some or all of these requirements through extensions to the RSVP-TE and IGP (ISIS, OSPF) protocols and procedures.

This document introduces the techniques for establishing TE LSPs across multiple domains. The functional components of these techniques are separated into the mechanisms for discovering reachability and TE information, for computing the paths of LSPs, and for signaling the LSPs. Note that the aim is this document is not to detail each of those techniques which are covered in separate documents, but rather to propose a framework for inter-domain MPLS Traffic Engineering.

For the purposes of this document, a domain is considered to be any collection of network elements within a common sphere of address management or path computational responsibility. Examples of such domains include IGP areas and Autonomous Systems. However, domains of computational responsibility may also exist as sub-domains of areas or ASs. Wholly or partially overlapping domains are not within the scope of this document.

1.1. Nested Domains

Nested domains are outside the scope of this document. It may be that some domains that are nested administratively or for the purposes of address space management can be considered as adjacent domains for the purposes of this document, however the fact that the domains are nested is then immaterial.

In the context of MPLS TE, domain A is considered to be nested within domain B if domain A is wholly contained in Domain B, and domain B is fully or partially aware of the TE characteristics and topology of domain A.

For further consideration of nested domains see [MRN]

1.2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Signaling Options

Three distinct options for signaling TE LSPs across multiple domains are identified. The choice of which options to use may be influenced by the path computation technique used (see section 3), although some path computation may apply to multiple TE LSP types. The choice may further depend on the application to which the TE LSPs are put and the nature, topology and switching capabilities of the network.

A comparison of the usages of the different signaling options is beyond the scope of this document and should be the subject of a separate applicability statement.

2.1. LSP Nesting

Forwarding Adjacencies (FAs) are introduced and explained in detail in [HIER]. No further description is necessary in this document.

FAs can be used in support of inter-domain TE LSPs. In particular, an FA may be used to achieve connectivity between any pair of LSRs within a domain. The ingress and egress of the FA LSP could be the edge nodes of the domain in which case connectivity is achieved across the entire domain, or they could be any other pair of LSRs in the domain.

The technique of carrying one TE LSP within another is termed LSP nesting. An FA may provide a TE LSP tunnel to transport (i.e. nest) multiple TE LSPs along a common part of their paths. Alternatively, a TE LSP may carry (i.e. nest) a single LSP in a one-to-one mapping.

The signaling trigger for the establishment of an FA LSP may be the receipt of a signaling request for the TE LSP that it will carry, or may be a management action to 'pre-engineer' a domain to be crossed by TE LSPs that would be used as FAs by the traffic that has to traverse the domain. Furthermore, the mapping (inheritance rules) between attributes of the nested and FA LSPs (including bandwidth) may be statically pre-configured or, for on-demand FA LSPs, may be dynamic according to the properties of the nested LSPs.

Note that a hierarchical LSP may be constructed to span multiple domains or parts of domains, however how or whether such an LSP could be advertised as an FA that spans domains is open for study. The end points of a hierarchical LSP are not necessarily on domain boundaries, so nesting is not limited to domain boundaries.

Note also that the IGP/EGP routing topology is maintained unaffected by the LSP connectivity and TE links introduced by FA LSPs. That is, the routing protocols do not exchange messages over the FA LSPs, and such LSPs do not create adjacencies between routers. During this operation the SENDER_TEMPLATE and SESSION objects remain unchanged along the entire length of the LSP.

2.2. Contiguous LSP

A single contiguous LSP is established from ingress to egress in a single signaling exchange. No further LSPs are required be established to support this LSP. Signaling occurs between adjacent neighbors only (no tunneling), and hop-by-hop signaling is used.

2.3. LSP Stitching

In the LSP stitching model separate LSPs (referred to as a TE LSP segments) are established and are "stitched" together in the data plane so that a single end-to-end label switched path is achieved. The distinction is that the component LSP segments are signaled as distinct TE LSPs in the control plane. Each signaled TE LSP segment

has a different source and destination.

LSP stitching can be used in support of inter-domain TE LSPs. In particular, an LSP segment may be used to achieve connectivity between any pair of LSRs within a domain. The ingress and egress of the LSP segment could be the edge nodes of the domain in which case connectivity is achieved across the entire domain, or they could be any other pair of LSRs in the domain.

The signaling trigger for the establishment of a TE LSP segment may be the establishment of the previous TE LSP segment, the receipt of setup request for TE LSP that it plans to stitch to a local TE LSP segment, or may be a management action.

2.4. Hybrid Methods

There is nothing to prevent the mixture of signaling methods described above when establishing a single, end-to-end, inter-domain TE LSP. It may be desirable in this case for the choice of the various methods to be indicated along the path perhaps through the RRO.

If there is a desire to restrict which methods are used, this MUST be signaled as described in the next section.

2.5. Control of Downstream Choice of Signaling Method

Notwithstanding the previous section, an ingress LSR MAY wish to restrict the signaling methods applied to a particular LSP at domain boundaries across the network. Such control, where it is required, may be achieved by the definition of appropriate new flags in the SESSION-ATTRIBUTE object or the Attributes Flags TLV of the LSP_ATTRIBUTES object [ATTRIB]. Before defining a mechanism to provide this level of control, the functional requirement to control the way in which the network delivers a service must be established and due consideration must be given to the impact on interoperability.

3. Path Computation Techniques

The discussion of path computation techniques within this document is limited significantly to the determination of where computation may take place and what components of the full path may be determined.

The techniques used are closely tied to the signaling methodologies described in the previous section in that certain computation techniques may require the use of particular signaling approaches and vice versa.

Any discussion of the appropriateness of a particular path computation technique in any given circumstance is beyond the scope of this document and should be described in a separate applicability statement.

3.1. Management Configuration

Path computation may be performed by offline tools or by a network planner. The resultant path may be supplied to the ingress LSR as part of the TE LSP or service request, and encoded by the ingress LSR as an ERO on the Path message that is sent out.

There is no reason why the path provided by the operator should not span multiple domains if the relevant information is available to the planner or the offline tool. The definition of what information is needed to perform this operation and how that information is gathered, is outside the scope of this document.

3.2. Head End Computation

The head end, or ingress, LSR may assume responsibility for path computation when the operator supplies part or none of the explicit path. The operator MUST, in any case, supply at least the destination address (egress) of the LSP.

3.2.1. Multi-Domain Visibility Computation

If the ingress has sufficient visibility of the topology and TE information for all of the domains across which it will route the LSP to its destination then it may compute and provide the entire path. The quality of this path is best if the ingress has full visibility into all relevant domains rather than just sufficient visibility to provide some path to the destination.

Extreme caution must be exercised in consideration of the distribution of the requisite TE information. See section 4.

3.2.2. Partial Visibility Computation

It may be that the ingress does not have full visibility of the topology of all domains, but does have information about the connectedness of the domains and the TE resource availability across the domains. In this case, the ingress is not able to provide a fully specified strict explicit path from ingress to egress. However, the ingress can supply an explicit path that comprises:
- explicit hops from ingress to the local domain boundary
- loose hops representing the domain entry points across the network
- a loose hop identifying the egress.

Alternatively, the explicit path may be expressed as:
- explicit hops from ingress to the local domain boundary
- strict hops giving abstract nodes representing each domain in turn
- a loose hop identifying the egress.

These two explicit path formats may be mixed.

This form of explicit path relies on some further computation technique being applied at the domain boundaries. See section 3.3.

As with the multi-domain visibility option, extreme caution must be exercised in consideration of the distribution of the requisite TE information. See section 4.

3.2.3. Local Domain Visibility Computation

A final possibility for ingress-based computation is that the ingress LSR has visibility only within its own domain, and connectivity information only as far as determining one or more domain exit points that may be suitable for carrying the LSP to its egress.

In this case the ingress builds an explicit path that comprises just:
- explicit hops from ingress to the local domain boundary
- a loose hop identifying the egress.

3.3. Domain Boundary Computation

If the partial explicit path methods described in sections 3.2.2 or 3.2.3 are applied then the LSR at each domain boundary is responsible for ensuring that there is sufficient path information added to the Path message to carry it at least to the next domain boundary (that is, out of the new domain).

If the LSR at the domain boundary has full visibility to the egress then it can supply the entire explicit path. Note however, that the ERO processing rules of [RFC3209] state that it SHOULD only update the ERO as far as the next specified hop (that is, the next domain boundary if one was supplied in the original ERO) and, of course, MUST NOT insert ERO subobjects immediately before a strict hop.

If the LSR at the domain boundary has only partial visibility (using the definitions of section 3.2.2) it will fill in the path as far as the next domain boundary, and will supply further domain/domain boundary information if not already present in the ERO.

If the LSR at the domain boundary has only local visibility into the immediate domain it will simply add information to the ERO to carry the Path message as far as the next domain boundary.

3.4. Path Computation Element

The computation techniques in sections 3.2 and 3.3 rely on topology and TE information being distributed to the ingress LSR and those LSRs at domain boundaries. These LSRs are responsible for computing paths. Note that there may be scaling concerns with distributing the required information - see section 4.

An alternative technique places the responsibility for path computation with a Path Computation Element (PCE). There may be either a centralized PCE, or multiple PCEs (each having a local visibility and collaborating in a distributed fashion to compute an end to end path) across the entire network and even within any one domain. The PCE may collect topology and TE information from the same sources as would be used by LSRs in the paragraph, or though other means.

Each LSR called upon to perform path computation (and even the offline management tools described in section 3.1) may abdicate the task to a PCE of its choice. The selection of PCE(s) may be driven by static configuration or the dynamic discovery by means of IGP or BGP extensions.

3.4.1. Multi-Domain Visibility Computation

A PCE may have full visibility, perhaps through connectivity to multiple domains. In this case it is able to supply a full explicit path as in section 3.2.1.

3.4.2. Path Computation Use of PCE When Preserving Confidentiality

Note that although a centralized PCE or multiple collaborative PCEs may have full visibility into one or more domains, it may be desirable (e.g to preserve confidentiality) that the full path is not provided to the ingress LSR. Instead, a partial path is supplied (as in section 3.2.2 or 3.2.3) and the LSRs at each domain boundary are required to make further requests for each successive segment of the path.

In this way an end-to-end path may be computed using the full network capabilities, but confidentiality between domains may be preserved. Optionally, the PCE(s) may compute the entire path at the first request and hold it in storage for subsequent requests, or it may recompute the best path on each request or at regular intervals.

It may be the case that the centralized PCE or the collaboration between PCEs may define a trust relationship greater than that normally operational between domains.

3.4.3. Per-Domain Computation Servers

A third way that PCEs may be used is simply to have one (or more) per domain. Each LSR within a domain that wishes to derive a path across the domain may consult its local PCE.

This mechanism could be used for all path computations within the domain, or specifically limited to computations for LSPs that will leave the domain where external connectivity information can then be restricted to just the PCE.

3.5. Optimal Path Computation

An optimal route might be defined as the route that would be computed in the absence of domain boundaries. It is easy to construct examples that show that partitioning a network into domains, and the resulting loss or aggregation of routing information may lead to the computation of routes that are other than optimal. It is impossible to guarantee optimal routing in the presence of aggregation / abstraction / summarization of routing information.

It is beyond the scope of this document to define what is an optimum path for an inter-domain TE LSP. This debate is abdicated in favor of requirements documents and applicability statements. Note, however, that the meaning of certain computation metrics may differ between domains (see section 5.6).

4. Distributing Reachability and TE Information

The path computation techniques described in the previous section make certain demands upon the distribution of reachability information and the TE capabilities of nodes and links within domains as well as the TE connectivity across domains.

Currently, TE information is distributed within domains by additions to IGPs [RFC3630], [RFC3784].

In cases where two domains are interconnected by one or more links (that is, the domain boundary falls on a link rather than on a node), there SHOULD be a mechanism to distribute the TE information associated with the links to the corresponding domains. This would facilitate better path computation and reduce TE-related crankbacks on these links.

Where a domain is a subset of an IGP area, filtering of TE information may be applied at the domain boundary. This filtering may be one way, or two way.

Where information needs to reach a PCE that spans multiple domains, the PCE may snoop on the IGP traffic in each domain, or play an active part as an IGP-capable node in each domain. The PCE might also receive TEDB updates from a proxy within the domain.

It could be possible that an LSR that performs path computation (for example, and ingress LSR) obtains the topology and TE information of not just its own domain, but other domains as well. This information may be subject to filtering applied by the advertising domain (for example, the information may be limited to FAs across other domains, or the information may be aggregated or abstracted).

Where any cross-domain reachability and TE information needs to be advertised, consideration must be given to TE extensions to BGP, and how these may be fed to the IGPs. Techniques for inter-domain TE aggregation are also for further study. However, it must be noted that any extensions that cause a significant increase in the amount of processing (such as aggregation computation) at domain boundaries, or a significant increase in the amount of information flooded (such as detailed TE information) need to be treated with extreme caution and compared carefully with the scaling requirements expressed in [INTER-AREA] and [INTER-AS].

5. Comments on Advanced Functions

This section provides some non-definitive comments on the constraints placed on advanced MPLS TE functions by inter-domain MPLS. It does not attempt to state the implications of using one inter-domain technique or another. Such material is deferred to appropriate applicability statements where statements about the capabilities of existing or future signaling, routing and computation techniques to deliver the functions listed should be made.

5.1. LSP Re-Optimization

Re-optimization is the process of moving a TE LSP from one path to another, more preferable path (where no attempt is made in this document to define 'preferable' as no attempt was made to define 'optimal'). Make-before-break techniques are usually applied to ensure that traffic is disrupted as little as possible. The Shared Explicit style is usually used to avoid double booking of network resources.

Re-optimization may be available within a single domain. Alternatively, re-optimization may involve a change in route across several domains or might involve a choice of different transit domains.

Re-optimization requires that all or part of the path of the LSP be re-computed. The techniques used may be selected as described in section 3, and this will influence whether the whole or part of the path is re-optimized.

The trigger for path computation and re-optimization may be an operator request, a timer, or information about a change in availability of network resources. This trigger MUST be applied to the point in the network that requests re-computation and controls re-optimization and may require additional signaling.

Note also that where multiple diverse paths are applied end-to-end (i.e. not simply within protection domains - see section 5.5) the point of calculation for re-optimization (whether it is PCE, ingress, or domain entry point) needs to know all such paths before attempting re-optimization of any one path.

5.2. LSP Setup Failure

When an inter-domain LSP setup fails in some domain other than the first, various options are available for reporting and retrying the LSP.

In the first instance, a retry may be attempted within the domain that contains the failure. That retry may be attempted by nodes wholly within the domain, or the failure may be referred back to the LSR at the domain boundary.

If the failure cannot be bypassed within the domain where the failure occurred (perhaps there is no suitable alternate route, perhaps rerouting is not allowed by domain policy, or perhaps the Path message specifically bans such action), the error MUST be reported back to the previous or head-end domain.

Subsequent repair attempts may be made by domains further upstream, but will only be properly effective if sufficient information about the failure and other failed repair attempts is also passed back upstream [CRANKBACK]. Note that there is a tension between this requirement and that of confidentiality although crankback aggregation may be applicable at domain boundaries.

Further attempts to signal the failed LSP may apply the information about the failures as constraints to path computation, or may signal them as specific path exclusions [EXCLUDE].

When requested by signaling, the failure may also be systematically reported to the head-end LSR.

5.3. LSP Repair

An LSP that fails after it has been established may be repaired dynamically by re-routing. The behavior in this case is either like that for re-optimization, or for handling setup failures (see previous two sections).

Fast Reroute may also be used (see below).

5.4. Fast Reroute

MPLS Traffic Engineering Fast Reroute ([FRR]) defines local protection schemes intended to provide fast recovery (in 10s of msecs) of fast-reroutable TE LSPs upon link/SRLG/Node failure. A backup TE LSP is configured and signaled at each hop, and activated upon detecting or being informed of a network element failure. The node immediately upstream of the failure (called the PLR (Point of Local Repair)) reroutes the set of protected TE LSPs onto the appropriate backup tunnel(s) and around the failed resource.

In the context of inter-domain TE, there are several different failure scenarios that must be analyzed. Provision of suitable solutions may be further complicated by the fact that [FRR] specifies two distinct modes of operation referred to as the "one to one mode" and the "facility back-up mode".

The failure scenarios specific to inter-domain TE are as follows:

- Failure of a domain edge node that is present in both domains. There are two sub-cases:
  - The PLR and the MP are in the same domain
  - The PLR and the MP are in different domains.
- Failure of a domain edge node that is only present in one of the domains.
- Failure of an inter-domain link.

The techniques that must be employed to use Fast Reroute for the different methods of signaling LSPs identified in section 2 differ considerably. These should be explained further in applicability statements of, in the case, of a change in base behavior, in implementation guidelines specific to the signaling techniques.

Note that after local repair has been performed, it may be desirable to re-optimize the LSP (see section 5.1). If the point of re-optimization (for example the ingress LSR) lies in a different domain to the failure, it may rely on the delivery of a PathErr or Notify message to inform it of the local repair event.

5.5. Comments on Path Diversity

Diverse paths may be required in support of load sharing and/or protection. Such diverse paths may be required to be node diverse, link diverse, fully path diverse (that is, link and node diverse), or SRLG diverse.

Diverse path computation is a classic problem familiar to all graph theory majors. The problem is compounded when there are areas of 'private knowledge' such as when domains do not share topology information. The problem is generally considered to be easier and more efficient when the diverse paths can be computed 'simultaneously' on the fullest set of information. That being said, various techniques (out of the scope of this document) exist to ensure end to end path diversity across multiple domains.

Many network technologies utilize 'protection domains' because they fit well with the capabilities of the technology. As a result, many domains are operated as protection domains. In this model, protection paths converge at domain boundaries.

5.6. Domain-Specific Constraints

While the meaning of certain constraints, like bandwidth, can be assumed to be constant across different domains, other TE constraints (such as resource affinity, color, metric, priority, etc.) may have different meanings in different domains and this may impact the ability to support DiffServ-aware MPLS, or to manage pre-emption.

In order to achieve consistent meaning and LSP establishment, this fact must be considered when performing constraint-based path computation or when signaling across domain boundaries.

A mapping function can be derived for most constraints based on policy agreements between the Domain administrators.

5.7. Policy Control

Domain boundaries are natural points for policy control. There is little to add on this subject except to note that a TE LSP that cannot be established on a path through one domain because of a policy applied at the domain boundary, may be satisfactorily established using a path that avoids the demurring domain. In any case, when a TE LSP signaling attempt is rejected due to non compliance with some policy constraint, this SHOULD be reflected to the ingress LSR.

5.8. Inter-domain OAM

Some elements of OAM may be intentionally confined within a domain. Others (such as end-to-end liveness and connectivity testing) clearly need to span the entire multi-domain TE LSP. Where issues of confidentiality are strong, collaboration between PCEs or domain boundary nodes might be required in order to provide end-to-end OAM.

The different signaling mechanisms described above may need refinements to [LSPPING], [BFD-MPLS] or the use of [TUNTRACE] to gain full end-to-end visibility. These protocols should, however, be considered in the light of confidentiality requirements.

Route recording is a commonly used feature of signaling that provides OAM information about the path of an established LSP. When an LSP traverses a domain boundary, the border node may remove or aggregate some of the recorded information for confidentiality or other policy reasons.

5.9. Point to Multipoint

Inter-domain point-to-multipoint (P2MP) requirements are explicitly out of scope of this document. They may be covered by other documents dependent on the details of MPLS TE P2MP solutions.

6. Security Considerations

Requirements for security within domains are unchanged from [RFC3209] and [RFC3473], but requirements for inter-domain security are, if anything, more significant.

Authentication techniques identified for use with RSVP-TE can only operate across domain boundaries if there is coordination between the administrators of those domains.

Confidentiality may also be considered to be security factors.

Applicability statements for particular combinations of signaling, routing and path computation techniques are expected to contain detailed security sections.

7. Acknowledgements

The authors would like to extend their warmest thanks to Kireeti Kompella for convincing them to expend efforts on this document.

Grateful thanks to Dimitri Papadimitriou and Tomohiro Otani for their review and suggestions on the text.

8. Intellectual Property Considerations

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in

9. Normative References

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

[RFC3209] Awduche, et al, "Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3473] Berger, L., Editor "Generalized Multi-Protocol Label Switching (GMPLS) Signaling - Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC3667] Bradner, S., "IETF Rights in Contributions", BCP 78, RFC 3667, February 2004.

[RFC3668] Bradner, S., Ed., "Intellectual Property Rights in IETF Technology", BCP 79, RFC 3668, February 2004.

[HIER] Kompella K., Rekhter Y., "LSP Hierarchy with Generalized MPLS TE", draft-ietf-mpls-lsp-hierarchy-08.txt, March 2002 (work in progress).

[INTER-AREA] Le Roux, Vasseur et Boyle, "Requirements for support of Inter-Area and Inter-AS MPLS Traffic Engineering", draft-ietf-tewg-interarea-mpls-te-req-02.txt, June 2004 (work in progress).

[INTER-AS] Zhang, R., Vasseur, JP. et al, "MPLS Inter-AS Traffic Engineering requirements", draft-ietf-tewg-interas-mpls-te-req-07.txt, June 2004 (work in progress).

10. Informational References

[RFC3630] Katz, D., Yeung, D., Kompella, K., "Traffic Engineering Extensions to OSPF Version 2", RFC 3630, September 2003

[RFC3784] Li, T., Smit, H., "IS-IS extensions for Traffic Engineering", RFC 3784, June 2004.

[ATTRIB] A. Farrel, D. Papadimitriou, JP. Vasseur, "Encoding of Attributes for Multiprotocol Label Switching (MPLS) Label Switched Path (LSP) Establishment Using RSVP-TE", draft-ietf-mpls-rsvpte-attributes-03.txt, March 2004 (work in progress).

[BFD-MPLS] R. Aggarwal and K. Kompella, "BFD For MPLS LSPs", (work in progress).

[CRANKBACK] Farrel, A., et al., "Crankback Signaling Extensions for MPLS Signaling", draft-ietf-ccamp-crankback-01.txt, January 2004 (work in progress).

[EXCLUDE] Lee et all, Exclude Routes - Extension to RSVP-TE, draft-ietf-ccamp-rsvp-te-exclude-route-01.txt, December 2003 (work in progress).

[FRR] Ping Pan, et al, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", draft-ietf-mpls-rsvp-lsp-fastreroute-06.txt, (work in progress).

[LSPPING] Kompella, K., et al., " Detecting Data Plane Liveliness in MPLS", Internet Draft draft-ietf-mpls-lsp-ping-05.txt, February 2004 (work in progress).

[MRN] Papadimitriou, D., et al., "Generalized MPLS Architecture for Multi-Region Networks", draft-vigoureux-shiomoto-ccamp-gmpls-mrn-04.txt, February 2004 (work in progress).

[OVERLAY] G. Swallow et al, "GMPLS RSVP Support for the Overlay Model", draft-ietf-ccamp-gmpls-overlay-04.txt, April 2004 (work in progress).

[TUNTRACE] Bonica, R., et al., "Generic Tunnel Tracing Protocol

(GTTP) Specification", draft-ietf-ccamp-tunproto-00,
March 2004 (work in progress).

11. Authors' Addresses

Adrian Farrel
Old Dog Consulting
EMail: adrian@olddog.co.uk

Jean-Philippe Vasseur
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough , MA - 01719
USA
Email: jpv@cisco.com

Arthi Ayyangar
Juniper Networks, Inc
1194 N.Mathilda Ave
Sunnyvale, CA 94089
USA
Email: arthi@juniper.net

12. Disclaimer of Validity

13. Full Copyright Statement