A collaborative PCE-Based mechanism for E2E recovery within MPLS-networks

EL KAMEL Ali[a], Youssef Habib[b]

[a]*Research Unit Prince*
Tunisia
Email: ali.elkamel@isima.rnu.tn
[b]*FSM, Monastir, Tunisia*

Abstract

This paper suggests a new mechanism for inter domain recovery purpose within MPLS-based networks. This mechanism is based on efficient collaboration between several entities called PCE (Path Computation Element). We denote a PCE per domain. All PCEs should communicate in order to ensure propitious End-to-End failure handling, recovery and restoration. Based on normative instructions described in the [RFC 5298] and a novel approach presented in [RFC5441], known as the BRPC approach (Backward Recursive PCE-based Computation), the new mechanism offers an opportunity to achieve E2E recovery using up-to-date information and giving a way to maintain optimal network states as well in intra-domain scope as in inter domain scope, in order to generate a global visibility of the entire network without care about heterogeneity neither autonomy of crossed domains. Simulation results prove that the proposed solution is able to resolve, more efficiently, inter domain recovery issue regardless the AS policies and rules and is able to overcome the inter-domain routing protocol (BGP, Border Gateway Protocol) shortcuts and divergences.

Key words: MPLS, E2E recovery, PCE, PCEP

1. Introduction

Today, the Multi-Protocol Label Switching (MPLS) is being deployed as an emergent technology for both intra and inter domain traffic engineering offering more flexibility and performance for operators to ensure efficient E2E

service in spite of heterogeneity and autonomy among crossed areas. However, the potential of MPLS in the Internet context is almost partly explored due to several policy divergences between Autonomous Systems (ASs) and structural constraints of the current inter-domain routing protocol (BGP :Border Gateway Protocol) mainly used to ensure the exchange of traffic among domains.
MPLS and GMPLS networks were originally limited to single domain environments. Increasingly, multi-domain MPLS and GMPLS networks are being considered, where 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 Interior Gateway Protocol (IGP) areas and ASs or BGP confederation. Furthermore, the [RFC4726] defines a framework for inter-domain G/MPLS traffic engineering. Various schemes and processes have been introduced and discussed in order to establish Label Switched Paths (LSPs) in multi- domain environments. This issue has for long been a critical purpose since the established LSP should cross multi-domains discerned usually as heterogeneous and autonomous. In order to deliver appropriate service to costumer over G/MPLS networks, ISP should define propitious mechanisms to support Protection and recovery, both in intra-domain and inter domain contexts. Basis of such mechanisms have been announced and described into the RFC4428.
Furthermore, explosive extension of the Internet has ratified, for the last few years, the requirements to extend MPLS to the inter-domain context, leading Service Providers to recently point out the definition of frameworks and approaches closely related to the resolution of the intention. The Path Computation Element (PCE) [RFC4655] is one of such proposed architecture. The PCE was chartered at IETF in the beginning of 2006. The purpose of this working group is the computation of paths for G/MPLS traffic engineering across a bundle of Autonomous Systems, generally equipped with different organizational architectures. This obvious diversity has implied specific extensions as well to current intra-domain routing protocol (IGP) as to inter-domain routing protocol (BGP), leading to the definition of mandatory entities and protocols required to deliver path computation information.
This paper deals with the problem of inter-domain recovery mechanisms and looks on the specification of efficient solution to handle E2E LSP Tunnels protection and restoration despite policy disagreements among crossed domains. The proposed solution is based on collaboration between per-domain PCE (Path Computation Element) in order to establish a backup LSP Tun-

nel that bypassed an inter-domain link failure.
Mainly, the basic procedure of computing E2E backup LSP tunnel is based on an alternative call of two recursive procedures in order to establish E2E backup LSP tunnel that can be used to reroute flows around an inter-domain link failure. Those procedures are respectively called Backward-Recursive PCE Computation (BRPC) and Forward-Recursive PCE Computation (FRPC). BRPC is applied just if the process of backup path establishment reaches a domain to which the original working LSP tunnel does not belong to. Conversely, FRPC is applied within a domain to which the working LSP tunnel belongs to. Requests of establishing the backup path are ensured by the PCEP (PCE communication protocol) protocol [RFC5440]. Due to restriction of PCEP protocol to IGP area and BGP confederation, an extension of the standard PCEP protocol was proposed (Internet Draft[9]) that may handle PCE-OAM(PCE Operations And Management) on inter domain context leading to support PCEP messages exchanging between PCE which are not necessary belonging to the same IGP/BGP areas. Moreover, discovery of neighbour PCEs can be achieved efficiently using the IGP/BGP extensions [RFC5088 ,RFC5089,1].At each domain, resource availability information can be reclaimed from the local PCE using the Downstream Backup Path Tree (DBPT) or from the local Master Node (MN), using specific databases. More description is given below.
This paper is structured as follows. The next section presents a brief overview of related work. Section 3 defines basics of the proposed mechanism and describes principle of the proposed recursive procedures. Performances evaluations are presented in Section 4. Conclusion and future work are given in Section 5.

2. Previous Work

Most recent research effort has addressed the intra-domain protection and restoration mechanisms [RFC3496], but only few works have been devoted to the End-to-End context. Moreover, it has been attested that any intra-domain mechanism may be practically feasible on inter-domain scope. Likewise, no inter-domain mechanisms is actually proved to be applicable through End-to-End recovery scheme. In fact, most proposed approaches address one-to-one or peer-to-peer recovery issue. Thus, those solutions are also limited to satisfy inter-domain recovery between at most two ASs.
In [2], it has been proved that the standard inter-domain routing protocol

(BGP) is generally associated with a long convergence properties leading to potential latency in internet path failure, failover and repair. Moreover, for two years, research in [3] has demonstrated that the inter domain failover may reach over 3 minutes and can cause, therefore, several routing fluctuations up to 15 minutes. It has also been announced that such fluctuations cause critical end-to-end packet loss rate and delay that may reach respectively a factor of 30 and 4 during path restoration. In [RFC2439], it has been asserted that routing fluctuations is generally caused by capricious changes in the topology which make routing protocol unstable. Indeed, the protocol BGP evaluates reach ability basing on advertising AS paths and considering as reached those who are stable and suppressing those considered as flapping networks. Although this feature avoids routing deficiencies, it may cause long convergence times and raises the trade-off between stability and convergence. Furthermore, a solution has been proposed to solve inter-domain recovery issue. The main objective was to define a backup path for corresponding working LSP regardless the heterogeneity and the autonomy of various crossed domains. The objective has been faced with intra-domain recovery mechanisms inability due to several problems of scalability and inter-provider fault signalling divergence. The proposed solution, defined as IBLBT(Inter-domain Boundary Local Bypass Tunnel)[5], deals with the inter-domain MPLS recovery problem and is based on the establishment of independent protection mechanisms within each domain using concatenated primary and backup LSPs, minimal protection signalling between domains (using local repair bypass tunnels), and local repair at the domain boundaries.
From another hand, IETF has proposed several studies related to the context of inter-domain traffic engineering and fault recovery, generally, within next generation of networks based on emergent technologies like G/MPLS. Likewise, a framework proposed by [6] describes briefly the various failure cases to be addressed by Inter-Domain Fast Rerouting. Indeed, the failure scenarios associated with inter-domain TE may be caused by:

- 1) A crash of a domain edge node that is present in both domains. Recovery mechanisms should then take in consideration the sub-cases of co-locating or not of the PSL (Point Switching LSR) and the PML (Point Merging LSR) within the same domain.

- 2) A failure of a domain edge node that is only present in one of the domains and

- 3) A Failure of an inter-domain link.

Finally, [7] presents a novel solution for the setup and maintenance of independent protection mechanisms within individual domains and merged at the domain boundaries. This innovative solution offers significant advantages including fast recovery across multiple non-homogeneous domains and big scalability.
In conclusion, several approaches have been proposed to deal with the inter-domain TE and recovery issue. However, most solutions are based on a specification of per-domain computation mechanisms which should merge at domain boundaries. Moreover, no assumptions has been specified by those solutions on how to collaborate at domains frontiers and how to ensure E2E backup path establishment in spite of locally-defined policies and rules. The main issue that should be focused is how to address E2E recovery? this issue requires the definition of practical solutions and techniques that are able to deal efficiently with failure protection and recovery in E2E context.

3. Proposed Mechanism

3.1. Mechanism Overview and Architecture Basis

The proposed mechanism is based on the approach REEQoS[12]. It requires the definition of one Master Node (Mn) per domain. All MNs should be able to communicate over a private infrastructure denote MN-BackBone. Moreover, specific entities known as PCE (Path Computation Element) are to be defined per domain. Therefore, every IGP/BGP area is equipped with at least one PCE. As it has been denoted in [8], the PCE is responsible of handling failure and finding optimal backup path within a local domain. Communication between PCEs is ensured by the PCE-communication protocol (PCEP) [RFC5440].

The establishment of the E2E working LSP tunnel is ensured by MNs[12]. Indeed, the source should determine the closest MN, noted MN_1, capable of serving its admission Request using local configuration or basing on IGP discovery feature (RFC 5088 and RFC 5089). The local configuration is usually done by the network administrator. The Path establishment request is then relayed until reaching a MN_n such as the TE LSP destination resides in the domain D_n. At each step, the MN_i should selects two path segments: $I-LSP_i$ (Internal LSP) used for forwarding incoming packets within domain

D_i, and $E - LSP_i^{i+1}$ (External LSP) used to route flows from the domain D_i to a downstream domain D_{i+1}. Next domain can be statistically configured or dynamically discovered via IGP/BGP extensions. Thus, each MN_i should send a Path Request (XPATH) toward the next selected MN_{i+1}. If M_i discovered multiple neighbours MN_{i+1}^j, j¿1, it may select one MN from the previous subset and maintains locally the remaining nodes for further use. The selection of the MN_{i+1} can be achieved using local policies or heuristics such as first incoming response or low overloaded one.
It's also possible that some path requests have any positive response, or, that a MN_i can not find an appropriate I-LSP and/or E-LSP that connects domain D_i to a next domain D_{i+1}. In such case, the procedure is aborted and a XPathErr message is returned to the MN_{i-1}. Likewise, the MN_{i-1} restarts another Path Request using the remaining subset of relative discovered MNs, if they exist, or propagates conversely the XPathErr message to the upstream MN.
At domain D_n, the MN_n selects an I-LSP between the Ingress Node from where the Path Request XPATH of the upstream MN has been received and the TE LSP destination. The establishment is achieved using the RSVP-TE or the CR-LDP protocols. Therefore, it returns, through the reverse established path, a XRESV message in order to confirm E2E path establishment. As it has been discussed in [12], the propagation is ensured using the RRO (Record Routing Object) using Abstract Nodes identifiers such as AS Numbers. Every MN_i belonging to the established path should update respectively the I-LSPDB and the E-LSPDB databases with selected $I - LSP_i$ and $E - LSP_i$, and should define the association between them within its LEDB(Label Equivalency DataBase). Finally, an E2E tunnel has been computed that supports the required QoS of the flow asking for being admitted on an E2E basis. During the E2E working LSP Tunnel setup, one MN may receive more than one response from neighbour MNs. Every MN passes several received responses to the co-located PCE. At each domain D_i, the PCE_i should establish and maintain several DBPTs as to serve incoming requests of establishing E2E backup LSP tunnel once an inter-domain failure has happened.
A DBPT is defined as a MP2P (Mutli-point to point) TE LSP tree returned by PCE_i to PCE_{i-1} as response to a path computation request PCReq. As defined in RFC4461, a P2MP intra-domain MPLS-TE LSPs tree is a TE LSP unidirectional tree that is initiated at an ingress Node within a domain and has one or more leaves as Egress nodes from the same domain. Further,

the TE LSP tree is based on gathering several explicit paths, which may be constructed using strict path method or loose path method, as specified on [RFC3209]. Besides, an explicit path can be made using various constraint-based computation algorithm such as cost-based (CSPF) or QoS-based and may use any combination of later listed algorithms such as faire-cost QoS algorithm [RFC4461].
Accordingly to REEQoS approach [12], an E2E LSP tunnel is defined as a concatenation of a set of two path segments, named respectively, I-LSP and E-LSP. The MN_i, which refers to the Master Node of the domain D_i, transmits an XPATH request toward all neighbours only if both an I-LSP and E-LSP are selected within the domain D_i, to support incoming admission requests from multiple flows, received through, the upstream MN(i-1), or from the source. The MN_i may receive many responses, thus, it should select the appropriate one and transmits the remaining toward the co-located PCE_i. Each PCE_i should compute the Downstream Backup Path Tree (DBPT) using received responses and the local databases: I-LSPDB and E-LSPDB. Extensively in this work, a $DBPT_i^j$ is defined as a MP2P (Mutli-point to point)TE LSP tree returned by PCE_j to PCE_{j-1} as response to a path computation request PCReq. A P2MP (Point to Multipoint) tree is a TE LSP unidirectional tree rooted at Ingress node i from the domain D_j and have leaves from the set of ingress nodes of the downstream domain D_{j+1}. The ingress node of the domain D_j is defined as the node through which a flow admission request is received from the source, or, by which, a request XPATH, is transmitted from MN_{j-1} toward local MN. Further, the TE LSP tree is based on gathering several explicit paths, which may be constructed using strict path method or loose path method, as specified on [RFC3209]. Besides, an explicit path can be made using various constraint-based computation algorithm such as cost-based (CSPF) or QoS-based and may use any combination of later listed algorithms such as faire-cost QoS algorithm [RFC4461].
At each domain D_i between the source domain D_1 and the destination domain D_n, the PCE_i creates a tree of potential paths to the destination and associates it with the original working LSP Tunnel segment. The PCE should maintain the selected tree available for incoming requests. This is done simultaneously and independently at each crossed domain. Each branch of a DBPT is returned as an Explicit path (in which case, all hops are listed) or a loose path (in which only Ingress and Egress Nodes are specified), as defined in RFC3209. The choice between two models is fixed by the Network

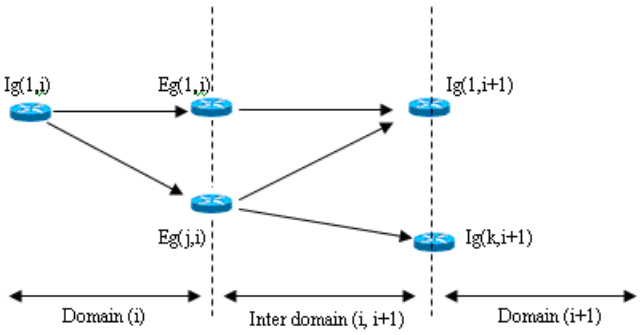

Figure 1: Per-domain DBPT establishment

operator. Indeed, explicit rooting is used when no resource share is planned within a local domain. On the other hand, loose paths allow resources sharing. Obviously, the selection is made by network operator accordingly to local administrative policies and rules.

3.2. Per-domain Downstream Backup path tree (DBPT)

A $DBPT_i^j$ is defined as a MP2P (Mutli-point to point)TE LSP tree returned by PCE_j to PCE_{j-1} as response to a path computation request PCReq transmitted by the Path Computation Element PCE_{j-1} from the domain D_{j-1} toward the PCE_j from the domain D_j, and which is admitted at domain D_j via ingress node Ig_i^j.

A P2MP MPLS-TE LSPs tree is a TE LSP unidirectional tree that is initiated at an ingress Node within a domain and has one or more leaves as multiple ingress nodes from one or more downstream domains [RFC4461]. Further, the TE LSP tree is based on gathering several explicit paths, which may be constructed using strict path method, loose path method or any combination of both methods, as specified on [RFC3209]. Besides, an explicit path can be made using various constraint-based computation algorithm such as cost-based (CSPF) or QoS-based and may use any combination of later listed algorithms such as faire-cost QoS algorithm [RFC4461]. Let denote $DBPT_i^j$ as the Downstream Backup Path Tree rooted at Ingress Node Ig_i within the domain D_j. This tree is defined as a gathering of several I-LSP, each one defined as an object RRO. Let denote also $Lf^*_{Ig_i^j}$ as the set of leaves

of the tree $DBPT_i^j$ belonging to the downstream domain D_{j+1}. A leaf $Lf_{Ig_i^j}^k$ of a tree $DBPT_i^j$ identifies the k-th ingress Node from the domain D_{j+1}, that it exists at least an Egress node Eg_p^j from domain D_j, an I-LSP joining Ig_i^j to Eg_p^j, and an E-LSP joining Eg_p^j with Ig_k^{j+1}. The path between Ig_i^j and Ig_k^{j+1} can be defined using strict model, loose model, or any combination of both models. The choice is Administrator-dependant and relies on local policies applied with the scope of the AS.
At each domain, the PCE should maintain multiple $DBPT_i^j$ associated to each ingress node Ig_i^j from which a working LSP Tunnel is initiated or is crossing. Every P2MP tree is assigned a unique identifier, noted P2MP ID or P2ID, as depicted in [RFC4461]. This identifier is constant for the whole LSPs belonging to the same tree. The correspondence between the $DBPT_i$ and its P2ID is maintained by the PCE_i.

3.3. Forward-Recursive PCE-based Computation procedure (FRPC)

The FRPC procedure is applied within a domain to which the original working LSP tunnel belongs to. The procedure consists on discovering available I-LSP that can join Ingress Node to the local Egress node of the working LSP segment, slice of the whole working LSP tunnel. Otherwise, the PCE should select an I-LSP and an E-LSP, together they are able to support required class of service. Once found, corresponding RRO is maintained until receiving a Confirmation (PCRep)/Path Error (PCErr) message from downstream domain. The operation is repeated until the destination domain, at which it exists an LSP toward the destination, or a joining point between the computed path and the original LSP tunnel is reached.
At destination domain, a Confirmation message is returned recursively to upstream PCE. The confirmation is carried using a PCRep message and may contain an RRO object that specifies the selected segment path that may be used to construct the whole backup LSP tunnel. Every PCE associates the received RRO with the local one and transmitted the confirmation toward its upstream PCE. The operation is repeated until reaching the source domain, defined as the closest upstream AS to the failure point. If a PCE_i can not found an I-LSP/E-LSP within local domain which can support required QoS constraints, it proceeds to novel LSP segments establishment , or carried an Error Message to the upstream PCE. In this work, we do not consider the process of establishing new path segments, therefore, in such situation; en error message is propagated toward upstream PCE. The error can be for-

warded using a PCRep message.
The procedure FRPC uses local LSP and LSP states databases, defined respectively as I-LSPDB and I-LSPSDB. Correspondingly, selection of E-LSP is based on E-LSPDB and E-LSPSDB. This information can be gathered from the co-located MN. Procedure FRPC can be described as follow:

1. Step 1: the PCC ingress node determines local PCE_1, to which it sends a PCReq message in order to establish a Backup LSP Tunnel toward the destination. Having discovered next PCE (it may be a set of PCEs) using IGP/BGP extensions, The PCE_1 selects appropriate path segment from local databases (I-LSP and E-LSP databases) and sends a PCReq to the selected next PCE via the selected combination.
2. Step i: for i: = 1 to n-1, when the PCE_i receives a PCReq from its upstream PCE_{i-1}, it should proceed as follows:
   (a) Step i.1: the PCE_i checks of available I-LSP that can support QoS-constraints involved within the request message, first, which is initiated at Ingress Node from where the PCReq has been received, and more, which has the Egress node belonging to the original working LSP tunnel. Once Found, the I-LSP is added to the path segment received from upstream PCE_{i-1} and The procedure is stopped. The backup LSP tunnel is computed.
   (b) Step i.2: Otherwise, if no I-LSP has been found that satisfies previous assumptions, the PCE_i should check available combination (I-LSP,E-LSP) having the Final extremity , which is an ingress node from the next domain, belongs to the original working LSP tunnel. Once found, the selected segment is also added to the path segment received from PCE (i-1) and The procedure is stopped. The backup LSP tunnel is computed.
   (c) Step i.3: Otherwise, if no combination (I-LSP, E-LSP) has been found that may support required QoS-constraints with assymption denoted in i.2, The PCE_i selects available combination (I-LSP, E-LSP) that only can support required class of service. The selected path segment is added to the segment received from previous PCE_{i-1} and a new PCReq is communicated to the next PCE_{i+1} , based on the information gathered with the selected combination(I-LSP , E-LSP).
3. Step n: The PCE_n may receive a PCReq from an upstream PCE_{n-1}. It selects appropriate I-LSP toward LSP destination using local I-LSP database and starts the confirmation process toward the PCE_1.

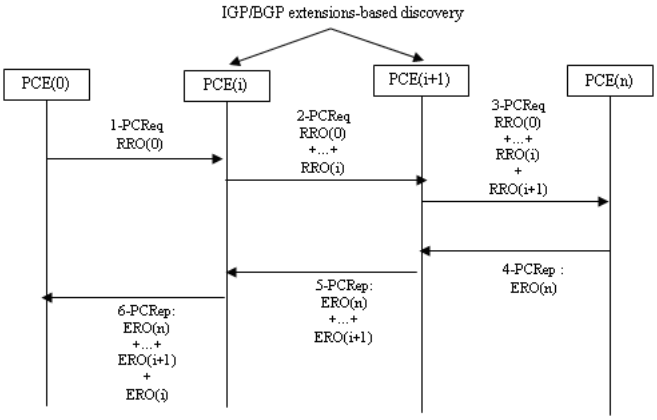

Figure 2: A backup LSP tunnel establishment diagram using FRPC procedure

3.4. Backward-Recursive PCE-based Computation procedure (FRPC)

When the PCReq message reaches a domain that is not crossed by the original working LSP tunnel, the local PCE should initiate a BRPC procedure. The BRPC procedure relies on communication between per-domain PCEs and aims to recursively establish a backup LSP tunnel using the per-domain computed DBPT.
Indeed, if the PCReq reaches a domain D_i which is not crossed by the working LSP tunnel, the PCE_i transmits the request to one of neighbouring PCE_{i+1}. Discovery of adjacent PCE can be achieved using IGP/BGP extension and requests throughout heterogeneous AS can be attained using the PCEP extension defined into the draft [9]. The PCE of the source domain should receive a PCReq from the PCC ingress node, which is the root of the segment path, part of the whole working LSP tunnel. The procedure BRPC can be achieved as follow:

1. Step 1: First, the PCC ingress node should determine the local-PCE and its capability of serving its path computation request. At each step of the process, the next PCE can either be statically configured or dynamically discovered via IGP/BGP extensions ([RFC5088] and [RFC5089]). The path computation request is then relayed until reaching a PCE_n such that the TE LSP destination resides in the domain D_n. If any PCE can be found or the next-hop PCE of choice is unavailable, the procedure is stopped and a path computation error is

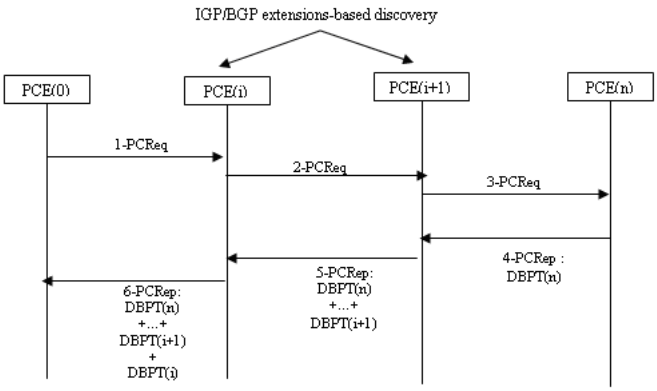

Figure 3: A backup LSP tunnel establishment diagram using BRPC procedure

returned. If PCE_{i-1} discovers multiple PCEs from the adjacent domains , it selects a set of these PCEs based on some local policies or heuristics. This set may be maintained for further purpose.

2. Step 2: At the destination domain D_n, the PCE_n computes the $DBPT_n$, which is made of the list of QoS-constrained I-LSP between every Ingress node I(j,n) and the TE LSP destination using a suitable QoS-based path computation algorithm and returns the resulting tree to PCE_{n-1} as a list of RRO objects.
3. Step i: For k:= n-1 to 1, the local PCE_k receives the DBPT computed by the PCE_{k+1}. Thus, it computes available segments of backup LSP tunnel using local I-LSP and E-LSP databases and the received DBPT from downstream PCE. The resulting tree is transmitted toward the upstream PCE.
4. step n: The PCE_1, from which the PCReq has been initiated, may receive a PCRep message containing a RRO object describing the backup LSP tunnel constructed using the procedure BRPC. The PCE_1 selects an appropriate path that it communicate to the PCC which starts the flow rerouting around the failure point.

3.5. Illustrative example

As shown in figure 4, the PCE_i should specify a P2MP(Point to Multipoint) tree which is, in this case, rooted at ingress node Ig(1,i) and have two leafs defined respectively $Ig(1, i+1)_1$ from domain $D(i+1)_1$ and $Ig(1, i+1)_2$

from domain $D(i+1)_2$. Two branches are defined in this tree respectively as I-LSP (1') and I-LSP (1") to which two inter-domain segments, respectively E-LSP (2') and E-LSP (2"), are added. Branches are maintained at the PCE_i respectively as $Ig(1,i) \rightarrow Eg(k,i), Ig(1,i+1)_1$ and $Ig(1,i) \rightarrow Eg(j,i), Ig(1,i+1)_2$ using loose path model. The LSP established using segments (1) and (2) defines the working LSP. This path does not belong to the DBPT (1,i), thus, it is maintained by the MN and will not be transmitted to the co-located PCE.

If a failure occurs at an inter-domain link (segment 2), the MN_i, which detects the failure should transmit an order to the Ig_1^i. The order consists on a specific notification message by which the Ingress node should request the PCE_i to select another LSP from the set $DBPT_1^i$ in order to bypass the failed link. The PCE_i, receiving the request from the ingress node, looks on local $DBPT_1^i$ in order to find another LSP joining the ingress node with another Egress Node Eg_k^i and, moreover, where it exists a E-LSP between this Egress Node and the second extremity of the failed link, which is in this case, the ingress node $Ig(1,i+1)_1$,belonging to the downstream domain $D(i+1)_1$.
If no E-LSP satisfies the previous condition, the PCE looks next time at an LSP joining the originate Ingress node Ig(1,i) with an Egress node Eg(j,i) from the DBPT (i) and, moreover, where it exists an E-LSP between the reached Egress Node and a downstream domain $D(i+1)_2$. At this case, the path computation request is forwarded to the $PCE(i+1)_2$ of the domain $D(i+1)_2$ via the selected ingress node $Ig(1,i+1)_2$. The ingress node receives then a request from the Eg (j, i) that it transmits to the $PCE(i+1)_2$ in order to solicit a local I-LSP toward the destination.
In the same way, the PCE(i+1) form domain $D(i+1)_1$ or domain $D(i+2)_2$ processes to the establishment of E2E backup path based on local computed DBPT and local databases I-LSPDB and E-LSPDB. If at any time, a connection point is reached between the processed backup LSP tunnel and the original working LSP Tunnel, the failure is considered bypassed. The full process is then stopped and packets are rerouted through the new established path from the ingress node Ig(1, i) to the point of connection. Otherwise, the establishment of the new backup path is repeated within each domain until reaching the destination domain.

The per-domain selection of backup LSP tunnel segment is based on two recursive procedure: BRPC (Backup path recursive path computation) al-

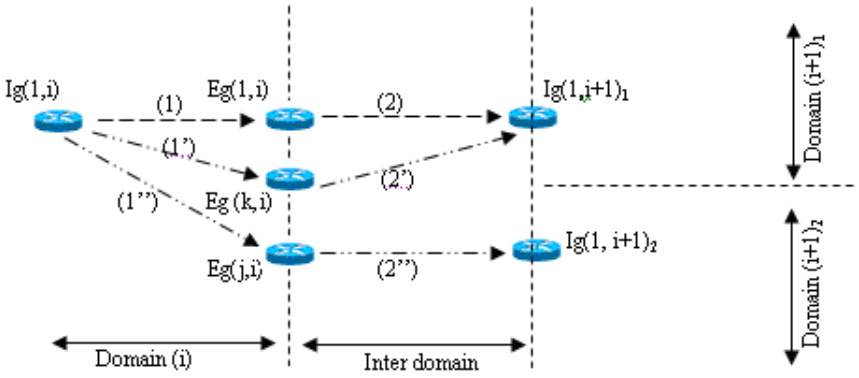

Figure 4: Example of a DBPT establishment proposed within the solution

gorithm [RFC5441] and FRPC (Forward-recursive Path Computation). The proposed mechanism uses the PCEP (Path computation Element Protocol) protocol [RFC5440] and its extension defined in [9] to exchange required messages in order to ensure the process of establishing an inter-domain backup path. At each domain (Di), the PCE should select the appropriate procedure to be locally run using followed assumptions:

1. If the Path Computation Request (PCReq) has reached a domain (Di) to which, the original working LSP Tunnel belongs to, the procedure FRPC is applied.
2. Conversely, if the Path Computation Request (PCReq) reached a domain (Di) to which the original working LSP Tunnel does not belongs to, the procedure BRPC is applied.

Figure 2 shows an example of an alternative use of recursive procedures. First, let suppose four independent ASs numbered respectively AS1, AS2, AS3 and AS4. Every AS is equipped with several entry Ingess nodes and exit Egress Nodes. Let denote I(x,y) as the x-th Ingress Node belonging to the y-th AS. Similarly, let denote E(x,y) as the x-th Egress Node belonging to the y-th AS. A working LSP Tunnel has been established using REEQoS Model. The working LSP Tunnel is defined as follows: $I(1,1) \rightarrow E(1,1) \rightarrow I(1,2) \rightarrow E(1,2) \rightarrow I(1,4) \rightarrow E(1,4)$.
Let suppose also that a link failure has occurred at inter-domain edge defined by (E(1,1), I(1,2)). The MN(1), which is the Master Node of the domain

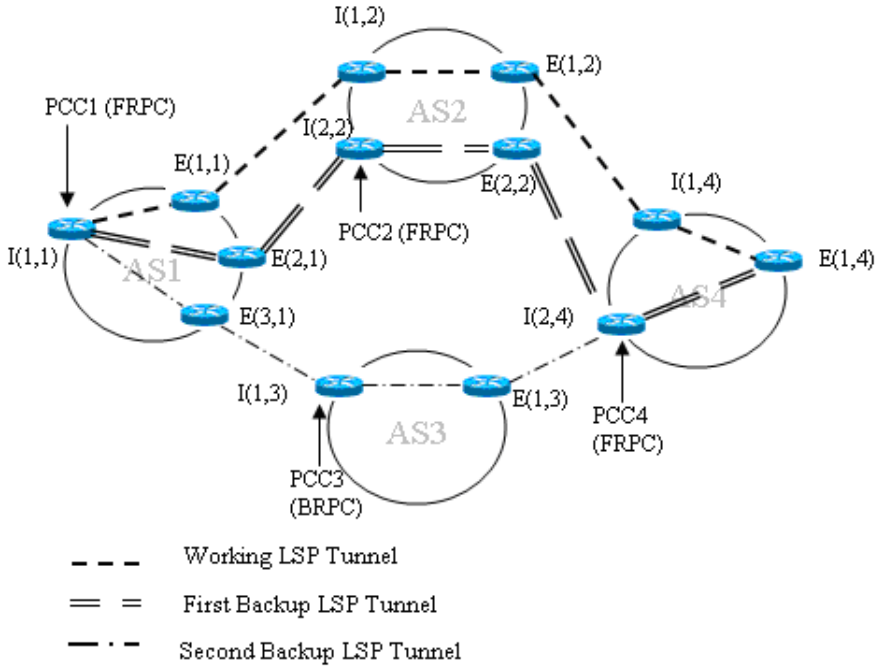

Figure 5: E2E Backup path establishment using alternative call to BRPC and FRPC

(D1), should detect the failure, since the link is on its management and control scope. Furthermore, MN(1) should notify the failure to the I(1,1), since this ingress node represents locally, the source of working LSP Tunnel. The later selected ingress node should operate as a PCC (Path Computation Client) (this is noted in the figure as PCC1) and requests the establishment of a backup LSP Tunnel from the PCE(1) in order to bypass the failure. The request can be achieved using a PCReq message as defined by the PCEP protocol.

3.5.1. Scenario 1: Backup LSP tunnel and Working LSP Tunnel cross the same AS

At AS (1), considered as the upstream domain of the failure point, the PCE(1) looks at local DBPT(1) and tries to find another branch that have a leaf which belongs to the same next domain as the working original LSP.

Let suppose, in the example, that it is the branch defined as follows: I(1,1)-E(2,1),I(2,2). Thus, a PCReq is transmitted from the PCE(1) toward the PCE(2) in order to start an LSP establishment process throughout the domain AS2. Since the Request has been transmitted to a PCE of a domain to which the original working LSP tunnel belongs to, the procedure FRPC is applied. Indeed, the PCE should find an I-LSP from I(2,2) toward the Egress node belonging to the working LSP within actual domain, E(1,2). Once found, the failure is considered bypassed and response is propagated reversely until reaching the source I(1, 1). Then, the backup path is defined as follows: $I(1,1) \rightarrow E(2,1), I(2,2) \rightarrow E(1,2)$. The selected backup path is spread using the PCRep message defined by the PCEP protocol.
Otherwise, if any I-LSP between I(2,2) and E(1,2) from the AS2 has been found, the PCE computes a new I-LSP and E-LSP from the ingress node I(2,2) that are capable of supporting QoS constraints announced within the request PCReq. Then, a new PCReq is forwarded to the PCE of the next selected AS which should operate similarly as the previous PCE. Perhaps, the establishing of the new I-LSP and E-LSP can be renounced. In fact, before computing new segments of the backup LSP path, the PCE should check the existence of appropriate I-LSP and E-LSP from I-LSP and E-LSP databases, respectively, I-LSPDB, and E-LSPDB, associated with the co-located MN. Basing on the LSP-states given respectively within databases I-LSPSDB and E-LSPSDB, the PCE can select the propitious segment (I-LSP'E-LSP) that is used to forward the request of establishing backup path to the next downstream domain. As in the example, the PCE(2) selects the path segment defined as follows: $I(2,2) \rightarrow E(2,2), I(2,4)$.

3.5.2. Scenario 2: Backup LSP Tunnel and Working LSP tunnel cross two different ASs

At AS(1), PCC1 requests the establishment of a backup path to the local PCE(1). The Later should check for available I-LSP and E-LSP that may support required FEC announced with the request. Let suppose that the PCE responses by a branch from the DBPT(1) , defined as follow: I(1,1)→E(3,1),I(1,3). The PCReq message is then forwarded to PCE(3) . As the request is addressed to a domain to which the working LSP Tunnel does not belong to, the procedure BRPC is applied. In fact, the PCE (3) determines a neighbour PCE to which it should transmit a PCReq message with appropriate QoS -constraints as it has received from the upstream PCE(1). The discovery of neighbour PCEs can be achieved using IGP/BGP

discovery extensions. Transmission of PCReq and reception of PCRep in the inter-domain context can also be achieved using the extension introduced within the Internet Draft[9].
PCE(4) should receive a PCReq from PCE(3). It checks whether the working LSP tunnel belongs to the same AS or not. Affirmatively, it applies the FRPC procedure and consults various databases in order to find an appropriate I-LSP that joins the backup LSP tunnel to the working LSP tunnel. Once found, the path segment is returned toward the upstream PCE(3). This later should connect the two branches of the local DBPT and the path segment received from PCE(4). The resulting path segment is also returned to PCE(1). The PCE(1) configures new backup LSP tunnel and starts the rerouting procedure.
At every domain boundaries, the Egress node, also considered as a PCC, receives the PCReq from the local PCE and should transmit it to a PCC belonging to a downstream domain. At inter domain scope, the PCC-PCC communication is ensured by an extension of the standard PCEP protocol. The PCC of the source domain should have information on correspondent PCC of the destination domain. This can be done using PCEP extension over BGP/MPLS IP-VPN, described in [13]. Indeed, the specification of the PCEP protocol into the RFC5441 does not describe communication basis between two PCCs. Moreover, in order to conserve confidentiality, it has been affirmed that PCEP should be applied within IGP areas or BGP confederation. The use of PCEP in an inter domain scope should consider inter-domain TE LSP and should extend PCEP messages to be able to be transferred over BGP (Border Gateway Protocol) [RFC1771].

3.6. Inter-domain PCEP extension

The PCEP extension proposed in [9] gives a way of exchanging PCReq/PCRep messages on an inter-domain scope. This is done by the definition of new object called 'PCE Sequence Object' that represents the PCE topology tree. This assumes that every PCE is associated with a public Identifier, such as IPv4/IPv6 prefix, as it has been done with Master-Nodes specification and discovery into the REEQoS approach [12].
Moreover, PCE discovery can be achieved using IGP/BGP extensions as it has been defined into [RFC5073] and [14]. Once discovered, the PCEP messages can be forwarded both in intra and inter domain context. Some relevant problems have been announced, but not treated in the RFC5441. It has been signalled in section 3 [General Assumptions], that a sort of local

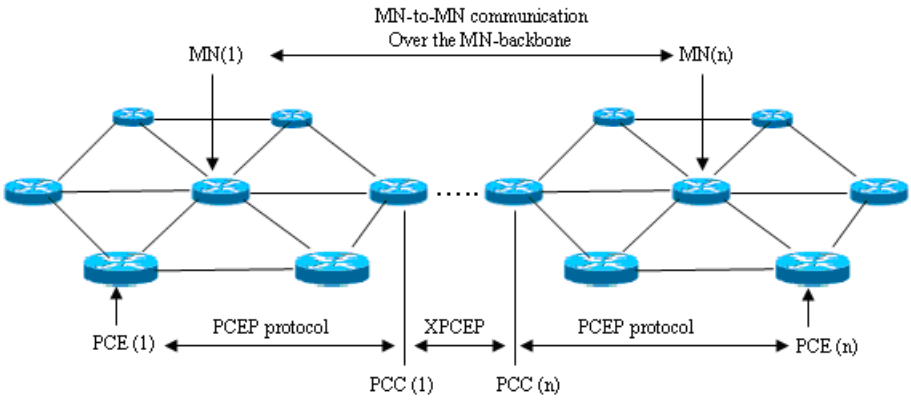

Figure 6: PCEP extension for inter-domain PCE communication

constraint-mapping based on per-domain policy agreements is usually required in order to overcome constraints disagreements between Operators at border nodes. This can be achieved at PCC-to-PCC communications within domains boundaries, where a sort of translation is required in order to convert Per-domain policy-based constraints, involved into the PCReq message, in order to meet local policies.

4. Performance analysis

In order to evaluate the proposed mechanism, two techniques were used. First, we present an analytic model of the proposed solution and we prove efficiency introduced with the use of the procedures FRPC and BRPC. We also demonstrate the benefit obtained using the alternative call of the previous path computation procedures in order to establish optimal backup LSP tunnel at convenient delay and with opportune resources utilisation. Furthermore, we have used the network simulator NS2 (release 2.26) with several modifications and extensions associated with the deployment of specific agents located at dedicated LSRs within the topology. More details are given below.

4.1. Analytic evaluation

Let denote p_k the probability of finding a connection point at domain k. Conversely, let denote q_k the probability of finding a connection point at inter-

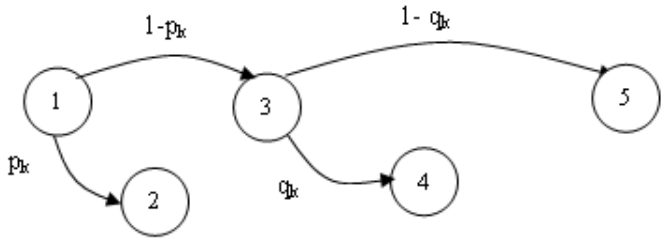

Figure 7: Markov diagram of the probability of finding required I-LSP and E-LSP

domain scope. At every domain k, the probability of finding a LSP segment that may be used to establish an E2E backup LSP tunnel is described using the graph below:

The probability of finding a backup LSP tunnel at domain k is noted Pr_k. It can be defined as follow:

$$\begin{cases} Pr_k = p_k + q_k(1-p_k) + (1-p_k)(1-q_k)Pr_{k+1} \forall k < n \\ Pr_n = p_n \end{cases} \tag{1}$$

Let suppose that $\forall k$; $p_k = p$ and $q_k = q$ the system above can be expressed as follow

$$\begin{cases} Pr_k = p + q(1-p) + (1-p)(1-q)Pr_{k+1} \forall k < n \\ Pr_n = p \end{cases} \tag{2}$$

The probability at a domain k may be simplified as follow

$$\begin{cases} Pr_k = \alpha + \beta Pr_{k+1} \forall k < n \\ \alpha = p + q(1-p) \\ \beta = (1-p)(1-q) \end{cases} \tag{3}$$

Moreover, it is possible to demonstrate that the probability Pr_k can be defined as follow

$$Pr_k = \alpha \sum_{i=0}^{n-(k+1)} \beta^i + \beta^{n-k} p \tag{4}$$

Where n defines the destination domain and k defines the upstream domain closest to the failure point. This can be proved using the recurrence proof

principle. First, the assumption is correct for k=n-1;

$$\begin{cases} Pr_n = p \\ Pr_{n-1} = \alpha + \beta Pr_n = \alpha + \beta P \\ Pr_{n-1} = \alpha \sum_{i=0}^{n-((n-1)+1)} \beta^i + \beta^{n-(n-1)} p \end{cases} \tag{5}$$

Let suppose that it remains correct for k=j; we must prove that it remains also correct for k=j-1. Indeed,

$$\begin{cases} Pr_j = \alpha + \beta Pr_{j+1} Pr_j = \alpha \sum_{i=0}^{n-(j+1)} \beta^i + \beta^{n-j} p \\ Pr_{j-1} = \alpha + \beta Pr_j \\ Pr_{j-1} = \alpha + \beta(\alpha \sum_{i=0}^{n-(j+1)} \beta^i + \beta^{n-j} p) \\ Pr_{j-1} = \alpha + \alpha \sum_{i=0}^{n-(j+1)} \beta\beta^i + \beta\beta^{n-j} p \\ Pr_{j-1} = \alpha + \alpha \sum_{i=1}^{n-j} \beta^i + \beta^{n-(j-1)} p \\ Pr_{j-1} = \alpha\beta^0 + \alpha \sum_{i=1}^{n-j} \beta^i + \beta^{n-(j-1)} p \\ Pr_{j-1} = \alpha \sum_{i=0}^{n-(j-1)-1} \beta^i + \beta^{n-(j-1)} p \\ Pr_{j-1} = \alpha \sum_{i=0}^{n-((j-1)+1)} \beta^i + \beta^{n-(j-1)} p \end{cases} \tag{6}$$

That it is, the probability of finding a backup LSP tunnel from domain k to a domain n is defined as follows:

$$Pr_k = \alpha \sum_{i=0}^{n-(k+1)} \beta^i + \beta^{n-k} p \tag{7}$$

In order to find an E2E backup LSP tunnel, it may be necessary to compute the probability of finding it at the starting domain. However, finding a backup LSP segment at domain k requires finding a backup LSP segment at domain k+1. The procedure is recursive since the probability of finding a backup LSP tunnel at domain k depends on the probability of finding a backup path on domain i+1, and so on. The complexity of the procedure at worst case is O(nlogn), where n represents the number of domains connecting the initial domain to the destination domain.
From another hand, the probability of finding a backup LSP tunnel from a domain k to a destination domain n, when the establishment crosses domains to which the working LSP does not belongs to, is defined as the probability of finding both an I-LSP an E-LSP that does not connects the working LSP Tunnel. Explicitly, this probability can be computed without considering the probability of finding an I-LSP or an E-LSP, or both, that connect the working LSP tunnel. Those probabilities are defined as follows:

- The probability of finding both an I-LSP and E-LSP that does not connect the working LSP Tunnel: (1-p)(1-q)
- The probability of finding an I-LSP that connects the working LSP tunnel with an E-LSP that does not: p(1-q)
- The probability of finding an I-LSP that does not connect the working LSP tunnel with an E-LSP that does: (1-p)q
- Finally, the probability of finding an I-LSP and an E-LSP that both connect the working LSP tunnel: pq

The probability of finding a backup LSP tunnel using the BRPC procedure is defined as:

$$Pr_k = Pr_{k+1}[1 - (p(1-q) + q(1-p) + pq)] \tag{8}$$

considereing same assymptions, we consider that :

$$\begin{cases} Pr_k = \beta Pr_{k+1} \\ \beta = (1-p)(1-q) \end{cases} \tag{9}$$

Similarly, the probability of finding a backup LSP tunnel can be presented as follow:

$$Pr_k = \beta^{n-k} p \forall k \leq n \tag{10}$$

The probability of finding a backup LSP tunnel using the BRPC procedure is less than the probability of finding such backup LSP Tunnel using the FRPC procedure. Indeed,

$$Pr_k^{FRPC} - Prk^{BRPC} = \alpha \sum_{i=0}^{n-(k+1)} \beta^i \geq 0 \tag{11}$$

This is due to the factor of finding a segment path that connects the original working LSP tunnel.
Moreover, let suppose a failure has occurred between domain k and domain k+1. The number of crossed domains needed to establish the backup LSP tunnel is exactly n-k, where n is the destination domain, using the BRPC procedure. This is due to the fact that the PCReq message is propagated

toward the destination before the backup path establishment is started. However, it can be less then n-k using the FRPC procedure. This depends on the probability of finding a local segment path that connects the original LSP tunnel. In this case, the procedure is stopped and the backup LSP tunnel is considered established.
Let suppose a failure has occurred between a domain k and a domain k+1. Similarly, let denote $\Pi_{i,j}^{m}$ the backup LSP tunnel that joins the LSR i (from domain k) to the LSR j, where j is the first connection point between the established backup LSP tunnel and the original working LSP tunnel and m is the number of crossed domains before reaching the connection point.

Let denote $\Gamma_{i,j}^{m}$ its cost. The shortest backup LSP tunnel is defined as $\Pi_{i,j}^{*}$ such as $\Gamma_{i,j}^{*} = \min_m \Gamma_{i,j}^{m}$. It is obvious that FRPC ensures less cost then BRPC. However, the previous cost is evaluated at E2E level and does not consider local costs when segment paths are established. Indeed, the BRPC procedure is based on the break-before-make model in which connection is found before making any resources reservation. The FRPC requires reserving resources at each domain before transmitting requests to next domain. Such process may introduce resources wasting since no guarantee is offered before reaching the destination domain. The propagation of PCReq, toward destination domain, offers a guarantee of establishing backup LSP tunnel without resources wasting nor network performances degradation. Optimisation is more ensured using BRPC procedure.

4.2. Simulation results

We have considered another simulation topology (figure 9), containing 4 ASs, noted respectively, AS1, AS2, AS3 and AS4. All ASs are connected in a meshed way. Every AS contains 4 LSR. For each AS_i, we denote $LSR_i^j \forall j \leq 4$ as the j^{th} LSR belonging to the AS number i. The source S wishes to transmit a VBR traffic having a packet size of 250Mb and an exponential variation of the inter leaving period. The working LSP tunnel is: $S \rightarrow LSR_{AS1}^{1} \rightarrow LSR_{AS2}^{2} \rightarrow LSR_{AS2}^{1} \rightarrow LSR_{AS2}^{4} \rightarrow LSR_{AS3}^{1} \rightarrow LSR_{AS3}^{4} \rightarrow D$ For simplicity purpose, an LSR is elected per domain to be the local MN. Furthermore, the MN agent and the PCE agent are co-located within the same node. Selected nodes are: LSR_{AS1}^{1};LSR_{AS2}^{1};LSR_{AS3}^{1};LSR_{AS4}^{1} Simulation aims to evaluate various E2E performances such as delay required to establish an E2E backup LSP tunnel which bypassed rapidly the failure point. Results are

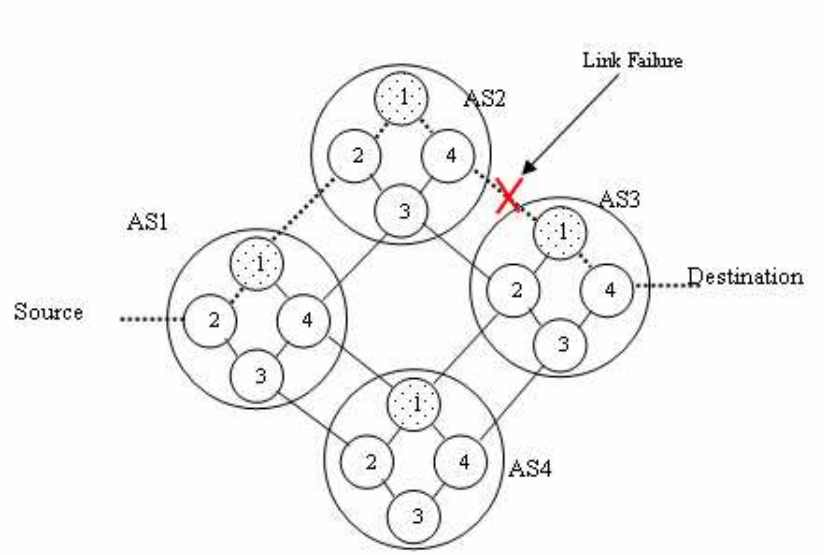

Figure 8: Simulation topology

compared with related approaches such as IBLBT (Inter domain Boundary Local Bypass Tunnel) and standard E2E recovery mechanism.

For this purpose, a failure is planned to happen on link $LSR^4_{AS2} \rightarrow LSR^1_{AS3}$. We define an E2E Backup LSP Tunnel as follow: $S \rightarrow LSR^2_{AS1} \rightarrow LSR^3_{AS1} \rightarrow LSR^4_{AS1} \rightarrow LSR^1_{AS4} \rightarrow LSR^2_{AS3} \rightarrow LSR^4_{AS3} \rightarrow D$ This LSP tunnel is to be used when the E2E recovery mechanism is applied. Furthermore, we define associated gateways for the LSR^1_{AS1} as follows:

- Gateway LSR: LSR^1_{AS1}
- Concatenation PSL: LSR^2_{AS2}
- Proxy Gateway LSR: LSR^4_{AS1}
- Proxy Concatenation PSL: LSR^3_{AS2}

Different listed nodes are used to run the IBLBT mechanism. In order to prove the efficiency of the proposed approach, we evaluate three performance parameters. We estimate respectively, the required recovery time, the E2E Packet Loss rate and the E2E packet disorder.
In this simulation, recovery time is from the receiver's perspective (D-LSR)

Table 1: Comparison between various approaches for inter domain recovery

	BGP recovery Model	E2E Recovery Model	IBLBT	Proposed Mechanism
Time Rec	64s	47.28ms	31.34 ms	29.67ms
Pkt Loss	47%	22%	13.5%	15.9%
Pkt disorder	66.7%	36.18%	9.87%	7.67%

and represents the difference in time between the reception of the last packets on the primary LSP tunnel and reception of the first packets on the backup LSP tunnel. The recovery time includes failure detection time, time for the transmission of failure notification messages, protection switching time, and transmission delay from the recovery point to the merge point. Both recovery and merge points are mechanism-dependant.

Table1 shows Comparison of several recovery models. The recovery speed benefits of the new proposed mechanism is more evident then the IBLBT approach and the end-to-end scheme. Indeed, it is known that IBLBT takes more time before rerouting activation since several updates are applied on local LFIB in order to start the rerouting process via the gateways and proxies. E2E recovery mechanism takes over 47 ms to start the protection process. This is due to notification and activation process which should reach points of repair (PSL and PML). The BGP recovery model remains although clearly divergent as it has been depicted in literature. The greatest variation of recovery time reaches over 53%between BGP model and the new proposed model. Similarly, the new mechanism ensures lower packet loss rate that can reach a factor of 3,94 lower than the packet loss rate ensured by BGP.
Finally, the packet disorder ensured by the BGP model can reach over a factor of 5.26 more than the amount ensured by the proposed mechanism.
Although Packet disorder and Recovery time are better in proposed mechanism than in other mechanism, the amount of lost packets is greater than the IBLBT model. This is due to the establishment process which involves messages propagation. Such time may induce queue overload at some LSRs, leading consequently to loose packets. A solution can be made using queues with high storage capacities.
Those results validate recent presumptions on BGP divergences and shortcuts. They justify and prove impact and degradation on network perfor-

mances when using the widely used inter domain protocol (BGP) for E2E recovery purpose. Furthermore, we have evaluated received packet on LSR^4_{AS2} , which is the closest upstream node of the failure point. The simulation consists on computing received packets at LSR^4_{AS2} using respectively the standard BGP model, the E2E recovery model and the proposed mechanism. The evaluation is started after 50 sec from the beginning of the simulation in order to allow the convergence of the network.
Figure 10 shows that the proposed mechanism is more able to maintain a steady state compared with similar approaches. The BGP model takes more time before reaching the stability that have gone more than 1 min in this example. Otherwise, the proposed mechanism and the E2E recovery are able to ensure stability at nodes by reserving minimum amount of received packets before reaching the stable state. Eventually, the time needed for reaching this stable state is less then 60 s in two models. Furthermore, the proposed mechanism is able to reduce at most the overload of nodes by diminishing the number of received packets. The ratio factor of received packets between the E2E recovery model and the proposed model is over 1,11. It reaches a factor of 2,52 between the proposed mechanism and the BGP model.

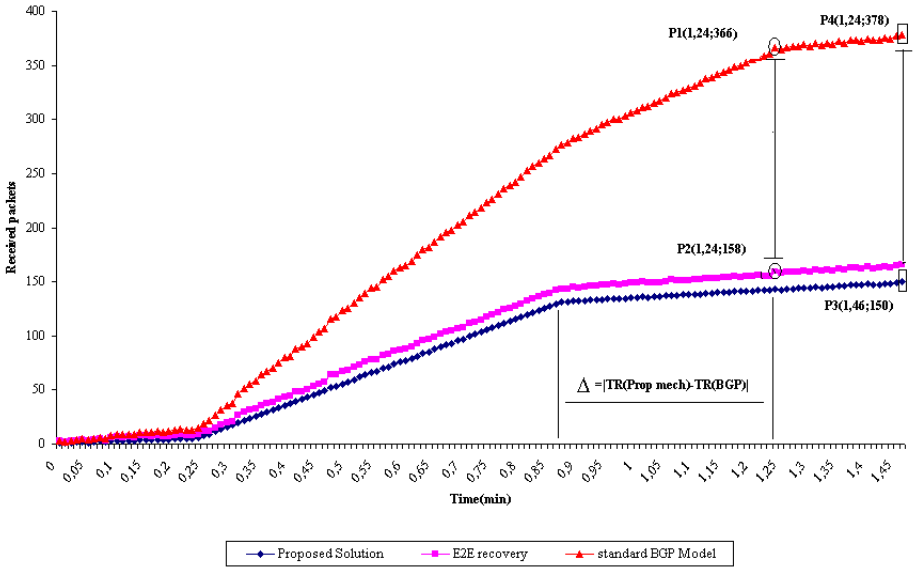

Figure 9: LSR^4_{AS2} overload using various recovery mechanisms

5. Conclusion

This paper deals with the E2E recovery issue on MPLS-based multi-domains networks. It presents a novel approach for failure handling and traffic protection despite heterogeneity and autonomy of crossed autonomous systems (AS). The proposed mechanism defines a reactive alternation between two Path computation procedures respectively called BRPC (Backward Recursive PCE Computation) and FRPC (Forward Recursive PCE Computation).
The FRPC is used even when the process of establishing E2E backup LSP tunnel reaches a domain to which the original working LSP Tunnel belongs to. Otherwise, the BRPC procedure is applied. The two procedures are based on a concatenation of per-domain path segment that, gathered together, define the E2E backup LSP tunnel. Furthermore, establishment of local segment path is ensured by specific entities called PCE (Path Computation Element). One PCE is denoted per domain. At FRPC call, the PCE should use locally defined databases (I-LSPDB and E-LSPDB defined accordingly to REEQoS approach) in order to find a combination of I-LSP and E-LSP, that together, can handle actual flows. Conversely, in the BRPC call, the PCE should transmit the request to the downstream domain and waits for responses before making decision on the convenient segment path. Decision is made using locally defined tree that exposes alternative paths rooted at the same Ingress node as the working LSP tunnel. This tree is called DBPT (Downstream backup path tree). Local DBPT and the DBPT received from the downstream domain are used to establish a resulting tree, which the PCE should transmit to its upstream PCE. The procedure is applied recursively until reaching the source domain. So, the PCE chooses the appropriate tunnel, basing on previous received trees and orders the new backup path to the ingress node which starts immediately flows rerouting.
Simulations have proved efficiency of the new mechanism in terms of resources utilisation and E2E performances. The proposed mechanism offers more reliability concerning time recovery and Packet loss. Moreover, this approach is able to support simultaneous points of failure since the mechanism is applied on an E2E scope. Scalability is also ensured since communication is limited to a PCE-to-PCE basis and does not include other LSRs into the establishment process. Finally, the proposed mechanism is able to recover from various types of failure: inter-domain link failure or border node failure. Indeed, our approach considers each of them as a failure point which

the process of backup LSP tunnel aims to bypass it.
Although the proposed mechanism offers opportunities to the E2E recovery issue, it does not consider locally-defined security-based constraints that may differs among domains. Operators should cooperate in order to alleviate privacy limitations when several messages for path computation are exchanged. Moreover, the proposed approach does not present any information on how PCEP messages are routed, mainly in an inter-domain context and how to map for equivalency between requested performances when crossing different ASs.

References

[1] Vijayanand, C., Bhattacharya, S. and Kumar, P., *BGP Protocol extensions for PCE Discovery across Autonomous systems*, Work in Progress, June 2007

[2] Y. Rekhter, T. J. Watson, and T. Li, *A border gateway protocol 4 (BGP4)* IETF RFC 1771, Mar. 1995.

[3] C. Labovits et al., *Delayed Internet routing convergence* IEEE/ACM Trans. Networking, vol. 9, no. 3, pp. 293-306, June 2001.

[4] Changcheng Huang and Donald Messier . *A Fast and Scalable Inter-Domain MPLS Protection Mechanism.* JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 6, NO. 1, MARCH 2004.

[5] A.Farrel, J-P Vasseur, A.Ayyangar,*A Framework for InterDomain MPLS Traffic Engineering.* Nov 2006, IETF RFC 4726

[6] Changcheng Huang and Donald Messier *Inter-Domain MPLS Restoration*, Design of Reliable Communication Networks (DRCN) 2003, Banff, Alberta. Canada, October 19-22, 2003

[7] Oki, E.; Inoue, I.; Shiomoto, K., *Path computation element (PCE)-based traffic engineering in MPLS and GMPLS networks* , Sarnoff Symposium, 2007 IEEE, April 30 2007-May,Page(s):1 - 5

[8] Q. Zhao, David Amzallag, Daniel King, *PCE-based Computation Procedure To Compute Shortest Constrained P2MP Inter-domain Traffic Engineering Label Switched Paths*, Internet-Draft, Mars 2009

[9] V. Sharma and F. Hellstrand, *Framework for multi-protocol label swtiching (mpls)-based recovery* 2003, request for comments: 3469

[10] El Kamel Ali and Youssef Habib; *an efficient hybrid mechanism for MPLS-based network*, accepted for publication in the 14th international Symposium on Computers and communications (ISCC09), July 5-8 2009, Tunisia.

[11] A.El Kamel and H. Youssef, *REEQOS: an RSVP-TE based approach for E2E QoS provisioning within MPLS domains*, VECOS2008, (Leeds UK 2-3 July 2008) published online within the British Computer Society(BCS)

[12] K. Kumaki , T. Murai , *PCEP extensions for a BGP/MPLS IP-VPN* , March 8, 2009 , Network Working Group,(Internet Draft) draft-kumaki-murai-pce-pcep-extension-l3vpn-02.txt,

[13] S. Matsushima, T.Murakami, K.Kenechi,*BGP extension for MPLS P2MP-LSP*, IEICE - Transactions on Information and Systems, Volume E89-D, Issue 1 (January 2006) , Pages 211-218

[14] C. Villamizar, R. Chandra, and R. Govindan, *BGP Route Flap Damping*, IETF RFC 2439,Nov. 1998.

[15] A.Awduche, L.Berger, T.Li, V.Srinivasan, G.Swallow,*RSVP-TE: Extension to RSV for LSP tunnels*, December 2001, IETF RFC3209

[16] A.Farrel, J-P Vasseur, A.Ashr, *A path Computation Element (PCE)-based architecture*, August 2006, IETF RFC 4655.

[17] S. Yasukawa, *Signaling Requirements for Point-to-Multipoint Traffic-Engineered MPLS Label Switched Paths (LSPs)*, April 2006,IETF RFC 4461

[18] J.P. Vasseur, J.L. Le Roux , *IGP Routing Protocol Extensions for Discovery of Traffic Engineering Node Capabilities*, December 2007, IETF RFC5073.

[19] Le Roux, J.L., Vasseur, J.-P., Ikejiri, Y., Zhang, R., *OSPF protocol extensions for Path Computation Element (PCE) Discovery*, RFC5088, January 2008.

[20] Le Roux, J.L., Vasseur, J.-P., Ikejiri, Y., Zhang, R., *IS-IS protocol extensions for Path Computation Element (PCE) Discovery*, RFC5089, January 2008.

[21] JP. Vasseur, JL. Le Roux, *Path Computation Element (PCE) Communication Protocol (PCEP)*, March 2009, IETF RFC5440.

[22] Q. Vohra, E. Chen, *BGP Support for Four-octet AS Number Space*, May 2007, IETF RFC 4893