REEQOS: An RSVP-TE approach for the End-to-End QoS provisioning within MPLS Domains

Ali El Kamel and Habib Youssef
Research Unit PRINCE
ISITCom of Hammam Sousse, University of Sousse, Tunisia.
{Ali.Elkamel@isima.rnu.tn ; Habib.Youssef@fsm.rnu.tn }

Abstract

This paper exposes a new approach, denoted REEQOS, for supporting QoS both in intra and inter-domain, generally named autonomous system (AS)[RFC 1771]. This approach is based firstly on MPLS technology and uses RSVP-TE extension (RFC 3209) for establishing two kinds of Label switched paths: I-LSP (Internal LSP) within every AS and E-LSP (External LSP) for inter AS routing. RSVP-TE is used in a local way (intra-domain level) to make pre-established LSPs that will be stored on a specific Database named LSPDB. The state of these LSPs is placed and updated periodically in another specific Database named LSPSDB. The same principle of managing LSPs is performed as well on internal environment as on external environment. Hence, we denote internal databases respectively I-LSPDB and I-LSPSDB and external ones respectively E-LSPDB an E-LSPSDB. REEQOS gives a way to support failure handling and explores RSVP-TE capability to define LSP recovery and resources re-optimization mechanisms. Accordingly to simulation results, REEQOS is proved to be an efficient approach for supporting End-to-End QoS without worry about heterogeneous crossed domains.

Keywords: IP networks, MPLS, Traffic Engineering (TE), RSVP-TE, E2E QoS.

1. INTRODUCTION

Today, the ability to ensure Quality of service requirements through IP networks is a major challenge facing Service providers (SP). Due to the expansion of Internet scales, the network is organized into several areas that are generally named Autonomous Systems (AS), each under the control of a single authority or administration. Hence, to be consistent and widely deployed, an inter-domain QoS-ensuring mechanism must be capable of handling domains heterogeneity and must enforce QoS requirements respectively for intra-domain and inter-domain. However, standard routing protocols such as OSPF [RFC 2328] and BGP [RFC 1771] do not convey any QoS information when performing data forwarding.

On the other hand, Traffic Engineering (TE) [RFC 3272] focuses on the performance optimization of networks, in order to achieve efficient utilization and load balancing of network resources. TE addresses an optimization problem of finding and maintaining 'best' end-to-end paths between source-destination pairs. However, a path may cross several heterogeneous domains where every domain imposes different QoS policies that should be taken into account when establishing end-to-end paths. Some solutions are made to resolve this problem such as RSVP (Resource Reservation Protocol) [RFC 3031] and RSVP-TE (RSVP with Traffic Engineering) [RFC3209, RFC3473]. However, most related work has focused on exploiting these techniques to ensure QoS provisioning within local boundaries of a single domain. The inter-domain issue hasn't yet received sufficient attention although it's a major factor of end-to-end QoS provisioning.

This document presents a new approach to ensure both intra and inter domain QoS. It's based on deploying two levels of monitoring and controlling schemes, intra-domain level and inter-domain level. The first one helps achieve a high-performance routing mechanism to ensure local QoS within one Autonomous System (AS). The second level focuses on routing data between AS's without performance degradation, nor service disruption. Our approach, as described later, uses the RSVP-TE extension to establish a control-level LSP tunnel. This tunnel is established at the AS level and is based on nested model [RFC 5151] which consists of a concatenation of two kinds of LSPs: internal LSP and External LSP. The two LSPs are joined in a hierarchical way to construct an H-LSP [RFC 5150].

This paper is structured as follows. First, we present some of the related work on the provisioning of inter-domain QoS. Section 3 focuses on the problem formulation and discuses weaknesses within previous work. Then, in Section 4 we present our solution. Performance results are presented in Section 5. We conclude in Section 6.

2. RELATED WORK

The inter-domain routing problem is being started by a framework for QoS-based Internet routing, adopting the traditional separation between intra- and inter-domain routing. This framework was defined by Crawley et al. [3]. They discussed the goals of an inter-domain QoS routing and the associated issues that must be addressed, and provided general guidelines that should be followed by any viable solution to QoS routing in the Internet. However, they did not specify the set of QoS metrics to be transported neither the algorithms for using such metrics in the choice of inter-domain routes. Hence, Xiao et al. [4] define a series of statistical metrics for QoS information advertisement and routing, adopted as well for inter-domain QoS and intra-domain routing. The main drawback within this approach is that it only supports one QoS metric, making it difficult to simultaneously satisfy different requirements, especially, internal requirements and external requirements. On an other hand, Prior [5] has focused on making abstraction of internal requirements and gives an extension to the BGP routing protocol conveying three different QoS metrics, and a path selection algorithm using a combination of these metrics. Although this approach has improved routing mechanisms by avoiding path congestion, it has been proved that this solution results in an important overhead and routes instabilities, due to much signaling messages used to establish and update virtual trunks between domains.

Further, Cristallo [6] proposes an approach for inter-domain traffic engineering which has been implemented under the name MESCAL (Management of End to end quality of Service in the internet At Large) [8]. This approach is based on pre-establishing roles for every AS. Then, traffic is forwarded based on its QoS class (QC-x). This approach gives an opportunity to the differentiated service issue and requires defining several consented QoS classes between all ASs. Such problem is the main drawback facing the practical implementation of this approach. Further, it was confirmed that this solution suffers from several bugs, since it does not address certain issues and behaviors like bandwidth reservation, multicast issues and security considerations [8].

3. PROBLEM ANALYSIS

To ensure E2E QoS, current inter and intra domain routing protocols must be QoS aware [7]. First, QoS across the internet can be achieved by employing respectively QOSPF [9,10] for internal process and QBGP[14] for external process. However, the model of QOSPF suffers from several deficiencies such as the lack of support of resources recovery. Further, QOSPF doesn't allow new techniques of traffic engineering, where it doesn't support resources optimization nor path computation as introduced in RSVP-TE. Such deficiency doesn't allow having a global view about traffic and paths states.

An inter-domain solution that supports QoS-based routing was introduced in the MESCAL approach [1], which uses a new enhanced protocol called Q-BGP [14]. Q-BGP is an enhanced version of the BGP (Border Gateway Protocol) [RFC 1771], which is widely used today for best-effort inter-domain routing.

Experiments have shown that using Q-BGP results in the discovery of improved QoS-aware routes across meta-QoS-class planes compared to using standard BGP. However, while the quantity of Q-BGP messages is greater than for plain BGP, experimental results indicate that, Q-BGP doesn't scale well to Internet-sized AS topologies. For large ASs the signaling overhead of A-BGP is more than three times that of BGP. The injection of static QoS information into BGP can have a detrimental effect on QoS if QoS resources are not engineered appropriately or if Q-BGP route selection policies are not carefully selected. However, Injecting dynamically measured QoS-information may alleviate this problem, but care must be taken to dampen route fluctuations to avoid instabilities.

Generally, most related work was focused on providing both inter and intra domain QoS using heterogeneous techniques in order to achieve E2E reliability. Such heterogeneity is proved to be a major factor for boundary inconsistency since several environment may be deployed at both inter and intra scheme. Worse, using assorted techniques needs provisioning miscellaneous controlling strategies in order to have a global overview of the E2E monitoring. Certainly, E2E monitoring should be done basing on homogenous techniques in order to alleviate incongruity among inter domain and intra-domain QoS provisioning processes.

4. REEQOS APPROACH

4.1 Terminology

The REEQOS approach is based on the following concepts:

MN: Master Node. There is one master node per AS whose role is to maintain state information about internal LSPs and external end-to-end LSPs.
I-Label: Internal label
E-Label: External label
L-LSR: Local Label Switching Router.
LFIB: Label forwarding Information Base.
ILSR: Ingress Label Switching Router.
ELSR: External Label Switching Router.
ILSPDB (resp. ELSPDB): Internal (resp. External) LSP Database. A database lodged at the Master Node which stores I-LSPs (resp. E-LSPs)
ILSPSDB (resp. ELSPSDB): Internal (resp. External) LSP state Database A database lodged at the MN that stores states of I-LSPs (resp. E-LSPs).
I-LSP (resp. E-LSP) Request: Internal (resp. External) LSP Request. A specific message used by ingress I-LSR (resp. E-LSR) node to request an Internal (resp. external) path through a local domain (resp. toward another domain).
I-label (resp. E-label) Response: I-Label (resp. E-Label) Response. A message used by an MN to return a selected label I-Label (resp. E-label) to the ingress node I-LSR (resp. E-LSR).
LEDB: Label equivalency Database: a database used both by I-LSP Manager and E-LSP Manager to associate E-labels with I-Labels.

4.2 Architecture of proposed Approach

REEQOS avoids major deficiencies in reported approaches. Both internal (within a domain) and external (between domains) QoS support is enabled using homogenous tools and techniques. REEQOS architecture is based on the use of MPLS technology [RFC 3031], coupled with RSVP-TE protocol, since they enable efficient routing with differentiated service support, balanced-resources utilization, and resources optimization. Hence, we assume that all nodes are MPLS speakers as well as RSVP-TE capable.
REEQOS approach is based on separating monitoring and signaling plane from forwarding plane. The first plane is guaranteed by master nodes (MNs). The MNs constitute a private backbone which we designate MN-backbone. Every MN should ensure two functions: the first function is related to intra-domain level and consists of monitoring and signaling pre-established LSPs within a local domain. The second function consists of ensuring inter-domain forwarding using Autonomous-System-Level LSP establishment.
REEQOS focuses on the setup of an End-to-End LSP Tunnel by joining two-level path segments using a hierarchical hybrid method of LSP signaling. This is done by considering local domains as abstract nodes. Hence, the initial topology, divided into several logical domains, will be viewed as a new topology where local domains are replaced by abstract nodes. Local behavior within every domain is omitted, and the focus is given to inter-domain management in the same way as it's done with intra-domain scheme.
Within an AS, every Ingress node should establish paths to all possible egress nodes of the AS using the protocol RSVP-TE [RFC3209]. The setup of paths is based on selective FEC (forwarding Equivalency Class) that may be locally supported. When a path is established, the ingress node should transmit the resulting Record Routing Object (RRO) to the MN. Then, the MN stores the received object into its I-LSPDB and I-LSPSDB and starts monitoring it. If traffic arrives at any ingress node, this node sends an I-LSP request to the corresponding MN, which consults its database to find an available path that can satisfy the flow resources requirements. Once found, the Label is returned to the ingress node using the I-Label response message.
As shown in Figure 1, when a source S desires to send data toward a destination D, it starts by requesting the establishment of a path to the nearest MN (we assume that the source knows the set of MNs which are in its neighborhood). Receiving this request, the MN uses RSVP-TE capability for supporting AS numbering to establish a path to the final destination. This path is established between MNs and doesn't focus on local domains. The main negotiation is done between MNs aiming to setup an E2E tunnel crossing several AS's. The problem of routing traffic within a domain is not treated at the setup process. This is performed at the forwarding level.

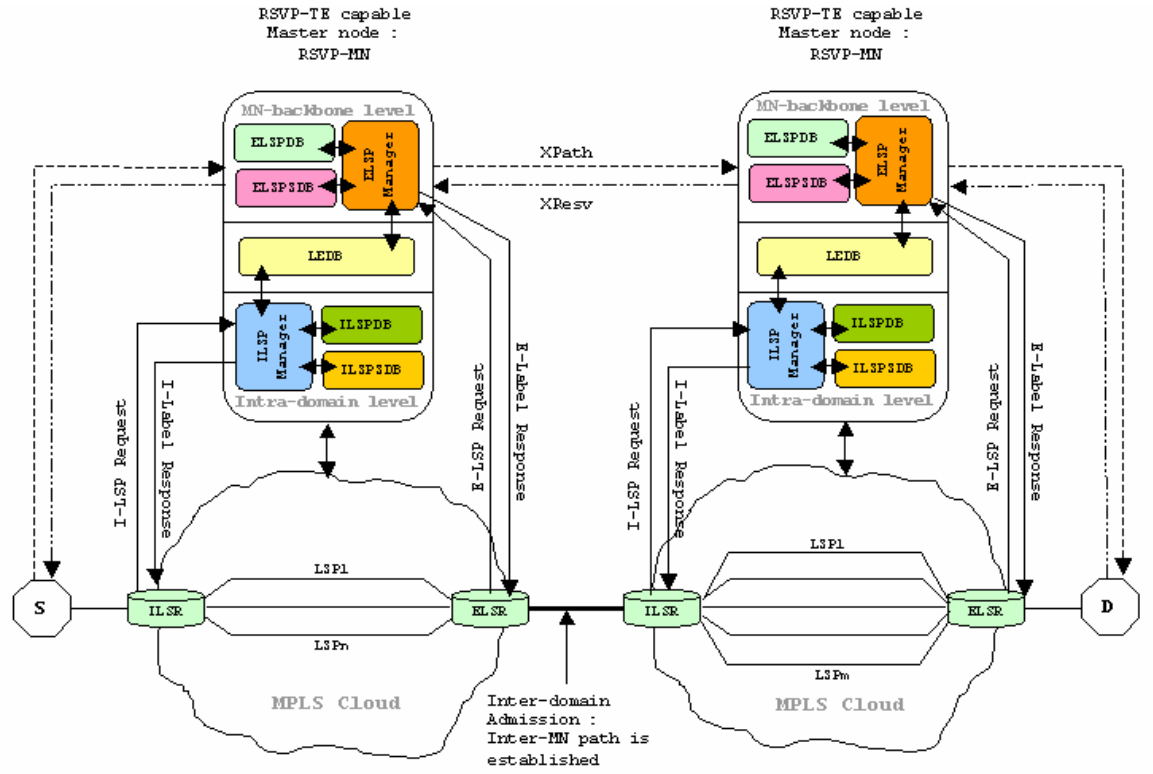

FIGURE 1: REEQOS Architecture.

The confirmation process of the established Path is initiated at the last AS which should use the Explicit Routing object to propagate confirmation message to the originating AS. We call this message XResv since it's inspired by the standard description of Resv Message.
When the source requires a path, no reservation is made within crossed AS's. The Tunnel resulting from an XPath establishment process is an RRO object composed only of sub objects containing the identifiers of crossed AS's. The E-LSP manager should co-operate with the I-LSP Manager when incoming traffic needs to cross an AS.

4.3 Hybrid signaling method for establishing end-to-end LSP tunnels

Started at a source, the traffic will receive an AS-level label. This label defines the starting point of the tunnel that the traffic should follow to reach the destination. The source should request a label (E-Label) by sending a PATH message to the nearest AS. Then, we consider that $E\text{-}Label_x$ is the label used to cross the x^{th} AS. The MN establishes an LSP using the stitched signaling model [RFC 5151] at the AS level.
When a flow needs to cross a local domain, the E-Label will not be withdrawn. The ingress node should request another label (I-label) that will be used to cross the local domain. The I-Label should be designed when the LSP tunnel setup is processed. Association between internal labels (I-label) and external labels (E-label) is defined in the LEDB. The I-Label is stacked over the E-Label to build an LSP stack as described by the Nested-LSP process defined in [RFC 4726].
For internal LSP establishment, we use contiguous LSP process [RFC 4726] to define paths connecting all ingress nodes to all egress nodes. This choice is justified by needs of global monitoring and scalability to manage the whole set of internal nodes.
At an ELSR, the I-label is pulled from the received packet. A Message request of NHOP (Next HOP) is transmitted by the ELSR to the appropriate MN. As a result, the MN returns an E-label that is used to reach the next AS. Fundamental problem of rerouting and failure support are treated later.

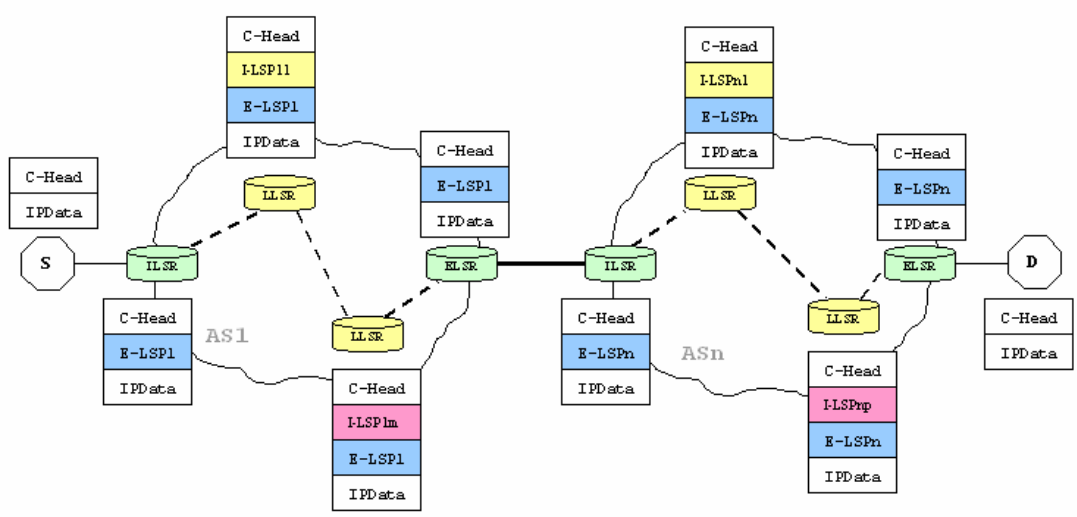

FIGURE 2: Hierarchical LSP setup of End-to-End LSP tunnel.

4.4 Autonomous LSPs tunnel setup: XPath/ XResv process

A path joining the source to the destination should be established using the hybrid method depicted in previous section. The source sends a path request to the nearest MN.
When it receives the Path request message, the MN should perform the following procedures in order to achieve end-to-end path establishment with QoS requirements support:
1. Carry out the policies expressed into the path request message and try to find the appropriate I-LSP that can supply policies requirements.
2. Neighborhood Discovery Mechanism (NDM): the MN should determine all the Master-Nodes that are in its neighborhood avoiding the MN from which it has received the path setup message. It may use the BGP-NLRI capability [12], or it can exploit the RSVP-TE extension with the introduction of Hello messages described in [RFC 3209].
3. NHOP selection (NHOPS) and Optimal NHOP selection (ONHOPS): the MN should send the Path setup request to all neighboring MNs. When it receives a path message, the neighboring MN tries to find an I-LSP that may support QoS requirements. Three possible cases can take place:
   a. The MN finds that an I-LSP can supply QoS requirements. In such case, it updates its databases with new path establishment and starts doing the same work done by the previous MN (2). It should also return an acceptance message to the previous MN. If the MN receives one acceptance message, it updates its E-LSPDB by indicating the egress node and the label that should be used to reach the NHOP AS. Else, if more then one acceptance message is received, the MN stores all of them in its E-LSPDB. Every E-LSP is associated with a label and an egress node. The combination of the egress node and the label defines the NHOP that should be used. Such solution can be useful to ensure Path recovery in a border node failure case or inter-AS link failure.
   b. As the Path establishment is processed, every crossed AS should wait for Resv message from the destination, or should wait a PathErr indicating “Path establishment failure”. It should then propagate the Resv/PathErr message to the Previous AS, or to the source if it’s an end point.

Upon the reception of the path message, the destination creates a Resv message that sends it through the reverse RRO object. This object is also included within the Resv message and will be used by every crossed MN to update/confirm the E-LSPDB.
At the reception of the Resv Message, every MN should carry out the RRO object and updates its E-LSPDB or confirm it. Every E-Label should be associated with an I-Label. The MN should store all paths in its LEDB which it uses to establish the H-LSP through the local domain.

4.5 LSP failure handling

REEQOS provides a way to handle setup failure. The standard RSVP-TE [RFC 3209] defines some specific messages that are used to support error notification between RSVP capable nodes. Some messages are exchanged between MNs through the MN-backbone in order to signal failures due to policy control [RFC2205] or

routing problems [RFC3209]. To avoid confusion between Local failure handling and Inter-domain failure handling, we denote Error message as XPathErr.
In a failure state, as no I-LSP can support actual QoS requirements, an XPathErr message is returned to the upstream MN revealing the error 'Policy control failure/ Intra-domain policy failure'. Previous MN waits for all responses before propagating the XPathErr message to the source. If none of requests has been accepted, the upstream MN considers a path-establishment failure and propagates an error 'Routing problem/ No route available toward destination' to the source.
When processing with the establishment of XPath, Every MN should determine and evaluate inter-domain links that are capable for supporting incoming flows based on their FEC. If any link can't support QoS policy requirements, the MN should propagate the error 'Policy control failure/ inter-domain policy failure' toward previous MN.
In order to ovoid time waste and to limit waiting period, the MN which sends the XPath message starts a timer that it uses to reject timeout-overcoming responses. If no XPathErr/Acceptance message is received, the MN should consider that the path can not be established due to unrecognized causes and propagates an XPathErr toward the source indicating the error 'Routing problem/ Reason Unknown'.

5. SIMULATIONS AND EVALUATIONS

In order to evaluate the performance aspect of our proposed approach, we have resorted to ns2 simulations. The first experiment is done to prove the efficiency of the approach REEQOS with respect to the time needed to establish end-to-end tunnels. All nodes are RSVP enabled. We have used a given RSVP-TE patch [I1, I4] introduced within ns2. We have introduced this extension so every node within the simulated topology becomes RSVP-TE speaker and, then, may support path establishment accordingly to several path setup models, especially nested model [RFC 3209].
Further, each MN is modeled by an agent. Every agent is RSVP-TE capable and uses the patch Network Management System (NMS) [I4]. We have also joined all those specific nodes by a direct link meaning that they constitute a specific backbone. Every MN-agent is associated with a specific database which defines pre-established I-LSPs. This database is implemented as a file that the agent can access to find the appropriate LSP. Respectively, External LSPs are stored within another file which presents external LSP database.

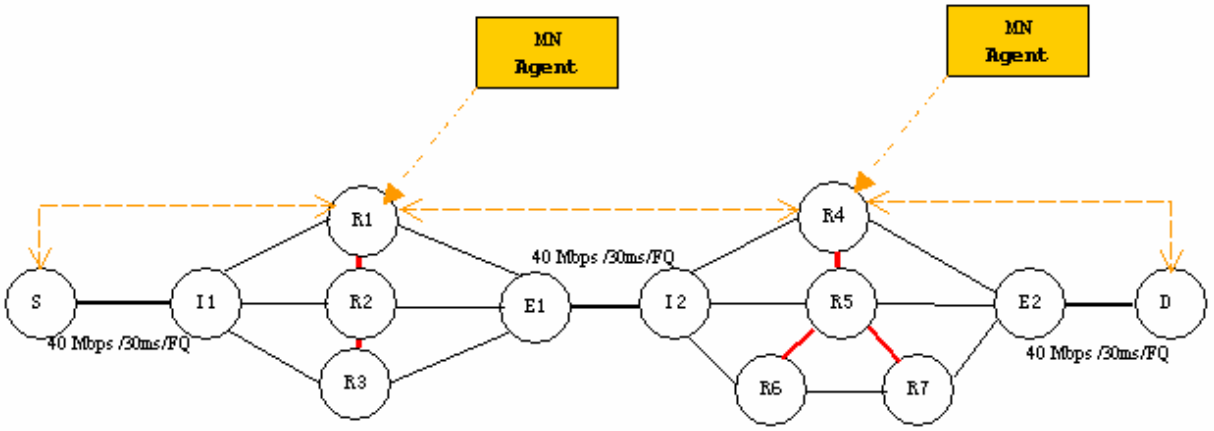

FIGURE 3 : Experimental topology

The experimental topology used is shown in Figure 3. We have assumed that we have one source and one destination. All experienced flows are forwarded from the source S toward the destination D. We have supposed also that we have two Autonomous systems AS1 and AS2. The two AS are constituted by one ingress node, one egress node and several core nodes. Table 3 gives an overview about all links attributes. We have assumed that we need to forward three kinds of flows: Best-effort flows (BE), Resource-constraint flows (Assured Forwarding, AF) and delay-constraint flows (Expedited Forwarding, EF). A description of internal pre-established LSPs within every AS is given below (Table 1).
First, we have focused on the time needed to establish End-to-End LSP tunnel. All considered flows are AF. Thus, the source S should requests an increasing number of LSP with the same FEC toward the destination. We have compared results with other approaches. Figure 4 shows that REEQOS takes less time to establish End-to-End

tunnels, especially when the number of requests is increasing. Our simulations were made for requests number varying in the interval [2-20]. The establishment of 20 LSP tunnels needs over 135 ms. However, using RSVP (based on stitched model), the same number of requests took 207 ms.
For three requests, the RSVP protocol ensures lowest time for establishing LSP tunnel. This is because available resources are not immensely requested by flows.

TABLE 1: Configuration of pre-established I-LSP

Autonomous System	AS ID	FEC		LSP ID	Explicit Route
AS1	1	AF	LSP1	1	I1,R1,E1
		EF	LSP2	2	I1,R2,R1,E1
			LSP3	3	I1,R2,R3,E1
		BE	LSP4	4	I1,R2,E1
AS2	2	AF	LSP1	1	I2,R4,R5,E2
			LSP2	2	I2,R4,R5,R7,E2
		EF	LSP3	3	I2,R6,R7,E2
			LSP4	4	I2,R5,E2
			LSP5	5	I2,R6,R5,E2
		BE	LSP6	6	I2,R6,R5,R4,E2
			LSP7	7	I2,R6,R5,R7,E2

However, when the number of request goes more than 3, the situation becomes more complex for RSVP to make decision about resources reservation, as they become less available. As the number of flows increases, the capability of RSVP to serve efficiently all requests is degraded. The capability of REEQOS to maintain scalability with End-to End LSP tunnel setup is due to its hierarchical management approach. Indeed, impact of internal failures is not propagated to external inter-domain links. The failure is handled internally without inter-domain performance decline. This is considered an asset of REEQOS approach.

TABLE 1: Experimental Links attributes

link	attributes
I1-R1	40 Mbps/60ms/DropTail
I1-R2	15Mbps/20ms/DropTail
I1-R3	10Mbps/80ms/DropTail
R1-R2	30Mbps/15ms/DropTail
R2-R3	30Mbps/15ms/DropTail
R1-E1	35Mbps/10ms/DropTail
R2-E1	30Mbps/70ms/DropTail
R3-E1	35Mbps/10ms/DropTail
I2-R4	35Mbps/25ms/DropTail

link	attributes
I2-R5	15Mbps/20ms/DropTail
I2-R6	20Mbps/15ms/DropTail
R6-R7	20Mbps/10ms/DropTail
R4-R5	40Mbps/40ms/DropTail
R5-R6	20Mbps/10ms/DropTail
R5-R7	35Mbps/25ms/DropTail
R4-E2	15Mbps/70ms/DropTail
R5-E2	35Mbps/15ms/DropTail
R7-E2	40Mbps/10ms/DropTail

In another simulation, we evaluate REEQOS with QoS-aware extensions of OSPF and BGP. These extensions are given by [I2]. Indeed, we have compared the time needed to setup End-to-End tunnel. Our simulation was made using two kinds of flows: AF and EF.

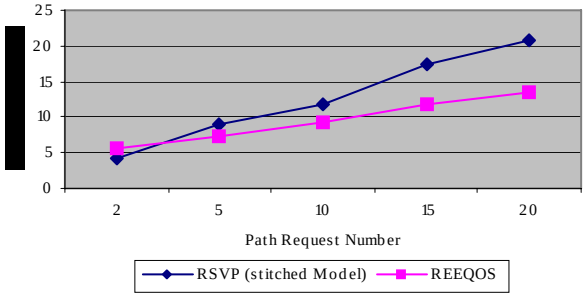

FIGURE 4: LSP Tunnel Setup time

Figure 5 shows that REEQOS ensures less time setup also using AF flows or EF flows. For a few number of requests, all approaches gives approximately the same time for E2E tunnel setup. However, more the number of requests is increasing, the standard enhanced-protocols need more time to establish E2E tunnel. For 20 requests the ratio variation between needed time is evaluated at 76,11% for AF. Respectively, the ratio variation between necessary time reached 81,91% for EF.

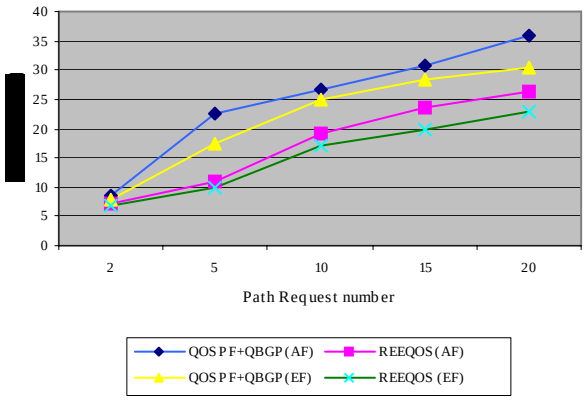

FIGURE 5: LSP Time Setup for AF and EF within various approaches

The next simulation consists on evaluating the delay needed to forward a given set of flows using three approaches: the standard QOSPF coupled with QBGP, the RSVP using stitched model and our approach, REEQOS.

We have generated 5 flows as follows: one BE, 2 EF and 2 AF. The two AF flows are VBR with a burst time of 500 ms, a generated packet size of 25 Mbits transmitted during the ON period at full link speed followed by an off period. The idle time is fixed at 20 ms. EF flows are also VBR with burst time of 100 ms , a generated packet size of 10Mbits and an idle time of 10 ms. BE flows are CBR with a rate of 20Mbps and a packet size of 10Mbits.

Although RSVP gives an important gain by reducing the delay variation between several kinds of flows, REEQOS seems to be more appropriate as it ensures more balanced delay among a set of flows that belongs to the same FEC.

However, as shown in figure 6, REEQOS does not give importance to BE flows and we have found that, for the new approach, the number of BE flows should be reduced as much as possible. Certainly, REEQOS is not appropriate to forward BE flows and should be avoided when the most routed flows are BE.

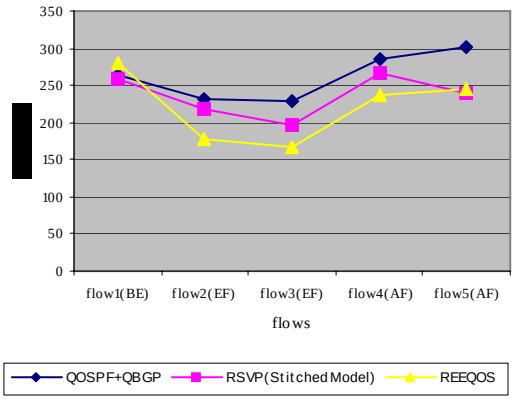

FIGURE 6: Delay within various approaches

REEQOS is appropriate to ensure delay balancing among flows having the same FEC. As noticed in the figure 6, the mean delay variation of AF is evaluated at 27,8 ms when using RSVP; however, it's roughly fewer than 9,9 ms for REEQOS. Similarly for EF, the variation is respectively 20,5 ms for RSVP and 12,1 ms for REEQOS.

6. CONCLUSION

This paper proposes a new approach for ensuring End-to-End QoS within multi-heterogeneous domains infrastructure. The new approach is called REEQOS. It's based on RSVP-TE which is used to ensure intra and

inter domain routing. Previous approaches are mainly based on extensions of standard IP protocols such as QOSPF and QBGP. Such extensions are introduced to satisfy QoS both in intra and inter-domain, using standard protocol enhancement.
REEQOS exhibited superior performance with respect to previous approaches. The improvement of new approach is mainly given by capabilities provided within RSVP-TE such as failure handling, failure recovery, and resources optimization. However, REEQOS doesn't result in performance improvement for BE traffics. Simulation results show that REEQOS penalizes BE traffic in the presence of AF and EF flows. This does not constitute a major drawback as long as we don't have starvation of BE flows.
More extensive simulations with large topologies are required. This work is in progress.

REFERENCES

[1] M.P. Howarth, P. Flegkas, G. Pavlou, N. Wang, P. Trimintzios, D. Griffin, J. Griem, M. Boucadair, P. Morand, H. Asgari and P. Georgatsos, "Provisioning for Inter-domain quality of service: the MESCAL approach" IEEE Communications Magazine, June 2005.
[2] M.Boucadair , "Meta-QoS-Class : a step toward global QoS inter-domain services", France Telecom R&D, October 2004.
[3] E. Crawley, R. Nair, B. Rajagopalan, and H. Sandick, "A framework for QoS-based routing in the Internet," RFC 2386 (Informational), Aug. 1998.
[4] L. Xiao, J. Wang, K.S. Lui, and K. Nahrstedt, "Advertising interdomain QoS routing information," IEEE J. Sel. Areas Commun., vol.22, no.10, pp.1949–1964, Dec. 2004.
[5] R. Prior, "inter domain QoS routing: Optimal and practical study", IEICE Trans. Commun., vol.E90–B, NO.3 march 2007
[6] G. Cristallo, C. Jacquenet, "An Approach to Inter-domain Traffic Engineering", Proceedings of XVIII World Telecommunications Congress (WTC2002), September 2002.
[7] K.H. Ho, N. Wang, P. Trimintzios, G. Pavlou ,"Traffic Engineering for Inter-domain Quality of Service", Centre for Communication Systems Research, University of Surrey, UK
[8] P. Morand, M.Boucadair, H.Asgari, R.Egan, M.Irons, J. Griem, D.Griffin, J.Spensor, P.Flegkas, P.Trimintzios, T Damilatis ,P.Georgatsos , " Issues in MESCAL Inter-Domain QoS Delivery: Technologies, Bi-directionality, Inter-operability, and Financial Settlements", Thales Research & Technology (TRT) UK Limited, January 2004.
[9] Eric S.Crawley , " QOSPF: Quality of Service Extensions to OSFP or Quality of Service Path First Routing" Bay Networks Inc.
[10] G. Apostolopoulos, D. Williams, S. Kamat, R. Guerin, A. Orda and T. Przygienda, "QoS Routing Mechanisms and OSPF Extensions," RFC 2676, August 1999.
[11] A.Beben , "EQ-BGP: an efficient inter-domain routing protocol ", Institue of telecommunication Warsaw university of Technology, Poland.
[12]. Cristallo, G., Jacquenet, C, " Providing Quality of Service Indication by the BGP-4 Protocol: the QOS_NLRI attribute", <draft- jacquenet-qos-nlri-00.txt>, Internat draft
[13] JP. Vasseur, Y. Ikejiri , R. Zhang, "Reoptimization of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) loosely routed Label Switch Path (LSP) ",<draft-ietf-ccamp-loose-path-reopt-02.txt>, NTT Communications Corporation, February 8, 2006
[14] M. Boucadair," QoS-Enhanced Border Gateway Protocol", <draft-boucadair-qos-bgp-spec-01.txt>, France Telecom R&D, July 2005.

Request for Comments

[RFC1771] Y. Rekhter, T.Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995
[RFC2328] J.Moy, "OSPF Version 2", RFC2328, April 1998
[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001
[RFC3036] L. Andersson,P. Doolan,N. Feldman, A. Fredette, B. Thomas,"LDP specification", RFC 3036, January 2001
[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.
[RFC3212] B.Jamoussi, L.Anderson, R.Callon,R.Dantu,P.Doolan, N.Feldman, A.fredette,M.Girish,E.Gray, J.Hainanen, T.Kilty, A.Malis," Constraint-Based LSP Setup using LDP",RFC3212,January2002
[RFC3272] D. Awduche, A. Chiu, A. Elwalid, X. Xiao, I. Widjaja, "Overview and Principles of Internet Traffic Engineering", RFC 3272, May 2002

[RFC3473] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", January 2003
[RFC4726] A. Farrel , J.-P. Vasseur, A. Ayyangar , A Framework for Inter-Domain Multiprotocol Label Switching Traffic Engineering, IETF Trust Nov 2006.
[RFC4736] Vasseur, JP., Ed., Ikejiri, Y., and R. Zhang, "Reoptimization of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Loosely Routed Label Switched Path (LSP)",RFC 4736 , November 2006.
[RFC5150] Ayyangar, A., Kompella, K., Vasseur, JP., and A. Farrel,"Label Switched Path Stitching with Generalized Multiprotocol Label Switching Traffic Engineering (GMPLS TE)", RFC 5150, February 2008.
[RFC5151] Farrel, A., Ed., Ayyangar, A., and JP. Vasseur, "Inter-Domain MPLS and GMPLS Traffic Engineering : Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 5151, February 2008.

Downloads

[I1] Hierarchical MPLS Patch for NS2 **:** *http://www.ideo-labs.com*
[I2] QBGP and QOSPF Patch for NS2.1b9; *http:// public.planetmirror.com/ pub/ sourceforge/ q/qo/*
[I3] Standard BGP-4 and compagnion OSPFv2 tool; *ftp://ftp.openbsd.org/pub/openBSD/OpenBGPD/*
[I4] RSVP-TE patch; Network Management Station NMS; *http://netgroup-serv.iet.unipi.it/rsvp-te_ns*