The NSIS QOS Model for Inter-domain Signaling to Enable End-to-End QoS Provisioning Over Heterogeneous Domains

Jian Zhang and Edmundo Monteiro*

Laboratory of Communications and Telematics (LCT), University of Coimbra
CISUC-DEI, Polo II, 3030-290 Coimbra, Portugal
{zhang and edmundo}@dei.uc.pt

Abstract. This paper describes a NSIS QoS Model for inter-domain signaling (InterDomain-QOSM) between adjacent domains to enable end-to-end QoS provisioning over heterogeneous network domains. Specifically, it assumes a distinct separation between the intra-domain control plane and the inter-domain control plane at each administrative domain and is intended to implement a common inter-domain control interface that allows the QoS negotiation and setup of inter-domain traffic streams while hiding the heterogeneity of intra-domain control mechanisms in use in a chain of heterogeneous network domains. The operation mode of the InterDomain-QoSM is first described and then the additional QSPEC parameters for fulfilling the common inter-domain interface are specified, followed by the illustrations of how the InterDomain-QOSM interacts with some typical intra-domain QoS models to achieve the end-to-end QoS provisioning over heterogeneous domains in a standardized and dynamic way.

1 Introduction

Although a number of QoS (Quality of Service) architectures (e.g., IntServ [1] and Diffserv [2, 3]) has been proposed by the Internet Community, there are still some barriers to overcome to realize the end-to-end QoS provisioning over heterogeneous network domains. Among them, one major barrier to the achievement of end-to-end QoS over heterogeneous environments is the lack of a standardized and dynamic approach to perform inter-domain QoS interactions between adjacent domains. To address this barrier, the consensus of the Internet community is that a distinct separation between intra-domain control plane and inter-domain control plane must be made and a common inter-domain control interface must be available at each administrative domain that allows the inter-domain interactions independent from intra-domain control mechanisms so that the QoS negotiation and setup of inter-domain traffic streams can be implemented in a standardized and dynamic way.

* This work has been supported by the European Commission under IST Project EuQoS

The IETF NSIS (Next Steps in Signaling) Working Group has been working on a generic signaling architecture [4] for the Internet since 2001, where the NSIS protocol suite is structured in two layers: a generic (lower) layer, termed NTLP (NSIS Transport Layer Protocol), which is responsible for moving signaling messages around and independent of any particular signaling applications it will transport; and an upper layer, termed NSLP (NSIS Signaling Layer Protocol), which contains functionality such as message formats and sequences, specific to a particular signaling application. Moreover, the QoS NSIS Signaling Layer Protocol (QoS-NSLP) [5] specifies a generic model for carrying end-to-end QoS signaling information in IP networks. Each network along the end-to-end path is expected to implement a specific QOSM (QoS Model) that interprets the requests and guides the necessary behaviors of the RMF (Resource Management Function) module of a QNE (QoS-NSLP aware NSIS node), in a manner that is appropriate to the technology in use in the network, to ensure the delivery of the requested QoS. RMD-QOSM [6] and Y.1541-QOSM [7] are examples of the QOSMs currently being developed by the NSIS Working Group, of which the RMD-QOSM describes a QoS model for DiffServ network domains that use the Resource Management in DiffServ (RMD) framework [8–10] and the Y.1541-QOSM describes a QoS model for networks that use ITU-T Y.1541 QoS Classes [11]. Note that the QoS-NSLP is designed to be able to signal QoS reservations, independent of the QOSM in use. All information specific to a QOSM is encapsulated in a separate QoS-NSLP object, the QSPEC, which is opaque to the QoS-NSLP and will be interpreted only by the RMF and the PCF (Policy Control Function) of a QNE. The NSIS QSPEC draft [12] is defining a template for the QSPEC, which contains a set of QSPEC parameters for both the QoS description and the QSPEC control information to ensure the interoperability of QOSMs.

This paper presents a NSIS QoS Model for inter-domain signaling (InterDomain-QOSM) which aims at implementing a common inter-domain interface between adjacent domains so that the inter-domain interactions can be realized in a standardized and dynamic way to facilitate the end-to-end QoS provisioning over heterogeneous network domains. In particular, the operation model of the InterDomain-QOSM is presented and the additional QSPEC parameters for fulfilling the common inter-domain control interface are specified, followed by the illustrations of how the InterDomain-QOSM interacts with some typical intra-domain QoS models to achieve the end-to-end QoS provisioning over heterogeneous network domains in a standardized and dynamic way.

2 Definitions and Terms

Some terms used throughout this paper are defined below.

A ***SLA*** (Service Level Agreement) is concluded between a customer and a provider, where the customer can be a end-user or a peer provider. A SLA providers a guarantee that traffic offered by a customer that meets certain stated

conditions, will receive one or more particular service levels. The guarantees may be hard or soft, may carry certain tariffs, and may also carry certain monetary or legal consequences if they not met.

A ***SLS*** (Service Level Specification) contains the technical details of the agreement specified by a SLA. A SLS has, as its scope, the acceptance and treatment of traffic meeting certain conditions and arriving from a end-user or a peer provider. Two types of SLS (and subsequently of SLAs) are distinguished here: *cSLS* (*customer SLS*) established between end-users and providers and *pSLS* (*peer SLS*) established between peer domains, presumably (logically) adjacent, where one domain is the service provider and the other domain is the customer.

A ***inter-domain control agent*** is a domain-wide centralized agent at an administrative domain, which implements a common inter-domain control interface and is responsible for the inter-domain interactions between adjacent domains via the common inter-domain interface.

A ***intra-domain control agent*** denotes an abstract entity which is responsible for performing all intra-domain control mechanisms in a manner appropriate to the specific network technology in use at an administrative domain. Note that it can be implemented in a centralized or distributed mode, i.e., a single domain-wide intra-domain control agent (centralized mode) or a set of local intra-domain control agents (distributed mode).

3 The Distinct Separation of Intra-domain Control Plane and Inter-domain Control Plane

To facilitate the realization of end-to-end QoS provisioning over heterogeneous network domains, one consensus of the Internet community is that a distinct separation between the intra-domain control plane and the inter-domain control plane must be made and a common inter-domain control interface must be available at each administrative domain that allows the inter-domain interactions independent from the intra-domain control mechanisms and the QoS negotiation and setup of inter-domain traffic streams implemented in a standardized and dynamic way [13].

Fig. 1 shows a high-level view of such distinct separation made at two adjacent domains. More specific, at each administrative domain, the intra-domain control agent is responsible for performing all intra-domain control mechanisms in a manner appropriate to the network technology in use at the domain and the inter-domain control agent implements a common inter-domain control interface and is responsible for the inter-domain interactions with its peer via the common inter-domain interface. Note that the intra-domain control agent shown in Fig. 1 is an abstract entity, which can be implemented in a centralized or distributed mode, i.e., via a single domain-wide intra-domain control agent (centralized mode) or a set of local intra-domain control agents (distributed mode). Whereas, the inter-domain control agent is normally (or always) implemented in a centralized mode, i.e., a network-wide centralized inter-domain control agent exists

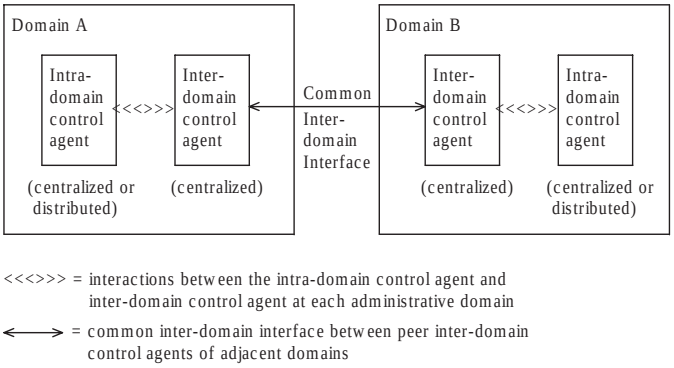


Fig. 1. The high-level view of the inter-domain interactions between two adjacent domains where the distinct separation between the intra-domain and inter-domain control planes is made and a common inter-domain control interface exists.

at each domain, which is well-known to the intra-domain control agent(s) at its domain.

3.1 The Requirements of the Inter-domain Control Plane

The requirements of the inter-domain control plane (i.e., the functions provided by the inter-domain control agent in Fig. 1) which is required to implement a common inter-domain control interface to facilitate the support of end-to-end QoS provisioning over heterogeneous network domains are summarized below. Note that they are derived closely based on the ones outlined by the proposed Diffserv Control Plane Elements (DCPEL) BOF in its document [13].

The Requirements of the Inter-domain Control Plane:

- A common inter-domain control interface, which allows the QoS negotiation and set-up of inter-domain traffic streams while hiding intra-domain characteristics from inter-domain interactions (i.e., independent from the specifics of the intra-domain control plane), must be implemented by the inter-domain control plane.
- Signaling Communications over the common inter-domain interface must be made based on a well-understood information model for SLSs. This model should allow the definition of different degrees of SLSs, from per-flow, more suitable for end-hosts or small networks, to per-aggregate, more suitable for large networks. It should also allow the identification of the SLS validity and a set of time periods over each the SLS must be available (activated), besides the information about the QoS characteristics.
- The inter-domain control plane at each domain must be able to keep established and/or available/offered pSLSs. The pSLS is associated with the identity of the network domain offering or requesting the SLS.

- The inter-domain control plane must allow network domains negotiate and set up pSLSs between adjacent domains. Policy information specific to the requester, or other general policies must be checked to determine if the requested SLS can the accepted.
- The inter-domain control plane at each domain must be able to ensure that the traffic streams its domain sends are in conformity with the established agreement. Packets might need to be re-marked from one internal traffic class identifier to the inter-domain SLS identifier, which then might need to be re-marked from the inter-domain SLS identifier to another internal traffic class identifier used at its adjacent domain.
- The inter-domain control plane should be able to support the QoS query, request, response and monitor operations in a chain of heterogeneous network domains on a per-flow or per-aggregate basis via the common inter-domain control interface.
- The inter-domain control plane should be able to support the automatic inter-domain adjustment in the scenario of mobile end customers.

4 The Overview of the NSIS InterDomain-QOSM

The InterDomain-QOSM described in this paper assumes the distinct separation between the intra-domain control plane and the inter-domain control plane at each administrative domain and then tries to fulfill the above requirements of the inter-domain control plane by implementing the inter-domain control agent (see Fig. 1) through specifying a NSIS QOSM. The operation model and the basic features of the InterDomain-QOSM are presented below, respectively.

4.1 The Operation Model of the InterDomain-QOSM

The operation model of the InterDomain-QOSM is illustrated in Fig. 2, where at each administrative domain, the domain-wide centralized inter-domain control agent implements the NSIS InterDomain-QOSM and the intra-domain control agent is an abstract entity which can deploy any intra-domain QoS model (e.g., centralized or distributed, NSIS based or non-NSIS based). Moreover, the inter-domain control agent is located at a well-known QNE at its domain where the QoS-NSLP is stateful and the path-coupled or path-decoupled NTLP are both possible to be used to discover its peers at the adjacent domains. Note that the InterDomain-QOSM assumes that the pSLSs between the adjacent domains have been established or discovered by some other protocols (e.g., QoS-aware BGP protocol) and maintained at the inter-domain control agent; the negotiation and setup of pSLSs between adjacent domains are out of the scope of the InterDomain-QOSM currently.

Then, the QoS requests originating from an intra-domain QoS trigger will be processed first by the intra-domain control agent at its domain and when the requests need the supports of other domains (i.e., this domain is not the destination

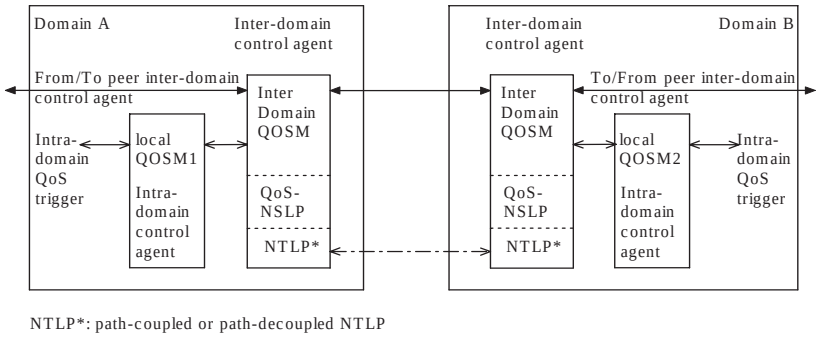


Fig. 2. The operation model of InterDomain-QOSM.

one), they will be forwarded to the inter-domain control agent which can facilitate the end-to-end QoS provisioning over heterogeneous network domains automatically and dynamically through the standardized hop-by-hop inter-domain interactions with its peers.

4.2 Basic features of InterDomain-QOSM

The basic features of the InterDomain-QOSM described in this paper include:

- The SLS parameters and QoS control information required for the inter-domain QoS interactions are specified by using/extending the QSPEC template in [12].
- The InterDomain-QOSM resides on top of the QoS-NSLP [5] and NTLP [4], which means that it uses the messages, objects and procedures defined by the QoS-NSLP for signaling exchanges with other QNEs and depends on the NTLP to discover the peer inter-domain control agents at the adjacent domains.
- The InterDomain-QOSM makes no assumptions about the implementation mechanisms of intra-domain control agent. That is to say that the intra-domain control agent might be centralized or distributed, NSIS based or non-NSIS based.
- The InterDomain-QOSM makes no assumption about the method that the underlying NTLP might use to discover the peer inter-domain control agents at adjacent domains.

The QoS-NSLP has defined four types of messages to deal with the QoS signaling operations. The RESERVE message is used to create, refresh, modify or remove the QoS-NSLP operation states and the reservation states of the deployed QOSM. The QUERY message is used to request information about the data path or probe the network information for support of certain QOS models without making a reservation. The RESPONSE message is used to provide information

about the result of a previous QoS-NSLP message. The NOTIFY messages are used to convey unsolicited information to another QNE.

5 The Description of InterDomain-QOSM

5.1 Additional QSPEC Parameters for InterDomain-QOSM

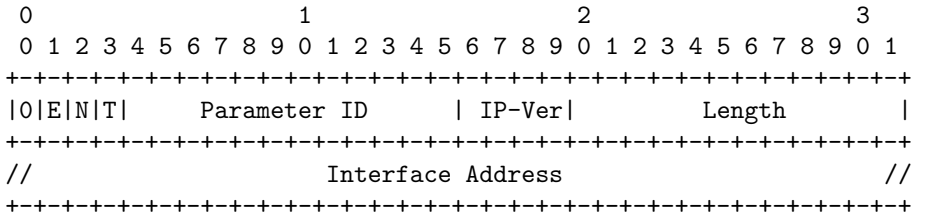
As mentioned before, the NSIS QSPEC template draft [12] has defined a set of QSPEC parameters for both the QoS description and the QSPEC control information to try to ensure the interoperability of existing QOSMs. However, to efficiently support the InterDomain-QOSM, some additional QSPEC parameters need to be defined. First of all, a new parameter termed <Ingress Border Router> that contains the IP interface of the ingress border router from which the signaled traffic stream will be admitted into the adjacent downstream domain need to be added to the QSPEC object <QSPEC Control Information> of the QSPEC template.

Secondly, to describe the time periods over which a SLS will be available or activated, the following <Time Specification> parameters need to be added to the QSPEC objects <QoS Desired>, <QoS Available>, <QoS Reserved> and <Minimum QoS> of the QSPEC template.

$$< TimeSpecification > = < AbsoluteTimeSpecification > | \\ < RelativeTimeSpecification >$$

The formats of the above new QSPEC parameters are presented below, which follow the general QSPEC formats defined in [12]. Note that, the first word (32 bits) of any QSPEC parameter is the parameter header; its Parameter ID field contains the ID the IANA assigns to the parameter and its Length field indicates the total number of words in this parameter after the parameter header itself.

<Ingress Border Router> parameter



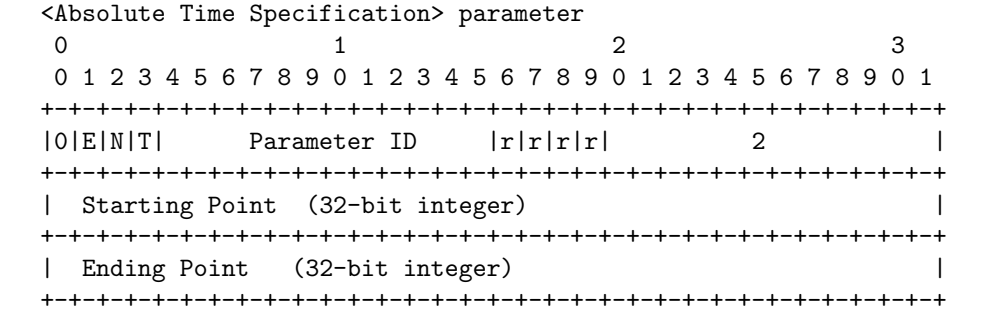
E flag: if this flag is set, it indicates that an error has occurred when this parameter was interpreted.

N flag: if this flag is set, it indicates that at least one QNE this signaling message has crossed through can not support this parameter.

T flag: it is set only when a signaling message is tunnelled through a domain and the egress QNE of the domain can not update this parameter correctly.

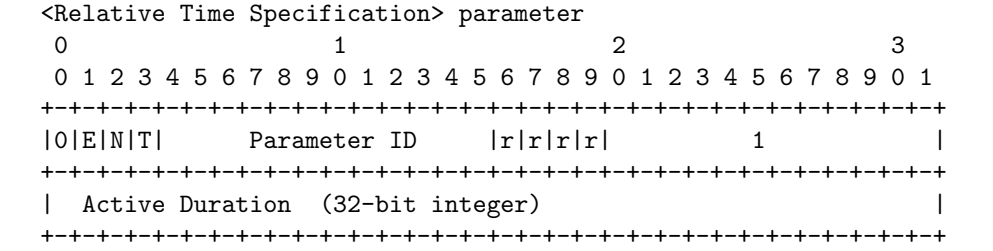
where the Interface Address field specifies the IP interface of the ingress border router of the adjacent downstream domain where the signaled traffic stream will be accepted. The Length field will depend on which version (IPv4 or IPv6) of IP address is used. It is an optional QSPEC control information parameter.

<Absolute Time Specification> parameter



where E, N and T flags have the same meanings as the above and the fields Starting Point and Ending Point specify the absolute time values of the starting and ending points of a time period over which a SLS described by other QSPEC parameters will be available or need to be activated, respectively. The format of the absolute time values follow the one defined by the IETF Network Time Protocol. Moreover, both of them must be nonnegative and are measured in microseconds. Now they are represented as a 32-bit integer and can be changed afterwards if necessary. It is an optional QSPEC QoS description parameter.

<Relative Time Specification> parameter



where E, N and T flags have the same meanings as the above and the Active Duration field specifies the length of a time period over which a SLS described by other QSPEC parameters will need to be activated. It must be nonnegative and is measured in microseconds. Now it is represented as a 32-bit integer and can be changed afterwards if necessary. It is also an optional QSPEC QoS description parameter.

5.2 The Discovery of Peer Inter-domain Control Agent

Mainly, the discovery of peer inter-domain control agent can be performed either by using the specific discovery method described at this new NSIS draft or manual configuration or any other discovery techniques. The InterDomain-QOSM makes no assumptions about that.

5.3 Illustrations of the Interactions of the InterDomain-QOSM with Some Typical Intra-domain QoS Models

Several inter-domain interaction scenarios are illustrated below to show how the InterDomain-QOSM operates to facilitate the realization of end-to-end QoS provisioning over heterogeneous network domains. Note that the purpose of the illustrations is not the enumeration of all possible scenarios, instead it aims to demonstrate the operation model presented in section 2.3 by deploying some typical intra-domain QoS models at adjacent domains. Moreover, throughout this section, we assume that Domain B is adjacent to Domain A along the direction towards the flow destination and the *pSLS* between Domain A and B has already been in place. Furthermore, for the case that a non-NSIS QoS Model is deployed at a domain, currently we assume that the domain deploys a domain-wide centralized intra-domain control agent and the inter-domain and intra-domain control agents will reside together and they interact with each other via a set of standardized APIs.

Case 1: inter-domain signaling when RMD-QOSM deployed at Domain A and Y.1541-QOSM at Domain B

When an egress QNE at Domain A receive a local QoS-NSLP RESERVE message to inform it of the successful reservations at this domain, it should construct a InterDomain-QOSM QSPEC based on the QSPEC of the original RESERVE message it received. Specifically, the InterDomain-QOSM QSPEC contains all the QSPEC parameters from the original QSPEC as well as one new parameter that specifies the IP interface of the ingress border router via which the signaled traffic flow will be accepted into domain B. Then, the egress node sends a new RESERVE message with this InterDomain-QOSM QSPEC to the well-known inter-domain control agent at its domain, which will maintain the IP interfaces of the above egress node and ingress border router via the support from the underlying NSIS GIST. Then, the inter-domain control agent at Domain A will check that whether the requested SLS at the InterDomain-QOSM QSPEC fits in the pSLS between Domain A and Domain B. If there is a positive outcome, the inter-domain control agent at Domain A will forward the received RESERVE message to its peer at Domain B.

When the inter-domain control agent at Domain B receives a RESERVE message, it should first extract the <Ingress Border Router> parameter and the SLS parameters from the InterDomain-QOSM QSPEC and then perform the following actions:

a. Authenticate that the RESERVE message is indeed from a peer.
b. Check that the requested SLS fall within the pSLS with Domain A.
c. Determine whether the reservation request may be accepted (possibly according to the policies of the domain).

In case that all these decisions have positive outcomes, the inter-domain control agent at Domain B will modify the received RESERVE message (e.g.,

remove the <Ingress Border Router> parameter from the InterDomain-QOSM QSPEC and add its authentication information) and send it to the ingress node of Domain B (this ingress node is discovered via the extracted <Ingress Border Router¿ parameter>. Next, the intra-domain QoS operations at domain B will be proceeded in the same way as described in [7].

When an egress QNE at Domain B receives a local QoS-NSLP RESERVE message which indicates that the requested reservations have been made successfully at this domain, it means that Domain B is a transit domain. For this case, the egress QNE at Domain B should first discover the IP interface of the ingress border router of its next downstream domain for the signaled flow, construct a InterDomain-QOSM QSPEC based on the received QSPEC and the IP interface of the discovered ingress border router and then send a new RESERVE message with the InterDomain-QOSM QSPEC to the inter-domain control agent at Domain B to signal a new inter-domain interaction request.

For the case that Domain B is the destination domain, a QoS-NSLP RESPONSE message will be created and propagated in Domain B to indicate the result of the above RESERVE message. When the RESPONSE message reaches the ingress node of Domain B, it will forward this RESPONSE message to the well-known inter-domain control agent at its domain. After the inter-domain control agent determines that the RESPONSE message is indeed from an authorized node, it will send the RESPONSE to its peer at Domain A, which will then forward it to the stored egress node where the signaled traffic stream flows out of Domain A. Next, the propagation of the RESPONSE message at domain A will follow the same rules as defined in [6].

Case 2: inter-domain signaling when RMD-QOSM deployed at Domain A and non-NSIS QOSM at Domain B

The operations at Domain A and the inter-domain interactions between Domain A and B are exactly the same as described in Case 1. Moreover, after the inter-domain control agent at Domain B receives a RESERVE message from its peer at Domain A, it will take the same actions as the above. In case that all the actions have positive outcomes, the inter-domain control agent will send the extracted SLS parameters and the IP interface of the ingress border router where the signaled traffic stream will be admitted into Domain B to the intra-domain control agent via the standardized APIs. Next, the intra-domain control agent will apply its intra-domain control mechanisms to the requested SLS.

For the case that the requested QoS reservations have been made successfully at Domain B and Domain B is a transmit domain, the intra-domain control agent should send a positive response plus the requested SLS parameters and the IP interface of the ingress border router of next downstream domain where the signaled traffic flow will traverse to the inter-domain control agent so that the inter-domain control agent can perform the inter-domain interactions with its peer at next hop domain.

For the case that Domain B is the destination domain, the intra-domain control agent just needs to send its response to the request to the inter-domain

control agent, which will forward the response to Domain A by sending a QoS-NSLP RESPONSE message to its peer at Domain A. Next, the propagation of the RESPONSE message at domain A will follow the same procedures as described in Case 1.

Case 3: inter-domain signaling when non-NSIS QOSM deployed at Domain A and Y.1541-QOSM at Domain B

When the intra-domain control agent successfully makes the QoS reservations for a traffic flow, it will send the inter-domain control agent an inter-domain reservation result with the SLS parameters describing the QoS requirements of the flow and the IP interface of the ingress border router via which the flow will be admitted into Domain B. Note that we make no assumptions about how the intra-domain control agent at domain A can discover the IP interface of that ingress border router of Domain B and currently several mechanisms can be used.

When the inter-domain control agent at Domain A receives the request, it will construct a InterDomain-QOSM QSPEC based on the received SLS parameters and the IP interface of the ingress border router of domain B and send a new RESERVE message with the InterDomain-QOSM QSPEC to its peer at domain B.

As long as the inter-domain control agent at domain B receives the RESERVE message, it will first extract all contained parameters from the InterDomain-QOSM QSPEC and then perform the same actions as described above. In case that all the actions have positive outcomes, the inter-domain control agent will modify the received RESERVE message (e.g., remove the <Ingress Border Router> parameter from the InterDomain-QOSM QSPEC and add its authentication information) and send it to the ingress node of Domain B. Next, the intra-domain QoS signalling operations at domain B will be proceeded in the same way as described in [7].

For the case that Domain B is a transit domain, the egress QNE at Domain B will take similar actions as described in Case 1 to signal to its inter-domain control agent the inter-domain QoS reservation request.

For the case that Domain B is the destination domain, a QoS-NSLP RESPONSE message will be created and propagated in Domain B. After the RESPONSE message is forwarded to the inter-domain control agent at Domain A, it will be sent to the intra-domain control agent via a API call. After that, the intra-domain control agent at Domain A can inform the flow sender the result of the reservation request by using its specific intra-domain signaling mechanisms.

The above illustrations show that although different intra-domain QoS models (centralized or distributed, NSIS based or non-NSIS based) might be deployed at a domain, the inter-domain interactions can be performed in a standardized way as long as the InterDomain-QOSM is used by the inter-domain control agent, which facilitate the realization of end-to-end QoS provisioning over heterogeneous network domains.

6 Discussions

The InterDomain-QOSM in this paper assumes the concept of distinct separation between the intra-domain control plane and the inter-domain control plane at each administrative domain and aims at realizing the QoS negotiation and set up of inter-domain traffic streams in a standardized and dynamic way that is independent from the intra-domain control mechanisms in use at each domain by utilizing the IETF NSIS protocols. In other words, it can be used with any kind of intra-domain QoS models, no matter they are centralized or distributed, NSIS based or non-NSIS based. The current solution provided by the IETF NSIS WG for fulfilling the end-to-end QoS provisioning over heterogeneous domains requires that all nodes across the whole chains of heterogeneous domains must be NSIS QoS-NSLP capable (i.e., must support QoS-NSLP) and the edge nodes must be able to support all NSIS QOSMs used by the chains of domains. Apparently, this is very hard to be satisfied in the heterogeneous IP networks like Internet. Whereas, for the InterDomain-QOSM presented in this paper, only the inter-domain control agent at each domain need to be NSIS QoS-NSLP capable and in case that a NSIS intra-domain QOSM is deployed at a domain, the edge nodes at the domain need to support only the NSIS intra-domain QOSM and the InterDomain-QOSM.

The domain-wide centralized inter-domain control agent could become the bottleneck and failure point of the end-to-end network control architecture. The traditional hot standby of the inter-domain control agent can be used to improve its availability. Moreover, the NSIS protocol suites (QoS-NSLP and NTLP) have provided some mechanisms like soft states and refreshing to discover the routing path change (in this paper, means the inter-domain routing path change) and node failure effectively. Furthermore, after the message association (i.e., the TCP connection) is established between two inter-domain control agent peers by using the NSIS handshake mechanisms, it can be reused by the subsequent inter-domain interaction requests and normally only one message association is needed, which significantly improves the scalability of the InterDomain-QOSM.

In the end, the usage of NSIS protocols in mobile environments is being addressed by this NSIS draft now [14]. We will study the support of automatic inter-domain adjustment in the scenario of mobile end customers by utilizing its mechanisms. Additionally, we are aware that more QSPEC parameters might be needed for the InterDomain-QOSM as more discussions and studies proceed.

7 Conclusions

A new NSIS QoS Model for inter-domain signaling (InterDomain-QOSM) is proposed in this paper, which aims at implementing a common inter-domain interface between adjacent domains so that the inter-domain interactions for provisioning end-to-end QoS over heterogeneous network domains can be realized in a standardized way, independent of the specific intra-domain control mechanisms in use at each domain. In particular, the operation model of the

InterDomain-QOSM is presented and the additional QSPEC parameters for realizing the common inter-domain control interface are specified. Moreover, the interactions between the InterDomain-QOSM and some typical intra-domain QoS models are described to demonstrate the InterDomain-QOSM's capability of achieving the end-to-end QoS provisioning over heterogeneous network domains in a standardized and dynamic way. The advantages and disadvantages of using the InterDomain-QOSM for inter-domain signaling are also discussed. We will set up the test bed to evaluate its performances quantitatively in the near future.

References

1. Wroclawski, J.: The Use of RSVP with IETF Integrated Services. RFC 2210, September 1997.
2. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An Architecture for Differentiated Services. RFC 2475, December 1998.
3. Nichols K., Jacobson V., Zhang L.: A Two-bit Differentiated Services Architecture for the Internet: RFC 2638, July 1999.
4. Hancock, R., Karagiannis, G., Loughney, J., Van den Bosch. S.: Next Steps in Signaling (NSIS) Framework. RFC 4080, June 2005.
5. Manner, J., Karagiannis, G., McDonald, A., Bosch, S.: NSLP for Quality-of-Service signaling. IETF NSIS Working Group, work in progress.
6. Bader, A., et. al.: RMD-QOSM - The Resource Management in Diffserv QOS Model. IETF NSIS Working Group, work in progress.
7. Ash, J., et. al.: Y.1541-QOSM – Y.1541 QoS Model for Networks Using Y.1541 QoS Classes. IETF NSIS Working Group, work in progress.
8. Westberg, L., et al.: Resource Management in Diffserv (RMD): A Functionality and Performance Behavior Overview. IFIP PFHSN'02.
9. G. Karagiannis, et al.: RMD - a lightweight application of NSIS. Networks 2004, Vienna, Austria.
10. Marquetant A., Pop O., Szabo R., Dinnyes G., Turanyi Z.: Novel Enhancements to Load Control - A Soft-State, Lightweight Admission Control Protocol. Proc. of the 2nd Int. Workshop on Quality of Future Internet Services, Coimbra, Portugal, Sept. 24-26, 2001, pp. 82-96.
11. ITU-T Recommendation Y.1541: Network Performance Objectives for IP-Based Services, May 2002.
12. Ash, J., et. al.: QoS-NSLP QSPEC Template. IETF NSIS Working Group, work in progress.
13. Mendes, P., Nichols, K.: Requirements for DiffServ Control Plane Elements. draft-mendes-dcpel-requirements-00 (work in progress), July 2006.
14. Lee, S., Jeong, S., Tschofenig, H., Fu, X., Manner, J.: Applicability Statement of NSIS Protocols in Mobile Environments. draft-ietf-nsis-applicability-mobility-signaling-04 (work in progesss), March 2006.