NSIS Working Group
Internet-Draft
Expires: April 2007

J. Zhang
Queen Mary, Univ. of London
E. Monteiro
University of Coimbra
P. Mendes
DoCoMo Euro-Labs
G. Karagiannis
University of Twente
J. Andres-Colas
Telefonica I+D

InterDomain-QOSM: The NSIS QOS Model to Fulfill the E2E QoS Control in the ITU-T RACF Functional Architecture

<draft-zhang-nsis-interdomain-qosm-03.txt>

Status of this Memo

Copyright Notice

Abstract

This document has three goals. First of all, it presents our analysis of how to use the NSIS signaling (inter-domain QOSM and intra-domain QOSM) to fulfill the QoS control in accord with the ITU-T RACF functional architecture. For this goal, we discuss how the ITU-T RACF entities in the ITU-T RACF functional architecture can be mapped to the NSIS entities and how the RACF reference points can be implemented by using the NSIS protocol suites and QOSMs. Secondly, we aim at specifying an NSIS Inter-domain QOSM for E2E QoS control across heterogeneous IP networks and applying this Inter-domain QOSM to the e2e QoS control in the ITU-T RACF functional architecture based on the above ITU-T RACF analysis. The detailed description of the NSIS Inter-domain QOSM are given and the e2e QoS control scenarios in the ITU-T RACF architecture (including RACF Push and Pull resource control modes), which will be covered by the NSIS Inter-domain QOSM are described and implemented. Thirdly, we specify and implement those QSPECs that will be used by the Inter-domain QOSM for the e2e QoS control in the ITU-T RACF architecture.

Table of Contents

1. Introduction

Although lots of efforts (e.g., IntServ [RFC2210] and Diffserv [RFC2475], [RFC2638]) had been made by the Internet community to address efficient Quality-of-Service (QoS) support in IP networks, there are still some barriers to overcome before the end-to-end QoS

provisioning can be truly enabled over heterogeneous IP networks across different operators' ASs (Autonomous System). Among them, one major barrier to the achievement of end-to-end QoS over heterogeneous environments is the lack of a standardized and automatic approach to perform inter-operator-domain QoS interactions between adjacent ASs while hiding the heterogeneities of the intra-domain QoS control mechanisms in use at each operator domain. To fully address this barrier, we believe that a distinct separation between the intra-domain QoS control plane and the inter-domain QoS control plane within each AS must be made, an interface between the intra-domain and inter-domain QoS control planes at the AS must be clarified and standardized, and an interface between the peer inter-domain QoS control planes at adjacent ASs must be standardized and implemented in a way that the network operator's internal confidentials don't need to be exposed. With the above separation and interfaces, the automatic QoS negotiation and setup of inter-domain traffic streams over a chain of heterogeneous network domains will be enabled in a standardized and dynamic way, fully independent from the intra-domain QoS mechanisms in use at each AS.

Recently, the ITU-T has been working on the standardization of the Next Generation Network (NGN) by proposing its definitions of the functional architecture, reference points and procedures of NGN across the service control, resource control and transport stratums. Among them, the ITU-T Y.RACF [Y.RACF] presents the requirements of QoS control over heterogeneous networks and defines the resource and admission control functional architecture and reference points for QoS control across end-to-end path. However, the implementation of the functional architecture and those reference points is untouched in the ITU-T Y.RACF document.

Meanwhile, the IETF Next Steps in Signaling (NSIS) Working Group proposed a flexible IP signaling solution [RFC4080] for the Internet, where the NSIS protocol suite is structured in two layers: a generic (lower) layer, termed NSIS Transport Layer Protocol (NTLP), which is responsible for moving upper-layer signaling messages between NSIS entities and is independent of any particular signaling applications on top of it; and an upper layer, termed NSIS Signaling Layer Protocol (NSLP), which contains functionality such as upper-layer message formats and sequences, specific to a particular signaling application. Currently, the General Internet Signaling Transport (GIST) protocol [GIST] provides a concrete solution for the NTLP. Moreover, the QoS NSIS Signaling Layer Protocol (QoS-NSLP) [QoS-NSLP] defines message types and generic QoS control information for supporting the QoS signaling application together with a class of QoS Models (QOSM). A QOSM defines the detailed QoS-related procedures and operations (e.g., negotiation, setup, update and release of network resources) to achieve the requested QoS target in a manner that is consistent with either the QoS control mechanism used at a network domain (intra-domain QOSM) or between adjacent operator domains (inter-domain QOSM). The RMD-QOSM [RMD-QOSM] and Y.1541-QOSM [Y.1541-QOSM] are examples of the NSIS based intra-domain QOSMs.

This document has three goals. First of all, it aims at analyzing how to use the NSIS signaling protocol suites to realize the end-to-end QoS control across heterogeneous network domains in accord with the ITU-T RACF functional architecture. For this purpose, we study how the RACF entities in the ITU-T RACF functional architecture can be mapped to the NSIS entities and how the RACF reference points can be implemented by using the NSIS protocols. Furthermore, we propose to seperate the inter-domain QoS control clearly from the intra-domain QoS control and apply different NSIS QOSMs (NSIS inter-domain and intra-domain QOSMs) to them. With this approach, the QoS negotiation and setup of inter-domain traffic streams over a chain of heterogeneous operator domains can be fulfilled in a standardized and transparent way, fully independent from the intra-domain QoS mechanisms at each AS. By transparent, we mean that operators do not have to reveal any details about the internal function of their networks, including the used QoS signalling protocols.

Secondly, this document aims at specifying the above NSIS Inter-domain QOSM and applying it to the e2e QoS control in the ITU-T RACF functional architecture. The detailed descriptions of how the NSIS Inter-domain QOSM will support the e2e QoS control under the ITU-T RACF Push and Pull resource control modes are presented along with its interactions with different intra-domain QOSMs. The NSIS QSPEC objects that will be used to carry the necessary information elements between the ITU-T RACF reference points are also defined.

The structure of this specification is as follows. Section 2 defines terminology, and Section 3 gives an overview of inter-domain signaling requirements for end-to-end QoS control and then describes the aims and scopes of this draft document. Section 4 presents the analysis of applying the NSIS signaling to QoS control in the ITU-T RACF functional architecture and the basic features of our proposed InterDomain-QOSM are summarized in Section 5. The detailed descriptions of the InterDomain-QOSM, such as the QSPEC [NSIS-QSPEC] parameters, the operation modes and the signaling procedures and operations for fulfilling the e2e QoS control, etc, are presented in Section 6. In addition, Section 7 discusses the security consideration raised by the InterDomain-QOSM and the IANA considerations are given in Section 8. Finally, we discuss some open issues related to the mapping between the ITU-T RACF entities and the NSIS entities and some details of the InterDomain-QOSM in Section 9.

2. Terminology

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

The terminology defined by GIST [GIST], QoS-NSLP [QoS-NSLP] and ITU-T Y.RACF [Y.RACF] applies to this draft.

In addition, the following terms are used:

Edge node: Node on the boundary of an administrative domain.

Ingress node: Edge node that handles the traffic as it enters the domain.

Egress node: Edge node that handles the traffic as it leaves the domain.

Inter-domain QoS controller: Abstract entity which is responsible for the inter-domain control mechanisms within its administrative domain, in cooperation with its logically adjacent domains via a common inter-domain interface. Depending on the kind of domain (size, network technology, method used to assure the intra-domain QOS, etc.), the inter-domain QoS controller can be implemented in a fully centralized, fully distributed or hybrid (i.e. an intermediate approach between fully centralized and fully distributed) mode. Please refer to Section 4.1 for the details of the implementation modes.

Intra-domain QoS controller: 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. As happens with the inter-domain control agent, it can be implemented in a centralized, decentralized or hybrid mode.

Customer: Business entity which has the ability to subscribe to the services offered by providers.

Provider: Business entity which owns an administrative domain and is

responsible for its operation, especially for the provision of Internet connectivity.

Service Level Agreement (SLA): Contract between a customer, which can be an end-user or an administrative domain, and an administrative domain, which acts as a provider, where the provider guarantees that traffic offered by a customer meeting 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 are not met.

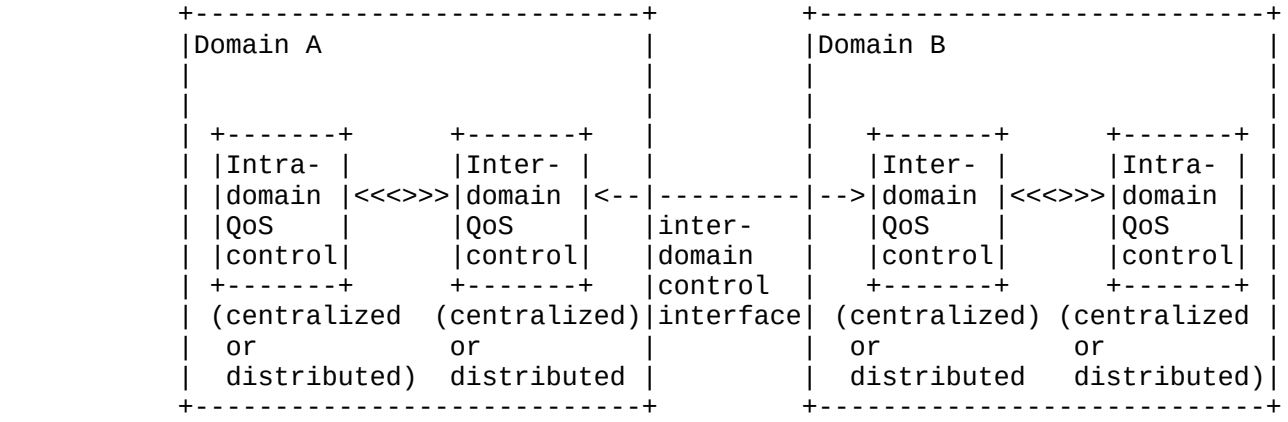
Service Level Specification (SLS): Technical details of the agreement specified by a SLA. A SLS has, as its scope, the acceptance and treatment of traffic meeting certain conditions and arriving from a certain customer.

3. Overview and Requirements of Inter-domain Signaling for End-to-End QoS Control

There are scenarios that can increase their data forwarding performance by separating the control plane heavy processing from the data forwarding processing. Such scenarios are for example, described in [draft-hancock-nsis-pds-problem-03], which achieve this separation by implementing outsourcing. The outsourcing takes place when nodes located on the data forwarding give over either the complete or a part of their control plane responsibilities, such as resource management, to one or more central controlling entities. Such scenarios are able to use signaling that can propagate off path towards the central controlling entities.

Several off path signaling scenarios can be distinguished, but in this draft we mainly concentrate on the path decoupled type of signaling, where signaling messages can travel on path but they might also be transferred to nodes off the data path. Off path signaling can be realized by using GIST, which can support path decoupled signaling, see [draft-hancock-nsis-pds-problem-03] and an inter-domain QOSM that in combination with the QoS-NSLP realizes a distinct separation between the intra-domain control plane and the inter-domain control plane at each administrative domain. Furthermore, the inter-domain QOSM can specify, by using a QSPEC, a common inter-domain interface between adjacent domains so that the inter-domain interactions will be fulfilled in a standardized and dynamic way to facilitate the realization of end-to-end QoS provisioning over heterogeneous network domains.

Figure 1 shows a high-level view of such distinct separation made at two adjacent domains. More specific, at each administrative domain, the intra-domain QoS controller 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 QoS controller 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 both the intra-domain and inter-domain QoS controllers shown in Figure 1 are the abstract entity, which can be implemented in a centralized or distributed mode (see Section 5.1). Moreover, the interface between the intra-domain and inter-domain QoS controller within a domain is standardized in this document.



<<<>>> = standardized interface between the intra-domain and inter-domain QoS controller within an administrative domain
<----> = common inter-domain interface between peer inter-domain QoS controllers at adjacent domains

Figure 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.

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 Figure 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 [DCPEL-requirements] and from some of the requirements provided in [Y.RACF].

Before listing the Inter-domain Control Plane requirements we will list a number of high level requirements when the overall NSIS signaling has to be used in supporting the ITU-T Y.RACF [Y.RACF] functional architecture.

Some of these requirements are copied/taken from [Y.RACF] and are:

* Control the QoS-related transport resources within NSIS aware networks and at the network boundaries in accordance with their capabilities;

* Support CPE's differing intelligence and capabilities;

* Support resource and admission control within a single administrative domain and between administrative domains;

* Support both relative QoS control and absolute QoS-control;

* Verify resource availability on an end-to-end basis;

* Support QoS differentiation over various categories of packet traffic including packet-type flows and user policies;

* Support QoS signaling

* Authorize requests for QoS and operate only on the authorised requests for QoS;

* Support distributed and centralized transport resource control architectures.

The resource and admission control functional architecture should meet the following optional high-level requirements:

* Support methods for resource-based admission control

* Have access to and make use of information provided by network management on performance monitoring to assist in making resource-based admission decisions;

* Have access to and make use of the network status information provided by the underlying network infrastructure in support of end-to-end QoS when transport functions detect and report a failure;

* Make use of the service priority information for priority handling (e.g., admission control based on service priority information). This includes passing of service information between entities where applicable;

* Support path selection (using NSIS discovery mechanism) between ingress and egress points within a single domain to satisfy QoS resource requirements.

The Requirements of the Inter-domain Control Plane are:

o 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.

o 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 SLSs. The SLS 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 SLSs 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;

  * support the automatic inter-domain adjustment in the scenario of mobile end customers;

  * support both relative QoS control and absolute QoS control;

  * verify resource availability within its purview;

  * support QoS differentiation over various categories of packet traffic including flows and user designations;

  * operate only on authorized requests for QoS;

  * make use of the service priority information for priority handling;

  * have access to make and use of information provided network management and performance management related to resource control;

* support path selection (using NSIS discovery mechanism) between ingress and egress points within a single domain.

* support distributed and centralised resource control architectures;

* support the following QoS resource control modes:

  a) Push mode: the policy and resource management decisions are pushed towards the intra-domain control plane

  b) Pull mode: the policy and resource management decisions are requested by the intra-domain control plane upon receiving path coupled signaling.

* QoS resource control should meet the following operational requirements:

  * support methods for resource usage and/or QoS treatments

  * have access to make and use of information provided network management and performance management related to resource control

  * support path selection (using NSIS discovery mechanism) between ingress and egress points within a single domain.

o The inter-domain QoS resource control process should consists of three logical states:

* Authorization: QoS resource is authorized based on operator specific policy rules

* Reservation: QoS resource is reserved based on authorized resource and resource availability

* Commitment: QoS resource is committed for the requested real time flows

3.2 The Aims and Scope of this draft

First of all, an analysis will be done on how to use NSIS signaling, in combination with inter-domain QOSMs and intra-domain QOSMs to realise the QOS control in accordance with the ITU-T RACF functional architecture, see [Y.RACF]. This can be accomplished by analysing how the Y.RACF entities in the ITU-T Y.RACF functional architecture can be mapped to NSIS aware entities and how the ITU-T RACF reference points can be implemented by using the NSIS protocol suites.

Secondly, it is aimed to specify an NSIS Inter-domain QOSM for end-to-end QOS control across heterogeneous IP networks and apply this Inter-domain QOSM to the end-to-end QoS control in the ITU-T Y.RACF functional architecture according to the above described ITU-T RACF analysis. This can be accomplished by presenting the detailed description of the NSIS Inter-domain QOSM and the end-to-end QoS control scenarios used in the ITU-T RACF functional architecture which are supported by the NSIS Inter-domain QOSM should be specified in detail.

Furthermore, this draft aims to specify those QSPEC objects that can be used by the Inter-domain QOSM for the end-to-end QoS control in the ITU-T Y.RACF architecture. This can be accomplished by specifying the QSPEC objects that will be used to carry the informational elements to implement the necessary interfaces of the Inter-domain QOSM.

The scope of the draft covers the definition of the interface between the intra-domain and inter-domain QoS control planes within a domain and the definition and implementation of the inter-domain interface between peer inter-domain QoS control planes at adjacent domains by specifying the InterDomain-QOSM. Note that both these interfaces are mapped from the similar interfaces used in the ITU-T RACF architecture. For the case that non-NSIS solutions are used as the intra-domain QoS control mechanism, the implementation of RACF Rd reference point for the interactions between the intra-domain and inter-domain QoS control planes within an AS has to be specified by that non-NSIS solution, which is left to other drafts to address.

4. The Analysis of Applying the NSIS Signaling to QoS Control in the ITU-T RACF Functional Architecture

4.1 Overview

The ITU-T RACF document [Y.RACF] defines the functional architecture and reference points for the resource and admission control functions at each AS (see Figure 2, which is copied from Figure 5 of [Y.RACF]), which includes the SCF (Service Control Functions), PD-FE (Policy Decision Functional Entity), TRC-FE (Transport Resource Control Functional Entity), TRE-FE (Transport Resource Enforcement Functional Entity), PE-FE (Policy Enforcement Functional Entity) and NACF (Network Attachment Control Functions). The CPE/CPN (Customer Premises Equipment/Customer premises Equipment) may be connected to the PE-FE in access network domains and the PE-FE can reside at the

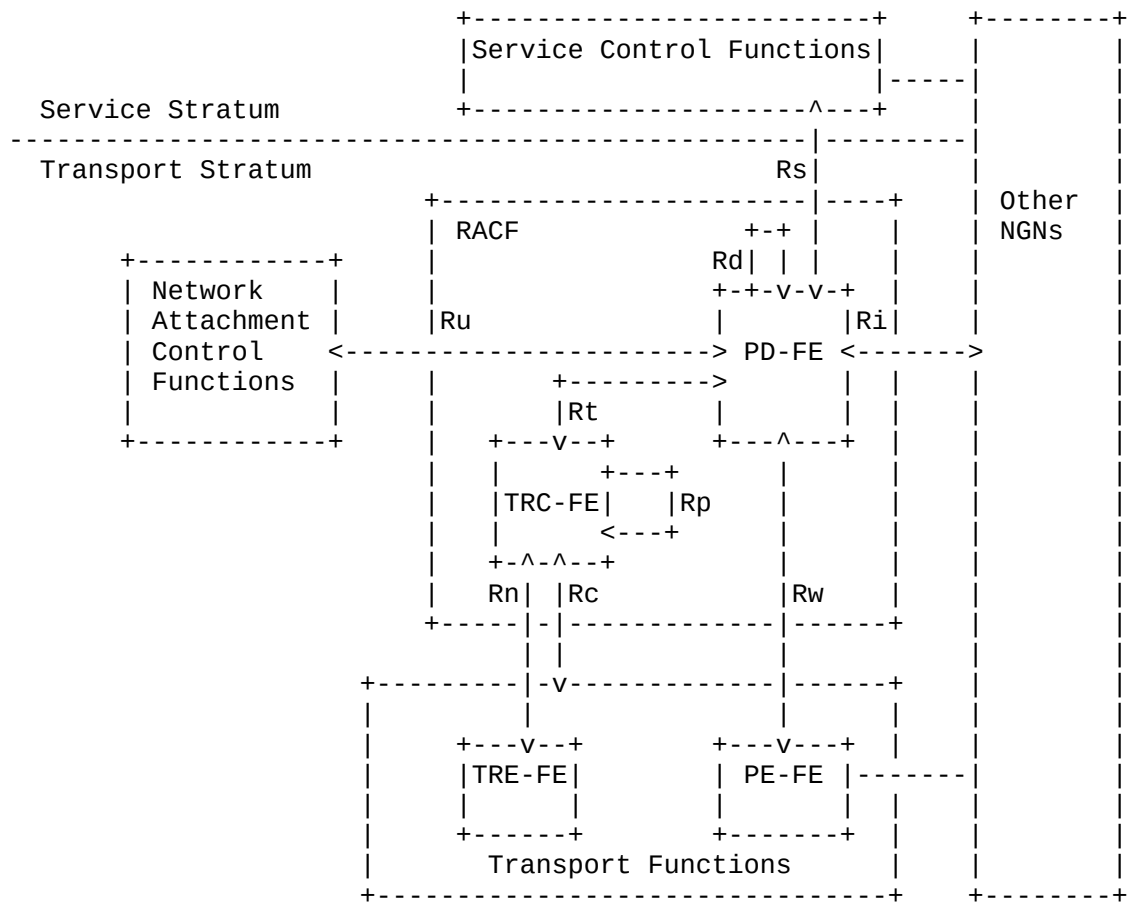


Figure 2: ITU-T RACF functional architecture

network boundary to interconnect with other NGNs. Other NGNs may include access networks only or core networks only or both them. The transport functions could also apply to access networks and core networks. The ITU-T RACF consists of two types of resource and admission control functional entities: the PD-FE and the TRC-FE. The PD-FE provides a single contact point to the SCF and hides the details of transport network to the SCF. The PD-FE makes the final decision regarding network resource and admission control based on network policy rules, SLAs, service information provided by the SCF, transport subscription information provided by the NACF in access networks, and resource-based admission decision results provided by TRC-FE. The PD-FE controls the gates in the PE-FEs at per flow level. Note that the PD-FE consists of transport technology-independent resource control functions and is independent of the SCF as well. The policy rules used by PD-FE are service-based and are assumed to be provided by the network operators.

The TRC-FE deals with the diversity of underlying transport technologies and provide the resource-based admission control decision results to PD-FE. The TRC-FE is service-independent and consists of transport technology-dependent resource control functions. The PD-FE requests the TRC-FE instances in the involved transport networks through the Rt reference point to detect and determine the requested QoS resource along the media flow path. The TRC-FE may collect and maintain the transport network topology and the transport resource status information and authorize resource admission control of a transport network based on network information such as topology and/or connectivity, network and element resource availability, as well as the transport subscription information in access networks. Moreover, in the ITU-T RACF functional architecture, the implementation and physical configuration of the PD-FE and TRC-FE are flexible: they can be distributed or centralized, and may be a stand-alone device or part of an integrated device; the PD-FE may contact only one designated TRC-FE instance, and then TRC-FE instances communicate with each other through the Rp reference point to detect and determine the requested QoS resource from edge to dege in the involved network, or the PD-FE may contact multiple TRC-FE instances and determine the requested QoS resource from edge to edge.

In addition, in the ITU-T RACF functional architecture, the SCF represents an abstract notion of the functional entities in the service stratum of NGN that request the QoS resource and admission control for media flows of a given service via the Rs reference point; the NACF includes a collection of functional entities that provide a variety of functions for user access network management and configuration based on the user profiles; the PE-FE in the transport stratum is a packet-to-packet gateway at the boundary of different packet networks and/or between the CPE and access network; the TRE-FE in the transport stratum enforces the transport resource policy rules instructed by the TRC-FE at the technology-depedent aggregate level. Currently, the scope and functions of the TRE-FE and the Rn reference point in [Y.RACF] are for further study. Furthermore, an inter-domain reference point Ri is designated to support inter-operator domain PD-FE communication for e2e QoS control when the QoS requirements for a given service can not be passed over the end-to-end path through application layer signaling. However, there are no any details of Ri in [Y.RACF], which are still for further studies.

As we can see from the ITU-T RACF document, it defines only the RACF functional architecture and reference points to ensure the inter-operability of the QoS and resource control within heterogeneous network environments but leaves the implementations of them untouched deliberately. Meanwhile, the IETF NSIS Working Group proposed a flexible IP signaling architecture [RFC4080] for IP networks, where different NSIS QOSMs can be defined to realize heterogeneous QoS control mechanisms used at underlying network

domains. This section presents an analysis of how to fulfill the e2e QoS control in accord with the definitions of the ITU-T RACF functional architecture and reference points by using the NSIS protocol suites. More importantly, we adopt the idea of distinct separation between the intra-domain and inter-domain QoS control planes at each AS to realize the standardized and transparent inter-operator-domain QoS interactions while hiding the heterogeneities of the intra-domain QoS control mechanisms. By transparent, we mean that operators do not have to reveal any details about the internal function of their networks, including the used QoS signalling protocols. The analyses of applying the NSIS inter-domain QOSM for the inter-domain QoS control and applying the NSIS intra-domain QOSM for the intra-domain QoS control in the ITU-T RACF functional architecture are discussed in this section, respectively. Finally, the mapping between the ITU-T RACF entities and the NSIS entities is given based on the analyses.

4.2. The Analysis of Applying the NSIS Intra-domain QOSM for Intra-domain QoS Control in the ITU-T RACF Functional Architecture

In order to analyse how the NSIS Intra-domain QOSM concept can be applied and used by the ITU-T RACF architecture, a list with the ITU-T RACF functional entities and their features is given in subsections 4.2.1.1 to 4.2.1.6. Section 4.2.1.7 presents the QoS features that can be supported by the CPE. Subsequently, in Section 4.2.1.8, the typical NSIS intra-domain QOSM features will be compared with the features supported by the ITU-T RACF functional entities.

4.2.1 The ITU-T RACF functional entities

As mentioned in Section 4.1, the RACF functional entities specified in [Y.RACF] include: Service Control Function (SCF), Network Attachment Control Functions (NACF), Policy Decision Functional Entity (PD-FE), Transport Resource Control Functional Entity (TRC-FE), Policy Enforcement Functional Entity (PE-FE), Transport Resource Enforcement Functional Entity (TRE-FE).

The texts given in the subsections 4.2.1.1 to 4.2.1.7 are copied from [Y.RACF].

4.2.1.1 Service control functions

The following texts are copied from [Y.RACF].

"The SCF in different domains can interact with PD-FE via the Rs reference point. The SCF makes requests for transport resources and may receive notifications when resources are reserved and released.

* The SCF shall provide information to the PD-FE to identify media flows and their required QoS characteristics (e.g., service class, bandwidth).

* The SCF may provide service priority information to the PD-FE to facilitate appropriate priority handling (e.g., priority processing of the resource request, resource pre-emption if needed).
* The SCF may request resource usage information through the PD-FE for charging or other usage metering.
* The SCF may provide service information to the PD-FE to facilitate appropriate dynamic firewall working mode selection.
* The SCF shall indicate when the resource is to be committed (i.e. opening gate and allocating bandwidth). A resource may either be committed immediately or just reserved for a later commitment.
* When a NAPT function is required, the SCF shall request address binding (mapping) information and perform required modifications in signalling messages. This includes any address information modifications that may be required for binding.
* When the pull mode along with a path-coupled resource reservation mechanism is used, the SCF shall indicate to the PD-FE whether it should be notified when resources are reserved, modified and released.
* When an authorisation token mechanism is used, the PD-FE may provide the SCF one or multiple authorisation tokens, which shall be included in a signalling message to CPE.", from [Y.RACF]

4.2.1.2 Network Attachment Control Functions (NACF)

The following texts are copied from [Y.RACF].

"Network attachment control functions (NACF) provide the following:

* Dynamic provision of IP address and other user equipment configuration parameters.
* Authentication of user access network, prior or during the IP address allocation procedure.
* Authorisation of user access network, based on user profiles (e.g., access transport subscription).
* Access network configuration, based on user profiles.
* Location management.

The PD-FE in the access network interacts with the NACF via the Ru reference point to obtain the transport subscription information and the binding information of the logical/physical port address to an assigned IP address.", from [Y.RACF]

4.2.1.3 Policy decision functional entity (PD-FE)

The following text is copied from [Y.RACF].

"The PD-FE handles the QoS resource requests received from the SCF via the Rs reference point or from PE-FE via the Rw reference point. The PD-FE contains the following functions:

* Final decision point (FDP): This function first checks the QoS resource request based on service information, network policy rules and transport subscription information, and then interacts with the TRC-FE via the Rt reference point to detect and determine the requested QoS resource within the involved access and/or core transport networks.
* The FDP makes the final admission decision for media flows of a given service based on network policy rules, service information, transport subscription information, and decision on resource availability.
* The FDP indicates the loss of connectivity: It informs the SCF that the transport resource previously granted is lost. The SCF may request PD-FE to relinquish all resources associated with the session.
* QoS mapping - Technology independent (QMTI): This function maps the service QoS parameters and priority received from the SCF via the Rs reference point to network QoS parameters (e.g., Y.1541 class) and priority based on the network policy rules.
* Gate control (GC): This function controls PE-FE to install and enforce the final admission decisions via the Rw reference point (e.g., opening or closing the gate). The action to pass or drop IP packets is based on a set of IP gates (packet classifiers, e.g., IP 5-tuple) and transport interface identification information (e.g., VLAN/VPN ID) as needed.
* IP packet marking control (IPMC): This function takes decisions on packet marking and remarking of flows. The marking may consider the priority of the flow and traffic engineering parameters.
* NAPT control and NAT traversal (NAPTC): This function interacts with PE-FE and SCF to provide the address binding information for NAPT control and NAT traversal as needed.
* Rate limiting control (RLC): This function makes decisions on the bandwidth limits of flows (e.g., for policing).
* Firewall working mode selection (FWMS): This function selects the working mode of the firewall based on the service information. Four packet inspection modes could be identified (static packet filtering, dynamic packet filtering, stateful inspection, deep packet inspection).
* Core network path selection (CNPS): This function chooses the core network ingress and/or egress path for a media flow based on the service information and technology independent policy rules at the involved PD-FE.
* Network selection (NS): This function locates core networks that are involved to offer the requested QoS resource. It locates the PE-FE instances that are involved to enforce the final admission decisions.

The PD-FE shall make the final policy decisions based on the service information (e.g., service type, flow description, bandwidth, priority), transport network information (e.g., resource admission

result, network policy rules) and transport subscription information (e.g., maximum upstream/downstream capacity). The policy decision shall provide sufficient information to make the PE-FE perform the resource control operation e.g., gate opening/closing, bandwidth allocation/rate limiting, packet marking, traffic policing/shaping, NAPT and address latching. The policy decisions may be composed of flow ID, IP addresses, bandwidth, gate status, time/volume limit, traffic descriptor etc.

The PD-FE can be stateful or stateless depending on the complexity of the specific network environment, application characteristics and deployment architecture.

* The stateless PD-FE only maintains the transaction state information, e.g., state held for the duration of a request-response operation. In order to be stateless, the PD-FE shall generate the resource control session information for each resource control request from the SCF, which can be stored in the SCF, TRC-FE or PE-FE and used to retrieve the state information together with pertinent information flows.
* The stateful PD-FE may maintain a variety of resource control session information within PD-FE, such as the session duration, the resource control session information (e.g., the association between SCF and PD-FE, PD-FE and TRC-FE, PD-FE and PE-FE), the resource reservation limit (e.g., time limit/volume limit), resource reservation status (i.e. authorized, reserved, or committed) and physical/logical connection ID.", from [Y.RACF]

4.2.1.4 Transport Resource Control Functional Entity (TRC-FE)

The following text is copied from [Y.RACF].

"TRC-FE is responsible for transport technology dependent resource control as follows:

* Resource status monitoring and network information collection
  The TRC-FE collects and maintains the network information and resource status information. The resource status information may be specific to the resource based admission control scheme being used by TRC-FE, i.e., whether it is accounting, out-of-band measurements, in-band measurements, or reservation-based.
* Resource based admission control
  On receipt of the resource request from PD-FE, the TRC-FE shall perform resource based admission control based on the QoS and priority requirements received from the PD-FE (e.g., bandwidth and Y.1541 class), in conjunction with the resource utilization information and transport dependent policy rules, and shall update the resource status and return the result to PD-FE.
* Transport dependent policy control

Transport dependent policy rules are a set of rules specific to a transport sub-network and technology. The TRC-FE ensures that a request from the PD-FE matches the transport specific policy rules (e.g., access link policy rules, core transport network policy rules), as multiple PD-FEs can request resources from the same TRC-FE. The TRC-FE shall coordinate the resource requests from PD-FEs and take into account transport dependent policy rules to decide if the resource requests can be supported (e.g., usage/constraints of particular transport QoS class and total capacity).

The TRC-FE provides the following basic functions:

* QoS mapping - Technology dependent (QMTD): This function maps the network QoS parameters and classes received from the PD-FE via the Rt reference point to transport (technology dependent) QoS parameters and classes based on specific transport policy rules, and accommodating the diversity of transport technologies.
* When mapping network QoS parameters to transport (technology dependent) QoS parameters, TRC-FE considers the underlying transport technology. A set of network QoS parameters may be mapped to different sets of transport (technology dependent) QoS parameters based on transport technologies. The TRC-FE has knowledge of the QoS related features of the underlying transport network and map the network QoS parameters to the best matching transport (technology dependent) QoS parameters for given transport technology. The mapping policy rules need to be provided by network operators.
* Technology dependent decision point (TDDP): This function receives and responds to the QoS resource request from PD-FE via the Rt reference point. This function detects and determines the availability of requested QoS resource based on the network topology and resource status information, as well the transport subscription information in access networks. It may make path selection between ingress and egress points within its purview of a sub-domain to satisfy the QoS resource requirements. If the requested resource is available, this function updates the resource status to include the new application request and responds PD-FE with a positive answer (e.g., resource available), otherwise, it responds PD-FE with a negative answer (e.g., resource unavailable).
* Network topology maintenance (NTM): This function collects and maintains the transport network topology information via the Rc reference point. Note that the Rc reference point can be connected to any transport functions including PE-FE, TRE-FE and other entities defined in [Y.2012] to obtain the relevant resource information.
* Network resource maintenance (NRM): This function collects and maintains the transport resource status information via the Rc reference point.
* Element resource control (ERC): This function controls the QoS-related resources in the intermediate transport elements at the aggregate level (e.g., VLAN, VPN, LSP). Note that the ERC is for further study.

The implementation of the TRC-FE in various access networks may be different according to access transport technologies and corresponding QoS mechanisms in the data plane. The implementation of the TRC-FE may be different in various core networks according to core transport technologies and corresponding QoS mechanisms in the data plane. ", from [Y.RACF].

4.2.1.5 Policy Enforcement Functional Entity (PE-FE)

The following text is copied from [Y.RACF].

"The PE-FE enforces the network policy rules instructed by the PD-FE on a per-subscriber and per-IP flow basis. It should be able to perform the following functions based on flow information such as classifier (e.g., IPv4 5-tuple) and flow direction, as well as transport interface identification information (e.g., VLAN/VPN ID, LSP Label) as needed. The functions of the PE-FE include:

* Opening and closing gate: enabling or disabling packet filtering for an IP media flow. A gate is unidirectional, associated with a media flow in either the upstream or downstream direction. When a gate is open, all of the packets associated the flow are allowed to pass through; when a gate is closed, all of the packets associated with the flow are blocked and dropped.
* Rate limiting and bandwidth allocation
* Traffic classification and marking
* Traffic policing and shaping
* Mapping of IP-layer QoS information onto link layer QoS information based on pre-defined static policy rules (e.g., setting 802.1p priority values)
* Network address and port translation
* Media relay (i.e. address latching) for NAT traversal
* Collecting and reporting resource usage information (e.g., start-time, end-time, octets of sent data)
* Packet-filtering-based firewall: inspecting and dropping packets based on pre-defined static security policy rules and gates installed by PD-FE.

There are four packet inspection modes for packet-filtering-based firewall:

* Static packet filtering: inspecting packet header information and dropping packets based on static security policy rules. This is the default packet inspection mode applied for all flows.
* Dynamic packet filtering: inspecting packet header information and dropping packets based on static security policy rules and dynamic gate status.
* Stateful inspection: inspecting packet header information as well as TCP/UDP connection state information and dropping packets based on static security policy rules and dynamic gate status.

* Deep packet inspection: inspecting packet header information, TCP/UDP connection state information and the content of payload together, and dropping packets based on static security policy rules and dynamic gate status.", from [Y.RACF].

4.2.1.6 Transport resource enforcement functional entity (TRE-FE)

The following text is copied from [Y.RACF].

"The TRE-FE enforces the transport resource policy rules instructed by the TRC-FE at the technology-dependent aggregate level (e.g., VLAN, VPN and MPLS). It should be able to perform the functions based only on transport link information (e.g., VLAN/VPN ID, and LSP Label). For example a TRE-FE may be used to modify the bandwidth associated with an LSP, or to set ATM traffic management parameters such as cell rate or burst size. Note that the scope and functions of the TRE-FE are for further study.", from [Y.RACF].

4.2.1.7 Customer Premises Equipment (CPE)

The following text is copied from [Y.RACF].

"According to the capability of QoS negotiation, the CPE can be categorised as follows:

* Type 1-CPE without QoS negotiation capability (e.g., vanilla soft phone, gaming consoles)
  The CPE does not have any QoS negotiation capability at either the transport or the service stratum. It can communicate with the SCF for service initiation and negotiation, but cannot request QoS resources directly.
* Type 2-CPE with QoS negotiation capability at the service stratum (e.g., SIP phone with SDP/SIP QoS extensions).
  The CPE can perform service QoS negotiation (such as bandwidth through service signalling but is unaware of attributes specific to the transport. The service QoS concerns characteristics pertinent to the application.
* Type 3-CPE with QoS negotiation capability at the transport stratum (e.g., UMTS UE).
  The CPE support RSVP-like or other transport signalling (e.g., GPRS session management signalling, ATM PNNI/Q.931). it is able to directly perform transport QoS negotiation throughout the transport facilities (e.g., DSLAM, CMTS, SGSN/GGSN).

Note that the SCF shall be able to invoke the resource control process for all types of CPE.", from [Y.RACF].

4.2.1.8 Comparison between NSIS intra-domain QOSM features and features supported by the ITU-T RACF functional entities

This draft consideres an Intra-domain QOSM as a QOSM that can be used within one administrative domain and that supports either a centralised or distributed QoS management approach.

The centralised approach mainly uses one Intra-domain QoS controller that is usually located off-path. However, more than one Inter-domain QoS controllers can be used within one administrative domain. In this situation the centralised Intra-domain QoS controller(s) is (are) considered to be the entitie(s) that provide the Policy Decision Point (PDP). In addition to these entitie(s), the centralised Intra-domain QOSM consists of entities that can be managed by the centralised Intra-domain QOS controllers. These entities are located on path and can be considered as Policy Enforcement Points (PEP).

The distrbuted approach uses more than one Intra-domain QoS controllers that are usually located on path and can be either located on the boundary of the administrative domain or on each on path node within the administrative domain. However, it is possible that the distributed Intra-domain QoS controllers located at the boundaries of the administrative domain can provide more features than the ones located within the domian and are not boundary nodes. In the distributed QoS management approach it is considered that the distributed Intra-domain QoS controllers are PDP and PEP.

By analysing Sections 4.2.1.1 to 4.2.1.6 it can be observed that the PD-FE, TRC-FC and SCF and NACF are mainly used by the control plane, while the functional entities PE-FE and TRE-FE are mainly used by the data plane. However, the latter two functional entities could also perform a limited number of control functions, such as bandwidth availability control and bandwidth modification. The PD-FE and TRC-FC are considered to be PDPs while the PE-FE and TE-FE are considered to be PEPs. All these functional entities can be used for both the push and pull modes of QoS resource control scenarios.

This means that the PD-FE, TRC-FE, PE-FE, TRE-FE can be considered as NSIS PDP and/or PEP Intra-domain QOS controllers.

The Type 1-CPE and Type 2-CPE cannot perform on-path QoS negotiations and therefore, it is considered that the CPE is used for the Push mode QoS resource control scenario. In this case it is considered that the CPE is not NSIS aware. The Type 3-CPE can perform on-path QoS negotiations and therefore, it is considered that the CPE is used for the Pull mode QoS resource control scenario. In this case it is considered that the CPE is NSIS aware.

4.3 The Analysis of Applying the NSIS Inter-domain QOSM for Inter-domain QoS control in the ITU-T RACF Functional Architecture

The inter-operator-domain communications for e2e QoS control in the ITU-T functional architecture are discussed in section 10 of [Y.RACF], where two ways of passing the QoS requirements for a given service over e2e paths. For the RACF Push resource control mode, the QoS requirements for a given service are proposed to be passed over the e2e path through the application layer signaling or through the Ri reference point; whereas, for the RACF Pull resource control mode, the QoS requirements for a given service are proposed to be passed over the e2e path through path-coupled QoS signaling (e.g., NSIS). However, due to the fact that the current NSIS intra-domain QOSMs (e.g., RMD-QOSM [RMD-QOSM] and Y.1541-QOSM [Y.1541-QOSM]) are all dedicated to a specific QoS control mechanism but the RACF PD-FE entity is located at the technology-independent control layer, we argue that the QoS-NSLP messages carrying those intra-domain QOSM QSPECs will not be understood by the RACF PD-FE when the on-path NSIS entities trigger the QoS request to the PD-FE and a NSIS inter-domain QOSM, which should also be independent from the underlying intra-domain QoS mechanisms, is needed to fulfill the e2e QoS control in the ITU-T RACF architecture.

Moreover, in the RACF model the procedures for QoS control are focused on how the service control function requests QoS (authorization and reservation) to the PD-FE, and how the later pushs the admission control decisions into the network nodes. So, all described procedures in [Y.RACF] are local to one operator network. The InterDomain-QoSM, provides the RACF model with the PD-FE/PD-FE communication needed for transparent end-to-end QoS control. By transparent, we mean that operators do not have to reveal any details about the internal function of their networks, including the used QoS signalling protocols.

Below we provide an analysis how the major issues that need to be consider to apply the InterDomain-QoSM to the ITU-T RACF model for inter-domain QoS control. Starting from the CPE, the InterDomain-QoSM follows the same RACF assumptions about the QoS capabilities of the CPE. According to the capability of QoS negotiation, the CPEs can be categorized as follows (see further in Section 4.2.1.7):

* Type 1: CPE without QoS negotiation capability. The CPE does not have any QoS negotiation capability at either transport or service stratum. It can communicate with Service Control Functions for service initiation and negotiation, but cannot request QoS resources directly. So, in this case it is up the the access network to set the most usefull SLSs based on the type of previous CPE service negotiations and by using the capability provided by the InterDomain-QoSM.

* Type 2: CPE with QoS negotiation capability at the service stratum (e.g. SIP CPE). The CPE can perform service QoS negotiation (such as bandwidth) through service layer signalling, but is unaware of QoS attributes specific to the transport. When the CPE is initiating communication sessions that span beyond its access network, this CPE QoS requests are passed to the InterDomain-QoSM.

* Type 3: CPE with QoS negotiation capability at the transport stratum (e.g. UMTS CPE). The CPE supports RSVP-like or other transport layer signalling. It is able to directly perform transport QoS negotiation throughout the transport facilities. In this case the RSVP-like signalling is used to configure network devices in the access network, being control passed to the InterDomain-QoSM to pass network border. In each network the control can be passed from the InterDomain-QoSM back to the RSVP-like protocol.

In order to support the end-to-end communication of different type of CPEs, the InterDomain-QoSM support the two QoS resource control modes described in the RACF:

* Push Mode: In this case the CPE (of type 2) communicates with the RACF Service Control Function (SCF), and the later issue a request to the RACF for QoS resource authorization and reservation. The RACF pushes the decisions to transport functions for policy and resource enforcement. This mode can be also used for CPE of type 1, in which case, the SCFs determine the QoS requirements of the requested service on behalf of CPEs, and based on inter-domain information that may be provided by the InterDomain-QoSM.

* Pull Mode: The SCFs issue a request to RACF for QoS resource authorization, and QoS resource reservation and the decisions are requested by Transport Functions upon receiving transport-layer QoS signalling messages. In mode is suitable for CPEs of type three, which can explicitly request the QoS resource reservation through transport-layer QoS signalling.

In what concerns the three resource control state described by RACF (Authentication, Reservation and Commitment), the InterDomain-QoSM does not cover the committed state. That is to say, the InterDomain-QoSM describes a mechanism to reserve resources (SLSs) for different types of traffic, but does not say anything about how/when the SLSs are committed. The commitment state can be included by considering the validity of the SLSs negotiated by the InterDomain-QoSM.

From the architecture point of view, an NSIS entity named Inter-domain QNE implements the NSIS Inter-domain QoSM and in charge of the inter-operator-domain interactions at each AS. Moreover, the Inter-domain QNE can be implemented in three possible ways:

i) Fully centralized, which means that the Inter-domain QNE functionality is implemented in an interior network node.

ii) Fully distributed, which means that the Inter-domain QNE functionality is implemented in all edge network nodes.

iii) A hybrid approach of i) and ii), in which the Inter-domain QNE is co-located with interior network nodes close to edge devices. This is while in option ii) we have one inter-domain QNE implemented in each edge router (which does not separate data and control plane), in this option we have one Inter-domain QNE controlling a subset of edge devices and we separated the data from the control plane.

Each of these approaches has advantages and disadvantages. For instance:

- The centralized option does not need the synchronization between several Inter-domain QNEs in the same network, but has scalability and resilience problems. In terms of signaling, it needs an off-path NSIS QoS signaling to fulfill the ITU-T RACF Ri reference point.

- The fully distributed option presents the highest scalability and resilience properties, but it incorporates the constraint that the signaling will be processed on the nodes which also handle the data flows themselves. From the signaling point of view, there is no need for a new off-path QoS signaling and the Ri reference point can be implemented by using the on-path NSIS QoS signaling, since the signaling can be done by using QoS-NSLP in two steps, inter-domain and intra-domain.

- The hybrid option seems to provide a good compromise between the de-coupling of signaling and data and the needed scalability and resilience. In terms of signaling, it needs an off-path inter-domain QoS signaling to implement the Ri reference point. In addition, it may also need an off-path NSLP intra-domain signaling to implement the Rd reference point to synchronize the set of Inter-domain QNEs (i.e., the inter-domain PD-FEs).

If fact, the most suitable solution (fully centralized, fully distributed or hybrid) will strongly depend on the characteristics of the domain, such size, network technology, and method used to assure QoS. These operation modes of the inter-domain QNE are an add-on to the RACF, since the RACF specificiation does not mention this issue. In what concerns the RACF entities, we propose to slip the PD-FE functions into the inter-domain PD-FE for inter-domain QoS control and the intra-domain PD-FE for intra-domain QoS control and map the Inter-domain QNE to the inter-domain PD-FE. thus, for the case that more than one InterDomain-QNEs exist at an operator AS, they can interact with each other via the RACF Rd reference point.

Here we focus our analysis on the inter-domain PD-FE, which interacts with the intra-domain PD-FE and PE-FE. Furthermore, the InterDomain-QoSM will be used to fulfill the Ri reference point between peer inter-domain PD-FE at adjacent operator domains. This

inter-domain QoS control can be done based on two scenarios: in one scenario (push mode), the CPE requests QoS to the SCF or it is the SCF that handle QoS requests on behalf of the CPEs. In another scenario (pull mode), the CPE requests QoS via a path-coupled QoS signalling in the transport stratum. In any case the inter-domain QoS control is due by the InterDomain-QoSM via the NSIS path-decoupled message association created over the Ri reference point of the PD-FE (see section 5.2.1 - GIST analysis). In other words, the path-coupled signaling is only used between CPEs and the access network and inside each network being the inter-domain signaling done by InterDomain-QoSM via Ri reference point. This usage of the path-coupled signalling, means that each network can use a different path-coupled signaling implementation, since that signalling is never used end-to-end.

4.4 The mapping between ITU-T RACF Entities and NSIS Entities

Based on the results of the analysis done in Sections 4.2 and 4.3, it can be observed that the ITU-T RACF PD-FE, TRC-FE functional entities can be considered as NSIS PDP Intra-domain and Inter-domain QOS controllers, while the ITU-T RACF PE-FE and TRC-FE functional entities can be considered as NSIS PDP and/or PEP Intra-domain QoS controllers.

In addition to the analysis given in Sections 4.2 and 4.3, it should be observed that all functional entities support, in addition to QoS features, also NAT and network management features. In this draft we will only consider the QoS features without analysing the rest of the features.

The NACF function is mainly used for network attachment, e.g., authentication, authorization, dynamic provisioning of IP addresses and mobility support. Therefore, this functional entity and its interactions will not be considered in the mapping process of the RACF entities to NSIS entities.

The SCF function can be considered to be a functional entity that can be managed by non NSIS aware signaling. Therefore, also this functional entity is not considered in the mapping process.

The ITU-T CPE functional entity can be considered as a NSIS QNI or QNR when used in association with the pulled mode of QOS resource control.

Based on the above, we provide the following mapping between the ITU-T RACF functional entities to the NSIS entities.

* (Inter-domain) RACF TRC-FE is mapped to TRC-FE (NSIS) Interdomain QoS controller
* (Inter-domain) RACF PD-FE is mapped to PD-FE (NSIS) Interdomain QoS controller

* (Intra-domain) RACF TRC-FE is mapped to TRC-FE (NSIS) Intra-domain QoS controller
* (Intra-domain) RACF PD-FE is mapped to PD-FE (NSIS) Intra-domain QoS controller
* (Intra-domain) RACF PE-FE is mapped to PE-FE (NSIS) Intra-domain QoS controller
* (Intra-domain) RACF TRE-FE is mapped to TRE-FE (NSIS) Intra-domain QoS controller

Additional observations that can be made are the following. The TRC-FE and TRE-FE are technology dependent functional entities. This draft will mainly focus on technology independent features and therefore these two functions and their interactions will not be further considered in the mapping process from the RACF entities to NSIS entities.

The intercommunication between the NSIS entities is accomplished using the NSIS protocol suites and is specified in the following way:

* between NSIS PD-FE Inter-domain QoS controllers is done using a QSPEC that carries the Rd++ information elements.
  Rd++ is the interface that equals to Rd, but that will have to be extended in the future to fulfil the Ri interface.

  The Ri interface is a logical interface that will be supported by using the NSIS protocol suite. The Ri informational elements, specified in [Y.RACF], are carried by a NSIS QSPEC, that we denote in this draft as Ri_QSpec.

* between the PD-FE (NSIS) inter-domain QoS controller and the PD-FE (NSIS) intra-domain QoS controller is accomplished using a QSPEC, denoted as Rd_QSpec, that carries the Rd informational elements specified in [Y.RACF].

* between the PD-FE (NSIS) intra-domain QoS controller and another PD-FE (NSIS) intra-domain QoS controller is accomplished using the same Rd_QSpec as above. Note that the intercommunication between these entities could also be performed using other types of Intra-domain QOSMs.

* between the PD-FE (NSIS) inter-domain QoS controller and the PE-FE (NSIS) intra-domain QoS controller is accomplised using the Rw_QSpec, which carries the Rw informational elements specified in [Y.RACF].

* between the PD-FE (NSIS) intra-domain QoS controller and the PE-FE (NSIS) intra-domain QoS controller is accomplised using the same Rw_QSpec as above.

5. The Basic Features of Interdomain-QOSM

The rest of this document specifies the NSIS Inter-domain QOSM which can be applied to the ITU-T RACF functional architecture for for e2e QoS control across heterogeneous operator domains. The basic features of the Interdomain-QOSM are described here.

5.1 Overview

The NSIS Interdomain-QOSM aims at realizing the inter-operator-domain QoS interactions between adjacent operator ASs in a standarized way while hiding the heterogeneities of the intra-domain QoS control mechanisms in use at each domain. As mentioned above, the Inter-domain QNE that will implement the Interdomain-QOSM should support three possible operation mode: fully centralized, fully distributed and hybrid, and it should also be able to interact with different intra-domain QOSMs deployed at each operator domain. To achieve the above objectives of the Interdomain-QOSM, a set of supports from the underlying NSIS GIST and QoS-NSLP protocols are needed, especially for the Inter-domain QNE discovery and the transport of InterDomain-QOSM messages. Moreover, to successfully apply the Interdomain-QOSM to the e2e QoS control in the ITU-T RACF functional architecture, the impact of the Interdomain-QOSM on the RACF architecture should also be analyzed. Finally, we discuss the e2e QoS control scenarios the Interdomain-QOSM can support for the ITU-T RACF architecture.

5.2 The Assumptions for the Interdomain-QOSM

This part provides the first analysis of how to include the InterDomain-QoSM in the NSIS protocol stack, by describing a set of assumptions about NSIS that are central to the development of the proposed QOSM. It introduces section 6.6, which allows us to go back to NSIS with some proposals for adjustments in order to fulfill all the requirements of the described InterDomain-QoSM.

This section analysis the potential requirements of the InterDomain-QOSM on the GIST [GIST] and QoS-NSLP [QoS-NSLP]:

i) We analyze the possible impact of the InterDomain-QoSM on GIST, namely its support for message association between edge devices and the inter-domain QoS controller, between the inter-domain QoS controller and the edge devices, and between two inter-domain QoS controllers (in the case of a distributed operation mode of the InterDomain-QoSM.

ii) We analyze until what extend can QoS-NSLP signaling and the defined QSpec be re-used.

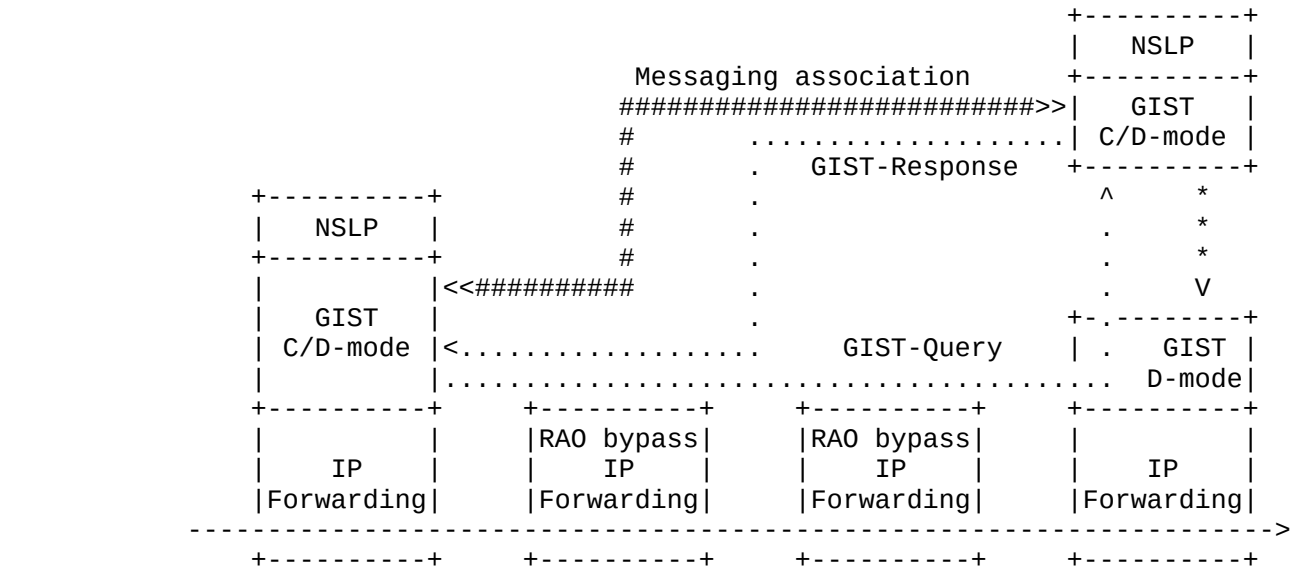
Furthermore, regarding to the functional architecture and entities defined in the ITU-T RACF document [Y.RACF], we consider only the technology independent QoS control features and thus, the RACF TRC-FE and TRE-FE entities are not covered by our analysis and mapping in this document.

5.2.1 GIST Analysis

The NSIS working group is currently developing a protocol suite in which the signaling messages will be processed on the nodes which also handle the data flows themselves ("path-coupled signaling"). Complementary to this method, a complementary routing method partially decoupled from the data path is being analyzed. This new off-path Message Routing Method (MRM) allows the signaling and data paths to be partially decoupled, without sacrificing the integration with routing.

The major assumption that the InterDomain-QoSM makes of NSIS is the support of an off-path MRM.

The current proposal for an off-path MRM [draft-hancock-nsis-pds-problem-03] defines two discovery mechanisms, one starting in one off-path node and finishing in one on-path node, and another starting in one on-path node and finishing in one off-path node. Figure 3 illustrates these two methods.



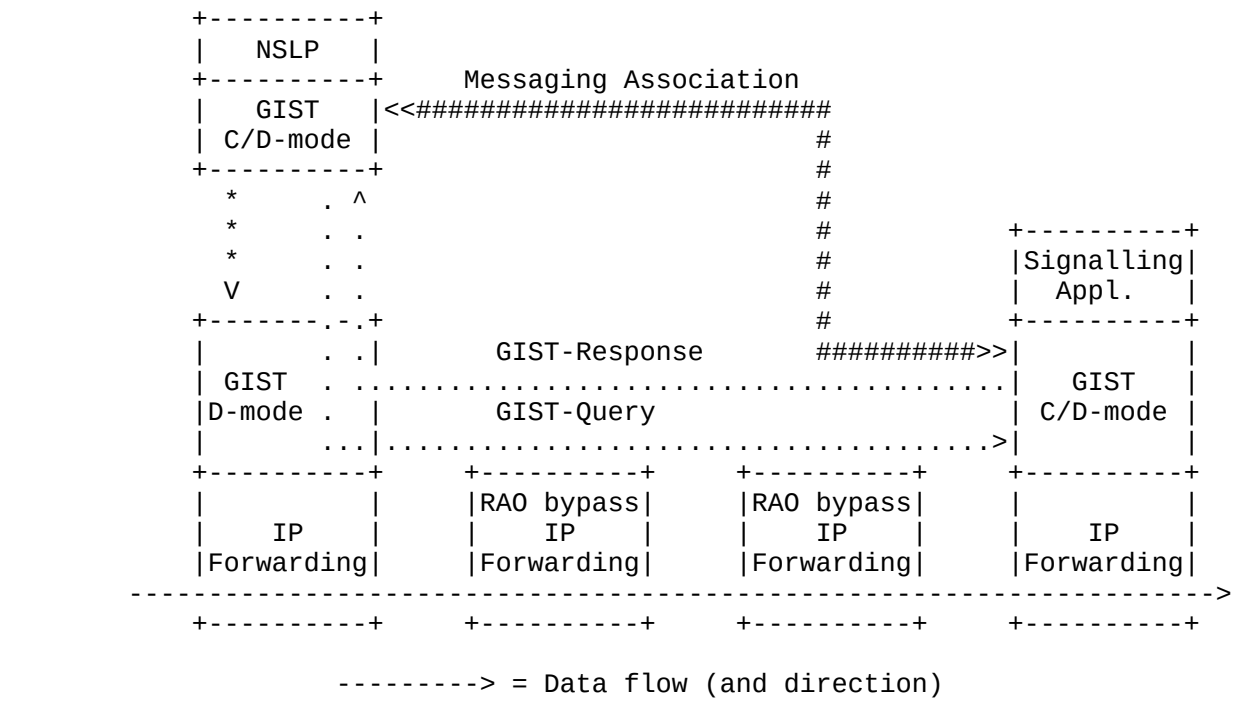
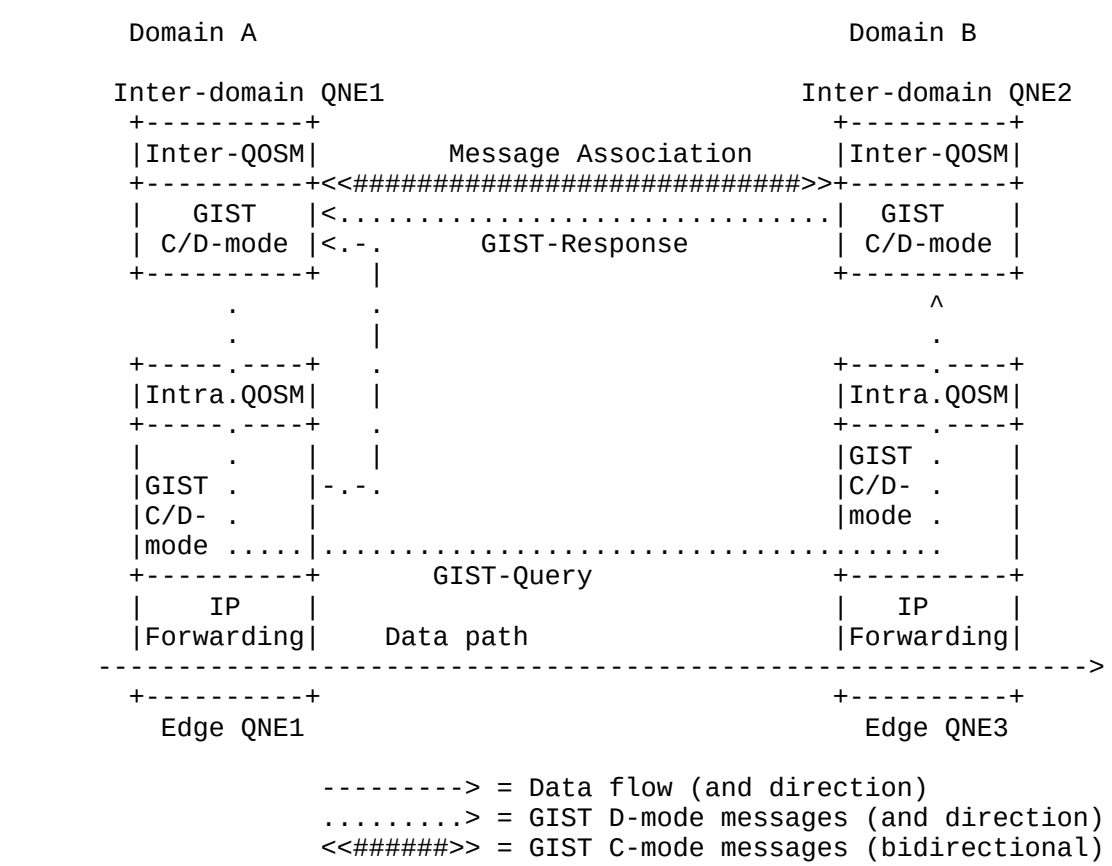


Figure 3: discovering a downstream off-path node from a on-path node (top figure) and discovering a downstream on-path node from an off-path node (bottom figure).

These two methods are of use to discover a inter-domain QNE from an edge device by which flows enter a domain (ingress device), and for an inter-domain QNE to discover an edge device by which flows exit a domain (egress device). However, these two discovery mechanism do not support the discovery of one QoS controller by its peers. This is a kind of off-path to off-path discovery mechanism.

The off-path MRM proposal mention "Off-path 'server' discovery from another off-path node" in section 3.1, but does not describe that mechanism. Nevertheless, this off-path to off-path discovery mechanism may be build by using the two methods (on-path to off-path discovery and vice-versa) described in the off-path MRM proposal by allowing the configuration of an on-path node for selecting a specific off-path device. This is one downstream on-path node (i.e., the edge routers in the case of the InterDomain-QoSM) should be configured to select an off-path QoS controller to which its received GIST-QUERY message should be forwarded.

Figure 4 illustrates the setup of an association between two off-path inter-domain QNEs located in two different domains. After the edge QNE1 at Domain A processes the QoS-NSLP message from its upstream interior QNE, it will connect to the inter-domain QNE1 in its domain which is configured to serve it (via GIST D-mode or C-mode depending on the configuration or requirement). Next, the inter-domain QNE1 sends a GIST-Query message, which is forwarded by the Edge QNE1 in its domain and intercepted by the Edge QNE3 in Domain B. Then, this intercepted Query message is forwarded to the inter-domain QNE2 in Domain B, which is configured to serve Edge QNE3. To this end, the inter-domain QNE2 at Domain B knows the necessary info of its peer at Domain A and can send the GIST-Response message directly to its peer (here, i.e., inter-domain QNE1 at Domain A). Finally, a message association is set up between them.



---------> = Data flow (and direction)
.........> = GIST D-mode messages (and direction)
<<######>> = GIST C-mode messages (bidirectional)

Figure 4: discovering a downstream off-path node from an upstream off-path node.

This off-path discovery mechanism can be applied to discover peer off-path devices in different networks, as illustrated in Figure 4, and to discover peer off-path devices inside the same network. The later may be used in a scenario in which a domain uses distributed inter-domain QNEs -- a set of inter-domain QNEs each controlling a subset of edge nodes.

5.2.2 QoS-NSLP Analysis

In the example illustrated in Section 5.2.1, the inter-domain QNEs implement the InterDomain-QoSM by signaling QoS between domains, while QoS-NSLP [QoS-NSLP] is used to support an IntraDomain-QoSM. This is, the inter-domain QNE may trigger a specific ingress device, which may use QoS-NSLP to signal the needed QoS among all QoS-NSLP aware routers inside the domain from the triggered ingress device until the indicated egress device.

However, the use of QoS-NSLP to signal between ingress and egress devices is not mandatory for the InterDomain-QoSM. Actually, the InterDomain-QOSM makes no assumptions about the implementation mechanisms of the IntraDomain-QoSM. That is to say intra-domain resources may be controlled in a centralized or distributed way, based on NSIS protocols or not. Nevertheless, a distributed implementation of the IntraDomain-QoSM based on QoS-NSLP signalling over several intra-domain QNEs is more close to the work being done in NSIS (independent from if the intra-domain signalling is done on-path or off-path based on the use of a new off-path MRM also inside a domain).

In any case, the InterDomain-QoSM makes use of the messages, objects and procedures defined by QoS-NSLP for signaling exchanges between inter-domain QNEs. However, the InterDomain-QoSM depends on the GIST to discover the peer inter-domain QNEs in adjacent domains. This means that QoS-NSLP is used to signal between inter-domain QNEs, over a set of NSIS message associations, as described in section 5.1.

Moreover, the SLS parameters and QoS control information required for the inter-domain QoS interactions are specified by using/extending the QSPEC template in [NSIS-QSPEC].

5.3 The support of ITU-T RACF end-to-end QoS control via the InterDomain-QOSM

The inter-operator-domain communications for e2e QoS control in the ITU-T functional architecture are discussed in section 10 of [Y.RACF], where two ways of passing the QoS requirements for a given

service over e2e paths. For the RACF Push resource control mode, the QoS requirements for a given service are proposed to be passed over the e2e path through the application layer signaling or through the Ri reference point; whereas, for the RACF Pull resource control mode, the QoS requirements for a given service are proposed to be passed over the e2e path through path-coupled QoS signaling (e.g., NSIS).

The InterDomain-QoSM will be used to fulfill the Ri reference point between peer inter-domain PD-FE at adjacent operator domains. This inter-domain QoS control can be done based on two scenarios: for the RACF Push mode, when the application layer signaling is not available or incapable to carry the e2e QoS requirements, the CPE requests QoS to the SCF or it is the SCF that handle QoS requests on behalf of the CPEs and, then the e2e QoS requirements are forwarded to the inter-domain PD-FE. In another scenario (the RACF Pull mode), the CPE requests QoS via a path-coupled QoS signalling in the transport stratum. In any case the inter-domain QoS control is due by the InterDomain-QoSM via the NSIS path-decoupled message association created over the Ri reference point of the PD-FE (see section 5.2.1 - GIST analysis). That is to say, the path-coupled signaling is only used between CPEs and the access network and inside each network being the inter-domain signaling done by InterDomain-QoSM via Ri reference point. This usage of the path-coupled signalling, means that each network can use a different path-coupled signaling implementation and different NSIS intra-domain QOSM(s), since that signalling is never used end-to-end.

6. InterDomain-QOSM, Detailed Description

6.1 Additional QSPEC Parameters for End-to-End QoS Control By the InterDomain-QOSM

TBD

6.2 The Operation Modes of the InterDomain-QOSM

To address the scalability issue for deploying the InterDomain-QOSM in real IP network domains, three possible ways to implement the Inter-domain QNE (see Section 4.3) are provided: fully centralized, fully distributed and hybrid. Moreover, there are two resource control scenarios in the ITU-T RACF functional architecure: RACF Push and Pull resource control modes in [Y.RACF]. Thus, to apply the Interdomain-QOSM to fully fulfill the e2e QoS control in the ITU-T RACF architecture, the Interdomain-QOSM will have to support 6 possible operation combinations: fully centralized, fully distributed and hybrid under the RACF Push and Pull modes, respectively.

6.2.1 Operation mode 1: fully centralized

In this operation mode, a single off-path NSIS inter-domain PD-FE will exist at an AS that deploys the InterDomain-QOSM to take care of all the inter-domain QoS interaction requests from/to the domain (see Figures 1 and 4 at http://www.dcs.qmul.ac.uk/~jianzhang/Interdomain-QOSM%20Mapping.pdf). Moreover, a centralized or distributed intra-domain PD-FE will also exist at each AS and be responsible for the intra-domain QoS control at the AS. The intra-domain PD-FE can be implemented by a NSIS intra-domain QOSM (for RACF Pull mode) or any intra-domain QoS control mechanisms (for RACF Push mode) and it will interact with the inter-domain PD-FE via the ITU-T RACF Rd reference point. The off-path NSIS inter-domain PD-FE has to support the NSIS protocol suites and implement the Interdomain-QOSM and the PE-FE at the boundary of each AS must also support the GIST off-path Message Routing Method (MRM) to help the discovery of the peer NSIS inter-domain PD-FE at adjacent operator domains and transport the Interdomain-QOSM messages (i.e, implementing the ITU-T RACF Ri reference point).

Under the RACF Push mode, the CPE is non-NSIS aware and the QoS requests will be triggered by the SCF to the PD-FE(s) at the source domain; at the subsequent operator domains, the QoS requests will be triggered by the inter-domain QoS interactions. Whereas, under the RACF Pull mode, the CPE is NSIS aware and acts as the QNI to trigger the QoS request at the source domain; at the subsequent operator domains, the QoS requests will first be triggered by the inter-domain QoS interactions and then the on-path NSIS aware nodes will send their requests to the intra-domain QOSM(s) for the intra-domain QoS control.

6.2.2 Operation mode 2: fully distributed

In this operation mode, the NSIS inter-domain PD-FE will exist at each edge node of an AS that deploys the InterDomain-QOSM to take care of the inter-domain QoS interaction requests from/to the domain via the edge node (see Figures 2 and 5 at http://www.dcs.qmul.ac.uk/~jianzhang/Interdomain-QOSM%20Mapping.pdf). Moreover, a centralized or distributed intra-domain PD-FE will also exist at each AS and be responsible for the intra-domain QoS control at the AS. The intra-domain PD-FE can be implemented by a NSIS intra-domain QOSM (for RACF Pull mode) or any intra-domain QoS control mechanisms (for RACF Push mode). For the case that the intra-domain PD-FE is also distributed at each edge node of the AS, the inter-domain and intra-domain PD-FEs will interact via the RACF Rd interface implemented internally, otherwise, it will interact with the inter-domain PD-FE via the external RACF Rd interface.

Each edge node at the AS will have to implement the Interdomain-QOSM to take care of the inter-domain QoS interactions at its edge node. Under the RACF Push mode, the CPE is non-NSIS aware and the QoS requests will be triggered by the SCF to the PD-FE(s) at the source domain; at the subsequent operator domains, the QoS requests will be triggered by the inter-domain QoS interactions. Whereas, under the

RACF Pull mode, the CPE is NSIS aware and acts as the QNI to trigger the QoS request at the source domain; at the subsequent operator domains, the QoS requests will first be triggered by the inter-domain QoS interactions and then the on-path NSIS aware nodes will send their requests to the intra-domain QOSM(s) for the intra-domain QoS control.

6.2.3 Operation mode 3: hybrid

In this operation mode, a number of off-path NSIS inter-domain PD-FEs will exist at an AS, and each of them will deploy the InterDomain-QOSM and be responsible for handling the inter-domain QoS interaction requests from/to a set of edge QNEs (see Figs 3 and 6 at http://www.dcs.qmul.ac.uk/~jianzhang/Interdomain-QOSM%20Mapping.pdf). Normally the set of edge QNEs assigned to different inter-domain PD-FEs should be disjoint to reduce the synchronization requirement between different NSIS inter-domain PD-FEs.

Moreover, a centralized or distributed intra-domain PD-FE will also exist at each AS and be responsible for the intra-domain QoS control at the AS. The intra-domain PD-FE can be implemented by a NSIS intra-domain QOSM (for RACF Pull mode) or any intra-domain QoS control mechanisms (for RACF Push mode). For the case that the intra-domain and inter-domain PD-FEs are located at the same node of the AS, they will interact via the RACF Rd interface implemented internally, otherwise, they will interact with the external RACF Rd interface.

Every off-path NSIS inter-domain PD-FE should support the NSIS protocol suites and implement the Interdomain-QOSM and the edge PE-FE at the AS must also support the GIST off-path Message Routing Method (MRM) to help the discovery of the peer NSIS inter-domain PD-FE at adjacent operator domains and transport the Interdomain-QOSM messages (i.e, implementing the ITU-T RACF Ri reference point). Furthermore, the off-path NSIS inter-domain PD-FEs within the AS can interact with each other via the RACF Rd reference point.

Under the RACF Push mode, the CPE is non-NSIS aware and the QoS requests will be triggered by the SCF to the PD-FE(s) at the source domain; at the subsequent operator domains, the QoS requests will be triggered by the inter-domain QoS interactions. Whereas, under the RACF Pull mode, the CPE is NSIS aware and acts as the QNI to trigger the QoS request at the source domain; at the subsequent operator domains, the QoS requests will first be triggered by the inter-domain QoS interactions and then the on-path NSIS aware nodes will send their requests to the intra-domain QOSM(s) for the intra-domain QoS control.

6.3 Message Format

TBD

6.4 InterDomain-QOSM Node State Management

TBD

6.5 InterDomain-QOSM Operations and Sequences of Events

TBD

6.5.1 Basic unidirectional operation

TBD

6.5.1.1 Successful reservation

TBD

6.5.1.2 Unsuccessful reservation

TBD

6.5.1.3 Refresh reservation

TBD

6.5.1.4 Modification of reservation

TBD

6.5.1.5 InterDomain release procedure

TBD

6.6 Inter-domain QNE Discovery and Transport of InterDomain-QOSM Messages

TBD

6.6.1 Requirements of InterDomain-QOSM to the Underlying Path-coupled NTLP

TBD

6.6.2 Requirements of InterDomain-QOSM to the Underlying path-decoupled NTLP

TBD

6.7 Handling of Additional Errors

TBD

7. Security Consideration

The operation mode of the InterDomain-QOSM might produce some security concerns and this will be discussed and clarified later.

8. IANA Considerations

This section provides guidance to the Internet Assigned Numbers Authority (IANA) regarding registration of values related to the QSPEC template, in accordance with BCP 26 RFC 2434 [RFC2434].

The InterDomain-QOSM requires a new IANA registry. In addition, the new QSPEC parameters which will be defined in the next version of this document, need to be assigned the QSPEC Parameter ID for them.

9. Open Issues

This section includes the issues that we will do or we think should be analysed in the next version of the draft. Currently, the open issues include:

- All the missing subsections in Section 6 will be done in the next version of the draft.
- The detailed analyses of implementing the relevant ITU-T RACF reference points to support e2e QoS control by using NSIS will be given in the next version of the draft. The QSPEC parameters necessary for the implementation will also be given in the next version.
- The analyses for how to adapt the NSIS QOSMs to apply to the ITU-T RACF functional architecture in this document could be moved to a new draft for further comprehensive studies so that the current NSIS QOSM drafts, such as [RMD-QOSM] and [Y.1541-QOSM], need not do the same analysis again.
- The mapping between the ITU-T RACF entities and the NSIS entities for e2e QoS control need more stuides and discussion with the ITU-T and NSIS people and could be refined in the next version.
- The application of the Interdomain-QOSM to the e2e QoS control in the ITU-T RACF functional architecture also needs more studies and discussions.
- The support of the automatic inter-domain adjustment in the scenario of mobile end customers.

10. Acknowledgments

The authors would like to thank John Loughney and Robert Hancock for the helpful suggestions on this InterDomain-QOSM work.

11. References

11.1 Normative References

[GIST] Schulzrinne, H., and Hancock, R., "GIST: General Internet Signaling Transport", work in progress.

[QoS-NSLP] Manner, J., Karagiannis, G., McDonald, A. and Bosch, S., "NSLP for Quality-of-Service signaling", work in progress.

[RMD-QOSM] Bader, A., et. al., "RMD-QOSM - The Resource Management in Diffserv QOS Model," work in progress.

[NSIS-QSPEC] Ash, J., et. al., "QoS-NSLP QSPEC Template," work in progress.

11.2 Informative References

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

[RFC2210] Wroclawski, J., "The Use of RSVP with IETF Integrated Services," RFC 2210, September 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z. and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[RFC2638] Nichols K., Jacobson V., Zhang L. "A Two-bit Differentiated Services Architecture for the Internet", RFC 2638, July 1999.

[RFC4080] Hancock, R., Karagiannis, G., Loughney, J., and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, June 2005.

[DCPEL-requirements] Mendes, P., and Nichols, K., "Requirements for DiffServ Control Plane Elements", draft-mendes-dcpel-requirements-00 (work in progress), January 2006.

[draft-hancock-nsis-pds-problem-03] Hancok, R., Kappler, C., Quittek, J., Stiemerling, M., "A Problem Statement for Partly-Decoupled Signalling in NSIS", draft-hancock-nsis-pds-problem-03, (work in progress), February 2006.

[Y.RACF] ITU-T Recommendation Y.2111, "Resource and admission control functions in Next Generation Networks", 2006.

[Y.2012] ITU-T Recommendation Y.2012, "Functional requirements and architecture of the NGN".

[Y.1541-QOSM] Ash, J., et. al., "Y.1541-QOSM -- Y.1541 QoS Model for Networks Using Y.1541 QoS Classes," work in progress.

Authors's Addresses

Jian Zhang
Dept. of Computer Science
Queen Mary, Univ. of London
Mile End, London E1 4NS
UK
Email: jian.zhang@dcs.qmul.ac.uk

Edmundo Monteiro
Dept. of Informatics Engineering
Univ. of Coimbra
Polo II - Pinhal de Marrocos
3030-290 Coimbra, Portugal
Email: edmundo@dei.uc.pt

Paulo Mendes
Future Networking Laboratory
NTT DoCoMo Euro-Labs
Landsbergerstr 312
80687 Munich
Germany

Phone: +49 89 56824 226
Email: mendes@docomolab-euro.com
URI: http://www.docomolab-euro.com/

Georgios Karagiannis
University of Twente
P.O. Box 217
7500 AE Enschede, The Netherlands
Email: g.karagiannis@ewi.utwente.nl

Jorge Andres-Colas
Advanced Networks Planning
Telefonica I+D
Emilio Vargas, 6
28043 Madrid, Spain
Email: jorgeac@tid.es

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement