Available online at www.sciencedirect.com
SCIENCE DIRECT
Journal of Network and Computer Applications 28 (2005) 285–302
Journal of NETWORK and COMPUTER APPLICATIONS
www.elsevier.com/locate/jnca

Service level agreements for DiffServ-based services' provisioning

Christos Bouras[a,b,*], Afrodite Sevasti[b,c]

[a]RA Computer Technology Institute-RACTI, Kolokotroni 3, Patras 26221, Greece
[b]Department of Computer Engineering and Informatics, University of Patras, Rion, Patras 26500, Greece
[c]Greek Research and Technology Network-GRNET, 56 Mesogion Av., Athens 11574, Greece

Received 13 January 2004; received in revised form 24 June 2004; accepted 6 July 2004

Abstract

The evolution of mechanisms for providing Quality-of-Service (QoS) over the contemporary network infrastructures has introduced the need for regulation and management of the emerging QoS services with the use of Service Level Agreements (SLAs). SLAs define the qualitative and quantitative characteristics of the services provided from a network provider to peering networks or customers. In this work, we define a template for the SLA structure to support the provision of a QoS service between two peering domains and then we proceed with the definition of an end-to-end SLA across consecutive domains, based on the bilateral ones. We also propose a model for the service provisioning procedures.

Keywords: Service Level Agreement; DiffServ-based service; Provisioning; End-to-end SLA; QoS

1. Introduction

A Service Level Agreement (SLA) is an explicit statement of the expectations and obligations that exist in a business relationship between two entities: a service provider and a customer (Rajan et al., 2000). Bilateral SLAs can also be defined among organizations that have a symbiotic relationship, with each being a customer of the other's

* Corresponding author. Address: Computer Technology Institute, 61 Riga Feraiou Str, Patras 26221, Greece. Tel.: +30-2610-960375; fax: +30-2610-960358.
E-mail addresses: sevasti@grnet.gr (C. Bouras), sevasti@grnet.gr (A. Sevasti).

1084-8045/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2004.07.001

services. The SLA provides a means of defining the service. It specifies what the customer wants and what the supplier is committing to provide. It defines the standards for the quality of the service provided, setting performance objectives that the supplier must achieve. It also defines the procedure and the reports that must be provided to track and ensure compliance with the SLA. In the field of telecommunications networking, SLAs play a significant role, reinforced by the latest advances in differentiated services' provisioning.

The availability of high-speed transmission media and networking equipment, as well as the evolution of quality-demanding applications has focused research interest on the provision of Quality-of-Service (QoS) in addition to the traditional best-effort model of the Internet. A number of alternatives for service differentiation and QoS provision have been proposed and standardized, but in the case of IP-based backbone networks the Differentiated Services (DiffServ) architecture has prevailed, due to its scalability and deployment feasibility. The provisioning of IP services according to the DiffServ framework has introduced complexity in the corresponding business model and has raised the requirements for controlled resource allocation and management, definition, monitoring and verification of the quality provided. At this point, the appropriate definition of SLAs between customers and service providers is envisaged to provide the controlled environment required. In this framework, SLAs will act as mediators for mutual service provisioning between peering domains.

The DiffServ framework stands out for attempting to provide service differentiation to traffic in a scalable manner, by suggesting the aggregation of individual application flows with similar quality needs. It introduces the definition of different service classes to which such aggregates are appointed and the implementation of mechanisms for differential treatment by network elements (Per-Hop-Behaviour, PHB) of the packets belonging to each service class. A PHB is thus describing the treatment of aggregated traffic in a manner that ensures the quality guarantees provided by the corresponding service class.

Although, DiffServ has been initially confronted with a positive attitude, due to its scalability, the DiffServ framework mechanisms have proved difficult to deploy and monitor in a large scale in production networks. Based on the DiffServ framework, a number of service models constructed by a combination of DiffServ mechanisms have been proposed and experimentally evaluated up to our days. However, real-world implementations of DiffServ-based services in production networks have not successfully operated in large-scale yet. Missing DiffServ functionality from IP routers, translation to last-mile (end user access links) QoS, considerable operational and economical paradigm shifts required from operators, lack of a flexible business model, inadequacy of service verification infrastructure, inadequate standardization and architectural gaps are some of the major deployment problems analysed in (Paxson et al., 1998).

We believe that the DiffServ framework and DiffServ-based services do have a significant potential in upgrading the best-effort service model in today's Internet. However, due to its probabilistic rather than deterministic differentiation mechanisms, the provisioning model of DiffServ has to be thoroughly specified and standardized as soon as possible. Among the deployment problems already mentioned, a flexible business model for intra-domain development and peering agreements according to the existent agreements are considered crucial for the successful deployment of DiffServ-based

services in production networks. We believe that SLAs are of crucial importance on this basis.

Today, the installation of SLAs between customers and providers is a rather static and labor-intensive task. The procedures involved in this process are proprietary to the provider and, in many cases; these procedures are invoked on a low frequency basis (e.g. when updating a Virtual Private Network (VPN) topology). By its proprietary nature, such a process does not allow for an open-service architecture, such as that of DiffServ-based services, to be built upon interconnected IP networks. It should be understood that standardization of the technical parts of the basic process may allow for a highly developed level of automation and dynamic negotiation of Service Level Specifications (SLSs) between peering providers or customers and providers. This automation may prove helpful in providing customers (as well as providers) with the technical means for the dynamic provisioning of QoS guaranteed transport services. SLAs and SLSs are essential for delivering the obtained QoS from one end-user to another across multiple domains.

So far there have been several efforts towards the standardization of definition of SLAs and their instantiation in QoS-enabled networks (Bouras et al., 2002; Fankhauser and Plattner, 1999; Neilson et al., 1999; Nichols et al., 1999). In production networks, service providers use their own customized SLAs for qualitative IP services provisioning. Moreover, the provisioning model usually concerns a backbone network service provider and its directly attached customers. The case of multi-domain QoS provisioning in which quality parameters of the network have to be mapped along neighbouring domains and need to be consistent along the end-to-end path is rarely addressed. Furthermore, processes for the establishment of end-to-end SLAs in such cases are not mature enough yet. Our proposal attempts to address these issues.

In this work, we are initially presenting the basic principles for the deployment of DiffServ-based service contracts (SLAs) in a bilateral fashion (between peering domains). For this purpose, we use the case of a service based on the Expedited Forwarding (EF) DiffServ PHB (Salsano, 2000), for serving high-priority and quality demanding traffic. Furthermore, we propose a methodology for establishing an end-to-end SLA based on the bilateral SLAs, using as our reference architecture that of the GEANT core pan-European research network, interconnecting the European National Research and Education Networks (NRENs) and through them campuses and institutions, user groups and end users all over Europe. Apart from the end-to-end SLA establishment, we propose a provisioning model for the set-up and coordination of SLA-based service deployment and operation.

2. Bilateral SLAs

Bilateral SLAs aim at the detailed description of service provisioning, availability and guarantees between two peering domains supporting one or more compatible services. The SLA describes how each one of the two domains provides a specific service to the service-eligible traffic accepted from its neighbour and vice versa.

The proposed bilateral SLA specification comprises of two parts (see also Bouras et al., 2002):

- The administrative/legal part.
- The SLS part, defining the set of parameters and their values, for the provision of a DiffServ-based service to a traffic aggregate by a DiffServ domain.

After the definition of the bilateral SLA, the next steps are to define the mechanisms for SLA negotiation and, of course, for the establishment of end-to-end services based in the individual SLAs.

Each instantiation of a SLS comprises a so-called Service Level Object (SLO) and contains the parameters and their values that describe the DiffServ-based service a specified flow is to receive over the transport domain.

Bi-directional services are also be possible by the combination of two SLOs taken atomically when negotiating a service pertaining to two flows, one at each direction. These SLOs will comprise a Transport Service, which is part of the SLA defined between two domains, among which the bi-directional service is established. Fig. 1 displays an SLA template and two instantiations of it, bringing the aforementioned individual SLA components together. The SLA instantiation on the left is an example of a bi-directional SLA containing two uni-directional SLOs. These SLOs roughly define the provision of an EF-based service over the GEANT backbone to the Greek NREN (GRNET) for EF connectivity with the German NREN (DFN). The SLA instantiation on the bottom right of Fig. 1 defines the provisioning of the EF-based service over the GRNET backbone.

In the following sections, a more detailed specification of the proposed SLA and SLS template is provided.

2.1. The administrative/legal part of the SLA

The administrative/legal part of the SLA is suggested to comprise of a number of fields that define the procedures and framework for the provision of the service that the SLA is established for Proposed fields are:

- *Administrative and technical parties involved*. This section should contain at least one administrative and one technical contact from each of the two sides participating in the SLA.
- *Duration in time*. This section should contain the period for which the SLA is valid. This period can differ from the period defined at the ‘service schedule’ field of the SLS part of the SLA, but the value of the ‘service schedule’ field has to be a period WITHIN the period defined at this section of the SLA. The ‘service schedule’ is a set of time periods for which the service is active, while the SLA duration is a time period for which the SLA for the service’s provision is valid.
- *Availability guarantees*. This section should define the calculation of the service’s availability figures and how these will be derived (e.g. from the trouble ticketing

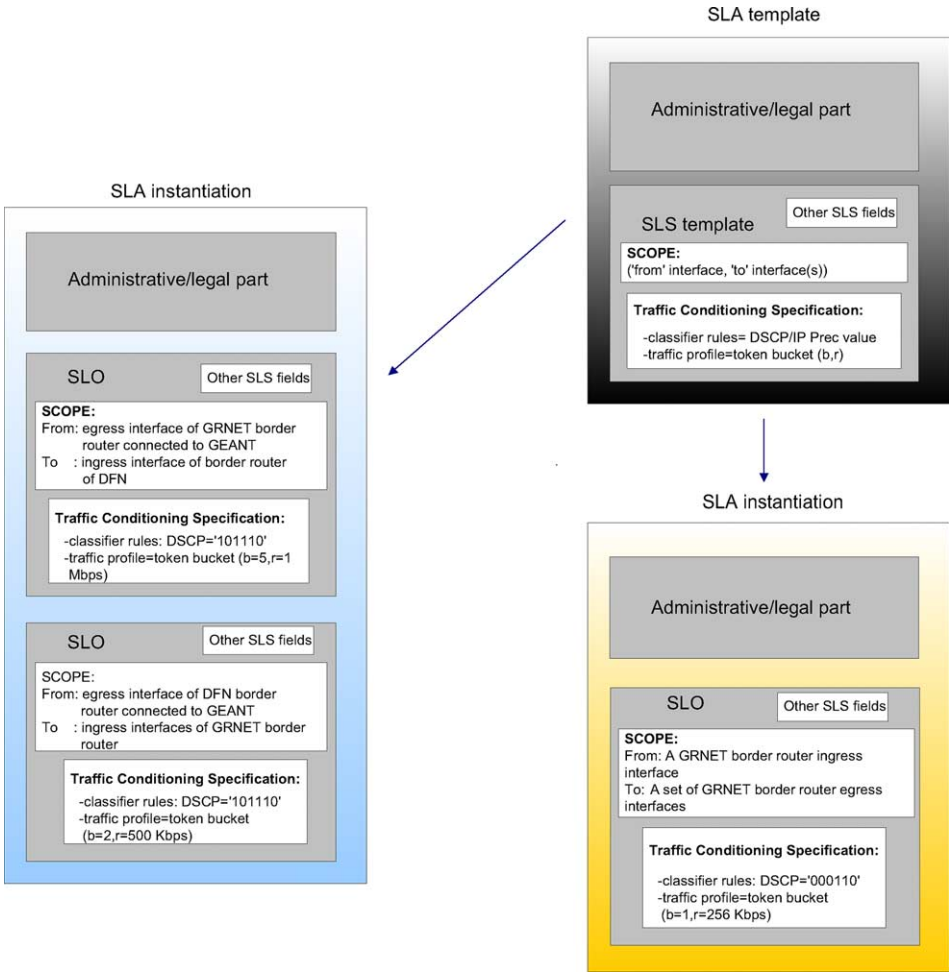

Fig. 1. SLA template, SLA instantiations, SLS and SLOs.

system). The section should also provide a service availability ratio according to the SLA's duration in time in comparison, an Unavailable Time Limit (UTL) and formulas for the calculation of compensation for unavailability.

- *Monitoring*. This section should specify how and when (constantly vs. periodically) is the SLA monitored. It should specify the points of network topology where monitoring equipment is installed or where measurements are retrieved from. It should also specify the SLS metrics that are visible to the client and how the client can have access to this monitoring data.
- *Response times*. This section concerns the overall response times guaranteed by the provider in cases of client requests for adjustment of the SLA (and/or SLS) and for necessary configuration of the relevant devices.

- *Fault handling-trouble ticket*. This section should specify the actions taken by the provider when faults concerning the delivery of the service defined in the SLS occur and the corresponding reaction times.
- *Quality and performance of support and helpdesk*. This section should thoroughly specify the contracted service's support infrastructure.
- *Pricing of the contracted service*. Pricing of the service provided is a crucial part of a SLA between a client and a provider of network services. In order for a DiffServ pricing scheme that will efficiently reflect the service value and will maximize or meet several criteria (client revenue, efficient resource allocation, accepted service requests, etc.) a very thorough and interdependent with the SLA monitoring and accounting infrastructure has to be used.
- *Description of the service*. A general description of the provided service, describing qualitatively its characteristics (in terms of, e.g. delay, packet loss, throughput) and operation has to be provided here.

2.2. The SLS part

The proposed SLA template applies directly to the case where a transport domain establishes agreements for the provision of connectivity services with its customers in a uni-directional manner. Based on this assumption, the SLS part of the SLA is proposed to contain the following fields:

(i) *Scope*. The scope field should define the topological region to which the service defined at the SLS will be provided. This field, according to (Blake, 1998), must specify where packets conforming to the SLS are entering and exiting a DiffServ domain. The recommended field is:(egress interface of upstream domain, set of ingress interfaces of downstream domains).

(ii) *Flow description*. The flow description field will indicate for which IP packets the QoS guarantees of the specific SLS is to be enforced or in other words, which packets will receive the PHB treatment resulting in the QoS guarantees of the SLS. The flow descriptor is suggested to be the DSCP or IP Precedence value that can uniquely identify the packets to receive the SLA-specific service. However, additional information, already present in the packets (source or destination IP addresses, protocol type, etc.) or derived from the network topology, can optionally be included in the flow description field.

(iii) *Performance guarantees*. The performance guarantees field depicts the guarantees that the network offers to the customer for the packet stream described by the flow descriptor over the topological extent given by the scope value. A set of performance parameters for service-compliant traffic (in accordance with the IETF IP Performance Metrics Working Group, Roth, 2003) that applies to the case of the EF-based service but also to other DiffServ-based services is the following:

- *One-way delay (OWD)*. It is suggested to be guaranteed as the maximum packet transfer delay measured between the scope-defined points. A quintile could also be optionally defined to specify the delay guarantee in 99.5% of the cases, since users might find the worst-case figure misleading.

- *Instantaneous Packet Delay Variation (IPDV)*. It is suggested to be guaranteed as the maximum packet transfer delay variation measured between the scope-defined points. Again a quintile could also be optionally defined to specify the IPDV guarantee in the majority of cases.
- *One-way packet loss (OWPL)*. It is suggested to be guaranteed as the ratio of lost in-profile packets between the scope endpoints over the total of injected in-profile packets at the ingress point defined by the scope field. It is suggested that the appropriate numbers are based on the actual contracted values for the transmission lines and modified (increased) to take into account the service-induced figures.
- *Capacity*. It is defined as the rate measured at the set of egress points (defined by the scope field) of all packets identified by the flow descriptor.
- *Maximum Transmission Unit (MTU)*. It is the largest physical packet size in bytes that the SLS guarantees to be transmitted without being fragmented. The suggested value for a WAN is 4470 bytes.

(iv) *Traffic envelope and traffic conformance*. The traffic envelope is a set of traffic conformance (TC) parameters describing how the QoS service entitled traffic aggregate from an upstream domain should look like in order to get the guarantees indicated by the performance parameters of the SLS. The traffic conformance algorithm itself is part of the SLS, describes how is traffic examined against the targeted/contracted behaviour and has as its input the traffic conformance parameters. It is possible to have either a binary-based or a multi-level based TC algorithm, with the binary-based algorithm identifying packets as either 'in-profile' or 'out-of-profile' as appropriate.

(v) *Excess treatment*. This attribute specifies how excess traffic (or out-of-profile traffic, according to the profile described by the traffic envelope and traffic conformance field) is treated (e.g. dropping of packets).

(vi) *Service schedule*. This field indicates the start time and end time of the period for which the service is provided. It is suggested to be of a month range, either a single month or a group of sequential months.

(vii) *Reliability*. Reliability should define allowed mean downtime per year (MDT) and maximum allowed time to repair (TTR) in case of breakdown for the provision of the service described by the SLS. The values of these parameters must be compliant with the guarantees provided via the administrative part of the SLA.

3. End-to-and SLA establishment

SLA definition between two peers is the structural unit for the establishment of e2e services. Provided that bilateral SLAs are properly defined all the way from the desired origin to the desired destination, proper mechanisms (such as the Bandwidth Brokers, see also (Davie, 2002; Goderis, 2000; Internet2 QoS group) can evaluate all connections between consecutive peers and determine the resources (according to the SLAs) that are available for serving requests for the specific service. This procedure can successively conclude with a valid outcome on whether the end-to-end service can be provided or not

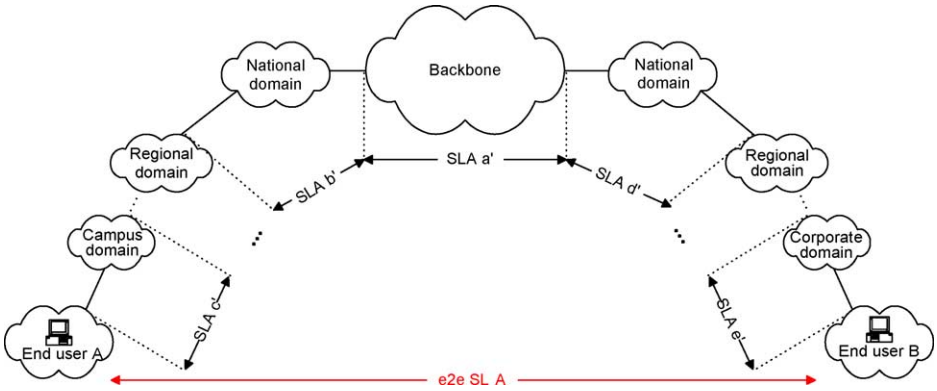

Fig. 2. E2e SLA establishment topology.

(based on the individual SLAs), and which are the specific quality features of the service provided.

End-to-end configuration and seamless provisioning of QoS has a number of peculiarities that must be dealt with. An end-to-end SLA is essential in co-ordinating the service's provision across multiple independently managed domains in a way that end users perceive a stable and predictable service with predefined quality guarantees, regardless of the domains and bilateral SLAs involved. Instead of providing an automated mechanism for e2e SLA establishment, this section will attempt to define the necessary off-line procedures.

As depicted in Fig. 2, in order for the e2e SLA to be established, a chain of bilateral SLAs must exist in advance. The figure depicts an indicative scenario for the provisioning of a service supported by DiffServ mechanisms across consecutive transport domains from one end-user A located in a campus network, to another end-user B located in a corporate domain. In order for this communication to be feasible, traffic crosses a number of regional and national backbones, through an international backbone network.

The individual bilateral SLAs must be defined in a consistent manner, in such a way that no part of the e2e path is left uncovered. The aim of each bilateral SLA between domain D1 and domain D2 is to define the procedural and qualitative guarantees provided as D2 carries the SLA-defined specific portion of traffic of D1 across D2. Instead, the aim of the e2e SLA is to define the guarantees provided to SLA-compliant traffic originating from end-user's A premises up to the end-user B equipment.

In order for the e2e SLA to be established a number of steps must be taken:

Step 1: Collection of the e2e chain SLAs. This step of the e2e SLA establishment procedure should initially perform a validation check of the bilateral SLAs along the path from the one end user to the other. This procedure should ensure that bilateral SLAs exist along the path from the source to the destination and are compliant with the requested services' primary principles, for example absolute priority scheduling and policing at ingress of each domain for the case of the EF-based DiffServ service.

In cases where even one of the involved SLAs fails to provide the basic guarantees of the corresponding service class, then the e2e SLA cannot be established. In such cases, an alternative e2e path through domains with appropriate bilateral SLAs should be sought for.

Step 2: Filling in the administrative/legal part of the e2e SLA. At this step the administrative part of the e2e SLA must be filled in, as follows:

- *Administrative and technical parties involved*: This field is more likely to contain the service administrative and technical contacts for the end-users' access domains, derived from the corresponding bilateral SLAs (i.e. SLA c' and SLA e' in Fig. 2).
- *Duration in time*: This section should contain the period for which the e2e SLA is valid. This period has to belong to a common time period among all 'service schedule' fields of the bilateral SLA involved and if such a time period exists, it is up to the end-users' to define the e2e SLA's duration as part of that time period.
- *Availability guarantees*: This section should contain the e2e service's availability in time units. This field can also be explicitly derived from the corresponding fields of the involved bilateral SLAs. For a typical backbone network, and the bilateral SLAs signed with adjacent domains, unavailability or degraded performance guarantees could be of half or one day's order of magnitude. The e2e SLA has to anticipate for the worst-case scenario, in which all bilateral SLAs' unavailability periods never overlap. In that case, the unavailability guarantees provided by the e2e SLA are calculated as

$$\text{unavailability}_{\text{e2e}} = 100 - \left(\sum_i \text{unavailability}_{\text{SLA}_i}\right)\%$$

  where unavailability is expressed in percentage of the SLAs duration in time.
- *Monitoring*: This section should specify how and when (constantly vs. periodically) will the e2e SLA be monitored. It should specify the points of network topology where monitoring equipment is installed or where measurements are retrieved from. This section should also specify non-network oriented metrics for the evaluation of the end-user perceived quality by the service provision, which are most likely to depend on the application(s) using the service. More details on a proposed monitoring infrastructure are provided in Teitelbaum and Shalunov (2002).
- *Response times*: This section concerns the overall response time guaranteed in cases of end-users' requests for adjustment of the e2e SLA. This field should anticipate for the maximum corresponding field among all involved bilateral SLAs.
- *Fault handling-trouble ticket procedures*: This section should specify the actions taken by the e2e SLA administrative and/or technical contacts when faults concerning the delivery of the service defined in the e2e SLA occur. It should define the procedures for the involved bilateral SLAs' contact people to be informed. It should anticipate for the worst-case scenario of overall reaction times.
- *Quality and performance of support and helpdesk*: This section should specify the contracted service's support infrastructure. It is recommended that the e2e SLA appoints support contacts within the end-users' access domains and that these contacts are then responsible for communication with the different domain helpdesks along the chain of bilateral SLAs.
- *Pricing of the contracted service*: Pricing of the e2e service is an extremely demanding functionality that should take into consideration the pricing structures along the end-to-end path as well as compensations in cases of SLA violations.

- *Description of the service*: This section should contain a general description of the provided service, describing qualitatively its characteristics (in terms of, e.g. delay, packet loss, throughput), operation and use.

Step 3: Definition of scope and flow description for the e2e SLA. According to the basic principles of bilateral SLAs already presented, the scope and flow description fields of the e2e SLA should be defined as follows:

- The scope field should define the topological region to which the service defined at the SLA is provided. For the e2e SLA, this field should specify the egress interface of the access domain (covered by SLA c' in Fig. 2) through which the source end-user's traffic is injected to the topology and the ingress interface of the destination domain (covered by SLA e' in Fig. 2) through which traffic reaches the destination end-user.
- The flow description field in an e2e SLA should uniquely identify the packets entitled to the specific service, sent from end-user A to end-user B through a number of interconnected domains. As such it should definitely specify the DSCP value of packets (as marked by end-user A, e.g. DSCP 46 for EF traffic) and preferably a valid (IP source, IP destination address) pair to ensure proper identification and treatment of packets by the end-user's A access domain and all the involved domains on the e2e path.

Step 4: Determination of the e2e SLA performance guarantees, based on bilateral SLAs' guarantee. At this point, it has to be clarified that bilateral SLAs, such as that between the backbone domain (e.g. GEANT) and national domains (e.g. GRNET) of Fig. 2, usually concern the bulk of a service class's traffic served through consecutive domains. However, an e2e SLA is related to the quality and quantity delivered to a limited number of flows between two end users. As such, the e2e SLA is proposed to initially adopt the qualitative guarantees derived from the bilateral SLAs involved in the service provision along the path between the two users. At the same time, the e2e SLA is proposed to define the quantitative metrics (throughput, MTU) according to the specific needs of the end users. An important step of the e2e SLA establishment procedure is to ensure that the existent bilateral SLAs are such that they can support the e2e SLA requested. In other words, in order for the e2e SLA to be feasible:

- The throughput of traffic supported by the chain of bilateral SLAs must be at any part of the e2e chain (i) larger than the sum of already supported e2e SLAs and (ii) larger than or equal to the sum of already supported e2e SLAs plus the throughput of the e2e SLA requested.
- The minimum MTU value along the chain of bilateral SLAs has to be larger or equal than the MTU of the e2e SLA requested.

The metrics required for the e2e SLA establishment in the case of the EF-based service are:

- OWD from the premises of end-user A up to the premises of end-user B. OWD is an additive metric and therefore, the guarantees provided by the e2e SLA must obey to:

$$d_{\mathrm{e2e}} \geq \sum_i d_i$$

where d_i belongs to each one of the bilateral SLAs i, combined in order to build the e2e SLA.

- *Capacity*. Guaranteed capacity for the e2e SLA must be equal to or less than the minimum capacity guarantee provided to the flow(s) identified by the aforementioned 'flow description field' over all the involved bilateral SLAs

$$c_{\text{e2e}} \leq \min_i \{c_i\}$$

It is at this point that the establishment of the e2e SLA depends on whether the total available (not dedicated to other e2e SLAs) capacity along the chain of the bilateral SLAs is sufficient to satisfy the current e2e SLA's capacity demand.

- *IPDV*. Guaranteed IPDV for the e2e SLA must be equal to or larger than the sum of the jitter guarantees provided by all the involved bilateral SLAs

$$j_{\text{e2e}} \geq \sum_i j_i$$

where j_i belongs to each one of the bilateral SLAs i, combined in order to build the e2e SLA.

- *OWPL*. Guaranteed packet loss for the e2e SLA must anticipate for the worst-case scenario, in which, as the source end-user's packets cross consecutive domains, the maximum number of drops occurs in the range of each bilateral SLA. Thus,

$$l_{\text{e2e}} \leq \prod_i l_i$$

where l_i is the maximal packet loss guaranteed by each one of the bilateral SLAs i, combined in order to build the e2e SLA.

- *MTU*. The MTU value that is valid for the e2e SLA is the minimum MTU value over all the involved bilateral SLAs

$$\text{MTU}_{\text{e2e}} = \min_i \{\text{MTU}_i\}$$

Again here, the establishment of the e2e SLA depends on whether the minimum MTU value along the chain of the bilateral SLAs is sufficient in order not to violate the current e2e SLA's MTU value.

Step 5: E2e SLA traffic envelope and traffic conformance definition. A usual common traffic conformance algorithm (TCA) is that of a token bucket with r as the rate (in bits per second) and b (in packets) as the depth parameters, which identifies packets as either 'in-profile' or 'out-of-profile' based on an average rate and burstiness of the flow. For the e2e SLA, the token bucket TCA should be applied to all marked according to the SLA-compliant traffic injected by end-user A to the ingress interface of his access domain.

For the token bucket parameters, depending on the service for which the SLA is established, different values can be used. For the case of the high-quality EF-based service the following values are suggested

$$b = \{1 \ldots 3\} \text{ packets}, \quad r = 1.2 \times c_{\text{e2e}}$$

where c_{e2e} is the contracted by the e2e SLA capacity for the specific service class between the two end-users (see also Verma, 1999 for more details on these values).

Step 6: E2e SLA operational fields. For the e2e SLA, excess traffic (or out-of-profile traffic, according to the profile described by the traffic envelope and traffic conformance field) is recommended to be either dropped or remarked as best-effort at the ingress interface of end-user's A access domain.

The service schedule field defines the start time and end time of the period for which e2e service according to the SLA is provided. It should obey to the limitations of the administrative part of the e2e SLA and should be equal to or less than the e2e SLA's duration period.

Reliability should define allowed mean downtime per unit of time for the service provision (e.g. a day, a week, a month, etc.) and maximum allowed time to repair (TTR) in case of breakdown for the provision of the e2e service described by the e2e SLA.

3.1. End-to-end SLA verification

In order for the verification of an e2e SLA based on a chain of bilateral SLAs, a monitoring infrastructure has to be defined. This monitoring infrastructure should consist of:

- ☐ Monitoring equipment/functionality placed in intermediate positions along the e2e path from end-user A to end-user B (Fig. 2), referred to as Service Providers' Monitoring Equipment (SPME) from now on.
- ☐ Monitoring equipment/functionality located at the premises of each end-user, referred to as End-users' Monitoring Equipment (EME) from now.

As already explained, bilateral SLAs signed between service providers tend to be of a more permanent nature than e2e SLAs between end-users. Therefore, the existence of SPME is primarily essential for the establishment and monitoring of bilateral SLAs. SPME has to be located in critical positions of the domains involved in a bilateral SLA, in order to constantly monitor performance of the service provided and indicate possible causes and origins of a service malfunction.

For the case of a bilateral SLA, SPME is compulsory to exist on all interfaces included in the scope field of the SLA. For example, in the case of a bilateral SLA for EF-based

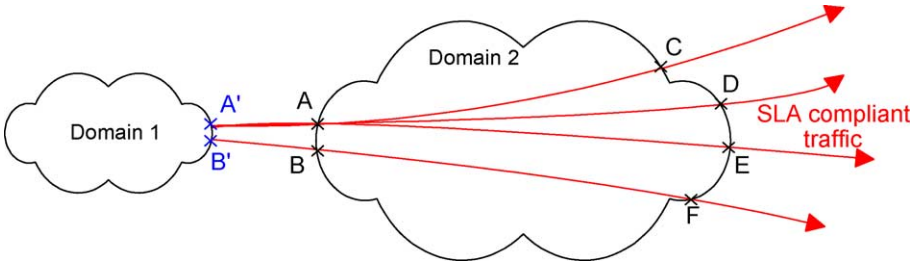

Fig. 3. Monitoring infrastructure's suggested locations for a bilateral SLA.

service connectivity between Domains 1 and 2 (Fig. 3), SPME should exist on all interfaces A–E in order for the SLA to be properly monitored.

For its own purposes or for the purpose of monitoring bilateral SLAs with upstream domains, Domain 1 of Fig. 3 might also choose to place SPME on interfaces A′ and B′. Furthermore, each domain might choose to deploy a monitoring infrastructure within its administrative borders. This infrastructure, although not directly involved in the bilateral SLA monitoring procedure, might help in isolating deficiencies in the service provision within a domain. The latter will be particularly useful when monitoring between edge interfaces (e.g. A and C) results in violation of the bilateral SLA guarantees.

Provided that bilateral SLAs along the e2e path between two end-users are monitored as already outlined, then the quality guarantees of each individual bilateral SLA are constantly monitored. They can, therefore, be used in the e2e SLA establishment process that was described in the previous sections, in order to derive the e2e guarantees that can be achieved.

However, after the establishment of the e2e SLA, the end-users must also be provided with tools (EME) to verify the quality and quantity of throughput provided by the service. Due to the nature of e2e SLAs, which are of a less permanent nature than bilateral SLAs between domains, EME cannot be based on hardware and complex procedures. Therefore, it is suggested that end-users are provided with a set of software-based, active monitoring tools, referred to as Software Management Tools (SMTs) from now on, allowing them to observe the performance of the provided service at regular intervals. SMTs are also strongly suggested because they do not require time synchronization between the end-users' equipment and are, therefore, easier to deploy. SMTs provided to end-users must be accompanied by a set of scripts for processing the logs created during the SMTs' operation and guidelines for a set of parameters that need to be configured for each SMT's operation.

Any indication of violation of the guaranteed quality and throughput emerging from the EME, will have to be communicated to the e2e SLA's technical parties involved (see also Section 4 on relevant procedures). After that, an investigation of the individual bilateral SLA's monitoring data along the e2e path will have to performed in a recursive manner, in order for the problem to be located and solved. The hierarchy of SPME already outlined (both in the borders of consecutive domains and the interior of each domain) should be exploited in this direction, based on the procedures for fault handling specified in each bilateral SLA.

4. Service provisioning procedures

The provision of a DiffServ-based service connectivity between two end-users has to be established through a number of phases, depicted in Fig. 4. At the beginning, a negotiation phase should clarify the entities involved, the purpose for which service connectivity will be used, the feasibility of service provision, etc.

During the service set-up phase, all details about the service's provision have to be collected, the necessary SLA/SLSs have to be signed and detailed configuration of the equipment involved must be performed.

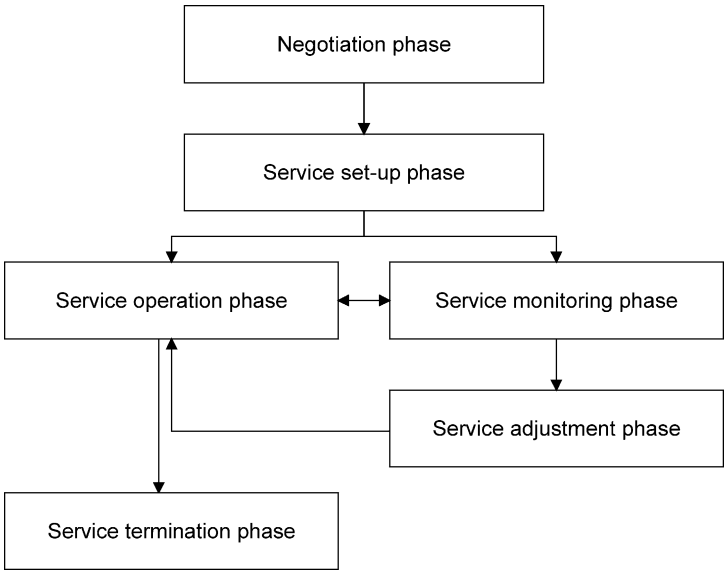

Fig. 4. Phases for service provision.

During the service operation phase, no specific activities have to be performed unless indications of service failure occur. In such a case, measures have to be taken so that the service operation is restored. In parallel to the service operation phase, the monitoring phase should take place, comprising of constant measurement activities with the purpose of verifying the service's required quality. Within the monitoring phase it might occur that the service's performance deviates from the desired one. At this point a service adjustment phase will have to be initiated, involving adjustment of configuration along the service's provision path.

A service adjustment phase always results in new service operation and monitoring phases, running in parallel, until the service's provision time frame expires and the service termination phase is introduced. This section will mainly deal with the negotiation and service set-up phases, while also attempting to assign responsibilities for the rest of the phases.

Due to the multiple domains involved in the provision of an end-to-end DiffServ-based service, it is necessary for a number of entities to be appointed and involved in the different service provision phases. The following paragraphs attempt to provide a methodology for this, based on the GEANT–NREN architecture used as a reference model.

For the co-ordination of the negotiation, set-up and operation phases it is strongly recommended that the end-users appoint a common representative (the Service Provision Coordinator, SPC) who will be the mediator between the involved networks and end-user sides, coordinating the service provision establishment procedure as well as any tasks required during the operation phase.

It is also strongly recommended that a technical person is appointed as responsible for the service provision and implementation for each of the end-user sides. In consistence with the provisioning scenario of Fig. 2, Fig. 5 depicts how a technical contact

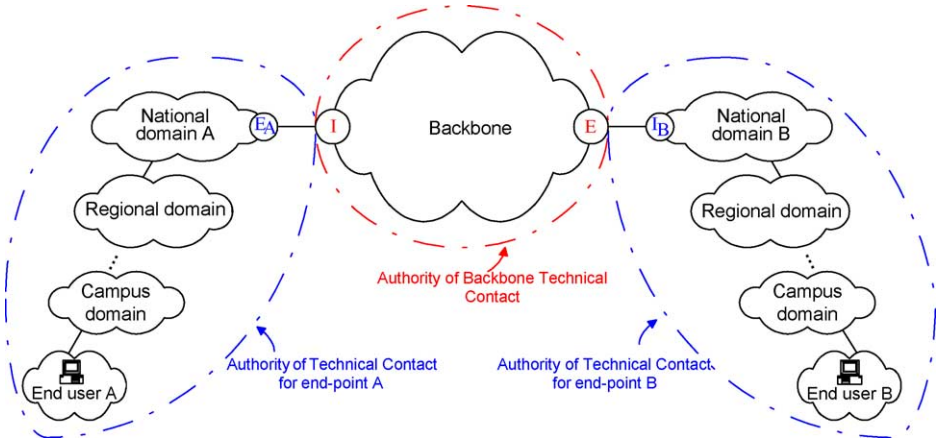

Fig. 5. Delegation of authorities for service provisioning procedures.

(Technical Contact A or TC A) should be responsible for the service set-up and maintenance from end-user's A domain up to the egress interface of national domain A (E_A) and, in an analogous manner, another technical person (Technical Contact B or TC B) should be responsible for the service from the national domain B ingress interface (I_B) up to end-user's B domain. Ideally these technical contacts should belong to the NOC of each side's national domain.

Similarly, the backbone network has to appoint a technical person for the provision and maintenance of services supported by offered SLAs. As depicted in Fig. 5, the backbone technical contact (BTC) will be responsible for the specific service provisioning from *I* up to *E*, while at the same time providing any feedback required to the TCs from each end-user's side.

From Fig. 5, it is obvious that the A and B TCs, being responsible for service set-up and provisioning at each end-user's side, will have under their supervision the set-up and operation of the service for more than one domains (at least two in an international connectivity basis: national domain and end-user domain). This makes their job quite demanding, in the sense that they might have to coordinate service provisioning beyond the borders of the domain they can directly control. Therefore, their duties, apart from communicating with the BTC will include providing technical assistance to all the domain administrators involved in their authority (see 'blue' clouds in Fig. 5). This means that TC A and TC B will have to translate specific service provision rules (such as priority scheduling for the case of EF-based services) to the specific equipment available within their authority whenever they are requested to do so. Moreover, they will be responsible (with the help of the SPC) for collecting and maintaining all necessary contact information for technical contacts within their authority region.

In this way, service provisioning from a technical point of view will be performed in a hierarchical manner, with the BTC and each end-user side TC being on the top of the hierarchy and any other technical entities involved in each end-user side, being co-ordinated by the corresponding end-user side TC (see Fig. 6).

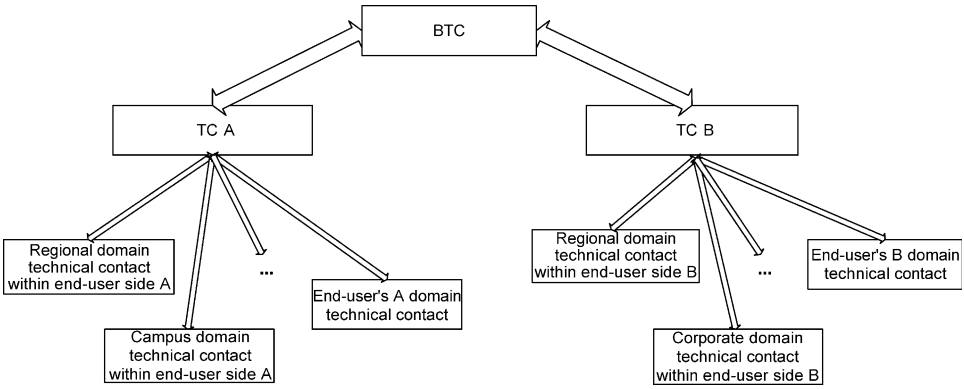

Fig. 6. Hierarchical communication of technical contacts involved in service provision wrt Fig. 1.

Apart from the technical responsibility, it is required that each end-user side appoints a person responsible for the performance evaluation of the service from the involved applications' point of view. These Performance Evaluation Contacts (PEC A and PEC B) are, in other words, responsible for checking whether the service implementation is delivering to the end-users the quality they need and if not will advice adjustments to the SLA/SLSs. Their recommendations for adjustments should then be delivered to the TCs of each side via the SPC in order to be translated into re-configuration actions in the equipment involved.

Fig. 7 depicts a possible way for the proposed entities' communication, with the SPC acting as an intermediate between TCs, PECs and the user sides. Alternatively, in order to reduce communication overhead, end-users could avoid direct contact with the SPC and communicate any information via the PEC of each end-user side.

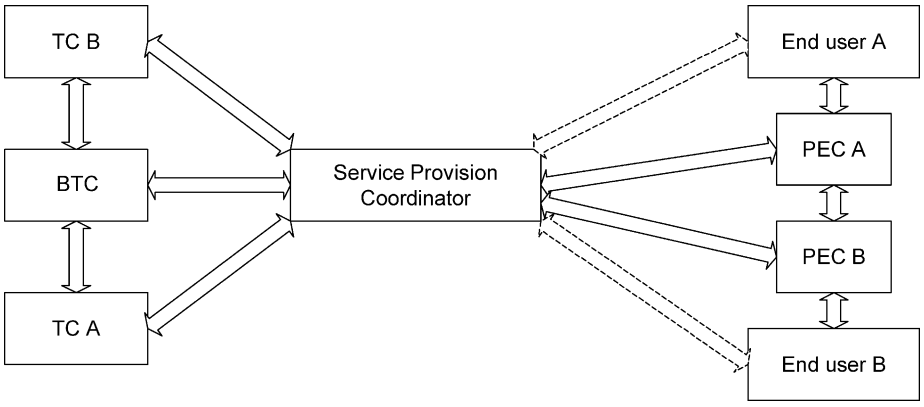

Fig. 7. Entities involved in the provision of the SLA-defined service.

5. Conclusions

SLA specification for DiffServ-enabled networks aims at ensuring compatibility of the services provided across consecutive domains, providing positive quality guarantees and setting out the limits of the services provided. Such SLAs move one step forward in the direction of traditional ones, in the sense that they do not only have to specify availability, security, quantity of allocated resources and a number of other quantitative values, but also have to specify the values of appropriate quality parameters. In networks where QoS is inherently supported (such as ATM), the provision of SLAs comes as a natural delimitation of the relevant parameters. However, in IP networks where best-effort traffic has no quality guarantees, the introduction of qualitative services requires a thorough and accurate engineering of QoS metrics in the SLA specification on top of the guarantees for availability and characteristics of the transport medium, security, fault handling, etc.

In this work, we have defined a framework for the establishment of a bilateral SLA according to the principles of DiffServ-based service provisioning. The proposed administrative and SLS parts of the SLA are thoroughly presented, in an effort to capture all the technical parameters entailed in provisioning a service with qualitative guarantees. Based on the bilateral SLA specification, a methodology for the establishment of end-to-end SLAs is proposed and the co-ordination of entities involved in the end-to-end SLA establishment is described. Although this work makes a step towards the definition of structured and detailed SLAs for QoS guarantees' provisioning in IP networks, more work is needed in order for DiffServ-based SLAs to become fully functional and efficient, and thus comprise useful tools for network administrators and providers. Another major area of interest is to devise the mechanisms and procedures for identifying and handling violations of the proposed pre-defined SLAs, for re-negotiation and pricing of SLAs, incorporating also compensation mechanisms in cases of failures. Such issues have not been addressed by this work and will be part of our future work on SLAs for QoS-enabled IP networks.

References

Blake S, et al. An architecture for differentiated Services IETF RFC 2475, December 1998.

Bouras C, Campanella M, Sevasti A. SLA definition for the provision of an EF-based service 16th International Workshop on Communications Quality and Reliability (CQR 2002), Okinawa, Japan, May 14–16 2002 p. 17–21.

Davie B, et al. An expedited forwarding PHB (Per-Hop behavior) IETF RFC 3246, March 2002.

Fankhauser G, Plattner B. DiffServ bandwidth brokers as mini-markets Workshop on Internet Service Quality Economics, MIT, US, December 2–3 1999.

Goderis D, et al. D1.1: Functional architecture definition and top level design, TEQUILA project: traffic engineering for quality of service in the internet, at large scale IST-1999-11253, September 2000.

Internet2 QoS group, QBone bandwidth broker architecture, Work in progress, accessible at: http://qbone.internet2.edu/ bb/bboutline2.html.

Neilson R, Wheeler J, Reichmeyer F, Hares S, editors. A discussion of bandwidth broker requirements for Internet2 Qbone deployment. Internet2 Qbone BB Advisory Council, Version 0.7, August.

Nichols K, Jacobson V, Zhang L. A two-bit differentiated services architecture for the Internet IETF RFC 2638, July 1999.

Paxson V, Almes G, Mahdavi J, Mathis M. Framework for IP performance metrics IETF RFC 2330, May 1998.
Rajan R, Celenti E, Dutta S. Service level specification for inter-domain QoS negotiation, draft-somefolks-sls-00.txt Internet Draft, November 2000.
Roth R, et al. IP QoS across multiple management domains: practical experiences from pan-European experiments. IEEE Commun Magaz 2003;41(1).
Salsano S, et al. Definition and usage of SLSs in the AQUILA consortium, draft-salsano-aquila-sls-00.txt Internet Draft, November 2000.
Teitelbaum B, Shalunov S. Why premium IP service has not deployed (and probably never will) Internet2 QoS Working Group Informational Document, May 3 2002 found at: http://mail.internet2.edu:8080/guest/archives/qbone-arch-dt/log200205/msg00000.html.
Verma D. Supporting service level agreements on IP networks. USA: McMillan Technical Publishing; 1999.

Further Reading

Liakopoulos A, Maglaris B, Bouras C, Sevasti A. Providing and verifying advanced IP services in hierarchical DiffServ—the case of GEANT. Int J Commun Syst 2004;321–36.

Christos Bouras obtained his Diploma and PhD from the Computer Science and Engineering Department of Patras University (Greece). He is currently an Associate Professor in the above department. Also he is a scientific advisor of Research Unit 6 in Research Academic Computer Technology Institute (CTI), Patras, Greece. His research interests include Analysis of Performance of Networking and Computer Systems, Computer Networks and Protocols, Telematics and New Services, QoS and Pricing for Networks and Services, e-learning, Networked Virtual Environments and WWW Issues. He has extended professional experience in Design and Analysis of Networks, Protocols, Telematics and New Services. He has published 150 papers in various well-known refereed conferences and journals. He is a co-author of five books in Greek. He has been a PC member and referee in various international journals and conferences. He has participated in R&D projects such as RACE, ESPRIT, TELEMATICS, EDUCATIONAL MULTIMEDIA, ISPO, EMPLOYMENT, ADAPT, STRIDE, EUROFORM, IST, GROWTH and others. Also he is member of, experts in the Greek Research and Technology Network (GRNET), Advisory Committee Member to the World Wide Web Consortium (W3C), Task Force for Broadband Access in Greece, ACM, IEEE, EDEN, AACE and New York Academy of Sciences.

Afrodite Sevasti obtained her Diploma from the Computer Engineering and Informatics Department of Patras University in Greece. She holds a Master of Science in Computer Science & Engineering from the same Department, where she is also a PhD candidate. She also holds a Master of Science in Information Networking from the Information Networking Institute of Carnegie Mellon University. She has worked as an R&D Computer Engineer at the RA Computer Technology Institute (Greece) and she is currently with the Greek Research and Technology Network (GRNET) S.A. Her main interests and expertise lie in the fields of Computer Networks, Telematics, Distributed Systems and especially in technologies and architectures of high performance networks, in traffic and network resources' management, in Managed Bandwidth Services, provisioning of Quality of Service (QoS), SLAs and pricing/billing of next generation networks. She has published 17 papers in well-known refereed conferences and journals. She has participated in several R&D projects.