A Distributed Admission Control Model for CoS Networks using QoS and SLS Monitoring

Solange Lima, Paulo Carvalho, Alexandre Santos, Vasco Freitas
University of Minho, Department of Informatics, 4710-057 Braga, Portugal

***Abstract*— Achieving an admission control strategy for CoS networks covering both intra-domain and end-to-end operation is still an open issue. This paper discusses how AC can be carried out without adding significant complexity to the network control plane and proposes a distributed service-oriented AC model for these networks. The model only involves the network edge nodes leaving the network core unchanged. Ingress nodes perform implicit or explicit service-dependent AC based on both QoS and SLSs utilization metrics, obtained through edge-to-edge on-line monitoring performed at egress nodes. From an end-to-end perspective, the flow request is used both for AC and available service computation. Relevant aspects of the model interrelated areas and implementation key points are also discussed.**

I. Introduction

Both in flow-based and class-based QoS architectures controlling the admission of traffic entering the network allows to: (i) avoid over-allocation of existing network resources; (ii) avoid new flows from impairing flows already accepted; (iii) fulfill service level agreements and specifications (SLA/SLS); and (iv) prevent instability and assure QoS. Despite its need, the complexity introduced by AC in the network control plane has to be carefully assessed as Internet traffic is highly dynamic and not every application has strict QoS requirements.

Despite the existing proposals (discussed in section II-C), achieving a generic, yet feasible and light, AC model for multi-service CoS networks, able to operate both intra- domain and end-to-end, is still an open issue. This paper proposes a new and encompassing service-oriented AC model. The underlying idea is to take advantage of the consensual need for on-line QoS and SLS monitoring in CoS networks and use the resulting information to perform distributed AC. Resorting to edge-to-edge on-line monitoring of relevant QoS parameters for each service type and SLS utilization (which are used to update an Ingress-Egress Service Matrix) the proposed model controls both the QoS levels in the domain and the sharing of the existing SLSs between domains. The end-to-end operation is treated as a repetitive process of AC on a domain basis and available service computation. The model design is driven by simplicity, easiness of deployment and flexibility as regards technological, service and application evolution goals. These goals are relevant when deploying the model across multiple administrative domains with distinct QoS solutions. This is achieved without changes in the core, and reducing state information, signaling, intrusion and latency.

The paper is structured as follows: the AC problem statement focusing on its perspectives, driving vectors and current approaches is reviewed in section II. The description of the proposed AC model, including its related areas, operational details and key points are discussed in section III. Conclusions are presented in section IV.

II. The Admission Control Problem

A. AC Perspectives

When AC takes an SLS as reference, two AC perspectives can be considered: (i) *flow AC* ensures that the admitted flows from a customer are within the capacity of the contracted SLS; or (ii) *SLS AC* ensures that the accepted SLSs for a service type can be honored through proper configuration and provisioning (see Fig. 1). Although these are distinct AC perspectives, they follow similar principles. Whereas flow AC is based on the traffic profile and QoS objectives of a flow, SLS AC is based on the aggregate traffic profile and QoS objectives of the SLS. In fact, the semantic of the process is equivalent, only changing the granularity upon which the decision is taken. Therefore, the proposed model, described here for flow AC, can be applied both to flow AC and SLS AC, with minor changes.

B. AC Vectors

Three vectors shall be considered in AC: assurance level, control complexity and (over)provisioning. Overprovisioning is actually the most common way to provide QoS guarantees in network backbones. Although for few ISPs overprovisioning is an attainable solution, it leads to poor resource utilization and sometimes is not available, or it is too expensive. So further control has to be in place so that QoS requirements can be honored. In our opinion, some degree of overprovisioning is recommended to relax and simplify the AC process.

The control complexity introduced by the AC process has to be balanced with the assurance level. Depending on the QoS

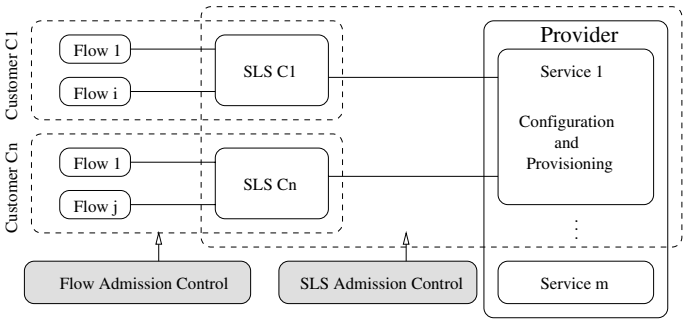

Fig. 1. Flow AC and SLS AC

guarantees and predictability required, more or less complex AC strategies can be used, with strict or relaxed control of network resources and QoS parameters. The type and number of network nodes (e.g. edge, core, central entities) involved directly or controlled by the AC process can also vary, affecting the solution complexity.

C. AC Approaches: A Service Oriented Overview

Associated with CoS-based architectures, such as Diffserv, several AC approaches have been defined, with the common aim of avoiding per-flow state information in the core nodes due to scalability reasons. Some proposals suggest the use of central entities for AC and resource management (bandwidth brokers) [1], [2]. However, the well-known problems of centralization led to several decentralized AC approaches. To provide quantitative service guarantees (e.g. for hard real-time traffic) current AC proposals need to control the state and the load of traffic aggregates in the core nodes [2], [3], or even perform AC in these nodes [3]. These solutions tend to require significant network state information and, in many cases, changes in all network nodes. Furthermore, as they are closely tied to network topology and routing, their complexity increases with the network dynamics.

Providing qualitative service guarantees (e.g. for soft real-time) leads to reduced control information and overhead, but eventually to QoS degradation. Obtaining a good compromise between efficient resources utilization and QoS guarantee is a major challenge. In this context, measurement-based AC (MBAC) solutions have deserved special attention. Initially performed in all network nodes, recent studies suggest that AC decisions should be carried out only at the edges (end-systems or edge routers), using either active (EMBAC) or passive measurement strategies of network load and/or QoS parameters [4], [5], [6]. Despite not requiring changes in the network, EMBAC increases the initial latency and network load as probing is carried out on a per application basis.

The need to control elastic traffic, for more efficient network utilization, has also been discussed and implicit AC strategies (without explicit signaling between the application and the network) have been defined [7]. Conversely, AC approaches for streaming applications commonly use signaling between the application and the network where, upon a traffic profile and QoS objectives description, the network sends an explicit acceptance/rejection message.

A complete survey comparing the main features and limitations of current AC strategies is available in [8].

III. Proposed Admission Control Model

The initial considerations in the design of the AC model were: (i) the control of distinct network services and assurance levels, supporting different application QoS requirements and traffic profiles; (ii) the operation intra-domain and end-to-end, controlling both the available resources in a domain, the sharing of the existing SLS between domains and the end-to-end QoS requirements; (iii) the overhead, efficiency and scalability of the control strategy, i.e. accomplishing AC without adding significant complexity to the network control plane; and (iv) the easiness of deployment and integration in the Internet, introducing minor changes to the CoS network.

The model is based both on edge-to-edge on-line QoS monitoring of relevant QoS parameters for each service type and on SLS utilization control. A monitoring module, present at each egress router, measures the QoS parameters of each service, taking into account the origin ingress router, and also the egress SLSs occupancy. These measurements, which reflect the service availability in the domain, are then used for updating an Ingress-Egress Service Matrix used by AC at the corresponding ingress routers. The AC module operates based on service-dependent AC equations and proper parameters threshold intervals. The decision process can be implicit or explicit, depending on the service characteristics, candidate application types and QoS guarantees.

For flexibility and portability reasons the AC and the monitoring modules are independent. Thus, the monitoring process and its implementation details are hidden from AC module, and can be changed without compromising AC.

A. Model Areas

The model interrelates four main areas (see Fig. 2): (i) *service definition* involves the definition of the parameters and semantic of SLSs and of basic services adapted to different application types; (ii) *on-line monitoring* keeps track of QoS and SLS status in the domain; (iii) *AC decision criteria* involves the establishment of service dependent equations; and (iv) *CoS traffic characterization* provides the knowledge of the statistical properties of the classes in the domain. Finally, the use of policy-based network management concepts is being considered for managing all the involved model components. Security issues, such as authentication and authorization, will be covered in the future. Relevant aspects of each model area will be discussed in more detail in the next subsections.

1) Service Definition: A Service Level Agreement (SLA) is defined as a contract between a customer and a service provider or between service providers, specifying the expected service level. The technical part of an SLA - Service-Level Specification (SLS) - describes the QoS-related parameters.

The definition of SLSs is a key aspect for QoS provisioning. A standardized set of SLS parameters and semantics is critical for delivering end-to-end QoS and for simplifying SLS negotiations. Several working groups are committed to SLS

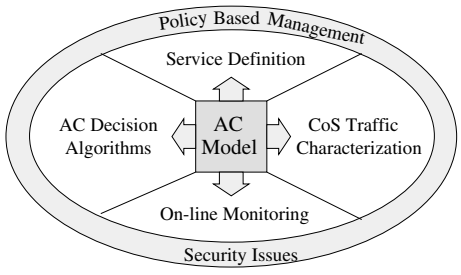

Fig. 2. Model Areas

TABLE I

SERVICE LEVEL AGREEMENT (SLA) TEMPLATE.

Administrative Information	
Administrative entities involved	
Description of service behavior	
Validity of contract	
Pricing/Tariffs	
Helpdesk info/Trouble tickets	
Monitoring/Accounting rules and Type of reports	
Response time to changes	
Other rules: e.g. provisioning	
SLS	
Scope of the Service	- Ingress interfaces - Egress interfaces
Traffic Classifying Rules	- Multi-field criterion - DSCP or ToS Precedence
Traffic Conditioning Rules	- Conformance algorithm - Conformance parameters - Treatment on excess
Expected QoS Parameters	- Delay, jitter, loss,... - Qualitative objectives - Quantitative objectives
Service Reliability	- Mean downtime - Time to repair,...
Service Scheduling	- Start/End time
Others (future study)	- Route, security, ...

TABLE II

UPPER BOUND ON QOS PARAMETERS FOR SOME APPLICATIONS (RT: REAL-TIME; VOIP/I: VOIP/INTERACTIVE; NI: NON-INTERACTIVE; WWW: WWW/FREE SERVICES; SV: STREAM VIDEO (VHS QUALITY)

ITU-T	Class 0	Class 1	Class 2	Class U	
App.	RT	VoIP/I	NI	WWW	SV
IPTD	150 ms	400 ms	1 s	Undef.	400 ms
IPDV	50 ms	50 ms	1 s	Undef.	17 ms
IPLR	10^{-3}	10^{-3}	10^{-3}	Undef.	10^{-5}
IPER	10^{-4}	10^{-4}	10^{-4}	Undef.	10^{-4}

definition [9], [10]. Taking these inputs into account, a possible SLA template including relevant parameters and their typical contents are defined in Table I. Although a large combination of QoS, performance and reliability parameters is possible, service providers will offer a limited number of services. To instantiate the SLS template in quantitative and qualitative standard services adapted to different application types is, in fact, the major objective. To fulfill this, substantial work has been done on identifying the relevant QoS parameters and of the perceived quantitative quality of applications [11], [12]. Table II summarizes acceptable QoS parameters upper bounds for common applications and services. These inputs and Diffserv PDB definitions are used to identify the services and corresponding QoS parameters to test the AC model.

2) On-line Monitoring: Monitoring is also a critical aspect in the proposed model as it is used for QoS and SLS control, which drive AC decisions. Although off-line monitoring is a common approach for SLS control and auditing, current studies highlight the need to perform it on-line [13], [14]. For active QoS control, monitoring has to be on-line so that proper decisions can be taken in useful time.

The problematic of monitoring involves the definition of metrics, measurement methodologies and timing decisions. ITU-T work on QoS in IP networks and particularly IETF IPPM have defined a set of standard QoS and performance metrics and have proposed measuring methodologies for them [12], [15]. Several tools useful for measuring the SLS metrics have also been developed and tested [11], [16].

The measurement methodology can be either passive, active or combination thereof. Passive measurements are made on existing traffic and are particularly suitable for troubleshooting; active measurements inject extra traffic in the network for measurement purposes, allowing to emulate a wide range of test scenarios and to check if QoS and SLS objectives are met in a more straightforward way. The overhead introduced, regarding the traffic pattern in use and the additional traffic load it puts in the network, needs to be considered. However, small traffic volumes may be enough to obtain meaningful measures and these are required in a per-class basis [13], [17]. Defining the location of measurement points is also needed. Measuring edge-to-edge performance and QoS combining link-by-link measures is not an efficient and easy solution. Thus, the use of edge-to-edge monitoring points leads to a more convenient and lighter approach.

Timing decisions deal with the synchronization between measurement points and the periodicity of measurements. For synchronization purposes well-known solutions based on NTP and GPS are usually used. Periodicity decisions should consider that a small time granularity increases the metric computation and dissemination overhead, and eventually leads to an excessive reactivity to short-time traffic fluctuations, whereas a sparse granularity may lead to out-of-date network state information. Depending on the measured parameter and metric purposes, timing definitions can vary significantly. The operating timescales for AC processes, running from few seconds to minutes, are not the most critical.

3) AC Decision Algorithms: In any AC strategy the admission criterion plays a crucial role as regards service guarantees and network efficiency. There are more or less conservative proposals [18], which consider the estimation and control of parameters such as available bandwidth, delay, loss or ECN marks. Most of AC approaches only control the available bandwidth or capacity, comparing it with the flow requested rates. Although being simple for a single link or node-by-node AC, controlling it along the full path is not straightforward. Methodologies and tools for estimating the available path capacity and available bandwidth are in [11], [19]. AC decisions based on thresholds for the other mentioned QoS parameters are also used. They accept or reject a new flow by checking the controlled parameter against a pre-defined limit. Tuning these limits, making them useful indicators of the overall QoS status is a fundamental aspect.

4) CoS Traffic Characterization: The statistical properties of traffic when aggregated into classes [20] need to be considered so that proper thresholds or safety margins to AC can be established. For instance, classes which exhibit long-range dependence may need large safety margins as this property has a significant impact on queuing behavior and on the nature of

congestion, leading to unexpected QoS degradation. Knowing the usual per class traffic volumes is also relevant for traffic forecasting and provisioning.

B. Model Operation Description

Fig. 3 presents the location of the main tasks involved in the model in order to assure intra-domain QoS by controlling the QoS parameters and the fair sharing of the SLSs.

Apart from the usual classification and TC (represented in white) present in CoS networks, specific tasks are needed. Ingress routers perform explicit or implicit AC, depending on the CoS and application type (see section III-C). Egress routers perform on-line QoS monitoring and SLS control. Ingress-Egress QoS Monitoring measures relevant parameters for each service (service metrics), using appropriate time-scales and methodologies (see section III-A.2). The resulting measures reflect the available service from each ingress. SLS Control monitors the usage of SLSs at each egress with downstream domains, to ensure that (internal) traffic to other domains does not exceed the negotiated profiles, and packet drop will not occur by a simple and indiscriminate TC process. QoS monitoring statistics and SLS utilization and associated parameters are then sent to the corresponding ingress routers to update the Ingress-Egress service matrix used for distributed AC. This notification can be carried out either periodically, when a metric value or its variation exceeds a limit or when the SLS utilization exceeds a safety threshold.

The end-to-end case is viewed as a repetitive process of admission control and available service computation (see Fig. 4). In each domain, each ingress performs admission control. If explicit signaling is used (e.g. using RSVP) and the flow is accepted, the ingress node adds the domain service metric values to the flow request to inform the downstream domain of the available service so far. Using the incoming and its own measures each domain may decide if the flow can be accepted. The last AC decision can be taken by the receiver. If the flow is rejected, the application is notified directly from the failure point. This solution leads to a generic AC model, which can be applied both to source and transit domains.

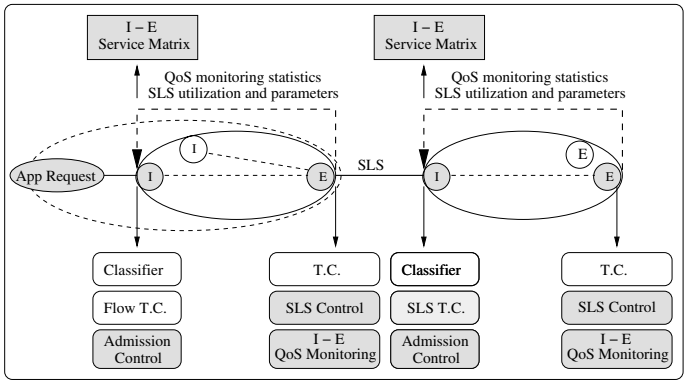

Fig. 3. Domain activities location

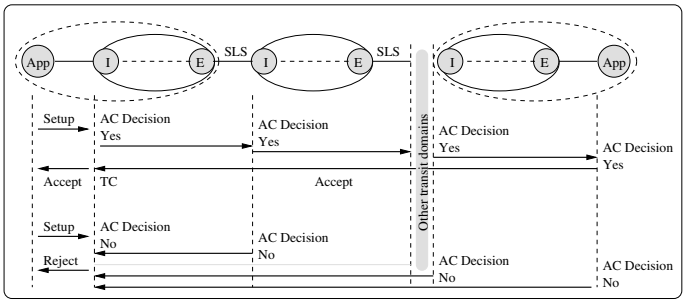

Fig. 4. End-to-end Admission Control Procedure

C. The Criterion for AC

Explicit AC - Explicit flow AC requires two initial verifications (see Fig. 5): (i) SLS Utilization Control checks if the SLS can accommodate the new flow's traffic profile; (ii) QoS Control checks if, for the corresponding egress node and service, the domain QoS metrics, the SLS QoS parameters agreed with the downstream domain[1] and the previous measures (if any) fulfill the application QoS requirements.

Each AC decision is based on a service dependent AC equation and thresholds, defined to achieve specific service guarantees. In general, a conservative criterion will take the worst-case working scenario (e.g. flow peak rates, concurrent AC taking place at other ingress nodes, optimistic measures, etc.). For each class, admission thresholds must be stricter than the class QoS objectives, which in turn, must be stricter than the requirements of all accepted flows.

In the admission process, if one of the tested conditions fails, the flow request is rejected, and the application notified. When the flow is accepted in the domain, the notification may be generated either locally (local admission) or remotely (end-to-end admission). The latter case occurs when an end-to-end availability check is required. In this case (see Fig. 4), the request comprising the QoS measures is propagated across the domains up to the destination, and the notification is sent back to the source, where it may be used to configure flow TC.

Implicit AC - Implicit AC, oriented to applications which

[1]While domain QoS metrics are always checked, when the destination of the flow request is inside the domain, SLS verification is not mandatory. However defining intra-domain SLSs will turn the AC process generic and independent of the destination's location.

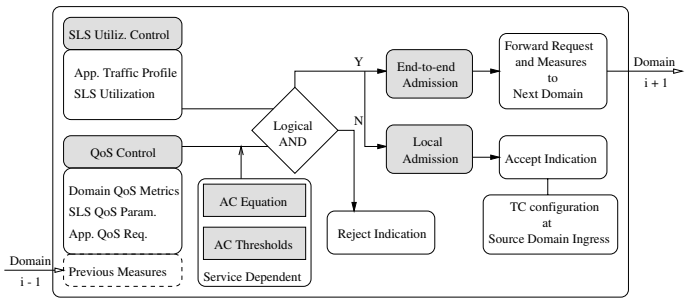

Fig. 5. Admission Control Criterion

do not use signaling and in particular to elastic applications, use implicit detection of flows [7]. This type of AC, likely to be implemented only in the source domain, will be restricted to SLS information and QoS monitoring. Two possible implicit reject actions are (i) SYN packets discarding or (ii) simply packet discarding based on flow accept/reject tables [7].

D. Model Key Points Discussion

The proposed model has important features that should be highlighted, such as: (i) only edge nodes are involved, i.e., the network core is treated as a black-box; (ii) the state information is service/SLS and Ingress-Egress based, which is particularly suitable for SLS auditing; (iii) per-flow state information is only kept at the source domain ingress router for TC, while other downstream domains maintain the TC based on the SLS traffic profile, as usual; and (iv) the signaling process for intra and inter domain operation is simple (the flow request is used for AC and end-to-end available service computation, and does not imply soft/hard state behavior and symmetric routing paths[2].

Performing AC using on-line QoS monitoring avoids extra control mechanisms and simplifies the network control plane. When performed in a systematic way, measurements can be intrinsically auto-corrective and can detect short or long-term traffic fluctuations, depending on the measuring time unit or interval. Additionally, the effect of cross traffic and other internally generated traffic (e.g. routing, management and multicast traffic) is implicitly taken into account.

When comparing to EMBAC solutions, the proposed model reduces the initial AC latency (as the metrics values are available on-line) and avoids per-application intrusive traffic to obtain the metrics. It also allows controlling different services types, QoS parameters and SLS utilization simultaneously. Usually this is only covered in centralized (BB) approaches.

As regards model implementation, key points under current research are: (i) the periodicity of measurements (and corresponding updates), as it determines the validity of information used in AC; (ii) the adequacy of AC equations and thresholds for each service type; (iii) the avoidance of over or false acceptance resulting from concurrent AC decisions at multiple ingress points; (iv) the choice of which egress and SLS to use when more than one path and SLS fulfill the flow request; and (v) the forecast of future network loads (difficult in monitoring based approaches). The first two points (detailed in section III-A) and the use of safety margins to tolerate load fluctuations (e.g. due to concurrent AC) are being tuned in a simulation prototype developed using the Network Simulator (ns-v2). The selection of egress nodes is based on topological information, whereas the selection of SLS is based on specific domain policy rules. When the estimation of future loads is required, the information state of accepted SLSs for the corresponding time period can be used.

[2]There is no guarantee that the path used for the flow data is the same used for the flow request. This may not be problematic providing that the new path is established maintaining the same QoS characteristics. In fact, the new metrics will reflect the load variation and AC will act accordingly.

IV. Conclusions

The proposed AC model, based on on-line QoS and SLS monitoring, is simple, easy to deploy and provides the required flexibility to accommodate distinct network services both intra-domain and end-to-end. The AC strategy only involves the edge nodes in a domain and avoids complex AC signaling. The intra-domain operation controls both the QoS levels of the services in the domain and the utilization of the contracted SLSs with downstream domains using an AC module at ingress nodes and a monitoring module at egress nodes. The end-to-end operation uses the flow request for both AC at domain entrance and end-to-end available service check, avoiding extra control mechanisms. As monitoring is a systematic per-class process, both intrusion and AC latency are reduced. The amount of state information required for AC decisions is kept on an ingress-egress service basis. Per-flow state information is only kept at source domain for flow TC. Model deployment issues regarding the definition of services, on-line monitoring, AC decision criteria and per class traffic characterization have been identified and discussed. Currently, the model is being tested for a limited number of services and critical efficiency aspects are being studied in a simulation testbed.

References

[1] B. Teitelbaum, S. Hares, L. Dunn, R. N. V. Narayan, and F. Reichmeyer, "Internet2 QBone: building a testbed for differentiated services", *IEEE Network*, vol. 13, no. 5, p. 8...16, September/October 1999.

[2] Z.-L. Zhang, Z. Duan, L. Gao, and Y. Hou, "Decoupling QoS Control from Core Routers: A Novel Bandwidth Broker Architecture for Scalable Support of Guaranteed Services", in *SIGCOMM'00*, 2000.

[3] I. Stoica and H. Zhang, "Providing Guaranteed Services Without Per Flow Management", in *ACM SIGCOMM'99*, Oct. 1999.

[4] L. Breslau *et al.*, "Endpoint Admission Control: Architectural Issues and Performance", in *ACM SIGCOMM'00*, 2000.

[5] C. Cetinkaya, V. Kanodia, and E. Knightly, "Scalable Services via Egress Admission Control", *IEEE Transactions on Multimedia*, vol. 3, no. 1, p. 69...81, Mar. 2001.

[6] V. Elek, G. Karlsson, and R. Ronngren, "Admission Control Based on End-to-End Measurements", in *IEEE INFOCOM'00*, 2000.

[7] R. Mortier *et al.*, "Implicit Admission Control", *IEEE Journal on Selected Areas in Comm.*, vol. 18, no. 12, p. 2629...2639, Dec. 2000.

[8] S. Lima, "A Comparative Analysis of Admission Control Strategies", *Technical Report TR0102l*, Mar. 2002.

[9] D. Goderis *et al.*, "Service Level Specification Semantics and Parameters", *IETF draft: draft-tequila-sls-02.txt*, Feb. 2002.

[10] A. Sevasti and M. Campanella, "Service Level Agreements Specification for IP Premium Service", *Geant and Sequin Projects*, Oct. 2001.

[11] S. Leinen and V. Reijs, "D9.7 - Testing of Traffic Measurement Tools", *Geant Project*, Sept. 2002.

[12] T. Chahed, "IP QOS Parameters", *TF-NGN*, Nov. 2000.

[13] A. Liakopoulos, "D2.1 - Monitoring and Verifying Premium IP SLAs", *Sequin Project*, Apr. 2002.

[14] P. Bhoj, S. Singhal, and S. Chutani, "SLA Management in Federated Environments", *Computer Networks*, vol. 35, no. 1, Jan. 2001.

[15] V. Paxson, G. Almes, J. Mahadavi, and M. Mathis, "Framework for IP Performance Metrics", *IETF RFC2330*, 1998.

[16] "CAIDA Tools", 2002, http://www.caida.org/tools/index.xml.

[17] F. Georgatos *et al.*, "Providing Active Measurements as a Regular Service for ISPs", *PAM 2001*, Apr. 2001.

[18] A. Bak, W.Burakowski, F. Ricciato, S. Salsano, and H. Tarasiuk, "Traffic Handling in AQUILA QoS IP Networks", in *QoFIS'01*, Sept. 2001.

[19] C. Dovrolis and M. Jain, "End-to-End Available Bandwidth: Measurement methodology, Dynamics, and Relation with TCP Throughput", in *ACM SIGCOMM'02*, Aug. 2002.

[20] S. Lima, P. Carvalho, A. Santos, and V. Freitas, "Long Range Dependence of Internet Traffic Aggregates", *Networking 2002*, May 2002.