Available online at www.sciencedirect.com
SCIENCE DIRECT
Computer Communications 29 (2006) 1687–1695
computer communications
www.elsevier.com/locate/comcom

Service-driven inter-domain QoS monitoring system for large-scale IP and DVB networks ☆

A. Mehaoua[a,*], T. Ahmed[b], H. Asgari[c], M. Sidibe[a], A. Nafaa[a], G. Kormentzas[d], T. Kourtis[d], C. Skianis[d]

[a] CNRS-PRiSM Laboratory 45, University of Versailles, Avenue des Etats Unis, 78035 Versailles, France
[b] CNRS-LaBRI Laboratory, University of Bordeaux, 351 Cours de la Libération, 3405 Talence, France
[c] Thales Research and Technology (TRT), Worton Grange, Reading RG2 0SB, UK
[d] National Center for Scientific Research 'Demokritos', Institute of Informatics & Telecommunications, 15310 Aghia Paraskevi Attikis, P.O. Box 60228, Athens, Greece

Available online 2 September 2005

Abstract

There is a growing synergy between well-established Service Providers (SP), Content Providers (CP), and Network Providers (NP), to propose new value-added services, and hence opening new markets to generate further revenues. Meanwhile, the explosive increasing amount of multimedia content to be offered in the Internet and the heterogeneity of the underlying networking technologies demand the provision of new QoS-enabled mechanisms and architecture to efficiently control, manage and monitor the networks. Quality of service monitoring is becoming crucial to SPs for providing quantified QoS-based services and service assurance and to NPs for managing network resources. This paper proposes a framework for large scale inter-domain QoS monitoring in heterogeneous networks including IP and DVB networks that has been developed in the IST-ENTHRONE project of European Commission. One of the main aims is actually to allow high cooperation between different providers while keeping intact the authority, confidentiality, and full control of each provider over its underlying resources. The proposed monitoring framework consists of a layered architecture with two signaling protocols namely an inter-domain monitoring signaling protocol (EQoS-RM), and an intra-domain active measurement signaling protocol (Emon). The proposed QoS monitoring system is service-driven in the sense that it aimed at providing in service verification of QoS performance guarantees for the services offered to the users by the providers. To achieve this, it uses both QoS probes that perform both active and passive monitoring at different levels of abstraction employing node and network wide measurements and application-level perceived quality meters for detecting quality degradation. As such, this framework specifies three types of QoS monitoring components operating at different levels: at network element or node, at network and at service levels. This proposed system also provides monitoring information to NPs in order to assist in managing the operational status of their networks. Design and implementation of the proposed QoS monitoring system is described in this paper. Some experimental assessments of this service-driven QoS monitoring system prove its functioning in terms of accuracy and responsiveness in providing the necessary results.

Keywords: IP; DVB; QoS; SLA/SLS; Active measurements; Inter-domain monitoring

1. Introduction

This article describes an integrated large-scale inter-domain QoS monitoring system designed for use in multi-domain heterogeneous networking environment including IP and non-IP (DVB) networks for the purpose of supporting cross-network audiovisual service offering. The proposed QoS monitoring system has been developed in the IST ENTHRONE project for providing the means for service assurance and resource management. The QoS monitoring system is aimed at (1) *Assisting Service Providers* to verify whether the QoS performance

☆ This work is supported by the Sixth EU Framework Program for Research and Development 2003-2007, IST-ENTHRONE Integrated Project (http://www.enthrone.org), contract no. 507637.
* Corresponding author
E-mail addresses: mea@prism.uvsq.fr (A. Mehaoua), tad@labri.fr (T. Ahmed), hamid.asgari@thalesgroup.com (H. Asgari), mas@prism.uvsq.fr (M. Sidibe), anaf@prism.uvsq.fr (A. Nafaa), gkorm@iit.demokritos.gr (G. Kormentzas), kourtis@iit.demokritos.gr (T. Kourtis), skianis@iit.demokritos.gr (C. Skianis).

0140-3664/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2005.07.028

guarantees committed in Service Level Agreement (SLA) are in fact being met; (2) *Assisting network providers* in making provisioning decisions for optimizing the usage of network resources (both at intra- and inter-domain levels) according to short- and medium-term changes as well as providing measurement information for long-term planning in order to optimize network usage and avoid undesirable conditions.

We assume the performance requirements of a customer's requested service are described in the agreed SLA and consequently its Service Level Specification (SLS) part. These SLA/SLSs are the basic elements in the operation of our proposed QoS-based monitoring system. SLAs formalize service level negotiations conducted between customer (or Content Consumer) and provider for specific Qos-based service. The SLS is a subset of a SLA that denotes the technical characteristics of a service offered. These service technical characteristics refer to the provisioning aspects of the service, e.g. request, activation and delivery aspects from network perspectives. In this article, two types of SLS (and consequently of SLAs) are distinguished, customer-to-provider SLSs (cSLSs), and provider-to-provider SLSs (pSLSs) [1]. In ENTHRONE, The cSLA/cSLS is established between end-customers and service providers. The pSLS is established between the service and network providers or between network providers. The pSLS is agreed between providers for exchanging traffic in the Internet, with the purpose of expanding the geographical span of their offered services. pSLSs are meant to support aggregated traffic (i.e. serving many customers), and it is assumed that they are already in place prior to any cSLS agreements with end customers. cSLSs can differ depending on the type of services offered because different cSLS types have different QoS requirements.

The goal of inter-domain monitoring is not only to measure QoS metrics across domains, but also provide information in order to guarantee the contracted end-to-end services by means of tuning and controlling network resources. The problem of end-to-end QoS monitoring is not simply reduced to the concatenation of single domain QoS measurements but some multi-dimensional aspects must also be taken into consideration. One important aspect is the co-operation of providers in the service delivery chain. Here, it is assumed for monitoring at inter-domain scale, it is essential for providers to co-operate based on an agreed framework formulating the configuration of monitoring elements and service, the execution of measurements, the composition of results in an appropriate way, and the exchange of measurement data between providers. Building on the above requirements, the functions required for QoS monitoring over heterogeneous networks include: (1) QoS-based service monitoring at both QoS performance and perceived quality levels, (2) QoS-based resource monitoring for performance monitoring at traffic class, node, path, and network levels, (3) a set of protocols for exchanging the monitoring results.

There are a number of working groups in the Internet Engineering Task Force (IETF) related to measurements and monitoring such as Remote MONitoring (RMON), IP Performance Metrics (IPPM), Real-Time Flow Measurement (RTFM], IP Flow Information Export (IPFIX), and Packet Sampling (PSAMP). These working groups are defining metrics, developing a common IP traffic flow measurement technology, and specifying a standard set of capabilities for sampling packets through statistical and other methods, respectively. There exist numerous monitoring tools, such as the RIPE Test Traffic Measurement (TTM), NetFlow, SFlow, NIMI (National Internet Measurement Infrastructure) [2], Network Analysis Infrastructure (NAI), cflowd, RTG high-performance SNMP statistics monitoring system, Sskitter, NeTraMet, CoralReef, and Beluga of CAIDA (Cooperative Association for Internet Data Analysis), and so on.

There has also been some work at the intra-domain level to use measurement information for tackling network performance degradation and managing congestion in operational networks as well as addressing service level monitoring among them are NetSCOPE, RONDO, KeyNOTE, ProactiveNET and others. In references [3,4], all of these activities are provided. These measurement tools and systems collect, analyze and visualize forms of Internet or Intranet traffic data such as network topology, traffic load, performance, and routing. An intra-domain QoS monitoring system was developed in TEQUILA project for IP-based networks featuring IP connectivity users and network providers in its business model.

There has also been some work on monitoring and measurements at inter-domain level, by European research projects [5]. To mention some, the objective of the IST-INTERMON project has been to develop an integrated inter-domain QoS monitoring, analysis and modeling system to be used in multi-domain Internet infrastructure for the purpose of planning, operational control and optimization [6]. The proposed solution assumes that a centralized manager negotiates monitoring operation with every domain along the service delivery path. This results in a scalability problem for the INTERMON system as the inter-domain network expands. The focus of the IST-MoMe project has been the enhancement of inter-domain real-time QoS architectures with integrated monitoring and measurement capabilities. The objective of the IST-SCAMPI project was to develop an open and extensible network monitoring architecture for the Internet including a passive monitoring adapter at 10 Gbps speeds, and other measurement tools to be used for denial-of-service detection, SLS auditing, quality-of-service, traffic engineering, traffic analysis, billing and accounting [7]. IST-LOBSTER is its follow on project aimed at deploying an advanced pilot European Internet Traffic Monitoring Infrastructure based on passive monitoring sensors at speeds starting from 2.5 Gbps and possibly up to 10 Gbps [8]. Finally, IST-AQUILA project is developing inter-domain QoS-metrics measurement

mechanisms, based on the BGRP proposal, to enable measurement based admission control (MBAC) in large-scale IP environment [9].

Our work differs from the previous IST projects in that (1) its end to end scope and business model encompasses content providers, service providers, network providers and customers; (2) end-to-end service monitoring is tackled using an overlay network of service-level monitoring components communicating in a cascaded fashion; (3) network-specific measurements are collected and translated to network-independent format using XML-based MPEG-21 data models; (4) application-level perceived quality meters (PQoS) are coupled with network-level quality probes (NQoS). The overall aim is at providing the means to monitor the services, networks, and resources at both intra- and inter-domain levels. Additionally, to develop and utilize Quality Meters to measure the perceived quality level of an audio–visual stream as part of service level monitoring.

The reminder of this paper is organized as follows. Section 2 describes the overall inter-domain QoS monitoring system architecture, components, signaling protocols and operations. Section 3 presents some experimental results evaluating the performance of the system. Finally, conclusion is provided in Section 4.

2. Large-scale inter-domain QoS monitoring system architecture

Fig. 1 shows the overall QoS monitoring system architecture and the testbed configuration. Its components and the associated signalling protocols are depicted. For efficiency and scalability reasons, the monitoring management architecture is structured in three levels: service-, network- and node-monitoring plans.

In ENTHRONE, an Integrated Management System (IMS) has a number of functional facilities/components for each entity such as SP, CP, CC and NP for managing the end-to-end service delivery. The IMS Dispatcher component and especially its Service Manager located at the SP deals with the customer subscriptions (cSLAs), contracts with NPs through pSLSs, the services owned by SP and the access to the service, which has been chosen. We assume that detecting service quality degradation for an actively running audiovisual service is carried out by means of Perceived Quality (PQoS) measurements at end-user side. A PQoS meter can be part of the Service Provider's (SP) Management System which is located at Content Consumer's Terminal. Any cSLS violation is reported to the Service Manager sub-system. Upon its jurisdiction depending on the persistent violation of cSLS, the Service Manager

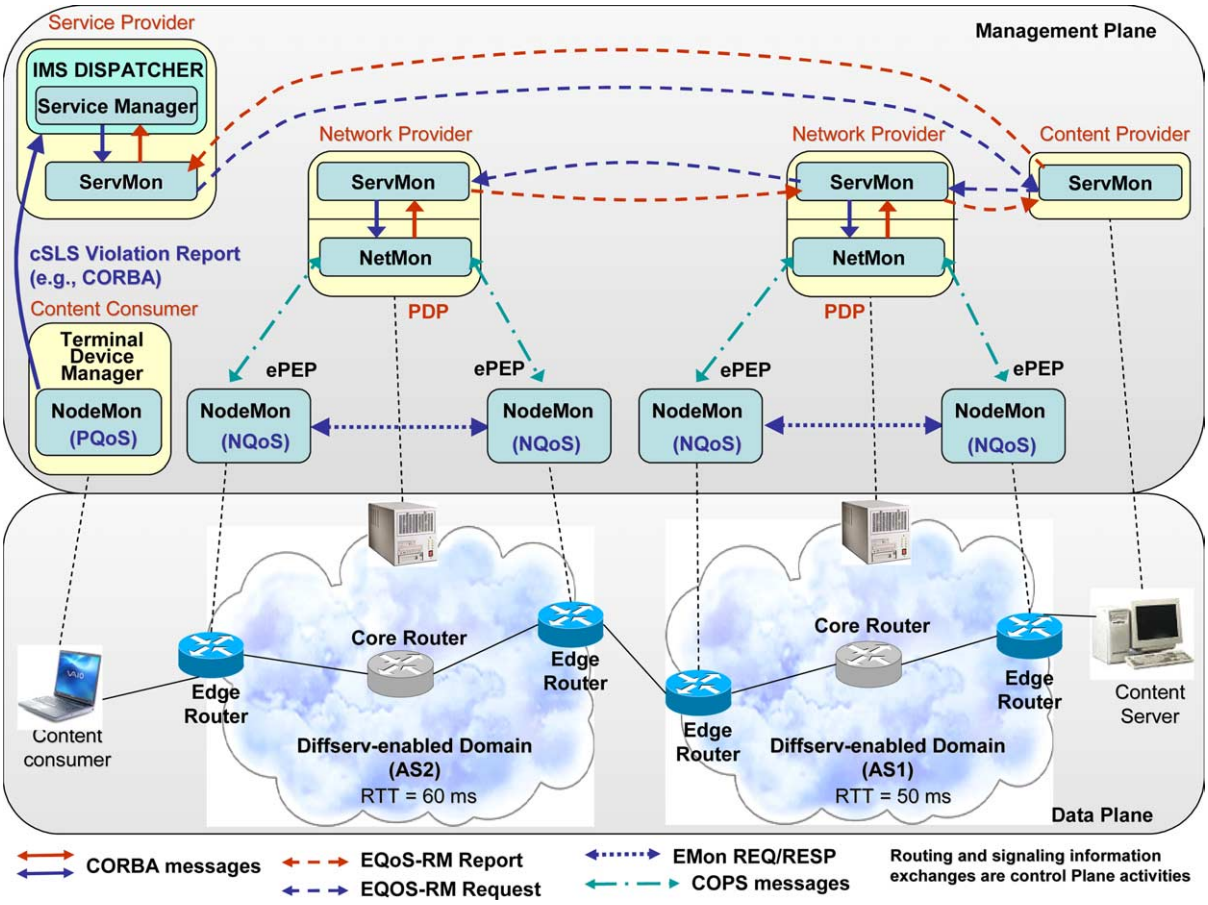

Fig. 1. Overall inter-domain QoS monitoring architecture and the testbed configuration.

decides to initiate high-level actions. The service Manger is in responsible for identifying the cause of QoS degradation and the responsible entity (which could be the terminal, the network or the content server). It notifies the terminal that the QoS degradation has been identified and corrective measures are being undertaken. Consequently, an end-to-end procedure and a top-down procedure (from service level to node level) are invoked to determine the entity that is responsible for this degradation. Hence, appropriate corrective actions could be taken by the IMS Dispatcher such as content/traffic adaptation, transcoding/transrating, pSLS re-negotiations, path switching, re-routing, Terminal Device reconfiguration, CP/NP notification, etc. In the following sections, we describe in detail the QoS monitoring system components and the related monitoring procedures.

2.1. QoS monitoring system components

Four distinct monitoring components and two signaling protocols are defined in order to fulfill the requirements while adding a number of design features for ensuring a scalable solution. The solution includes the features for minimizing the amount of monitoring information exchange, processing the raw data and providing aggregated results at the source by dispersing the data collection systems at node level, performing QoS monitoring processes at the aggregated levels, and controlling the synthetic traffic insertion. These components are called the *Integrated Management Supervisor Dispatcher*, *Node*, *Network*, and *Service Level Monitors. EQoS-RM* and *EMon* are the signaling protocols for monitoring exchanges at inter- and intra-domain levels, respectively.

Node level monitors (NodeMon) are deployed only at network domain edges. They perform active traffic measurements between any two edge nodes of an AS and collect passive measurement information. We distinguish between network-level QoS measurement (NQoS) from application-level measurement (PQoS). In DVB networks and at node level, standalone measurement tools such as passive 'Protocol Analyzers' are used to measure related parameters of DVB applications. In addition, PQoS probes are used to examine application level perceived quality of audio–visual Digital Items. PQoS monitors are regarded as Node Level Monitors since they are managed by other network monitoring agents. In Enthrone, a set of PQoS probes capable of measuring PQoS parameters (especially audio and video quality of streaming video encoded in MPEG-4) and protocol analysers for measuring protocol related parameters of DVB applications (at MPEG Transport Stream level) are developed. These PQoS monitors perform per-flow measurements, providing effective application-level QoS metrics and viewer-perceived quality. This helps to (1) detect cSLS violations (i.e. QoS degradations) to launch specific QoS failure location discovery (e.g. figure out the responsible domain/s); and (2) drive appropriate adaptation actions such as multimedia content adaptation, new round of SLS re-negotiations, new load balancing initiatives, network domain bypassing, etc.

Network level monitor (NetMon), is responsible for intra-domain monitoring that utilizes network-wide performance and traffic measurements collected by all underlying Node Level Monitors in order to build a physical and logical network view (i.e. the view of the established QoS routes across the network). At NetMon level, the measurement information is further processed and aggregated so that only relevant QoS metrics are reported back to the monitoring component at the service level (i.e. ServMon). Each NP coordinates NodeMon operations in its domain by means of intra-domain control signaling protocol (SNMP, COPS, CLI, etc.), whatever is appropriate.

Service Level Monitor (ServMon) is to perform customer/provider-related service level monitoring, auditing, reporting, and initiating some appropriate actions. Each NP has a Service Level Monitor for inter-domain QoS reporting using XML-based measurement statistics. We have also given a specific role to the Service Level Monitor at the Service Provider that owns and offers value-added services. The ServMon at SP is in charge of coordinating the service level monitoring procedures and to proceed with the information provided by others ServMon entities of the networks involved in the end-to-end chain of QoS delivery. The advantage of the separation between the ServMon and the NetMon is to abstract the service level functions from network specific functions. Particularly, ServMon deals with the service classes such as Gold, Silver, Bronze services, while NetMon deals with the QoS related parameters at the network level.

Service manager at IMS Dispatcher, is the entity that receives 'QoS degradation Alert' from PQoS agents which are assumed to be located in terminals or at the boundaries of NP's domain. Consequently, on-demand QoS/resource monitoring is activated by end-user perceived quality degradation. Upon the persistency of cSLS violations, Service Manager then initiates a *QoS degradation location discovery* process by requesting the Service Level Monitor to report on the service performance. It should be noted that IMS Dispatcher is located at the SP premise, and in general has the roles of coordination between QoS monitoring, QoS adaptation, content generation, and service management at both end-user and provider levels. This obviously implies predefined policies and rules to convey the corresponding service and monitoring parameters.

Inter-domain end-to-end QOS monitoring signaling protocol (EQoS-RM). This protocol carries service-level resource monitoring messages between *ServMon* located at each domain and *NetMon* components. This protocol uses a set of MPEG-21/XML compliant signaling messages based on simple request/response mode. It is compliant with the two-layering architecture model proposed by IETF Next Steps in Signalling (NSIS) framework [10]. As depicted in

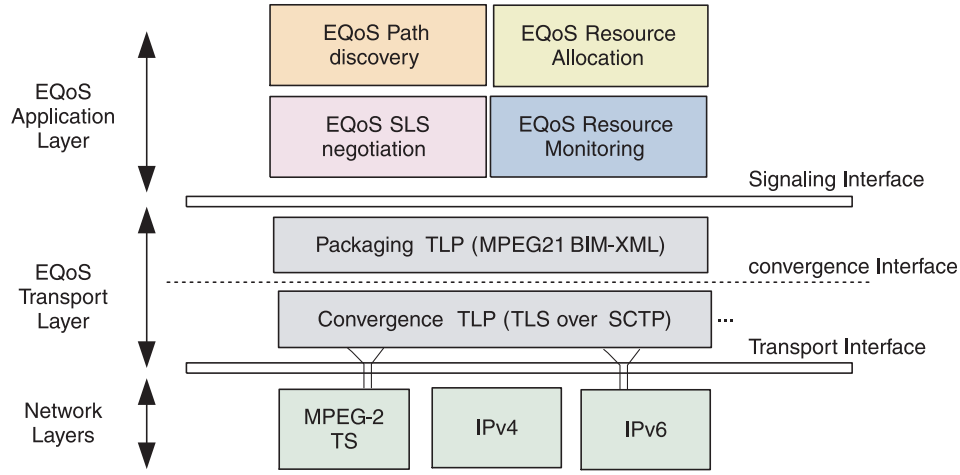

Fig. 2. EQOS-RM protocol layered architecture.

Fig. 2, EQOS is composed of an (1) EQOS Transport Layer Protocol (EQOS TLP) which is independent of any particular signaling application, provides an abstraction at the transport level since only generic send/receive functions are visible to the upper layers; and an (2) EQOS Application Layer Protocol (EQOS ALP) which contains signaling-specific application functionalities including SLS commitments, resource reservation, inter-domain QoS routing, and services monitoring as well. For bandwidth-saving, interoperability, reliability and security purposes, a packaging sub-layer and a convergence sub-layer are defined at EQOS-TLP layer to compile EQOS-RM messages to Binary XML (BIM) format using MPEG-21 Digital Item Description Language and EXPWAY BinXML 3.0 toolkit [11]. Exchanging securely these messages is possible by means of IETF Transport Layer Security (TLS) over Stream Control Transport (SCTP) protocol [12].

The TLS Protocol [13] which is also used by EMON and COPS signaling protocols allows monitoring entities to authenticate each other before the setup of any monitoring activities with the negotiation of a cryptographic context for every requested 'SLS monitoring jobs'. Messages authenticate and integrity is then guaranteed. SCTP [14] is a reliable transport protocol operating on top of a connectionless packet network such as IP. The design of SCTP includes appropriate congestion avoidance behaviour and resistance to flooding and masquerade attacks.

Intra-domain active measurement signalling protocol (Emon). This EMon (Enthrone Monitoring) protocol has been defined to support secure and fast-responsive intra-domain communication between *NodeMon* peers. Emon protocol is based on Datagram TLS (DTLS) [15] and undertakes the configuration, synchronization, and management of active measurement sessions between edge-domain *NodeMon* agents. There are actually two EMon operating modes: *fully synchronized mode* and *asynchronous timer based mode*. More details about EMon protocol is given in [16].

2.2. QoS monitoring operations

2.2.1. Service monitoring set-up/configuration procedure

Before launching any service monitoring operations, a monitoring set-up phase requests for configuring all effective monitoring agents along the service path specified through pSLS agreements. Thus at each crossed NP domain, a vertical monitoring configuration from NP-ServMon to NodeMon takes place to basically register a new agreed pSLS. This monitoring set-up procedure is started by the ServMon (SP) after a successful pSLS negotiation. The setup procedure instantiates a NP-related 'Monitoring Job' at specific network edges for a specific traffic class (e.g. load monitoring for a pSLS), while the effective pSLS monitoring starts later-on at IMS Dispatcher/Service Manager initiative (continuous and on-demand monitoring).

2.2.2. Continuous service monitoring procedure

The continuous monitoring is performed on a per-domain basis and it is based on periodic active and/or passive measurements of pre-established p-SLS. Using the specified measurement frequency, the NodeMons regularly send back their measurements reports to the NetMon. The NetMon aggregates the different received measurement reports and evaluate the degree of conformance of the pSLS crossing its domain. These p-SLS status information are then made available to the NP-ServMon for being exchanged with the IMS-dispatcher during the 'on-demand' monitoring procedure.

2.2.3. On-demand service monitoring procedure

This on-demand monitoring operation is triggered by the IMS Dispatcher that aims at locating the domain(s) that is/are the source(s) of end-to-end QoS degradation. For quick responses, this operation is organized to take a time in the order of magnitude of the RTT—Round Trip Time. The procedure uses EQoS-RM messages, which are exchanged

between every ServMon's along the service delivery path in a cascaded fashion used as the QoS peering model between providers. This procedure ultimately aims to verify each pSLS conformance status along the path by collecting the associated pSLS status information per domain a.

3. Performance evaluation

3.1. The testbed configuration

In order to evaluate the proposed monitoring system, we set up a test-bed depicted in Fig. 1, comprising of two distinct network domains. The test-bed is deployed to validate the end-to-end monitoring and to evaluate its response time and accuracy in providing the results responsiveness. We particularly emphasize the ability of our monitoring system to capture the instantaneous network dynamics, which assists (1) NPs to reconfiguring their resources for prospective pSLS commitments; (2) NPs to redistribute the available resources proportional to the required QoS differentiation level based on policies; (3) SPs to verify the continual operation of their offered services and initiate remedial actions in case of service disturbance; and (4) CPs and End-Users in content adaptation as anticipated in the MPEG-21 framework to adjust to the imposed network constraints (e.g. access network limitation).

Two autonomous domains, AS1 and AS2, are considered representing two NPs configured to have an egde-to-edge domain RTT of 50 and 60 ms, respectively. We also included two PC platforms to represent, respectively, Content Provider (Content Server) and Content Consumer (end user). Note that both of them may be (in practice) located in different arbitrary networks.

Each domain (NP) is composed of three routers: two edge routers which also host the NodeMons and one Linux-based core router. The core router is running 'NIST Net'[1] software to emulate the NP network-wide (WAN) behavior. We configured NIST Net to introduce constant transit delay of 25 and 30 ms in AS1 and AS2, respectively, with an additional standard delay deviation of a 1 ms.

Each NP implements its own DiffServ (Differentiated Services) policy based network management with its proper DSCP-based traffic class identification. Both edge and core routers have DiffServ capabilities for traffic classification, traffic conditioning and various scheduling disciplines. Traffic classification and traffic conditioning (including packet remarking) occurs at NP boundaries to comply with the inter-domain QoS mapping and binding occurred at the service management level and during pSLS negotiation. Inter-domain DSCP (DiffServ Code Point) values are agreed between adjacent ASs during the pSLS negotiation. A dedicated DSCP value signals a given service class on the inter-domain links. Therefore, each domain is aware of the mapping between agreed inter-domain DSCP values at the inter-domain level and the local DSCP value at the domain level. At the ingress interface of each domain the mapping between the inter-domain DSCP and local DSCP is performed by packet remarking. Similarly at the egress point of the domain, the local DSCP value is replaced with the outgoing DSCP value of the corresponding service class. This mapping allows end-to-end QoS continuity across multiple domains.

It should be noted that DiffServ defines router forwarding behaviors known as Per Hop Behaviors (PHB). A PHB includes the differential treatment individual packets receive, implemented by queue management disciplines. DiffServ specified the following PHBs: *Expedited Forwarding* (EF) for Premium services [21], *Assured Forwarding* (AF) for Olympic services [22], and *Best-Effort* (BE) as the 'default' PHB. For the purposes of our experiments we use these traffic classes, termed as EF, AF, and BE for differential treatment by the appropriate PHBs implemented by queuing and scheduling disciplines.

In Network Provider domain, both ServMon and NetMon are located on the same host, although they may be separated in practice. Several QoS metrics are measured in active or passive mode depending on their importance and impact in the overall QoS delivery and degradation. Thus, QoS metrics that have a short-term impact on QoS are rather actively tracked, while QoS metrics with long-term reverberation are monitored passively in preventive manner. The QoS metrics of interest that are measured in cross-domain are as follows: one-way transmission delay [17], one-way packet loss [19], and delay variation (jitter) [18].

In order to have an accurate stable reference clock source, the different NodeMon are synchronized using the NTP protocol. An NTP server located at the University of Versailles delivers a synchronization precision with a margin of millisecond.

In order to *actively* measure a broad range of QoS metrics, we have designed and implemented a NodeMon agent for conducting active measurements in IP domains. It is called Active Monitoring Agent (AMA) and its main responsibility is to continuously measure the packet's inter-arrival time (jitter)[2], observed packet loss rate, and cross-domain transit delay for the available Per Domain Behaviors (PDB). Since TLS requires a reliable transport channel typically TCP, we adopted with EMon a modified version of TLS, named 'Datagram TLS' and proposed by Modadugu and Rescorla [20]. Since DTLS is very similar to TLS, preexisting TLS protocol implementations in EQOS can be reused.

[1] NIST Net is a network emulation package that runs on Linux. For more information visit: http://www-x.antd.nist.gov/nistnet/

[2] In this article, packet inter-arrival time, delay variation, and jitter are used interchangably.

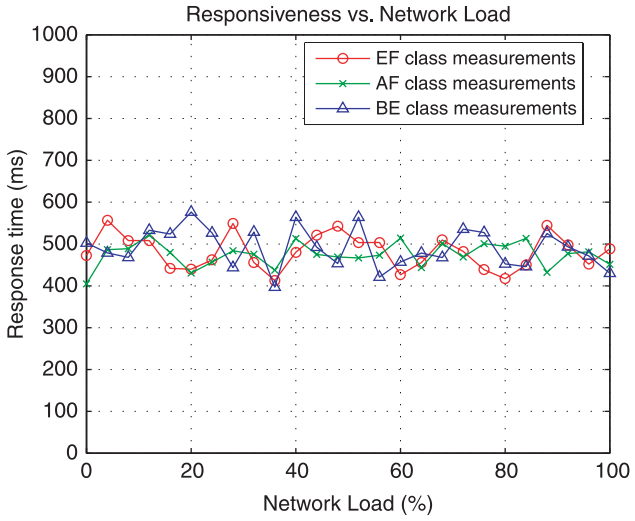

Fig. 3. Monitoring system response time for different level of network load.

3.2. Monitoring system response time analysis

Fig. 3 shows the response time of the monitoring system when the network load is gradually increased in steps by 4% of the total capacity of links between two edge routers. Here, the response time stands for the time elapsed between the monitoring order issuance at IMS Dispatcher and the time when the monitoring results are received. The response time does not account for the time of effective active measurement, and consider only the protocols' interactions involved in ordering and retrieving a monitoring task.

We instantiated three distinct *Monitoring-Jobs* that simultaneously operate to collect active measurements between Edge1 and Edge2. Each Monitoring Job is configured to measure the response time of a single traffic class (EF, AF, or BE). The active measurement interval is fixed at 15 s. During the experimentation, each time we increase the network load by alternatively adding a new flow belonging to one of the traffic classes till fully fulfill the available bandwidth. The EF traffic class, however, is not saturated and is dimensioned to conform to the Expedited Forwarding specification, i.e. the transit delays are kept to minimum by avoiding the en-queuing at network nodes. In this way, only the synthetic injected traffic is affected by the network conditions.

It should be noted that we assumed that the EF traffic has a fixed bandwidth share that allow the traffic to be serviced even during the congestion periods that may affect AF and BE traffic. Note that the signalling traffic (EQoS, COPS and EMon) is marked as EF traffic and treated by the network preferentially. As a consequence, the signalling information is not affected by network conditions (i.e. load, traffic models,…).

In Fig. 3, it is clearly revealed that the measured values of the response time for each service class are rather stable over the time. The oscillations are due to the fact of TCP/SCTP natural behavior as explained above. Since all signaling traffic (EQoS-RM, COPS, EMon, and SNMP) was marked as EF traffic, fairly good response time was maintained. Hence, the network load dynamics affect only the user traffic nor signaling/management traffic.

Since signaling messages are marked as EF traffic and all traffic classes are measured through the same protocols' interactions process, the monitoring system response time oscillates around 500 ms for all services classes. Therefore, based on the scale of the network, one (SP or NP) may set an appropriate confidence interval so as to ignore the minor oscillations that may arise when traffic classes are monitored, to approximate the monitoring response time.

3.3. Monitoring system accuracy analysis

In order to characterize our monitoring system accuracy, we explicitly introduce in the network specific delay, jitter, and loss rate for each service class, and then measured the QoS metrics related to these service classes. Table 1 gives the values of QoS parameters configured in NIST Net network emulator for each class of service.

Three monitoring jobs were created to measure the respective QoS metric related to each traffic class (EF, AF, BE). The measurement interval was set to 2 s. The measurements were repeated 25 times to get more information about the *long-term* accuracy of our monitoring system and its ability to continuously perform measurements and produce measurement results.

Given the potential NTP clock lag (1 ms), the QoS metrics measured by our monitoring system were very close to the ones introduced as shown in Figs. 4 and 5. Especially, both delay and jitter accuracy falls below 1 ms most of the time.

As shown in Fig. 4, the delay measurements are quite accurate for the three traffic classes. An important observation is that the oscillation (see measurement 7–12 and measurement 17–19) in the delay measurements coincides for the three traffic classes. During these measurements, the three monitoring jobs were affected by

Table 1
One-way delay, delay variation, and loss ratio values configured for each class of service

	One-way-delay (ms)	One-way-delay - variation (ms)	One-way-loss-rate (%)	Flow identification (DSCP)
EF services	30	5	0	0xB8
AF services	35	10	15	0x28
BE services	40	15	30	0x00

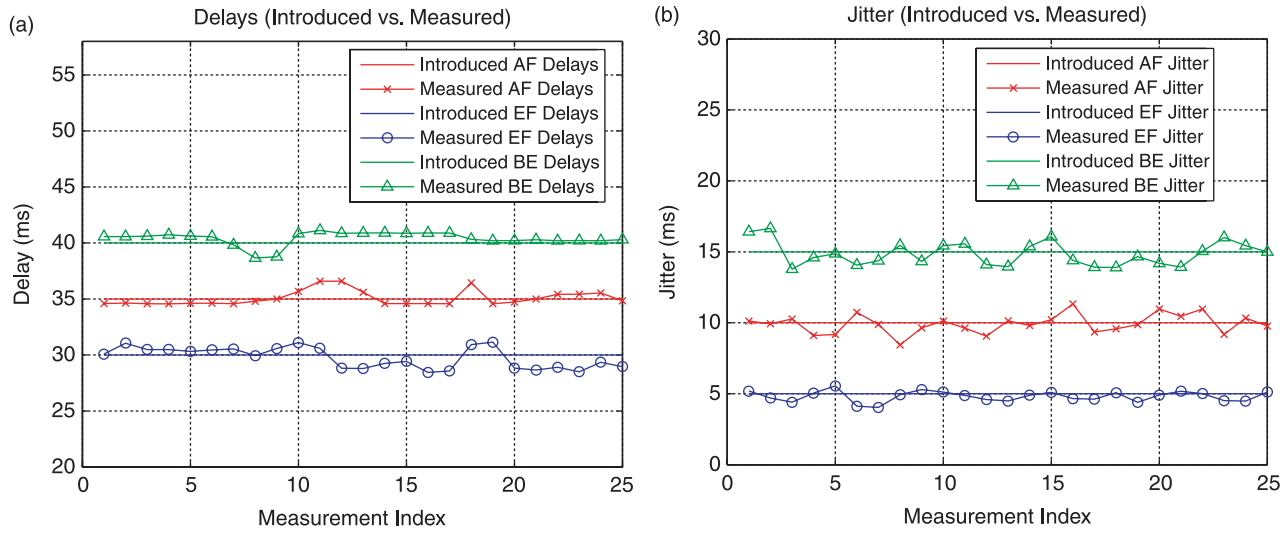

Fig. 4. One-way delay and Jitter measurements for EF, AF and BE traffic classes.

the same accuracy gap. This is, in part, caused by the synchronization lag between the peer NodeMons associated to the three monitoring jobs. Additionally, NIST Net was configured to introduce the, delay, jitter, and loss values averaged over longer terms. Therefore, when short-term measurements (2 s in our case) are conducted, some different measurements values are expected.. In addition, the measured jitter exhibit high oscillations (up to 10 ms) as a consequence of the short-term delay variation.

Fig. 5 shows the packet loss measurements. It is observed that the loss measures displayed over the time more fluctuation around the introduced mean loss rate for AF and BE traffic. This is due to the loss burstiness exhibited by NIST Net that uses well-known Gilbert (good/bad) model to generate the packet loss pattern.

The above results show that traffic classes and consequently pSLSs can be accurately and individually monitored in both 'On-Demand' and 'Continuous' modes, independently to the measurement interval. However, the measurement interval should be carefully set to reduce traffic control overhead and provide good system responsiveness.

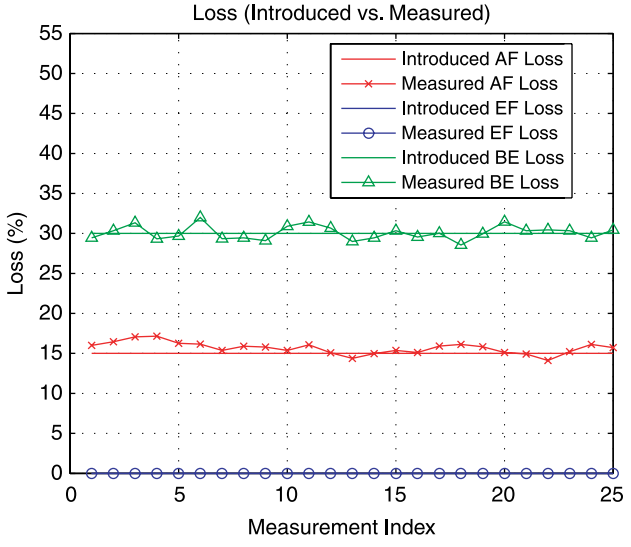

Fig. 5. Packet loss ratio measured for EF, AF and BE traffic classes.

4. Conclusion

This paper describes a service-driven QoS monitoring system for large-scale heterogeneous network technologies involving both IP and non-IP (e.g. DVB) network domains. The proposed QoS monitoring system is service-driven in the sense that it aimed at providing in service verification of QoS performance guarantees for the services offered to the users by the service providers. The monitoring system provides the means for remedial actions to be taken in case of service degradation or failure, e.g. on non-conformance to SLSs. The monitoring system also assists network providers in making provisioning decisions for optimizing the usage of network resources. It is shown that the proposed QoS monitoring framework consists of a layered monitoring architecture associated with two signaling protocols; an inter-domain monitoring signaling protocol named EQoS-RM, and an intra-domain active measurement signaling protocol named EMon. The proposed monitoring system is distributed in order to guarantee quick response times and to minimize management traffic. This ensures small reaction times and helps maintain stability as the network size increases. Based on the assessment results, we showed that the proposed monitoring system provides good accuracy for both one-way delay, jitter, and packet loss. We also demonstrated the ability of the monitoring system in providing measurements in relatively short timescales at traffic class granularities in order to assist various management and control functions. In summary, we believe that

the proposed QoS monitoring system can assist service providers to support large number of customers and contribute towards operationally optimized and engineered networks.

References

[1] P.Flegkas, ed., Mescal Delivrable D1.1: 'Specification of Business Models and a Functional Architecture for Inter-domain QoS Delivery', http://www.mescal.org/ Public Deliverables.

[2] V. Paxson, J. Mahdavi, A. Adams,, M. Mathis, An architecture for large-scale internet measurement, IEEE Communications Magazine 36 (8) (1998) 48–54.

[3] A. Asgari, P. Trimintzios, G. Pavlou, R. Egan,, Scalable monitoring support for resource management and service assurance, IEEE Network Magazine 18 (2004) 6–18.

[4] KeyNOTE monitoring solutions are available at www.keynote.com. ProactiveNET monitoring solutions are available at www.proactive-net.com. RTG high-performance SNMP statistics monitoring system is available at sourceforge.net/projects/rtg/.

[5] European IST (Information Society Technologies) research projects, for more information visit: www.cordis.lu/ist/. Specifically for IST-INTERMON visit: www.ist-intermon.org/, for IST-MoMe visit: www.ist-mome.org/, and for IST-SCAMPI visit: www.ist-scampi.org/.

[6] U. Hofmann, I. Miloucheva, T. Pfeiffenberger, INTERMON: complex QoS/SLA analysis in large scale internet environment WISICT 2004, Proceedings of the Winter International Symposium on Information and Communication Technologies, Cancun, Mexico, January 5–8th 2004.

[7] J. Coppens, E.P. Markatos, J. Novotny, M. Polychronakis, V. Smotlacha, S. Ubik, SCAMPI — a scaleable monitoring platform for the Internet, Proceedings of the Second International Workshop on Inter-Domain Performance and Simulation (IPS 2004), Budapest, Hungary, 22-23 March 2004.

[8] IST-LOBSTER Home Page, at http://www.ist-lobster.org/about/objectives.html.

[9] IST-AQUILA Home Page, at http://www-st.inf.tu-dresden.de/aquila/.

[10] Next Steps in Signaling, Working Group, IETF, http://www.ietf.org/html.charters/nsis-charter.html.

[11] Expway Inc., 'A BIN XML toolkit 3.0', available at: www.expway.com.

[12] A. Jungmaier, et al. 'Transport Layer Security over Stream Control Transmission Protocol', IETF, RFC 3436, December 2002.

[13] T. Dierks, et al. 'The Transport Layer Security Protocol', IETF, RFC 2246, January 1999.

[14] R. Stewart et al, 'Stream Control Transmission Protocol', IETF, RFC 2960, October 2000.

[15] E. Rescorla and N. Modadugu, 'Datagram Transport Layer Security', IETF, draft-rescorla-dtls-03.txt, February 2004.

[16] A. Kourtis, H. Asgari, A. Mehaoua, E. Borcoci, S. Eccles, E. Le Doeuff, P. Bretillon, J. Lauterjung, M. Stiemerling, ENTHRONE Deliverable D21, 'Overall Network Architecture', May 2004, available at http://www.enthrone.org.

[17] G. Almes, S. Kalidindi, M. Zekauskas 'A One-way Delay Metric for IPPM', IETF, RFC 2679, September 1999.

[18] C. Demichelis, P. Chimento 'IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)', Request for Comments, IETF, RFC 3393, November 2002.

[19] G. Almes, S. Kalidindi, M. Zekauskas 'A One-way Packet Loss Metric for IPPM', Request for Comments, IETF, RFC 2680, September 1999.

[20] N. Modadugu, E. Rescorla, The design and implementation of datagram TLS, Proceedings of ISOC NDSS 2004, February 2004.

[21] Jacobson, V., Nichols, K., Poduri K.'An Expedited Forwarding PHB', .IETF, RFC 2598, June 1999.

[22] J. Heinanen et al., 'Assured Forwarding PHB Group', IETF, RFC 2597, June 1999.