

## A PROACTIVE SERVICE LEVEL AGREEMENT MANAGEMENT (SLAM) ARCHITECTURE IN AN INTRANET NETWORK

Codruț MITROI<sup>1</sup>

*În cazul unei rețele Intranet, administratorul rețelei deține rolul furnizorului de servicii pentru utilizatorii din cadrul organizației, sens în care acesta realizează managementul SLA-urilor (SLAM), menținând un echilibru între cerințele tot mai accentuate de servicii ale beneficiarilor și costurile de operare ale rețelei.*

*Articolul prezintă, pornind de la conceptul general al SLAM, o arhitectură proactivă a SLAM în cadrul unei rețele Intranet în vederea maximizării calității experienței (QoE) utilizatorilor.*

*The Service Level Agreements Management (SLAM) represents all technical and procedural activities performed by a communication service provider in order to maintain the requirements derived from the SLAs. In case of an Intranet network, the administrator plays the role of a service provider for the different enterprise users and has to maintain a balance between the most pronounced customers requirements and the networks operational costs.*

*In this paper it is proposed, starting from the general concept of SLAM, an originally (in the author's opinion) proactive SLAM architecture concept which improves the user's quality of experience (QoE).*

**Keywords:** Service Level Agreement, Service Level Agreement Management, Quality of Experience, Key Quality Indicator, Key Performance Indicator

### 1. Introduction

The present informational society is based exclusively on the IT&C development, this domain being capable to assure a large spectrum of services, such as multimedia, data transfer, e-commerce, e-banking, e-learning and so on.

In order to align to this society's needs, any kind of organization, either a private company or a governmental authority must adapt or optimise their informational flows to allow an accurate and quick process, fulfilling very strong demands of availability, integrity, confidentiality and non-repudiation for the transmitted information.

---

<sup>1</sup> PhD student, Depart. of Automatics and Industrial Information, University POLITEHNICA of Bucharest, Romania, e-mail: mcodrut@deti.ro

For a geographically wide spread organization that uses an Intranet network, which depends not only on its own IT&C resources but also on private or public communication operators' resources, the quality of service assurance to the users, either internal employees or external customers, depends totally on the network administrator's/IT department's ability to assure the non-violation of the initial service level agreement. In order to do that, the network administrator/IT department must apply technical and procedural mechanisms in case of the internal IT&C resources and monitors permanently the agreements signed with external communication operators.

## 2. Informational stack model within an organization

Generally speaking, IT&C organization's needs undergo greater changes comparing to these of a communication operator, based on the new business opportunities demands, which are very strong, or on the customer needs.

Starting from the hierarchization presented in [1], it is developed an informational stack model inside an organization, which is represented in Fig. 1.

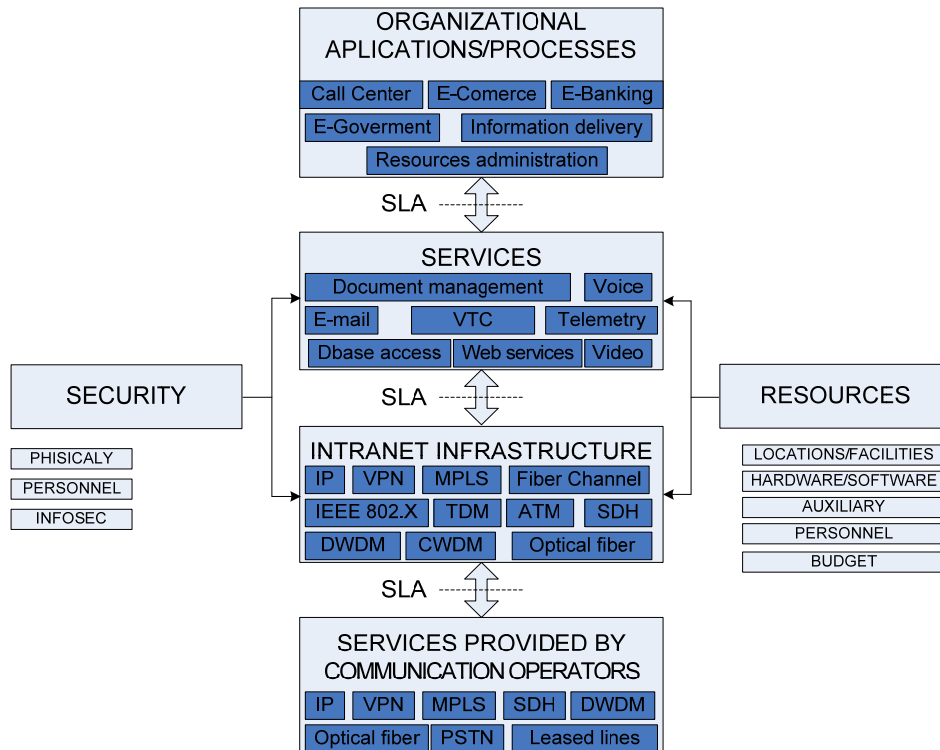


Fig. 1. Informational stack model within an organization

As we can see in the figure, in order to achieve the organization's strategic targets, we develop inside it different applications or processes which can vary depending on the organization, but there are also similar applications/processes for all of them, such as call-center, information delivery through data base access, enterprise resource planning and so on. To achieve these applications/processes it is necessary the activation of certain services, in some cases many services could be activated for a single application/process.

There are many interaction points among the elements represented in the model [2]. Those interaction points are grouped into a physical or logical interface, which can be located on a vertical plane (between elements which belong to different levels) or on a horizontal plane (on the same level) – Fig. 2.

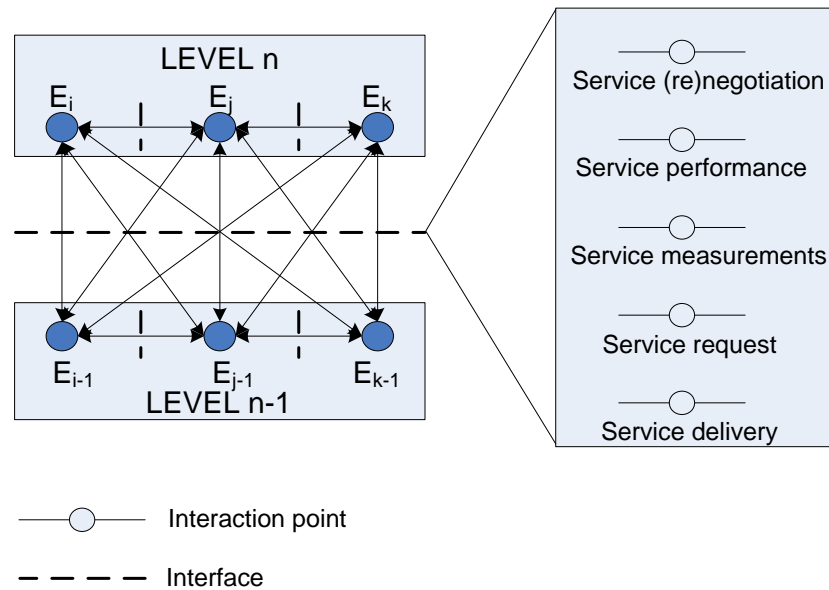


Fig. 2. The relationship between informational model elements, interfaces and interaction points

The interaction point through which a service is delivered between two elements is called *Service Access Point* – (SAP), within this there could be defined and implemented a service level agreement.

### 3. Performance indicators

In order to establish and implement SLA related to the different levels of the organization's informational system hierarchy, we need a mapping of the aims and needs derived from the strategic targets into measurable parameters corresponding to the hierarchy's lower level. One of the problems an administrator

must deal with is to define and to correlate the performance indicators with the quality indicators related to the Intranet infrastructure.

The performance indicator which globally describes the proper functioning mode between different components of the model presented in Fig. 1 is known as *Quality of Experience* (QoE) [3], and it is a concept which accommodates all the elements which characterised the final user perception about a service performance, related to his service expectations.

In the table below, it is illustrated some of the QoE elements for a VoIP phone service user from an organization and the expectation level regarding quality.

Table 1

QoE for a voice service	
QoE element	Expectation
Fiability	100 %
Availability	100%
Conectivity	Instantly
Voice signal quality	Similar to the PSTN telephony
Voice signal delay	Indistinguishable
Supplementary services	Totally available

In order to evaluate the quality level, we can use some computing methods, which could simulate various services, and depending on the organization specificity, these methods must be adapted.

The most known methods are:

- i) *Mean Opinion Score* (MOS) evaluation [4], which is applicable for voice calls. MOS values vary between 1 and 5 and have some subjectivity level;
- ii) The E – mathematical model [5], which represents an objective method for voice calls measuring conducting to a transmission evaluation factor computing – R. R values vary between 0 and 100, according to the equation (1):

$$R = R_0 - I_s - I_d - I_e + A \quad (1)$$

$R_0$  – signal to noise ratio value

$I_s$  – distortion effect which joins voice signal

$I_d$  – delay effect

$I_e$  – packet loss and jitter effects

A – compensation factor

- iii) Traffic queuing models based on binomial, Erlang, Engset or Poisson model, which offer a performance predictibility for the telephone network;

- iv) The response model developed by NetForecast for the Internet protocol [6], which supplies an application response time – R, according to the equation (2):

$$R = 2(D + L + C) + \left( D + \frac{C}{2} \right) \left( \frac{T-2}{M} \right) + D \ln \left( \frac{T-2}{M+1} \right) + \frac{\max \left( 8P \frac{1+OHD}{B}, \frac{DP}{W} \right)}{1 - \sqrt{L}} \quad (2)$$

B – minimum line speed (bps)

C – processing time (s)

D – delay (s)

L – packet loss (%)

M – multiplexing factor

OHD – overhead (%)

P – payload (bytes)

T – application switching counts

W – transmission window width (bytes)

In order to evaluate application or service performance, we use KQI/KPI model [7], which is built from a *Key Quality Indicator*, in charge of information delivering regarding performance level of an application or service and a *Key Performance Indicator*, which describes the resources involved in services assurance. It is obvious that for a KQI computing we need information from many KPIs.

Each KQI/KPI indicator is defined by some specific thresholds, such as warning or error threshold (with minimum and maximum level). Between the two indicators there is a correlation, which can be represented into a two function form:  $f(P_1, P_2, \dots, P_n)$ , characteristic for KPI parameters, respectively  $F(S_1, \dots, S_n)$ , for KQI parameters, like in Fig. 3.

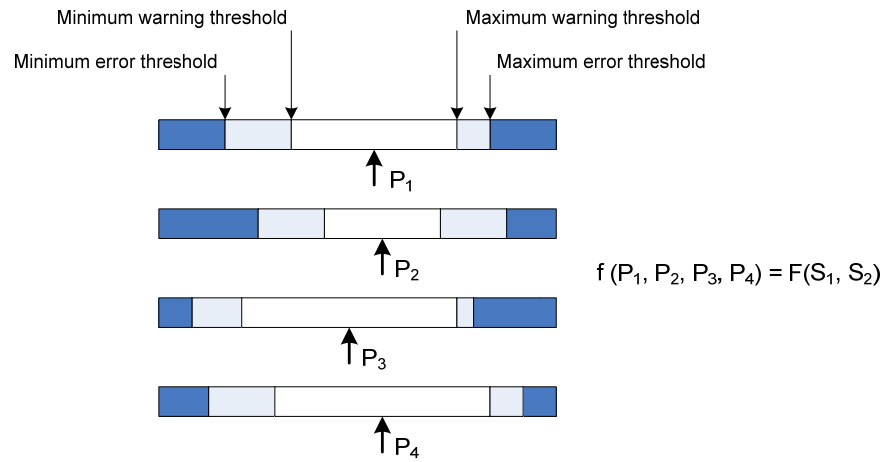


Fig. 3. Relationship between KQI and KPI [7]

As we can see, one set of KPI values, placed into the warning area, could generate a KQI degradation and, as this set grows up, the service could become unfunctional., In the table below, it is illustrated a set of KQI/KPI, which determines specific service quality with impact to the QoE into an organization:

Table 2

**The relationship between KQI/KPI indicators and QoE for some organizational services**

KQI	KPI					
	MTBF, MTTR	Loss of service	Demanding/processed transactions	Delay, jitter	Packet loss	Access violations
Availability	All services	All services	N/A	N/A	N/A	N/A
Video-audio quality	N/A	N/A	N/A	Voice VTC Video Help-desk	Voice VTC Video Help-desk	N/A
Response time	N/A	All services	Dbase access	Voice VTC Video Help-desk	Dbase access	N/A
Connect time	N/A	All services	Dbase access	All services	Dbase access	N/A
Useful traffic	N/A	N/A	Dbase access	N/A	All services	All services
Confidentiality	N/A	N/A	N/A	N/A	N/A	All services
Integrity	N/A	N/A	N/A	N/A	N/A	All services
Non-repudiation	N/A	N/A	N/A	N/A	N/A	All services

N/A: not applicable

#### 4. SLA management in an Intranet network

SLA management (SLAM) represents the continuous process in order to define, accept, deliver, measure and monitor the organisations services, so that the QoE level for all users be maximized, with the corresponding Intranet operation costs minimizing [8], [9].

Intranet SLAM is an end to end management, which includes all the SLAs dealt by network administrator with communication operators (Fig. 4).

The main stages in SLAM life-cycle are the following:

- Service development – consists in user demands identification and Intranet network resources which are involved in this demand assurance. Following this identification, it results a service model;
- Service negotiation – consists in the compromise which an Intranet administrator deals with the users. Starting from the users QoE, the administrator reserves resources in order to establish if the SLA can be observed;
- Service delivery – consists in service activation according to the SLA;
- Service monitoring – consists in KQI/KPI collection, this comparison with the SLA registered values, detection of the SLA violation cases and solution of this kind of situation;
- Service quality analysis – consists, on the one hand, in verification together with user of the QoE level and identification of that demand evolution, and, on the other hand, in establishing the Intranet resource using mode and the service influence on other Intranet delivered services.

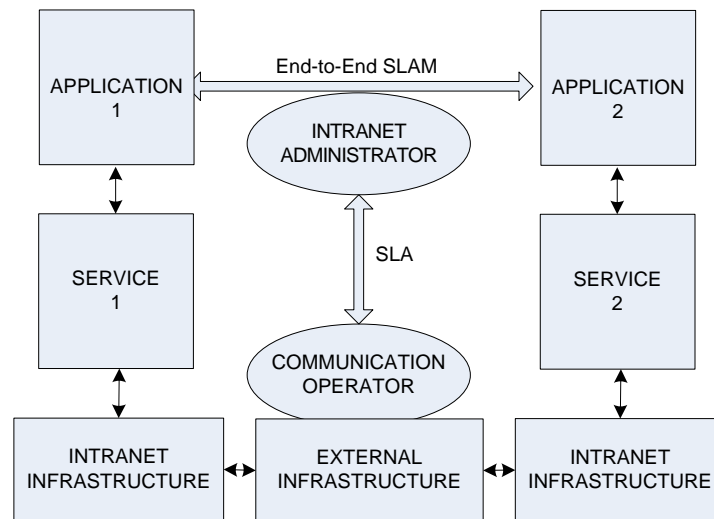


Fig. 4. SLA Management within an Intranet network

In order to facilitate permanent improvement of service quality, SLAM uses a circular process, which allows continuous adjustment of initial SLAs or taking measures (even administrative measures) in case of SLAs violations (Fig. 5).

The compliance with negotiated SLA is done through KQI/KPI measurement deliveries at well defined time intervals and their collection, so that this process does not contribute to service delivery condition (greater connection time or delays in service delivery due to processing of the measurement related information or the congestion produced by a traffic peak generated by this kind of information).

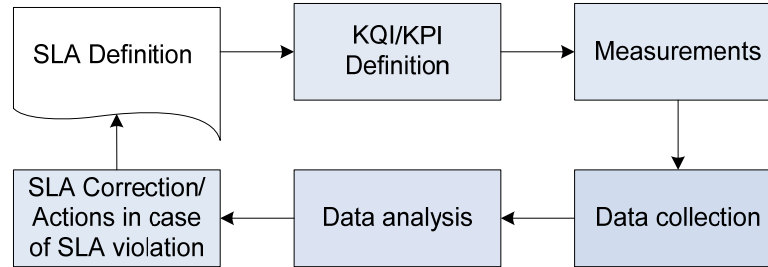


Fig. 5. SLAM process

From the data analysis point of view, this can be designated to Intranet administrator (for internal diagnosis and corrections performing or to audit the SLA which is completed with network operators), to different users (in order to compare SLAs with their own QoE) or to organizational staff (in order to evaluate if the organizational processes are close to the organization's target).

The delivered reports will have a format corresponding to customer's needs, from raw data or messages/alarms in various formats (SNMP, Netflow, RMON etc.) to graphics or global charts in order to contribute to decision regarding the evolution of organisational processes.

### 5. Case study – a proactive SLAM architecture concept in an Intranet network for organisational QoE maximisation

In this section, there will be presented an originally (in the author's opinion) proactive SLAM architecture which is centred within a multi-site distributes Intranet network (as an example an Intranet with 3 sites □ 2 branches and 1 headquarter is chosen) according to Fig. 6, which uses L3 VPN MPLS to transport various internal services and also based on purchased connections from the communication provider in different technologies, such as: SDH, VPN MPLS and DWDM.

Unlike a reactive approach, which assumes, first of all, a post factum issue regarding incidents which appear along SLA assurance or even a triggering of an incident resolution mechanism after users claim, the proposed architecture aims at a possible appearing incident identification, followed by that structuring according



to some well defined profiles and implementation of mechanisms which are in charge with their solution [10].

For that purpose, in the administration area there will be presented more logical elements which make possible a preliminary identification of this kind of problems and their solving before they could produce SLA degradation or more service unavailability.

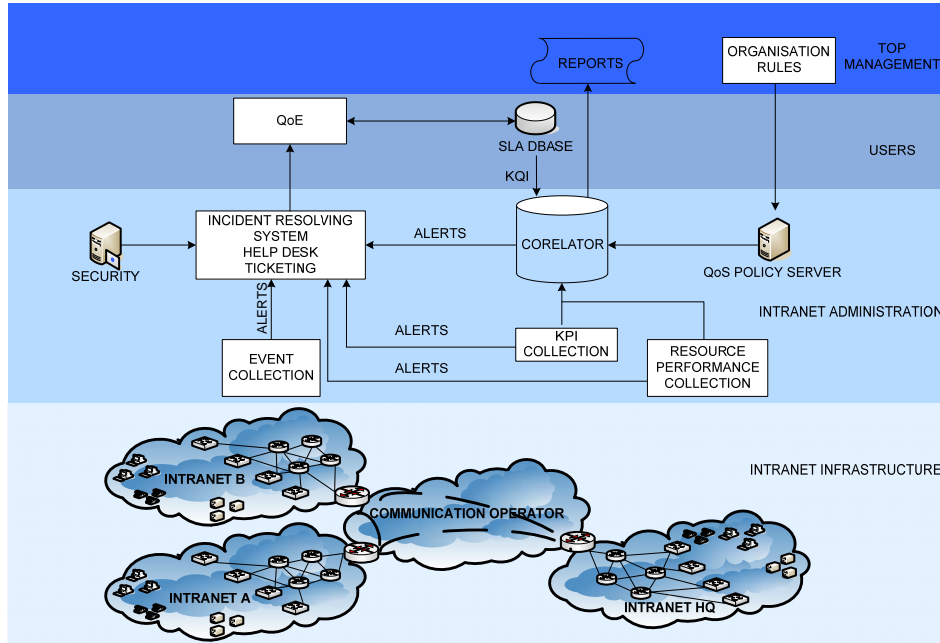


Fig. 6. A proactive SLA management architecture concept within an Intranet network

First of all, there will be developed a collection mechanism for performance indicators KPI, aiming to gather information related to these indicators (e.g. through SNMP). In addition to the collection mechanism it can also be imagined an alerting module, in the case when KPI values exceeded some preconfigured thresholds, like in Fig. 3, in this case alerts activate directly to the incident resolving system.

For example in the case of VoIP service, the alert thresholds for delay and jitter, two very important KPI parameters, could be established to a 10% less values (135ms, respectively 27 ms) than the maximum allowable values for correct service activity. Concurrently, within this mechanism there are provided some interfaces collecting information regarding the incident points with communication operators infrastructure, in order to obtain relevant KPI parameters and compare these values with the operator negotiated SLA.

Another collection mechanism in this architecture refers to the performance of the resources, which compounds Intranet network infrastructure,

such as processors or memory load level in case of network active elements (routers, switches, servers etc.) for a period of time. Similarly to KPI collector, there can be some imposed alert thresholds, for example a 80% processor load, a 60% usage of memory and a 75% buffer filling which could alert directly the incident solving mechanism.

Last but not least, within the collection elements, there is also present the event collection module, its role being to deliver information regarding „environmental condition“ changing, such as information regarding some events produced in the power supply system or the deterioration of the microclimate. Taking into account the particular sensibility of this kind of parameters, with major impact on service availability, all the alerts of this module are directly forwarded to the incident solving mechanism.

An important element from the architecture proposed is the module in charge with the aggregation and correlation between different parameters which are collected from the network and the reference values, derived, on the one hand, from KQI data base, as a result of SLA negotiation between administrator and users and, on the another hand, from the global QoS policies imposed by top management as a result of following the organizations targets through organizational processes/businesses. This is also the place where each profile regarding parameters is defined, so that the overflow of normal values, which constitutes alerts delivered to the incident solving mechanism, must be already structured in order to start the specific solving procedure performed by various incident treating level resources (technical and human).

The parameters' summary review is delivered as reports to the users and to the organization staff. The main KQI parameters, which are reported, are availability, connection time, useful traffic, integrity and so on.

Regarding security, starting with the major impact which the security components have inside an organisation, any kind of alert with regard to the integrity, confidentiality and non repudiation of delivered services is transmited directly to the incident resolving system. The collection module takes data from the three major environments: global security environment (GSE) regarding the sites where Intranet HQ, A and B are located, local security environment (LSE) regarding the rooms where elements of Intranet network are placed and electronic security environment (ESE) which deals with all hardware and software resources that belong to Intranet. According to Fig. 1, the three major domains in which security concept evoluates are: physical security, personnel security and Infosec.

It is obvious that even if security is often considered as an independent domain with its own rules, it is better to integrate major security KQI/KPI into the SLAM from the beginning, in order to develop a complete SLAM, which otherwise can be complicated by adding further demands generated from security condition.

The most important element of the proposed architecture is the incident solving system, which is built from a large complex made of technical, procedural and human resources. Its target is the collection of all the alerts delivered by collection modules and their handling in the shortest time possible.

In the table below, there is a generic mechanism designated as an example to collect and to escalate some of the hardware incidents, which may appear:

Table 3

**Treating mechanism for hardware incidents**

Type of incident	Detection mode	Alert threshold	Escalation level	Action mode
Hardware	SNMP	One incident of severity 1 (for example instable stages of a redundant module inside a router, switch or server)	1	Profile classification, ticket issue, dispatch, incident solving
		Five incidents of severity 1 or one incident of priority 2 (for example a non functionality of a redundant module inside a router, switch or server)	2	Profile classification, ticket issue, dispatch, incident solving
		One incident of severity 3 (for example a non functionality of a network element like router, switch, server)	3	Profile classification, ticket issue, incident solving

The Intranet administrator must also interact with the communication operator NOC in order to solve very quickly any kind of violation of SLA.

In order to assure an efficient incident treatment, the following supplementary measures are necessary:

- Prioritisation of the information provided by collection modules according to severity level;
- Establishing alert profiles and its coherent allocation within the incident solving system in order to prevent the initiation of many incident tickets for the same alert;
- Preliminary documentation of some kind of alerts in order to accelerate their treatment and solving process;
- Alerts simulation in order to train the human resource in charge with treating and solving the incidents.

Even with this kind of measure, it is quite difficult to measure the efficiency level of a proactive SLAM architecture, taking into consideration the important contribution of users in the whole SLAM process, because some of them are tempted to report minor incidents or minor degradation of QoE. Some of

this degradation could be transformed, in correlation with other events, into major incidents. A possible indicator to estimate the efficiency of this architecture could be the percentage of incident solving before any user claims, for the total number of incidents which are relieved in Intranet network.

## 5. Conclusions

SLA management within an organization contributes to achieving strategic organizational targets much more quickly, through a reliable and secure medium in order to deliver information and communication services to the users.

Starting from a general concept of SLAM, in this paper it is proposed a proactive architecture concept in order to convince the QoE users of the following advantages of the Intranet administration:

- A better identification of incidents before this can produce major disruption;
- A better Intranet resource planning, through service development information;
- A much closer approach to the user's needs and demands, including the user co-participation within SLAM;
- A better vision offered to top level organizations' management.

## REFERENCES

- [1] *The TeleManagement Forum and the Open Group*, SLA Management Handbook, **vol. 4**: Enterprise Perspective (GB923), 2004
- [2] *H. Mathieu, F. Biennier*, A Service Level Agreement Management architecture to improve an information system, business processes administration and evolution, *Schedae Informaticae*, **vol. 16**, Jagiellonian University, Institute of Computer Science, 2007
- [3] *K. Kilkki*, Quality of Experience in communications ecosystem, *Journal of Universal Computer Science*, **vol. 14**, no. 5 (2008), pp. 615-624
- [4] *ITU-T Recommendation P.800*, Methods for subjective determination of transmission quality, 1996;
- [5] *L. Carvalho, E. Mota, R. Aguiar, A. Barreto*, An E-Model Implementation for Speech Quality Evaluation in VoIP Systems, *IEEE Symposium Computers and Communications*, pp. 1530-1536, IEEE, 2005
- [6] *P. Sevcik, J. Bartlett*, Understanding Web Performance, Netforecast Report October 2001;
- [7] *E. Toktar, G. Pujolle, E. Jamhour, M.C. Penna, M. Fonseca*, An XML-based Model for SLA Definition with Quality and Performance Indicators, *Proceedings of the 7th IEEE international conference on IP operations and management*, 2007, pp. 196-199
- [8] *N.J. Muller*, Managing Service Level Agreements, *International Journal of Network Management*, **vol. 9**, 1999, pp. 155 – 166
- [9] *E. Marilly, O. Martinot, S. Betgé-Brezetz, G. Delègue*, Requirements for Service Level Agreement Management, *Alcatel CIT*, 2010
- [10] *M. Rudraswamy*, Proactive Performance Management, Cisco Systems, Inc., TM Forum Case Study, August 2008.