Service Level Specification Semantics, Parameters and negotiation requirements.

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document identifies the basic information to be handled by Service Level Specification (SLS, [RFC 2475], [DS-TERMS]) when considering the deployment of value-added IP service offerings over the Internet. Such IP service offerings can be provided together with a given quality of service (QoS), which is expected to be defined in such SLS, from a technical standpoint. Since these IP services are likely to be provided over the whole Internet, their corresponding...
QoS will be based upon a set of technical parameters that both customers and services providers will have to agree upon. From this perspective, this draft aims at listing (and promoting a standard formalism for) a set of basic parameters which will actually compose the elementary contents of a SLS.

Such a specification effort tries to address the following concerns:

- Provide a standard set of information to be negotiated between a customer and a service provider or amongst services providers within the context of processing a SLS;

- Provide the corresponding semantics of such information, so that it might be appropriately modeled and processed by the above-mentioned parties (in an automated fashion).

Table of Contents

1. Introduction
1.1 Motivation
1.2 Objective
2. Basic assumptions and terminology
3. SLS content & template
3.1 Scope
3.2 Flow Identification
3.3 Traffic Conformance Testing
3.4 Excess Treatment
3.5 Performance Guarantees
3.6 Service Schedule
3.7 Reliability
4. Service Level Specification examples
4.1 Virtual Leased Line
4.2 Real-time micro-flows
4.3 Minimum rate guarantee with allowed excess
4.4 Qualitative Olympic Services
4.5 The funnel services
4.6 Best Effort Traffic
5. SLS negotiation requirements
6. Security considerations
7. Acknowledgements

0. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (RFC-2119).
1. Introduction

1.1 Motivation

This document is presented to the IETF community (and the Diffserv WG more specifically) to gauge the interest for advancing the work on the specification of a SLS definition, its semantics and its potential negotiation protocol(s). This interest may be gauged at a future BoF session (e.g., San Diego meeting), specifically on the subject of SLS negotiation across administrative boundaries (customer - provider; provider - provider).

1.2 Objective

This document presents an outline for the definition of a Service Level Specification format, the semantics that go behind this representation, and some early ideas on the requirements on negotiation of SLSs.

The need to have such an agreed set of Service Level Specification parameters and semantics is manifold.

First, it is necessary to be able to allow for a highly developed level of automation and dynamic negotiation of Service Level Specifications between customers and providers. Automation and dynamics are indeed helpful in providing customers (as well as providers) the technical means for the dynamic provisioning of quality of service. The automation in itself is e.g. necessary to allow roaming (dial-in) and to enable mobile users to have access and negotiate a transport Service Level, independent of their point of attachment to the network.

Second, the design and the deployment of Bandwidth Broker capabilities [TWOBIT] in a multi-vendor environment requires a standardized set of semantics for Service Level Specifications being negotiated at different locations:

- between the customer and the service provider (namely between the Customer Premises Equipment (CPE) and its point of attachment to the IP network managed by the service provider);

- within an administrative domain (for intra-domain SLS negotiation purposes);

- between administrative domains (for inter-domain negotiation purposes).

While the representation and semantics behind a Service Level
Specification need to be standardized, this document does not assume that the syntax, nor the SLS negotiation protocol need to be uniquely defined. E.g. the negotiation could make use of various other protocols such as http, rsvp, IPCP, DHCP, etc. The latter is ffs, and as such not part of this document.

The document is structured as follows.

Section 2 lists the basic assumptions underlying this work and some terminology.

Section 3 describes the parameters of the Service Level Specification (template). This draft only describes the semantics of the SLS-attributes, omitting all implementation details as for instance the attribute data types (at this moment).

Section 4 provides some examples of relevant SLS specifications, with the aim to show the usage of the templates. The SLS formalism defined in section 3 allows making a distinction between qualitative and quantitative SLSs:

- SLSs depicting qualitative services should yield the specification of relative QoS indicators, such as a low IP datagram loss ratio. From this standpoint, best effort traffic is expected to be qualified by a SLS of that range of qualitative services.

- SLSs depicting quantitative services should yield the accurate measurement of QoS indicators, such as e.g., transit delay.

Sections 5 and 6 finally describe some SLS (protocol) negotiation requirements and security considerations respectively.

The material presented in this draft derives from work within the IST-TEQUILA project [TEQUILA].

2. Basic assumptions and terminology

The basic assumption of this draft is that IP services will be deployed over a public IP infrastructure, which will be (partly if not completely) composed of diffserv-aware network elements ([RFC-2475], [DS-MODEL]). These network elements are able to process Per Hop Behaviors (PHBs), including the Assured Forwarding PHB ([RFC-2597]), and the Expedited Forwarding PHB ([RFC-2598]).

Customers of such services include Internet Service Providers (ISP), who may well establish QoS-based peering agreements between themselves, and usual customers of ISPs, like those who compose both
the residential and the corporate market.

The terminology used in this draft is in agreement with the DiffServ Working Group terminology introduced and specified in [RFC-2475], section 1.2 "terminology".

3. SLS content & template

The following describes the attributes of the Service Level Specification. It should be remarked that some SLS-features are not yet specified in this draft. For example, the Internet2 QoS Working Group specifies a SLS for the EF-based Premium Service [QBONE]. One of the attributes, i.e. "Route", is used for inter-domain routing aspects. This and other SLS features are for further study.

3.1. Scope

The scope of a SLS associated to a given service offering indicates where the Quality of Service (QoS) policy for that specific service offering is to be enforced. Therefore the scope uniquely identifies the geographical/topological region over which the QoS is to be enforced by indicating the boundaries of that region.

A SLS is associated with uni-directional traffic flows. Note however that this does not exclude the provisioning by providers of bidirectional contracts, by combining one or more SLSs.

The associated scope of the SLS MUST be expressed by a couple of ingress and egress interfaces. Ingress/egress denote respectively the entry/exit points of the IP packets relative to the region (network).

Scope = (ingress, egress) with ingress/egress defined as
- Ingress: interface identifier | set of interface identifiers | all
- Egress : interface identifier | set of interface identifiers | all

Remarks:
- "|" denotes an exclusive OR.
- "all" is logically equal to unspecified.

The semantics allows for the following combinations of (ingress, egress) interfaces:
- (1,1) - one-to-one communication
- (1,N) - one-to-many communication (N>1)
- (1,all) - one-to-any communication
- (N,1) - many-to-one communication (N>1)
- (all,1) - any-to-one communication

Remark that this excludes e.g. the many-to-many communication. Either ingress OR egress MUST be specified to exactly ONE interface identifier (with a non-exclusive OR).

In the sequel SLSs with an associated scope (topology) of (1,1); (1,N); (N,1) will be called respectively Pipe, Hose and Funnel SLSs.

Disclaimer:

An ingress (or egress) interface identifier should uniquely determine the boundary link as defined in [RFC-2475] on which packets arrive/depart at the border of a DS domain. This link identifier MAY be an IP address, but it may also be determined by a layer-two identifier in case of e.g. ethernet, or for unnumbered links like in e.g., PPP-access configurations. The interface identifier(s) may also implicitly be derived from the source or destination address information in the Flow Identification field (see next). More detailed specifications are for further study.

3.2. Flow Identification

The flow identification (Flow Id) of a SLS associated to a given service offering indicates for which IP packets the QoS policy for that specific service offering is to be enforced.

A Flow Id identifies a stream of IP datagrams sharing at least one common characteristic. A SLS Flow Id MAY formally be specified by setting one or more of the following attributes:

Flow Id = (DSCP, source information, destination information, application information)

- Differentiated Services Code Point (DSCP) = specified value [RFC-2474]

- Source information = source address | set of source addresses | set of source prefixes | all
Thus, the Flow Id may be expressed by information attributes related to the source/destination nodes, the application or the DS field in the IP header. The Flow Id provides the necessary information for classifying the packets at a DS boundary node.

This datagram classification can either be Behaviour Aggregate (BA) or Multi-Field (MF) classification based.

In case of BA-classification [RFC-2475], the DSCP attribute MUST be specified and the other attributes MUST NOT be specified.

In case of MF-classification all attributes MAY be specified. Remark that MF classification may as well depict micro-flows as aggregate flows [DS-MODEL].

Note that there are restrictions involved in combining scope and flow identification within a certain SLS instance.

3.3 Traffic Conformance Testing

Traffic Conformance Testing is the set of actions which uniquely identifies the "in-profile" and "out-of profile" (or excess) packets of an IP stream (identified by Flow-Id). Traffic Conformance Testing will usually be done at a DS-boundary node.

The SLS specifies the Traffic Conformance Testing as a combination of the Traffic Conformance Parameters and the Traffic Conformance Algorithm. The Traffic Conformance Parameters describe the reference values the traffic (identified by the Flow ID) will have to comply with, thus yielding the notions of "In" and "Out" of profile traffics. The Traffic Conformance Algorithm is the mechanism enabling unambiguously to identify all "in" or "out" of profile packets based on these Conformance parameters.

The following gives a (non-exhaustive) list of potential conformance parameters.

- Peak rate p
- Token bucket rate \( r \)
- bucket depth \( b \)
- Minimum MTU \( m \)
- Maximum MTU \( M \)

Notes:

Examples:

- Conformance parameters = token bucket parameters \( (b, r) \); conformance algorithm = token bucket algorithm.

- Conformance parameters = peak rate \( p \); conformance algorithm = (flow) rate must be smaller than \( p \) (at all time scales)

- Conformance parameters = maximum MTU; conformance algorithm = all packets allowed with size smaller than MTU

The detailed specification of these parameters together with conformance algorithms is for further study.

3.4. Excess Treatment

This section describes how the service provider will process excess traffic, i.e. out-of-profile traffic. The process takes place after Traffic Conformance Testing, described previously.

Excess traffic may be dropped, shaped and/or remarked. The SLS MUST specify the appropriate action by the following attribute.

- Excess Treatment

If Excess Treatment is not indicated, then excess traffic is dropped. Depending on the appropriate action, more parameters MAY be required (for further study).

- If excess traffic is shaped, then shaping parameters should be given, e.g. the (output) shaping rate.

- If excess traffic is marked or remarked, then Marking parameters should be given, e.g. "coloring" the packets with drop precedence equal to "red". Packet reordering MUST be avoided when a remarking operation occurs.
3.5. Performance Guarantees

The performance parameters describe the service guarantees the network offers to the customer for the packet stream described by the Flow Id and over the geographical/topological extent given by the scope. All service guarantees are for the in-profile traffic; no guarantees are given for excess (out-of-profile) packets.

There are four performance parameters:

- delay | optional quantile
- jitter | optional quantile
- packet loss
- throughput

The following definitions always consider the (measurable) performance parameters related to the packet stream specified by the Flow Id.

The delay and jitter indicate respectively the maximum packet transfer delay and packet transfer delay variation from ingress to egress.

Delay and jitter may either be specified as worst case (deterministic) bounds or as quantiles. Indeed, the worst case delay/jitter bounds will be very rare events and customers may find measurements of e.g. 99.5th percentile a more relevant empirical gauge of delay/jitter.

The packet loss indicates the packet loss probability for in-profile packets from ingress to egress

\[
\text{packet loss} = \frac{\text{lost in-profile packets between ingress and egress}}{\text{offered (injected) in-profile packets at ingress}}
\]

The throughput is the rate measured at egress counting all (non-lost) injected in-profile packets at ingress.

Remark about the relation between throughput and excess treatment.

- If excess traffic is allowed (shaped/marked), then "throughput" indicates a minimum guarantee. It is the guaranteed throughput for
in-profile packets while extra available resources may eventually
be allocated to the out-of-profile traffic.

- If excess traffic is dropped, then "throughput" indicates a
maximum guarantee.

Disclaimer about throughput

The performance parameter "throughput" as indicated above is the
guaranteed throughput the network provider offers to the customer
(between ingress and egress). There is however a tight relationship
between packet loss (p), throughput (R) and conformance parameters
(if all indicated of course).

Take e.g. the token bucket parameters (b,r) as conformance
parameters. If the packet loss is small (e.g. 10E-6), then the
network (implicitly) guarantees a throughput R = r. Therefore it is
not yet clear for the authors whether the (guaranteed) throughput R
must be specified in the SLS as a separate parameter, or whether R
can be derived from e.g. the token bucket parameters.

This issue is further study.

Quantitative performance guarantees

A performance parameter is said to be quantified if its value is
specified to a numeric (quantitative) value.

The service guarantee offered by the SLS is said to be quantitative
IF at least one of the 4 performance parameters is quantified.

Qualitative performance guarantees

If none of the SLS performance parameters are quantified, then the
performance parameters "delay" and "packet loss" MAY be "qualified".

Possible qualitative values (for delay and/or loss): high, medium,
low.

Relative delay guarantees:

- gold service : value = low
- silver service : value = medium
- bronze service: value = high or not indicated

Relative loss guarantees
- green service: value = low
- yellow service: value = medium
- red service: value = high or not indicated

The quantification of relative difference between <high/medium/low> is a provider policy (e.g. high = 2 x medium; medium = 2 x low).

The above taxonomy yields the following combinations of qualitative services.

<table>
<thead>
<tr>
<th>Delay</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>gold green</td>
</tr>
<tr>
<td>medium</td>
<td>gold yellow</td>
</tr>
<tr>
<td>high</td>
<td>gold red</td>
</tr>
</tbody>
</table>

The service guarantee offered by the SLS is said to be qualitative if it is NOT quantitative and either delay or loss (non-exclusive) are qualified to "medium" or "low", i.e. excluding bronze/red from the above.

The service guarantee offered by the SLS is said to be best-effort if it is NOT quantified nor qualified.

3.6. Service schedule

The service schedule indicates the start time and end time of the service, i.e. when is the service available.

This might be expressed as collection of the following parameters:
- Time of the day range
- Day of the week range
- Month of the year range
Some examples are:
- Time of the day range
  08h00-18h00

- Day of the week range
  A single day
  A group of sequential days

- Month of the year range
  A single month
  A group of sequential months

- Year range
  A single year
  A group of sequential years

Remark: service schedule "from now on" [now, infinity] can be captured by putting the above to their full range.

3.7. Reliability

Reliability indicates the maximum allowed mean downtime per year (MDT) and the maximum allowed time to repair (TTR) in case of service breakdown (e.g. in case of cable cut).

The Mean Down Time might be expressed in minutes per year and the Maximum Time To Repair might be expressed in seconds.

3.8 Others

Other parameters such as route, security, etc... remain for further study.


Within this section a number of example instantiations of SLSs are presented to illustrate the potential use of the SLS template defined above.

4.1. Virtual Leased Line

The following specifies the SLS for a (uni-directional) VLL with quantified throughput guarantee (with guaranteed throughput of e.g 1 Mbps) and packet loss
- Scope: one-to-one communication (Pipe model), (Ingress, Egress) specified

- Flow specification: DSCP-value (e.g. DSCP indicating the EF-PHB). Another possibility is setting the (source,destination) IP-addresses.

- Traffic Conditioning: leaky bucket \((b,r)\), \(r = 1\text{ Mbps}\)

- Excess Treatment = dropping. Thus only in-profile packets are allowed.

- Performance Parameters: guaranteed throughput \(R = r\). packet loss = \(10^{-6}\).

- Service Schedule: may be indicated

- Reliability: may be indicated

4.2. Real-time micro-flows

- Scope: one-to-one communication (Pipe model), (Ingress, Egress) specified

- Flow specification: (source IP-address, destination IP-address, source port number, destination port number, protocol)

- Traffic Conditioning: leaky bucket \((b,r)\), peak rate \(p = r = 64\text{ Kbps}\)

- Excess Treatment = dropping.

- Performance Parameters: delay = 10 msec, packet loss = \(10^{-3}\), guaranteed throughput \(R = r\).

4.3 Minimum rate guarantee with allowed excess

The following could be for bulk FTP traffic that requires a minimum throughput, but would take everything it can get (TCP). Also adaptive applications, like video streaming, that however require a minimum throughput for the service.

- Scope: one-to-one (Pipe)

- Flow specification: e.g. DSCP-value indicating a possible AF-PBH.

- Traffic Conformance Parameters: \((b,r)\) MUST be indicated (peak rate is optional)
- Excess Treatment: Remarking MUST be indicated (excess is given a higher drop precedence)
- Performance guarantees: guaranteed throughput $R = r$.

4.4. Qualitative Olympic services

The following SLS is meant for the Olympic Service. It could be used for differentiating applications such as web-browsing and e-mail traffic.

SLS 1 (on-line web-browsing) - Scope: one-to-one (pipe) or one-to-many (hose)
- Flow specification: MAY be indicated
- Traffic Conformance Parameters: token parameters $(b, r)$ The token bucket rate $r$ indicates an (average) maximum Committed Access Rate (CAR) for which "better-than-best-effort" treatment will be applied.
- Excess Treatment: remarking.
- Performance Parameter: Delay and Packet loss are indicated as "low": gold/green class

SLS2 : (background e-mail traffic)

This is identical to SLS1 but targeting the silver/green class.

4.5. The Funnel service

The service offered by the funnel model is primarily a protection service: the customer wants to set a maximum on the amount of traffic (characterized by a DSCP) entering his network. It could e.g. be used for business customers to restrict the amount of web browsing traffic entering their network.

```
/---------------\
|Network _____|_____ B
A_______|____/ |_____ C
/\a(out) | __/\ |_______D
\---------------/
```

Figure 4: Funnel model
In [Figure 4], the customer A requires that the traffic entering his network from B, C and D does not exceed the rate a_out.

- Scope: Funnel (N|all,1).

- Flow specification: DSCP MUST be indicated. The filter (see below) is applied to all traffic characterized by the DSCP -value.

- Traffic Conformance Parameters: (b, r) MUST be indicated. The token bucket parameters indicate the maximum allowed throughput (r = a_out) towards the customer network on the specified egress interface. This maximum or filter is applied to all packets marked with the DSCP-value indicated above.

- Excess treatment: dropping (this is actually the service offered by the network).

- Performance Parameter: not specified.

4.6. Best effort traffic

- Scope : all models

- Flow specification : none

- Traffic Conformance Parameters: if not indicated, then the full link capacity is allowed

- Excess Treatment: not specified

- Performance Parameters: none

- Service Schedule: may be indicated.

- Reliability: may be indicated.

5. SLS negotiation requirements

[This section is informational and preliminary. More detailed study is required.]

A major goal of the availability of an SLS template is helping in the deployment of dynamical SLS negotiation procedures between customer and providers or between providers. This draft only discussed the SLS template and its basic contents. The SLS negotiation protocol is for further study. The following lists a number of conditions which should be met by a (to be defined) SLS negotiation protocol.
The SLS negotiation protocol MUST allow for:

- Original service requests, according the components of the specified SLS.

- Service acknowledgement (ACK), indicating agreement with the requested service level.

- Service rejection (NAK) but indicating the possibility of offering a closely related service (or indication of alternative DSCP to use for a particular service). The reply message may indicate the related offering by overwriting the proposed SLS attributes (hints).

- Service rejection (REJECT) indicating incapability of providing the service.

- The ACK/NACK procedures require a reliable transport mode for such a negotiation protocol.

- Service modification from both user and provider.

The following are further requirements for the overall network architecture which SHOULD be fulfilled.

- The protocol should be able to interact with feedback of events related to the service. For example performance degradation MAY result in re-negotiation of the SLS.

- The protocol should preferentially make use of / be an extension of existing specifications protocol design work available such as RSVP ([RFC-2205]) or PPP/IPCP ([RFC-1661]).

6. Security considerations

The information which will yield the instantiation of a SLS template to address the specific requirements of a customer in terms of the quality associated to the service it has subscribed to may require the activation of security features so that:

- Identification and authentication of the requesting entity needs to be performed;

- Identification and authentication of the peering entities which will participate in the SLS negotiation process needs to be performed;

- Preservation of the confidentiality of the information to be
conveyed during the SLS negotiation and instantiation procedures between the peering entities is a MUST.

7. Acknowledgements

Part of this work has been funded under the European Commission 5th framework IST program.

The authors would like to acknowledge all their colleagues in the TEQUILA project for their input and reflection on this work.

References

[TEQUILA] IST-Tequila project http://www.ist-tequila.org/


Full copyright statement

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works.

However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Authors Addresses

Danny Goderis
Alcatel Corporate Research Center
Fr. Wellesplein 1, 2018 Antwerpen, Belgium.
Phone  : 32-3-240-
Fax     : 32-3-240-9932
E-mail: Danny.Goderis@Alcatel.be

Yves T’Joens
Alcatel Corporate Research Center
Fr. Wellesplein 1, 2018 Antwerpen, Belgium.
Phone  : 32-3-240-
Fax     : 32-3-240-9932
E-mail: Yves.TJoens@Alcatel.be
Carmelo Zaccone
Alcatel Corporate Research Center
Fr. Wellesplein 1, 2018 Antwerpen, Belgium.
Phone : 32-3-240-8344
Fax : 32-3-240-9932
E-mail: Carmelo.Zaccone@Alcatel.be

Christian Jacquenet
France Telecom Research and Development
FT R&D /DMI
42, rue des Coutures
BP6243
14066 CAEN CEDEX 04
France
Tel : +33 2 31 75 94 28
Fax : +33 2 31 73 56 26
e-mail : christian.jacquenet@francetelecom.fr

George Memenios
Research Associate, Telecommunications Laboratory NTUA
Heroon Polytechniou 9
157 73 Zografou, Athens, Greece
Phone : +30 1 772 1494
Fax : +30 1 772 2534
E-mail: gmemen@telecom.ntua.gr

George Pavlou
Centre for Communication Systems Research (CCSR)
Univ. of Surrey, Guildford, Surrey GU2 7XH, UK
Phone : +44 (0)1483 259480
Fax : +44 (0)1483 876011
E-mail: G.Pavlou@eim.surrey.ac.uk

Richard Egan
Racal Research Ltd
Worton Drive
Worton Grange Industrial Estate
Reading, Berkshire RG2 OSB
tel: +44 118 986 8601
fax: +44 118 923 8399
e-mail : richard.egan@rrl.co.uk

David Griffin
Department of Electronic and Electrical Engineering
University College London
Torrington Place, London WC1E 7JE, UK
Phone: +44 (0)20 7679 3557
Fax: +44 (0)20 7388 9325
Email: D.Griffin@ee.ucl.ac.uk

Panos Georgatsos
Algosystems S.A.
4, Sardeon str., 172 34 Athens, Greece
Phone: 30-1-93-10-281
Fax: 30-1-93-52-873
E-mail: pgeorgat@algo.com.gr

Leonidas Georgiadis
Aristotel Univ. of Thessaloniki, Faculty of Engineering
School of Electrical and Computer Engineering, Telecommunications Dept.
PO Box 435, Thessaloniki, 54006, Greece
Phone: 30-31-996385
Fax: 30-31-996312
E-mail: leonid@eng.auth.gr