Network Working Group
Internet Draft
Document: draft-tequila-sls-03.txt
Category: Best Current Practice
Expires April 2004

D. Goderis
Alcatel
D. Griffin
University College London
C. Jacquenet
France Telecom
G. Pavlou
University of Surrey
Editors

October 2003

Attributes of a Service Level Specification (SLS) Template
<draft-tequila-sls-03.txt>

Status of this Memo

Abstract

This document depicts a standard set of information to be (dynamically) negotiated between a customer and an IP service provider or between service providers, by means of instantiated Service Level Specifications (SLS). It also specifies 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

The deployment of value-added IP service offerings over the Internet has yielded a tremendous effort for the definition, the specification and possibly the standardization of the notion of Quality of Service (QoS), which generally encompasses a wide set of elementary parameters, such as the maximum transit delay, the inter-packet delay variation, or the packet loss rate.

Because the subscription to an IP service offering implies the definition of a contractual agreement between the customer and the corresponding IP Service Provider (ISP), the level of quality that will be associated to the deployment of such service will be based upon a set of the aforementioned parameters both parties will have to

agree upon.

From this perspective, this document aims at listing (and promoting a standard formalism for) a set of basic parameters that will compose the elementary contents of a SLS, hence yielding the specification of a (hopefully) standardized SLS template that should dramatically facilitate the enforcement of IP QoS policies, especially with an inter-domain context where QoS-based IP service offerings are deployed over the whole Internet.

Thus, this document presents an outline for the definition of the SLS parameters and the semantics that go behind this representation. As such, the document is structured as follows:

- Section 4 lists the basic assumptions this work relies upon, and also provides a glossary of the terms used in this draft,

- Section 5 specifies the SLS template, while section 6 provides some example of SLS instantiations, with the goal to show how such templates could be used,

- Finally, sections 7 and 8 provide a list of requirements as far as the use of a SLS negotiation protocol is concerned, and some security considerations, respectively.

2. 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 [2].

3. Changes since the Previous Version

The following changes have been made since the previous version of the document:

- Most of the text has been cleaned up and the overall organization of the document has been reviewed,

- A section on SLS negotiation protocol requirements has been added,

- Both the References and Authors' sections have been updated,

- Remaining typos have been corrected.

4. Basic Assumptions

4.1. A DiffServ-driven Approach

The basic assumption of this document is that IP service offerings will be deployed over a public IP infrastructure (namely the

Internet) where part of if not all the network devices (namely the IP routers) will be DiffServ-capable, as per [3]. In particular, these

routers support Per Hop Behaviors (PHB), like the Assured Forwarding (AF) PHB ([4]) and the Expedited Forwarding (EF) PHB ([5]).

In this document, ISPs are in charge of the exploitation of the underlying IP infrastructure that will support the QoS-based IP service offerings customers will have the ability to subscribe to, while the level of quality associated to these services is technically described in SLS templates.

Furthermore, the DiffServ-related terminology used in this document fully complies with [6].

4.2. Positioning SLS Templates in a Layered Model

The Differentiated Services specification effort has yielded the identification of a set of elementary functions and concepts, whose respective interactions can be depicted according to a layered approach, as per the following figure 1.

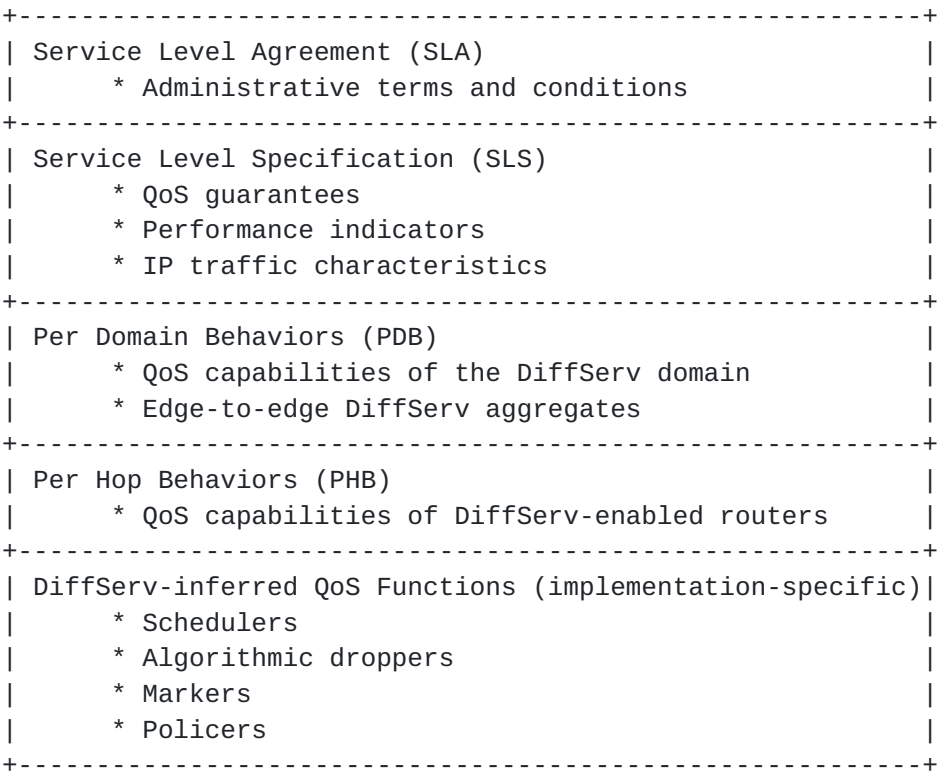

Fig. 1: A Layered Model of DiffServ.

As per figure 1, each of the layer displays its own QoS capabilities. According to the definition of a Per-Domain Behavior (PDB, [7]), the specification of such PDBs should include the reference to the (lower layer) PHB(s) the PDB "layer" relies upon.

Furthermore, the mapping between instantiated SLS templates and PDBs remains an unexplored area: for example, a SLS is service-oriented and customer-specific, whereas a PDB is customer-unaware.

5. Service Level Specification Template

The following sub-sections provide a description of the attributes that MAY be conveyed and valued in a given SLS template.

5.1. The Scope Attribute

The Scope attribute of a SLS template indicates where the QoS policy for the corresponding IP service offering is to be enforced. Therefore, the scope uniquely identifies the network region where the QoS policy will be enforced, by defining the boundaries of such region.

The scope of a SLS MUST be expressed by a couple of ingress and egress interfaces. Ingress and egress respectively denote the entry and exit points of the network region that will convey the IP datagrams associated to the corresponding service offering.

The introduction of the notion of ingress and egress interfaces implicitly states that SLS templates refer to uni-directional IP flows, where an IP flow is a set of IP datagrams that share at least one common characteristic, e.g. the same destination address. Obviously, the direction dimension of a SLS template does not exclude the provisioning of bi-directional SLS templates, thanks to the combination of at least two SLS templates.

5.1.1. Semantics of the Scope Attribute

Scope = (ingress, egress), where:

- Ingress = Interface (I/F) Identifier | Set of I/F Identifiers | Any

- Egress = Interface Identifier | Set of I/F Identifiers | Any

Note that "|" denotes an exclusive OR, while "Any" is logically equivalent to "Unspecified".

5.1.2. Possible Combinations of the Scope Attribute

The following combinations are permitted:

(1, 1), which reflects a one-to-one (peer-to-peer) communication. This kind of scope refers to "Pipe" SLS templates in the rest of the document,

(1, N), which reflects a one-to-many communication (N > 1), e.g. a videoconferencing service. This kind of scope refers to "Hose" SLS templates in the rest of the document,

(1, Any), which reflects a one-to-any communication, e.g. a broadcasting service,

(N, 1), which reflects a many-to-one communication, e.g. an IP Virtual Private Network (VPN) service offering, deployed according to a hub-and-spoke topology. This kind of scope refers to "Funnel" SLS templates in the rest of the document,

(Any, 1), which reflects an any-to-one communication (e.g. all the IP traffic of a stub domain that has a single exit point towards the Internet).

This scope taxonomy currently excludes the case of many-to-many communication types, which would be denoted as (M, N) according to the above semantics: either the ingress or the egress interfaces MUST be unique, whereas scopes of the (M, N) type could be de-composed into M instances of scopes of the (1, N) types, a.k.a. M instances of Hose SLSes.

Also, there SHOULD be a 1:1 relationship between the interface identifier and the link the interface is attached to. The corresponding link identifier MAY be an IP address, but it may also be any other identification means both parties (customer and provider) would have agreed upon: for example, layer 2 link identifiers could be used in either Ethernet or PPP (Point-to-Point Protocol, [8]) access links.

5.2. The Flow Identifier (Flow ID) Attribute

The Flow Identifier (Flow ID) attribute of a SLS template refers to the IP flow, defined as a set of IP datagrams that share at least one common characteristic, and which corresponds to the IP service offering whose level of quality is technically depicted in the aforementioned SLS. This parameter provides an input for IP datagram classification to be performed by a DiffServ boundary node. Such a classification can either reflect a Behavior Aggregate (BA) or a Multi-Field (MF) taxonomy.

The MF-based classification may either depict micro-flows or macro-flows, based on the source prefix attribute, for example (see section 5.2.1 below).

5.2.1. Semantics of the Flow ID Attribute

A given SLS template MUST contain one and only one Flow ID attribute, which MAY formally be described by one or a combination of the following attribute.

Flow ID = {DiffServ Information, Source information, Destination

Information, Application Information}, where:

- DiffServ Information = DSCP Value | Set of DSCP Values | Any

- Source Information = Source IP address | Set of source IP addresses | Source Prefix | Set of Source Prefixes | Source AS | Any

- Destination Information = Destination IP address | Set of destination IP addresses | Destination Prefix | Set of Destination Prefixes | Destination AS | Any

- Application Information = Protocol number | Source Port | Destination Port | (Source Port, Destination Port) | Any

5.2.2. Usage of the Flow ID Attribute

In the case of a BA-based classification, the DiffServ information MUST be provided, while the remaining information of the Flow ID attribute MUST NOT be specified. As an example, an Ordered Aggregate (OA) that defines a stream of AF-marked IP datagrams could be described by a single Flow ID attribute using several DSCP values, indicating as many drop precedence levels. Note that the DSCP value of the Flow ID's DiffServ information does not necessarily relate to a specific PHB, but rather is a means (among others) for identifying an IP flow.

In the case where the Flow IP attribute is valued with the (IP source address, IP destination address) pair while the Scope attribute is left unspecified, there is therefore no specific assumption about the ingress and egress points that the corresponding traffic will cross. Furthermore, it is the responsibility of the service provider to select the route (thanks to the enforcement of a routing if not a traffic engineering policy) that will convey this traffic across the DiffServ domain.

On the other hand, if both the Scope and Flow ID attributes of a SLS template have been specified so that the (Ingress I/F, Egress I/F) pair as well as the (Source IP Address, Destination IP Address) pair have been explicitly valued, then the route followed by the flow between the two hosts MUST go through the Ingress and Egress interfaces.

5.3. The Performance Attribute

The Performance attribute describes the network level of quality that is associated to the transportation of an IP flow, as it has been defined by the Flow ID attribute of the SLS template, and within the limits defined by the Scope attribute of the same SLS template.

The Performance attribute is a set of indicators, and four indicators have been defined so far, according to the following semantics.

5.3.1. Semantics of the Performance Attribute

The following indicators compose the Performance attribute of a SLS template.

- One-way delay ([9]), measurement period, optional quantile

- Inter-packet delay variation ([10]), measurement period, optional quantile

- Packet loss rate ([11]), measurement period

- Throughput, measurement period

For a given SLS template, all these indicators refer to an IP flow which has been described by the valued Flow ID attribute of the SLS, and within the ingress and egress domain boundaries, as per the Scope attribute of the SLS. Such indicators are measured during a period of time which is specified by the "measurement period" indication associated to each indicator.

The quantile indication is an optional parameter that is relevant to reflect an empirical gauge of the corresponding performance indicators. For example, a SLS template whose Performance attribute would contain the triplet (delay = 10 ms, measurement period = 5 min, quantile = 10E-3) means that the customer's expectation is that the probability of delays greater than 10 ms is less than 10E-3 for any measurement period of 5 minutes.

Such Performance attribute semantics therefore yields the specification of arrays like N (delay/loss, quantile) pairs. The more pairs, the better the delay probability can be approximated as a tail distribution.

As for the throughput indicator, it is measured at the egress point (as defined in the Scope attribute of the SLS), by counting all the outgoing IP datagrams described by the Flow ID attribute of the SLS.

5.3.2. Quantitative aspects of the Performance Attribute

One of the performance indicators of the Performance attribute is said to be quantitative whenever its value is expressed as a numeric value. Then, the QoS reflected by an instantiated SLS is said to be quantitative when at least one of the indicators of the Performance attribute of the SLS is quantified.

5.3.3. Qualitative aspects of the Performance Attribute

If none of the indicators of the Performance attribute of a given SLS

has been quantified, then such indicators MAY be valued so that they reflect a qualitative QoS. The corresponding values of these

indicators MAY therefore be of the following kind: "low", "medium", "high".

From a commercial perspective, such values MAY be associated to the definition of QoS-based IP service offerings, such as the "Bronze" service (e.g. with a delay indicator valued at "high"), the "Silver" service, (e.g. with a loss indicator valued at "medium"), and the "Gold" service (e.g. with a (delay, loss) pair valued at "low").

5.4. The Traffic Conformance Attribute

The Traffic Conformance attribute of a SLS template is a set of indicators that aim at describing how an IP flow (as depicted by the Flow ID attribute of the SLS) should "look like" (e.g. in terms of volume (per unit of time)) so that the customer be serviced according to the level of quality that has been described in the Performance attribute of the SLS for this traffic.

The indicators of the Traffic Conformance attribute are the input data for traffic conformance algorithms, whereas traffic conformance testing functions are operated at the boundaries of a DiffServ domain, thanks to the contents of the Traffic Conformance attribute and the aforementioned algorithm.

Basic traffic conformance testing relies upon a set of actions that yield the identification of "in-profile" and "out-of-profile" IP datagrams of a given IP flow (as depicted by the Flow ID attribute of the SLS). From this standpoint, the indicators that have been valued in the Traffic Conformance attribute of a given SLS describe the reference values the IP flow will have to comply with, hence the notions of "in-profile" and "out-of-profile" traffics.

The traffic conformance algorithm is the means that unambiguously identifies in-profile and out-of-profile IP datagrams, based upon the valued indicators of the Traffic Conformance attribute of the SLS.

Furthermore, there MAY be cases where traffic conformance testing actions are iterative, hence the notion of multi-level traffic conformance testing, where an IP datagram of a given flow will be tagged (thanks to a particular action taken by the traffic conformance algorithm) to reflect its belonging to a specific level.

In such cases, the Traffic Conformance attribute of the SLS template MUST indicate the level the indicators refer to.

5.4.1. Semantics of the Traffic Conformance attribute

Indicators that MAY be conveyed by the Traffic Conformance attribute include:

- Multi-Level Conformance Testing n (n being an integer)

- Peak Rate p (expressed in bits per second or kilobits per second)

- Token Bucket Rate r (expressed in bits per second or kilobits per second)

- Bucket Depth b (expressed in bytes)

- Maximum Transfer Unit (MTU) M (expressed in bytes)

- Minimum Packet Size m (expressed in bytes).

5.4.2. Usage of the Traffic Conformance attribute

5.4.2.1. Basic Conformance Testing

Basic conformance testing MAY rely upon the use of a token bucket algorithm, whereas the indicators of the Traffic Conformance attribute of the SLS template will be the token bucket rate r and the bucket depth b.

Also, when defining the MTU indicator of the Traffic Conformance attribute of the SLS, then the corresponding conformance algorithm will consist in the following:

- If the size of the incoming IP datagram is smaller or equal to MTU, then the datagram will be forwarded,

- If the size of the incoming datagrams is strictly greater than the MTU, then the datagram will be dropped.

5.4.2.2. Two-Level Conformance Testing

A two-rate three-colour marker relies upon the use of two token buckets, whose respective rates are denoted r1 and r2 (with r2 > r1). Both buckets contain green and yellow tokens, respectively. In this case (where the indicators of the Traffic Conformance attribute of the SLS are the (r1, b1) and (r2, b2) characteristics of the token buckets), a simple traffic conformance algorithm is the following:

- If there are green and yellow tokens left in the respective buckets, an incoming datagram will be tagged "green",

- If there are yellow tokens left only, an incoming datagram will be tagged "yellow",

- The incoming datagram will be tagged "red" otherwise.

5.5. The Excess Treatment Attribute

The SLS template MUST describe how out-of-profile traffic flows will be processed, and this is the role of the Excess Treatment attribute. By default, if the Excess Treatment attribute is not specified in the SLS template, in excess traffic will be dropped.
As a consequence, the semantics of the Excess Treatment attribute of the SLS template will consist in describing a specific action to be taken by the (DiffServ-enabled) router: such actions MAY consist in re-marking the IP datagrams (i.e. modifying the value of the DSCP bits), storing in-excess traffic in specific queues, etc. (a combination of elementary actions, e.g. "re-mark then store" SHOULD also be possible).

5.6. The Service Schedule Attribute

The Service Schedule attribute of a SLS template reflects the "working hours" of the corresponding service, by indicating both start and end times of the service. This attribute might be expressed as a collection of the following indicators:

- Time of the day range, e.g. a service is available from 08:00 to 17:00,

- Day of the week range, e.g. a service available from Monday to Friday,

- Month of the year range, e.g. the service is available from June 2003.

5.7. The Reliability Attribute

The Reliability attribute of a SLS reflects the maximum Mean Down Time (MDT) per year, as well as the maximum Mean Time To Repair (MTTR) as far as the availability of the service is concerned. Reference units for the Reliability attribute SHOULD be minutes per year for the MDT indicator, and seconds for the MTTR indicator.

5.8. Additional Attributes

The current version of this draft has proposed and defined a set of attributes that SHOULD be conveyed in a SLS template. Obviously, there may be a need for conveying additional information, and updated versions of this document should reflect such requirement as appropriate.

6. Examples of Instantiated SLS Templates

6.1. SLS for a Virtual Leased Line Service

Let us assume the availability of a (unidirectional) Virtual Leased

Line (VLL) service offering, provided with a guaranteed throughput of

1 Mbit/s, a guaranteed one-way transit delay of 20 ms for a 10E-3 quantile, as well as a guaranteed packet loss rate of 0%.

Therefore, the value attributes of the corresponding SLS template will be the following:

- Scope = (1, 1)

- Flow ID = ((Set of) Source Addresses, (Set of) Destination Addresses, EF marking) - there may be several IP networks that may communicate through this virtual leased line, and all the IP traffic that will be conveyed by this VLL will be EF-marked.

- Traffic Conformance = (b, r, drop), where r = 1 Mbit/s (token bucket algorithm), and out-of-profile traffic will be dropped.

- Performance = (20 ms, 5 min, 10E-3, 0%), where delay = 20 ms, measured during a period of 5 minutes with an associated quantile of 10E-3, and with a 0% of packet loss rate (which implies that the throughput guarantee is identical to the token bucket rate r, hence 1 Mbit/s.

- Service Schedule = (24/24, 7/7) - for example.

- Reliability = (MTTR = 30 s) - for example.

In this example, it's worth mentioning that the throughput guarantee has been derived from the packet loss rate, the token bucket rate and the action to be taken for out-of-profile traffic (drop).

6.2. The Funnel Service

The Funnel service would aim at protecting local traffic (within an enterprise) from Internet traffic, such as HTTP. An example of such service is depicted in figure 2 below:

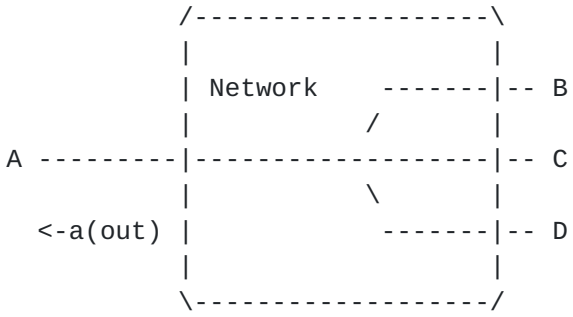

Fig. 2: Example of a Funnel Service.

In figure 2, customer A requires that the traffic entering his

network and coming from B, C or D, does not exceed the a(out) rate.

The attributes of the corresponding SLS would therefore be the following:

- Scope = (N, 1)

- Flow ID = (DSCP). The filter for incoming traffic will be applied on the DSCP marking.

- Traffic Conformance = (b, r, drop). The token bucket algorithm reflects the maximum allowed (incoming) throughput (r = a(out)) on the specified egress interface, as defined in the Scope attribute. Out-of-profile traffic will be dropped.

6.3. SLS for Best Effort Traffic

The attributes of a Best Effort (BE) SLS would be the following:

- Scope = all combinations that have been defined in section 5.1.2 of the document.

There would be no indication of the Flow ID attribute, nor the Traffic Conformance, nor the Performance attributes. Nevertheless, both the Service Schedule and the Reliability attributes MAY be valued.

7. SLS Negotiation Protocol Requirements

The information that is conveyed in SLS templates by means of specific attributes will be negotiated between the customer and the service provider parties. As such, this information will be exchanged thanks to a communication protocol, which SHOULD address the following requirements.

- The SLS negotiation protocol should use of a reliable transport mode, given the importance of the QoS information to be exchanged between the customer and the service provider,

- The protocol architecture should provide a means for a dynamic SLS negotiation and subscription procedure, so that it may introduce a high level of automation in the actual negotiation and invocation of the corresponding IP service offerings,

- The protocol should support a reporting mechanism that may be used for statistical information retrieval,

- The protocol should support the appropriate security mechanisms to provide some guarantees as far as the preservation of the confidentiality of the information contained in a SLS template is concerned.

8. Security Considerations

This draft has identified a set of information that will be exchanged between a customer and a service provider by means of a SLS template negotiation and instantiation procedure. As such, it raises the issue of the security associated to the provisioning of such information, by means of a protocol which should be able to address the requirements discussed in the previous section 7. In particular, the following security features SHOULD be considered:

- Identification and authentication of the requesting entity (a.k.a. the customer), if not both parties,

- Identification and authentication of the peering entities that will participate in the SLS negotiation process,

- Preservation of the confidentiality of the information to be exchanged between both parties during the SLS negotiation and instantiation procedures.

9. References

[1] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.
[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997
[3] Blake, S., et al., "An Architecture for Differentiated Services", RFC 2475, December 1998.
[4] Heinanen, J., et al., "Assured Forwarding PHB Group", RFC 2597, June 1999.
[5] Davie, B., et al., "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, March 2002.
[6] Grossman, D., "New Terminology and Clarifications for Diffserv", RFC 3260, April 2002.
[7] Nichols, K., Carpenter, B., "Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification", RFC 3086, April 2001.
[8] Simpson, W., et al., "The Point-to-Point Protocol (PPP)", RFC 1661, STD 0051, July 1994.
[9] Almes, G., Kalidindi, S., "A One-Way-Delay Metric for IPPM", RFC 2679, September 1999.
[10] Demichelis, C., Chimento, P., "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", RFC 3393, November 2002.
[11] Almes, G., et al., "One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

10. Acknowledgments

Part of this work has been funded by the European Commission, within

the context of the TEQUILA (Traffic Engineering for Quality of

Service in the Internet At Large Scale, www.ist-tequila.org) project, which was itself part of the IST (Information Society Technologies) research program.

The authors would also like to thank W. Almesberger, M. Brunner, S. De Cnodder, S. Salsano, A. Kamienski, as well as A. Malick for their useful comments and suggestions that have been sent on the sls@ist-tequila.org mailing list, and also during private conversations.

11. Authors' Addresses

Maarten Buchli
Alcatel Corporate Research Center
Fr. Wellesplein 1,
2018 Antwerpen
Belgium
Phone: +32 3 240 7081
Email: maarten.buchli@alcatel.be

Richard Egan
Thales Research and Technology Ltd.
Worton Drive
Worton Grange Industrial Estate
Reading, Berkshire RG2 OSB
United Kingdom
Phone: +44 118 923 8375
Email: richard.egan@thalesgroup.com

Panos Georgatsos
Algonet S.A.
206, Sygrou Avenue,
176 72 Kalithea
Athens
Greece
Phone: +30 210 955 8356
Email: pgeorgat@egreta.gr

Leonidas Georgiadis
Aristotel Univ. of Thessaloniki
PO Box 435, Thessaloniki, 54006,
Greece
Phone: +30 31 996385
Email: leonid@eng.auth.gr

Danny Goderis
Alcatel Corporate Research Center
Fr. Wellesplein 1,
2018 Antwerpen

Belgium
Phone: +32 3 240 7853
Email: Danny.Goderis@Alcatel.be

David Griffin
Department of Electronic and Electrical Engineering
University College London
Torrington Place, London WC1E 7JE
United Kingdom
Phone: +44 (0)20 7679 7606
Email: dgriffin@ee.ucl.ac.uk

Christian Jacquenet
France Telecom
3, avenue Fran ois Ch teau
CS 36901
35069 Rennes Cedex
France
Phone: +33 2 99 87 63 31
Email: christian.jacquenet@francetelecom.com

George Memenios
Algonet S.A.
206, Sygrou Avenue,
176 72 Kalithea
Athens
Greece
Phone: +30 210 955 8331
Email: memenios@egreta.gr

George Pavlou
Centre for Communication Systems Research (CCSR)
Univ. of Surrey, Guildford, Surrey GU2 7XH,
United Kingdom
Phone: +44 1483 689480
Email: G.Pavlou@eim.surrey.ac.uk

Olivier Poupel
Alcatel Research and Innovation
Route de Nozay
91461 Marcoussis
France
Phone: +33 1 69 63 47 07
Email: olivier.poupel@alcatel.fr

Yves T'Joens
Alcatel Corporate Research Center
Fr. Wellesplein 1, 2018 Antwerpen
Belgium
Phone: +32 3 240 7890
Email: Yves.TJoens@alcatel.be

Sven Van den Bosch
Alcatel Corporate Research Center

Fr. Wellesplein 1, 2018 Antwerpen
Belgium
Phone: +32 3 240 8103
Email: sven.van_den_bosch@alcatel.be

Full Copyright Statement