Network Working Group Lou Berger - Editor (Movaz Networks)
Internet Draft
Expiration Date: July 2004

January 2004

GMPLS - Communication of Alarm Information

draft-berger-ccamp-gmpls-alarm-spec-01.txt

Status of this Memo

Abstract

This document describes an extension to Generalized MPLS (Multi-Protocol Label Switching) signaling to support communication of alarm information. GMPLS signaling already supports the control of alarm reporting, but not the communication of alarm information. This document presents both a functional description and GMPLS-RSVP specifics of such an extension. This document also proposes modification of the RSVP ERROR_SPEC object.

Contents

1. Introduction

GMPLS Signaling provides mechanisms that can be used to control the reporting of alarms associated with an LSP. This support is provided via Administrative Status Information [RFC3471] and the Admin_Status object [RFC3473]. These mechanisms only control if alarm reporting is inhibited. No provision is made for communication of alarm information within GMPLS.

The extension described in this document defines how the alarm information associated with a GMPLS label-switched path (LSP) may be communicated along the path of the LSP. Communication both upstream and downstream is supported. The value in communicating such alarm information is that this information is then available at every node along the LSP for display and diagnostic purposes. Alarm information may also be useful in certain traffic protection scenarios, but such uses are out of scope of this document. Alarm communication is supported via a new object, new error/alarm information TLVs, and a new Administrative Status Information bit.

The communication of alarms, as described in this document, is controllable on a per LSP basis. Such communication may be useful within network configurations where not all nodes support communication to a user for reporting of alarms and/or communication is needed to support specific applications. The support of this functionality is optional.

The communication of alarms within GMPLS does not imply any modification in behavior of processing of alarms, or for the communication of alarms outside of GMPLS.

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 [RFC2119].

1.1. Background

Problems with data plane state can often be detected by associated data plane hardware components. Such data plane problems are typically filtered based on elapsed time and local policy. Problems that pass the filtering process are normally raised as alarms. These alarms are available for display to operators. They also may be collected centrally through means that are out of the scope of this document.

Not all data plane problems cause the LSP to be immediately torn down. Further, there may be a desire, particularly in optical

transport networks, to retain an LSP and communicate relevant alarm information even when the data plane state has failed completely.

Although error information can be reported using PathErr, ResvErr and Notify messages, these messages typically indicate a problem in signaling state and can only report one problem at at a time. This makes it hard to correlate all of the problems that may be associated with a single LSP and to allow an operator examining the status of an LSP to view a full list of current problems. This situation is exacerbated by the absence of any way to communicate that a problem has been resolved and a corresponding alarm cleared.

The extensions defined in this document allow an operator or a software component to obtain a full list of current alarms associated with all of the resources used to support an LSP. The extensions also ensure that this list is kept up-to-date and synchronized with the real alarm status in the network. Finally, the extensions make the list available at every node traversed by an LSP.

2. Alarm Information Communication

A new object is introduced to carry alarm information details. The details of alarm information are much like the error information carried in the existing ERROR_SPEC objects. For this reason the communication of alarm information uses a format that is based on the communication of error information.

The new object introduced to carry alarm information details is called an ALARM_SPEC object. This object has the same format as the ERROR_SPEC object, but uses a new C-Num to avoid the semantics of error processing. Also, additional TLVs are defined for the IF_ID ALARM_SPEC objects to support the communication of information related to a specific alarm. These TLVs may also be useful when included in ERROR_SPEC objects, e.g., when the ERROR_SPEC object is carried within a Notify message.

While the details of alarm information are like the details of existing error communication, the semantics of processing differ. Alarm information will typically relate to changes in data plane state, without changes in control state. Alarm information will always be associated with in-place LSPs. Such information will also typically be most useful to operators and applications other than control plane protocol processing. Finally, while error information is communicated within PathErr, ResvErr and Notify messages [RFC3473], alarm information will be carried within Path and Resv messages.

Path messages are used to carry alarm information to downstream nodes and Resv messages are used to carry alarm information to upstream nodes. The intent of sending alarm information both upstream and downstream is to provide the same visibility to alarm information at any point along an LSP. The communication of multiple alarms associated with an LSP is supported. In this case, multiple ALARM_SPEC objects will be carried in the Path or Resv messages.

The addition of alarm information to Path and Resv messages is controlled via a new Administrative Status Information bit. Administrative Status Information is carried in the Admin_Status object.

3. GMPLS-RSVP Details

This section provides the GMPLS-RSVP [RFC3473] specification for communication of alarm information. The communication of alarm information is optional. This section applies to nodes that support communication of alarm information.

3.1. ALARM_SPEC Objects

The ALARM_SPEC objects use the same format as the ERROR_SPEC object, but with class number of TBA (to be assigned by IANA in the form 11bbbbbb).

- IPv4 ALARM_SPEC object: Class = TBA, C-Type = 1
  Definition same as IPv4 ERROR_SPEC [RFC2205].

- IPv6 ALARM_SPEC object: Class = TBA, C-Type = 2
  Definition same as IPv6 ERROR_SPEC [RFC2205].

- IPv4 IF_ID ALARM_SPEC object: Class = TBA, C-Type = 3
  Definition same as IPv4 IF_ID ERROR_SPEC [RFC3473].

- IPv6 IF_ID ALARM_SPEC object: Class = TBA, C-Type = 4
  Definition same as IPv6 IF_ID ERROR_SPEC [RFC3473].

3.1.1. IF_ID ALARM_SPEC (and ERROR_SPEC) TLVs

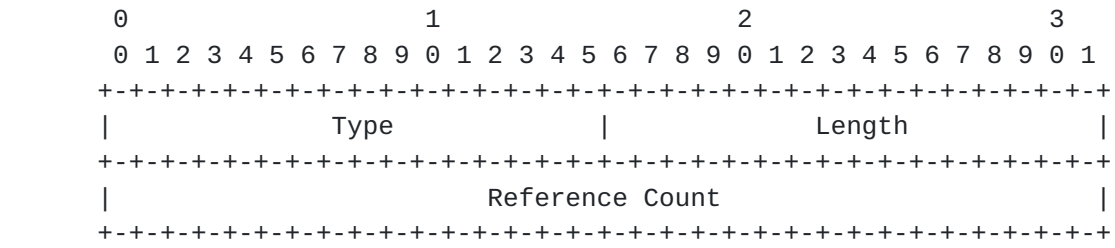
The following new TLVs are defined for use with the IPv4 and IPv6 IF_ID ALARM_SPEC objects. They may also be used with the IPv4 and IPv6 IF_ID ERROR_SPEC objects. See [RFC3471] section 9.1.1 for the original definition of these values. Note the length provided below is for the total TLV. All TLVs defined in this section are optional.

No rules apply to the relative ordering of these TLVs. These TLVs MUST be listed after any interface identifying TLVs.

[Note: Type values are TBA (to be assigned) by IANA]

Type	Length	Description
512	8	REFERENCE_COUNT
513	8	SEVERITY
514	8	GLOBAL_TIMESTAMP
515	8	LOCAL_TIMESTAMP
516	variable	ERROR_STRING

The Reference Count TLV has the following format:

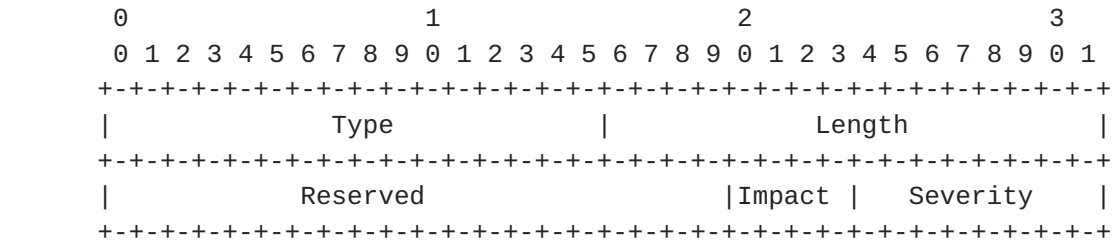


Reference Count: 32 bits

The number of times this alarm has been repeated. This field MUST NOT be set to zero.

Only one Reference Count TLV may be included in an object.

The Severity TLV has the following format:



Reserved: 24 bits

This field is reserved. It MUST be set to zero on generation and MUST be ignored on receipt.

Impact: 4 bits

Indicates the impact of the alarm indicated in the TLV. The following values are defined:

Value	Definition
0	Unspecified impact
1	Non-Service Affecting
2	Service Affecting

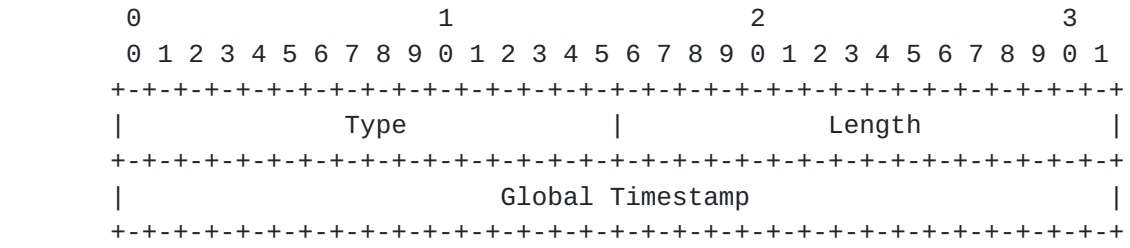
Severity: 8 bits

Indicates the impact of the alarm indicated in the TLV. The following values are defined:

Value	Definition
0	Reserved
1	Critical
2	Major
3	Minor
4	Warning

Only one Severity TLV may be included in an object.

The Global Timestamp TLV has the following format:

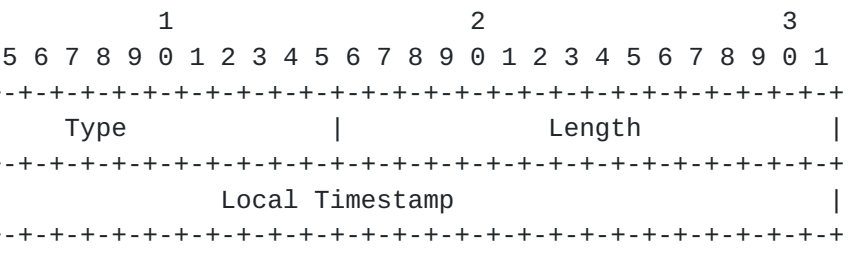


Global Timestamp: 32 bits

The number of seconds since 0000 UT on 1 January 1970, according to the clock on the node that originates this TLV.

Only one Global Timestamp TLV may be included in an object.

The Local Timestamp TLV has the following format:

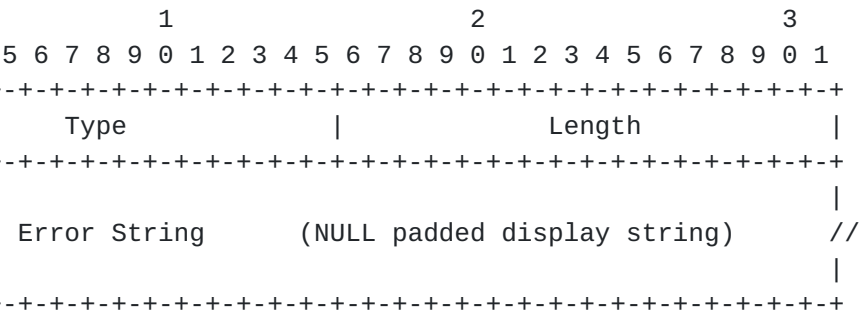


Local Timestamp: 32 bits

Number of seconds reported by the local system clock at the time the associated alarm was detected on the node that originates this TLV.

Only one Local Timestamp TLV may be included in an object.

The Error String TLV has the following format:



Error String: 32 bits minimum (variable)

A string of characters, representing the type of error/alarm. This string is padded to the next largest 4 byte boundary using null characters. Null padding is not required when the string is 32-bit aligned. The contents of error string are implementation dependent. See the condition types listed in Appendices of [GR833] for a list of example strings.

Multiple Error String TLVs may be included in an object.

3.1.2. Procedures

This section applies to nodes that support the communication of alarm information. ALARM_SPEC objects are carried in Path and Resv messages. Multiple ALARM_SPEC objects MAY be present. The IPv4 and IPv6 formats of the ALARM_SPEC object, C-Type 1 and 2, SHOULD NOT be used as they do not support the inclusion of the TLVs defined above.

Nodes that support the communication of alarm information, SHOULD record the information contained in a received ALARM_SPECs for later use. All ALARM_SPEC objects received in Path messages SHOULD be passed unmodified downstream in the corresponding Path messages. All ALARM_SPEC objects received in Resv messages SHOULD be passed unmodified upstream in the corresponding Resv messages. ALARM_SPEC objects are merged in transmitted Resv messages by including a copy of all ALARM_SPEC objects received in corresponding Resv Messages.

To advertise local alarm information, a node generates an ALARM_SPEC object for each alarm and adds it to both the Path and Resv messages for the affected LSP. The IPv4 or IPv6 IF_ID ALARM_SPEC object format SHOULD be used. In all cases, appropriate Error Node Address, Error Code and Error Values MUST be set, see below for a discussion on Error Code and Error Values. The InPlace and NotGuilty flags SHOULD NOT be set. When the IPv4 or IPv6 IF_ID ALARM_SPEC object format is used, TLVs SHOULD be included to identify the interface, if any, the severity, the time and a brief string associated with the alarm. The reference count TLV MAY also be included. ALARM_SPEC objects received from other nodes are not effected by the addition of local ALARM_SPEC objects, i.e., they continue to be processed as described above. The choice of which alarm or alarms to advertise and which to omit is a local policy matter, and may configurable by the user.

Note, ALARM_SPEC objects SHOULD NOT be added to LSPs that are in "alarm communication inhibited." ALARM_SPEC objects MAY be added to LSPs that are "administratively down". These states are indicated by the I and A bits of the Admin_Status object, see Section 3.2.

To remove local alarm information, a node simply removes the matching locally generated ALARM_SPEC objects from the outgoing Path and Resv messages. A node MAY modify a locally generated ALARM_SPEC object.

Normal refresh and trigger message processing applies to Path or Resv message that contain ALARM_SPEC objects. Note that changes in ALARM_SPEC objects from one message to the next may include a modification in the contents of a specific ALARM_SPEC object, or a change in the number of ALARM_SPEC objects present. All changes in ALARM_SPEC objects SHOULD be processed as trigger messages.

3.1.3. Error Codes and Values

The Error Codes and Values used in ALARM_SPEC objects are the same as those used in ERROR_SPEC objects. New Error Code values for use with both ERROR_SPEC and ALARM_SPEC objects may be assigned to support alarm types defined by other standards.

In this document we define one new Error Code. The Error Code uses the value TBA (by IANA) and is referred to as "Alarms". The values used in the Error Values field are the same as the values used for IANAItuProbableCause in the Alarm MIB [ALARM-MIB].

3.1.4. Backwards Compatibility

The support of ALARM_SPEC objects is optional. Non-supporting nodes will pass the objects through the node unmodified, because the ALARM_SPEC object has a C-Num of the form 11bbbbbb.

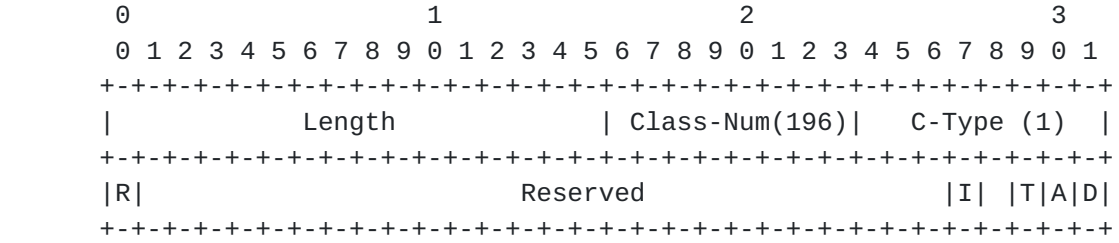
This allows alarm information to be collected and examined in a network built from a collection of nodes some of which support the communication of alarm information, and some of which do not.

3.2. Controlling Alarm Communication

Alarm information communication is controlled via Administrative Status Information as carried in the Admin_Status object. A new bit is defined, called the I bit, that indicates when alarm communication is to be inhibited. The definition of this bit does not modify the procedures defined in Section 7 of [RFC3473].

3.2.1. Updated Admin Status Object

The format of the Admin_Status object is updated to include the I bit:



Inhibit Alarm Communication (I): 1 bit
When set, indicates that alarm communication is disabled for the LSP and that nodes SHOULD NOT add local alarm information.

See [RFC3471] for the definition of the remaining bits.

3.2.2. Procedures

The I bit may be set and cleared using the procedures defined in Sections 7.2 and 7.3 of [RFC3473]. A node that receives (or generates) an Admin_Status object with the A and I bits set (1), SHOULD remove all locally generated alarm information from the matching LSP's outgoing Path and Resv messages. When a node receives (or generates) an Admin_Status object with the A and I bits clear (0), it should add any local alarm information to the matching LSP's outgoing Path and Resv messages. The processing of non-locally generated ALARM_SPEC objects MUST NOT be impacted by the contents of the Admin_Status object. Note, per [RFC3473], the absence of the Admin_Status object is equivalent to receiving an object containing values all set to zero (0).

When generating Notify messages for LSPs with the I bit set, the TLVs described in this document MAY be added to the ERROR_SPEC object sent in the the Notify message.

3.3. Message Formats

This section presents the RSVP message related formats as modified by this document. The formats specified in [RFC3473] served as the basis of these formats.

The format of a Path message is as follows:

```
<Path Message> ::=      <Common Header> [ <INTEGRITY> ]
                        [ [<MESSAGE_ID_ACK> | <MESSAGE_ID_NACK>] ... ]
                        [ <MESSAGE_ID> ]
                        <SESSION> <RSVP_HOP>
                        <TIME_VALUES>
                        [ <EXPLICIT_ROUTE> ]
                        <LABEL_REQUEST>
                        [ <PROTECTION> ]
                        [ <LABEL_SET> ... ]
                        [ <SESSION_ATTRIBUTE> ]
                        [ <NOTIFY_REQUEST> ]
                        [ <ADMIN_STATUS> ]
                        [ <POLICY_DATA> ... ]
                        [ <ALARM_SPEC> ... ]
                        <sender descriptor>
```

<sender descriptor> is not modified by this document.

The format of a Resv message is as follows:

```
<Resv Message> ::=      <Common Header> [ <INTEGRITY> ]
                        [ [<MESSAGE_ID_ACK> | <MESSAGE_ID_NACK>] ... ]
                        [ <MESSAGE_ID> ]
                        <SESSION> <RSVP_HOP>
                        <TIME_VALUES>
                        [ <RESV_CONFIRM> ]  [ <SCOPE> ]
                        [ <NOTIFY_REQUEST> ]
                        [ <ADMIN_STATUS> ]
                        [ <POLICY_DATA> ... ]
                        [ <ALARM_SPEC> ... ]
                        <STYLE> <flow descriptor list>
```

<flow descriptor list> is not modified by this document.

3.4. Relationship to GMPLS UNI

[GMPLS-UNI] defines how GMPLS may be used in an overlay model to provide a user-to-network interface. In this model, restrictions may be applied to the information that is signaled between an edge-node and a core-node. This restriction allows the core network to limit the information that is visible outside of the core. This restriction may be made for confidentiality, privacy or security reasons. It may also be made for operational reasons, for example if the information is only applicable within the core network.

The extensions described in this document are candidates for filtering as described in [GMPLS-UNI]. In particular the following observations apply.

- An ingress or egress core-node MAY filter alarms from the GMPLS core to the overlay UNI LSP. This may be to protect information about the core network, or to indicate that the core network is performing or has completed recovery actions for the GMPLS LSP.

- An ingress or egress core-node MAY modify alarms from the GMPLS core when sending to the overlay UNI LSP. This may facilitate the UNI client's ability to understand the failure and its effect on the data plane, and enable the UNI client to take corrective actions in a more-appropriate manner.

- Similarly, an egress core-node MAY choose to not request alarm reporting on Path messages that it sends downstream to the overlay network.

- Further, even when alarm reporting is requested along the whole length of an overlay LSP, an ingress or egress core-node MAY choose to selectively filter alarms that are reported to the overlay network. This may be to protect information about the core network, or may reflect the fact that the core network intends to take remedial action and does not want the overlay network to operate on the alarm information.

3.5. Relationship to GMPLS E-NNI

GMPLS may be used at the external network-to-network (E-NNI) interface, see [GMPLS-ASON]. At this interface, restrictions may be applied to the information that is signaled between an egress and an ingress core- node.

This restriction allows the ingress core network to limit the information that is visible outside of its core network. This restriction may be made for confidentiality, privacy or security reasons. It may also be made for operational reasons, for example if the information is only applicable within the core network.

The extensions described in this document are candidates for filtering as described in [GMPLS-ASON]. In particular the following observations apply.

- An ingress or egress core-node MAY filter internal core network alarms. This may be to protect information about the internal network, or to indicate that the core network is performing or has completed recovery

actions for this LSP.

- An ingress or egress core-node MAY modify internal core network alarms. This may facilitate the peering E-NNI (i.e. the egress core-node) to understand the failure and its effect on the data plane, and take corrective actions in a more-appropriate manner or prolong the generated alarms upstream/downstream as appropriated.

- Similarly, an egress/ingress core-node MAY choose to not request alarm reporting on Path messages that it sends downstream.

- Further, even when alarm reporting is requested along the whole length of an end-to-end LSP, an egress or an ingress core-node MAY choose to selectively filter alarms that are reported through the UNI. This may be to protect information about the whole core network, or may reflect the fact that the core network intends to take remedial action and does not want the overlay network to operate on the alarm information.

4. Security Considerations

Some operators may consider alarm information as sensitive. To support environments where this is the case, implementations SHOULD allow the user to disable the generation of ALARM_SPEC objects.

This document introduces no additional security considerations. See [RFC3473] for relevant security considerations.

5. IANA Considerations

IANA is requested to administer assignment of new values for namespaces defined in this document. This section uses the terminology of BCP 26 "Guidelines for Writing an IANA Considerations Section in RFCs" [BCP26].

This document defines a new RSVP "ALARM_SPEC object" with a Class-Num of the form 11bbbbbb. The value 197 is suggested. The C-type values associated with this object should read "Same values as ERROR_SPEC (C-Num 6)". The text associated with ALARM_SPEC object should also read "The ALARM_SPEC object uses the Error Code and Values from the ERROR_SPEC object."

Additionally, Section 3.1.3 defines a new Error Code. The Error Code is "Alarms" and uses Error Values defined in the Alarm MIB [ALARM-MIB]. The suggested Error code value is 28.

This document also defines the TLVs for use with the IF_ID ERROR_SPEC objects defined in [RFC3473]. Please see Section 3.1.1 for a list of TLV description and (suggested) type values.

Note that the type values are not sequential with existing ERROR_SPEC object TLV assignments. This is intentional and is intended to provide space for future error TLVs.

This document also defines the I bit in the Admin Status Object, see Section 3.2.1. This bit field was originally defined in Section 7.1 of [RFC3473]. We recommend that IANA being managing assignment of bits in the Admin Status Object, and that the bits be allocated through IETF Consensus actions.

6. Intellectual Property Considerations

This section is taken from Section 10.4 of [RFC2026].

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

7. References

7.1. Normative References

[RFC3471] Berger, L., Editor, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, January 2003.

[RFC3473] Berger, L., Editor, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling - Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[ALARM-MIB] Chisholm, S., Romascanu, D., "Alarm MIB", draft-ietf-disman-alarm-mib-17.txt, December 2003.

7.2. Informative References

[GR833] Bellcore, "Network Maintenance: Network Element and Transport Surveillance Messages" (GR-833-CORE), Issue 3, February 1999.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119.

[GMPLS-UNI] Swallow, G., Drake, J., Ishimatsu, H., and Rekhter, Y. "GMPLS UNI: RSVP Support for the Overlay Model", draft-ietf-ccamp-gmpls-overlay-02.txt, October 2003, work in progress.

[GMPLS-ENNI] Papadimitriou, D., Editor, "Generalized MPLS (GMPLS) RSVP-TE Signaling in support of Automatically Switched Optical Network (ASON)", draft-ietf-ccamp-gmpls-rsvp-te-ason-01.txt, January 2004, work in progress.

8. Contributors

Contributors are listed in alphabetical order:

Lou Berger
Movaz Networks, Inc.
7926 Jones Branch Drive
Suite 615
McLean VA, 22102
Phone: +1 703 847-1801
Email: lberger@movaz.com

Deborah Brungard
AT&T Labs, Room MT D1-3C22
200 Laurel Avenue

Middletown, NJ 07748, USA
Phone: (732) 420-1573
Email: dbrungard@att.com

Igor Bryskin
Movaz Networks, Inc.
7926 Jones Branch Drive
Suite 615
McLean VA, 22102
Email: ibryskin@movaz.com

Adrian Farrel
Old Dog Consulting

Phone: +44 (0) 1978 860944
Email: adrian@olddog.co.uk

Dimitri Papadimitriou (Alcatel)
Francis Wellesplein 1
B-2018 Antwerpen, Belgium

Phone: +32 3 240-8491
Email: dimitri.papadimitriou@alcatel.be

Arun Satyanarayana
Movaz Networks, Inc.
7926 Jones Branch Drive
Suite 615
McLean VA, 22102
Phone: +1 703 847-1785
Email: aruns@movaz.com

9. Contact Address

Lou Berger
Movaz Networks, Inc.
7926 Jones Branch Drive
Suite 615
McLean VA, 22102
Phone: +1 703 847-1801
Email: lberger@movaz.com

10. Full Copyright Statement

Generated on: Fri Jan 30 09:45:03 2004