                       GMPLS RSVP-TE Extensions for
        Operations, Administration, and Maintenance (OAM) Configuration

Abstract

   Operations, Administration, and Maintenance (OAM) is an integral part
   of transport connections; hence, it is required that OAM functions be
   activated/deactivated in sync with connection commissioning/
   decommissioning, in order to avoid spurious alarms and ensure
   consistent operation. In certain technologies, OAM entities are
   inherently established once the connection is set up, while other
   technologies require extra configuration to establish and configure
   OAM entities. This document specifies extensions to Resource
   Reservation Protocol - Traffic Engineering (RSVP-TE) to support the
   establishment and configuration of OAM entities along with Label
   Switched Path signaling.

Copyright Notice

   Copyright (c) 2014 IETF Trust and the persons identified as the
   document authors. All rights reserved.

   This document is subject to BCP 78 and the IETF Trust's Legal
   Provisions Relating to IETF Documents
   (http://trustee.ietf.org/license-info) in effect on the date of
   publication of this document. Please review these documents
   carefully, as they describe your rights and restrictions with respect
   to this document. Code Components extracted from this document must
   include Simplified BSD License text as described in Section 4.e of
   the Trust Legal Provisions and are provided without warranty as
   described in the Simplified BSD License.

Table of Contents

1. Introduction

   GMPLS is designed as an out-of-band control plane supporting dynamic
   connection provisioning for any suitable data-plane technology,
   including spatial switching (e.g., incoming port or fiber to outgoing
   port or fiber); wavelength-division multiplexing (e.g., Dense
   Wavelength Division Multiplexing (DWDM)); time-division multiplexing
   (e.g., Synchronous Optical Networking and Synchronous Digital
   Hierarchy (SONET/SDH), G.709); and Ethernet Provider Backbone
   Bridging - Traffic Engineering (PBB-TE) and MPLS. In most of these
   technologies, there are Operations, Administration, and Maintenance
   (OAM) functions employed to monitor the health and performance of the
   connections and to trigger data plane (DP) recovery mechanisms.
   Similar to connection provisioning, OAM functions follow general
   principles but also have some technology-specific characteristics.

   OAM is an integral part of transport connections. Therefore, it is
   required that OAM functions be activated/deactivated in sync with
   connection commissioning/decommissioning, in order to avoid spurious
   alarms and ensure consistent operation. In certain technologies, OAM
   entities are inherently established once the connection is set up,
   while other technologies require extra configuration to establish and
   configure OAM entities. In some situations, the use of OAM
   functions, such as Fault Management (FM) and Performance Management
   (PM), may be optional (based on network management policies). Hence,
   the network operator must be able to choose which set of OAM
   functions to apply to specific connections and which parameters
   should be configured and activated. To achieve this objective, OAM
   entities and specific functions must be selectively configurable.

   In general, it is required that the management-plane and
   control-plane connection establishment mechanisms be synchronized
   with OAM establishment and activation. In particular, if the GMPLS
   control plane is employed, it is desirable to bind OAM setup and
   configuration to connection establishment signaling to avoid two
   separate management/configuration steps (connection setup followed by
   OAM configuration), as these separate steps increase delay and
   processing time; more importantly, they may be prone to
   misconfiguration errors. Once OAM entities are set up and
   configured, proactive as well as on-demand OAM functions can be
   activated via the management plane. On the other hand, it should be
   possible to activate/deactivate proactive OAM functions via the GMPLS
   control plane as well. In some situations, it may be possible to use
   the GMPLS control plane to control on-demand OAM functions too.

This document describes requirements for OAM configuration and
control via Resource Reservation Protocol - Traffic Engineering
(RSVP-TE). Extensions to the RSVP-TE protocol are specified,
providing a framework to configure and control OAM entities along
with the capability to carry technology-specific information.
Extensions can be grouped into generic elements that are applicable
to any OAM solution and technology-specific elements that provide
additional configuration parameters that may only be needed for
a specific OAM technology. This document specifies the technology-
agnostic elements and specifies the way that additional
technology-specific OAM parameters are provided. This document
addresses end-to-end OAM configuration, that is, the setup of OAM
entities bound to an end-to-end Label Switched Path (LSP), and
configuration and control of OAM functions running end-to-end in the
LSP. Configuration of OAM entities for LSP segments and tandem
connections is outside the scope of this document.

The mechanisms described in this document provide an additional
option for bootstrapping OAM that is not intended to replace or
deprecate the use of other technology-specific OAM bootstrapping
techniques, e.g., LSP ping [RFC4379] for MPLS networks. The
procedures specified in this document are intended only for use in
environments where RSVP-TE signaling is used to set up the LSPs that
are to be monitored using OAM.

1.1. Requirements Language

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].

2. Technology-Specific OAM Requirements

This section summarizes various technology-specific OAM requirements
that can be used as a basis for an OAM configuration framework.

MPLS OAM requirements are described in [RFC4377], which provides
requirements to create consistent OAM functionality for MPLS
networks. The following list is an excerpt of MPLS OAM requirements
documented in [RFC4377] that bear direct relevance to the discussion
set forth in this document:

o It is desired that the automation of LSP defect detection be
   supported. It is especially important in cases where large
   numbers of LSPs might be tested.

o In particular, some LSPs may require automated testing
   functionality from the ingress LSR (Label Switching Router) to the
   egress LSR, while others may not.

o Mechanisms are required to coordinate network responses to
   defects. Such mechanisms may include alarm suppression,
   translating defect signals at technology boundaries, and
   synchronizing defect detection times by setting appropriately
   bounded detection time frames.

The MPLS Transport Profile (MPLS-TP) defines a profile of MPLS
targeted at transport applications [RFC5921]. This profile specifies
the specific MPLS characteristics and extensions required to meet
transport requirements, including providing additional OAM,
survivability, and other maintenance functions not currently
supported by MPLS. Specific OAM requirements for MPLS-TP are
specified in [RFC5654] and [RFC5860]. MPLS-TP poses the following
requirements on the control plane to configure and control OAM
entities:

o From [RFC5860]: OAM functions MUST operate and be configurable
   even in the absence of a control plane. Conversely, it SHOULD be
   possible to configure as well as enable/disable the capability to
   operate OAM functions as part of connectivity management, and it
   SHOULD also be possible to configure as well as enable/disable the
   capability to operate OAM functions after connectivity has been
   established.

o From [RFC5654]: The MPLS-TP control plane MUST support the
   configuration and modification of OAM maintenance points as well
   as the activation/deactivation of OAM when the transport path or
   transport service is established or modified.

Ethernet Connectivity Fault Management (CFM) defines an adjunct OAM
flow that monitors connectivity in order to check the liveliness of
Ethernet networks [IEEE.802.1Q-2011]. With PBB-TE
[IEEE.802.1Q-2011], Ethernet networks support explicitly routed
Ethernet connections. CFM can be used to track the liveliness of
PBB-TE connections and detect data-plane failures. In the IETF, the
GMPLS Ethernet Label Switching (GELS) (see [RFC5828] and [RFC6060])
work extended the GMPLS control plane to support the establishment of
PBB-TE data-plane connections. Without control-plane support,
separate management commands would be needed to configure and
start CFM.

GMPLS-based OAM configuration and control need to provide a general
framework to be applicable to a wide range of data-plane technologies
and OAM solutions. There are three typical data-plane technologies

used for transport applications: wavelength based, such as Wavelength
Switched Optical Networks (WSON); Time-Division Multiplexing (TDM)
based, such as Synchronous Digital Hierarchy (SDH) and Synchronous
Optical Networking (SONET); and packet based, such as MPLS-TP
[RFC5921] and Ethernet PBB-TE [IEEE.802.1Q-2011]. For all these data
planes, the operator MUST be able to configure and control the
following OAM functions:

o It MUST be possible to explicitly request the setup of OAM
   entities for the signaled LSP and provide specific information for
   the setup if this is required by the technology.

o Control of alarms is important to avoid false alarm indications
   and reporting to the management system. It MUST be possible to
   enable/disable alarms generated by OAM functions. In some cases,
   selective alarm control may be desirable when, for instance, the
   operator is only concerned about critical alarms. Therefore,
   alarms that do not affect service should be inhibited.

o When periodic messages are used for liveliness checks (Continuity
   Checks (CCs)) of LSPs, it MUST be possible to set the frequency of
   messages. This allows proper configuration for fulfilling the
   requirements of the service and/or meeting the detection time
   boundaries posed by possible congruent connectivity-check
   operations of higher-layer applications. For a network operator
   to be able to balance the trade-off between fast failure detection
   and data overhead, it is beneficial to configure the frequency of
   CC messages on a per-LSP basis.

o Proactive Performance Monitoring (PM) functions are used to
   continuously collect information about specific characteristics of
   the connection. For consistent measurement of Service Level
   Agreements (SLAs), it MUST be possible to set common configuration
   parameters for the LSP.

o The extensions MUST allow the operator to use only a minimal set
   of OAM configuration and control features if supported by the OAM
   solution or network management policy. Generic OAM parameters, as
   well as parameters specific to data-plane technology or OAM
   technology, MUST be supported.

3. RSVP-TE-Based OAM Configuration

   In general, two types of maintenance points can be distinguished:
   Maintenance Entity Group End Points (MEPs) and Maintenance Entity
   Group Intermediate Points (MIPs). MEPs reside at the ends of an LSP
   and are capable of initiating and terminating OAM messages for Fault
   Management (FM) and Performance Monitoring (PM). MIPs, on the other

hand, are located at transit nodes of an LSP and are capable of
reacting to some OAM messages but otherwise do not initiate messages.
"Maintenance Entity" (ME) refers to an association of MEPs and MIPs
that are provisioned to monitor an LSP.

When an LSP is signaled, a forwarding association is established
between endpoints and transit nodes via label bindings. This
association creates a context for the OAM entities monitoring the
LSP. On top of this association, OAM entities may be configured to
unambiguously identify MEs.

In addition to ME identification parameters, proactive OAM functions
(e.g., CC and PM) may have additional parameters that require
configuration as well. In particular, the frequency of periodic CC
packets, and the measurement interval for loss and delay
measurements, may need to be configured.

The above parameters may be derived from information related to LSP
provisioning; alternatively, pre-configured default values can be
used. In the simplest case, the control plane MAY provide
information on whether or not OAM entities need to be set up for the
signaled LSP. If OAM entities are created, control-plane signaling
MUST also provide a means to activate/deactivate OAM message flows
and associated alarms.

OAM identifiers, as well as the configuration of OAM functions, are
technology specific (i.e., they vary, depending on the data-plane
technology and the chosen OAM solution). In addition, for any given
data-plane technology, a set of OAM solutions may be applicable.
Therefore, the OAM configuration framework allows selecting a
specific OAM solution to be used for the signaled LSP and provides
means to carry detailed OAM configuration information in technology-
specific TLVs.

Administrative Status Information is carried in the Admin_Status
object. Administrative Status Information is described in [RFC3471],
and the Admin_Status object is specified for RSVP-TE in [RFC3473].
Two bits are allocated for the administrative control of OAM
monitoring: the "OAM Flows Enabled" (M) and "OAM Alarms Enabled" (O)
bits. When the "OAM Flows Enabled" bit is set, OAM mechanisms MUST
be enabled; if it is cleared, OAM mechanisms MUST be disabled. When
the "OAM Alarms Enabled" bit is set, OAM-triggered alarms are enabled
and associated consequent actions MUST be executed, including the
notification to the management system. When this bit is cleared,
alarms are suppressed and no action SHOULD be executed, and the
management system SHOULD NOT be notified.

The LSP_ATTRIBUTES and LSP_REQUIRED_ATTRIBUTES objects are defined in
[RFC5420] to provide means to signal LSP attributes and options in
the form of TLVs. Options and attributes signaled in the
LSP_ATTRIBUTES object can be passed transparently through LSRs not
supporting a particular option or attribute, while the contents of
the LSP_REQUIRED_ATTRIBUTES object MUST be examined and processed by
each LSR. The "OAM MEP entities desired" bit is allocated in the
Attribute Flags TLV [RFC5420] to be used in the LSP_ATTRIBUTES
object. If the "OAM MEP entities desired" bit is set, it indicates
that the establishment of OAM MEP entities is required at the
endpoints of the signaled LSP. The "OAM MIP entities desired" bit is
allocated in the Attribute Flags TLV to be used in the LSP_ATTRIBUTES
or LSP_REQUIRED_ATTRIBUTES objects. If the "OAM MIP entities
desired" bit is set in the Attribute Flags TLV in the
LSP_REQUIRED_ATTRIBUTES object, it indicates that the establishment
of OAM MIP entities is required at every transit node of the
signaled LSP.

3.1. Establishment of OAM Entities and Functions

In order to avoid spurious alarms, OAM functions should be set up and
enabled in the appropriate order. When using the GMPLS control plane
for both LSP establishment and enabling OAM functions on the LSPs,
the control of both processes is bound to RSVP-TE message exchanges.

An LSP may be signaled and established without OAM configuration
first, and OAM entities may be added later with a subsequent
re-signaling of the LSP. Alternatively, the LSP may be set up with
OAM entities with the first signaling of the LSP. The procedures
below apply to both cases.

Before initiating a Path message with OAM configuration information,
an initiating node MUST establish and configure the corresponding OAM
entities locally. But until the LSP is established, OAM source
functions MUST NOT start sending any OAM messages. In the case of
bidirectional connections, in addition to the OAM source function,
the initiator node MUST set up the OAM sink function and prepare it
to receive OAM messages. During this time the OAM alarms MUST be
suppressed (e.g., due to missing or unidentified OAM messages). To
achieve OAM alarm suppression, Path messages MUST be sent with the
"OAM Alarms Enabled" Admin_Status flag cleared.

When the Path message arrives at the receiver, the remote end MUST
establish and configure OAM entities according to the OAM information
provided in the Path message. If this is not possible, a PathErr
message SHOULD be sent, and neither the OAM entities nor the LSP
SHOULD be established. If OAM entities are established successfully,
the OAM sink function MUST be prepared to receive OAM messages but

MUST NOT generate any OAM alarms (e.g., due to missing or
unidentified OAM messages). In the case of bidirectional
connections, in addition to the OAM sink function, an OAM source
function MUST be set up and, according to the requested
configuration, the OAM source function MUST start sending OAM
messages. A Resv message MUST then be sent back, including the
Attribute Flags TLV, with the appropriate setting of the "OAM MEP
entities desired" and "OAM MIP entities desired" flags, and the OAM
Configuration TLV that corresponds to the established and configured
OAM entities and functions. Depending on the OAM technology, some
elements of the OAM Configuration TLV MAY be updated/changed, i.e.,
if the remote end does not support a certain OAM configuration it may
suggest an alternative setting, which may or may not be accepted by
the initiator of the Path message. If it is accepted, the initiator
will reconfigure its OAM functions according to the information
received in the Resv message. If the alternate setting is not
acceptable, a ResvErr message MAY be sent, tearing down the LSP.
Details of this operation are technology specific and should be
described in accompanying technology-specific documents.

When the initiating side receives the Resv message, it completes any
pending OAM configuration and enables the OAM source function to send
OAM messages.

After this exchange, OAM entities are established and configured for
the LSP, and OAM messages are exchanged. OAM alarms can now be
enabled. During the period when OAM alarms are disabled, the
initiator sends a Path message with the "OAM Alarms Enabled"
Admin_Status flag set. The receiving node enables OAM alarms after
processing the Path message. The initiator enables OAM alarms after
it receives the Resv message. Data-plane OAM is now fully
functional.

If an egress LSR does not support the extensions defined in this
document, according to [RFC5420], it will silently ignore the new LSP
attribute flags as well as the TLVs carrying additional OAM
configuration information, and therefore no error will be raised that
would notify the ingress LSR about the missing OAM configuration
actions on the egress side. However, as described above, an egress
LSR conformant to the specification of this document will set the LSP
attribute flags and include the OAM Configuration TLV in the Resv
message indicating the configuration of the OAM mechanisms;
therefore, by detecting the missing information in the Resv message,
an ingress LSR will be able to recognize that the remote end does not
support the OAM configuration functionality, and therefore it SHOULD
tear down the LSP and, if appropriate, signal the LSP without any OAM
configuration information.

3.2. Adjustment of OAM Parameters

There may be a need to change the parameters of an already-
established and configured OAM function during the lifetime of the
LSP. To do so, the LSP needs to be re-signaled with the updated
parameters. OAM parameters influence the content and timing of OAM
messages and also identify the way that OAM defects and alarms are
derived and generated. Hence, to avoid spurious alarms, it is
important that both sides -- OAM sink and source -- are updated in a
synchronized way. First, the alarms of the OAM sink function should
be suppressed and only then should expected OAM parameters be
adjusted. Subsequently, the parameters of the OAM source function
can be updated. Finally, the alarms of the OAM sink side can be
enabled again.

In accordance with the above operation, the LSP MUST first be
re-signaled with the "OAM Alarms Enabled" Admin_Status flag cleared,
including the updated OAM Configuration TLV corresponding to the new
parameter settings. The initiator MUST keep its OAM sink and source
functions running unmodified, but it MUST suppress OAM alarms after
the updated Path message is sent. The receiver MUST first disable
all OAM alarms and then update the OAM parameters according to the
information in the Path message and reply with a Resv message
acknowledging the changes by including the OAM Configuration TLV.
Note that the receiving side can adjust the requested OAM
configuration parameters and reply with an updated OAM Configuration
TLV in the Resv message, reflecting the values that are actually
configured. However, in order to avoid an extensive negotiation
phase, in the case of adjusting already-configured OAM functions, the
receiving side SHOULD NOT update the parameters requested in the Path
message to an extent that would provide lower performance (e.g.,
lower frequency of monitoring packets) than what had previously been
in place.

The initiator MUST only update its OAM sink and source functions
after it receives the Resv message. After this Path/Resv message
exchange (in both unidirectional and bidirectional LSP cases), the
OAM parameters are updated, and OAM is running according to the new
parameter settings. However, OAM alarms are still disabled. A
subsequent Path/Resv message exchange with the "OAM Alarms Enabled"
Admin_Status flag set is needed to enable OAM alarms again.

3.3. Deleting OAM Entities

   In some cases, it may be useful to remove some or all OAM entities
   and functions from an LSP without actually tearing down the
   connection.

   To avoid any spurious alarms, first the LSP MUST be re-signaled with
   the "OAM Alarms Enabled" Admin_Status flag cleared but with OAM
   configuration unchanged. Subsequently, the LSP is re-signaled with
   "OAM MEP entities desired" and "OAM MIP entities desired" LSP
   attribute flags cleared, and without the OAM Configuration TLV, this
   MUST result in the deletion of all OAM entities associated with the
   LSP. All control-plane and data-plane resources in use by the OAM
   entities and functions SHOULD be freed up. Alternatively, if only
   some OAM functions need to be removed, the LSP is re-signaled with
   the updated OAM Configuration TLV. Changes between the contents of
   the previously signaled OAM Configuration TLV and the currently
   received TLV represent which functions MUST be removed/added.

   OAM source functions MUST be deleted first, and only after the "OAM
   Alarms Disabled" can the associated OAM sink functions be removed;
   this will ensure that OAM messages do not leak outside the LSP. To
   this end, the initiator, before sending the Path message, MUST remove
   the OAM source, hence terminating the OAM message flow associated to
   the downstream direction. In the case of a bidirectional connection,
   it MUST leave in place the OAM sink functions associated to the
   upstream direction. The remote end, after receiving the Path
   message, MUST remove all associated OAM entities and functions and
   reply with a Resv message without an OAM Configuration TLV. The
   initiator completely removes OAM entities and functions after the
   Resv message arrives.

4. RSVP-TE Extensions

4.1. LSP Attribute Flags

   In RSVP-TE, the Flags field of the SESSION_ATTRIBUTE object is used
   to indicate options and attributes of the LSP. The Flags field has
   8 bits and hence is limited to differentiate only 8 options.
   [RFC5420] defines new objects for RSVP-TE messages to allow the
   signaling of arbitrary attribute parameters, making RSVP-TE easily
   extensible to support new applications. Furthermore, [RFC5420]
   allows options and attributes that do not need to be acted on by all
   Label Switching Routers (LSRs) along the path of the LSP. In
   particular, these options and attributes may apply only to key LSRs
   on the path, such as the ingress LSR and egress LSR. Options and
   attributes can be signaled transparently and only examined at those
   points that need to act on them. The LSP_ATTRIBUTES and

LSP_REQUIRED_ATTRIBUTES objects are defined in [RFC5420] to provide
means to signal LSP attributes and options in the form of TLVs.
Options and attributes signaled in the LSP_ATTRIBUTES object can be
passed transparently through LSRs not supporting a particular option
or attribute, while the contents of the LSP_REQUIRED_ATTRIBUTES
object MUST be examined and processed by each LSR. One TLV is
defined in [RFC5420]: the Attribute Flags TLV.

One bit (bit number 10): "OAM MEP entities desired" is allocated in
the Attribute Flags TLV to be used in the LSP_ATTRIBUTES object. If
the "OAM MEP entities desired" bit is set, it indicates that the
establishment of OAM MEP entities is required at the endpoints of the
signaled LSP. If the establishment of MEPs is not supported, an
error MUST be generated: "OAM Problem/MEP establishment not
supported".

If the "OAM MEP entities desired" bit is set and additional
parameters need to be configured, an OAM Configuration TLV MAY be
included in the LSP_ATTRIBUTES or LSP_REQUIRED_ATTRIBUTES object.

One bit (bit number 11): "OAM MIP entities desired" is allocated in
the Attribute Flags TLV to be used in the LSP_ATTRIBUTES or
LSP_REQUIRED_ATTRIBUTES objects. If the "OAM MEP entities desired"
bit is not set, then this bit MUST NOT be set. If the "OAM MIP
entities desired" bit is set in the Attribute Flags TLV in the
LSP_REQUIRED_ATTRIBUTES object, it indicates that the establishment
of OAM MIP entities is required at every transit node of the signaled
LSP. If the establishment of a MIP is not supported, an error MUST
be generated: "OAM Problem/MIP establishment not supported". If an
intermediate LSR does not support the extensions defined in this
document, it will not recognize the "OAM MIP entities desired" flag
and, although the LSP_REQUIRED_ATTRIBUTES object was used, it will
not configure MIP entities and will not raise any errors. If LSRs
that do not support the extensions defined in this document are to be
assumed as present in the network, the ingress LSR SHOULD collect
per-hop information about the LSP attributes utilizing the LSP
Attributes sub-object of the Record Route object (RRO) as defined in
[RFC5420]. When the Record Route object is received, the ingress
SHOULD check whether all intermediate LSRs set the "OAM MIP entities
desired" flag indicating support of the function; if not, depending
on operator policy, the LSP MAY need to be torn down.

4.2. OAM Configuration TLV

   This TLV provides information about which OAM technology/method
   should be used and carries sub-TLVs for any additional OAM
   configuration information. One OAM Configuration TLV MAY be carried
   in the LSP_ATTRIBUTES or LSP_REQUIRED_ATTRIBUTES object in Path and
   Resv messages. When carried in the LSP_REQUIRED_ATTRIBUTES object,
   it indicates that intermediate nodes MUST recognize and react on the
   OAM configuration information.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |            Type (3)           |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    OAM Type   |                  Reserved                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   ~                            sub-TLVs                           ~
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
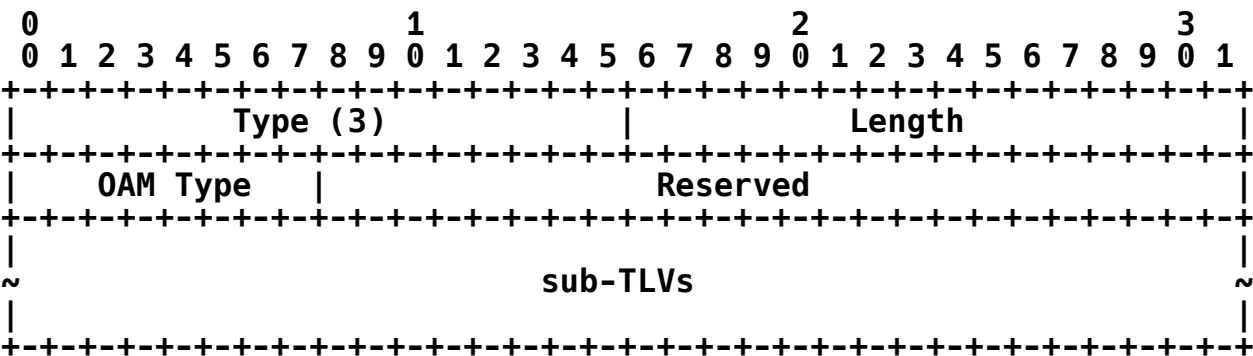
   Type: indicates a new type: the OAM Configuration TLV (3).

   OAM Type: specifies the technology-specific OAM method. When carried
   in the LSP_REQUIRED_ATTRIBUTES object, if the requested OAM method is
   not supported at any given node an error MUST be generated: "OAM
   Problem/Unsupported OAM Type". When carried in the LSP_ATTRIBUTES
   object, intermediate nodes not supporting the OAM Type pass the
   object forward unchanged as specified in [RFC5420]. Ingress and
   egress nodes that support the OAM Configuration TLV but that do not
   support a specific OAM Type MUST respond with an error indicating
   "OAM Problem/Unsupported OAM Type".

```
      OAM Type              Description
     ------------        --------------------
       0-255               Reserved
```

   This document defines no types. IANA maintains the values in a new
   "RSVP-TE OAM Configuration Registry".

   Length: indicates the total length of the TLV in octets. The TLV
   MUST be zero-padded so that the TLV is 4-octet aligned.

   Two groups of TLVs are defined: generic sub-TLVs and technology-
   specific sub-TLVs. Generic sub-TLVs carry information that is
   applicable independent of the actual OAM technology, while
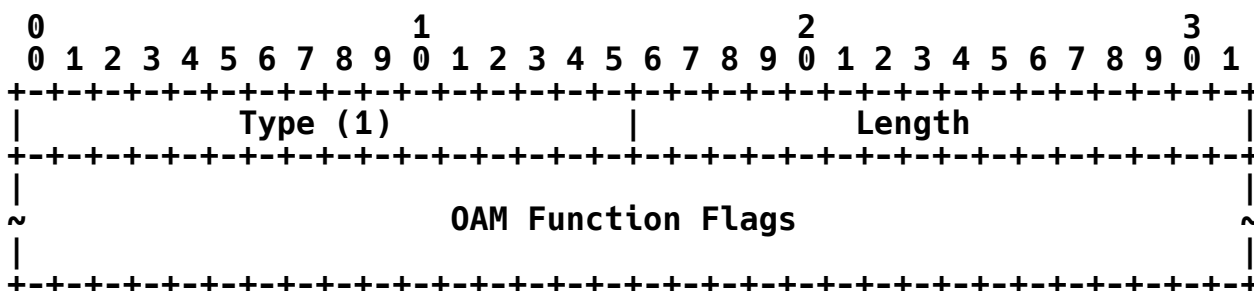   technology-specific sub-TLVs are providing configuration parameters

for specific OAM technologies. This document defines one generic
sub-TLV (see Section 4.2.1), while it is foreseen that technology-
specific sub-TLVs will be defined by separate documents.

The receiving node, based on the OAM Type, will check to see if a
corresponding technology-specific OAM configuration sub-TLV is
included in the OAM Configuration TLV. If the included technology-
specific OAM configuration sub-TLV is different from what is
specified in the OAM Type, an error MUST be generated: "OAM Problem/
OAM Type Mismatch". IANA maintains the sub-TLV space in the new
"RSVP-TE OAM Configuration Registry".

Note that there is a hierarchical dependency between the OAM
configuration elements. First, the "OAM MEP entities desired" flag
needs to be set. Only when that flag is set MAY an OAM Configuration
TLV be included in the LSP_ATTRIBUTES or LSP_REQUIRED_ATTRIBUTES
object. When this TLV is present, based on the "OAM Type" field, it
MAY carry a technology-specific OAM configuration sub-TLV. If this
hierarchy is broken (e.g., "OAM MEP entities desired" flag is not set
but an OAM Configuration TLV is present), an error MUST be generated:
"OAM Problem/Configuration Error".

4.2.1. OAM Function Flags Sub-TLV

The OAM Configuration TLV MUST always include a single instance of
the OAM Function Flags Sub-TLV, and it MUST always be the first
sub-TLV. "OAM Function Flags" specifies which proactive OAM
functions (e.g., connectivity monitoring, loss and delay measurement)
and which fault management signals MUST be established and
configured. If the selected OAM Function or Functions are not
supported, an error MUST be generated: "OAM Problem/Unsupported OAM
Function".

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type (1)          |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                     OAM Function Flags                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

OAM Function Flags is a bitmap with extensible length based on the
Length field of the TLV. Bits are numbered from left to right. The
TLV is padded to 4-octet alignment. The Length field indicates the
size of the padded TLV in octets. IANA maintains the OAM Function
Flags in the new "RSVP-TE OAM Configuration Registry". This document
defines the following flags:

```
OAM Function Flag bit #          Description
----------------------- --------------------------------------------
 0                               Continuity Check (CC)
 1                               Connectivity Verification (CV)
 2                               Fault Management Signal (FMS)
 3                               Performance Monitoring/Loss (PM/Loss)
 4                               Performance Monitoring/Delay (PM/Delay)
 5                               Performance Monitoring/Throughput Measurement
                                 (PM/Throughput)
```

4.2.2. Technology-Specific Sub-TLVs

If technology-specific configuration information is needed for a
specific "OAM Type", then this information is carried in a
technology-specific sub-TLV. Such sub-TLVs are OPTIONAL, and an OAM
Configuration TLV MUST NOT contain more than one technology-specific
sub-TLV. IANA maintains the OAM technology-specific sub-TLV space in
the new "RSVP-TE OAM Configuration Registry".

4.3. Administrative Status Information

Administrative Status Information is carried in the Admin_Status
object, which is specified for RSVP-TE in [RFC3473]. Administrative
Status Information is described in [RFC3471].

Two bits (bit numbers 23 and 24) are allocated by this document for
the administrative control of OAM monitoring: the "OAM Flows Enabled"
(M) and "OAM Alarms Enabled" (O) bits. When the "OAM Flows Enabled"
bit is set, OAM mechanisms MUST be enabled; if it is cleared, OAM
mechanisms MUST be disabled. When the "OAM Alarms Enabled" bit is
set, OAM-triggered alarms are enabled and associated consequent
actions MUST be executed, including the notification to the
management system. When this bit is cleared, alarms are suppressed,
and no action SHOULD be executed; additionally, the management system
SHOULD NOT be notified. For a detailed description of the use of
these flags, see Section 3.

4.4. Handling OAM Configuration Errors

To handle OAM configuration errors, a new Error Code "OAM Problem"
(40) is introduced. To refer to specific problems, a set of Error
Values are defined under the "OAM Problem" error code.

If a node does not support the establishment of OAM MEP or MIP
entities it MUST use the error value "MEP establishment not
supported" or "MIP establishment not supported", respectively, in the
PathErr message.

If a node does not support a specific OAM technology/solution, it
MUST use the error value "Unsupported OAM Type" in the PathErr
message.

If a different technology-specific OAM Configuration TLV is included
than what was specified in the OAM Type, an error MUST be generated
with error value "OAM Type Mismatch" in the PathErr message.

There is a hierarchy between the OAM configuration elements. If this
hierarchy is broken, the error value "Configuration Error" MUST be
used in the PathErr message.

If a node does not support a specific OAM Function, it MUST use the
error value "Unsupported OAM Function" in the PathErr message.

4.5. Considerations on Point-to-Multipoint OAM Configuration

RSVP-TE extensions for the establishment of point-to-multipoint
(P2MP) LSPs are specified in [RFC4875]. A P2MP LSP is comprised of
multiple source-to-leaf (S2L) sub-LSPs. These S2L sub-LSPs are set
up between the ingress and egress LSRs and are appropriately combined
by the branch LSRs using RSVP semantics to result in a P2MP TE LSP.
One Path message may signal one or multiple S2L sub-LSPs for a single
P2MP LSP. Hence, the S2L sub-LSPs belonging to a P2MP LSP can be
signaled using one Path message or split across multiple Path
messages.

P2MP OAM mechanisms are very specific to the data-plane technology;
therefore, in this document we only highlight the basic principles of
P2MP OAM configuration. We consider only the root-to-leaf OAM flows,
and as such, aspects of the configuration of return paths are outside
the scope of our discussions. We also limit our consideration to the
case where all leaves must successfully establish OAM entities with
identical configuration in order for the P2MP OAM to be successfully
established. In any case, the discussion set forth below provides

only guidelines for P2MP OAM configuration. However, at a minimum,
the procedures below SHOULD be specified for P2MP OAM configuration
in a technology-specific document.

The root node may use a single Path message or multiple Path messages
to set up the whole P2MP tree. In the case when multiple Path
messages are used, the root node is responsible for keeping the OAM
configuration information consistent in each of the sent Path
messages, i.e., the same information MUST be included in all Path
messages used to construct the multicast tree. Each branching node
will propagate the Path message downstream on each of the branches;
when constructing a Path message, the OAM configuration information
MUST be copied unchanged from the received Path message, including
the related Admin_Status bits, LSP attribute flags, and OAM
Configuration TLV. The latter two also imply that the LSP_ATTRIBUTES
and LSP_REQUIRED_ATTRIBUTES objects MUST be copied for the upstream
Path message to the subsequent downstream Path messages.

Leaves MUST create and configure OAM sink functions according to the
parameters received in the Path message; for P2MP OAM configuration,
there is no possibility for parameter negotiation on a per-leaf
basis. This is due to the fact that the OAM source function,
residing in the root of the tree, will operate with a single
configuration, which then must be obeyed by all leaves. If a leaf
cannot accept the OAM parameters, it MUST use the RRO Attributes
sub-object [RFC5420] to notify the root about the problem. In
particular, if the OAM configuration was successful, the leaf would
set the "OAM MEP entities desired" flag in the RRO Attributes
sub-object in the Resv message. On the other hand, if OAM entities
could not be established, the Resv message should be sent with the
"OAM MEP entities desired" bit cleared in the RRO Attributes
sub-object. Branching nodes should collect and merge the received
RROs according to the procedures described in [RFC4875]. This way,
the root, when receiving the Resv message (or messages if multiple
Path messages were used to set up the tree), will have clear
information about which of the leaves could establish the OAM
functions. If all leaves established OAM entities successfully, the
root can enable the OAM message flow. On the other hand, if at some
leaves the establishment was unsuccessful, additional actions will be
needed before the OAM message flow can be enabled. Such action could
be to set up two independent P2MP LSPs:

o One LSP with OAM configuration information towards leaves that can
   support the OAM function. This can be done by pruning from the
   previously signaled P2MP LSP the leaves that failed to set up OAM.

o The other P2MP LSP could be constructed for leaves without OAM
   entities.

The exact procedures will be described in technology-specific
documents.

5. IANA Considerations

5.1. Admin_Status Object Bit Flags

IANA maintains a registry called "Generalized Multi-Protocol Label
Switching (GMPLS) Signaling Parameters" with a sub-registry called
"Administrative Status Information Flags".

IANA has allocated two new flags as follows:

Bit Number	Hex Value	Name	Reference
23	0x00000100	OAM Flows Enabled (M)	[RFC7260]
24	0x00000080	OAM Alarms Enabled (O)	[RFC7260]

5.2. LSP Attribute Flags

IANA maintains a registry called "Resource Reservation Protocol-
Traffic Engineering (RSVP-TE) Parameters" with a sub-registry called
"Attribute Flags".

IANA has allocated two new flags as follows:

Bit No.	Name	Attribute Flags Path	Attribute Flags Resv	RRO	Reference
10	OAM MEP entities desired	Yes	Yes	Yes	[RFC7260]
11	OAM MIP entities desired	Yes	Yes	Yes	[RFC7260]

5.3. New LSP Attributes

IANA maintains a registry called "Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Parameters" with a sub-registry called "Attributes TLV Space".

IANA has allocated one new TLV type as follows:

Type	Name	Allowed on LSP_ATTRIBUTES	Allowed on LSP_REQUIRED_ATTRIBUTES	Reference
3	OAM Configuration TLV	Yes	Yes	[RFC7260]

5.4. RSVP Error Code

IANA maintains a registry called "Resource Reservation Protocol (RSVP) Parameters" with a sub-registry called "Error Codes and Globally-Defined Error Value Sub-Codes".

IANA has allocated one new Error Code as follows:

Error Code	Meaning	Reference
40	OAM Problem	[RFC7260]

The following Error Value sub-codes are defined for this new Error Code:

Value	Description	Reference
0	Reserved	[RFC7260]
1	MEP establishment not supported	[RFC7260]
2	MIP establishment not supported	[RFC7260]
3	Unsupported OAM Type	[RFC7260]
4	Configuration Error	[RFC7260]
5	OAM Type Mismatch	[RFC7260]
6	Unsupported OAM Function	[RFC7260]
7-32767	Unassigned	
32768-65535	Reserved for Private Use	[RFC7260]

5.5. RSVP-TE OAM Configuration Registry

   IANA has created a new registry called "RSVP-TE OAM Configuration
   Registry".

   IANA has created sub-registries as defined in the following
   subsections. The registration procedures specified are as defined in
   [RFC5226].

5.5.1. OAM Types Sub-Registry

   IANA has created the "OAM Types" sub-registry of the "RSVP-TE OAM
   Configuration Registry" as follows:

      Range | Registration Procedures
      ------+-------------------------
      0-255 | IETF Review

   There are no initial values in this registry. IANA shows the
   registry as follows:

      OAM Type Number | OAM Type Description | Reference
      ----------------+---------------------+--------------
       0-255 | Unassigned |

5.5.2. OAM Sub-TLVs Sub-Registry

   IANA has created the "OAM Sub-TLVs" sub-registry of the "RSVP-TE OAM
   Configuration Registry" as follows:

   Range | Note | Registration Procedures
   -------------+------------------------------+------------------------
   0-31 | Generic Sub-TLVs | IETF Review
   32-65534 | Technology-specific Sub-TLVs | IETF Review
   65535-65536 | Experimental Sub-TLVs | Reserved for
                | | Experimental Use

   IANA has populated the registry as follows:

      Sub-TLV Type | Description | Reference
      -------------+------------------------------+----------
          0 | Reserved | [RFC7260]
          1 | OAM Function Flags Sub-TLV | [RFC7260]
        2-65534 | Unassigned
      65535-65536 | Reserved for Experimental Use | [RFC7260]

5.5.3. OAM Function Flags Sub-Registry

   IANA has created the "OAM Function Flags Sub-Registry" sub-registry
   of the "RSVP-TE OAM Configuration Registry".

   New values in the registry are allocated by IETF Review [RFC5226].
   There is no top value to the range. Bits are counted from bit 0 as
   the first bit transmitted.

   IANA has populated the registry as follows:

   | OAM Function Flag | Description |
Bit Number	
0	Continuity Check (CC)
1	Connectivity Verification (CV)
2	Fault Management Signal (FMS)
3	Performance Monitoring/Loss (PM/Loss)
4	Performance Monitoring/Delay (PM/Delay)
5	Performance Monitoring/Throughput Measurement (PM/Throughput)
>=6	Unassigned

6. Security Considerations

   The signaling of OAM-related parameters and the automatic
   establishment of OAM entities based on RSVP-TE messages add a new
   aspect to the security considerations discussed in [RFC3473]. In
   particular, a network element could be overloaded if a remote
   attacker targeted that element by sending frequent periodic messages
   requesting liveliness monitoring of a high number of LSPs. Such an
   attack can efficiently be prevented when mechanisms for message
   integrity and node authentication are deployed. Since the OAM
   configuration extensions rely on the hop-by-hop exchange of exiting
   RSVP-TE messages, procedures specified for RSVP message security in
   [RFC2747] can be used to mitigate possible attacks.

   For a more comprehensive discussion of GMPLS security and attack
   mitigation techniques, please see the Security Framework for MPLS and
   GMPLS Networks [RFC5920].

7. Acknowledgements

   The authors would like to thank Francesco Fondelli, Adrian Farrel,
   Loa Andersson, Eric Gray, and Dimitri Papadimitriou for their useful
   comments.

8. References

8.1. Normative References

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119, March 1997.

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

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

[RFC5226]   Narten, T. and H. Alvestrand, "Guidelines for Writing an
            IANA Considerations Section in RFCs", BCP 26, RFC 5226,
            May 2008.

[RFC5420]   Farrel, A., Papadimitriou, D., Vasseur, JP., and A.
            Ayyangarps, "Encoding of Attributes for MPLS LSP
            Establishment Using Resource Reservation Protocol Traffic
            Engineering (RSVP-TE)", RFC 5420, February 2009.

8.2. Informative References

[IEEE.802.1Q-2011]
            IEEE, "IEEE Standard for Local and metropolitan area
            networks -- Media Access Control (MAC) Bridges and Virtual
            Bridged Local Area Networks", IEEE Std 802.1Q, 2011.

[RFC2747]   Baker, F., Lindell, B., and M. Talwar, "RSVP Cryptographic
            Authentication", RFC 2747, January 2000.

[RFC4377]   Nadeau, T., Morrow, M., Swallow, G., Allan, D., and S.
            Matsushima, "Operations and Management (OAM) Requirements
            for Multi-Protocol Label Switched (MPLS) Networks",
            RFC 4377, February 2006.

[RFC4379]   Kompella, K. and G. Swallow, "Detecting Multi-Protocol
            Label Switched (MPLS) Data Plane Failures", RFC 4379,
            February 2006.

[RFC4875]   Aggarwal, R., Papadimitriou, D., and S. Yasukawa,
            "Extensions to Resource Reservation Protocol - Traffic
            Engineering (RSVP-TE) for Point-to-Multipoint TE Label
            Switched Paths (LSPs)", RFC 4875, May 2007.

   [RFC5654] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N.,
              and S. Ueno, "Requirements of an MPLS Transport Profile",
              RFC 5654, September 2009.

   [RFC5828] Fedyk, D., Berger, L., and L. Andersson, "Generalized
              Multiprotocol Label Switching (GMPLS) Ethernet Label
              Switching Architecture and Framework", RFC 5828,
              March 2010.

   [RFC5860] Vigoureux, M., Ward, D., and M. Betts, "Requirements for
              Operations, Administration, and Maintenance (OAM) in MPLS
              Transport Networks", RFC 5860, May 2010.

   [RFC5920] Fang, L., "Security Framework for MPLS and GMPLS
              Networks", RFC 5920, July 2010.

   [RFC5921] Bocci, M., Bryant, S., Frost, D., Levrau, L., and L.
              Berger, "A Framework for MPLS in Transport Networks",
              RFC 5921, July 2010.

   [RFC6060] Fedyk, D., Shah, H., Bitar, N., and A. Takacs,
              "Generalized Multiprotocol Label Switching (GMPLS) Control
              of Ethernet Provider Backbone Traffic Engineering
              (PBB-TE)", RFC 6060, March 2011.

Authors' Addresses

    Attila Takacs
    Ericsson
    Konyves Kalman krt. 11.
    Budapest 1097
    Hungary

    EMail: attila.takacs@ericsson.com

    Don Fedyk
    Hewlett-Packard Company
    153 Taylor Street
    Littleton, MA 01460
    USA

    EMail: don.fedyk@hp.com

    Jia He
    Huawei
    PR China

    EMail: hejia@huawei.com