             Transparent Interconnection of Lots of Links (TRILL)
          Operations, Administration, and Maintenance (OAM) Framework

Abstract

   This document specifies a reference framework for Operations,
   Administration, and Maintenance (OAM) in Transparent Interconnection
   of Lots of Links (TRILL) networks. The focus of the document is on
   the fault and performance management aspects of TRILL OAM.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc7174.

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

   This document specifies a reference framework for Operations,
   Administration, and Maintenance (OAM) [RFC6291] in Transparent
   Interconnection of Lots of Links (TRILL) networks.

   TRILL [RFC6325] specifies a protocol for shortest-path frame routing
   in multi-hop networks with arbitrary topologies and link
   technologies, using the IS-IS routing protocol. TRILL capable
   devices are referred to as TRILL Switches or RBridges (Routing
   Bridges). RBridges provide an optimized and transparent Layer 2
   delivery service for Ethernet unicast and multicast traffic. Some
   characteristics of a TRILL network that are different from IEEE 802.1
   bridging are the following:

   - TRILL networks support arbitrary link technology between TRILL
      Switches. Hence, a TRILL Switch port may not have a 48-bit Media
      Access Control (MAC) address [802] but might, for example, have an
      IP address as an identifier [TRILL-IP] or no unique identifier
      (e.g., PPP [RFC6361]).

   - TRILL networks do not enforce congruence of unicast and multicast
      paths between a given pair of RBridges.

   - TRILL networks do not impose symmetry of the forward and reverse
      paths between a given pair of RBridges.

   - TRILL Switches terminate spanning tree protocols instead of
      propagating them.

   In this document, we refer to the term "OAM" as defined in [RFC6291].
   The Operations aspect involves finding problems that prevent proper
   functioning of the network. It also includes monitoring of the
   network to identify potential problems before they occur.
   Administration involves keeping track of network resources.
   Maintenance activities are focused on facilitating repairs and

upgrades as well as corrective and preventive measures.
[ISO/IEC7498-4] defines 5 functional areas in the OSI model for
network management, commonly referred to as FCAPS:

- Fault Management

- Configuration Management

- Accounting Management

- Performance Management

- Security Management

The focus of this document is on the first and fourth functional
aspects, Fault Management and Performance Management, in TRILL
networks. These primarily map to the Operations and Maintenance
parts of OAM.

This document provides a generic framework for a comprehensive
solution that meets the requirements outlined in [RFC6905]. However,
specific mechanisms to address these requirements are considered to
be outside the scope of this document. Furthermore, future
document(s) will specify the optional reporting of errors in TRILL
user traffic, such as the use of a reserved or unknown egress
nickname, etc.

1.1. Terminology

Definitions of many OAM terms can be found in [RFC7087].

The following acronyms are used in this document:

BFD - Bidirectional Forwarding Detection [RFC5880]

CFM - Connectivity Fault Management [802.1Q]

ECMP - Equal-Cost Multipath

FGL - Fine-Grained Label(ing) [RFC7172]

IEEE - Institute for Electrical and Electronic Engineers

IP - Internet Protocol (includes both IPv4 and IPv6)

LAN - Local Area Network

MA - Maintenance Association

MAC - Media Access Control [802]

ME - Maintenance Entity

MEP - Maintenance End Point

MIP - Maintenance Intermediate Point

MP - Maintenance Point (MEP or MIP)

OAM - Operations, Administration, and Maintenance [RFC6291]

PPP - Point-to-Point Protocol [RFC1661]

RBridge - Routing Bridge, a device implementing TRILL [RFC6325]

RDI - Reverse Defect Indication

TRILL - Transparent Interconnection of Lots of Links [RFC6325]

TRILL Switch - an alternate name for an RBridge

VLAN - Virtual LAN [802.1Q]

1.2. Relationship to Other OAM Work

   OAM is a technology area where a wealth of prior art exists. This
   document leverages concepts and draws upon elements defined and/or
   used in the following documents:

   - [RFC6905] defines the requirements for TRILL OAM that serve as the
      basis for this framework. It also defines terminology that is
      used extensively in this document.

   - [802.1Q] specifies the Connectivity Fault Management (CFM)
      protocol, which defines the concepts of Maintenance Domains,
      Maintenance End Points, and Maintenance Intermediate Points.

   - [Y.1731] extends Connectivity Fault Management in the following
      areas: it defines fault notification and alarm suppression
      functions for Ethernet. It also specifies mechanisms for Ethernet
      performance management, including loss, delay, jitter, and
      throughput measurement.

   - [RFC7175] defines a TRILL encapsulation for BFD that enables the
      use of the latter for network fast failure detection.

   - [RFC5860] and [RFC6371] specify requirements and a framework for
      OAM in MPLS-based networks.

2. TRILL OAM Model

2.1. OAM Layering

      In the TRILL architecture, the TRILL layer is independent of the
      underlying link-layer technology. Therefore, it is possible to
      run TRILL over any transport layer capable of carrying TRILL
      packets such as Ethernet [RFC6325], PPP [RFC6361], or IP
      [TRILL-IP]. Furthermore, TRILL provides a virtual Ethernet
      connectivity service that is transparent to higher-layer entities
      (Layer 3 and above). This strict layering is observed by TRILL
      OAM.

      Of particular interest is the layering of TRILL OAM with respect
      to:

   - BFD, which is typically used for fast failure detection.

   - Ethernet CFM [802.1Q] on paths from an external device, over a
      TRILL campus, to another external device, especially since TRILL
      Switches are likely to be deployed where existing 802.1 bridges
      can be such external devices.

   - Link OAM, on links interior to a TRILL campus, which is link-
      technology-specific.

   Consider the example network depicted in Figure 1 below, where a
   TRILL network is interconnected via Ethernet links:

```
                          LAN                LAN
           +---+   +---+  =====  +---+  ============  +---+
   +--+    |   |   |   |  | +--+ |   |  | +--+   +--+ |   |    +--+
   |B1|---|RB1|---|RB2|---|B2|---|RB3|---|B3|---|B4|---|RB4|---|B5|
   +--+    |   |   |   |  | +--+ |   |  | +--+   +--+ |   |    +--+
           +---+   +---+  =====  +---+  ============  +---+


    a. Ethernet CFM (Client Layer) on path over the TRILL campus
       >---o----------------------------------------------o---<


    b. TRILL OAM (Network Layer)
              >------o-----------o--------------------<


    c. Ethernet CFM (Transport Layer) on interior Ethernet LANs
                  >---o--o---<       >---o--o---o--o---<


    d. BFD (Media Independent Link Layer)
              #---#   #---------#   #----------------#


    e. Link OAM (Media Dependent Link Layer)
       *---*   *---*   *---*   *---*   *---*   *---*   *---*    *---*


    Legend:  >, < MEP     o MIP     # BFD Endpoint     * Link OAM Endpoint

                     Figure 1: OAM Layering in TRILL
```

   Where Bn and RBn (n= 1,2,3, ...) denote IEEE 802.1Q bridges and TRILL
   RBridges, respectively.

2.1.1. Relationship to CFM

   In the context of a TRILL network, CFM can be used as either a
   client-layer OAM or a transport-layer OAM mechanism.

   When acting as a client-layer OAM (see Figure 1a), CFM provides fault
   management capabilities for the user, on an end-to-end basis over the
   TRILL network. Edge ports of the TRILL network may be visible to CFM
   operations through the optional presence of a CFM Maintenance
   Intermediate Point (MIP) in the TRILL Switches' edge Ethernet ports.

   When acting as a transport-layer OAM (see Figure 1c), CFM provides
   fault management functions for the IEEE 802.1Q bridged LANs that may
   interconnect RBridges. Such bridged LANs can be used as TRILL level

links between RBridges. RBridges directly connected to the
intervening 802.1Q bridges may host CFM Down Maintenance End Points
(MEPs).

2.1.2. Relationship to BFD

One-hop BFD (see Figure 1d) runs between adjacent RBridges and
provides fast link as well as node failure detection capability
[RFC7175]. Note that TRILL BFD also provides some testing of the
TRILL protocol stack and thus sits a layer above Link OAM, which is
media specific. BFD's fast failure detection helps support rapid
convergence in TRILL networks. The requirements for BFD are
different from those of the TRILL OAM mechanisms that are the prime
focus of this document. Furthermore, BFD does not use the frame
format described in Section 3.1.

TRILL BFD differs from TRILL OAM in two significant ways:

1. A TRILL BFD transmitter is always bound to a specific TRILL
    output port.

2. TRILL BFD messages can be transmitted by the originator out of a
    port to a neighbor RBridge when the adjacency is in the Detect or
    2-Way states as well as when the adjacency is in the Report (Up)
    state [RFC7177].

In contrast, TRILL OAM messages are typically transmitted by
appearing to have been received on a TRILL input port (refer to
Section 2.2 for details). In that case, the output ports on which
TRILL OAM messages are sent are determined by the TRILL routing
function. The TRILL routing function will only send on links that
are in the Report state and have been incorporated into the local
view of the campus topology.

2.1.3. Relationship to Link OAM

Link OAM (see Figure 1e) depends on the nature of the technology used
in the links interconnecting RBridges. For example, for Ethernet
links, the OAM described in Clause 57 of [802.3] may be used.

2.2. TRILL OAM in the RBridge Port Model

TRILL OAM processing can be represented as a layer situated between
the port's TRILL encapsulation/decapsulation function and the TRILL
forwarding engine function on any RBridge port. TRILL OAM requires
services of the RBridge forwarding engine and utilizes information
from the IS-IS control plane. Figure 2 below depicts TRILL OAM

processing in the context of the RBridge Port Model defined in
[RFC6325]. In this figure, double lines represent flow of both
frames and information.

This figure shows a conceptual model. It is to be understood that
implementations need not mirror this exact model as long as the
intended OAM requirements and functionality are preserved.

```
              +-------------------------------------------+----
              |          (Flow of OAM Messages)      RBridge
              |      +---------------------+
              |      |+------------------+||  Forwarding Engine,
              |      ||                  ||  IS-IS, etc.
              |      ||                  ||  Processing of
              |      V                   V  TRILL packets
              +-------------------------------------------+-----
                     ||                   ||     ...other ports
                 +-----------+        +-----------+
UP MEP    /\ | TRILL OAM |        | TRILL OAM | /\ UP MEP
MIP       () |   Layer   |        |   Layer   | () MIP
DOWN MEP  \/ +-----------+        +-----------+ \/ DOWN MEP
             |   TRILL    |        |   TRILL    |
             | Encap/Decap|        | Encap/Decap|
             +-----------+        +-----------+
             |End-Station |        |End-Station |
             |VLAN &      |        |VLAN &      |
             |Priority    |        |Priority    |
             |Processing  |        |Processing  |
             +-----------+        +-----------+ <-- ISS
             |802.1/802.3 |        |802.1/802.3 |
             |Low-Level   |        |Low-Level   |
             |Control     |        |Control     |
             |Frame       |        |Frame       |
             |Processing, |        |Processing, |
             |Port/Link   |        |Port/Link   |
             |Control     |        |Control     |
             |Logic       |        |Logic       |
             +-----------+        +-----------+
             | 802.3PHY   |        | 802.3PHY   |
             |(Physical   |        |(Physical   |
             | interface) |        | interface) |
             +-----------+        +-----------+
                 ||                   ||
               Link                 Link
```

                Figure 2: TRILL OAM in RBridge Port Model

Note that the terms "MEP" and "MIP" in the above figure are explained
in detail in Section 2.6 below.

2.3. Network, Service, and Flow OAM

OAM functions in a TRILL network can be conducted at different
granularity. This gives rise to 'Network', 'Service', and 'Flow'
OAM, listed in order of finer granularity.

Network OAM mechanisms provide fault and performance management
functions in the context of a 'test' VLAN or fine-grained label
[RFC7172]. The test VLAN can be thought of as a management or
diagnostics VLAN that extends to all RBridges in a TRILL network. In
order to account for multipathing, Network OAM functions also make
use of test flows (both unicast and multicast) to provide coverage of
the various paths in the network.

Service OAM mechanisms provide fault and performance management
functions in the context of the actual VLAN or fine-grained label set
for which end-station service is enabled. Test flows are used here,
as well, to provide coverage in the case of multipathing.

Flow OAM mechanisms provide the most fine-grained fault and
performance management capabilities, where OAM functions are
performed in the context of end-station flows within VLANs or fine-
grained labels. While Flow OAM provides the most granular control,
it clearly poses scalability challenges if attempted on large numbers
of flows.

2.4. Maintenance Domains

The concept of Maintenance Domains, or OAM Domains, is well known in
the industry. IEEE [802.1Q] defines the notion of a Maintenance
Domain as a collection of devices (for example, network elements)
that are grouped for administrative and/or management purposes.
Maintenance Domains usually delineate trust relationships, varying
addressing schemes, network infrastructure capabilities, etc.

When mapped to TRILL, a Maintenance Domain is defined as a collection
of RBridges in a network for which connectivity faults and
performance degradation are to be managed by a single operator. All
RBridges in a given Maintenance Domain are, by definition, managed by
a single entity (for example, an enterprise or a data center
operator, etc.). [RFC6325] defines the operation of TRILL in a
single IS-IS area, with the assumption that a single operator manages
the network. In this context, a single (default) Maintenance Domain
is sufficient for TRILL OAM.

However, when considering scenarios where different TRILL networks
need to be interconnected, for example, as discussed in [TRILL-ML],
then the introduction of multiple Maintenance Domains, and
Maintenance Domain hierarchies, becomes useful to map and enforce
administrative boundaries. When considering multi-domain scenarios,
the following rules must be followed: TRILL OAM Domains must not
partially intersect but must either be disjoint or nest to form a
hierarchy (that is, a higher Maintenance Domain may completely
enclose a lower domain). A Maintenance Domain is typically
identified by a Domain Name and a Maintenance Level (a numeric
identifier). If two domains are nested, the encompassing domain must
be assigned a higher Maintenance Level number than the enclosed
domain. For this reason, the encompassing domain is commonly
referred to as the 'higher' domain, and the enclosed domain is
referred to as the 'lower' domain. OAM functions in the lower domain
are completely transparent to the higher domain. Furthermore, OAM
functions in the higher domain only have visibility to the boundary
of the lower domain (for example, an attempt to trace the path in the
higher domain will depict the entire lower domain as a single-hop
between the RBridges that constitute the boundary of that lower
domain). By the same token, OAM functions in the higher domain are
transparent to RBridges that are internal to the lower domain. The
hierarchical nesting of domains is established through operator
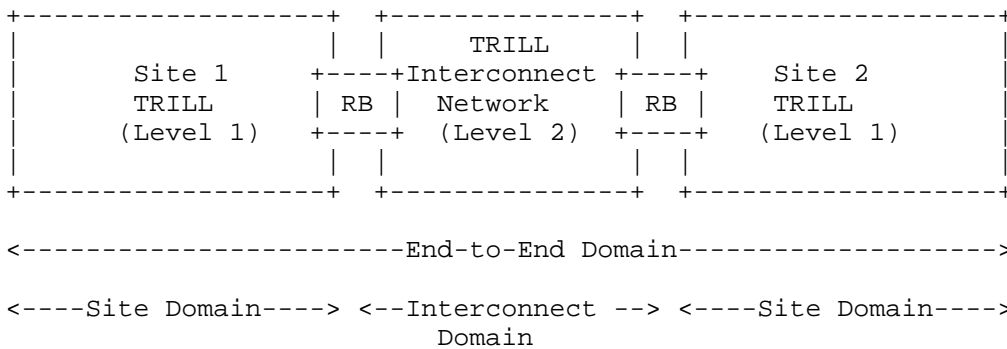configuration of the RBridges.

```
   +------------------+  +--------------+  +------------------+
   |                  |  |    TRILL     |  |                  |
   |     Site 1       +----+Interconnect +----+    Site 2      |
   |     TRILL        | RB |  Network     | RB |    TRILL      |
   |    (Level 1)     +----+ (Level 2)    +----+  (Level 1)    |
   |                  |  |              |  |                  |
   +------------------+  +--------------+  +------------------+

   <---------------------End-to-End Domain-------------------->

   <----Site Domain----> <--Interconnect --> <----Site Domain---->
                    Domain
```

Figure 3: TRILL OAM Maintenance Domains

2.5. Maintenance Entity and Maintenance Entity Group

TRILL OAM functions are performed in the context of logical endpoint
pairs referred to as Maintenance Entities (ME). A Maintenance Entity
defines a relationship between two points in a TRILL network where
OAM functions (for example, monitoring operations) are applied. The
two points that define a Maintenance Entity are known as Maintenance
End Points (MEPs) -- see Section 2.6 below. The set of Maintenance

End Points that belong to the same Maintenance Domain are referred to
as a Maintenance Association (MA). On the network path in between
MEPs, there can be zero or more intermediate points, called
Maintenance Intermediate Points (MIPs). MEPs can be part of more
than one ME in a given MA.

2.6. MEPs and MIPs

OAM capabilities on RBridges can be defined in terms of logical
groupings of functions that can be categorized into two functional
objects: Maintenance End Points (MEPs) and Maintenance Intermediate
Points (MIPs). The two are collectively referred to as Maintenance
Points (MPs).

MEPs are the active components of TRILL OAM: MEPs source TRILL OAM
messages periodically or on-demand based on operator configuration
actions. Furthermore, MEPs ensure that TRILL OAM messages do not
leak outside a given Maintenance Domain, for example, out of the
TRILL network and into end stations. MIPs, on the other hand, are
internal to a Maintenance Domain. They are the more passive
components of TRILL OAM, primarily responsible for forwarding TRILL
OAM messages and selectively responding to a subset of these
messages.

The following figure shows the MEP and MIP placement for the
Maintenance Domains depicted in Figure 3 above.

```
      TRILL Site 1          Interconnect       TRILL Site 2
   +----------------+ +-----------------+ +----------------+
   |                | |                 | |                |
   |  +---+  +---+  +---+  +---+  +---+  +---+  +---+  +---+ |
   |  |RB1|--|RB2|--|RB3|--|RB4|--|RB5|--|RB6|--|RB7|--|RB8| |
   |  +---+  +---+  +---+  +---+  +---+  +---+  +---+  +---+ |
   |                | |                 | |                |
   +----------------+ +-----------------+ +----------------+

      <E-----------I--------------------I------------E>

      <E------I----E><E----I-------I----E><E-----I-----E>

   Legend E: MEP       I: MIP
```
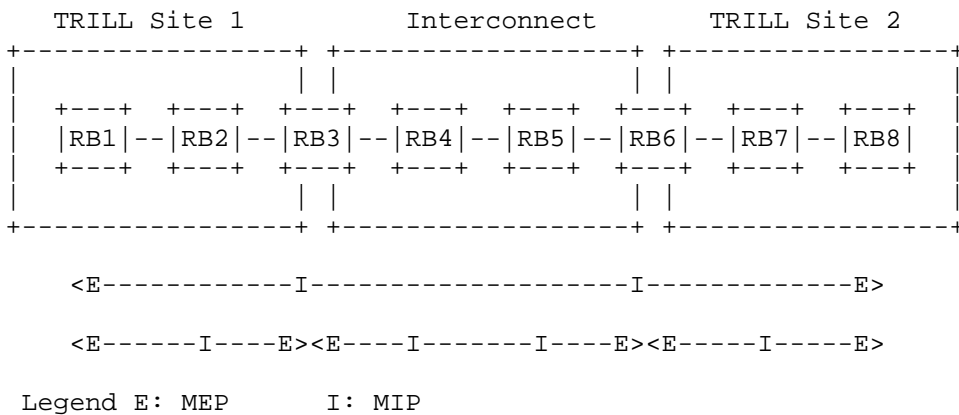
                      Figure 4: MEPs and MIPs

A single RBridge may host multiple MEPs of different technologies,
for example, TRILL OAM MEP(s) and [802.1Q] MEP(s). This does not
mean that the protocol operation is necessarily consolidated into a
single functional entity on those ports. The protocol functions for
each MEP remain independent and reside in different shims in the
RBridge Port Model of Figure 2: the TRILL OAM MEP resides in the
"TRILL OAM Layer" block whereas a CFM MEP resides in the "End-Station
VLAN & Priority Processing" block.

In the model of Section 2.2, a single MEP and/or MIP per MA can be
instantiated per RBridge port. A MEP is further qualified with an
administratively set direction (UP or DOWN), as follows:

- An UP MEP sends and receives OAM messages through the RBridge
   forwarding engine. This means that an UP MEP effectively
   communicates with MEPs on other RBridges through TRILL interfaces
   other than the one that the MEP is configured on.

- A DOWN MEP sends and receives OAM messages through the link
   connected to the interface on which the MEP is configured.

In order to support TRILL OAM functions on sections, as described in
[RFC6905], while maintaining the simplicity of a single TRILL OAM
Maintenance Domain, the TRILL OAM layer may be implemented on a
virtual port with no physical layer (Null PHY). In this case, the
Down MEP function is not supported, since the virtual port does not
attach to a link; as such, a Down MEP on a virtual port would not be
capable of sending or receiving OAM messages.

A TRILL OAM solution that conforms to this framework:

- must support the MIP function on TRILL ports (to support Fault
   Isolation).

- must support the UP MEP function on a TRILL virtual port (to
   support OAM functions on sections, as defined in [RFC6905]).

- may support the UP MEP function on TRILL ports.

- may support the DOWN MEP function on TRILL ports.

2.7. Maintenance Point Addressing

TRILL OAM functions must provide the capability to address a specific
Maintenance Point or a set of one or more Maintenance Points in an
MA. To that end, RBridges need to recognize two sets of addresses:

- Individual MP addresses

- Group MP addresses

   TRILL OAM will support the Shared MP address model, where all MPs on
   an RBridge share the same Individual MP address. In other words,
   TRILL OAM messages can be addressed to a specific RBridge but not to
   a specific port on an RBridge.

   One cannot discern, from observing the external behavior of an
   RBridge, whether TRILL OAM messages are actually delivered to a
   certain MP or another entity within the RBridge. The Shared MP
   address model takes advantage of this fact by allowing MPs in
   different RBridge ports to share the same Individual MP address. The
   MPs may still be implemented as residing on different RBridge ports,
   and for the most part, they have distinct identities.

   The Group MP addresses enable the OAM mechanism to reach all the MPs
   in a given MA. Certain OAM functions, for example, pruned tree
   verification, require addressing a subset of the MPs in an MA. Group
   MP addresses are not defined for such subsets. Rather, the OAM
   function in question must use the Group MP addresses combined with an
   indication of the scope of the MP subset encoded in the OAM Message
   Channel. This prevents an unwieldy set of responses to Group MP
   addresses.

3. OAM Frame Format

3.1. Motivation

   In order for TRILL OAM messages to accurately test the data path,
   these messages must be transparent to transit RBridges. That is, a
   TRILL OAM message must be indistinguishable from a TRILL Data packet
   through normal transit RBridge processing. Only the target RBridge,
   which needs to process the message, should identify and trap the
   packet as a control message through normal processing. Additionally,
   methods must be provided to prevent OAM packets from being
   transmitted out as native frames.

   The TRILL OAM packet format defined below provides the necessary
   flexibility to exercise the data path as closely as possible to
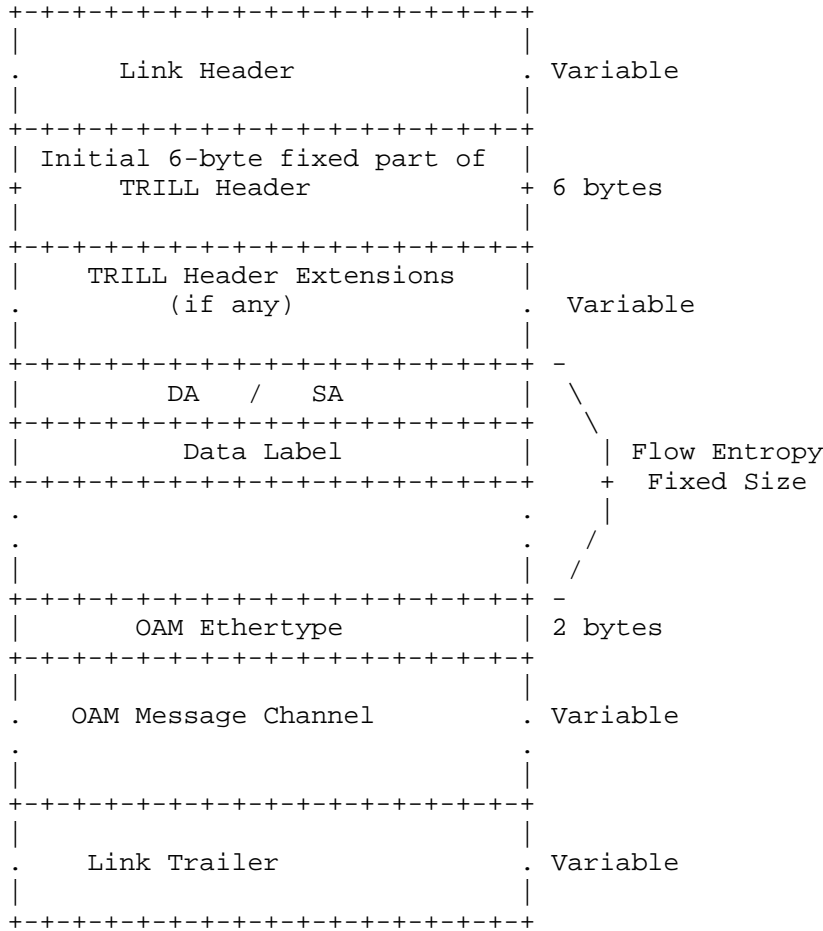   actual data packets.

```
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |                             |
        .         Link Header         . Variable
        |                             |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        | Initial 6-byte fixed part of |
        +         TRILL Header         + 6 bytes
        |                             |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |    TRILL Header Extensions   |
        .          (if any)           . Variable
        |                             |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ -
        |        DA    /    SA         | \
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  \
        |         Data Label          |  | Flow Entropy
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  +  Fixed Size
        .                             .  |
        .                             .  /
        |                             | /
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ -
        |        OAM Ethertype        | 2 bytes
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |                             |
        .     OAM Message Channel      . Variable
        .                             .
        |                             |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |                             |
        .         Link Trailer         . Variable
        |                             |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                    Figure 5: OAM Frame Format

   The TRILL Header and the Link Header and Trailer need to be as
   similar as practical to the TRILL Header and the Link Header and
   Trailer of the normal TRILL Data packet corresponding to the traffic
   that OAM is testing.

   The OAM Ethertype demarcates the boundary between the Flow Entropy
   field and the OAM Message Channel. The OAM Ethertype is expected at
   a deterministic offset from the TRILL Header, thereby allowing
   applications to clearly identify the beginning of the OAM Message
   Channel. Additionally, it facilitates the use of the same OAM frame
   structure by different Ethernet technologies.

The Link Trailer is usually a checksum, such as the Ethernet Frame
Check Sequence, which is examined at a low level very early in the
frame input process and automatically generated as part of the low-
level frame output process. If the checksum fails, the frame is
normally discarded with no higher-level processing.

3.2. Determination of Flow Entropy

The Flow Entropy field is a fixed-length field that is populated with
either real packet data or synthetic data that mimics the intended
flow. It always starts with a destination and source MAC address
area followed by a Data Label area (either a VLAN or fine-grained
label).

For a Layer 2 flow (that is, non-IP) the Flow Entropy field must
specify the desired Ethernet header, including the MAC destination
and source addresses as well as a VLAN tag or fine-grained label.

For a Layer 3 flow, the Flow Entropy field must specify the desired
Ethernet header, the IP header, and UDP or TCP header fields,
although the Ethernet-layer header fields are also still present.

Not all fields in the Flow Entropy field need to be identical to the
data flow that the OAM message is mimicking. The only requirement is
for the selected flow entropy to follow the same path as the data
flow that it is mimicking. In other words, the selected flow entropy
must result in the same ECMP selection or multicast pruning behavior
or other applicable forwarding paradigm.

When performing diagnostics on user flows, the OAM mechanisms must
allow the network operator to configure the flow entropy parameters
(for example, Layer 2 and/or 3) on the RBridge from which the
diagnostic operations are to be triggered.

When running OAM functions over test flows, the TRILL OAM may provide
a mechanism for discovering the flow entropy parameters by querying
the RBridges dynamically, or it may allow the network operator to
configure the flow entropy parameters.

3.2.1. Address Learning and Flow Entropy

Edge TRILL Switches, like traditional 802.1 bridges, are required to
learn MAC address associations. Learning is accomplished either by
snooping data packets or through other methods. The Flow Entropy
field of TRILL OAM messages mimics real packets and may impact the
address-learning process of the TRILL data plane. TRILL OAM is
required to provide methods to prevent any learning of addresses from

the Flow Entropy field of OAM messages that would interfere with
normal TRILL operation. This can be done, for example, by
suppressing/preventing MAC address learning from OAM messages.

3.3. OAM Message Channel

The OAM Message Channel provides methods to communicate OAM-specific
details between RBridges. CFM [802.1Q] and [RFC4379] have
implemented OAM message channels. It is desirable to select an
appropriate technology and reuse it, instead of redesigning yet
another OAM channel. TRILL is a transport layer that carries
Ethernet frames, so the TRILL OAM model specified earlier is based on
the CFM [802.1Q] model. The use of the CFM [802.1Q] encoding format
for the OAM Message Channel is one possible choice. [TRILL-OAM]
presents a proposal on the use of CFM [802.1Q] payload as the OAM
Message Channel.

3.4. Identification of OAM Messages

RBridges must be able to identify OAM messages that are destined to
them, either individually or as a group, so as to properly process
those messages.

TRILL, as defined in [RFC6325], does not specify a method to identify
OAM messages. The most reliable method to identify these messages,
without imposing restrictions on the Flow Entropy field, involves
modifying the definition of the TRILL Header to include an "Alert"
flag. This flag signals that the content of the TRILL packet is a
control message as opposed to user data. The use of such a flag
would not be limited to TRILL OAM and may be leveraged by any other
TRILL control protocol that requires in-band behavior. The TRILL
Header currently has two reserved bits that are unused. One of those
bits may be used as the Alert flag. In order to guarantee accurate
in-band forwarding behavior, RBridges must not use the Alert flag in
ECMP hashing decisions. Furthermore, to ensure that this flag
remains protocol agnostic, TRILL OAM mechanisms must not rely solely
on the Alert flag to identify OAM messages. Rather, these solutions
must identify OAM messages based on the combination of the Alert flag
and the OAM Ethertype.

Since the above mechanism requires modification of the TRILL Header,
it is not backward compatible. TRILL OAM solutions should provide
alternate methods to identify OAM messages that work on existing
RBridge implementations, thereby providing backward compatibility.

4. Fault Management

   Section 4.1 below discusses proactive fault management, and
   Section 4.2 discusses on-demand fault management.

4.1. Proactive Fault Management Functions

   Proactive fault management functions are configured by the network
   operator to run periodically without a time bound or are configured
   to trigger certain actions upon the occurrence of specific events.

4.1.1. Fault Detection (Continuity Check)

   Proactive fault detection is performed by periodically monitoring the
   reachability between service endpoints, that is, MEPs in a given MA,
   through the exchange of Continuity Check messages. The reachability
   between any two arbitrary MEPs may be monitored for a specified path,
   all paths, or any representative path. The fact that TRILL networks
   do not enforce congruence between unicast and multicast paths means
   that the proactive fault detection mechanism must provide procedures
   to monitor the unicast paths independently of the multicast paths.
   Furthermore, where the network has ECMP, the proactive fault
   detection mechanism must be capable of exercising the equal-cost
   paths individually.

   The set of MEPs exchanging Continuity Check messages in a given
   domain and for a specific monitored entity (flow, network, or
   service) must use the same transmission period. As long as the fault
   detection mechanism involves MEPs transmitting periodic heartbeat
   messages independently, then this OAM procedure is not affected by
   the lack of forward/reverse path symmetry in TRILL.

   The proactive fault detection function must detect the following
   types of defects:

   - Loss of continuity to one or more remote MEPs

   - Unexpected connectivity between isolated VLANs or fine-grained
      labels (mismerge)

   - Unexpected connectivity to one or more remote MEPs

   - Mismatch of the Continuity Check transmission period between MEPs

4.1.2. Defect Indication

   TRILL OAM must support event-driven defect indication upon the
   detection of a connectivity defect. Defect indications can be
   categorized into two types; these types are discussed in the
   following subsections.

4.1.2.1. Forward Defect Indication

   Forward defect indication is used to signal a failure that is
   detected by a lower-layer OAM mechanism. A forward defect indication
   is transmitted away from the direction of the failure. For example,
   consider a simple network comprised of four RBridges connected in
   series: RB1, RB2, RB3, and RB4. Both RB1 and RB4 are hosting TRILL
   OAM MEPs, whereas RB2 and RB3 have MIPs. If the link between RB2 and
   RB3 fails, then RB2 can send a forward defect indication towards RB1
   while RB3 sends a forward defect indication towards RB4.

   Forward defect indication may be used for alarm suppression and/or
   for the purpose of interworking with other layer OAM protocols.
   Alarm suppression is useful when a transport/network-level fault
   translates to multiple service- or flow-level faults. In such a
   scenario, it is enough to alert a network management station (NMS) of
   the single transport/network-level fault in lieu of flooding that NMS
   with a multitude of Service or Flow granularity alarms.

4.1.2.2. Reverse Defect Indication (RDI)

   RDI is used to signal that the advertising MEP has detected a loss-
   of-continuity defect. RDI is transmitted in the direction of the
   failure. For example, consider the same series network as that in
   Section 4.1.2.1. If RB1 detects that is has lost connectivity to RB4
   because it is no longer receiving Continuity Check messages from the
   MEP on RB4, then RB1 can transmit an RDI towards RB4 to inform the
   latter of the failure. If the failure is unidirectional (it is
   affecting the direction from RB4 to RB1), then the RDI enables RB4 to
   become aware of the unidirectional connectivity anomaly.

   In the presence of equal-cost paths between MEPs, RDI must be able to
   identify on which equal-cost path the failure was detected.

   RDI allows single-sided management, where the network operator can
   examine the state of a single MEP and deduce the overall health of a
   monitored entity (network, flow, or service).

4.2. On-Demand Fault Management Functions

   On-demand fault management functions are initiated manually by the
   network operator either as a one-time occurrence or as an action/test
   that continues for a time bound period. These functions enable the
   operator to run diagnostics to investigate a defect condition.

4.2.1. Connectivity Verification

   As specified in [RFC6905], TRILL OAM must support on-demand
   Connectivity Verification for unicast and multicast. The
   Connectivity-Verification mechanism must provide a means for
   specifying and carrying in the messages:

   - variable-length payload/padding to test MTU-related connectivity
      problems.

   - test message formats as defined in [RFC2544].

4.2.1.1. Unicast

   A unicast Connectivity Verification operation must be initiated from
   a MEP and may target either a MIP or another MEP. For unicast,
   Connectivity Verification can be performed at either Network or Flow
   granularity.

   Connectivity verification at the Network granularity tests
   connectivity between a MEP on a source RBridge and a MIP or MEP on a
   target RBridge over a test flow in a test VLAN or fine-grained label.
   The operator must supply the source and target RBridges for the
   operation, and the test VLAN/flow information uses pre-set values or
   defaults.

   Connectivity Verification at the Flow granularity tests connectivity
   between a MEP on a source RBridge and a MIP or MEP on a target
   RBridge over an operator-specified VLAN or fine-grained label with
   operator-specified flow parameters.

   The above functions must be supported on sections, as defined in
   [RFC6905]. When Connectivity Verification is triggered over a
   section, and the initiating MEP does not coincide with the edge
   (ingress) RBridge, the MEP must use the edge RBridge nickname instead
   of the local RBridge nickname on the associated Connectivity
   Verification messages. The operator must supply the edge RBridge
   nickname as part of the operation parameters.

4.2.1.2. Multicast

   For multicast, the Connectivity Verification function tests all
   branches and leaf nodes of a multi-destination distribution tree for
   reachability. This function should include mechanisms to prevent
   reply storms from overwhelming the initiating RBridge. This may be
   done, for example, by staggering the replies through the introduction
   of a random delay timer, with a preset upper bound, on the responding
   RBridge (CFM [802.1Q] uses similar mechanisms for Linktrace Reply
   messages to mitigate the load on the originating MEP). The upper
   bound on the timer value should be selected by the OAM solution to be
   long enough to accommodate large distribution trees, while allowing
   the Connectivity Verification operation to conclude within a
   reasonable time. To further prevent reply storms, Connectivity
   Verification operation is initiated from a MEP and must target MEPs
   only. MIPs are transparent to multicast Connectivity Verification.

   Per [RFC6905], multicast Connectivity Verification must provide the
   following granularity of operation:

   A. Un-pruned Tree

       - Connectivity Verification for un-pruned multi-destination
          distribution tree. The operator in this case supplies the
          tree identifier (root nickname) and campus-wide diagnostic
          VLAN or fine-grained label.

   B. Pruned Tree

       - Connectivity Verification for a VLAN or fine-grain label in a
          given multi-destination distribution tree. The operator in
          this case supplies the tree identifier and VLAN or fine-
          grained label.

       - Connectivity Verification for an IP multicast group in a given
          multi-destination distribution tree. The operator in this
          case supplies: the tree identifier, VLAN or fine-grained
          label, and IP (S,G) or (*,G).

4.2.2. Fault Isolation

   TRILL OAM must support an on-demand connectivity fault localization
   function. This is the capability to trace the path of a flow on a
   hop-by-hop (RBridge-by-RBridge) basis to isolate failures. This
   involves the capability to narrow down the locality of a fault to a
   particular port, link, or node. The characteristic of
   forward/reverse path asymmetry, in TRILL, renders Fault Isolation
   into a direction-sensitive operation. That is, given two RBridges, A

and B, localization of connectivity faults between them requires
running Fault Isolation procedures from RBridge A to RBridge B as
well as from RBridge B to RBridge A. Generally speaking, single-
sided Fault Isolation is not possible in TRILL OAM.

Furthermore, TRILL OAM should support Fault Isolation over
distribution trees for both un-pruned as well as pruned trees. The
former allows the tracing of all active branches of a tree, whereas
the latter allows tracing of the active subset of branches associated
with a given flow.

5. Performance Monitoring

   Performance monitoring functions are optional in TRILL OAM, per
   [RFC6905]. These functions can be performed both proactively and on-
   demand. Proactive management involves a scheduling function, where
   the performance monitoring probes can be triggered on a recurring
   basis. Since the basic performance monitoring functions involved are
   the same, we make no distinction between proactive and on-demand
   functions in this section.

5.1. Packet Loss

   Given that TRILL provides inherent support for multipoint-to-
   multipoint connectivity, then packet loss cannot be accurately
   measured by means of counting user data packets. This is because
   user packets can be delivered to more RBridges or more ports than are
   necessary (for example, due to broadcast, un-pruned multicast, or
   unknown unicast flooding). As such, a statistical means of
   approximating packet loss rate is required. This can be achieved by
   sending "synthetic" (TRILL OAM) packets that are counted only by
   those ports (MEPs) that are required to receive them. This provides
   a statistical approximation of the number of data frames lost, even
   with multipoint-to-multipoint connectivity. TRILL OAM mechanisms for
   synthetic packet loss measurement should follow the statistical
   considerations specified in [MEF35], especially with regard to the
   volume/frequency of synthetic traffic generation and associated
   impact on packet loss count accuracy.

   Packet loss probes must be initiated from a MEP and must target a
   MEP. This function should be supported on sections, as defined in
   [RFC6905]. When packet loss is measured over a section, and the
   initiating MEP does not coincide with the edge (ingress) RBridge, the
   MEP must use the edge RBridge nickname instead of the local RBridge
   nickname on the associated loss measurement messages. The user must
   supply the edge RBridge nickname as part of the operation parameters.

   TRILL OAM mechanisms should support one-way and two-way Packet Loss
   Monitoring. In one-way monitoring, a source RBridge triggers Packet
   Loss Monitoring messages to a target RBridge, and the latter is
   responsible for calculating the loss in the direction from the source
   RBridge towards the target RBridge. In two-way monitoring, a source
   RBridge triggers Packet Loss Monitoring messages to a target RBridge,
   and the latter replies to the source with response messages. The
   source RBridge can then monitor packet loss in both directions
   (source to target and target to source).

5.2. Packet Delay

   Packet delay is measured by inserting timestamps in TRILL OAM
   packets. In order to ensure high accuracy of measurement, TRILL OAM
   must specify the timestamp location at fixed offsets within the OAM
   packet in order to facilitate hardware-based timestamping. Hardware
   implementations must implement the timestamping function as close to
   the wire as practical in order to maintain high accuracy.

   TRILL OAM mechanisms should support one-way and two-way Packet Delay
   Monitoring. In one-way monitoring, a source RBridge triggers Packet
   Delay Monitoring messages to a target RBridge, and the latter is
   responsible for calculating the delay in the direction from the
   source RBridge towards the target RBridge. This requires
   synchronization of the clocks between the two RBridges. In two-way
   monitoring, a source RBridge triggers Packet Delay Monitoring
   messages to a target RBridge, and the latter replies to the source
   with response messages. The source RBridge can then monitor packet
   delay in both directions (source to target and target to source) as
   well as the cumulative round-trip delay. In this case as well,
   monitoring the delay in a single direction requires clock
   synchronization between the two RBridges, whereas monitoring the
   round-trip delay does not require clock synchronization. Mechanisms
   for clock synchronization between RBridges are outside the scope of
   this document.

6. Operational and Manageability Considerations

6.1. TRILL OAM Configuration

   RBridges may be configured to enable TRILL OAM functions via the
   device Command Line Interface (CLI) or through one of the defined
   management protocols, such as the Simple Network Management Protocol
   (SNMP) [RFC3410] or the Network Configuration Protocol (NETCONF)
   [RFC6241].

In order to maintain the plug-and-play characteristics of TRILL, the
number of parameters that need to be configured on RBridges, in order
to activate TRILL OAM, should be kept to a minimum. To that end,
TRILL OAM mechanisms should rely on default values and auto-discovery
mechanisms (for example, leveraging IS-IS) where applicable. The
following is a non-exhaustive list of configuration parameters that
apply to TRILL OAM.

6.1.1. Maintenance Domain Parameters

   - Maintenance Domain Name
     An alphanumeric name for the Maintenance Domain. This is an IETF
     [RFC2579] DisplayString, with the exception that character codes
     0-31 (decimal) are not used. The recommended default value is the
     character string "DEFAULT".

   - Maintenance Domain Level
     An integer in the range 0 to 7 indicating the level at which the
     Maintenance Domain is to be created. Default value is 0.

6.1.2. Maintenance Association Parameters

   - MA Name
     An alphanumeric name that uniquely identifies the Maintenance
     Association. This is an IETF [RFC2579] DisplayString, with the
     exception that character codes 0-31 (decimal) are not used. The
     recommended default value is a character string set to the value
     of the VLAN or fine-grained label as "vl" or "fgl" concatenated
     with the VLAN ID or FGL ID as an unsigned decimal integer, for
     example, "vl42".

   - List of MEP Identifiers
     A list of the identifiers of the MEPs that belong to the MA. This
     is optional and required only if the operator wants to detect
     missing MEPs as part of the Continuity Check function.

6.1.3. Maintenance Endpoint Parameters

   - MEP Identifier
     An integer, unique over a given Maintenance Association,
     identifying a specific MEP. CFM [802.1Q] limits this to the range
     1 to 8191. This document recommends expanding the range from 1 to
     65535 so that the RBridge nickname can be used as a default value.
     This will help keep TRILL OAM low-touch in terms of configuration
     overhead.

   - Direction
     Indicates whether this is an UP MEP or DOWN MEP.

   - Associated Interface
      Specifies the interface on which the MEP is configured.

   - MA Context
      Specifies the Maintenance Association to which the MEP belongs.

6.1.4. Continuity Check Parameters (Applicable per MA)

   - Transmission Interval
      Indicates the interval at which Continuity Check messages are sent
      by a MEP.

   - Loss Threshold
      Indicates the number of consecutive Continuity Check messages that
      a MEP must not receive from any one of the other MEPs in its MA
      before indicating either a MEP failure or a network failure.
      Recommended default value is 3.

   - VLAN, Fine-Grained Label, and Flow Parameters
      The VLAN or fine-grained label and flow parameters to be used in
      the Continuity Check messages.

   - Hop Count
      The hop count to be used in the Continuity Check messages.

6.1.5. Connectivity Verification Parameters (Applicable per Operation)

   - MA context
      Specifies the Maintenance Association in which the Connectivity
      Verification operation is to be performed.

   - Target RBridge Nickname (unicast), Tree Identifier (multicast),
      and IP Multicast Group
      For unicast, the nickname of the RBridge that is the target of the
      Connectivity Verification operation. For multicast, the target
      Tree Identifier for un-pruned tree verification or the Tree
      Identifier and IP multicast group (S, G) or (*, G) for pruned tree
      verification.

   - VLAN, Fine-Grained Label, and Flow Parameters
      The VLAN or fine-grained label and flow parameters to be used in
      the Connectivity Verification message.

   - Operation Timeout Value
      The timeout on the initiating MEP before the Connectivity
      Verification operation is declared to have failed. The
      recommended default value is 5 seconds.

- Repeat Count
  The number of Connectivity Verification messages that must be
  transmitted per operation. The recommended default value is 1.

- Hop Count
  The hop count to be used in the Connectivity Verification
  messages.

- Reply Mode
  Indicates whether the response to the Connectivity Verification
  operation should be sent in-band or out-of-band.

- Scope List (Multicast)
  List of MEP Identifiers that must respond to the message.

6.1.6. Fault Isolation Parameters (Applicable per Operation)

- MA Context
  Specifies the Maintenance Association in which the Fault Isolation
  operation is to be performed.

- Target RBridge Nickname (unicast), Tree Identifier (multicast),
  and IP Multicast Group
  For unicast, the nickname of the RBridge that is the target of the
  Fault Isolation operation. For multicast, the target Tree
  Identifier for un-pruned tree tracing or the Tree Identifier and
  IP multicast group (S, G) or (*, G) for pruned tree tracing.

- VLAN, Fine-Grained Label, and Flow Parameters
  The VLAN or fine-grain label and flow parameters to be used in the
  Fault Isolation messages.

- Operation Timeout Value
  The timeout on the initiating MEP before the Fault Isolation
  operation is declared to have failed. The recommended default
  value is 5 seconds.

- Hop Count
  The hop count to be used in the Fault Isolation messages.

- Reply Mode
  Indicates whether the response to the Fault Isolation operation
  should be sent in-band or out-of-band.

- Scope List (Multicast)
  List of MEP Identifiers that must respond to the message.

6.1.7. Packet Loss Monitoring

   - MA Context
      Specifies the Maintenance Association in which the Packet Loss
      Monitoring operation is to be performed.

   - Target RBridge Nickname
      The nickname of the RBridge that is the target of the Packet Loss
      Monitoring operation.

   - VLAN, Fine-Grained Label, and Flow Parameters
      The VLAN or fine-grained label and flow parameters to be used in
      the Packet Loss Monitoring messages.

   - Transmission Rate
      The transmission rate at which the Packet Loss Monitoring messages
      are to be sent.

   - Monitoring Interval
      The total duration of time for which a single Packet Loss
      Monitoring probe is to continue.

   - Repeat Count
      The number of probe operations to be performed. For on-demand
      monitoring, this is typically set to 1. For proactive monitoring,
      this may be set to allow for infinite monitoring.

   - Hop Count
      The hop count to be used in the Packet Loss Monitoring messages.

   - Mode
      Indicates whether one-way or two-way loss measurement is required.

6.1.8. Packet Delay Monitoring

   - MA Context
      Specifies the Maintenance Association in which the Packet Delay
      Monitoring operation is to be performed

   - Target RBridge Nickname
      The nickname of the RBridge that is the target of the Packet Delay
      Monitoring operation.

   - VLAN, Fine-Grained Label, and Flow Parameters
      The VLAN or fine-grained label and flow parameters to be used in
      the Packet Delay Monitoring messages.

- Transmission Rate
  The transmission rate at which the Packet Delay Monitoring
  messages are to be sent.

- Monitoring Interval
  The total duration of time for which a single Packet Delay
  Monitoring probe is to continue.

- Repeat Count
  The number of probe operations to be performed. For on-demand
  monitoring, this is typically set to 1. For proactive monitoring
  this may be set to allow for infinite monitoring.

- Hop Count
  The hop count to be used in the Packet Delay Monitoring messages.

- Mode
  Indicates whether one-way or two-way delay measurement is
  required.

6.2. TRILL OAM Notifications

   TRILL OAM mechanisms should trigger notifications to alert operators
   to certain conditions. Such conditions include but are not limited
   to:

   - Faults detected by proactive mechanisms.

   - Reception of event-driven defect indications.

   - Logged security incidents pertaining to the OAM Message Channel.

   - Protocol errors (for example, as caused by misconfiguration).

   Notifications generated by TRILL OAM mechanisms may be via SNMP,
   Syslog messages [RFC5424], or any other standard management protocol
   that supports asynchronous notifications.

6.3. Collecting Performance Monitoring Metrics

   When performing the optional TRILL OAM performance monitoring
   functions, two RBridge designations are involved: a source RBridge
   and a target RBridge. The source RBridge is the one from which the
   performance monitoring probe is initiated, and the target RBridge is
   the destination of the probe. The goal is to monitor performance
   characteristics between the two RBridges. The RBridge from which the

network operator can extract the results of the probe (the
performance monitoring metrics) depends on whether one-way or two-way
performance monitoring functions are performed:

- In the case of one-way performance monitoring functions, the
  metrics will be available at the target RBridge.

- In the case of two-way performance monitoring functions, all the
  metrics will be available at the source RBridge, and a subset will
  be available at the target RBridge. More specifically, metrics in
  the direction from source to target as well as the direction from
  target to source will be available at the source RBridge. Metrics
  in the direction from source to target will be available at the
  target RBridge.

7. Security Considerations

   TRILL OAM must provide mechanisms for:

- Preventing denial-of-service attacks caused by exploitation of the
  OAM Message Channel, where a rogue device may overload the
  RBridges and the network with OAM messages. This could lead to
  interruption of the OAM services and, in the extreme case, disrupt
  network connectivity. Mechanisms such as control-plane policing
  combined with shaping or rate limiting of OAM messaging can be
  employed to mitigate this.

- Optionally authenticating at communicating endpoints (MEPs and
  MIPs) that an OAM message has originated at an appropriate
  communicating endpoint.

- Preventing TRILL OAM packets from leaking outside of the TRILL
  network or outside their corresponding Maintenance Domain. This
  can be done by having MEPs implement a filtering function based on
  the Maintenance Level associated with received OAM packets.

   For general TRILL Security Considerations, see [RFC6325].

8. Acknowledgments

   We thank Gayle Noble, Dan Romascanu, Olen Stokes, Susan Hares, Ali
   Karimi, and Prabhu Raj for their thorough review of this work and
   their comments.

9. References

9.1. Normative References

   [802]   IEEE, "IEEE Standard for Local and Metropolitan Area
                Networks - Overview and Architecture", IEEE Std 802-2001,
                8 March 2002.

   [802.1Q]   IEEE, "IEEE Standard for Local and metropolitan area
                networks - Media Access Control (MAC) Bridges and Virtual
                Bridge Local Area Networks", IEEE Std 802.1Q-2011, 31
                August 2011.

   [RFC2544]   Bradner, S. and J. McQuaid, "Benchmarking Methodology for
                Network Interconnect Devices", RFC 2544, March 1999.

   [RFC2579]   McCloghrie, K., Ed., Perkins, D., Ed., and J.
                Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD
                58, RFC 2579, April 1999.

   [RFC6291]   Andersson, L., van Helvoort, H., Bonica, R., Romascanu,
                D., and S. Mansfield, "Guidelines for the Use of the
                "OAM" Acronym in the IETF", BCP 161, RFC 6291, June 2011.

   [RFC6325]   Perlman, R., Eastlake 3rd, D., Dutt, D., Gai, S., and A.
                Ghanwani, "Routing Bridges (RBridges): Base Protocol
                Specification", RFC 6325, July 2011.

   [RFC6905]   Senevirathne, T., Bond, D., Aldrin, S., Li, Y., and R.
                Watve, "Requirements for Operations, Administration, and
                Maintenance (OAM) in Transparent Interconnection of Lots
                of Links (TRILL)", RFC 6905, March 2013.

   [RFC7172]   Eastlake 3rd, D., Zhang, M., Agarwal, P., Perlman, R, and
                D. Dutt, "Transparent Interconnection of Lots of Links
                (TRILL): Fine-Grained Labeling", RFC 7172, May 2014.

   [RFC7177]   Eastlake 3rd, D., Perlman, R., Ghanwani, A., Yang, H.,
                and V. Manral, "Transparent Interconnection of Lots of
                Links (TRILL): Adjacency", RFC 7177, May 2014.

9.2. Informative References

   [802.3]   IEEE, "IEEE Standard for Information technology -
              Telecommunications and information exchange between
              systems - Local and metropolitan area networks - Specific
              requirements - Part 3: Carrier sense multiple access with
              collision detection (CSMA/CD) access method and physical
              layer specifications", IEEE Std 802.3-2012, December
              2012.

   [ISO/IEC7498-4]
              ISO/IEC, "Information processing systems -- Open Systems
              Interconnection -- Basic Reference Model -- Part 4:
              Management framework", ISO/IEC 7498-4, 1989.

   [MEF35]   Metro Ethernet Forum, "MEF 35 - Service OAM Performance
              Monitoring Implementation Agreement", April 2012.

   [RFC1661] Simpson, W., Ed., "The Point-to-Point Protocol (PPP)",
              STD 51, RFC 1661, July 1994.

   [RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart,
              "Introduction and Applicability Statements for Internet-
              Standard Management Framework", RFC 3410, December 2002.

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

   [RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March
              2009.

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

   [RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection
              (BFD)", RFC 5880, June 2010.

   [RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J.,
              Ed., and A. Bierman, Ed., "Network Configuration Protocol
              (NETCONF)", RFC 6241, June 2011.

   [RFC6361] Carlson, J. and D. Eastlake 3rd, "PPP Transparent
              Interconnection of Lots of Links (TRILL) Protocol Control
              Protocol", RFC 6361, August 2011.

   [RFC6371]   Busi, I., Ed., and D. Allan, Ed., "Operations,
               Administration, and Maintenance Framework for MPLS-Based
               Transport Networks", RFC 6371, September 2011.

   [RFC7087]   van Helvoort, H., Ed., Andersson, L., Ed., and N.
               Sprecher, Ed., "A Thesaurus for the Interpretation of
               Terminology Used in MPLS Transport Profile (MPLS-TP)
               Internet-Drafts and RFCs in the Context of the ITU-T's
               Transport Network Recommendations", RFC 7087, December
               2013.

   [RFC7175]   Manral, V., Eastlake 3rd, D., Ward, D., and A. Banerjee,
               "Transparent Interconnection of Lots of Links (TRILL):
               Bidirectional Forwarding Detection (BFD) Support", RFC
               7175, May 2014.

   [TRILL-IP] Wasserman, M, Eastlake 3rd, D., and D. Zhang,
               "Transparent Interconnection of Lots of Links (TRILL)
               over IP", Work in Progress, March 2014.

   [TRILL-ML] Perlman, R., Eastlake 3rd, D., Ghanwani, A., and H. Zhai,
               "Flexible Multilevel TRILL (Transparent Interconnection
               of Lots of Links)", Work in Progress, January 2014.

   [TRILL-OAM] Senevirathne, T., Salam, S., Kumar, D, Eastlake 3rd, D.,
               Aldrin, S., and Y. Li, "TRILL Fault Management", Work in
               Progress, February 2014.

   [Y.1731]   ITU-T, "OAM functions and mechanisms for Ethernet based
               networks", ITU-T Recommendation Y.1731, February 2008.

Authors' Addresses

   Samer Salam
   Cisco
   595 Burrard Street, Suite 2123
   Vancouver, BC V7X 1J1
   Canada

   EMail: ssalam@cisco.com

   Tissa Senevirathne
   Cisco
   375 East Tasman Drive
   San Jose, CA 95134
   USA

   EMail: tsenevir@cisco.com

   Sam Aldrin
   Huawei Technologies
   2330 Central Expressway
   Santa Clara, CA 95050
   USA

   EMail: sam.aldrin@gmail.com

   Donald Eastlake 3rd
   Huawei Technologies
   155 Beaver Street
   Milford, MA 01757
   USA

   Phone: 1-508-333-2270
   EMail: d3e3e3@gmail.com