Operations and Management Area Working Group   T. Mizrahi
Internet Draft   Marvell
Intended status: Informational   N. Sprecher
Expires: July 2011   Nokia Siemens Networks
                                                 E. Bellagamba
                                                      Ericsson
                                                 Y. Weingarten
                                         Nokia Siemens Networks
                                              January 24, 2011

An Overview of
Operations, Administration, and Maintenance (OAM) Mechanisms
draft-ietf-opsawg-oam-overview-03.txt

Status of this Memo

   This Internet-Draft is submitted to IETF in full conformance with the
   provisions of BCP 78 and BCP 79.

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

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

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

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

   This Internet-Draft will expire on July 24, 2011.

Copyright Notice

Abstract

   Operations, Administration, and Maintenance (OAM) is a general term
   that refers to a toolset that can be used for fault detection and
   localization, and for performance measurement. OAM mechanisms have
   been defined for various layers in the protocol stack, and are used
   with a variety of protocols.

   This document presents an overview of the OAM mechanisms that have
   been defined and are currently being defined by the IETF, as well as
   a comparison to other OAM mechanisms that have been defined by the
   IEEE and ITU-T.

Table of Contents

1. Introduction

   OAM is a general term that refers to a toolset that can be used for
   detecting, isolating and reporting connection failures or measurement
   of connection performance parameters. The term OAM has been used over
   the years in several different contexts, as discussed in [OAM Soup].
   In the context of this document OAM refers to Operations,
   Administration, and Maintenance, i.e., this document refers to OAM in
   the context of monitoring communication entities, e.g., nodes, paths,
   physical links, or logical links. Other aspects associated with the
   OAM acronym, such as management, are outside the scope of this
   document.

   OAM was originally used in the world of telephony, and has been
   adopted in packet based networks. OAM mechanisms are used in various
   layers in the protocol stack, and are applied to a variety of
   different protocols.

   The IETF has defined OAM for several protocols, and is currently
   working on defining several new OAM protocols. A summary of these
   protocols, old and new, is listed below:

   o MPLS LSP Ping, as defined in [LSP Ping] is an OAM mechanism for
      point to point MPLS LSPs. The IETF is currently working on an
      extension to the LSP Ping for point to multipoint MPLS - [P2MP
      Ping].

   o Virtual Circuit Connectivity Check (VCCV) for Pseudowires, as
      defined in [VCCV].

   o ICMP Echo request, also known as Ping, as defined in [ICMPv4], and
      [ICMPv6]. ICMP Ping is a very simple and basic mechanism in
      failure diagnosis, and is not traditionally associated with OAM,
      but it is presented in this document for the sake of completeness,
      since both LSP Ping and VCCV are to some extent based on ICMP
      Ping.

   o Bidirectional Forwarding Detection (BFD) is defined in [BFD] as a
      framework for a lightweight generic OAM mechanism. The intention
      is to define a base mechanism that can be used with various
      encapsulation types, network environments, and in various medium
      types.

   o The OAM requirements for MPLS Transport Profile (MPLS-TP) are
     defined in [MPLS-TP OAM], and the toolset is described in [MPLS-TP
     OAM FW]. The OAM toolset for MPLS-TP is currently being defined in
     the MPLS working group.

   o IP Performance Metrics (IPPM) is a working group in the IETF that
     defined common metrics for performance measurement, as well as a
     protocol for measuring delay and packet loss in IP networks.
     Alternative protocols for performance measurement are defined, for
     example, in MPLS-TP OAM [MPLS-TP OAM], and in Ethernet OAM [ITU-T
     Y.1731].

   In addition to the OAM mechanisms defined by the IETF, the IEEE and
   ITU-T have also defined various OAM mechanisms. These various
   mechanisms defined by the three standard organizations are often
   tightly coupled, and have had a mutual effect on each other. The ITU-
   T and IETF have both defined OAM mechanisms for MPLS LSPs, [ITU-T
   Y.1711] and [LSP Ping]. The following OAM standards by the IEEE and
   ITU-T are to some extent linked to IETF OAM mechanisms listed above,
   and are also discussed in this document:

   o OAM mechanisms for Ethernet based networks have been defined by
     both the ITU-T in [ITU-T Y.1731], and by the IEEE in [IEEE
     802.1ag]. The IEEE 802.3 standard defines OAM for one-hop Ethernet
     links [IEEE 802.3ah].

   o The ITU-T has defined OAM for MPLS LSPs in [ITU-T Y.1711].

   This document summarizes the OAM mechanisms defined in the standards
   above. The focus is on OAM mechanisms defined by the IETF. These
   mechanisms will be compared with the relevant OAM mechanisms defined
   by the ITU-T and IEEE, where applicable. We first present a
   comparison of the terminology used in various OAM standards, and then
   summarize the OAM functions that each OAM standard provides.

   Table 1 summarizes the OAM standards discussed in this document.

```
   +-----------+-------------------------------------+---------------+
   |           | Title                               |Standard/Draft |
   +-----------+-------------------------------------+---------------+
   |ICMPv4 Ping| Internet Control Message Protocol   | RFC 792       |
   |           |                                     |               |
   +-----------+-------------------------------------+---------------+
   |ICMPv6 Ping| Internet Control Message Protocol   | RFC 4443      |
   |           | (ICMPv6) for the Internet Protocol  |               |
```

		Version 6 (IPv6) Specification	
BFD	Bidirectional Forwarding Detection	RFC 5880	
		Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)	RFC 5881
		Generic Application of Bidirectional Forwarding Detection	RFC 5882
		Bidirectional Forwarding Detection (BFD) for Multihop Paths	RFC 5883
		Bidirectional Forwarding Detection for MPLS Label Switched Paths (LSPs)	RFC 5884
		Bidirectional Forwarding Detection for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)	RFC 5885
IETF MPLS OAM (LSP Ping)	Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks	RFC 4377	
		A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM)	RFC 4378
		Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures	RFC 4379
		Operations and Management (OAM) Requirements for Point-to-Multipoint MPLS Networks	RFC 4687
MPLS-TP OAM	Requirements for OAM in MPLS-TP	RFC 5860	
		MPLS Generic Associated Channel	RFC 5586
		MPLS-TP OAM Framework	[MPLS-TP OAM FW] - work in

| | | |progress |
| | +---------------------------------------+--------------+
	MPLS-TP OAM Analysis	[OAM Analysis]
			- work in
		progress
+-----------+---------------------------------------+--------------+
PW VCCV	Pseudowire Virtual Circuit	RFC 5085
	Connectivity Verification (VCCV):	
	A Control Channel for Pseudowires	
+-----------+---------------------------------------+--------------+
|IPPM | Framework for IP Performance Metrics | RFC 2330 |
| +---------------------------------------+--------------+
| | IPPM Metrics for Measuring | RFC 2678 |
| | Connectivity | |
| +---------------------------------------+--------------+
| | A One-way Delay Metric for IPPM | RFC 2679 |
| +---------------------------------------+--------------+
| | A One-way Packet Loss Metric for IPPM| RFC 2680 |
| +---------------------------------------+--------------+
| | A Round-trip Delay Metric for IPPM | RFC 2681 |
| +---------------------------------------+--------------+
| | A One-way Active Measurement Protocol| RFC 4656 |
| | (OWAMP) | |
| +---------------------------------------+--------------+
| | A Two-Way Active Measurement Protocol| RFC 5357 |
| | (TWAMP) | |
+-----------+---------------------------------------+--------------+
|ITU-T | Operation & Maintenance mechanism |[ITU-T Y.1711] |
|MPLS OAM | for MPLS networks | |
| +---------------------------------------+--------------+
	Assignment of the 'OAM Alert Label'	RFC 3429
	for Multiprotocol Label Switching	
	Architecture (MPLS) Operation and	
	Maintenance (OAM) Functions	
+-----------+---------------------------------------+--------------+
ITU-T	OAM Functions and Mechanisms for	[ITU-T Y.1731]
Ethernet	Ethernet-based Networks	
OAM		
+-----------+---------------------------------------+--------------+
|IEEE | Connectivity Fault Management |[IEEE 802.1ag] |
|CFM | | |

```
+-----------+--------------------------------------+---------------+
|IEEE       | Media Access Control Parameters,     |[IEEE 802.3ah] |
|802.3      | Physical Layers, and Management      |               |
|link level | Parameters for Subscriber Access     |               |
|OAM        | Networks                             |               |
+-----------+--------------------------------------+---------------+
```
                  Table 1 Summary of OAM Standards

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [KEYWORDS].

3. Basic Terminology

3.1. Abbreviations

AIS   Alarm Indication Signal

APS   Automatic Protection Switching

BDI   Backward Defect Indication

BFD   Bidirectional Forwarding Detection

CC   Continuity Check

CCM   Continuity Check Message

CV   Connectivity Verification

DM   Delay Measurement

DTE   Data Terminal Equipment

FDI   Forward Defect Indication

FFD   Fast Failure Detection

ICMP   Internet Control Message Protocol

L2TP   Layer Two Tunneling Protocol

LCCE   L2TP Control Connection Endpoint

   LM   Loss Measurement

   LSP   Label Switching Path

   LSR   Label Switching Router

   MA   Maintenance Association

   ME   Maintenance Entity

   MEG   Maintenance Entity Group

   MEP   Maintenance End Point

   MHF   MIP Half Function

   MIP   Maintenance Intermediate Point

   MP   Maintenance Point

   MPLS   Multiprotocol Label Switching

   MPLS-TP MPLS Transport Profile

   OAM   Operations, Administration, and Maintenance

   PE   Provider Edge

   PW   Pseudowire

   PWE3   Pseudowire Emulation Edge-to-Edge

   RDI   Remote Defect Indication

   TTSI   Trail Termination Source Identifier

   VCCV   Virtual Circuit Connectivity Verification

3.2. Terminology used in OAM Standards

3.2.1. General Terms

   A wide variety of terms is used in various OAM standards. Each of the
   OAM standards listed in the reference section includes a section that
   defines the relevant terms. A thesaurus of terminology for MPLS-TP
   terms is presented in [MPLS-TP Term], and provides a good summary of
   some of the OAM related terminology.

This section presents a comparison of the terms used in various OAM
standards, without fully quoting the definition of each term. For a
formal definition of each term, refer to the references at the end of
this document. The comparison focuses on three basic terms, and is
summarized in [section 3](#)   ..2.6.

[3.2.2](#). OAM Maintenance Entities and Communication Links

A Maintenance Entity (ME) is a point-to-point relationship between
two Maintenance Points (MP). The connectivity between these
Maintenance Points is managed and monitored by the OAM protocol.

A pair of MPs engaged in an ME are connected by a communication Link.
The term "Link" in this context is a generic term that may refer to
one of several types of connection, e.g. a single physical
connection, a set of physical connections, or a virtual link such as
an MPLS LSP. The term Link is used throughout this document to refer
to the connection between the MPs that is monitored by an OAM
protocol.

The term Maintenance Entity (ME) is defined in ITU-T standards (e.g.
[ITU-T Y.1731]). Various terms are used to refer to an ME. For
example, in MPLS LSP Ping ([LSP Ping]) terminology, an ME is simply
referred to as an LSP. BFD does not explicitly use a term that is
equivalent to ME, but rather uses the term "session", referring to
the relationship between two nodes using a BFD protocol.

MPLS-TP has defined the terms ME and Maintenance Entity Group (MEG)
in [MPLS-TP OAM FW], similar to the terms defined by ITU-T.

[3.2.3](#). OAM Maintenance Points

A Maintenance Point (MP) is a functional entity that is defined at a
node in the network, and either initiates or reacts to OAM messages.
A Maintenance End Point (MEP) is one of the end points of an ME, and
can initiate OAM messages and respond to them. A Maintenance
Intermediate Point (MIP) is an intermediate point between two MEPs,
that does not initiate OAM frames, but is able to respond to OAM
frames that are destined to it, and to forward others.

The terms MEP and MIP are defined in ITU-T standards (e.g. [ITU-T
Y.1731]). The term Maintenance Point is a general term for MEPs and
MIPs, and is used in [IEEE 802.1ag].

The 802.1ag defines a finer distinction between Up MPs and Down MPs.
An MP is a bridge interface, that is monitored by an OAM protocol
either in the direction facing the network, or in the direction

facing the bridge. A Down MP is an MP that receives OAM packets from, and transmits them to the direction of the network. An Up MP receives OAM packets from, and transmits them to the direction of the bridging entity.

MPLS-TP has defined the terms MEP and MIP and their functional characteristics in [MPLS-TP OAM FW], similar to the terms defined by ITU-T.

3.2.4. Connectivity Verification and Continuity Checks

Two distinct classes of failure management functions are used in OAM protocols, connectivity verification and continuity checks. The distinction between these terms is defined in [MPLS-TP OAM], and is used similarly in this document.

Continuity checks are used to verify the liveness of a link, and are typically sent proactively, though they can be invoked on-demand as well.

A connectivity verification function allows an MP to check whether it is connected to a peer MP or not. A connectivity verification (CV) protocol typically uses a CV message, followed by a CV reply that is sent back to the originator. A CV function can be applied proactively or on-demand.

Connectivity verification and continuity checks are considered complementary mechanisms, and are often used in conjunction with each other.

3.2.5. Link Failures

The terms Failure, Fault, and Defect are intermittently used in the standards, referring to a malfunction that can be detected by a connectivity or a continuity check. In some standards, such as [IEEE 802.1ag], there is no distinction between these terms, while in other standards each of these terms refers to a different type of malfunction.

The ITU-T distinguishes between these terms in [ITU-T G.806]. The term Fault refers to an inability to perform a required action, e.g., an unsuccessful attempt to deliver a packet. The term Defect refers to an interruption in the normal operation, such as a consecutive period of time where no packets are delivered successfully. The term Failure refers to the termination of the required function. While a Defect typically refers to a limited period of time, a failure refers to a long period of time.

3.2.6. **Summary of OAM Terms used in the Standards**

   Table 2 provides a comparison of the terminology used in different
   OAM standards.

	Maintenance Point Terminology	Maintenance Entity Terminology	Link Failure Terminology
ICMPv4 Ping	-Host -Gateway		
ICMPv6 Ping	Node		
BFD	System	Session	-Failure -Session is declared down
LSP Ping	LSR	LSP	-Failure -Fault = typically a local isolated failure
PW VCCV	-PE -LCCE	PW	-Failure -Fault
IPPM	-Host -End system	-Path -Measurement session	Connectivity is indicated by a Boolean value. Thus, a failure is referred to as a path with a measurement value "false".
ITU-T Y.1711	LSR	LSP	-Fault, Defect, Failure: as defined in [ITU-T G.806]
ITU-T Y.1731	-MEP -MIP	ME	-Fault, Defect, Failure: as defined in [ITU-T G.806]
MPLS-TP OAM	-End Point, MEP -Intermediate Point, MIP	-LSP -PW -Section	-Fault, Defect, Failure: as defined in [ITU-T G.806]

```
+ --------- + ---------- + --------- + ------------------------ +
|IEEE       |-MP (Down,Up)| ME        |-Failure                  |
|802.1ag    |   -MEP      |           |-Fault                    |
|           |   -MIP      |           |-Defect                   |
|           |   -MHF      |           |                          |
+ --------- + ---------- + --------- + ------------------------ +
|IEEE       | DTE         | Link      |-Failure                  |
|802.3ah    |             |           |-Fault                    |
+-----------+------------+-----------+--------------------------+
```
                    Table 2 Summary of OAM Terms

4. OAM Functions

4.1. ICMP Ping

   ICMP provides a connectivity verification function for the Internet
   Protocol. The originator transmits an echo request packet, and the
   receiver replies with an echo reply. ICMP ping is defined in two
   variants, [ICMPv4] is used for IPv4, and [ICMPv6] is used for IPv6.

4.2. Bidirectional Forwarding Detection (BFD)

4.2.1. Overview

   While multiple OAM mechanisms have been defined for various protocols
   in the protocol stack, Bidirectional Forwarding Detection [BFD],
   defined by the IETF BFD working group, is a generic OAM mechanism
   that can be deployed over various encapsulating protocols, and in
   various medium types. The IETF has defined variants of the protocol
   for IP ([BFD IP], [BFD Multi]), for MPLS LSPs [BFD LSP], and for PWE3
   [BFD VCCV]. BFD for MPLS-TP is currently evolving in the MPLS working
   group (e.g. [MPLS-TP Ping BFD]).

   BFD includes two main OAM functions, using two types of BFD packets:
   BFD Control packets, and BFD Echo packets.

4.2.2. BFD Control

   BFD supports a bidirectional continuity check, using BFD control
   packets, that are exchanged within a BFD session. BFD sessions
   operate in one of two modes:

o Asynchronous mode: in this mode BFD control packets are sent
  periodically. When the receiver detects that no BFD control packet
  have been received during a predetermined period of time, a
  failure is detected.

o Demand mode: in this mode, BFD control packets are sent on-demand.
  Upon need, a system initiates a series of BFD control packets to
  verify the link. BFD control packets are sent independently in
  each direction of the link.

Each of the end-points of the monitored path maintains its own
session identification, called a Discriminator, both of which are
included in the BFD Control Packets that are exchanged between the
end-points. At the time of session establishment, the Discriminators
are exchanged between the two-end points. In addition, the
transmission (and reception) rate is negotiated between the two end-
points, based on information included in the control packets. These
transmission rates may be renegotiated during the session.

During normal operation of the session, i.e. no failures are
detected, the BFD session is in the Up state. If no BFD Control
packets are received during a fixed period of time, called the
Detection Time, the session is declared to be Down. The detection
time is a function of the negotiated transmission time, and a
parameter called Detect Mult. Detect Mult determines the number of
missing BFD Control packets that cause the session to be declared as
Down. This parameter is included in the BFD Control packet.

4.2.3. BFD Echo

The echo function is used for connectivity verification. A BFD echo
packet is sent to a peer system, and is looped back to the
originator. The echo function can be used proactively, or on-demand.

4.3. LSP Ping

The IETF MPLS working group has defined OAM for MPLS LSPs. The
requirements and framework of this effort was defined in [MPLS OAM
FW] and [MPLS OAM], respectively. The corresponding OAM mechanism
defined, in this context, is LSP Ping [LSP Ping].

LSP Ping is based on ICMP Ping and just like its predecessor may be
used in one of two modes:

o "Ping" mode: In this mode LSP ping is used for end-to-end
  connectivity verification between two LSRs.

   o "Traceroute" mode: This mode is used for hop-by-hop fault
     localization.

   LSP Ping extends the basic ICMP Ping operation (of data-plane
   connectivity and continuity check) with functionality to verify
   data-plane vs. control-plane consistency for a Forwarding Equivalence
   Class (FEC) and also Maximum Transmission Unit (MTU) problems. The
   traceroute functionality may be used to isolate and localize the MPLS
   faults, using the Time-to-live (TTL) indicator to incrementally
   identify the sub-path of the LSP that is successfully traversed
   before the faulty link or node.

   It should be noted that LSP Ping does support unique identification
   of the LSP within an addressing domain. The identification is checked
   using the full FEC identification. LSP Ping is easily extensible to
   include additional information needed to support new functionality,
   by use of Type-Length-Value (TLV) constructs. The usage of TLVs is
   typically not easy to perform in hardware, and is thus typically
   handled by the control plane.

   LSP Ping supports both asynchronous, as well as, on-demand
   activation. In addition, extensions for LSP Ping are being defined
   for point-to-multipoint LSPs in [P2MP LSP Ping] and for MPLS Tunnels
   in [MPLS LSP Ping].

4.4. PWE3 Virtual Circuit Connectivity Verification (VCCV)

   VCCV, as defined in [VCCV], provides end-to-end fault detection
   and diagnostics for PWs (regardless of the underlying tunneling
   technology). The VCCV switching function provides a control channel
   associated with each PW (based on the PW Associated Channel Header
   (ACH) which is defined in [PW ACH]), and allows sending OAM packets
   in-band with PW data (using CC Type 1: In-band VCCV).

   VCCV currently supports the following OAM mechanisms: ICMP Ping, LSP
   Ping, and BFD. ICMP and LSP Ping are IP encapsulated before being
   sent over the PW ACH. BFD for VCCV supports two modes of
   encapsulation - either IP/UDP encapsulated (with IP/UDP header) or
   PW-ACH encapsulated (with no IP/UDP header) and provides support to
   signal the AC status. The use of the VCCV control channel provides
   the context, based on the MPLS-PW label, required to bind and
   bootstrap the BFD session to a particular pseudo wire (FEC),
   eliminating the need to exchange Discriminator values.

VCCV consists of two components: (1) signaled component to
communicate VCCV capabilities as part of VC label, and (2) switching
component to cause the PW payload to be treated as a control packet.

VCCV is not directly dependent upon the presence of a control plane.
The VCCV capability negotiation may be performed as part of the PW
signaling when LDP is used. In case of manual configuration of the
PW, it is the responsibility of the operator to set consistent
options at both ends.

4.5. IP Performance Metrics (IPPM)

4.5.1. Overview

The IPPM working group [IPPM FW] in the IETF defines common criteria
and metrics for measuring performance of IP traffic. Some of the key
RFCs published by this working group have defined metrics for
measuring connectivity [rfc2678], delay [RFC2679, RFC 2681], and
packet loss [RFC2681].

The IPPM working group has defined not only metrics for performance
measurement, but also protocols that define how the measurement is
carried out. The One-way Active Measurement Protocol [OWAMP] and the
Two-Way Active Measurement Protocol [TWAMP] define a method and
protocol for measuring delay and packet loss in IP networks.

OWAMP [OWAMP] enables measurement of one-way characteristics of IP
networks, such as one-way packet loss and one-way delay. For its
proper operation OWAMP requires accurate time of day setting at its
end points.

TWAMP [TWAMP] is a similar protocol that enables measurement of two-
way (round trip) characteristics. TWAMP does not require accurate
time of day, and, furthermore, allows the use of a simple session
reflector, making it an attractive alternative to OWAMP.

OWAMP and TWAMP use two separate protocols: a Control plane protocol,
and a Test plane protocol.

4.5.2. Control and Test Protocols

OWAMP and TWAMP control protocols run over TCP, while the test
protocols run over UDP. The purpose of the control protocols is to
initiate, start, and stop test sessions, and for OWAMP to fetch
results. The test protocols introduce test packets (which contain
sequence numbers and timestamps) along the IP path under test
according to a schedule, and record statistics of packet arrival.

Multiple sessions may be simultaneously defined, each with a session
identifier, and defining the number of packets to be sent, the amount
of padding to be added (and thus the packet size), the start time,
and the send schedule (which can be either a constant time between
test packets or exponentially distributed pseudo-random). Statistics
recorded conform to the relevant IPPM RFCs.

OWAMP and TWAMP test traffic is designed with security in mind. Test
packets are hard to detect because they are simply UDP streams
between negotiated port numbers, with potentially nothing static in
the packets. OWAMP and TWAMP also include optional authentication
and encryption for both control and test packets.

4.5.3. OWAMP

OWAMP defines the following logical roles: Session-Sender, Session-
Receiver, Server, Control-Client, and Fetch-Client. The Session-
Sender originates test traffic that is received by the Session-
Receiver. The Server configures and manages the session, as well as
returning the results. The Control-Client initiates requests for
test sessions, triggers their start, and may trigger their
termination. The Fetch-Client requests the results of a completed
session. Multiple roles may be combined in a single host - for
example, one host may play the roles of Control-Client, Fetch-Client,
and Session-Sender, and a second playing the roles of Server and
Session-Receiver.

In a typical OWAMP session the Control-Client establishes a TCP
connection to port 861 of the Server, which responds with a server
greeting message indicating supported security/integrity modes. The
Control-Client responds with the chosen communications mode and the
Server accepts the modes. The Control-Client then requests and fully
describes a test session to which the Server responds with its
acceptance and supporting information. More than one test session
may be requested with additional messages. The Control-Client then
starts a test session and the Server acknowledges. The Session-
Sender then sends test packets with pseudorandom padding to the
Session-Receiver until the session is complete or until the Control-
client stops the session. Once finished, the Fetch-Client sends a
fetch request to the server, which responds with an acknowledgement
and immediately thereafter the result data.

4.5.4. TWAMP

TWAMP defines the following logical roles: session-sender, session-
reflector, server, and control-client. These are similar to the

OWAMP roles, except that the Session-Reflector does not collect any packet information, and there is no need for a Fetch-Client.

In a typical TWAMP session the Control-Client establishes a TCP connection to port 862 of the Server, and mode is negotiated as in OWAMP. The Control-Client then requests sessions and starts them. The Session-Sender sends test packets with pseudorandom padding to the Session-Reflector which returns them with insertion of timestamps.

4.6. ITU-T Y.1711

4.6.1. Overview

As mentioned above (4.3.), the IETF defined LSP Ping as an OAM mechanism for MPLS. The ITU-T has also defined an OAM protocol for MPLS, defined in recommendation [ITU-T Y.1711]. This recommendation defines mechanisms for connectivity verification and fast failure detection, as well as mechanism for reporting defects that have been identified in an LSP.

MPLS OAM packets per Y.1711 are detected by a reserved MPLS label value. The reserved value is 14, and is defined in [OAM Label] as the 'OAM Alert Label'.

4.6.2. Connectivity Verification (CV)

The CV function is used to detect connectivity defects in an LSP. CV frames are sent proactively at a rate of 1 per second. Each frame contains the Trail-Termination Source Identifier (TTSI), indicating the identity of the transmitting LSR.

The CV function can detect any of the following defect conditions.

o Loss of Connectivity Verification (LOCV): A loss of connectivity
   is detected when no CV OAM packets are received in a period of 3
   consecutive transmission periods.
   It should be noted that the LOCV defect is in fact loss of
   continuity when using the terminology defined in
3   ..2.4.

o TTSI Mismatch: A TTSI mismatch is detected when a CV frame with an
   unexpected TTSI is received.

o TTSI Mismerge: A TTSI mismerge is detected when the CV frames
   received in a given LSP contain some frame with an expected TTSI,
   and some frames with an unexpected TTSI.

   o Excess: An excess is detected when at least 5 CV frames are
     received during a period of 3 consecutive transmission periods.

4.6.3. **Fast Failure Detection (FFD)**

   The FFD function is a proactive function, used for fast detection of
   connectivity defects. While CV is typically sufficient for path
   failure detection and reporting, protection switching mechanisms
   typically require faster detection. FFD is very similar to CV in
   terms of the packet format, and the possible defect conditions, but
   FFD allows a configurable transmission frequency. The default
   transmission rate of FFD frames is 20 per second, i.e., every 50 ms,
   allowing fast detection for protection switching applications.

4.6.4. **Forward Defect Indication (FDI)**

   The FDI function is used by an LSR to report a defect to affected
   client layers, allowing them to suppress alarms about this defect.
   In MPLS-TP OAM this function is referred to as Client Failure
   Indication.

   FDI packets are sent at a rate of 1 per second.

4.6.5. **Backward Defect Indication (BDI)**

   The BDI function is used by an LSR to inform a peer LSR about a
   defect condition on an LSP for which they are the end points of.
   In MPLS-TP OAM this function is referred to as Remote Defect
   Indication.

   BDI packets are sent at the same transmission rate as FDI.

4.7. **ITU-T Y.1731**

4.7.1. **Overview**

   The [ITU-T Y.1731] defines a protocol for Ethernet OAM. It is
   presented in this document as a reference point. Y.1731 defines
   various OAM functions, including continuity and connectivity
   verification, and functions for performance monitoring.

4.7.2. **ETH-CC**

   The Ethernet Continuity Check function is a proactive function that
   allows a MEP to detect loss of continuity with any of the other MEPs
   in the MEG. This function also allows detection of other defect
   conditions, such as unintended connectivity between two MEGs (also

known as a mismerge). The ETH-CC function is used for one of three
possible applications: fault management, performance monitoring (see
4.6.10.), and protection switching.

Continuity Check Messages (CCM) are transmitted periodically at a
constant rate. There are 7 possible transmission periods, from 3.33
ms to 10 min. When the ETH-CC function detects a defect, it reports
one of the following defect conditions:

o Loss of continuity (LOC): Occurs when at least when no CCM
  messages have been received from a peer MEP during a period of 3.5
  times the configured transmission period.

o Unexpected MEG level: The MEG level is a 3-bit number that defines
  the level of hierarchy of the MEG. This defect condition occurs
  when a CCM is received from a peer MEP with a MEG level that is
  lower than the expected MEG level.

o Mismerge: Occurs when a CCM is received from a peer MEP with an
  unexpected MEG ID.

o Unexpected MEP: Occurs when a CCM is received from a peer MEP with
  an unexpected transmitting MEP ID.

o Unexpected period: Occurs when the transmission period field in
  the CCM does not match the expected transmission period value.

4.7.3. ETH-LB

The Ethernet loopback function verifies connectivity with a peer MEP
or MIP. The loopback function is performed on-demand, by sending a
loopback message (LBM) to the peer MEP or MIP. The peer node then
responds with a loopback reply (LBR).

More precisely, it is used for one of two purposes:

o Bidirectional connectivity test.

o Bidirectional in-service / out-of-service test. The in-service
  mode refers to a test that is run under traffic, while the out-of-
  service test requires other traffic to be halted.

4.7.4. ETH-TST

The test function is very similar to the loopback function, but is
unidirectional, i.e., the ETH-TST PDUs are terminated by the receiver
rather than being looped back to the sender.

4.7.5. **ETH-LT**

   The Ethernet linktrace is an on-demand function that is used for path
   discovery to a given target, or for locating a failure in a broken
   path.

4.7.6. **ETH-AIS**

   The Alarm Indication Signal indicates that a MEG should suppress
   alarms about a defect condition at a lower MEG level, i.e., since a
   defect has occurred in a lower hierarchy in the network, it should
   not be reported by the current node.

   A MEP that detects a failure periodically sends AIS messages to
   higher hierarchies. AIS messages are sent periodically at a
   recommended rate of 1 packet per second, until the defect condition
   is resolved.

4.7.7. **ETH-LCK**

   The lock function is used for administrative locking. A MEP can
   initiate administrative locking, resulting in interruption of data,
   e.g., for out-of-service ETH-LB or ETH-TST.

   A MEP that initiates an administrative locking notifies its peer MEPs
   to halt all relevant traffic until administrative/diagnostic
   condition is removed. ETH-LCK frames are used to report to higher MEG
   levels about the lock. The LCK frame, much like an AIS frame,
   indicates to the receiving MEP that it should suppress alarms about
   the locked link.

4.7.8. **ETH-RDI**

   The Remote Defect Indication allows the sender to indicate that it
   encountered a defect conditions. The receiving MEPs are then aware
   that there is a defect condition in the MEG.

4.7.9. **ETH-APS**

   The Y.1731 standard defines the frame format for Automatic Protection
   Switching frames. The protection switching operations are defined in
   other ITU-T standards.

4.7.10. **ETH-LM**

   The loss measurement function allows a MEP to measure the packet loss
   rate from/to a given MEP in the MEG. Each MEP maintains counters of

   transmitted and received in-profile packets to/from each of its peer
   MEPs. These counters are incorporated in the ETH-LM frames, allowing
   the MEPs to compute the packet loss rate.

   The ETH-LM function measures the far-end loss, referring to traffic
   FROM the MEP to its peer, as well as the near-end loss, referring to
   traffic from the peer MEP TO the local MEP.

   ETH-LM is performed in one of two possible modes:

   o Single-ended LM: in this mode loss measurement is performed on-
     demand. The initiator sends an LM message (LMM) to its peer MEP,
     and the peer responds with an LM reply (LMR).

   o Dual-ended LM: in this mode loss measurement is performed
     proactively. The continuity check message (CCM) is used for
     proactive LM. The LM counters are piggy-backed into the CCM, and
     allow proactive loss measurement.

4.7.11. ETH-DM

   The delay measurement function is an on-demand function that allows a
   MEP to measure the frame delay and frame delay variation to a peer
   MEP.

   ETH-DM can be performed in one of two modes of operation:

   o One-way DM: in this mode, a MEP transmits a 1DM frame containing
     the time of its transmission, TxTimeStampf. The receiving MEP
     receives the 1DM frame and records the time of reception, RxTimef.
     The receiving MEP can then compute the one-way delay by: RxTimef -
     TxTimeStampf.

   o Two-way DM: in this mode, a MEP transmits a delay measurement
     message (DMM) containing its transmission time, TxTimeStampf. The
     peer MEP receives the DMM and responds with a delay measurement
     reply (DMR). Upon receiving the DMR, the initiating MEP records
     the time of its reception, RxTimef, and computes the round trip
     delay by: RxTimef - TxTimeStampf.

   Each MEP maintains a time-of-day clock that is used for timestamping
   delay measurement frames. It should be noted that in one-way DM it is
   implicitly assumed that the clocks of the two peer MEPs are
   synchronized by a time synchronization protocol.

4.8. IEEE 802.1ag

4.8.1. Overview

While the [ITU-T Y.1731] was defined in the ITU-T, the IEEE defined
the [IEEE 802.1ag] as a standard for connectivity fault management in
Ethernet based networks. While the two standards are to some extent
overlapping, they can also be viewed as two complementary parts of a
single Ethernet OAM picture. The two standards use a common packet
format. There are a few differences between the two standards in
terms of terminology: the term MEG level, used in Y.1731, as referred
to as Maintenance Domain level in 802.1ag; the Y.1731 standard uses
the term MEG, while the 802.1ag equivalent is Maintenance Association
(MA).

While Y.1731 defines multiple OAM functions (see section 4.6), the
802.1ag standard focuses on three main OAM functions: continuity
check, loopback, and linktrace, and defines them with great detail.

4.8.2. Continuity Check

See 4.6.2.

4.8.3. Loopback

See 4.6.3.

4.8.4. Linktrace

See 4.6.5.

4.9. IEEE 802.3ah

4.9.1. Overview

The [IEEE 802.3ah] defines Ethernet for the Last Mile (EFM). With
respect to OAM, this standard was designed as an Ethernet link-layer
OAM, for single-hop Ethernet links, allowing to monitor remote
networking devices that are not managed by a centralized management
system. The OAM functions in this standard are described below.

4.9.2. Remote Failure Indication

This function allows a node to notify a peer about a defect in the
receive path. Some physical interfaces allow unidirectional traffic,
where even if one direction of the link fails, the reverse direction
can still be used to convey the remote failure indication.

4.9.3. Remote Loopback

The remote loopback function provides a diagnostic mode that is used
to verify the link connectivity, and to measure the packet loss rate.
When a bridge interface is configured to loopback mode, all incoming
traffic through the interface is looped and sent back to the
originator.

4.9.4. Link Monitoring

Link monitoring provides an event notification function, allowing
peer devices to communicate defect conditions and diagnostic
information.

4.10. MPLS-TP OAM

4.10.1. Overview

The MPLS working group is currently working on defining the OAM
toolset that fulfill the requirements for MPLS-TP OAM. The full set
of requirements for MPLS-TP OAM are defined in [MPLS-TP OAM], and
include both general requirements for the behavior of the OAM
mechanisms and a set of operations that should be supported by the
OAM toolset. The set of mechanisms required are further elaborated
in [MPLS-TP OAM FW], that describes the general architecture of the
OAM system as well as giving overviews of the functionality of the
OAM toolset.

Some of the basic requirements for the OAM toolset for MPLS-TP are:

o MPLS-TP OAM must be able to support both an IP based and non-IP
   based environment. If the network is IP based, i.e. IP routing and
   forwarding are available, then the MPLS-TP OAM toolset should rely
   on the IP routing and forwarding capabilities. On the other hand,
   in environments where IP functionality is not available, the OAM
   tools must still be able to operate without dependence on IP
   forwarding and routing.

o OAM packets and the user traffic are required to be congruent
   (i.e. OAM packets are transmitted in-band) and there is a need to
   differentiate OAM packets from user-plane ones. Inherent in this
   requirement is the principle that MPLS-TP OAM be independent of
   any existing control-plane, although it should not preclude use of
   the control-plane functionality.

4.10.2. Generic Associated Channel

In order to address the requirement for in-band transmission of MPLS-
TP OAM traffic, MPLS-TP uses a Generic Associated Channel (G-ACh),
defined in [G-ACh] for LSP-based OAM traffic. This mechanism is based
on the same concepts as the PWE3 ACH and VCCV mechanisms. However,
to address the needs of LSPs as differentiated from PW, the following
concepts were defined for [G-ACh]:

o An Associated Channel Header (ACH), that uses a format similar to
   the PW Control Word, is a 4-byte header that is added to OAM
   packets.

o A Generic Associated Label (GAL). The GAL is a reserved MPLS label
   value. The reserved value is 13, and indicates the existence of
   the ACH immediately after it.

4.10.3. MPLS-TP OAM Toolset

To address the functionality that is required of the OAM toolset, the
MPLS WG conducted an analysis of the existing IETF and ITU-T OAM
mechanisms and their ability to fulfill the required functionality.
The conclusions of this analysis are documented in [OAM Analysis].
The MPLS working group currently plans to use a mixture of OAM
mechanisms that are based on various existing standards, and adapt
them to the requirements of [MPLS-TP OAM]. Some of the main building
blocks of this solution are based on:

o Bidirectional Forwarding Detection ([BFD], [BFD LSP]) for
   proactive continuity check and connectivity verification.

o LSP Ping as defined in [LSP Ping] for on-demand connectivity
   verification.

o New protocol packets, using G-ACH, to address different
   functionality.

o Performance measurement protocols that are based on the
   functionality that is described in [ITU-T Y.1731].

The following sub-sections describe the OAM tools that will be
defined for MPLS-TP as described in [MPLS-TP OAM FW].

4.10.3.1. Continuity Check and Connectivity Verification

Continuity Check and Connectivity Verification (CC-V) are OAM
operations generally used in tandem, and compliment each other. These

functions are generally run proactively, but may also be used on-
demand, either due to bandwidth considerations or for diagnoses of a
specific condition. Proactively [MPLS-TP OAM] states that the
function should allow the MEPs to monitor the liveness and
connectivity of a transport path. In on-demand mode, this function
should support monitoring between the MEPs and, in addition, between
a MEP and MIP.[MPLS-TP OAM FW] highlights the need for the CC-V
messages to include unique identification of the MEG that is being
monitored and the MEP that originated the message. The function, both
proactively and in on-demand mode, need to be transmitted at regular
rates pre-configured by the operator.

4.10.3.2. Diagnostic Tests

Diagnostic testing is a protocol that allows a network to send
special test data on a transport path. For example, this could be
used as part of bandwidth utilization measurement.

4.10.3.3. Route Tracing

[MPLS-TP OAM] defines that there is a need for functionality that
would allow a path end-point to identify the intermediate and end-
points of the path. This function would be used in on-demand mode.
Normally, this path will be used for bidirectional PW, LSP, and
sections, however, unidirectional paths may be supported only if a
return path exists.

4.10.3.4. Lock Instruct

The Lock Instruct function is used to notify a transport path end-
point of an administrative need to disable the transport path. This
functionality will generally be used in conjunction with some
intrusive OAM function, e.g. Performance measurement, Diagnostic
testing, to minimize the side-effect on user data traffic.

4.10.3.5. Lock Reporting

Lock Reporting is a function used by an end-point of a path to report
to its far-end end-point that a lock condition has been affected on
the path.

4.10.3.6. Alarm Reporting

Alarm Reporting is a function used by an intermediate point of a
path, that becomes aware of a fault on the path, to report to the
end-points of the path. [MPLS-TP OAM FW] states that this may occur
as a result of a defect condition discovered at a server sub-layer.

This generates an Alarm Indication Signal (AIS) that continues until the fault is cleared. The consequent action of this function is detailed in [MPLS-TP OAM FW].

4.10.3.7. Remote Defect Indication

Remote Defect Indication (RDI) is used proactively by a path end-point to report to its peer end-point that a defect is detected on a bidirectional connection between them. [MPLS-TP OAM] points out that this function may be applied to a unidirectional LSP only if there a return path exists. [MPLS-TP OAM FW] points out that this function is associated with the proactive CC-V function.

4.10.3.8. Client Failure Indication

Client Failure Indication (CFI) is defined in [MPLS-TP OAM] to allow the propagation information from one edge of the network to the other. The information concerns a defect to a client, in the case that the client does not support alarm notification.

4.10.3.9. Packet Loss Measurement

Packet Loss Measurement is a function used to verify the quality of the service. This function indicates the ratio of packets that are not delivered out of all packets that are transmitted by the path source.

There are two possible ways of determining this measurement:

o Using OAM packets, it is possible to compute the statistics based on a series of OAM packets. This, however, has the disadvantage of being artificial, and may not be representative since part of the packet loss may be dependent upon packet sizes.

o Sending delimiting messages for the start and end of a measurement period during which the source and sink of the path count the packets transmitted and received. After the end delimiter, the ratio would be calculated by the path OAM entity.

4.10.3.10. Packet Delay Measurement

Packet Delay Measurement is a function that is used to measure one-way or two-way delay of a packet transmission between a pair of the end-points of a path (PW, LSP, or Section). Where:

o One-way packet delay is the time elapsed from the start of
   transmission of the first bit of the packet by a source node until
   the reception of the last bit of that packet by the destination
   node.

o Two-way packet delay is the time elapsed from the start of
   transmission of the first bit of the packet by a source node until
   the reception of the last bit of the loop-backed packet by the
   same source node, when the loopback is performed at the packet's
   destination node.

Similarly to the packet loss measurement this could be performed in
either of the two ways outlined above.

4.11. Summary of OAM Functions

Table 3 summarizes the OAM functions that are supported in each of
the standards that were analyzed in this section.

Standard	Continuity Check	Connectivity Verification	Path Discovery	Defect Indications	Performance Monitoring	Other Functions
ICMP Ping		Echo				
BFD	BFD Control	BFD Echo				
LSP Ping		"Ping" mode	"Traceroute" mode			
PW VCCV		VCCV				
IPPM					-Delay measurement -Packet loss measurement	

```
+ --------- + ----- + ------ + ------ + -------- + ----- + ------ +
|ITU-T      |-CV    |        |        |          |       |        |
|Y.1711     |-FFD   |        |        |          |       |        |
+ --------- + ----- + ------ + ------ + -------- + ----- + ------ +
|ITU-T      |ETH-CC |ETH-LB  |ETH-LT  |-ETH-RDI  |-ETH-LM|-ETH-LCK|
|Y.1731     |       |        |        |-ETH-AIS  |-ETH-DM|-ETH-APS|
|           |       |        |        |          |       |-ETH-TST|
+ --------- + ----- + ------ + ------ + -------- + ----- + ------ +
|IEEE       |CC     |Loopback|Linktrac|          |       |        |
|802.1ag    |       |        |e       |          |       |        |
+ --------- + ----- + ------ + ------ + -------- + ----- + ------ +
|IEEE       |       |Remote  |        |-Remote   |       |        |
|802.3ah    |       |Loopback|        | Failure  |       |        |
|           |       |        |        | Indication|      |        |
|           |       |        |        |-Link     |       |        |
|           |       |        |        | Monitoring|      |        |
+ --------- + ----- + ------ + ------ + -------- + ----- + ------ +
|MPLS-TP    |CC     |CV      |Route   |-Alarm    |-LM    |-Diagnos|
|OAM        |       |        |Tracing | Reporting|-DM    | tic Tes|
|           |       |        |        |-Client   |       | s      |
|           |       |        |        | Failure  |       |-Lock   |
|           |       |        |        | Indication|      |        |
|           |       |        |        |-Remote   |       |        |
|           |       |        |        | Defect   |       |        |
|           |       |        |        | Indication|      |        |
+-----------+-------+--------+--------+-----------+-------+--------+
```

Table 3 Summary of OAM Functions

4.12. Summary of Continuity Check Mechanisms

A key element in some of the OAM standards that are analyzed in this
document is the continuity check. It is thus interesting to present a
more detailed comparison of the connectivity check mechanisms defined
in OAM standards. Table 4 can be viewed as an extension of Table 3,
but is presented separately for convenience. The table compares the
OAM standards that support a continuity check. MPLS-TP is not
included in the comparison, as the continuity check mechanism in
MPLS-TP has not yet been defined.

The "Tx Interval" column in the table specifies the period between
two consequent message transmissions, while the "Source Identifier"
column specifies the name of the field in the OAM packet that is used
as the identifier of the transmitter. The "Error Codes" column

specifies the possible error codes when the unidirectional
connectivity check detects a failure.

	Mechanism	Tx Interval	UC/MC	Source Identifier	Error Codes
BFD	BFD Control	Negotiated during session	UC	My Discriminator	Control Detection Time Expired
ITU-T Y.1711	CV FFD	CV: 1s FFD: parameter, default: 50 ms	UC	TTSI	-Loss of CV (LOCV) -TTSI Mismatch -TTSI Mismerge -Excess
ITU-T Y.1731 / IEEE 802.1ag	CC	7 possible periods: 3 1/3 ms 10 ms 100 ms 1 s 10 s 1 min 10 min	UC/MC	MEP ID	-Loss of Continuity(LOC) -Unexpected MEG level -Mismerge -Unexpected MEP -Unexpected period

Table 4 Summary of OAM Terms

5. Security Considerations

There are no security implications imposed by this document.

6. IANA Considerations

There are no new IANA considerations implied by this document.

7. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

8. References

8.1. Normative References

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

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

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

[MPLS OAM FW] Allan, D., Nadeau, T., "A Framework for Multi-Protocol
               Label Switching (MPLS) Operations and Management
               (OAM)", RFC 4378, February 2006.

[MPLS OAM P2MP] Yasukawa, S., Farrel, A., King, D., and Nadeau, T.,
               "Operations and Management (OAM) Requirements for
               Point-to-Multipoint MPLS Networks", RFC 4687,
               September 2006.

[OAM Label]   Ohta, H., "Assignment of the 'OAM Alert Label' for
               Multiprotocol Label Switching Architecture (MPLS)
               Operation and Maintenance (OAM) Functions", RFC 3429,
               November 2002.

[MPLS-TP OAM] Vigoureux, M., Ward, D., Betts, M., "Requirements for
               OAM in MPLS Transport Networks", RFC 5860, May 2010.

[G-ACh]   Bocci, M., Vigoureux, M., Bryant, S., "MPLS Generic
               Associated Channel", RFC 5586, June 2009.

[VCCV]   Nadeau, T., Pignataro, C., "Pseudowire Virtual Circuit
               Connectivity Verification (VCCV): A Control Channel
               for Pseudowires", RFC 5085, December 2007.

[ICMPv4]   Postel, J., "Internet Control Message Protocol", STD 5,
               RFC 792, September 1981.

[ICMPv6]   Conta, A., Deering, S., and M. Gupta, "Internet Control
               Message Protocol (ICMPv6) for the Internet Protocol
               Version 6 (IPv6) Specification", RFC 4443, March 2006.

   [IPPM FW]   Paxson, V., Almes, G., Mahdavi, J., and Mathis, M.,
                  "Framework for IP Performance Metrics", RFC 2330, May
                  1998.

   [IPPM Con]   Mahdavi, J., Paxson, V., "IPPM Metrics for Measuring
                  Connectivity", RFC 2678, September 1999.

   [IPPM 1DM]   Almes, G., Kalidindi, S., Zekauskas, M., "A One-way
                  Delay Metric for IPPM", RFC 2679, September 1999.

   [IPPM 1LM]   Almes, G., Kalidindi, S., Zekauskas, M., "A One-way
                  Packet Loss Metric for IPPM", RFC 2680, September
                  1999.

   [IPPM 2DM]   Almes, G., Kalidindi, S., Zekauskas, M., "A Round-trip
                  Delay Metric for IPPM", RFC 2681, September 1999.

   [OWAMP]   Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and
                  Zekauskas, M., "A One-way Active Measurement Protocol
                  (OWAMP)", RFC 4656, September 2006.

   [TWAMP]   Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and
                  Babiarz, J., "A Two-Way Active Measurement Protocol
                  (TWAMP)", RFC 5357, October 2008.

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

   [BFD IP]   Katz, D., Ward, D., "Bidirectional Forwarding Detection
                  (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, June
                  2010.

   [BFD Gen]   Katz, D., Ward, D., "Generic Application of
                  Bidirectional Forwarding Detection (BFD)", RFC 5882,
                  June 2010.

   [BFD Multi]   Katz, D., Ward, D., "Bidirectional Forwarding Detection
                  (BFD) for Multihop Paths", RFC 5883, June 2010.

   [BFD LSP]   Aggarwal, R., Kompella, K., Nadeau, T., and Swallow,
                  G., "Bidirectional Forwarding Detection (BFD) for MPLS
                  Label Switched Paths (LSPs)", RFC 5884, June 2010.

   [BFD VCCV]   Nadeau, T., Pignataro, C., "Bidirectional Forwarding
                  Detection (BFD) for the Pseudowire Virtual Circuit
                  Connectivity Verification (VCCV)", RFC 5885, June
                  2010.

[IEEE 802.1ag]"Connectivity Fault Management", December 2007.

[ITU-T Y.1731]"OAM Functions and Mechanisms for Ethernet-based
              Networks", February 2008.

[ITU-T Y.1711]"Operation & Maintenance mechanism for MPLS networks",
              February 2004.

[IEEE 802.3ah]"Media Access Control Parameters, Physical Layers, and
              Management Parameters for Subscriber Access Networks",
              clause 57, September 2004.

8.2. Informative References

[OAM Soup]   Andersson, L., Van Helvoort, H., Bonica, R., Romascanu,
               D., Mansfield, S., "The OAM Acronym Soup", draft-ietf-
               opsawg-mpls-tp-oam-def, June 2010.

[OAM Analysis] Sprecher, N., Bellagamba, E., Weingarten, Y., "MPLS-TP
               OAM Analysis", draft-ietf-mpls-tp-oam-analysis, July
               2010.

[MPLS-TP OAM FW] Busi, I., Niven-Jenkins, B., Allan, D., "MPLS-TP OAM
               Framework", work-in-progress, draft-ietf-mpls-tp-oam-
               framework, July, 2010.

[MPLS-TP Term]Van Helvoort, H., Andersson, L., Sprecher, N., "A
               Thesaurus for the Terminology used in Multiprotocol
               Label Switching Transport Profile (MPLS-TP)
               drafts/RFCs and ITU-T's Transport Network
               Recommendations", draft-ietf-mpls-tp-rosetta-stone,
               May 2010.

[MPLS-TP Ping BFD] Bahadur, N., Aggarwal, R., Ward, D., Nadeau, T.,
               Sprecher, N., Weingarten, Y., "LSP-Ping and BFD
               encapsulation over ACH", draft-ietf-mpls-tp-lsp-ping-
               bfd-procedures, March 2010.

[P2MP Ping]   Saxena, S., Farrel, A. , Yasukawa, S., "Detecting Data
               Plane Failures in Point-to-Multipoint Multiprotocol
               Label Switching (MPLS) - Extensions to LSP Ping",
               draft-ietf-mpls-p2mp-lsp-ping, March 2010.

[ITU-T G.806] "Characteristics of transport equipment - Description
               methodology and generic functionality", January 2009.

Authors' Addresses

   Tal Mizrahi
   Marvell
   6 Hamada St.
   Yokneam, 20692
   Israel

   Email: talmi@marvell.com

   Nurit Sprecher
   Nokia Siemens Networks
   3 Hanagar St. Neve Ne'eman B
   Hod Hasharon,   45241
   Israel

   Email: nurit.sprecher@nsn.com

   Elisa Bellagamba
   Ericsson
   6 Farogatan St.
   Stockholm,   164 40
   Sweden

   Phone: +46 761440785
   Email: elisa.bellagamba@ericsson.com

   Yaacov Weingarten
   Nokia Siemens Networks
   3 Hanagar St. Neve Ne'eman B
   Hod Hasharon,   45241
   Israel

   Phone: +972-9-775 1827
   Email: yaacov.weingarten@nsn.com