Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 5, 2010

N. Sprecher, Ed.
Nokia Siemens Networks
H. van Helvoort, Ed.
Huawei
E. Bellagamba
Ericsson
Y. Weingarten
Nokia Siemens Networks

March 4, 2010

MPLS-TP OAM Analysis
draft-ietf-mpls-tp-oam-analysis-01.txt

Abstract

This document analyzes the set of requirements for Operations, Administration, and Maintenance (OAM) for the Transport Profile of MPLS(MPLS-TP) as defined in [MPLS-TP OAM Reqs], to evaluate whether existing OAM tools (either from the current MPLS toolset or from the ITU-T documents) can be applied to these requirements. Eventually, the purpose of the document is to recommend which of the existing tools should be extended and what new tools should be defined to support the set of OAM requirements for MPLS-TP. This document reports the conclusions of the MPLS-TP design team discussions concerning the MPLS-TP OAM tools at IETF75.

This Internet-Draft will expire on September 5, 2010.

Copyright Notice

Table of Contents

1. Introduction 4
1.1. Scope 4
1.2. Organization of the document 4
1.3. Contributing Authors 5
1.4. LSP Ping 5
1.5. MPLS BFD 6
1.6. PW VCCV 7
1.7. IETF Performance Measurement 8
1.8. ITU Recommendation Y.1731 9
1.9. Acronyms 11
2. Architectural requirements and general principles of operation 11
2.1. Architectural and Principles of Operation - Recommendations and Guidelines 13
3. MPLS-TP OAM Functions 15
3.1. Continuity Check and Connectivity Verification 15
3.1.1. Existing tools 15
3.1.2. Gap analysis 16
3.1.3. Recommendations and Guidelines 17
3.2. Alarm Reporting 17
3.2.1. Existing tools 17
3.2.2. Recommendations and Guidelines 17
3.3. Diagnostic 17
3.3.1. Existing tools 17
3.3.2. Recommendations and Guidelines 18
3.4. Route Tracing 18
3.4.1. Existing tools 18
3.4.2. Recommendations and Guidelines 18
3.5. Loopback tool 18
3.6. Lock Instruct 18
3.6.1. Existing tools 19
3.6.2. Recommendations and Guidelines 19
3.7. Lock Reporting 19
3.7.1. Existing tools 19

3.7.2. Recommendations and Guidelines 19
3.8. Remote Defect Indication 19
3.8.1. Existing tools 19
3.8.2. Recommendations and Guidelines 20
3.9. Client Failure Indication 20
3.9.1. Existing tools 20
3.9.2. Recommendations and Guidelines 20
3.10. Packet Loss Measurement 20
3.10.1. Existing tools 21
3.10.2. Recommendations and Guidelines 21
3.11. Packet Delay Measurement 21
3.11.1. Existing tools 22

3.11.2. Recommendations and Guidelines 22
4. Recommendations 22
5. MPLS-TP OAM Documents Organization 24
5.1. Document 1: "Encapsulation of BFD and LspPing in ACH" . . 24
5.2. Document 2: "Extended BFD" 25
5.3. Document 3: "Extended LSP Ping" 25
5.4. Document 4: "Extensions for Lock Instruct" 26
5.5. Document 5: "AIS and Lock Reporting" 26
5.6. Document 6: "Client Fault Indication" 26
5.7. Document 7: "Packet Loss" 27
5.8. Document 8: "Packet Delay" 27
5.9. Document 9: "Diagnostic Tests" 27
6. IANA Considerations 27
7. Security Considerations 27
8. Acknowledgements 27
Appendix A. Proactive CC and CV BFD tool analysis 27
Appendix A.1. Possible Solution 28
Appendix A.2. Backward compatibility 29
Appendix A.3. Definition of BFDv2 29
Appendix A.3.1. New semantic for Discriminator fields 29
Appendix A.3.2. New MEP ID field 30
Appendix A.4. Two different ACH encapsulation of OAM tool . . . 30
Appendix A.4.1. New tool based on current BFD 31
Appendix A.4.2. New tool based on the extended BFD 31
Appendix A.4.3. New tool like Y.1731 CCM 31
Appendix A.5. Remote Defect Indication 31
Appendix A.6. Point to Multipoint transport paths 32
Appendix A.7. Security Considerations 32
9. Informative References 32

Authors' Addresses 34

1. Introduction

1.1. Scope

OAM (Operations, Administration, and Maintenance) plays a significant role in carrier networks, providing methods for fault management and performance monitoring in both the transport and the service layers in order to improve their ability to support services with guaranteed and strict Service Level Agreements (SLAs) while reducing their operational costs.

[MPLS-TP Reqs] in general, and [MPLS-TP OAM Reqs] in particular define a set of requirements for OAM functionality in MPLS-Transport Profile (MPLS-TP) for MPLS-TP Label Switched Paths (LSPs) (network infrastructure) and Pseudowires (PWs) (services).

The purpose of this document is to analyze the OAM requirements and evaluate whether existing OAM tools defined for MPLS can be used to meet the requirements, identify which tools need to be extended to comply with the requirements, and which new tools need to be defined. We also take the ITU-T OAM toolset, as defined in [Y.1731], as a candidate to base these new tools upon. The existing tools that are

evaluated include LSP Ping (defined in [LSP Ping]), MPLS Bi-directional Forwarding Detection (BFD) (defined in [BASE BFD]) and Virtual Circuit Connectivity Verification (VCCV) (defined in [PW VCCV] and [VCCV BFD]), and the ITU-T OAM toolset defined in [Y.1731].

This document reports the conclusions of the MPLS-TP design team discussions on the MPLS-TP OAM tools at IETF75 and the guidelines that were agreed. The guidelines refer to a set of existing OAM tools that need to be enhanced to fully support the MPLS-TP OAM requirements and identify new tools that need to be defined. The organizational structure of the documents on MPLS-TP OAM tools was also discussed and agreed at IETF75 and is described later in this document.

1.2. Organization of the document

Sections 1.4 - 1.8 provide an overview of the existing MPLS tools.

Section 2 of the document analyzes the requirements that are documented in [MPLS-TP OAM Reqs] and provides basic principles of operation for the OAM functionality that is required.

Section 3 evaluates which existing tools can provide coverage for the different OAM functions that are required to support MPLS-TP.

The recommendations are summarized in section 4, and reflect the

guidelines which were agreed by the MPLS-TP design team during the meetings at IETF 75. These guidelines relate to the functionality could be covered by the existing toolset and what extensions or new tools would be needed in order to provide full coverage of the OAM functionality for MPLS-TP.

The OAM tools for MPLS-TP OAM will be defined in a set of documents. Section 5 describes the organization of this set of documents as agreed by the MPLS-TP design team at IETF75.

1.3. Contributing Authors

Yaakov Stein (Rad), Annamaria Fulignoli (Ericsson), Italo Busi (Alcatel Lucent)

1.4. LSP Ping

LSP Ping is a variation of ICMP Ping and traceroute [ICMP] adapted to the needs of MPLS LSP. Forwarding, of the LSP Ping packets, is based upon the LSP Label and label stack, in order to guarantee that the echo messages are switched in-band (i.e. over the same data route) of the LSP. However, it should be noted that the messages are transmitted using IP/UDP encapsulation and IP addresses in the 127/8 (loopback) range. The use of the loopback range guarantees that the LSP Ping messages will be terminated, by a loss of connectivity or inability to continue on the path, without being transmitted beyond the LSP. For a bi-directional LSP (either associated or co-routed) the return message of the LSP Ping could be sent on the return LSP. For unidirectional LSPs and in some case for bi-directional LSPs, the return message may be sent using IP forwarding to the IP address of the LSP ingress node.

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.

As mentioned above, LSP Ping requires the presence of the MPLS control plane when verifying the consistency of the data-plane against the control-plane. However, LSP Ping is not dependent on the MPLS control-plane for its operation, i.e. even though the propagation of the LSP label may be performed over the control-plane via the Label Distribution Protocol (LDP).

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.

LSP Ping can be activated both in on-demand and pro-active (asynchronous) modes, as defined in [MPLS-TP OAM Reqs].

[P2MP LSP Ping] clarifies the applicability of LSP Ping to MPLS P2MP LSPs, and extends the techniques and mechanisms of LSP Ping to the MPLS P2MP environment.

[MPLS LSP Ping] extends LSP Ping to operate over MPLS tunnels or for a stitched LSP.

As pointed out above, TTL exhaust is the method used to terminate flows at intermediate LSRs. This is used as part of the traceroute of a path and to locate a problem that was discovered previously.

Some of the drawbacks identified with LSP Ping include - LSP Ping is considered to be computational intensive as pointed out in [MPLS BFD]. The applicability for a pro-active mode of operation is analyzed in the sections below. Use of the loopback address range (to protect against leakage outside the LSP) assumes that all of the intermediate nodes support some IP functionality. Note that ECMP is not supported in MPLS-TP, therefore its implication on OAM capabilities is not analyzed in this document.

1.5. MPLS BFD

BFD (Bidirectional Forwarding Detection) [BASE BFD] is a mechanism that is defined for fast fault detection for point-to-point connections. BFD defines a simple packet that may be transmitted over any protocol, dependent on the application that is employing the mechanism. BFD is dependent upon creation of a session that is agreed upon by both ends of the link (which may be a single link, LSP, etc.) that is being checked. The session is assigned a separate identifier by each end of the path being monitored. This session identifier is by nature only unique within the context of node that assigned it. As part of the session creation, the end-points negotiate an agreed transmission rate for the BFD packets. BFD supports an echo function to check the continuity, and verify the reachability of the desired destination. BFD does not support neither a discovery mechanism nor a traceroute capability for fault localization, these must be provided by use of other mechanisms. The BFD packets support authentication between the routers being checked.

BFD can be used in pro-active (asynchronous) and on-demand modes, as

defined in [MPLS-TP OAM Reqs], of operation.

[MPLS BFD] defines the use of BFD for P2P LSP end-points and is used to verify data-plane continuity. It uses a simple hello protocol which can be easily implemented in hardware. The end-points of the LSP exchange hello packets at negotiated regular intervals and an end-point is declared down when expected hello packets do not show up. Failures in each direction can be monitored independently using the same BFD session. The use of the BFD echo function and on-demand activation are outside the scope of the MPLS BFD specification.

The BFD session mechanism requires an additional (external) mechanism to bootstrap and bind the session to a particular LSP or FEC. LSP Ping is designated by [MPLS BFD] as the bootstrap mechanism for the BFD session in an MPLS environment. The implication is that the session establishment BFD messages for MPLS are transmitted using a IP/UDP encapsulation.

In order to be able to identify certain extreme cases of mis-connectivity, it is necessary that each managed connection have its own unique identifiers. BFD uses Discriminator values to identify the connection being verified, at both ends of the path. These discriminator values are set by each end-node to be unique only in the context of that node. This limited scope of uniqueness would not identify a misconnection of crossing paths that could assign the same discriminators to the different sessions.

1.6. PW VCCV

[PW 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.

1.7. IETF Performance Measurement

OWAMP (One-Way Active Measurement Protocol) [RFC4656] enables measurement of unidirectional characteristics of IP networks, such as packet loss and one-way delay. For its proper operation OWAMP requires accurate time of day setting at its end points.

TWAMP (Two-Way Active Measurement Protocol) [RFC5357] 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.

Both OWAMP and TWAMP consist of inter-related control and test protocols, although "TWAMP Light" eliminates the need for the control protocol.

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 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.

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.

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.

1.8. ITU Recommendation Y.1731

[Y.1731] specifies a set of OAM procedures and related packet data

unit (PDU) formats that meet the transport network requirements for OAM. These PDU and procedures address similar requirements to those outlined in [MPLS-TP OAM Reqs].

The PDU and procedures defined in [Y.1731] are described for an Ethernet environment, with the appropriate encapsulation for that environment. However, the actual PDU formats are technology agnostic and could be carried over different encapsulations, e.g. VCCV control channel. The OAM procedures, likewise, could be supported by

MPLS-TP nodes just as they are supported by Ethernet nodes.

[Y.1731] describes procedures to support the following OAM functions:

- Connectivity and Continuity Monitoring - for pro-active mode end-to-end checking
- Loopback functionality - to verify connectivity to intermediate nodes in an on-demand mode
- Link Trace - provides information on the intermediate nodes of the path being monitored, may be used for fault localization. This is activated in an on-demand mode.
- Alarm Indication Signaling - for alarm suppression in case of faults that are detected at the server layer, activated pro-actively.
- Remote Defect Indication - as part of the Connectivity and Continuity Monitoring packets, performed pro-actively
- Locked Signal - for alarm suppression in case of administrative locking at the server layer. This function is performed pro-actively.
- Performance monitoring - including measurement of packet delays both uni and bi-directional (on-demand), measurement of the ratio of lost packets (pro-active), the effective bandwidth that is supported without packet loss, and throughput measurement.

The PDU defined in [Y.1731] includes various information elements (fields) including information on the MEG-Level, etc. Addressing of

the PDU as defined in [Y.1731] is based on the MAC Address of the nodes, which would need to be adjusted to support other addressing schemes. The addressing information is carried in <Type, Length, Value> (TLV) fields that follow the actual PDU. In the LBM PDU the MAC address is used to identify the MIP to which the message is intended

1.9. Acronyms

This draft uses the following acronyms:

AC	Attachment Circuit
ACH	Associated Channel Header
BFD	Bidirectional Forwarding Detection
CC-V	Continuity Check and Connectivity Verification
FEC	Forwarding Equivalence Class
G-ACH	Generic Associated Channel Header
LDP	Label Distribution Protocol
LSP	Label Switched Path
MPLS-TP	Transport Profile for MPLS
OAM	Operations, Administration, and Maintenance
OWAMP	One Way Active Measurement Protocol
PDU	Packet Data Unit
PW	Pseudowire
RDI	Remote Defect Indication
SLA	Service Level Agreement
TLV	Type, Length, Value
TTL	Time-to-live
TWAMP	Two Way Active Measurement Protocol
VCCV	Virtual Circuit Connectivity Verification

2. Architectural requirements and general principles of operation

[MPLS-TP OAM Reqs] defines a set of requirements on OAM architecture and general principles of operations which are evaluated below:

- [MPLS-TP OAM Reqs] requires that OAM mechanisms in MPLS-TP are independent of the transmission media and of the client service being emulated by the PW. The existing tools comply with this requirement.

- [MPLS-TP OAM Reqs] requires that the 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 MUST be able to operate by relying on the IP routing and forwarding capabilities. All of the existing MPLS tools (i.e. LSP Ping, VCCV Ping, MPLS BFD, and VCCV BFD) can support this functionality. The Y.1731 toolset does not specifically support this functionality, but rather relies on underlying technologies for forwarding. The forwarding could also be supported over IP, e.g. by using a VCCV extension. Note that some of the MPLS-TP tools such as Alarm Report are very transport oriented and may not support IP functionality.

- [MPLS-TP OAM Reqs] requires that MPLS-TP OAM MUST be able to operate without IP functionality and without relying on control and/or management planes. It is required that OAM functionality MUST NOT be dependent on IP routing and forwarding capabilities. Except for the LSP Ping operation of verifying the data-plane vs. the control-plane, the existing tools do not rely on control and/or management plane, however the following should be observed regarding the reliance on IP functionality:

  * LSP Ping, VCCV Ping, and MPLS BFD make use of IP header (UDP/IP) and do not completely comply with the requirement. In the on-demand mode, LSP Ping also may use IP forwarding to reply back to the source router. This dependence on IP, has further implications concerning the use of LSP Ping as the bootstrap mechanism for BFD for MPLS. There are extensions to LSP-Ping that are under discussion that allow LSP-Ping to restrict replies to the backside of a bidirectional LSP.

    * VCCV BFD supports the use of PW-ACH encapsulated BFD sessions for PWs and can comply with the requirement.

    * Y.1731 PDU are technology agnostic and thereby not dependent on IP functionality. These PDU could be carried by VCCV or G-ACH control channels.

- [MPLS-TP OAM Reqs] requires that OAM tools for fault management do not rely on user traffic, and the existing MPLS OAM tools and Y.1731 already comply with this requirement.

- It is also required that OAM packets and the user traffic are congruent (i.e. OAM packets are transmitted in-band) and there is a need to differentiate OAM packets from user-plane ones.

    * For PWs, VCCV provides a control channel that can be associated with each PW which allows sending OAM packets in band of PWs and allow the receiving end-point to intercept, interpret, and process them locally as OAM messages. VCCV defines different VCCV Connectivity Verification Types for MPLS (like ICMP Ping, LSP Ping and IP/UDP encapsulated BFD and PW-ACH encapsulated BFD).

    * Currently there is no distinct OAM payload identifier in MPLS shim. BFD and LSP Ping packets for LSPs are carried over UDP/IP and are addressed to the loopback address range. The router at the end-point intercepts, interprets, and processes the packets. [MPLS G-ACH] generalizes the use of the PW ACH and enables provision of control channels at the MPLS LSP and sections levels. This new mechanism would support carrying the

existing MPLS OAM messages or the Y.1731 messages at the LSP and the section levels to be transmitted over the G-ACH.

- [MPLS-TP OAM Reqs] requires that the MPLS-TP OAM mechanism allows the propagation of AC (Attachment Circuit) failures and their clearance across a MPLS-TP domain

    * BFD for VCCV supports a mechanism for "Fault detection and AC/PW Fault status signaling." This can be used for both IP/UDP encapsulated or PW-ACH encapsulated BFD sessions, i.e. by setting the appropriate VCCV Connectivity Verification

Type.This mechanism could support this requirement. Note that in the PWE3 WG there are two proposals regarding how to transmit the AC failures over an ACH that may be applicable to this requirement.

- [MPLS-TP OAM Reqs] requires a single OAM technology and consistent OAM capabilities for LSPs, PWs, and Sections. The existing set of tools defines a different way of operating the OAM functions (e.g. LSP Ping to bootstrap MPLS BFD vs. VCCV). Currently, the Y.1731 functionality is defined for Ethernet paths, and the procedures could readily be redefined for the various MPLS-TP path concepts.

- [MPLS-TP OAM Reqs] requires allowing OAM packets to be directed to an intermediate point of a LSP/PW. Technically, this could be supported by the proper setting of the TTL value. It is also recommended to include the identifier of the intermediate point within the OAM message to allow the intermediate point to validate that the message is really intended for it. The information can be included in an ACH-TLV according to the definitions in [MPLS-TP ACH TLV]. The applicability of such a solution needs to be examined per OAM function. For details, see below.

- [MPLS-TP OAM Reqs] suggests that OAM messages MAY be authenticated. BFD defines support for optional authentication fields using different authentication methods as defined in [BASE BFD]. Other tools should support this capability as well. Y.1731 functionality uses the identification of the path for authentication. Authentication information could be included in an optional TLV field according to the definitions in [MPLS-TP ACH TLV] when not available in the OAM PDU.

2.1. Architectural and Principles of Operation - Recommendations and Guidelines

Based on the requirements analysis above, the following guidelines should be followed to create an OAM environment that could more fully support the requirements cited:

- Define a generalized addressing scheme that can also support unique identification of the monitored paths (or connections).

- Use G-ACH for LSP and section levels.

- Define architectural element that is based on LSP hierarchy to apply the mechanisms to segments and concatenated segments.

- Apply BFD to these new mechanisms using the control channel encapsulation, as defined above - allowing use of BFD for MPLS-TP independent of IP functionality. This could be used to address the CC-V functionality, described below.

- Similarly, LSP Ping could be extended to use only the LSP path (in both directions) without IP Forwarding. Addressing for PW can be included by using the VCCV mechanism. LSP Ping could be used to address the CC-V, Route Tracing, RDI, and Lock/Alarm Reporting functionality cited in the requirements.

- The Y.1731 PDU set could be used as a basis for defining the information units to be transmitted over the G-ACH. The actual procedures and addressing schemes would need to be adjusted for the MPLS-TP environment.

- Define a mechanism that could be used to idnetify an intermediate point of a path in a unique way, to support the maintenance functions. This addressing should be flexible to allow support for different addressing schemes, and would supplement the TTL exception mechanism to allow an OAM packet to be intercepted by intermediate nodes.

Creating these extensions/mechanisms would fulfill the following architectural requirements, mentioned above:

- Independence of IP forwarding and routing, when needed.

- OAM packets should be transmitted in-band.

- Support a single OAM technology for LSP, PW, and Sections.

In addition, the following additional requirements can be satisfied:

- Provide the ability to carry other types of communications (e.g., APS, Management Control Channel (MCC), Signaling Control Channel (SCC)), by defining new types of communication channels for PWs, Sections, and LSPs.

- The design of the OAM mechanisms for MPLS-TP MUST allow the ability to support vendor specific and experimental OAM functions.

3. MPLS-TP OAM Functions

The following sections discuss the required OAM functions that were identified in [MPLS-TP OAM Reqs].

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 may be split into separate mechanisms. Together they are used to detect loss of traffic continuity and misconnections between path end-points and are useful for applications like Fault Management, Performance Monitoring and Protection Switching, etc. To guarantee that CC-V can identify misconnections from cross-connections it is necessary that the tool use network-wide unique identifiers for the path that is being checked in the session.

3.1.1. Existing tools

LSP Ping provides much of the functionality required for co-routed bidirectional LSPs. As observed above, LSP Ping may be operated in both asynchronous and on-demand mode. Addressing is based on the full FEC identification that provides a unique identifier, and the basic functionality only requires support for the loopback address range in each node on the LSP path.

BFD defines functionality that can be used to support the pro-active OAM CC-V function when operated in the asynchronous mode. However, the current definition of basic BFD is dependent on use of LSP Ping to bootstrap the BFD session. Regarding the connectivity functional aspects, basic BFD has a limitation that it uses only locally unique (to each node) session identifiers.

VCCV can be used to carry either LSP Ping or BFD packets that are not IP/UDP encapsulated for CC-V on a PW. Note that PW termination/ switching points use only locally unique (to each node) labels. The PW label identifies the path uniquely only at the LSP level.

Y.1731 provides functionality for all aspects of CC-V for an Ethernet environment, this could be translated for the MPLS-TP environment. The CCM PDU defined in [Y.1731] includes the ability to set the frequency of the messages that are transmitted, and provides for attaching the address of the path (in the Ethernet case - the MEG

Level) and a sequencing number to verify that CCM messages were not

dropped.

3.1.2. Gap analysis

LSP Ping could be used to cover the cases of co-routed bidirectional LSPs. However, there is a certain amount of computational overhead involved with use of LSP Ping (as was observed in sec 1.1), the verification of the control-plane, and the need to support the loopback functionality at each intermediate node. LSP Ping uses a fully qualified LSP identifier, and when used in conjunction with VCCV would use the PW label to identify the transport path. LSP Ping can be extended to bypass the verification of the control plane

BFD could be extended to fill the gaps indicated above. The extension would include:

- A mechanism should be defined to carry BFD packets over LSP without reliance on IP functionality.
- A mechanism should be defined to bootstrap BFD sessions for MPLS that is not dependent on UDP.
- BFD needs to be used in conjunction with "globally" unique identifiers for the path or ME being checked to allow connectivity verfication support. There are two possibilities, to allow BFD to support this new type of identifier -
  - Change the semantics of the two Discriminator fields that exist in BFD and have each node select the ME unique identifier. This may have backward compatibility implications.
  - Create a new optional field in the packet carrying the BFD that would identify the path being checked, in addition to the existing session identifiers.
- Extensions to BFD would be needed to cover P2MP connections.

Use of the Y.1731 functionality is another option that could be considered. The basic PDU for CCM includes (in the flags field) an indication of the frequency of the packets [eliminating the need to

"negotiate" the frequency between the end-points], and also a flag used for RDI. The procedure itself would need adaptation to comply with the MPLS environment.

An additional option would be to create a new tool that would give coverage for both aspects of CC-V according to the requirements and the principles of operation (see section 2.1). This option is less preferable.

3.1.3. Recommendations and Guidelines

Extend LSP Ping to fully support the on-demand Connectivity Verification function resolving the gaps described above. Extend BFD to support proactive Continuity Check & Connectivity Verification (CC-V) resolving the gaps described above.

Note that [MPLS BFD] defines a method for using BFD to provide verification of multipoint or multicast connectivity.

3.2. Alarm Reporting

Alarm Reporting is a function that is used by an intermediate point in a path to notify the end-points of the path of a fault or defect condition indirectly affecting that path. Such information may be used by the endpoints, for example, to suppress alarms that may be generated by maintenance end-points of the path. This function should also have the capability to differentiate an administrative lock from a failure condition at a different execution level.

3.2.1. Existing tools

There is no mechanism defined in the IETF to support this function. Y.1731 does define a PDU and procedure for this functionality.

3.2.2. Recommendations and Guidelines

Define a new tool and PDU to support Alarm Reporting. The PDU should be transmitted over a G-ACH. The frequency of transmision after the alarm is raised and the continued frequency until it is cleared should be indicated in the definition.

Describe also how the Alarm Reporting functionality may be supported

in the control-plane and management-plane.

3.3. Diagnostic

A diagnostic test is a function that is used between path end-points to verify bandwidth throughput, packet loss, bit errors, etc. This is usually performed by sending packets of varying sizes at increasing rates (until the limits of the service level) to measure the actual utilization.

3.3.1. Existing tools

There is no mechanism defined in the IETF to support this function. [Y.1731] describes a function that is dependent on sending a series of TST packets (this is a PDU whose size can be varied) at differing

frequencies.

3.3.2. Recommendations and Guidelines

Define a new tool and PDU to support Diagnostic.

3.4. Route Tracing

Functionality of route determination is used to determine the route of a connection across the MPLS transport network. [MPLS-TP OAM Reqs] defines that this functionality MUST allow a path end-point to identify the intermediate and end-points of the path. This functionality MUST support co-routed bidirectional paths, and MAY support associated bidirectional and unidirectional p2p paths, as well as p2mp unidirectional paths. Unidirectional path support is dependent on the existence of a return path to allow the original end-point to receive the trace information.

3.4.1. Existing tools

LSP Ping supports a trace route function that could be used for bidirectional paths. Support of unidirectional paths would be dependent on the ability of identifying a return path.

3.4.2. Recommendations and Guidelines

Extend LSP Ping to support the Route Trace functionality and to address additional options, i.e. PW and p2mp unidirectional LSP.

3.5. Loopback tool

Editor's note: In recent discussions a requirement was raised to support multiple maintenance points on a single node and the definition of the Loopback function that would appropriately test theconnectivity of these MP in order to identify fault location. This functionality must be more fully specified in the OAM Framework document before further analysis.

3.6. Lock Instruct

The Lock instruct function allows the system to block off transmission of data along a LSP. When a path end-point receives a command, e.g. from the management system, that the path is blocked, the end-point informs the far-end that the path has been locked and that no data should be transmitted. This function is used on-demand.

3.6.1. Existing tools

There is no mechanism defined in the IETF to support this function, but LSP Ping could be extended to support this functionality between the path endpoints. Y.1731 does define a PDU and procedure for this functionality.

3.6.2. Recommendations and Guidelines

Extend LSP Ping to support Lock instruct. The frequency at which these messages are transmitted until the lock situation is cleared, should be clearly indicated.

3.7. Lock Reporting

Lock reporting is used by an intermediate point to notify the end points of a transport path (that the intermediate point is a member of) that an external lock condition exits for this transport path. This function is used proactively.

3.7.1. Existing tools

There is no mechanism defined in neither the IETF nor in Y.1731 to support this function.

3.7.2. Recommendations and Guidelines

Define a new tool and PDU to support Lock reporting. This tool could be designed similarly to the Alarm Reporting tool (described above), but would need to be initiated by an intermediate point of the transport path.

3.8. Remote Defect Indication

Remote Defect Indication (RDI) is used by a path end-point to notify its peer end-point that a defect, usually a unidirectional defect, is detected on a bi-directional connection between them.

This function should be supported in pro-active mode.

3.8.1. Existing tools

There is no mechanism defined in the IETF to fully support this functionality, however BFD supports a mechanism of informing the far-end that the session has gone down, and the Diagnostic field indicates the reason. Similarly, when LSP Ping is used for a co-routed bidirectional LSP the far-end LER could notify that there was a misconnectivity.

In [Y.1731] this functionality is defined as part of the CC-V function as a flag in the PDU.

3.8.2. Recommendations and Guidelines

Extend BFD (which is recommended to be used for proactive CC-V) to transmit the signal of Remote Defect Indication without disrupting the CC-V functionality. Such an extension could be similar to that suggested by the ITU recommendation.

3.9. Client Failure Indication

Client Failure Indication (CFI) function is used to propagate an indication of a failure to the far-end sink when alarm suppression in the client layer is not supported.

3.9.1. Existing tools

There is a possibility of using the BFD over VCCV mechanism for "Fault detection and AC/PW Fault status signaling". However, there is a need to differentiate between faults on the AC and the PW. In the PWE3 WG there are some proposals regarding how to transmit the CFI over an ACH.

3.9.2. Recommendations and Guidelines

Use PWE3 tool to propagate Client Fail Indication via an ACH.

3.10. Packet Loss Measurement

Packet Loss Measurement is a function that is 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 -

- 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.

- 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.

3.10.1. Existing tools

There is no mechanism defined in the IETF to support this function. [Y.1731] describes a function that is based on sending the CCM packets [used for CC-V support (see sec 3.1)] for proactive support

and specialized loss-measurement packets for on-demand measurement. These packets include information (in the additional TLV fields) of packet counters that are maintained by each of the end-points of a path. These counters maintain a count of packets transmitted by the ingress end-point and the count of packets received from the far-end of the path by the egress end-point.

3.10.2. Recommendations and Guidelines

One possibility is to define a mechanism to support Packet Loss Measurement, based on the delimiting messages. This would include a way for delimiting the periods for monitoring the packet transmissions to measure the loss ratios, and computation of the ratio between received and transmitted packets.

A second possibility would be to define a functionality based on the description of the loss-measurement function defined in [Y.1731] that is dependent on the counters maintained, by the MPLS LSR (as described in [RFC3813], of received and transmitted octets. Define a new PDU for the message that utilizes G-ACH. This option appears more suitable for performance monitoring statistics, which in transport applications are based on the continuous monitoring of the traffic interested (100 ms gating).

3.11. 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:

- 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.

- 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 one of two ways -

- Using OAM packets - checking delay (either one-way or two-way) in transmission of OAM packets. May not fully reflect delay of larger packets, however, gives feedback on general service level.

- Using delimited periods of transmission - may be too intrusive on the client traffic.

3.11.1. Existing tools

There is no mechanism defined in the IETF toolset that fulfills all of the MPLS-TP OAM requirements.

[Y.1731] describes a function in which specific OAM packets are sent with a transmission time-stamp from one end of the managed path to the other end (these are transparent to the intermediate nodes). The delay measurement is supported for both one-way and two-way measurement of the delay. It should be noted that the functionality on the one-way delay measurement is dependent upon a certain degree of synchronization between the time clocks of the two-ends of the transport path.

3.11.2. Recommendations and Guidelines

Define a mechanism that would support Packe Delay Measurement, based on the procedures defined in [Y.1731]. The mechanism should be based on measurement of the delay in transmission and reception of OAM packets, transmitted in-band with normal traffic. Define an appropriate PDU that would utilize the G-ACH.

4. Recommendations

As indicated above, LSP-Ping could easily be extended to support some of the functionality between the path end-points and between an end-point of a path and an intermediate point. BFD could also be extended to support some of the functions between the end-points of a path. Some of the OAM functions defined in [Y.1731] (especially for performance monitoring) could also be adapted.

The guidelines that are used in this document are as follows:

- Re-use/extend existing IETF protocols wherever applicable.

- Define new message format for each of the rest of the OAM functions, which are aligned with the ACH and ACH-TLV definitions, and includes only relevant information.

- Adapt Y.1731 functionality where applicable (mainly for performance monitoring).

The recommendations on the MPLS-TP OAM tools are as follows:

- Define a maintenance entity that could be applied both to LSPs and PWs that would support management of a sub-path. This entity should allow for transmission of traffic by means of label stacking and proper TTL setting.

- Extend the control and the management planes to support the configuration of the OAM maintenance entities and the set of functions to be supported by these entities.

- Define a mechanism that would allow the unique addressing of the elements that need to be monitored, e.g., the connections, end-points, and intermediate points of a path. This mechanism needs to be flexible enough to support different addressing schemes, e.g. IP addresses, NSAP, connection names. As pointed out above, LSP Ping uses the full FEC identifier for the LSP - this could easily be applied to Section OAM since this would be considered as a stacked LSP.

- The appropriate assignment of network-wide unique identifiers for transport paths, needed to support connectivity verification, should be considered.

- Extend existing MPLS tools to disengage from IP forwarding mechanisms.

- Extend BFD to support the proactive CC-V functionalities. The extensions should address the gaps described above.

- Extend LSP Ping to support the on-demand Connectivity Verification functionality. The extensions should address the gaps described above.

- Define a new PDU which will be transmitted over G-ACH to support the Alarm Reporting functionality for data-plane implementations. Describe how Alarm Reporting can be supported by a control-plane and by a management-plane.

- Define a new PDU which will be transmitted over G-ACH to support the Lock Reporting functionality. Use the same procedures as for Alarm Reporting.

- Extend BFD to support the Remote Defect Indication (RDI) functionality. The extensions should address the gaps described

above.

- Extend LSP-Ping to support the Route tracing functionality. The extensions should address the gaps described above.

- Extend LSP-Ping to support the Lock Instruct functionality between end-points of a path. The extensions should address the gaps described above.

- Use PWE3 tool to transmit Client Fault Indication (CFI) via ACH. There are already some proposals in the PWE3 WG.

- Define a new PDU which will be transmitted over G-ACH to support the Packet Loss Measurement functionality. Base the functionality on the procedures defined in Y.1731.

- Define a new PDU which be transmitted over G-ACH to support the Packet Delay Measurement functionality. Base the functionality on the procedures defined in Y.1731. For one-way delay measurement define mechanisms to ensure a certain degree of synchronization between the time clocks of the two-ends of the transport path.

- Define a new PDU which be transmitted over G-ACH to support the Diagnostic functionality.

- The tools may have the capability to authenticate the messages. The information may be carried in a G-ACH TLV.

5. MPLS-TP OAM Documents Organization

The following paragraphs list the set of documents necessary to cover the OAM functionalities analyzed above. This compilation of documents is one of the outcomes of the MEAD team discussions that took place during IETF75 in Stockholm.

It should be noted that the various document titles listed here may not reflect the draft titles that will be chosen at the time that the drafts are written, but they serve just as a topic pointer from the current analysis.

5.1. Document 1: "Encapsulation of BFD and LspPing in ACH"

The scope of the document is to define the usage of LSP Ping and BFD in both IP and IP-less environments. As described in the following paragraphs, BFD and Lsp Ping need to be extended in order to be compliant with [MPLS-TP OAM Reqs]. However, this document should be focused on the existing Lsp Ping and BFD, without necessarily

referring to their extended versions.

The draft "nitinb-mpls-tp-lsp-ping-bfd-procedures" will be considered as the starting point for this definition.

In particular, the following sections will be taken into account for the scope:

- nitinb-mpls-tp-lsp-ping-bfd-procedures section 2 ("LSP-Ping extensions") for addressing the "Lsp Ping encapsulation in ACH"
- nitinb-mpls-tp-lsp-ping-bfd-procedures section 5 ("Running BFD over MPLS-TP LSPs") for addressing the "BFD encapsulation in ACH"

5.2. Document 2: "Extended BFD"

The scope of the document is to define the BFD extension and behavior to meet the requirements for MPLS-TP proactive Continuity Check and Connectivity Verification functionality and the RDI functionality as defined in [MPLS-TP OAM Reqs].

The document will likely take the name "draft-asm-mpls-tp-bfd-cc-cv-00" and will be formed by the merging of the following two drafts:

- draft-fulignoli-mpls-tp-bfd-cv-proactive-and-rd
- draft-boutros-mpls-tp-cc-cv-01.txt

5.3. Document 3: "Extended LSP Ping"

The scope of the document is to define:

- A place holder for On Demand Connectivity Verification if LSP Ping needs to be enhanced over and above the encapsulations changes (defined in Document 1 "Encapsulation of BFD and LSP Ping in ACH").

- Usage of LSP Ping with MIPs and MEPs, which is partially covered in nitinb-mpls-tp-lsp-ping-bfd-procedures.

- Route Trace. This topic has already been partially covered in "draft-boutros-mpls-tp-path-trace-00" and "nitinb-mpls-tp-lsp-ping-bfd-procedures", which will be considered as starting point for the Route Trace functionality included in Document 3. The Route Trace section should also cover these aspects:

  * LSP Ping Loose ends. This section will describe what to do when receiving an LSP Ping with MIP and MEP ids.

  * In an IP-Less environment Route Trace works only in co-routed bidirectional LSP.

  * In Y.1731 the CV function is separate from the Route Trace function, it should be captured how LSP Ping works for Route Trace using TTL.

5.4. Document 4: "Extensions for Lock Instruct"

A new document describing the LSP Ping extensions to accomplish the Lock Instruct desired behavior is needed. Some material useful for this scope can be found in "draft-boutros-mpls-tp-loopback-02".

5.5. Document 5: "AIS and Lock Reporting"

A new document is need for the definition of the AIS and Lock Reporting, however the document definition has been temporarily deferred by the MEAD team. Therefore this paragraph will be updated

in future versions.

5.6. Document 6: "Client Fault Indication"

A new document describing Client Fault Indication procedure needs to be defined.

The following two drafts indicating a client fault indication transported across MPLS-TP network will be compared and merged in the new document:

- "draft-he-mpls-tp-csf", which describes a tool to propagate a client failure indication across an MPLS-TP network in case the propagation of failure status in the client layer is not supported.

- "draft-martini-pwe3-static-pw-status", which describes the usage of PW associated channel to signal PW status messages in case a static PW is used without a control plane

It is worth noting that a Client Failure Indication is used if the client does not support its own OAM (IP and MPLS as clients use their own). It has been also agreed that CFI is used on PW and not on client directly mapped on LSP MPLS-TP.

5.7. Document 7: "Packet Loss"

A new document needs to be defined in order to describe a stand alone tool for Packet Loss measurements that can work both proactively and on demand. The tool will be functionally based on Y.1731.

5.8. Document 8: "Packet Delay"

A new document needs to be defined about the Packet Delay measurement which will be based on Y.1731 from the functionality point of view. Moreover, [MPLS-TP OAM Frwk] needs to be updated in order to clarify the functionality behavior expected from this tool.

5.9. Document 9: "Diagnostic Tests"

One or more new documents are needed for the tools definition for Diagnostic Tests. However, the documents definition has been temporarily deferred by the MEAD team until a clearer definition of "diagnostic test" in [MPLS-TP OAM Reqs].

6. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

7. Security Considerations

This document does not by itself raise any particular security considerations.

8. Acknowledgements

The authors wish to thank the MEAD team for their review and proposed enhancements to the text.

Appendix A. Proactive CC and CV BFD tool analysis

This appendix is focused on analyzing possible solutions and evaluating their pros&cons for defining an MPLS-TP OAM mechanism BFD based,to meet the requirements for proactive Continuity Check and Connectivity Verification functionality as required in [MPLS-TP OAM Reqs].

The BFD tool needs to be extended for the CV functionality by the addition of a unique identifier in order to meet the requirements. Proactive Continuity Check (CC) and Continuity Verification (CV) function are used together to detect loss of continuity (LOC), unintended connectivity between two MEs (e.g. mismerging or misconnection) as well as unintended connectivity within the ME with an unexpected MEP. It MUST operate both in bidirectional p2p and in

unidirectional p2mp connection.

The mechanism MUST foresee the configuration of the transmit frequency.

The mechanism is RECOMMENDED be the same for LSP, (MS-)PW and Section (See [MPLS-TP OAM Reqs])

Appendix A.1. Possible Solution

Several solutions have been analyzed:

1. Define a new BFD version (BFDv2) that extends the current BFD (BFDv1) to support also CV functionality. The new BFD version can be obtained by:

   * changing the semantic of MY discriminator and Your discriminator fields [BASE BFD],

   * adding a new globally unique source MEP ID field in the BFD packet for the CV functionality to the existing session identifier.

2. Define two separate tools, running with two different ACH encapsulations (i.e. two different ACH channel types):

   * the current BFD with only CC functionality however profiled in behavior to meet the CC MPLS-TP requirement;

   * a new tool that meet all the MPLS-TP OAM proactive CV requirement.

The new tool can be:

1. based on current BFD;

2. an extension of the ACH encapsulation for the current BFD;

3. a new tool like Y.1731 CCM;

All analyzed solutions imply extension of CV types, foreseen by [PW

VCCV] yet extended by [VCCV BFD], in order to include the MPLS-TP OAM mechanism too. This is due to the fact that VCCV also includes mechanisms for negotiating the control channel and connectivity verification (i.e. OAM functions) between PEs.

Appendix A.2. Backward compatibility

For backward compatibility, it is possible to run the current BFD that supports only CC functionality on some transport paths and the new tool that supports CC and proactive CV functionality on other transport paths. In any case only one tool for OAM instance at time, configurable by operator, can run.

A MEP that is configured to support proactive CV functionality MUST be capable to receive existing BFD packets (encapsulated with GAL/ G-ACH or PW-ACH) that supports only CC functionality and MUST consider them as an unexpected packet, i.e. detect a misconnection defect and vice versa.

The context of MPLS-TP OAM packets is based on MPLS label and G-ACH, eliminating in the BFD the need to exchange Discriminator values. An MPLS-TP node that desires to interoperate with a current BFD can apply the same discriminator field semantic as described in [BASE BFD] or:

- It MUST set the My discriminator field to a nonzero value (it can be a fixed value);

- It MUST reflect back the received value of My discriminator field into the transmitted Your discriminator field, or set it to zero if that value is unknown.

Appendix A.3. Definition of BFDv2

Common to both solutions detailed in this section are the following considerations:

- The Channel Type field of the G-ACH is the one proposed by [VCCV BFD], i.e. 0x0007, indicating the raw BFD control packet;

- The version number of the protocol needs to be updated to protocol version 2 respect to protocol version 1 defined in [BASE BFD].

Appendix A.3.1. New semantic for Discriminator fields

A possible BFD extension can be obtained changing the semantic of the two 32 bit fields, My Discriminator and Your Discriminator, to form a one 64 bit field carrying the globally unique MEP Identifier.

One of the disadvantages of this solution is on the too limited number of octets available for the globally unique MEP ID field: that doesn't allow the possibility to have different format of ME identifier.

Appendix A.3.2. New MEP ID field

This solution adds the new field required for the CV functionality, i.e. a globally unique MEP Identifier section, after the mandatory section of a BFD control packet and before the optional Authentication section.

The advantages of this solution are that the discriminator behavior of the current BFD protocol as defined in [BASE BFD] is unchanged and on the variable length of the MEP ID Section.

Appendix A.4. Two different ACH encapsulation of OAM tool

The current BFD, with only CC functionality, is encapsulated in the G-ACh using as Channel type code point the 0x0007 value as described in [VCCV BFD]. This mechanism can be also extended to Section OAM and LSP OAM.

In order to meet the MPLS-TP OAM proactive CV requirement, a new tool has to be introduced, encapsulated into the G-ACh with a new channel type code point. Common to all solutions detailed below are the following G-ACh format:

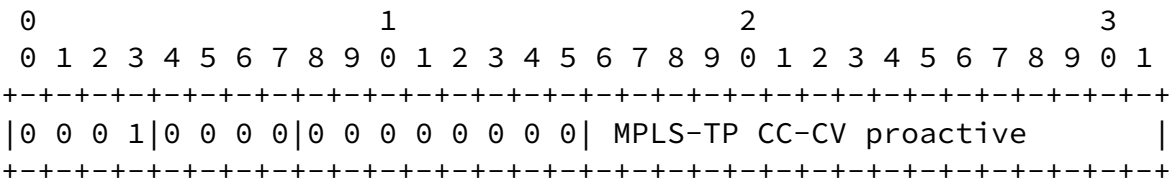

Figure 1: ACH Encapsulation

- first nibble: set to 0001b to indicate a channel associated with a PW, a LSP or a Section;

- Version and Reserved fields are set to 0;

- G-ACH Channel Type field with a new TBD code point meaning "MPLS-TP

CC-CV proactive" indicating that the message is an MPLS-TP OAM CC-CV proactive message. The value MUST be assigned

The sections below describe the format of the different possible new tool.

Appendix A.4.1. New tool based on current BFD

A new tool can be obtained introducing a globally unique MEP Identifier TLV between the ACH and the current BFD (defined in [BASE BFD]) Control packet.

The benefit of this solution is to maintain the basic state machine and protocol version of BFD as defined in [BASE BFD] and [bfdMultipoint]; considerations on the optional Authentication Section is described in section Appendix A.7.

Appendix A.4.2. New tool based on the extended BFD

The solutions and considerations are the same of what described in section Appendix A.3.2 except the ACH Channel type code, rather than the Version field, distinguishes between existing BFD (supporting CC) and the new tools (supporting both CC&CV).

The Version field in this case is set to 0 (this is the first version for this tool).

Appendix A.4.3. New tool like Y.1731 CCM

To be inserted

Appendix A.5. Remote Defect Indication

Remote Defect Indication (RDI) is used by a MEP to notify its peer MEP that a defect is detected on a bi-directional connection between them). RDI is only used for bidirectional connections and is associated with proactive CC & CV packet generation.[MPLS-TP OAM Frwk] The Diagnostic (Diag) field of the Current BFD can be used for this functionality. However, there isn't a total correspondence among the values foreseen by [BASE BFD] and the defect conditions detected by the proactive CC-CV tool that require the RDI function.

A solution could be that any defect that requires the RDI information being sent to the peer MEP is encoded in the Diagnostic (Diag) field with the value 1 (corresponding to the "Control Detection Time Expired" in [BASE BFD]. The value 0 indicates RDI condition has been cleared.

For the solution in section Appendix A.4.3 , RDI is foreseen in the packet format with a single bit.

Appendix A.6. Point to Multipoint transport paths

Solution described in section Appendix A.4.3 is valid for both bidirectional and unidirectional connection: in unidirectional connection only source MEP is enabled only to generate CC/CV OAM packets and sink MEP is enabled only to receive CC/CV OAM packets.

The BFD tool has a straightforward state machine for bidirectional path. Anyway the behavior and state machine need to be modified for the unidirectional connection; this is described in [bfdMultipoint].

Appendix A.7. Security Considerations

Base BFD [BASE BFD] foresees an optional authentication section; that can be extended even to the tool proposed in this document.

Authentication methods that require checksum calculation on the outgoing packet must extend the checksum even on the ME Identifier Section. This is possible but seems uncorrelated with the solution proposed in section Appendix A.4.1 in this case it could be better to use the simple password authentication method.

It is also worth noticing that the interactions between authentication and connectivity verification need further analysis.

9. Informative References

[RFC 2119]

Bradner, S., "Internet Control Message Protocol", BCP 14, RFC 2119, March 1997.

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

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

[PW ACH] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385, February 2006.

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

[BASE BFD] Katz, D. and D. Ward, "Bidirectional Forwarding Detection", ID draft-ietf-bfd-base-09.txt, February 2009.

[MPLS BFD] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "BFD For MPLS LSPs", ID draft-ietf-bfd-mpls-07.txt, June 2008.

[VCCV BFD] Nadeau, T. and C. Pignataro, "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)", ID draft-ietf-pwe3-vccv-bfd-07.txt, February 2008.

[bfdMultipoint] Katz, D. and D. Ward, "Bidirectional Forwarding Detection for Multipoint Networks", ID draft-katz-ward-bfd-multipoint-02.txt, February 2009.

[P2MP LSP Ping] Nadeau, T. and A. Farrel, "Detecting Data Plane Failures

in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping", ID draft-ietf-mpls-p2mp-lsp-ping-06.txt, June 2008.

[MPLS LSP Ping] Bahadur, N. and K. Kompella, "Mechanism for performing LSP-Ping over MPLS tunnels", ID draft-ietf-mpls-lsp-ping-enhanced-dsmap-00, June 2008.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol", RFC 4656, September 2006.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol", RFC 5357, Oct 2008.

[MPLS-TP OAM Reqs] Vigoureux, M., Betts, M., and D. Ward, "Requirements for OAM in MPLS Transport Networks", ID draft-ietf-mpls-tp-oam-requirements-01, April 2009.

[MPLS-TP OAM Frwk] Busi, I. and B. Niven-Jenkins, "MPLS-TP OAM Framework and Overview", ID draft-ietf-mpls-tp-oam-requirements-01, March 2009.

[MPLS-TP Reqs] Niven-Jenkins, B., Nadeau, T., and C. Pignataro, "Requirements for the Trasport Profile of MPLS", ID draft-ietf-mpls-tp-requirements-06, April 2009.

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

[MPLS-TP ACH TLV] Boutros, S., Bryant, S., Sivabalan, S., Swallow, G., and D. Ward, "Definition of ACH TLV Structure", ID draft-ietf-mpls-tp-ach-tlv-00, June 2009.

[RFC3813] Srinivasan, C., Viswanathan, A., and T. Nadeau,

"Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)", RFC 3813, June 2004.

[Y.1731] International Telecommunications Union - Standardization, "OAM functions and mechanisms for Ethernet based networks", ITU Y.1731, May 2006.

Authors' Addresses

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

Email: nurit.sprecher@nsn.com

Huub van Helvoort (editor)
Huawei
Kolkgriend 38, 1356 BC Almere
Netherlands

Phone: +31 36 5316076
Email: hhelvoort@huawei.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