Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 8, 2009

N. Sprecher, Ed.
Nokia Siemens Networks
T. Nadeau, Ed.
BT
H. van Helvoort, Ed.
Huawei
Y. Weingarten
Nokia Siemens Networks
July 07, 2008

MPLS-TP OAM Analysis
draft-sprecher-opsawg-mplstp-oam-analysis-00.txt

Status of this Memo

Abstract

The intention of this document is to analyze the set of requirements for OAM in MPLS-TP as defined in [MPLS-TP OAM Requirements], to verify whether the existing MPLS OAM tools can be applied to these requirements, identify which of the existing tools need to be extended, and which new tools should be defined. 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.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Table of Contents

1. Introduction

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

[MPLS-TP Requirements] in general and [MPLS-TP OAM Requirements] in particular define a set of requirements on OAM functionality in MPLS-TP for MPLS-TP LSPs (network infrastructure) and PWs (services).

The purpose of this document is to analyze the OAM requirements and verify whether the existing OAM tools defined for MPLS can be used to fulfill the requirements, identify which tools need to be extended to comply with the requirements, and which new tools need to be defined. The existing tools that are evaluated include LSP Ping (defined in [LSP Ping]), MPLS BFD (defined in [MPLS BFD]) and Virtual Circuit Connectivity Verification (defined in [PW VCCV] and [VCCV BFD]).

1.1. LSP Ping

LSP Ping is a variation of ICMP Ping and Traceroute [ICMP] that is adapted to MPLS LSP. Addressing is based upon the LSP Label and label stack in order to guarantee that the echo messages are switched in-band of the LSP. 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 not be transmitted outside the LSP.

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 FEC and also MTU problems. The traceroute functionality is used to isolate and localize the MPLS faults, using the TTL to incrementally verify the path. While LSP Ping is dependent upon the label propogation that may be performed over the control-plane via LDP, there is no direct dependence of LSP Ping on the control-plane.

LSP Ping can be activated both in on-demand and pro-active modes.

[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.

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

TTL exhaust is the method for terminating flows at intermediate LSRs.

LSP Ping is considered to be computational intensive and does not guarantee verification of the same data path in case of bundling.

1.2. MPLS BFD

BFD (Bidirectional Forwarding Detection) is a mechanism that is defined for fast fault detection. BFD defines a simple packet that may be transmitted over any protocol, dependent on the application that is employing the mechanism. BFD does not support a discovery mechanism nor support a traceroute capability for fault localization, these must be provided by use of other mechanisms. 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 BFD packets support authentication between the routers being checked.

[MPLS BFD] defines the use of BFD for P2P LSP end-points and is used to verify data-plane connectivity and to check 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 independently be monitored using the same BFD session.

There is a need for a mechanism to bootstrap a BFD session and LSP Ping is designated by [MPLS BFD] to bootstrap the BFD session in an MPLS environment. The session BFD messages for MPLS are transmitted using a IP/UDP encapsulation.

BFD can work in pro-active and on-demand modes of operation.

1.3. PW VCCV

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

VCCV supports the following OAM mechanisms: ICMP Ping, LSP Ping and BFD. 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 control channel provides the context required to bind the BFD session to a particular pseudo wire (FEC).

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.

1.4. Organization of the document

The analysis of the architectural requirements and the general principles of operations are discussed first and then the requirements on the set of OAM functions.

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 in MPLS-TP.

2. Architectural requirements and general principles of operation

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

- o [MPLS-TP OAM Requirements] 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.

- o [MPLS-TP OAM Requirements] 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. The existing tools do not rely on control and/or management plane, however the following should be observed regarding the reliance on IP.

  * LSP Ping makes use of IP header (UDP/IP) and does not comply with the requirement. This has further implications concerning the use of LSP Ping as the bootstrap mechanism for BFD for MPLS.

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

o [MPLS-TP OAM Requirements] requires that OAM tools for fault management do not rely on user traffic, and the existing MPLS OAM tools 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) ad there is a need to differentiate OAM packets from user-plane ones.

  * For PWs, VCCV provides a control channel 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/UD 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.

o [MPLS-TP OAM Requirements] 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.

o [MPLS-TP OAM Requirements] defines Maintenance Domain, Maintenance End Points (MEPs) and Maintenance Intermediate Points (MIPs). Means should be defined to provision these entities, both by static configuration (as it is required to operate OAM in the absence of any control plane or dynamic protocols) and by a control plane.

o [MPLS-TP OAM Requirements] requires a single OAM technology and consistent OAM capabilities for LSPs, PWs and Tandem Connections. There is currently no mechanism to support OAM for Tandem Connections. Also, the existing set of tools defines a different way of operating the OAM functions (e.g. LSP Ping to bootstrap MPLS BFD vs. VCCV) and provide incomplete coverage of OAM capabilities.

o [MPLS-TP OAM Requirements] requires allowing OAM packets to be directed to an intermediate node on a LSP/PW. Technically this can be supported by the proper setting of the TTL value, but it is

need to be examined per OAM function. For details, see below.

- [MPLS-TP OAM Requirements] suggests that OAM messages MAY be authenticated. BFD has a support for authentication. Other tools should support this capability as well.

2.1. Recommendations and Guidelines

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

- Extend the Associate Channel (AC) to provide a control channel at the path level. This could then be associated with a LSP or a Tandem Connection (TC). The ACH should then become a common mechanism for PW, LSP, and Tandem Connection.

- Create a VPCV (Virtual Path Connectivity Verification) definition that would apply the definitions and functionality of VCCV to the MPLS-TP environment for LSP or Tandem Connection.

- Apply BFD to this new mechanism using the control channel encapsulation, as defined above - allowing use of BFD for MPLS-TP independent of IP routing.

- A mechanism that be defined to create TCME and allow transmission of the traffic via the Tandem Connection using label stacking and proper TTL settings (having the knowledge of the necessary hop count).

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

- Independence of IP forwarding and routing.

- OAM packets should be transmitted in-band.

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

In addition, the following additional requirements:

- Provide the ability to carry other types of communications (e.g., APS, Management Control Channel (MCC), Signalling Control Channel (SCC)). New types of communication channels and CV can be defined for both PWs 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 Requirements].

LSP Ping is not considered a candidate to fulfil the required functionality, due its failure to comply with the basic requirement of independence from IP routing and forwarding, as documented in the Section 4 of this document.

3.1. Continuity Check

Continuity Check (CC) is used to detect loss of continuity between MEPs, or a MEP and MIP, and is useful for applications like Fault Management, Performance Monitoring and Protection Switching, etc.

3.1.1. Existing tools

MPLS BFD can be used to support the OAM Continuity Check function. It can be operated in a pro-active mode. However, the current definition is dependent on LSP Ping to bootstrap the BFD session.

VCCV can be used as a platform for CC - using BFD packets that are not IP/UDP encapsulated in pro-active mode.

3.1.2. Gaps

The following gaps are identified for support of CC in MPLS-TP environment:

- o A mechanism should be defined to bootstrap BFD sessions for MPLS that is not dependent on UDP.

- o Need extensions to BFD to cover P2MP connections.

3.1.3. Recommendations and Guidelines

Extend BFD to resolve the gaps.

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

3.2. Connectivity Verification

Connectivity Verification is a function that is used to check connectivity between MEPs in a maintenance domain. This function may be activated on-demand in reaction to a fault discovered in CC or for more thorough testing of the connections.

3.2.1. Existing tools

MPLS BFD supports OAM Connectivity Verification and it can be operated in both pro-active and on-demand modes.

3.2.2. Gaps

The following gaps are identified:

- o See section 5.1.2

- o BFD supports verification between MEP to MEP only.

3.2.3. Recommendations and Guidelines

As BFD works on a session basis, it seems complicated to extend it to work also between MEP and MIP. It is recommended to define a new simpler tool to support Connectivity Verification.

3.3. Alarm Suppression

Alarm Suppression is a function that is used by a server layer MEP to notify a failure condition to its client layer MEP(s) in order to suppress alarms that may be generated by maintenance domains of the client layer as a result of the failure condition in the server layer.

3.3.1. Existing tools

There is no mechanism defined in the IETF to support this function.

3.3.2. Recommendations and Guidelines

Define a tool to support Alarm Suppression.

3.4. Lock Indication

Lock Indication is a function that is used to indicate an administrative locking of a server layer MEP which may result in consequential interruption of data traffic forwarding towards the client layer MEP(s) expecting this traffic. The reception of a Lock Indication allows a MEP to differentiate between a defect condition and an administrative locking action at the server layer MEP.

3.4.1. Existing tools

There is no mechanism defined in the IETF to support this function.

3.4.2. Recommendations and Guidelines

Define a tool to support Lock Indication.

3.5. Packet Loss Measurement

Continuity Check (CC) is used to detect loss of continuity between MEPs, or a MEP and MIP, and is useful for applications like Fault Management, Performance Monitoring and Protection Switching, etc.

3.5.1. Existing tools

There is no mechanism defined in the IETF to support this function.

3.5.2. Recommendations and Guidelines

Define a tool to support Packet Loss Measurement.

3.6. Diagnostic Test

A diagnostic test is a function that is used between MEPs to verify bandwidth throughput, packet loss, bit errors, etc.

3.6.1. Existing tools

There is no mechanism defined in the IETF to support this function.

3.6.2. Recommendations and Guidelines

Define a tool to support Diagnostic Test.

3.7. Trace Route

Trace route is a function that is used to determine the route of a connection across the MPLS transport network.

3.7.1. Existing tools

LSP Ping supports trace route but as it does not comply with the requirement for OAM functions to be independent on IP routing and forwarding capabilities, it can not be utilized for MPLS-TP

3.7.2. Recommendations and Guidelines

Define a new tool to support Trace Route.

3.8. Delay Measurment

Delay Measurement is a function that is used to measure one-way or two-way delay of a packet transmission between a pair of MEPs. 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 first 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.

3.8.1. Existing tools

There is no mechanism defined in the IETF to support this function.

3.8.2. Recommendations and Guidelines

Define a tool to support Delay Measurment.

3.9. 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.

This function should be supported in pro-active mode.

3.9.1. 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.

3.9.2. Recommendations and Guidelines

Either create a dedicated mechanism for this functionality or extend the BFD session functionality to support the functionality without disrupting the CC or CV functionality.

3.10. Client Signal Fail

Client Signal Fail function (CSF) is used to propagate a Client Failure indication to the far-end sink when alarm suppression in the client layer is not supported.

3.10.1. Existing tools

There is no mechanism defined in the IETF to support this function.

3.10.2. Recommendations and Guidelines

Define a tool to support Delay Measurment.

4. Recommendation

- o Define a Tandem Connection entity and allow the transmission of traffic by means of label stacking and proper TTL setting.

- o Extend ACH to provide a control channel for LSPs and Tandem Connections.

- o Define a VPCV mechanism for LSP and Tandem Connection. This mechanism will use the same principles of operation as VCCV. The ACH should be extended to support CV types for each of the tool that are defined below, in a way that is consistent for PW, LSP and Tandem Connection.

- o 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.

- o Tools should be defined to support the following functions:

  * Connectivity verification

  * Alarm suppression

  * Lock indication

  * Packet loss measurement

  * Diagnostic test

  * Trace-route

  * Delay measurement

  * Remote defect indication

  * Client signal fail

- The tools should have the capability to authenticate the messages.

Note:We may consider having a document to define common CC and CV types of ACH for the use of VCCV and VPCV.

5. IANA Considerations

This document makes no request of IANA.

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

6. Security Considerations

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

7. Acknowledgements

The authors wish to thank xxxxxxx for his review and proposed enhancements to the text.

8. Informative References

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

[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.

[MP BFD] Katz, D. and D. Ward, "BFD for Multipoint Networks", ID draft-katz-ward-bfd-multipoint-01.txt, December 2007.

[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-01.txt, February 2008.

[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.

[MPLS-TP OAM Requirements] Vigoreux, M. and M. Betts, "Requirements for OAM in MPLS Transport Networks", ID draft-author-mpls-tp-oam-requirements-00, July 2008.

[MPLS-TP Requirments] Nadeau, T. and C. Pignataro, "Requirements for the Trasport Profile of MPLS", ID draft-jenkins-mpls-mplstp-requirements-00, July 2008.

Authors' Addresses

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

Email: nurit.sprecher@nsn.com

Tom Nadeau (editor)
BT
United State

Email: tom.nadeau@bt.com

Huub van Helvoort (editor)
Huawei
B
Netherlands

Email: hhelvoort@huawei.com

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

Email: yaacov.weingarten@nsn.com

Full Copyright Statement

Intellectual Property