MPLS Working Group  I. Busi (Ed)
Internet Draft                Alcatel-Lucent
Intended status: Informational  B. Niven-Jenkins (Ed)
BT
Expires: September 2009  March 9, 2009

MPLS-TP OAM Framework and Overview
draft-busi-mpls-tp-oam-framework-01.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

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document.

Busi et al.  Expires September 9, 2009  [Page 1]
Abstract

Multi-Protocol Label Switching (MPLS) Transport Profile (MPLS-TP) is based on a profile of the MPLS and pseudowire (PW) procedures as specified in the MPLS Traffic Engineering (MPLS-TE), pseudowire (PW) and multi-segment PW (MS-PW) architectures complemented with additional Operations, Administration and Maintenance (OAM) procedures for fault, performance and protection-switching management for packet transport applications that do not rely on the presence of a control plane.

This document provides a framework that supports a comprehensive set of OAM procedures that fulfills the MPLS-TP OAM requirements [11].

Table of Contents

1. Introduction....................................................3
   1.1. Contributing Authors....................................3
2. Conventions used in this document............................3
   2.1. Terminology............................................4
   2.2. Definitions............................................4
3. Functional Components........................................5
   3.1. Maintenance Entity....................................6
   3.2. Maintenance End Points (MEPs)........................7
   3.3. Maintenance Intermediate Points (MIPs)...............8
   3.4. Server MEPS...........................................9
4. Reference Model..............................................9
   4.1. MPLS-TP Section Monitoring...........................12
   4.2. MPLS-TP LSP End-to-End Monitoring....................13
   4.3. MPLS-TP LSP Tandem Connection Monitoring............14
   4.4. MPLS-TP PW Monitoring................................15
   4.5. MPLS-TP MS-PW Tandem Connection Monitoring.........16
5. OAM Functions for pro-active monitoring....................17
   5.1. Continuity Check and Connectivity Verification........17
      5.1.1. Applications for proactive CC & CV function....19
   5.2. Remote Defect Indication................................20
      5.2.1. Configuration considerations....................20
      5.2.2. Applications for Remote Defect Indication.....20
   5.3. Alarm Suppression......................................21
   5.4. Lock Indication........................................21
   5.5. Packet Loss Measurement................................21
   5.6. Client Signal Fail.....................................22
6. OAM Functions for on-demand monitoring......................22
   6.1. Continuity Check and Connectivity Verification.......22
      6.1.1. Configuration considerations....................23
   6.2. Packet Loss Measurement................................23
1. Introduction

As noted in the MPLS-TP framework [8], the overall architecture of MPLS-TP is based on a profile of the MPLS-TE and (MS-)PW architectures defined in RFC 3031 [2], RFC 3985 [5] and [6] complemented with additional OAM procedures for fault, performance and protection-switching management for packet transport applications that do not rely on the presence of a control plane.

In line with [12], existing MPLS OAM mechanisms will be used wherever possible and extensions or new OAM mechanisms will be defined only where existing mechanisms are not sufficient to meet the requirements.

The MPLS-TP OAM framework provides a comprehensive set of OAM procedures while satisfying the MPLS-TP OAM requirements [11]. In this regard, it is similar to existing SONET/SDH and OTH OAM mechanisms (e.g. [13]).

[Editor’s note - Sections 1, 2 and 3 of this version of the draft have been already reviewed by MEAD. Further revisions will be undertaken and the outcome of these revisions included in the next version of this draft]

1.1. Contributing Authors

Italo Busi, Ben Niven-Jenkins, Annamaria Fulignoli, Enrique Hernandez-Valencia, Lieven Levrau, Dinesh Mohan, Vincenzo Sestito, Nurit Sprecher, Huub van Helvoort, Martin Vigoureux, Yaacov Weingarten, Rolf Winter

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 RFC-2119 [1].
2.1. Terminology

LME  LSP Maintenance Entity

LTCME LSP Tandem Connection Maintenance Entity

[Editor’s note - Difference or similarity between tandem connection monitoring (TCM) and Path Segment Tunnel (PST) need to be defined and agreed]

ME  Maintenance Entity

[Editor’s note - There is a need to define whether to support OAM on p2mp transport path there is a need to introduce the MEG concept]

MEP  Maintenance End Point

MIP  Maintenance Intermediate Point

PME  PW Maintenance Entity

PTCME PW Tandem Connection Maintenance Entity

SME  Section Maintenance Entity

2.2. Definitions

Concatenated Segment: see [10]

Co-routed bidirectional path: see [10]

Layer network: see [10]

Section: see [10]

OAM flow: An OAM flow is a traffic flow between a pair of MEPs or a MEP and a MIP that is used to monitor a ME [Editor’s note - a MEG depending on what we decide for this point]. The OAM flow is associated to a unique ME and contains the OAM monitoring, signalling and notification messages necessary to monitor and maintain that ME. The exact mix of message types in an OAM flow will be dependent on the technology being monitored and the exact deployment scenario of that technology (e.g. some deployments may proactively monitor the connectivity of all transport paths whereas other deployments may only reactively monitor transport paths)
MIP: A MIP terminates and processes OAM messages and generates OAM messages in reaction to received OAM messages.

MEP Source: A MEP acts as MEP source for the OAM flow that it originates and inserts into its associated ME.

MEP Sink: A MEP acts as a MEP sink for the OAM flow that it terminates and processes from it associated ME.

OAM Message: An OAM information element that performs some OAM functionality (e.g. continuity and connectivity verification)

OAM Packet: A packet that carries one or more OAM messages (i.e. OAM information elements).

Path: See Transport Path

Segment: see [10]

Sublayer: see [10]

Tandem Connection: see [10]

Transport Path: see [10]

Unidirectional path: see [10]

3. Functional Components

MPLS defines the use of Label Switched Paths (LSPs) and Pseudowires (PWs) ([2], [5] and [7]) that are used to connect service end points. MPLS-TP builds on this framework the need to transport service traffic, based on certain performance and quality measurements. In order to verify and maintain these performance and quality measurements, we need to use the OAM functionality not only on an transport paths (e.g. LSP or MS-PW), but also on arbitrary parts of transport paths, defined as Tandem Connections in [10], between any two arbitrary points along a path.

MPLS-TP OAM operates in the context of Maintenance Entities (MEs).

A Maintenance Entity can be viewed as the association of two (or more) Maintenance End Points (MEPs), see below. The MEPs that form an ME are configured and managed to limit the scope of an OAM flow within the ME the MEPs belong to.
Each MEP resides at the boundaries of the ME that they are part of. An ME may also include a set of zero or more Maintenance Intermediate Points (MIPs), which reside within the Maintenance Entity, between the MEPs.

A MEP is capable of initiating and terminating OAM messages for fault management and performance monitoring.

A MIP is capable of terminating OAM messages but it generates OAM messages only in reaction to received OAM messages.

This functional model defines the relationships between all OAM entities from a maintenance perspective, to allow each Maintenance Entity to monitor and manage the layer network under its responsibility and easily localize problems.

MEPs and MIPs are associated with a particular Maintenance Entity.

When a control plane is not present, the management plane configures MEPs and MIPs. Otherwise they can be configured either by the management plane or by the control plane.

[Editor’s note - Need to align the two paragraphs above with the outcome of the on-going discussion on the mailing list regarding the usage of control plane to configure OAM]

3.1. Maintenance Entity

A Maintenance Entity can be viewed as the association of two (or more) Maintenance End Points (MEPs). An example of an ME with more than two MEPs is a point-to-multipoint ME monitoring a point-to-multipoint transport path (or point-to-multipoint tandem connection). The MEPs that form an ME should be configured and managed to limit the OAM responsibilities of an OAM flow within a network or sub-network, or a transport path or segment, in the specific layer network that is being monitored and managed. Any maintenance point in between MEPs is a Maintenance Intermediate Points (MIP).

A Maintenance Entity may be defined to monitor and manage unidirectional point-to-point or point-to-multipoint transport paths or tandem connections, or co-routed bidirectional point-to-point transport paths and tandem connections in an MPLS-TP layer network.

MPLS-TP OAM functions are designed to be applied either on an end-to-end basis, e.g., between the LERs of a given LSP or T-PEs of a given PW, or on a per tandem connection basis, e.g., between any LER/LSR of a given LSP or any T-PE/S-PE of a given PW.
The end points of a tandem connection are MEPs because the tandem connection is by definition a Maintenance Entity.

Therefore, in the context of MPLS-TP LSP or PW Maintenance Entity (defined below) LERs and T-PEs can be MEPs while LSRs and S-PEs may be MIPs. In the case of Tandem Connection Maintenance Entity (defined below), LSRs and S-PEs can be either MEPs or MIPs.

The following properties apply to all MPLS-TP MEs:

- They can be nested but not overlapped, e.g. a ME may cover a segment or a concatenated segment of another ME, and may also include the forwarding engine(s) of the node(s) at the edge(s) of the segment or concatenated segment, but all its MEPs and MIPs are no longer part of the encompassing ME. It is possible that MEPs of nested MEs reside on a single node.

- Each OAM flow is associated with a single Maintenance Entity.

- OAM packets are subject to the same forwarding treatment (e.g. fate share) as the data traffic, but they can be distinguished from the data traffic using the GAL and ACH constructs \[9\] for LSP and the ACH construct \[6\] \[9\] for (MS-)PW.

3.2. Maintenance End Points (MEPs)

Maintenance End Points (MEPs) are the end points of a ME. MEPs are responsible for activating and controlling all of the OAM functionality for the ME. A MEP may initiate an OAM packet to be transferred to its corresponding MEP, or to an intermediate MIP that is part of the ME.

MEPs prevent OAM packets corresponding to a ME from leaking outside that ME:

- A MEP sink terminates all the OAM packets that it receives corresponding to its ME and does not forward them further along the path. If the pro-active CC&CV OAM tool detects an unintended connectivity, all traffic on the path is blocked (i.e. all received packets are dropped, including user-data packets).

- A MEP source tunnels all the OAM packets that it receives, upstream from the associated ME, via label stacking. These packets are not processed within the ME as they belong to another ME.

[Editor’s - Need to rephrase the bullet above to clarify what it actually means]
MPLS-TP MEP notifies a fault indication to the MPLS-TP client layer network.

A MEP of a tandem connection is not necessarily coincident with the termination of the MPLS-TP transport path (LSP or PW), though it can monitor it for failures or performance degradation (e.g. count packets) within the boundary of the tandem connection.

[Editor’s note - The MEP of a TCM monitors the transport paths’ connectivity within the scope of the TCM. This means that failures or performance degradations within the TCM are detected by the TCM MEP while failures or performance degradations outside the TCM are not detected by the TCM MEP.

Is the text above sufficient to explain this concept?]

A MEP of an MPLS-TP transport path coincides with transport path termination and monitors it for failures or performance degradation on an end-to-end scope (e.g. count packets). Note that both MEP source and MEP sink coincide with transport paths’ source and sink terminations.[Editor’s note - Add some text regarding MEP identification]

3.3. Maintenance Intermediate Points (MIPs)

A Maintenance Intermediate Point (MIP) is a point between the two MEPs in an ME that is capable of reacting to some OAM packets and forwarding all the other OAM packets while ensuring fate sharing with data plane packets. A MIP belongs to only one ME.

A MIP does not initiate unsolicited OAM packets, but may be addressed by OAM packets initiated by one of the MEPs of the ME. A MIP can generate OAM packets only in response to OAM packets that are sent on the ME it belongs to.

[Editor’s note - It is needed to describe about how this is achieved (e.g. TTL expiry). Is this description in the scope of this document?]

MIPs are unaware of any OAM flows running between MEPs or between MEPs and other MIPs. MIPs can only receive and process OAM packets addressed to the MIP itself.

A MIP takes no action on the MPLS-TP transport path.

[Editor’s note - Add some text regarding MIP identification]
3.4. Server MEPs

A server MEP is a MEP of an ME that is either:

- defined in a layer network below the MPLS-TP layer network being referenced, or
- defined in a sub-layer of the MPLS-TP layer network that is below the sub-layer being referenced.

A server MEP coincides with either a MIP or a MEP in the client (MPLS-TP) layer network.

For example, a server MEP can be either:

- A termination point of a physical link (e.g. 802.3), an SDH VC or OTH ODU for the MPLS-TP Section layer network, defined in section 4.1.
- An MPLS-TP Section MEP for MPLS-TP LSPs, defined in section 4.2.
- An MPLS-TP LSP MEP for MPLS-TP PWs, defined in section 4.4.
- An MPLS-TP LSP Tandem Connection MEP for higher-level LTCMEs, defined in section 4.3.
- An MPLS-TP PW Tandem Connection MEP for higher-level PTCMEs, defined in section 4.5.

The server MEP can run appropriate OAM functions for fault detection within the server (sub-)layer network, and notifies a fault indication to the MPLS-TP layer network.

4. Reference Model

The reference model for the MPLS-TP framework builds upon the concept of an ME, and its associated MEPs and MIPs, to support the functional requirements specified in [11].

The following MPLS-TP MEs are specified in this document:

- A Section Maintenance Entity (SME), allowing monitoring and management of MPLS-TP Sections (between MPLS LSRs).
- A LSP Maintenance Entity (LME), allowing monitoring and management of an end-to-end LSP (between LERs).
o A PW Maintenance Entity (PME), allowing monitoring and management of an end-to-end SS/MS-PWs (between T-PEs).

o An LSP Tandem Connection Maintenance Entity (LTCME), allowing monitoring and management of an LSP Tandem Connection between any LER/LSR along the LSP.

o A MS-PW Tandem Connection Maintenance Entity (PTCME), allows monitoring and management of a SS/MS-PW Tandem Connection between any T-PE/S-PE along the (MS-)PW.

The MEs specified in this MPLS-TP framework are compliant with the architecture framework for MPLS MS-PWs [7] and MPLS LSPs [2].

Hierarchical LSPs are also supported. In this case, each LSP Tunnel in the hierarchy is a different sub-layer network that can be monitored, independently from higher and lower level LSP tunnels in the hierarchy, end-to-end (from LER to LER) by an LME. Tandem Connection monitoring via LTCME are applicable on each LSP Tunnel in the hierarchy.
Figure 1 reference model for the MPLS-TP OAM framework. The figure depicts portions of two MPLS-TP enabled subnetworks, Subnetwork A and Subnetwork Z. In Subnetwork A, LSR 1 is adjacent to LSR 2 via the MPLS Section Sec12 and LSR2 is adjacent to LSR3 via the MPLS Section Sec23. Similarly, In Subnetwork Z, LSR X is adjacent to LSR Y via the MPLS Section SecXY and LSR Y is adjacent to LSR Z via the MPLS Section SecYZ. In addition, LSR 3 is adjacent to LSR X via the MPLS Section 3X.

Figure 1 also shows a bi-directional MS-PW (PW15) between AC1 on LSR 1 (TPE1) and AC2 on LSR Z (TPEZ). The MS-PW consists of 3 bi-directional PW Segments: 1) PW Segment 1 (PW1) between LSR 1 (TPE1) and LSR 3 (SPE3) via the bi-directional PSN13 LSP, 2) PW Segment 3 (PW3) between LSR 3 (SPE3) and LSR X (SPEX), and 3) PW Segment 5.
(PW5) between LSR X (SPEX) and LSR Z (TPEZ) via the bi-directional
PSNXZ LSP.

The MPLS-TP OAM procedures that apply to an instance of a given ME
are expected to operate independently from procedures on other
instances of the same ME and certainly of other MEs. Yet, this does
not preclude that multiple MEs may be affected simultaneously by the
same network condition, for example, a fiber cut event.

Note that there are no constrains imposed by this OAM framework on
the number, or type, of MEs that may be instantiated a particular
node. In particular, when looking at Figure 1, it should be possible
to configure one or more MEPs from the same node if each MEP shares
the same node.

The subsections below define the MEs specified in this MPLS-TP OAM
architecture framework document. Unless otherwise stated, all
references to subnetworks, LSRs, MPLS Sections, LSP, pseudowires and
MEs in this Section are made in relation to those shown in Figure 1.

[Editor’s note – Do we need to use the "Subnetwork" definition? For
the scope of this description, I think we could use "OAM domain" or
"administrative domain"]

4.1. MPLS-TP Section Monitoring

An MPLS-TP Section ME (SME) is an MPLS-TP maintenance entity intended
to monitor the forwarding behaviour of an MPLS Section as defined in
[10]. An SME may be configured on any MPLS section. SME OAM packets
fate share with the user data packets sent over the monitored MPLS
Section.

An SME is intended to be deployed for applications where it is
preferable to monitor the link between the topologically adjacent
MPLS (and MPLS-TP enabled) LSRs rather than monitoring the individual
LSP or PW segments traversing the MPLS Section and the server layer
technology does not provide adequate OAM capabilities.

A representative application is collecting link-level PM statistics
at the node-to-node interfaces (NNI) in MPLS-TP sub-network domains.
Figure 2 Reference Example of MPLS-TP Section MEs (SME)

Figure 2 shows 5 Section MEs configured in the path between AC1 and AC2: 1) Sec12 ME associated with the MPLS Section between LSR 1 and LSR 2, 2) Sec23 ME associated with the MPLS Section between LSR 2 and LSR 3, 3) Sec3X ME associated with the MPLS Section between LSR 3 and LSR X, 4) SecXY ME associated with the MPLS Section between LSR X and LSR Y, and 5) SecYZ ME associated with the MPLS Section between LSR Y and LSR Z.

4.2. MPLS-TP LSP End-to-End Monitoring

An MPLS-TP LSP ME (LME) is an MPLS-TP maintenance entity intended to monitor the forwarding behaviour of an end-to-end LSP between two (e.g., a point-to-point LSP) or more (e.g., a point-to-multipoint LSP) LERs. An LME may be configured on any MPLS LSP. LME OAM packets fate share with user data packets sent over the monitored MPLS-TP LSP.

An LME is intended to be deployed in scenarios where it is desirable to monitor the forwarding behaviour of an entire LSP between its LERs, rather than, say, monitoring individual PWs. A representative application is collecting PM statistics of PSN LSP that is being used to provide a "tunnelling services" for a number of other LSPs.
Figure 3 depicts 2 LMEs configured in the path between AC1 and AC2: 1) the PSN13 LME between LER 1 and LER 3, and 2) the PSNXZ LME between LER X and LER Y. Note that the presence of a PSN3X LME in such a configuration is optional, hence, not precluded by this framework. For instance, the SPs may prefer to monitor the MPLS-TP Section between the two LSRs rather than the individual LSPs.

4.3. MPLS-TP LSP Tandem Connection Monitoring

An MPLS-TP LSP Tandem Connection Monitoring ME (LTCME) is an MPLS-TP maintenance entity intended to monitor the forwarding behaviour of an LSP tandem connection between a given pair of LSRs. Multiple LTCMEs MAY BE configured on any LSP. The LSR may or may not be immediately adjacent at the MPLS-TP layer. LTCME OAM packets fate share with the user data packets sent over the monitored LSP segment.

A LTCME can be defined between the following entities:

- LER and any LSR of a given LSP.
- Any two LSRs of a given LSP.

An LTCME is intended to be deployed in scenarios where it is preferable to monitor the behaviour of a part of an LSP rather than the entire LSP itself. A representative application is when there is a need to monitor a part of an LSP that extends beyond the administrative boundaries of an MPLS-TP enabled administrative domain.

Note that LTCMEs are equally applicable to hierarchical LSPs.
Figure 4 MPLS-TP LSP Tandem Connection Monitoring ME (LTCME)

Figure 4 depicts a variation of the reference model in Figure 1 where there is an end-to-end PSN LSP (PSN1Z LSP) between PE1 and PEZ. PSN1Z LSP consists of, at least, three stitched LSP Segments: PSN13, PSN3X and PSNXZ. In this scenario there are two separate LTCMEs configured to monitor the forwarding behaviour of the PSN1Z LSP: 1) a LTCME monitoring the PSN13 LSP Segment on Subnetwork 123 (PSN13 LTCME), and 2) a LTCME monitoring the PSNXZ LSP Segment on Subnetwork XYZ (PSNXZ LTCME).

It is worth noticing that LTCMEs can coexist with the LME monitoring the end-to-end LSP and that LTCME MEPs and LME MEPs can be coincident in the same node (e.g. PE1 node supports both the PSN1Z LME MEP and the PSN13 LTCME MEP).

4.4. MPLS-TP PW Monitoring

An MPLS-TP PW ME (PME) is an MPLS-TP maintenance entity intended to monitor the end-to-end forwarding behaviour of a SS-PW or MS-PW between a pair of T-PEs. A PME MAY be configured on any SS-PW or MS-PW. PME OAM packets fate share with the user data packets sent over the monitored PW.
A PME is intended to be deployed in scenarios where it is desirable to monitor the forwarding behaviour of an entire PW between a pair of MPLS-TP enabled T-PEs rather than monitoring the LSP aggregating multiple PWs between PEs. A representative application is on either SS-PW or MS-PW used to emulate traffic for which an SLA with QoS commitments may apply (e.g., an emulated DS1/E1 or the emulated CBR connection of an ATM VCC/VPC).

Figure 5 depicts a MS-PW (PW15) consisting of three segments: PW1, PW3 and PW5 and its associated end-to-end PME (PW15 PME).

4.5. MPLS-TP MS-PW Tandem Connection Monitoring

An MPLS-TP MS-PW Tandem Connection Monitoring ME (PTCME) is an MPLS-TP maintenance entity intended to monitor the forwarding behaviour of an MS-PW tandem connection between a given pair of PEs. Multiple PTCMEs MAY be configured on any MS-PW. The PEs may or may not be immediately adjacent at the MS-PW layer. PTCME OAM packets fate share with the user data packets sent over the monitored MS-PW Segment.

A PTCME can be defined between the following entities:

- Any two S-PEs of a given MS-PW. It can span several PW segments.

A PTCME is intended to be deployed in scenarios where it is preferable to monitor the behaviour of a part of a MS-PW rather than the entire end-to-end PW itself. A representative application is to collect PM statistics for the MS-PW Segment within a given network domain of an inter-domain PW.
Figure 6 MPLS-TP MS-PW Tandem Connection Monitoring (PTCME)

Figure 6 depicts the same MS-PW (PW15) between AC1 and AC2 as in Figure 5. In this scenario there are two separate PTCMEs configured to monitor the forwarding behaviour of PW15: 1) a PTCME monitoring the PW1 MS-PW Segment on Subnetwork 123 (PW1 PTCME), and 2) a PTCME monitoring the PW4 MS-PW Segment on Subnetwork XYZ with (PW5 PTCME).

It is worth noticing that PTCMEs can coexist with the PME monitoring the end-to-end MS-PW and that PTCME MEPs and PME MEPs can be coincident in the same node (e.g. TPE1 node supports both the PW15 PME MEP and the PW1 PTCME MEP).

5. OAM Functions for pro-active monitoring

5.1. Continuity Check and Connectivity Verification

Proactive Continuity and Connectivity Verification (CC & CV) function is used to detect loss of continuity (LOC), unexpected connectivity between two MEs (e.g. mismerging or misconnection) as well as unexpected connectivity within the ME with an unexpected MEP.

Proactive CC & CV is based upon the generation of OAM pro-active CC/CV packets, carrying a unique ME identifier, at a regular configurable timing rate and the detection of LOC when these packets do not arrive. If the received ME identifier does not match the expected ME identifier, a connectivity defect has occurred. The default CC/CV transmission periods are application dependent (see section 5.1.1.)
For statically provisioned connections, the transmission period and the ME identifier are statically configured at both MEPs. For dynamically established connections, the transmission period and the ME identifier are signaled via the control plane.

In a bidirectional point-to-point transport path, when a MEP is enabled to generate pro-active CC/CV packets with a configured transmission period, it also expects to receive pro-active CC/CV packets from its peer MEP with the same transmission period. In a unidirectional transport path (point-to-point or point-to-multipoint), only the source MEP is enabled to generate packets with CC/CV information. This MEP does not expect to receive any packets with CC/CV information from its peer MEPs in the ME.

MIPs as well as intermediate nodes not supporting MPLS-TP OAM are transparent to the pro-active CC/CV information and forward pro-active CC/CV packets as regular data packets.

When CC & CV is enabled, a MEP periodically transmits pro-active CC/CV packets with frequency of the configured transmission period.

When a MEP enabled to receive pro-active CC/CV packets

When CC & CV is enabled, a MEP detects loss of continuity (LOC) defect with a peer MEP when it receives no pro-active CC/CV packets from the peer MEP within the interval equal to 3.5 times the transmission period.

When a pro-active CC/CV packet is received, a MEP is able to detect a mis-connectivity defect (e.g. mismerge or misconnection) with another ME when the received packet carries an incorrect ME identifier.

If pro-active CC/CV packets are received with a transmission period different than expected, CC/CV period mis-configuration defect is detected.

[Editor’s note - We need to understand whether a mechanism for auto-negotiate the actual transmission period such that in case of period mis-configuration the two MEPs converge on the slower speed is required. It is anyway important to report to the operator the fact that the negotiated speed mismatches the configured one. Do we need to add some text to capture the capability to auto-negotiate the rate between MEPs?]
A receiving MEP notifies the equipment fault management process when it detects the above defect conditions.

If a MEP detects an unexpected connectivity it MUST block all the traffic (including also the user data packets) that it receives from the misconnected connection.

It is worth noticing that the OAM requirements document [11] recommends that CC-CV proactive monitoring is enabled on every ME in order to reliably detect connectivity defects.

However, CC-CV proactive monitoring can be disabled by an operator on a ME. In this case a dLOC can be a connectivity problem (e.g. a misconnection with a connection where CC-CV proactive monitoring is not enabled) and not necessarily a continuity problem, with a consequent wrong traffic delivering.

For these reasons, the traffic block consequent action SHOULD be applied even when a LOC condition occurs.

The activation of the traffic block consequent action should be configurable (i.e. it should be possible to enable/disable the consequent action) in case of LOC condition; that in order to enable/disable the proactive CC-CV monitoring on a ME in a not traffic affecting way.

5.1.1. Applications for proactive CC & CV function

CC & CV is applicable for fault management, performance monitoring, or protection switching applications.

- Fault Management: default transmission period is 1s (i.e. transmission rate of 1 packet/second)
- Performance Monitoring: default transmission period is 100ms (i.e. transmission rate of 10 packets/second)
- Protection Switching: in order to achieve sub-50ms recovery time the default transmission period is 3.33ms (i.e. transmission rate of 300 packets/second) although a transmission period of 10ms can also be used. In some cases, when a slower recovery time is acceptable, it is also possible to relax the transmission period.
of Yms, and an OAM message propagation time of Zms, the transmission period should be set to no greater than \( t = (X-Y-Z)/n \) assuming that switchover will not be triggered until n protection switching messages have failed to be received.]

5.2. Remote Defect Indication

The Remote Defect Indication (RDI) is an indicator that is transmitted by a MEP to communicate to its peer MEPs that a signal fail condition exists. RDI is only used for bidirectional connections and is associated with proactive CC & CV packet generation.

[Editor’s note - Add more specific information about the signal fail conditions reported by RDI.]

A MEP that has identified a signal fail related defect should include the RDI in all pro-active CC/CV packets that it generates for the duration of the signal fail condition existence.

A MEP that receives the packets with the RDI information should determine that its peer MEP has encountered a defect condition associated with a signal fail (i.e. detect an RDI defect).

MIPs should be transparent to the RDI indicator and transparently forwards pro-active CC/CV packets that include the RDI indicator, i.e. the MIP should not perform any actions nor examine the indicator.

When the signal fail condition clears, the MEP should clear the RDI indicator from subsequent transmission of pro-active CC/CV packets.

A MEP also clears the RDI defect upon reception of a pro-active CC/CV packet from the source MEP with the RDI indicator cleared.

5.2.1. Configuration considerations

In order to support RDI indication, the RDI transmission rate and PHB of the MEP should be configured as part of the CC & CV configuration.

5.2.2. Applications for Remote Defect Indication

RDI is applicable for the following applications:

- Single-ended fault management - A receiving MEP detects the RDI defect condition, which when correlated with other defect conditions in the receiving MEP may become a fault case.
o Contribution to far-end performance monitoring - The indication of
   the far-end defect condition is used as input to the performance
   monitoring process.

5.3. Alarm Suppression

Alarm Indication Signal function (AIS) is used to suppress alarms
following detection of defect conditions at the server (sub) layer.

- Packets with AIS information can be issued at a MEP, including a
  Server MEP, upon detecting signal fail conditions.

A server MEP is responsible for notifying the MPLS-TP layer network
MEP upon fault detection in the server layer network to which the
server MEP is associated.

Only Server MEPS can issue MPLS-TP packets with AIS information. Upon
detection of a signal fail condition the Server MEP can immediately
start transmitting packets with AIS information periodically. A
Server MEP continues to transmit periodic packets with AIS
information until the signal fail condition is cleared.

Upon receiving a packet with AIS information a MEP detects an AIS
defect condition and suppresses loss of continuity alarms associated
with all its peer MEPS. A MEP resumes loss of continuity alarm
generation upon detecting loss of continuity defect conditions in the
absence of AIS condition.

Specific configuration information required by a MEP to support AIS
transmission is the following:

- PHB - identifies the per-hop behaviour of packet with AIS
  information.

A MIP is transparent to packets with AIS information and therefore
does not require any information to support AIS functionality.

5.4. Lock Indication

To be incorporated in a future revision of this document

5.5. Packet Loss Measurement

To be incorporated in a future revision of this document
5.6. Client Signal Fail

To be incorporated in a future revision of this document

6. OAM Functions for on-demand monitoring

6.1. Continuity Check and Connectivity Verification

In order to preserve network resources, e.g. bandwidth, processing time at switches, it may be preferable to not use continual proactive CC & CV. In order to perform fault management functions network management may invoke periodic on-demand bursts of on-demand CC/CV packets. Use of on-demand CC & CV is dependent on the existence of a bi-directional connection ME.

An additional use of on-demand CC & CV would be to detect and locate a problem of connectivity when a problem is suspected or known based on other tools. In this case the functionality will be triggered by the network management in response to a status signal or alarm indication.

On-demand CC & CV is based upon generation of on-demand CC/CV packets that should uniquely identify the ME that is being checked. The on-demand functionality may be used to check either an entire ME (end-to-end) or between a MEP to a specific MIP.

On-demand CC & CV may generate a one-time burst of on-demand CC/CV packets, or be used to invoke periodic, non-continuous, bursts of on-demand CC/CV packets. The number of packets generated in each burst is configurable at the MEPs, and should take into account normal packet-loss conditions.

When invoking a periodic check of the ME, the source MEP should issue a burst of on-demand CC/CV packets that uniquely identifies the ME being verified. The number of packets and their transmission rate should be pre-configured and known to both the source MEP and the target MEP or MIP. The source MEP should use the TTL field to indicate the number of hops necessary, when targeting a MIP and use the default value when performing an end-to-end check [IB => This is quite generic for addressing packets to MIPs and MEPs so it is better to move this text in section 2]. The target MEP/MIP shall return a reply on-demand CC/CV packet for each packet received. If the expected number of on-demand CC/CV reply packets is not received at source MEP, a LOC state is detected.

[Editor’s note - We need to add some text for the usage of on-demand CC&CV with different packet sizes, e.g. to discover MTU problems.]
When a connectivity problem is detected (e.g. via a pro-active CC&CV OAM tool), on demand CC&CV tool can be used to check the path. The series should check CC&CV from MEP to peer MEP on the path, and if a fault is discovered, by lack of response, then additional checks may be performed to each of the intermediate MIP to locate the fault.

6.1.1. Configuration considerations

For on-demand CC & CV the MEP should support configuration of number of packets to be transmitted/received in each burst of transmissions and the transmission rate should be either pre-configured or negotiated between the different nodes.

In addition, when the CC & CV packet is used to check connectivity toward a target MIP, the number of hops to reach the target MIP should be configured.

The PHB of the on-demand CC/CV packets should be configured as well.

[Editor’s note – We need to be better define the reason for such configuration]

6.2. Packet Loss Measurement

To be incorporated in a future revision of this document

6.3. Diagnostic Test

To be incorporated in a future revision of this document

6.4. Trace routing

To be incorporated in a future revision of this document

6.5. Packet Delay Measurement

To be incorporated in a future revision of this document

7. OAM Protocols Overview

To be incorporated in a future revision of this document

8. Security Considerations

A number of security considerations important in the context of OAM applications.
OAM traffic can reveal sensitive information such as passwords, performance data and details about e.g. the network topology. The nature of OAM data therefore suggests to have some form of authentication, authorization and encryption in place. This will prevent unauthorized access to vital equipment and it will prevent third parties from learning about sensitive information about the transport network.

Mechanisms that the framework does not specify might be subject to additional security considerations.

9. IANA Considerations

No new IANA considerations.

10. Acknowledgments

The authors would like to thank all members of the teams (the Joint Working Team, the MPLS Interoperability Design Team in IETF and the T-MPLS Ad Hoc Group in ITU-T) involved in the definition and specification of MPLS Transport Profile.

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

11.1. Normative References


11.2. Informative References


Authors’ Addresses

Italo Busi (Editor)
Alcatel-Lucent
Email: Italo.Busi@alcatel-lucent.it

Ben Niven-Jenkins (Editor)
BT
Email: benjamin.niven-jenkins@bt.com

Contributing Authors’ Addresses

Annamaria Fulignoli
Ericsson
Email: annamaria.fulignoli@ericsson.com

Enrique Hernandez-Valencia
Alcatel-Lucent
Email: enrique@alcatel-lucent.com

Lieven Levrau
Alcatel-Lucent
Email: llevrau@alcatel-lucent.com

Dinesh Mohan
Nortel
Email: mohand@nortel.com

Busi et al. Expires September 9, 2009 [Page 26]
Vincenzo Sestito  
Alcatel-Lucent  
Email: vincenzo.sestito@alcatel-lucent.it

Nurit Sprecher  
Nokia Siemens Networks  
Email: nurit.sprecher@nsn.com

Huub van Helvoort  
Huawei Technologies  
Email: hhelvoort@huawei.com

Martin Vigoureux  
Alcatel-Lucent  
Email: martin.vigoureux@alcatel-lucent.fr

Yaacov Weingarten  
Nokia Siemens Networks  
Email: yaacov.weingarten@nsn.com

Rolf Winter  
NEC  
Email: Rolf.Winter@nw.neclab.eu