Internet Engineering Task Force (IETF)
Request for Comments: 6428
Category: Standards Track
ISSN: 2070-1721

D. Allan, Ed.
Ericsson
G. Swallow, Ed.
Cisco Systems, Inc.
J. Drake, Ed.
Juniper

November 2011

Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile

Abstract

Continuity Check, Proactive Connectivity Verification, and Remote Defect Indication functionalities are required for MPLS Transport Profile (MPLS-TP) Operations, Administration, and Maintenance (OAM).

Continuity Check monitors a Label Switched Path for any loss of continuity defect. Connectivity Verification augments Continuity Check in order to provide confirmation that the desired source is connected to the desired sink. Remote Defect Indication enables an end point to report, to its associated end point, a fault or defect condition that it detects on a pseudowire, Label Switched Path, or Section.

This document specifies specific extensions to Bidirectional Forwarding Detection (BFD) and methods for proactive Continuity Check, Continuity Verification, and Remote Defect Indication for MPLS-TP pseudowires, Label Switched Paths, and Sections using BFD as extended by this memo.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6428.

Table of Contents

1. Introduction

In traditional transport networks, circuits are provisioned on two or more switches. Service providers need Operations, Administration, and Maintenance (OAM) tools to detect mis-connectivity and loss of continuity of transport circuits. Both pseudowires (PWs) and MPLS-TP Label Switched Paths (LSPs) [12] emulating traditional transport circuits need to provide the same Continuity Check (CC), proactive Continuity Verification (CV), and Remote Defect Indication (RDI) capabilities as required in RFC 5860 [3]. This document describes the use of Bidirectional Forwarding Detection (BFD) [4] for CC, proactive CV, and RDI of a PW, LSP, or Sub-Path Maintenance Entity (SPME) between two Maintenance Entity Group End Points (MEPs).

As described in RFC 6371 [13], CC and CV functions are used to detect loss of continuity (LOC) and unintended connectivity between two MEPs (e.g., mis-merging or mis-connectivity or unexpected MEP).

RDI is an indicator that is transmitted by a MEP to communicate to its peer MEP that a signal fail condition exists. RDI is only used for bidirectional LSPs and is associated with proactive CC and CV BFD control packet generation.

This document specifies the BFD extension and behavior to satisfy the CC, proactive CV monitoring, and the RDI functional requirements for both co-routed and associated bidirectional LSPs. Supported encapsulations include Generic Associated Channel Label (GAL) / Generic Associated Channel (G-ACh), Virtual Circuit Connectivity Verification (VCCV), and UDP/IP. Procedures for unidirectional point-to-point (P2P) and point-to-multipoint (P2MP) LSPs are for further study.

This document utilizes identifiers for MPLS-TP systems as defined in RFC 6370 [9]. Work is ongoing in the ITU-T to define a globally-unique semantic for ITU Carrier Codes (ICCs), and future work may extend this document to utilize ICCs as identifiers for MPLS-TP systems.

The mechanisms specified in this document are restricted to BFD asynchronous mode.

2. Conventions Used in This Document

2.1. Terminology

ACH: Associated Channel Header

BFD: Bidirectional Forwarding Detection

CC: Continuity Check

CV: Connectivity Verification

GAL: Generic Associated Channel Label

G-ACh: Generic Associated Channel

LDI: Link Down Indication

LKI: Lock Instruct

LKR: Lock Report

LSP: Label Switched Path

LSR: Label Switching Router

ME: Maintenance Entity

MEG: Maintenance Entity Group

MEP: Maintenance Entity Group End Point

MIP: Maintenance Entity Group Intermediate Point

MPLS: Multiprotocol Label Switching

MPLS-OAM: MPLS Operations, Administration and Maintenance

MPLS-TP: MPLS Transport Profile

MPLS-TP LSP: Unidirectional or bidirectional Label Switched Path representing a circuit

MS-PW: Multi-Segment Pseudowire

NMS: Network Management System

OAM: Operations, Administration, and Maintenance [14]

PW: Pseudowire

PDU: Protocol Data Unit

P/F: Poll/Final

RDI: Remote Defect Indication

SPME: Sub-Path Maintenance Entity

TTL: Time To Live

TLV: Type Length Value

VCCV: Virtual Circuit Connectivity Verification

2.2. 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 RFC 2119 [1].

3. MPLS-TP CC, Proactive CV, and RDI Mechanism Using BFD

This document describes procedures for achieve combined CC, CV, and RDI functionality within a single MPLS-TP MEG using BFD. This augments the capabilities that can be provided for MPLS-TP LSPs using existing specified tools and procedures.

3.1. Existing Capabilities

A CC-only mode may be provided via protocols and procedures described in RFC 5885 [7] with ACH channel 7. These procedures may be applied to bidirectional LSPs (via the use of the GAL) as well as PWs.

Implementations may also interoperate with legacy equipment by implementing RFC 5884 [8] for LSPs and RFC 5085 [10] for PWs, in addition to the procedures documented in this memo. In accordance with RFC 5586 [2], when BFD control packets are encapsulated in an IP header, the fields in the IP header are set as defined in RFC 5884 [8]. When IP encapsulation is used, CV mis-connectivity defect detection can be performed by inferring a globally unique source on the basis of the combination of the source IP address and My Discriminator fields.

3.2. CC, CV, and RDI Overview

The combined CC, CV, and RDI functionality for MPLS-TP is achieved by multiplexing CC and CV PDUs within a single BFD session. The CV PDUs are augmented with a Source MEP-ID TLV to permit mis-connectivity detection to be performed by sink MEPs.

The interleaving of PDUs is achieved via the use of distinct encapsulations and code points for generic associated channel (G-ACh) encapsulated BFD depending on whether the PDU format is CC or CV:

- CC format: defines a new code point in the Associated Channel Header (ACH) described in RFC 5586 [2]. This format supports Continuity Check and RDI functionalities.

- CV format: defines a new code point in the Associated Channel Header (ACH) described in RFC 5586 [2]. The ACH with "MPLS-TP Proactive CV" code point indicates that the message is an MPLS-TP BFD proactive CV message, and information for CV processing is appended in the form of the Source MEP-ID TLV.

RDI is communicated via the BFD diagnostic field in BFD CC messages, and the diagnostic code field in CV messages MUST be ignored. It is not a distinct PDU. As per [4], a sink MEP SHOULD encode a diagnostic code of "1 - Control Detection Time Expired" when the time since the last received BFD control packet exceeds the detection time, which is equal to the remote system's Transmit Interval multiplied by the remote system's Detect Multiplier (which is set to 3 in this document). A sink MEP SHOULD encode a diagnostic code of "5 - Path Down" as a consequence of the sink MEP receiving LDI. A sink MEP MUST encode a diagnostic code of "9 - mis-connectivity defect" when CV PDU processing indicates a mis-connectivity defect. A sink MEP that has started sending diagnostic code 5 SHOULD NOT change it to 1 when the detection timer expires.

3.3. ACH Code Points for CC and Proactive CV

Figure 1 illustrates the G-ACh encoding for BFD CC-CV-RDI functionality.

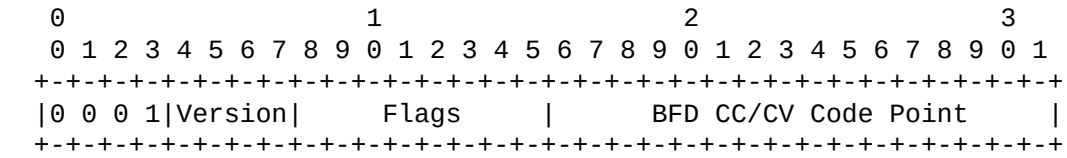

Figure 1: ACH Indication of MPLS-TP CC/CV/RDI

The first nibble (0001b) indicates the G-ACh as per RFC 5586 [2].

The version and the flags are set to 0 as specified in [2].

The code point is either

- BFD CC code point = 0x0022, or

- BFD proactive CV code point = 0x0023.

CC and CV PDUs apply to all pertinent MPLS-TP structures, including PWs, MPLS LSPs (including SPMEs), and Sections.

CC and CV operations are simultaneously employed on a maintenance entity (ME) within a single BFD session. The expected usage is that normal operation is to send CC BFD protocol data units (PDUs) interleaved with a CV BFD PDU (augmented with a Source MEP-ID and identified as requiring additional processing by the different ACh channel types). The insertion interval for CV PDUs is one per second. Detection of a loss of continuity defect occurs when the time since the last received BFD control packet exceeds the detection time, which is equal to the session periodicity times the remote system's Detect Multiplier (which is set to 3 for the CC code point). Mis-connectivity defects are detected in a maximum of one second.

3.4. MPLS-TP BFD CC Message Format

The format of an MPLS-TP CC message is shown below.

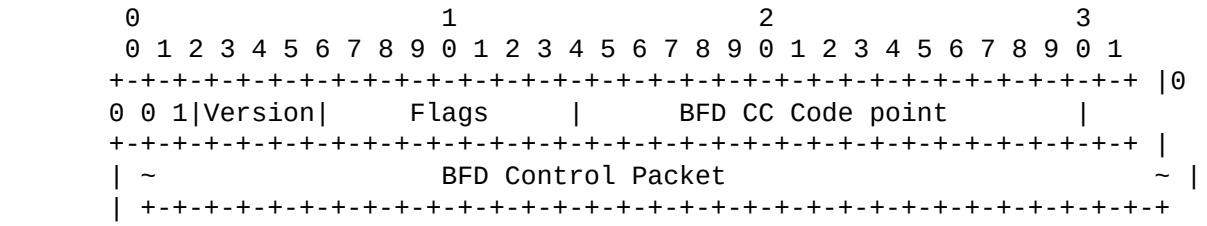

Figure 2: MPLS-TP CC Message

As shown in Figure 2, the MPLS-TP CC message consists of the BFD control packet as defined in [4] pre-pended by the G-ACh.

3.5. MPLS-TP BFD Proactive CV Message Format

The format of an MPLS-TP CV Message is shown below.

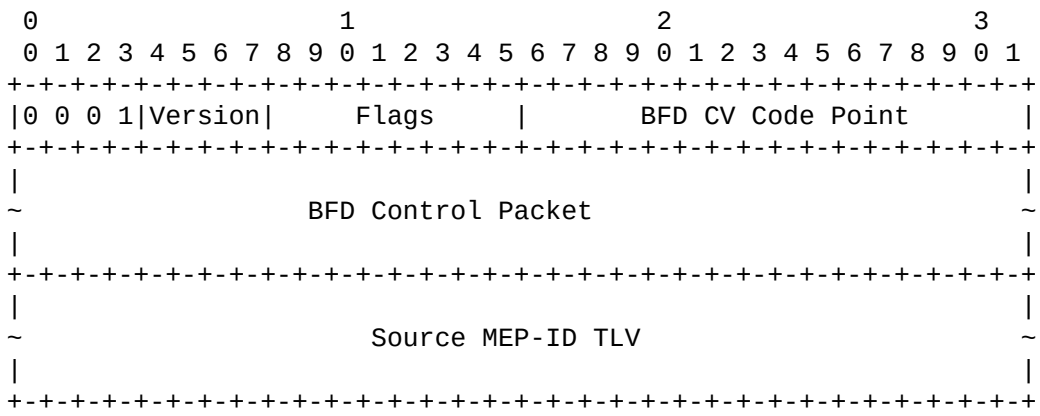

Figure 3: MPLS-TP CV Message

As shown in Figure 3, the MPLS-TP CV message consists of the BFD control packet as defined in [4], pre-pended by the ACH and appended by a Source MEP-ID TLV.

A Source MEP-ID TLV is encoded as a 2-octet field that specifies a Type, followed by a 2-octet Length field, followed by a variable-length Value field. A BFD session will only use one encoding of the Source ID TLV.

The length in the BFD control packet is as per [4]; the length of the Source MEP-ID TLV is not included. There are three possible Source MEP TLVs (corresponding to the MEP-IDs defined in [9]). The type fields are:

0 - Section MEP-ID

1 - LSP MEP-ID

2 - PW MEP-ID

When the GAL is used, the TTL field of the GAL MUST be set to at least 1, and the GAL MUST be the end of stack label (S=1) as per [2].

A node MUST NOT change the value in the Source MEP-ID TLV.

When digest-based authentication is used, the Source ID TLV MUST NOT be included in the digest.

3.5.1. Section MEP-ID

The IP-compatible MEP-ID for MPLS-TP Sections is the interface ID. The format of the Section MEP-ID TLV is:

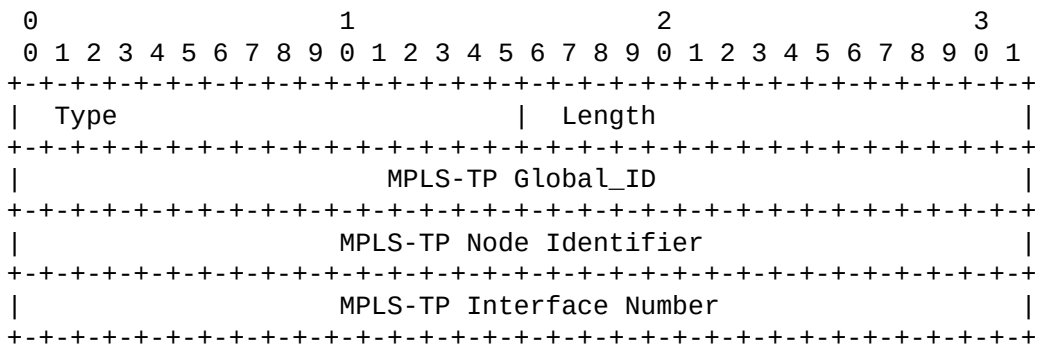

Figure 4: Section MEP-ID TLV Format

Where the Type is of value '0'. The Length is the length of the value fields. The MPLS-TP Global_ID, Node Identifier, and Interface Numbers are as per [9].

3.5.2. LSP MEP-ID

The fields for the LSP MEP-ID are as defined in [9]. This is applicable to both LSPs and SPMEs. This consists of the 32-bit MPLS-TP Global_ID, the 32-bit Node Identifier, followed by the 16-bit Tunnel_Num (that MUST be unique within the context of the Node Identifier), and the 16-bit LSP_NUM (that MUST be unique within the context of the Tunnel_Num). The format of the TLV is:

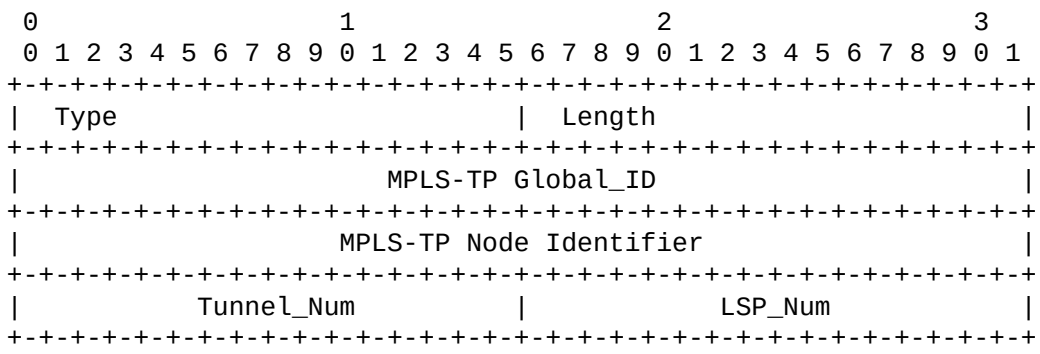

Figure 5: LSP MEP-ID TLV Format

Where the type is of value '1'. The length is the length of the value fields. The MPLS-TP Global_ID, Node Identifier, Tunnel_Num, and LSP_Num are as per [9].

3.5.3. PW End Point MEP-ID

The fields for the MPLS-TP PW End Point MEP-ID are as defined in [9]. The format of the TLV is:

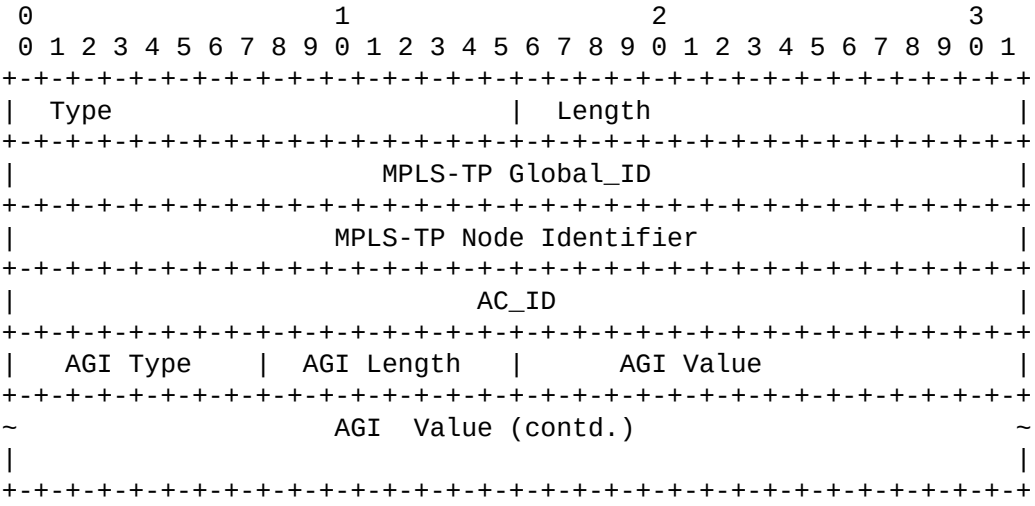

Figure 6: PW End Point MEP-ID TLV Format

Where the type is value '2'. The length is the length of the following data: the Global_ID, Node Identifier, and Attachment Circuit ID (AC_ID) are as per [9]. The Attachment Group Identifier (AGI) Type is as per [6], and the AGI Length is the length of the AGI value field.

3.6. BFD Session in MPLS-TP Terminology

A BFD session corresponds to a CC and proactive CV OAM instance in MPLS-TP terminology. A BFD session is enabled when the CC and proactive CV functionality are enabled on a configured Maintenance Entity (ME).

When the CC and proactive CV functionality are disabled on an ME, the BFD session transitions to the ADMIN DOWN state, and the BFD session ends.

A new BFD session is initiated when the operator enables or re-enables the CC and CV functionality.

All BFD state changes and P/F exchanges MUST be done using CC packets. P/F and session state information in CV packets MUST be ignored.

3.7. BFD Profile for MPLS-TP

BFD operates in asynchronous mode utilizing the encapsulation defined in Section 3 for all sessions in a given MEG. For LSPs, SPMEs, and Sections, this is GAL/G-ACh-encapsulated BFD using the code points specified in Section 3.3. For PWs, this is G-ACh or GAL/G-ACh-encapsulated BFD using the code points specified in Section 3.3. In this mode, the BFD control packets are periodically sent at a configurable time rate. This rate is a fixed value common for both directions of MEG for the lifetime of the MEG.

This document specifies bidirectional BFD for P2P transport LSPs; hence, all BFD packets MUST be sent with the M bit clear.

There are two modes of operation for bidirectional LSPs: one in which the session state of both directions of the LSP is coordinated, and one constructed from BFD sessions in such a way that the two directions operate independently but are still part of the same MEG. A single bidirectional BFD session is used for coordinated operation. Two independent BFD sessions are used for independent operation. It should be noted that independent operation treats session state and defect state as independent entities. For example, an independent session can be in the UP state while receiving RDI. For a coordinated session, the session state will track the defect state.

In coordinated mode, an implementation SHOULD NOT reset bfd.RemoteDiscr until it is exiting the DOWN state.

In independent mode, an implementation MUST NOT reset bfd.RemoteDiscr upon transitioning to the DOWN state.

Overall operation is as specified in RFC 5880 [4] and augmented for MPLS in RFC 5884 [8]. Coordinated operation is as described in [4]. Independent operation requires clarification of two aspects of [4]. Independent operation is characterized by the setting of bfd.MinRxInterval to zero by the MEP that is typically the session originator (referred to as the source MEP), and there will be a session originator at either end of the bidirectional LSP. Each source MEP will have a corresponding sink MEP that has been configured to a transmission interval of zero.

This memo specifies a preferred interpretation of the base specification on how a MEP behaves with a BFD transmit rate set to zero. One interpretation is that no periodic messages on the reverse component of the bidirectional LSP originate with that MEP; it will only originate messages on a state change.

The first clarification is that, when a state change occurs, a MEP set to a transmit rate of zero sends BFD control messages with a one-second period on the reverse component until such time that the state change is confirmed by the session peer. At this point, the MEP set to a transmit rate of zero can resume quiescent behavior. This adds robustness to all state transitions in the RxInterval=0 case.

The second clarification is that the originating MEP (the one with a non-zero bfd.TxInterval) will ignore a DOWN state received from a zero-interval peer. This means that the zero-interval peer will continue to send DOWN state messages that include the RDI diagnostic code as the state change is never confirmed. This adds robustness to the exchange of RDI on a unidirectional failure (for both session types DOWN with a diagnostic of either control detection period expired or neighbor signaled session down offering RDI functionality).

A further extension to the base specification is that there are additional OAM protocol exchanges that act as inputs to the BFD state machine. These are the Link Down Indication [5] and the Lock Instruct/Lock Report transactions, the Lock Report interaction being optional.

3.7.1. Session Initiation and Modification

Session initiation occurs starting from MinRx = 1 second, MinTx >= 1 second, and the detect multiplier = 3.

Once in the UP state, Poll/Final discipline is used to modify the periodicity of control message exchange from their default rates to the desired rates and to set the detect multiplier to 3.

Note that in the Poll/Final process a receiver of a new timer value with a poll flag can reject the timer value by tearing the session, or it can return its preferred timer value with the final flag. Note also that the receiver of a new timer value with a final flag can reject the timer value by tearing the session, or it can return its preferred timer value with the poll flag.

Once the desired rate has been reached using the Poll/Final mechanism, implementations SHOULD NOT attempt further rate modification.

In the rare circumstance where an operator has a reason to further change session parameters, beyond the initial migration from default values, Poll/Final discipline can be used with the caveat that a peer implementation may consider a session change unacceptable and/or bring the BFD session down via the use of the ADMIN DOWN state.

3.7.2. Defect Entry Criteria

There are further defect criteria beyond those that are defined in [4] to consider given the possibility of mis-connectivity defects. The result is the criteria for an LSP direction to transition from the defect-free state to a defect state is a superset of that in the BFD base specification [4].

The following conditions cause a MEP to enter the defect state for CC PDUs (in no particular order):

1. BFD session times out (loss of continuity defect).

2. Receipt of a Link Down Indication or Lock Report.

The following will cause the MEP to enter the mis-connectivity defect state for CV operation (again, not in any particular order):

1. BFD control packets are received with an unexpected encapsulation (mis-connectivity defect), these include:

   - receiving an IP encoded CC or CV BFD control packet on an LSP configured to use GAL/G-ACh, or
   - vice versa

   (Note there are other possibilities that can also alias as an OAM packet.)

2. Receipt of an unexpected globally unique Source MEP identifier (mis-connectivity defect). Note that as each encoding of the Source MEP-ID TLV contains unique information (there is no mechanical translation possible between MEP-ID formats), receipt of an unexpected Source MEP-ID type is the same as receiving an unexpected value.

3. Receipt of a session discriminator that is not in the local BFD database in the Your Discriminator field (mis-connectivity defect).

4. Receipt of a session discriminator that is in the local database but does not have the expected label (mis-connectivity defect).

5. If BFD authentication is used, receipt of a message with incorrect authentication information (password, MD5 digest, or SHA1 hash).

The effective defect hierarchy (order of checking) is:

1. Receiving nothing.

2. Receiving Link Down Indication, e.g., a local link failure, an MPLS-TP LDI, or Lock Report.

3. Receiving from an incorrect source (determined by whatever means).

4. Receiving from a correct source (as near as can be determined), but with incorrect session information.

5. Receiving BFD control packets in all discernable ways correct.

3.7.3. Defect Entry Consequent Action

Upon defect entry, a sink MEP will assert signal fail into any client (sub-)layers. It will also communicate session DOWN to its session peer using CC messages.

The blocking of traffic as a consequent action MUST be driven only by a defect's consequent action as specified in Section 5.1.1.2 of RFC 6371 [13].

When the defect is mis-connectivity, the Section, LSP, or PW termination will silently discard all non-OAM traffic received. The sink MEP will also send a defect indication back to the source MEP via the use of a diagnostic code of mis-connectivity defect (9).

3.7.4. Defect Exit Criteria

3.7.4.1. Exit from a Loss of Continuity Defect

For a coordinated session, exit from a loss of connectivity defect is as described in Figure 7, which updates RFC 5880 [4].

For an independent session, exit from a loss of connectivity defect occurs upon receipt of a well-formed BFD control packet from the peer MEP as described in Figures 8 and 9.

3.7.4.2. Exit from a Mis-Connectivity Defect

Exit from a mis-connectivity defect state occurs when no CV messages with mis-connectivity defects have been received for a period of 3.5 seconds.

3.7.5. State Machines

The following state machines update RFC 5880 [4]. They have been modified to include LDI and LKR as specified in [5] as inputs to the state machine and to clarify the behavior for independent mode. LKR is an optional input.

The coordinated session state machine has been augmented to indicate LDI and optionally LKR as inputs to the state machine. For a session that is in the UP state, receipt of LDI or optionally LKR will transition the session into the DOWN state.

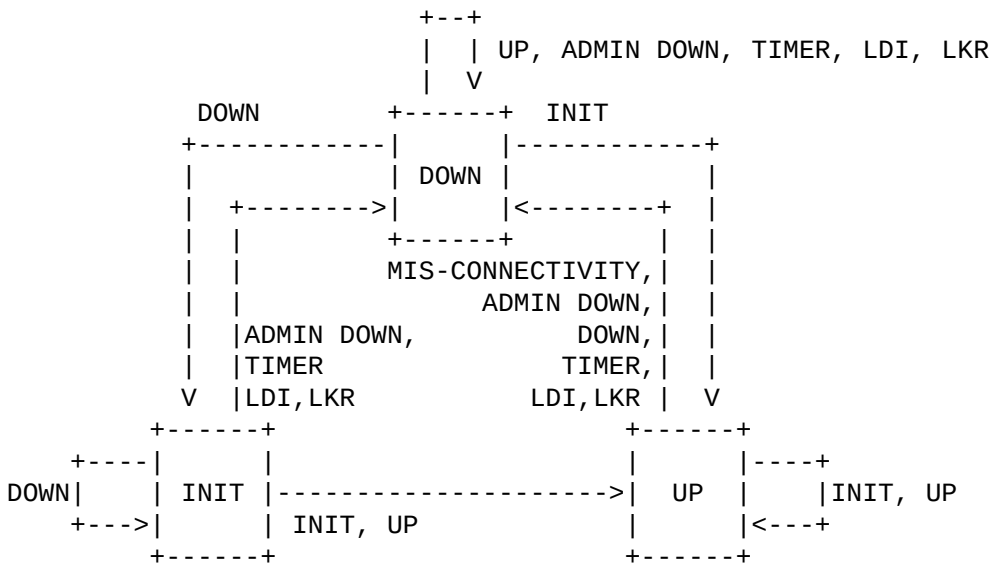

Figure 7: MPLS CC State Machine for Coordinated Session Operation

For independent mode, there are two state machines: one for the source MEP (which requested bfd.MinRxInterval=0) and one for the sink MEP (which agreed to bfd.MinRxInterval=0).

The source MEP will not transition out of the UP state once initialized except in the case of a forced ADMIN DOWN. Hence, LDI and optionally LKR do not enter into the state machine transition from the UP state, but do enter into the INIT and DOWN states.

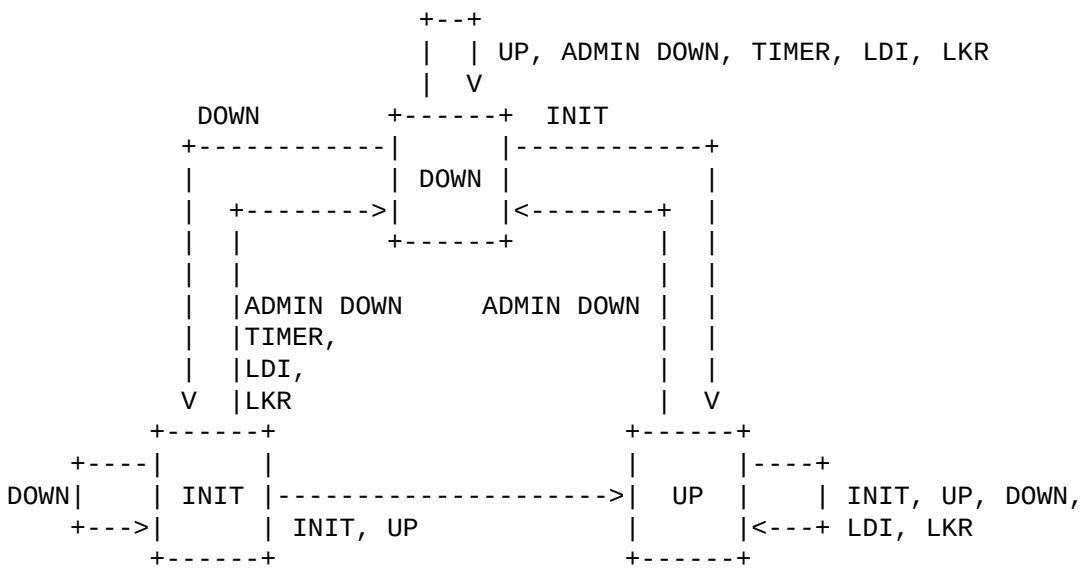

Figure 8: MPLS CC State Machine for Source MEP for Independent Session Operation

The sink MEP state machine (for which the transmit interval has been set to zero) is modified to:

1) Permit direct transition from DOWN to UP once the session has been initialized. With the exception of via the ADMIN DOWN state, the source MEP will never transition from the UP state; hence, in normal unidirectional fault scenarios, it will never transition to the INIT state.

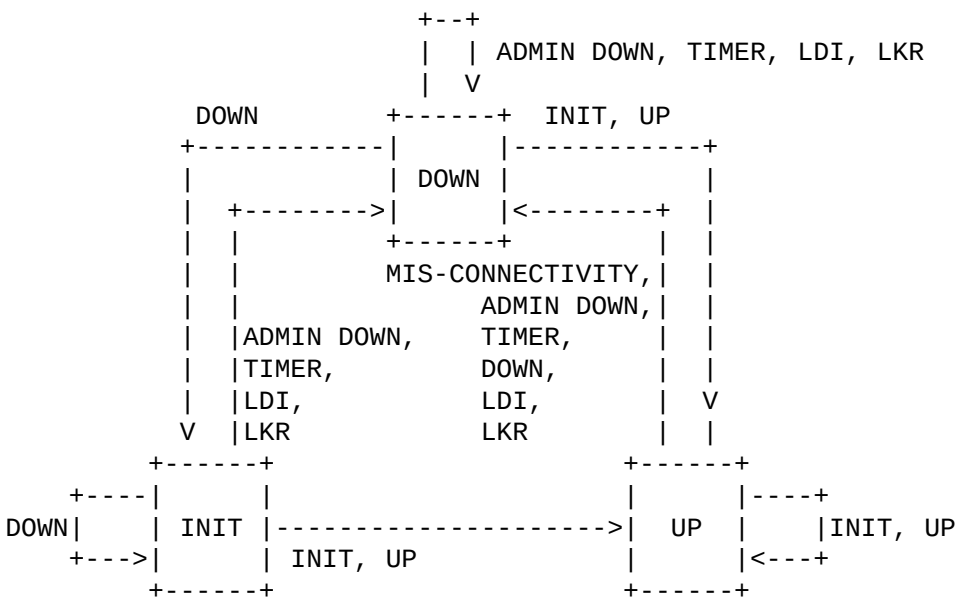

Figure 9: MPLS CC State Machine for the Sink MEP
for Independent Session Operation

3.7.6. Configuration of MPLS-TP BFD Sessions

The configuration of MPLS-TP BFD session parameters and the coordination of the same between the source and sink MEPs are out of scope of this memo.

3.7.7. Discriminator Values

In the BFD control packet, the discriminator values either are local to the sink MEP or have no significance (when not known).

The My Discriminator field MUST be set to a non-zero value (which can be a fixed value). The transmitted Your Discriminator value MUST reflect back the received value of the My Discriminator field or be set to zero if that value is not known.

Per Section 7 of RFC 5884 [8], a node MUST NOT change the value of the My Discriminator field for an established BFD session.

4. Configuration Considerations

The following is an example set of configuration parameters for a BFD session:

```
Mode and Encapsulation
----------------------
RFC 5884 - BFD CC in UDP/IP/LSP
RFC 5885 - BFD CC in G-ACh
RFC 5085 - UDP/IP in G-ACh
 MPLS-TP - CC/CV in GAL/G-ACh or G-ACh
```

For MPLS-TP, the following additional parameters need to be configured:

1) Session mode, coordinated or independent
2) CC periodicity
3) The MEP-ID for the MEPs at either end of the LSP
4) Whether authentication is enabled (and if so, the associated parameters)

The discriminators used by each MEP, both bfd.LocalDiscr and bfd.RemoteDiscr, can optionally be configured or locally assigned. Finally, a detect multiplier of 3 is directly inferred from the code points.

5. IANA Considerations

IANA has allocated two channel types from the "Pseudowire Associated Channel Types" registry in RFC 4385 [15].

```
0x0022   MPLS-TP CC message
0x0023   MPLS-TP CV message
```

IANA has created a "CC/CV MEP-ID TLV" registry. The parent registry is the "Pseudowire Associated Channel Types" registry of RFC 4385 [15]. All code points within this registry shall be allocated according to the "Standards Action" procedures as specified in [11]. The items tracked in the registry will be the type, associated name, and reference.

The initial values are:

```
0 - Section MEP-ID
1 - LSP MEP-ID
2 - PW MEP-ID
```

IANA has assigned the following code point from the "Bidirectional Forwarding Detection (BFD) Parameters" registry, "BFD Diagnostic Codes" subregistry [4]:

9 - mis-connectivity defect

6. Security Considerations

The use of CV improves network integrity by ensuring traffic is not "leaking" between LSPs.

Base BFD foresees an optional authentication section (see Section 6.7 of [4]) that can be applied to this application. Although the Source MEP-ID TLV is not included in the BFD authentication digest, there is a chain of trust such that the discriminator associated with the digest is also associated with the expected MEP-ID; this will prevent impersonation of CV messages in this application.

This memo specifies the use of globally unique identifiers for MEP-IDs. This provides absolutely authoritative detection of persistent leaking of traffic between LSPs. Non-uniqueness can result in undetected leaking in the scenario where two LSPs with common MEP-IDs are misconnected. This would be considered undesirable but rare; it would also be difficult to exploit for malicious purposes as, at a minimum, both a network end point and a node that was a transit point for the target MEG would need to be compromised.

7. References

7.1. Normative References

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

[2] Bocci, M., Ed., Vigoureux, M., Ed., and S. Bryant, Ed., "MPLS Generic Associated Channel", RFC 5586, June 2009.

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

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

[5] Swallow, G., Ed., Fulignoli, A., Ed., Vigoureux, M., Ed., Boutros, S., and D. Ward, "MPLS Fault Management Operations, Administration, and Maintenance (OAM)", RFC 6427, November 2011.

[6] Martini, L., "IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)", BCP 116, RFC 4446, April 2006.

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

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

[9] Bocci, M., Swallow, G., and E. Gray, "MPLS Transport Profile (MPLS-TP) Identifiers", RFC 6370, September 2011.

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

[11] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

7.2. Informative References

[12] Bocci, M., Ed., Bryant, S., Ed., Frost, D., Ed., Levrau, L., and L. Berger, "A Framework for MPLS in Transport Networks", RFC 5921, July 2010.

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

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

[15] 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.

8. Acknowledgments

Nitin Bahadur, Rahul Aggarwal, Tom Nadeau, Nurit Sprecher, and Yaacov Weingarten also contributed to this document.

9. Contributing Authors

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

Sami Boutros
Cisco Systems, Inc.
EMail: sboutros@cisco.com

Martin Vigoureux
Alcatel-Lucent
EMail: martin.vigoureux@alcatel-lucent.com

Siva Sivabalan
Cisco Systems, Inc.
EMail: msiva@cisco.com

David Ward
Juniper
EMail: dward@juniper.net

Robert Rennison
ECI Telecom
EMail: robert.rennison@ecitele.com

Editors' Addresses

Dave Allan
Ericsson
EMail: david.i.allan@ericsson.com

George Swallow
Cisco Systems, Inc.
EMail: swallow@cisco.com

John Drake
Juniper
EMail: jdrake@juniper.net