

Network working group
Internet Draft
Category: Standards Track
Created: March 9, 2010
Expires: September 2010

M. Chen(Ed.)
Huawei Technologies Co.,Ltd
N. So(Ed.)
Verizon

Return Path Specified LSP Ping

[draft-chen-mpls-return-path-specified-lsp-ping-02.txt](#)

Abstract

This document defines extensions to the failure-detection protocol for Multiprotocol Label Switching (MPLS) Label Switched Paths (LSPs) known as "LSP Ping" that allow selection of the LSP to use for the echo reply return path. Enforcing a specific return path can be used to verify bidirectional connectivity and also increase LSP ping robustness. It may also be used by Bidirectional Forwarding Detection (BFD) for MPLS bootstrap signaling thereby making BFD for MPLS more robust.

Status of this Memo

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

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

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

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

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

This Internet-Draft will expire on August 15, 2009.

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.

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](#) [[RFC2119](#)].

Table of Contents

- [1. Introduction.....3](#)
- [2. Problem Statements and Solution Overview.....3](#)
 - [2.1. Limitations of Existing Mechanisms for Bidirectional LSPs.4](#)
 - [2.2. Limitations of Existing Mechanisms for Handling Unreliable Return Paths.....4](#)
- [3. Extensions.....5](#)
 - [3.1. Reply Via Specified Path mode.....6](#)
 - [3.2. Reply Path \(RP\) TLV.....6](#)
 - [3.3. RP TLV sub-TLVs.....7](#)
 - [3.3.1. IPv4 RSVP Tunnel sub-TLV.....8](#)
 - [3.3.2. IPv6 RSVP Tunnel sub-TLV.....9](#)
 - [3.3.3. Bidirectional sub-TLV.....10](#)
 - [3.3.4. Any Candidate sub-TLV.....10](#)
- [4. Theory of Operation.....11](#)
 - [4.1. Sending an Echo Request.....11](#)
 - [4.2. Receiving an Echo Request.....12](#)
 - [4.3. Sending an Echo Reply.....13](#)
 - [4.4. Receiving an Echo Reply.....13](#)
- [5. Security Considerations.....14](#)
- [6. IANA Considerations.....14](#)
 - [6.1. Reply mode.....14](#)
 - [6.2. RP TLV.....15](#)
 - [6.3. Sub-TLVs for RP TLV.....15](#)
- [7. Contributors.....15](#)
- [8. Acknowledgments.....16](#)

| | | |
|----------------------|---|--------------------|
| 9. | References..... | 16 |
| 9.1. | Normative References..... | 16 |
| 9.2. | Informative References..... | 17 |
| | Authors' Addresses..... | 18 |

[1.](#) Introduction

This document defines extensions to the failure-detection protocol for Multiprotocol Label Switching (MPLS) Label Switched Paths (LSPs) known as "LSP Ping" [[RFC4379](#)] that can be used to specify the return paths for the echo reply message, increasing the robustness of LSP Ping, reducing the opportunity for error, and improving the reliability of the echo reply message. A new reply mode, which is referred to as "Reply via specified path", is added and a new Type-Length-Value (TLV), which is referred to as Reply Path (RP) TLV, is defined in this memo.

With the extensions described in this document, a bidirectional LSP and a pair of unidirectional LSPs (one for each direction) could both be tested with a single operational action, hence providing better control plane scalability. The defined extensions can also be utilized for creating a single Bidirectional Forwarding Detection (BFD) [[BFD](#)], [[BFD-MPLS](#)] session for a bidirectional LSP or for a pair of unidirectional LSPs (one for each direction).

In this document, term bidirectional LSP includes the co-routed bidirectional LSP defined in [[RFC3945](#)] and the associated bidirectional LSP that is constructed from a pair of unidirectional LSPs (one for each direction), and which are associated with one another at the LSP's ingress/egress points [[RFC5654](#)].

[2.](#) Problem Statements and Solution Overview

MPLS LSP Ping is defined in [[RFC4379](#)]. It can be used to detect data path failures in all MPLS LSPs, and was originally designed for unidirectional LSPs.

LSP are increasingly being deployed to provide bidirectional services. The co-routed bidirectional LSP is defined in [[RFC3471](#)] and [[RFC3473](#)], and the associated bidirectional LSP is defined in [[RFC5654](#)]. With the deployment of such services, operators have a desire to test both directions of a bidirectional LSP in a single operation.

Additionally, when testing a single direction of an LSP (either a unidirectional LSP, or a single direction of a bidirectional LSP)

using LSP Ping, the validity of the result may be affected by the success of delivering the echo response message. Failure to exchange these messages between the egress Label Switching Router (LSR) and the ingress LSR can lead to false negatives where the LSP under test is reported as "down" even though it is functioning correctly.

2.1. Limitations of Existing Mechanisms for Bidirectional LSPs

With the existing LSP Ping mechanisms as defined in [[RFC4379](#)], operators have to enable LSP detection on each of the two ends of a bidirectional LSP independently. This not only doubles the workload for the operators, but may also bring additional difficulties when checking the backward direction of the LSP under the following conditions:

1. The LSR that the operator logged on to perform the checking operations might not have out-of-band connectivity to the LSR at the far end of the LSP. That can mean it is not possible to check the return direction of a bidirectional LSP in a single operation -
- the operator must log on to the LSR at the other end of the

LSP

to test the return direction.

2. The LSP being tested might be an inter-domain/inter-AS LSP where the operator of one domain/AS may have no right to log on to the LSR at the other end of the LSP since this LSR resides in another domain/AS. That can make it completely impossible for the operator to check the return direction of a bidirectional LSP.

Associated bidirectional LSPs have the same issues as those listed for co-routed bidirectional LSPs.

This document defines a mechanism to allow the operator to request that both directions of a bidirectional LSP be tested by a single LSP Ping message exchange.

2.2. Limitations of Existing Mechanisms for Handling Unreliable Return Paths

[RFC4379] defines 4 reply modes:

1. Do not reply
2. Reply via an IPv4/IPv6 UDP packet
3. Reply via an IPv4/IPv6 UDP packet with Router Alert
4. Reply via application level control channel.

Obviously, the issue of the reliability of the return path for an echo reply message does not apply in the first of these cases.

[RFC4379] states that the third mode may be used when the IP return path is deemed unreliable. This mode of operation requires that all intermediate nodes must support the Router Alert option and must understand and know how to forward MPLS echo replies.

This is a rigorous requirement in deployed IP/MPLS networks especially since the return path may be through legacy IP-only routers. Furthermore, for inter-domain LSPs, the use of the Router Alert option may encounter significant issues at domain boundaries where the option is usually stripped from all packets. Thus, the use of this mode may itself introduce issues that lead to the echo reply messages not being delivered.

And in any case, the use modes 2 or 3 cannot guarantee the delivery of echo responses through an IP network that is fundamentally unreliable. The failure to deliver echo response messages can lead to false negatives making it appear that the LSP has failed.

Allowing the ingress LSR to control the path used for echo reply messages, and in particular forcing those messages to use an LSP rather than being sent through the IP network, enables an operator to apply an extra level of deterministic process to the LSP Ping test.

This document defines extensions to LSP Ping that can be used to specify the return paths of the echo reply message in an LSP echo request message.

3. Extensions

LSP Ping defined in [RFC4379] is carried out by sending an echo request message. It carries the Forwarding Equivalence Class (FEC) information of the tested LSP which indicates which MPLS path is being verified, along the same data path as other normal data packets belonging to the FEC.

LSP Ping [RFC4379] defines four reply modes that are used to direct the egress LSR in how to send back an echo reply. This document

defines a new reply mode, the Reply Via Specified Path mode. This new mode is used to direct the egress LSR of the tested LSP to send the echo reply message back along the path specified in the echo request message.

In addition, a new TLV, the Reply Path (RP) TLV, is defined in this document. The RP TLV consists of one or more sub-TLVs that can be used to carry the specified return path information to be used by the echo reply message.

3.1. Reply Via Specified Path mode

A new reply mode is defined to be carried in the Reply Mode field of the LSP Ping echo request message.

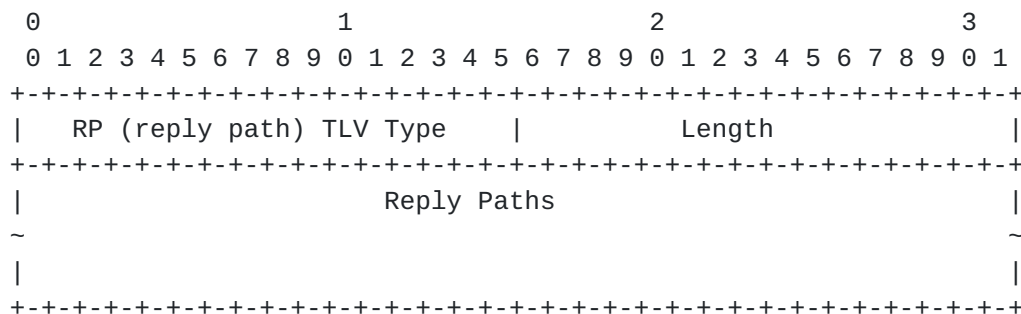
The recommended value of the Reply Via Specified Path mode is 5 (This is to be confirmed by the IANA).

| Value | Meaning |
|-------|--------------------------|
| ----- | ----- |
| 5 | Reply via specified path |

The Reply Via Specified Path mode is used to notify the remote LSR receiving the LSP Ping echo request message to send back the echo reply message along the specified paths carried in the Reply Path TLV.

3.2. Reply Path (RP) TLV

The Reply Path (RP) TLV is optionally included in an echo request message. It carries the specified return paths that the echo reply message is required to follow. The format of RP TLV is as follows:



RP TLV Type field is 2 octets in length, and the type value is TBD by IANA.

The Length field is 2 octets in length. It defines the length in octets of the Reply Paths field.

The Reply Paths field is variable in length. It has several nested sub-TLVs that describe the specified paths the echo reply message is required to follow.

When the Reply Mode field is set to "Reply via specified path" in an LSP echo request message, the RP TLV MUST be present.

3.3. RP TLV sub-TLVs

Each of the FEC sub-TLVs defined in [[RFC4379](#)] is applicable to be a sub-TLV for inclusion in the RP TLV for expressing a specific return path.

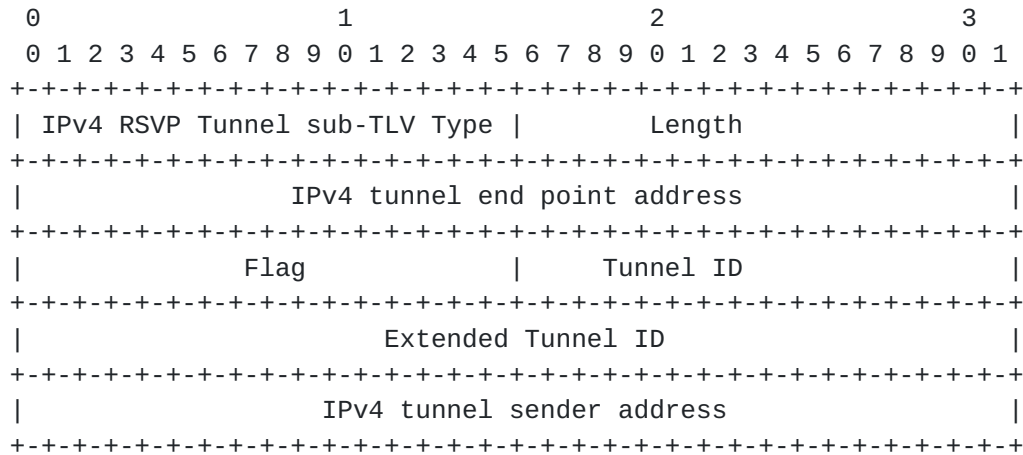
In addition, four more new sub-TLVs are defined: IPv4 RSVP Tunnel sub-TLV, IPv6 RSVP Tunnel sub-TLV, Bidirectional sub-TLV and Any Candidate sub-TLV. Detailed definition is in the following sections.

With those sub-TLVs defined in [[RFC4379](#)] and the sub-TLVs defined in this document, it could provide following options for return paths specifying:

1. Specify a particular LSP as return path
 - use those sub-TLVs defined in [[RFC4379](#)],
2. Specify a more generic tunnel FEC as return path
 - use the IPv4/IPv6 RSVP Tunnel sub-TLVs defined in [Section 3.3.1](#) and [Section 3.3.2](#) of this document
3. Specify the reverse path of the bidirectional LSP as return path
 - use the Bidirectional sub-TLV defined in [Section 3.3.3](#) of this document.
4. Force return path to pure IP path
 - use the Any Candidate sub-TLV only
5. Allow any LSPs except specific or general ones as return path
 - use the Any Candidate sub-TLV,
 - and include other sub-TLVs

3.3.1. IPv4 RSVP Tunnel sub-TLV

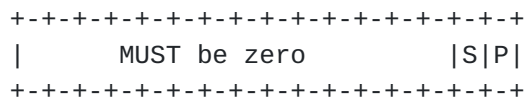
The IPv4 RSVP Tunnel sub-TLV is used in the RP TLV to allow the operator to specify a more generic tunnel FEC other than a particular LSP as the return path. The egress LSR chooses any LSP from the LSPs that have the same Tunnel attributes and satisfy the conditions carried in the Flag field. The format of IPv4 RSVP Tunnel sub-TLV is as follows:



The IPv4 RSVP Tunnel sub-TLV is derived from the RSVP IPv4 FEC TLV that is defined in Section 3.2.3 [RFC4379]. All fields have the same semantics as defined in [RFC4379] except that the LSP-ID field is omitted and a new Flag field is defined.

The IPv4 RSVP Tunnel sub-TLV Type field is 2 octets in length, and the recommended type value is 19 (to be confirmed by IANA).

The Flag field is 2 octets in length, it is used to notify the egress LSR how to choose the return path. The Flag field is a bit vector and has following format:



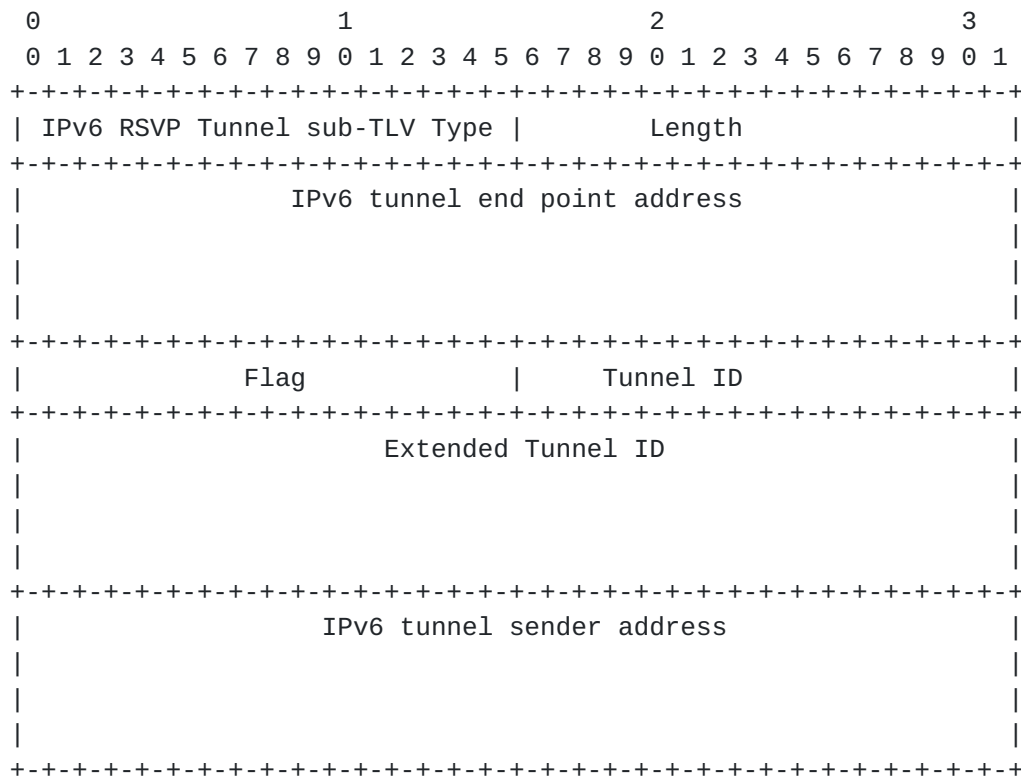
P (Primary): the return path MUST be chosen from the LSPs that have the same Tunnel attributes and the LSP MUST be the primary LSP.

S (Secondary): the return path MUST be chosen from the LSPs that have the same Tunnel attributes and the LSP MUST be the secondary LSP.

P bit and S bit MUST not both be set. If P bit and S bit are both not set, the return path could be any one of the LSPs that have the same Tunnel attributes.

3.3.2. IPv6 RSVP Tunnel sub-TLV

The IPv6 RSVP Tunnel sub-TLV is used in the RP TLV to allow the operator to specify a more generic tunnel FEC other than a particular LSP as the return path. The egress LSR chooses an LSP from the LSPs that have the same Tunnel attributes and satisfy the conditions carried in the Flag field. The format of IPv6 RSVP Tunnel sub-TLV is as follows:



The IPv6 RSVP Tunnel sub-TLV is derived from RSVP IPv6 FEC TLV that is defined in [Section 3.2.4 of \[RFC4379\]](#). All fields have the same

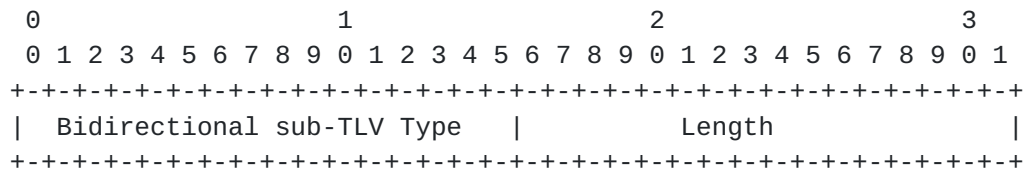
semantics as defined in [RFC4379] except that the LSP-ID field is omitted and a new Flag field is defined..

The IPv6 RSVP Tunnel sub-TLV Type field is 2 octets in length, and the recommended type value is 20 (to be confirmed by IANA).

The Flag field is 2 octets in length and is identical to that described in Section 3.3.

3.3.3. Bidirectional sub-TLV

The Bidirectional sub-TLV is used in the RP TLV when the return path is required to follow the reverse direction of the tested bidirectional LSP. The format of Bidirectional sub-TLV is as follows:

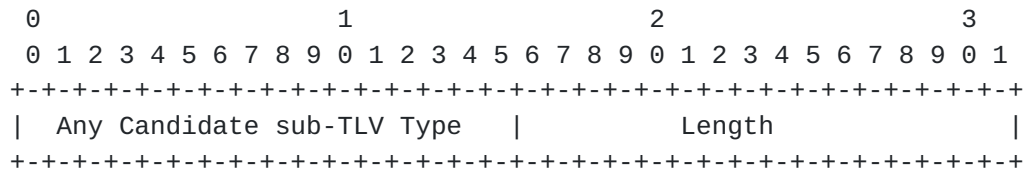


The Bidirectional sub-TLV Type field is 2 octets in length, and the recommended type value is 17 (to be confirmed by IANA).

The Length field is 2 octets in length, the value of length field MUST be 0, which means that there are no value fields following.

3.3.4. Any Candidate sub-TLV

The Any Candidate sub-TLV is used in the RP TLV when the return path is required to exclude the paths that are identified by any other reply path sub-TLVs carried in the echo request message. This is very useful when one or more previous LSP Ping attempts failed. By carrying an Any Candidate sub-TLV and the previous failed reply path sub-TLVs, a new LSP Ping echo request could be used to help the egress LSR to select another candidate path when sending echo reply message. If there is only an Any Candidate sub-TLV included in the echo request (i.e., no other sub-TLVs are present in the RP TLV), the egress LSR MUST select a non-LSP path (e.g., an IP path) as the return path. This is very useful when reverse MPLS path problems are suspected which can be confirmed when the echo reply is forced to follow an IP path. The format of the Any Candidate sub-TLV is as follows:



The Any Candidate sub-TLV Type field is 2 octets in length, and the recommended type value is 18 (to be confirmed by IANA).

The Length field is 2 octets in length, the value of length field MUST be 0, it means that there is no any value fields follows.

4. Theory of Operation

The procedures defined in this document currently only apply to "ping" mode. The "traceroute" mode is out of scope for this document.

In [RFC4379], the echo reply is used to report the LSP checking result to the LSP Ping initiator. This document defines a new reply mode and a new TLV (RP TLV) which enable the LSP ping initiator to specify or constrain the return path of the echo reply. Similarly the behavior of echo reply is extended to detect the requested return path by looking at a specified path FEC TLV. This enables LSP Ping to detect failures in both directions of a path with a single operation, this of course cuts in half the operational steps required to verify the end to end bidirectional connectivity and integrity of an LSP.

When the echo reply message is intended to test the return MPLS LSP path, the destination IP address of the echo reply message MUST never be used in a forwarding decision. To avoid this possibility the destination IP address of the echo reply message that is transmitted along the specified return path MUST be set to numbers from the range 127/8 for IPv4 or 0:0:0:0:0:FFFF:127/104 for IPv6, and the IP TTL MUST be set 1. Of course when the echo reply message is not intended for testing the specified return path, the procedures defined in [RFC4379] (the destination IP address is copied from the source IP address) apply unchanged.

4.1. Sending an Echo Request

When sending an echo request, in addition to the rules and procedures defined in Section 4.3 of [RFC4379], the reply mode of the echo request MUST be set to "Reply via specified path", and a RP TLV MUST be carried in the echo request message correspondingly. The

RP TLV includes one or several reply path sub-TLV(s) to identify the return path(s) the egress LSR should use for its reply.

For a bidirectional LSP, since the ingress LSR and egress LSR of a bidirectional LSP are aware of the relationship between the forward and backward direction LSPs, only a Bidirectional sub-TLV SHOULD be carried within the RP TLV. If the operator wants the echo reply to be sent along a different path other than the reverse direction of the bidirectional LSP, another FEC sub-TLV SHOULD be carried in the RP TLV instead.

In some cases, operators may want to treat two unidirectional LSPs (one for each direction) as a pair. There may not be any binding relationship between the two LSPs. Using the mechanism defined in this document, operators can run LSP Ping one time from one end to complete the failure detection on both unidirectional LSPs. To accomplish this, the echo request message MUST carry (in the RP TLV) a FEC sub-TLV that belongs to the backward LSP.

4.2. Receiving an Echo Request

"Ping" mode processing as defined in [Section 4.4 of \[RFC4379\]](#) applies in this document. In addition, when an echo request is received, if the egress LSR does not know the reply mode defined in this document, an echo reply with the return code set to "Malformed echo request" and the Subcode set to zero will be send back to the ingress LSR according to the rules of [\[RFC4379\]](#). If the egress LSR knows the reply mode, according to the RP TLV, it SHOULD find and select the desired return path, if there is no such path, an echo reply with Errored TLVs [\[RFC4379\]](#) that contains the RP TLV SHOULD be sent back to the ingress LSR, which is used to tell the ingress LSR that the requested return path does not exist.

As described in [Section 3.3.4](#) of this document, the Any Candidate sub-TLV has two functions: 1) helping the egress LSR to exclude some undesired paths, and 2) indicating whether the return path SHOULD be tested (by carrying the FEC stack TLV of the return path).

If an Any Candidate sub-TLV is present, the egress LSR MUST exclude the paths identified by those FEC sub-TLVs carried in the RP TLV and select other path to send the echo reply.

If no Any Candidate sub-TLV is present, it means that the echo reply is REQUIRED not only to send along the specified path, but to detect the selected return path as well (by carrying the FEC stack TLV of the return path). In addition, the FEC validate results of forward

path LSP SHOULD not affect the egress LSR continue to test return path LSP.

4.3. Sending an Echo Reply

As described in [[RFC4379](#)], the echo reply message is a UDP packet, and it MUST be sent only in response to an MPLS echo request. The source IP address is a routable IP address of the replier, the source UDP port is the well-know UDP port for LSP ping.

When the echo reply is intended to test the return path, the destination IP address of the echo reply message MUST never be used in a forwarding decision. To avoid this problem, the IP destination address of the echo reply message that is transmitted along the specified return path MUST be set to numbers from the range 127/8 for IPv4 or 0:0:0:0:0:FFFF:127/104 for IPv6, and the IP TTL MUST be set 1. If the echo reply is required to test the return path, the echo reply MUST have a FEC stack TLV describing the return path, which is used for the ingress LSR to perform FEC validation. The FEC stack TLV of the forward path MUST NOT be copied to the echo reply. And the FEC stack TLV of forward LSP MUST not be copied to the echo reply.

If the echo reply message is not intended for testing the specified return path, the same as defined in [[RFC4379](#)], the destination IP address and UDP port are copied from the source IP address and source UDP port of the echo request.

When sending the echo reply, the RP TLV carried in the received echo request MAY be copied to the echo reply to give the Ingress LSR enough information about the reverse direction of the tested path to verify the consistency of the data plane against control plane.

4.4. Receiving an Echo Reply

The rules and process defined in [Section 4.6 of \[RFC4379\]](#) apply here. When an echo reply is received, if the reply mode is "Reply via specified path" and a FEC stack TLV exists, it means that the echo reply has both Ping result reporting and reverse path checking functions. The ingress LSR MUST do FEC validation as an egress LSR does when receiving an echo request, the FEC validation process (relevant to "ping" mode) defined in [Section 4.4.1 of \[RFC4379\]](#) applies here.

When an echo reply is received with return code set to "Malformed echo request received" and the Subcode set to zero. It is possible

that the egress LSR may not know the "Reply via specified path" reply mode, the operator may choose to re-perform another LSP Ping by using one of the four reply modes defined [[RFC4379](#)].

On receipt of an echo reply with an Errored TLVs and an RP TLV is carried, if the return code is not set to "TLV not understood", it means that the egress LSR could not find a matched return path as specified. Operators may choose to specify another LSP as the return path or use other methods to detect the path.

When the LSP Ping initiator fails after some time to receive the echo reply message, the operator MAY initiate another LSP Ping by resending a new echo request carrying a RP TLV that includes an Any Candidate sub-TLV and the previous sent reply path sub-TLV(s) (Bidirectional sub-TLV or FEC sub-TLVs) to notify the egress LSR to send echo reply message along any other workable path (no matter what MPLS LSP or IP path) excluding the path(s) identified by those Bidirectional sub-TLV or/and FEC sub-TLVs. Hence it could improve the reliability of the echo reply message. In such a mode, the echo reply SHOULD NOT be used to detect the return path.

5. Security Considerations

Security considerations discussed in [[RFC4379](#)] apply to this document. In addition to that, in order to prevent using the extension defined in this document for "proxying" any possible attacks, the return path LSP MUST have destination to the same node where the forward path is from.

6. IANA Considerations

IANA is requested to make the following allocations from registries under its control.

6.1. Reply mode

IANA is requested to assign a new reply mode as follows:

Reply mode:

| Value | Meaning |
|-------|--------------------------|
| ----- | ----- |
| 5 | Reply via specified path |

6.2. RP TLV

IANA is requested to assign a new TLV type (TBD) from the range of 0-16383. We suggest that the value 20 be assigned for the new RP TLV type.

| Type | Value Field |
|-------|-------------|
| ----- | ----- |
| 20 | Reply Path |

6.3. Sub-TLVs for RP TLV

This document defines four new sub-TLV Types (described in [Section 3.4](#), [3.5](#), [3.6](#) and [3.7](#)) of RP TLV, and those FEC sub-TLVs defined in [[RFC4379](#)] are applicable for inclusion in RP TLV.

IANA is requested to assign sub-TLVs as follows. The following numbers are suggested:

| Sub-type | Value Field | Reference |
|----------|------------------|---------------|
| ----- | ----- | ----- |
| 17 | Bidirectional | this document |
| 18 | Any Candidate | this document |
| 19 | IPv4 RSVP Tunnel | this document |
| 20 | IPv6 RSVP Tunnel | this document |

7. Contributors

The following individuals also contributed to this document:

Ehud Doron
Orckit-Corrigent

E-Mail: ehudd@orckit.com

Ronen Solomon
Orckit-Corrigent

E-Mail: RonenS@orckit.com

Ville Hallivuori
Tellabs
Sinimaentie 6 C
FI-02630 Espoo, Finland

E-Mail: ville.hallivuori@tellabs.com

8. Acknowledgments

The authors would like to thank Adrian Farrel and Peter Ashwood-Smith for their review, suggestion and comments to this document.

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4379] K. Kompella., et al., "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", [RFC 4379](#), February 2006.
- [BFD] D. Katz, D. and Ward, D., "Bidirectional Forwarding Detection", [draft-ietf-bfd-base](#), work in progress.
- [BFD-MPLS] Aggarwal, R., Kompella, K., Nadeau, T., and Swallow, G., "BFD For MPLS LSPs", [draft-ietf-bfd-mpls](#), work in progress.
- [BFD-IP] D. Katz, D. Ward, "BFD for IPv4 and IPv6 (Single Hop)", [draft-ietf-bfd-v4v6-1hop-08.txt](#).

9.2. Informative References

- [RFC3471] L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", [RFC 3471](#), January 2003.
- [RFC3473] L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling", [RFC 3473](#), January 2003.
- [RFC3945] E. Mannie, "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", [RFC 3945](#), October 2004.
- [RFC5654] Niven-Jenkins, B. (Ed.), Brungard, D. (Ed.), Betts, M. (Ed.) Sprecher, N., and Ueno, S., "Requirements of an MPLS Transport Profile", [RFC 5654](#), September 2009.

Authors' Addresses

Mach(Guoyi) Chen
Huawei Technology Co., Ltd.
No. 9 Xixi Road
Shangdi Information Industry Base
Hai-Dian District, Beijing 100085
China

EMail: mach@huawei.com

So Ning
Verizon
2400 N. Glem Ave.,
Richerson, TX 75082

Phone: +1 972-729-7905
EMail: ning.so@verizonbusiness.com

Frederic Jounay
France Telecom
2, avenue Pierre-Marzin
22307 Lannion Cedex
FRANCE

EMail: frederic.jounay@orange-ftgroup.com

Simon Delord
Telstra
242 Exhibition St
Melbourne VIC 3000
Australia

EMail: simon.a.delord@team.telstra.com

Xinchun Guo
Huawei Technology Co., Ltd.
No. 9 Xixi Road
Shangdi Information Industry Base
Hai-Dian District, Beijing 100085
China

E-Mail: guoxinchun@huawei.com

Wei Cao
Huawei Technology Co., Ltd.
No. 9 Xixi Road
Shangdi Information Industry Base
Hai-Dian District, Beijing 100085
China

E-Mail: caoweigne@huawei.com