     Controlling State Advertisements of Non-negotiated LDP Applications

Abstract

   There is no capability negotiation done for Label Distribution
   Protocol (LDP) applications that set up Label Switched Paths (LSPs)
   for IP prefixes or that signal point-to-point (P2P) Pseudowires (PWs)
   for Layer 2 Virtual Private Networks (L2VPNs). When an LDP session
   comes up, an LDP speaker may unnecessarily advertise its local state
   for such LDP applications even when the peer session is established
   for some other applications like Multipoint LDP (mLDP) or the Inter-
   Chassis Communication Protocol (ICCP). This document defines a
   solution by which an LDP speaker announces to its peer its
   disinterest in such non-negotiated applications, thus disabling the
   unnecessary advertisement of corresponding application state, which
   would have otherwise been advertised over the established LDP
   session.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   The LDP Capabilities specification [RFC5561] introduced a mechanism
   to negotiate LDP capabilities for a given feature between peer Label
   Switching Routers (LSRs). The capability mechanism ensures that no
   unnecessary state is exchanged between peer LSRs unless the
   corresponding feature capability is successfully negotiated between
   the peers.

   Newly defined LDP features and applications, such as Typed Wildcard
   Forwarding Equivalence Class (FEC) [RFC5918], Inter-Chassis
   Communication Protocol [RFC7275], mLDP [RFC6388], and L2VPN Point-to-
   multipoint (P2MP) PW [RFC7338] make use of LDP capabilities framework
   for their feature negotiation. However, the earlier LDP applications
   allowed LDP speakers to exchange application state without any
   capability negotiation. This, in turn, results in the unnecessary
   advertisement of state when a given application is not enabled on one
   of the LDP speakers. These earlier LDP applications include (i)
   application to establish LSPs for IP unicast prefixes and (ii)
   application to signal when L2VPN P2P PW [RFC4447] [RFC4762]. For
   example, when bringing up and using an LDP peer session with a remote
   Provider Edge (PE) LSR for purely ICCP-signaling reasons, an LDP
   speaker may unnecessarily advertise labels for IP (unicast) prefixes
   to this ICCP-related LDP peer.

   Another example of unnecessary state advertisement can be cited when
   LDP is to be deployed in an IP dual-stack environment. For instance,
   an LSR that is locally enabled to set up LSPs for both IPv4 and IPv6
   prefixes may advertise (address and label) bindings for both IPv4 and
   IPv6 address families towards an LDP peer that is interested in IPv4
   bindings only. In this case, the advertisement of IPv6 bindings to
   the peer is unnecessary, as well as wasteful, from the point of view
   of LSR memory/CPU and network resource consumption.

   To avoid this unnecessary state advertisement and exchange, currently
   an operator is typically required to configure and define filtering
   policies on the LSR, which introduces unnecessary operational
   overhead and complexity for such deployments.

   This document defines a solution based on LDP Capabilities [RFC5561]
   by which an LDP speaker may announce to its peer(s) its disinterest
   (or non-support) for state to set up IP Prefix LSPs and/or to signal
   L2VPN P2P PW at the time of session establishment. This capability
   helps in avoiding unnecessary state advertisement for such feature
   applications. This document also states the mechanics to dynamically

   disable or enable the state advertisement for such applications
   during the session lifetime. The "uninteresting" state of an
   application depends on the type of application and is described later
   in Section 3.1.

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 [RFC2119].

   The term "IP" in this document refers to both IPv4 and IPv6 unicast
   address families.

3. Non-negotiated LDP Applications

   For the applications that existed prior to the definition of the LDP
   Capabilities framework [RFC5561], an LDP speaker typically
   advertises, without waiting for any capabilities exchange and
   negotiation, its corresponding application state to its peers after
   the session establishment. These early LDP applications include:

      o IPv4/IPv6 Prefix LSPs Setup
      o L2VPN P2P FEC 128 and FEC 129 PWs Signaling

   The rest of This document uses the following shorthand terms for
   these earlier LDP applications:

   o "Prefix-LSPs": Refers to an application that sets up LDP LSPs
      corresponding to IP routes/prefixes by advertising label bindings
      for Prefix FEC (as defined in RFC 5036).

   o "P2P-PWs": Refers to an application that signals FEC 128 and/or
      FEC 129 L2VPN P2P PWs using LDP (as defined in RFC 4447).

   To disable unnecessary state exchange for such LDP applications over
   an established LDP session, a new capability is being introduced in
   this document. This new capability controls the advertisement of
   application state and enables an LDP speaker to notify its peer its
   disinterest in the state of one or more of these "Non-negotiated" LDP
   applications at the time of session establishment. Upon receipt of
   such a capability, the receiving LDP speaker, if supporting the
   capability, disables the advertisement of the state related to the
   application towards the sender of the capability. This new
   capability can also be sent later in a Capability message either to
   disable a previously enabled application's state advertisement or to
   enable a previously disabled application's state advertisement.

3.1. Uninteresting State

   A uninteresting state of a non-negotiated LDP application:

   - is the application state that is of no interest to an LSR and need
      not be advertised to the LSR;

   - need not be advertised in any of the LDP protocol messages;

   - is dependent on application type and specified accordingly.

3.1.1. Prefix-LSPs

   For the Prefix-LSP application type, the uninteresting state refers
   to any state related to IP Prefix FEC (such as FEC label bindings,
   LDP Status). This document, however, does not classify IP address
   bindings (advertised via ADDRESS message) as a uninteresting state
   and allows the advertisement of IP address bindings. The reason for
   this allowance is that an LSR typically uses peer IP address(es) to
   map an IP routing next hop to an LDP peer in order to implement its
   control plane procedures. For example, mLDP [RFC6388] uses a peer's
   IP address(es) to determine its upstream LSR to reach the Root node
   as well as to select the forwarding interface towards its downstream
   LSR. Hence, in an mLDP-only network, while it is desirable to
   disable advertisement of label bindings for IP (unicast) prefixes,
   disabling advertisement of IP address bindings will break mLDP
   functionality. Similarly, other LDP applications may also depend on
   learnt peer IP addresses; hence, this document does not put IP
   address binding into a uninteresting state category to facilitate
   such LDP applications.

3.1.2. P2P-PWs

   For the P2P-PW application type, the uninteresting state refers to
   any state related to P2P PW FEC 128 / FEC 129 (such as FEC label
   bindings, Media Access Control (MAC) address withdrawal, and LDP PW
   Status). In this document, the term "state" will mean to refer to
   the "uninteresting state" for an application, as defined in this
   section.

4. Controlling State Advertisement

   To control advertisement of uninteresting state related to non-
   negotiated LDP applications defined in Section 3, a new capability
   TLV is defined as follows.

4.1. State Advertisement Control Capability

   The "State Advertisement Control Capability" is a new Capability
   Parameter TLV defined in accordance with Section 3 of LDP
   Capabilities specification [RFC5561]. The format of this new TLV is
   as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|U|F|   SAC Capability (0x050D)  |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|S|   Reserved   |                                               |
+-+-+-+-+-+-+-+-+-+                                               |
|                                                               |
~              State Advertisement Control Element(s)           ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
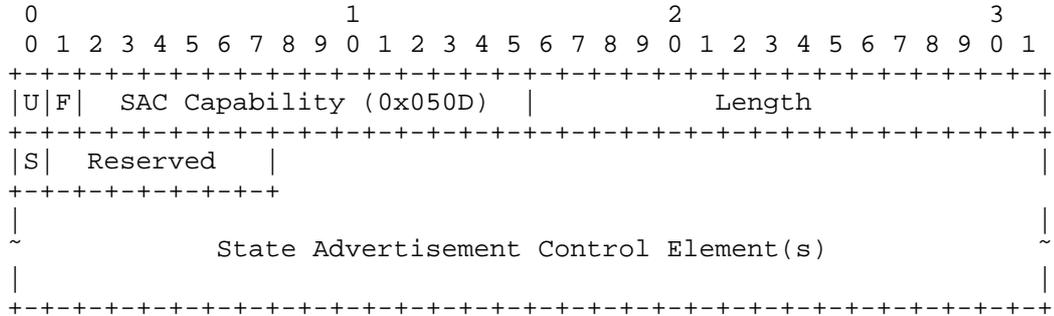
   Figure 1: Format of a "State Advertisement Control Capability" TLV

   The value of the U-bit for the TLV MUST be set to 1 so that a
   receiver MUST silently ignore this TLV if unknown to it, and continue
   processing the rest of the message. Whereas, The value of F-bit MUST
   be set to 0. Once advertised, this capability cannot be withdrawn;
   thus, the S-bit MUST be set to 1 in an Initialization and Capability
   message.

   The capability data associated with this State Advertisement Control
   (SAC) Capability TLV is one or more State Advertisement Control
   Elements, where each element indicates enabling/disabling of
   advertisement of uninteresting state for a given application. The
   format of a SAC Element is defined as follows:

```
            0 1 2 3 4 5 6 7
           +-+-+-+-+-+-+-+-+
           |D| App |Unused |
           +-+-+-+-+-+-+-+-+
```
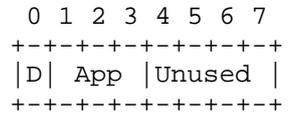
   Figure 2: Format of "State Advertisement Control Element"

   Where:
   D-bit: Controls the advertisement of the state specified in the "App"
   field:
      1: Disable state advertisement
      0: Enable state advertisement
         When sent in an Initialization message, the D-bit MUST be set
         to 1.

App: Defines the legacy application type whose state advertisement is
   to be controlled. The value of this field is defined as follows:

   1: IPv4 Prefix-LSPs (LSPs for IPv4 prefixes)
   2: IPv6 Prefix-LSPs (LSPs for IPv6 prefixes)
   3: FEC 128 P2P-PW (L2VPN PWid FEC signaling)
   4: FEC 129 P2P-PW (L2VPN Generalized PWid FEC signaling)

   Any other value in this field MUST be treated as an error.

Unused: Must Be Zero (MBZ) on transmit and ignored on receipt.

The "Length" field of the SAC Capability TLV (in octets) is computed
as follows:

   Length (in octets) = 1 + number of SAC elements

For example, if there are two SAC elements present, then the "Length"
field is set to 3 octets. A receiver of this capability TLV can
deduce the number of elements present in the TLV by using the
"Length" field.

This document uses the term "element" to refer to a SAC Element.

As described earlier, the SAC Capability TLV MAY be included by an
LDP speaker in an Initialization message to signal to its peer LSR
that state exchange for one or more applications needs to be disabled
on the given peer session. This TLV can also be sent later in a
Capability message to selectively enable or disable these
applications. If there is more than one element present in a SAC
Capability TLV, the elements MUST belong to distinct app types and
the app type MUST NOT appear more than once. If a receiver receives
such a malformed TLV, it SHOULD discard this TLV and continue
processing the rest of the message. If an LSR receives a message
with a SAC capability TLV containing an element with the "App" field
set to a value other than defined above, the receiver MUST ignore and
discard the element and continue processing the rest of the TLV.

To control more than one application state, a sender LSR can either
send a single capability TLV in a message with multiple elements
present or send separate messages with a capability TLV specifying
one or more elements. A receiving LSR, however, MUST treat each
incoming capability TLV with an element corresponding to a given
application type as an update to its existing policy for the given
type.

To understand capability updates from an example, let us consider two
LSRs, S (LDP speaker) and P (LDP peer), both of which support all the
non-negotiated applications listed earlier. By default, these LSRs
will advertise state for these applications, as configured, to their
peer as soon as an LDP session is established. Now assume that P
receives from S a SAC capability in an Initialization message with
"IPv6 Prefix-LSPs" and "FEC 129 P2P-PW" applications disabled. This
updates P's outbound policy towards S to advertise state related to
only IPv4 Prefix-LSPs and FEC 128 P2P-PW applications. Later, P
receives another capability update from S via a Capability message
with "IPv6 Prefix-LSPs" enabled and "FEC 128 P2P-PWs" disabled. This
results in P's outbound policy towards S to advertise both IPv4 and
IPv6 Prefix-LSPs application state and disable both FEC 128 and FEC
129 P2P-PWs signaling. Finally, P receives another update from S via
a Capability message that specifies to disable all four non-
negotiated applications states, resulting in P outbound policy
towards S to block/disable state for all these applications and only
advertise state for any other application, as applicable.

4.2. Capabilities Procedures

The SAC capability conveys the desire of an LSR to disable the
receipt of unwanted/unnecessary state from its LDP peer. This
capability is unilateral and unidirectional in nature, and a
receiving LSR is not required to send a similar capability TLV in an
Initialization or Capability message towards the sender of this
capability. This unilateral behavior conforms to the procedures
defined in the Section 6 of LDP Capabilities [RFC5561].

After this capability is successfully negotiated (i.e., sent by an
LSR and received/understood by its peer), then the receiving LSR MUST
NOT advertise any state related to the disabled applications towards
the capability-sending LSR until and unless these application states
are explicitly enabled again via a capability update. Upon receipt
of a capability update to disable an enabled application state during
the lifetime of a session, the receiving LSR MUST also withdraw from
the peer any previously advertised state corresponding to the
disabled application.

If a receiving LDP speaker does not understand the SAC capability
TLV, then it MUST respond to the sender with an "Unsupported TLV"
notification as described in "LDP Capabilities" [RFC5561]. If a
receiving LDP speaker does not understand or does not support an
application specified in an application control element, it SHOULD
silently ignore/skip such an element and continue processing rest of
the TLV.

4.2.1. State Control Capability in an Initialization Message

   The LDP Capabilities framework [RFC5561] dictates that the S-bit of
   the capability parameter in an Initialization message MUST be set to
   1 and SHOULD be ignored on receipt.

   An LDP speaker determines (e.g., via some local configuration or
   default policy) if it needs to disable Prefix-LSPs and/or P2P-PW
   applications with a peer LSR. If there is a need to disable, then
   the SAC TLV needs to be included in the Initialization message with
   respective SAC elements included with their D-bit set to 1.

   An LDP speaker that supports the SAC capability MUST interpret the
   capability TLV in a received Initialization message such that it
   disables the advertisement of the application state towards the
   capability sending LSR for Prefix-LSPs and/or P2P-PW applications if
   their SAC element's D-bit is set to 1.

4.2.2. State Control Capability in a Capability Message

   If the LDP peer supports "Dynamic Announcement Capability" [RFC5561],
   then an LDP speaker may send a SAC capability in a Capability message
   towards the peer. Once advertised, these capabilities cannot be
   withdrawn; hence, the S-bit of the TLV MUST be set to 1 when sent in
   a Capability message.

   An LDP speaker may decide to send this TLV towards an LDP peer if one
   or more of its Prefix-LSPs and/or P2P-PW applications get disabled,
   or if a previously disabled application gets enabled again. In this
   case, the LDP speaker constructs the TLV with appropriate SAC
   elements and sends the corresponding capability TLV in a Capability
   message.

   Upon receipt of this TLV in a Capability message, the receiving LDP
   speaker reacts in the same manner as it reacts upon the receipt of
   this TLV in an Initialization message. Additionally, the peer
   withdraws/advertises the application state to/from the capability-
   sending LDP speaker according to the capability update.

5. Applicability Statement

   The procedures defined in this document may result in a disabling
   announcement of label bindings for IP Prefixes and/or P2P PW FECs
   and, hence, should be used with caution and discretion. This
   document recommends that this new SAC capability and its procedures
   SHOULD be enabled on an LSR only via a configuration knob. This knob
   could either be a global LDP knob or be implemented per LDP neighbor.
   Hence, it is recommended that an operator SHOULD enable this

capability and its associated procedures on an LSR towards a neighbor
only if it is known that such bindings advertisement and exchange
with the neighbor is unnecessary and wasteful.

The following table summarizes a non-exhaustive list of typical LDP
session types on which this new SAC capability and its procedures are
expected to be applied to disable advertisement of uninteresting
state:

Session Type(s)	Uninteresting State
===	===
P2P-PW FEC 128-only	IP Prefix LSPs + P2P-PW FEC 129
P2P-PW only (FEC 128/129)	IP Prefix LSPs
IPv4-only on a Dual-Stack LSR	IPv6 Prefix LSPs + P2P-PW
IPv6-only on a Dual-Stack LSR	IPv4 Prefix LSPs + P2P-PW
mLDP-only	IP Prefix LSPs + P2P-PW
ICCP-only	IP Prefix LSPs + P2P-PW

It is to be noted that if an application state needs changing after
session initialization (e.g., to enable a previously disabled
application or to disable a previously enabled application), the
procedures defined in this document expect LSR peers to support the
LDP "Dynamic Announcement" Capability to announce the change in SAC
capability via an LDP Capability message. However, if any of the
peering LSRs do not support this capability, the alternate option is
to force reset the LDP session to advertise the new SAC capability
accordingly during the following session initialization.

The following are some additional important points that an operator
needs to consider regarding the applicability of this new capability
and associated procedures defined in this document:

- An operator SHOULD disable Prefix-LSP state on any Targeted LDP
   (tLDP) session that is established for ICCP-only and/or PW-only
   purposes.

- An operator MUST NOT disable Prefix-LSP state on any tLDP session
   that is established for reasons related to remote Loop-Free
   Alternate (LFA) Fast Re-Route (FRR) [RLFA].

-   In a remote network that is LFA FRR [RLFA] enabled, it is
    RECOMMENDED not to disable Prefix-LSP state on a tLDP session even
    if the current session type is PW-only and/or ICCP-only. This is
    recommended because any remote/tLDP neighbor could potentially be
    picked as a remote LFA PQ node.

-   This capability SHOULD be enabled for Prefix-LSPs in the scenarios
    when it is desirable to disable (or enable) advertisement of "all"
    the prefix label bindings. For scenarios in which a "subset" of
    bindings need to be filtered, the existing filtering procedures
    pertaining to label binding announcement should be used.

-   Using label advertisement filtering policies in conjunction with
    the procedures defined in this document for Prefix-LSPs is
    allowed. In such cases, the label bindings will be announced as
    per the label filtering policy for the given neighbor when Prefix-
    LSP application is enabled.

6. Operational Examples

6.1. Disabling Prefix-LSPs and P2P-PWs on an ICCP Session

   Consider two PE routers, LSR1 and LSR2, that understand/support SAC
   capability TLV and have an established LDP session to exchange ICCP
   state related to dual-homed devices connected to these LSRs. Let us
   assume that both LSRs are provisioned not to exchange any state for
   Prefix-LSPs (IPv4/IPv6) and P2P-PWs (FEC 128/129) application.

   To indicate their disinterest in these applications, the LSRs will
   include a SAC capability TLV (with four SAC elements corresponding to
   these four applications with D-bit set to 1 for each one) in the
   Initialization message. Upon receipt of this TLV in Initialization
   message, the receiving LSR will disable the advertisement of
   IPv4/IPv6 label bindings, as well as P2P PW FEC 128/129 signaling,
   towards its peer after session establishment.

6.2. Disabling Prefix-LSPs on a L2VPN/PW tLDP Session

   Consider LSR1 and LSR2 have an established tLDP session for P2P-PW
   applications to exchange label bindings for FEC 128/129. Given that
   there is no need to exchange IP label bindings amongst the PE LSRs
   over a PW tLDP session in most typical deployments, let us assume
   that LSRs are provisioned to disable IPv4/IPv6 Prefix-LSPs
   application state on the given PW session.

   To indicate their disinterest in Prefix-LSP applications over a PW
   tLDP session, the LSRs will follow/apply the same procedures as
   described in previous section. As a result, only P2P-PW-related
   state will be exchanged between these LSRs over this tLDP session.

6.3. Disabling Prefix-LSPs Dynamically on an Established LDP Session

   Assume that LSRs from previous sections were initially provisioned to
   exchange both Prefix-LSP and P2P-PW state over the session between
   them and also support the "Dynamic Announcement" Capability of
   [RFC5561]. Now, assume that LSR1 is dynamically provisioned to
   disable (IPv4/IPv6) Prefix-LSPs over a tLDP session with LSR2. In
   this case, LSR1 will send a SAC capability TLV in a Capability
   message towards LSR2 with application control elements defined for
   IPv4 and IPv6 Prefix-LSPs with the D-bit set to 1. Upon receipt of
   this TLV, LSR2 will disable Prefix-LSPs application state(s) towards
   LSR1 and withdraw all previously advertised application state from
   LSR1. To withdraw label bindings from its peer, LSR2 MAY use a
   single Prefix FEC Typed Wildcard Label Withdraw message [RFC5918] if
   the peer supports the Typed Wildcard FEC capability.

   This dynamic disability of Prefix-LSPs application does not impact
   L2VPN P2P-PW application on the given session, and both LSRs should
   continue to exchange state related to PW Signaling applications.

6.4. Disabling Prefix-LSPs on an mLDP-only Session

   Assume that LSR1 and LSR2 have formed an LDP session to exchange mLDP
   state only. In typical deployments, LSR1 and LSR2 also exchange
   bindings for IP (unicast) prefixes upon mLDP session, which is
   unnecessary and wasteful for an mLDP-only LSR.

   Using the procedures defined earlier, an LSR can indicate its
   disinterest in Prefix-LSP application state to its peer upon session
   establishment time or dynamically later via an LDP capabilities
   update.

   In reference to Section 3.1, the peer disables the advertisement of
   any state related to IP Prefix FECs, but it still advertises IP
   address bindings that are required for the correct operation of mLDP.

6.5. Disabling IPv4 or IPv6 Prefix-LSPs on a Dual-Stack LSR

   In IP dual-stack scenarios, LSR2 may advertise unnecessary state
   (e.g., IPv6 prefix label bindings) towards peer LSR1 corresponding to
   IPv6 Prefix-LSP applications once a session is established mainly for
   exchanging state for IPv4. The similar scenario also applies when

advertising IPv4 Prefix-LSP state on a session meant for IPv6. The
SAC capability and its procedures defined in this document can help
to avoid such unnecessary state advertisement.

Consider an IP dual-stack environment where LSR2 is enabled for
Prefix-LSPs application for both IPv4 and IPv6, but LSR1 is enabled
for (or interested in) only IPv4 Prefix-LSPs. To avoid receiving
unwanted state advertisement for IPv6 Prefix-LSP applications from
LSR2, LSR1 can send a SAC capability with an element for IPv6 Prefix-
LSPs with the D-bit set to 1 in the Initialization message towards
LSR2 at the time of session establishment. Upon receipt of this
capability, LSR2 will disable all IPv6 label binding advertisements
towards LSR1. If IPv6 Prefix-LSP applications are later enabled on
LSR1, LSR1 can update the capability by sending a SAC capability in a
Capability message towards LSR2 to enable this application
dynamically.

7. Security Considerations

   The proposal introduced in this document does not introduce any new
   security considerations beyond those that already apply to the base
   LDP specification [RFC5036] and to MPLS and GMPLS [RFC5920].

8. IANA Considerations

   This document defines a new LDP capability parameter TLV. IANA has
   assigned the following value from "TLV Type Name Space" in the "Label
   Distribution Protocol (LDP) Parameters" registry as the new code
   point for the new LDP capability TLV code point.

```
+--------+--------------------+-----------+----------------------+
| Value  | Description        | Reference |Notes/Registration Date|
+--------+--------------------+-----------+----------------------+
| 0x050D | State Advertisement | RFC 7473 |                      |
|        | Control Capability |           |                      |
+--------+--------------------+-----------+----------------------+
```

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,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC5036] Andersson, L., Ed., Minei, I., Ed., and B. Thomas, Ed.,
              "LDP Specification", RFC 5036, October 2007,
              <http://www.rfc-editor.org/info/rfc5036>.

   [RFC5561] Thomas, B., Raza, K., Aggarwal, S., Aggarwal, R., and JL.
              Le Roux, "LDP Capabilities", RFC 5561, July 2009,
              <http://www.rfc-editor.org/info/rfc5561>.

9.2. Informative References

   [RFC4447] Martini, L., Ed., Rosen, E., El-Aawar, N., Smith, T., and
              G. Heron, "Pseudowire Setup and Maintenance Using the
              Label Distribution Protocol (LDP)", RFC 4447, April 2006,
              <http://www.rfc-editor.org/info/rfc4447>.

   [RFC4762] Lasserre, M., Ed., and V. Kompella, Ed., "Virtual Private
              LAN Service (VPLS) Using Label Distribution Protocol (LDP)
              Signaling", RFC 4762, January 2007,
              <http://www.rfc-editor.org/info/rfc4762>.

   [RFC5918] Asati, R., Minei, I., and B. Thomas, "Label Distribution
              Protocol (LDP) 'Typed Wildcard' Forward Equivalence Class
              (FEC)", RFC 5918, August 2010,
              <http://www.rfc-editor.org/info/rfc5918>.

   [RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS
              Networks", RFC 5920, July 2010,
              <http://www.rfc-editor.org/info/rfc5920>.

   [RFC6388] Wijnands, IJ., Ed., Minei, I., Ed., Kompella, K., and B.
              Thomas, "Label Distribution Protocol Extensions for Point-
              to-Multipoint and Multipoint-to-Multipoint Label Switched
              Paths", RFC 6388, November 2011,
              <http://www.rfc-editor.org/info/rfc6388>.

   [RFC7275] Martini, L., Salam, S., Sajassi, A., Bocci, M.,
              Matsushima, S., and T. Nadeau, "Inter-Chassis
              Communication Protocol for Layer 2 Virtual Private Network
              (L2VPN) Provider Edge (PE) Redundancy", RFC 7275, June
              2014, <http://www.rfc-editor.org/info/rfc7275>.

   [RFC7338] Jounay, F., Ed., Kamite, Y., Ed., Heron, G., and M. Bocci,
              "Requirements and Framework for Point-to-Multipoint
              Pseudowires over MPLS Packet Switched Networks", RFC 7338,
              September 2014, <http://www.rfc-editor.org/info/rfc7338>.

   [RLFA]   Bryant, S., Filsfils, C., Previdi, S., Shand, M., and N.
              So, "Remote Loop-Free Alternate (LFA) Fast Re-Route
              (FRR)", draft-ietf-rtgwg-remote-lfa-11, Work in Progress,
              January 2015.

Acknowledgments

Authors' Addresses

   Kamran Raza
   Cisco Systems, Inc.
   2000 Innovation Drive
   Ottawa, ON K2K-3E8
   Canada
   EMail: skraza@cisco.com

   Sami Boutros
   Cisco Systems, Inc.
   3750 Cisco Way
   San Jose, CA 95134
   United States
   EMail: sboutros@cisco.com