Internet Engineering Task Force (IETF)
Request for Comments: 8223
Updates: 7473
Category: Standards Track
ISSN: 2070-1721

S. Esale
R. Torvi
Juniper Networks
L. Jalil
Verizon
U. Chunduri
Huawei
K. Raza
Cisco Systems, Inc.

August 2017

Application-Aware Targeted LDP

Abstract

Recent Targeted Label Distribution Protocol (tLDP) applications, such as remote Loop-Free Alternates (LFAs) and BGP auto-discovered pseudowires, may automatically establish a tLDP session with any Label Switching Router (LSR) in a network. The initiating LSR has information about the targeted applications to administratively control initiation of the session. However, the responding LSR has no such information to control acceptance of this session. This document defines a mechanism to advertise and negotiate the Targeted Application Capability (TAC) during LDP session initialization. As the responding LSR becomes aware of targeted applications, it may establish a limited number of tLDP sessions for certain applications. In addition, each targeted application is mapped to LDP Forwarding Equivalence Class (FEC) elements to advertise only necessary LDP FEC label bindings over the session. This document updates RFC 7473 for enabling advertisement of LDP FEC label bindings over the session.

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 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8223.

Table of Contents

1. Introduction

LDP uses the Extended Discovery mechanism to establish the Targeted LDP (tLDP) adjacency and subsequent session, as described in [RFC5036]. A Label Switching Router (LSR) initiates Extended Discovery by sending a tLDP Hello to a specific address. The remote LSR decides to either accept or ignore the tLDP Hello based on local configuration only. A tLDP application is an application that uses a tLDP session to exchange information such as FEC label bindings ("FEC" stands for "Forwarding Equivalence Class") with a peer LSR in the network. For an application such as FEC 128 pseudowire, the remote LSR is configured with the source LSR address so that it can use that information to accept or ignore a given tLDP Hello.

However, applications such as remote Loop-Free Alternates (LFAs) and BGP auto-discovered pseudowires automatically initiate asymmetric Extended Discovery to any LSR in a network based on local state only. With these applications, the remote LSR is not explicitly configured with the source LSR address. So, the remote LSR either responds to all tLDP Hellos or ignores them.

In addition, since the session is initiated and established after adjacency formation, the responding LSR has no information on targeted applications available from which it can choose a session with a targeted application that it is configured to support. Also, the initiating LSR may employ a limit per application on locally initiated automatic tLDP sessions; however, the responding LSR has no such information to employ a similar limit on the incoming tLDP sessions. Further, the responding LSR does not know whether the source LSR is establishing a tLDP session for configured applications, automatic applications, or both.

This document proposes and describes a solution to advertise the Targeted Application Capability (TAC), consisting of a list of targeted applications, during initialization of a tLDP session. It also defines a mechanism to enable a new application and disable an old application after session establishment. This capability advertisement provides the responding LSR with the necessary information to control the acceptance of tLDP sessions per application. For instance, an LSR may accept all BGP auto-discovered tLDP sessions as described in [RFC6074] but may only accept a limited number of remote LFA tLDP sessions as described in [RFC7490].

Also, the tLDP application is mapped to LDP FEC element types to advertise specific application FECs only, avoiding the advertisement of other unnecessary FECs over a tLDP session.

1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

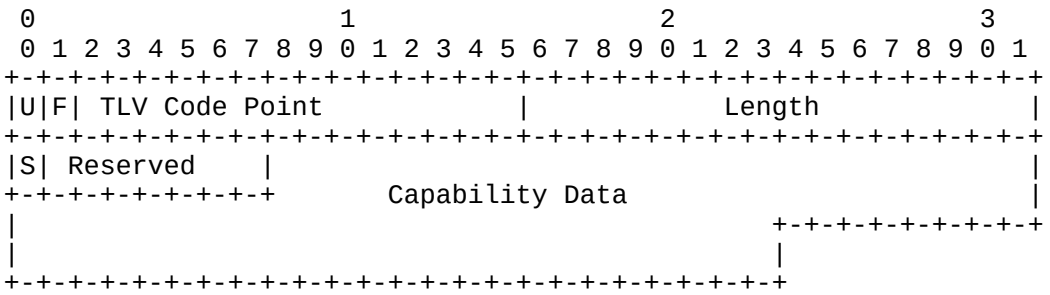
In addition to the terminology defined in [RFC7473], this document uses the following terms:

```
tLDP    : Targeted LDP
TAC     : Targeted Application Capability
TAE     : Targeted Application Element
TA-Id   : Targeted Application Identifier
SAC     : State Advertisement Control
LSR     : Label Switching Router
mLDP    : Multipoint LDP
PQ node : Remote LFA next hops
RSVP-TE : RSVP Traffic Engineering
P2MP    : Point-to-Multipoint
PW      : Pseudowire
P2P-PW  : Point-to-Point Pseudowire
MP2MP   : Multipoint-to-Multipoint
HSMP LSP: Hub and Spoke Multipoint Label Switched Path
LSP     : Label Switched Path
MP2P    : Multipoint-to-Point
MPT     : Merge Point
```

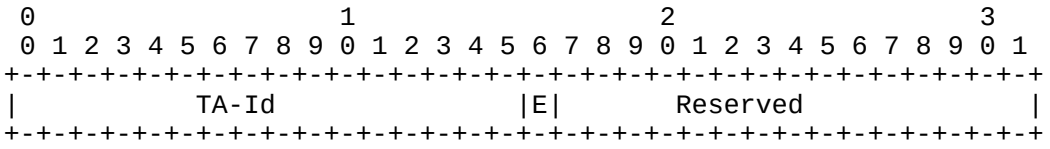
2. Targeted Application Capability

2.1. Encoding

An LSR MAY advertise that it is capable of negotiating a tLDP application list over a tLDP session by using the capability advertisement as defined in [RFC5561] and encoded as follows:



Flag "U" MUST be set to 1 to indicate that this capability must be silently ignored if unknown. The TAC's Capability Data field contains the Targeted Application Element (TAE) information, encoded as follows:



TA-Id: A 16-bit Targeted Application Identifier value.

E: E-bit (Enable bit). Indicates whether the sender is advertising or withdrawing the TAE. The E-bit value is used as follows:

1 - The TAE is advertising the targeted application.
0 - The TAE is withdrawing the targeted application.

2.2. Procedures

At tLDP session establishment time, an LSR MAY include a new capability TLV, the TAC TLV, as an optional TLV in the LDP Initialization message. The TAC TLV's Capability data MAY consist of zero or more TAEs, each pertaining to a unique TA-Id that an LSR supports over the session. If the receiver LSR receives the same TA-Id in more than one TAE, it MUST process the first element and

ignore the duplicate elements. If the receiver LSR receives an unknown TA-Id in the TAE, it MUST silently ignore such a TAE and continue processing the rest of the TLV.

If the receiver LSR does not receive the TAC TLV in the Initialization message or it does not understand the TAC TLV, the TAC negotiation is considered unsuccessful and the session establishment proceeds as per [RFC5036]. On receipt of a valid TAC TLV, an LSR MUST generate its own TAC TLV with TAEs consisting of unique TA-Ids that it supports over the tLDP session. If there is at least one common TAE between the TAC TLV it has received and its own, the session MUST proceed to establishment as per [RFC5036]. If not, an LSR MUST send a 'Session Rejected/Targeted Application Capability Mismatch' Notification message to the peer and close the session. The initiating LSR SHOULD tear down the corresponding tLDP adjacency after sending or receiving a 'Session Rejected/Targeted Application Capability Mismatch' Notification message to or from the responding LSR, respectively.

If both of the peers support the TAC TLV, an LSR decides to establish or close a tLDP session based on the negotiated list of targeted applications. For example, an initiating LSR advertises A, B, and C as TA-Ids, and the responding LSR advertises C, D, and E as TA-Ids. Then, the negotiated TA-Id as per both LSRs is C. In another example, an initiating LSR advertises A, B, and C as TA-Ids, and the responding LSR, which acts as a passive LSR, advertises all of the applications -- A, B, C, D, and E -- as TA-Ids that it supports over this session. The negotiated targeted applications as per both LSRs are then A, B, and C. Finally, if the initiating LSR advertises A, B, and C as TA-Ids and the responding LSR advertises D and E as TA-Ids, then the negotiated targeted applications as per both LSRs are "none". Therefore, if the intersection of the sets of received and sent TA-Ids is null, then the LSR sends a 'Session Rejected/Targeted Application Capability Mismatch' Notification message to the peer LSR and closes the session.

When the responding LSR playing the active role [RFC5036] in LDP session establishment receives a 'Session Rejected/Targeted Application Capability Mismatch' Notification message, it MUST set its session setup retry interval to a maximum value -- that is, 0xFFFF. The session MAY stay in a non-existent state. When it detects a change in the initiating LSR or local LSR configuration pertaining to the TAC TLV, it MUST clear the session setup backoff delay associated with the session to reattempt session establishment. An LSR detects the configuration change on the other LSR upon receipt of a tLDP Hello message that has a higher configuration sequence number than the earlier tLDP Hello message.

When the initiating LSR playing the active role in LDP session establishment receives a 'Session Rejected/Targeted Application Capability Mismatch' Notification message, it MUST either (1) close the session and tear down the corresponding tLDP adjacency or (2) set its session setup retry interval to a maximum value -- that is, 0xFFFF.

If the initiating LSR decides to tear down the associated tLDP adjacency, the session is closed on the initiating LSR as well as the responding LSR. It MAY also take appropriate actions. For instance, if an automatic session intended to support the remote LFA application is rejected by the responding LSR, the initiating LSR may inform the IGP to calculate another PQ node [RFC7490] for the route or set of routes. More specific actions are a local matter and are outside the scope of this document.

If the initiating LSR sets the session setup retry interval to maximum, the session MAY stay in a non-existent state. When this LSR detects a change in the responding LSR configuration or its own configuration pertaining to the TAC TLV, it MUST clear the session setup backoff delay associated with the session in order to reattempt session establishment.

After a tLDP session using the TAC mechanism has been established, the initiating and responding LSRs MUST distribute FEC label bindings for the negotiated applications only. For instance, if the tLDP session is established for a BGP auto-discovered pseudowire, only FEC 129 label bindings MUST be distributed over the session. Similarly, an LSR operating in downstream on-demand mode MUST request FEC label bindings for the negotiated applications only.

If the TAC and the Dynamic Capability [RFC5561] are negotiated during session initialization, the TAC MAY be renegotiated after session establishment by sending an updated TAC TLV in the LDP Capability message. The updated TAC TLV carries TA-Ids with an incremental update only. The updated TLV MUST consist of one or more TAEs with the E-bit set (1) or off (0), to advertise or withdraw the new application and the old application, respectively. This may lead to advertisements or withdrawals of certain types of FEC label bindings over the session or to teardown of the tLDP adjacency and, subsequently, the session.

The TAC is advertised on the tLDP session only. If the tLDP session changes to a link session, an LSR SHOULD withdraw it with the S-bit set to 0. Similarly, if the link session changes to tLDP, an LSR SHOULD advertise it via the Capability message. If the capability negotiation fails, this may lead to destruction of the tLDP session.

By default, an LSR SHOULD accept tLDP Hellos in order to then accept or reject the tLDP session based on the application information.

In addition, an LSR SHOULD allow the configuration of any TA-Id in order to facilitate the use of private TA-Ids by a network operator.

2.3. LDP Message Procedures

2.3.1. Initialization Message

1. The S-bit of the TAC TLV MUST be set to 1 to advertise the TAC and SHOULD be ignored on receipt, as described in [RFC5561].

2. The E-bit of the TAE MUST be set to 1 to enable the targeted application and SHOULD be ignored on receipt.

3. An LSR MAY add the State Advertisement Control Capability by mapping the TAE to the State Advertisement Control (SAC) elements as defined in Section 4.

2.3.2. Capability Message

After a change to local configuration, the initiating or responding LSR may renegotiate the TAC via the Capability message.

1. The S-bit of the TAC is set to 1 or 0 to advertise or withdraw it.

2. After the configuration change, if there is no common TAE between its new TAE list and the peer's TAE list, the LSR MUST send a 'Session Rejected/Targeted Application Capability Mismatch' Notification message and close the session.

3. If there is a common TAE, an LSR MAY also update the SAC Capability based on the updated TAC, as described in Section 4, and send the updated TAC and SAC Capability in a Capability message to the peer.

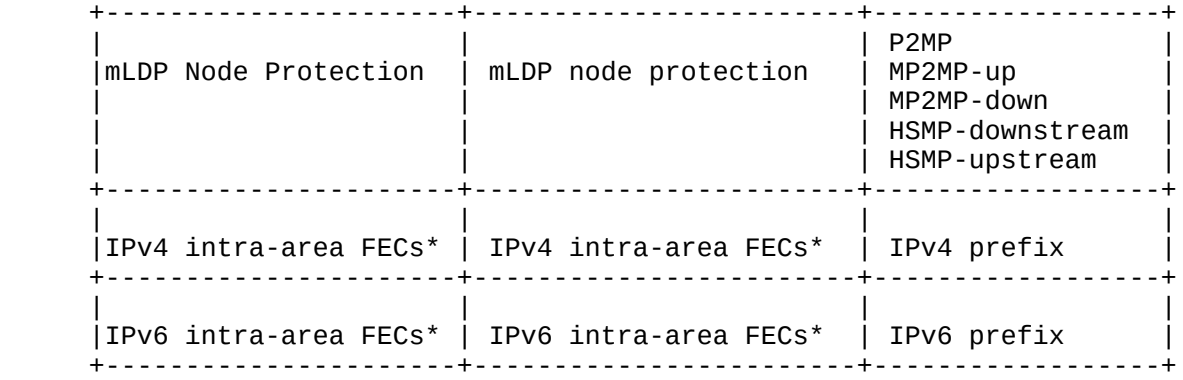
4. A receiving LSR processes the Capability message with the TAC TLV. If the S-bit is set to 0, the TAC is disabled for the session.

5. If the S-bit is set to 1, the LSR processes a list of TAEs from the TAC's data with the E-bit set to 1 or 0 to update the peer's TAE.

3. Targeted Application FEC Advertisement Procedures

The tLDP application MUST be mapped to LDP FEC element types as follows to advertise only necessary LDP FEC label bindings over the tLDP session.

Targeted Application	Description	FEC Mappings
LDPv4 Tunneling	LDP IPv4 over RSVP-TE or other MPLS tunnel	IPv4 prefix
LDPv6 Tunneling	LDP IPv6 over RSVP-TE or other MPLS tunnel	IPv6 prefix
mLDP Tunneling	mLDP over RSVP-TE or other MPLS tunnel	P2MP MP2MP-up MP2MP-down HSMP-downstream HSMP-upstream
LDPv4 remote LFA	LDPv4 over LDPv4 or other MPLS tunnel	IPv4 prefix
LDPv6 remote LFA	LDPv6 over LDPv6 or other MPLS tunnel	IPv6 prefix
LDP FEC 128 PW	LDP FEC 128 Pseudowire	PWid FEC element
LDP FEC 129 PW	LDP FEC 129 Pseudowire	Generalized PWid FEC element
LDP Session Protection	LDP session protection	FEC types as per protected session
LDP ICCP	LDP Inter-Chassis Communication Protocol	None
LDP P2MP PW	LDP P2MP Pseudowire	P2MP PW Upstream FEC element



* Intra-area FECs: FECs that are on the shortest-path tree and are not leafs of the shortest-path tree.

4. Interaction of Targeted Application Capabilities and State Advertisement Control Capabilities

As described in this document, the set of TAEs negotiated between two LDP peers advertising the TAC represents the willingness of both peers to advertise state information for a set of applications. The set of applications negotiated by the TAC mechanism is symmetric between the two LDP peers. In the absence of further mechanisms, two LDP peers will both advertise state information for the same set of applications.

As described in [RFC7473], the SAC TLV can be used by an LDP speaker to communicate its interest or disinterest in receiving state information from a given peer for a particular application. Two LDP peers can use the SAC mechanism to create asymmetric advertisements of state information between the two peers.

The TAC negotiation facilitates the awareness of targeted applications to both of the peers. It enables them to advertise only necessary LDP FEC label bindings corresponding to negotiated applications. With the SAC, the responding LSR is not aware of targeted applications. Thus, it may be unable to communicate its interest or disinterest in receiving state information from the peer. Therefore, when the responding LSR is not aware of targeted applications such as remote LFAs and BGP auto-discovered pseudowires, the TAC mechanism should be used, and when the responding LSR is aware (with appropriate configuration) of targeted applications such as FEC 128 pseudowire, the SAC mechanism should be used. Also, after the TAC mechanism makes the responding LSR aware of targeted applications, the SAC mechanism may be used to communicate its

disinterest in receiving state information from the peer for a particular negotiated application, creating asymmetric advertisements.

Thus, the TAC mechanism enables two LDP peers to symmetrically advertise state information for negotiated targeted applications. Further, the SAC mechanism enables both of them to asymmetrically disable receipt of state information for some of the already-negotiated targeted applications. Collectively, the TAC mechanism and the SAC mechanism can both be used to control the FEC label bindings that are advertised over the tLDP session. For instance, suppose that the initiating LSR establishes a tLDP session, using the TAC mechanism, with the responding LSR for remote LFA and FEC 129 PW targeted applications. So, each LSR advertises the corresponding FEC label bindings. Further, suppose that the initiating LSR is not the PQ node for the responding LSR's remote LFA IGP calculations. In such a case, the responding LSR may use the SAC mechanism to convey its disinterest in receiving state information for remote LFA tLDP applications.

For a given tLDP session, the TAC mechanism can be used without the SAC mechanism, and the SAC mechanism can be used without the TAC mechanism. It is useful to discuss the behavior that occurs when the TAC and SAC mechanisms are used on the same tLDP session. The TAC mechanism MUST take precedence over the SAC mechanism with respect to enabling applications for which state information will be advertised. For a tLDP session using the TAC mechanism, the LDP peers MUST NOT advertise state information for an application that has not been negotiated in the most recent TAE list (referred to as a non-negotiated application). This is true even if one of the peers announces its interest in receiving state information that corresponds to the non-negotiated application by sending a SAC TLV. In other words, when the TAC mechanism is being used, the SAC mechanism cannot and should not enable state information advertisements for applications that have not been enabled by the TAC mechanism.

On the other hand, the SAC mechanism MUST take precedence over the TAC mechanism with respect to disabling state information advertisements. If an LDP speaker has announced its disinterest in receiving state information for a given application to a given peer using the SAC mechanism, its peer MUST NOT send state information for that application, even if the two peers have negotiated the corresponding application via the TAC mechanism.

For the purposes of determining the correspondence between targeted applications defined in this document and application state as defined in [RFC7473], an LSR MUST use the following mappings:

LDPv4 Tunneling - IPv4 Prefix-LSPs
LDPv6 Tunneling - IPv6 Prefix-LSPs
LDPv4 Remote LFA - IPv4 Prefix-LSPs
LDPv6 Remote LFA - IPv6 Prefix-LSPs
LDP FEC 128 PW - FEC 128 P2P-PW
LDP FEC 129 PW - FEC 129 P2P-PW

An LSR MUST map the targeted application to the LDP capability as follows:

mLDP Tunneling - P2MP Capability, MP2MP Capability, and HSMP LSP Capability TLV

mLDP Node Protection - P2MP Capability, MP2MP Capability, and HSMP LSP Capability TLV

5. Use Cases

5.1. Remote LFA Automatic Targeted Session

The LSR determines that it needs to form an automatic tLDP session with a remote LSR based on IGP calculation as described in [RFC7490] or some other mechanism outside the scope of this document. The LSR forms the tLDP adjacency and constructs an Initialization message with the TAC TLV consisting of the TAE as the remote LFA during session establishment. The receiver LSR processes the LDP Initialization message and verifies whether it is configured to accept a remote LFA tLDP session. If it is, it may further verify that establishing such a session does not exceed the configured limit for remote LFA sessions. If all of these conditions are met, the receiver LSR may respond back with an Initialization message with the TAC corresponding to the remote LFA, and subsequently the session may be established.

After the session using the TAC mechanism has been established, the sender and receiver LSRs distribute IPv4 or IPv6 FEC label bindings over the session. Further, the receiver LSR may determine that it does not need these FEC label bindings. So, it may disable the receipt of these FEC label bindings by mapping the TAE to the State Advertisement Control Capability as described in Section 4.

5.2. FEC 129 Auto-discovery Targeted Session

BGP auto-discovery may determine whether the LSR needs to initiate an auto-discovery tLDP session with a border LSR. Multiple LSRs may try to form an auto-discovered tLDP session with a border LSR. So, a service provider may want to limit the number of auto-discovered tLDP sessions that a border LSR can accept. As described in Section 2, LDP may convey targeted applications with the TAC TLV to a border LSR. A border LSR may establish or reject the tLDP session based on local administrative policy. Also, as the receiver LSR becomes aware of targeted applications, it can also employ an administrative policy for security. For instance, it can employ a policy to accept all auto-discovered sessions from a source addresses list.

Moreover, the sender and receiver LSRs must exchange FEC 129 label bindings only over the tLDP session.

5.3. LDP over RSVP and Remote LFA Targeted Session

An LSR may want to establish a tLDP session with a remote LSR for LDP-over-RSVP tunneling and remote LFA applications. The sender LSR may add both of these applications as a unique TAE in the TAC data of a TAC TLV. The receiver LSR may have reached a configured limit for accepting remote LFA automatic tLDP sessions, but it may have been configured to accept LDP-over-RSVP tunneling. In such a case, the tLDP session is formed for both LDP-over-RSVP tunneling and remote LFA applications, as both need the same FECs -- IPv4, IPv6, or both.

5.4. mLDP Node Protection Targeted Session

A Merge Point (MPT) LSR may determine that it needs to form an automatic tLDP session with the upstream point of local repair (PLR) LSR for MP2P and MP2MP LSP [RFC6388] node protection as described in [RFC7715]. The MPT LSR may add a new tLDP application -- mLDP protection -- as a unique TAE in the TAC data of a TAC TLV and send it in the Initialization message to the PLR. If the PLR is configured for mLDP node protection and establishing this session does not exceed the limit of either mLDP node protection sessions or automatic tLDP sessions, the PLR may decide to accept this session. Also, the PLR may respond back with the Initialization message with a TAC TLV that has one of the TAEs as mLDP protection, and the session proceeds to establishment as per [RFC5036].

6. Security Considerations

The procedures described in this document do not introduce any changes to LDP security considerations as described in [RFC5036].

As described in [RFC5036], DoS attacks via Extended Hellos, which are required to establish a tLDP session, can be addressed by filtering Extended Hellos using access lists that define addresses with which Extended Discovery is permitted. Further, as described in Section 5.2 of this document, an LSR can employ a policy to accept all auto-discovered Extended Hellos from the configured source addresses list.

Also, for the two LSRs supporting the TAC, the tLDP session is only established after successful negotiation of the TAC. The initiating and receiving LSRs MUST only advertise TA-Ids that they support -- in other words, what they are configured for over the tLDP session.

7. IANA Considerations

IANA has assigned the following code point for the new Capability Parameter TLV defined in this document. The code point has been assigned from the "TLV Type Name Space" sub-registry of the "Label Distribution Protocol (LDP) Parameters" registry.

Value	Description	Reference
0x050F	Targeted Application Capability	RFC 8223

IANA has assigned a new status code from the "Status Code Name Space" sub-registry of the "Label Distribution Protocol (LDP) Parameters" registry.

Value	E	Description	Reference
0x0000004C	1	Session Rejected/Targeted Application Capability Mismatch	RFC 8223

IANA has created a new registry called "LDP Targeted Application Identifier" in the "Label Distribution Protocol (LDP) Parameters" registry. The range is 0x0001-0xFFFE. Values in the range 0x0001-0x1FFF in this registry shall be allocated according to the "IETF Review" procedure [RFC8126]; values in the range 0x2000-0xF7FF shall be allocated according to the "First Come First Served" procedure [RFC8126]. The initial values are as follows.

Value	Description	Reference
0x0000	Reserved	RFC 8223
0x0001	LDPv4 Tunneling	RFC 8223
0x0002	LDPv6 Tunneling	RFC 8223
0x0003	mLDP Tunneling	RFC 8223
0x0004	LDPv4 Remote LFA	RFC 8223
0x0005	LDPv6 Remote LFA	RFC 8223
0x0006	LDP FEC 128 PW	RFC 8223
0x0007	LDP FEC 129 PW	RFC 8223
0x0008	LDP Session Protection	RFC 8223
0x0009	LDP ICCP	RFC 8223
0x000A	LDP P2MP PW	RFC 8223
0x000B	mLDP Node Protection	RFC 8223
0x000C	LDPv4 Intra-area FECs	RFC 8223
0x000D	LDPv6 Intra-area FECs	RFC 8223
0x000E-0xF7FF	Unassigned	
0xF800-0xFBFF	Available for Private Use	
0xFC00-0xFFFE	Available for Experimental Use	
0xFFFF	Reserved	RFC 8223

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5036] Andersson, L., Ed., Minei, I., Ed., and B. Thomas, Ed., "LDP Specification", RFC 5036, DOI 10.17487/RFC5036, October 2007, <https://www.rfc-editor.org/info/rfc5036>.

[RFC5561] Thomas, B., Raza, K., Aggarwal, S., Aggarwal, R., and JL. Le Roux, "LDP Capabilities", RFC 5561, DOI 10.17487/RFC5561, July 2009, <https://www.rfc-editor.org/info/rfc5561>.

[RFC7473] Raza, K. and S. Boutros, "Controlling State Advertisements of Non-negotiated LDP Applications", RFC 7473, DOI 10.17487/RFC7473, March 2015, <https://www.rfc-editor.org/info/rfc7473>.

[RFC7715] Wijnands, IJ., Ed., Raza, K., Atlas, A., Tantsura, J., and Q. Zhao, "Multipoint LDP (mLDP) Node Protection", RFC 7715, DOI 10.17487/RFC7715, January 2016, <https://www.rfc-editor.org/info/rfc7715>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[RFC6074] Rosen, E., Davie, B., Radoaca, V., and W. Luo, "Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)", RFC 6074, DOI 10.17487/RFC6074, January 2011, <https://www.rfc-editor.org/info/rfc6074>.

[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, DOI 10.17487/RFC6388, November 2011, <https://www.rfc-editor.org/info/rfc6388>.

[RFC7490] Bryant, S., Filsfils, C., Previdi, S., Shand, M., and N. So, "Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)", RFC 7490, DOI 10.17487/RFC7490, April 2015, <https://www.rfc-editor.org/info/rfc7490>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Acknowledgments

The authors wish to thank Nischal Sheth, Hassan Hosseini, Kishore Tiruveedhula, Loa Andersson, Eric Rosen, Yakov Rekhter, Thomas Beckhaus, Tarek Saad, Lizhong Jin, and Bruno Decraene for their detailed reviews. Thanks to Manish Gupta and Martin Ehlers for their input to this work and many helpful suggestions.

Contributors

The following people contributed substantially to the content of this document and should be considered co-authors:

Chris Bowers
Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
United States of America
Email: cbowers@juniper.net

Zhenbin Li
Huawei
Bldg. No. 156 Beiqing Rd.
Beijing 100095
China
Email: lizhenbin@huawei.com

Authors' Addresses

Santosh Esale
Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
United States of America

Email: sesale@juniper.net

Raveendra Torvi
Juniper Networks
10 Technology Park Drive
Westford, MA 01886
United States of America

Email: rtorvi@juniper.net

Luay Jalil
Verizon
1201 East Arapaho Road
Richardson, TX 75081
United States of America

Email: luay.jalil@verizon.com

Uma Chunduri
Huawei
2330 Central Expressway
Santa Clara, CA 95050
United States of America

Email: uma.chunduri@huawei.com

Kamran Raza
Cisco Systems, Inc.
2000 Innovation Drive
Ottawa, ON K2K-3E8
Canada

Email: skraza@cisco.com