

MPLS Working Group
INTERNET-DRAFT
Updates: 7473 (if approved)
Intended Status: Proposed Standard
Expires: December 29, 2017

Santosh Esale
Raveendra Torvi
Juniper Networks
Luay Jalil
Verizon
Uma Chunduri
Huawei
Kamran Raza
Cisco Systems, Inc.
June 27, 2017

Application-aware Targeted LDP
draft-ietf-mpls-app-aware-tldp-09

Abstract

Recent targeted Label Distribution Protocol (tLDP) applications such as remote loop-free alternate (LFA) and BGP auto discovered pseudowire may automatically establish a tLDP session to 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 Targeted Applications 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 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/lid-abstracts.html>

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

Copyright and License Notice

Copyright (c) 2017 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. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

| | | |
|-------|---|----|
| 1 | Introduction | 4 |
| 1.1 | Conventions Used in This Document | 4 |
| 1.2 | Terminology | 5 |
| 2. | Targeted Application Capability | 5 |
| 2.1 | Encoding | 5 |
| 2.2 | Procedures | 6 |
| 2.3 | LDP message procedures | 8 |
| 2.3.1 | Initialization message | 8 |
| 2.3.2 | Capability message | 9 |
| 3. | Targeted Application FEC Advertisement Procedures | 9 |
| 4. | Interaction of Targeted Application Capabilities and State Advertisement Control Capabilities | 10 |
| 5. | Use cases | 12 |
| 5.1 | Remote LFA Automatic Targeted session | 12 |
| 5.2 | FEC 129 Auto Discovery Targeted session | 13 |
| 5.3 | LDP over RSVP and Remote LFA targeted session | 13 |
| 5.4 | mLDP node protection targeted session | 13 |
| 6. | Security Considerations | 14 |
| 7. | IANA Considerations | 14 |
| 8. | Acknowledgments | 15 |
| 9. | Contributing Authors | 15 |
| 10. | References | 16 |

| | | |
|------|----------------------------------|----|
| 10.1 | Normative References | 16 |
| 10.2 | Informative References | 16 |
| | Authors' Addresses | 17 |

1 Introduction

LDP uses the extended discovery mechanism to establish the tLDP adjacency and subsequent session as described in [RFC5036]. A LSR initiates extended discovery by sending tLDP Hello to specific address. The remote LSR decides to either accept or ignore the tLDP Hello based on local configuration only. Targeted LDP application is an application that uses tLDP session to exchange information such as FEC-Label bindings 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 given tLDP Hello.

However, applications such as Remote LFA and BGP auto discovered pseudowire 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 or ignores all tLDP Hellos.

In addition, since the session is initiated and established after adjacency formation, the responding LSR has no targeted applications information available to choose a session with 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, automatic or both applications.

This document proposes and describes a solution to advertise Targeted Application Capability (TAC), consisting of a targeted application list, during initialization of a tLDP session. It also defines a mechanism to enable an 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 defined in [RFC6074] but may only accept limited number of Remote LFA tLDP sessions as defined in [RFC7490]

Also, the targeted LDP application is mapped to LDP FEC element type 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 RFC 2119 [RFC2119] and RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2 Terminology

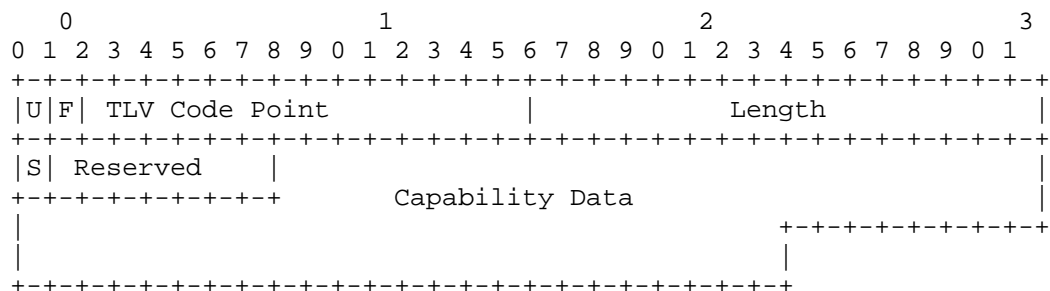
In addition to the terminology defined in [RFC7473], this document uses the following terms:

tLDP : Targeted LDP
 TAC : Targeted Application Capability
 TAE : Targeted Application Element
 TA-Id : Targeted Application Identifier
 SAC : State Advertisement Control Capability
 LSR : Label Switching Router
 mLDP : Multipoint LDP
 PQ : Remote-LFA nexthops
 RSVP-TE : RSVP Traffic Engineering
 P2MP : Point-to-Multipoint
 PW : Pseudowire
 P2P-PW : Point-to-point Psuedowire
 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 targeted LDP application list over a tLDP session by using the Capability Advertisement as defined in [RFC5561] and encoded as follows:



This document defines a new optional capability TLV of type TBD1 called 'Targeted Application Capability (TAC)'. Flag "U" MUST be set to 1 to indicate that this capability must be silently ignored if unknown. The TAC's Capability Data contains the Targeted Application Element (TAE) information encoded as follows:

Targeted Application Element(TAE)

```

      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
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Targ. Appl. Id                   |E|   Reserved                   |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Targeted Application Identifier (TA-Id):

a 16 bit Targeted Application Identifier value.

E-bit: The 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, a LSR MAY include a new capability TLV, 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 a 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 the 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 TAE common between the TAC TLV it has received and its own, the session MUST proceed to establishment as per [RFC5036]. If not, A LSR MUST send a 'Session Rejected/Targeted Application Capability Mis-Match' Notification message to the peer and close the session. The

initiating LSR SHOULD tear down the corresponding tLDP adjacency after sent or receipt of a 'Session Rejected/Targeted Application Capability Mis-Match' Notification message to or from the responding LSR respectively.

If both the peers support TAC TLV, an LSR decides to establish or close a tLDP session based on the negotiated targeted application list. 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 the LSRs is C. 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 the applications - A, B, C, D and E - as TA-Ids that it supports over this session. Then the negotiated targeted applications as per both the LSRs are A, B and C. Finally, If the initiating LSR advertises A, B and C as a TA-Ids and the responding LSR advertises D and E as TA-Ids, then the negotiated targeted applications as per both the LSRs are none. Therefore, if the intersection of the sets of received and sent TA-Id is null, then LSR sends 'Session Rejected/Targeted Application Capability Mis-Match' 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 Mis-Match' Notification message, it MUST set its session setup retry interval to a maximum value, as such 0xffff. The session MAY stay in NON EXISTENT state. When it detects a change in the initiating LSR or local LSR configuration pertaining to TAC TLV, it MUST clear the session setup back off delay associated with the session to re-attempt the session establishment. A LSR detects configuration change on the other LSR with the receipt of 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 Mis-Match' Notification message, either it MUST close the session and tear down the corresponding tLDP adjacency or it MUST set its session setup retry interval to a maximum value, as such 0xffff.

If the initiating LSR decides to tear down the associated tLDP adjacency, the session is closed on the initiating 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 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 TAC TLV, it MUST clear the session setup back off delay associated with the session in order to re-attempt the session establishment.

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

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

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

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

In addition, LSR SHOULD allow the configuration of any TA-Id in order to facilitate private TA-Id's usage by a network operator.

2.3 LDP message procedures

2.3.1 Initialization message

1. The S-bit of the Targeted Application Capability TLV MUST be set to 1 to advertise Targeted Application Capability and SHOULD be ignored on the receipt as defined in [RFC5561]
2. The E-bit of the Targeted Application Element MUST be set to 1 to

enable Targeted application and SHOULD be ignored on the receipt.

3. An LSR MAY add State Control Capability by mapping Targeted Application Element to State Advertisement Control (SAC) Elements as defined in Section 4.

2.3.2 Capability message

The initiating or responding LSR may re-negotiate the TAC after local configuration change with the Capability message.

1. The S-bit of TAC is set to 1 or 0 to advertise or withdraw it.
2. After configuration change, If there is no common TAE between its new TAE list and peers TAE list, the LSR MUST send a 'Session Rejected/Targeted Application Capability Mis-Match' Notification message and close the session.
3. If there is a common TAE, a LSR MAY also update SAC Capability based on updated TAC as described in section 4 and send the updated TAC and SAC capabilities in a Capability message to the peer.
4. A receiving LSR processes the Capability message with 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, a LSR process a list of TAEs from TACs capability data with E-bit set to 1 or 0 to update the peer's TAE.

3. Targeted Application FEC Advertisement Procedures

The targeted LDP 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 control protocol | None |
| LDP P2MP PW | LDP P2MP Pseudowire | P2MP PW Upstream FEC Element |
| mLDP Node Protection | mLDP node protection | P2MP MP2MP-up MP2MP-down HSMP-downstream HSMP-upstream |
| IPv4 intra-area FECs | IPv4 intra-area FECs | IPv4 prefix |
| IPv6 intra-area FECs | IPv6 intra-area FECs | IPv6 prefix |

Intra-area FECs : FECs that are on the shortest path tree and not
leaves 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 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], State Advertisement Control(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 advertisement of state information between the two peers.

The TAC negotiation facilitates the awareness of targeted applications to both 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 to receive state information from the peer. Therefore, when the responding LSR is not aware of targeted applications such a remote LFA and BGP auto discovered pseudowires, TAC mechanism should be used and when the responding LSR is aware (with appropriate configuration) of targeted applications such as FEC 128 pseudowire, SAC mechanism should be used. Also after TAC mechanism makes the responding LSR aware of targeted application, 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, both TAC and SAC mechanisms can be used to control the FEC-label bindings that are advertised over the tLDP session. For instance, suppose the initiating LSR establishes a tLDP session to the responding LSR for Remote LFA and FEC 129 PW targeted applications with TAC. So each LSR advertises the corresponding FEC-Label bindings. Further, suppose the initiating LSR is not the PQ node for responding LSRs 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 targeted LDP application.

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 when 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 an un-negotiated application). This is true even if one of the peers announces its interest in receiving state information that corresponds to the un-negotiated application by sending a SAC TLV. In other words, when TAC is being used, SAC cannot and should not enable state information advertisement for applications that have not been enabled by TAC.

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 that 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 - FEC128 P2P-PW
- LDP FEC 129 PW - FEC129 P2P-PW

An LSR MUST map Targeted Application to 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 to remote LSR based on IGP calculation as described in [RFC7490] or some other mechanism, which is outside the scope of this document. The LSR

forms the tLDP adjacency and constructs an Initialization message with TAC TLV with TAE as 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 these conditions are met, the receiver LSR may respond back with an Initialization message with TAC corresponding to Remote LFA, and subsequently the session may be established.

After the session has been established with TAC capability, the sender and receiver LSR 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 targeted application element to state 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 a border LSR can accept. As described in Section 2, LDP may convey targeted applications with TAC TLV to 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 session from source-list.

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

5.3 LDP over RSVP and Remote LFA targeted session

A LSR may want to establish a tLDP session to a remote LSR for LDP over RSVP tunneling and Remote LFA applications. The sender LSR may add both these applications as a unique Targeted Application Element in the Targeted Application Capability 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 and Remote LFA applications as both need same FECs - IPv4 or IPv6 or both.

5.4 mLDP node protection targeted session

A merge point LSR may determine that it needs to form automatic tLDP session to the upstream point of local repair (PLR) LSR for MP2P and MP2MP LSP [RFC6388] node protection as described in the [RFC7715]. The MPT LSR may add a new targeted LDP application - mLDP protection - as a unique TAE in the Targeted Application Capability 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 Capability procedure described in this document does not introduce any change to LDP Security Considerations section 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, a LSR can employ a policy to accept all auto-discovered Extended Hellos from the configured source addresses list.

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

7. IANA Considerations

This document requires the assignment of a new code point for a Capability Parameter TLVs from the IANA managed LDP registry "TLV Type Name Space", corresponding to the advertisement of the Targeted Applications capability. IANA is requested to assign the lowest available value after 0x050B.

| Value | Description | Reference |
|-------|----------------------------------|-----------------|
| ----- | ----- | ----- |
| TBD1 | Targeted Applications capability | [this document] |

This document requires the assignment of a new code point for a status code from the IANA managed registry "STATUS CODE NAME SPACE" on the Label Distribution Protocol (LDP) Parameters page, corresponding to the notification of session Rejected/Targeted

Application Capability Mis-Match. IANA is requested to assign the lowest available value after 0x0000004B.

| Value | E | Description | Reference |
|-------|---|---|-----------------|
| TBD2 | 1 | Session Rejected/Targeted Application Capability Mis-Match | [this document] |

This document also creates a new name space 'the LDP Targeted Application Identifier' on the Label Distribution Protocol (LDP) Parameters page, that is to be managed by IANA. The range is 0x0001-0xFFFFE, with the following values requested in this document.

| Value | Description | Reference |
|------------------|--|-----------------|
| 0x0000 | Reserved | [this document] |
| 0x0001 | LDPv4 Tunneling | [this document] |
| 0x0002 | LDPv6 Tunneling | [this document] |
| 0x0003 | mLDP Tunneling | [this document] |
| 0x0004 | LDPv4 Remote LFA | [this document] |
| 0x0005 | LDPv6 Remote LFA | [this document] |
| 0x0006 | LDP FEC 128 PW | [this document] |
| 0x0007 | LDP FEC 129 PW | [this document] |
| 0x0008 | LDP Session Protection | [this document] |
| 0x0009 | LDP ICCP | [this document] |
| 0x000A | LDP P2MP PW | [this document] |
| 0x000B | mLDP Node Protection | [this document] |
| 0x000C | LDPv4 Intra-area FECs | [this document] |
| 0x000D | LDPv6 Intra-area FECs | [this document] |
| 0x0001 - 0x1FFF | Available for assignment by IETF Review | |
| 0x2000 - 0F7FF | Available for assignment as first come first served | |
| 0xF800 - 0xFBFF | Available for private use | |
| 0xFC00 - 0xFFFFE | Available for experimental use | |
| 0xFFFF | Reserved | [this document] |

8. Acknowledgments

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

9. Contributing Authors

Chris Bowers
Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
USA
EMail: cbowers@juniper.net

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

10. References

10.1 Normative References

- [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>>.
- [RFC7473] Kamran Raza, Sami Boutros, "Controlling State Advertisements of Non-negotiated LDP Applications", RFC 7473, March 2015, <<http://www.rfc-editor.org/info/rfc7473>>.
- [RFC7715] IJ. Wijnands, E. Rosen, K. Raza, J. Tantsura, A. Atlas, Q. Zhao, "mLDP Node Protection", RFC 7715, January 2016, <<http://www.rfc-editor.org/info/rfc7715>>.
- [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>>.
- [RFC8174] B. Leiba, "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC8174, May 2017, <<http://www.rfc-editor.org/info/rfc8174>>.

10.2 Informative References

- [RFC7490] S. Bryant, C. Filsfils, S. Previdi, M. Shand, N. So,

"Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)",
April 2015.

[RFC6074] E. Rosen, B. Davie, V. Radoaca, and W. Luo, "Provisioning,
Auto-Discovery, and Signaling in Layer 2 Virtual Private
Networks (L2VPNs)", January 2011.

[RFC6388] IJ. Wijnands, I. Minei, K. Kompella, B. Thomas, "Label
Distribution Protocol Extensions for Point-to-Multipoint
and Multipoint-to-Multipoint Label Switched Paths",
November 2011.

Authors' Addresses

Santosh Esale
Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089
USA
EMail: sesale@juniper.net

Raveendra Torvi
Juniper Networks
10 Technology Park Drive
Westford, MA 01886
USA
EMail: rtorvi@juniper.net

Luay Jalil
Verizon
1201 E Arapaho Rd
Richardson, TX 75081
USA
Email: luay.jalil@verizon.com

Uma Chunduri
Huawei
2330 Central Expy
Santa Clara, CA 95050
USA
Email: uma.chunduri@huawei.com

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

