MPLS Working Group
INTERNET-DRAFT
Intended Status: Proposed Standard
Expires: October 4, 2014

Santosh Esale
Raveendra Torvi
Chris Bowers
Juniper Networks

April 2, 2014

Applications aware LDP Targeted Session
draft-esale-mpls-appl-aware-ldp-targeted-session-00

Abstract

Recent Targeted LDP applications such as Remote LFA and BGP auto discovery FEC 129 pseudowire may automatically establish a targeted LDP session to any LSR in the core network. The sender LSR has information about the targeted applications to administratively control initiation of the session. However the receiver LSR has no such information to control the acceptance of this session. This document defines a mechanism to advertise Targeted Application Capability during session initialization. As the receiver LSR becomes aware of targeted LDP applications, it may establish a limited number of sessions for certain applications. In addition, each targeted application is mapped to LDP FEC Elements to advertise only necessary 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/1id-abstracts.html

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

Table of Contents

1 Introduction

LDP can use the extended discovery mechanism to establish a targeted adjacency and subsequent session as described in [RFC5036]. An LSR initiates extended discovery by sending the targeted Hello to a specific address. The remote LSR decides either to accept or ignore the Hello based on local configuration only. For an application such as FEC 128 pseudowire and LDP over RSVP tunneling, the remote LSR is configured with the source LSR address, so the remote LSR can use that information to accept or ignore any given LDP Hello.

Applications such as remote LFA and FEC 129 pseudowire automatically initiate asymmetric extended discovery to any LSR in the network based on local state. In these applications, the remote LSR is not explicitly configured with the source LSR address, so the remote LSR either responds to all LDP requests or ignores all LDP requests.

In addition, since the session is initiated and established after adjacency formation, the receiver LSR has no targeted application information to choose the targeted applications it would like to support. While the sender LSR may employ a limit per application on locally initiated automatic targeted sessions, the receiver LSR currently has no mechanism to apply a similar limit on the incoming targeted sessions. Also, the receiver LSR does not know whether the source LSR is establishing the session for a configured or an automatic application.

This document proposes and describes a solution to advertise targeted application capability, consisting of a targeted application list, during initialization of a targeted session. It also defines a mechanism to enable a new application and disable an old application after session establishment. This capability advertisement provides the remote LSR with the necessary information to control the targeted sessions per application. For instance, an LSR may wish to accept all FEC 129 targeted sessions but may only accept limited number of Remote LFA targeted sessions.

Also, targeted applications may be mapped to LDP FEC type to advertise specific application FECs only, avoiding the advertisement of unnecessary FECs over the session.

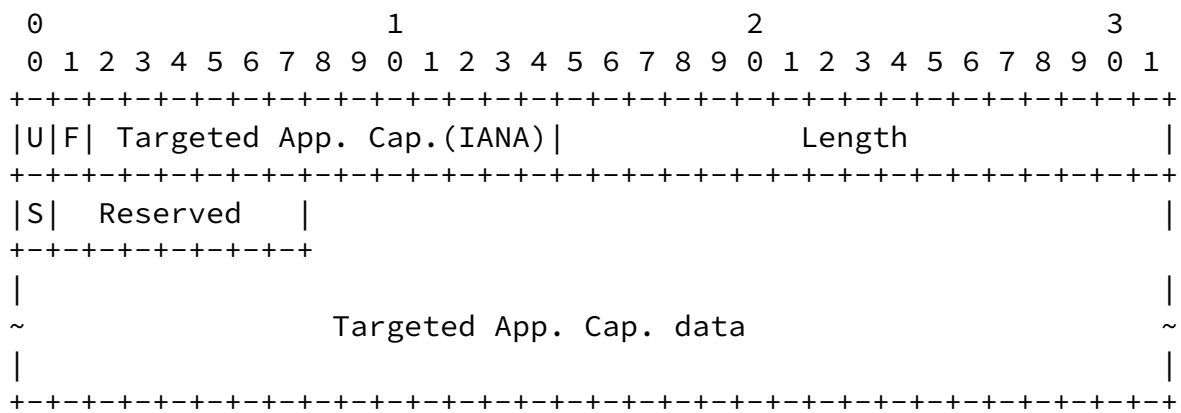
1.1 Terminology

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].

2. Targeted Application Capability

An LSR MAY advertise that it is capable of negotiating a targeted application list over a session by using the Capability Advertisement as defined in [RFC5561].

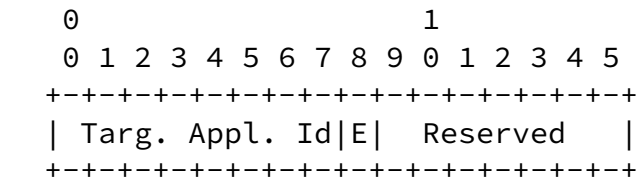
A new optional capability TLV is defined, 'Targeted Application Capability (TAC)'. Its encoding is as follows:



U: set to 1. Ignore, if not known.
F: Set to 0. Do not forward.
S: MUST be set to 1 and ignored on receipt.

Targeted Application Capability data:
A Targeted Applications Capability data consists of none, one or more Targeted Application Elements. Its encoding is as follows:

Targeted Application Element(TAE)



Targeted Application Identifier (TA-Id):

0x0001: LDPv4 Tunneling
0x0002: LDPv6 Tunneling
0x0003: mLDP Tunneling
0x0004: LDPv4 Remote LFA
0x0005: LDPv6 Remote LFA
0x0006: FEC 128 Pseudowire
0x0007: FEC 129 Pseudowire

E-bit: It indicates whether the sender is advertising or withdrawing the Targeted Application. The E-bit value is used as follows:

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

The length of TAC depends on the number of TAE elements. For instance, if two TAE elements are added, the length is set to 5.

If both the peers advertise TAC, an LSR decides to establish or close a targeted session based on the negotiated targeted application element list.

3. Targeted Application Capability Procedures

At targeted session establishment time, an LSR MAY include a new capability TLV, Targeted Application Capability (TAC) TLV, as an optional TLV in the LDP Initialization message. The TAC TLV's Capability data MUST consists of none, one or more Targeted

Application Element(TAE) each pertaining to a unique Targeted Application Identifier(TA-Id). If the receiver LSR receives the same TA-Id in more than one TAE element, it MUST discard the TAC TLV and behave as if TAC TLV is not received. If the receiver LSR receives an unknown TA-Id in a TAE element, it SHOULD silently ignore such a TAE element and continue processing the rest of the TLV.

If the receiver LSR does not receive the TAC in the Initialization message or it does not understand the TAC TLV, the TAC negotiation MUST be considered unsuccessful and the session establishment MUST proceed as per [RFC5036]. On the receipt of a valid TAC TLV, an LSR MUST generate its own TAC TLV with TAE elements consisting of unique TA-Ids that it MAY support over the targeted session. If there is at least one TAE element 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 sender LSR playing the passive role in LDP session establishment MAY destroy the corresponding targeted adjacency.

When the receiver LSR playing the active role 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 0xffff. The session MAY stay in non-operational state. When it detects a change in the sender LSR configuration or local configuration pertaining to TAC TLV, it

MUST clear the session setup back off delay associated with the session to re-attempt the session establishment.

When the sender LSR playing the active role in LDP session establishment receives a 'Session Rejected/Targeted Application Capability Mis-Match' Notification message, either it MUST set its session setup retry interval to a maximum value, as 0xffff or it MUST destroy the corresponding targeted adjacency with the session. This leads to destruction of the session.

If it sets the session setup retry interval to maximum, the session MAY stay in a non-operational state. When this LSR detects a change in the receiver LSR configuration or its own configuration pertaining to TAC TLV, it MUST clear the session setup back off delay associated with the session to re-attempt the session establishment.

If it decides to destroy the associated targeted adjacency, the session is destroyed on the sender as well as the receiver LSR. The sender LSR MAY take appropriate actions if it is unable to bring up the targeted session. For instance, if an automatic session intended to support the Remote LFA application is rejected by the receiver LSR, the sender LSR MAY inform the IGPs to calculate another PQ node for the route or set of routes. More specific actions are a local matter and outside the scope of this document.

After an LDP session has been established with TAC capability, the sender and receiver LSR MUST distribute FEC label bindings for the negotiated applications only. For instance, if the LDP session is established for FEC 129 pseudowire, only FEC 129 label bindings MUST be distributed over the session. Similarly, a LSR MUST request FEC label bindings for the negotiated applications only.

If the Targeted Application Capability and Dynamic Capability, as defined in RFC5561, are negotiated during session Initialization, TAC MAY be re-negotiated after session establishment by sending the updated TAC TLV in LDP Capability message. The Updated TLV MUST consist of one or more TAE elements 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 FEC types over the session or destruction of the adjacency and subsequently the session.

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

As described in this document, the set of Targeted Application Elements 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 [I-D.draft-ietf-mpls-ldp-ip-pw-capability], 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 for any particular application.

For a given LDP 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 LDP session. The TAC mechanism takes precedence over the SAC mechanism with respect to enabling applications for which state information will be advertised. For an LDP 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 Targeted Application Elements 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 enable state information advertisement for applications that have not been enabled by TAC.

On the other hand, the SAC mechanism takes 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 [I-D.draft-ietf-mpls-ldp-ip-pw-capability] an LSR MAY using the following mappings:

```
LDPv4 Tunneling - IPv4 Label switching
LDPv6 Tunneling - IPv6 Label switching
LDPv4 Remote LFA - IPv4 Label switching
LDPv6 Remote LFA - IPv6 Label switching
FEC 128 Pseudowire - P2P PW FEC128 signaling
FEC 129 Pseudowire - P2P PW FEC129 signaling
```


An LSR MAY map Targeted Application to LDP capability as follows:

mLDP Tunneling - P2MP Capability, MP2MP Capability

5. Targeted Application capability in LDP messages

5.1 TAC in LDP Initialization message

1. The S-bit of the Targeted Application Capability parameter MUST be set to 1 to advertise Targeted Application Capability and SHOULD be ignored on the receipt. The E-bit of the Targeted Application Element MUST be set to 1 to enable Targeted application.

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

3. The LSR MAY add a different Hold time value for an automatic targeted session.

5.2 TAC in LDP Capability message

1. The S-bit of Targeted Application Capability is set to 1 and ignored on receipt.

2. If there is no common Targeted Application element between its new TAC and peers TAC, the LSR MUST send a 'Session Rejected/Targeted Application Capability Mis-Match 'Notification message and close the session.

3. If there is a common Targeted Application Element, a LSR MAY also update State Advertisement Control Capability as per Section 4 and send these capabilities in a Capability message to the peer.

4. A receiving LSR processes the Capability message and its Targeted Applications Capability TLV. The S-bit is ignored on receipt.

5. Process a List of Targeted Application Elements from capability data with E-bit set to 1 to construct peers Targeted Application Capability.

7. Use cases

7.1 Remote LFA Automatic Targeted session

An LSR determines that it needs to form a automatic targeted session

to remote PQ node based on IGP calculation as described in [I-D.draft-ietf-rtgwg-remote-lfa] or some other mechanism, which is outside the scope of this document. The LSR forms the targeted adjacency and during session setup, constructs an Initialization message with Targeted Applications Capability (TAC) with Targeted Application Element (TAE) as Remote LFA. The receiver LSR processes the LDP Initialization message and verifies whether it is configured to accept a Remote LFA targeted 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.

7.2 FEC 129 Auto Discovery Targeted session

BGP auto discovery or other mechanisms outside the scope of this document MAY determine whether an LSR needs to initiate an auto-discovery targeted session with a border LSR. Multiple LSRs MAY try to form an auto-discovery LDP targeted session with a border LSR. So a service provider may want to limit the number of auto-discovery targeted sessions a border LSR MAY accept. As described in Section 3, LDP MAY convey Targeted Applications with TAC TLV to border LSR. A border LSR may establish or reject the session based on local administrative policy. Also, as the receiver LSR would be aware of targeted application, it can also employ an administrative policy for security. For instance, it can employ a policy 'accept all auto-discovered session from source-list'.

Moreover, the sender and receiver LSR MUST exchange FEC 129 application states only over the targeted session, i.e. FEC 129 label bindings only.

7.3 LDP over RSVP and Remote LFA targeted session

A LSR may want to establish a targeted session to a remote LSR for LDP over RSVP tunneling and Remote LFA. 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 automatic targeted sessions for Remote LFA, but it may also be configured to accept LDP

over RSVP tunneling. In this case, the targeted session is formed for both LDP over RSVP and Remote LFA applications as both needs same FECs - IPv4 and/or IPv6.

Also, the sender and the receiver LSR MUST distributes IPv4 and or IPv6 FEC label bindings only over the session.

8 Security Considerations

The Capability procedure described in this document will apply and does not introduce any change to LDP Security Considerations section described in [RFC5036].

9 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 draft]

This document requires the assignment of a new code point for a status code from the IANA managed registry "STATUS CODE NAME SPACE", corresponding to the notification of session Rejected/Targeted Application Capability Mis-Match. IANA is requested to assign the lowest available value after 0x0000004B.

Value	Description	Reference
TBD2	Session Rejected/Targeted Application Capability Mis-Match	[This draft]

This document also creates a new name space 'the LDP Targeted

Application Element type' that is to be managed by IANA. The range is 0-65535, with the following values requested in this document.

0x0000: Reserved
0x0001: LDPv4 Tunneling
0x0002: LDPv6 Tunneling
0x0003: mLDP Tunneling
0x0004: LDPv4 Remote LFA
0x0005: LDPv6 Remote LFA

0x0006: FEC 128 Pseudowire
0x0007: FEC 129 Pseudowire

The allocation policy for this space is 'Standards Action with Early Allocation'.

10. Acknowledgments

The authors wish to thank Nischal Sheth, Hassan Hosseini and Kishore Tiruveedhula for doing the detailed review. Thanks to Manish Gupta and Martin Ehlers for their input to this work and for many helpful suggestions.

11 References

11.1 Normative References

[RFC5036] Andersson, L., Ed., Minei, I., Ed., and B. Thomas, Ed., "LDP Specification", RFC 5036, October 2007.

[RFC5561] Thomas, B., Raza, K., Aggarwal, S., Aggarwal, R., and JL. Le Roux, "LDP Capabilities", RFC 5561, July 2009.

[I-D.draft-ietf-mpls-ldp-ip-pw-capability] Kamran Raza, Sami Boutros, "Disabling IPoMPLS and P2P PW LDP Application's State Advertisement", draft-ietf-mpls-ldp-ip-pw-capability-06 (work in progress), December 19, 2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997..

11.2 Informative References

[I-D.draft-ietf-rtgwg-remote-lfa] S. Bryant, C. Filsfils, S. Previdi,M. Shand, "Remote LFA FRR", draft-ietf-rtgwg-remote-lfa-04 (work in progress), November 22, 2013.

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

[RFC4762] M. Lasserre, and V. Kompella, "Virtual Private LAN Service VPLS) Using Label Distribution Protocol (LDP) Signaling", RFC 4762, January 2007.

[RFC4447] L. Martini, E. Rosen, El-Aawar, T. Smith, and G. Heron,

"Pseudowire Setup and Maintenance using the Label Distribution Protocol", RFC 4447, April 2006.

[RFC5331] Aggarwal, R., Rekhter, Y., and E. Rosen, "MPLS Upstream Label Assignment and Context-Specific Label Space", RFC 5331, August 2008.

Authors' Addresses

Santosh Esale
Juniper Networks
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
US
EMail: sesale@juniper.net

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

Chris Bowers
Juniper Networks
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
US
EMail: cbowers@juniper.net