Ability for a stateful PCE to request and obtain control of a LSP
draft-raghu-pce-lsp-control-request-03

Abstract

   The stateful Path Computation Element (PCE) communication Protocol
   (PCEP) extensions provide stateful control of Multiprotocol Label
   Switching (MPLS) Traffic Engineering Label Switched Paths (TE LSP)
   via PCEP, for a model where a Path Computation Client (PCC) delegates
   control over one or more locally configured LSPs to a stateful PCE.
   There are use-cases in which a stateful PCE may wish to request and
   obtain control of one or more LSPs from a PCC. This document
   describes a simple extension to stateful PCEP to achieve such an
   objective.

Requirements Language

   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 [RFC2119].

Status of This Memo

This Internet-Draft will expire on December 31, 2017.

Table of Contents

1. Introduction

Stateful PCEP extensions [I-D.ietf-pce-stateful-pce] specifies a set
of extensions to PCEP [RFC5440] to enable stateful control of TE LSPs
between and across PCEP sessions in compliance with [RFC4657]. It
includes mechanisms to effect LSP state synchronization between PCCs
and PCEs, delegation of control of LSPs to PCEs, and PCE control of
timing and sequence of path computations within and across PCEP

sessions. The stateful PCEP defines the following two useful network
operations:

o Delegation: As per [RFC8051], an operation to grant a PCE
   temporary rights to modify a subset of LSP parameters on one or
   more LSPs of a PCC. LSPs are delegated from a PCC to a PCE and
   are referred to as "delegated" LSPs.

o Revocation: As per [I-D.ietf-pce-stateful-pce], an operation
   performed by a PCC on a previously delegated LSP. Revocation
   revokes the rights granted to the PCE in the delegation operation.

For Redundant Stateful PCEs (section 5.7.4. of
[I-D.ietf-pce-stateful-pce]), during a PCE failure, one of the
redundant PCE could request to take control over an LSP. The
redundant PCEs MAY use a local policy or a proprietary election
mechanism to decide which PCE would take control. In this case, a
mechanism is needed for a stateful PCE to request control of one or
more LSPs from a PCC, so that a newly elected primary PCE can request
to take over control.

In case of virtualized PCEs (vPCE) running as virtual network
function (VNF), as the computation load in the network increases, a
new instance of vPCE could be instantiated to balance the current
load. The PCEs could use proprietary algorithm to decide which LSPs
to be assigned to the new vPCE. Thus having a mechanism for the PCE
to request control of some LSPs is needed.

In some deployments, the operator would like to use stateful PCE for
global optimization algorithms but would still like to keep the
control of the LSP at the PCC. In such cases, a stateful PCE could
request to take control during the global optimization and return the
delegation once done.

This specification provides a simple extension, by using this a PCE
can request control of one or more LSPs from any PCC over the
stateful PCEP channel. The procedures for granting and relinquishing
control of the LSPs are specified in accordance with the
specification [I-D.ietf-pce-stateful-pce].

2. Terminology

The following terminologies are used in this document:

PCC: Path Computation Client.

PCE: Path Computation Element

   PCEP: Path Computation Element communication Protocol.

   PCRpt: Path Computation State Report message.

   PCUpd: Path Computation Update Request message.

   PLSP-ID: A PCEP-specific identifier for the LSP.

3. LSP Control Request Flag

   The SRP object is defined in [I-D.ietf-pce-stateful-pce] and
   included here for ease of reference. [Editor's Note - The figure
   would be removed at the time of publication.]

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                            Flags                          |C|R|
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         SRP-ID-number                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   //                        Optional TLVs                        //
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
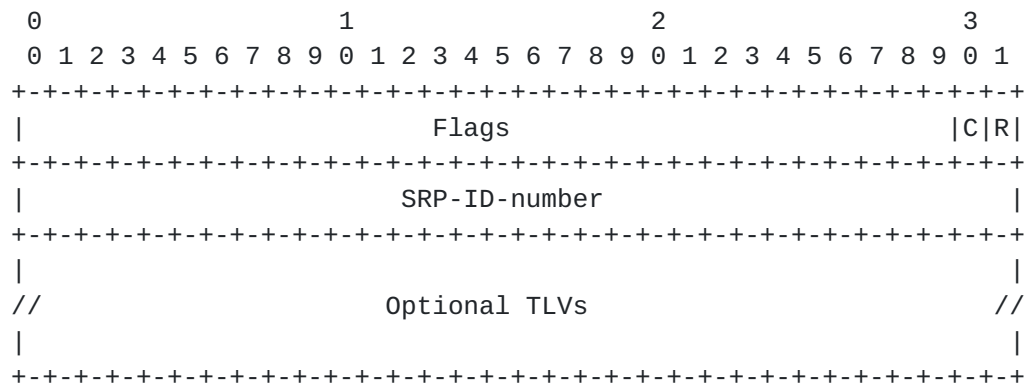
                        Figure 1: The SRP Object

   A new flag, the "LSP Control Request Flag" (C), is introduced in the
   Stateful PCE Request Parameters (SRP) object. On a PCUpd message, a
   PCE sets the C Flag to 1 to indicate that, it wishes to gain control
   of LSP(s). The LSP is identified by the LSP object. A PLSP-ID of
   value other than 0 and 0xFFFFF is used to identify the LSP for which
   the PCE requests control. The PLSP-ID value of 0 indicates that the
   PCE is requesting control of all LSPs originating from the PCC that
   it wishes to delegate. The flag has no meaning in the PCRpt and
   PCInitiate message and SHOULD be set to 0 on transmission and MUST be
   ignored on receipt.

4. Operation

   During normal operation, a PCC that wishes to delegate the control of
   an LSP sets the D Flag to 1 in all PCRpt messages pertaining to the
   LSP. The PCE confirms the delegation by setting D Flag to 1 in all
   PCUpd messages pertaining to the LSP. The PCC revokes the control of
   the LSP from the PCE by setting D Flag to 0 in PCRpt messages
   pertaining to the LSP. If the PCE wishes to relinquish the control

of the LSP, it sets D Flag to 0 in all PCUpd messages pertaining to
the LSP.

If a PCE wishes to gain control over an LSP, it sends a PCUpd message
with C Flag set to 1 in SRP object. The LSP for which the PCE
requests control is identified by the PLSP-ID. The PLSP-ID of 0
indicates that the PCE wants control over all LSPs originating from
the PCC. If the LSP(s) is/are already delegated to the PCE making
the request, the PCC ignores the C Flag. A PCC can decide to
delegate the control of the LSP at its own discretion. If the PCC
grants or denies the control, it sends PCRpt message with D Flag set
to 1 and 0 respectively in accordance with according with stateful
PCEP [I-D.ietf-pce-stateful-pce] . If the PCC does not grant the
control, it MAY choose to not respond, and the PCE may choose to
retry requesting the control preferably using exponentially
increasing timer. A PCE ignores the C Flag on the PCRpt message.

In case multiple PCEs request control over an LSP, and if the PCC is
willing to grant the control, the LSP MUST be delegated to only one
PCE chosen by the PCC based on its local policy.

It should be noted that a legacy implementation of PCC, that does not
understand the C flag in PCUpd message, would simply ignore the flag
and the request to grant control over the LSP.

[I-D.ietf-pce-pce-initiated-lsp] describes the setup, maintenance and
teardown of PCE-initiated LSPs under the stateful PCE model. It also
specify how a PCE MAY obtain control over an orphaned LSP that was
PCE-initiated. A PCE implementation can apply the mechanism
described in this document in conjunction with those in
[I-D.ietf-pce-pce-initiated-lsp].

5. Security Considerations

The security considerations listed in [I-D.ietf-pce-stateful-pce]
apply to this document as well. However, this document also
introduces a new attack vectors. An attacker may flood the PCC with
request to delegate all its LSPs at a rate which exceeds the PCC's
ability to process them, either by spoofing messages or by
compromising the PCE itself. The PCC can simply ignore these
messages with no extra actions. Securing the PCEP session using
mechanism like Transport Layer Security (TLS) [I-D.ietf-pce-pceps] is
RECOMMENDED.

6. IANA Considerations

This document requests IANA actions to allocate code points for the protocol elements defined in this document.

6.1. SRP Object Flags

The SRP object is defined in [I-D.ietf-pce-stateful-pce] and the registry to manage the Flag field of the SRP object is requested in [I-D.ietf-pce-pce-initiated-lsp]. IANA is requested to make the following allocation in the aforementioned registry.

Bit	Description	Reference
TBD (suggested value 30)	LSP Control Request Flag (c-bit)	This document

7. Manageability Considerations

All manageability requirements and considerations listed in [RFC5440] and [I-D.ietf-pce-stateful-pce] apply to PCEP protocol extensions defined in this document. In addition, requirements and considerations listed in this section apply.

7.1. Control of Function and Policy

A PCE or PCC implementation SHOULD allow the operator to configure the policy based on which it honor the request to control the LSPs. Further, the operator MAY be to be allowed to trigger the LSP control request at the PCE.

7.2. Information and Data Models

The PCEP YANG module [I-D.ietf-pce-pcep-yang] could be extended to include mechanism to trigger the LSP control request.

7.3. Liveness Detection and Monitoring

Mechanisms defined in this document do not imply any new liveness detection and monitoring requirements in addition to those already listed in [RFC5440].

7.4. Verify Correct Operations

Mechanisms defined in this document do not imply any new operation verification requirements in addition to those already listed in [RFC5440] and [I-D.ietf-pce-stateful-pce].

7.5. Requirements On Other Protocols

   Mechanisms defined in this document do not imply any new requirements
   on other protocols.

7.6. Impact On Network Operations

   Mechanisms defined in [RFC5440] and [I-D.ietf-pce-stateful-pce] also
   apply to PCEP extensions defined in this document. Further, the
   mechanism described in this document can help the operator to request
   control of the LSPs at a particular PCE.

8. Acknowledgements

   TBD.

9. References

9.1. Normative References

   [I-D.ietf-pce-stateful-pce]
              Crabbe, E., Minei, I., Medved, J., and R. Varga, "PCEP
              Extensions for Stateful PCE", draft-ietf-pce-stateful-
              pce-21 (work in progress), June 2017.

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

   [RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation
              Element (PCE) Communication Protocol (PCEP)", RFC 5440,
              DOI 10.17487/RFC5440, March 2009,
              <http://www.rfc-editor.org/info/rfc5440>.

9.2. Informative References

   [I-D.ietf-pce-pce-initiated-lsp]
              Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "PCEP
              Extensions for PCE-initiated LSP Setup in a Stateful PCE
              Model", draft-ietf-pce-pce-initiated-lsp-10 (work in
              progress), June 2017.

   [I-D.ietf-pce-pcep-yang]
              Dhody, D., Hardwick, J., Beeram, V., and j.
              jefftant@gmail.com, "A YANG Data Model for Path
              Computation Element Communications Protocol (PCEP)",
              draft-ietf-pce-pcep-yang-03 (work in progress), June 2017.

   [I-D.ietf-pce-pceps]
              Lopez, D., Dios, O., Wu, Q., and D. Dhody, "Secure
              Transport for PCEP", draft-ietf-pce-pceps-14 (work in
              progress), May 2017.

   [RFC4657] Ash, J., Ed. and J. Le Roux, Ed., "Path Computation
              Element (PCE) Communication Protocol Generic
              Requirements", RFC 4657, DOI 10.17487/RFC4657, September
              2006, <http://www.rfc-editor.org/info/rfc4657>.

   [RFC8051] Zhang, X., Ed. and I. Minei, Ed., "Applicability of a
              Stateful Path Computation Element (PCE)", RFC 8051,
              DOI 10.17487/RFC8051, January 2017,
              <http://www.rfc-editor.org/info/rfc8051>.

Authors' Addresses

   Aswatnarayan Raghuram
   AT&T
   200 S Laurel Aevenue
   Middletown, NJ 07748
   USA

   Email: ar2521@att.com

   Al Goddard
   AT&T
   200 S Laurel Aevenue
   Middletown, NJ 07748
   USA

   Email: ag6941@att.com

   Chaitanya Yadlapalli
   AT&T
   200 S Laurel Aevenue
   Middletown, NJ 07748
   USA

   Email: cy098d@att.com

   Jay Karthik
   Cisco Systems, Inc.
   125 High Street
   Boston, Massachusetts 02110
   USA

   Email: jakarthi@cisco.com

   Siva Sivabalan
   Cisco Systems, Inc.
   2000 Innovation Drive
   Kanata, Ontario K2K 3E8
   Canada

   Email: msiva@cisco.com

   Jon Parker
   Cisco Systems, Inc.
   2000 Innovation Drive
   Kanata, Ontario K2K 3E8
   Canada

   Email: jdparker@cisco.com

   Dhruv Dhody
   Huawei Technologies
   Divyashree Techno Park, Whitefield
   Bangalore, Karnataka 560066
   India

   Email: dhruv.ietf@gmail.com