Workgroup: PCE Working Group
Internet-Draft:
draft-wang-pce-vlan-based-traffic-
forwarding-07
Published: 11 January 2023
Intended Status: Standards Track
Expires: 15 July 2023
Authors: Y. Wang (China Telecom)
A. Wang (China Telecom)
B. Khasanov (Yandex LLC)
F. Qin (China Mobile)
H. Chen (Futurewei)
C. Zhu (ZTE Corporation)

PCEP Procedures and Extension for VLAN-based Traffic Forwarding

Abstract

This document defines the Path Computation Element Communication Protocol (PCEP) extension for VLAN-based traffic forwarding in native IP network and describes the essential elements and key processes of the data packet forwarding system based on VLAN info to accomplish the End to End (E2E) traffic assurance for VLAN-based traffic forwarding in native IP network.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 15 July 2023.

Table of Contents

1. Introduction

[RFC8283] introduces the extension to the architecture described in [RFC4655] where PCE acts as a central controller and gets more responsibility for LSP provisioning on each hop. Based on such mechanism, the PCE can calculate the optimal path for various applications and send the instructions to the network equipment via PCEP protocol, thus control the packet forwarding and achieve the QoS assurance for prioritized traffic. .

[RFC8735] describes the scenarios of QoS assurance for hybrid cloud-based application within one domain and traffic engineering in multi-domains. It proposes also the following requirements for the potential solution:

1. Should be applied both in native IPv4 and IPv6 environment.

2. Should be same procedures for the intra-domain and inter-domain scenario.

3. Should utilize the existing forwarding capabilities of the deployed network devices.

Due to large scale of Ethernet interfaces used in operators network and need to establish P2P connectivity for them, an operator should currently use either VPWS or EVPN with MPLS signaling. This is not suitable for Native IP scenarios. Thus PCECC architecture can solve that problem for Native IP networks by building the end-to-end dedicated path based on a VLAN header to control the forwarding behavior of a packet. Similar with the PCECC for LSP [RFC9050], this document defines a Path Computation Element Communication Protocol (PCEP) Extension for VLAN-based traffic forwarding by using the VLAN info contained in the Ethernet frame in native IP network and the mechanism is actually the PCECC for VSP(VLAN Switching Path). It is an end to end traffic guarantee mechanism based on the PCEP protocol in the native IP environment, which can ensure the connection-oriented network communication. The overall QoS assurance effect is achieved via the central controller by calculating and deploying the optimal VSP to bypass the congested nodes and links, thus avoids the resource reservation on each nodes in advance.

Compared with other traffic assurance technologies such as MPLS or SRv6 which is supported only in IPv6 environment and has the obvious packet overhead problems, the VLAN-based traffic forwarding (VTF) mechanism uses a completely new address space which will not conflict with other existing protocols and can easily avoid these problems and be deployed in IPv4 and IPv6 environment simultaneously. It is suitable for IPv4 and IPv6 networks and can leverage the existing PCE technologies as much as possible.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] .

3. Terminology

The following terms are defined in this draft:

*PCC: Path Computation Client

*PCE: Path Computation Element

*PCEP: PCE Communication Protocol

*PCECC: PCE-based Central Controller

*LSP: Lable Switching Path

*PST: Path Setup Type

4. Capability Advertisement

During the PCEP Initialization Phase, PCEP Speakers (PCE or PCC) advertise their support of VLAN-based traffic forwarding extensions. This document defines a new Path Setup Type (PST)[RFC8408] for PCECC, as follows:

*PST=TBD1: Path is a VLAN-based traffic forwarding type.

A PCEP speaker MUST indicate its support of the function described in this document by sending a PATH-SETUP-TYPE-CAPABILITY TLV in the OPEN object with this new PST included in the PST list.

Because the path is set up through PCE, a PCEP speaker must advertise the PCECC capability by using PCECC-CAPABILITY sub-TLV which is used to exchange information about their PCECC capability as per PCEP extensions defined in [RFC9050]

A new flag is defined in PCECC-CAPABILITY sub-TLV for VLAN-based traffic forwarding.

V (VLAN-based-forwarding-CAPABILITY - 1 bit - TBD2): If set to 1 by a PCEP speaker, it indicates that the PCEP speaker supports the capability of VLAN based traffic forwarding as specified in this document. The flag MUST be set by both the PCC and PCE in order to support this extension.

If a PCEP speaker receives the PATH-SETUP-TYPE-CAPABILITY TLV with the newly defined path setup type, but without the V bit set in PCECC-CAPABILITY sub-TLV, it MUST:

*Send a PCErr message with Error-Type=10(Reception of an invalid object) and Error-Value TBD3(PCECC VLAN-based-forwarding-CAPABILITY bit is not set).

*Terminate the PCEP session

5. PCEP message

As per [RFC8281] ,the PCInitiate message sent by a PCE was defined to trigger LSP instantiation or deletion with the SRP and LSP object included during the PCEP initialization phase. The Path Computation LSP State Report message (PCRpt message) was defined in [RFC8231], which is used to report the current state of a LSP. A PCC can send a

LSP State Report message in response to a LSP instantiation. Besides, the message can either in response to a LSP Update Request from a PCE or asynchronously when the state of a LSP changes .

[RFC9050] defines an object called Central Controller Instructions (CCI) to specify the forwarding instructions to the PCC. During the coding process used for central controller instructions, the CCI object contains the label information and is carried within PCInitiate or PCRpt message.

This document specify two new CCI object-types for VLAN-based traffic forwarding in the Native IP network and are said to be mandatory in a PCEP message when the object must be included and are considered to be valid. In addition, this document extends the PCEP message to handle the VLAN-based traffic forwarding path in the native IP network with the new CCI object.

5.1. The PCInitiate message

The PCInitiate message[RFC8281] extended in[RFC9050] can be used to download or remove labels by using the CCI Object.

Based on the extended PCInitiate message and PCRpt described in [I-D.ietf-pce-pcep-extension-native-ip], the (BGP Peer Info (BPI) Object and the Peer Prefix Association (PPA) Object are used to establish multi BGP sessions and advertise route prefixes among different BGP sessions before setting up a VLAN-based traffic forwarding path.

This document extends the PCInitiate message as shown below:

```
<PCInitiate Message> ::= <Common Header>
                              <PCE-initiated-lsp-list>
   Where:
      <Common Header> is defined in [RFC5440]

      <PCE-initiated-lsp-list> ::= <PCE-initiated-lsp-request>
                                   [<PCE-initiated-lsp-list>]

      <PCE-initiated-lsp-request> ::=
                           (<PCE-initiated-lsp-instantiation>|
                            <PCE-initiated-lsp-deletion>|
                            <PCE-initiated-lsp-central-control>)

      <PCE-initiated-lsp-central-control> ::= <SRP>
                                              <LSP>
                                              <cci-list>|
                                              ((<BPI>|<PPA>)
                                              <new-CCI>)

      <cci-list> ::=  <new-CCI>
                      [<cci-list>]

Where:
       <cci-list> is as per
       [RFC9050].
       <PCE-initiated-lsp-instantiation> and
       <PCE-initiated-lsp-deletion> are as per [RFC8281].
       <BPI> and <PPA> are as per
       [draft-ietf-pce-pcep-extension-native-ip-09]
```

When PCInitiate message is used to create VLAN-based forwarding instructions, the SRP, LSP and CCI objects MUST be present. The error handling for missing SRP, LSP or CCI object is as per [RFC9050]. Further only one of BPI, PPA or one type of CCI objects MUST be present. If none of them are present, the receiving PCE MUST send a PCErr message with Error-type=6 (Mandatory Object missing) and Error-value=TBD4 (VLAN-based forwarding object missing). If there are more than one of BPI, PPA or more than one type of CCI objects, the receiving PCC MUST send a PCErr message with Error-type=19(Invalid Operation) and Error-value=TBD5(Only one of BPI, PPA or one type of the CCI objects for VLAN can be included in this message).

5.2. The PCRpt message

The PCRpt message is used to report the state and confirm the VLAN info that was allocated by the PCE, to be used during the state synchronization phase or as acknowledgement to PCInitiate message.

The format of the PCRpt message is as follows:

```
<PCRpt Message> ::= <Common Header>
                          <state-report-list>
     Where:

        <state-report-list> ::= <state-report>[<state-report-list>]

        <state-report> ::= (<lsp-state-report>|
                          <central-control-report>)

        <lsp-state-report> ::= [<SRP>]
                             <LSP>
                             <path>

        <central-control-report> ::= [<SRP>]
                                   <LSP>
                                   <cci-list>|
                                   ((<BPI>|<PPA>)
                                   (<new-CCI>)


       Where:
         <path> is as per [RFC8231] and the LSP and SRP object are
         also defined in [RFC8231].
         <BPI> and <PPA> are as per
         [draft-ietf-pce-pcep-extension-native-ip-09]
```

The error handling for missing LSP or CCI object is as per [RFC9050]. Further only one of BPI, PPA or one type of CCI objects MUST be present. If none of them are present, the receiving PCE MUST send a PCErr message with Error-type=6 (Mandatory Object missing) and Error-value=TBD4 (VLAN-based forwarding object missing). If there are more than one of BPI, PPA or more than one type of CCI objects, the receiving PCC MUST send a PCErr message with Error-type=19(Invalid Operation) and Error-value=TBD5(Only one of BPI, PPA or one type of the CCI objects for VLAN can be included in this message).

6. VSP Operations

Based on [RFC8281] and [RFC9050], in order to set up a PCE-initiated VSP based on the PCECC mechanism, a PCE needs to send a PCInitiate message with the PST set to TBD1 in SRP for the PCECC to the ingress PCC.

The VLAN-forwarding instructions from the PCECC needs to be sent after the initial PCInitiate and PCRpt message exchange with the ingress PCC. On receipt of a PCInitiate message for the PCECC VSP, the PCC responds with a PCRpt message with the status set to 'Going-up', carrying the assigned PLSP-ID and set the D(Delegate) flag and C(Create) flag(see Figure 1).

After that, the PCE needs to send a PCInitiate message to each node along the path to download the VLAN instructions. The new CCI for the VLAN operations in PCEP are sent via the PCInitiate message by defining a new PCEP object for CCI operations. The fields in the LSP-IDENTIFIERS TLV are described for the RSVP-signaled LSPs but are applicable to the PCECC VSP as well. So the LSP object is included in the PCInitiate message can still be used to identify the PCECC VSP for this instruction and the process is the same.

When the PCE receives this PCRpt message with the PLSP-ID, it assigns VLANs along the path and sets up the path by sending a PCInitiate message to each node along the path of the VSP, as per the PCECC technique. The ingress PCC would receive one VLAN forwarding CCI Object which contains VLAN on the logical subinterface and the Peer IP address. The transit PCC would receive two VLAN crossing CCI Objects with the O bit set for the out-VLAN on the egress subinterface and the O bit unset for the in-VLAN on the ingress subinterface. Similar with the transit PCC, the egress PCC would receive two VLAN crossing CCI Objects but the out-VLAN on the egress subinterface is set to 0. Once the VLAN operations are completed, the PCE MUST send a PCUpd message to the ingress PCC.

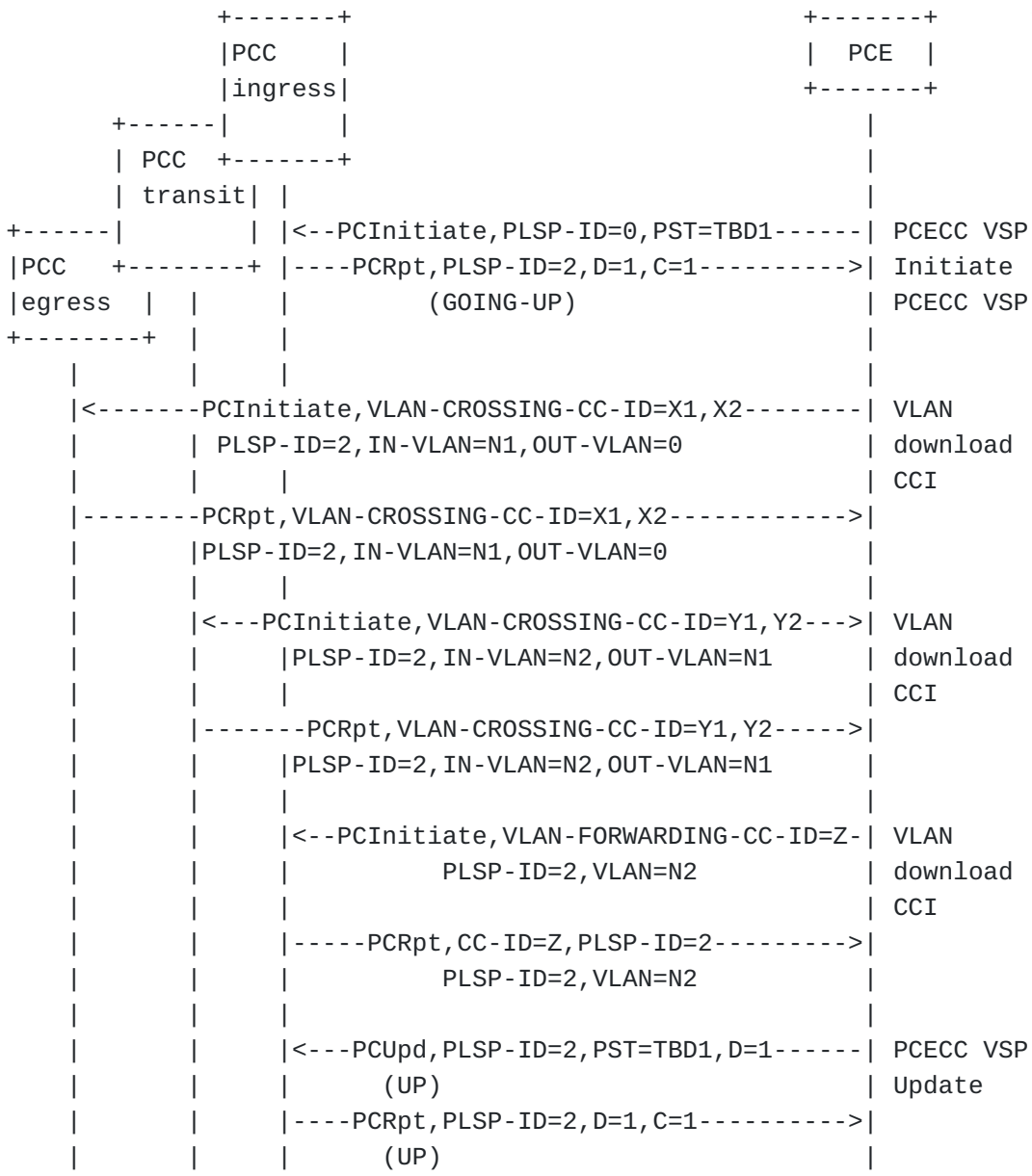
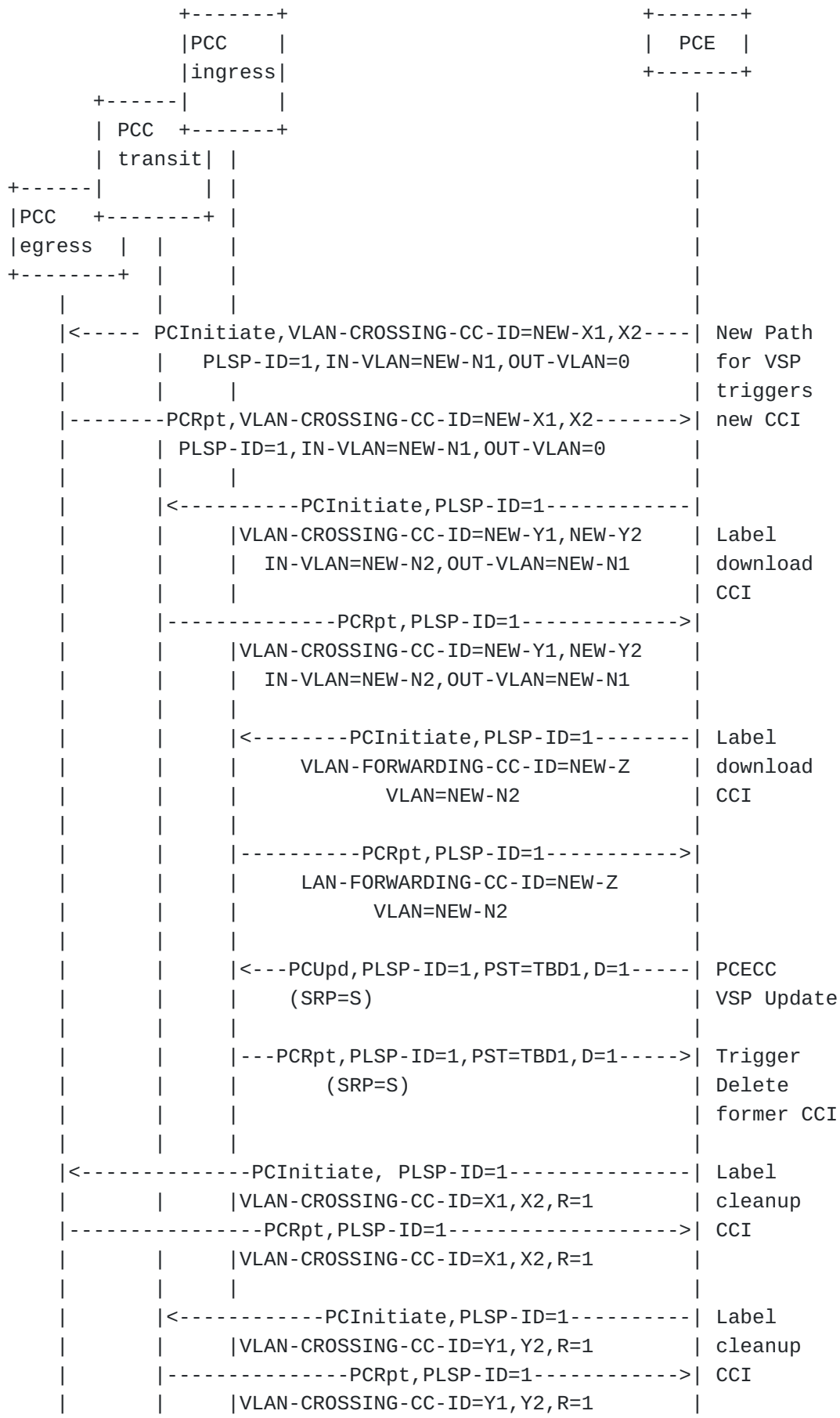


Figure 1: PCE-Initiated PCECC VSP

In order to delete an LSP based on the PCECC, the PCE sends CCI and SRP object with the R bit set to 1 via a PCInitiate message to each node along the path of the VSP to clean up the label-forwarding instruction.

As per [RFC9050], the PCECC VSP also follows the same make-before-break principles. As shown in the figure 2, new path for VSP triggers the new CCI Distribution process. The PCECC firstly updates the new VLAN instructions and informs each node along the new path through the new VLAN crossing CCI Objects and VLAN forwarding CCI Objects to download the new VSP. The PCUpd message then triggers the traffic switch on the updated path. On receipt of the PCRpt message corresponding to the PCUpd message, the PCE does the cleanup

operation for the former VSP,which is the same as the LSP update process.


PCC ingress
PCC transit
PCC egress
PCE
PCInitiate,VLAN-CROSSING-CC-ID=NEW-X1,X2
PLSP-ID=1,IN-VLAN=NEW-N1,OUT-VLAN=0
New Path for VSP triggers new CCI
PCRpt,VLAN-CROSSING-CC-ID=NEW-X1,X2
PLSP-ID=1,IN-VLAN=NEW-N1,OUT-VLAN=0
PCInitiate,PLSP-ID=1
VLAN-CROSSING-CC-ID=NEW-Y1,NEW-Y2
IN-VLAN=NEW-N2,OUT-VLAN=NEW-N1
Label download CCI
PCRpt,PLSP-ID=1
VLAN-CROSSING-CC-ID=NEW-Y1,NEW-Y2
IN-VLAN=NEW-N2,OUT-VLAN=NEW-N1
PCInitiate,PLSP-ID=1
VLAN-FORWARDING-CC-ID=NEW-Z
VLAN=NEW-N2
Label download CCI
PCRpt,PLSP-ID=1
LAN-FORWARDING-CC-ID=NEW-Z
VLAN=NEW-N2
PCUpd,PLSP-ID=1,PST=TBD1,D=1
(SRP=S)
PCECC VSP Update
PCRpt,PLSP-ID=1,PST=TBD1,D=1
(SRP=S)
Trigger Delete former CCI
PCInitiate, PLSP-ID=1
VLAN-CROSSING-CC-ID=X1,X2,R=1
Label cleanup CCI
PCRpt,PLSP-ID=1
VLAN-CROSSING-CC-ID=X1,X2,R=1
PCInitiate,PLSP-ID=1
VLAN-CROSSING-CC-ID=Y1,Y2,R=1
Label cleanup CCI
PCRpt,PLSP-ID=1
VLAN-CROSSING-CC-ID=Y1,Y2,R=1

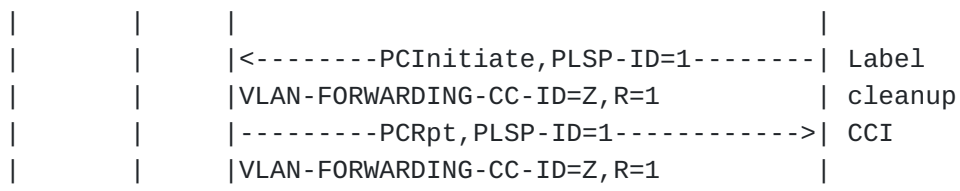


Figure 2: PCECC VSP Update

7. VLAN-based traffic forwarding Procedures

The target deployment environment of VLAN based traffic forwarding mechanism is for both Native IPv4 and IPv6. In such scenarios, the BGP is used for the prefix distribution among underlying devices(PCCs), no MPLS is involved.

In order to set up the VLAN-based traffic forwarding paths for different applications in native IP network, multiple BGP sessions should be deployed between the ingress PCC and egress PCC at the edge of the network respectively.

Based on the business requirements, the PCE calculates the explicit route and sends the route information to the PCCs through PCInitiate messages. When the PCInitiate message is received, the packet to be guaranteed will be labeled with corresponding VLAN tag, that is done by the ingress PCC (See Appendix A). The labeled packet will be further sent to the PCC's specific subinterface identified by the VLAN tag and then be forwarded. Similarly, after receive of the PCInitiate message, the packet will be re-labeled with new VLAN tag and then be forwarded by the transit PCC and the egress PCC(See Appendix A). For PCC, there is no corresponding VLAN allocation mechanism at present which is different with the label in MPLS, so the mechanism of allocating and managing VLAN ID by PCC will not be considered in this draft as per [RFC9050].

The whole procedures mainly focused on the end-to-end traffic assurance for key applications so that it can ensure the adequacy of VLAN quantity. During the packet forwarding process, the packet can be encapsulated with reserved multicast MAC addresses(e.g. 0180:C200:0014 for ISIS level 1, 0180:C200:0015 for ISIS level 2) thus does not need to be changed hop by hop by each PCC.

7.1. Multiple BGP Session Establishment Procedures

As described in section 4, multiple BGP sessions should be deployed between the ingress device and egress device at the edge of the network respectively in order to carry information of different applications. As per [I-D.ietf-pce-pcep-extension-native-ip], the PCE should send the BPI (BGP Peer Info) Object to the ingress and egress device with the indicated Peer AS and Local/Peer IP address. The Ingress and egress devices will receive multiple BPI objects to establish sessions with different next hop. The specific process is as follows:

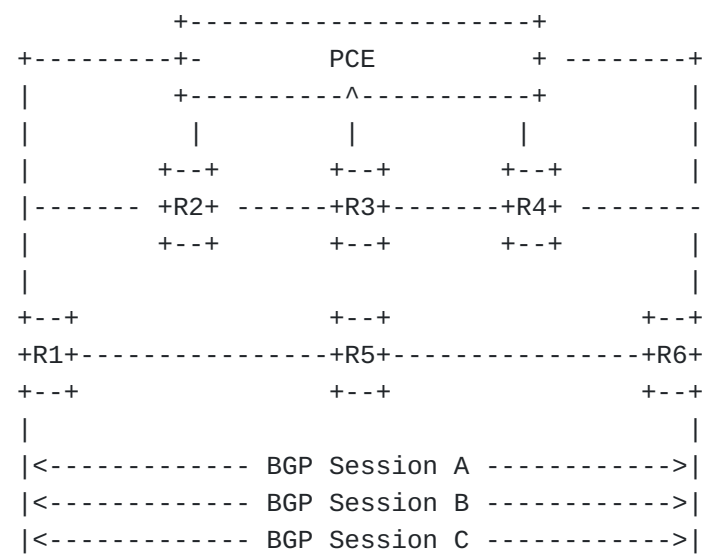


Figure 3: BGP Session Establishment Procedures

7.2. BGP Prefix Advertisement Procedures

The detail procedures for BGP prefix advertisement procedures is introduced in [I-D.ietf-pce-pcep-extension-native-ip], using PCInitiate and PCRpt message pair.

The BGP prefix for different BGP sessions should be sent to the ingress and egress device respectively. The end-to-end traffic for key application can be identified based on these BGP prefix informations and be further assured. As per [I-D.ietf-pce-pcep-extension-native-ip], the PPA(Peer Prefix Association) object with list of prefix subobjects and the peer address will be sent through the PCInitiate and PCRpt message pair. Through BGP protocol, the ingress device can learn different BGP prefix of the egress device based on the different sessions.

7.3. VLAN mapping info Advertisement Procedures

After the BGP prefix for different BGP session are successfully advertised, information of different applications should be forwarded to different VLAN-based traffic forwarding paths. In order to set up a VLAN-based traffic forwarding path, the PCE should send the VLAN forwarding CCI Object with the VLAN-ID included to the ingress PCC and the VLAN crossing CCI Object to the transit PCC and egress PCC.

7.3.1. VLAN-Based forwarding info Advertisement Procedures

The detail procedures for VLAN-Based forwarding info advertisement contained in the VLAN forwarding CCI Object are shown below, using PCInitiate and PCRpt message pair.

The VLAN forwarding CCI Object should be sent through the PCInitiate and PCRpt message pair. After the PCC receives the CCI object (with the R bit set to 0 in SRP object) in PCInitiate message, the PCC's subinterface will set up the specific VLAN based on the VLAN forwarding CCI object, source and destination BGP prefix learnt before. When the ingress PCC receives a packet, based on the source and destination IP, the packet that needs to be guaranteed will be matched and then be labeled with corresponding VLAN tag. After that, The labeled packet will be further forwarded to the specific subinterface.

When PCC receives the VLAN forwarding CCI Object with the R bit set to 1 in SRP object in PCInitiate message, the PCC should withdraw the VLAN-Based forwarding info advertisement to the peer that indicated by this object.

On receipt of a PCInitiate message for the PCECC VSP, the PCC should report the result via the PCRpt messages, with the corresponding SRP and CCI object included.

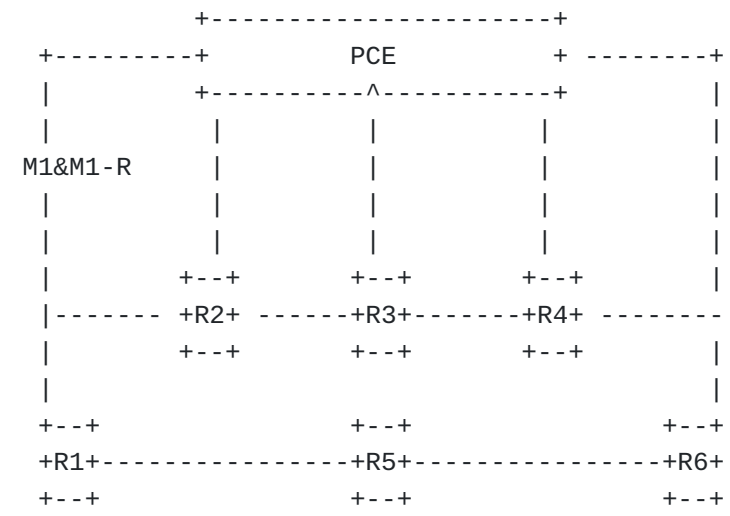


Figure 4: VLAN-Based forwarding info Advertisement Procedures for Ingress PCC

The message number, message peers, message types and message key parameters in the above figures are shown in the table below:

Table 1: Message Information

No.	Peers	Type	Message Key Parameters
M1 M1-R	PCE/R1	PCInitiate PCRpt	CC-ID=X1(Symbolic Path Name=Class A) VLAN Forwarding CCI Object (Peer_IP=R6_A,Interface_Address=INF1, VLAN_ID=VLAN_R1_R2)

7.3.2. VLAN-Based crossing info Advertisement Procedures

The detail procedures for VLAN-Based crossing info advertisement contained in the VLAN crossing CCI Object are shown below, using PCInitiate and PCRpt message pair.

The PCC would receive VLAN crossing CCI Objects with the in-VLAN CCI without the O bit set and the out-VLAN CCI with the O bit set. The in-VLAN tag and an out-VLAN tag in the CCI Objects specifies a new VLAN forwarding path. After the process of VLAN-Based forwarding info advertisement mentioned above, the PCC's subinterface will set up the specific VLAN based on the VLAN crossing CCI Object(with the R bit set to 0 in SRP object) contained in the PCInitiate message. When the transit PCC receives a data packet that has been labeled with VLAN by ingress PCC before, based on matching process of the VLAN tag, the in-VLAN tag of this data packet will be replaced by a new out-VLAN tag of the current transit PCC. The packet with the new VLAN tag will be further forwarded to the next hop.

For the egress PCC, the out-VLAN tag should be 0 which indicates it is the last hop of the transmission. So the egress PCC will directly remove the in-VLAN tag of the packet and the packet will be forwarded.

When PCC receives the VLAN crossing CCI Object with the R bit set to 1 in SRP object in PCInitiate message, the PCC should withdraw the VLAN-Based crossing info advertisement to the peer that indicated by this object.

On receipt of a PCInitiate message for the PCECC VSP, the PCC should report the result via the PCRpt messages, with the corresponding SRP and CCI object included.

When the out-VLAN tag conflicts with a pre-defined VLAN tag or the PCC can not set up a VLAN forwarding path with the out-VLAN tag, an error (Error-type=TBD6, VLAN-based forwarding failure, Error-value=TBD7, VLAN crossing CCI Object peer info mismatch) should be reported via the PCRpt message.

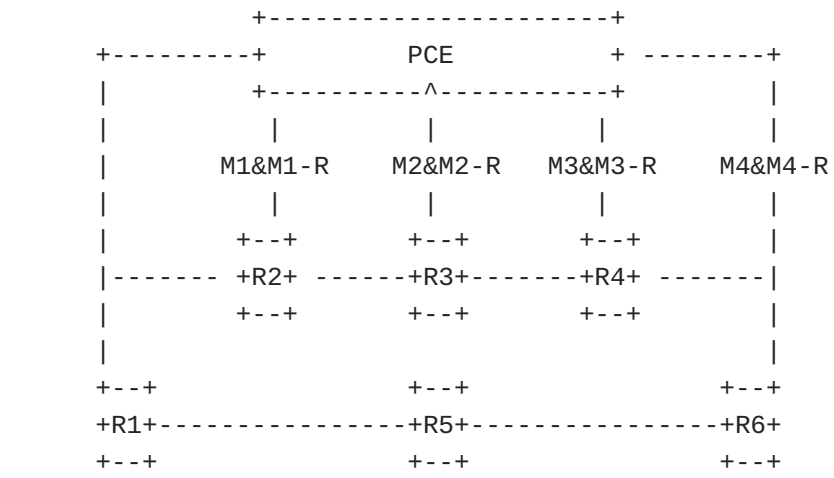


Figure 5: VLAN-Based crossing info Advertisement Procedures
for transit PCC and egress PCC

The message number, message peers, message type and message key parameters in the above figures are shown in below table:

Table 2: Message Information

No.	Peers	Type	Message Key Parameters
M1 M1-R	PCE/R2	PCInitiate	CC-ID=X1(Symbolic Path Name=Class A)
		PCRpt	VLAN crossing CCI Object(IN)
			(O=0,Interface_Address=INF1,IN_VLAN_ID=VLAN_R1_R
			VLAN crossing CCI Object(OUT)
			(O=1,Interface_Address=INF2,OUT_VLAN_ID=VLAN_R2_
M2 M2-R	PCE/R3	PCInitiate	CC-ID=X1(Symbolic Path Name=Class A)
		PCRpt	VLAN crossing CCI Object(IN)
			(O=0,Interface_Address=INF1,IN_VLAN_ID=VLAN_R2_R
			VLAN crossing CCI Object(OUT)
			(O=1,Interface_Address=INF2,OUT_VLAN_ID=VLAN_R3_
M3 M3-R	PCE/R4	PCInitiate	CC-ID=X1(Symbolic Path Name=Class A)
		PCRpt	VLAN crossing CCI Object(IN)
			(O=0,Interface_Address=INF1,IN_VLAN_ID=VLAN_R3_R
			VLAN crossing CCI Object(OUT)
			(O=1,Interface_Address=INF2,OUT_VLAN_ID=VLAN_R4_
M4 M4-R	PCE/R6	PCInitiate	CC-ID=X1(Symbolic Path Name=Class A)
		PCRpt	VLAN crossing CCI Object(IN)
			(O=0,Interface_Address=INF1,IN_VLAN_ID=VLAN_R4_R
			VLAN crossing CCI Object(OUT)
			(O=1,Interface_Address=INF2,OUT_VLAN_ID=0)

8. New PCEP Objects

The Central Control Instructions (CCI) Object is used by the PCE to specify the forwarding instructions is defined in [RFC9050]. This document defines two other CCI object-types for VLAN-based traffic forwarding. All new PCEP objects are compliant with the PCEP object format defined in [RFC5440].

8.1. VLAN forwarding CCI Object

The VLAN forwarding CCI Object is used to set up the specific VLAN forwarding path including the logical subinterface that will be used for traffic forwarding to the specific hop. Combined with this type of CCI Object and the Peer Prefix Association object(PPA) defined in [I-D.ietf-pce-pcep-extension-native-ip], the ingress PCC will identify the traffic that needs to be protected. This object should only be included and sent to the ingress PCC of the end2end path.

CCI Object-Class is 44.

CCI Object-Type is TBD8 for VLAN forwarding info in the native IP network.

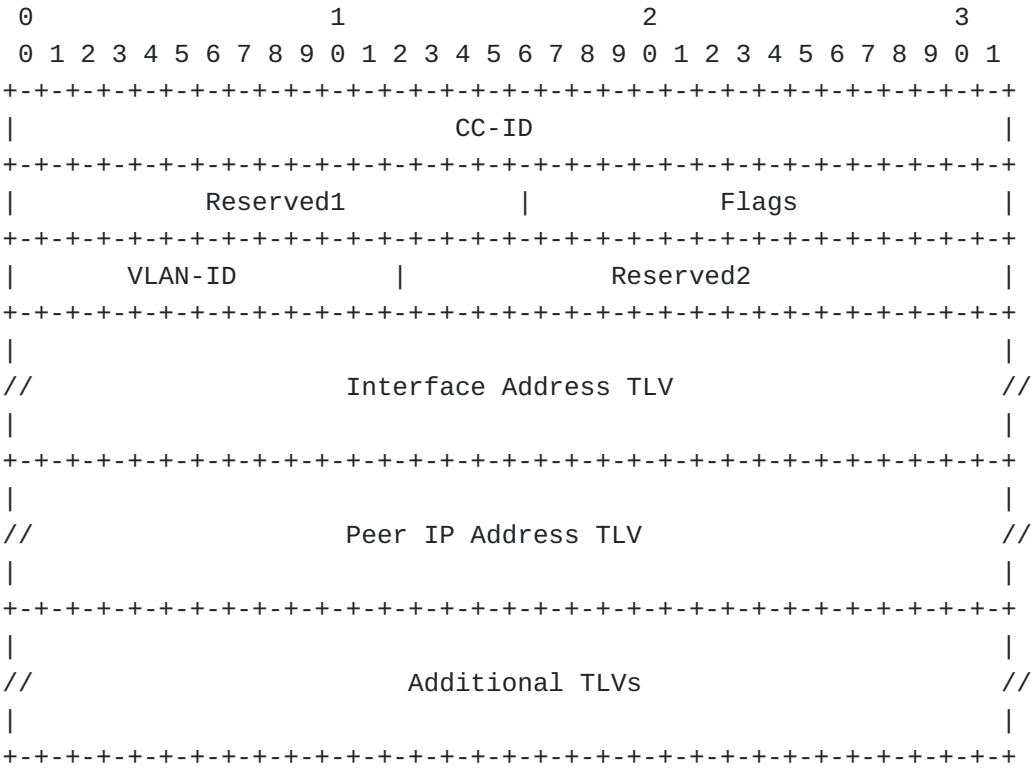


Figure 6: VLAN Forwarding CCI Object

The fields in the CCI object are as follows:

CC-ID: is as described in [RFC9050]. Following fields are defined for CCI Object-Type TBD8.

Reserved1(16 bits): is set to zero while sending, ignored on receipt.

Flags(16 bits): is used to carry any additional information pertaining to the CCI. Currently no flag bits are defined.

VLAN ID(12 bits):the ID of the VLAN forwarding path that the PCC will set up on its logical subinterface in order to transfer the packet to the specific hop.

Reserved2(20 bits): is set to zero while sending, ignored on receipt.

Interface Address TLV [RFC8779] MUST be included in this CCI Object-Type TBD8 to specify the interface which will set up the vlan defined in the VLAN Forwarding CCI Object.

The Peer IP Address TLV [RFC8779]MUST be included in this CCI Object-Type TBD8 to identify the end to end TE path in VLAN-based traffic forwarding network and MUST be unique.

8.2. Address TLVs

[RFC8779] defines IPV4-ADDRESS, IPV6-ADDRESS, and UNNUMBERED-ENDPOINT TLVs for the use of Generalized Endpoint. The same TLVs can also be used in the CCI object to find the Peer address that matches egress PCC and further identify the packet to be guaranteed. If the PCC is not able to resolve the peer information or can not find the corresponding ingress device, it MUST reject the CCI and respond with a PCErr message with Error-Type = TBD6 ("VLAN-based forwarding failure") and Error Value = TBD9 ("Invalid egress PCC information").

8.3. VLAN crossing CCI Object

The VLAN crossing CCI object is defined to control the transmission-path of the packet by VLAN-ID. This new type of CCI Object can be carried within a PCInitiate message sent by the PCE to the transit PCC and the egress PCC in the VLAN-based traffic forwarding scenarios.

CCI Object-Class is 44.

CCI Object-Type is TBD10 for VLAN crossing info in the native IP network.

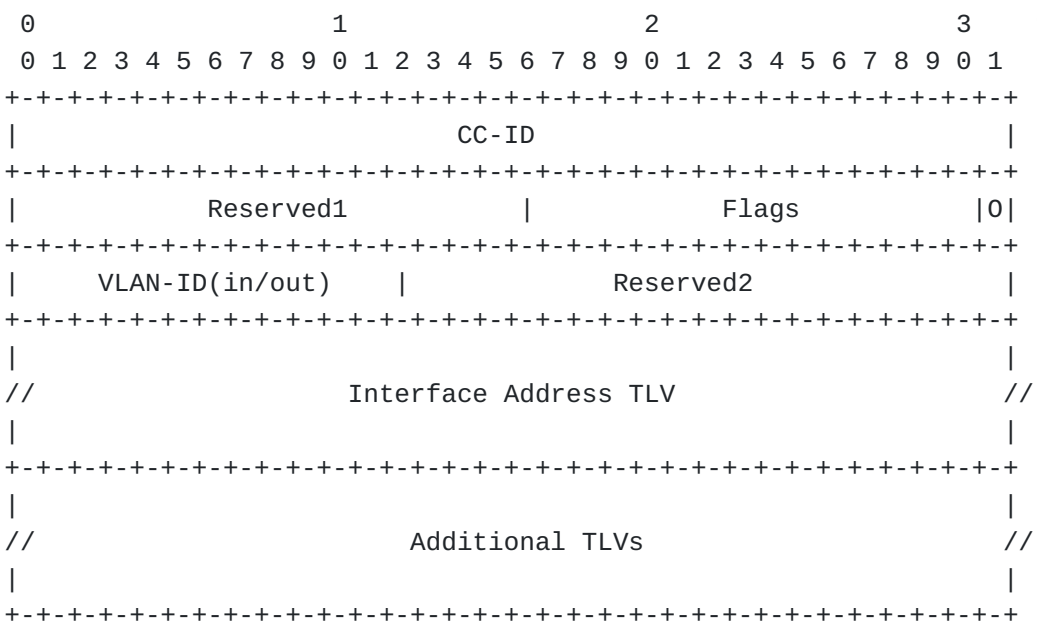


Figure 7: VLAN Crossing CCI Object

CC-ID: is as described in [RFC9050]. Following fields are defined for CCI Object-Type TBD10.

Reserved1(16 bits): is set to zero while sending, ignored on receipt.

Flags(16 bits): is used to carry any additional information pertaining to the CCI. Currently, the following flag bit are defined:

* O bit (out-label) : If the bit is set to '1', it specifies the VLAN is the out-VLAN, and it is mandatory to encode the egress interface information(via Interface Address TLVs in the CCI object). If the bit is not set or set to '0', it specifies the VLAN is the in-VLAN, and it is mandatory to encode the ingress interface information.

VLAN ID(12 bits): The ID of the VLAN switching path. When the O bit is set to 0, the VLAN is the in-VLAN and the ID indicates a VLAN forwarding path which is used to identify the traffic that needs to be protected. When the O bit is set to 1, the VLAN is the out-VLAN and it indicates the ID of the VLAN forwarding path that the PCC will set up on its logical subinterface in order to transfer the packet labled with this VLAN ID to the specific hop. To the transit PCC, the value must not be 0 to indicate it is not the last hop of the VLAN-based traffic forwarding path. To the egress PCC, the value must be 0 to indicate it is the last hop of the VLAN-based traffic forwarding path.

Reserved2(8 bits): is set to zero while sending, ignored on receipt.

Interface Address TLV [RFC8779] MUST be included in this CCI Object-Type TBD8 to specify the interface which will set up the vlan defined in the VLAN Forwarding CCI Object.

9. IANA Considerations

9.1. Path Setup Type Registry

[RFC8408] created a sub-registry within the "Path Computation Element Protocol (PCEP) Numbers" registry called "PCEP Path Setup Types". IANA is requested to allocate a new code point within this registry, as follows:

Value	Description	Reference
TBD1	VLAN-Based Traffic Forwarding Path	This document

9.2. PCECC-CAPABILITY sub-TLV's Flag field

[RFC9050] created a sub- registry within the "Path Computation Element Protocol (PCEP) Numbers" registry to manage the value of the PCECC-CAPABILITY sub- TLV's 32-bits Flag field. IANA is requested to allocate a new bit position within this registry, as follows:

Value	Description	Reference
TBD2(V)	VLAN-Based Forwarding CAPABILITY	This document

9.3. PCEP Object Types

IANA is requested to allocate new registry for the PCEP Object Type:

Object-Class Value	Name	Reference
44	CCI Object-Type TBD8: VLAN forwarding CCI TBD10: VLAN crossing CCI	This docume

9.4. PCEP-Error Object

IANA is requested to allocate new error types and error values within the "PCEP-ERROR Object Error Types and Values" sub-registry of the PCEP Numbers registry for the following errors:

Error-Type	Meaning	Error-value	Reference
6	Mandatory Object missing	TBD4:VLAN-based forwarding object missing	This docume
10	Reception of an invalid object	TBD3:PCECC VLAN-based-forwarding -CAPABILITY bit is not set	This docume
19	Invalid Operation	TBD5: Only one of BPI, PPA or one type of the CCI objects for VLAN can be included in this message	This docume
TBD6	VLAN-based forwarding failure	TBD7: VLAN crossing CCI Object peer info mismatch	This docume
		TBD9: Invalid egress PCC information	This documen

10. Appendix-VLAN switching process

IEEE 802.1Q protocol provides a standard method for implementing VLAN tags. In addition to 802.1Q protocol, there are different implementation methods for VLAN tagging and untagging which is out of the scope of this document. The example below is a feasible implementation method based on a newly defined VLAN-Forwarding routing table and a VLAN-Crossing routing table which can be used to implement the label switching process of VLAN.

VLAN-Forwarding routing table maintained on the ingress PCC is as follows, which is used to match the packet based on the source and destination BGP prefixes.

Table 3: VLAN-Forwarding routing table

Dst IP Address	Interface	VLAN
Prefixes from R6 Session1	INF 1	VLAN_R1_R2
Prefixes from R6 SessionX	INF X	X
	...	

VLAN-Crossing routing table maintained on the transit PCC and egress PCC is as follows. Through the mapping of the in-VLAN and the out-VLAN, the data packet will be transferred to the specific interface and be switched on the out VLAN for the transit PCC or 0 for the egress PCC.

Table 4: VLAN-Crossing routing table

IN-Interface	IN-VLAN	OUT-Interface	OUT-VLAN
INF1	VLAN_R1_R2	INF2	VLAN_R2_R3
INF3	X	INF4	Y
INF5	Z	INF6	0
	...		

11. Normative References

[I-D.ietf-pce-pcep-extension-for-pce-controller] Li, Z., Peng, S., Negi, M. S., Zhao, Q., and C. Zhou, "Path Computation Element Communication Protocol (PCEP) Procedures and Extensions for Using the PCE as a Central Controller (PCECC) of LSPs", Work in Progress, Internet-Draft, draft-ietf-pce-pcep-extension-for-pce-controller-14, 5 March 2021, <https://www.ietf.org/archive/id/draft-ietf-pce-pcep-extension-for-pce-controller-14.txt>.

[I-D.ietf-pce-pcep-extension-native-ip] Wang, A., Khasanov, B., Fang, S., Tan, R., and C. Zhu, "PCEP Extension for Native IP Network", Work in Progress, Internet-Draft, draft-ietf-pce-pcep-extension-native-ip-19, 21 September 2022, <https://www.ietf.org/archive/id/draft-ietf-pce-pcep-extension-native-ip-19.txt>.

[RFC2119] Bradner, S. and RFC Publisher, "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>.

[RFC4655] Farrel, A., Vasseur, J.-P., Ash, J., and RFC Publisher, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

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

[RFC8231] Crabbe, E., Minei, I., Medved, J., Varga, R., and RFC Publisher, "Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE", RFC 8231, DOI 10.17487/RFC8231, September 2017, <https://www.rfc-editor.org/info/rfc8231>.

[RFC8281] Crabbe, E., Minei, I., Sivabalan, S., Varga, R., and RFC Publisher, "Path Computation Element Communication Protocol (PCEP) Extensions for PCE-Initiated LSP Setup in a Stateful PCE Model", RFC 8281, DOI 10.17487/RFC8281, December 2017, <https://www.rfc-editor.org/info/rfc8281>.

[RFC8283] Farrel, A., Ed., Zhao, Q., Ed., Li, Z., Zhou, C., and RFC Publisher, "An Architecture for Use of PCE and the PCE Communication Protocol (PCEP) in a Network with Central Control", RFC 8283, DOI 10.17487/RFC8283, December 2017, <https://www.rfc-editor.org/info/rfc8283>.

[RFC8408] Sivabalan, S., Tantsura, J., Minei, I., Varga, R., and J. Hardwick, "Conveying Path Setup Type in PCE Communication Protocol (PCEP) Messages", RFC 8408, DOI 10.17487/RFC8408, July 2018, <https://www.rfc-editor.org/info/rfc8408>.

[RFC8735] Wang, A., Huang, X., Kou, C., Li, Z., Mi, P., and RFC Publisher, "Scenarios and Simulation Results of PCE in a Native IP Network", RFC 8735, DOI 10.17487/RFC8735, February 2020, <https://www.rfc-editor.org/info/rfc8735>.

[RFC8779] Margaria, C., Ed., Gonzalez de Dios, O., Ed., and F. Zhang, Ed., "Path Computation Element Communication Protocol (PCEP) Extensions for GMPLS", RFC 8779, DOI 10.17487/RFC8779, July 2020, <https://www.rfc-editor.org/info/rfc8779>.

[RFC9050] Li, Z., Peng, S., Negi, M., Zhao, Q., Zhou, C., and RFC Publisher, "Path Computation Element Communication Protocol (PCEP) Procedures and Extensions for Using the PCE as a Central Controller (PCECC) of LSPs", RFC 9050, DOI 10.17487/RFC9050, July 2021, <https://www.rfc-editor.org/info/rfc9050>.

Authors' Addresses

Yue Wang
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China

Email: wangy73@chinatelecom.cn

Aijun Wang
China Telecom

Beiqijia Town, Changping District
Beijing
Beijing, 102209
China

Email: wangaj3@chinatelecom.cn

Boris Khasanov
Yandex LLC
Ulitsa Lva Tolstogo 16
Moscow

Email: bhassanov@yandex-team.ru

Fengwei Qin
China Mobile
32 Xuanwumenxi Ave.
Beijing
100032
China

Email: qinfengwei@chinamobile.com

Huaimo Chen
Futurewei
Boston,
United States of America

Email: Huaimo.chen@futurewei.com

Chun Zhu
ZTE Corporation
50 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China

Email: zhu.chun1@zte.com.cn