Management Information Base for the PCE Communications Protocol (PCEP) for Path-Key-Based Inter-Domain Path Computation
draft-dhody-pce-pcep-pathkey-mib-00

Abstract

This memo defines an experimental portion of the Management Information Base for use with network management protocols in the Internet community. In particular, it describes managed objects for modeling of the Path Computation Element communication Protocol (PCEP) for communications between a Path Computation Client (PCC) and a Path Computation Element (PCE), or between two PCEs when path-key-based inter-domain path computation is requested.

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/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on April 9, 2011.
Copyright Notice

Copyright (c) 2010 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.

This Internet-Draft will expire on April 9, 2011.

Table of Contents

1. Introduction .................................................. 3
2. Terminology ................................................. 3
3. The Internet-Standard Management Framework .................. 4
4. PCEP Pathkey MIB Module Architecture ....................... 4
5. Example of the PCEP PathKey MIB module usage ............... 4
6. Object definitions ........................................... 5
   6.1. PCE-PCEP-PATHKEY-DRAFT-MIB ............................. 5
   6.2. Objects for inclusion in module PCE-PCEP-DRAFT-MIB ...... 15
7. IANA Considerations .......................................... 15
8. Security Considerations ...................................... 15
9. References .................................................. 16
   9.1. Normative References ................................. 16
   9.2. Informative References .............................. 17
1. Introduction

The Path Computation Element (PCE) defined in [RFC4655] is an entity that is capable of computing a network path or route based on a network graph, and applying computational constraints. A Path Computation Client (PCC) may make requests to a PCE for paths to be computed.

The PCE communication protocol (PCEP) is designed as a communication protocol between PCCs and PCEs for point-to-point (P2P) path computations and is defined in [RFC5440].

If confidentiality is required between domains, Path-Key-Based mechanism is described in [RFC 5520]. For preserving the confidentiality of the "Confidential Path Segment (CPS)", the PCE returns a path containing a loose hop in place of the segment that must be kept confidential.

[PCE-PCEP-DRAFT-MIB] defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community for P2P path computations.

This memo defines an experimental portion of the Management Information Base for use with network management protocols in the Internet community. In particular, it describes managed objects for modeling of Path Computation Element communication Protocol (PCEP) [RFC5440] for communications between a Path Computation Client (PCC) and a Path Computation Element (PCE), or between two PCEs in path-key-based inter-domain path computations.

Some objects maybe moved to [PCE-PCEP-DRAFT-MIB] after consensus with the authors and working group, these are defined in section 6.2.

2. Terminology

The following terminology is used in this document.

CPS: Confidential Path Segment. A segment of a path that contains nodes and links that the AS policy requires to not be disclosed outside the AS.

Domain: Any collection of network elements within a common sphere of address management or path computational responsibility. Examples of domains include Interior Gateway Protocol (IGP) areas and Autonomous Systems (ASs).

PCC: Path Computation Client: any client application requesting a path computation to be performed by a Path Computation Element.

PCE: Path Computation Element. An entity (component, application, or network node) that is capable of computing a network path or route based on a network graph and applying computational constraints.

P2P: Point-to-Point

3. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578] and STD 58, RFC 2580 [RFC2580].

4. PCEP Pathkey MIB Module Architecture

The PCEP Pathkey MIB will contain the following information:

- PCEP Pathkey counters, timers and configurations
- PCEP Pathkey table of CPS related information.

5. Example of the PCEP PathKey MIB module usage

In this section we provide an example (pcePcepPathKeyTable 1) of using the MIB objects described in Section 6 (Object definitions) to monitor. While this example is not meant to illustrate every permutation of the MIB, it is intended as an aid to understanding some of the key concepts. It is meant to be read after going through the MIB itself.
pcePcepPathKeyTable 1 of the PCE-PCEP-PATHKEY-DRAFT-MIB module:
{
  pcePcepPathKey                 (4512),
  pcePcepPathKeyPath             (10.1.1.1 S
              10.1.1.2 S),
  pcePcepPathKeyRequestSource    (x.x.x.x),
  pcePcepPathKeyRequestId        (10),
  pcePcepPathKeyRetrieved        (1),
  pcePcepPathKeyRetrieveSource   (y.y.y.y),
  pcePcepPathKeyDiscardTime      (10),
  pcePcepPathKeyReuseTime        (30)
}

6. Object definitions

6.1. PCE-PCEP-PATHKEY-DRAFT-MIB

This MIB module makes references to the following documents.

[RFC2578], [RFC2580], [RFC3411], [RFC2863], [RFC3813].

PCE-PCEP-PATHKEY-DRAFT-MIB DEFINITIONS ::= BEGIN

IMPORTS
  MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE,
  Unsigned32,
  Counter32,
  OCTET STRING,
  experimental
  FROM SNMPv2-SMI
    -- [RFC2578]

  PcePcepIdentifier,
  FROM PCE-TC-STD-MIB

  MODULE-COMPLIANCE,
  OBJECT-GROUP,
  NOTIFICATION-GROUP
  FROM SNMPv2-CONF;
    -- [RFC2580]
This MIB module defines a collection of objects for managing PCE communication protocol (PCEP) for Path-Key-Based Inter-Domain Path Computation.

-- Revision history
REVISION
"201009171200Z" -- 17 Sep 2010 12:00:00 EST

DESCRIPTION
"draft-00 version"
 ::= { experimental 9999 } --

-- Notifications --

cpePcepPathKeyNotifications OBJECT IDENTIFIER ::= 
   { pcePcepPathKeyDraftMIB 0 } 

cpePcepPathKeyMIBObjects OBJECT IDENTIFIER ::= 
   { pcePcepPathKeyDraftMIB 1 } 

cpePcepPathKeyConformance OBJECT IDENTIFIER ::= 
   { pcePcepPathKeyDraftMIB 2 } 

cpePcepPathKeyObjects OBJECT IDENTIFIER ::= 
   { pcePcepPathKeyMIBObjects 1 }
-- PCE Pathkey Objects

pcePcepPathKeyDiscardTimer OBJECT-TYPE
SYNTAX  Unsigned32
UNITS   "minutes"
MAX-ACCESS read-create
STATUS mandatory
DESCRIPTION "The value which indicates a period of time after the expiration of which a PCE discard unwanted path-keys."
::= { pcePcepPathKeyObjects 1 }

pcePcepPathKeyReUseTimer OBJECT-TYPE
SYNTAX  Unsigned32
UNITS   "minutes"
MAX-ACCESS read-create
STATUS mandatory
DESCRIPTION "The value which indicates a period of time which should expire before an old path-key could be reused for a new CPS."
::= { pcePcepPathKeyObjects 2 }

pcePcepPathKeyRetainStatus OBJECT-TYPE
SYNTAX   INTEGER { enabled(1),
                      disabled(2) }
MAX-ACCESS read-create
STATUS   optional
DESCRIPTION "The path-key retain status of this PCE to retain the path-key and CPS for debugging purposes."
::= { pcePcepPathKeyObjects 3 }

pcePcepPathKeysGenerated OBJECT-TYPE
SYNTAX   Counter32
MAX-ACCESS read-only
STATUS   mandatory
DESCRIPTION "The number of path-keys generated by this PCE."
::= { pcePcepPathKeyObjects 4 }
pcePcepPathKeyExpandUnknown  OBJECT-TYPE
SYNTAX   Counter32
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The number of attempts to expand an unknown path-key."
::= { pcePcepPathKeyObjects 5 }

pcePcepPathKeyExpandExpired  OBJECT-TYPE
SYNTAX   Counter32
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The number of attempts to expand an expired path-key."
::= { pcePcepPathKeyObjects 6 }

pcePcepPathKeyExpandSame  OBJECT-TYPE
SYNTAX   Counter32
MAX-ACCESS read-only
STATUS optional
DESCRIPTION
"The number of attempts to expand the same path-key."
::= { pcePcepPathKeyObjects 7 }

pcePcepPathKeyExpiredNoExpansion  OBJECT-TYPE
SYNTAX   Counter32
MAX-ACCESS read-only
STATUS optional
DESCRIPTION
"The number of path-keys expired without any attempt to expand it."
::= { pcePcepPathKeyObjects 8 }

pcePcepPathKeyExpansionSuccess  OBJECT-TYPE
SYNTAX   Counter32
MAX-ACCESS read-only
STATUS optional
DESCRIPTION
"The number of path-key expansion requests (PCReq) which had successful retrieval."
::= { pcePcepPathKeyObjects 9 }
pcePcepPathKeyExpansionFailures OBJECT-TYPE
SYNTAX   Counter32
MAX-ACCESS read-only
STATUS   optional
DESCRIPTION
   "The number of path-key expansion requests (PCReq)
   which had failed retrieval."
 ::= {  pcePcepPathKeyObjects 10 }

pcePcepPathKeyConfig OBJECT-TYPE
SYNTAX      INTEGER {
   enabled(1),
   disabled(2)
 }
MAX-ACCESS  read-create
STATUS      mandatory
DESCRIPTION
   "The path-key based inter domain computation
   configuration."
 ::= {  pcePcepPathKeyObjects 11 }

pcePcepPathKeyTable  OBJECT-TYPE
SYNTAX      SEQUENCE OF pcePcepPathKeyEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
   "This table contains information about the
   Pathkey CPS of PCE."
 ::= {  pcePcepPathKeyObjects 12 }

pcePcepPathKeyEntry OBJECT-TYPE
SYNTAX      pcePcepPathKeyEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
   "An entry in this table represents a path-key and CPS.
   An entry is only created when a path-key generated by
   PCE during inter-domain computation."

INDEX       { pcePcepPathKey }
 ::= {  pcePcepPathKeyTable 1 }
pcePcepPathKeyEntry ::= SEQUENCE {
    pcePcepPathKey                 Unsigned32,
    pcePcepPathKeyPath             OCTET STRING,
    pcePcepPathKeyRequestSource    PcePcepIdentifier,
    pcePcepPathKeyId                Unsigned32,
    pcePcepPathKeyRetrieved        INTEGER,
    pcePcepPathKeyRetrieveSource   PcePcepIdentifier,
    pcePcepPathKeyDiscardTime      Unsigned32,
    pcePcepPathKeyReuseTime        Unsigned32,
}

pcePcepPathKey OBJECT-TYPE
SYNTAX  Unsigned32
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
    "The path-key value to identify a CPS."
::= {  pcePcepPathKeyEntry 1 }

pcePcepPathKeyPath OBJECT-TYPE
SYNTAX  OCTET STRING (SIZE (0..1024))
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
    "The CPS associated with the pathkey.
    This field is a displayable string in the format of XXX.XXX.XXX.XXX <space> S/L <newline> repeated for each hop address. The S/L character stands for Strict/Loose route.
    This field is meaningless unless pcePcepPathKey is not empty."
::= {  pcePcepPathKeyEntry 2 }

pcePcepPathKeyRequestSource OBJECT-TYPE
SYNTAX  PcePcepIdentifier
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
    "Source that issued the original request that led to the creation of the path-key."
::= {  pcePcepPathKeyEntry 3 }
pcePcepPathKeyRequestId OBJECT-TYPE
SYNTAX  Unsigned32
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The request ID of the original PCReq that led
to the creation of the path-key."
::= { pcePcepPathKeyEntry 4 }

pcePcepPathKeyRetrieved OBJECT-TYPE
SYNTAX      INTEGER {
            TRUE(1),
            FALSE(2)
        }
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"It specifies whether the path-key is retrieved
or not."

pcePcepPathKeyRetrieveSource OBJECT-TYPE
SYNTAX  PcePcepIdentifier
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"If the path-key is retrieved then by which
PCC."
::= { pcePcepPathKeyEntry 6 }

pcePcepPathKeyDiscardTime OBJECT-TYPE
SYNTAX  Unsigned32
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The time after which the path segment associated
with the path-key will be discarded."
::= { pcePcepPathKeyEntry 7 }

pcePcepPathKeyReuseTime OBJECT-TYPE
SYNTAX  Unsigned32
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The time after which the path-key will be available
for re-use."
::= { pcePcepPathKeyEntry 8 }

---
--- Notifications
---

pcePcepPathKeyExpandUnknownNtf NOTIFICATION-TYPE
OBJECTS     
            
    pcePcepPathKeyExpandUnknown

    
STATUS      mandatory
DESCRIPTION  "This notification is sent when an attempt to expand an
unknown path-key is made. The value of the counter
pcePcepPathKeyExpandUnknown is also increased at this
time."
::= { pcePcepPathKeyNotifications 1 }

pcePcepPathKeyExpandExpiredNtf NOTIFICATION-TYPE
OBJECTS     
            
    pcePcepPathKeyExpandExpired

    
STATUS      mandatory
DESCRIPTION  "This notification is sent when an attempt to expand an
expired path-key is made. The value of the counter
pcePcepPathKeyExpandExpired is also increased at this
time."
::= { pcePcepPathKeyNotifications 2 }

pcePcepPathKeyExpandSameNtf NOTIFICATION-TYPE
OBJECTS     
            
    pcePcepPathKeyExpandSame

    
STATUS      optional
DESCRIPTION  "This notification is sent when a duplicate attempt to
expand the same path-key is made. The value of the
counter pcePcepPathKeyExpandSame is also increased at
this time."
::= { pcePcepPathKeyNotifications 3 }
**pcePcepPathKeyExpandSameNtf** NOTIFICATION-TYPE
  OBJECTS {
    pcePcepPathKeyExpiredNoExpansion
  }
  STATUS optional
  DESCRIPTION "This notification is sent when path-key expires without
  any attempt to expand it. The value of the counter
  pcePcepPathKeyExpiredNoExpansion is also increased at
  this time."
  ::= { pcePcepPathKeyNotifications 4 }

--************************************************************************
-- Module Conformance Statement
--************************************************************************

pcePcepPathKeyGroups
  OBJECT IDENTIFIER ::= { pcePcepPathKeyConformance 1 }

pcePcepPathKeyCompliances
  OBJECT IDENTIFIER ::= { pcePcepPathKeyConformance 2 }

--
-- Full Compliance
--

pcePcepPathKeyModuleFullCompliance MODULE-COMPLIANCE
  STATUS current
  DESCRIPTION "The Module is implemented with support
  for read-create and read-write. In other
  words, both monitoring and configuration
  are available when using this MODULE-COMPLIANCE."
  MODULE -- this module
  MANDATORY-GROUPS { pcePcepPathKeyGeneralGroup,
    pcePcepPathKeyNotificationsGroup }

  ::= { pcePcepPathKeyCompliances 1 }
-- Read-Only Compliance
--

pcePcepPathKeyModuleReadOnlyCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION
"The Module is implemented with support for read-only. In other words, only monitoring is available by implementing this MODULE-COMPLIANCE."

MODULE -- this module
MANDATORY-GROUPS { pcePcepPathKeyGeneralGroup,
} ::= { pcePcepPathKeyCompliances 2 }

-- units of conformance

pcePcepPathKeyGeneralGroup OBJECT-GROUP
OBJECTS {
  pcePcepPathKeyDiscardTimer,
pcePcepPathKeyReUseTimer,
pcePcepPathKeysGenerated,
pcePcepPathKeyExpandUnknown,
pcePcepPathKeyExpandExpired,
pcePcepPathKeyConfig,
pcePcepPathKey,
pcePcepPathKeyPath,
pcePcepPathKeyRequestSource,
pcePcepPathKeyRequestId,
pcePcepPathKeyRetrieved,
pcePcepPathKeyRetrieveSource,
pcePcepPathKeyDiscardTime,
pcePcepPathKeyReuseTime
}
STATUS current
DESCRIPTION
"Objects that apply to all PCEP Pathkey MIB implementations."

 ::= { pcePcepPathKeyGroups 1 }
pcePcepPathKeyNotificationsGroup NOTIFICATION-GROUP
   NOTIFICATIONS { pcePcepPathKeyExpandUnknownNtf, pcePcepPathKeyExpandExpiredNtf }

DESCRIPTION
   "The notifications for a PCEP Pathkey MIB implementation."
   ::= { pcePcepPathKeyGroups 2 }

END

6.2. Objects for inclusion in module PCE-PCEP-DRAFT-MIB

Following object may be moved to [PCE-PCEP-DRAFT-MIB] after consensus
with the authors and working group.

pcePcepPathKeyConfig

7. IANA Considerations

TBD

8. Security Considerations

This MIB module can be used for configuration of certain objects, and
anything that can be configured can be incorrectly configured, with
potentially disastrous results.

There are a number of management objects defined in this MIB module
with a MAX-ACCESS clause of read-create. Such objects may be
considered sensitive or vulnerable in some network environments. The
support for SET operations in a non-secure environment without proper
protection can have a negatie effect on network operations. These
are the tables and objects and their sensitivity/vulnerability:

- pcePcepPathKeyDiscardTimer: Setting this value incorrectly may
cause the expiration of Pathkey before attempt to retrieve the
  CPS.

- pcePcepPathKeyReUseTimer: Setting this value incorrectly may cause
  the re-use of pathkey which may not guarantee the uniqueness of
  path-key values.

The user of the PCE-PCEP-PATHKEY-DRAFT-MIB module must therefore be
aware that support for SET operations in a non-secure environment
without proper protection can have a negative effect on network
The readable objects in the PCE-PCEP-PATHKEY-DRAFT-MIB module (i.e., those with MAX-ACCESS other than not-accessible) may be considered sensitive in some environments since, collectively, they provide information about the amount and frequency of path computation requests and responses within the network and can reveal some aspects of their configuration.

In such environments it is important to control also GET and NOTIFY access to these objects and possibly even to encrypt their values when sending them over the network via SNMP.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

9. References

9.1. Normative References


9.2. Informative References


Authors’ Addresses

Dhruv Dhody
Huawei Technology
Leela Palace
Bangalore, Karnataka 560008
INDIA

EMail: dhruvd@huawei.com
Udayasree Palle
Huawei Technology
Leela Palace
Bangalore, Karnataka  560008
INDIA
EMail: Udayasreepalle@huawei.com

Quintin Zhao
Huawei Technology
125 Nagog Technology Park
Acton, MA  01719
US
EMail: qzhao@huawei.com

Daniel King
Old Dog Consulting
UK
EMail: daniel@olddog.co.uk