Management Information Base (MIB) for the PCE Communications Protocol (PCEP) for Path-Key based Confidentiality in Inter-Domain Path Computation.

draft-dhody-pce-pcep-pathkey-mib-04

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 confidentiality in inter-domain path computation is requested.

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 http://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 February 18, 2013.

Copyright Notice

Copyright (c) 2012 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.
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 ...... 19
7. IANA Considerations ............................................. 20
8. Security Considerations ........................................ 20
9. References .................................................... 21
   9.1. Normative References ..................................... 21
   9.2. Informative References .................................... 22
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 [RFC5520]. 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 confidentiality in inter-domain path computations.

Some objects may be 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).

Path-Key: A Key used to replace or retrieve the Confidential Path Segment (CPS).

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 [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 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),
  pcePcepPathKeyCPSIndex    (1),
  pcePcepPathKeyRequestSource  (x.x.x.x),
  pcePcepPathKeyRequestId    (10),
  pcePcepPathKeyRetrieved    (1),
  pcePcepPathKeyRetrieveSource (y.y.y.y),
  pcePcepPathKeyDiscardTime  (10),
  pcePcepPathKeyReuseTime    (30)
}

pcePcepPathKeyHopTable 1 of the PCE-PCEP-PATHKEY-DRAFT-MIB module :
{
  pcePcepPathKeyHopListIndex     1,
  pcePcepPathKeyHopIndex         1,
  pcePcepPathKeyHopAddrType      ipv4 (1),
  pcePcepPathKeyHopIpAddr        "192.168.100.1",
  pcePcepPathKeyHopIpPrefixLen   32,
  pcePcepPathKeyHopType          strict (2)
}
{
  pcePcepPathKeyHopListIndex     1,
  pcePcepPathKeyHopIndex         2,
  pcePcepPathKeyHopAddrType      ipv4 (1),
  pcePcepPathKeyHopIpAddr        "192.168.100.2",
  pcePcepPathKeyHopIpPrefixLen   32,
  pcePcepPathKeyHopType          strict (2)
}

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]

TimeStamp
  FROM SNMPv2-TC -- [RFC2579]

PcePcepIdentifier,
  FROM PCE-TC-STD-MIB

MplsLSPID, MplsPathIndex, TeHopAddressType, TeHopAddress, TeHopAddressUnnum
  FROM MPLS-TC-STD-MIB -- [RFC3811]

MODULE-COMPLIANCE,
  OBJECT-GROUP,
  NOTIFICATION-GROUP
  FROM SNMPv2-CONF; -- [RFC2580]

pcePcepPathkeyDraftMIB MODULE-IDENTITY
  LAST-UPDATED "201208171200Z" -- Aug 17, 2012
  ORGANIZATION "Path Computation Element (PCE) Working Group"
  CONTACT-INFO "

Dhruv Dhody
Udayasree Palle
Quintin Zhao
Huawei Technology
Daniel King
OldDog Consulting

EMail: dhruv.dhody@huawei.com
EMail: udayasree.palle@huawei.com
EMail: quintin.zhao@huawei.com
EMail: daniel@oldog.co.uk
EMail comments directly to the PCE WG Mailing List at pce@ietf.org
WG-URL: http://www.ietf.org/html.charters/pce-charter.html"

DESCRIPTION
"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
"201208171200Z" -- 17 Aug 2012 12:00:00 EST
DESCRIPTION "
Main Changes from -03 draft:
1. Adding of DEFVAL for some objects.
2. Editorial Changes.

REVISION
"201202221200Z" -- 22 Feb 2012 12:00:00 EST
DESCRIPTION "
Main Changes from -02 draft:
1. Editorial Changes.
2. Updated Contact Information.

REVISION
"201109051200Z" -- 05 Sept 2011 12:00:00 EST
DESCRIPTION "
Main Changes from -01 draft:
1. Added pcePcepPathKeyCPSIndex.
2. Added pcePcepPathKeyHopListIndex.
3. Removed pcePcepPathKeyHopNum.
4. Updated Contact Information.

REVISION
"201103081200Z" -- 08 Mar 2011 12:00:00 EST
DESCRIPTION "
Main Changes from -00 draft:
1. Added HopTable to store the CPS hops.
2. Added Path Key Creation Time.

REVISION
"201009171200Z" -- 17 Sep 2010 12:00:00 EST
DESCRIPTION "
draft-00 version"
::= { experimental 9999 } --
-- Notifications --

pcePcepPathKeyNotifications OBJECT IDENTIFIER ::= { pcePcepPathKeyDraftMIB 0 }

pcePcepPathKeyMIBObjects OBJECT IDENTIFIER ::= { pcePcepPathKeyDraftMIB 1 }

pcePcepPathKeyConformance OBJECT IDENTIFIER ::= { pcePcepPathKeyDraftMIB 2 }

pcePcepPathKeyObjects OBJECT IDENTIFIER ::= { pcePcepPathKeyMIBObjects 1 }

--

-- PCE Pathkey Objects

--

pcePcepPathKeyDiscardTimer OBJECT-TYPE
SYNTAX  Unsigned32
UNITS   "minutes"
MAX-ACCESS read-write
STATUS mandatory
DESCRIPTION
"The value which indicates a period of time after the expiration of which a PCE discard unwanted path-keys."
DEFVAL {10} ::= { pcePcepPathKeyObjects 1 }

pcePcepPathKeyReUseTimer OBJECT-TYPE
SYNTAX  Unsigned32
UNITS   "minutes"
MAX-ACCESS read-write
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."
DEFVAL {30} ::= { pcePcepPathKeyObjects 2 }
pcePcepPathKeyRetainStatus OBJECT-TYPE
SYNTAX INTEGER {
    enabled(1),
    disabled(2)
}
MAX-ACCESS read-write
STATUS optional
DESCRIPTION
"The path-key retain status of this PCE to retain the
path-key and CPS for debugging purposes."
DEFVAL (disabled(2))
::= { 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-write
  STATUS   mandatory
  DESCRIPTION
           "The path-key based inter domain computation
configuration."
  DEFVAL { disabled(2) }
  ::= {  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 }
Internet-Draft         PCE-PCEP-PATHKEY-DRAFT-MIB            August 2012

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,
pcePcepPathKeyCPSIndex         MplsPathIndex,
pcePcepPathKeyRequestSource    PcePcepIdentifier,
pcePcepPathKeyRequestId        Unsigned32,
pcePcepPathKeyRetrieved        INTEGER,
pcePcepPathKeyRetrieveSource   PcePcepIdentifier,
pcePcepPathKeyCreationTime     TimeStamp,
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 }

pcePcepPathKeyCPSIndex OBJECT-TYPE
SYNTAX     MplsPathIndex
MAX-ACCESS read-only
STATUS     mandatory
DESCRIPTION
"The HopList index of the CPS. This index is used to expand Hops in
pcePcepPathKeyHopTable."
 ::= { 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 }

pcePcepPathKeyId 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."
::= { pcePcepPathKeyEntry 5 }

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

pcePcepPathKeyCreationTime OBJECT-TYPE
SYNTAX  TimeStamp
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The value of sysUpTime at which Path Key was generated by PCE."
::= { pcePcepPathKeyEntry 7 }
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 8 }

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 9 }

pcePcepPathKeyHopTable  OBJECT-TYPE
SYNTAX      SEQUENCE OF pcePcepPathKeyHopEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
"This table contains information about the
Pathkey Hop in the CPS of PCE."
::= { pcePcepPathKeyObjects 13 }

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

INDEX       { pcePcepPathKeyHopListIndex,
             pcePcepPathKeyHopIndex }

::= { pcePcepPathKeyHopTable 1 }
pcePcepPathKeyHopEntry ::= SEQUENCE {
  pcePcepPathKeyHopListIndex     MplsPathIndex,
  pcePcepPathKeyHopIndex         MplsPathIndex,
  pcePcepPathKeyHopAddrType      TeHopAddressType,
  pcePcepPathKeyHopIpAddr        TeHopAddress,
  pcePcepPathKeyHopIpPrefixLen   InetAddressPrefixLength,
  pcePcepPathKeyHopAddrUnnum     TeHopAddressUnnum,
  pcePcepPathKeyHopLspId         MplsLSPID,
  pcePcepPathKeyHopType          INTEGER,
}

pcePcepPathKeyHopListIndex OBJECT-TYPE
SYNTAX  MplsPathIndex
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The primary index into this table identifying a particular CPS. All hops in the CPS will have the same ListIndex. This corresponds to pcePcepPathKeyCPSIndex in pcePcepPathKeyEntry."
 ::= { pcePcepPathKeyHopEntry 1 }

pcePcepPathKeyHopIndex OBJECT-TYPE
SYNTAX  MplsPathIndex
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The secondary index into this table identifying a particular Hop."
 ::= { pcePcepPathKeyHopEntry 2 }

pcePcepPathKeyHopAddrType OBJECT-TYPE
SYNTAX TeHopAddressType
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The Hop Address Type of this CPS hop. Note that lspid(5) is a valid option only for tunnels signaled via CRLDP."
DEFVAL { ipv4 }
 ::= { pcePcepPathKeyHopEntry 2 }
pcePcepPathKeyHopIpAddr OBJECT-TYPE
SYNTAX TeHopAddress
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"The Hop Address for this CPS hop. The type of this address is determined by the value of the corresponding pcePcepPathKeyHopAddrType."
DEFVAL { '00000000'h } -- IPv4 address 0.0.0.0
 ::= { pcePcepPathKeyHopEntry 4 }

pcePcepPathKeyHopIpPrefixLen OBJECT-TYPE
SYNTAX InetAddressPrefixLength
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"If pcePcepPathKeyHopAddrType is set to ipv4(1) or ipv6(2), then this value will contain an appropriate prefix length for the IP address in object pcePcepPathKeyHopIpAddr. Otherwise this value is irrelevant and should be ignored."
DEFVAL { 32 }
 ::= { pcePcepPathKeyHopEntry 5 }

pcePcepPathKeyHopAddrUnnum OBJECT-TYPE
SYNTAX TeHopAddressUnnum
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"If pcePcepPathKeyHopAddrType is set to unnum(4), then this value will contain the interface identifier of the unnumbered interface for this hop. This object should be used in conjunction with pcePcepPathKeyHopIpAddr which would contain the LSR Router ID in this case."
 ::= { pcePcepPathKeyHopEntry 6 }
pcePcepPathKeyHopLspId OBJECT-TYPE
SYNTAX MplsLSPID
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"If pcePcepPathKeyHopAddrType is set to lspid(5), then this value will contain the LSPID of a tunnel of this hop. The present tunnel being configured is tunneled through this hop (using label stacking). This object is otherwise insignificant and should contain a value of 0 to indicate this fact."
::= { pcePcepPathKeyHopEntry 7 }

pcePcepPathKeyHopType OBJECT-TYPE
SYNTAX INTEGER {strict(1), loose(2)}
MAX-ACCESS read-only
STATUS mandatory
DESCRIPTION
"Denotes whether this hop is routed in a strict or loose fashion."
DEFVAL { strict }
::= { pcePcepPathKeyHopEntry 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 }

pcePcepPathKeyExpiredNoExpansionNtf 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,
                            pcePcepPathKeyNotificationsGroup
  }
  ::= { pcePcepPathKeyCompliances 2 }

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

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

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: dhruv.dhody@huawei.com

Udayasree Palle
Huawei Technology
Leela Palace
Bangalore, Karnataka  560008
INDIA

EMail: udayasree.palle@huawei.com
Quintin Zhao
Huawei Technology
125 Nagog Technology Park
Acton, MA 01719
US
EMail: quintin.zhao@huawei.com

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