Networking Working Group                              Rich Bradford (Ed)
Internet-Draft                                              JP Vasseur
                                                   Cisco Systems, Inc.
                                                        Adrian Farrel
                                                   Old Dog Consulting

Intended Status: Standards Track
Expires: Aug 23, 2008
                                                         Feb 23, 2008

**draft-bradford-ccamp-path-key-ero-01.txt**

# RSVP Extensions for Path Key Support

## Status of this Memo

Abstract

Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Traffic Engineering (TE) Label Switched Paths (LSPs) may be computed by Path Computation Elements (PCEs). Where the TE LSP crosses multiple domains, such as Autonomous Systems (ASes), the path may be computed by multiple PCEs that cooperate, with each responsible for computing a segment of the path. To preserve confidentiality of topology with each AS, the PCE supports a mechanism to hide the contents of a segment of a path, called the Confidential Path Segment (CPS), by encoding the contents as a Path Key Subobject (PKS). This document describes the addition of this information to Resource Reservation Protocol (RSVP) signaling by inclusion in the Explicit Route Object (ERO) and Record Route Object (RRO).

Table of contents



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 RFC-2119 [RFC2119].

## 1. Introduction

Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Traffic Engineering (TE) Label Switched Paths (LSPs) are signaled using the TE extensions to the Resource Reservation Protocol (RSVP-TE) [RFC3209], [RFC3473]. The routes followed by MPLS and GMPLS TE LSPs may be computed by Path Computation Elements (PCEs) [RFC4655].

Where the TE LSP crosses multiple domains, such as Autonomous Systems (ASes), the path may be computed by multiple PCEs that cooperate, with each responsible for computing a segment of the path. To preserve confidentiality of topology with each AS, the PCE Communications Protocol (PCEP) [PCEP] supports a mechanism to hide the contents of a segment of a path, called the Confidential Path Segment (CPS), by encoding the contents as a Path Key Subobject (PKS) [PCE-PKS].

This document defines RSVP-TE protocol extensions necessary to support the use of Path Key Segments in MPLS and GMPLS signaling.

## 2. Terminology

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.

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.

PKS: Path Key Subobject. A subobject of an Explicit Route Object which encodes a CPS, so as to preserve confidentiality.

## 3. RSVP-TE Path Key Subobject

The Path Key Subobject (PKS) may be carried in the Explicit Route Object (ERO) of a RSVP-TE Path message [RFC3209]. The PKS is a fixed-length subobject containing a Path-Key and a PCE-ID. The Path Key is an identifier, or token used to represent the CPS within the context of the PCE identified by the PCE-ID. The PCE-ID identifies the PCE that can decode the Path Key using a reachable IPv4 or IPv6 address of the PCE. In most cases, the decoding PCE is also the PCE that computed the Path Key and the associated path. Because of the IPv4 and IPv6 variants, two subobjects are defined as follows.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|    Type     |     Length    |           Path Key            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    PCE ID (4 bytes)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

L

The L bit SHOULD NOT be set, so that the subobject represents a strict hop in the explicit route.

Type

Subobject Type for a Path Key with 32-bit PCE ID as assigned by IANA.

Length

The Length contains the total length of the subobject in bytes, including the Type and Length fields. The Length is always 8.

PCE ID

A 32-bit identifier of the PCE that can decode this key. The identifier MUST be unique within the scope of the domain that the CPS crosses, and MUST be understood by the LSR that will act as PCC for the expansion of the PKS. The interpretation of the PCE-ID is subject to domain-local policy. It MAY be an IPv4 address of the PCE that is always reachable, and MAY be an address that is restricted to the domain in which the LSR that is called upon to expand the CPS lies. Other values that have no meaning outside the domain (for example, the Router ID of the PCE) MAY be used to increase security or confidentiality.

```
 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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |L|    Type     |     Length    |           Path Key            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                        PCE ID (16 bytes)                      |
 |                                                               |
 |                                                               |
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

L

As above.

Type

Subobject Type for a Path Key with 128-bit PCE ID as assigned by IANA.

Length

The Length contains the total length of the subobject in bytes, including the Type and Length fields. The Length is always 20.

PCE ID

A 128-bit identifier of the PCE that can decode this key. The identifier MUST be unique within the scope of the

domain that the CPS crosses, and MUST be understood by the LSR that will act as PCC for the expansion of the PKS. The interpretation of the PCE-ID is subject to domain-local policy. It MAY be an IPv6 address of the PCE that is always reachable, but MAY be an address that is restricted to the domain in which the LSR that is called upon to expand the CPS lies. Other values that have no meaning outside the domain (for example, the IPv6 TE Router ID) MAY be used to increase security (see Section 5).

Note: The twins of these sub-objects are carried in PCEP messages as defined in [PCE-PKS]. Ideally, IANA assignment of the subobject types will be identical.

### 3.1. Explicit Route Object Processing Rules

This section to be completed in a future release.

### 3.2. Reporting Path Key Segments in Record Route Objects

This section to be completed in a future release.

## 4. Security Considerations

- Confidentiality of the CPS (can other network elements probe for expansion of path-keys, possibly at random?).

- Authenticity of the path-key (resilience to alteration by intermediaries, resilience to fake expansion of path-keys).

- Resilience from DNS attacks (insertion of spurious path-keys; flooding of bogus path-key expansion requests).

Most of the interactions required by this extension are point to point, can be authenticated and made secure as described in [PCEP] and [RFC3209]. These interactions are listed in [PCE-PKS]

Thus, the major security issues can be dealt with using standard techniques for securing and authenticating point-to-point communications. In addition, it is recommended that the PCE providing a decode response should check that the LSR that issued the decode request is the head end of the decoded ERO segment.

Further protection can be provided by using a PCE ID to identify the decoding PCE that is only meaningful within the domain that contains the LSR at the head of the CPS. This may be an IP address that is only reachable from within the domain, or some not-address value. The former requires configuration of policy on the PCEs, the latter requires domain-wide policy.

# 5. Manageability Considerations

## 5.1. Control of Function Through Configuration and Policy

The treatment of a path segment as a CPS, and its substitution in a PCReq ERO with a PKS, is a function that SHOULD be under operator and policy control where a PCE supports the function. The operator SHOULD be given the ability to specify which path segments are to be replaced and under what circumstances. For example, an operator might set a policy that states that every path segment for the operator's domain will be replaced by a PKS when the PCReq has been issued from outside the domain.

# 6. IANA considerations

The IANA section will be detailed in further revision of this document.

It will include code point requests for the three new ERO sub-objects, and a new ErrorSpec Error Code.

Note: The twins of these sub-objects are be carried in PCEP messages as defined in [PCE-PKS]. Ideally, IANA assignment of the subobject types will be identical.

# 7. References

## 7.1. Normative References

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

[PCEP] Vasseur, J.P., Le Roux, J.L., Ayyangar, A., Oki, E., Ikejiri, A., Atlas, A., Dolganow, A., "Path Computation Element (PCE) communication Protocol (PCEP)", draft-ietf-pce-pcep, work in progress.

## 7.2. Informational References

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V. and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3473] Berger, L., et al. "GMPLS Singlaling RSVP-TE extensions", RFC3473, January 2003.

[PCE-PKS] Bradford, R., Vasseur, J.P., Farrel, A., "Preserving Topology Confidentiality in Inter-Domain Path Computation Using a Key-Based Mechanism", draft-ietf-pce-path-key, work in progress.

[RFC4655] Farrel, A., Vasseur, J.P., Ash, J., "Path Computation Element (PCE) Architecture", RFC 4655, August 2006.

# 8. Authors' Addresses:

Rich Bradford (Editor)
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA - 01719
USA
Email: rbradfor@cisco.com

J.-P Vasseur
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA - 01719
USA
Email: jpv@cisco.com

Adrian Farrel
Old Dog Consulting
EMail: adrian@olddog.co.uk

## Full Copyright Statement



## Intellectual Property