

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: August 17, 2014

A. Ripke
T. Dietz
J. Quittek
NEC
R. da Silva
Telefonica I+D
February 13, 2014

PCP Tunnel-ID Option
draft-ripke-pcp-tunnel-id-option-00

Abstract

This document describes a new Port Control Protocol (PCP) option called TUNNEL_ID. It serves for identifying a Third Party in addition to the means that PCP's THIRD_PARTY option already provides for that purpose.

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 August 17, 2014.

Copyright Notice

Copyright (c) 2014 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.

Table of Contents

1. Introduction	2
2. Terminology	3
3. Target Scenario	3
4. Format	4
5. Behavior	5
5.1. Generating a Request	5
5.2. Processing a Request	6
5.3. Processing a Response	6
6. Alternative	6
7. IANA Considerations	6
8. Security Considerations	6
9. References	7
9.1. Normative References	7
9.2. Informative References	7
Authors' Addresses	7

1. Introduction

The IETF has specified the Port Control Protocol (PCP) ([RFC6887]) to control how packets are translated and forwarded by a PCP-controlled device such as a network address translator (NAT) or firewall.

This draft focuses on the application of PCP's THIRD_PARTY option that is used when the PCP client sends requests that concern other internal hosts than the host of the PCP client. This is, for example, the case if port mapping requests for a carrier grade NAT (CGN) are not sent from PCP clients at the subscribers, but from a portal of the carrier at which subscribers can request port mappings.

The issue addressed by the TUNNEL_ID option is that there are CGN deployments that do not distinguish internal hosts by their IP address only, but use further identifiers for unique subscriber identification. This is, for example, the case if a CGN supports overlapping private IP address spaces according to [RFC1918] for internal hosts of different subscribers. Then different internal hosts are identified and mapped at the CGN by their IP address and an additional ID, for example, the ID of a tunnel between the CGN and the subscriber. In such cases, the IP address contained in the THIRD_PARTY option is not sufficient. An additional identifier needs to be carried by the PCP protocol in order to uniquely identify the Internal Host. The TUNNEL_ID option serves this purpose.

The TUNNEL_ID option is defined for use in combination with the THIRD_PARTY option for the PCP opcodes MAP and PEER.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

The terminology defined in the specification of PCP [RFC6887] applies.

3. Target Scenario

This section illustrates the use of the TUNNEL_ID option in a scenario for a port mapping requests via a carrier portal.

The scenario shown in Figure 1 has a carrier operating a CGN and a portal for subscribers to request port mappings at the CGN. The portal communicates with the CGN using PCP. For this purpose the portal is co-located with a PCP client and the CGN is co-located with a PCP server. The way subscribers interact with the portal for requesting port mapping for their internal hosts is not specified in this scenario.

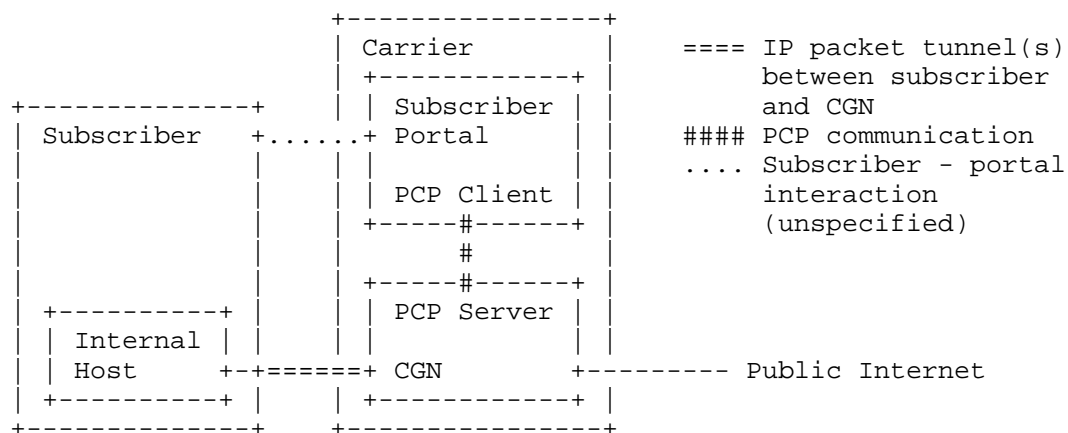


Figure 1: Carrier portal for port mapping requests

The internal hosts use private IP addresses as specified in [RFC1918]. Since there is no NAT between the internal host and the CGN, there is an overlap of addresses used by internal hosts at different subscribers. That is why the CGN needs more than just the

internal host's IP address to distinguish internal hosts at different subscribers. A commonly deployed method for solving this issue is using an additional identifiers for this purpose. A very good candidate for this additional identifier at the CGN is the ID of the tunnel that connects the CGN to the subscriber's network.

Requests for port mappings from the portal to the CGN need to uniquely identify the internal host for which a port mapping is to be established or modified. Already existing for this purpose is the THIRD_PARTY option that can be used to specify the internal host's IP address. The TUNNEL_ID option is introduced for carrying the additional (tunnel) information needed to identify the internal host in this scenario.

The additional identifier for internal hosts needs to be included in MAP requests from the PCP client in order to uniquely identify the internal host that should have its address mapped. This is the purpose that the new TUNNEL_ID serves in this scenario. It carries the additional identifier, that is the tunnel ID, that serves for identifying an internal host in combination with the internal host's (private) IP address. The IP address of the internal host is included in the PCP client's mapping requests by using the THIRD_PARTY option.

The information carried by the TUNNEL_ID is not just needed to identify an internal host in a PCP request. The CGN needs this information in its internal mapping tables for translating packet addresses and for forwarding packets to subscriber-specific tunnels.

4. Format

The TUNNEL_ID option is formatted as shown in Figure 2.

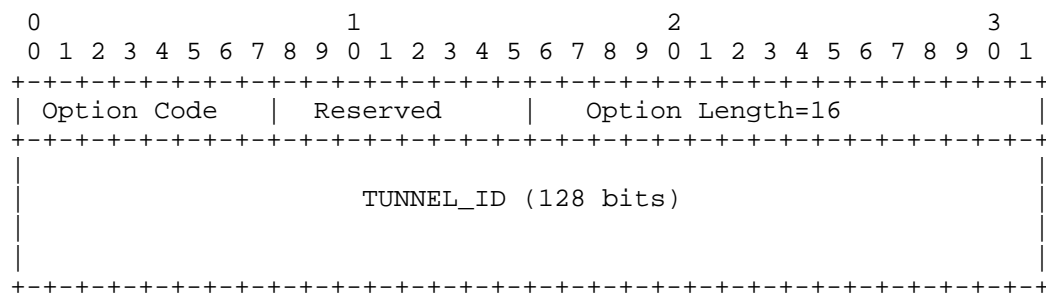


Figure 2: TUNNEL_ID Option

- o Option Name: TUNNEL_ID

- o Number: TBD
- o Purpose: Identifies a request of an external IP address and port.
- o Valid for opcodes: MAP, PEER, and all other for which the THIRD_PARTY option is valid for.
- o Length: 16 octets
- o May appear in: Request. Must appear in response if it appeared in the associated request.
- o Maximum occurrences: 1

The fields are as follows:

- o TUNNEL_ID: A vendor specific tunnel identifier that can be used to identify a subscriber's CGN session and the port ranges to apply this request to.

The tunnel identifier field can contain any vendor specific value to identify a tunnel. The option number is in the mandatory-to-process range (0-127), meaning that a request with a TUNNEL_ID option is executed by the PCP server if and only if the TUNNEL_ID option is supported by the PCP server.

5. Behavior

The following sections describe the operations of a PCP client and a PCP server when generating the request and processing the request and response.

5.1. Generating a Request

In addition to generating a PCP request that is described in [RFC6887] the following has to be applied. The TUNNEL_ID option can be used together either with a PCP MAP or PEER opcode. It MUST be used in combination with the THIRD_PARTY option which provides an IP address and port entered by the subscriber. The TUNNEL_ID option holds the respective tunnel identifier to allow the CGN to uniquely identify the internal host (specified in the THIRD_PARTY option) for which the port mapping is to be established or modified. If the tunnel identifier is shorter than 128 bits then the TUNNEL_ID option field is to be filled up with leading zeros up to 128 bits.

5.2. Processing a Request

The TUNNEL_ID option is in the mandatory-to-process range and if the PCP server does not support this option it MUST return an UNSUPP_OPTION response. If the provided TUNNEL_ID is unknown/unavailable the PCP server MUST return a TUNNEL_ID_UNKNOWN response.

5.3. Processing a Response

If the PCP client receives a TUNNEL_ID_UNKNOWN response back for its previous request it SHOULD report an error message. To where to report an error message is implementation dependent.

6. Alternative

An alternative to identify a tunnel affiliation in the given scenario could be using the DESCRIPTION ([I-D.ietf-pcp-description-option]) option to carry a tunnel ID option. The DESCRIPTION option is to allow a text description to be attached to a port mapping. But using the DESCRIPTION option for a tunnel ID might not be appropriate because it specifies using UTF-8 and another requirement is that the description text must not be null terminated, which cannot always be met.

7. IANA Considerations

The following PCP Option Code is to be allocated in the mandatory-to-process range:

TUNNEL_ID

[NOTE for IANA: Please allocate a PCP Option Code at <http://www.iana.org/assignments/pcp-parameters/pcp-parameters.xml#option-rules>]

The following PCP Result Code is to be allocated:

TUNNEL_ID_UNKNOWN

[NOTE for IANA: Please allocate a PCP Result Code at <http://www.iana.org/assignments/pcp-parameters/pcp-parameters.xml#result-codes>]

8. Security Considerations

As this option is related to the use of the THIRD_PARTY option the corresponding security considerations apply. Especially, the network on which the PCP messages are sent must be fully trusted.

9. References

9.1. Normative References

- [RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, April 2013.

9.2. Informative References

- [I-D.ietf-pcp-description-option]
Boucadair, M., Penno, R., and D. Wing, "PCP Description Option", draft-ietf-pcp-description-option-04 (work in progress), February 2014.

Authors' Addresses

Andreas Ripke
NEC
Heidelberg
Germany

Email: ripke@neclab.eu

Thomas Dietz
NEC
Heidelberg
Germany

Email: dietz@neclab.eu

Juergen Quittek
NEC
Heidelberg
Germany

Email: quittek@neclab.eu

Rafael Lopez da Silva
Telefonica I+D
Madrid
Spain

Email: ralds@tid.es