

PCP Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 29, 2013

M. Boucadair
France Telecom
T. Reddy
P. Patil
D. Wing
Cisco
May 28, 2013

Using PCP to Reveal a Host behind NAT
draft-boucadair-pcp-nat-reveal-01

Abstract

This document describes how to use PCP to retrieve the identity of a host behind a NAT. Two use cases are discussed and the PCP applicability is analyzed. This document extends PCP with a new OpCode called QUERY Opcode.

The proposed mechanism is valid for all NAT flavors including NAT44, NAT64 or NPTv6.

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 November 29, 2013.

Copyright Notice

Copyright (c) 2013 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.	Requirements Language and Terminology	3
3.	Problem Space	3
3.1.	Policy and Charging Control Architecture	3
3.2.	NAT between the PCEF and AF	4
3.3.	NAT before PCEF	5
4.	PCP Applicability	6
4.1.	NAT between the PCEF and AF	6
4.2.	NAT before PCEF	7
5.	QUERY OpCode	9
5.1.	QUERY Request Format	9
5.2.	QUERY Response Format	10
5.3.	Generating a QUERY Request	11
5.4.	Processing a QUERY Request	12
5.5.	Processing a QUERY Response	13
6.	Applicability Scope of QUERY OpCode	13
7.	IANA Considerations	13
8.	Security Considerations	13
9.	References	14
9.1.	Normative References	14
9.2.	Informative References	14
	Authors' Addresses	15

[1.](#) Introduction

As reported in [\[RFC6269\]](#), several issues are encountered when an IP address is shared among several subscribers. These issues are encountered in various deployment contexts: e.g., Carrier Grade NAT (CGN), application proxies or A+P [\[RFC6346\]](#).

This document extends Port Control Protocol [\[RFC6887\]](#) to identify a host among those sharing the same IP address in certain scenarios.

The proposed technique can be used independently or combined with the host identifier, denoted as HOST_ID defined in [\[I-D.ietf-intarea-nat-reveal-analysis\]](#).

Additional scenarios requiring host identification are listed in [\[I-D.boucadair-intarea-host-identifier-scenarios\]](#).

2. Requirements Language and Terminology

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 [\[RFC2119\]](#).

This note uses terminology defined in [\[RFC6887\]](#).

3. Problem Space

3.1. Policy and Charging Control Architecture

Figure 1 depicts a reference architecture of a mobile network [\[RFC6342\]](#).

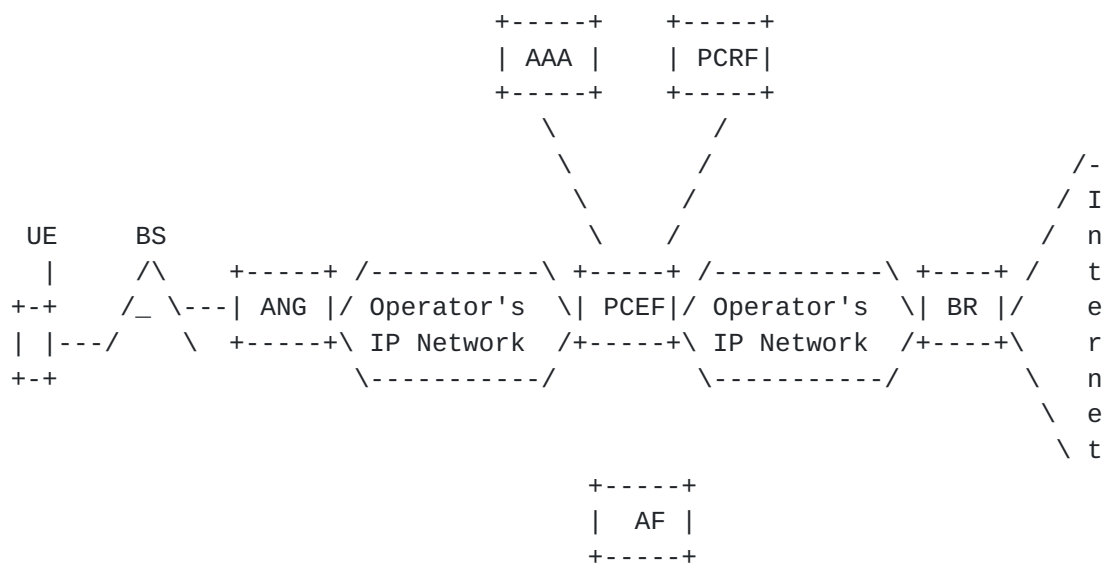


Figure 1: Mobile Network Architecture

The main involved functional elements are:

- o UE (User Equipment) is a mobile node.
- o Policy and Charging Rule Function (PCRF) which is responsible for determining which policy and charging control rules are to be applied [\[TS.23203\]](#).
- o Policy and Charging Enforcement Function (PCEF) which performs policy enforcement (e.g., Quality of Service (QoS)) and flow-based charging [\[TS.23203\]](#).
- o Application Function (AF) is an element offering applications that require dynamic policy and/or charging control [\[TS.23203\]](#).

- o Access Network Gateway (ANG), Base Station (BS) and Border Router (BR) are defined in [RFC6342].

[Section 3.2](#) and [Section 3.3](#) explain the encountered problems to identify individual UEs when a NAT is involved in the data path. The use of PCP to solve those problems is analyzed in [Section 4](#).

[3.2.](#) NAT between the PCEF and AF

Figure 2 shows a scenario where a NAT function is located between the PCEF and AF.

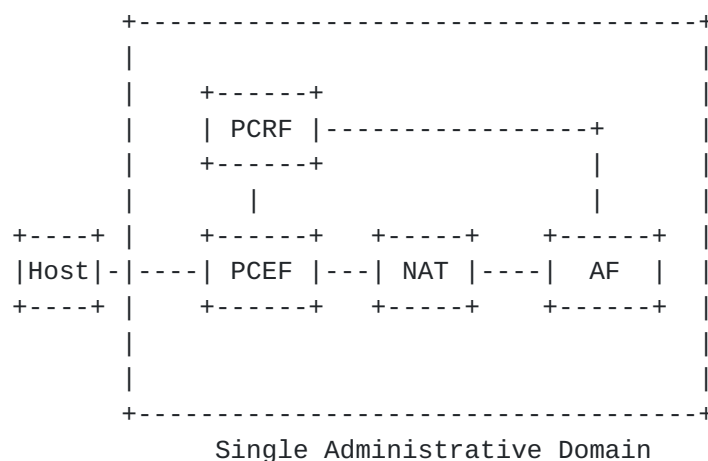


Figure 2: NAT between PCEF and AF

The main issue in this case is that PCEF, PCRF and AF all receive information bound to the same UE but cannot correlate between the piece of data visible for each entity. Concretely,

- o PCEF is aware of the IMSI (International Mobile Subscriber Identity) and an internal IP address assigned to the UE.
- o AF receives an external IP address and port as assigned by the NAT function.
- o PCRF is not able to correlate between the external IP address/port assigned by the NAT and the internal IP address and IMSI of the UE. For instance, the offered QoS on internal IPv4 address and the (shared) external IPv4 address may need to be correlated for accounting purposes.
- o The IP address seen by the AF is shared among multiple UEs using NAT, the PCRF needs to be able to inspect the NAT binding to disambiguate among the individual UEs. AF will not be able to treat UE traffic based on policy provided by PCRF.

This scenario can be generalized as follows (Figure 3):

- o Policy Enforcement Point (PEP, [[RFC2753](#)])
- o Policy Decision Point (PDP, [[RFC2753](#)])

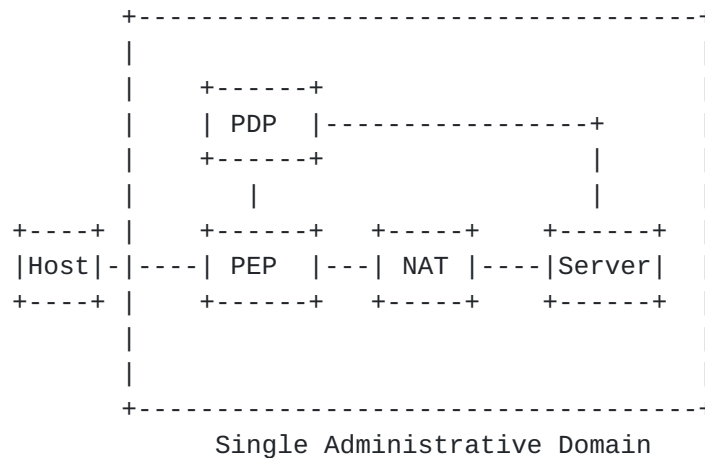


Figure 3: NAT between PEP and Server

3.3. NAT before PCEF

Figure 4 shows an alternative scenario in which a NAT function is located before PCEF. The main issue is that PCEF and AF are only aware of the external IP address and the external port number assigned by the NAT function. PCEF/AF will fail to identify each UE behind NAT since multiple UEs share the same external IP address and thus are unable to treat incoming connections differently.

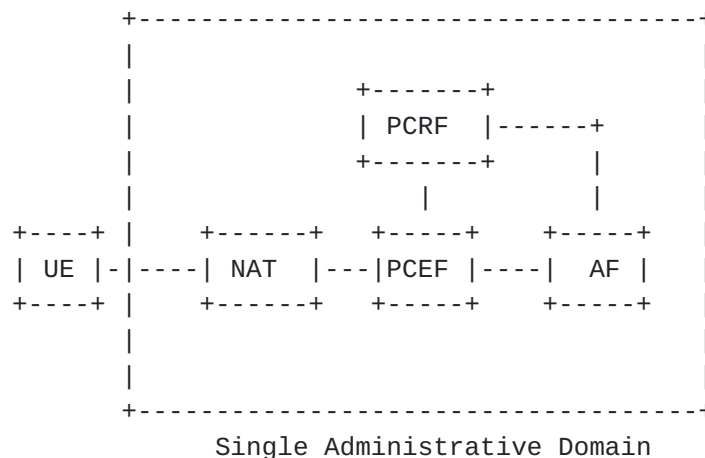
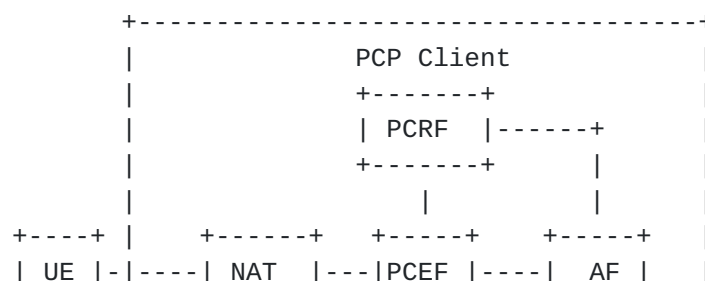


Figure 4: NAT before PCEF

This scenario can be generalized as follows (Figure 5):



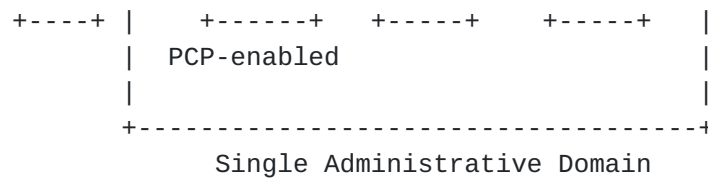
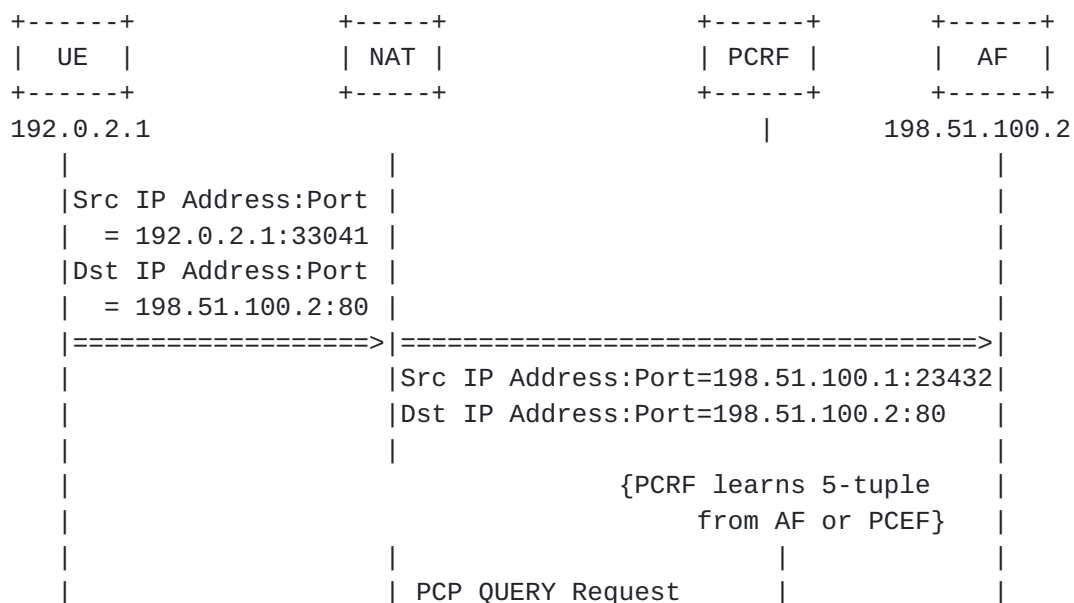


Figure 7: NAT before PCEF

The updated interaction between PCRF, PCEF and AF is detailed below:

- o The PCP server controlling the NAT is configured to accept QUERY requests [Section 5](#) from authorized PCP clients such as PCRF. Query requests must not be received in the Internet-facing interface but from an internal interface (e.g., dedicated management interface).
- o PCRF generates a PCP QUERY request with External IP Address, External Port, Remote Peer IP address, Remote Peer Port and Protocol fields for the flow learnt from PCEF or AF.
- o PCRF learns the internal IP address and internal port number in the QUERY response. This correlation is used by the PCRF to retrieve the UE's policy to be passed to the PCEF.

Figure 8 shows an example of the use of QUERY OpCode. In this example, an HTTP connection is initiated by the UA (192.0.2.1:33041) to an HTTP server (198.51.100.2:80). The NAT assigns 198.51.100.1/23432 as external IP Address/Port. PCRF learns Internal IP Address and Port associated with the NAT mapping using PCP QUERY request/response.




```

|                                     | External IP:Port = |                                     |
|                                     | 198.51.100.1:23432 |                                     |
|                                     | Remote Peer IP:Port = |                                     |
|                                     | 198.51.100.2:80    |                                     |
|                                     | Protocol = TCP      |                                     |
|                                     | <=====            |                                     |
|                                     | PCP QUERY Response  |                                     |
|                                     | External IP:Port =  |                                     |
|                                     | 198.51.100.1:23432 |                                     |
|                                     | Internal IP:Port =  |                                     |
|                                     | 192.0.2.1:33041    |                                     |
|                                     | Protocol = TCP      |                                     |
|                                     | Lifetime = 1000 sec |                                     |
|                                     | =====>          |                                     |
|                                     |                                     |                                     |
|                                     | Generate Policy Rules |                                     |

```

Figure 8: Usage Example

5. QUERY OpCode

This section defines a new PCP OpCode which can be used to query PCP-aware NAT to retrieve the Internal IP Address and Internal Port of a given mapping.

The PCP Server MUST provide a configuration option to allow administrators to enable/disable QUERY OpCode.

5.1. QUERY Request Format

The following diagram shows the format of the OpCode-specific information in a request for the QUERY OpCode.

```

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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
|                                     QUERY Nonce (96 bits)                                     |
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Protocol | Reserved (24 bits) |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| External Port | Remote Peer Port |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
|                                     External IP Address (128 bits)                                     |
|
|
|

```

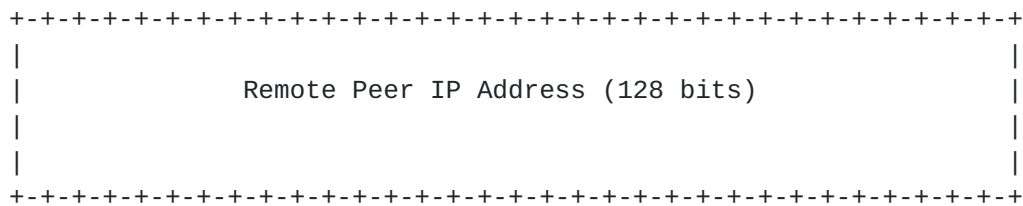



Figure 9: Query Opcode Request

These fields are described below:

Requested Lifetime (in common header): This field is positioned to 0.

Mapping Nonce: Random value chosen by the PCP client. See [Section 12.2 of \[RFC6887\]](#)

Protocol: Upper-layer protocol associated with this OpCode. Values are taken from the IANA protocol registry [[proto_numbers](#)]. For example, this field contains 6 (TCP) if the OpCode is describing a TCP mapping. Protocol MUST NOT be zero.

Reserved: 24 reserved bits, MUST be set to 0 on transmission and MUST be ignored on reception.

External Port: External port allocated by NAT for the flow. External Port MUST NOT be zero

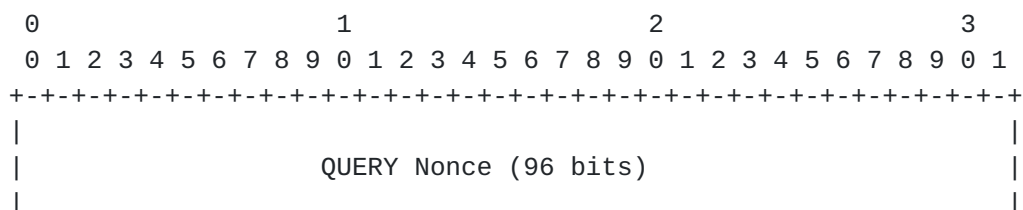
Remote Peer Port: Remote peer's port for the flow. Remote Peer Port MUST NOT be zero

External IP address: External IP address allocated by NAT for the flow. External IP address MUST NOT be zero

Remote Peer IP address: Remote peer IP address for the flow. Remote Peer IP address MUST NOT be zero.

5.2. QUERY Response Format

The following diagram shows the format of OpCode-specific information in a response packet for the QUERY OpCode:



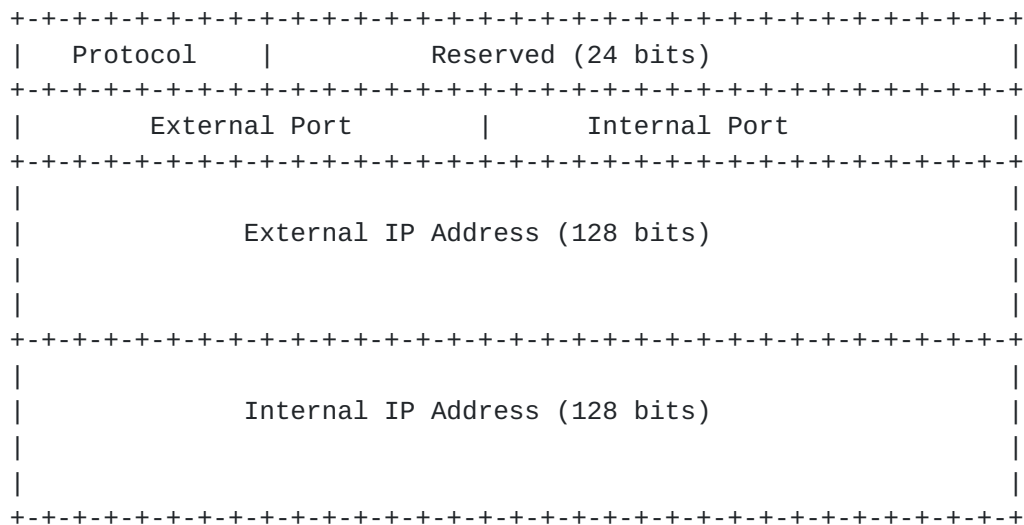


Figure 10: Query Opcode Response

These fields are described below:

Lifetime (in common header): On a success response, this indicates the lifetime for this mapping, in seconds. On an error response, this indicates that mapping does not exist.

Mapping Nonce: Copied from the request.

Protocol: Copied from the request.

Reserved: 24 reserved bits, MUST be set to 0.

External Port: Copied from the request.

External IP address: Copied from the request.

Internal Port: Internal Port as assigned by the PCP-controlled device.

Internal IP address: Internal IP address as assigned by the PCP-controlled device.

5.3. Generating a QUERY Request

This section describes the operation of a PCP client when sending requests with the QUERY OpCode.

PCP QUERY request is used by an authorized third party PCP client that is only aware of the 5-tuple {External IP address and Port, Protocol, Remote Peer IP address and Port} and needs to learn the Internal IP address and Port associated with the NAT mapping. The request MUST contain non-zero values of Protocol, External Port, Remote Peer Port, External IP address and Remote Peer IP address. The Requested Lifetime MUST be set to zero.

5.4. Processing a QUERY Request

This section describes the operation of a PCP server when processing a QUERY request.

For EIM/EIF port-mapping NAT, the processing of the QUERY request is as follows:

- o If any of the values Protocol, External Port and External IP address are equal to zero, the request is invalid and the PCP server MUST return a MALFORMED_REQUEST to the client.
- o If Protocol, External Port and External IP address do not match any existing implicit dynamic mapping, then the PCP server MUST return NONEXIST_MAP error response (also needed in [[I-D.boucadair-pcp-failure](#)]).
- o If Protocol, External Port and External IP address match an existing implicit dynamic mapping, then the PCP server MUST build a QUERY response with the Internal IP address, Internal Port and the lifetime associated with the mapping.

For EDM port-mapping NAT, the processing of the QUERY request is as follows:

- o If any of the values Protocol, External Port, Remote Peer Port, External IP address and Remote Peer IP Address are zero, the request is invalid and PCP server MUST return a MALFORMED_REQUEST to the client.
- o If Protocol, External Port, Remote Peer Port, External IP address and Remote Peer IP address do not match any existing implicit dynamic mapping then the PCP server MUST return NONEXIST_MAP error response (also needed in [[I-D.boucadair-pcp-failure](#)]).
- o If Protocol, External Port, Remote Peer Port, External IP address and Remote Peer IP address matches an existing implicit dynamic mapping then the PCP server builds a QUERY response with the Internal IP address, Internal Port and the lifetime associated with the mapping.

PCP QUERY requests received on the Internet-facing interface MUST be silently dropped.

In DS-Lite context [[RFC6333](#)], the Internal IP address returned in the QUERY response MUST be the IPv6 address of the remote tunnel endpoint and not the internal private IPv4 address.

5.5. Processing a QUERY Response

After performing common PCP response processing by the PCP Client, the response is further matched with a previously-sent QUERY request by comparing the QUERY Nonce, External IP Address, External Port and Protocol. On a SUCCESS response, the PCP Client can use the Internal IP Address and Port in the QUERY response as needed.

6. Applicability Scope of QUERY OpCode

The PCP-Reveal solution is designed for needs within one single administrative domain (i.e., the PCP Client and PCP Server are managed by the same entity). Considerations related to the activation of the PCP-Reveal solution in an inter-domain context is out of scope of this document.

7. IANA Considerations

Authors of this document request IANA to assign the following OpCode:

- o QUERY

The following error code is requested:

- o NONEXIST_MAP

8. Security Considerations

Security considerations discussed in [[RFC6887](#)] are to be taken into account. In particular, QUERY OpCode MUST NOT be implemented or used unless the network on which the PCP QUERY messages are to be sent is fully trusted. For example if Access Control Lists (ACLs) are installed on the PCP server, and the network between the PCP client and the PCP server, so those ACLs allow only communications from a trusted PCP client to the PCP server.

QUERY OpCode may be generated by non legitimate PCP Clients; the PCP Server MUST enforce some policies such as rate limit QUERY messages. QUERY requests received from non legitimate PCP Clients are silently dropped.

PCP authentication [[I-D.ietf-pcp-authentication](#)] MAY be used.

9. References

9.1. Normative References

- [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.
- [proto_numbers] IANA, , "Protocol Numbers", 2010, <<http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml>>.

9.2. Informative References

- [I-D.boucadair-intarea-host-identifier-scenarios] Boucadair, M., Binet, D., Durel, S., Chatras, B., Reddy, T., and B. Williams, "Host Identification: Use Cases", [draft-boucadair-intarea-host-identifier-scenarios-03](#) (work in progress), March 2013.
- [I-D.boucadair-pcp-failure] Boucadair, M. and R. Penno, "Analysis of Port Control Protocol (PCP) Failure Scenarios", [draft-boucadair-pcp-failure-06](#) (work in progress), May 2013.
- [I-D.ietf-intarea-nat-reveal-analysis] Boucadair, M., Touch, J., Levis, P., and R. Penno, "Analysis of Solution Candidates to Reveal a Host Identifier (HOST_ID) in Shared Address Deployments", [draft-ietf-intarea-nat-reveal-analysis-10](#) (work in progress), April 2013.
- [I-D.ietf-pcp-authentication] Wasserman, M., Hartman, S., and D. Zhang, "Port Control Protocol (PCP) Authentication Mechanism", [draft-ietf-pcp-authentication-01](#) (work in progress), October 2012.
- [RFC2753] Yavatkar, R., Pendarakis, D., and R. Guerin, "A Framework for Policy-based Admission Control", [RFC 2753](#), January 2000.

- [RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", [RFC 6269](#), June 2011.
- [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", [RFC 6333](#), August 2011.
- [RFC6342] Koodli, R., "Mobile Networks Considerations for IPv6 Deployment", [RFC 6342](#), August 2011.
- [RFC6346] Bush, R., "The Address plus Port (A+P) Approach to the IPv4 Address Shortage", [RFC 6346](#), August 2011.
- [TS.23203] 3GPP, , "Policy and charging control architecture", September 2012.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tiredddy@cisco.com

Prashanth Patil
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marthalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: praspati@cisco.com

Dan Wing
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134
USA

Email: dwing@cisco.com