PCP
Internet-Draft
Intended status: Standards Track
Expires: August 20, 2013

S. Kiesel
University of Stuttgart
R. Penno
Cisco Systems

February 16, 2013

PCP Server Discovery based on well-known IP Address
draft-kiesel-pcp-ip-based-srv-disc-00

Abstract

The Port Control Protocol (PCP) provides a mechanism to control how incoming packets are forwarded by upstream devices such as Network Address Translator IPv6/IPv4 (NAT64), Network Address Translator IPv4/IPv4 (NAT44), IPv6 and IPv4 firewall devices, and a mechanism to reduce application keep alive traffic.

This document establishes a well-known IP address for the PCP Server and documents how PCP clients embedded in endpoints can use it during the discovery and regular operation phases.

Requirements Language

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].

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 20, 2013.

Copyright Notice

Table of Contents

1. Introduction

The Port Control Protocol (PCP) [I-D.ietf-pcp-base] provides a mechanism to control how incoming packets are forwarded by upstream devices such as Network Address Translator IPv6/IPv4 (NAT64), Network Address Translator IPv4/IPv4 (NAT44), IPv6 and IPv4 firewall devices, and a mechanism to reduce application keep alive traffic.

But before a PCP client can perform any of these tasks it needs to discover one or more PCP servers. Several algorithms have been specified that produce a suitable PCP Server address given PCP client (i.e., the address may vary for different clients or different points of network attachment, etc.). These approaches are based on user input, DHCP [I-D.ietf-pcp-dhcp] or default router, which is the one detailed in the PCP base document [I-D.ietf-pcp-base].

But unfortunately in many deployments, the first-hop router does not run a PCP server, or DHCP cannot be used. These and other problems are described in detail in the Appendix.Appendix A.

This document follows a different approach: it establishes a well-known address for the PCP Server (TBD: this approach could easily be generalized in order to discover other services as well. But this is for further study). PCP clients are expected to send requests to this address during the PCP Server discovery process. A PCP Server configured with the anycast address could optionally redirect or return a list of unicast PCP Servers to the client.

2. PCP Server Discovery based on well-known IP Address

2.1. Well-Known PCP Server IP Address (WkPsdIPa)

IANA is requested to register a single IPv4 address 192.0.0.X (TBD) and a single IPv6 address 2001::XXXX (TBD) within the respective Special Purpose Address Registries as the well-known IP anycast addresses for PCP Servers. These addresses are called WkPsdIPa (well-known PCP server discovery IP address(es)) in this document.

2.2. PCP Discovery Client behavior

PCP Clients that need to discover PCP servers should first send a PCP request to its default router. This is important because in the case of cascaded PCP Servers, all of them need to be discovered in order of hop distance from the client. The PCP client then SHOULD send a PCP request to the WkPsdIPa. PCP Clients must be prepared to receive an error and try other discovery methods.

2.3. PCP Discovery Server behavior

PCP Server can be configured to listen on the WkPsdIPa for incoming PCP requests.

PCP responses are sent from that same IANA-assigned address (see Page 5 of [RFC1546]).

3. Deployment Considerations

Network operators should install one or more PCP Servers as specified above. Depending on the network deployment scenario they may use IP routing tables, or other suitable mechanisms to direct PCP requests to one of these servers.

[TBD: explain in more detail] This works fine even with cascaded access routers with NATs. After each router hop the operator may decide whether to handle the discovery requests, e.g., using a static routing table entry, or whether let them flow "automatically" towards the Internet backbones using the default routing table entry.

3.1. Multiple PCP Servers, Symmetric Routing

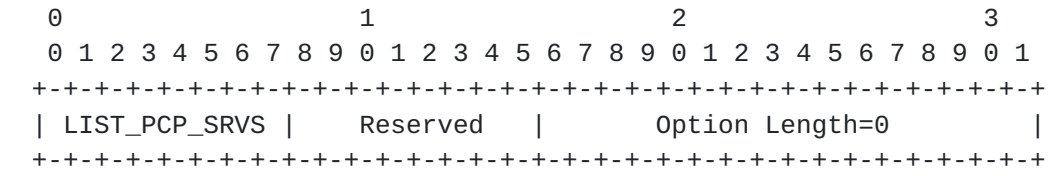
In the case of symmetric routing all inbound and outbound packets from a PCP client traverse the same PCP Server or controlled device. Multiple PCP Servers sharing an anycast address in a symmetric routing scenario are used for two purposes: ease of network configuration and redundancy. In the case of redundancy, If there is a network or routing change a PCP client might start interacting with a different PCP Server sharing the same anycast address. From a PCP Client point of view this would be the same as a PCP Server reboot and a PCP Client could find out about it by examining the Epoch field during the next PCP request or ANNOUNCE message.

3.2. Multiple PCP Servers, Assymetric Routing

In the case of asymmetric routing inbound packets from a PCP client traverse a different PCP Server or controlled device than outbound packets. If these PCP Servers are firewalls, the PCP client would need to create mappings on both of them in order to properly communicate with other hosts. But if these PCP Servers share an anycast address the PCP Client will create mappings in only on, when in fact should create mapping on both of them.

Therefore in order to support this scenario we propose a new option for the ANNOUNCE opcode. This will allow a PCP Client to request from a PCP Server a list of unicast IP addresses associated with other PCP Servers. The client can then proceed to create mappings on these PCP Servers using their unicast addresses.

This Option:
Option Name: LIST_PCP_SRVS
Number: TBA (IANA)
Purpose: Allows a PCP Client to request from a PCP Server a list of all PCP Servers configured
Valid for Opcodes: ANNOUNCE
Length: 0x0
May appear in: request and reply
Maximum occurrences in request: 1



The Reply from the PCP Server would be a list of IP addresses

Length in reply: 128 bits * number of IP addresses
Maximum occurrences in reply: as many as fit within maximum PCP message size

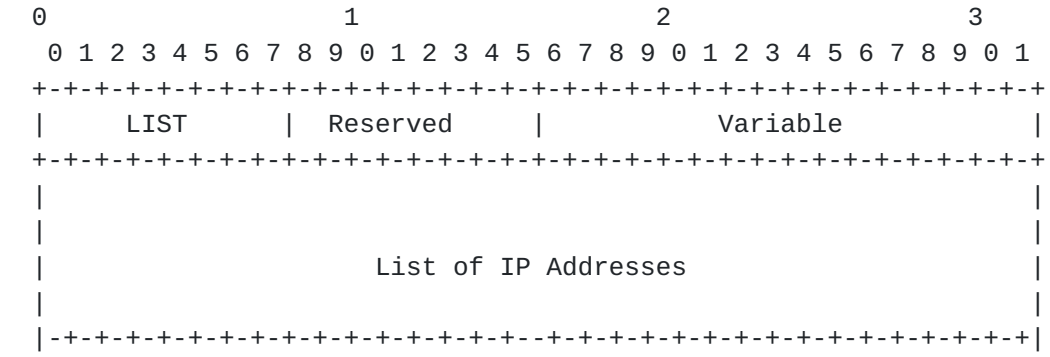


Figure 1: List of PCP Servers

4. IANA Considerations

4.1. Registration of IPv4 Special Purpose Address

IANA is requested to register a single IPv4 address in the IANA IPv4 Special Purpose Address Registry [RFC5736].

[RFC5736] itemizes some information to be recorded for all designations:

1. The designated address prefix.

Prefix: TBD by IANA. Prefix length: /32

2. The RFC that called for the IANA address designation.

This document.

3. The date the designation was made.

TBD.

4. The date the use designation is to be terminated (if specified as a limited-use designation).

Unlimited. No termination date.

5. The nature of the purpose of the designated address (e.g., unicast experiment or protocol service anycast).

protocol service anycast.

6. For experimental unicast applications and otherwise as appropriate, the registry will also identify the entity and related contact details to whom the address designation has been made.

N/A.

7. The registry will also note, for each designation, the intended routing scope of the address, indicating whether the address is intended to be routable only in scoped, local, or private contexts, or whether the address prefix is intended to be routed globally.

Typically used within a network operator's network domain, but in principle globally routable.

8. The date in the IANA registry is the date of the IANA action, i.e., the day IANA records the allocation.

TBD.

4.2. Registration of IPv6 Special Purpose Address

IANA is requested to register a single IPv6 address in the IANA IPv6 Special Purpose Address Block [RFC4773].

[RFC4773] itemizes some information to be recorded for all designations:

1. The designated address prefix.

Prefix: TBD by IANA. Prefix length: /128

2. The RFC that called for the IANA address designation.

This document.

3. The date the designation was made.

TBD.

4. The date the use designation is to be terminated (if specified as a limited-use designation).

Unlimited. No termination date.

5. The nature of the purpose of the designated address (e.g., unicast experiment or protocol service anycast).

protocol service anycast.

6. For experimental unicast applications and otherwise as appropriate, the registry will also identify the entity and related contact details to whom the address designation has been made.

N/A.

7. The registry will also note, for each designation, the intended routing scope of the address, indicating whether the address is intended to be routable only in scoped, local, or private contexts, or whether the address prefix is intended to be routed globally.

Typically used within a network operator's network domain, but in principle globally routable.

8. The date in the IANA registry is the date of the IANA action, i.e., the day IANA records the allocation.

TBD.

4.3. PCP Option

The following PCP Option should be allocated:

LIST_PCP_SRVS

5. Security Considerations

TBD

6. Acknowledgements

Ted Lemon for insightful DHCP discussions and Dave Thaler for pointing out the asymmetric routing case.

7. References

7.1. Normative References

[RFC1546] Partridge, C., Mendez, T., and W. Milliken, "Host Anycasting Service", RFC 1546, November 1993.

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

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2732] Hinden, R., Carpenter, B., and L. Masinter, "Format for Literal IPv6 Addresses in URL's", RFC 2732, December 1999.

[RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, January 2005.

[RFC4773] Huston, G., "Administration of the IANA Special Purpose IPv6 Address Block", RFC 4773, December 2006.

[RFC5736] Huston, G., Cotton, M., and L. Vegoda, "IANA IPv4 Special Purpose Address Registry", RFC 5736, January 2010.

7.2. Informative References

[DhcpRequestParams]
OpenFlow, "OpenFlow Switch Specification", February 2011, <http://msdn.microsoft.com/en-us/library/windows/desktop/aa363298%28v=vs.85%29.aspx>.

[I-D.chen-pcp-mobile-deployment]
Chen, G., Cao, Z., Boucadair, M., Ales, V., and L. Thiebaut, "Analysis of Port Control Protocol in Mobile Network", draft-chen-pcp-mobile-deployment-02 (work in progress), October 2012.

[I-D.ietf-dhc-container-opt]
Droms, R. and R. Penno, "Container Option for Server Configuration", draft-ietf-dhc-container-opt-06 (work in progress), December 2012.

[I-D.ietf-pcp-base]
Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)",

draft-ietf-pcp-base-29 (work in progress), November 2012.

[I-D.ietf-pcp-dhcp]
Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", draft-ietf-pcp-dhcp-05 (work in progress), September 2012.

Appendix A. Problems with Other Discovery methods

Several algorithms have been specified that allows PCP Client to discover the PCP Servers on a network . However, each of this approaches has technical or operational issues that will hinder the fast deployment of PCP.

A.1. DHCP PCP Options

There are two problems with DHCP Options: DHCP Server on Home Gateways (HGW) and Operating Systems DHCP clients

Currently what the HGW does with the options it receives from the ISP is not standardized in any general way. As a matter of practice, the HGW is most likely to use its own customer-LAN-facing IP address for the DNS server address. As for other options, it's free to offer the same values to the client, offer no value at all, or offer its own IP address if that makes sense, as it does (sort of) for DNS.

In scenarios where PCP Server resides on ISP network and is intended to work with arbitrary home gateways that don't know they are being used in a PCP context, that won't work, because there's no reason to think that the HGW will even request the option from the DHCP server, much less offer the value it gets from the server on the customer-facing LAN. There is work on the DHC WG to overcome some of these limitations [I-D.ietf-dhc-container-opt] but in terms of deployment it also needs HGW to be upgraded.

The problems with Operating Systems is that even if DHCP PCP Option were made available to customer-facing LAN, host stack DHCP enhancements are required to process or request new DHCP PCP option. One exception is Windows [DhcpRequestParams]

Finally, in the case of IPv6 there are networks where there is DHCPv6 infrastructure at all or some hosts do not have a DHCPv6 client.

A.2. Default Router

If PCP server does not reside in first hop router, whether because subscriber has a existing home router or in the case of Wireless Networks (3G, LTE) [I-D.chen-pcp-mobile-deployment], trying to send a request to default router will not work.

A.3. User Input

A regular subscriber can not be expected to input IP address of PCP Server or network domain name. Moreover, user can be at a Wi-Fi hotspot, Hotel or related. Therefore relying on user input is not

reliable.

A.4. Domain Name System Based

There are three separate category of problems with NAPTR [RFC3958]

1. End Points: It relies on PCP client determining the domain name and supporting certain DNS queries

2. DNS Servers: DNS server need to be provisioned with the necessary records

3. CPEs: CPEs might interfere with DNS queries and the DHCP domain name option conveyed by ISP that could be used to bootstrap NAPTR might not be relayed to home network.

Authors' Addresses

Sebastian Kiesel
University of Stuttgart Computing Center
Allmandring 30
Stuttgart 70550
Germany

Email: ietf-alto@skiesel.de
URI: http://www.rus.uni-stuttgart.de/nks/

Reinaldo Penno
Cisco Systems
170 West Tasman Dr
San Jose CA
USA

Email: repenno@cisco.com