Abstract

A multihomed network may have a PCP server on each router connecting to each upstream network, providing firewall or prefix translation functions to hosts in the network. In these networks, a PCP client needs to discover all of those PCP servers and then send PCP requests to them individually.

This document proposes a multicast mechanism to discover PCP servers.

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 December 25, 2012.

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 (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
1. Introduction

Using Port Control Protocol (PCP) [I-D.ietf-pcp-base] a host can create mappings with its NAT or firewall. PCP expects only one PCP server. In a multihomed network, there may be multiple PCP servers and the PCP client is unaware of all designated PCP Servers in the network. For example, there may be a PCP server integrated into every firewall device connecting to each network. Hence there is a need for PCP client to discover all such PCP Servers with specific functionalities so that the PCP client can make appropriate PCP requests to each one of them.

This document proposes a means by which a PCP client can discover all such PCP servers within the network. Each PCP server in the network joins a certain multicast. Using the new DISCOVER OpCode, defined in this document, each PCP client sends a DISCOVER request to that multicast group address. Each PCP server responds with a DISCOVER response. The PCP client then sends regular unicast PCP request messages (e.g., MAP or PEER OpCodes) to each of those discovered PCP servers.

2. Notational Conventions

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].

3. DISCOVER OpCode

DISCOVER : Discover PCP servers listening on specific multicast groups.

PCP Servers SHOULD provide a configuration option to allow administrators to disable DISCOVER support if they wish. PCP DISCOVER requests are only designed to discover appropriate PCP servers on the network. The request does not offer functionality defined by other OpCodes described in [I-D.ietf-pcp-base].

The following diagram shows the usage of DISCOVER OpCode, where PCP Server1 and PCP Server2 join the same multicast group (for e.g. ALL-IPv6-FIREWALLS)
3.1. PCP Server joining a multicast group

Each PCP server in the network joins a certain multicast group based on other functionalities embedded with it. Consider a scenario in which a firewall also implements a Port Control Protocol (PCP) [I-D.ietf-pcp-base] Server, in which case it joins a multicast group ALL-IPv6-FIREWALLS.

A PCP server can join more than one multicast groups if it offers multiple functionalities within the same device.

3.2. Generating a DISCOVER Request

To discover the PCP servers listening on each of the assigned multicast addresses of interest to the PCP client, the PCP client sends a DISCOVER request to each of those multicast addresses.

A Discover Nonce is included in the request by the PCP client. The Discover Nonce is randomly chosen by the PCP client, and is used as part of validation of PCP responses.
To accommodate packet loss, the request SHOULD be transmitted several times with a random jitter between them to each of the multicast address. It is RECOMMENDED to transmit the DISCOVER Request a total of three times with the first retransmission after 5 seconds plus a random value between 0-2.5 seconds, and again at 10 seconds plus a random value between 0-5 seconds.

Periodic PCP DISCOVER requests should be made to determine the updated list of PCP servers in the network. A PCP client can send DISCOVER messages periodically every 600 seconds to each of the multicast addresses.

3.3. Processing a DISCOVER Request

When a PCP server listening on one of the multicast groups as described in Section 3.1 receives a PCP DISCOVER Opcode, after successful parsing and processing, it generates a SUCCESS response with zero Assigned Lifetime. If a PCP DISCOVER Request is received on an unassigned multicast group, it should be ignored.

Each PCP Server sends a separate DISCOVER response with unicast source address signaling to the PCP client that the source IPv6 address of DISCOVER response is the PCP Server address. The Discover Nonce field from the request is copied into the PCP DISCOVER response.

3.4. Processing a DISCOVER Response

A DISCOVER request sent to the multicast group will result in zero, one, or more responses from each of the addresses multicast in Section 3.1. If the network contains multiple servers then multiple DISCOVER responses will normally be received. After regular PCP response processing, a PCP client should check using the Discover Nonce from the response to match with a previously sent DISCOVER request and hence also determine the capability of the PCP server.

If a DISCOVER request results in one or more DISCOVER response then the client can update its PCP server list with the source addresses of all DISCOVER responses. This list is essentially a list of all PCP Servers in the network. Future specifications that use PCP DISCOVER to discover PCP servers will also define how PCP clients will use the discovered PCP server list.

A PCP server may join or leave a network unexpectedly (e.g., device failure, link failure, or link recovery). To accommodate these situations, the PCP client should also periodically send PCP DISCOVER requests to each of the multicast groups to ensure that the client has an updated list of PCP Servers.
3.5. Discover Option Packet Format

The DISCOVER Opcode has a similar layout for both request and response.

The following diagram shows the format of the Opcode-specific information in a request for the DISCOVER Opcode:

The Requested Lifetime value MUST be set to zero in the PCP common header.

```
0                   1                   2                   3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                 Discover Nonce (96 bits)                      |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Discover Nonce: Random value chosen by the PCP client.

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

```
0                   1                   2                   3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                 Discover Nonce (96 bits)                      |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Discover Nonce: Copied from the request.

4. Operational Considerations

This document defines a set of multicast addresses in several scopes. Operationally, the choice of which scope is appropriate is made by the administration. A reasonable default value in system configurations might be Organization-Local (e.g., all firewalls operated by the organization). However, a large organization might well choose Site-Local or Admin-Local, and consider that "site" or "administrative" domain to include the set of Firewalls advertising a default route into a specific part of its network.
5. Security Considerations

The principal security threat in this algorithm is a security threat inherent to IP multicast routing and any application that runs on it. A rogue system can join a multicast group and respond to discovery requests pretending to be PCP servers. Discovery of such rogue systems as PCP servers, in itself, is not a security threat if there is a means for the PCP client to authenticate and authorize the discovered PCP servers.

In addition, the security considerations in [I-D.ietf-pcp-base] also apply to this use.

6. IANA Considerations

This note requests of the IANA the assignment of a new PCP Opcode

<table>
<thead>
<tr>
<th>value</th>
<th>Opcode</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>DISCOVER</td>
</tr>
</tbody>
</table>

This note also requests of the IANA the assignment of a set of multicast addresses as described in Section 2.7 of the IP Version 6 Addressing Architecture [RFC4291] from the registry [v6mult]. This set of addresses is referred to as "ALL-IPv6-FIREWALLS". One address should be assigned for each of the following scopes: Link-Local, Admin-Local, Site-Local, and Organization-Local.

7. References

7.1. Normative References


7.2. Informative References


Authors' Addresses

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka  560103
India
Email: tireddy@cisco.com

Prashanth Patil
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli 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

Fred Baker
Cisco Systems, Inc.
Santa Barbara, California  93117
USA
Email: fred@cisco.com