Update to the PCP specification
draft-cheshire-pcp-unsupp-family-04

Abstract

The Port Control Protocol allows clients to request mappings in NAT gateways and firewalls. This document specifies the PCP UNSUPP_FAMILY error code, which enables PCP servers to inform clients when the requested external address family is not supported. This document also removes the requirement for the PCP server to validate the mapping nonce, which proved to be unhelpful in practice.

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 16, 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
1. 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 "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

2. PCP Unsupported Family Error

The Port Control Protocol [RFC6887] allows clients to request mappings in NAT gateways and firewalls. A client can request a mapping to an external IPv6 address or to an external IPv4 address. The client signifies which family of external address it desires by the type of address it puts into the Suggested External Address field.

If the client wants an external IPv6 address, then it populates the Suggested External Address field with a native IPv6 address. In the overwhelmingly common case where the client doesn’t know the external address when it makes its initial request, this will be the all-zeros IPv6 address (::).

If the client wants an external IPv4 address, then it populates the Suggested External Address field with an IPv4-mapped IPv6 address (the first 80 bits set to zero, the next 16 set to one). In the overwhelmingly common case where the client doesn’t know the NAT’s external address when it makes its initial request, this will be the all-zeros IPv4 address (::ffff:0:0).

Note that while the specific address placed in the Suggested External Address field is merely a suggestion that the PCP server is free to ignore, the address family is not. If the suggested address cannot be provided, another address of the same family SHOULD be provided if possible, but if the suggested address *family* cannot be provided by this PCP server, it MUST return a PCP error reply containing the UNSUPP_FAMILY error code.

Many gateway devices, particularly early ones, may not be able to provide both external address families. For example, an IPv4-only NAT cannot provide an external IPv6 address.

Even with gateway devices that can support both external address families, the ability to provide the an external address of the
requested family may depend on the family of the client’s internal address. For example, a gateway that supports native IPv6, and traditional NAT44, but not NAT64, can provide mappings from an internal IPv6 address to an external IPv6 address (typically the same address when no address translation is being performed), and can provide mappings from an internal IPv4 address to an external IPv4 address, but not mappings from an internal IPv6 address to an external IPv4 address. When such a gateway receives a request to map an internal IPv6 address to an external IPv4 address it MUST return the UNSUPP_FAMILY error code.

Note that it is possible and valid for a given internal address and port to have two mappings simultaneously, one to an external IPv4 address and one to an external IPv6 address. The handling of outbound packets is determined by the outbound destination address; for example, an outbound IPv6 packet addressed to an IPv6 address in the NAT64 gateway’s IPv6 address pool is translated to the corresponding IPv4 packet before forwarding; an outbound IPv6 packet addressed to some other routable IPv6 address is forwarded unmodified.

A client that can handle both IPv6 and IPv4 external addresses MAY send two requests, and then determine its behaviour based on the responses it receives. For example, if the client requests and receives an IPv6 external address, it may create a DNS AAAA record giving that IPv6 address. If the client requests and receives an IPv4 external address, it may create a DNS address record giving that IPv4 address. If the client requests and receives both families of external address, it may create both DNS records. Or, if one external address is sufficient for the client, then it MAY first request its preferred address family, and only if that fails with an UNSUPP_FAMILY error, request the other family.

2.1. Implications for RFC 6887

Various sections of the PCP specification [RFC6887] describe clients and servers identifying a mapping by examining the three-tuple of (internal port, protocol, internal address) in a request or reply. For example:

If the internal port, protocol, and internal address match an existing static mapping (which will have no nonce), then a PCP reply is sent giving the external address and port of that static mapping, using the nonce from the PCP request. The server does not record the nonce.
It is possible that a mapping might already exist for a requested internal address, protocol, and port. If so, the PCP server takes the following actions...

If no mapping exists for the internal address, protocol, and port, and the PCP server is able to create a mapping using the suggested external address and port, it SHOULD do so.

After performing common PCP response processing, the response is further matched with a previously sent MAP request by comparing the internal IP address (the destination IP address of the PCP response, or other IP address specified via the THIRD_PARTY option), the protocol, the internal port, and the mapping nonce. Other fields are not compared, because the PCP server sets those fields.

Everywhere that RFC 6887 refers to using the "internal port, protocol, and internal address" to identify a particular mapping, it should be read to mean the four-tuple of

\{ \text{int port, protocol, internal address, external address family} \}.

PCP clients and servers that only support one external address family can continue to use the previous three-tuple \{ \text{internal port, protocol, internal address} \} to identify a mapping, since they only support one external address family, and unilaterally reject requests and responses containing the unsupported family. For PCP servers this means rejecting requests containing the unsupported address family via the UNSUPP_FAMILY error code. For PCP clients this should be a non-issue because a PCP client should never receive a reply containing an external address family it didn’t request, but should a client receive such a reply from a misbehaving PCP server offering an external address family the client did not request, the client MUST silently ignore the erroneous reply.

An implication of this update to the PCP specification is that when renewing a mapping, a PCP client MUST include a suggested external address of the correct family, so that the gateway device can identify which mapping is being renewed. Ideally a PCP client SHOULD record the previously-granted external address and use that as the suggested external address in its renewal request, to facilitate recovery in the event of gateway state loss, but at the very least a PCP client MUST provide an all-zeroes suggested external address of the correct family (just as it must have indicated the desired address family in its initial request that created the mapping).
3. New Nonce Check Behavior

The PCP specification [RFC6887] states that if a client requests a mapping (or renews a mapping, which is the same thing, from the server’s point of view) and the requested mapping already exists, but with a different nonce, then the server returns a NOT_AUTHORIZED error.

This has proved to be problematic. The nonce exists primarily to allow the client to validate that the responses it receives from the PCP server are legitimate, and have not been fraudulently generated by an off-path attacker. Requiring the PCP server to also verify that the nonce matches causes unnecessary failures.

For example, if a client reboots or otherwise suffers a loss of state, it may not have a record of nonces it previously used. Suppose this client then requests a mapping from an external IPv4 address to its internal IP address at TCP port 22, so that it can receive ssh logins. If the same client machine had previously requested such a mapping with a different nonce, then the new request will fail with a NOT_AUTHORIZED error. This is unhelpful and misleading. The client does in fact have a mapping. Incoming connection requests to its external address and port will in fact be forwarded to it at port 22. The PCP server is simply refusing to tell the client what the external address and port are, hindering the client’s ability to use the mapping.

The same scenario also exists in the case where (i) a different internal host had previously requested a mapping to its internal port 22, (ii) that host then left the network, and (iii) the newly vacated internal IP address is then assigned to new host. When this happens, the new host will be unable to usefully request a mapping to its internal port 22 until the old mapping expires. The new host will actually have a mapping to its internal port 22, and will actually receive incoming connection requests arriving at the external address and port, but the PCP server will refuse to tell the client what the external address and port are, thereby hindering the new host from communicating that external address and port to the peer it wishes to receive connections from. This is not helpful.

This PCP security check does not prevent the new host from learning the external address and port by other circuitous means. For example, the new host could discover the external address and port by sending outbound traffic a destination it controls, and having that destination report back the source address and port.

Furthermore, this PCP security check is inconsistent with other PCP behaviour. It makes PCP behave differently for explicit dynamic
versus other kinds of mappings. Indeed, requests matching static mappings are not subjected to the nonce check and will result in a response containing the static mapping’s current state. There is no reason that MAP requests matching a dynamic mapping should return less information.

Therefore, the nonce check behaviour described below MUST be implemented instead.

3.1. Nonce Check for MAP Requests

If operating in the Simple Threat Model (Section 18.1 of PCP specification [RFC6887]), and the internal port, protocol, internal address, and external address family match an existing explicit dynamic mapping, but the mapping nonce does not match, then the existing mapping nonce is updated to the new nonce, the lifetime is updated (subject to the PCP server policy for maximum and minimum lifetimes) and an appropriate PCP reply is sent, using the new nonce and assigned lifetime.

This specification makes no statement about mapping nonce with the Advanced Threat Model.

3.2. Nonce Check for PEER Requests

If operating in the Simple Threat Model (Section 18.1 of PCP specification [RFC6887]), and the internal port, protocol, internal address, and external address family match a mapping that already exists, but the mapping nonce does not match (that is, a previous PEER request was processed), then the existing mapping nonce is updated to the new nonce, the lifetime is updated (subject to the PCP server policy for maximum and minimum lifetimes) and an appropriate PCP reply is sent, using the new nonce and assigned lifetime.

This specification makes no statement about mapping nonce with the Advanced Threat Model.

3.3. Returning NOT_AUTHORIZED error

A NOT_AUTHORIZED error should still be returned, as described in Section 15.1 of PCP specification [RFC6887], when a PCP client attempts to delete a static mapping (i.e., a mapping created outside of PCP itself) or an outbound (implicit or PEER-created) mapping.
4. IANA Considerations

IANA should allocate the following PCP Result Code:

14 UNSUPP_FAMILY: Unsupported external address family, e.g., IPv6 in a NAT that handles only IPv4. This is a long lifetime error.

5. Security Considerations

This new error code leaks no sensitive information and creates no new security vulnerabilities.

6. Normative References


Authors’ Addresses

Stuart Cheshire
Apple Inc.
1 Infinite Loop
Cupertino, California  95014
USA

Phone: +1 408 974 3207
Email: cheshire@apple.com

Simon Perreault
Viagenie
246 Aberdeen
Quebec, QC  G1R 2E1
Canada

Phone: +1 418 656 9254
Email: simon.perreault@viagenie.ca
URI:  http://viagenie.ca