Updates to the PCP Specification

Stuart Cheshire <cheshire@apple.com>
Simon Perreault <simon.perreault@viagenie.ca>

Document History

- draft-cheshire-pcp-unsupp-family-00
    - Submitted 28th May 2013
- draft-cheshire-pcp-unsupp-family-05
    - Submitted 14th July 2013

Document Topics

- Address Family Selection
- Nonce Checking

Address Family Selection

- Client needs to indicate
  desired external address family
- Server may be able to provide both:
  - IPv6 firewall
  - NAT64
- Server needs to respect client indication

Why is this Important?

- Client inadvertently requests IPv6
  - Server returns IPv4
  - Client works
- Server updated to support IPv6
  - Server returns IPv6
  - Client fails

Nonce Checking

- PCP specification [RFC6887] states client must request/renew using correct nonce
- What if client doesn't know correct nonce?
  - After reboot
  - Connecting to a new network

Why is this Important?

- Client actually has active mapping
- But can’t access it via PCP
  - Can learn of it via indirect means, such as STUN

Proposed Solution

- Requests/renewals with mismatched nonce treated as “read-only” renewal
- Learns about mapping, but can’t modify it until it expires

Implications

- Client requests mapping
- Client learns of pre-existing mapping (which has different nonce)
- Mapping is not modified
- Remaining mapping lifetime is returned (e.g. 100 minutes)

Renewal

- Client renews mapping roughly halfway to expiry (50 minutes)
- Mapping is not modified
- Remaining mapping lifetime is returned (50 minutes)

Renewal

- Client renews mapping roughly halfway to expiry (25 minutes)
- Mapping is not modified
- Remaining mapping lifetime is returned (25 minutes)

Renewal

- Client renews mapping roughly halfway to expiry (12 minutes)
- Mapping is not modified
- Remaining mapping lifetime is returned (12 minutes)

Renewal

- And so on…
- Client renews mapping with increasing rapidity until it expires
- Client then gets a new mapping with its new nonce
- Protocol then works correctly

Discussion Issues

- Impostor fraudulently “claims” a mapping
- Legitimate owner of that internal address then thrashes the PCP server with large number of packets until it reclaims ownership of the mapping