Pimp Your NAT!

Applicability of NAT-PMP for use with Service Provider NAPT Gateways
NAT-PMP Overview

- Very lightweight alternative to UPnP-IGD for dynamic port forwarding service at NAPT gateways.
- It does exactly three things:
  - Maps exterior ports to interior ports at the requesting client’s interior address.
  - Answers client queries about the exterior address paired with the client.
  - Notifies clients when translation state is reset.
Some Packets

- **Map Request:**

  ```
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Vers = 0 | OP = x | Reserved (MUST be zero) |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Internal Port | Requested External Port |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Requested Port Mapping Lifetime in Seconds |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  
  Opcodes supported:
  1 - Map UDP
  2 - Map TCP
  ```

- **Map Response:**

  ```
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Vers = 0 | OP = 128 + x | Result Code |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Seconds Since Start of Epoch |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Internal Port | Mapped External Port |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Port Mapping Lifetime in Seconds |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  ```
Expectations

- Endpoint independent filtering of mapped ports.
- IP address pooling behavior is “paired” (see RFC 4787).
- Clients and server in one administrative domain.
Proxying with NAT444

- Recursive forwarding of mapping requests.
- Translating interior to exterior on the way up.
- Translating exterior to interior on the way down.
- Propagate exterior address downward.
- Synchronize the elapsed time in epoch count.
Proxying with DS-Lite

- Much simpler! No translation required.
- Caching state possible, but not recommended.
- Should still synchronize elapsed time in epoch and propagate exterior address downward.
UNSAF Considerations

- Hairpins are pushed up to the outermost NAPT.
- Could be regarded as suboptimal in NAT444.
- Unavoidable in DS-Lite.
Security Considerations

- SP-NAT server will need to apply per-subscriber resource limits, which means a new response code in the NAT-PMP specification.

- Client and relay authorization not defined.
  - Deliberately left out of original NAT-PMP specification.
  - Unwritten assumption: require IPsec w/ IKE between client and server if authorization is required.
Questions? Flames?

- Please remember to state your name and speak clearly at the microphone.