UPDATE PROXY

IETF 104 PRAGUE, MARCH 2019
TOM PUSATERI
Client query:
_b._dns-sd._udp.example.com. PTR

Response:
cb007100.example.com
cb007200.example.com

Client queries:
_iPP._tcp.cb007100.example.com. PTR
_iPP._tcp.cb007100.example.com. PTR
UNICAST SERVICE DISCOVERY

- Reduce DNS Update to trusted infrastructure
- Announcements proxied through UPDATE to authoritative servers
  - uses existing authoritative servers with IP subnet-to-subdomain model
  - subdomains can be created on demand minimizing configuration
- Transparent to clients making unicast queries to browseable domains
- Transition from multicast to unicast independently
OVERVIEW

- Map IP subnet to subdomain, ensure authoritative server accepts UPDATEs
- Passively monitor mDNS announcements, send UPDATEs
- Refresh via unicast “QU”, delete upon receiving “goodbye” announcements
- Periodically send query for _services._dns-sd._udp.local on active IP subnets
- May include TIMEOUT resource records to have authoritative server remove services or include OPT Lease Update Lifetime in UPDATE.
DISCOVERING SUBDOMAIN

- Address derived domain enumeration using local resolver
  - `dr._dns-sd._udp.0.113.0.203.in-addr.arpa`
  - Response: `bldg7a.example.com`
- Fall back to local configuration or...
- Algorithmic subdomain label generation
  - `203.0.113.0/24 becomes cb007100.example.com`
  - Once created, proxy creates `0.113.0.203.in-addr.arpa`
Clients may query _dns-updateproxy-tls._tcp.<ip-subnet>.in-addr.arpa via unicast to find Update proxy.

Make TLS connection to target, port and begin sending unicast announcements.
## COMPARISON TO DISCOVERY PROXY

<table>
<thead>
<tr>
<th></th>
<th>Discovery Proxy</th>
<th>Update Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>on demand</td>
<td>all services</td>
</tr>
<tr>
<td><strong>Response Time</strong></td>
<td>cache dependent</td>
<td>immediate</td>
</tr>
<tr>
<td><strong>IP multicast increase</strong></td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
</tr>
<tr>
<td><strong>unicast increase</strong></td>
<td>none</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td><strong>DNSSEC</strong></td>
<td>NSEC not possible</td>
<td>NSEC works</td>
</tr>
<tr>
<td><strong>Complexity</strong></td>
<td>Authoritative + full mDNS + relay</td>
<td>passive mDNS + UPDATE xmit</td>
</tr>
</tbody>
</table>
OUTSTANDING ISSUES

- Verify creation of all necessary records for client browsing are documented
- Verify subdomain cleanup after failover
- Discuss registration of services in multiple subdomains, dr vs. r
- PUSH subscriptions to unicast authoritative
IMPLEMENTATIONS

- rupdateproxy - [https://github.com/pusateri/rupdateproxy](https://github.com/pusateri/rupdateproxy)
  - Listens to mDNS announcements and builds local cache
  - Creates UPDATEs for new cache entries to send to authoritative
  - TODO:
    - UPDATEs with TSIG and TCP, TLS
    - Subdomain discovery and registration
    - dynamic interface support
    - Integration with switch/router platform for deployment