Stateful Multi-Link DNS Service Discovery

draft-lemon-stateful-dnssd-00

Ted Lemon <Ted.Lemon@nominum.com>

Goals

- Extend DNSSD-hybrid (don't reinvent the wheel)
- Populate DNS zones based on service discovery announcements
- Support standard DNS protocol infrastructure (primary/secondary servers, zone transfers, DNSSEC)
- Make service discovery announcements more secure
- Provide a means of announcing services for devices on network infrastructure (e.g. LLNs) that do not support multicast
- Elimination of need for regular multicast queries on networks where multicast is expensive

Disadvantages to this approach

- Doesn't actually eliminate multicast until every service can advertise using SIG(0) secure DNS updates, which may never happen, and certainly will take time.
- Maintaining state is more work than doing stateless queries through a cache.
- Requires stable naming infrastructure (difficult particularly on ad-hoc networks such as homenets)
- Requires forwarders on each local link to support link-based trust model (same model used by mDNS)
    - It is possible that we could use a secure pairing protocol to avoid this problem; however, mDNS proxies are still required on all links where legacy mDNS support is required
- Services will probably want to support mDNS *as well as* Stateful ML-DNSSD

This sounds hard: why do it?

- The primary motivation for this work is to support stateful naming in homenets.
- Probably also applicable to managed networks
- Potentially can be quite a bit more secure than mDNS hybrid
- Provides functionality not provided by mDNS hybrid: support for LLNs without multicast

Overview

- Services discover Stateful ML-DNSSD by using DNSSD queries to find the DNSSD registration zone, and then looking up well-known names in that zone
- This must be repeated whenever a link state change is noticed
- Devices check to see if DNSSD is available and use it if so (this is, as far as we know, already universally supported)
- Services that support stateful ML-DNSSD use DNS updates signed with SIG(0) to advertise
- Services that only support mDNS are discovered using hybrid proxy
- Zones are populated using both methods; the DNS server occasionally purges stale entries.

Status

- Current spec is pretty sketchy
- No implementation yet
- Not clear that DNS Update is the right way to do this.
  - Could just use a single HTTPS transaction rather than a bunch of DNS updates

What do people think of doing this?