dnssd requirements

draft-ietf-dnssd-requirements-01

Kerry Lynn <kerlyn@ieee.org>

Stuart Cheshire <cheshire@apple.com>

Marc Blanchet <marc.blanchet@viagenie.ca>
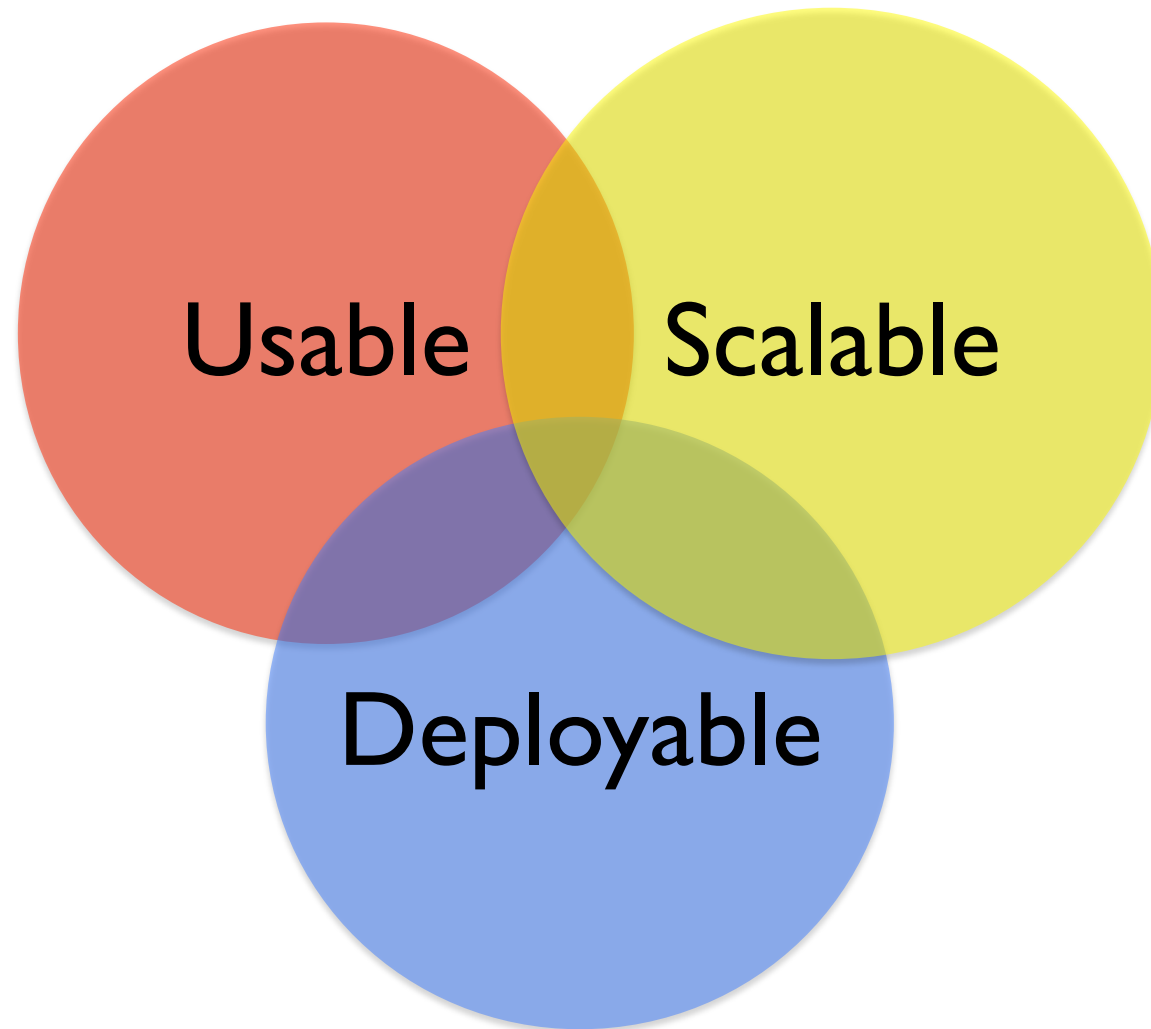
Daniel Migault <mglt.biz@gmail.com>

IETF 89, London, 3 March 2014

Goals

- DNS-Based Service Discovery among links (and link technologies)
  - Zero configuration (local)
  - Minimal configuration (global)
  - Administrative control where desired

dnssd requirements "tussle"

Usability

- Smooth continuum of user experience from single link to site to global
  - Principle of least astonishment
    - Do we need a model of naming? (e.g. RFC 1498)
    - Do we need a model of users? (admins & others)
- Convenient user interface
  - Not long flat list of service names
  - Leverage file system browser experience?

Scalability

- In terms of:
  - Network traffic
  - CPU and memory requirements on network entities
  - Total number of services
    - Conceivable that in some deployment scenarios, e.g. building automation, response might exceed 64KB

Deployability

- Incremental deployability (e.g. "islands" of infrastructure-less functionality can be merged)
- Identify what changes to existing network elements will be required and attempt to minimize those changes (e.g. may be easier to revise clients than servers)
- Suitable out-of-the box defaults should enable zero-config use on many small- to medium-sized networks, while still allowing for administrative control in networks where that's appropriate

Security

- Authorization versus authentication (e.g. which services are authorized to advertise?)

- Avoid manual configuration of every service entry in a directory

- Avoid solving "new" security problems
  - Attempt to leverage existing solutions

Requirements Discussion

Changes since last draft

- Previous version was draft-ietf-dnssd-requirements-00
- Added new authors
- Minor edits for clarity
- Improved terminology section
  - Introduced some shorthand acronyms, e.g. "SSD"
- Added REQ 9 for usability
- Added some additional discussion of threats in the Security section

REQ1

The scope of the discovery should be either automatically determined by the discovering devices or configured (by selection) in the case of multiple choices.

REQ2

For use cases A, B and C*,
there should be a zero configuration
mode of operation.

A: Personal network
B: Small home network
C: Larger home or small
business network

REQ3

For use cases D and E*, there should
be a way to configure the scope
of the discovery and also support
both smaller (ex: department) and
larger (ex: campus-wide) discovery.

D: Enterprise networks
E: Higher Education

REQ4

For use cases D and E*, there should be an incremental way to deploy the solution.

D: Enterprise networks
E: Higher Education

REQ5

The new solution should integrate or at least should not break any current link scope DNS-SD/mDNS protocols and deployments.

REQ6

The new solution must be capable of spanning multiple links (hops) and network technologies.

REQ7

The new solution must be scalable to thousands of nodes with minimal configuration and without degrading network performance.

REQ8

The new solution should enable a way to provide a consistent user experience whether local or global services are being discovered.

REQ9

The information presented by the new solution should reflect reality.
That is, new information should be available in a timely fashion and stale information should not persist.