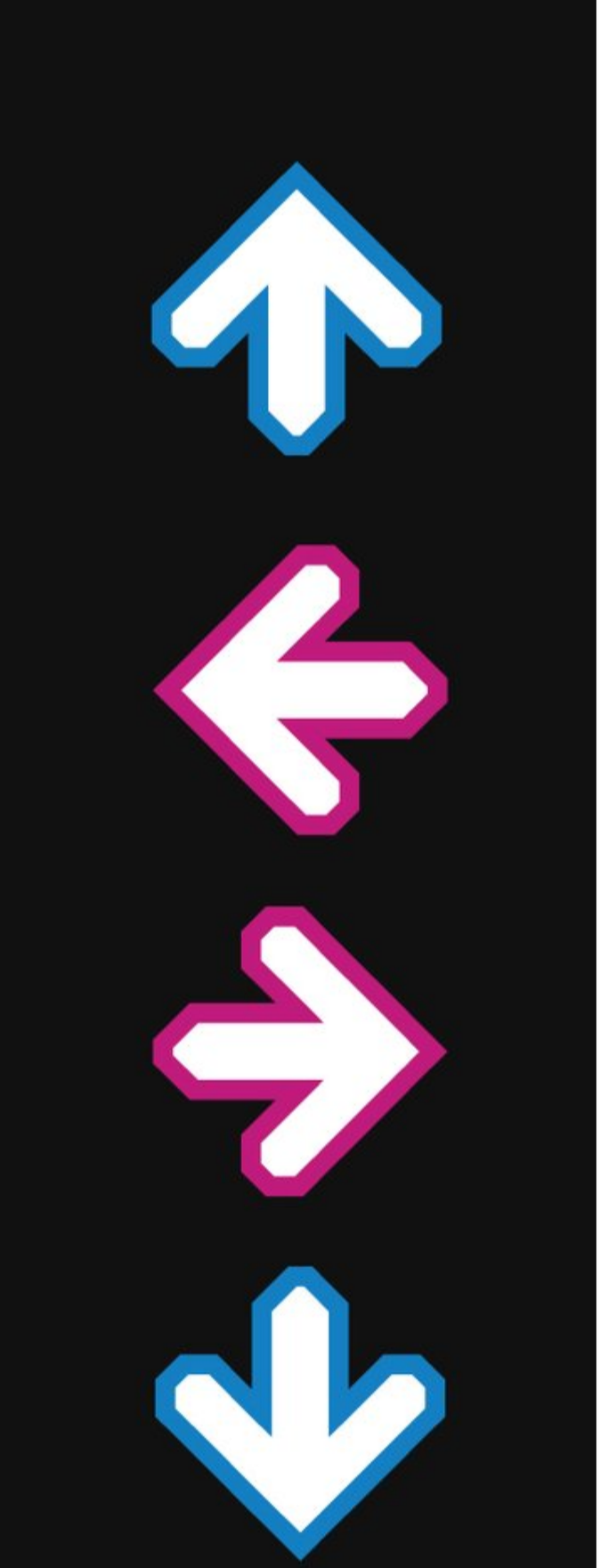

Discovery of Designated Resolvers

draft-ietf-add-ddr

Tommy Pauly, Tommy Jensen,
Eric Kinnear, Patrick McManus, Chris Wood
ADD
IETF 111, July 2021, Virtual

Status

-02 draft published July 8

5 open issues, generally minor

1 open PR (discussion on it later)

Recent changes

Removed “equivalence”, only talk about “designated”

Cleaned up use of SVCB and address hints

Clarified behavior of _dns.resolver.arpa

Updated examples and guidance for _dns.resolver.arpa queries

resolver.arpa use

Issue #21

Concern is use of resolver.arpa instead of X.X.X.X.in-addr.arpa

Current rationale is to mimic ipv4only.arpa

Querying specific resolver information

Doesn’t require a record per resolver address

Authenticated, Opportunistic, and More?

Issue #18

Authenticated discovery allows trusted redirection to a designated resolver

- Trust based on a known name or IP address
  - Validated in the certificate
  - Matching IP address allows going from “1.1.1.1” to a broader set of addresses, etc

Authenticated, Opportunistic, and More?

Issue #18

Opportunistic discovery allows use of an encrypted protocol on the same IP address as the known Do53 resolver

Allows encrypted DNS to a private address

Useful to prevent DNS observation by others on a network (public Wi-Fi, home networks, etc)

List discussion about the value of this; what do we think?

Authenticated, Opportunistic, and More?

Issue #18

A complete mismatch between the provisioned IP address and the designated resolver is currently disallowed

- This is the local CPE -> ISP resolver case
- DDR currently considers authenticating this case out of scope, but the unauthenticated hint exists
- PR #11 is an attempt solve this with a different security model and weaker identity guarantees
- Another approach here is to simply disallow automatic use, but allow system policy or user approval to allow this

Questions?