DNS Resolver Discovery Protocol

draft-mglt-dprive-add-rdp-00

Daniel Migault

Motivations

The DNS resolving service can be achieved via:

- multiple DNS resolvers
- over multiple transports (Do53, DoT, DoH)

To perform a selection one needs to know what is available

The DNS Resolver Discovery Protocol (DRDP) enables:

1. A DNS client to discover available resolvers / transports
2. A Resolver to inform other transports are available

Requirements

- REQ 1: DRDP MAY be used by a DNS client (Do53, DoT, DoH, ...) to discover resolving service or by a resolver to advertise other resolving services are available.
- REQ 2: DRDP MUST be able to list dynamically locally and globally resolving services available to the DNS client.
- REQ 3: DRDP MUST at least return DNS transport parameters associated of the resolving services and MAY be extended with additional parameters.
- REQ 4: DRDP MUST return selection parameters in a standard format to ease automation.

Requirements

- REQ 5: DRDP MUST return selection parameters that can be displayed to an end user either as a simple notification of when user interaction is involved in the selection process.
- REQ 6: DRDP MUST enable a resolving service provider to indicate a preference between multiple provided resolving services.
- REQ 7: DRDP SHOULD be able to narrow down the discovery to a subset of resolving services.
- REQ 8: DRDP MUST provide authenticated information
- REQ 9: DRDP deployment MUST NOT be disruptive for the legacy DNS client or infrastructure and legacy client SHOULD be able to incrementally include DRDP.

Information returned by RDP

Resolver identity (hostname.example.com)

- example.com: **resolving domain**
  - meaningful to the end user (# legal entity)
  - not user friendly but can be used as a key
  - represents the provider of the resolving service
- hostname: resolver networking identifier
  - not expected to be meaningful to the end user.

Resolver parameters

- transport, TLS, URI template ?, specific services ? ...

High Level View

- A **resolving domain** can host multiple resolving services
- RDP uses DNS messages:
    - DNS is always understood by the resolver and the client

High Level View

RDP performed by the DNS client:

1. Discover the **resolving domains** (local and global)
2. Within each **resolving domain**
   - Discover the various resolving services

RDP performed by the resolver:

1. Resolver informs the DNS client of other alternatives

Resolving Domain Discovery

- Global **resolving domain** are hosted under _dns.rdns.arpa

```
b._dns.rdns.arpa  PTR <resolving domain0>
b._dns.rdns.arpa  PTR <resolving domain1>
[...]
```

- Local resolvers are identified with an IP address
  - **resolving domain** are derived from a reverse resolution

Resolving Service Discovery

1. all resolving services

```
_dns.example.com. SVCB 0 svc.example.com.
svc.example.com.  SVCB 12 ( svc0.example.net.
                            port="5353" ux="Legacy Resolver" )
svc.example.com.  SVCB 1 ( svc1.example.net.  alpn="dot"
                           port="5353" esniconfig="..."
                           ux="Preferred Example's Choice" )
svc.example.com.  SVCB 3 ( svc2.example.net. alpn="h2"
                           port="5353" esniconfig="..." ux= )
svc.example.com.  SVCB 2 ( svc3.example.net. alpn="h3"
                           port="5353" esniconfig="..." ux= )
```

Resolving Service Discovery

2. narrowing down the discovery on sub services

```
### Definition of the resolving service subsets
_dns.example.com PTR _53._dns.example.com
_dns.example.com PTR _853._dns.example.com
_dns.example.com PTR _443._dns.example.com

### services instances per service subset
_53._dns.example.com. SVCB 0 svc0.example.com.
svc0.example.com.     SVCB 12 ( svc0.example.net.
                                port="5353" ux="Legacy Resolver" )
_853._dns.example.com. SVCB 0 svc1.example.com.
svc1.example.com.      SVCB 1 ( svc1.example.net.  alpn="dot"
                                port="5353" esniconfig="..."
                                ux="Preferred Example's Choice" )

_443_dns.example.com.  SVCB 0 svc4.example.net.
svc4.example.com.      SVCB 3 ( svc2.example.net. alpn="h2"
                                port="5353" esniconfig="..." ux= )
svc4.example.com.      SVCB 2 ( svc3.example.net. alpn="h3"
                                port="5353" esniconfig="..."
                                ux="Testing QUIC")
```

Thanks!