DNS Resolver Discovery Protocol

draft-mglt-dprive-add-rdp-02

Daniel Migault

Motivations

DRDP aims to address the first two areas of the charter:

- Mechanism that allows clients to discover DNS resolvers that support encryption and that are available to the client either on the public Internet or on private or local networks.
- Communication of DNS resolver information to clients for use in selection decisions.

To reflect the end user or application policy, collected information needs to be:

- from multiple resolvers
- up-to-date
- certified

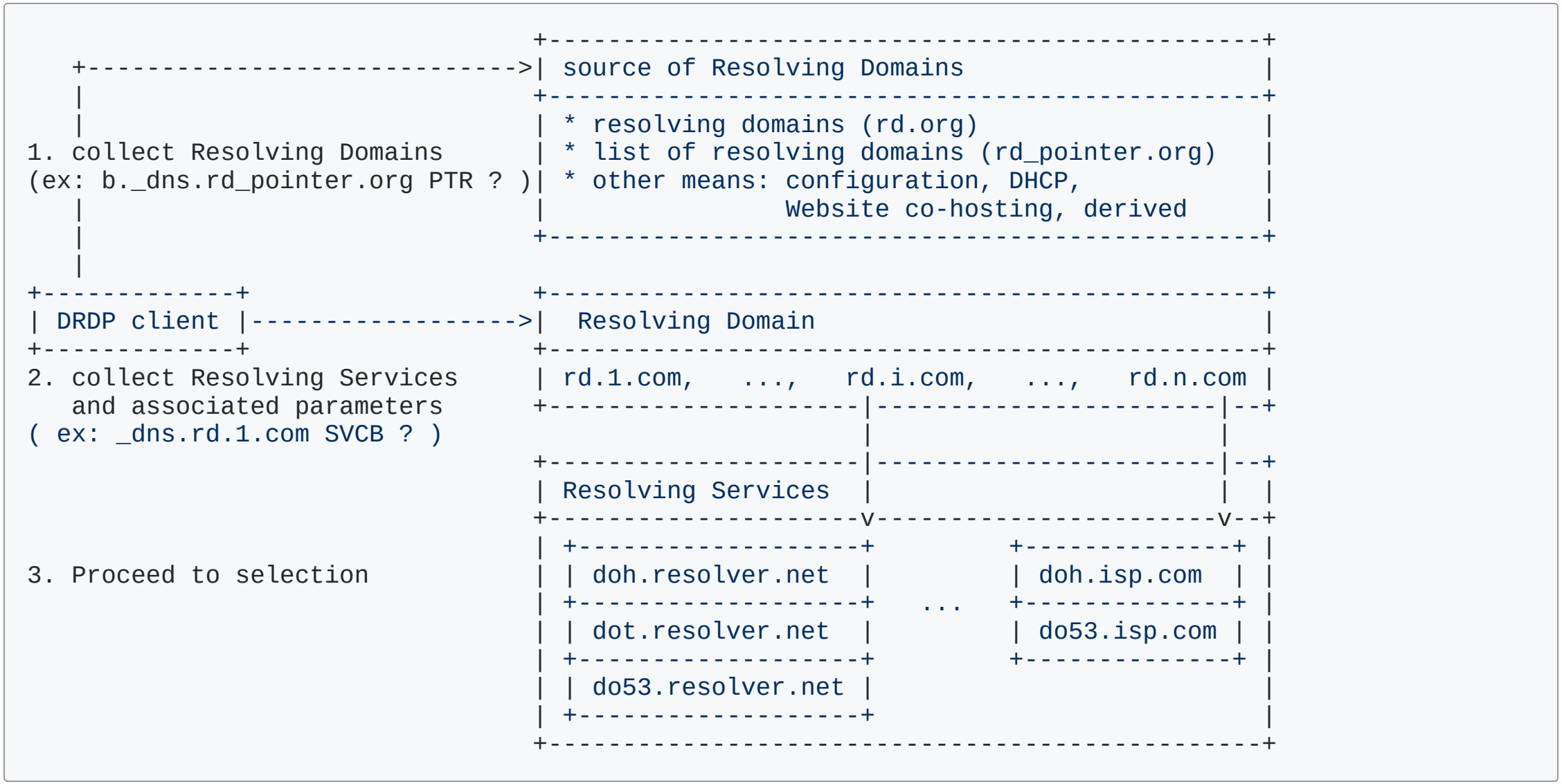
The client begins with knowledge of the address of the Do53 resolver. Same Provider Auto Upgrade requires a centralized list of IP addresses to turn this into a DoH URI Template. Reasons this is bad:

- Not scalable
- Hard to maintain up-to-date
- Entire possibilities are irrelevant for most end users
    - open resolvers, resolver of other ISPs than mine
- Provides a party with control on who is listed or not

But also the resolvers available to a DNS client are contextual:

- may involve non-publicly available resolvers (resolvers provided by ISPs or enterprise)
- may involve a subset of pre-selected resolvers (selection may be performed by a third party)public-dns.info, curl
- ...

Architecture



DNS client can run DRDP as follows:

```
drdp -pointer rd_pointer.org
drdpd -rd rd.org
```

Which information might clients want to know about a resolver? Foreseen parameters could be:

- user-display
- uri_template
- auth_domain (default none)
- scope_domain
- resolving_zones (default all)
- filtering
- ip_subnet (default all)
- dnssec (default yes)
- (those associated to TLS)

Use case 1: Resolving Services Discovery from pointer.org

Ex: pointer.org is a configuration parameter in an application or PvD

```
1. b._dns.rd_pointer.org PTR ?
            <- rd.1.net  <resolving domains >
            <- ...
            <- rd.n.org

2. for each resolving domain rd.i.org:
  _dns.rd.i.org. SVCB 0 svc.example.com.
   svc.example.com.    SVCB 12 ( svc0.example.net.
                       port="5353" user-display="Legacy Resolver" )
   svc.example.com.    SVCB 1 ( svc1.example.net.  alpn="dot"
                       port="5353" esniconfig="..."
                       user-display="Preferred Example's Choice" )
   svc.example.com.    SVCB 3 ( svc2.example.net. alpn="h2"
                       port="5353" esniconfig="..." user-display= )
   svc.example.com.    SVCB 2 ( svc3.example.net. alpn="h3"
                              port="5353" user-display="" )
   svc*.example.net    TLSA
```

Advantage:

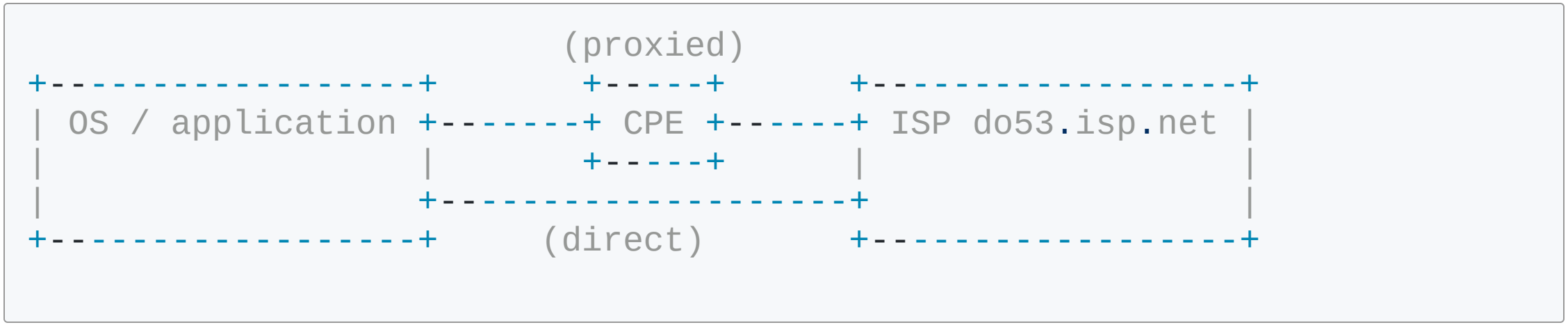
- up to date list as well as parameters associated to each resolving service
- trust is delegated to the pointer
- not limited to DoH but includes Do53, DoT, DoH, DoQ, ...
- Flexible: SvcParamKey makes it re-usable with HTTPS RRset (see draft-pauly-dprive-adaptive-dns-privacy

Use case 2: Resolving Services Discovery provided by ISPs

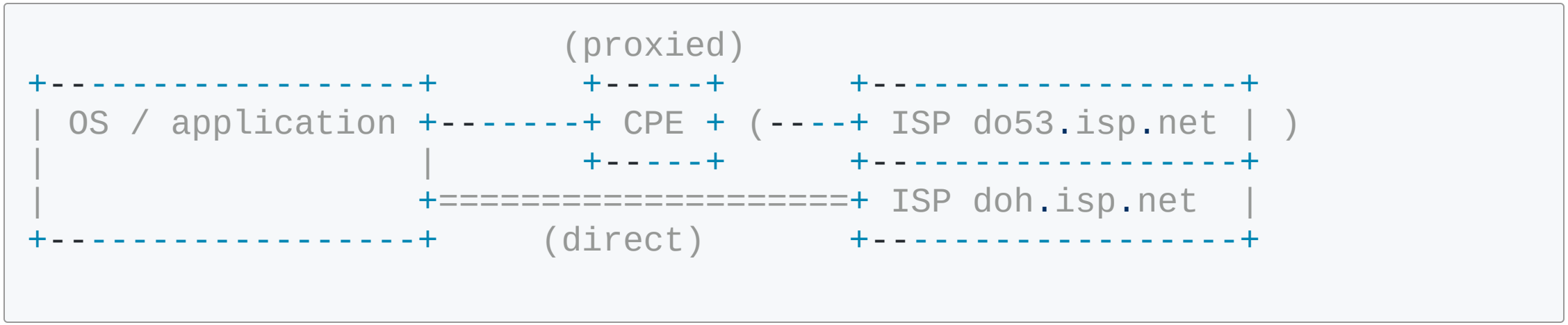
Problem: How can I upgrade connectivity to encrypted DNS?

Particularities:

- contextual to network location (not globally reachable)
- ISP advertises its resolver using unsecured DHCP
- IP addressed may be private
- DNS traffic may be proxied or direct
- CPE are hard to upgrade (eventually)



Scenario 1: CPE cannot be upgraded



Unless necessary traffic is sent to doh.isp.net

- .home.arpa is sent to the CPE

Generate the pointer:

1. Retrieve the public IPv4 address (STUN) from the private IPv4
2. Perform a reverse lookup fqdn.isp.net
3. Run drdp -pointer fqdn.isp.net

Optionally do the same from the advertised resolver IP address

Resolving Domain Pointer from IP WAN

```
$ dig myip.opendns.com @resolver1.opendns.com
;; ANSWER SECTION:
myip.opendns.com.       0       IN      A       96.22.11.129

$dig -x 96.22.11.129
;; ANSWER SECTION:
129.11.22.96.in-addr.arpa. 86400 IN     PTR     modemcable129.11-22-96.mc.videotron.ca.

$ drdp -pointer modemcable129.11-22-96.mc.videotron.ca.
```

Resolving services from WAN

- asserts a relation between the IP provider and Resolving Service
- (should include) a SVCB redirection to third party resolver to assert the delegation
- should indicate the served network using a SvcParameter

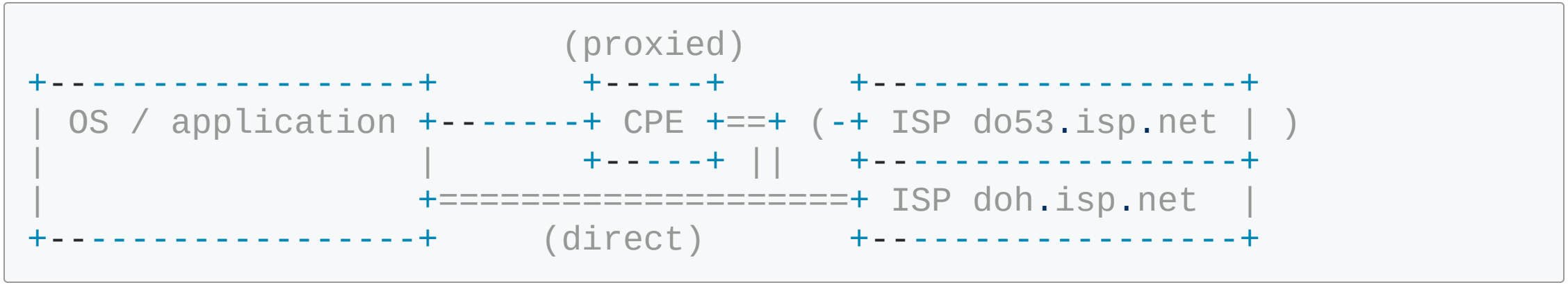
Resolving Domain from resolvers IP addresses

```
$ resolvectl status
link 3 (wlo1)
  [...]
  Current DNS Server: 192.168.0.1
         DNS Servers: 192.168.0.1
                      23.233.128.16
                      24.225.128.17
dig -x 23.223.128.16
;; ANSWER SECTION:
16.128.223.23.in-addr.arpa. 43200 IN    PTR     a23-223-128-16.deploy.static.akamaitechnologies.com.

$ dig -x 24.225.128.17
17.128.225.24.in-addr.arpa. 32198 IN    PTR     dns12.videotron.ca.

$ drdp -pointer dns12.videotron.ca.
```

Scenario 2: CPE can be upgraded



OS / application / CPE upgrade to doh.isp.net is similar to Scenario 1

The CPE becomes a service of the homenet
DNS-SD on home.arpa to find the Resolving Service

- need to convert SvcParam to TXT entries
- DNSSEC needs some setting

DNS-SD over the Registered Homenet Domain may benefit from the security of DNSSEC

- needs to be provided

Overall it seems that the definition of a discovery protocol may need involve:

- DRDP (SvcParameter, terminology such as resolving domains...)
  - SvcParameter may be provided using other mechanisms
- derivation of contextual resolving domain or pointers of resolving domains
- use cases involving the CPE need collaboration with homenet / dnssd WG

Note that DRDP and the CPE use case are two diferent drafts.

Thanks!