Multicast DNS-Based Service Discovery for Encrypted DNS Services (EDNS-SD) draft-liu-add-dnssd-edns-01

Dongjie Liu, Zhiwei Yan, Guanggang Geng, Guoqiang Zeng

@IETF 124

Motivations

The Local Network Privacy Gap

- Problem: Encrypted DNS (DoT, DoH, DoQ) widely adopted on public internet, but local networks without centralized infrastructure remain vulnerable.
- Local DNS traffic often plaintext → exposes device activities, service dependencies, user behavior.
- Traditional discovery (DHCP, RA) lacks:
  - Flexibility for encrypted DNS parameters
  - Operation in infrastructure-less environments
  - Real-time updates

Motivations

Why mDNS/DNS-SD?

Ideal Foundation for Local Service Discovery:

- Zero-configuration - No central server required
- Topology independent - Works in isolated/offline networks
- Real-time updates - Seconds vs. DHCP's lease-based delays (minutes-hours)
- Rich parameter negotiation - TXT records carry protocol details

Solution Overview

- Use mDNS/DNS-SD to discover encrypted DNS resolvers in local networks

- New service types:
  - _dot._tcp (DoT)
  - _doh._tcp (DoH)
  - _doq._udp (DoQ)

- Rich TXT record parameters for configuration
- Works without central infrastructure
- Real-time service updates

Solution

Service Types & Instance Format

Service Types:

Service Type	Protocol	Transport
_dot._tcp	DoT	TCP
_doh._tcp	DoH	TCP
_doq._udp	DoQ	UDP

Instance Name Format:
<Instance>.<Service>.<Domain>
Example: SecurityDoH._doh._tcp.local

Solution

Resource Records

- PTR: Service discovery & enumeration
- SRV: Service location (host + port)
  - <Instance>.<Service>.<Domain> [Class] [TTL] SRV <Priority> <Weight> <Port> <Target>
  - Target: Hostname offering the service (A/AAAA must resolve)
  - Example: HomeDoT._dot._tcp.local. 120 IN SRV 0 5 853 router.home.local.
- TXT: Service parameters (path, ALPN, etc.)
  - Standardized TXT Record Parameters: path, alpn, pri, domain, fp_sha256

Solution

Discovery Process

- 1. Service Advertisement:
  - EDNS resolver broadcasts PTR, SRV, TXT records via mDNS
- 2. Client Discovery:
  - Client → Network: Query _services._dns-sd._udp.local
  - Client ← Network: Response with service types (_dot._tcp, etc.)
  - Client → Network: Query specific instances
  - Client ← Network: Get SRV/TXT records + resolve addresses
  - Client → Resolver: Establish encrypted connection

Next Steps

- This issue will be considered by ADD?
- The solution makes sense?
- Next?