

# DHCP and Router Advertisement Options for Encrypted DNS Discovery

<https://tools.ietf.org/html/draft-btw-add-home>

January 2021

M. Boucadair (Orange)  
T. Reddy (McAfee)  
D. Wing (Citrix)  
N. Cook (Open-Xchange)  
Tommy Jensen (Microsoft)

# Overall Approach

- Rely upon existing mechanisms to distribute DNS server information: DHCP, DHCPv6, and RA
- Typical communication flow
  - Clients ask for one or more encrypted DNS (e.g., DoT, DoH) by *setting dedicated flags* in the options
  - Servers reply with ADN(s), a list of IP addresses, and a port number, if the requested encrypted DNS is supported
    - It is *RECOMMENDED to return both an ADN + a list of IP addresses*
    - *One or more* encrypted DNS types may be returned
    - These services may be bound to the *same or distinct IP addresses*
    - *Alternate port numbers* can be returned when default port number are not in use
    - If a list of IP addresses is returned, that list is *ordered*
    - Some recommendations to *optimize* the message size are included

# Main Changes Since IETF#108

- Return a list of IP addresses instead of relying upon legacy DNS options
  - This is to **avoid probing**
  - Useful if available encrypted DNS services are not available on the same IP address(es)
- **Generalize** the specification so that the options are not tied with a particular deployment
- **Clarify** the relationship with DEER

# Question #1: URI Templates in RA/DHCP?

- Why?
  - Provide a customized DNS configuration within a local network

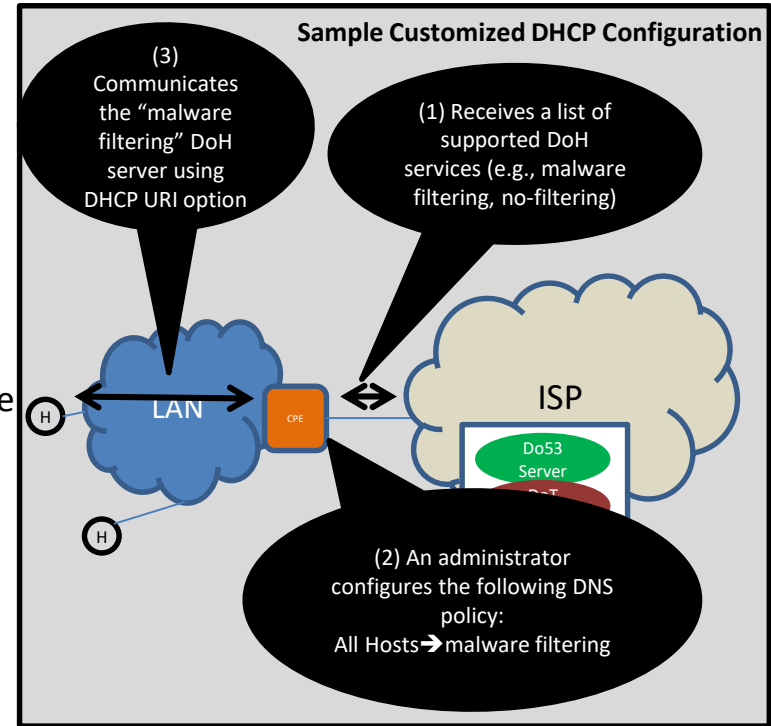
- There are trade-offs

- Some issues

- Create a **dependency** between DHCP servers (access routers) and DoH resolvers
    - May **increase the size** of RA/DHCP messages

- Some advantages

- Fills a void as there is **no standard** means to retrieve the URI information from the DoH server
    - Clients can **immediately use** the service(s); no need for extra queries to retrieve the URIs
    - Avoids Do53 lookups
    - Does **not interfere** with DNS exchanges to “customize” the available services
    - It is not subject to **external attacks**
    - Avoids the client to fallback to SUDN (opportunistic encryption)



## Suggestions:

- Define RA/DHCP options to convey URI Templates
- These options, when available, take precedence over DEER

# Question #2: No @List is Returned

- If the client receives a Do53 @List and an ADN, should the client use that list to resolve the ADN or should that list be assumed as locators to reach encrypted DNS servers?

## **Suggestion:**

- Recommend to always return a list of @es, unless Do53 and encrypted DNS terminate on the same @es

## **Motivation:**

- Optimize the message size

# Next Steps

- Consider adopting this document as a WG item
- Questions?