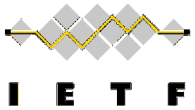
Analysis of DNS Forwarder Scenario Relative to DDR and DNR

Barbara Stark

Chris Box

IETF 111, July 2021



1

What this draft is

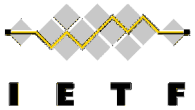
This draft analyzes the behaviors that residential end users and home network owners (e.g., parents of young children) might experience when operating systems and clients support DDR and/or DNR for discovery of encrypted DNS services and the CE router of the home network offers itself as the Do53 resolver.

This draft has two goals:

- determine if the analysis it provides is accurate
- and, if it is accurate, determine if the behavior is acceptable to the WG (and no action should be taken) or if there should be something done to properly address the use case (e.g., changes to either of the discovery mechanisms, implementation best practices, other?).

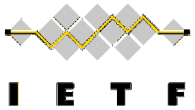
Why Home Network CE Routers do DNS Forwarding

- Provide local name resolution
- Captive portal (Note that [RFC8952] defines an architecture that does not rely on "breaking" DNS; however, there exist many legacy devices with captive portals that do rely on "breaking" DNS.)
- Provide filtering (e.g., parental controls) and DNS-based vulnerability assessment in the CE router. Note that [I-D.ietf-add-requirements] describes this sort of filtering and monitoring behavior as an attack; nonetheless, this functionality is popular with many people -- especially parents.
- Caching responses to improve DNS performance



Assumptions

- Common OSs support both DNR and DDR
- Some applications (e.g., browsers) support DDR
- No Certificate Authority will sign a certificate with a private IP address in a SAN

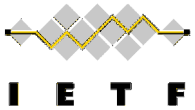


Scenario 1: CE Router not updated

Result: The OS/app will not discover a local Encrypted Resolver. OS/app may subsequently use some non-standard mechanism to select an Encrypted Resolver (we really have no idea what they'll do).

Note: the DDR and DNR proposals in their current form do not satisfy the requirement "R4.2 Achieving requirement 4.1 SHOULD NOT require any changes to DNS forwarders hosted on non-upgradable legacy network devices."

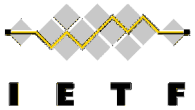
Note: non-upgraded legacy routers will not satisfy the [I-D.ietf-add-ddr] requirement that a "DNS forwarder SHOULD NOT forward queries for "resolver.arpa" upstream."; but this doesn't change the Result.



Scenario 2: Updated CE router provides DNR

Results:

- OSs might use the Encrypted Resolver, if they feel like it; but, then again, they might not.
- Applications that try "resolver.arpa" will not use the Encrypted Resolver, because that will fail as in Scenario 1.
- Local name resolution is broken?¶
- Legacy captive portal is now broken? // initial testing suggests this may be ok in many cases
- Filtering in the CE router (parental controls and other security mechanisms enabled by the home network owner) is now broken
- Any filtering deployed in the core network resolver continues to operate
- No local caching

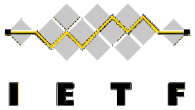


Scenario 3: Updated CE router supports opportunistic encryption to its DNS forwarder and provides its info in DNR and DDR

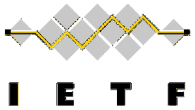
Note: These upgrades are estimated to be complex.

Results:

- Some OSs and applications accept DDR Opportunistic Discovery, resulting in use of the CE router's Encrypted Resolver.
- Some OSs and applications do not.
- Across a range of households, and even within a single household, there is inconsistent behavior.



Is the analysis accurate?



If the analysis is accurate, what are the next steps?

- No action (accept the breakage and keep going)?
- Changes to DDR or DNR?
- Implementation best practices for applications that want to accommodate this use case?
- Other?