Encrypted DNS Discovery and Deployment Considerations for Home Networks

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

July 2020

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

Agenda

- Scope & Approach
- Main Changes since IETF#107
- One Discussion Point
- Next Steps

Target *add* Work Item

Excerpt from the WG Charter:

*"Define a 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**"*

With a focus on home networks deployment specifics

Home Network Specifics

- The CPE is ***key*** to, e.g.,
  - Provide local services
  - Apply per-device policies
  - Isolate infected home devices
  - Offer better localized caching
  - Ensure IPv4 service continuity
  - Collaborate with the network to filter DDoS attacks close to the source
  - …

Approach

- Rely upon existing mechanisms to distribute DNS server information (DNS authentication domain name (ADN))
  - DHCP, DHCPv6, and RA

- These mechanisms can be used:
  - Between the CPE and an ISP's network and/or
  - Within the home network
    - Between the CPE and an internal router
    - Between endhosts and a router/CPE

- Typical communication flow:
  - Clients ask for one or more Encrypted DNS (e.g., DoT, DoH)
  - Servers reply with ADN(s) if the requested Encrypted DNS is supported

Main Changes Since IETF#107

- **Pick** one solution for the discovery of URI templates
  - Dedicated DHCP/RA option vs. Directly from the server
- **Simplify** the procedure for involving a forwarder in the CPE
- Add a new section to discuss **legacy** CPEs
- Update the **Security** section to discuss both active and passive attacks (RFC3552)

Main Changes Since IETF#107 (1)

- **Pick** one solution for the discovery of URI templates
  - ~~Dedicated DHCP/RA option vs.~~ Directly from the server

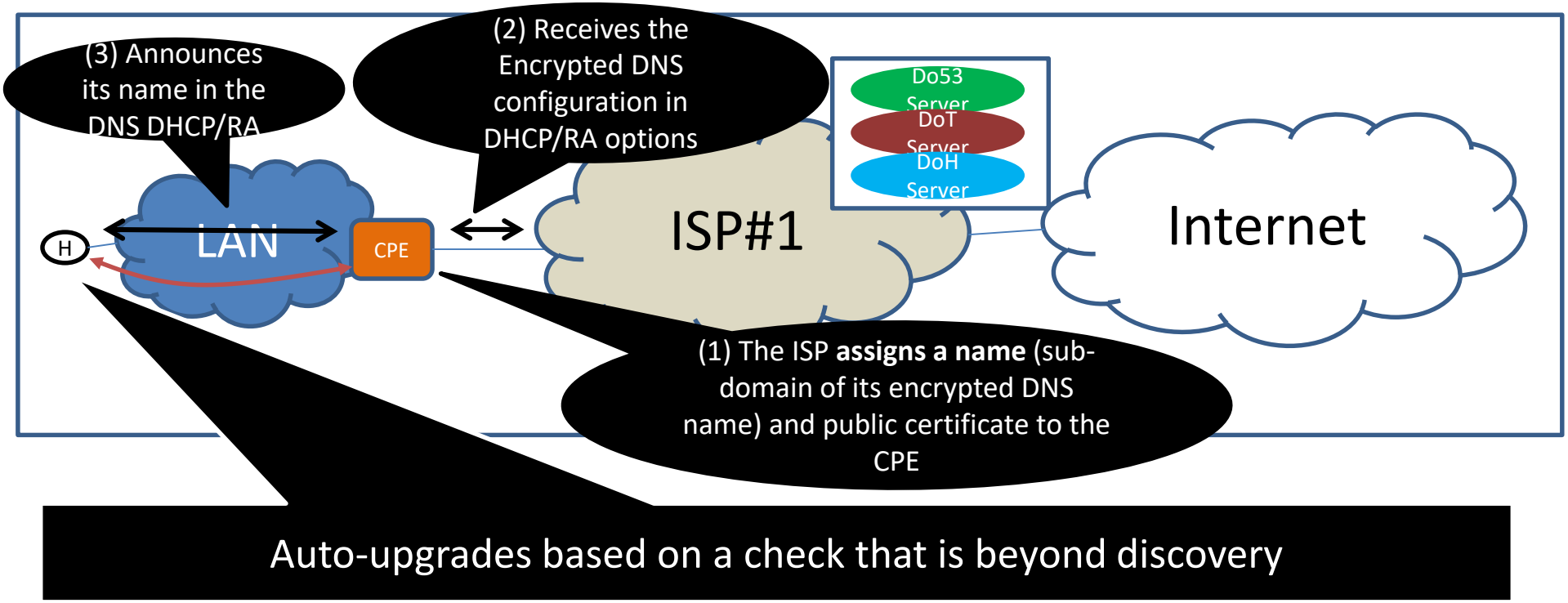
https://doh.example.com/.well-known/resinfo

The ADN discovered using DHCP/RA

Well-known URI requested in draft-btw-add-rfc8484-clarification

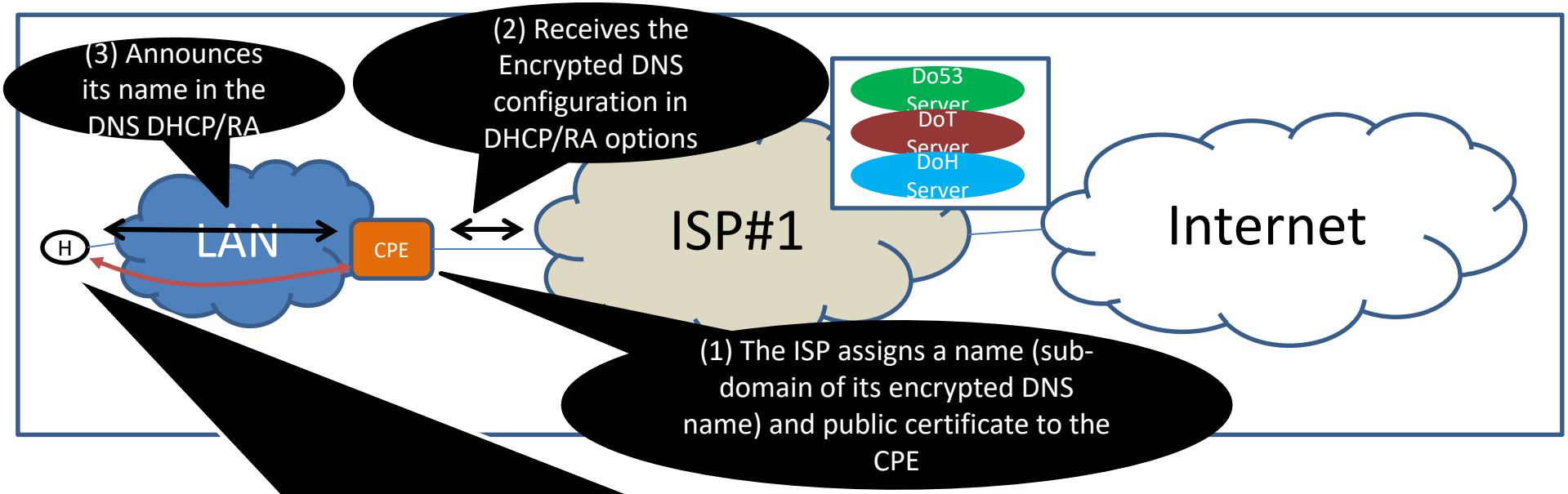
Main Changes Since IETF#107 (2)

- **Simplify** the procedure for involving a forwarder in the CPE



Main Changes Since IETF#107 (2)

- **Simplify** the procedure for involving a forwarder in the CPE



Auto-upgrades, **e.g.,** because left-most label of the pre-configured AND would match the subjectAltName value in the server certificate (CPE)

Left-most label matching is permitted if the domains and CPE are managed by the ISP and an (out-of-band) agreement with the client to enable wild-card white-listing for the ISP managed subdomains

Discussion Point: Locating Services

- **Current design**: The ADN and a list of IP@es are returned using separate options:
  - ADNs are returned using a NEW option
  - The list of IP@ is returned using existing DNS options
  - *Straightforward* if all services terminate on the same @
    - If not, and if the client requested more than one service, the client will need to try to list to find the @ that corresponds to each DNS service: *Inefficient?*
- **Alternate design**: Return both the ADN and a list of @es in the NEW option
  - Solve the above inefficiency
  - But *exacerbates the message size* if all services terminate on the same @

Any preference?

Some Frequent Questions (1)

Does the I-D mandate the CPE to be a managed CPE?	• ***No***. The options can be supported by managed and unmanaged CPEs
Does the I-D impose an ISP's Encrypted DNS server to be returned in the options?	• ***No***. The server can be operated by the ISP, public, private, or local
Does the I-D mandate the CPE to always relay the DNS information received from the access network?	• ***No***. This is configuration-based
Does the I-D mandate the CPE to always behave as a forwarder?	• ***No***. This is deployment-specific and configuration-based

Some Frequent Questions (2)

Can DoH/DoT servers be hosted on CPEs?

- ***Yes***. CPEs are hardened to host network security services, see for example, https://prplfoundation.org/project/prplwrtt, https://iopsys.eu/product/,https://securehomeplatform.mcafee.com, https://securingsam.com/

Can CPEs be upgraded?

- ***Not every CPE can be upgraded but CPEs can be updated***
  - This is the model that is usually followed for managed CPEs.
  - In addition to the use TR-69/TR-369, LxC/Docker is also considered to host the network/application services on CPE to ease upgrade and avoid failures; see for example technicolor and openwrt-funding-round-two

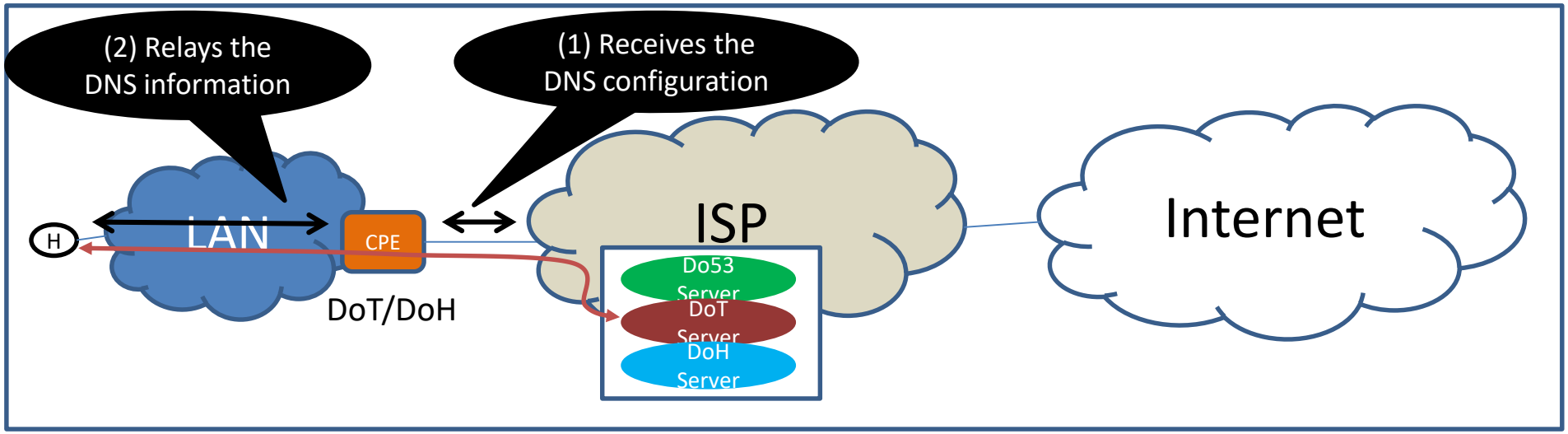
Next Steps

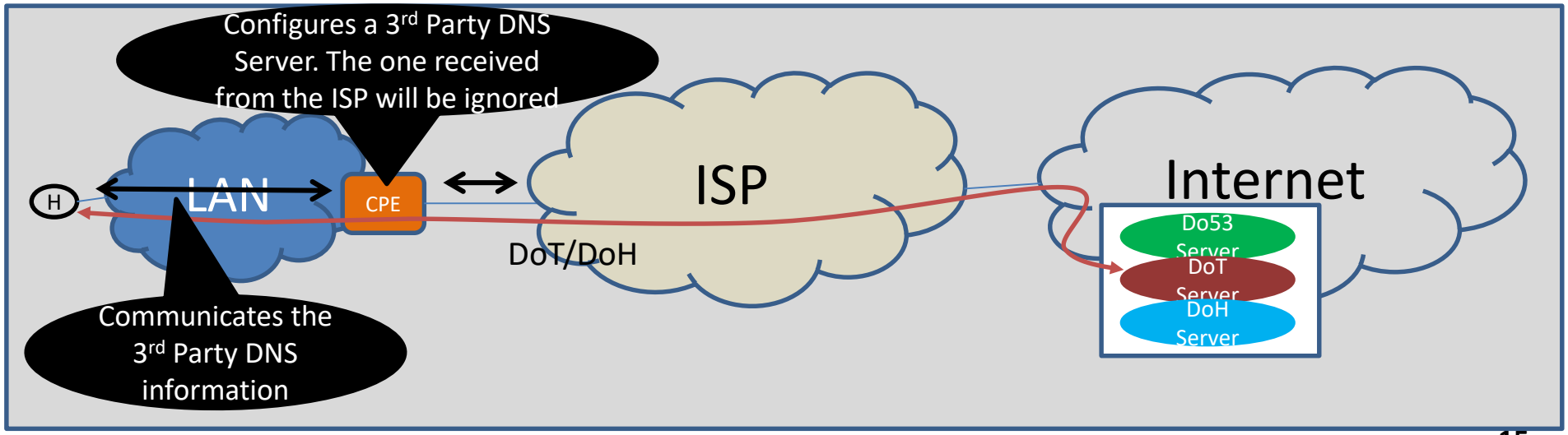
- Consider adopting this document as a WG item

- Questions?

Appendix

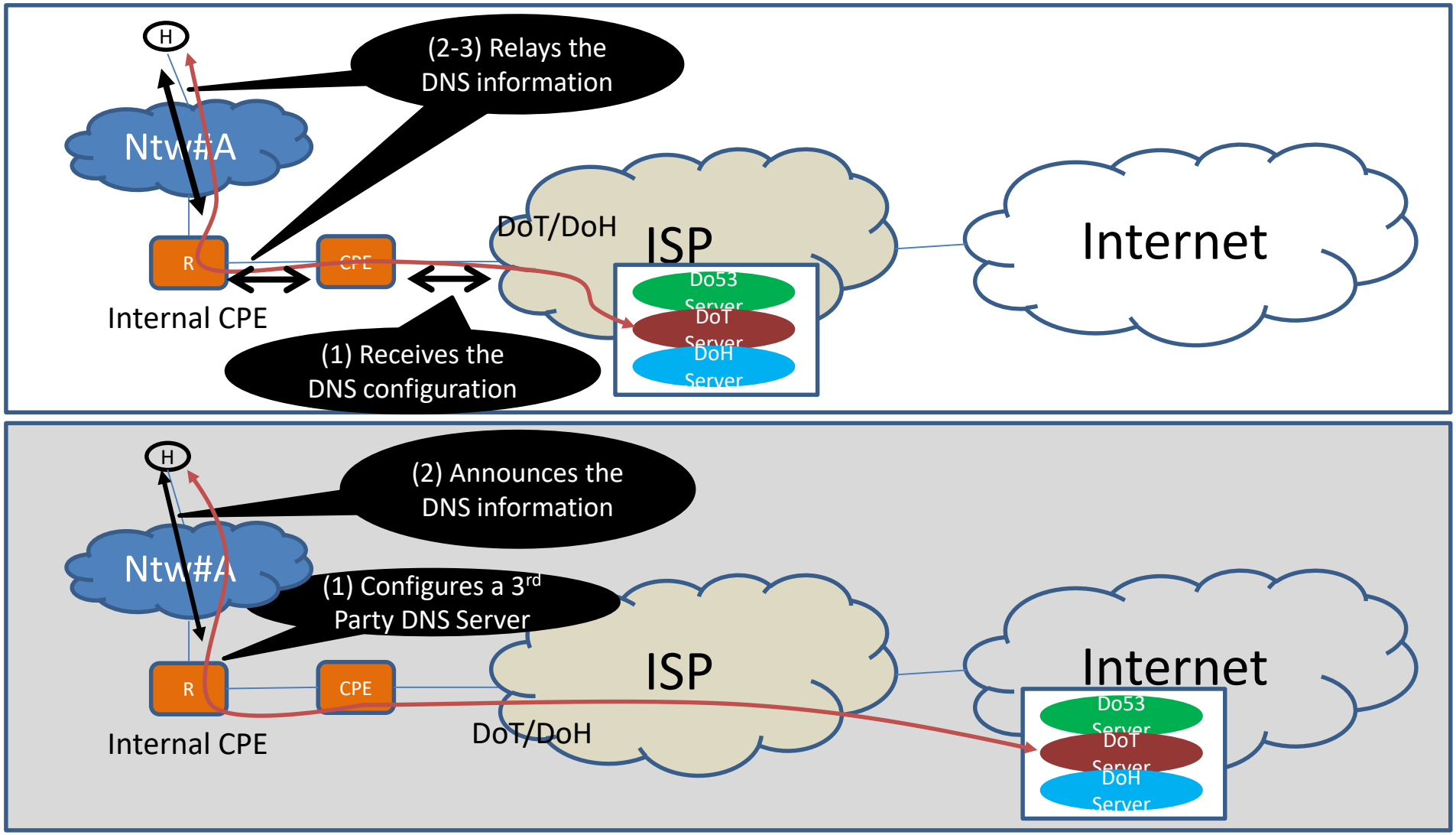
Sample Encrypted DNS Deployments: Managed CPEs





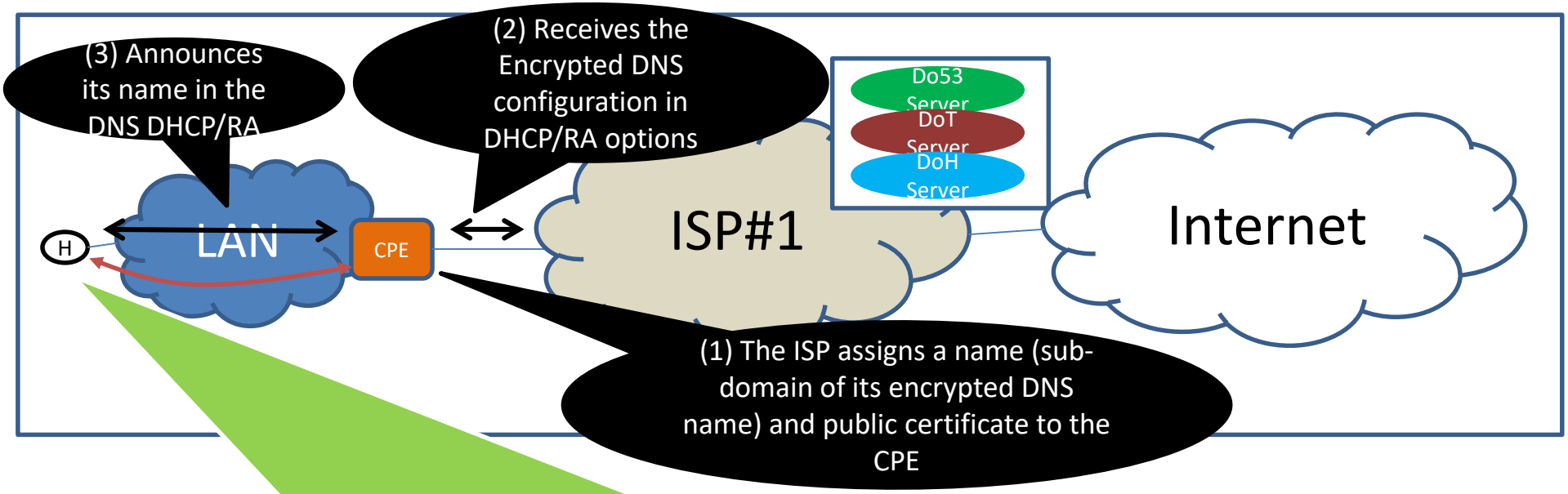
DoT/DoH: Means DoT and/or DoH

Sample Encrypted DNS Deployments: Unmanaged CPEs



Verified Resolvers

- **Simplify** the procedure for involving a forwarder in the CPE



Auto-upgrades if the client succeeds to verify the server's signatory as [draft-reddy-add-server-policy-selection-03]

Main Changes Since IETF#107 (3)

- Add a new section to discuss **legacy** CPEs

- Fallback to use the special-use domain name to discover the DoH/DoT server and the RESINFO RRtype to retrieve the list of supported DoH services
  - I-D.pp-add-resinfo

- ***The DHCP/RA option to discover ADN takes precedence over special-use domain name*** since the special-use domain name is susceptible to both internal and external attacks whereas DHCP/RA is only vulnerable to internal attacks