A visual guide to the ADD Requirements Draft

https://tools.ietf.org/html/draft-box-add-requirements-00

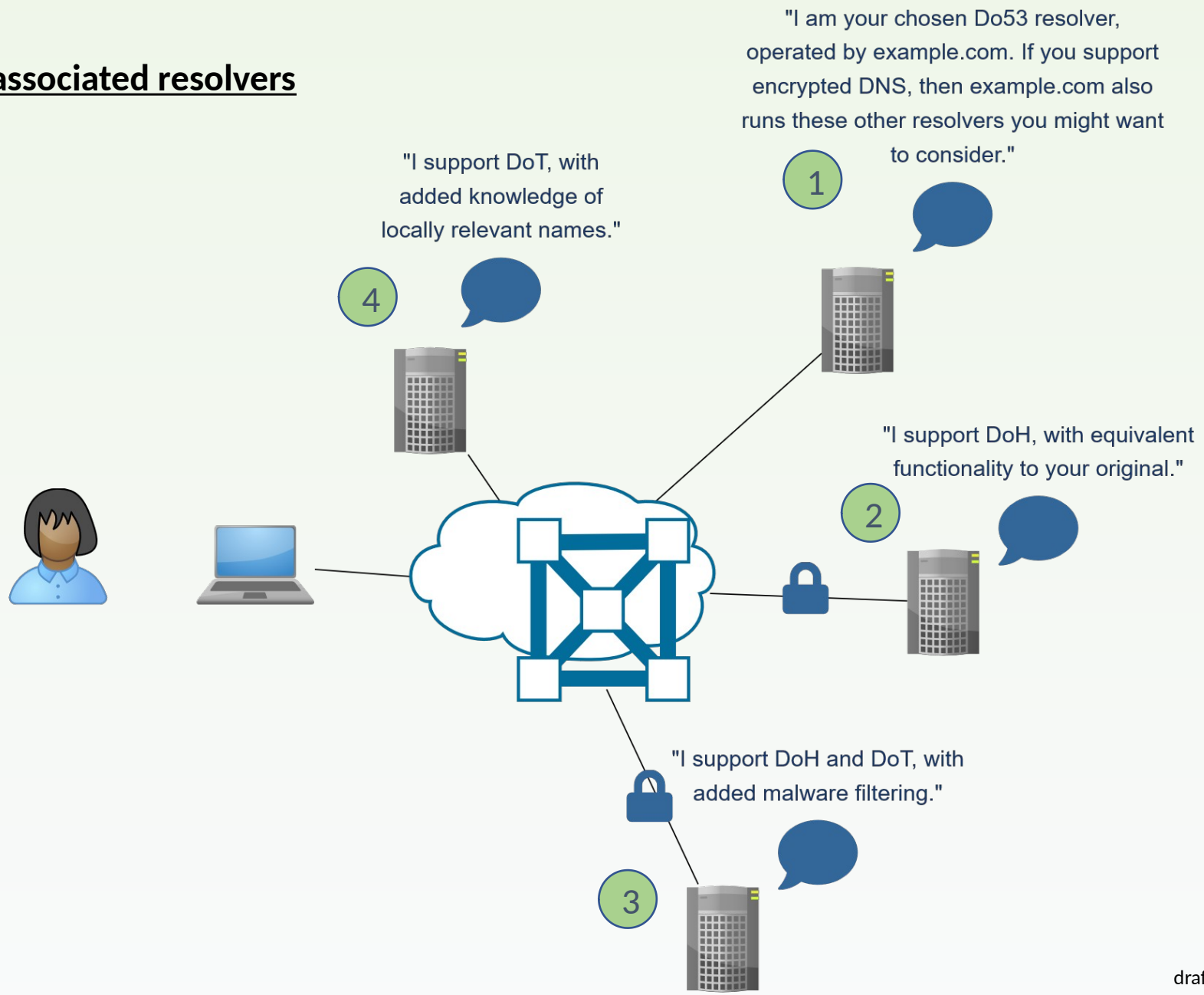
https://github.com/ietf-wg-add/draft-add-requirements/

C Box, T Pauly, C Wood, T Reddy
September 10 2020

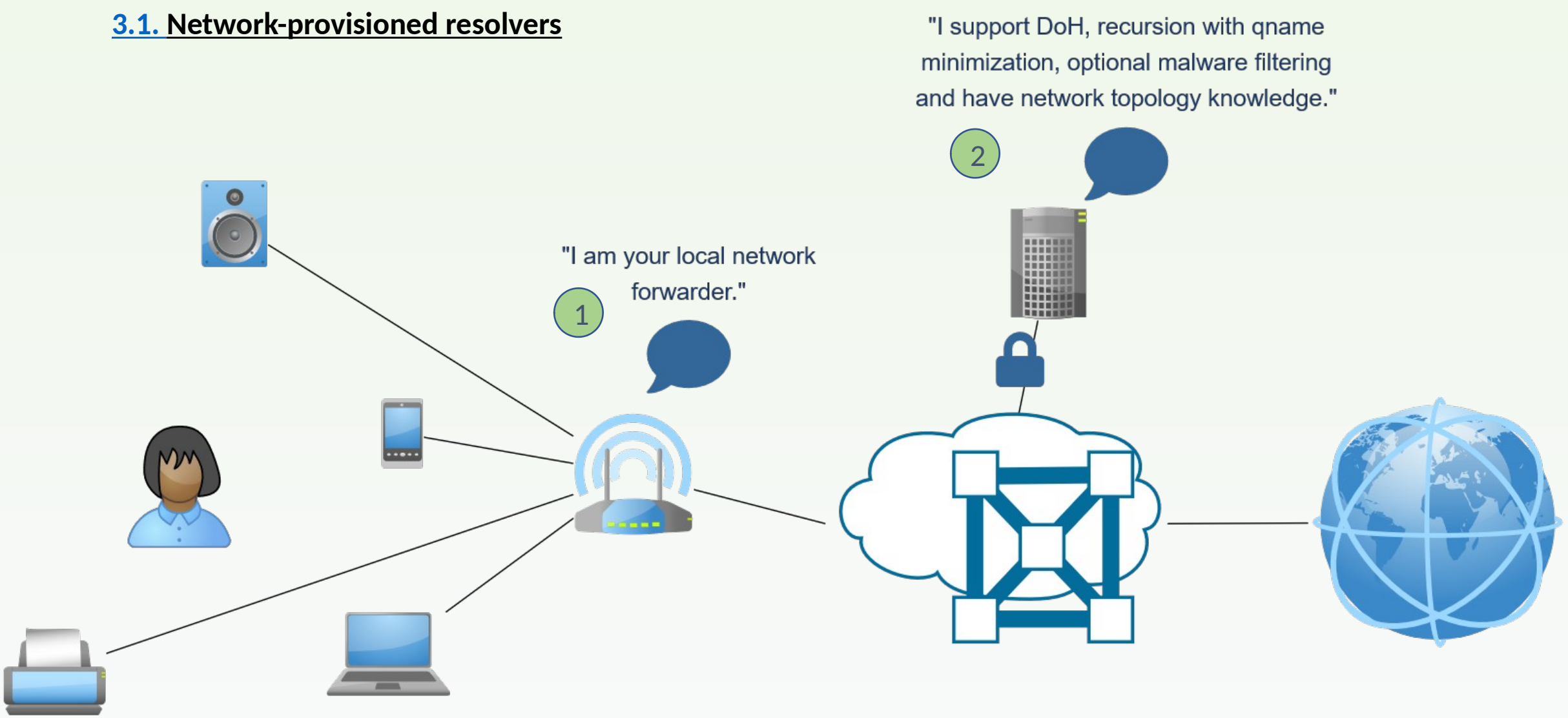
Introduction

- How we got here
- Current structure of the draft ---------->
- An alternative: Daniel Migault's pull request
  - section 3: Discovery of associated resolvers
  - section 4: Direct Discovery of resolvers
  - section 5: Discovered information

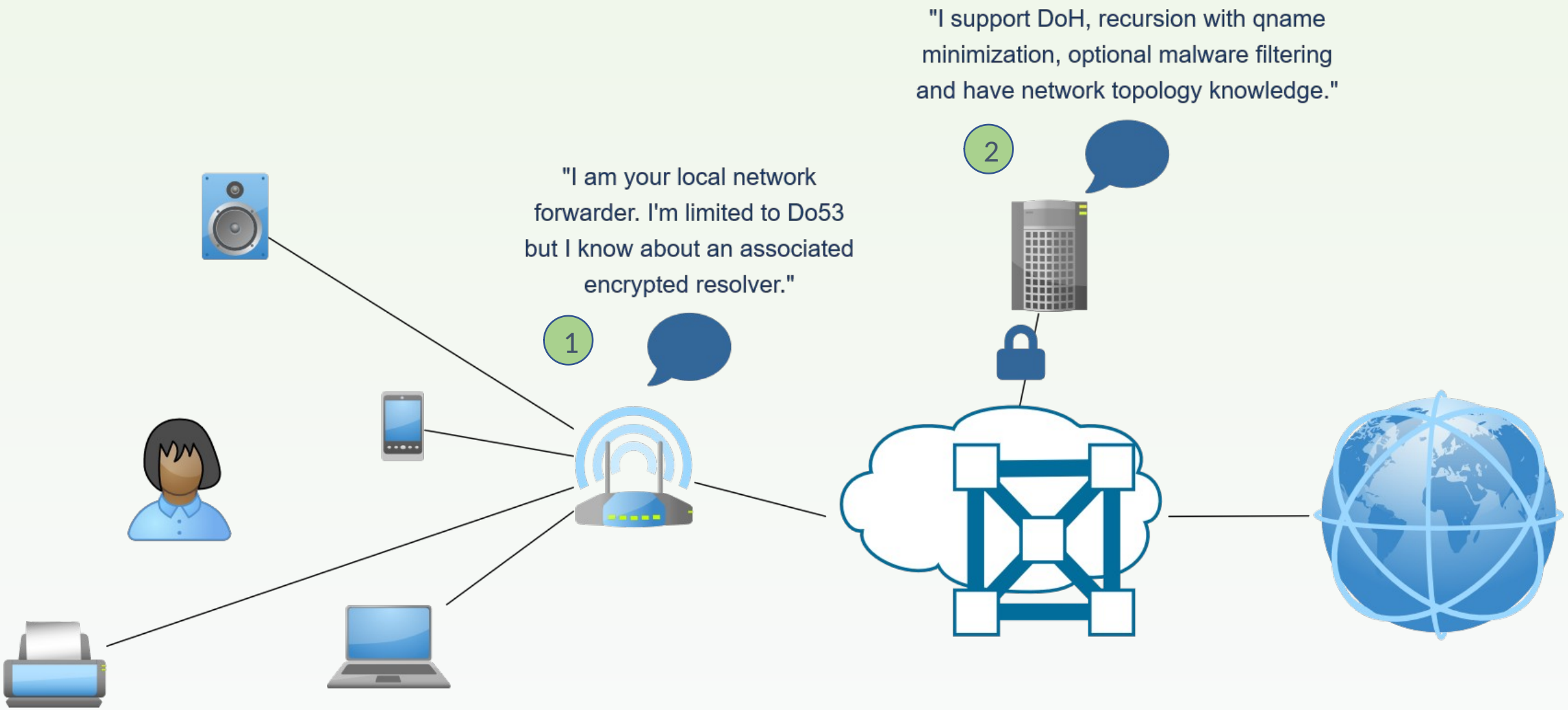
3. Discovery of associated resolvers



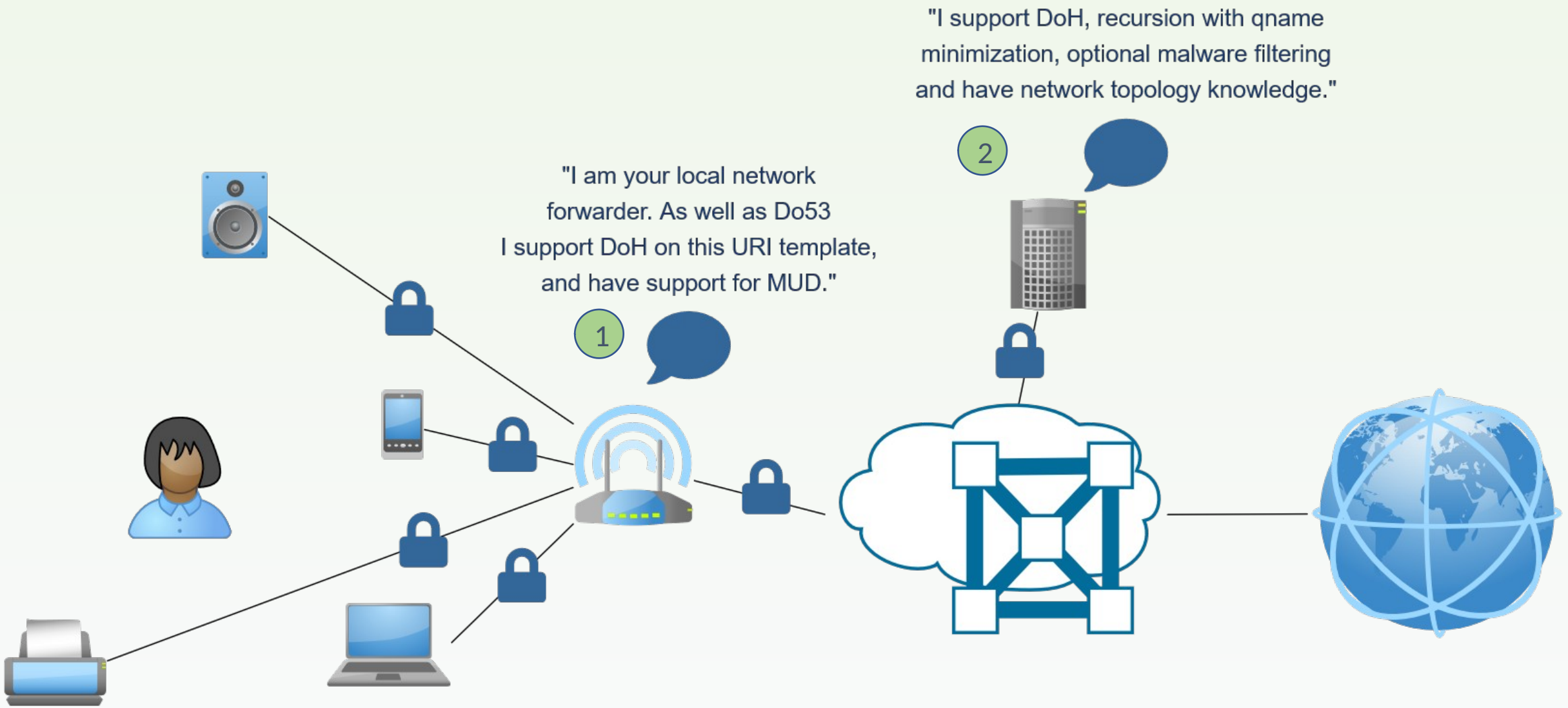
3.1. Network-provisioned resolvers



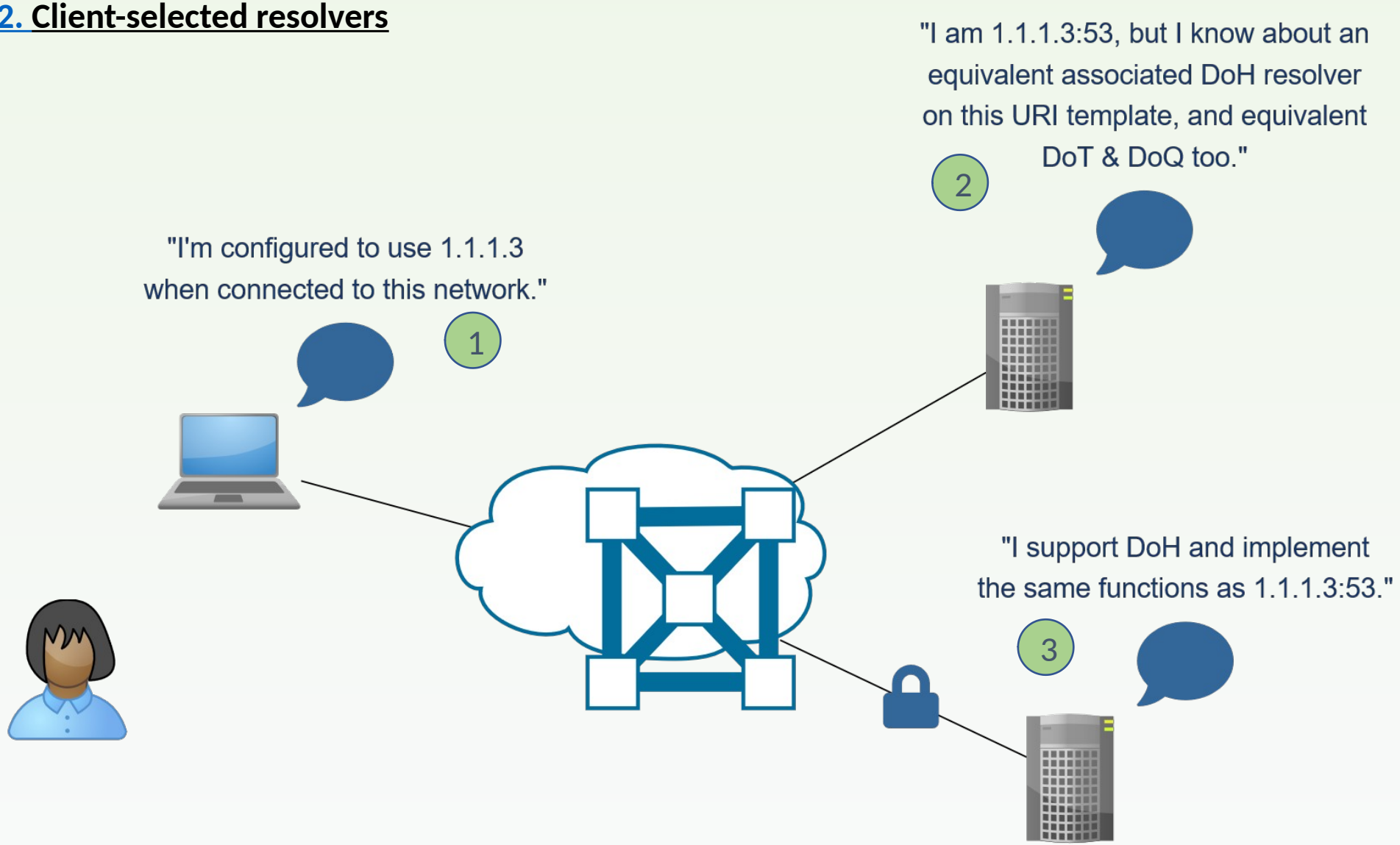
3.1.1. Unencrypted forwarder



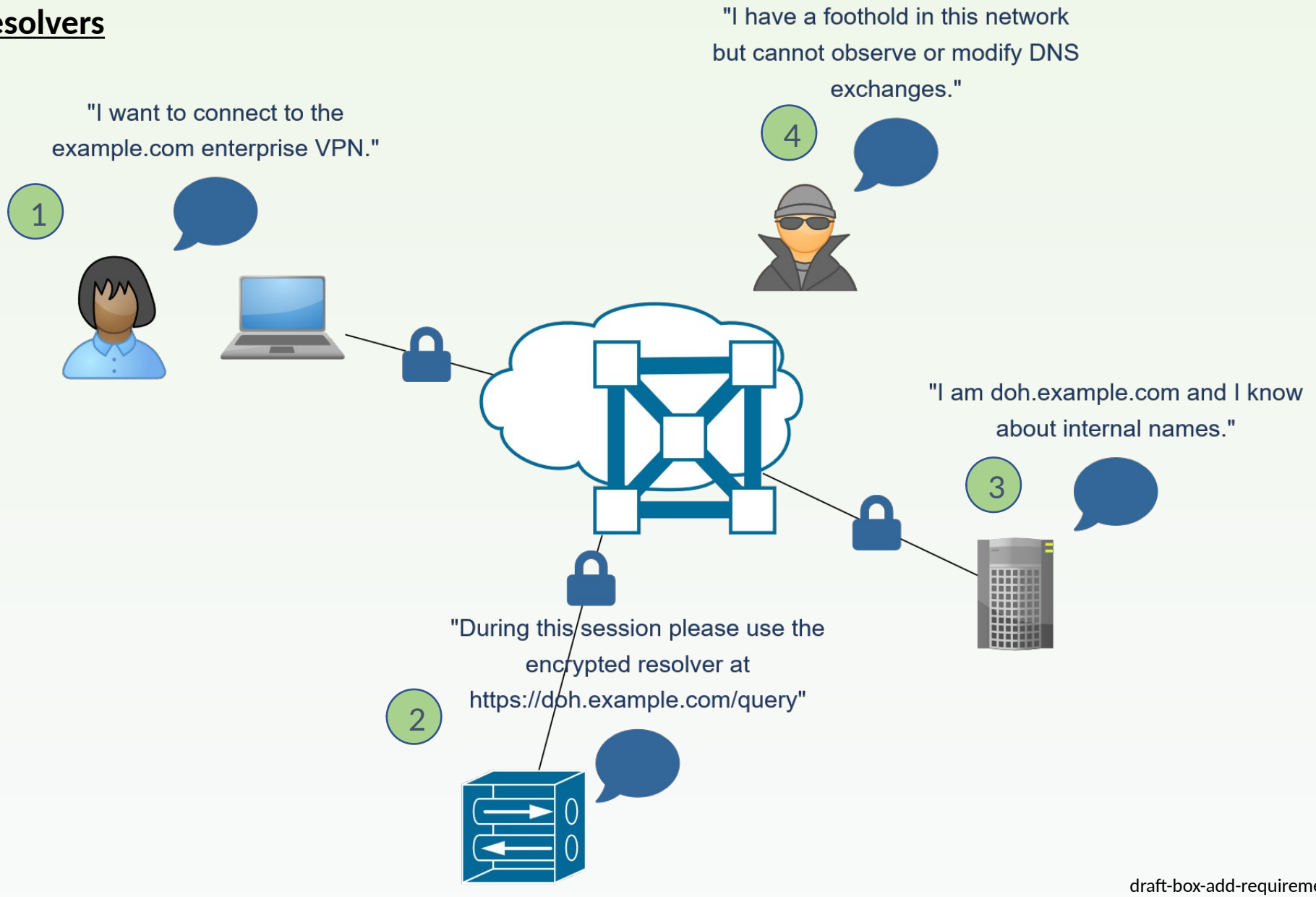
3.1.2. Encrypted forwarder



3.2. Client-selected resolvers



3.3. VPN resolvers

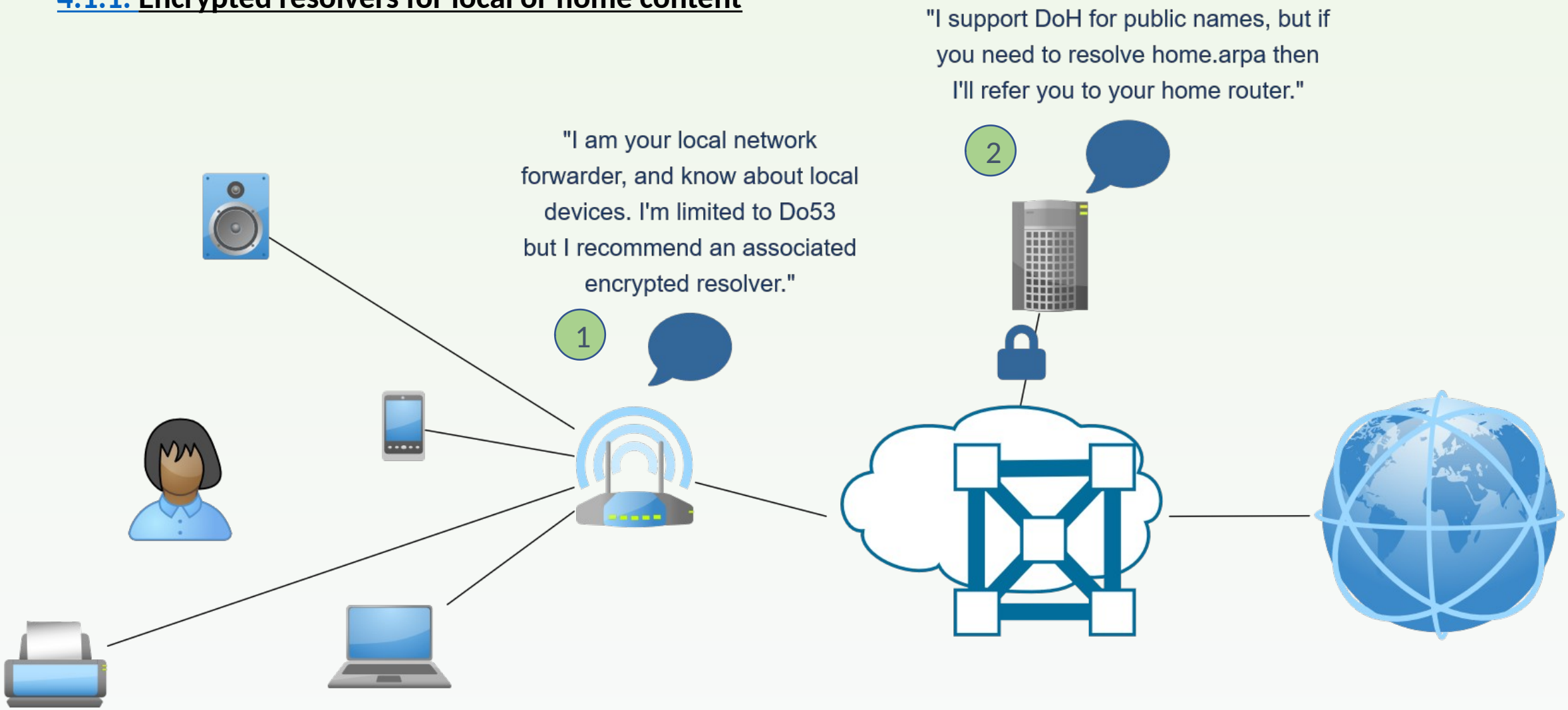


4. Discovery of limited domain resolvers

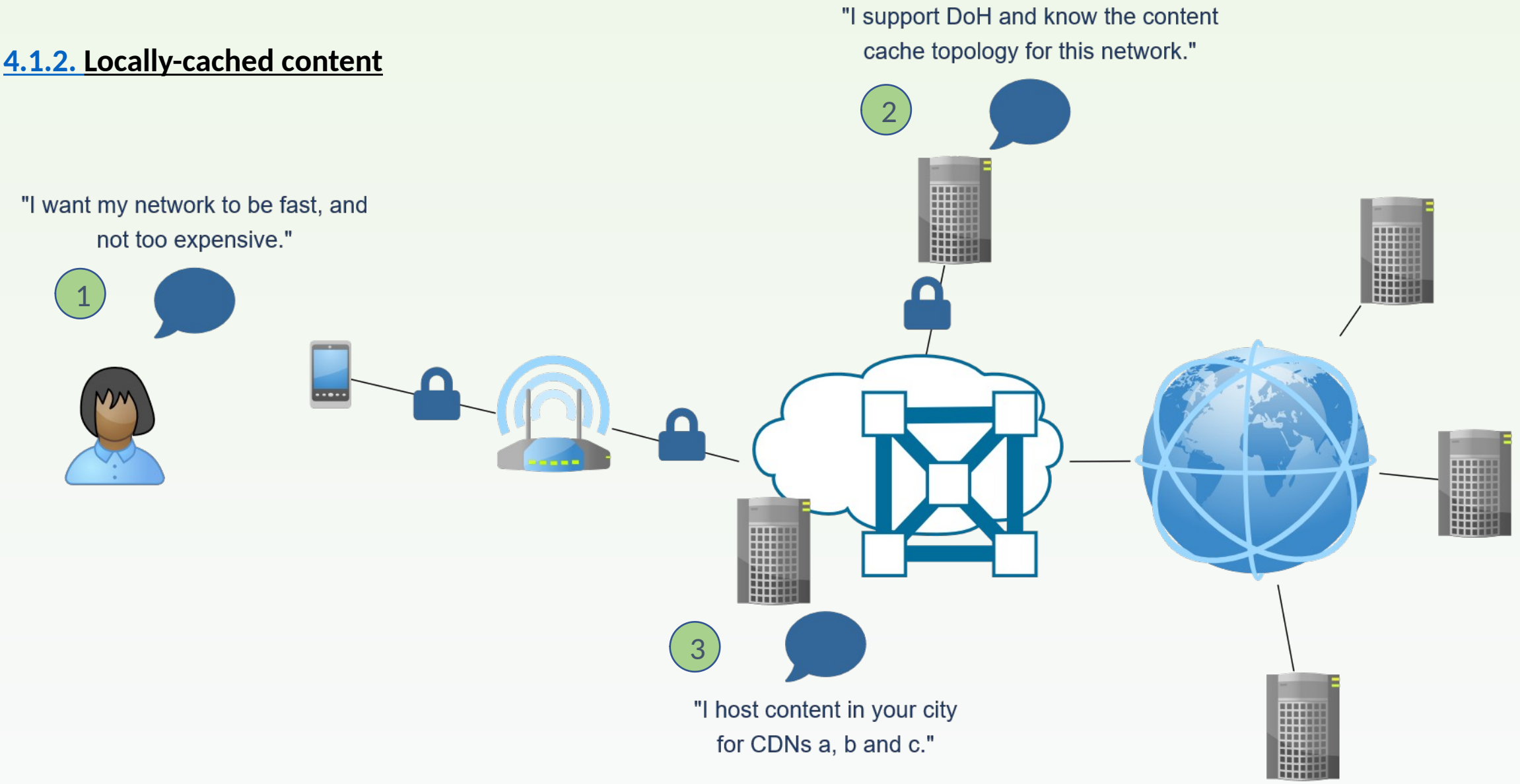
- Discovering an encrypted resolver for a subset of names allows a client to perform Split DNS while maintaining the benefits of encrypted DNS.
- A client could use a client-selected encrypted resolver for public domains, but use a different encrypted resolver for enterprise-private domains.
- Such domain-specific resolver discovery mechanisms additionally need to provide some information about the applicability and capabilities of encrypted resolvers.

The next three slides cover mapping between a locally-hosted domain and a resolver, then there's one on content providers.

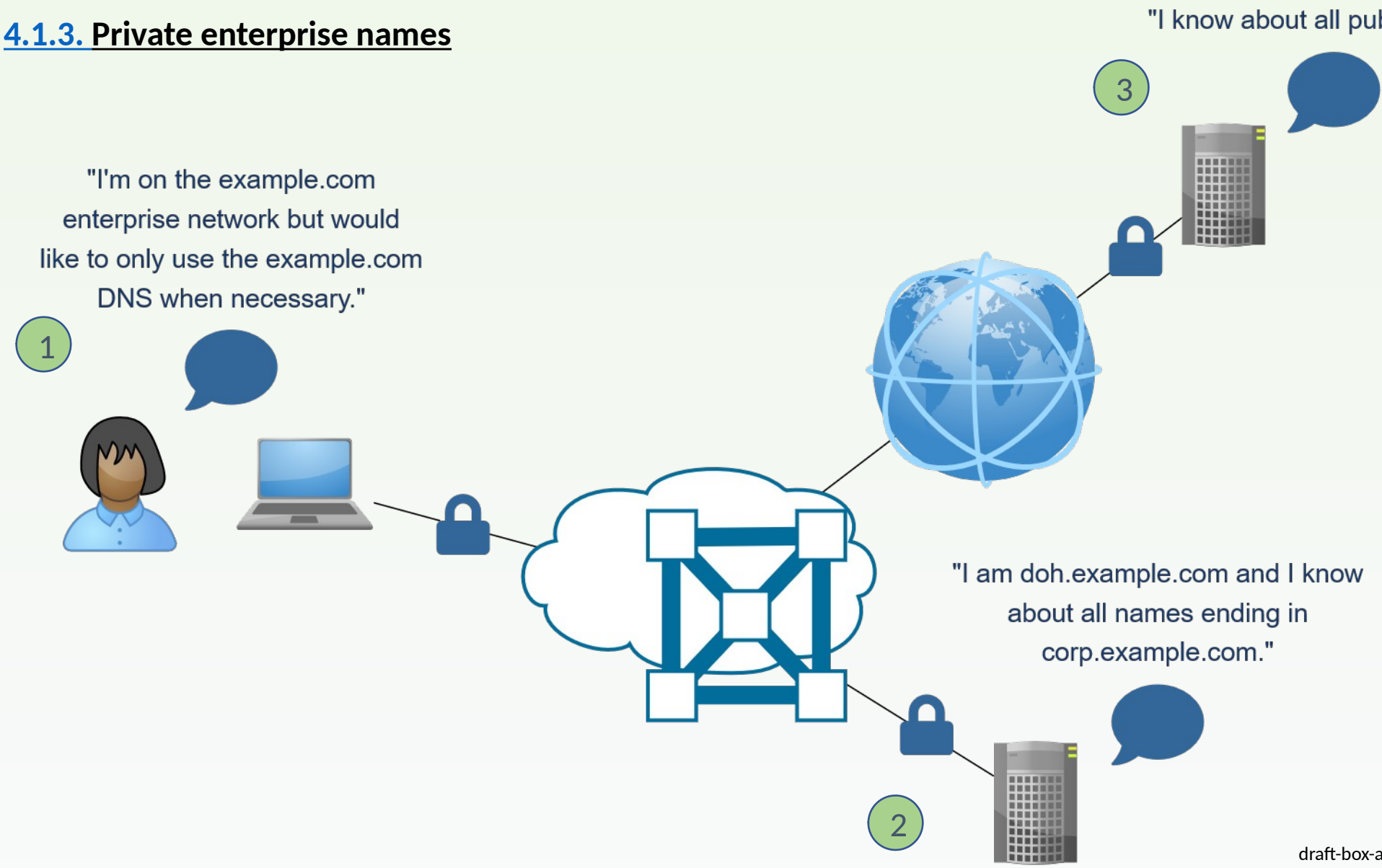
4.1.1. Encrypted resolvers for local or home content



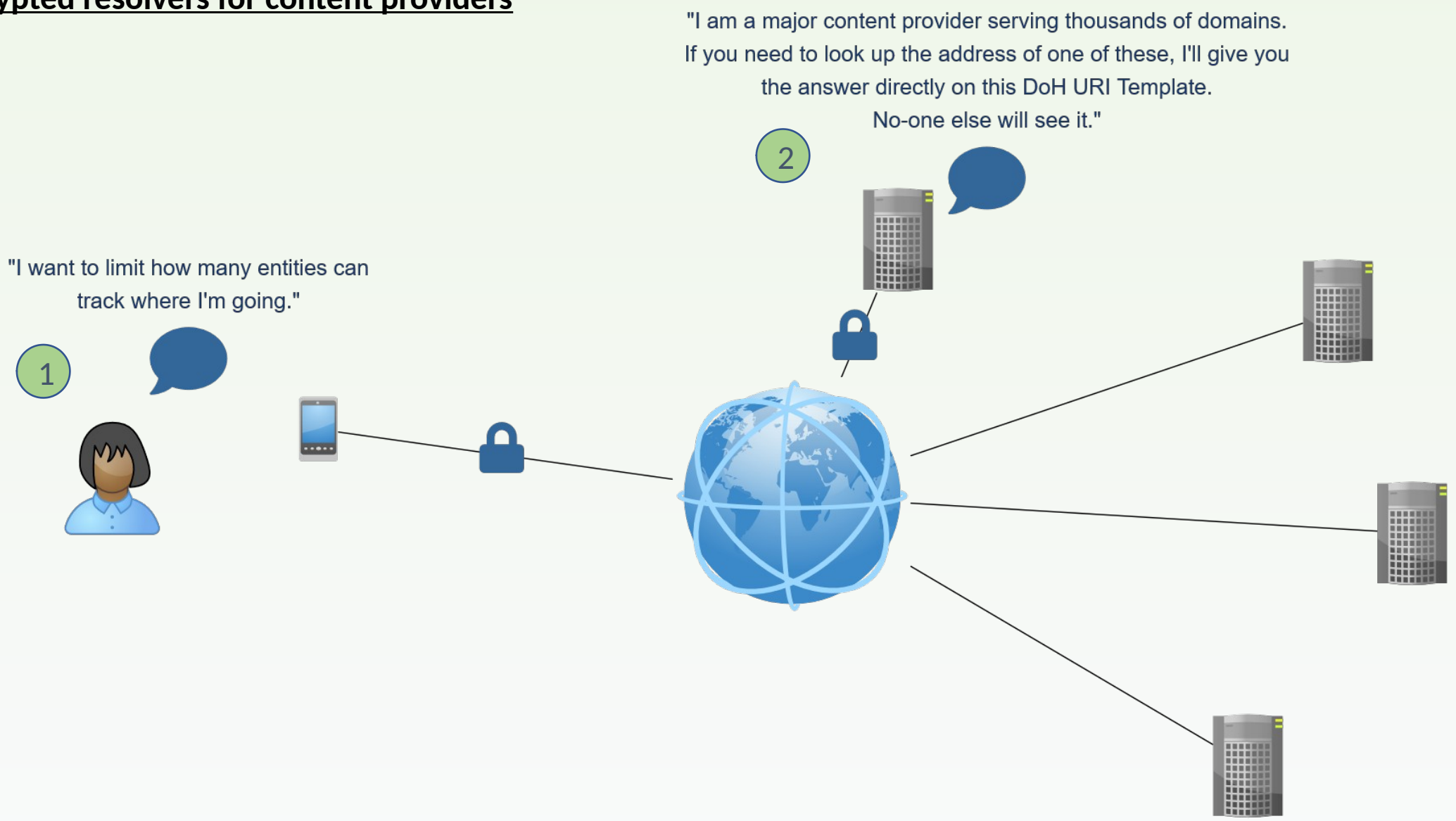
4.1.2. Locally-cached content



4.1.3. Private enterprise names



4.2. Encrypted resolvers for content providers



5. Privacy and security requirements

- Clients cannot assume the network doesn’t have an attacker
- Attackers must be prevented from:
  - Redirecting secure DNS to themselves
  - Overriding user preferences
  - Causing clients use a resolver lacking authenticated delegation
  - Influence discovery to use a resolver not involved with service delivery
- Standards must not place requirements on clients to select particular resolvers
- Opportunistic encryption is not recommended
- If encrypted DNS fails to work, local client policy decides whether to:
  - Fail open by using unencrypted DNS
  - Fail closed
  - Present a choice to the user
- Failing open is generally not recommended, except for cases such as captive portal detection

Improving the draft

Please file issues in the repo, or comment on existing ones.

Repo link: https://github.com/ietf-wg-add/draft-add-requirements/

There are many issues already! 21 currently open. But more issues = better review. https://github.com/ietf-wg-add/wg-materials/blob/master/Using%20Github.md says "*make them short and limited to one specific item*".

Some of these require wider debate, e.g. on list and at this meeting.

As improvements are made, this always contains the HTML formatted copy of the latest repo text: https://ietf-wg-add.github.io/draft-add-requirements/draft-add-requirements.html

Revisions will of course be published to datatracker: https://datatracker.ietf.org/doc/draft-box-add-requirements/