

Homelab DNS

HLB - September 2025

25 September 2025

Overview

- Part A 🍉
 - Overview of DNS
 - Two types of DNS servers
 - Overview of DNS Queries
- Part B 🍦
 - Advantages to your own local resolver
 - Hosting and Self-Hosting Considerations
- Out of Scope
 - Encrypted DNS (e.g., DoH, DoT) and DNSSEC
 - Firewalling to redirect DNS (e.g., DNAT/Masquerading NAT rules)
 - Running your own authoritative server (e.g., BIND, SOA records, etc.)

What is DNS?

- Hierarchical and distributed system
- Translates human readable names into numerical IP addresses (and other record types)
- Core component and early part of the internet (Introduced 1983-1985)
- Port 53 (default)

Define “DNS Server”... 🤔

Two Types of DNS Servers in Homelab Contexts

- Recursive DNS servers / resolvers
 - Responds to queries from clients and fetches DNS records
 - May query other recursive resolvers
 - May cache DNS responses

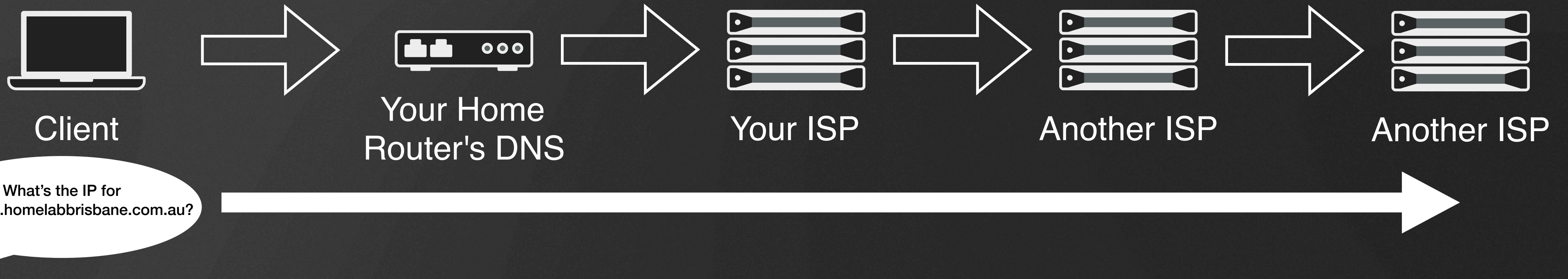
Define “DNS Server”... 🤔

Two Types of DNS Servers in Homelab Contexts

- Authoritative DNS servers
 - “Owns” (is the authority for) the specific DNS zone
 - Answers queries from recursive DNS resolvers
 - (Including root servers and TLD servers for the purposes of this presentation)

Resolvers

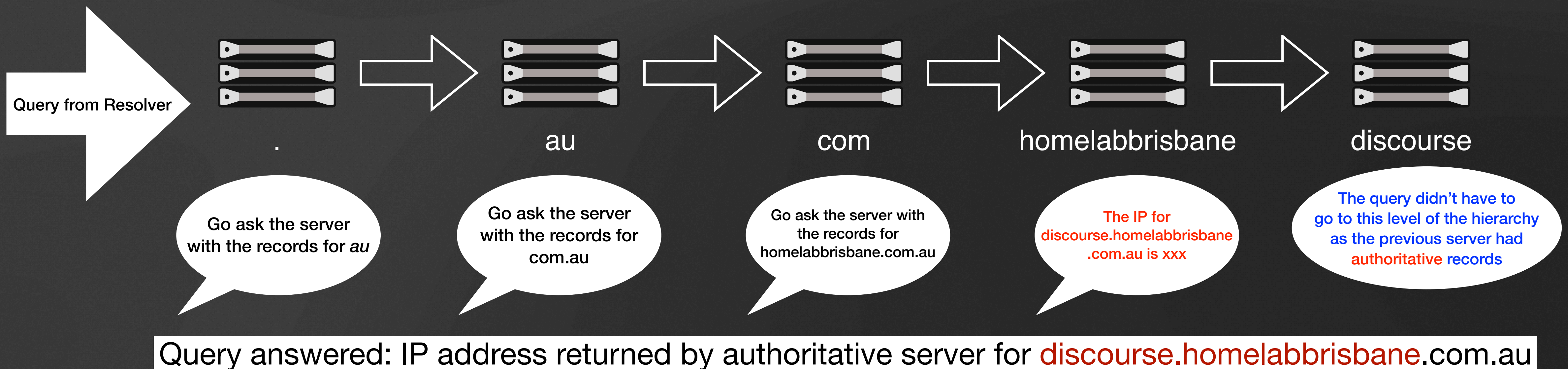
- Takes requests from clients (or other resolvers) and forwards them to authoritative servers, if necessary
- e.g., Your laptop queries your local “DNS server” (your router, a resolver), which queries your ISP’s DNS resolver, which may query another upstream provider’s DNS resolver....



Authoritative Servers

What's the IP for discourse.homelabbrisbane.com.au?

- “Owns” the records in each DNS zone (level of the hierarchy; e.g., au, com, homelabbrisbane)
- May be authoritative for one or more levels in the DNS hierarchy
- Note: Simplified for the purpose of this presentation, including root servers and TLD roots in the definition of authoritative servers



DNS Query Flow

- Clients query resolvers, resolvers work “upstream” to authoritative servers until the zone’s “owner” is located
- Very rare for queries to work their way up to the root servers
 - DNS queries are cached
 - e.g., You visit TikTok every half hour. Your phone, your router, your ISP, etc. all have cached the DNS entries. No need to do DNS lookups all the way up and down the hierarchy
 - e.g., Your ISP’s resolver is asked for DNS records for uncommon-website.com.au. Your ISP’s resolver can direct the query immediately to the .com.au authoritative server
 - Some resolvers may also be authoritative for DNS zones
 - e.g., Telstra’s DNS resolver is asked for DNS records for xyz.com.au, and that domain’s DNS is hosted by Telstra -> authoritative records returned immediately

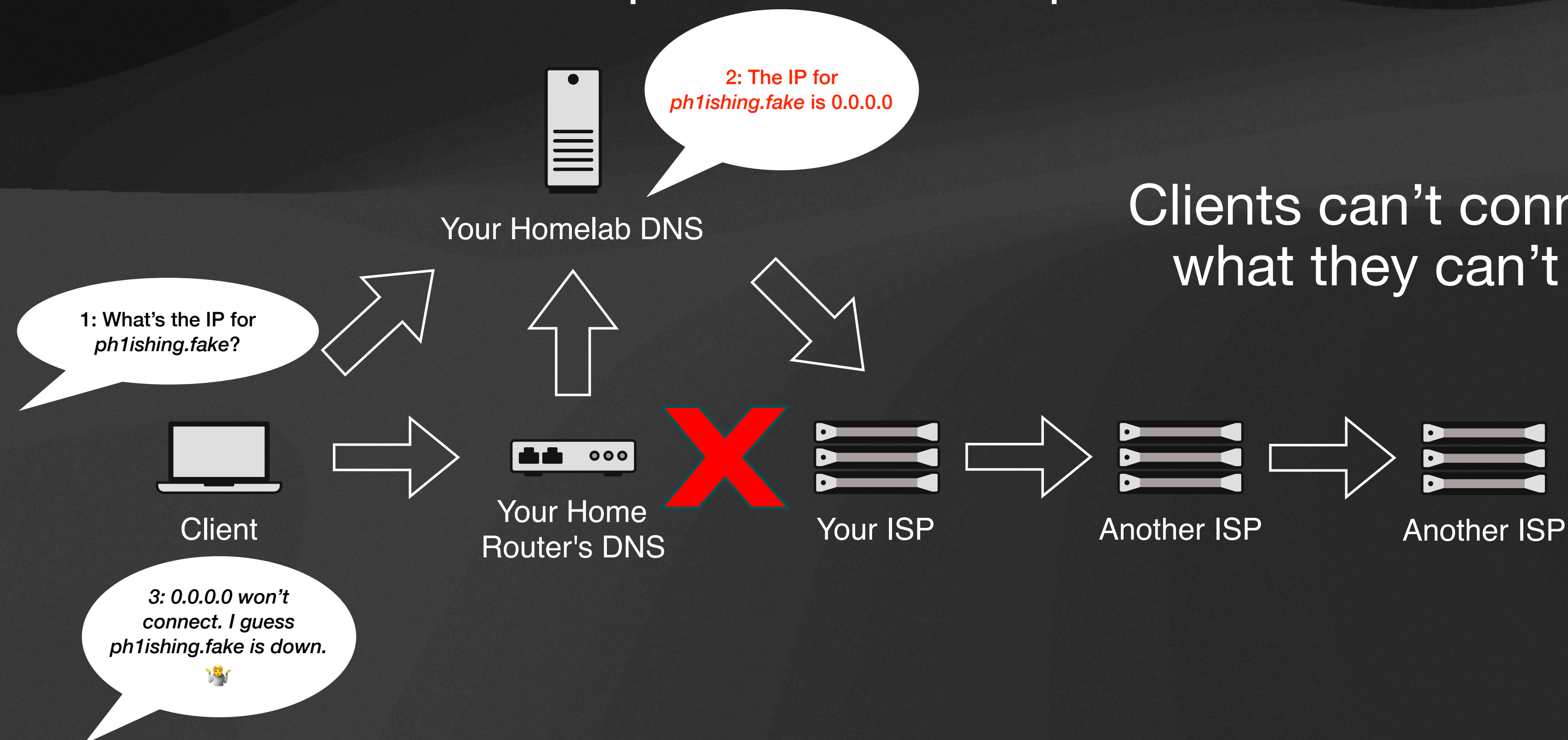
So?

What does this have to do with my homelab?

- Ad blocking / anti-malware / parental controls / anti-telemetry
- Increased network visibility
- DNS related hosting & self-hosting considerations
- Misconceptions & closing notes

Ad Blocking / Anti-Malware / Parental Controls / Anti-Telemetry

- Local resolver to replace or sit upstream of your router can return “authoritative” responses to DNS queries...



Clients can't connect to what they can't find.

Blocklists

How Does My Local Resolver Know What to Block?

- Plenty of free block lists available, e.g.,
- Hagezi blocklist(s)
<https://github.com/hagezi/dns-blocklists>
- OISD blocklist(s)
<https://oisd.nl/>
- EasyList(s)
<https://easylist.to/>
- Steven Black’s Blocklist(s)
<https://github.com/StevenBlack/hosts>
- Note: Lots of overlap between lists - experiment and see what suits you

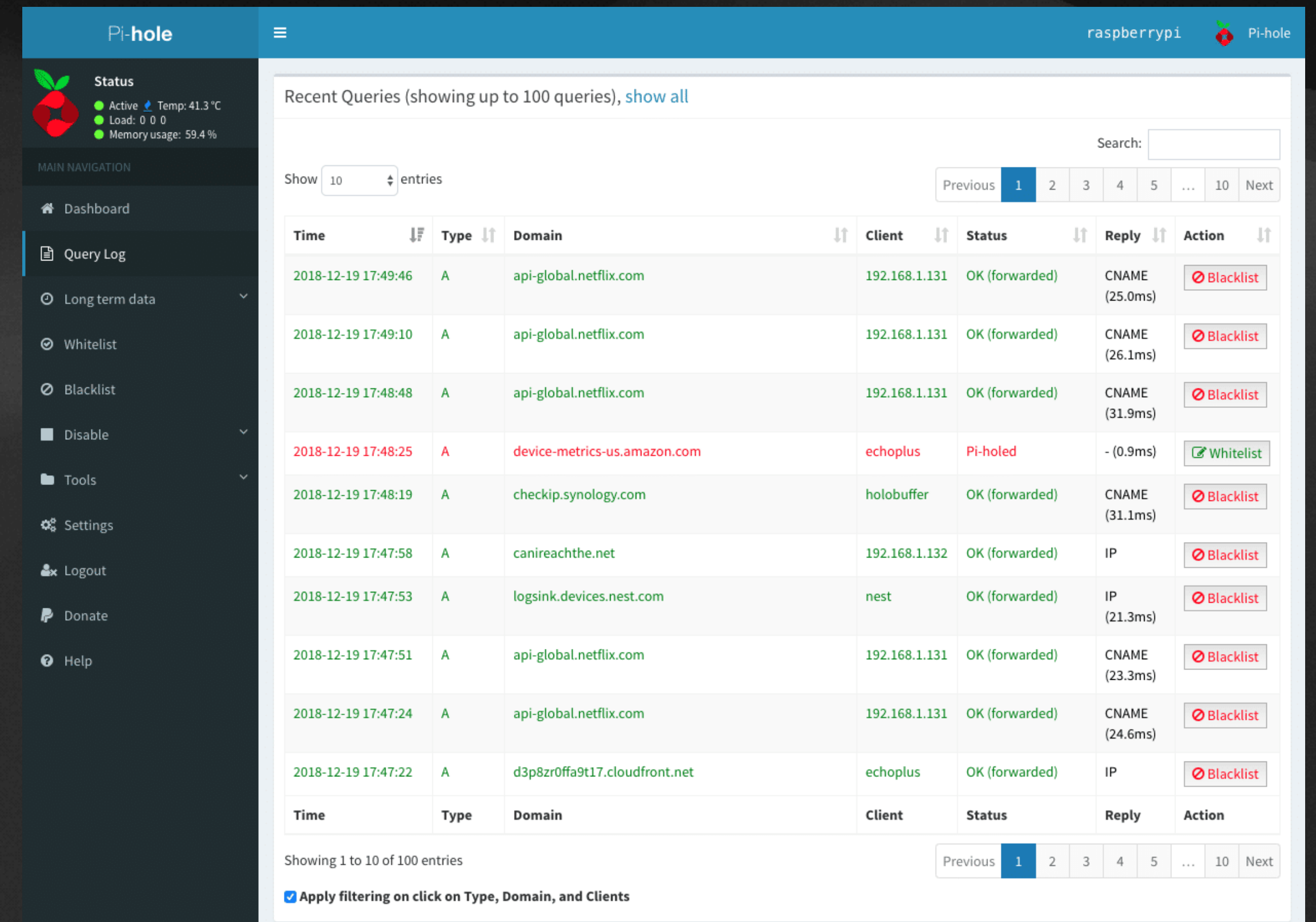
1. [Overview](#)
2. [Multi light](#) - Hand brush: Light protection
3. [Multi normal](#) - Broom: All-round protection
4. [Multi pro](#) - Big broom: Extended protection (Recommended) : [Full](#) - [Mini](#)
5. [Multi pro++](#) - Sweeper: Maximum protection (more aggressive) : [Full](#) - [Mini](#)
6. [Multi ultimate](#) - Ultimate Sweeper: Aggressive protection : [Full](#) - [Mini](#)
7. [Fake](#) - Protects against internet scams, traps & fakes!
8. [Pop-Up Ads](#) - Protects against annoying and malicious pop-up ads!
9. [Threat Intelligence Feeds](#) - Increases security significantly! (Recommended) : [Full](#) - [Medium](#) - [Mini](#) - [IPs](#)
10. [Newly Registered Domains - NRD](#) - Favoured by threat actors to launch malicious campaigns!
11. [DoH/VPN/TOR/Proxy Bypass](#) - Prevent methods to bypass your DNS! : [Full](#) - [DoH only](#) - [DoH IPs](#)
12. [Safesearch not supported](#) - Prevent the use of search engines that do not support Safesearch!
13. [Dynamic DNS](#) - Protects against the malicious use of dynamic DNS services!
14. [Badware Hoster](#) - Protects against the malicious use of host services!
15. [URL Shortener](#) - Blocks link/URL shortener!
16. [Most Abused TLDs](#) - Protects against known malicious Top Level Domains!
17. [DNS Rebind Protection](#) - Prevents attackers from resolving domains to local IPs!
18. [Anti Piracy](#) - Protects against piracy!
19. [Gambling](#) - Protects against gambling content! : [Full](#) - [Medium](#) - [Mini](#)
20. [NSFW](#) - Protects against adult content!
21. [Native Tracker](#) - Broadband tracker of devices, services and operating systems
22. [Supporter](#) - Leave a star (top right)!
23. [Recommendation](#) - [Which version of the lists should I use?](#)
24. [Online DNS Services](#)
25. [About](#) : [Repository](#) - [Referral Domains](#) - [Support Me](#) - [Sponsor Me](#)
26. [FAQ](#) - Frequently Asked Questions
27. [Discussions](#)
28. [Sources](#)
29. [Disclaimer](#)
30. [Contact](#)

Host file recipe	Readme	Raw hosts	Unique domains	Non GitHub mirror
Unified hosts = (adware + malware)	Readme	link	245,988	link
Unified hosts + fakenews	Readme	link	252,090	link
fakenews	Readme	link	2,188	link
Unified hosts + gambling	Readme	link	256,525	link
gambling	Readme	link	6,635	link
Unified hosts + porn	Readme	link	324,666	link
porn	Readme	link	75,483	link
Unified hosts + social	Readme	link	253,115	link
social	Readme	link	3,242	link
Unified hosts + fakenews + gambling	Readme	link	258,713	link
fakenews + gambling	Readme	link	8,829	link
Unified hosts + fakenews + porn	Readme	link	326,854	link
fakenews + porn	Readme	link	77,677	link
Unified hosts + fakenews + social	Readme	link	255,303	link
fakenews + social	Readme	link	5,436	link
Unified hosts + gambling + porn	Readme	link	331,289	link
gambling + porn	Readme	link	82,118	link
Unified hosts + gambling + social	Readme	link	259,738	link
gambling + social	Readme	link	9,877	link
Unified hosts + porn + social	Readme	link	327,878	link
porn + social	Readme	link	78,724	link
Unified hosts + fakenews + gambling + porn	Readme	link	333,477	link
fakenews + gambling + porn	Readme	link	84,312	link
Unified hosts + fakenews + gambling + social	Readme	link	261,926	link
fakenews + gambling + social	Readme	link	12,071	link
Unified hosts + fakenews + porn + social	Readme	link	330,066	link
fakenews + porn + social	Readme	link	80,918	link
Unified hosts + gambling + porn + social	Readme	link	334,501	link
gambling + porn + social	Readme	link	85,359	link
Unified hosts + fakenews + gambling + porn + social	Readme	link	336,689	link
fakenews + gambling + porn + social	Readme	link	87,502	link

Increased Network Visibility

- DNS logs provide insight to where your devices are connecting to
- Note: Some devices have hard coded DNS resolvers (e.g., Google Smart Home devices) or use encrypted DNS and won't query your local resolver ∴ no visibility

(Screenshot from Pi-Hole website)



The screenshot shows the Pi-hole dashboard interface. On the left is a sidebar with navigation links: Dashboard, Query Log, Long term data, Whitelist, Blacklist, Disable, Tools, Settings, Logout, Donate, and Help. The main content area displays 'Recent Queries (showing up to 100 queries), show all'. It includes a search bar, a 'Show 10 entries' dropdown, and a table of query logs. The table has columns for Time, Type, Domain, Client, Status, Reply, and Action. The first query shows a successful A record lookup for api-global.netflix.com from client 192.168.1.131. The second query shows a Pi-holed status for device-metrics-us.amazon.com from client echoplus. The third query shows a successful A record lookup for checkip.synology.com from client holobuffer. The fourth query shows a successful A record lookup for canireachthe.net from client 192.168.1.132. The fifth query shows a successful A record lookup for logsink.devices.nest.com from client nest. The sixth query shows a successful A record lookup for api-global.netflix.com from client 192.168.1.131. The seventh query shows a successful A record lookup for api-global.netflix.com from client 192.168.1.131. The eighth query shows a successful A record lookup for d3p8zr0ffa9t17.cloudfront.net from client echoplus. The table also includes a 'Blacklist' button for each query.

Time	Type	Domain	Client	Status	Reply	Action
2018-12-19 17:49:46	A	api-global.netflix.com	192.168.1.131	OK (forwarded)	CNAME (25.0ms)	Blacklist
2018-12-19 17:49:10	A	api-global.netflix.com	192.168.1.131	OK (forwarded)	CNAME (26.1ms)	Blacklist
2018-12-19 17:48:48	A	api-global.netflix.com	192.168.1.131	OK (forwarded)	CNAME (31.9ms)	Blacklist
2018-12-19 17:48:25	A	device-metrics-us.amazon.com	echoplus	Pi-holed	- (0.9ms)	Whitelist
2018-12-19 17:48:19	A	checkip.synology.com	holobuffer	OK (forwarded)	CNAME (31.1ms)	Blacklist
2018-12-19 17:47:58	A	canireachthe.net	192.168.1.132	OK (forwarded)	IP	Blacklist
2018-12-19 17:47:53	A	logsink.devices.nest.com	nest	OK (forwarded)	IP (21.3ms)	Blacklist
2018-12-19 17:47:51	A	api-global.netflix.com	192.168.1.131	OK (forwarded)	CNAME (23.3ms)	Blacklist
2018-12-19 17:47:24	A	api-global.netflix.com	192.168.1.131	OK (forwarded)	CNAME (24.6ms)	Blacklist
2018-12-19 17:47:22	A	d3p8zr0ffa9t17.cloudfront.net	echoplus	OK (forwarded)	IP	Blacklist

Local Self-Hosted DNS Resolvers

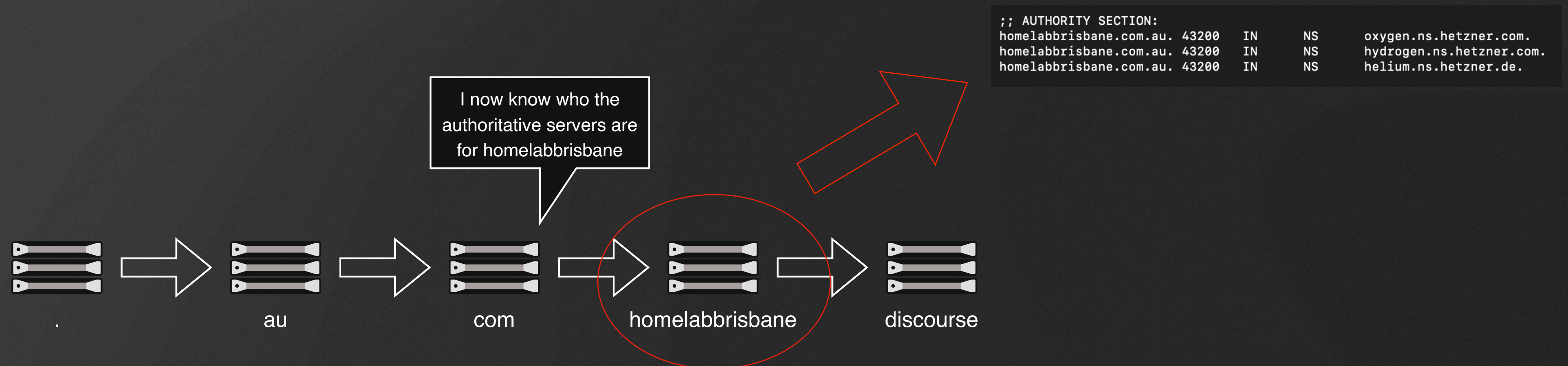
- AdGuard Home (Self-hosted) - adguard.com
Docker/Linux/macOS/RaspberryPi/FreeBSD
- Pi-Hole (Self-hosted) - pi-hole.net
Docker & Linux
- Technetium DNS (Self-hosted) - technitium.com
Windows/Linux/macOS/Raspberry Pi
- Functionality may be available in your router (e.g., MikroTik RouterOS)

Other Potential Resolver Options

- NextDNS (Free & Paid Tiers) - nextdns.io
- Control-D (Paid Tier)
Similar functionality to locally hosted options
- Public resolvers with some built in filtering:
 - Cloudflare Public DNS (1.1.1.1)
 - “Malware Protection” (1.1.1.2)
 - “Family Protection” (1.1.1.3)
 - Quad9 (9.9.9.9)
 - Control-D (Free Tier) including Malware, Ads & Tracking, Family Friendly options

Authoritative: Hosting & Self-Hosting

- On a technical level, “buying [licensing] a domain name” gives you the right to dictate which authoritative servers are listed in the DNS hierarchy
- e.g., DNS queries sent via `.` *[root]* → *au* → *com* looking for *homelabbrisbane* will be directed to the authoritative servers



Authoritative: Hosting & Self-Hosting

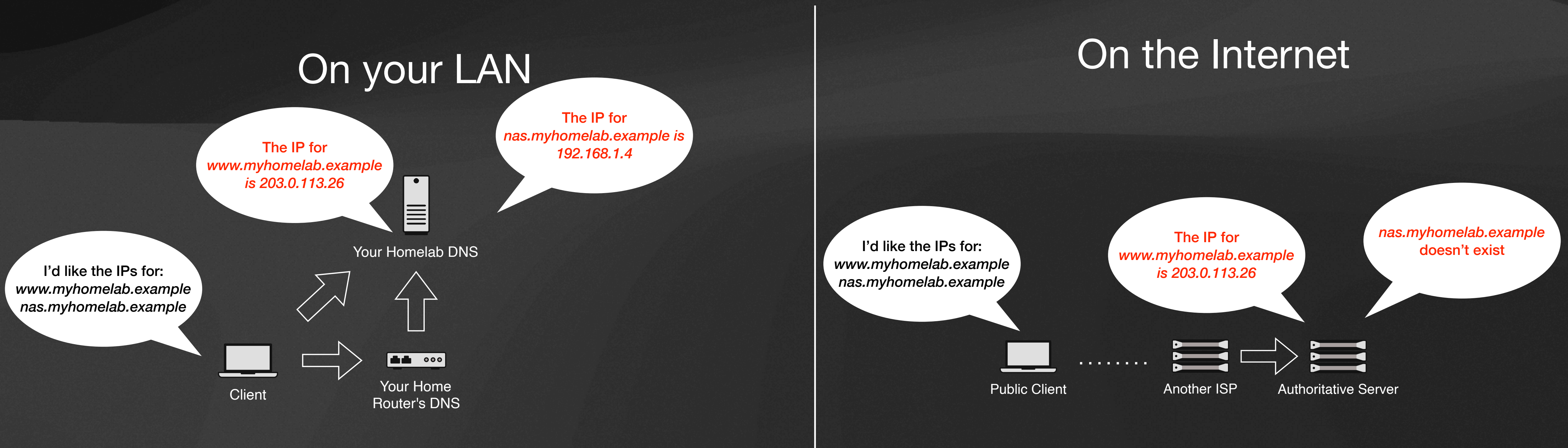
Common Record Types

- A
Name = IP address (e.g., www.abc.net.au = 123.123.123.123, router.local = 192.168.0.1)
- AAAA
Functional equivalent of A for IPv6
- CNAME
Canonical Name, i.e., alias (e.g., www.abc.net.au = abc.net.au, followed by an “A” query for abc.net.au to resolve the IP)
- MX
Mail eXchange, i.e., mail sent to <user>@domain gets delivered to IP address x.x.x.x
- TXT
Text. Used for administrative purposes (e.g., proving control over a DNS zone via _acme-challenge, SPF/DKIM/DMARC for mail)

Hosting & Self-Hosting

Split DNS

- A local resolver can resolve local self-hosted things on your LAN, and your public services can be resolved as per normal



Misconceptions & Other Considerations

- Local blocking DNS resolvers are not a silver bullet
- Some devices don't respect local DNS resolvers issued via DHCP (e.g., Google smart devices hard coded to 8.8.8.8) and some devices/browsers bypass DNS by using encrypted DNS (e.g., DoH, DoT)
- “Classic” DNS is not encrypted. Your ISP/resolver(s), etc. can see your DNS lookups
- DNS doesn't *propagate*. DNS is cached - if you change an authoritative record, it doesn't get “pushed” out to the world, you are waiting for other resolvers' caches to expire

Homelab DNS - Take Away

- Local resolvers are powerful tools
 - Control what devices on your network can “find” by controlling the DNS on your network (e.g., block ads, issue DNS names to internal services)
 - Monitor what your devices are doing by monitoring their DNS lookups
- Authoritative resolvers are [generally] the single source of truth for a public domain name
 - Understand what is in your DNS zone and why