Protect Your Network

Let’s learn how DNS works and build a sinkhole that will protect your network

What is AdGuard & Why Does it Matter?

AdGuardHome is a network-wide software solution designed to block intrusive ads, malicious trackers, and other unwanted content before it even reaches your devices.

Protects Your Home Network: As AGH filters traffic at the DNS level, all devices connected to your network benefit automatically.

Better Network Speeds: Blocks unwanted traffic, you reduce unnecessary data usage and improve network efficiency.

Safer Web Browsing: Block phishing and other malicious links before they even reach the device.

Custom Filter Lists: Easily enable, disable, or add specific blocklists for comprehensive or targeted protection

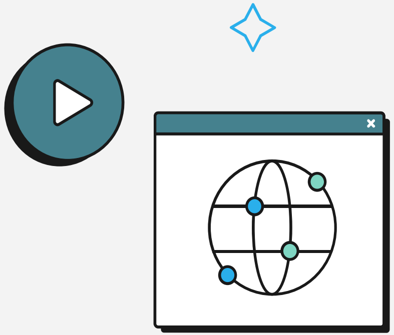


Table of contents

01

What is DNS? 🤔

02

All about DNS Resolvers

03

Is DNS really secure? 👀

04

Why block a DNS request?

05

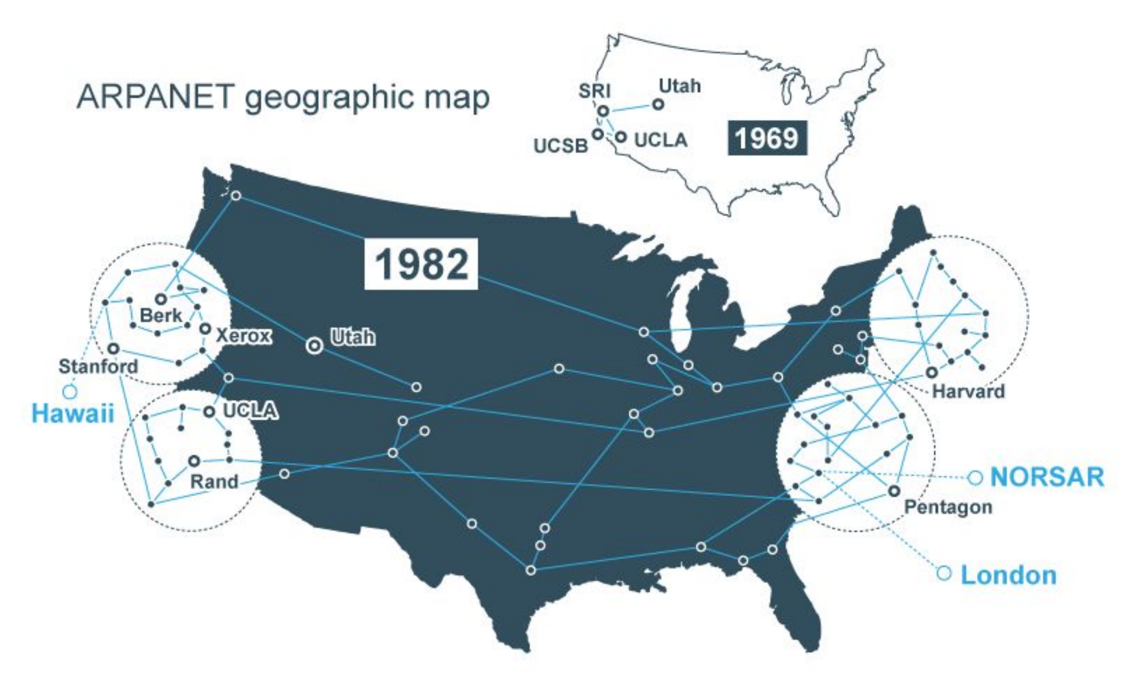
AdGuard and PiHole

06

Some Interesting Stuff

ARPANET – History Time

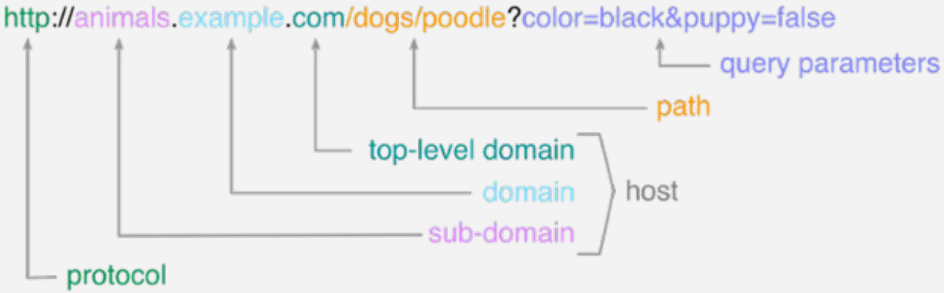
Advanced Research Projects Agency Network (ARPANET)



What is DNS?

DNS (Domain Name System) is effectively the phonebook of the internet. It converts domain names (e.g., *example.com*) into numerical IP addresses (e.g., *93.184.216.34*) so that computers and other devices can communicate with servers.

Each time you type a URL or click a link, a DNS query is made to find the corresponding IP address.



http://animals.example.com/dogs/poodle?color=black&puppy=false

query parameters

path

top-level domain

domain

sub-domain

host

protocol

What is a DNS Resolver

A DNS resolver is the component that receives a DNS query (for example, *www.example.com*) and proceeds to locate the corresponding IP address, returning it to the client (your computer, phone, etc.).

Some DNS Resolvers

- Your ISP - ACT Fibernet, Jio, Airtel
- Cloudflare, Google, Cisco, NextDNS, AdGuard
- Setup your own using unbound :)

When you perform a DNS Lookup on Google.com for the 27th time
I am once again asking
for your [redacted] i [redacted] p [redacted]

Security Threats with DNS 🚨

DNS Spoofing (Cache Poisoning)

Attacker manipulates DNS responses so that a DNS resolver caches false information, users to be redirected to malicious sites even when typing legitimate domain names.

Man-in-the-Middle (MitM)

Attacker intercepts DNS traffic (for instance, on public Wi-Fi) and modifies the responses on-the-fly.

DNS Hijacking

DNS Hijacking is when an attacker gains unauthorized control over DNS records (often by compromising a domain registrar or router) and redirects traffic to malicious servers.

NXDomain Flood Attack

A specialized DDoS technique where attackers send large volumes of DNS queries for non-existent domains (NXDomain). Server spends resources searching for records that don’t exist.

How to connect to a DNS Server?

Plain DNS

Plain DNS traffic is easily readable by anyone who can intercept or monitor network traffic. This lack of encryption also makes it susceptible to certain types of attacks and tampering.

DNS over HTTPS

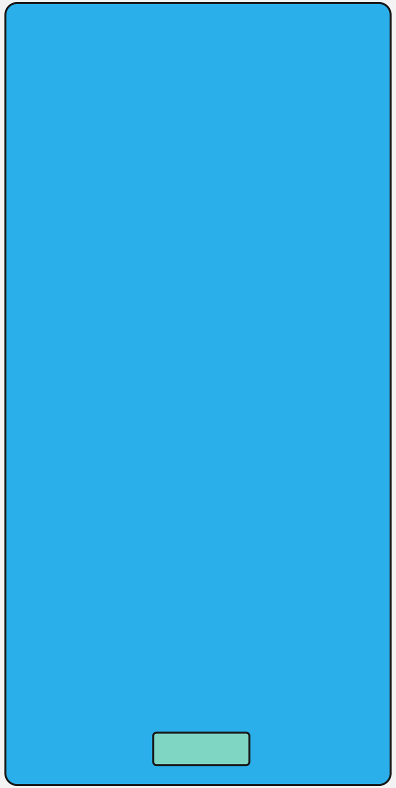
DNS-over-HTTPS (DoH) encapsulates DNS queries and responses within regular HTTPS traffic. As a result, DNS queries become significantly more private, preventing third parties (e.g., ISPs, network administrators, or malicious actors) from intercepting or tampering with them in transit

DNS over TLS

DNS-over-TLS (DoT) is a protocol that encrypts DNS queries and responses using the Transport Layer Security (TLS) protocol. DoT typically uses a dedicated port (853) for encrypted DNS communications. Less prevalent compared to **DoH**

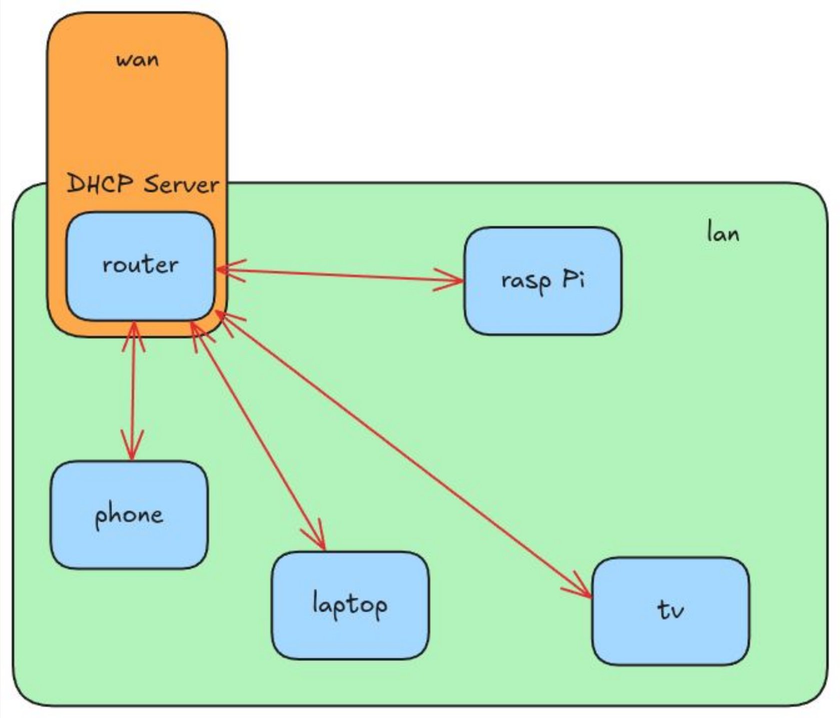
> 50%

More than 50% of your DNS traffic is Telemetry and Ads

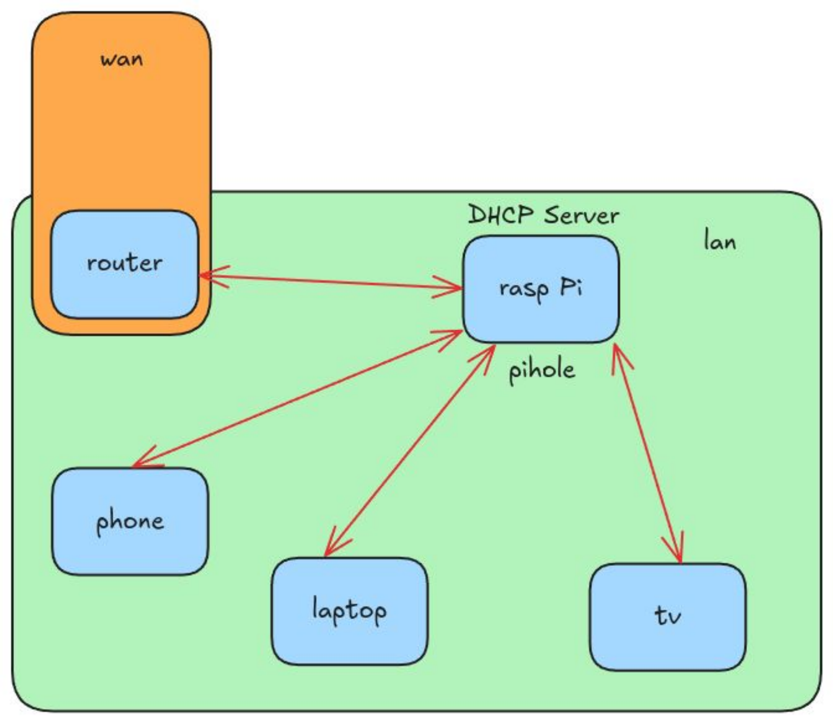


Let’s Configure a AdBlocker

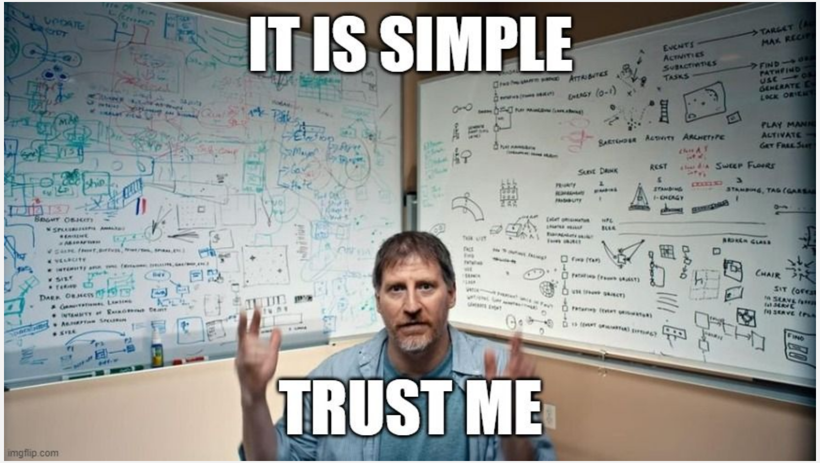
A General Home Network

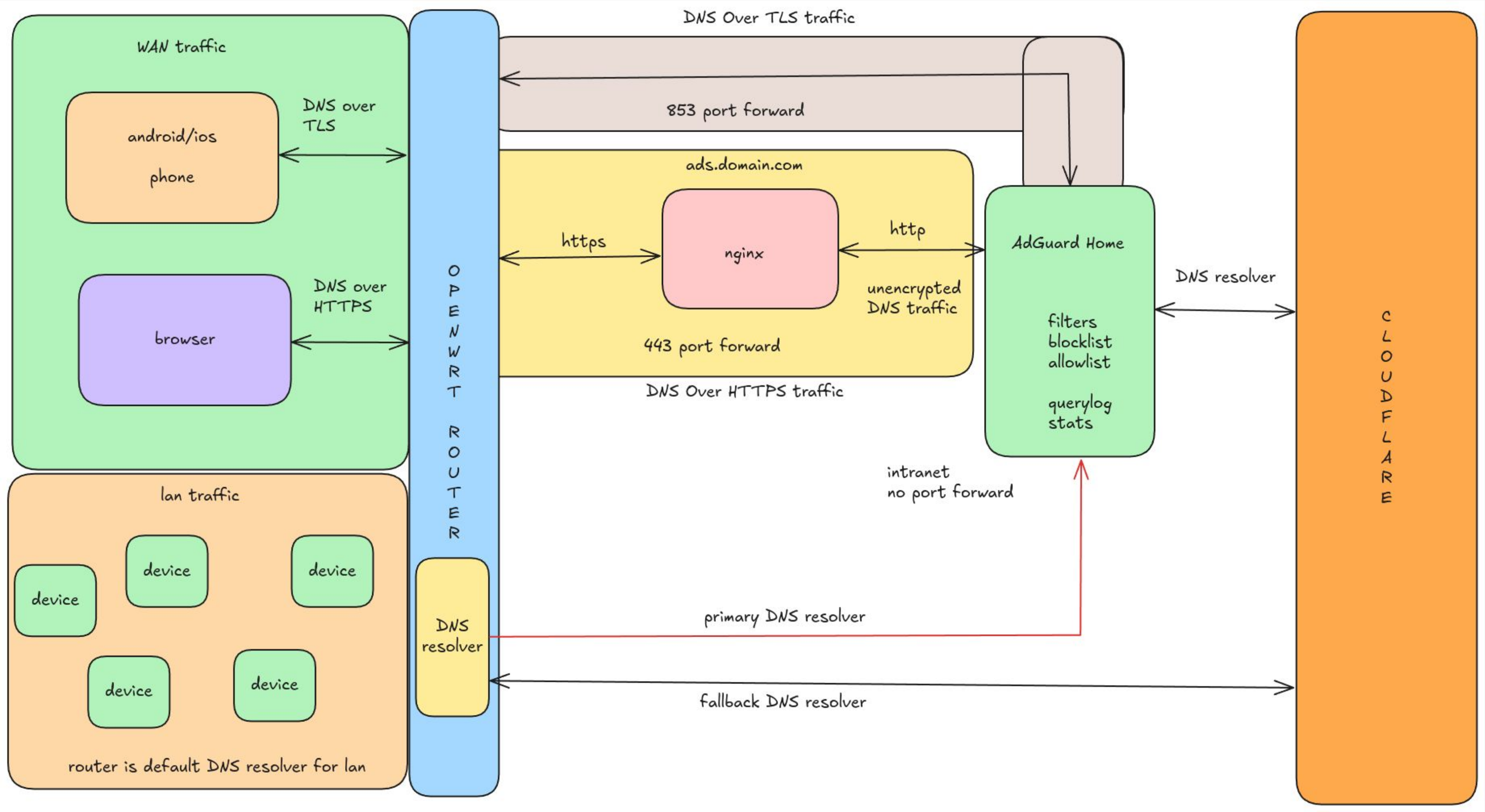


Basic AdBlock Setup



Let’s add more Functionality




DNS Over TLS traffic
WAN traffic
android/ios
phone
DNS over
TLS
853 port forward
ads.domain.com
https
nginx
http
AdGuard Home
DNS over
HTTPS
browser
unencrypted
DNS traffic
DNS resolver
filters
blocklist
allowlist
querylog
stats
443 port forward
DNS Over HTTPS traffic
OPENWRT ROUTER
CLOUDFLARE
intranet
no port forward
lan traffic
device
device
device
device
device
DNS
resolver
primary DNS resolver
fallback DNS resolver
router is default DNS resolver for lan

But Wait, aren’t you still being tracked?

External DNS Resolvers

They typically have large, globally distributed server networks that can resolve queries quickly.

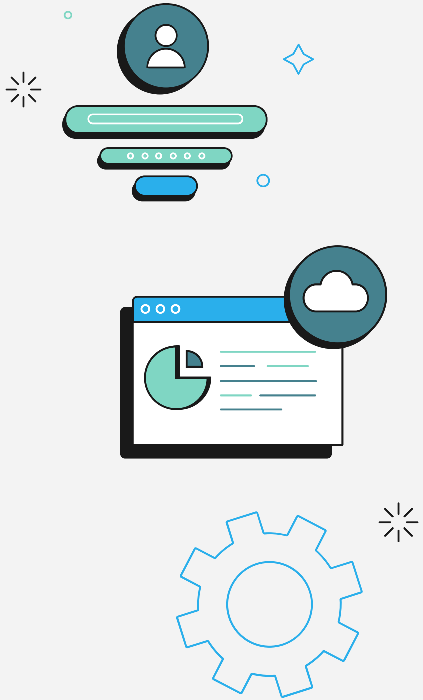
High availability, if Cloudflare goes down, half the internet does, pretty reliable

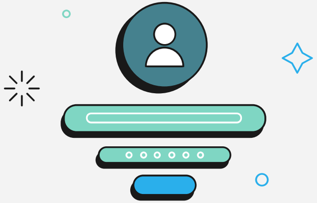
Self Managed

Self-managed resolvers like **unbound** recursively query the DNS hierarchy themselves (from root servers down to authoritative name servers) rather than relying on a third-party service.

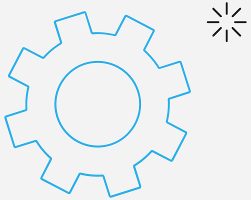
Initial lookups might be slower than large public DNS providers.

full autonomy over your DNS data





Live Demonstration



Until the DNS Propagates...

Any Questions?

Resources

Blog on TLS - https://ikarus.sg/lets-encrypt-dot-android/

Cloudflare Learning - https://www.cloudflare.com/learning/dns/what-is-dns/

PiHole and AdGuard Documentation

Online Community and Forums :D

Thanks!