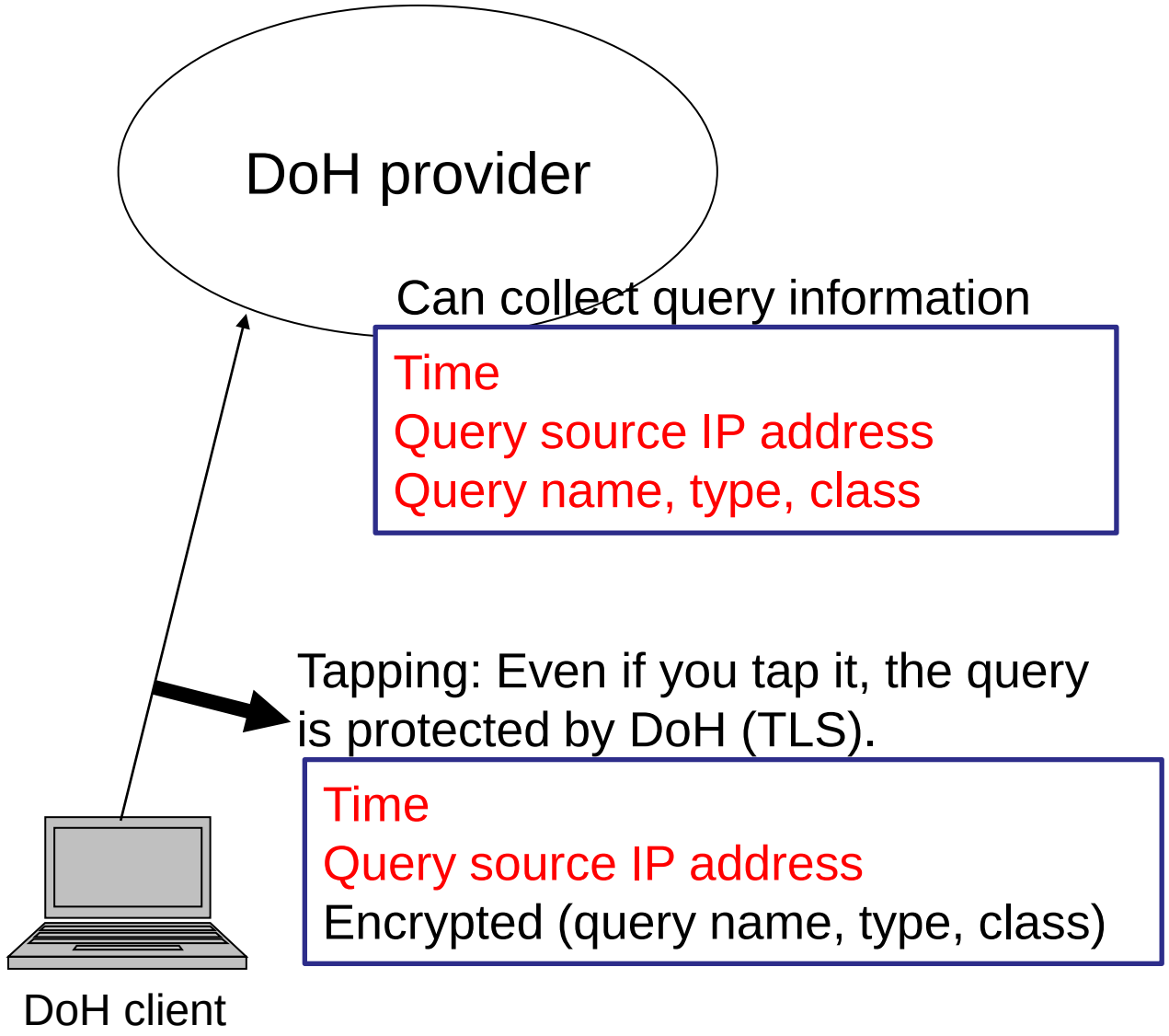
Keep my privacy:
DNS over HTTPS over CGN, public NAT64
(or IPv6 transition technologies, Open HTTP proxies)

Kazunori Fujiwara, JPRS
fujiwara@jprs.co.jp

Privacy issues of DNS over HTTPS (DoH)

- Sensitive data in DNS queries
  - Time
  - Query source IP address
  - DNS query (name, type, class)
- DoH hides DNS query (name, class, type) by encryption
- Privacy issues
  - query source IP address is not protected
  - DoH providers can collect the whole data

- **<u>How can I hide my IP address from DoH providers ?</u>**

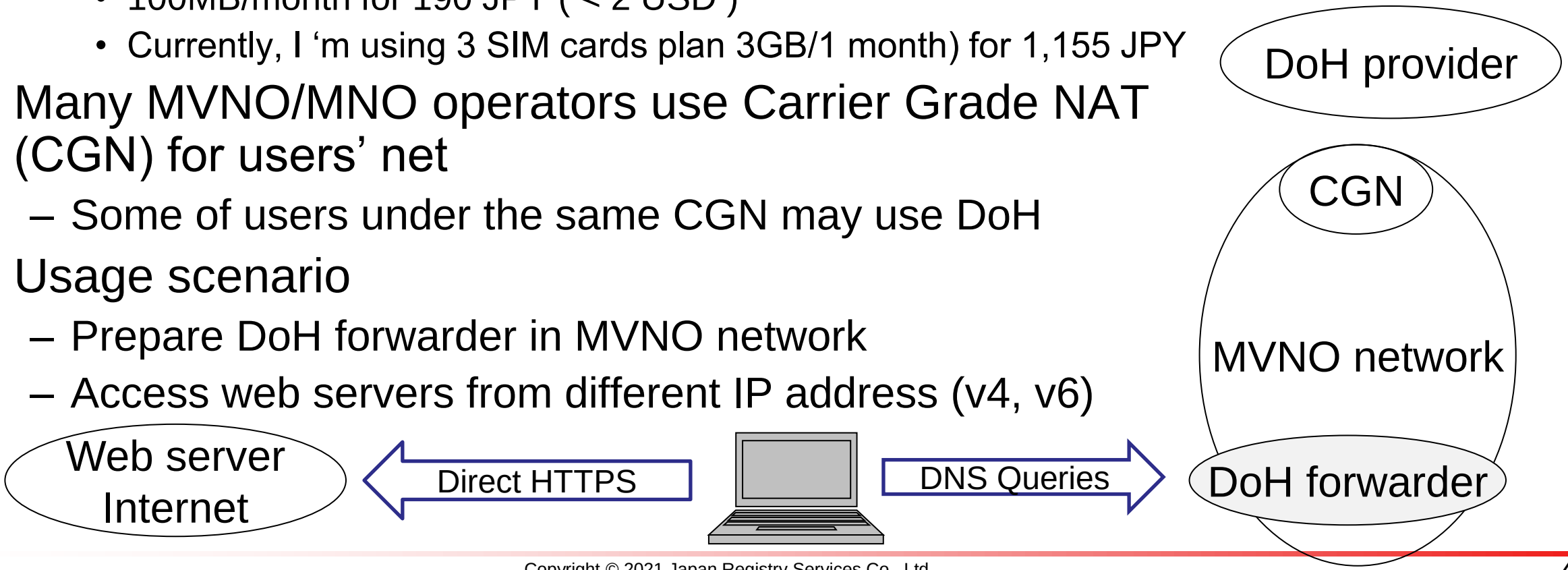


How to hide query source IP address ?

- Previous proposals also tried to hide query source IP addresses
  - Tor's DNS … requires Tor network
  - Oblivious DNS (DoH) … requires service providers
- Simpler solutions to hide (I'm happy if I can do it by myself)
  - "The best place to hide a leaf is in a forest."
  - We can hide query source IP addresses under
    - IPv4 NAT (CGN, NAT64, IPv6 transition technologies)
    - Open HTTP(S) Proxy (or Tor HTTPS)
- And more, we can use different IP address (direct connection) to access web servers

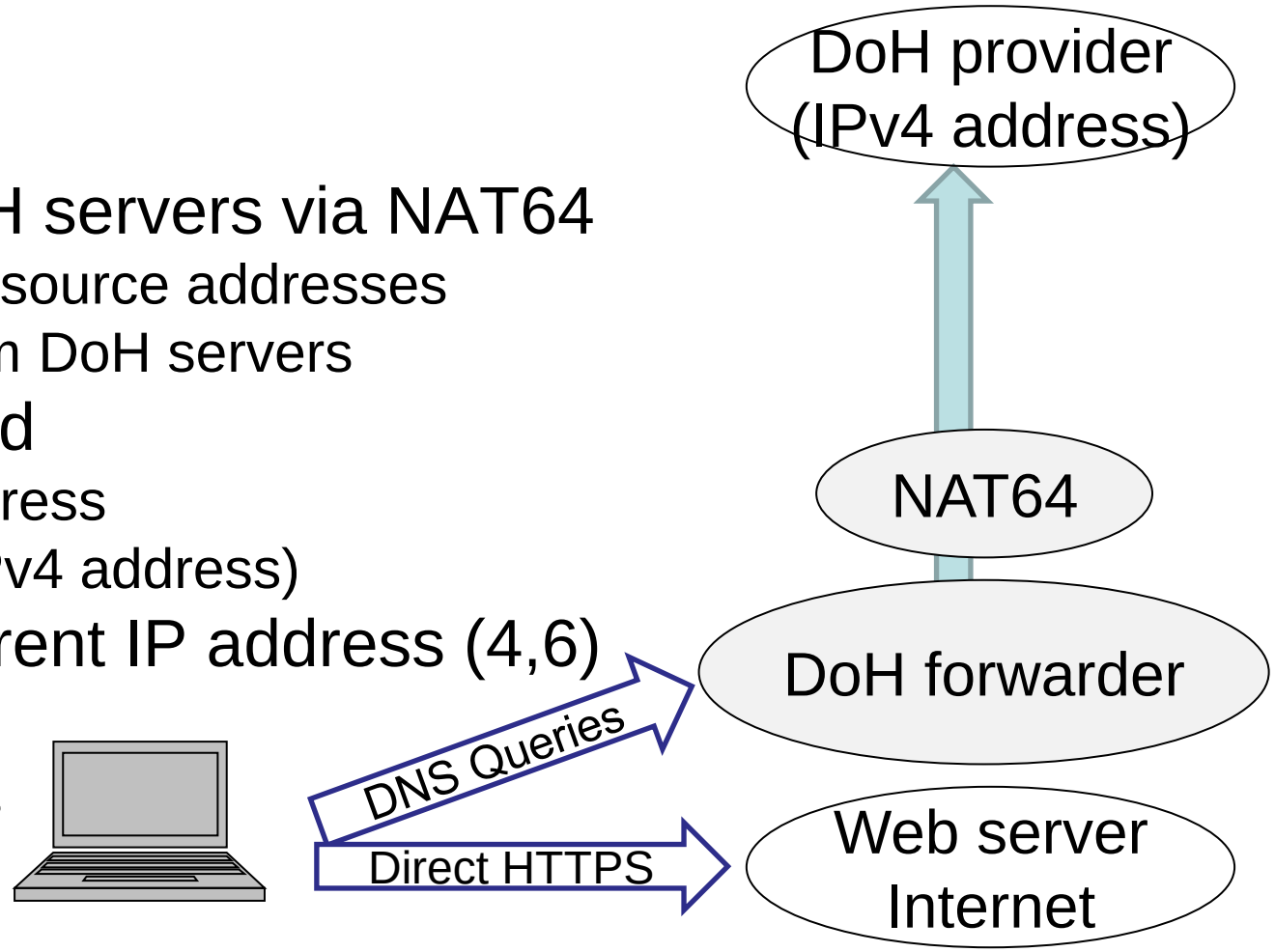
Idea: DoH over CGN

- We can hide query source IP address under low-priced mobile network
  - In Japan, it is easy to purchase a SIM card
    - 100MB/month for 190 JPY (< 2 USD)
    - Currently, I ‘m using 3 SIM cards plan 3GB/1 month) for 1,155 JPY
- Many MVNO/MNO operators use Carrier Grade NAT (CGN) for users’ net
  - Some of users under the same CGN may use DoH
- Usage scenario
  - Prepare DoH forwarder in MVNO network
  - Access web servers from different IP address (v4, v6)



Idea: DoH over NAT64

- Public NAT64 services: see https://nat64.xyz/
  - They translates/rewrites source IPv6 addresses to (shared) IPv4 address
- Usage scenario
  - Send DoH queries to IPv4 DoH servers via NAT64
    - NAT64 rewrites IPv6 DoH query source addresses
    - It hides source IPv6 address from DoH servers
  - Special DoH forwarder required
    - That connect to NAT64 IPv6 address
      (NAT64 prefix + DoH server's IPv4 address)
  - Access web servers from different IP address (4,6)
  - To increase anonymity
    - multiple NAT64 services/prefixes
    - multiple DoH providers

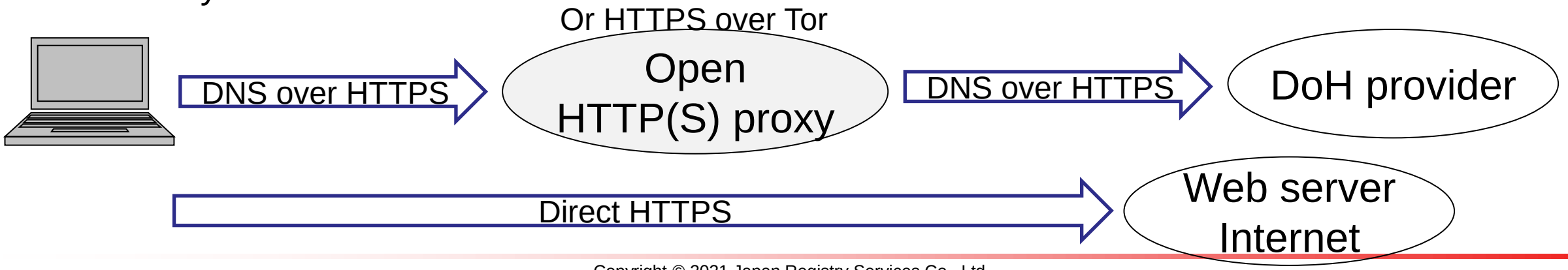


Idea: DoH over IPv6 transition technology

- IPv4 over IPv6 services (DS-Lite, MAP-E)
  - In many cases, multiple subscribers share one IPv4 address
  - When multiple users use DoH under the shared IPv4 address, DoH providers can know one global IPv4 address only
- Use scenario
  - Disable IPv6 at a client
  - Or, prepare DoH forwarder that connects to DoH server via IPv4 only
- Problem
  - It is weak because source IP address of DoH and web access are the same
  - Disabling IPv6 goes against IPv6 transition

Idea: DoH over open HTTP(S) proxies

- Because
  - Proxies cannot know the DoH query
  - DoH provider cannot know original query source IP address
- Usage scenario
  - Send DoH queries via (open)HTTPS proxy
  - Access web servers using direct HTTPS connection
  - Requires special browsers or DoH forwarder that send DoH queries via HTTP proxy
- Problem: We cannot get permissions to use open proxies
- Solution
  - DoH over Tor
  - Providers may offer special open HTTPS proxies that can connect to public DoH servers only



Tool: getting my IPv4 address via DNS

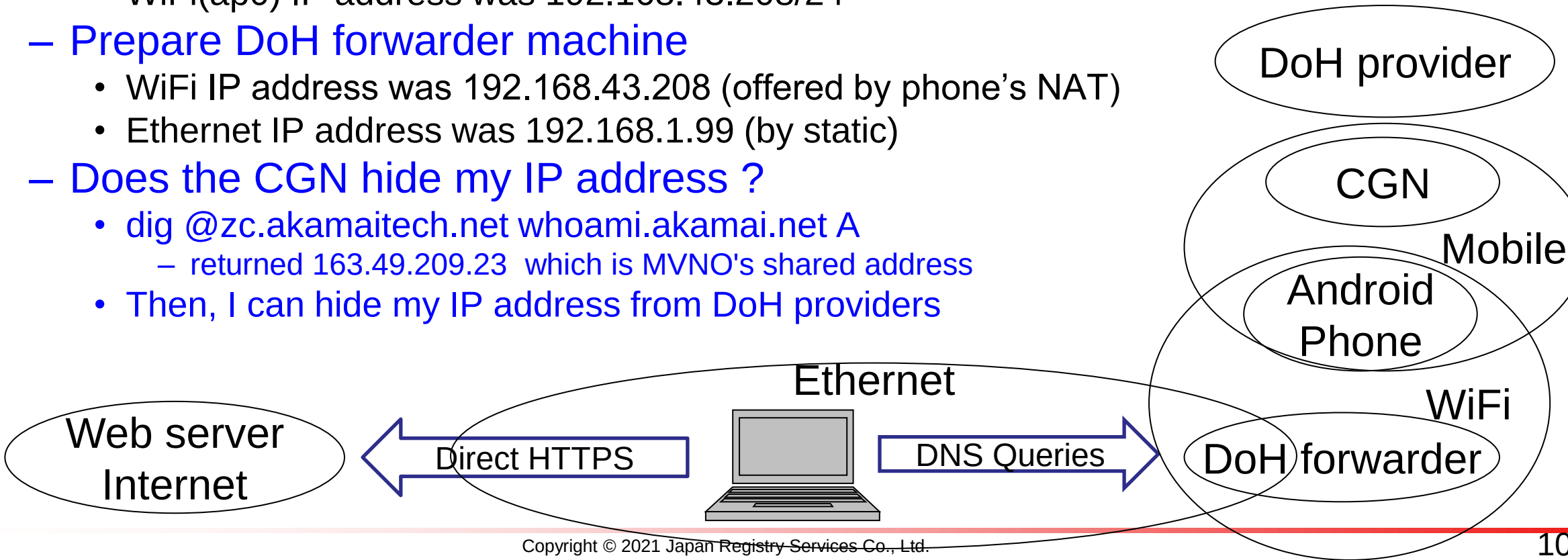
- Akamai provides "whoami.akamai.net"
  - Example: dig +short A whoami.akamai.net
  - It returns resolver's IP address in use
- We can use the service to know my IP address
  - First, dig akamai.net ns
    - returns akamai.net name server addresses
  - Next, "dig @(akamai.net IPv4 server address) whoami.akamai.net A
    - returns my IPv4 address
  - dig @(akamai.net IPv6 server address) whoami.akamai.net AAAA
    - returns my IPv6 address

Tools: DoH forwarder

- DoH forwarder
  - Receives queries from clients via port 53 UDP, TCP
  - Forwards queries to servers via DoH
- doh-forwarder
  - https://github.com/kpadron/doh-forwarder
  - Receives queries from clients via port 53 UDP, TCP
  - Forwards queries to a DoH server
- fujiwara's DNS Forwarder: I made my own DNS forwarder
  - Written in perl (depends on Net::DNS and IO::Socket::SSL)
  - Receiveing queries from clients via UDP, TCP, (DoT), DoH
  - Forwarding queries to a server via UDP, TCP, (DoT), DoH
  - Each TCP (DoT, DoH) connection is closed on every query
    - It reduces performance, however, it will improve privacy
  - NAT64 is supported (uses IPv4 server and rewrites to NAT64 address)
  - caching functions
  - Limited functions: No ACLs, No performance, ...
  - Usage: DNSforwarder.pl -u UDP_listen -t TCP_listen -U UDP_server -H DoH_URL -N NAT64 prefix
    - UDP_server is used to resolve hostnames of DoH_URL on this usage

Evaluation of DoH over CGN (1)

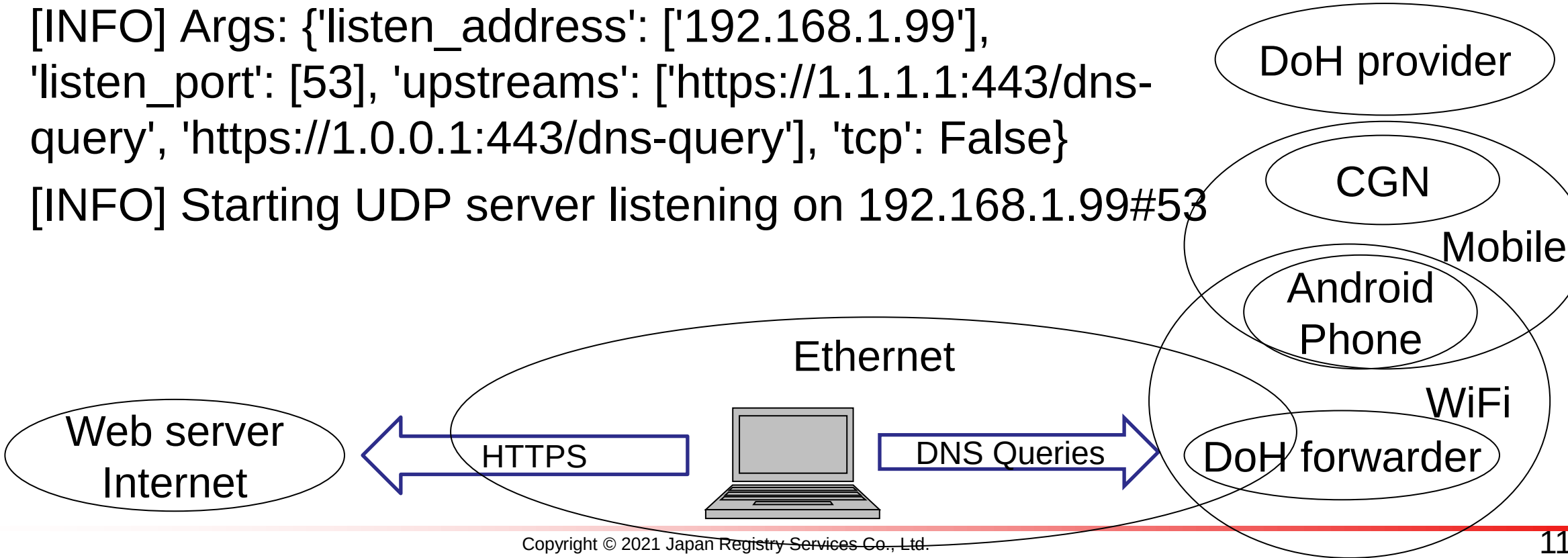
- Environment
  - MVNO: Excite mobile (https://bb.excite.co.jp/exmb/sim/)
  - Android phone as WiFi/NAT router (WiFi Tethering)
    - Outgoing(ccmni1) IP address was 100.73.209.188 (RFC 6598 Shared Address Space)
    - WiFi(ap0) IP address was 192.168.43.208/24
  - Prepare DoH forwarder machine
    - WiFi IP address was 192.168.43.208 (offered by phone's NAT)
    - Ethernet IP address was 192.168.1.99 (by static)
  - Does the CGN hide my IP address ?
    - dig @zc.akamaitech.net whoami.akamai.net A
      - returned 163.49.209.23 which is MVNO's shared address
    - Then, I can hide my IP address from DoH providers



Evaluation of DoH over CGN (2)

- Run dns-forwarder at DoH forwarder machine

```
# python3.7 doh-forwarder.py  -l 192.168.1.99 -p 53
[INFO] Starting DNS over HTTPS forwarder
[INFO] Args: {'listen_address': ['192.168.1.99'], 'listen_port': [53], 'upstreams': ['https://1.1.1.1:443/dns-query', 'https://1.0.0.1:443/dns-query'], 'tcp': False}
[INFO] Starting UDP server listening on 192.168.1.99#53
```



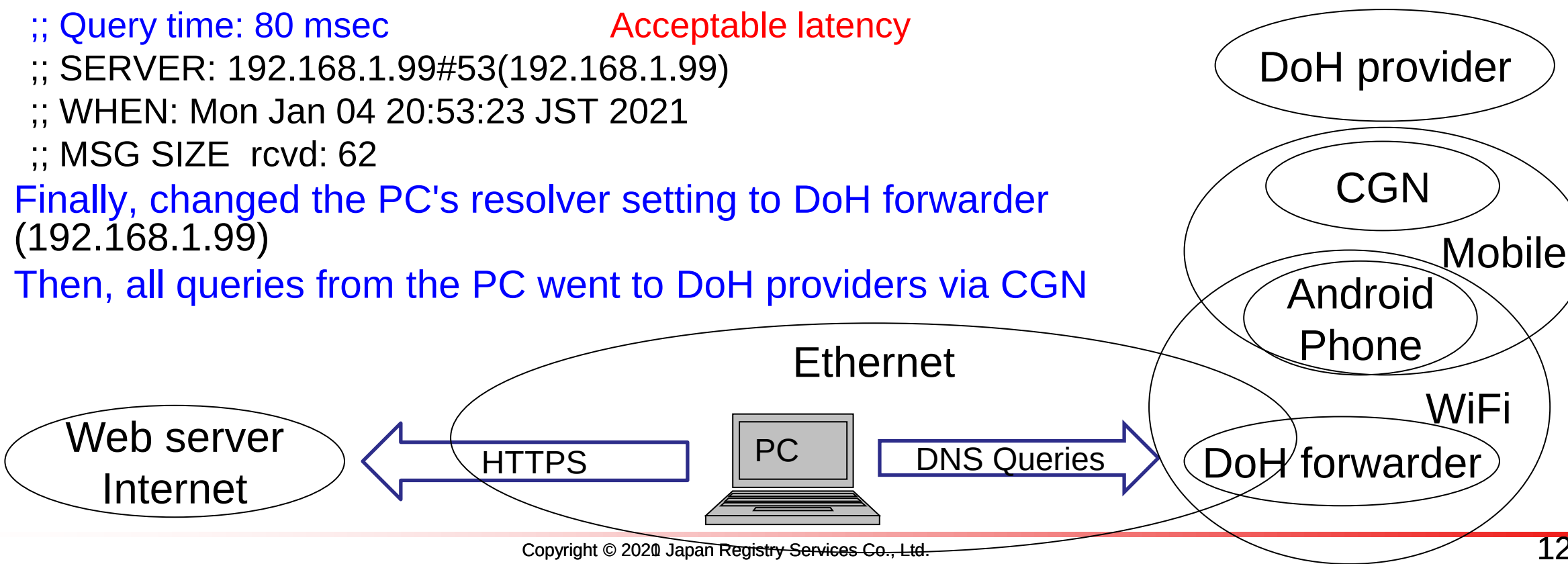
Evaluation of DoH over CGN (3)

- Checked responses from DoH forwarder
  - Client: dig @DoHforwarder whoami.akamai.net

```
;whoami.akamai.net.          IN     A
;; ANSWER SECTION:
whoami.akamai.net.     26     IN     A      162.158.117.105
;; Query time: 80 msec                    Acceptable latency
;; SERVER: 192.168.1.99#53(192.168.1.99)
;; WHEN: Mon Jan 04 20:53:23 JST 2021
;; MSG SIZE  rcvd: 62
```

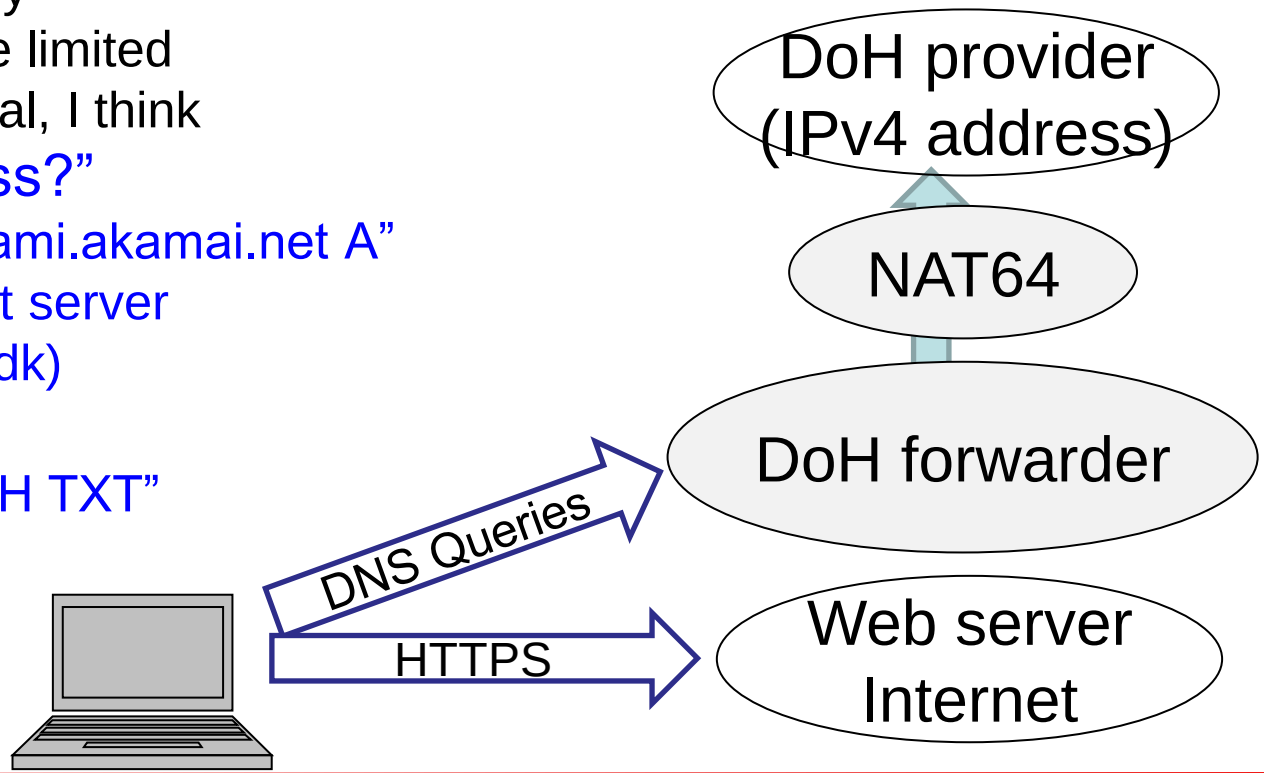
Cloudflare's IP address

- Finally, changed the PC's resolver setting to DoH forwarder (192.168.1.99)
- Then, all queries from the PC went to DoH providers via CGN



Evaluation of DoH over NAT64 (1)

- Choose one NAT64 prefix from https://nat64.xyz/
  - Provider: Kasper Dupont
  - Location: The Netherlands / Amsterdam
  - NAT64 prefix: 2a00:1098:2b::/96
  - Agree and follow the terms of service: https://nat64.net/tos
    - No Abuse: It is an experiment / temporary
    - No flood: DNS queries from a person are limited
    - No illegal access: DoH server is not illegal, I think
  - "Does the NAT64 hide my IPv6 address?"
    - "dig @2a00:1098:2b::23.74.25.192 whoami.akamai.net A"
      NAT64 prefix + IPv4 of akamai.net server
      returned 46.235.231.114 (nat64.dyndns.dk)
  - Which node answered from NAT64 ?
    - "dig @2a00:1098:2b::1.1.1.1 id.server CH TXT"
      returned TXT "AMS"
      ;; Query time: 238 msec
      (from Japan)

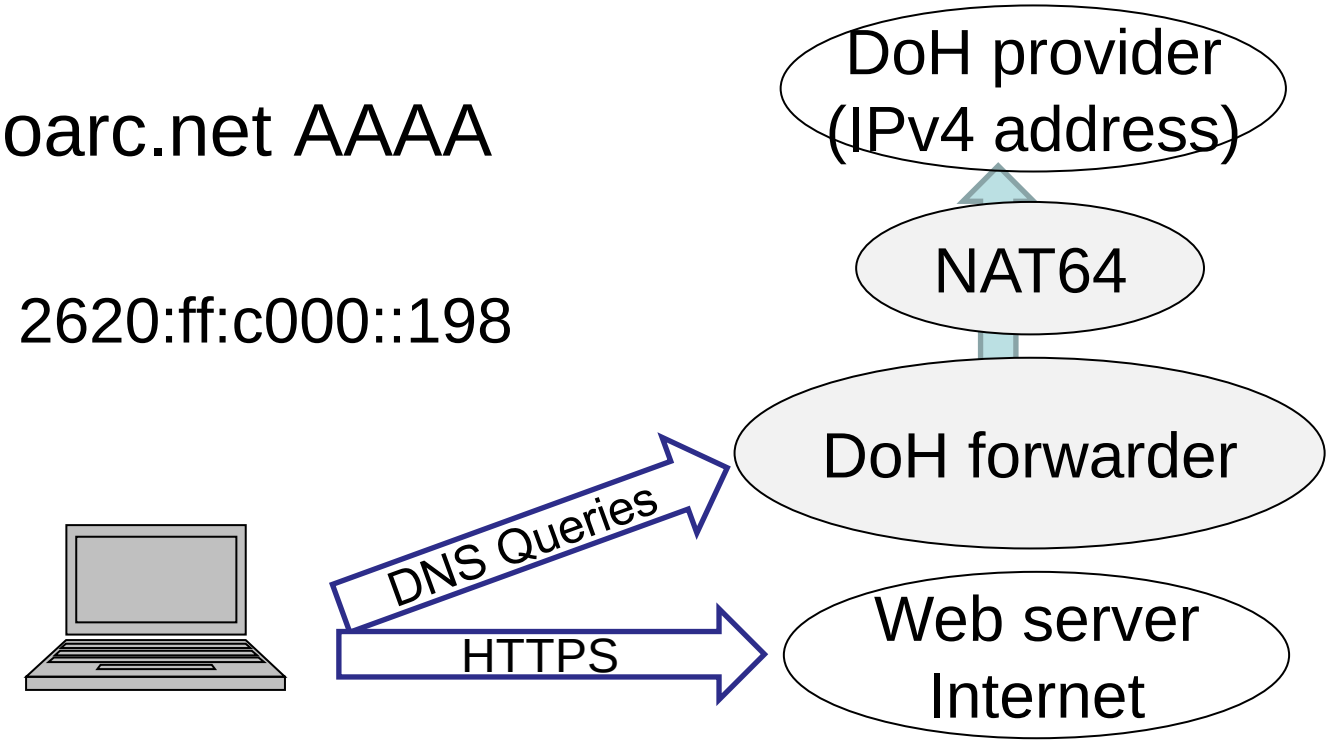


Evaluation of DoH over NAT64 (2)

- Start special DoH forwarder
  - perl DNSforwarder.pl -u 203.178.129.11/53 -U 8.8.8.8 -H https://cloudflare-dns.com/dns-query -N 2a00:1098:2b::
  - DoH forwarder's listen address is 203.178.129.11 port 53
    - DoH server address is https://cloudflare-dns.com/dns-query
    - to resolve "cloudflare-dns.com", the proxy uses 8.8.8.8 resolver
      → cloudflare-dns.com IN A 104.16.249.249
    - NAT64 address is 2a00:1098:2b::
      - DNSforwarder.pl rewrites DoH server's IP address to NAT64 prefix + IPv4 address 2a00:1098:2b::104.16.249.249 at connect

Evaluation of DoH over NAT64 (3)

- dig @DoHforwarder id.server CH TXT
  - ;; ANSWER SECTION:
  - id.server. 1 CH TXT "AMS"
    Cloudflare's AMS node
  - ;; Query time: 955 msec
- dig @DoHforwarder www.dns-oarc.net AAAA
  - ;; ANSWER SECTION:
  - www.dns-oarc.net. 120 IN AAAA 2620:ff:c000::198
  - ;; Query time: 1035 msec



Limitations of DoH over CGN/NAT64

- DoH over CGN / NAT64 / Open Proxies nullify the traffic control of CDNs.
- DoH providers can track by using TLS session information
  - My DNS Forwarder closes TCP/TLS session on every query
- Public NAT64 services are located in Europe only
  - High latency (1 second !) from Japan
    - because UDP RTT is 238ms

Conclusion

- DoH providers can know both query source IP addresses and DNS queries
  - These are the sensitive dataset for privacy
- To protect our privacy, we can hide our source IP addresses by existing tools
  - DoH over CGN with low priced MVNO SIM: feasible
  - DoH over NAT64: feasible in European region
  - ~~DoH (with IPv4 address) over DS-Lite or MAP-E may hide client IP address~~
  - DoH over open HTTP(S) proxies (or Tor): feasible (not tested)
- Any questions and suggestions ?