DNS Privacy: DoT and DoH

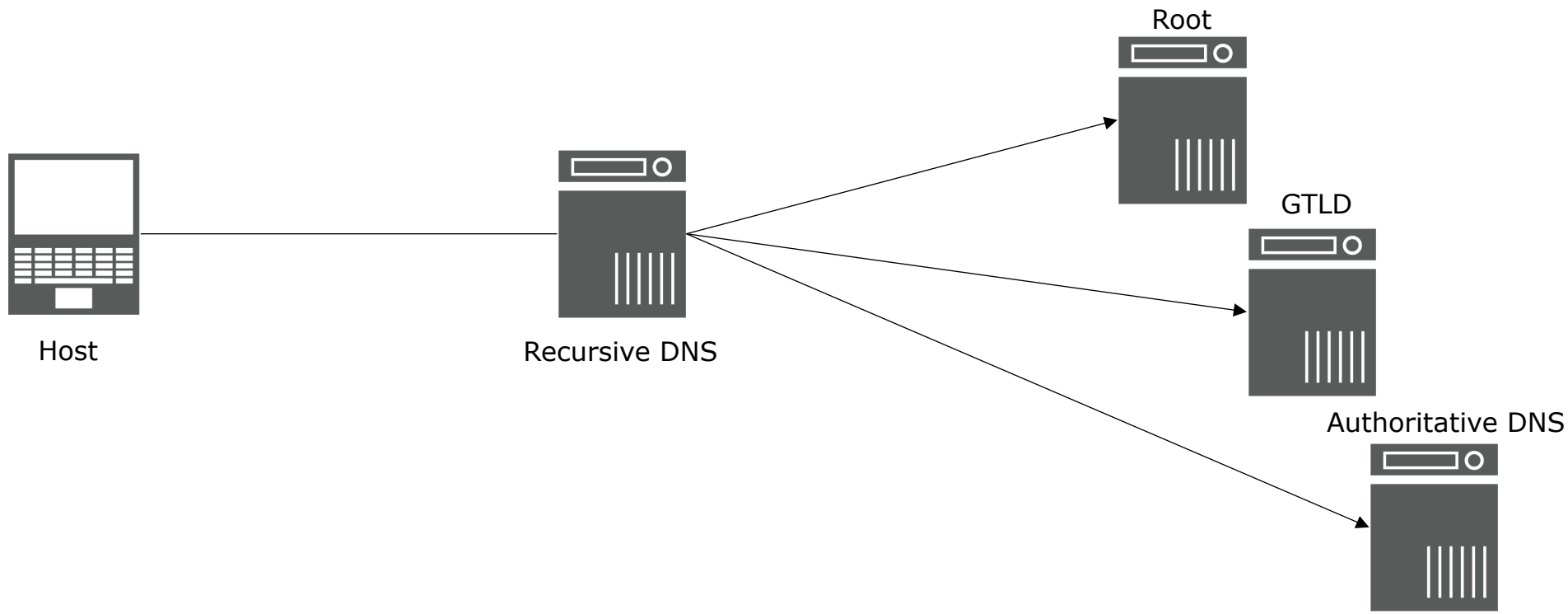
Module 6

Overview

- DNS Overview
- DNS Privacy
- DNS over TLS
- DNS over HTTPS
- Issues and Concerns

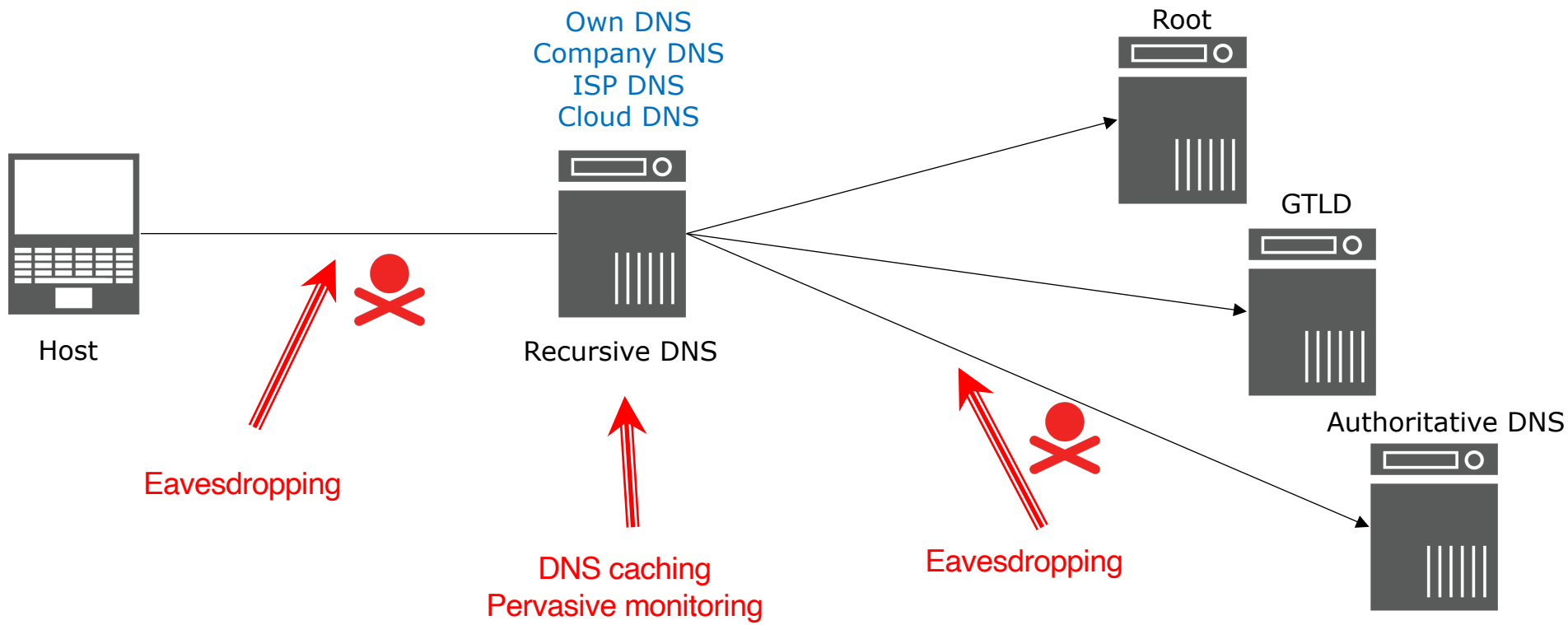
DNS Overview

- DNS is a distributed, hierarchical system for translating objects
  - A critical piece of the Internet infrastructure



DNS Privacy

- Traditionally, privacy is not considered a requirement in DNS
  - DNS is public data
- The lack of privacy protection in DNS is actively exploited



DNS Privacy – What's in a Query?

- DNS requests contain fields that are considered private

```
dig @ns.apnic.net www.apnic.net
```

QNAME

```
2001:dc0:2001:210:6d…  58687  2001:dd8:b:201::12          53     DNS  Standard query 0x7fac A www.apnic.net OPT
2001:dd8:b:201::12     53     2001:dc0:2001:210:6dea:1ff…  58687  DNS  Standard query response 0x7fac A www.apnic.net CNAME www.apnic.net.cdn.cloudflare.net A 104.20.36.173
```

Source IP address

```
▶ Frame 747: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0
▶ Ethernet II, Src: Apple_92:51:06 (8c:85:90:92:51:06), Dst: Cisco_f4:b7:81 (1c:df:0f:f4:b7:81)
▶ Internet Protocol Version 6, Src: 2001:dc0:2001:210:6dea:1ffe:13b8:3299, Dst: 2001:dd8:b:201::12
▶ User Datagram Protocol, Src Port: 58687, Dst Port: 53
▼ Domain Name System (query)
    [Response In: 748]
    Transaction ID: 0x7fac
  ▶ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▼ www.apnic.net: type A, class IN
        Name: www.apnic.net
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▼ Additional records
    ▼ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▶ Z: 0x0000
        Data length: 12
      ▶ Option: COOKIE
```

Reveals info about someone's browsing and Internet activities

DNS Cloud Providers

- There have been an increase of third-party cloud DNS providers over the years.

- Why we use them?
  - It's free and generally fast
  - Avoid surveillance and blocking
  - Lack of trust in the current provider
  - Focus on privacy

Public DNS Providers	
Google	8.8.8.8 8.8.4.4
Cloudflare DNS	1.1.1.1
Quad9	9.9.9.9
OpenDNS	208.67.222.222 208.67.220.220

DNS Privacy – Standards

- Aims to provide confidentiality of DNS transactions
  - Encrypted transport

- Actively discussed in DNS Privacy Exchange (dprive) WG in IETF
- DNS Privacy Considerations
  - RFC 7626 and draft-ietf-dprive-rfc7626-bis-03

- DNS Privacy Standards
  - DNS over TLS
  - DNS over HTTPS

DNS over TLS (DoT)

- RFC 7858 – DNS over TLS
- RFC 8310 – Usage Profiles for DoT

- Uses port 853
- DNS queries are sent over TLS-encrypted TCP connections
- Avoids spoofing, eavesdropping and DNS-based filters

DoT - Profiles

- Strict
  - Requires an encrypted and authenticated to a privacy-enabling DNS server and creates TLS connections
  - Failure to establish connection results to no service

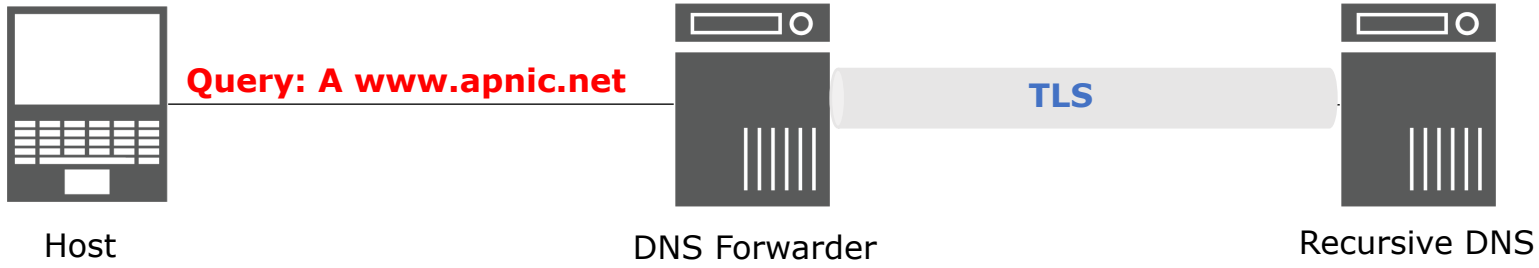
- Opportunistic
  - Desires privacy when possible
  - DNS server may be obtained by DHCP or an untrusted source

DoT – Architecture

SETUP 1:

Host must run a DoT-capable resolver
No DNS Traffic will show to eavesdropper

SETUP 2:



Local recursive server forwards queries via TLS
Typically sent to chosen/trusted local or cloud DNS

Configure DoT – Stubby Resolver

- Stubby is a local DNS privacy stub resolver
  - Runs as a daemon
  - Listens on loopback interface
  - Sends out queries via TLS
- Check the config at
  - `/usr/local/etc/stubby/stubby.yml`

```
dns_transport_list:
  - GETDNS_TRANSPORT_TLS

listen_addresses:
  - 127.0.0.1
  - 0::1

upstream_recursive_servers:
# The Surfnet/Sinodun servers
  - address_data: 145.100.185.15
    tls_auth_name: "dnsovertls.sinodun.com"
    tls_pubkey_pinset:
      - digest: "sha256"
        value: <some-key-here>
```

Configure DoT – Stubby Resolver

```
[01:34:41.015869] STUBBY: Read config from file /usr/local/etc/stubby/stubby.yml
[01:34:41.016923] STUBBY: DNSSEC Validation is OFF
[01:34:41.016935] STUBBY: Transport list is:
[01:34:41.016938] STUBBY:   - TLS
[01:34:41.016942] STUBBY: Privacy Usage Profile is Strict (Authentication required)
[01:34:41.016945] STUBBY: (NOTE a Strict Profile only applies when TLS is the ONLY transport!!)
[01:34:41.016947] STUBBY: Starting DAEMON....
[01:35:36.355313] STUBBY: 145.100.185.15                    : Conn opened: TLS - Strict Profile
[01:35:37.209618] STUBBY: 145.100.185.15                    : Verify passed : TLS
[01:35:37.350007] STUBBY: 145.100.185.16                    : Conn opened: TLS - Strict Profile
[01:35:38.226970] STUBBY: 145.100.185.16                    : Verify passed : TLS
[01:35:47.556375] STUBBY: 145.100.185.15                    : Conn closed: TLS - Resps=     1, Timeouts  =     0, Curr_auth =Success,
Keepalive(ms)= 10000
[01:35:47.556417] STUBBY: 145.100.185.15                    : Upstream   : TLS - Resps=     1, Timeouts  =     0, Best_auth =Success
[01:35:47.556426] STUBBY: 145.100.185.15                    : Upstream   : TLS - Conns=     1, Conn_fails=     0, Conn_shuts=      0, Backoffs
=     0
[01:35:48.608148] STUBBY: 145.100.185.16                    : Conn closed: TLS - Resps=     1, Timeouts  =     0, Curr_auth =Success,
Keepalive(ms)= 10000
[01:35:48.608193] STUBBY: 145.100.185.16                    : Upstream   : TLS - Resps=     1, Timeouts  =     0, Best_auth =Success
[01:35:48.608205] STUBBY: 145.100.185.16                    : Upstream   : TLS - Conns=     1, Conn_fails=     0, Conn_shuts=      0, Backoffs
=     0
```

Configure DoT - Forwarder

BIND

```
options {
    ...
    forwarders { 127.0.0.1 port 853; };
    forward only;
};
server 127.0.0.1 {
    tcp-only yes;
};
```

Unbound

```
forward-zone:
  name: "."
  forward-addr: 1.1.1.1@853#cloudflare-dns.com
  forward-tls-upstream: yes
```

DNS Traffic without DoT

6528	6.280240	2001:dc0:2001:210:75…	52782	2001:dd8:b:201::12	53	DNS	Standard query 0xeaf4 A apnic.net OPT
6529	6.281338	2001:dd8:b:201::12	53	2001:dc0:2001:210:759c:46e…	52782	DNS	Standard query response 0xeaf4 A apnic.net A 203.119.101.61

```
▶ Frame 6528: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
▶ Ethernet II, Src: Apple_92:51:06 (8c:85:90:92:51:06), Dst: Cisco_f4:b7:81 (1c:df:0f:f4:b7:81)
▶ Internet Protocol Version 6, Src: 2001:dc0:2001:210:759c:46ea:5962:1ac5, Dst: 2001:dd8:b:201::12
▶ User Datagram Protocol, Src Port: 52782, Dst Port: 53
▼ Domain Name System (query)
    [Response In: 6529]
    Transaction ID: 0xeaf4
  ▶ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▼ apnic.net: type A, class IN
        Name: apnic.net
        [Name Length: 9]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▶ Additional records
```

DNS Traffic with DoT

46425	13.722600	2001:dc0:2001:210:81…	56133	2a04:b900:0:100::38	853	TLSv1.2	Client Hello
47098	14.031010	2a04:b900:0:100::38	853	2001:dc0:2001:210:813e:113…	56133	TLSv1.2	Server Hello
47100	14.031278	2a04:b900:0:100::38	853	2001:dc0:2001:210:813e:113…	56133	TLSv1.2	Certificate, Server Key Exchange, Server Hello Done
47116	14.033054	2001:dc0:2001:210:81…	56133	2a04:b900:0:100::38	853	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
47964	14.340459	2a04:b900:0:100::38	853	2001:dc0:2001:210:813e:113…	56133	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
47966	14.341004	2001:dc0:2001:210:81…	56133	2a04:b900:0:100::38	853	TLSv1.2	Application Data
488…	14.690309	2a04:b900:0:100::38	853	2001:dc0:2001:210:813e:113…	56133	TLSv1.2	Application Data
80858	24.693741	2001:dc0:2001:210:81…	56133	2a04:b900:0:100::38	853	TLSv1.2	Encrypted Alert
82580	25.001328	2a04:b900:0:100::38	853	2001:dc0:2001:210:813e:113…	56133	TLSv1.2	Encrypted Alert

```
▶ Frame 48851: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface 0
▶ Ethernet II, Src: Cisco_f4:96:81 (1c:df:0f:f4:96:81), Dst: Apple_92:51:06 (8c:85:90:92:51:06)
▶ Internet Protocol Version 6, Src: 2a04:b900:0:100::38, Dst: 2001:dc0:2001:210:813e:1136:f394:bf16
▶ Transmission Control Protocol, Src Port: 853, Dst Port: 56133, Seq: 3344, Ack: 453, Len: 154
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: dns
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 149
      Encrypted Application Data: 3a2defb8c3f03139855a3c6f284f52d6dc32891b00fcab7d...
```

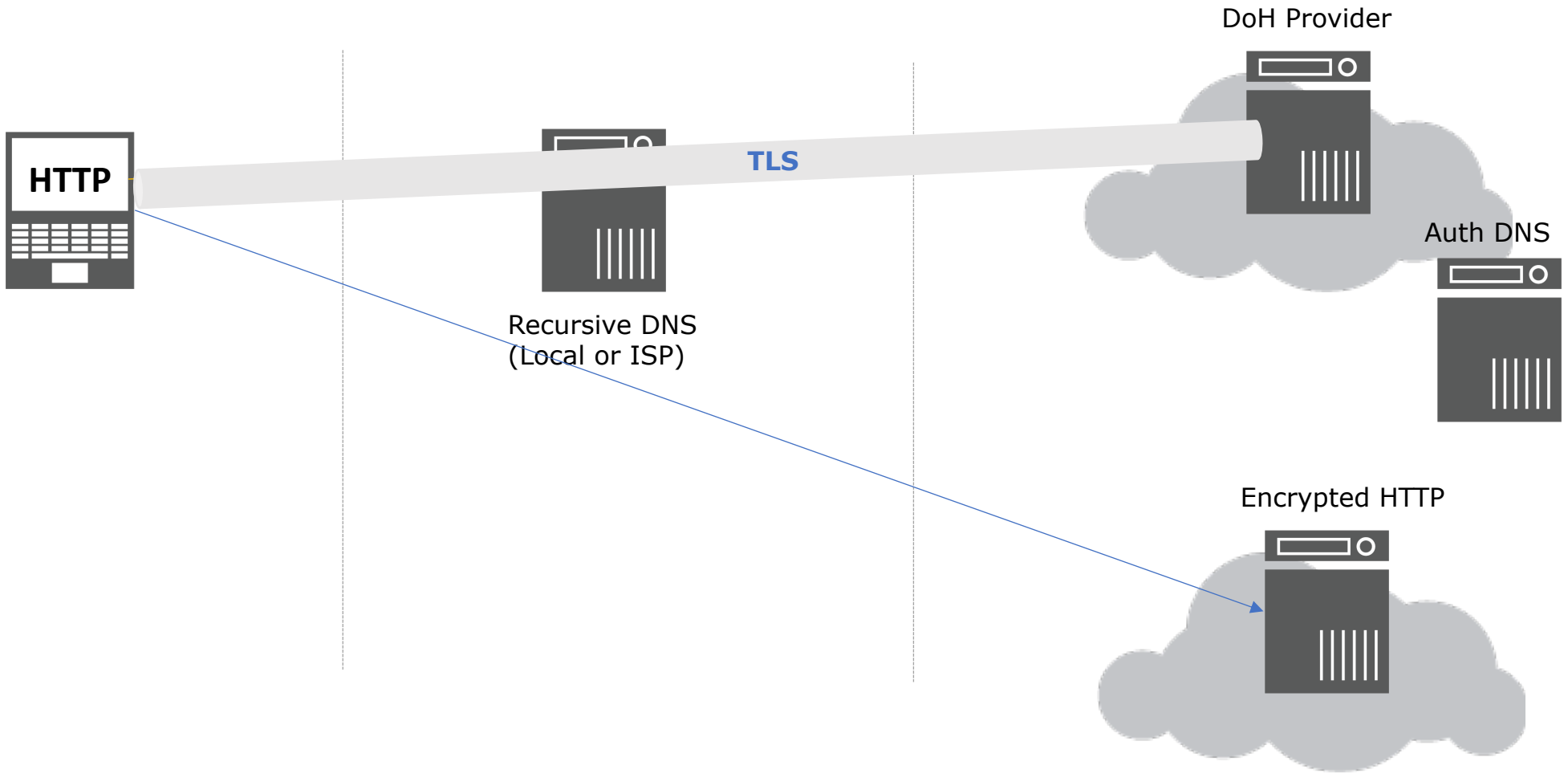
DNS over HTTPS (DoH)

- RFC 8484 – DNS over HTTPS
- DNS queries done securely over HTTPS

- Use cases:
  - prevents on-path devices from interfering with DNS operations
  - allows web applications to access DNS information via existing browser APIs

- Client follows a URI template to construct the URL to use for resolution
  - Uses the "application/dns-message" type

DoH – Architecture



DoH – URI format

Client encodes DNS query as an HTTP request (GET or POST)

```
:method = GET
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
accept = application/dns-message
```

```
:method = POST
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query
accept = application/dns-message
content-type = application/dns-message
content-length = 33
```

A successful HTTP Response will have 2xx status code

```
:status = 200
content-type = application/dns-message
content-length = 61
cache-control = max-age=3709
```

DoH – URI format

```
curl -H 'accept: application/dns-json' 'https://cloudflare-dns.com/dns-query?name=academy.apnic.net&type=AAAA' | jq
```

```
curl -H 'accept: application/dns-json' 'https://dns.google/resolve?name=academy.apnic.net&type=AAAA' | jq
```


```
{
  "Status": 0,
  "TC": false,
  "RD": true,
  "RA": true,
  "AD": true,
  "CD": false,
  "Question": [
    {
      "name": "academy.apnic.net.",
      "type": 28
    }
  ],
  "Answer": [
    {
      "name": "academy.apnic.net.",
      "type": 28,
      "TTL": 86400,
      "data": "2001:dd8:9:2::101:88"
    }
  ]
}
```

DoH Public Available Servers

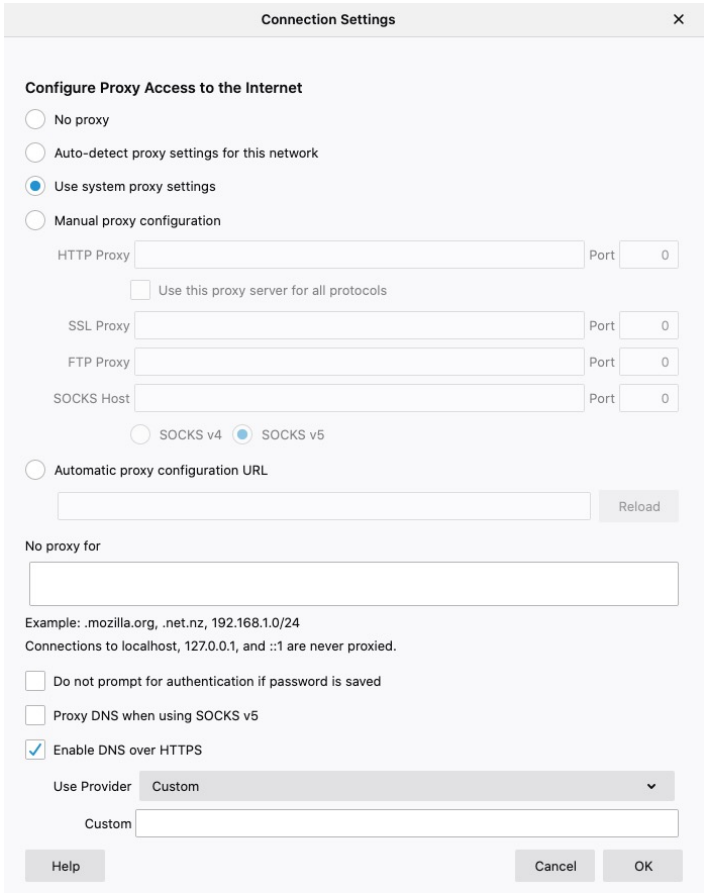
- DoH is supported by major providers
- There's a growing number of public servers to choose from
- You can also setup your own

Public DNS Providers	
Google	https://dns.google/dns-query
Cloudflare DNS	https://cloudflare-dns.com/dns-query
Quad9	https://dns.quad9.net/dns-query
PowerDNS	https://doh.powerdns.org
OpenDNS	https://doh.opendns.com/dns-query

https://github.com/curl/curl/wiki/DNS-over-HTTPS

DoH – Enabling in Firefox

Firefox supports DoH and plans to enable DoH protection by default



Trusted Recursive Server

about:networking#dns

DNS

Refresh | Autorefresh every 3 seconds

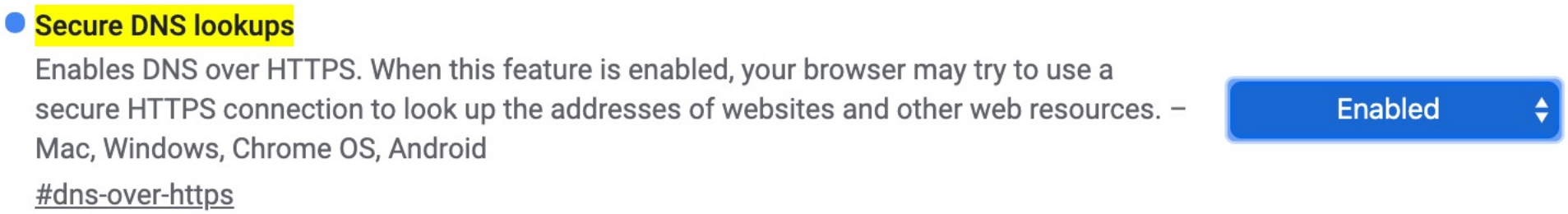
TRR Values
0 – off
1 – FF pick
3 – TRR only
5 – explicit off

Hostname	Family	TRR	Addresses	Expires (Seconds)
www.google.com.au	ipv4	true	172.217.167.99	53
www.cloudflare.com	ipv4	true	104.17.210.9 104.17.209.9	104
cloudflare-dns.com	ipv6	false	2606:4700::6810:f8f9 2606:4700::6810:f9f9	113
cgi1.apnic.net	ipv4	true	202.12.29.250	1172
w.usabilla.com	ipv4	true	13.211.226.87 3.105.55.226	59
ogs.google.com	ipv4	true	172.217.25.142	55
www.apnic.net	ipv4	true	104.20.22.173 104.20.36.173	57
sentry.io	ipv4	true	35.188.42.15	6664
snippets.cdn.mozilla.net	ipv4	false	13.35.146.126 13.35.146.33 13.35.146.72 13.35.146.91	81
ssl.gstatic.com	ipv4	true	172.217.167.67	53
mozilla.cloudflare-dns.com	ipv4	false	2606:4700::6810:f9f9 2606:4700::6810:f8f9 104.16.249.249 104.16.248.249	81

DoH – Enabling in Chrome

Chrome supports DoH as an experimental feature

`chrome://flags/#dns-over-https`



DoH – Using Proxy

- Several proxy servers available

Cloudflare

```
# cloudflared proxy-dns
INFO[0000] Adding DNS upstream                           url="https://1.1.1.1/dns-query"
INFO[0000] Adding DNS upstream                           url="https://1.0.0.1/dns-query"
INFO[0000] Starting metrics server                       addr="127.0.0.1:63194"
INFO[0000] Starting DNS over HTTPS proxy server          addr="dns://localhost:53"
```

Dnscrypt-proxy

```
# dnscrypt-proxy
[2019-11-26 22:12:27] [NOTICE] Source [public-resolvers.md] loaded
[2019-11-26 22:12:27] [NOTICE] dnscrypt-proxy 2.0.19
[2019-11-26 22:12:27] [NOTICE] Now listening to 127.0.0.1:53 [UDP]
[2019-11-26 22:12:27] [NOTICE] Now listening to 127.0.0.1:53 [TCP]
```

Issues and Criticisms

- Privacy issues
  - DNS data will not be subject to local laws if using third party DNS provider
- DNS Centralisation
  - Cloud providers have majority of the market share
- Debugging and protection
  - Unable to localize DNS filters
  - Can be used for data exfiltration

Future of DNS Privacy

- In terms of support,
  - DoT is supported in Android Pie, BIND, Unbound, and most public resolvers
  - DoH is supported by major public resolvers.
    - Windows will support DoH
    - Web services provider support DoH

- In terms of discussion,
  - active Internet drafts on
    - Authoritative DNS-over-TLS Operational Considerations
    - DNS Privacy Service Operators
  - IETF DPRIVE and ADD working groups


Questions

Thank You!