DoH and DoT Forwarder using BIND9
DOCUMENTATION
DoH

DNS over HTTPS (DoH) is a protocol that enhances the security and privacy of DNS resolution by encapsulating DNS queries and responses within HTTPS requests and responses. This document outlines the steps required to configure IPv6 DNS over HTTPS using BIND9.

BIND9 is an open-source DNS software that translates domain names into IP addresses and vice versa, offering robust features for DNS service management and deployment.

Environment:
The configuration detailed in this documentation was implemented on a Linux Mint operating system installed within a virtual machine running on Oracle VirtualBox.

1. **Configuration Steps**

a. Install BIND9

Ensure that BIND9 is installed on your server. If it's not already present, you can use the package manager to install it. Execute the following commands in the terminal:

```
sudo apt-get update
sudo apt-get install bind9
```

b. Edit named.conf

Modify the named.conf file to include configurations for DoH with ephemeral keys and IPv6 support. This involves adding the necessary directives to enable DoH functionality. Open the named.conf file in a text editor and add the following lines:

```
listen-on-v6 tls ephemeral http local { any; };
```

listen-on-v6 specifies that BIND9 should listen for incoming connections over IPv6.

Note:
When the name ephemeral is used, BIND9 generates ephemeral keys and certificates for the currently running named process. This enhances security by ensuring that each session uses unique encryption keys.

Once these configurations are saved, start the BIND9 service:

```
sudo systemctl start bind9
```

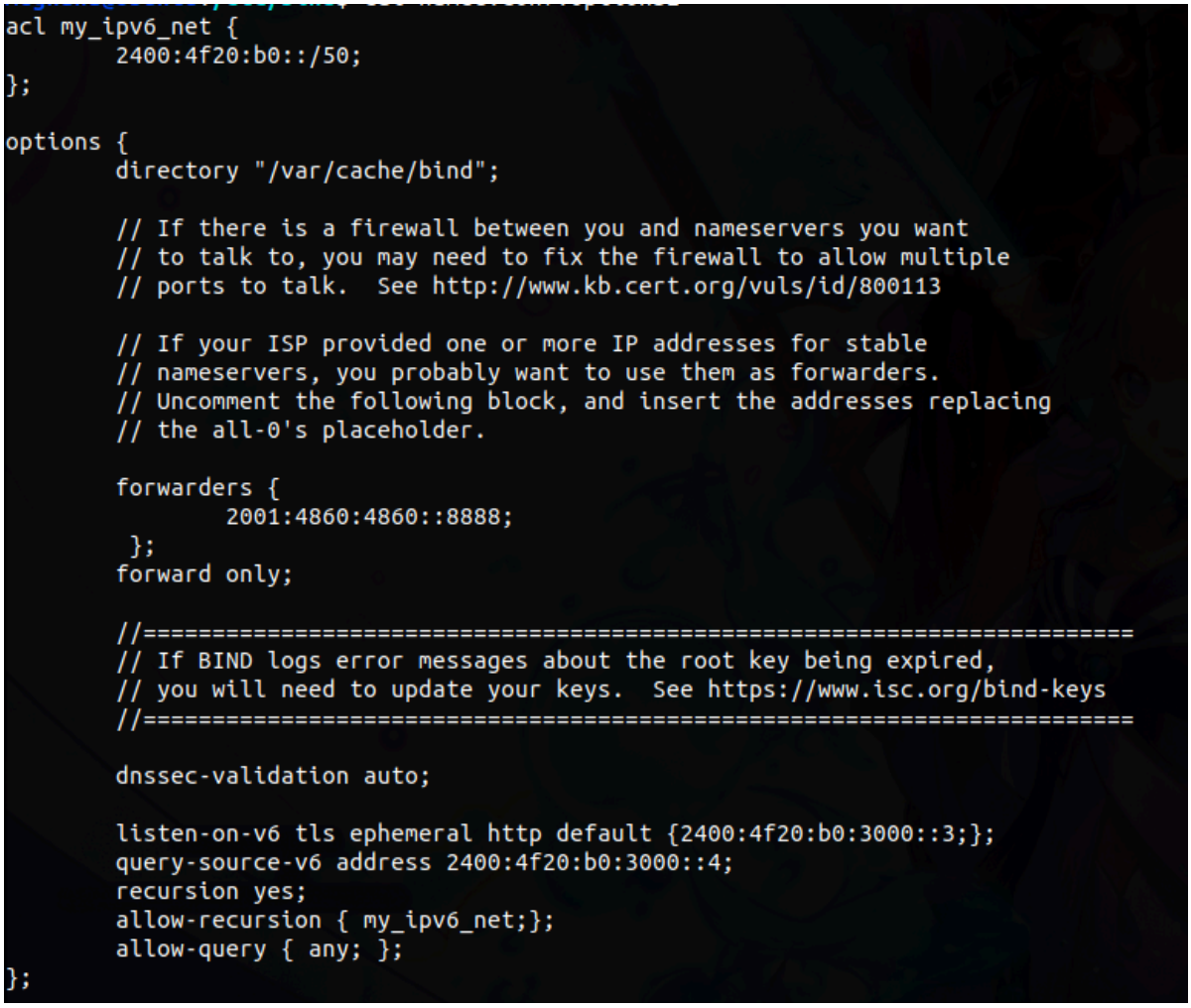
For any of the changes made subsequently restart the BIND9 service:

```
sudo systemctl restart bind9
```

With these steps completed, your BIND9 server should now be configured to support DNS over HTTPS using IPv6.

2. **Testing**

Initial Configuration in Existing DNS IPv6 Testbed *(Not tested)*



```
acl my_ipv6_net {
        2400:4f20:b0::/50;
};

options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                2001:4860:4860::8888;
         };
        forward only;

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================

        dnssec-validation auto;

        listen-on-v6 tls ephemeral http default {2400:4f20:b0:3000::3;};
        query-source-v6 address 2400:4f20:b0:3000::4;
        recursion yes;
        allow-recursion { my_ipv6_net;};
        allow-query { any; };
};
```

Working on our own systems using virtual box

Error Message:

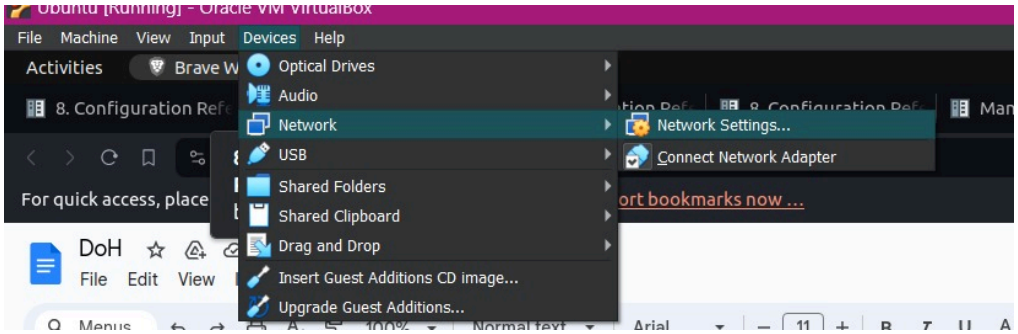
```
meghana@Ubuntu:/etc/bind$ ping -6 2001:4680:4680::8888
ping: connect: Network is unreachable
meghana@Ubuntu:/etc/bind$
```

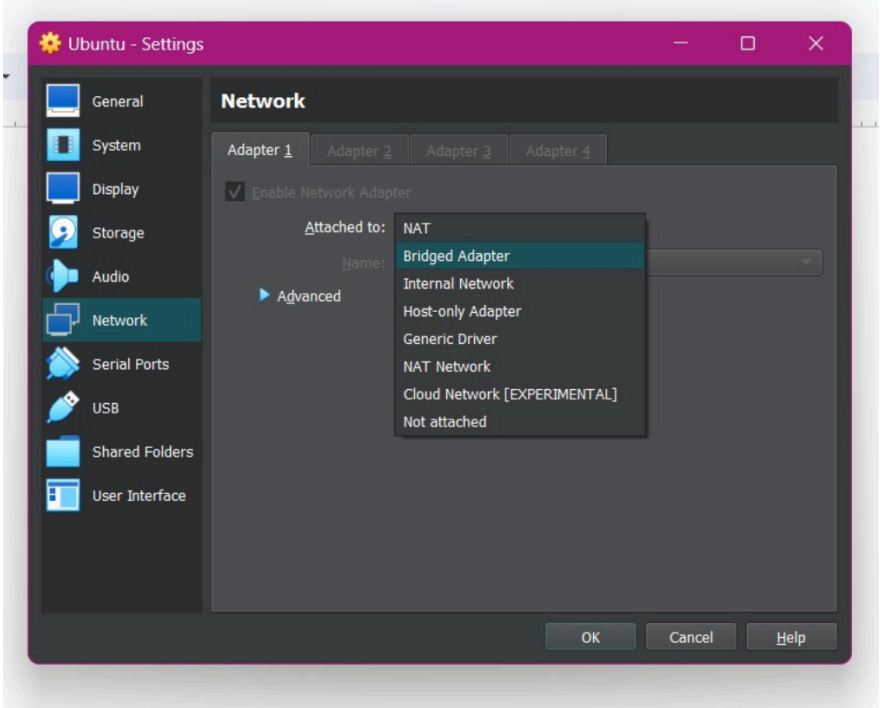
After changing:

```
meghana@Ubuntu:~$ ping -6 2001:4860:4860:0:0:0:0:8888
PING 2001:4860:4860:0:0:0:0:8888(2001:4860:4860::8888) 56 data bytes
^C
--- 2001:4860:4860:0:0:0:0:8888 ping statistics ---
41 packets transmitted, 0 received, 100% packet loss, time 41786ms
```

(Improvement)

1. **Change Network Settings in VirtualBox:**
   Update the network settings of the VirtualBox VM to use a Bridged Adapter instead of NAT. This adjustment ensures proper utilization of the IPv6 address from the main system and facilitates IP communication.






```
acl access_list{
      localhost; // Local computer itself
      localnets; // Local network it is a part of
};
controls { };

options {
      directory "/var/cache/bind";

      // If there is a firewall between you and nameservers you want
      // to talk to, you may need to fix the firewall to allow
multiple
      // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

      // If your ISP provided one or more IP addresses for stable
      // nameservers, you probably want to use them as forwarders.
      // Uncomment the following block, and insert the addresses
replacing
      // the all-0's placeholder.

      forwarders {
            2606:4700:4700::1111; // Cloudflare
            2606:4700:4700::1001;
```

```
            2001:4860:4860::8888; // Google
        };
       forward only;


//============================================================================
=====
       // If BIND logs error messages about the root key being
expired,
       // you will need to update your keys.  See
https://www.isc.org/bind-keys

//============================================================================
=====
       dnssec-validation auto;
       recursion yes;

       allow-query { access_list; };

       listen-on port 443 tls ephemeral http default { any; };
       listen-on-v6 port 443 tls ephemeral http default { any; };
};
```

```
meghana@meghana-VirtualBox:/etc/bind$ ping -6 google.com
PING google.com(maa03s43-in-x0e.1e100.net (2404:6800:4007:828::200e)) 56 data bytes
^C
--- google.com ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13532ms
```

The functionality of the "dig" command is verified to be operational when utilizing IPv6 and DNS over HTTPS (DoH). However, "dig" functionality is observed to be non-operational when attempting to use IPv4 and DoH. Additionally, "dig" does not function solely with IPv6.

```
meghana@meghana-VirtualBox:/etc/bind$ dig -6 google.com aaaa
;; communications error to ::1#53: connection refused
;; communications error to ::1#53: connection refused
;; communications error to ::1#53: connection refused

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> -6 google.com aaaa
;; global options: +cmd
;; no servers could be reached
```

```
meghana@meghana-VirtualBox:/etc/bind$ dig +https google.com aaaa
;; Connection to 127.0.0.53#443(127.0.0.53) for google.com failed: connection refused.
;; Connection to 127.0.0.53#443(127.0.0.53) for google.com failed: connection refused.
;; Connection to 127.0.0.53#443(127.0.0.53) for google.com failed: connection refused.
```

Despite attempts, connectivity to all addresses remains unattainable.

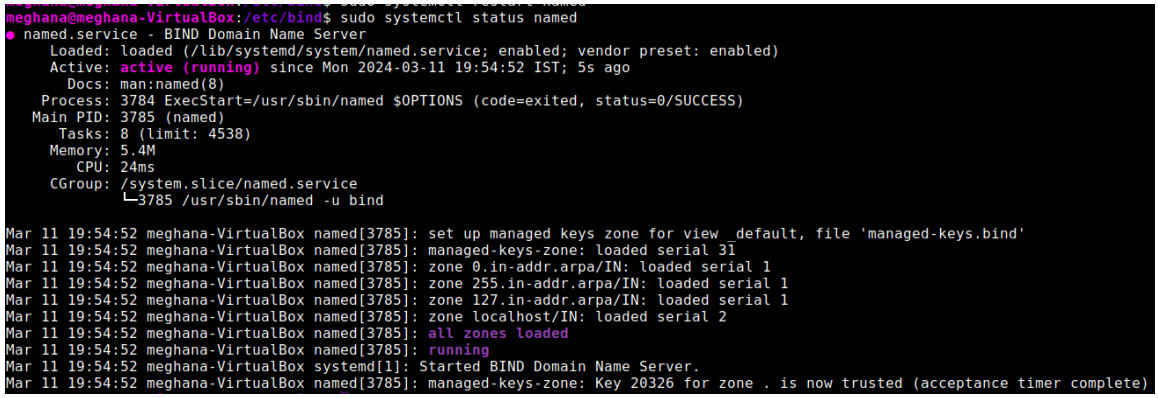
```
meghana@meghana-VirtualBox:/etc/bind$ sudo systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-03-11 19:35:30 IST; 17min ago
       Docs: man:named(8)
    Process: 2830 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 2831 (named)
      Tasks: 11 (limit: 4538)
     Memory: 6.0M
        CPU: 108ms
     CGroup: /system.slice/named.service
             └─2831 /usr/sbin/named -u bind

Mar 11 19:35:30 meghana-VirtualBox named[2831]: zone 127.in-addr.arpa/IN: loaded serial 1
Mar 11 19:35:30 meghana-VirtualBox named[2831]: all zones loaded
Mar 11 19:35:30 meghana-VirtualBox named[2831]: running
Mar 11 19:35:30 meghana-VirtualBox systemd[1]: Started BIND Domain Name Server.
Mar 11 19:35:30 meghana-VirtualBox named[2831]: network unreachable resolving './DNSKEY/IN': 2001:4860:4860::8888#53
Mar 11 19:35:30 meghana-VirtualBox named[2831]: network unreachable resolving './DNSKEY/IN': 2606:4700:4700::1111#53
Mar 11 19:35:30 meghana-VirtualBox named[2831]: network unreachable resolving './DNSKEY/IN': 2606:4700:4700::1001#53
Mar 11 19:35:30 meghana-VirtualBox named[2831]: managed-keys-zone: Unable to fetch DNSKEY set '.': SERVFAIL
Mar 11 19:38:09 meghana-VirtualBox named[2831]: listening on IPv6 interface enp0s3, 2409:4071:6e0e:42c8:8dd9:d4bd:9575:c772#443
Mar 11 19:38:09 meghana-VirtualBox named[2831]: listening on IPv6 interface enp0s3, 2409:4071:6e0e:42c8:773c:4a77:630f:de72#443
```

Changed file:

```
acl access_list{
      localhost; // Local computer itself
      localnets; // Local network it is a part of
      127.0.0.53;
};



controls { };

options {
      directory "/var/cache/bind";

      // If there is a firewall between you and nameservers you want
      // to talk to, you may need to fix the firewall to allow
multiple
      // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

      // If your ISP provided one or more IP addresses for stable
```

```
      // nameservers, you probably want to use them as forwarders.
      // Uncomment the following block, and insert the addresses
replacing
      // the all-0's placeholder.

      forwarders {
            2606:4700:4700::1111; // Cloudflare
            2606:4700:4700::1001;
            2001:4860:4860::8888; // Google
       };
      forward only;


//============================================================================
====
      // If BIND logs error messages about the root key being expired,
      // you will need to update your keys.  See
https://www.isc.org/bind-keys

//============================================================================
====
      dnssec-validation auto;
      recursion yes;

      allow-query { access_list; };
      allow-query-cache { access_list; };
      allow-recursion { access_list; };

      listen-on-v6 { ::1; };
      listen-on { 127.0.0.1; 127.0.0.53; };
      listen-on port 443 tls ephemeral http default { 127.0.0.1;
127.0.0.53; };
      listen-on-v6 port 443 tls ephemeral http default { ::1; };
};
```

Status is all clear now.



Dig for IPv4 and IPv6 are working.

```
meghana@meghana-VirtualBox:/etc/bind$ dig google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5387
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             124     IN      A       142.250.195.238

;; Query time: 168 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Mar 11 19:55:44 IST 2024
;; MSG SIZE  rcvd: 55

meghana@meghana-VirtualBox:/etc/bind$ dig -6 google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> -6 google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9735
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0df603ca8686a0c10100000065ef146fc2532944622bb8d0 (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             300     IN      A       142.250.77.142

;; Query time: 324 msec
;; SERVER: ::1#53(::1) (UDP)
;; WHEN: Mon Mar 11 19:55:51 IST 2024
;; MSG SIZE  rcvd: 83
```

Dig for Ipv6 With HTTPS is working.

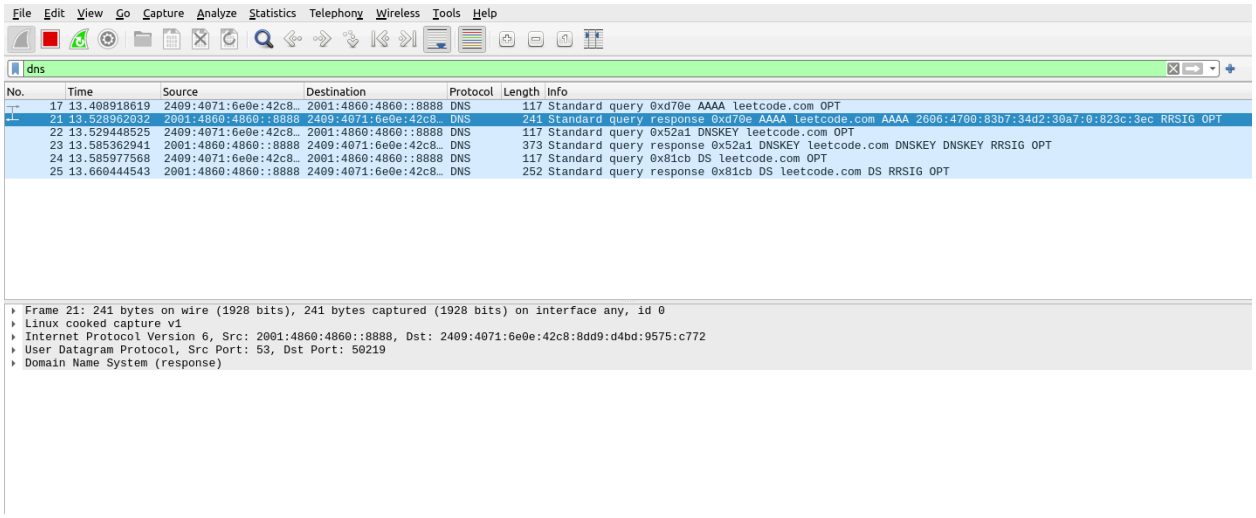
```
meghana@meghana-VirtualBox:/etc/bind$ dig -6 +https google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> -6 +https google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52522
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: bbc62b5be2e5aab50100000065ef14803364253176a673ad (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             283     IN      A       142.250.77.142

;; Query time: 0 msec
;; SERVER: ::1#443(::1) (HTTPS)
;; WHEN: Mon Mar 11 19:56:08 IST 2024
;; MSG SIZE  rcvd: 83
```

The functionality of IPv4 with DNS over HTTPS (DoH) remains unresolved.

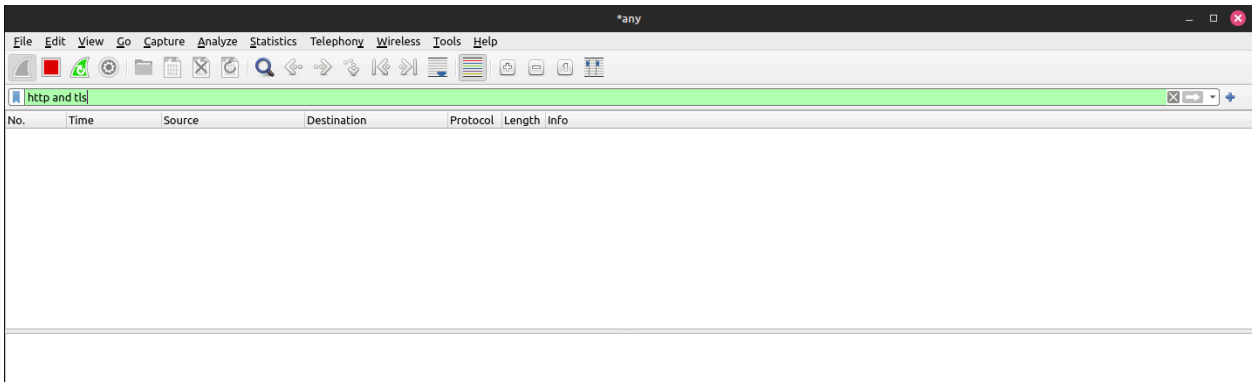
For the results:

While conducting packet tracing, we experimented with sending requests using the dig command and attempted to capture them using Wireshark. Typically, under normal circumstances, deciphering the content of an HTTP request is challenging due to encryption, as seen in protocols like QUIC and TLS. When utilizing display filters set to HTTP, we observed that packets directed to the specified DNS resolver were not captured, but we were successful in capturing them using DNS display filters.

This observation supports a point outlined in the BIND9 documentation, indicating that forwarding with DNS over HTTPS (DoH) is not currently implemented. Despite the DoH server receiving requests from the client, it forwards these requests using traditional DNS (UDP) rather than DoH.

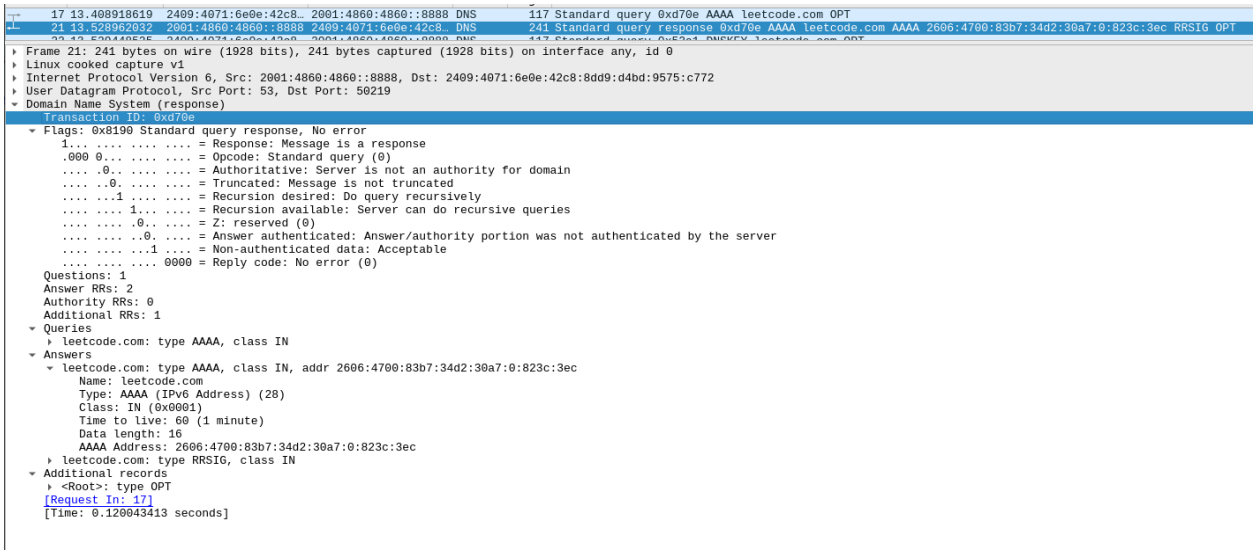


Above are the packet capture in the case of DNS (this shouldn't have appeared if it was DoH).



Nothing appears for DoH.

```
meghana@meghana-VirtualBox:/etc/bind$ dig -6 +https leetcode.com aaaa

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> -6 +https leetcode.com aaaa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17153
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3f06e5c8582676580100000065ef20bff7923cd25f173172 (good)
;; QUESTION SECTION:
;leetcode.com.                  IN      AAAA

;; ANSWER SECTION:
leetcode.com.           60      IN      AAAA    2606:4700:83b7:34d2:30a7:0:823c:3ec

;; Query time: 252 msec
;; SERVER: ::1#443(::1) (HTTPS)
;; WHEN: Mon Mar 11 20:48:23 IST 2024
;; MSG SIZE  rcvd: 97
```

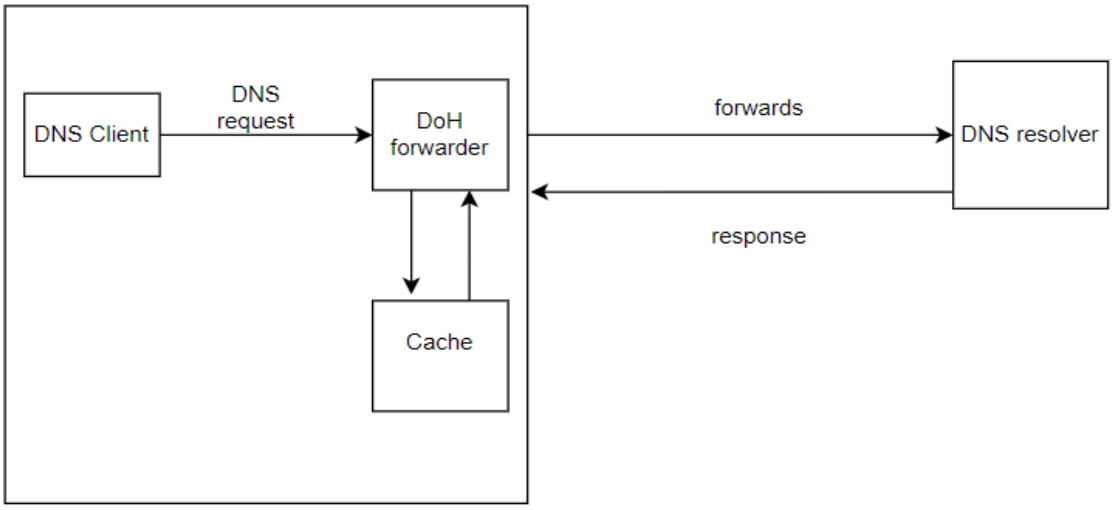

17 13.408918619 2409:4071:6e0e:42c8… 2001:4860:4860::8888 DNS 117 Standard query 0xd70e AAAA leetcode.com OPT
21 13.528962032 2001:4860:4860::8888 2409:4071:6e0e:42c8… DNS 241 Standard query response 0xd70e AAAA leetcode.com AAAA 2606:4700:83b7:34d2:30a7:0:823c:3ec RRSIG OPT
Frame 21: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 6, Src: 2001:4860:4860::8888, Dst: 2409:4071:6e0e:42c8:8dd9:d4bd:9575:c772
User Datagram Protocol, Src Port: 53, Dst Port: 50219
Domain Name System (response)
Transaction ID: 0xd70e
Flags: 0x8190 Standard query response, No error
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....1 .... = Non-authenticated data: Acceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 1
Queries
leetcode.com: type AAAA, class IN
Answers
leetcode.com: type AAAA, class IN, addr 2606:4700:83b7:34d2:30a7:0:823c:3ec
Name: leetcode.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 16
AAAA Address: 2606:4700:83b7:34d2:30a7:0:823c:3ec
leetcode.com: type RRSIG, class IN
Additional records
<Root>: type OPT
[Request In: 17]
[Time: 0.120043413 seconds]

DoT (DNS over TLS) forwarder using BIND9

DNS over TLS (DoT) is a network security protocol for encrypting and wrapping Domain Name System (DNS) queries and answers via the Transport Layer Security (TLS) protocol. This provides an additional layer of security for the queries.

Observation:
BIND9 doesn't have a native support for DoH as a forwarder. So when the packets were traced using wireshark, they were sent on normal DNS, and not over https. Only the path from client to the forwarder is over https, but from forwarder to dns server, it's normal DNS.

The DoT(DNS over TLS) forwarder is present in the development version 9.19.10



Working: When a DNS over TLS (DoT) forwarder receives a DNS request from a client, it initially checks its cache for the requested entry. If the entry is not found in the cache, the forwarder securely forwards the request to a DNS resolver using TLS. Subsequently, the DNS resolver responds to the request also through TLS.

Approach 1 (doesn't work in the background)**:**
Building the development version of BIND9 (9.19.21) and setting it up as a DoT forwarder:

Installation and building

Persistent issue with the following is that we are unable to run it in the background using systemctl as it is unable to find the named.service file.

1. Install the tar.xz file from the official isc website.
   (Link: https://www.isc.org/download/)
   The version installed in the testing system is 9.19.21
2. Run the following to open the tar.xz file

```
tar xf bind-9.19.21.tar.xz
```

3. Run the following commands to install the possibly missing packages:

```
sudo apt update
sudo apt install liburcu-dev
sudo apt install libuv1-dev
sudo apt install libnghttp2-dev
sudo apt install libssl-dev
sudo apt install libcap-dev
sudo apt install libjemalloc-dev
```

4. Now make the file using the following commands to complete the installation.

```
cd bind-9.19.21
./configure
make
sudo make install
```

5. Create a named.conf file in the /usr/local/etc and check the version as well as some debugging carried out using the following commands:

```
sudo touch /usr/local/etc/named.conf
named -v //Check the version
named -g //Debugging (runs it in foreground)

sudo rndc-confgen -a //create rndc.key in /usr/local/etc
```

6. Start the DNS and check the status

```
sudo named
sudo systemctl start named
sudo systemctl enable named
```

7. In another tab make requests like

```
dig -6 +tls leetcode.com
dig -6 +tls google.com aaaa
```

named.conf used for the testing

```
 acl access_list{
      localhost; // Local computer itself
      localnets; // Local network it is a part of
      127.0.0.53;
};



controls { };

options {
      directory "/var/cache/bind";
      // If there is a firewall between you and nameservers you want
      // to talk to, you may need to fix the firewall to allow multiple
      // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

      // If your ISP provided one or more IP addresses for stable
      // nameservers, you probably want to use them as forwarders.
      // Uncomment the following block, and insert the addresses replacing
      // the all-0's placeholder.

      forwarders port 853 tls ephemeral{
            2606:4700:4700::1111; // Cloudflare
            2606:4700:4700::1001;
            2001:4860:4860::8888; // Google
       };
      forward only;


//========================================================================
      // If BIND logs error messages about the root key being expired,
      //    you    will    need    to    update    your    keys.        See
https://www.isc.org/bind-keys

//========================================================================
      dnssec-validation auto;
      recursion yes;

      allow-query { access_list; };
      allow-query-cache { access_list; };
      allow-recursion { access_list; };

      listen-on-v6 { ::1; };
```

```
        listen-on { 127.0.0.1; 127.0.0.53; };
        listen-on port 853 tls ephemeral { 127.0.0.1; 127.0.0.53; };
        listen-on-v6 port 853 tls ephemeral { ::1; };
};
```

Results:

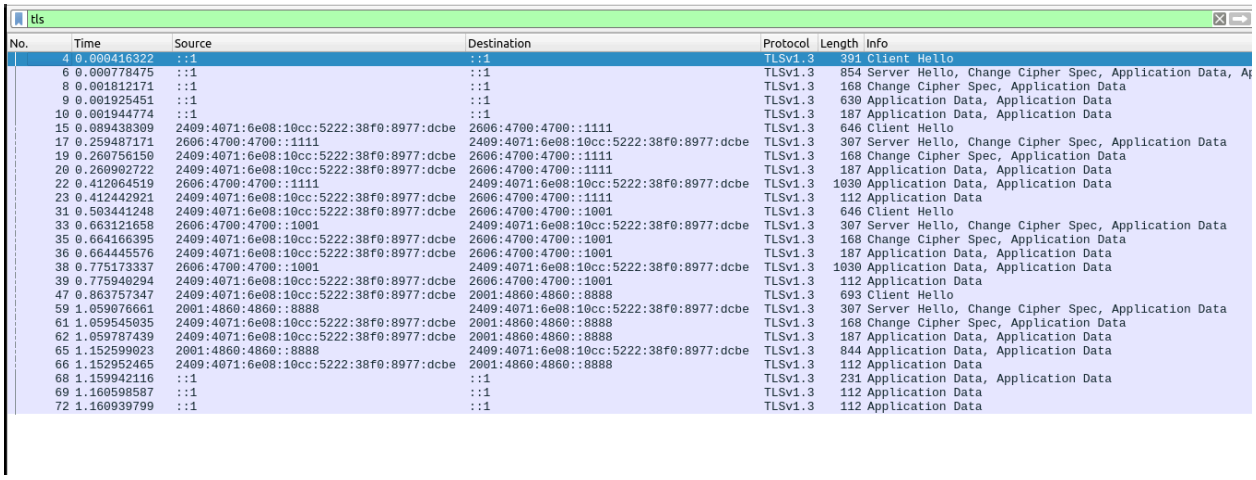
Dig queries of different kind

```
meghana@meghana-VirtualBox:~/Documents$ dig -6 +tls google.com aaaa

; <<>> DiG 9.19.21 <<>> -6 +tls google.com aaaa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36645
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4a79d317fab014540100000065fb087037b8065f68757566 (good)
;; QUESTION SECTION:
;google.com.                    IN      AAAA

;; ANSWER SECTION:
google.com.             300     IN      AAAA    2404:6800:4007:817::200e

;; Query time: 696 msec
;; SERVER: ::1#853(::1) (TLS)
;; WHEN: Wed Mar 20 21:31:52 IST 2024
;; MSG SIZE  rcvd: 95
```

```
meghana@meghana-VirtualBox:~/Documents$ dig -6 +tls leetcode.com

; <<>> DiG 9.19.21 <<>> -6 +tls leetcode.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18283
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 72e9dc3ba5e402670100000065fb04269fc9897e0ad03581 (good)
;; QUESTION SECTION:
;leetcode.com.                  IN      A

;; ANSWER SECTION:
leetcode.com.           300     IN      A       104.22.27.181
leetcode.com.           300     IN      A       104.22.26.181
leetcode.com.           300     IN      A       172.67.6.3

;; Query time: 765 msec
;; SERVER: ::1#853(::1) (TLS)
;; WHEN: Wed Mar 20 21:13:34 IST 2024
;; MSG SIZE  rcvd: 117
```

Dig queries along with their packet traces.

```
meghana@meghana-VirtualBox:/etc$ dig -6 +tls leetcode.com aaaa

; <<>> DiG 9.19.21 <<>> -6 +tls leetcode.com aaaa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45654
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6b2950aec674f2500100000065fb27b36a1f652bb7b4830a (good)
;; QUESTION SECTION:
;leetcode.com.                  IN      AAAA

;; ANSWER SECTION:
leetcode.com.           60      IN      AAAA    2606:4700:8de7:35d4:8fdd:0:823c:3
ec

;; Query time: 1155 msec
;; SERVER: ::1#853(::1) (TLS)
;; WHEN: Wed Mar 20 23:45:15 IST 2024
;; MSG SIZE  rcvd: 97
```



tls

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000416322	::1	::1	TLSv1.3	391	Client Hello
6	0.000778475	::1	::1	TLSv1.3	854	Server Hello, Change Cipher Spec, Application Data, Ap
8	0.001812171	::1	::1	TLSv1.3	168	Change Cipher Spec, Application Data
9	0.001925451	::1	::1	TLSv1.3	630	Application Data, Application Data
10	0.001944774	::1	::1	TLSv1.3	187	Application Data, Application Data
15	0.089438309	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1111	TLSv1.3	646	Client Hello
17	0.259487171	2606:4700:4700::1111	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	307	Server Hello, Change Cipher Spec, Application Data
19	0.260756150	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1111	TLSv1.3	168	Change Cipher Spec, Application Data
20	0.260902722	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1111	TLSv1.3	187	Application Data, Application Data
22	0.412064519	2606:4700:4700::1111	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	1030	Application Data, Application Data
23	0.412442921	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1111	TLSv1.3	112	Application Data
31	0.503441248	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1001	TLSv1.3	646	Client Hello
33	0.663121658	2606:4700:4700::1001	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	307	Server Hello, Change Cipher Spec, Application Data
35	0.664166395	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1001	TLSv1.3	168	Change Cipher Spec, Application Data
36	0.664445576	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1001	TLSv1.3	187	Application Data, Application Data
38	0.775173337	2606:4700:4700::1001	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	1030	Application Data, Application Data
39	0.775940294	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1001	TLSv1.3	112	Application Data
47	0.863757347	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2001:4860:4860::8888	TLSv1.3	693	Client Hello
59	1.059076661	2001:4860:4860::8888	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	307	Server Hello, Change Cipher Spec, Application Data
61	1.059545035	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2001:4860:4860::8888	TLSv1.3	168	Change Cipher Spec, Application Data
62	1.059787439	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2001:4860:4860::8888	TLSv1.3	187	Application Data, Application Data
65	1.152599023	2001:4860:4860::8888	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	844	Application Data, Application Data
66	1.152952465	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2001:4860:4860::8888	TLSv1.3	112	Application Data
68	1.159942116	::1	::1	TLSv1.3	231	Application Data, Application Data
69	1.160598587	::1	::1	TLSv1.3	112	Application Data
72	1.160939799	::1	::1	TLSv1.3	112	Application Data

Source	Destination	Protocol	L
::1	::1	TLSv1.3	
::1	::1	TLSv1.3	
::1	::1	TLSv1.3	
::1	::1	TLSv1.3	
::1	::1	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1111	TLSv1.3	
2606:4700:4700::1111	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1111	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1111	TLSv1.3	
2606:4700:4700::1111	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1111	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1001	TLSv1.3	
2606:4700:4700::1001	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1001	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1001	TLSv1.3	
2606:4700:4700::1001	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2606:4700:4700::1001	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2001:4860:4860::8888	TLSv1.3	
2001:4860:4860::8888	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2001:4860:4860::8888	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2001:4860:4860::8888	TLSv1.3	
2001:4860:4860::8888	2409:4071:6e08:10cc:5222:38f0:8977:dcbe	TLSv1.3	
2409:4071:6e08:10cc:5222:38f0:8977:dcbe	2001:4860:4860::8888	TLSv1.3	
::1	::1	TLSv1.3	
::1	::1	TLSv1.3	
::1	::1	TLSv1.3	

Faced Errors

1. On doing ./configure there were errors faced due to missing packages due to which the make file wasn't generating. On looking at the missing package and some trial and error the required packages were found and are documented in the installation section.

   One of the error messages

```
checking whether C compiler accepts -fno-strict-aliasing... yes
checking whether C compiler accepts -Werror -fno-delete-null-pointer-checks... yes
checking whether C compiler accepts -fdiagnostics-show-option... yes
checking whether the linker accepts -Wl,--export-dynamic... yes
checking for pkg-config... /usr/bin/pkg-config
checking pkg-config is at least version 0.9.0... yes
checking liburcu flavor... liburcu
checking for liburcu >= 0.13.0 liburcu-cds >= 0.13.0... no
checking for liburcu >= 0.10.0 liburcu-cds >= 0.10.0... no
configure: error: Package requirements (liburcu >= 0.10.0 liburcu-cds >= 0.10.0) were not
 met:

No package 'liburcu' found
No package 'liburcu-cds' found

Consider adjusting the PKG_CONFIG_PATH environment variable if you
installed software in a non-standard prefix.

Alternatively, you may set the environment variables LIBURCU_CFLAGS
and LIBURCU_LIBS to avoid the need to call pkg-config.
See the pkg-config man page for more details.
```

   Resolution: on searching package names using the following command

```
sudo apt search <package_name>
```

2. On running named -v the following error message is displayed:

```
meghana@meghana-VirtualBox:/etc/bind-9.19.21$ named -v
named: error while loading shared libraries: libisc-9.19.21.so: cannot open shared object file: No such file
or directory
```

Trial 1: This is presumed to be caused by the multiple bind servers that have been created as a result of running the development version installation as well as the stable installation using apt. On uninstalling the makes using the command below after running the same ./configure options

```
sudo make uninstall
```

On doing so-

```
BIND 9.18.18-0ubuntu0.22.04.2-Ubuntu (Extended Support Version) <id:>
```

This is because we can't have multiple versions of the same package on the same system. Hence the older version has to be removed.

Uninstalling the older version

a. Copy the older configuration files for reference (if needed)

```
cp named.conf.options ~/Documents/ipv6-dns-config
```

b. Run the following commands:

```
sudo systemctl stop bind9
sudo apt-get purge bind9
sudo rm -rf /etc/bind
sudo rm -rf /var/cache/bind
sudo apt-get update
```

Followed the configuration shown in installation after this.

(Issue isn't resolved after doing this)

Trial 2 (success): There is a lack of named.conf file so to create one.

```
sudo touch /etc/named.conf
```

After trying the command the results remained the same.

```
meghana@meghana-VirtualBox:/etc$ sudo named -v
named: error while loading shared libraries: libisc-9.19.21.so: cannot
open shared object file: No such file or directory
```

Resolution:

Run the command

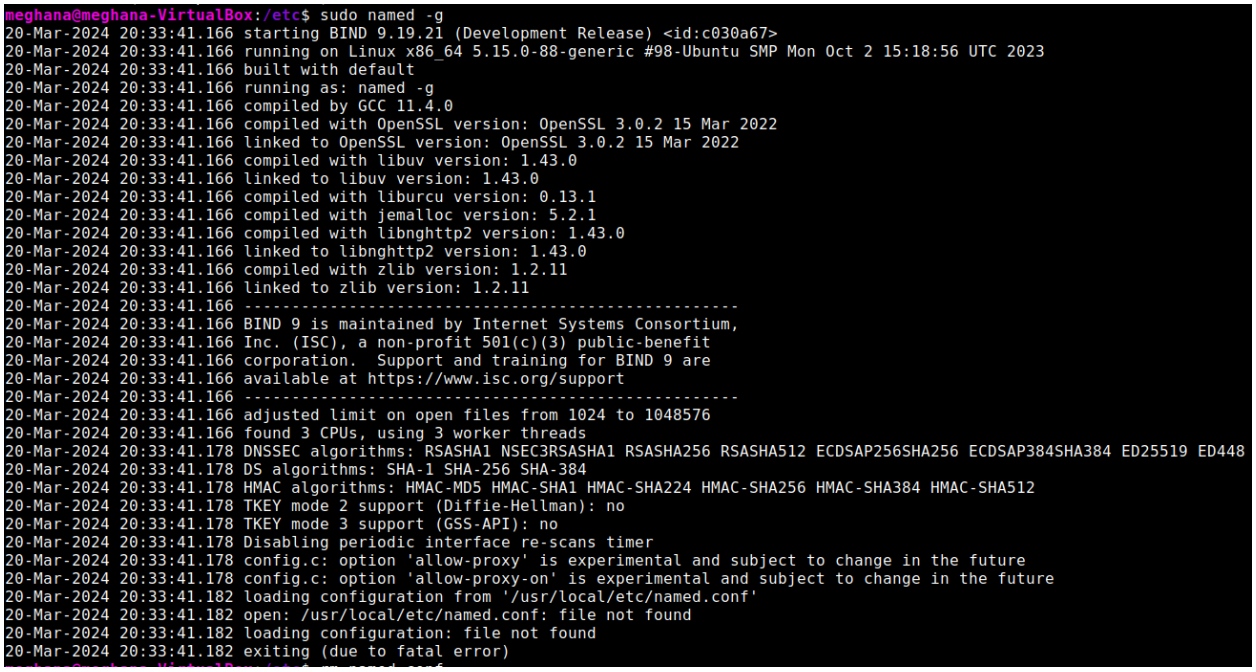
```
sudo ldconfig
```

After this the issue is resolved and the version number is displayed.

Even on installing back bind9 using apt the version remains the same

```
meghana@meghana-VirtualBox:/etc$ sudo named -v
BIND 9.19.21 (Development Release) <id:c030a67>
```

3. Issue was faced on running the command for debugging.



The error says that the named.conf file is searched in the /usr/local/etc folder. On adding that the named version is displayed as well as the logs are working completely without error.

4. One big factor is that running

```
sudo systemctl start named
sudo systemctl status named
```

Only starts the named bind9 file that may be installed using apt.
(Have to look into configuration changes if needed)

However to start the server use the command `sudo named -g`. This however makes it run in the foreground only (can be used for debugging).
In another tab make tls requests using dig and use the configuration for named.conf as defined before.
Solution for the above:
Added the `daemon on;` to the `options` block in the named.conf file and then ran the following commands

```
sudo named
sudo systemctl start named
sudo systemctl enable named
```

This allows the new named to run in the background as well.
Trying to make it run in the background without the daemon on; addition, the named is not recognized as a service.

```
 acl access_list{
      localhost; // Local computer itself
      localnets; // Local network it is a part of
      127.0.0.53;
};



controls { };

options {
      directory "/var/cache/bind";
      daemon on;
      // If there is a firewall between you and nameservers you want
      // to talk to, you may need to fix the firewall to allow multiple
      // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

      // If your ISP provided one or more IP addresses for stable
      // nameservers, you probably want to use them as forwarders.
      // Uncomment the following block, and insert the addresses replacing
      // the all-0's placeholder.

      forwarders port 853 tls ephemeral{
            2606:4700:4700::1111; // Cloudflare
            2606:4700:4700::1001;
            2001:4860:4860::8888; // Google
       };
      forward only;


//========================================================================
      // If BIND logs error messages about the root key being expired,
      //    you    will    need    to    update    your    keys.        See
https://www.isc.org/bind-keys

//========================================================================
      dnssec-validation auto;
      recursion yes;

      allow-query { access_list; };
      allow-query-cache { access_list; };
```

```
      allow-recursion { access_list; };

      listen-on-v6 { ::1; };
      listen-on { 127.0.0.1; 127.0.0.53; };
      listen-on port 853 tls ephemeral { 127.0.0.1; 127.0.0.53; };
      listen-on-v6 port 853 tls ephemeral { ::1; };
};
```

However after running these commands once they are not running again.

Observations:
Running bind9 in the foreground requires the installation of a stable bind9-utils version

---

Approach 2 (works in background too)

Installation is done in a different way by adding the repo of the dev version of bind to the docs and that allows the installation of the development version of bind using apt.

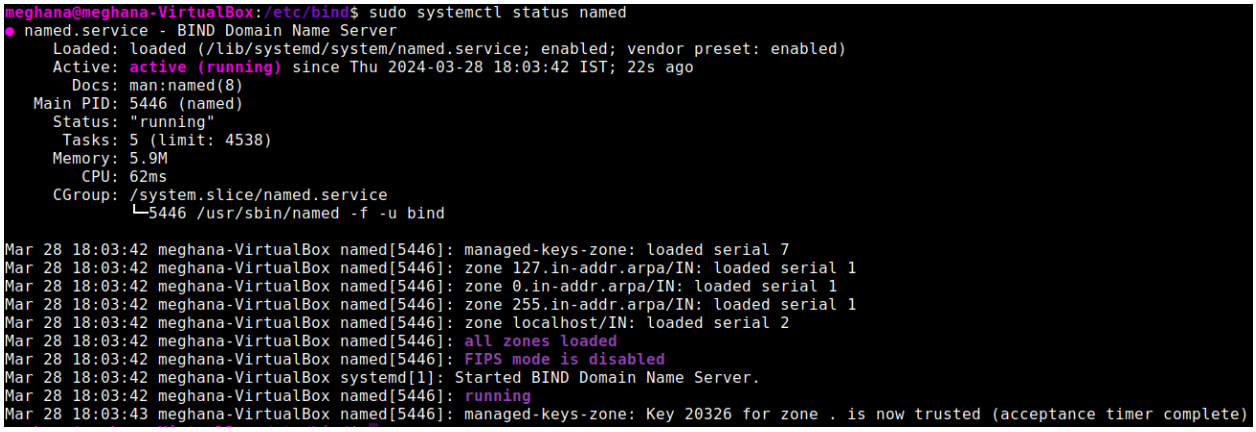
Configuration is written in a similar fashion and this is able to run in the background normally.

DoT
Installation

1. The following allows you to add the bind9 development release packages and that when downloading the latest development one is the one that is installed.
   ```
   sudo add-apt-repository ppa:isc/bind-dev
   ```
2. Install bind9
   ```
   sudo apt-get update
   sudo apt-get install bind9
   ```
3. Update the named.conf.options file in the `/etc/bind` folder
4. To enable the service to run in background and start it
   ```
   sudo systemctl enable named
   sudo systemctl start named
   ```
5. To restart bind after any configuration changes
   ```
   sudo systemctl restart named
   ```
6. To check the status

```
sudo systemctl status named
```

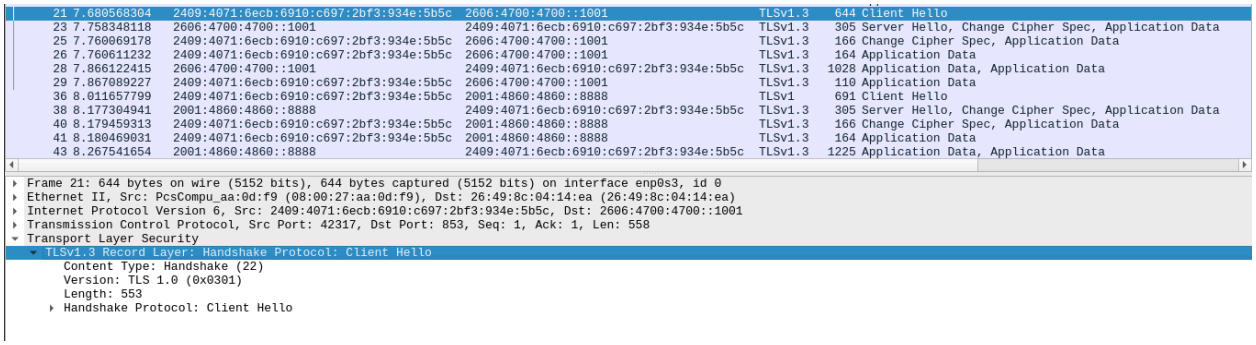
Configuration fileOutput Screenshots



Packet traces screenshots

```
meghana@meghana-VirtualBox:~$ dig -6 +tls microsoft.com
;; Connection to ::1#853(::1) for microsoft.com failed: timed out.
;; no servers could be reached


; <<>> DiG 9.19.22-1+ubuntu22.04.1+deb.sury.org+1-Ubuntu <<>> -6 +tls microsoft.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57766
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c849a5061e377fe70100000066056abd854f4096279b269d (good)
;; QUESTION SECTION:
;microsoft.com.                 IN      A

;; ANSWER SECTION:
microsoft.com.          3600    IN      A       20.231.239.246
microsoft.com.          3600    IN      A       20.76.201.171
microsoft.com.          3600    IN      A       20.236.44.162
microsoft.com.          3600    IN      A       20.70.246.20
microsoft.com.          3600    IN      A       20.112.250.133

;; Query time: 659 msec
;; SERVER: ::1#853(::1) (TLS)
;; WHEN: Thu Mar 28 18:33:57 IST 2024
;; MSG SIZE  rcvd: 150
```

The below packet traces depict the tls requests being sent to the dns servers configured in the configuration file.



The pcapng files are stored in the following drive link

DoT packets

Errors faced

1. Servers couldnt be reached (tries 3 times)

```
meghana@meghana-VirtualBox:/etc/bind$ dig -6 +tls leetcode.com
;; Connection to ::1#853(::1) for leetcode.com failed: timed out.
;; no servers could be reached

;; Connection to ::1#853(::1) for leetcode.com failed: timed out.
;; no servers could be reached

;; Connection to ::1#853(::1) for leetcode.com failed: timed out.
;; no servers could be reached
```

Observed that the dns server is reachable by using ping

```
meghana@meghana-VirtualBox:/etc/bind$ ping -6 2606:4700:4700::1111
PING 2606:4700:4700::1111(2606:4700:4700::1111) 56 data bytes
64 bytes from 2606:4700:4700::1111: icmp_seq=1 ttl=58 time=323 ms
64 bytes from 2606:4700:4700::1111: icmp_seq=2 ttl=58 time=244 ms
64 bytes from 2606:4700:4700::1111: icmp_seq=3 ttl=58 time=265 ms
64 bytes from 2606:4700:4700::1111: icmp_seq=4 ttl=58 time=185 ms
^C
--- 2606:4700:4700::1111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 184.701/254.297/323.336/49.547 ms
```

Sudo systemctl status named gives the following output

Mar 28 16:59:24 meghana-VirtualBox named[3647]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints

Mar 28 16:59:24 meghana-VirtualBox named[3647]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints

Mar 28 16:59:24 meghana-VirtualBox named[3647]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints

Mar 28 16:59:24 meghana-VirtualBox named[3647]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record in hints
There is nothing broken and it will get taken care of upstream. (as said in ubuntu stack overflow)
The older configuration and download being used earlier was uninstalled and the changes were observed. (None work below implying that the situation hasn't changed)

1. Dig works (temporarily didn't work)
2. Dig -6 works normally
3. Dig with tls doesn't work
4. Dig with -6 and tls doesn't work

However the status has now changed
Old-

```
meghana@meghana-VirtualBox:/etc/bind$ sudo systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-03-28 16:59:24 IST; 11min ago
       Docs: man:named(8)
   Main PID: 3647 (named)
     Status: "running"
      Tasks: 8 (limit: 4538)
     Memory: 6.8M
        CPU: 48ms
     CGroup: /system.slice/named.service
             └─3647 /usr/sbin/named -f -u bind

Mar 28 16:59:24 meghana-VirtualBox named[3647]: zone 255.in-addr.arpa/IN: loaded serial 1
Mar 28 16:59:24 meghana-VirtualBox named[3647]: all zones loaded
Mar 28 16:59:24 meghana-VirtualBox named[3647]: FIPS mode is disabled
Mar 28 16:59:24 meghana-VirtualBox named[3647]: running
Mar 28 16:59:24 meghana-VirtualBox systemd[1]: Started BIND Domain Name Server.
Mar 28 16:59:24 meghana-VirtualBox named[3647]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
Mar 28 16:59:24 meghana-VirtualBox named[3647]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
Mar 28 16:59:24 meghana-VirtualBox named[3647]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints
Mar 28 16:59:24 meghana-VirtualBox named[3647]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
Mar 28 16:59:24 meghana-VirtualBox named[3647]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record in hints
```

New -

```
meghana@meghana-VirtualBox:/etc/bind$ sudo systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-03-28 18:03:42 IST; 22s ago
       Docs: man:named(8)
   Main PID: 5446 (named)
     Status: "running"
      Tasks: 5 (limit: 4538)
     Memory: 5.9M
        CPU: 62ms
     CGroup: /system.slice/named.service
             └─5446 /usr/sbin/named -f -u bind

Mar 28 18:03:42 meghana-VirtualBox named[5446]: managed-keys-zone: loaded serial 7
Mar 28 18:03:42 meghana-VirtualBox named[5446]: zone 127.in-addr.arpa/IN: loaded serial 1
Mar 28 18:03:42 meghana-VirtualBox named[5446]: zone 0.in-addr.arpa/IN: loaded serial 1
Mar 28 18:03:42 meghana-VirtualBox named[5446]: zone 255.in-addr.arpa/IN: loaded serial 1
Mar 28 18:03:42 meghana-VirtualBox named[5446]: zone localhost/IN: loaded serial 2
Mar 28 18:03:42 meghana-VirtualBox named[5446]: all zones loaded
Mar 28 18:03:42 meghana-VirtualBox named[5446]: FIPS mode is disabled
Mar 28 18:03:42 meghana-VirtualBox systemd[1]: Started BIND Domain Name Server.
Mar 28 18:03:42 meghana-VirtualBox named[5446]: running
Mar 28 18:03:43 meghana-VirtualBox named[5446]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
```

This doesnt fix the issue where bind9 isnt working in the background as well
Using dig with TLS works in the foreground works in this case as well.

Resolution - The terminals were closed once and then opened again. Somehow the things are running normally now (How is a good question which we do not have the answer of - maybe an instability thing).

Error:
On observing with other websites there is the case where the server cannot be reached 1-2 times before getting an output. Or the servers aren't able to reach at all.

Resolution: Just waited for some time.
This could be attributed to poor internet connection and possible unreachability of servers.

```
meghana@meghana-VirtualBox:~$ dig -6 +tls geeksforgeeks.com
;; Connection to ::1#853(::1) for geeksforgeeks.com failed: timed out.
;; no servers could be reached


; <<>> DiG 9.19.22-1+ubuntu22.04.1+deb.sury.org+1-Ubuntu <<>> -6 +tls geeksforgeeks.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48720
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 83144cea3f1cfbc40100000066056d1fdc70097c1679b906 (good)
;; QUESTION SECTION:
;geeksforgeeks.com.             IN      A

;; ANSWER SECTION:
geeksforgeeks.com.      10472   IN      A       199.59.243.225

;; Query time: 859 msec
;; SERVER: ::1#853(::1) (TLS)
;; WHEN: Thu Mar 28 18:44:07 IST 2024
;; MSG SIZE  rcvd: 90
```

```
meghana@meghana-VirtualBox:~$ dig -6 +tls google.com
;; Connection to ::1#853(::1) for google.com failed: timed out.
;; no servers could be reached

;; Connection to ::1#853(::1) for google.com failed: timed out.
;; no servers could be reached


; <<>> DiG 9.19.22-1+ubuntu22.04.1+deb.sury.org+1-Ubuntu <<>> -6 +tls google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29533
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c30004e5572b23fd0100000066056be25d82a1303e86008e (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             300     IN      A       172.217.31.206

;; Query time: 635 msec
;; SERVER: ::1#853(::1) (TLS)
;; WHEN: Thu Mar 28 18:38:50 IST 2024
;; MSG SIZE  rcvd: 83
```