Discover how to implement DNS-over-TLS in a Linux environment

DNS-over-TLS (DoT) is a security protocol that encrypts DNS traffic between clients and resolvers. It ensures the confidentiality and integrity of DNS queries and responses, protecting against eavesdropping and tampering. While DNS-over-TLS is not natively supported in all Linux distributions, there are alternative methods to implement it.

One popular option is to use Stubby, a DNS privacy application that acts as a local DNS stub resolver. Stubby supports DNS-over-TLS and can be easily configured to forward DNS queries to a DNS-over-TLS capable resolver.

To implement DNS-over-TLS using Stubby in a Linux environment, follow these steps:

1. Install Stubby:

   ```
   sudo apt-get install stubby
   ```

2. Configure Stubby: Edit the Stubby configuration file /etc/stubby/stubby.yml using a text editor. Uncomment the following lines and modify them as needed:

   ```
   resolution_type: GETDNS_RESOLUTION_STUB
   dns_transport_list:
    - GETDNS_TRANSPORT_TLS
   tls_authentication: GETDNS_AUTHENTICATION_REQUIRED
   tls_query_padding_blocksize: 128
   upstream_recursive_servers:
    - address_data: 1.1.1.1
      tls_auth_name: "cloudflare-dns.com"
    - address_data: 9.9.9.9
      tls_auth_name: "dns.quad9.net"
   ```

3. Restart Stubby:

   ```
   sudo systemctl restart stubby
   ```

4. Configure the system to use Stubby as the DNS resolver: Edit the /etc/resolv.conf file and set the DNS server to 127.0.0.1:

   ```
   nameserver 127.0.0.1
   ```

   Note: Some Linux distributions dynamically generate the /etc/resolv.conf file. In such cases, you may need to modify the network configuration files to set the DNS server to 127.0.0.1.

5. Test DNS-over-TLS: Use the dig command to perform a DNS query and verify that it is using DNS-over-TLS:

   ```
   dig example.com
   ```

   Look for the flags section in the output. If you see flags: qr rd ra ad, it indicates that DNS-over-TLS is working.