|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Pratik Pujari** | | |
| **UID no.** | **2020300054** | **Class:** | **Comps C Batch** |
| **Experiment No.** | 7 | | |

|  |  |
| --- | --- |
| **AIM:** | To configure a DNS server using the bind9 package |
| **THEORY:** | **What is a DNS server?**  The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as ‘google.com’ or ‘nytimes.com’ into web browsers, DNS is responsible for finding the correct IP address for those sites. Browsers then use those addresses to communicate with origin servers or CDN edge servers to access website information. This all happens thanks to DNS servers: machines dedicated to answering DNS queries.  **How Does a DNS Work?**  The DNS is responsible for converting the hostname, what we commonly refer to as the website or web page name, to the IP address. The act of entering the domain name is referred to as a DNS query and the process of finding the corresponding IP address is known as DNS resolution.  DNS queries can be of three types: recursive query, iterative query or non-recursive query.   1. Recursive query – These are queries where a DNS server has to respond with the requested resource record. If a record cannot be found, the DNS client has to be shown an error message. 2. Iterative query – These are queries for which the DNS client will continue to request a response from multiple DNS servers until the best response is found, or an error or timeout occurs. If the DNS server is unable to find a match for the query, it will refer to a DNS server authoritative for a lower level of the domain namespace. This referral address is then queried by the DNS client and this process continues with additional DNS servers. 3. Non-recursive query – these are queries which are resolved by a DNS resolver when the requested resource is available, either due to the server being authoritative or because the resource is already stored in cache.   DNS Lookup  **Primary and Secondary DNS Servers**  In most cases, a primary and a secondary DNS server are configured on your router or computer when you connect to your internet service provider. There are two DNS servers in case one of them happens to fail, in which case the second is used to resolve hostnames you enter.  **Protecting Yourself From DNS Attacks**  There are two things you should do to avoid becoming a victim of a DNS settings attack. The first is to install antivirus software so that malicious programs are caught before they can do any damage.  The second is to pay close attention to the appearance of important websites you visit regularly. If you visit one and the site looks off in some way—maybe the images are all different or the site's colors have changed, or menus don't look right, or you find misspellings (hackers can be dreadful spellers)—or you get an "invalid certificate" message in your browser, it might be a sign that you're on a faked website.  **DNS Caching**  DNS caching is the process of storing DNS data on the DNS records closer to a requesting client to be able to resolve the DNS query earlier. This avoids the problem of additional queries further down the chain and improves web page load times and reduces bandwidth consumption.  The amount of time that the DNS records are stored in DNS cache is called time to live or TTL.  What Is DNS Cache and How to Flush It - KeyCDN Support |
| **DNS Server** | |
| **CALCULATION:** |  |
| **SIMULATION:** |  |
| **OUTPUT TABLE:** |  |
| **CONCLUSION:** | |