For the DARPA Internet, the DNS offers the name service. On the internet, it is a widely utilized technique. A hosts.txt file, which included host names and addresses, was previously maintained by SRI. The key issue was that as the days went by, the file became larger and its dissemination became more expensive. The best answer for this issue was a distributed naming system. This solution was predicated on the premise that it would have the same contents as host.txt, be maintained in a distributed fashion, and work well. For distributed name servers, the hierarchical name scheme seems to be the best option. The name servers and resolvers are the two parts of the DNS. Typically, name servers are informational databases that respond with the knowledge they have. The name server with the necessary information is located using the resolver. Most frequently, centralizing the resolver is advantageous. The DNS offers two methods—zones and caching—for delivering results from the source to the desired destination. Zones are comprehensive databases that are managed for certain businesses. Caching is a technique whereby we save data locally to respond to similar inquiries in the future without having to repeat the full procedure as the complete response is already cached and can be accessed much more quickly. Although hosts.txt is still in use, a recent analysis revealed that only about 5000 hosts were accessible, whereas utilizing DNS made at least 20,000 hosts accessible.

Most hosts and subdomains fall under one of the six top-level domains, such as edu, com, etc. One resolver can look below domains thanks to the DNS basic algorithm. Most resolvers are designed to be able to connect to the root node because, once there, they can access any domain and, if partitioned, all local domain namespaces. The revolver will reach the root much more quickly after it begins caching the data, but if it notices something that isn't in the cache, it will still visit the root. Instead of traveling to the top, the caching allows for a straight leap near the solution by not only storing the ultimate solution but also the intermediate steps. Even if the root has redundancy, if caching is not used, it will get overloaded with requests. This strategy also enables us to lessen the traffic that the root encounters. DNS deployment uncovered several issues that weren't very shocking. In the worst circumstances, when there was a lot of traffic, it was shown to take between 30 and 60 seconds. Another issue was observed to be negative caching. When compared to using TCP, using datagrams is a far superior alternative; yet, this was required due to the poor network speed. In addition to retrieving the response, it also collected some additional data, often a preview of the user's next question. Given the poor performance, the caching policy performs better, but it only has a few problems, such as failing to keep the same TTL for identical RRS, which is done by system administrators. Security is an issue since resolvers will cache the data, allowing attackers to send out false information that may be stored and spread, leading to numerous mistakes. Because of temporary failures and other name systems that must be integrated into the operating system, changing systems to utilize DNS is not an easy process. It is difficult and highly skilled labor to maintain a distributed database.