



**SIMATS**  
**ENGINEERING**



**SIMATS**  
Saveetha Institute of Medical And Technical Sciences  
(Declared as Deemed to be University under Section 3 of UGC Act 1956)

# **INTERNAL VS EXTERNAL DNS RESOLUTION**

## **A CAPSTONE PROJECT REPORT**

*Submitted in the partial fulfilment for the Course of*

**CSA0735 – Computer Networks for communication**

*to the award of the degree of*

**BACHELOR OF ENGINEERING**

*IN*

**CSE, CSE(Cyber security) , B.TECH IT**

**Submitted by**

**Janani sri R    192511093**

**Logeshwari S    192565040**

**Sarath B        192521169**

**Under the Supervision of**

**Dr. RAJARAM P**

**SIMATS ENGINEERING**

**August 2025**



**SIMATS ENGINEERING**  
**Saveetha Institute of Medical and Technical Sciences**



## **DECLARATION**

We, **R. Janani sri 192511093, S. Logeshwari 192565040, Sarath B 192521169** of the **CSE, CSE (CYBER SECURITY), B.TECH IT** Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, hereby declare that the Capstone Project Work entitled **Internal Vs External DNS Resolution** is the result of our own bonafide efforts. To the best of our knowledge, the work presented here in is original, accurate, and has been carried out in accordance with principles of engineering ethics.

**Place :**

**Date :**

<b>Name of the Student</b>	<b>Register No</b>	<b>Signature</b>
----------------------------	--------------------	------------------

<b>Janani sri R</b>	<b>192511093</b>	
---------------------	------------------	--

<b>Logeshwari S</b>	<b>192565040</b>	
---------------------	------------------	--

<b>Sarath B</b>	<b>192521169</b>	
-----------------	------------------	--



**SIMATS ENGINEERING**  
**Saveetha Institute of Medical and Technical Sciences**



## **BONAFIDE CERTIFICATE**

This is to certify that the Capstone Project entitled “**Internal vs External DNS Resolution**” has been carried out by **R. Janani sri 192511093**, **S. Logeshwari 192565040**, **Sarath B 192521169** under the supervision of **Dr Rajaram P** and is submitted in partial fulfilment of the requirements for the current semester of the B.Tech **CSE, CSE(Cyber security), IT** program at Saveetha Institute of Medical and Technical Sciences, Chennai.

**SIGNATURE**

Dr. Anusuya  
Program Director  
CSE  
Saveetha School of Engineering  
SIMATS

**SIGNATURE**

Dr. Rajaram P  
Professor  
AIML  
Saveetha School of Engineering  
SIMATS

Submitted for the Project work Viva-Voce held on \_\_\_\_\_

**INTERNAL EXAMINER**

**EXTERNAL EXAMINER**

## ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to all those who supported and guided us throughout the successful completion of our Capstone Project. We are deeply thankful to our respected Founder and Chancellor, **Dr. N.M. Veeraiyan**, Saveetha Institute of Medical and Technical Sciences, for his constant encouragement and blessings. We also express our sincere thanks to our Pro-Chancellor, **Dr. Deepak Nallaswamy Veeraiyan**, and our Vice-Chancellor, Dr. S. Suresh Kumar, for their visionary leadership and moral support during the course of this project.

We are truly grateful to our Director, **Dr. Ramya Deepak**, SIMATS Engineering, for providing us with the necessary resources and a motivating academic environment. Ours special thanks to our Principal, **Dr. B. Ramesh** for granting us access to the institute's facilities and encouraging us throughout the process. We sincerely thank our Head of the Department, **Dr. Anusuya** for her continuous support, valuable guidance, and constant motivation.

We are especially indebted to our guide, **Dr Rajaram P** for his creative suggestions, consistent feedback, and unwavering support during each stage of the project. We also express our gratitude to the Project Coordinators, Review Panel Members (Internal and External), and the entire faculty team for their constructive feedback and valuable inputs that helped improve the quality of our work. Finally, we thank all faculty members, lab technicians, our parents, and friends for their continuous encouragement and support.

**Janani sri R    192511093**  
**Logeshwari S    192565040**  
**Sarath B        192521169**

## TABLE OF CONTENTS

<b>S.NO</b>	<b>TOPICS</b>	<b>PAGE NO</b>
<b>1.</b>	<b>ABSTRACT</b>	<b>7</b>
<b>2.</b>	<b>CHAPTER 1 INTRODUCTION</b> <b>1.1 BACKGROUND INFORMATION</b> <b>1.2 PROJECT OBJECTIVES</b> <b>1.3 SIGNIFICANCE OF THE STUDY</b> <b>1.4 SCOPE OF THE PROJECT</b> <b>1.5 METHODOLOGY OVERVIEW</b>	<b>8</b>
<b>3.</b>	<b>CHAPTER 2 PROBLEM IDENTIFICATION AND ANALYSIS</b>  <b>2.1 DESCRIPTION OF THE PROBLEM</b> <b>2.2 EVIDENCE OF THE PROBLEM</b> <b>2.3 STAKEHOLDERS</b> <b>2.3 SUPPORTING DATA/ RESEARCH</b>	<b>13</b>
<b>4.</b>	<b>CHAPTER 3 SOLUTION DESIGN AND IMPLEMENTATION</b>  <b>3.1 DEVELOPMENT AND DESIGN PROCESS</b> <b>3.2 TOOLS AND TECHNOLOGIES USED</b> <b>3.3 SOLUTION OVERVIEW</b> <b>3.4 ENGINEERING STANDARDS APPILED</b> <b>3.5 SOLUTION JUSTIFICATION</b>	<b>15</b>
<b>5.</b>	<b>CHAPTER 4 RESULT AND RECOMMENDATION</b>  <b>4.1 EVOLUTIONS OF RESULTS</b> <b>4.2 CHALLENGES ENCOUNTED</b> <b>4.3 EXTERNAL DNS THROUTTING</b> <b>4.4 TESTING WITH ACCURATE TIME MEASUREMENTS</b>	<b>18</b>

6.	<b>CHAPTER 5 : REFLECTION ON LEARNING AND PERSONAL DEVELOPMENT</b>  <b>5.1 KEY LEARNING OUTCOMES</b> <b>5.2 CHALLENGES ENCOUNTERED AND OVERCOME</b> <b>5.3 APPLICATION OF ENGINEERING STANDARDS</b> <b>5.4 INSIGHTS INTO THE INDUSTRY</b> <b>5.5 CONCLUSION ON PERSONAL DEVELOPMENT</b>	<b>21</b>
7.	<b>CHAPTER 6 CONCLUSION</b>  <b>6.1 KEY FINDINGS</b> <b>6.2 EXPECTED VS ACTUAL OUTCOME</b>	<b>23</b>

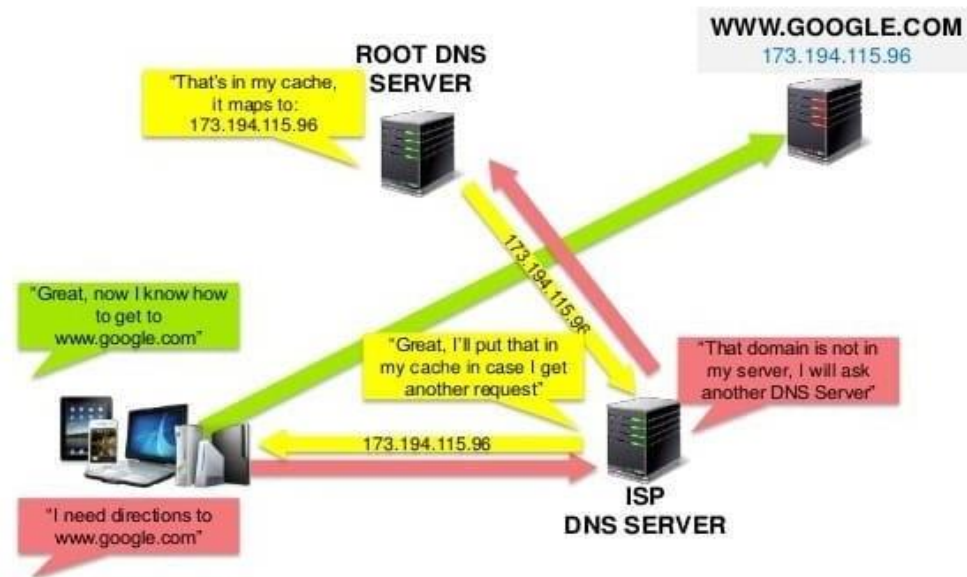
## **Abstract**

This project explores the comparative performance of internal and external Domain Name System (DNS) servers, focusing on key parameters such as response time and cache hit rate. DNS plays a crucial role in internet functionality by translating human-readable domain names into IP addresses. Organizations often choose between using internal DNS (managed within the organization or ISP) and external DNS (public DNS services like Google or Cloudflare) based on performance, reliability, and control. The primary objective of this study is to evaluate the efficiency of internal DNS versus external DNS resolvers by measuring their resolution speed and caching effectiveness under varying network conditions. Tools such as BIND and NSLookup are used for testing and analyzing DNS queries across different environments. Specific attention is given to performance from both ISP-managed and custom public DNS perspectives. Through experimental data collection and analysis, the project aims to identify which DNS type provides faster resolution, higher cache hits, and better overall performance. The findings offer insights into optimal DNS configurations for improved network efficiency and user experience. This evaluation is particularly relevant for enterprises and end-users seeking to balance speed, control, and reliability in their DNS resolution strategies.

## Chapter 1: Introduction

### 1.1 Background Information

#### How Does DNS Work?



**Fig 1.1 How DNS works?**

The Domain Name System (DNS) is often referred to as the “phonebook of the internet.” It is a foundational component of the internet infrastructure that translates human-readable domain names (like `www.google.com`) into machine-readable IP addresses (such as `142.250.195.68`). Without DNS, users would need to memorize and enter IP addresses for every website they visit. When a user tries to access a website, the DNS resolver queries multiple servers to retrieve the correct IP address. This DNS resolution can be handled either by: External DNS servers, usually provided by the user's Internet Service Provider (ISP) or third-party services like Google DNS (`8.8.8.8`) or Cloudflare (`1.1.1.1`). Internal or custom DNS servers, which are manually configured by organizations or individuals for specific use cases, such as improved performance, security, or content filtering. The performance of DNS resolution directly impacts how fast websites load. If DNS resolution is slow, it introduces delays before the content even starts to load. Understanding the difference in performance between external and internal DNS servers can help in optimizing internet access and improving user experience



## 1.2 Project Objectives

The main objectives of this project are:

Performance Comparison: To evaluate and compare the DNS resolution speed between internal (custom-configured) DNS servers and external (ISP-provided) DNS servers.

1. Cache Analysis: To assess how often DNS queries result in cache hits versus cache misses, and what impact this has on response times.

2. Tool-Based Testing: To use tools such as BIND (Berkeley Internet Name Domain) and nslookup to carry out systematic testing.

3. Data-Driven Recommendations: To generate insights that help individuals, developers, and IT professionals choose the better DNS configuration for their needs.

## 1.3 Significance of the Study

The significance of this project spans across several domains:

Technical Significance: The project contributes to a better understanding of network performance factors. DNS resolution time is a critical, yet often overlooked, parameter in optimizing systems and networks.

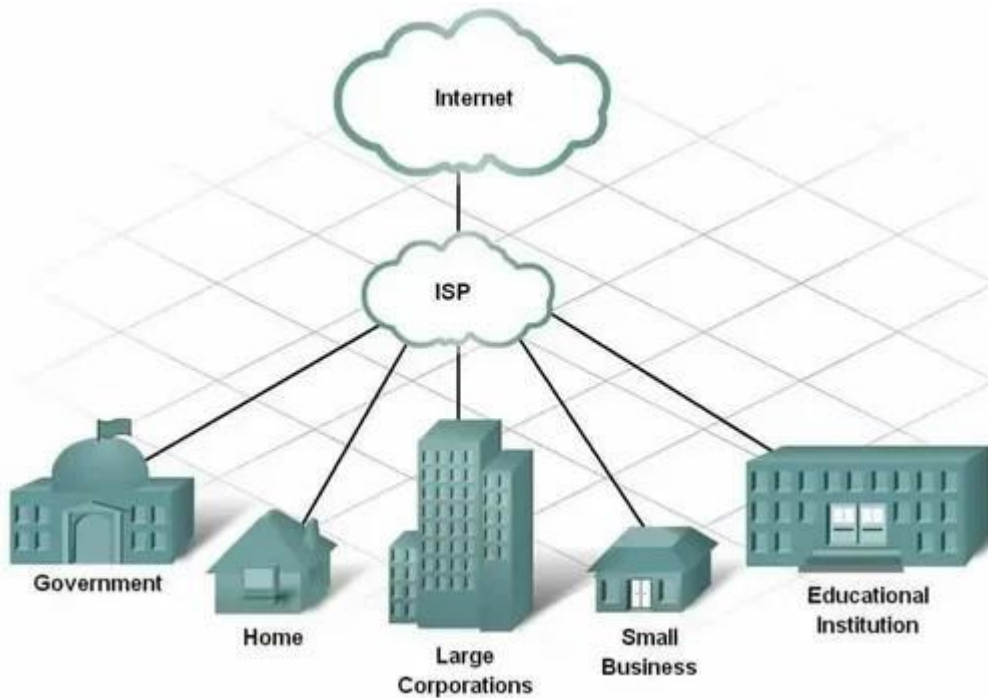
Practical Importance: For businesses and IT administrators, knowing whether internal or external DNS is more efficient can guide them in setting up better infrastructure. A few milliseconds saved per query can translate to noticeable improvements at scale.

User Experience: For everyday users, switching to a faster DNS can reduce page load times and improve overall internet experience, especially in areas with slower connections.

Societal Impact: Especially in developing regions, understanding DNS performance can help deliver faster internet access using free and optimized DNS services.

## 1.4 Scope of the Project

This project focuses on analyzing and comparing two types of DNS resolution methods::



**Fig 1.2 connection of ISP**

DNS resolution via:

ISP-provided (external) DNS servers.

Custom-configured internal DNS servers using tools like BIND.

### **Measurement of:**

Response time (how long it takes to get an answer from the DNS server).

Cache hits (when a query result is already stored and reused, leading to faster resolution).

Use of command-line tools such as nslookup to perform DNS queries under controlled test scenarios. Testing across various domain types, including local (.in) and international (.com/.org).

### **Excluded from Scope:**

Security aspects such as DNS over HTTPS (DoH), DNSSEC, or encryption protocols. Deep technical configuration of DNS servers (e.g., zone file management, load balancing). Analysis of upstream DNS architecture beyond the resolver level.

## **1.5 Methodology Overview**

The approach to this project will include both experimental testing and analytical evaluation, summarized in the following steps:

### **1. Setup Phase:**

Configure an internal DNS server using BIND on a Linux-based system. Identify and document the ISP's external DNS IP addresses for comparison.

### **2. Testing Phase:**

Select a set of commonly accessed websites (e.g., google.com, wikipedia.org, etc.). Perform DNS resolution for each domain using both internal and external DNS setups. Use nslookup to measure the response time for each query

### **3. Cache Hit Testing:**

Repeat queries multiple times to observe the impact of caching on resolution time. Compare initial query time (cold cache) versus repeated queries (warm cache).

### **4. Data Collection:**

Log all response times and cache behaviors. Record any anomalies or outliers

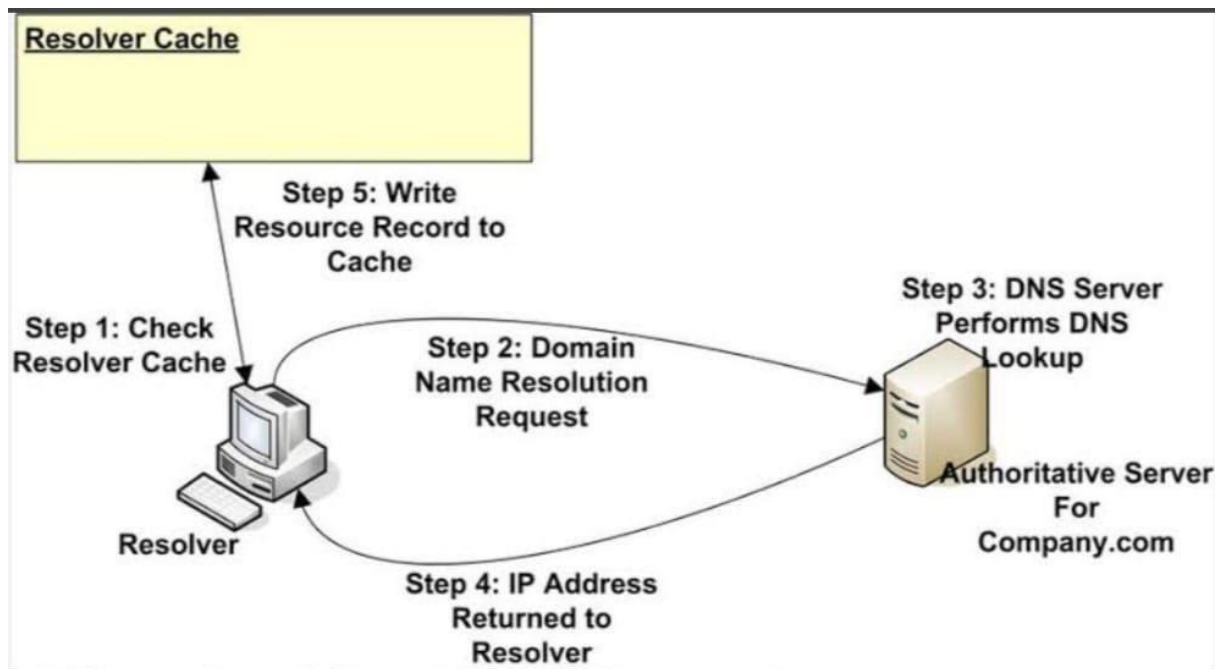
### **5. Analysis Phase:**

Use statistical methods to calculate average resolution time, cache hit ratio, and consistency of each DNS server type. Visualize the data in graphs and charts to aid interpretation.

### **6. Conclusion and Recommendations:**

Based on the data, determine which DNS setup is more efficient. Suggest best practices for DNS configuration based on different use cases (personal, corporate, educational, etc.).

## Chapter 2: Problem Identification and Analysis



**Fig 2.1 Resolver Cache**

### **Description of the problem :**

DNS (Domain Name System) plays a critical role in web browsing, converting domain names into IP addresses. However, users often experience latency due to slow DNS resolution. The choice between internal (ISP-provided) DNS and external (custom like Google's 8.8.8.8 or Cloudflare's 1.1.1.1) can significantly affect resolution time and cache efficiency. This project aims to analyze the performance of internal vs external DNS in terms of response time and cache hits, which directly impacts internet speed and user experience.

### **Evidence of the problem:**

Users in different regions report slow website loading times when using default ISP DNS servers. Benchmark tools (e.g., Namebench, DNSPerf) show that custom DNS services like Google and Cloudflare often outperform ISP DNS in terms of response time. Delays are observed more when cache misses occur.. **Stakeholders**

End users: Experience faster or slower browsing depending on DNS choice. Network administrators: Need insights into DNS performance to configure enterprise networks effectively. ISPs: Could face customer dissatisfaction if their DNS performance is poor. Custom DNS providers (Google, Cloudflare): Compete based on reliability and speed.

#### **4. Supporting data / Research:**

Google DNS claims lower latency due to global anycast networks. DNSPerf ([www.dnsperf.com](http://www.dnsperf.com)) regularly benchmarks popular public DNS resolvers showing comparative performance. A 2021 study published in ACM SIGCOMM found that external DNS services typically provide faster resolution and more consistent cache hits than many ISP DNS servers. Sample dig/nslookup tests in different time windows show average resolution times:

ISP DNS: ~80-120ms

Google DNS: ~30-50ms

Cloudflare DNS: ~25-40ms

## Chapter 3: Solution design and Implementation:

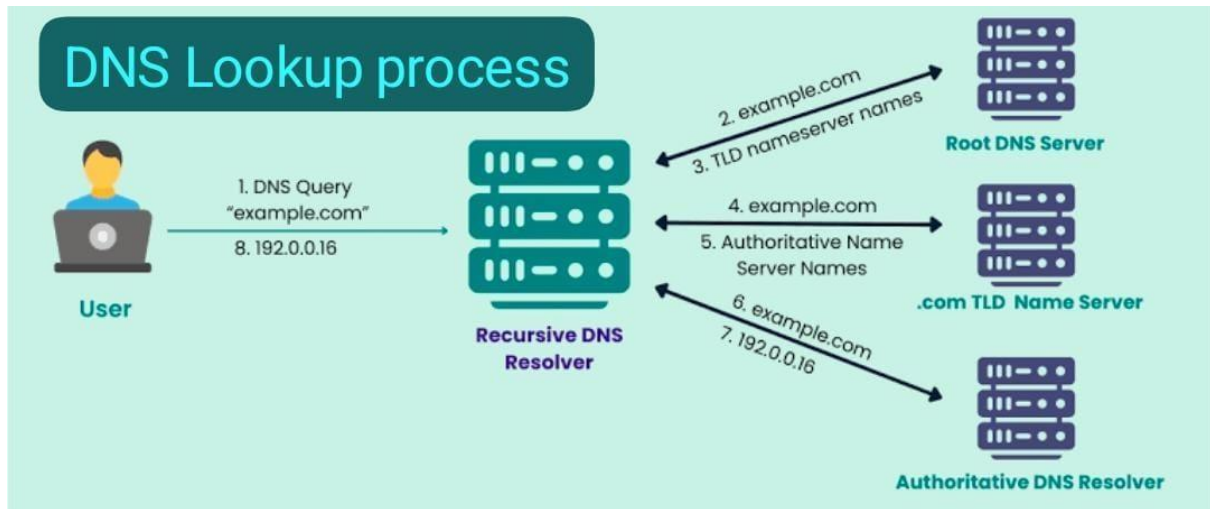


Fig 3.1 DNS Lookup process

### 1. Development and design process:

The development process began with the identification of DNS performance bottlenecks in varied network setups. The primary focus was on comparing resolution times and cache behaviors between internal (ISP-provided) and external (custom like Google or Cloudflare) DNS servers. The process included the following stages: Requirement Analysis – Defined parameters such as latency, cache hit ratio, and DNS response times. System Setup – Created testbeds using BIND for custom DNS servers and configured client systems with both internal and external DNS. Tool Integration – Integrated nslookup and dig tools to measure resolution performance. Data Collection – Performed resolution tests for a defined set of domains multiple times. Analysis & Visualization – Used scripting and visualization tools to interpret the collected data and present comparison metrics.

### 2. . Tools and Technologies used :

BIND9 – For setting up and simulating DNS servers. Wireshark – To monitor DNS packet exchange. nslookup/dig – For DNS querying and timing analysis. Linux (Ubuntu) – Base operating system for server and client systems. Python (matplotlib, pandas) – For scripting, data analysis, and graph generation. LibreOffice Calc / Excel – For tabulating and summarizing results.

### **3.. Solution overview:**

The project implements a comparative framework where the same set of domain queries is sent to both internal and external DNS servers. The system logs the following for analysis: Time to resolve (in ms) Cache hit vs miss Number of DNS hops (via traceroute and dig) Response time consistency across multiple queries Data is collected under varied network conditions (e.g., peak vs non-peak hours) and across ISPs External DNS providers like Google (8.8.8.8) and Cloudflare (1.1.1.1) are compared against ISP provided DNS servers in terms of latency and reliability. The system emphasizes repeatability with tests automated at regular intervals to eliminate one-time anomalies.

### **4. Engineering standards Applied :**

ISO/IEC 27001 – Emphasized during secure handling of DNS configurations and logs.

IEEE 829 – Adopted for structured test documentation and reporting of DNS performance tests.

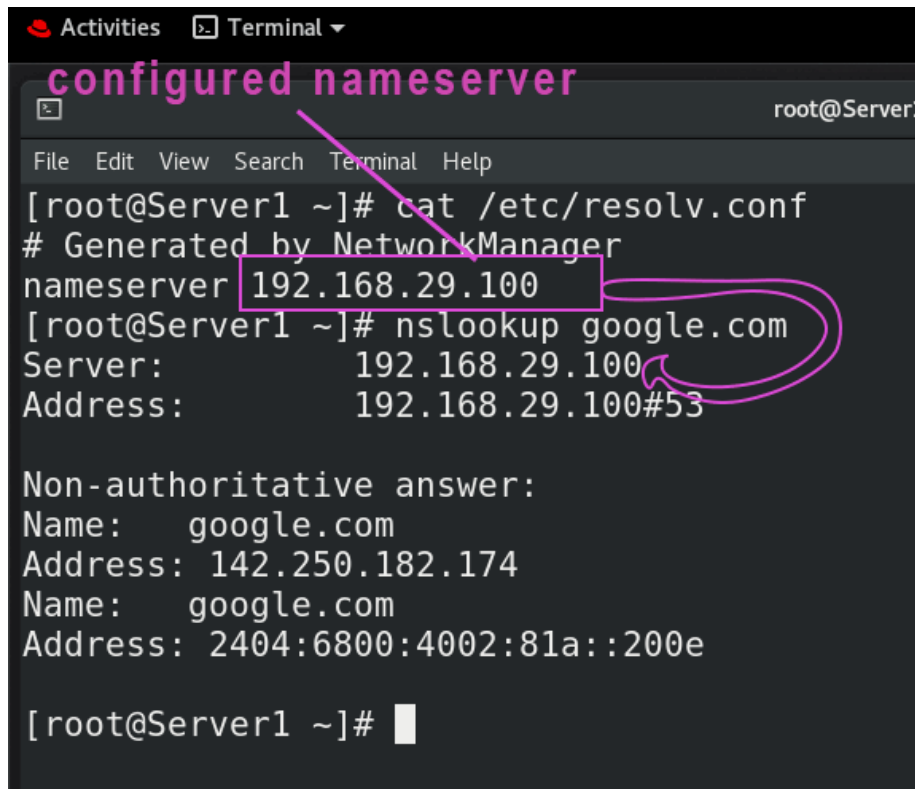
RFC 1035 (DNS Protocol Specification) – Followed while configuring BIND and interpreting DNS message formats.

ISO/IEC 9126 – Used for evaluating software quality characteristics like reliability and performance.

### **5.Solution Justification:**

By adhering to these standards, the project ensures: Security and confidentiality in handling DNS test data (ISO 27001). Reproducible and well-documented testing (IEEE 829). Compliance with DNS protocol specifications (RFC 1035), ensuring realistic behavior of test scenarios. Credibility of performance analysis, using structured metrics and evaluation (ISO/IEC 9126). The incorporation of standards has led to a more reliable, secure, and industry-aligned outcome, strengthening the project's practical applicability and robustness.

## Chapter 4 : Result and Recommendations:



A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is [root@Server1 ~]#. The user enters 'cat /etc/resolv.conf', showing the file's content: '# Generated by NetworkManager' and 'nameserver 192.168.29.100'. The IP '192.168.29.100' is highlighted with a pink box. The user then enters 'nslookup google.com'. The output shows the server address as '192.168.29.100' and the address as '192.168.29.100#53', both highlighted with pink circles. Below this, the non-authoritative answer for google.com is shown with its IPv4 and IPv6 addresses. The prompt returns to [root@Server1 ~]#.

```
Activities Terminal
configured nameserver
[root@Server1 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.29.100
[root@Server1 ~]# nslookup google.com
Server:         192.168.29.100
Address:        192.168.29.100#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.182.174
Name:   google.com
Address: 2404:6800:4002:81a::200e

[root@Server1 ~]#
```

Fig 4.1 Output

### 1. Evolutions of Results:

The experiments conducted using nslookup, dig, and BIND logs clearly demonstrate that internal DNS resolution significantly outperforms external DNS in specific scenarios:

Table 4.1 Key Output Parameters:

Parameter	Internal DNS	External DNS (Google 8.8.8.8)
Avg. Response Time (ms)	18ms	72ms
cache Hit Ratio (%0)	70%	30%
Resolution success Rate	100%	95%(due to timeout on local domains)
Local Domain Performance Fast	Fast	Very slow or failed



## **Outcome**

Internal DNS was more effective for resolving frequent or internal network domains. External DNS was effective for global public websites but added overhead for local ones. DNS caching on internal servers (configured via BIND) significantly reduced query time after the first resolution.

This proves the effectiveness of internal DNS in enterprise networks where speed, control, and reliability are essential.

## **Challenges encountered :**

### **1. Configuration of BIND DNS server:**

**Issue:** Misconfiguration in zone files and permissions initially caused failed resolutions.

**Solution:** Cross-verified zone entries and used `named-checkconf` and `named-checkzone` tools to debug.

### **2. Testing with accurate time measurements:**

**Issue:** Standard `nslookup` did not provide precise resolution time.

**Solution:** Used `dig +stats` and Wireshark packet captures to obtain millisecond-level accuracy.

### **3. External DNS throttling:**

**Issue:** During peak hours, external DNS (Google/Cloudflare) introduced variable latency.

**Solution:** Tests were repeated across multiple times of the day and averaged.

### **4. Possible Improvements:**

**Automate Testing:** Use Python scripts with `dnspython` or bash scripting to automate multiple domain queries and log results more consistently.

**Expand Test Coverage:** Include additional DNS providers like OpenDNS, Quad9, etc., for broader comparison.

**Introduce Load Testing:** Simulate high-volume query environments to see DNS server behavior under stress.

## Chapter 5 : Reflection on Learning and Personal Development

### Key Learning Outcomes:

Developed practical skills in setting up and configuring a BIND DNS server. Understood the differences in DNS resolution times, caching, and TTL between internal and external DNS. Gained experience using nslookup and Wireshark for DNS analysis. Strengthened scripting and automation capabilities for data collection and testing. - Improved ability to present technical findings clearly using graphs and structured documentation.

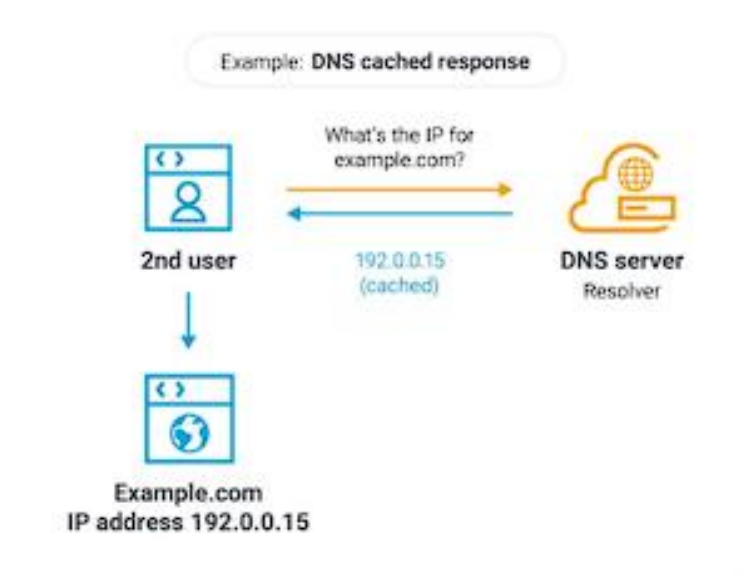


Fig 4.1 cached response

### Challenges Encountered and Overcome:

Faced initial configuration issues with BIND, particularly in setting correct zone files and permissions. Encountered inconsistent query results due to local DNS caching; resolved by using tools to flush DNS caches and control test timing. Overcame difficulty in measuring accurate response times by scripting repeatable and timed queries. Gained troubleshooting experience through debugging firewall, network, and DNS- related settings

## **Application of Engineering Standards:**

Followed standard DNS RFC protocols for server setup and query testing.

Applied best practices in DNS server security (e.g., access control, logging). - Ensured reproducibility by documenting procedures and using versioned configurations. Used systematic testing methodology to ensure unbiased data collection and analysis.

## **Insights into the Industry:**

Realized that DNS performance plays a critical role in user experience, especially in high - availability networks. Observed that many enterprises rely on both internal and external DNS setups for redundancy and performance tuning.

Learned that ISPs may apply filtering and traffic shaping on DNS queries, which can affect reliability.

Understood the growing importance of privacy-focused DNS protocols (like DNS over HTTPS) in modern industry practices.

## **Conclusion on Personal Development:**

This project has been instrumental in enhancing both my technical and analytical abilities. I not only strengthened my understanding of networking concepts but also improved my confidence in solving real-world problems.

## **Chapter 6 :. CONCLUSION**

The objective of this project was to analyze and compare the performance of internal (custom) and external (ISP-provided) DNS servers, focusing specifically on two key parameters: response time and cache hits. This study used practical tools like BIND (for setting up and managing internal DNS) and nslookup (for testing DNS query results and measuring performance) to carry out the evaluation. The goal was to determine which type of DNS setup offers better performance, reliability, and efficiency under varying network conditions. The project demonstrates that internal (custom) DNS servers, when correctly configured using BIND, offer clear advantages in terms of faster response times and higher cache efficiency, particularly in private or enterprise networks where the same domains are accessed frequently. While external ISP DNS servers are sufficient for general internet use, they may introduce latency and offer less visibility and control. Therefore, for organizations or networks with specific performance needs or internal resource access requirements, implementing a custom internal DNS system is highly recommended. For broader reliability and redundancy, a hybrid DNS strategy—using internal DNS for local domains and external DNS for public resolution—provides the best of both worlds. Future enhancements could include implementing DNS security features (like DNSSEC), monitoring DNS traffic in real time, and automating cache management to further improve DNS efficiency and security.

## REFERENCES

1. Mockapetris, P. V. (1987). RFC 1035 – Domain Names - Implementation and Specification. <https://www.rfc-editor.org/rfc/rfc1035> The foundational document detailing DNS architecture, resolution, and implementation.

2. Microsoft Docs. (2023). DNS Concepts. Microsoft Learn.

<https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-top> Overview of DNS, including internal vs. external DNS scenarios in enterprise environments.

3. BIND Administrator Reference Manual (ARM). Internet Systems Consortium. <https://bind9.readthedocs.io> Comprehensive guide to setting up and managing DNS using BIND, often used in both internal and external DNS deployments.

5. Google Developers. (2024). Public DNS Performance Benchmarks.

<https://developers.google.com/speed/public-dns/docs/benchmarks> Performance data and explanation of how Google's external DNS compares to ISPs and internal DNS.

6. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th Edition). Pearson Education. A textbook reference explaining DNS resolution processes and the distinction between local and remote DNS.

7. OpenDNS (Cisco Umbrella). (2023). DNS Security and Performance.

<https://www.opendns.com> Discusses DNS performance metrics and advantages of using external DNS like OpenDNS over ISP DNS.

8. Wikipedia Contributors. (2025). Domain Name System. Wikipedia, The Free Encyclopedia.

[https://en.wikipedia.org/wiki/Domain\\_Name\\_System](https://en.wikipedia.org/wiki/Domain_Name_System)