Group 8 Presentation

ICT 223
Linux OS and Network Management

GROUP MEMBERS

S/N	NAME	REGISTRATION NUMBER	SIGNATURE
1.	ENOSI MALONGO PHILIPO	T/DEG/2023/1457	
2.	EMILIANA S ELIA	T/DEG/2023/1489	
3.	MALONGO YOHANA MASALU	T/DEG/2023/1452	
4.	HANA MARTINI ISSAKI	T/DEG/2023/1393	
5.	WILBROAD A. GEJE	T/DEG/2023/1496	
6.	PALADIUS J JACOBO	T/DEG/2023/1475	
7.	HIPOLITI DANIEL PETER	T/DEG/2023/1374	

QUESTION

Title: Local DNS Query Tool

Description: Allows LAN users to query domain names and see results (IP address, TTL, etc).

Features:

- Input domain and optional DNS server
- Show A and MX records
- Query time logging

The goal is to show how a user within a Local Area Network (LAN) can query domain names and retrieve information like IP addresses and Time-to-Live (TTL). We'll use the nslookup and dig commands, which are standard tools for DNS lookups.

Domain Name System (DNS): A hierarchical system that translates human-readable domain names into IP addresses.

Local DNS Query Tool: as described. This sounds like a very useful utility for network administrators, developers, and even advanced home users within a Local Area Network (LAN).

How Do I Perform a DNS Lookup Using Command-Line Tools?

- To perform the DNS lookup using the command line, here is the process:
  - Open Terminal.
  - Enter dig domain.com to perform a DNS lookup for the domain.
- To specify a record type, use dig -t recordtype domain.com.

Features

Input Domain and Optional DNS Server

- This shows core functionality of querying a domain, and the ability to specify a custom DNS server.

Steps:

- ✓ Open your Command Prompt (Windows) or Terminal (macOS/Linux).
- ✓ Query a domain using the default DNS server (usually provided by your router/ISP):

Command: nslookup google.com

Expected Output: You'll see something similar to this (IP addresses and server names will vary):

Server: your.local.dns.server.ip

Address: your.local.dns.server.ip#53

Non-authoritative answer:

Name: google.com

Addresses: 2607:f8b0:4004:80c::200e

142.250.193.14

Explanation: This shows that nslookup used your default DNS server to resolve google.com to its IP addresses.

- Query a domain using a specific public DNS server (e.g., Google Public DNS 8.8.8.8):

  Command: nslookup google.com 8.8.8.8

Expected Output:

Server: dns.google

Address: 8.8.8.8#53

Non-authoritative answer:

Name: google.com

Addresses: 2607:f8b0:4004:802::200e

142.250.193.14

Explanation: This demonstrates the flexibility to use a different DNS server for the query, which is useful for testing or bypassing local DNS issues.

Show A and MX Records:

- This shows retrieving specific types of DNS records.

Steps:

- **Show A (Address) Records:** These map a domain name to an IPv4 address. You've already done this implicitly with the previous nslookup commands, but let's be explicit.
- **Command (using dig for clearer output including TTL):** dig A google.com
  - ✓ dig: The command-line tool used to query DNS name servers.
  - ✓ A: Specifies that you want the **A record**, which maps a domain name to an **IPv4 address**.
  - ✓ google.com: The domain name you want to look up.

Expected Output (look for the "ANSWER SECTION"):

; <<>> DiG 9.16.1-Ubuntu <<>> A google.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36622

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;google.com. IN A

;; ANSWER SECTION:

google.com. 300 IN A 142.250.193.14

google.com. 300 IN A 172.217.160.142

;; Query time: 1 msec

;; SERVER: 127.0.0.53#53(127.0.0.53)

;; WHEN: Tue Jun 24 10:11:45 2025

;; MSG SIZE rcvd: 71

Explanation: The "ANSWER SECTION" clearly shows google.com with its A records (IP addresses) and their associated TTL values (e.g., 300 seconds).

- **Show MX (Mail Exchanger) Records:** These specify the mail servers responsible for accepting email for a domain.

Command: dig MX google.com

- ✓ **MX Records** specify which mail servers handle email for the domain.
- ✓ Each **MX record** has a **priority number** (lower = higher priority).
- ✓ The **ADDITIONAL SECTION** may include the IP addresses of those mail servers.

Expected Output (look for the "ANSWER SECTION"):

; <<>> DiG 9.16.1-Ubuntu <<>> MX google.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37722

;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;google.com. IN MX

;; ANSWER SECTION:

google.com. 300 IN MX 50 alt4.aspmx.l.google.com.

google.com. 300 IN MX 10 aspmx.l.google.com.

google.com. 300 IN MX 20 alt1.aspmx.l.google.com.

google.com. 300 IN MX 30 alt2.aspmx.l.google.com.

google.com. 300 IN MX 40 alt3.aspmx.l.google.com.

;; Query time: 2 msec

;; SERVER: 127.0.0.53#53(127.0.0.53)

;; WHEN: Tue Jun 24 10:11:45 2025

;; MSG SIZE rcvd: 154

Explanation: The "ANSWER SECTION" lists the mail servers for google.com (e.g., aspmx.l.google.com) along with their priority (the numbers like 10, 20) and TTL.

Query Time Logging:

Both nslookup and dig inherently show the query time, which fulfills this requirement.

Steps:

- **Review previous outputs:** Look at the output from the dig commands.
- **Point out the "Query time" line:**

- **Example (from dig output):** ;; Query time: 1 msec
- **Explanation:** This line explicitly indicates how long the DNS query took to complete. This is crucial for troubleshooting network latency or slow DNS resolution.

Summary of Practical Demonstration:

- By running these simple command-line tools, you can effectively demonstrate the core features of a "Local DNS Query Tool":
- **Input domain and optional DNS server:** Shown by nslookup google.com and nslookup google.com 8.8.8.8.
- **Show A and MX records:** Clearly visible in the dig A google.com and dig MX google.com outputs.
- **Query time logging:** Present as the "Query time" line in the dig command outputs

REFERENCE

- Comer, D. E. (2018). Computer networks and internets (6th ed.). Pearson.
- Kerrisk, M. (2010). The Linux programming interface: A Linux and UNIX system programming handbook..
- GNU Project. (n.d.). The GNU C Library: Name Service Switch.Retrieved June 8, 2025.
- Mockapetris, P. (1987). Domain names - concepts and facilities (RFC 1034). Internet Engineering Task Force (IETF).

END OF PRESENTATION

THANKS!!!!