Windowns Networking Commands: nslookup

Connect with me: Youtube | LinkedIn | WhatsApp Channel | Web | Facebook | Twitter

- Download PDF
- To access the updated handouts, please click on the following link: https://yasirbhutta.github.io/windows/docs/nslookup.html

Here are practical tasks to help you learn and apply the nslookup command in Windows:

1. Perform a Simple DNS Lookup

Task: Use nslookup to find the IP address of a website (e.g., google.com).

Command:

```
nslookup google.com
```

Goal: Identify the IP address associated with the domain name.

In DNS queries, the term non-authoritative answer refers to a response that comes from a DNS server that is not the original source of the DNS data for the queried domain. Instead, this type of response is derived from cached data or information that the server has retrieved from other sources.

2. Find the Domain Name for an IP Address

Task: Use nslookup to perform a reverse DNS lookup (find the domain name associated with a given IP address).

Command:

```
nslookup <IP address>
```

Goal: Verify if the IP address resolves to a domain name and understand reverse DNS lookups.

3. Specify a Different DNS Server

Task: Query a domain name using a specific DNS server (e.g., Google DNS at 8.8.8.8).

Command:

```
nslookup example.com 8.8.8.8
```

```
nslookup example.com 1.1.1.1
```

Goal: Compare how different DNS servers resolve the same domain and check if using a specific server changes the result.

4. Find Mail Server Records (MX Records) for a Domain

Task: Look up the mail exchange (MX) records for a domain (e.g., gmail.com).

Command:

```
nslookup -type=mx gudgk.edu.pk
```

Goal: Identify the mail servers responsible for handling emails for that domain.

An **MX (Mail Exchange) record** is a type of DNS record used to specify the mail server responsible for receiving email on behalf of a domain. MX records direct email to the servers that handle a domain's email services, and they are an essential part of the DNS system for email delivery.

5. Find Name Server Records (NS Records) for a Domain

Task: Look up the name servers responsible for a domain (e.g., yahoo.com).

Command:

```
nslookup -type=ns gudgk.edu.pk
```

Goal: Identify the authoritative name servers for the domain.

Authoritative name servers are DNS servers that have the complete information for a particular domain. They store the original source of the DNS records (like A, MX, NS records) for that domain. They are responsible for responding to queries about the domain's configuration.

6. Find All DNS Records for a Domain

Task: Retrieve all available DNS records (A, MX, NS, etc.) for a domain.

Command:

```
nslookup -type=any example.com
```

Goal: See all DNS records related to a domain to understand its DNS configuration.

7. Change the Default DNS Server Temporarily

Task: Change the default DNS server for your queries (e.g., to Cloudflare DNS 1.1.1.1) and query a domain.

Command:

```
nslookup
server 1.1.1.1
google.com
```

Goal: Test DNS resolution with a different DNS server and compare the results with your default DNS server.

8. Troubleshoot DNS Resolution Issues

Task: Troubleshoot DNS resolution problems by performing multiple lookups for a domain (e.g., a website that fails to load).

Command:

```
nslookup google.com
nslookup google.com 8.8.8.8
nslookup google.com 1.1.1.1
```

Goal: Compare results from different DNS servers to check if the issue lies with your DNS server or network.

9. Check for DNS Propagation

Task: Query a recently updated domain using different DNS servers to check if the new DNS records have propagated.

Command:

```
nslookup newwebsite.com 8.8.8.8
nslookup newwebsite.com 1.1.1.1
```

Goal: Check if the updated DNS information has spread across the internet by querying multiple DNS servers.

10. Test Multiple DNS Queries in Interactive Mode

Task: Enter interactive mode in nslookup to perform multiple queries without re-entering the command.

Command:

```
nslookup
google.com
yahoo.com
example.com
exit
```

Goal: Practice querying multiple domains in a single session, making it easier to test various domains and servers.