Lab 1: HTTP/DNS

How to write the report: Each student may work individually or in a group of up to three members. If working in a group, all students must submit the same PDF file that includes all exercises and the names of every group member. You are have to run the provided examples and use them to illustrate the underlying concepts. For the exercises, analyze the observed behavior, describe your findings, include relevant images, and document the steps you followed to obtain your results.

EX 1: HTTP 1.0 vs HTTP 1.1

Telnet, short for TELecommunication NETwork, is a simple text-based protocol defined in RFC 854. It allows a user to open a TCP connection to a remote host. While it was historically used for remote shell logins, its main use today is for testing raw TCP services such as HTTP, SMTP, or POP3 by manually typing commands. To use Telnet, the command format is `telnet [host] [port]`. If no port is specified, it defaults to port 23. When sending an HTTP request, you typically need to press Enter twice to complete and send the request.

For example, Telnet can be used to test an HTTP connection by opening a session on port 80. After connecting, you can manually type an HTTP request. Using HTTP/1.0, the request would look like:

```
telnet example.com 80

GET / HTTP/1.0

Host: example.com
```

When using HTTP/1.1, the syntax is slightly different but follows the same principle:

```
telnet example.com 80

GET / HTTP/1.1

Host: example.com
```

Exercise: Use Telnet to test HTTP connections. First, with HTTP/1.0, connect to info.cern.ch and access the first webpage. Then, with both HTTP/1.0 and HTTP/1.1, connect to google.com and perform a search. Finally, connect to example.com and access the page located at /test.

Ex2: HTTP/2.0

Curl, short for Client for URL, is a command-line tool used to transfer data to or from a server using URLs. It supports many different protocols, including HTTP, HTTPS, FTP, SFTP, SMTP, and others. To use curl, the general format is `curl [version] [option] [URL]`.

For example, Curl can be used to test an HTTP connection by sending a request to a server. By using the -v option, you can see detailed information about the request and response, and with --http2, you can force the use of HTTP/2. To request the homepage of Google with verbose output over HTTP/2, the command would look like:

```
curl -v --http2 https://www.google.com/
```

Exercise: Using Curl, browse "www.cnam.fr" and "www.wikipedia.com" while requesting HTTP/2.0. Observe and describe the interaction between the client and the server.

Ex3: DNS

Nslookup, short for Name Server Lookup, is a command-line tool used to query the Domain Name System (DNS). It allows you to find the IP address associated with a domain name or, conversely, to find the domain name associated with an IP address. Nslookup can be used in a single-line query with the format `nslookup [options] [domain] [server]`, or in interactive mode simply by typing `nslookup`.

For example, Nslookup can be used to request all available DNS records for the domain repubblica.it. By specifying the record type, you can retrieve different kinds of information and the command would look like:

```
nslookup -type=ANY repubblica.it
```

Note: The `ANY` parameter is blocked by the majority of websites, so it is usually necessary to specify a specific type of DNS record, such as `A, MX, or CNAME`.

Exercises: First, find your public IP address and perform an nslookup. Then, compare the domains cnam.fr, lecnam.net, and roc.cnam.fr by using nslookup with record types A, MX, and NS. Finally, use nslookup to find the public IP address of www.louvre.fr and make an HTTP/2.0 request to https://louvre.fr/.