# Networking- M1 international

# Lab 1 : Web and DNS

**<u>You can work in groups of 1 or 2 students.</u>**
**<u>You must deliver a written report (preferably a pdf) to the mail address ravaioli@i3s.unice.fr no more than one hour after the end of the lab.</u>**

READ THE APPENDIX BEFORE STARTING THE LAB

## *PRELIMINARY : TYPICAL RTT IN AN IP NETWORK*

The objective of this first exercise is to figure out the typical distances in IP networks. Here is a set of domains in the Internet that are organized based on their geographical distance with respect to our local position (Sophia-Antipolis).

1. For each site, use nslookup (see appendix) to find one mail exchanger and one dns server for this domain. Report in a table their names/IPs
   a) Local domain: unice.fr
   b) European domain: aalto.fi
   c) US domains : bu.edu
   d) New-Zealand domain :waikato.ac.nz
2. Report the average RTT obtained using 5 pings ( -c option of ping - see the manpage of ping) towards the web server of each domain (obtained by adding www to the domain name).

## *WEB : WITH AND WITHOUT A WEB CLIENT*

### Case 1: http://iutsa.unice.fr/~urvoy/R1/index.html

1. In the above URL, which part corresponds to the server and which part corresponds to the path of the object on the server?
2. Connect using telnet on the server. Once the TCP channel is established, enter a GET command so as to retrieve the URL with non persistent HTTP connection. You must have a GET and a host line so that the server answers correctly.
3. Which part of the answer corresponds to the control information and which part corresponds to the data (the object).
4. What is the response status and what does it means?
5. Create a GET request that is syntactically correct but asks for a non available object. What is

the response status given by the server and what does it mean?

6. Create a syntactically correct GET request, asking for an existing object but replace the keyword GET by GIT. What is the response status given by the server and what does it mean? What are the types of requests supported by this server?
7. Do a correct request (correct syntax and an existing object) in HTTP/1.1 and add the following line to the header after the host option :

| Connection: Keep-Alive |
|---|

What are the changes in the returned HTTP header and in the TCP connection?

## Case 2: http://iutsa.unice.fr/~urvoy/R1/Part2/index.html

1. Set up a TCP connection and download, using telnet, the object for the new URL under study. Copy the data part of the answer into a file that you name Part2.html. Open the file in one tab of Firefox and open a second tab in which you open directly the URL. Compare the content of both tabs and the source code of the page (right click in the window to ask for the source code the current page). What are the differences in the source code and visual appearance?
2. Fix the problem so that the local content (first tab) is similar to the second tab. Describe the operations you did?
3. Prove that the server automated the operations you did manually using the Web Console of Firefox.

## *Uploading data to the server*

Using the Web console of firefox, compare the upload operations performed for the two following URLs : http://iutsa.unice.fr/~urvoy/R1/Part3/index.html, and http://iutsa.unice.fr/~urvoy/R1/Part3/index2.html.

Hint : empty the console once the page has been downloaded so as to see only the operation performed when you click on Send.

## *DNS*

## Simple queries

1. Open a terminal window and type nslookup www.unice.fr . What is the IP of the server that responded?
2. Let us now ask for a more verbose response:

   nslookup www.unice.fr -debug

   Explain the different parts of the response
3. Combine the *watch* (under Linux) and the *nslookup* www.google.fr *-debug* commands. If you have a Windows machine, just run the query many times. Which field varies and why?

### Authoritative vs. Non authoritative responses

1. Open a terminal window and type *nslookup www.google.fr*. Why is it that the answer be flagged as "non authoritative"?
2. We are now going to travel through the hierarchy of DNS servers starting from one of the root servers (list in appendix). You are only allowed to consider authoritative answers. You want to resolve [www.google.fr](www.google.fr). Use the Web site [http://legacy.zoneedit.com/lookup.html](http://legacy.zoneedit.com/lookup.html) to do so : ask for ANY record type. Detail the different steps, listing the number of DNS servers you crossed and the ones you queried.
3. If we apply the same procedure as above to the case of www.unice.fr, why is it that the first answer (returned by the root server) is similar ? Do the same with zzzzzzz.fr.

## ANALYSIS OF A TRACE FROM A WEB BROWSING SESSION

Open the trace http_espn.dmp with Wireshark. It records the loading of a single Web page.

1. What are the transport level protocols that you have observe in the trace. Use a **protocol hierarchy** function of the **statistics** menu.
2. How many conversations do you have at the IP, TCP and UDP in the trace? Use the **conversations** function of the **statistics** menu.
3. What does the Ethernet level information of the **conversations** function of the **statistics** menu indicates?
4. Let us now focus on DNS traffic. Create a filter to filter only DNS queries. To do this, position the cursor on the DNS flags in the lower window, then right click to create the filter using the **Prepare As filtered** and then the **Selected** option. How many such requests do you find?
5. Report the response time of the first two DNS request using the time column.
6. Let us consider HTTP requests. Use the **HTTP - Requests** option from the **Statistics** menu. Interpret the result and show that it is in line with the DNS requests that were performed by the client.
7. Analyze the first three HTTP packets (use an http filter) and explain what happened?

## *APPENDIX : TOOLS*

### Telnet

telnet : enables to establish a TCP channel with a remote machine on a specific port

Syntax: telnet machine port

Ex: telnet [www.google.fr](www.google.fr) 80

### Ns-lookup

nslookup enables to query the default dns resolver or any dns server (provided that dns service is not blocked by a firewall).

Usage : nslookup -type=XX  host  -debug

where XX ∈ {A,NS,MX,CNAME, ANY} and host is an IP address, a name of a machine or domain or an IP address.

**Note that on the first two lines, nslookup always report the id of the server. The answer to the query comes afterwords.**

## List of root servers :

| | |
|---|---|
| a.root-servers.net. | g.root-servers.net. |
| b.root-servers.net. | h.root-servers.net. |
| c.root-servers.net. | i.root-servers.net. |
| d.root-servers.net. | j.root-servers.net. |
| e.root-servers.net. | k.root-servers.net. |
| f.root-servers.net. | l.root-servers.net. |
| | m.root-servers.net. |

## Wireshark

Filter examples.Note that for a filter to be effectively apply, you must push the Apply button.

Examples

| Filter | Comments |
|---|---|
| http | All  HTTP traffic |
| ip.addr==134.59.136.5 | Traffic sent or received for the IP address 134.59.136.5 |
| http and ip.addr==134.59.136.5 | HTTP traffic sent or received for the IP address 134.59.136.5 |
| dns | All DNS requests/responses |