Title: Anatomy of a Web Connection: A Brief Analysis

Author: Diogo Cruz

Date: 18/03/2022

Index

Introductory Note:

The objectives of this assignment are the following:

- Identify the technologies, processes, actors and business models involved in a web connection.
- Identify some of possible social and economic implications associated with the identified technologies, processes, actors and business models.

To accomplish this, we will use the *Windows Command Prompt* and type "*tracert*" followed by a web address of a site of our choosing. We decided to use the website for the Tokyo University of Arts (www.geidai.ac.jp)

1. Summary / Abstract

The important role of this assignment is to study and comment on what happens during a web connection, explaining the steps along the way.

By analyzing the output of the *tracert* command, which returns the names or IP addresses of the routers that form a connection between us and the desired site, we will see the paths that are created between the connections until we reach it. From that we will be able to take conclusions about the paths that were created, the hops between the connections, what they represent, the operations involved, the technologies used, and the parties involved.

The goal is also, as mentioned above, to attempt to make the sequential identification of operations, processes, techniques and technologies involved in each and try to situate these processes, techniques and technologies in the framework of the ISO OSI model, as well as some of the possible social and economic implications.

2. Framework

The web wasn't always like this. Things have changed a lot since the beginning of web connections.

"In its early days it was a static network designed to shuttle a small freight of bytes or a short message between two terminals; it was a repository of information where content was published and maintained only by expert coders. Today, however, immense quantities of information are uploaded and downloaded, […] now we are all commentators, publishers, and creators.
In the 1980s and 1990s, the Internet widened in scope to encompass the IT capabilities of universities and research centers, and, later on, public entities, institutions, and private enterprises from around the world. The Internet underwent immense growth; it was no longer a state-controlled project, but the largest computer network in the world."
(Article from the book Change: 19 Key Essays on How the Internet Is Changing Our Lives)

It does, in fact, touch almost every aspect of how we live, work, socialize, shop, and play. We rely on it for most of our daily tasks, from simple ones to the more complex.

It's thanks to a collection of processes, techniques, actors and technologies involved that this is all possible. This is something not perceived by the "common user" as it is hidden behind an abstract layer to hide its real complexity. And in todays' world, more than ever before, they encompass significant social and economic implications.

3. Web Connection: Protocols/Mechanisms Involved

During an Internet connection we have essentially two main participants: **clients** and **servers**. In its' most basic form, the client sends requests to the server and if the server receives it, returns a response to the client.

Clients are the typical web user's internet-connected devices (*i.e.*, your computer connected to your Wi-Fi, or your phone connected to your mobile network). Servers are computers that store webpages, sites, or apps. When a client device wants to access a webpage, a copy of the webpage is downloaded from the server onto the client machine to be displayed in the user's web browser.

However, it is not as simple as it may seem, there are many other parts involved in a web connection. Components like the web browser, DNS, TCP/IP, HTTP, *etc.* are all vital parts to make a connection work and we will now explain them in greater detail.

3.1 Web Browser

The client (most likely) is using a device connected to the Internet and has a web browser where it can look up whatever the client wants. But what exactly is a web browser and how does it work?

A web browser is an application used to access and view websites on the WWW *(World Wide Web)*. Common web browsers include Microsoft Edge, Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

When a user makes a request to a web page, the web browser will send an HTTP *(Hypertext Transfer Protocol)* request message to the server, asking it to send a copy of the website to the user. This message, and all other data sent between the client and the server, is sent across your internet connection using TCP/IP *(Transmission Control Protocol/Internet Protocol)*

We will develop on these topics *(HTTP, TCP/IP)* later on.

3.2 DNS

The DNS *(Domain Name System)* is a naming system for computers, services, or other resources connected to the Internet and it works like an address book for websites. When you type a web address in your browser, the browser looks at the DNS to find the website's IP address before it can retrieve the website. The browser needs to find out which server the website lives on, so it can send HTTP messages to the right place.

3.3 TCP/IP

TCP *(Transmission Control Protocol)* and IP *(Internet Protocol)* are communication protocols that define how data should be broken into packets, addressed, transmitted, routed and received at the destination. It functions as an abstraction layer between internet applications and the routing and switching fabric

Common TCP/IP protocols include:

- **Hypertext Transfer Protocol (HTTP)** handles the communication between a web server and a web browser.
- **HTTP Secure** handles secure communication between a web server and a web browser.
- **File Transfer Protocol** handles transmission of files between computers.

In terms of architecture, TCP/IP can be divided in 4 layers, from the topmost layer (application) to the lowest (link):

- **Application layer** – applications and processes interact with software applications to implement a communicating component. This can be done on the same host, or on different ones
- **Transport layer** - performs host-to-host communications, determines how much data should be sent where and at what rate and helps ensuring that data units are delivered error-free and in sequence. These communications can be on the local network, as well as on remote networks
- **Internet layer** - provides a uniform networking interface, hiding the actual topology of the underlying network connections. Responsible for sending the packets from any network, and any computer still they reach the destination irrespective of the route they take
- **Link layer** - defines the networking methods in the local network link on which hosts communicate, this is done without routers.

3.4 Packets

Before we talked about packets to describe the format in which the data is sent from server to client. So, what exactly is it?

When data is sent across the web, it is sent in thousands of small chunks. There are multiple reasons why data is sent in small packets. They are sometimes dropped or corrupted, and it's easier to replace small chunks when this happens. Additionally, the packets can be routed along different paths, making the exchange faster and allowing many different users to download the same website at the same time. If each website was sent as a single big chunk, only one user could download it at a time, which obviously would make the web very inefficient and not much fun to use.

3.5 HTTP

Hypertext Transfer Protocol (HTTP) is an application-layer protocol for transmitting hypermedia documents, such as HTML *(Hyper Text Markup Language)*.

HTTP follows a classical client-server model, with a client opening a connection to make a request, then waiting until it receives a response. HTTP is a stateless protocol, meaning that the server does not keep any data (state) between two requests.

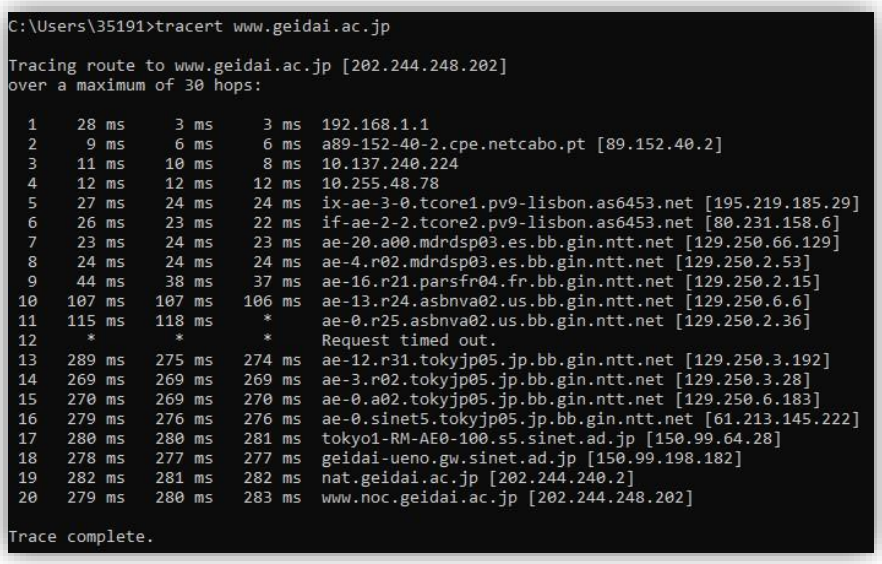
4. Traceroute *(tracert)* command

The traceroute command identifies the route a packet takes on an IP network between your computer and the destination web server. As a rule, we have truly little or no control on how a packet gets from point A to point B. What traceroute offers beyond the ping command is that it lists every hop along the path between the two computers. This can help you identify if communications are taking too many hops in the wrong direction or whether certain nodes are out of commission.

Normally traceroute uses ICMP (Internet Control Message Protocol) echo packets with a varying TTL (Time to Live). Usually, each hop is queried three times, for better and accurate results.

4.1 Executing the command

The command was executed on Windows: tracert www.geidai.ac.jp



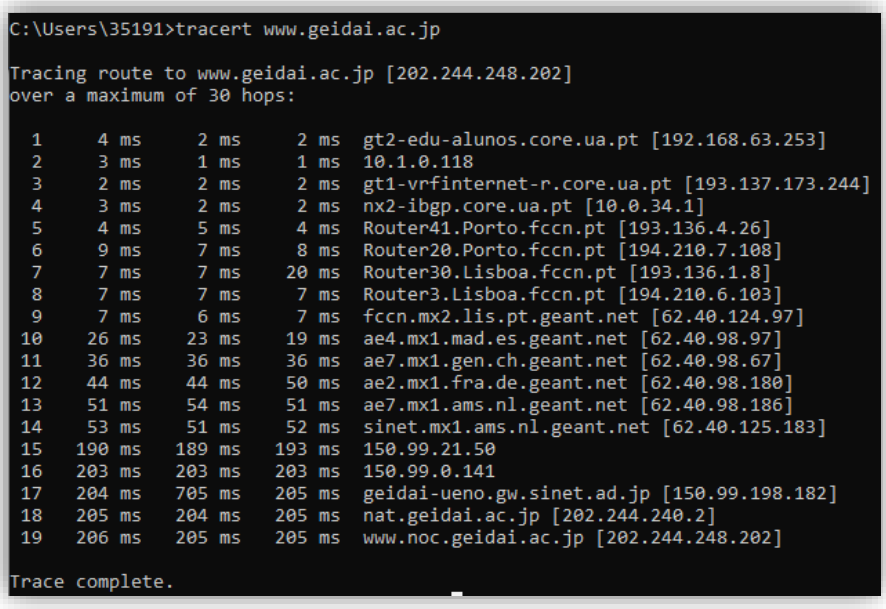
```
C:\Users\35191>tracert www.geidai.ac.jp

Tracing route to www.geidai.ac.jp [202.244.248.202]
over a maximum of 30 hops:

  1    28 ms     3 ms     3 ms  192.168.1.1
  2     9 ms     6 ms     6 ms  a89-152-40-2.cpe.netcabo.pt [89.152.40.2]
  3    11 ms    10 ms     8 ms  10.137.240.224
  4    12 ms    12 ms    12 ms  10.255.48.78
  5    27 ms    24 ms    24 ms  ix-ae-3-0.tcore1.pv9-lisbon.as6453.net [195.219.185.29]
  6    26 ms    23 ms    22 ms  if-ae-2-2.tcore2.pv9-lisbon.as6453.net [80.231.158.6]
  7    23 ms    24 ms    23 ms  ae-20.a00.mdrdsp03.es.bb.gin.ntt.net [129.250.66.129]
  8    24 ms    24 ms    24 ms  ae-4.r02.mdrdsp03.es.bb.gin.ntt.net [129.250.2.53]
  9    44 ms    38 ms    37 ms  ae-16.r21.parsfr04.fr.bb.gin.ntt.net [129.250.2.15]
 10   107 ms   107 ms   106 ms  ae-13.r24.asbnva02.us.bb.gin.ntt.net [129.250.6.6]
 11   115 ms   118 ms     *     ae-0.r25.asbnva02.us.bb.gin.ntt.net [129.250.2.36]
 12     *        *        *     Request timed out.
 13   289 ms   275 ms   274 ms  ae-12.r31.tokyjp05.jp.bb.gin.ntt.net [129.250.3.192]
 14   269 ms   269 ms   269 ms  ae-3.r02.tokyjp05.jp.bb.gin.ntt.net [129.250.3.28]
 15   270 ms   269 ms   270 ms  ae-0.a02.tokyjp05.jp.bb.gin.ntt.net [129.250.6.183]
 16   279 ms   276 ms   276 ms  ae-0.sinet5.tokyjp05.jp.bb.gin.ntt.net [61.213.145.222]
 17   280 ms   280 ms   281 ms  tokyo1-RM-AE0-100.s5.sinet.ad.jp [150.99.64.28]
 18   278 ms   277 ms   277 ms  geidai-ueno.gw.sinet.ad.jp [150.99.198.182]
 19   282 ms   281 ms   282 ms  nat.geidai.ac.jp [202.244.240.2]
 20   279 ms   280 ms   283 ms  www.noc.geidai.ac.jp [202.244.248.202]

Trace complete.
```

Fig 1: Output of the *tracert* command inside home network, at 16h28 20/03/2022



```
C:\Users\35191>tracert www.geidai.ac.jp

Tracing route to www.geidai.ac.jp [202.244.248.202]
over a maximum of 30 hops:

  1     4 ms     2 ms     2 ms  gt2-edu-alunos.core.ua.pt [192.168.63.253]
  2     3 ms     1 ms     1 ms  10.1.0.118
  3     2 ms     2 ms     2 ms  gt1-vrfinternet-r.core.ua.pt [193.137.173.244]
  4     3 ms     2 ms     2 ms  nx2-ibgp.core.ua.pt [10.0.34.1]
  5     4 ms     5 ms     4 ms  Router41.Porto.fccn.pt [193.136.4.26]
  6     9 ms     7 ms     8 ms  Router20.Porto.fccn.pt [194.210.7.108]
  7     7 ms     7 ms    20 ms  Router30.Lisboa.fccn.pt [193.136.1.8]
  8     7 ms     7 ms     7 ms  Router3.Lisboa.fccn.pt [194.210.6.103]
  9     7 ms     6 ms     7 ms  fccn.mx2.lis.pt.geant.net [62.40.124.97]
 10    26 ms    23 ms    19 ms  ae4.mx1.mad.es.geant.net [62.40.98.97]
 11    36 ms    36 ms    36 ms  ae7.mx1.gen.ch.geant.net [62.40.98.67]
 12    44 ms    44 ms    50 ms  ae2.mx1.fra.de.geant.net [62.40.98.180]
 13    51 ms    54 ms    51 ms  ae7.mx1.ams.nl.geant.net [62.40.98.186]
 14    53 ms    51 ms    52 ms  sinet.mx1.ams.nl.geant.net [62.40.125.183]
 15   190 ms   189 ms   193 ms  150.99.21.50
 16   203 ms   203 ms   203 ms  150.99.0.141
 17   204 ms   705 ms   205 ms  geidai-ueno.gw.sinet.ad.jp [150.99.198.182]
 18   205 ms   204 ms   205 ms  nat.geidai.ac.jp [202.244.240.2]
 19   206 ms   205 ms   205 ms  www.noc.geidai.ac.jp [202.244.248.202]

Trace complete.
```

Fig 2: Output of the *tracert* command in University of Aveiro, at 14h26 22/03/2022

What we are seeing here are all the hops between different IP addresses, each one is queried three times, called a ping. Ping messages are ICMP echo requests and the ICMP echo reply messages that is used to test if a certain host is reachable. The user sends the ICMP echo request to the host and then waits for their reply. If no message is returned after some time, we get a Request Timeout.

University of Aveiro Network

Hop	Name	Local	Network/Operator/Owner	IP
0	get2-edu-alunos.core.ua.pt	Aveiro	UA Network/STIC/UA	192.168.63.253
1		Aveiro	UA Network/STIC/UA	10.1.0.118
2	gt1-vrfinternet-r.core.ua.pt	Aveiro	UA Network/STIC/UA	193.137.173.244
3	nx2-ibgp.core.ua.pt	Aveiro	UA Network/STIC/UA	10.0.34.1
4	Router41.Porto.fccn.pt	Porto	FCCN	193.136.4.26
5	Router20.Porto.fccn.pt	Porto	FCCN	194.210.7.108
6	Router30.Lisboa.fccn.pt	Lisboa	FCCN	193.136.1.8
7	Router3.Lisboa.fccn.pt	Lisboa	FCCN	194.210.6.103
8	fccn.mx2.lis.pt.geant.net	Lisboa	FCCN / GEANT	62.40.124.97
9	ae4.mx1.mad.es.geant.net	Madrid	GEANT	62.40.98.97
10	ae7.mx1.gen.ch.geant.net	Genova	GEANT	62.40.98.67
11	ae2.mx1.fra.de.geant.net	Frankfurt	GEANT	62.40.98.180
12	ae7.mx1.ams.nl.geant.net	Amsterdam	GEANT	62.40.98.186
13	sinet.mx1.ams.nl.geant.net	Amsterdam	SINET/GEANT	62.40.125.183
14		Tokyo	Research Organization of Information and Systems	150.99.21.50
15		Tokyo	Research Organization of Information and Systems	150.99.0.141
16	geidai-ueno.gw.sinet.ad.jp	Tokyo	Research Organization of Information and Systems	150.99.198.182
17	nat.geidai.ac.jp	Tokyo	Research Organization of Information and Systems	202.244.240.2
18	www.noc.geidai.ac.jp	Tokyo	Research Organization of Information and Systems	202.244.248.202

Technologies used: IPv4 communication protocol at OSI Layer 3 (Network). ICMP is situated in Layer 4 (Transport).

4.2 Interpreting the results

4.2.1 Hops

A hop is the journey from one computer to another. A traceroute readout typically will display three separate columns for the hop time, as each traceroute sends out three separate packets of information to each computer. The players involved between hops are often telecom operators or university communication centers, sometimes also going through private IP addresses.

As we can see from *Fig. 1* on hop 12 there was “Request timed out”. The probable reason is that the router did not respond to the ICMP echo request that we sent. This can be due to many different causes like network congestion, failure of the ARP request, packet filtering, routing error or even for security reasons

because there are some situations where a key router can be attacked, something that attackers can explore.

A possible attack could be an ICMP Flood DDoS *(Distributed Denial of Service)* attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings). By flooding the target with request packets, the network is forced to respond with an equal number of reply packets. This causes the target to become inaccessible to normal traffic.

Another one could be an ICMP packet magnification, where the attacker sends forged ICMP echo packets to vulnerable networks' broadcast addresses and when all the systems on those networks send ICMP echo replies to the victim, they consume the target system's available bandwidth and creating a denial of service (DoS) to legitimate traffic.

As we can clearly see from *Fig. 2* connection is made in less hops, faster, without any Request Timeouts and travelling through different routers until it reaches its' destination. The reason for this can be the location, given that the *tracert* commands were made with about 40km of distance from each other, another reason is that one was a home network and the other one came from a university network.

4.2.2 Logs

We tried the "*tracert*" command various times of day and different locations (University of Aveiro and home network) and the results obtained from the logs show a slight variation between locations and even in the same network there are some differences when executed at different times.

A reason for this might be that at a specific time, a path can be overwhelmed with a large number of requests, making it harder to respond back. This will increase latency, which is not good. To avoid this problem, the following requests are going to be sent through other routers, so that the connection can be as efficient as possible.

5. Social and Economic Implications

There are several implications when making a web connection. Although it looks simple enough for us, the amount of work put in the technologies, processes, actors, and business models involved is remarkable.

From physical aspects such as computer/routers problems to more complex subjects like the social and economic aspect. If there is a certain event affecting a specific area, for example the COVID-19 pandemic, many companies and services will have to adapt, in this example they had to make changes to survive in the "new world", where everyone worked from home and web technologies were used more than ever before.

Furthermore, social aspects such as the current invasion that Ukraine is suffering from Russia also implicates measures relating to web connections, in this case in a negative way, as many companies and services shut down their operations in Russia, preventing them from accessing things we take for granted, like social media pages or online services, making them nearly isolated from the rest of the world, affecting both their lives and their work.

6. Conclusion

From this assignment we gained a greater knowledge about what happens during a web connection, the tools used and all the implications that are associate with it.

Also, with the *"tracert"* command we were able to see the players involved in a connection, as well as the technologies, processes, actors, and business models.

From all these things learned during the making of this assignment we took several notes, including the social and economic implications as well as a better knowledge of what happens during a typical web session.

7. References

[1] How the Web works [19/03/2022] URL: https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works

[2] Traceroute Command [19/03/2022] URL: https://www.sciencedirect.com/topics/computer-science/traceroute-command

[3] Simple History of the Internet: Looking at the Evolution of Internet Connection [19/03/2022] URL: https://nectmodem.com/simple-history-of-the-internet-looking-at-the-evolution-of-internet-connection/

[4] How do computers connect over the Internet? URL: https://www.computerhope.com/issues/ch001358.htm

[5] What is TCP/IP and How Does It Work? [19/03/2022] URL: https://www.techtarget.com/searchnetworking/definition/TCP-IP

[6] How does the Internet work? [19/03/2022] URL: https://developer.mozilla.org/en-US/docs/Learn/Common_questions/How_does_the_Internet_work

[7] IP Tracker [20/03/2022] URL: https://www.ip-tracker.org/

[8] What is an ICMP Flood DDoS Attack? [20/03/2022] URL: https://www.netscout.com/what-is-ddos/icmp-flood

[9] NFSI Internet Services [21/03/2022] URL: http://www.nfsi.pt/

[10] Who is FCCN [21/03/2022] URL: https://www.fccn.pt/en/quem-somos/

[11] Russia is nearly isolated online. What does that mean for the internet's future? [22/03/2022] URL: https://www.nbcnews.com/tech/internet/russia-nearly-isolated-online-mean-internets-future-rcna19389