



Anatomy of a Web Connection: A Brief Analysis

Aspetos Profissionais e Sociais da Engenharia Informática

Ricardo Rodriguez (98388)

13/03/2022



Índice

1. Introdução	3
2. Contexto	3
3. Conexão Web	3
3.1. Web Browser	3
3.2. Modelo OSI	4
3.2.1. Camada física	4
3.2.2. Camada de ligação de dados	4
3.2.3. Camada de rede	4
3.2.4. Camada de transporte	5
3.2.5. Camada de sessão	5
3.2.6. Camada de apresentação	5
3.2.7. Camada aplicacional	5
3.3. TCP/IP	5
3.4. HTTP	6
3.5. DNS	6
3.6. ICMP	6
4. <i>Traceroute</i>	7
4.1. Execução do comando	7
4.2. Interpretação dos resultados obtidos	8
4.2.1. Identificação dos <i>hops</i>	8
4.2.2. Os <i>logs</i> do <i>traceroute</i> são iguais em tempos e localizações diferentes?	9
4.2.3. Que entidades estão envolvidas em cada <i>hop</i> ?	10
5. Implicações socioeconómicas	10
6. Ocorrências numa sessão <i>web</i>	11
7. Conclusão	12
Referências	13



1. Introdução

Neste relatório, iremos abordar de forma detalhada o comando *traceroute*, executando-o e interpretando os resultados obtidos.

Os principais objetivos deste relatório são:

- Fornecer uma identificação plausível das tecnologias, processos, atores e modelos de negócio envolvidos numa conexão *web*;
- Identificar possíveis implicações sociais e económicas associadas com as entidades envolvidas numa conexão *web*.

2. Contexto

No contexto atual, o crescimento exponencial da tecnologia, juntamente com as ferramentas que estas proporcionam, levam à existência de um espaço cibernético onde a maior parte dos utilizadores não sabe o que realmente está a acontecer em segundo plano.

Desta forma, a maior parte dos utilizadores inexperientes na área da informática não compreende como funcionam as conexões na internet - os processos, as tecnologias e as entidades que estão envolvidas, os dados que são armazenados, bem como uma série de outros fatores que cobijam a privacidade de cada indivíduo.

3. Conexão Web

Numa conexão *web*, existem duas entidades diferentes: o servidor e o cliente. Os servidores são um sistema que disponibiliza aplicações, websites e outros tipos de serviços para um cliente. O cliente é um dispositivo capaz de aceder à internet que consome um serviço providenciado por um servidor. Definido agora o que é uma conexão *web*, é importante compreender as tecnologias que a suportam.

3.1. Web Browser

Um *browser* é um programa que permite a navegação na internet por um dispositivo, interagindo com o utilizador para apresentar a informação que está a ser transmitida pela web através do protocolo HTTP, que será abordado posteriormente.

A maior parte dos *browsers* permite, também, adicionar extensões que personalizam a experiência do utilizador.

3.2. Modelo OSI

O modelo OSI fornece é um modelo conceitual que padroniza a comunicação entre diferentes computadores, descrevendo as diferentes funções numa rede de computadores.

No modelo OSI, existem sete camadas de abstração relativas à comunicação numa rede: camada física, camada de ligação de dados, camada de rede, camada de transporte, camada de sessão, camada de apresentação e a camada aplicacional.

3.2.1. Camada física

É a camada mais subjacente no modelo OSI. Esta define as especificações elétricas e físicas relativas ao equipamento físico usado na transmissão de dados como cabos de fibra ótica, *hubs*, repetidores e outras dispositivos. Protocolos: Modem, 802.11 WiFi, USB, Bluetooth...

3.2.2. Camada de ligação de dados

Na camada de ligação de dados, existe uma separação dos pacotes transmitidos por subpartes, designadas de quadros, e a correção de erros caso tenham ocorrido na camada anterior. Protocolos: Ethernet, IEEE 802.1Q, ARP...

3.2.3. Camada de rede

A camada de rede define o roteamento dos pacotes, encontrando o melhor caminho para a transmissão dos mesmos. Desta forma, este faz a entrega conforme o endereço lógico de destino como, por exemplo, o IP (protocolo de internet). Protocolos: IP (divide-se em IPv4, IPv6), ICMP, IPSec...

3.2.4. Camada de transporte

A camada de transporte é responsável pela forma como a comunicação vai ser estabelecida, uma vez que já se foi definido o percurso dos pacotes na camada anterior. Assim, esta é que garante o envio e a receção dos pacotes que vêm na camada de rede. Protocolos: TCP, UDP, RIP...

3.2.5. Camada de sessão

A camada de sessão, tal como o nome indica, é responsável pela sessão entre os dispositivos. Posto isto, esta cria, recria, gere, encerra e autentica as conexões entre diferentes entidades. Protocolos: ASP, NetBIOS, PAP, SCP...

3.2.6. Camada de apresentação

Esta camada é responsável pela tradução dos dados de forma a serem interpretados pela camada aplicacional, o que pode envolver a conversão, compactação e criptografia dos dados. Protocolos: TLS, XDR...

3.2.7. Camada aplicacional

É a camada no topo do modelo OSI. Nesta camada, os dados traduzidos pela camada anterior interagem diretamente com a respetiva aplicação. Deste modo, as aplicações conseguem aceder a *websites*, enviar emails e outros serviços que dependem da rede para funcionarem. Protocolos: HTTP, SSH, Telnet, BitTorrent, DNS, RTP, FTP...

3.3. TCP/IP

O TCP/IP é o protocolo padrão na comunicação entre dispositivos na internet. Este consiste em:

- Um endereço IP que torna um computador na internet único, de forma a que se possa identificar precisamente com quem queremos comunicar. Pertence à camada de rede do modelo OSI.

- TCP – protocolo de transporte na internet que funciona como um aperto de mãos, onde uma entidade envia uma mensagem e a outra confirma a entrega da mesma, garantindo a integridade do processo. Pertence à camada de transporte do modelo OSI.
- UDP – semelhante ao anterior, diferenciando-se por não confirmar a receção da mensagem, não assegurando a integridade do processo. Pertence à camada de transporte do modelo OSI.

3.4. HTTP

O *HyperText Transfer Protocol*, ou HTTP, é um protocolo que permite a transferência de conteúdo de uma página *web* entre o servidor e a máquina do cliente. É um protocolo *stateless*, o que significa que não guarda nenhum tipo de dados sobre a conexão (ao contrário dos dados de sessão ou das *cookies*). É normalmente baseado na camada de transporte TCP/IP, podendo também ser utilizado por protocolos diferentes. Pertence à camada aplicacional segundo o modelo OSI.

3.5. DNS

O DNS, também conhecido por *domain name system*, são as “páginas amarelas” da internet, na medida em que fazem o mapeamento entre um nome de domínio (*google.com*) e o respetivo endereço IP (*64.233.185.102*).

3.6. ICMP

O ICMP é um protocolo usado para comunicações na camada da rede, integrando o protocolo IP, pois a sua principal utilidade é o fornecimento de mensagens de erro relativos ao protocolo IP, de forma a que os computadores alterem o seu comportamento. Devido às suas características enquanto um bom protocolo de teste de rede, este é usado nos comandos *traceroute* e *tracert*.

4. Traceroute

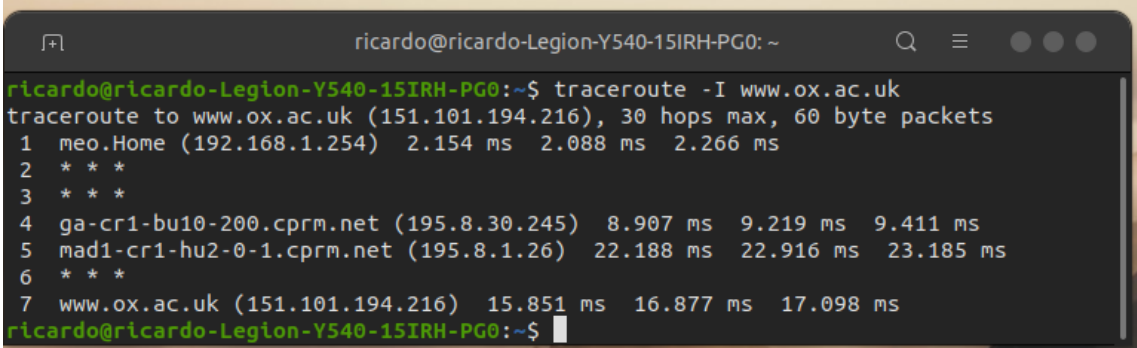
O comando *traceroute* é uma ferramenta de diagnóstico de rede disponível no sistema operativo *Linux* que analisa o percurso dos pacotes IP desde a sua origem até ao endereço de destino especificado, listando todos os routers intermédios, também designados de *hops*, que intervieram no transporte dos pacotes. Existem, ainda, outras variantes deste comando presentes em outros sistemas operativos, como o *tracert* no Windows.

O *traceroute* começa por enviar três sondas com um TTL inicial (*time-to-live*) igual a 1. Cada *router* intermédio que recebe os pacotes IP decrementa o TTL do pacote por uma unidade e, quando o valor do TTL chegar a 0, o respetivo *router* cancela o envio do pacote IP e retorna uma mensagem especificando que o tempo para alcançar o endereço de destino foi excedido.

Enquanto os pacotes IP não chegam ao destino, o valor inicial do TTL das sondas vai sendo incrementado por uma unidade, até chegar ao limite de 30 *hops* (valor pré-definido que pode ser alterado).

4.1. Execução do comando

Executando o comando '*traceroute www.ox.ac.uk*', obtêm-se os seguintes resultados:



```
ricardo@ricardo-Legion-Y540-15IRH-PG0: ~  
ricardo@ricardo-Legion-Y540-15IRH-PG0:~$ traceroute -I www.ox.ac.uk  
traceroute to www.ox.ac.uk (151.101.194.216), 30 hops max, 60 byte packets  
 1  meo.Home (192.168.1.254)  2.154 ms  2.088 ms  2.266 ms  
 2  * * *  
 3  * * *  
 4  ga-cr1-bu10-200.cprm.net (195.8.30.245)  8.907 ms  9.219 ms  9.411 ms  
 5  mad1-cr1-hu2-0-1.cprm.net (195.8.1.26)  22.188 ms  22.916 ms  23.185 ms  
 6  * * *  
 7  www.ox.ac.uk (151.101.194.216)  15.851 ms  16.877 ms  17.098 ms  
ricardo@ricardo-Legion-Y540-15IRH-PG0:~$
```

Fig. 1 | Comando executado às 14:23 em ambiente residencial

```
ricardo@ricardo-Legion-Y540-15IRH-PG0: ~  
ricardo@ricardo-Legion-Y540-15IRH-PG0:~$ traceroute -I www.ox.ac.uk  
traceroute to www.ox.ac.uk (151.101.130.216), 30 hops max, 60 byte packets  
1  meo.Home (192.168.1.254)  1.133 ms  1.546 ms  2.189 ms  
2  * * *  
3  * * *  
4  ga-cr1-bu10-200.cprm.net (195.8.30.245)  8.955 ms  9.534 ms  10.059 ms  
5  mad1-cr1-hu2-0-1.cprm.net (195.8.1.26)  22.607 ms  22.815 ms  23.268 ms  
6  199.27.73.8 (199.27.73.8)  25.707 ms  20.594 ms  20.826 ms  
7  www.ox.ac.uk (151.101.130.216)  19.075 ms  18.005 ms  18.691 ms  
ricardo@ricardo-Legion-Y540-15IRH-PG0:~$
```

Fig. 2 | Comando executado às 21:50 em ambiente residencial

```
ricardo@ricardo-Legion-Y540-15IRH-PG0: ~  
ricardo@ricardo-Legion-Y540-15IRH-PG0:~$ traceroute -I www.ox.ac.uk  
traceroute to www.ox.ac.uk (151.101.130.216), 30 hops max, 60 byte packets  
1  gt2-edu-alunos.core.ua.pt (192.168.63.253)  3.005 ms  2.939 ms  2.925 ms  
2  10.1.0.118 (10.1.0.118)  2.910 ms  9.363 ms  9.353 ms  
3  gt1-vrfinetnet-r.core.ua.pt (193.137.173.244)  9.343 ms  9.333 ms  9.323 ms  
4  nx2-ibgp.core.ua.pt (10.0.34.1)  9.309 ms  9.299 ms  9.288 ms  
5  Router41.Porto.fccn.pt (193.136.4.26)  9.271 ms  9.261 ms  9.251 ms  
6  Router40.Porto.fccn.pt (194.210.7.208)  9.242 ms  6.018 ms  5.960 ms  
7  Router60.Lisboa.fccn.pt (193.136.1.10)  19.368 ms  19.353 ms  27.334 ms  
8  Router3.Lisboa.fccn.pt (194.210.6.203)  27.284 ms  27.273 ms  27.262 ms  
9  fccn-ias-geant-gw.mx2.lis.pt.geant.net (83.97.88.209)  27.251 ms  27.241 ms  27.231 ms  
10 ae4.mx1.mad.es.geant.net (62.40.98.97)  36.860 ms  36.850 ms  36.839 ms  
11 * * *  
12 151.101.130.216 (151.101.130.216)  34.200 ms  34.183 ms  34.176 ms
```

Fig. 3 | Comando executado na Universidade de Aveiro às 17:03

4.2. Interpretação dos resultados obtidos

4.2.1. Identificação dos *hops*

Cada um dos passos intermédios, ou *hops*, representam uma máquina que recebeu o pacote IP, encaminhando-o para o *router* seguinte até chegar ao destino.

Podem existir três fatores diferentes que justificam os *hops* serem assinalados por asteriscos: o tráfego IP foi bloqueado por uma *firewall* e, desta forma, o pacote parou; houve um problema na rede e o pacote foi cancelado; a máquina não está configurada para responder ao encaminhamento de pacotes IP e os dados sobre a mesma não foram apresentados, o que não significa que o pacote não passou pelo mesmo.

Tipicamente, cada *hop* lista o seu *domain name system* (DNS), o seu endereço IP e, de seguida, um conjunto de três valores numéricos que fazem parte do *Round-Trip*

Time (RTT), que representam o tempo mínimo, médio e máximo do transporte dos pacotes até ao router atual, respetivamente.

Hop	Device or Media	Location	IP Address	Network/Operator/ Owner
1	gt2-edu-alunos.core.ua.pt	Aveiro	192.168.63.253	UA Network/STIC/UA
2	***	***	10.1.0.118	UA Network/STIC/UA
3	gt1-vrfinetnet-r.core.ua.pt	Aveiro	193.137.173.244	UA Network/STIC/UA
4	nx2-ibgp.core.ua.pt	Aveiro	10.0.34.1	UA Network/STIC/UA
5	Router41.Porto.fccn.pt	Porto	193.136.4.26	FCCN
6	Router40.Porto.fccn.pt	Alenquer	194.210.7.208	FCCN
7	Router60.Lisboa.fccn.pt	Lisboa	193.136.1.10	FCCN
8	Router3.Lisboa.fccn.pt	Alenquer	194.210.6.203	FCCN
9	fccn-ias-geant- gw.mx2.lis.pt.geant.net	Amsterdam	83.97.88.209	GEANT Vereniging
10	ae4.mx1.mad.es.geant.net	Cambridge	62.40.98.97	GEANT Vereniging
11	***	***	***	***
12	***	USA	151.101.130.216	FASTLY

Tab. 1 | *Interpretação dos resultados obtidos através do [IP Tracker](#)*

4.2.2. Os logs do *traceroute* são iguais em tempos e localizações diferentes?

Analisando as *logs* obtidas em tempos diferentes para a mesma localização, apresentadas anteriormente, verificam-se desigualdades entre as mesmas. A diferença no congestionamento da rede durante a tarde, em que o número de pedidos é maior, e ao final da noite, quando o tráfego na rede é menor, pode ser a razão desta assimetria.

Desta forma, para evitar um enorme fluxo de pedidos para as mesmas entidades, os pedidos são redirecionados por outras vias, aliviando a rede e tornando-a mais rápida para estas situações.

Caso os pedidos sejam feitos em localizações diferentes, as *logs* também o são, dado que os pontos de origem são geograficamente distintos e, consequentemente, os *hops* variam entre trajetos diferentes.

4.2.3. Que entidades estão envolvidas em cada *hop*?

Interpretando os resultados do *traceroute* para diferentes endereços de destino e analisando os endereços de cada *hop* através de um [IP tracker](#) genérico, verifica-se que a maioria das entidades envolvidas neste processo são organizações de grande escala, nomeadamente operadoras provedoras de internet, ou entidades relacionadas com os pontos de origem e de destino, como as instituições de ensino demonstradas anteriormente.

5. Implicações socioeconómicas

Em retrospectiva, a criação da internet mudou o estilo de trabalho e de vida no quotidiano. Atualmente, milhões de pessoas utilizam este “novo” universo diariamente para ler notícias, comunicar com outras pessoas, ver vídeos e milhares de outras funcionalidades que estão acessíveis a um clique de distância.

Contudo, é importante referir que as conexões *web* trazem uma série de implicações sociais e económicas.

A nível social, as *cookies* solicitadas pelos *websites* são uma afronta ao direito à privacidade do indivíduo, podendo conter informações sensíveis sobre estes, tal como abordaremos no próximo capítulo. No entanto, a expansão da internet permitiu a globalização das comunicações, uma vez que diferentes nós na internet podem comunicar entre si de forma rápida para partilha de informação, como nunca antes feito.

A nível económico, as entidades envolvidas numa conexão *web* têm de ter uma estrutura capaz de ser escalável e suportar um fluxo crescente de utilizadores, evitando problemas nas conexões estabelecidas, quebras de performance e indisponibilidade dos servidores, podendo perder grandes quantias monetárias caso isto se verifique.

A internet ofereceu uma panóplia de vantagens ao mundo contemporâneo, aumentando a produtividade no trabalho através da automatização de tarefas, da facilidade na comunicação e partilha de dados e da existência de ferramentas que agilizam os processos de trabalho, bem como no estilo de vida das pessoas através das redes sociais, da digitalização do mundo do entretenimento e da disponibilidade de toda a informação possível na mesma.

Posto isto, é inegável assinalar a importância que a internet tem na sociedade e na economia mundial, uma vez que reformou por completo o estilo de vida das pessoas e o *modus operandi* das empresas, apresentando tanto vantagens como desvantagens referidas anteriormente.

6. Ocorrências numa sessão *web*

Numa sessão típica na internet, os utilizadores são questionados se pretendem aceitar as *cookies*, podendo configurar as mesmas para atingir os requisitos mínimos de utilização do *website*.

Normalmente, o utilizador comum toma decisões espontâneas sem qualquer tipo de reflexão e aceita qualquer tipo de *cookies* nos *websites* que frequenta diariamente, evitando analisar os tipos de dados recolhidos.

As *cookies* são um ficheiro armazenado no nosso dispositivo que guarda informação dos *websites* visitados para que, quando este seja acedido uma próxima vez, este verifique o seu conteúdo. Tipicamente, as *cookies* guardam informações pessoais como o histórico de produtos visualizados, as opções de preferência que são escolhidas, bem como outras informações.

Estas podem ser benéficas para os *websites*, uma vez que evitam a persistência desta informação numa base de dados, tendo estes de estar guardados no dispositivo do cliente, poupando recursos ao servidor. Por outro lado, as *cookies* trazem uma série de complicações ao nível do direito à privacidade dos utilizadores, na medida em que as entidades que podem ter acesso a estas informações pessoais, sejam *websites* ou *hackers*, podem ler e/ou partilhar informação que são tomadas como seguras para proveito próprio.

Existem vários tipos de dados a serem coletados aos utilizadores, entre eles:

- A obtenção de informação relativa à interação do utilizador com o *website* como, por exemplo, os produtos que este visualizou. Isto pode ajudar a traçar o perfil do utilizador para fins publicitários, apresentando anúncios personalizados que terão uma maior probabilidade de terem a atenção do cliente.
- Obtenção de dados sensíveis como o endereço IP, para determinar a localização da vítima, ou informação relativa ao dispositivo/browser.
- Obtenção de *cookies* externas – o *website* lê informação que foi registada por outro *website* e acumula a informação obtida durante a sessão, enviando-a de volta para o *website* criador da cookie.

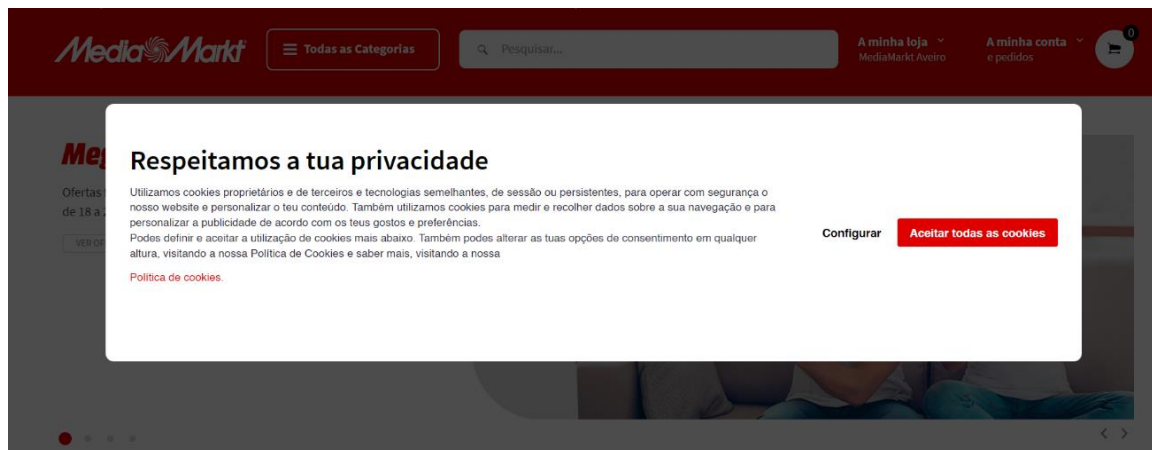


Fig. 4 | *Pedido de aceitação de cookies num website popular*

7. Conclusão

Neste relatório, foi analisado o percurso de um pacote desde a sua origem até ao endereço de destino pretendido, identificando as tecnologias, processos, entidades e modelos de negócio, através da utilização do comando *traceroute*.

Da mesma forma, foram refletidas as implicações socioeconómicas provocadas por uma simples conexão *web*, bem como o que ocorre durante estas sessões *web*.



Referências

Fortinet. *What is Traceroute: What Does it Do & How Does It Work?* [Acessado a 14/03/2022] URL: <https://www.fortinet.com/resources/cyberglossary/traceroutes>

Mozilla. *HTTP* [Acessado a 17/03/2022]. URL: <https://developer.mozilla.org/pt-BR/docs/Web/HTTP>.

Wikipedia. *TCP/IP* [Acessado a 18/03/2022]. URL: <https://pt.wikipedia.org/wiki/TCP/IP>

Cloudflare. *What is the OSI Model?* [Acessado a 18/03/2022]. URL: <https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/>

Forcepoint. *The OSI model defined.* [Acessado a 18/03/2022]. URL: <https://www.forcepoint.com/cyber-edu/osi-model>

Wikipedia. *ICMP* [Acessado a 18/03/2022]. URL: https://pt.wikipedia.org/wiki/Internet_Control_Message_Protocol

FCCN. *Quem Somos* [Acessado a 19/03/2022]. URL: <https://www.fccn.pt/>

Cogent. *About cogent* [Acessado a 19/03/2022]. URL: <https://www.cogentco.com/en/about-cogent>

Vox. *Why every website wants you to accept its cookies* [Acessado a 21/03/2022]. URL: <https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy>

OSI Model. *OSI-Model.* [Acessado a 21/03/2022]. URL: <https://osi-model.com/>