

Redes e Comunicações

Ferramentas “Traceroute”

Grupo 1

10/10/2011

SPT Traceroute

Esta ferramenta permite apenas testar o traceroute, observando-se:

- 4-5 - Salto Intercontinental Austrália → Seattle(13438 Km em linha recta)

$$t_{4med} = (1.156 \text{ ms} + 1.096 \text{ ms} + 1.103 \text{ ms}) / 3 = 1,1 \text{ ms}$$

$$t_{5med} = (144.797 \text{ ms} + 144.701 \text{ ms} + 145.597 \text{ ms}) / 3 = 145 \text{ ms}$$

$$t_5 - t_4 = 145 - 1,1 = 143,9 \text{ ms rtt.}$$

O tempo de ida será então de $143,9 / 2 = 71,95 \text{ ms}$

$$d = v * t \iff t = d / v \iff t = 13438000 / 3 * 10^8 = 44 \text{ ms}$$

Como 71,95 ms é próximo de 44 ms podemos concluir que a ligação é feita através de um cabo transoceânico, já que 71,95 ms é bem menos que 250 ms o que exclui a hipótese da comunicação ter sido feita através de satélite.

- 12-13 há duas respostas distintas, o que denota que o salto 12 está ligado a 2 routers, que estão há mesma distância, e este pode escolher um dos dois routers, o que significa que apesar do caminho dos pacotes estar à partida pré-definido este é dinâmico podendo alterar entre uma das duas hipóteses, isto só é possível devido a configuração do router que encaminhou o pacote, neste caso o router presente em Washington. Caso existam vários pacotes, podem ainda ser enviados para routers diferentes, de modo a distribuir a carga.

Devido ao valor de cerca de 40 ms ida (80/2 rtt) podemos também concluir que a ligação é feita através de um cabo de fibra trans-atlântico.

- 13-14 há três respostas distintas, o que denota que os saltos 13 estão ligados a 3 routers diferentes, aplica-se também o que foi referido no salto 12-13.
- 14-15 há duas respostas distintas, o que denota que os saltos 14 estão ligados a 2 routers diferentes.
- 15-16 há três respostas distintas, o que denota que os saltos 15 estão ligados a 3 routers diferentes.
- A partir do salto 17 cada router só está ligado a outro router.
- Nos saltos 20, 24, 25 e 26 não houve uma resposta em tempo útil, o que significa que o router não respondeu ou então respondeu num espaço de tempo muito elevado.

Traceroute Output

FROM mirror.sptel.com.au TO polo.uminho.pt.

traceroute to polo.uminho.pt (193.136.9.241), 30 hops max, 40 byte packets

```
1 fe0-0.chr01-kent-syd.comindico.com.au (203.220.0.1) 0.834 ms 0.528 ms 0.591 ms
2 ge1-10.dls01-kent-syd.comindico.com.au (203.220.112.48) 1.329 ms 1.242 ms 3.611 ms
3 75.112.220.203.unassigned.comindico.com.au (203.220.112.75) 1.254 ms 1.100 ms 1.090
ms
4 syd-sot-ken-crt1-pos-8-0.tpgi.com.au (202.7.162.245) 1.156 ms 1.096 ms 1.103 ms
5 ge5-0-5d0.cir1.seattle7-wa.us.xo.net (216.156.100.37) 144.797 ms 144.701 ms 145.597
ms
6 4.59.232.53 (4.59.232.53) 157.246 ms 157.395 ms 156.868 ms
7 ae-32-52.ebr2.Seattle1.Level3.net (4.69.147.182) 157.349 ms 157.734 ms 159.436 ms
8 ae-2-2.ebr2.Denver1.Level3.net (4.69.132.54) 174.614 ms 174.398 ms 174.881 ms
9 ae-3-3.ebr1.Chicago2.Level3.net (4.69.132.62) 198.801 ms 198.922 ms 199.066 ms
10 ae-1-100.ebr2.Chicago2.Level3.net (4.69.132.114) 198.992 ms 199.784 ms 199.088 ms
11 ae-6-6.ebr2.Washington12.Level3.net (4.69.148.145) 218.118 ms 217.935 ms 218.019 ms
12 ae-5-5.ebr2.Washington1.Level3.net (4.69.143.221) 218.019 ms 218.197 ms 218.105 ms
13 ae-41-41.ebr2.Paris1.Level3.net (4.69.137.49) 298.388 ms ae-44-
44.ebr2.Paris1.Level3.net (4.69.137.61) 299.185 ms 297.877 ms
14 ae-46-46.ebr1.Frankfurt1.Level3.net (4.69.143.137) 298.995 ms ae-45-
45.ebr1.Frankfurt1.Level3.net (4.69.143.133) 298.634 ms ae-48-48.ebr1.Frankfurt1.Level3.net
(4.69.143.145) 300.528 ms
15 ae-61-61.csw1.Frankfurt1.Level3.net (4.69.140.2) 312.097 ms 298.439 ms ae-81-
81.csw3.Frankfurt1.Level3.net (4.69.140.10) 298.517 ms
16 ae-4-90.edge5.Frankfurt1.Level3.net (4.69.154.201) 300.024 ms ae-1-
60.edge5.Frankfurt1.Level3.net (4.69.154.9) 299.043 ms ae-3-80.edge5.Frankfurt1.Level3.net
(4.69.154.137) 299.208 ms
17 DANTE.edge5.Frankfurt1.Level3.net (212.162.4.10) 298.634 ms 299.647 ms 298.829 ms
18 so-5-0-0.rt1.gen.ch.geant2.net (62.40.112.162) 306.814 ms 306.915 ms 309.561 ms
19 as0.rt1.mad.es.geant2.net (62.40.112.26) 328.635 ms 328.659 ms 330.408 ms
20 * * *
21 ROUTER3.10GE.Lisboa.fccn.pt (193.137.0.27) 380.266 ms 379.007 ms 378.918 ms
22 Router2.10GE.DWDM.Porto.fccn.pt (193.136.1.2) 385.226 ms 383.575 ms 383.542 ms
23 UMinho.Braga.fccn.pt (193.136.4.100) 386.093 ms 385.393 ms 384.960 ms
24 * * *
25 * * *
26 * * *
27 polo.uminho.pt (193.136.9.241) 384.699 ms 384.634 ms 384.684 ms
```

CentralOPS

Domain Dossier Investigate domains and IP addresses

domain or IP address

☐ domain whois record ☐ DNS records ☒ traceroute
☐ network whois record ☐ service scan

CentralOPS trata-se de uma ferramenta que possibilita realizar várias acções mencionadas na figura a cima, contudo nesta tarefa só iremos analisar o traceroute.

- 7-8 muda de Estado (Dallas-Atlanta) o que demora cerca de 20 ms
- 11-12 Transatlantico por cabo porque é bem menos que 250 ms o que exclui a hipótese da comunicação ter sido feita através de satélite.
- 23,24,25 não houve uma resposta em tempo útil, o que significa que o router não respondeu ou então respondeu num espaço de tempo muito elevado.

Traceroute

Tracing route to **polo.uminho.pt [193.136.9.241]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	19	1	4	70.84.211.97	61.d3.5446.static.theplanet.com
2	0	0	0	70.87.254.5	po101.dsr02.dllstx5.networklayer.com
3	1	1	0	70.85.127.109	po52.dsr02.dllstx3.networklayer.com
4	0	0	0	70.87.255.45	e6-1.ibr04.dllstx3.networklayer.com
5	1	0	0	4.71.122.1	te-3-4.car4.dallas1.level3.net
6	1	1	0	4.69.145.62	vlan60.csw1.dallas1.level3.net
7	1	1	4	4.69.151.134	ae-63-63.ebr3.dallas1.level3.net
8	21	20	20	4.69.134.22	ae-7-7.ebr3.atlanta2.level3.net
9	34	34	34	4.69.132.86	ae-2-2.ebr1.washington1.level3.net
10	35	34	35	4.69.134.134	ae-71-71.csw2.washington1.level3.net
11	34	34	34	4.69.134.149	ae-72-72.ebr2.washington1.level3.net
12	123	113	113	4.69.137.49	ae-41-41.ebr2.paris1.level3.net
13	123	122	122	4.69.143.137	ae-46-46.ebr1.frankfurt1.level3.net
14	121	120	121	4.69.140.14	ae-91-91.csw4.frankfurt1.level3.net
15	121	120	179	4.69.154.201	ae-4-90.edge5.frankfurt1.level3.net
16	122	122	122	212.162.4.10	dante.edge5.frankfurt1.level3.net
17	130	130	131	62.40.112.162	so-5-0-0.rt1.gen.ch.geant2.net
18	151	151	151	62.40.112.26	as0.rt1.mad.es.geant2.net
19	177	177	176	62.40.124.98	fccn-gw.rt1.mad.es.geant.net
20	177	177	177	193.137.0.27	router3.10ge.lisboa.fccn.pt
21	181	181	181	193.136.1.2	router2.10ge.dwdm.porto.fccn.pt
22	183	183	183	193.136.4.100	uminho.braga.fccn.pt
23	*	*	*		
24	*	*	*		
25	*	*	*		
26	183	183	183	193.136.9.241	polo.uminho.pt

Trace complete

What is my ip address

General IP Information

IP:	193.136.19.11
Decimal:	3246920459
Hostname:	tuna.di.uminho.pt
ISP:	FCCN (Fundacao para a Computacao Cientifica Nacion
Organization:	Universidade do Minho
Services:	None detected
Type:	Unknown

Geolocation Information

Country:	Portugal
State/Region:	Braga
City:	Braga
Latitude:	41.55
Longitude:	-8.4333

Este serviço permite-nos obter informação sobre polo.uminho.pt.

Possibilitando saber que este tem como ip 193.136.19.11 e qual a sua localização geográfica.

Traceroute

Tracing route to 193.136.19.11

Hop	Time	Host	IP	Location
1	0.524	10.0.0.1	10.0.0.1	, ,
2	84.19	10.20.62.254	10.20.62.254	, ,
3	47.857	r2-l3tca-cr2.nextweb.net	216.237.3.33	Irvine, CA, United States
4	25.508	ge-6-15.car2.Tustin1.Level3.net	4.79.142.41	, , United States
5	55.024	ae-2-4.bar2.Tustin1.Level3.net	4.69.132.226	, , United Kingdom
6	11.031	ae-46-46.ebr3.LosAngeles1.Level3.net	4.69.153.58	, , United States
7	91.963	ae-4-4.ebr4.Washington1.Level3.net	4.69.132.82	, , United Kingdom
8	88.212	ae-84-84.csw3.Washington1.Level3.net	4.69.134.186	, , United States
9	80.723	ae-82-	4.69.134.153	, , United States

		82.ebr2.Washington1.Level3.net		
10	187.935	ae-41-41.ebr2.Paris1.Level3.net	4.69.137.49	, , United States
11	194.277	ae-47-47.ebr1.Frankfurt1.Level3.net	4.69.143.141	, , United States
12	214.15	ae-61-61.csw1.Frankfurt1.Level3.net	4.69.140.2	, , United States
13	212.331	ae-1-60.edge5.Frankfurt1.Level3.net	4.69.154.9	, , United States
14	188.641	DANTE.edge5.Frankfurt1.Level3.net	212.162.4.10	, , Germany
15	185.224	so-5-0-0.rt1.gen.ch.geant2.net	62.40.112.162	, , United Kingdom
16	258.167	as0.rt1.mad.es.geant2.net	62.40.112.26	, , United Kingdom
17	307.75	fccn-gw.rt1.mad.es.geant.net	62.40.124.98	, , United Kingdom
18	261.718	Router3.10GE.Lisboa.fccn.pt	193.137.0.10	Lisboa, 14, Portugal
19	233.782	Router2.10GE.DWDM.Porto.fccn.pt	193.136.1.2	Lisbon, 14, Portugal
20	257.963	UMinho.Braga.fccn.pt	193.136.4.100	, , Portugal
21	N/A	tuna.di.uminho.pt	193.136.19.11	, ,

Este não permite identificar os três probes, o que significa que só é enviado um probe para cada salto, retornando este o tempo, a localização de cada router e respectivo ip.

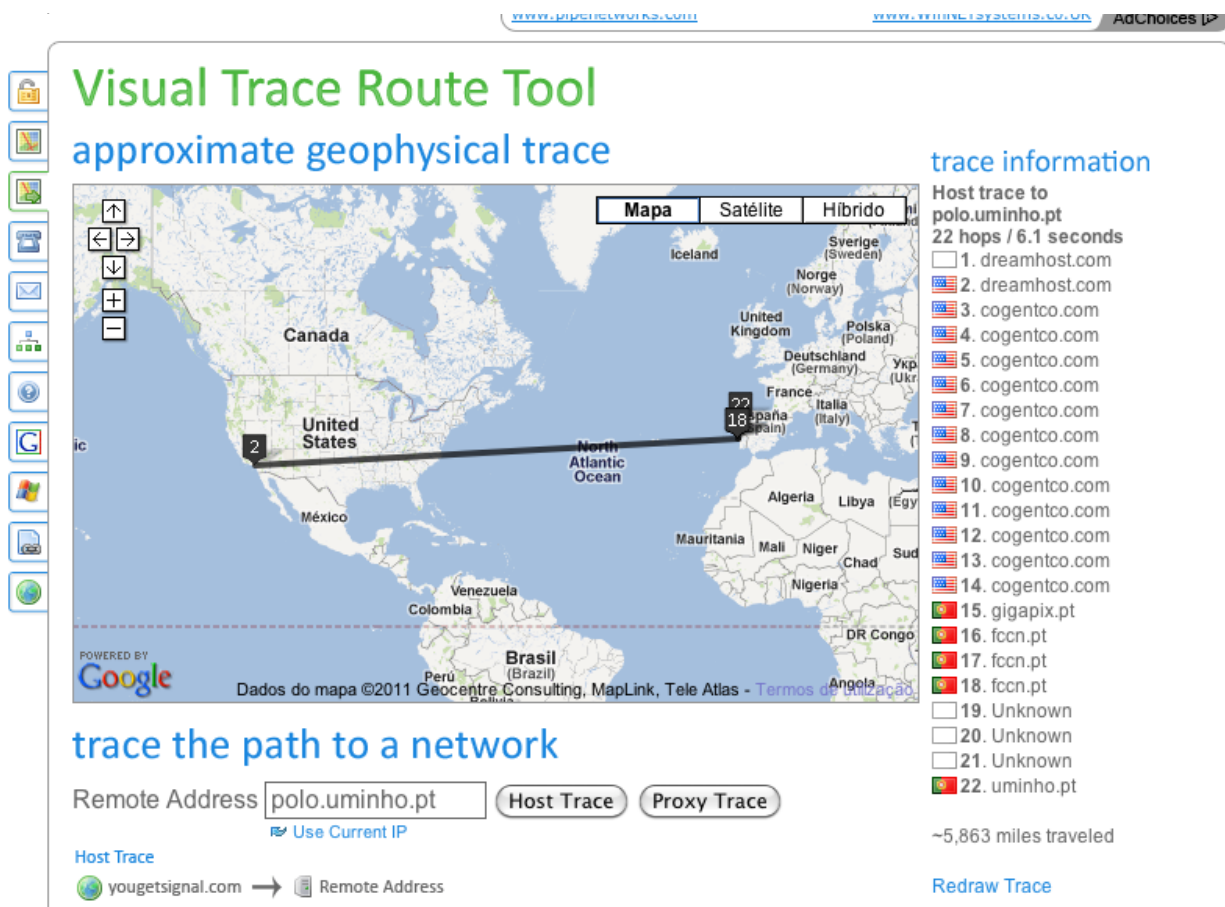
Em cada salto sabe-se que à mesma distância existe pelo menos um router disponível, o que não invalida a presença de outros pois ao ser enviada apenas uma probe só poderemos obter resposta de um router.

Uma das vantagens visíveis que esta ferramenta apresenta em relação à primeira ferramenta utilizada é o facto de esta apresentar uma localização mais precisa do IP de cada salto.

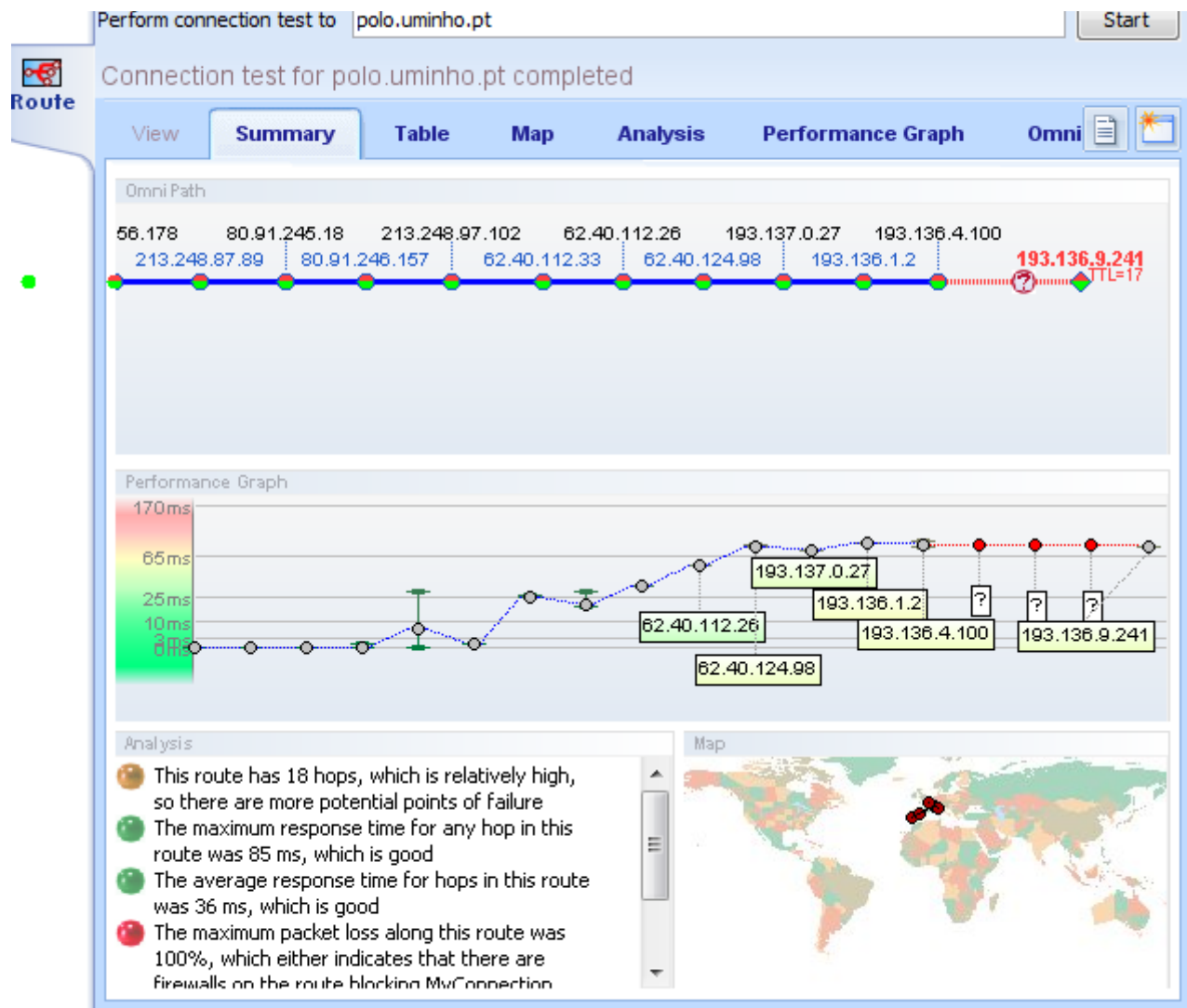
Visual Trace Route Tool

Esta ferramenta permite-nos obter o caminho que os pacotes percorrem até chegarem ao seu destino. Neste caso o caminho que foi percorrido deste o host do yougetsignal.com até ao polo.uminho.pt. Podemos então observar que foram efectuados 22 “saltos” desde a origem ao destino demorando cerca de 6.1 segundos. Sendo 14 deles nos Estados Unidos, 3 são desconhecidos uma vez que não responderam em tempo útil e 5 dentro de Portugal.

Além disso podemos ainda ficar a conhecer a distância total percorrida que neste caso foi de 5863 milhas, ou seja, cerca de 3664 Km.



My Connection Server



Com esta ferramenta podemos observar quantos saltos tem o caminho, 18 neste caso em particular, podemos ainda conhecer o tempo máximo de resposta de cada salto, 85 ms, e ainda saber o seu tempo médio de resposta, 36 ms.

Além disso podemos ainda verificar a existência da perda dos pacotes, da sua percentagem e do local onde foram perdidos, que no caso apresentado será após o IP 193.136.4.100 que corresponde a UMinho.Braga.fccn.pt o que já foi possível observar através da primeira ferramenta utilizada.

É ainda fornecido um gráfico com a performance da ligação que como podemos observar se vai deteriorando à medida que avançamos no caminho.

Conclusão

Como podemos verificar cada serviço tem as suas particularidades, completando-se mutuamente, se por um lado alguns deles se focam mais no caminho percorrido pelos pacotes enviados, dando informação das várias opções que podem tomar, como no caso do salto 12-13 na primeira ferramenta, outras como a *Visual Trace Route* permite-nos ter uma visão mais gráfica desse caminho disponibilizando um mapa com o caminho percorrido pelo pacote. Existem ainda outras que nos dão a informação da performance dos diferentes routers entre cada salto, que é o caso do *My Connection Server*, que além disso ainda nos permite visualizar de uma maneira muito intuitiva o local onde um pacote se perdeu.

No caso da ferramenta *Central Ops* ela além de fornecer a informação que é dada por outras ferramentas, como o Traceroute, fornece-nos uma informação bastante detalhada do host pretendido, como por exemplo a data de registo, o seu titular e ainda informação sobre o servidos.

A ferramenta *WhatIs My Ip Address* pretende fornecer uma informação mais ligada à localização geográfica dando por exemplo a latitude e a longitude do host indicado.

Podemos então concluir que para se conseguir obter uma informação totalmente detalhada e extensiva não nos podemos cingir a apenas uma das ferramentas, mas devemos antes saber combiná-las de modo a obter o que procuramos.