

# Artigo Traceroute

Rafael Gonçalves de Oliveira Viana

2017

## Resumo

Este artigo tem como objetivo uma apresentação do funcionamento do Traceroute, uma ferramenta de gerenciamento de rede. O Traceroute é utilizado para detectar falhas como, por exemplo, gateways intermediários que descartam pacotes ou rotas que excedem a capacidade de um datagrama ip entre outras. Também será de vital importância para esse artigo uma abordagem ao seu protocolo e o funcionamento dos mesmos.

**Palavras-chaves:** Análise de Rede, ICMP, Traceroute, UDP, Roteamento.

## INTRODUÇÃO

A Internet é uma agregação grande e complexa de hardware de rede, conectados entre si por gateways. Seguir a rota que os pacotes seguem (ou encontrar o gateway que está descartando seus pacotes) pode ser difícil. Nesse artigo estaremos abordando o Traceroute, será levantado também alguns conceitos dos protocolos por trás do seu funcionamento.

## 1 PROTOCOLOS

### 1.1 IPv4 - 'Campo TTL'

O IP é o elemento comum encontrado na Internet pública dos dias de hoje. É descrito no RFC 791 da IETF, que foi pela primeira vez publicado em Setembro de 1981. Este documento descreve o protocolo da camada de rede mais popular e atualmente em uso. Esta versão do protocolo é designada de versão 4, ou IPv4. O IPv6 tem endereçamento de origem e destino de 128 bits, oferecendo mais endereçamentos que os 32 bits do IPv4.

Entre os 12 campos do IPv4 descrito no RFC 791 falaremos do TTL, que seria um campo de oito bits presente no IPv4, o TTL (time to live, ou seja, tempo para viver) ajuda a prevenir que os datagramas persistam (ex. andando aos círculos cumutadores) numa rede. O campo TTL limita a vida de um datagrama em segundos, mas tornou-se num campo de contagem de nós caminhados. Cada comutador de pacotes que um datagrama atravessa decrementa o campo TTL em um valor. Quando o campo TTL chega a zero, o pacote não é seguido por um comutador de pacotes e é descartado. O propósito do TTL é evitar que datagramas entrem em um loop de roteamento, o que pode ocorrer devido a algum tipo de falha durante o roteamento dos pacotes. Quando um roteador recebe um datagrama cujo

TTL é igual a 0 (zero), ele não o encaminhará mais. Em vez disso, o roteador irá descartar o pacote e enviar de volta ao host que o originou uma mensagem ICMP do tipo Tempo Excedido. Essa mensagem contém o endereço IP do roteador como endereço de origem - e esse é o segredo do traceroute.(REIS, 2015)

## 1.2 ICMP

O protocolo ICMP (Internet Control Message Protocol - Protocolo de Mensagens de Controle de Internet), especificado no [RFC 792], é usada por hospedeiros e roteadores para comunicar informações de camada de rede entre si. A utilização mais comum do ICMP é para comunicação de erros. Por exemplo, ao rodar uma sessão Telnet, FTP ou HTTP, é possível que você já tenha encontrado uma mensagem de erro como "Rede Inalcançável". Essa mensagem teve sua origem no ICMP. Em algum ponto, um roteador IP não conseguiu descobrir um caminho para o hospedeiro especificado em sua aplicação Telnet, FTP ou HTTP. O roteador criou e enviou uma mensagem ICMP do tipo 3 a seu hospedeiro indicando o erro. O ICMP é frequentemente considerado parte do IP, mas em termos de arquitetura, está logo acima do IP, pois mensagens ICMP são carregadas dentro de datagramas IP. Isto é, mensagens ICMP são carregadas como carga útil IP, exatamente como segmentos TCP ou UDP, que também são carregados como carga útil IP. De maneira semelhante, quando um hospedeiro recebe um datagrama IP com ICMP especificado como protocolo de camada superior, ele demultiplexa o conteúdo do datagrama para ICMP, exatamente como demultiplexaria o conteúdo de um datagrama para TCP ou UDP. Mensagens ICMP têm um campo de tipo e um campo de código. Além disso, contêm o cabeçalho e os primeiros 8 bytes do datagrama IP que causou a criação da mensagem ICMP em primeiro lugar (de modo que o remetente pode determinar o datagrama que casou o erro). Assim, o protocolo ICMP é usado por todos os roteadores para assinalar um erro, chamado de Delivery Problem ou, em português, Problema de Entrega. (KUROSE; ROSS, 2010)

Alguns tipos de mensagens ICMP selecionadas são mostradas na Tabela 1, note que mensagens ICMP não são usadas somente para sinalizar condições de erro. Uma outra mensagem ICMP interessante é a de redução de fonte. Essa mensagem é pouco usada na prática sua finalidade original era realizar controle de congestionamento, permitindo que o roteador congestionado enviasse uma mensagem ICMP de redução de fonte a um hospedeiro para obrigar esse hospedeiro a reduzir sua velocidade de transmissão.

As principais mensagens de erro ou informacionais do ICMP geralmente são enviadas automaticamente em uma das seguintes situações:

1. Um pacote IP não consegue chegar ao seu destino, por exemplo, quando o tempo de vida (TTL) do pacote está expirado (o contador chegou à zero). Esta mensagem é o tempo de vida expirado ou "time exceeded".
2. O roteador não consegue retransmitir os pacotes na frequência adequada, ou seja, o roteador está congestionado (mensagem "source quench").
3. O roteador indica uma rota melhor para o host que está enviando pacotes (mensagem de redirecionamento de rota ou "redirect").
4. Quando um host de destino ou rota não está alcançável (mensagem "destination unreachable" ou destino inalcançável).

5. Quando o host ou o roteador descobrem um erro de sintaxe no cabeçalho do IP (mensagem “parameter problem”).

Existem diversas outras mensagens que o ICMP pode fornecer e cada uma é representada por um tipo e código.([NASCIMENTO, 2016](#))

Tabela 1 – Tipos de mensagens ICMP

Tipo de mensagem ICMP	Código	Descrição
0	0	resposta de eco(para ping)
3	0	rede de destino inalcançavel
3	1	hospedeiro de destino inalcançavel
3	2	protocolo de destino inalcançavel
3	3	porta de destino inalcançavel
3	6	rede de destino desconhecida
3	7	hospedeiro de destino desconhecido
4	0	redução da fonte(controle de congestionamento)
8	0	solicitação de eco
9	0	anúncio do roteador
10	0	descoberta do roteador
11	0	TLL expirado
12	0	cabeçalho IP inválido

## 2 TRACEROUTE

O utilitário traceroute, que foi escrito por Van Jacobson em 1987, é uma ferramenta de diagnóstico que nos permite ver a rota que datagramas IP seguem quando são enviados de um host a outro. O traceroute faz uso do protocolo ICMP e do campo TTL no cabeçalho IP do datagrama. O valor a ser usado neste campo varia entre os sistemas operacionais, sendo comuns os valores 128 para sistemas Windows e 64 para sistemas baseados em Unix, como o Linux (em pacotes normais; o traceroute utiliza valores totalmente diferentes).

### 2.1 Funcionamento

Traceroute utiliza o campo TTL "time to live" do protocolo IP e tenta obter uma resposta ICMP TIME\_EXCEEDED de cada gateway ao longo do caminho para algum host.

O Traceroute nos permite acompanhar a rota de um hospedeiro a qualquer outro hospedeiro do mundo. O interessante é que o Traceroute é implementado com mensagens ICMP. Para determinar os nomes e endereços de roteadores entre a fonte e o destino, o Traceroute da fonte envia uma série de datagramas comuns ao destino. O primeiro desses datagramas tem um TTL de 1, o segundo tem TTL de 2, o terceiro tem um TTL de 3 e assim por diante. A fonte também aciona temporizadores para cada um dos datagramas. Quando o enésimo datagrama chega ao enésimo roteador, o enésimo roteador observa que o TTL do datagrama acabou de expirar (seu TTL é decrementado em um antes de ser encaminhado adiante. O propósito do TTL é evitar que datagramas entrem em um loop de roteamento, o que pode ocorrer devido a algum tipo de falha durante o roteamento dos pacotes. Quando um roteador recebe um datagrama cujo TTL é igual a 0 (zero), ele não o encaminhará mais. Em vez disso, o roteador irá descartar o pacote e enviar de volta ao

host que o originou uma mensagem ICMP). Segundo as regras do protocolo IP, o roteador descarta o datagrama e envia uma mensagem ICMP de aviso à fonte (tipo 11 código 10, para maiores informações consultar ...). Essa mensagem de aviso inclui o nome do roteador e, seu endereço IP. Quando chega à fonte, a mensagem obtém, do temporizador, o tempo de viagem de ida e voltae, da mensagem ICMP, o nome e o endereço IP do enésimo roteador.([KUROSE; ROSS, 2010](#))

O Traceroute sabe quando deve parar de enviar seguimentos UDP, quando uma mensagem chega ao hospedeiro de destino. Como esse datagrama contém um seguimento UDP com um número de porta improvavel, o hospedeiro de destino devolve à fonte uma mensagem ICMP indicando que porta não pôde ser alcançada(mensagem tipo 3, código 3). Quando recebe essa mensagem ICMP particular, o hospedeiro da fonte sabe que não precisa enviar mais pacotes de sondagem.(Na verdade, o programa Traceroute padrão envia conjuntos de três pacotes com o mesmo TLL, assim, o Rraceroute proe três resultados para cada TLL). Desse modo, o hospedeiro da fonte fica a par do número e das identidades de roteadores que estão entre ele e o hospedeiro de destino e o tempo de viagem de ida e volta entre os dois hospedeiros. Note que o programa cliente Traceroute tem de ser capaz de instruir o sistema operacional para que este gere datagramas UDP com valores específicos de TLL. Também tem de poder ser avisado por seu sistema operacional quando chegam mensagens ICMP.

Agora que você entende como o Traceroute funciona, é provável que queira brinca um pouco com ele, esse será o proximo passo desse Artigo.

## 2.2 Linux X Windows

O comando Unix / Linux ‘traceroute’ e os comandos do‘ tracert’ do Microsoft Windows ‘executam a tarefa de rastreamento de caminhos de rede, mas eles o fazem de maneiras ligeiramente diferentes. Ambas as ferramentas para rastreamento de rotas de rede enviam um pacote com TTL (Time To Live) configurado para 1 e denunciam a sua destinação. Então, eles enviam um pacote com TTL = 2 e relatam seu destino. Eles continuam até que os pacotes alcancem seu destino final ou o limite TTL seja excedido. A diferença é que Unix / Linux ‘traceroute’ usa pacotes UDP (User Datagram Protocol) para um número de porta alto aleatório, enquanto o Microsoft Windows usa pacotes ICMP (Internet Control Message Protocol). Essa diferença é crítica ao tentar entender por que o traceroute às vezes falha. Os conjuntos de regras de firewall e as listas de controle de acesso do roteador (ACLs) entre você e o destino devem ser examinados para determinar se eles permitem as altas portas UDP (números de portas acima de 1024) e / ou ICMP.([FAQ, 2016](#))

Além disso, as opções de linha de comando para Microsoft Windows ‘tracert’ diferem das opções de linha de comando para Unix / Linux‘ traceroute’. No entanto, as opções de linha de comando para Unix / Linux ‘traceroute’ também diferem entre as versões do Unix. Leia a página do manual para o seu sistema Unix / Linux para explorar as opções de solução de problemas disponíveis.

Outras diferenças são que o Windows enviará uma solicitação DNS PTR desde o início e, em seguida, enviará solicitações ICMP ECHO. Em cada salto, ele enviará uma solicitação de DNS PTR e depois passará para o próximo salto. O Linux começa com o envio de pacotes UDP para um número de porta alto imediatamente. Quando finalmente chegar ao último salto, ele enviará uma solicitação de massa de DNS PTR para cada salto no caminho que determinou. ([DARREN, 2010](#))

## 2.3 Comandos Traceroute

### SINTAXE

```
traceroute [-m Max_ttl] [-n] [-p Port] [-q Nqueries] [-r] [-s SRC_Addr] [-t TypeOfService] [-v] [-w WaitTime] Host [PacketSize]
```

O único parâmetro obrigatório para o comando traceroute é o nome ou o número IP do host destino. O tamanho do pacote UDP (UDP probe packet) é de 38 bytes, mas pode ser aumentado especificando o tamanho do pacote (em bytes) após o nome ou número IP do destino.

#### 2.3.1 Opções de comando

1. -m Max\_ttl

Especifica um "time-to-live" máximo (número máximo de hops) usado nos pacotes de pesquisa UDP. O default é 30 hops (o mesmo default utilizado para conexões TCP).

2. -n

Mostra o endereço IP de cada gateway encontrado no caminho (da origem ao destino).

3. -p Port

Especifica o número base da porta UDP utilizada na pesquisa do traceroute. O default é 33434. O comando traceroute depende de um intervalo de portas UDP abertas de "base a base + número de hops - 1" no host destino. Se uma porta UDP não está disponível, esta opção pode ser usada para pegar um intervalo de portas não utilizadas.

4. -q Nqueries

Especifica o número de pacotes UDP (UDP probes) que o comando traceroute envia a cada Max\_ttl. O default é três pacotes.

5. -r

Desvia das tabelas de roteamento e envia os pacotes de pesquisa diretamente a um host. Se este host não está na rede, um erro é retornado. Esta opção pode ser usada para "dar" um comando ping em um host local através de uma interface que não está registrada nas tabelas de roteamento.

6. -s SRC\_Addr

Usa o endereço especificado (SRC\_Addr) como o endereço de origem dos pacotes UDP enviados. Em hosts com mais de um endereço IP, a opção -s pode ser usada para forçar o endereço de origem a ser uma interface específica e não, necessariamente, aquela de onde o pacote foi enviado. Se o endereço IP especificado não for válido, um erro é retornado e nada é enviado.

7. -t TypeOfService

Atribui um valor entre 0 e 255 para a variável TypeOfService do pacote de pesquisa UDP. O default é 0 (zero). Esta opção pode ser utilizada para descobrir se diferentes tipos de serviços resultam em diferentes caminhos.

8. -v

Recebe pacotes diferentes de TIME-EXCEEDED e PORT-UNREACHABLE.

9. -w WaitTime

Especifica o tempo (em segundos) a esperar pela resposta a um pacote de pesquisa UDP. O default é 3 segundos.

10. Host

Especifica o host destino, pelo nome ou pelo seu número IP. Este parâmetro é obrigatório. PacketSize Especifica o tamanho (em bytes) do pacote UDP de pesquisa (probe). O default é 38 bytes.

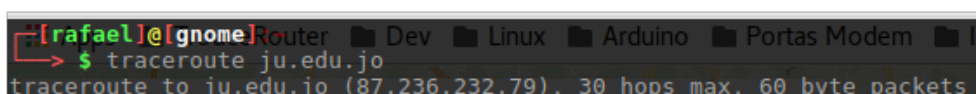
### 3 EXEMPLO DE ANÁLISE DE CUMUTAÇÃO DE REDE UTILIZANDO TRACEROUTE

A cumutação de pacotes que a Internet utiliza visa percorrer os melhores caminhos possíveis, sendo assim lentidões na rede ocasionada por diversos problemas, podem influenciar significativamente na rota dos pacotes, se possível consultar Kurrose 2010 para melhores exemplos, de problemas originadores de lentidões na rede. O exemplo dado nesse artigo tem como objetivo demonstrativo com intuito de analisar mensagens ICMP relatadas pelo Traceroute, e mapear essas mensagens utilizando os IPs disponíveis nas respostas das mensagens ICMPs, juntamente com auxílio da página [www.localizaip.com.br](http://www.localizaip.com.br), que nos fornece coordenadas geográficas, referente a endereços de IPs, com essas coordenadas (latitude e longitude) foi mapeado a rota utilizada, com auxílio do aplicativo Google Earth .

#### 3.0.1 Análise

Será utilizado um site do oriente médio para exemplificação com o nome de endereço `ju.edu.jo`, esse endereço é de uma página web hospedada na Jordânia. Com o comando padrão do traceroute (utilizando Linux e Mac, se for windows utilizar o comando `trace`), que é "`traceroute Host`"(substituindo o Host pelo endereço do alvo), começamos a encaminhar sondas encrementando progrecivamente o TLL (citado no tópico protocolos, em alguns casos não falaremos diretamente sobre o TLL, porém indiretamente considere que em cada pacote reenviado o valor do campo TLL e encrementado), assim começamos nossa sondagem pela rede até a máquina final.

1. Utilizando o traceroute mandamos três requisição para cada enlace até o endereço `ju.edu.jo` com 30 saltos no max, e pacotes de 60 byte em cada requisição que é de padrão quando não especificado no corpo do comando (para mais detalhes de comandos consultar a seção de Comandos do Traceroute) Figura 1.



```
[rafael]@[gnome]Router Dev Linux Arduino Portas Modem I
> $ traceroute ju.edu.jo
traceroute to ju.edu.jo (87.236.232.79), 30 hops max, 60 byte packets
```

Figura 1 – Início de comando traceroute com um hostname alvo

2. Na Figura 2 os três pacotes são enviados para o roteador de borda com endereço 192.168.1.1, situado na cidade de Coxim, e são respondidos em ordem pelo mesmo com tempo de RTT 0.756 ms, 0.957 ms, 1.129 ms sucessivamente.

```
1 TP-LINK.Home (192.168.1.1) 0.756 ms 0.957 ms 1.129 ms
```

Figura 2 – Pacotes são respondidos pelo roteador de borda

3. Na Figura 3 os pacotes encaminhados da borda da rede, chegam para o provedor de internet, em Brasília sendo respondidos pelo mesmo em ordem com o tempo de RTT 27.885 ms, 29.145 ms, 32.545 ms sucessivamente.

```
2 Oi-Lo10-cpce-ms-alk-01.brasiltelecom.net.br (201.10.196.83) 27.614 ms 29.804 ms 32.173 ms
```

Figura 3 – Pacotes são respondidos pelo provedor de Internet

4. Na Figura 4, o endereço do roteador do provedor nacional Brt-G0-0-0-2-cpce-ms-rotd-xr02.brasiltelecom.net.br, também em Brasília, recebe os pacotes com TTL zerado, forçando o envio de mensagens ICMP de volta com tempo de RTT de 37.990 ms, 37.994 ms, 41.575 ms sucessivamente.

```
3 BrT-G0-0-0-2-cpce-ms-rotd-xr02.brasiltelecom.net.br (200.199.193.135) 37.990 ms 37.994 ms 41.575 ms
```

Figura 4 – Pacotes sendo comutados pelos roteadores do provedor nacional

5. Na Figura 5, o endereço do roteador do provedor de internet nacional Brt-G0-0-2-cpce-ms-rotd-xr02.brasiltelecom.net.br, também em Brasília, recebe os pacotes com TTL zerado, forçando o envio de mensagens ICMP de volta com tempo de RTT foi 62.117 ms, 63.523 ms, 65.936 ms sucessivamente.

```
4 BrT-G5-0-2-etce-df-rotn-j01.brasiltelecom.net.br (200.199.193.159) 62.117 ms 63.523 ms 65.936 ms
```

Figura 5 – Pacotes sendo comutados pelos roteadores do provedor nacional

6. Figura 6, o traceroute não conseguiu resolver as rotas nos três pacotes enviados, perdendo os, sendo assim na próxima sondagem ele tentara uma outra rota.



Figura 6 – Pacotes perdidos

7. Figura 7, nessa parte dois pacotes são encaminhados para o roteador de endereço te-0-0-0-ETCE-DF-ROTB-01.brasiltelecom.net.br, esse roteador é nacional se encontra em Brasília, o mesmo visualiza o TTL zerado, dos pacotes retorna mensagens ICMP para o roteador inicial da requisição com tempo de 68.123 ms e 73.770 ms, e um pacote é encaminhado direto para o roteador do servidor Carrier-Grade NAT RFC6598 de endereço 100.120.64.14, Internacional situado no Oceano Atlântico, que por sua vez, visualiza o TTL zerado retornando uma mensagem ICMP para o roteador inicial, o RTT desse roteador é de 72.279 ms.

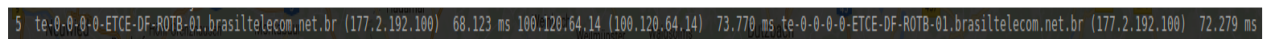


Figura 7 – Pacotes sendo comutados pelos roteadores do provedor nacional e internacional

8. Na Figura 8, os pacotes são comutados até o um provedor Carrier-Grade NAT RFC6598, localizado no Oceano Atlântico, com endereço de ip 100.122.17.130 o pacote encaminhado para esse endereço teve um tempo de RTT de 200.617 ms, já o outro pacote foi encaminhado para o mesmo servidor porém com o ip 100.122.17.148 teve um tempo de RTT de 179.446 ms.

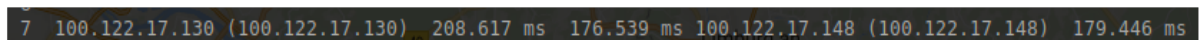


Figura 8 – Pacotes sendo comutados pelo servidor Internacional compartilhado Carrier-Grade NAT RFC6598, situado no Oceano Atlântico

9. Na Figura 9, assim como na Figura 8 os pacotes são enviados até o enlace de um conjunto de roteadores no Oceano Atlântico conhecido como Carrier-Grade NAT RFC6598, que é uma abordagem para o design da rede IPv4 em que os sites finais, em particular as redes residenciais, são configurados com endereços de rede privada que são convertidos para endereços IPv4 públicos por Dispositivos de rede de endereço de rede da middlebox incorporados na rede do operador de rede, permitindo o compartilhamento de pequenos pools de endereços públicos entre vários sites finais. Isso altera a função NAT e a sua configuração das instalações do cliente para a rede do provedor de serviços da Internet, por isso que a sonda do Traceroute encontra alguns endereços ips vinculado a esse provedor, o endereço de ip 100.122.17.149 com tempo de RTT de 191.133 ms, no endereço ip 100.122.17.171 com tempo de RTT de



180.897 e no endereço ip 100.122.17.167 com tempo de 171.525 ms.([KUARSINGH; CIANFARANI, 2014](#))

```
8 100.122.17.149 (100.122.17.149) 191.133 ms 100.122.17.171 (100.122.17.171) 180.897 ms 100.122.17.167 (100.122.17.167) 171.525 ms
```

Figura 9 – Pacotes sendo comutados pelo servidor Internacional compartilhado Carrier-Grade NAT RFC6598, situado no Oceano Atlântico.

10. Na Figura 10, os pacotes foram encaminhados para o endereço ae4-650.cr2-nyc6.ip4.gtt.net do provedor Internacional Tinet GmbH na cidade de New York nos United States, com RTT de 197.991 ms, 202.254 ms e 202.207 ms, sucessivamente.

```
9 ae4-650.cr2-nyc6.ip4.gtt.net (173.205.51.93) 197.991 ms 202.254 ms 202.207 ms
```

Figura 10 – Pacotes sendo cumutados até provedor Internacional Tinet GmbH na cidade de New York nos United States.

11. Na Figura 11, os pacotes foram encaminhados para o endereço ip 141.136.105.222, do provedor GTT Communications Inc, localizado na cidade de Frankfurt Am Main, na Germany, com RTT de 294.974 ms, 295.028 ms e 297.926 ms, sucessivamente.

```
10 et-9-1-0.cr0-mrs1.ip4.gtt.net (141.136.105.222) 294.974 ms 295.028 ms 297.926 ms
```

Figura 11 – Pacotes sendo cumutados até provedor Internacional, GTT Communications Inc, na cidade de Frankfurt Am Main, na Germany.

12. Na Figura 12, os pacotes foram encaminhados para o endereço ip 46.33.83.18, do provedor GTT Communications Inc , localizado na cidade de Isenburg, na Germany, com RTT de 334.051 ms, 336.230 ms e 339.446 ms, sucessivamente.

```
11 ip4.gtt.net (46.33.83.18) 334.051 ms 336.230 ms 339.446 ms
```

Figura 12 – Pacotes sendo cumutados até provedor Internacional, GTT Communications Inc, na cidade de Isenburg, na Germany.

13. Na Figura 13, os pacotes foram encaminhados para o endereço ip 213.139.41.2, do provedor Jordan Telecommunications Company, localizado na cidade de Amman, na Jordan, com RTT de 299.414 ms, 300.090 ms e 299.396 ms, sucessivamente.

```
12 213.139.41.2 (213.139.41.2) 299.414 ms 300.090 ms 299.396 ms
```

Figura 13 – Pacotes sendo cumutados até provedor Internacional, Jordan Telecommunications Company, na cidade de Amman, na Jordan.

14. Na Figura 14, os pacotes foram encaminhados para o endereço ip 213.139.32.206, do provedor Jordan Telecommunications Company, também localizado na cidade de Amman, na Jordan, com RTT de 310.995 ms, 311.614 ms e 311.892 ms, sucessivamente.

```
13 213.139.32.206 (213.139.32.206) 310.995 ms 311.614 ms 311.892 ms
```

Figura 14 – Pacotes sendo cumutados até provedor Internacional, Jordan Telecommunications Company, na cidade de Amman, na Jordan.

O ultimo salto realizados nos roteadores até a maquina final mostrado na Figura 14, mostra o funcionamento do traceroute, os outros 17 saltos restantes são descartados pelo traceroute, ja que não existe mais roteadores disponiveis para realizar a sondagem como podemos observar na Figura 15 .

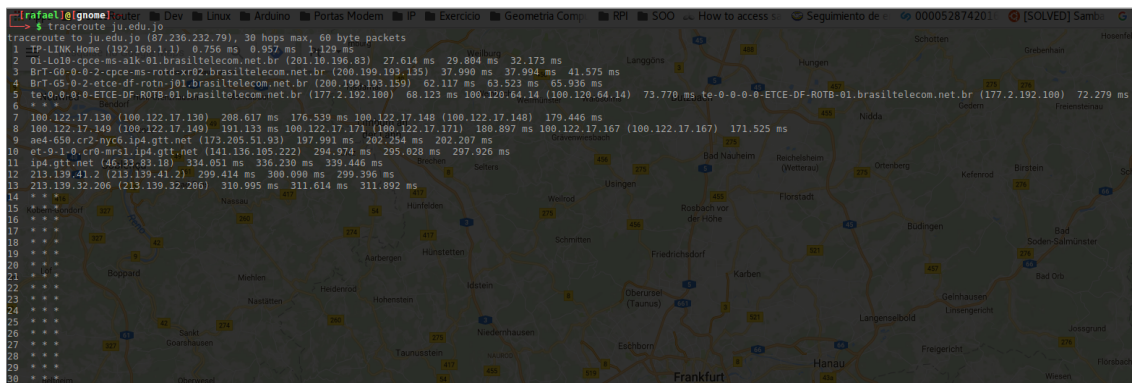


Figura 15 – Resultado final da sondagem utilizando o Traceroute.

### 3.0.2 Mapeamento utilizando Google Earth

Com base nos endereços IPs fornecido pelo Traceroute, foi descoberto as coordenadas geográficas dos IPs, pelo o site [www.localizaip.com.br](http://www.localizaip.com.br), com essas coordenadas foi

mapeado a apenas as rota Internacionais que os pacotes traferam, utilizando o Google Earth para fazer as marcações no Mapa Figura 16.

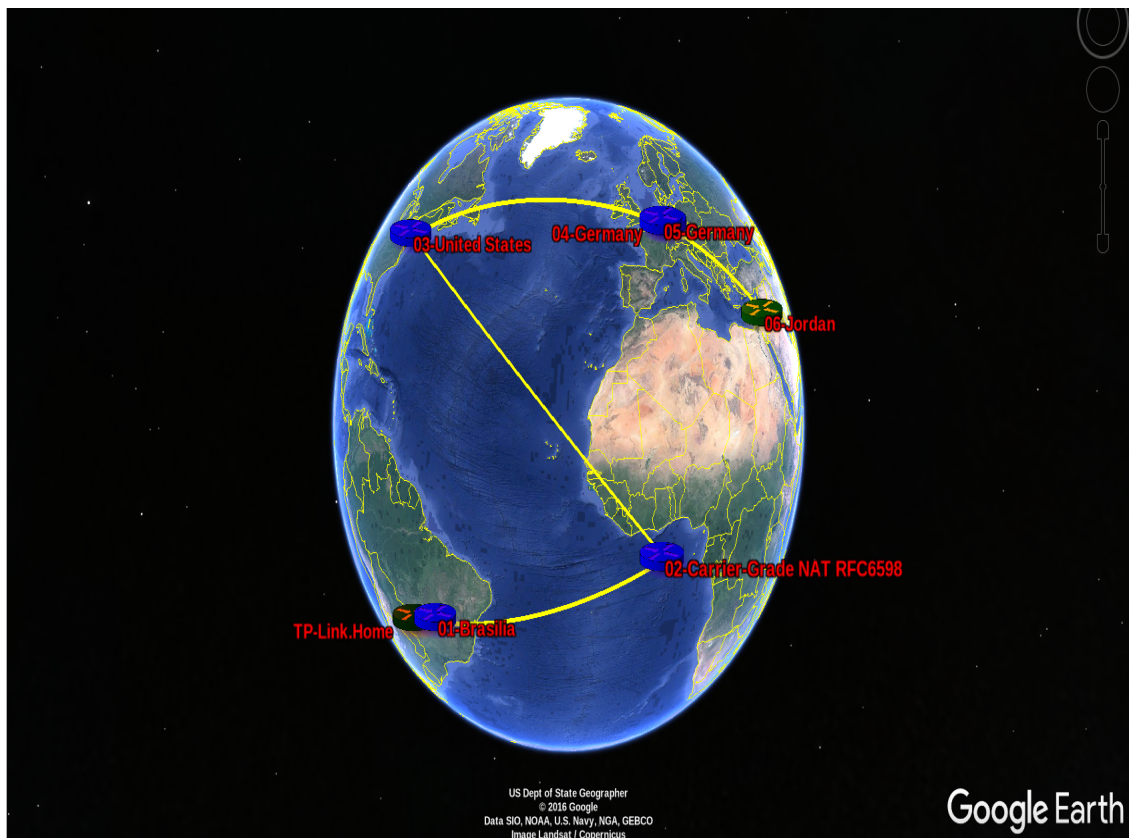


Figura 16 – Mapeamento das rotas Internacioais, até a Jordania apartir dos endereços de IPs fornecido pelo Traceroute.

Este modelo de artigo é limitado em número de exemplos de comandos.

## 4 CONSIDERAÇÕES FINAIS

Com a ferramenta Traceroute podemos analisar pacotes até seu destino, podendo assim observar por onde nossos pacotes estão passando, facilitando assim a apuração de possíveis problemas relacionados as rotas, que os pacotes tomam pela Internet, sendo possivel a analise de ponta-a-ponta de maquinas finais.

## Referências

DARREN, D. Protocol fundamentals - traceroute differences between windows and linux. Agost. 2010. Disponível em: <<https://mellowd.co.uk/ccie/?p=634>>. Acesso em: 01 jun. 2017. 4

FAQ, T. How unix and windows traceroutes differ. March. 2016. Disponível em: <http://www.tech-faq.com/how-unix-and-windows-traceroutes-differ.htmls>. Acesso em: 01 jun. 2017. 4

KUARSINGH, V. J.; CIANFARANI, J. *CARRIER-GRANDE NAT(CGN) DEPLOYMENT WITH BGP/MPLS IP VPNS*. [S.l.], 2014. 9

KUROSE, J. F.; ROSS, K. W. *REDES DE COMPUTADORES E A INTERNET UMA ABORDAGEM TOP-DOWN*. 5. ed. RUA NELSON FRANCISCO, 26, LIMÃO, SÃO PAULO: PERSON EDUCATION DO BRASIL, 2010. ISBN 978-85-88639-97-3. 2, 4

NASCIMENTO, M. B. D. Protocolo icmp, ping e traceroute. Out. 2016. Disponível em: <http://www.dltec.com.br/blog/cisco/protocolo-icmp-ping-e-traceroute/>. Acesso em: 01 jun. 2017. 3

REIS, F. dos. Curso de redes - como funciona o utilitario traceroute. Nov. 2015. Disponível em: <http://www.bosontreinamentos.com.br/redes-computadores/curso-de-redes-como-funciona-o-utilitario-traceroute>. Acesso em: 02 jun. 2017. 2