

# Ataque de Negação de Serviço DoS e Ataque de Negação de Serviço Distribuído DDoS

Rafael Gonçalves de Oliveira Viana

2017

## Resumo

Este artigo tem como objetivo uma apresentação do funcionamento de ataques de negação de serviço DoS(Denial-of-Service) e DDoS(Distributed Denial-of-Service) que nada mais é uma versão do ataque DoS porém distribuído.

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

## Introdução

A atual infra-estrutura de roteamento ainda é extremamente vulnerável a ataques de negação de serviço (Denial of Service - DoS). Tais ataques são caracterizados pelo completo desconhecimento da sua verdadeira origem ou não e visam tornar inacessíveis os serviços providos pela vítima. Este objetivo geralmente é alcançado através do envio de pacotes a uma taxa maior do que podem ser servidos pela vítima, fazendo com que legítimas requisições ao serviço não sejam atendidas. Em sua versão distribuída (Distributed DoS), os pacotes são enviados de diferentes origens e o tráfego agregado.

## 1 Funcionamento

Devido à técnica datagrama usada no protocolo IP, o anonimato do atacante é facilmente mantido, pois é possível injetar pacotes na rede com endereço de origem forjado. Em outras palavras, não existe uma entidade ou um mecanismo responsável pela verificação da autenticidade da fonte. Como toda infra-estrutura de roteamento é baseada exclusivamente no endereço de destino, pacotes com endereço de origem forjado geralmente alcançam a vítima sem dificuldades. Outra característica que permite a execução de ataques anônimos é a ausência de estado nos roteadores. Nenhuma informação relativa aos pacotes roteados é armazenada para consultas futuras. Em consequência, o encaminhamento de pacotes não deixa “rastros”, tornando impossível deduzir a rota percorrida por um pacote. A identificação da fonte também é dificultada caso ataques indiretos sejam empregados. Tais ataques são caracterizados pelo uso de estações intermediárias entre o atacante e a vítima, de forma a ocultar a sua verdadeira origem(LAUFER; VELLOSO; DUARTE, 2005)

## 2 Código Si/mplificado

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 (KUROSE; ROSS, 2010).

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	TTL expirado
12	0	cabeçalho IP inválido

## 2.1 UDP

O protocolo UDP, é definido pelo [RFC 768], faz parte os protocolos de transporte, e só faz apenas o que a camada de transporte pode fazer que é quase nada, faz a multiplexação/demultiplexação e algumas verificações de erros, ele nada adiciona ao IP. Na verdade, se o criador de aplicação escolher o UDP, e vez de TCP, a aplicação estará se comunicando quase diretamente com o IP. O UDP pega as mensagens do processo de aplicação, anexa o número de porta da fonte e do destino para o serviço de multiplexação/demultiplexação, adiciona dois outros pequenos campos e passa o segmento resultante à camada de rede, que encapsula o segmento em um datagrama IP e, em seguida, faz uma tentativa de melhor esforço para entregar o segmento ao hospedeiro receptor. Se o segmento chegar ao hospedeiro receptor, o UDP usará o número de porta de destino para entregar os dados do segmento ao processo de aplicação correto. Note que com o UDP, não há apresentação entre as entidades remetente e destinatária da camada de transporte antes de enviar um segmento. Por essa razão, dizemos que o UDP é não orientado para conexão.(KUROSE; ROSS, 2010)

## 3 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).

### 3.1 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 *n*ésimo datagrama chega ao *n*ésimo roteador, o *n*ésimo 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 Tabela 1. 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 volta "RTT ", da mensagem ICMP, o nome e o endereço IP do *n*ésimo 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 improvável, o hospedeiro de destino devolve à fonte uma mensagem ICMP indicando que porta não pôde ser alcançada(mensagem tipo 3, código 3 Tabela 1). Quando recebe essa mensagem ICMP particular, o hospedeiro da fonte sabe que não precisa enviar mais pacotes de sondagem (O programa Traceroute por padrão envia conjuntos de três pacotes com o mesmo TTL, assim, o Traceroute espera três resultados para cada TTL). 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 "RTT"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 TTL. Também tem de poder ser avisado por seu sistema operacional quando chegam mensagens ICMP.

### 3.2 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 (saltos). 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](#))

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 alta 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)

### 3.3 Comandos Traceroute

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.

#### 3.3.1 Opções de comando Linux Ubuntu/Debian

O exemplo de sintaxe de comando a seguir mostra todas as opções disponíveis:

**traceroute** [-m Max\_ttl] [-n] [-p Port] [-q Nqueries] [-r] [-s SRC\_Addr] [-t Type-OfService] [-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 60 bytes, mas pode ser aumentado especificando o tamanho do pacote (em bytes) após o nome ou número IP do destino.

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 60 bytes.

### 3.3.2 Opções de comando Windows

Há várias opções de linha de comando que podem ser usadas com o TRACERT, embora as opções geralmente não sejam necessárias para a solução de problema padrão.

O exemplo de sintaxe de comando a seguir mostra todas as opções disponíveis:

**tracert** [-d] [-h maximum\_hops] [-j host-list] [-w timeout] [target\_host]

O único parâmetro obrigatório para o comando tracert é o nome ou o número IP do host destino. O que os parâmetros fazem:

1. -d

Especifica que não devem ser resolvidos endereços para nomes de host.

2. -h maximum\_hops

Especifica o número máximo de saltos para procurar o destino.

3. -j host-list

Especifica a rota de origem livre ao longo da lista de hostst.

4. -w timeout

Espera o número de milissegundos especificado por tempo limite para cada. resposta

5. target\_host

Especifica o nome ou o endereço IP do host de destino.

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

## 4 Exemplo de análise de cumutação de rede utilizando Traceroute

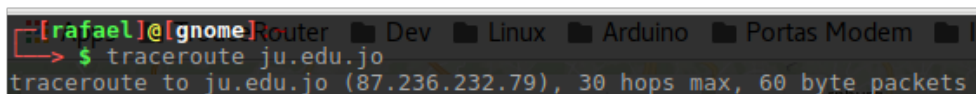
A cumutação de pacotes que a Internet utiliza visa percorrer os melhores caminhos possíveis, sendo assim lentidões na rede ocasionada por diversos problemas, podem influenciar significativamente na rota dos pacotes, se possível consultar (KUROSE; ROSS, 2010) para melhores exemplos, de problemas originadores 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 nelas, com o auxílio da página [www.localizaip.com.br](http://www.localizaip.com.br), que nos fornece coordenadas geográficas (essas coordenadas não são exatas, são informações disponíveis pelos provedores), referente aos endereços de IPs obtidos nas mensagens ICMP, com essas coordenadas (latitude e longitude) foi mapeado a rota(suposta rota), utilizada pelos pacotes, com auxílio do aplicativo Google Earth.

### 4.0.1 Análise

Será utilizado um site do oriente médio para exemplificação, com o nome de endereço "ju.edu.jo", esse endereço pertence a uma máquina hospedada na Jordânia. Com o comando padrão do Traceroute (utilizando Linux, 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 TTL (citado na seção ??, não falaremos diretamente sobre o TTL, porém considere indiretamente que, em cada salto o valor do campo TTL é incrementado pelo traceroute a cada salto), assim começamos nossa sondagem pela rede até a máquina hospedeira.

1. Utilizando o traceroute foi encaminhado três requisição para cada enlace de rede até a máquina hospedeira com endereço ju.edu.jo com 30 saltos no max, e pacotes de 60 byte em cada requisição que é de padrão (sistema Linux), quando não especificado no corpo do comando (para mais detalhes de comandos consultar a seção 3.3), 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 sondagem com um hospedeiro alvo.

2. Na Figura 2 os três pacotes são enviados para o roteador de borda(roteador que tem conexão com a WAN) com endereço 192.168.1.1, situado na cidade de Coxim, e são respondidos em ordem pelo mesmo com os tempos de RTT de 0.756 ms, 0.957 ms e 1.129 ms.



```
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.

- Na Figura 3 os pacotes encaminhados da borda da rede, chegam para o provedor de Internet nacional, na cidade Brasília, recebe o os pacotes com TTL zerado, forçando o envio de mensagens ICMP de volta para a máquina originadora da requisição com tempos de RTT de 27.885 ms, 29.145 ms e 32.545 ms.

```
2 0i-Lol0-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 nacional, na cidade de Brasília no Brasil.

- Na Figura 4, o endereço do roteador do provedor nacional 200.199.193.135, também na cidade de Brasília, recebe os pacotes com TTL zerado, forçando o envio de mensagens ICMP de volta para máquina originadora da requisição com tempos de RTT de 37.990 ms, 37.994 ms, 41.575 ms.

```
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, na cidade de Brasília no Brasil.

- Na Figura 5, o endereço do roteador do provedor nacional 200.199.193.159, também na cidade de Brasília, recebe os pacotes com TTL zerado, forçando o envio de mensagens ICMP de volta para a máquina originadora da requisição com tempos de RTT de 62.117 ms, 63.523 ms, 65.936 ms.

```
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.

- Figura 6, o traceroute não conseguiu resolver as rotas, nos três pacotes enviados, foram respondido mensagens ICMP de tipo 3 (citado na seção ?? ), sendo assim na próxima sondagem ele tentará uma outra rota se disponível.

```
6 * * * Bendorf
```

Figura 6 – Pacotes perdidos.

- Figura 7, nessa parte dois pacotes são encaminhados para o roteador de endereço 177.2.192.100, esse roteador é nacional se encontra na cidade de Brasília, o mesmo



visualiza o TTL zerado, dos pacotes e retorna mensagens ICMP para a máquina originadora da requisição com tempo de RTT 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, que por sua vez, visualiza o TTL zerado retornando uma mensagem ICMP para o máquina originadora da requisição, o RTT desse roteador é de 72.279 ms.

```
5 te-0-0-0-ETCE-DF-ROTB-01.brasilelecom.net.br (177.2.192.100) 68.123 ms 100.120.64.14 (100.120.64.14) 73.770 ms te-0-0-0-ETCE-DF-ROTB-01.brasilelecom.net.br (177.2.192.100) 72.279 ms
```

Figura 7 – Pacotes sendo comutados pelos roteadores do provedor nacional e provedor de compartilhamento IPv4 Carrier-Grade NAT RFC6598

8. Na Figura 8, os pacotes são comutados até o um provedor Carrier-Grade NAT RFC6598, 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.

```
7 100.122.17.130 (100.122.17.130) 208.617 ms 176.539 ms 100.122.17.148 (100.122.17.148) 179.446 ms
```

Figura 8 – Pacotes sendo comutados pelo servidor Internacional compartilhado IPv4 Carrier-Grade NAT RFC6598.

9. Na Figura 9, assim como na Figura 8 os pacotes são enviados até o enlace de um conjunto de roteadores 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 ea 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 (RFC, 2015).

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 RTT de 171.525 ms.

```
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 pelos servidores Internacionais compartilhados Carrier-Grade NAT RFC6598.

10. Na Figura 10, os pacotes foram encaminhados para o endereço 173.205.51.93 do provedor Internacional Tinet GmbH na cidade de New York nos United States, com tempos de RTT de 197.991 ms, 202.254 ms e 202.207 ms.

```
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 tempos de RTT de 294.974 ms, 295.028 ms e 297.926 ms..

```
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 tempos de RTT de 334.051 ms, 336.230 ms e 339.446 ms.

```
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.

```
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.

```
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 último salto realizados nos roteadores até a maquina hospedeira foi o de numero 13, mostrado na Figura 14, mostrando assim o funcionamento do traceroute, os outros 17 saltos restantes são descartados pelo traceroute (como citado na secção 3.1), já que não existe mais roteadores acessíveis disponiveis para dar continuidade a sondagem, Figura 15.

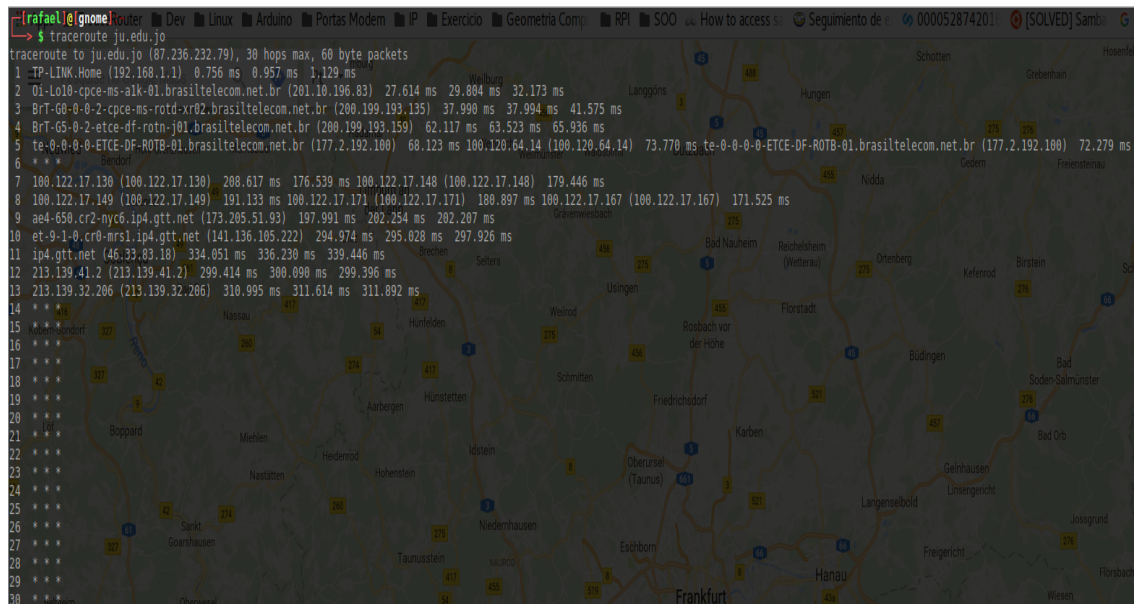


Figura 15 – Resultado final da sondagem utilizando o Traceroute.

#### 4.0.2 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) (contendo variações nas coordenadas), com essas coordenadas foi mapeado a apenas as rota Internacionais que os pacotes traferam na Internet (a coordenada que foi apresentada pelo [localizaip.com](http://localizaip.com) referente aos IPs dos roteadores Carrier-Grade NAT RFC6598 apontaram para as coordenadas Latitude=0.0 e Longitude=0.0, sendo assim a posição geográfica não corresponde com a posição real), utilizando o Google Earth para fazer as marcações no Mapa Gobl Figura 16.

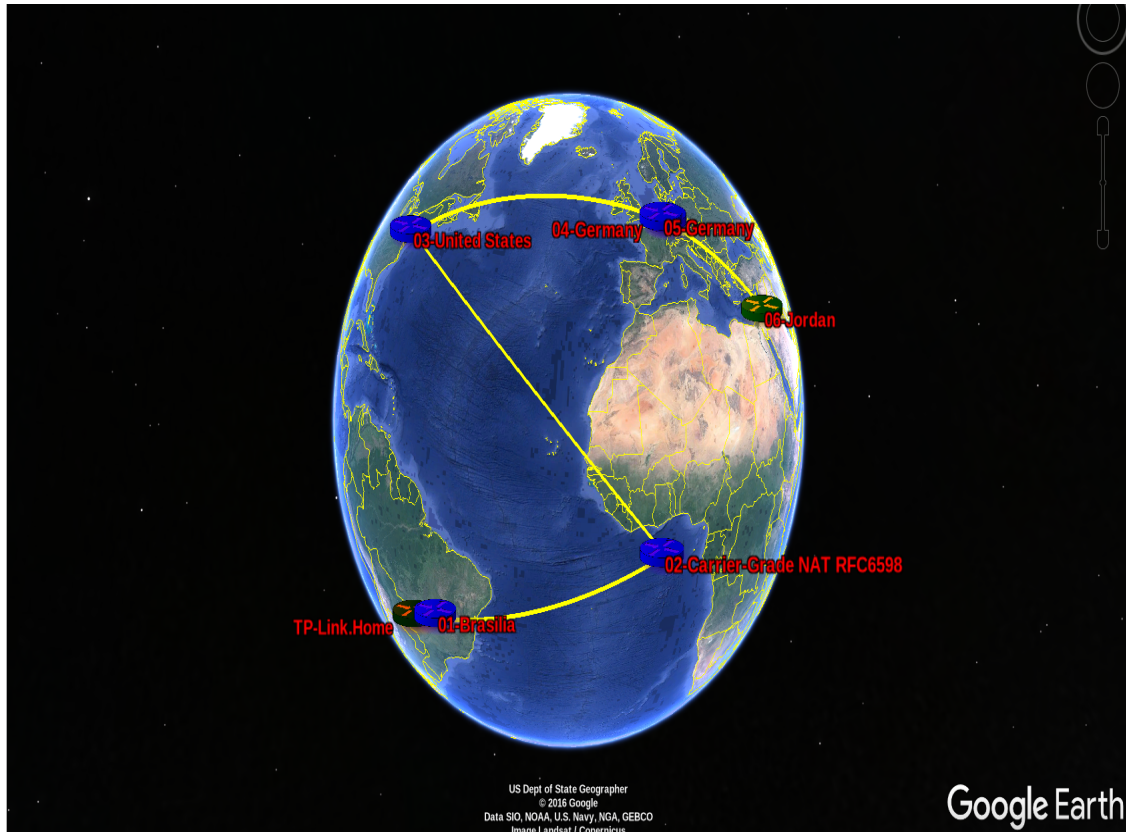


Figura 16 – Mapeamento das rotas Internacioais, até a Jordania apartir dos endereços de IPs fornecido pelo Traceroute.

## 5 Considerações finais

Com a ferramente Traceroute podemos análisar o percurso dos pacotes até seu destino, podendo assim observar por onde nossos pacotes estão passando (sendo cumutados pela rede), melhorando a apuração de possíveis problemas (firewalls, congestionamentos na rede, entre outros), entre a máquina remetente e a máquina destinatária, sendo possível, a análise por meio de respostas ICMP (citado na ??) provocadas propositalmente pelos campos TTL zerados (citado na secção ??) ou por portas altas não acessível, saltando pelos roteadores do núcleo da rede um-a-um até a máquina hospedeira.

## 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. 5
- 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
- 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, 3, 4, 7
- LAUFER, R. P.; VELLOSO, P. B.; DUARTE, O. Um novo sistema de rastreamento de pacotes ip contra ataques de negação de serviço. In: *XXIII Simpósio Brasileiro de Redes de Computadores-SBRC'2005*. [S.l.: s.n.], 2005. 1
- 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. 2
- RFC datatracker. Iana-reserved ipv4 prefix for shared address space, carrier-grade nat rfc6598. Oust. 2015. Disponível em: <<https://datatracker.ietf.org/doc/rfc6598/>>. Acesso em: 02 jun. 2017. 9