

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: Roteamento, IP, UDP, TCP SYN, Ping.

Introdução

A Internet é uma agregação grande e complexa de hardware de rede, conectada entre eles 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 porém, será levantado protocolos que o traceroute utiliza para seu funcionamento porém muito breve.

1 Protocolos

1.1 IPv4

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 é campo de oito bits, o TTL (time to live, ou seja, tempo para viver) ajuda a prevenir que os datagramas persistam (ex. andando aos círculos) numa rede. Historicamente, 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) é um protocolo que permite gerenciar as informações relativas aos erros nas máquinas conectadas. Devido aos poucos controles que o protocolo IP realiza, ele não corrige estes erros mas os mostra para os protocolos das camadas vizinhas. Assim, o protocolo ICMP é usado por todos os roteadores para assinalar um erro, chamado de Delivery Problem ou, em português, Problema de Entrega.

O ICMP é um protocolo integrante do Protocolo IP, definido pela RFC 792, e utilizado para fornecer relatórios de erros ao host que deu origem aos pacotes enviados na rede. Qualquer computador que utilize o protocolo IP precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado.

Os gateways (roteadores) devem também estar programados para enviar mensagens ICMP quando receberem pacotes que provoquem algum tipo de erro ou detectarem algum problema listado no protocolo ICMP. O ICMP é transportado no campo de dados do pacote IP e identificado como tipo de protocolo “1” pelo cabeçalho do IP.

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 ou código.([NASCIMENTO, 2016](#))

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. Toda vez que um datagrama chega a um roteador, 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 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)

2.2 Comandos Traceroute

SINTAXE

```
traceroute [-m Max_ttl] [-n] [-p Port] [-q Nqueries] [-r] [-s SRC_Addr] [-t TypeOf-Service] [-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.

2.2.1 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.

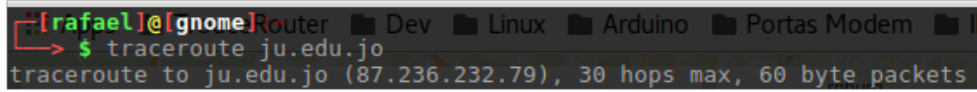
3 Exemplo de reconhecimento de cumutação de rede utilizando Traceroute

A cumutação de pacotes que a Internet utiliza visa percorrer os melhores caminhos possíveis, sendo assim lentidão na rede ocasionada por diversos problemas, se possível consultar Kurrose 2010 para melhores exemplos, de problemas originadores de lentidão 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 do ICMP, juntamente com auxilio da página www.localizaip.com.br, que nos fornece posições geograficas, referente a endereços de ips, com essas informações geograficas (latitude e longitude) foi mapeado a rota utilizada, com auxilio do aplicativo Google Earth .

3.0.1 Reconhecimento

Será utilizado um site do oriente médio para exemplificação com o nome de endereço ju.edu.jo, esse endereço é de uma pagina web hospedada na Jordânia. Com o comando padrão do Traceroute (em caso de linux, caso do seu sistema for windows utilizar trace, o restante é igual), que é "traceroute Host", começamos a encaminhar sondas encrementando progrecivamente o TLL (citado no tópico protocolos), assim começamos nossa sondagem pela rede ate a maquina final.

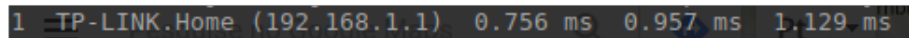
1. Utilizando o traceroute mandamos três requisição para cada enlace até o endereço ju.edu.jo com 30 saltos no max, e pacotes de 60 byte em cada requisição que é de padrão quando não especificado no corpo do comando (para mais detalhes de comandos consultar a secção de Comandos do Traceroute) Figura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

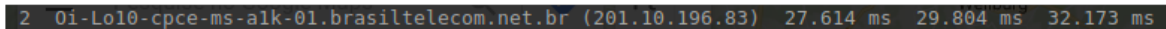
2. Na Figura 2 os três pacotes são enviados para o roteador de borda com endereço 192.168.1.1, situado na cidade de Coxim, e são respondidos em ordem pelo mesmo com tempo de RTT 0.756 ms, 0.957 ms, 1.129 ms sucessivamente.



```
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

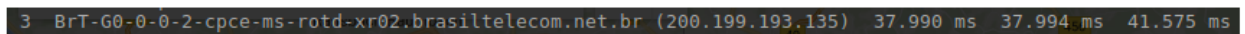
3. Na Figura 3 os pacotes encaminhados da borda da rede, chegam para o provedor de internet, em Brasilia sendo respondidos pelo mesmo em ordem com o tempo de RTT 27.885 ms, 29.145 ms, 32.545 ms sucessivamente.



```
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-rot-d-xr02.brasiltelecom.net.br, também em Brasilia, recebe o os pacotes com TLL 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-rot-d-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-rot-d-xr02.brasiltelecom.net.br, também em Brasilia, recebe o os pacotes com TLL 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. Na Figura 6, 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.

```
5 te-0-0-0-ETCE-DF-ROTB-01.brasiltelecom.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.brasiltelecom.net.br (177.2.192.100) 72.279 ms
```

Figura 6 – Pacotes sendo comutados pelos roteadores do provedor nacional e internacional

7. Na Figura 7 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 pacote 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) 200.617 ms 176.539 ms 100.122.17.148 (100.122.17.148) 179.446 ms
```

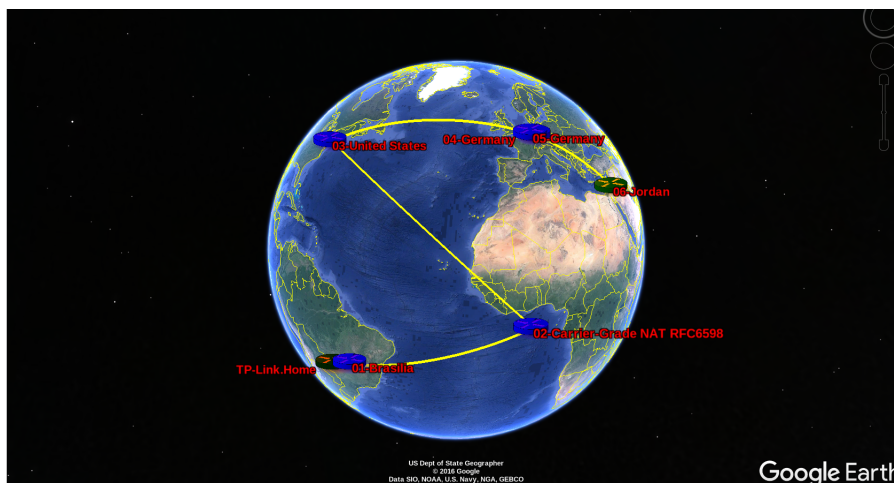
Figura 7 – Pacotes sendo comutados pelo servidor Internacional Carrier-Grade NAT RFC6598 situado no Oceano Atlântico



3.0.2 Levantamento de rotas

3.0.3 Mapeamento Utilizando Google Eart

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



4 Considerações finais

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Referências

NASCIMENTO, M. B. do. 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. Citado na página 2.

REIS, F. dos. Protocolo icmp, ping e traceroute. Nov. 2015. Disponível em: <http://www.bosontreinamentos.com.br/redes-computadores>. Acesso em: 02 jun. 2017. Citado 2 vezes nas páginas 2 e 3.