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 abortagem ao seus protrocolo 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 abortando o Trouceroute porém, será levantado protolocos que o trouceroute 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.

Ente 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 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:

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”.

O roteador não consegue retransmitir os pacotes na frequência adequada, ou seja, o roteador está congestionado (mensagem “source quench”).

O roteador indica uma rota melhor para o host que está enviando pacotes (mensagem de redirecionamento de rota ou “redirect”).

Quando um host de destino ou rota não está alcançável (mensagem “destination unreachable” ou destino inalcançável).

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)

1.3 Recuo do ambiente

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 Recuo do ambiente

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

3 Mais exemplos no Modelo Canônico de Trabalhos Acadêmicos

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

4 Consulte o manual da classe abntex2

Considerações finais

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer 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 na página 2.