ARTIGO TRACEROUTE

Rafael Gonçalves de Oliveira Viana[1]

Resumo: 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.

Palavras-chave: Roteamento, IP, UDP ,TCP SYN, Ping.

1 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.

2 DESENVOLVIMENTO

2.1 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.(**??**)

[1] UFMS, rafaelgov95@gmail.com

2.2 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.

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

4 CONSIDERAÇÕES FINAIS

Considerações finais considerações finais considerações finais considerações finais considerações finais considerações finais considerações finais.

REFERÊNCIAS BIBLIOGRÁFICAS

TANEBAUM, A. S. **Sistemas Operacionais Modernos**. 3. ed. São Paulo: Pearlson Prentice Hall, 2010. 638 p.