11

4 - Traceroute

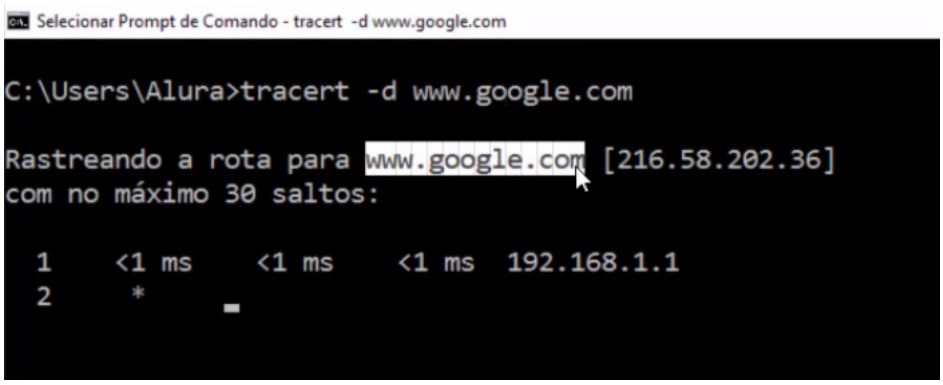
Transcrição

No teste do ping, vimos que a conectividade com a máquina do Google foi estabelecida com sucesso. Se sabemos que passamos por várias máquinas intermediarias, será que existe alguma forma de verificar qual é a rota que a informação está fazendo, saindo do meu computador passando pelas máquinas intermediárias até chegar a máquina do Google? Existe, esta é uma ferramenta administrativa chamada *Traceroute*. Dentro dela, assim como no ping, teremos um protocolo chama de ICMP, que fará essas verificações para saber quais são as máquinas intermediárias que participam do processo.

Para usá-la, no Windows nós digitaremos na linha de comando (no Linux considerar traceroute -n):

```
C:\Users\Alura>tracert -d www.google.com
```

Usamos o `-d` (`-n` no Linux) para que ele não faça a tradução DNS.



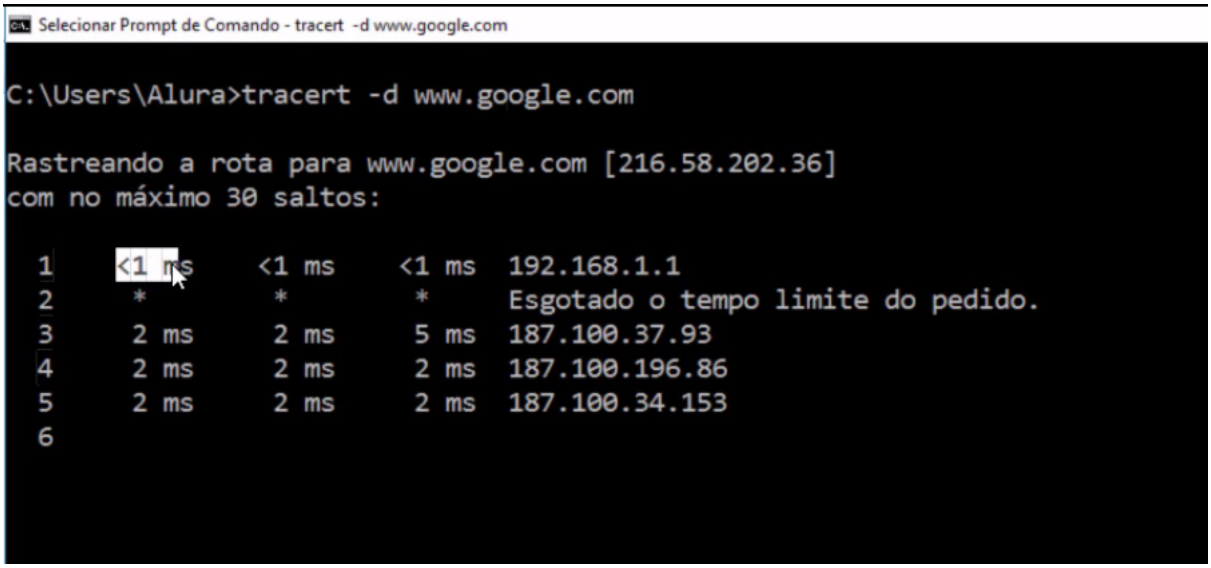
(1:21) - Observe que ocorreu a mesma tradução que foi feita no ping, por meio do servidor DNS que transformou o `www.google.com` para o endereçamento IP da máquina do Google. Mas as informações retornadas, foram diferentes.

```
C:\Users\Alura>tracert -d www.google.com

Rastreando a rota para www.google.com [216.58.202.36]
com no máximo 30 saltos:

1   <1 ms    <1 ms    192.168.1.1
2    *             *
```

Na primeira coluna, teremos o número de identificação da máquina por onde passou a informação da minha máquina. Ela foi a primeira a participar no processo de envio de dados. Mas a informação ainda passará por outras máquinas.



(02:33) - Mas observe os três intervalos de tempo que são mostrados nas outras colunas. Eles são os mesmos do ping e se referem ao processo de envio da minha máquina até o servidor do Google e de volta. Por que recebemos três informações?

(02:51) - Vamos pensar um exemplo do mundo real. Quando saímos do trabalho e vamos para a casa, temos a ideia de pegar uma rota específica. Mas pode ser que o caminho esteja congestionado e eu seja obrigado a buscar uma rota alternativa. Na rede, pode ocorrer o mesmo. Podemos enviar um pacote com informações, mas pode ser que no segundo seguinte, seja necessário buscar uma nova rota para chegar no site do Google. Para identificar se será necessário enviar uma rota diferente, três pacotes diferentes em intervalos diferentes são enviados para ver se alguma outra máquina poderia atuar como um ponto de parada.

(04:13) - Na primeira coluna, percebemos que quem recebeu os três pacotes foi o mesmo IP, ou seja, todos foram enviados pela mesma rota. Mas a máquina 2 não retornou nenhuma informação de tempo de retorno. Isso provavelmente aconteceu por dois motivos: o administrador pode ter desabilitado a resposta do ICMP da máquina, para evitar a sobrecarga de tráfego e por questões de segurança. Este teste que estamos realizando com a conectividade, pode ser um processo inicial de um teste de invasão de redes, que começa pela verificação de qual é o sistema que a empresa está trabalhando, quais as possíveis portas que estão abertas para conseguir o acesso. Para evitar esse tipo de problema de invasão, alguns provedores desabilita a resposta do ICMP. Mas ele está funcionando, tanto que ele passou a informação para a máquina número 3 que continuou passando para a próxima. Até chegar na décima máquina, que é o servidor do Google:

```
10   117 ms    117 ms  116 ms  216.58.202.36
```

Existiram várias passagens intermediárias da informação até finalmente chegarmos na máquina do Google.