

Funcionamento e uso do Ping

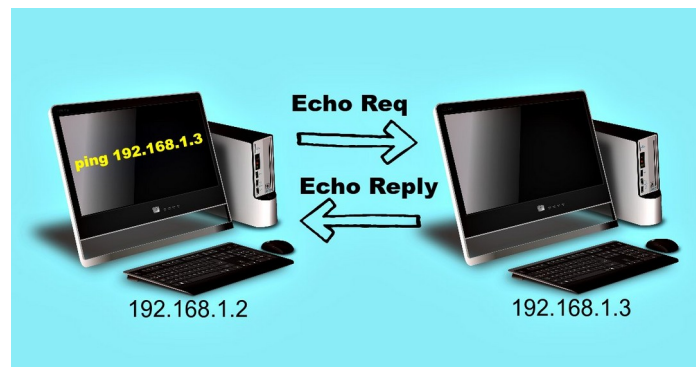
O Ping é baseado em duas mensagens, o echo request e echo reply.

Quando você entra no prompt de comandos do Windows e, por exemplo, digita “ping www.dltec.com.br”, na realidade seu computador está enviando mensagens de “echo request” ao servidor onde a página da DlteC está hospedada.

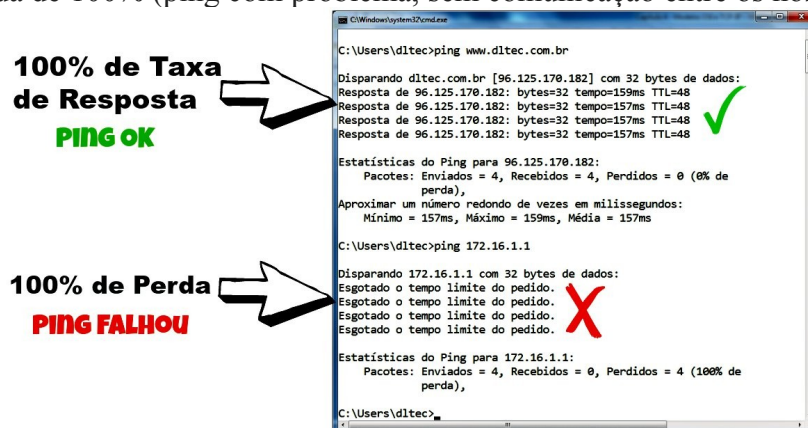
Ao receber essa mensagem de “echo request” nosso servidor responde seu computador com um “echo reply”.

Caso o servidor não responda seu computador indicará um timeout (tempo de resposta expirado), indicando que não houve resposta.

Veja na figura abaixo um exemplo de ping enviado do host com endereço IP 192.168.1.2 para o host com o IP 192.168.1.3.



Veja um exemplo de teste de ping no Windows com taxa de resposta de 100% (ping bem sucedido) e depois com perda de 100% (ping com problema, sem comunicação entre os hosts).



O teste de ping é utilizado para verificar se há comunicação fim a fim, ou seja, entre origem e destino.

Esse teste é realizado na camada-3 do modelo OSI (ou Internet do TCP/IP) e não se importa com os dispositivos (roteadores e switches) que estão no meio do caminho.

Vale a pena lembrar que as mensagens de ping podem ser bloqueadas por firewalls e/ou IPS's (Intrusion Prevention System), portanto nem sempre não obter uma resposta a um ping significa necessariamente um erro, pode ser que esse teste esteja bloqueado por motivos de segurança.

O comando ping básico é o mesmo em maioria dos sistemas operacionais.

Portanto, se você digitar “ping www.google.com” no Windows, Cisco IOS, MAC OS, Linux ou Unix ele vai funcionar.

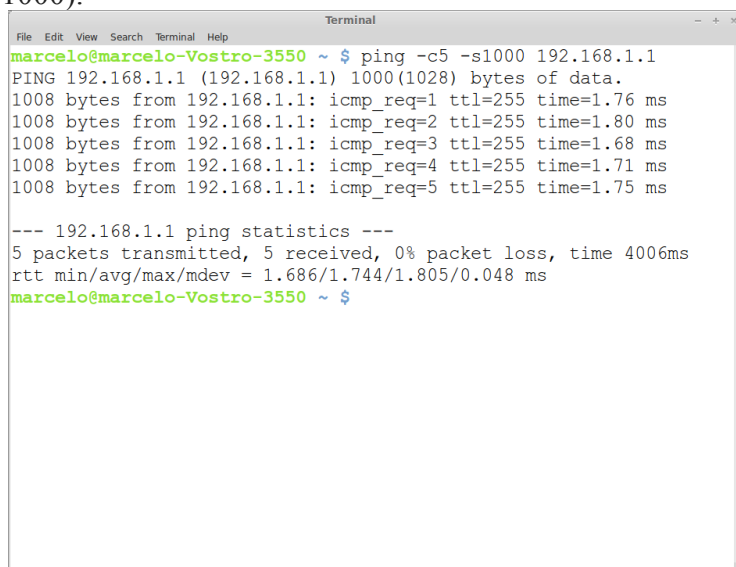
Um detalhe interessante é que se você digitar apenas o ping e o endereço IP ou URL no Linux ele dispara echos request até que você interrompa o teste.

Já no Windows serão disparados apenas quatro requests, sendo que para o Windows disparar pings sem como no Linux você precisa utilizar a opção “-t”, por exemplo, “ping -t 192.168.1.10”.

Outra opção bastante utilizada com o ping é alterar o tamanho do pacote para o máximo que o segmento testado suporta, por exemplo, 1500 bytes em uma rede LAN.

Para isso no Windows você pode utilizar a opção “-l 1500” e no Linux “-s 1500”.

Veja exemplo na tela abaixo onde no linux serão disparados 5 requests (opção -c5) com tamanho de 1000 bytes (opção -s1000).

A screenshot of a Linux terminal window titled "Terminal". The prompt is "marcelo@marcelo-Vostro-3550 ~". The user has entered the command "ping -c5 -s1000 192.168.1.1". The output shows five successful ping requests, each with 1008 bytes of data and a response time between 1.68 ms and 1.80 ms. Below the individual requests, a summary line shows "5 packets transmitted, 5 received, 0% packet loss, time 4006ms" and "rtt min/avg/max/mdev = 1.686/1.744/1.805/0.048 ms". The prompt returns to "marcelo@marcelo-Vostro-3550 ~".

```
marcelo@marcelo-Vostro-3550 ~ $ ping -c5 -s1000 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 1000(1028) bytes of data.
1008 bytes from 192.168.1.1: icmp_req=1 ttl=255 time=1.76 ms
1008 bytes from 192.168.1.1: icmp_req=2 ttl=255 time=1.80 ms
1008 bytes from 192.168.1.1: icmp_req=3 ttl=255 time=1.68 ms
1008 bytes from 192.168.1.1: icmp_req=4 ttl=255 time=1.71 ms
1008 bytes from 192.168.1.1: icmp_req=5 ttl=255 time=1.75 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.686/1.744/1.805/0.048 ms
marcelo@marcelo-Vostro-3550 ~ $
```

Funcionamento e uso do Traceroute

Já o trace ou traceroute tem a função de testar o caminho que o pacote está seguindo até seu destino, ou seja, ele é um teste ponto a ponto.

O traceroute está baseado no funcionamento do campo TTL do protocolo IP (Time to Live ou Tempo de Vida), sendo que o tempo de vida de um pacote é um contador que é decrementado a cada salto ou nó que o pacote IP passa.

Cada sistema operacional define um TTL para seus pacotes, em roteadores Cisco o TTL é definido com o valor de 255. Abaixo seguem os valores padrões de TTL para os sistemas operacionais mais comuns:

UNIX: 255

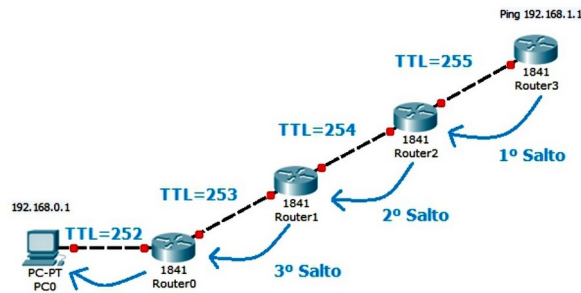
Linux: 64

Linux: 255

Windows: 128

Cisco: 255

Por exemplo, quando um roteador Cisco origina um pacote ele coloca o tempo de vida como 255 e a cada roteador que esse pacote passar será decrementado em 1, ou seja, se o caminho entre o originador do pacote e o destino existirem 3 roteadores quando o pacote chegar ao destino ele terá o valor de TTL 252.



Analisando a figura acima se um pacote IP trafegar por um número de saltos muito grande ele tem seu tempo de vida expirado o roteador que recebeu o pacote com TTL igual a zero deve enviar uma mensagem à origem do pacote com uma mensagem ICMP indicando esse problema.

Nessa mensagem vem o IP do roteador e com isso o computador consegue saber por onde o problema ocorreu.

Portanto, podemos utilizar essa característica para determinar o caminho que o pacote está passando entre a origem e o destino, para isso o host onde foi originado o traceroute manda um pacote com TTL igual a 1, no primeiro salto o pacote expira e o roteador responde com seu IP.

Depois envia um pacote com TTL igual a 2, aí ele conhece o roteador que está no segundo salto, sendo que esse processo se repete até que o pacote atinja seu destino e o caminho é traçado.

Na tela da figura abaixo você vai ver um exemplo do “tracert” que é o comando do Windows para o “traceroute” (Cisco, Unix e Linux).

```
C:\Windows\system32\cmd.exe
C:\Users\dltec>tracert www.dltec.com.br

Rastreando a rota para dltec.com.br [96.125.170.182]
com no máximo 30 saltos:

 1  2 ms  2 ms  2 ms  192.168.1.1
 2  2 ms  2 ms  2 ms  192.168.1.1
 3  11 ms  9 ms  9 ms  gvt-10.b3.cta.gvt.net.br [177.42.96.1]
 4  11 ms  9 ms  9 ms  177.99.179.static.host.gvt.net.br [177.99.179.129]
 5  13 ms  15 ms  14 ms  gvt-te-0-2-4-0-rc01.cta.gvt.net.br [187.115.212.26]
 6  12 ms  11 ms  15 ms  gvt-te-0-5-0-0-rc03.cta.gvt.net.br [189.59.247.206]
 7  19 ms  37 ms  22 ms  187.115.214.233.static.host.gvt.net.br [187.115.214.233]
 8  24 ms  23 ms  23 ms  gvt-te-0-0-0-4-rt02.spo.gvt.net.br [187.115.214.194]
 9  171 ms  179 ms  184 ms  Xe0-1-1-0-grtsaosi2.red.telefonica-wholesale.net [84.16.10.201]
10  191 ms  285 ms  226 ms  176.52.249.197
11  171 ms  165 ms  163 ms  Xe2-0-0-0-grtmiana2.red.telefonica-wholesale.net [94.142.118.250]
12  174 ms  186 ms  181 ms  softlayer-AE-0-0-grtmiana2.red.telefonica-wholesale.net [213.140.51.19
0]
13  128 ms  129 ms  171 ms  ae7.bbr01.tn01.mia01.networklayer.com [173.192.18.174]
14  152 ms  154 ms  153 ms  ae1.bbr01.sr02.hou02.networklayer.com [173.192.18.162]
15  157 ms  200 ms  158 ms  ae3.bbr01.eq01.dal03.networklayer.com [173.192.18.218]
16  158 ms  159 ms  159 ms  ae5.dar01.sr01.dal07.networklayer.com [173.192.18.179]
17  159 ms  159 ms  162 ms  pol.fcr01.sr01.dal07.networklayer.com [50.22.118.131]
18  * * *
    Esgotado o tempo limite do pedido.
19  157 ms  159 ms  159 ms  web.dltec.com.br [96.125.170.182]

Rastreamento concluído.
```

Note que no décimo oitavo salto o computador não obteve resposta, pois provavelmente existe um bloqueio por motivos de segurança nesse roteador.

Para alcançar o destino nosso pacote teve que percorrer 19 saltos, ou seja, passou por 19 roteadores entre a origem e o destino.

Disponível em: <https://www.dltec.com.br/blog/cisco/protocolo-icmp-ping-e-traceroute/>