



Davi Ventura C. Perdigão - 82148

Packet Internet Grouper é uma funcionalidade nativa do SO que tem por objetivo verificar a conectividade entre dois equipamentos em uma rede IP. Na sua execução, emprega mensagens do protocolo ICMP (Internet Control Message) para determinar se o equipamento está ativo ou inativo. Envia uma mensagem do tipo echo “ECHO REQUEST” para um equipamento de destino e aguarda a resposta do echo do tipo “ECHO REPLY”. O intervalo entre os dois eventos é chamada de *round trip time* (rtt). Se a resposta não chegar até o final do intervalo, assume-se que expirou. A expiração está relacionada com o Time to Live (ttl) que é decrementado em cada máquina em que o pacote é processado.

Prática

Configure no Virtual Box duas Máquinas Virtuais com o sistema operacional debian mínimo (<https://www.debian.org/CD/netinst/>). Mantenha a rede local como padrão vinda do virtual box em modo NAT. Execute os comandos ‘ip link show’ e ‘ip show address’ para identificar o endereço lógico de rede e endereço físico MAC da placa de rede (Geralmente segue o padrão “ens”). Como mostra as figuras 1 e 2.

```
rca_dri@vm-wordpress-hmg-02:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether c2:f0:c3:d5:7f:d3 brd ff:ff:ff:ff:ff:ff
rca_dri@vm-wordpress-hmg-02:~$
```

Figura 01: Endereço físico

```
rca_dri@vm-wordpress-hmg-02:~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether c2:f0:c3:d5:7f:d3 brd ff:ff:ff:ff:ff:ff
    inet 200.131.9.63/24 brd 200.131.3.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::c0f0:c3ff:fed5:7fd3/64 scope link
        valid_lft forever preferred_lft forever
rca_dri@vm-wordpress-hmg-02:~$
```

Figura 02: Endereço lógico

01) Execute o ping entre as duas máquinas virtuais e informe o rtt min/avg/max/max/mdev.

```
C:\Users\davi.perdigao>ping 192.168.0.101

Disparando 192.168.0.101 com 32 bytes de dados:
Resposta de 192.168.0.101: bytes=32 tempo=2ms TTL=64
Resposta de 192.168.0.101: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.0.101: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.0.101: bytes=32 tempo=1ms TTL=64

Estatísticas do Ping para 192.168.0.101:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
    Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 1ms. Máximo = 2ms. Média = 1ms
```

02) Instale o pacote arping e encontre as diretivas de tempo da questão 01.

```
C:\Users\davi.perdigao>arp -a

Interface: 192.168.0.107 --- 0xc
Endereço IP      Endereço físico    Tipo
192.168.0.1      68-ff-7b-76-e0-8e  dinâmico
192.168.0.100    d0-9c-7a-ec-a4-35  dinâmico
192.168.0.101    a4-77-33-9b-87-7a  dinâmico
192.168.0.103    00-b8-b6-3c-c7-a5  dinâmico
192.168.0.105    24-05-0f-d9-7b-c1  dinâmico
192.168.0.112    f0-86-20-da-6a-c2  dinâmico
192.168.0.255    ff-ff-ff-ff-ff-ff  estático
224.0.0.22       01-00-5e-00-00-16  estático
224.0.0.251      01-00-5e-00-00-fb  estático
224.0.0.252      01-00-5e-00-00-fc  estático
239.255.102.18   01-00-5e-7f-66-12  estático
239.255.255.250  01-00-5e-7f-ff-fa  estático
255.255.255.255  ff-ff-ff-ff-ff-ff  estático
```

03) Encontre as diretivas de tempo da questão 01 para os sites www.ufmg.br, www.uit.br e www.harvard.edu.

```
C:\Users\davi.perdigao>ping www.uit.br

Disparando uit.br [186.202.153.93] com 32 bytes de dados:
Resposta de 186.202.153.93: bytes=32 tempo=12ms TTL=55
Resposta de 186.202.153.93: bytes=32 tempo=12ms TTL=55
Resposta de 186.202.153.93: bytes=32 tempo=13ms TTL=55
Resposta de 186.202.153.93: bytes=32 tempo=13ms TTL=55

Estatísticas do Ping para 186.202.153.93:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 12ms, Máximo = 13ms, Média = 12ms
```

```
C:\Users\davi.perdigao>ping www.ufmg.br

Disparando www.ufmg.br [150.164.250.1] com 32 bytes de dados:
Resposta de 150.164.250.1: bytes=32 tempo=5ms TTL=54
Resposta de 150.164.250.1: bytes=32 tempo=3ms TTL=54
Resposta de 150.164.250.1: bytes=32 tempo=7ms TTL=54
Resposta de 150.164.250.1: bytes=32 tempo=3ms TTL=54

Estatísticas do Ping para 150.164.250.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 3ms, Máximo = 7ms, Média = 4ms
```

```

C:\Users\davi.perdigao>www.harvard.edu

Disparando pantheon-systems.map.fastly.net [199.232.114.133] com 32 bytes de dados:
Resposta de 199.232.114.133: bytes=32 tempo=8ms TTL=60
Resposta de 199.232.114.133: bytes=32 tempo=8ms TTL=60
Resposta de 199.232.114.133: bytes=32 tempo=8ms TTL=60
Resposta de 199.232.114.133: bytes=32 tempo=8ms TTL=60

Estatísticas do Ping para 199.232.114.133:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 8ms, Máximo = 8ms, Média = 8ms

```

04) Explique o motivo das diferenças de tempo encontradas entre a questão 01 e questão 03.

Na questão 1, os IP's foram buscados da minha propria rede local, por isso, o trajeto do pacote é menor comparado com os pacotes da questão 3.

05) Altere o tamanho do pacote icmp para 16000 bytes e veja como ficou a saída para os endereços das questões anteriores.

```

C:\Windows\System32>ping -s 4 192.168.0.101

Disparando 192.168.0.101 com 32 bytes de dados:
Resposta de 192.168.0.101: bytes=32 tempo=1ms TTL=64
  Carimbo de data/hora: 192.168.0.101 : 69176072 ->
    192.168.0.101 : 69176072 ->
    192.168.0.107 : 69267793
Resposta de 192.168.0.101: bytes=32 tempo=1ms TTL=64
  Carimbo de data/hora: 192.168.0.101 : 69177084 ->
    192.168.0.101 : 69177084 ->
    192.168.0.107 : 69268804
Resposta de 192.168.0.101: bytes=32 tempo=25ms TTL=64
  Carimbo de data/hora: 192.168.0.101 : 69178127 ->
    192.168.0.101 : 69178127 ->
    192.168.0.107 : 69269847
Resposta de 192.168.0.101: bytes=32 tempo=1ms TTL=64
  Carimbo de data/hora: 192.168.0.101 : 69179121 ->
    192.168.0.101 : 69179121 ->
    192.168.0.107 : 69270841

Estatísticas do Ping para 192.168.0.101:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 1ms, Máximo = 25ms, Média = 7ms

```

06) Instale o iptraf execute o ping para o endereço www.uit.br e capture os pacotes icmp.

Como o Debian não foi utilizado, não é possível utilizar “iptraf”, porém os pacotes podem ser igualmente capturados utilizando o WIRESHARK, conforme feito na imagem abaixo:

The image displays two side-by-side windows. The left window is Wireshark, titled 'Capturing from Ethernet', showing a packet capture list with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 749 is highlighted, showing an ICMP Echo (ping) reply from 186.202.153.93 to 192.168.0.107. A detailed view of this packet is shown below the list, indicating it is 74 bytes on wire and 74 bytes captured on interface \Device\NPF_{C751DEE7...}. The right window is a Windows Command Prompt, titled 'C:\WINDOWS\system32\cmd. X', showing the output of a ping command to 186.202.153.93. The output shows 20 successful responses, each 32 bytes, with a time of 9ms and TTL=57. The statistics at the bottom indicate 20 packets sent, 20 received, and 0% loss.

No.	Time	Source	Destination	Protocol	Length	Info
746	49.333755	177.54.145.79	192.168.0.107	TCP	66	[TCP Keep-Alive ACK] 443 → 49909 [ACK] Seq=1 Ack=2 Win=
747	49.418413	192.168.0.107	192.168.0.255	UDP	86	57621 → 57621 Len=44
748	50.170715	192.168.0.107	186.202.153.93	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (
749	50.180610	186.202.153.93	192.168.0.107	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=57 (
750	50.415235	142.251.129.138	192.168.0.107	QUIC	137	Protected Payload (KP0)
751	50.441125	192.168.0.107	142.251.129.138	QUIC	75	Protected Payload (KP0), DCID=d5e2295c0cd149c4
752	50.872765	192.168.0.107	35.186.224.25	UDP	1287	62009 → 443 Len=1245

```
Disparando uit.br [186.202.153.93] com 32 bytes de dados:
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57
Resposta de 186.202.153.93: bytes=32 tempo=9ms TTL=57

Estatísticas do Ping para 186.202.153.93:
  Pacotes: Enviados = 20, Recebidos = 20, Perdidos = 0 (0% de
perda),
  Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 9ms, Máximo = 10ms, Média = 9ms
Control-C
^C
```

