

ICMP

Para os exercícios 1 a 4 fiz o seguinte no CMD

```
C:\Users\User>ping -n 10 ualg.pt

Pinging ualg.pt [193.136.224.33] with 32 bytes of data:
Reply from 193.136.224.33: bytes=32 time=84ms TTL=55
Reply from 193.136.224.33: bytes=32 time=29ms TTL=55
Reply from 193.136.224.33: bytes=32 time=28ms TTL=55
Reply from 193.136.224.33: bytes=32 time=31ms TTL=55
Reply from 193.136.224.33: bytes=32 time=33ms TTL=55
Reply from 193.136.224.33: bytes=32 time=29ms TTL=55
Reply from 193.136.224.33: bytes=32 time=28ms TTL=55
Reply from 193.136.224.33: bytes=32 time=33ms TTL=55
Reply from 193.136.224.33: bytes=32 time=27ms TTL=55
Reply from 193.136.224.33: bytes=32 time=28ms TTL=55

Ping statistics for 193.136.224.33:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 27ms, Maximum = 84ms, Average = 35ms
```

1

IP do host: 192.168.1.110

IP do dest: 193.136.224.33

2

O ICMP (internet control message protocol) não possui número de porta de origem e de destino porque este protocolo serve para comunicar informações da camada de rede entre hosts e routers, logo, não é protocolo de transporte como o TCP e o UDP então não possui números de portas de destino nem de origem. O ICMP para identificar a mensagem que está a ser recebida utiliza uma combinação tipo/código.

3

O tipo do ICMP é o 8 e número do código é 0. O ICMP conta com campos como checksum, identifier, sequence number, e data fields. O checksum, o identifier e o sequence number têm 2 bytes cada um.

```
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d5a [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Response frame: 704]
  ▶ Data (32 bytes)
```

4

O tipo do ICMP é o tipo 0 e o número do código é o 0. O ICMP conta com campos como checksum, identifier, sequence number, e data fields. O checksum, o identifier e o sequence number têm 2 bytes cada um tal como no request.

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x555a [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Request frame: 702]
  [Response time: 84,028 ms]
  ▼ Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
    [Length: 32]
```

Para os seguintes exercícios fiz isto no cmd.

```
C:\Users\User>tracert ualg.pt

Tracing route to ualg.pt [193.136.224.33]
over a maximum of 30 hops:

 1      6 ms      5 ms      2 ms    192.168.1.1
 2     33 ms     12 ms     17 ms    10.17.127.254
 3     33 ms     15 ms     14 ms    10.137.227.81
 4     42 ms     18 ms     18 ms    10.255.48.82
 5     33 ms     24 ms     18 ms    Router3.Lisboa.fccn.pt [193.136.251.1]
 6     26 ms     19 ms     19 ms    Router30.Lisboa.fccn.pt [194.210.6.102]
 7     38 ms     19 ms     18 ms    Router13.Evora.fccn.pt [194.210.6.121]
 8      *        *        *        Request timed out.
 9      *        *        *        Request timed out.
10    40 ms     29 ms     22 ms    www.ualg.pt [193.136.224.33]

Trace complete.
```

5

IP do host: 192.168.1.110

IP do dest: 193.136.224.33

6

Não, o número de protocolo IP não seria 01 se o ICMP usasse pacotes UDP como em Unix/Linux. O número de protocolo deveria ser 0x11 se o ICMP usasse pacotes UDP.

7

Tem os mesmos campos do ICMP ping request da primeira parte deste lab.

8

O pacote de erro ICMP não é o mesmo que os pacotes de ICMP ping request. O pacote de erro contém o cabeçalho IP e os primeiros 8 bytes do pacote ICMP original ao qual o erro de refere.

9

Os 3 últimos pacotes ICMP são do tipo 0 (echo reply) e os de erro são do tipo 11 (TTL expirado) Eles são diferentes porque os datagramas chegaram ao host de destino antes do TTL expirar.

```
> Frame 889: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{C73F9624-6EA4-48F7-84A2-92694EAC7D94}
> Ethernet II, Src: AskeyCompute_1b:8b:74 (78:29:ed:1b:8b:74), Dst: AzureWaveTec_1b:ad:5f (14:d4:24:1b:ad:5f)
> Internet Protocol Version 4, Src: 193.136.224.33, Dst: 192.168.1.13
> Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xffd8 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 38 (0x0026)
  Sequence Number (LE): 9728 (0x2600)
  [Request frame: 886]
  [Response time: 40,326 ms]
> Data (64 bytes)

...

> Frame 368: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{C73F9624-6EA4-48F7-84A2-92694EAC7D94}
> Ethernet II, Src: AskeyCompute_1b:8b:74 (78:29:ed:1b:8b:74), Dst: AzureWaveTec_1b:ad:5f (14:d4:24:1b:ad:5f)
> Internet Protocol Version 4, Src: 194.210.6.121, Dst: 192.168.1.13
> Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4ee [correct]
  [Checksum Status: Good]
  Unused: 00
  Length: 17
  [Length of original datagram: 68]
  Unused: 0000
> Internet Protocol Version 4, Src: 192.168.1.13, Dst: 193.136.224.33
> Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7e1 [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 1 (0x0001)
```

10

Apresentam todos mais ou menos os mesmos tempos, isto no caso que eu fiz para a ualg.pt. Já na figura 4, existe uma ligação que demora mais que outras que de new york para pastourelle.

```
C:\Users\User>tracert ualg.pt

Tracing route to ualg.pt [193.136.224.33]
over a maximum of 30 hops:

  1    6 ms    5 ms    2 ms  192.168.1.1
  2   33 ms   12 ms   17 ms  10.17.127.254
  3   33 ms   15 ms   14 ms  10.137.227.81
  4   42 ms   18 ms   18 ms  10.255.48.82
  5   33 ms   24 ms   18 ms  Router3.Lisboa.fccn.pt [193.136.251.1]
  6   26 ms   19 ms   19 ms  Router30.Lisboa.fccn.pt [194.210.6.102]
  7   38 ms   19 ms   18 ms  Router13.Evora.fccn.pt [194.210.6.121]
  8    *      *      *      Request timed out.
  9    *      *      *      Request timed out.
 10   40 ms   29 ms   22 ms  www.ualg.pt [193.136.224.33]

Trace complete.
```