Universidade Federal de Uberlândia – UFU

Bacharelado em Sistemas de Informação - Campus Monte Carmelo

GSI524 - Redes de computadores - 2021/1

RENAN JUSTINO REZENDE SILVA - 11921BSI223

Atividade 9

ICMP

• O objetivo desta atividade é entender melhor o ICMP. Leia o texto e execute os passos que estão no arquivo (Wireshark_ICMP.pdf). Durante os passos no arquivo, serão indicados itens para serem respondidos. As perguntas a seguir referem-se à atividade no arquivo (Wireshark_ICMP.pdf).

```
C:\Users\Renato>ping -n 10 www.ust.hk

Disparando www.ust.hk [143.89.12.134] com 32 bytes de dados:
Resposta de 143.89.12.134: bytes=32 tempo=325ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=325ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=328ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=326ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=326ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=326ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=330ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=328ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=326ms TTL=48
Resposta de 143.89.12.134: bytes=32 tempo=329ms TTL=48

Estatísticas do Ping para 143.89.12.134:
    Pacotes: Enviados = 10, Recebidos = 10, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 325ms, Máximo = 330ms, Média = 326ms
```

Figura 1: ping –n 10 www.ust.hk

1. Qual é o endereço IP do seu host? Qual é o endereço IP do host de destino?

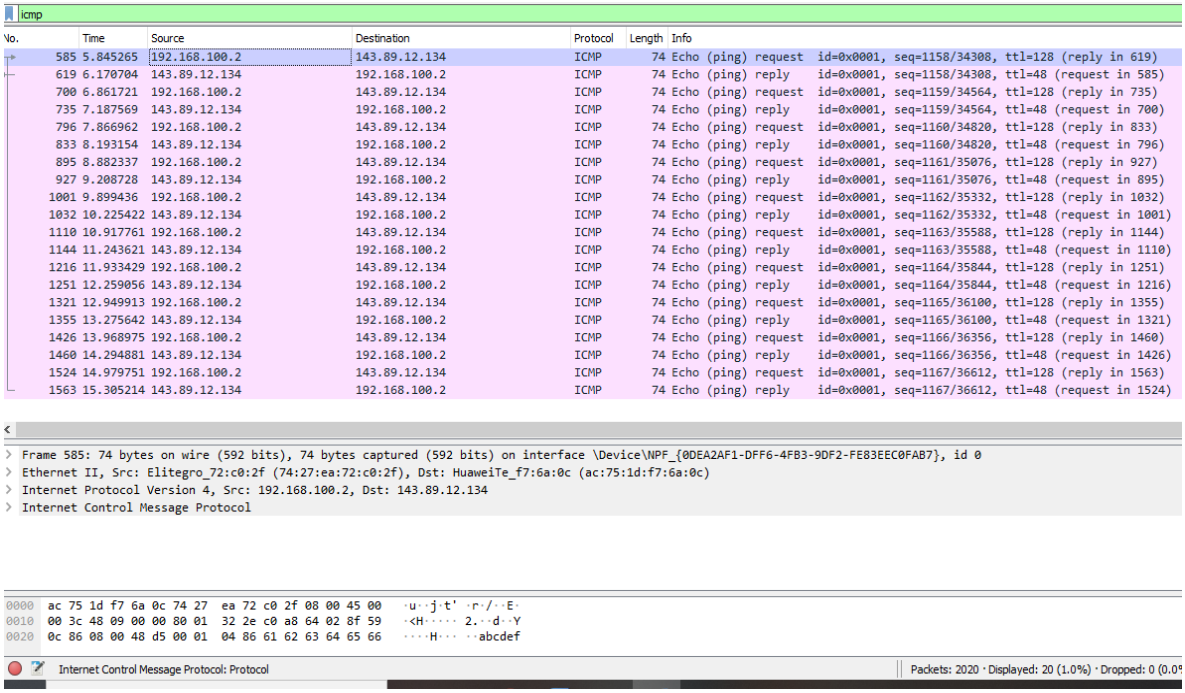

Figura 2: Pacotes ICMP do ping

R = O endereço IP de meu host é o 192.168.100.2 e o endereço IP do host de destino é o 143.89.12.134

2. Por que um pacote ICMP não tem números de porta de origem e destino?

R = Pelo fato de que o pacote ICMP ter sido feito para comunicar informações da camada de rede dos hosts e não nos processos da camada de aplicação. O pacote ICMP tem seu tipo, código que identifica o recebimento da mensagem. Não há uso de portas para direcionamento de mensagem.

3. Examine um dos pacotes de solicitação de ping enviados por seu host. Quais são o tipo de ICMP e os números de código? Que outros campos este pacote ICMP possui? Quantos bytes são os campos de checksum, número de sequência e identificador?

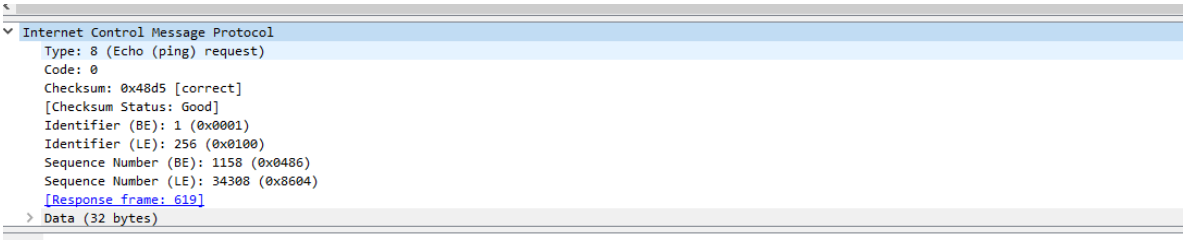

Figura 3: Um dos pacotes ICMP

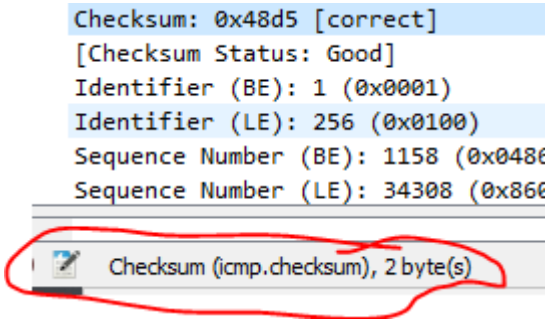

Figura 4: Checksum 2 bytes

R = O tipo de ICMP é o 8 (Echo) (Ping) request). O código é o 0. Possui os campos checksum, identificador, número de sequência, dados. Os campos checksum, sequence number e identifier possuem 2 bytes cada um.

4. Examine o pacote de resposta de ping correspondente. Quais são o tipo de ICMP e os números de código? Que outros campos este pacote ICMP possui? Quantos bytes são os campos de checksum, número de sequência e identificador?

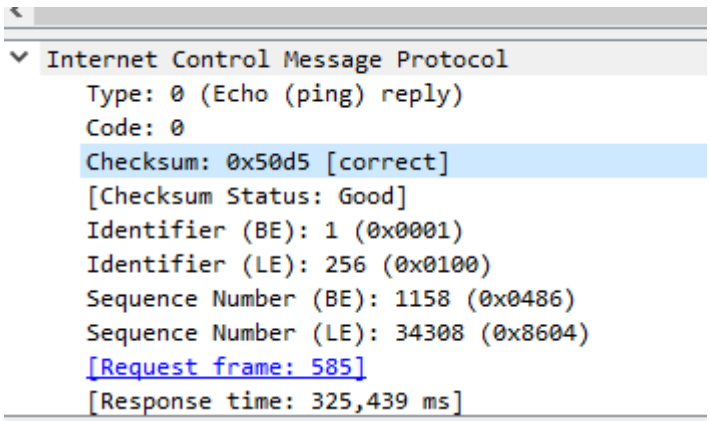

Figura 5: Ping reply

R = O tipo de ICMP é o 0. (Echo (ping) reply). O código é numero 0. Possui os campos de checksum, identificador, número de sequência, tempo de resposta, frame request. Os campos identificador, número de sequência e checksum possuem 2 bytes cada um.

5. Qual é o endereço IP do seu host? Qual é o endereço IP do host de destino de destino?

```
C:\Users\Renato>tracert www.inria.fr

Rastreando a rota para inria.fr [128.93.162.83]
com no máximo 30 saltos:

  1    <1 ms    <1 ms    <1 ms  192.168.100.1
  2     *        11 ms     *     terra-200-225-254-248.dynamic.idial.com.br [200.225.254.248]
  3     2 ms     3 ms     3 ms  100.127.5.35
  4     *        3 ms      *     187-032-149-225.static.ctbctelecom.com.br [187.32.149.225]
  5   121 ms   121 ms   122 ms  100.126.3.206
  6   123 ms   121 ms   124 ms  100.127.6.98
  7    18 ms    14 ms    22 ms  100.127.6.154
  8   121 ms   120 ms   121 ms  et-2-1-2-0.sac.border-b.mia.algartelecom.com.br [168.197.23.185]
  9   120 ms   131 ms   129 ms  ae40.cr6-mia1.ip4.gtt.net [98.124.189.121]
 10   221 ms   220 ms   220 ms  et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
 11   220 ms   221 ms   223 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 12   222 ms   221 ms   228 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 13   221 ms   221 ms   221 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 14   222 ms   221 ms   222 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 15   221 ms   228 ms   221 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Rastreamento concluído.
```

Figura 6: tracert www.inria.fr

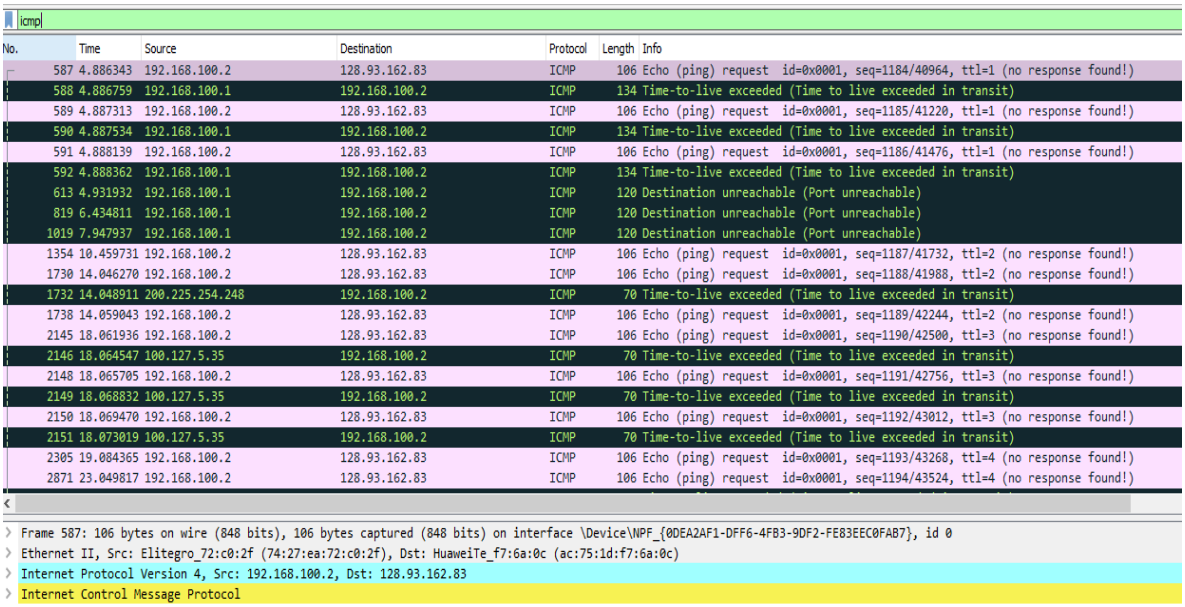

Figura 7: Pacotes ICMP tracert

R = O endereço IP de meu host é o 192.168.100.2 e o endereço IP do host de destino é o 128.93.162.83

6. Se o ICMP enviar pacotes UDP (como no Unix/Linux), o número do protocolo IP ainda seria 01 para os pacotes examinados? Se não, o que seria?

R = Não, pois caso o ICMP enviar pacotes UDP o número do protocolo IP é o 0x11 no lugar de 01.

7. Examine o pacote de eco ICMP em sua captura de tela. Isso é diferente dos pacotes de consulta de ping ICMP na primeira metade deste laboratório? Se sim, como assim?

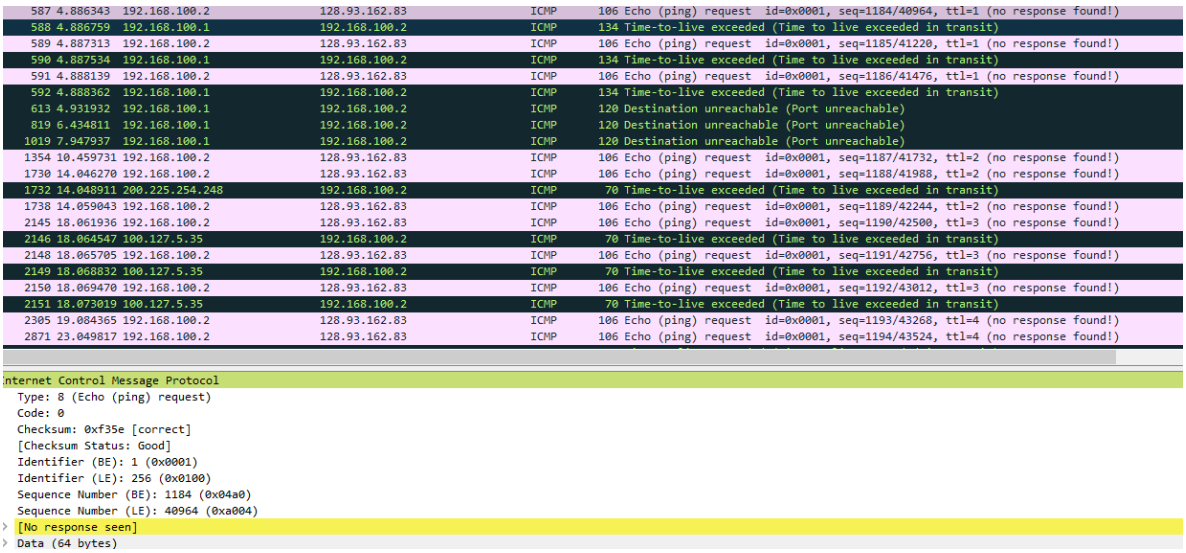

Figura 8: Pacotes ICMP tracert Echo

R = Não, possuem os mesmos campos ICMP, o que muda no pacote em si seria o valor de ttl e o no response found.

8. Examine o pacote de erro ICMP em sua captura de tela. Ele tem mais campos do que o pacote de eco ICMP. O que está incluído nesses campos?

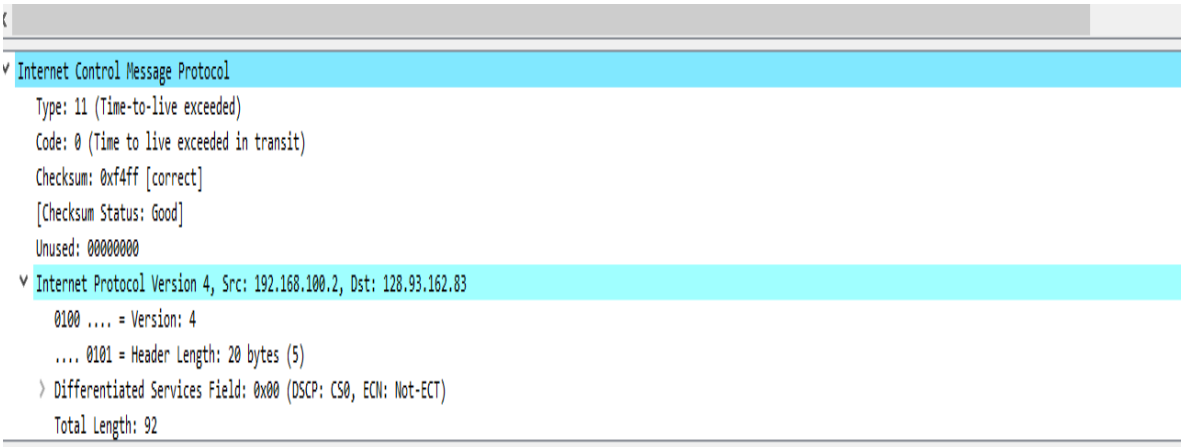

Figura 8: Pacote erro ICMP ttl exceeded

R = O pacote não é o mesmo de ping, ele possui alguns campos diferentes, como unused, tipo diferente que é o 11, embaixo o cabeçalho ipv4. Considerando os campos apenas da aba ICMP, possuem menos campos do que o pacote eco.

9. Examine os últimos três pacotes ICMP recebidos pelo host de origem. Como esses pacotes são diferentes dos pacotes de erro ICMP? Por que eles são diferentes?

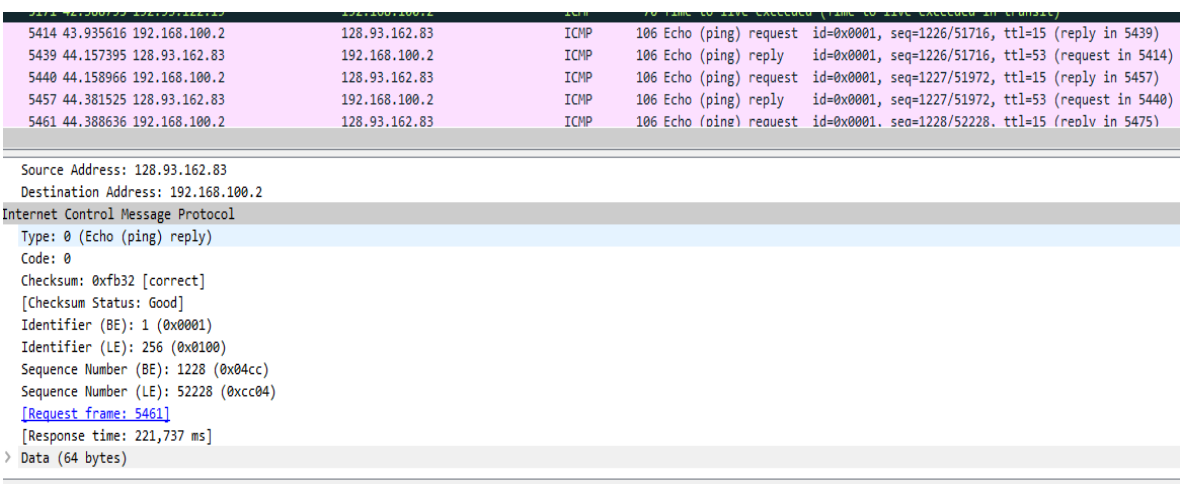

Figura 9: Um dos três últimos pacotes

R = O tipo é o 0, diferente do de erro que é o 11, os pacotes são diferentes pelo fato dos datagramas irem pro host de destino antes de expirar o TTL.

10. Dentro das medições do tracert, existe um link cujo atraso é significativamente maior do que outros? Consulte a captura de tela na Figura 4, há um link cujo atraso é significativamente maior do que outros? Com base nos nomes dos roteadores, você consegue supor a localização dos dois roteadores no final deste link?

Figura 10: Figura 4 do Wireshark ICMP lab usado para esta questão

R = Há um link de cidades e países, como por exemplo, nyc.opentransit.net para PASCR1.pastourelle, ou seja de New York (EUA) para Pastourelle, depois de Pastourelle para Aubervilliers que fica na França, depois de Aubervilliers para Bagnolet.