



ATIVIDADE ACADÊMICA: Redes de Computadores:  
Networking, Roteamento e Transmissão

TRABALHO: Atividade 4

ALUNOS: Rafael Hansen Klauck

Para realizar essa atividade, rodei o comando `sudo tcpdump -i en0 -w` para poder analisar os pacotes da rede. Após deixar o comando executando por um tempo, abri ele no Wireshark. Como minha rede tem suporte para IPV6, minha máquina acabava priorizando a utilização dele, por isso não conseguia ver nenhum pacote ICMPv4. Então, para que fosse possível visualizar tantos pacotes ICMPv4 e v6, eu abri um segundo terminal para executar o comando `traceroute`.

### Foram encontrados pacotes ICMP v4 e v6?

No.	Time	Source	Destination	Protocol	Length	Info
143	2.547752	2884:2a4c:140f:5000::...	2880:3f0:4001:83b::...	ICMPv6	70	Echo (ping) request id=0x7473, seq=0, hop limit=255 (reply in 145)
145	2.565935	2880:3f0:4001:83b::...	2884:2a4c:140f:5000::...	ICMPv6	70	Echo (ping) reply id=0x7473, seq=0, hop limit=60 (request in 143)
198	3.551757	2884:2a4c:140f:5000::...	2880:3f0:4001:83b::...	ICMPv6	70	Echo (ping) request id=0x7473, seq=1, hop limit=255 (reply in 199)
199	3.569951	2880:3f0:4001:83b::...	2884:2a4c:140f:5000::...	ICMPv6	70	Echo (ping) reply id=0x7473, seq=1, hop limit=60 (request in 198)
284	4.556763	2884:2a4c:140f:5000::...	2880:3f0:4001:83b::...	ICMPv6	70	Echo (ping) request id=0x7473, seq=2, hop limit=255 (reply in 285)
285	4.575776	2880:3f0:4001:83b::...	2884:2a4c:140f:5000::...	ICMPv6	70	Echo (ping) reply id=0x7473, seq=2, hop limit=60 (request in 284)
348	5.181169	fe80::1	2884:2a4c:140f:5000::...	ICMPv6	86	Neighbor Solicitation for 2884:2a4c:140f:5000::c1b:79e3:4b10:5ba7 from fc:40:09:0c:61:26
349	5.181225	fe80::180a:c08b:54b::...	fe80::1	ICMPv6	78	Neighbor Advertisement 2884:2a4c:140f:5000::c1b:79e3:4b10:5ba7 (sol)
357	5.560230	2884:2a4c:140f:5000::...	2880:3f0:4001:83b::...	ICMPv6	70	Echo (ping) request id=0x7473, seq=3, hop limit=255 (reply in 358)
358	5.578147	2880:3f0:4001:83b::...	2884:2a4c:140f:5000::...	ICMPv6	70	Echo (ping) reply id=0x7473, seq=3, hop limit=60 (request in 357)
385	5.953801	192.168.1.10	172.217.29.225	ICMP	70	Destination unreachable (Port unreachable)
400	6.033966	192.168.1.10	172.217.29.225	ICMP	70	Destination unreachable (Port unreachable)
411	6.014189	192.168.1.10	172.217.29.225	ICMP	70	Destination unreachable (Port unreachable)
421	6.166831	2884:2a4c:140f:5000::...	2880:3f0:4001:80e::...	ICMPv6	136	Destination Unreachable (Port unreachable)
493	6.564589	2884:2a4c:140f:5000::...	2880:3f0:4001:83b::...	ICMPv6	70	Echo (ping) request id=0x7473, seq=4, hop limit=255 (reply in 497)
497	6.582519	2880:3f0:4001:83b::...	2884:2a4c:140f:5000::...	ICMPv6	70	Echo (ping) reply id=0x7473, seq=4, hop limit=60 (request in 493)
589	7.771938	2884:2a4c:140f:5000::...	2880:3f0:4001:80e::...	ICMPv6	136	Destination Unreachable (Port unreachable)
689	7.638572	2884:2a4c:140f:5000::...	2880:3f0:4001:80e::...	ICMPv6	136	Destination Unreachable (Port unreachable)
1289	13.263477	192.168.1.1	192.168.1.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1380	13.290398	192.168.1.1	192.168.1.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1382	13.292147	192.168.1.1	192.168.1.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
1384	13.295961	10.255.255.240	192.168.1.10	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1315	13.323951	10.255.255.240	192.168.1.10	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1317	13.326668	10.255.255.240	192.168.1.10	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

### Quais os tipos de ICMP forma capturados?

Para o **ICMPv4** foram encontrados Time-to-Life exceeded(tipo 11) e Destination unreachable(tipo 3).

Para o **ICMPv6** foram encontrados Echo Ping(request), Echo Ping(replay), Neighbor Solicitation, Neighbor Advertisement (136) e Destination Unreachable.

## Quais os campos do ICMP encontrados?

**ICMPv4:** Type, code, checksum, checksum status, unused.

```

Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0x815f [correct]
  [Checksum Status: Good]
  Unused: 00000000
  > Internet Protocol Version 4, Src: 192.168.1.10, Dst: 172.217.29.174
  > User Datagram Protocol, Src Port: 62591, Dst Port: 33436
  > Data (12 bytes)
```

Algo que é importante de comentar é que o type, o code, e o checksum são campos fixos no cabeçalho. Os demais campos, o conteúdo pode alterar, dependendo do tipo de mensagem, como podemos ver na imagem a abaixo, que tem conteúdo diferente da anterior.

```

Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 3 (Port unreachable)
  Checksum: 0x0411 [correct]
  [Checksum Status: Good]
  Unused: 00000000
  > Internet Protocol Version 4, Src: 172.217.29.225, Dst: 192.168.1.10
  > User Datagram Protocol, Src Port: 443, Dst Port: 62072
```

**ICMPv6:** type, code, checksum, checksum status, identifier, sequence, Timestamp from Echo data e Timestamp from Echo data (relative).

```

Internet Control Message Protocol v6
  Type: Echo (ping) request (128)
  Code: 0
  Checksum: 0x12ce [correct]
  [Checksum Status: Good]
  Identifier: 0x7473
  Sequence: 0
  [Response In: 145]
  Timestamp from Echo data: Mar 20, 2025 22:01:04.778730000 -03
  [Timestamp from Echo data (relative): 0.000036000 seconds]
```

Assim como no ICMPv4, o type, o code, e o checksum são campos fixos no cabeçalho, já os demais podem alterar

```

Internet Control Message Protocol v6
  Type: Neighbor Solicitation (135)
  Code: 0
  Checksum: 0x12fc [correct]
  [Checksum Status: Good]
  Reserved: 00000000
  Target Address: fe80::1
  > ICMPv6 Option (Source link-layer address : b6:6c:ad:dc:79:41)

```

## Qual o tamanho dos dados ICMP?

ICMPv4: O tamanho dos dados ICMP varia conforme o tipo da mensagem. No caso da mensagem ICMP Time-to-live exceeded (Type 11) capturada, o Wireshark mostra o campo Data (12 bytes), indicando que a mensagem carrega 12 bytes de dados após o cabeçalho ICMP. Portanto, o tamanho dos dados ICMP nesse pacote é de 12 bytes. Esses dados representam uma cópia do cabeçalho IP e dos primeiros bytes do pacote original que causou o erro, conforme definido pelo padrão do protocolo ICMP.

```

Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0x815f [correct]
  [Checksum Status: Good]
  Unused: 00000000
  > Internet Protocol Version 4, Src: 192.168.1.10, Dst: 172.217.29.174
  > User Datagram Protocol, Src Port: 62591, Dst Port: 33435
  > Data (12 bytes)

```

ICMPv6: Embora o Wireshark não exiba o campo Data (X bytes) explicitamente, a presença de campos como Timestamp from Echo data indica que a mensagem ICMPv6 Echo Request carrega dados além do cabeçalho. O cabeçalho ocupa 8 bytes, e o restante corresponde aos dados, que incluem informações como timestamps usados no cálculo do tempo de resposta (RTT). Se analisarmos a imagem a seguir, vemos que esse pacote tem um length de 70 bytes. Sabemos que o cabeçalho IPv6 tem um tamanho fixo

de 40 bytes. Outra informação é que o cabeçalho ICMPv6 de uma mensagem Echo Request tem em seu cabeçalho o Type (8 bits), Code (8 bits), Checksum (16 bits), Identifier (16 bits) e Sequence Number (16 bits), segundo a [RFC 4443](#) (segunda imagem a seguir). Com isso, sabemos que o tamanho do cabeçalho ICMPv6 para essa mensagem é de 64 bits ou 8 bytes. Como o pacote inteiro é de 70 bytes, podemos fazer a seguinte conta:

$$ICMP\ data = 70\ (length\ total) - 40\ (IPv6) - 8\ (ICMPv6) = 22\ bytes$$

```
> Frame 143: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: b6:6c:ad:dc:79:41 (b6:6c:ad:dc:79:41), Dst: zte_0c:61:26 (fc:40:09:0c:61:26)
v Internet Protocol Version 6, Src: 2804:2a4c:140f:5000:8c1b:79e3:4810:5ba7, Dst: 2800:3f0:4001:83b::200e
  0110 .... = Version: 6
  > .... 0000 0000 .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0100 0000 0000 0000 0000 = Flow Label: 0x40000
  Payload Length: 16
  Next Header: ICMPv6 (58)
  Hop Limit: 255
  > Source Address: 2804:2a4c:140f:5000:8c1b:79e3:4810:5ba7
  > Destination Address: 2800:3f0:4001:83b::200e
  [Stream index: 4]
v Internet Control Message Protocol v6
  Type: Echo (ping) request (128)
  Code: 0
  Checksum: 0x12ce [correct]
  [Checksum Status: Good]
  Identifier: 0x7473
  Sequence: 0
  [Response In: 145]
  Timestamp from Echo data: Mar 20, 2025 22:01:04.778730000 -03
  [Timestamp from Echo data (relative): 0.000036000 seconds]
```

### Echo Request Message

0								1								2								3							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type								Code								Checksum															
Identifier																Sequence Number															
Data ...																															

## Qual a diferença entre o tamanho dos pacotes capturados?

A diferença entre o tamanho dos pacotes ICMP capturados foi de 66 bytes, considerando o maior pacote com 136 bytes e o menor com 70 bytes. Essa variação ocorre devido às diferenças entre os tipos de mensagens ICMP (como Echo Request, Time Exceeded ou Destination Unreachable) e a quantidade de dados ou cabeçalhos encapsulados em cada tipo.

411	6.014109	192.168.1.10	172.217.29.225	ICMP	70 Destination unreachable (Port unreachable)
421	6.166831	2804:2a4c:140f:5000...	2800:3f0:4001:80e:...	ICMPv6	136 Destination Unreachable (Port unreachable)