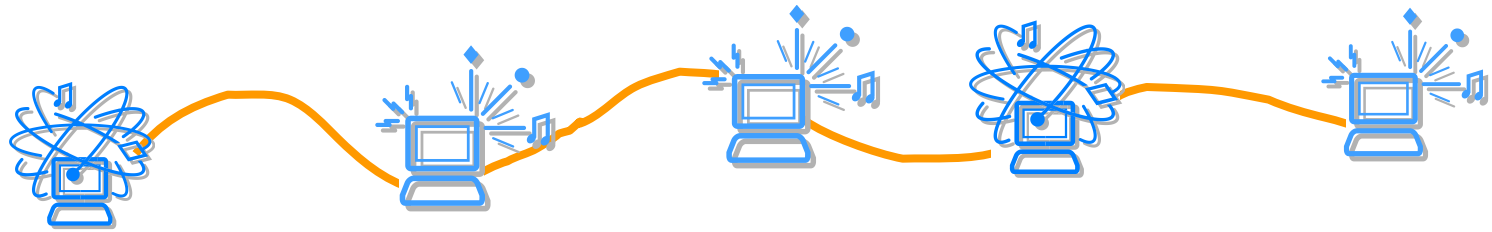
Camada de Rede: Protocolo IP



Instituto Superior de Engenharia de Lisboa

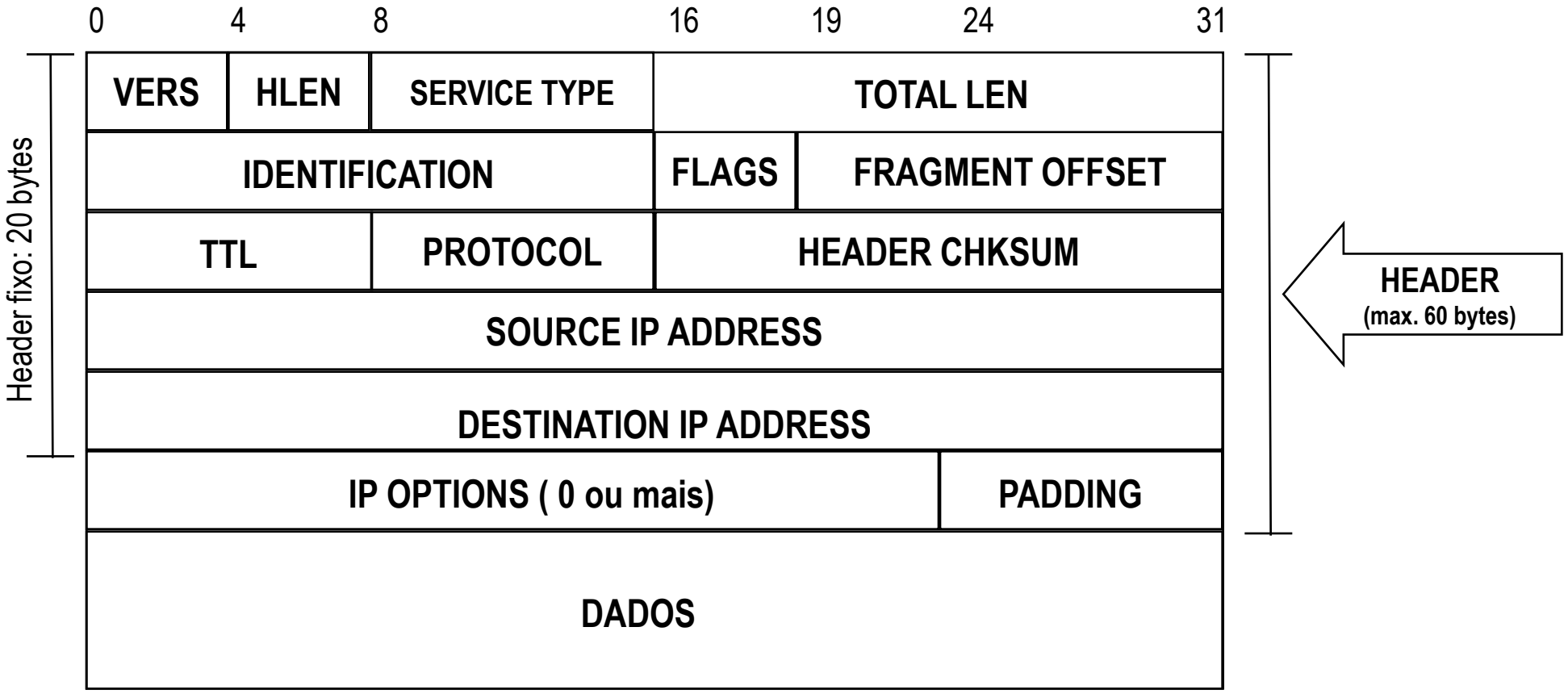
Departamento de Engenharia de Electrónica e Telecomunicações e de Computadores

Redes de Computadores

Nível Rede - Internet Protocol (IP)

- Características
  - Fornece comunicação não fiável entre duas máquinas
    - Define unidade de transferência do protocolo - Datagramas
  - Responsável pelo encaminhamento dos datagramas
  - Verifica a validade do cabeçalho dos datagramas recebidos
    - Não dá garantias acerca da integridade dos dados
  - Testa o MTU (Maximum Transfer Unit) da rede
  - Fragmenta os datagramas de acordo com o MTU
  - Recebe e envia mensagens ICMP de controle e informação de erros
  - Definido no RFC 791

Datagrama IP (1)



Datagrama IP (2)

- Campos do Datagrama

  VERS - Versão do IP (actualmente v4 - futuramente v6)

  HLEN - Dimensão do *header* (0..15 em múltiplos de 32 bit)

  SERVICE TYPE - ver adiante

  TOTAL LEN - Dimensão do Datagrama

  IDENTIFICATION, FLAGS, FRAGMENT OFFSET - ver adiante

  TTL - Time To Live - Número de *routers* que o Datagrama pode passar

  PROTOCOL - Protocolo de nível superior

  HEADER CHECKSUM - Campo de verificação da integridade do *header*

  SOURCE IP - Endereço de origem

  DESTINATION IP - Endereço de destino

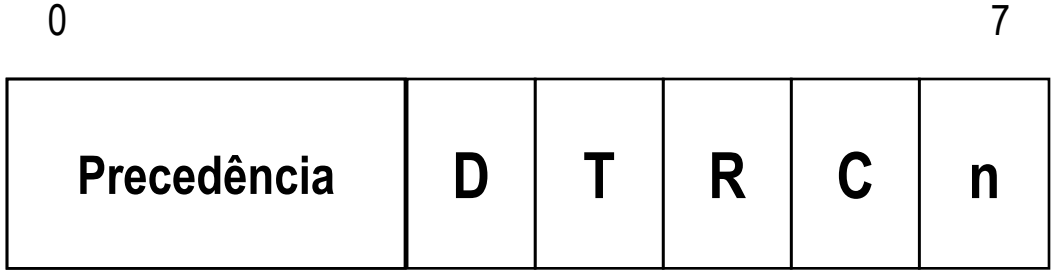
  OPTIONS, PADDING - ver adiante

Datagrama IP (3) - Campo Protocol

ip	0	IP	# internet protocol, pseudo protocol number
icmp	1	ICMP	# internet control message protocol
igmp	2	IGMP	# Internet Group Management
ggp	3	GGP	# gateway-gateway protocol
ipencap	4	IP-ENCAP	# IP encapsulated in IP (officially ``IP'')
tcp	6	TCP	# transmission control protocol
egp	8	EGP	# exterior gateway protocol
udp	17	UDP	# user datagram protocol
xns-idp	22	XNS-IDP	# Xerox NS IDP
rdp	27	RDP	# "reliable datagram" protocol
iso-tp4	29	ISO-TP4	# ISO Transport Protocol class 4
ddp	37	DDP	# Datagram Delivery Protocol
ospf	89	OSPFIGP	# Open Shortest Path First IGP
ipip	94	IPIP	# Yet Another IP encapsulation
encap	98	ENCAP	# Yet Another IP encapsulation

Datagrama IP (4) - Service Type

- Formato do campo ***Service Type***



Precedência: 0 - Normal → 7 Network control

D - *Low Delay*
T - *High Throughput*
R - *High Reliability*
C - *Low Cost*
n - reservado

(exclusivos)

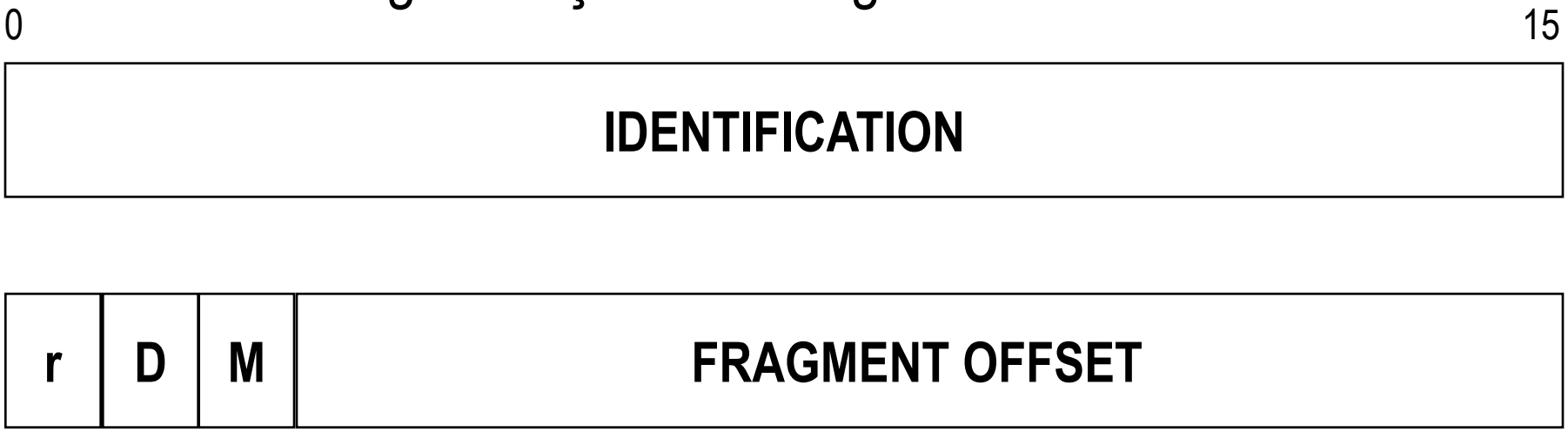
Definido no RFC 1340 e 1349

Routing baseado no ToS

- Implementação IP nos Routers
  - *Queues* de datagramas independentes consoante o ToS
  - Definição dos custos das interfaces consoante o ToS
- Aplicações
  - Protocolos geram ToS com base na funcionalidade
    - Telnet e Comandos FTP (D – *low delay*) / Dados FTP (T – *high throughput*)
  - Encaminhar tráfego com base no tipo de meio físico
    - Cabo Submarino (D) / Ligação por satélite (T)

Datagrama IP (5) - Fragmentação

- Controle da Fragmentação de Datagramas

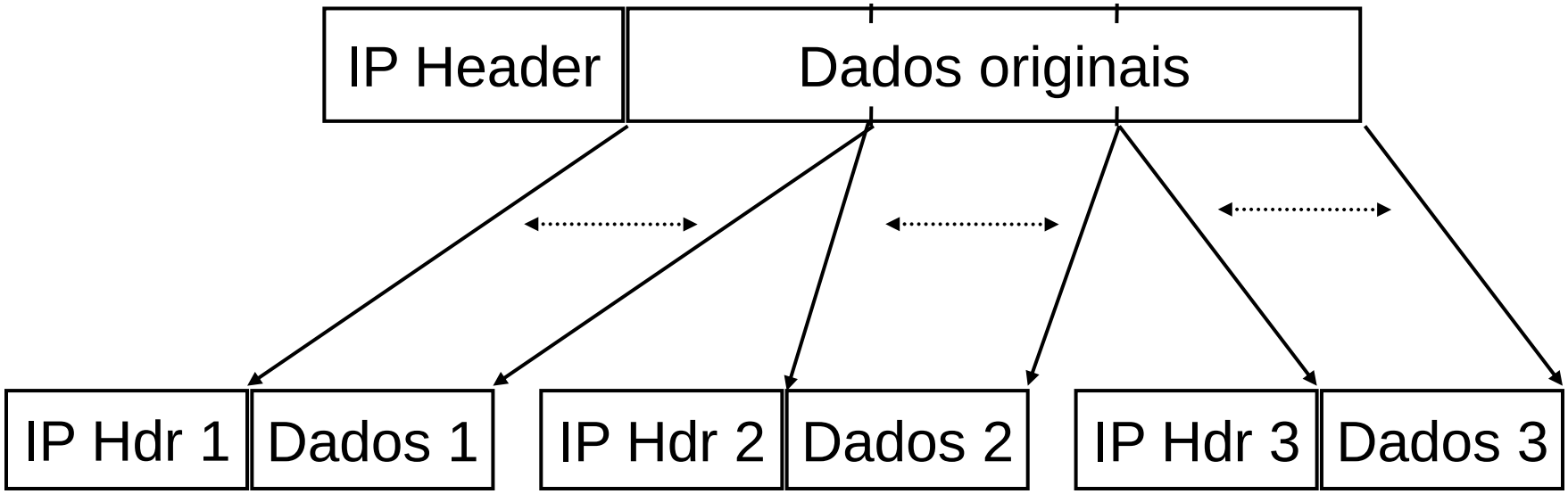


FRAGMENT OFFSET :
Medido em múltiplos de 64 bits (8 bytes)

D : 1 - Não fragmentar (DF)
M : 1 - Há mais fragmentos a seguir
r : Reservado

Fragmentação IP

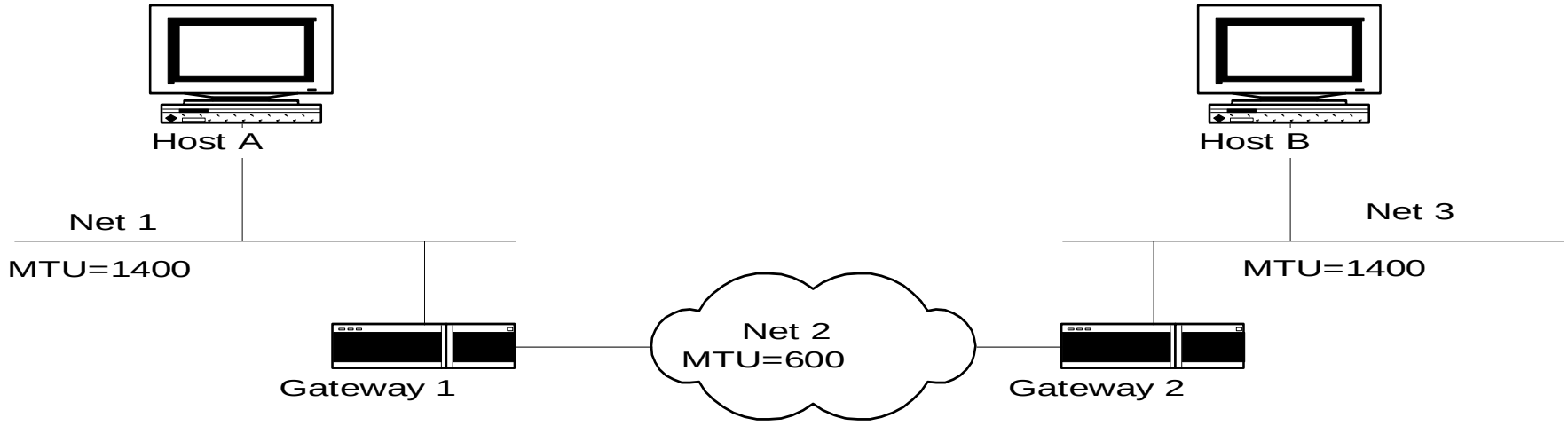
- Objectivos
  - Partir os dados em blocos com uma dimensão que seja possível enviar através das redes físicas (visto que estas possuem limitações) ou seja respeitando o MTU (Maximum Transfer Unit)



Fragmentação IP (cont.)

- Características
  - O *header* Original é copiado para cada fragmento e depois modificado (flags, fragment offset, length,...)
    - Algumas opções IP também são copiadas (RFC 791)
  - Fragmentos podem ser fragmentados de novo ao longo do caminho
    - Sub-fragmentos têm o mesmo formato dos fragmentos
  - Se o DF bit está activo e é necessário fragmentar:
    - O datagrama é descartado
    - É gerada uma mensagem ICMP
  - Os *headers* das camadas transporte e aplicação não aparecem em todos os fragmentos.
    - Problema se for preciso espreitar nesses *headers* (Firewalls).

Fragmentação IP



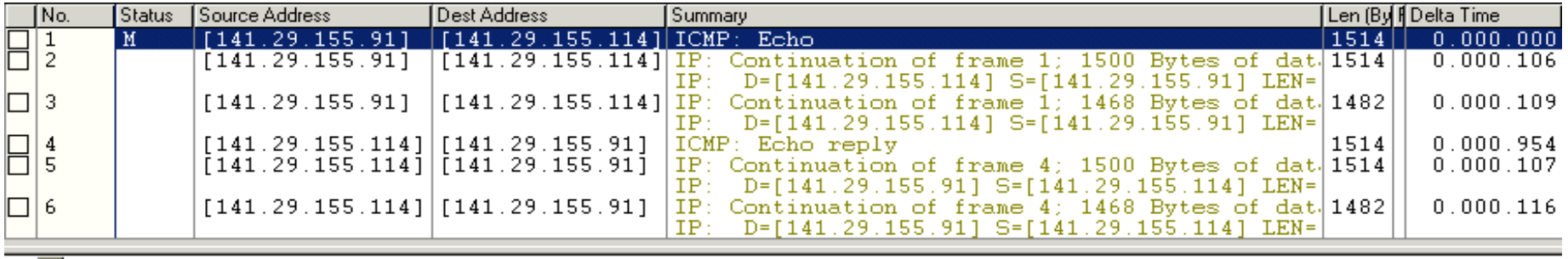
DATAGRAM HEADER	DATA 1 600 OCTETS	DATA 2 600 OCTETS	DATA 3 200 OCTETS

FRAGMENT 1 HEADER	DATA 1	FRAGMENTO 1 (offset = 0)
FRAGMENT 2 HEADER	DATA 2	FRAGMENTO 2 (offset = 600 / 8)
FRAGMENT 3 HEADER	DATA3	FRAGMENTO 3 (offset = 1200 / 8)

Reagrupamento (*Reassembly*)

- Características
  - O reagrupamento de fragmentos é feito no destino final
  - Se um fragmento se perde, todo o datagrama é descartado (passado um tempo)

Exemplo de fragmentação IP (1)



No.	Status	Source Address	Dest Address	Summary	Len (By	Delta Time
1	M	[141.29.155.91]	[141.29.155.114]	ICMP: Echo	1514	0.000.000
2		[141.29.155.91]	[141.29.155.114]	IP: Continuation of frame 1; 1500 Bytes of dat. IP: D=[141.29.155.114] S=[141.29.155.91] LEN=	1514	0.000.106
3		[141.29.155.91]	[141.29.155.114]	IP: Continuation of frame 1; 1468 Bytes of dat. IP: D=[141.29.155.114] S=[141.29.155.91] LEN=	1482	0.000.109
4		[141.29.155.114]	[141.29.155.91]	ICMP: Echo reply	1514	0.000.954
5		[141.29.155.114]	[141.29.155.91]	IP: Continuation of frame 4; 1500 Bytes of dat. IP: D=[141.29.155.91] S=[141.29.155.114] LEN=	1514	0.000.107
6		[141.29.155.114]	[141.29.155.91]	IP: Continuation of frame 4; 1468 Bytes of dat. IP: D=[141.29.155.91] S=[141.29.155.114] LEN=	1482	0.000.116

```
DLC: Ethertype=0800, size=1514 bytes
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:       000. ....   = routine
IP:       ...0 ....   = normal delay
IP:       .... 0...   = normal throughput
IP:       .... .0..   = normal reliability
IP:       .... ..0.   = ECT bit - transport protocol will ignore the CE bit
IP:       .... ...0   = CE bit - no congestion
IP: Total length    = 1500 bytes
IP: Identification  = 36920
IP: Flags           = 2X
IP:       .0.. ....   = may fragment
IP:       ..1. ....   = more fragments
IP: Fragment offset = 0 bytes
IP: Time to live    = 128 seconds/hops
IP: Protocol        = 1 (ICMP)
IP: Header checksum = 33E0 (correct)
IP: Source address      = [141.29.155.91]
IP: Destination address = [141.29.155.114]
IP: No options
IP:
ICMP: Echo
```

Exemplo de fragmentação IP (2)

No.	Status	Source Address	Dest Address	Summary	Len (By	Delta Time
1	M	[141.29.155.91]	[141.29.155.114]	ICMP: Echo	1514	0.000.000
2		[141.29.155.91]	[141.29.155.114]	IP: Continuation of frame 1; 1500 Bytes of dat. IP: D=[141.29.155.114] S=[141.29.155.91] LEN=	1514	0.000.106
3		[141.29.155.91]	[141.29.155.114]	IP: Continuation of frame 1; 1468 Bytes of dat. IP: D=[141.29.155.114] S=[141.29.155.91] LEN=	1482	0.000.109
4		[141.29.155.114]	[141.29.155.91]	ICMP: Echo reply	1514	0.000.954
5		[141.29.155.114]	[141.29.155.91]	IP: Continuation of frame 4; 1500 Bytes of dat. IP: D=[141.29.155.91] S=[141.29.155.114] LEN=	1514	0.000.107
6		[141.29.155.114]	[141.29.155.91]	IP: Continuation of frame 4; 1468 Bytes of dat. IP: D=[141.29.155.91] S=[141.29.155.114] LEN=	1482	0.000.116

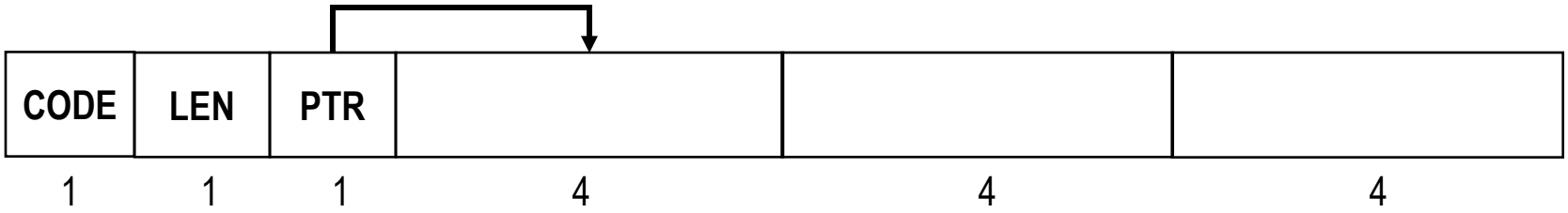
```
IP: Continuation of frame 1
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:       000. ....   = routine
IP:       ...0 ....   = normal delay
IP:       .... 0...   = normal throughput
IP:       .... .0..   = normal reliability
IP:       .... ..0.   = ECT bit - transport protocol will ignore the CE bit
IP:       .... ...0   = CE bit - no congestion
IP: Total length    = 1500 bytes
IP: Identification  = 36920
IP: Flags           = 2X
IP:       .0.. ....   = may fragment
IP:       ..1. ....   = more fragments
IP: Fragment offset = 1480 bytes
IP: Time to live    = 128 seconds/hops
IP: Protocol        = 1 (ICMP)
IP: Header checksum = 3327 (correct)
IP: Source address      = [141.29.155.91]
IP: Destination address = [141.29.155.114]
IP: No options
IP:
IP: [1480 bytes of continuation data]
IP:
```

Exemplo de fragmentação IP (3)

No.	Status	Source Address	Dest Address	Summary	Len (By	Delta Time
1	M	[141.29.155.91]	[141.29.155.114]	ICMP: Echo	1514	0.000.000
2		[141.29.155.91]	[141.29.155.114]	IP: Continuation of frame 1; 1500 Bytes of dat IP: D=[141.29.155.114] S=[141.29.155.91] LEN=	1514	0.000.106
3		[141.29.155.91]	[141.29.155.114]	IP: Continuation of frame 1; 1468 Bytes of dat IP: D=[141.29.155.114] S=[141.29.155.91] LEN=	1482	0.000.109
4		[141.29.155.114]	[141.29.155.91]	ICMP: Echo reply	1514	0.000.954
5		[141.29.155.114]	[141.29.155.91]	IP: Continuation of frame 4; 1500 Bytes of dat IP: D=[141.29.155.91] S=[141.29.155.114] LEN=	1514	0.000.107
6		[141.29.155.114]	[141.29.155.91]	IP: Continuation of frame 4; 1468 Bytes of dat IP: D=[141.29.155.91] S=[141.29.155.114] LEN=	1482	0.000.116

```
IP: Continuation of frame 1
    IP: ----- IP Header -----
    IP:
    IP: Version = 4, header length = 20 bytes
    IP: Type of service = 00
    IP:       000. ....   = routine
    IP:       ...0 ....   = normal delay
    IP:       .... 0...   = normal throughput
    IP:       .... .0..   = normal reliability
    IP:       .... ..0.   = ECT bit - transport protocol will ignore the CE bit
    IP:       .... ...0   = CE bit - no congestion
    IP: Total length    = 1468 bytes
    IP: Identification  = 36920
    IP: Flags           = 0X
    IP:       .0.. ....   = may fragment
    IP:       ..0. ....   = last fragment
    IP: Fragment offset = 2960 bytes
    IP: Time to live    = 128 seconds/hops
    IP: Protocol        = 1 (ICMP)
    IP: Header checksum = 528E (correct)
    IP: Source address      = [141.29.155.91]
    IP: Destination address = [141.29.155.114]
    IP: No options
    IP:
    IP: [1448 bytes of continuation data]
    IP:
```

Opções IP (1)

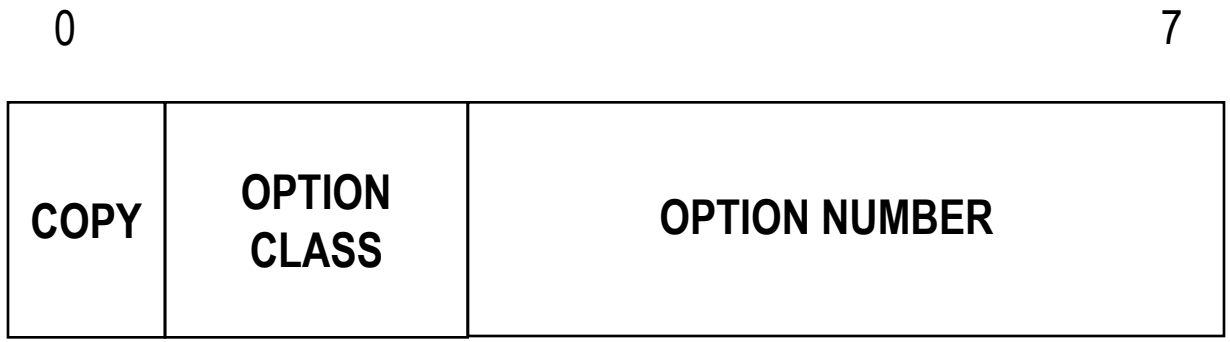


- Loose Source Routing (83h) - Caminho do datagrama com eventuais saltos
- Strict Source Routing (89h) - Caminho exacto a percorrer pelo datagrama
- Record Route (07h) - “Grava” o caminho percorrido
- Time Stamp (44h) - Determina o tempo calculado no percurso
- Stream Identifier - Identifica o tipo de dados transportados no datagrama (obsoleta)
- Security Handling - Os dados poderão estar cifrados ou apenas acessíveis para um grupo específico (uso militar)
- No Operation (01h) - Para as opções serem múltiplas de 32 bits (padding - 1 byte)
- End Option List (00h) - Marca o fim da lista de opções (padding - 1 byte)

- Tamanho máximo de 40 bytes visto que o header IP tem no máximo 60 bytes (15x4)

Opções IP (2)

- Campo **Option Code**

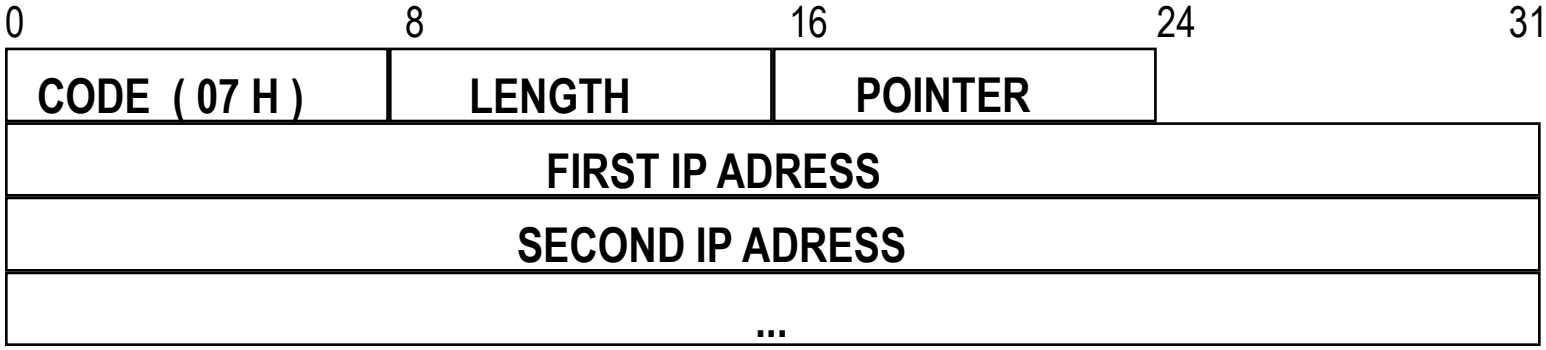


COPY:
1 - A opção deve ser copiada para todos os fragmentos
0 - A opção deve ser apenas copiada para o primeiro fragmento

OPTION CLASS :
0 - Datagram or Network Control
1 - Reservada
2 - *Debugging* e Medida
3 - Reservada

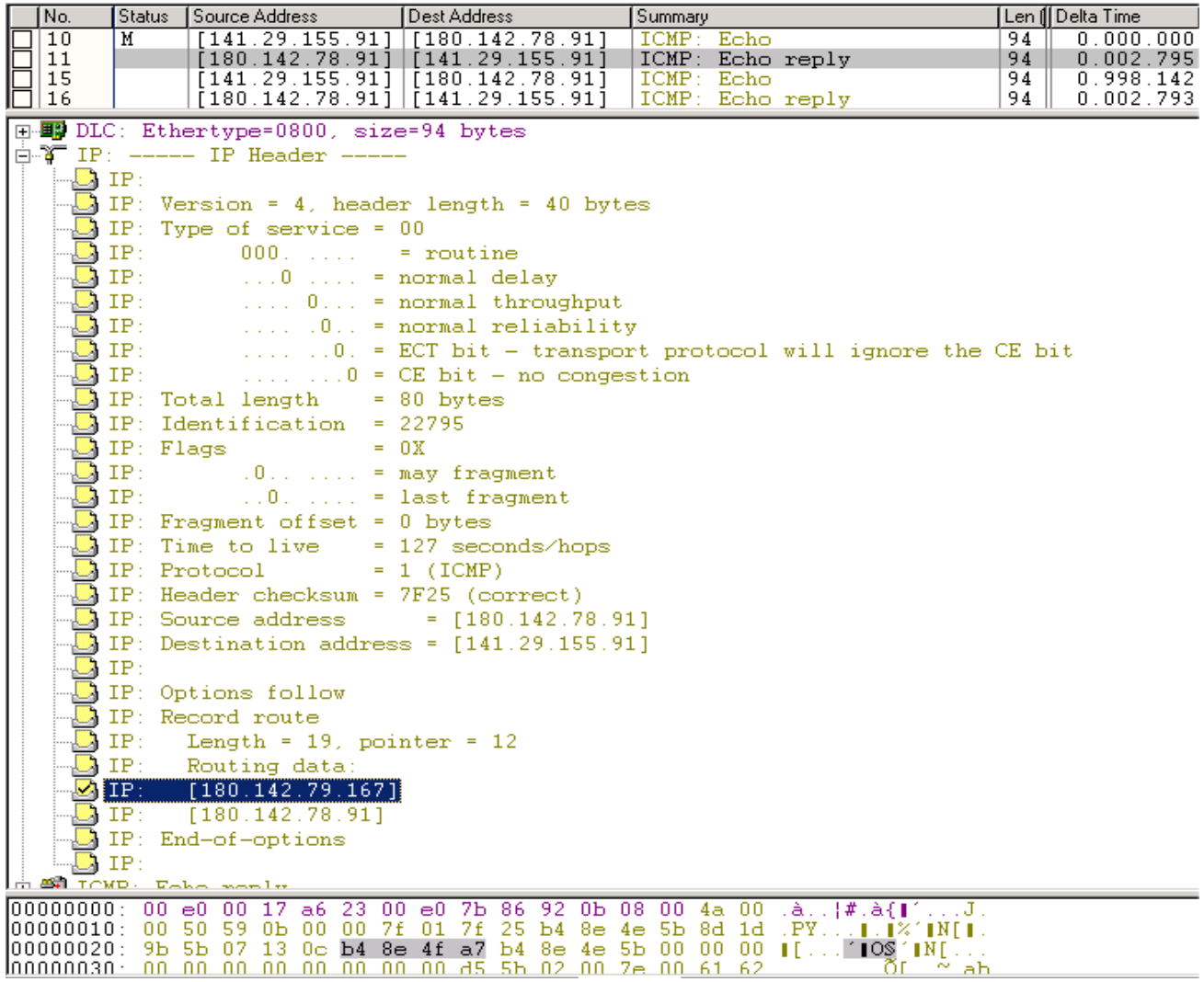
Opções IP (3)

- RECORD ROUTE



- POINTER - Indica a próxima posição livre na lista de IP

Opções IP – *Record Route*



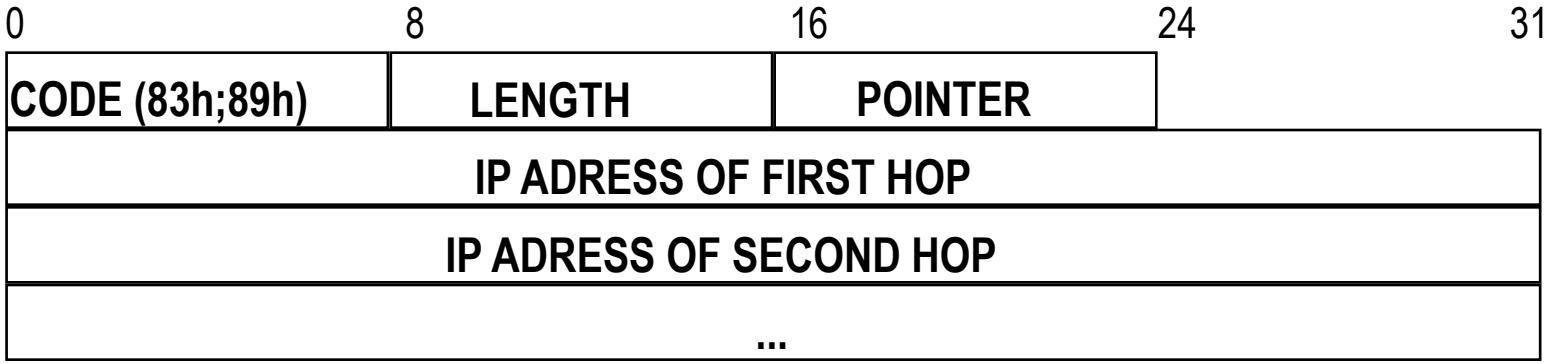
No.	Status	Source Address	Dest Address	Summary	Len	Delta Time
10	M	[141.29.155.91]	[180.142.78.91]	ICMP: Echo	94	0.000.000
11		[180.142.78.91]	[141.29.155.91]	ICMP: Echo reply	94	0.002.795
15		[141.29.155.91]	[180.142.78.91]	ICMP: Echo	94	0.998.142
16		[180.142.78.91]	[141.29.155.91]	ICMP: Echo reply	94	0.002.793

```
DLC: Ethertype=0800, size=94 bytes
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 40 bytes
IP: Type of service = 00
IP:       000. ....   = routine
IP:       ...0 ....   = normal delay
IP:       .... 0...   = normal throughput
IP:       .... .0..   = normal reliability
IP:       .... ..0.   = ECT bit - transport protocol will ignore the CE bit
IP:       .... ...0   = CE bit - no congestion
IP: Total length    = 80 bytes
IP: Identification  = 22795
IP: Flags           = 0X
IP:       .0.. ....   = may fragment
IP:       ..0. ....   = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live    = 127 seconds/hops
IP: Protocol        = 1 (ICMP)
IP: Header checksum = 7F25 (correct)
IP: Source address      = [180.142.78.91]
IP: Destination address = [141.29.155.91]
IP:
IP: Options follow
IP: Record route
IP:   Length = 19, pointer = 12
IP:   Routing data:
IP:     [180.142.79.167]
IP:     [180.142.78.91]
IP: End-of-options
IP:
ICMP: Echo reply
```

```
00000000: 00 e0 00 17 a6 23 00 e0 7b 86 92 0b 08 00 4a 00  .à..¦#.à{▮´...J.
00000010: 00 50 59 0b 00 00 7f 01 7f 25 b4 8e 4e 5b 8d 1d  .PY...▮.▮%´▮N[▮.
00000020: 9b 5b 07 13 0c b4 8e 4f a7 b4 8e 4e 5b 00 00 00  ▮[...´▮O§´▮N[...
00000030: 00 00 00 00 00 00 00 00 d5 5b 02 00 7e 00 61 62            Õ[  ~ ab
```

Opções IP (4)

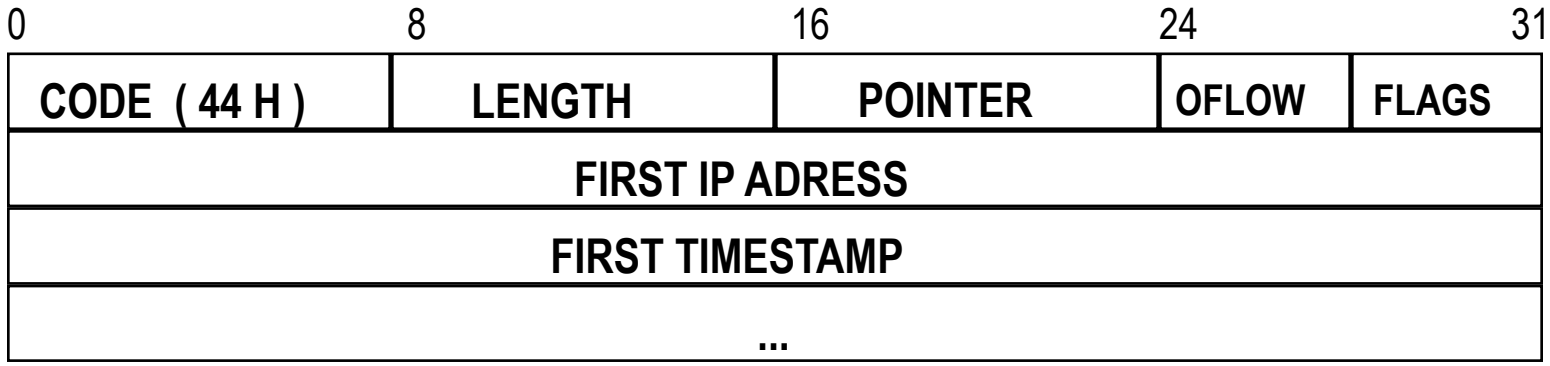
- SOURCE ROUTE



- POINTER - Indica a posição na lista do endereço IP que deve ser analisado e seguido no próximo *router*

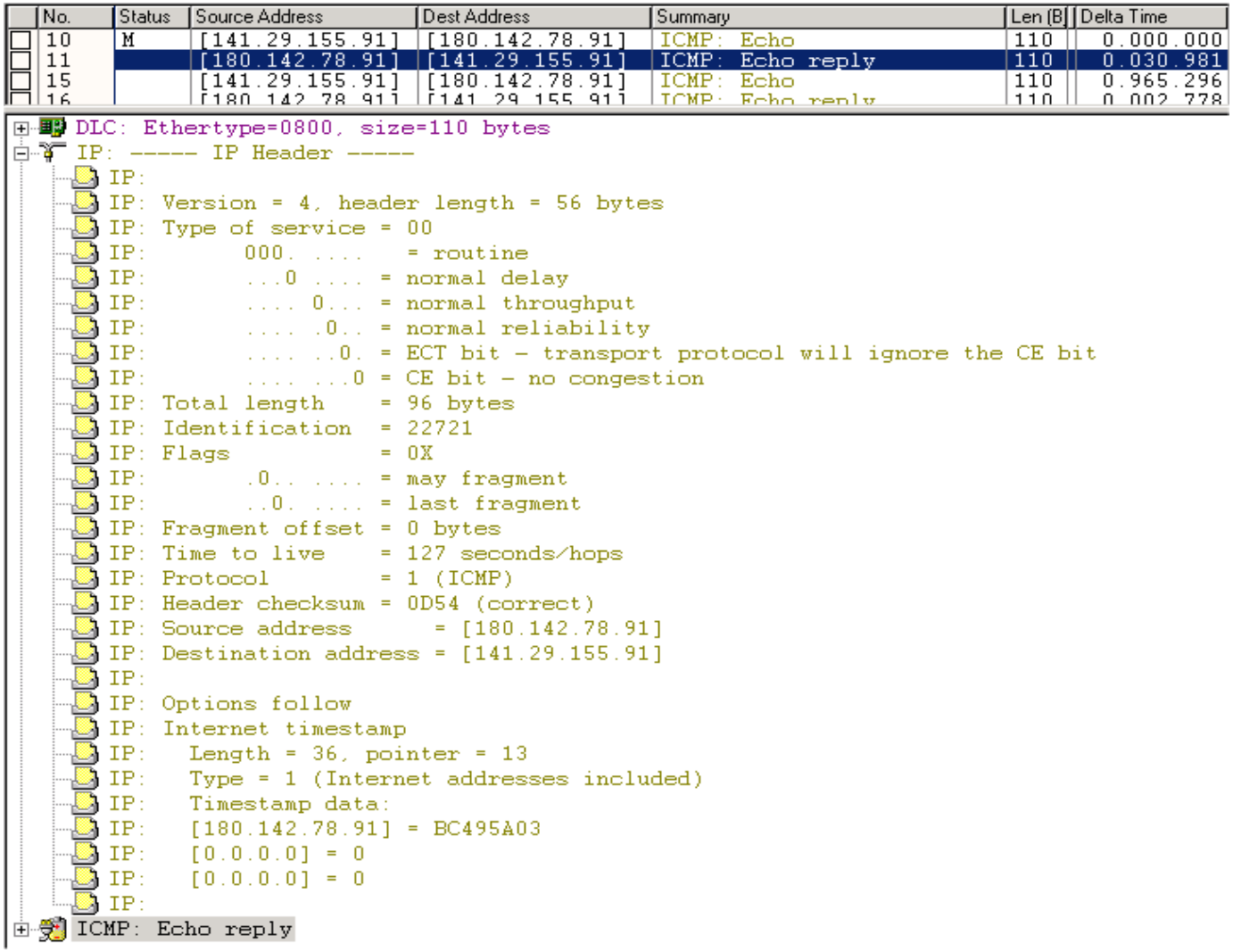
Opções IP (5)

- TIMESTAMP



FLAGS	Significado
0 0	*Gateways* preenchem apenas *Timestamp.*
0 1	*Gateways* preenchem *Timestamp* e endereço IP.
1 1	Endereço IP colocado pelo emissor. Apenas preenchem o Timestamp as Gateways que constarem na lista de IPs.

Opções IP – *Timestamp*



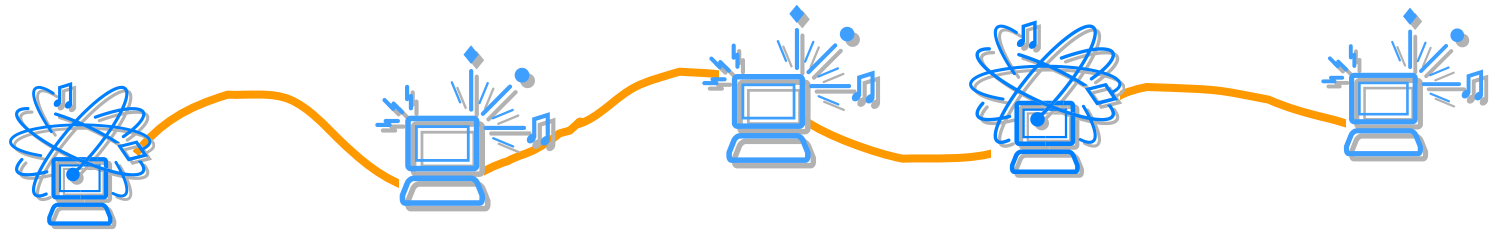
No.	Status	Source Address	Dest Address	Summary	Len (B)	Delta Time
10	M	[141.29.155.91]	[180.142.78.91]	ICMP: Echo	110	0.000.000
11		[180.142.78.91]	[141.29.155.91]	ICMP: Echo reply	110	0.030.981
15		[141.29.155.91]	[180.142.78.91]	ICMP: Echo	110	0.965.296
16		[180.142.78.91]	[141.29.155.91]	ICMP: Echo reply	110	0.002.778

```
DLC: Ethertype=0800, size=110 bytes
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 56 bytes
IP: Type of service = 00
IP:       000. ....   = routine
IP:       ...0 ....   = normal delay
IP:       .... 0...   = normal throughput
IP:       .... .0..   = normal reliability
IP:       .... ..0.   = ECT bit - transport protocol will ignore the CE bit
IP:       .... ...0   = CE bit - no congestion
IP: Total length    = 96 bytes
IP: Identification  = 22721
IP: Flags           = 0X
IP:       .0.. ....   = may fragment
IP:       ..0. ....   = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live    = 127 seconds/hops
IP: Protocol        = 1 (ICMP)
IP: Header checksum = 0D54 (correct)
IP: Source address      = [180.142.78.91]
IP: Destination address = [141.29.155.91]
IP:
IP: Options follow
IP: Internet timestamp
IP:   Length = 36, pointer = 13
IP:   Type = 1 (Internet addresses included)
IP:   Timestamp data:
IP:   [180.142.78.91] = BC495A03
IP:   [0.0.0.0] = 0
IP:   [0.0.0.0] = 0
IP:
ICMP: Echo reply
```

Sumário

- Endereços IP – Generalidades
- Protocolo IP
- Fragmentação de pacotes IP
- Opções IP

Camada de Rede: Protocolo ICMP



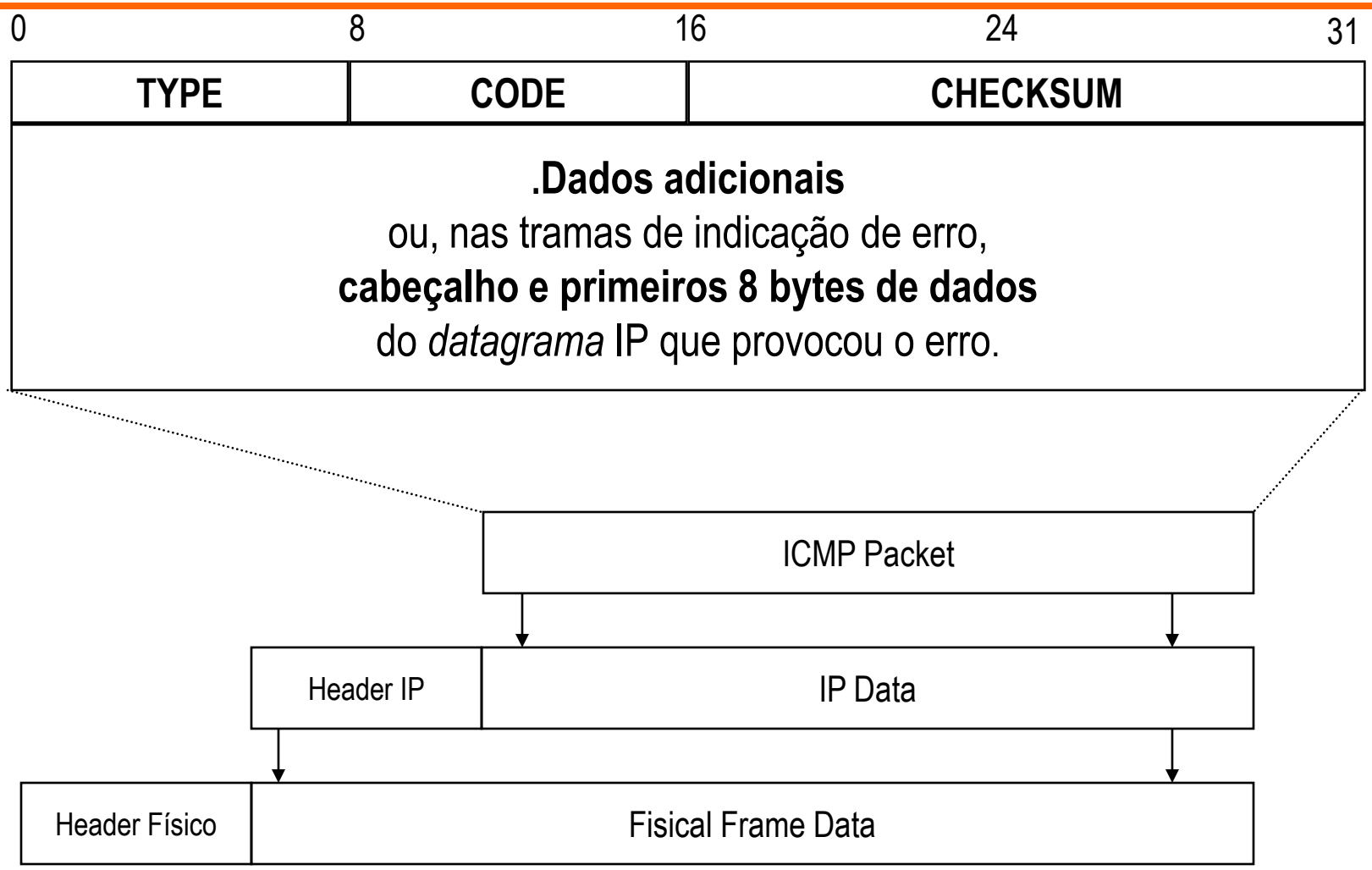
Instituto Superior de Engenharia de Lisboa
Departamento de Engenharia, Electrónica, Telecomunicações e Computadores
Redes de Computadores

Internet Control Message Protocol - ICMP

- Funcionalidades
  - Informar máquina de origem da ocorrência de erros
  - Detectar problemas e falhas na rede
  - Configuração de Routers e máquinas

- Características
  - Implementado juntamente com o IP
  - Transportado num datagrama IP
  - Não permite informar os routers intermédios
  - Não especifica o que fazer quando há erros

Formato da trama ICMP



Formato da trama ICMP (2)

- Campos
  - Type
  - Code

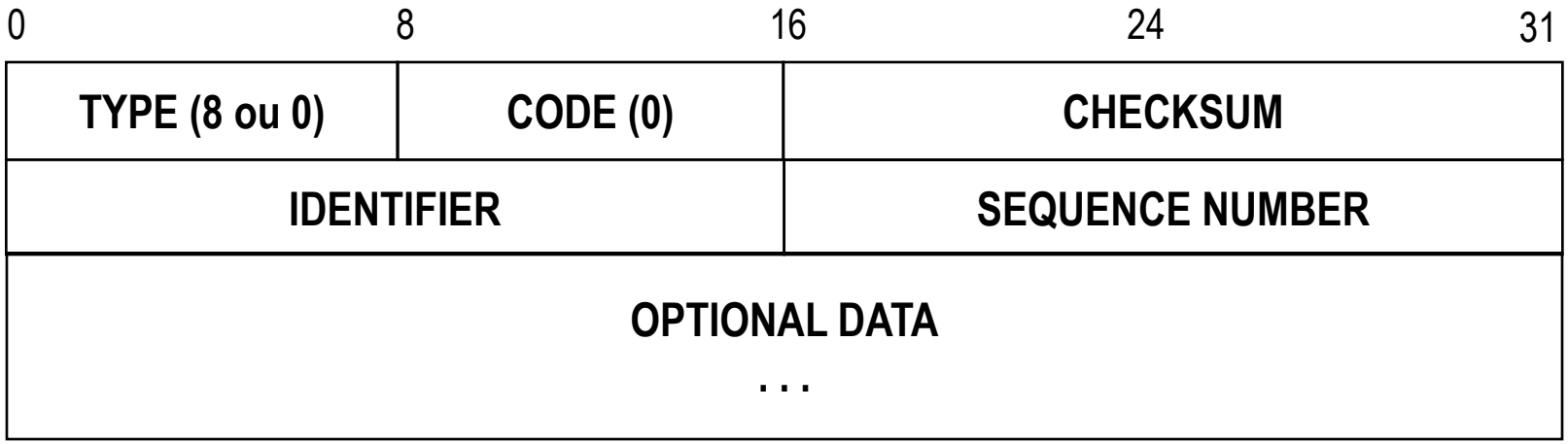
Type	Code	Description
0		Echo reply.
3	0	Net unreachable.
3	1	Host unreachable.
3	2	Protocol unreachable.
3	3	Port unreachable.
3	4	Fragmentation needed and DF set.
3	5	Source route failed.
4		Source quench.
5	0	Redirect datagrams for the network.
5	1	Redirect datagrams for the host.
5	2	Redirect datagrams for the type of service and network.
5	3	Redirect datagrams for the type of service and host.
8		Echo request.
11	0	Time to live exceeded in transit.
11	1	Fragment reassemble time exceeded.
12		Parameter problem.
13		Timestamp.
14		Timestamp reply.
15		Information request.
16		Information reply.
17		Address Mask Request
18		Address Mask Reply

Tramas ICMP (1)

- Echo Request / Reply
  - Mensagens para funções de teste e controlo da rede
    - Usadas pelo comando PING
- Destination Unreachable
  - Enviado por um router que deita fora um Datagrama
    (nem todos os datagramas perdidos são detectados)
    - CODE - Indica a razão da perda do datagrama
- Timestamp Request / Reply
  - Mensagens para sincronização dos relógios das máquinas

Tramas ICMP (2)

- Echo Request/Reply



- IDENTIFIER - Distingue entre aplicações na mesma máquina
- SEQ. NUMBER - Distingue entre mensagens da mesma aplicação
- O comando ping usa estas tramas

Comando Ping

- Usado para:
  - testar se um destino é atingivel por IP
  - Calcular o round trip time (RTT)
  - contar o número de hops para o destino (usa o TTL)
  - Pode usar a opção de record route.

- Exemplo de output:
  - Reply from 164.107.144.3: 48 bytes in 47 msec. TTL: 253

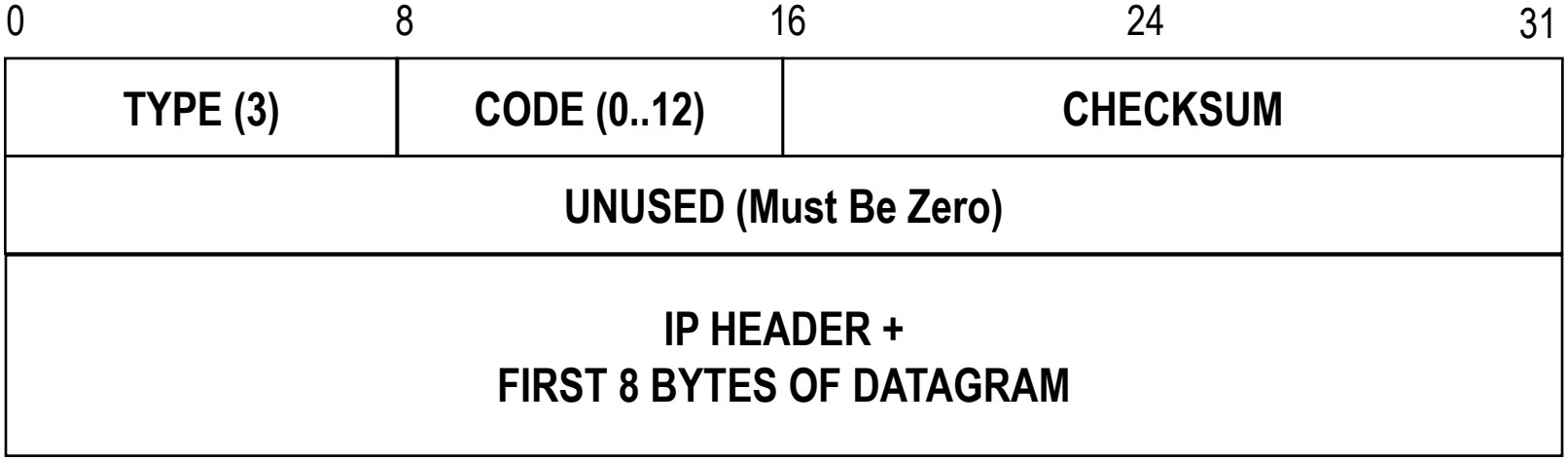
Comando PING

```
Usage: ping [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] destination-list

Options:
  -a            Resolve addresses to hostnames.
  -n count      Number of echo requests to send.
  -l size       Send buffer size.
  -f            Set Don't Fragment flag in packet.
  -i TTL        Time To Live.
  -v TOS        Type Of Service.
  -r count      Record route for count hops.
  -s count      Timestamp for count hops.
  -j host-list  Loose source route along host-list.
  -k host-list  Strict source route along host-list.
  -w timeout    Timeout in milliseconds to wait for each reply.
```

Tramas ICMP (3)

- Destination Unreachable (Type 3)

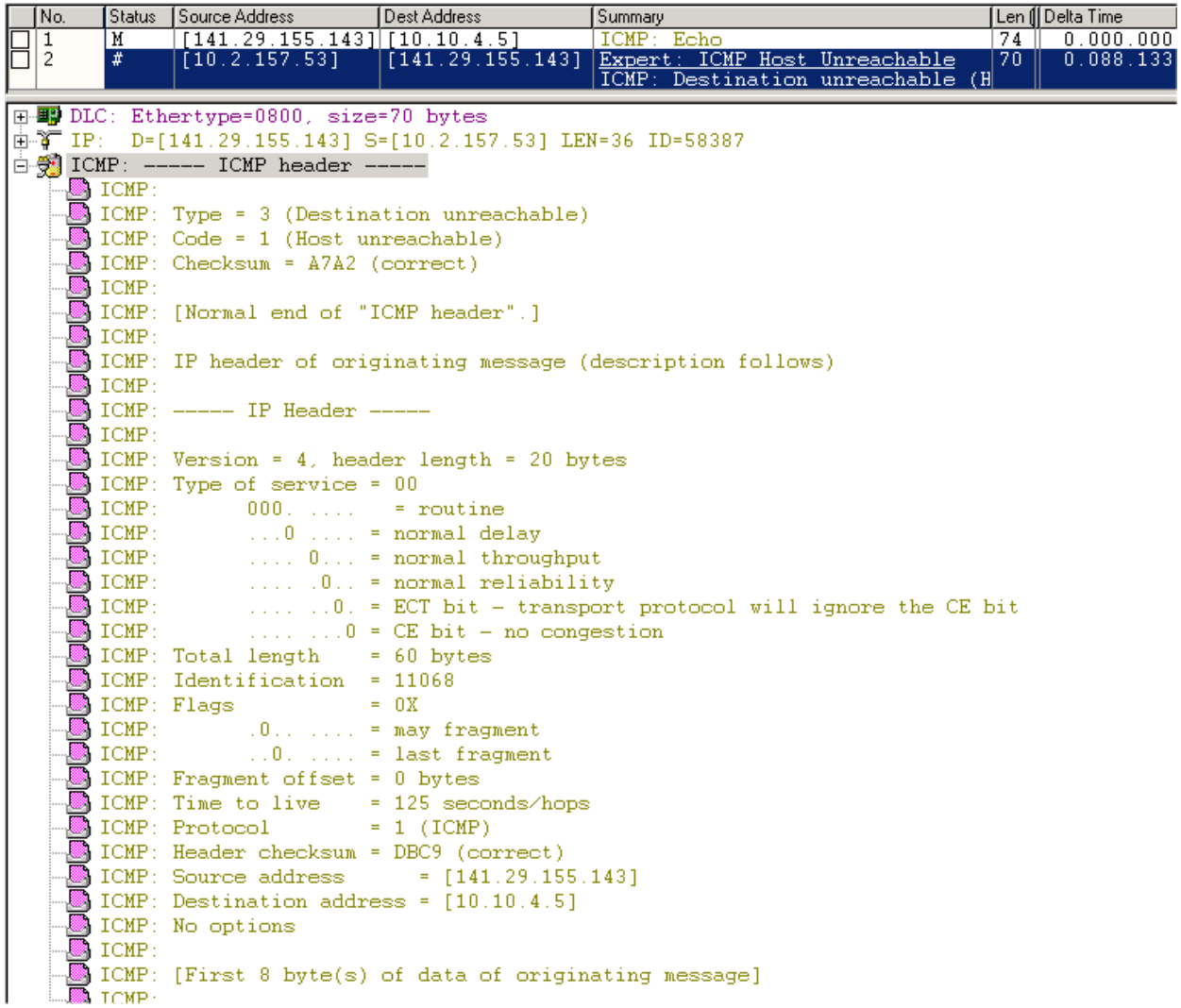


- Code

0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation needed and DF set
5	Source Route Failed
6	Destination Network Unknown

7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network Administratively Prohibited
10	Communication with Destination Host Administratively Prohibited
11	Network Unreachable for type of service
12	Host Unreachable for type of service

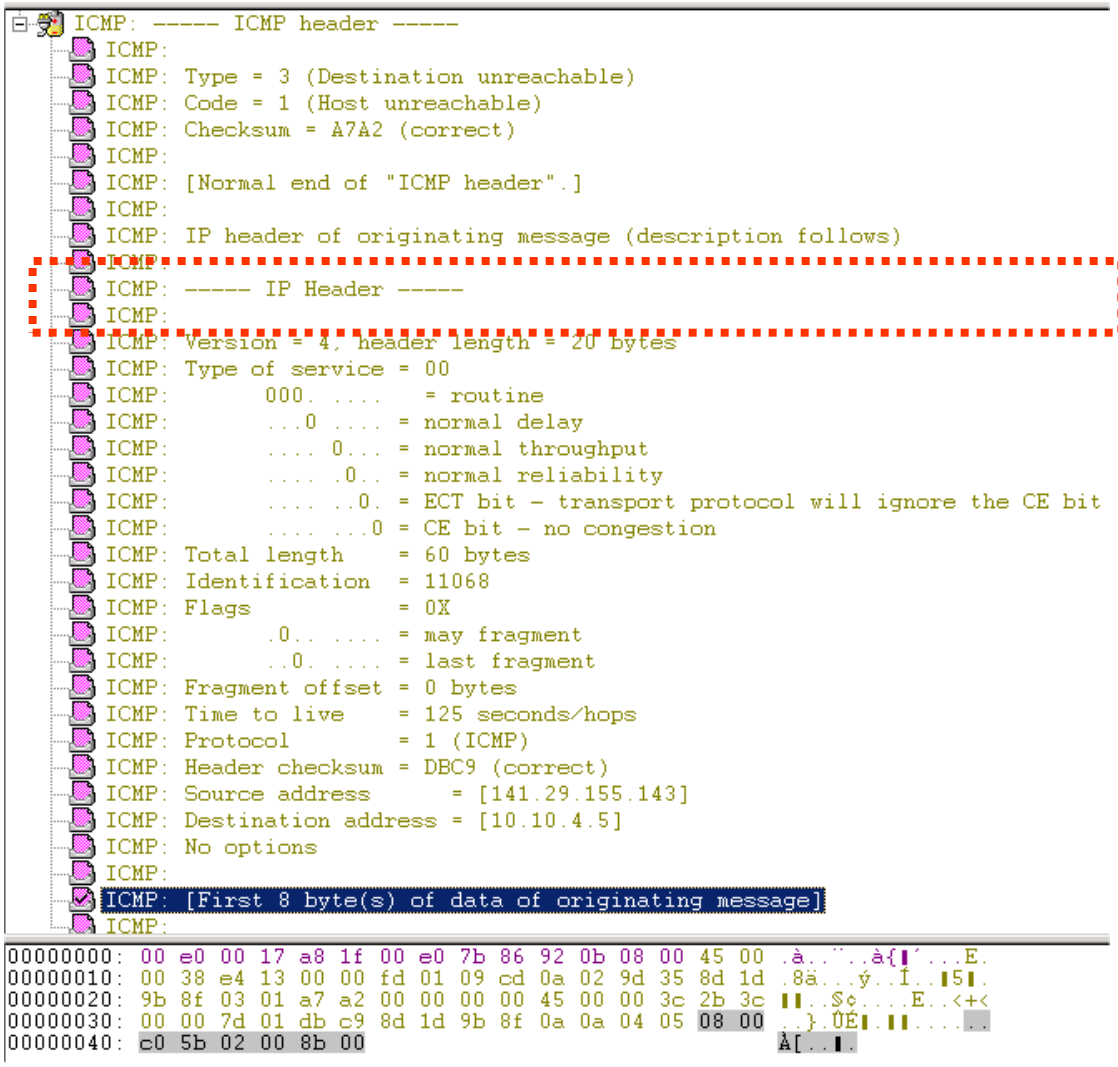
ICMP Destination Unreachable (Type 3)



No.	Status	Source Address	Dest Address	Summary	Len	Delta Time
1	M	[141.29.155.143]	[10.10.4.5]	ICMP: Echo	74	0.000.000
2	#	[10.2.157.53]	[141.29.155.143]	Expert: ICMP Host Unreachable ICMP: Destination unreachable (H	70	0.088.133

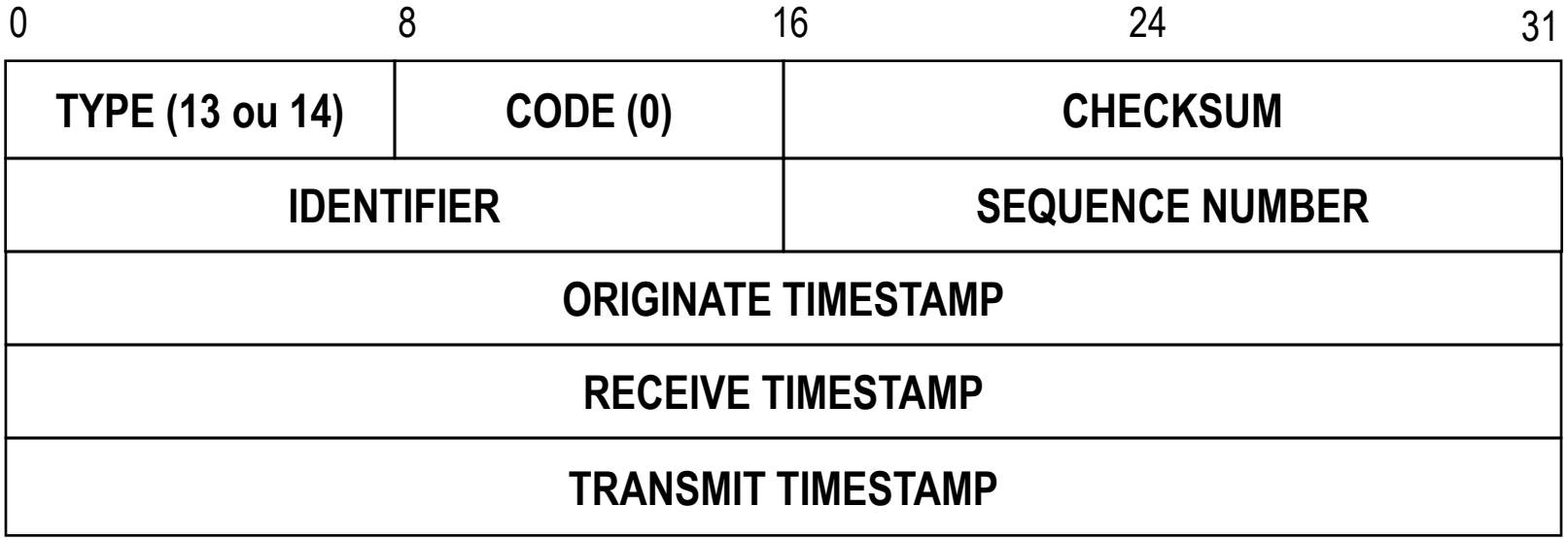
```
DLC: Ethertype=0800, size=70 bytes
IP:  D=[141.29.155.143] S=[10.2.157.53] LEN=36 ID=58387
ICMP: ----- ICMP header -----
ICMP:
ICMP: Type = 3 (Destination unreachable)
ICMP: Code = 1 (Host unreachable)
ICMP: Checksum = A7A2 (correct)
ICMP:
ICMP: [Normal end of "ICMP header".]
ICMP:
ICMP: IP header of originating message (description follows)
ICMP:
ICMP: ----- IP Header -----
ICMP:
ICMP: Version = 4, header length = 20 bytes
ICMP: Type of service = 00
ICMP:       000. ....   = routine
ICMP:       ...0 ....   = normal delay
ICMP:       .... 0...   = normal throughput
ICMP:       .... .0..   = normal reliability
ICMP:       .... ..0.   = ECT bit - transport protocol will ignore the CE bit
ICMP:       .... ...0   = CE bit - no congestion
ICMP: Total length    = 60 bytes
ICMP: Identification  = 11068
ICMP: Flags           = 0X
ICMP:       .0.. ....   = may fragment
ICMP:       ..0. ....   = last fragment
ICMP: Fragment offset = 0 bytes
ICMP: Time to live    = 125 seconds/hops
ICMP: Protocol        = 1 (ICMP)
ICMP: Header checksum = DBC9 (correct)
ICMP: Source address      = [141.29.155.143]
ICMP: Destination address = [10.10.4.5]
ICMP: No options
ICMP:
ICMP: [First 8 byte(s) of data of originating message]
ICMP:
```

Cabeçalho IP + 8 bytes dos dados



Tramas ICMP (4)

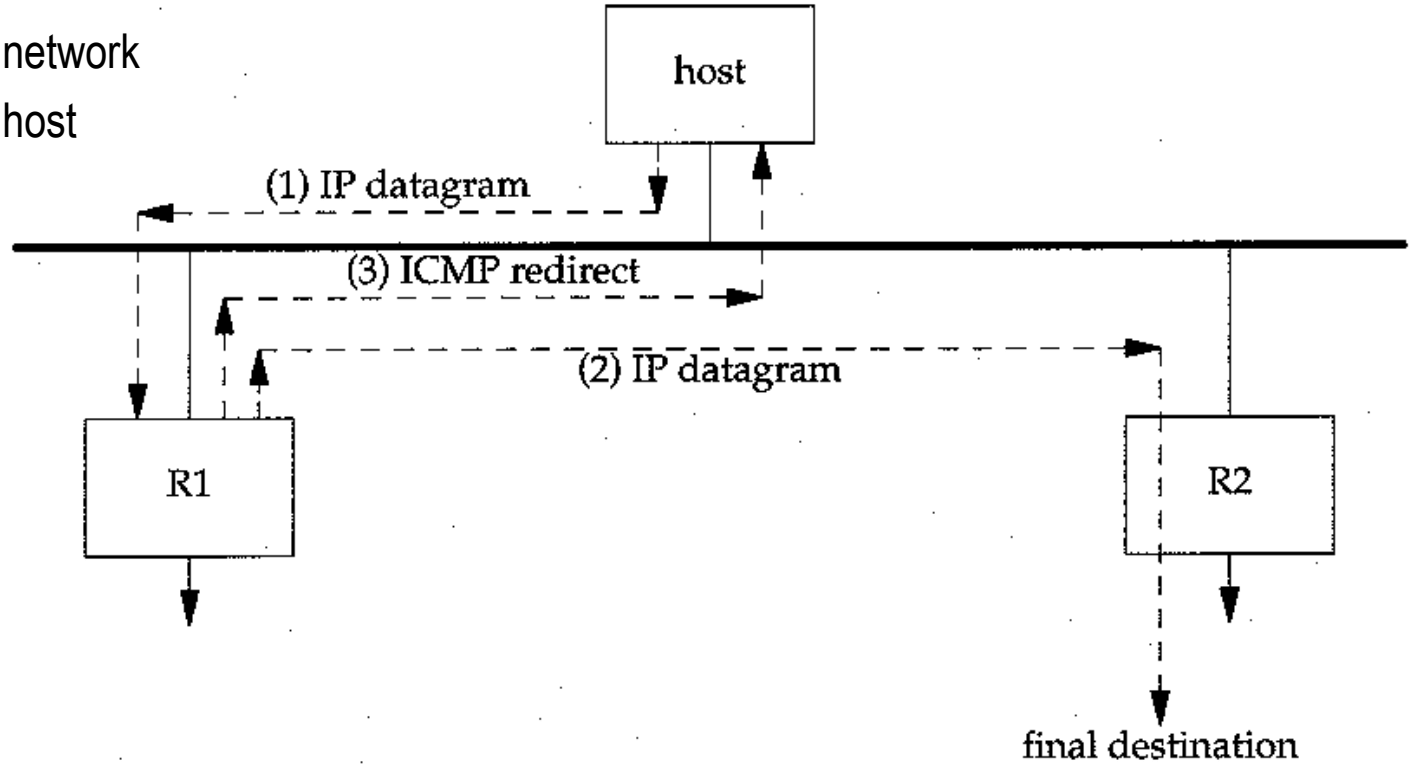
- Timestamp Request/Reply



- IDENTIFIER - Distingue entre aplicações na mesma máquina
- SEQ. NUMBER - Distingue entre mensagens da mesma aplicação
- Usado para sincronização de relógio entre máquinas

Tramas ICMP (5)

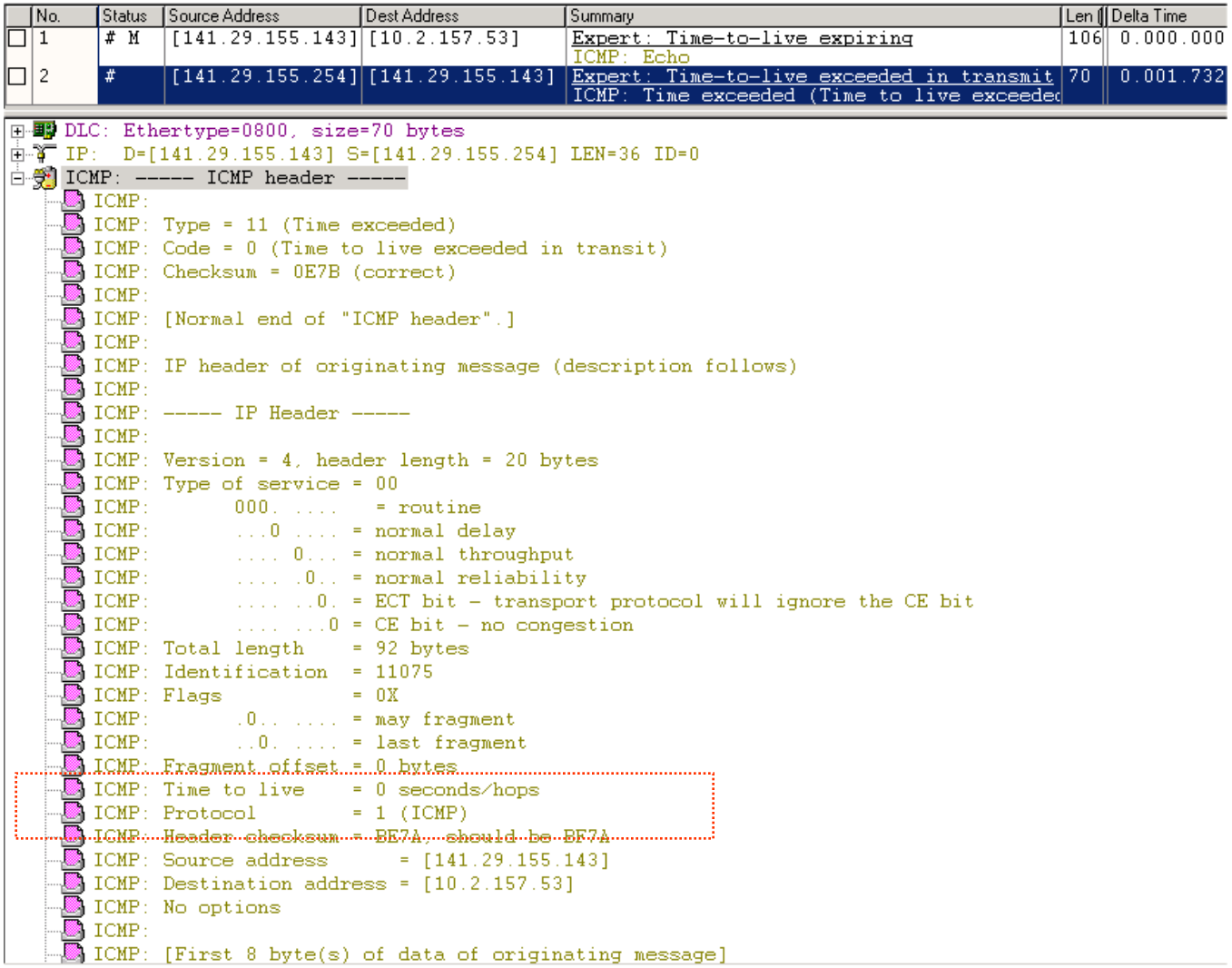
- Redirect
  - O router informa que o datagrama devia ter sido enviado para outro router
    - CODE
      - 0 - network
      - 1 - host



Tramas ICMP (6)

- Time Exceeded for a Datagram
  - O campo TTL do datagrama chegou a zero
    - CODE = 0 - em trânsito (router decrementa 1 unidade)
    - CODE = 1 - no processamento (router decrementa mais que 1 unidade)
- Address Mask Request / Reply
  - Para uma máquina diskless pedir a sua máscara de rede (usado em conjunto com o protocolo RARP)
- Parameter Problem on a datagram
  - Problemas não contemplados nas outras mensagens ICMP

ICMP Time-to-live exceeded in transit



No.	Status	Source Address	Dest Address	Summary	Len	Delta Time
1	# M	[141.29.155.143]	[10.2.157.53]	Expert: Time-to-live expiring ICMP: Echo	106	0.000.000
2	#	[141.29.155.254]	[141.29.155.143]	Expert: Time-to-live exceeded in transmit ICMP: Time exceeded (Time to live exceeded	70	0.001.732

```
DLC: Ethertype=0800, size=70 bytes
IP:  D=[141.29.155.143] S=[141.29.155.254] LEN=36 ID=0
ICMP: ----- ICMP header -----
ICMP:
ICMP: Type = 11 (Time exceeded)
ICMP: Code = 0 (Time to live exceeded in transit)
ICMP: Checksum = 0E7B (correct)
ICMP:
ICMP: [Normal end of "ICMP header".]
ICMP:
ICMP: IP header of originating message (description follows)
ICMP:
ICMP: ----- IP Header -----
ICMP:
ICMP: Version = 4, header length = 20 bytes
ICMP: Type of service = 00
ICMP:       000. ....   = routine
ICMP:       ...0 ....   = normal delay
ICMP:       .... 0...   = normal throughput
ICMP:       .... .0..   = normal reliability
ICMP:       .... ..0.   = ECT bit - transport protocol will ignore the CE bit
ICMP:       .... ...0   = CE bit - no congestion
ICMP: Total length    = 92 bytes
ICMP: Identification  = 11075
ICMP: Flags           = 0X
ICMP:       .0.. ....   = may fragment
ICMP:       ..0. ....   = last fragment
ICMP: Fragment offset = 0 bytes
ICMP: Time to live    = 0 seconds/hops
ICMP: Protocol        = 1 (ICMP)
ICMP: Header checksum = BE7A, should be BF7A
ICMP: Source address      = [141.29.155.143]
ICMP: Destination address = [10.2.157.53]
ICMP: No options
ICMP:
ICMP: [First 8 byte(s) of data of originating message]
```

Path MTU Discovery

- Path MTU – mais pequeno MTU num caminho entre duas máquinas

- Mecanismo “Path MTU Discovery” pode ser usado no TCP e UDP:
  - Enviar datagramas grandes de teste com a flag “Don’t fragment” activa
  - Se o datagrama precisar de ser fragmentado serão recebidas mensagens ICMP
  - Reduzir o tamanho até não serem recebidas mensagens ICMP
  - Enviar datagramas de dados com a dimensão máxima encontrada

Sumário

- Funcionalidades ICMP
- Mensagens ICMP