



# Reti di Calcolatori I

Prof. Roberto Canonico

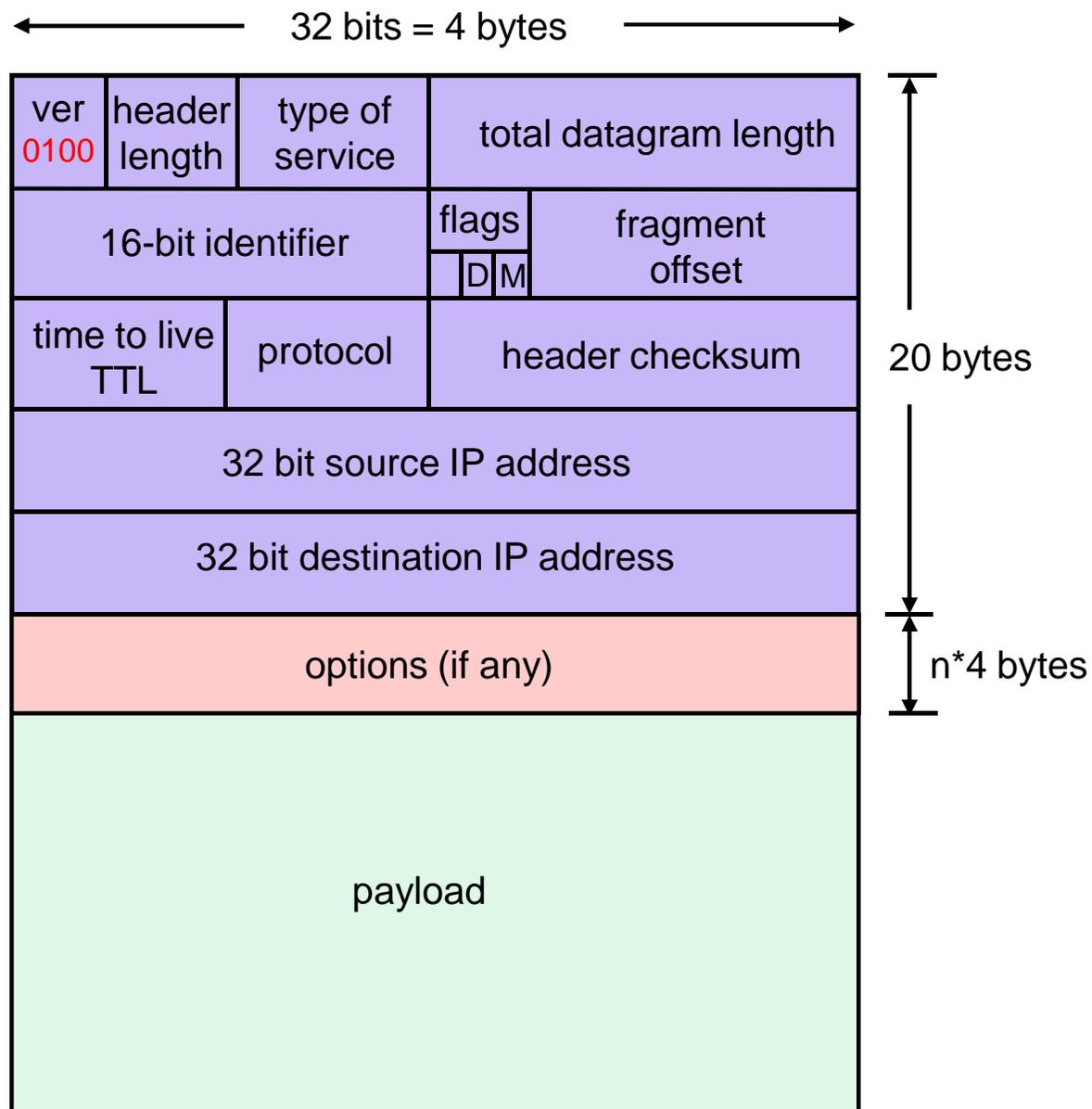
Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione

Corso di Laurea in Ingegneria delle Telecomunicazioni

Corso di Laurea in Ingegneria dell'Automazione

A.A. 2017-2018

# Struttura di un datagram IP versione 4



# Campi dell'header IP versione 4

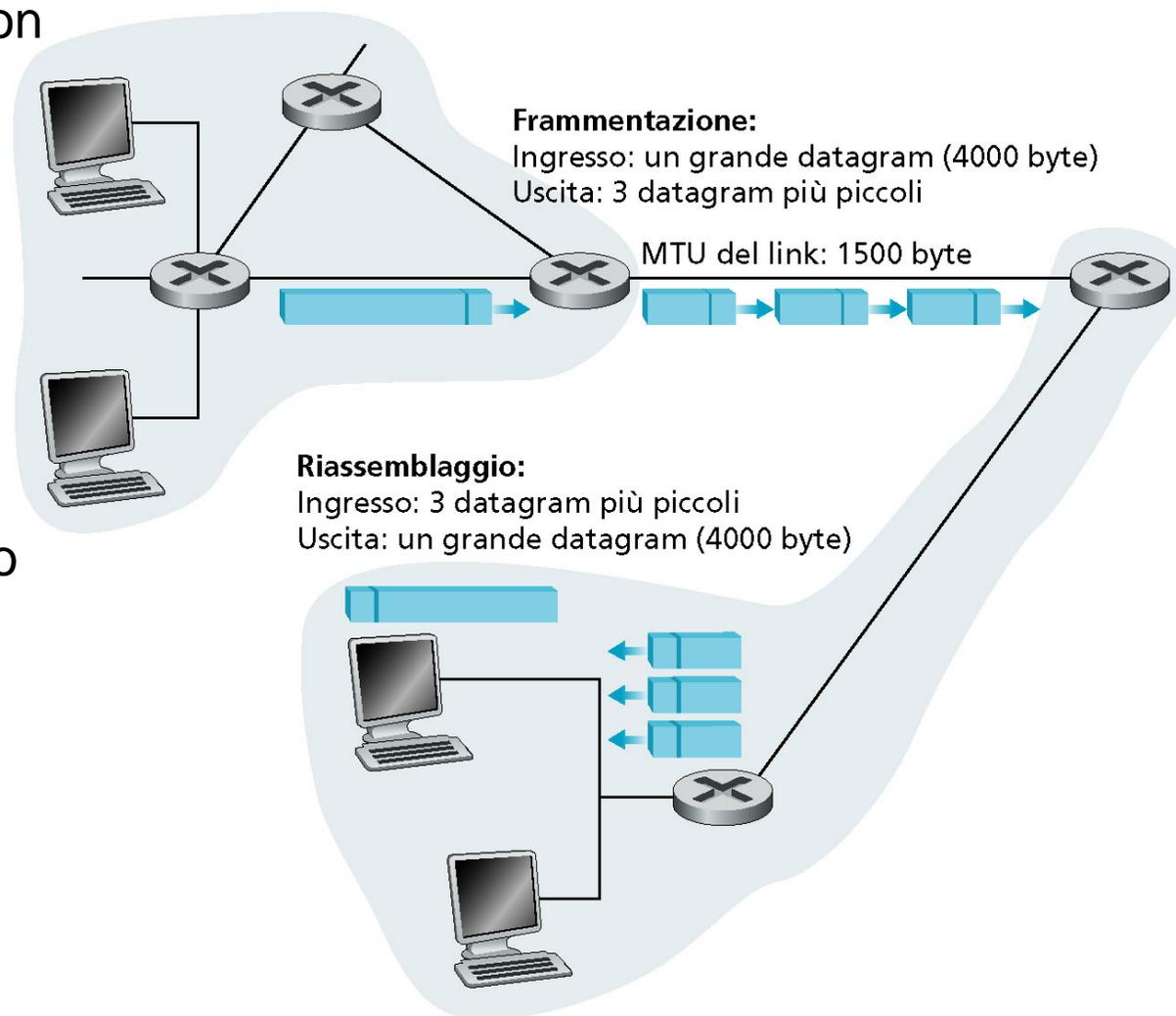
- In IPv4 l'**header** è costituito da una parte a struttura fissa (20 byte) ed una opzionale di lunghezza multipla di 4 byte
- **IP header length (4 bit)**: lunghezza dell'header, in multipli di 32 bit (max 60 byte)
- **Type-of-Service (8 bit)**: specifica il tipo di servizio che si richiede alla rete
  - usato, in pratica, per scopi differenti
- **Total length (16 bit)**: indica la lunghezza in byte dell'intero pacchetto (header+dati)
- **Time-to-live TTL (8 bit)**: numero residuo di router attraversabili
  - viene decrementato di 1 da ogni router, a 0 il pacchetto viene scartato
  - serve, in caso di percorsi circolari (*loop*), ad evitare che un pacchetto resti perennemente in circolo
- **Protocol (8 bit)**: indica il protocollo di livello superiore associato al payload
  - il valore 6 indica TCP, 17 indica UDP
  - serve al de-multiplexing dei pacchetti a destinazione
- **Header checksum (16 bit)**: serve a verificare l'integrità dell'header IP
- **Source IP Address (32 bit)**: indirizzo IP del nodo mittente del pacchetto
- **Destination IP Address (32 bit)**: indirizzo IP del nodo destinatario del pacchetto
- **Identification (16 bit), Flags (3 bit), Fragment Offset (13 bit)**: sono usati in caso di frammentazione del pacchetto da parte di un router
  - consentono al nodo destinatario di ricostruire il pacchetto originario

# Campi Identification, Flags e Fragment offset

- Questi campi servono a gestire la frammentazione dei pacchetti IPv4
- Un pacchetto IPv4 può essere “spezzato” da un router in una sequenza di pacchetti che singolarmente viaggiano verso il destinatario
- Il livello IP del destinatario finale si occupa del “riassembaggio” del pacchetto originario prima di consegnarlo allo strato superiore
- Un pacchetto può essere frammentato anche più volte lungo il percorso
- La necessità di frammentare un pacchetto si presenta quando la dimensione del pacchetto supera la Maximum Transmissible Unit (MTU) sul link di uscita
- Il valore di MTU dipende dalla tecnologia usata al livello 2
  - Es. in Ethernet la MTU è 1500 byte
- **Identification**
  - Questo campo (16 bit) è un identificativo del datagramma
  - Serve ad associare diversi frammenti ad un unico pacchetto originario
- **Flags**
  - Il bit D (*don't fragment*) indica se il pacchetto può essere frammentato
  - Il bit M (*more fragments*) indica se il pacchetto è l'ultimo frammento
- **Fragment offset**
  - 13 bit, identifica la posizione del frammento all'interno del pacchetto

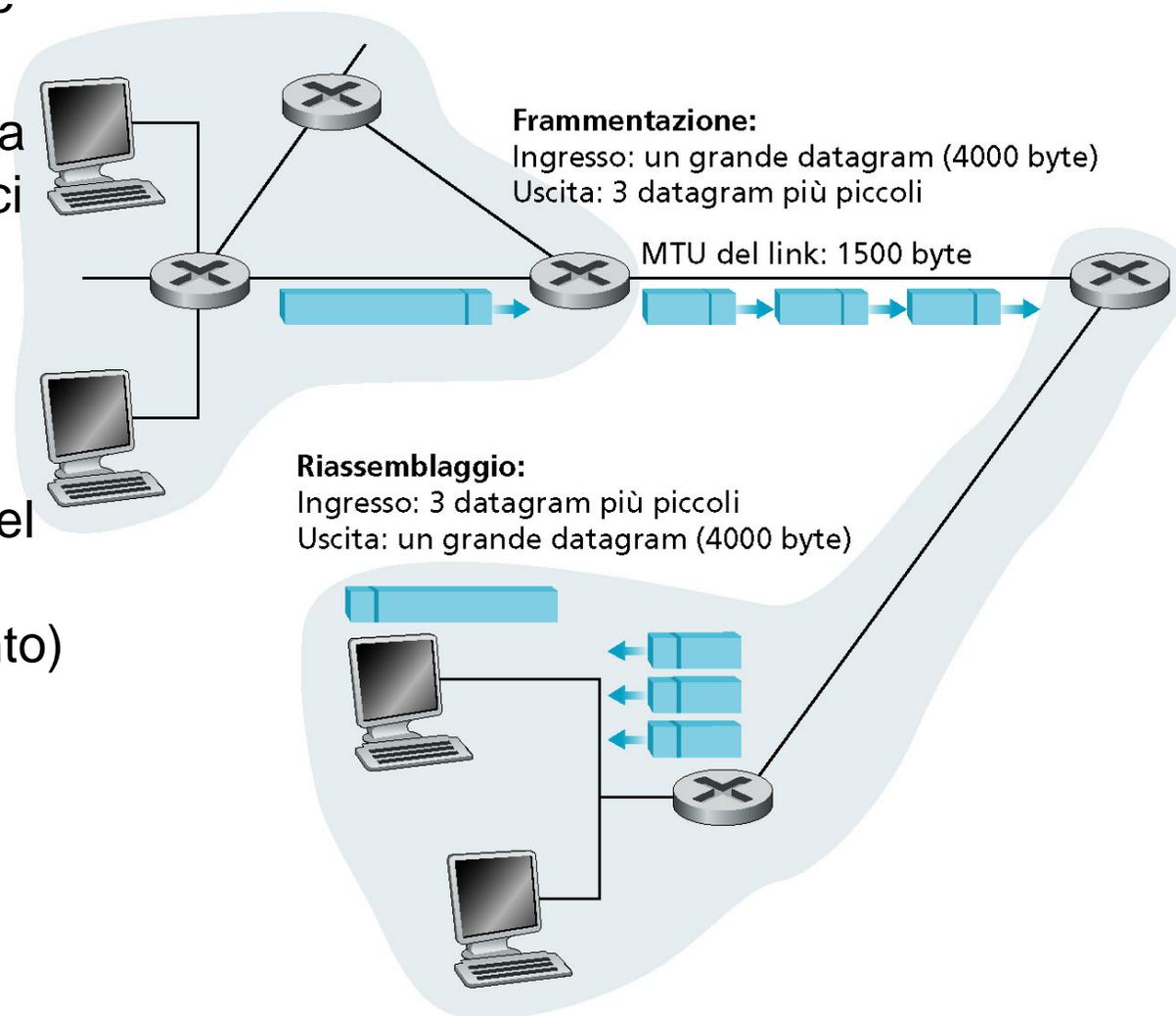
# Frammentazione e riassettaggio IP

- Se un pacchetto di dimensione  $N$  arriva ad un router e deve essere trasmesso su un link di uscita con MTU  $M < N$ , il pacchetto è **frammentato**
- Ogni frammento è trasmesso come singolo pacchetto IP
- La dimensione del payload di ogni frammento è un multiplo di 8 byte
- Tutti i frammenti hanno lo stesso ID number



## Frammentazione e riassetblaggio IP (2)

- Tutti i frammenti (tranne l'ultimo) hanno un payload di dimensione multipla di 8 byte
- Essendo la dimensione massima di un datagramma 65535 byte, ci possono essere al massimo  $65536/8$  cioè 8192 frammenti per ogni datagramma
- La posizione del payload di un frammento rispetto al payload del pacchetto originario è espressa mediante un offset (spiazzamento) di 13 bit



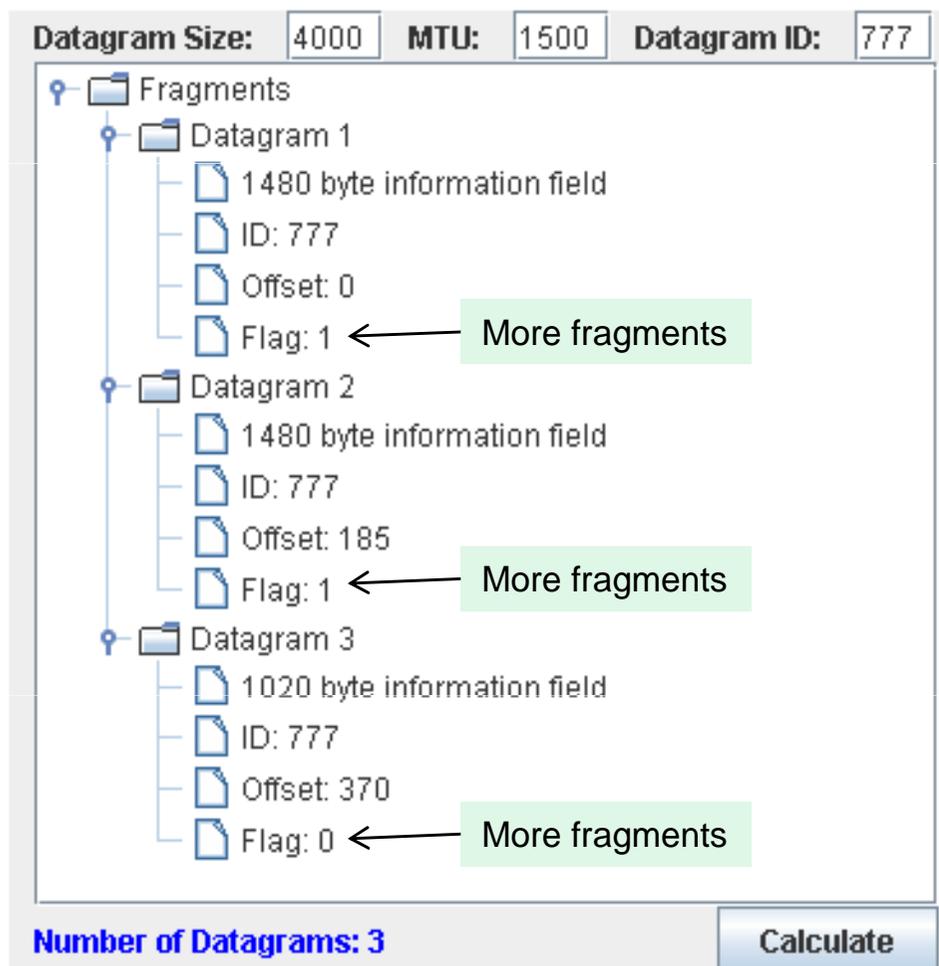
# Frammentazione IP: esempio 1

- N = 4000, MTU = 1500
- Tre frammenti, ciascuno con header 20 byte
- Frammento 1:
  - payload 1480
  - offset 0
- Frammento 2:
  - payload 1480
  - offset  $(1480/8)=185$
- Frammento 3:
  - payload 1020
  - offset  $(1480+1480)/8=370$

NOTA:

$$20+1480+1480+1020=4000$$

Note: Datagram size includes an IP header of 20 bytes.  
MTU and Datagram size must be greater than 30, and all values must be less than  $2^{16} - 1$  (65535).



This applet was coded by Ryan Gilbert in 2008, a student at Arizona State University.  
It replaces an applet coded by Albert Huang in 1997 as part of course work at the University of Pennsylvania.

# Frammentazione IP: esempio 2

- Il pacchetto IP raffigurato di seguito deve attraversare un link avente Maximum Transfer Unit (MTU) pari a 1500 bytes. Come verrà trattato?

## Original IP Datagram

Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0	345	5140	0	0	0

## IP Fragments (Ethernet)

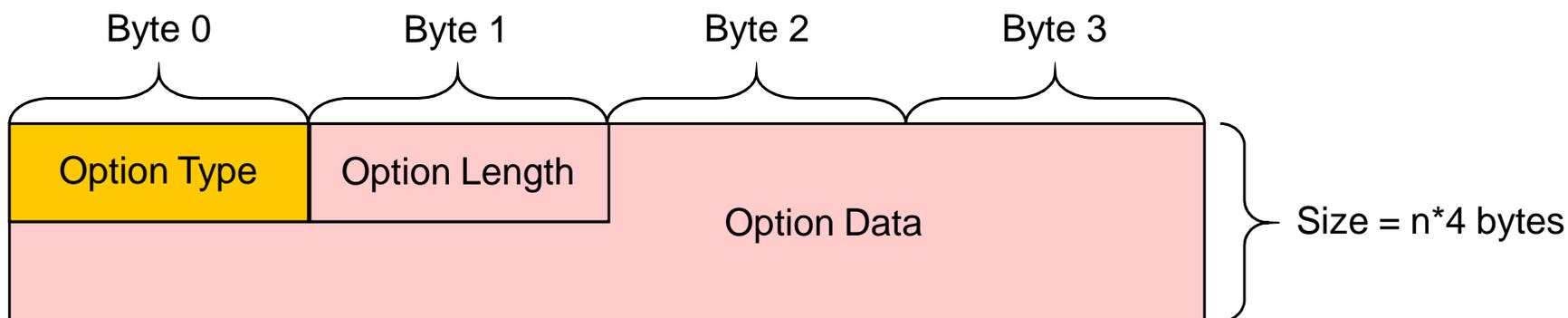
Sequence	Identifier	Total Length	DF May / Don't	MF Last / More	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555

# Frammentazione: problemi e come evitarli

- Il compito di riassettaggio è oneroso
- Il destinatario deve collezionare tutti i frammenti del pacchetto originario prima di consegnare il payload al livello superiore
- Se non termina entro un determinato tempo, tutti i frammenti arrivati sono scartati
- Può essere una tecnica per attaccare un host bersaglio
- Per evitare la frammentazione dei pacchetti lungo il percorso, talvolta si effettua un *path MTU discovery*, cioè si determina la più piccola MTU lungo il percorso da un host A ad un host B
  - Conoscendo il path MTU, A evita del tutto la frammentazione se invia pacchetti di dimensione minore a tale valore
- Un esempio di path MTU discovery
  - A invia un pacchetto ICMP echo request a B di massima dimensione con flag D=1
  - Se il pacchetto incontra sul percorso un router che non riesce a trasmettere il pacchetto, A riceve un messaggio ICMP “Destination unreachable: Fragmentation needed”
  - A dimezza la dimensione e ritrasmette, se riceve da B l’echo reply incrementa la dimensione di un quarto, altrimenti dimezza
  - Ecc...

- L'header IP può essere esteso con dei campi “Opzione” mediante le quali si intende chiedere una elaborazione “speciale” del pacchetto da parte dei router
  - Security
  - Source routing
  - Route recording
  - Stream identification
  - Timestamping
- Per la presenza delle opzioni, l'header IP può essere di lunghezza variabile
  - Questo è il motivo della presenza del campo Header Length
  - Se l'opzione non occupa 4 byte (o un suo multiplo), vengono inseriti dei bit di riempimento (tutti zero)
  - Nei router in cui il dataplane è implementato in hardware, l'elaborazione di questi campi non è effettuata in hardware (*fast path*) ma in software (*slow path*), oppure questi campi sono ignorati
    - Gli attacchi DoS di tipo “Christmas Tree” consistono nel trasmettere pacchetti IP con diverse opzioni (inutili) nell'header al fine di sovraccaricare i router

# Formato generale delle opzioni dell'header IPv4



Option Type byte

Subfield Name	Size (bits)	Description
Copied	1	If 1: Option to be copied in all fragments If 0: Option only kept in first fragment
Option Class	2	0: Control Options                      1: Unused 2: Debugging/Measurement          3: Unused
Option Number	5	Up to 32 different Options for each class