



---

# Bloque IV: El nivel de red

## Tema 9: IP

---



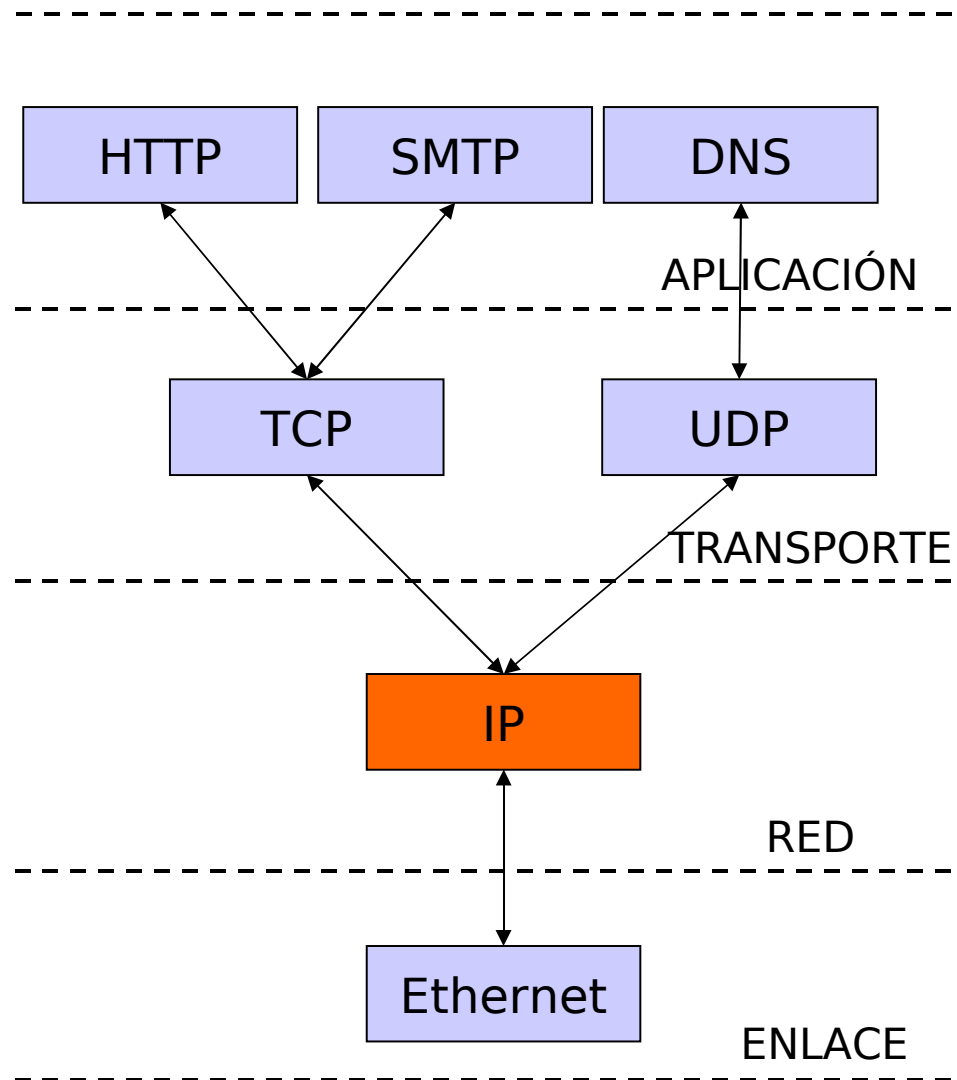
# Índice

---

- Bloque IV: El nivel de red
  - Tema 9: IP
    - Introducción
    - Cabecera IP
    - Fragmentación IP
  
- **Referencias**
  - Capítulo 4 de “Redes de Computadores: Un enfoque descendente basado en Internet”. James F. Kurose, Keith W. Ross. Addison Wesley, 2ª edición. 2003.
  - Capítulos 3 y 11 de “TCP/IP Illustrated, Volume 1: The Protocols”, W. Richard Stevens, Addison Wesley, 1994.

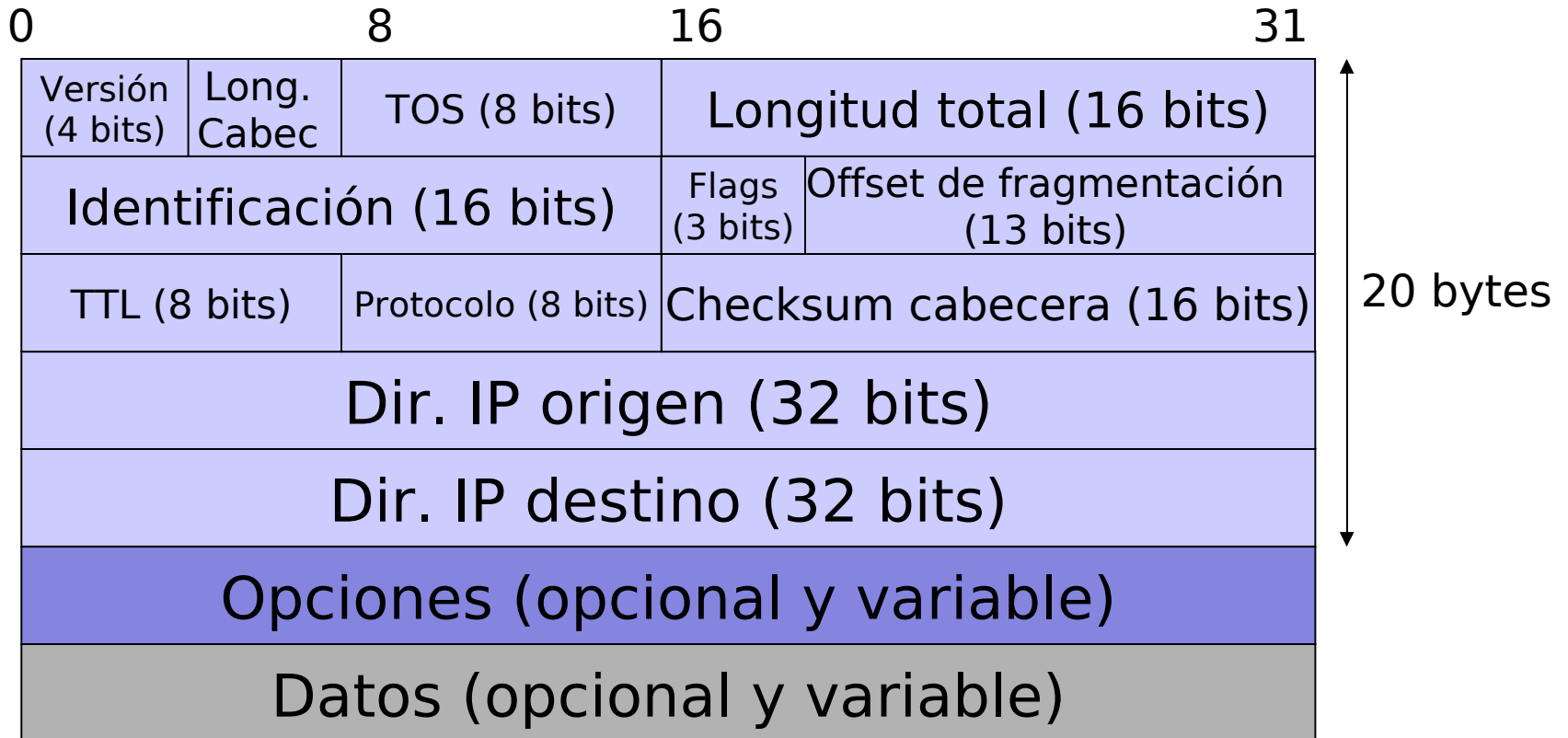
# Introducción

- Internet Protocol – Especificado en el RFC 791.
- IP proporciona un servicio de entrega de datagramas no fiable y no orientado a conexión
  - **No fiable:**
    - No hay garantía de que el datagrama alcance su destino.
    - Sigue un esquema “best effort”: Cuando algo va mal (p.e: un router con buffers agotados) ejecuta un algoritmo simple de gestión de errores: descarta el datagrama y trata de enviar un mensaje ICMP a la fuente.
  - **No orientado a conexión:**
    - IP no mantiene información de estado relativa a datagramas. Cada datagrama se gestiona independientemente de otros datagramas.
    - Los datagramas se pueden recibir desordenados.





# Cabecera IP





# Cabecera IP

---

- Utilizamos “network byte order”: ordenación de bytes “big endian”. Es el orden que se requiere en TCP/IP para transmitir los bytes en la red. Considerando palabras de 32 bits: bits 0-7 primero, bits 8-15 a continuación, etc., siendo el bit 0 el más significativo.
- **Versión:** Versión actual de IP (4).
- **Longitud de cabecera:** Número de bytes en la cabecera (incluidas las opciones si las hubiera (< 60 bytes)).
- **Tipo de servicio (TOS):** 3 bits de precedencia (no se usan) + 4 bits de información + 1 bit que no se usa
  - Bits de información:
    - Minimizar retardo
    - Maximizar “throughput”
    - Maximizar fiabilidad
    - Minimizar coste económico
  - De los 4 bits de información, sólo uno puede estar a 1 con cada servicio. RFC 1350 indica cual es el uso que se debe hacer de estos bits para cada aplicación estándar.
- **Longitud total:** Longitud total de datagrama IP en bytes.
  - Utilizando este campo y el de longitud de la cabecera se puede saber con exactitud dónde comienza la zona de datos del datagrama IP y su longitud.
  - Campo de 16 bits: máximo tamaño es 65535 bytes.
  - Muchas aplicaciones limitan actualmente la longitud de los datagramas IP a 8192 bytes (caso de aquellas que utilizan NFS).
  - Se precisa este campo porque un datagrama IP puede llegar a ser de menor tamaño que el mínimo exigido por el nivel de enlace (Ethernet, 46 bytes). En estos casos se añaden bytes para configurar la trama del nivel de enlace.



# Cabecera IP

---

- **Identificación:** identifica unívocamente el datagrama IP enviado por una máquina.
  - Normalmente se incrementa en una unidad cada vez que se envía un datagrama.
- **Flags y offset de fragmentación:** Campos para fragmentación.
- **TTL (Time To Live):** Establece un tiempo máximo de vida para el datagrama. Previene bucles indefinidos por problemas de enrutamiento.
  - Establece un límite en el número de “routers” por los que puede pasar un datagrama: normalmente 32 o 64.
  - Cada vez que el datagrama pasa por un “router”, se decrementa en una unidad el valor de este campo.
  - Cuando vale 0 se descarta el datagrama y se notifica al remitente con un mensaje ICMP.
- **Protocolo:** usado por IP para demultiplexar. Permite identificar de qué protocolo de la capa de transporte son los datos enviados.
- **Checksum de cabecera:** Sólo para la cabecera. Se calcula:
  - Se pone a cero
  - Se calcula la suma complemento a uno (en bloques de 16 bits) de la cabecera.
  - El complemento a uno de esta suma se almacena en el checksum.
  - En recepción, se hace la suma complemento a uno de la cabecera. Si no da todos unos, se considera error, se descarta el datagrama y no se notifica.
  - Como cada router decrementa el campo TTL para cada datagrama que enruta, debe actualizarse el checksum.



# Cabecera IP

---

- **Dirección IP de origen y destino:** 32 bits cada una.
- **Opciones:** Información opcional de longitud variable. Las opciones definidas son:
  - Seguridad y gestión de restricciones (para aplicaciones militares) RFC 1108.
  - Registro de enrutamiento (record route): cada “router” marca su hora y dirección IP (máximo 9 routers).
  - Timestamp: Va anotando la ruta y además pone una marca de tiempo en cada salto (máximo 4 routers).
  - Lista estricta de enrutamientos (strict source routing): La cabecera contiene la ruta paso a paso que debe seguir el datagrama (máximo 9).
  - Lista difusa de enrutamientos (loose source routing): la cabecera lleva una lista de routers por los que debe pasar el datagrama, pero puede pasar además por otros (máximo 9).
  - La longitud ha de ser múltiplo de 32 bits. Si hace falta, se añaden bytes PAD para cumplir esta condición.



# Fragmentación IP

---

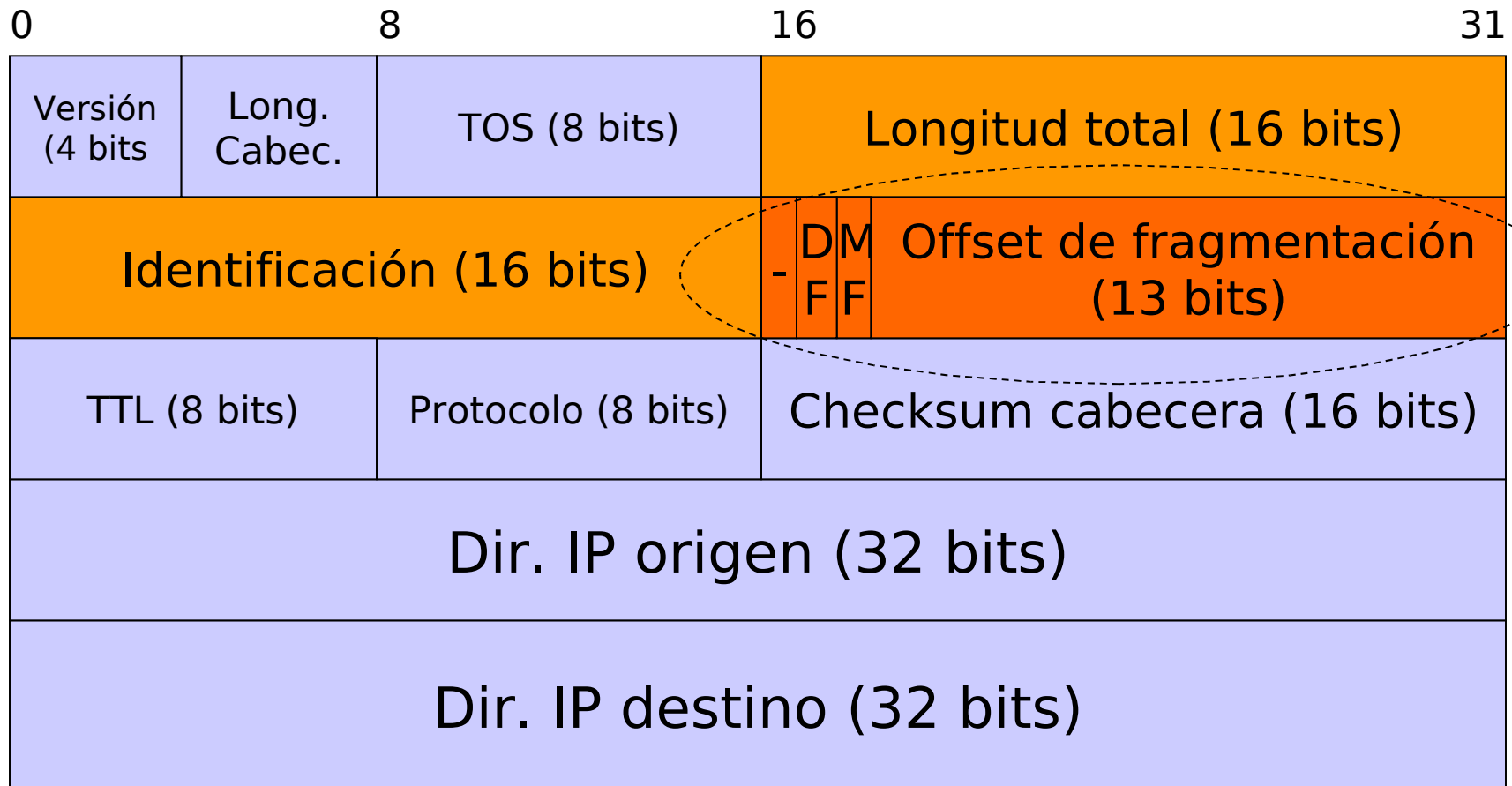
- El nivel físico de la red impone un límite superior al tamaño de la trama que se puede transmitir (**MTU** – Maximum Transmission Unit).
  - Ethernet: 1500 bytes
  - Token Ring: 4440 bytes
- Cuando el nivel IP recibe un datagrama, identifica la interfaz de red a utilizar y la interroga sobre su MTU:
  - Compara la respuesta con la longitud del datagrama.
  - Se hace fragmentación si la longitud del datagrama es mayor que el MTU.
- El reensamblaje de datagramas IP fragmentados se produce cuando el datagrama alcanza el **destino final**:
  - Lo hace el nivel IP del destino.
  - La fragmentación es transparente al nivel de transporte.
- En la cabecera IP se almacena la información relacionada con la fragmentación IP.





# Fragmentación IP

- Cabecera IP – Campos para fragmentación





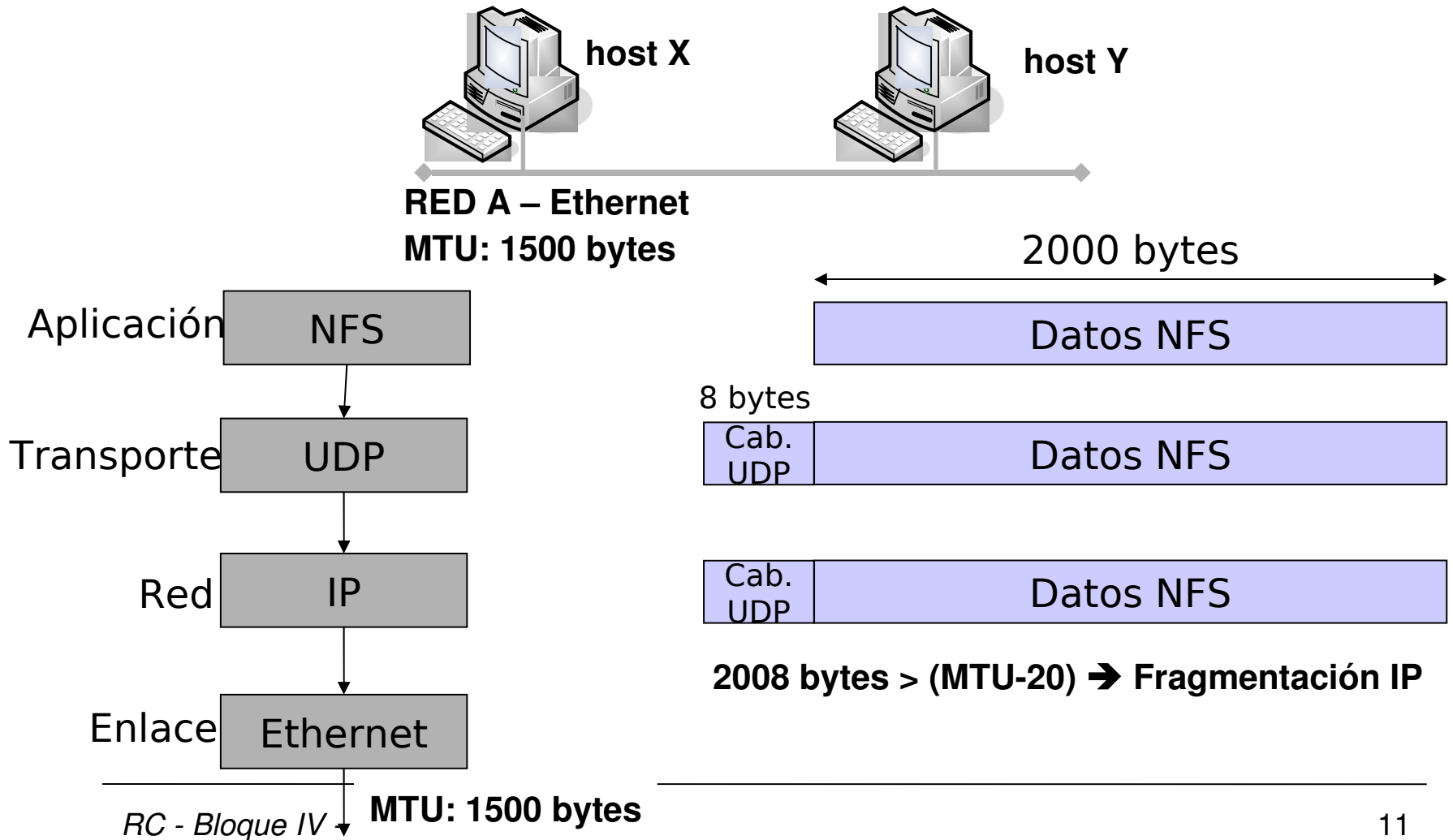
# Fragmentación IP

---

- Identificación: valor único para cada datagrama IP transmitido → Todos los fragmentos de un datagrama contienen el mismo valor.
- Flags:
  - El primer bit está reservado.
  - Bit DF (Don't Fragment): a 1 si se prohíbe fragmentar el datagrama IP.
  - Bit MF (More Fragments): a 1 si hay más fragmentos a continuación → Se pone a 0 en el último fragmento.
- Offset de fragmento: desplazamiento en múltiplos de 8 bytes del fragmento desde el origen del datagrama original.
- Longitud total: se cambia la longitud total del datagrama por longitud total del fragmento.
  
- El tamaño de cada fragmento debe ser múltiplo de 8 bytes, excepto el último fragmento → Por el campo offset de fragmento.
- Si está activado el flag DF y es necesario fragmentar → Se genera un mensaje de error ICMP Unreachable Error (Fragmentation Required).

# Fragmentación IP: Ejemplo 1

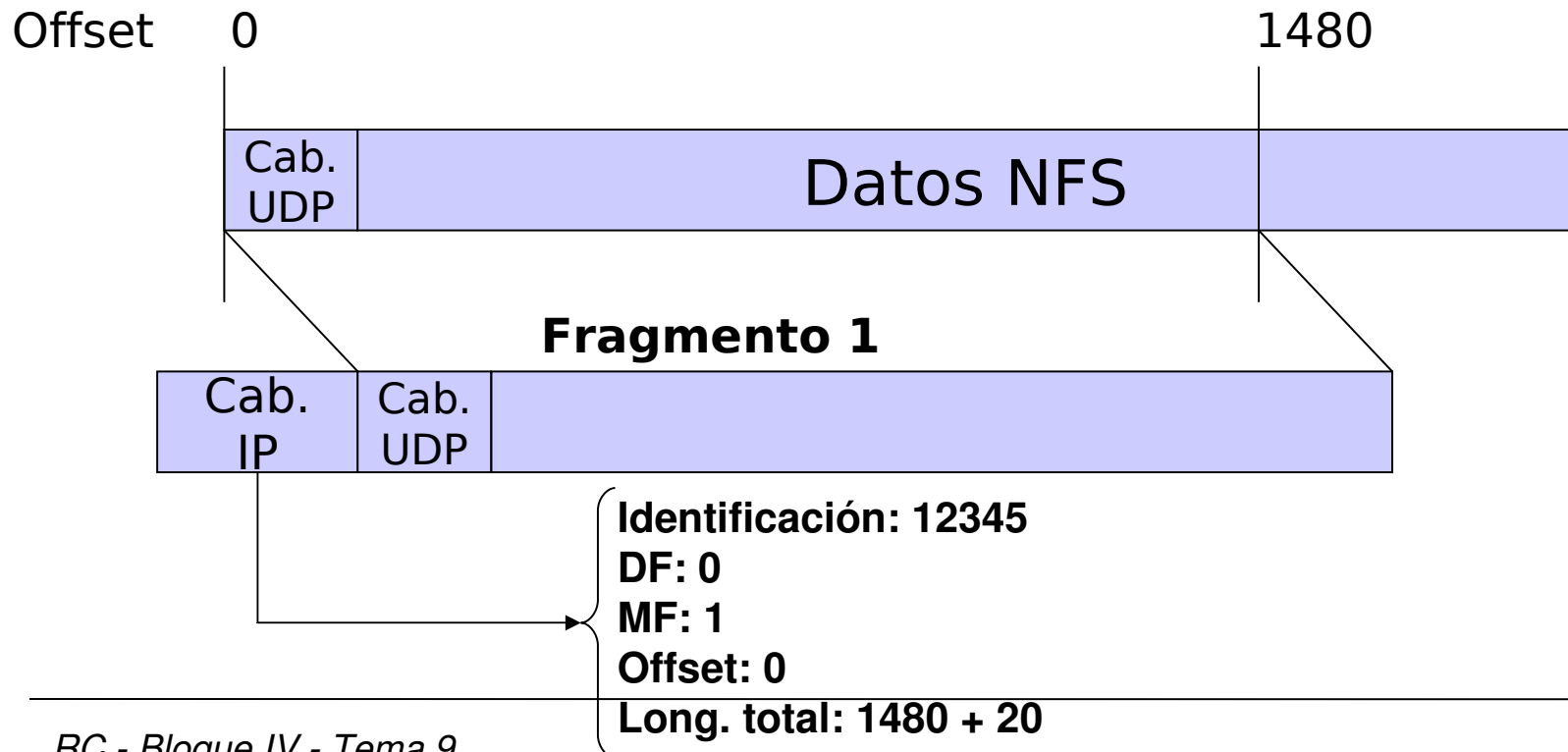
- Desde el host X se envían al host Y 2000 bytes de datos NFS (utilizando el protocolo UDP).





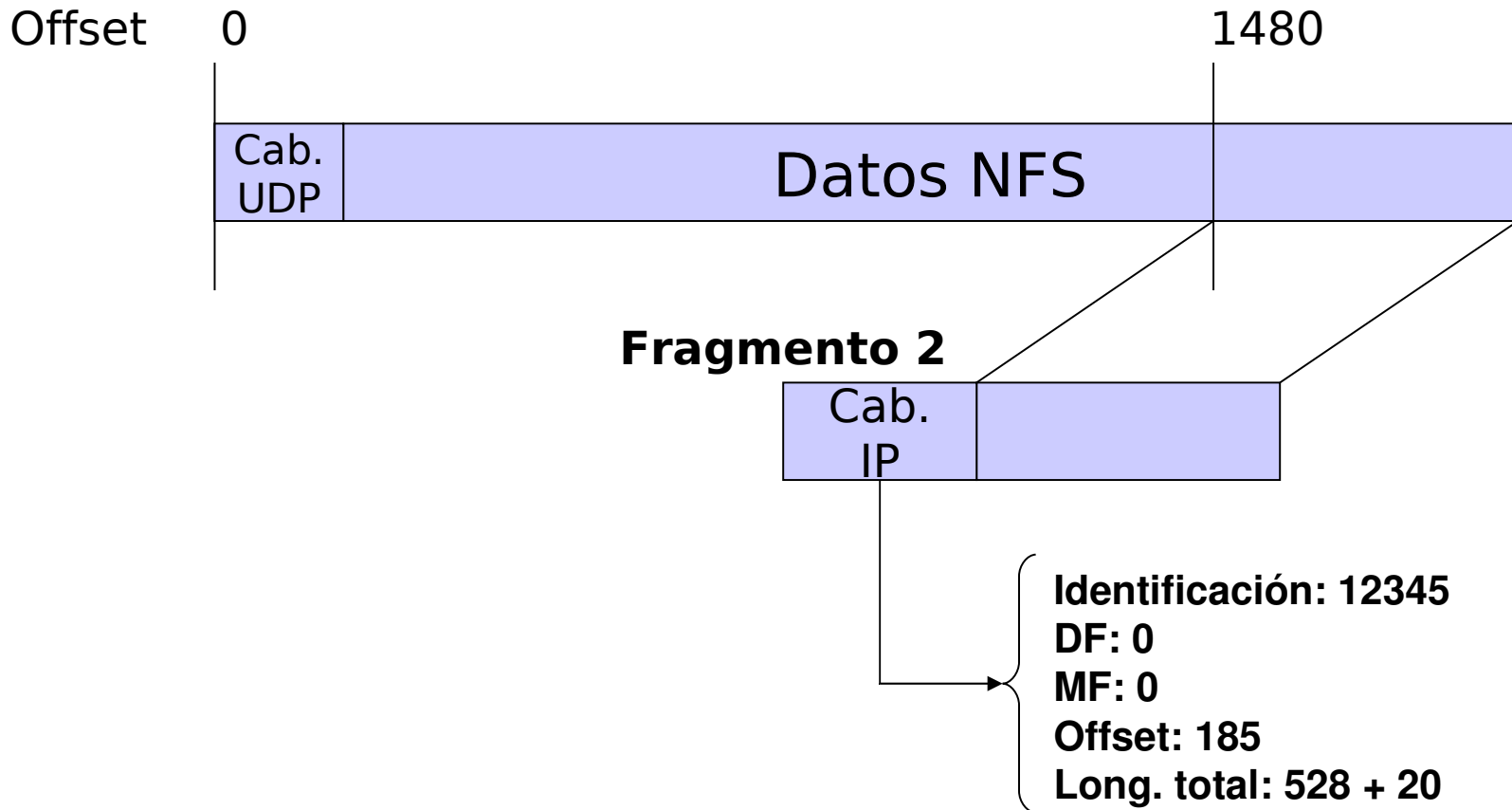
# Fragmentación IP: Ejemplo 1

- MTU = 1500 bytes
- Cada fragmento lleva una cabecera IP →  $1500 - 20 = 1480$ 
  - ¿Es 1480 múltiplo de 8?  $1480/8 = 185$  → Si
- Dividir 2008 bytes en fragmentos de 1480 bytes:
  - Fragmento 1: 1480 bytes + 20 bytes (cab. IP)
  - Fragmento 2: 528 bytes + 20 bytes (cab. IP)



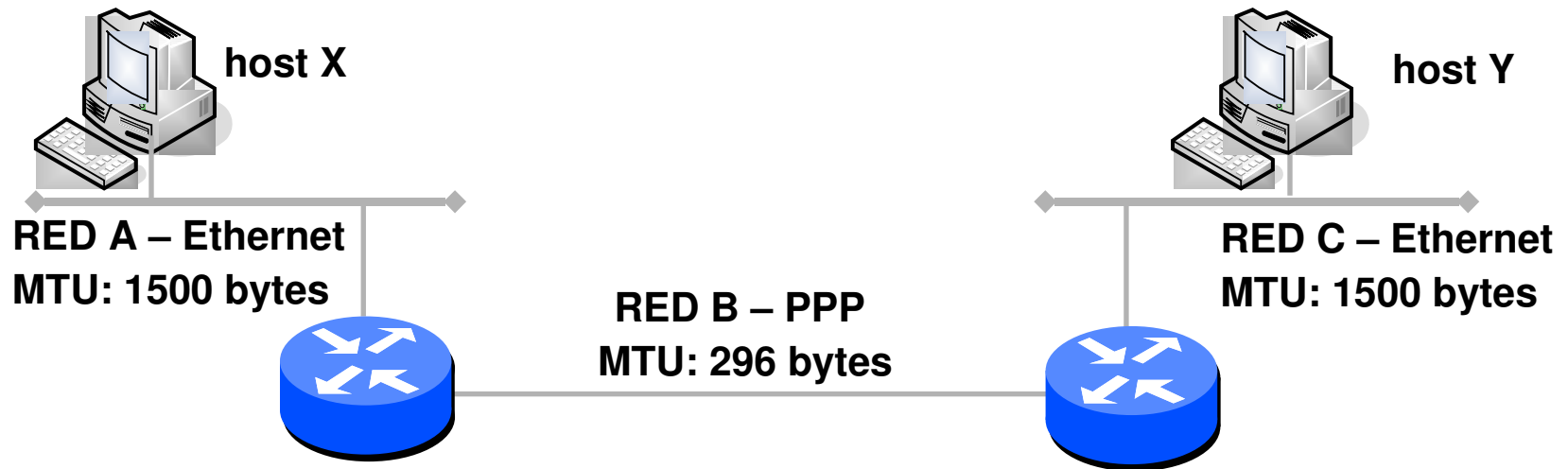


# Fragmentación IP: Ejemplo 1



# Fragmentación IP: Ejemplo 2

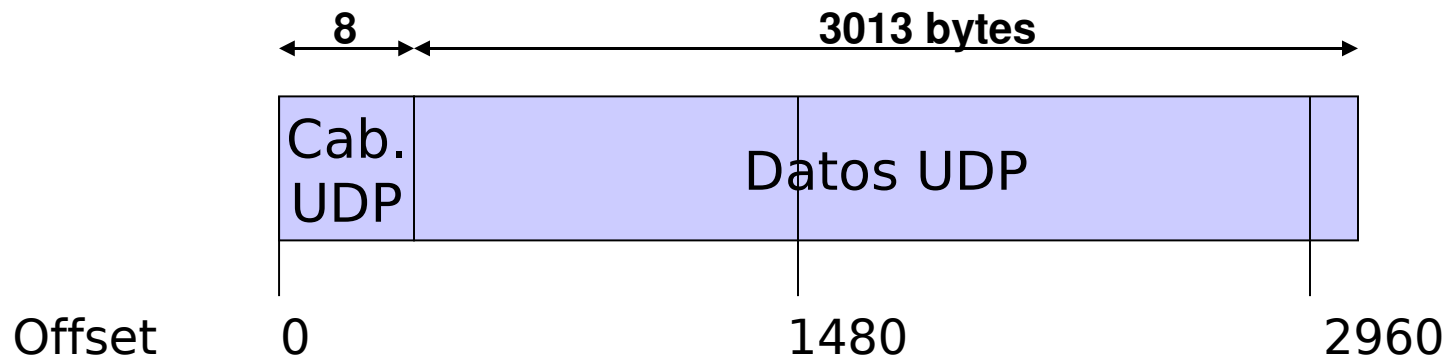
- Desde el host X se envían al host Y 3013 bytes de datos UDP (sin incluir la cabecera UDP).





# Fragmentación IP: Ejemplo 2

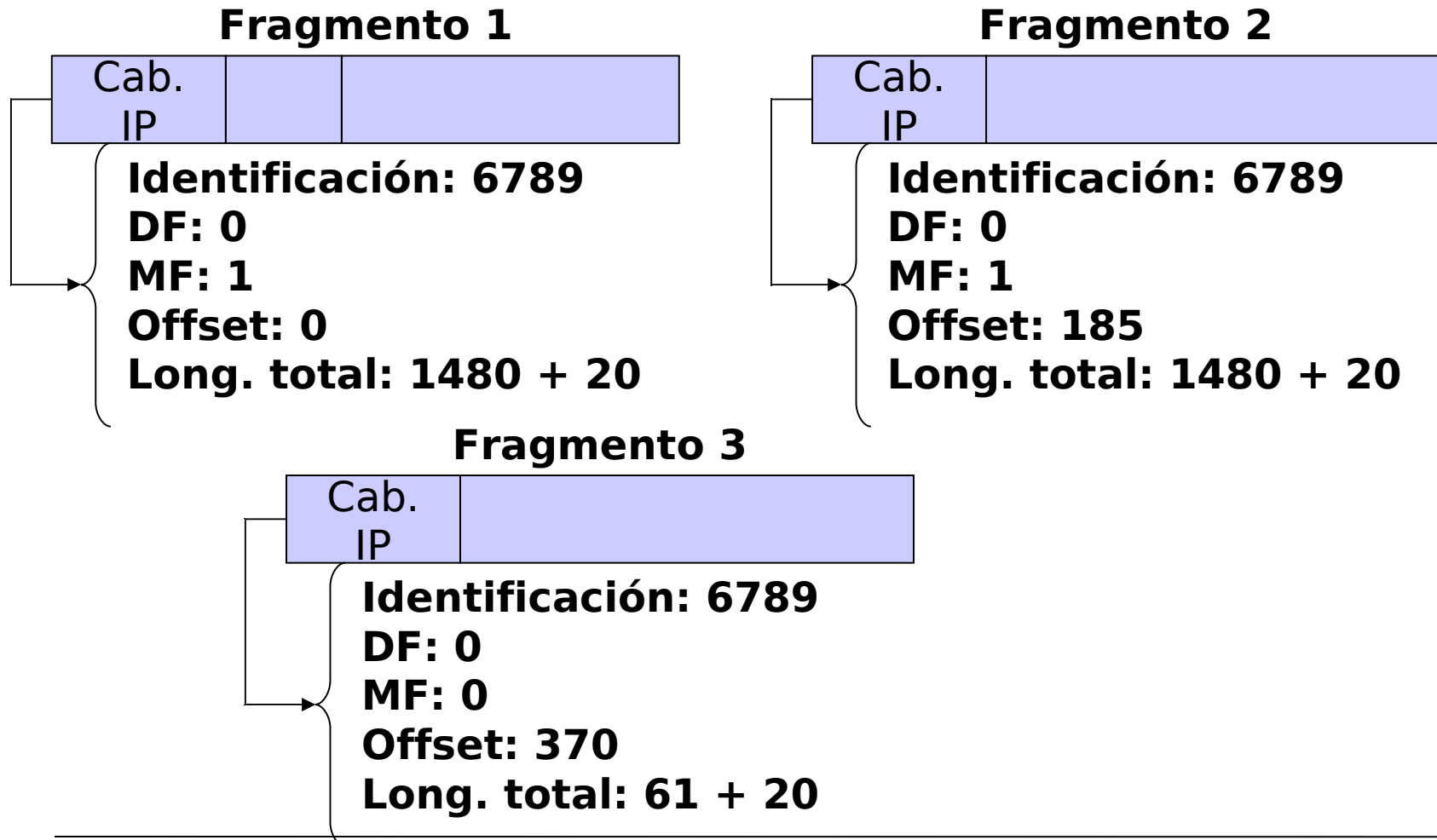
- Red A
  - MTU: 1500 bytes – 20 bytes (cab. IP) = 1480 bytes (1480/8=185 → Múltiplo de 8)
  - 3013 bytes + 8 bytes = 3021 bytes de datos IP
  - Dividir 3021 bytes en fragmentos de 1480
    - Fragmentos 1 y 2: 1480 bytes
    - Fragmento 3: 61 bytes





# Fragmentación IP: Ejemplo 2

- Red A:







# Fragmentación IP: Ejemplo 2

---

- Red B
  - MTU: 296 bytes – 20 bytes (cab. IP) = 276 bytes  
( $276/8=34.5 \rightarrow$  No es múltiplo de 8  $\rightarrow$  Primer múltiplo menor de 276  $\rightarrow$  272 bytes)
  - ¿Se reagrupan los fragmentos? NO!
  - Dividir el Fragmento 1  $\rightarrow$  Dividir 1480 bytes en fragmentos de 272 bytes:
    - 5 fragmentos de 272 bytes y 1 fragmento de 120 bytes
  - Dividir el Fragmento 2  $\rightarrow$  Igual que el fragmento 1
  - Dividir el Fragmento 3  $\rightarrow$  No: 81 bytes  $\leq$  MTU

# Fragmentación IP: Ejemplo 2

- Red B



Fragmento 1.1  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 0  
Long. total: 272 +  
20

Fragmento 1.3  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 68  
Long. total: 272 +  
20

Fragmento 1.5  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 136  
Long. total: 272 +  
20

Fragmento 1.2  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 34  
Long. total: 272 +  
20

Fragmento 1.4  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 102  
Long. total: 272 +  
20

Fragmento 1.6  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 170  
Long. total: 120 +  
20

# Fragmentación IP: Ejemplo 2

- Red B



Fragmento 2.1  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 185  
Long. total: 272 +  
20

Fragmento 2.3  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 253  
Long. total: 272 +  
20

Fragmento 2.5  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 321  
Long. total: 272 +  
20

Fragmento 2.2  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 219  
Long. total: 272 +  
20

Fragmento 2.4  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 287  
Long. total: 272 +  
20

Fragmento 2.6  
Identificación: 6789  
DF: 0  
MF: 1  
Offset: 355  
Long. total: 120 +  
20



# Fragmentación IP: Ejemplo 2

---

- Red B

Fragmento 3



Fragmento 3  
Identificación: 6789  
DF: 0  
MF: 0  
Offset: 370  
Long. total: 61 + 20

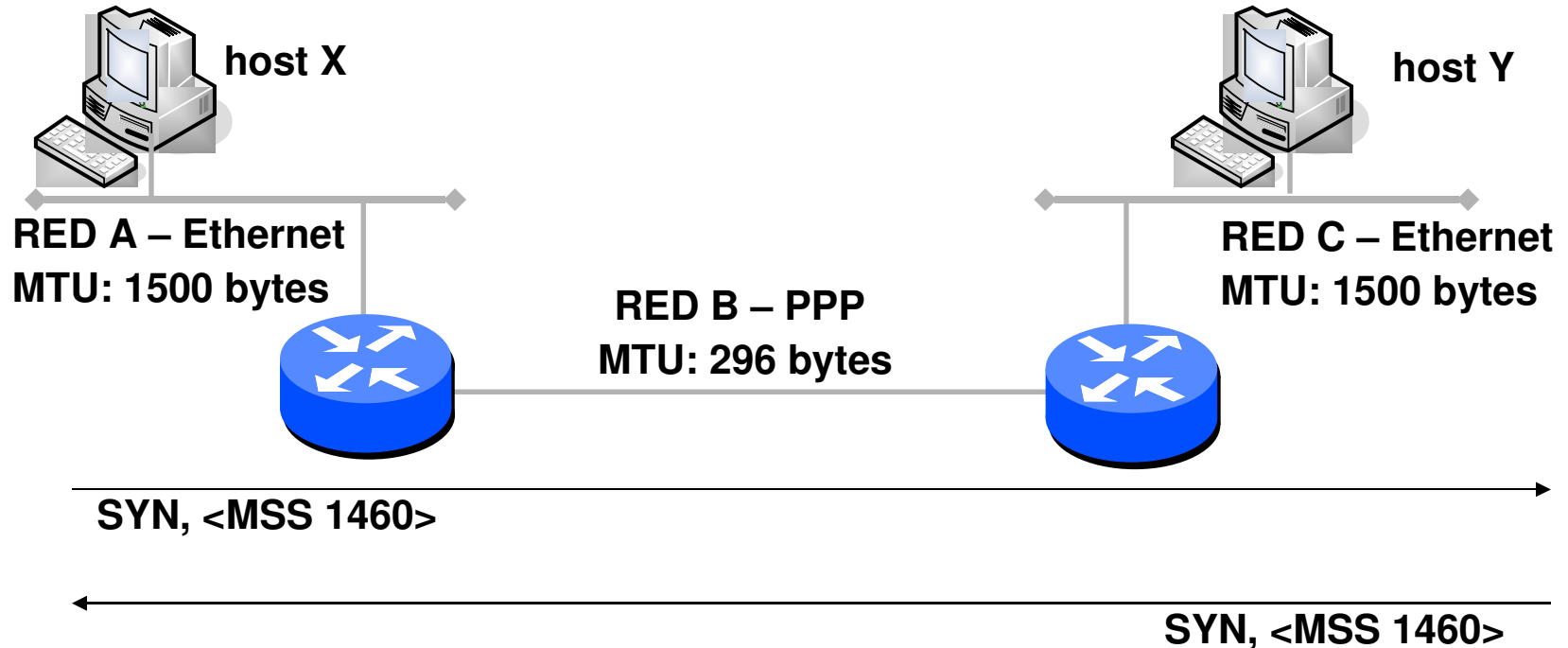


# Fragmentación IP: Ejemplo 2

---

- Red C
  - MTU: 1500 bytes
  - ¿Qué fragmentos circulan por la red C: los mismos que por la red A o por la red B?
  - No se reagrupan hasta llegar al destino final →  
Los mismos que por la red B.

# Fragmentación IP: Ejemplo 2



- Desde A se envían a B 3013 bytes de datos TCP (sin incluir la cabecera TCP).



# Fragmentación IP: Ejemplo 2

- Red A
  - MSS: 1460 bytes
  - Dividir 3013 bytes en segmentos de 1460 bytes:
    - Segmento 1: 1460 bytes (0-1459)
    - Segmento 2: 1460 bytes (1460-2919)
    - Segmento 3: 93 bytes (2920-3012)

## Segmento 1



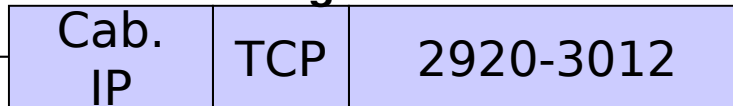
Identificación: 67890  
DF: 0  
MF: 0  
Offset: 0  
Long. total: 1480 + 20

## Segmento 2



Identificación: 67891  
DF: 0  
MF: 0  
Offset: 0  
Long. total: 1480 + 20

## Segmento 3



Identificación: 67892  
DF: 0  
MF: 0  
Offset: 0  
Long. total: 113 + 20



# Fragmentación IP: Ejemplo 2

---

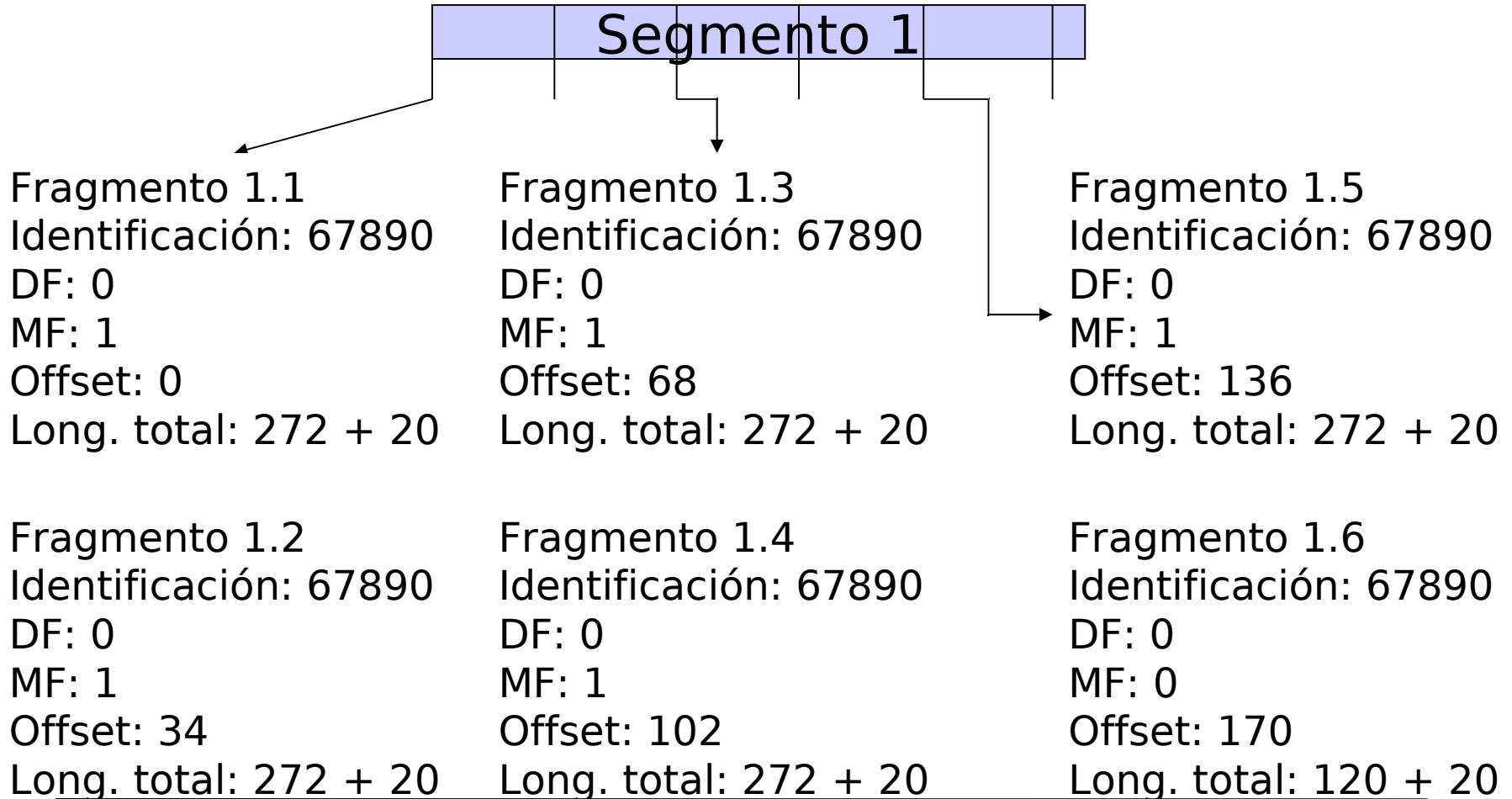
- Red B
  - MTU: 296 bytes – 20 bytes (cab. IP) = 276 bytes  
( $276/8=34.5 \rightarrow$  No es múltiplo de 8  $\rightarrow$  Primer múltiplo menor de 276  $\rightarrow$  272 bytes)
  - Dividir el segmento 1  $\rightarrow$  Dividir 1480 bytes en fragmentos de 272 bytes:
    - 5 fragmentos de 272 bytes y 1 fragmento de 120 bytes
  - Dividir el segmento 2  $\rightarrow$  Igual que el fragmento 1
  - Dividir el segmento 3  $\rightarrow$  No: 113 bytes  $\leq$  MTU





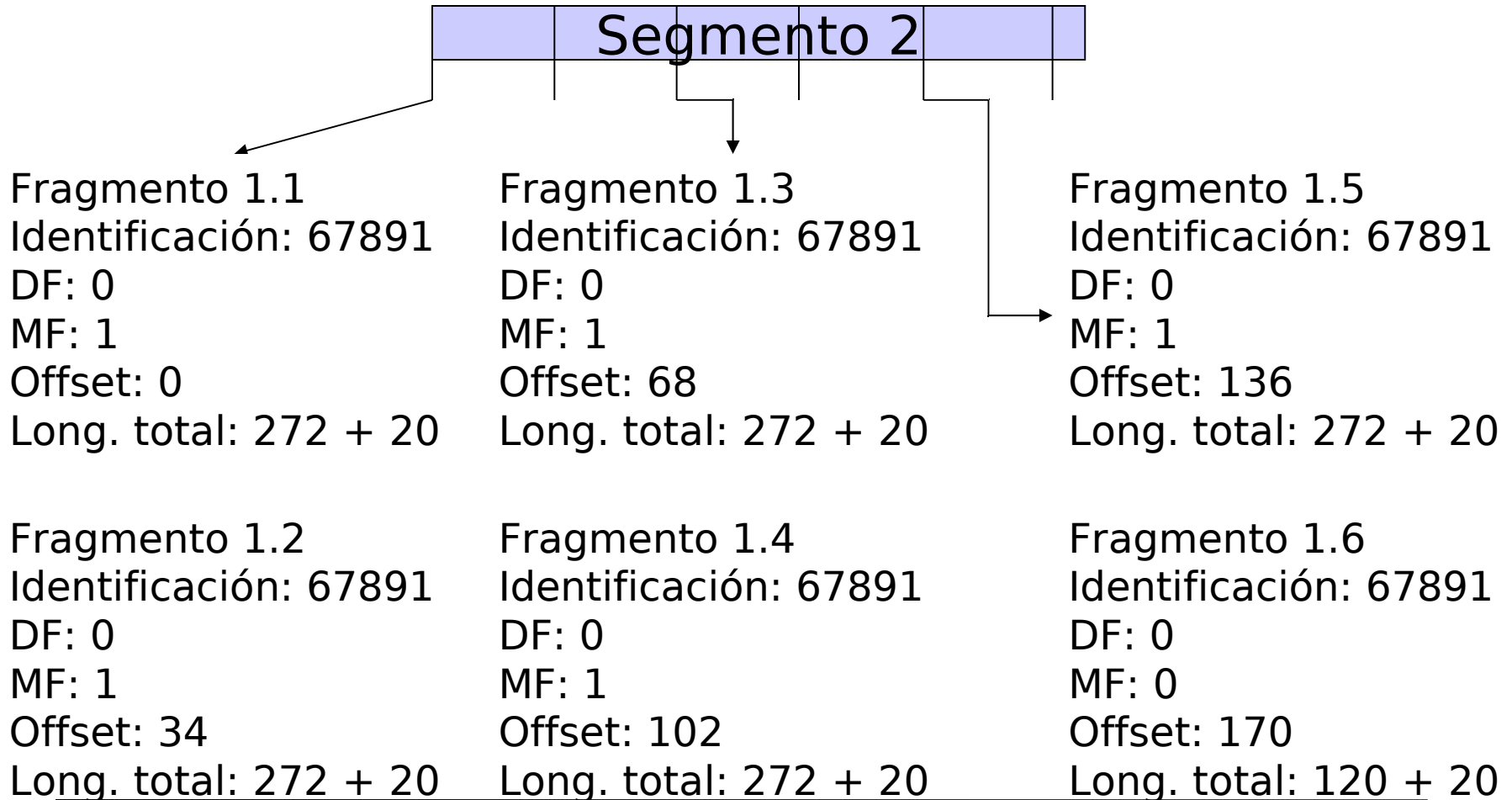
# Fragmentación IP: Ejemplo 2

- Red B



# Fragmentación IP: Ejemplo 2

- Red B





# Fragmentación IP: Ejemplo 2

---

- Red B

Segmento 3



Identificación: 67892

DF: 0

MF: 0

Offset: 0

Long. total: 113 + 20



# Fragmentación IP: Ejemplo 2

---

- Red C
  - MTU: 1500 bytes
  - ¿Qué fragmentos circulan por la red C: los mismos que por la red A o por la red B?
  - No se reagrupan hasta llegar al destino final →  
Los mismos que por la red B.