Bloque IV: El nivel de red

Tema 9: ICMP

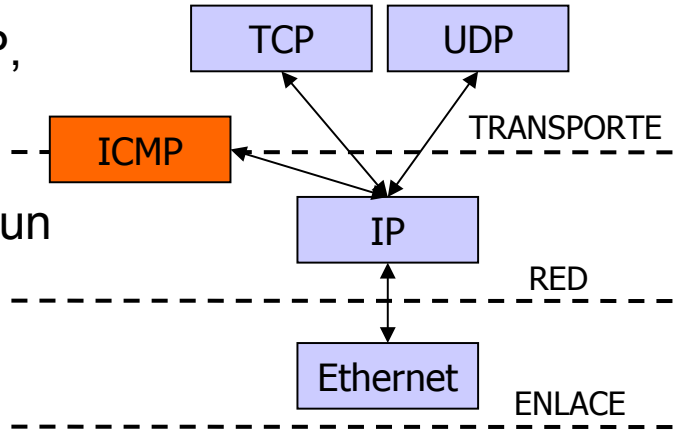
Índice

- Bloque IV: El nivel de red
  - Tema 9: ICMP
    - Introducción
    - Ping
    - Traceroute
    - Fragmentación IP

- **Lecturas recomendadas:**
  - Capítulo 4, sección 4.4.3, de “Redes de Computadores: Un enfoque descendente”. James F. Kurose, Keith W. Ross. Addison Wesley.
  - Capítulo 8 de “TCP/IP Illustrated, Volume 1: The Protocols”, W. Richard Stevens, Addison Wesley.

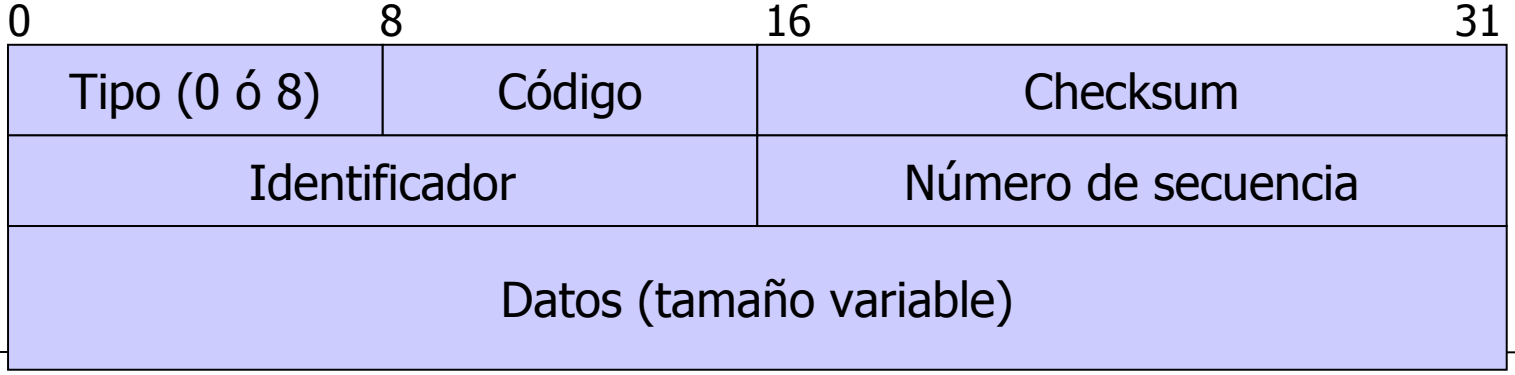
Introducción

- Internet Control Message Protocol
- IP no tiene mecanismos para obtener información de diagnóstico → Para eso está ICMP.
- ICMP comunica mensajes de error y otras condiciones que requieren atención. Dos tipos de mensajes: error y consulta.
- Los mensajes ICMP se transmiten dentro de datagramas IP (RFC 792)
- Mensajes ICMP más empleados:
  - Petición y respuesta de eco → ping
  - Destino inalcanzable
    - Puerto inalcanzable: utilizado por UDP, cuando el destino no dispone de un proceso en el puerto de destino.
    - Máquina o red inalcanzable: Lo envía un router cuando no puede entregar o reenviar un datagrama IP.
  - Redirect
  - Fragmentación requerida
  - Tiempo excedido



Ping

- Packet InterNet Groper: herramienta de diagnóstico que comprueba si un nodo de la red es alcanzable.
- Cliente: Envía ICMP echo request
- Servidor: Responde con ICMP echo reply
- Formato mensajes ICMP echo request y reply:
  - Identificador: en UNIX es el identificador del proceso.
  - Número de secuencia: inicialmente 0, y se incrementa con cada echo request.
- Opción de registro de ruta o timestamp.
- Existen variedad de implementaciones (presentación de resultados, opciones del programa...).

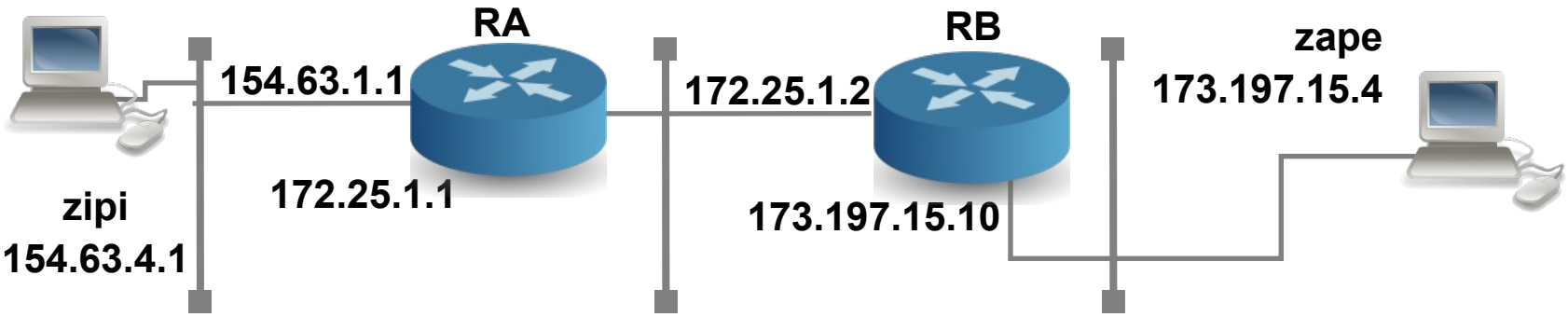


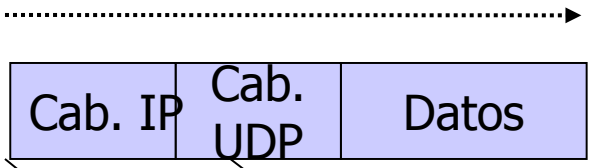
Traceroute

- Problemas del ping con registro de ruta:
  - Falta de espacio en la cabecera IP
    - Registro de ruta: máximo 9 routers
    - Timestamp: máximo 4 routers (o 9 timestamps sin direcciones IP)
  - No todos los routers soportan la opción de registro de ruta
  - No hay control sobre los relojes de los routers
- Solución: **traceroute**
  - Herramienta de diagnóstico que permite ver la ruta que sigue un datagrama hacia un destino.

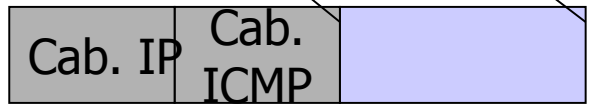
- Se basa en: datagramas UDP, el campo TTL de la cabecera IP y los mensajes de error ICMP Puerto inalcanzable y Tiempo excedido
  - Sólo requiere que el protocolo UDP esté operativo en el destinatario.
  - Cuando un router al decrementar el campo TTL obtiene 0 → Genera un mensaje de error ICMP Tiempo excedido
  - Cuando UDP recibe un datagrama para un puerto vacío → Genera un mensaje de error ICMP Puerto inalcanzable

Traceroute: Funcionamiento





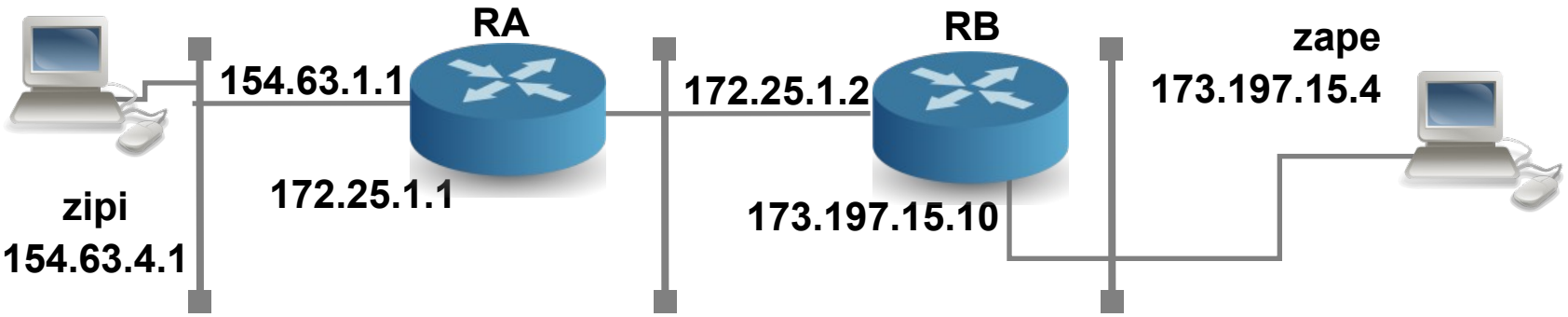
IP origen: 154.63.4.1
IP destino: 173.197.15.4
TTL = 1

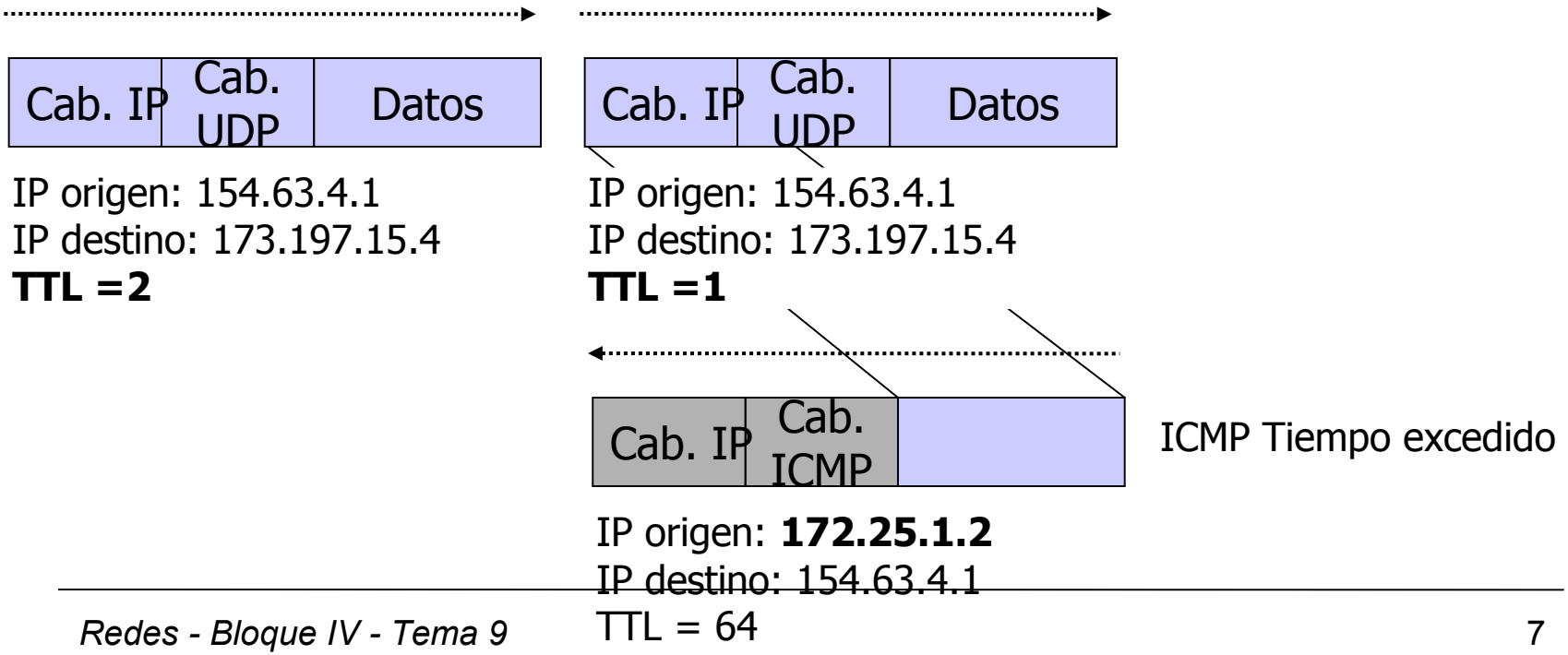


ICMP Tiempo excedido

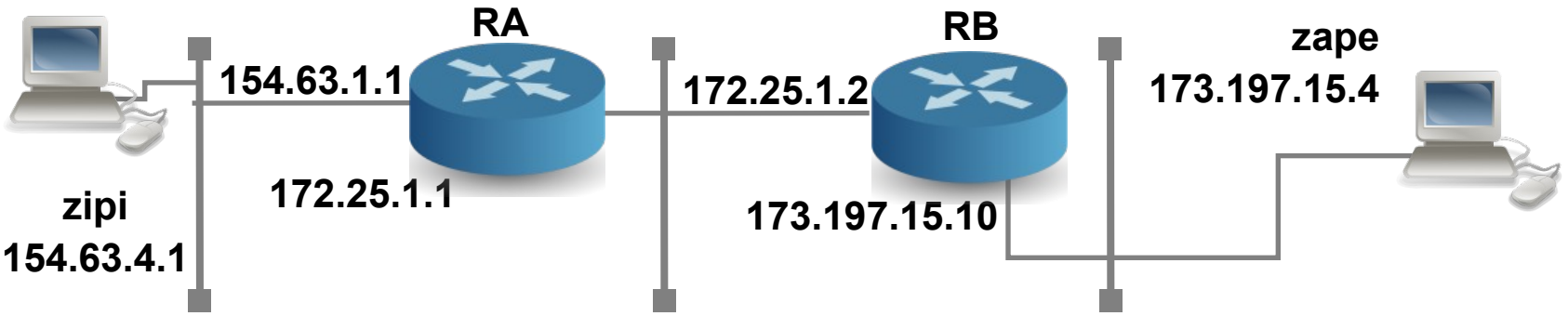
IP origen: **154.63.1.1**
IP destino: 154.63.4.1
TTL = 64

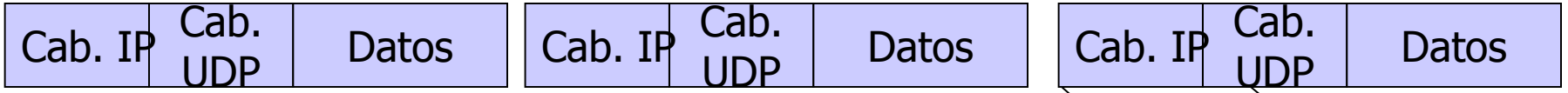
Traceroute: Funcionamiento





Traceroute: Funcionamiento



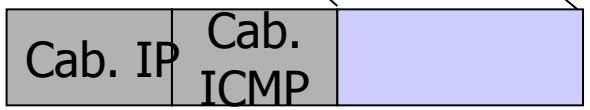


IP origen: 154.63.4.1
IP destino: 173.197.15.4
TTL =3

IP origen: 154.63.4.1
IP destino: 173.197.15.4
TTL =2

Puerto destino: 33348
IP origen: 154.63.4.1
IP destino: 173.197.15.4
TTL =1

ICMP Puerto inalcanzable



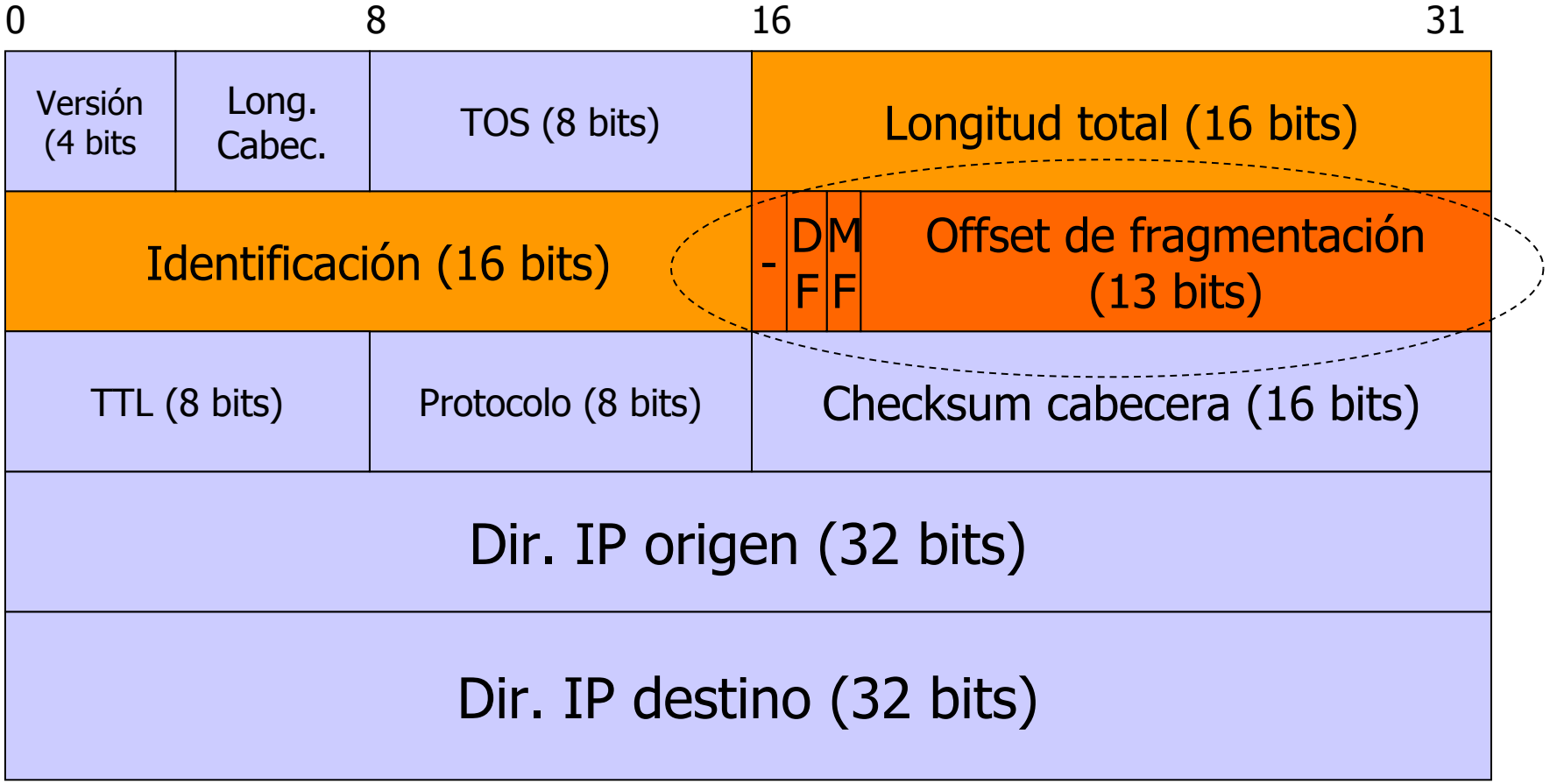
IP origen: **173.197.15.4**
IP destino: 154.63.4.1
TTL = 64

Fragmentación IP

- El nivel de enlace de la red impone un límite superior al tamaño de la trama que se puede transmitir: **MTU** – Maximum Transmission Unit (tamaño máximo del campo de datos de enlace).
  - Ethernet: 1500 bytes
  - Token Ring: 4440 bytes
- Cuando el nivel de red (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 los fragmentos alcanzan el **destino final**:
  - Lo hace IP en el 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



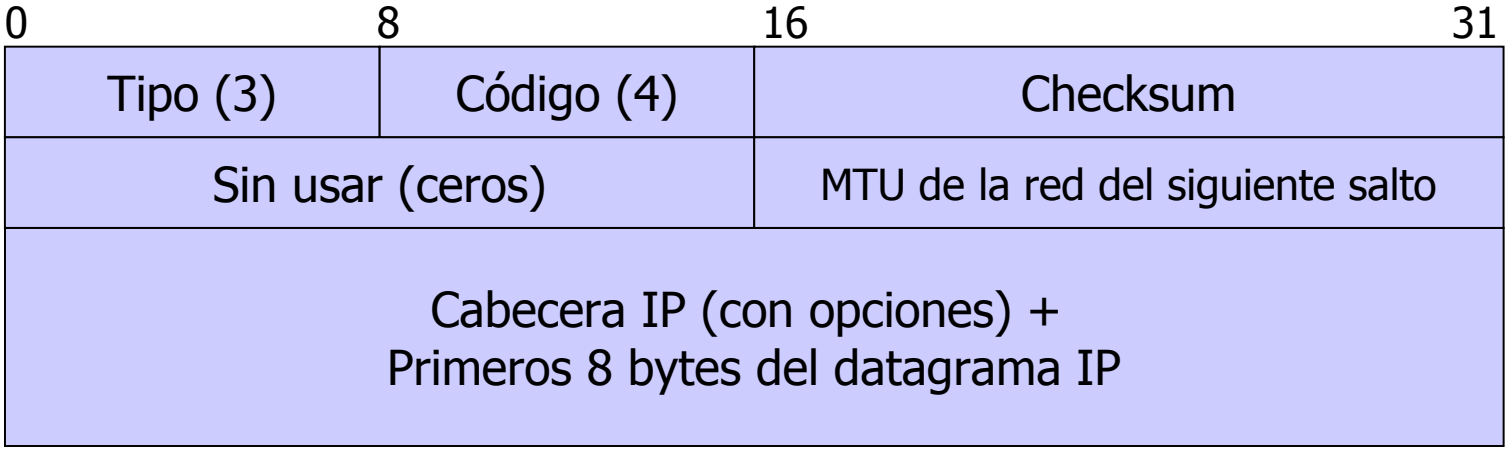
Fragmentación IP

- **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.

Fragmentación IP: Error ICMP

- Error ICMP Unreachable Error (Fragmentation Required)
  - Mensaje de error utilizado por un router cuando tiene que fragmentar un datagrama IP pero tiene el flag DF activado.
  - Incluye el MTU de la red que provocó el error y una copia de la cabecera del mensaje descartado.



Fragmentación IP: Path MTU Discovery

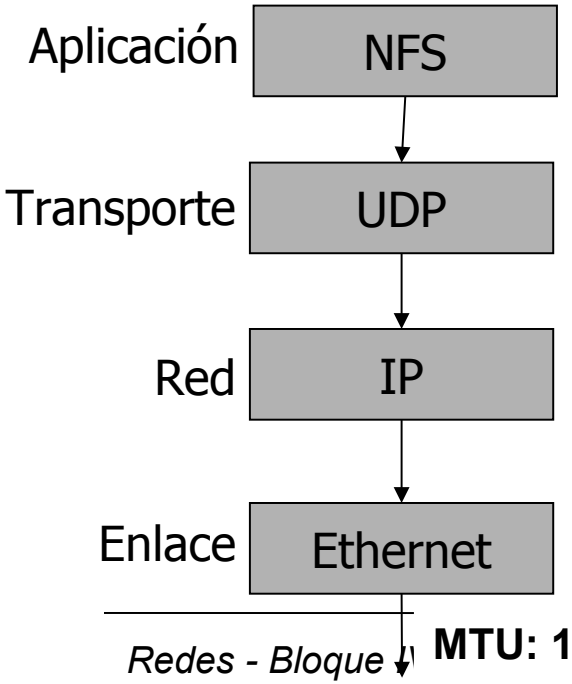
- Este mensaje de error es utilizado en un mecanismo denominado **Path MTU discovery** que permite averiguar el MTU mínimo durante una comunicación y reducir la fragmentación IP.
  - Sólo se implementa en el host origen.
  - Path MTU: MTU mínimo en cualquier red en el camino entre dos hosts.
- Funcionamiento del Path MTU discovery:
  - Se habilita el bit DF (Don't Fragment) en los datagramas enviados.
  - Si algún router en el camino necesita fragmentar → Generará el mensaje ICMP Fragmentación requerida
  - Si se recibe un mensaje ICMP Fragmentación requerida con el nuevo MTU:
    - Si eran datos TCP → TCP debe reducir el tamaño del segmento (en base al nuevo MTU) y retransmitir.
    - Sino (p.e. UDP) → IP fragmenta los datagrama en base al nuevo MTU.
  - Como las rutas cambian dinámicamente → Se puede probar un MTU mayor pasado un cierto intervalo (RFC 1191 recomienda 10 minutos).

Fragmentación IP: Ejercicio 1

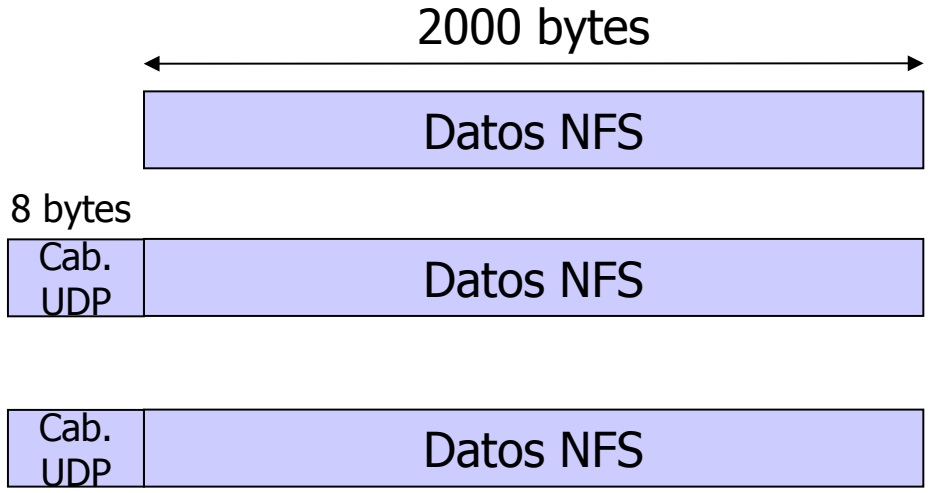
- Desde el host X se envían al host Y 2000 bytes de datos NFS (utilizando el protocolo UDP).

RED A – Ethernet

MTU: 1500 bytes

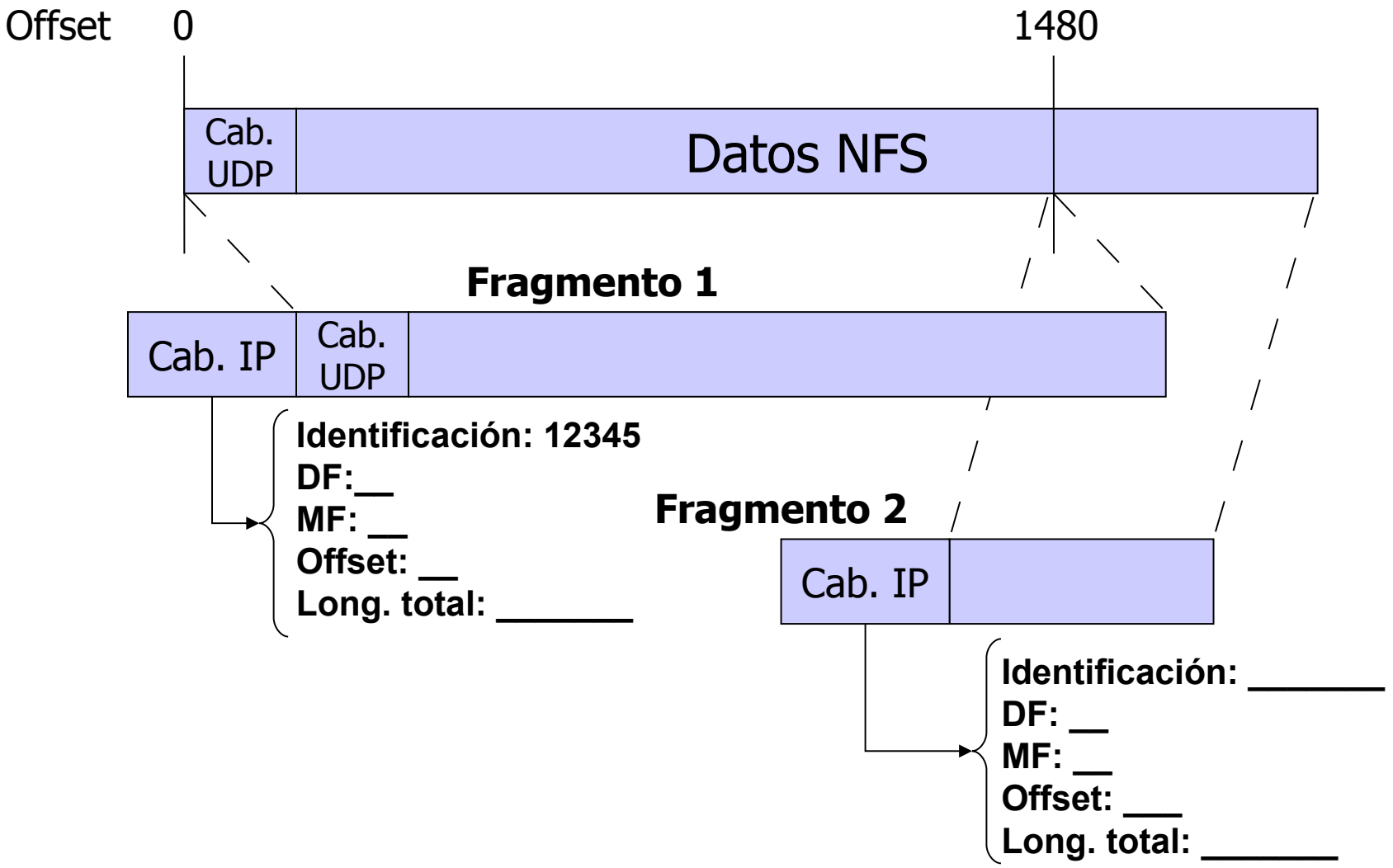


MTU: 1500 bytes



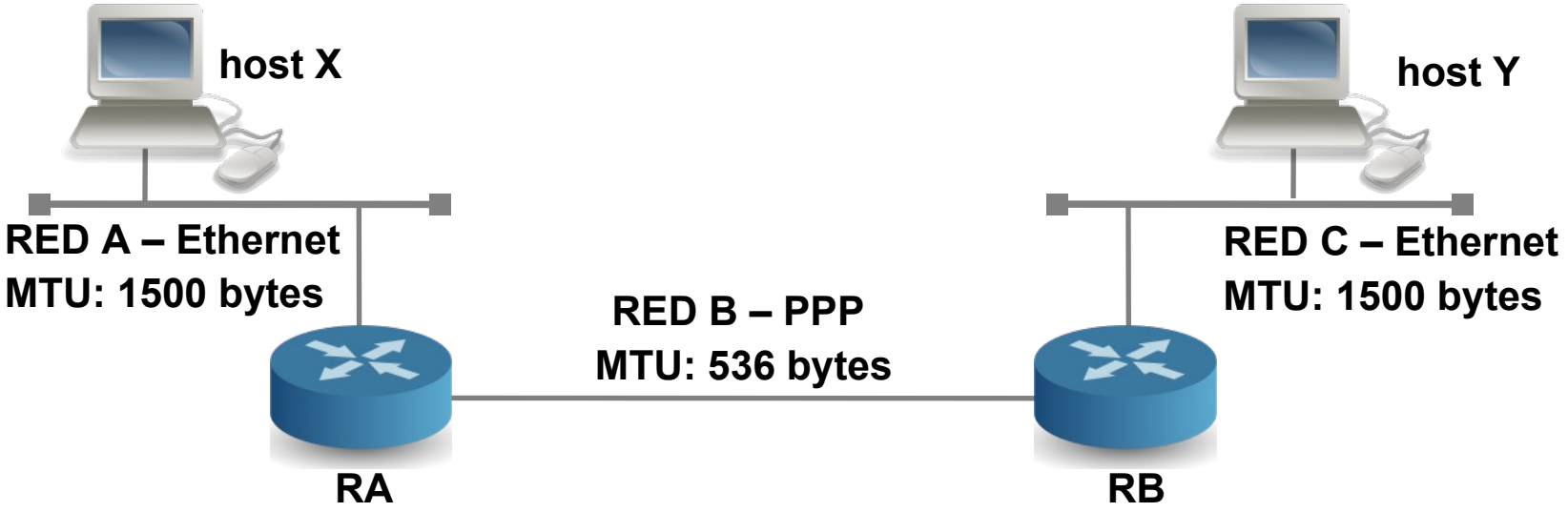
2008 bytes > (MTU-20) → Fragmentación IP

Fragmentación IP: Ejercicio 1



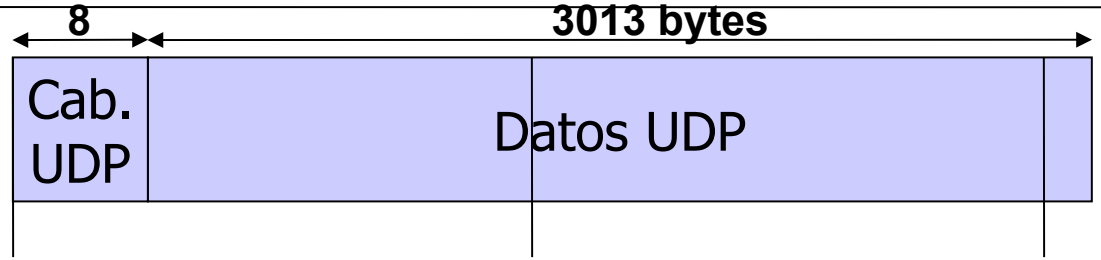
Fragmentación IP: Ejercicio 2

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

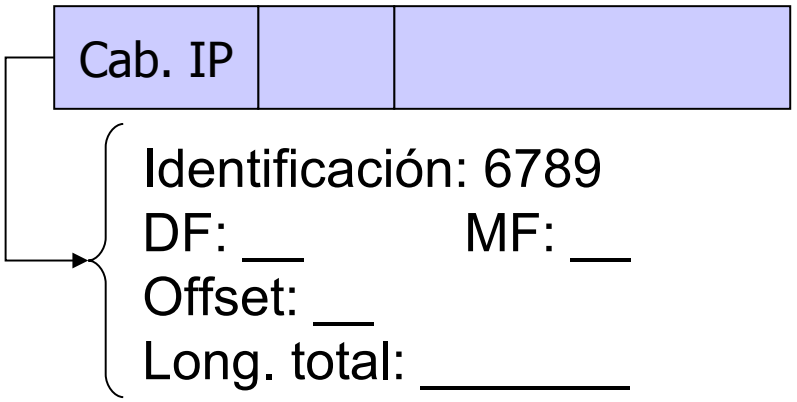


Fragmentación IP: Ejercicio 2

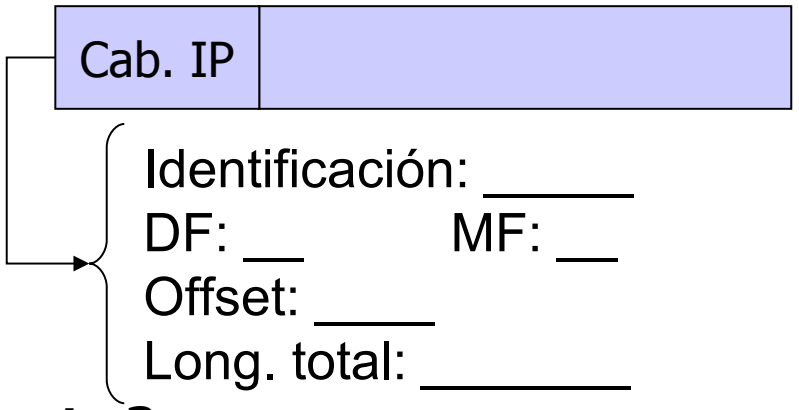
- Red A



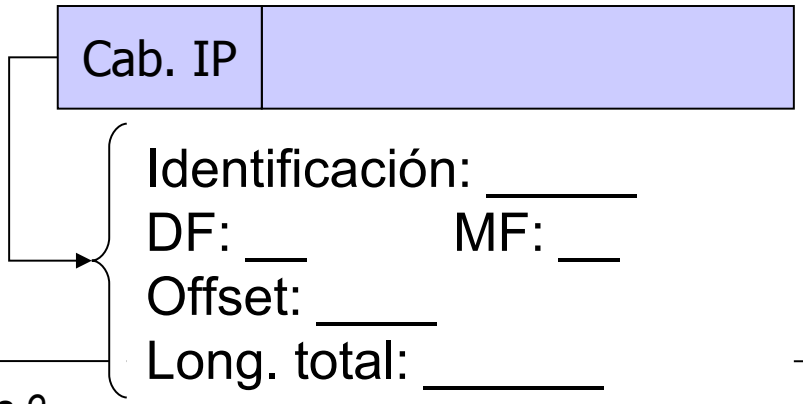
Fragmento 1



Fragmento 2



Fragmento 3



Fragmentación IP: Ejercicio 2

- Red B
  - ¿Se reagrupan los fragmentos antes de volver a fragmentarlos?
    - Sí
    - No
  - ¿Cuál es el tamaño de fragmento en la red B?
    - 516 bytes
    - 512 bytes
  - ¿Por qué?

Fragmentación IP: Ejercicio 2

- Red B

Fragmento 1.1
Identificación: _____
DF: __
MF: __
Offset: __
Long. total: _____

Fragmento 1.2
Identificación: _____
DF: __
MF: __
Offset: __
Long. total: _____

Fragmento 1.3
Identificación: _____
DF: __
MF: __
Offset: ____
Long. total: _____

Fragmentación IP: Ejercicio 2

- Red B

Fragmento 2.1
Identificación: _____
DF: __
MF: __
Offset: __
Long. total: _____

Fragmento 2.2
Identificación: _____
DF: __
MF: __
Offset: __
Long. total: _____

Fragmento 2.3
Identificación: _____
DF: __
MF: __
Offset: ____
Long. total: _____

Fragmentación IP: Ejercicio 2

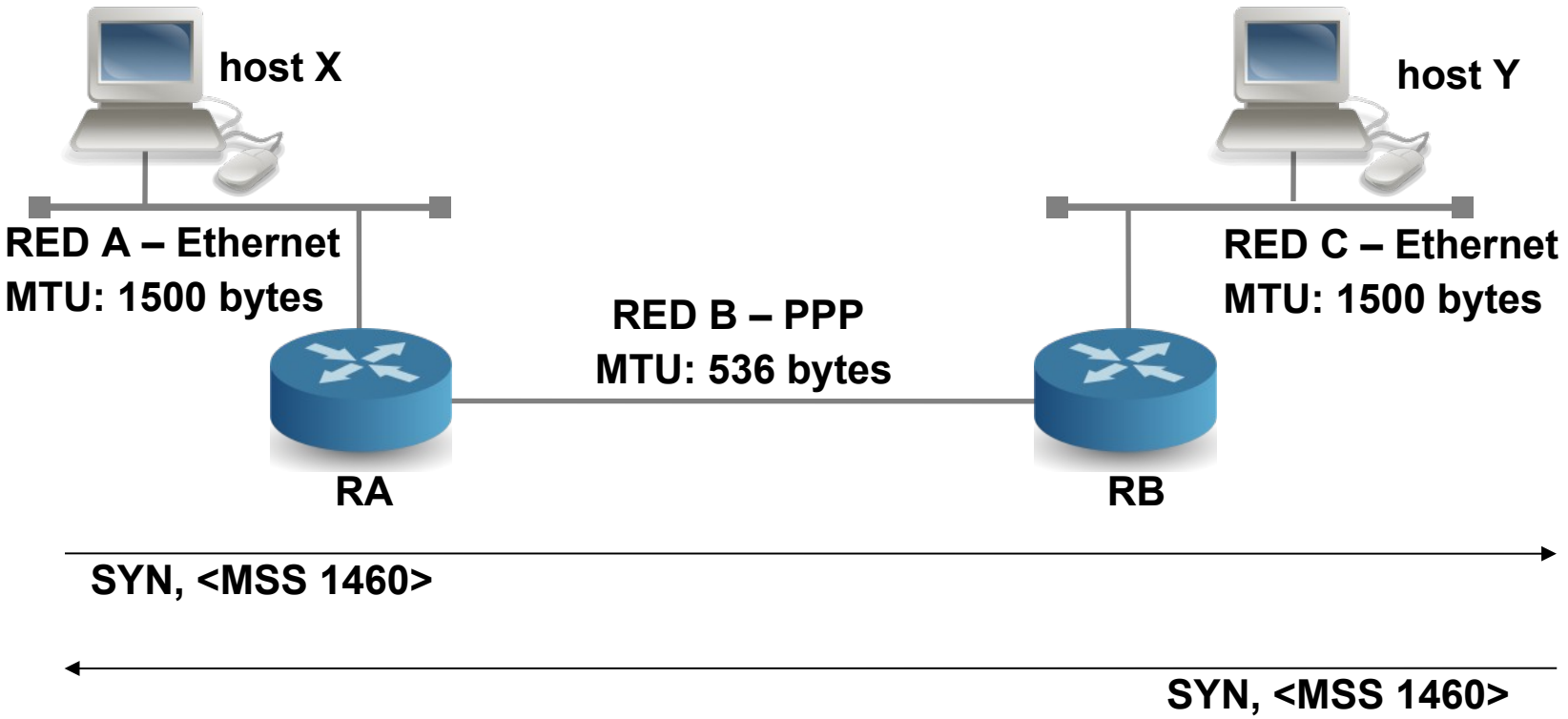
- Red B

Fragmento 3

Fragmento 3
Identificación: _____
DF: __
MF: __
Offset: ____
Long. total: _____

- Red C
  - ¿Qué fragmentos circulan por la red C: los mismos que por la red A o por la red B?

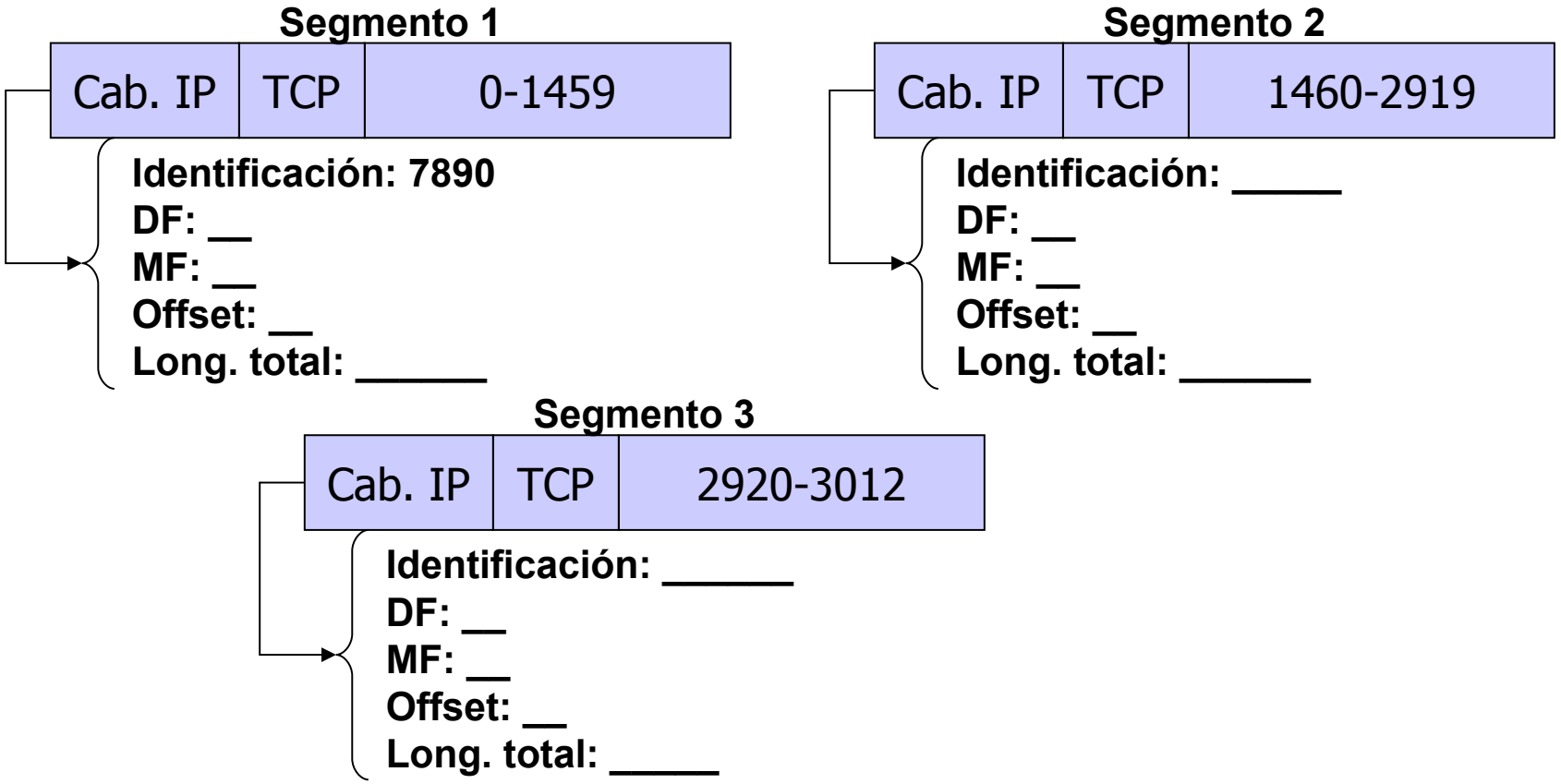
Fragmentación IP: Ejercicio 3



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

Fragmentación IP: Ejercicio 3

- Red A



Fragmentación IP: Ejercicio 3

- Red B

Fragmento 1.1
Identificación: _____
DF: __
MF: __
Offset: __
Long. total: _____

Fragmento 1.2
Identificación: _____
DF: __
MF: __
Offset: ___
Long. total: _____

Fragmento 1.3
Identificación: _____
DF: __
MF: __
Offset: ____
Long. total: _____

Fragmentación IP: Ejercicio 3

- Red B

Fragmento 1.1
Identificación: _____
DF: __
MF: __
Offset: __
Long. total: _____

Fragmento 1.2
Identificación: _____
DF: __
MF: __
Offset: ___
Long. total: _____

Fragmento 1.3
Identificación: _____
DF: __
MF: __
Offset: ____
Long. total: _____

Fragmentación IP: Ejercicio 3

- Red B

Segmento 3

Identificación: _____
DF: __
MF: __
Offset: ____
Long. Total: _____

- Red C
  - ¿Qué fragmentos circulan por la red C: los mismos que por la red A o por la red B?

Resumen

- Principales comandos de red:
  - **ip address**: ver configuración de red.
  - **netstat**: ver puertos ocupados y más cosas.
  - **nslookup** y **dig**: enviar peticiones DNS.
  - **route**: ver y modificar la tabla de enrutamiento.
  - **ping**
  - **traceroute**
    - Versión gráfica: https://traceroute-online.com/
    - Desde múltiples orígenes: https://tools.keycdn.com/traceroute