

Alta Disponibilidad en Redes

Ruteo

Tablas de ruteo

Acceso dividido

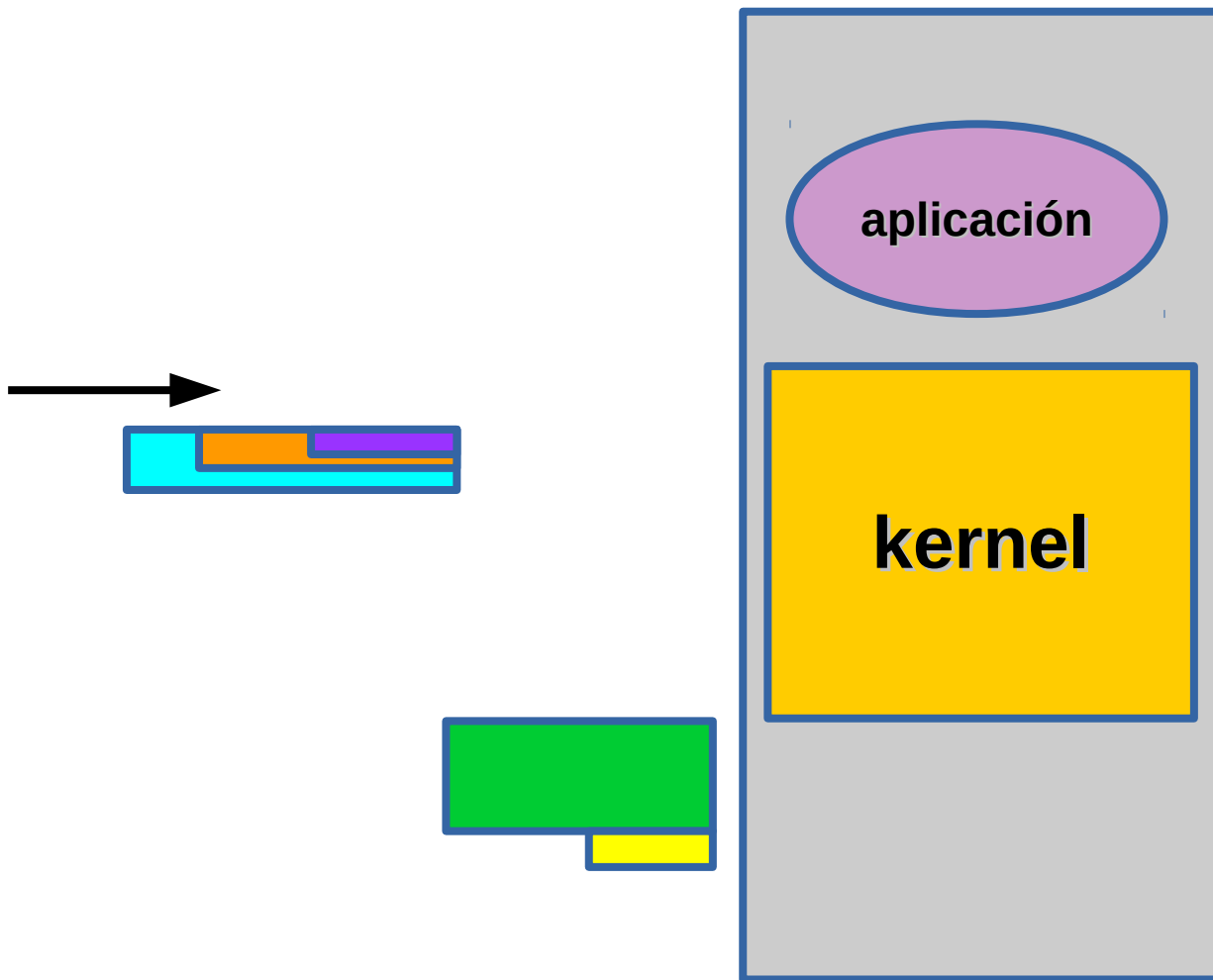
Ruteo por origen

Clasificación de tráfico

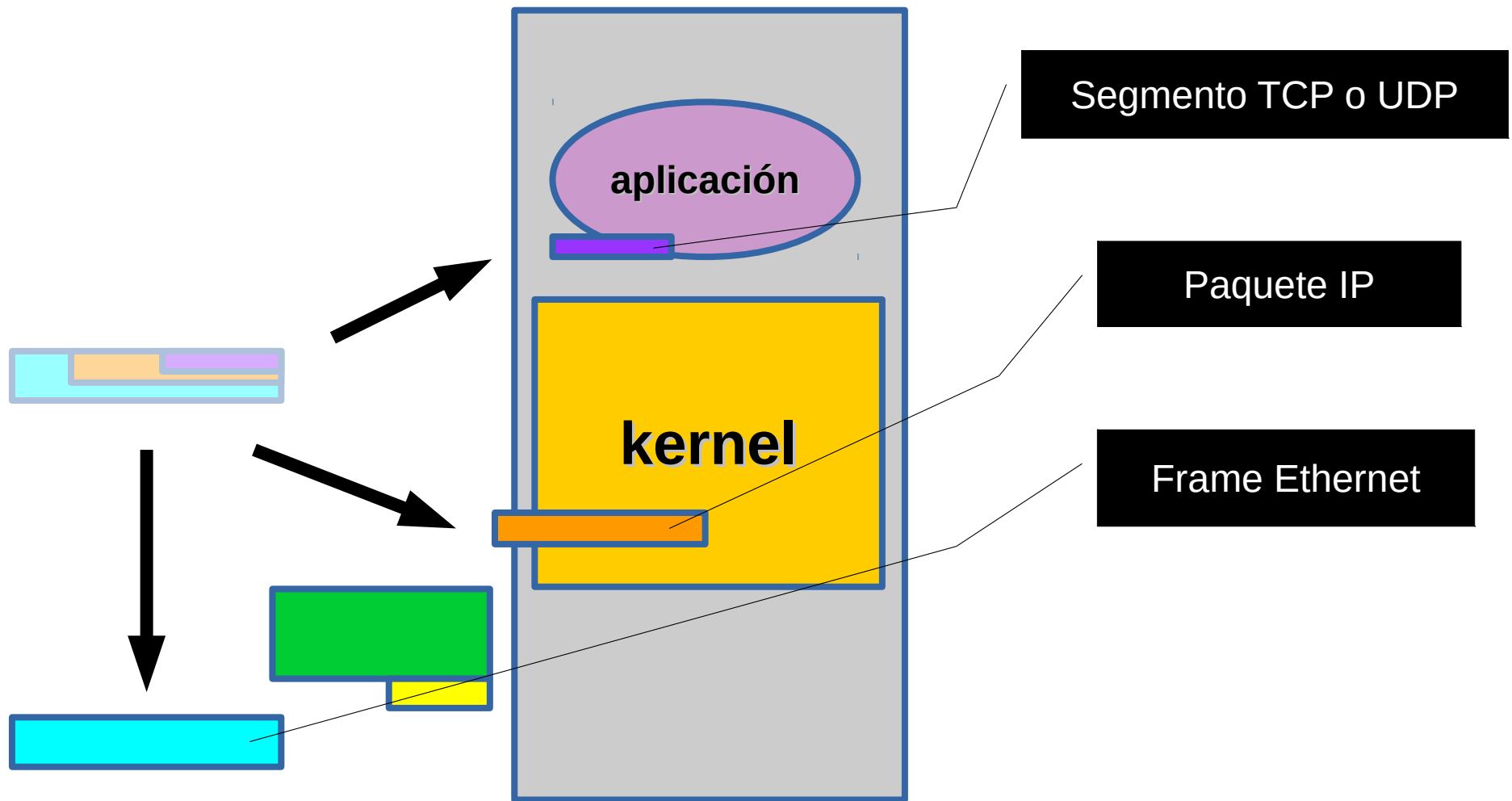
Balance de carga

Utilitarios ip e iptables

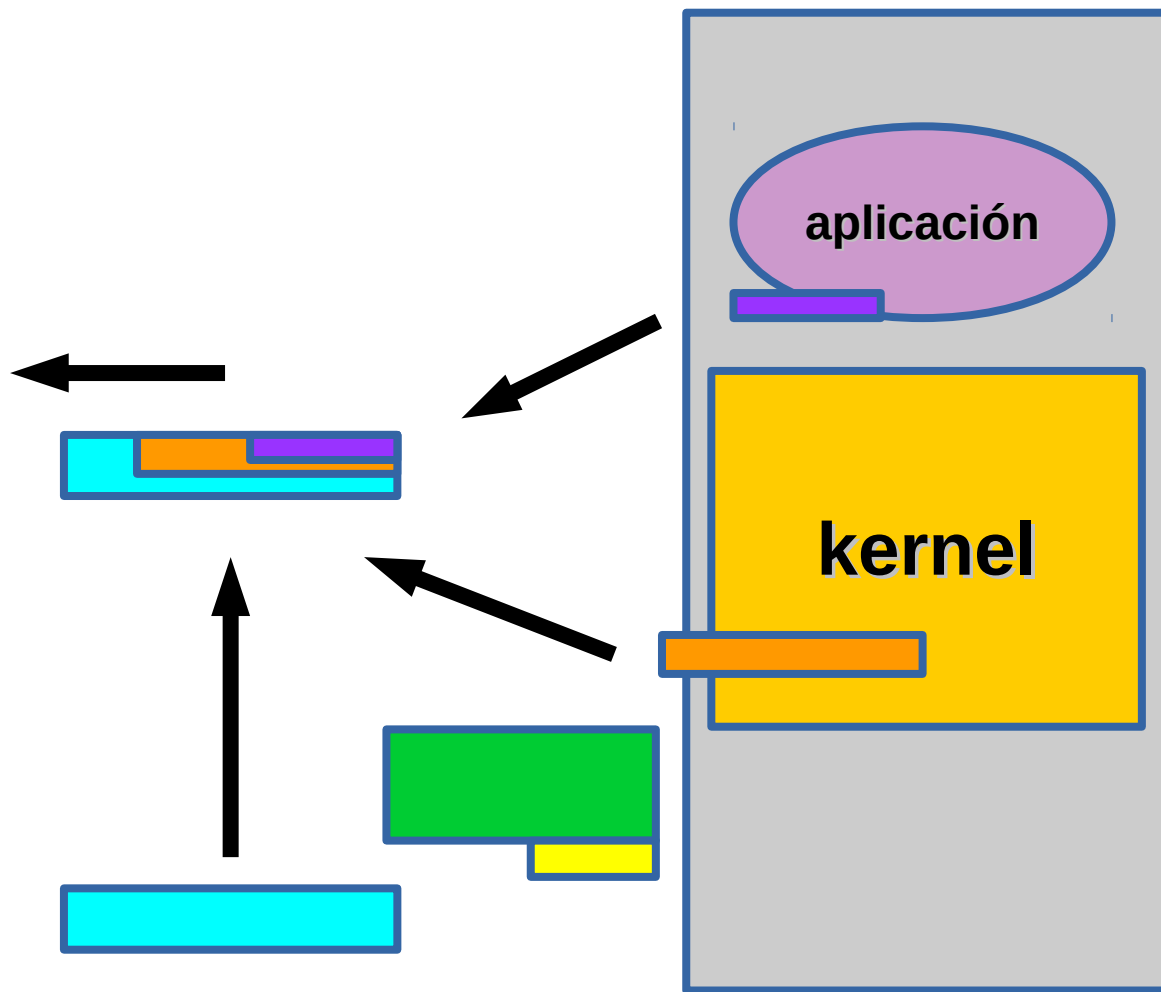
El viaje de los paquetes



El viaje de los paquetes



El viaje de los paquetes



El viaje de los paquetes

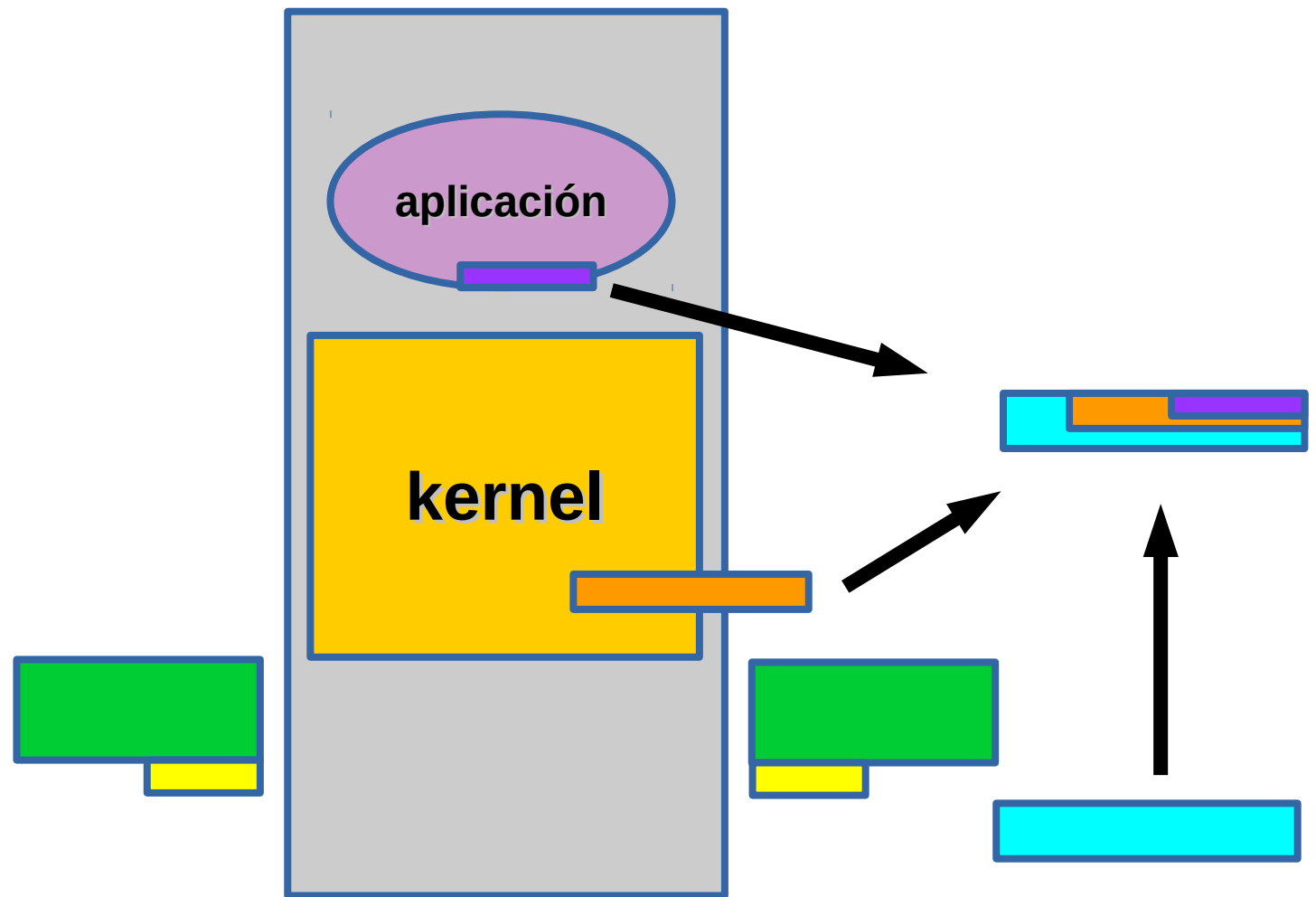


Tabla de ruteo

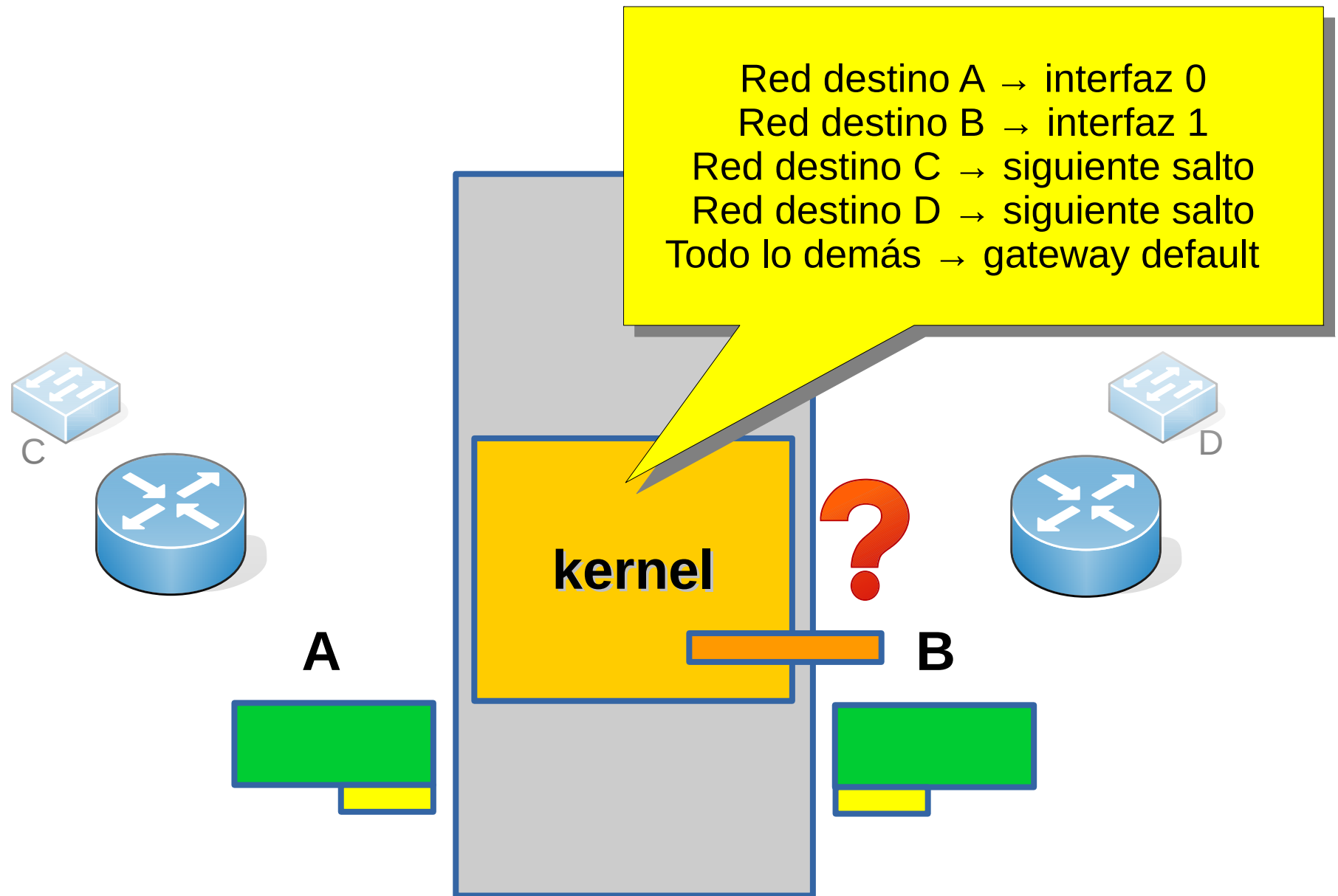
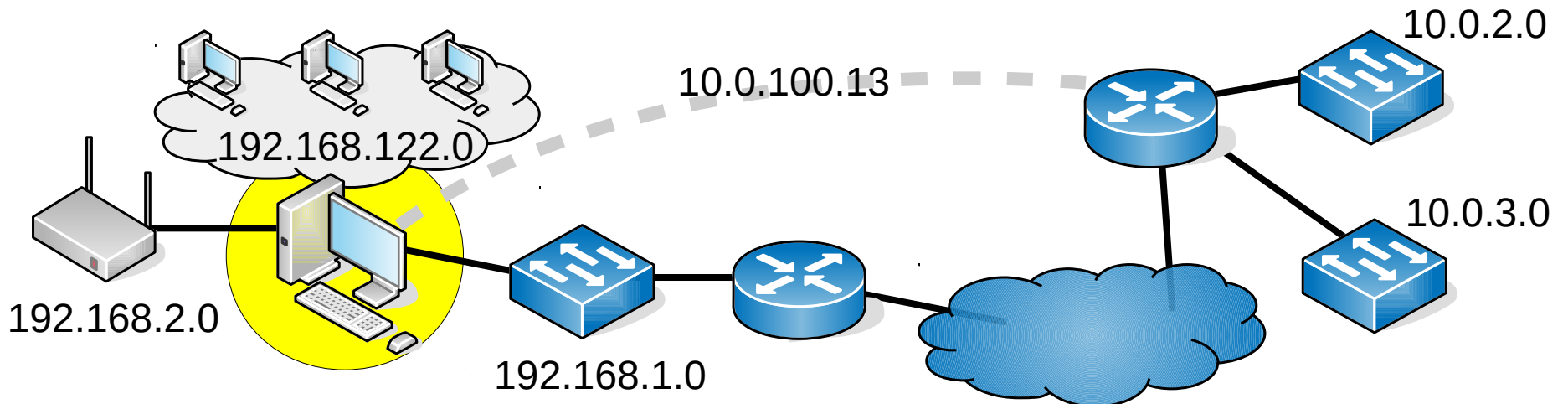


Tabla de ruteo

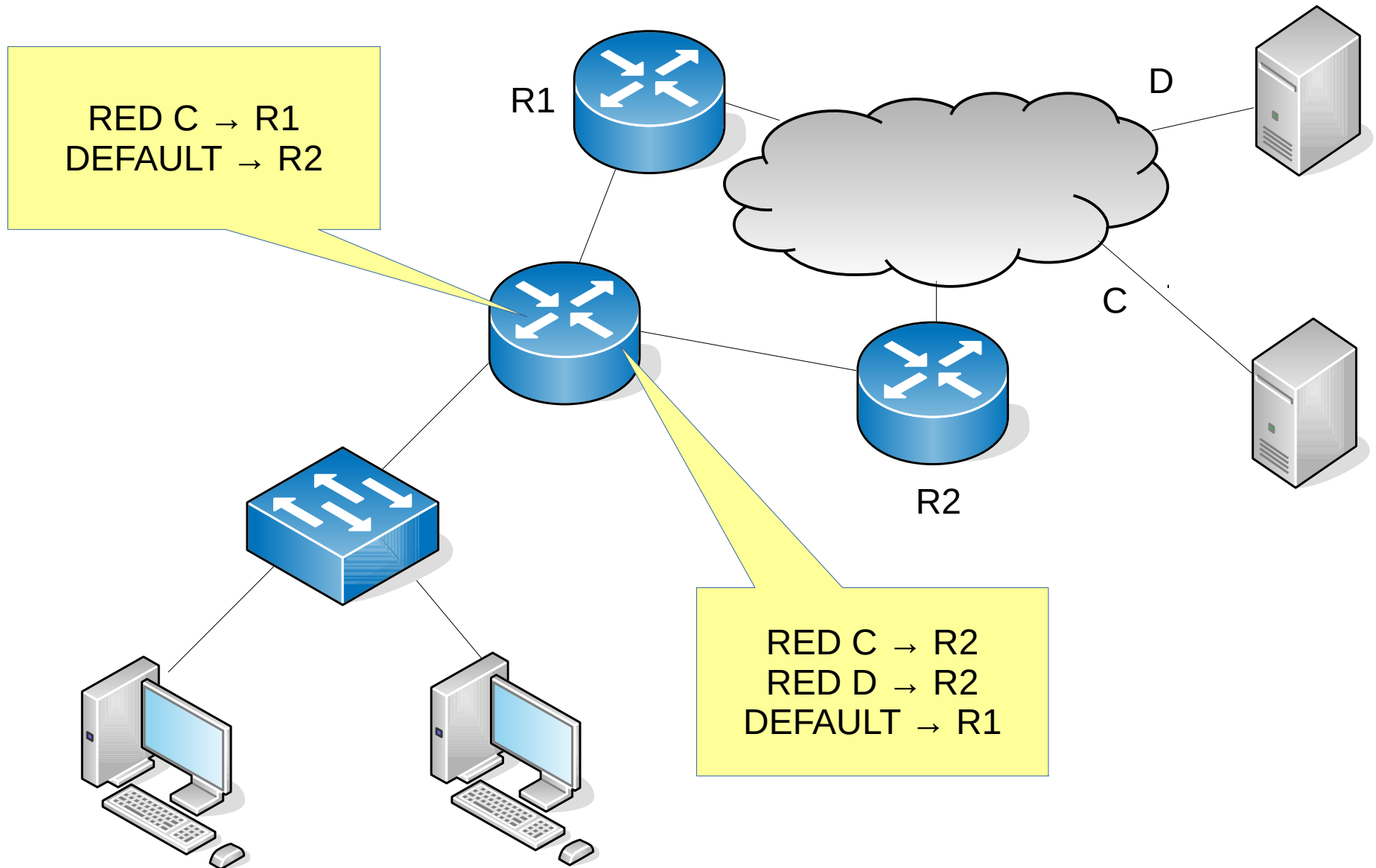
```
$ route -n
```

Kernel IP routing table

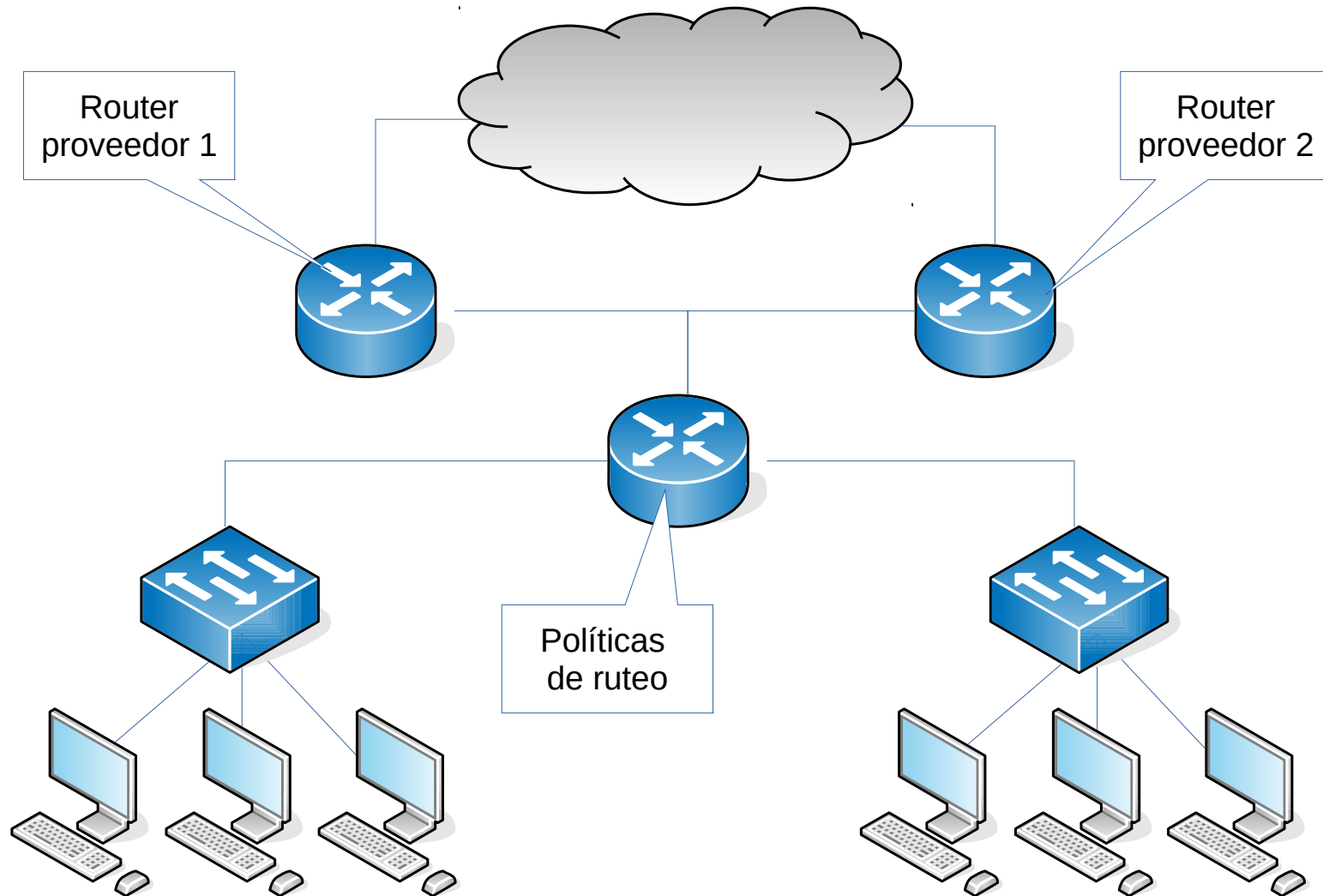
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.1.1	0.0.0.0	UG	1024	0	0	eth0
10.0.2.0	10.0.100.13	255.255.255.0	UG	0	0	0	tun0
10.0.3.0	10.0.100.13	255.255.255.0	UG	0	0	0	tun0
10.0.100.13	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.122.0	0.0.0.0	255.255.255.0	U	0	0	0	virbr0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	wlan0



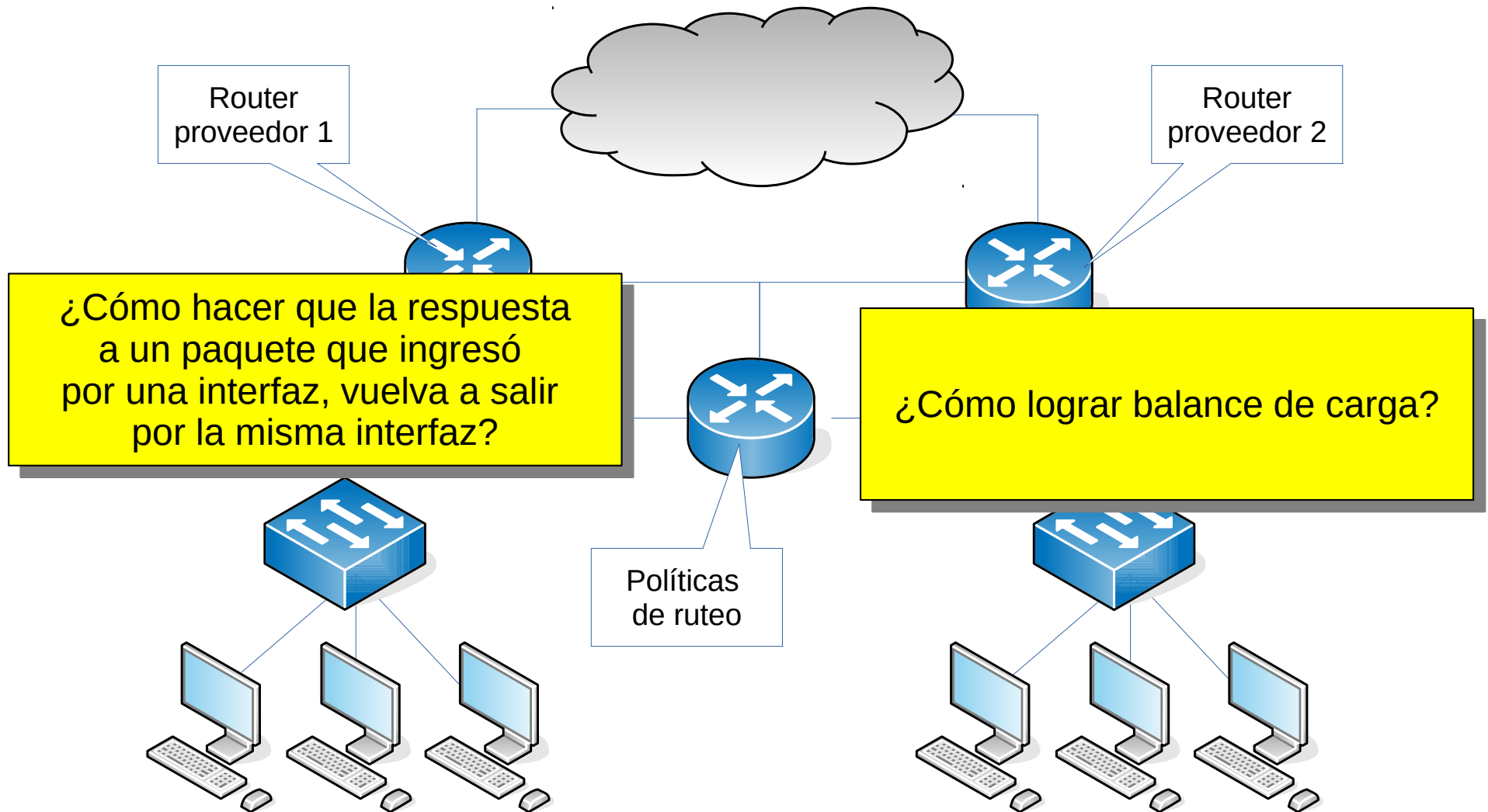
Más de una tabla de ruteo



Split access (acceso dividido)



Split access (acceso dividido)



Ruteo por políticas

- Usado en routers
- Más de una tabla de ruteo
 - Tabla **main** (por defecto) y las creadas por el usuario
- Algún mecanismo para decidir qué tabla de ruteo se aplicará a cada paquete que es reenviado
 - Si no se encuentra una regla para asignar una tabla, se utiliza la tabla main
 - Las reglas en una tabla específica tendrán prioridad sobre cualquiera de las de la tabla main

¿Qué tabla de ruteo se usará?

1

- Política según el origen
 - Los paquetes usan una tabla de ruteo u otra dependiendo de cuál es la dirección de host o de red origen

2

- Política según la clase de tráfico
 - Los paquetes se clasifican según criterios arbitrarios
 - Origen, destino, protocolo, aplicación...
 - Cada clase usa una tabla de ruteo asignada

3

- Política de balance de carga
 - Es posible establecer una ruta por defecto *multipath*
 - Toma alternativamente uno de varios caminos
 - Alterna entre ellos en alguna proporción de veces definida por el usuario

Comando ip

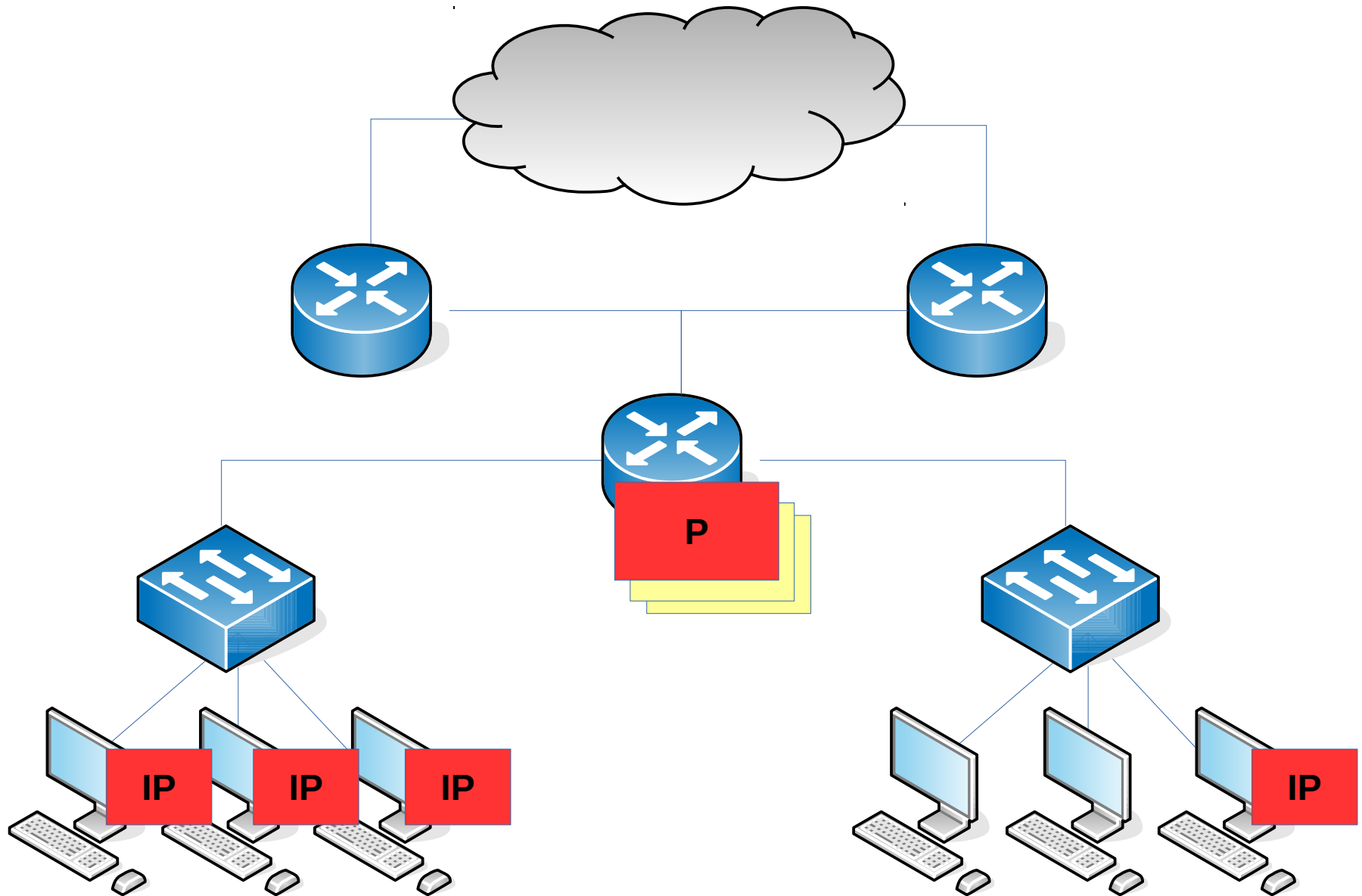
Comando	Propósito
<code>ip link list</code>	Consultar interfaces del sistema
<code>ip address show</code>	Consultar direcciones de las interfaces
<code>ip neigh show</code>	Tabla ARP del sistema
<code>ip route show</code>	Tabla de ruteo
<code>ip route list table main</code>	Tabla de ruteo principal
<code>ip route list table T</code>	Tabla de ruteo T
<code>ip route flush table main</code>	Borrar rutas de tabla principal
<code>ip rule add from 10.0.0.0/24 table T</code>	Agregar una regla de asignación de tabla de ruteo
<code>ip rule list</code>	Consultar las reglas de asignación ingresadas

S.A. con política según el origen

- Política según el origen
 - La idea es simplemente separar los hosts de las redes locales en grupos, estáticamente, por cualquier criterio conveniente
 - Y derivar el tráfico de cada grupo por rutas diferentes y fijas
- Por cada host o red con dirección **IP** que se quiere conducir por el acceso **P**:
 - `ip rule add from IP table P`
 - **P** puede ser un número, o un nombre agregado al archivo `/etc/iproute2/rt_tables`



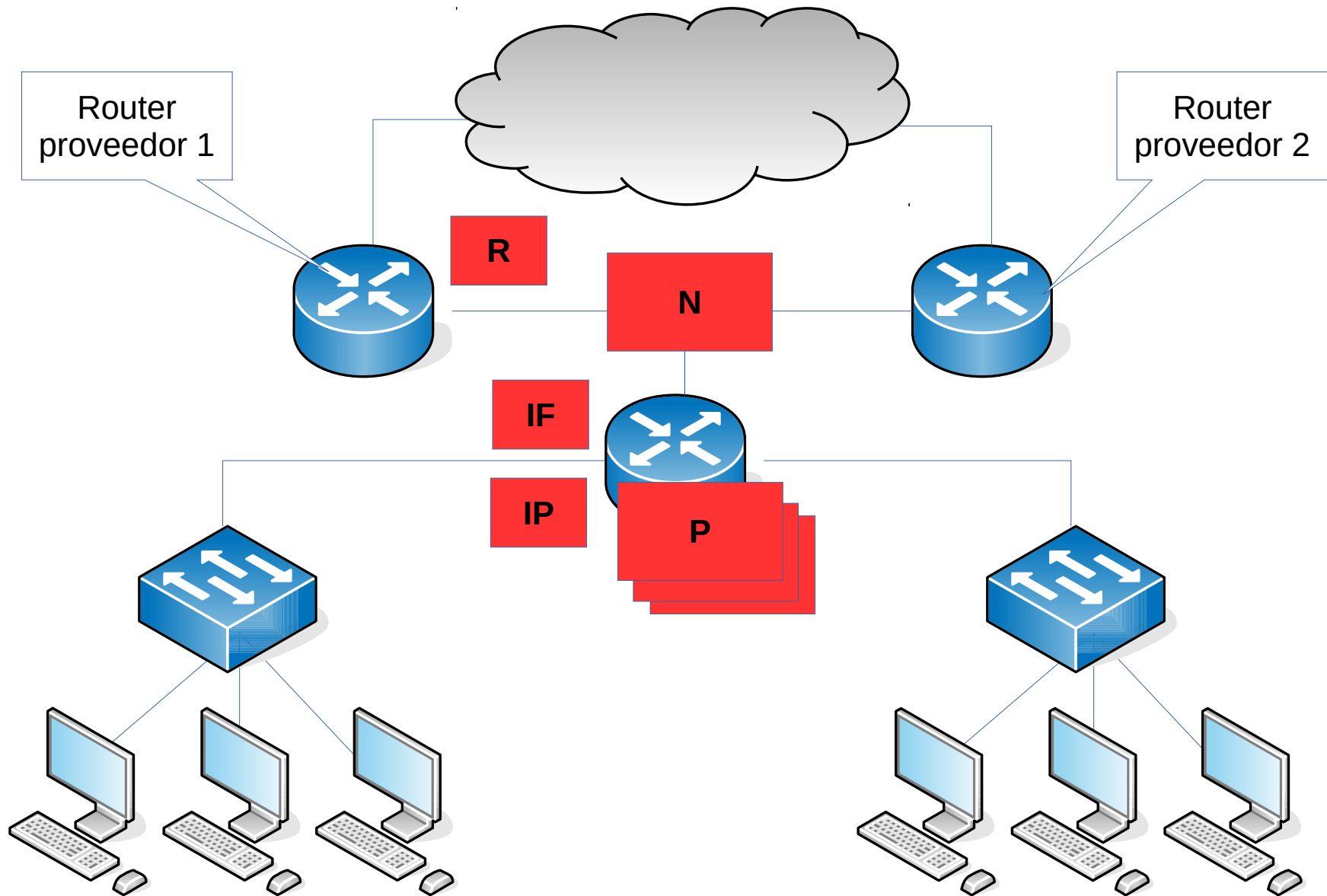
S.A. con política según el origen



S.A. con política según el origen

- Datos de cada acceso
 - Id de la tabla de ruteo (**P**)
 - Número o nombre en /etc/iproute2/rtable
 - Dirección del router del proveedor (**R**)
 - Dirección de la red donde se ubica el router del proveedor (**N**)
 - Interfaz del router de la organización que comunica con el router del proveedor (**IF**)
 - Dirección de dicha interfaz (**IP**)
- Con estos datos, por cada acceso disponible:
 - 1. Se insertan las reglas de ruteo en la tabla correspondiente:
 - `ip route add N dev IF src IP table P`
 - `ip route add default via R table P`
 - 2. Se inserta en la tabla **main** la regla de ruteo al gateway de ese acceso:
 - `ip route add N dev IF src IP`

S.A. con política según el origen



S.A. con clases de tráfico

- Política según la clase de tráfico
 - Se definen clases de tráfico por conjuntos de condiciones
 - Los paquetes que cumplen cada conjunto de condiciones pertenecen a una clase de tráfico
 - El comando iptables permite reconocer las condiciones y marcar los paquetes



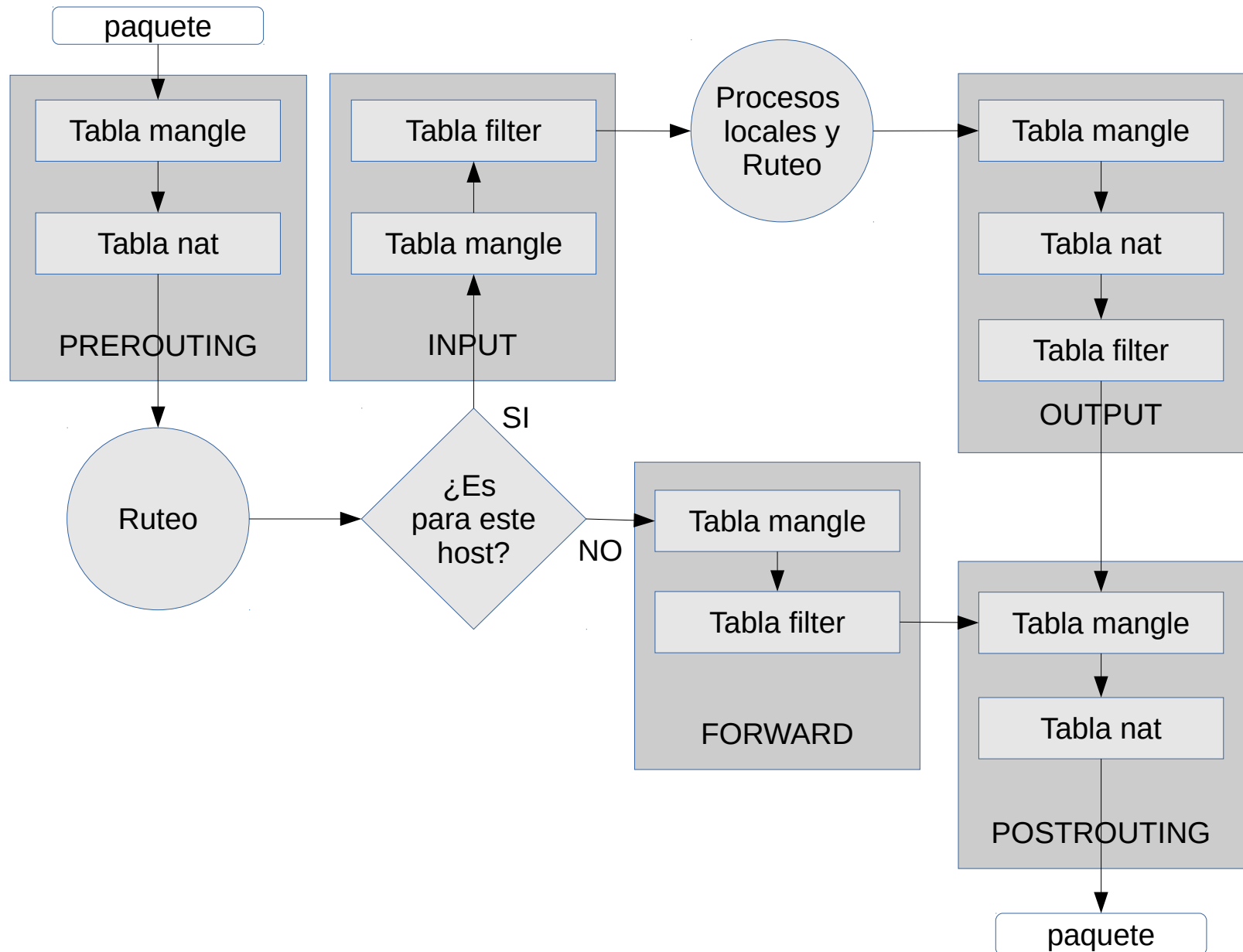
Netfilter e iptables

- Netfilter: mecanismo general del kernel para manipular paquetes IP
- Iptables: comando de usuario para controlar Netfilter
- Distingue los paquetes según tres clases
 - Entrantes (dirección destino pertenece al host)
 - Salientes (dirección origen pertenece al host)
 - A reenviar (ninguna de las direcciones pertenece)
- Usos
 - Firewalls, ingeniería de tráfico, marcado de paquetes para casos especiales de ruteo...

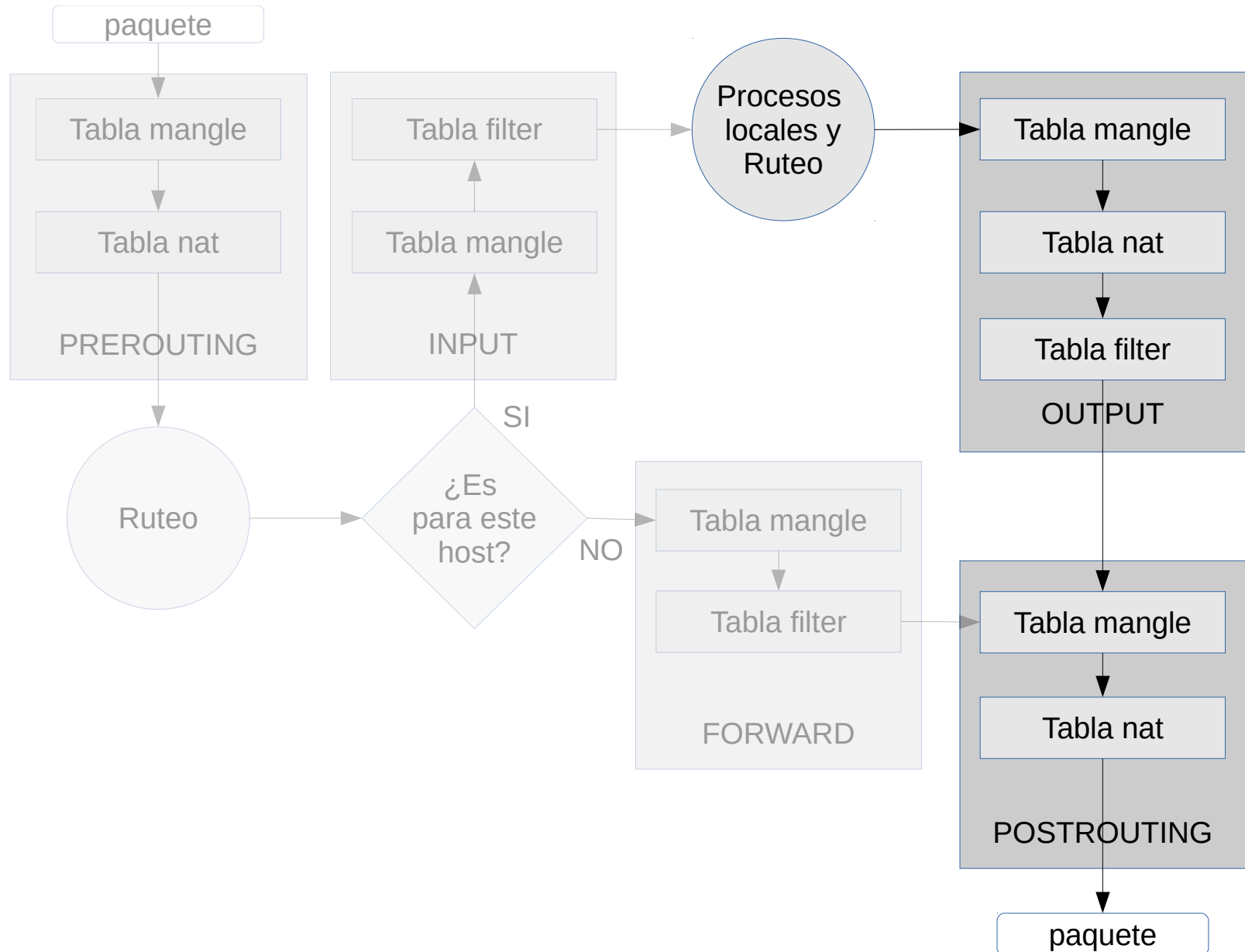
Netfilter e iptables

- **Reglas**
 - **Condiciones** que cumple cada paquete y **acciones** que se tomarán en cada caso
 - Se agrupan en **cadenas** ubicadas en **tablas**
- **Condiciones**
 - Interfaz de entrada o de salida
 - Direcciones origen o destino, redes de origen o de destino
 - Protocolo de transporte TCP o UDP, ports origen o destino
- **Cadenas**
 - Según el lugar donde se aplican las reglas en el camino del paquete a través del kernel
 - INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING
 - Otras cadenas definidas por el usuario
- **Tablas**
 - Según la función o propósito de las reglas
 - Tablas raw, mangle, nat, filter, security
- **Acciones**
 - ACCEPT, REJECT, DROP, MASQUERADE, MARK, TRACE
 - <http://www.iptables.info>

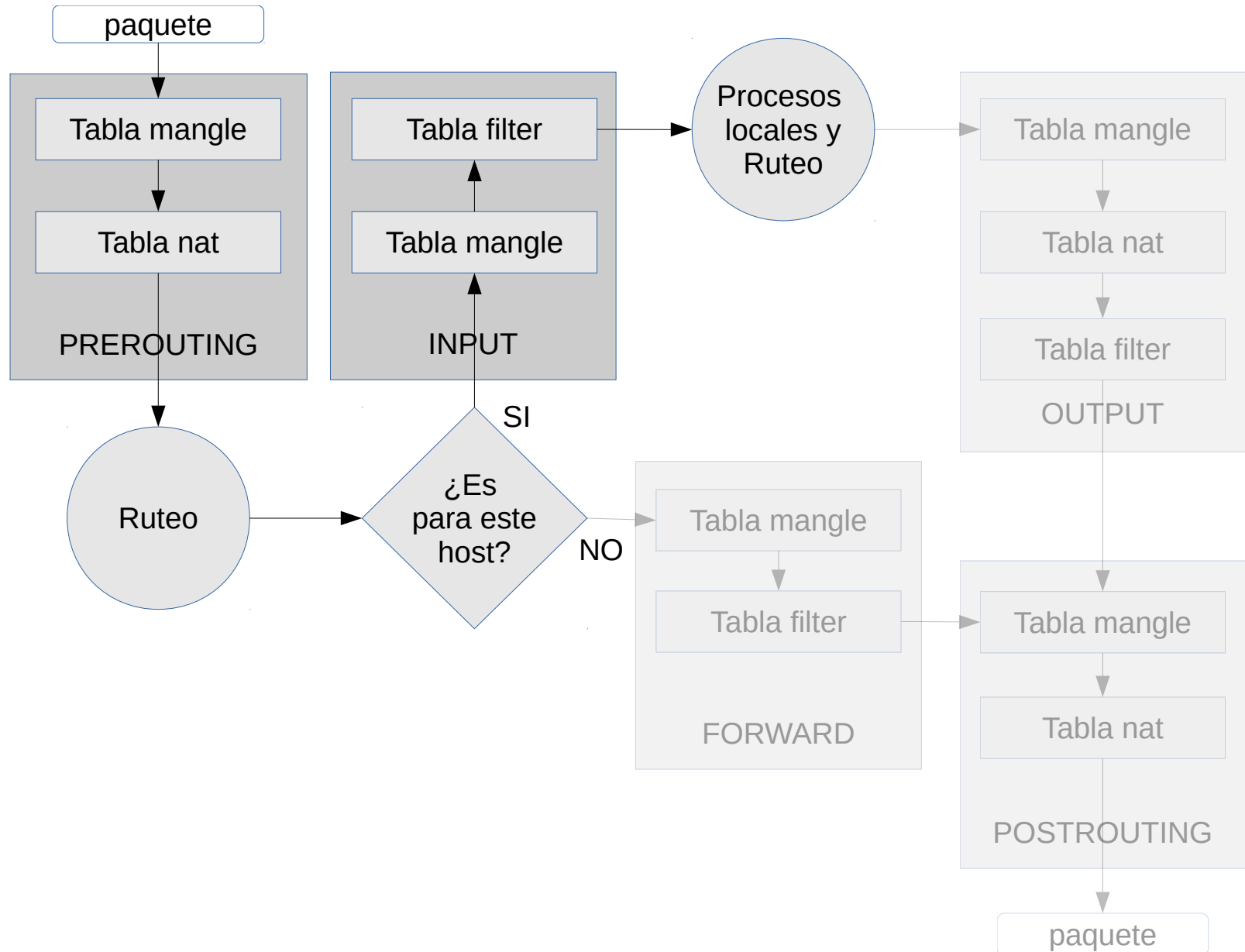
Tablas y cadenas



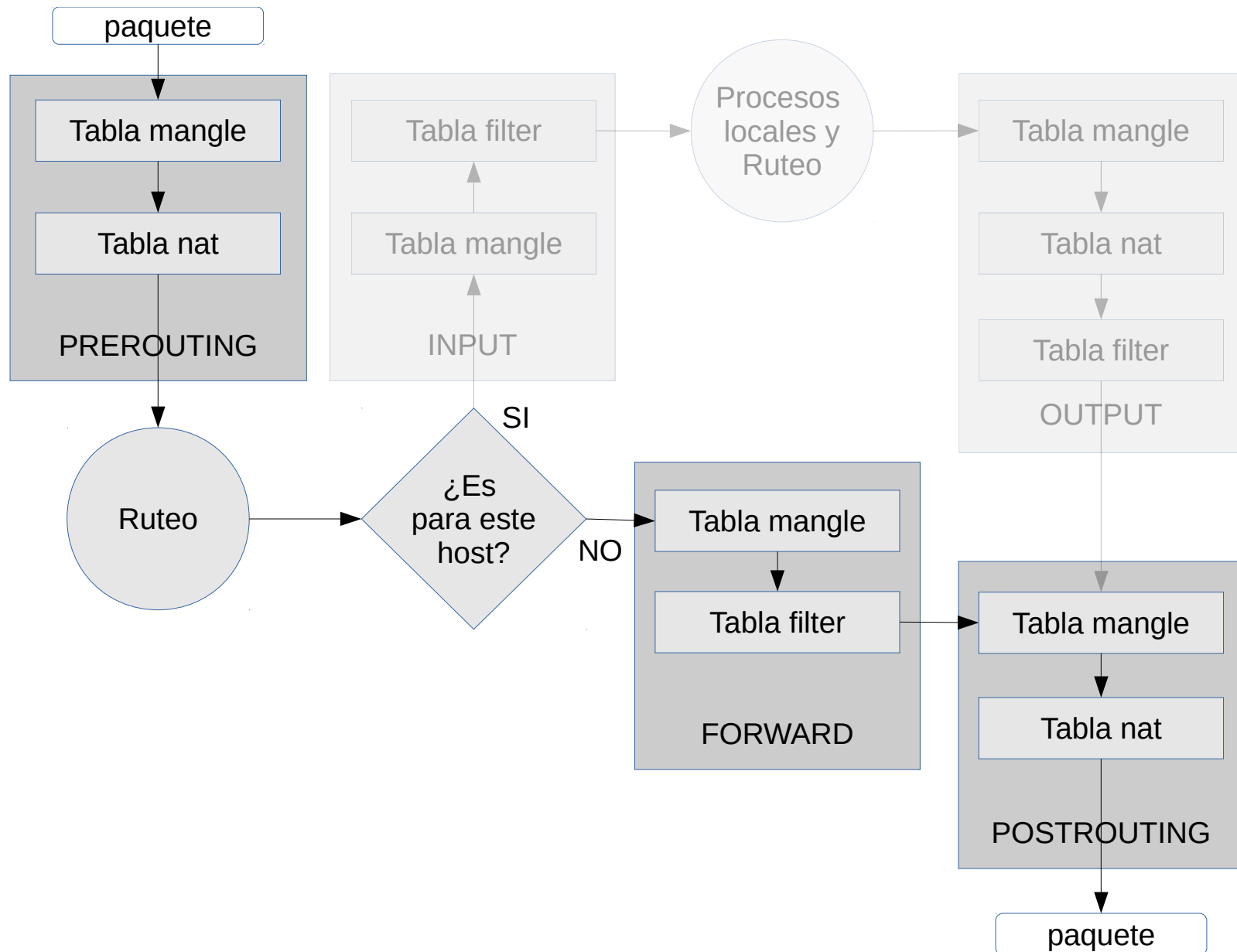
Paquetes salientes



Paquetes entrantes



Paquetes reenviados



Políticas por clase de tráfico

- Como antes, se definen las tablas de ruteo por cada acceso
- Se definen las reglas que marcan cada clase de tráfico:

```
iptables -t mangle -A PREROUTING -p tcp  
--dport X -s S -d D -j MARK --set-mark Z
```
- Luego se establecen las reglas que derivan el tráfico con cada marca Z a la tabla de ruteo P que se desee:

```
ip rule add fwmark Z table P
```

Política de balance de carga

- La ruta por defecto del router de la organización puede alternarse entre dos o más accesos
- El administrador define la proporción en que se utilizan

```
ip route add default scope global nexthop  
via R1 dev IF1 weight W1 nexthop via R2 dev  
IF2 weight W2
```

- W1 y W2 son pesos numéricos que se encuentran en la relación deseada (p. ej. W1=1, W2=2).