Bloque IV: El nivel de red

Tema 7: IP

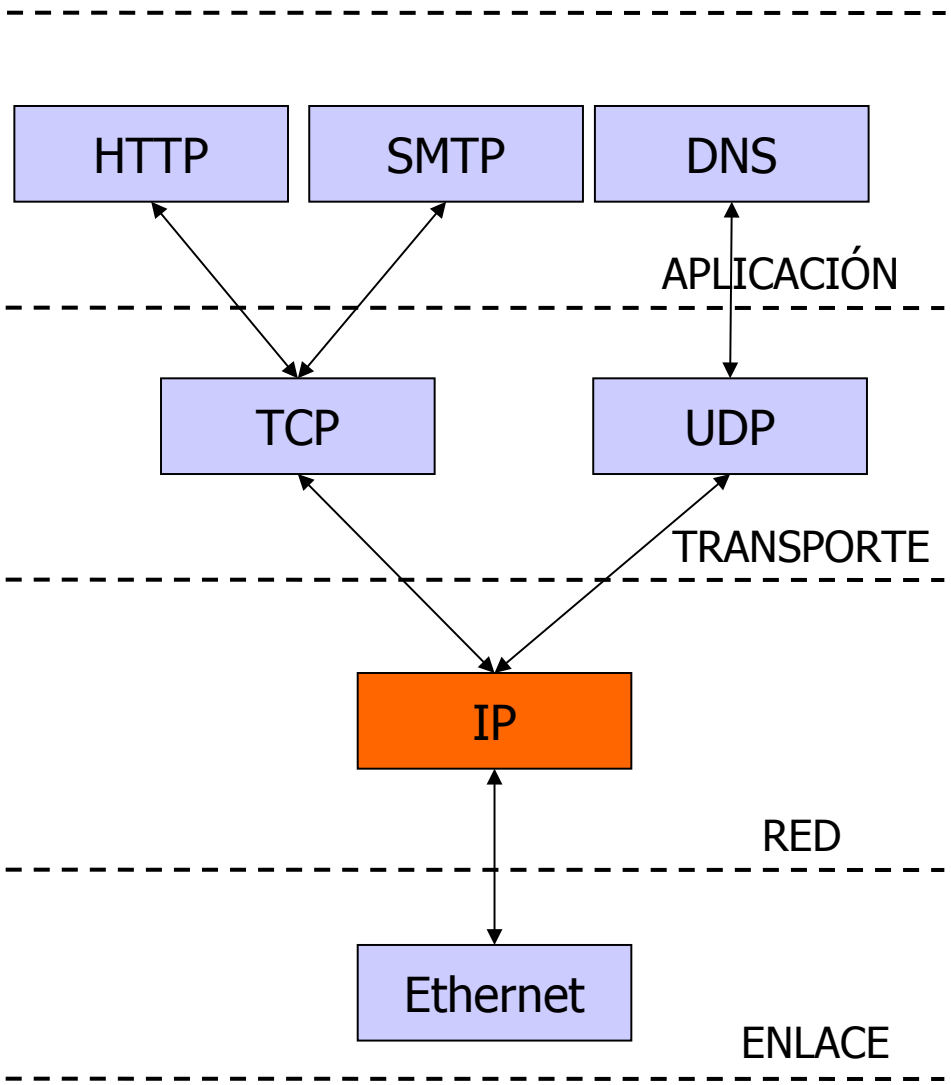
Índice

- Bloque IV: El nivel de red
  - Tema 7: IP
    - Introducción
    - Cabecera IP
    - Subredes
      - Introducción
      - Máscara de subred
      - Direcciones de subred
      - Subredes de tamaño variable
    - DHCP
    - NAT

- **Lecturas recomendadas:**
  - Capítulo 4, secciones 4.4.1 y 4.4.2, de “Redes de Computadores: Un enfoque descendente”. James F. Kurose, Keith W. Ross. Addison Wesley.

Introducción

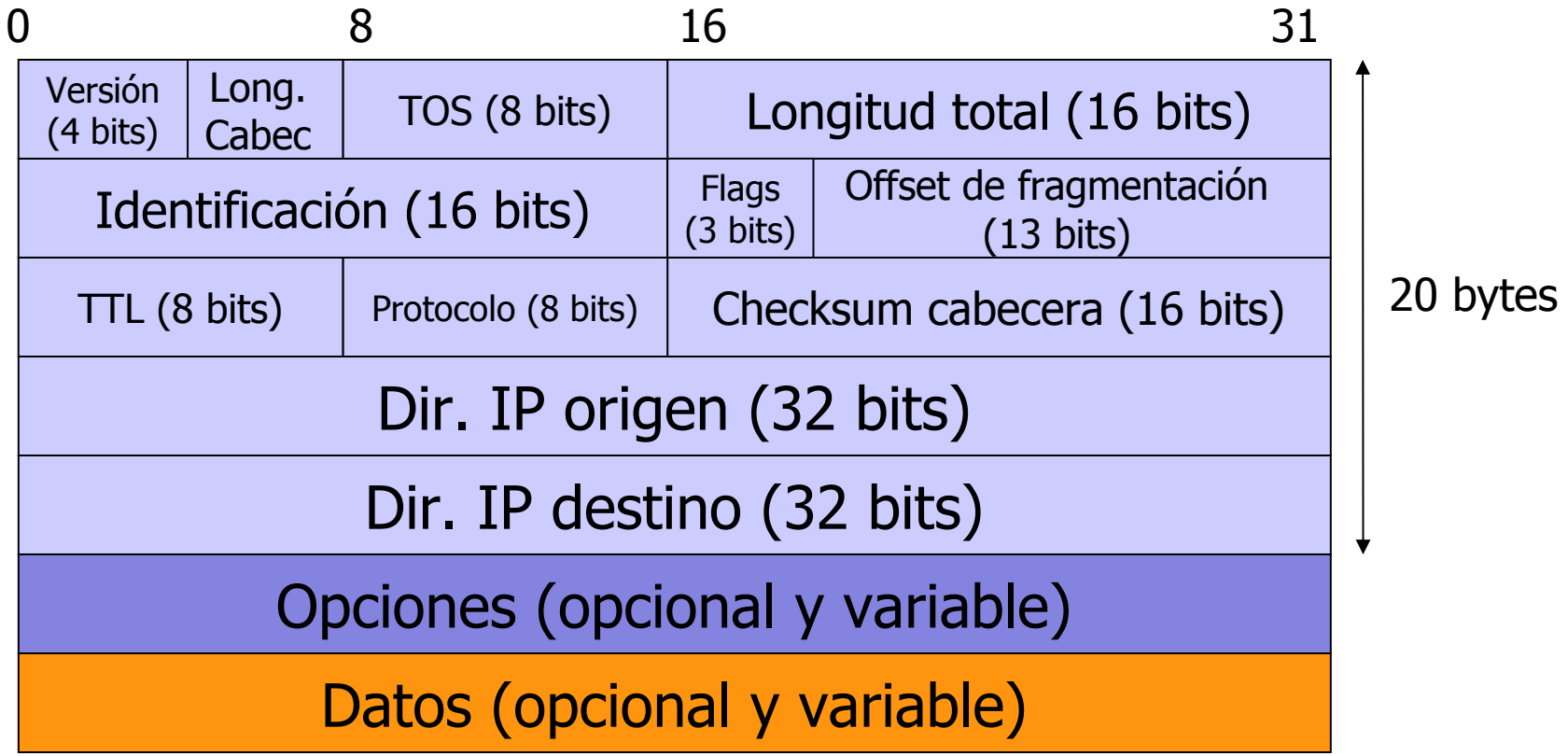
- Internet Protocol – Especificado en el RFC 791.
- IP proporciona un servicio de entrega de datagramas **no fiable** y **no orientado a conexión**.



Introducción

- No fiable:
  - No hay garantías de que un datagrama alcance su destino final.
  - IP sigue un modelo “best effort”: lo hará “*lo mejor que pueda*”.
  - En caso de que haya algún problema, IP tiene un sistema de gestión de errores simple: descartar algún datagrama (normalmente el último recibido).
- No orientado a conexión:
  - IP no mantiene información del estado de los datagramas.
  - Cada datagrama es tratado independientemente → Dos datagramas hacia un mismo destino pueden seguir caminos diferentes.
  - Los datagramas se pueden recibir desordenados.

Cabecera IP


0
8
16
31
Versión (4 bits)
Long. Cabec
TOS (8 bits)
Longitud total (16 bits)
Identificación (16 bits)
Flags (3 bits)
Offset de fragmentación (13 bits)
TTL (8 bits)
Protocolo (8 bits)
Checksum cabecera (16 bits)
Dir. IP origen (32 bits)
Dir. IP destino (32 bits)
Opciones (opcional y variable)
Datos (opcional y variable)
20 bytes

Cabecera IP

- TCP/IP usa la ordenación de bytes “big endian” (de izqda a dcha):
  - Si un equipo usa el formato “little endian” (de dcha a izqda) debe hacer la conversión al transmitir y al recibir.

- **Versión**: Versión actual de IP (4).
- **Longitud de cabecera**: Número de palabras de 32 bits de la cabecera, incluidas las opciones si las hubiera (< 60 bytes).

- **Tipo de servicio** (TOS): diseñado para QoS (Quality of Service), aunque nunca fue ampliamente usado. Redefinido (RFC 2474, 3260) en dos campos:
  - **Servicios diferenciados** (DS): campo de 6 bits utilizado para dar soporte a QoS mediante la técnica de DS.
  - **Explicit Congestion Notification** (ECN): indicador de congestión o futura congestión en un router (2 bits).

Cabecera IP

- **Longitud total:** longitud total de datagrama IP en bytes.
  - Longitud total – longitud cabecera = tamaño datos.
  - Campo de 16 bits: máximo tamaño es 65535 bytes.
  - Se precisa este campo porque algunos protocolos del nivel inferior pueden no conocer de manera precisa el tamaño del datagrama encapsulado.
  - Por ejemplo, en Ethernet el tamaño mínimo de datos son 46 bytes, por lo que puede ser necesario un relleno. Un datagrama IP puede ser menor y, en ese caso, IP no sabría cuanto de esos 46 bytes son realmente datos 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.

Cabecera IP

- **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: valor recomendado 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.

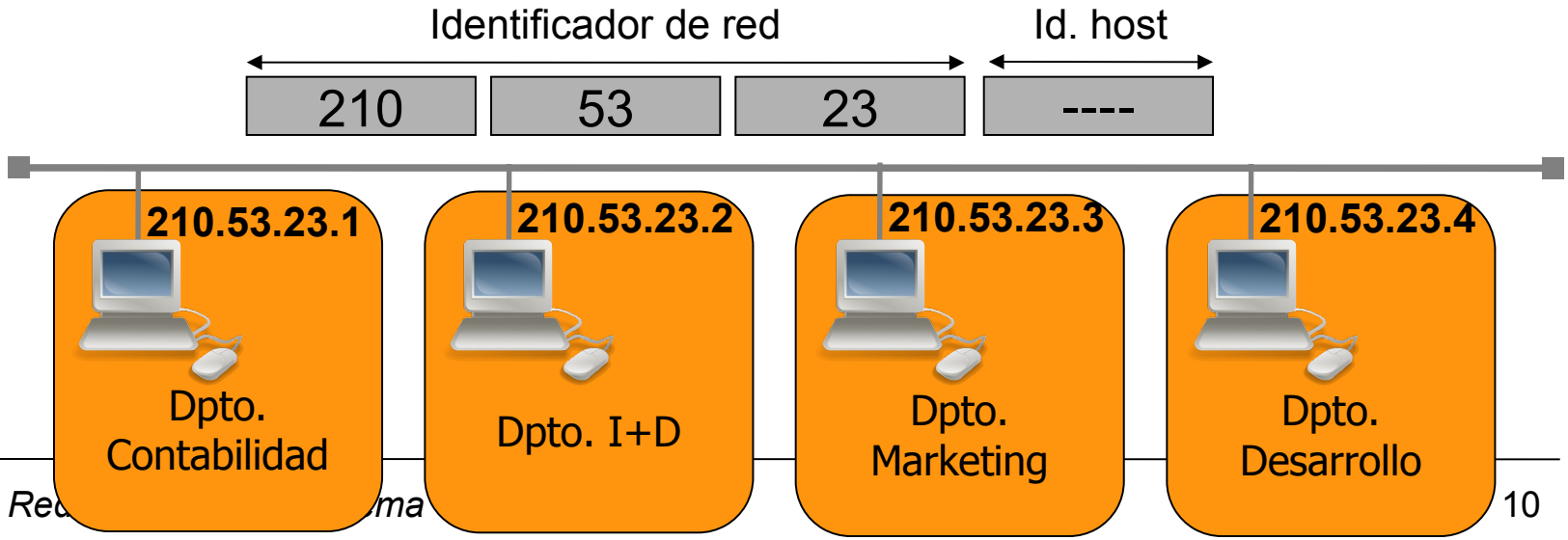
- **Dirección IP de origen y destino**: 32 bits cada una.

Cabecera IP

- **Opciones**: Información opcional de longitud variable. Algunas opciones son:
  - Registro de enrutamiento (record route): cada router marca su hora y dirección IP (máximo 9 routers).
  - Timestamp: se registra 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).
  - NoOp: la longitud ha de ser múltiplo de 32 bits. Esta opción permite añadir bytes de relleno para cumplir esta condición.

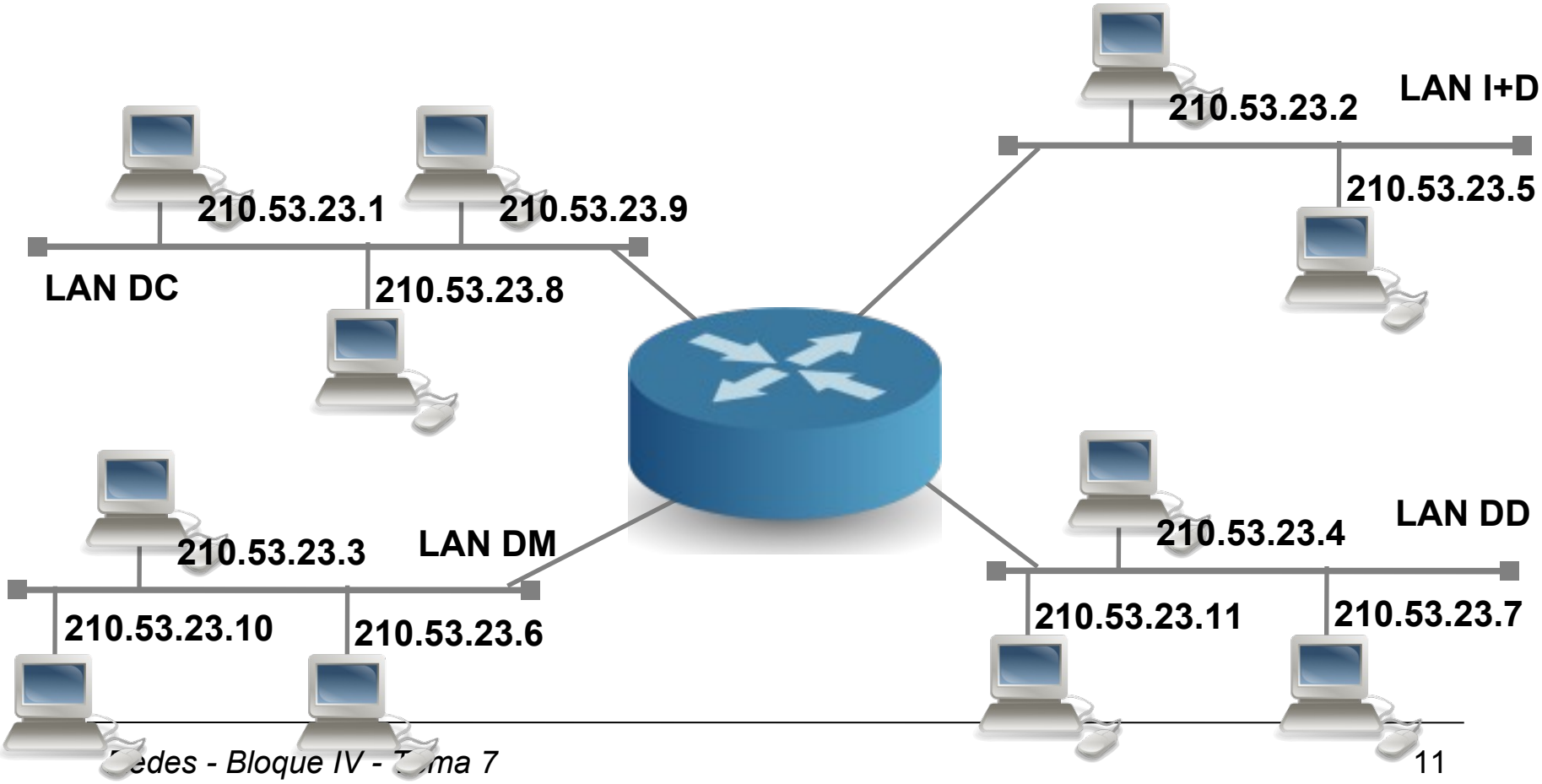
Subredes: Introducción

- Subredes: consiste en dividir una red en partes mas pequeñas.
  - Nivel jerárquico intermedio entre red y host.
  - Utiliza unos bits de la parte del identificador de host para la subred.
  - Organización jerárquica de la red→ Visión externa como una sola red, aunque internamente esté dividida en subredes.
- Por ejemplo, partimos de una dirección clase C: 210.53.23.0
  - Tenemos una empresa y 4 departamentos.
  - Inicialmente no realizamos ningún tipo de división, porque la empresa es demasiado pequeña.



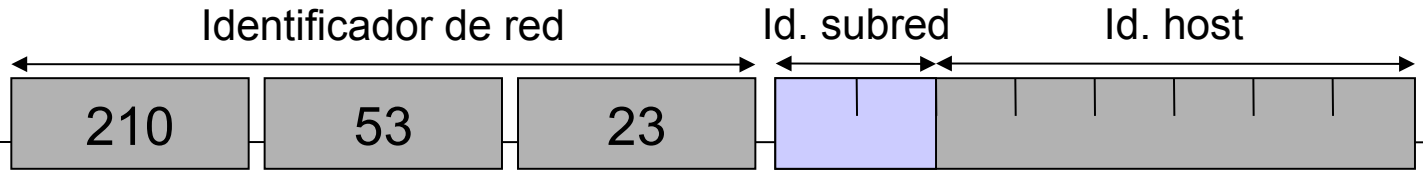
Subredes: Introducción

- Pero la empresa crece, y cada departamento necesita una LAN → Solución: asignar aleatoriamente las direcciones IP.
- Problema: la tabla de enrutamiento para el router es enorme (necesito una entrada para cada máquina).



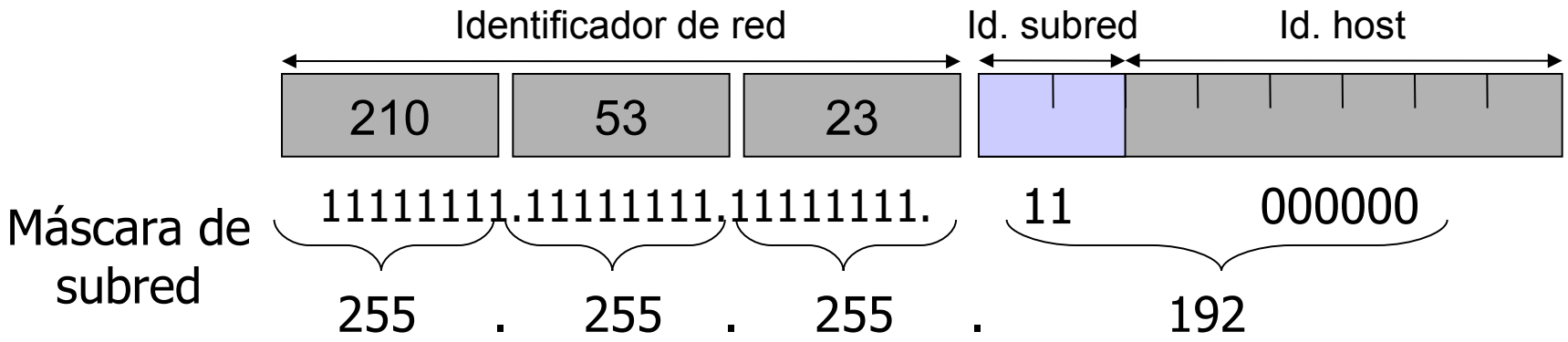
Subredes: Introducción

- Solución → Subredes: dividir el espacio de direcciones en 4 grupos.
  - 0-255
    - 0-63 para el dpto. de contabilidad
    - 64-127 para el dpto. de I+D
    - 128-191 para el dpto. de marketing
    - 192-255 para el dpto. de desarrollo
- Y en binario:
  - 0-255
    - 0-63 = 00 XX XXXX
    - 64-127 = 01 XX XXXX
    - 128-191 = 10 XX XXXX
    - 192-255 = 11 XX XXXX
- **Identificador de subred**: con los 2 primeros bits del identificador de host, sabremos a que departamento (subred) pertenece una máquina.



Máscara de subred

- Indica cuantos bits forman el identificador de red y subred, y cuantos forman el identificador host.
  - Se ponen a 1 todos los bits correspondientes al identificador de red o subred.
  - Se ponen a 0 todos los bits correspondientes al identificador de host
- Cada máquina almacena su dirección IP y su máscara de subred.



- Una dirección IP siempre tiene una máscara asociada: 210.53.23.65 y 255.255.255.192
- Otra notación más breve: 210.53.23.65**/26** (se utilizan 26 bits para identificador de red y subred).

Máscara de subred: Ejercicio

- Indica los bits de identificador de red, subred y host para las siguientes IPs y máscaras:

10.58.26.129	181.23.117.89	198.58.201.89
255.255.0.0	255.255.255.0	255.255.255.0
bits red:	bits red:	bits red:
bits subred:	bits subred:	bits subred:
bits host:	bits host:	bits host:
10.58.26.129	181.23.117.89	198.58.201.89
255.255.240.0	255.255.254.0	255.255.255.192
bits red:	bits red:	bits red:
bits subred:	bits subred:	bits subred:
bits host:	bits host:	bits host:

Direcciones de subred

- Direcciones IP reservadas: en cada subred hay dos direcciones reservadas → la dirección de subred y la de broadcast en la subred.

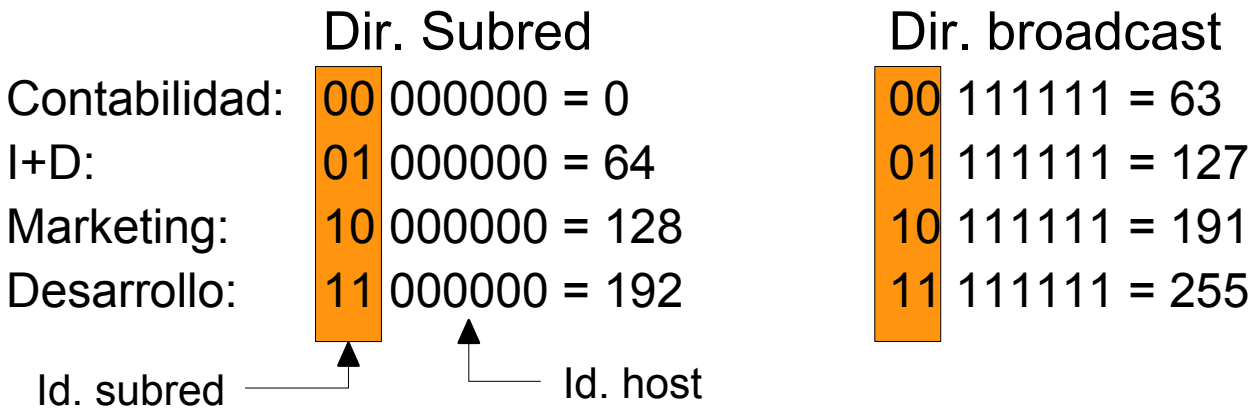
- **Dirección de subred**:
  - Dirección IP que identifica a una subred.
  - Se calcula para cada subred poniendo a 0 el identificador de host.
  - Coincide con la primera IP del rango.
  - Es equivalente a: dirección IP AND máscara de subred.

- **Dirección de broadcast en la subred**:
  - Se calcula poniendo todo a 1 el identificador de host.
  - Coincide con la última IP del rango.
  - Representa a todas las máquinas de la subred.

- Entonces, nº subredes = $2^{\text{bits subred}}$ y nº hosts = $2^{\text{bits host}} - 2$

Direcciones de subred

- Calcular las direcciones de subred y de broadcast del ejemplo:



Subred	Rango	Máscara	Dir. subred	Dir. broadcast
Contabilidad	210.53.23.0-63	255.255.255.192	210.53.23.0	210.53.23.63
I+D	210.53.23.64-127	255.255.255.192	210.53.23.64	210.53.23.127
Marketing	210.53.23.128-191	255.255.255.192	210.53.23.128	210.53.23.191
Desarrollo	210.53.23.192-255	255.255.255.192	210.53.23.192	210.53.23.255

Máscaras de subred de tamaño variable

- Fixed Length Subnet Masks (**FLSM**): todas las subredes usan la misma máscara → Desperdicio de direcciones IP.
- Si cada departamento tiene los siguientes hosts:
  - Contabilidad: 10 hosts → 52 IPs sin usar
  - I+D: 53 hosts → 9 IPs sin usar
  - Marketing: 24 hosts → 38 IPs sin usar
  - Desarrollo: 8 hosts → 54 IPs sin usar

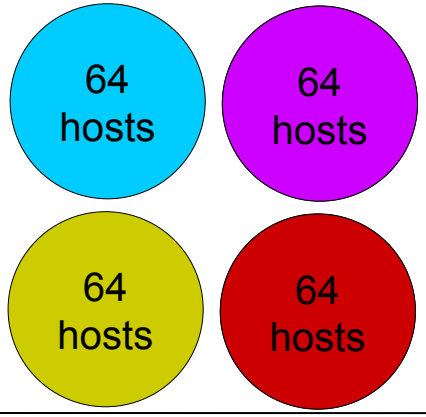
- Variable Length Subnet Masks (**VLSM**): cada subred usa la máscara de subred óptima para su número de hosts.
  - Ordenar las subredes de mayor a menor n.º de hosts
  - Calcular la máscara para cada subred usando FLSM

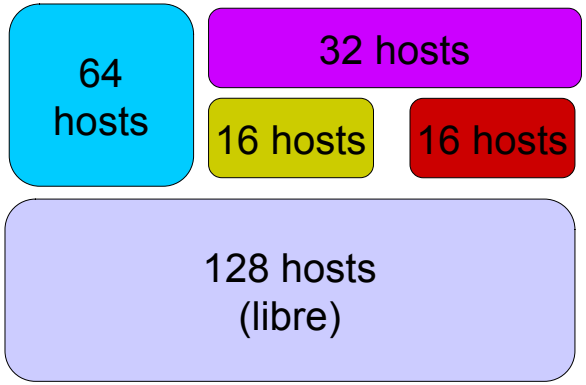
Máscaras de subred de tamaño variable

- I+D: 53 hosts → 6 bits id host → 2 bits id subred
- Marketing: 24 hosts → 5 bits id host → 3 bits id subred
- Contabilidad: 10 hosts → 4 bits id host → 4 bits id subred
- Desarrollo: 8 hosts → 4 bits id host → 4 bits id subred

Subred	Rango	Máscara	Dir. subred	Dir. broadcast
I+D	210.53.23.0-63	255.255.255.192	210.53.23.0	210.53.23.63
Marketing	210.53.23.64-95	255.255.255.224	210.53.23.64	210.53.23.95
Contabilidad	210.53.23.96-111	255.255.255.240	210.53.23.96	210.53.23.111
Desarrollo	210.53.23.112-127	255.255.255.240	210.53.23.112	210.53.23.127

FLSM





VLSM

Subredes: Ejercicio 1

- Queremos organizar la red de nuestra empresa, teniendo en cuenta la siguiente distribución por departamentos:
  - Dpto. contabilidad: 12 ordenadores
  - Dpto. I+D: 18 ordenadores
  - Dpto. desarrollo: 21 ordenadores
    - Sección de Análisis: 13 ordenadores
    - Sección de Implementación: 8 ordenadores
  - Dpto. marketing: 10 ordenadores
  - Dpto. administración: 10 ordenadores
- Disponemos de una dirección clase C: **195.35.12.0**

- Calcular la máscara de subred, id de red y rango de IPs de cada subred usando FLSM y VLSM.

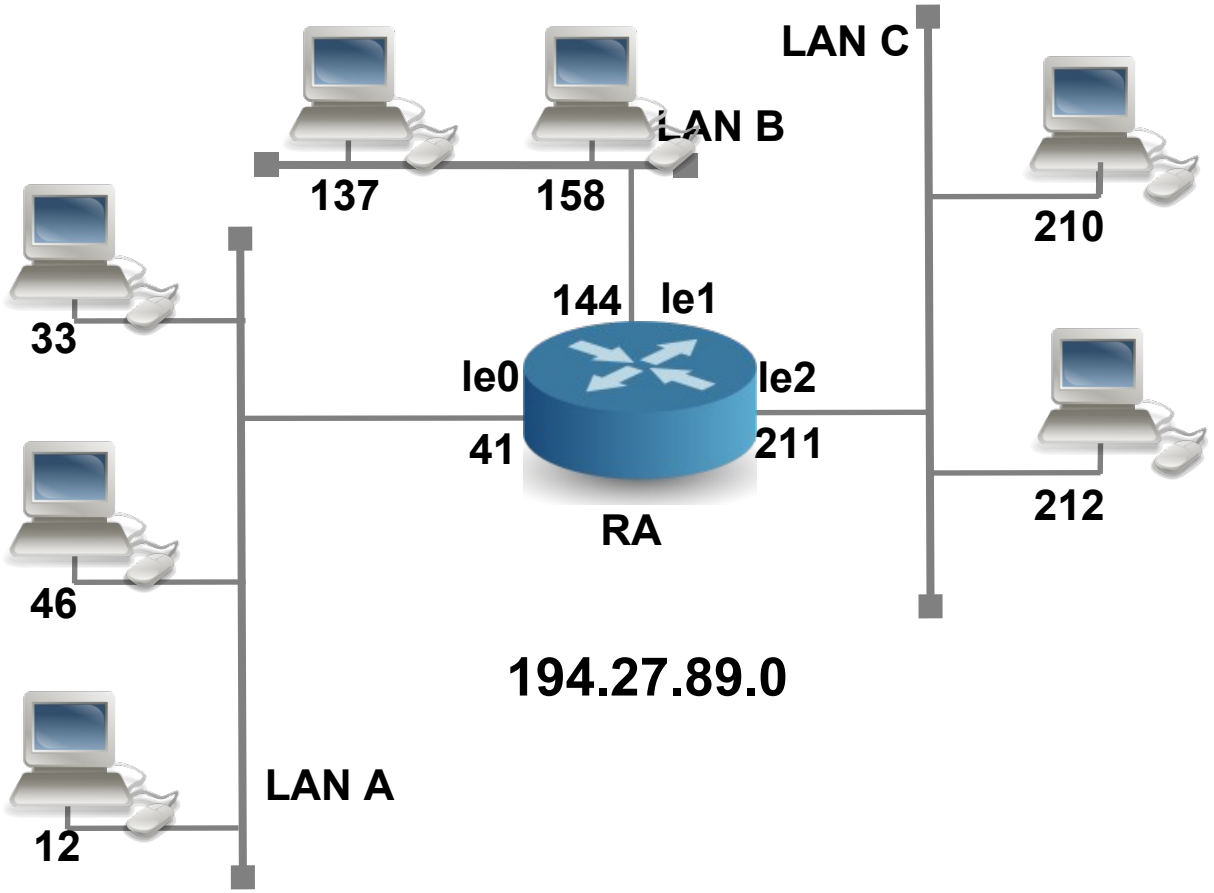
Subredes: Ejercicio 2

- Queremos organizar la red de nuestra empresa, teniendo en cuenta la siguiente distribución por departamentos:
  - Dpto. contabilidad: 52 ordenadores
  - Dpto. I+D: 12 ordenadores
  - Dpto. desarrollo: 71 ordenadores
  - Dpto. marketing: 10 ordenadores
  - Dpto. administración: 26 ordenadores
- Disponemos de una dirección clase C: **196.89.27.0**

- Calcular la máscara de subred, id de red y rango de IPs de cada subred usando FLSM y VLSM.

Subredes: Ejercicio 3

- Calcular las máscaras de subred, id subred y dirección de broadcast de subred, de A, B y C



Subredes: Ejercicio 3

- 33 = 0010 0001
- 46 = 0010 1110
- 12 = 0000 1100
- 41 = 0010 1001

Subred	Máscara (bin)	Máscara
A		
B		
C		

- 137 = 1000 1001
- 158 = 1001 1110
- 144 = 1001 0000

Subred	Id. subred (bin)	Id. subred
A		
B		
C		

- 210 = 1101 0010
- 211 = 1101 0011
- 212 = 1101 0100

Subred	Broadcast (bin)	Broadcast
A		
B		
C		

DHCP

- Una vez que la red está organizada → Asignar direcciones IP.
  - Normalmente, a los routers se les asigna manualmente.
  - ¿Y a los hosts …?
- Dynamic Host Configuration Protocol: permite asignar direcciones IP dinámica y automáticamente a los hosts (**plug-and-play**):
  - Las direcciones IP se asignan durante un tiempo limitado (desde horas a días), después es necesario renovarlas.
  - También incluye otros parámetros como máscaras de subred, router por defecto (antes se utilizaba ICMP o BOOTP) y servidores DNS.
- Se basa en el modelo cliente-servidor
  - Cliente DHCP: cualquier máquina "nueva" en la red que se esté iniciando y necesite una configuración de red
  - Servidor DHCP: garantiza que todas las direcciones IP son únicas (durante su tiempo de vida).
- Métodos de asignación de direcciones:
  - Estática o manual: se asigna una dirección IP a una máquina concreta (en base a su dirección MAC). Evita que se conecten clientes no identificados.
  - **Dinámica**: se utiliza un rango de direcciones IP y cada ordenador de la red está configurado para solicitar su dirección IP al iniciarse la interfaz.
    - Permite la reutilización dinámica de las direcciones IP.
    - Facilita la instalación de nuevas máquinas en la red.
  - Automática: similar al modo Dinámico, pero un equipo siempre obtiene la misma IP.

DHCP: Funcionamiento

- Modelo cliente-servidor basado en UDP: puerto 67 para el servidor y 68 para el cliente.
- Mensajes DHCP: el cliente incluye un identificador de transacción en el mensaje de descubrimiento, que deberá ser repetido en los siguientes.
  - **Discovery**: mensaje difundido en la red por el cliente para descubrir el/los servidores DHCP.
  - **Offer**: mensaje que contiene la dirección IP que el servidor ofrece al cliente DHCP.
    - Incluye la dirección MAC del cliente, la IP ofertada, la máscara, el tiempo de validez y la dirección del servidor.
  - **Request**: el cliente seleccionará una dirección de las ofertadas.
    - En caso de existir varios servidores, se indica el servidor del que se acepta la oferta.
  - **Acknowledgement**: el servidor confirma la solicitud del cliente y le indica cualquier otra información solicitada por el cliente.
- El cliente no tiene dirección IP → Todos los mensajes tienen como destino la dirección de **broadcast** 255.255.255.255

DHCP: Alternativa

- ¿Y qué pasa si no hay un servidor DHCP en mi red?
- Se definen las direcciones IP **link-local**: **169.254.0.0/16**

- APIPA (Automatic Private IP Addressing): permiten a un host auto-asignarse una IP para poder operar en una LAN cuando no hay ningún tipo de servidor disponible:
  - Se escoge una IP del rango aleatoriamente.
  - Se comprueba mediante ARP que nadie la tiene asignada.
  - En cuanto obtiene una IP “válida”, deja de usarse.

NAT: Direcciones privadas

- Cuando contratamos una banda ancha, mi ISP me proporciona **una dirección IP**, pero ¿y si quiero conectar más de un dispositivo a Internet?
  - Varios PCs, consolas, teléfonos, TV, ...

- Direcciones IP públicas: identifican unívocamente un dispositivo en Internet.
- **Direcciones IP privadas**: exclusivamente para uso interno.
  - Los dispositivos de la red privada se pueden comunicar entre si con esas direcciones.
  - Pero no se pueden comunicar con el exterior (Internet) → Solución: NAT.

- Rangos de direcciones IP privadas:
  - Clase A: **10.0.0.0** (1 red)
  - Clase B: **172.16.0.0 – 172.31.0.0** (16 redes)
  - Clase C: **192.168.0.0 – 192.168.255.0** (256 redes)

NAT

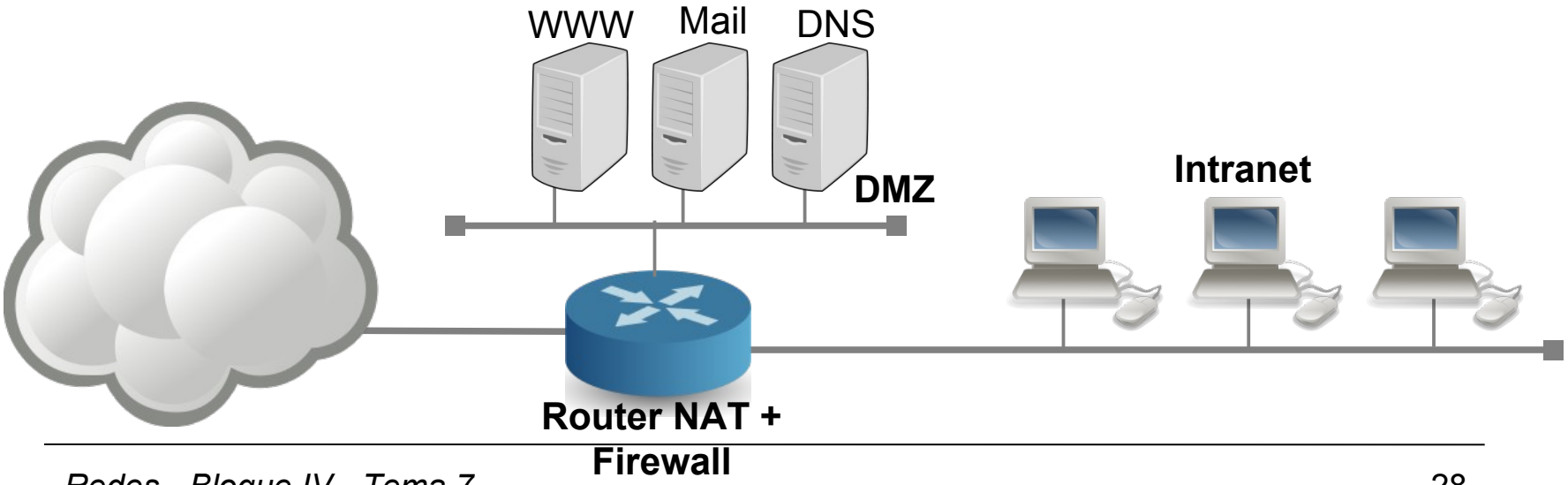
- **Network Address Translation**: consiste en modificar la dirección IP origen y/o destino de un datagrama IP al pasar a través de un router o firewall:
  - Permite a múltiples máquinas en una red privada acceder a Internet usando una única dirección IP pública.

- Surge debido a dos problemas: escasez de direcciones IP y escalabilidad del enrutamiento.
  - También ofrece seguridad: no se admiten conexiones desde fuera.

- Tipos de NAT:
  - **NAPT** (Network Address Port Translation): múltiples máquinas comparten una única dirección IP pública → La traducción se realiza mapeando números de puerto.
  - **Basic NAT** (o NAT estático o NAT 1 a 1): sólo se realiza el mapeo de direcciones IP → Cada dirección IP privada tiene asignada una dirección IP pública.

NAT

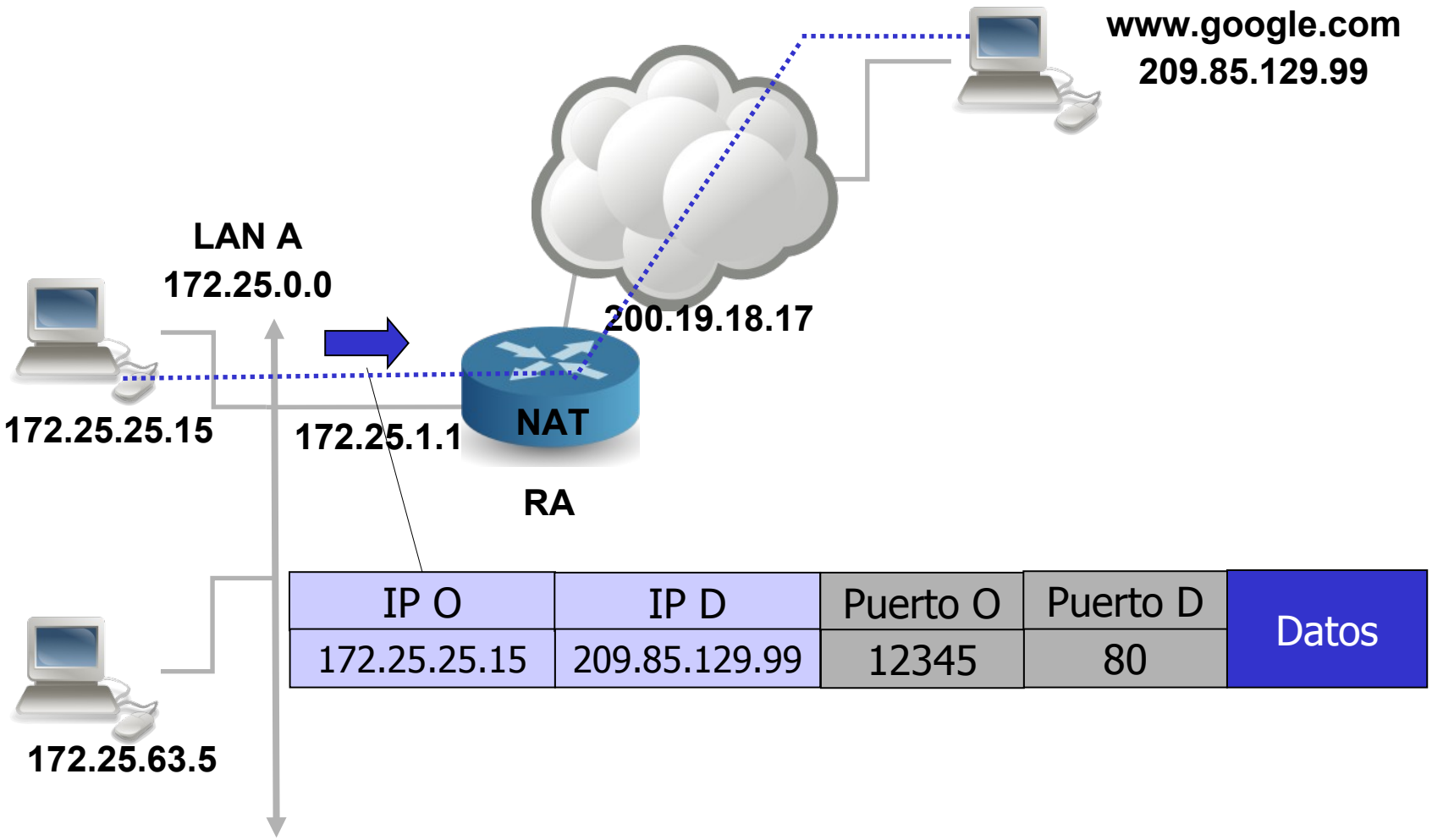
- Configuración típica:
  - La red interna (intranet) utiliza una dirección IP privada.
  - El router de la red tiene una interfaz con IP privada (conectada a la red interna) y otra interfaz con IP pública (conectada a Internet).
  - El router se encarga de realizar NAT e incluye un firewall.
  - Desde Internet parece que la comunicación se está realizando directamente con el router.
  - Los servidores públicos (Web, mail, DNS) se incluyen en una red independiente (DMZ o DeMilitarized Zone).



NAT

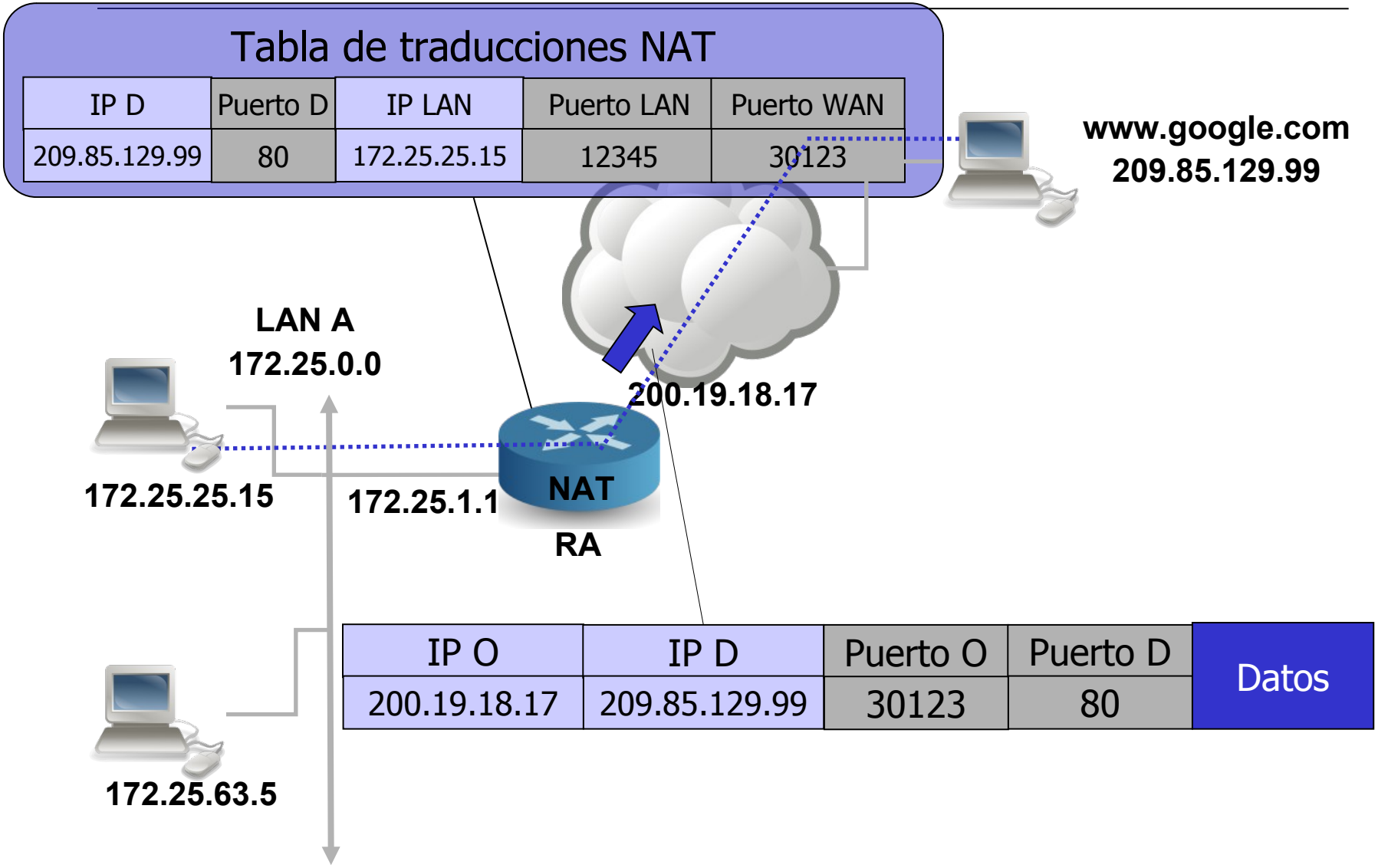
- **DMZ** (DeMilitarized Zone): parte de una red que se sitúa entre la red interna de una organización e Internet:
  - Se permiten las conexiones desde las redes externa e interna al DMZ.
  - Desde el DMZ sólo se permiten las conexiones a la red externa → Esto protege la red interna en caso de que una máquina de la DMZ sea comprometida.
  - En la DMZ se incluyen todos los servidores accesibles desde el exterior: servidor Web, correo electrónico, DNS, …
- **Firewall**: dispositivo configurado para permitir, denegar o actuar de intermediario en las comunicaciones de una red.
  - Puede ser hardware o software.
  - Permite controlar el tráfico entre redes de diferentes zonas de confianza.
  - Normalmente, separa una red interna (intranet: alto nivel de confianza) de una red externa (Internet: confianza nula), evitando accesos irregulares a la red interna.
  - Por ejemplo: *iptables*.

NAPT: Funcionamiento

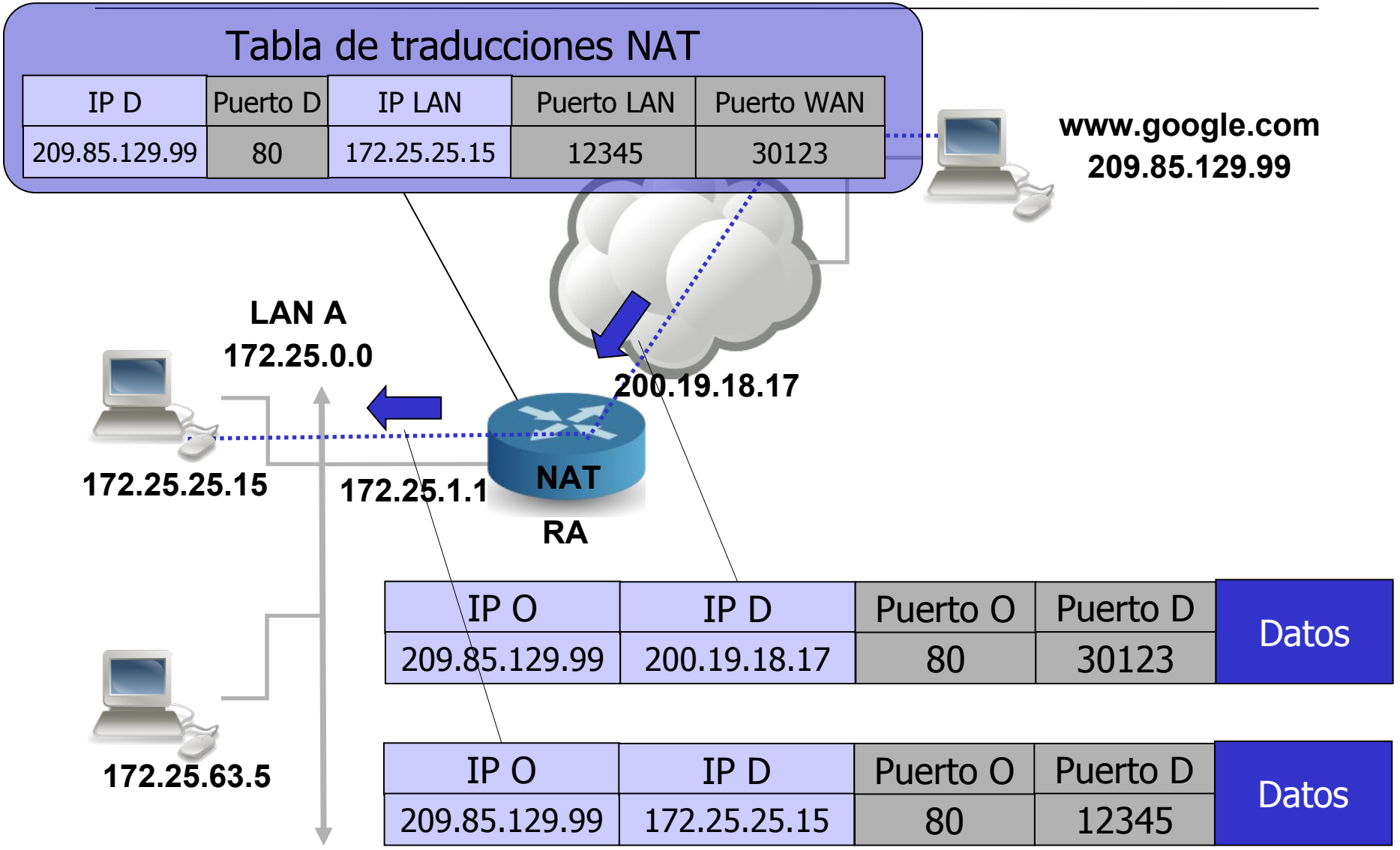


IP O	IP D	Puerto O	Puerto D	Datos
172.25.25.15	209.85.129.99	12345	80	

NAPT: Funcionamiento



NAPT: Funcionamiento



NAT

- Ventajas:
  - Seguridad: no se permiten conexiones bidireccionales. Una máquina interna debe iniciar la conexión con una máquina de Internet → Evita conexiones maliciosas desde el exterior.
  - Solución para la escasez de direcciones IPv4:
    - Utilizar direcciones IP públicas sólo para máquinas que requieran conexión bidireccional a Internet.
    - Direcciones privadas para las máquinas que sólo se conectan a Internet.
- Inconvenientes:
  - No existe una conectividad extremo a extremo real:
    - Se usan los números de puerto para direccionar hosts, no procesos.
    - Los routers sólo deberían implementar hasta el nivel de red.
  - Es un parche para la escasez de direcciones, cuando IPv6 soluciona el problema de raíz.
  - Plantea problemas en las aplicaciones que requieren que se inicien conexiones desde el exterior (p.e. FTP) → Desarrollo de técnicas específicas para estos casos (p.e. FTP pasivo), que se conocen genéricamente como **NAT traversal**. → **UPnP** (Universal Plug and Play): permite descubrir y configurar un NAT próximo.