SUBREDES
VLANS

IES Alonso de Ercilla
Puerta de Murcia, 13
45300 Ocaña
www.iesalonsodeercilla.com

UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro
Financiado como parte de la respuesta de la Unión a la pandemia de COVID-19

Las enseñanzas de Formación Profesional de Grado Superior: **Desarrollo de Aplicaciones Multiplataforma**, que durante el presente curo se está impartiendo en nuestro Centro, está siendo cofinanciado por el **Programa Operativo del Fondo Social Europeo de Castilla la Mancha, a través De los recursos adicionales REACT-UE**

SUBREDES

Una subred, abreviatura de "subnetwork" en inglés, es una división lógica de una red de dispositivos más grande. Una red se puede subdividir en múltiples subredes para mejorar la gestión, el rendimiento y la seguridad de la red. Cada subred tiene una dirección IP única y puede contener un conjunto específico de dispositivos y hosts conectados.

Las subredes se crean mediante el uso de una máscara de subred, que define qué parte de la dirección IP se utilizará para identificar la red y qué parte se utilizará para identificar los hosts individuales dentro de esa red.

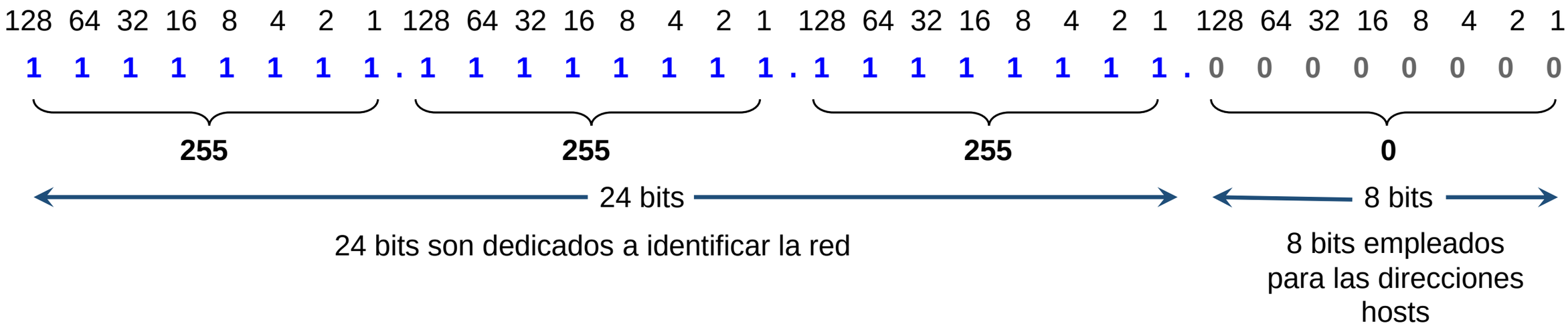
Esto permite una organización más eficiente de las direcciones IP y facilita el enrutamiento de paquetes dentro de la red.

Cada subred puede tener su propio rango de direcciones IP, lo que permite una mayor flexibilidad en la asignación de direcciones a dispositivos y hosts. Además, las subredes pueden ayudar a controlar el tráfico de red al segmentar la red en unidades más pequeñas, lo que reduce la congestión y mejora el rendimiento.

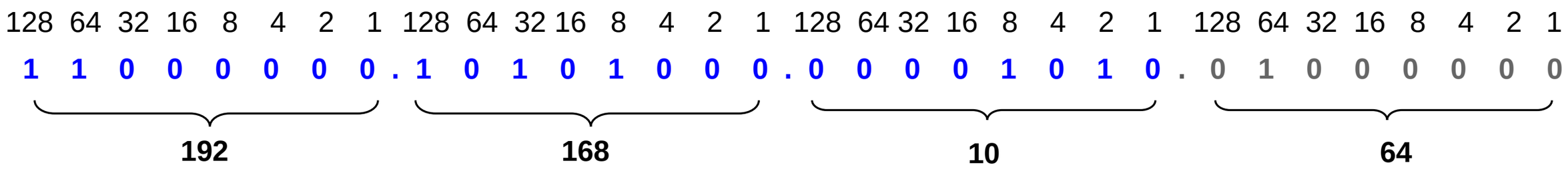
En resumen, una subred es una porción de una red más grande que se divide lógicamente para una mejor gestión, rendimiento y seguridad de la red.

Para saber si un equipo está dentro de una red y cuantos equipos posibles hay en ella, necesitamos conocer la máscara de red

Cuando decimos que una red tiene una máscara de red 255.255.255.0 o /24, quiere decir lo siguiente:



Por ejemplo, en la dirección de red 192.168.10.64/24, el 192.168.10 (azul) es la parte de red, y el .64 es el número de host

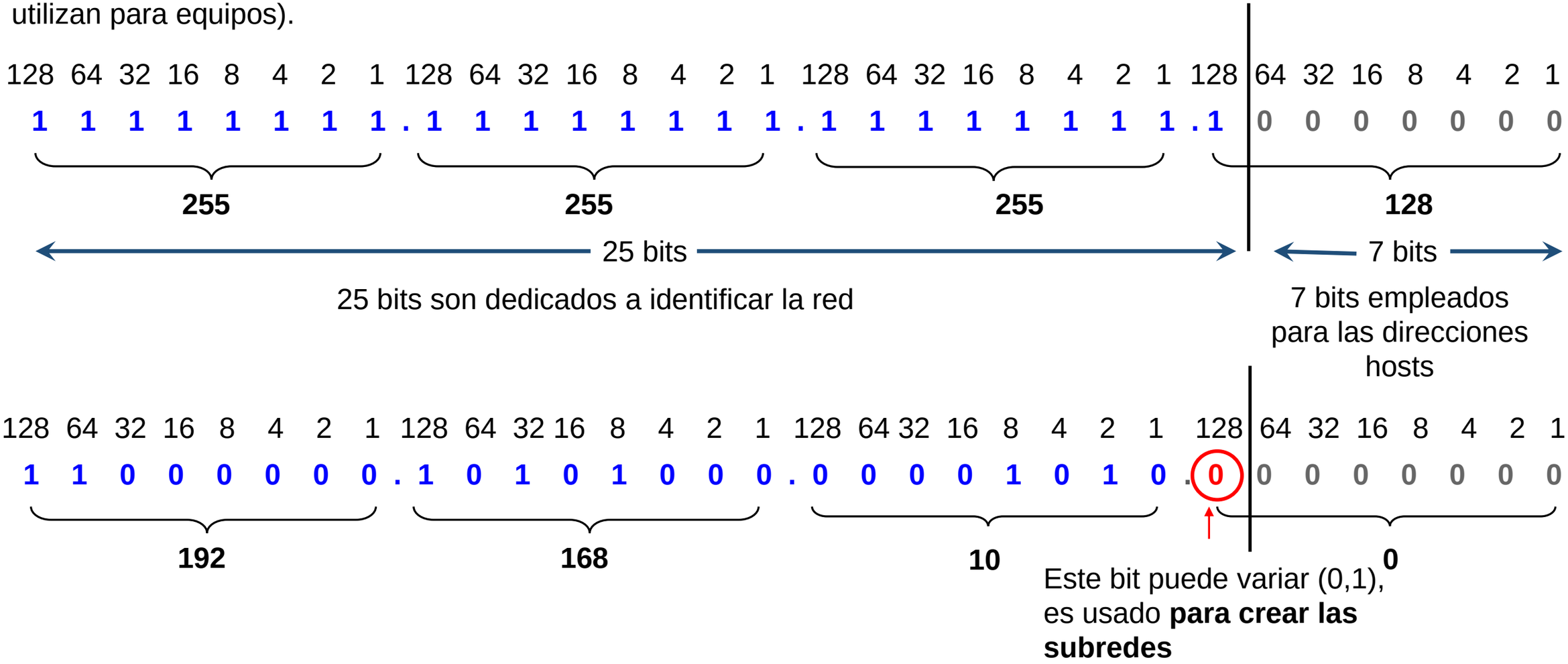


Con una máscara /24 podemos identificar hasta 256 dispositivos (0-255), pero la primera y última IP no pueden ser utilizadas ya que la primera es utilizada para identificar la red, y la última es la dirección de broadcast (multidifusión). Por lo tanto, podemos disponer de 254 IPs para equipos. En el ejemplo anterior:

Red: **192.168.10.0/24**
Broadcast: **192.168.10.255/24**

EJEMPLO 2 SUBREDES:
Pongamos el caso que disponemos de la siguiente dirección de red 192.168.10.0, y quiero dividir esta red en 2 subredes distintas, de al menos126 equipos en cada una.

Si quiero tener 126 equipos en cada una, necesitaré al menos 7 bits para hosts 2^7=128 (primera y última IP no se utilizan para equipos).



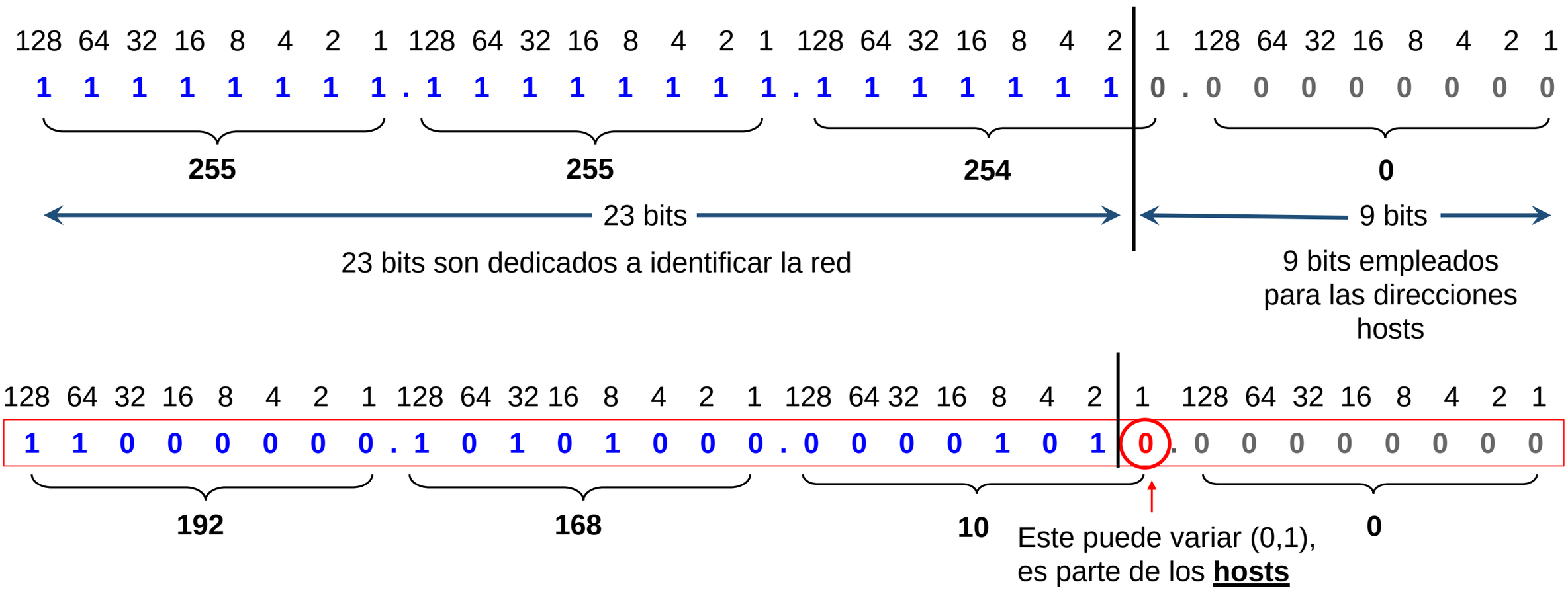
Por un lado, tenemos la red en la cual el número marcado en rojo se mantiene a 0, por lo que la primera subred viene identificada por:
192.168.10.0/25 – 192.168.10.127 (128 en total)
La segunda subred (el número marcado en rojo se pone a 1):
192.168.10.128/25 – 192-168.10.255 (128 en total)

Poner en funcionamiento estas dos subredes implica disponer de 2 interfaces de red en el router.

Nota: existe la posibilidad de usar una única interfaz haciendo uso de técnicas como generar **VLANs**, que analizaremos en los siguientes apartados.

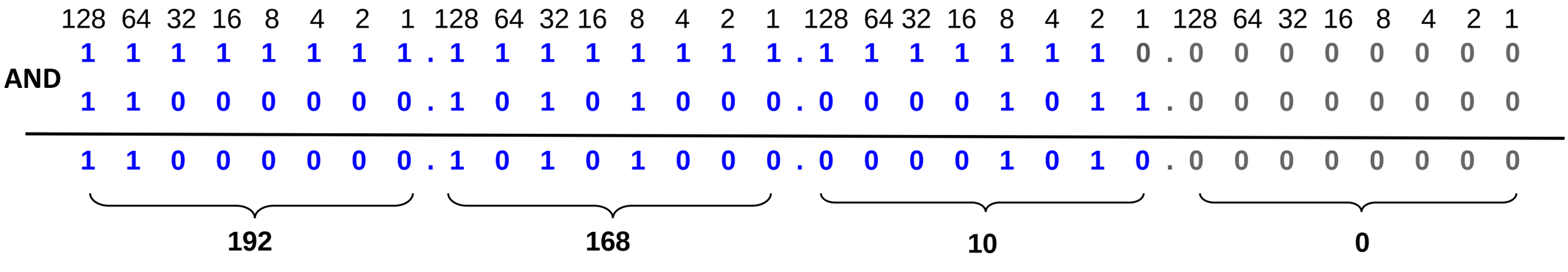
Siguiendo con el ejemplo anterior, supongamos que aplicamos una máscara de red /23 a la red 192.168.10.0

Quitamos un bit a los dedicados a identificar la red (23), y se lo añadimos a los dedicados al hosts (9).



Por tanto, la red 192.168.10.0/23 dispone de un total de 512 Ips (510) para hosts.
Rango de IPs: **192.168.10.1 – 192.168.11.254** (quitamos la de red y la de broadcast)
Nota que ahora el tercer dígito cambia, por lo que por ejemplo la IP 1**92.168.11.200** estaría de entro de la red **192.168.10.0/23**

SI REALIZAMOS LA OPERACIÓN AND ENTRE MÁSCARA DE RED E IP DEL HOST, NOS DARÁ LA IP DE RED



EJEMPLO:

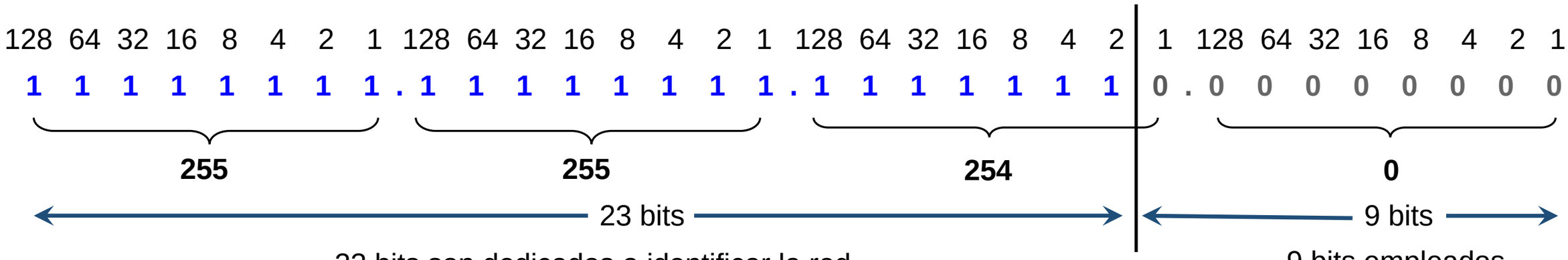
Se necesita diseñar 2 redes que al menos puedan disponer de 500 equipos en cada red. ¿Cuál sería la configuración más óptima ? Indica para cada una de las redes: IP de red, máscara de red, puerta de enlace, dirección broadcast, rango de IPs para resto de equipos. ¿Es posible separar estas redes para que los equipos no ambas redes no puedan verse? Elegir IPs de clase C.

Lo primero, 2 redes ya implican disponer de al menos 2 interfaces de red. En el caso de un router doméstico o de oficina (SoHo), es común que en su parte trasera tenga un pequeño switch incorporado con 4 puertos Ethernet. Estos puertos permiten la conexión de dispositivos en una red local (LAN), lo que facilita la configuración de **una única LAN** con varios dispositivos conectados a través del switch integrado.

Sin embargo, es importante tener en cuenta que existen routers con más de 4 puertos o que permiten la configuración de múltiples LAN o VLAN utilizando diferentes interfaces físicas o virtuales. Por lo tanto, la capacidad de configurar solo 1 LAN en un router doméstico o de oficina puede depender de sus características específicas y configuración predeterminada.

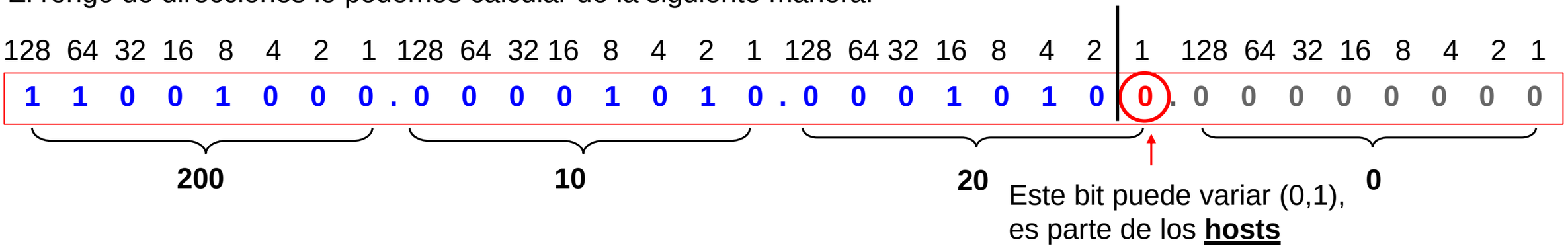
En resumen, para tener múltiples redes, se necesitan al menos dos interfaces de red en un router, y es común que los routers SoHo tengan un pequeño switch integrado en su parte trasera para permitir la conexión de dispositivos en una única LAN. Sin embargo, la capacidad de configurar múltiples LAN puede variar según el modelo y las características del router.

RED 1:
Si necesito 500 equipos, es necesario al menos 9 bits dedicados a hosts (2^9 = 512), por lo que la máscara de red dispondría de 23 bits, quedando finalmente la máscara de red: 255.255.254.0



Las IPs de red deben ser de clase C, deberemos elegir en el rango 192.0.0.0 – 223.255.255.255

Elegimos la red 200.10.20.0/23.
Como puerta de enlace elegimos la primera IP disponible de la red: 200.10.20.1
El rengo de direcciones lo podemos calcular de la siguiente manera:



Por tanto, la red 200.10.20.0/23 dispone de un total de 512 IPs (510 para hosts).
Rango de IPs: **200.10.20.1 – 200.10.21.254** (quitamos la de red 200.10.20.0 y la de broadcast 200.10.20.255)

RED 2:
El procedimiento es el mismo que el anterior. Dado que tenemos libertad de elegir una IP que identifique a la red siempre y cuando esté dentro del rango de direcciones de clase C, elegiremos la IP 200.10.30.0/23.
Esto implica que el rango de direcciones disponibles es desde 200.10.30.1-200.10.31.254

RESUMEN:
RED 1
Dirección de red: 200.10.20.0/23
Máscara de red: 255.255.254.0
Broadcast: 200.10.21.255
Gateway: 200.10.20.1 (por regla general elegimos la primera IP disponible, pero no tiene que ser así siempre)
Rango de IP’s destinadas a hosts: 200.10.20.2 - 200.10.21.254

RED 2
Dirección de red: 200.10.30.0/23
Máscara de red: 255.255.254.0
Broadcast: 200.10.31.255
Gateway: 200.10.30.1 (por regla general elegimos la primera IP disponible, pero no tiene que ser así siempre)
Rango de IP’s destinadas a hosts: 200.10.30.2 - 200.10.31.254

CONFIGURACIÓN EN LOS EQUIPOS
ROUTER:
Como ya se ha indicado, en el router necesitamos disponer de 2 interfaces de red para asignar las 2 LANs, en las cuales deberemos indicar al menos la puerta de enlace y la máscara de red. También tendremos que verificar las reglas de Firewall para permitir el trafico de red, y ajustar el servidor DHCP en el rango adecuado (normalmente se deja un margen para IPs estáticas, pero dependerá de los requisitos de red.)

REGLAS:
A parte de la indicada en el paso anterior, es necesario establecer una regla de privacidad entre ambas redes, denegando el tráfico entre la red 200.10.20.0/23 y la red 200.10.30.0/23

EQUIPOS RED 1 y 2:
Al menos que se indique lo contrario, los equipos deberán establecer una configuración de red automática, es decir, por DHCP.

VLANs (Redes de Área Local Virtual)

Una **VLAN (Virtual LAN)** es una tecnología que permite dividir una red física en múltiples redes lógicas. Aunque todos los dispositivos estén conectados a la misma infraestructura física (como un switch), con VLANs pueden comportarse como si estuvieran en redes separadas. Esto mejora la **seguridad**, el **rendimiento** y la **organización del tráfico**, sin necesidad de tener múltiples switches físicos.

Cada VLAN se identifica mediante un **ID** o **etiqueta (tag)**, generalmente bajo el estándar **IEEE 802.1Q**. Los switches que soportan VLANs permiten enviar tráfico **etiquetado**, de modo que una misma interfaz física pueda transportar múltiples VLANs. A esto se le conoce como **enlace trunk**.

¿Por qué usar VLANs?

- **Seguridad**: Aísla grupos de dispositivos. Por ejemplo, separa usuarios de oficina de servidores.
- **Organización**: Facilita la gestión de red por departamentos, ubicaciones o funciones.
- **Reducción de tráfico**: El tráfico broadcast se limita a cada VLAN, mejorando el rendimiento.
- **Flexibilidad**: Permite crear redes lógicas sin importar la ubicación física de los dispositivos.
- **Aislamiento**: Un fallo o un ataque en una VLAN no afecta a las demás.
- **Mejor gestión**: Facilita la asignación de políticas específicas a cada segmento.

Trunking

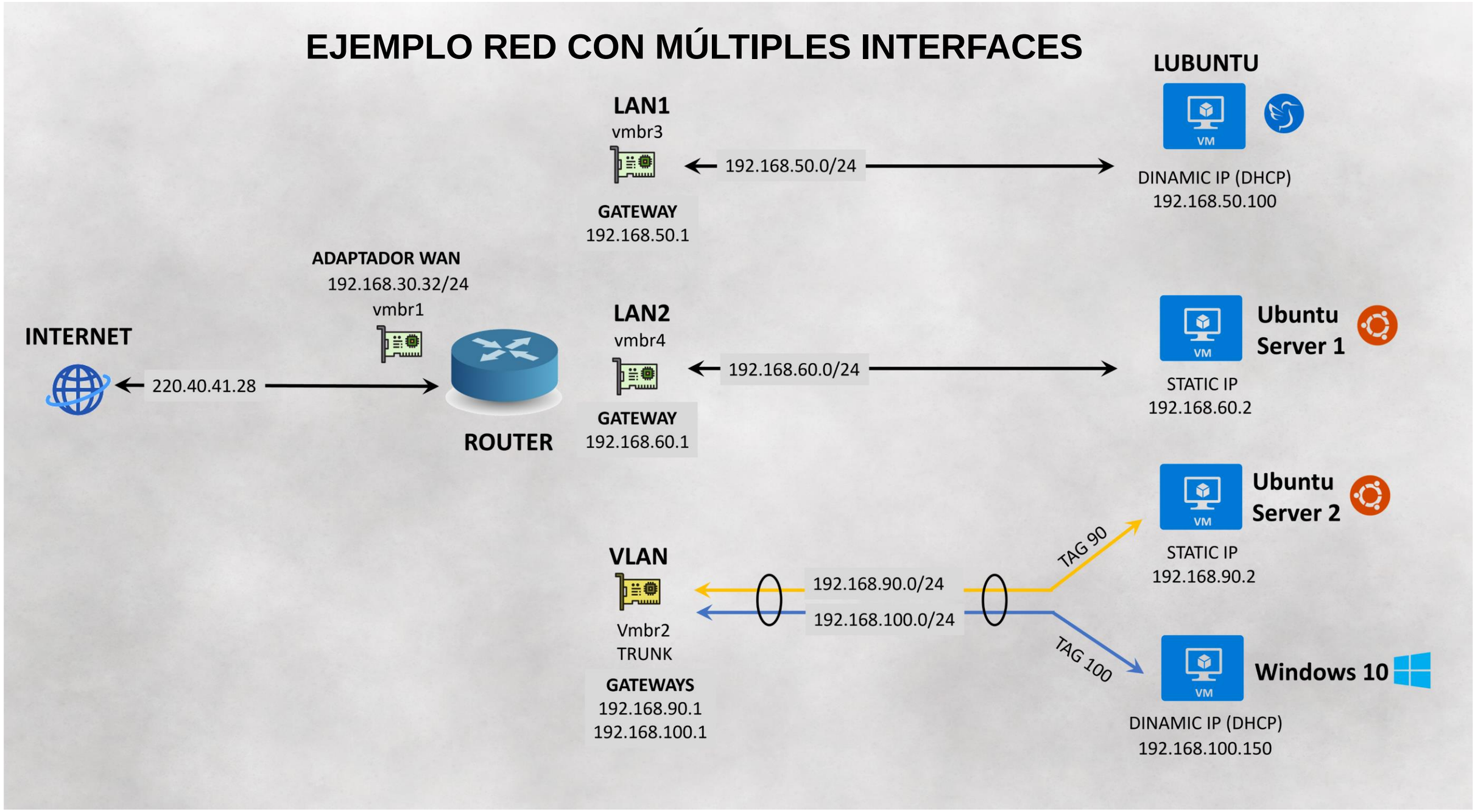
El trunking es una técnica utilizada en redes de área local (LAN), para permitir la transmisión de tráfico de múltiples VLANs a través de un único enlace físico o puerto. El trunking se implementa comúnmente en **switches de capa2 gestionables, los de capa 3 y routers** para facilitar la comunicación entre dispositivos de red y transportar tráfico de VLANs diferentes.

Cuando se configura un enlace como trunk, se agregan etiquetas VLAN a los paquetes de datos que se transmiten a través de ese enlace. Estas etiquetas VLAN identifican a qué VLAN pertenece cada paquete de datos, y permiten que los dispositivos en ambos extremos del enlace comprendan y enruten adecuadamente el tráfico de VLANs específicas.

Esto proporciona una mayor flexibilidad en el diseño de redes y simplifica la administración al reducir la cantidad de cables y puertos requeridos.

Comparativa: Dispositivos y Soporte para VLANs

Dispositivo	¿Permite crear VLANs?	¿Soporta tráfico de múltiples VLANs (Trunk)?	¿Puede enrutar entre VLANs?	Consideraciones clave
Switch no gestionable	❌ No	❌ No	❌ No	Solo funciona en una red plana, ignora etiquetas VLAN.
Switch de capa 2 (gestionable)	✅ Sí	✅ Sí (con trunk 802.1Q)	❌ No	Permite segmentar la red, pero necesita router para comunicación entre VLANs.
Switch de capa 3	✅ Sí	✅ Sí	✅ Sí	Puede enrutar entre VLANs sin necesidad de router externo. Ideal para entornos grandes.
Router doméstico (SOHO)	❌ No (en general)	❌ No	❌ No (limitado)	Normalmente no gestiona VLANs, salvo modelos avanzados o con firmware especial (OpenWRT, etc.).
Router profesional	✅ Sí (limitado)	✅ (si tiene interfaz trunk)	✅ Sí	Algunos modelos gestionan VLANs en interfaces y enrutan entre ellas. Muy usado en entornos corporativos.



En el entorno representado:

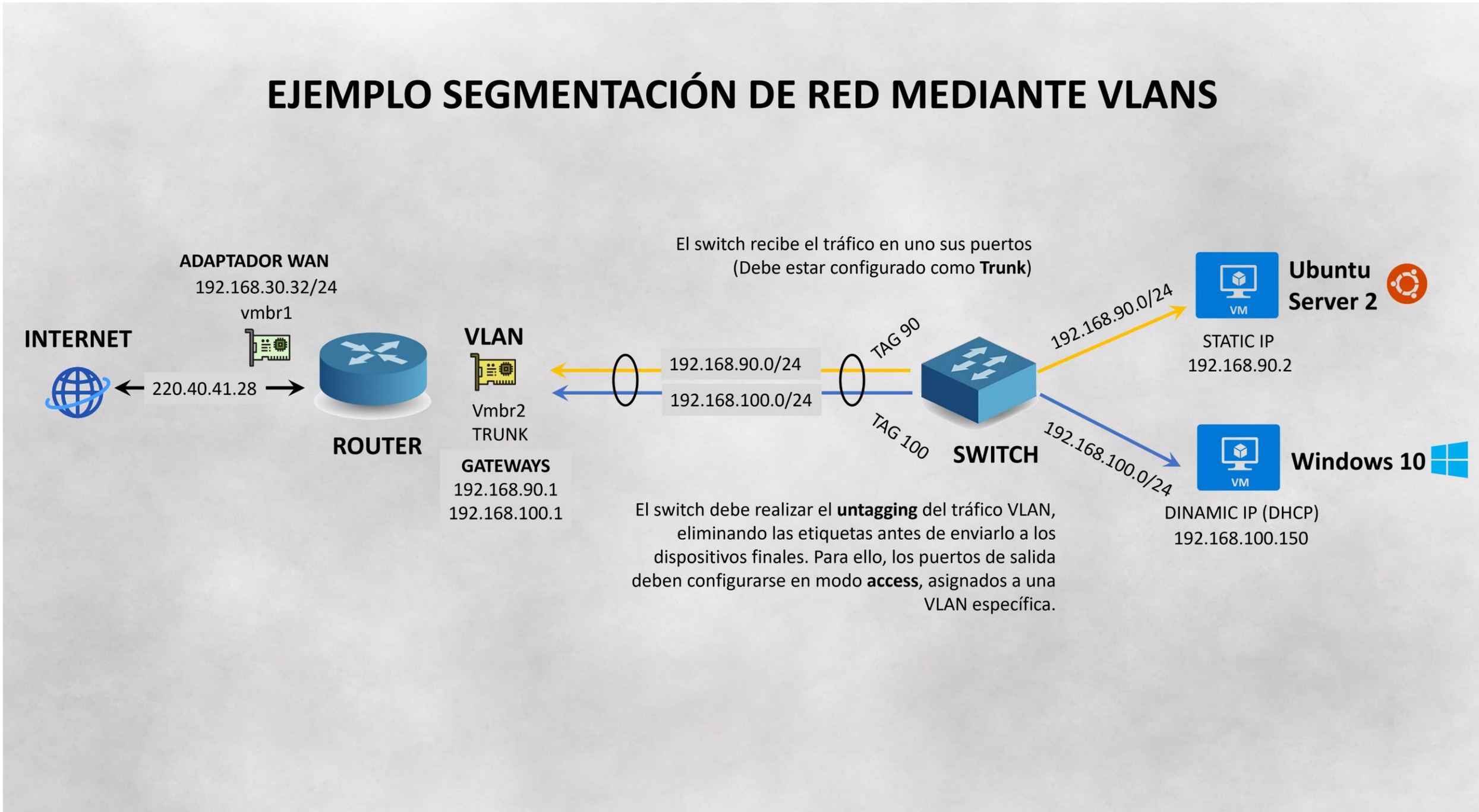
•Se utiliza vmbr2 como **interfaz trunk**.

•Se han definido dos VLANs:

- •**VLAN 90**: Red 192.168.90.0/24 → asignada a Ubuntu Server 2.
- •**VLAN 100**: Red 192.168.100.0/24 → asignada a Windows 10.

Ambas redes se mantienen aisladas gracias a las etiquetas VLAN, a pesar de compartir la misma interfaz física.

Es necesario que ambos equipos (Ubuntu y Windows 10) configuren correctamente sus adaptadores de red para conectar con la red adecuada. Este escenario es muy común en **entornos virtualizados.**



A diferencia con el ejemplo anterior, donde debíamos configurar el adaptador de red de las máquinas para conectarse a la VLAN adecuada, en este esquema podemos ver cómo el switch actúa como **segmentador** de red, recibiendo tráfico etiquetado (**trunk**) y reenviándolo a puertos de acceso (**access**), donde elimina las etiquetas VLAN y entrega el tráfico correspondiente a cada red.

Esta es la configuración más utilizada en entornos físicos, debido a evitar tener que realizar configuraciones complejas en los hosts.