TEMA 0. Revisión Protocolo IPv4

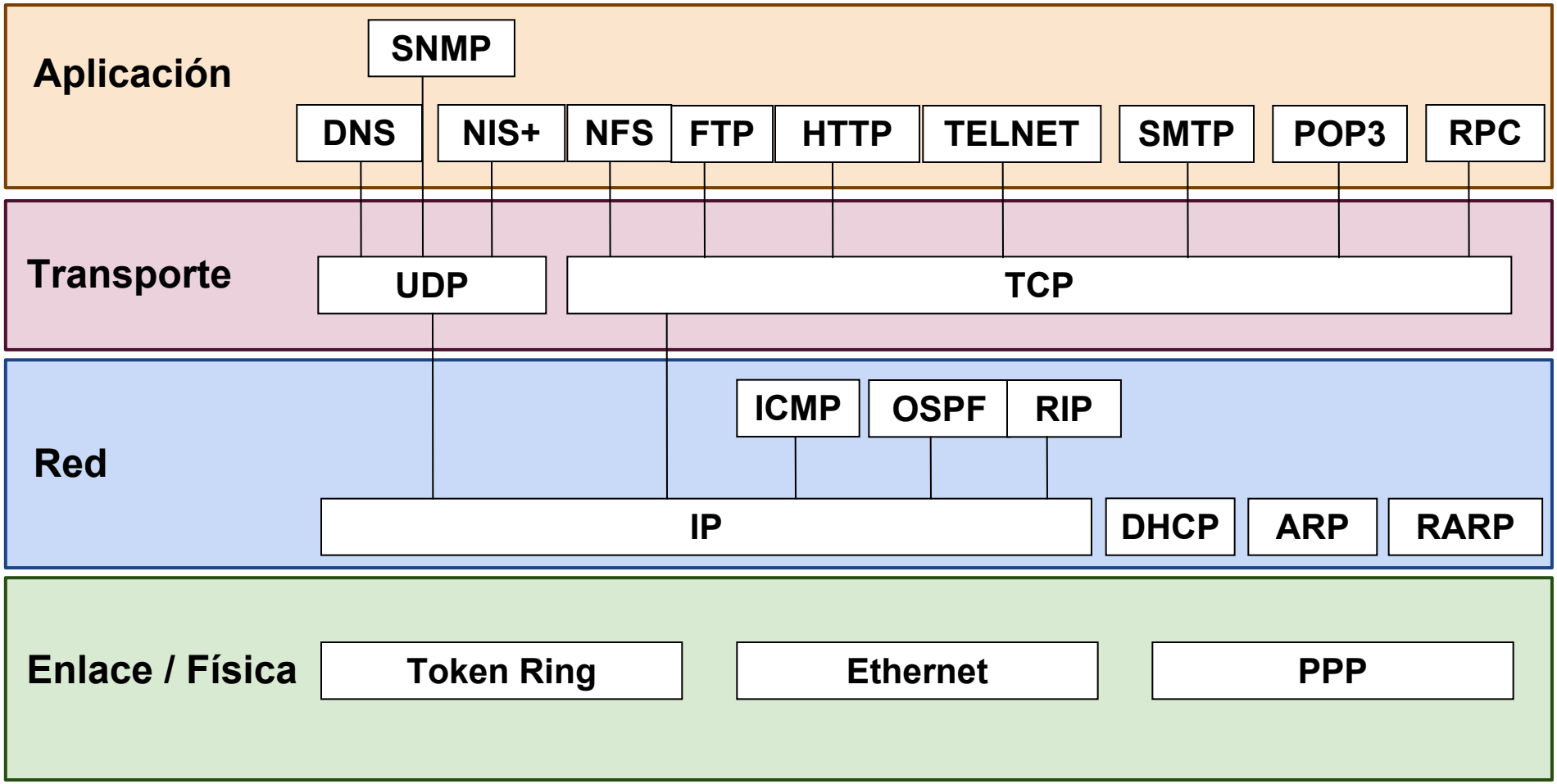
PROFESORES:

Rafael Moreno Vozmediano

Rubén Santiago Montero

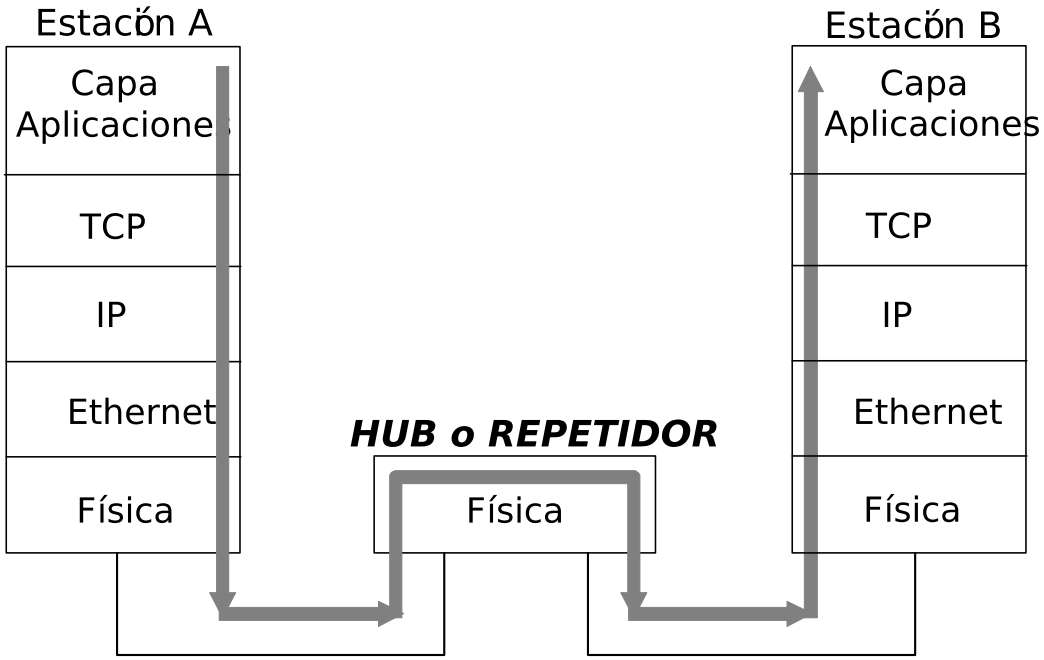
Juan Carlos Fabero Jiménez

Arquitecturas TCPI/IP



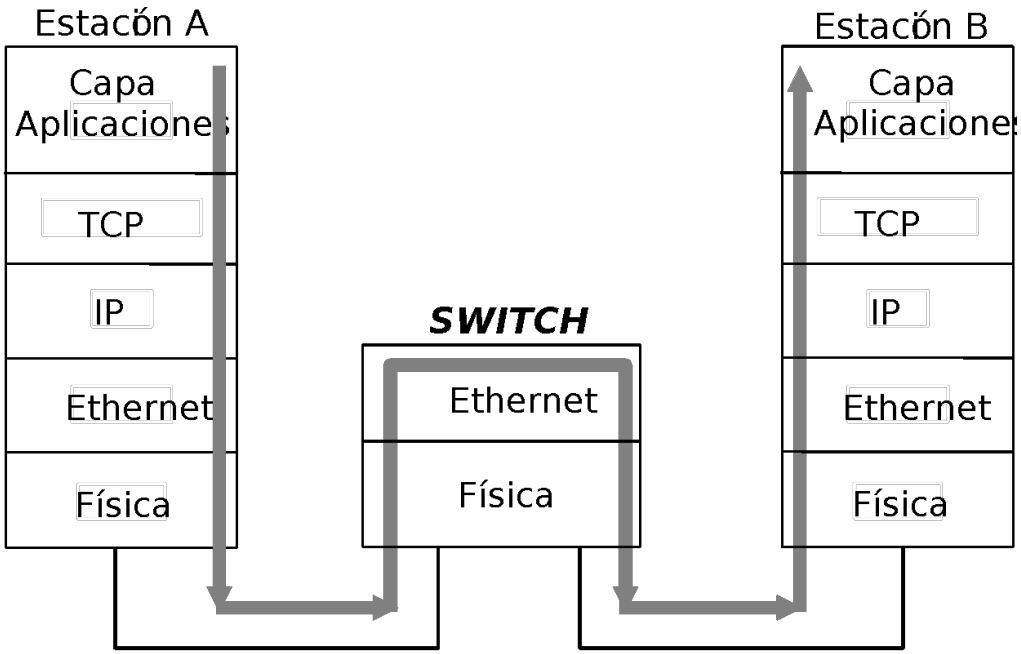
Arquitectura en Capas: Hub

- Son dispositivos que trabajan a nivel de la capa física
- Retransmiten bit a bit la información que les llega por una entrada al resto de salidas
- Pueden interconectar estaciones o segmentos de red del mismo tipo (por ejemplo, Ethernet) y velocidad



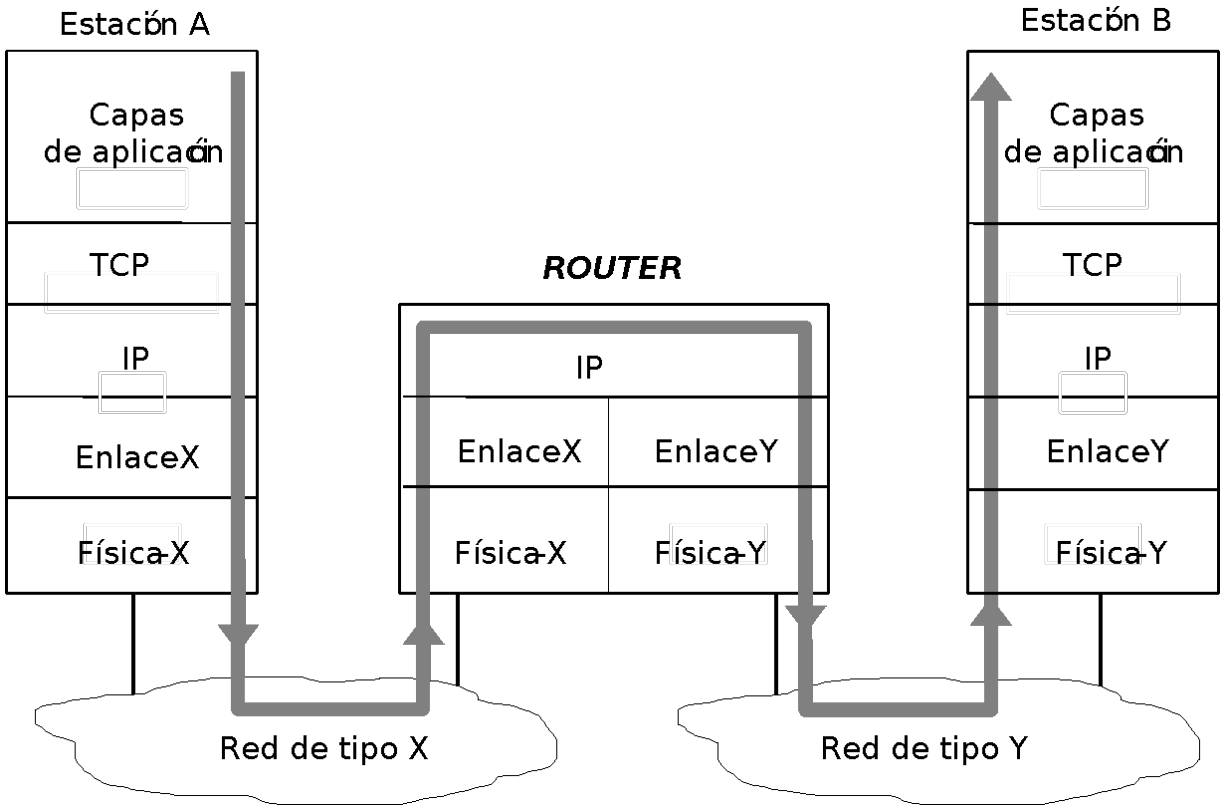
Arquitectura en Capas: Switch

- Son dispositivos que trabajan a nivel de la capa MAC
- Reenvía la trama por la salida adecuada en función de la dir. MAC destino
- Pueden almacenar la trama completa y realizar detección de errores
- Pueden interconectar estaciones y redes del mismo tipo, aunque pueden trabajar con implementaciones de distinta velocidad (ej. 100Base-TX y 1000Base-T)



Arquitectura en Capas: Router

- Son dispositivos que trabajan a nivel de la capa de red (IP)
- Pueden interconectar redes de distinto tipo
- Realizan dos funciones básicas:
  - Conversión de formatos
  - Encaminamiento



El protocolo IP

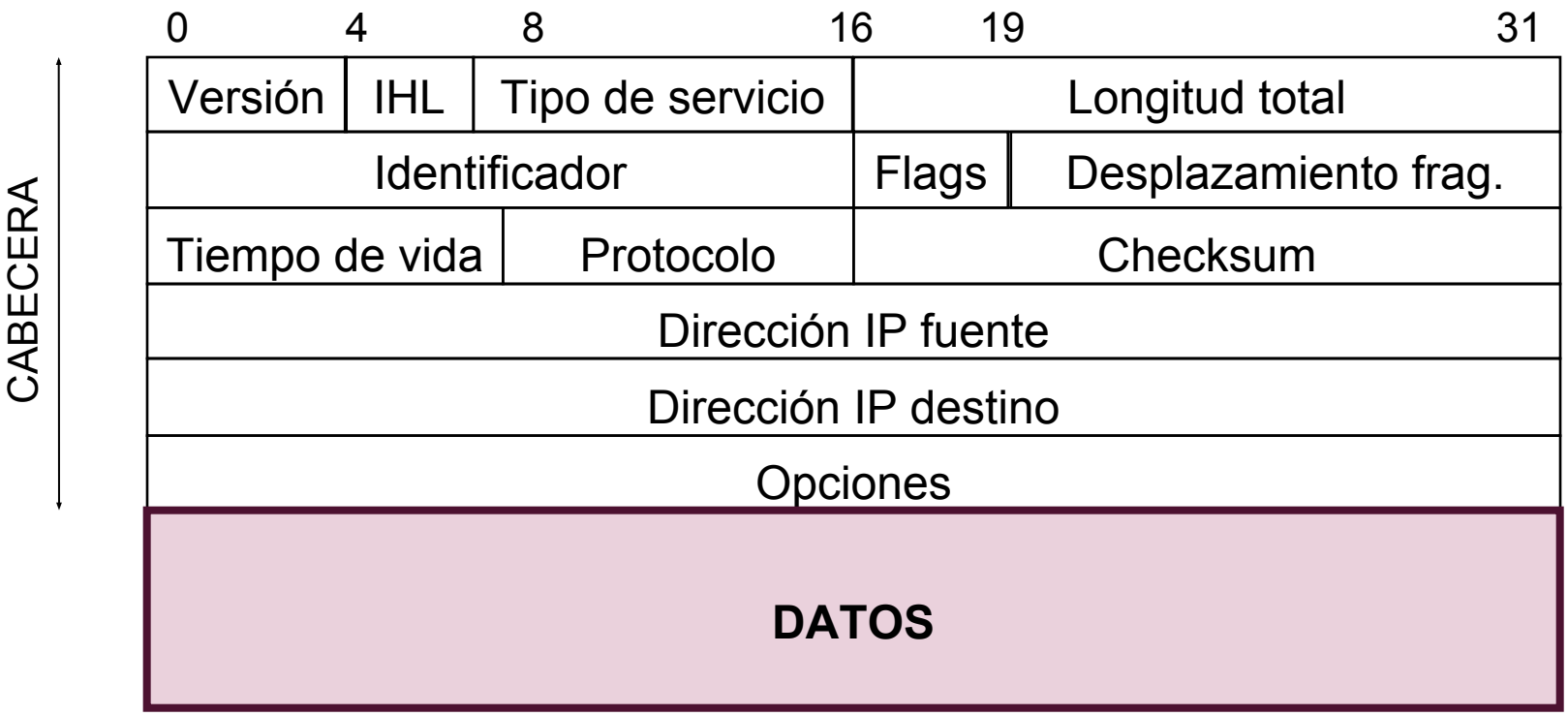
Protocolo de red de Internet

- Proporciona un servicio básico de entrega de paquetes
  - Sobre el que se construyen las redes TCP/IP.
- Protocolo **no orientado a conexión** (no fiable)
  - No realiza detección ni recuperación de paquetes perdidos o erróneos
  - No garantiza que los paquetes lleguen en orden
  - No garantiza la detección de paquetes duplicados

Funciones básicas del protocolo IP

- **Direccionamiento**
  - Esquema global de direccionamiento
- **Fragmentación y reensamblaje** de paquetes
  - División del paquetes en fragmentos de un tamaño aceptable por la red
- **Encaminamiento** de datagramas
  - Encaminado de paquetes atendiendo a información de tabla de rutas
  - La construcción de tablas de rutas puede ser
    - Manual (routing estático)
    - Mediante algún protocolo de routing dinámico: RIP, OSPF, BGP, etc.

El protocolo IP: Formato de Datagramas



El protocolo IP: Direcciones y Máscaras de red

Direcciones IPv4

- Las direcciones IP constan de 4 bytes (32 bits)
- Para expresarlas se utiliza la “notación de punto”
  - Ejemplo: 128.2.7.9 = 10000000 . 00000010 . 00000111 . 00001001

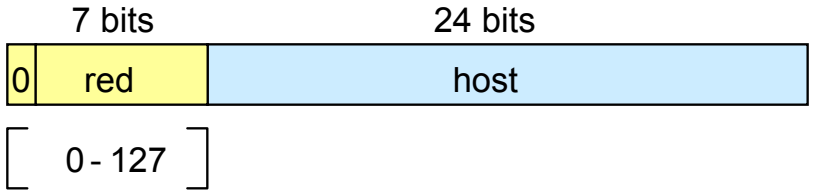
Tipos de direcciones IPv4

- Unicast
  - Un único host
- Multicast
  - Un grupo de hosts
- Broadcast
  - Todos los hosts dentro de mi red local

El protocolo IP: Direcciones y Máscaras de red

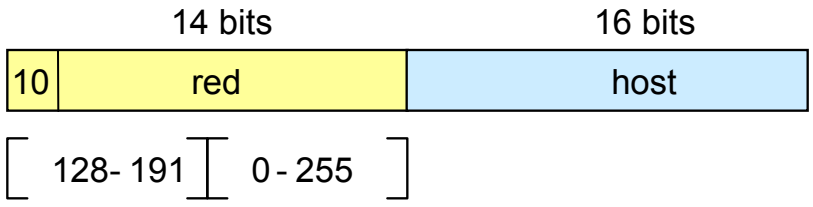
Direcciones IPv4 basadas en clase (classful)

Clase A



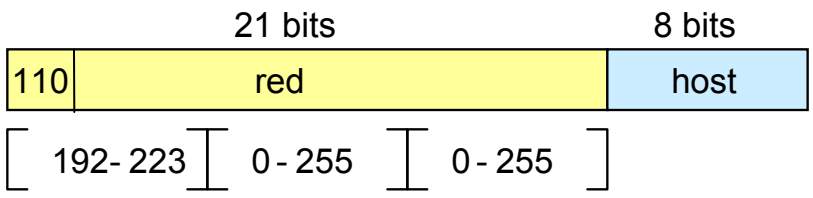
2^7 = 128 redes
2^{24} = 16.777.216 hosts
Ejemplo: ***26***.56.120.9

Clase B



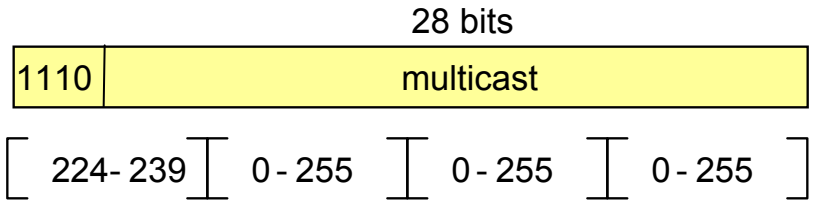
2^{14} = 16.384 redes
2^{16} = 65.536 hosts
Ejemplo: ***147.96***.50.110

Clase C



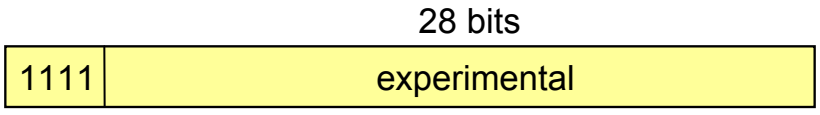
2^{21} = 2.097.152 redes
2^8 = 256 hosts
Ejemplo: ***217.6.95***.44

Clase D



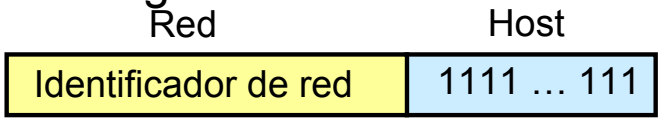
Ejemplo: ***224.0.0.1***

Clase E



El protocolo IP: Direcciones Especiales

- **Direcciones reservadas para redes privadas**
  - Existen un conjunto de direcciones reservadas para uso privado.
  - No son válidas para su uso en Internet
    - Se pueden asignar a redes aisladas de Internet
    - Se pueden asignar redes conectadas a través de un router que hace traducción de direcciones de red (NAT)
  - Los rangos de direcciones IP privadas son los siguientes:
    - 10.0.0.0 – 10.255.255.255 ~ 1 red privada de clase A
    - 172.16.0.0 – 172.31.255.255 ~ 16 redes privadas de clase B
    - 192.168.0.0 – 192.168.255.255 ~ 256 redes privadas de clase C
- **Direcciones de loopback (127.x.y.z)**
  - Direcciones de bucle interno (loopback)
  - Casi todas las máquinas tienen como dirección de loopback la **127.0.0.1**
- **Direcciones broadcast (terminadas en 11...111)**
  - Se utilizan para enviar un paquete a todas las máquinas de la red local
  - Formato de las direcciones broadcast
    - Todos los bits de identificador de host se ponen a valor 1
    - Último valor del rango de direcciones de la red



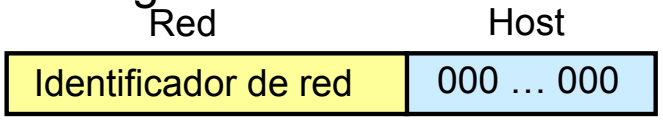
El protocolo IP: Direcciones Especiales

Direcciones de red (terminadas en 00...000)

- Se utilizan para representar a una red completa en las tablas de encaminamiento
- Nunca se utilizan como dirección destino ni se asignan a un host concreto
- Ejemplo de tabla de rutas en Linux (orden **netstat –nr**)

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Iface
192.168.1.0     0.0.0.0         255.255.255.0   U         eth0
192.168.2.0     0.0.0.0         255.255.255.0   U         eth1
0.0.0.0         192.168.1.1     255.255.255.0   UG        eth0
```

- Formato de las direcciones de red
  - Todos los bits de identificador de host se ponen a valor 0
  - Primer valor del rango de direcciones de la red



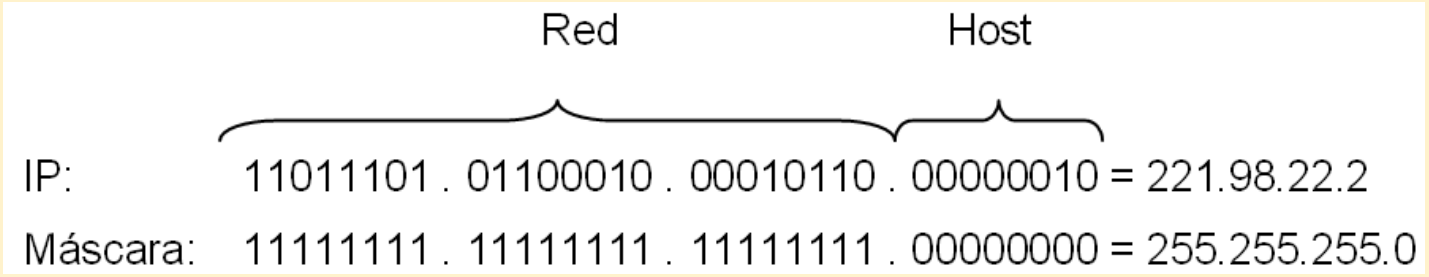
El protocolo IP: Máscaras de Red

La máscara de red indica:

- Qué parte de la dirección IP identifican a la red
  - Bits de la máscara a 1
- Qué parte de la dirección IP identifican al host dentro de la red
  - Bits de la máscara a 0

Ejemplo

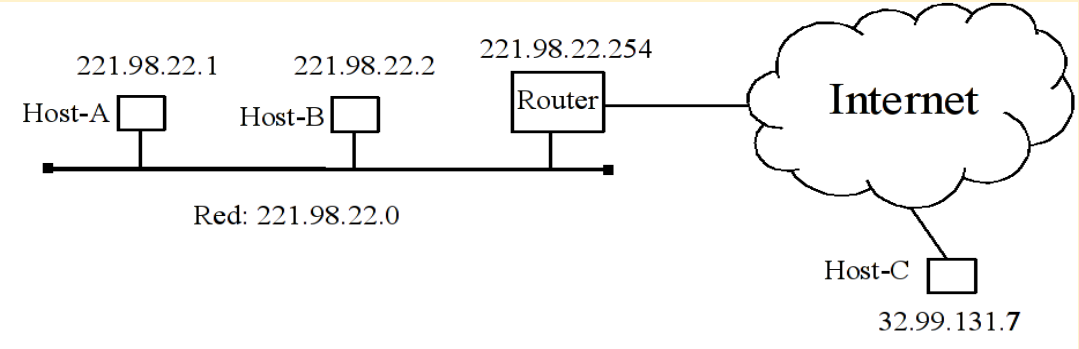
- Dirección de clase C: 221.98.22.2
- Máscara: 255.255.255.0



- **Notación alternativa:** 221.98.22.2/24
  - El valor **/24** indica la longitud de la parte de red (nº de unos de la máscara)
  - Esta notación se denomina **Dirección IP Extendida** o notación **CIDR** *(Classless Interdomain Routing)*

El protocolo IP: Máscaras de Red

Ejemplo: Máscaras de red y tablas de encaminamiento



- Enviar paquete Host-A → Host-B
  - Host-A envía paquete directamente a través de su red local
- Enviar paquete Host-A → Host-C
  - Host-A envía el paquete al router y este se encargará de encaminarlo hasta su destino
- Para saber cómo tiene que tratar el paquete, el Host-A:
  - Aplica la máscara de red a la dirección destino. Convierte la dirección del host destino en una dirección de red
  - Consulta la tabla de encaminamiento y decide a quién debe entregar el paquete (host destino o router)
- La máscara de red es en nuestro caso el siguiente valor:
  - 255.255.255.0

El protocolo IP: Máscaras de Red

Ejemplo: Máscaras de red y tablas de encaminamiento

- **Aplicación:** Realizar Y-lógica bit a bit entre la dirección destino y la máscara:

  Dirección del Host-B:

```
221.98.22.2      = 11011101 . 01100010 . 00010110 . 00000010
255.255.255.0    = 11111111 . 11111111 . 11111111 . 00000000
221.98.22.0      = 11011101 . 01100010 . 00010110 . 00000000
```

  Dirección del Host-C:

```
32.99.131.7      = 00100000 . 01100010 . 10000011 . 00000111
255.255.255.0    = 11111111 . 11111111 . 11111111 . 00000000
32.99.131.0      = 00100000 . 01100010 . 10000011 . 00000000
```

- El Host-A consulta su tabla de encaminamiento

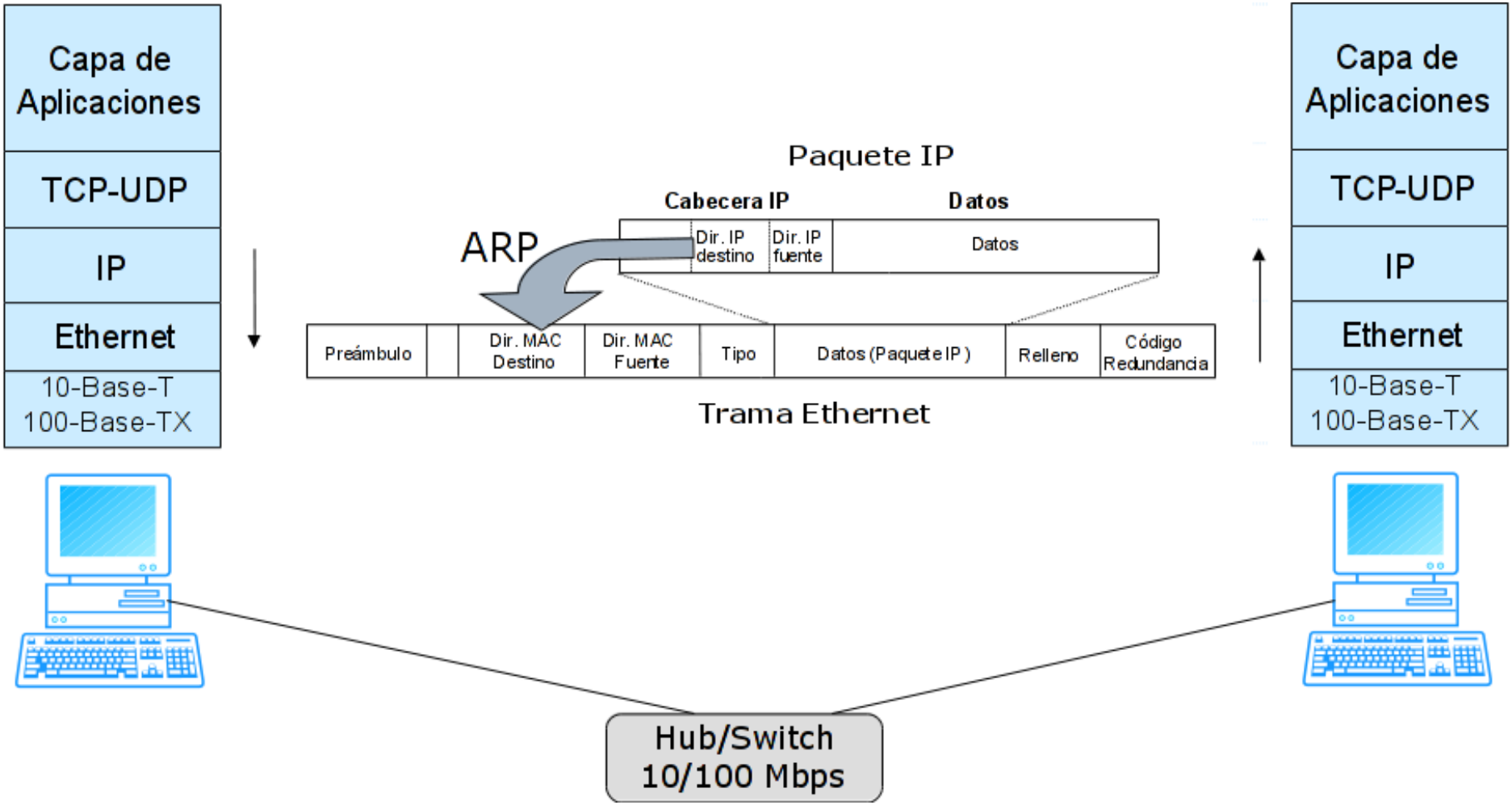
Destination	Gateway
221.98.22.0	0.0.0.0
0.0.0.0 (default)	221.98.22.254
127.0.0.1	127.0.0.1

- Dirección de Gateway del propio remitente (0.0.0.0), el paquete irá por la red local
- Dirección de Gateway es la de un router, se usa ese router.
- Si la dirección no aparece en la tabla se usa el **Default Router.**

Protocolo de traducción de direcciones: ARP

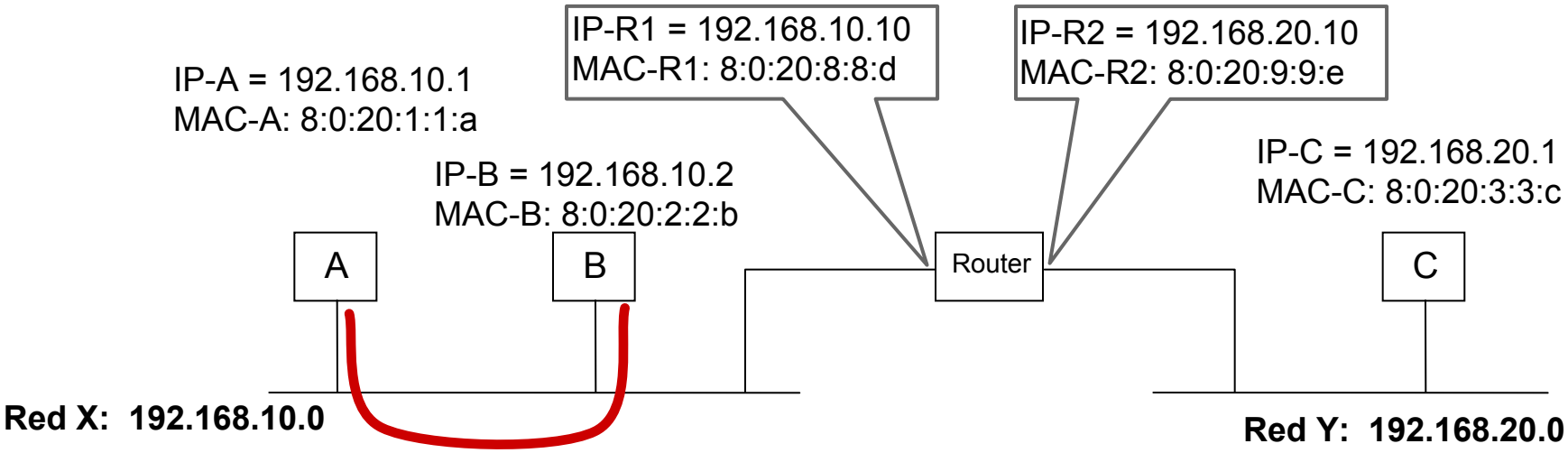
ARP: Address Resolution Protocol

- Traducción: Dirección IP → Dirección MAC



Protocolo de traducción de direcciones: ARP

Procedimiento de comunicación completo (Hosts en la misma red)

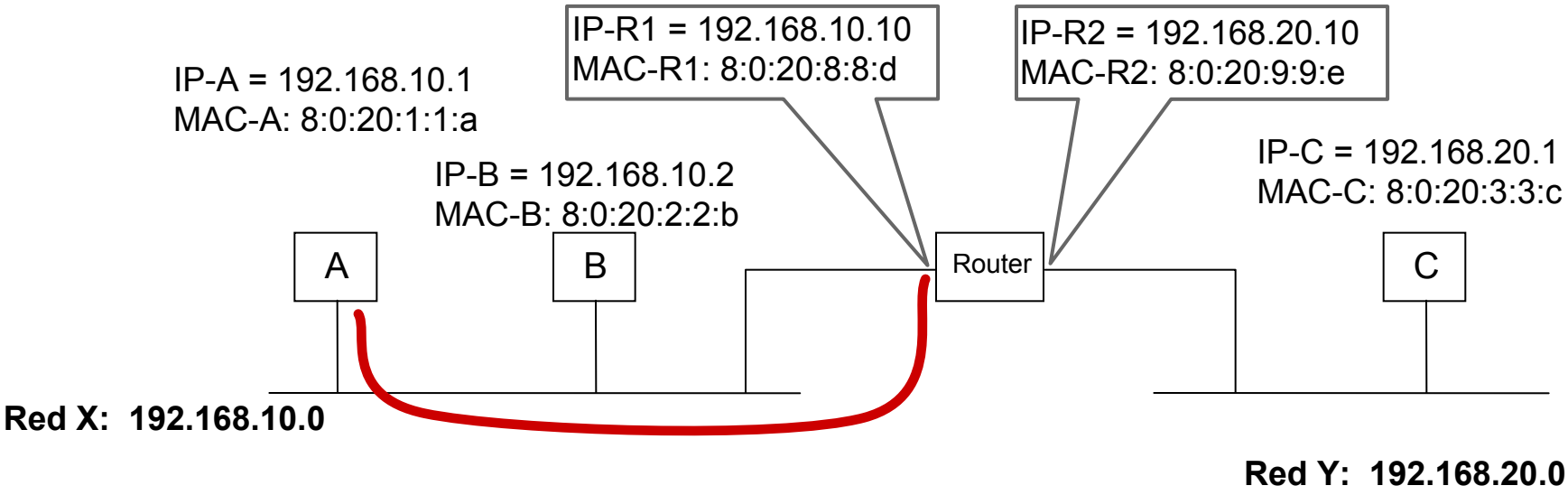


- La estación A aplica el siguiente procedimiento:
- Aplica la máscara de red a la dirección IP destino (IP-B)
- Consulta la tabla de encaminamiento → host destino en la misma red (Red X)
- Utiliza el protocolo ARP para averiguar la MAC asociada a IP-B (MAC-B)
- Envía el paquete IP a la estación B, a través de la Red X, dentro de una trama

Dir. MAC origen: MAC- A **Dir. MAC destino**: MAC-B	**Dir. IP origen**: IP-A **Dir. IP destino**: IP-B	**DATOS**
Cabecera Ethernet	**Cabecera IP**	

Protocolo de traducción de direcciones: ARP

Procedimiento de comunicación completo (Hosts en distinta red)



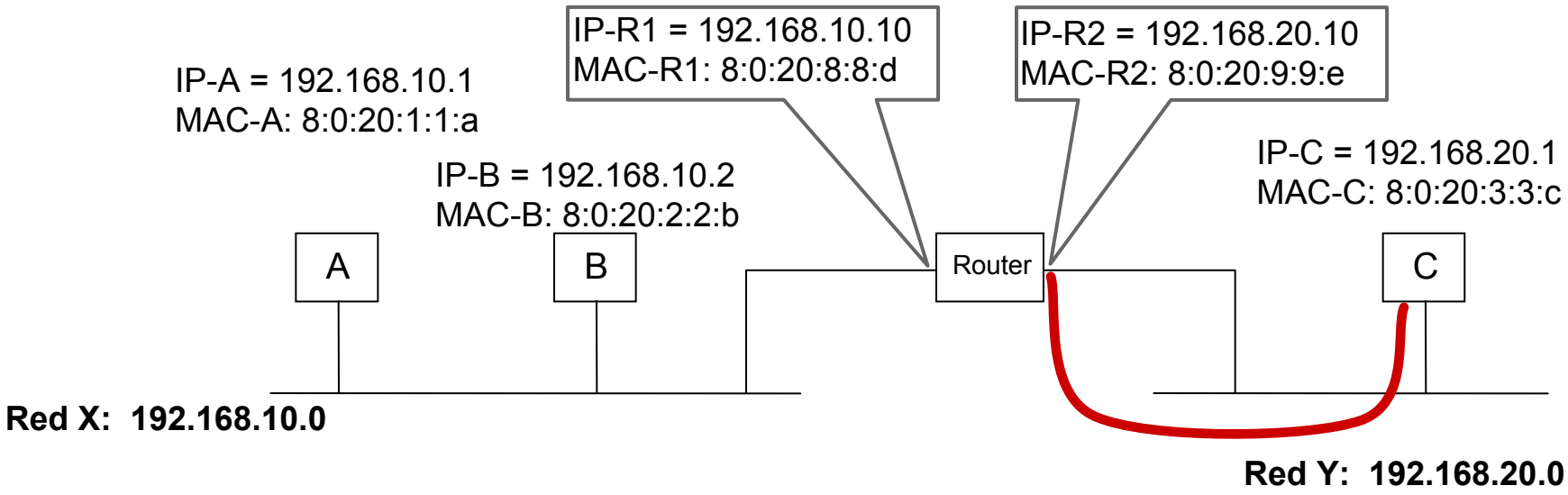
La estación A aplica el siguiente procedimiento:

- Aplica la máscara de red a la dirección IP destino (IP-C)
- Consulta la tabla de encaminamiento → destino está en otra red (Red Y)
- Utiliza el protocolo ARP para averiguar la MAC del default router (MAC-R1)
- Envía el paquete IP al router, a través de la Red X,

Dir. MAC origen: MAC- A **Dir. MAC destino**: MAC-R1	**Dir. IP origen**: IP-A **Dir. IP destino**: IP-C	**DATOS**
Cabecera Ethernet	**Cabecera IP**	

Protocolo de traducción de direcciones: ARP

Procedimiento de comunicación completo (Hosts en distinta red)



Cuando el router recibe el paquete, aplica el siguiente procedimiento:

- El paquete va dirigido a otra máquina (IP-C), el router debe reenviar el paquete
- Aplica la máscara de red a la dirección IP destino (IP-C)
- Consulta la tabla de encaminamiento → el destino está en su red (Red Y)
- Utiliza el protocolo ARP para averiguar la MAC asociada a IP-C (MAC-C)
- Envía un paquete IP a través de la Red Y

Dir. MAC origen: MAC- R1 **Dir. MAC destino**: MAC-C	**Dir. IP origen**: IP-A **Dir. IP destino**: IP-C	**DATOS**
Cabecera Ethernet	**Cabecera IP**	

Organización en redes: Subredes

Ventajas de las subredes

- Permite aislar el tráfico entre las distintas subredes
- Se reduce el tráfico global
- Permite limitar y proteger el acceso a las distintas subredes
- La comunicación entre éstas se realiza mediante un router
- Permite organizar la red en áreas o departamentos
- Se asigna a cada departamento un subconjunto de direcciones IP
- La gestión de las direcciones IP se puede delegar en el propio área o departamento
    - Se descentraliza la tarea de asignación de direcciones
    - Se facilita la tarea del administrador de la red

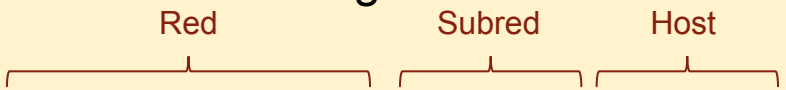
Organización en redes: Subredes

Ejemplo: Supongamos la red de la clase B: 150.23.0.0

- Tenemos 16 bits para identificar a host (2^{16} hosts)


```
    IP:   150. 23.5.7 = 10010110.00010111.00000101.00000111
Máscara:  255.255.0.0 = 11111111.11111111.00000000.00000000
```

- Esta red se puede dividir, por ejemplo, en 256 subredes con 256 hosts cada una
  - Usamos 8 bits para identificar a la subred (2^8 = 256 subredes)
  - Usamos 8 bits para identificar a host (2^8 = 256 hosts)
- Nos queda la siguiente organización:
  - Subred 0: 150.23.0.0 (Dpto. de administración)
  - Subred 1: 150.23.1.0 (Dpto. de RRHH)
  - .....
  - Subred 255: 150.23.255.0 (Dpto. comercial)
- Por tanto la máscara de subred adecuada es la siguiente:

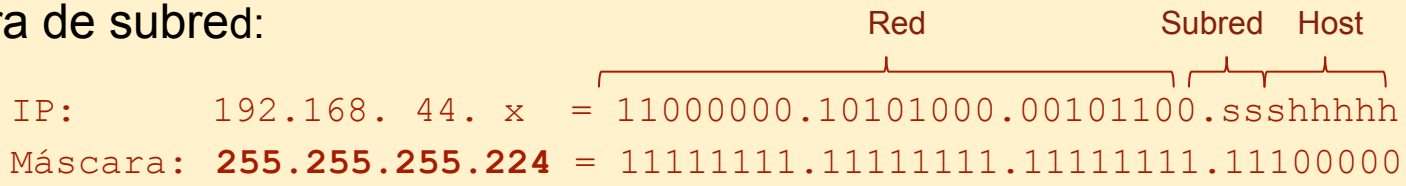



```
     IP:      150. 23. 5. 7 = 10010110.00010111.00000101.00000111
     Máscara: 255.255.255.0 = 11111111.11111111.11111111.00000000
```

Organización en redes: Subredes

Ejemplo: Supongamos la red de la clase C: 192.168.44.0

- Queremos dividir la red en 8 subredes
  - 3 bits para identificar la subred (2^3 = 8 subredes)
  - 5 bits para identificar el host (2^5 = 32 hosts por subred)
- Máscara de subred:



- Organización resultante:

Subred **192.168.44.0**
- hosts: de **192.168.44.1** al **192.168.44.30**
- broadcast : **192.168.44.31**

Subred **192.168.44.32**
- hosts: de **192.168.44.33** al **192.168.44.62**
- broadcast : **192.168.44.63**

Subred **192.168.44.64**
- hosts: de **192.168.44.65** al **192.168.44.94**
- broadcast: **192.168.44.95**

Subred **192.168.44.96**
- hosts: de **192.168.44.97** al **192.168.44.126**
- broadcast: **192.168.44.127**

Subred **192.168.44.128**
- hosts: de **192.168.44.129** al **192.168.44.158**
- broadcast: **192.168.44.159**

Subred **192.168.44.160**
- hosts: de **192.168.44.161** al **192.168.44.190**
- broadcast: **192.168.44.191**

Subred **192.168.44.192**
- hosts: de **192.168.44.193** al **192.168.44.222**
- broadcast: **192.168.44.223**

Subred **192.168.44.224**
- hosts: de **192.168.44.225** al **192.168.44.254**
- broadcast: **192.168.44.255**

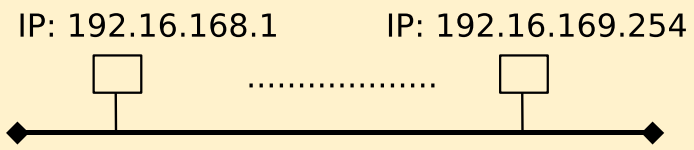
Organización en redes: Superredes

Necesidad de usar superredes (*supernetting*)

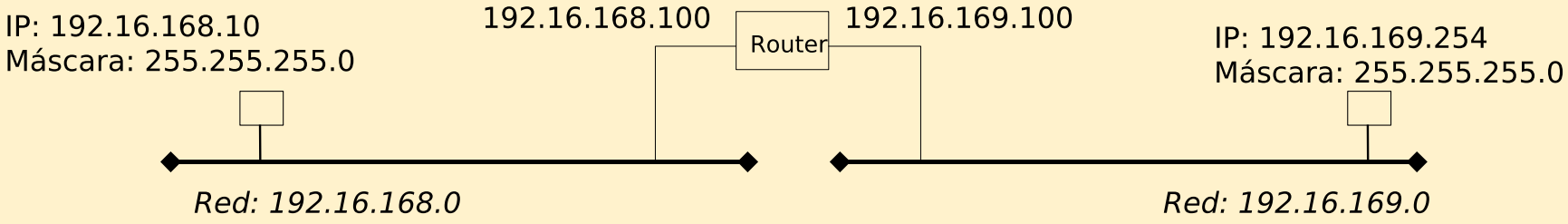
- El supernetting surge por la necesidad de agrupar varias direcciones consecutivas de clase C
- Los routers gestionan estas superredes como una única dirección

Ejemplo: Se solicitan dos direcciones de clase C para organizar una red de 500 hosts:

- 192.16.168.0
- 192.16.169.0



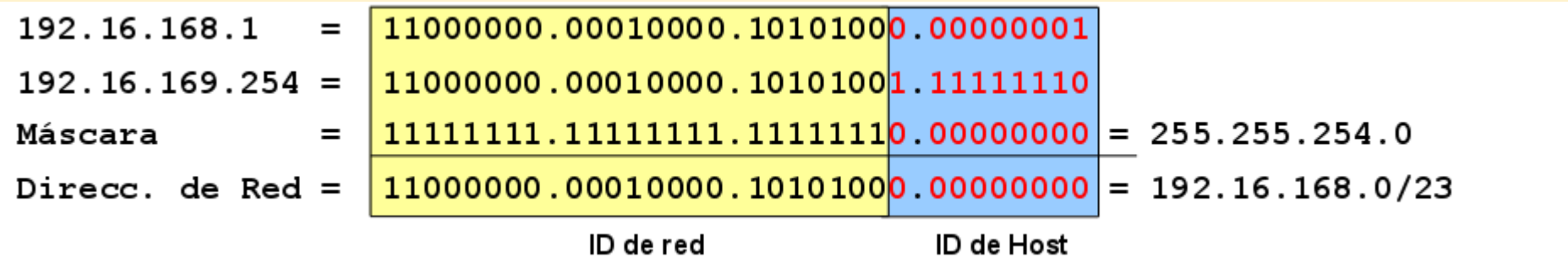
- Si las máquinas se configuran con la máscara de clase C (255.255.255.0)
  - Los dos conjuntos de direcciones quedarían lógicamente aislados
  - Sería necesario utilizar un router para interconectar ambas redes.
  - En Internet, la ruta a esta red se tiene que desglosar en dos rutas separadas, una para cada red



Organización en redes: Superredes

Ejemplo (continuación):

- Si queremos que las máquinas puedan estar ubicadas en la misma red local y se vean unas a otras sin necesidad de usar ningún router, es necesario utilizar una máscara de red distinta



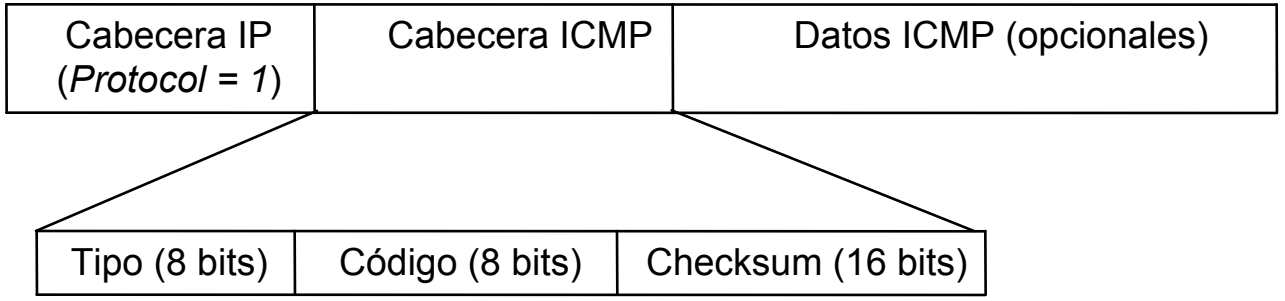
Protocolo ICMP

ICMP: Internet Control Message Protocol

- Es un protocolo para el intercambio de mensajes de control en la red.
- Los mensajes ICMP se pueden clasificar en dos tipos:
  - **Mensajes de error**
    - Permiten informar de situaciones de error en la red
    - Ejemplos: destino inalcanzable, tiempo excedido, problema de parámetro, etc.
  - **Mensajes informativos**
    - Permiten intercambiar información sobre la presencia o el estado de un determinado sistema
    - Ejemplos: mensajes de ECHO, anuncio o solicitud de router, redirecciones, etc.

Protocolo ICMP: Formato del Mensaje

- Los mensajes ICMP se transmiten dentro de **paquetes IP**
  - El protocolo ICMP se corresponde con el identificador 1
- La **cabecera ICMP** contiene la siguiente información:
  - **Tipo** (8 bits): Indica el tipo del mensaje ICMP
  - **Código** (8 bits): Ofrece información adicional sobre el contenido del mensaje. Su significado depende del tipo del mensaje.
  - **Checksum** (16 bits): Es un campo para detectar errores en el mensaje ICMP.

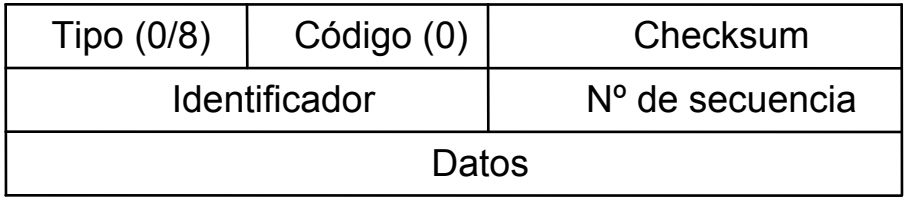


Protocolo ICMP: Tipos de Mensajes

	Tipo	Significado
Mensajes Informativos	0	Echo Reply
	5	Redirect
	8	Echo Request
	9	Router Solicitation
	10	Router Advertisement
Mensajes de error	3	Destination Unreachable
	4	Source Quench
	11	Time Exceeded
	12	Parameter Problem

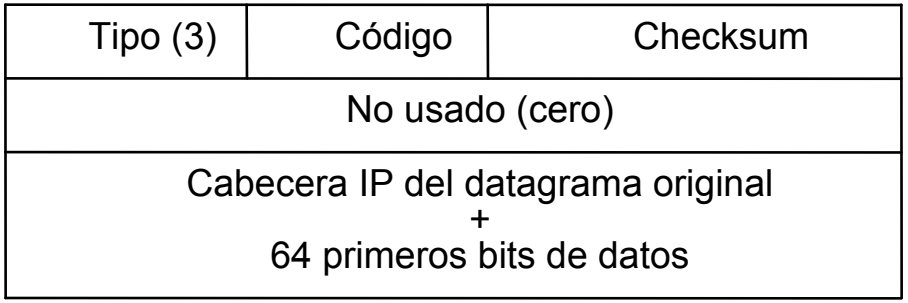
Protocolo ICMP: Echo Request/Reply

- Se utilizan para ver si un computador es alcanzable (habitualmente con **ping**)
- Formato de los mensajes Echo Request/Echo Reply
  - Los **tipos** son 8 (Echo Request) y 0 (Echo Reply)
  - **Código** = 0
  - **Identificador:** Permite establecer la correspondencia entre solicitud (Request) y respuesta (Reply); ambos con el mismo identificador.
  - **Secuencia:** También se utiliza para establecer la correspondencia entre solicitud y respuesta, cuando se envían varios Echo Requests consecutivos con el mismo identificador.
  - **Datos:** Contiene un número determinado de bytes, generados aleatoriamente por la herramienta de diagnóstico. El tamaño se puede especificar como un parámetro de la orden **ping**



Protocolo ICMP: Destination Unreachable

- Estos mensajes los envía el router cuando el destino de un paquete es inalcanzable, para informar al host emisor del paquete de esta situación
- **Formato del mensaje**
  - Tipo = 3
  - Código
    - Especifica la razón por la cual el destino es inalcanzable
    - Véase a continuación la lista de códigos



Protocolo ICMP: Destination Unreachable

Valores del campo Código

0: Network unreachable

- Fallo en el link hacia la red
- Routing incorrecto

1: Host unreachable

- Máquina apagada o desconectada de la red
- Dirección IP incorrecta

2: Protocol unreachable

- Nº de protocolo incorrecto en el paquete IP
- Protocolo no disponible (por ej. OSPF, BGP, etc.)

3: Port unreachable: Puerto UDP cerrado

4: Fragmentation needed but the Do Not Fragment bit was set

5: Source route failed

6: Destination network unknown: Routing incorrecto o Dirección IP incorrecta

7: Destination host unknown: Routing incorrecto o Dirección IP incorrecta

9: Destination network administratively prohibited: Red protegida con un Firewall

10: Destination host administratively prohibited: Host protegido con un Firewall