



REDES

*Grados Ing. Informática / Ing. de Computadores / Ing. del Software / Doble Grado
Universidad Complutense de Madrid*

TEMA 4. La capa de red. Protocolo IP

PROFESORES:

Julio Septi3n del Castillo
Juan Carlos Fabero Jim3nez
Rafael Moreno Vozmediano
Guadalupe Mi3ana Roper
Sergio Bernab3 Garc3a
Sandra Catal3n Pallar3s

Contenidos

1. Repaso de conceptos
2. Protocolo IP: formato del datagrama y fragmentación
3. Protocolo IP: direcciones y máscaras
4. Protocolo ARP
5. Subredes, superredes y CIDR
6. Protocolo ICMP
7. Encaminamiento (routing)

Contenidos

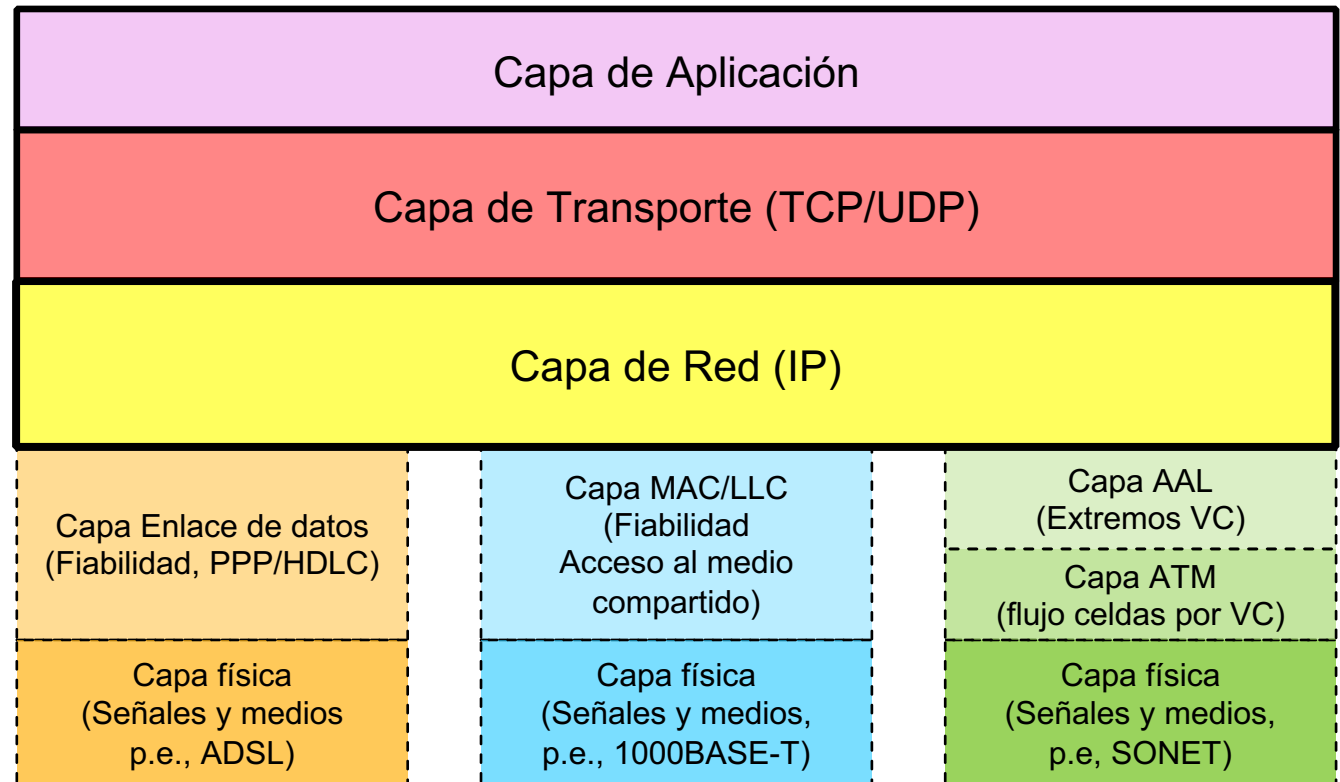
1. Repaso de conceptos
2. Protocolo IP: formato del datagrama y fragmentación
3. Protocolo IP: direcciones y máscaras
4. Protocolo ARP
5. Subredes, superredes y CIDR
6. Protocolo ICMP
7. Encaminamiento (routing)

Arquitecturas de red: OSI vs TCP/IP

Arquitectura
OSI (7 capas)

Aplicación
Presentación
Sesión
Transporte
Red
Enlace
Física

Modelo TCP/IP (5-6 capas)

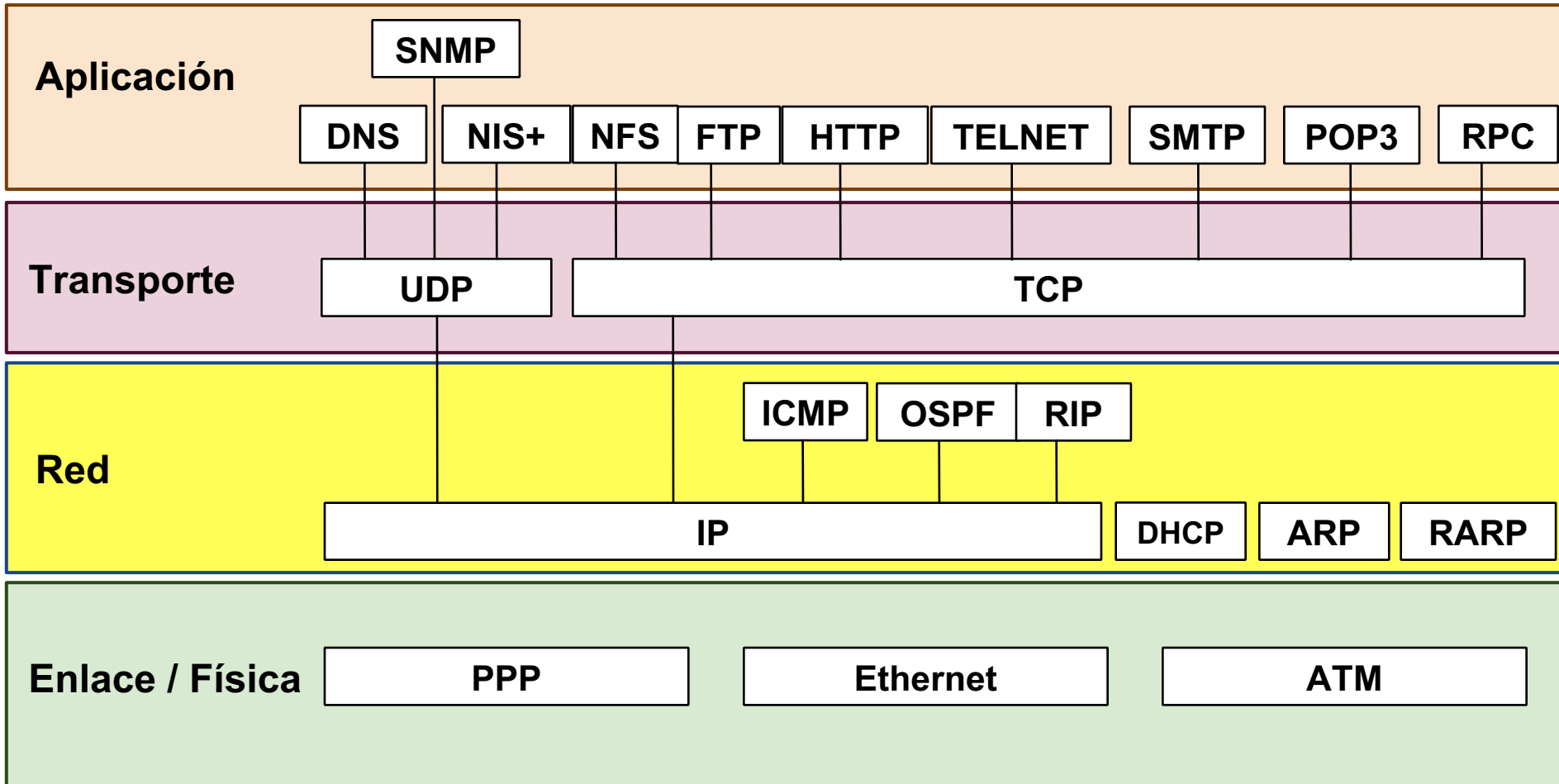


Pto a Pto

LANs

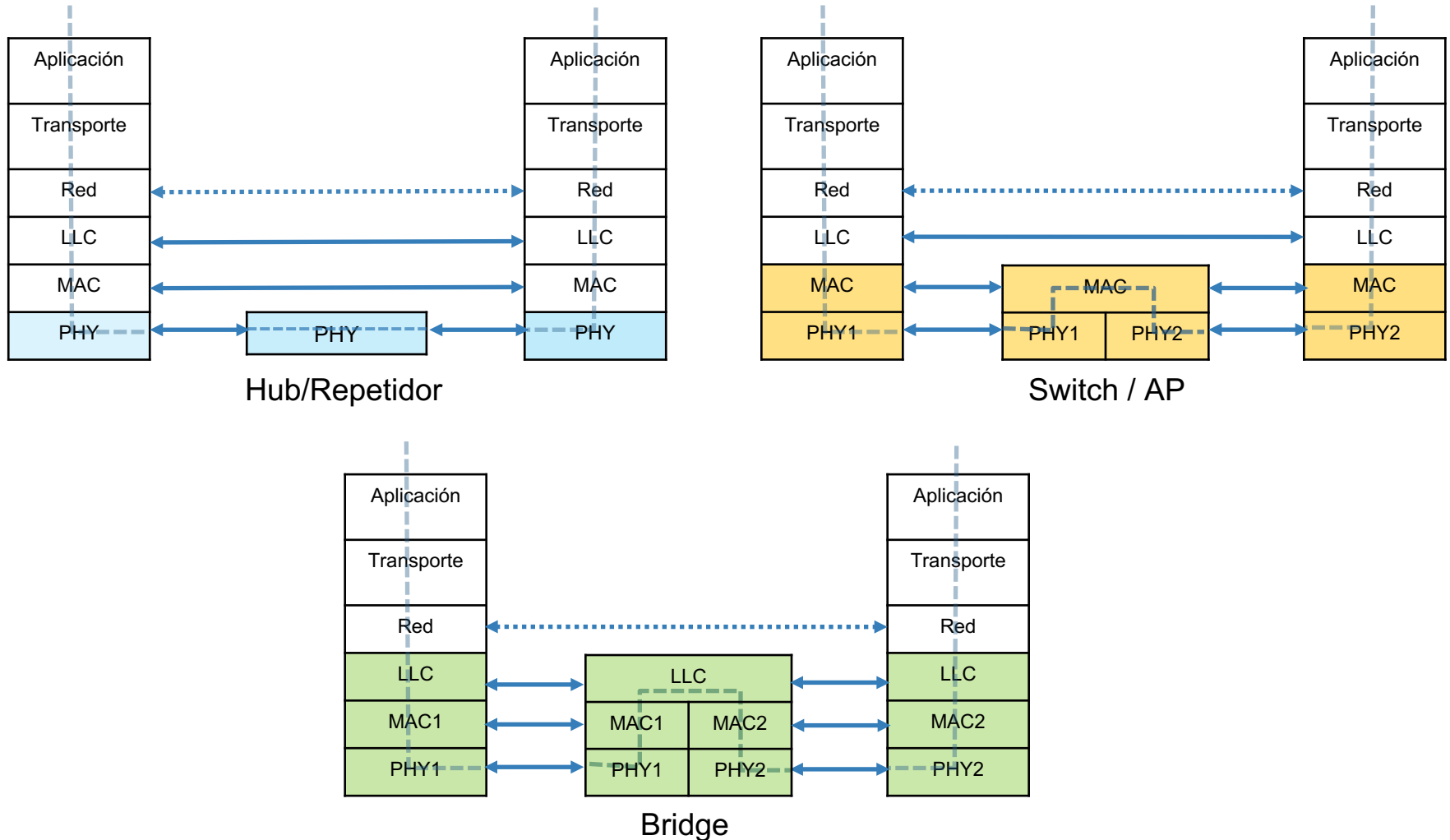
WANS (ATM)

Arquitecturas TCP/IP



Dispositivos de interconexión de redes LAN

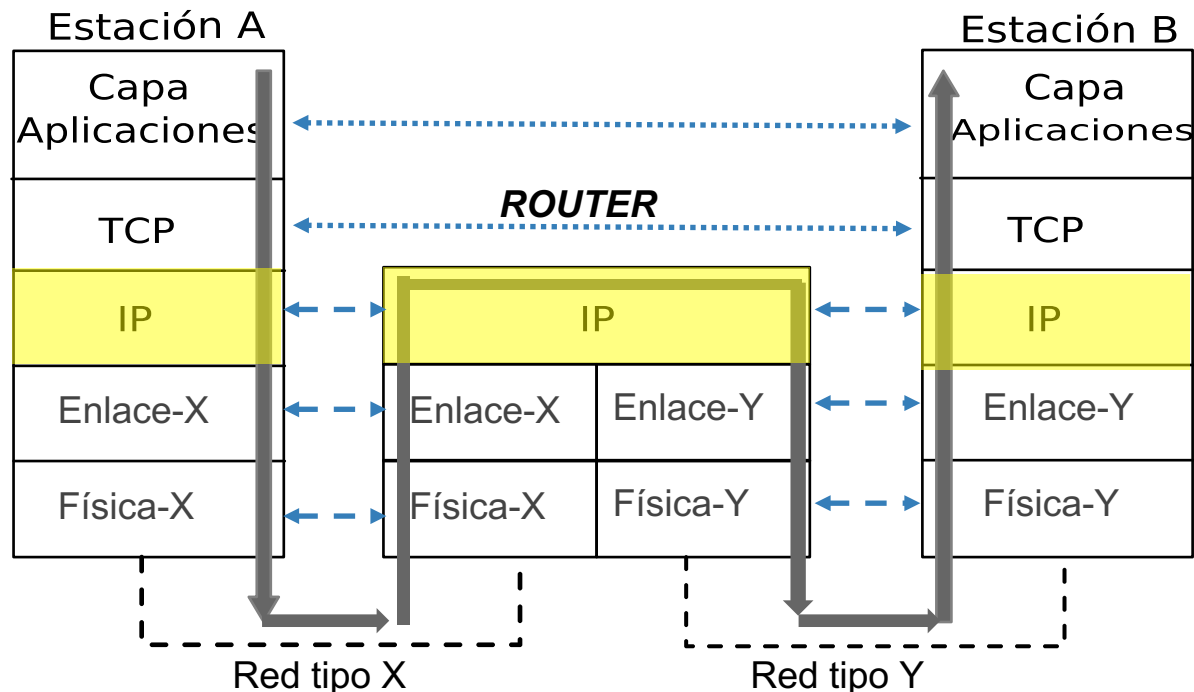
- Hemos visto diferentes dispositivos de interconexión



Principales dispositivos de red

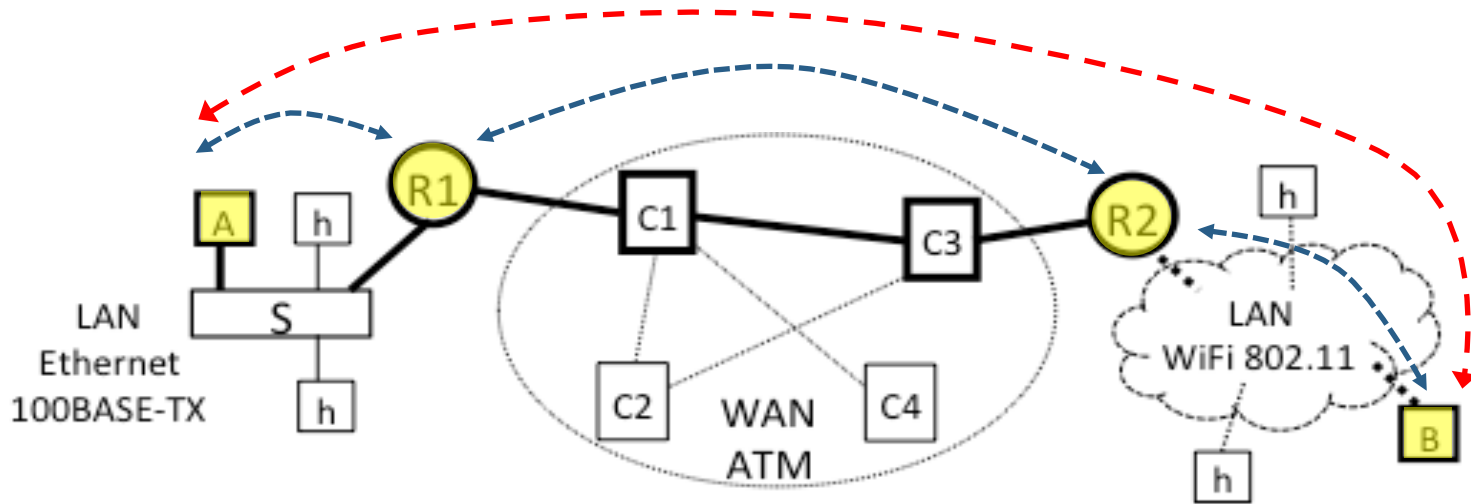
Encaminadores (routers)

- Son dispositivos que trabajan a nivel de la capa de red
- Interconectan al menos dos redes, que pueden ser de tipos distintos
- Funciones básicas:
 - Encaminamiento de paquetes, a través de una ruta con una serie de saltos
 - Con cada salto atraviesa una red diferente
 - Encapsulado del paquete en cada salto en la tecnología de la red (tramas ethernet o wifi o PPP, flujo de celdas ATM...)



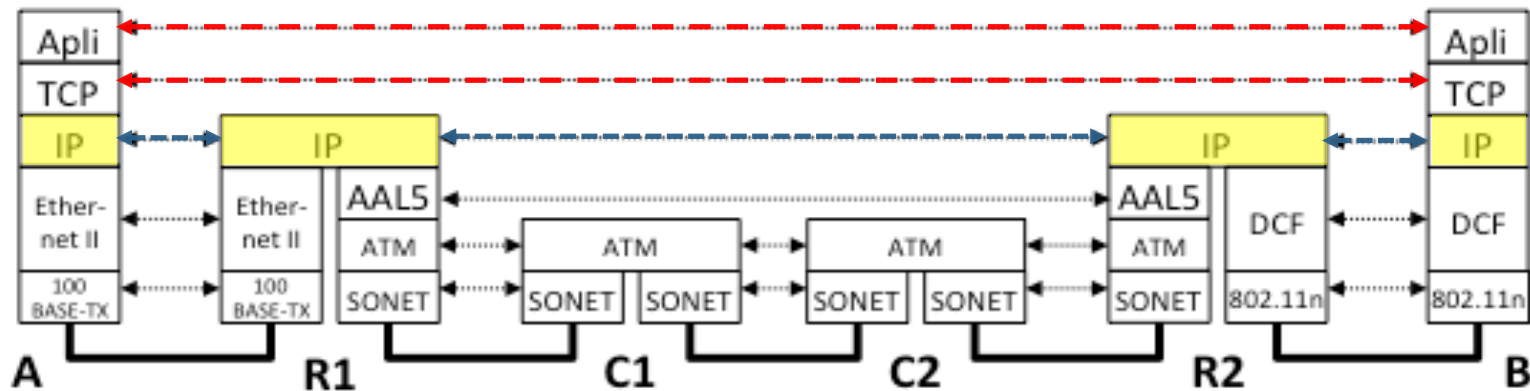
Principales dispositivos de red

Encaminadores y rutas



Usuario

Usuario



Contenidos

1. Repaso de conceptos
2. Protocolo IP: formato del datagrama y fragmentación
3. Protocolo IP: direcciones y máscaras
4. Protocolo ARP
5. Subredes, superredes y CIDR
6. Protocolo ICMP
7. Encaminamiento (routing)

El protocolo IP

Protocolo de red de Internet: IP (Internet Protocol)

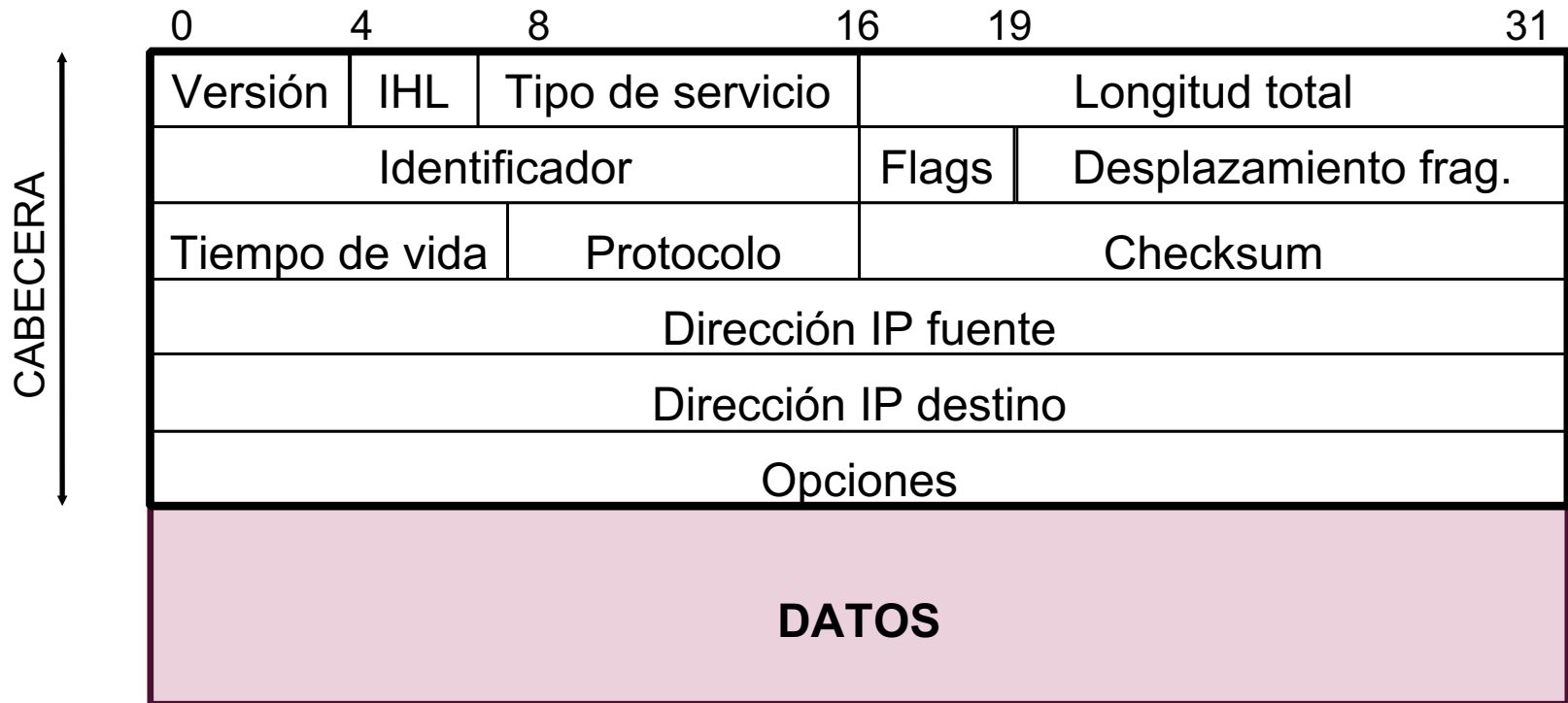
- Proporciona un servicio básico de entrega de paquetes
 - Sobre el que se construyen las redes TCP/IP
- Protocolo **no orientado a conexión y no fiable**
 - No realiza detección ni recuperación de paquetes perdidos o erróneos
 - No garantiza que los paquetes lleguen en orden
 - No garantiza la detección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

Funciones básicas del protocolo IP

- **Direccionamiento**
 - Esquema global de direccionamiento de redes y nodos, jerárquico
- **Encaminamiento de paquetes: 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.
- **Fragmentación y reensamblado** de los datagramas
 - División del datagrama en fragmentos de un tamaño aceptable por cada red

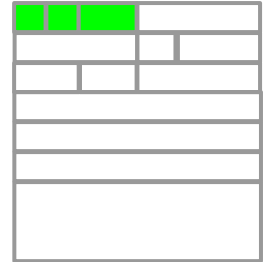
El protocolo IP: Formato del datagrama

- **Formato del Datagrama IP (versión 4)**
 - Organizado en palabras de 32 bits
 - Cabecera fija 5 palabras + Opciones + Datos



El protocolo IP: Formato del datagrama

- **Versión (4 bits):** valor=4 (IPv4)
- **Longitud de la cabecera (IHL) (4 bits)**
 - En palabras de 32 bits
 - Tamaño máximo de la cabecera = 15 palabras (60 bytes)
 - En realidad indica el tamaño del campo Opciones
- **Tipo de servicio (8 bits)**



0	1	2	3	4	5	6	7
Prioridad			Calidad de servicio (QoS)				Reserv.

- **Prioridad**
 - Especifica la prioridad del datagrama (hasta 8 niveles)
 - Un paquete de alta prioridad debe ser reexpedido por un router antes que un paquete de baja prioridad (aunque éste llegase antes)
- **QoS:** Puede tomar los siguientes valores
 - 1000 → Minimizar retardo
 - 0100 → Maximizar rendimiento (velocidad de transmisión)
 - 0010 → Maximizar fiabilidad (seguridad en la entrega)
 - 0001 → Minimizar coste monetario
 - 0000 → Servicio normal

El protocolo IP: Formato del datagrama

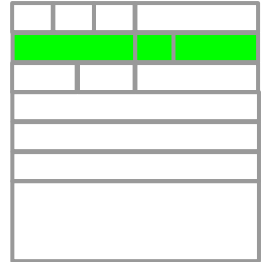
- **Longitud total (16 bits)**
 - Longitud del datagrama (cabecera + datos) medida en bytes
 - Campo Longitud Total ocupa 16 bits
 - Longitud máxima del datagrama: 2^{16} bytes = 64 Kbytes
- **Tiempo de vida (TTL, *Time To Live*) (8 bits)**
 - N° routers que puede atravesar el paquete (N° saltos)
 - Se decrementa en cada router
 - Cuando TTL=0 el paquete debe ser descartado
- **Protocolo (8 bits)**
 - Protocolo de la capa superior al que deben entregarse los datos
 - 1: Internet Control Message Protocol (ICMP)
 - 2: Internet Group Management Protocol (IGMP)
 - 6: Transmission Control Protocol (TCP)
 - 8: Exterior Gateway Protocol (EGP)
 - 17: User Datagram Protocol (UDP)
- **Checksum (16 bits)**
 - Suma de control de la cabecera (no de datos, sólo paridad)



El protocolo IP: Formato del datagrama

FRAGMENTACION IP:

- Cuando un datagrama IP debe atravesar una red se comprueba:
Long Total \leq MTU de la red (Maximum Transfer Unit de la red, capacidad de datos de la trama)
- Si no se cumple, se divide en varios datagramas fragmentos que siguen su viaje hasta el destino de forma independiente
- Se reconstruye el datagrama original SOLO en destino.
- Se reparten los datos en varios datagramas, cada uno con una cabecera con mismo origen y destino y distintos campos que permiten la reconstrucción del original.
- Para cada fragmento se debe cumplir: **Long Total fragmento \leq MTU**

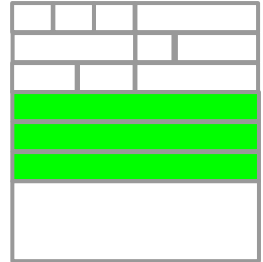


• Campos para FRAGMENTACION:

- **Identificador (16 bits):** Número que identifica al datagrama original
- **Flags (3 bits):**
 - **MF (More Fragments):** si está a 1 indica que no es el último fragmento
 - **DF (Don't Fragment):** si es 1 prohíbe la fragmentación
- **Desplazamiento del fragmento (Offset) (13 bits):**
 - Posición de los datos del fragmento en los datos del datagrama original.
 - En bloques de de 8 bytes!!!! (sólo tenemos 13 bits)

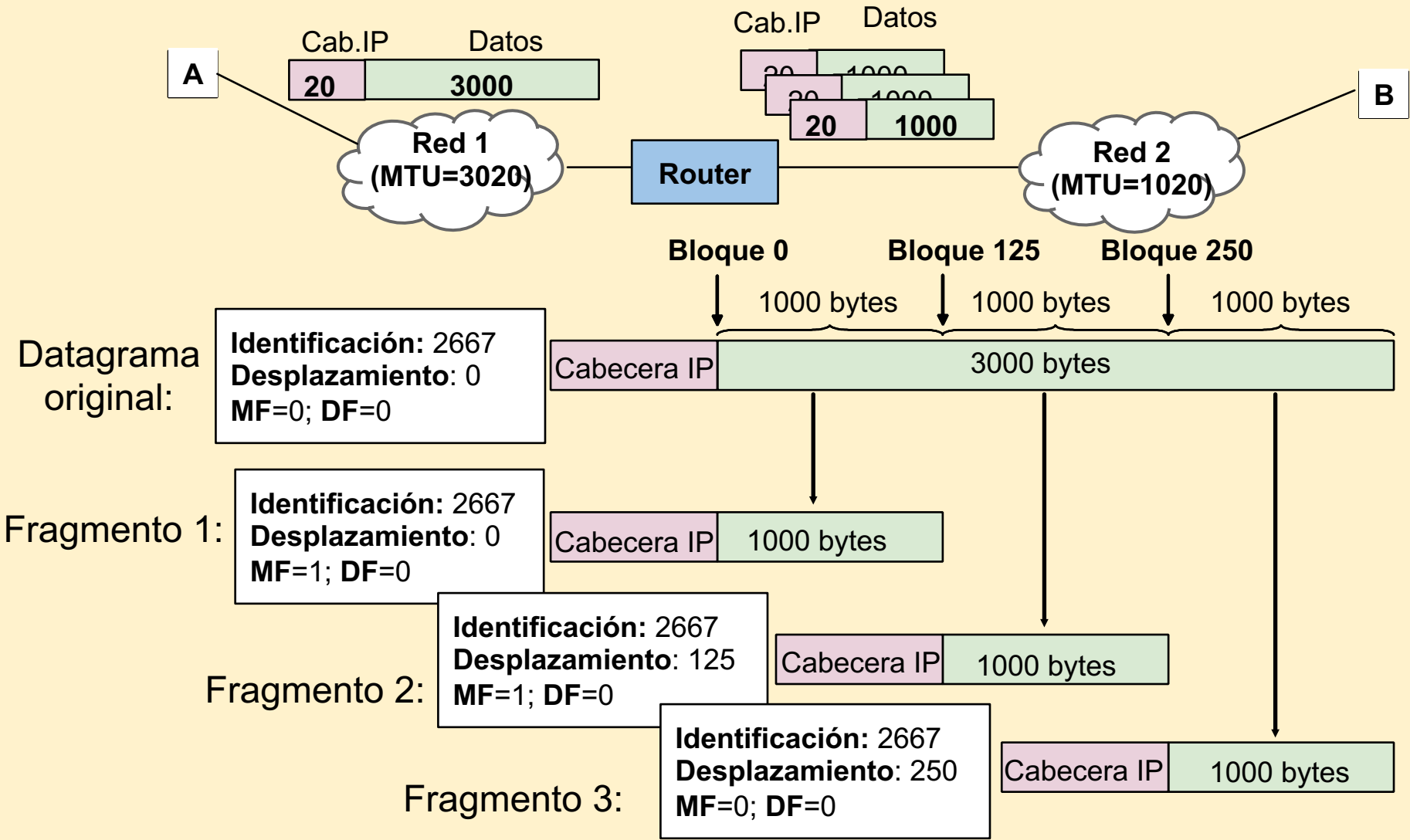
El protocolo IP: Formato del datagrama

- **Direcciones IP origen y destino (32 bits c.u.)**
 - Identifican al host emisor y al receptor del datagrama
 - Se interpretan de forma jerárquica: parte red + parte host
 - Determinan la forma en que se organiza Internet
 - Las vemos más adelante
- **Opciones**
 - Campo opcional, con opciones especiales
 - Ejemplos: encaminamiento de origen, sello de ruta, sello de tiempo, etc.
 - Tamaño máximo del campo opciones: 10 palabras de 32 bits



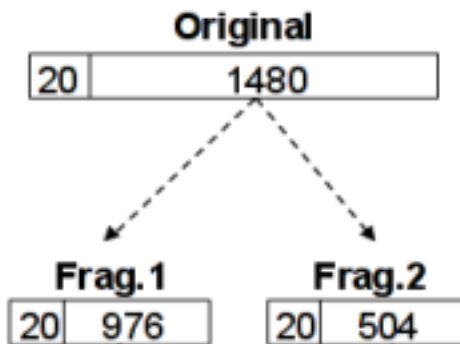
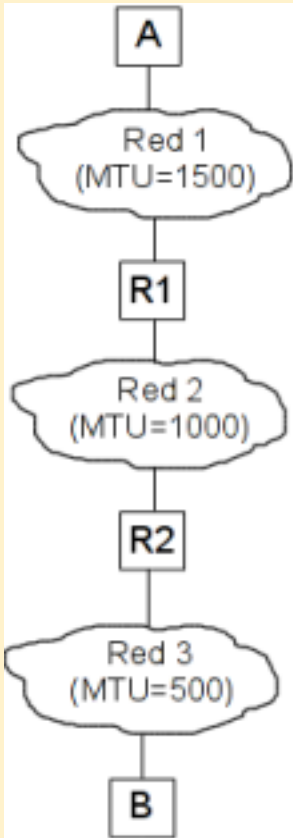
El protocolo IP: Fragmentación

Ejemplo



El protocolo IP: Fragmentación

Ejemplo:



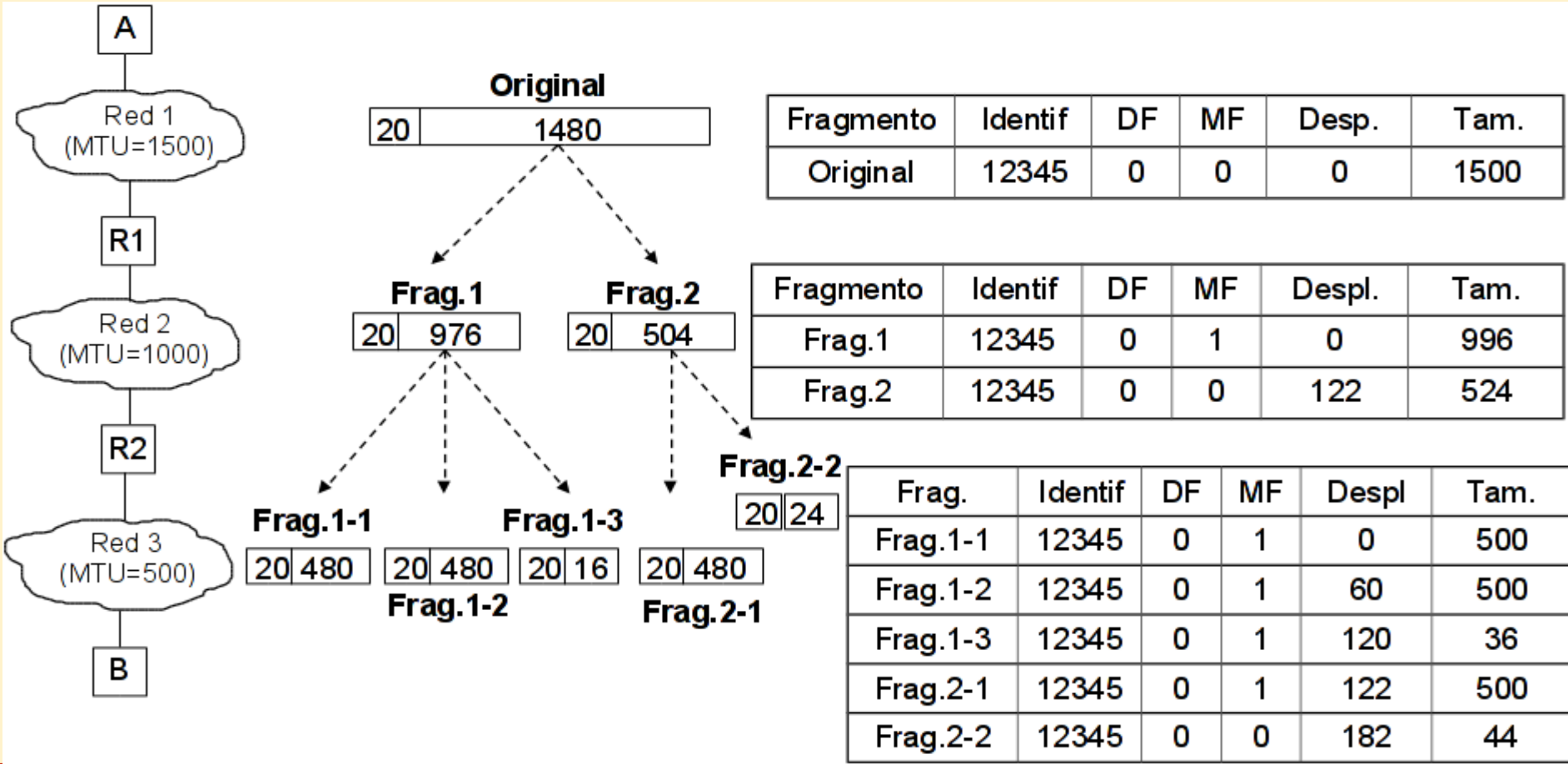
Fragmento	Identif	DF	MF	Desp.	Tam.
Original	12345	0	0	0	1500

Fragmento	Identif	DF	MF	Despl.	Tam.
Frag.1	12345	0	1	0	996
Frag.2	12345	0	0	122	524

- A genera un datagrama del tamaño máximo permitido por Red1, que llega sin problemas hasta R1
- R1 comprueba que $1500 > 1000$ (MTU de Red2)
- En Red2 la MTU admitiría 20 + 980 bytes de datos.
Pero hay que comprobar cuántos bloques de 8 son 980 bytes:
-> $980 / 8 = 122$ y sobran 4 bytes.
- El primer fragmento tiene desplazamiento 0 ("primero"), y admite 122 bloques (976 bytes) pero no 123 (984 bytes)
- En el segundo fragmento se incluyen 1480-976 bytes = 504 bytes, y se usa un desplazamiento de 122 bloques, y bit MF=0 ("último")

El protocolo IP: Fragmentación

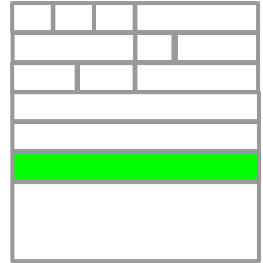
- Para cada fragmento R2 realiza la misma operación: comprueba si tamaño > 500 (MTU de Red3)
- En Red3 la MTU admitiría 20 + 480 bytes de datos -> $480 / 8 = 60$ exactamente.
- El primer fragmento 1-1 admite 60 bloques (480 bytes), los demás sucesivamente.
- Los desplazamientos en F1-1, F1-2, F1-3, etc., se suman relativos al que traía cada fragmento de partida
- Sólo el ultimo fragmento de fragmento puede tener el bit MF=0 (“último”)



El protocolo IP: Campo Opciones

Encaminamiento estricto de origen (*Strict Source Routing*)

- Proporciona un medio para que el emisor del paquete pueda especificar la ruta explícita que debe seguir el datagrama
 - Se recomienda filtrar o, al menos, dar la posibilidad, los datagramas IP que contengan esta opción o la de encaminamiento relajado desde el origen (LSRR, Loose Source and Record Route) (RFC7126).



Registro de ruta (*Record Route*)

- Proporciona un medio para registrar la ruta exacta que ha seguido el datagrama en el camino hacia su destino (direcciones de los routers por los que ha pasado el datagrama)

Sello de tiempo de Internet (*Internet Timestamp*)

- Proporciona un medio para registrar los instantes temporales en los que el paquete ha pasado por cada router y, adicionalmente, las direcciones de estos routers

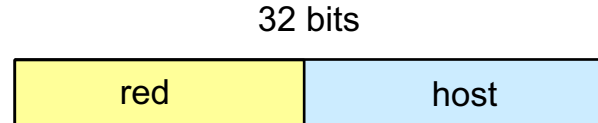
Contenidos

1. Repaso de conceptos
2. Protocolo IP: formato del datagrama y fragmentación
- 3. Protocolo IP: direcciones y máscaras**
4. Protocolo ARP
5. Subredes, superredes y CIDR
6. Protocolo ICMP
7. Encaminamiento (routing)

El protocolo IP: Direcciones

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
- Direcciones jerárquicas:
 - Parte red (común a todos los nodos de la red)
 - Parte nodo o host



Tipos de direcciones IPv4

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

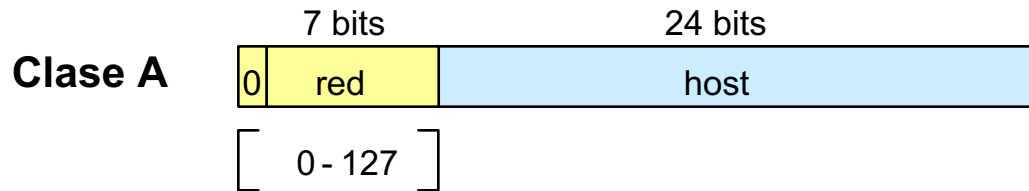
El protocolo IP: Direcciones

Administración y registro de direcciones

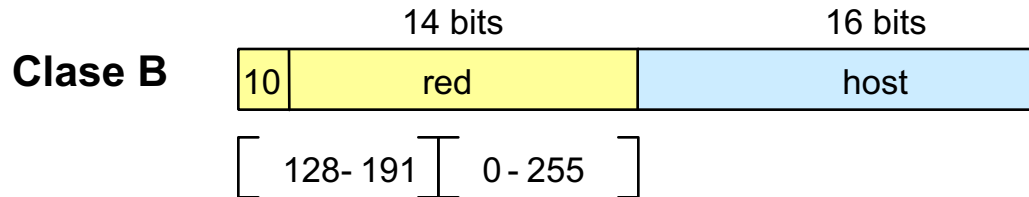
- **Entidades regionales de registro de Internet:** La parte que identifica a la red es fija para cada red y es necesario solicitarla a una de las entidades regionales de registro de Internet (**RIR, Regional Internet Registries**)
- Cada RIR es responsable de administrar y registrar las direcciones IP de su región geográfica:
 - **ARIN** (*American Registry for Internet Numbers*): Norteamérica
 - **RIPE** (*Reseaux IP Europeens*): Europa y Oriente Medio
 - **APNIC** (*Asia Pacific Network Information Center*): Asia-Pacífico
 - **LACNIC** (*Latin American and Caribbean Network Information Center*): Sudamérica y países caribeños
 - **AfriNIC** (*African Network Information Center*): África

El protocolo IP: Direcciones

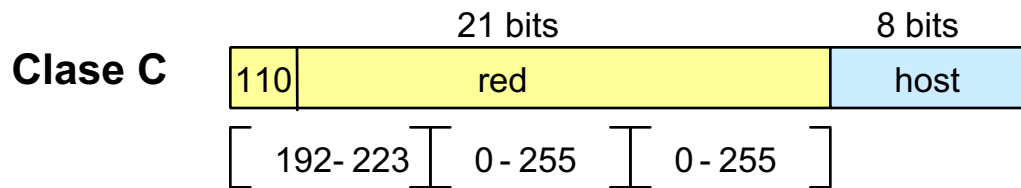
Direcciones IPv4 basadas en clase (classful)



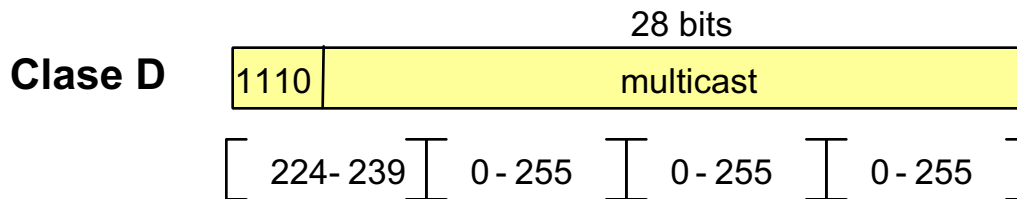
$2^7 = 128$ redes
 $2^{24} = 16.777.216$ direcciones
Ejemplo: **26**.56.120.9



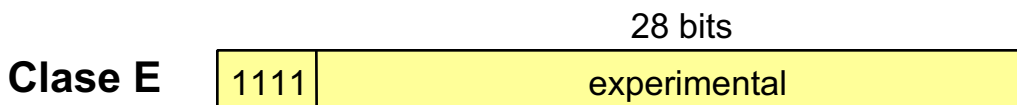
$2^{14} = 16.384$ redes
 $2^{16} = 65.536$ direcciones
Ejemplo: **147.96**.50.110



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



Ejemplo: **224.0.0.1**



El protocolo IP: Direcciones

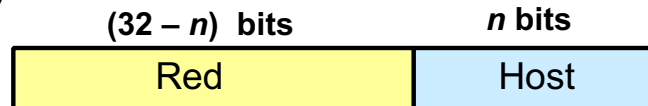
Direcciones IPv4 sin clase (classless)

Ejemplo: Problema de las direcciones con clases

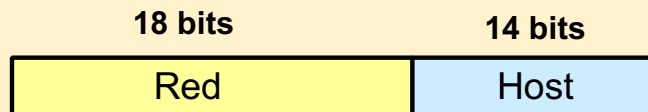
- Una empresa/institución necesita aprox. 15.000 direcciones IP
 - Con el direccionamiento con clase tiene que contratar una red clase B completa (65.536 direcciones)
 - El coste es muy elevado (más direcciones de las necesarias)
 - Se desaprovechan las mayoría de las direcciones (más de 50.000)
- Usando direcciones sin clases
 - Se puede contratar un conjunto más ajustado (en potencias de 2)
 - En este caso, se pueden contratar $2^{14} = 16.384$ direcciones

Formato de las direcciones sin clase

- Los campos de red y host no están limitados a un número entero de bytes



Ejemplo: En el ejemplo anterior con n=14



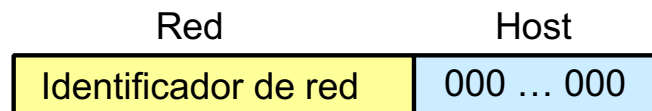
El protocolo IP: Direcciones especiales

Direcciones de red (terminadas en 00...000), es el “nombre” de la red.

- Se utilizan para representar a una red completa en las tablas de rutas o encaminamiento, donde los routers almacenan los destinos conocidos
- Nunca se utilizan como dirección destino ni se asignan a un host concreto
- Ejemplo de tabla de rutas en Linux:

```
# 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    0.0.0.0         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 disponible en la red



El protocolo IP: Direcciones especiales

Ejemplo: Direcciones de red

- Red de clase A:

Red (8)	Host (24)
00011011	.00000000.00000000.00000000

 = 27.0.0.0
- Red de clase B:

Red (16)	Host (16)
10001110.01011000	.00000000.00000000

 = 142.88.0.0
- Red de clase C:

Red (24)	Host (8)
11000111.01000011.11101111	.00000000

 = 199.67.239.0
- Red sin clase (n=14):

Red (18)	Host (14)
01011010.00100000.10	000000.00000000

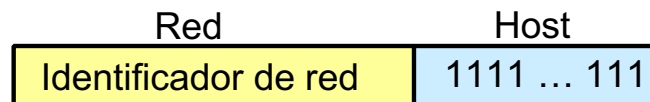
 = 90.32.128.0
- Red sin clase (n=5):

Red (27)	Host (5)
10001111.00011010.00000111.011	00000

 = 143.26.7.96

El protocolo IP: Direcciones especiales

- **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**
- **Dirección del propio nodo (“yo”)**
 - 0.0.0.0
- **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 disponible en la red



El protocolo IP: Direcciones especiales

Ejemplo: Direcciones de broadcast

- Red de clase A: Red (8) Host (24)
00011011.1111111.11111111.11111111 = 27.255.255.255
- Red de clase B: Red (16) Host (16)
10001110.01011000.11111111.11111111 = 142.88.255.255
- Red de clase C: Red (24) Host (8)
11000111.01000011.11101111.11111111 = 199.67.239.255
- Red sin clase (n=14): Red (18) Host (14)
01011010.00100000.10111111.11111111 = 90.32.191.255
- Red sin clase (n=5): Red (27) Host (5)
10001111.00011010.00000111.01111111 = 143.26.7.127
- Dir. broadcast universal: 255.255.255.255

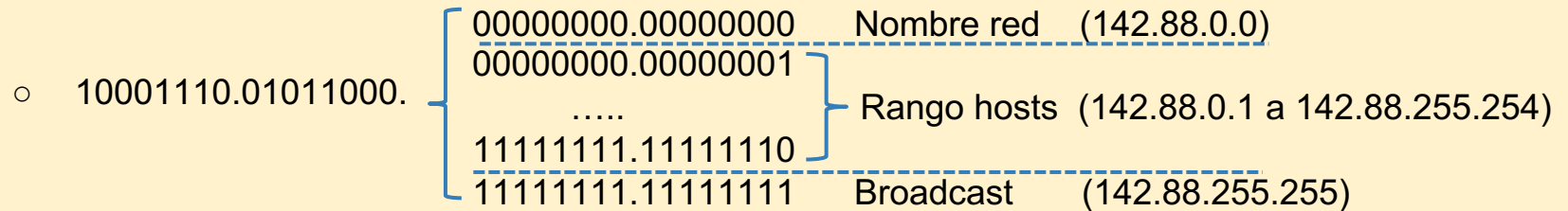
El protocolo IP: Direcciones especiales

- **Direcciones disponibles para hosts:**

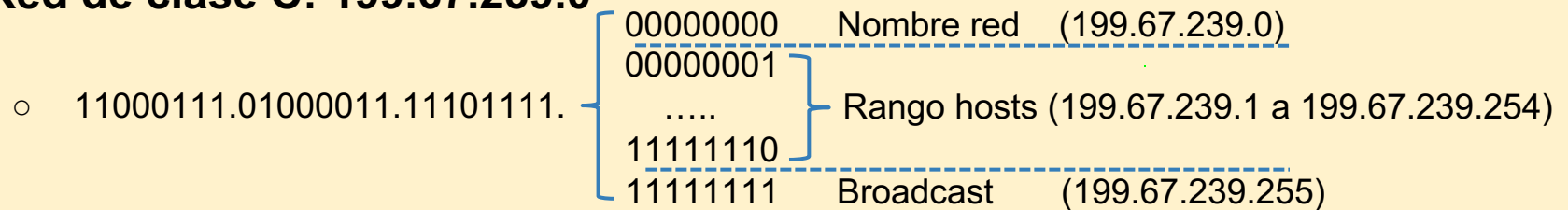
Es todo el rango entre el nombre de la red y la dirección de broadcast: $2^n - 2$

Ejemplos:

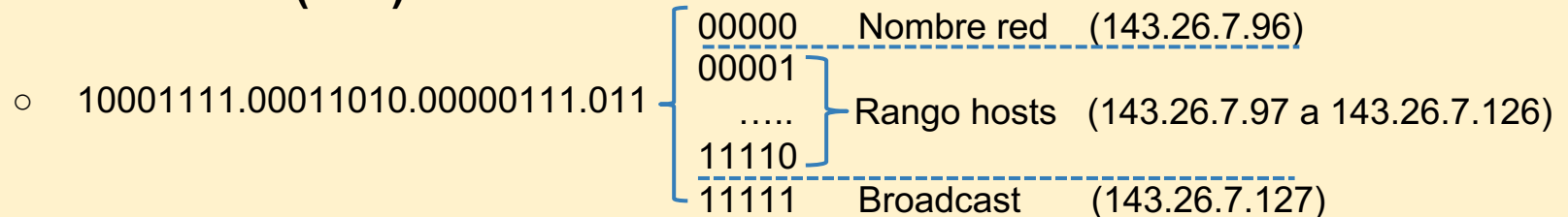
- **Red de clase B: 142.88.0.0**



- **Red de clase C: 199.67.239.0**



- **Red sin clase (n=5): 143.26.7.96**



El protocolo IP: Direcciones especiales

- **Direcciones reservadas para redes privadas**
 - Existe un conjunto de direcciones reservadas para uso privado
 - No son válidas para su uso en Internet, como direcciones públicas
 - Se pueden asignar a redes aisladas de Internet
 - Se pueden asignar a redes conectadas a través de un router que hace **traducción de direcciones de red** (NAT), p.e., las redes domésticas
 - Los rangos de direcciones IP privadas son los siguientes:
 - La red 10.0.0.0 ~ 1 red de clase A
 - Las redes 172.16.0.0 a 172.31.0.0 ~ 16 redes de clase B
 - Las redes 192.168.0.0 a 192.168.255.0 ~ 256 redes de clase C

Las redes domésticas típicamente utilizan una red privada de clase C:

- La 192.168.0.0
- Al router por defecto se le suele asignar la IP 192.168.0.1, y al resto de los nodos las direcciones sucesivas.
- Imprescindible el uso de NAT en el router que da acceso a Internet, cambiando estas direcciones “privadas” o locales, por otras públicas que gestiona el ISP.

El protocolo IP: Máscaras de red

La máscara de red indica:

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

Aplicada la AND bit a bit a una dirección de un host, permite **extraer la red a la que pertenece**. (Es el paso previo para poder luego buscar como llegar a esa red)

Ejemplo:


- Dirección de clase C: 221.98.22.2
- Máscara: 255.255.255.0

	Red	Host	
IP:	11011101 . 01100010 . 00010110 . 00000010 = 221.98.22.2		
Máscara:	11111111 . 11111111 . 11111111 . 00000000 = 255.255.255.0		
Red:	11011101 . 01100010 . 00010110 . 00000000 = 221.98.22.0		

- **Notación alternativa (significa lo mismo): 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

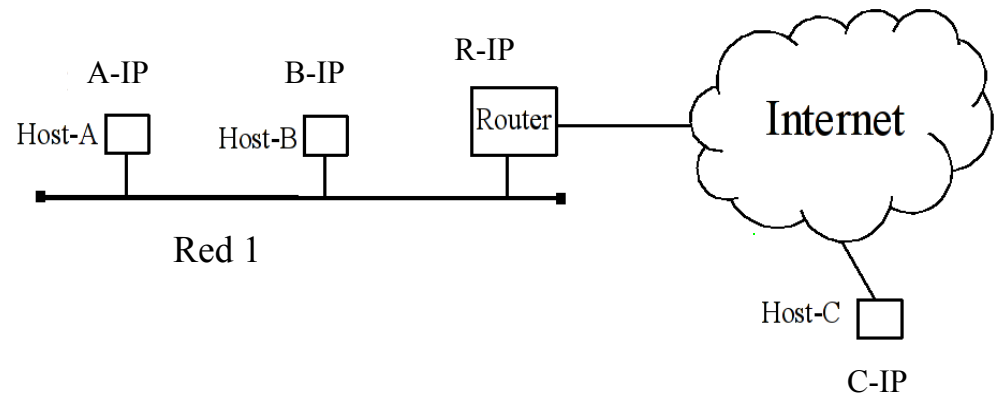
				Notación CIDR (Dir. IP extendida)
				
Dir. de clase A =	Red (8) 00011011.	Host (24) 00000111.10000010.00000011	= 27.7.130.3	} 27.7.130.3/8
Máscara =	11111111.	00000000.00000000.00000000	= 255.0.0.0	
Dir. de clase B =	Red (16) 10001110.01011000.	Host (16) 00001100.00000100	= 142.88.12.4	} 142.88.12.4/16
Máscara =	11111111.11111111.	00000000.00000000	= 255.255.0.0	
Dir. de clase C =	Red (24) 11000111.01000011.11101111.	Host (8) 00000110	= 199.67.239.6	} 199.67.239.6/24
Máscara =	11111111.11111111.11111111.	00000000	= 255.255.255.0	
Dir. sin clase =	Red (18) 01011010.00100000.10	Host (14) 000011.00000101	= 90.32.131.5	} 90.32.131.5/18
Máscara =	11111111.11111111.11	000000.00000000	= 255.255.192.0	
Dir. sin clase =	Red (27) 10001111.00011010.00000111.011	Host (5) 00011	= 143.26.7.99	} 143.26.7.99/27
Máscara =	11111111.11111111.11111111.111	0000	= 255.255.255.224	

El protocolo IP: Forwarding

Forwarding:

- Es la decisión de cuál es el **siguiente salto** para una datagrama, que toma cualquier nodo, host o router
- Se basa en la **tablas de rutas** con todos los destinos (redes) alcanzables
- Por ejemplo, en el host A la mínima tabla de rutas necesaria sería:

Red Destino:	Por:
Red 1	A-IP (yo)
Default (resto)	R-IP



- Partiendo de la dirección IP del destino en el datagrama, A hace:
 - 1- Le aplica la máscara de red: obtiene la **Red de destino**
 - 2- Busca en la tabla de rutas esa red de destino:
 - Misma red que A (Red 1): lo entrega A de forma **DIRECTA**
 - Otra red (Default): entrega **INDIRECTA**, de A al Router R-IP, que ya decidirá cómo hacerlo llegar hasta dicha red.

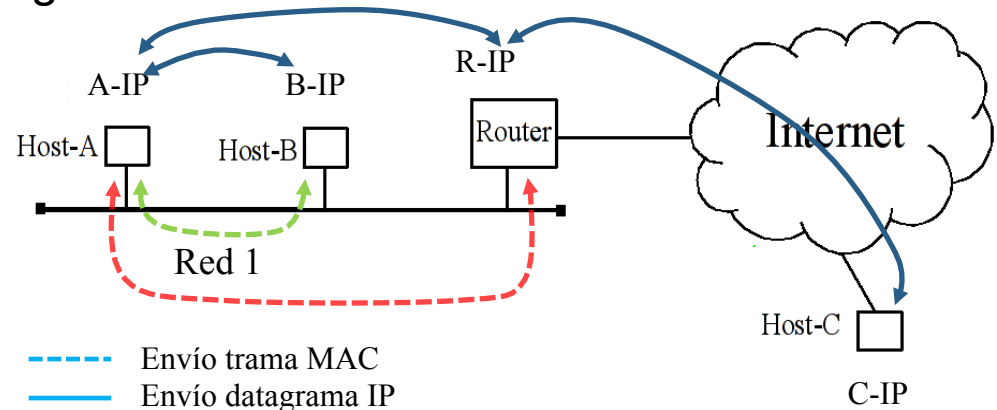
El protocolo IP: Forwarding

En el ejemplo anterior, podemos distinguir los dos tipo de envío:

- Envío de datagrama **A-IP** → **B-IP**
 - Host-A envía el datagrama directamente al destino B-IP a través de su red local, encapsulado en una trama MAC: **A-MAC** → **B-MAC** (**entrega directa**)
- Envío de datagrama **A-IP** → **C-IP**
 - Host-A gestiona solo el primer salto del datagrama, lo envía al router R-IP a través de su red local, encapsulado en una trama: **A-MAC** → **R-MAC** (**entrega indirecta**)
 - El Router se encargará de extraerlo y encaminarlo hasta su destino, haciendo un nuevo forwarding

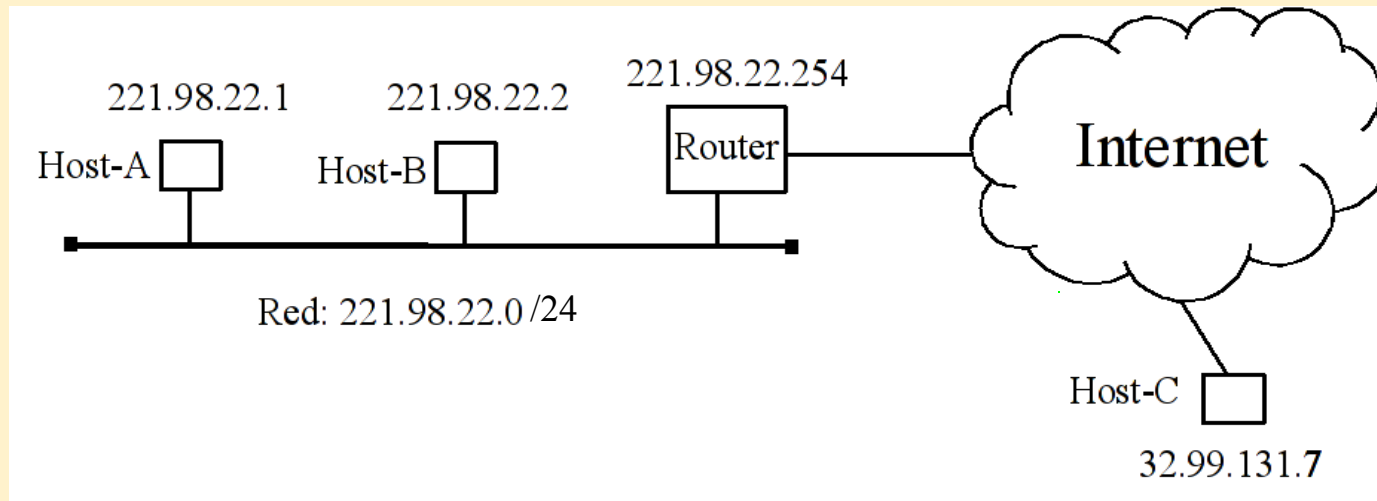
Tabla rutas en A:

Red Destino:	Por:
Red 1	A-IP (yo)
Default (resto)	R-IP



El protocolo IP: Máscaras de red

Ejemplo:



- Tabla de encaminamiento del Host-A, con formato real:

Destino	Por... (router)	Máscara	Flags	Interfaz de red
Destination	Gateway	Genmask	Flags	Iface
221.98.22.0	0.0.0.0	255.255.255.0	U	eth0
0.0.0.0	221.98.22.254	0.0.0.0	UG	eth0

(Destino = "0.0.0.0" representa resto de redes por defecto)

El protocolo IP: Máscaras de red

Ejemplo: (cont.)

- Para saber cómo tiene que tratar el paquete, el Host-A:
 - Consulta la tabla de encaminamiento y aplica, una a una, las máscaras de red (“Genmask”) a la dirección destino → Convierte la dir. del host destino en una dir. de red
 - Si la dirección de red resultante coincide con la dirección “Destination” de la tabla de rutas, se entrega el paquete al router indicado (“Gateway”)
 - Si ese gateway es 0.0.0.0, el destino está en la propia red
 - Si no hay ninguna coincidencia, no se puede enviar el paquete (destination unreachable)
 - Si hay entrada por defecto, coincide para todas las demás redes

Destination	Gateway	Genmask	Flags	Iface
221.98.22.0	0.0.0.0	255.255.255.0	U	eth0
0.0.0.0	221.98.22.254	0.0.0.0	UG	eth0

El protocolo IP: Máscaras de red

Ejemplo: (cont.)

- Para enviar paquete Host-A → Host-B
 - Coincide la combinación Genmask/Destination de la primera entrada de la tabla de encaminamiento

```
IP destino:  221.98.22.2   = 11011101 . 01100010 . 00010110 . 00000010
Máscara:      255.255.255.0 = 11111111 . 11111111 . 11111111 . 00000000
Red destino: 221.98.22.0   = 11011101 . 01100010 . 00010110 . 00000000
```

- El Gateway asociado a la red destino 221.98.22.0 es 0.0.0.0 (“yo”)
⇒ El destino está en la propia red (A hará entrega directa a B)

- Para enviar paquete Host-A → Host-C
 - Coincide la combinación Genmask/Destination de la segunda entrada de la tabla de encaminamiento (default router o router predeterminado)

```
IP destino:  32.99.131.7 = 00100000 . 01100011 . 10000011 . 00000111
Máscara:      0.0.0.0    = 00000000 . 00000000 . 00000000 . 00000000
Red destino:  0.0.0.0    = 00000000 . 00000000 . 00000000 . 00000000
```

- El Gateway asociado a la red destino (0.0.0.0) es 221.98.22.254
⇒ El paquete se envía a través de este router (A hace entrega indirecta a R)

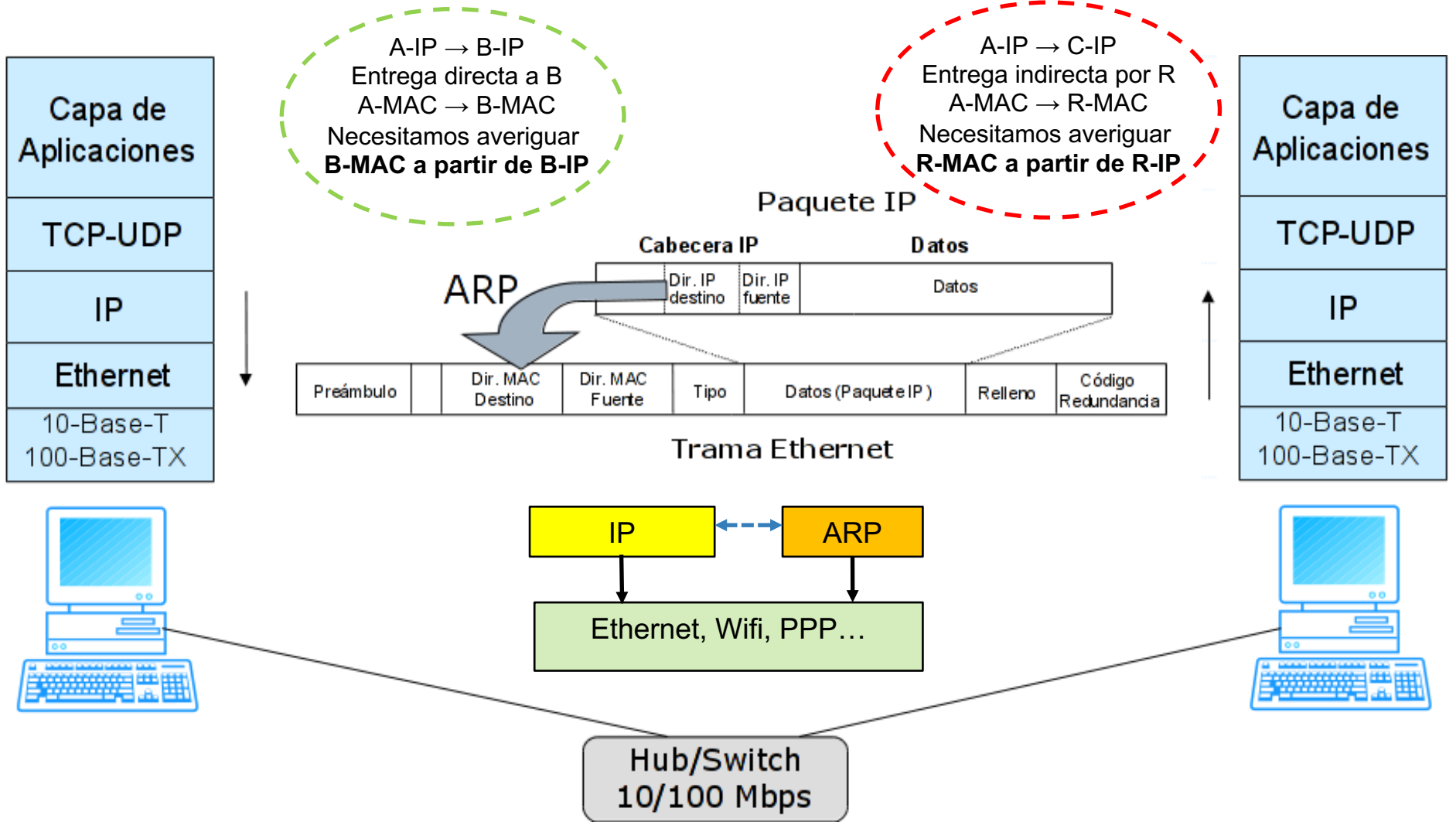
Contenidos

1. Repaso de conceptos
2. Protocolo IP: formato del datagrama y fragmentación
3. Protocolo IP: direcciones y máscaras
- 4. Protocolo ARP**
5. Subredes, superredes y CIDR
6. Protocolo ICMP
7. Encaminamiento (routing)

Protocolo de traducción de direcciones: ARP

ARP: Address Resolution Protocol

- Traducción: **Dirección IP → Dirección MAC** (RARP: Reverse ARP)



Protocolo de traducción de direcciones: ARP

La tabla ARP

- Mantiene las direcciones IP de las últimas máquinas con las que nos hemos comunicado y las direcciones MAC asociadas
- Ejemplo de tabla ARP en Linux:

```
# arp -an
? (147.96.80.1) at 0:0:c:9f:f0:50 [ether] on eth0
? (147.96.80.11) at 54:a0:50:7b:f5:8f [ether] on eth0
? (147.96.80.255) at ff:ff:ff:ff:ff:ff [ether] on eth0
? (147.96.80.10) at (incomplete) [ether] on eth0
```

Funcionamiento de ARP (Host-A quiere enviar un datagrama a Host-B)

1. Host-A consulta su **tabla ARP** para ver si la dirección MAC de Host-B está contenida en dicha tabla
2. Si la dirección MAC de Host-B no está en la tabla entonces entra en acción el

Protocolo ARP:

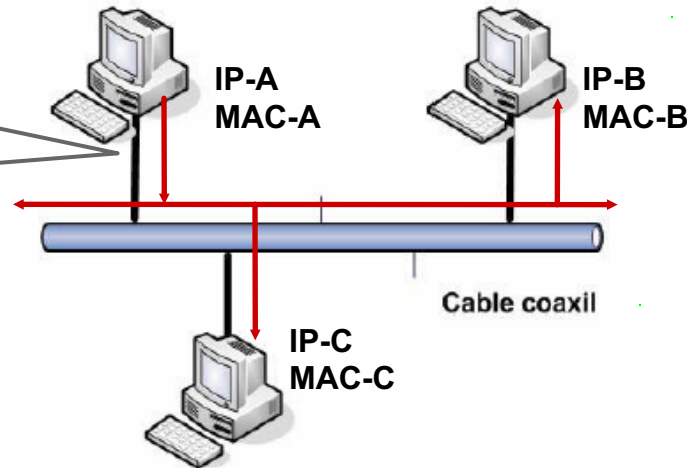
- Host-A envía un mensaje **broadcast** preguntando por la dirección MAC de Host-B → Mensaje **ARP Request**
- Host-B responde a Host-A informándole de su dirección MAC → Mensaje **ARP Response**. Se introduce IP-B/MAC-B en la tabla ARP.

Protocolo de traducción de direcciones: ARP

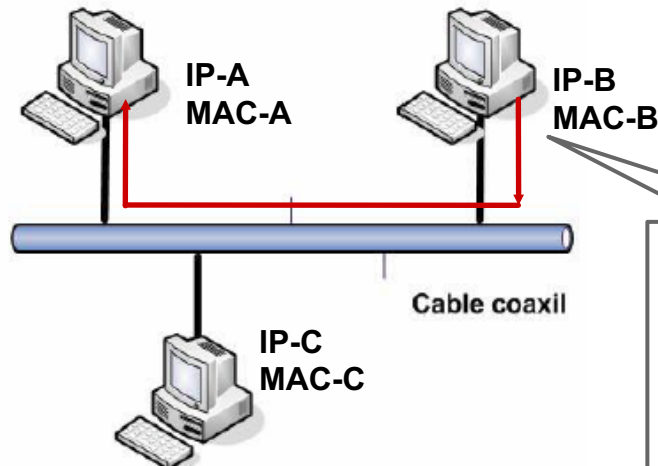
Funcionamiento de ARP (Host-A quiere enviar un datagrama al Host-B)

- Pregunta ARP

**ARP Request
(BROADCAST)**
Conozco IP-B
¿Cuál es su MAC-B?



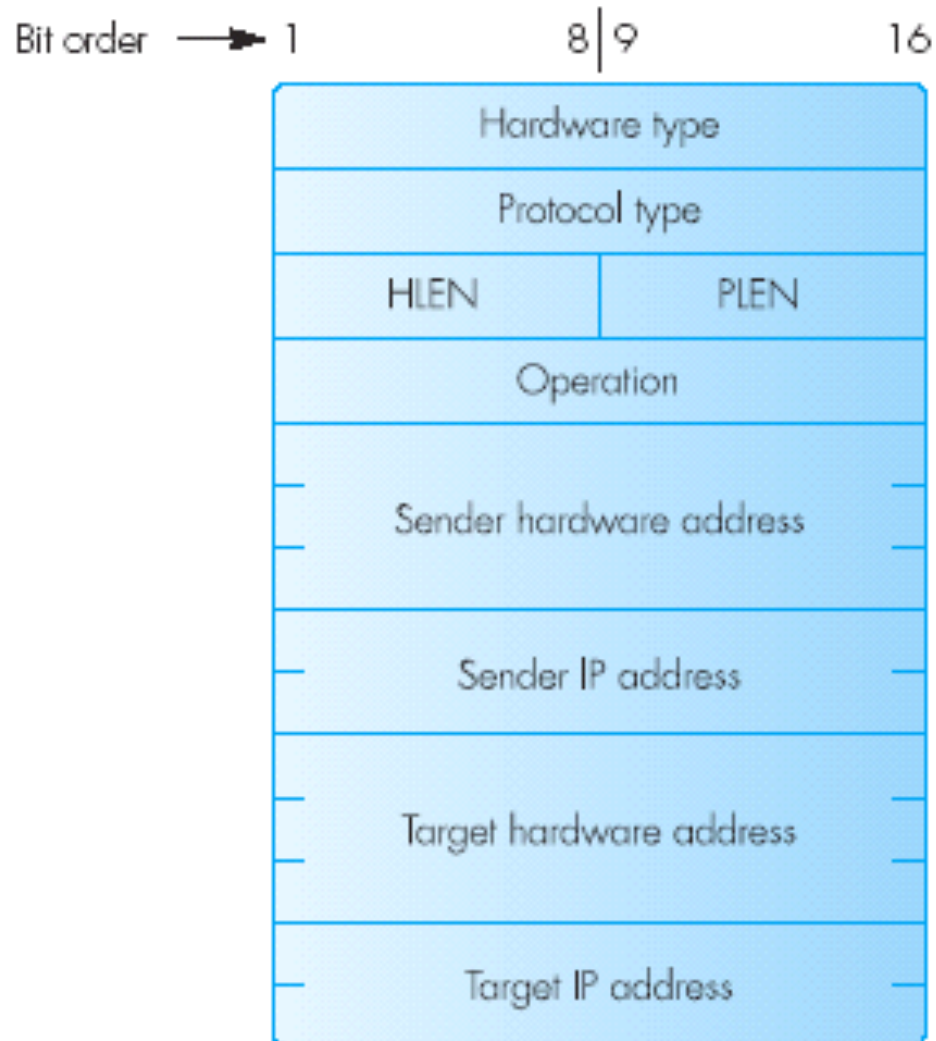
- Respuesta ARP



ARP Response
Soy IP-B y me
corresponde
esta MAC-B

Protocolo de traducción de direcciones: ARP

Formato del paquete ARP



HLEN = Hardware address length

PLEN = IP address length

Operation = 1 ARP request

= 2 ARP response

= 3 RARP request

= 4 RARP response

Protocolo de traducción de direcciones: ARP

Ejemplo de paquete ARP: Pregunta

ETHER: ----- Ether Header -----

ETHER:

ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)

ETHER: Source = 08:00:20:88:c9:ee

ETHER: Ethertype = 0806 (ARP)

ETHER:

ARP: ----- ARP/RARP Frame -----

ARP:

ARP: Hardware type = 1

ARP: Protocol type = 0800 (IP)

ARP: Length of hardware address = 6 bytes

ARP: Length of protocol address = 4 bytes

ARP: Opcode 1 (ARP Request)

ARP: Sender's hardware address = 08:00:20:88:c9:ee

ARP: Sender's protocol address = 200.96.21.31

ARP: Target hardware address = 00:00:00:00:00:00 (unknown)

ARP: Target protocol address = 200.96.21.120

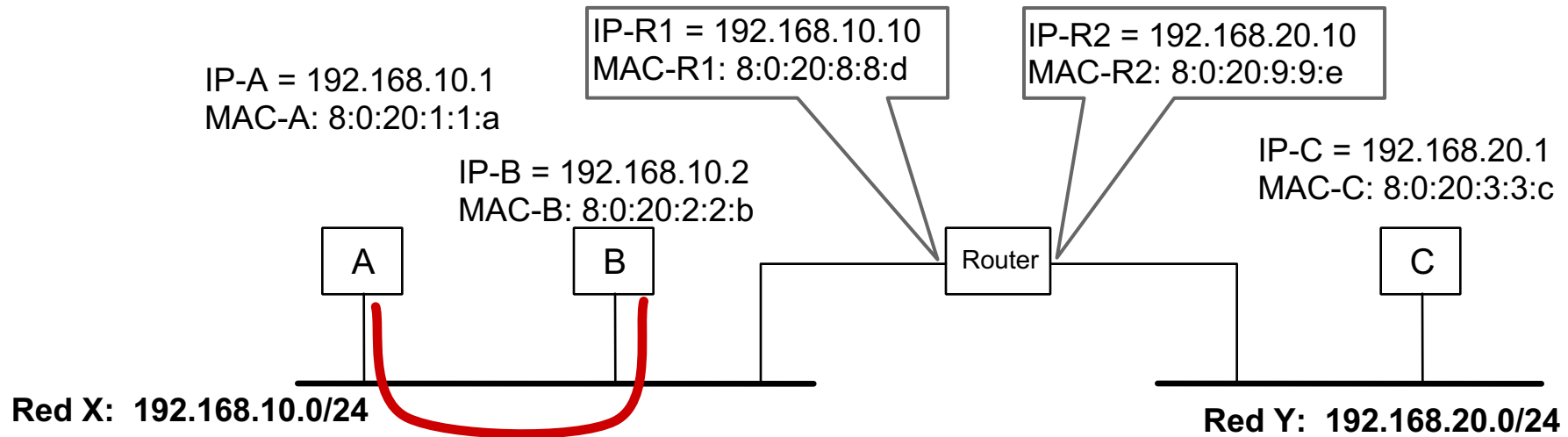
Protocolo de traducción de direcciones: ARP

Ejemplo de paquete ARP: Respuesta

```
ETHER:  ----- Ether Header -----  
ETHER:  
ETHER:  Destination = 08:00:20:88:c9:ee  
ETHER:  Source      = 00:03:ba:0d:e7:0e  
ETHER:  Ethertype = 0806 (ARP)  
ETHER:  
ARP:  ----- ARP/RARP Frame -----  
ARP:  
ARP:  Hardware type = 1  
ARP:  Protocol type = 0800 (IP)  
ARP:  Length of hardware address = 6 bytes  
ARP:  Length of protocol address = 4 bytes  
ARP:  Opcode 2 (ARP Reply)  
ARP:  Sender's hardware address = 00:03:ba:0d:e7:0e  
ARP:  Sender's protocol address = 200.96.21.120  
ARP:  Target hardware address = 08:00:20:88:c9:ee  
ARP:  Target protocol address = 200.96.21.31
```

Protocolo de traducción de direcciones: ARP

Procedimiento de forwarding completo con ARP (Hosts en la misma red)



Máscara: 255.255.255.0

Red Destino:	Por:
Red X	0.0.0.0
Default (resto)	R-IP

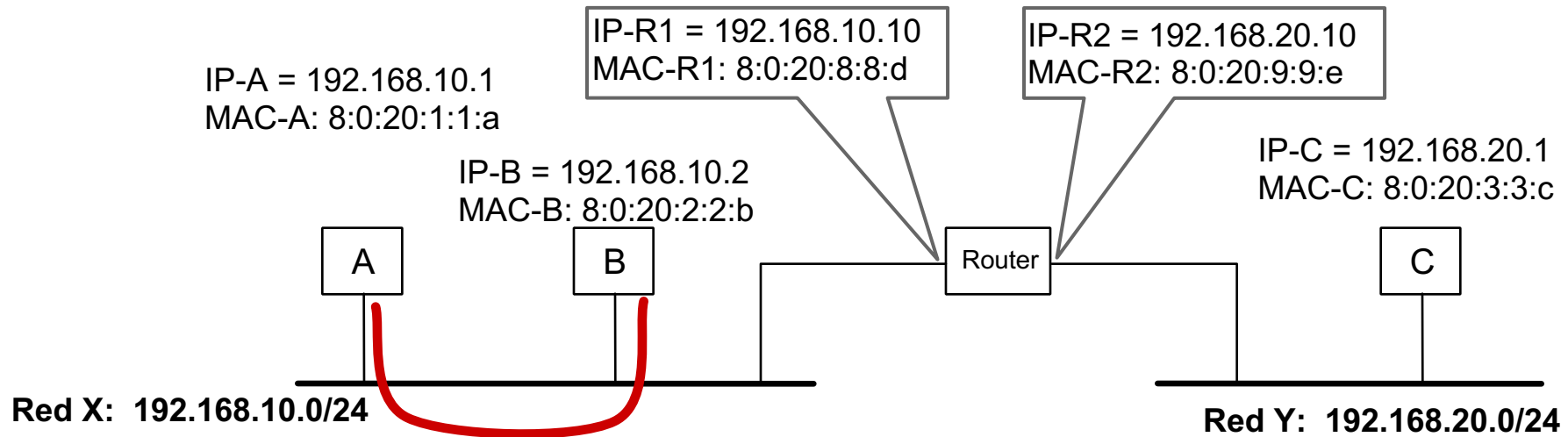
La estación A aplica el siguiente procedimiento:

- Aplica la máscara de red a la dirección IP destino (IP-B)
- Consulta su tabla de rutas → 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 B, a través de la Red X, dentro de una trama dirigida a MAC-B:

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

Protocolo de traducción de direcciones: ARP

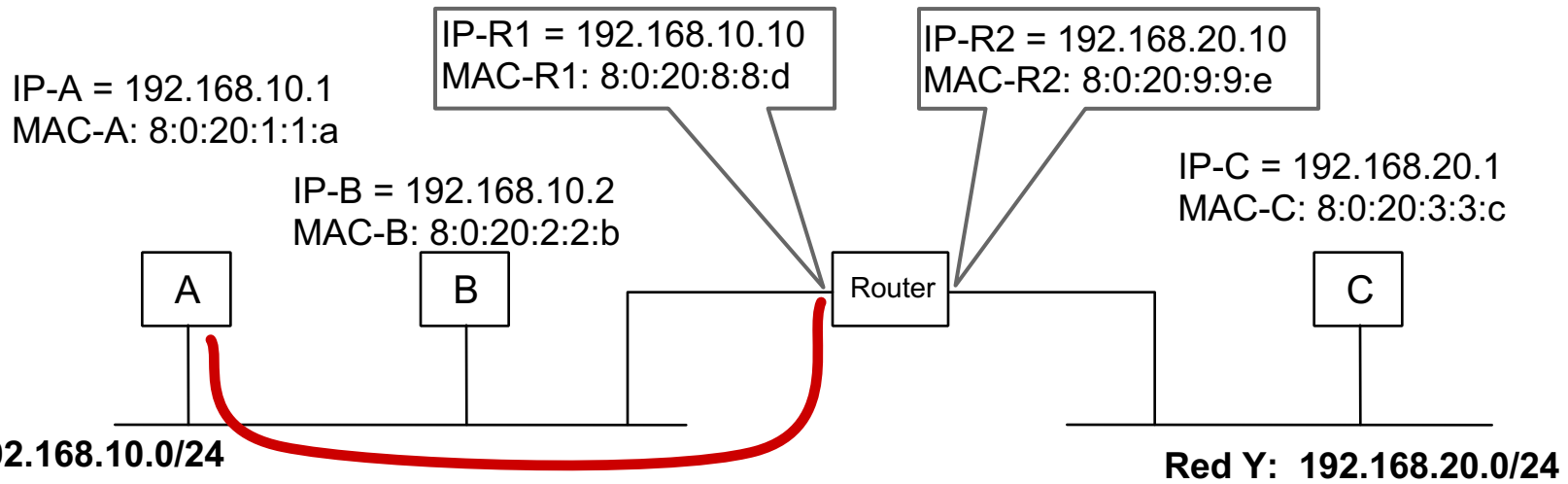
Procedimiento de forwarding completo con ARP (Hosts en la misma red)



Nº Trama	Dir MAC Origen	Dir MAC Destino	Tipo	Campos paquete ARP o IP		Contenido
1	MAC-A	ff:ff:ff:ff:ff:ff:ff:ff	ARP (0806h)	MAC-A, IP-A, - , IP-B		ARP Request
2	MAC-B	MAC-A	ARP (0806h)	MAC-B, IP-B, MAC-A, IP-A		ARP Response
3	MAC-A	MAC-B	IP (0800h)	Dir IP Origen: A-IP	Dir IP Destino: B-IP	Datos del datagrama

Protocolo de traducción de direcciones: ARP

Procedimiento de forwarding completo con ARP (Hosts en distinta red, sólo Red X)



Máscara: 255.255.255.0

La estación A aplica el siguiente procedimiento:

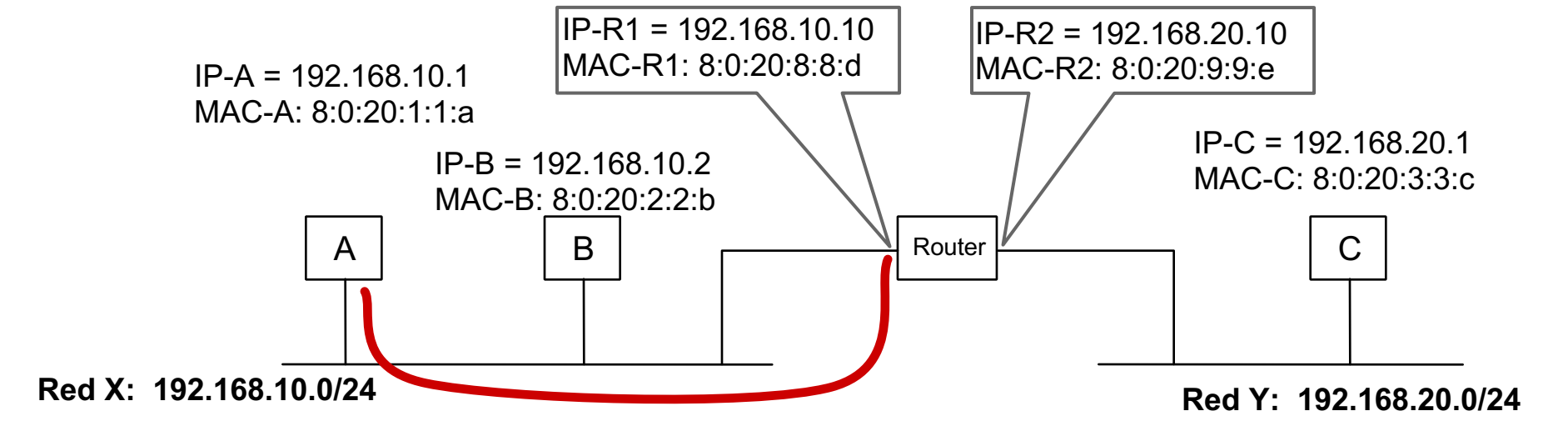
- Aplica la máscara de red a la dirección IP destino (IP-C)
- Consulta la tabla de rutas → destino en otra red (Red Y) por R-IP1
- Utiliza el protocolo ARP para averiguar la MAC del default router (MAC-R1)
- Entrega el paquete IP al router R, a través de la Red X dentro de una trama dirigida a MAC-R1:

Red Destino:	Por:
Red X	0.0.0.0
Default (resto)	IP-R1

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

Protocolo de traducción de direcciones: ARP

Procedimiento de forwarding completo con ARP (Hosts en distinta red, solo Red X)



Nº Trama	Dir MAC Origen	Dir MAC Destino	Tipo	Campos paquete ARP o IP		Contenido
1	MAC-A	ff:ff:ff:ff:ff:ff:ff:ff	ARP (0806h)	MAC-A, IP-A, - , IP-R1		ARP Request
2	MAC-R1	MAC-A	ARP (0806h)	MAC-R1, IP-R1, MAC-A, IP-A		ARP Response
3	MAC-A	MAC-R1	IP (0800h)	Dir IP Origen: A-IP	Dir IP Destino: C-IP	Datos del datagrama

Contenidos

1. Repaso de conceptos
2. Protocolo IP: formato del datagrama y fragmentación
3. Protocolo IP: direcciones y máscaras
4. Protocolo ARP
- 5. Subredes, superredes y CIDR**
6. Protocolo ICMP
7. Encaminamiento (routing)

Organización en redes: Subredes

Ventajas de las subredes

- Permiten aislar el tráfico entre las distintas partes de la red (subredes)
- Se reduce el tráfico global
- Permite limitar y proteger el acceso a las distintas subredes
- Permite organizar la red en áreas o departamentos
- Se asigna a cada departamento un subconjunto de direcciones IP

Se reparten los **n bits** del campo host original entre **s bits** (número de subredes) y **$n-s$ bits** (tamaño de cada subred):



- El reparto de bits lo decide el administrador
- Las subredes sólo existen dentro de la red: desde fuera, los routers ven la red completa
- La comunicación entre subredes se realiza mediante routers internos
- Se configuran en las tablas de rutas igual que las redes.
- Se utiliza una nueva **máscara** que incluye ahora los bits de Red + Subred
- Tenemos **nombre de la subred**, **dirección de broadcast**, rango de nodos...

Organización en redes: Subredes

Ejemplo: Supongamos la red de la clase B: 150.23.0.0/16

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

IP: 150. 23.5.7 = $\overbrace{10010110.00010111}^{\text{Red}}.\overbrace{00000101.00000111}^{\text{Host}}$

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 al host ($2^8 = 256 - 2 = 254$ hosts)
- Por tanto la máscara de subred adecuada es la siguiente (/24):

IP: 150. 23. 5. 7 = $\overbrace{10010110.00010111}^{\text{Red}}.\overbrace{00000101}^{\text{Subred}}.\overbrace{00000111}^{\text{Host}}$

Máscara: 255.255.255.0 = 11111111.11111111.11111111.00000000

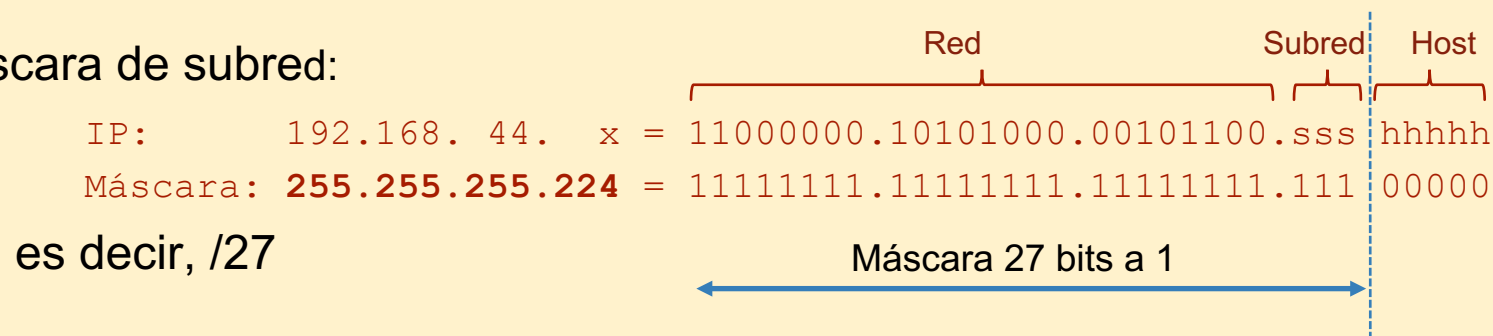
- Nos queda la siguiente organización:
 - Subred 0: 150.23.0.0/24 (Dpto. de administración)
 - Subred 1: 150.23.1.0/24 (Dpto. de RRHH)
 - ...
 - Subred 255: 150.23.255.0/24 (Dpto. comercial)

Organización en redes: Subredes

Ejemplo: Supongamos la red de la clase C: 192.168.44.0/24

- Queremos dividir la red en 8 subredes
 - 3 bits para identificar la subred ($2^3 = 8$ subredes)
 - 5 bits para identificar el host ($2^5 = 32$ dir. por subred, 30 hosts cada una)

- Máscara de subred:

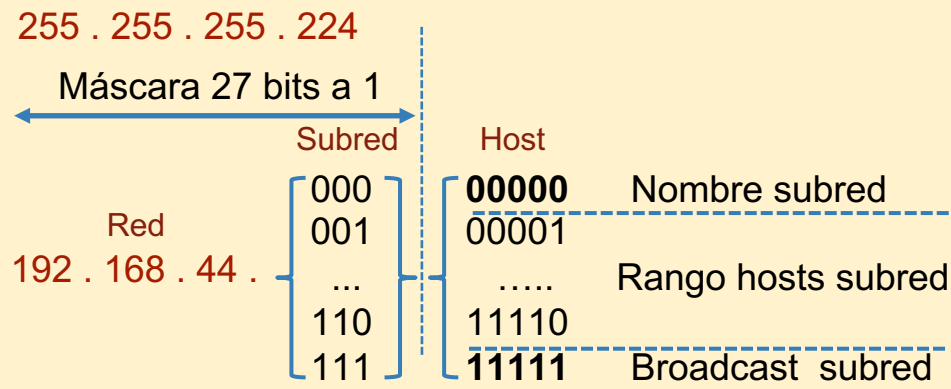


- La máscara de subred, aplicada a una dirección de destino, nos da la subred a la que pertenece.
- Indicamos las características completas de cada subred (nombre, rango de nodos y dirección de broadcast) en forma de tabla en la siguiente diapositiva

Organización en redes: Subredes

Ejemplo (cont)

- Organización resultante:

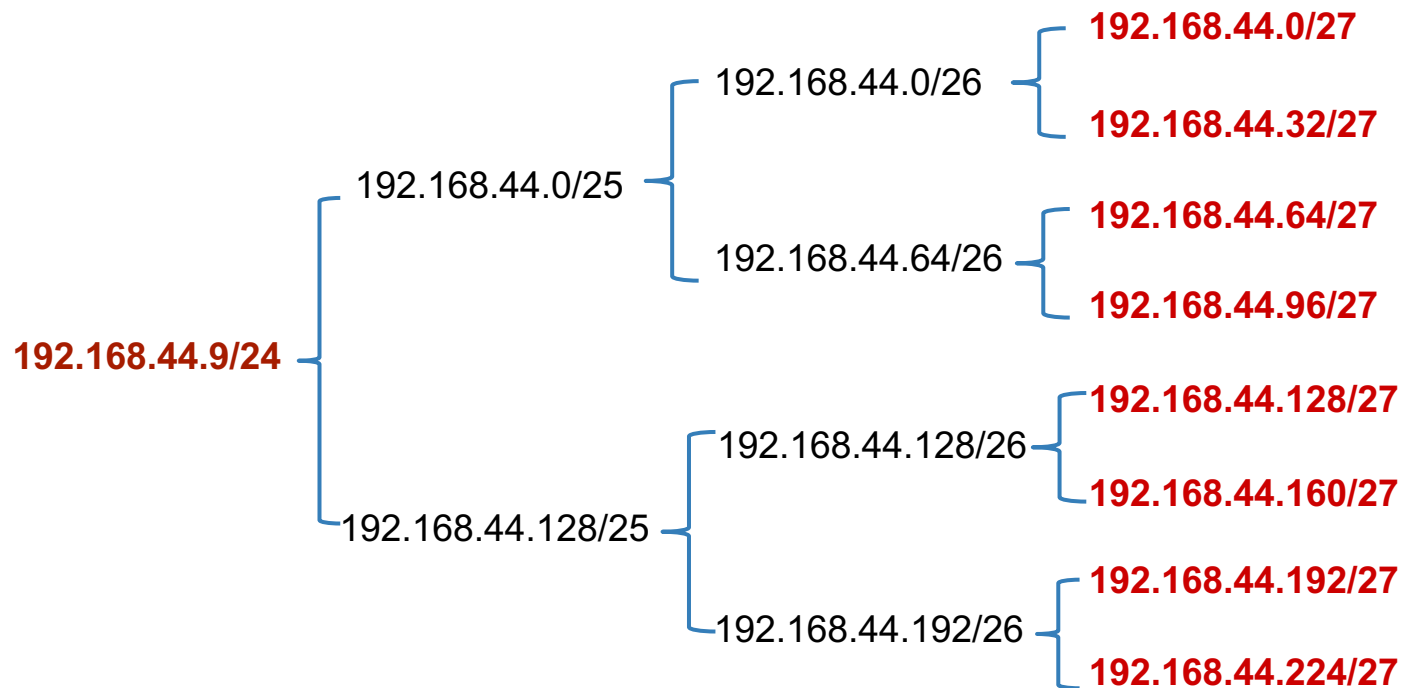


Nombre subred	Rango hosts	Dir. broadcast
192.168.44.0/27	192.168.44.1 al 192.168.44.30	192.168.44.31
192.168.44.32/27	192.168.44.33 al 192.168.44.62	192.168.44.63
192.168.44.64/27	192.168.44.65 al 192.168.44.94	192.168.44.95
192.168.44.96/27	192.168.44.97 al 192.168.44.126	192.168.44.127
192.168.44.128/27	192.168.44.129 al 192.168.44.158	192.168.44.159
192.168.44.160/27	192.168.44.161 al 192.168.44.190	192.168.44.191
192.168.44.192/27	192.168.44.193 al 192.168.44.222	192.168.44.223
192.168.44.224/27	192.168.44.225 al 192.168.44.254	192.168.44.255

Organización en redes: Subredes

Ejemplo (cont)

- Podemos ver el espacio de direcciones como un árbol binario
- La máscara **255 . 255 . 255 . 224**, profundizando en tres bits a partir de la dirección de red original en todas las ramas del árbol, nos lleva hasta las ocho subredes en las hojas del árbol:



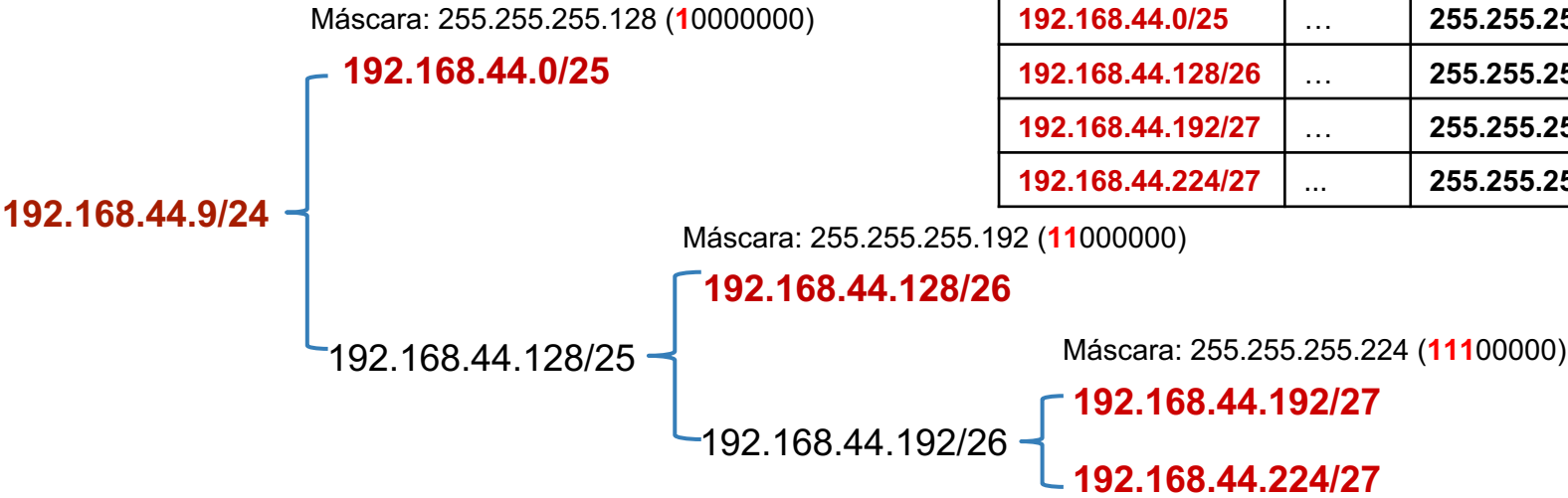
Organización en redes: Subredes

VLSM (*Variable Length Subnet Mask*): Máscaras de subred de longitud variable

- Muchas organizaciones utilizan una organización de direcciones de red con subredes de tamaños distintos.
- VLSM permite profundizar en cada rama del árbol de forma distinta, sólo hasta la subred del tamaño deseado.
- Para ello utiliza una máscara de longitud diferente para cada subred.
- Es preciso indicar en la tabla de rutas de los routers de la organización la máscara a usar con cada destino (subred)

Ejemplo: Dividimos la red del ejemplo anterior **192.168.44.9/24** (256 direcciones) en una subred con la mitad de la capacidad (128), otra de un cuarto (64), y otras dos de un octavo (32)

Dirección subred	Por...	Máscara
192.168.44.0/25	...	255.255.255.128
192.168.44.128/26	...	255.255.255.192
192.168.44.192/27	...	255.255.255.224
192.168.44.224/27	...	255.255.255.224



Organización en redes: Subredes

Ejemplo: Una red de clase C (200.21.32.0/24) quiere dividirse en cinco subredes:

Subred 1: 50 hosts

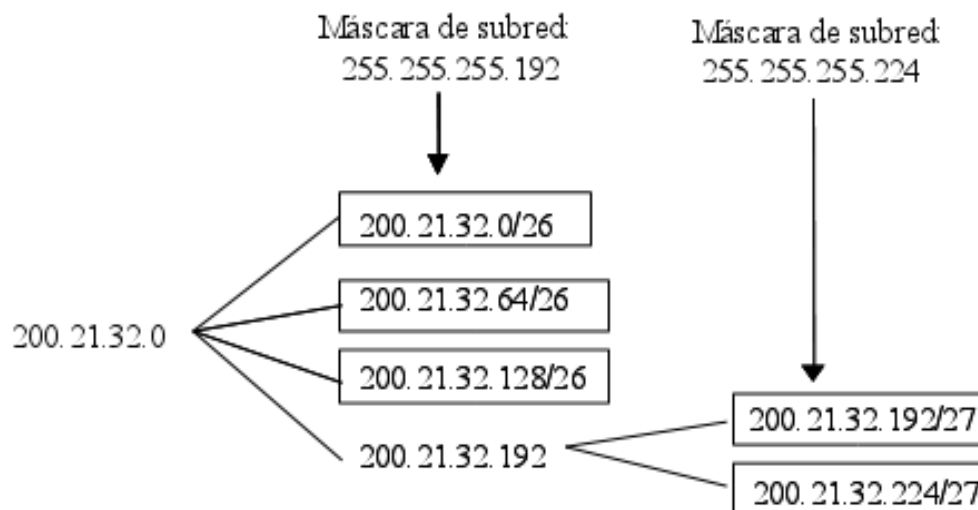
Subred 4: 30 hosts

Subred 2: 50 hosts

Subred 5: 30 hosts

Subred 3: 50 hosts

- Dividir la red en 4 (2^2) subredes de 62 (2^6-2) hosts cada una
 - Máscara = 11111111 . 11111111 . 11111111 . 11000000 = **255.255.255.192**
- Subdividir una de las redes en dos subredes de 30 (2^5-2) hosts cada una
 - Máscara = 11111111 . 11111111 . 11111111 . 11100000 = **255.255.255.224**

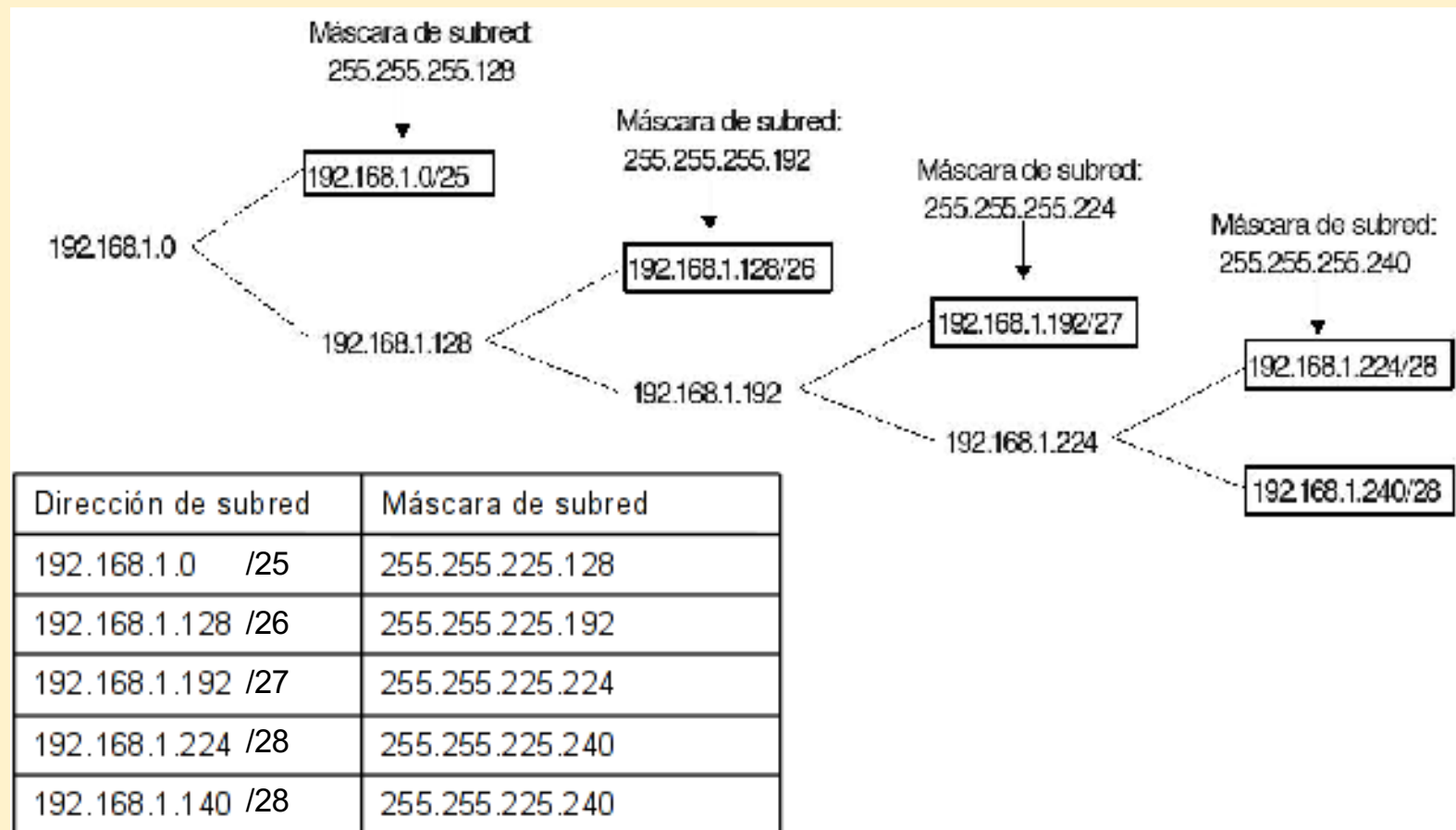


Dirección de subred	Máscara de subred
200.21.32.0 /26	255.255.255.192
200.21.32.64 /26	255.255.255.192
200.21.32.128 /26	255.255.255.192
200.21.32.192 /27	255.255.255.224
200.21.32.224 /27	255.255.255.224

Organización en redes: Subredes

Ejemplo: Una red de clase C (192.168.1.0/24) quiere dividirse en cinco subredes:

- Una subred de 126 hosts
- Una subred de 62 hosts
- Una subred de 30 hosts
- Dos subredes de 14 hosts cada una



Organización en redes: Superredes

El problema del agotamiento de direcciones IP

- Durante los años 80 y 90 la mayoría de direcciones solicitadas eran de clase B
 - Al ritmo de crecimiento de Internet (el nº de redes se duplicaba cada año) las direcciones de clase B se hubieran agotado en el año 1994
- En 1990 se estableció una política estricta de asignación de redes de clase A y B
 - La mitad del espacio de **direcciones de clase A** (números 64 a 127) se reservan para un uso futuro, que permita la transición a un nuevo esquema de direccionamiento (IPv6)
 - El resto de direcciones de clase A están agotadas
 - Sólo en casos particulares, y estudiados de forma individual, se podría asignar una dirección de clase A reservada
 - Las **direcciones de clase B** sólo se asignan a organizaciones que puedan demostrar la necesidad real de este tipo de dirección. Estas organizaciones deben cumplir los siguientes requisitos mínimos:
 - Tener al menos 4096 hosts
 - Tener al menos 32 subredes distintas
 - A las organizaciones que no cumplen estos requisitos se les asignan varias direcciones de clase **C consecutivas**

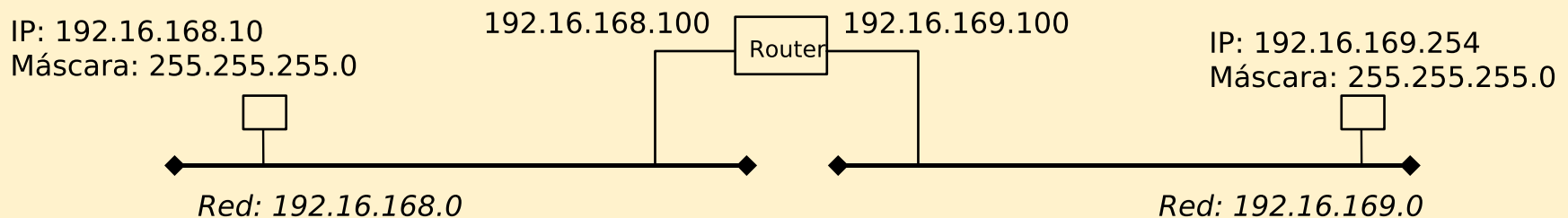
Organización en redes: Superredes

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:

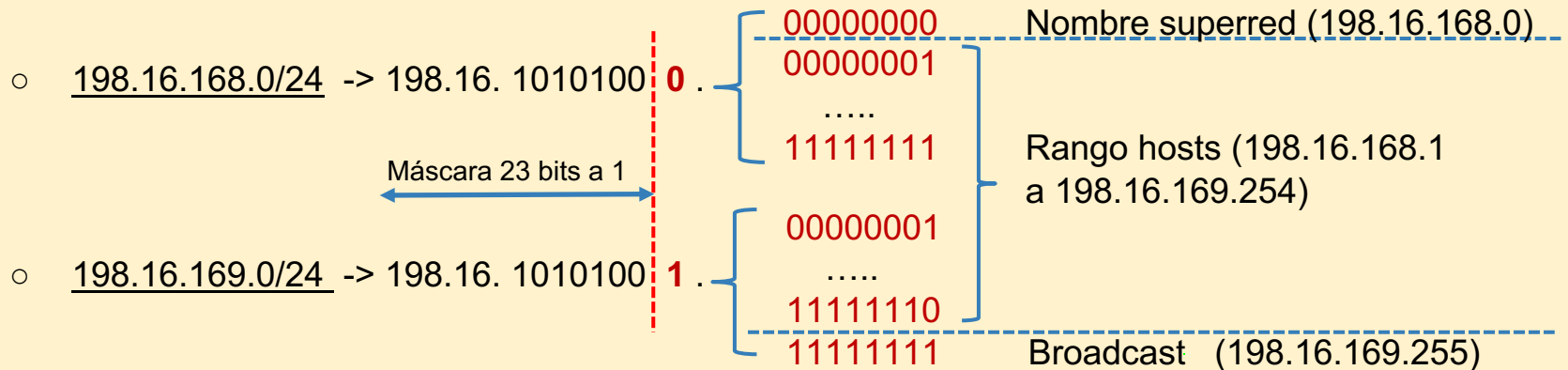
- 192.16.168.0
- 192.16.169.0
- Si las máquinas se configuran con la máscara de clase C (255.255.255.0)
 - Los dos conjuntos de direcciones quedarían lógicamente aislados
 - Sería necesario utilizar un router para interconectar ambas redes
 - En Internet, la ruta a esta red se tiene que desglosar en dos rutas separadas, una para cada red



Organización en redes: Superredes

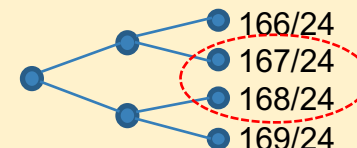
Ejemplo:

- Combinamos las dos redes de clase C:



- Necesitamos usar como máscara /23 (255.255.11111110.0 - > **255.255.254.0**)
 - La superred resultante sería **198.16.168.0 / 23**
 - Se puede incluir como destino en la tabla de rutas con esta máscara
 - Ahora es **una única red de 512 direcciones consecutivas**, no necesitan router para comunicarse entre sí los nodos 198.16.168.1 y 198.16.169.254.
- OJO: No puede fusionarse la 198.16.168.0 con la 198.16.167.0 aunque sean consecutivas, no forman parte de la misma rama del árbol binario y la máscara no da el mismo prefijo de superred.

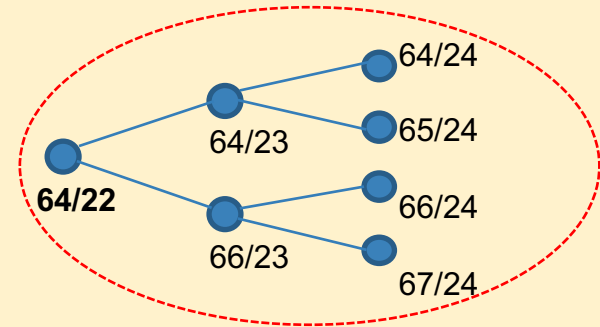
- Diagram illustrating why 198.16.167.0 and 198.16.168.0 cannot be combined:
- 198.16.167.0 → 198.16. 1010**011** **1** . xxxxxxxx
 - 198.16.168.0 → 198.16. 1010**100** **0** . xxxxxxxx
- A red dashed line separates the two binary representations at the 23rd bit position. A large blue 'X' is drawn over the first two lines, indicating that they cannot be combined into a single supernet.



Organización en redes: Superredes

Ejemplo: Una empresa dispone de 1000 hosts conectados a una misma red local. Esta empresa solicita cuatro direcciones de clase C consecutivas:

- 200.45.64.0
- 200.45.65.0
- 200.45.66.0
- 200.45.67.0



- Estas cuatro redes se une en una única superred de la siguiente forma:

200.45.64.0 =	11001000	00101101	010000	00	00000000	
200.45.65.0 =	11001000	00101101	010000	01	00000000	
200.45.66.0 =	11001000	00101101	010000	10	00000000	
200.45.67.0 =	11001000	00101101	010000	11	00000000	
Máscara =	11111111	11111111	111111	00	00000000	= 255.255.252.0
Dir. de Red =	11001000	00101101	010000	00	00000000	= 200.45.64.0/22
	ID de red			ID de Host		

Organización en redes: CIDR

CIDR (Classless Interdomain Routing): Encaminamiento inter-dominio sin clases

- Respuesta a los problemas que estaba teniendo Internet de:
 - Agotamiento de direcciones
 - Crecimiento de las tablas de ruta
- CIDR es el resultado de unir VLSM y Supernetting, y extenderlo a todo Internet
 - Elimina el concepto de clases (A, B y C)
- Tablas de rutas en CIDR
 - Las entradas en las tablas de rutas de los routers deben tener no sólo la dirección de la red destino, sino también su máscara
- Ventajas de CIDR:
 - Asignar redes ajustadas al tamaño necesario
 - Se asigna un identificador de red y una máscara del tamaño deseado
 - Reducir el número de entradas en las tablas de rutas “resumiendo” varias entradas en una sola (agregado de direcciones):
 - Vistas desde “lejos”, un grupo de redes próximas se puede agrupar en una única entrada de la tabla de rutas.

Organización en redes: CIDR

Ejemplo: Tablas de rutas y organización con CIDR

Tabla de R1

Destino	Router	Enlace
200.25.16.0/20	R2	E1

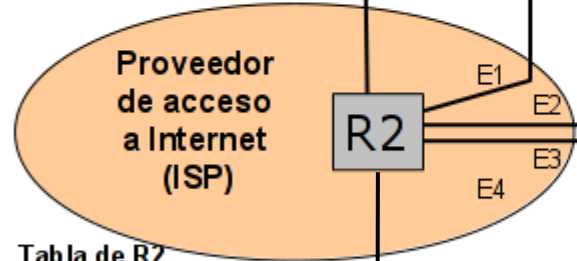
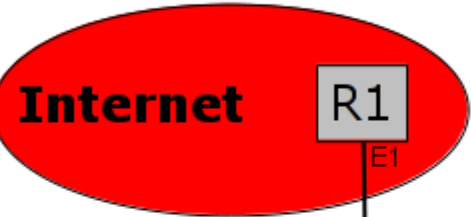


Tabla de R2

Destino	Router	Enlace
200.25.16.0/21	R3	E1
200.25.24.0/22	R4	E2
200.25.28.0/23	R5	E3
200.25.30.0/23	R6	E4

Tabla de R3

Destino	Router	Enlace
200.25.16.0/24	--	E1
200.25.17.0/24	--	E2
200.25.18.0/24	--	E3
200.25.19.0/24	--	E4
200.25.20.0/24	--	E5
200.25.21.0/24	--	E6
200.25.22.0/24	--	E7
200.25.23.0/24	--	E8

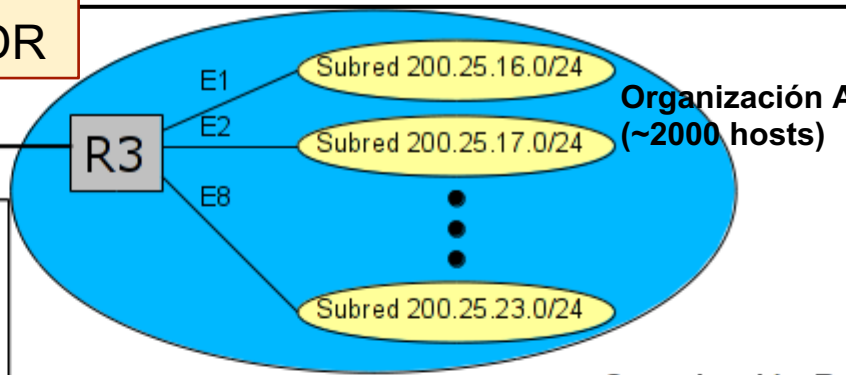


Tabla de R4

Destino	Router	Enlace
200.25.24.0/24	--	E1
200.25.25.0/24	--	E2
200.25.26.0/24	--	E3
200.25.27.0/24	--	E4

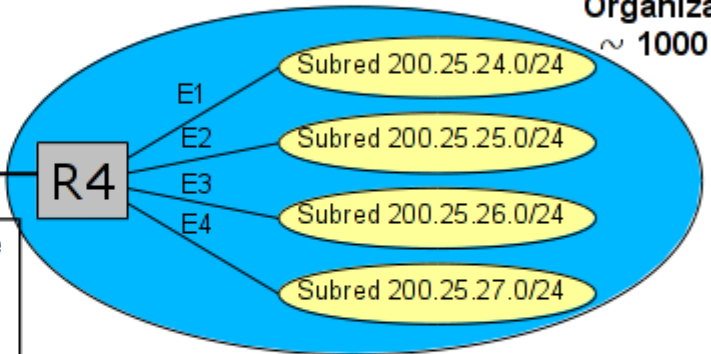


Tabla de R5

Destino	Router	Enlace
200.25.28.0/24	--	E1
200.25.29.0/24	--	E2

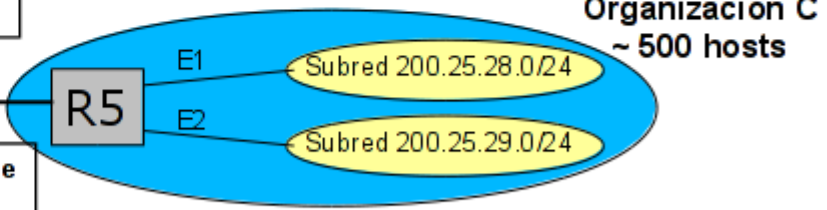
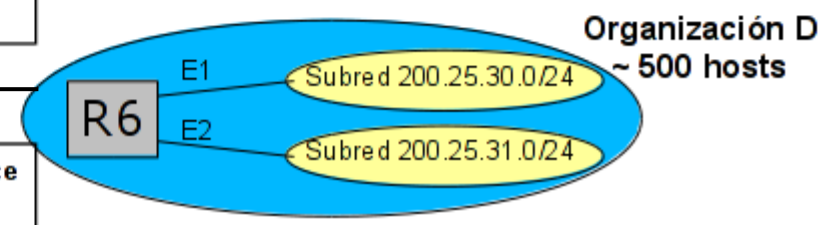


Tabla de R6

Destino	Router	Enlace
200.25.30.0/24	--	E1
200.25.31.0/24	--	E2



Contenidos

1. Repaso de conceptos
2. Protocolo IP: formato del datagrama y fragmentación
3. Protocolo IP: direcciones y máscaras
4. Protocolo ARP
5. Subredes, superredes y CIDR
- 6. Protocolo ICMP**
7. Encaminamiento (routing)

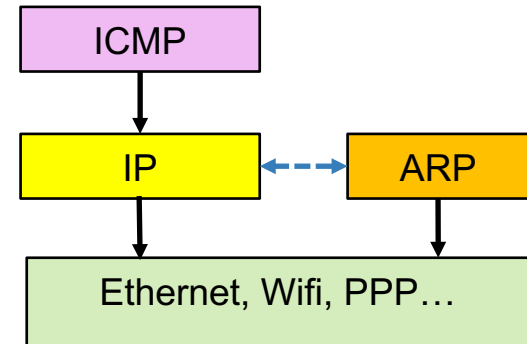
Protocolo ICMP

ICMP (Internet Control Message Protocol): Protocolo de mensajes de control de Internet

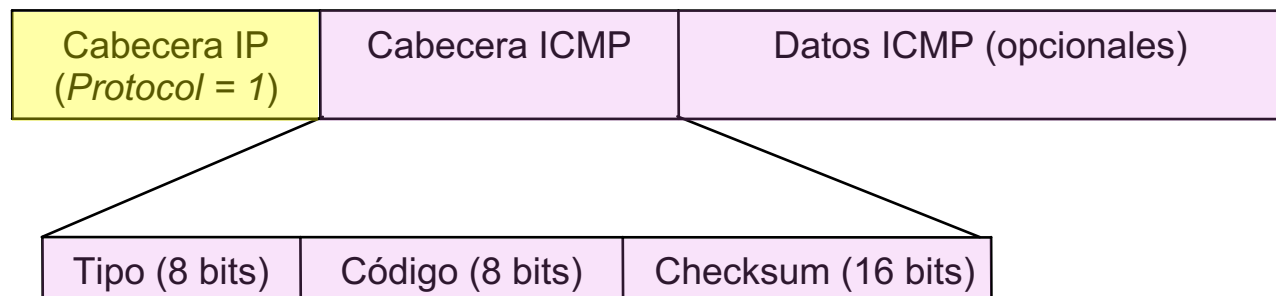
- Es un protocolo para el intercambio de mensajes de control en la red
- Los mensajes ICMP se pueden clasificar en dos tipos:
 - **Mensajes de error**
 - Permiten informar de situaciones de error en la red
 - Ejemplos: destino inalcanzable, tiempo excedido, problema de parámetro, etc.
 - **Mensajes informativos**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

Protocolo ICMP: Formato del mensaje

- Los mensajes ICMP se transmiten dentro de **paquetes IP**
 - ICMP se identifica en el datagrama IP con Protocolo=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 cuyo 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/Reply
 - **Tipos:** 8 (Echo Request) y 0 (Echo Reply)
 - **Código:** 0 (no hay subtipos)
 - **Identificador:** Permite establecer la correspondencia entre solicitud y respuesta, ya que ambas tienen el mismo identificador
 - **Secuencia:** También se utiliza para establecer la correspondencia entre solicitud y respuesta, cuando se envían varias solicitudes consecutivas 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`)

Tipo (0/8)	Código (0)	Checksum
Identificador		Nº de secuencia
Datos		

- > La orden `ping` funciona de forma un poco distinta en cada OS, para enviar un único paquete Echo Request usar: `ping dir_IP_destino -c 1`

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

Tipo (3)	Código	Checksum
No usado (cero)		
Cabecera IP del datagrama original + 64 primeros bits de datos		

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

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

3: Port unreachable: Puerto UDP cerrado

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

- Permite implementar el mecanismo de “Path MTU Discovery”

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

Protocolo ICMP: Destination Unreachable

Mecanismo “Path MTU Discovery” (PMTUD)

- Se utiliza para evitar la fragmentación de los paquetes IP
 - Para ello, el host origen debe ajustar el tamaño de los paquetes a la “MTU del camino” (MTU mínima de todas las redes que debe atravesar)
- El mecanismo para descubrir la MTU del camino (PMTUD) es el siguiente
 - El host origen envía el paquete ajustándose a la MTU de su red local y con el bit DF activado.
 - Si el paquete debe atravesar una red con una MTU menor, el encaminador no puede fragmentarlo, al estar el bit DF activado por lo que descarta el datagrama y devuelve al emisor un mensaje ICMP de tipo 3 (destino inalcanzable), código 4 (fragmentación necesaria)
 - El host origen envía un nuevo paquete, que se ajusta a la MTU de dicha red.
 - El proceso se repite hasta que el paquete llega al destino

Protocolo ICMP: Time Exceeded

- Este paquete lo puede enviar un router intermedio o el host destinatario:
 - Lo envía un router al host origen cuando descarta el paquete por haber agotado su tiempo de vida (**TTL de tránsito**)
 - Lo envía el host destinatario en el caso de un paquete fragmentado, cuando no puede reensamblar por falta de algún fragmento y se agota el tiempo de espera para reensamblado (**TTL de reensamblado**)
- Orden `traceroute`
 - Usa de este tipo de mensajes para descubrir la ruta a un determinado destino
- **Formato del mensaje**
 - Tipo: 11
 - Código: 0 (agotado TTL de tránsito) o 1 (agotado TTL de reensamblado)

Tipo (11)	Código (0/1)	Checksum
No usado		
Cabecera IP del datagrama original + 64 primeros bits de datos		

Protocolo ICMP: Otros mensajes

ICMP Redirect

- Los mensajes de redirección los envía un router cuando un host no está eligiendo la ruta adecuada hacia un determinado destino
- El mensaje de redirección le indica al host cuál es el camino más adecuado para alcanzar dicho destino

ICMP Source Quench

- Se utilizan para notificar al emisor que debe reducir el ritmo de envío de paquetes
- Los puede enviar un router intermedio o el host destinatario, cuando no tienen capacidad para procesar los paquetes procedentes de un determinado emisor

ICMP Parameter Problem

- Indica que se ha encontrado algún tipo de problema durante el procesamiento de los parámetros de la cabecera IP
 - Valor inválido en la cabecera o checksum erróneo
 - Campo opción necesario, pero no presente

Contenidos

1. Repaso de conceptos
2. Protocolo IP: formato del datagrama y fragmentación
3. Protocolo IP: direcciones y máscaras
4. Protocolo ARP
5. Subredes, superredes y CIDR
6. Protocolo ICMP
7. Encaminamiento (routing)

Encaminamiento: Introducción

- En una red de conmutación de paquetes, el **encaminamiento o routing** consiste en encontrar un camino, desde el origen al destino, a través de nodos de conmutación o encaminadores (routers) intermedios
- En caso de que existan varios caminos alternativos, es necesario decidir cuál es el **mejor camino posible** → “camino más corto”
- El camino más corto se define según una métrica de encaminamiento:
 - **Número de saltos:** tiene en cuenta el número de routers y/o redes intermedias que tiene que atravesar el paquete para alcanzar el destino
 - **Distancia geográfica:** tiene en cuenta la distancia (en Km) que tiene que recorrer el paquete para alcanzar el destino
 - **Retardo promedio:** tiene en cuenta el retardo de las líneas. Dado que éste es proporcional a la distancia, esta métrica es similar a la anterior
 - **Ancho de banda:** tiene en cuenta la velocidad de transmisión de las líneas por las que tiene que circular el paquete
 - **Nivel de tráfico:** tiene en cuenta el nivel de uso de las líneas, para intentar utilizar aquellas líneas con menor nivel de saturación
 - **Función de varias métricas**

Encaminamiento: Técnicas generales

Encaminamiento local

- Estas técnicas no tienen en cuenta la topología de la red
- Las técnicas más comunes son:
 - Encaminamiento aleatorio
 - Encaminamiento aislado
 - Inundación

Encaminamiento estático (no adaptativo)

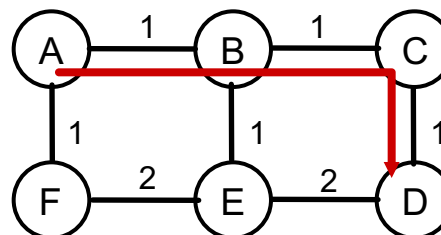
- Las decisiones de encaminamiento se basan en la topología de la red y en el uso de tablas de encaminamiento que recogen esa información:
 - El administrador construye manualmente las tablas de encaminamiento
 - No se adapta automáticamente a los cambios en la topología o estructura de la red

Encaminamiento dinámico (adaptativo)

- Las tablas de encaminamiento se crean y actualizan de forma automática, mediante el intercambio periódico de información entre los nodos de conmutación o encaminadores:
 - No necesitan intervención de un administrador
 - Se adaptan automáticamente a los cambios en la topología de la red
- Las técnicas (protocolos de routing dinámico) más comunes son:
 - Encaminamiento por **vectores de distancia**
 - Encaminamiento por **estado de los enlaces**

Encaminamiento estático

- Se basa en la **construcción manual de tablas de rutas** por el administrador de la red
- La construcción de tablas de encaminamiento debe cumplir el **principio de optimización**:
 - Si el camino más corto entre dos encaminadores A y D es a través de un encaminador intermedio B, entonces el camino más corto de B a D es a través de la misma ruta
 - Ejemplo:
 - A→D: ruta A-B-C-D
 - B→D: ruta B-C-D
 - C→D: ruta C-D
- Consecuencia del principio de optimización:
 - Para encaminar un paquete a lo largo del camino más corto, sólo es necesario **conocer la identidad del siguiente encaminador inmediato a lo largo del camino**
 - Este modo de encaminamiento se denomina **encaminamiento por siguiente salto** (*next-hop routing*) o **encaminamiento salto a salto** (*hop-by-hop routing*)



Encaminamiento por vector de distancias

- Cada encaminador o router mantiene una **tabla de encaminamiento** con una entrada por cada posible destino en la red
- Cada entrada de la tabla contiene:
 - El destino
 - El siguiente nodo para alcanzar dicho destino
 - La distancia al destino (usando una **métrica** concreta)
- Para construir la tabla de encaminamiento:
 - Cada router intercambian periódicamente información con sus **vecinos** (vectores de distancias)
 - Destinos (otros routers) alcanzables
 - Distancia a la que se encuentran
 - Con la información recibida de cada vecino, cada router actualizan su tabla de encaminamiento:

El vecino es mejor opción como siguiente salto hacia ese destino si su distancia, sumada a la que los separa a ambos, es menor que la conocida previamente.
- Este método se conoce como **algoritmo de Bellman-Ford**
- Algoritmo basado en vector de distancias: **RIP (Routing Information Protocol)**

Encaminamiento por vector de distancias

Ejemplo:

- La métrica puede representar, por ejemplo, el retardo de las líneas
- Para determinar el retardo de cada enlace se puede enviar un ping al vecino y calcular el tiempo de ida y vuelta
- Las tablas de rutas son:

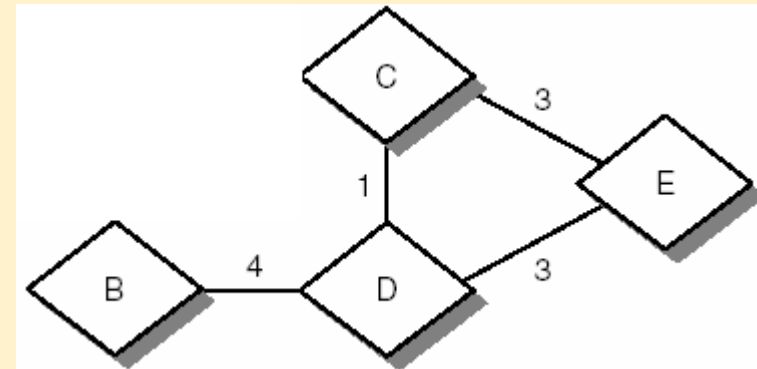


Tabla del nodo B

Des-tino	Siguiente Nodo	Distan-cia
C	D	5
D	D	4
E	D	7

Tabla del nodo C

Des-tino	Siguiente Nodo	Distan-cia
B	D	5
D	D	1
E	E	3

Tabla del nodo D

Des-tino	Siguiente Nodo	Distan-cia
B	B	4
C	C	1
E	E	3

Tabla del nodo E

Des-tino	Siguiente Nodo	Distan-cia
B	D	7
C	C	3
D	D	3

Encaminamiento por vector de distancias

Ejemplo (cont.):

- Supongamos que se añade un nuevo nodo
- Inicialmente el nodo A sólo conoce los nodos que tiene directamente conectados
 - Debe determinar la métrica a cada destino (ej. ping para determinar el retardo)

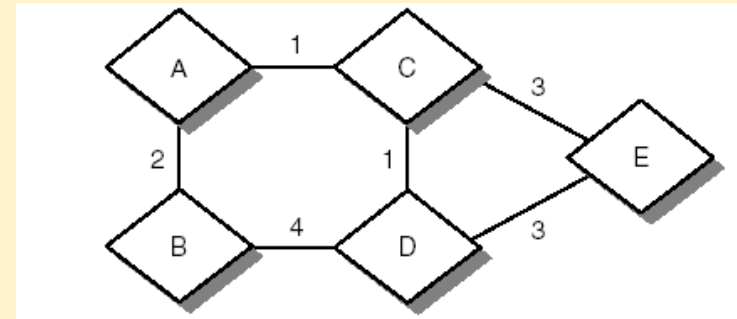


Tabla de encaminamiento inicial de A

Destino	Siguiente Nodo	Distancia
B	B	2
C	C	1

- A continuación, el nodo A recibe de sus nodos vecinos (B y C) información de encaminamiento (vectores de distancia):

Vectores de distancia B → A

→ A

Destino	Distancia
C	5
D	4
E	7

Vectores de distancia C

Destino	Distancia
B	5
D	1
E	3

Encaminamiento por vectores de distancia

Ejemplo (cont.):

- A partir de esta información, el nodo A construye su tabla de encaminamiento

Tabla de final de A

Destino	Siguiente Nodo	Distancia
B	B	2
C	C	1
D	C	2
E	C	4

- El nodo A difunde información de encaminamiento (vectores de distancia) a sus nodos vecinos
- El resto de nodos recalculan sus tablas de encaminamiento, que finalmente quedan de la siguiente forma:

Tabla del nodo B

Des- tino	Siguiente Nodo	Distan- cia
A	A	2
C	A	3
D	A/D*	4
E	A	6

Tabla del nodo C

Des- tino	Siguiente Nodo	Distan- cia
A	A	1
B	A	3
D	D	1
E	E	3

Tabla del nodo D

Des- tino	Siguiente Nodo	Distan- cia
A	C	2
B	A/B*	4
C	C	1
E	E	3

Tabla del nodo E

Des- tino	Siguiente Nodo	Distan- cia
A	C	4
B	C	6
C	C	3
D	D	3

Encaminamiento por estado de enlaces

Características:

- Cada encaminador mantiene información sobre la topología exacta de la red, la base de datos del estado de los enlaces (*link state database*)

Proceso de construcción de la base de datos

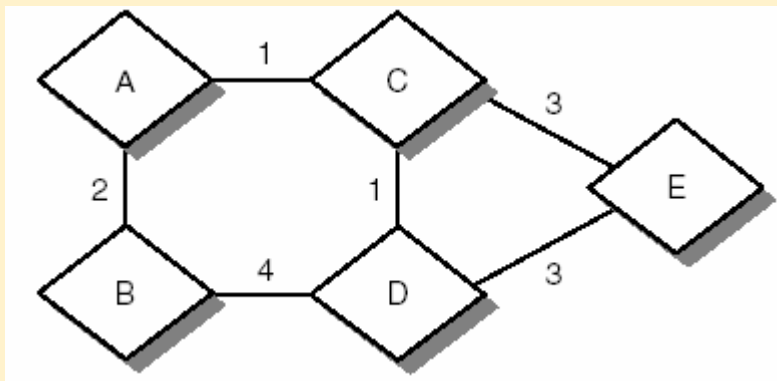
- Cada encaminador identifica a todos los nodos vecinos y determina la distancia o métrica a cada uno (estado del enlace)
- Cada nodo anuncia esta información a **todos** los nodos de la red, ej. por un mecanismo de inundación
- La información de enlaces locales y la recibida del resto de nodos de la red:
 - Se usa para construir la **base de datos del estado de los enlaces**
 - Todos los nodos manejan exactamente la misma base de datos
- A partir de la base de datos del estado de los enlaces:
 - Cada nodo construye un **mapa o árbol de rutas** de la red desde su punto de vista
 - La construcción del árbol o mapa de rutas se basa en el algoritmo de Dijkstra
 - En este árbol de rutas, cada nodo selecciona las rutas más cortas a cada destino y se eliminan posibles bucles

Ejemplo de algoritmo: OSPF (Open Shortest Path First)

Encaminamiento por estado de enlaces

Ejemplo:

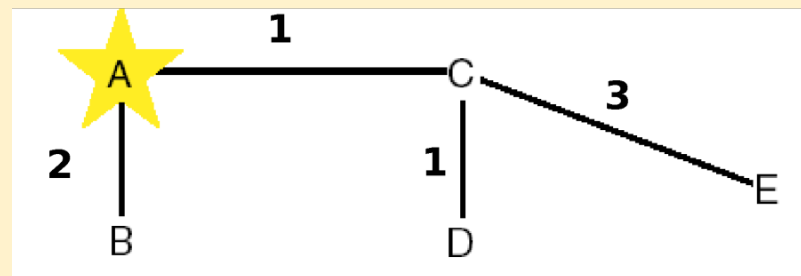
Red



Base de datos de estado de los enlaces
(común a todos los nodos)

A	B	C	D	E
B-2 C-1	A-2 D-4	A-1 D-1 E-3	C-1 B-4 E-3	C-3 D-3

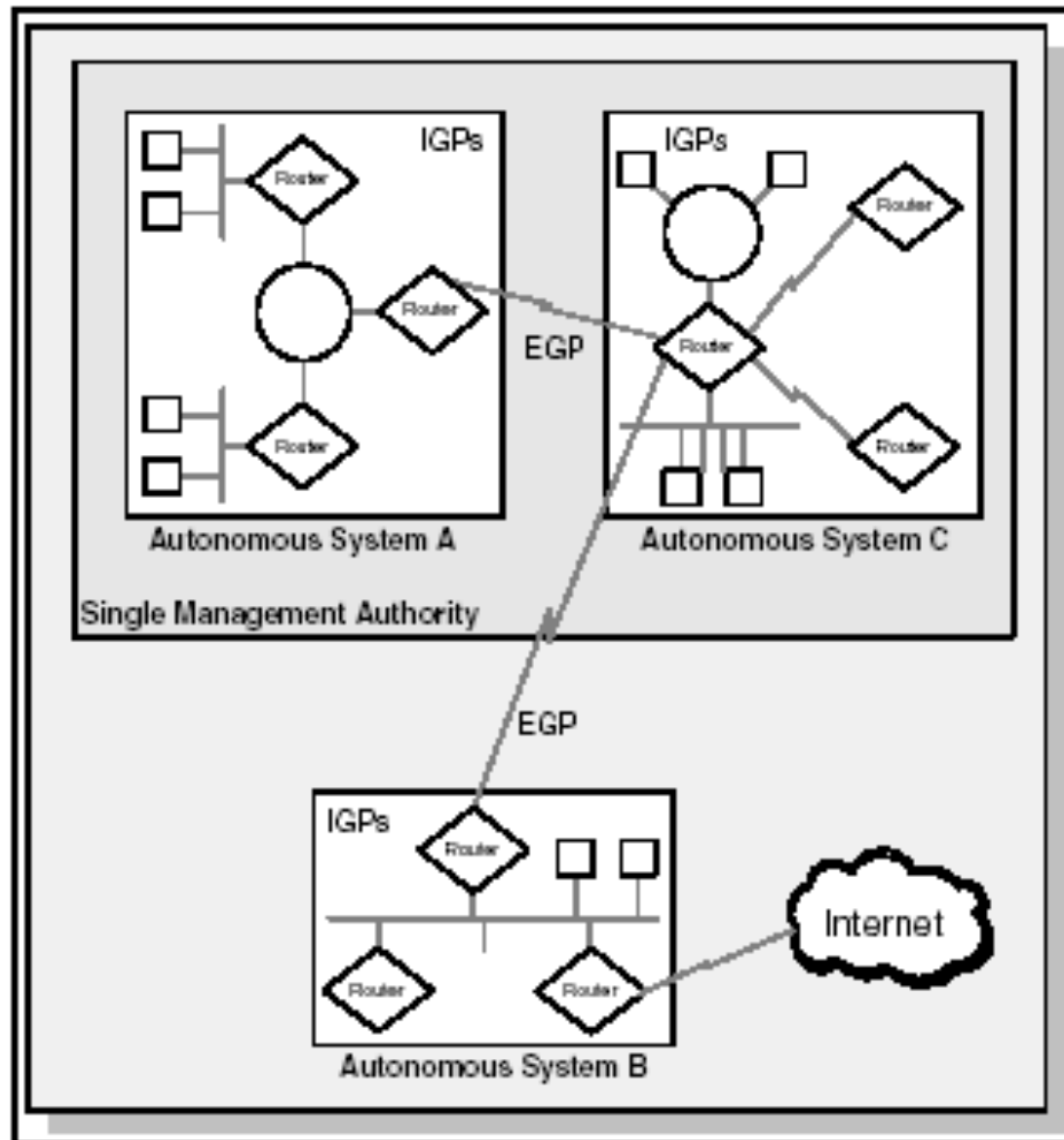
Árbol o mapa de rutas
para el nodo A



Encaminamiento en Internet

- Se usan algoritmos de **encaminamiento dinámico**
- Organización jerárquica de Internet: **Sistemas Autónomos (AS)**
 - **Protocolos Internos (IGP)**: Lo utilizan los routers internos, para el encaminamiento dentro de un AS:
 - **RIP**: Routing Information Protocol
 - **OSPF**: Open Shortest Path First
 - **IGRP**: Internal Gateway Routing Protocol (de CISCO)
 - **Protocolos Externos (EGP)**: Lo utilizan los routers frontera, para el encaminamiento entre distintos AS:
 - **EGP**: External Gateway Protocol (actualmente en desuso)
 - **BGP**: Border Gateway Protocol

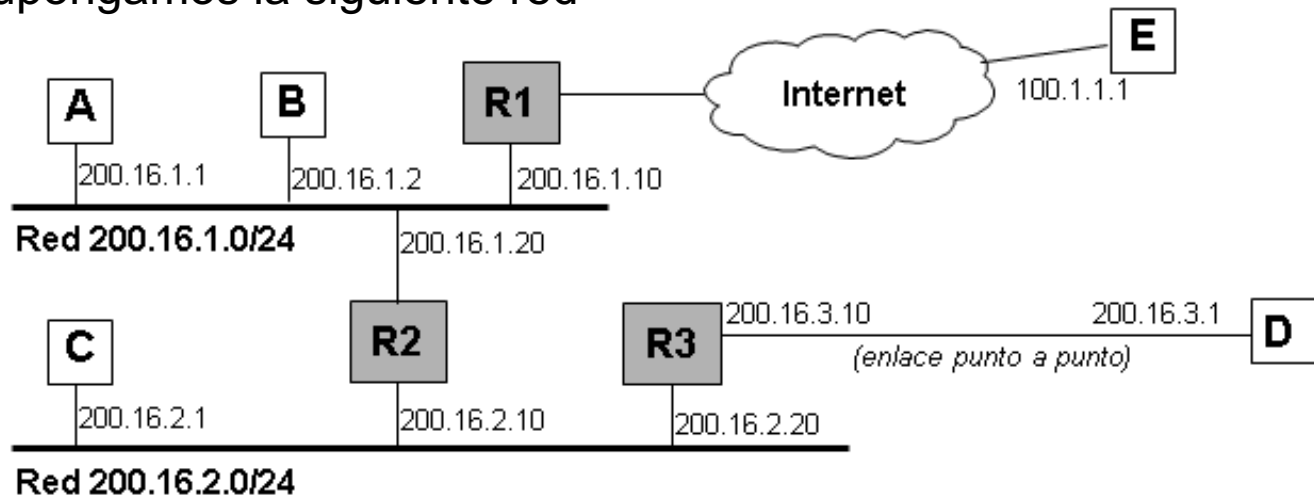
Encaminamiento en Internet



Encaminamiento en Internet

Tablas de encaminamiento en redes IP (1)

- Ejemplo: Supongamos la siguiente red



- La tabla de encaminamiento de la **estación A**, podría ser la siguiente:

```
# route -n
```

```
Kernel IP routing table
```

	Destination	Gateway	Genmask	Flags	Iface
1---	200.16.1.	0.0.0.0	255.255.255.0	U	eth0
2---	200.16.2.0	200.16.1.20	255.255.255.0	UG	eth0
3---	200.16.3.1	200.16.1.20	255.255.255.255	UGH	eth0
4---	0.0.0.0	200.16.1.10	0.0.0.0	UG	eth0

Encaminamiento en Internet

Tablas de encaminamiento en redes IP (2)

- Campos principales de la tabla de encaminamiento
 - **Destination:** Red o host destino
 - **Gateway:** El host o router que debe entregar o reexpedir el paquete
 - **Genmask:** Máscara de red asociada a la red destino
 - **Flags:** Indican el estado de la ruta
 - **U** → La ruta se puede usar (usable)
 - **H** → El campo Destination representa un Host y no una red
 - **G** → El host de entrega es un router (un camino indirecto)
 - **D** → La ruta es consecuencia de una redirección ICMP
 - **Iface:** Enlace o interfaz de red por el que se alcanza la red destino

Encaminamiento en Internet

Tablas de encaminamiento en redes IP (3)

- Entradas de la tabla de encaminamiento de la estación A

Entrada 1

Destination	Gateway	Genmask	Flags	Iface
200.16.1.0	0.0.0.0	255.255.255.0	U	eth0

- El destino es la propia red local de la estación A: entrega directa
- Para enviar un paquete a cualquier máquina de esa red destino (por ej. estación B), no es necesario utilizar ningún router (Gateway = 0.0.0.0), sino que se realiza la entrega directa del paquete a través de la propia red
- Esta entrada aparece automáticamente en la tabla de rutas, en el momento en que se configura la interfaz de red (eth0)

Entrada 2

Destination	Gateway	Genmask	Flags	Iface
200.16.2.0	200.16.1.20	255.255.255.0	UG	eth0

- El destino es una red diferente alcanzable de forma indirecta a través de un router
- Para enviar un paquete a cualquier máquina de esa red destino (por ej. estación C), es necesario entregar el paquete al router indicado (Gateway = 200.16.1.20)
- Esta entrada hay que añadirla a la tabla de rutas de forma manual o mediante algún protocolo de routing

Encaminamiento en Internet

Tablas de encaminamiento en redes IP (4)

- Entradas de la tabla de encaminamiento de la estación A (cont.)

Entrada 3

Destination	Gateway	Genmask	Flags	Iface
200.16.3.1	200.16.1.20	255.255.255.255	UGH	eth0

- El campo destino no se corresponde con una red, sino con un host (caso muy especial)
- Para enviar un paquete al host destino (en este caso, la estación D), es necesario entregar el paquete al router indicado (Gateway = 200.16.1.20)
- Esta entrada hay que añadirla a la tabla de rutas de forma manual o mediante algún protocolo de routing

Entrada 4

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	200.16.1.10	0.0.0.0	UG	eth0

- Esta entrada, cuyo campo destino tiene valor 0.0.0.0, se utiliza para definir el router predeterminado (*default router*)
- Esta entrada se utiliza cuando la red o host destino no coincide con ninguna de las entradas anteriores de la tabla de rutas (por ejemplo, en el caso de la estación E)
- En esta situación, el paquete se debe entregar al router predeterminado (200.16.1.10)
- Normalmente, esta entrada se añade al final de la tabla de rutas, de forma manual o mediante la lectura de un fichero de configuración.