

Xarxes de Computadors

Tema 2 - Redes IP

Temario

- ▶ 1) Introducción
- ▶ **2) Redes IP**
- ▶ 3) Protocolos UDP y TCP
- ▶ 4) Redes de área local (LAN)
- ▶ 5) Protocolos del nivel aplicación



Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – Redes IP

- ▶ **Introducción**
- ▶ Direcccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – Introducción

4	Transporte
3	Red
2	Enlace

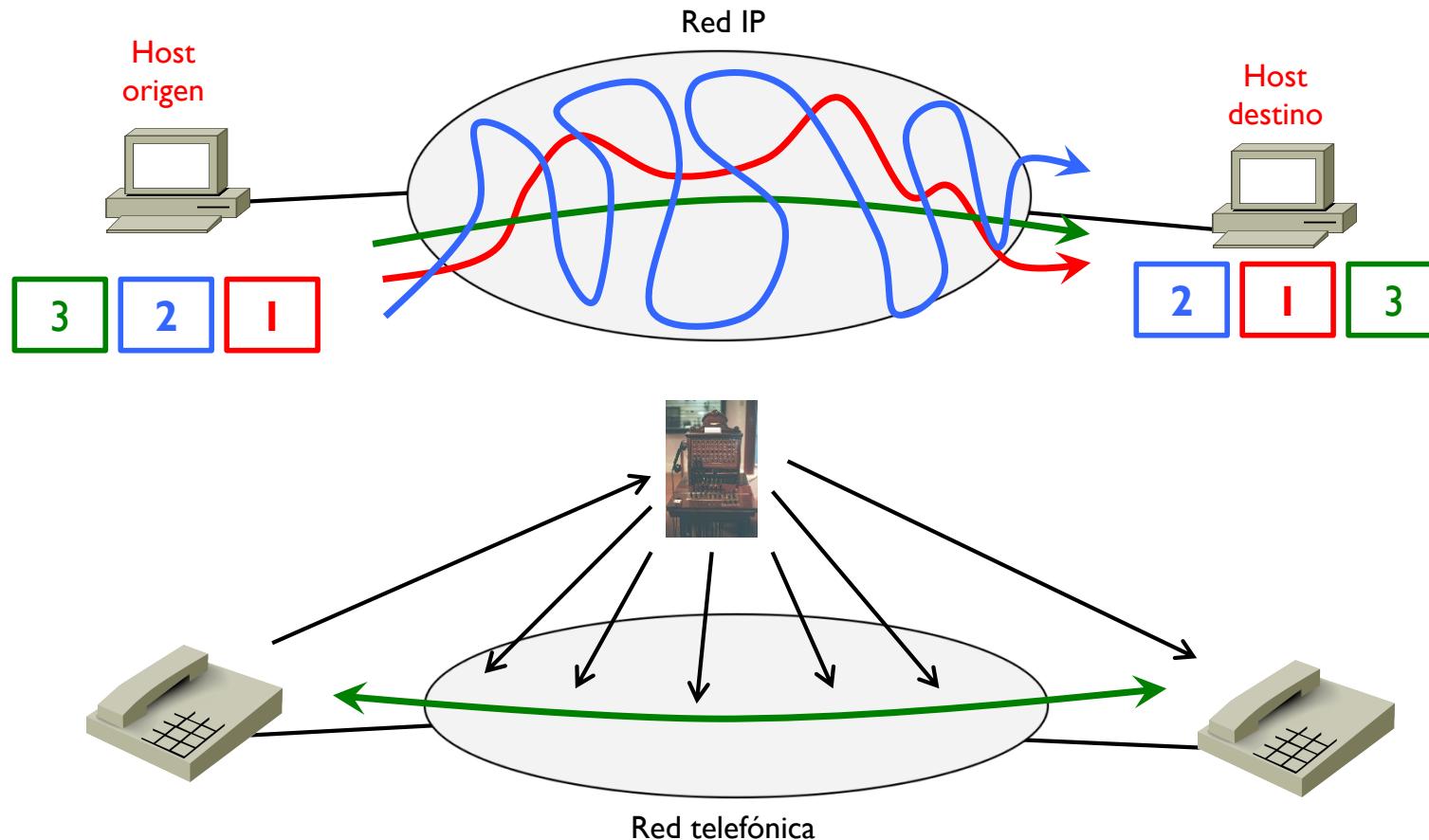
Internet Protocol (IP)

- ▶ La información base es el datagrama (o paquete IP)
- ▶ Tres propiedades de los datagramas
 - ▶ Cada datagrama es independiente de los otros y → no orientado a la conexión
 - ▶ Cada datagrama se trata lo mejor que se puede → best effort
 - ▶ Un datagrama se puede perder y no hay un mecanismo de recuperación → no fiable



Tema 2 – Introducción

- ▶ Cada datagrama es independiente de los otros y puede entregarse sin un orden determinado
→ no está orientado a la conexión



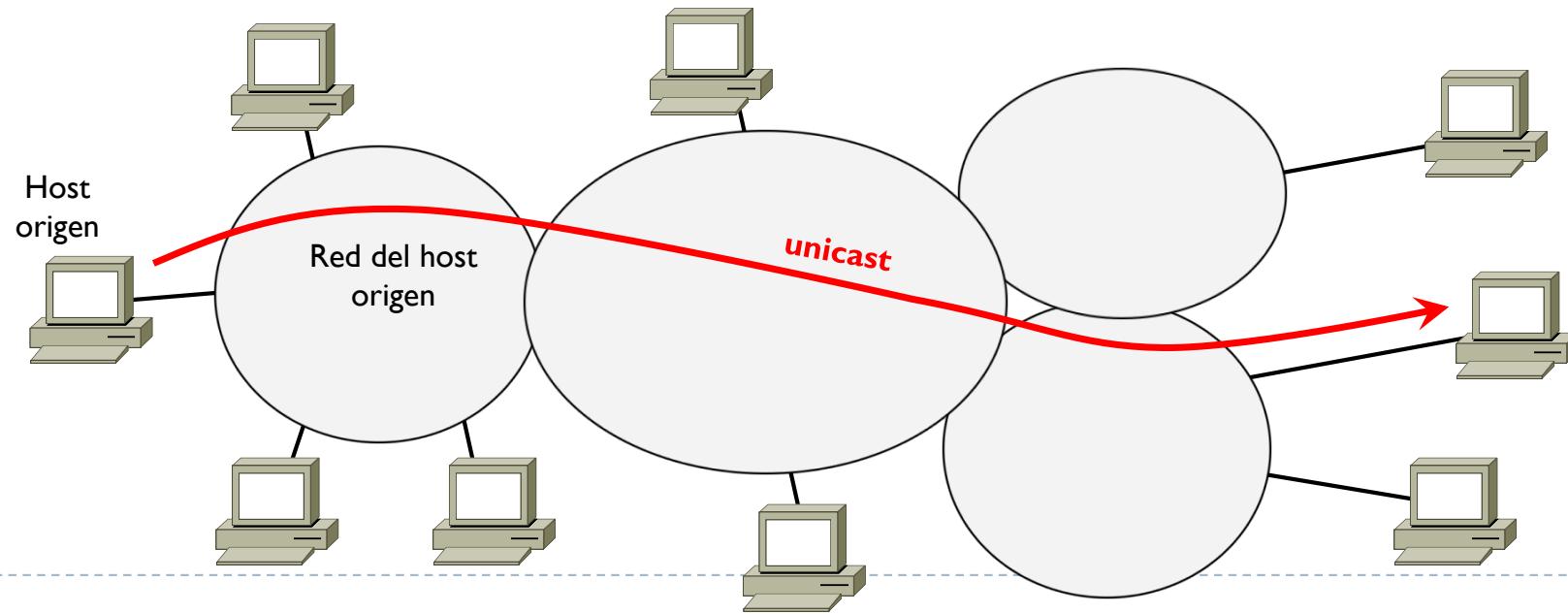
Tema 2 – Introducción

- ▶ Tres tipos de datagrama según quien es el destino
- ▶ **Unicast**
 - ▶ Un único destino
- ▶ **Broadcast**
 - ▶ Todos los destinos posibles de la red del host origen
- ▶ **Multicast**
 - ▶ Un grupo determinado de destinos (que pueden estar en cualquier sitio)



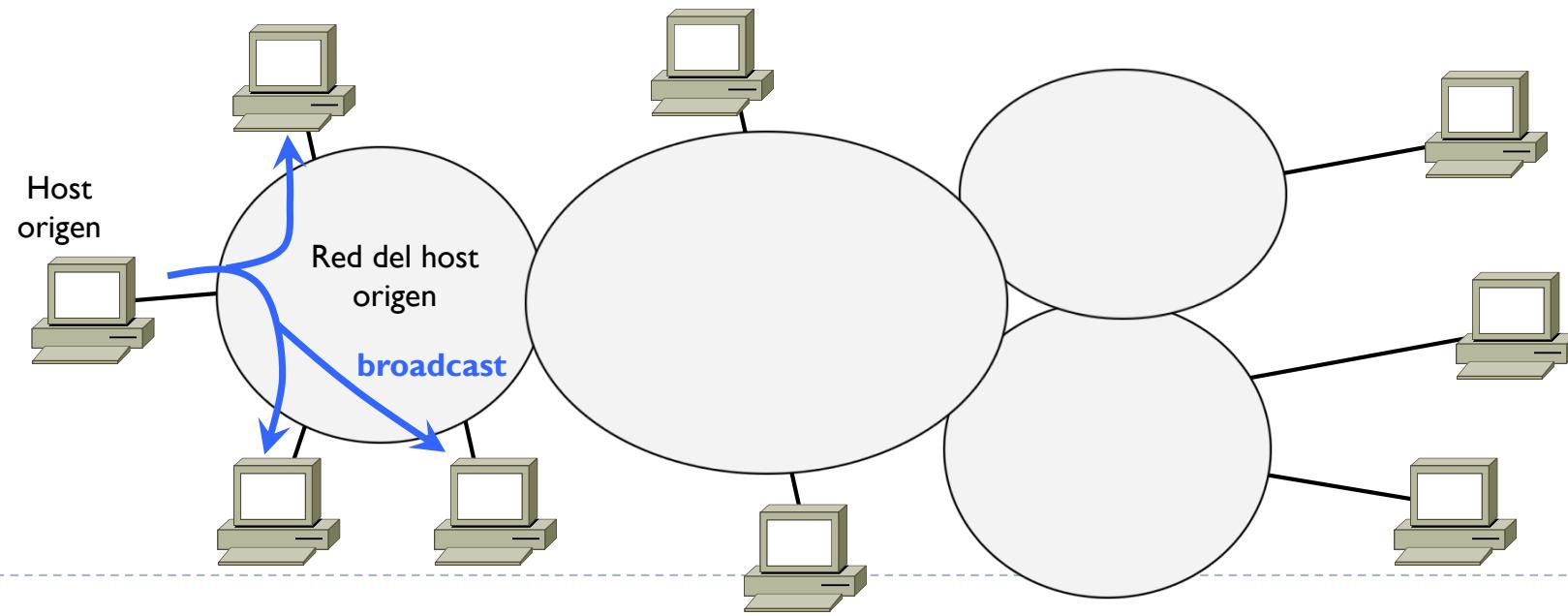
Tema 2 – Introducción

- ▶ Tres tipos de datagrama según quien es el destino
- ▶ Unicast
 - ▶ Un único destino
- ▶ Broadcast
 - ▶ Todos los destinos posibles de la red del host origen
- ▶ Multicast
 - ▶ Un grupo determinado de destinos (que pueden estar en cualquier sitio)



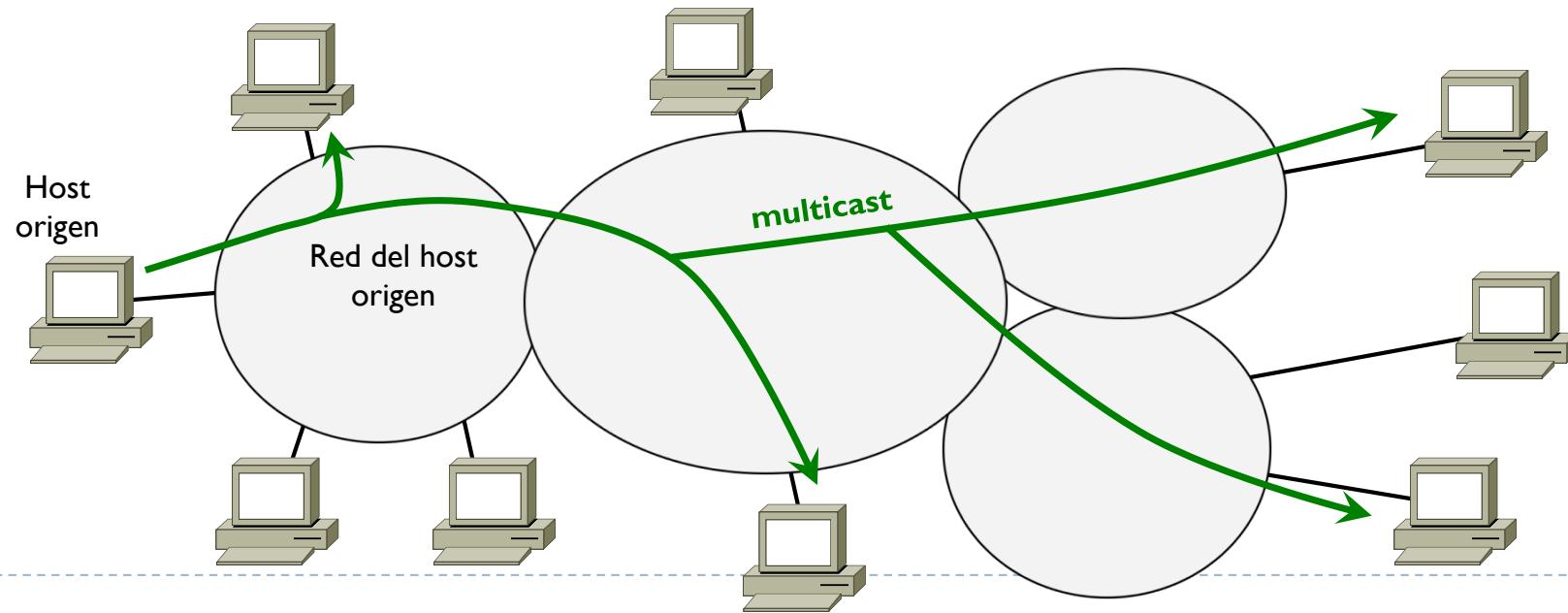
Tema 2 – Introducción

- ▶ Tres tipos de datagrama según quien es el destino
- ▶ Unicast
 - ▶ Un único destino
- ▶ Broadcast
 - ▶ Todos los destinos posibles de la red del host origen
- ▶ Multicast
 - ▶ Un grupo determinado de destinos (que pueden estar en cualquier sitio)



Tema 2 – Introducción

- ▶ Tres tipos de datagrama según quien es el destino
- ▶ Unicast
 - ▶ Un único destino
- ▶ Broadcast
 - ▶ Todos los destinos posibles de la red del host origen
- ▶ Multicast
 - ▶ Un grupo determinado de destinos (que pueden estar en cualquier sitio)



Tema 2 – Introducción

- ▶ Objetivo de la capa de red que resuelve el protocolo IP es entregar datagramas de un origen a un destino pasando a través de una o varias redes

→ **Direccionamiento IP**
manera con la cual los hosts, los routers y las redes se identifican

→ **Encaminamiento IP**
manera con la cual los datagramas viajan por las redes
("se encaminan")



Tema 2 – Redes IP

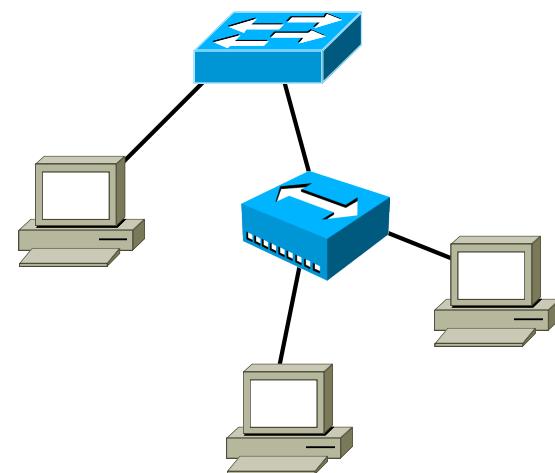
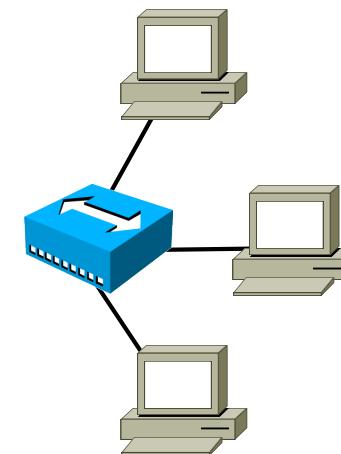
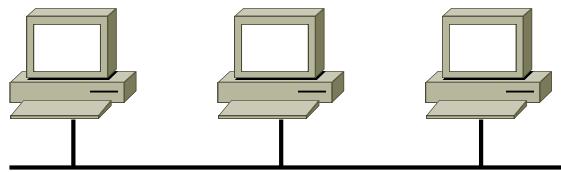
- ▶ Introducción
- ▶ **Direccionamiento y subnetting**
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – Direcccionamiento IP

- ▶ ¿Qué es una red IP?

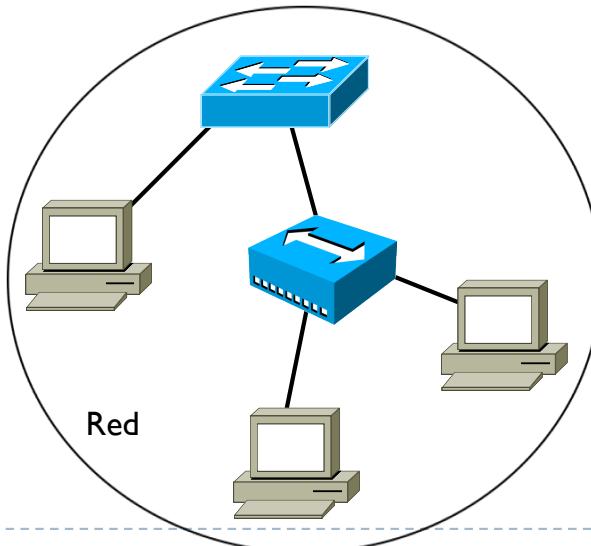
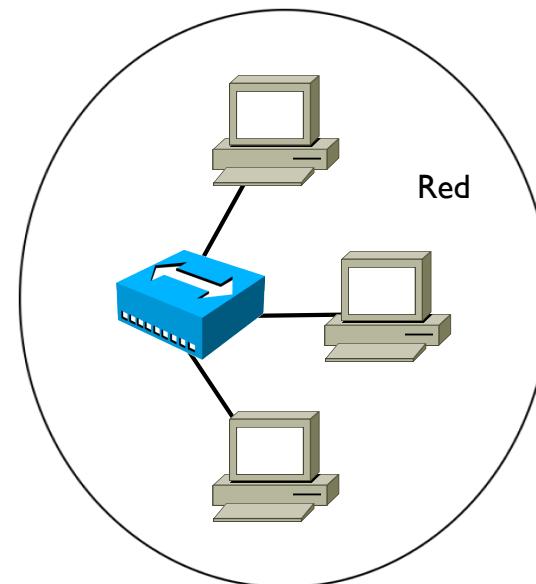
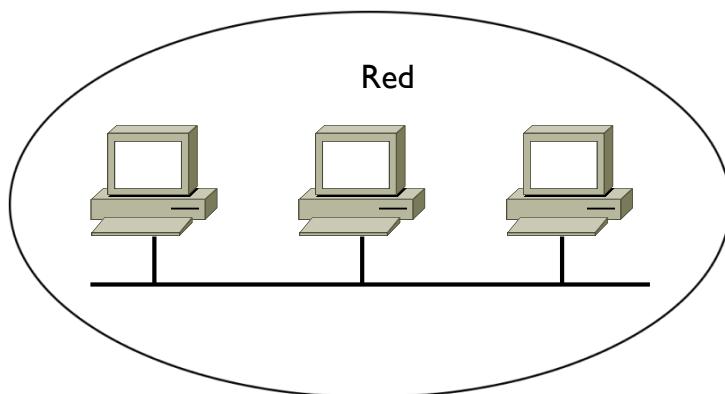
Un conjunto de hosts conectados entre sí a través de dispositivos de nivel 1 o 2



Tema 2 – Direcccionamiento IP

- ▶ ¿Qué es una red IP?

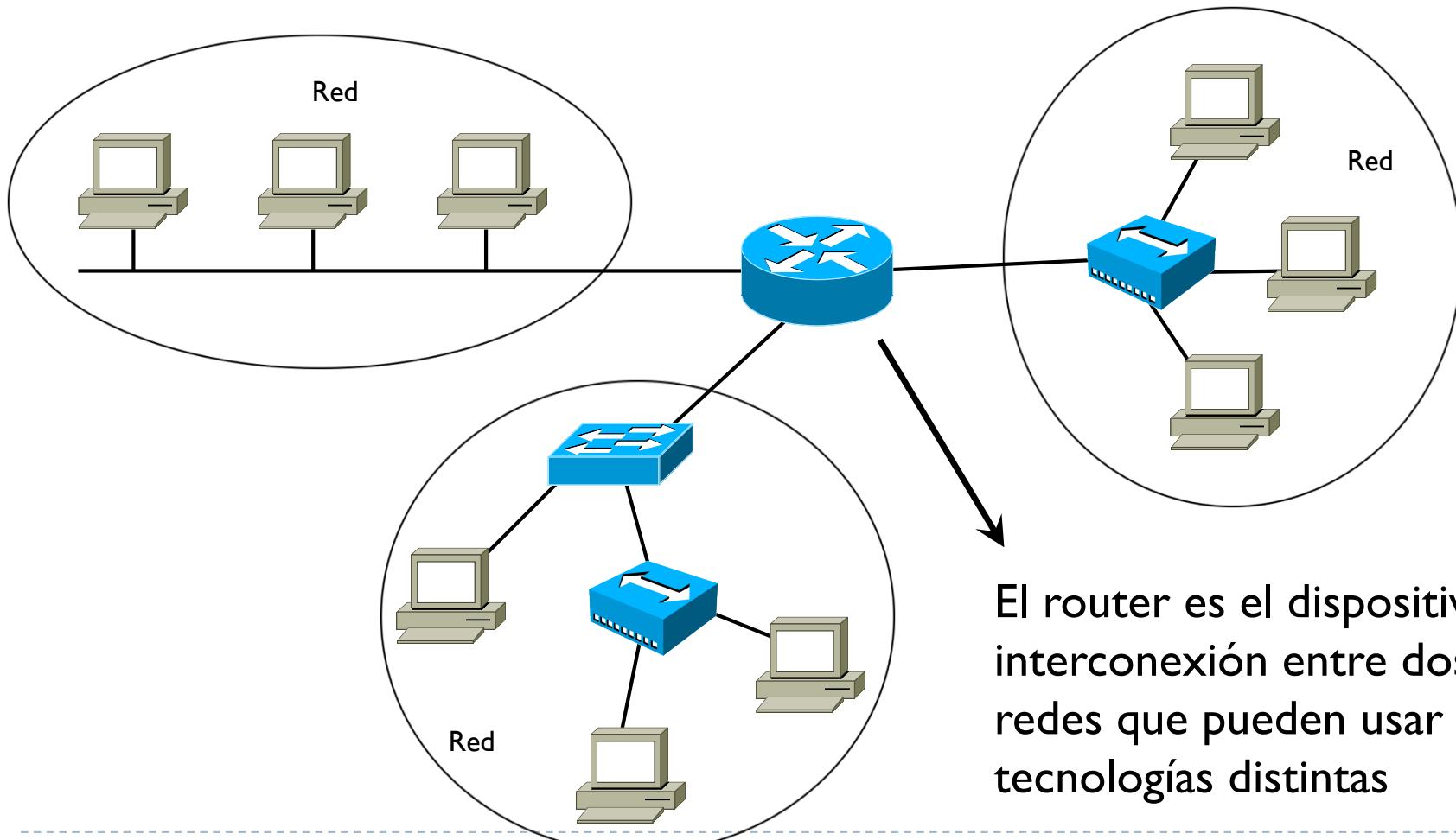
Un conjunto de hosts conectados entre sí a través de dispositivos de nivel 1 o 2



Tema 2 – Direcccionamiento IP

- ▶ ¿Qué es una red IP?

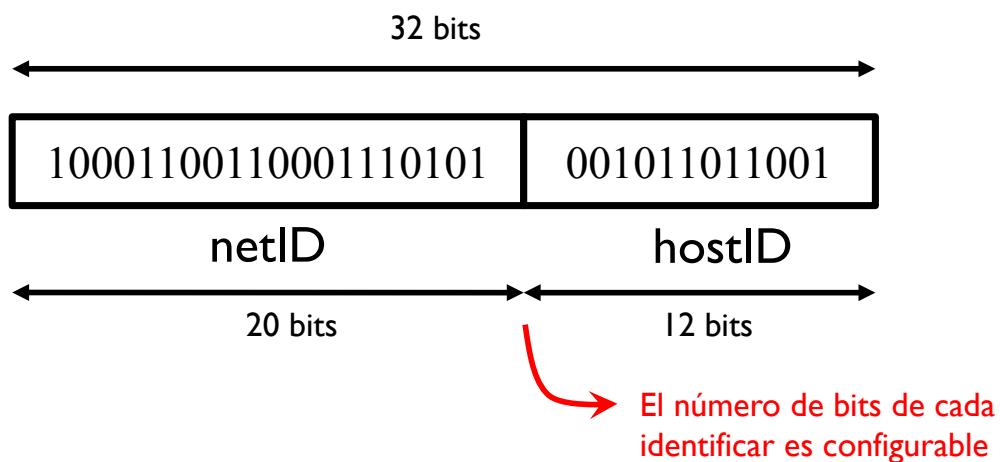
Un conjunto de hosts conectados entre sí a través de dispositivos de nivel 1 o 2



El router es el dispositivo de interconexión entre dos o mas redes que pueden usar tecnologías distintas

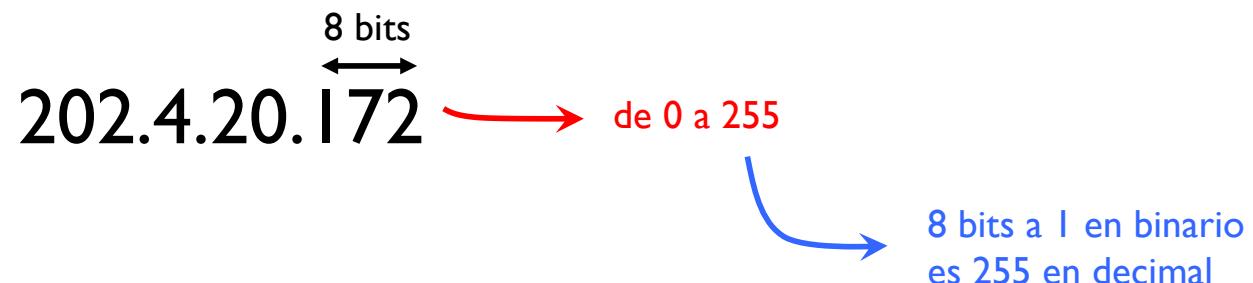
Tema 2 – Direccionamiento IP

- ▶ En direccionamiento se definen dos identificadores
 - **netID** - identificador de una red
Redes distintas deben tener netID distintos
 - **hostID** - identificador de host
Hosts de una misma rede deben tener hostID distintos y mismo netID
- ▶ Juntos en este orden forman una dirección IP (@IP) de 32 bits
 - ▶ La maquina hostID que pertenece a la red netID



Tema 2 – Direccionamiento IP

- ▶ Como no es viable representar números en binario, una @IP se representa como 4 decimales separados por un punto

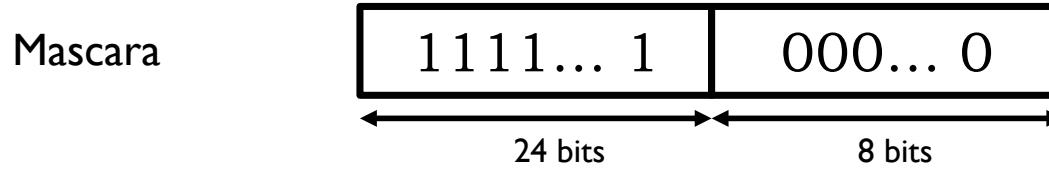
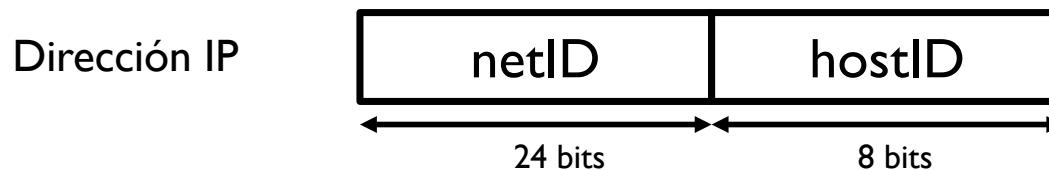


- ▶ ¿Pero como se reconoce la parte netID y hostID de una @IP?
- ▶ Dos maneras
 - ▶ Usando mascaras → mas usado
 - ▶ Usando las clases → método original, se mantiene la compatibilidad si no se usan mascaras, por defecto se considera la clase

Tema 2 – Direccionamiento IP

▶ Mascaras

- ▶ Otro número de 32 bits que va junto a una @IP
- ▶ Se usan 1 en correspondencia del netID y 0 en hostID
- ▶ También se representa con 4 decimales separados por un punto o como un único número decimal que representa el número de 1 seguidos



255. 255. 255. 0 4 decimales separados por un punto

/24

Un único decimal



Tema 2 – Direcccionamiento IP

▶ Ejemplos

- ▶ 202.4.20.171 / 255.255.255.0
 - ▶ netID = 202.4.20
 - ▶ hostID = 171
- ▶ 147.83.3.4 / 16
 - ▶ netID = 147.83
 - ▶ hostID = 3.4
- ▶ 71.45.202.127 / 8
 - ▶ netID = 71
 - ▶ hostID = 45.202.127
- ▶ /8, /16 y /24 → Mascaras “fáciles” → la separación netID/hostID cae en un .



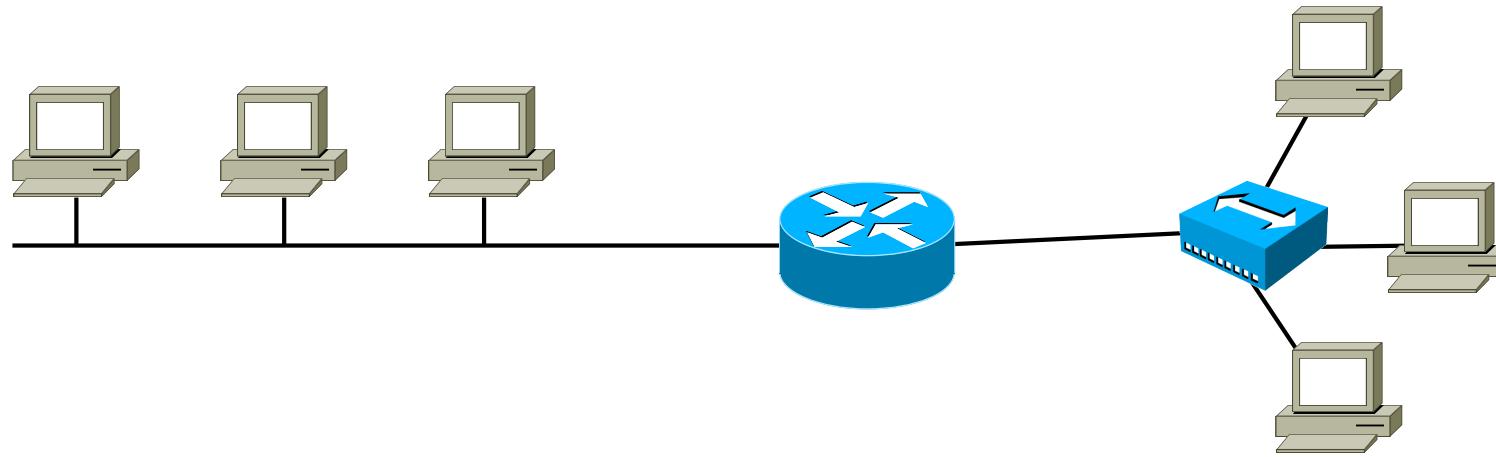
Tema 2 – Direccionamiento IP

- ▶ ¿cómo se asignan las @IP?
- ▶ Una @IP identifica una interfaz conectada a una red que envía y recibe datagramas
 - ▶ Se asignan a interfaces de equipos de nivel 3 o superior
 - ▶ Host y router SI
 - ▶ Switch y hub NO
- ▶ Las @IP con mismo netID pertenecen a la misma red
- ▶ El hostID identifica una interfaz de la red netID
 - ▶ Una interfaz pero no puede tener un hostID con todos los bits a 0 o todos a 1
- ▶ Todas las @IP deben ser distintas



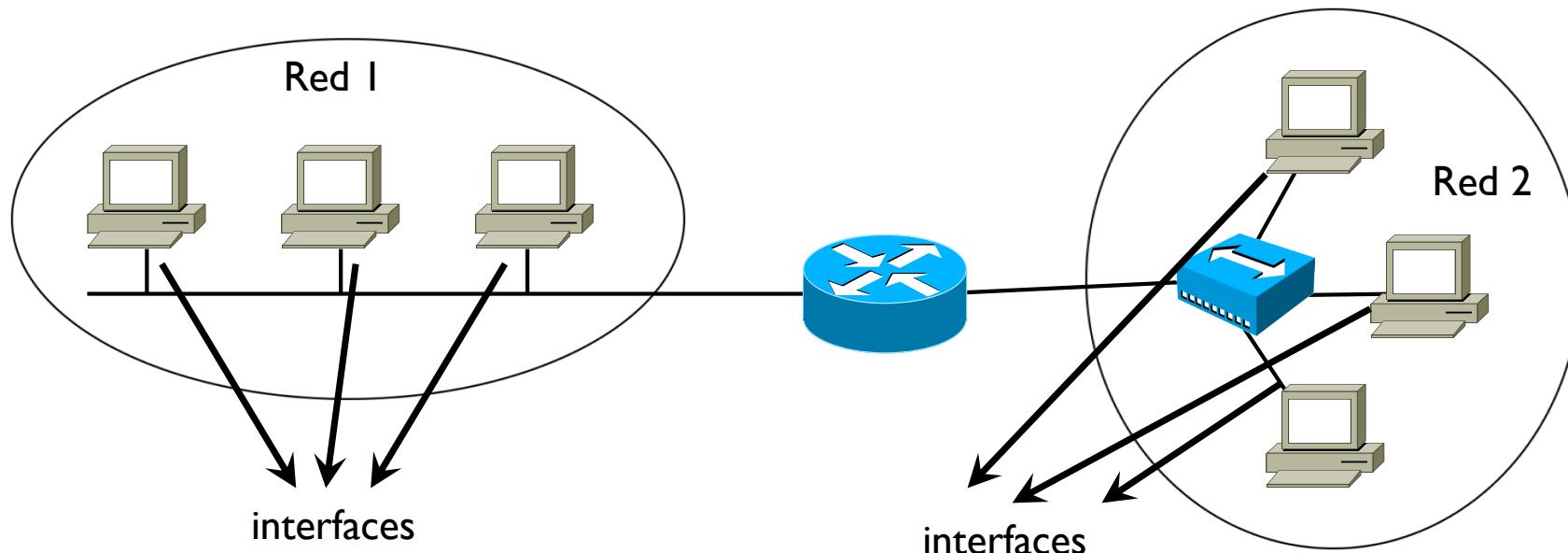
Tema 2 – Direcccionamiento IP

- ▶ Ejemplo



Tema 2 – Direcccionamiento IP

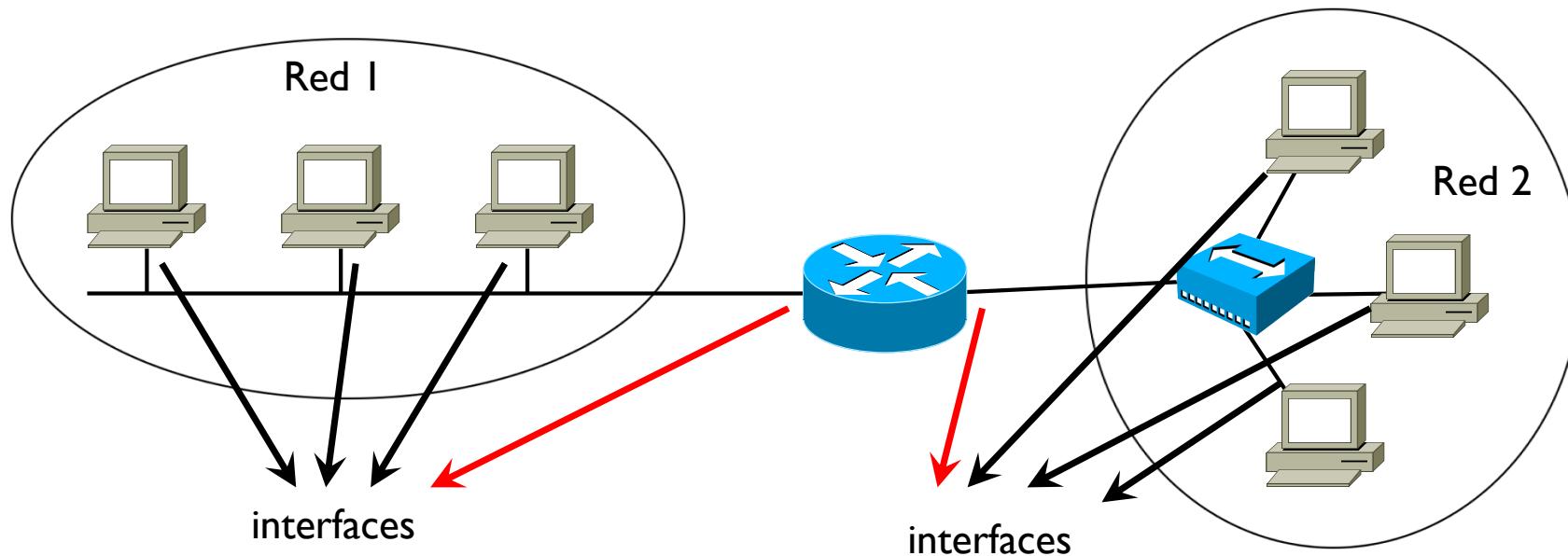
- ▶ Ejemplo



- ▶ Se identifican las redes y las interfaces que deben tener una @IP
- ▶ ¿Olvidamos algo?

Tema 2 – Direcccionamiento IP

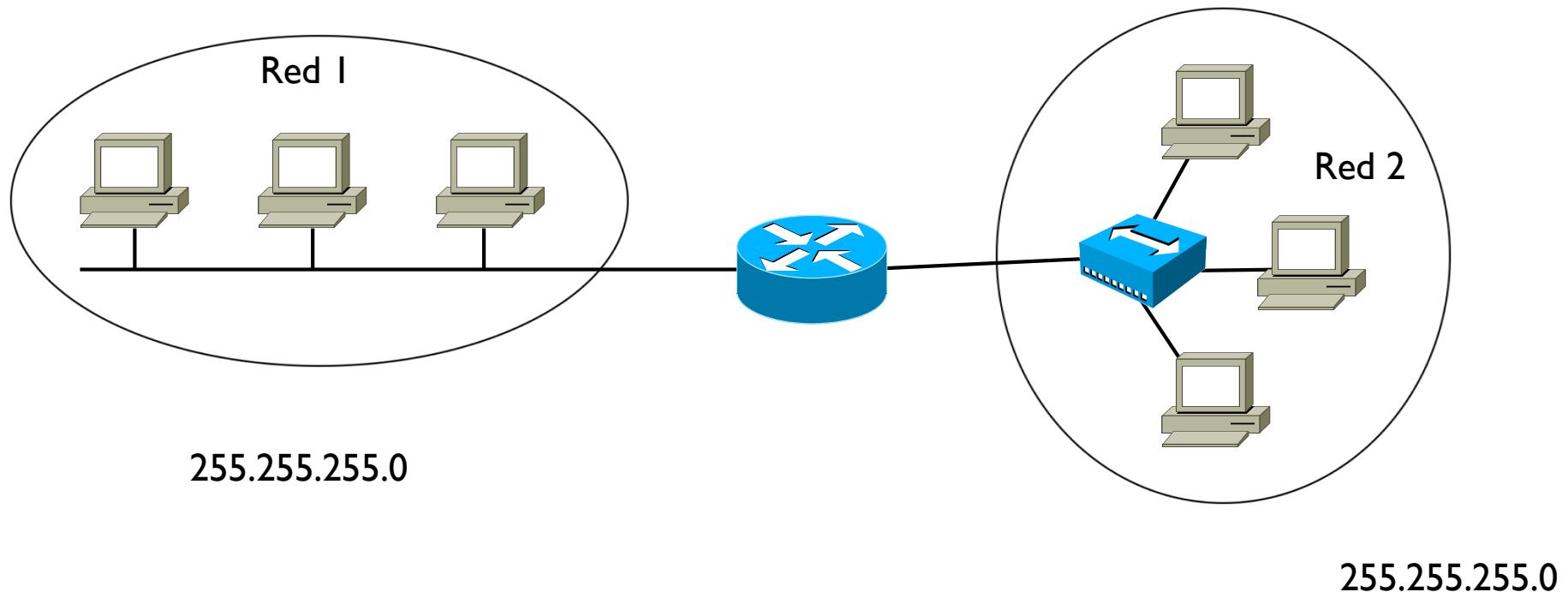
- ▶ Ejemplo



- ▶ Se identifican las redes y las interfaces que deben tener una @IP

Tema 2 – Direcccionamiento IP

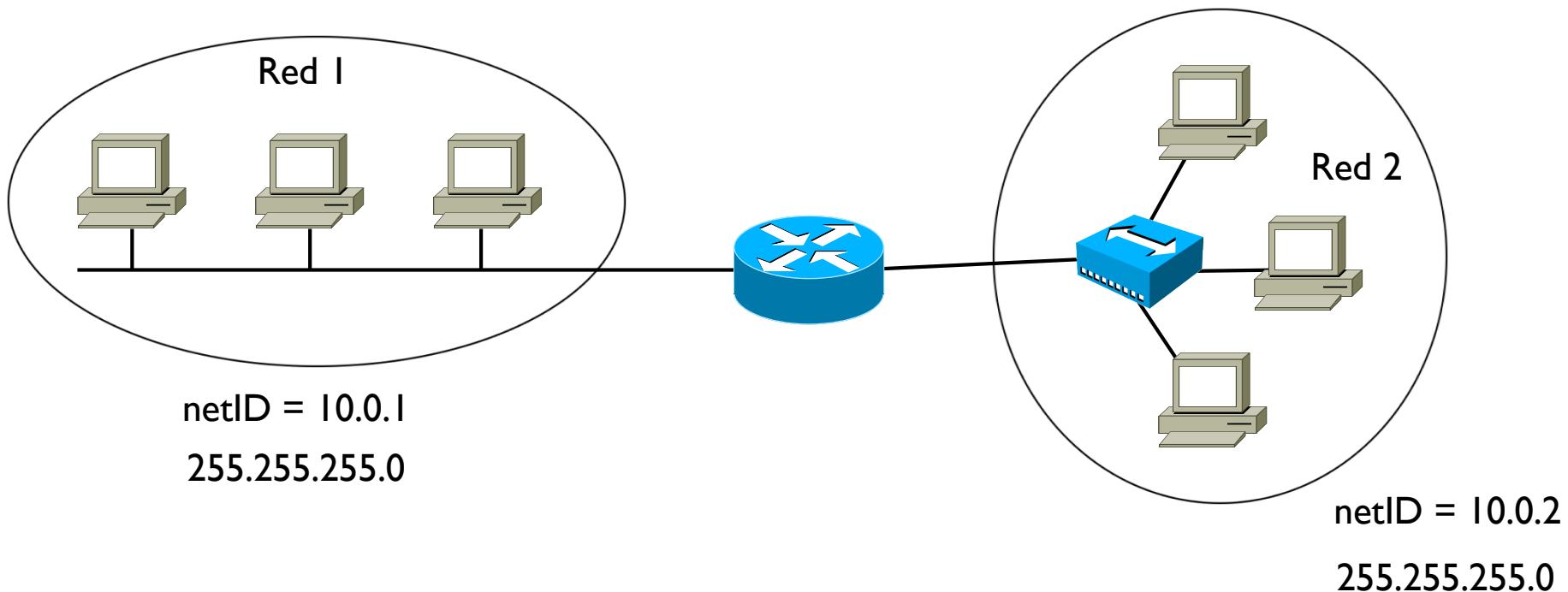
▶ Ejemplo



- ▶ Se definen las máscaras
- ▶ Cada red en principio puede tener una máscara cualquiera
- ▶ La selección puede depender del tamaño de la red (es decir, del número de interfaces con @IP)

Tema 2 – Direcccionamiento IP

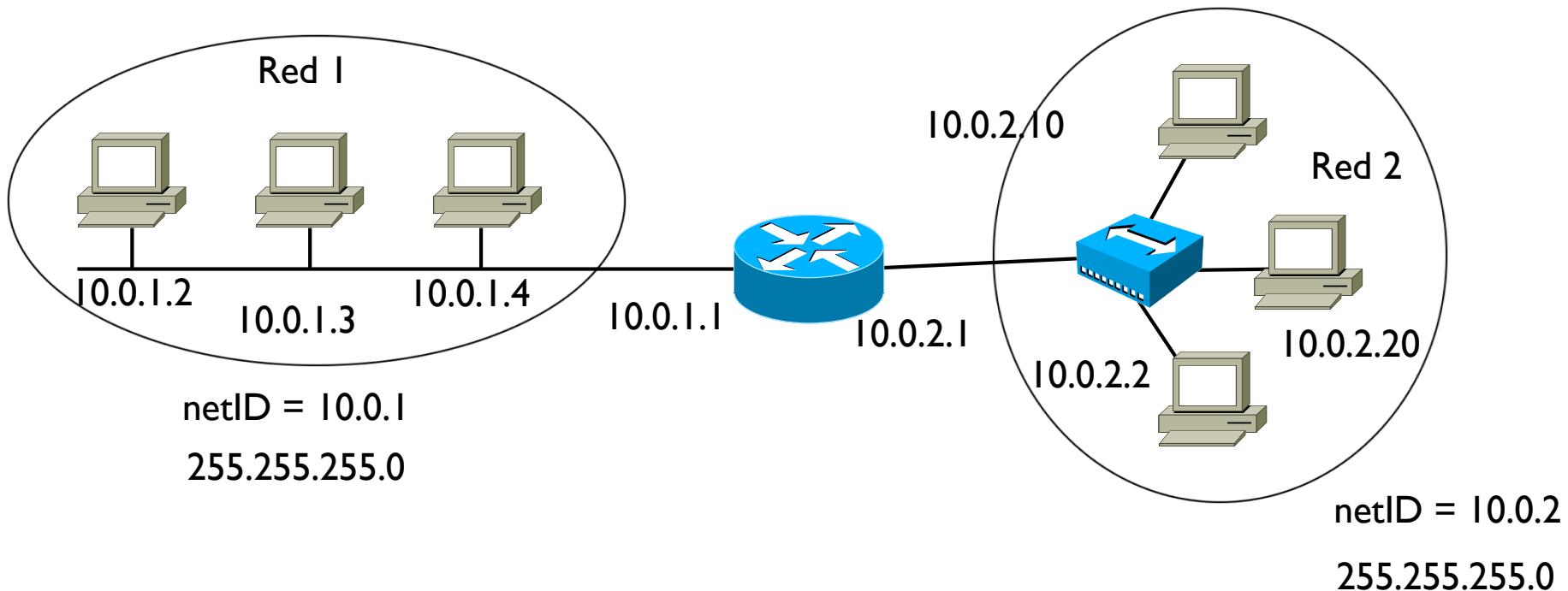
- ▶ Ejemplo



- ▶ Se asigna el netID a las redes
- ▶ Cada red debe tener un netID distinto

Tema 2 – Direcccionamiento IP

▶ Ejemplo



- ▶ Se asignan los hostID y se completan las @IP
 - ▶ En una misma red, no pueden haber dos hosts con mismo hostID
 - ▶ Pueden ser iguales entre hosts de redes distintas
 - ▶ No se pueden usar las combinaciones de todos 0 o todos 1

Tema 2 – Direccionamiento IP

- ▶ ¿Por qué no se pueden usar todos 0 o todos 1 en hostID?
- ▶ Tienen otro significado
- ▶ hostID con todos los bits a 0 identifica la dirección de red

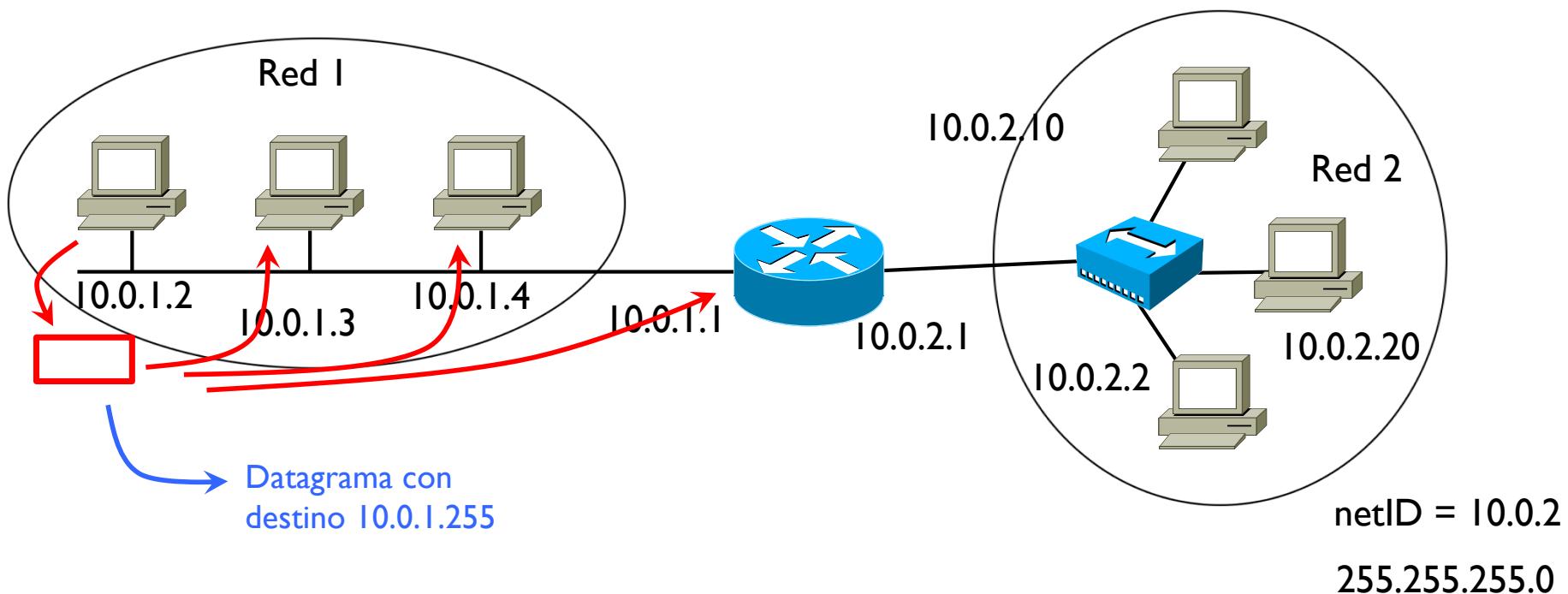


- ▶ hostID con todos los bits a 1 identifica la dirección de broadcast



Tema 2 – Direcccionamiento IP

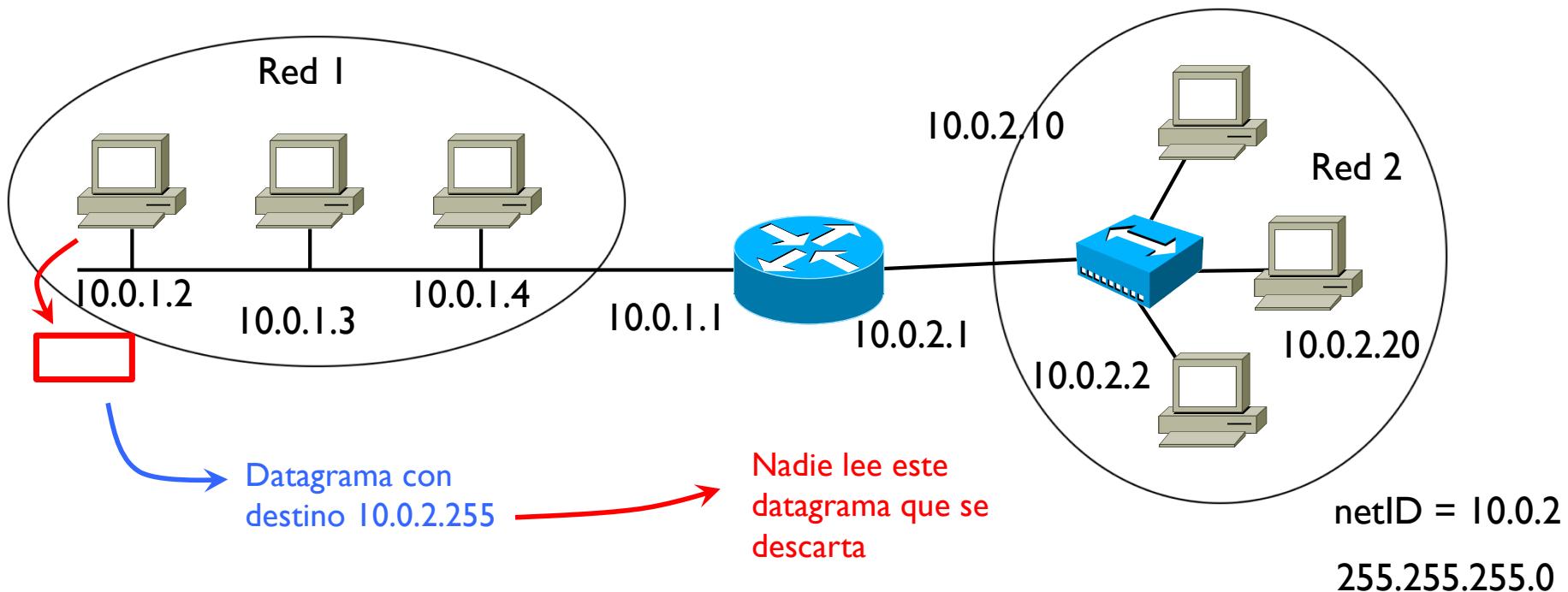
- ▶ hostID con todos los bits a 1 identifica la dirección de broadcast de la red



- ▶ Se envía un único datagrama pero este se recibe en todas las interfaces de la misma red del origen
- ▶ No pasa a otras redes
- ▶ No se puede enviar un datagrama en broadcast a otras redes

Tema 2 – Direcccionamiento IP

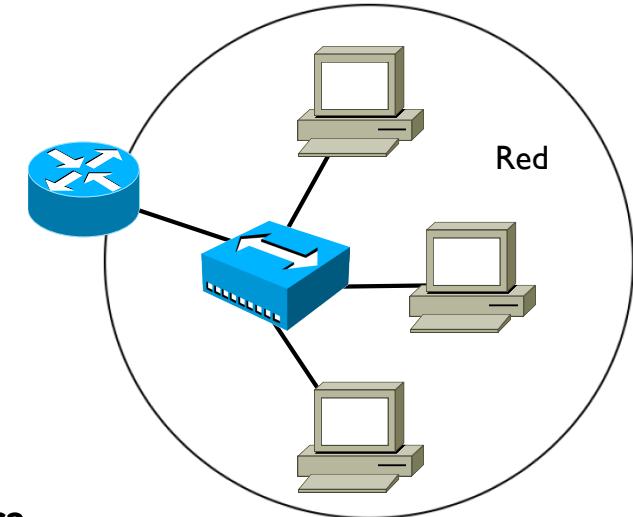
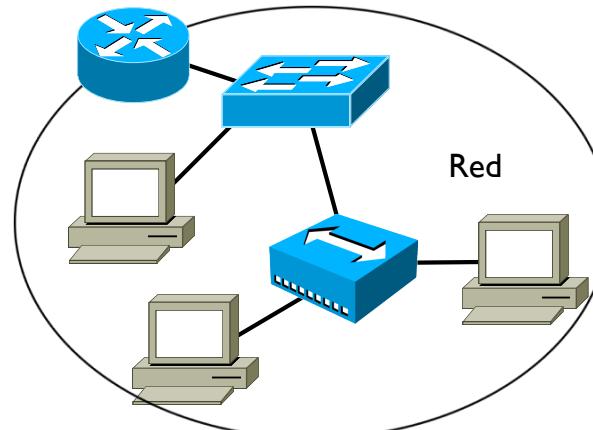
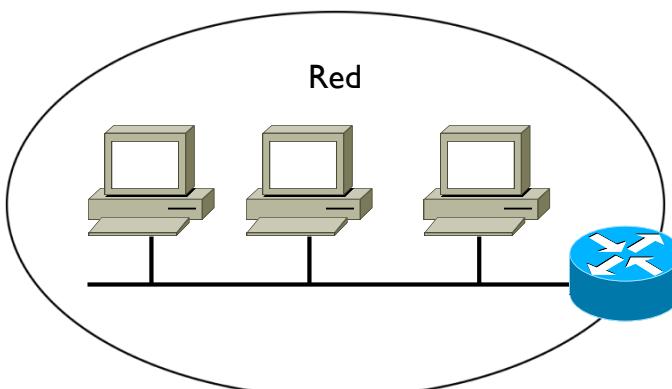
- ▶ hostID con todos los bits a 1 identifica la dirección de broadcast de la red



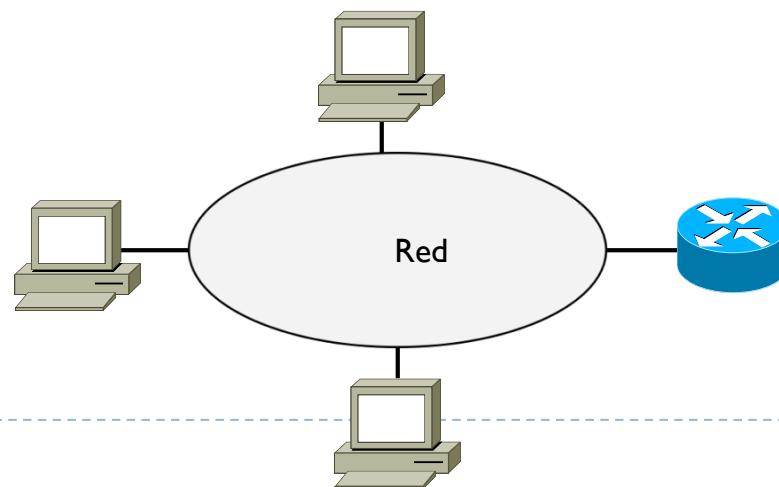
- ▶ No se puede enviar un datagrama en broadcast a otras redes

Tema 2 – Direcccionamiento IP

- ▶ En estas tres redes, solo hay @IP en los hosts y routers, los demás dispositivos no tienen
- ▶ Desde el punto de vista de la capa 3, estas tres redes son equivalentes

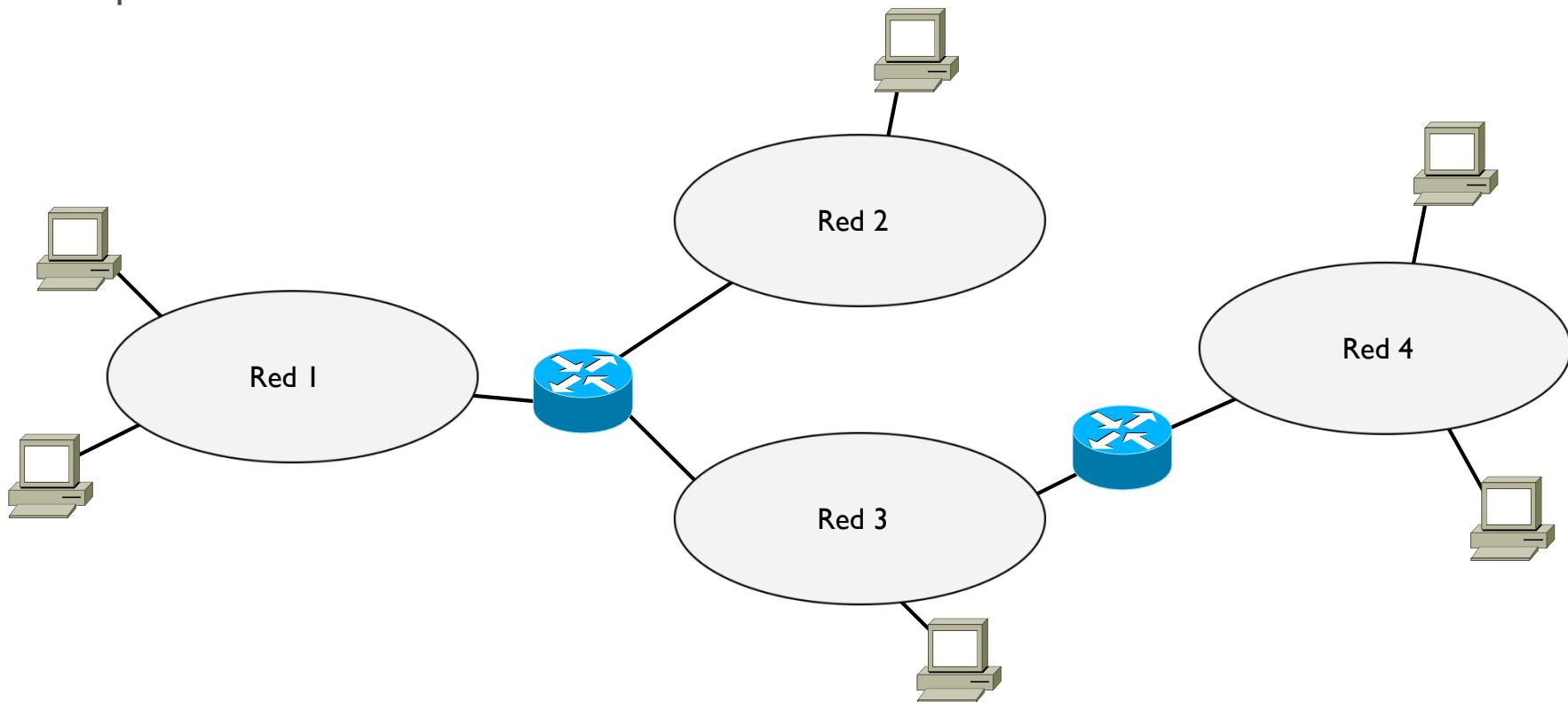


- ▶ Simplificamos el dibujo y las tres las dibujamos de esta manera

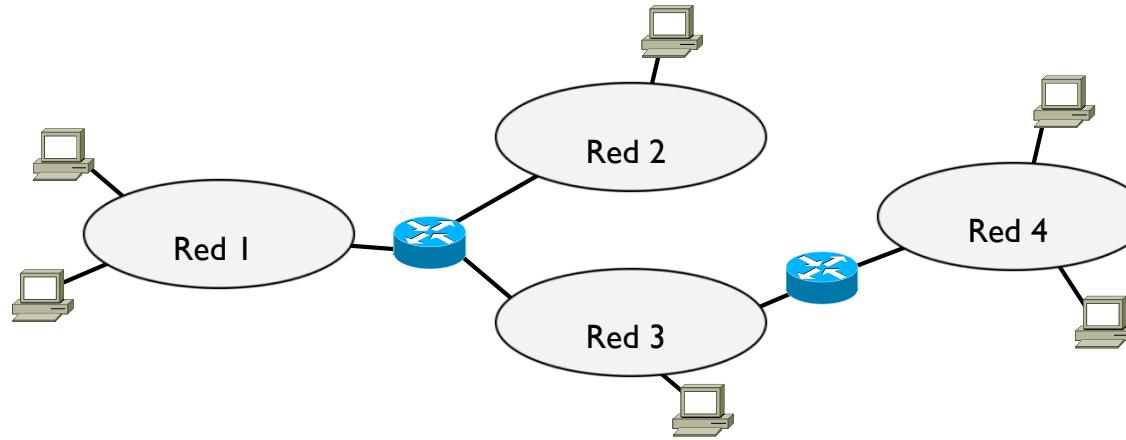


Tema 2 – Direcccionamiento IP

- ▶ Otro ejemplo
- ▶ Nos dicen
 - ▶ Mascaras /16
 - ▶ A partir de 147.8.0.0



Tema 2 – Direcccionamiento IP

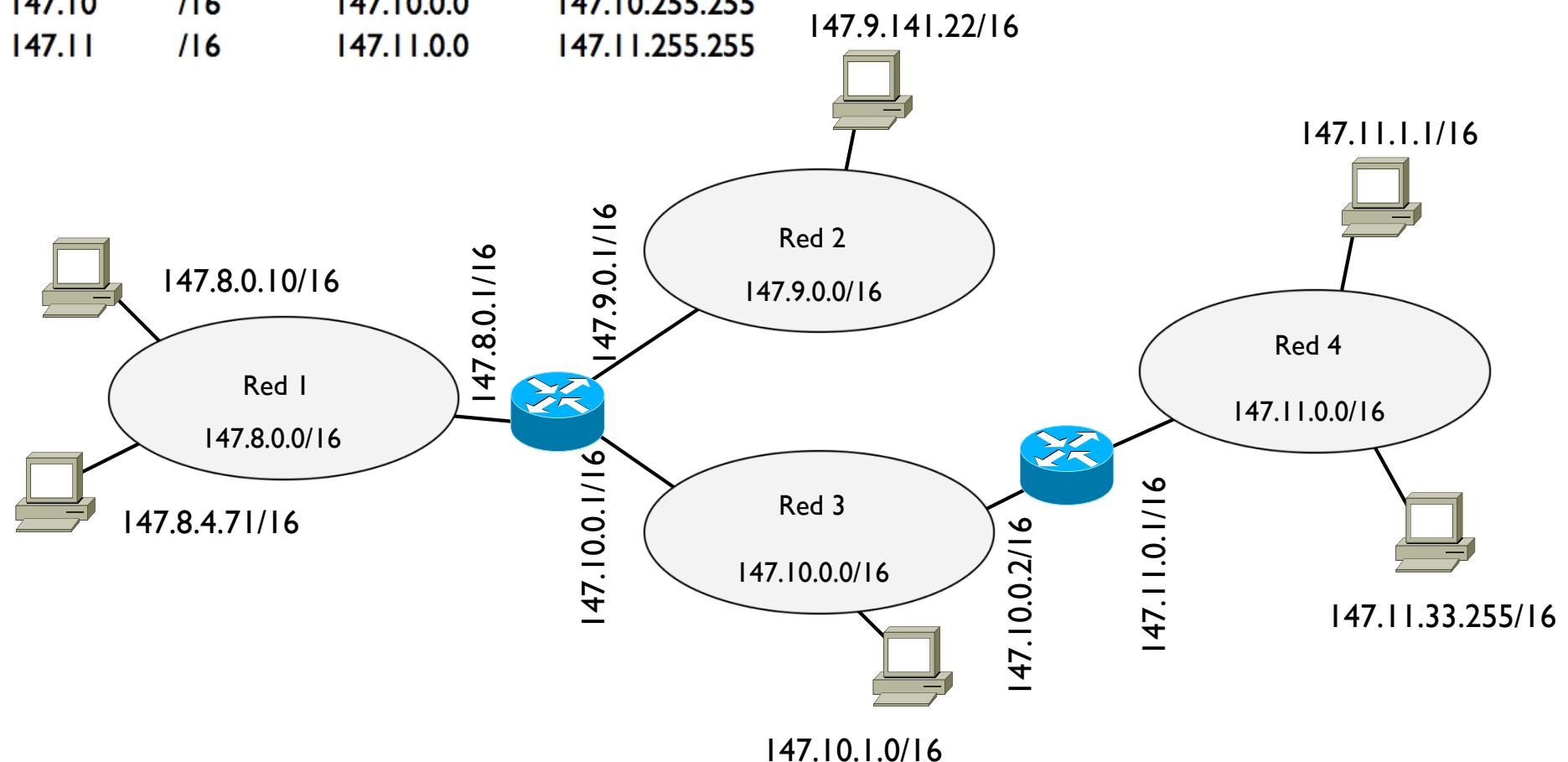


Red	netID	mascara	dirección de red	dirección broadcast
1	147.8	/16	147.8.0.0	147.8.255.255
2	147.9	/16	147.9.0.0	147.9.255.255
3	147.10	/16	147.10.0.0	147.10.255.255
4	147.11	/16	147.11.0.0	147.11.255.255



Tema 2 – Direcccionamiento IP

Red	netID	mascara	dirección de red	dirección broadcast
1	147.8	/16	147.8.0.0	147.8.255.255
2	147.9	/16	147.9.0.0	147.9.255.255
3	147.10	/16	147.10.0.0	147.10.255.255
4	147.11	/16	147.11.0.0	147.11.255.255



Tema 2 – Mascaras “menos” fáciles

- ▶ Ejemplos
 - ▶ 88.101.100.47 / 255.255.255.192
- 192 en binario es 1100 0000
 - ▶ La mascara es por lo tanto de $24 + 2 = 26$ bits
- 47 en binario es 0010 1111
 - ▶ netID = 88.101.100.00
 - ▶ hostID = 10 1111



Tema 2 – Mascaras “menos” fáciles

- ▶ Ejemplos
 - ▶ 172.192.24.77 / 255.255.240.0
- 240 en binario es 1111 0000
 - ▶ La mascara es por lo tanto de 16 + 4 = 20 bits
- Cae en el tercer decimal de la @IP
24 en binario es 0001 1000
 - ▶ netID = 172.192.0001
 - ▶ hostID = 1000.77



Tema 2 – Direccionamiento IP

- ▶ **Clases**
 - ▶ Si no se asigna una máscara a una @IP, por defecto se consideran las clases para saber el número de bits de netID y hostID
- ▶ **Clase A**
 - ▶ De 0.0.0.0 a 127.255.255.255 el netID es de 8 bits y el hostID de 24 bits
 - ▶ Todas aquellas @IP que empiezan con el bit más significativo a 0
- ▶ **Clase B**
 - ▶ De 128.0.0.0 a 191.255.255.255 el netID es de 16 bits y el hostID de 16 bits
 - ▶ Todas aquellas @IP que empiezan con los dos bits más significativos a 10
- ▶ **Clase C**
 - ▶ De 192.0.0.0 a 223.255.255.255 el netID es de 24 bits y el hostID de 8 bits
 - ▶ Todas aquellas @IP que empiezan con los tres bits más significativos a 110



Tema 2 – Direcccionamiento IP

▶ Clase D

- ▶ Para direcciones multicast (no se pueden usar como @IP de interfaces)
- ▶ De 224.0.0.0 a 239.255.255.255
- ▶ Todas aquellas @IP que empiezan con los 4 bits más significativo a 1110

▶ Clase E

- ▶ Reservados (tampoco se pueden usar como @IP de interfaces)
- ▶ De 240.0.0.0 a 255.255.255.255
- ▶ Todas aquellas @IP que empiezan con los 4 bits más significativo a 1111



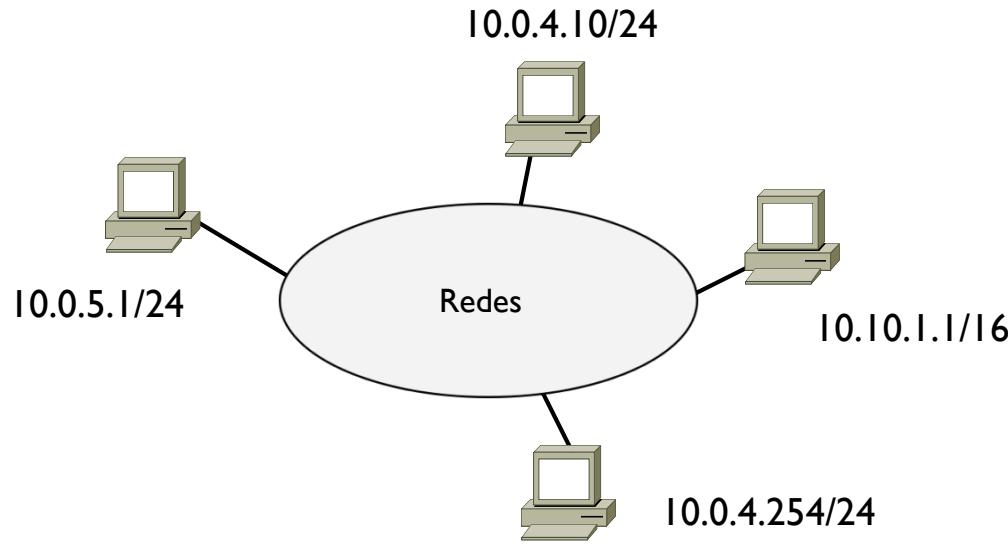
Tema 2 – Direcccionamiento IP

- ▶ El sistema con clases es el método original para saber el netID y hostID de una @IP
 - ▶ Este método resultó muy poco flexibles ya que permitía solo determinadas máscaras y tamaño de redes
-
- ▶ Se estandarizó el método Classless InterDomain Routing (CIDR)
 - ▶ RFC 1517-1520 y 1817
 - ▶ Permite el uso de máscaras
 - ▶ Los routers se pueden configurar como
 - ▶ Classfull → cuenta la clase de la dirección
 - ▶ Classless → cuenta la máscara de la dirección



Tema 2 – Direcccionamiento IP

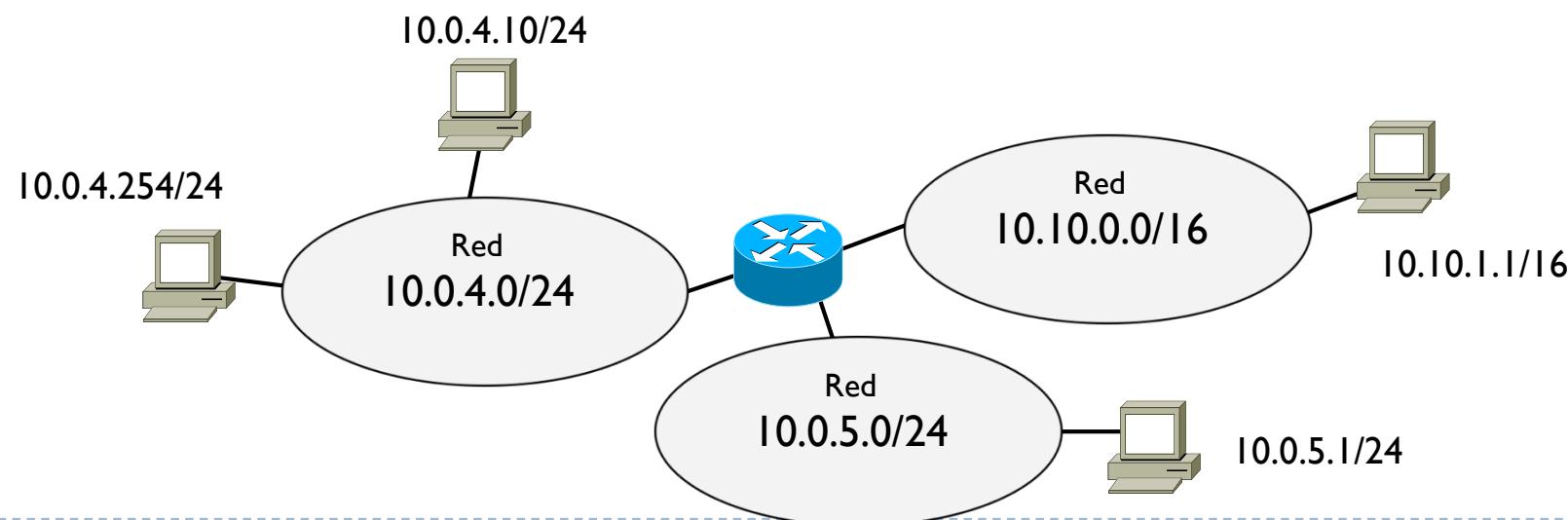
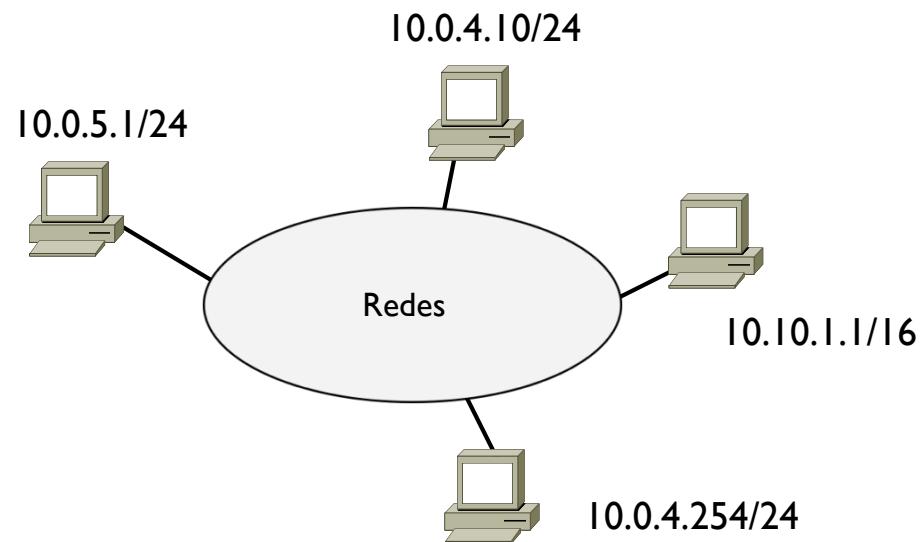
▶ Ejemplo



- ▶ ¿cuántas redes hay?
 - ▶ ¿cuál podría ser la configuración?
-

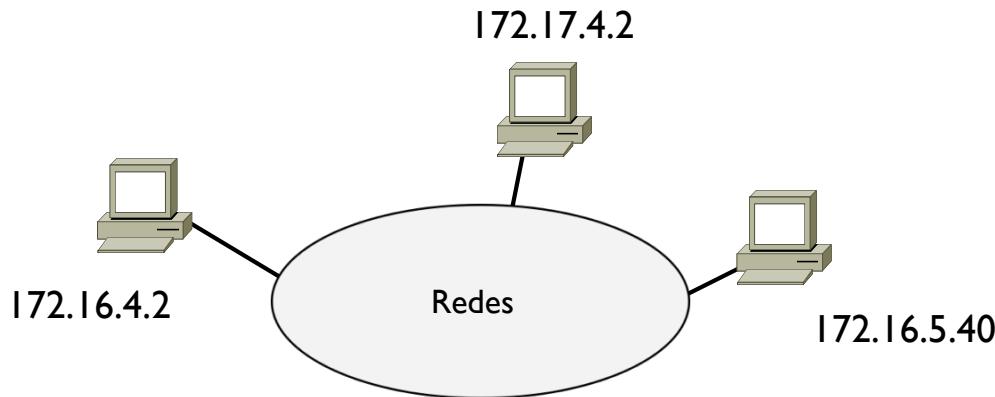
Tema 2 – Direccionamiento IP

- ▶ Contar los netID diferentes
 - ▶ 10.0.4
 - ▶ 10.0.5
 - ▶ 10.10
- 3 netID → 3 redes
- ▶ Una posible configuración



Tema 2 – Direcccionamiento IP

- ▶ Otro ejemplo

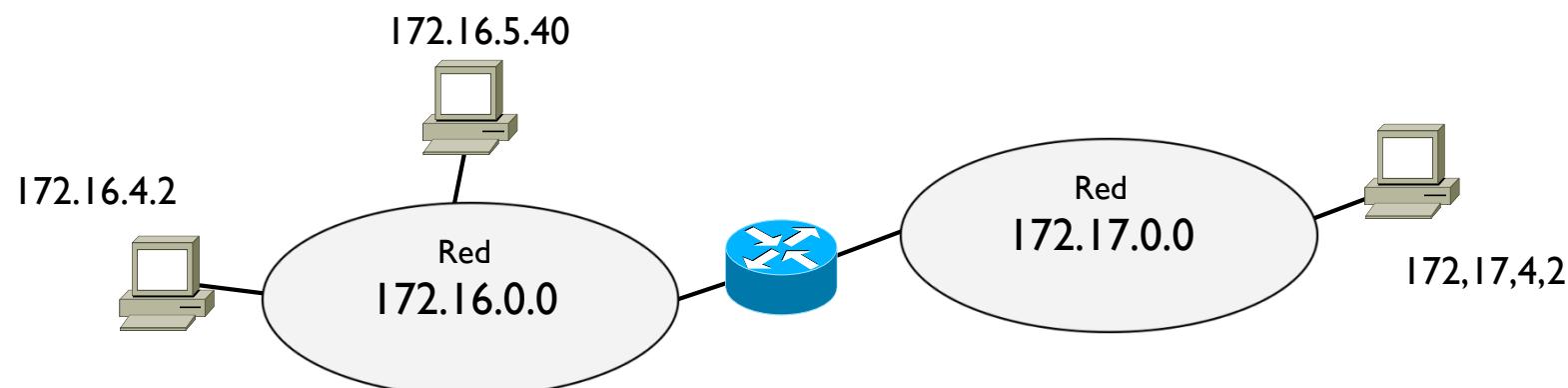
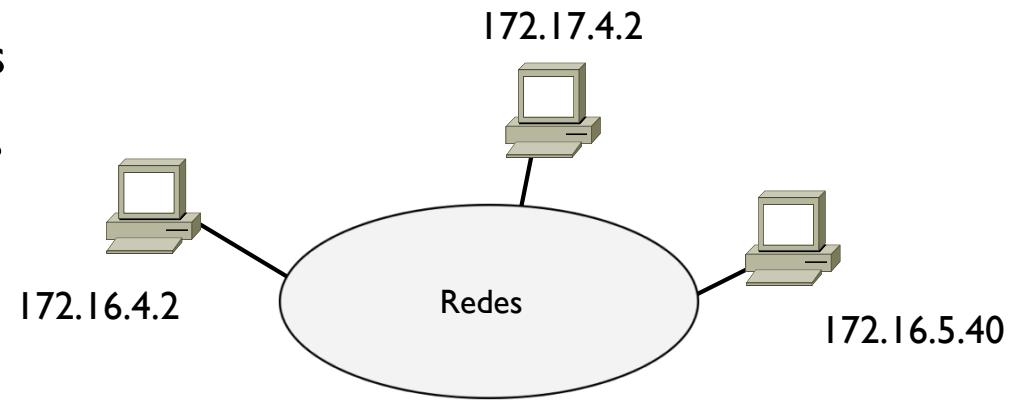


- ▶ ¿cuántas redes hay?
- ▶ ¿cuál podría ser la configuración?



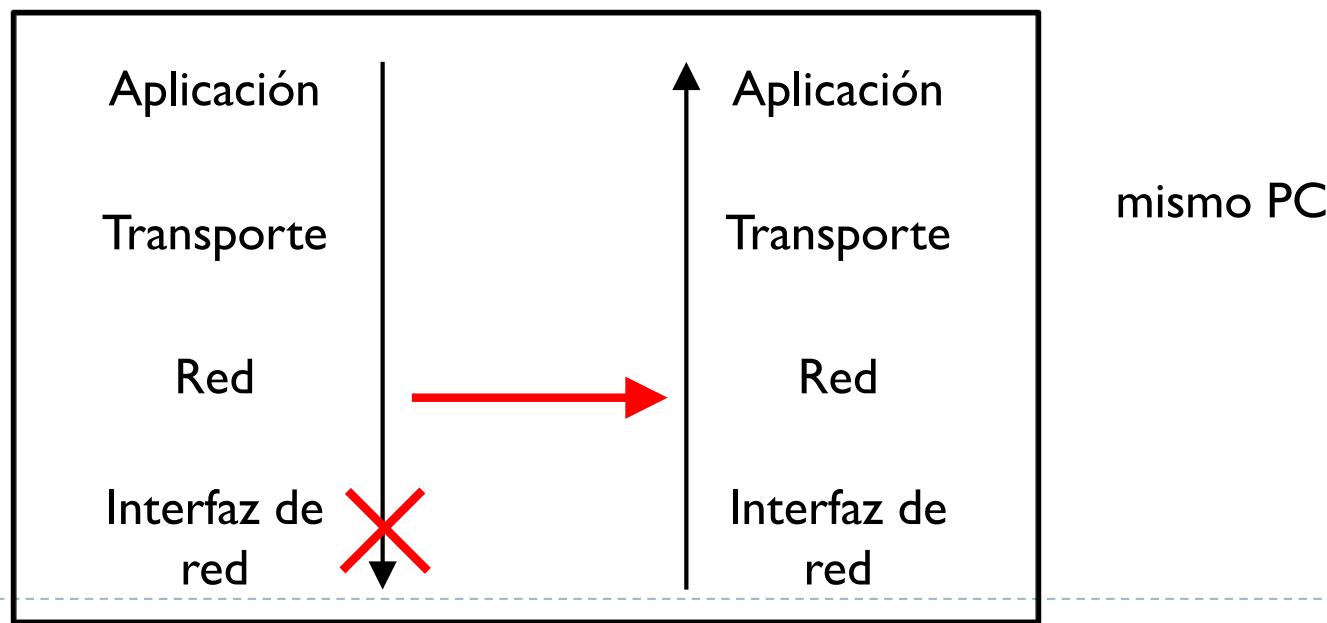
Tema 2 – Direccionamiento IP

- ▶ No hay mascaras, se usan las clases
- ▶ Todas son clase B, netID de 16 bits
- ▶ 172.16 } 2 netID → 2 redes
- ▶ 172.17 }
- ▶ Una posible configuración



Tema 2 – Direcccionamiento IP

- ▶ Direcciones particulares
- ▶ 0.0.0.0 → dirección inicial asignada a cada interfaz al arrancar
 - ▶ no es una dirección valida, no se puede usar
- ▶ 127.0.0.1 → dirección de loopback
 - ▶ Permite a dos aplicaciones lanzadas en una misma maquina comunicarse entre ellas como si estuvieran conectadas en red



Tema 2 – Direcccionamiento IP

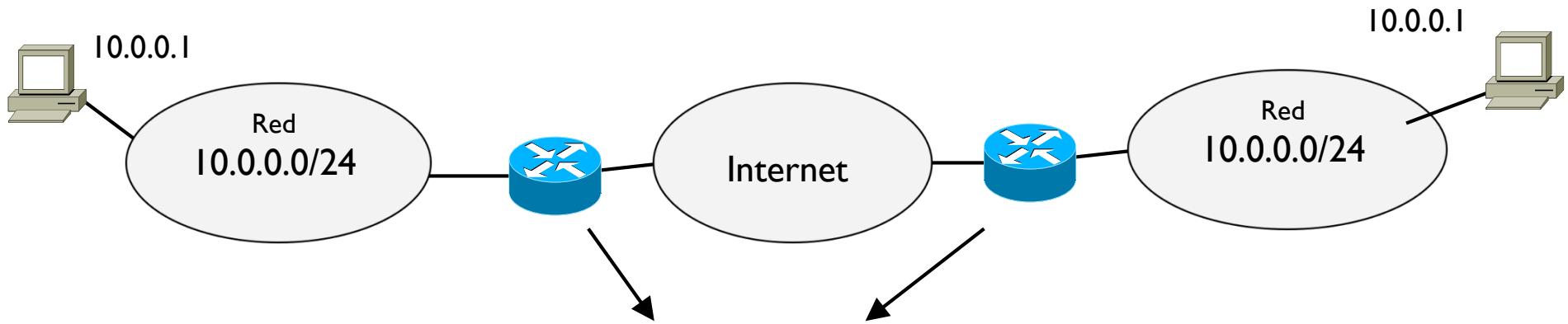
- ▶ **Direcciones privadas**
 - ▶ Direcciones que se recomienda usar en redes de área local
 - ▶ No se pueden usar para conectarse a Internet
 - ▶ Los routers de Internet descartan datagramas con estas direcciones
 - ▶ De esta manera se pueden duplicar @IP en sitios diferentes

- ▶ 10.0.0.0 – 10.255.255.255
- ▶ 172.16.0.0 – 172.31.255.255
- ▶ 192.168.0.0 – 192.168.255.255



Tema 2 – Direccionamiento IP

- ▶ Para que una red IP funcione, todos las @IP deben ser distintas
- ▶ Pero hay un número limitado de @IP
 - ▶ $2^{32} = 4$ mil millones de @IP
- ▶ Para aliviar esta restricción, se usan direcciones privadas



Para que haya dialogo entre los hosts pasando por Internet, estos dos routers deben “traducir” estas direcciones privadas a direcciones públicas, y mantener la unicidad de @IP en Internet
→ Mecanismo NAT (veremos más adelante)



Tema 2 – Subnetting

- ▶ RFC 950 y sus referencias en el documento
 - ▶ Eficiencia y flexibilidad, facilitar la gestión de redes, etc.
- ▶ Idea: de una única dirección de red, construir varias redes cumpliendo con determinados requisitos
 - ▶ Ejemplo: un ISP proporciona un rango de direcciones a una empresa para conectarse a Internet



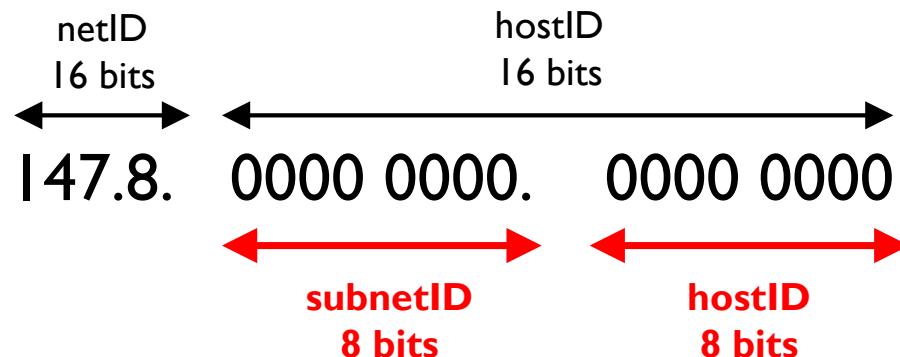
Tema 2 – Subnetting

- ▶ Ejemplo
 - ▶ Se proporciona el rango 147.8.0.0/16
- ▶ ¿cuántos hosts se pueden conectar a esta red?
 - ▶ 16 bits para el hostID → $2^{16} = 65536$
 - ▶ 2 @IP están reservadas para dirección de red y de broadcast
 - ▶ Quedan 65534 @IP para los hosts pero ...
 - ▶ ... no tiene ningún sentido tener una única red con 65534 hosts



Tema 2 – Subnetting

- ▶ Se usa subnetting, extendiendo el netID y ocupando más bits (subnetID)

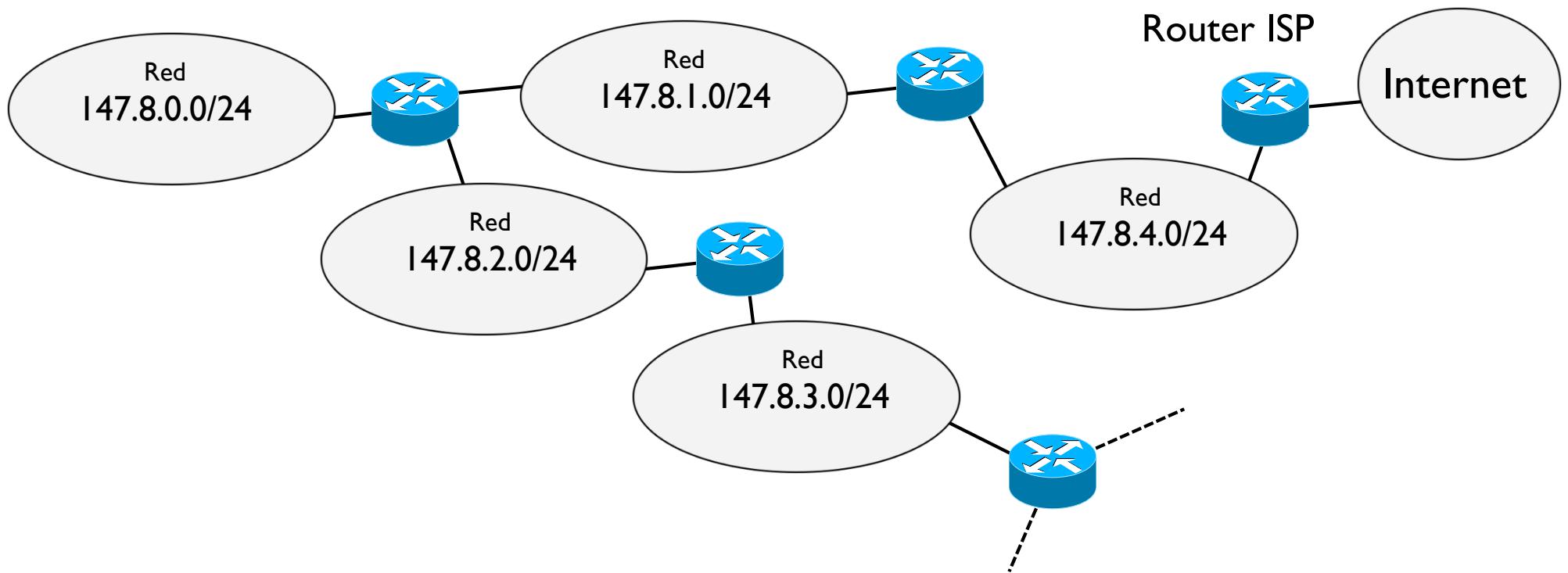


- ▶ Y creando varios netID distintos de 24 bits en lugar de 16
- ▶ 147.8.**0000 0000**. → 147.8.0.
- ▶ 147.8.**0000 0001**. → 147.8.1.
- ▶ 147.8.**0000 0010**. → 147.8.2.
- ▶ 147.8.**0000 0011**. → 147.8.3.
- ▶ 147.8.**0000 0100**. → 147.8.4.
- ▶ ...

**Cada netID diferente
identificará una red
diferente**

Tema 2 – Subnetting

- ▶ Por ejemplo



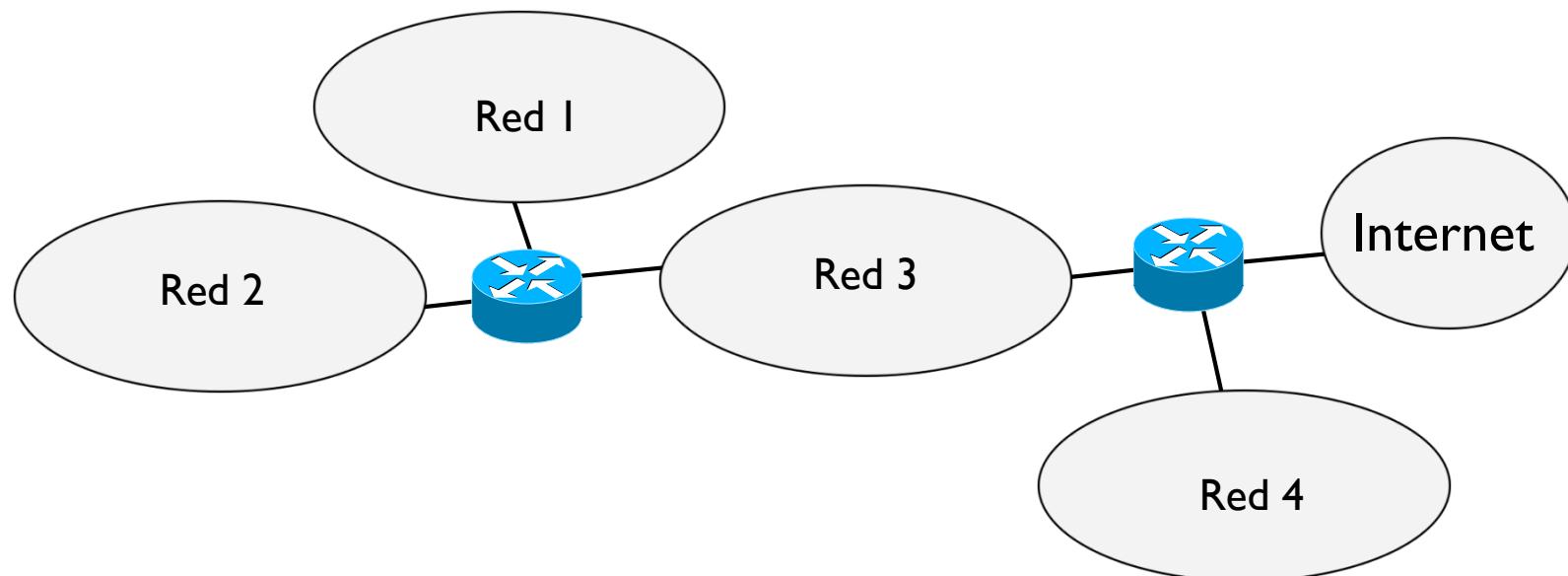
Tema 2 – Subnetting

- ▶ ¿cuántas redes se han creado?
 - ▶ subnetID de 8 bits → $2^8 = 256$ netID → 256 redes
- ▶ ¿cuántos hosts tendrá como máximo cada red?
 - ▶ hostID de 8 bits → $2^8 = 256$ hostID
 - ▶ Hay que restar 1 dirección de red y 1 dirección de broadcast
 - ▶ $256 - 2 = 254$ @IP
- ▶ ¿En total cuantas @IP habrá?
 - ▶ 256 redes con 254 @IP cada una = $256 * 254 = 65024$ @IP
- ▶ ¿se han perdido @IP respecto al caso de una única red?
 - ▶ Antes 65534 @IP – ahora 65024 @IP = se pierden 510 @IP
 - ▶ Se gana en flexibilidad



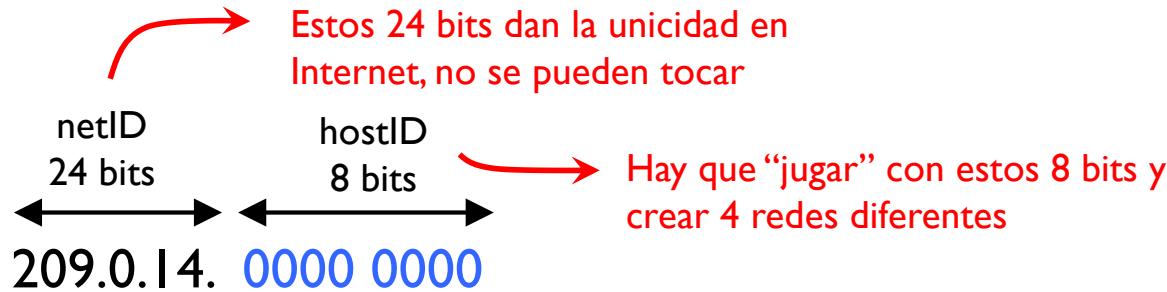
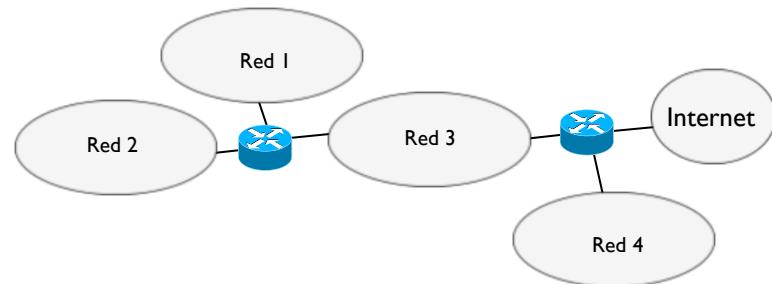
Tema 2 – Subnetting

- ▶ Otro ejemplo
- ▶ Se proporciona el rango 209.0.14.0/24 y se quiere determinado un direccionamiento valido para esta red



Tema 2 – Subnetting

- ▶ 4 redes
→ 2 bits de hostID pasan a subnetID



	subnetID	hostID	
	2 bits	6 bits	Se reduce a 6 bits
Red 1	209.0.14. 00 00 0000		
Red 2	209.0.14. 01 00 0000		
Red 3	209.0.14. 10 00 0000		
Red 4	209.0.14. 11 00 0000		



Tema 2 – Subnetting

- ▶ Las direcciones de red serán

Red 1 209.0.14.**00** 00 0000 → 209.0.14.0 / 26 La mascara es ahora de 26 bits

Red 2 209.0.14.**01** 00 0000 → 209.0.14.64 / 26

Red 3 209.0.14.**10** 00 0000 → 209.0.14.128 / 26

Red 4 209.0.14.**11** 00 0000 → 209.0.14.192 / 26

Las @IP entre 209.0.14.1 y 209.0.14.62 son @IP que se pueden asignar a las interfaces de la red 1

- ▶ y las direcciones de broadcast

Red 1 209.0.14.**00** **11** **1111** → 209.0.14.63

Red 2 209.0.14.**01** **11** **1111** → 209.0.14.127

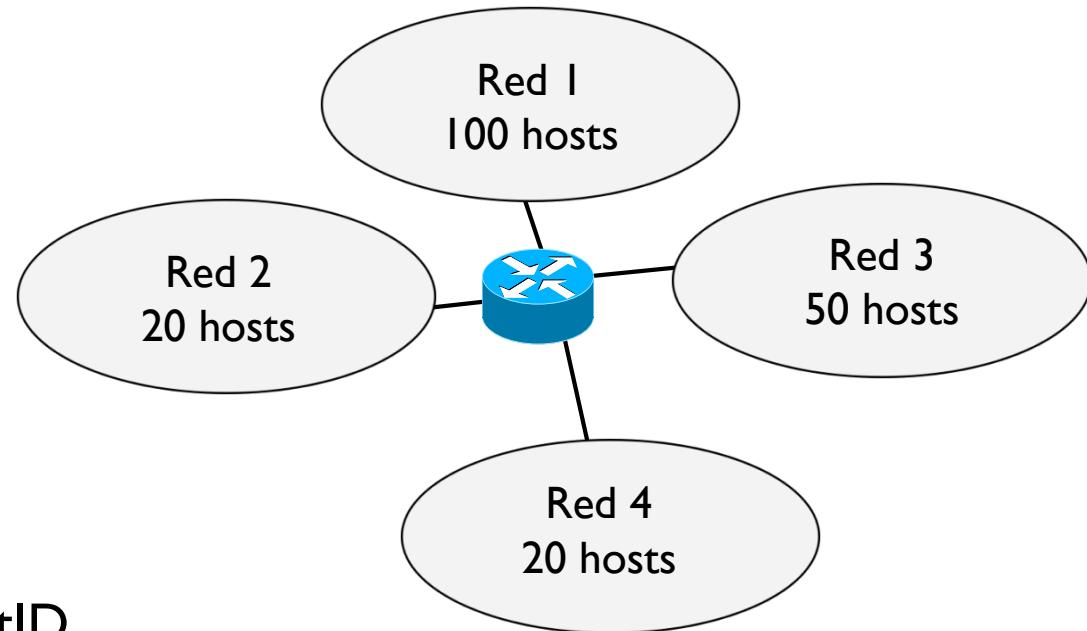
Red 3 209.0.14.**10** **11** **1111** → 209.0.14.191

Red 4 209.0.14.**11** **11** **1111** → 209.0.14.255

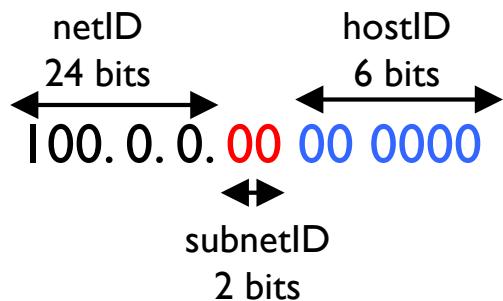


Tema 2 – Subnetting

- ▶ Otro ejemplo
- ▶ Se proporciona el rango 100.0.0.0/24



- ▶ 4 redes → 2 bits de subnetID



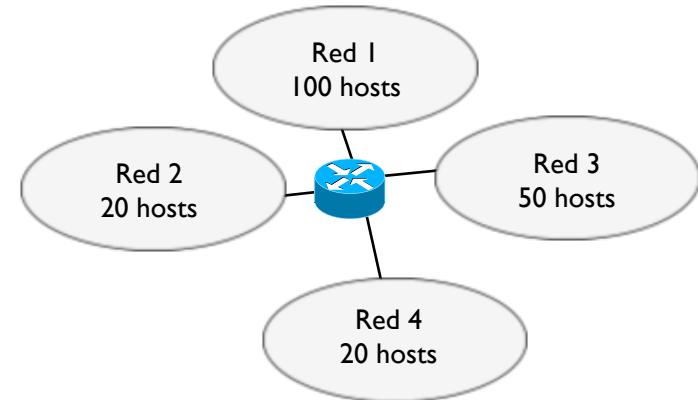
PROBLEMA!

Con 6 bits de hostID al máximo hay $2^6 = 64$ direcciones disponibles

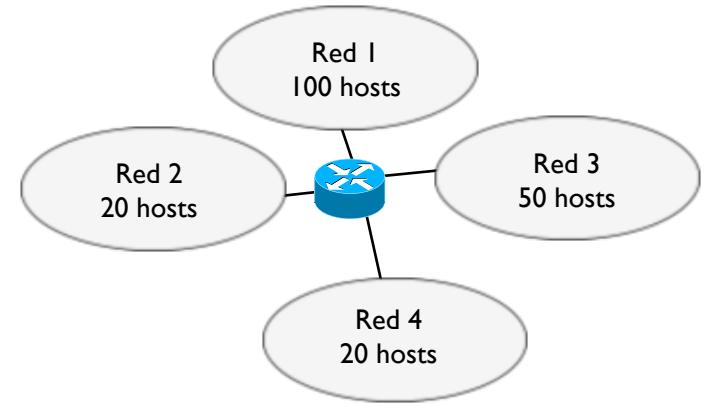
No suficientes para los 100 hosts de la red I

Tema 2 – Subnetting

- ▶ Hay que usar máscaras variables
 - ▶ Conviene empezar siempre con la red de mayor tamaño e ir en orden decreciente
- ▶ Red 1
 - ▶ 100 hosts + dirección de red + broadcast + @IP router = 103 @IP
 - ▶ Se busca la potencia de dos más proxima a 103 y que lo supere
 - ▶ → $2^6 = 64$ → no suficientes
 - ▶ → $2^7 = 128$ → deben ser 7 bits de hostID para direccionar 103 @IP
- ▶ Red 3
 - ▶ 50 hosts + dirección de red + broadcast + @IP router = 53 @IP
 - ▶ → $2^5 = 32$ → no suficientes
 - ▶ → $2^6 = 64$ → deben ser 6 bits de hostID para direccionar 53 @IP



Tema 2 – Subnetting



- ▶ **Red 2**
 - ▶ 20 hosts + dirección de red + broadcast + @IP router = 23 @IP
 - ▶ $\rightarrow 2^4 = 16 \rightarrow$ no suficientes
 - ▶ $\rightarrow 2^5 = 32 \rightarrow$ deben ser 5 bits de hostID

- ▶ **Red 3**
 - ▶ 20 hosts + dirección de red + broadcast + @IP router = 23 @IP
 - ▶ $\rightarrow 2^4 = 16 \rightarrow$ no suficientes
 - ▶ $\rightarrow 2^5 = 32 \rightarrow$ deben ser 6 bits de hostID



Tema 2 – Subnetting

- ▶ Las direcciones de red serán

		subnetID	hostID	
Red 1	100.0.0.	0	000 0000	→ 100.0.0.0 / 25
Red 3	100.0.0.	10 00 0000		→ 100.0.0.128 / 26
Red 2	100.0.0.	110 0 0000		→ 100.0.0.192 / 27
Red 4	100.0.0.	111 0 0000		→ 100.0.0.224 / 27

Cuidado que las direcciones no se deben SOLAPAR
Por ejemplo para la red 3 no se puede usar una combinación que empieza con el primer bit del subnetID a 0 ya que se solaparía con la red 1

- ▶ y las direcciones de broadcast

Red 1	100.0.0.0	111 1111	→ 100.0.0.127
Red 3	100.0.0.	10 11 1111	→ 100.0.0.191
Red 2	100.0.0.	110 1 1111	→ 100.0.0.223
Red 4	100.0.0.	111 1 1111	→ 100.0.0.255



Tema 2 – Ejercicios

- ▶ Dada una @IP y una mascara encontrar su red y dirección de broadcast
 - ▶ 190.33.109.133/25
 - ▶ 192.168.20.25/28
 - ▶ 27.14.2.71/13
-
- ▶ Es una @IP?
 - ▶ 82.74.0.0/14
 - ▶ 192.168.4.0/22
 - ▶ 172.16.22.192/25



Tema 2 – Ejercicios

- ▶ Encontrar un direccionamiento valido

- ▶ Rango inicial: 192.168.0.0/24
- ▶ Requisitos: 4 redes de 50 @IP

- ▶ Rango inicial: 20.4.4.0/22
- ▶ Requisitos: 4 redes de 200 @IP

- ▶ Rango inicial: 192.168.0.0/24
- ▶ Requisitos:
 - ▶ 3 red con 50 @IP
 - ▶ 2 red con 20 @IP



Tema 2 – Direccionamiento

- ▶ Internet requiere que todas las @IP sean distintas para poder identificar y localizar cada una de ella de manera inequívoca
 - ▶ Las @IP que se usan en Internet se llaman @IP publicas
 - ▶ Las @IP privadas no se transmiten por Internet (ya que se pueden usar y reusar en redes distintas y habría @IP duplicadas)
- ▶ Para que se respete esta unicidad, hay un organismo internacional que gestiona las @IP de Internet
 - ▶ Internet Assigned Number Authority (IANA), www.iana.org
 - ▶ Este organismo no proporciona las @IP a los usuarios directamente
 - ▶ Asigna bloques de direcciones libres a organismos regionales llamados RIR (Regional Internet Registry)
 - ▶ Hay 5 en el mundo
 - ▶ Los RIR asignan bloques más pequeños a los ISP
 - ▶ Los ISP son los que alquilan finalmente las @IP a los usuarios



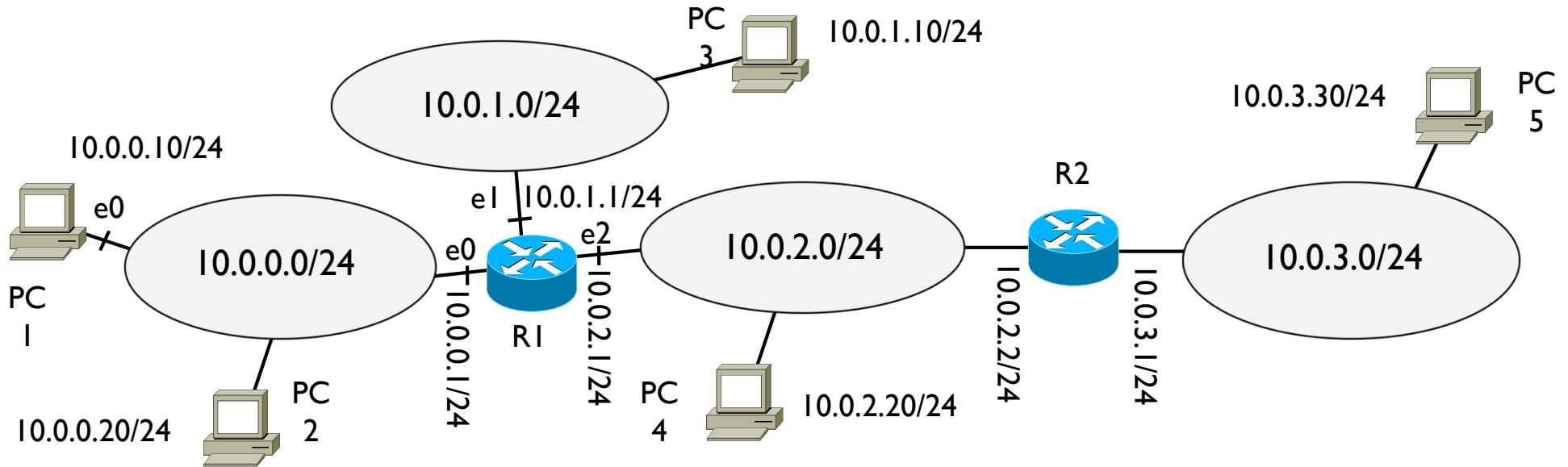
Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – Encaminamiento IP

- ▶ Manera con la cual los datagramas “caminan” por la red



- ▶ ¿Como sabe PC1 que existen PC2, PC3, ...?
 - ▶ ¿Cómo puede transmitirles datagramas?
- **Tabla de encaminamiento**
 - ▶ Base de datos que tiene cada router y host
 - ▶ Contiene la información necesaria para alcanzar todos los destinos

Tema 2 – Encaminamiento IP

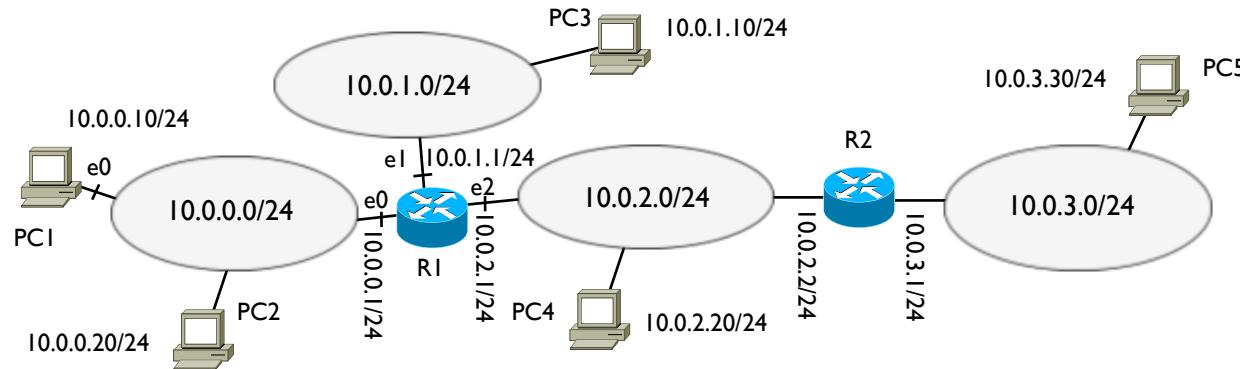


Tabla de encaminamiento de PC1

Adquisición	Destino	mascara	gateway	interfaz
Indica como se ha adquirido una entrada en la tabla	Indican cual son los destinos alcanzables por este dispositivo en terminos de @IP y mascara Los destinos pueden ser @IP, direcciones de red o todos los destinos		Indica si para alcanzar un destino se necesita pasar por un router o si el destino está en la misma red	Indica por que interfaz hay que transmitir para llegar al destino

Cada entrada de esta tabla forma lo que se llama una ruta hacia un destino

- Una ruta entre origen y destino se determina como suma de siguientes pasos (o saltos)
- Es decir cada elemento de esta red determina solo una parte de la ruta entera

Tema 2 – Encaminamiento IP

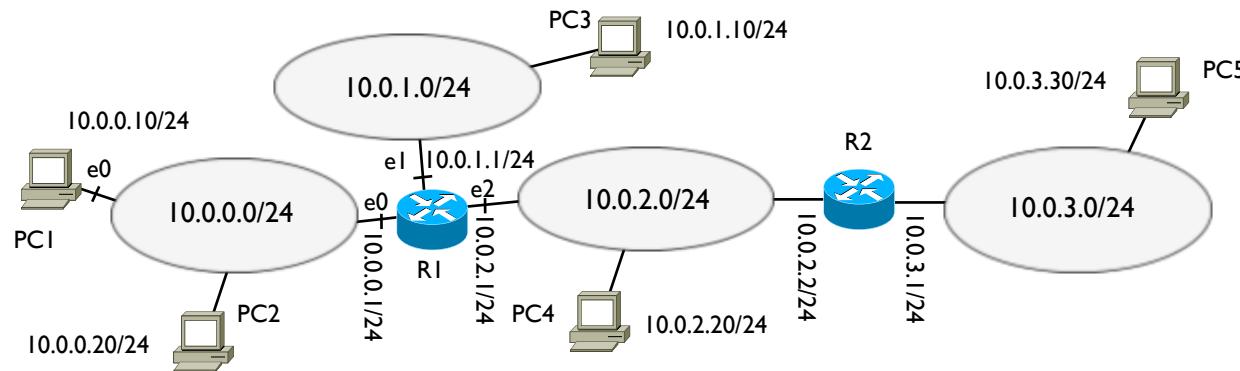


Tabla de encaminamiento de PC1

Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0

Al configurar la @IP de e0 de PC1, se crea esta entrada
Dice como transmitir a los destinos de 10.0.0.0/24
C: conexión directa (PC1 está conectado a la red 10.0.0.0/24 y puede llegar a todos los destinos de esta red)
Gateway 0.0.0.0: indica que no se necesita pasar por un router, los destinos son locales
e0: indica que hay que usar la interfaz llamada e0 para transmitir

El siguiente paso en este caso es enviar el datagrama al destino que está en la misma red que el origen

Tema 2 – Encaminamiento IP

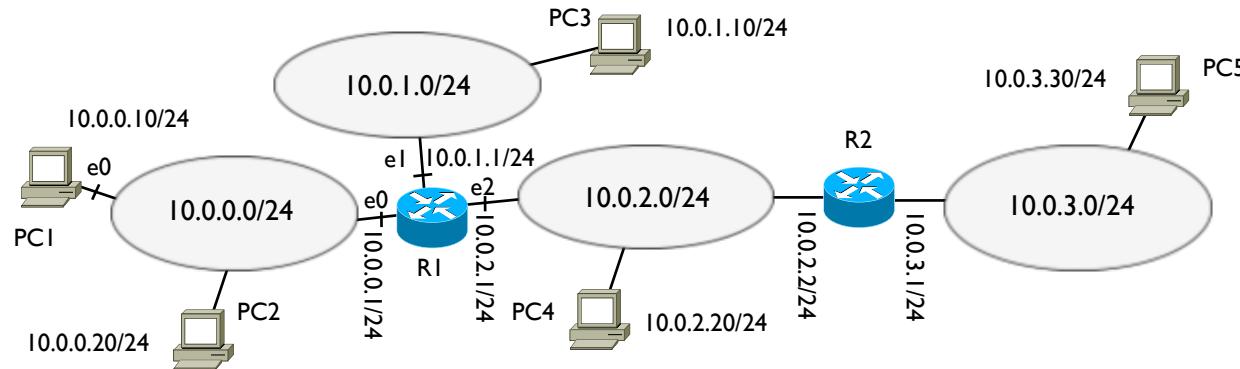


Tabla de encaminamiento de PC1

Adquisición	Destino	mascara	gateway	interfaz
C S Entrada estática (configurada manualmente)	10.0.0.0	255.255.255.0	0.0.0.0	e0
	10.0.1.10 La @IP de un host	255.255.255.255 Son todos 1 ya que todos los bits de la columna Destino identifican el destino	10.0.0.1 Hay que pasar por el router 10.0.0.1 para llegar al destino	e0

El siguiente paso es pasar el datagrama al router 10.0.0.1 transmitiendo por la interfaz e0 para llegar al host 10.0.1.10



Tema 2 – Encaminamiento IP

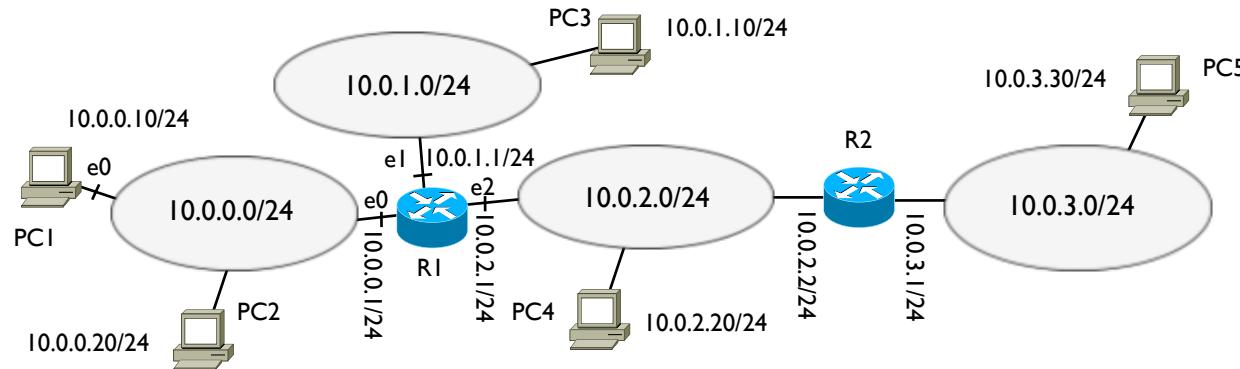


Tabla de encaminamiento de PC1

Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0
S	10.0.2.0	255.255.255.0	10.0.0.1	e0

Entrada estática (configurada manualmente)

Todos los destinos de esta red

Es la mascara de la red destino

Hay que pasar por el router 10.0.0.1 para llegar al destino

El siguiente paso es pasar el datagrama al router 10.0.0.1 transmitiendo por la interfaz e0 para poder llegar a cualquier @IP de la red 10.0.2.0/24



Tema 2 – Encaminamiento IP

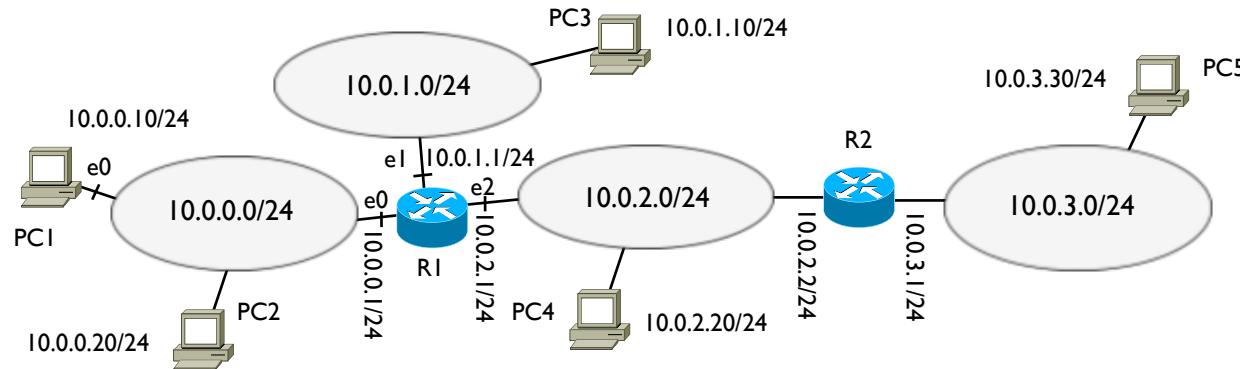


Tabla de encaminamiento de PC1

Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0
S	10.0.2.0	255.255.255.0	10.0.0.1	e0
S	0.0.0.0	0.0.0.0	10.0.0.1	e0

Entrada estática (configurada manualmente)

Cualquier destino

Cualquier mascara

Hay que pasar por el router 10.0.0.1 para llegar al destino

El siguiente paso es pasar el datagrama al router 10.0.0.1 transmitiendo por la interfaz e0 para poder llegar a cualquier @IP con cualquier mascara → ruta por defecto



Tema 2 – Encaminamiento IP

Tabla de encaminamiento de PCI

Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0
S	10.0.2.0	255.255.255.0	10.0.0.1	e0
S	0.0.0.0	0.0.0.0	10.0.0.1	e0

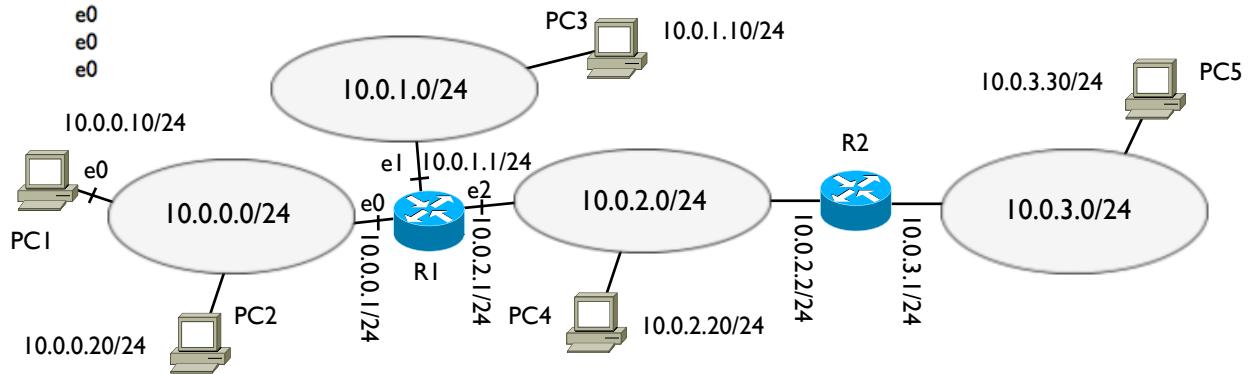


Tabla de encaminamiento de R1

Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0
C	10.0.1.0	255.255.255.0	0.0.0.0	e1
C	10.0.2.0	255.255.255.0	0.0.0.0	e2
S	10.0.3.0	255.255.255.0	10.0.2.2	e2



Tema 2 – Encaminamiento IP

Tabla de encaminamiento de PCI

Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0
S	10.0.2.0	255.255.255.0	10.0.0.1	e0
S	0.0.0.0	0.0.0.0	10.0.0.1	e0

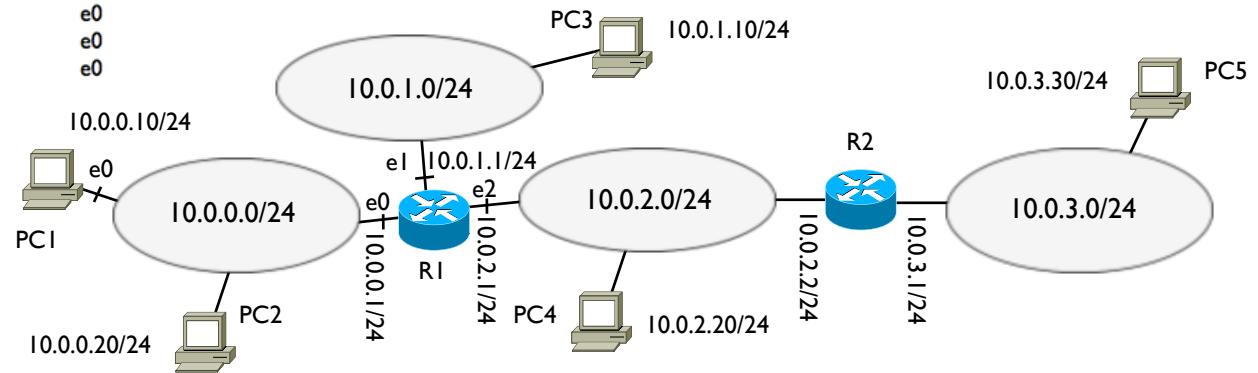


Tabla de encaminamiento de R1

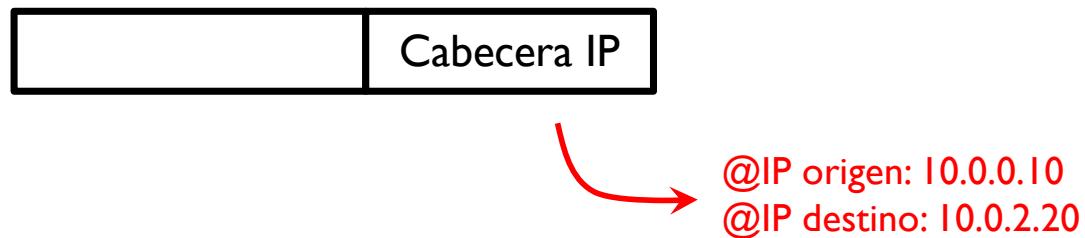
Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0
C	10.0.1.0	255.255.255.0	0.0.0.0	e1
C	10.0.2.0	255.255.255.0	0.0.0.0	e2
S	10.0.3.0	255.255.255.0	10.0.2.2	e2
S	10.0.3.30	255.255.255.255	10.0.2.2	e2



Tema 2 – Encaminamiento IP

Tabla de encaminamiento de PCI					Tabla de encaminamiento de RI				
Adquisición	Destino	mascara	gateway	interfaz	Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0	C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0	C	10.0.1.0	255.255.255.0	0.0.0.0	e1
S	10.0.2.0	255.255.255.0	10.0.0.1	e0	C	10.0.2.0	255.255.255.0	0.0.0.0	e2
S	0.0.0.0	0.0.0.0	10.0.0.1	e0	S	10.0.3.0	255.255.255.0	10.0.2.2	e2

- ▶ Funcionamiento
- ▶ Supongamos PCI quiere transmitir un datagrama a PC4 10.0.2.20



Tema 2 – Encaminamiento IP

Tabla de encaminamiento de PCI					Tabla de encaminamiento de RI				
Adquisición	Destino	mascara	gateway	interfaz	Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0	C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0	C	10.0.1.0	255.255.255.0	0.0.0.0	e1
S	10.0.2.0	255.255.255.0	10.0.0.1	e0	C	10.0.2.0	255.255.255.0	0.0.0.0	e2
S	0.0.0.0	0.0.0.0	10.0.0.1	e0	S	10.0.3.0	255.255.255.0	10.0.2.2	e2

- ▶ PCI mira su tabla y comprueba si el destino está en su misma red
 - 10. 0. 2. 20 AND (operación de AND bit a bit entre @IP y mascara de su red)
 - 255.255.255.0 → su mascara

- 10. 0. 2. 0 diferente de su red 10.0.0.0 → está en otra red

Tema 2 – Encaminamiento IP

Tabla de encaminamiento de PCI					Tabla de encaminamiento de RI				
Adquisición	Destino	mascara	gateway	interfaz	Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0	C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0	C	10.0.1.0	255.255.255.0	0.0.0.0	e1
S	10.0.2.0	255.255.255.0	10.0.0.1	e0	C	10.0.2.0	255.255.255.0	0.0.0.0	e2
S	0.0.0.0	0.0.0.0	10.0.0.1	e0	S	10.0.3.0	255.255.255.0	10.0.2.2	e2

- PCI consulta su tabla de encaminamiento a partir de la entrada con mayor numero de 1 en la mascara → **LONGEST MATCH LOOKUP**

10. 0. 2. 20 AND

255.255.255.255 → mascara mas grande (mayor número de 1)

10. 0. 2. 20 no hay ninguna entrada en la columna Destino con este valor



Tema 2 – Encaminamiento IP

Tabla de encaminamiento de PCI					Tabla de encaminamiento de RI				
Adquisición	Destino	mascara	gateway	interfaz	Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0	C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0	C	10.0.1.0	255.255.255.0	0.0.0.0	e1
S	10.0.2.0	255.255.255.0	10.0.0.1	e0	C	10.0.2.0	255.255.255.0	0.0.0.0	e2
S	0.0.0.0	0.0.0.0	10.0.0.1	e0	S	10.0.3.0	255.255.255.0	10.0.2.2	e2

- PCI consulta su tabla de encaminamiento a partir de la entrada con mayor numero de 1 en la mascara → **LONGEST MATCH LOOKUP**

10. 0. 2. 20 AND

255.255.255.0 → segunda mascara mas grande

Se pasa el datagrama al router,
PCI ha completado su tarea
(encontrar el siguiente paso)

10. 0. 2. 0 la tercera entrada en Destino coincide

→ la tabla dice en este caso enviar a 10.0.0.1 por e0



Tema 2 – Encaminamiento IP

Tabla de encaminamiento de PCI					Tabla de encaminamiento de RI				
Adquisición	Destino	mascara	gateway	interfaz	Adquisición	Destino	mascara	gateway	interfaz
C	10.0.0.0	255.255.255.0	0.0.0.0	e0	C	10.0.0.0	255.255.255.0	0.0.0.0	e0
S	10.0.1.10	255.255.255.255	10.0.0.1	e0	C	10.0.1.0	255.255.255.0	0.0.0.0	e1
S	10.0.2.0	255.255.255.0	10.0.0.1	e0	C	10.0.2.0	255.255.255.0	0.0.0.0	e2
S	0.0.0.0	0.0.0.0	10.0.0.1	e0	S	10.0.3.0	255.255.255.0	10.0.2.2	e2

- RI hará lo mismo, consulta su tabla y comprueba si el destino está en una de sus redes

10. 0. 2. 20 AND

255.255.255.0 → mascara de sus redes

10. 0. 2. 0 coincide con la tercera entrada de la tabla

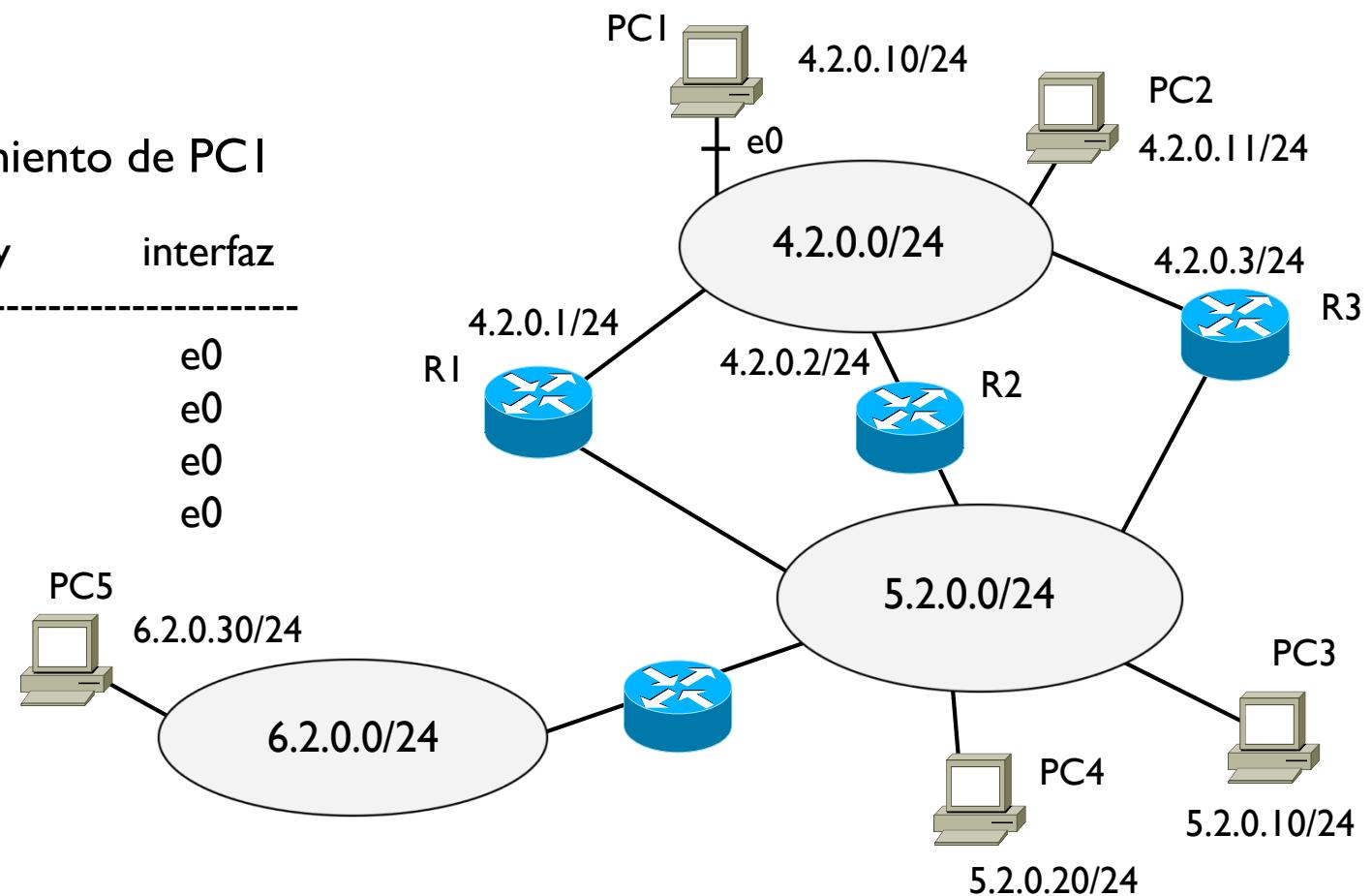
→ la tabla dice enviar por e2 al destino que está en mi red

Tema 2 – Encaminamiento IP

- ▶ El principio del Longest Match Lookup es importante
- ▶ Ejemplo

Tabla de encaminamiento de PCI

Destino/mascara	gateway	interfaz
4.2.0.0/24	0.0.0.0	e0
5.2.0.0/24	4.2.0.2	e0
0.0.0.0/0	4.2.0.1	e0
5.2.0.20/32	4.2.0.3	e0

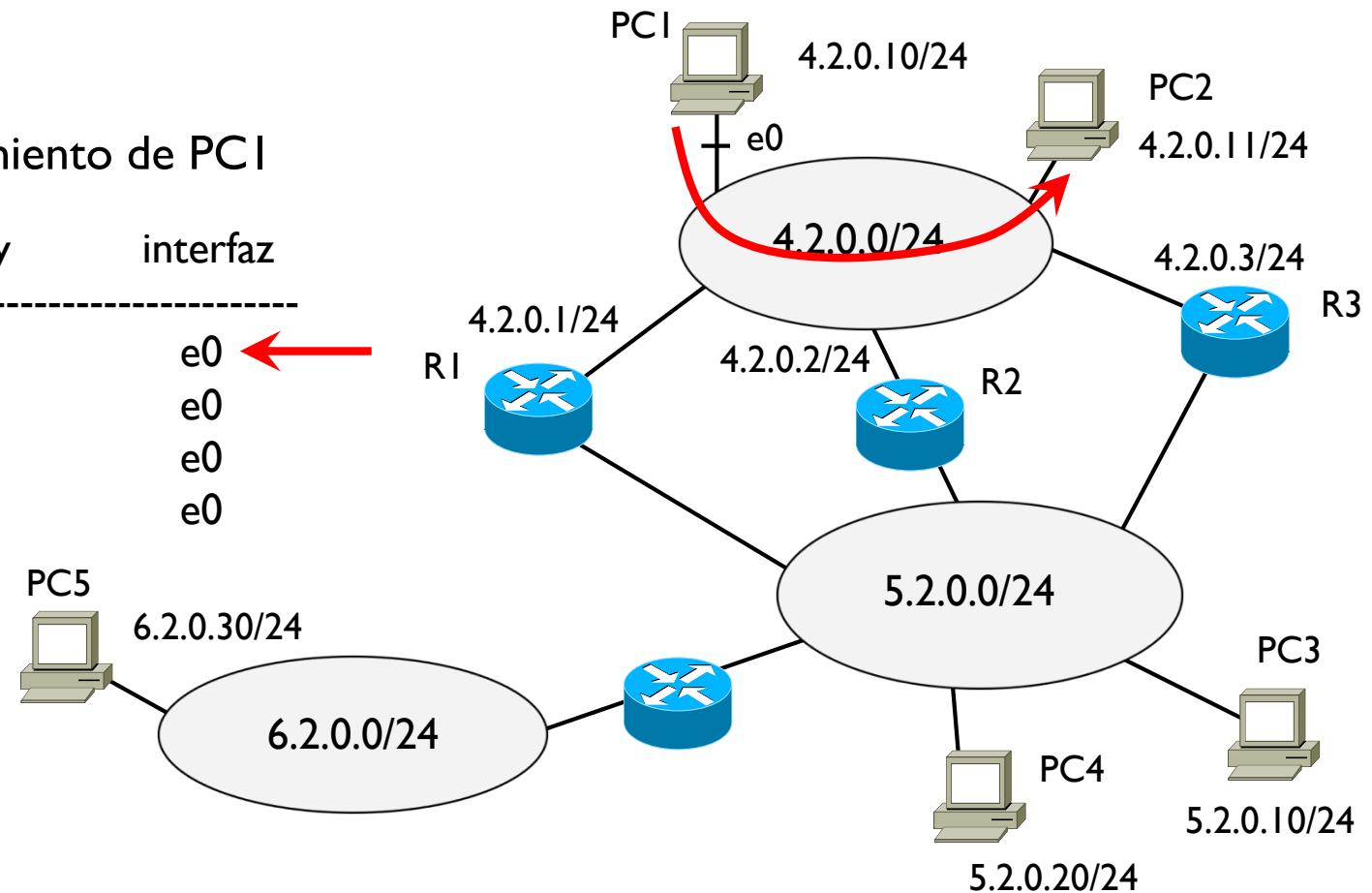


Tema 2 – Encaminamiento IP

- ▶ ¿Si PCI transmite a PC2 4.2.0.11 por donde se pasa?

Tabla de encaminamiento de PCI

Destino/mascara	gateway	interfaz
4.2.0.0/24	0.0.0.0	e0 ←
5.2.0.0/24	4.2.0.2	e0
0.0.0.0/0	4.2.0.1	e0
5.2.0.20/32	4.2.0.3	e0



PC2 pertenece a la misma red de PCI → ruta directa

Tema 2 – Encaminamiento IP

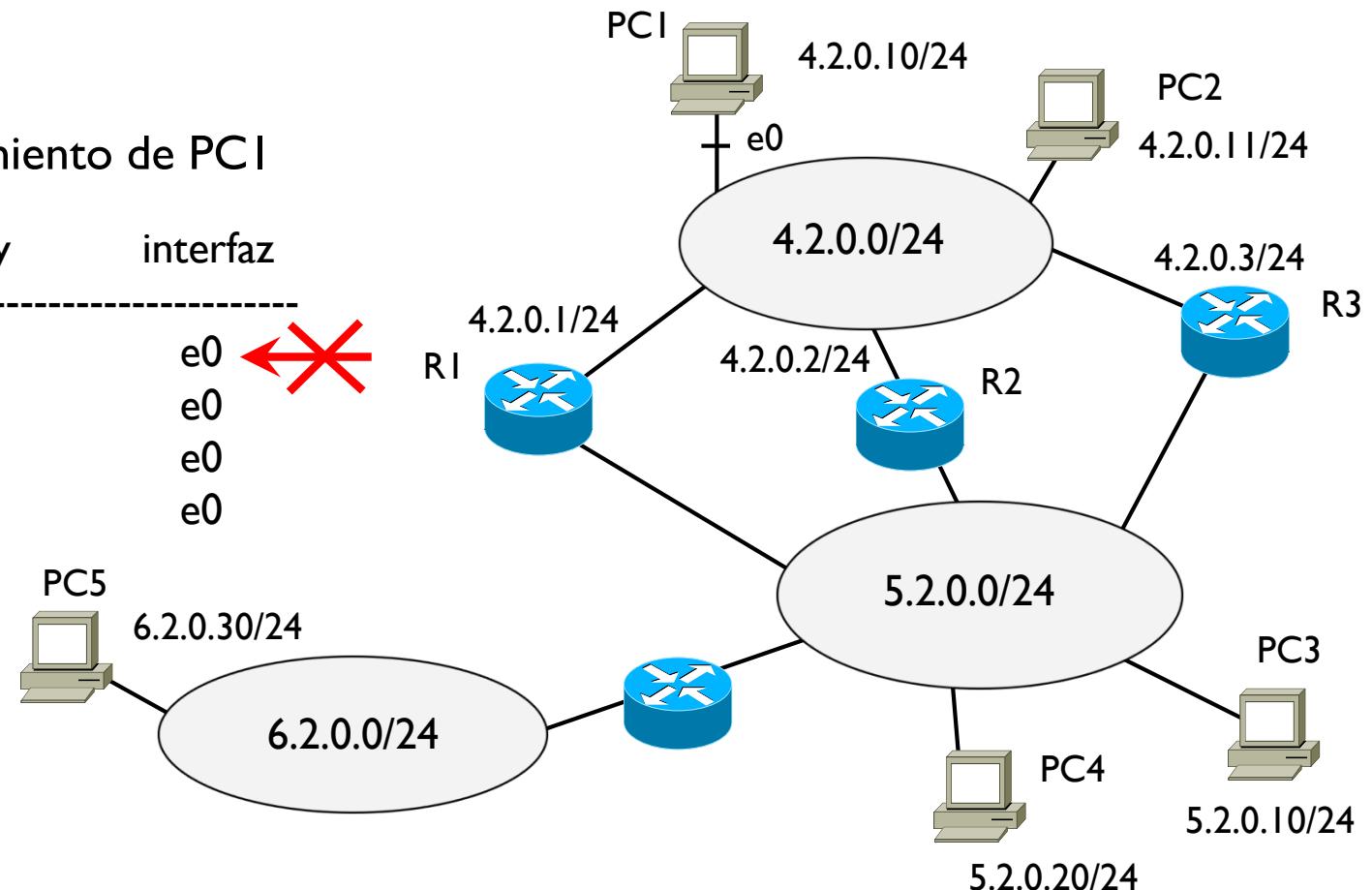
- ▶ ¿Si PCI transmite a PC3 5.2.0.10 por donde se pasa?

Tabla de encaminamiento de PCI

Destino/mascara	gateway	interfaz
4.2.0.0/24	0.0.0.0	e0 ← X
5.2.0.0/24	4.2.0.2	e0
0.0.0.0/0	4.2.0.1	e0
5.2.0.20/32	4.2.0.3	e0

5. 2. 0. 10 AND
255.255.255.0 =

5. 2. 0. 0 != 4.2.0.0



PC3 pertenece a otra red

Tema 2 – Encaminamiento IP

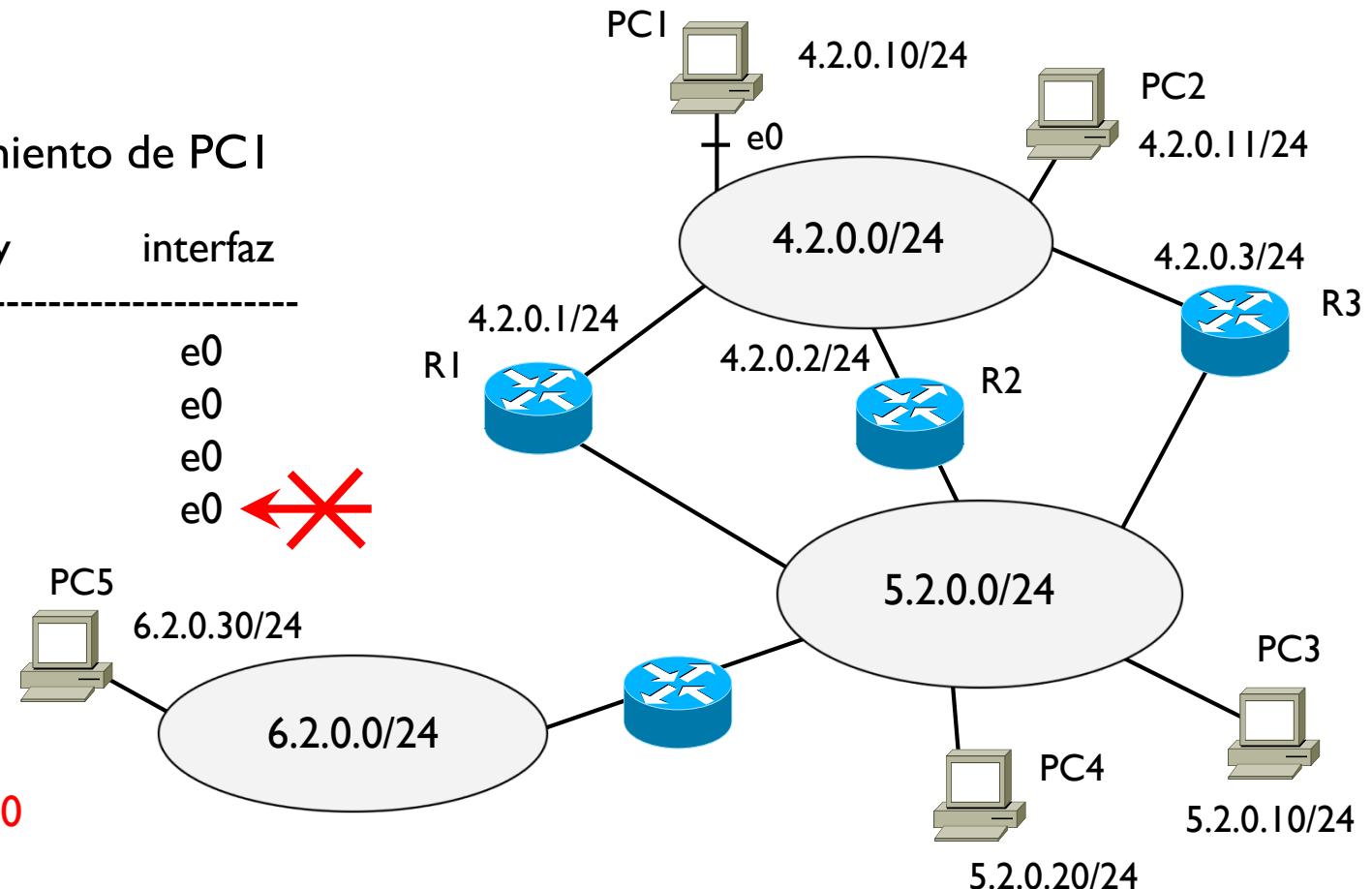
- ▶ ¿Si PCI transmite a PC3 5.2.0.10 por donde se pasa?

Tabla de encaminamiento de PCI

Destino/mascara	gateway	interfaz
4.2.0.0/24	0.0.0.0	e0
5.2.0.0/24	4.2.0.2	e0
0.0.0.0/0	4.2.0.1	e0
5.2.0.20/32	4.2.0.3	e0

5. 2. 0. 10 AND
255.255.255.255 =

5. 2. 0. 10 != 5.2.0.20



No se pasa por esta ruta

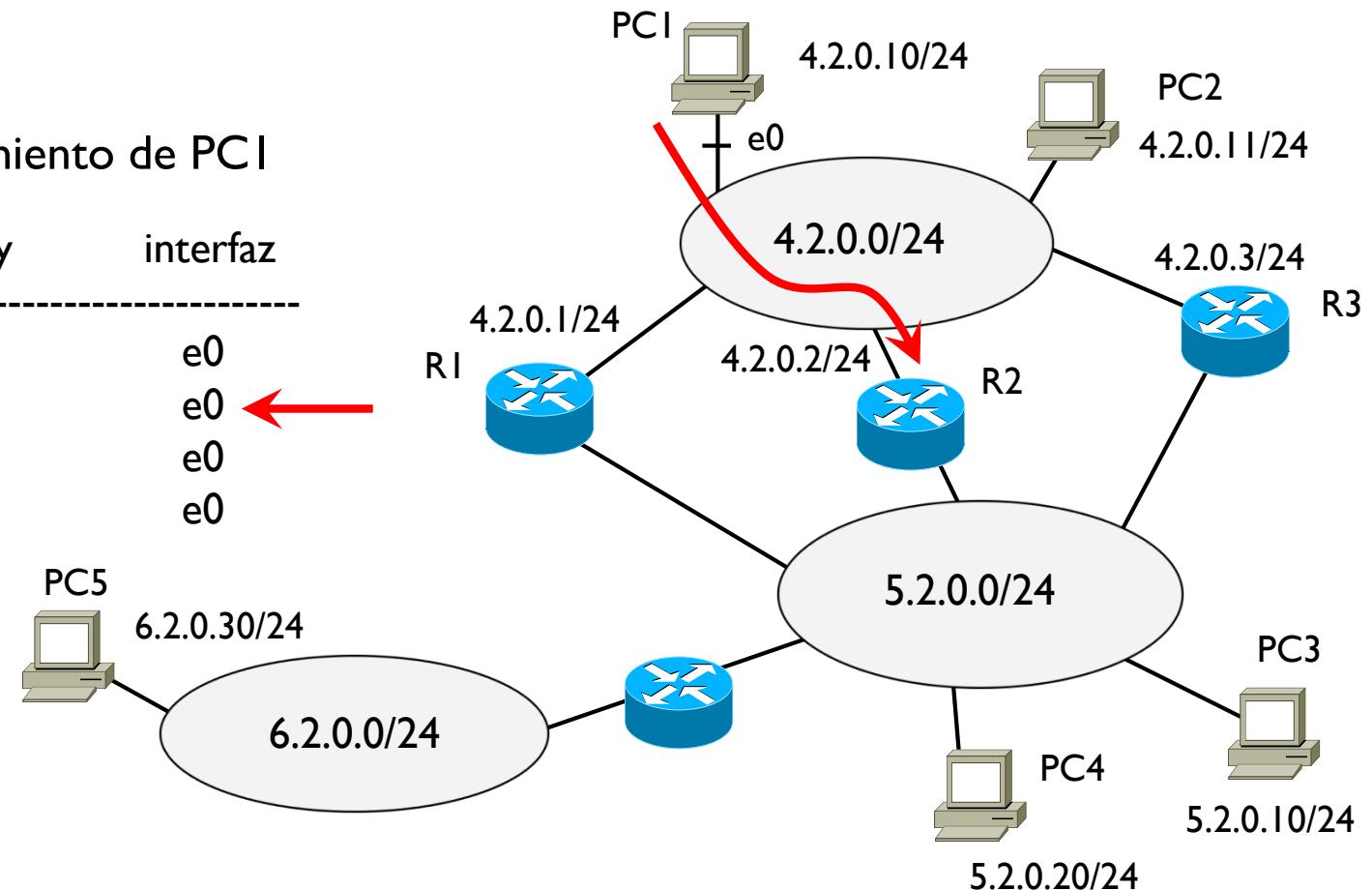
Tema 2 – Encaminamiento IP

- ▶ ¿Si PCI transmite a PC3 por donde se pasa?

Tabla de encaminamiento de PCI

Destino/mascara	gateway	interfaz
4.2.0.0/24	0.0.0.0	e0
5.2.0.0/24	4.2.0.2	e0 ←
0.0.0.0/0	4.2.0.1	e0
5.2.0.20/32	4.2.0.3	e0

$$\begin{aligned} & \text{5. 2. 0. 10 AND} \\ & 255.255.255.0 = \\ \hline & 5. 2. 0. 0 = 5.2.0.0 \end{aligned}$$



→ se pasa por el router 4.2.0.2

Tema 2 – Encaminamiento IP

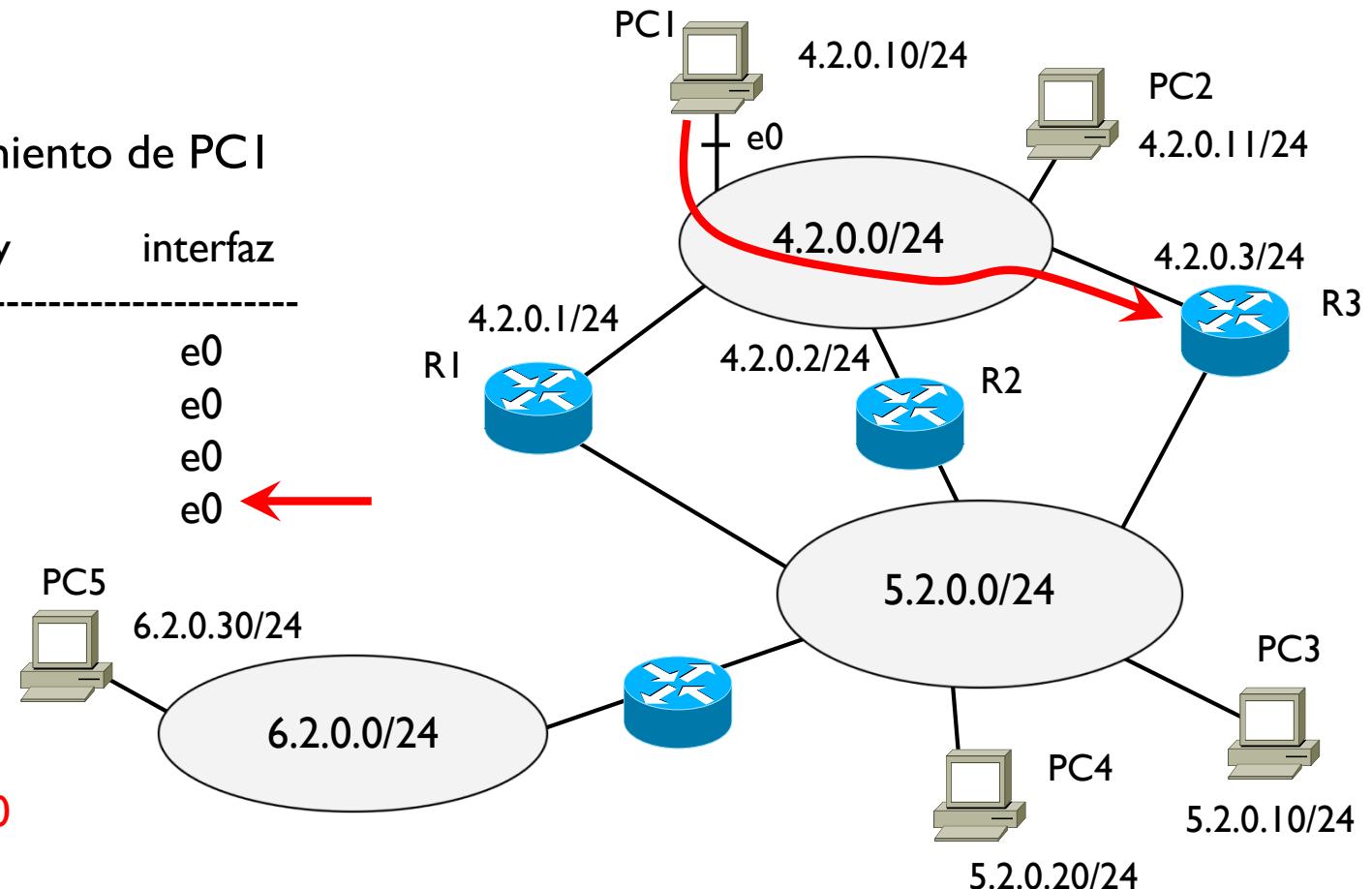
- ▶ ¿Si PCI transmite a PC4 5.2.0.20 por donde se pasa?

Tabla de encaminamiento de PCI

Destino/mascara	gateway	interfaz
4.2.0.0/24	0.0.0.0	e0
5.2.0.0/24	4.2.0.2	e0
0.0.0.0/0	4.2.0.1	e0
5.2.0.20/32	4.2.0.3	e0

5. 2. 0. 20 AND
255.255.255.255 =

5. 2. 0. 20 = 5.2.0.20



PC4 pertenece otra red → se pasa por 4.2.0.3

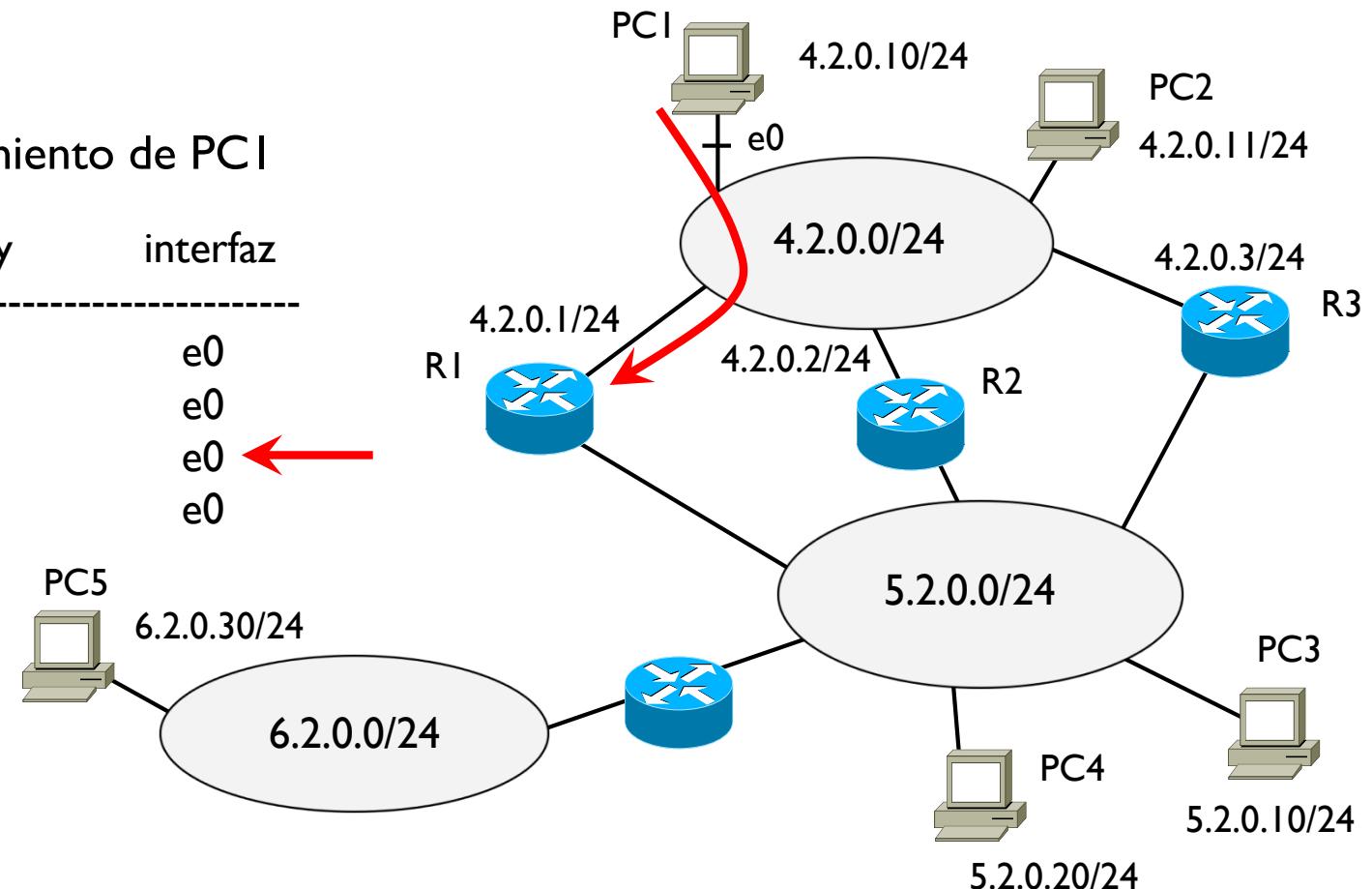
Tema 2 – Encaminamiento IP

- ▶ ¿Si PCI transmite a PC5 6.2.0.30 por donde se pasa?

Tabla de encaminamiento de PCI

Destino/mascara	gateway	interfaz
4.2.0.0/24	0.0.0.0	e0
5.2.0.0/24	4.2.0.2	e0
0.0.0.0/0	4.2.0.1	e0
5.2.0.20/32	4.2.0.3	e0

$$\begin{array}{l} \text{6. 2. 0. 30 AND} \\ \text{0. 0. 0. 0 =} \\ \hline \text{0. 0. 0. 0 = 0.0.0.0} \end{array}$$



PC5 pertenece otra red → se pasa por 4.2.0.1

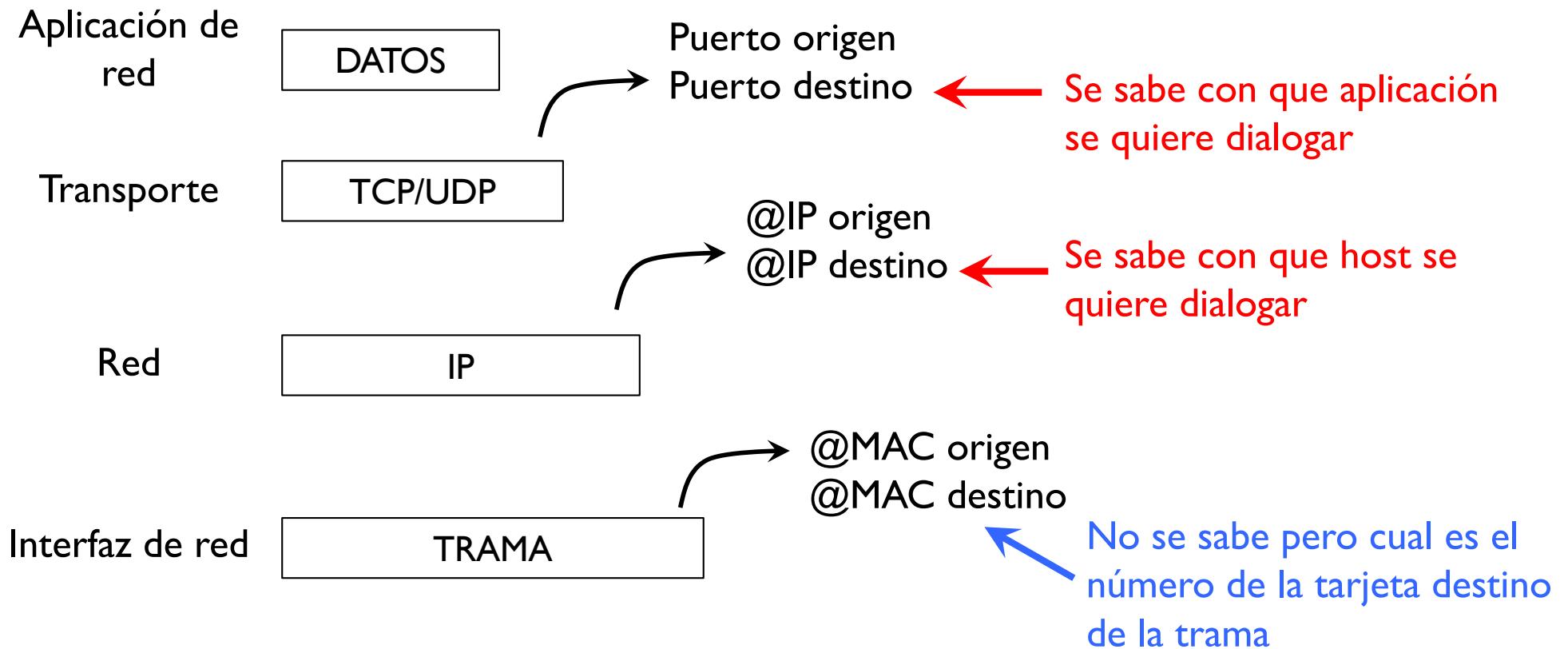
Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ **Protocolo ARP**
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – Address Resolution Protocol (ARP)

- ▶ Protocolo de resolución de direcciones (MAC)
- ▶ RFC 826



Tema 2 – Address Resolution Protocol (ARP)

Objetivo del ARP

- ▶ A partir de una @IP descubre la @MAC de otros dispositivos (hosts o routers) que pertenecen a la misma red
- ▶ Hosts y routers almacenan estas resoluciones en una tabla ARP
 - ▶ Las resoluciones consisten en asociar una @IP a una @MAC
 - ▶ Cada resolución tiene un tiempo de vida (duración); si no se recibe una trama con la misma asociación @IP-@MAC durante un tiempo, la resolución se borra
 - ▶ Las @IP son asignadas por un administrador mientras las @MAC son fijas, por lo tanto las @IP pueden cambiar y la resolución en la tabla ARP debe cambiar

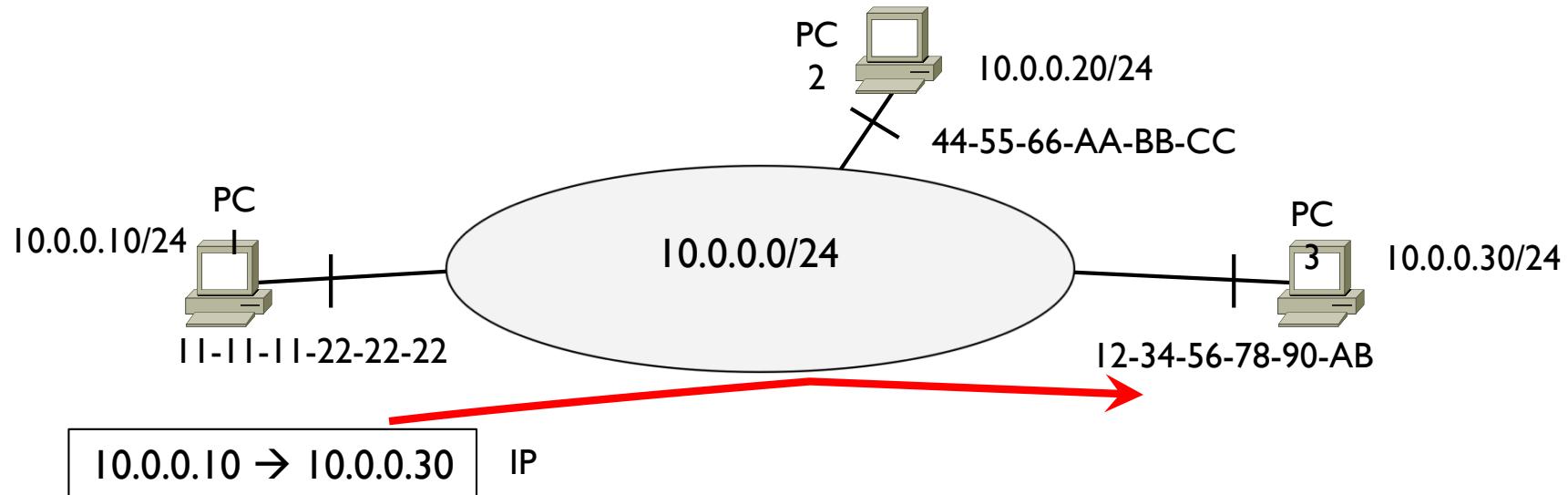
Tabla ARP → Al principio la tabla está vacía

@IP @MAC duración → Generalmente 5 o 20 minutos



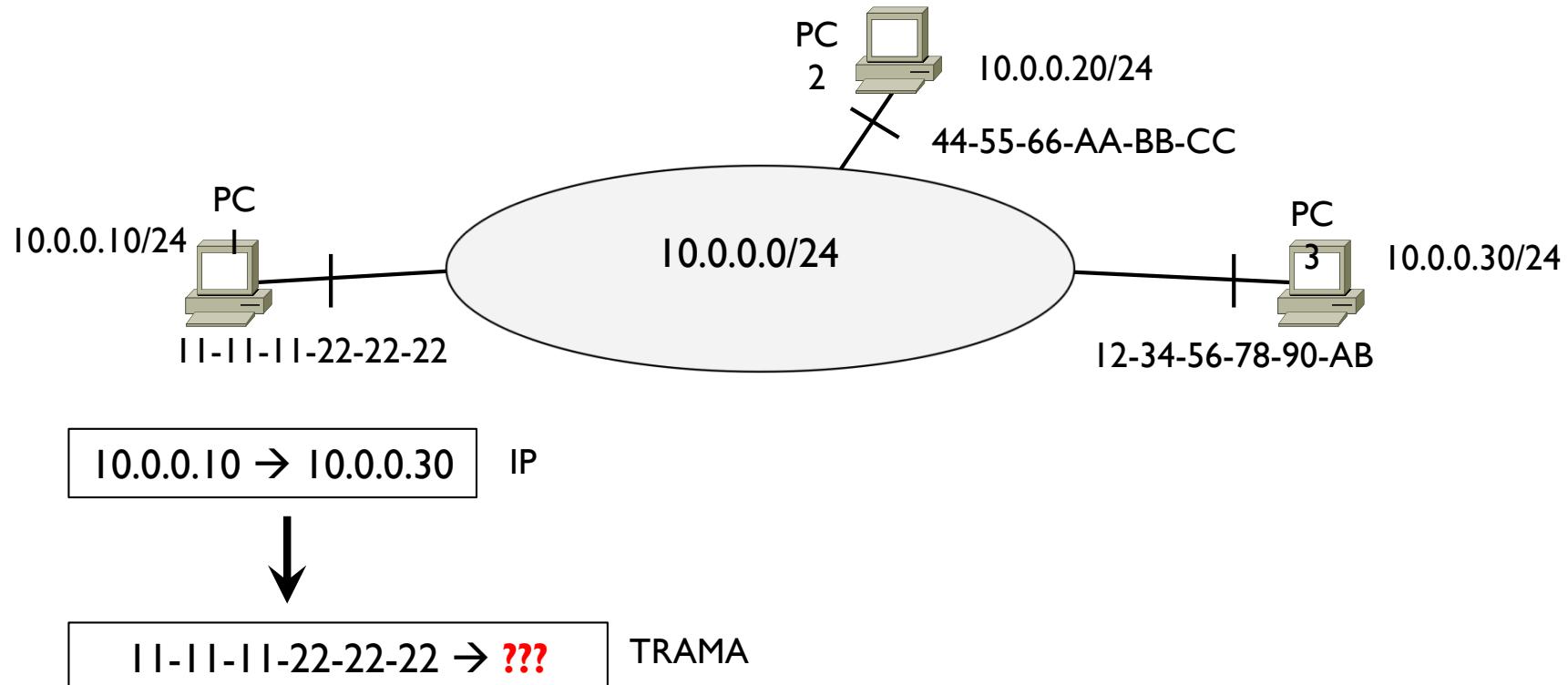
Tema 2 – Address Resolution Protocol (ARP)

- ▶ Ejemplo
 - ▶ Entrega directa (a un destino de la misma red del origen)



Tema 2 – Address Resolution Protocol (ARP)

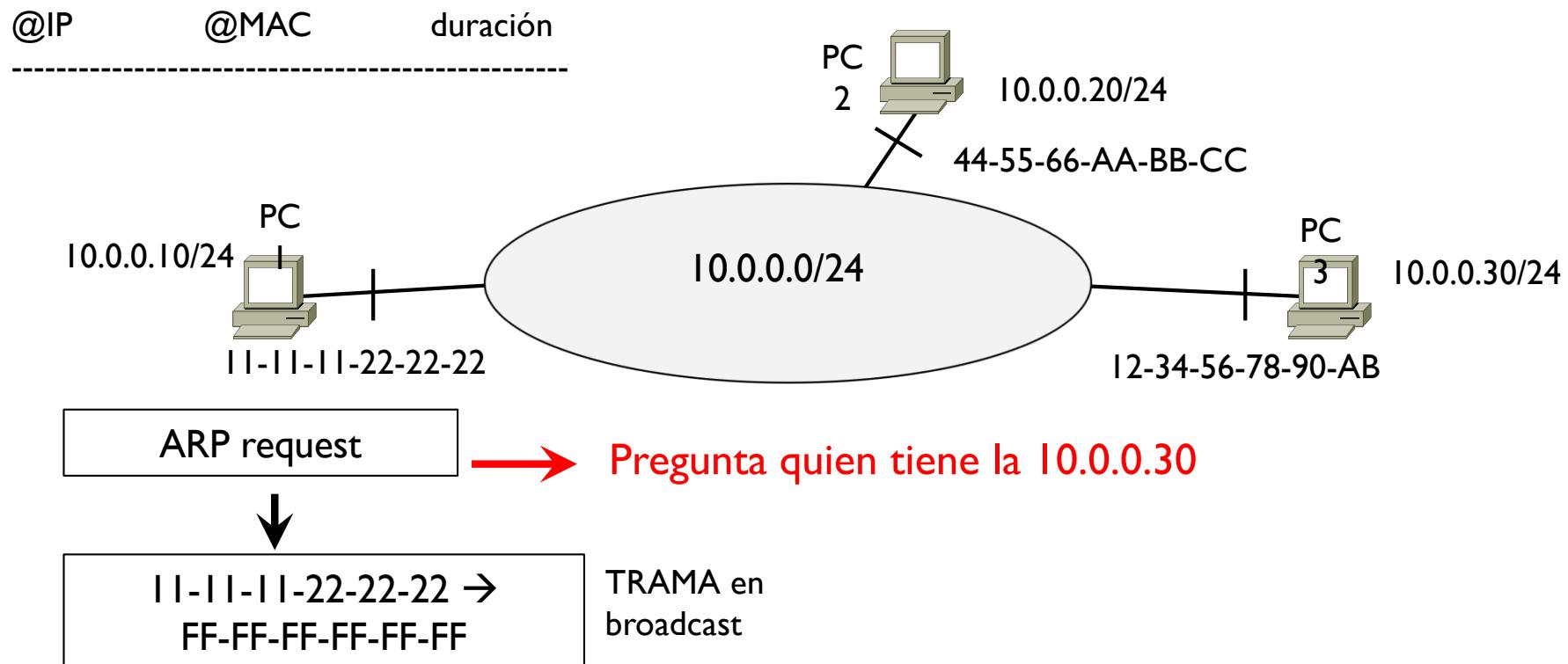
- ▶ Problema
 - ▶ Hay que encapsular el datagrama en una trama y saber la @MAC destino



Tema 2 – Address Resolution Protocol (ARP)

- ▶ PCI consulta su tabla ARP y no encuentra la resolución
- ▶ PCI envía un ARP request en broadcast en su red pidiendo la @MAC de la @IP 10.0.0.30

Tabla ARP de PCI

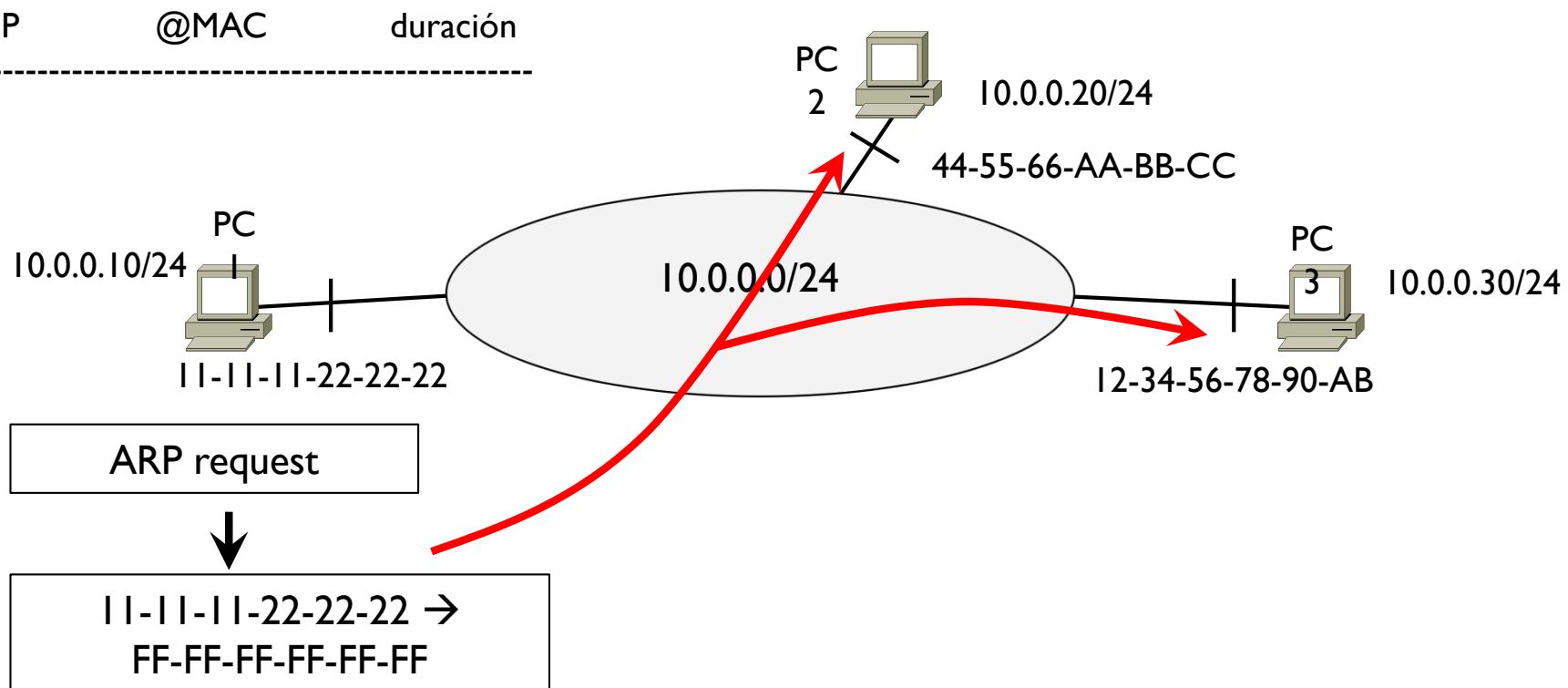


Tema 2 – Address Resolution Protocol (ARP)

- ▶ El ARP request es en broadcast → llega a todos los destinos de la 10.0.0.0/24
- ▶ Todos leen el ARP y miran si la pregunta es para ellos

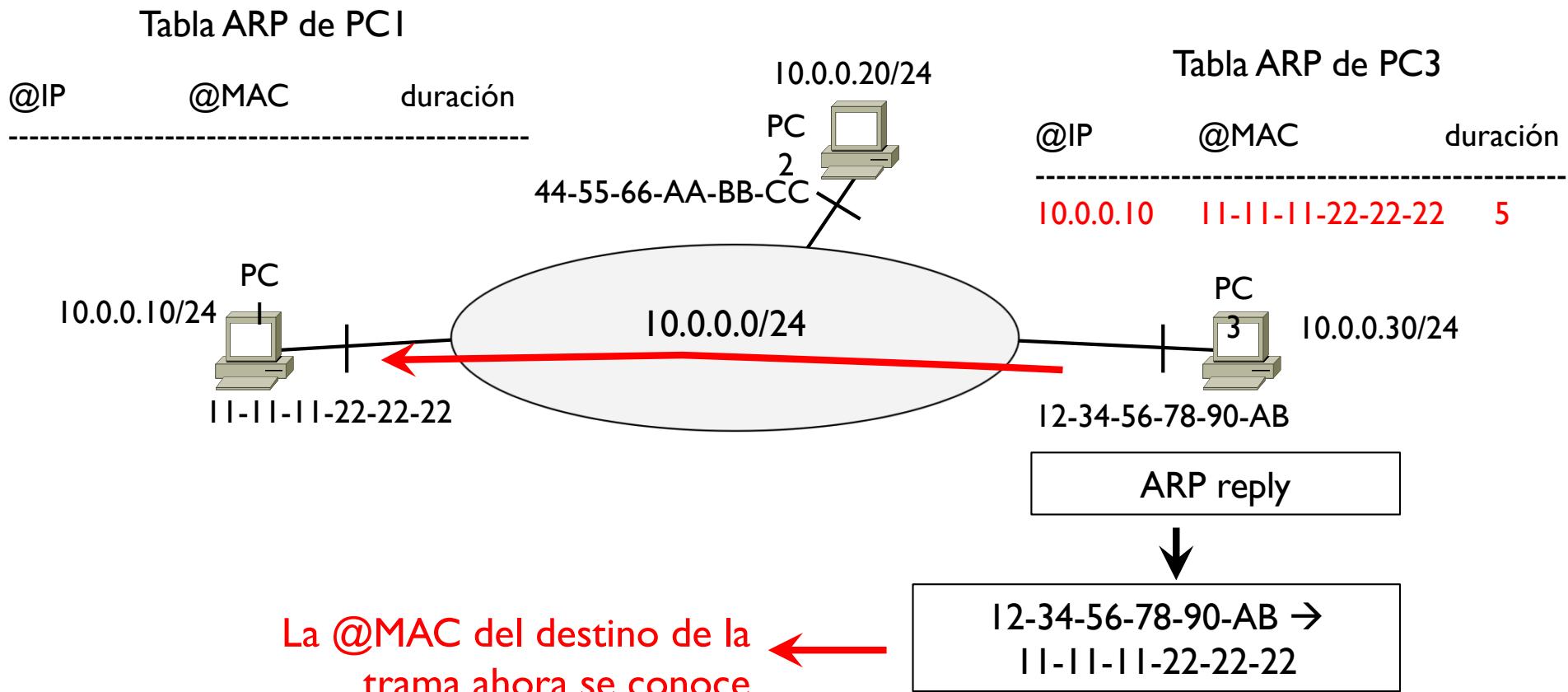
Tabla ARP de PCI

@IP	@MAC	duración
-----	------	----------



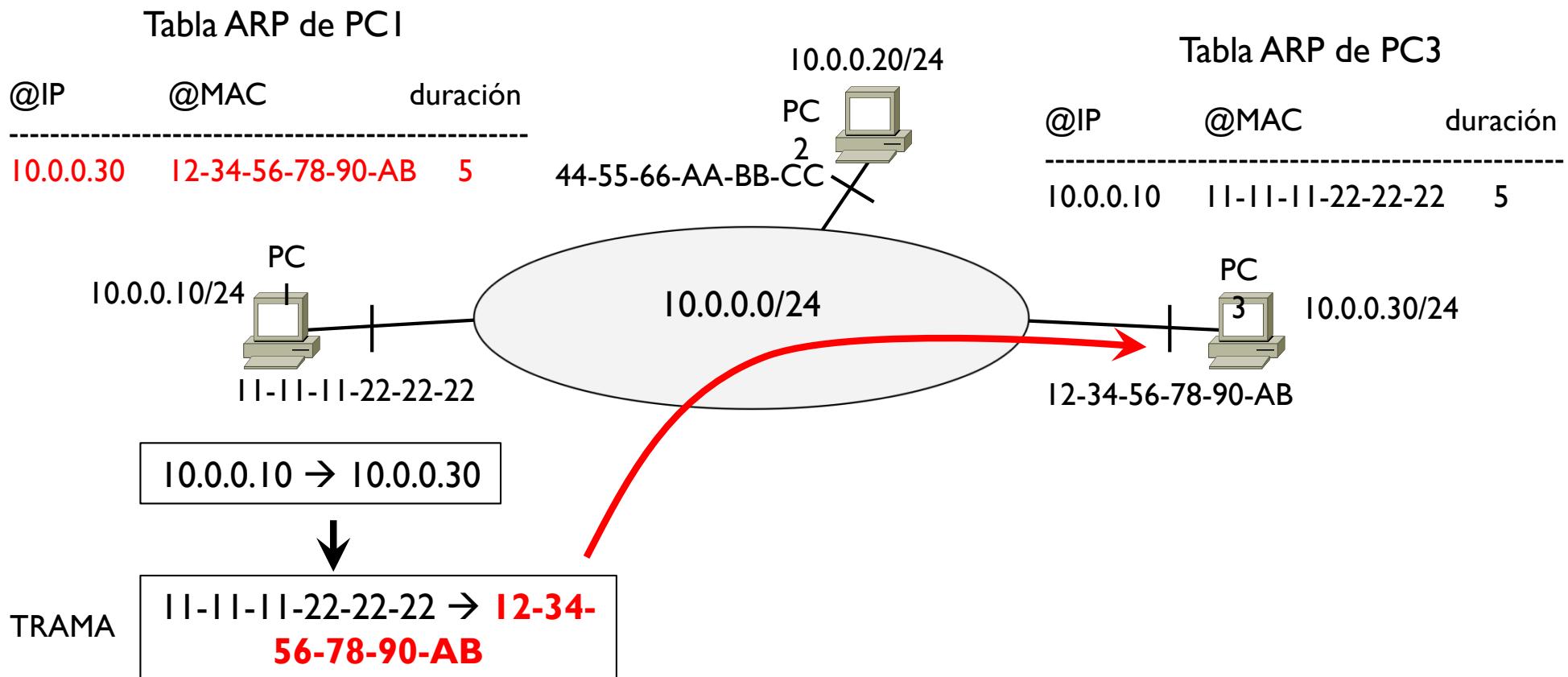
Tema 2 – Address Resolution Protocol (ARP)

- ▶ El preguntado es PC3
- ▶ Solo PC3 actualiza su tabla ARP y contesta con un ARP reply solo a PCI



Tema 2 – Address Resolution Protocol (ARP)

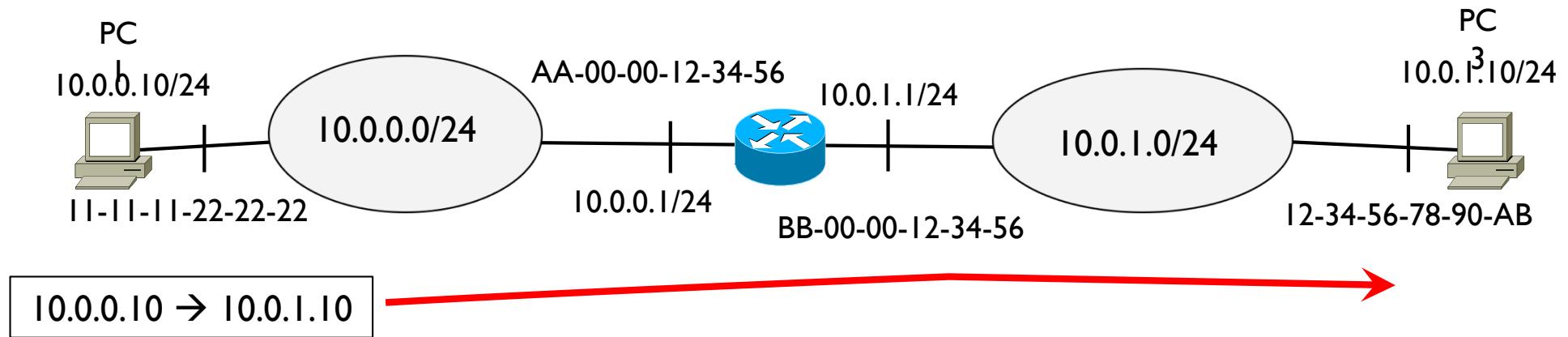
- ▶ PC1 recibe el ARP reply, actualiza su tabla ARP
- ▶ PC1 ahora puede transmitir datagramas a PC3



Tema 2 – Address Resolution Protocol (ARP)

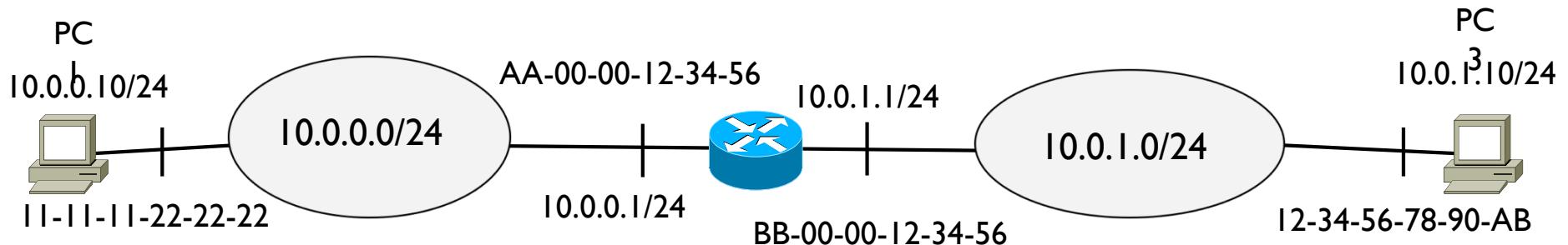
- ▶ Ejemplo

- ▶ Entrega indirecta (el destino está en otra red respecto al origen)



Tema 2 – Address Resolution Protocol (ARP)

- ▶ Problema
 - ▶ Encapsular el datagrama en una trama y saber la @MAC del destino de la trama



10.0.0.10 → 10.0.1.10



¿A quien hay que enviar la trama?

11-11-11-22-22-22 → ???

TRAMA

¿Hay que descubrir la @MAC de PC3?

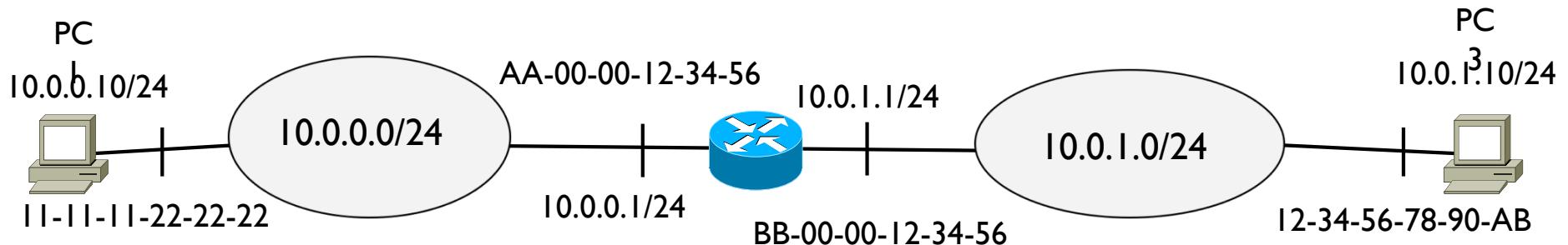
NO!!

Las tramas no cruzan redes, solo sirven para comunicar dispositivos en una misma red



Tema 2 – Address Resolution Protocol (ARP)

- ▶ Problema
 - ▶ Encapsular el datagrama en una trama y saber la @MAC del destino de la trama



10.0.0.10 → 10.0.1.10



¿A quien hay que enviar la trama?

11-11-11-22-22-22 → ???

TRAMA

Lo dice la tabla de encaminamiento!!!

Tabla de encaminamiento de PCI

Destino/mascara	gateway	interfaz
10.0.0.0/24	0.0.0.0	e0
0.0.0.0/0	10.0.0.1	e0

Hay que enviar por e0 al gateway 10.0.0.1

Tema 2 – Address Resolution Protocol (ARP)

- ▶ PCI envía un ARP request en broadcast en su red preguntando la @MAC de 10.0.0.1
- ▶ RI actualiza su tabla ARP con la asociación de @IP y @MAC de PCI

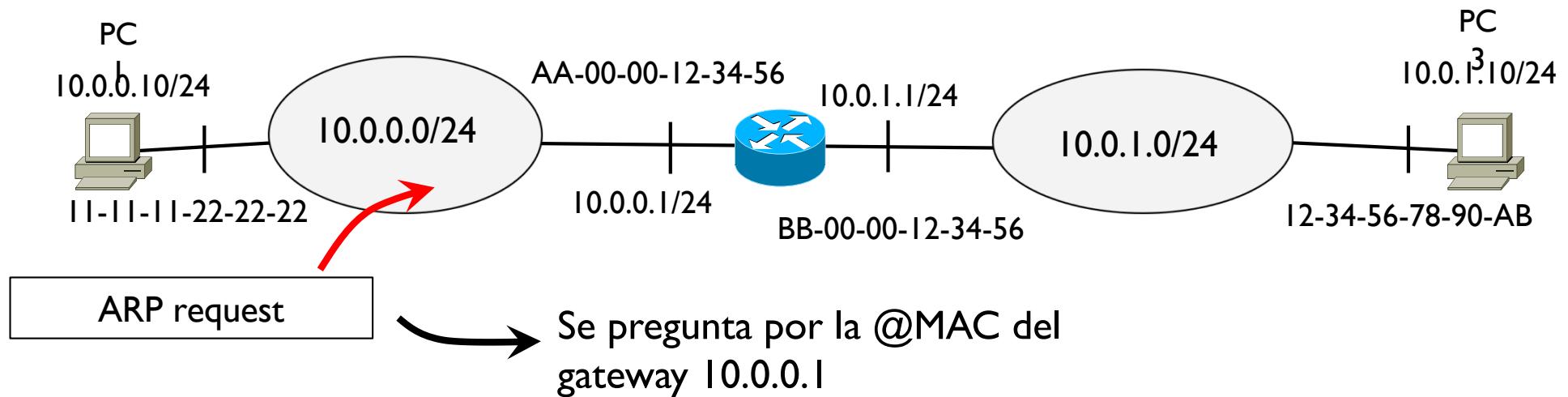
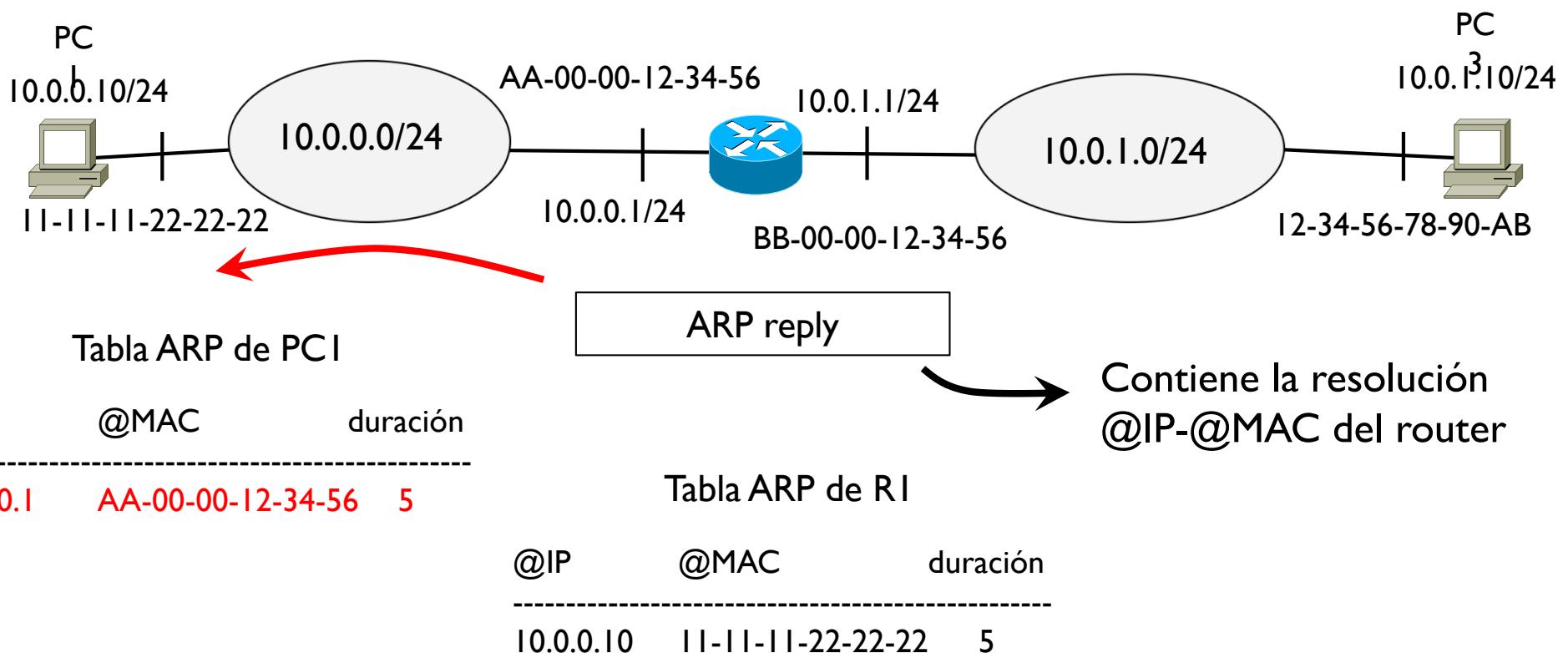


Tabla ARP de RI

@IP	@MAC	duración
10.0.0.10	11-11-11-22-22-22	5

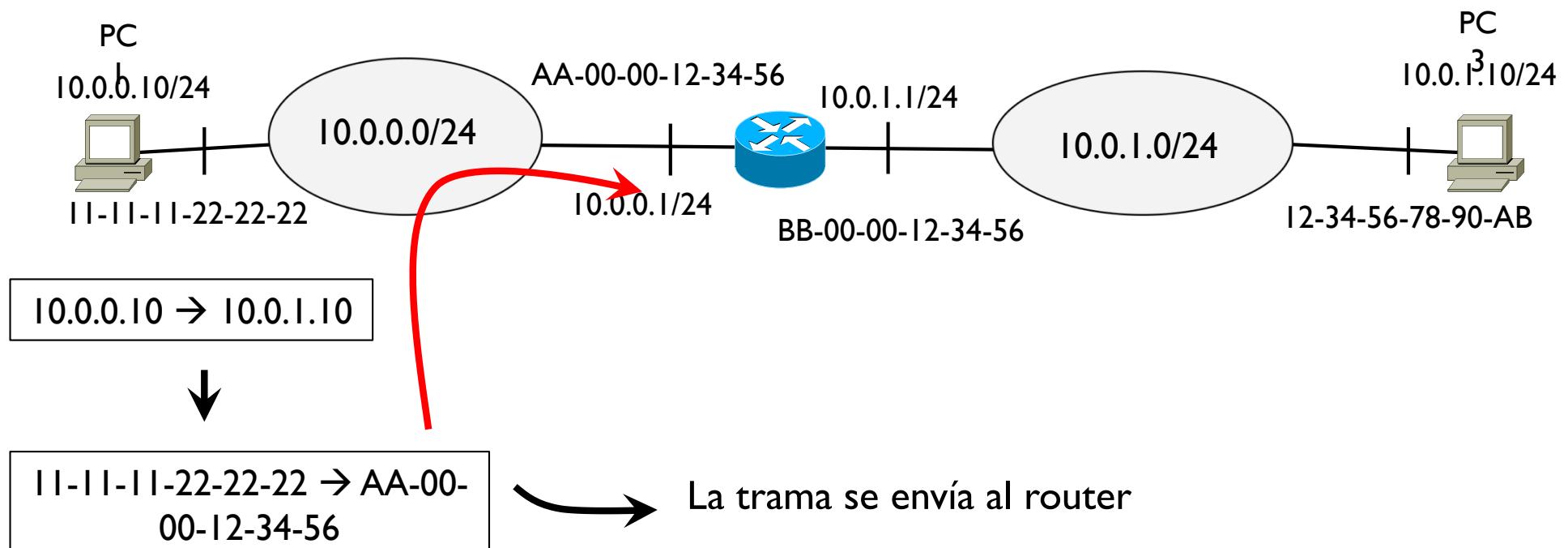
Tema 2 – Address Resolution Protocol (ARP)

- ▶ RI contesta con un ARP reply
- ▶ Contiene la resolución 10.0.0.1 – AA-00-00-12-34-56
- ▶ PCI actualiza su tabla



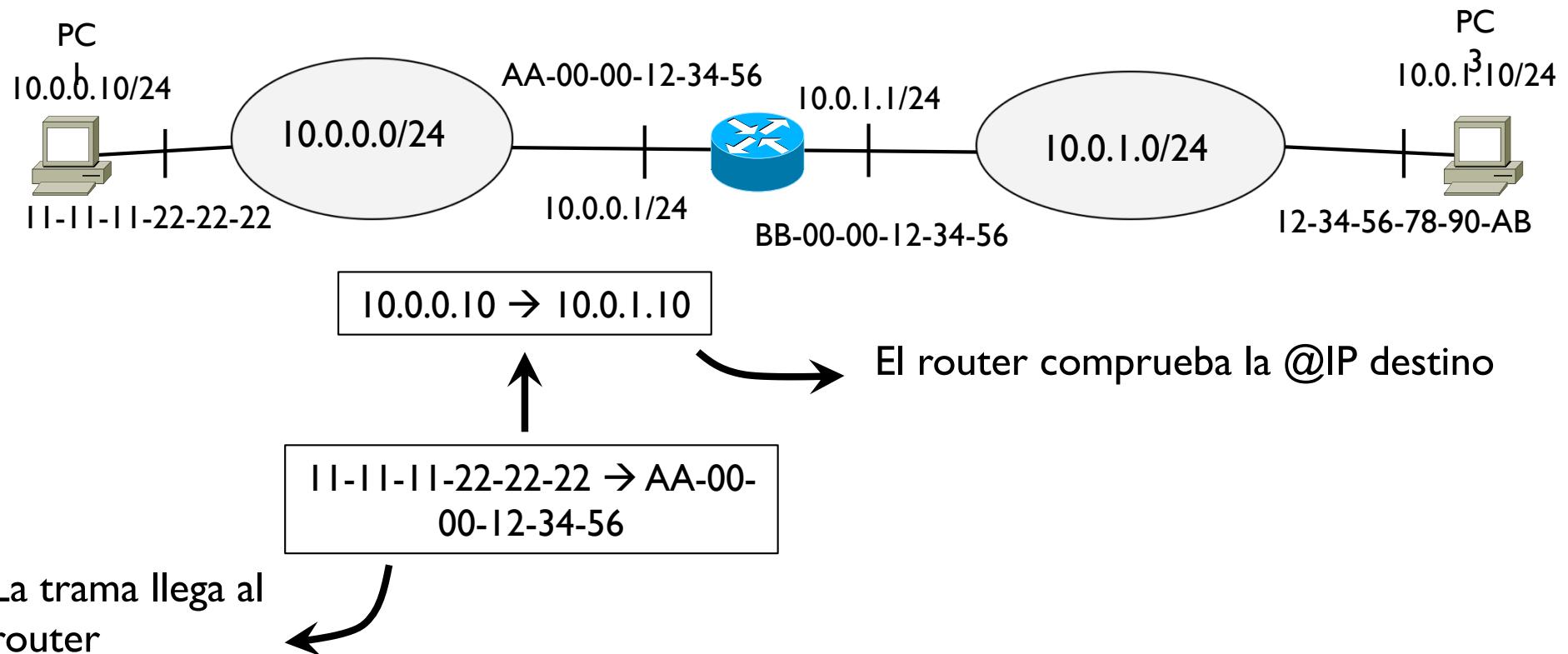
Tema 2 – Address Resolution Protocol (ARP)

- ▶ PC1 encapsula el datagrama para PC3 en una trama con destino la @MAC del router



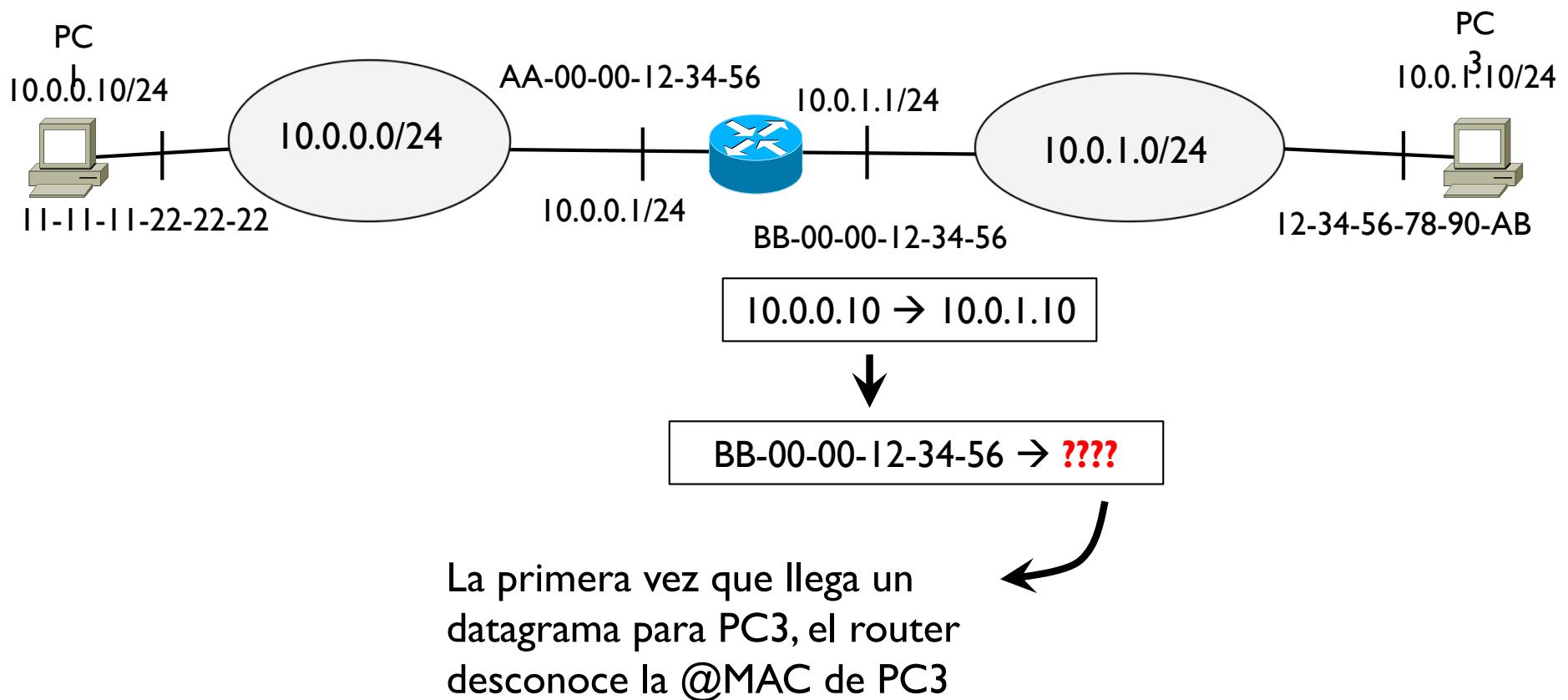
Tema 2 – Address Resolution Protocol (ARP)

- ▶ El router reconoce que es el destino y elimina la cabecera de trama
- ▶ El router comprueba la @IP destino y de su tabla de encaminamiento ve que el destino está conectado directamente a su otra red



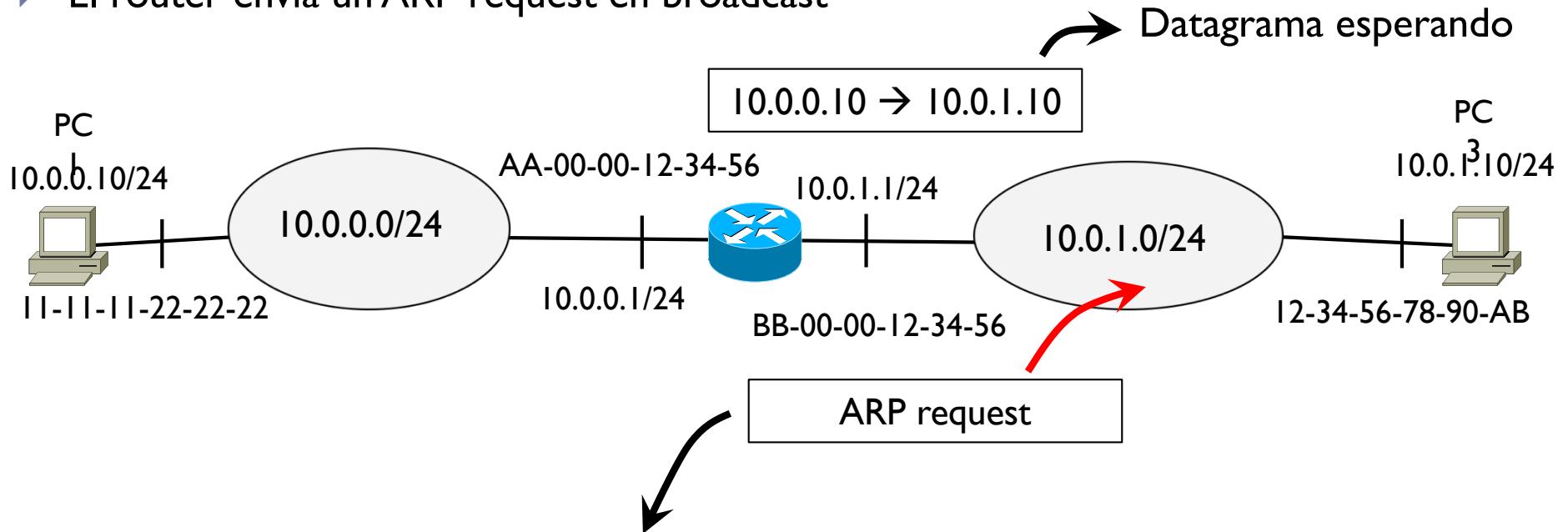
Tema 2 – Address Resolution Protocol (ARP)

- ▶ El router transfiere el datagrama a su interfaz de salida
- ▶ El router debe añadir ahora una nueva cabecera de trama para transmitir al destino
- ▶ El router comprueba su tabla ARP a ver si encuentra la @MAC de 10.0.1.10



Tema 2 – Address Resolution Protocol (ARP)

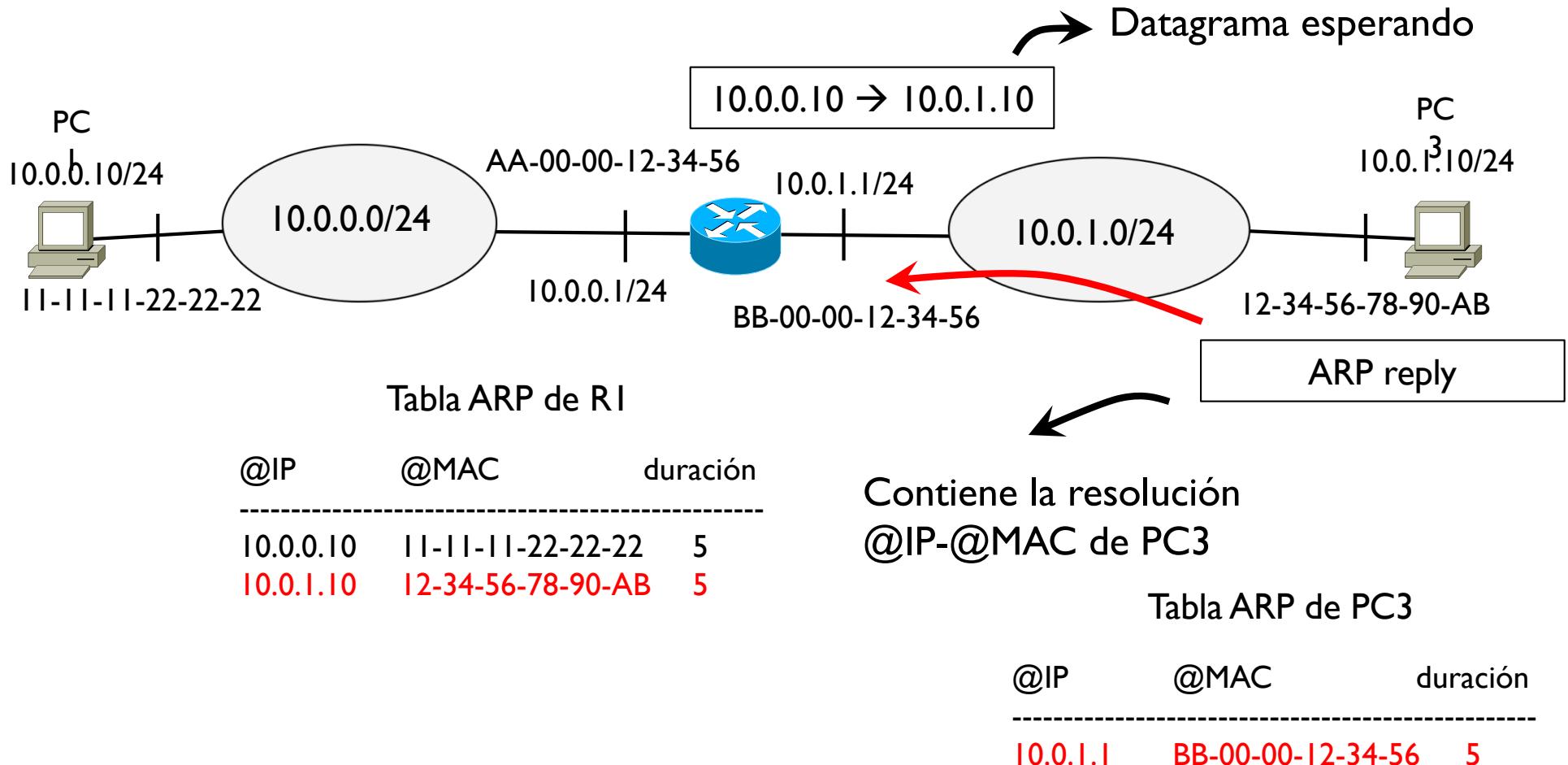
- ▶ Si es la primera vez que transmite algo a PC3 o ya ha pasado demasiado tiempo desde la última transmisión a PC3, el router debe descubrir la @MAC de PC3
- ▶ El router envía un ARP request en broadcast



El router pregunta sobre la
@MAC de 10.0.1.10

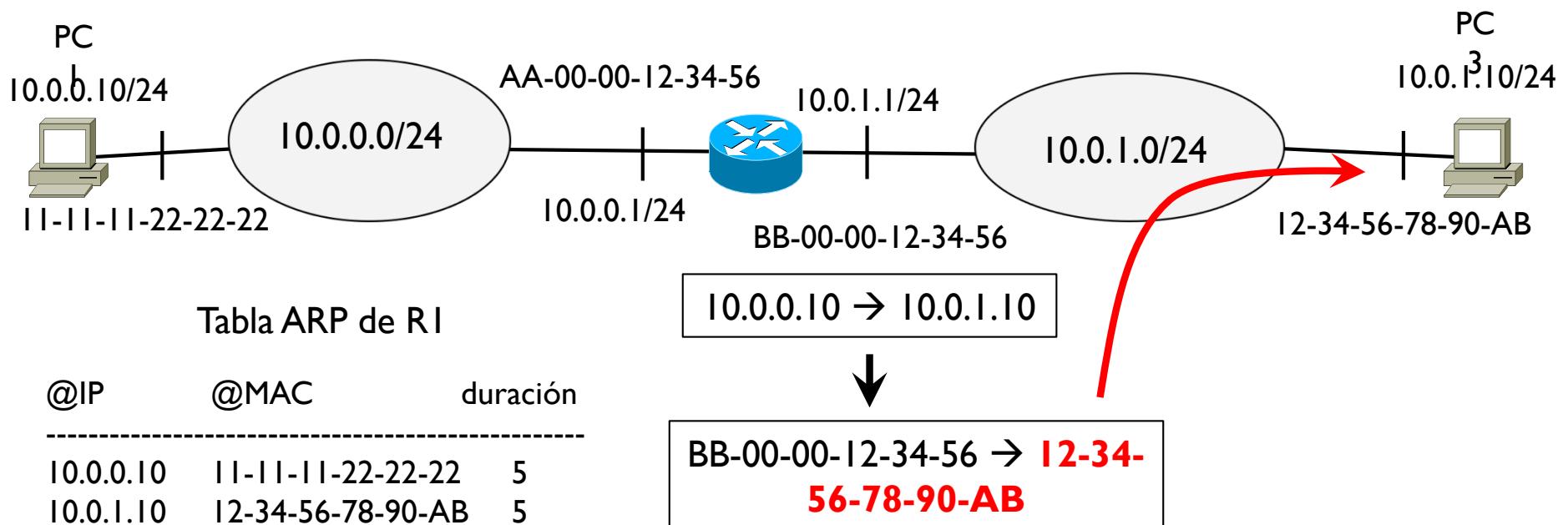
Tema 2 – Address Resolution Protocol (ARP)

- ▶ PC3 actualiza su tabla ARP con la @MAC del router
- ▶ PC3 contesta con un ARP reply que contiene su resolución



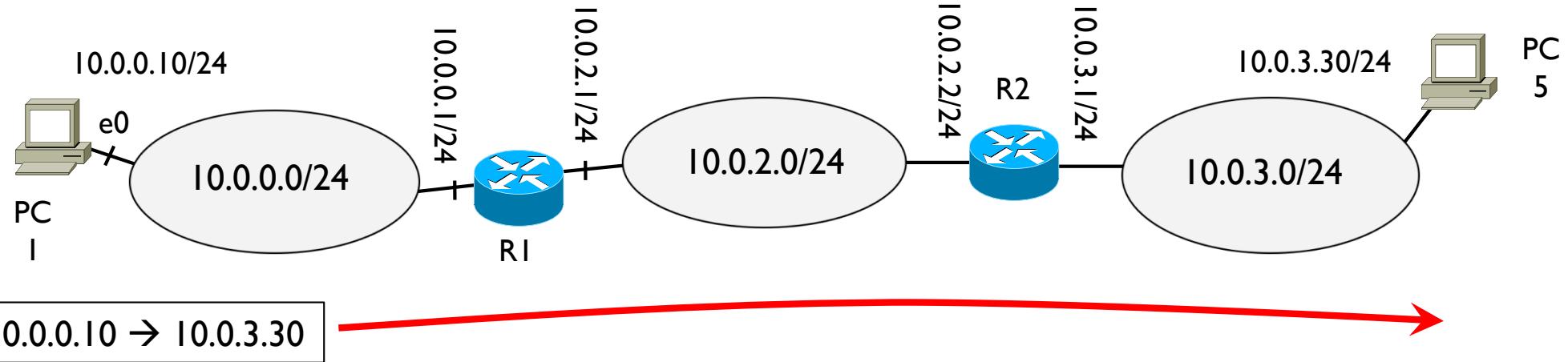
Tema 2 – Address Resolution Protocol (ARP)

- ▶ El router puede finalmente coger el datagrama en espera, encapsularlo en una trama con destino PC3 y enviarlo



Tema 2 – Address Resolution Protocol (ARP)

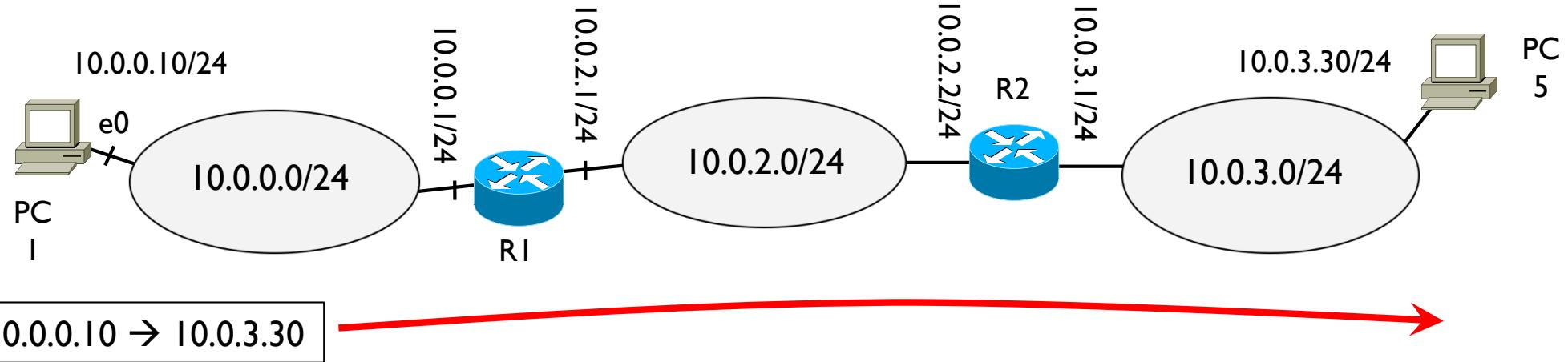
- ▶ ¿Y si hubieran mas redes intermedias?



- ▶ Lo mismo
- ▶ PC1 comprueba si tiene la @MAC de 10.0.0.1 (gateway hacia PC5) en la tabla ARP
 - ▶ Si ya la tiene de resoluciones anteriores, encapsula la trama y envía
 - ▶ Si no la tiene, ARP request y espera el ARP reply con la respuesta
 - ▶ Encapsula el datagrama en la trama y transmite al router R1

Tema 2 – Address Resolution Protocol (ARP)

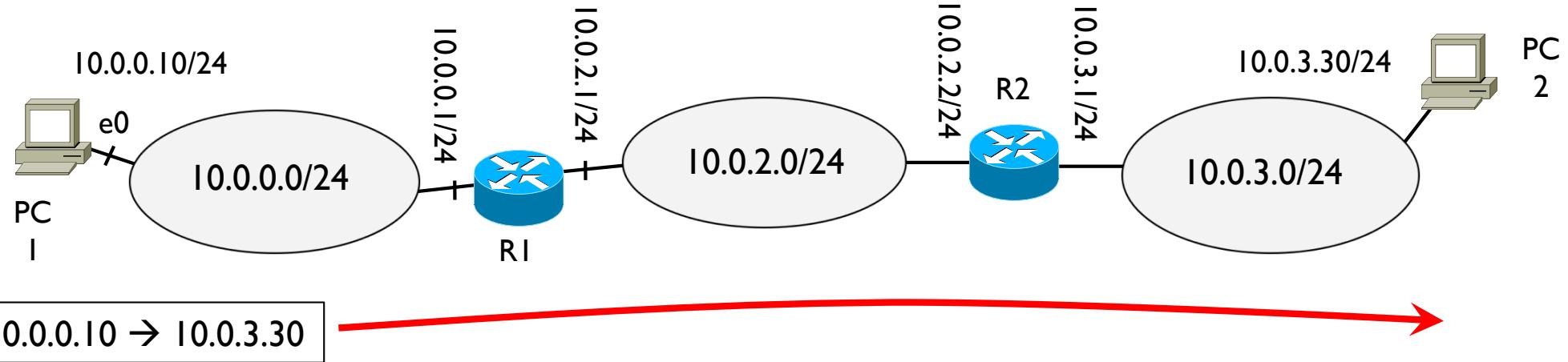
- ▶ ¿Y si hubieran mas redes intermedias?



- ▶ RI recibe la trama, quita la cabecera de trama, mueve el datagrama a su otra red y comprueba si tiene la @MAC de 10.0.2.2 en su tabla ARP
 - ▶ Si ya la tiene de resoluciones anteriores, encapsula la trama y envía
 - ▶ Si no la tiene, ARP request y espera el ARP reply con la respuesta
 - ▶ Encapsula el datagrama en la trama y transmite al router R2

Tema 2 – Address Resolution Protocol (ARP)

- ▶ ¿Y si hubieran mas redes intermedias?



- ▶ R2 recibe la trama, quita la cabecera de trama, mueve el datagrama a su otra red y comprueba si tiene la @MAC de 10.0.3.30 (destino final) en su tabla ARP
 - ▶ Si ya la tiene de resoluciones anteriores, encapsula la trama y envía
 - ▶ Si no la tiene, ARP request y espera el ARP reply con la respuesta
 - ▶ Encapsula el datagrama en la trama y transmite a PC5

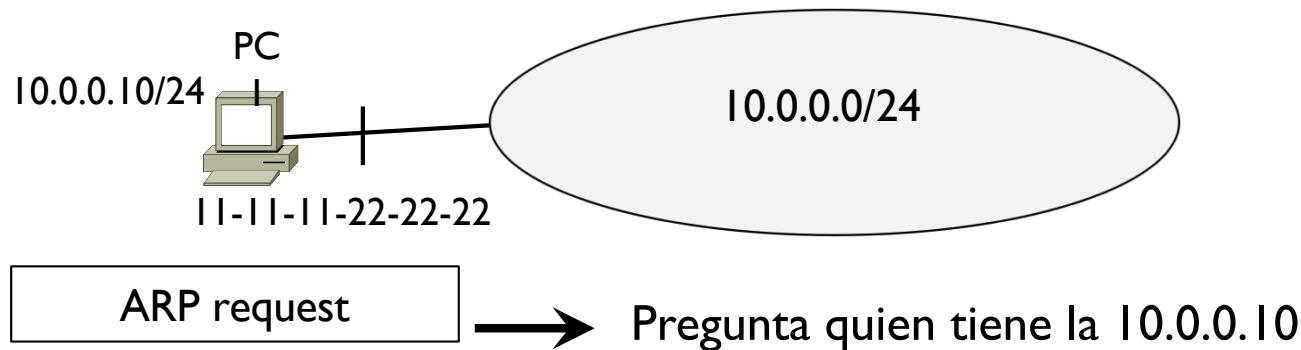
Tema 2 – Otras funciones del ARP

Reverse ARP

- ▶ RFC 903
- ▶ Averigua la @IP destino a partir de una @MAC (al revés que un ARP)

ARP gratuito

- ▶ Un host envía un ARP request en broadcast de esta forma



- ▶ ¿a que sirve?

Descubrir si la @IP de PCI está ya ocupada en la red 10.0.0.0/24

Si alguien contesta, es que tiene la misma @IP de PCI

→ @IP duplicada!!



Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ **Cabecera IP**
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – Cabecera IP

Datagrama



Cabecera IP, por defecto 20 bytes

0 31	3 4	7 8	15 16	18 19	
Versión	Longitud	Tipo de servicio		Longitud total	
	Identificación		Flags	Desplazamiento de fragmento	
Tiempo de vida		Protocolo		Checksum cabecera	
			Dirección IP origen		
			Dirección IP destino		
			Opciones		

Diagrama de la estructura de la cabecera IP:

- La cabecera tiene un tamaño fijo de 20 bytes.
- Los campos están numerados de 0 a 31 en la fila superior.
- Los campos se describen en la fila inferior:

 - Bytes 0-3: Versión (4 bits), Longitud (3 bits), Tipo de servicio (3 bits).
 - Bytes 4-7: Identificación (16 bits), Flags (3 bits), Desplazamiento de fragmento (13 bits).
 - Bytes 8-11: Tiempo de vida (8 bits), Protocolo (8 bits).
 - Bytes 12-15: Checksum cabecera (16 bits).
 - Bytes 16-31: Dirección IP origen (32 bits), Dirección IP destino (32 bits), Opciones (0-40 bytes).

- Un cuadro vertical indica que el total es $5 \times 32 \text{ bits} = 160 \text{ bits} = 20 \text{ bytes}$.



Tema 2 – Cabecera IP

- ▶ **Versión:** indica la versión del IP
 - ▶ 4 → IP (también se conoce como IPv4)
 - ▶ 6 → IPv6 (nueva versión)
 - ▶ esta versión no se trata en esta asignatura
 - ▶ direcciones de 128 bits
- ▶ **Longitud:** indica la longitud de la cabecera IP
 - ▶ Generalmente es de 20 bytes pero se pueden añadir opciones hasta un máximo de 60 bytes totales
- ▶ **Tipo de servicio:** indica el trato de los datagramas
 - ▶ Indica si algún datagrama hay que tratarlo de manera diferente
 - ▶ Realmente no se usa en Internet (todos los datagramas tienen el mismo valor en este campo)

Versión	Longitud	Tipo de servicio		Longitud total
Identificación			Flags	Desplazamiento de fragmento
Tiempo de vida	Protocolo	Checksum cabecera		
Dirección IP origen			Dirección IP destino	
Opciones				



Tema 2 – Cabecera IP

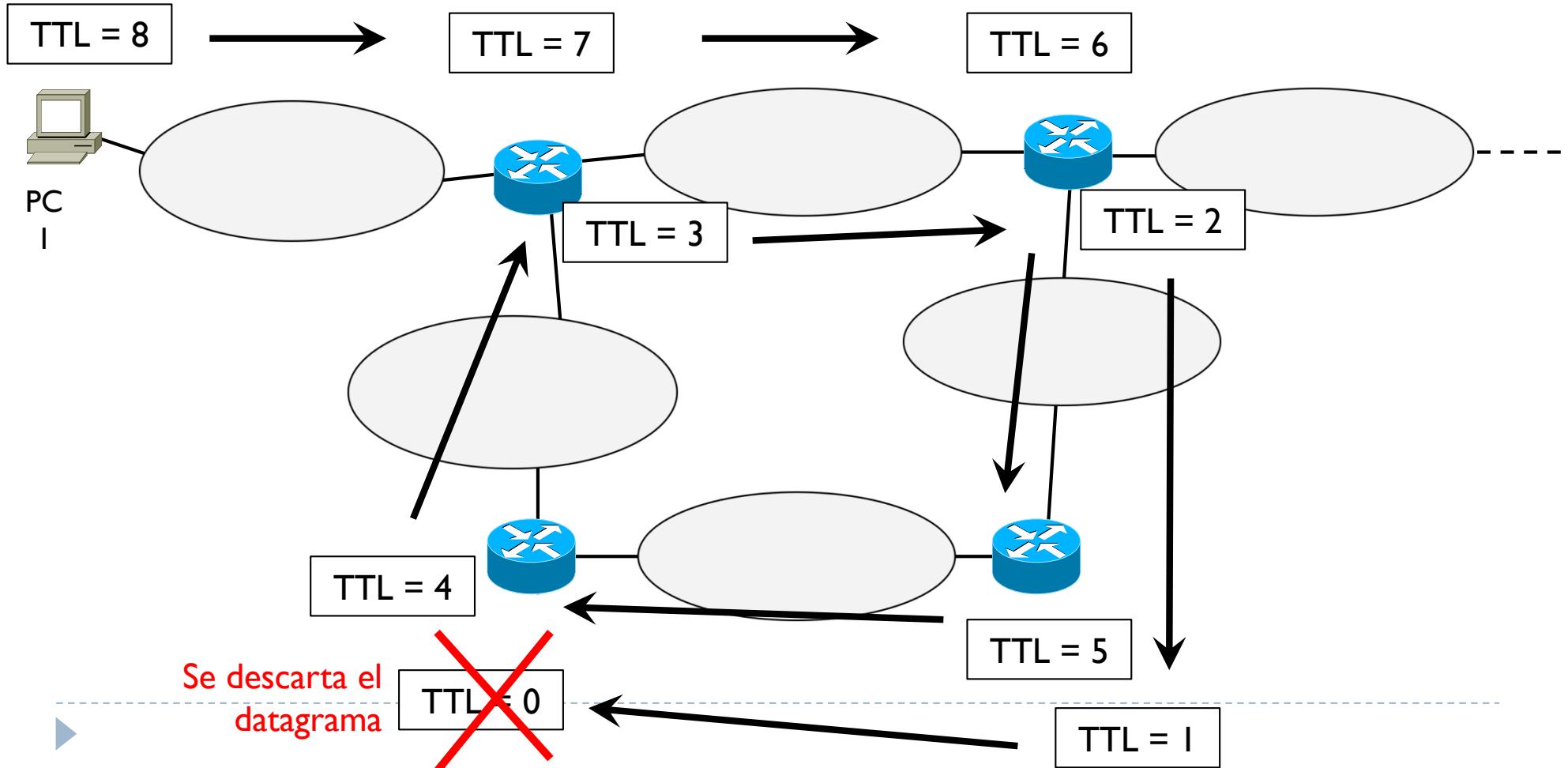
- ▶ **Longitud total**
 - ▶ Longitud total del datagrama, cabecera incluida
 - ▶ Máximo posible $2^{16}-1 = 65535$ bytes
- ▶ **Identificación + Flags + Desplazamiento de fragmento**
 - ▶ Se usan para fragmentar un datagrama
- ▶ **Tiempo de vida (TTL)**
 - ▶ El host origen del datagrama asigna un valor a este campo
 - ▶ Cada router intermedio disminuye este valor de 1
 - ▶ Si el TTL=0, el router descarta el datagrama
 - ▶ Sirve para evitar que un datagrama perdido se quede indefinidamente en las redes

Versión	Longitud	Tipo de servicio		Longitud total
Identificación		Flags	Desplazamiento de fragmento	
Tiempo de vida		Protocolo	Checksum cabecera	
Dirección IP origen				
Dirección IP destino				
Opciones				



Tema 2 – Cabecera IP

Versión	Longitud	Tipo de servicio		Longitud total		
Identificación		Flags	Desplazamiento de fragmento			
Tiempo de vida		Protocolo	Checksum cabecera			
Dirección IP origen						
Dirección IP destino						
Opciones						

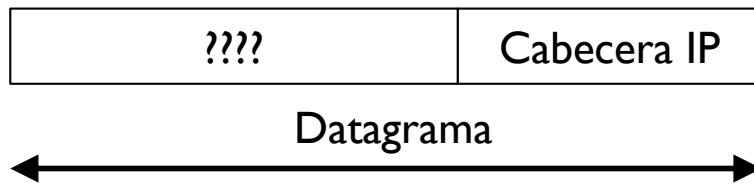


Tema 2 – Cabecera IP

Versión	Longitud	Tipo de servicio		Longitud total
Identificación			Flags	Desplazamiento de fragmento
Tiempo de vida	Protocolo	Checksum cabecera		
Dirección IP origen			Dirección IP destino	
Opciones				

▶ Protocolo

- ▶ Identifica que protocolo se ha encapsulado en este datagrama
- ▶ 6 → TCP 17 → UDP 1 → ICMP 0 → IP



▶ Checksum cabecera

- ▶ Como la transmisión no está exenta de errores, puede pasar que un bit que era 1 se lea como un 0 → **dato no valido**
- ▶ Este campo permite detectar si hay errores en la cabecera



Tema 2 – Cabecera IP

- ▶ Dirección IP origen
 - ▶ @IP del dispositivo que ha creado el datagrama
- ▶ Dirección IP destino
 - ▶ @IP del dispositivo que debe recibir el datagrama
- ▶ Opciones
 - ▶ Campo de longitud variable que puede contener información adicional
 - ▶ No se usa mucho
 - ▶ Por ejemplo, se puede copiar parte de un datagrama recibido en la respuesta, se puede definir una ruta concreta que debe seguir el datagrama, etc.

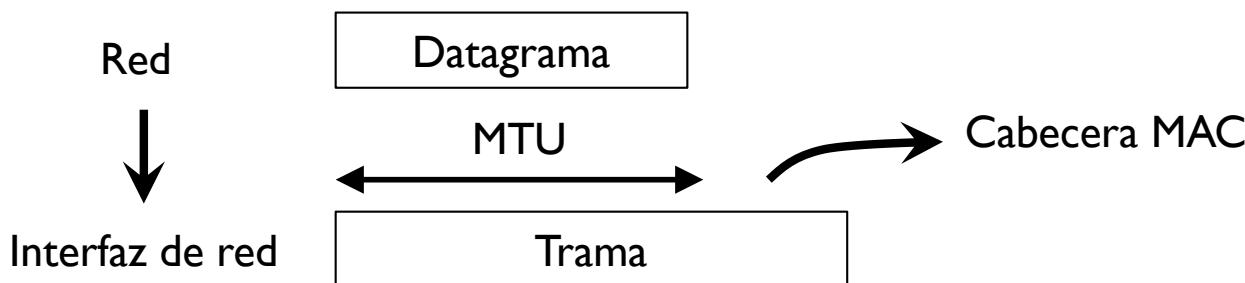
Versión	Longitud	Tipo de servicio		Longitud total
Identificación			Flags	Desplazamiento de fragmento
Tiempo de vida	Protocolo	Checksum cabecera		
Dirección IP origen				
Dirección IP destino				
Opciones				



Tema 2 – Cabecera IP

Fragmentación

- ▶ Se define un parámetro llamado Maximum Transfer Unit (MTU)
- ▶ Indica el máximo número de bytes que se pueden encapsular en una trama



- ▶ Cada tecnología de nivel interfaz de red impone su MTU

Ethernet 1500 bytes

WiFi 2312 bytes

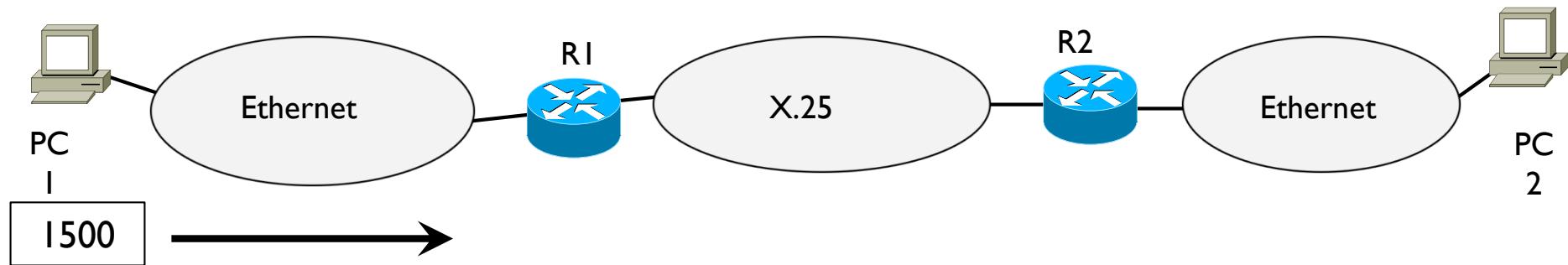
PPP 250 bytes

X.25 576 bytes



Tema 2 – Cabecera IP

Ejemplo

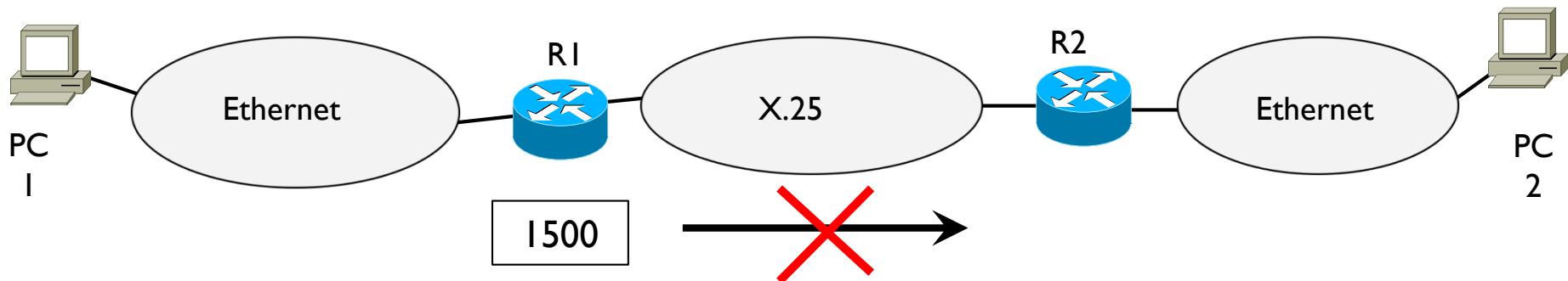


- ▶ PC1 conoce el MTU de su tarjeta Ethernet y ajusta el tamaño del datagrama para que sea de 1500 bytes (desconoce el resto)
- ▶ PC1 encapsula el datagrama en una trama y transmite



Tema 2 – Cabecera IP

Ejemplo

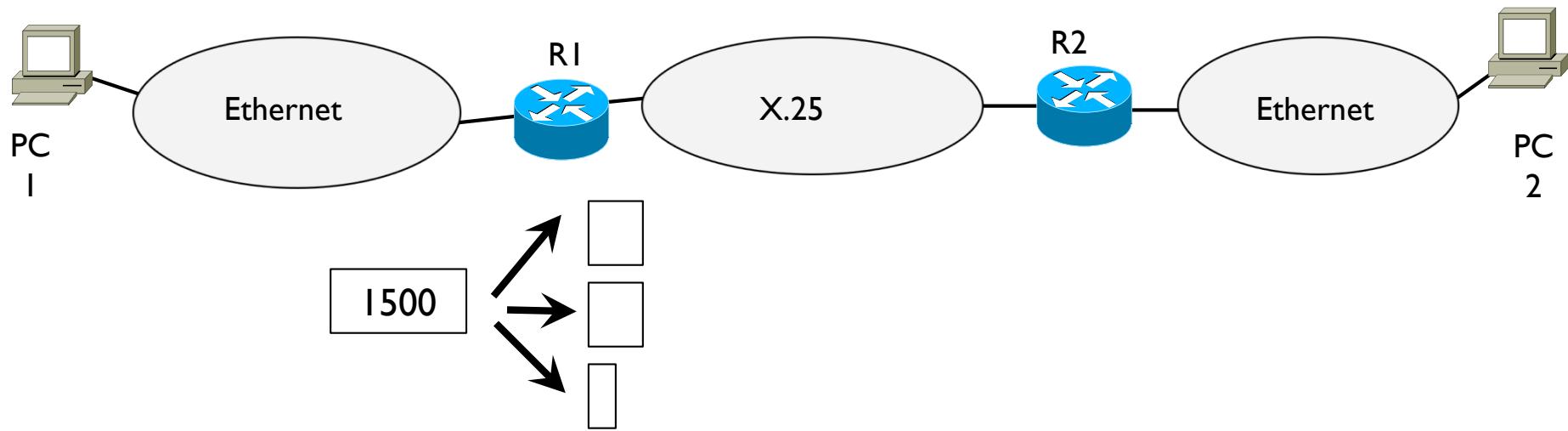


- ▶ R1 recibe la trama y quita la cabecera de trama
- ▶ R1 lee la cabecera IP y según lo que dice su tabla de encaminamiento mueve el datagrama a la interfaz de salida
- ▶ R1 intenta volver a crear una trama pero el MTU de la tarjeta de salida es menor que el tamaño del datagrama:
- ▶ **576 bytes vs. 1500 bytes**



Tema 2 – Cabecera IP

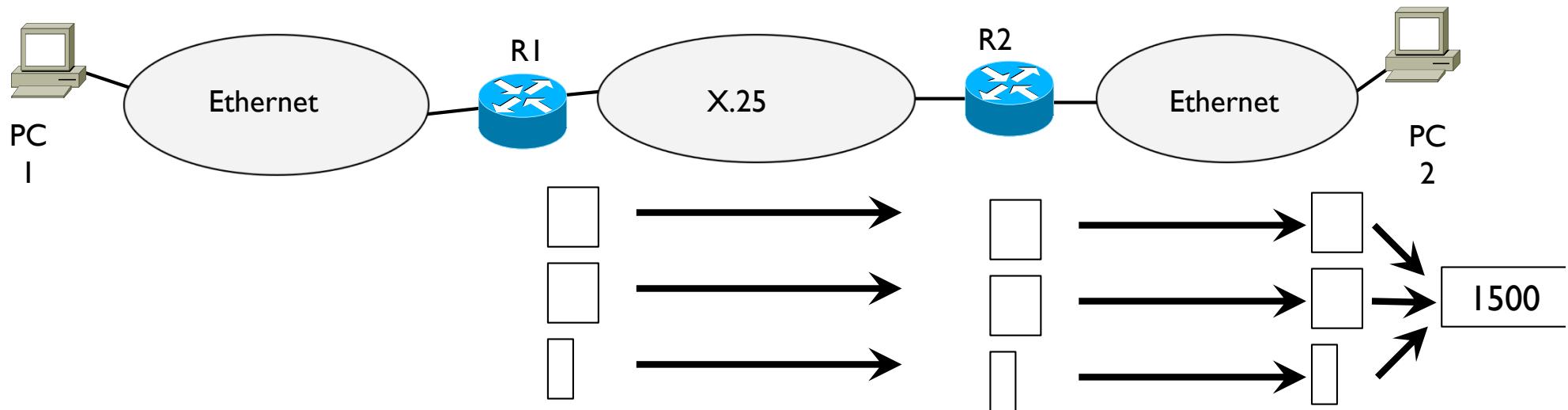
Ejemplo



- ▶ R1 debe fragmentar el datagrama en trocitos más pequeños
- ▶ Cada fragmento debe poderse encapsular en una trama usando X.25

Tema 2 – Cabecera IP

Ejemplo



- ▶ R1 transmite cada fragmento por separado
- ▶ Los fragmentos no se vuelven a juntar hasta el destino aunque se podría hacer antes

Tema 2 – Cabecera IP

Fragmentación

- ▶ Identificación + Flags + Desplazamiento de fragmento
- ▶ Permiten fragmentar un datagrama en fragmentos y volver a juntarlos en orden para volver el datagrama original



Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ **Protocolo ICMP**
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – Protocolo ICMP

- ▶ Internet Control Message Protocol
- ▶ RFC 792
 - ▶ Intercambio de mensajes de **supervisión** (query) o **error** entre dos hosts/routers en una red IP
 - ▶ Se encapsula directamente en datagrama IP (se salta en nivel de transporte)
 - ▶ Se pueden generar directamente a nivel IP o una aplicación
 - ▶ Un ICMP de error no puede generar otro ICMP



Tema 2 – Protocolo ICMP

- ▶ Un mensaje ICMP contiene 4 campos



- ▶ Tipo y código: definen que mensaje ICMP se está transmitiendo
- ▶ Checksum: como en la cabecera IP sirve para detectar error al recibir el mensaje
- ▶ Datos del ICMP: campo que depende del tipo de mensaje
 - ▶ Por ejemplo en el caso de ICMP de error, se copian en este campo los primeros 8 bytes del datagrama que ha generado el error



Tema 2 – Protocolo ICMP

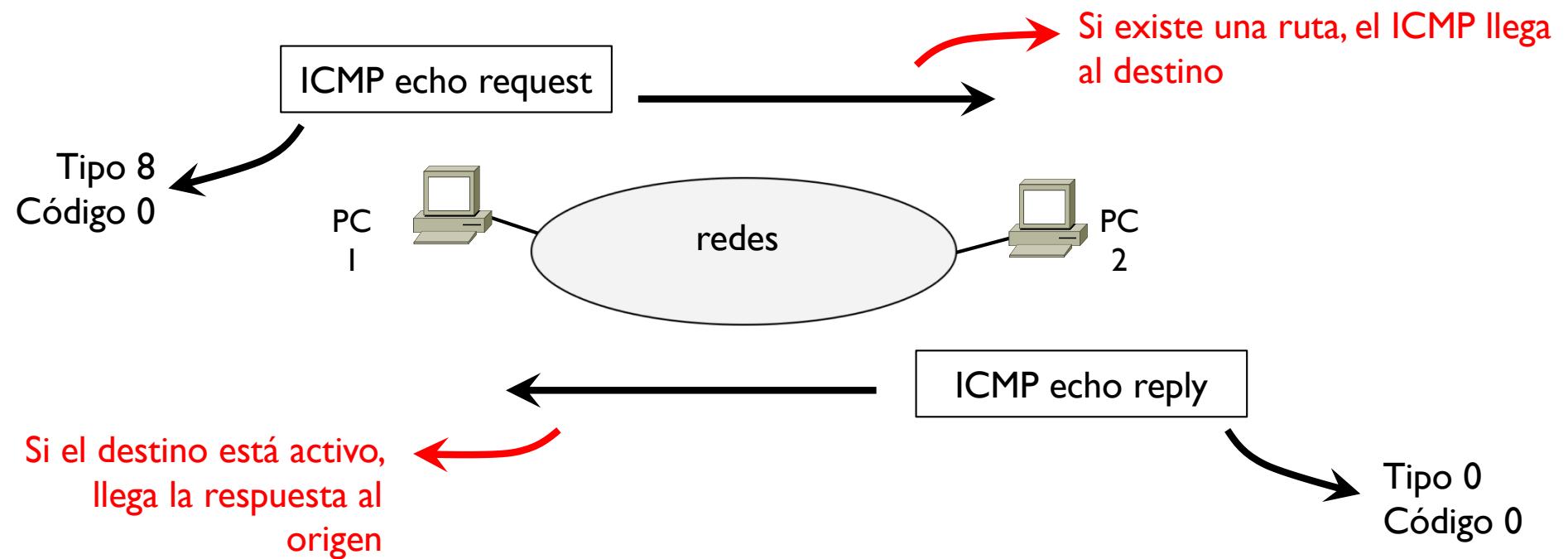
Algunos ejemplos

- ▶ Echo request / echo reply
 - ▶ Query
 - ▶ Se usa en la herramienta ping
 - ▶ Verifica la conectividad entre dos interfaces IP
 - ▶ Destino activo
 - ▶ Ruta existente
 - ▶ Permite medir el tiempo que tarda un datagrama en ir a un destino y volver entre dos interfaces IP
 - ▶ Round Trip Time (RTT)



Tema 2 – Protocolo ICMP

▶ Echo request / echo reply



Tema 2 – Protocolo ICMP

Algunos ejemplos

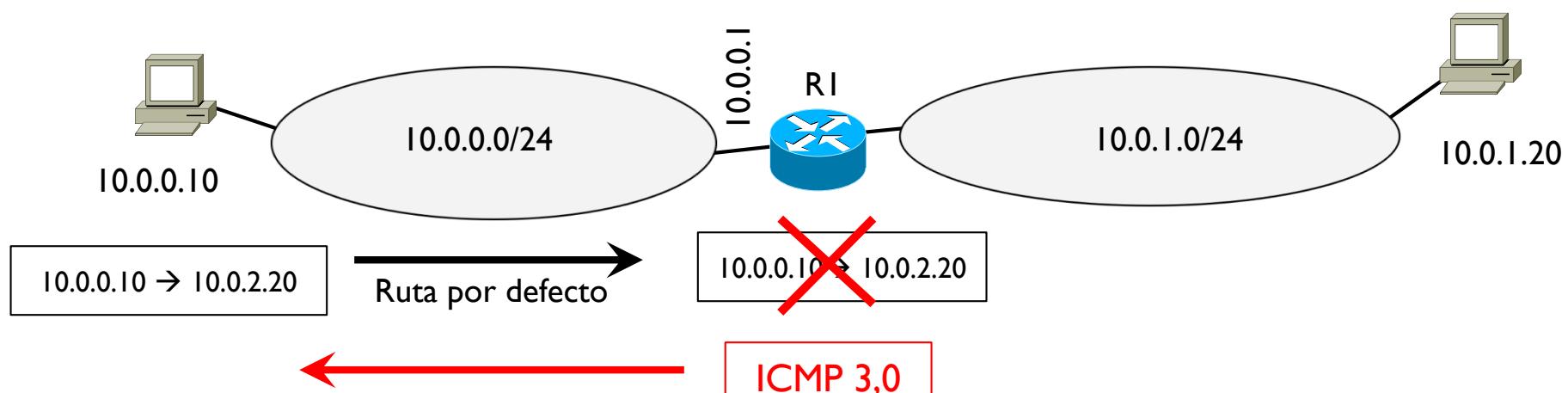
- ▶ Destino inalcanzable
 - ▶ Error
 - ▶ Cuando un datagrama se pierde en algún lugar, se envía un mensaje ICMP de error al origen del datagrama perdido notificando la perdida y a veces sugiriendo una posible solución
 - ▶ Si se pierde un mensaje ICMP de error, este no genera otro mensaje ICMP



Tema 2 – Protocolo ICMP

▶ Destino inalcanzable

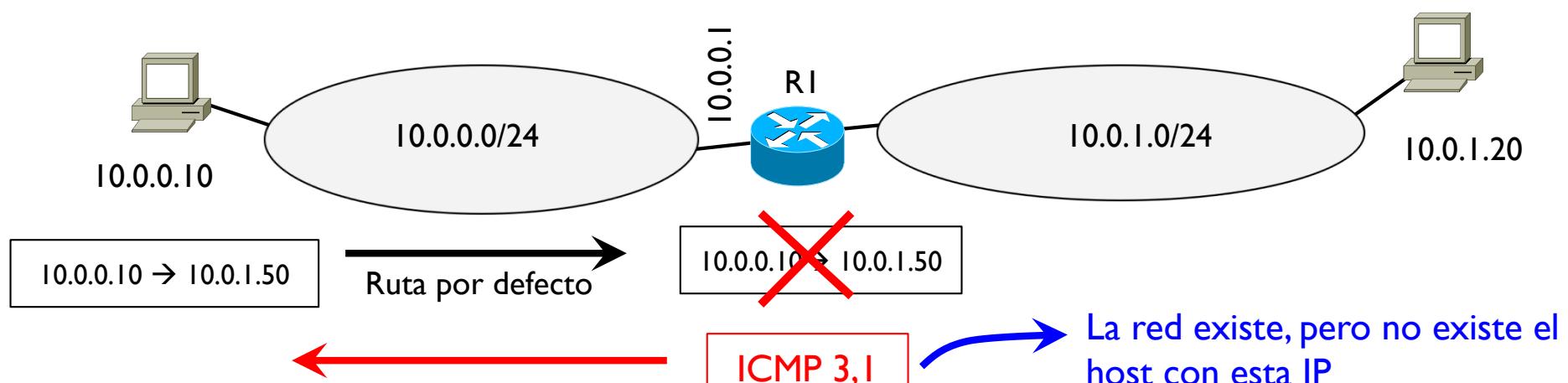
Tipo	Código	Error
3	0	No se llega a la red del destino (network unreachable)
3	1	No se llega al host (host unreachable)
3	2	No se llega al protocolo (protocol unreachable)
3	3	No se llega al puerto (port unreachable)
3	4	Se necesita fragmentación



Tema 2 – Protocolo ICMP

▶ Destino inalcanzable

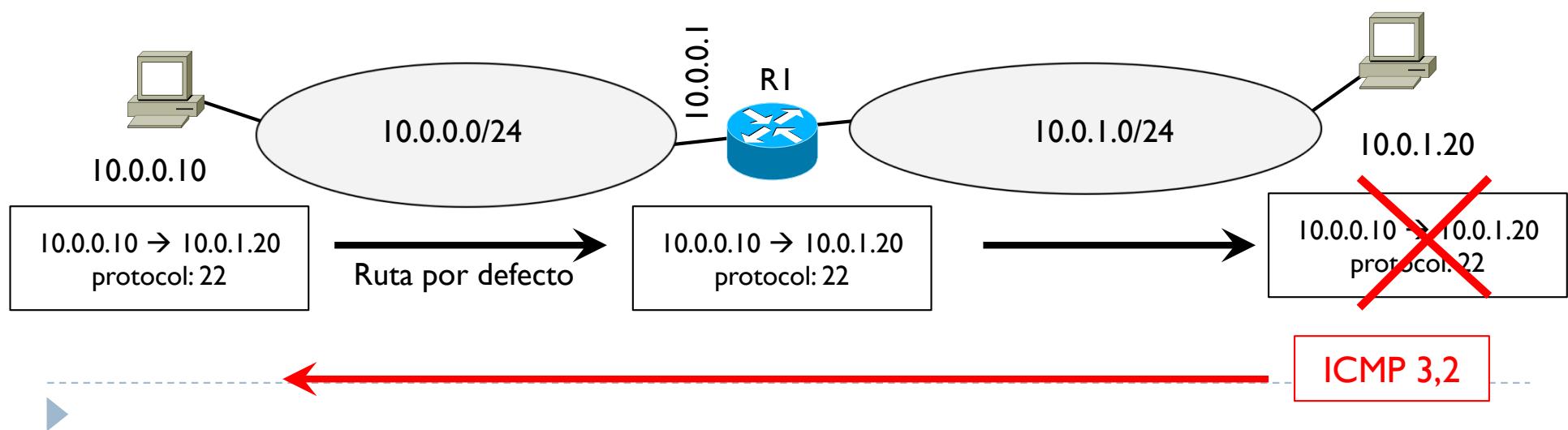
Tipo	Código	Error
3	0	No se llega a la red del destino (network unreachable)
3	1	No se llega al host (host unreachable)
3	2	No se llega al protocolo (protocol unreachable)
3	3	No se llega al puerto (port unreachable)
3	4	Se necesita fragmentación



Tema 2 – Protocolo ICMP

▶ Destino inalcanzable

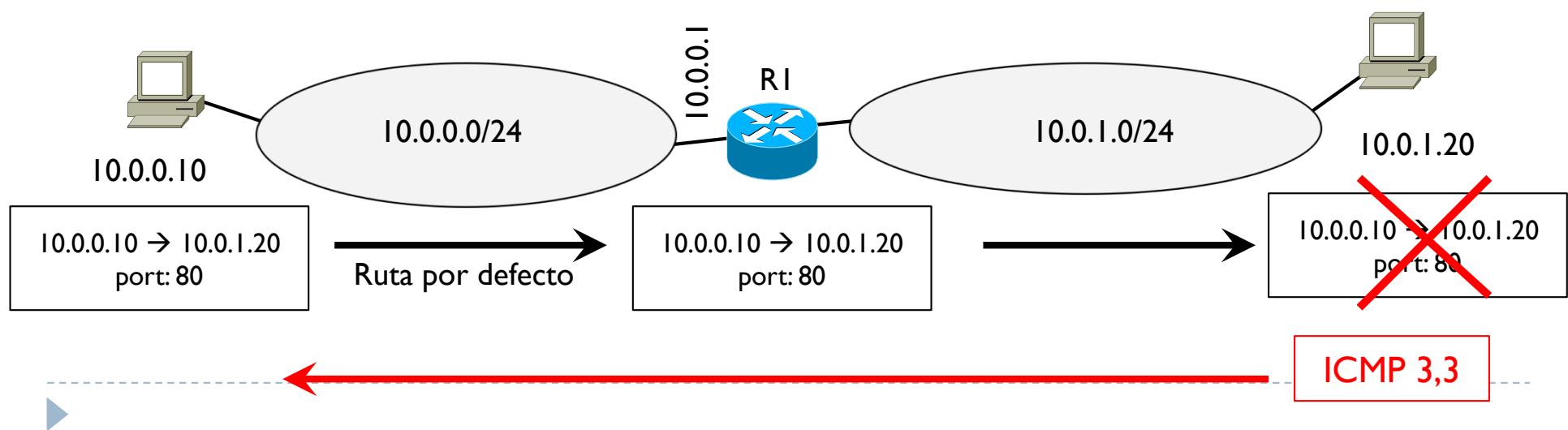
Tipo	Código	Error
3	0	No se llega a la red del destino (network unreachable)
3	1	No se llega al host (host unreachable)
3	2	No se llega al protocolo (protocol unreachable)
3	3	No se llega al puerto (port unreachable)
3	4	Se necesita fragmentación



Tema 2 – Protocolo ICMP

▶ Destino inalcanzable

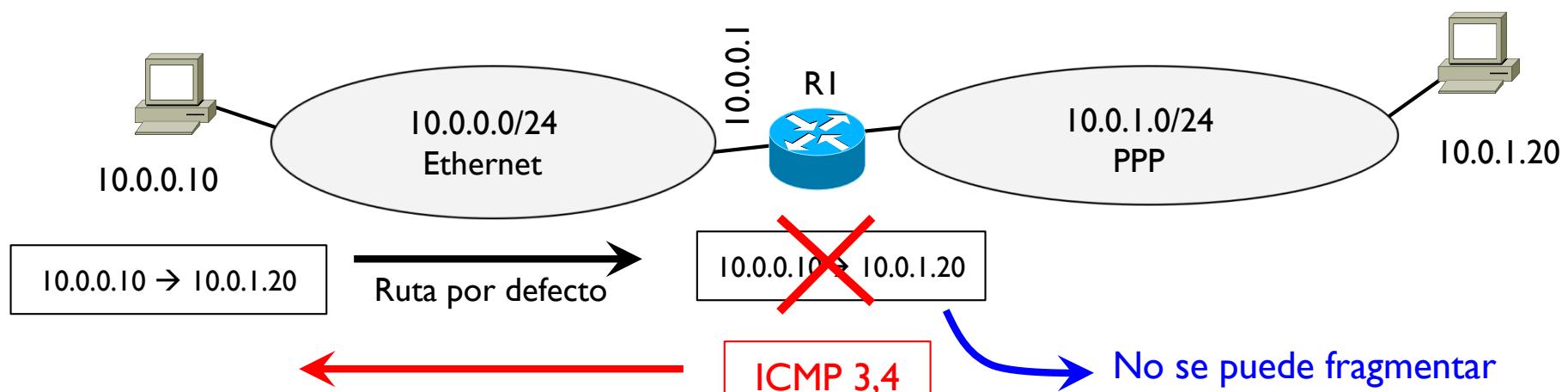
Tipo	Código	Error
3	0	No se llega a la red del destino (network unreachable)
3	1	No se llega al host (host unreachable)
3	2	No se llega al protocolo (protocol unreachable)
3	3	No se llega al puerto (port unreachable)
3	4	Se necesita fragmentación



Tema 2 – Protocolo ICMP

▶ Destino inalcanzable

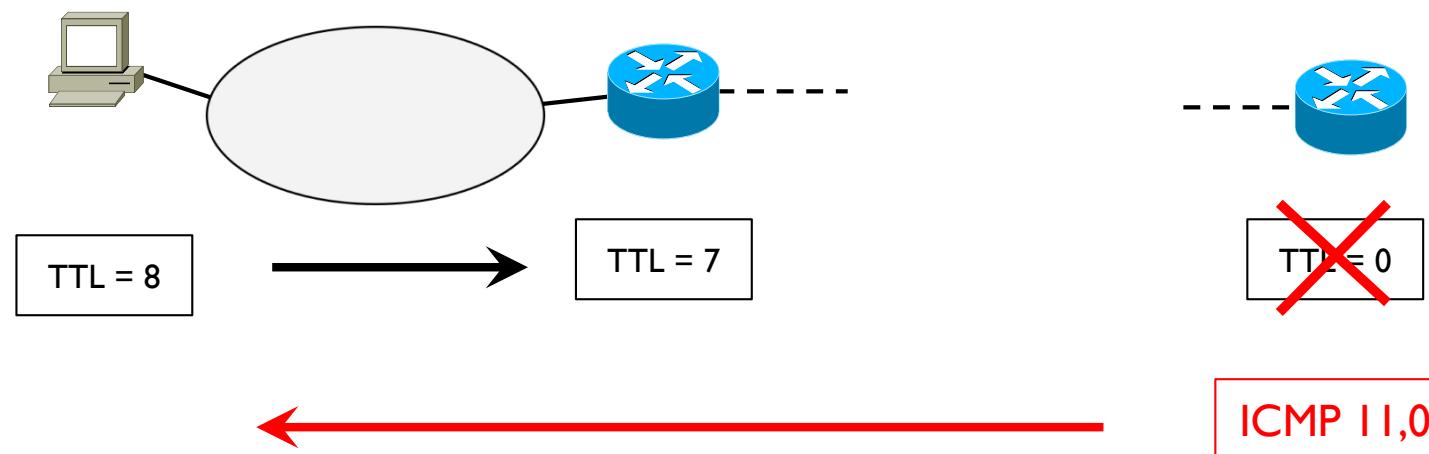
Tipo	Código	Error
3	0	No se llega a la red del destino (network unreachable)
3	1	No se llega al host (host unreachable)
3	2	No se llega al protocolo (protocol unreachable)
3	3	No se llega al puerto (port unreachable)
3	4	Se necesita fragmentación



Tema 2 – Protocolo ICMP

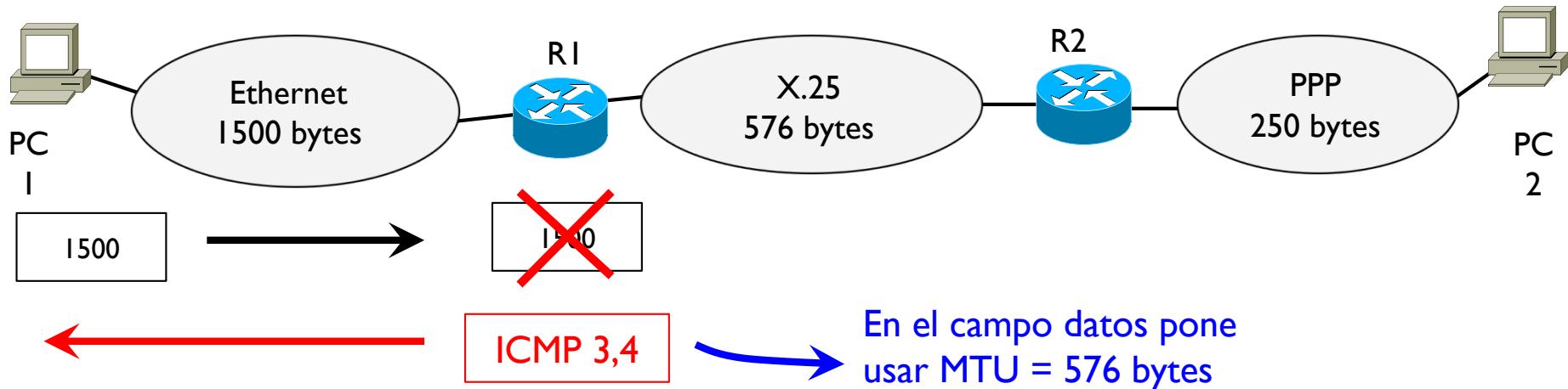
Algunos ejemplos

- ▶ Mensaje de tiempo excedido
 - ▶ Error
 - ▶ Cuando un datagrama llega a tener un TTL de 0
 - ▶ El datagrama se descarta y el router envía al origen un mensaje ICMP tipo 11, código 0



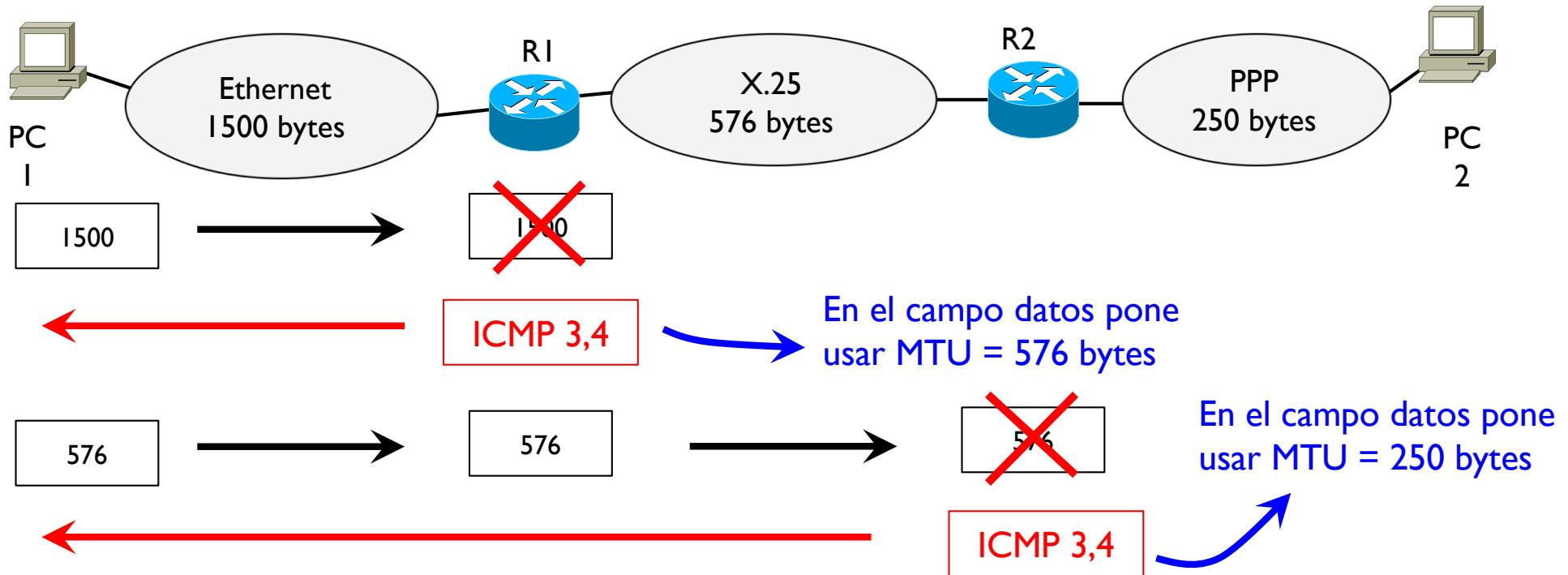
Tema 2 – MTU path discovery

- ▶ RFC 1191
- ▶ Objetivo: evitar la fragmentación de los datagramas
- ▶ Como: averiguar cual es la mínima MTU entre origen y destino usando datagramas que no permiten la fragmentación



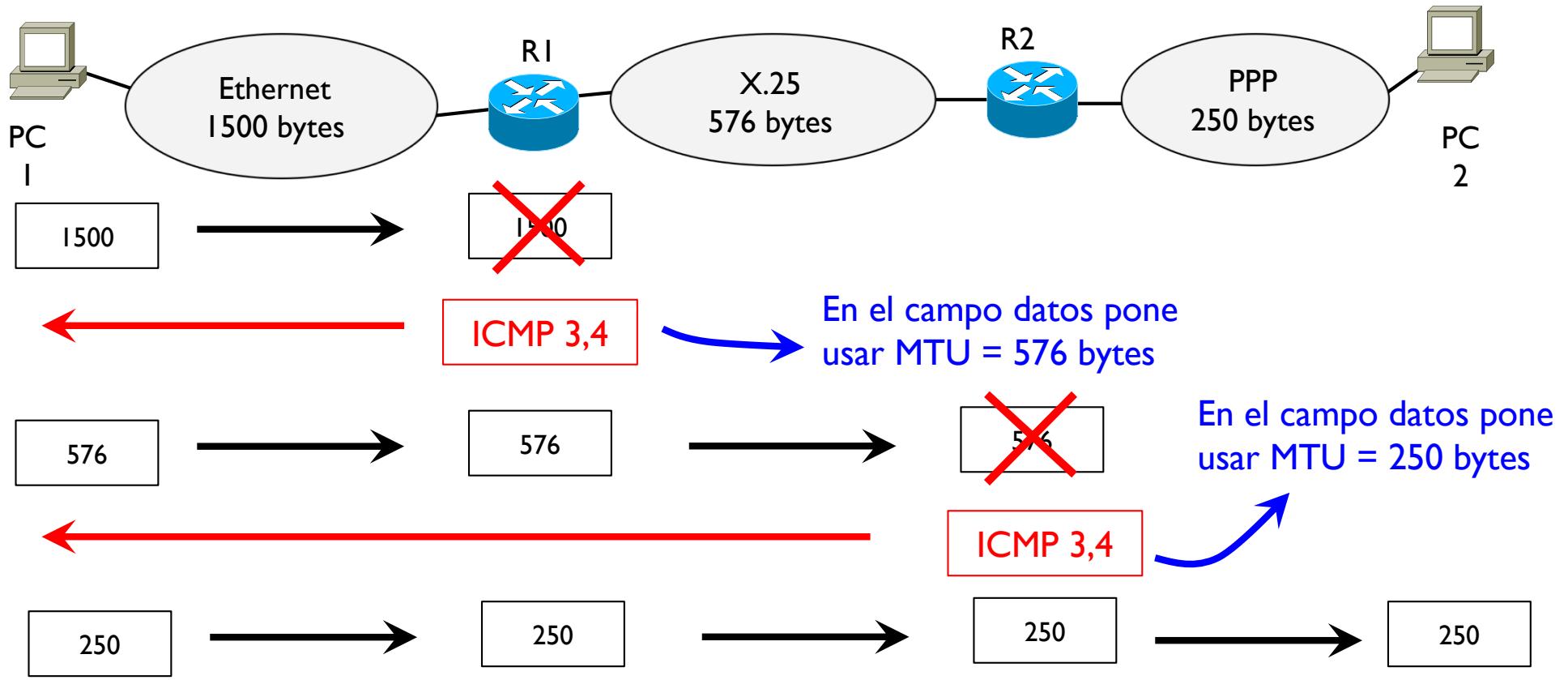
Tema 2 – MTU path discovery

- ▶ RFC 1191
- ▶ Objetivo: evitar la fragmentación de los datagramas
- ▶ Como: averiguar cual es la mínima MTU entre origen y destino usando datagramas que no permiten la fragmentación



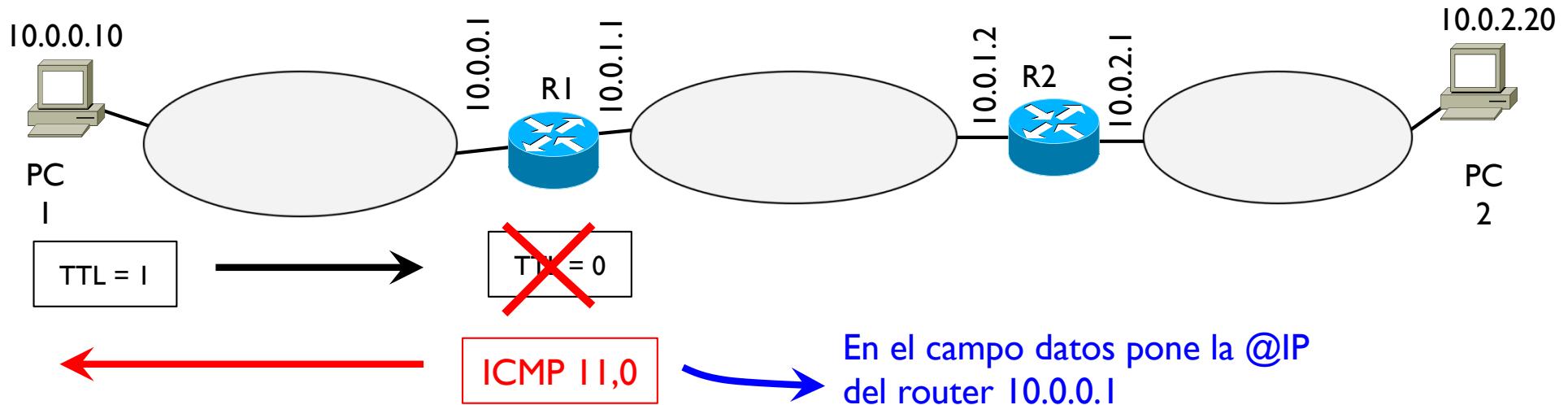
Tema 2 – MTU path discovery

- ▶ RFC 1191
- ▶ Objetivo: evitar la fragmentación de los datagramas
- ▶ Como: averiguar cual es la mínima MTU entre origen y destino usando datagramas que no permiten la fragmentación



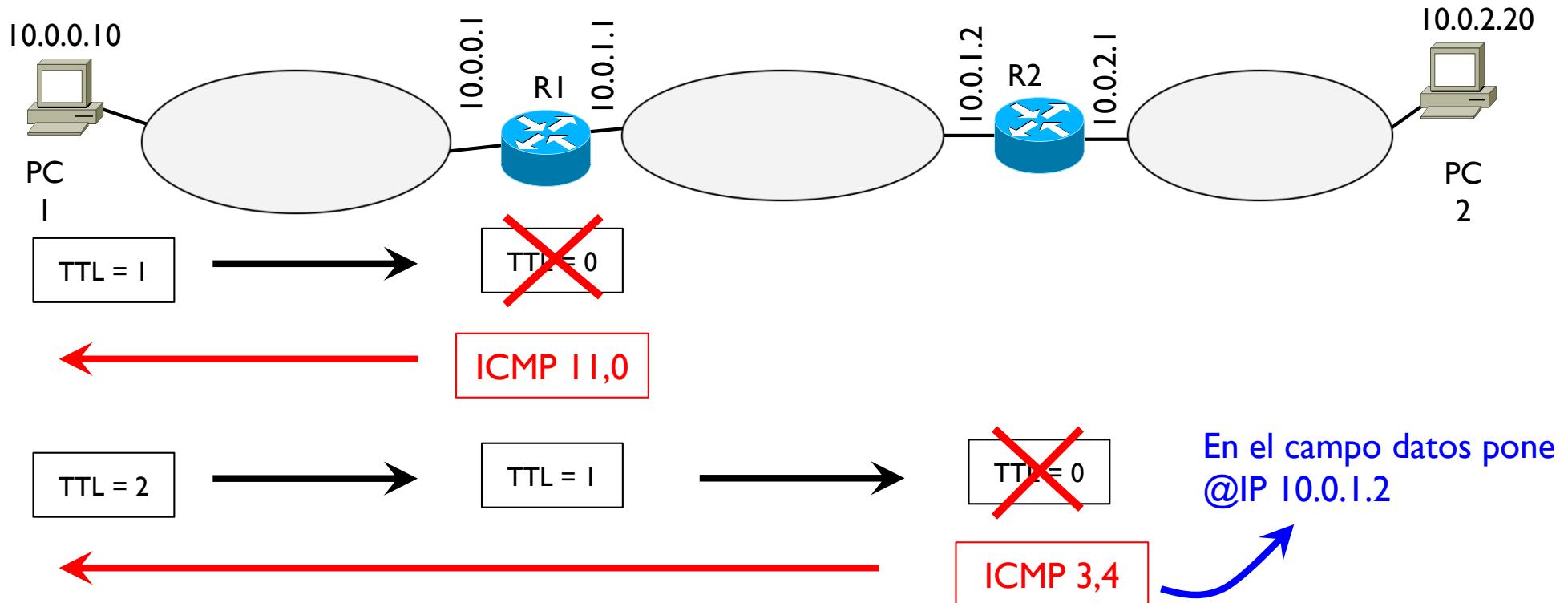
Tema 2 – Traceroute

- ▶ Tracert en Windows
- ▶ Aplicación que permite descubrir la ruta entre un origen y un destino
- ▶ Aprovecha el campo TTL y los mensajes ICMP



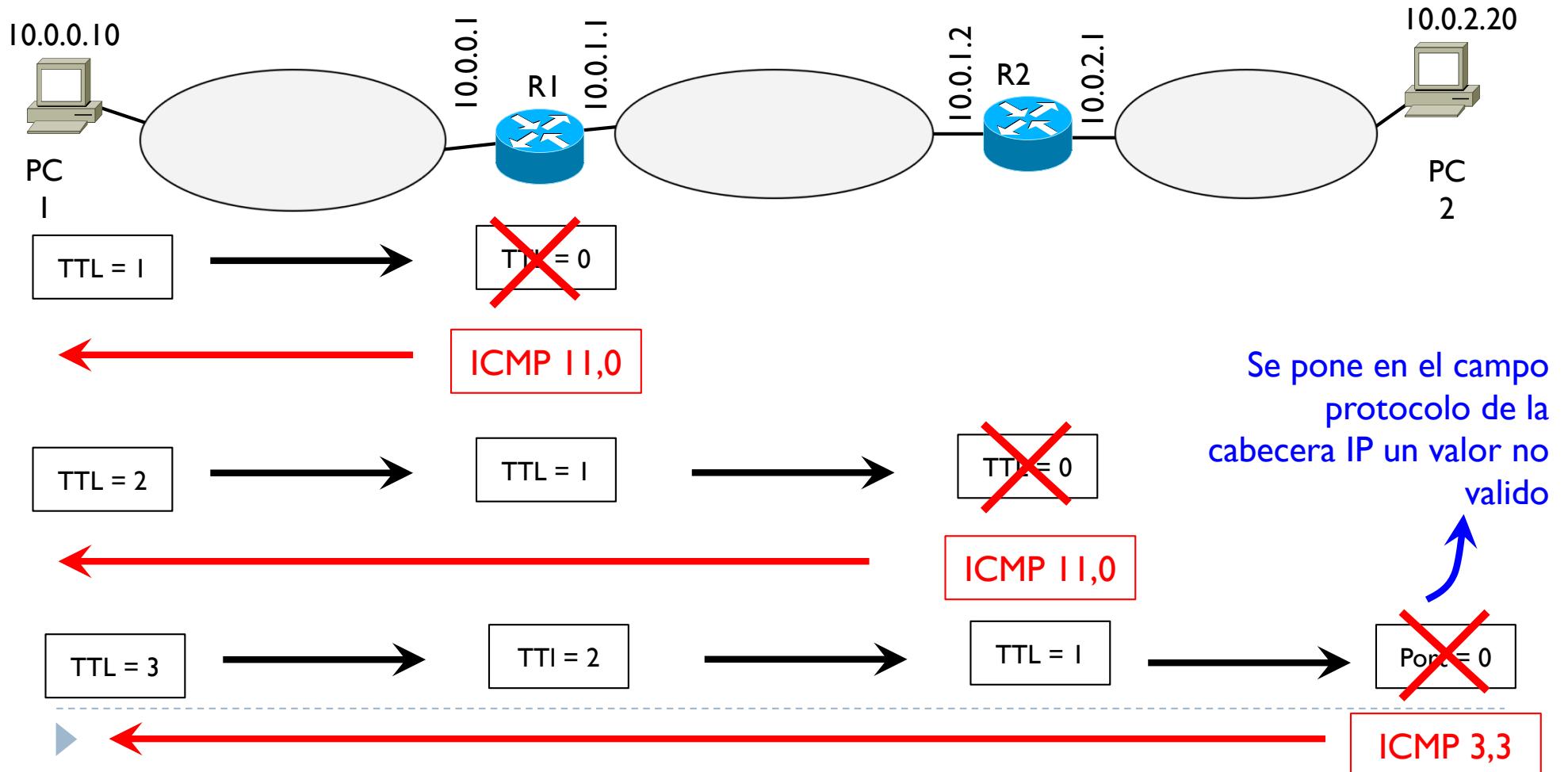
Tema 2 – Traceroute

- ▶ Tracert en Windows
- ▶ Aplicación que permite descubrir la ruta entre un origen y un destino
- ▶ Aprovecha el campo TTL y los mensajes ICMP



Tema 2 – Traceroute

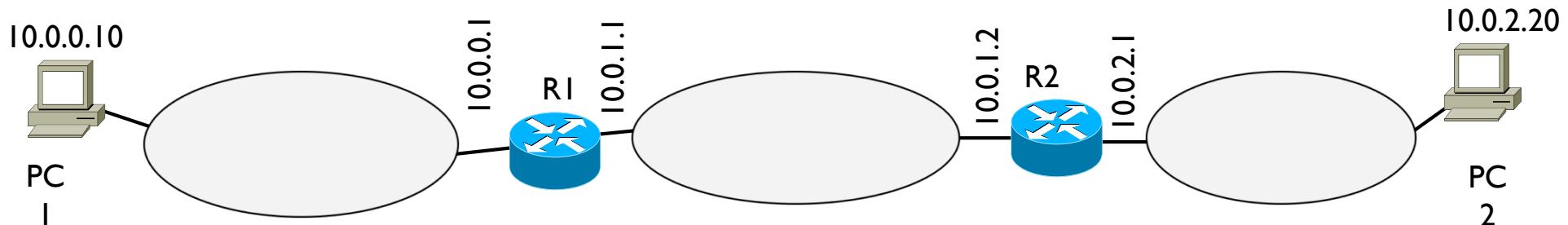
- ▶ Tracert en Windows
- ▶ Aplicación que permite descubrir la ruta entre un origen y un destino
- ▶ Aprovecha el campo TTL y los mensajes ICMP



Tema 2 – Traceroute

- ▶ Cada datagrama se envía 3 veces y la aplicación calcula el tiempo que se tarda para llegar a cada punto
 - ▶ El * indica que no se ha recibido el ICMP (por ejemplo se ha perdido)
- ▶ Por ejemplo, si desde PC1 10.0.0.10 se hace
- ▶ Traceroute 10.0.2.20

10.0.0.1	3 ms	2 ms	3 ms
10.0.1.2	5 ms	5 ms	6 ms
10.0.2.20	7 ms	*	8 ms



Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ **Protocolo DHCP**
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – DHCP

- ▶ La configuración de red de un host puede ser
 - ▶ Manual, un administrador la configura
 - ▶ Automática, a través de una aplicación de red y su protocolo
 - ▶ BOOTP (protocolo ya antiguo)
 - ▶ DHCP
- ▶ Dynamic Host Configuration Protocol
- ▶ RFC 2131



Tema 2 – DHCP

- ▶ Se basa en el paradigma cliente-servidor
- ▶ Un servidor DHCP puede asignar @IP a clientes y proporcionar parámetros adicionales de configuración
 - ▶ Mascara
 - ▶ Gateway (ruta por defecto para salir de la red)
 - ▶ Hostname, el nombre del cliente
 - ▶ Domain name, el nombre del dominio al que pertenece el cliente
 - ▶ @IP del servidor DNS del dominio
 - ▶ Servicios adicionales como un proxy
 - ▶ Etc.

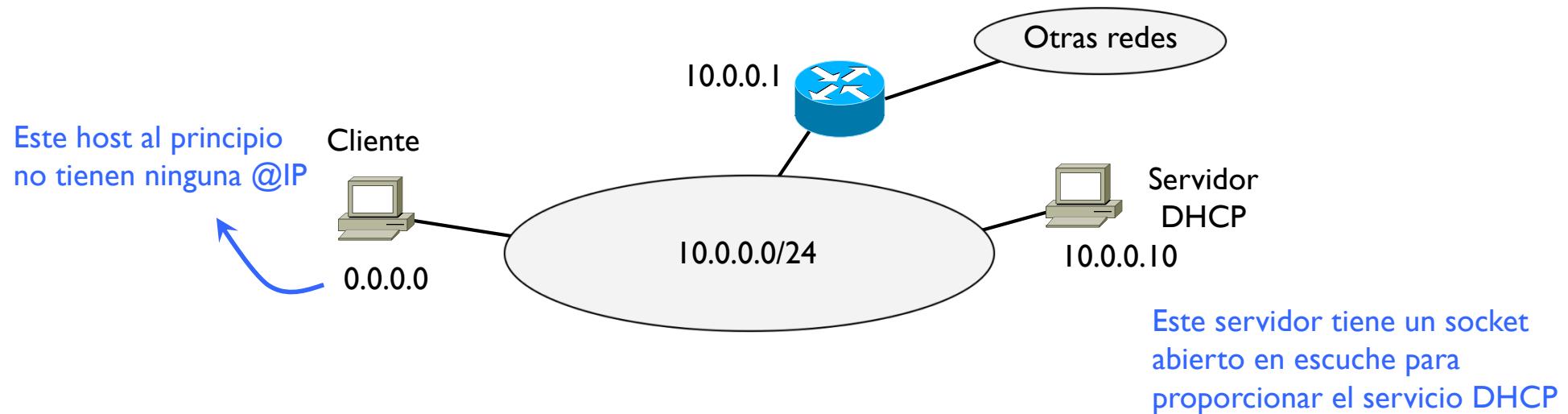


Tema 2 – DHCP

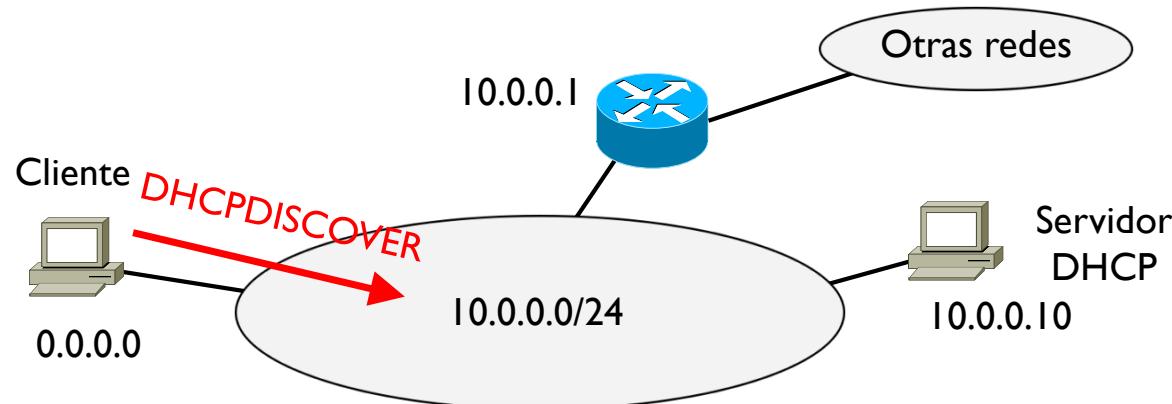
- ▶ La asignación puede ser
 - ▶ **Automática**, sin límite de tiempo (hasta que el cliente no libere la @IP, por ejemplo apagándose)
 - ▶ **Dinámica**, durante un periodo de tiempo determinado por el servidor
 - ▶ **Manual**, el servidor asigna @IP a determinadas direcciones MAC previamente configuradas manualmente por el administrador
- ▶ DHCP usa UDP como transporte
 - ▶ Servidor: puerto 67
 - ▶ Cliente: puerto 68



Tema 2 – DHCP ejemplo



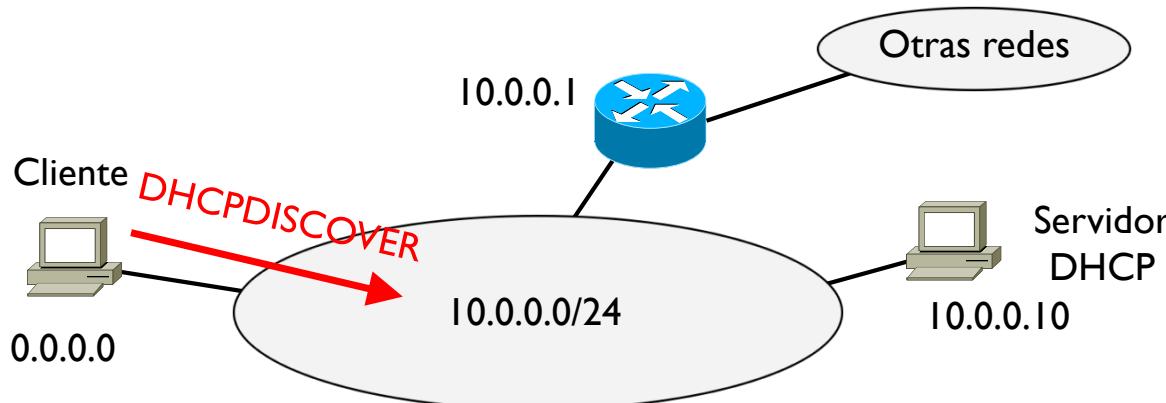
Tema 2 – DHCP ejemplo



Al arrancar la aplicación
DHCP en el cliente, este
envía un mensaje
DHCPDISCOVER para
descubrir si hay un servidor
DHCP en la red



Tema 2 – DHCP ejemplo



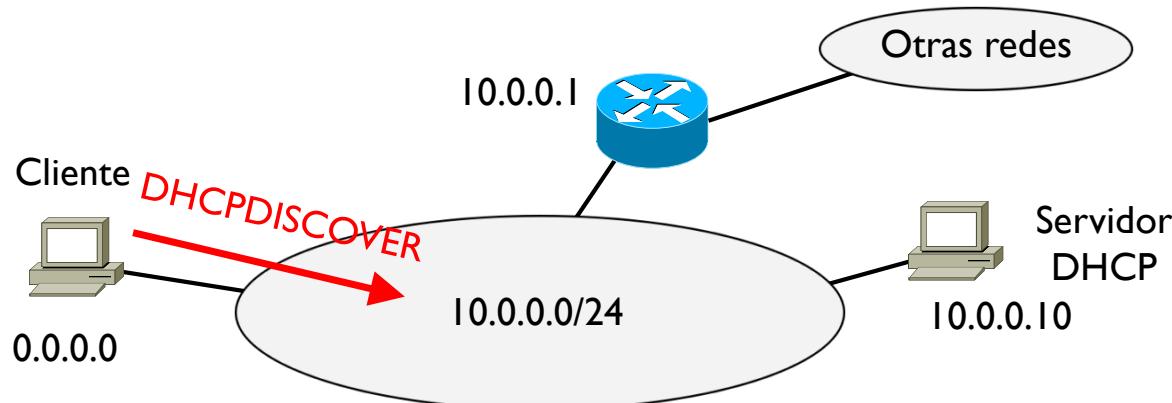
DHCPDISCOVER

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino 255.255.255.255

Como no se conoce la @IP del servidor ni tampoco la dirección de red, envía un datagrama con destino todos bits a 1, es decir 255.255.255.255
Este datagrama llega a todos los hosts y routers de la red



Tema 2 – DHCP ejemplo



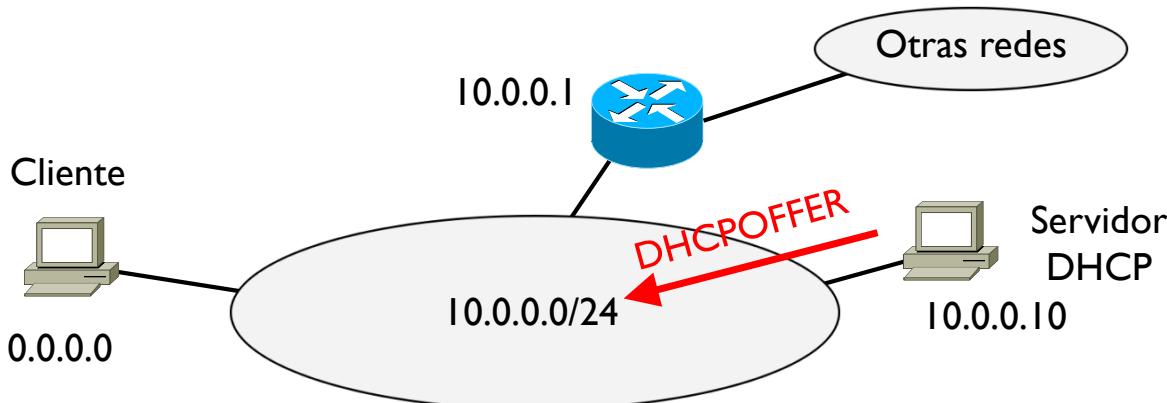
DHCPDISCOVER

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino
255.255.255.255

Al recibir este mensaje, todos los demás hosts lo descartarán ya que no tienen la aplicación con puerto 67 (servidor DHCP)
El servidor DHCP lee el mensaje y contesta



Tema 2 – DHCP ejemplo



DHCPDISCOVER

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino
255.255.255.255

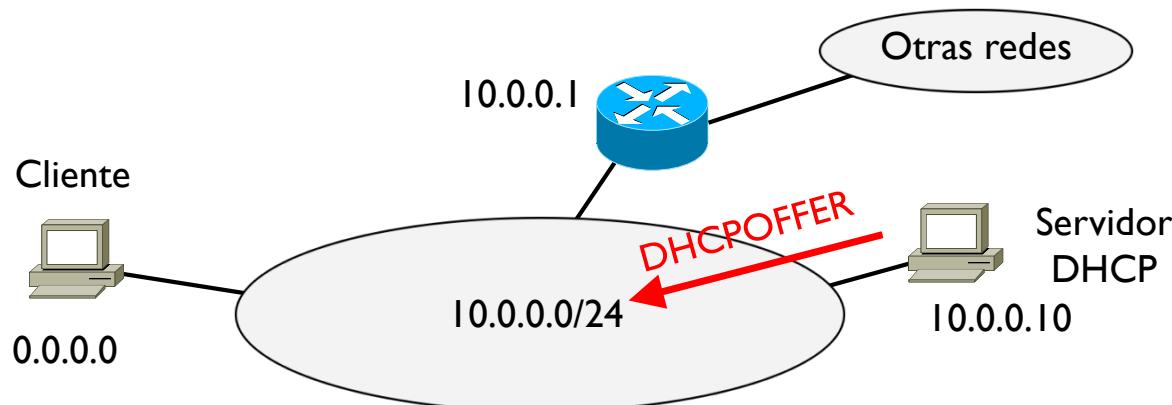
DHCPOFFER

- puerto origen 67
- puerto destino 68
- @IP origen 10.0.0.10
- @IP destino
255.255.255.255

Como el cliente aún no tiene @IP, se envía con destino 255.255.255.255
Este datagrama llega a todos los hosts y routers de la red



Tema 2 – DHCP ejemplo



DHCPDISCOVER

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino
255.255.255.255

Todos los demás hosts lo descartarán (puerto 68, aplicación cliente DHCP)
El cliente DHCP lee el mensaje y contesta con una petición explícita al servidor para poder configurarse con la @IP y los parámetros recibidos

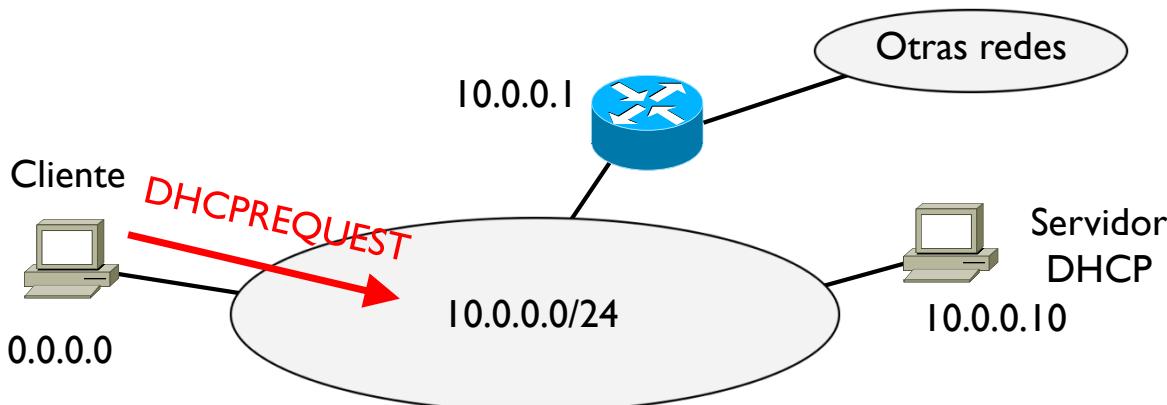
DHCPOFFER

- puerto origen 67
- puerto destino 68
- @IP origen 10.0.0.10
- @IP destino
255.255.255.255

Este mensaje contiene la @IP ofrecida y los demás parámetros de configuración



Tema 2 – DHCP ejemplo



DHCPDISCOVER

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino
255.255.255.255

DHCPOFFER

- puerto origen 67
- puerto destino 68
- @IP origen 10.0.0.10
- @IP destino
255.255.255.255

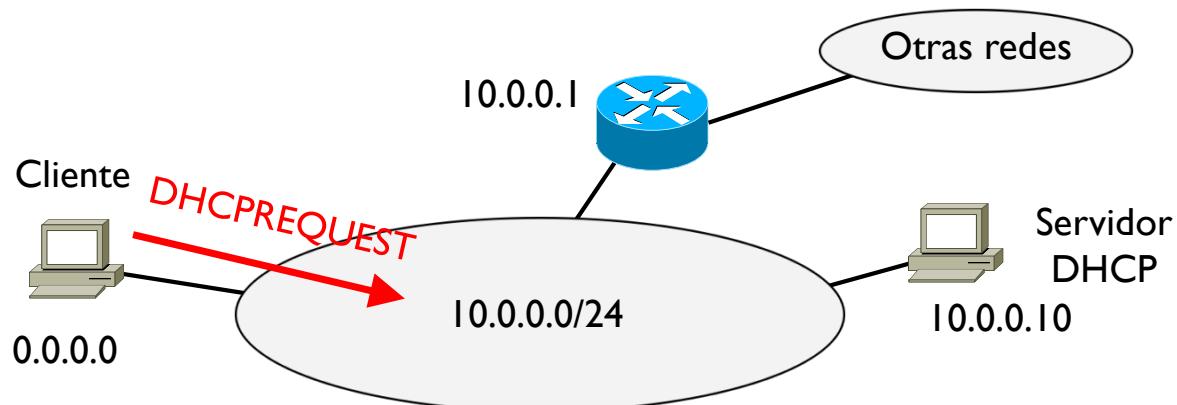
DHCPREQUEST

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino
255.255.255.255

Como aún no tiene @IP definitiva, se sigue usando @IP origen 0.0.0.0 y destino 255.255.255



Tema 2 – DHCP ejemplo



DHCPDISCOVER

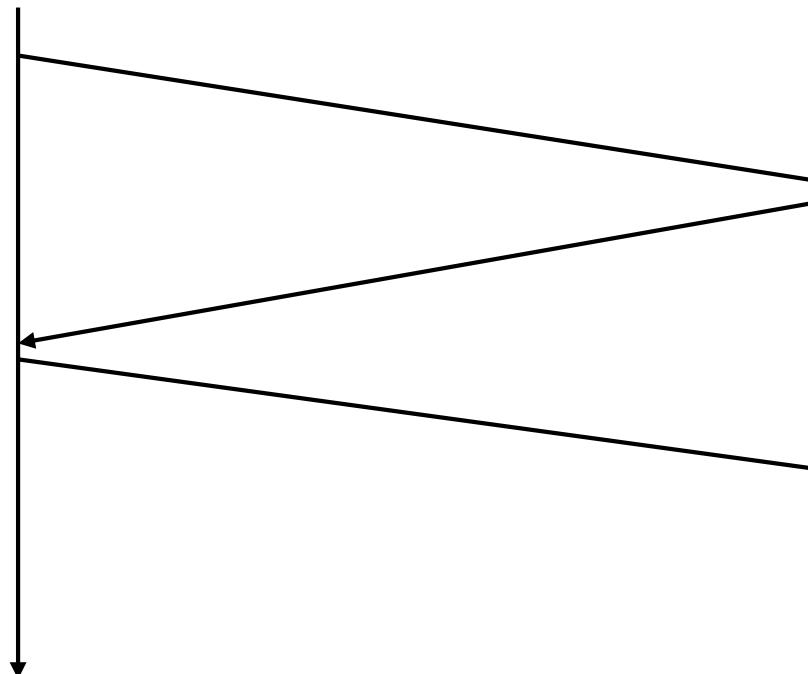
- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino
255.255.255.255

DHCPOFFER

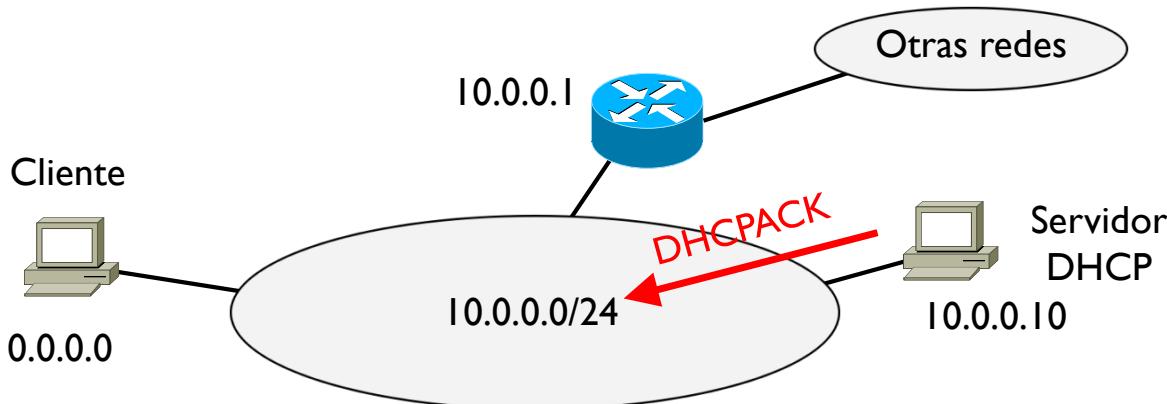
- puerto origen 67
- puerto destino 68
- @IP origen 10.0.0.10
- @IP destino
255.255.255.255

DHCPREQUEST

Todos los demás hosts lo descartarán (puerto 67, servidor DHCP)
El servidor DHCP lee el mensaje y contesta con un mensaje de confirmación final



Tema 2 – DHCP ejemplo



DHCPDISCOVER

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino 255.255.255.255

DHCPOFFER

DHCPOFFER

- puerto origen 67
- puerto destino 68
- @IP origen 10.0.0.10
- @IP destino 255.255.255.255

DHCPREQUEST

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino 255.255.255.255

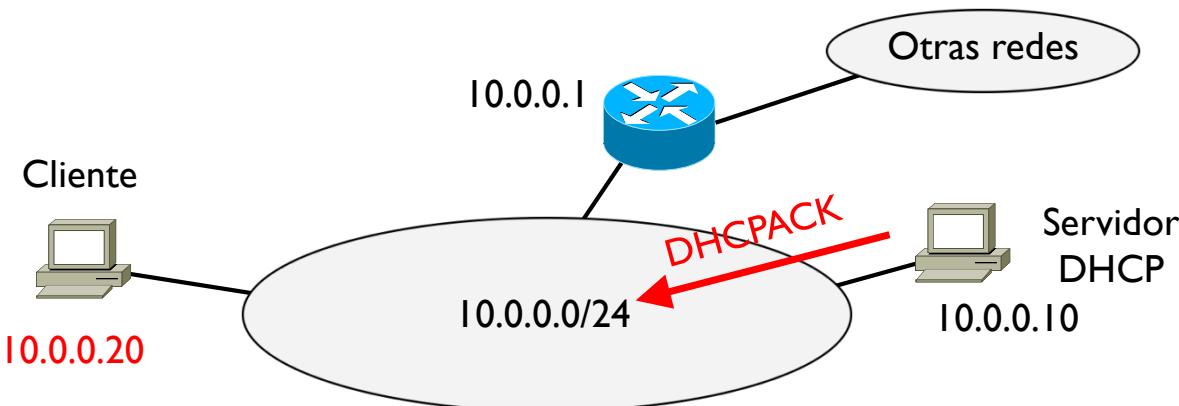
DHCPACK

- puerto origen 67
- puerto destino 68
- @IP origen 10.0.0.10
- @IP destino 255.255.255.255

Confirmación final que el cliente se puede configurar según lo ofrecido con DHCPOFFER



Tema 2 – DHCP ejemplo



DHCPDISCOVER

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino
255.255.255.255

DHCPOFFER

DHCPOFFER

- puerto origen 67
- puerto destino 68
- @IP origen 10.0.0.10
- @IP destino
255.255.255.255

DHCPREQUEST

- puerto origen 68
- puerto destino 67
- @IP origen 0.0.0.0
- @IP destino
255.255.255.255

El cliente se configura

DHCPACK

- puerto origen 67
- puerto destino 68
- @IP origen 10.0.0.10
- @IP destino
255.255.255.255

Tema 2 – DHCP detalles

- ▶ **Servidor y cliente deben estar en la misma red**
 - ▶ Porque cliente y servidor necesitan comunicarse sin que el cliente tenga configuración alguna
 - ▶ Existen DHCP relay agents que permiten retransmitir mensajes DHCP entre redes distintas (se necesita entonces un agent por red)
- ▶ **En una misma red puede haber más de un servidor DHCP**
 - ▶ Por razones de protección ante posibles fallos
 - ▶ En este caso todos contestarían con un DHCPOFFER y el cliente puede elegir uno y excluir los demás (especificándolo en el DHCPREQUEST)
- ▶ **Si un cliente se apaga y rearrastra**
 - ▶ Puede mantener la misma configuración y empezar directamente desde el paso (3)



Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ **Mecanismo NAT**
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad

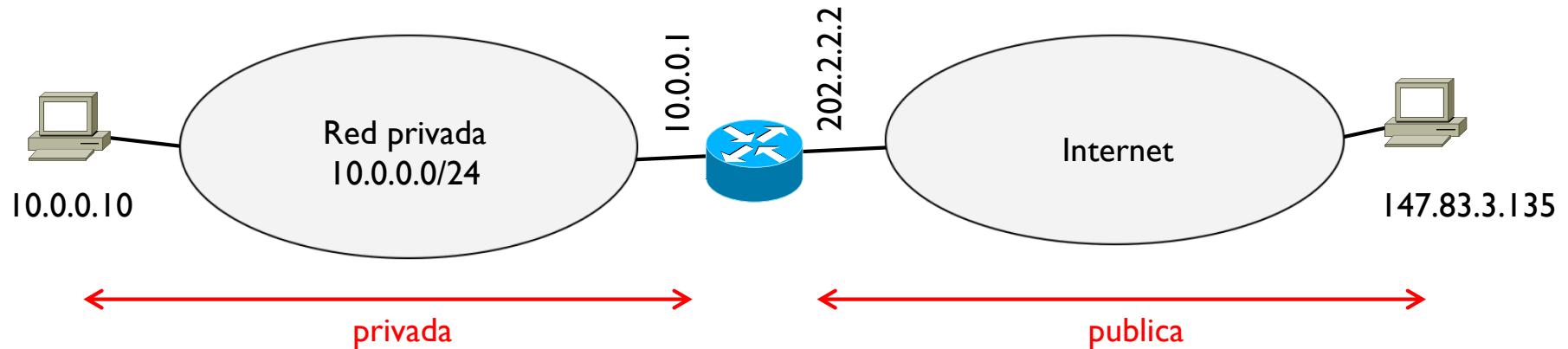


Tema 2 – NAT

- ▶ Network Address Translation
- ▶ RFC 1631, 2663, 3022
- ▶ Es un mecanismo (no es un protocolo)
- ▶ Objetivo
 - ▶ Permitir el uso de direcciones privadas (no visibles desde Internet) pero poder igualmente acceder a Internet
- ▶ Como
 - ▶ Traduciendo direcciones privadas en direcciones públicas
- ▶ Ventajas
 - ▶ Seguridad
 - ▶ Permite ahorrar @IP en Internet
 - ▶ Administración de la red (no depende de Internet ni del ISP)



Tema 2 – NAT



- ▶ Considerar un host en una red privada
- ▶ Si no hubiera NAT, este host no podría acceder ni recibir nada de Internet ya que su **@IP** es privada
- ▶ Se necesita configurar el router para que implemente NAT
 - ▶ Un router con NAT mantiene una tabla NAT donde se asocian **@IP** publicas con **@IP** privadas

Tema 2 – NAT

- ▶ **NAT estático**
 - ▶ Se asigna una @IP publica a una @IP privada
 - ▶ Principalmente para servidores
- ▶ **NAT dinámico**
 - ▶ Se configura un rango de @IP publicas y se asignan a las @IP privadas según se necesite
 - ▶ Principalmente para clientes
- ▶ **PAT o NAT por puertos o NAT overload**
 - ▶ Se usa una única @IP publica (generalmente la @IP del router hacia Internet) y se configura un rango de puertos
 - ▶ Todas las @IP privadas que van a Internet se traducen con la misma @IP publica
 - ▶ Principalmente para redes pequeñas



Tema 2 – NAT estático

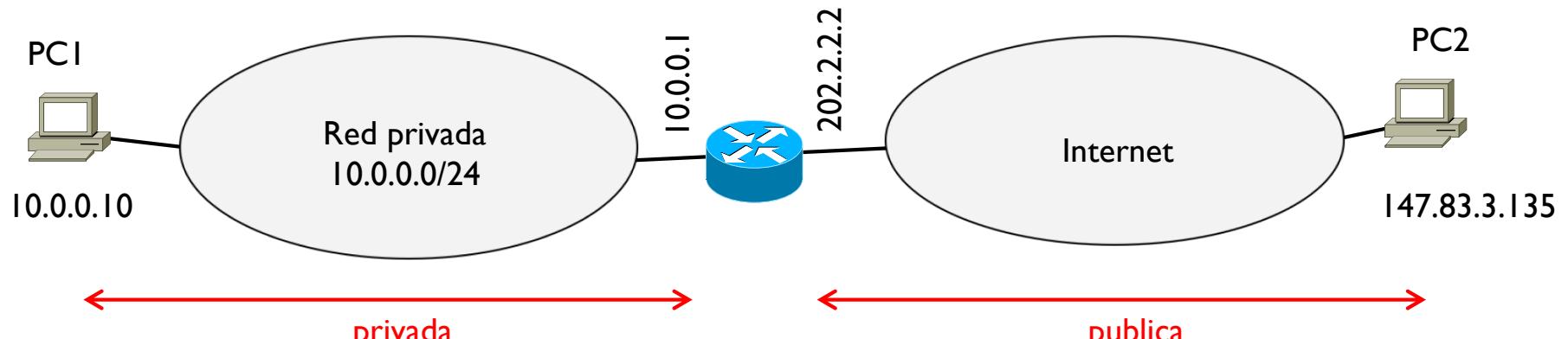
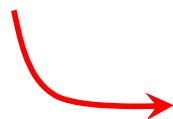


Tabla NAT

Direcciones internas	Direcciones externas



El router mantiene una tabla NAT con una columna con @IP internas (privadas) y otra columna con @IP externas (públicas)



Tema 2 – NAT estático

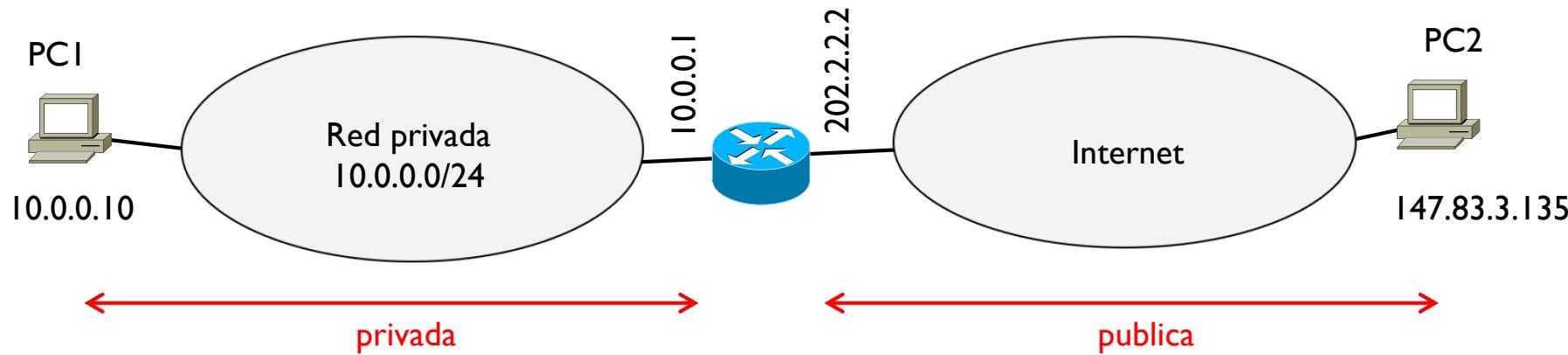
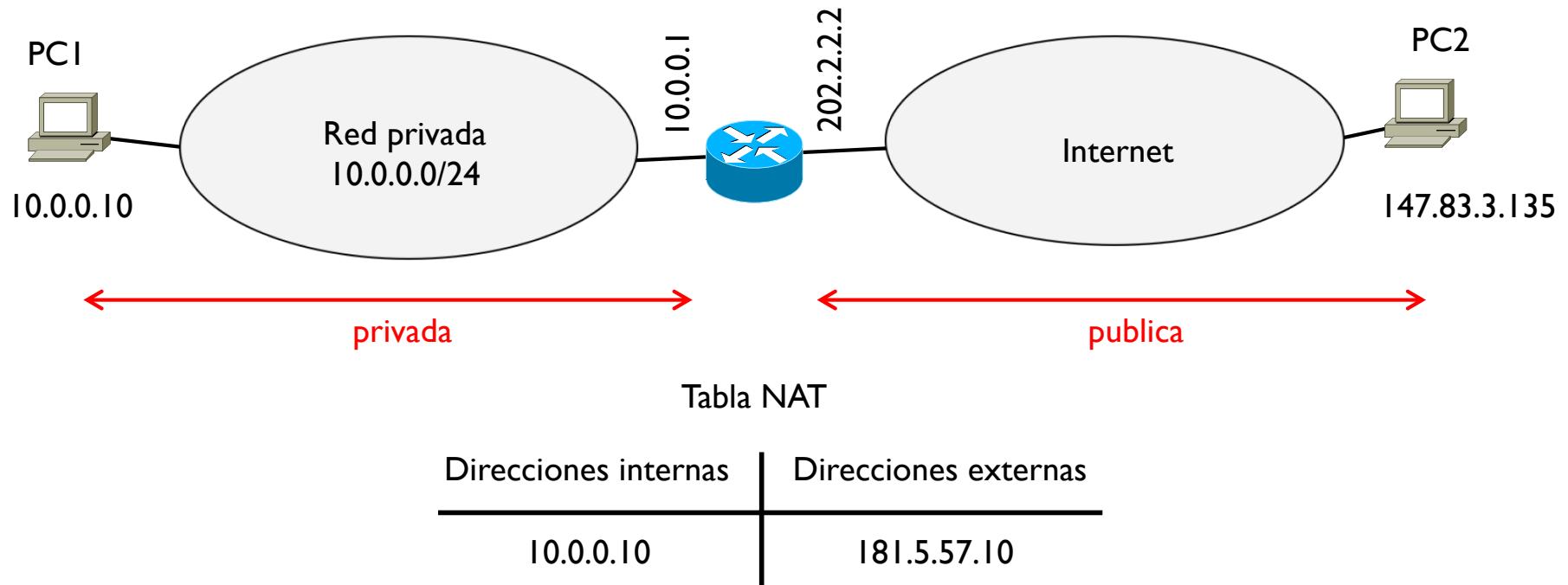


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10

En el caso de NAT estático, en el router se configura la traducción de la @IP privada 10.0.0.10 a la @IP pública 181.5.57.10

Tema 2 – NAT estático



10.0.0.10
→
147.83.3.135

El host interno PC1 quiere transmitir a PC2 de Internet
El datagrama tendrá estas @IP origen y destino



Tema 2 – NAT estático

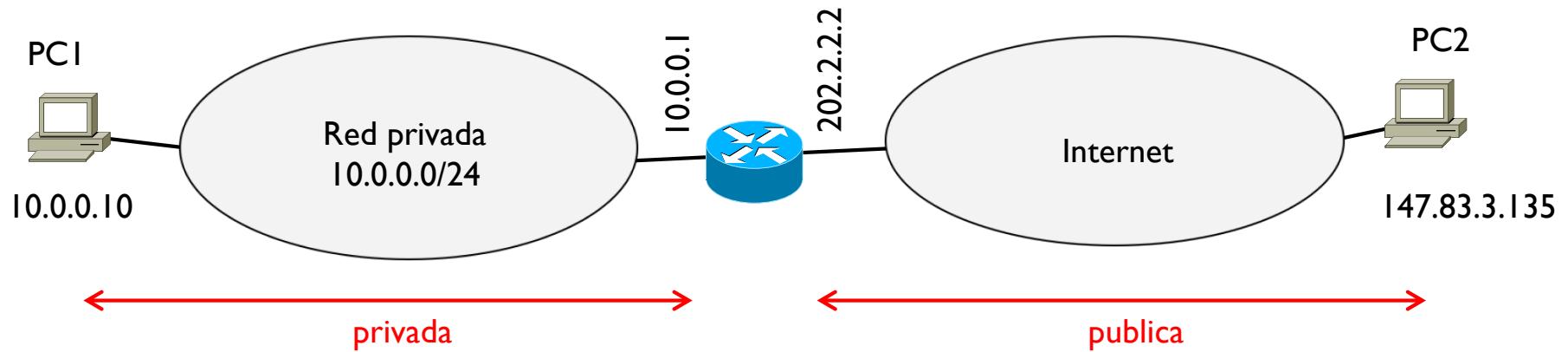
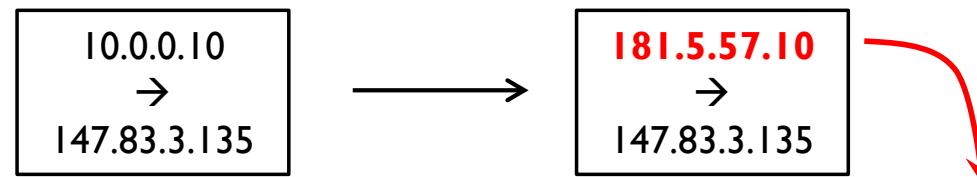


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



El router no puede transmitir este datagrama en Internet con esta @IP origen
El router substituye la @IP origen por la @IP que tiene asociada en la tabla NAT



Tema 2 – NAT estático

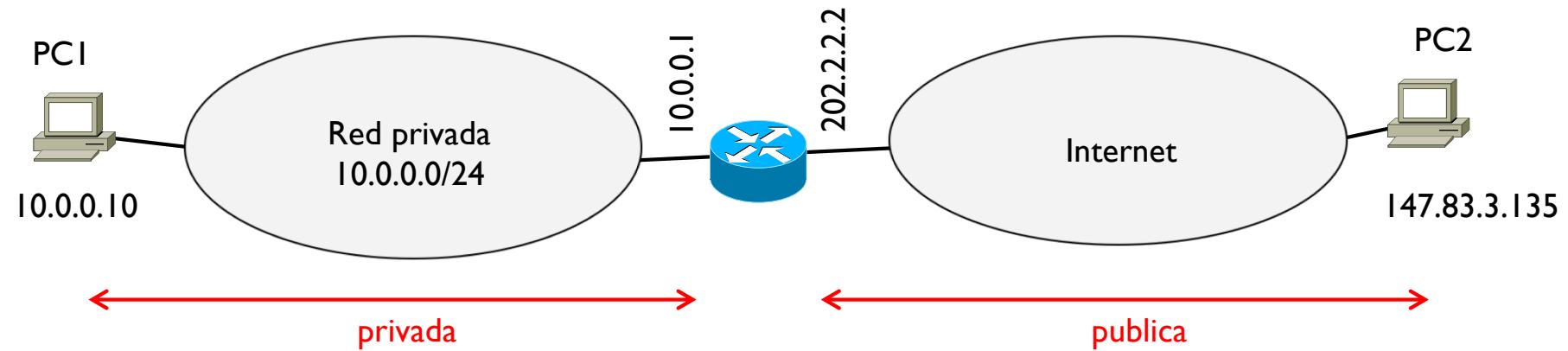
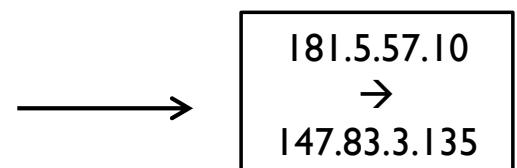


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



El destino PC2 recibe este datagrama con esta @IP origen
PC2 no puede saber cual es la @IP real de PCI



Tema 2 – NAT estático

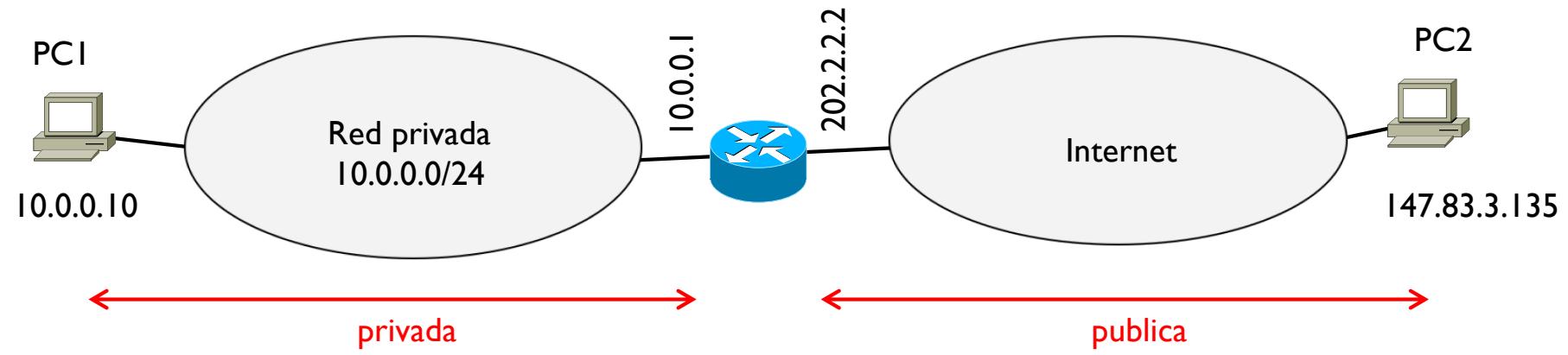
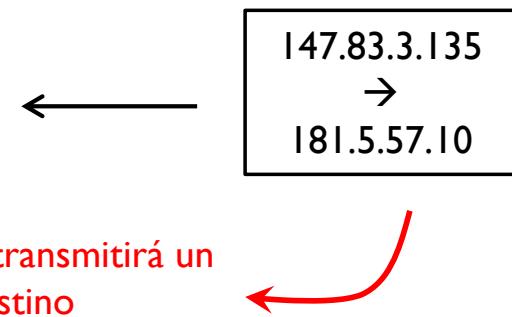


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



Si PC2 quiere contestar al PC1, PC2 transmitirá un datagrama con estas @IP origen y destino
Para PC2, la @IP de PC1 es 181.5.57.10



Tema 2 – NAT estático

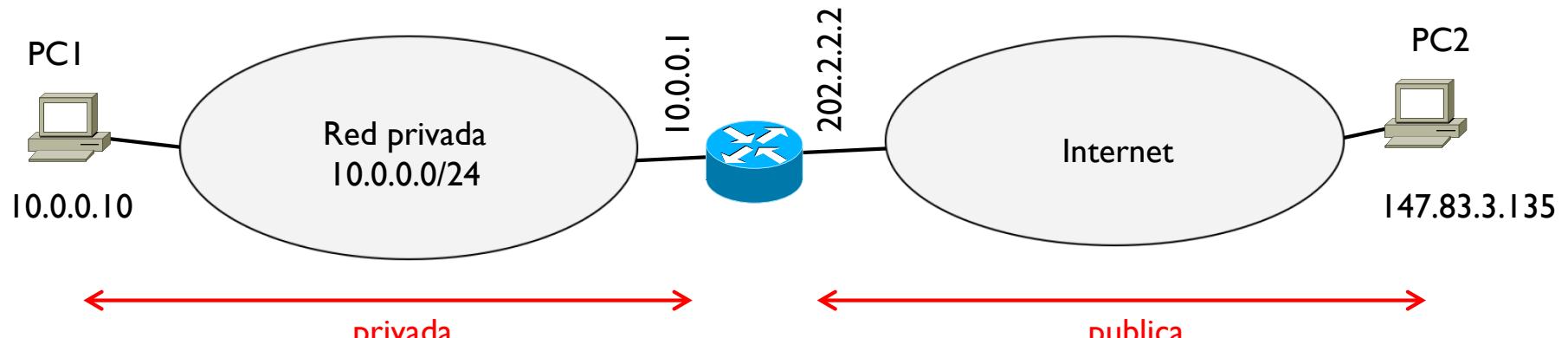
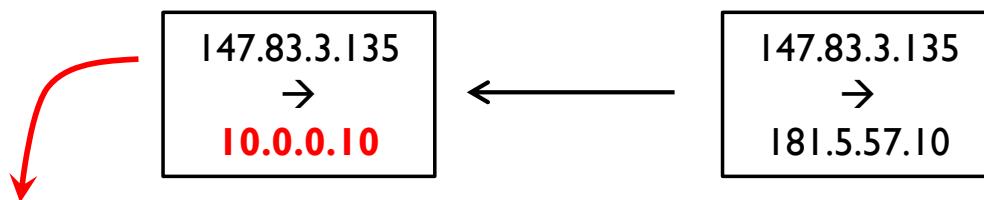


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



Cuando el datagrama llega al router, este hará la substitución inversa: cambia la @IP publica 181.5.57.10 en la @IP privada interna de PCI
En este caso la que cambia es la @IP destino



Tema 2 – NAT estático

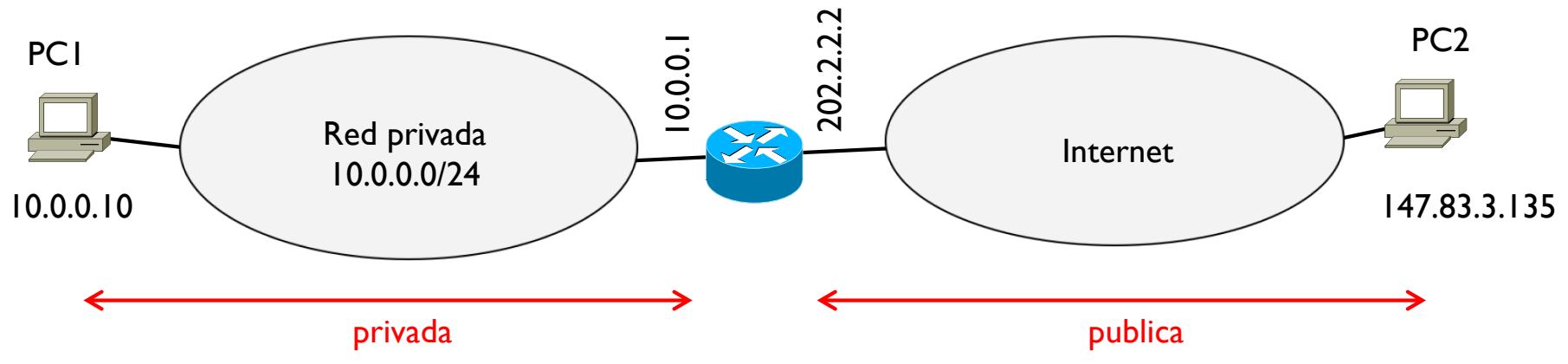
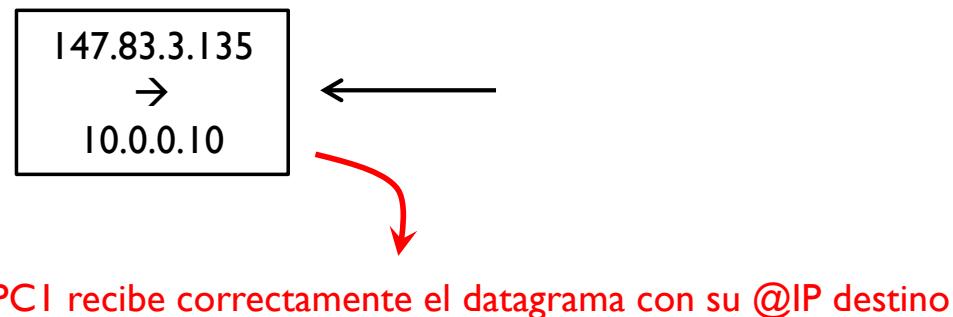


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10



PC1 recibe correctamente el datagrama con su @IP destino



Tema 2 – NAT estático

- ▶ Si hubiera más hosts de la red privada que necesitan un NAT estático, entonces habría que configurar una entrada en la tabla NAT para cada @IP privada

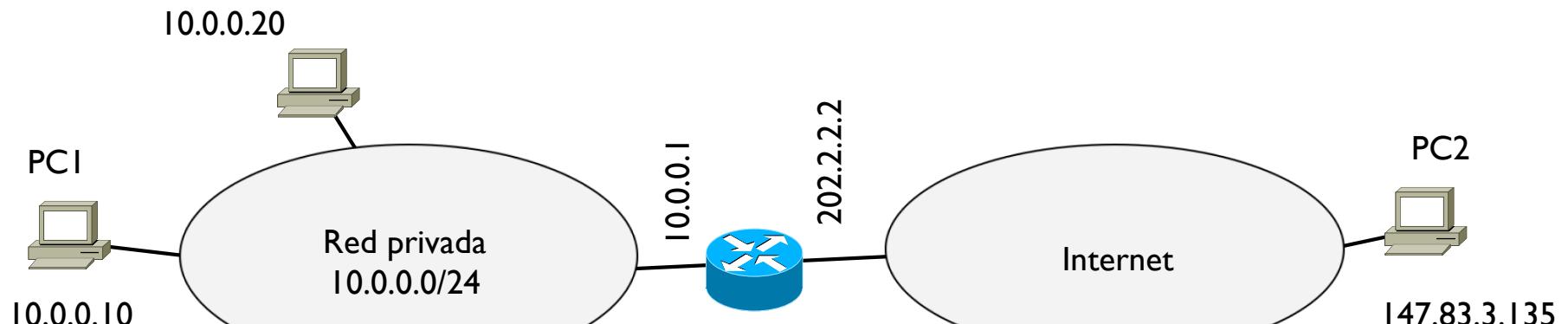
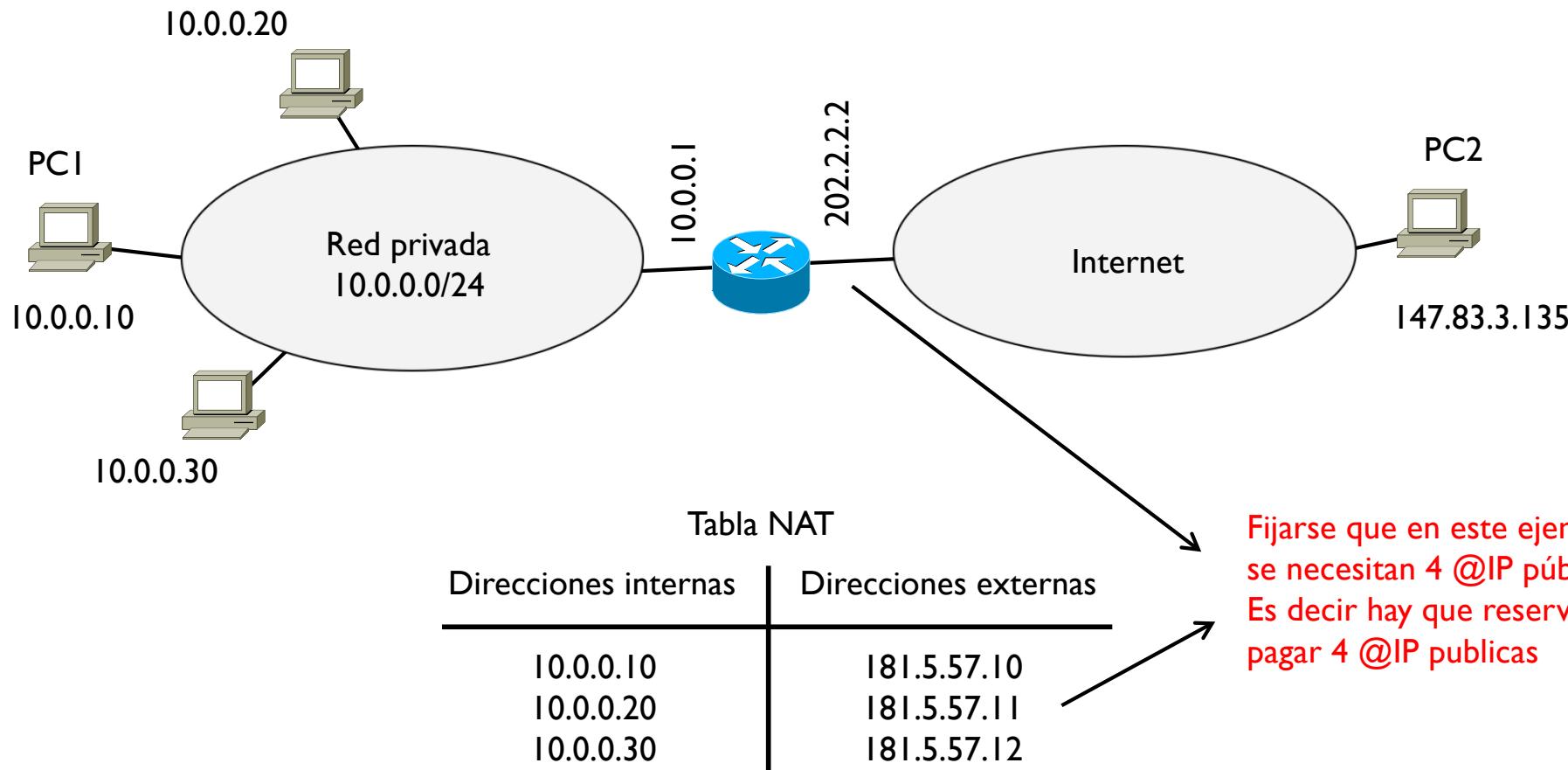


Tabla NAT

Direcciones internas	Direcciones externas
10.0.0.10	181.5.57.10
10.0.0.20	181.5.57.11
10.0.0.30	181.5.57.12

Tema 2 – NAT estático

- ▶ Si hubiera más hosts de la red privada que necesitan un NAT estático, entonces habría que configurar una entrada en la tabla NAT para cada @IP privada



Tema 2 – NAT dinámico

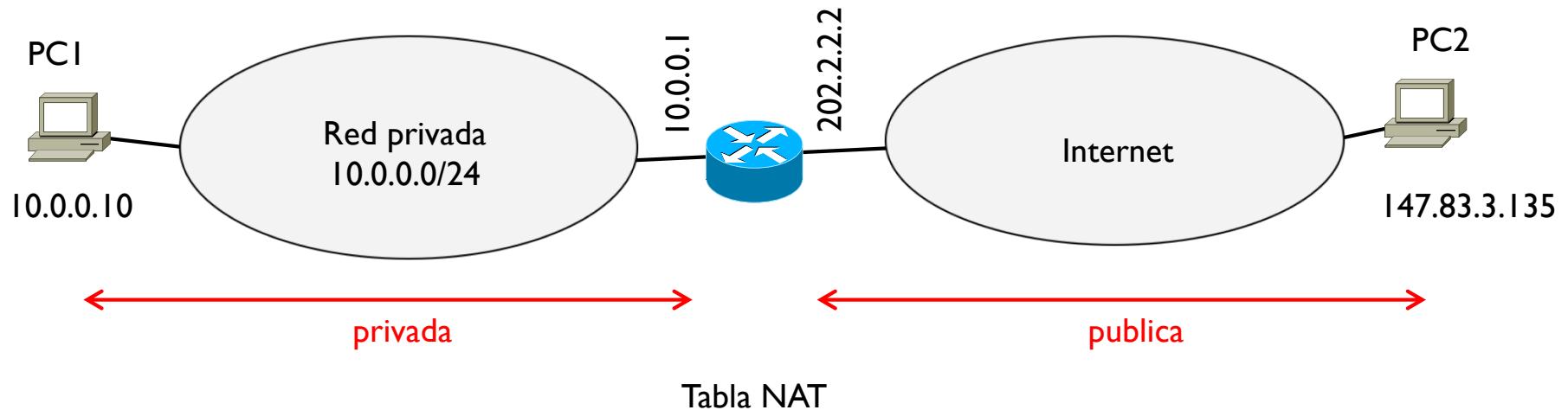


Tabla NAT

Direcciones internas	Direcciones externas	Duración
----------------------	----------------------	----------

Rango: 180.0.0.1-180.0.0.10

También en este caso el router mantiene una tabla NAT. Ahora pero esta tabla está inicialmente vacía y tiene una columna más que se llama duración. Y en el router se necesita configurar un rango de @IP publicas (previamente reservadas en Internet) disponibles para el NAT dinámico

Tema 2 – NAT dinámico

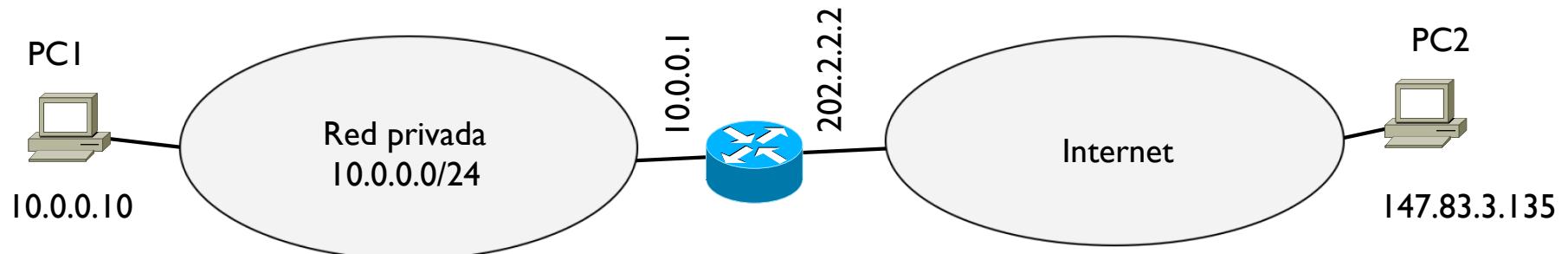


Tabla NAT		
Direcciones internas	Direcciones externas	Duración
		Rango: 180.0.0.1-180.0.0.10

10.0.0.10
→
147.83.3.135

La tabla NAT está inicialmente vacía

Como en el caso anterior, el host interno PCI quiere transmitir a PC2 de Internet
El datagrama tendrá estas @IP origen y destino



Tema 2 – NAT dinámico

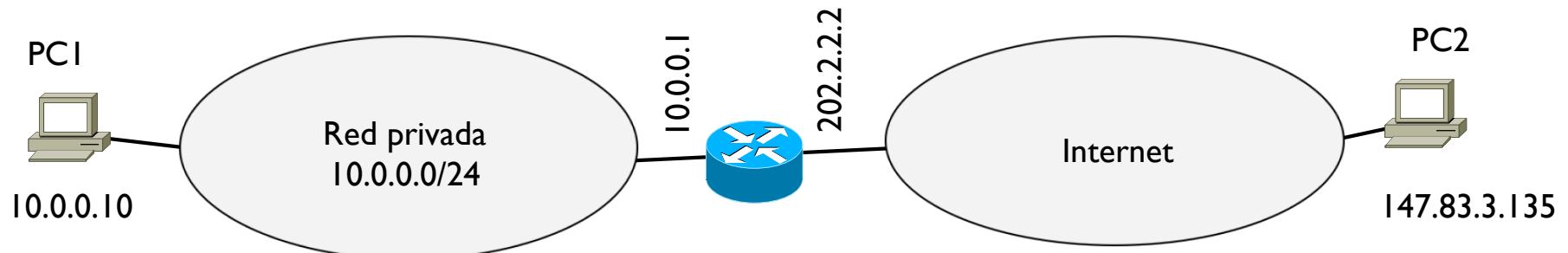
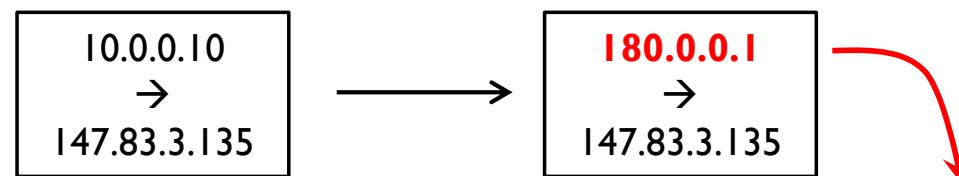


Tabla NAT			Rango: 180.0.0.1-180.0.0.10
Direcciones internas	Direcciones externas	Duración	
10.0.0.10	180.0.0.1	30 min	



Como en el caso anterior, este datagrama no se puede transmitir por Internet
El router substituye la @IP privada por la primera disponible del rango
Y además pone esta sustitución en la tabla NAT asignándole una duración



Tema 2 – NAT dinámico

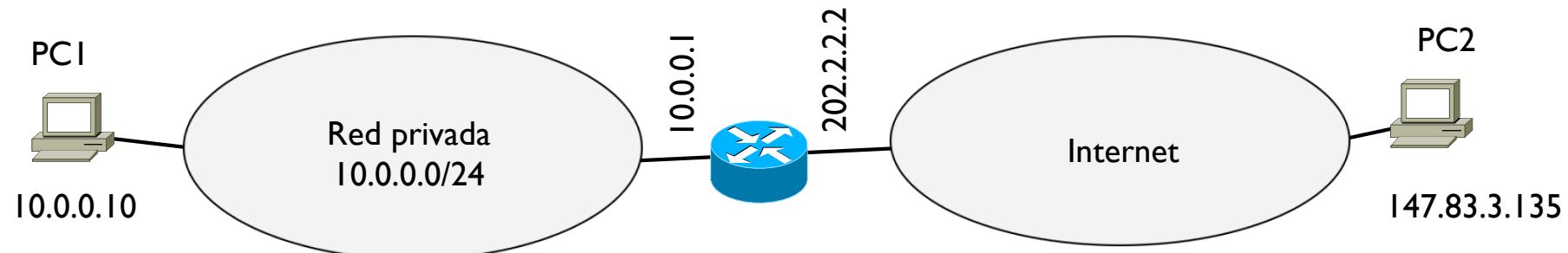
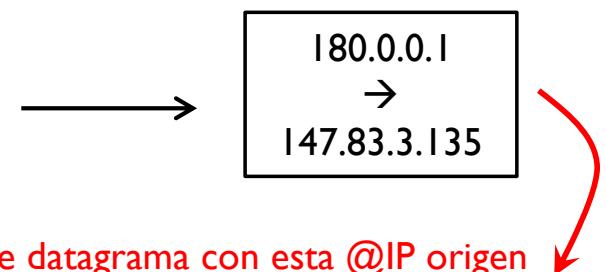


Tabla NAT			Rango: 180.0.0.1-180.0.0.10
Direcciones internas	Direcciones externas	Duración	
10.0.0.10	180.0.0.1	30 min	



El destino PC2 recibe este datagrama con esta @IP origen
PC2 no puede saber cual es la @IP real de PCI



Tema 2 – NAT dinámico

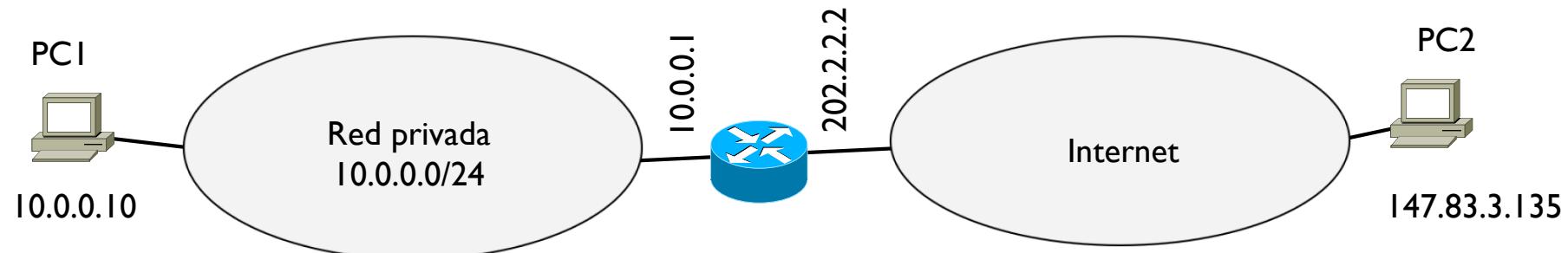
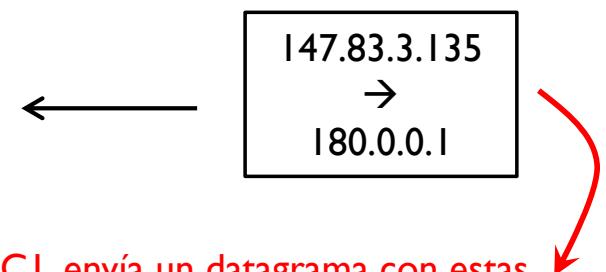


Tabla NAT			Rango: 180.0.0.1-180.0.0.10
Direcciones internas	Direcciones externas	Duración	
10.0.0.10	180.0.0.1	30 min	



Si PC2 quiere contestar a PC1, envía un datagrama con estas
@IP origen y destino



Tema 2 – NAT dinámico

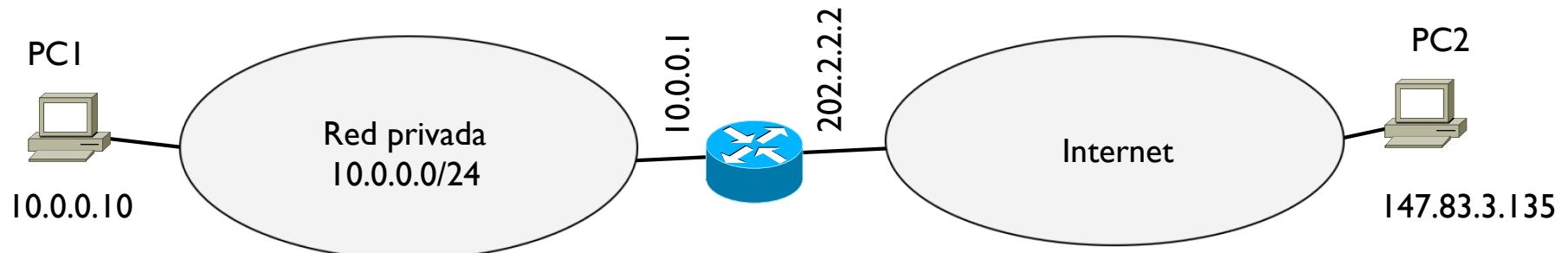
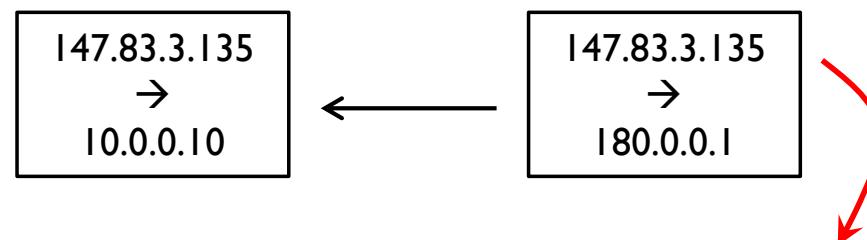


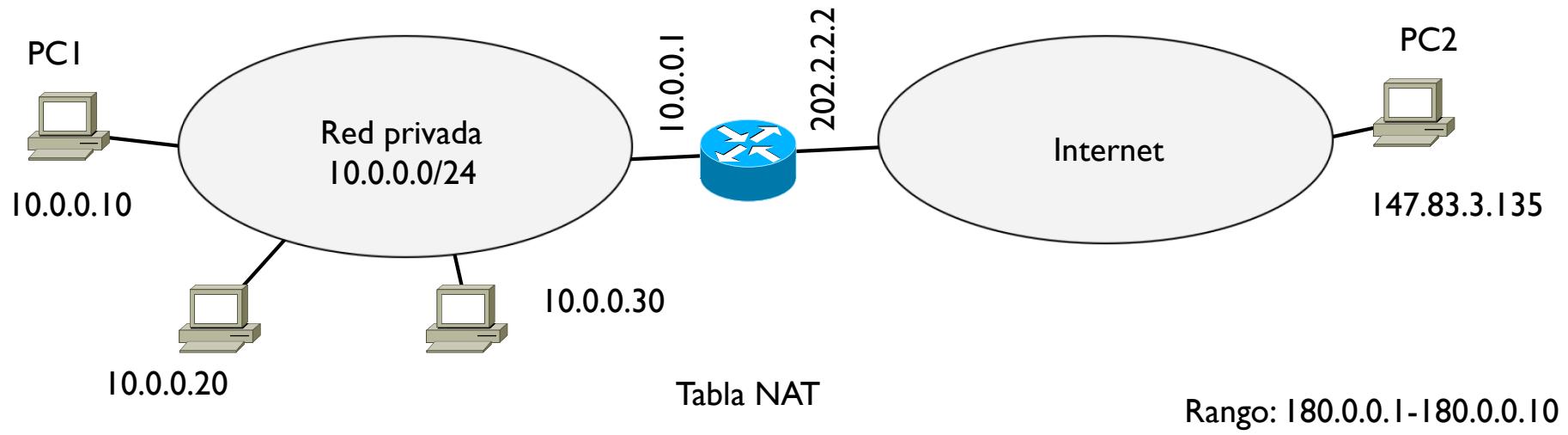
Tabla NAT			Rango: 180.0.0.1-180.0.0.10
Direcciones internas	Direcciones externas	Duración	
10.0.0.10	180.0.0.1	30 min	



Al recibir el datagrama, el router consulta la tabla NAT y hace la traducción inversa



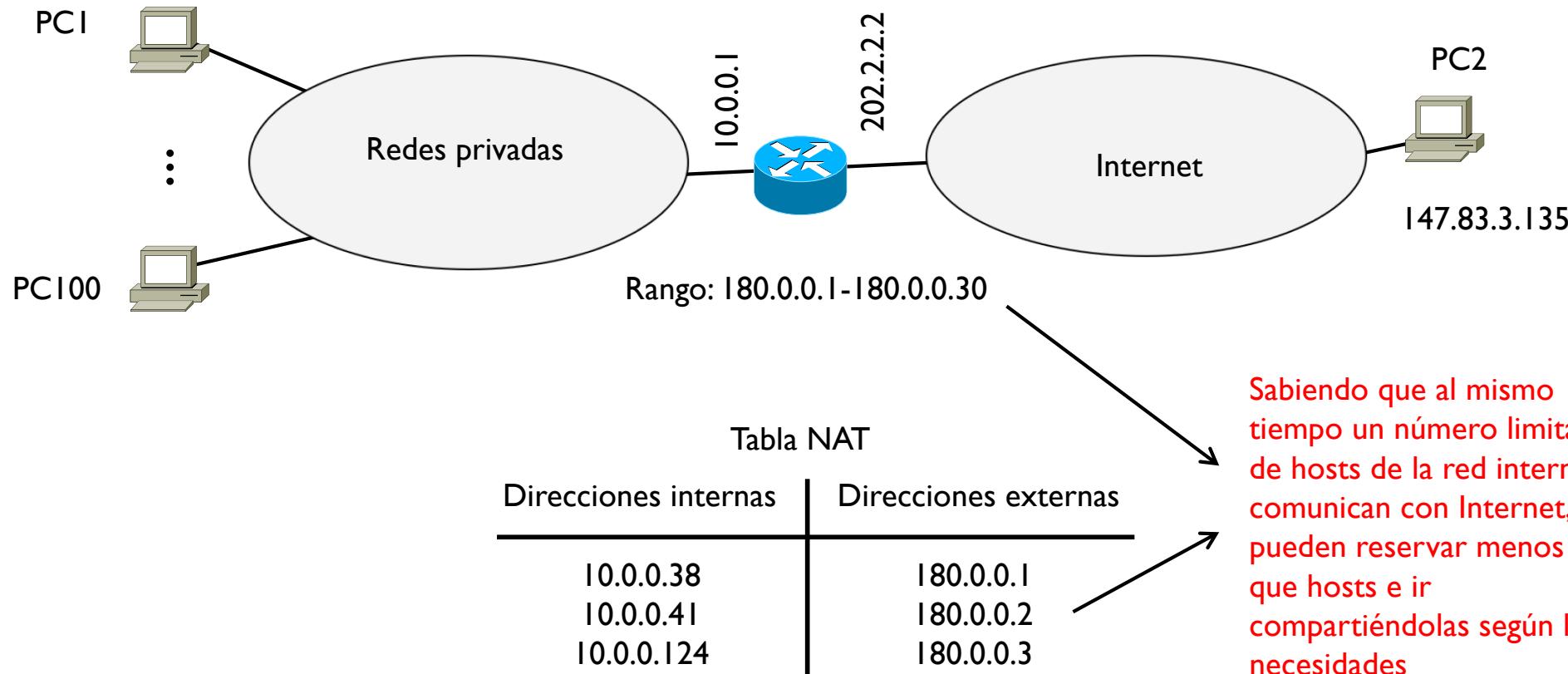
Tema 2 – NAT dinámico



Si hay otros PC de la red privada interna, estos no tienen entradas en la tabla NAT hasta que no envíen el primer datagrama hacia Internet
Si transmiten a Internet, el router asigna la primera @IP disponible del rango

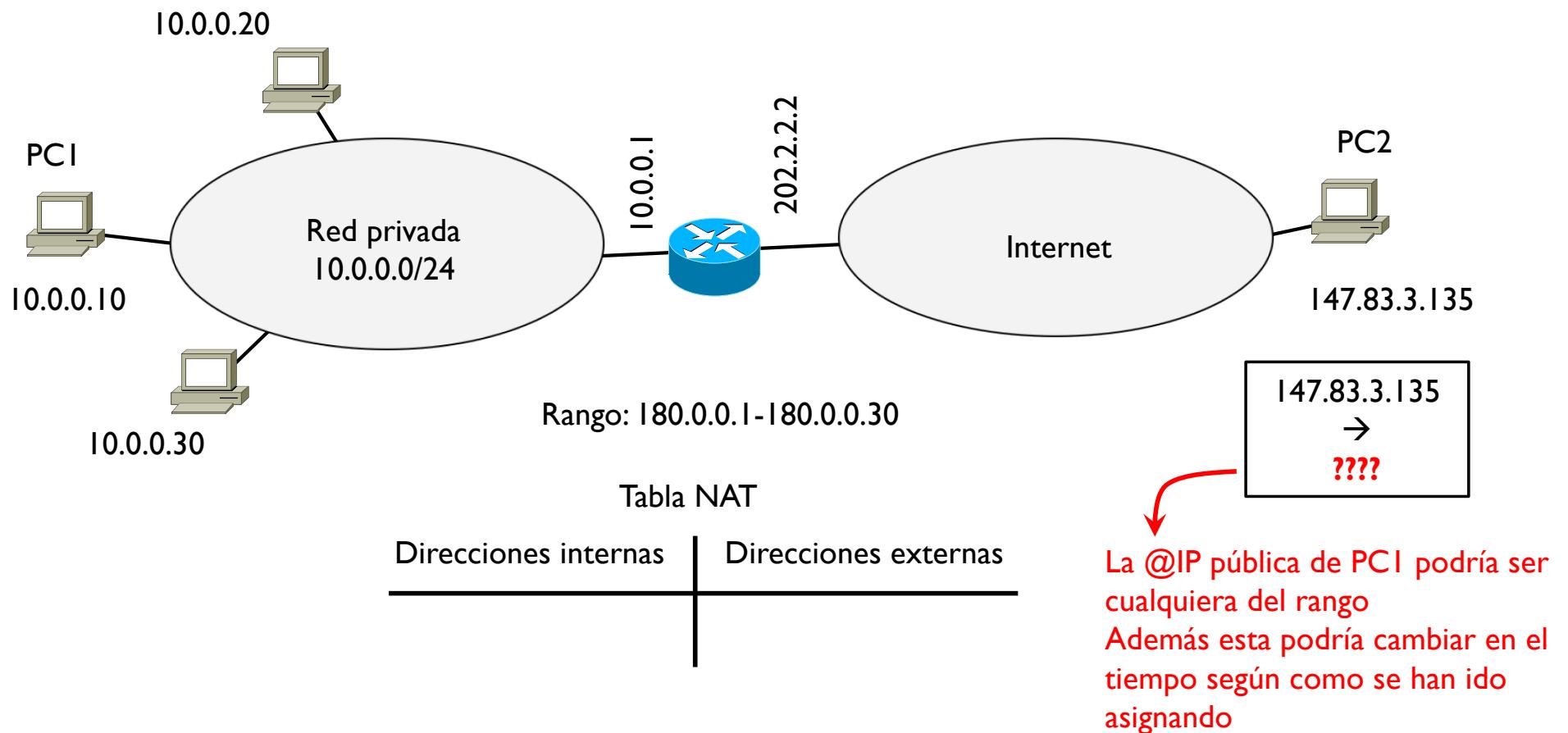
Tema 2 – NAT dinámico

- ▶ En este caso se podría reservar un número inferior de @IP públicas del número de host de la red privada



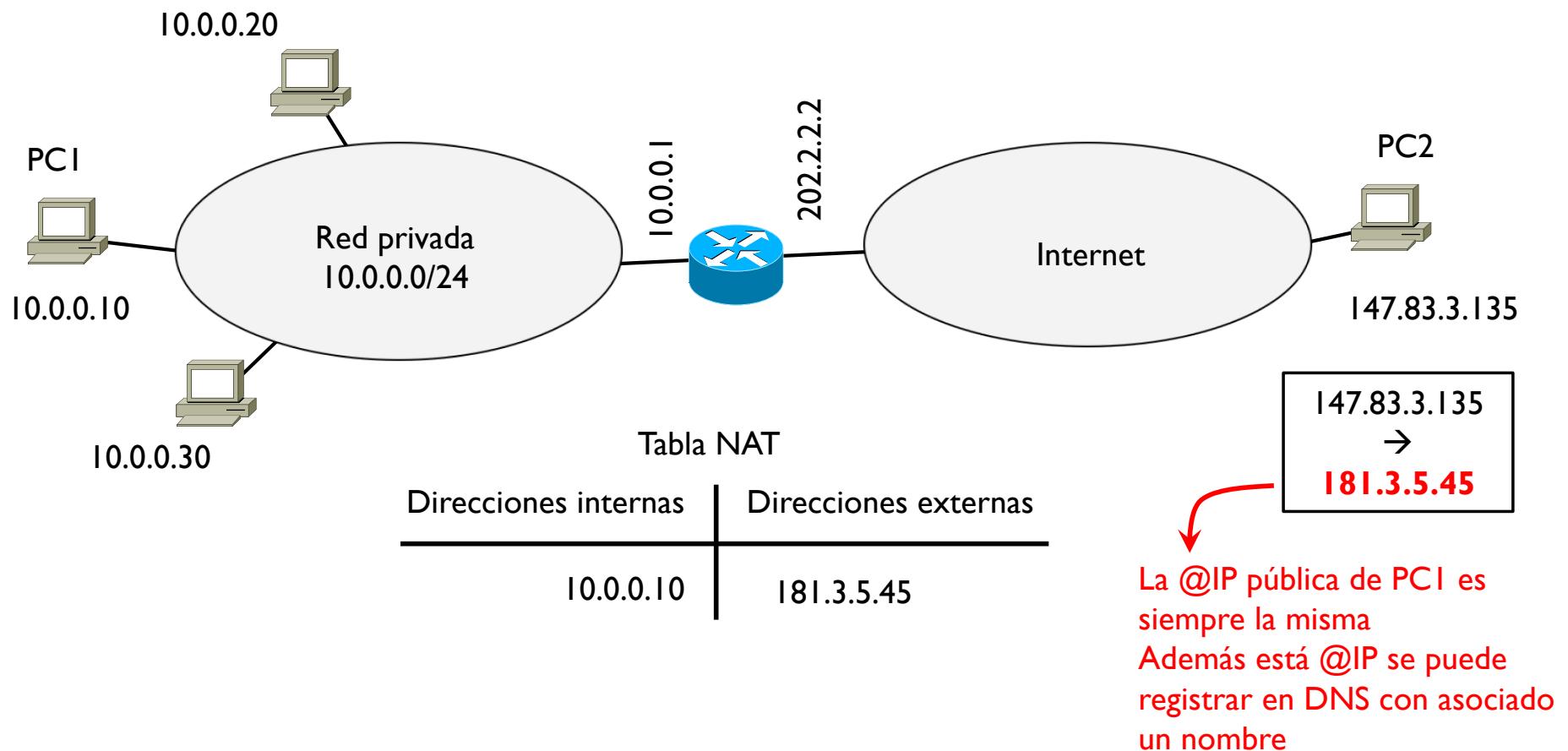
Tema 2 –NAT estático vs. dinámico

- ▶ En el caso de NAT dinámico, un host de Internet no puede empezar una comunicación con un host interno, ya que el externo no sabe cual es su @IP pública



Tema 2 –NAT estático vs. dinámico

- ▶ En el caso de NAT estático, un host de Internet puede empezar una comunicación con un host interno ya que este tiene asignada una @IP pública fija



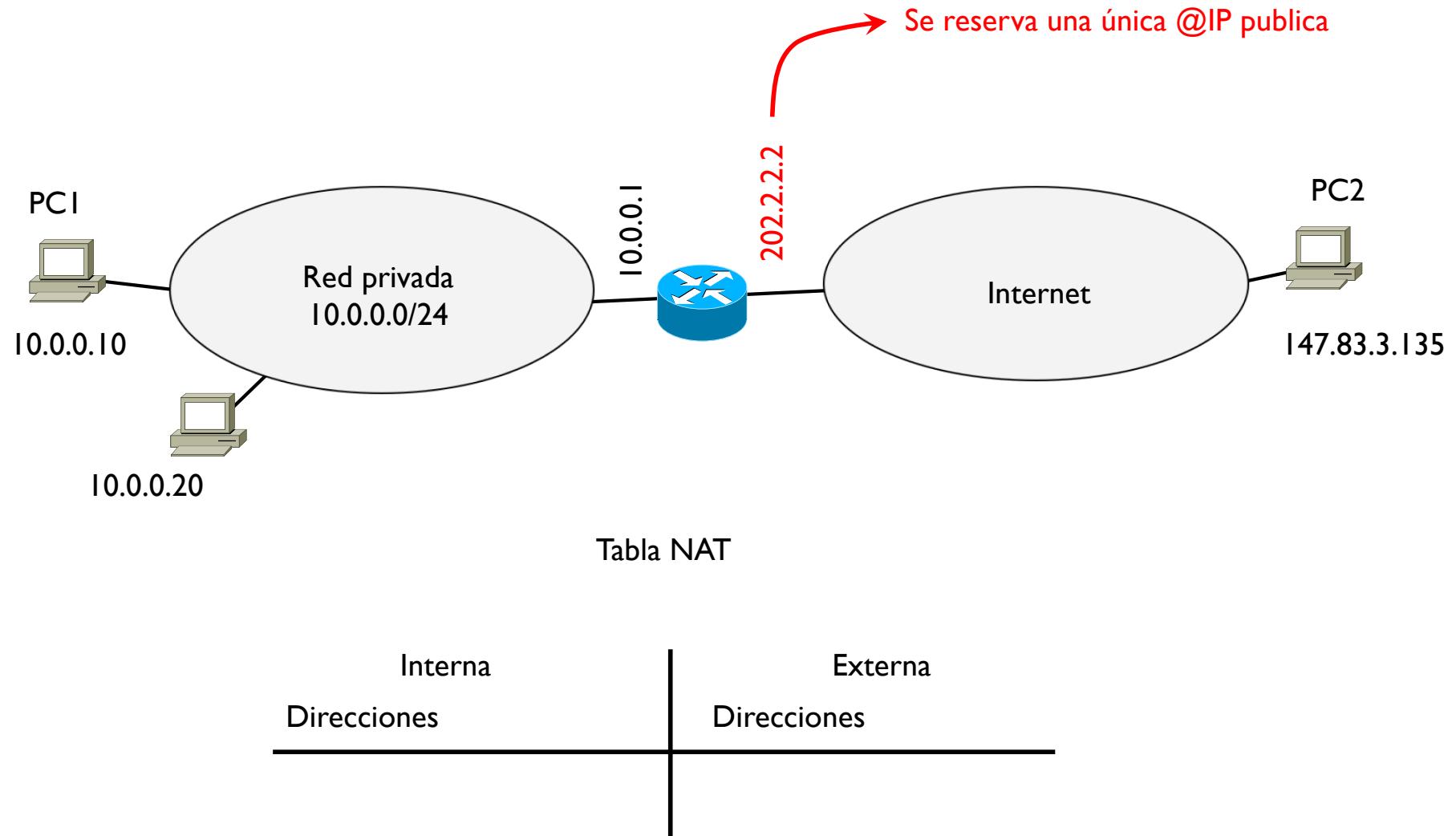
Tema 2 – NAT estático vs. dinámico

- ▶ Por esta razón, el NAT estático se usa generalmente para servidores que están en la red interna y deben ser alcanzables desde Internet con una @IP fija y conocida
- ▶ El NAT dinámico se usa generalmente para clientes, donde son estos que empiezan una comunicación con otro host (típicamente un servidor)
 - ▶ Por lo tanto el cliente es el primero en pasar por el router que crea la traducción correspondiente
 - ▶ El servidor contesta a la @IP que el router ha asignado al cliente traduciendo por lo tanto también la comunicación en sentido contrario



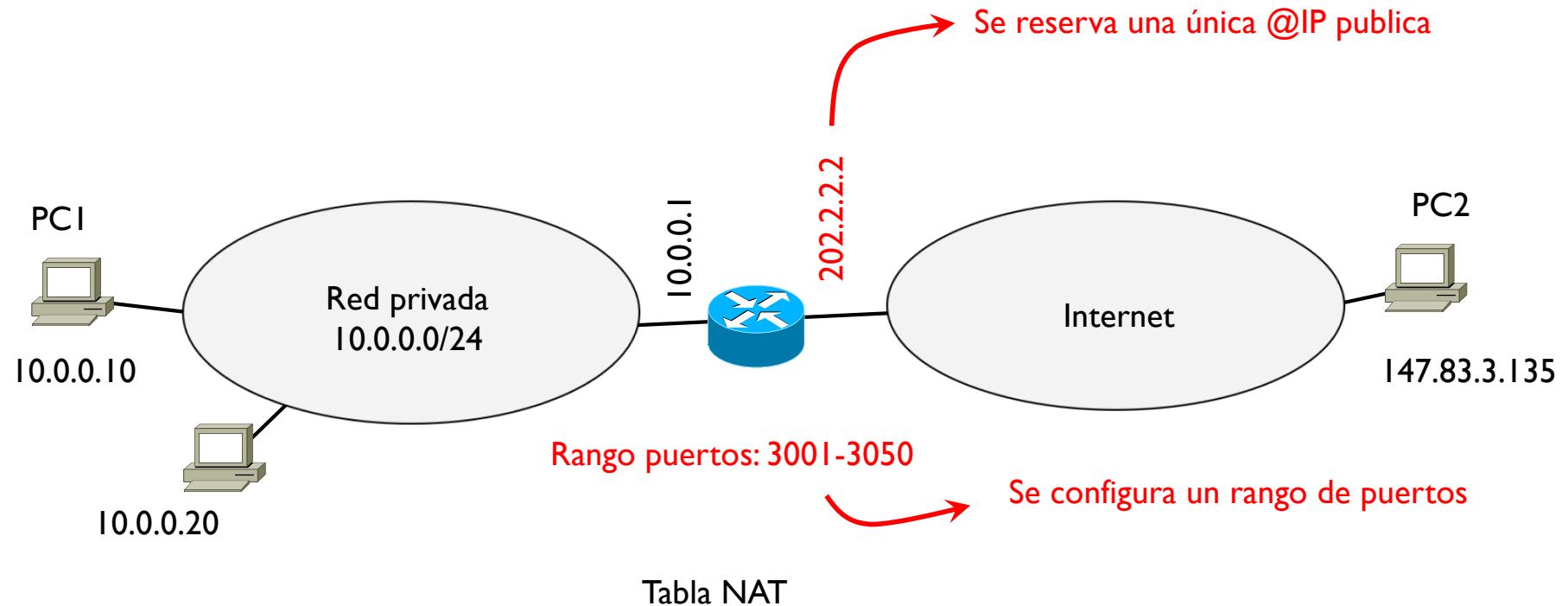
Tema 2 – PAT

▶ Port Address Translation



Tema 2 – PAT

▶ Port Address Translation

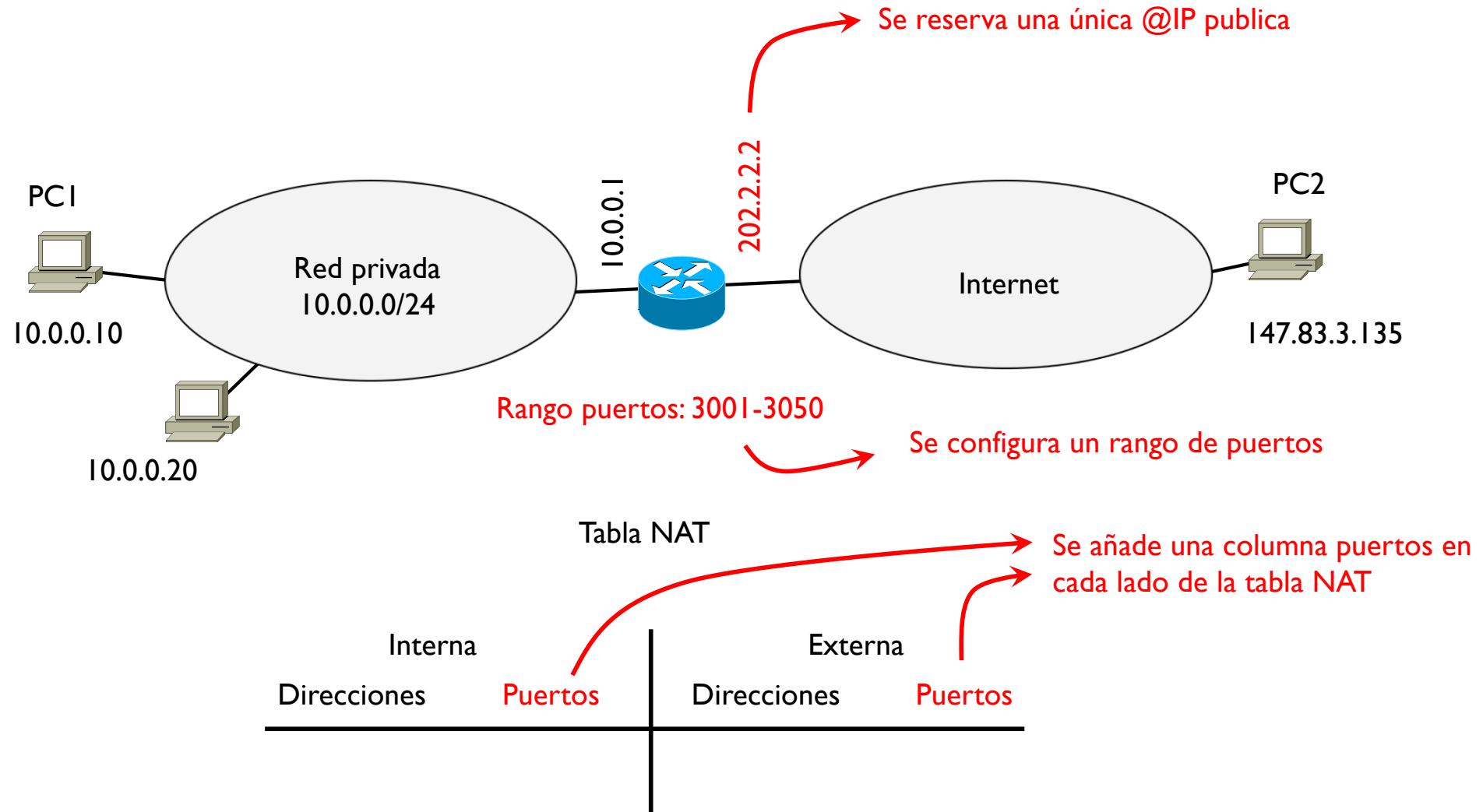


Interna Direcciones	Externa Direcciones

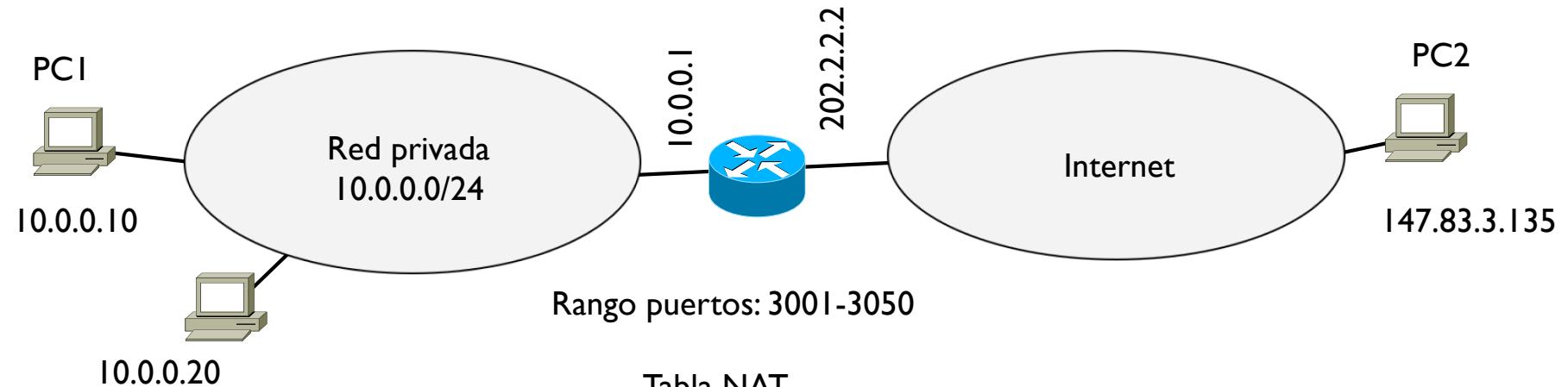


Tema 2 – PAT

▶ Port Address Translation



Tema 2 – PAT



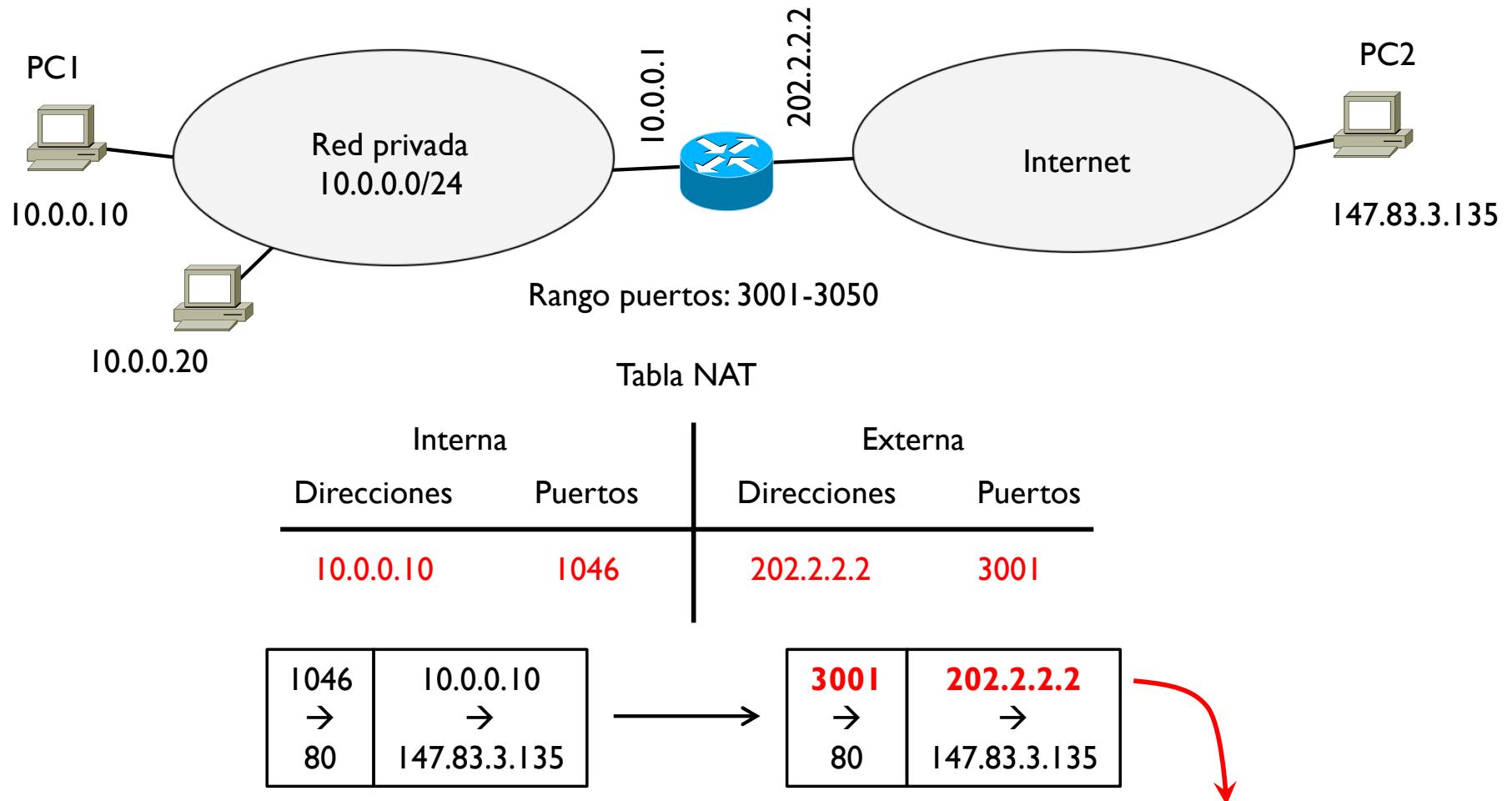
TCP	IP
1046 → 80	10.0.0.10 → 147.83.3.135

La tabla NAT está inicialmente vacía

El host interno PCI quiere transmitir a PC2 de Internet
En este caso interesan las @IP y también los puertos

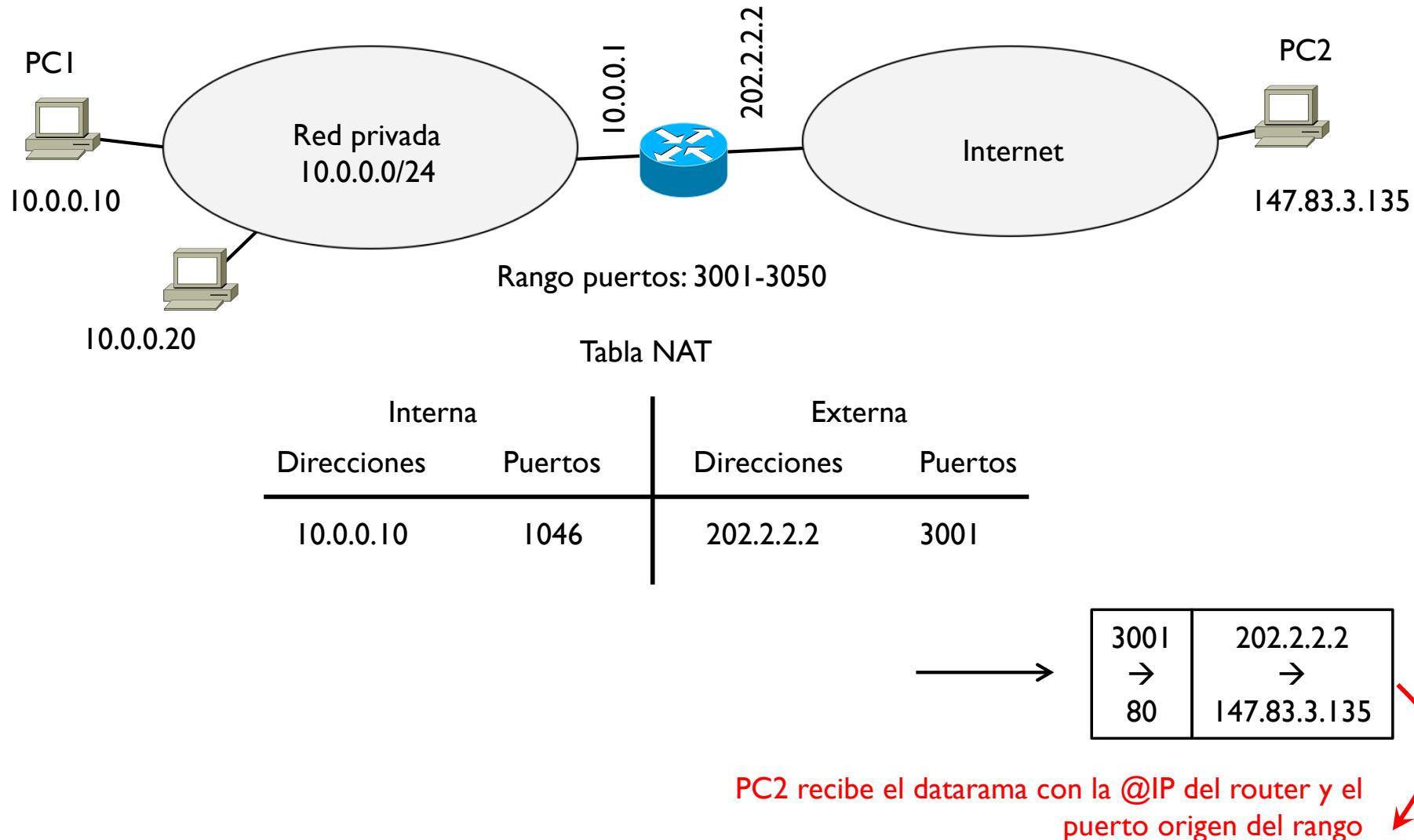


Tema 2 – PAT

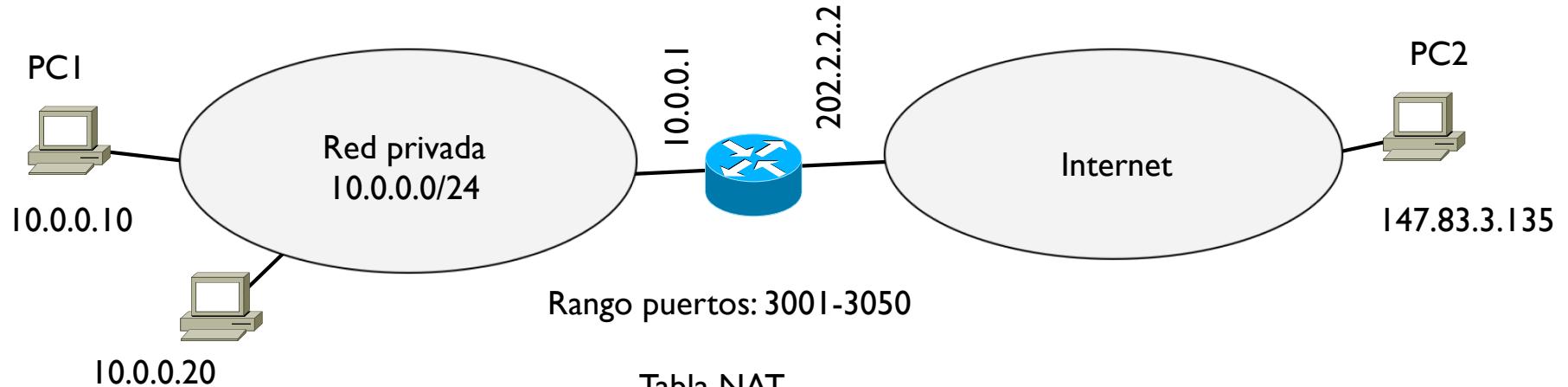


El router cambia la @IP privada origen por su propia @IP publica y cambia el puerto origen por el primer puerto disponible del rango

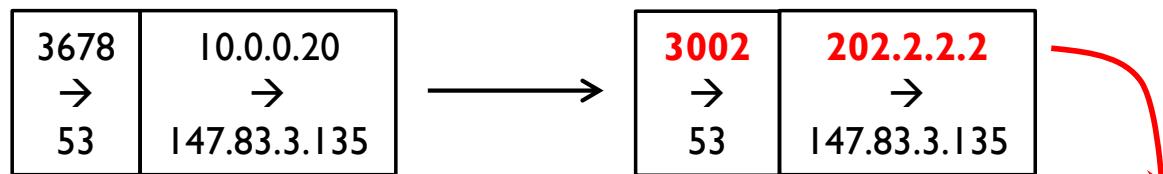
Tema 2 – PAT



Tema 2 – PAT



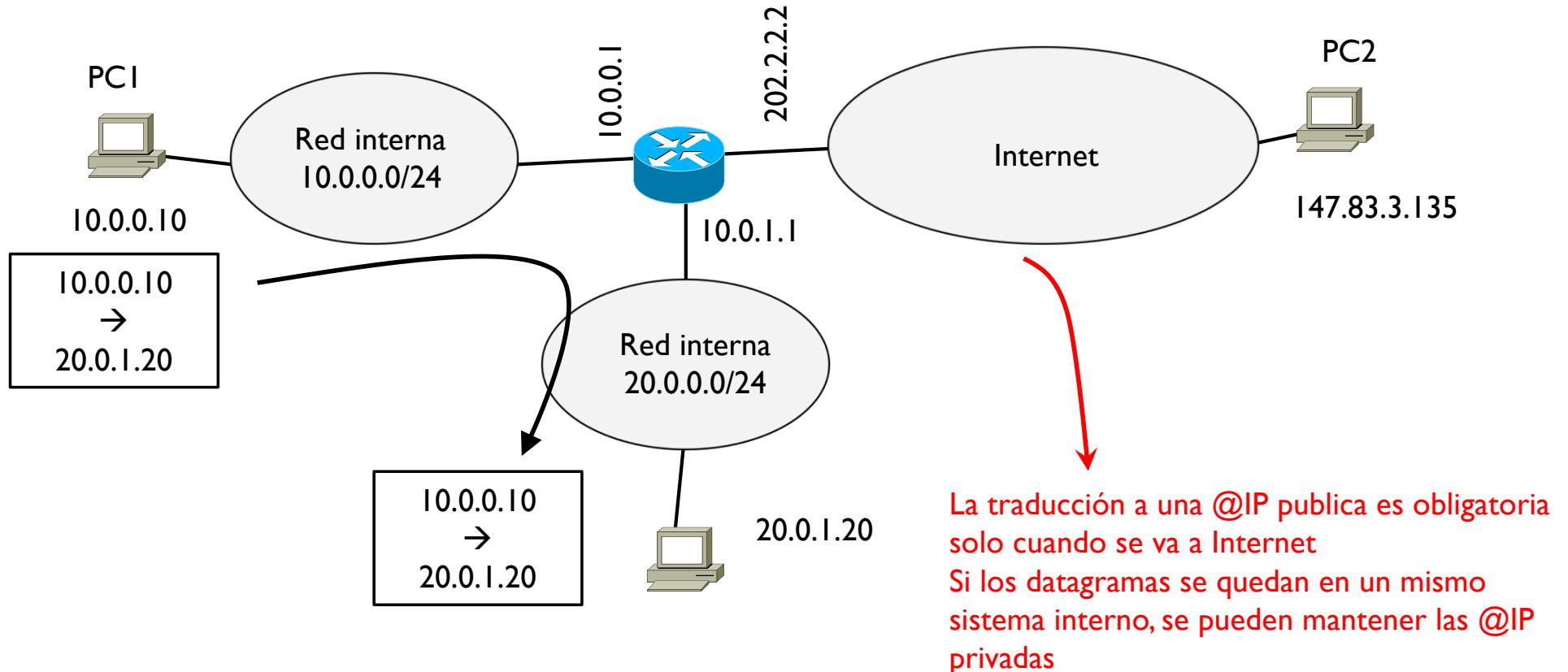
Interna		Externa	
Direcciones	Puertos	Direcciones	Puertos
10.0.0.10	1046	202.2.2.2	3001
10.0.0.20	3678	202.2.2.2	3002



Si otro PC transmite hacia Internet, el router vuelve a usar su @IP como origen y el siguiente puerto disponible del rango

Tema 2 – NAT detalles

- ▶ Una comunicación interna no necesita traducciones



Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ Alguna noción de seguridad



Tema 2 – Encaminamiento dinámico

Como se construyen las tablas de encaminamiento

▶ Estática

- ▶ El administrador decide las entradas y por lo tanto las rutas
- ▶ Enfoque viable para redes pequeñas
- ▶ Viable para los hosts configurando una única ruta que es la ruta por defecto

▶ Dinámica

- ▶ Los routers se intercambian mensajes y deciden las rutas según algunas métricas
 - ▶ Por ejemplo una métrica puede ser el número de routers, la congestión, fiabilidad, velocidad de transmisión, etc.
- ▶ De acuerdo con estas métricas y su significado, los routers llenan sus tablas de encaminamiento autónomamente



Tema 2 – Encaminamiento dinámico

El encaminamiento dinámico necesita

- ▶ **Protocolo de encaminamiento**
 - ▶ Coordina y define el contenido de los intercambios de mensajes
- ▶ **Algoritmo de encaminamiento**
 - ▶ Según la información y las métricas recibidas, decide las entradas en la tabla de encaminamiento



Tema 2 – Routing Information Protocol (RIP)

- ▶ RFC 1058 (RIPv1) RFC 2453 (RIPv2)
- ▶ Protocolo de encaminamiento
 - ▶ Usa un enfoque llamado vector-distancia
 - ▶ Cada router envía un mensaje RIP a sus routers vecinos cada 30s
 - ▶ Un mensaje RIP contiene las redes conocidas por el router y la métrica para llegar a ellas → RIPv2 añade la mascara de cada red
 - ▶ La métrica es el número de redes que hay que cruzar para llegar al destino
 - ▶ Indica la “distancia” para llegar a una red
 - ▶ La métrica máxima es 15
 - ▶ Una métrica 16 significa infinito (una red es ahora inalcanzable)
 - ▶ Para reconocer que el protocolo es RIP se usan puertos origen y destino 520



Tema 2 – Routing Information Protocol (RIP)

- ▶ RFC 1058 (RIPv1) RFC 2453 (RIPv2)

- ▶ Algoritmo de encaminamiento
 - ▶ Al recibir un mensaje RIP, un router compara el contenido de este con su tabla de encaminamiento y la modifica si
 - ▶ Descubre una nueva red
 - ▶ Descubre una nueva ruta a una red conocida con una métrica menor (debe ser menor, no modifica si es igual)
 - ▶ La métrica de una red conocida ha cambiado



Tema 2 – Routing Information Protocol (RIP)

▶ Mensaje RIP

Red 1 Mascara Métrica	Red 2 Mascara Métrica	Red 3 Mascara Métrica	...	Cabecera UDP Puerto origen 520 Puerto destino 520	Cabecera IP @IP del router @IP broadcast
-----------------------------	-----------------------------	-----------------------------	-----	---	--

El contenido del mensaje es un vector donde cada elemento contiene 3 datos
→ Por eso vector-distancia

En broadcast para que el mensaje llegue a todos los dispositivos de la red

▶ Tabla de encaminamiento

Adquisición	destino	mascara	gateway	interfaz	métrica
R					Se añade esta columna que indica la métrica para llegar a un destino

Indica que se ha aprendido por RIP

Tema 2 – Routing Information Protocol (RIP)

▶ Funcionamiento

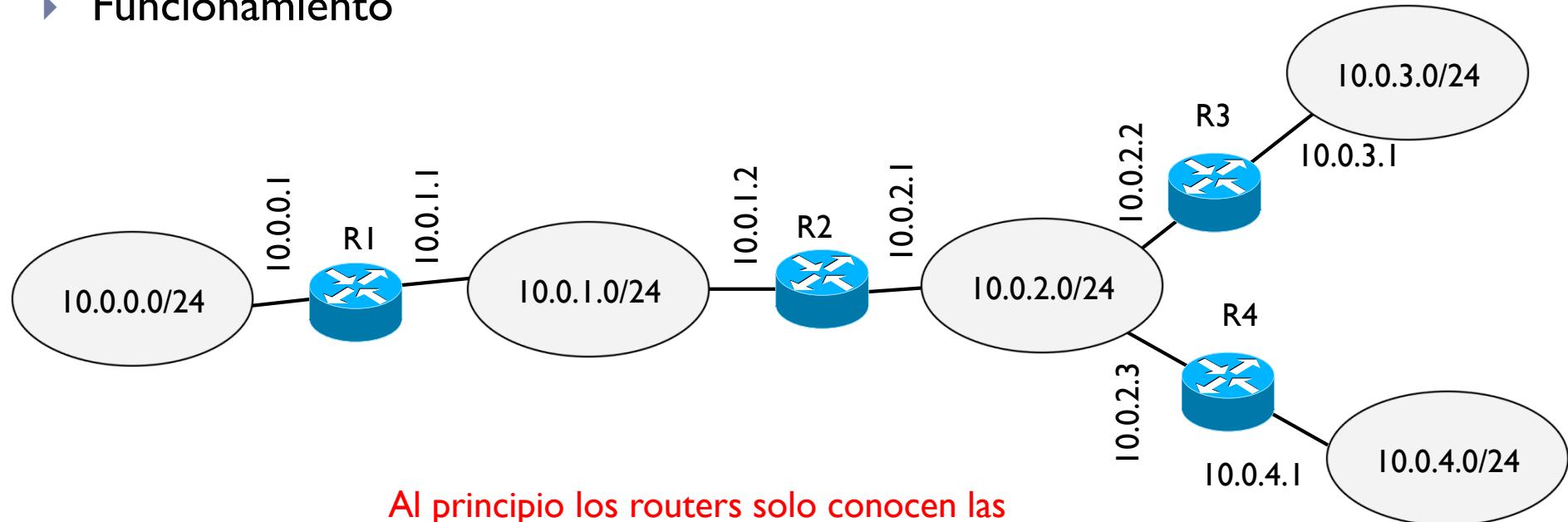


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1



Tema 2 – Routing Information Protocol (RIP)

- ▶ Al activar RIPv2, los routers empiezan a enviarse mensajes
- ▶ Suponemos empieza el router R1

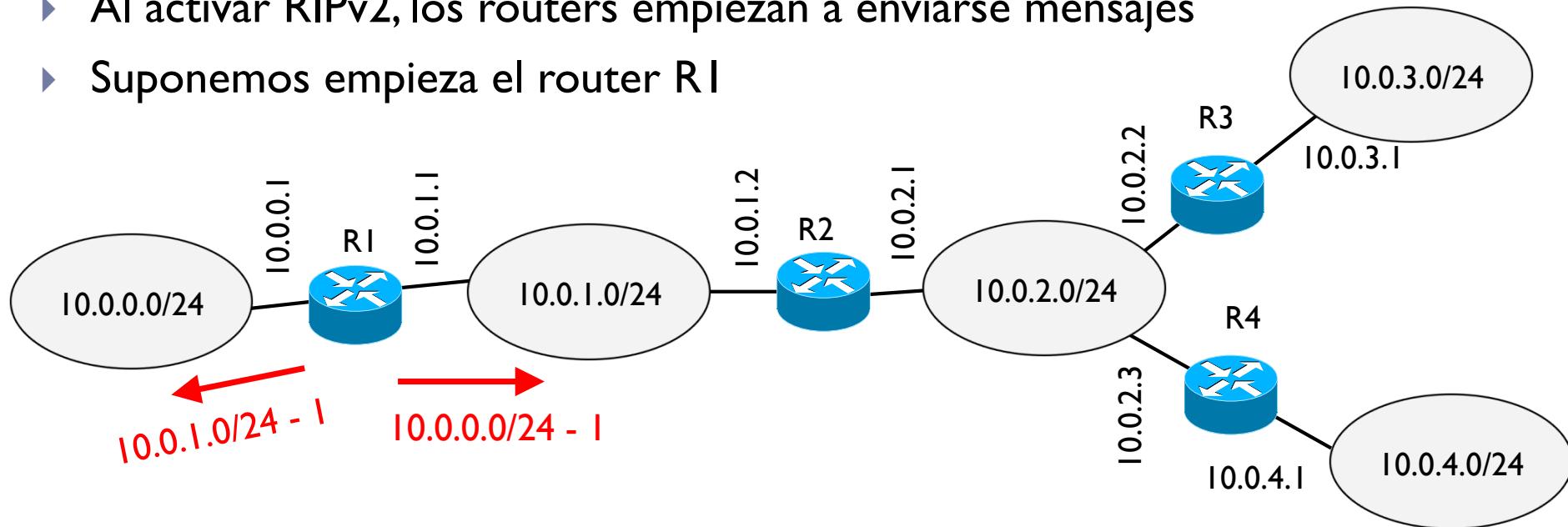


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1

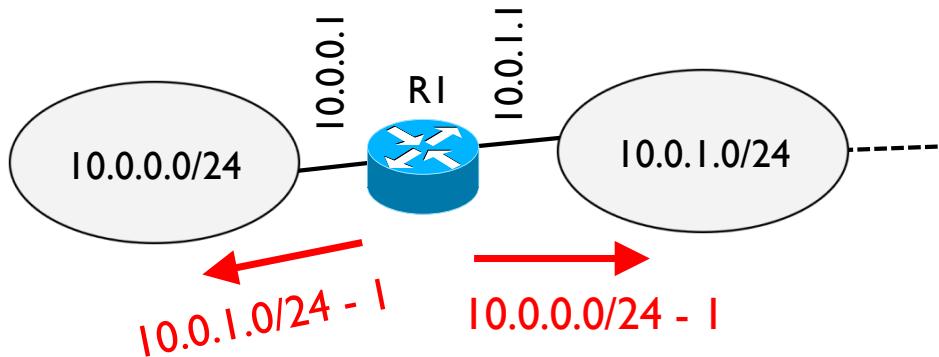
Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1



Tema 2 – Routing Information Protocol (RIP)

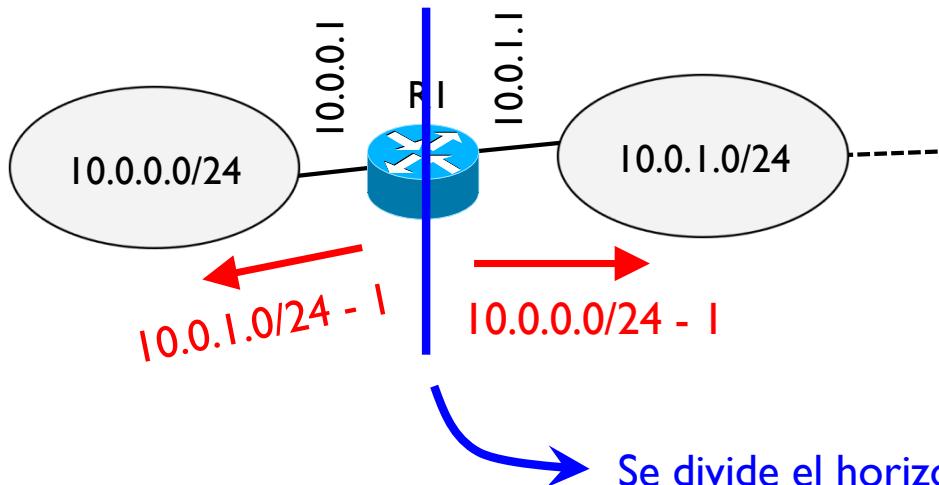
- ▶ Al activar RIPv2, los routers empiezan a enviarse mensajes
- ▶ Suponemos empieza el router RI



- ▶ Un router no envía todo lo que sabe
 - ▶ Transmite por una interfaz solo aquellas entradas de la tabla que el router no ha aprendido por la red de esta interfaz
- Principio llamado SPLIT-HORIZON

Tema 2 – Routing Information Protocol (RIP)

- ▶ Al activar RIPv2, los routers empiezan a enviarse mensajes
- ▶ Suponemos empieza el router RI



- ▶ Un router no envía todo lo que sabe
 - ▶ Transmite por una interfaz solo aquellas entradas de la tabla que el router no ha aprendido por la red de esta interfaz
- Principio llamado SPLIT-HORIZON

Se divide el horizonte en dos parte:

- En una parte hay la red por donde se envía el mensaje
- En la otra parte todo el resto

Se envía por una parte todo lo que se ha aprendido de la otra parte

En este ejemplo de las dos entradas que hay en la tabla de RI:

- Se envía a la derecha, las redes que hay a la izquierda
- Se envía a la izquierda, las redes que hay a la derecha



Tema 2 – Routing Information Protocol (RIP)

- ▶ Al activar RIPv2, los routers empiezan a enviarse mensajes
- ▶ Suponemos empieza el router R1

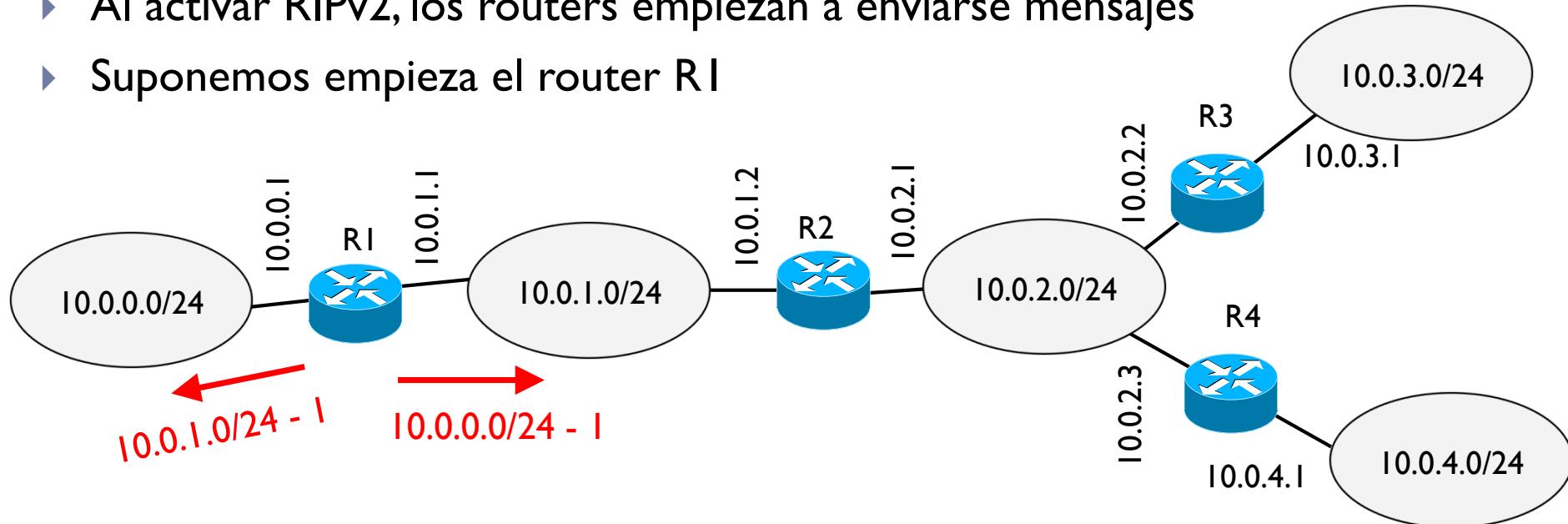


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1

Conocimiento nuevo,
Se añade

Tema 2 – Routing Information Protocol (RIP)

- ▶ Suponemos ahora envía el router R2

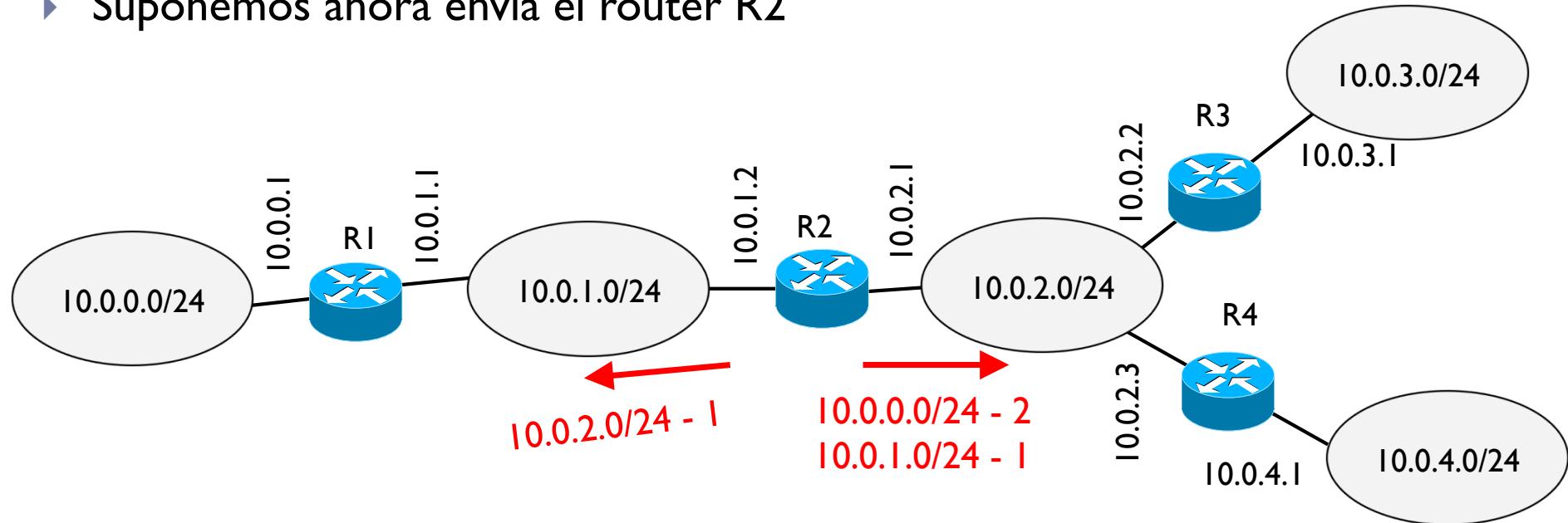


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1

Tema 2 – Routing Information Protocol (RIP)

- ▶ Suponemos ahora envía el router R2

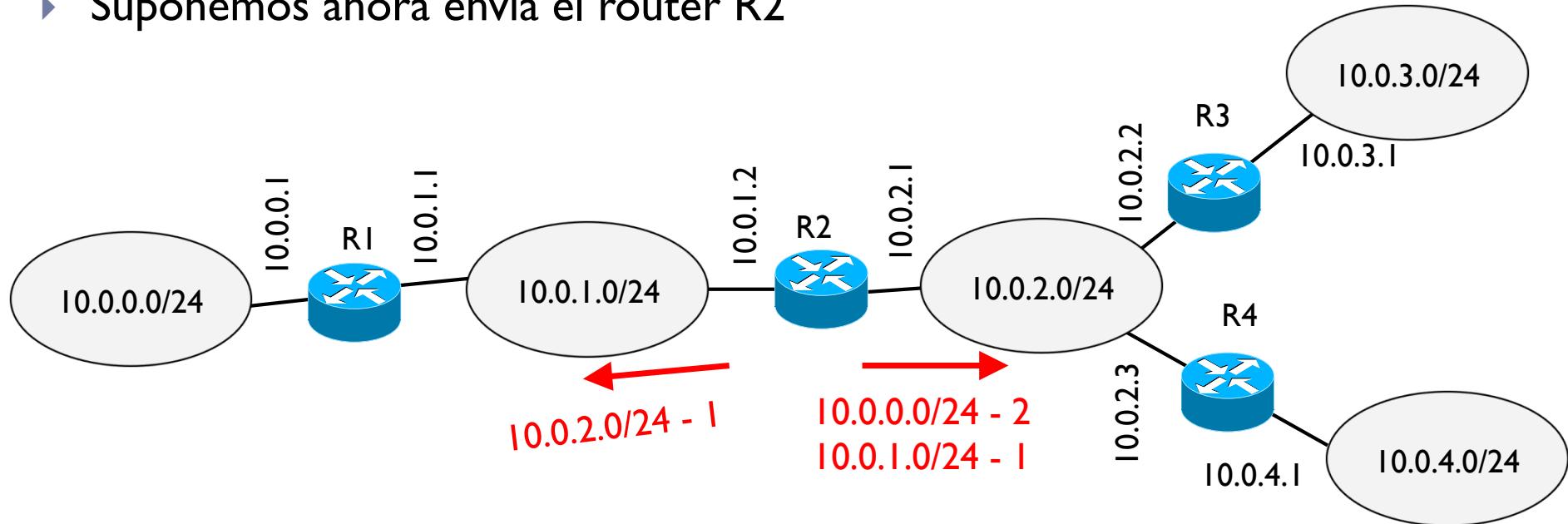


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	10.0.1.2	2

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1

Conocimientos nuevos,
Se añaden

Tema 2 – Routing Information Protocol (RIP)

- ▶ Suponemos ahora envía el router R3

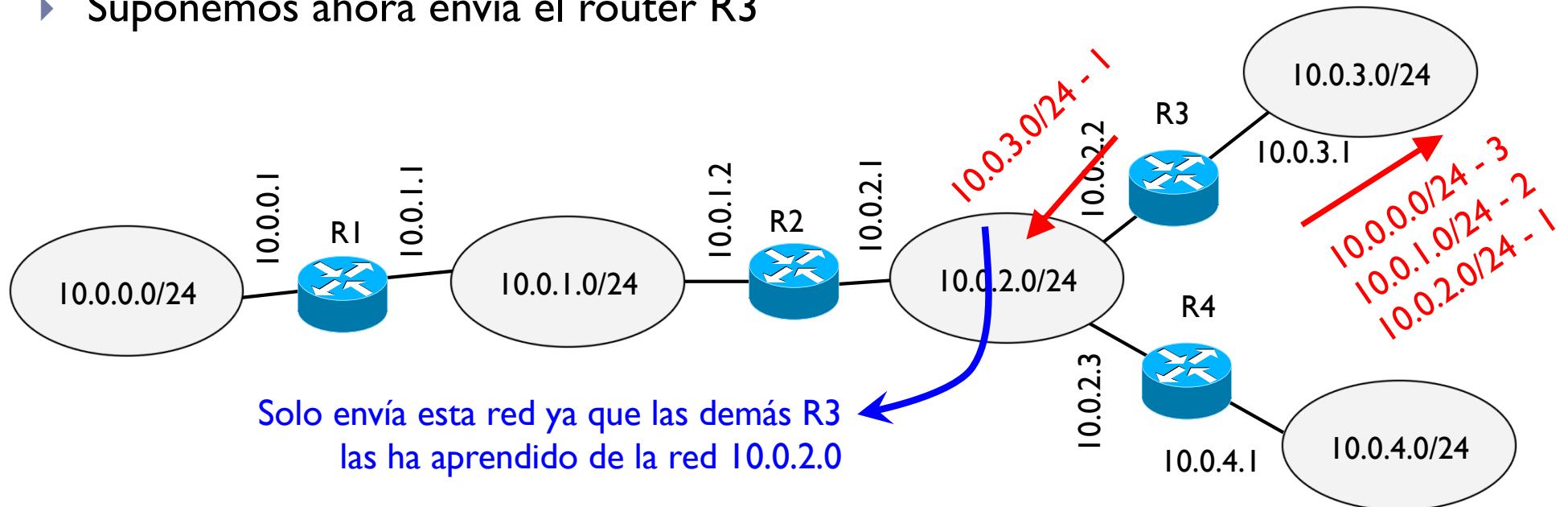


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	10.0.1.2	2

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2

Tema 2 – Routing Information Protocol (RIP)

- ▶ Suponemos ahora envía el router R3

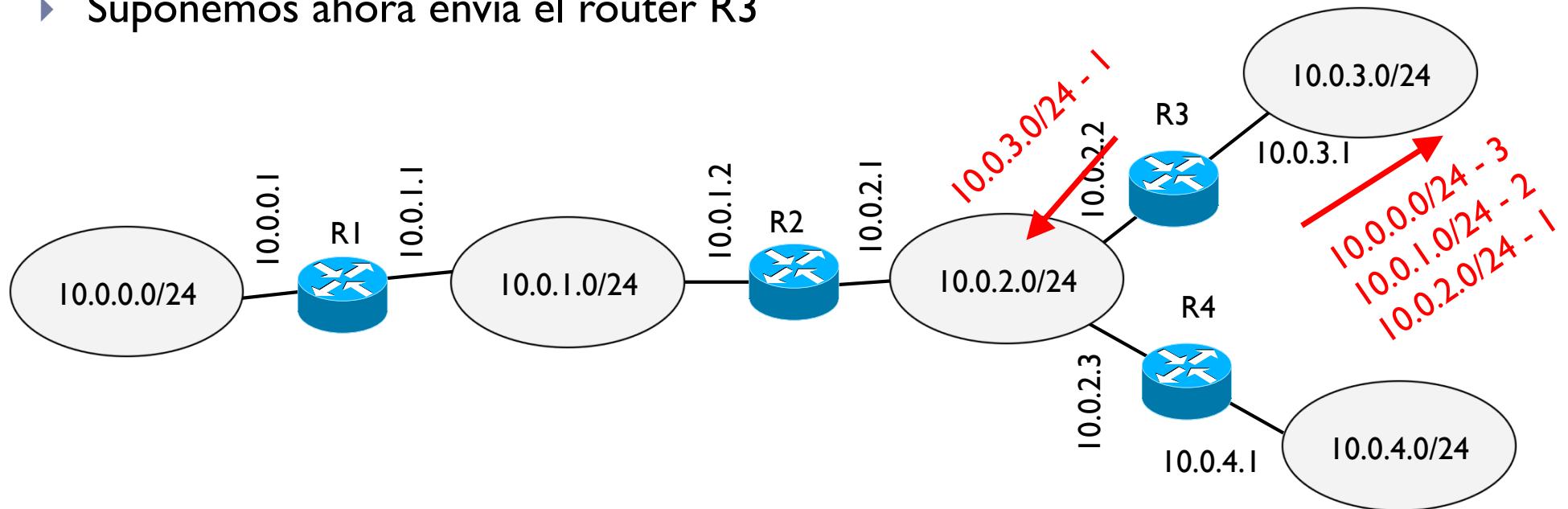


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	10.0.1.2	2

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2
10.0.3.0/24	10.0.2.2	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2

Tema 2 – Routing Information Protocol (RIP)

- Y por último el router R4

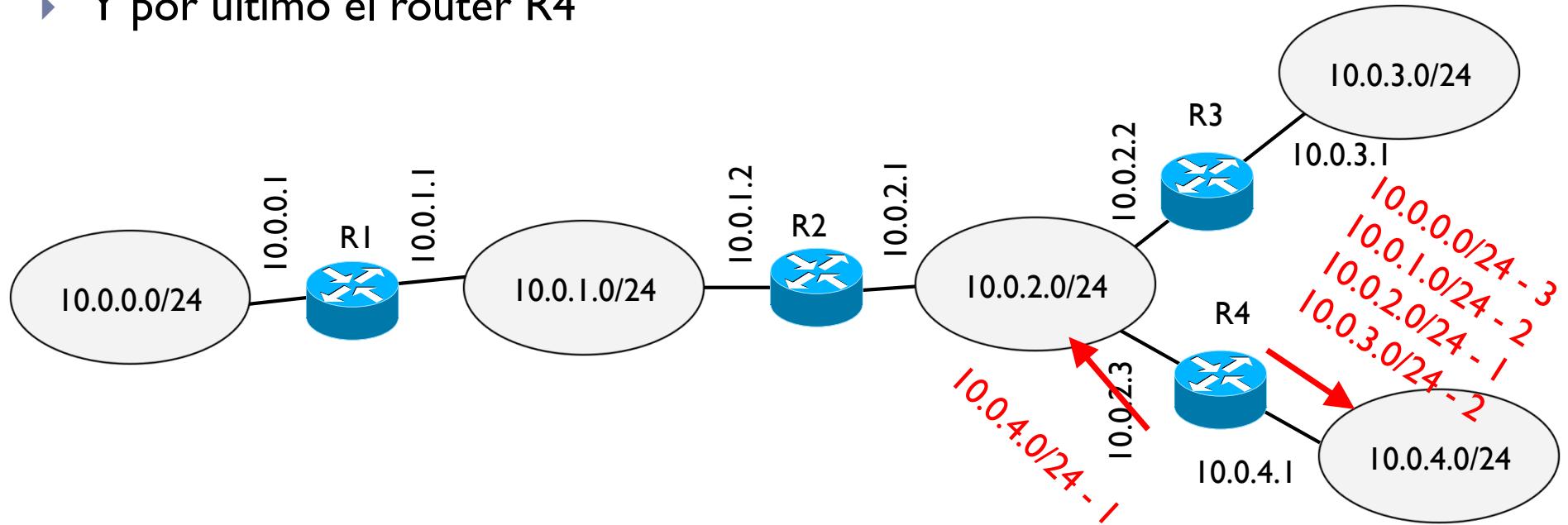


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	10.0.1.2	2

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2
10.0.3.0/24	10.0.2.2	2
10.0.4.0/24	10.0.2.3	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2
10.0.3.0/24	10.0.2.3	2



Tema 2 – Routing Information Protocol (RIP)

- Al acabar este primer ciclo de intercambio, los routers R2 y R3 tienen un conocimiento completo del sistema

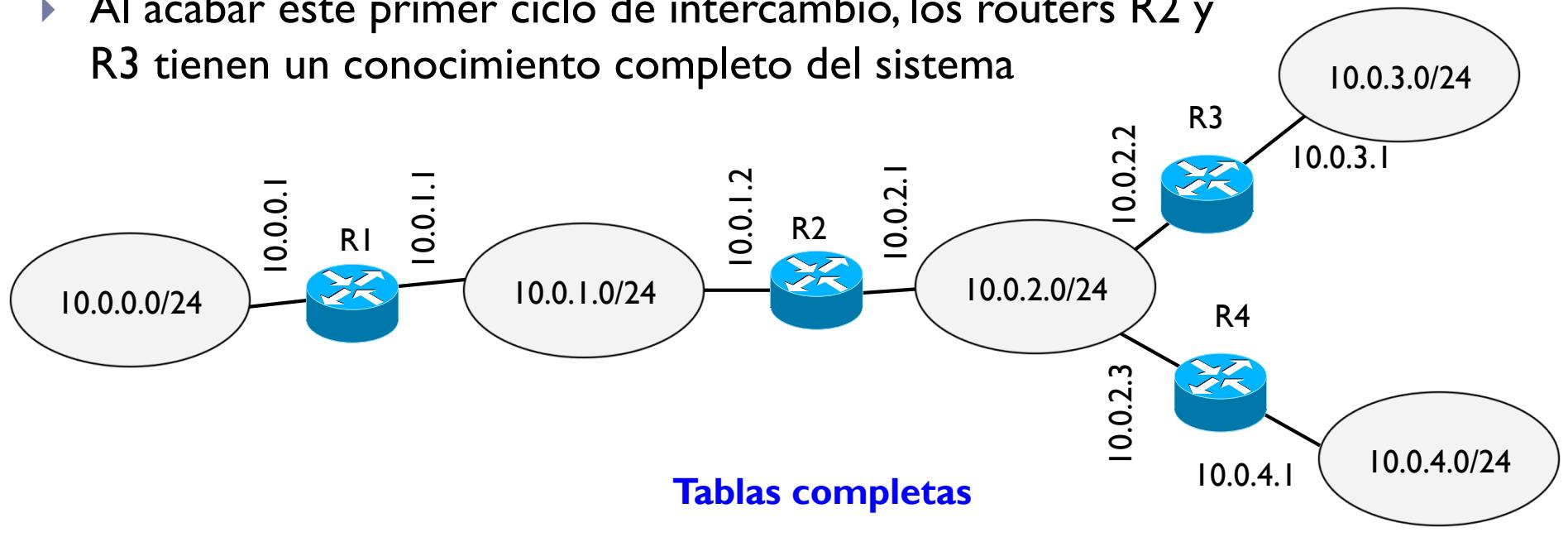


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	10.0.1.2	2

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2
10.0.3.0/24	10.0.2.2	2
10.0.4.0/24	10.0.2.3	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2
10.0.3.0/24	10.0.2.3	2

Tema 2 – Routing Information Protocol (RIP)

- ▶ Pasados 30s del primer envío, R1 vuelve a enviar un RIP

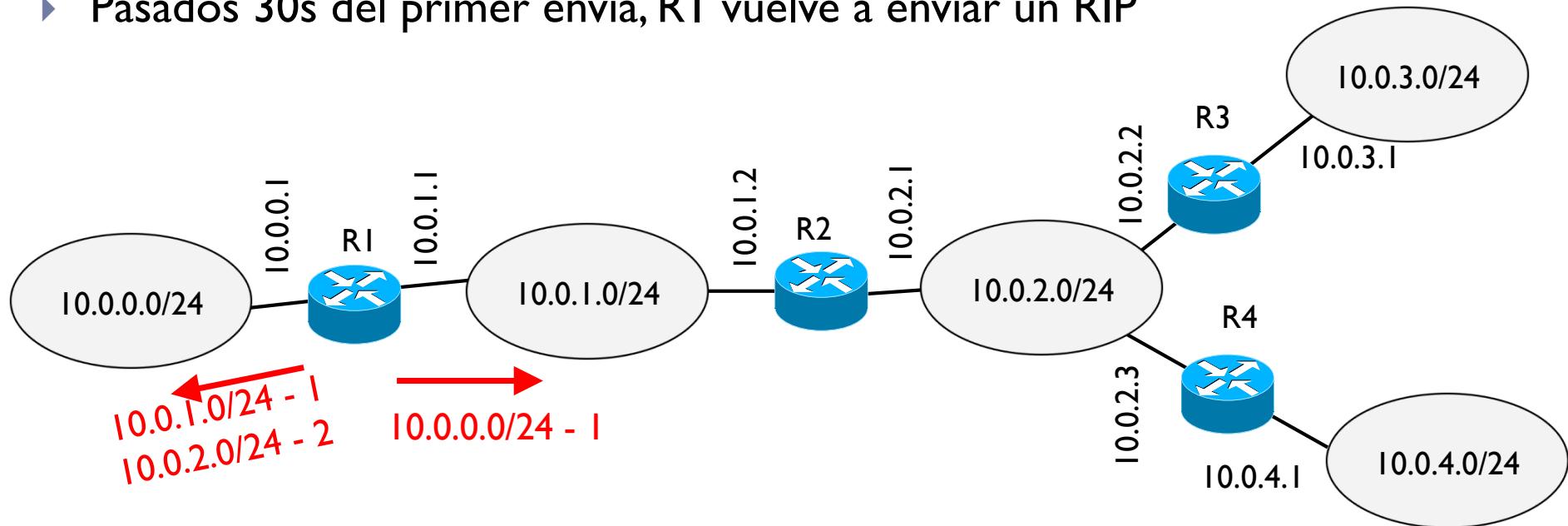


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	10.0.1.2	2

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2
10.0.3.0/24	10.0.2.2	2
10.0.4.0/24	10.0.2.3	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2
10.0.3.0/24	10.0.2.3	2



Tema 2 – Routing Information Protocol (RIP)

- ▶ Pasados 30s del primer envío, R2 vuelve a enviar un RIP

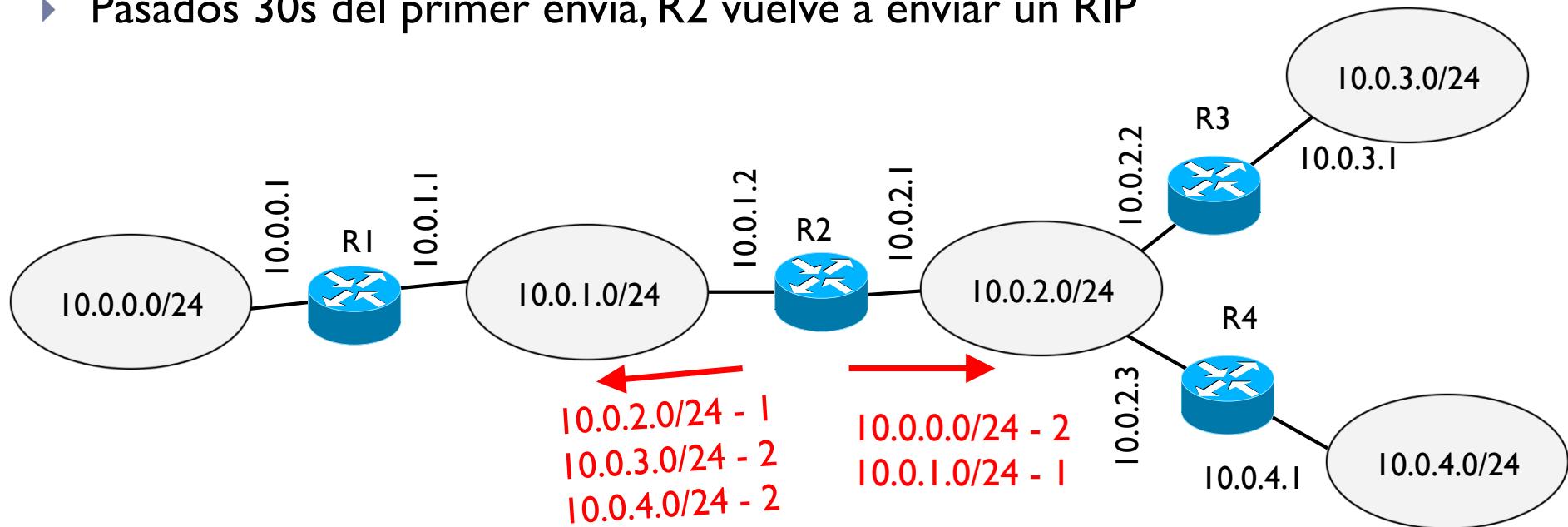


Tabla completa

Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	10.0.1.2	2
10.0.3.0/24	10.0.1.2	3
10.0.4.0/24	10.0.1.2	3

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2
10.0.3.0/24	10.0.2.2	2
10.0.4.0/24	10.0.2.3	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2
10.0.3.0/24	10.0.2.3	2

Tema 2 – Routing Information Protocol (RIP)

- ▶ Aunque las tablas son completas, el sistema sigue con los envío
- ▶ Después de R2 envía R3, R4 y pasado otros 30 s, vuelve a enviar R1, luego R2, R3, R4 y vuelta a empezar pasados 30 s, etc...
- ▶ Si no hay cambios en el sistema (un cambio de red, una nueva red, un nuevo router, etc.), los mensajes que se envían cada 30 s son siempre los mismos
- ▶ Estos mensajes sirven para notificar cambios cuando los hay y como verifica que todo funciona correctamente



Tema 2 – Routing Information Protocol (RIP)

- ▶ Supongamos un fallo en una interfaz de R1

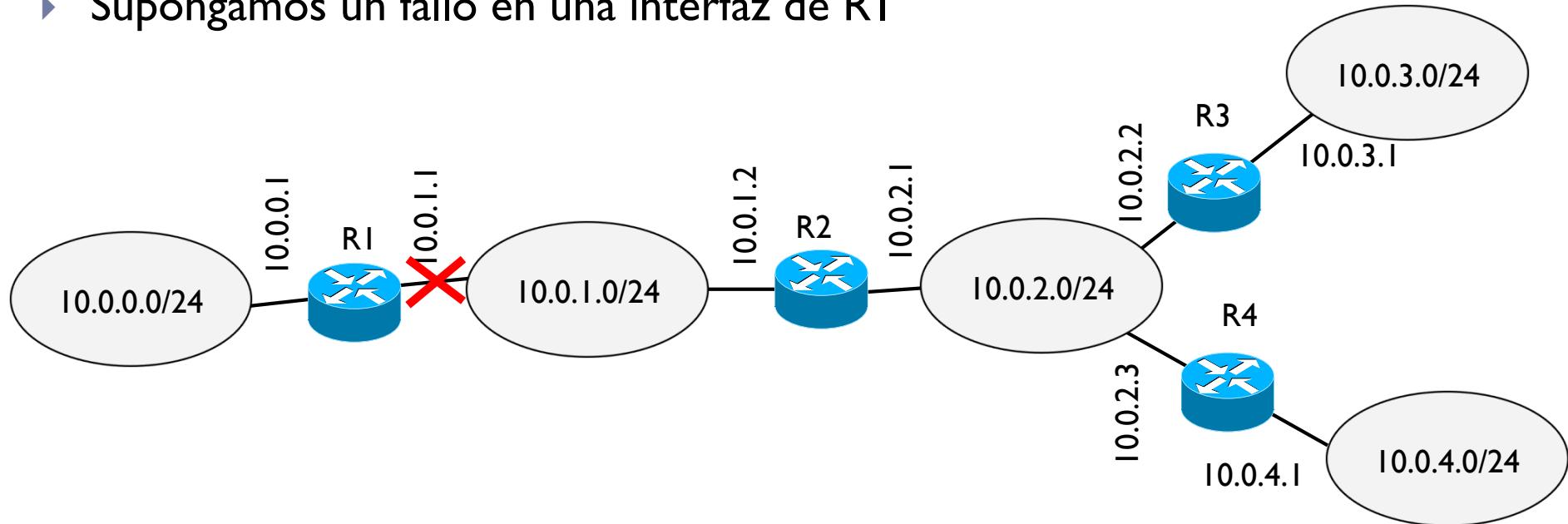


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	10.0.1.2	2
10.0.3.0/24	10.0.1.2	3
10.0.4.0/24	10.0.1.2	3

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2
10.0.3.0/24	10.0.2.2	2
10.0.4.0/24	10.0.2.3	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2
10.0.3.0/24	10.0.2.3	2



Tema 2 – Routing Information Protocol (RIP)

- ▶ RI detecta su fallo y pone métrica infinita 16 (**Poison reverse**)
- ▶ RI envía un mensaje en seguida para notificar el problema (**Triggered Update**)

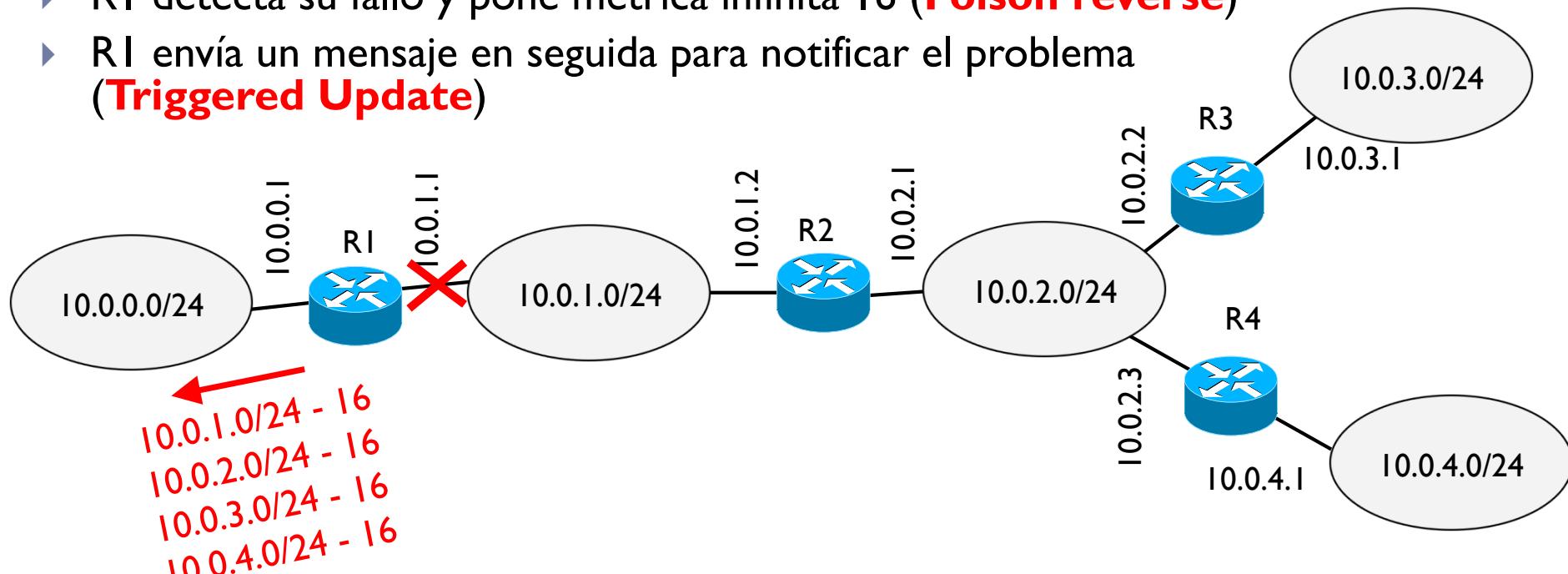


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	16
10.0.2.0/24	10.0.1.2	16
10.0.3.0/24	10.0.1.2	16
10.0.4.0/24	10.0.1.2	16

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	2
10.0.3.0/24	10.0.2.2	2
10.0.4.0/24	10.0.2.3	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2
10.0.3.0/24	10.0.2.3	2



Tema 2 – Routing Information Protocol (RIP)

- ▶ R2 detecta el fallo ya que no le llegan mensajes de R1
- ▶ R2 envía un mensaje en seguida a los demás routers usando métrica 16

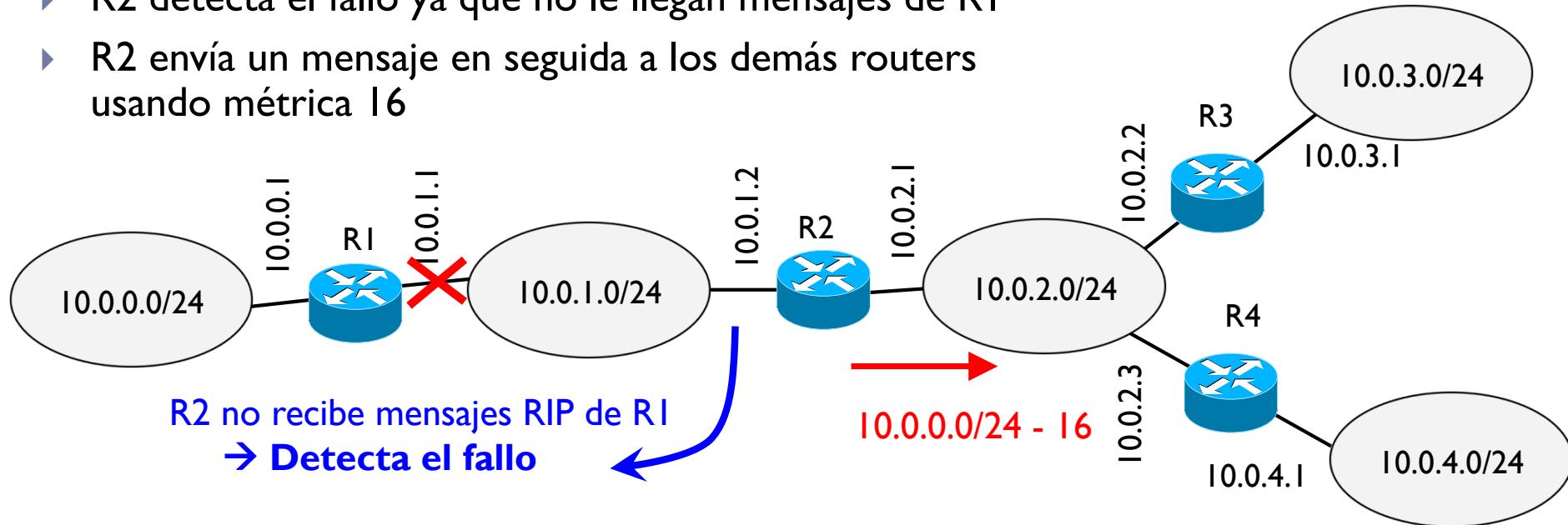


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	16
10.0.2.0/24	10.0.1.2	16
10.0.3.0/24	10.0.1.2	16
10.0.4.0/24	10.0.1.2	16

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	10.0.2.2	2
10.0.4.0/24	10.0.2.3	2

Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	3
10.0.1.0/24	10.0.2.1	2
10.0.3.0/24	10.0.2.3	2



Tema 2 – Routing Information Protocol (RIP)

- ▶ R3 y R4 reciben el mensaje y actualizan sus tablas
- ▶ Y propagan el mensaje a las demás redes

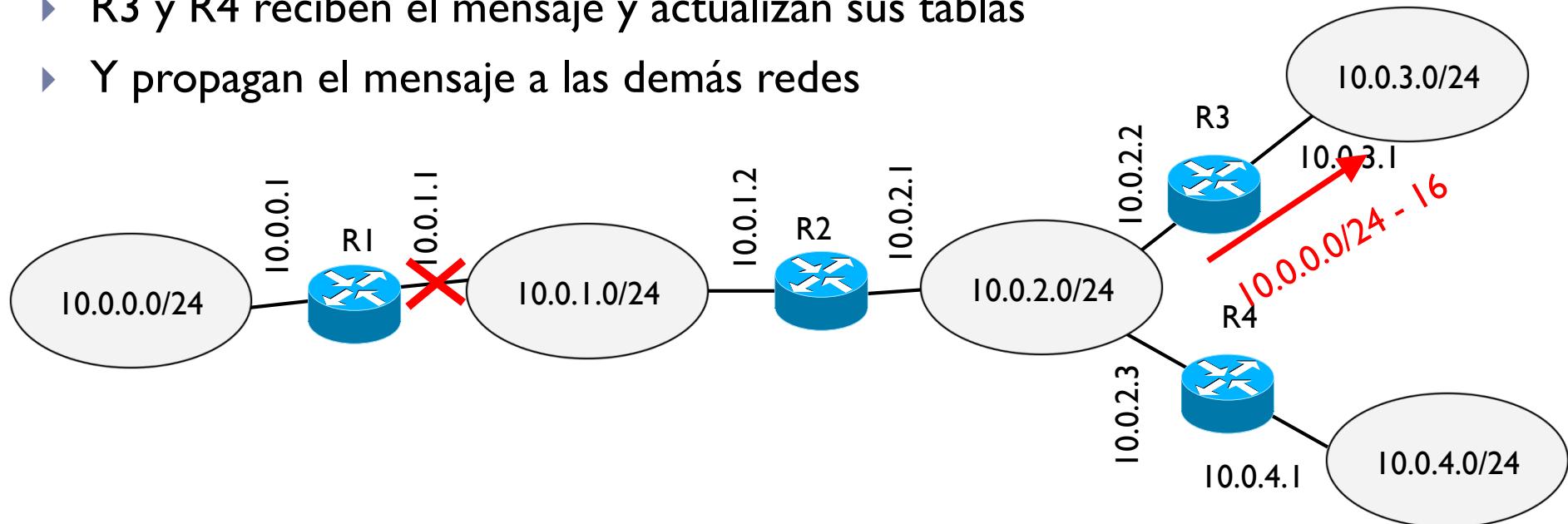


Tabla de R1

Red/mascara	gateway	métrica
10.0.0.0/24	0.0.0.0	1
10.0.1.0/24	0.0.0.0	16
10.0.2.0/24	10.0.1.2	16
10.0.3.0/24	10.0.1.2	16
10.0.4.0/24	10.0.1.2	16

Tabla de R2

Red/mascara	gateway	métrica
10.0.1.0/24	0.0.0.0	1
10.0.2.0/24	0.0.0.0	1
10.0.0.0/24	10.0.1.1	16
10.0.3.0/24	10.0.2.2	2
10.0.4.0/24	10.0.2.3	2

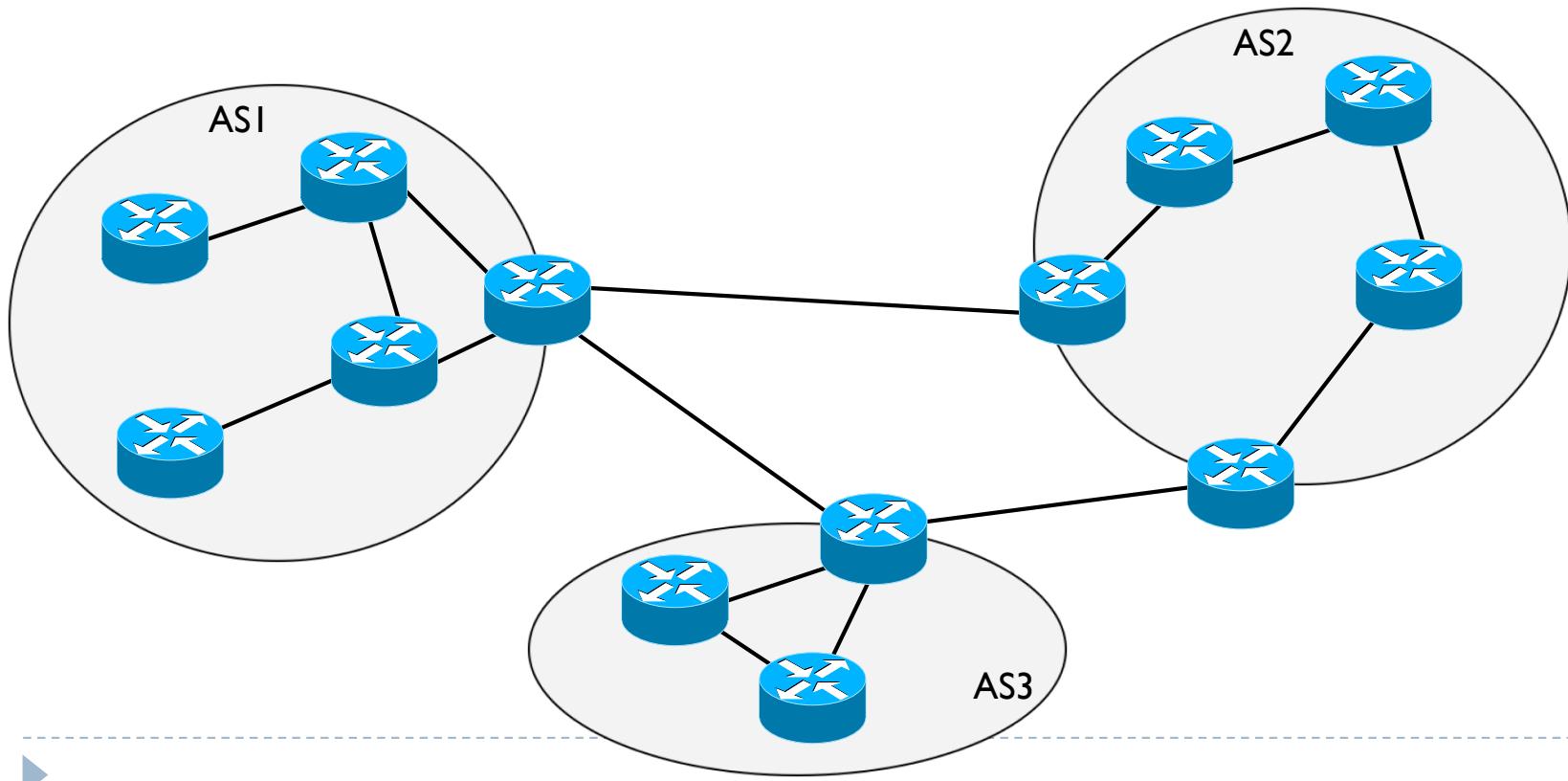
Tabla de R3

Red/mascara	gateway	métrica
10.0.2.0/24	0.0.0.0	1
10.0.3.0/24	0.0.0.0	1
10.0.0.0/24	10.0.2.1	16
10.0.1.0/24	10.0.2.1	2
10.0.3.0/24	10.0.2.3	2



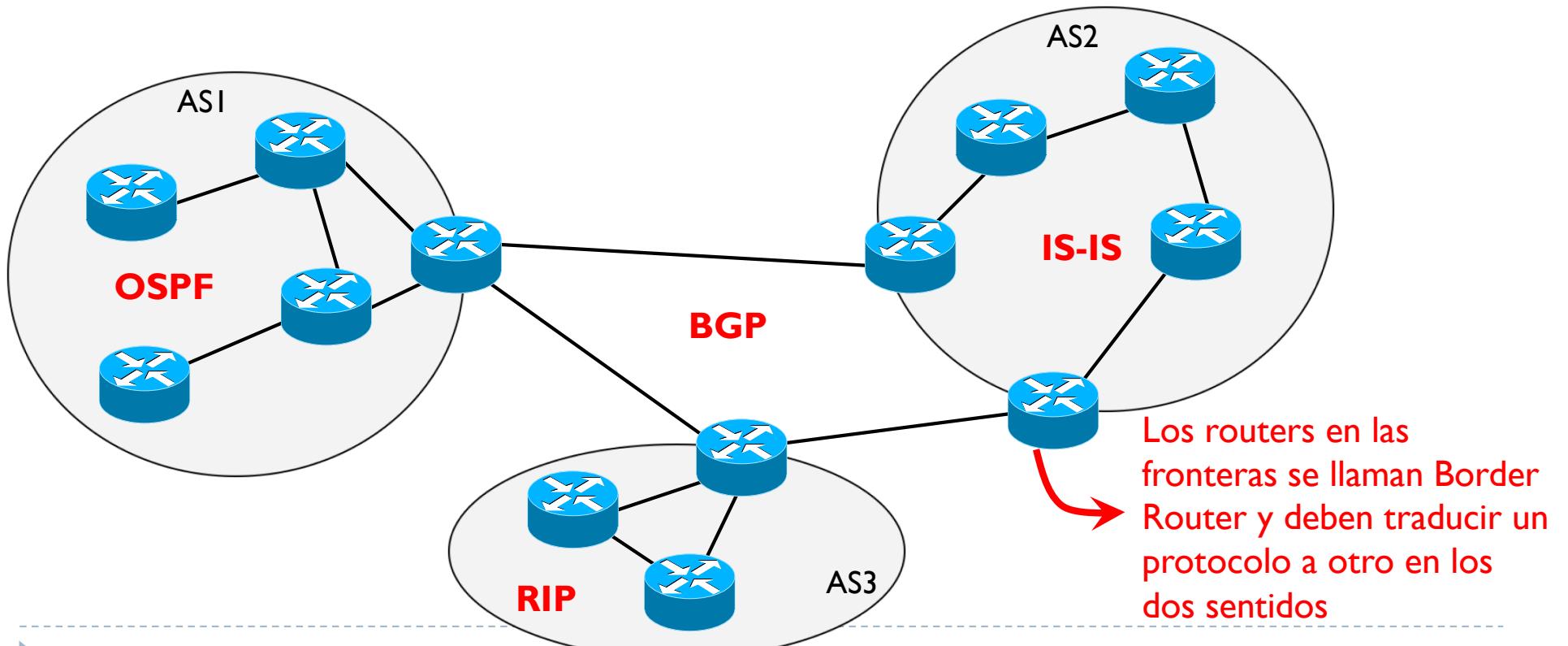
Tema 2 – Encaminamiento dinámico

- ▶ Dado el tamaño y estructura de Internet, usar un único protocolo de encaminamiento es inviable
- ▶ Internet está organizado en Sistemas Autónomos (AS)
 - ▶ Por ejemplo un ISP es un AS
 - ▶ Actualmente hay unos 50,000 AS en Internet



Tema 2 – Encaminamiento dinámico

- ▶ Cada AS tiene un número limitado de routers y redes
- ▶ En cada AS se usa un único protocolo de encaminamiento, llamado interno
 - ▶ RIP es un ejemplo pero hay mas como OSPF (RFC 1583), IS-IS (RFC 1142)
- ▶ Entre AS se usa un único protocolo de encaminamiento, llamado externo
 - ▶ En este caso en Internet solo se puede usar BGP (RFC 1771)



Tema 2 – Redes IP

- ▶ Introducción
- ▶ Direccionamiento y subnetting
- ▶ Encaminamiento
- ▶ Protocolo ARP
- ▶ Cabecera IP
- ▶ Protocolo ICMP
- ▶ Protocolo DHCP
- ▶ Mecanismo NAT
- ▶ Encaminamiento dinámico RIP
- ▶ **Alguna noción de seguridad**



Tema 2 – Seguridad en redes

- ▶ Objetivos de la seguridad
 - ▶ Confidencialidad: solo origen y destino deben poder entender el mensaje
 - ▶ Autentificación: origen y destino deben poder confirmar la identidad del otro
 - ▶ Integridad del mensaje: origen y destino quieren poder asegurar que el mensaje se recibe sin alterar y que nadie más lo haya podido recibir
 - ▶ Acceso y disponibilidad: los servicios deben ser accesibles y disponibles a los usuarios



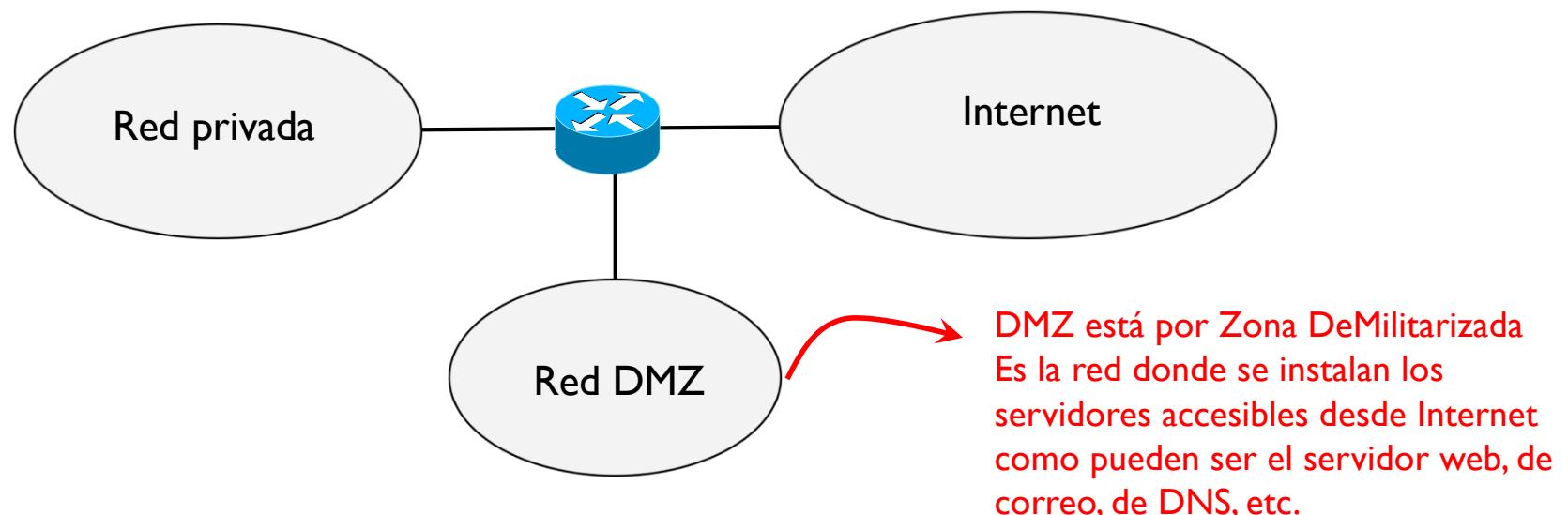
Tema 2 – Seguridad en redes

- ▶ Tipos de ataques
 - ▶ De reconocimiento de vulnerabilidad y acceso
 - ▶ Tipo de servidores, sistema operativo, @IP, etc.
 - ▶ Denegación del servicio
 - ▶ Inhabilitar o corromper un servicio o una red
 - ▶ Introducir gusanos, virus o troyanos
 - ▶ Acceder, modificar y atacar otros servicios desde dentro una red



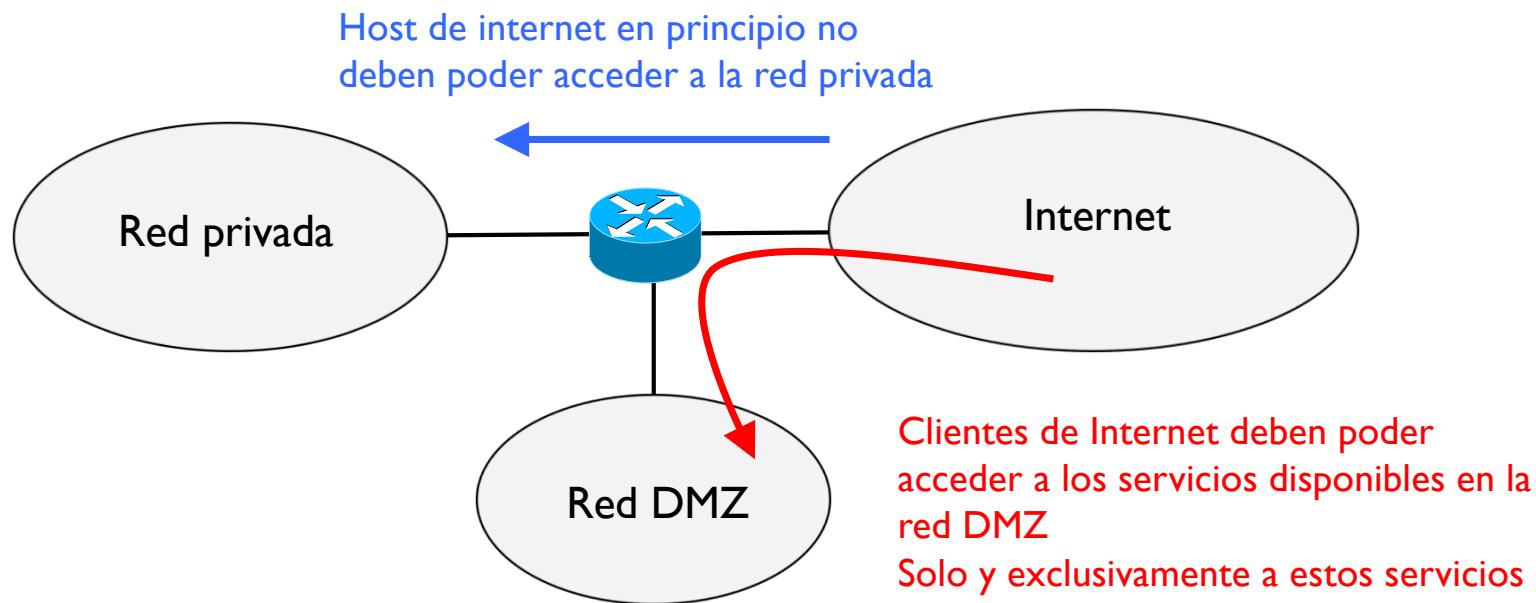
Tema 2 – Firewall y ACLs

- ▶ Un firewall (o cortafuego) es un equipo de red que permite controlar la entrada y salida de la información y, si necesario, filtrar aquella no permitida
- ▶ Generalmente la configuración de una red interna tiene esta estructura



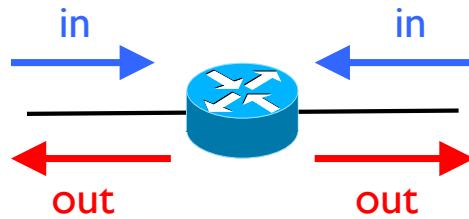
Tema 2 – Firewall y ACLs

- ▶ De manera que el acceso a las dos redes internas, la privada y la DMZ desde Internet debe estar controlada para evitar fallos de seguridad
- ▶ En concreto, el router necesita implementar funciones de Firewall para inspeccionar todos los datagramas y descartar los que no están permitidos



Tema 2 – Firewall y ACLs

- ▶ El control en el router se hace con Listas de Acceso (ACLs)
- ▶ Las ACLs se aplican a las interfaces del router y pueden ser de entrada o de salida



- ▶ Una ACL es una lista secuencial de condiciones de permiso o prohibición según
 - ▶ @IP origen y destino
 - ▶ Puertos origen y destino
 - ▶ Protocolo (IP, TCP, UDP, ICMP, etc.)
 - ▶ Estado (cualquiera o respuesta)

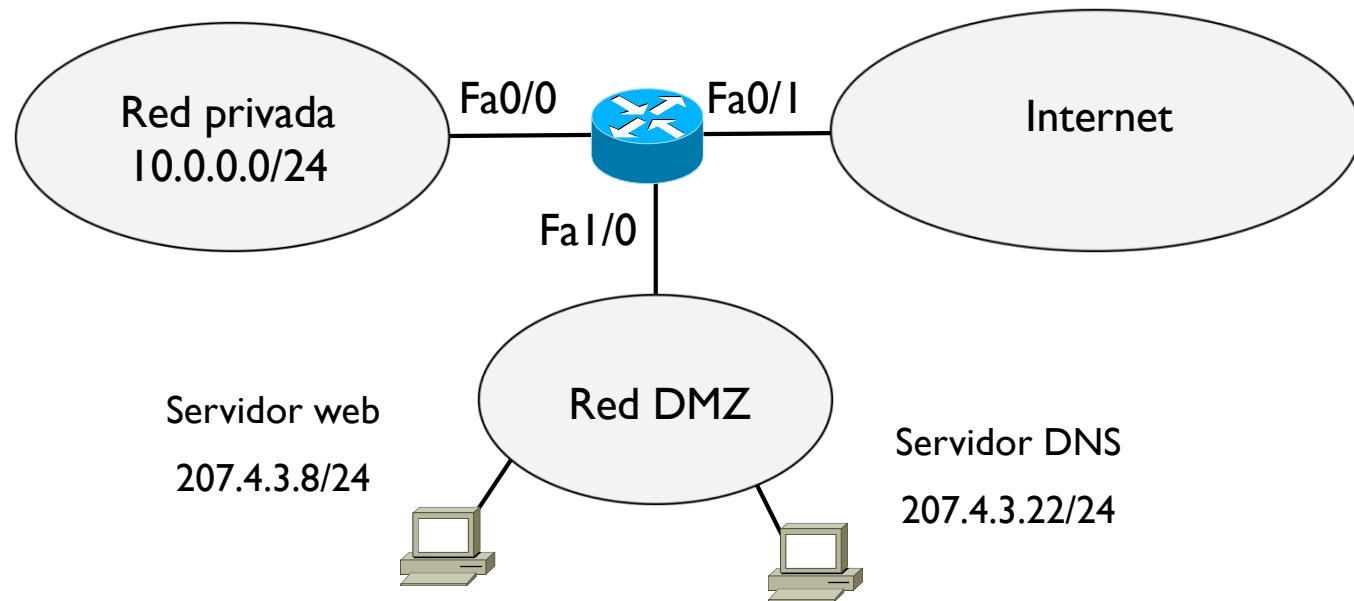


Tema 2 – Firewall y ACLs

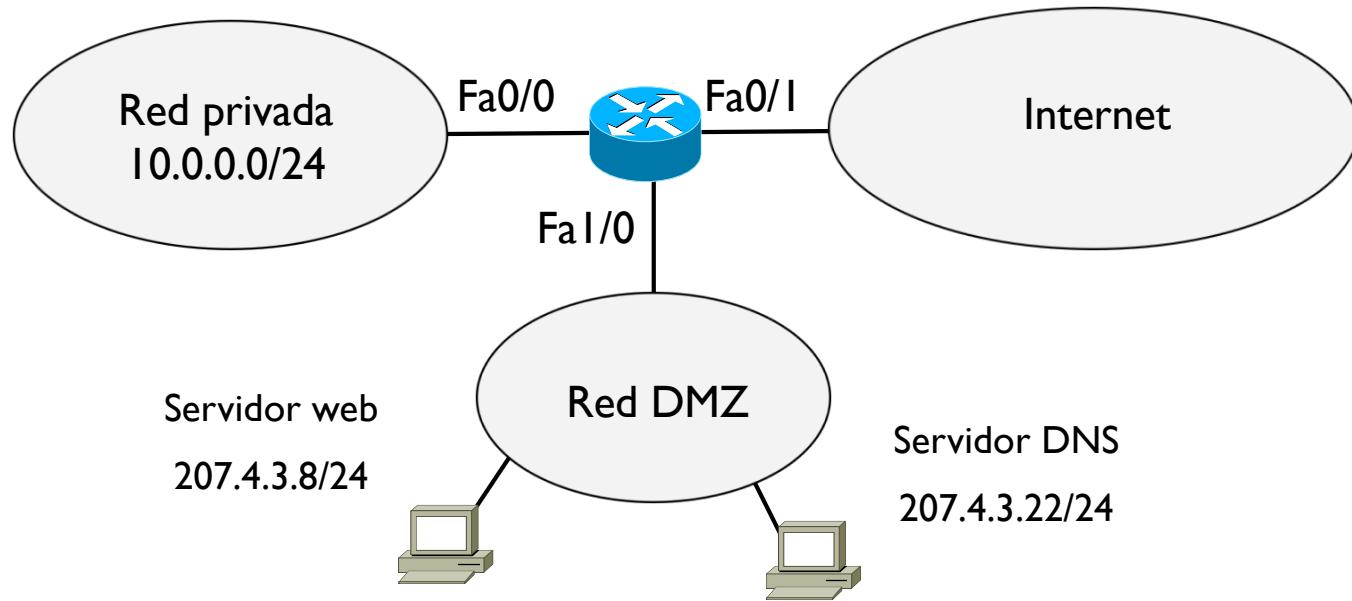
- ▶ Para evitar complicar una ACL mezclando permisos con prohibiciones, generalmente se usa uno de estos dos enfoques
- ▶ En el primero, se crea una lista de condiciones permitidas y se concluyen con una última línea que deniega todo lo que queda
 - ▶ Permitir condición_1
 - ▶ Permitir condición_2
 - ▶ ...
 - ▶ Permitir condición_n
 - ▶ Prohibir todo
- ▶ El segundo enfoque es el contrario del primero: la lista tiene una serie de condiciones prohibidas y se concluyen con una que permite todo
 - ▶ Prohibir condición_1
 - ▶ Prohibir condición_2
 - ▶ ...
 - ▶ Prohibir condición_n
 - ▶ Permitir todo



Tema 2 – Firewall y ACLs ejemplo

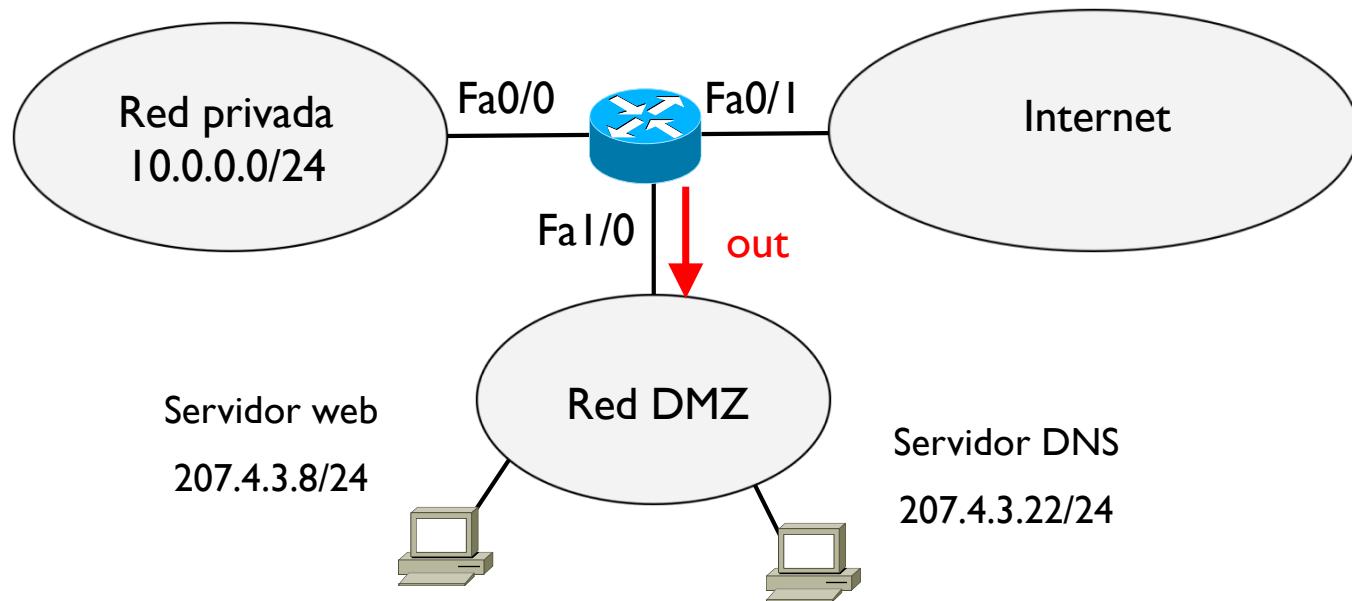


Tema 2 – Firewall y ACLs ejemplo



- ▶ Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ
- ▶ Hay que definir donde aplicar esta ACL
 - ▶ Se recomienda aplicarla siempre lo más próximo posible a la zona que se quiere proteger
 - ▶ En este caso conviene aplicarla a la interfaz Fa1/0 de salida respecto al router (es decir hacia la red DMZ)

Tema 2 – Firewall y ACLs ejemplo



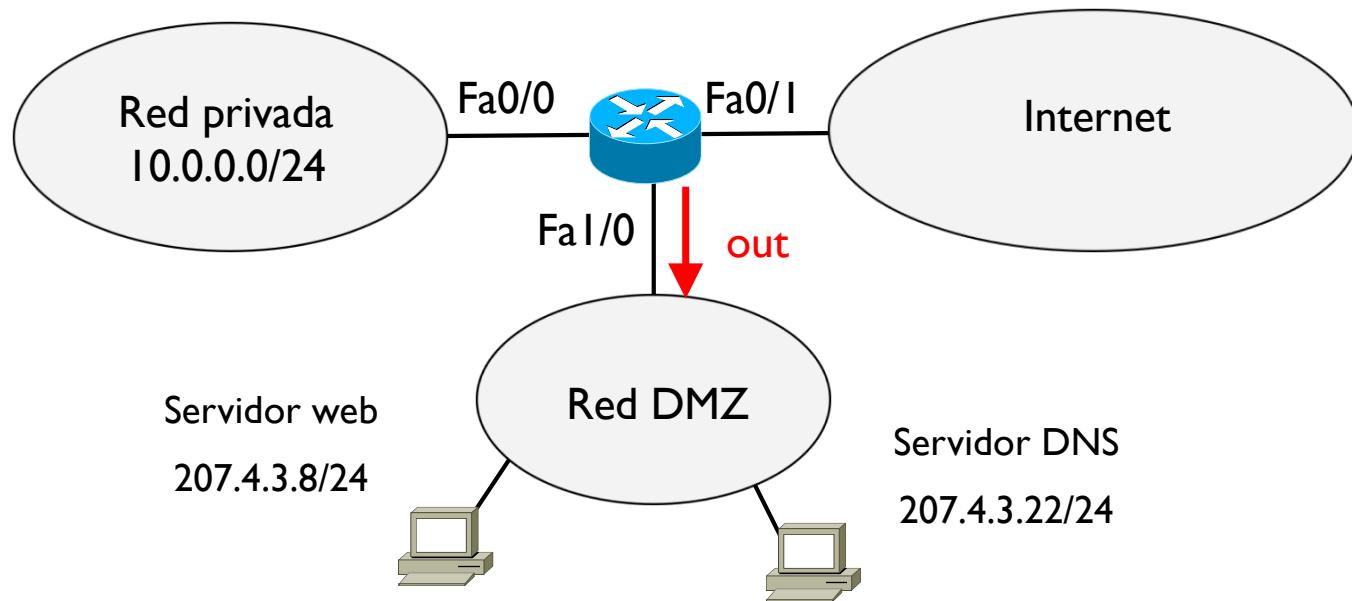
- ▶ Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80

 └──────────┘
 acción



Tema 2 – Firewall y ACLs ejemplo



- ▶ Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

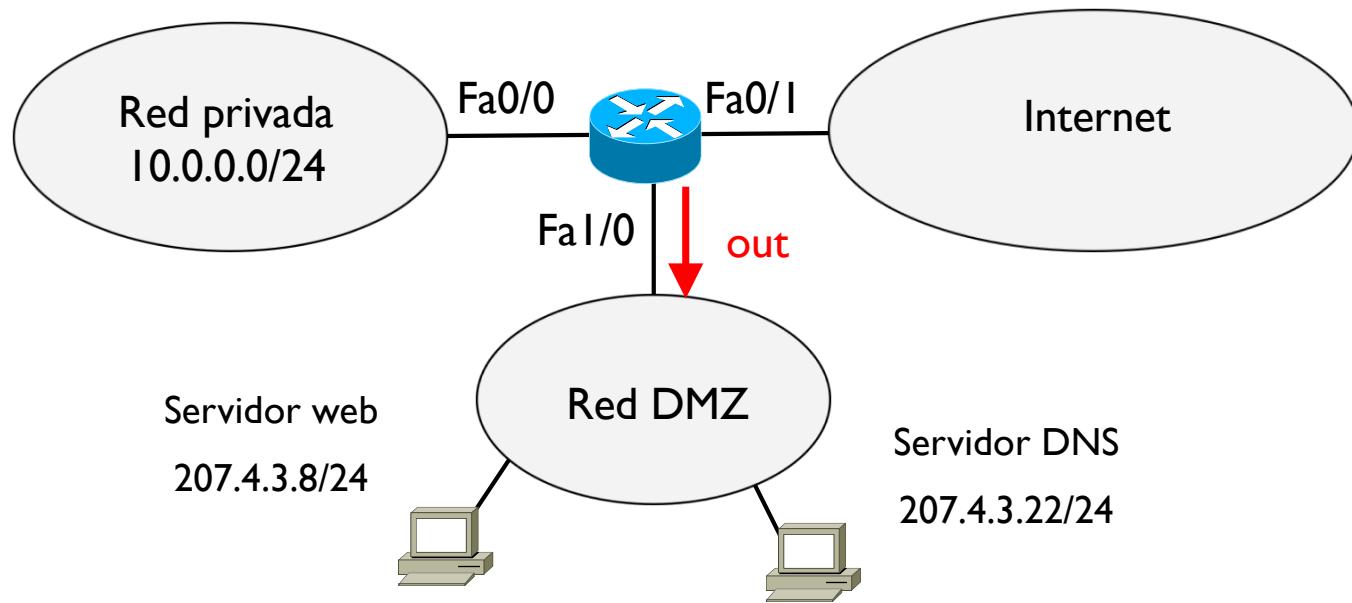
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80



Protocolo de transporte
usado por el servidor web



Tema 2 – Firewall y ACLs ejemplo



- ▶ Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

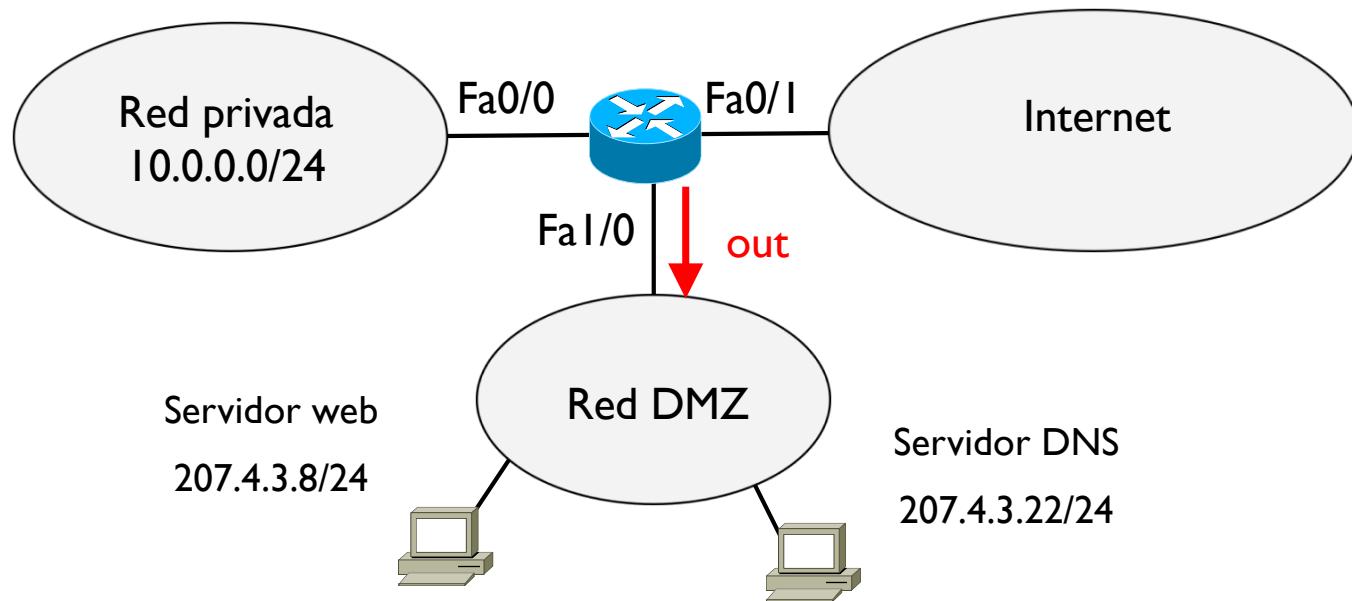
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80



La @IP origen puede ser
cualquiera



Tema 2 – Firewall y ACLs ejemplo



- ▶ Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

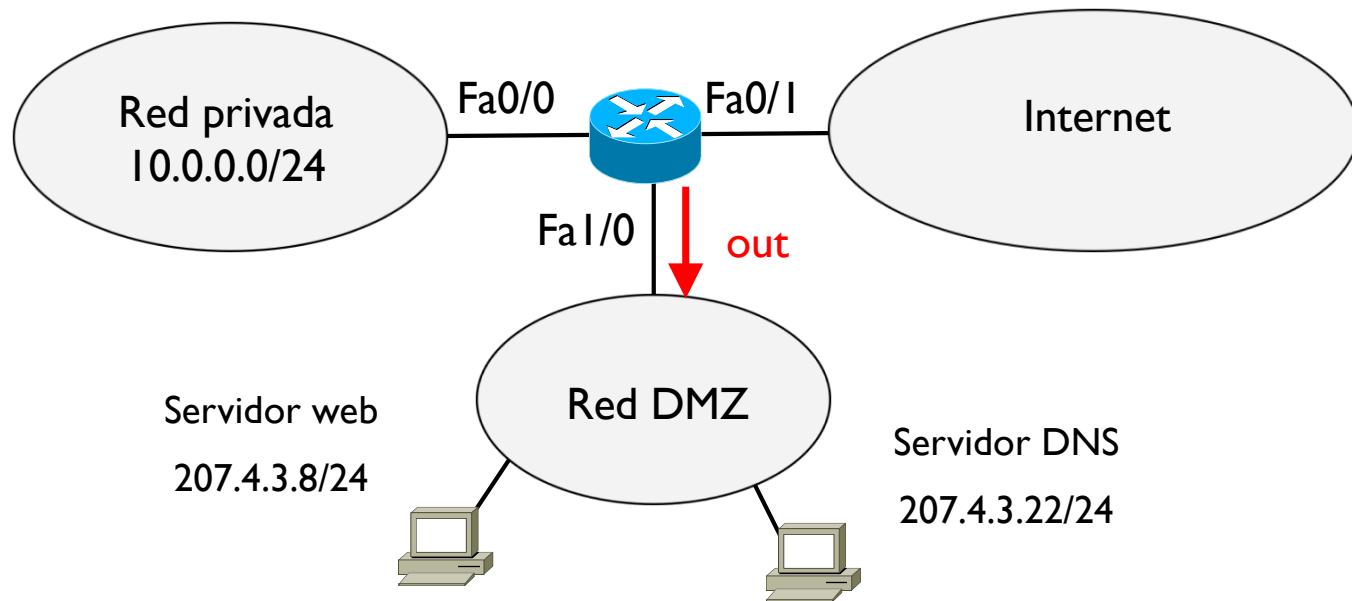
```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```



Se quiere acceder al servicio web
por lo tanto el puerto origen es un puerto
efímero mayor igual que 1024



Tema 2 – Firewall y ACLs ejemplo



- ▶ Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

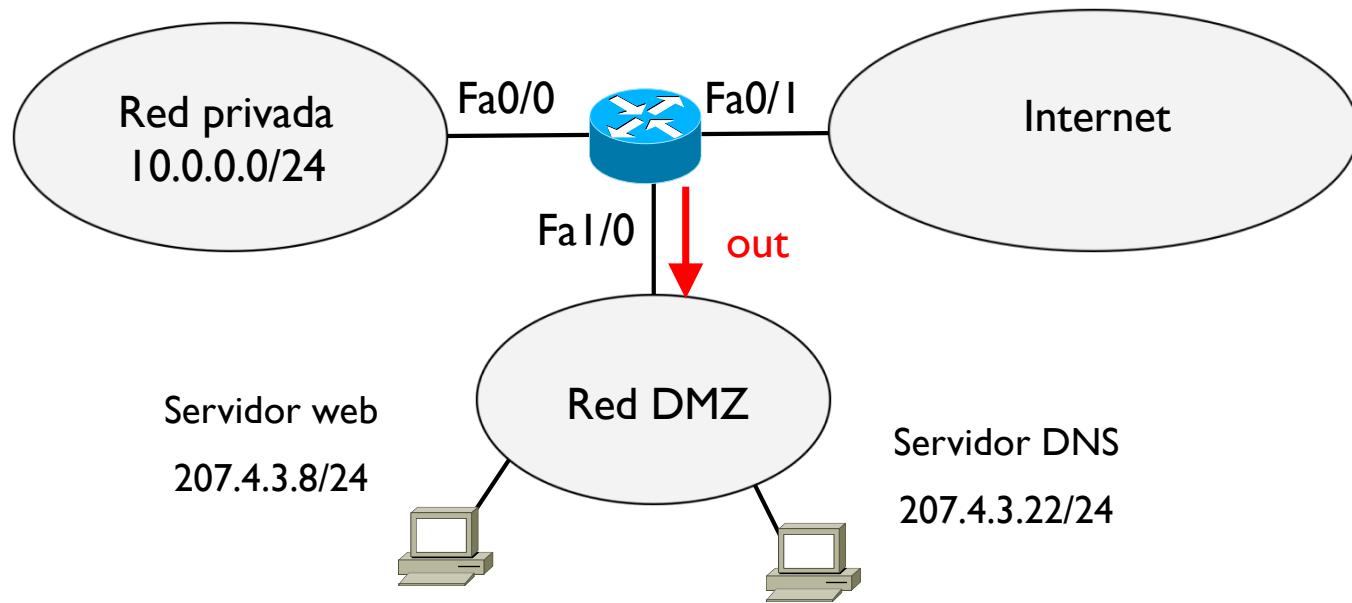
```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```



La @IP destino debe ser la del servidor web



Tema 2 – Firewall y ACLs ejemplo



- ▶ Hay que crear una primera ACL que controle el acceso a los dos servidores públicos de la red DMZ

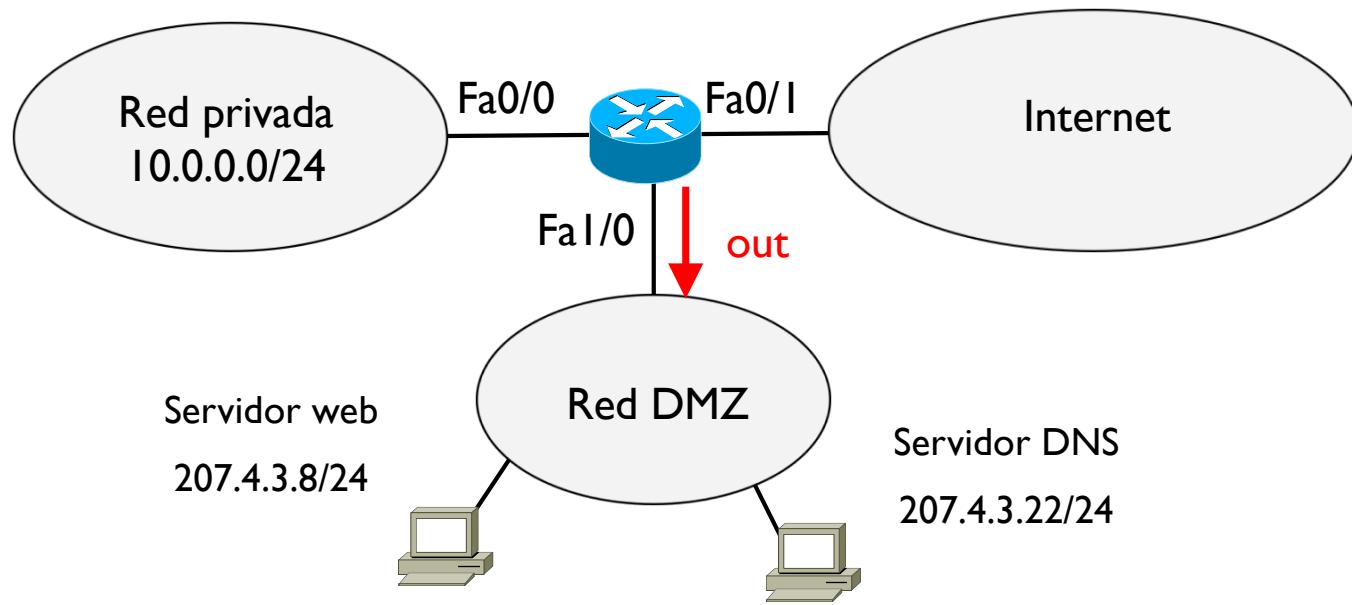
```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```



Se accede a este servidor exclusivamente para su servicio 80, es decir páginas web HTTP



Tema 2 – Firewall y ACLs ejemplo

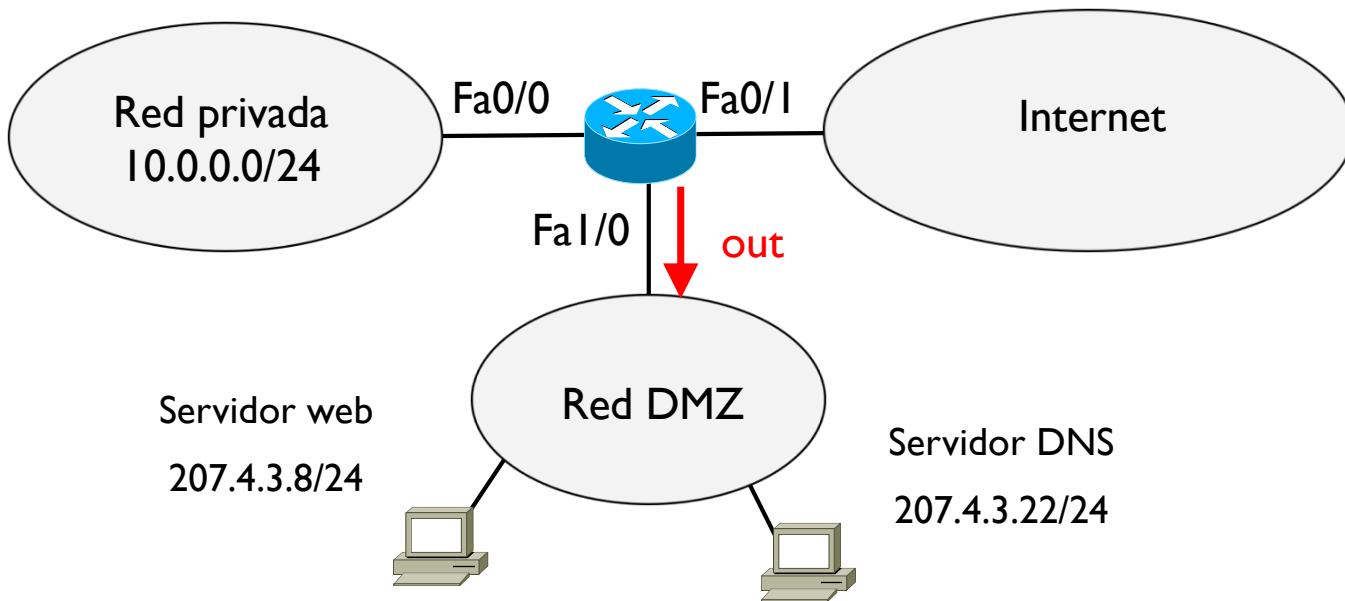


```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```

```
permitir UDP 0.0.0.0/0 ≥1024 207.4.3.22/24 53
```

Lo mismo con el servicio DNS que usa UDP

Tema 2 – Firewall y ACLs ejemplo



```
permitir TCP 0.0.0.0/0 ≥1024 207.4.3.8/24 80
```

```
permitir UDP 0.0.0.0/0 ≥1024 207.4.3.22/24 53
```

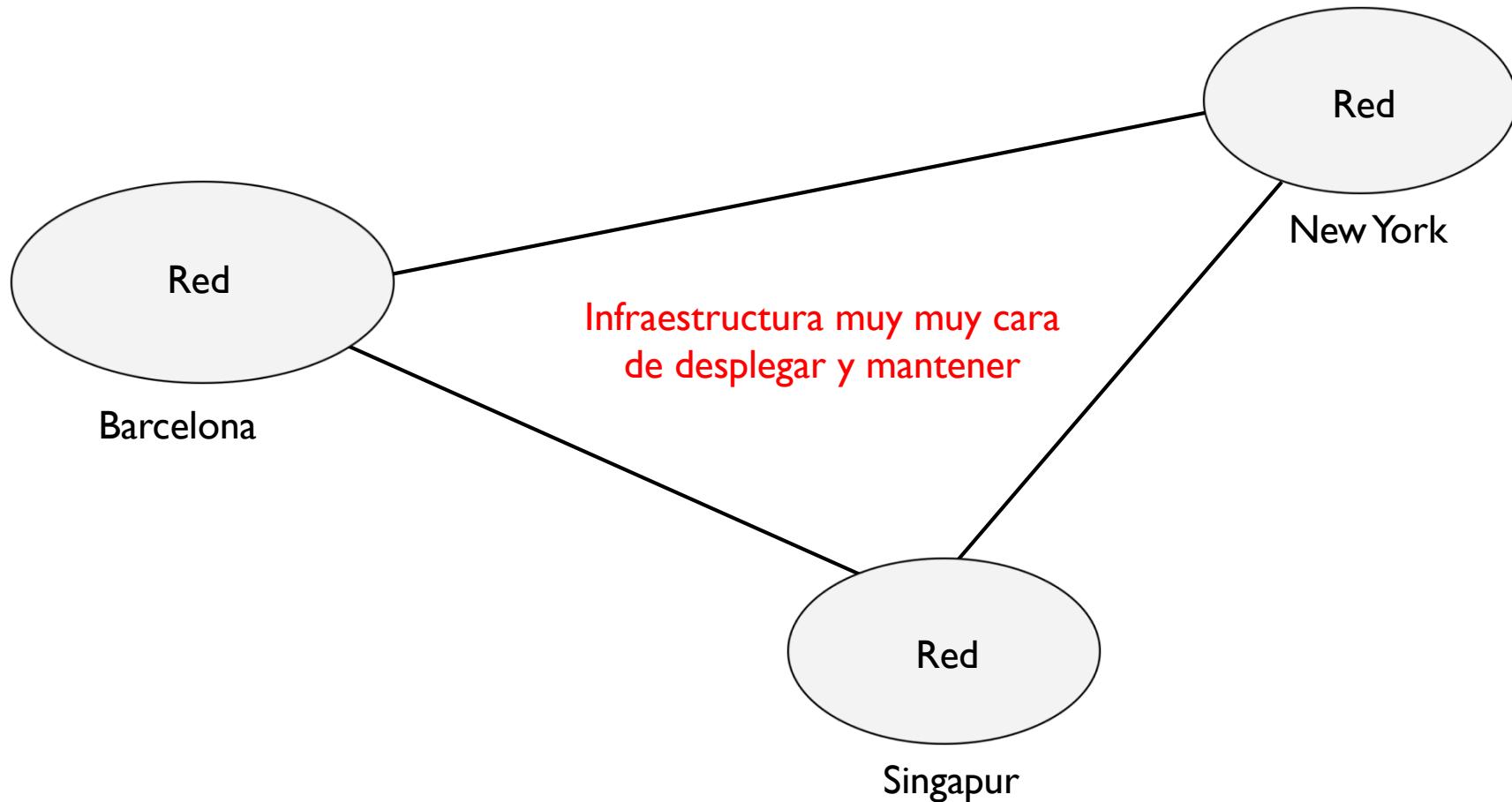
```
prohibir IP 0.0.0.0/0 0.0.0.0/0
```

Se denega todo. Como es una lista secuencial, si una de las dos primeras condiciones se verifica, se permite y se sale de la lista.

Esta última prohibición se haría solo si no se cumpliesen las dos primeras condiciones, es decir es como si fuera una regla por defecto que se hace en última instancia

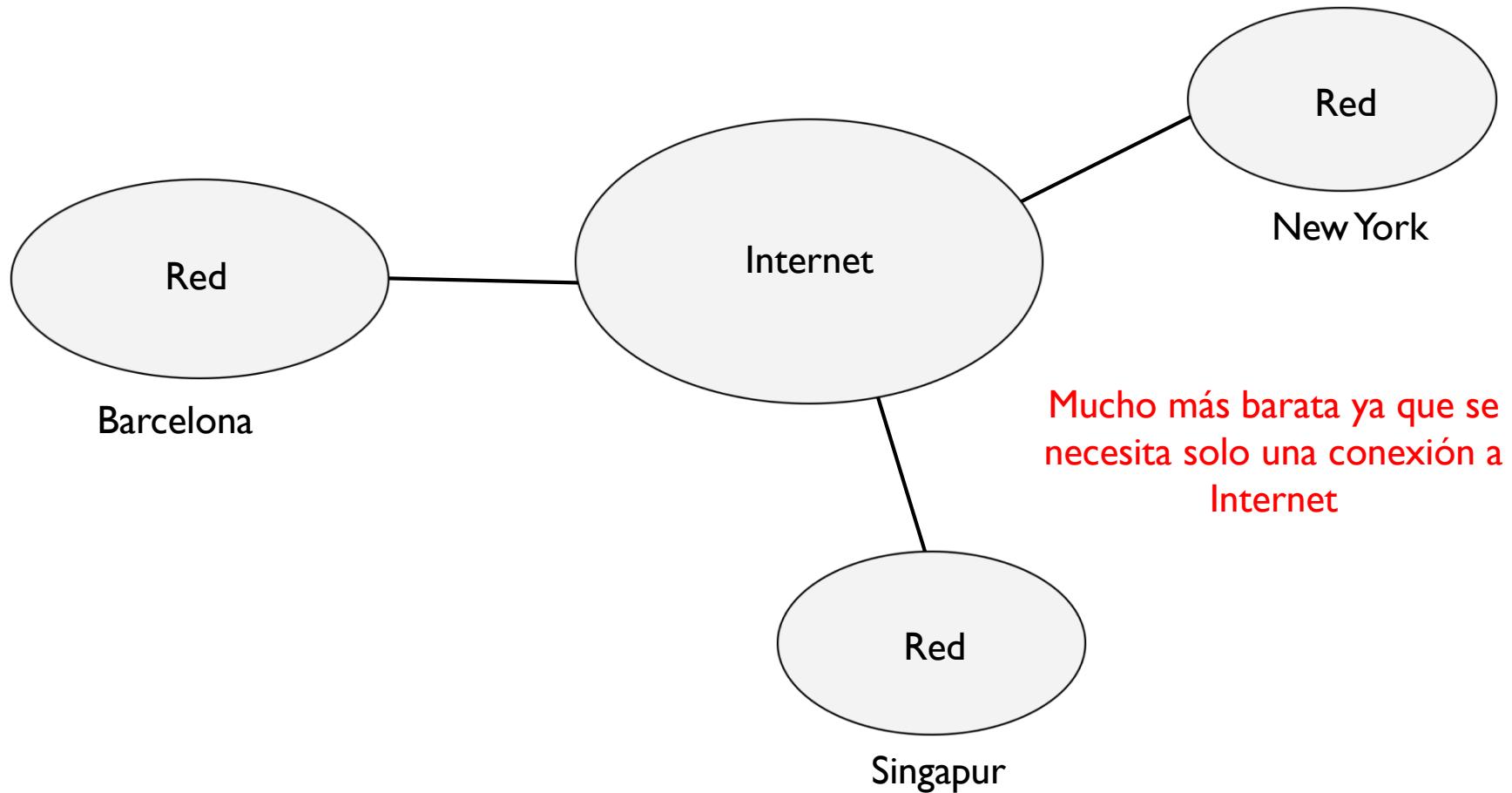
Tema 2 – Redes privadas virtuales

- ▶ Si una entidad tiene varias sucursales en diferentes lugares, necesita una infraestructura que las interconecte



Tema 2 – Redes privadas virtuales

- ▶ VPN: permite conectividad entre usuarios remotos usando Internet como si fuera una red privada



Tema 2 – Redes privadas virtuales

▶ Problemas

- ▶ Seguridad: Internet es una red pública, los datos enviados podrían ser recibido y leído por cualquiera o cualquiera podría hacerse pasar de sucursal
- ▶ Gestión: cada sucursal con su propia configuración, sus @IP, sus servicios, etc.



Tema 2 – Redes privadas virtuales

▶ Problemas

- ▶ Seguridad: Internet es una red pública, los datos enviados podrían ser recibido y leído por cualquiera o cualquiera podría hacerse pasar de sucursal
- ▶ Gestión: cada sucursal con su propia configuración, sus @IP, sus servicios, etc.

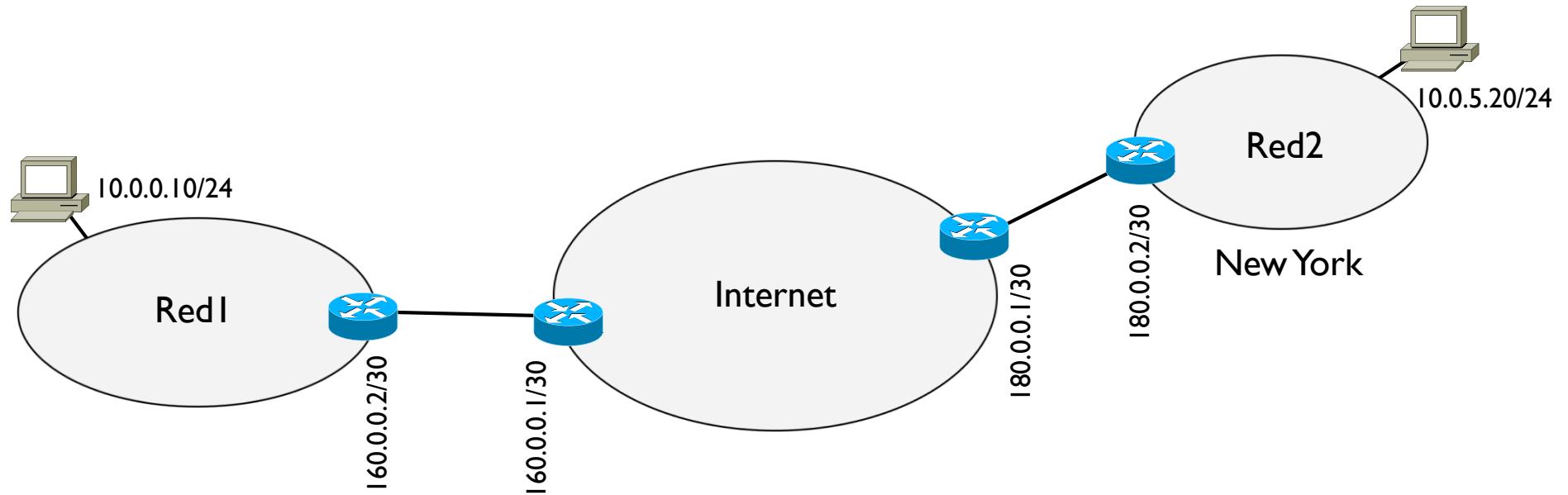
▶ Solución

- ▶ Seguridad: autentificación y encriptación
- ▶ Gestión: construcción de túneles (enlaces virtuales) entre sucursales por encima de Internet



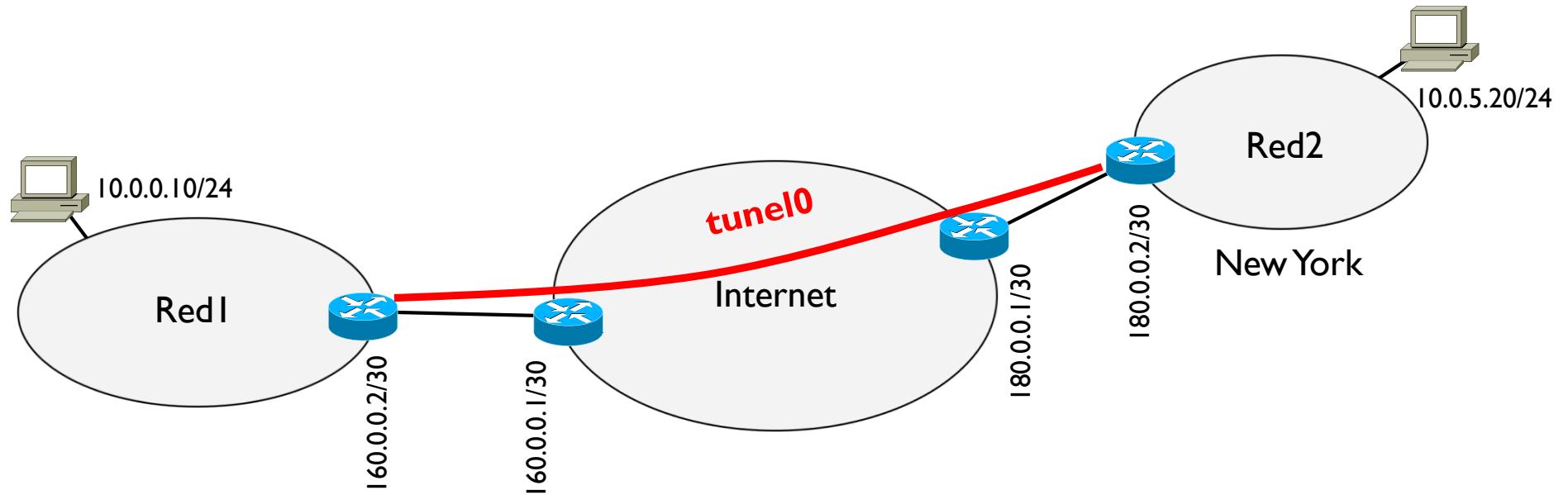
Tema 2 – Redes privadas virtuales

- ▶ Gestión: se configuran túneles entre routers



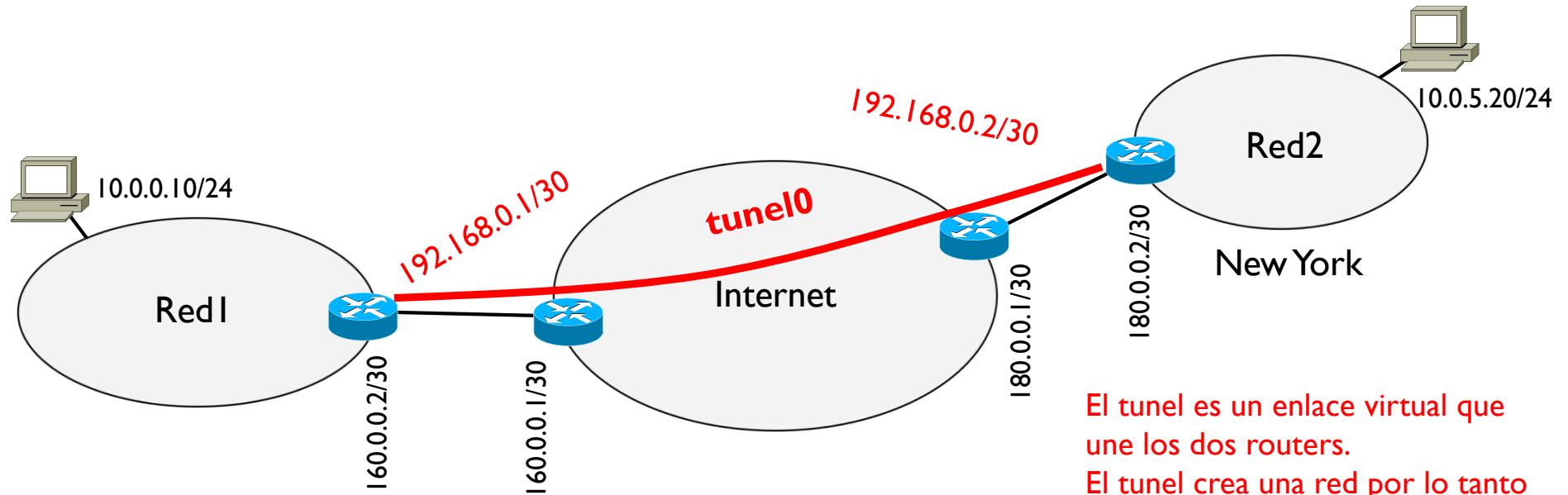
Tema 2 – Redes privadas virtuales

- ▶ Gestión: se configuran túneles entre routers



Tema 2 – Redes privadas virtuales

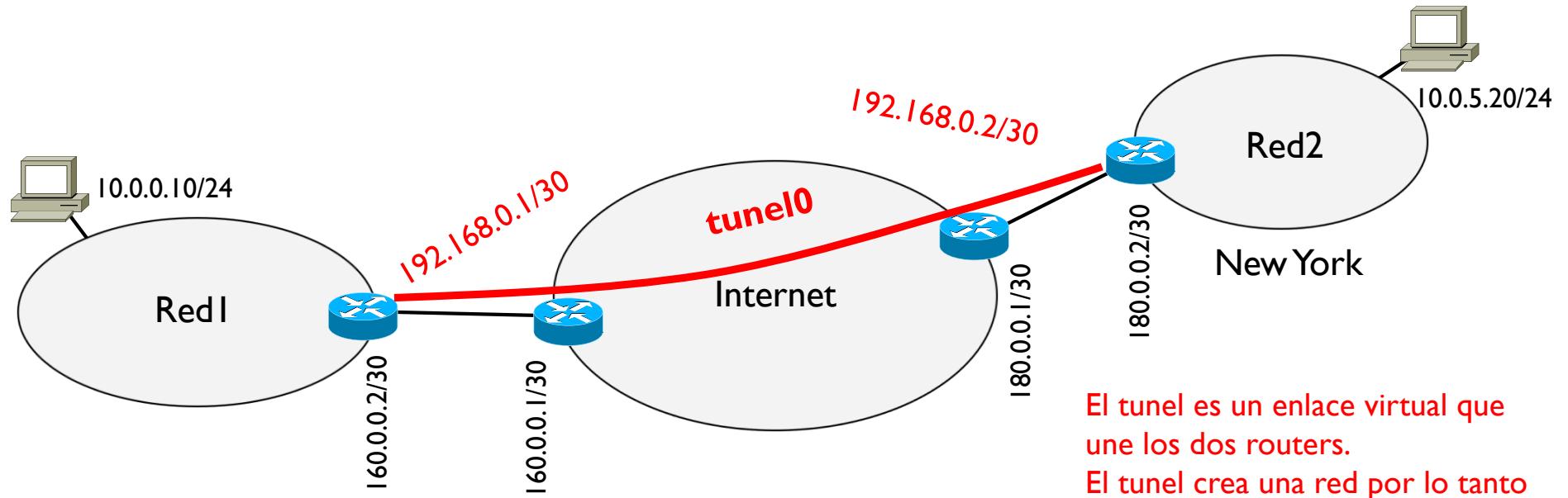
- ▶ Gestión: se configuran túneles entre routers



El tunel es un enlace virtual que une los dos routers.
El tunel crea una red por lo tanto hay que asignarle una @IP de red.
En el ejemplo es la $192.168.0.0/30$

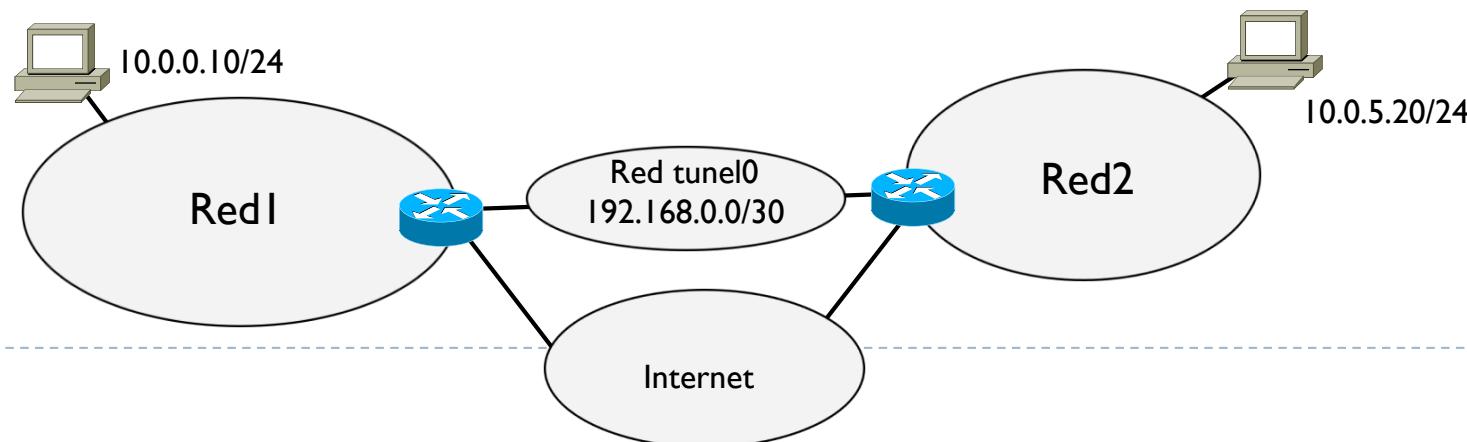
Tema 2 – Redes privadas virtuales

- ▶ Gestión: se configuran túneles entre routers



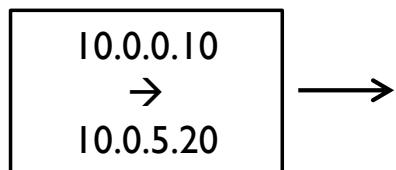
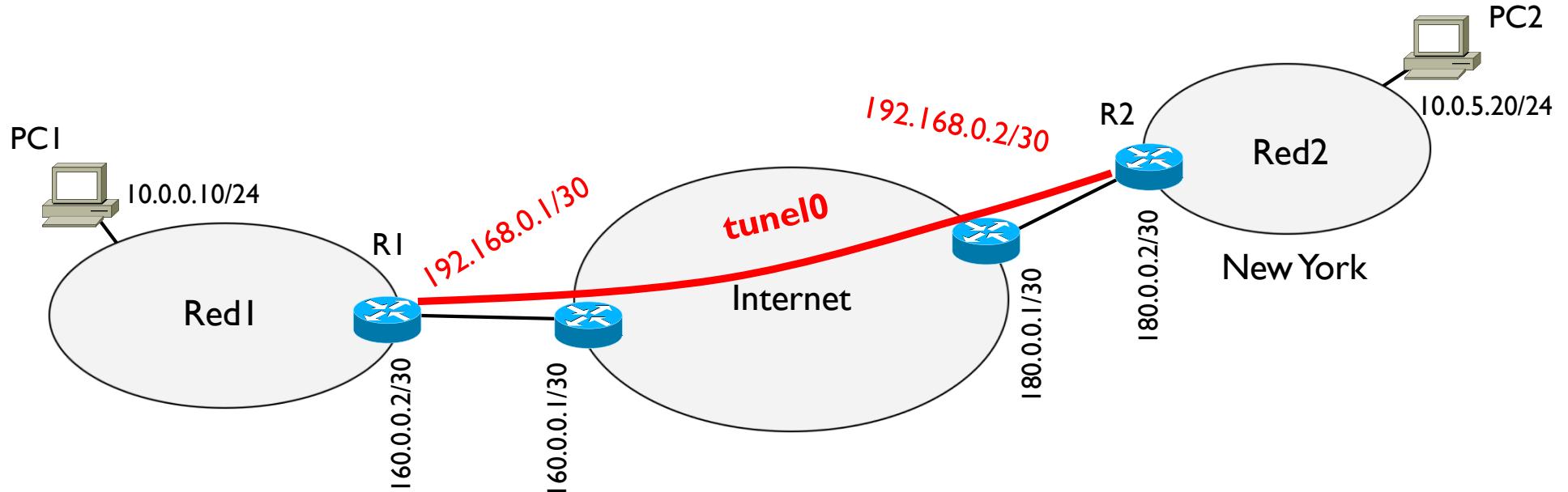
El tunel es un enlace virtual que une los dos routers.
El tunel crea una red por lo tanto hay que asignarle una @IP de red.
En el ejemplo es la 192.168.0.0/30

- ▶ Red1 y Red2 crean estar conectadas de esta forma



Tema 2 – Redes privadas virtuales

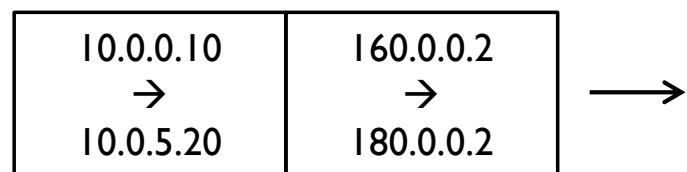
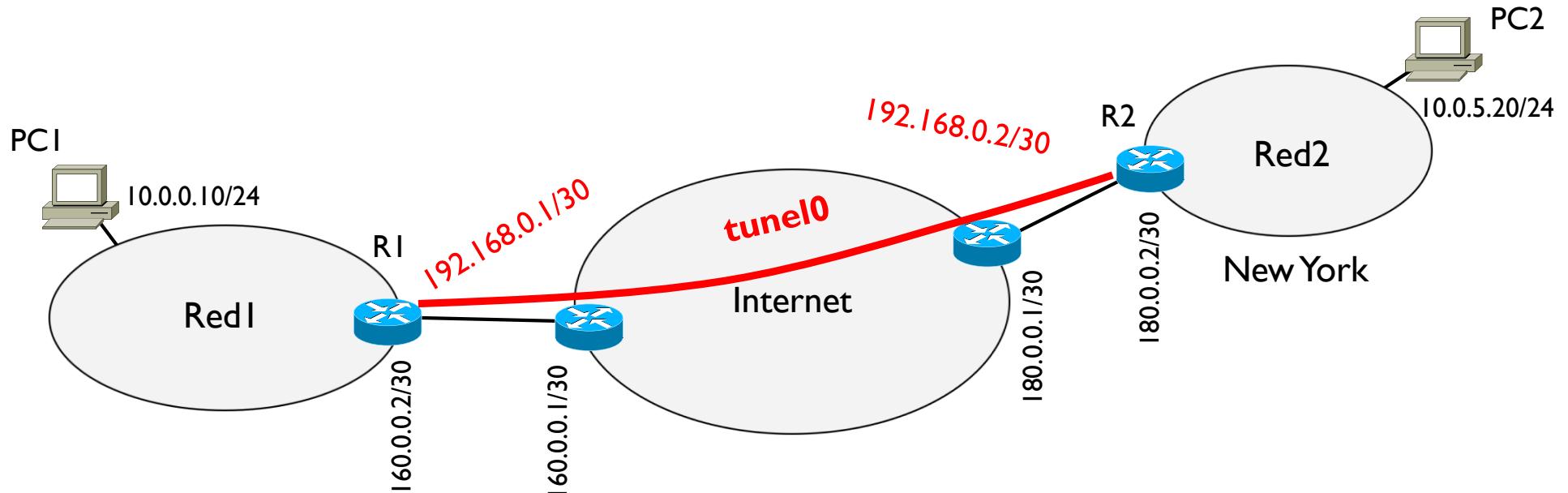
- ▶ Como funciona la transmisión entre estas dos redes



Si PC1 envía un datagrama a PC2, este llega al router R1

Tema 2 – Redes privadas virtuales

- ▶ Como funciona la transmisión entre estas dos redes

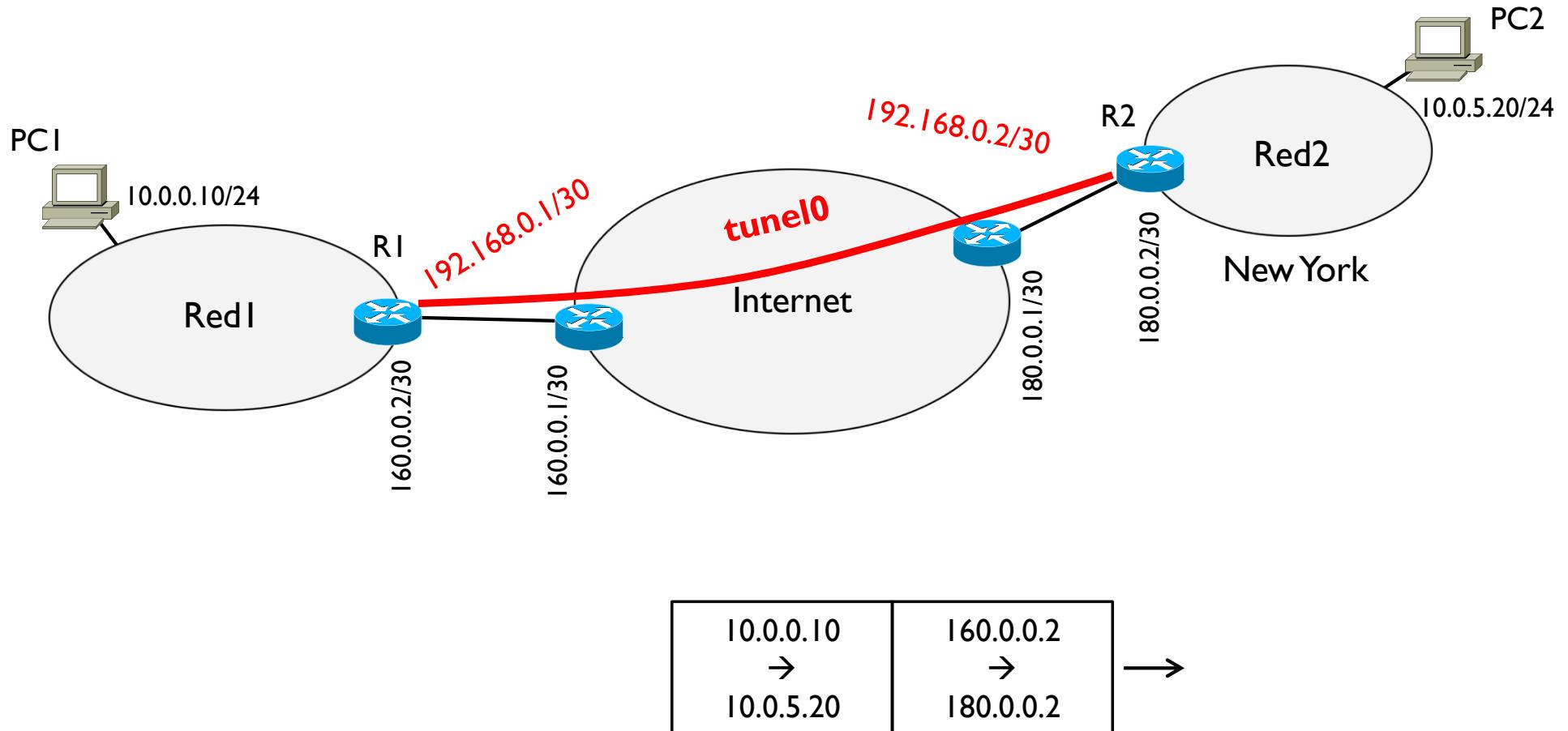


R1 encapsula este datagrama en otro datagrama poniendo como @IP origen y @IP destino las dos @IP publicas de los routers extremos del tunel



Tema 2 – Redes privadas virtuales

- ▶ Como funciona la transmisión entre estas dos redes



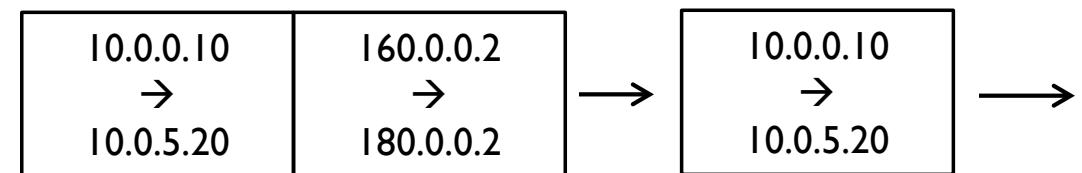
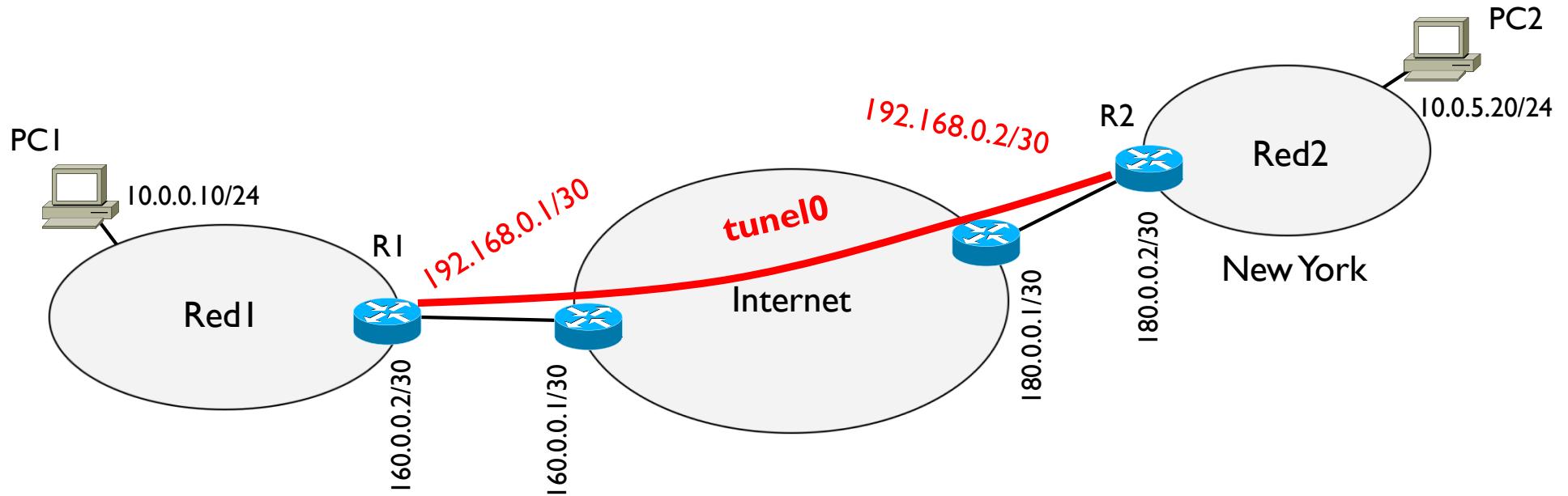
10.0.0.10 → 10.0.5.20	160.0.0.2 → 180.0.0.2
-----------------------------	-----------------------------

El datagrama se encamina por Internet usando la cabecera externa
(la que contiene las @IP publicas) y llega a R2

Todo lo que pasa en Internet (decremento TTL, checksum, etc.) solo
afecta la cabecera externa, la cabecera interna no se toca

Tema 2 – Redes privadas virtuales

- ▶ Como funciona la transmisión entre estas dos redes



R2 quita la cabecera externa y vuelve al datagrama original que había enviado PC1 y lo transmite a PC2



Tema 2 – Redes privadas virtuales

- ▶ Configuración de los routers: sin túnel

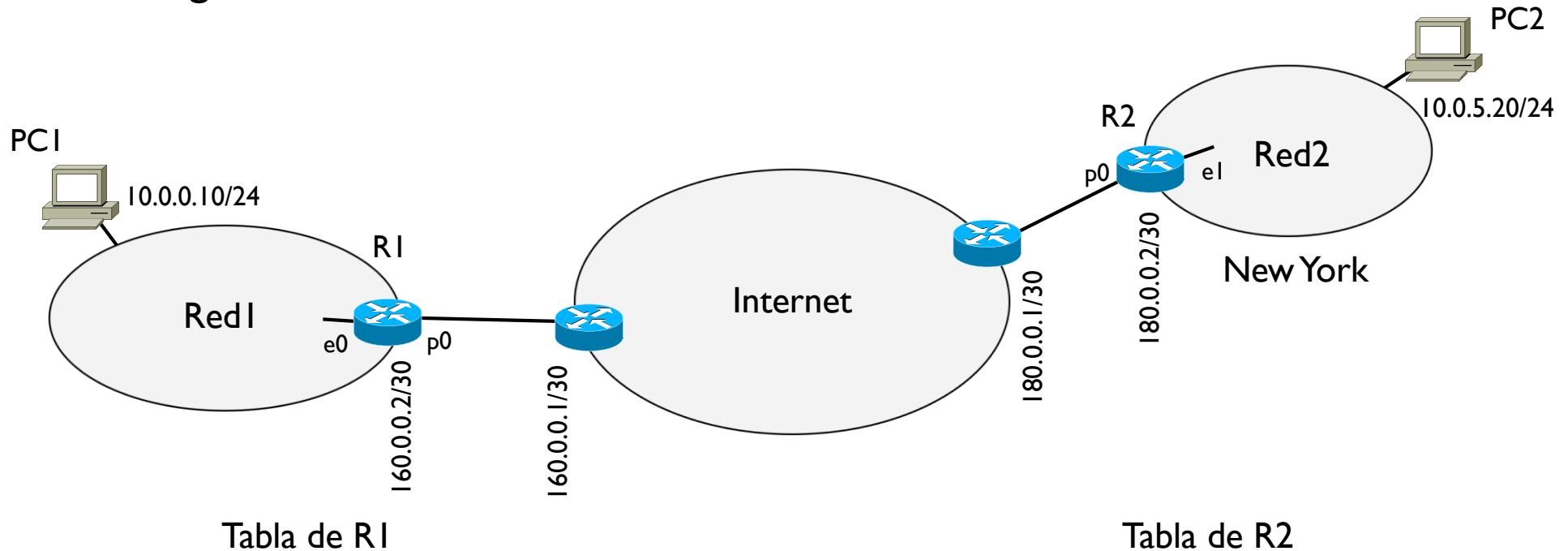


Tabla de R1

Red/mascara	gateway	interfaz
10.0.0.0/24	0.0.0.0	e0
160.0.0.0/30	0.0.0.0	p0
0.0.0.0/0	160.0.0.1	p0

Tabla de R2

Red/mascara	gateway	interfaz
10.0.5.0/24	0.0.0.0	e1
180.0.0.0/30	0.0.0.0	p0
0.0.0.0/0	160.0.0.1	p0

Tema 2 – Redes privadas virtuales

- ▶ Configuración de los routers: **con túnel**

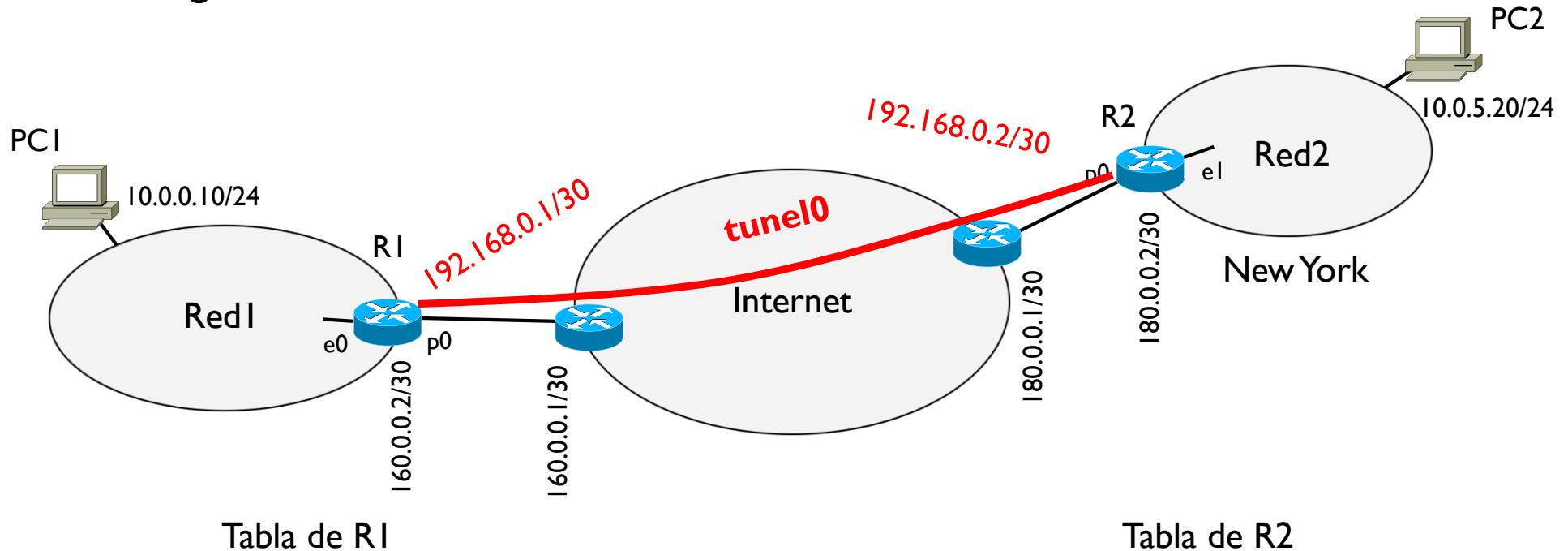


Tabla de R1

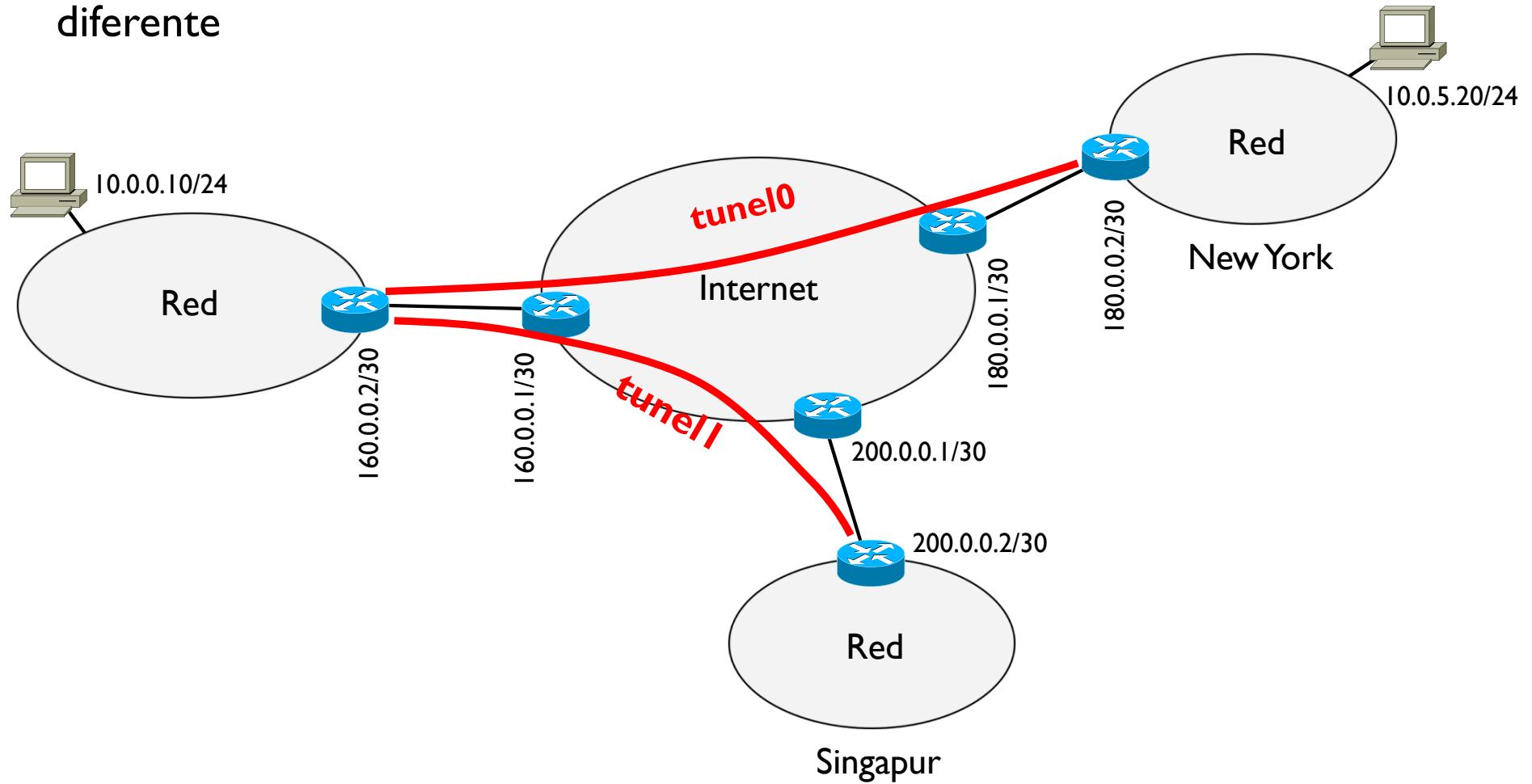
Red/mascara	gateway	interfaz
10.0.0.0/24	0.0.0.0	<code>e0</code>
160.0.0.0/30	0.0.0.0	<code>p0</code>
0.0.0.0/0	160.0.0.1	<code>p0</code>
192.168.0.0/30	0.0.0.0	tun0
10.0.5.0/24	192.168.0.2	tun0

Tabla de R2

Red/mascara	gateway	interfaz
10.0.5.0/24	0.0.0.0	<code>e1</code>
180.0.0.0/30	0.0.0.0	<code>p0</code>
0.0.0.0/0	160.0.0.1	<code>p0</code>
192.168.0.0/30	0.0.0.0	tun0
10.0.0.0/24	192.168.0.1	tun0

Tema 2 – Redes privadas virtuales

- ▶ Se pueden claramente configurar múltiples túneles, cada uno será una red diferente

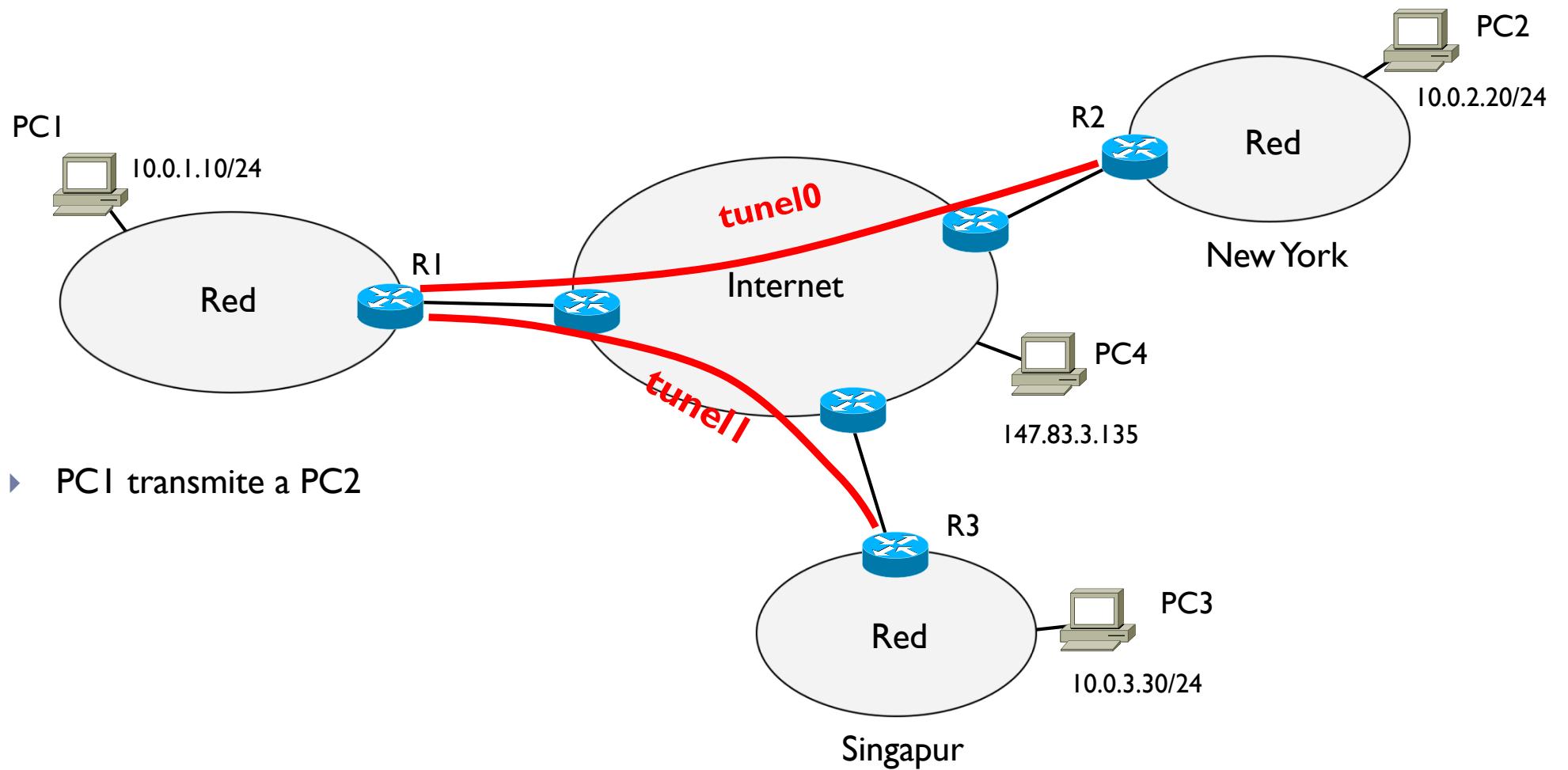


Tema 2 – Redes privadas virtuales

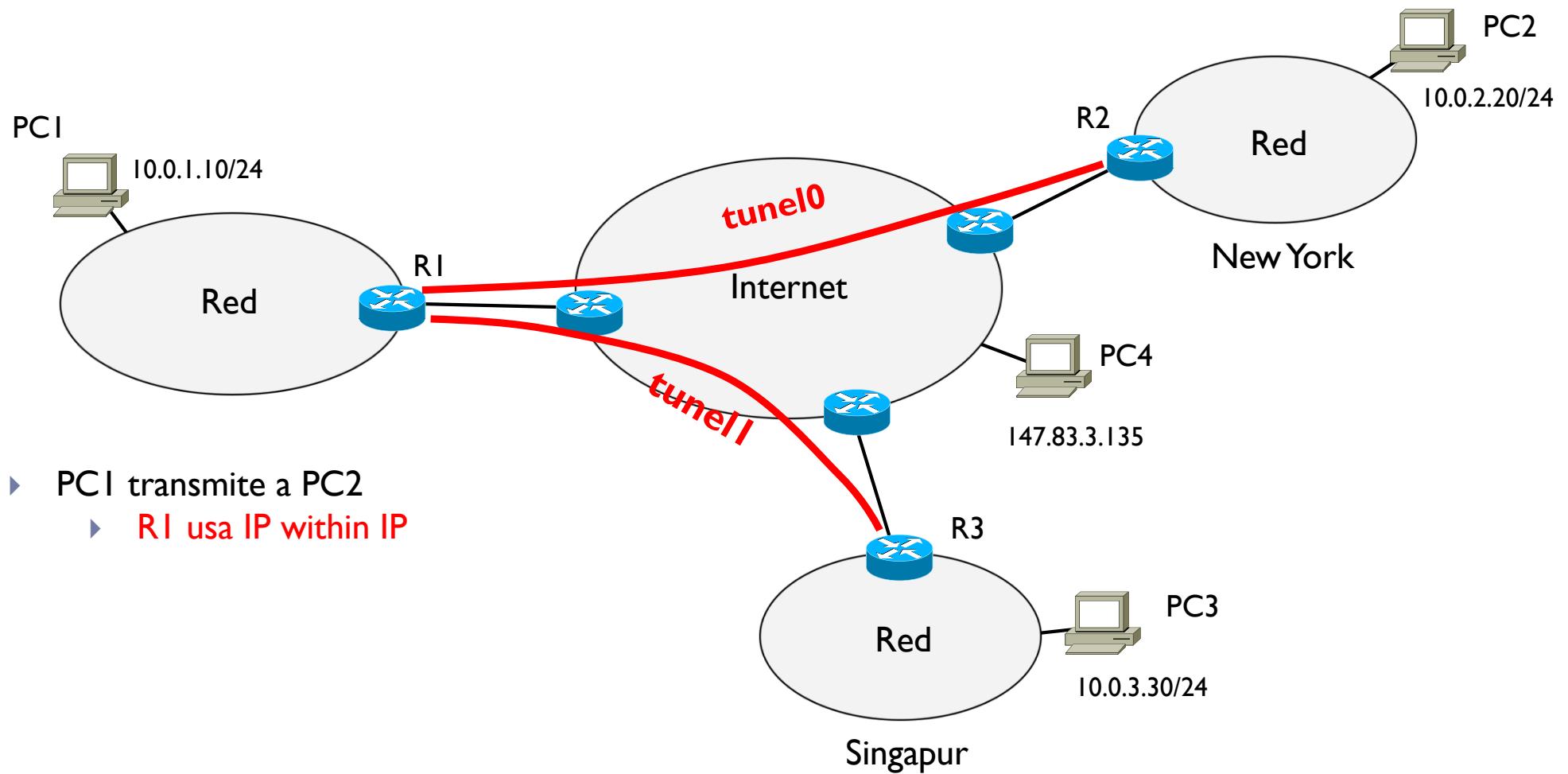
- ▶ Tipos de túneles
 - ▶ IP within IP (RFC 2003): túnel básico como hemos visto en el ejemplo
 - ▶ IPsec (RFC 2401): IP security, es como el IP within IP pero para construir el túnel los dos routers deben autenticarse y el contenido va encriptado
 - ▶ GRE (RFC 1702): Generic Routing Encapsulation, mismo concepto pero permite encapsular cualquier protocolo no solo para IP



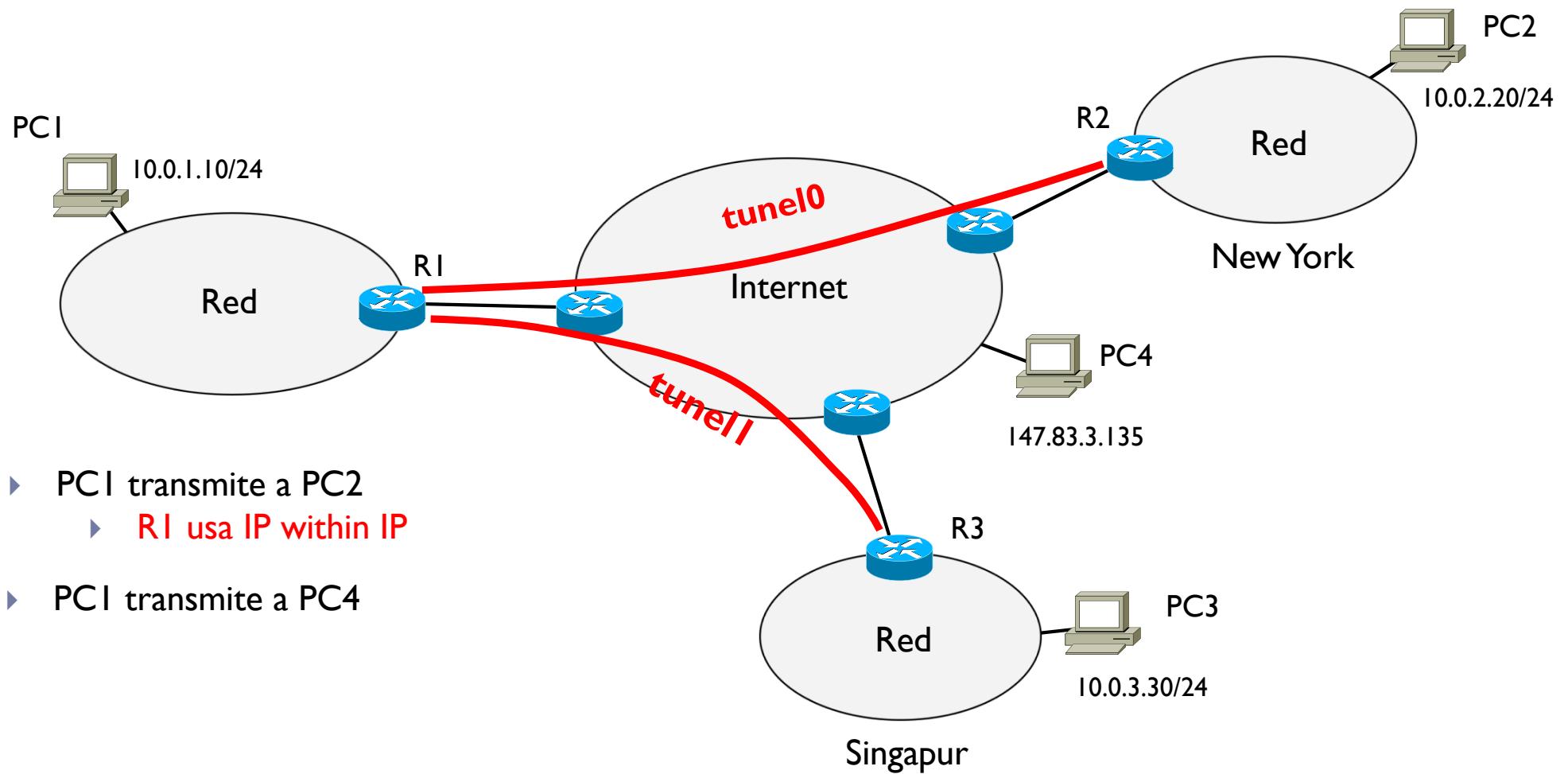
Tema 2 – Diferencia entre NAT y VPN



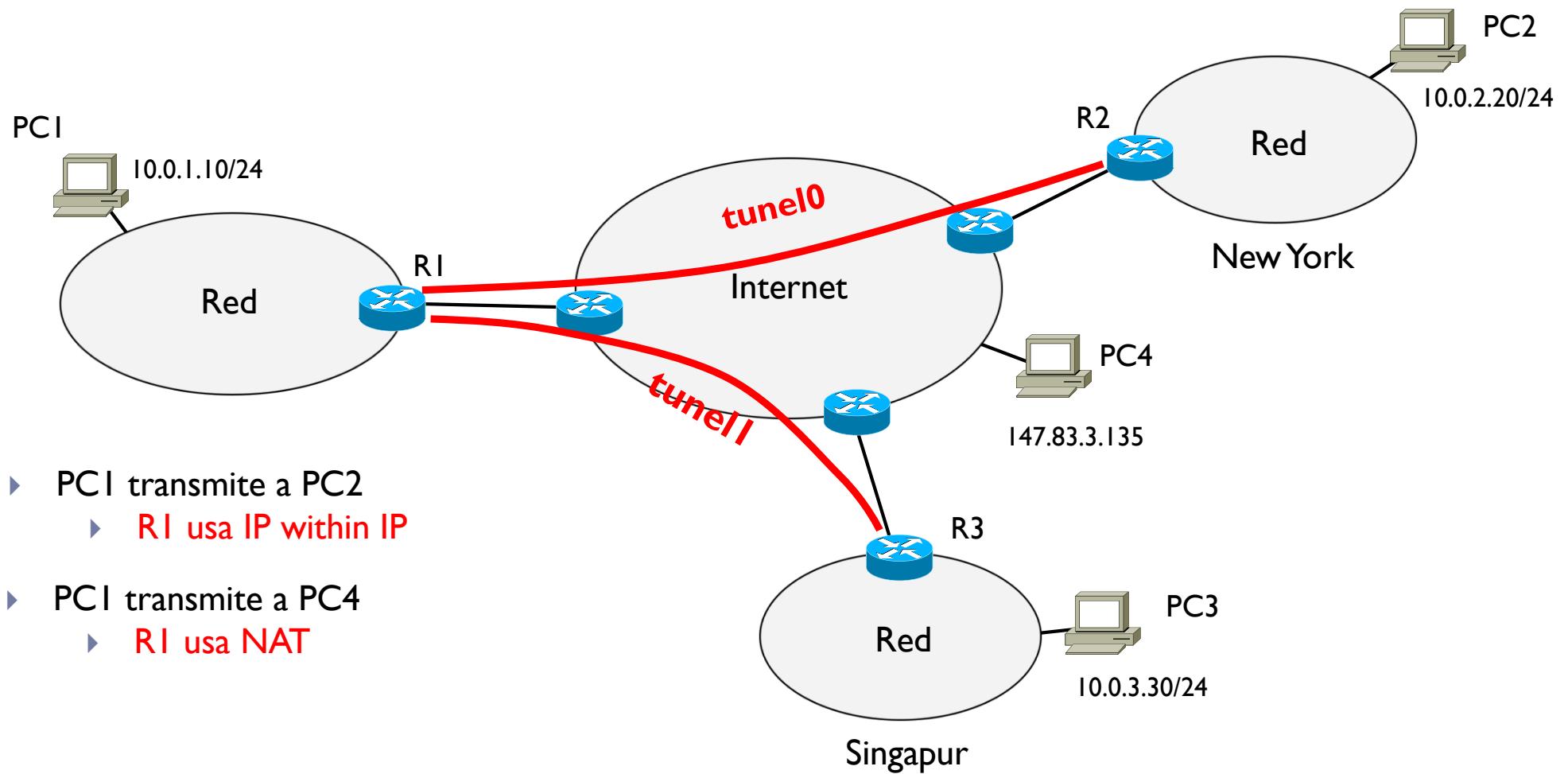
Tema 2 – Diferencia entre NAT y VPN



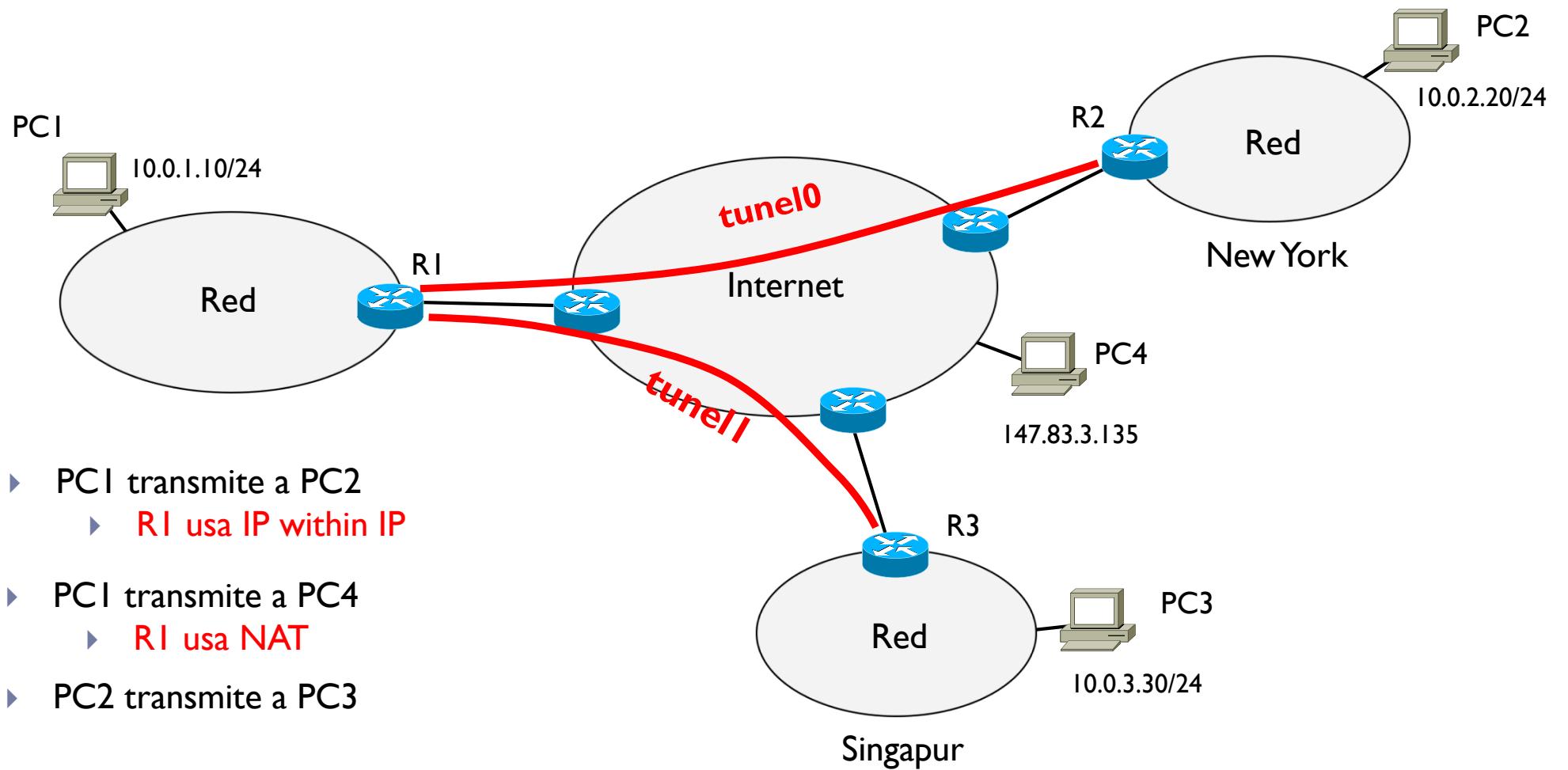
Tema 2 – Diferencia entre NAT y VPN



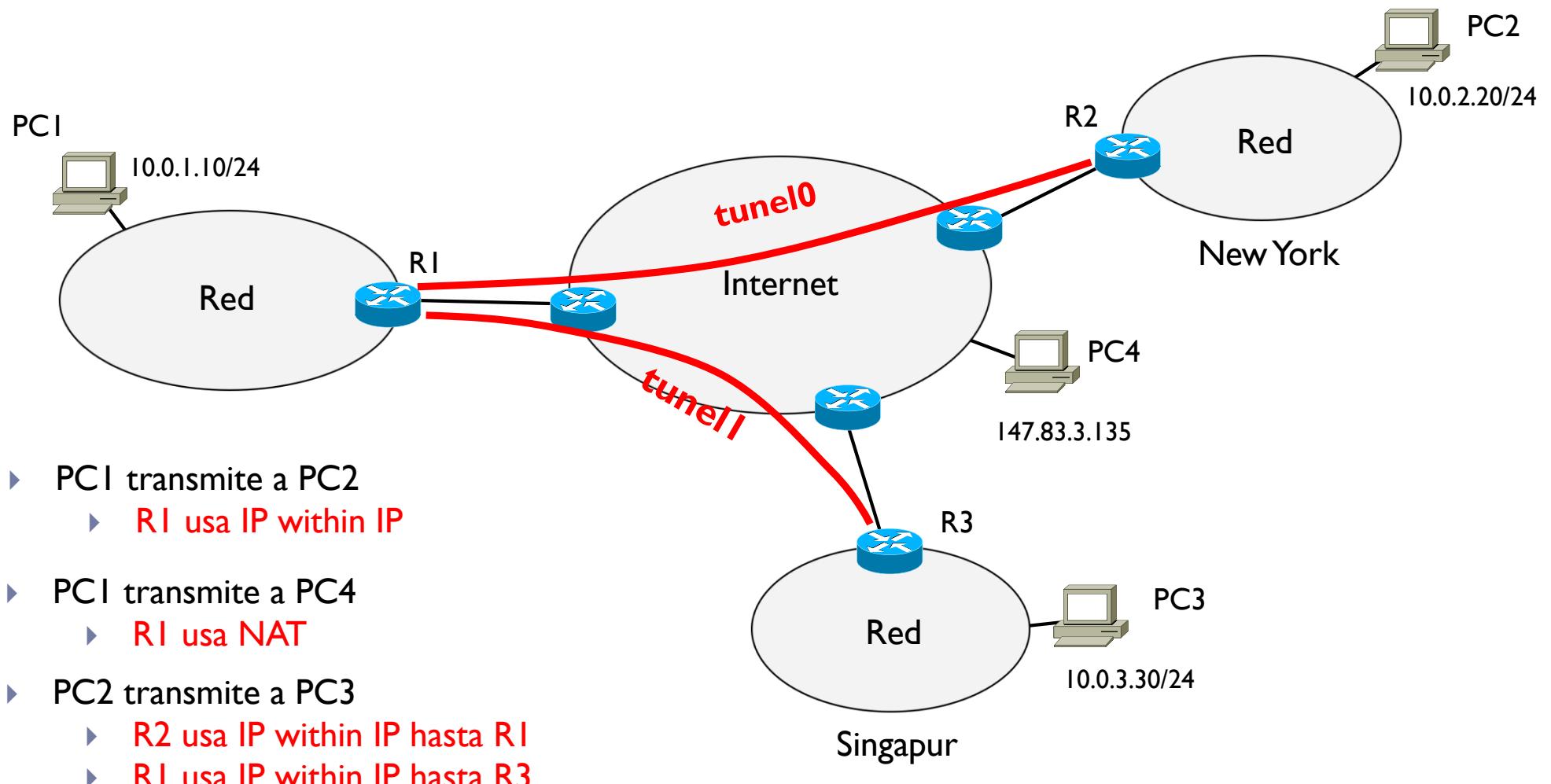
Tema 2 – Diferencia entre NAT y VPN



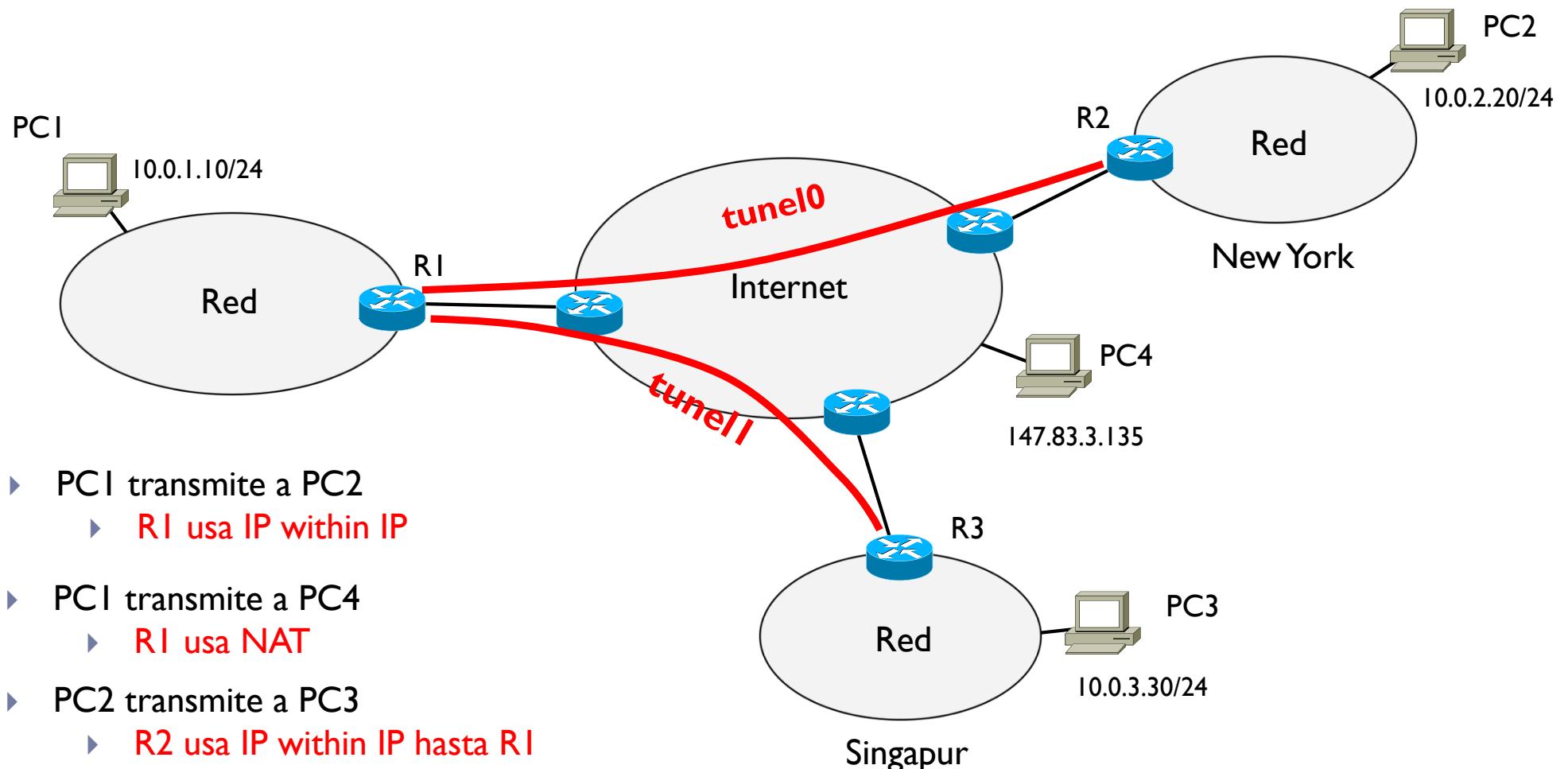
Tema 2 – Diferencia entre NAT y VPN



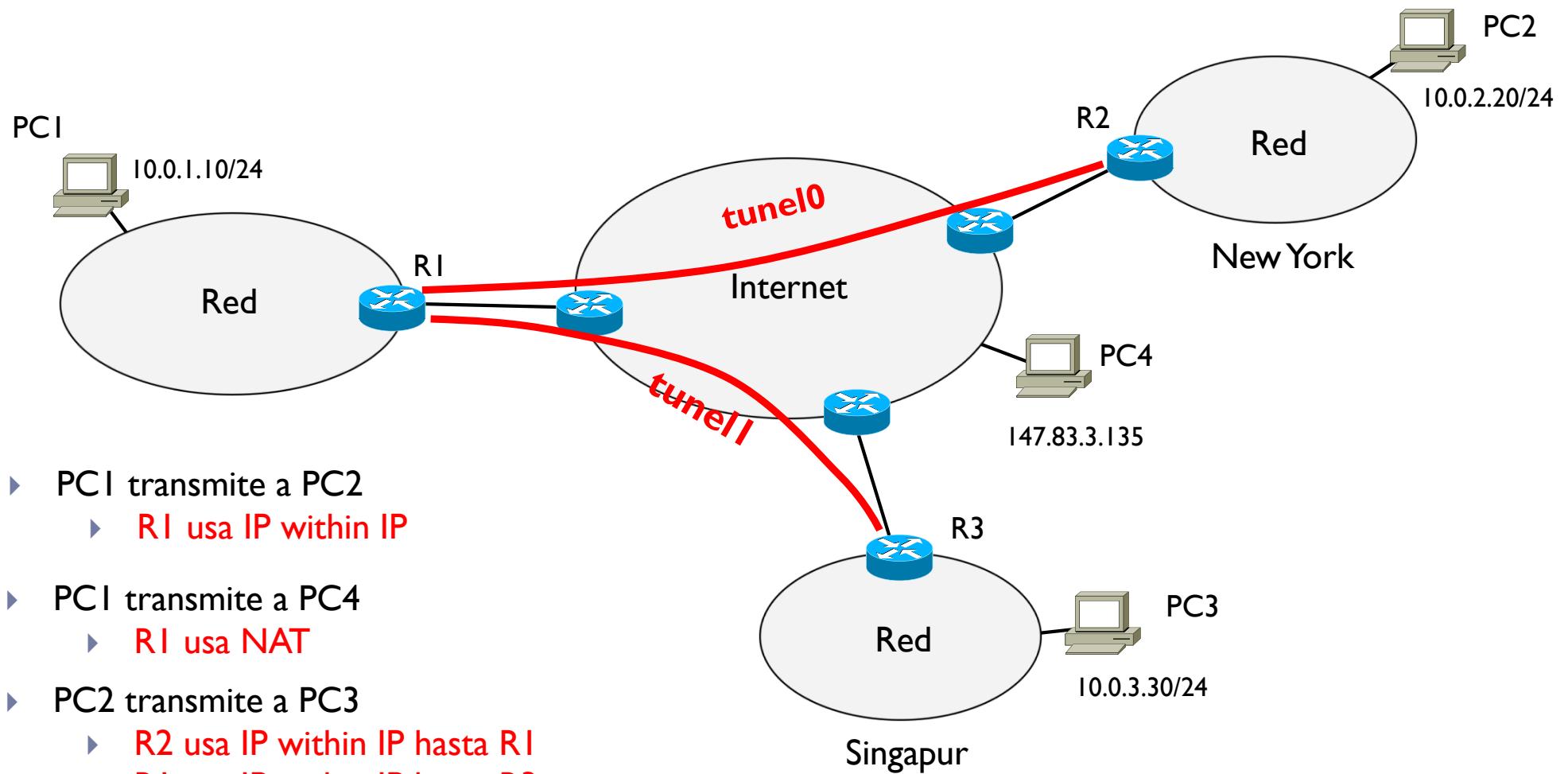
Tema 2 – Diferencia entre NAT y VPN



Tema 2 – Diferencia entre NAT y VPN



Tema 2 – Diferencia entre NAT y VPN



Xarxes de Computadors

Tema 2 - Redes IP