

Arquitectura de Redes - AdR

Tema 2: Capa de red

Iñaki G. Alonso González

Tema 2: Capa de red

Índice:

- 1. Introducción**
2. Redes orientadas a conexión. Redes no orientadas a conexión
3. Funciones de la capa de red
4. IPv4 datagrama
5. Direcciones IPv4
6. Protocolos de resolución de direcciones
7. Protocolos de gestión de red
8. Protocolos de encaminamiento
9. Movile IP
10. IPv6

T2: 2.1 Introducción

La capa de red: IP

- Es uno de los protocolos más importantes de la arquitectura TCP/IP
- Y dentro de la capa de red, es el protocolo más importante.
- Proporciona servicios a la capa de transporte.

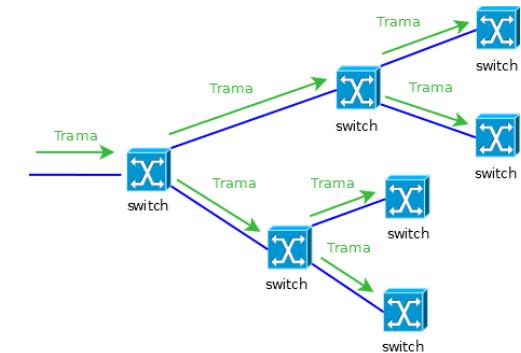
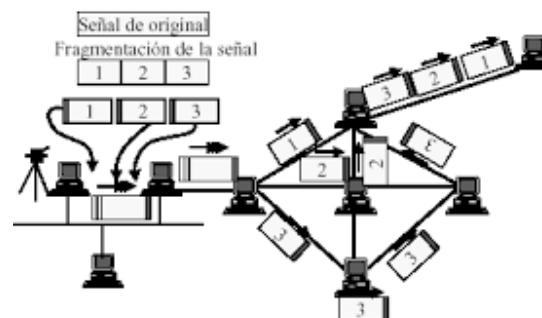
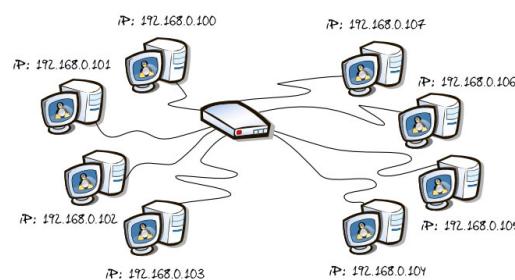
Las ideas o características del protocolo IP son:

- Direccionamiento universal: la capacidad de que los dispositivos conozcan la forma de como hacer llegar los datos de una máquina A a otra máquina B
- Independencia del protocolo de las capas inferiores: Ethernet, IEEE802.11 o sobre otros protocolos de capa de enlace.
- Un protocolo no orientado a conexión.
- Ofrece un servicio no fiable: realiza el encaminamiento sin mantener la “pista” de los paquetes que envía. No hay QoS, ni control de flujo, ni se retransmiten los paquetes perdidos.

T2: 2.1 Introducción

La capa de red: IP

Las principales funciones: direccionamiento, manejo de datagramas y encaminamiento.



Hay otros protocolos como IP NAT, IP Sec o IP Mobile, ...

[Esta foto](#) de Autor desconocido está bajo licencia [CC BY-SA-NC](#)

[Esta foto](#) de Autor desconocido está bajo licencia [CC BY-SA](#)

T2: 2.1 Introducción

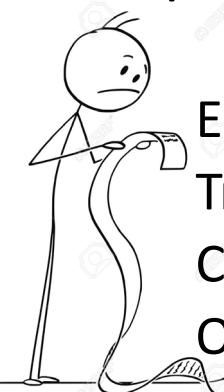
- Proporciona sus servicios a la capa de transporte.
- Direccionamiento: los dispositivos “saben” como hacer llegar los paquetes desde una máquina A, a otra B.
- Independencia de los protocolos de la capa 2.
- IP es un protocolo no orientado a conexión.
- Protocolo no fiable. IP no sigue la pista de los paquetes, de los errores. No hay retransmisión de los paquetes perdidos.
- No utiliza ACKs.



[dierstock.com](#) • 138909

T2: 2.1 Introducción

A pesar de las limitaciones de IP, los paquetes llegan la destino.



El establecimiento de conexión
Transporte de los paquetes garantizado
Comprobación de los errores
Otras funciones que dan calidad



Coste, tiempo,
recursos computacionales
ancho de banda



toerstock.com • 138909



Otras capas que realicen estas tareas

T2: 2.1 Introducción

Historia, estándares, versiones

- Las funciones que IP desempeña fueron definidas desde el nacimiento del protocolo TCP/IP y de manera formal en 1970.
- Sin embargo, es en el RFC 791 (1981) cuando el protocolo IP queda totalmente definido. Y es el protocolo que ha empleado durante más de 20 años.
- Pero no es la versión 1, sino la 4. No hubo versiones anteriores.
- IP nació cuando sus funciones fueron definidas y se separaron del protocolo de transporte TCP. TCP evolucionó en tres versiones e IP no.

T2: 2.1 Introducción

Historia, estándares, versiones

- De ahí que nace como IPv4.
- Hay una nueva versión de IP, IPv6 o *IP next generation Ipng*.
- ¿Qué pasa con la versión 5 de IP?
- Hay un protocolo experimental TCP/IP llamado *Internet Stream Protocol* (RFC 1190), se pensó que el protocolo de la capa IP sería la versión 5. De ahí el salto a la versión 6.

IP es un protocolo que hoy en día se está ejecutando en millones de máquinas y ejecutándose durante más de 20 años.

Tema 2: Capa de red

Índice:

1. Introducción
- 2. Redes orientadas a conexión. Redes no orientadas a conexión**
3. Funciones de la capa de red
4. IPv4 datagrama
5. Direcciones IPv4
6. Protocolos de resolución de direcciones
7. Protocolos de gestión de red
8. Protocolos de encaminamiento
9. Movile IP
10. IPv6

T2: 2.3 Redes orientadas a conexión. Redes no orientadas a conexión

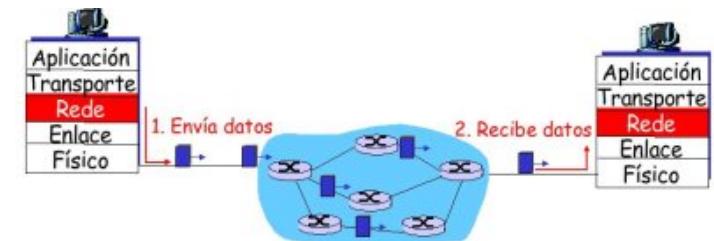
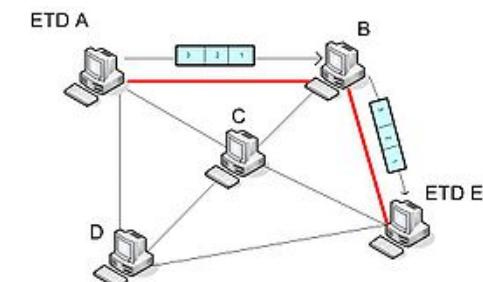
• Comutación de circuitos

- Dedicación de un circuito mientras dure la comunicación
- Los recursos son reservados antes de la comunicación.
- **Circuito virtual:** medio de transporte de datos a través de una red de paquetes de manera que parezca un enlace fijo entre la máquina origen y la máquina destino.
- Se debe establecer el camino previamente.
Hay una fase de establecimiento de la conexión.
- Los datos se entregan en orden.
- Técnicas: MDF, MDT



• Comutación de paquetes:

- En la cabecera de los paquetes hay información de la fuente y destino (direcciones IP).
- El servicio de la red es *best-effort*: Los paquetes siguen caminos distintos, se pueden perder, errores y entregados fuera de orden.



T2: 2.3 Redes orientadas a conexión. Redes no orientadas a conexión

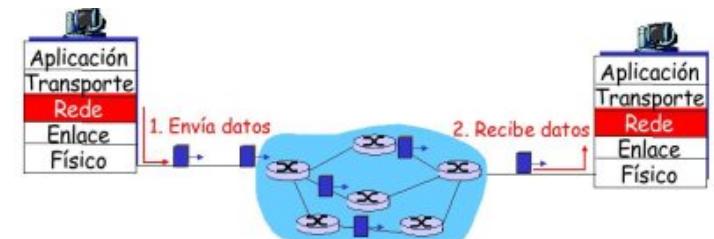
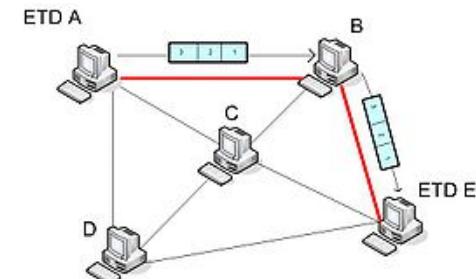
- **Protocolos orientados a conexión**

- Requieren que una conexión lógica entre dos dispositivos previa a la transferencia de datos.
 - Hay una fase de establecimiento. Se negocia entre los dos dispositivos.
 - Y una fase para finalizar la conexión.



- **Protocolos no orientados a conexión:**

- En la cabecera de los paquetes hay información de la fuente y destino (direcciones IP).
- El servicio de la red es *best-effort*: Los paquetes siguen caminos distintos, se pueden perder, errores y entregados fuera de orden.



Tema 2: Capa de red

Índice:

1. Introducción
2. Redes orientadas a conexión. Redes no orientadas a conexión
- 3. Funciones de la capa de red**
4. IPv4 datagrama
5. Direcciones IPv4
6. Protocolos de resolución de direcciones
7. Protocolos de gestión de red
8. Protocolos de encaminamiento
9. Movile IP
10. IPv6

T2: 2.3 Funciones de la capa de red

- **Funciones:** La entrega de los paquetes a través de la red
 1. **Direccionamiento.** Para hacer posible la entrega me hace falta definir un *mecanismo* para el direccionamiento de máquinas.
Cada máquina dentro de la red tiene un **dirección única**.
Las direcciones están organizadas de manera que se pueda encaminar los paquetes.
 2. **Encapsulado de los datos.** La capa IP acepta los datos de la capa de transporte los encapsula y prepara para ser transmitidos.
 3. **Fragmentación y reensamblado.** Los datagramas son pasados a la capa de enlace para ser transmitidos. El tamaño de las tramas puede variar dependiendo del protocolo de la capa de enlace.
 4. **Encaminamiento.** Cuando un paquete se envía a una máquina de la misma red es muy fácil ->*direct delivery*. Si no está en la misma red y la máquina destino está en otra red, es necesario dispositivos intermedios (**routers**) ->*indirect delivery*.

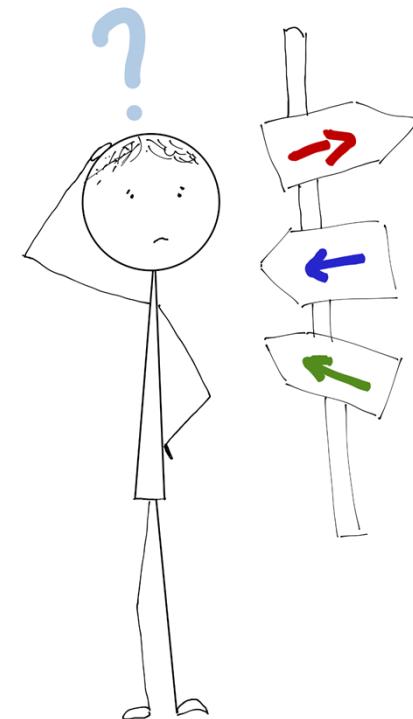
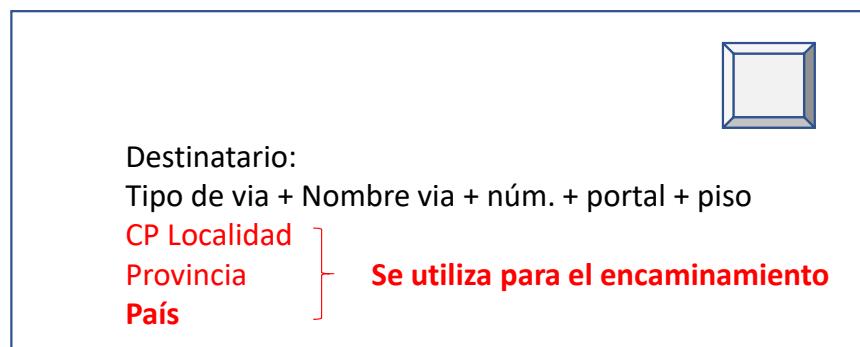
Tema 2: Capa de red

Índice:

1. Introducción
2. Redes orientadas a conexión. Redes no orientadas a conexión
3. Funciones de la capa de red
- 4. Direcciones IPv4**
5. IPv4 datagrama
6. Protocolos de resolución de direcciones
7. Protocolos de gestión de red
8. Protocolos de encaminamiento
9. Móvil IP
10. IPv6

T2: 2.4 Direcciones IPv4

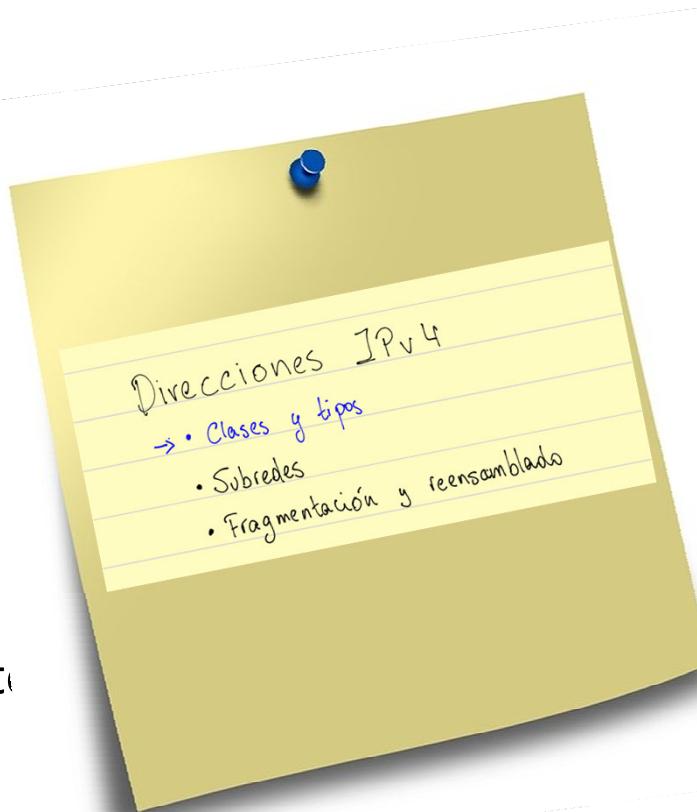
- El esquema de direcciones IP es relativamente simple aunque en los últimos tiempos aparecen conceptos como el **subnetting** que puede parecer un poco más complicado.
- Las direcciones IP tienen dos funciones:
 - **Identificación de la red**
 - **Encaminamiento (*Routing*)**



Tema 2: Capa de red

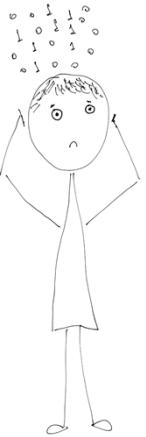
Índice:

1. Introducción
2. Redes orientadas a conexión
3. Funciones de la capa de red
4. IPv4 datagrama
- 5. Direcciones IPv4**
6. Protocolos de resolución de dominio
7. Protocolos de gestión de red
8. Protocolos de encaminamiento
9. Móvil IP
10. IPv6



T2: 2.4 Direcciones IPv4

- Las direcciones IP tienen 32 bits $\rightarrow 2^{32} = 4.294.967.296$ direcciones posibles
 - 32 bits de ceros y unos
 $8 \text{ bits. } 8 \text{ bits. } 8 \text{ bits. } 8 \text{ bits} = 2^8 \cdot 2^8 \cdot 2^8 \cdot 2^8 = 0\text{-}255. 0\text{-}255. 0\text{-}255. 0\text{-}255$



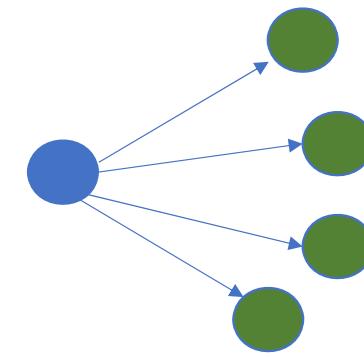
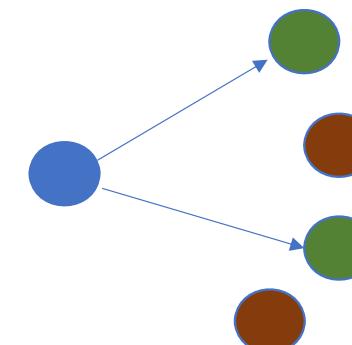
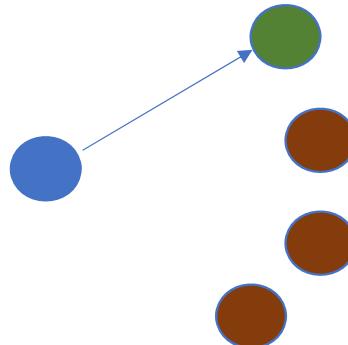
- Las direcciones MAC (48 bits) tienen una notación hexadecimal:

E352: 9DB2: F85C:1234

- En un principio el número de bits (espacio) de las direcciones IP se pensó que era lo suficiente amplio para cubrir las necesidades que incluso se reservaron direcciones IP para funciones determinadas como las que empiezan por 127.
 - **IANA** (Internet Assigned Number Authority) primera organización en gestionar las direcciones IP.
 - A finales de los 1990 aparece **ICANN** (Internet Corporation for Assigned Names and Numbers: supervisa a IANA como el registro de nombre DNS).
 - **RIRs** (Regional Internet Registries). IANA delega la asignación de direcciones IP.

T2: 2.4 Direcciones IPv4

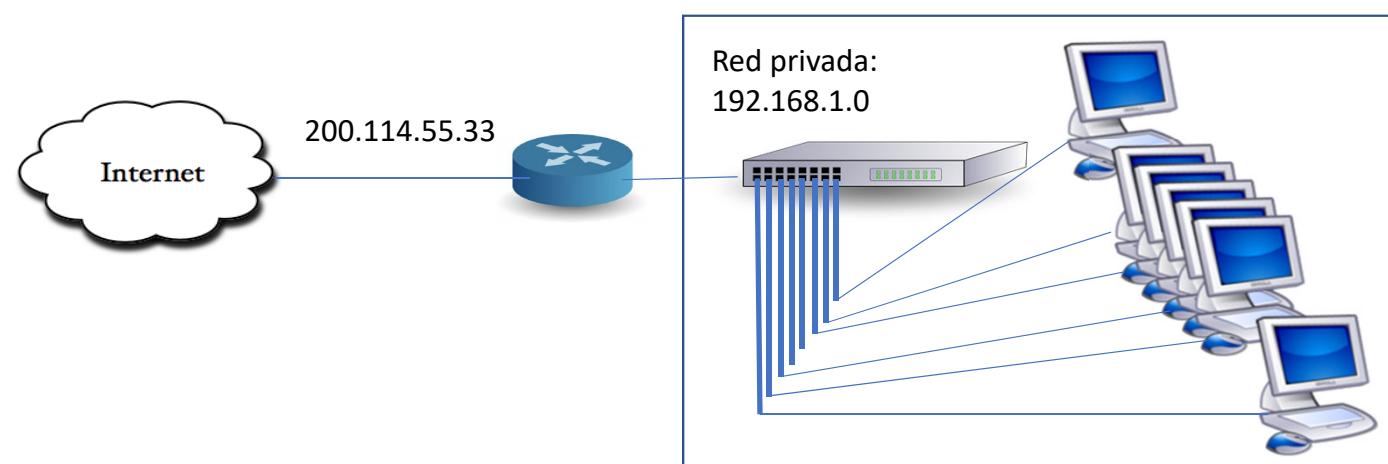
- Hay dos formas de configurar las direcciones IP:
 - Estática: son direcciones que se fijan manualmente y no cambian.
 - Dinámica: Hay un software o un servicio (DHCP o BOOTP) que asigna las direcciones a los distintos ordenadores o dispositivos que se conecten a la red.
- Tipos de direccionamiento:
 - Unicast: los mensajes son enviados de dispositivos a dispositivos.
 - Multicast: los mensajes son enviados a un grupo de dispositivos bajo algún criterio.
 - Broadcast: mensajes enviados a todos los dispositivos de la red.



T2: 2.4 Direcciones IPv4

- Hay dos tipos de direcciones IP:

- Pública:
 - Son direcciones conectadas directamente a Internet.
 - Son únicas e irrepetibles.
 - Ejemplos: servidores web o routers
- Privada: un organismo o empresa controla las direcciones que asigna a sus dispositivos.



Fotos de Autor desconocido bajo licencias y/o CC BY-SA-NC

T2: 2.4 Direcciones IPv4

- Las direcciones IP identifican **interfaces de red** y no dispositivos.
- Los routers tienen más de un interfaz de red y algunos equipos también (concepto de ***multihomed***).



- Por tanto cada interfaz de red tiene su dirección IP y es única.
- Los dispositivos que trabajan a nivel de las capas inferiores (física y de enlace) como switches, repetidores, *bridges* no tienen una dirección IP. Para la capa de red estos dispositivos son invisibles. De tener una dirección IP son para funcionalidades de gestión. En estos niveles se trabaja con la dirección MAC.



T2: 2.4 Direcciones IPv4

Categorías de esquemas de direccionamiento IP

- Direccionamiento *classful* (Convencional). En este esquema hay diferentes clases de direcciones IP: clase A, clase B, clase C, clases D y clase E.
- Subnetting: se utiliza parte de los bits destinados al **id. de host** como un identificador de subred.
 - El identificador de red no cambia.
 - Para identificar la línea que divide el **id. de subred** y el **id. de host** se utiliza un identificador de 32 bits llamado máscara. La submáscara tiene **el id. de red** y el **id. de subred** a “1” y el **id. de host** a “0”. Ejemplo: 255.255.255.224 ó 255.255.255.0
- Direccionamiento *classless*: la división entre el id. de red y el id. de host puede ser en cualquier punto. Para conocer el punto de la división se añade el número de bits utilizados como id. de red después de la dirección. Se le conoce como prefijo. Ejemplo: 227.82.157.160/**27**

Debido a las necesidades de optimizar el uso de las direcciones IP apareció esta técnica: *subnetting (CIDR)* y *network address translation (NAT)*.

Estas técnicas se diseñaron para un uso eficiente del espacio de direcciones IPv4.

Otra solución es el uso de IPv6, que expande el espacio de direcciones a 128 bits.

T2: 2.4 Direcciones IPv4

Esquema *classful* o por clases

Las direcciones IP tienen una estructura interna de dos componentes:

32 bits	
Bits identificador de red	Bits Identificador de máquina

- **Identificador de red:** de los 32 bits se asignan unos bits para identificar a la red.
- **Identificador de máquina:** el resto para identificar a las máquinas dentro de una red.
- Recuerda al concepto de número de teléfono: prefijo + usuario

928 555555

91 5555555

T2: 2.4 Direcciones IPv4

Esquema *classful* o por clases

Clase	Primer octecto	Rango de valores bits Primer octecto		Rango decimal 1 ^{er} octeto	Bytes Id.Red/ Id.Host	Rango decimal 4 octetos	Usos
A	0xxxxxxxx	00000001 $2^0 = 1$	01111110 $2^6+2^5+2^4+2^3+2^2+2^1+2^0 = 126$ $64+32+16+8+4+2=126$	1 a 126	1/3	1.0.0.0 a 126.255.255.255	Unicast Redes con millones de hosts
B	10xxxxxxxx	10000000 $2^7 = 128$ 128	10111111 $2^7+2^5+2^4+2^3+2^2+2^1+2^0 = 191$ 128+32+16+8+4+2+1=191	128 a 191	2/2	128.0.0.0 a 191.255.255.255	Unicast Redes de cientos a miles hosts
C	110xxxxx	11000000 $2^7+2^6 = 192$ 128+64=192	11011111 $2^7+2^6+2^4+2^3+2^2+2^1+2^0 = 223$ 128+64+16+8+4+2+1=223	192 a 223	3/1	192.0.0.0 a 223.255.255.255	Unicast 250 hosts
D	1110xxxx	11100000	11101111	224 a 239	--	224.0.0.0 a 239.255.255.255	IP multicasting
E	1111xxxx	11110000	11111111	240 a 255	--	240.0.0.0 a 255.255.255.255	Experimental uso

T2: 2.4 Direcciones IPv4

Direccionamiento *su Esquema classful o por clases*



¿Cómo sería el algoritmo que tendrían los routers para saber las clases de las direcciones IP de los paquetes que le llegan?

Ventajas:

- **Simplicidad y claridad.** Las divisiones entre los identificadores de red y máquinas están definidos.
- **Flexibilidad.** Tiene tres niveles de implementación para grandes, medianas y pequeñas organizaciones/empresas.
- **Fácil encaminamiento.** Los routers conocen fácilmente el id. de la red.
- **Direcciones reservadas.** El esquema contempla direcciones reservadas para uso especial o privado.

T2: 2.4 Direcciones IPv4

Esquema *classful* o por clases

- **Ventajas:**

- **Simplicidad y claridad.** Las divisiones entre los identificadores de red y máquinas están definidos.
- **Flexibilidad.** Tiene tres niveles de implementación para grandes, medianas y pequeñas organizaciones/empresas.
- **Fácil encaminamiento.** Los routers conocen fácilmente el id. de la red.
- **Direcciones reservadas.** El esquema contempla direcciones reservadas para uso especial o privado.

- **Desventajas:**

- **Ineficiencia** en cuanto al uso del espacio de direcciones.
- **Tablas de enrutamiento grandes.**
- A las grandes organizaciones se les asigna un bloque de direcciones que luego no se ajusta a su estructura interna.

T2: 2.4 Direcciones IPv4

Esquema *subnetting*

- Requiere de cierta familiaridad con los números binarios y operaciones booleanas como AND, y el concepto de máscara.
- El esquema de *classes* no siempre se ajusta a las necesidades de las empresas u organismos.
- RFC 950 (1985): *subnet addressing or subnetting*.
 - Añadir un nivel jerárquico más a las direcciones IP.
 - La parte de la red (**id. de red**) queda igual, pero la parte **id. de host** se divide en dos: **id. de subred + id. de hosts**.
 - Cada subred se comporta como una red.
- Introduciendo este nivel permite a las organizaciones una mejor gestión de las redes y adaptación a la estructura interna.
- Se introduce el concepto de máscara de subred.

T2: 2.4 Direcciones IPv4

Esquema *subnetting*

- Esta **máscara de subred** (32 bits) permite conocer cual es el **id. de subred** y cual es **id. de hosts**. Permite a los routers el encaminamiento por las subredes.
- Ejemplo:

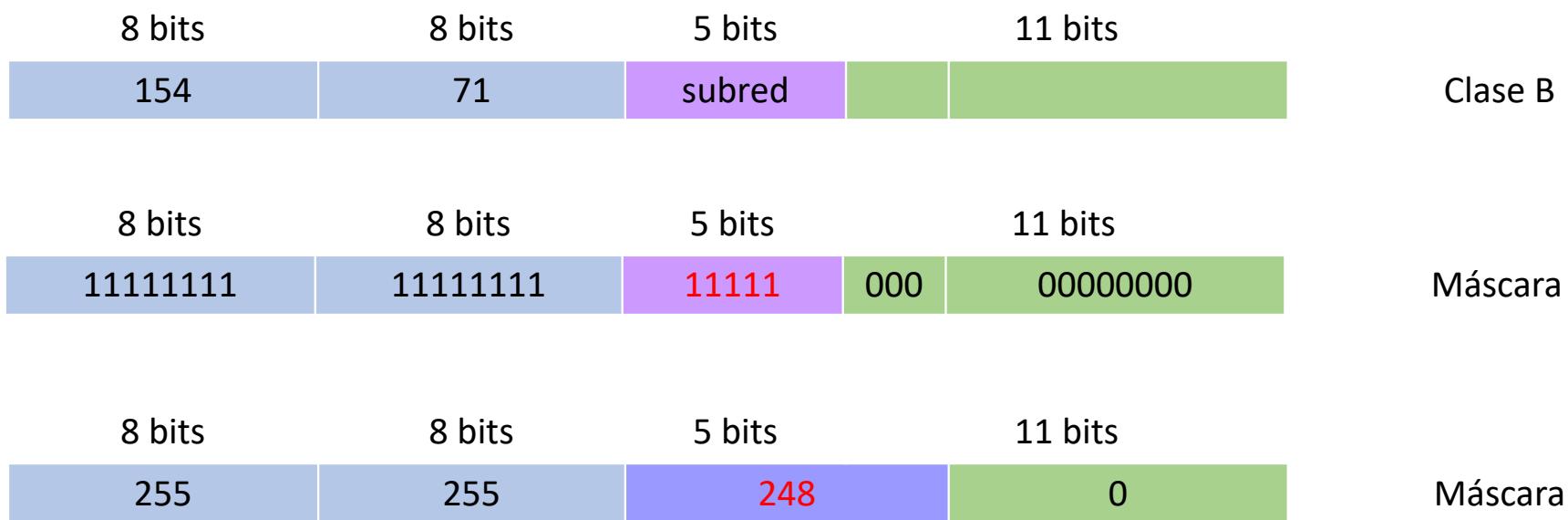


- Se realiza la operación AND con la dirección IP y la máscara

T2: 2.4 Direcciones IPv4

Esquema *subnetting*

- Ejemplo:



- Se realiza la operación AND con la dirección IP y la máscara

T2: 2.4 Direcciones IPv4

Esquema *subnetting*

- Se realiza la operación AND con la dirección IP y la máscara

8 bits	8 bits	5 bits	11 bits	
10011010 154	01000111 71	10010110 150	00101010 42	Dirección IP
AND				
8 bits	8 bits	5 bits	11 bits	
11111111	11111111	11111	000	00000000
Máscara				
8 bits	8 bits	5 bits	11 bits	
10011010 154	01000111 71	10010 000 144	0000000 0	Resultado IP de la subred

T2: 2.4 Direcciones IPv4

Esquema *subnetting*

- **Ventajas**

- **Mejor ajuste** a la estructura interna de la empresa/organización.
- **Flexibilidad:** el número de subredes y hosts por subred son planificadas según la estructura de la empresa.
- **Invisibilidad a Internet:** la organización interna de las subredes solo es vista por la propia organización. Cualquier cambio dentro de las subredes no es visto por el exterior.
- **No se requiere solicitar nuevas direcciones IP.** Si se añade nuevas máquinas o hosts, se dan de alta dentro de las subredes y no en las direcciones públicas.
- **Las tablas de enrutamiento de Internet** se restringe al **id. de red**. Los cambios dentro de la organización afectan únicamente a los **routers** internos a la organización.

T2: 2.4 Direcciones IPv4

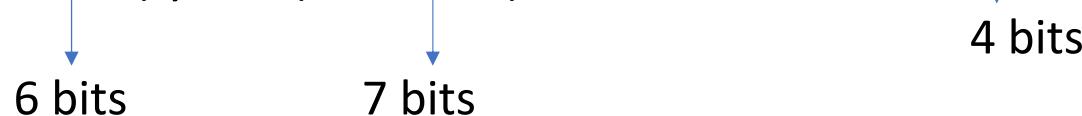
Esquema *subnetting*

- **Desventajas**

- La principal debilidad es que el subnetting introduce un único nivel jerárquico.
- Esquema ineficiente si hay diferencias en cuanto al número de hosts en las subredes. El **id. de subred** se elige en función de la subred de mayor número de hosts.

Ejemplo: 201.45.222.0/24 (Clase C) **11001001.00101101.11011110.00000000**

Se desea definir 6 subredes: SR1 (10 hosts), SR2 (10 hosts), SR3 (10 hosts), SR4 (10 hosts)
SR5 (50 hosts) y SR6 (100 hosts)



Para definir las subredes necesitamos 3 bits:

201.45.222.0/27 (Clase C) **11001001.00101101.11011110.00000000**

Con 5 bits: $2^5 - 1 = 31 - 2$ (subred y máscara) = 29 direcciones IPs para hosts

T2: 2.4 Direcciones IPv4

Esquema *subnetting*:

Solución: *Variable Length Subnet Masking (VLSM)*

- La idea es aplicar subred de subredes, es decir crear subredes a partir de subredes, tantas veces como sea necesario.
 - Se adapta a las necesidades de tener subredes de distinto tamaño.
 - Las subredes se despliegan en niveles jerárquicos y así conseguir redes de distinto número de hosts.
 - Cada “subred(subred)” tendrá su propia máscara y será diferente según la subred en la que se encuentre la máquina.
-
- <https://es.slideshare.net/pcolomes/vlsm-paulo-coloms-autoguardado>

T2: 2.4 Direcciones IPv4

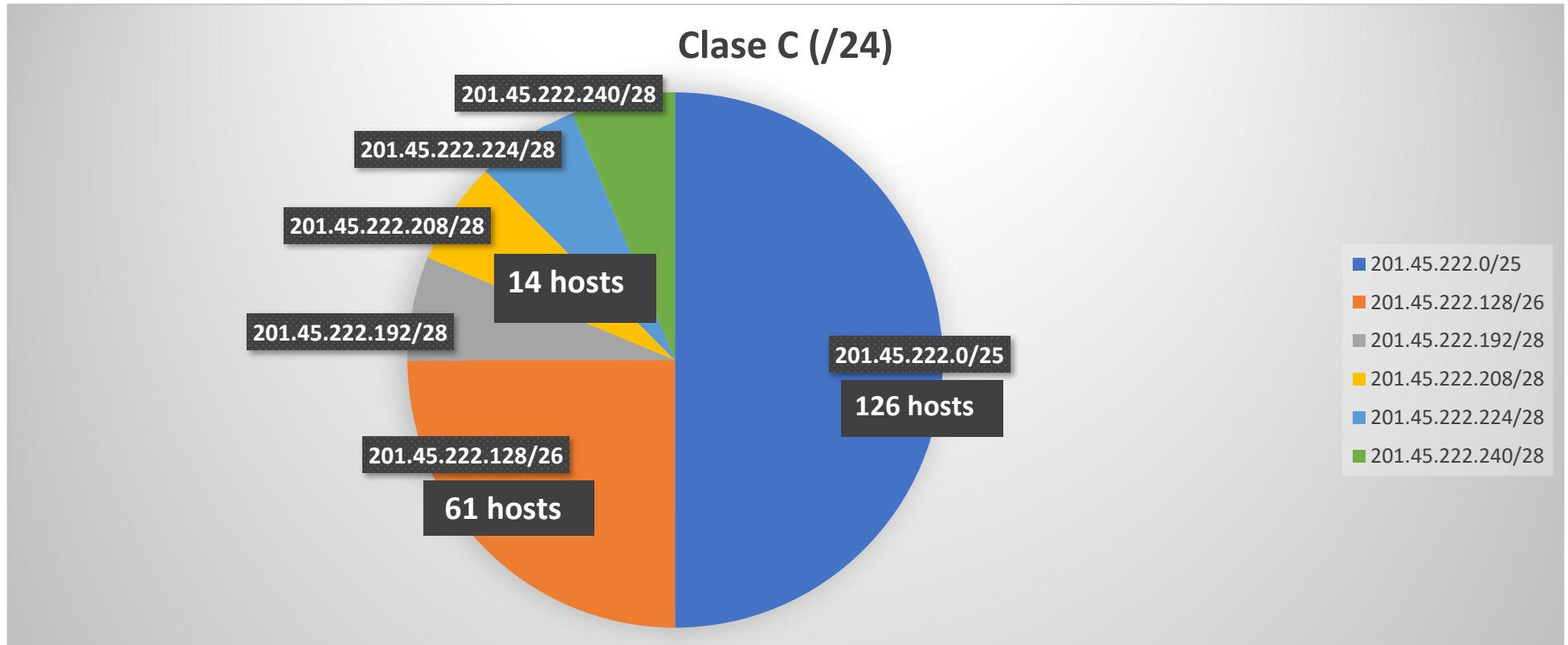
Ejemplo VLSM

- Dirección IP: 201.45.222.0/24 , (Clase C)

201	45	222	0			$2^8 - 2 = 254 \text{ hosts}$
11001001	00101101	11011110	00000000			
11111111	11111111	11011110	0	0000000		$2^7 - 2 = 126 \text{ hosts}$
11111111	11111111	11011110	1	0000000		201.45.222.0/25
11111111	11111111	11011110	1	0000000		201.45.222.128/25
11111111	11111111	11011110	1	0	000000	$2^6 - 2 = 62 \text{ hosts}$
11111111	11111111	11011110	1	1	000000	201.45.222.128/26
11111111	11111111	11011110	1	1	000000	201.45.222.192/26
11111111	11111111	11011110	1	1	0000	$2^4 - 2 = 14 \text{ hosts}$
11111111	11111111	11011110	1	1	0000	201.45.222.192/28
11111111	11111111	11011110	1	1	0100	201.45.222.208/28
11111111	11111111	11011110	1	1	1000	201.45.222.224/28
11111111	11111111	11011110	1	1	1100	201.45.222.240/28

T2: 2.4 Direcciones IPv4

Ejemplo VLSM



T2: 2.4 Direcciones IPv4

Esquema *Classless Inter-Domain Routing (CIDR)*

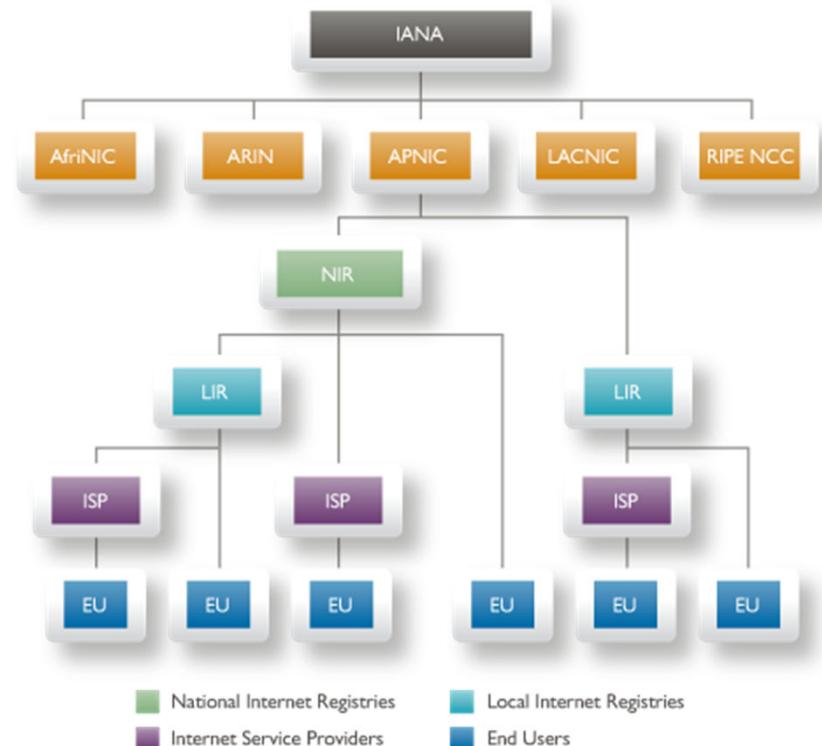
- El direccionamiento *subnetting* fue un importante evolución dentro del esquema de direccionamiento pero no suficiente.
- Este esquema es una aplicación del concepto VLSM a Internet, no a una red.
- Por su propio nombre, se eliminan las clases. No hay direcciones de clase A, B y C.
- CIDR también utiliza el concepto de máscara de subred, para indicar cuál es el **id.red**.
- La anotación de este esquema es con la representación “/[número de bits del id.red]”
- Ejemplo: 184.13.152.0/22

184	13	152	0		
10111000	00001101	100110	00	00000000	$2^{10}-2= 1022$ hosts
11111111	11111111	111111	00	00000000	Mask: 255.255.252.0

T2: 2.4 Direcciones IPv4

Esquema *Classless Inter-Domain Routing* (*CIDR*)

- En este esquema hay muchos niveles de jerárquicos. Se pueden dividir grandes bloques.
- IANA/ICANN divide direcciones en grandes bloques que luego distribuye a las 4 RIR (*regional Internet registries*): **APNIC** (*Asia y Pacífico*), **ARIN** (*América del Norte, Atlántico*), **LACNIC** (*América Latina y Caribe*) y **RIPE NCC** (*Europa*). Y estos a su vez se distribuyen a national Internet registries (NIRs), local Internet registries (LIRs) y/o a organizaciones proveedoras del servicio como los Internet service providers (ISPs)

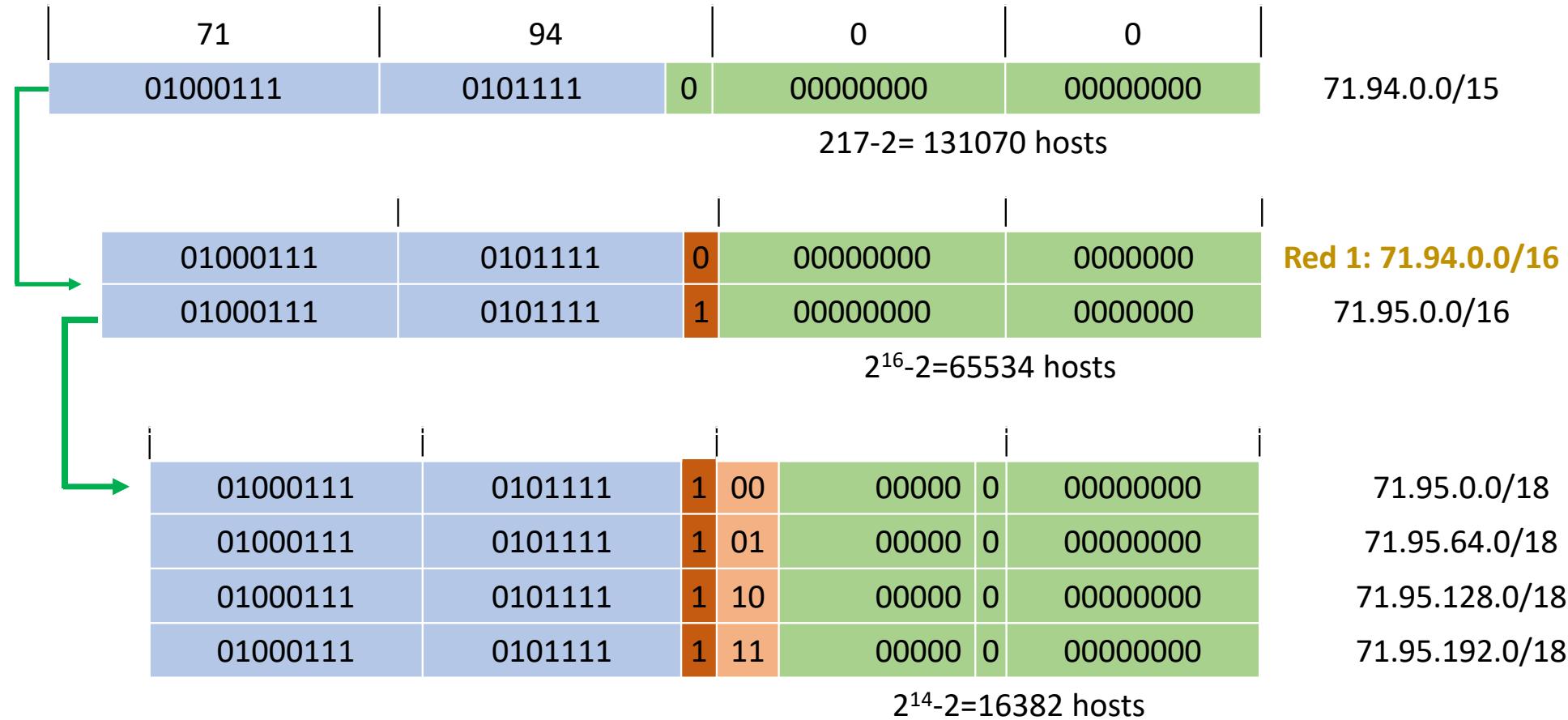


Fuente: <https://www.apnic.net/manage-ip/manage-resources/address-management-objectives/management-hierarchy/>

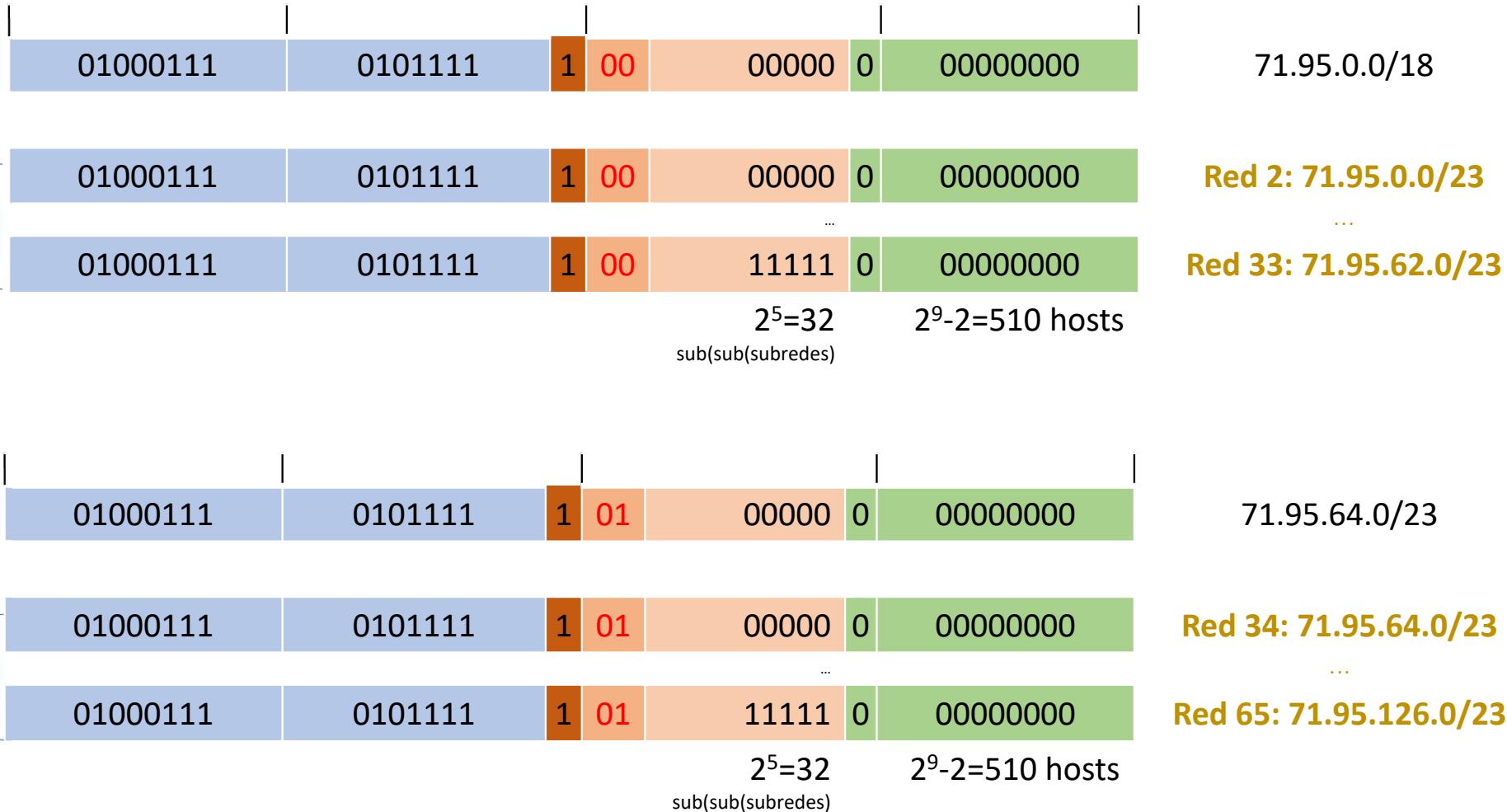
T2: 2.4 Direcciones IPv4

Ejemplo CIDR

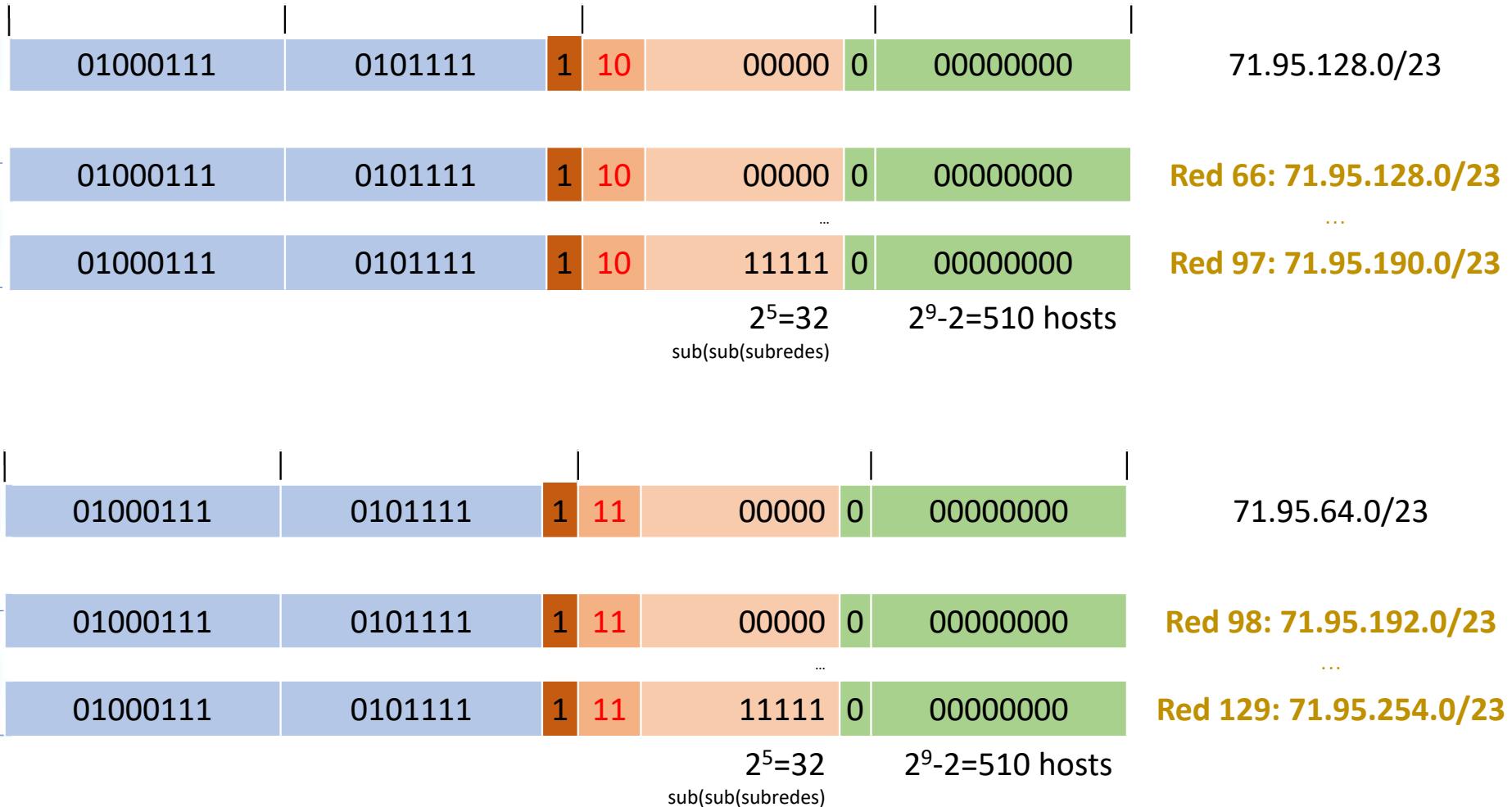
- Dirección IP: 71.94.0.0/15



T2: 2.4 Direcciones IPv4

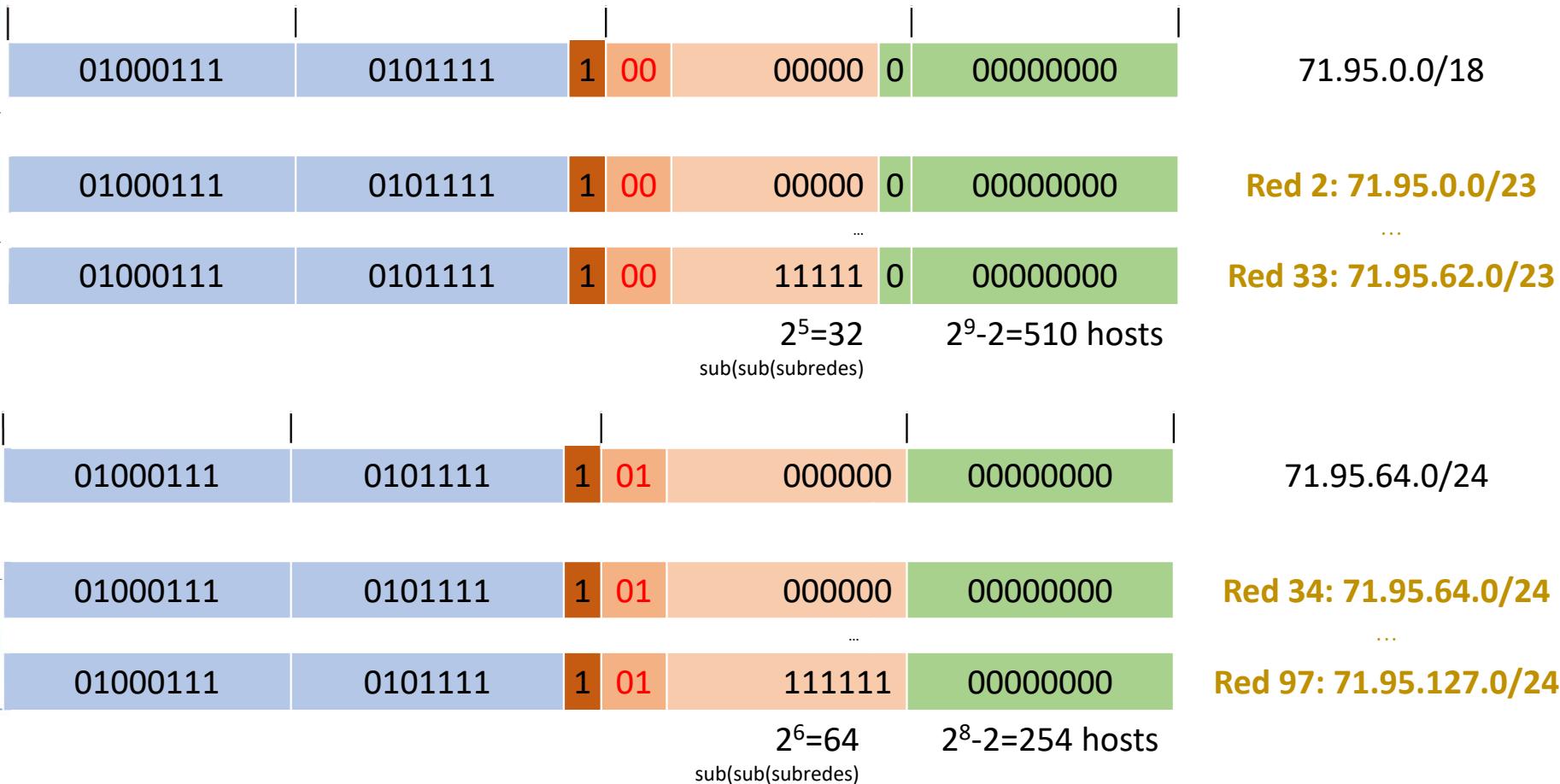


T2: 2.4 Direcciones IPv4



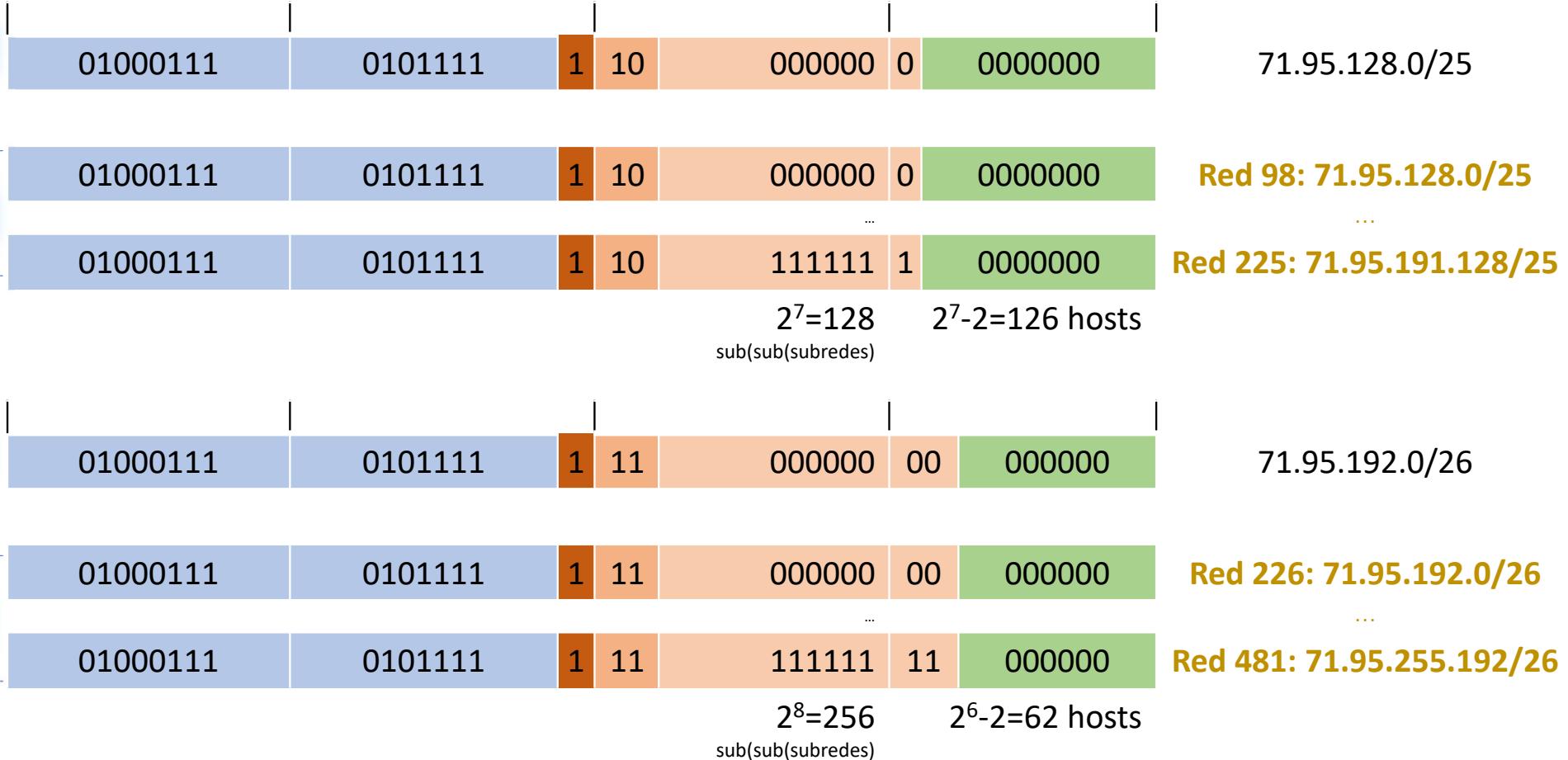
T2: 2.4 Direcciones IPv4

Otra posibilidad



T2: 2.4 Direcciones IPv4

Otra posibilidad



T2: 2.4 Direcciones IPv4

Direcciones reservadas

Rango de Direcciones		Clase	“Classless”	Usos
0.0.0	0.255.255.255	Clase A: 0.x.x.x	0/8	Reservada
10.0.0.0	10.255.255.255	Clase A: 10.x.x.x	10/8	Reservada: redes privadas
127.0.0.0	127.255.255.255	Clase A: 127.x.x.x	127/8	Direcciones de bucle
128.0.0.0	128.0.255.255	Clase B: 128.0.x.x	128.0/16	Reservada
169.254.0.0	169.254.255.255	Clase B: 169.254.x.x	169.254/16	Reservada
172.16.0.0	172.31.255.255	16 redes de Clase B: 172.16.x.x a 172.31.x.x <small>10101100.00010000.X.X a 10101100.00011111.X.X</small>	172.16/12	Reservada: redes privadas
191.255.0.0	191.255.255.255	Clase B: 191.255.x.x	191.255/16	Reservada
192.0.0.0	192.0.0.255	Clase C: 192.0.0.x	192.0.0/24	Reservada
192.168.0.0	192.168.255.255	256 redes de Clase C: 192.168.0.x a 192.168.255.x	192.168/16	Reservada: redes privadas
223.255.255.0	223.255.255.255	Clase C: 223.255.255.x	223.255.255/24	Reservada

T2: 2.3 Funciones de la capa de red

Estructura de las direcciones IP

- El encaminamiento se hace a partir del identificador de red. Es decir, los *routers* controlarán el identificador de la red para realizar el encaminamiento.
- Los routers deben conocer qué bits se utilizan en el identificador de la red.
- Y si el mensaje o paquete llega a un *router* conectado a la red de la dirección IP, se pasa a analizar el identificador de máquinas.
- Para ello es

T2: 2.3 Funciones de la capa de red

- **Direcciones especiales:**

- Red:

- Id. Red. 0

- Id. Red. 0.0

- Id. Red. 0.0.0

- Broadcast

- Id. Red. 1111111

- Id. Red. 1111111.1111111

- Id. Red. 1111111.1111111.1111111

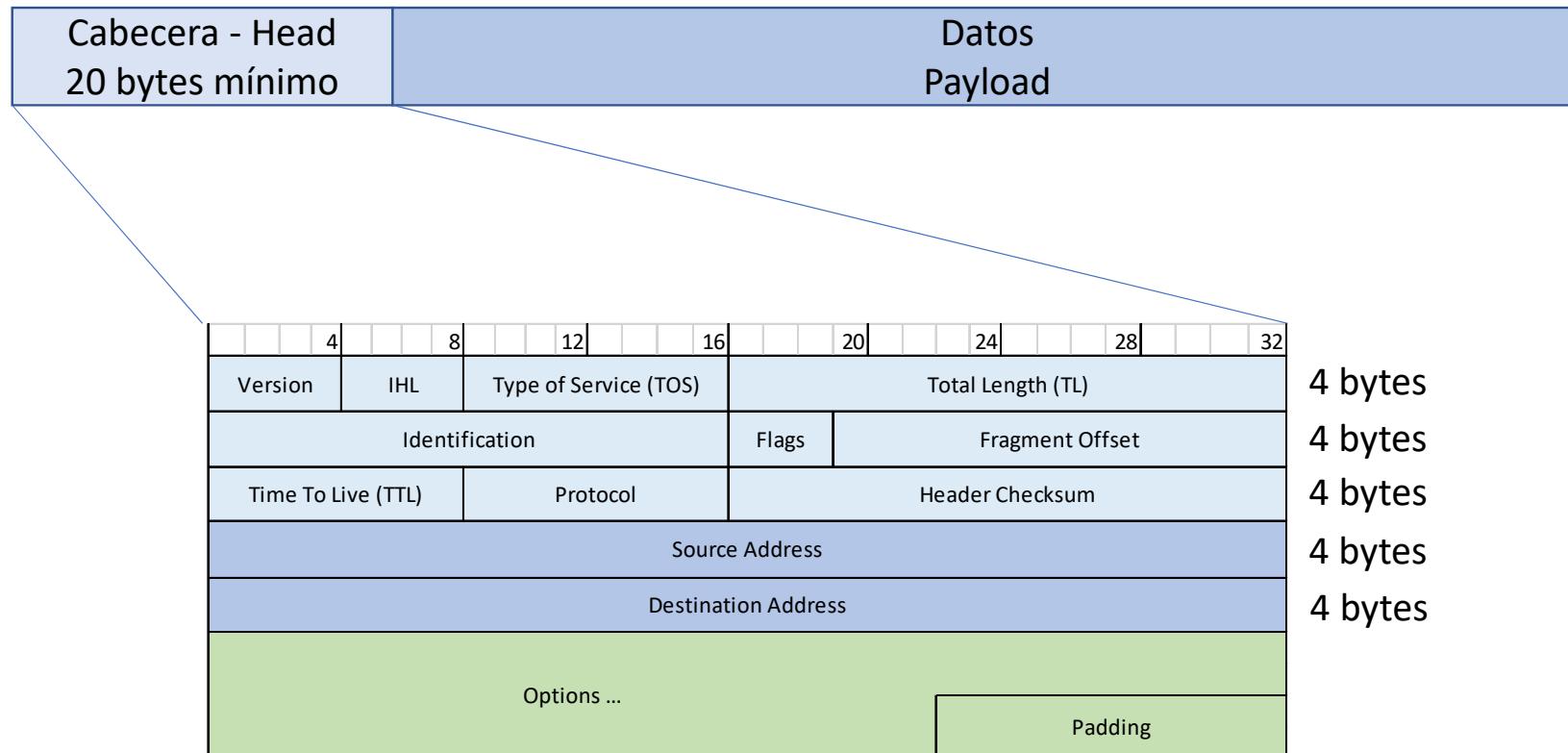
Tema 2: Capa de red

Índice:

1. Introducción
2. Redes orientadas a conexión. Redes no orientadas a conexión
3. Funciones de la capa de red
4. Direcciones IPv4
- 5. IPv4 datagrama**
6. Protocolos de resolución de direcciones
7. Protocolos de gestión de red
8. Protocolos de encaminamiento
9. Movile IP
10. IPv6

Tema 2: Capa de red

Formato de un datagrama RFC 791:



Tema 2: Capa de red

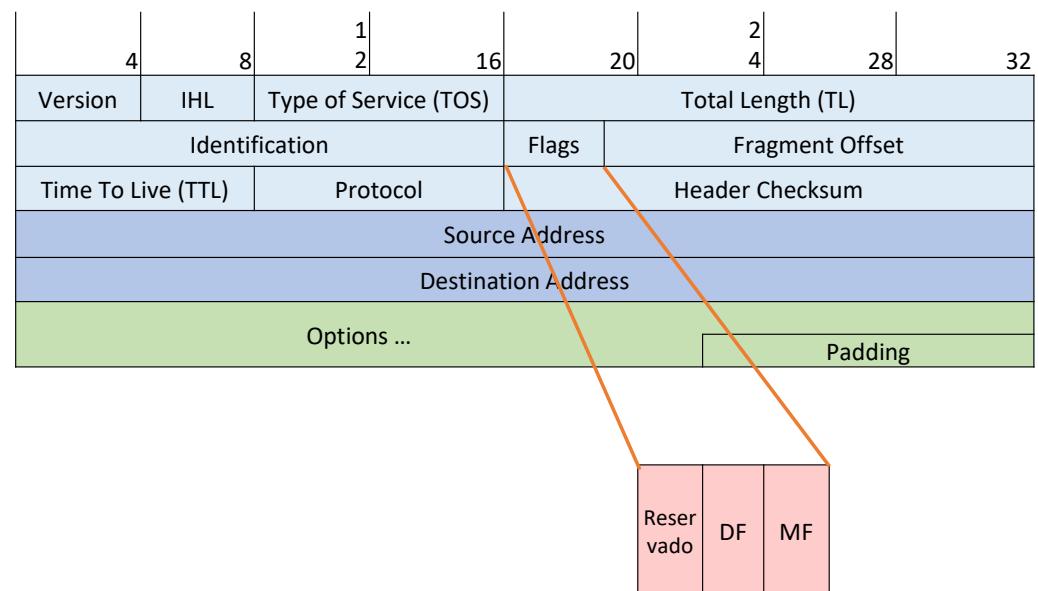
Formato de un datagrama RFC 791:

- **Versión (4 bits):** Identifica la versión de IP empleado. El propósito es asegurarse la compatibilidad.
- **IHL (4bits):** *Internet Header Length*: especifica la longitud de la cabecera cuenta bloques de 32 bits.
- **TOS (8bits):** *Type of Service*, un byte destinado a definir QoS, y utilizado en el servicio de Servicios Diferenciados.
- **TL (16 bits):** *Total Length*, indica la longitud total del paquete en bytes, $2^{16} = 65535$ bytes máximo de un paquete. Aunque son más pequeños.

Tema 2: Capa de red

Formato de un datagrama RFC 791:

- **Identification (16 bits):** Se utiliza si un mensaje es fragmentado o si un router tiene que fragmentar cuando pase a través de esa red. El receptor debe de leer este campo para recomponer el mensaje.
- **Flags (3 bits):** Se utiliza para gestionar la fragmentación de paquetes.
 - Reservado: No se utiliza
 - DF: Don't Fragment.
 - “1” no se fragmenta
 - MF: More Fragment
 - “1” hay más fragmentos
 - “0” último fragmento del mensaje



Tema 2: Capa de red

Formato de un datagrama RFC 791:

- **Fragment Offset (13 bits):** Cuando un mensaje se fragmenta, este campo especifica la posición dentro del mensaje. Se especifica en unidades de 8 bytes. El primer fragmento tiene un offset de 0.
- **TTL (8 bits):** *Time to Live*, especifica cuánto tiempo un datagrama “vive” o permanece en la red. Cada vez que el paquete atraviesa un router se decrementa hasta llegar a cero que se elimina.
- **Protocol (8 bits),** identifica el protocolo de la capa más alta. Está definido en el RFC 1700

Tema 2: Capa de red

Formato de un datagrama RFC 791:

Valor Hexadecimal	Valor Decimal	Protocolo
00	0	Reservado
01	1	ICMP
02	2	IGMP
03	3	GGP
04	4	IP-in-IP
06	6	TCP
08	8	EGP
11	17	UDP
32	50	Utilizado con IPSec
33	51	Utilizado con IPSec

Tema 2: Capa de red

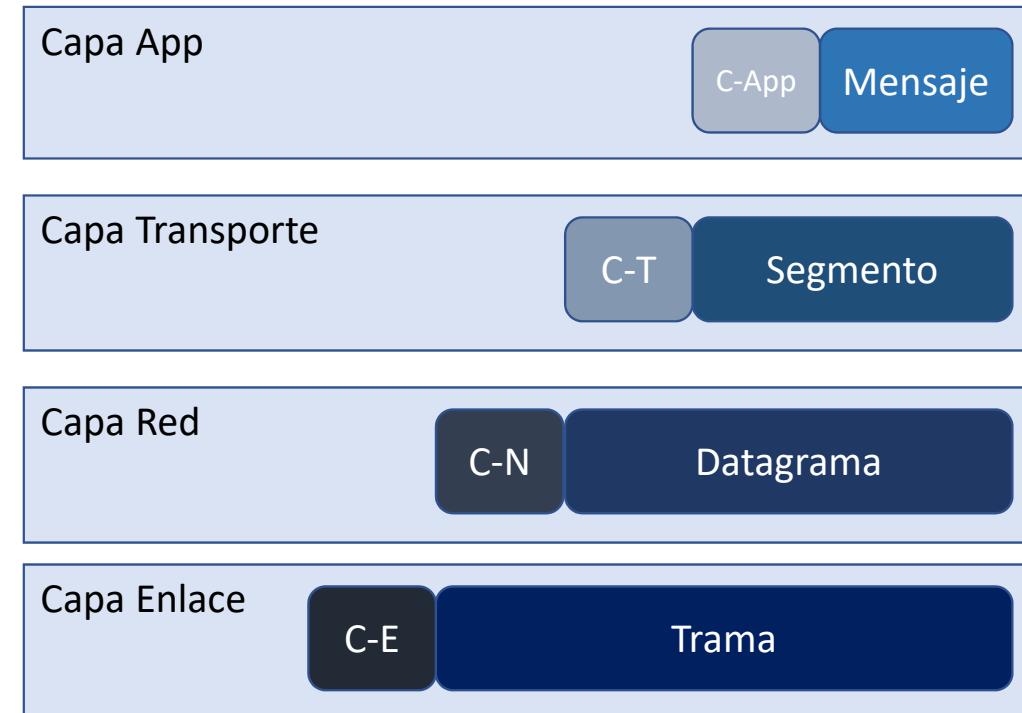
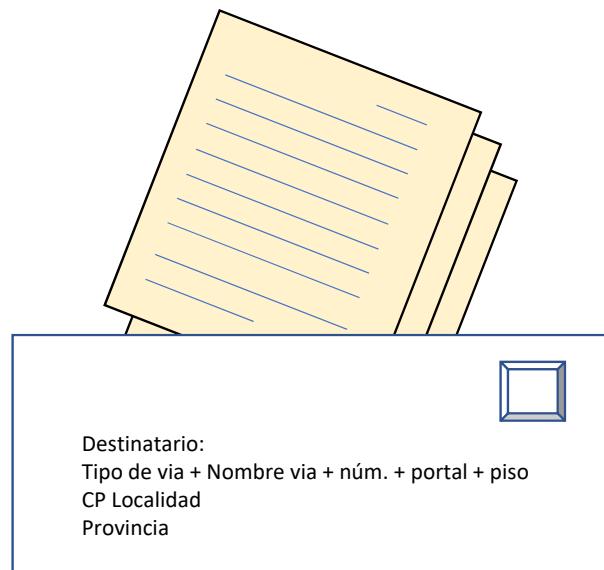
Formato de un datagrama RFC 791:

- **Header Checksum (16 bits):** es un CRC muy sencillo y calculado únicamente sobre la cabecera. Se cogen bloques de 16 bits y se suma. En cada salto se comprueba el CRC. Si está “no ok” se descarta.
- **Source Address (32 bits):** Dirección IP de la máquina de origen.
- **Destination Address (32 bits):** Dirección IP de la máquina destino.
- **Options (Variable)**
- **Padding (Variable):** se utiliza para completar el campo de opciones a 32 bits.
- **Data (Variable):**

Tema 2: Capa de red

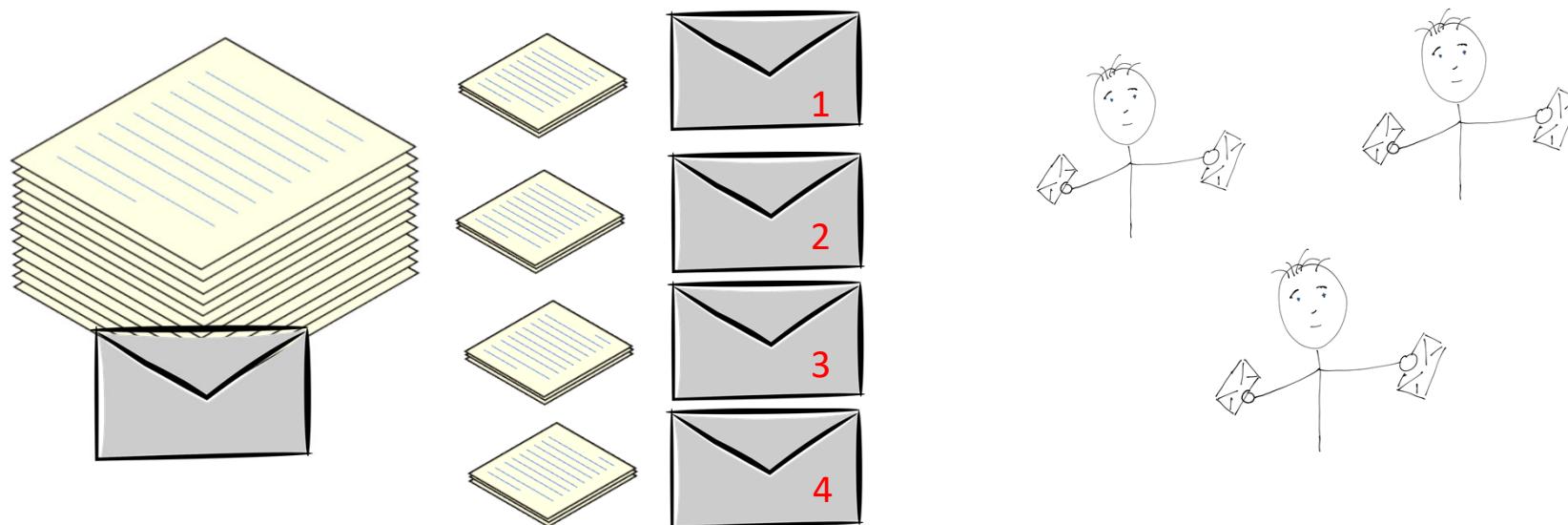
Encapsulación: es una de las funciones principales de la capa IP

Preparar los datos para que puedan llegar al destino



Tema 2: Capa de red

Fragmentación: muchas veces el mensaje es demasiado largo para ser transmitido que tiene que ser dividido.



Tema 2: Capa de red

Maximum Transmission Unit (MTU)

Los datos de las capas altas son encapsulados en un datagrama IP y estos datos son pasados a la capa de enlace y luego a la física.

Cada datagrama se debe ajustar al tamaño de una trama. Si el mensaje es mayor que el tamaño de la trama es necesario fragmentar el mensaje en varios datagramas.

Los datagramas son enviados individualmente y reensamblados en el destino.

El tamaño máximo depende las capas inferiores y de la tecnología: ejemplo Ethernet es de 1500 bytes.

Si la capa IP recibe un mensaje, y calcula el tamaño después de añadirle la cabecera es superior que MTU fijado por las capas inferiores, la capa IP fragmentará el mensaje.

Tema 2: Capa de red

Maximum Transmission Unit (MTU)

Determinar el tamaño óptimo de la MTU requiere conocer la MTU de cada enlace. Hay técnicas que evalúan qué valor de MTU, denominados *path MTU discovery*.

Uno de los mensajes de ICMP, es de “destino inalcanzable: se necesita fragmentación”. Este mensaje puede deberse a varias razones. Una de ellas puede ser porque el **bit DZ (Don’t Fragment)** esté activado. El paquete es desacartado y se envía este mensaje.

El origen vuelve a intentar retransmitir con una MTU más pequeña hasta que no se reciba este mensaje.

Tema 2: Capa de red

Maximum Transmission Unit (MTU)

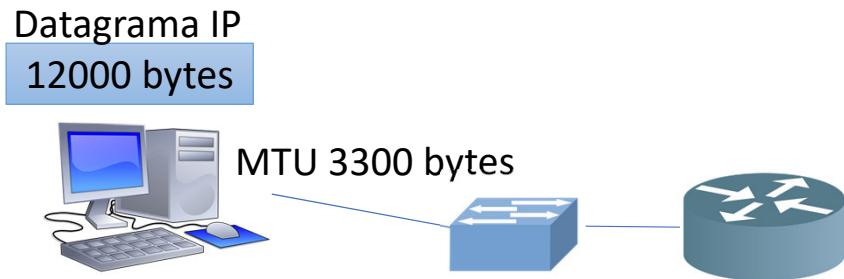
Al fragmentar un mensaje hay que tener en cuenta:

- Secuencia y recolocación. El receptor debe de ser capaz de gestionar el orden de los ficheros.
- Separación de los mensajes fragmentados.
- El destino debe de saber cuando puede recomponer el mensaje.
- Los fragmentos deben ser múltiplos de 8, por el tema del *offset*.
- El reensamblado sólo se hace en el destino.

Tema 2: Capa de red

Maximum Transmission Unit (MTU)

Ejemplo: una máquina quiere enviar un datagram IP de 12000 bytes con la cabecera incluida. Su conexión local tiene una MTU de 3300 bytes. La cabecera de IP es de 20 bytes.



Datagrama IP: 20 (H) + 11980 (D)

MTU de 3300 bytes:

1. Fragmento 1: 20 (H) + 3280 (D).
2. Fragmento 2: 20 (H) + 3280 (D).
3. Fragmento 3: 20 (H) + 3280 (D).
4. Fragmento 4: 20 (H) + 2140 (D).

Offset: $3280/8$ bytes = 410

Tema 2: Capa de red

Maximum Transmission Unit (MTU)

MF	Offset	Datos 11980 bytes
0	0	

MF	Offset	Datos 3280 bytes
1	0	

Fragmento 1: 0 - 3279 bytes

MF	Offset	Datos 3280 bytes
1	410	

Fragmento 2: 3280 - 6559 bytes

MF	Offset	Datos 3280 bytes
1	820	

Fragmento 3: 6560 - 9839 bytes

MF	Offset	Datos 2140 bytes
0	1230	

Fragmento 3: 9840 - 11979 bytes

calculo de offset

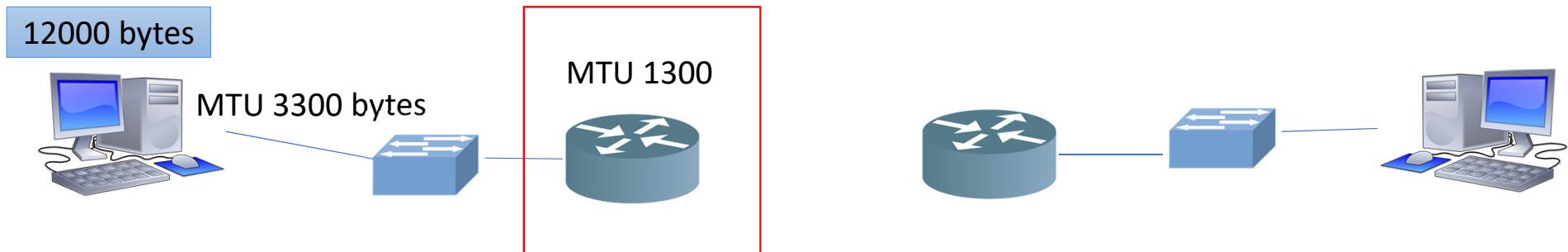
1. Fragmento 1: Offset = 0
2. Fragmento 2: $3280/8=410$.
3. Fragmento 3: $6560/8=820$
4. Fragmento 4: $9840/8=1230$

Offset: $3280/8$ bytes = 410

Tema 2: Capa de red

Maximum Transmission Unit (MTU)

Caso B



MTU de 1300 bytes:

1. Fragmento 1: 20 (H) + 1280 (D).
2. Fragmento 2: 20 (H) + 1280 (D).
3. Fragmento 3: 20 (H) + 720 (D).

Offset: $1280/8$ bytes = 160

Esta foto de Autor desconocido está bajo licencia CC BY-SA

Tema 2: Capa de red

Maximum Transmission Unit (MTU)

Caso B

MF	Offset	Datos
1	0	3280 bytes

Fragmento 1: 0 - 3279 bytes

MF	Offset	Datos
1	0	1280 bytes

Fragmento 1.1: 0 - 1279 bytes

MF	Offset	Datos
1	820	3280 bytes

Fragmento 3: 6560 - 9839 bytes

MF	Offset	Datos
1	820	1280 bytes

Fragmento 3.1: 6560 - 7839 bytes

MF	Offset	Datos
1	160	1280 bytes

Fragmento 1.2: 1280 - 2559 bytes

MF	Offset	Datos
1	320	720 bytes

Fragmento 1.3: 2560 - 3279 bytes

MF	Offset	Datos
1	410	3280 bytes

Fragmento 2: 3280 - 6559 bytes

MF	Offset	Datos
1	410	1280 bytes

Fragmento 2.1: 3280 - 4559 bytes

MF	Offset	Datos
1	1230	2140 bytes

Fragmento 3: 9840 - 11979 bytes

MF	Offset	Datos
1	1230	1280 bytes

Fragmento 4.1: 9840 - 11119 bytes

MF	Offset	Datos
1	570	1280 bytes

Fragmento 2.2: 4560 - 5839 bytes

MF	Offset	Datos
1	730	720 bytes

Fragmento 2.3: 5840 - 6559 bytes

MF	Offset	Datos
1	1390	860 bytes

Fragmento 4.2: 11120 - 11979 bytes

Calculo de offsets

Fragmento 1.1: Offset = 0

Fragmento 1.2: $1280/8=160$.

Fragmento 1.3: $2560/8=320$

Fragmento 2.1: $3280/8=410$

...

Tema 2: Capa de red

Índice:

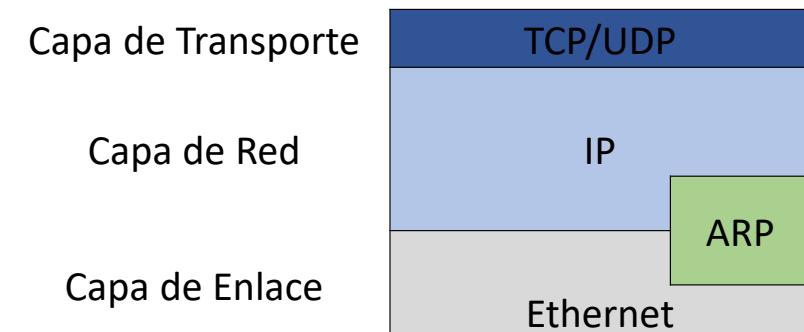
1. Introducción
2. Redes orientadas a conexión. Redes no orientadas a conexión
3. Funciones de la capa de red
4. Direcciones IPv4
5. IPv4 datagrama
- 6. Protocolos de resolución de direcciones**
7. Protocolos de gestión de red
8. Protocolos de encaminamiento
9. Movile IP
10. IPv6

Tema 2: 2.6 Protocolos de resolución de direcciones

Protocolo de Resolución de direcciones ARP (*Address Resolution Protocol*)

RFC 826

- En redes de área local, la primera conexión se hace a nivel de la capa de enlace → Dirección MAC del destino para que el *router* lo indique en la trama.
- Podríamos decir que se encuentra entre la capa 2 y 3.
- Asocia direcciones IP con direcciones MAC que se almacenan en la cache.
- Las direcciones MAC son fijas y están asociadas a la tarjeta (interfaz LAN).
- Antes de cualquier comunicación, se consulta la caché, si no se encuentra la MAC, se ejecuta el protocolo **ARP**.



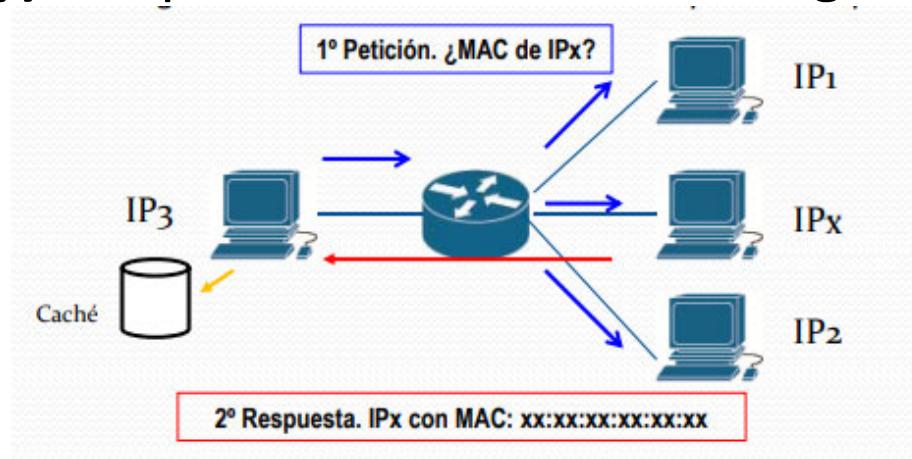
Tema 2: 2.6 Protocolos de resolución de direcciones

Protocolo de Resolución de direcciones ARP (*Address Resolution Protocol*)

RFC 826

Fases del protocolo ARP:

- **Petición (ARP-request):** se envía una trama con destino *broadcast* ¿Quién tiene la dirección IP_x?
- **Respuesta (ARP-replay):** respuesta con destino el origen con la dirección IP_x y MAC_x



Tema 2: 2.6 Protocolos de resolución de direcciones

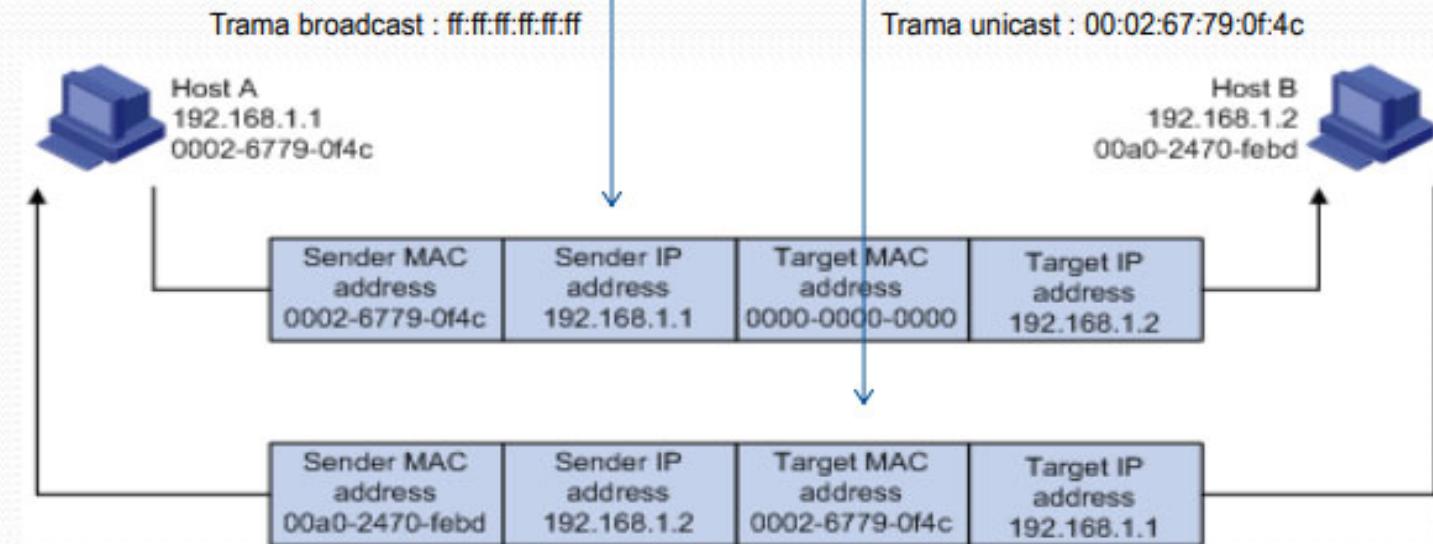
Protocolo de Resolución de direcciones ARP (*Address Resolution Protocol*)

RFC 826

C:\arp -a

C:\netstat -rn

Ejemplo contenido de tramas ARP-Request y ARP-Reply

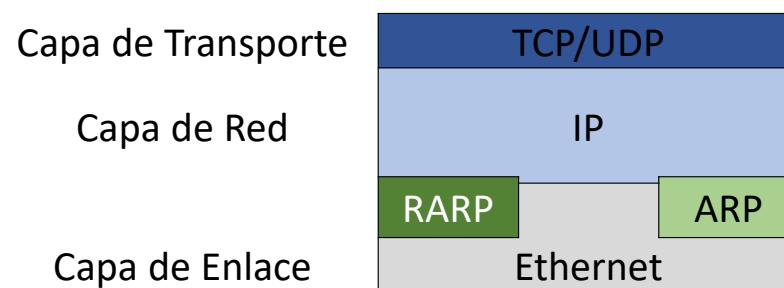


Tema 2: 2.6 Protocolos de resolución de direcciones

Protocolo de Resolución de direcciones inversa: RARP (*Reverse Address Resolution Protocol*)

RFC 826

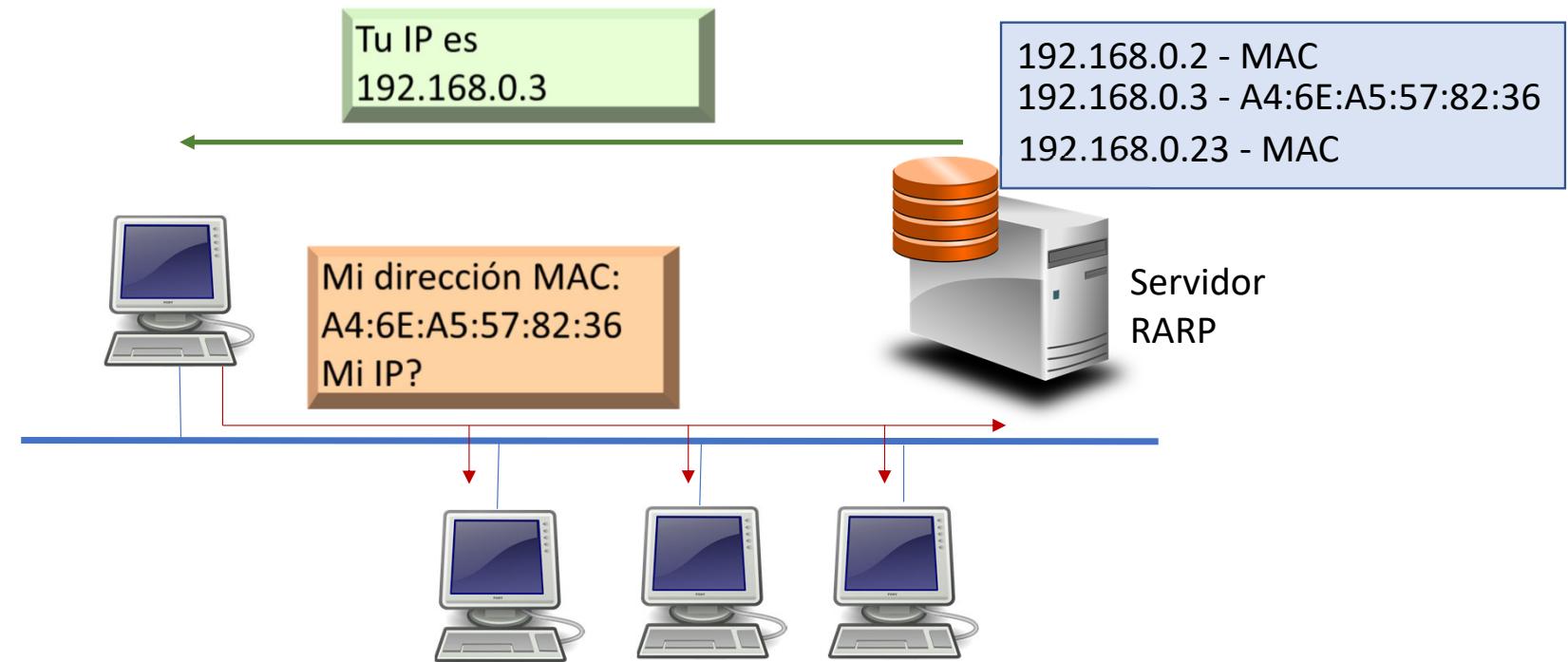
- Si un dispositivo desconoce su dirección IP, (equipos sin disco duro), debe obtenerla de un servidor remoto → **RARP**.
- Es un protocolo que se encuentra entre el nivel 2 y 3.



Tema 2: 2.6 Protocolos de resolución de direcciones

Protocolo de Resolución de direcciones inversa: RARP (*Reverse Address Resolution Protocol*)

RFC 826



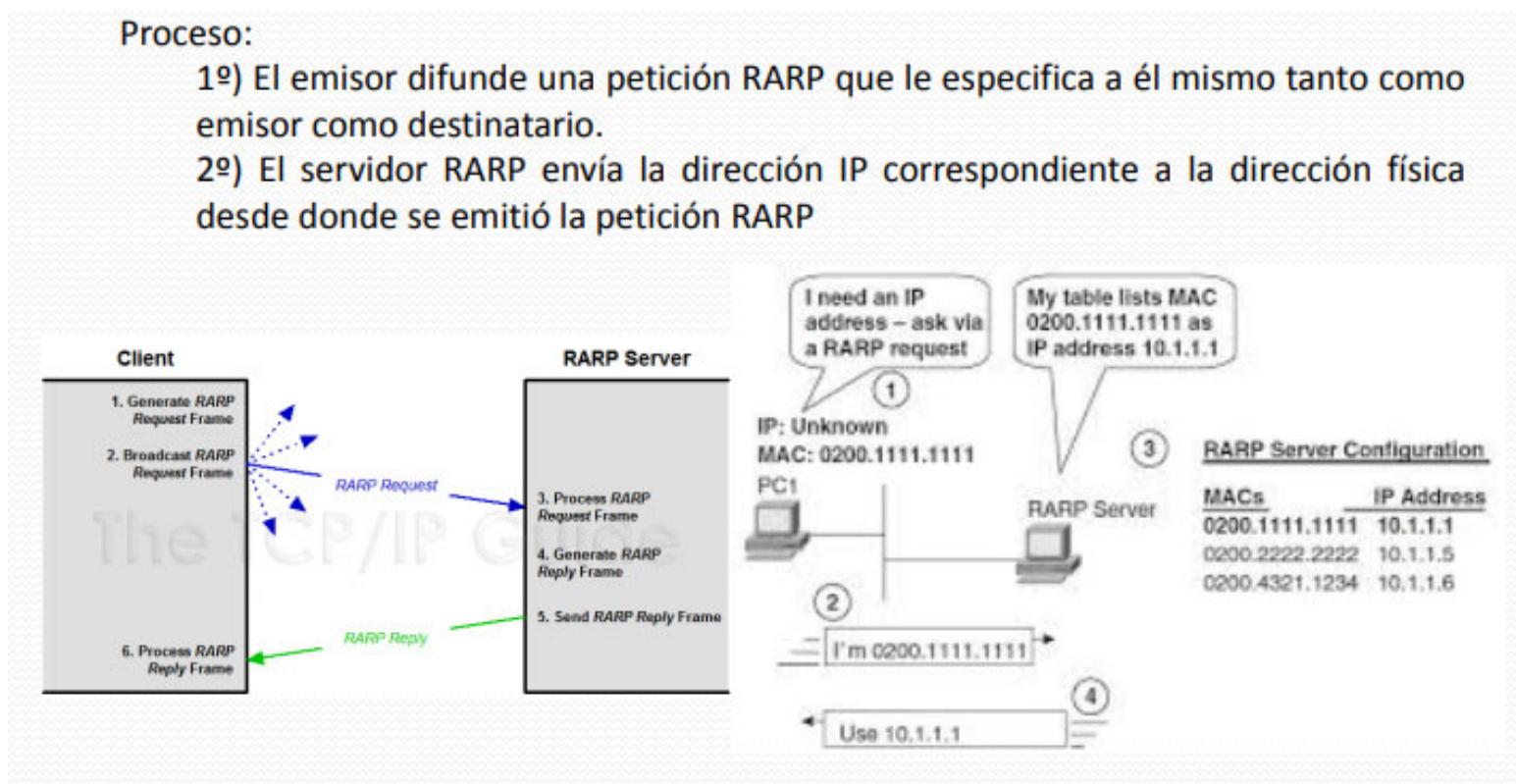
Tema 2: 2.6 Protocolos de resolución de direcciones

Protocolo de Resolución de direcciones inversa: RARP (*Reverse Address Resolution Protocol*)

RFC 826

Proceso:

- 1º) El emisor difunde una petición RARP que le especifica a él mismo tanto como emisor como destinatario.
- 2º) El servidor RARP envía la dirección IP correspondiente a la dirección física desde donde se emitió la petición RARP

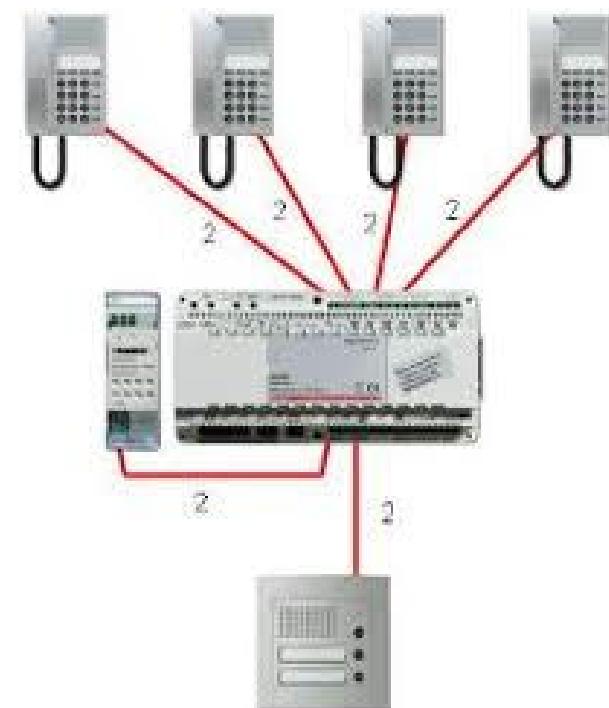


Tema 2: 2.6 Protocolos de resolución de direcciones

IP Network Address Translation – NAT Protocol

RFC 1631

- Esta tecnología permite que una única dirección IP pública sea compartida por muchas máquinas que tienen a su vez direcciones privadas.
Símil: centralita telefónica
- Esta tecnología permite que pueda existir muchas más máquinas que direcciones públicas.
- Y al mismo tiempo proporciona “algo” de seguridad, ya que las máquinas se encuentran en una red interna menos accesible.
- Las direcciones privadas son bloqueadas por los routers, sin embargo dentro o detrás de un router NAT es posible su uso.



Tema 2: 2.6 Protocolos de resolución de direcciones

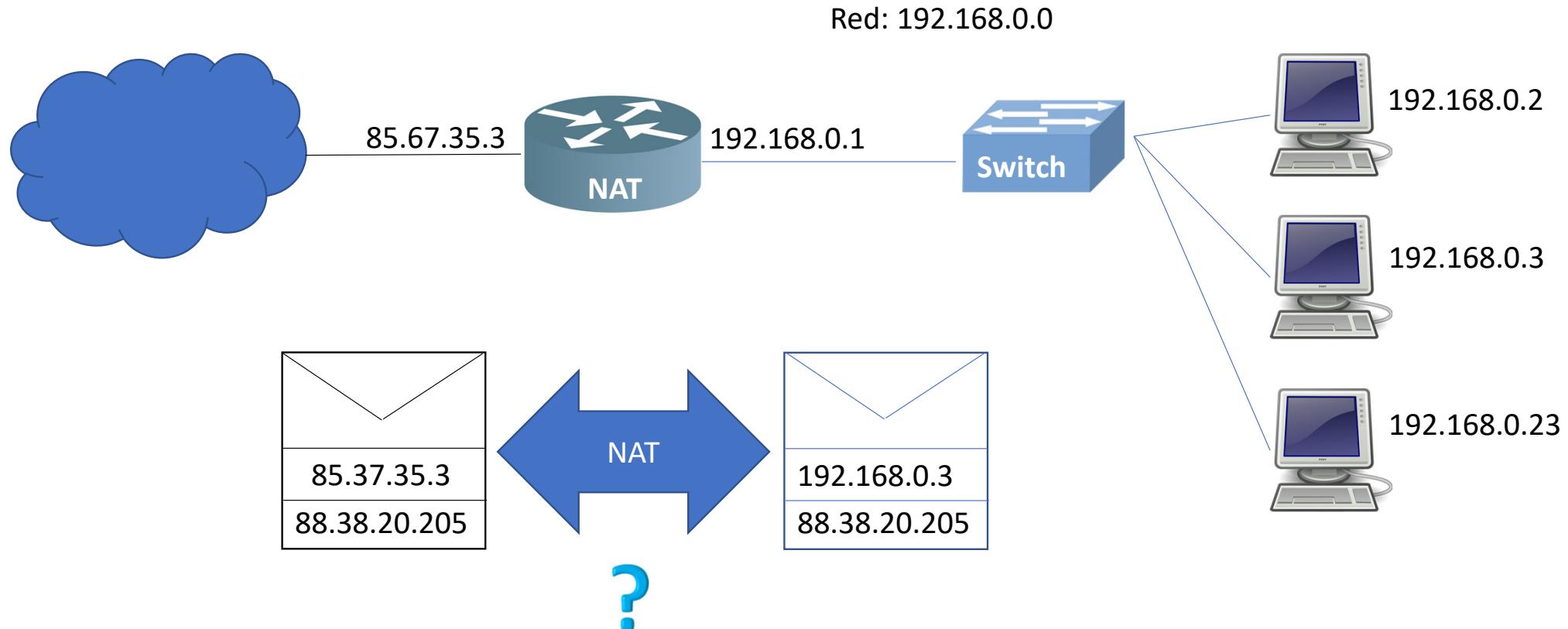
IP Network Address Translation – NAT Protocol

¿Por qué surge?

- El espacio de direcciones es finito y cada vez había más demanda de direcciones IP. Esto hizo que se incrementara el coste.
- Para las organizaciones y/o empresas tener muchas máquinas conectadas implica riesgo de seguridad porque pueden ser atacadas directamente y ser la puerta de entrada.
- La mayoría de las máquinas son clientes y no requieren de una dirección pública.
- Probabilidad de que determinadas máquinas accedan a Internet simultáneamente.

Tema 2: 2.6 Protocolos de resolución de direcciones

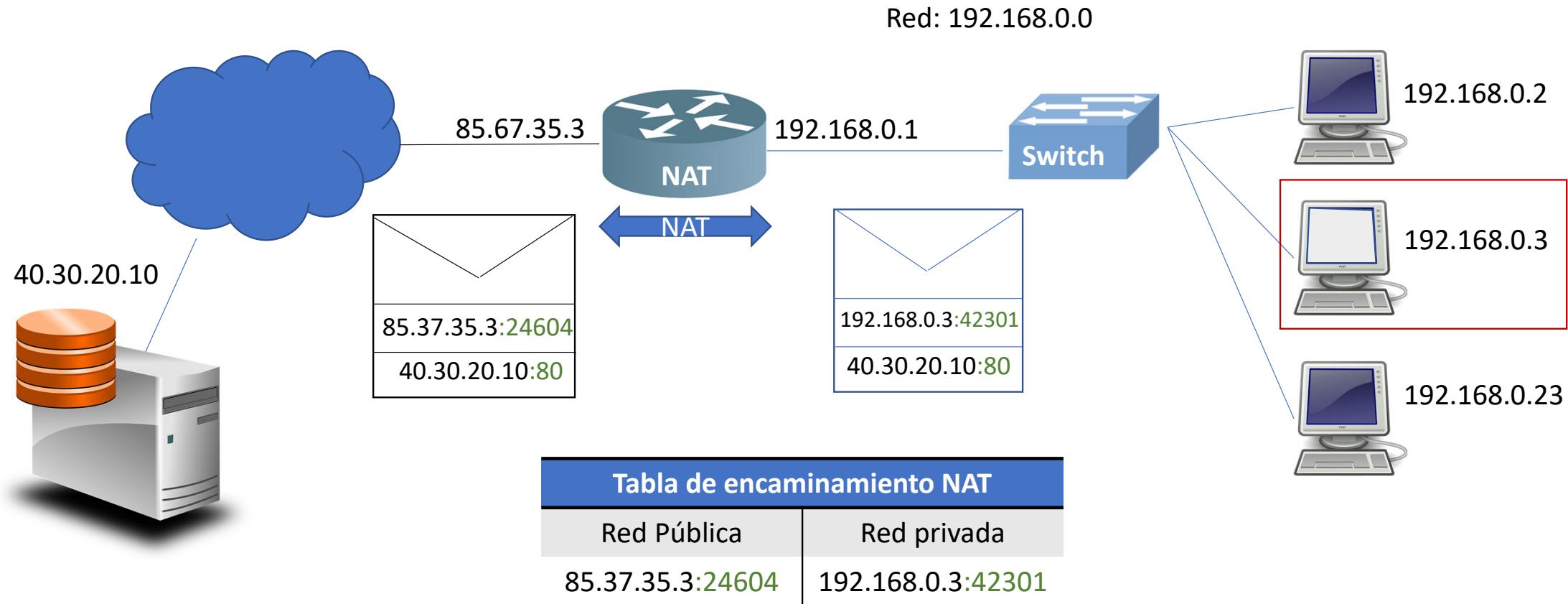
IP Network Address Translation – NAT Protocol



Esta foto de Autor desconocido está bajo licencia [CC BY-SA](#)

Tema 2: 2.6 Protocolos de resolución de direcciones

IP Network Address Translation – NAT Protocol



Esta foto de Autor desconocido está bajo licencia [CC BY-SA](#)

Tema 2: 2.6 Protocolos de resolución de direcciones

IP Network Address Translation – NAT Protocol

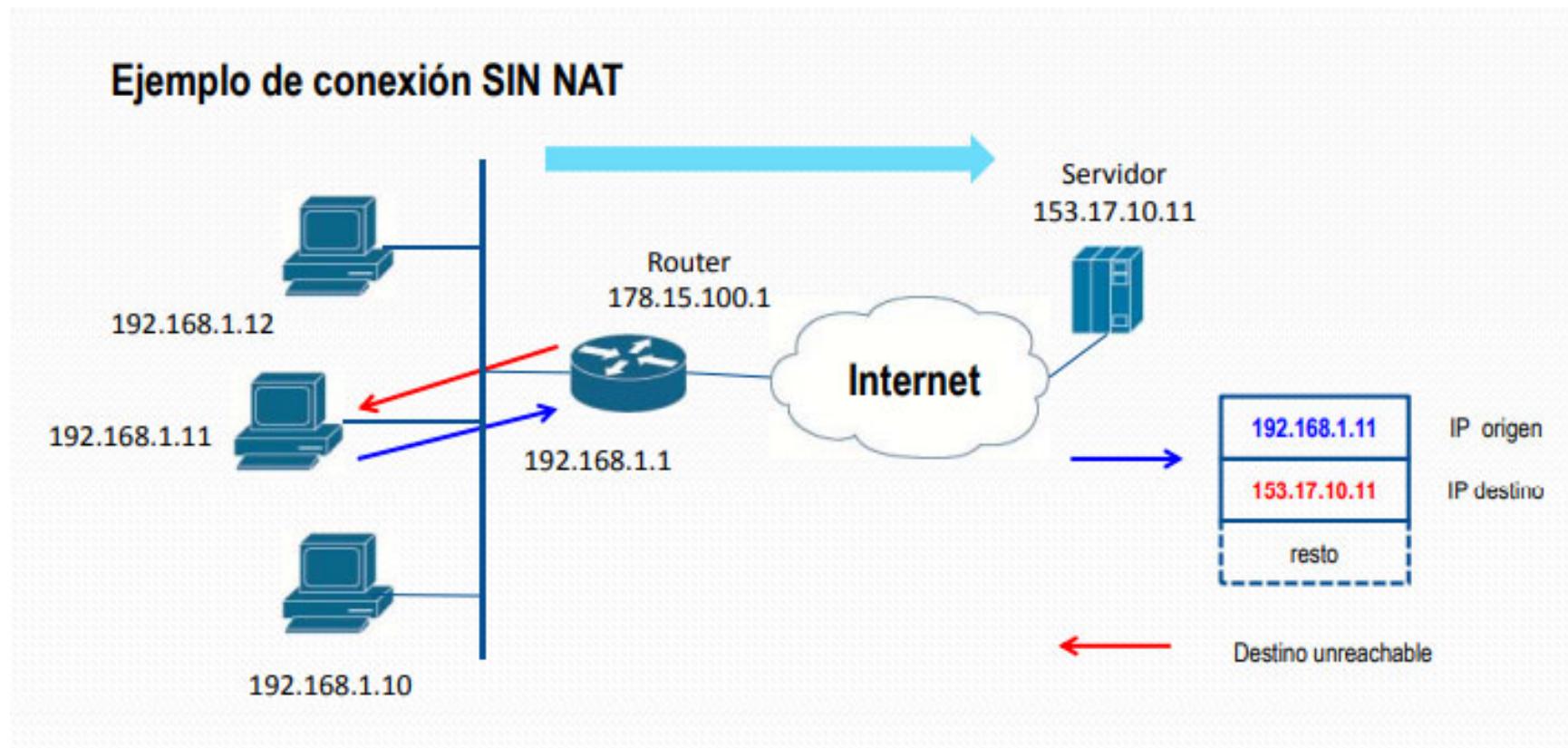
Mapeado de direcciones

- El software NAT en un *router* debe mantener una tabla que traduzca las direcciones de dentro y fuera.
 - Hay dos tipos de mapeado:
 - Estático: las máquinas siempre eligen la misma dirección IP pública.
 - Dinámico: se les asigna las direcciones IP públicas de manera aleatoria a las máquinas. Una vez que se termina la sesión se descarta y la dirección pública queda disponible.
- Es posible mezclar ambas formas de trabajo, que determinados dispositivos cuando salen, lo hagan con la misma IP.

- Al cambiar las direcciones IP el campo Checksum de la cabecera de los paquetes hay que recalcularlo.

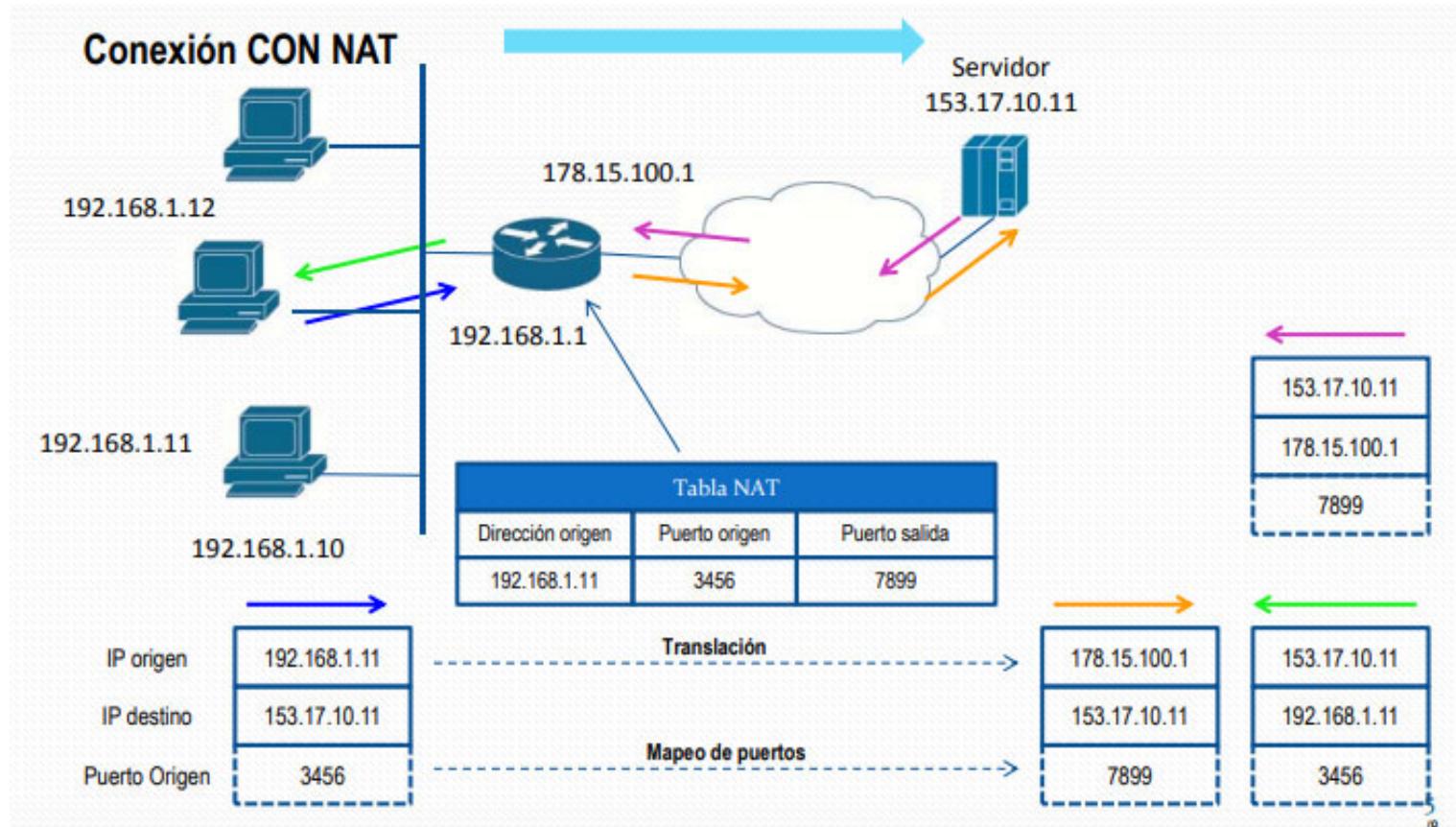
Tema 2: 2.6 Protocolos de resolución de direcciones

IP Network Address Translation – NAT Protocol



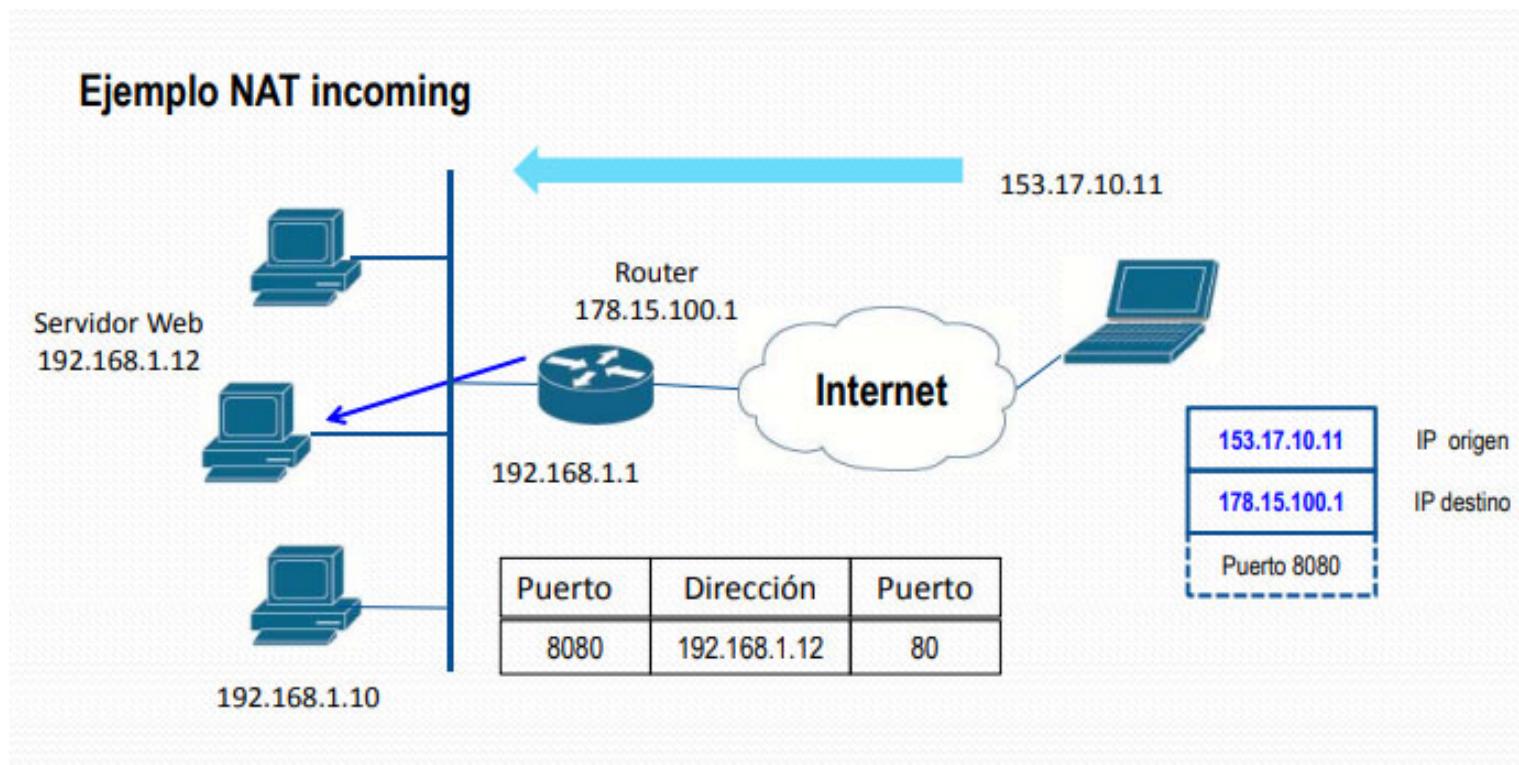
Tema 2: 2.6 Protocolos de resolución de direcciones

IP Network Address Translation – NAT Protocol



Tema 2: 2.6 Protocolos de resolución de direcciones

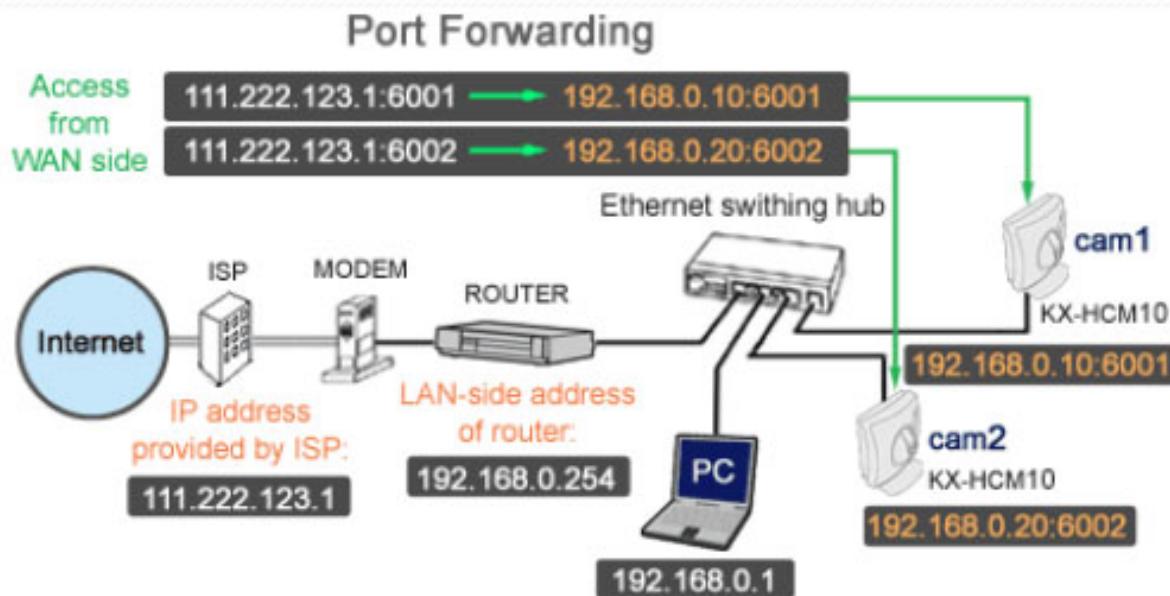
IP Network Address Translation – NAT Protocol



Tema 2: 2.6 Protocolos de resolución de direcciones

IP Network Address Translation – NAT Protocol

El mecanismo de "port forwarding" permite que datos de una red privada puedan ser transmitidos a través de una red pública, ya que los nodos de la red publica no pueden routearlos.



Tema 2: Capa de red

Índice:

1. Introducción
2. Redes orientadas a conexión. Redes no orientadas a conexión
3. Funciones de la capa de red
4. Direcciones IPv4
5. IPv4 datagrama
6. Protocolos de resolución de direcciones
- 7. Protocolos de gestión de red**
8. Protocolos de encaminamiento
9. Movile IP
10. IPv6

Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red:

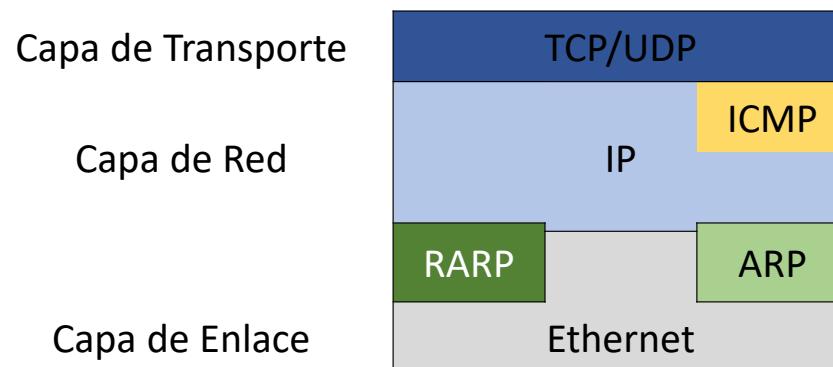
ICMP (*Internet Control Message Protocol*)

- Es un protocolo adjunto al protocolo IP y definido en el RFC 792.
- Implementan o dan soporte al reporte de información de error, tests, etc.
- IP es un protocolo no orientado a conexión, no fiable, y sin confirmación. A pesar de todo esto los datagramas llegan al destino.
- Y requiere de un protocolo que permita diagnosis.
- Ambos protocolos trabajan juntos:
 - IP realiza las tareas de direccionamiento, encapsulado y encaminamiento.
 - ICMP da soporte a IP, intercambiando mensajes entre los dispositivos.

Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red:

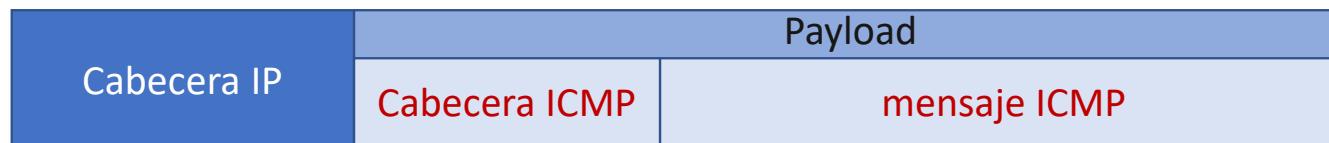
ICMP (*Internet Control Message Protocol*)



Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

- Los mensajes son encapsulados en datagramas IP para su transmisión.

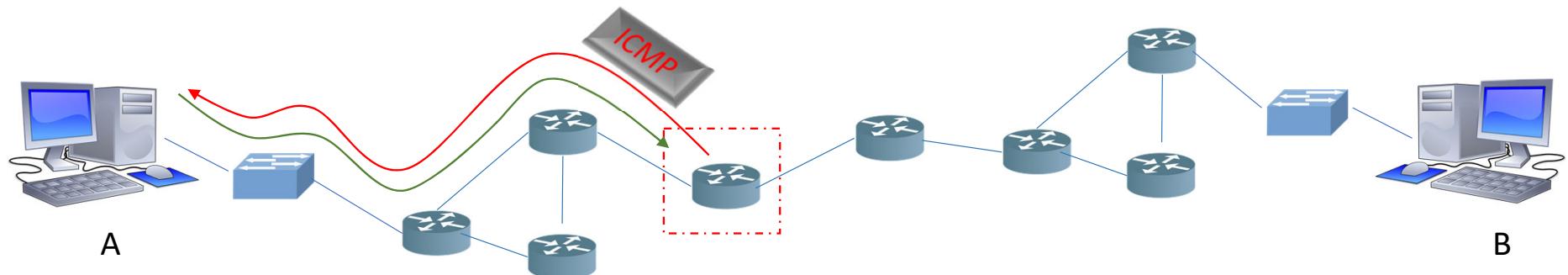


- Es un protocolo sencillo y que define básicamente mensajes de control.
- ICMP no define por si mismo los diferentes mensajes de control/error. Son los protocolos que hacen uso de ICMP. **Es decir, define un servicio de paso de mensajes a otros protocolos.**
- Por lo general el destinatario final es IP, aunque puede ser otro software de la jerarquía de protocolos TCP/IP.
- ICMP no utiliza puertos (TCP/UDP) para redireccionar sus mensajes a las diferentes aplicaciones.

Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

- En un principio estaba pensado para que los mensajes se intercambiase entre *routers*, sin embargo es posible enviar determinados mensajes los *hosts*.
- **Inconveniente:** cuando un error es detectado se informa mediante un mensaje ICMP, **pero** a la fuente original del datagrama.



Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

- Hay dos clases de mensajes ICMP:
 - **Mensajes de error:** dan información a la fuente de que ha ocurrido algún error. Son generados en respuesta a alguna acción.
 - **Mensajes de información o consulta:** son mensajes que permiten el intercambio de información entre los dispositivos para test. No manejan información de **error**. Son mensajes generados por las aplicaciones o como respuesta a otros mensajes ICMP.

Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

- **Tipos de mensajes.** Viene dado por un campo de 8 bits (*Type value*), 256 posibilidades.
 - **Mensajes de error:** *Type values* = [0-127].
 - **Mensajes de información o consulta:** *Type value* [128-255]
- Con estos 8 bits se definen mensajes de propósito general.
- Hay otro campo de 8 bits (*Code field*) que permite categorizar más los mensajes.

4	8	12	16	20	24	28	32
Type	Code	Checksum					
ICMP datos (dependiendo del mensaje)							

Tema 2: 2.7 Protocolos de gestión de red

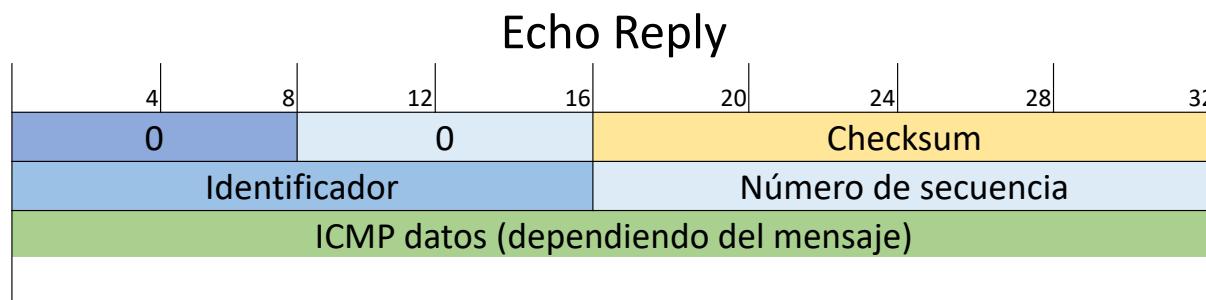
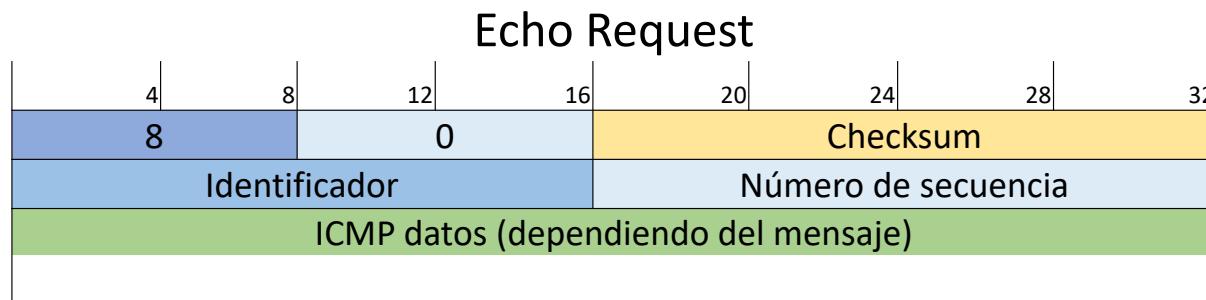
Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

Tipo ICMP	Tipo ICMPv6	Nombre del tipo	Código	Descripción
0	129	Echo Reply		Respuesta a un ping de red.
3	1	Destination Unreachable	0–15	Mensaje ICMP que informa que el paquete no puede ser entregado al destino.
5	137	Redirect Message	0–3	Permite al router informar al host de una mejor ruta.
8	128	Echo Request		Ping de red
9	134	Router Advertisement		Lo utilizan los routers para informar a los host de su existencia.
11	3	Time Exceeded	0 o 1	Informe de estado que o bien indica que el tiempo de vida (Time to Live, TTL) de un paquete ha expirado.
13	13	Timestamp (Request)		Mensaje que solicita el paquete de una marca de tiempo para el cálculo del tiempo de propagación y sincronización.
14	-	Timestamp Reply		Mensaje de respuesta a una petición de marca de tiempo enviado por el destinatario tras la recepción del mismo.
30	-	Traceroute		Utilizado para la implementación seguimiento de la ruta de un paquete. Hoy en día se utilizan "Echo Request" y "Echo Reply" para estos fines

<http://www.iana.org/assignments/icmp-parameters/icmp-parameters.txt>

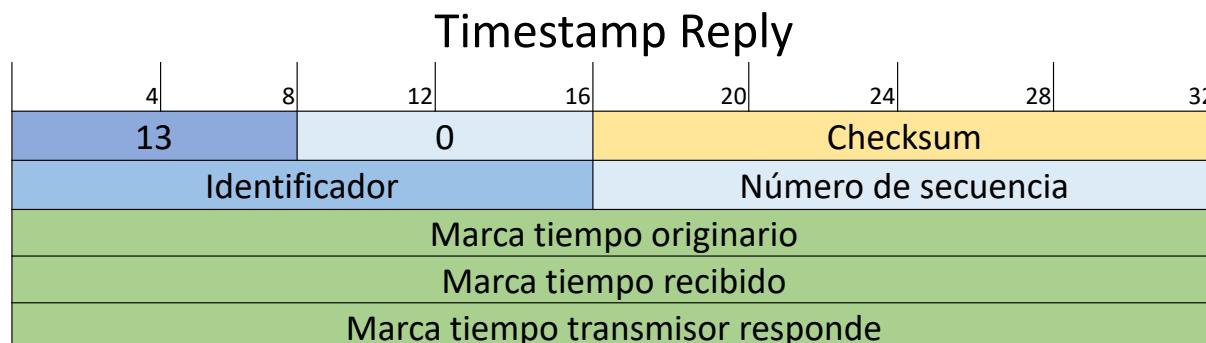
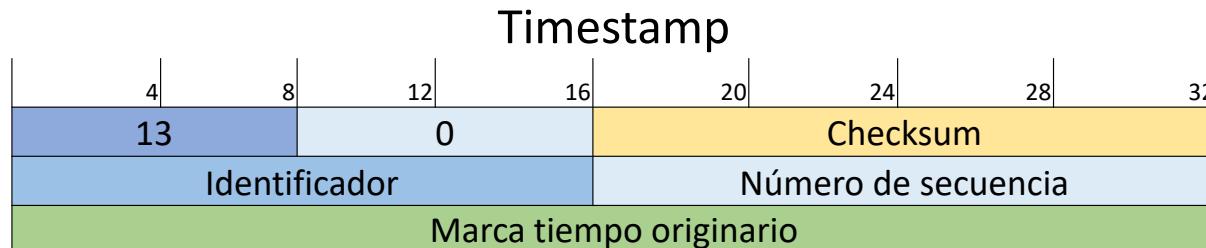
Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)



Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

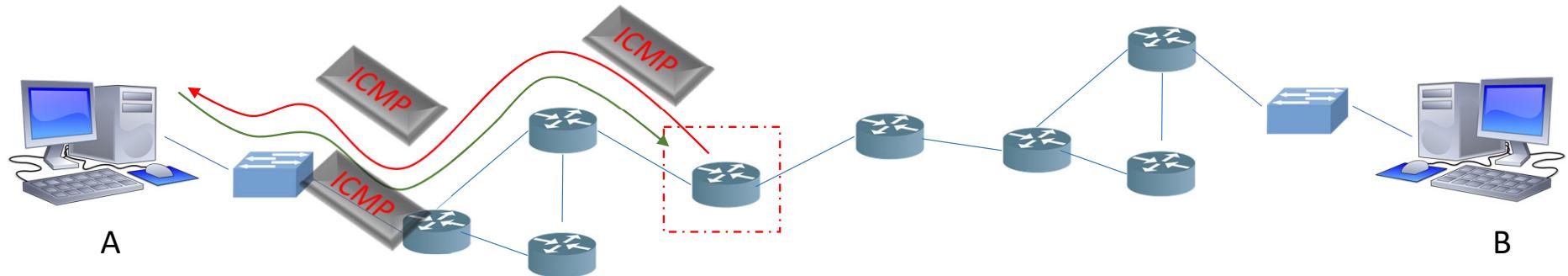


*La marca de tiempos es el valor de 32 bits en milisegundos desde medianoche UT

Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

- **Inconveniente:** Los mensajes de error son enviados en respuesta a muchas situaciones y potencialmente responden a mensajes de error, implicando -> bucle de mensajes



Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

- Para prevenir este tipo de situaciones, un mensaje de error **no debe generarse** en respuesta a:
 - A un **mensaje de error ICMP**.
 - A un **paquete multicast o broadcast**. Si se envía a 5000 usuarios y en la ruta cada uno de ellos encuentra un error intentarán enviar un mensaje ICMP.
 - Cuando un paquete se fragmenta, si hay errores sólo se envían con el primer fragmento.

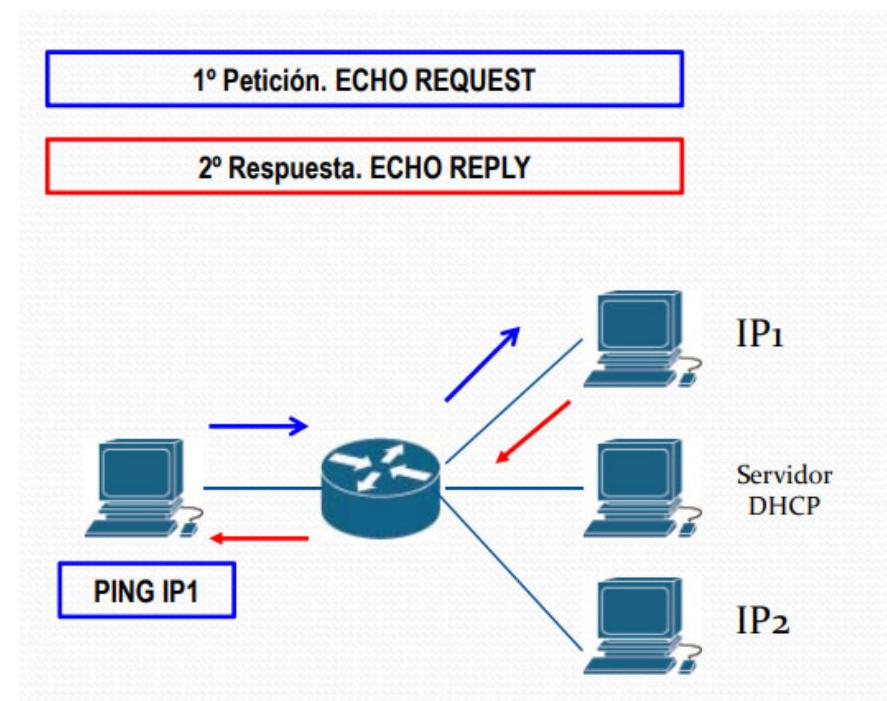
Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

- Herramientas que usan ICMP: ping

Da información:

- Si hay conectividad o no
- El tiempo que tarda

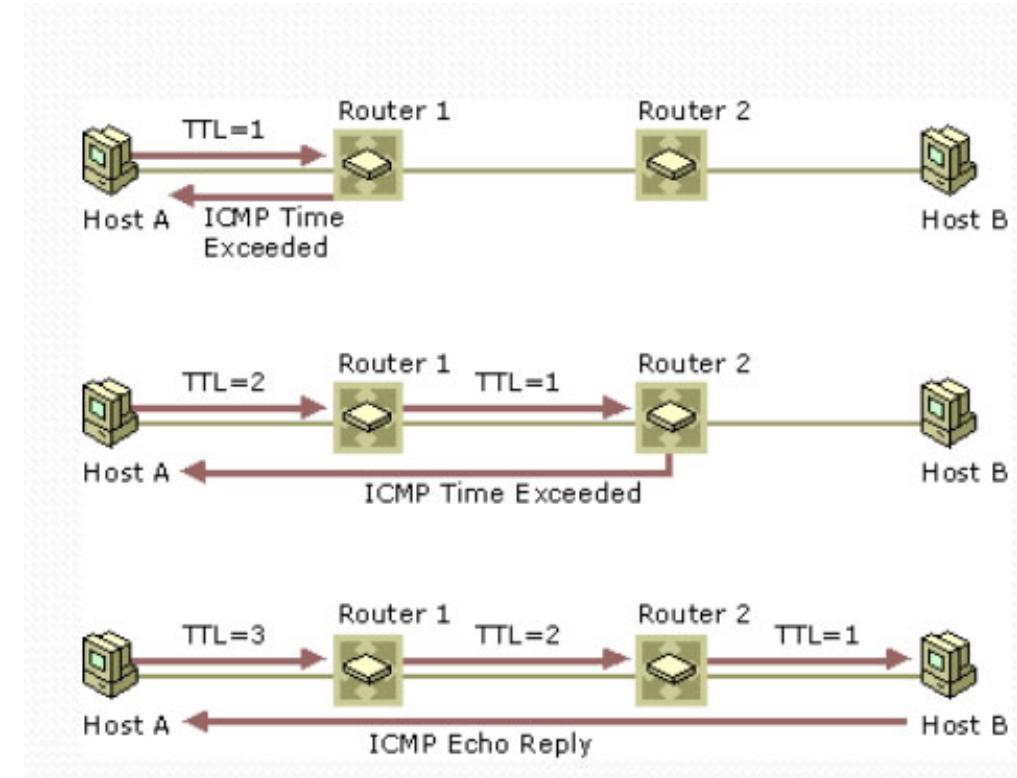


Tema 2: 2.7 Protocolos de gestión de red

Protocolos de gestión de red: ICMP (*Internet Control Message Protocol*)

- **Herramientas que usan ICMP: traceroute**

- Sirve para determinar cuales son los *routers* por los que pasa un paquete en su camino al equipo remoto.
- El ordenador local envía el paquete ECHO_REQUEST con el parámetro TTL (tiempo de vida) ajustado a 1 al dispositivo remoto. El primer router disminuye TTL en uno, es decir a cero, elimina el paquete y reenvía el mensaje ICMP TIME_EXCEEDED al destinatario.
- El ordenador de destino al recibir tal información repite el envío de ECHO_REQUEST, pero con el TTL ajustado en el valor de 2. El primero de los routers disminuye el TTL en 1, el segundo hará lo mismo ajustándolo a 0, y entonces de nuevo eliminará el paquete y enviará el mensaje TIME_EXCEEDED.
- ...



Tema 2: Capa de red

Índice:

1. Introducción
2. Redes orientadas a conexión. Redes no orientadas a conexión
3. Funciones de la capa de red
4. Direcciones IPv4
5. IPv4 datagrama
6. Protocolos de resolución de direcciones
7. Protocolos de gestión de red
- 8. Protocolos de encaminamiento**
9. Movile IP
10. IPv6

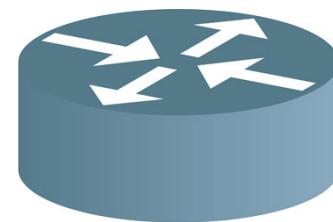
Tema 2: 2.8 Protocolos de encaminamiento

Los protocolos de encaminamiento pueden ser simples o complejos, dependerá de la proximidad de la fuente y el destino:

- Encaminamiento **directo** de datagramas. La fuente y el destino están en la misma red física.
- Encaminamiento **indirecto** de datagramas. La fuente y el destino no están en la misma red física. La fuente **no ve** al destino y los paquetes tienen que viajar a través de dispositivos intermedios, **routers**.
- Los *routers* no poseen información del estado relativa a las conexiones finales. Los paquetes son enviados utilizando únicamente **la dirección IP destino**.
- El envío de paquetes entre una misma fuente y destino pueden seguir rutas diferentes y no hay garantías de que lleguen.

Tema 2: 2.8 Protocolos de encaminamiento

- Routers: dispositivos responsables de realizar el encaminamiento dentro de la red.



- Los *routers* implementan los tres primeros niveles: físico, enlace y de red.

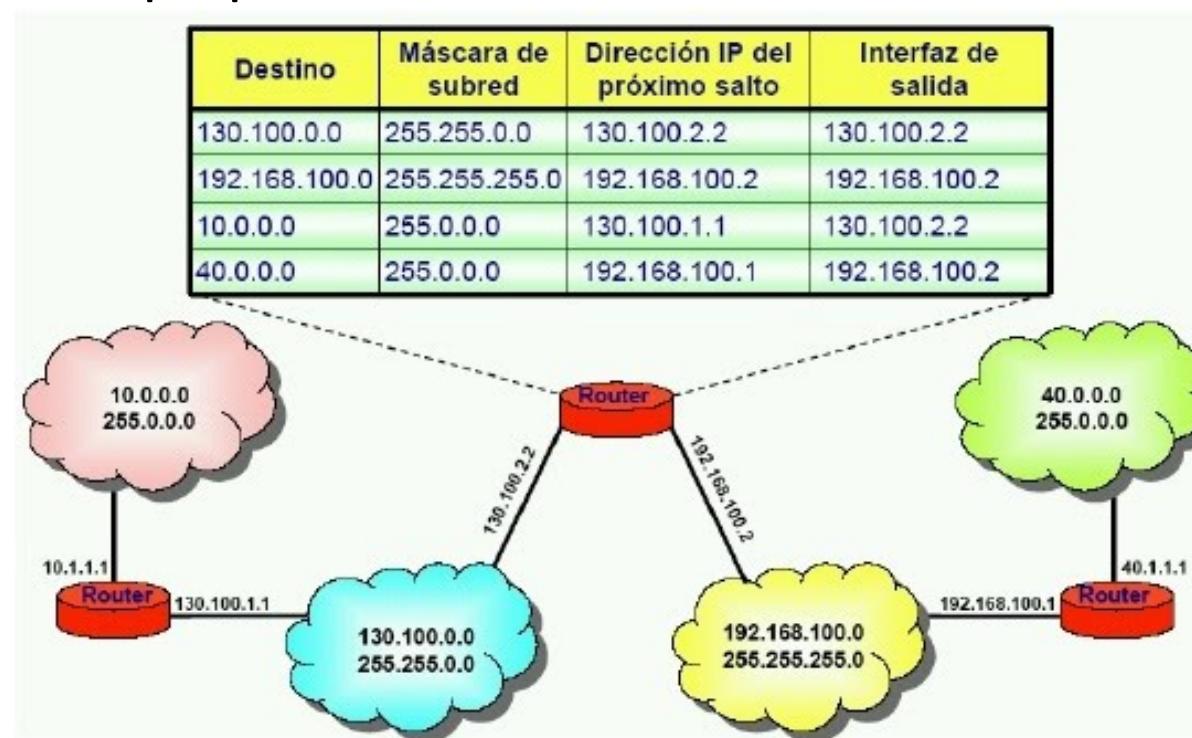
[Esta foto](#) de Autor desconocido está bajo licencia [CC BY-SA](#)

Tema 2: 2.8 Protocolos de encaminamiento

- Las tablas dinámicas tienen la ventaja de que se actualizan dependiendo del estado de la red, buscando caminos alternativos ante una desconexión, congestión, ...
- Los *routers* tienen que disponer de una “idea” de la arquitectura de la red incluyendo el “coste del enlace” en base a alguna métrica para saber el camino más corto.
- Métricas en base a algún coste:
 - Minimizar el número de routers o “saltos”.
 - Maximizar el caudal (ancho de banda).
 - Minimizar el nivel de ocupación de los enlaces.
 - Minimizar el retardo producido en los enlaces.
 - Maximizar la fiabilidad de los enlaces (minimizar la tasa de errores).

Tema 2: 2.8 Protocolos de encaminamiento

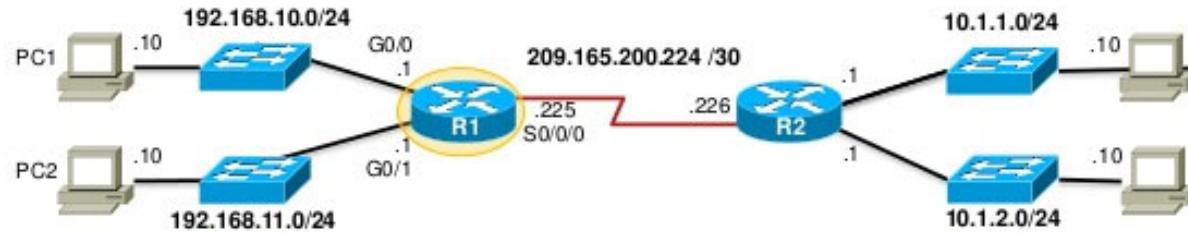
Para que sea posible el encaminamiento el **router** necesita averiguar por dónde encaminar los paquetes



Tema 2: 2.8 Protocolos de encaminamiento

Tablas de enrutamiento de router

Tabla de enrutamiento de router IPv4



```
R1#show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0 D 10.1.2.0/24 [90/21701121] via 209.165.200.226, 00:00:05, Serial0/0/0

192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks C 192.168.10.0/24 is directly connected, GigabitEthernet0/0 L 192.168.10.1/32 is directly connected, GigabitEthernet0/0

192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks C 192.168.11.0/24 is directly connected, GigabitEthernet0/1 L 192.168.11.1/32 is directly connected, GigabitEthernet0/1 209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks C 209.165.200.224/30 is directly connected, Serial0/0/0 L 209.165.200.225/32 is directly connected, Serial0/0/0

Tema 2: 2.8 Protocolos de encaminamiento

- Los protocolos de encaminamiento se basan en calcular la mejor ruta en base a una métrica. Y en cómo comparten la información entre los *routers*.
- Se pueden clasificar según donde se decide el camino:
 - **Encaminamiento fijado en el origen:** se decide en el origen y la información de encaminamiento se incluye en los paquetes (orientado a conexión)
 - **Encaminamiento salto a salto:** el origen sólo necesita conocer el siguiente paso hasta llegar al destino.
Lo importante es cómo saber el siguiente salto es el trabajo de la red (*routers*)

Tema 2: 2.8 Protocolos de encaminamiento

- Para que sea posible el encaminamiento es necesario definir tablas de encaminamiento. Estas pueden ser:
 - **Estáticas:** son generadas por el administrador de la red.
 - Se cargan anticipadamente.
 - El cálculo de las rutas es costoso.
 - Se realiza de forma centralizada.
 - Y rara vez la ruta cambia.
 - **Dinámicas:** son generadas por los protocolos de encaminamiento.
 - Cada *router* decide la ruta óptima en base a información obtenida por el **estado de la red**.
 - El cálculo de la ruta se hace en base a un **algoritmo**.
 - La ruta óptima puede cambiar con frecuencia.
- Las tablas pueden ser actualizadas periódicamente o cuando se solicite por algún evento.

Tema 2: 2.8 Protocolos de encaminamiento

- Otro clasificación en base a la **localización de la información de encaminamiento**:
 - **Global**: cada *router* contiene información completa de la topología de la red, de los enlaces y los envía a todos los *routers*.
Ejemplo: **encaminamiento por estado de enlace**
 - **Distribuido o descentralizada**: cada *router* solo conoce e interactúa con sus vecinos.
Las rutas óptimas se calculan de forma **iterativa**.
Ejemplo: **encaminamiento por vector distancia**
- Hay 2 protocolos muy conocidos:
 - Algoritmo del protocolo **de encaminamiento vector distancia** (Bellman-Ford)
 - Algoritmo del protocolo de **encaminamiento del estado de enlace** (camino más corto)

Tema 2: 2.8 Protocolos de encaminamiento

- Algoritmo del protocolo de **encaminamiento vector distancia** (Bellman-Ford)
 - Se basa en el número de saltos normalmente (otras métricas retardo, número de paquetes en cola, ...)
 - Los *routers* no conocen toda la topología de la red.
 - Inicialmente los *routers* conocen la distancia hasta los siguientes *routers*
 - Los *routers* usan este tipo de protocolo para mantener información de la distancia de las redes conocidas.
 - Regularmente los *routers* adaptan sus tablas con la información que intercambian con sus vecinos.
 - Las tablas contienen la información [**interfaz de salida, distancia(métrica)**]
 - Las tablas se actualizan con el intercambio del **vector distancia** con sus vecinos.

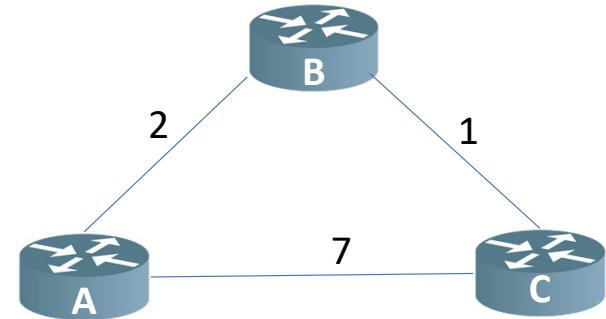
Tema 2: 2.8 Protocolos de encaminamiento

- Algoritmo del protocolo de **encaminamiento vector distancia** (Bellman-Ford)

Tabla de A		
Destino	Nodo Siguiente	Distancia
A	-	0
B	B	2
C	C	7

Tabla de B		
Destino	Nodo Siguiente	Distancia
A	A	2
B	-	0
C	C	1

Tabla de C		
Destino	Nodo Siguiente	Distancia
A	A	7
B	B	1
C	-	0



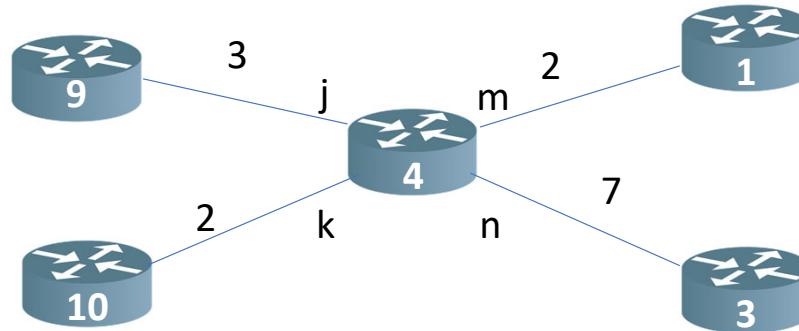
Se recibe VD de B

Tabla de A		
Destino	Nodo Siguiente	Distancia
A	-	0
B	B	2
C	B	3

Tabla de C		
Destino	Nodo Siguiente	Distancia
A	B	3
B	B	1
C	-	0

Tema 2: 2.8 Protocolos de encaminamiento

- Algoritmo del protocolo de **encaminamiento vector distancia** (Bellman-Ford)



Interfaz	Destino										
	1	2	3	4	5	6	7	8	9	10	11
j (+3)	12	3	15	3	12	5	6	18	0	7	15
k (+2)	5	8	3	2	10	7	4	20	5	0	15
m (+2)	0	5	3	2	19	9	5	22	2	4	7
n (+7)	7	2	0	7	8	5	8	12	11	3	2

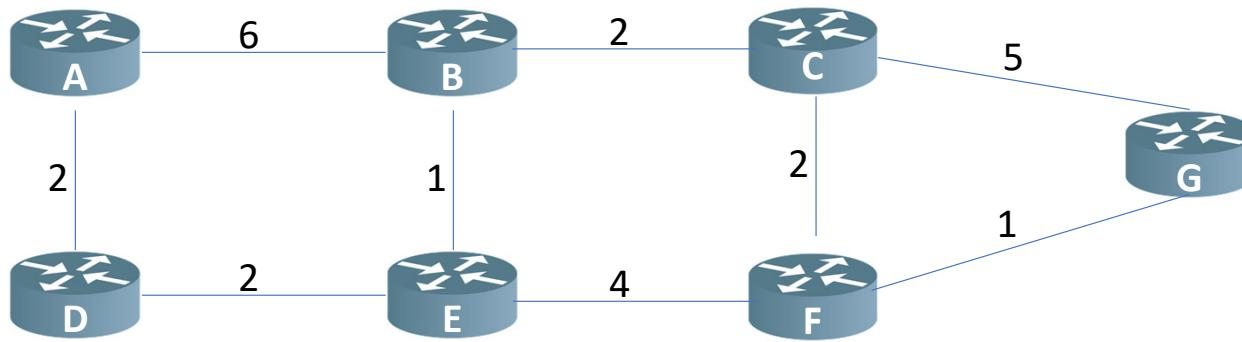
Nodo	Interfaz	Distancia
1	m	2
2	j	6
3	m	5
4	-	0
5	k	12
6	j	8
7	k	6
8	n	19
9	j	3
10	k	2
11	n	9

Tema 2: 2.8 Protocolos de encaminamiento

- Algoritmo del protocolo de **encaminamiento del estado de enlace** (camino más corto)
 - Se selecciona la ruta basado en la evaluación dinámica del camino más corto entre dos redes.
 - Cada *router* mantiene un “mapa” de la topología de la red.
 - Esta topología se adapta regularmente testeando el alcance.
 - La mejor ruta se calcula bajo cierta métrica.
 - Este protocolo es más potente que el del vector-distancia
- Protocolos híbridos que combinan las características de los dos, *path-vector*.

Tema 2: 2.8 Protocolos de encaminamiento

- **Algoritmo Dijkstra**

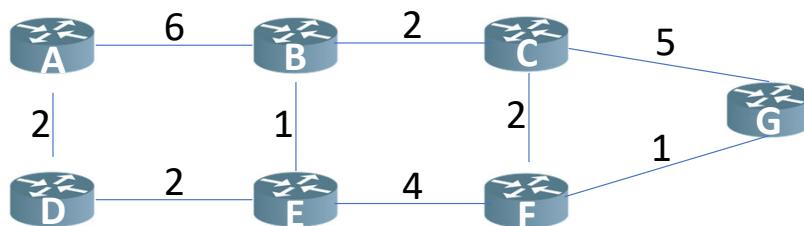


A	B	C	D	E	F	G
B - 6	A - 6	B - 2	A - 2	B - 1	C - 2	C - 5
D - 2	C - 2	F - 2	E - 2	D - 2	E - 4	F - 1
	E - 1	G - 5		F - 4	G - 1	

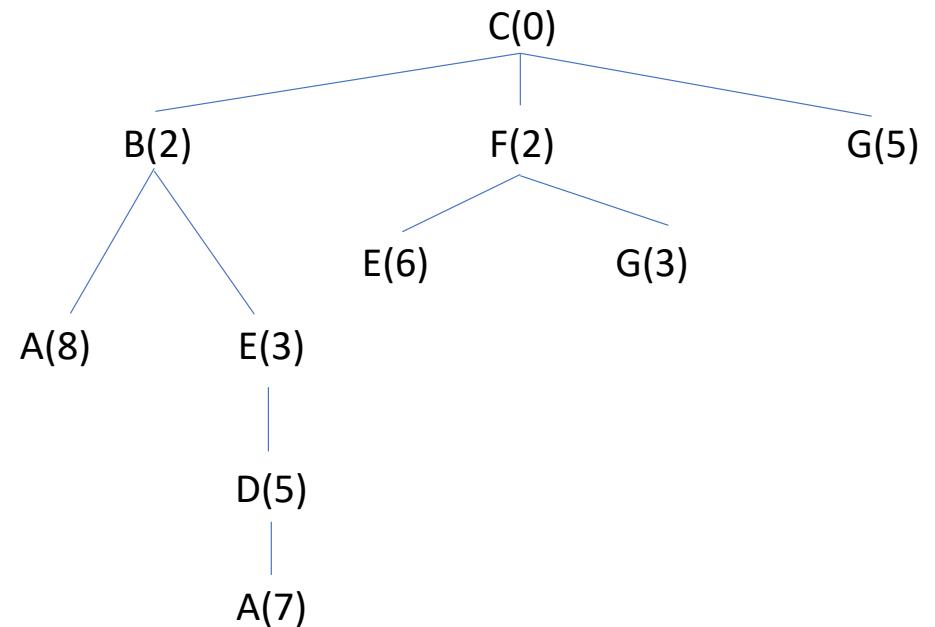
Esta foto de Autor desconocido está bajo licencia [CC BY-SA](#)

Tema 2: 2.8 Protocolos de encaminamiento

- **Algoritmo Dijkstra**



A	B	C	D	E	F	G
B - 6	A - 6	B - 2	A - 2	B - 1	C - 2	C - 5
D - 2	C - 2	F - 2	E - 2	D - 2	E - 4	F - 1
	E - 1	G - 5		F - 4	G - 1	



Esta foto de Autor desconocido está bajo licencia [CC BY-SA](#)

Tema 2: 2.8 Protocolos de encaminamiento

- **Arquitectura Core**

- *Routers core*: a medida que Internet fue creciendo la cantidad de información de encaminamiento también creció. Fue necesario crear una arquitectura de 2 niveles. Protocolos de encaminamiento *Gateway-to-Gateway Protocol (GGP)*
- *Routers non-core*: fueron puestos en la periferia y contenían parte de la información de encaminamiento. Protocolos *Exterior Gateway Protocol (EGP)*

Pero esta arquitectura no era escalable y no podía ajustarse al crecimiento que hacía Internet. Para resolver estas limitaciones surge los sistemas autónomos.

- **Sistemas autónomos**

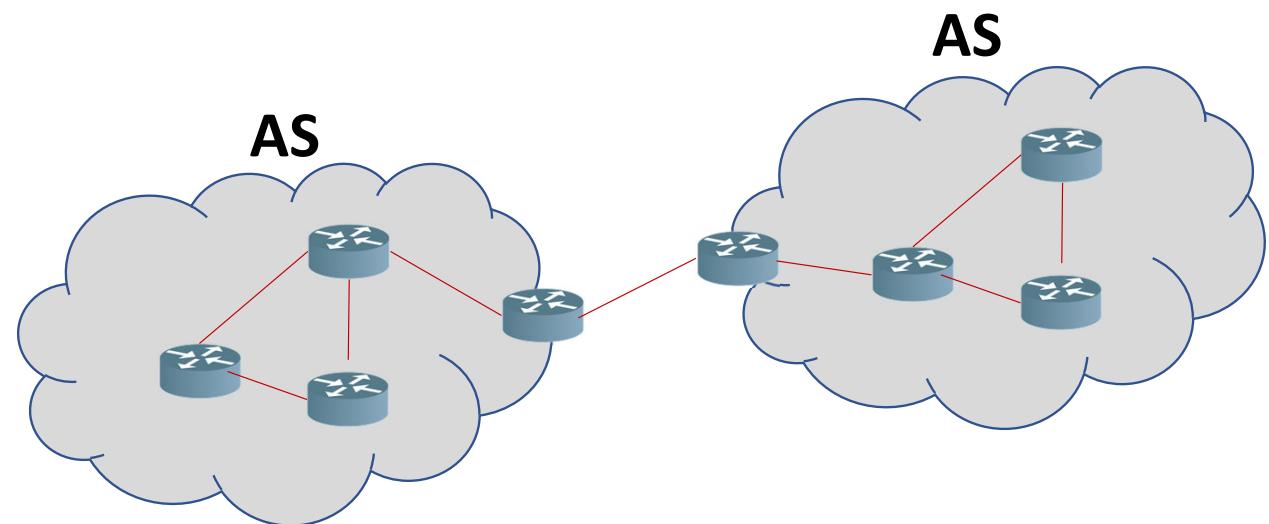
- Sistema autónomo (AS): es una red administrada independientemente como si fuese un dominio (ulpgc.es).
- Se trata de una arquitectura descentralizada.
- Internet como conjunto de AS independientes y gestionados por una organización.
- Los detalles que suceden dentro del AS son ocultos para el resto.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos

- Protocolos de encaminamiento **interior**: protocolos que intercambian información de encaminamiento dentro de un AS.
- Protocolos de encaminamiento **exterior**: protocolos que intercambian información de encaminamiento entre AS.

- En un sistema autónomo hay:
 - **Routers internos**
 - **Routers externos (border)**



[Esta foto](#) de Autor desconocido está bajo licencia [CC BY-SA](#)

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno vector distancia: *RIP, RIP-2, RIPng*

1. RIP (*Routing Information Protocol*)

- Está basado en el algoritmo de encaminamiento de **vector-distancia** (Bellman-Ford)
- Es uno de los primeros protocolos, y a pesar de sus limitaciones se sigue utilizando.
- Cada *router* envía la información de su tabla de encaminamiento mediante un mensaje especial usando UDP a todas las redes a las que está conectado.
- Los *routers* actualizan la información de sus tablas añadiendo 1 salto extra.
- Cuando un *router* adapta sus tablas las comparte con sus vecinos y así sucesivamente.
- Es un protocolo sencillo de implementar sobre todo para ASes pequeños.
- Los saltos no es la mejor métrica.
- Sólo permite 15 saltos.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno vector distancia: *RIP, RIP-2, RIPng*

2. RIP-2

- Incluye un nuevo formato de los mensajes.
- Contempla el esquema de direcciones *classless*.
- Autenticación.
- Multicast

3. RIPng (*next generation IPv6*)

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno vector distancia: *RIP, RIP-2, RIPng*

- Para cada red, se incluye la siguiente información:
 - Dirección de la red.
 - La distancia (coste).
 - La interfaz de salida.
- La medida de distancia es el **salto (hop)**.
- Si un *router* se conecta a la red directamente, la distancia es **1**. Si tiene que pasar por otro *router* la distancia es **2**, etc.
- Si una ruta es inaccesible tiene distancia **16 (∞)**.
- Cada *router* envía su tabla a otros *routers*.
- Cualquier *router* que reciba información de que puede alcanzar una ruta con **N** saltos, la distancia será **N+1**.
- La información se propaga por la red.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno vector distancia: *RIP, RIP-2, RIPng*

- Los mensajes se envían utilizando el protocolo **UDP** y puerto 520 (RIP-1 y RIP-2) y 521 (RIPng).
- Hay dos mensajes típicos en estos protocolos (RIP-1, RIP-2 y RIPng):
 - ***RIP Request***: mensaje enviado por un *router* a otro *router* solicitándoles toda la tabla o parte de ella.
 - ***RIP Response***: mensaje enviado por un *router* a otro *router*, el cual contiene la tabla o parte de ella. A pesar de su nombre **no solo se envía como respuesta a un mensaje *RIP Request***.
- Cuando un *router* se enciende, después de la inicialización, solicita información actualizada de la red a sus vecinos. Los *routers* responden con ***RIP Response***.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno vector distancia: *RIP, RIP-2, RIPng*

- Los *routers* no envían normalmente un mensaje **RIP Request** pidiendo la información. Se utiliza un *timer* (30 segundos).
- Cuando el *timer* expira, un mensaje **RIP Response** (no solicitado) se envía con la información.
- La información de la tabla no se considera nunca válida. Ya que una ruta puede dar error, y ser inalcanzable.
- Para evitar esta situación, cuando una ruta se registra en la tabla se activa otro *Timeout timer* (180 segundos).
 - Si se recibe un mensaje **RIP Response** con la información de la ruta, este *timer* se inicializa.
 - Si no la ruta fija a 16 el valor de la distancia y se marca para borrar, se activa un tercer *timer* (*Garbage-Collection*) de 120 segundos. Pasado este tiempo si no se ha levantado la ruta se elimina de la tabla.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno vector distancia: *RIP, RIP-2, RIPng*

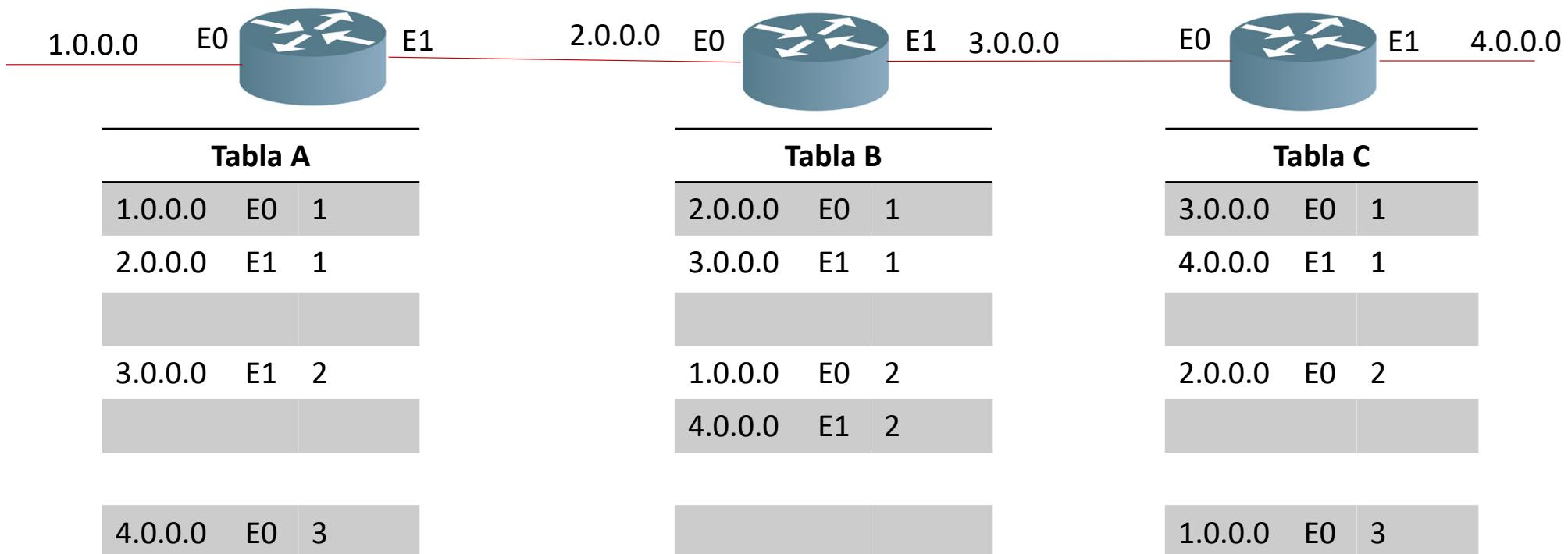
Desventajas

- Un algoritmo que es lento para que converja. Requiere de mucho tiempo para que toda la información llegue a todos los *routers*.
- Búcles.
- La métrica de saltos, no es la más adecuada.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno vector distancia: *RIP, RIP-2, RIPng*

1. RIP (*Routing Information Protocol*)



Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno estado-enlace: *OSPF (Open Shortest Path First)*

- Algoritmo que intenta solucionar los problemas de los protocolos RIP.
- Permite seleccionar rutas dinámicamente basados en el estado de la red.
- Permite soportar una topología jerárquica.
- Es más complejo que RIP.
- Sucesor de RIP, trabaja con los esquemas de direccionamiento VLSM y CIDR.
- El principal concepto detrás de OSPF es una estructura de datos denominada *link-state database LSDB (Link-State DataBase)* (base de datos de estado de enlace) de datos para construir la tabla y construir **un árbol con el camino más corto**.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno estado-enlace: OSPF (*Open Shortest Path First*)

Tipos de mensajes en OSPF

1. ***Hello***: permite descubrir a los *routers* vecinos.
2. ***Database Description***: mensajes que contiene información acerca de la base de datos.
3. ***Link State Request***: mensajes que solicitan a un *router* para actualizar la información o parte de la base de datos. En estos mensajes se especifican que rutas se quiere tener información.
4. ***Link State Update***: mensajes que contienen información del estado de las rutas. Y responde a un ***Link State Request***.
5. ***Link State Acknowledgment***: mensaje de confirmación a ***Link State Update***.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno estado-enlace: *OSPF (Open Shortest Path First)*

- Algoritmo que intenta solucionar los problemas de los protocolos RIP.
- Permite seleccionar rutas dinámicamente basados en el estado de la red.
- Permite soportar una topología jerárquica.
- Es más complejo que RIP.
- Sucesor de RIP, trabaja con los esquemas de direccionamiento VLSM y CIDR.
- El principal concepto detrás de OSPF es una estructura de datos denominada *link-state database LSDB (Link-State DataBase)* (base de datos de estado de enlace) de datos para construir la tabla y construir **un árbol con el camino más corto**.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno estado-enlace: **OSPF (Open Shortest Path First)**

- Construye un paquete LSP (Link State Packet) que contiene:
 - Información de quien lo envía
 - La lista de sus vecinos y quien lo envía.
- Este paquete LSP se envía por inundación a todos los routers de la red.
- Para controlar la inundación:
 - Los paquetes LSP se enumeran secuencialmente y tienen un tiempo de vida limitado.
 - No se envían por la ruta que llega.
- Se envía al principio y luego si hay cambios en la red.
- Calcula las rutas óptimas como el algoritmo de Dijkstra.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento interno estado-enlace: OSPF (*Open Shortest Path First*)

Tipos de mensajes en OSPF

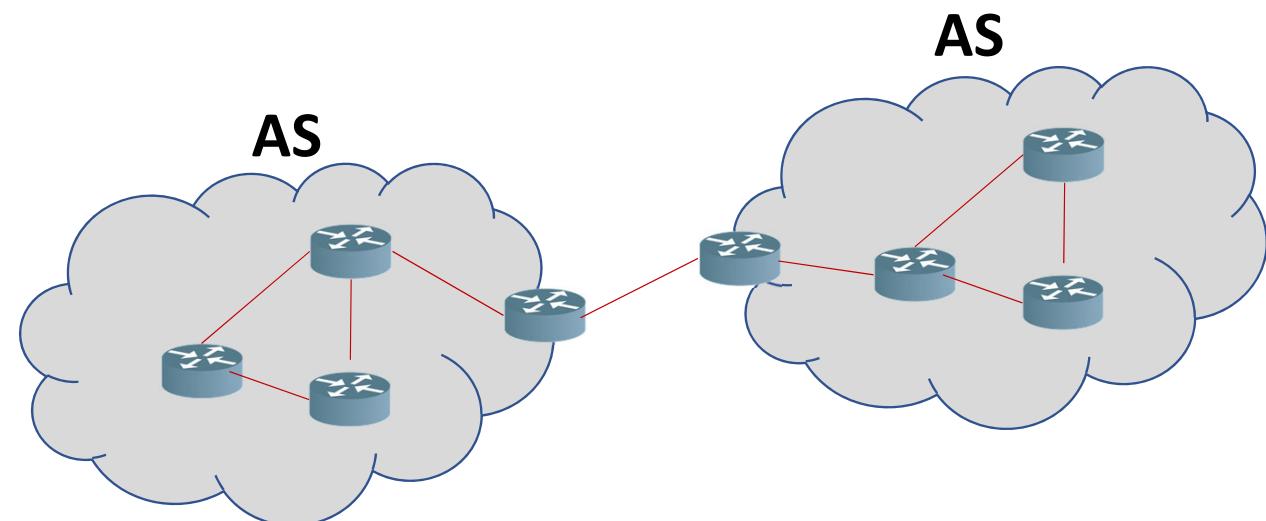
1. ***Hello***: permite descubrir a los *routers* vecinos.
2. ***Database Description***: mensajes que contiene información acerca de la base de datos.
3. ***Link State Request***: mensajes que solicitan a un *router* para actualizar la información o parte de la base de datos. En estos mensajes se especifican que rutas se quiere tener información.
4. ***Link State Update***: mensajes que contienen información del estado de las rutas. Y responde a un ***Link State Request***.
5. ***Link State Acknowledgment***: mensaje de confirmación a ***Link State Update***.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos

- Protocolos de encaminamiento **interior**: protocolos que intercambian información de encaminamiento dentro de un AS.
- Protocolos de encaminamiento **exterior**: protocolos que intercambian información de encaminamiento entre AS.

- En un sistema autónomo hay:
 - **Routers internos**
 - **Routers externos (border)**



[Esta foto](#) de Autor desconocido está bajo licencia [CC BY-SA](#)

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

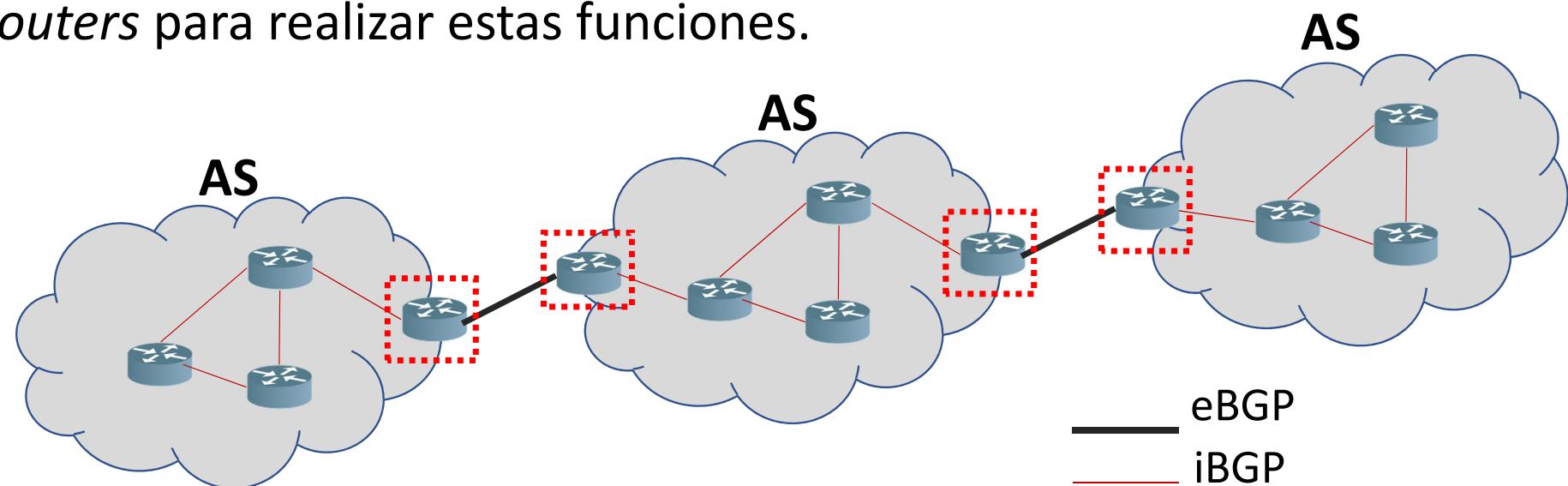
- Protocolo importante de funcionamiento en Internet.
- Es el enlace que une redes muy diferentes permitiendo el encaminamiento.
- RFCs:
 - RFC 1105 (1989 BGP-1)
 - RFC 1163(1990 BGP-2)
 - RFC 1267 (1991 BGP-3)
 - RFC 1654 (1994 BGP-4)
 - RFC 1771 (1995 BGP-4)
 - Suplementos (adicionales): RFC 1772, RFC 1773, RFC 1774
- Cualquier modificación de este protocolo implica coordinar a muchas organizaciones.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

- Su función primordial es la de intercambiar información entre 2 sistemas autónomos y determinar la ruta sin conocer lo que pasa dentro del AS.
- En cada **sistema autónomo AS**, se designa como mínimo uno o más *routers* para realizar estas funciones.



Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

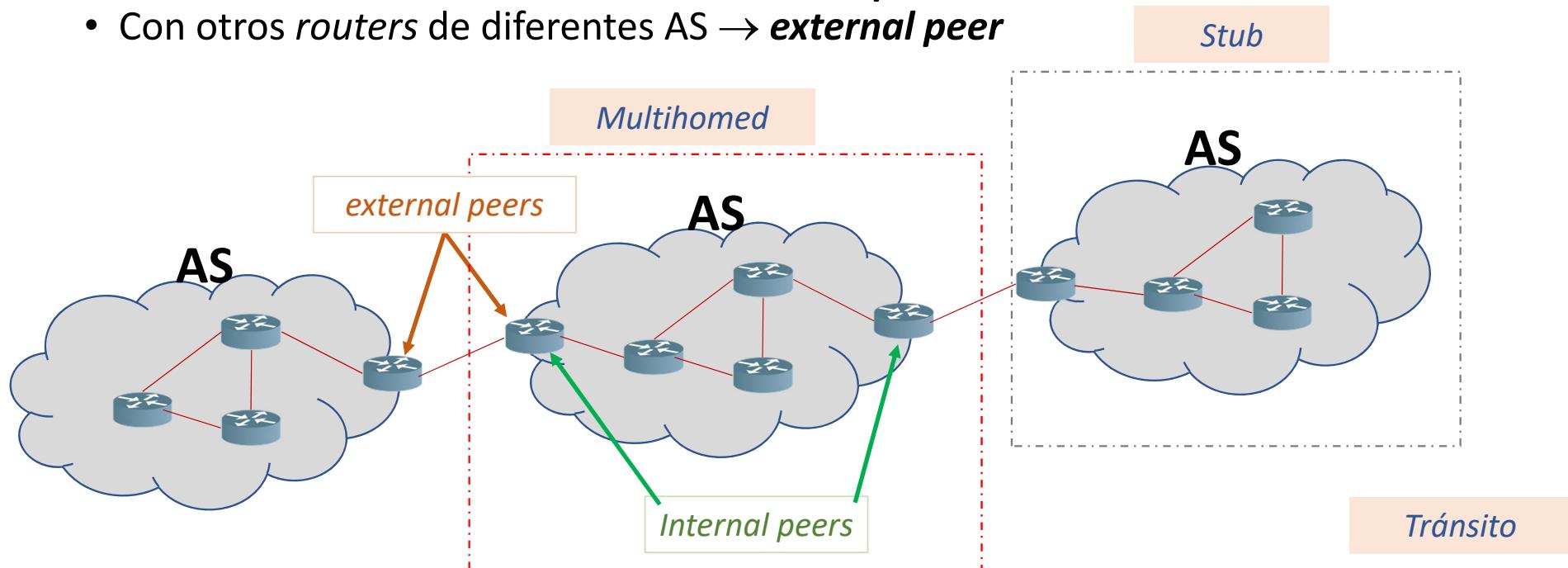
- En cada *router* BGP se almacena información sobre las **redes** y **rutas** en la tabla de encaminamiento (*Routing Information Bases*).
 - La tabla de encaminamiento contiene información más completa.
 - Las rutas se calculan de manera eficiente, evitando bucles y otros problemas.
- Esta información se intercambia entre *routers* BGPs y se propaga a través de la red.
- BGPs soporta cualquier topología de ASs.
- BGP establece sesiones con otros *routers* utilizando el protocolo TCP (puerto 179) para transmitir sus mensajes .
- BGP incluye un esquema de autenticación por seguridad.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

- Los *routers* configurados para usar BGP se denominan *BGP speaker*. Estos dispositivos intercambian información con:
 - Otros *routers BGP* del mismo AS → *internal peer*
 - Con otros *routers* de diferentes AS → *external peer*



Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

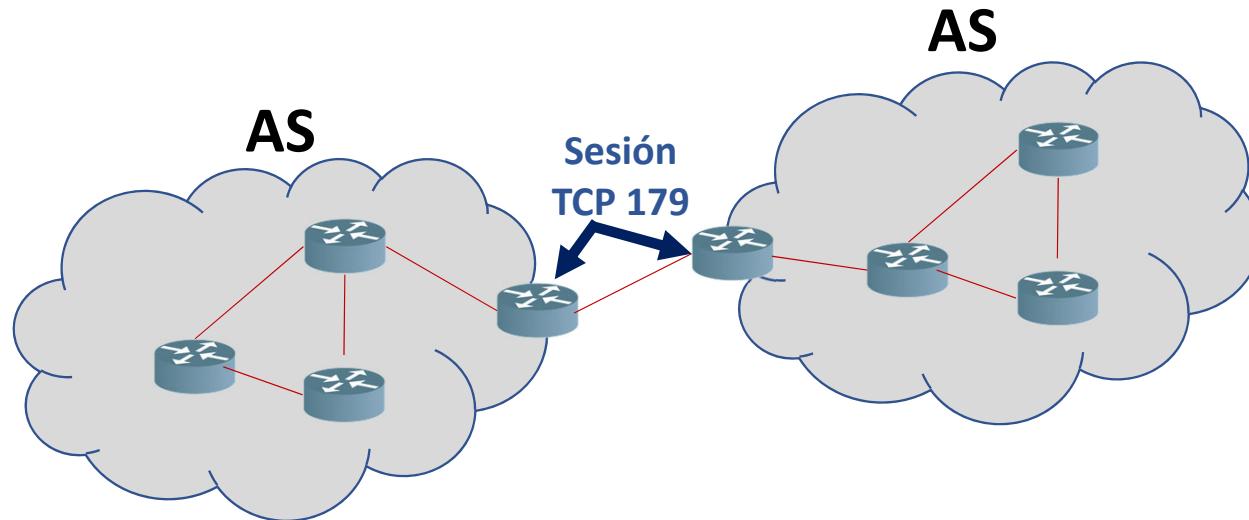
- Tipos de tráficos:
 - Tráfico local: se genera y termina en el mismo AS.
 - Tráfico de tránsito: ni se genera, ni se finaliza en el AS.
- Políticas de encaminamiento:
 - Políticas de no tránsito.
 - Políticas de tránsito restringido. A unos ASs si y a otros no.
 - Políticas de tránsito basados en algún criterio. Se permite cuando se cumpla el/los criterios (horario, capacidad, etc.)

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

- BGP utiliza el protocolo vector distancia, los detalles de la red están ocultos. Los nodos solo necesitan saber el siguiente salto.
- La información de encaminamiento se comparte mediante las sesiones TCP.



Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

- Todas las rutas activas se intercambian y mientras esté activa, los vecinos intercambian información actualizada.
- BGP es un protocolo incremental. Es decir después de que una tabla de encaminamiento es compartida, sólo se comparte los cambios:
 - Nuevas rutas
 - Desaparecen rutas
 - Cambios en los atributos de las rutas.
- BGP envía mensajes periódicamente (60 segundos) de 19 bytes para mantener la conexión.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

- Mensajes BGP:
 - OPEN: abre una sesión.
 - UPDATE: mensaje con información de encaminamiento, nueva ruta o rutas inalcanzables, etc. Con un mismo mensaje se dan de alta o bajas.
 - KEEPALIVE: mantiene la sesión en ausencia de mensajes UPDATE.
 - NOTIFICATION: informa de errores o cierra las sesiones.

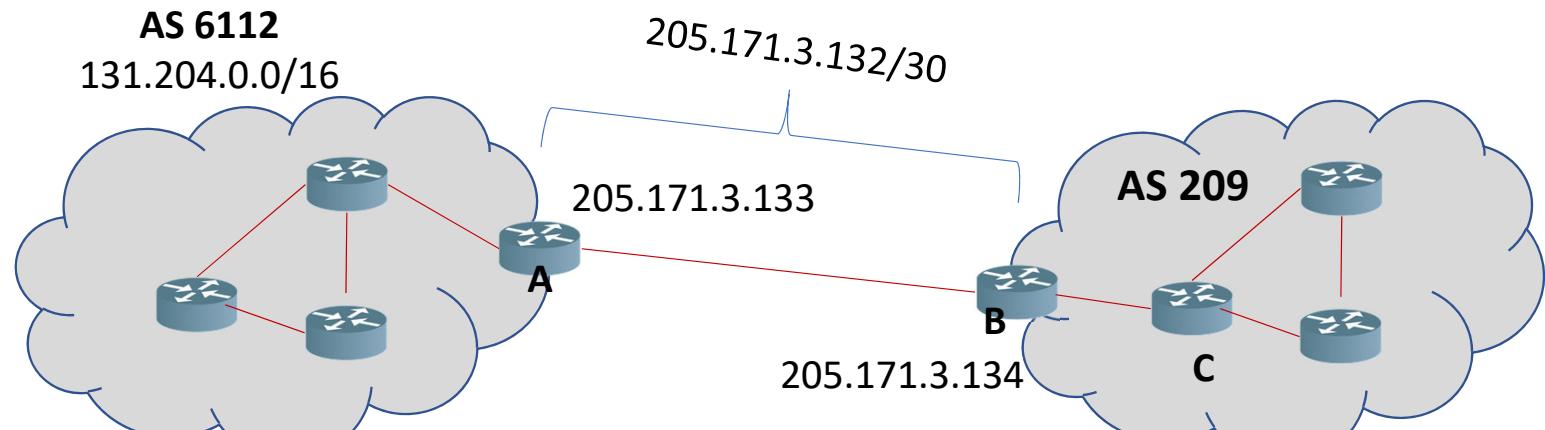
Origen	AS_Path	Next_Hop	MED	Local Preference	...
--------	---------	----------	-----	------------------	-----

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

Ejemplo: Consideremos la red de la figura, en la que una fuente de AS 209 desea llegar a un destino en el AS 6112. En este caso, el router A anunciará la dirección IP 131.204.0.0/16 al router B con un próximo salto de 205.171.3.133. Con BGP, la ruta se especifica con un prefijo de destino, por ejemplo, 131.204.0.0/16, más los atributos de la ruta que incluyen el camino del AS, por ejemplo, 6112, 209 (el camino contiene dos AS), y la dirección IP del siguiente salto, por ejemplo, 205.171.3.133.



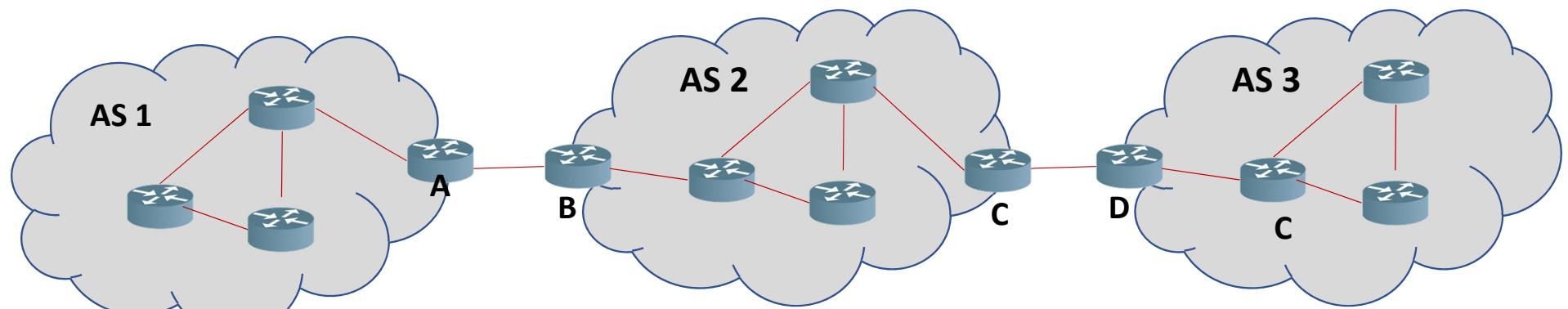
«Introduction to Computer Networks and Cybersecurity [Book]». Disponible en: <https://www.oreilly.com/library/view/introduction-to-computer/9781466572133/>.

Tema 2: 2.8 Protocolos de encaminamiento

Protocolos de encaminamiento exterior: BGP y EGP

BGP (*Border Gateway Protocol*)

Ejemplo: la red de la Figura, el AS 1 hace publicidad de AS 1 a AS 2, y luego el AS 2 hace publicidad a AS 3. El atributo de ruta AS en la “publicidad” enviada por el AS 1 es **AS 1** y el enviado por el AS 2 es **AS2 AS1**. El AS 3 envía el anuncio con el atributo **AS3 AS2 AS1**.



«Introduction to Computer Networks and Cybersecurity [Book]». Disponible en: <https://www.oreilly.com/library/view/introduction-to-computer/9781466572133/>.