

Arquitectura de protocolos IP



INTERCONEXIÓN DE REDES.....	4
1 TCP-IP: ESTRUCTURA DE PROTOCOLOS Y CONCEPTOS GENERALES	5
<i>Introducción a la Sección 1</i>	5
<i>Introducción</i>	6
<i>El modelo DoD y OSI.....</i>	7
<i>Arquitectura TCP-IP</i>	9
<i>Introducción al escenario de comunicación con TCP-IP.....</i>	11
<i>Escenario de comunicación con TCP-IP (I).....</i>	12
<i>Escenario de comunicación con TCP-IP (II)</i>	16
<i>Escenario de comunicación con TCP-IP (III)</i>	18
<i>Escenario de comunicación con TCP-IP (IV)</i>	20
<i>Escenario de comunicación con TCP-IP (V).....</i>	22
<i>Conclusión.....</i>	23
2 DIRECCIONAMIENTO BÁSICO	24
<i>Introducción a la Sección 2</i>	24
<i>Direcciones IP.....</i>	25
<i>Formato de las Direcciones IP y Notaciones</i>	26
<i>Introducción a estructura de direcciones IP</i>	28
<i>Estructura de las Direcciones IP.....</i>	29
<i>Máscara de red.....</i>	30
<i>Relación de ideas clave</i>	31
<i>¿A quién identifica una Dirección IP?</i>	32
<i>Clases de Direcciones IP.....</i>	33
<i>Más sobre clases de Direcciones IP.....</i>	34

<i>Direcciones públicas y Direcciones privadas</i>	36
<i>Direcciones de Difusión o Broadcast.....</i>	37
<i>Difusión dirigida</i>	38
<i>Otras direcciones restringidas</i>	39
<i>Conclusión.....</i>	40
3 PRINCIPIOS DE ENCAMINAMIENTO.....	41
<i>Introducción a la Sección 3.....</i>	41
<i>Encaminamiento: definición.....</i>	42
<i>Tablas de Encaminamiento</i>	43
<i>Tipos de Encaminamiento</i>	44
<i>Clasificación de protocolos de encaminamiento.....</i>	45
<i>Algoritmo vector-distancia.....</i>	46
<i>Algoritmo estado-enlace.....</i>	52
<i>Ejemplo.....</i>	53
<i>Formas de ver el encaminamiento.....</i>	55
<i>Encaminamiento con clase (CLASSFUL).....</i>	56
<i>Encaminamiento sin clase (CLASSLESS).....</i>	57
<i>Conclusión.....</i>	58
4 DIRECCIONAMIENTO IP EXTENDIDO	59
<i>Introducción a la Sección 4.....</i>	59
<i>Introducción</i>	60
<i>Subnetting Clásico.....</i>	61
<i>Introducción a los cálculos.....</i>	63
<i>Cálculo con subnetting clásico.....</i>	64
<i>VLSM: Máscaras de subred de longitud variable</i>	67
<i>Ejemplo de VLSM.....</i>	68
<i>Ejemplo de VLSM.....</i>	70
<i>Direccionamiento actual en Internet</i>	73
<i>CIDR.....</i>	75
<i>Relación de ideas clave</i>	76
<i>Agregación de rutas</i>	77
<i>Ejemplo de agregación.....</i>	78
<i>Subredes jerarquizadas</i>	80
<i>Conclusión.....</i>	82
5 PROTOCOLOS DE ENCAMINAMIENTO.....	83
<i>Introducción a la Sección 5.....</i>	83
<i>Mapa de protocolos.....</i>	84
<i>Mapa de protocolos (II).....</i>	85
<i>Protocolo RIP.....</i>	86
<i>Temporizadores en RIP</i>	87
<i>Formato de mensajes RIP.....</i>	88
<i>Ejemplo de un mensaje RIP.....</i>	90
<i>Formato de mensajes RIP (II)</i>	91
<i>Formato de mensajes RIP (III)</i>	100
<i>Protocolo OSPF</i>	101
<i>Protocolo OSPF (II).....</i>	102
<i>Inicialización</i>	103
<i>Inicialización (II).....</i>	106
<i>Inicialización (III)</i>	107
<i>Propagación de LSAs</i>	108
<i>Propagación de LSAs (II)</i>	109
<i>Algoritmo SPF.....</i>	111
<i>Algoritmo SPF (II).....</i>	112
<i>Conclusión.....</i>	114
6 ARQUITECTURA DE ENCAMINAMIENTO.....	115
<i>Introducción a la Sección 6.....</i>	115
<i>Arquitectura original de Internet</i>	116
<i>Introducción a los sistemas autónomos.....</i>	117

<i>Sistemas autónomos</i>	118
<i>IGP - Protocolo de Gateway Interior</i>	119
<i>EGP - Protocolo de Gateway Exterior</i>	120
<i>Protocolo BGP4</i>	121
<i>Funcionamiento de BGP4</i>	122
<i>Formato de Mensajes BGP</i>	125
<i>Mensaje OPEN</i>	126
<i>Mensaje NOTIFICATION</i>	127
<i>Mensaje KEEPALIVE</i>	128
<i>Mensaje UPDATE</i>	129
<i>Estructura actual de Internet</i>	130
<i>Conclusión</i>	131

Interconexión de redes

Bienvenidos al curso **Arquitectura de protocolos IP.**

En este curso pretendemos:

- Conectar redes de área local (LAN) independientes para crear redes de área amplia (WAN) y, a su vez, conectar esas redes WAN para crear redes incluso mayores, es lo que se denomina **INTERNETWORKING** (Interconexión de redes).
- Conexión de redes que utilizan diferentes protocolos. De ahí surge la arquitectura de protocolos TCP-IP como arquitectura universal de comunicaciones de datos. Cuando hablamos de redes IP, hablamos de interconectar redes que utilizan estos protocolos y que requieren de elementos de interconexión especiales: los routers. Un router no es otra cosa que un dispositivo de interconexión de nivel 3.
- Entender todo lo relacionado con estos dispositivos y el protocolo en el que se sustentan: IP (protocolo internet). Además, analizaremos el esquema de direccionamiento IP en profundidad y la evolución que ha habido a lo largo de la historia de las redes IP....como Internet.

¡¡ADELANTE!!

1 TCP-IP: estructura de protocolos y conceptos generales

Introducción a la Sección 1

Vas a comenzar el apartado 1:

TCP-IP: estructura de protocolos y conceptos generales

El objetivo de este primer capítulo es recordar conceptos relacionados con el proceso de comunicación entre dispositivos IP, es decir, la arquitectura de protocolos y su terminología, para luego adentrarnos en el mundo del direccionamiento y el encaminamiento IP.

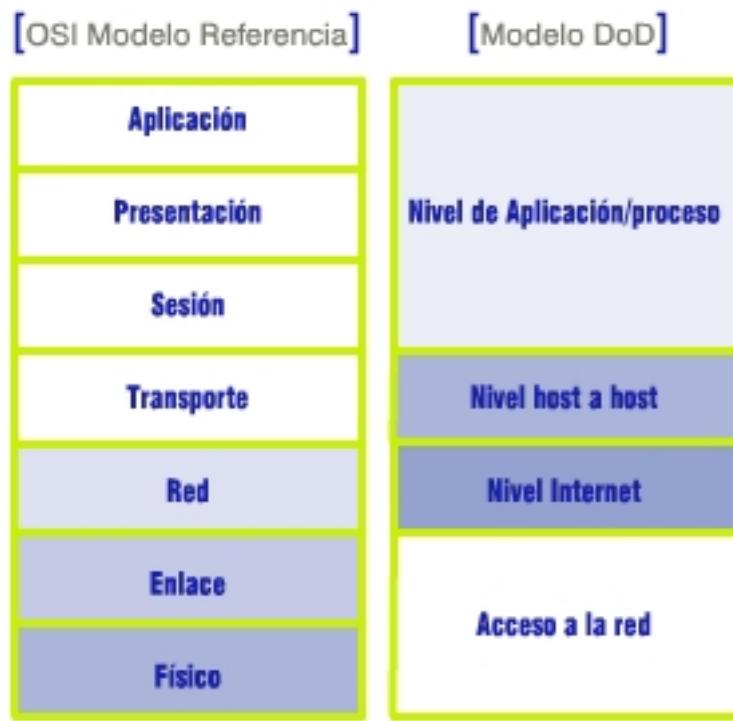
Introducción



La arquitectura de protocolos TCP-IP fue creada por el Departamento de Defensa (DoD) americano, para asegurar y preservar la integridad de los datos y mantener las comunicaciones en caso de una guerra nuclear.

En este primer capítulo recordaremos el modelo DoD y sus protocolos, para luego adentrarnos en el mundo del direccionamiento y el encaminamiento en redes IP, objetivo central de este curso.

El modelo DoD y OSI



El modelo DoD es una versión condensada del modelo OSI, con sólo cuatro niveles, según muestra la figura.

Aplicación

Se caracteriza por **multitud de protocolos estandarizados de facto**, cada uno de ellos especializado en una función determinada (descarga de páginas web, transferencia de ficheros, correo, etc.)

Nivel Host a Host

Realiza las **funciones relativas al nivel de transporte en OSI**, como creación de conexiones extremo a extremo fiables, secuenciamiento, etc.

Nivel Internet

Abarca los **protocolos relacionados con la transmisión lógica de los paquetes por toda la red**, el direccionamiento y el encaminamiento.

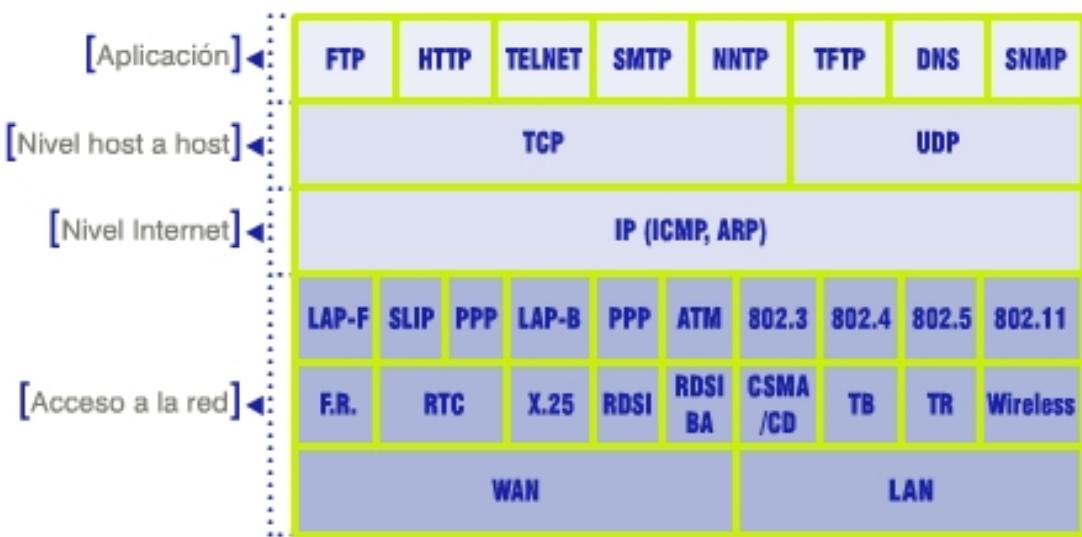
Nivel de acceso a la red

Abarca los niveles físico y de enlace del modelo OSI y corresponde a las tecnologías de red utilizadas. La principal característica del nivel Internet es su **independencia total y absoluta de cualquier tecnología de red utilizada**.

Arquitectura TCP-IP

Veamos ahora la arquitectura de protocolos asociada.

Recordemos los protocolos fundamentales de cada nivel.



En el nivel Internet encontramos el protocolo que define el mecanismo de envío no fiable de paquetes sin conexión: **Protocolo Internet, IP**.

Este protocolo, cuya unidad básica de transferencia de datos se denomina **DATAGRAMA**, incluye las direcciones IP origen y destino de los mensajes.

El software IP realiza funciones de encaminamiento, al elegir el camino por el cual enviar los datos.

Incluye una serie de normas sobre cómo los hosts y gateways (routers) deben procesar los paquetes, cómo y qué mensajes de error deben ser generados, y las condiciones bajo las cuales pueden descartarse paquetes.

Junto con el protocolo IP encontramos el **protocolo ICMP**, el cual provee de un mecanismo para que los routers notifiquen condiciones de error, al origen, en la entrega de datagramas.

El **protocolo ARP** provee de un mecanismo para "traducir" el direccionamiento lógico (IP) en direccionamiento físico de la LAN a la que se conecta el dispositivo (direcciones MAC).

En el nivel host a host encontramos dos protocolos:

El **Protocolo de Datagrama de Usuario (UDP)**, que proporciona un servicio no orientado a la conexión, y el mecanismo de identificación de procesos del nivel de aplicación mediante los llamados puertos.

El **protocolo TCP** que, por el contrario, provee de un mecanismo orientado a la conexión, con reconocimientos extremo a extremo, secuenciamiento y control de flujo.

Para realizar esta función, el protocolo TCP establece conexiones lógicas definidas a partir de los pares puerto y dirección IP origen y puerto y dirección IP destino, **permitiendo el multiproceso**.

Por último, los diferentes protocolos de nivel de aplicación, estándares de facto, realizan funciones específicas en relación a la aplicación utilizada. Por ejemplo:

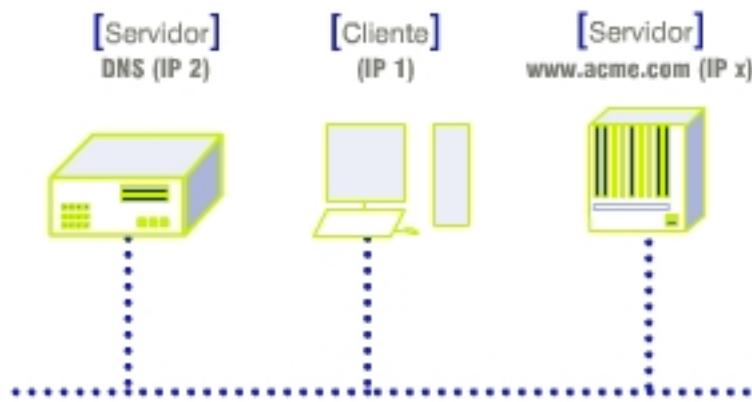
DNS: Protocolo de resolución de nombres de dominio.

HTTP: Protocolo de transferencia Hipertexto.

FTP: Protocolo de transferencia de ficheros.

SNMP: Protocolo Simple de Gestión de red...

Introducción al escenario de comunicación con TCP-IP



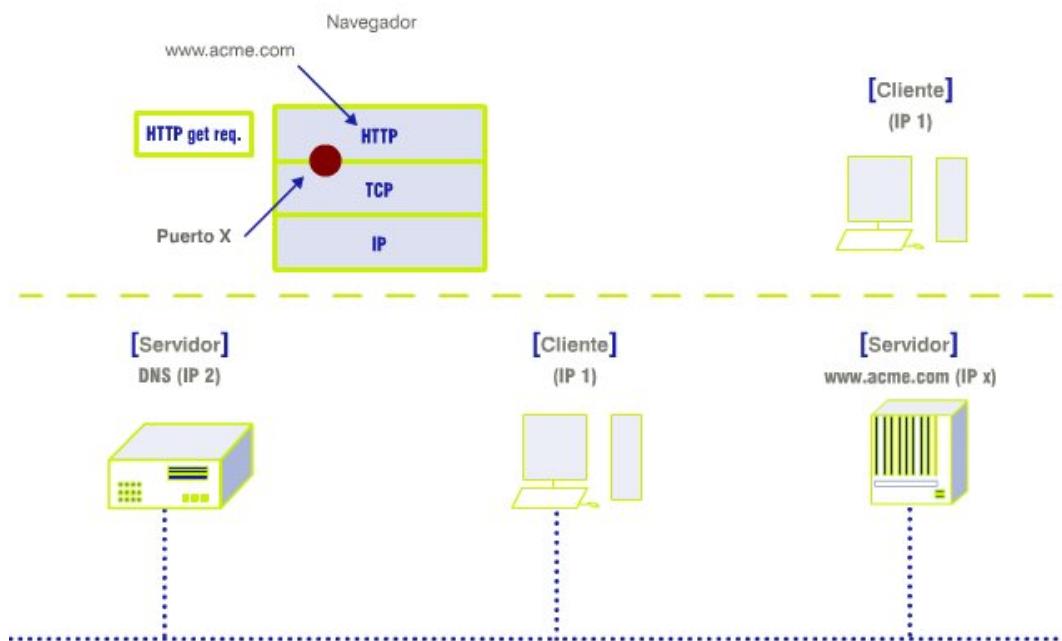
Finalmente, obviando los aspectos del encaminamiento que trataremos posteriormente en detalle, vamos a detallar el proceso de comunicación extremo a extremo entre un cliente y un servidor en una red IP.

Recuerda que, precisamente, las redes IP se caracterizan por ser una arquitectura cliente-servidor.

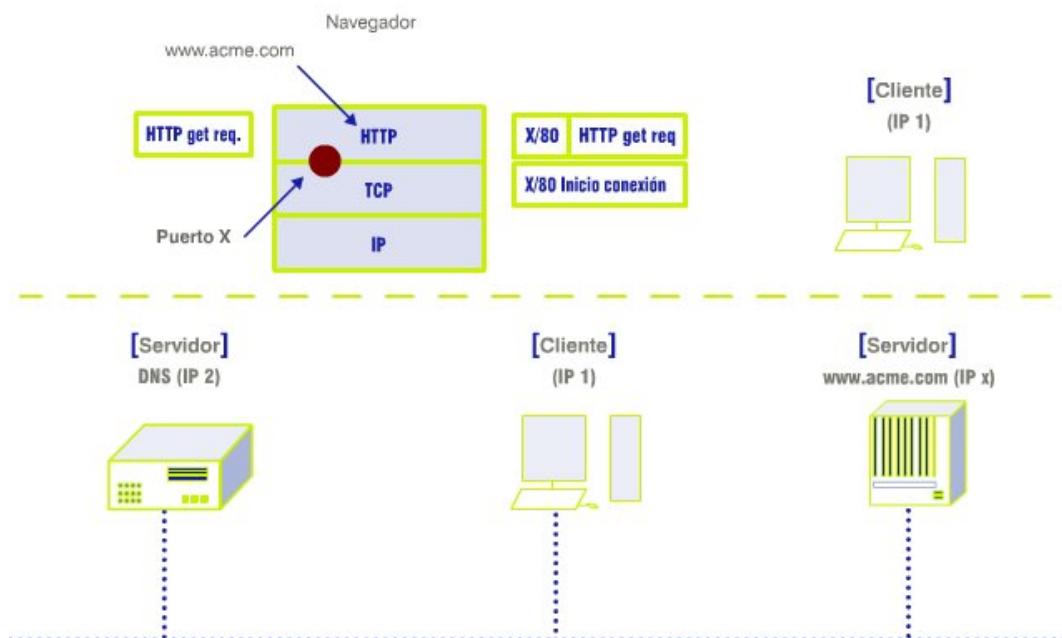
En el ejemplo que veremos a continuación, un cliente con dirección IP1 solicita las páginas de un servidor HTTP.

Veamos el proceso.

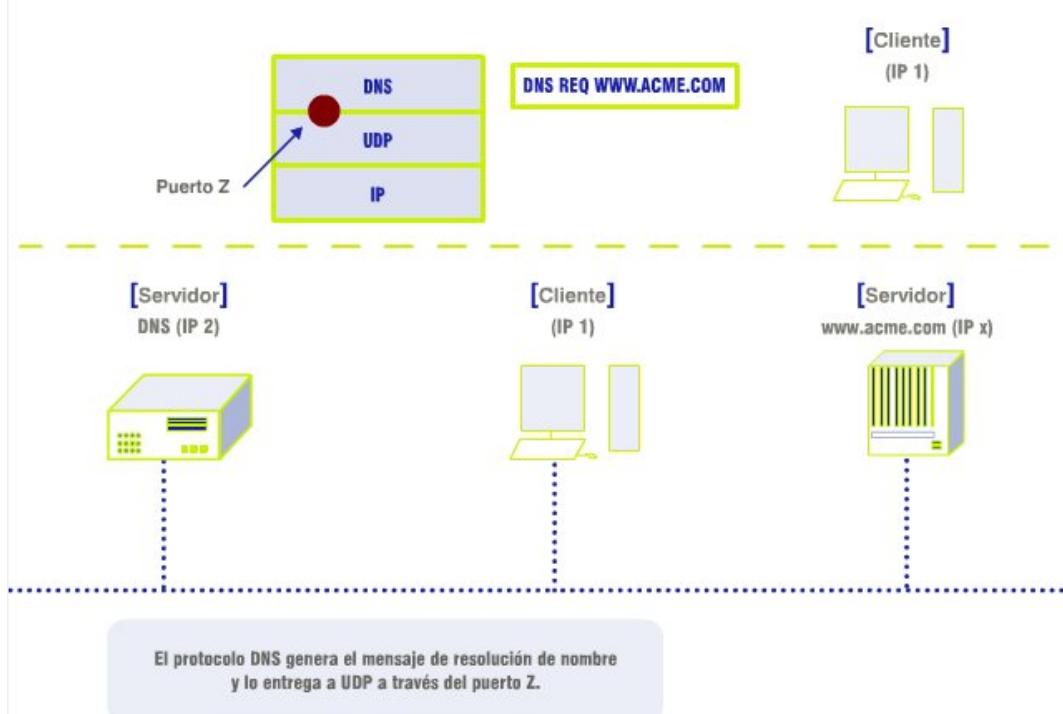
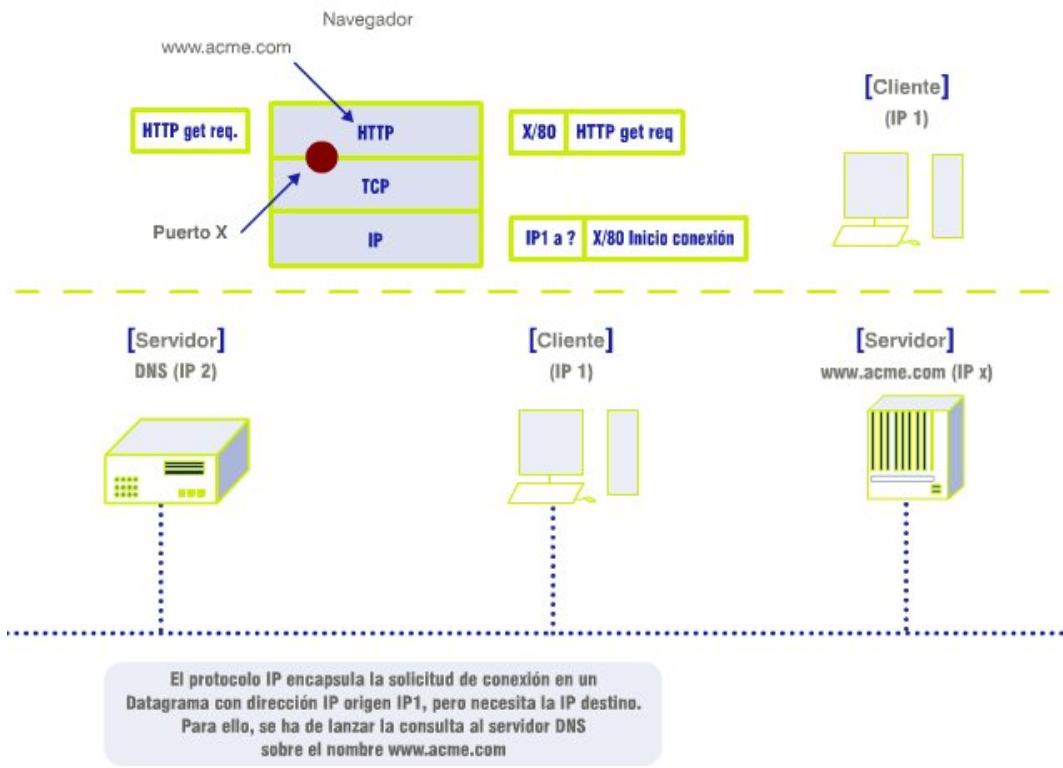
Escenario de comunicación con TCP-IP (I)

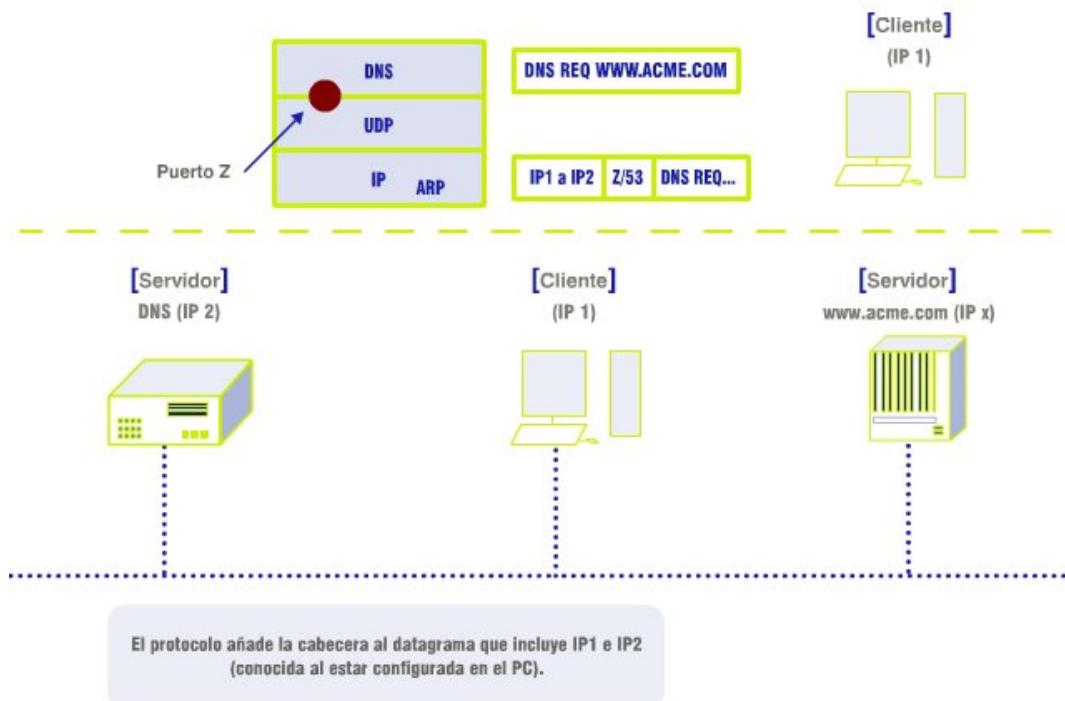
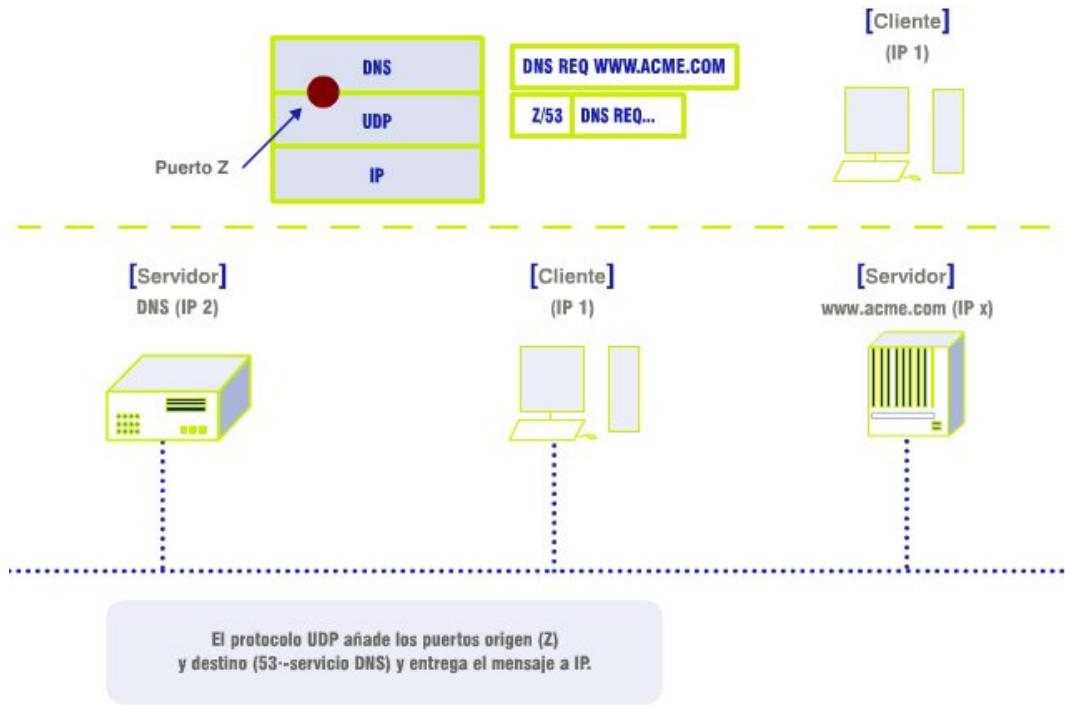


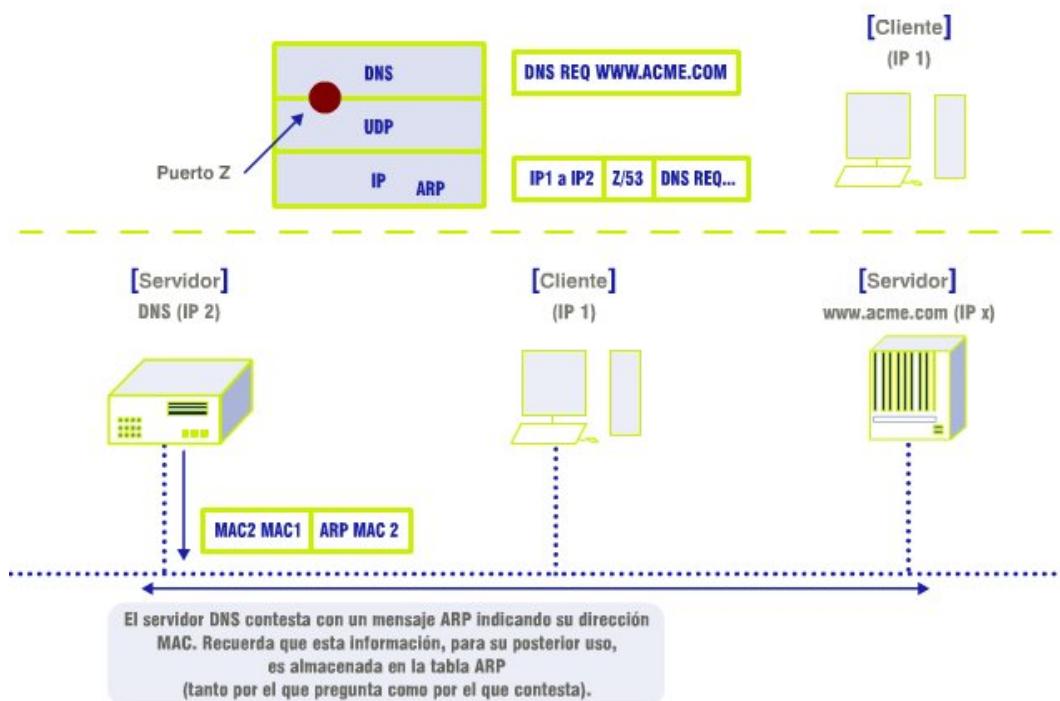
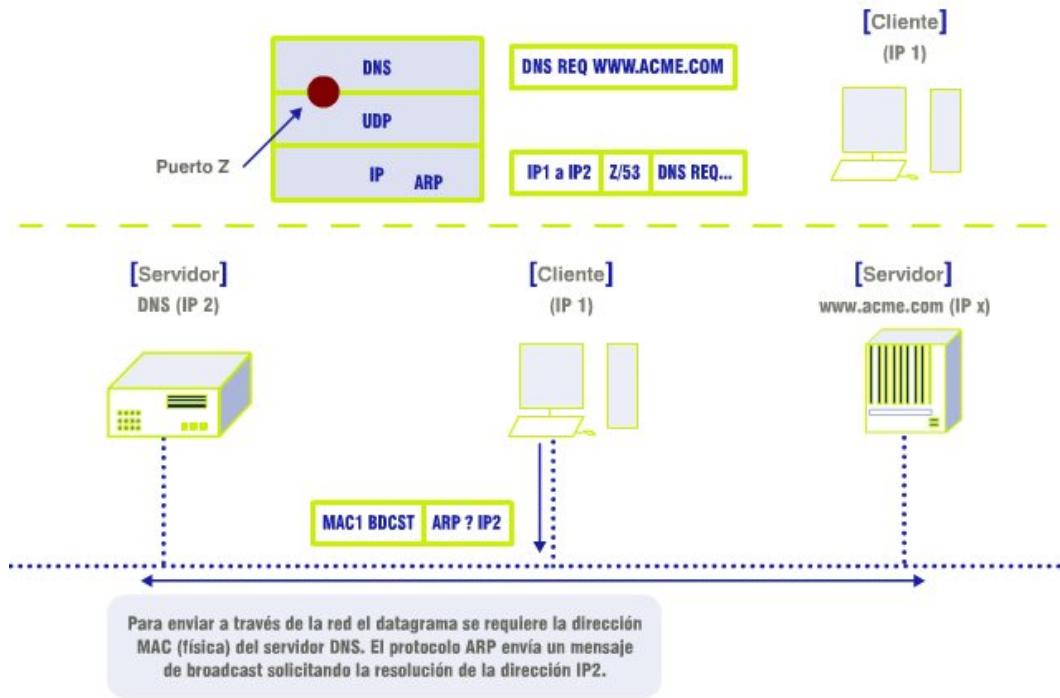
El cliente, a través de la aplicación cliente (navegador), solicita la página web de www.acme.com. Para ello, se comunica con el protocolo de aplicación HTTP. Éste escribe la petición (mensaje de solicitud HTTP) y la entrega a través de un puerto (X) al protocolo TCP.



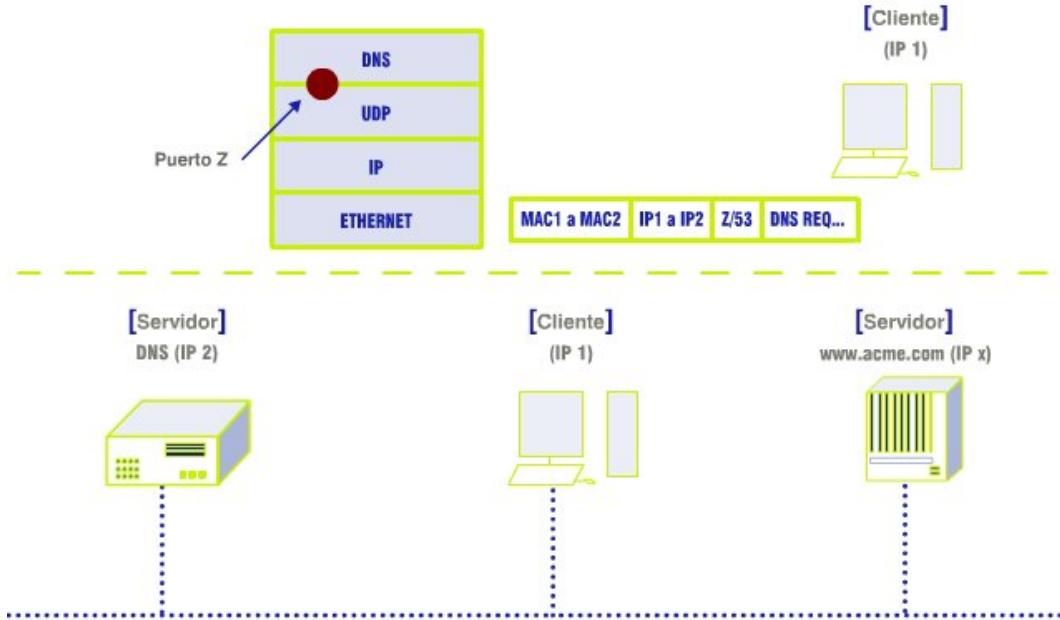
El protocolo TCP añade la información de puerto origen y destino (el 80 es el asociado a servicio HTTP). Antes de mandar la petición, ha de iniciar la conexión con el servidor, enviando un mensaje de inicio de conexión. Este mensaje es entregado al protocolo IP.



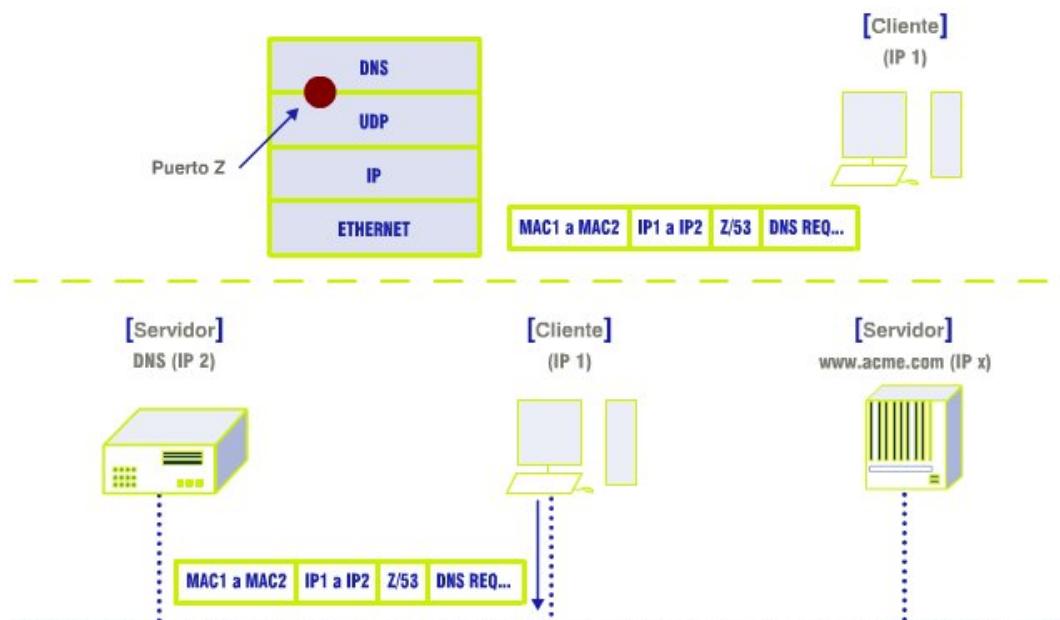




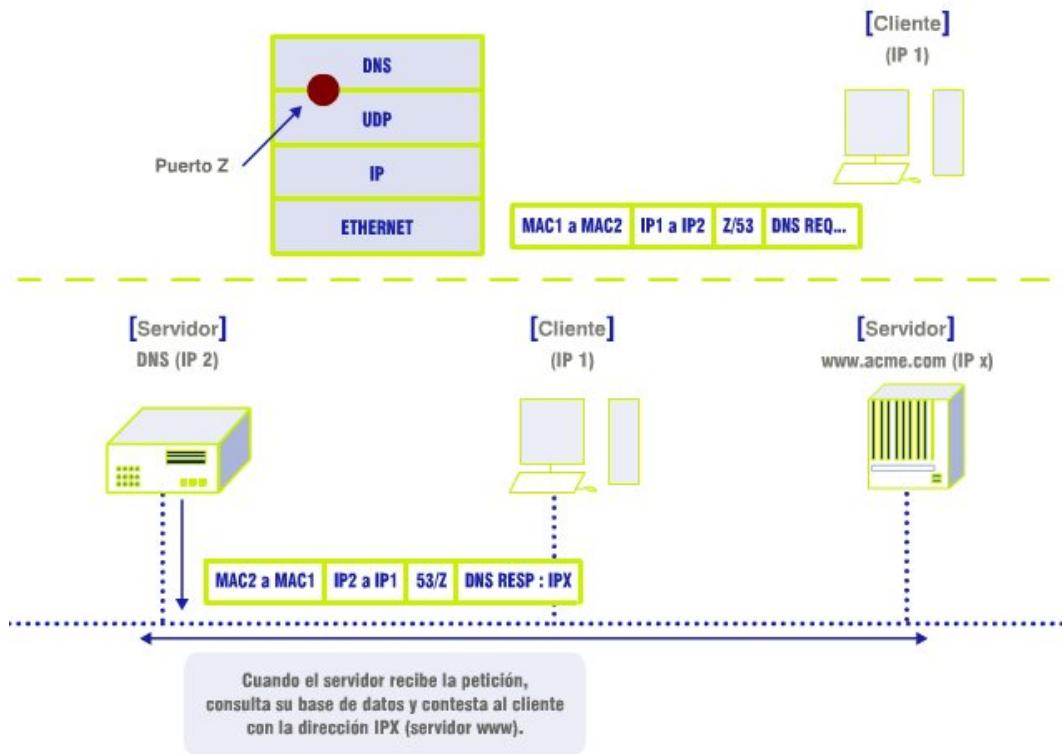
Escenario de comunicación con TCP-IP (II)



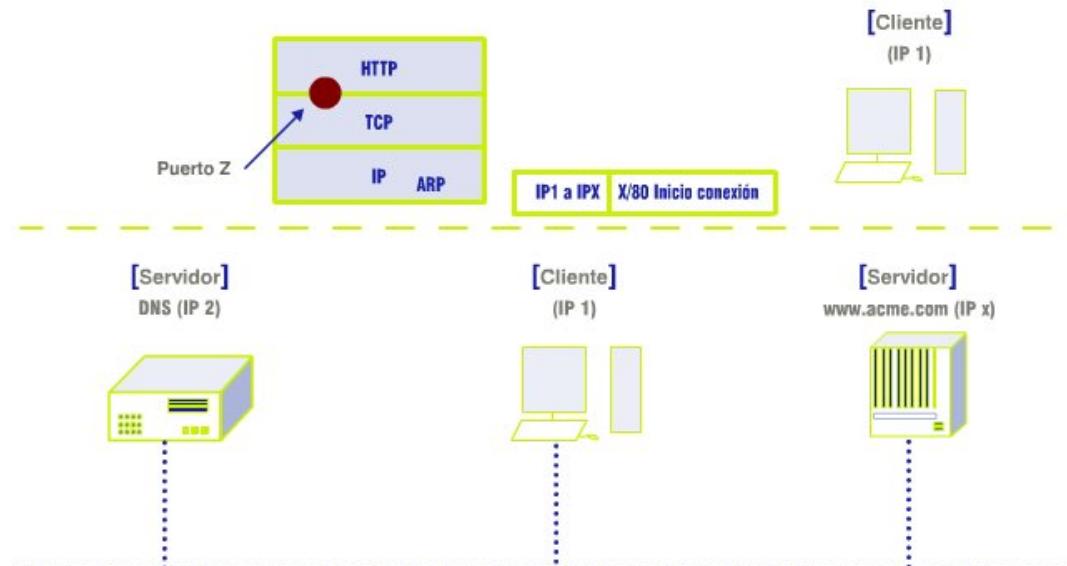
Con la dirección MAC del DNS,
el mensaje es encapsulado en una trama ethernet.



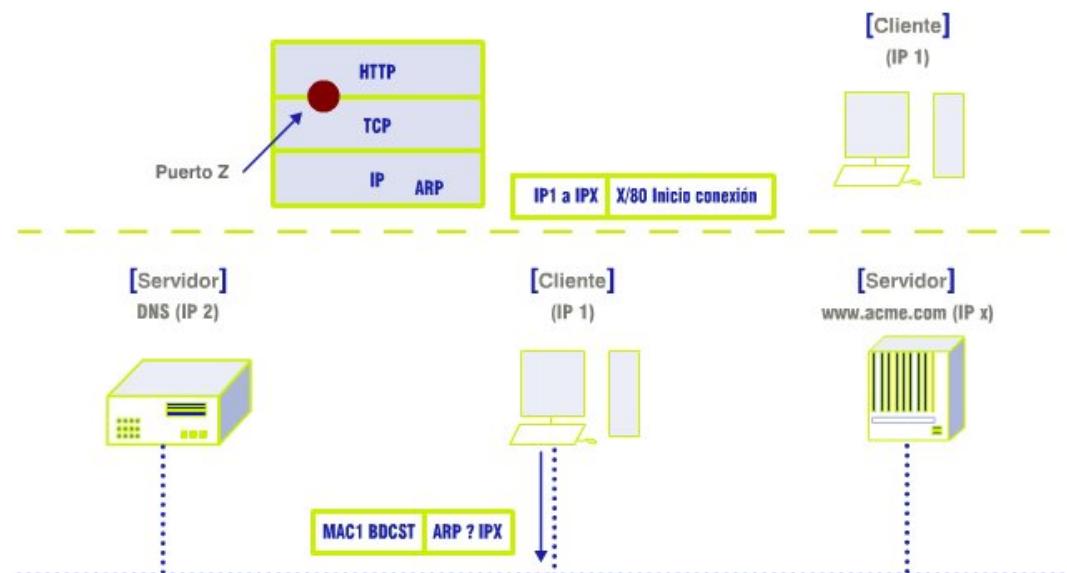
Finalmente, el mensaje DNS es entregado
al servidor a través de la red.



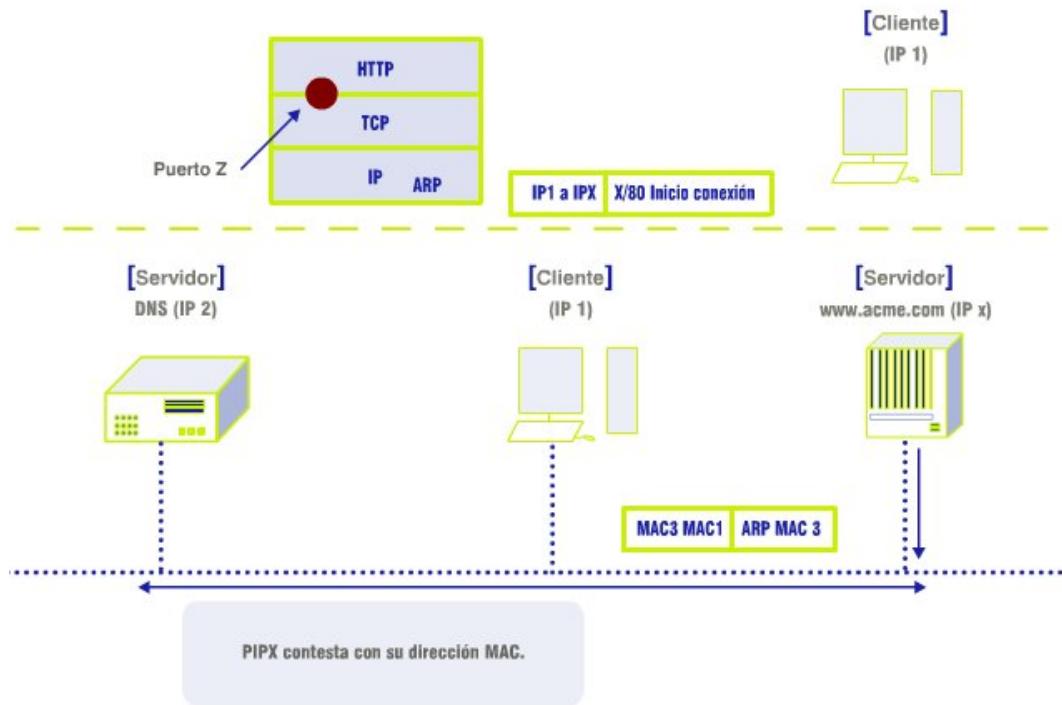
Escenario de comunicación con TCP-IP (III)



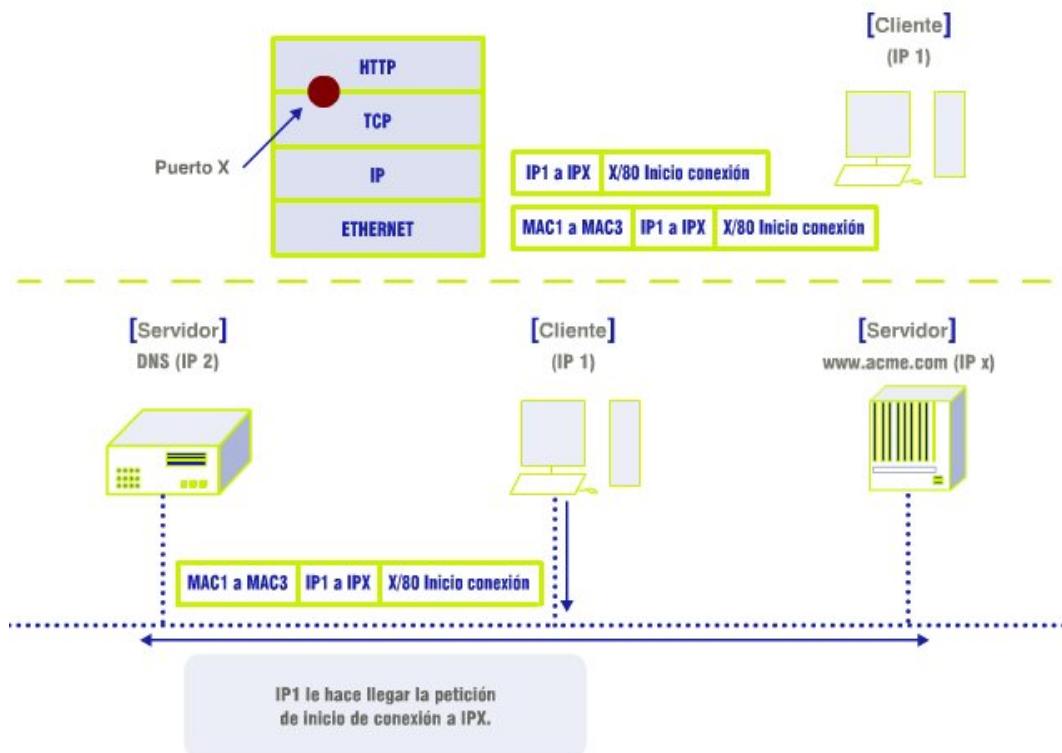
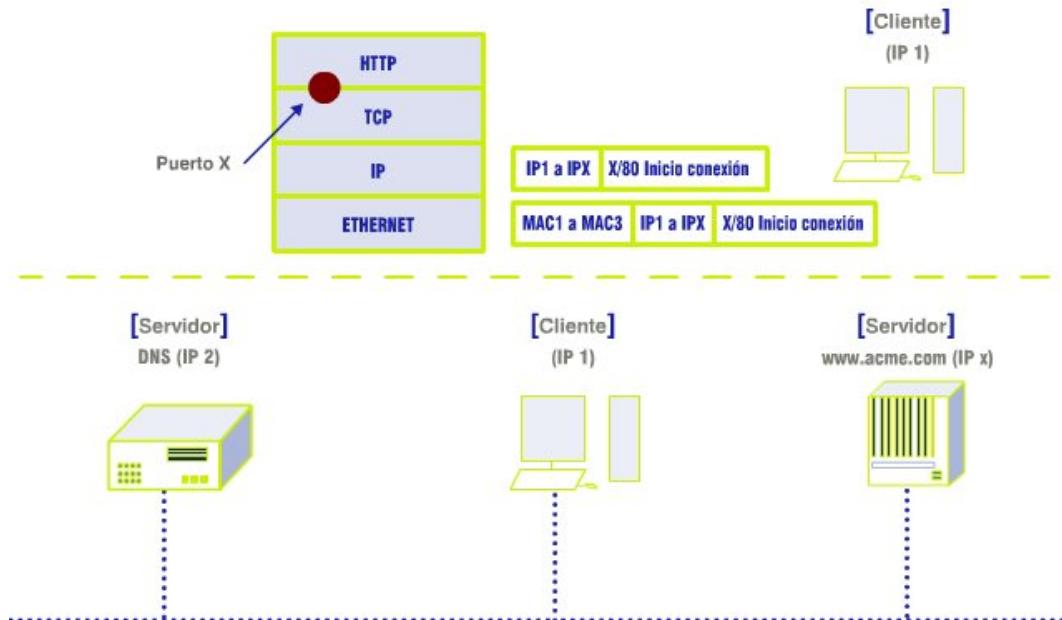
Ahora, el protocolo IP puede completar el datagrama incluyendo la IP destino.

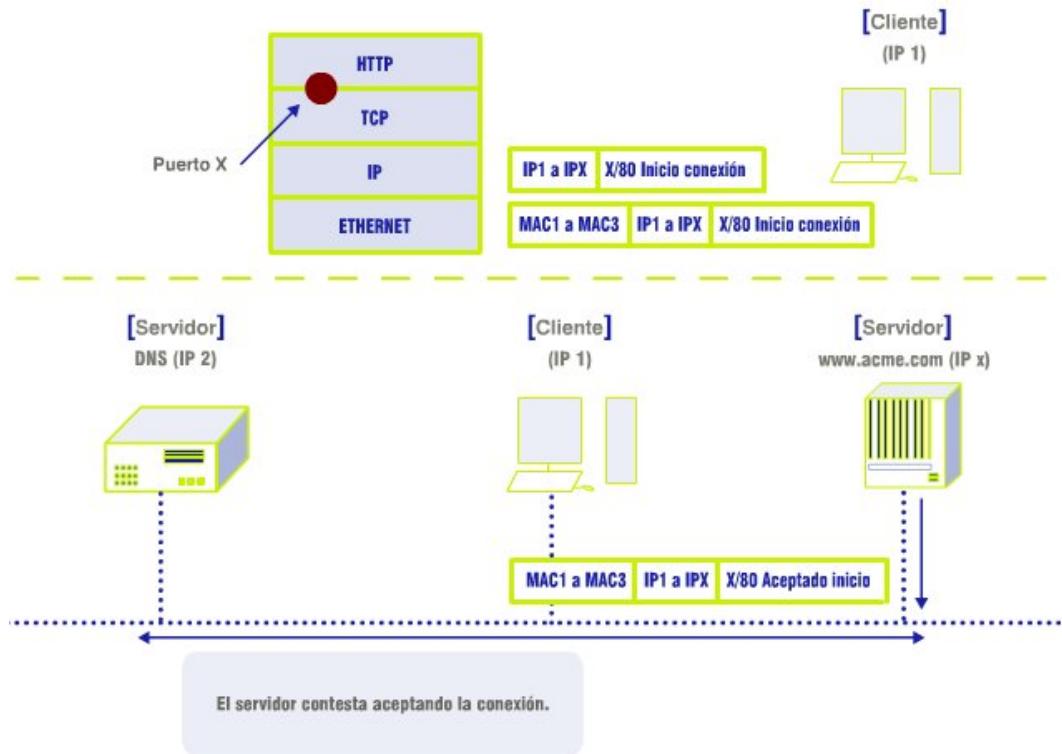


Para poder entregar por la red el datagrama al servidor WWW, requiere la dirección MAC del mismo. Por tanto, se lanza un nuevo mensaje ARP preguntando por la MAC de IPX.

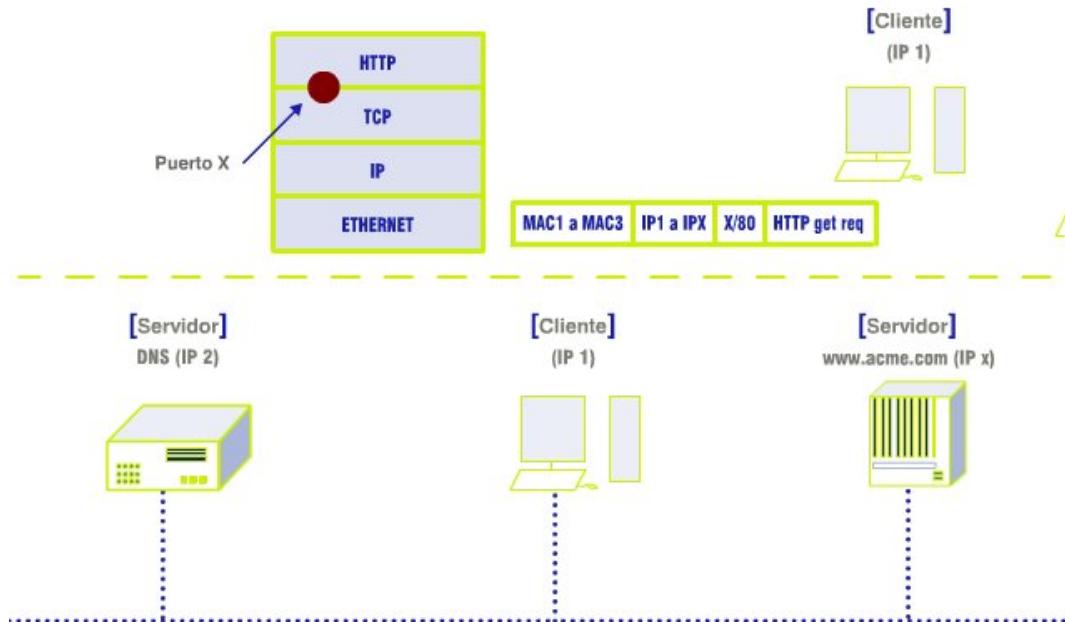


Escenario de comunicación con TCP-IP (IV)

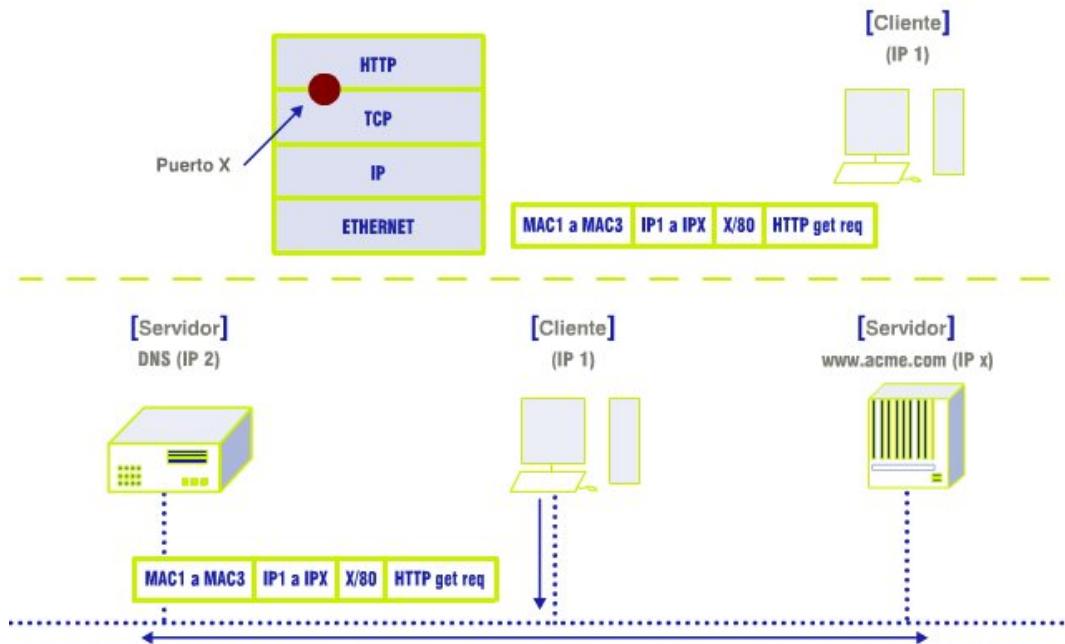




Escenario de comunicación con TCP-IP (V)



El cliente puede procesar, finalmente, la petición de página web.



La petición es enviada al servidor, y será procesada a través del puerto 80. Los datagramas conteniendo la página serán remitidos al cliente y recibidos a través del puerto X.

Conclusión



En este capítulo introductorio hemos repasado la arquitectura de protocolos TCP-IP y el proceso de comunicación (extremo a extremo) entre dos dispositivos de una red IP.

Esta arquitectura se basa en el empleo de un protocolo de nivel tres conocido como IP.

El esquema de direccionamiento que utiliza y los procesos de encaminamiento que se realizan localmente en los dispositivos y en los routers que interconectan las redes, son la base de este protocolo.

Para ello, un dispositivo ha de decidir (el propio direccionamiento IP proporciona los medios) si el destinatario de la información se encuentra en su red física (como en el ejemplo anterior).

De ser así, simplemente averigua la dirección MAC asociada a ese equipo y encapsula los datagramas en la tecnología LAN correspondiente.

Sin embargo, si se determina que la máquina destino no se encuentra ubicada en la propia red, se ha de recurrir a los routers y a los procesos de encaminamiento para que el datagrama llegue a su destino.

El esquema de direccionamiento, desde lo más básico hasta el direccionamiento extendido, y los routers y sus procesos de encaminamiento, son los temas que trataremos a partir de este momento.

2 Direccionamiento básico

Introducción a la Sección 2

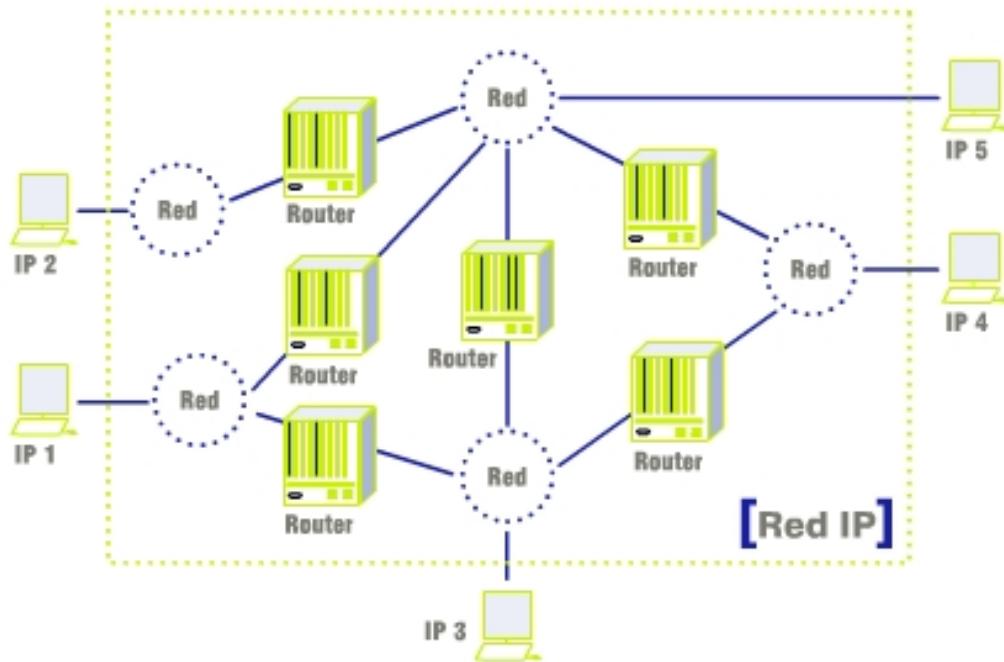
Vas a comenzar el apartado 2:

Direccionamiento básico

El objetivo de este capítulo es repasar los conceptos claves del direccionamiento IP y la terminología relacionada con el mismo.

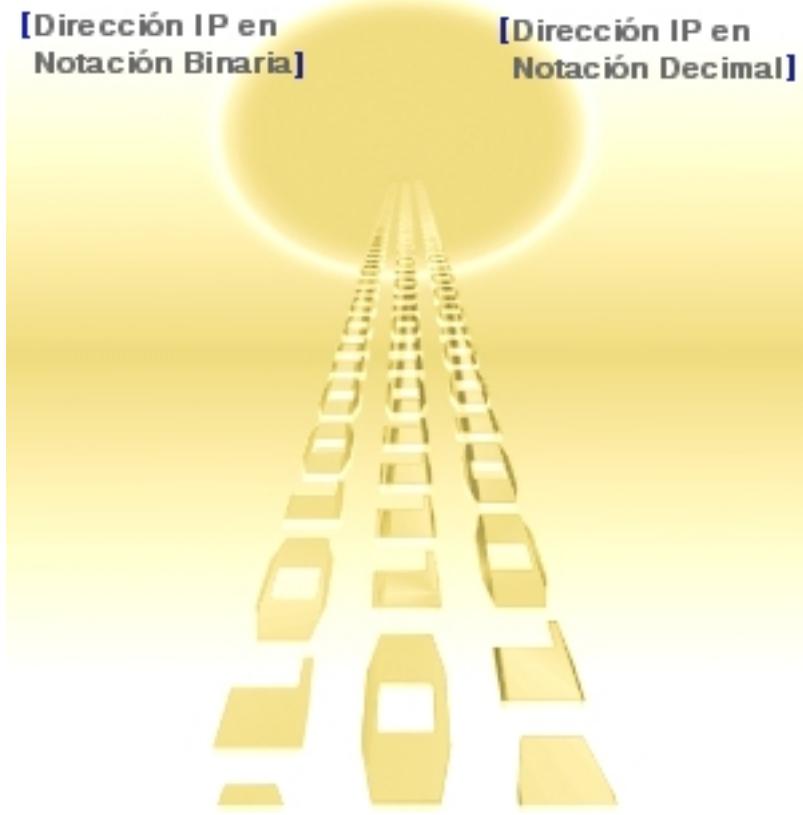
Direcciones IP

Recordemos que en una red IP, cada dispositivo conectado a ella tiene una **dirección IP**, que le identifica de manera única dentro de la red.



El protocolo IP utiliza estas direcciones para identificar origen y destino de la información y encaminar, a través de los routers, los datagramas.

Formato de las Direcciones IP y Notaciones



Veamos ahora cómo son esas direcciones IP.

[Dirección IP en Notación Binaria]

Una dirección IP es un número binario de 32 bits. Uno de los motivos que pudo influir en esta longitud es que coincidía con el tamaño de los registros internos de los ordenadores de la época.

Por ejemplo, **1101100010000000100101000110100**

Con 32 bits podemos escribir 2^{32} (4.294.967.296) direcciones diferentes. El conjunto de todas ellas se conoce como **espacio de direcciones**.

[Dirección IP en Notación Decimal]

Las personas no manejamos fácilmente números binarios de 32 bits, así que se inventó una notación más cómoda: la **notación decimal o de puntos**. En esta notación, se dividen los 32 bits en cuatro grupos de 8 bits (octetos o bytes).

Cada uno de estos octetos se escribe en decimal, separando un octeto del siguiente mediante un punto. Por ejemplo, la misma dirección (11011000.10000000.01001010.00110100) en notación decimal es **216.128.74.52**

Cada uno de los octetos de una dirección IP será siempre un número decimal entre 0 (00000000) y 255 (11111111), ya que este es el margen de números que pueden escribirse con 8 bits.

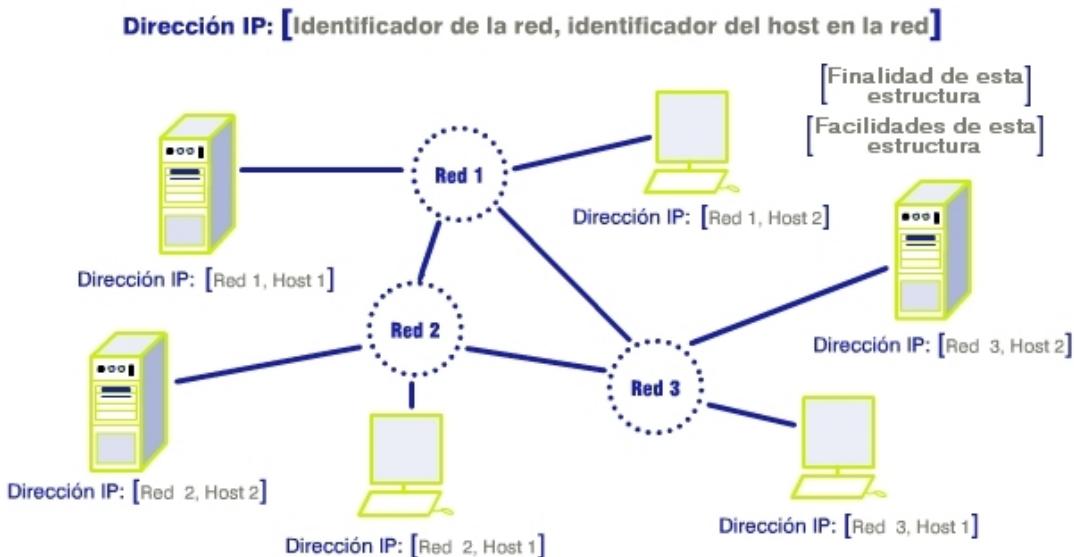
Introducción a estructura de direcciones IP



Al igual que los números telefónicos, las direcciones IP están estructuradas de tal forma que los dispositivos puedan ser localizados fácilmente.

Veamos.

Estructura de las Direcciones IP



La dirección IP de un dispositivo está estructurada en dos partes:

- Identificador de la red a la que está conectado el host.
- Identificador del host dentro de esa red.

Finalidad de esta estructura

Esta estructura tiene el fin de facilitar el proceso de encaminamiento de los routers. Para encaminar un datagrama, los routers analizarán en un principio el identificador de la red a la que pertenece, hasta alcanzar ésta. Una vez dentro de esa red, los routers tendrán que analizar el identificador del host de destino para encaminar el datagrama hasta él.

Fíjate en que este mismo principio es el utilizado en la red telefónica: los primeros dígitos de un número telefónico indican la central, y el resto, el abonado dentro de esa central.

Facilidades de esta estructura

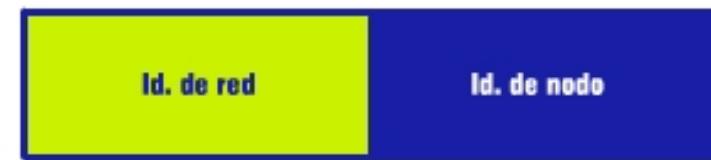
Podemos resaltar que el encaminamiento seguiría siendo posible aunque la dirección IP no tuviese esta estructura, es decir, si toda la dirección identificase directamente un host, sin información de a qué red está conectado. En este caso, los routers tendrían que analizar toda la dirección para encaminar el datagrama hacia su destino. Dado que pueden existir más de cuatro mil millones de direcciones distintas, esto haría mucho más costoso el proceso de encaminamiento.

Los routers sólo tienen que analizar el identificador de red para realizar el encaminamiento. Al haber muchas menos redes que hosts, el proceso es más sencillo.

Máscara de red

El identificador de red podrá tener el valor que se desee, en función del tamaño de la red. A redes grandes, prefijo pequeño, y viceversa.

¿Cómo determinamos, por tanto, cuál es el prefijo de la dirección IP?



101	Dirección IP
1111111111111111111100	Máscara de red
.....
101010101010101010100	Dirección de red
Prefijo de red	

Para definir el prefijo de la dirección IP, es decir, lo que se conoce como el identificador de red, se utiliza la denominada **MÁSCARA DE RED**.

Es un número binario de 32 bits que define en las posiciones a "1" el prefijo o identificador de red, y en las posiciones a "0" el sufijo o identificador de nodo.

Se realiza, sencillamente, la operación "AND" entre la dirección IP y su máscara de red, obteniendo como resultado la dirección de red (todos los bits del identificador de host quedan a cero).

Relación de ideas clave



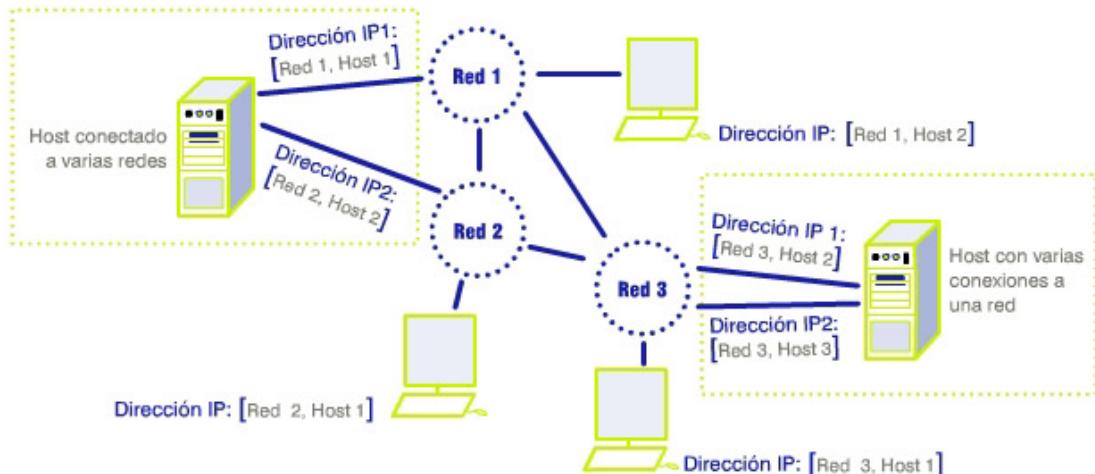
Hasta ahora hemos dicho que una dirección IP identifica un dispositivo en una red IP.

Sin embargo, realmente identifica una conexión del dispositivo.

Veamos.

¿A quién identifica una Dirección IP?

Una dirección IP identifica **una conexión** de un host a **una red**.



Hasta ahora hemos manejado la idea de que una dirección IP identificaba a un host dentro de la red IP de manera única. Es ahora el momento de ser un poco más estrictos: **Una dirección IP identifica una conexión de un host a una red**.

Con esta nueva definición y con la estructura de las direcciones IP (red, host), podemos entender algunas situaciones especiales como las que se muestran en la imagen.

Host conectado a varias redes

¿Cuál es la dirección IP de un host conectado a varias redes? Ya hemos visto que las direcciones IP identifican la red (sólo una) a la que el host está conectado. Como consecuencia, si un host está conectado a varias redes, deberá tener otras tantas direcciones IP.

Es decir, cada una de esas direcciones IP identificará una conexión de ese host a una red, de acuerdo con la definición que acabamos de dar. Fíjate en que el identificador de red de cada una de esas direcciones corresponde a las redes a las que está conectado el host.

Host con varias conexiones a una misma red

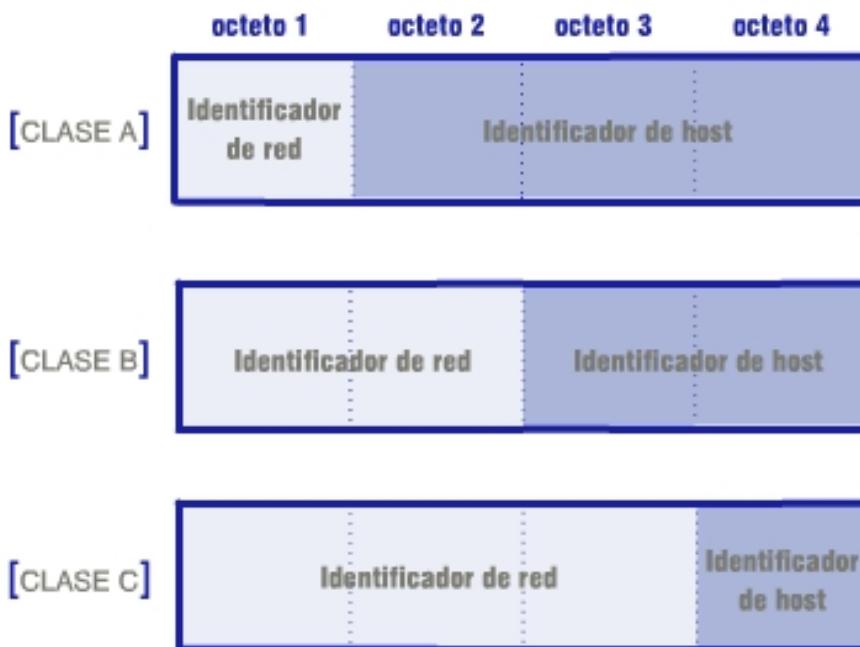
¿Cuál es la dirección IP de un host que dispone de varias conexiones a la misma red? Siguiendo con el razonamiento anterior, la respuesta es que puede disponer de tantas direcciones como conexiones a esa red tenga. A diferencia del caso anterior, estas direcciones tendrán el mismo identificador de red, diferenciándose por el identificador de host.

En este mismo escenario, también sería posible configurar varias interfaces de red para que compartieran una misma dirección IP. Este sería el caso, por ejemplo, en una configuración con tarjeta de red redundante.

Clases de Direcciones IP

El identificador de red o prefijo puede tener cualquier tamaño.

Sin embargo, en un principio, se definieron 3 prefijos predeterminados para facilitar el proceso de encaminamiento. De ahí el concepto de Clases de Direcciones.



Inicialmente se definieron distintas clases de direcciones IP, dependiendo de los tamaños en bits de los identificadores de red y de host dentro de la red:

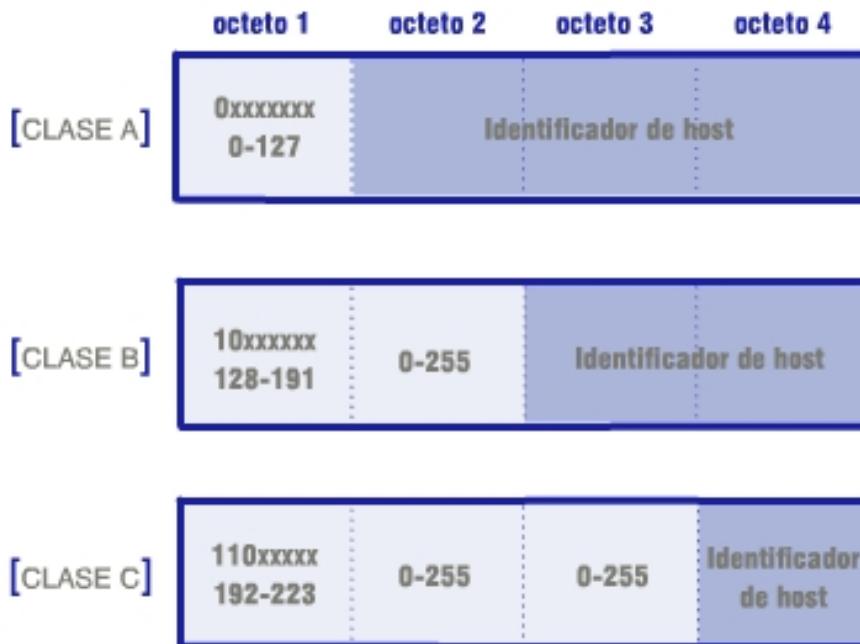
- **Clase A:** un octeto para el identificador de red y tres octetos para el identificador de host (redes grandes).
- **Clase B:** dos octetos para el identificador de red y dos octetos para el identificador de host (redes medianas).
- **Clase C:** tres octetos para el identificador de red y un octeto para el identificador de host (redes pequeñas).

La imagen muestra la situación de estos octetos en la dirección IP.

El objetivo de esta clasificación era asignar a las organizaciones que se conectaban a Internet bloques de direcciones IP de distintos tamaños según el tamaño de la red.

Más sobre clases de Direcciones IP

Para evitar la duplicidad de direcciones entre las clases, se utiliza el primer octeto de la dirección, prefijando los tres bits más significativos: **del 0 al 127 para clase A, del 128 al 191 para clase B y del 192 al 223 para clase C.**



Lo importante a destacar aquí es que **la clase va codificada dentro de la propia dirección**, no siendo necesario indicar esta información a través de la máscara de red.

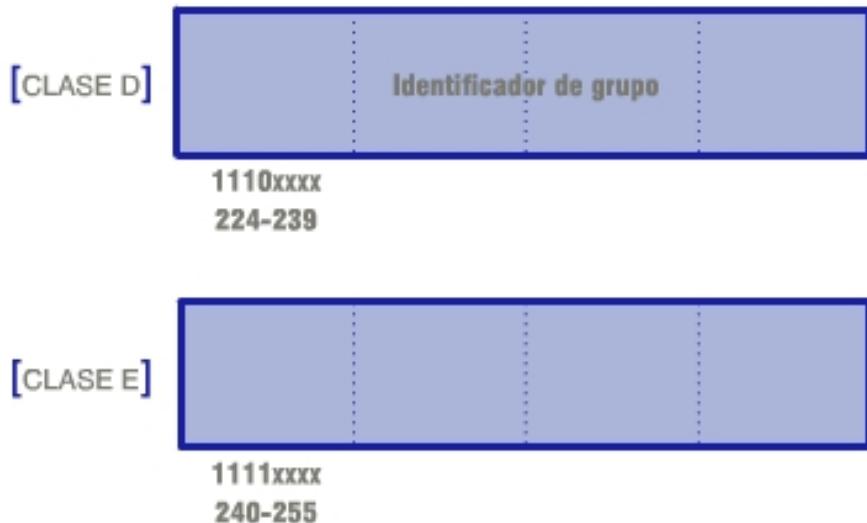
Simplemente fijándonos en el margen al que pertenece el valor del primer octeto, sabemos de qué clase es la dirección.

Existen otras dos clases de direcciones: la **clase D** y la **clase E**.

Las direcciones de clase D son **direcciones de multicast o multienvío**.

El multicast consiste en que un datagrama sea entregado a varios hosts de la red en lugar de a un solo host.

Una dirección de multicast identifica a un **grupo de hosts** dentro de la red.

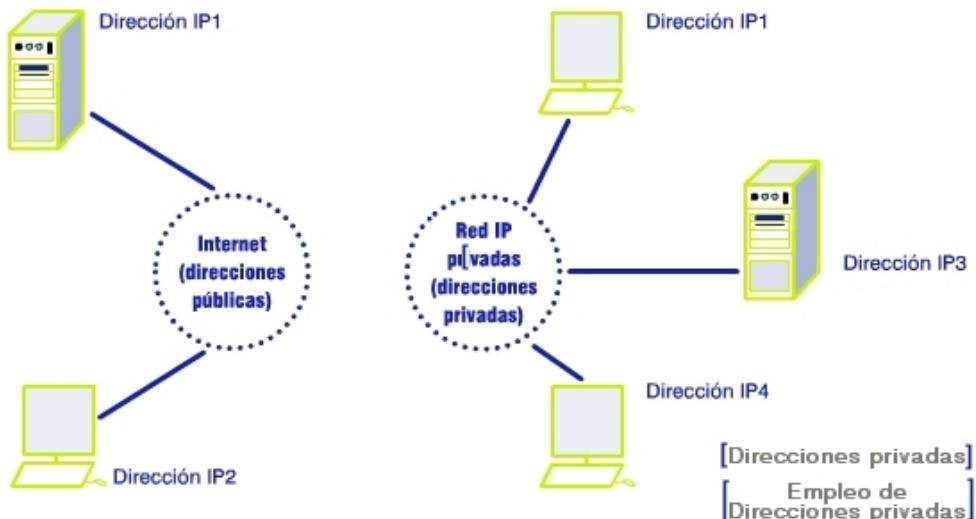


Por otra parte, las direcciones de clase E están reservadas para **USO experimental en proyectos de investigación** en la red.

Dado que su uso no está especificado, tampoco podemos hablar en este caso de una estructura interna tipo (identificador de red, identificador de host) para estas direcciones.

Al igual que para las clases A, B y C, las direcciones de clases D y E se reconocen por los valores que toman los primeros bits de la dirección, tal y como se indica en la imagen.

Direcciones públicas y Direcciones privadas



Una dirección IP pública es aquélla que identifica de manera única a un host conectado a **Internet**. De todas las direcciones IP que serían posibles en Internet, se han excluido algunas para utilizarlas como direcciones en redes IP privadas.

Direcciones privadas

Las direcciones reservadas para su uso como direcciones privadas (no utilizables en Internet) son:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

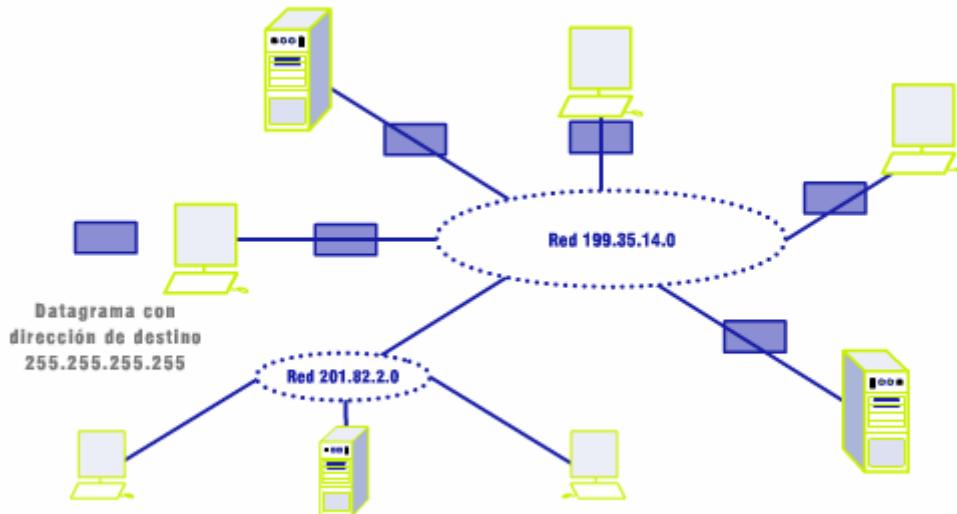
Estas direcciones **no podrán ser utilizadas como públicas en Internet**.

Empleo de Direcciones privadas

Aunque en una red aislada podríamos emplear cualquier conjunto de direcciones IP, se recomienda utilizar direcciones pertenecientes a estos rangos. De esta manera, si un datagrama de esa internet privada saliera accidentalmente a Internet, la Red simplemente lo descartaría porque sabe que la dirección no existe en Internet.

Las ventajas y desventajas de utilizar estas direcciones reservadas en una red IP aislada se tratan en la RFC1918 Address Allocation for Private Internets (Asignación de direcciones para internets privadas).

Direcciones de Difusión o Broadcast

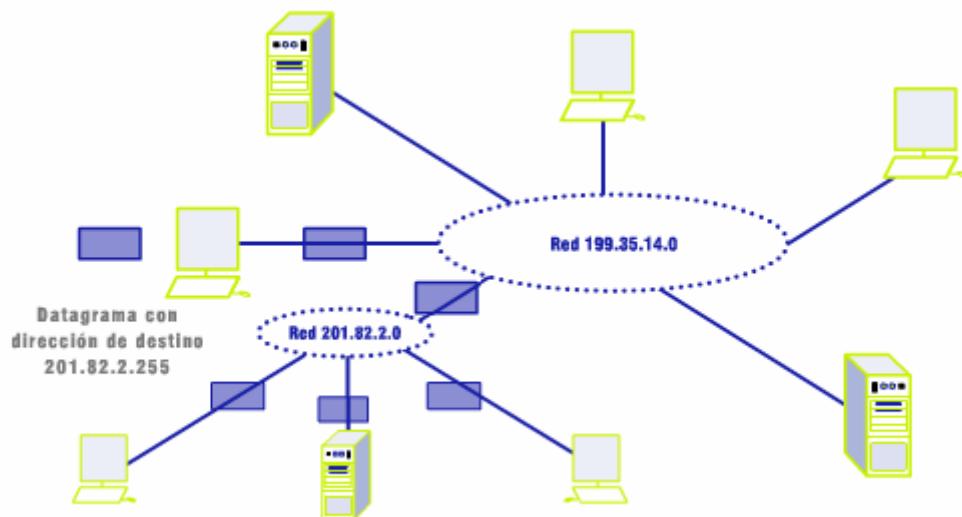


La **difusión** o **broadcast** consiste en hacer llegar un datagrama a todos los hosts conectados a una red.

La dirección de destino de un datagrama de broadcast será una dirección IP especial con el significado de todos los hosts de la red origen del datagrama.

En concreto, esta es la dirección que conocemos como **dirección de broadcast**, y que está compuesta por los 32 bits a 1, o en notación decimal: **255.255.255.255**.

Difusión dirigida



También es posible realizar **difusión dirigida**. Ésta consiste en enviar un datagrama desde una red para que se entregue a todos los hosts de **otra red**.

Al igual que en el caso anterior, es necesaria una dirección IP especial cuyo significado sea **todos los hosts de una red específica distinta de la red de origen**.

Esta dirección se construye con el identificador de la red en cuestión, y todos los bits del identificador de host a 1.

Otras direcciones restringidas



Hasta ahora hemos visto que ciertas direcciones, como las de Multicast, broadcast y difusión dirigida, no pueden ser asignadas a los dispositivos porque tienen un significado especial.

Además, también **está restringido el uso de “0” en la parte del identificador de host**, pues como vimos, se utiliza para identificar la totalidad de la red.

Por último, la red **127.0.0.0 no puede utilizarse debido a que define lo que se conoce como dirección de bucle o interna**.

Se utiliza para identificar “internamente” al dispositivo, es decir, los procesos de comunicación a través de TCP-IP que se generan dentro del sistema.

Conclusión



Las conexiones de los dispositivos a una red IP se identifican mediante direcciones de 32 bits, **constituidas por un prefijo o identificador de red y un sufijo o identificador de la conexión dentro de la red.**

En el esquema original de Internet se definieron 3 tipos de prefijos: A, B y C, dependiendo del tamaño de la red.

Los prefijos, en general, pueden identificarse mediante el uso de máscaras de red.

Del rango total de direcciones IP disponibles, existen una serie de restricciones: **las direcciones de difusión (a una red y en la red), las direcciones de identificación de red (la parte de host puesta a cero), la red 127.0.0.0 (dirección interna) y, por último, si hablamos de direccionamiento público (Internet), las direcciones reservadas para uso privado.**

Todo esto y el esquema de asignación por clases han llevado al agotamiento paulatino del espacio de direcciones (ROAS – Run Out of Address Space).

La solución definitiva será cambiar la versión de protocolo (IPv6) cuyo espacio de direcciones es mucho mayor (128 bits).

Sin embargo, mientras tanto, una serie de medidas están siendo tomadas para ralentizar dicho agotamiento. Entre ellas, cambiar el esquema de asignación de direcciones públicas, el VLSM y el CIDR. Las veremos más adelante.

3 Principios de Encaminamiento

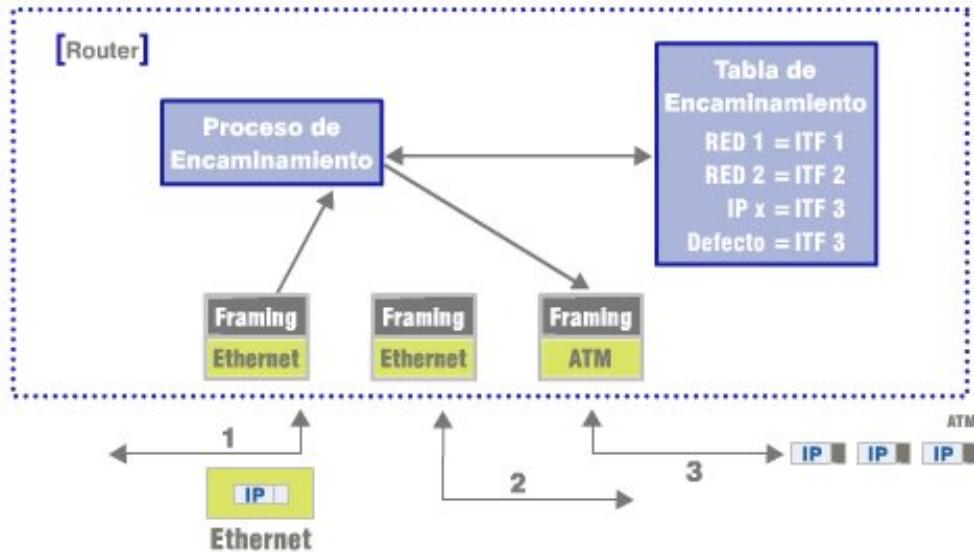
Introducción a la Sección 3

Vas a comenzar el apartado 3:

Principios de Encaminamiento

En el capítulo anterior definimos los conceptos básicos del direccionamiento. Vamos ahora a adentrarnos en el funcionamiento de los routers, la necesidad de protocolos de encaminamiento y cómo se clasifican.

Encaminamiento: definición



El encaminamiento es el proceso de reenvío de paquetes de una red a otra, utilizando direccionamiento lógico (nivel 3). La decisión de encaminamiento efectuada por un **router** se basa en tres decisiones:

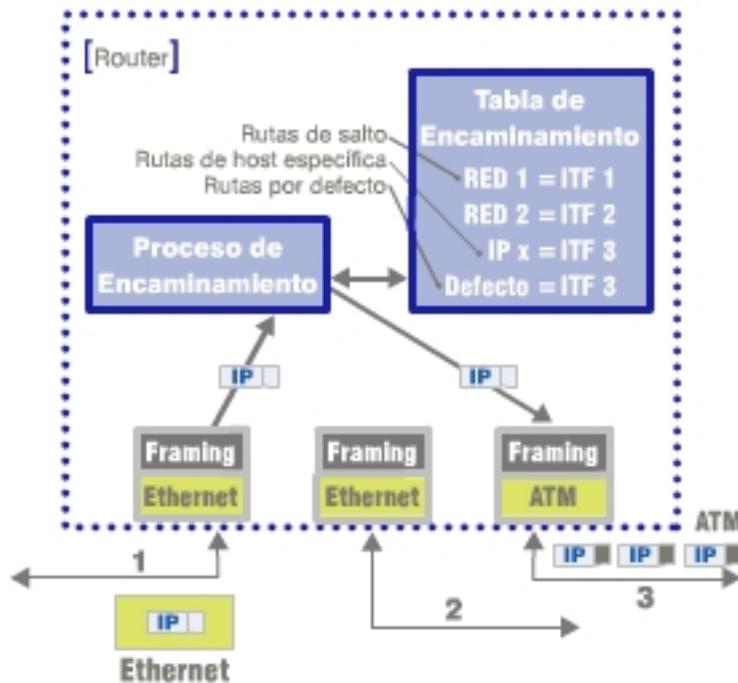
- ¿Es la dirección lógica parte de un protocolo de nivel 3 conocido? (por ejemplo IP)
- ¿Existe una entrada en la tabla de encaminamiento correspondiente a dicha dirección? Si no es así, el paquete se descarta y se envía un mensaje ICMP de error.
- Según la tabla de encaminamiento, ¿por qué interfaz del router ha de ser entregado el paquete? Escogida la interfaz se realiza un proceso de *framing* que consiste en encapsular el paquete y enviarlo al siguiente salto.

Tipos de Encaminamiento

Según el ejemplo de la figura, para alcanzar la dirección de red destino es necesario entregar el paquete a otro router. Esto es lo que se conoce por encaminamiento **INDIRECTO**.

Cuando un router define que la dirección destino se encuentra en una de las redes a las que está conectado directamente, se dice que se efectúa un proceso de encaminamiento **DIRECTO**.

Tablas de Encaminamiento



Las tablas de encaminamiento contienen toda la información necesaria para que un router pueda entregar un paquete al siguiente router o al destinatario final.

Cada máquina almacena información sobre posibles destinos y cómo alcanzarlos. Normalmente, sólo se guarda información sobre las redes destino y no sobre los host en dichas redes.

En la tabla se pueden presentar tres tipos de rutas

Rutas de salto

Indican el siguiente salto (o interfaz) para alcanzar una determinada red.

Rutas de host específicas

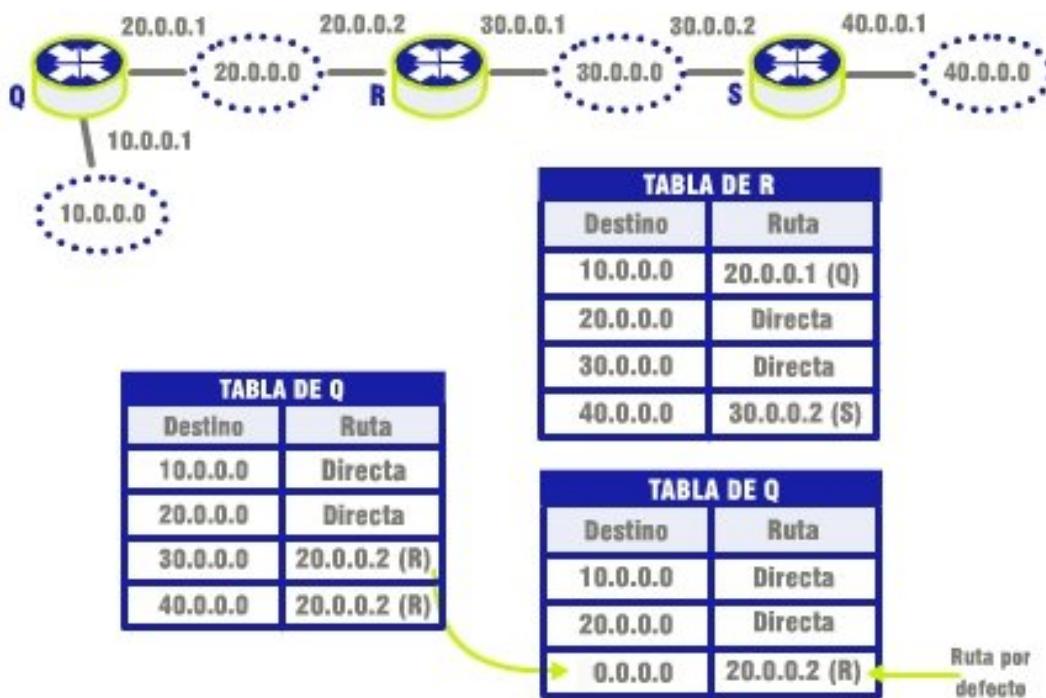
Indican el siguiente salto o interfaz para alcanzar un dispositivo en concreto.

Rutas por defecto (omisión)

Indican el siguiente salto si ninguna entrada corresponde a la dirección deseada.

Tipos de Encaminamiento

De acuerdo a la forma en que las tablas de encaminamiento son creadas, se puede dividir el encaminamiento en dos tipos: **estático** y **dinámico**.



El **encaminamiento estático** requiere que la tabla de encaminamiento sea introducida de forma manual.

Cualquier cambio de topología ha de realizarse manualmente, y es responsabilidad del administrador del equipo que la configuración de la red esté libre de bucles y todas las redes sean conocidas.

En el ejemplo, fíjate que los routers han de ser configurados en sus respectivas interfaces con direcciones IP asociadas a las redes a las que están conectados, además de configurar las tablas adecuadamente.

El **encaminamiento dinámico** es el proceso de utilización de **protocolos** para encontrar la información necesaria para crear y mantener actualizadas las tablas de encaminamiento, libres de bucles y con un único trayecto a cada red.

Aunque es más sencillo y eficaz que el anterior, requiere de mayor capacidad de procesamiento en el router y consume ancho de banda en los enlaces entre los routers, a través de los cuales se “comunican” sus tablas de encaminamiento.

Un **protocolo de encaminamiento** define el conjunto de reglas y mecanismos mediante los cuales los routers intercambian información de sus tablas de encaminamiento con routers vecinos.

Clasificación de protocolos de encaminamiento

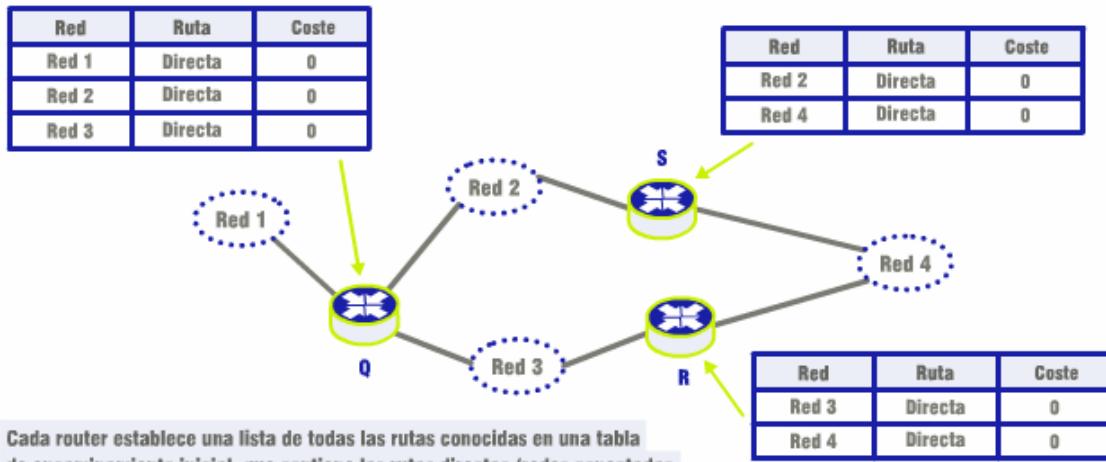


Los protocolos de encaminamiento se clasifican en función del algoritmo que utilizan: *vector-distancia* y *estado-enlace*.

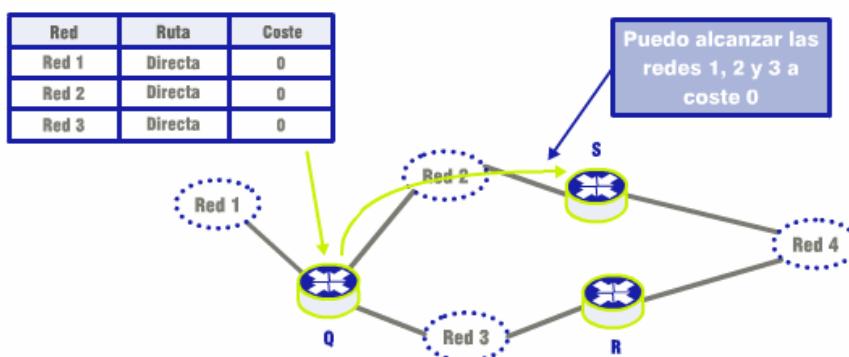
Veamos.

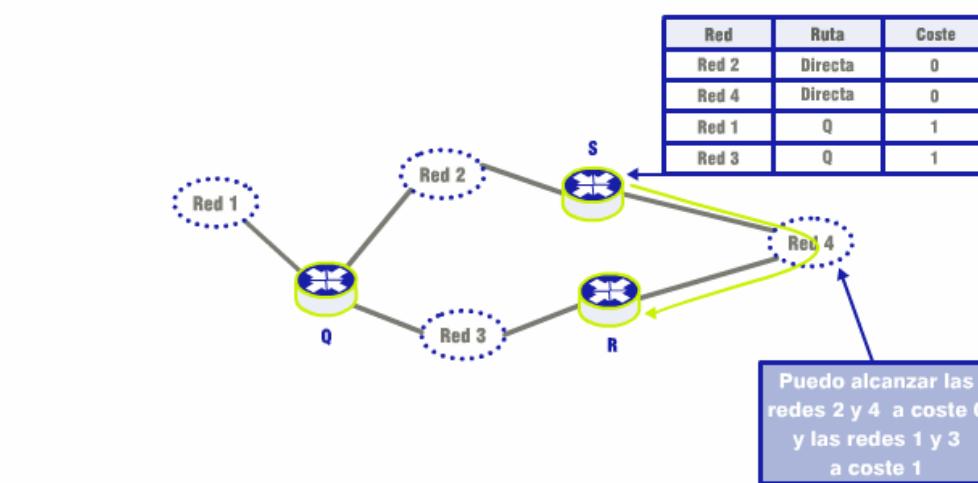
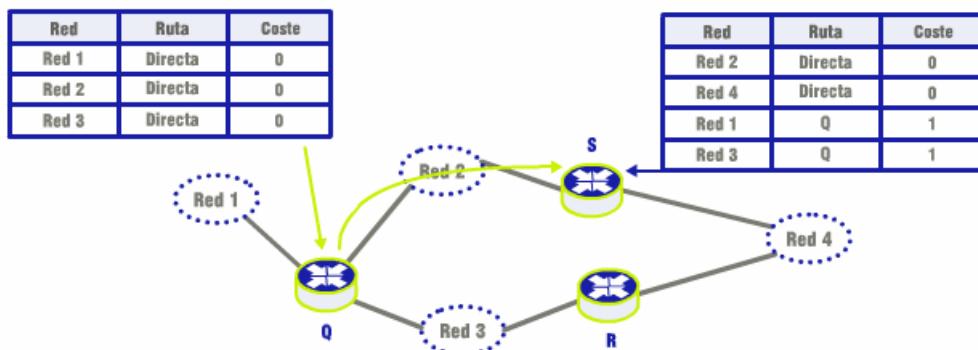
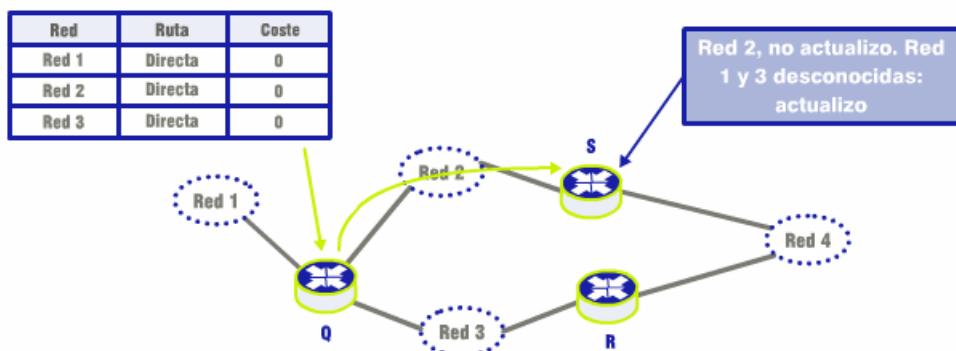
Algoritmo vector-distancia

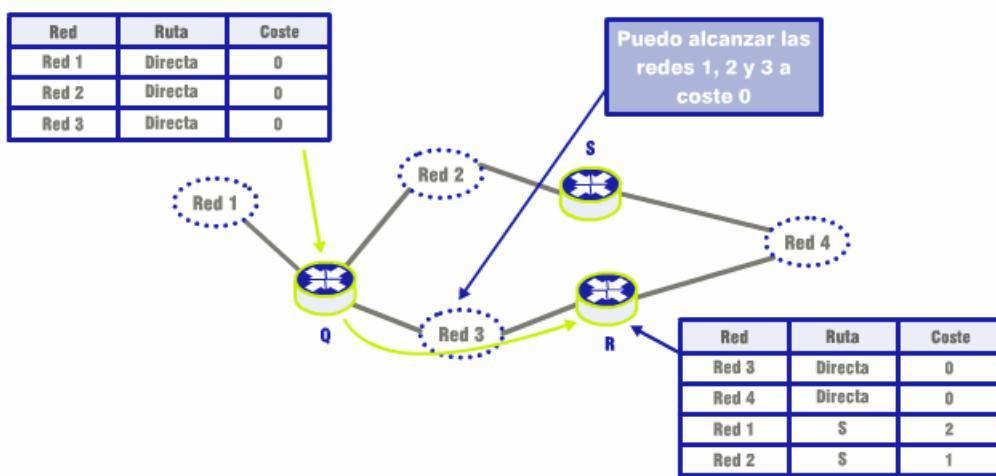
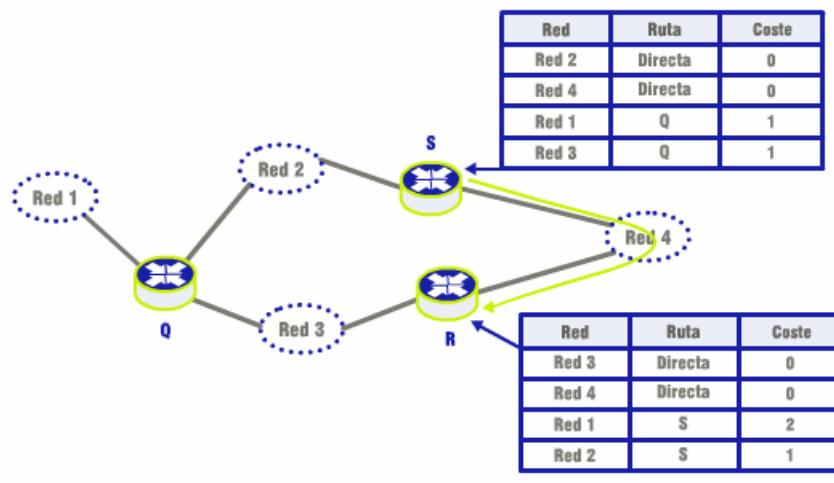
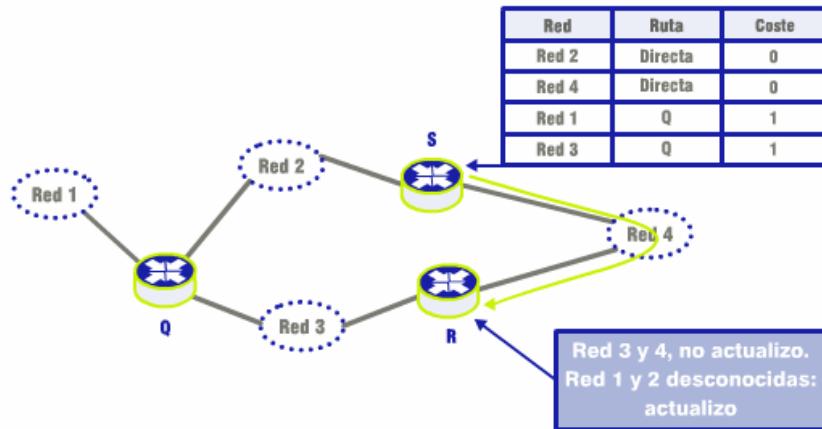
El término vector-distancia proviene del hecho de que los protocolos envían mensajes que contienen una lista de pares (V,D) donde V identifica el destino (llamado vector) y D es la distancia hacia el destino medida, típicamente, en número de saltos.

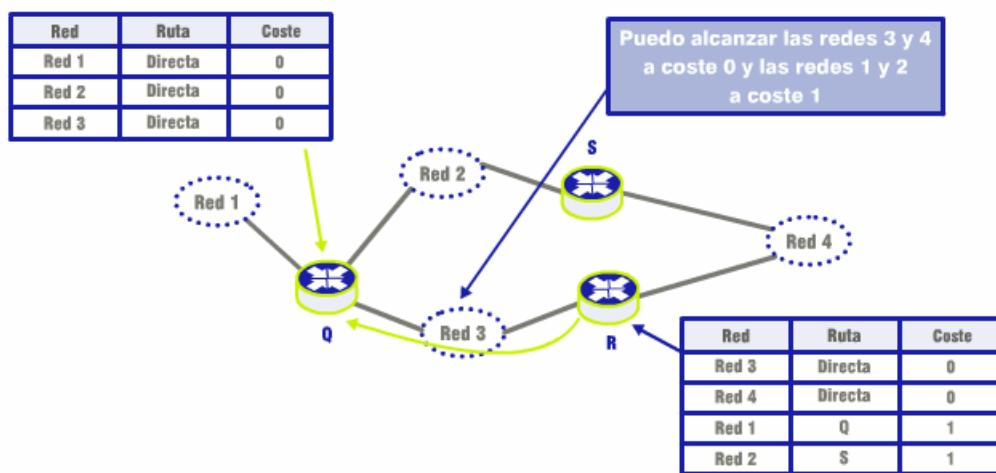
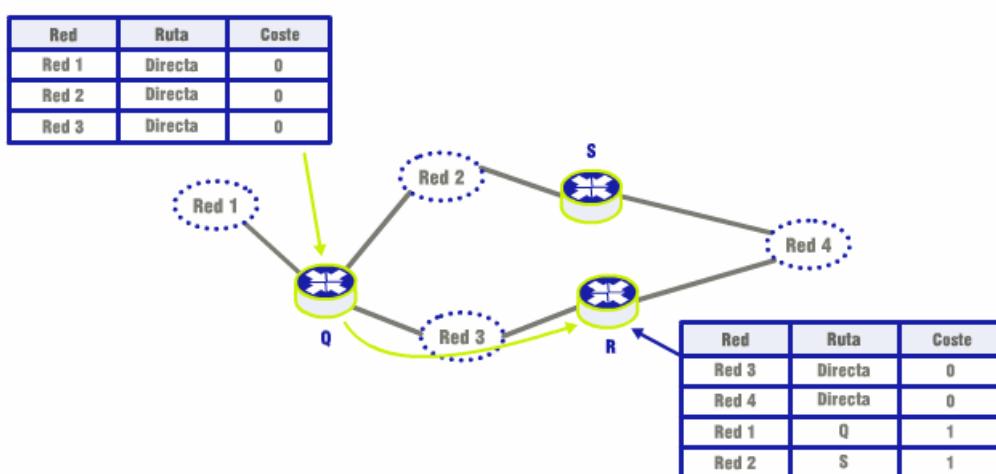
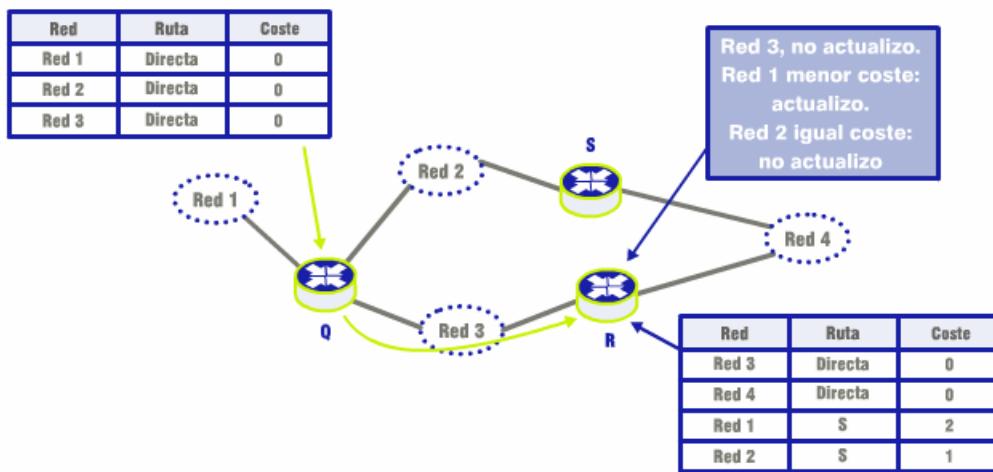


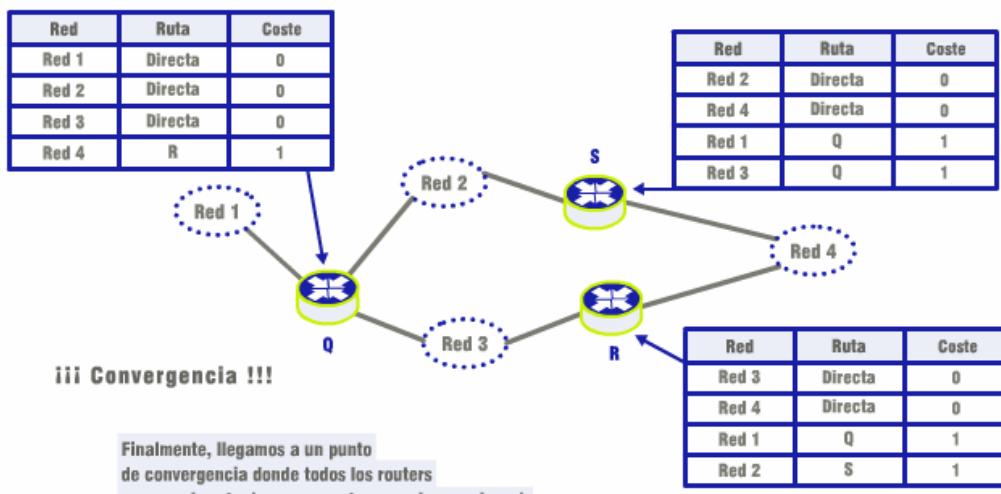
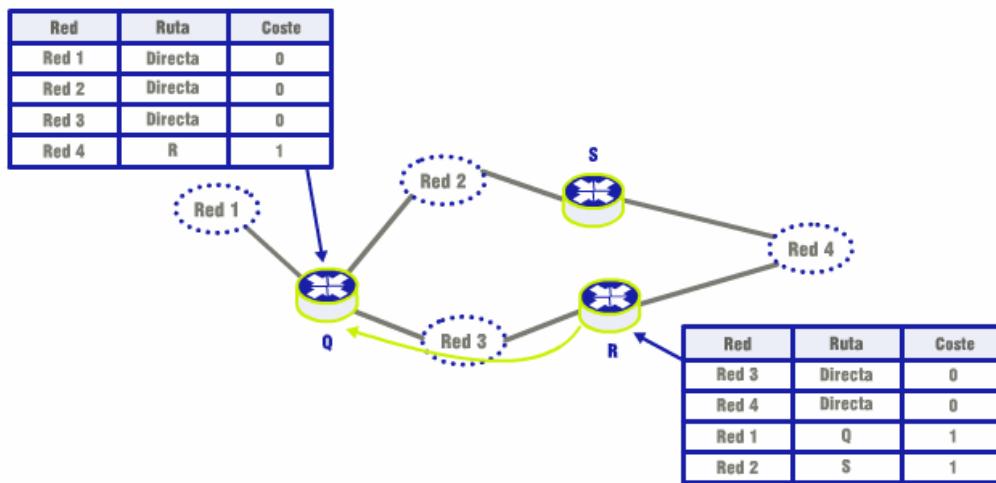
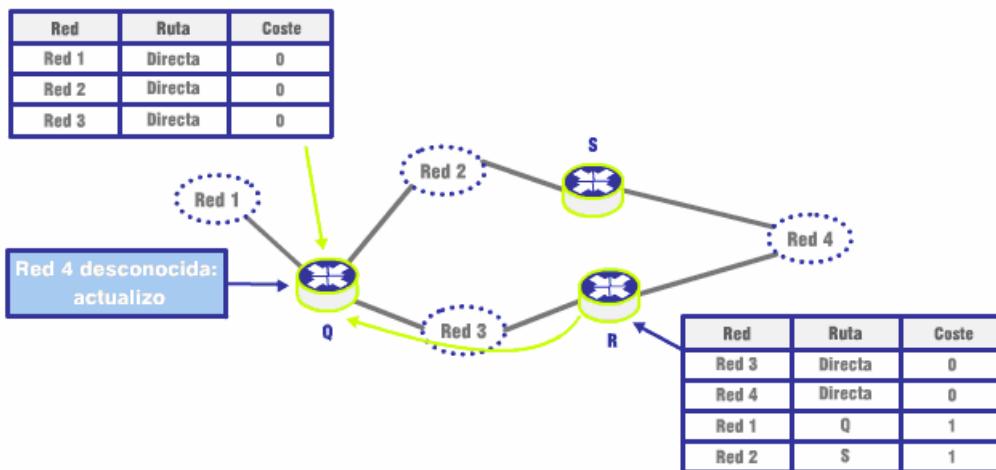
Cada router establece una lista de todas las rutas conocidas en una tabla de encaminamiento inicial, que contiene las rutas directas (redes conectadas directamente al router). Dicha tabla, básicamente, contiene tres valores: dirección de red destino, ruta para alcanzar la red y coste para alcanzar la red. Periódicamente, cada router envía una copia de su tabla a cualquier otro router que pueda alcanzar de forma directa. Fíjate que a mayor o igual coste, un router NO cambia la información de la ruta aprendida.

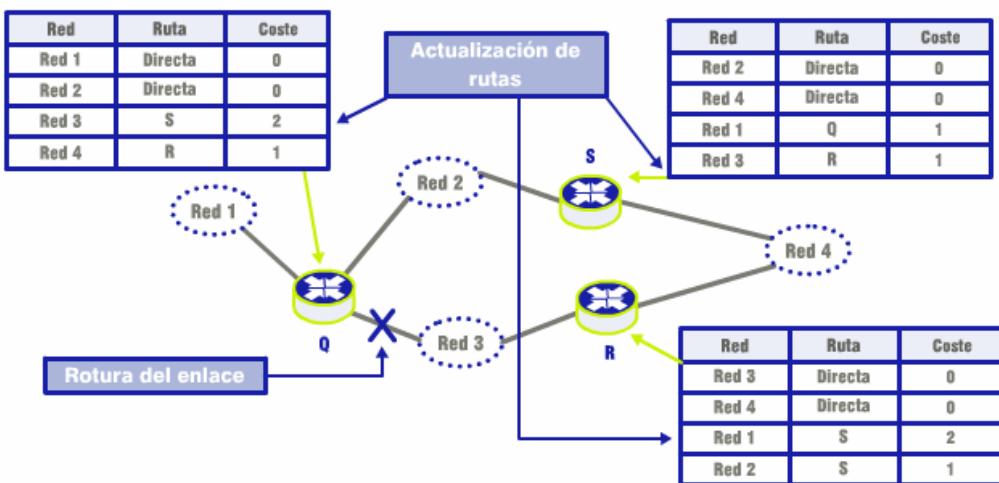
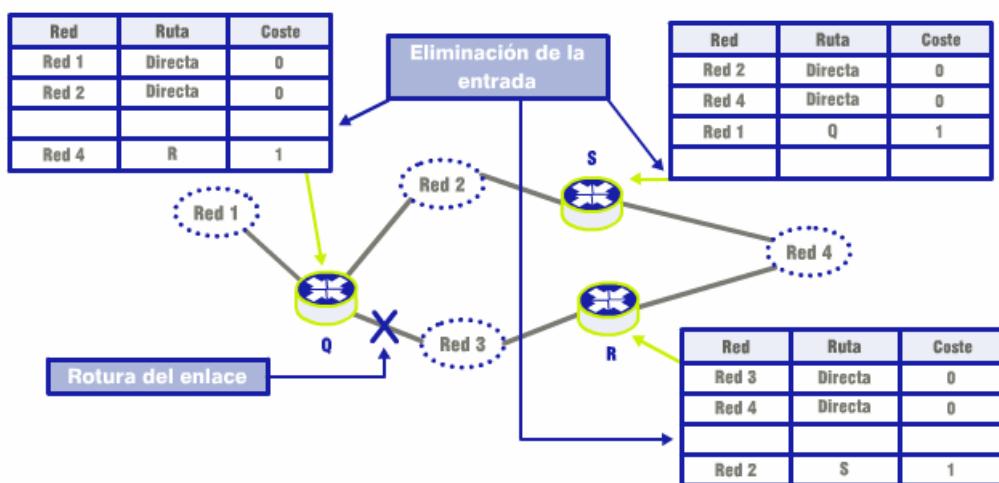
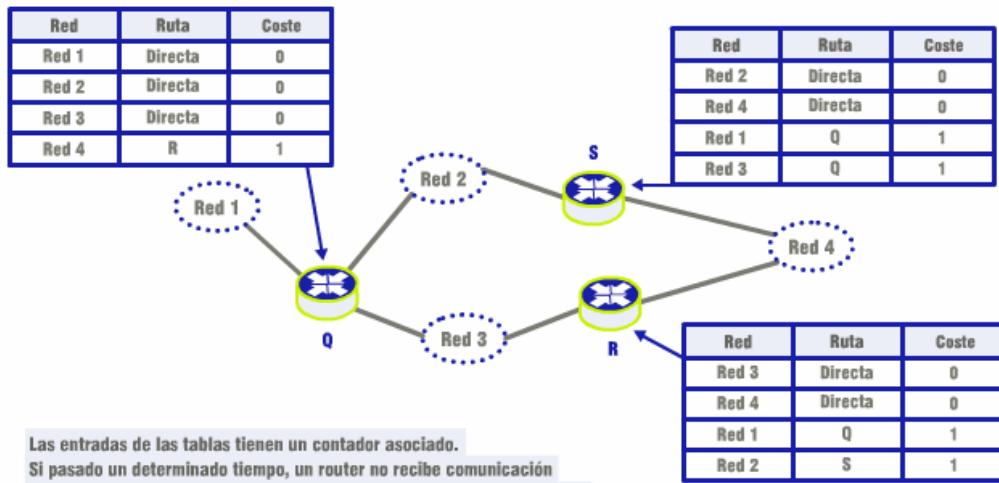












Algoritmo estado-enlace



Los protocolos basados en *vector-distancia* son sencillos de implementar, aunque sólo permiten conocer una ruta para cada red, ya que siempre se guarda la ruta de menor coste y las otras se desechan.

Ante cambios de topología el tiempo de propagación es bastante lento para actualizar nueva información.

El algoritmo *estado-enlace* suple esas deficiencias al proveer de un mapa topológico completo de la red.

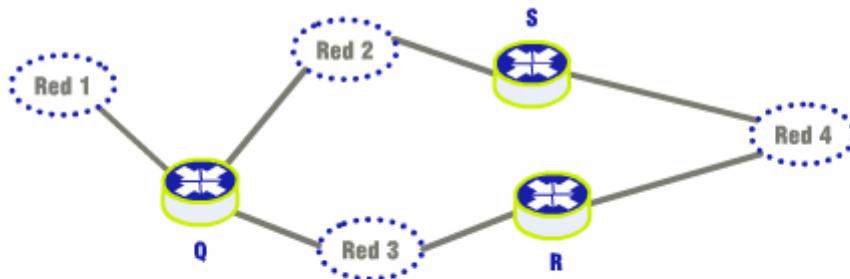
El algoritmo *Estado-enlace* o SPF (Shortest Path First), requiere que cada router participante tenga información de la topología completa de la red, es decir, que todos los routers tengan un mapa que muestre a los otros routers y las redes que conectan.

En términos abstractos, los routers corresponden a los nodos en un grafo y las redes a los arcos (enlaces) que conectan directamente a dos routers.

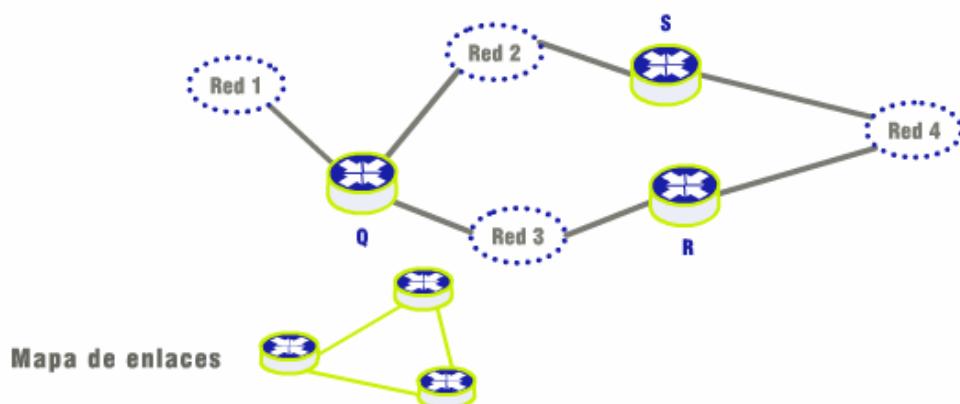
Ejemplo

\$Fichero: \$ B071_LANWAN/html/020311.htm

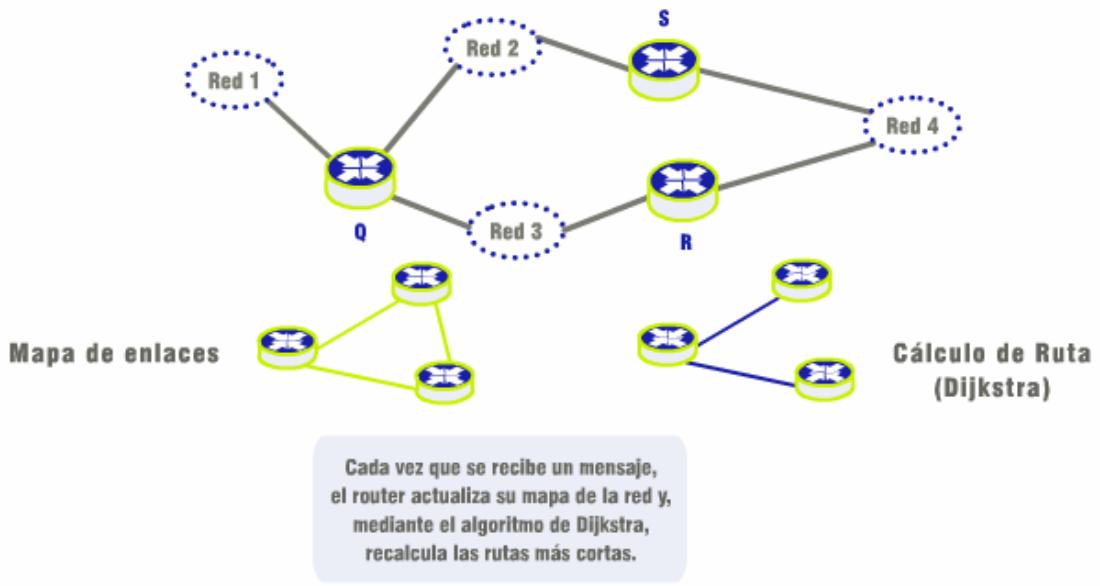
En lugar de enviar un mensaje que contenga una lista de destinos y saltos, un router que implementa SPF tiene dos funciones: probar el estado de todos los enlaces con routers vecinos y difundir periódicamente la información del estado del enlace a otros routers.



Para probar el estado del enlace,
un router envía periódicamente mensajes cortos que interrogan
si el vecino está activo, caso en el cual se define que el enlace está levantado (up),
o inactivo (enlace caído o down).



Para informar a otros routers participantes,
se difunde un mensaje que lista el estado de cada uno de los enlaces.
Este mensaje no especifica rutas sino la posibilidad de comunicación entre pares de routers.
El protocolo implementado entrega una copia de cada mensaje a los routers participantes
por difusión o punto a punto.



Formas de ver el encaminamiento



Parte del proceso de encaminamiento consiste en determinar la pertenencia de una determinada dirección IP a una red en particular ya que las tablas, normalmente, incluyen direcciones de red y no de host.

Veremos que, en función del esquema de clases de direcciones visto en capítulos anteriores, existen dos formas de ver el encaminamiento: **con clase (classful)** y **sin clase (classless)**.

Encaminamiento con clase (CLASSFUL)

Fundamentalmente, el encaminamiento con clase define que la máscara de red no es incluida en la información que transportan los protocolos de encaminamiento.

Esto obliga a que todos los dispositivos de una red han de tener **la misma máscara asociada**.

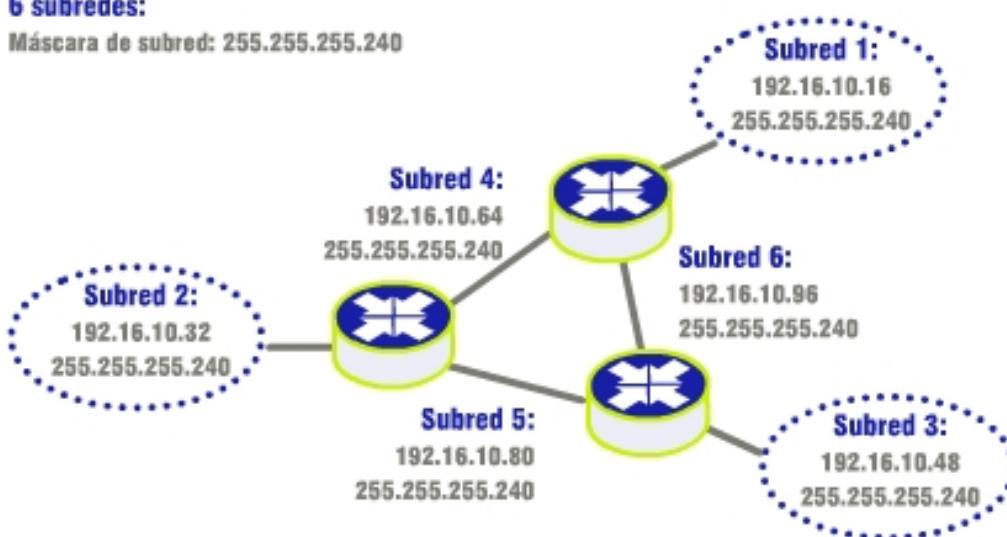
Clase C:

192.16.10.0

255.255.255.0

6 subredes:

Máscara de subred: 255.255.255.240



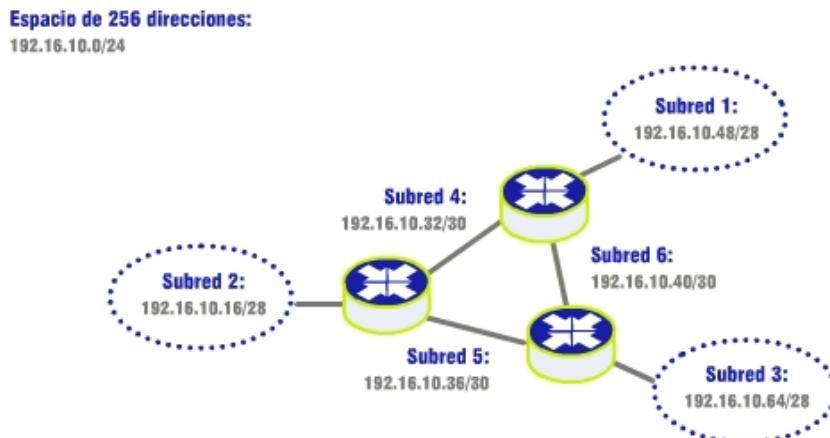
El problema de este tipo de encaminamiento es el desperdicio del espacio de direcciones disponibles, ya que hablamos de subnetting clásico para la creación de subredes (igual máscara de subred para todas las subredes, como veremos posteriormente).

En el ejemplo, a las conexiones WAN (que requieren únicamente dos direcciones IP) se les asigna la misma máscara de subred que al resto, desperdiciándose 12 direcciones por subred.

Encaminamiento sin clase (CLASSLESS)

A diferencia del anterior, el **encaminamiento sin clase** incluye la información de máscara de red en los mensajes de encaminamiento.

Esto permite el uso de diferentes máscaras, mediante lo que se conoce como el VLSM, optimizando el uso del espacio de direcciones disponible.



En el ejemplo anterior, a los enlaces WAN se les asignaba una subred con 14 direcciones IP, de las cuales sólo se utilizaban dos, ya que las otras subredes requerían de ese número de direcciones y todos habían de usar la misma máscara de subred. En el encaminamiento con clase utilizando **VLSM**, podemos asignar exactamente el espacio de direcciones necesario a cada subred, tal y como se muestra en la figura (14 para las subredes de hosts y 2 para cada enlace WAN).

Conclusión



La base fundamental del encaminamiento reside en el propio direccionamiento IP.

Un router procesa los datagramas recibidos y, a partir del identificador de red, selecciona la ruta apropiada para reenviar el datagrama al siguiente salto o al destino final.

Este proceso se basa en **tablas de encaminamiento** que pueden ser creadas de forma manual (encaminamiento estático) o automática (encaminamiento dinámico) con el uso de protocolos de encaminamiento.

Estos, a su vez, pueden ser de dos tipos: basados en el **algoritmo estado-enlace** o en el **algoritmo vector-distancia**.

La información del identificador de red de la dirección IP se extrae a partir de la **máscara de red**.

En el encaminamiento con clase, ésta es conocida, a partir del esquema de clases A, B y C.

En el encaminamiento sin clase, es necesario comunicar la máscara junto con la información de rutas, ya que no se utiliza el concepto de clases de direcciones, pero permite un uso más óptimo del espacio de direcciones mediante **VLSM**.

Esto lo veremos a continuación.

4 Direccionamiento IP extendido

Introducción a la Sección 4

Vas a comenzar el apartado 4:

Direccionamiento IP extendido

En este punto, conocemos los conceptos clave del encaminamiento y direccionamiento en redes IP. Sin embargo, el problema del agotamiento del espacio de direcciones IP en Internet ha llevado a una reestructuración de las políticas de asignación de direcciones y de creación de subredes. Estos son los conceptos que trataremos a continuación.

Introducción



En el esquema tradicional de direccionamiento IP, anterior al actual, el NIC (Network Information Center) asignaba bloques de direcciones clase A, B o C a las empresas u organizaciones, en función del tamaño de las redes.

Estas organizaciones, localmente, dividían el rango de direcciones mediante el proceso conocido como **Subnetting** clásico, para poder asignarlas a las diferentes subredes que componían la red global, y que el encaminamiento a través de los routers pudiese tener lugar.

Características

Recuerda que la máscara de red, que determina en las posiciones a "1" el identificador de red, para una dirección clase A es 255.0.0.0, para una clase B es 255.255.0.0 y para una clase C es 255.255.255.0.

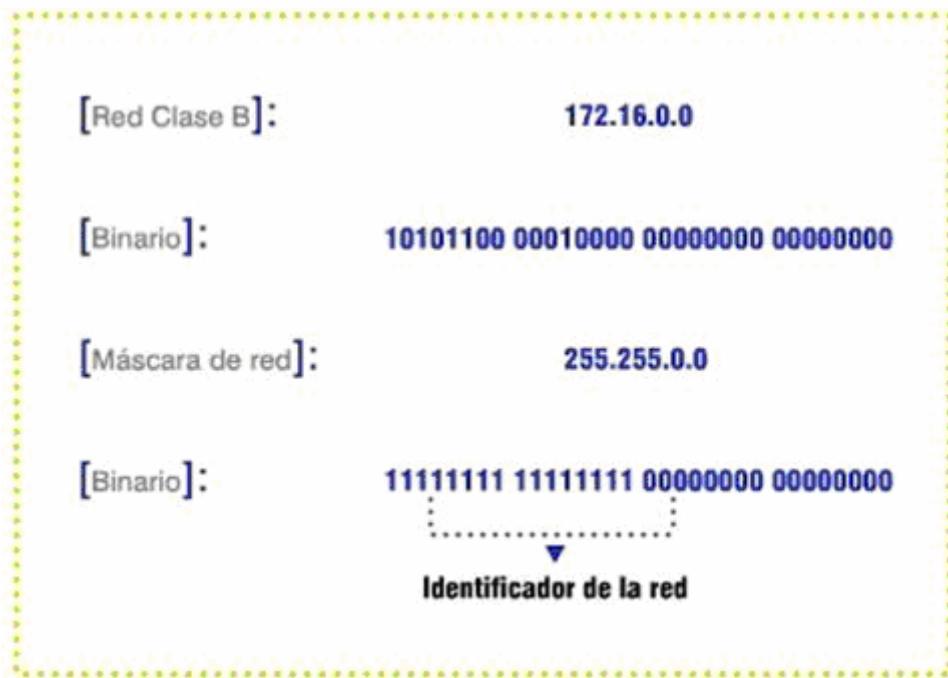
La creación de subredes basadas en este esquema determina que la red se divide en una serie de subredes, todas con la misma máscara de subred y el mismo número de direcciones IP en cada subred.

La máscara de subred es la misma máscara de red "ampliada", para que la condicionante del prefijo sea mayor.

Subnetting Clásico

Para ilustrar el subnetting clásico, veamos un ejemplo.

Digamos que a una organización se le ha asignado una dirección de red Clase B: 172.16.0.0



Al tener varias redes, necesita diferentes identificadores de red para cada una, por lo que se decide crear subredes.

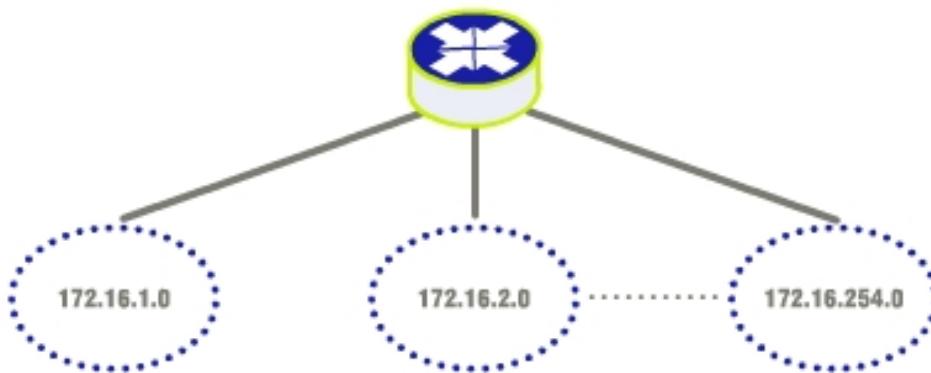
Partimos de una máscara de subred 255.255.255.0. La máscara determina qué porción de la dirección IP corresponde a la red y cuál al host.



Fíjate en la imagen: en binario, los "1s" corresponden al identificador de red y subred y los "0s" a la parte de host.

De esta forma, en este caso, en lugar de tener una red clase B con 65534 direcciones IP posibles, tenemos 254 subredes con 254 direcciones IP para cada una.

Red: 172.16.0.0
Número de direcciones IP: 65534
(172.16.0.1 al 172.16.225.254)
Máscara de subred: 255.255.255.0
Subredes: 254
De la 172.16.1.0 a la 172.16.254.0
Cada una con 254 direcciones IP



Introducción a los cálculos



El subnetting clásico es sencillo de calcular, y los routers simplifican su funcionamiento.

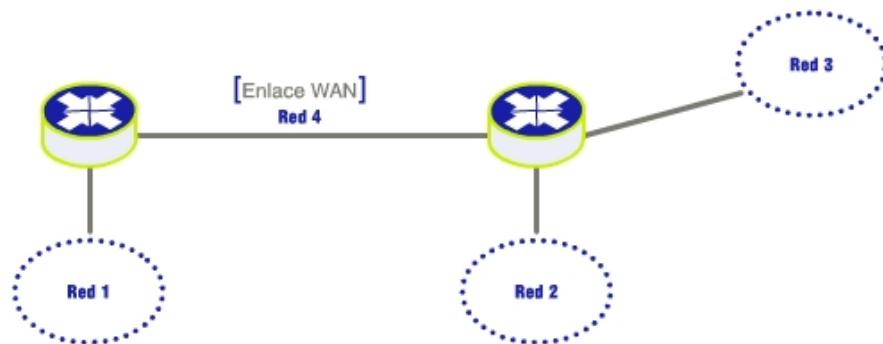
Recuerda que, en el esquema de clases, a partir del primer **byte** se determina la dirección de red.

Veamos ahora cómo se realizan los cálculos para el subnetting clásico.

Cálculo con subnetting clásico

Para el dimensionamiento de subredes se puede partir del número de direcciones necesarias para las subredes o del número de subredes totales.

Veamos el caso de la figura, donde a una organización se le asigna una dirección clase C y necesita al menos 30 direcciones por subred.



Se puede calcular el número de direcciones IP por subred con la fórmula $(2^n - 2)$, donde n es el número de bits puestos a cero en la máscara de subred. El (-2) representa las direcciones reservadas de broadcast a la subred (todos 1s) y la representación de la subred (todo 0s):

$$2^n - 2 \geq 30 \text{ direcciones IP} \quad n = 5$$

Para el cálculo del número de subredes se utiliza la misma fórmula, $(2^m - 2)$, donde m serán los bits adicionales que incluimos en la máscara de subred, es decir, $m+n =$ número de bits a "0" de la máscara de red original:

$$m+n=8$$

$$m= 8 - 5 = 3$$

$$2^m - 2 = 6 \text{ subredes posibles}$$

La máscara de subred se obtiene poniendo a "1" tantos bits adicionales como indica m:

Máscara de subred :

$$m = 3$$

255.255.255.11100000

255.255.255.224

El cálculo de los identificadores de cada subred se define combinando los bits correspondientes a la máscara de subred, siempre con los bits de identificador de host puestos a cero:

Direcciones de subred:

192.168.1.xxx00000

192.168.1.001000000 = 192.168.1.32

192.168.1.010000000 = 192.168.1.64

192.168.1.011000000 = 192.168.1.96

192.168.1.100000000 = 192.168.1.128

192.168.1.101000000 = 192.168.1.160

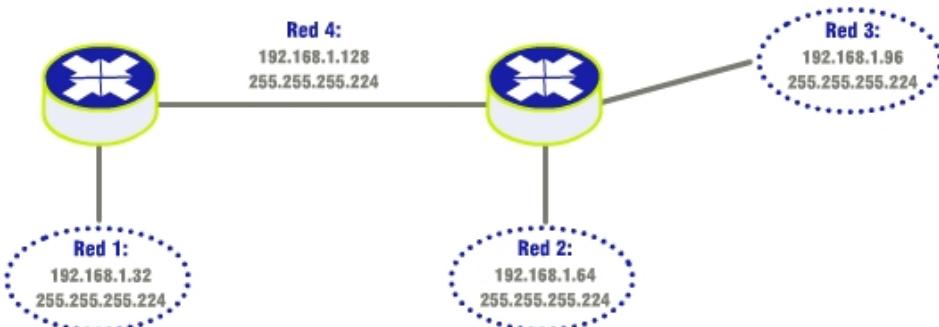
192.168.1.110000000 = 192.168.1.192

Por último, los rangos de direcciones IP para cada subred abarcan desde la siguiente a cada identificador de subred, hasta la anterior al identificador de la siguiente subred, la cual corresponde al broadcast de la subred.

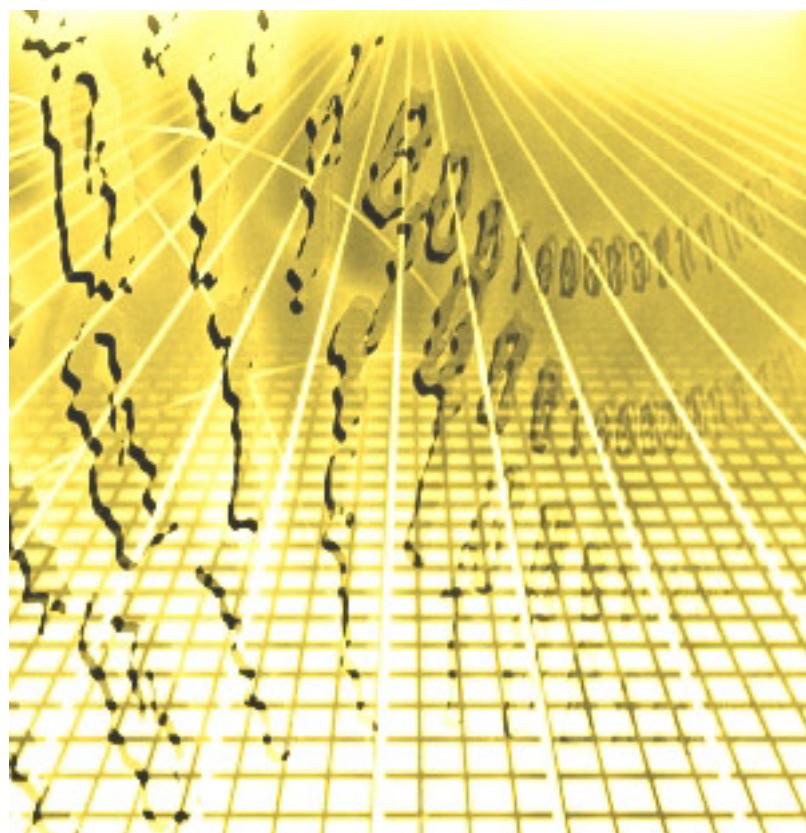
Identificador de Subred	Desde	Hasta	Dirección de Broadcast
192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223

Ahora sólo resta seleccionar 4 de las seis subredes para el esquema de red de la figura.

Fíjate que el enlace WAN corresponde a una subred, ya que los routers han de compartir direccionamiento IP a través de esas interfaces para poder comunicarse, por tanto hay que asignarles una subred, aunque sólo se requieran 2 direcciones IP.



VLSM: Máscaras de subred de longitud variable



El subnetting clásico presenta un inconveniente: al dimensionar con la misma máscara todas las subredes, se desperdician direcciones IP, como en el enlace WAN del ejemplo anterior.

El criterio de dimensionamiento se basa en el número de direcciones IP o en el número de subredes necesarias, lo que obliga a que todas las subredes tengan el mismo número de direcciones. **Hoy por hoy**, la creación de subredes se basa en **VLSM**.

El término máscara de subred de longitud variable (Variable Length Subnet Mask) hace referencia al hecho de que **una red puede dividirse en subredes con diferentes máscaras**, contrario al concepto de subnetting clásico que sólo permite el uso de una máscara de subred.

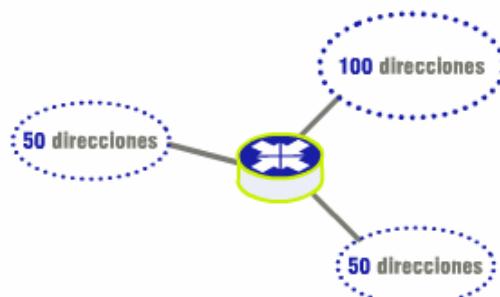
Esto aporta mayor flexibilidad al dividir una red, a la vez que se optimiza la asignación de hosts por subred, es decir, la utilización del espacio de direcciones, cuestión preponderante en Internet a raíz del agotamiento del espacio de direcciones.

Ejemplo de VLSM

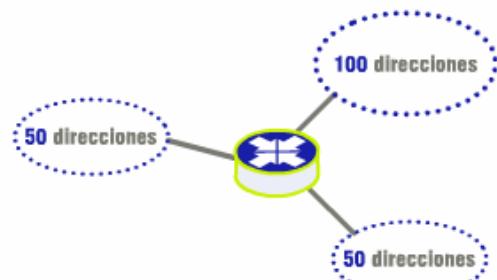
Veamos un ejemplo para aclarar los conceptos.

Partiendo de una red clase C (192.214.11.0), queremos dividirla en tres subredes. La primera con 100 direcciones IP y las otras dos con 50 c/u.

[Planteamiento]	
Dirección de red:	192.214.11.0
Máscara de Red:	255.255.255.0
Nº subredes:	3
Hosts subred 1:	100
Hosts subred 2 y 3:	50



[Planteamiento]	
Dirección de red:	192.214.11.0
Máscara de Red:	255.255.255.0
Nº subredes:	3
Hosts subred 1:	100
Hosts subred 2 y 3:	50

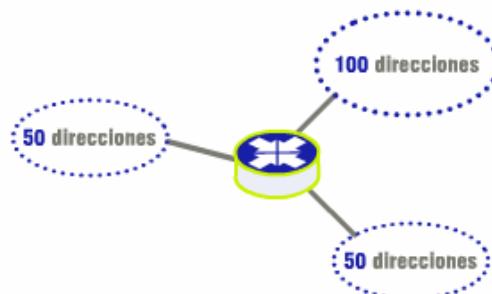


Si utilizamos subnetting clásico, fíjate en la tabla, podemos tener dos subredes con 128 hosts c/u, o 4 subredes de 64 hosts. Ningún caso satisface la propuesta.

[Subnetting clásico clase C]				
último byte	binario	nº subredes	nº hosts	
128	10000000	0	-	
192	11000000	2	62	
224	11100000	6	30	
240	11110000	14	14	
248	11111000	30	6	
252	11111100	62	2	

[Planteamiento]	
Dirección de red:	192.214.11.0
Máscara de Red:	255.255.255.0
Nº subredes:	3
Hosts subred 1:	100
Hosts subred 2 y 3:	50

[VLSM]	
Dirección de red:	192.214.11.0
Máscara de sRed 1:	255.255.255.128
Nº subredes:	2
Dir subred 1:	192.214.11.0
Dir subred 2:	192.214.11.128
Máscara de sred2:	255.255.255.192
Nº subredes:	2
Dir subred 3:	192.214.11.128
Dir subred 4:	192.214.11.192
Hosts subred:	64



Con VLSM, podemos dividir la red en dos subredes utilizando la máscara 255.255.255.128 y luego, subdividir una de las subredes en dos subredes adicionales, utilizando la máscara 255.255.255.192. El resultado es un subred con 128 hosts posibles y dos subredes de 64 hosts c/u.

[Planteamiento]	
Dirección de red:	192.214.11.0
Máscara de Red:	255.255.255.0
Nº subredes:	3
Hosts subred 1:	100
Hosts subred 2 y 3:	50

Red 1
192.214.11.0 (128 hosts)
Masc. 255.255.255.128
192.214.11.0 a 192.214.11.127

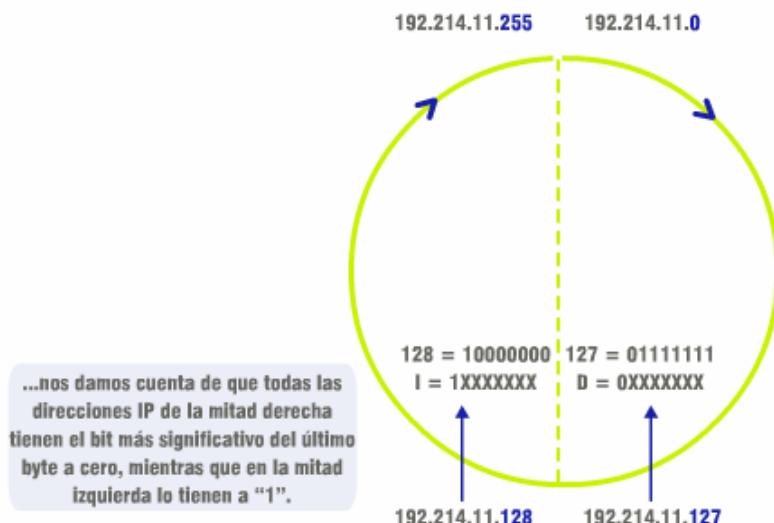
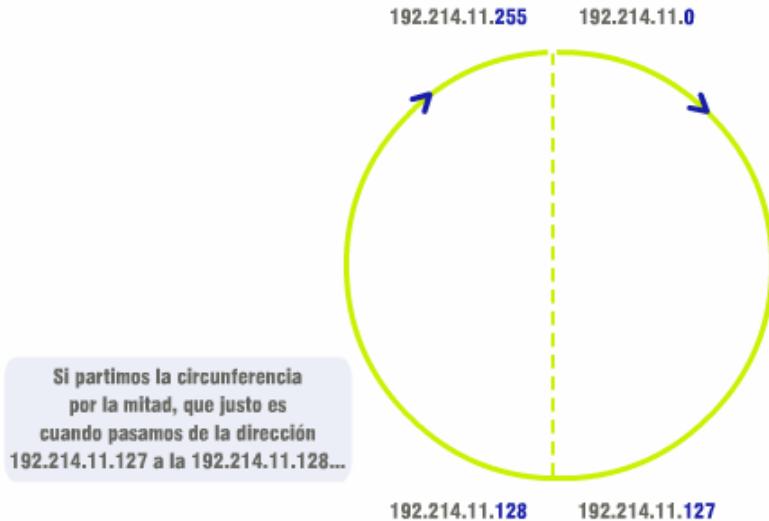
Red 2
192.214.11.128 (64 hosts)
Masc. 255.255.255.192
192.214.11.128 a 192.214.11.191

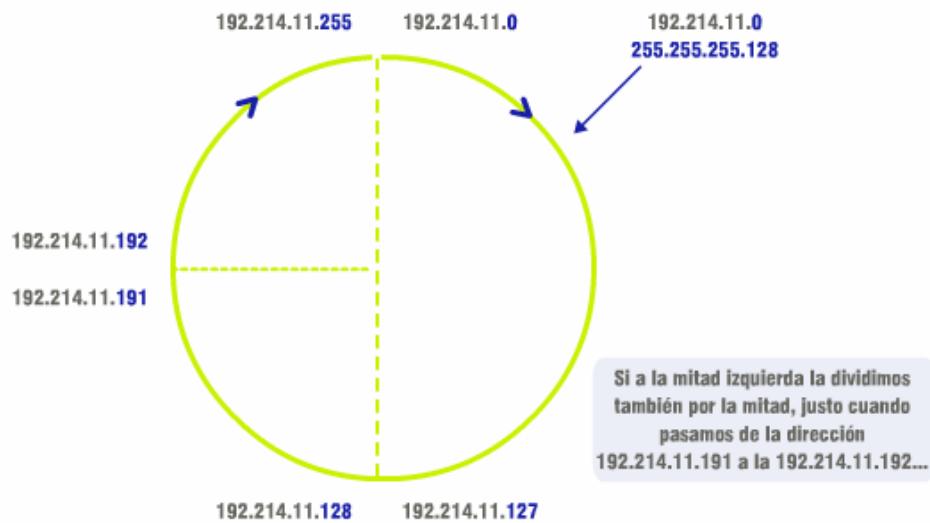
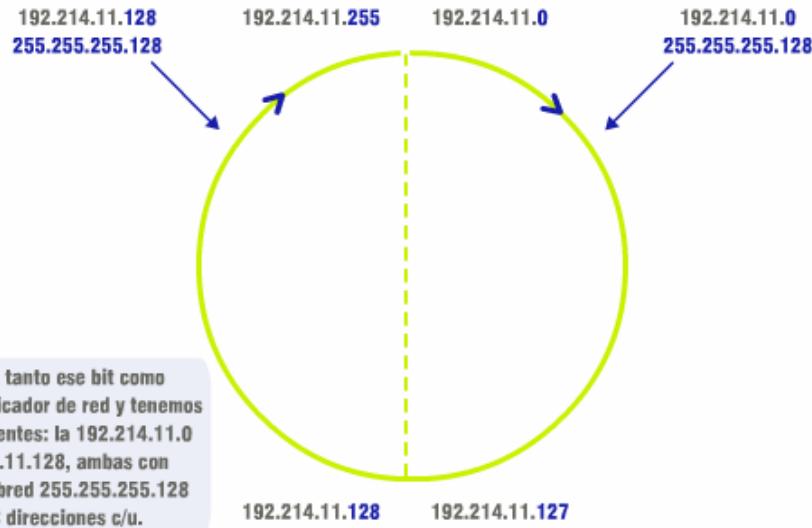
100 direcciones
50 direcciones
50 direcciones

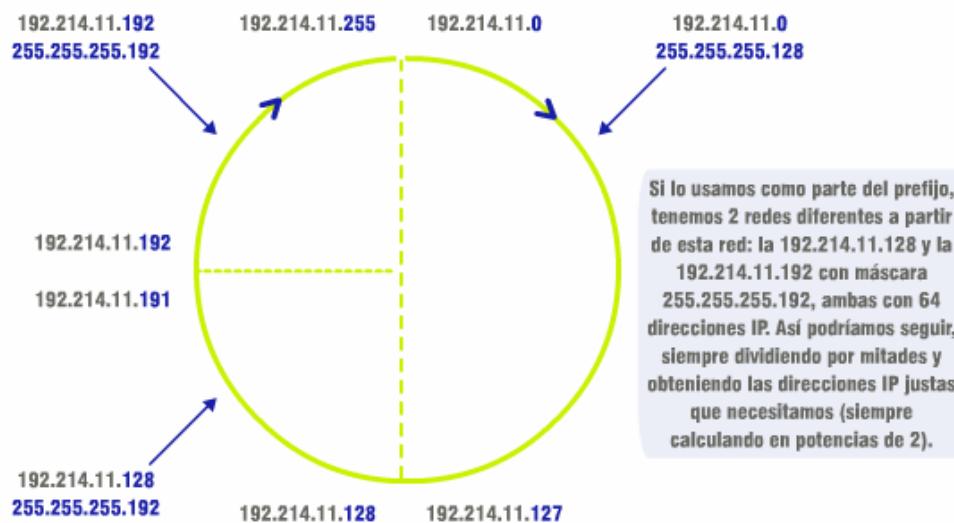
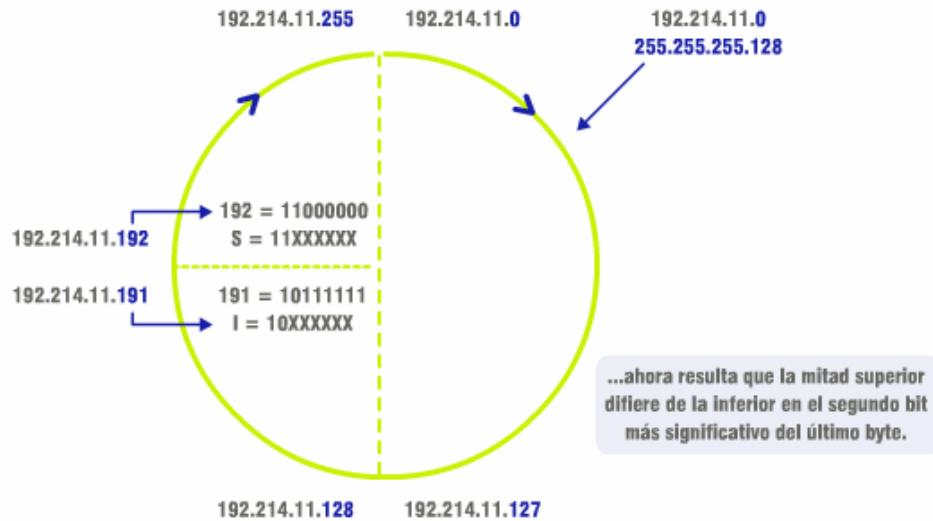
Red 3
192.214.11.192 (64 hosts)
Masc. 255.255.255.192
192.214.11.192 a 192.214.11.255

Ejemplo de VLSM

Piensa que el rango de direcciones IP es una circunferencia que empieza con la dirección 192.214.11.0 y acaba con la 192.214.11.255.







Direccionamiento actual en Internet

Anteriormente hablamos del problema del agotamiento de direcciones (**ROAS** – Run Out of Address Space).



Podemos concluir que VLSM permite ralentizar el agotamiento mediante una distribución más óptima del espacio de direcciones. Profundicemos un poco más en ello.

El esquema de clases, discutido en capítulos anteriores, no es eficiente desde hace unos años, la comunidad Internet, a través de la ICANN, gestiona la asignación de direcciones de forma diferente:

se asignan rangos de direcciones IP llamados **AGREGADOS**, según el **número de direcciones necesarias**, dividiendo, mediante VLSM, grandes espacios asignados a organismos regionales: el RIPE, ARIN y AP-NIC.

Cada uno de ellos gestiona una zona geográfica determinada.

Por ejemplo, el RIPE es el encargado de Europa y su zona de influencia.

Las direcciones asignadas previas a este cambio, se mantienen.

Lo que se hace es “**recolectar**” los rangos contiguos restantes para crear los llamados **AGREGADOS**.

Espacio de direcciones	Área de Asignación	Fecha
61.0.0.0 a 61.255.255.255	APNIC – Costa Pacífico	1997
62.0.0.0 a 62.255.255.255	RIPE – Europa	1997
63.0.0.0 a 64.255.255.255	ARIN	1997/1999
128.0.0.0 a 191.255.255.255	Varios (previo a la nueva estructura)	1993
192.0.0.0 a 192.255.255.255	Multiregional	1993
193.0.0.0 a 195.255.255.255	RIPE - Europa	1993
212.0.0.0 a 213.255.255.255	RIPE - Europa	1997/1999
204.0.0.0 a 209.255.255.255	ARIN - Norteamérica	1994/1996

En la imagen se puede observar parte de la asignación actual del espacio de direcciones IP.

CIDR

255.0.0.0 = /8	255.255.240.0 = /20
255.128.0.0 = /9	255.255.248.0 = /21
255.192.0.0 = /10	255.255.252.0 = /22
255.224.0.0 = /11	255.255.254.0 = /23
255.240.0.0 = /12	255.255.255.0 = /24
255.248.0.0 = /13	255.255.255.128 = /25
255.252.0.0 = /14	255.255.255.192 = /26
255.254.0.0 = /15	255.255.255.224 = /27
255.255.0.0 = /16	255.255.255.240 = /28
255.255.128.0 = /17	255.255.255.248 = /29
255.255.192.0 = /18	255.255.255.252 = /30
255.255.224.0 = /19	

Los Agregados se representan mediante un identificador de red que abarque las direcciones que se “agregan”, es decir, que se pueden representar conjuntamente sin incluir direcciones de otros rangos.

Para ello se crea un nuevo concepto: el CIDR.

El encaminamiento interdominio sin clase, CIDR (Classless Interdomain Routing), es un estándar que permite representar las redes y su máscara asociada mediante la notación X/N, donde X es el identificador de red y N el número de bits de la máscara de red.

No hablamos de clases de direcciones, sino de rangos o agregados, por ejemplo, el rango de direcciones comprendido entre 62.0.0.0 y 62.255.255.255 se representaría por el agregado **62.0.0.0/8**, es decir, una máscara equivalente a 255.0.0.0.

En la imagen puedes observar las combinaciones posibles de CIDR.

Fíjate que la representación por CIDR abarca desde 8 bits de prefijo (equivalente a una clase A) hasta 30, que sería lo mínimo para tener 2 direcciones IP en una subred.

Relación de ideas clave

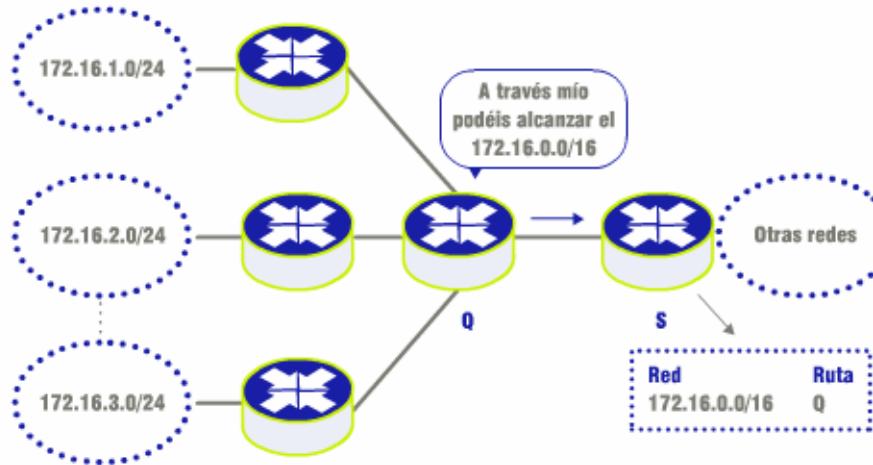


Es claro que el CIDR combinado con VLSM optimiza la asignación de direcciones y ralentiza el agotamiento del espacio público.

¿Pero qué más aportan?

Veamos.

Agregación de rutas



Cuando hablamos de encaminamiento, definimos que **un router posee tablas donde lista las redes y la ruta para llegar a ellas**. En una red muy grande, con cientos, incluso miles de subredes, estas tablas serían inmensas, consumiendo la capacidad de procesamiento de los routers.

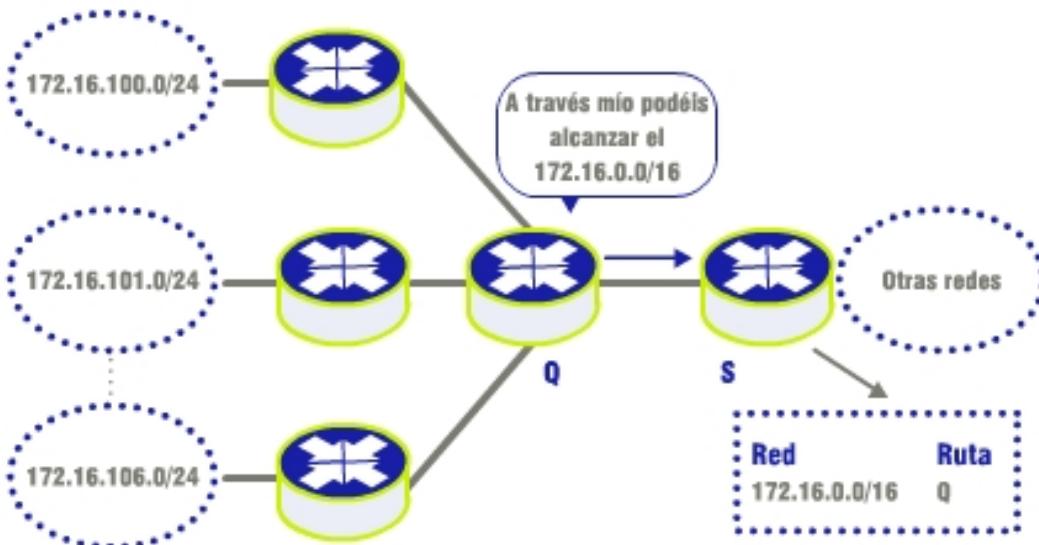
Sin embargo, un router externo a esta red, lo único que necesita es información de cómo llegar a ella, no a cada subred que la compone. **Ese problema se lo deja al router de "acceso" a la red.**

Esa capacidad de informar y registrar rutas "resumidas" a través de agregados de direcciones, es lo que se denomina **sumarización o agregación de rutas**.

Ejemplo de agregación

La agregación aporta una gran simplificación en las tablas de encaminamiento de los routers de Internet y cualquier red IP.

Veamos un ejemplo de cómo crear una ruta agregada.



Tenemos las siguientes redes conectadas al router que anuncia su existencia:

172.16.100.0/24

172.16.101.0/24

172.16.102.0/24

172.16.103.0/24

172.16.104.0/24

172.16.105.0/24

172.16.106.0/24

Para crear la ruta agregada seguimos los siguientes pasos:

Primero, representamos en binario las direcciones, como muestra la figura.

Segundo, de izquierda a derecha, seleccionamos los bits que coinciden entre todas las direcciones. En nuestro ejemplo, los **primeros 20 bits**.

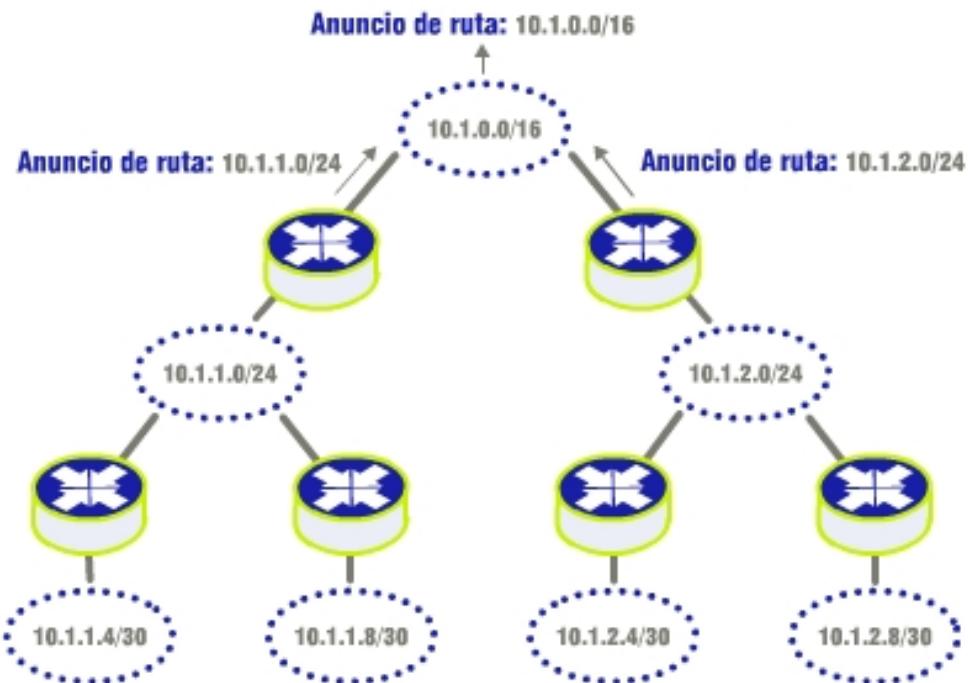
[Identificador de Red]	[Equivalente binario]
172.16.100.0	10101100.0001000.01100100.0
172.16.101.0	10101100.0001000.01100101.0
172.16.102.0	10101100.0001000.01100110.0
172.16.103.0	10101100.0001000.01100111.0
172.16.104.0	10101100.0001000.01101000.0
172.16.105.0	10101100.0001000.01101001.0
172.16.106.0	10101100.0001000.01101010.0
172.16.96.0 /20	10101100.0001000.01100000.0

En tercer lugar, convertimos a decimal la dirección resultante de dejar esos 20 bits y poner a cero los restantes: esa es la **ruta agregada** (la dirección de red que representa las 7 redes), seguida de /20 (indicador del prefijo).

Subredes jerarquizadas

La agregación siempre será mucho más eficiente y evitará problemas si se estructura jerárquicamente.

Veamos.



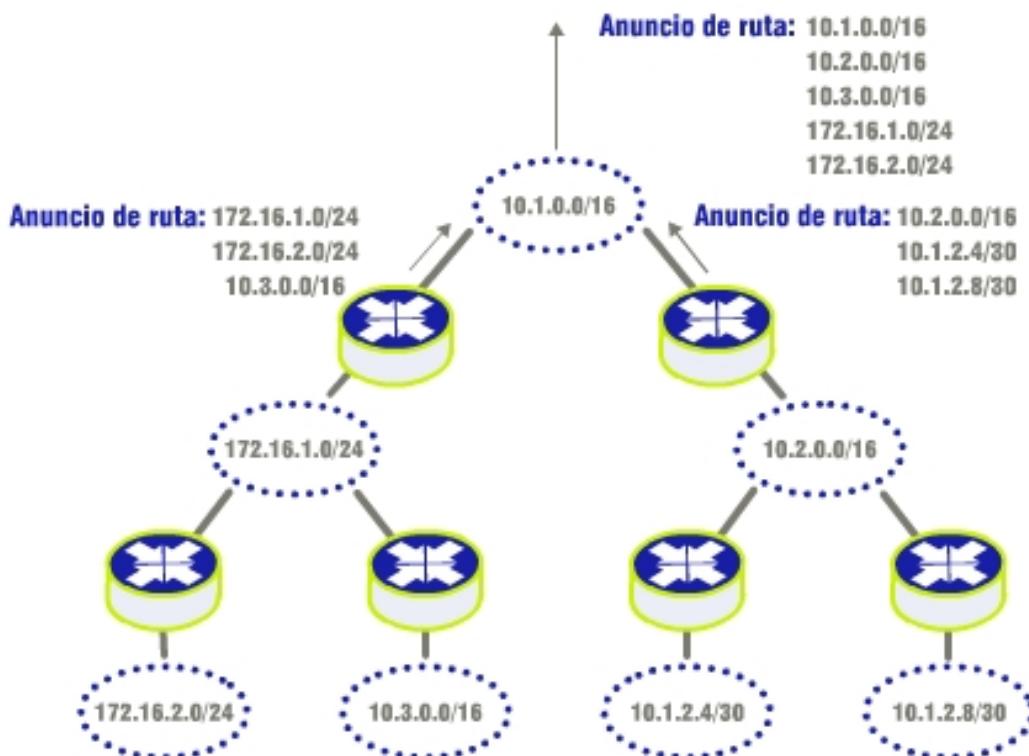
Una red jerarquizada, es aquella donde las subredes con mayor prefijo se sitúan “al final” de la estructura de árbol, y las de menor prefijo al principio, tal y como muestra la figura.

Permite utilizar protocolos con la opción de agregación de rutas habilitada.

En cambio, una red no jerarquizada es la que se muestra en la figura.

Fíjate que el anuncio de rutas no puede hacerse por agregación, pues algunas redes resultarían inaccesibles, al anunciar rutas agregadas que no proceden.

Esto implica el uso de protocolos sin opción de agregación.



Conclusión



La agregación siempre será mucho más eficiente y evitará problemas si se estructura jerárquicamente.

Veamos.

Los conceptos fundamentales del direccionamiento IP no cambian. Los routers reenvían datagramas basándose en la dirección IP destino, y en tablas de encaminamiento.

Sin embargo, el agotamiento del espacio de direcciones ha introducido un nuevo esquema de asignación, conocido como CIDR, que permite distribuir más racionalmente las direcciones IP públicas. También, el concepto de subredes varía introduciéndose el VLSM.

En cualquiera de los casos, para la selección de los protocolos de encaminamiento se ha de tener en cuenta si se realizará **encaminamiento con clase o sin clase**, y verificar apropiadamente el diseño de la red IP y la distribución de direcciones.

La agregación facilita y simplifica enormemente el trabajo de los routers, pero mal implementada puede ocasionar “**agujeros negros**”, es decir, el encaminamiento de datagramas hasta un punto donde no pueden alcanzar su destino.

5 Protocolos de encaminamiento

Introducción a la Sección 5

Vas a comenzar el apartado 5:

Protocolos de encaminamiento

En capítulos anteriores analizamos los principios básicos del encaminamiento. Vamos a ver ahora algunos de los protocolos de encaminamiento que implementan los algoritmos anteriormente estudiados y cómo se estructuran las redes desde el punto de vista de estos protocolos.

Mapa de protocolos

Nombre	Definición	Vector-Distancia	Estado-Enlace	Classless	Classfull
RIP v1	Routing Information Protocol	X		X	
RIPv2	Routing Information Protocol versión 2	X			X
IGRP	Interior Gateway Routing Protocol (protocolo propietario)	X		X	
EIGRP	Enhanced Interior Gateway Routing Protocol (protocolo propietario)	X	X		X
OSPF	Open Shortest Path First		X		X
IS-IS	Intermediate System to Intermediate System (arquitectura de protocolos OSI)		X		X
BGP	Borde Gateway Protocol	X			X

En la imagen puedes observar un mapa de los protocolos de encaminamiento más utilizados y su clasificación, de acuerdo a los tipos de encaminamiento que vimos anteriormente.

De ellos, IGRP y EIGRP son protocolos propietarios, y el protocolo IS-IS, cuyo funcionamiento es similar al OSPF, es un protocolo de la arquitectura OSI, compatible con IP y CLNP (connection-less network protocol).

Mapa de protocolos (II)

Nombre	Definición	Distancia Administrativa	Convergencia	Tamaño de la red
RIP v1	Routing Information Protocol	120	Lenta	Media
RIPv2	Routing Information Protocol versión 2	120	Lenta	Media
IGRP	Interior Gateway Routing Protocol (protocolo propietario)	100	Muy lenta	Grande
EIGRP	Enhanced Interior Gateway Routing Protocol (protocolo propietario)	90	Muy rápida	Grande
OSPF	Open Shortest Path First	110	Rápida	Grande
IS-IS	Intermediate System to Intermediate System (arquitectura de protocolos OSI)	115	Rápida	Muy grande
BGP	Borde Gateway Protocol*	N/A	N/A	N/A

(*) No aplica. Veremos más adelante el uso de BGP.

Cuando se utilizan protocolos de encaminamiento, es importante tener en cuenta no sólo el tipo de algoritmo y la clase de encaminamiento que utilizan , sino también una serie de características que los diferencian.

Veamos.

En una red IP se pueden utilizar varios protocolos de encaminamiento de forma simultánea, por lo que se recibe información de encaminamiento diversa.. La **Distancia Administrativa** se utiliza para preponderar la confianza que se tiene en rutas informadas a través de los diferentes protocolos, y se mide mediante un número entero.

La tabla muestra los valores por defecto asociados a los diferentes protocolos . Cero (0) representa la ruta de más confianza, y 255 define que no se enviarán paquetes por esa ruta.

La **convergencia** se define como el tiempo que le toma a los routers de una red ponerse de acuerdo y conocer un cambio en la topología de la misma, es decir, en sincronizar sus tablas de encaminamiento. A mayor tiempo de convergencia, menos eficiente el protocolo y mayor probabilidad de destinos inaccesible por largos periodos.

Finalmente, ciertos protocolos, por sus características de operación, están diseñados para **redes grandes**, y otros para redes más **pequeñas**.

Protocolo RIP



De todos los protocolos mencionados, vamos a definir y profundizar en el protocolo RIP, por ser uno de los más extendidos en su uso, además de ser representativo de los protocolos vector-distancia. Luego detallaremos el OSPF, como protocolo representativo del algoritmo estado-enlace.

El protocolo RIP, del tipo vector-distancia, utiliza como métrica para determinar el mejor camino, el número de saltos. Una ruta directa corresponde a métrica 1. También define un máximo de 15 saltos, siendo 16 conteo infinito (ruta no permitida).

Por ende, está diseñado para redes pequeñas o con pocos routers, y es ineficiente cuando existen enlaces WAN lentos.

La versión 1 sólo puede ser utilizada en encaminamiento con clase (classful), ya que los mensajes no contienen información de la máscara de subred.

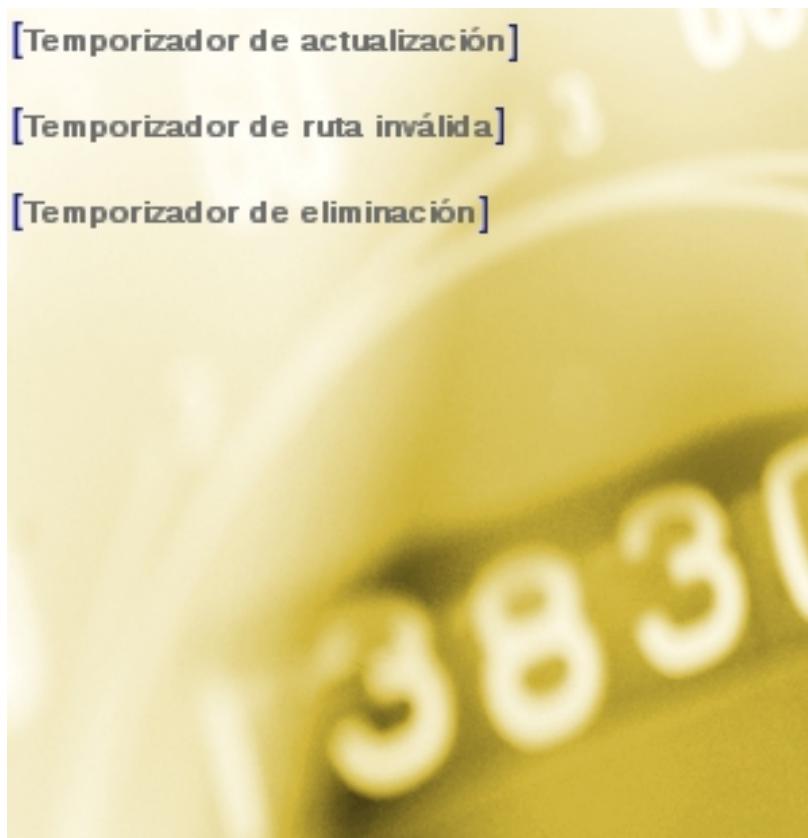
La versión 2, en cambio, es utilizada para encaminamiento sin clase (classless), ya que incluye esta información en los mensajes.

Temporizadores en RIP

[Temporizador de actualización]

[Temporizador de ruta inválida]

[Temporizador de eliminación]



Para proveer estabilidad en las tablas de encaminamiento de los routers que implementan RIP, el protocolo utiliza una serie de temporizadores.

RIP utiliza tres temporizadores para regular la estabilidad de la información de las tablas de encaminamiento.

Temporizador de actualización

Define que cada 30 segundos (típicamente), se envía la tabla de encaminamiento por todas las interfaces del router.

Temporizador de ruta inválida

Define el tiempo de expiración de una ruta (90 segundos).

Se determina que una ruta no es válida cuando pasado el periodo de tiempo no se han escuchado actualizaciones del router que anunció esa ruta en particular.

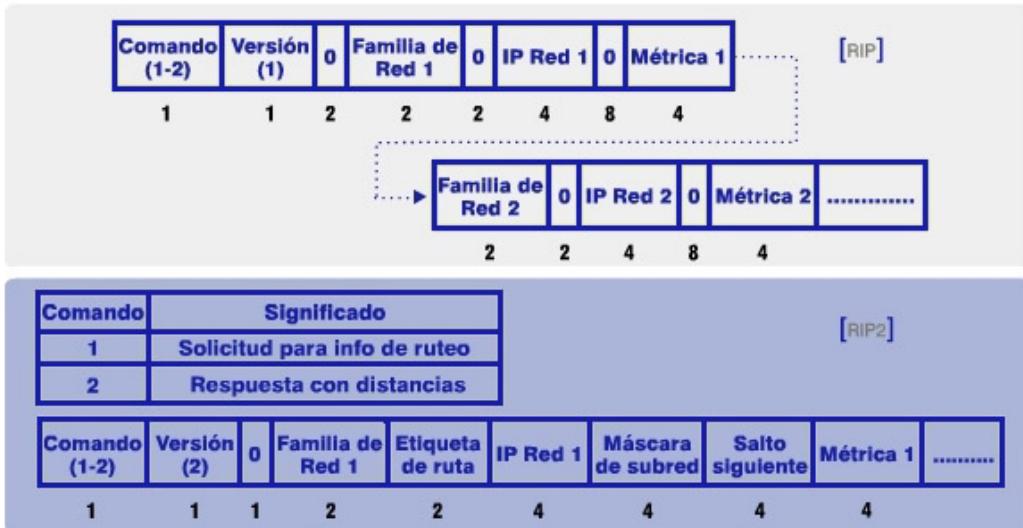
A continuación, el router envía a sus vecinos mensajes de actualización anunciando que la ruta no es válida.

Temporizador de eliminación

Define el tiempo que transcurre entre la definición de una ruta inválida y su eliminación permanente de la tabla (240 segundos).

Formato de mensajes RIP

Longitudes en bytes



Formato de mensajes RIP. RIP es un protocolo vector-distancia, y sigue la mecánica que vimos en capítulos anteriores. Se transporta utilizando UDP (puerto 520) mediante broadcast IP. Su implementación es muy sencilla.

En la figura se muestra el formato de un paquete RIPv1 y RIPv2. Fíjate que los mensajes serán tan grandes como la propia tabla de encaminamiento del router. Estos se difunden (broadcast) por todas las interfaces de un router, siendo interpretados por los routers que se encuentren conectados a ellas, es decir, los "vecinos".

Comando

Indica si el paquete es de solicitud o respuesta.

Versión

Especifica la versión RIP utilizada.

Familia de red

Especifica la familia de direcciones utilizada, ya que RIP está diseñado para transportar información de encaminamiento de diferentes protocolos de nivel 3. Para IP el valor es 2.

Etiqueta de la ruta

Diferencia entre rutas internas (conocidas por RIP) y rutas externas (conocidas de otros protocolos).

Dirección IP red

Define la dirección IP de red destino (en un solo paquete RIP se pueden definir hasta 25 rutas).

Máscara de subred

Define explícitamente la máscara del parámetro de red.

Máscara de subred

Define explícitamente la máscara del parámetro de red.

Salto siguiente

Indica la dirección IP del router al cual se deben enviar los paquetes con destino a la red definida.

Métrica

Indica el número de saltos para alcanzar la red.

Ejemplo de un mensaje RIP

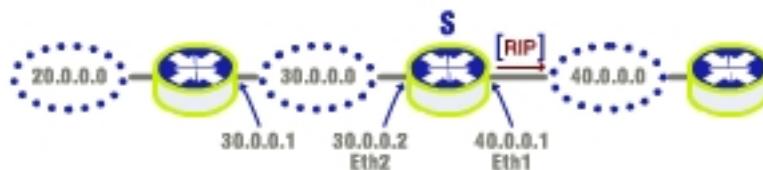


TABLA DE ENCAMINAMIENTO DE S			
Red	Ruta	Interfaz	Métrica (coste)
20.0.0.0	30.0.0.1	ETH2	2
30.0.0.0	30.0.0.2 (Directa)	ETH2	1
40.0.0.0	40.0.0.1 (Directa)	ETH1	1

Veamos el ejemplo de un mensaje RIPv1 enviado por el router S a través de la interfaz Ethernet 1. La tabla de encaminamiento de S se muestra en la figura.

El mensaje generado ha de contener las direcciones de red y la métrica para alcanzarlas, exceptuando la red asociada a la interfaz por donde se envía el mensaje.

El mensaje generado sería el que aparece en la siguiente pantalla.

Formato de mensajes RIP (II)

[mensaje RIPv1 enviado por la interfaz ETH1]

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....□¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

La cabecera ethernet
contiene como dirección destino broadcast.

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

La dirección MAC origen corresponde a la interfaz correspondiente del router.

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

El campo tipo de protocolo le indica a ethernet que contiene un datagrama IP.

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

El datagrama IP informa (en el campo tipo de protocolo de su cabecera, valor 17) que contiene un mensaje UDP.

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

La dirección IP origen (la del router) es 40.0.0.1

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

La dirección IP destino es broadcast (255.255.255.255).

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

La cabecera UDP indica que el puerto origen y el puerto destino corresponden al protocolo RIP (520 = 0208₁₆).

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....□¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

Ahora, éste es el mensaje RIP. El router que lo procesa determina, interpretando los campos, lo siguiente:

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....□¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

- Comando de respuesta (2).

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....□¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

- Versión de protocolo RIP = 1

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....□¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

- Familia de red = 2, es una dirección de red IP.

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00	-----
00 00 00 00 00 01

- Dirección de red 1 = 20.0.0.1

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00	-----
00 00 00 00 00 01

- Métrica = 2

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

- Familia de red = 2

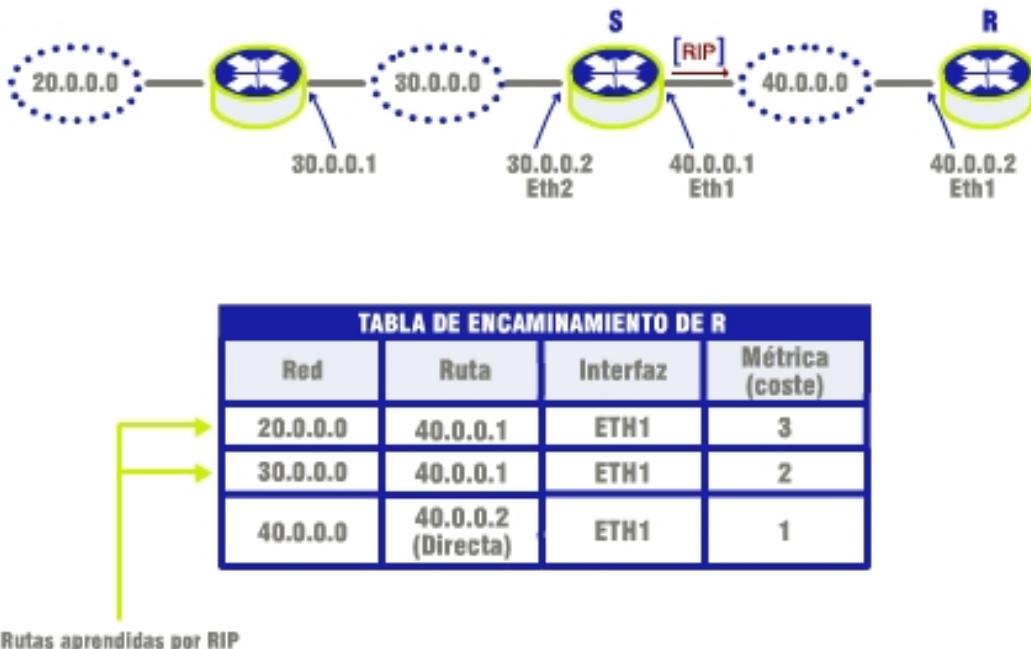
HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

- Dirección de red 2 = 30.0.0.1

HEX	ASCII
ff ff ff ff ff ff 00 e0 1e a9 c6 b7 08 00 45 00©Æ..E.
00 48 00 00 00 00 00 02 11 90 a5 28 00 00 01 ff ff	.H.....Û¥(....
ff ff 02 08 02 08 00 34 00 00 02 01 00 00 00 024.....
00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 00 02 00 00 1e 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01

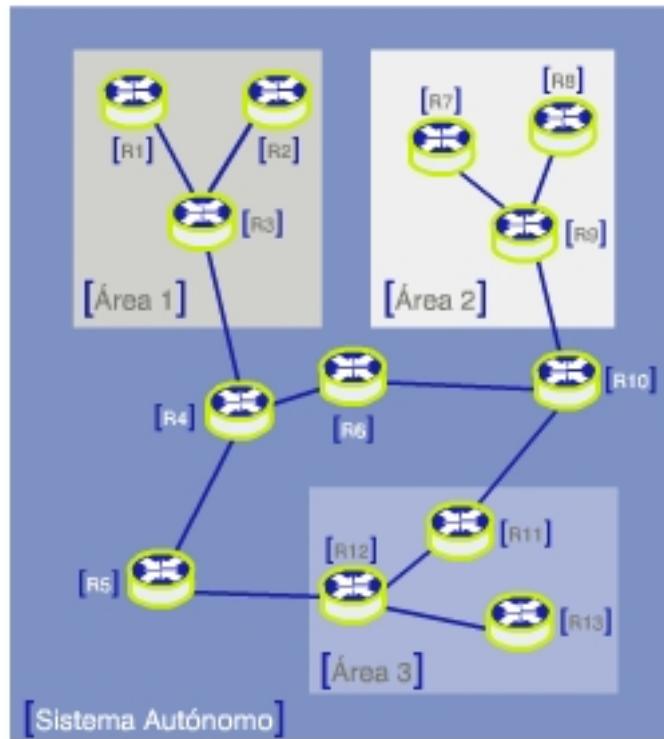
- Métrica = 1

Formato de mensajes RIP (III)



La resultante del envío de este mensaje RIP se refleja en la tabla de encaminamiento del router R.

Protocolo OSPF



El funcionamiento de RIP representa la generalidad de los protocolos tipo vector-distancia.

Veamos ahora un protocolo, tipo estado-enlace, indispensable hoy por hoy en las redes IP: el OSPF.

Open Shortest Path First es un protocolo de encaminamiento estado-enlace muy robusto y algo más complejo que RIP.

Su funcionamiento se basa en el envío de mensajes de anuncio de estado de enlace a todos los routers dentro de una misma área jerárquica. Dichas áreas jerárquicas son grupos de redes contiguas pertenecientes a un Sistema mayor (denominado autónomo y que definiremos más adelante), el cual se designa como la entidad de más valor en la jerarquía de áreas.

En la figura recuerda que, en definitiva, los enlaces entre los routers representan redes IP.

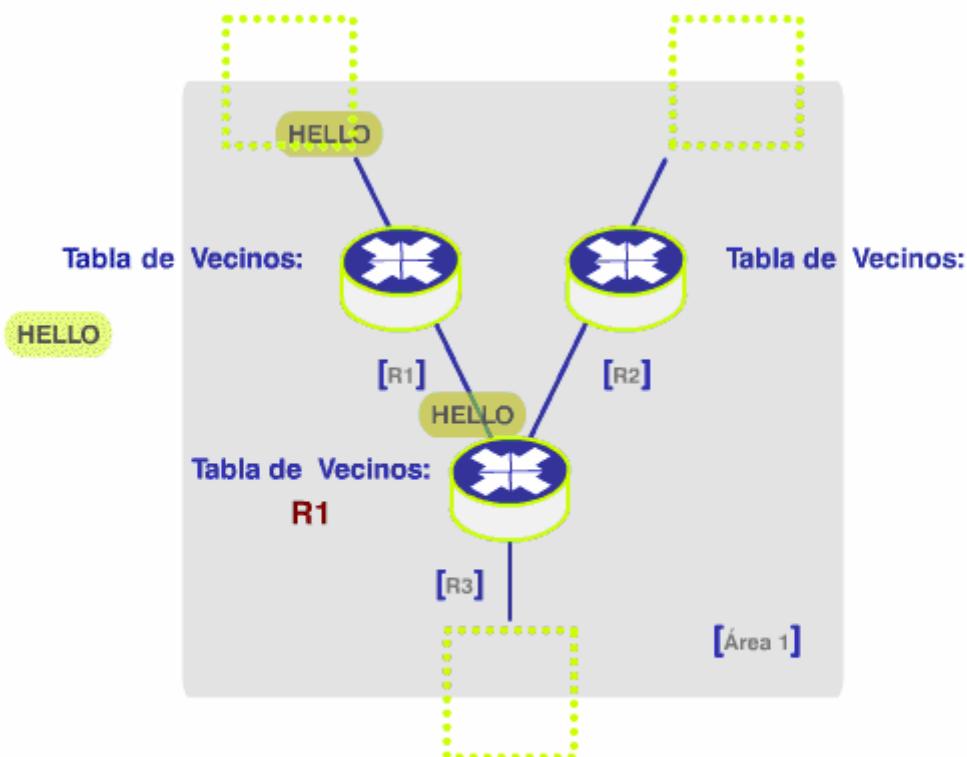
Protocolo OSPF (II)



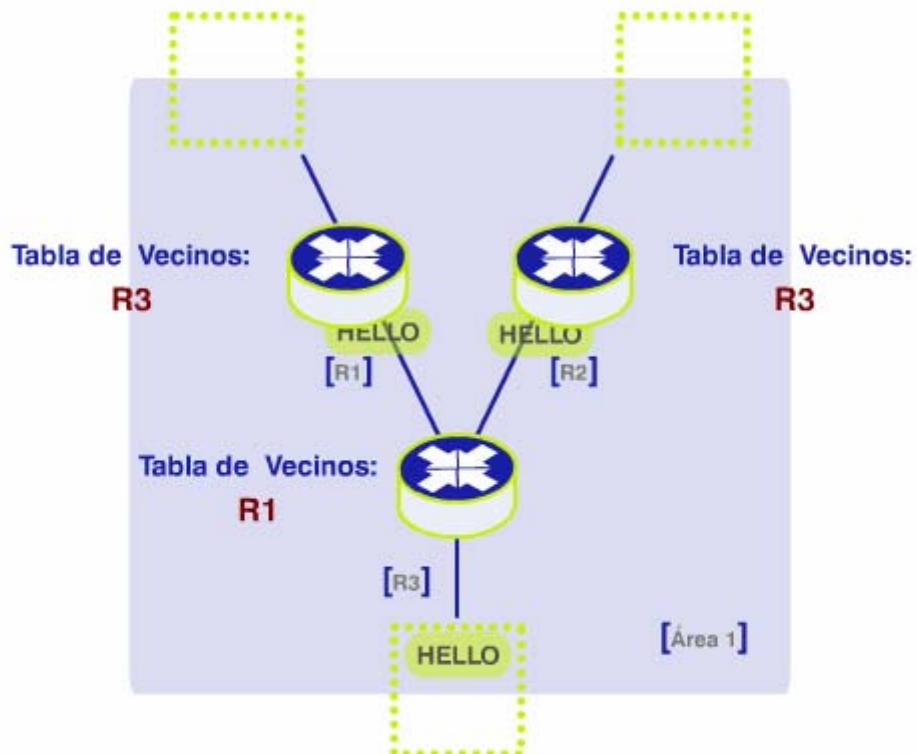
La operación del protocolo OSPF se puede dividir en tres categorías: Inicialización de vecinos y adyacencias, propagación de mensajes LSA y cálculo del algoritmo SPF.

Vamos a ver cada paso y sus definiciones.

Inicialización

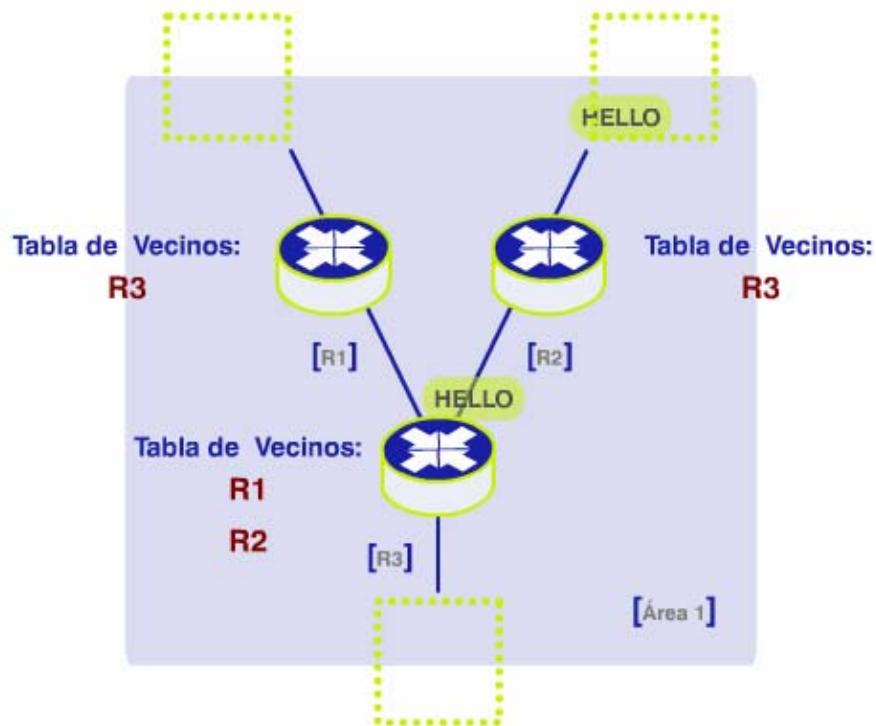


Un vecino es un router conectado a alguna de las interfaces del router dentro de su área, y con el que puede crear una adyacencia (conexión lógica).



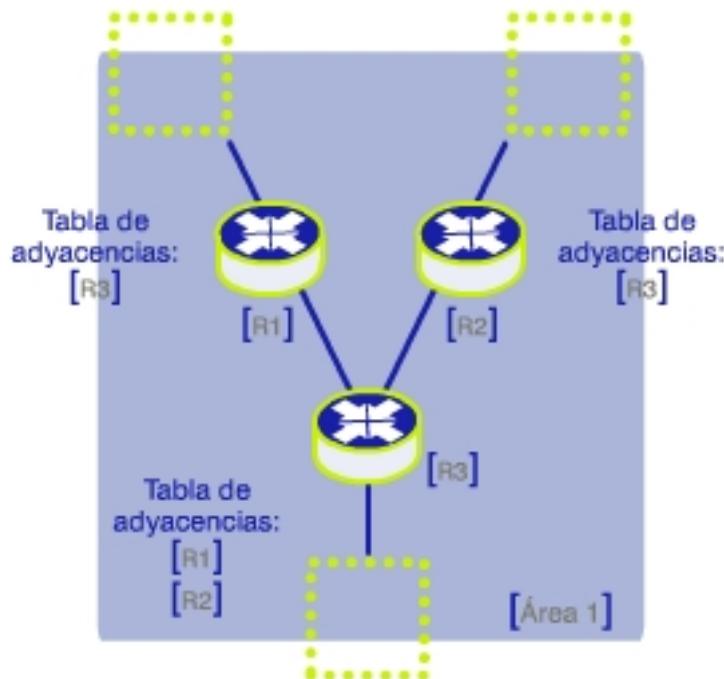
El proceso de inicialización comienza enviando mensajes de HELLO para descubrir los posibles vecinos.

Los routers que escuchan el mensaje añaden la información del anunciante a sus tablas de "vecinos" y contestan con mensajes de HELLO, de tal forma que el primer router pueda añadirlos a su propia tabla.



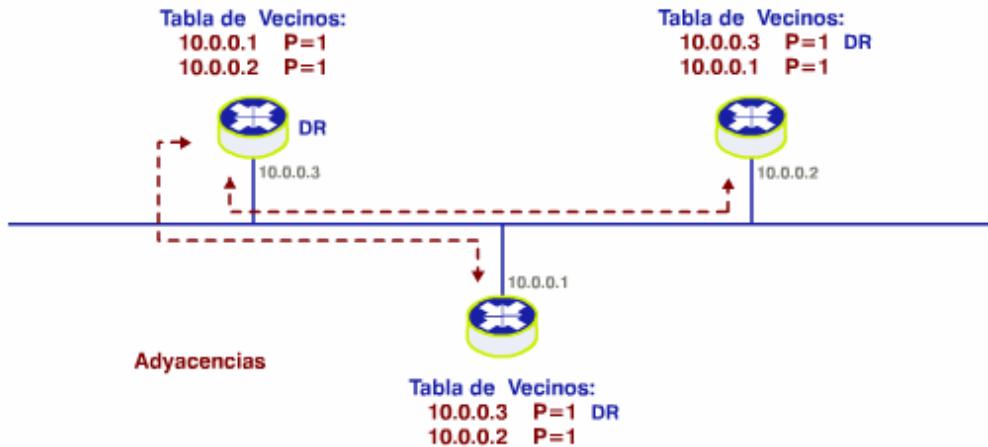
Una vez se han descubierto los vecinos, se establecen las adyacencias. Éstas han de ser definidas para que los routers puedan intercambiar mensajes de anuncio de estado del enlace (LSA).

Inicialización (II)



Por defecto, cuando dos routers están conectados mediante enlaces punto a punto o a través de redes NMBA (non broadcast multi access), es decir, redes como Frame Relay o ATM donde no existe difusión como en las LAN, la adyacencia se define inmediatamente después del intercambio de mensajes de hello entre los routers vecinos.

Inicialización (III)



En redes de difusión (LAN) es necesario escoger, de entre todos los routers conectados a la red, cuál será el router designado (DR), es decir, con el que los otros crearán sus adyacencias. Esto es para evitar adyacencias de todos con todos innecesariamente. También deberá existir un router designado de backup (BDR).

Para escoger el DR, en el intercambio de mensajes de HELLO, los routers analizan el campo de Prioridad y se escoge el de mayor valor o, a igual prioridad, el de mayor identificador (asociado a la dirección IP de mayor valor de sus interfaces).

Finalmente, las adyacencias se crearán de los routers con el designado. Recuerda que el intercambio de mensajes LSA se realizará sólo entre routers adyacentes.

Propagación de LSAs

Una vez definidas las adyacencias, pasamos a la siguiente fase: propagación de mensajes de anuncios de estado-enlace.

TIPO DE RED	DIRECCIÓN DE MULTICAST	DESCRIPCIÓN
Enlace punto a punto (enlace NMBA)	224.0.0.5	Mensaje para todos los routers que implementen OSPF
Difusión (LAN)	224.0.0.6	Mensaje para todos los routers designados (DR)

En lugar de intercambiar sus tablas de encaminamiento, en los protocolos que siguen el algoritmo estado-enlace se intercambian mensajes de actualización de estado de los enlaces (LSU—Link State Updates) entre los routers con adyacencias, mediante un mecanismo conocido como LSA Flooding (inundación de anuncios de estado de enlaces).

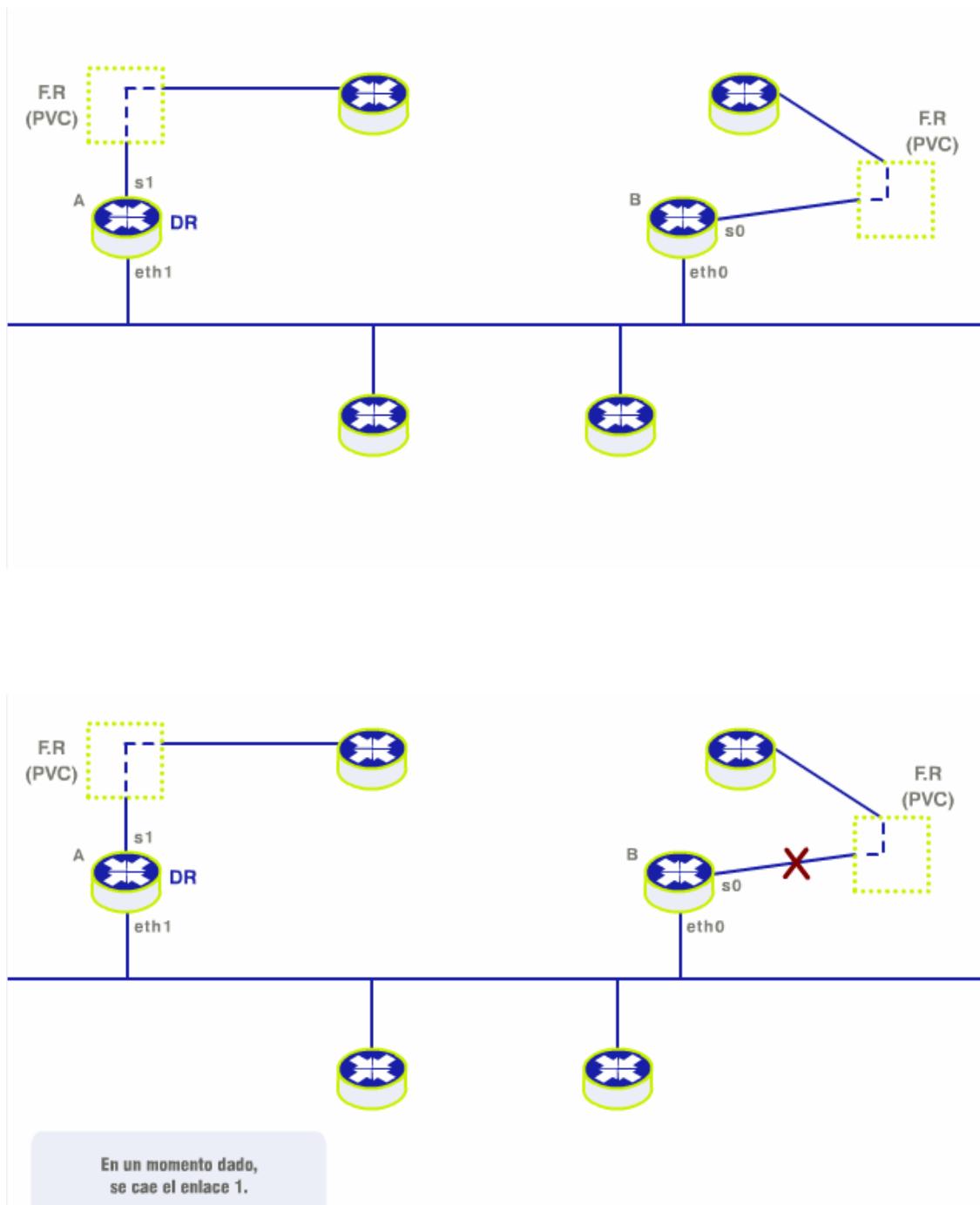
Estos mensajes, que se propagan por el área, permiten que todos los routers conozcan los enlaces que existen y el estado de los mismos, creando una base de datos topológica.

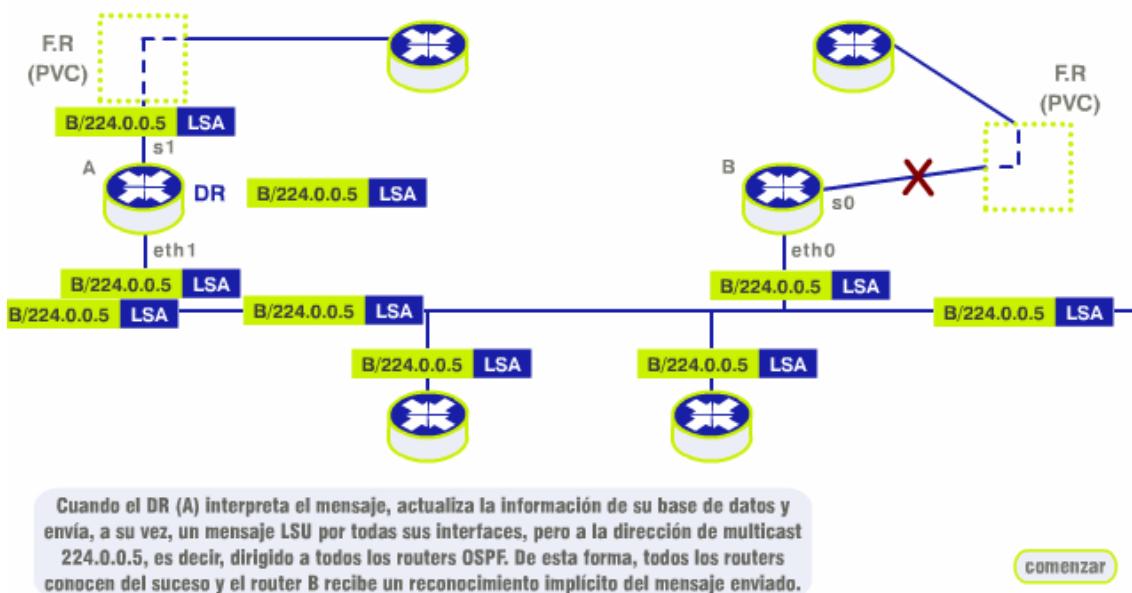
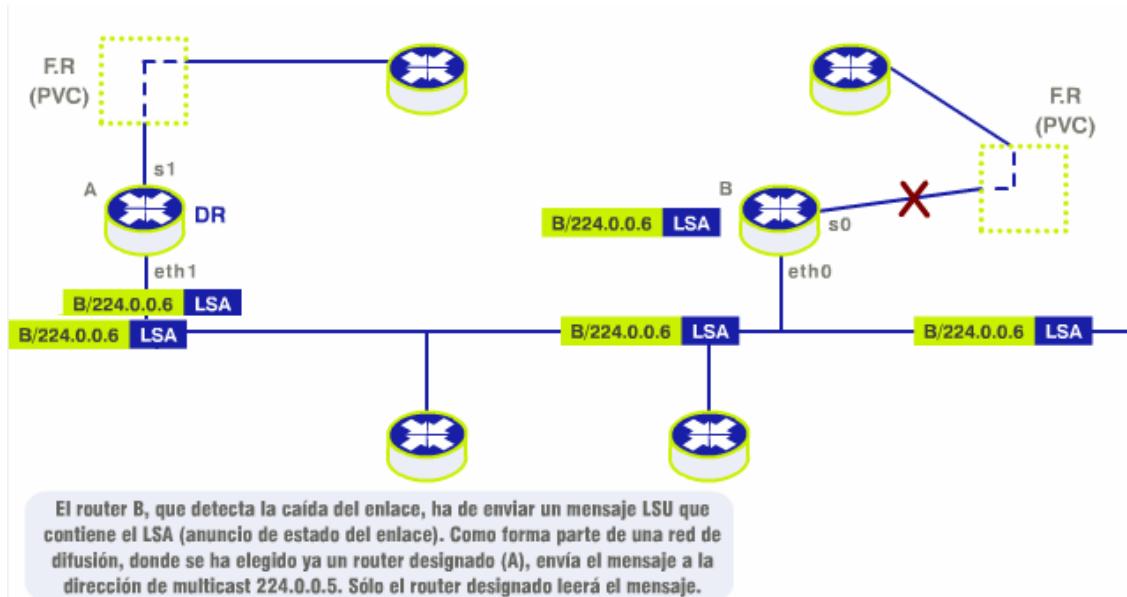
Para que el LSA flooding sea eficiente, se utiliza direccionamiento multicast, mediante direcciones reservadas para tal propósito, dependiendo del tipo de red que atraviese el mensaje, tal y como muestra la figura.

Propagación de LSAs (II)

\$Fichero: \$ B071_LANWAN/html/020526.htm

Para comprender mejor el mecanismo de anuncios LSU, veamos un ejemplo. En la red de la figura, supongamos que estamos en estado de convergencia.





Algoritmo SPF



Resumiendo, lo que hacen los routers, en el momento en el que se definen las adyacencias, es notificar del estado de sus enlaces mediante mensajes LSU multicast.

Éstos mensajes son retransmitidos por todos los routers de un área determinada, llegando un momento de convergencia en el que todos los routers conocen sobre todos los enlaces y el estado de los mismos, sincronizando las bases de datos topológicas.

Es aquí cuando tiene lugar el tercer paso del protocolo OSPF: cálculo del algoritmo SPF.

El algoritmo SPF se utiliza para crear la tabla de encaminamiento, basándose en el algoritmo de Dijkstra.

Para ello, es necesario asociar a cada enlace del router una métrica.

El coste de una ruta se calculará sumando las métricas correspondientes, y en la tabla se registrará la ruta con menor métrica.

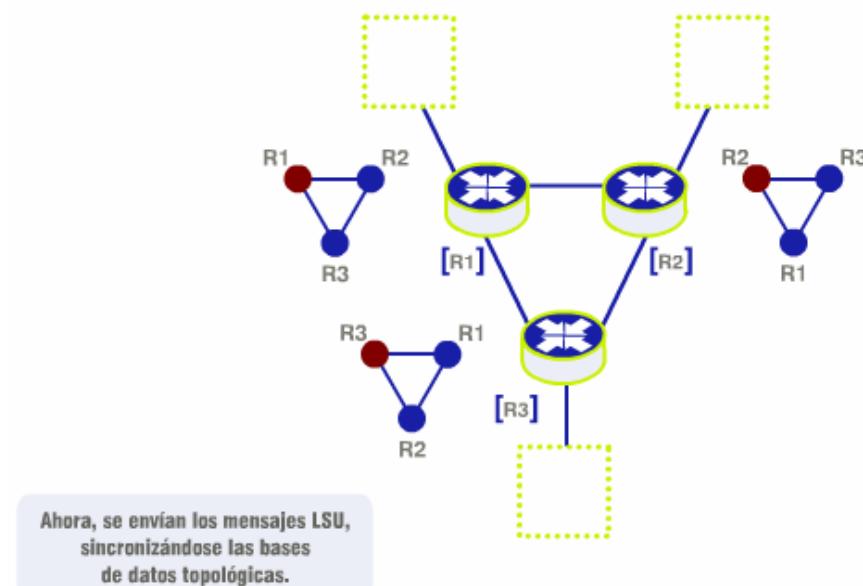
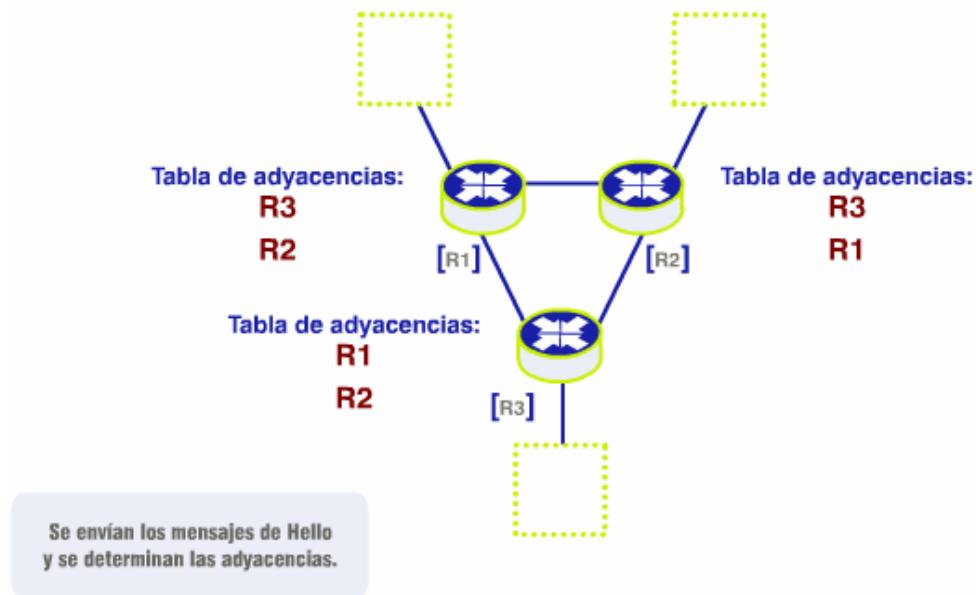
El valor de esa métrica (1 a 65535) se configura manualmente por el administrador, aunque los routers tienen valores definidos por defecto, por ejemplo, asociados al ancho de banda del enlace.

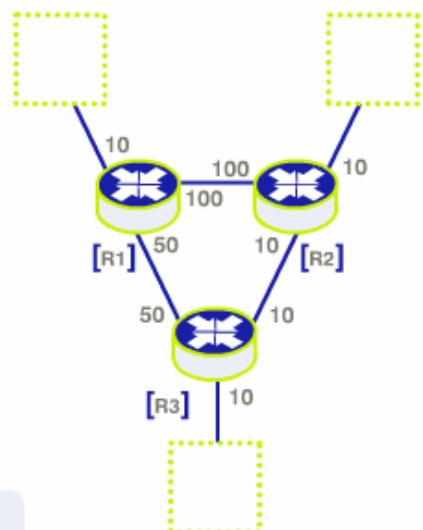
Algoritmo SPF (II)

\$Fichero: \$ B071_LANWAN/html/020529.htm

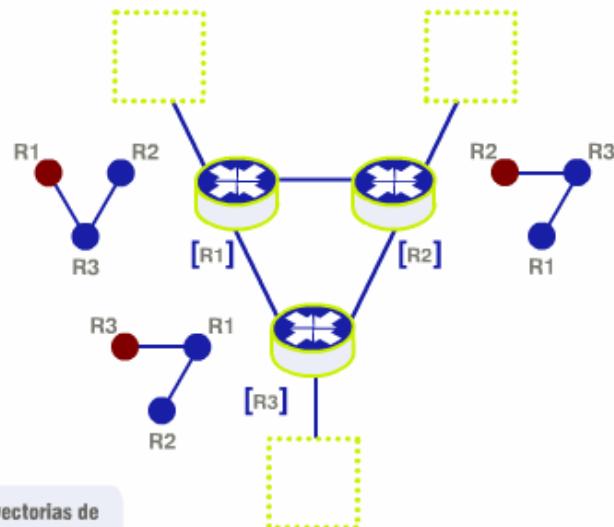
Veamos un ejemplo que ilustre la creación de las tablas de encaminamiento. Recuerda que ante cambios de topología, los anuncios permiten actualizar la base de datos topológica de cada router y recalcular la tabla con el algoritmo SPF.

[Algoritmo SPF (II)]





Utilizamos la métrica
indicada en las interfaces...



...y calculamos las trayectorias de
menor coste (métrica) para definir las
tablas de encaminamiento.

Conclusión



OSPF posee escalabilidad, es decir, es ideal para grandes redes con rápido crecimiento.

Otra de sus características es su compatibilidad con VLSM, rápida convergencia y diseño jerárquico.

El tipo de métrica que utiliza facilita controlar la distribución de tráfico y balanceo de carga. Permite conocer la totalidad de la red, es decir, su topología, y encaminar en función de variables como el campo TOS (type of service) de la cabecera IP.

RIP es sencillo, fácil de implementar, pero su uso ha de limitarse a redes medianas dado el límite de saltos que define (16). Con la versión 2 eliminamos la incompatibilidad con VLSM.

Estos dos protocolos ejemplarizan los dos algoritmos que hemos definido y son los más utilizados, dependiendo del tamaño de la red.

6 Arquitectura de encaminamiento

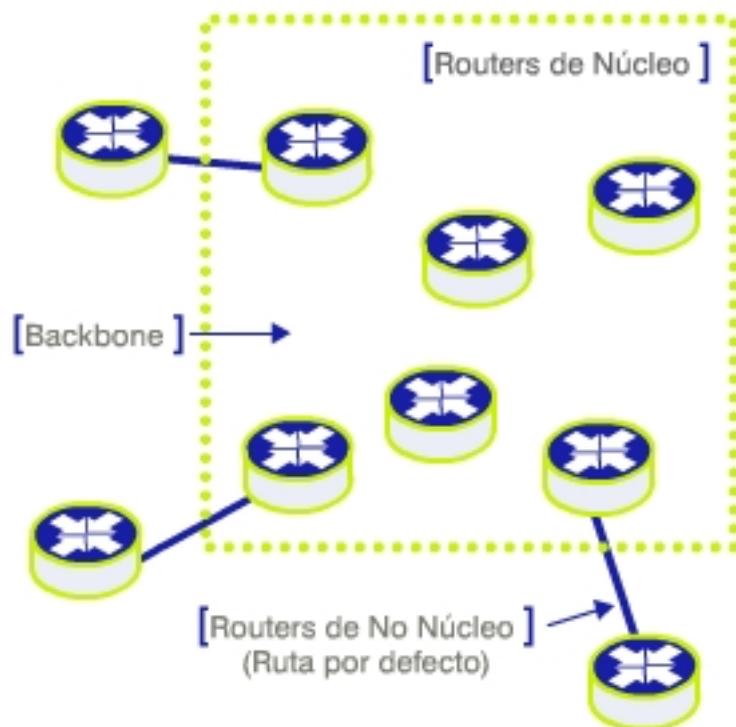
Introducción a la Sección 6

Vas a comenzar el apartado 6:

Arquitectura de encaminamiento

Finalmente, hemos llegado al punto culminante de este curso: el encaminamiento en Internet. Veremos cómo se estructura esa maraña de redes que existen en Internet y el “pegamento” que las mantiene unidas: el protocolo BGP4.

Arquitectura original de Internet



En términos generales, los primeros routers de Internet podían dividirse en dos grupos: los **routers de núcleo**, controlados por el InterNIC, y los **routers no núcleo**, controlados por grupos individuales.

Routers de núcleo

Contienen información completa sobre todas las redes y, en un principio, se configuraban sus tablas de encaminamiento de forma manual.

Routers no núcleo

Poseen rutas por defecto que apuntan a un router de núcleo. Sin embargo, la arquitectura de núcleo es ineficiente y no escalable.

Introducción a los sistemas autónomos

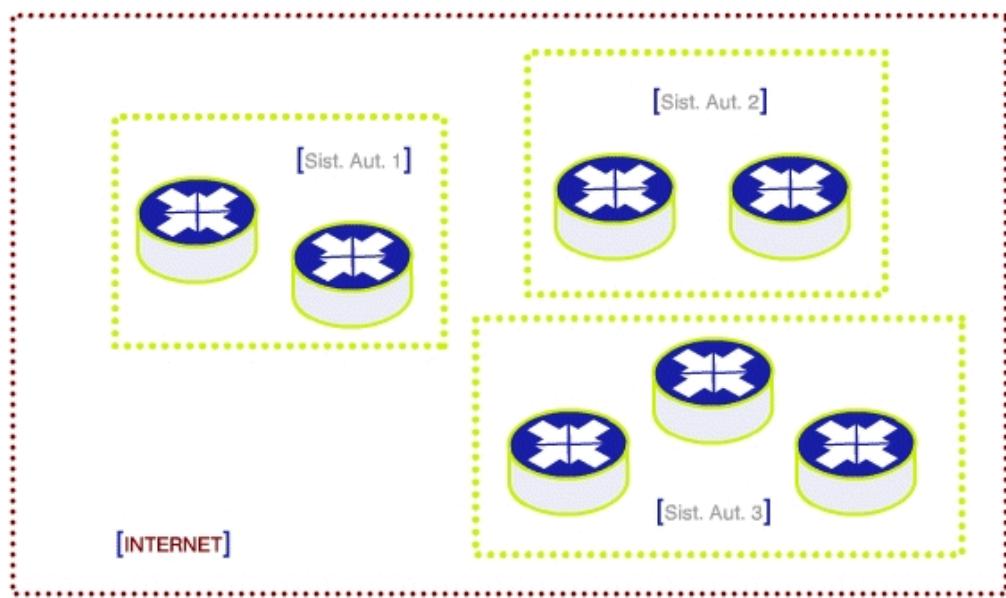


Es necesario implementar mecanismos que permitan a los routers no núcleo aprender rutas diferentes, y así poder seleccionar la más óptima.

Por otro lado, como las localidades individuales pueden tener una estructura de complejidad arbitraria, un sistema de núcleo no se conecta directamente a todas las redes, y es necesario un mecanismo que permita a los routers no núcleo informar al núcleo sobre las redes ocultas.

Es en este punto donde surge el concepto de sistemas autónomos, que vamos a ver a continuación.

Sistemas autónomos



En Internet, cada colección de redes y routers controlados por una autoridad administrativa (organización) se considera como un sistema autónomo. Dicha autoridad administrativa es responsable de que las rutas internas sean consistentes, y de seleccionar a un router como dispositivo de acceso a la red desde el mundo exterior.

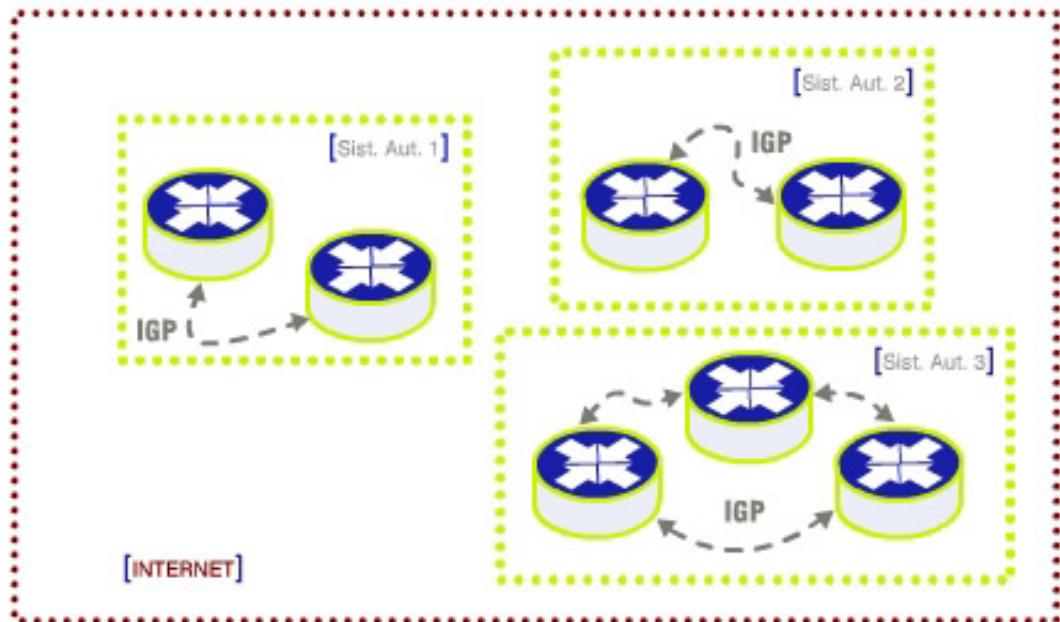
Cada sistema autónomo tiene libertad para seleccionar una arquitectura de encaminamiento interna, y es responsable de transferir información de accesibilidad hacia los routers de núcleo de Internet.

- Un sistema autónomo puede utilizar una arquitectura de encaminamiento propia, y posee información de todas sus redes.
- Designa uno o más routers para transferir la información a otros sistemas autónomos.
- Si existe conexión a Internet, deben transferir esa información a los routers núcleo de Internet.
- Dos routers que intercambian información y que pertenecen al mismo sistema autónomo son “vecinos interiores”. Si pertenecen a diferentes sistemas autónomos son “vecinos exteriores”.

IGP - Protocolo de Gateway Interior

Aunque la configuración manual de los routers se puede emplear en sistemas autónomos pequeños, no es adaptable a cambios o crecimiento rápido.

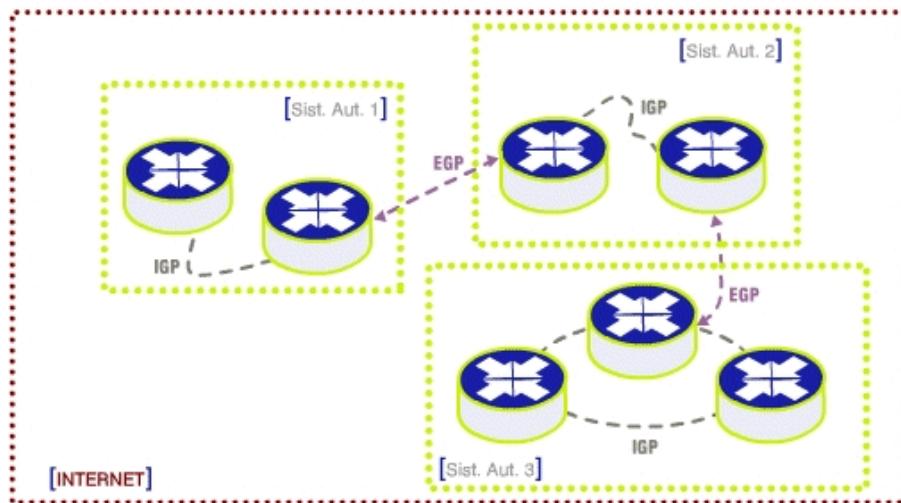
Normalmente, los routers interiores se comunican entre ellos intercambiando información, a partir de la cual construyen las tablas de encaminamiento del sistema autónomo al que pertenecen.



En general, no se ha desarrollado un único protocolo de encaminamiento a ser utilizado en los sistemas autónomos, por lo que se define genéricamente como IGP (Interior Gateway Protocol) a todo protocolo destinado al intercambio de información de encaminamiento entre routers pertenecientes a un sistema autónomo dado.

Los protocolos más utilizados como IGP son RIP y OSPF.

EGP - Protocolo de Gateway Exterior



[Resumiendo....](#)

La información obtenida dentro del sistema autónomo ha de ser compartida con otros sistemas autónomos. Para ello se designa uno o varios routers que actuarán como vecinos exteriores, es decir, intercambiarán información con routers exteriores de otro sistema autónomo (routers de borde o de frontera).

El conjunto de protocolos que se utilizan para este intercambio se conoce como EGP (Exterior Gateway Protocol). En la actualidad, el protocolo más difundido para el intercambio de información entre sistemas autónomos es BGP4 (Border Gateway Protocol Versión 4).

Resumiendo, Internet es un conjunto de Sistemas Autónomos o redes gestionadas por una organización que define sus propias políticas de encaminamiento.

Los routers del sistema autónomo crean sus tablas basadas en protocolos IGP (como RIP u OSPF) y, posteriormente, un router designado como de frontera o de borde, se encarga de comunicar esa información a su contraparte en otros sistemas autónomos, mediante el protocolo BGP4. Así, el encaminamiento en Internet está estructurado jerárquicamente.

Protocolo BGP4



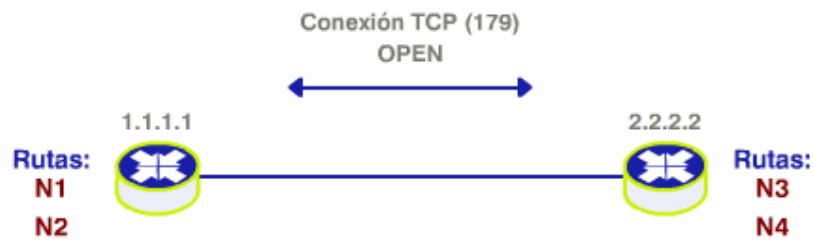
Vamos a ver el funcionamiento de ese “pegamento de Internet” en el que se convierte el protocolo BGP4.

BGP4 es uno de los protocolos de encaminamiento más complejos, dada la cantidad de información que transportan sus mensajes, destinado fundamentalmente para el intercambio de información entre routers de frontera de sistemas autónomos, aunque puede ser utilizado como protocolo IGP.

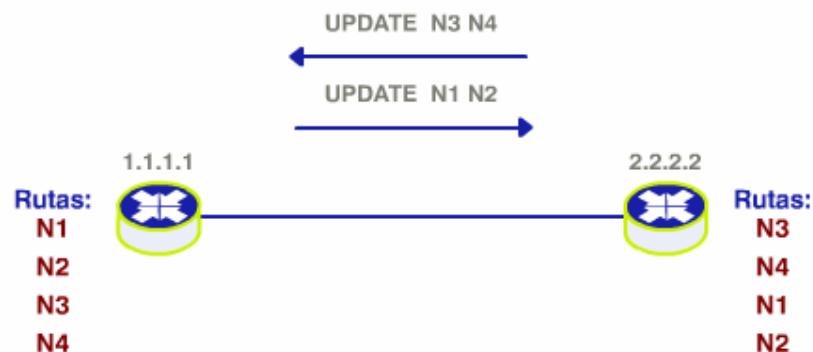
Se transporta mediante sesiones TCP al puerto 179, proveyendo fiabilidad al proceso de comunicación entre routers.

Funcionamiento de BGP4

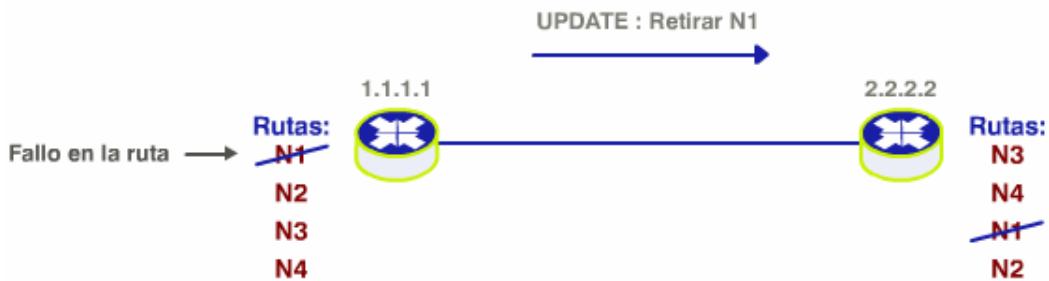
Fundamentalmente se basa en el establecimiento de “iguales” (peers) BGP que se hacen vecinos. Una vez establecida la relación, se intercambian la información de rutas hacia diversos sistemas autónomos y, ante cambios de configuración, se envían mensajes de actualización.



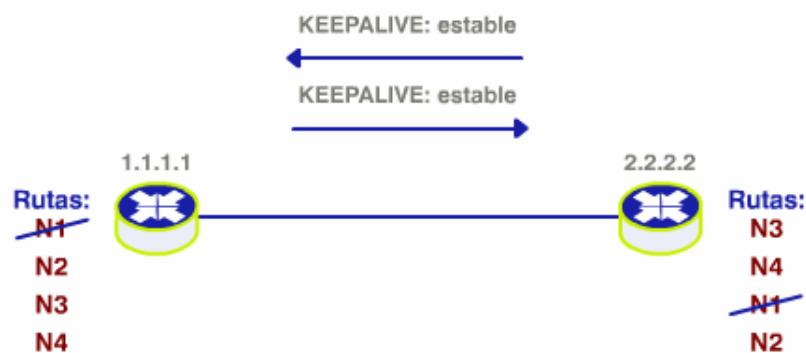
En primer lugar, dos routers BGP establecen una conexión TCP e intercambian mensajes de OPEN para hacerse vecinos.



Una vez constituidos como vecinos, intercambian la información de encaminamiento utilizando mensajes de UPDATE.

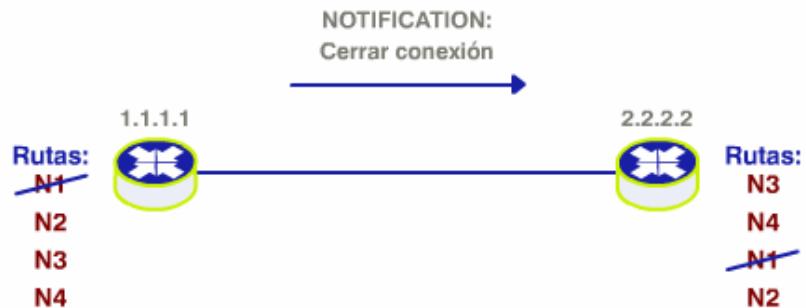


Si se presenta un cambio, por ejemplo una ruta no accesible, se notifica mediante mensajes de UPDATE.



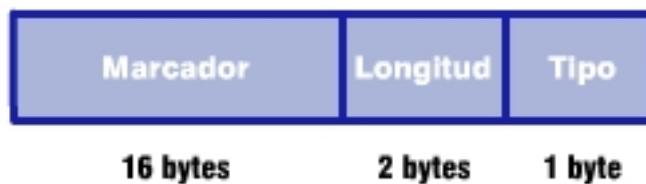
De no haber cambios, únicamente se intercambian mensajes del tipo KEEPALIVE para asegurar que la conexión se mantiene activa y que no hay cambios en el enrutamiento.

Error!!!



Un mensaje de NOTIFICATION se envía siempre que se encuentre una condición de error, siendo seguido por el cierre de conexión con el igual.

Formato de Mensajes BGP



Como hemos visto, el funcionamiento del BGP se basa en 4 mensajes: OPEN, KEEPALIVE, NOTIFICATION Y UPDATE.

Vamos a detenernos en cada uno de ellos.

Todos los mensajes BGP llevan una cabecera común, que se muestra en la figura. Recuerda que todos los mensajes se transportan en TCP (e IP, subsecuentemente).

Marcador (16 bytes)

Se utiliza para autenticación que puede predecir el receptor del mensaje, o para detectar pérdidas de sincronización entre iguales BGP.

Longitud (2 bytes)

Longitud total en bytes, incluyendo cabecera.

El tamaño del paquete BGP no puede ser menor de 19, ni mayor de 4096 bytes.

Tipo (1 byte)

Especifica el tipo de mensaje (OPEN, UPDATE, NOTIFICATION, KEEPALIVE).

Mensaje OPEN



Versión (1 byte)

Indica la versión BGP utilizada. Durante la negociación inicial, los iguales BGP se ponen de acuerdo sobre la versión a utilizar. Actualmente, la 4.

Sistema Autónomo (2 bytes)

Número de SA del portavoz BGP.

Temporizador de espera (2 bytes)

Máximo intervalo de tiempo, en segundos, que puede transcurrir entre la recepción de mensajes keepalive o update sucesivos. El contador de tiempo de espera se incrementa de cero hasta el valor establecido y se reinicia ante la recepción de un mensaje. Si se excede el tiempo, el vecino se considera "extinto". Si el contador de espera se establece en cero, se mantiene permanentemente la conexión TCP. Por defecto son 3 segundos.

Identificador (4 bytes)

Indica el ID del router BGP emisor. En algunos casos es la dirección IP más alta del router.

Longitud de opciones (2 bytes)

Indica la longitud total del campo de parámetros opcionales.

Parámetros opcionales (variable)

Campo constituido por tripletas tipo de parámetro (1 byte), longitud de parámetro (1 byte) y valor.

Mensaje NOTIFICATION

Un mensaje de NOTIFICATION se envía siempre que se encuentre una condición de error, siendo seguido por el cierre de conexión con el igual.

Error	Subtipo	Datos
1 byte	1 bytes	variable
Código de error		Subtipo
Error en la cabecera	1	Conexión no sincronizada
		Longitud mensaje incorrecta
		Tipo de mensaje incorrecto
Error mensaje OPEN	2	Número de versión no soportado
		AS de vecino erróneo
		Identificador BGP incorrecto
		Parámetro opcional no soportado
		Fallo de autenticación
		Temporizador de espera no aceptable
Error mensaje UPDATE	3	Lista de atributos mal formada
		Bucle de enrutamiento en el SA
		Campo de red erróneo
Temporizador espera agotado	4	
Cesar (errores fatales)	6	

El mensaje de notificación está compuesto por un campo de código de error (1 byte), el subtipo de error (1 byte) y un campo de datos (variable).

El código de error indica el tipo de la notificación y el de subcódigo aporta información más específica sobre la naturaleza del error.

El campo de datos contiene información relativa al error (como el número de sistema autónomo erróneo, etc.)

Mensaje KEEPALIVE

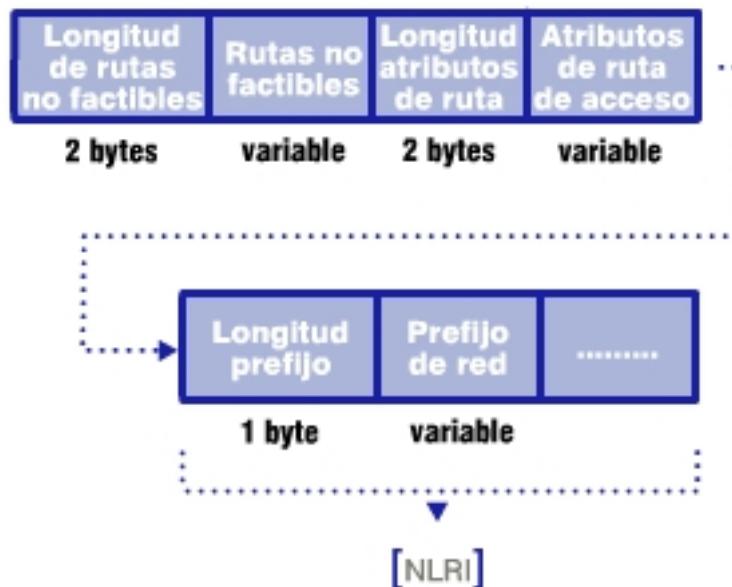
Marcador	Longitud (19)	Tipo (KEEP ALIVE)
16 bytes	2 bytes	1 byte

Los mensajes KEEPALIVE son mensajes periódicos que determinan si los vecinos son o no accesibles.

El tiempo de espera definido en el mensaje de OPEN es el intervalo máximo de tiempo que puede transcurrir en la recepción de dos mensajes KEEPALIVE consecutivos, aunque dicho mensaje no se envía en ese intervalo de tiempo si un UPDATE es enviado primero.

El mensaje está formado por los 19 bytes de cabecera BGP sin datos.

Mensaje UPDATE



El corazón de BGP es el concepto de actualización de encaminamiento, que proporciona toda la información necesaria para construir una imagen de a red, libre de bucles.

Los bloques del mensaje UPDATE son:

- Información de accesibilidad de la capa de Red (NLRI).
- Atributos de ruta de acceso.
- Rutas no factibles.

NLRI

Indica las redes que son publicadas (en formato CIDR, longitud y prefijo de red). Los atributos de acceso permiten detectar bucles.

Por ejemplo, el atributo AS-PATH, proporciona una lista de números de sistema autónomo que una ruta atraviesa antes de alcanzar el router BGP.

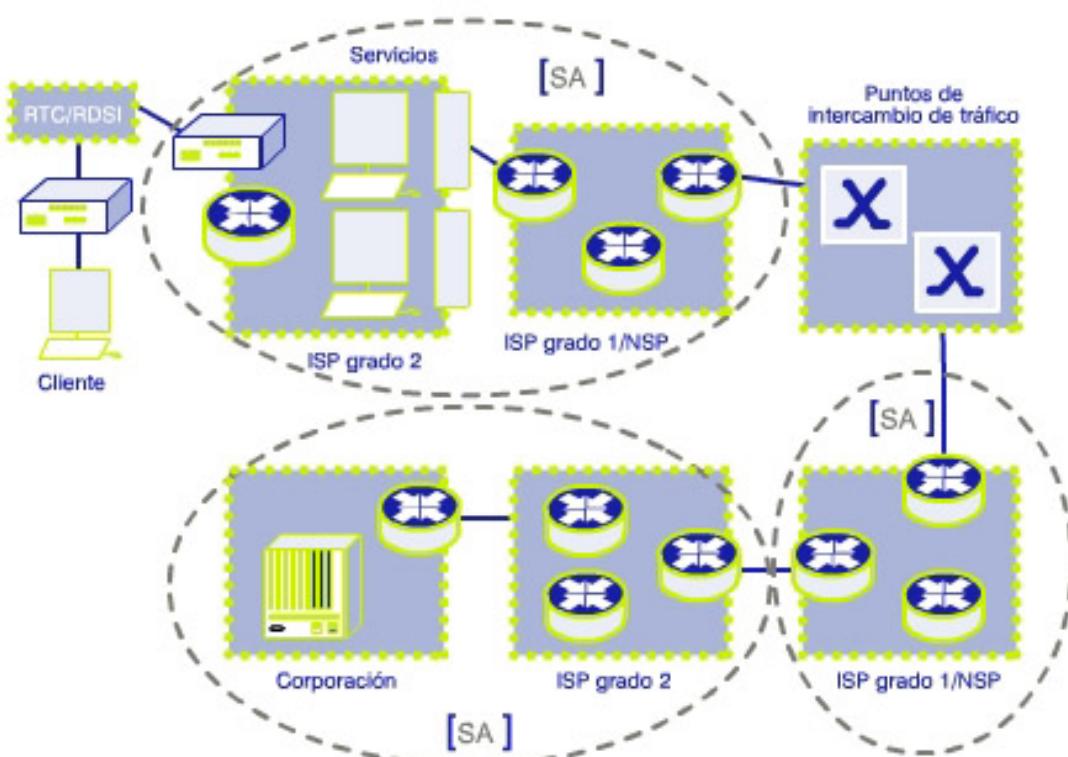
Rutas no factibles

La lista de rutas que se han vuelto inalcanzables (retiradas) se pueden notificar mediante el mensaje UPDATE, con el mismo formato de NLRI.

Estructura actual de Internet

Durante todo este curso hemos analizado el encaminamiento y los protocolos que se utilizan, así como el esquema de direccionamiento utilizado hoy por hoy.

Veamos todo esto aplicado a Internet.



Internet está constituida por una serie de redes comerciales, incluyendo los ISPs convencionales (nivel 2), conectadas unas a otras a través de ISPs nivel 1 (proveedores de transporte IP), como Sprint, UUNet, Qwest, etc.

Estos constituyen los sistemas autónomos definidos mediante un número asignado por la ICANN.

También pueden crearse sistemas autónomos a partir de redes de organizaciones o ISPs nivel 2.

Los ISP nivel 1 intercambian tráfico a través de los NAP (Network Access Points), que son redes de conmutación de alta velocidad donde se realiza el encaminamiento entre pares de routers de frontera o BGP.

El direccionamiento IP es también controlado por la ICANN, como vimos anteriormente, y se utiliza la asignación de agregados a los grandes ISPs que, a su vez, delegan espacios de direcciones mediante VLSM a los ISPs nivel 2 y redes de organizaciones.

Por tanto, los anuncios de rutas se basarán, fundamentalmente en agregados, disminuyendo la cantidad de rutas anunciadas entre sistemas autónomos.

Conclusión



Los conceptos de encaminamiento, protocolos (IGP y EGP), sistemas autónomos, direccionamiento, VLSM, CIDR, agregación, etc., son, hoy por hoy, el fundamento de Internet y, en general, de cualquier red IP (pública o privada).

Conociendo todo esto se puede dimensionar e implementar apropiadamente la política de direccionamiento y encaminamiento de la red IP de una organización o empresa de forma óptima y acertada, en relación a las recomendaciones de la comunidad Internet.