La capa de red

Formato de paquete IPv4

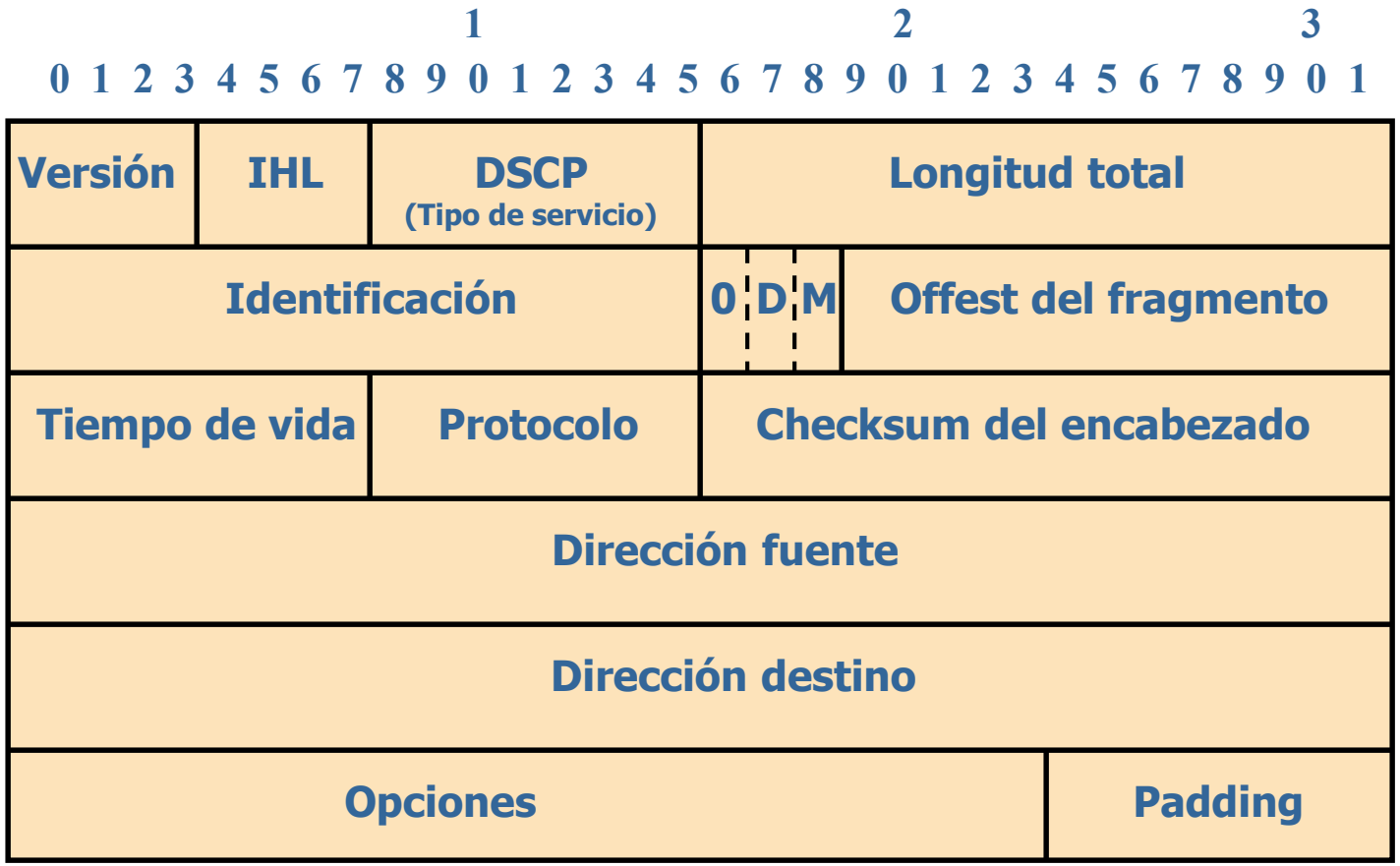
Protocolos auxiliares

Protocolos de enrutamiento

Esquema de direccionamiento

- Asignación de direcciones de red a cada componente para que pueda comunicarse con otros dispositivos internos y externos
- Una asignación no estructurada puede comprometer los requerimientos de escalabilidad y desempeño y complicar la administración de la red
- La asignación de nombres y direcciones se simplifica con una topología jerárquica e identificando la estructura organizacional de la empresa

Formato de paquete (IPv4)



- 0 =1
- 1=2
- 2=4
- 3=8
- 4=16
- 5=32
- 6=64
- 7=128
- 8=256
- 9=512

- 10= 1k
- 20=1M
- 30=1G
- 40=1T
- 50=1P
- 60=1E

57=128P

16=64K

33=8G

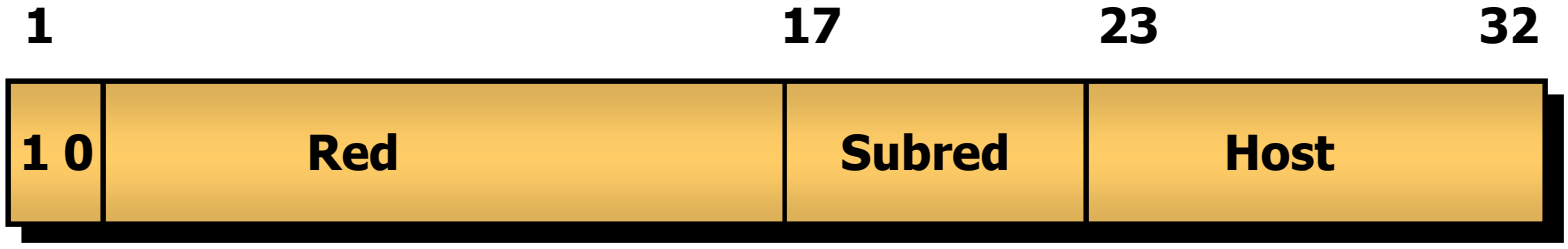
Clases de direcciones IP

Clase	Formato	Uso	MSB	Rango	# Host
A	R.H.H.H	Pocas redes de gran tamaño	0	1.0.0.0 126.0.0.0	16,777,214 (2^{24}-2)
B	R.R.H.H	Organizaciones de tamaño mediano	10	128.1.0.0 191.254.0.0	65,534 (2^{16}-2)
C	R.R.R.H	Organizaciones de tamaño pequeño	110	192.0.1.0 223.255.254.0	254 (2^{8}-2)
D	N/A	Grupos Multicast	1110	224.0.0.0 239.255.255.255	N/A
E	N/A	Experimental	1111	240.0.0.0 254.255.255.255	N/A

R = Red
H = Host

Subredes IP y máscara

Clase B



1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0

Máscara **255** **255** **252** **0**

- 6 bits para subred y 10 bits para host.
- 62 subredes **(2^6-2).**
- 1022 nodos para cada subred **(2^{10}-2)**.
- Las redes y nodos todos 1´s y todos 0´s están reservados.

Enrutamiento jerárquico

- Ningún enrutador necesita conocer la topología completa de la red para enviar un datagrama.
- A mediados de los 90s, Classless InterDomain Routing obvió la asignación jerárquica de direcciones en Internet: las direcciones se asignan en bloques, los enrutadores agrupan direcciones en una sola ruta y existen grandes bloques por zonas geográficas.

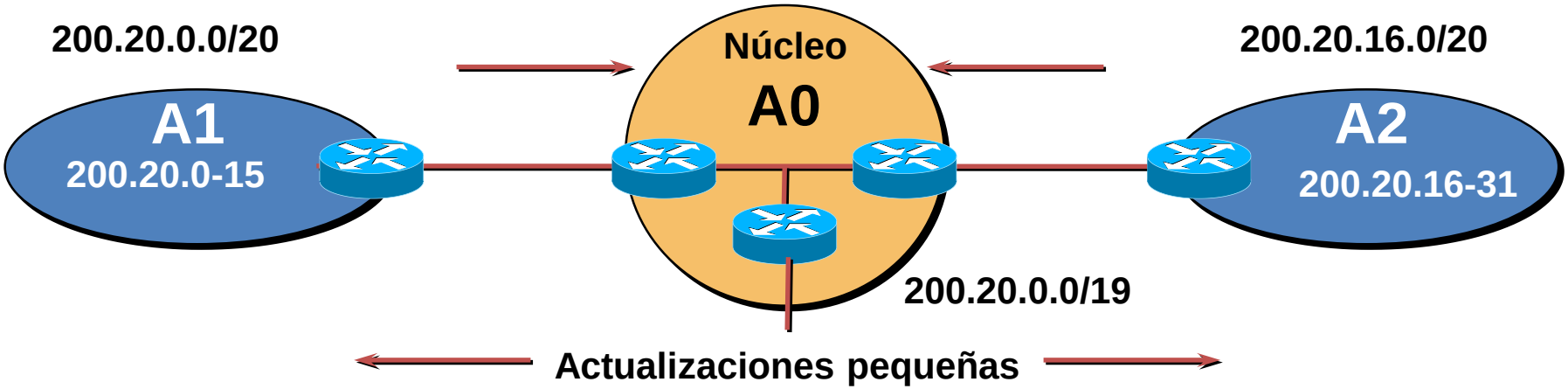
CIDR

- La longitud de la dirección de red (y subred) se indica por un prefijo
- Se pueden asignar rangos de direcciones con mayor flexibilidad
- Las tablas de ruteo son menores y se actualizan con menor frecuencia
- Soportado por la mayoría de protocolos actuales: RIP-2, EIGRP, OSPF-2, BG-4, IS-IS

Sumarización de rutas

- La sumarización permite a un enrutador agrupar muchos números de red en una sola entrada de su tabla de enrutamiento.
- Para poder realizar la agregación es necesario que el número de redes sea una potencia de 2 y que todas ellas compartan los bits que se encuentran más a la izquierda.
- Por ejemplo, las 8 redes clase C 192.108.168.0 a 192.108.175.0 pueden agregarse en 192.108.168.0/21

Sumarización

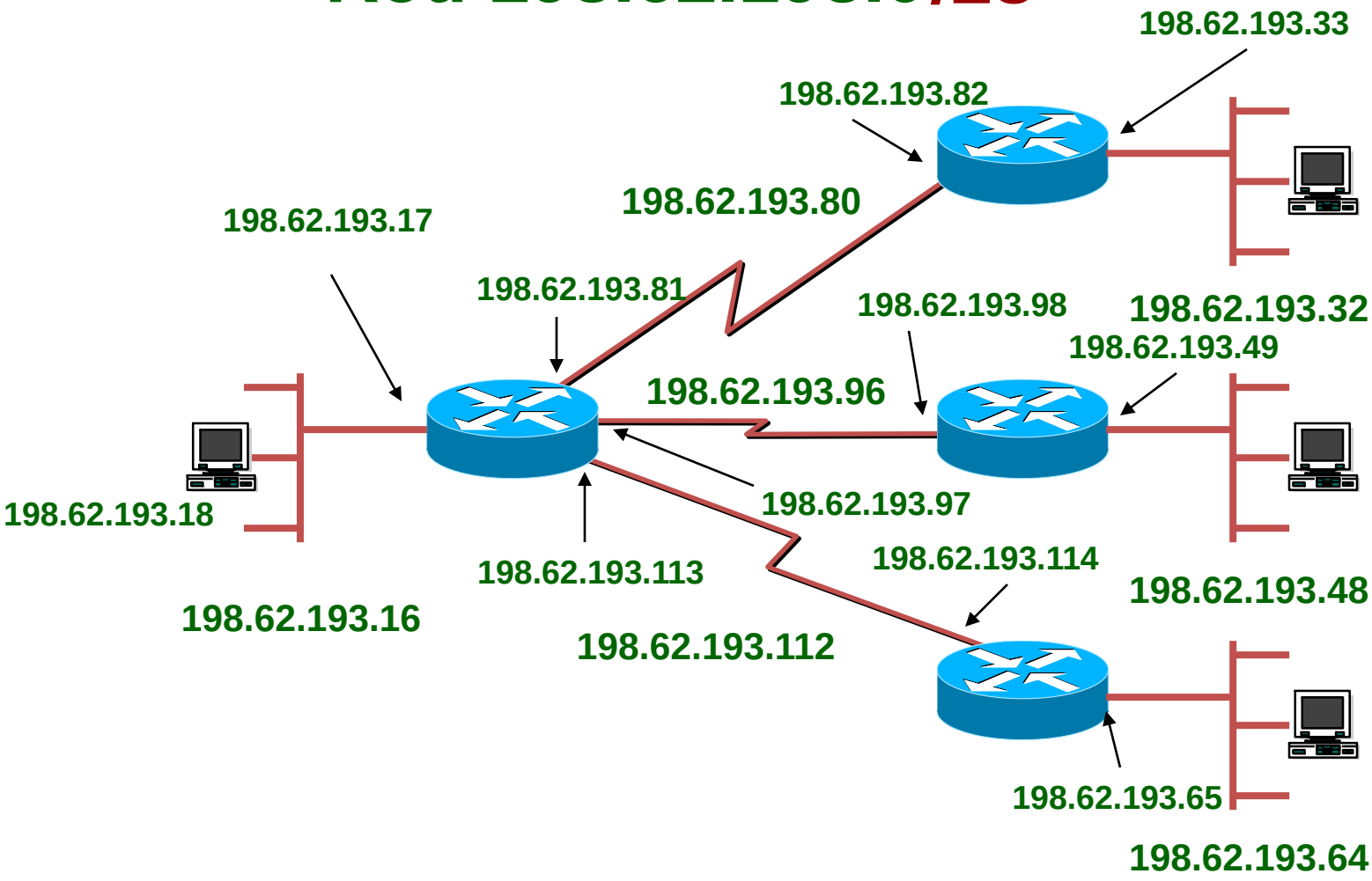


El núcleo inyecta sólo rutas agregadas en otras áreas

- Un grupo de bits identifica a un conjunto de redes.
- Se reduce el consumo de memoria y de procesador.
- Se agrega en el sentido del núcleo.

Máscaras de Longitud Variable

Red 198.62.193.0/28



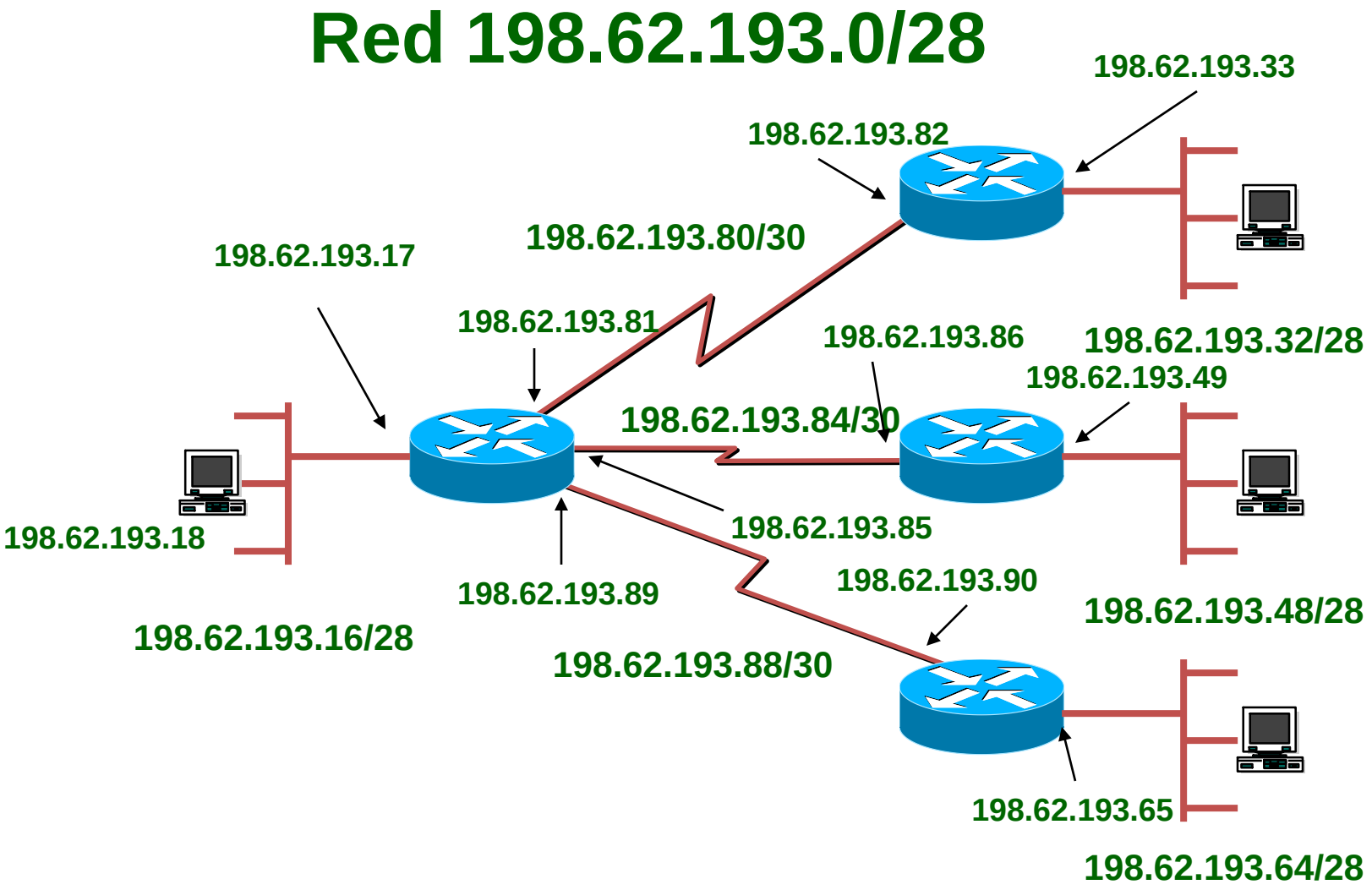
Máscaras de Longitud Variable

- El uso de máscaras de subred de longitud variable (VLSM) permite optimizar el espacio de direcciones disponible mediante la división de una (sub)red en subredes de diferente tamaño
- En el ejemplo anterior, la subred 198.62.193.80 puede tener una máscara de 30 bits, pudiendo crear 4 sub-subredes (*stubnets*):

  198.62.193.80, 198.62.193.84

  198.62.193.88, 198.62.193.92

Máscaras de Longitud Variable



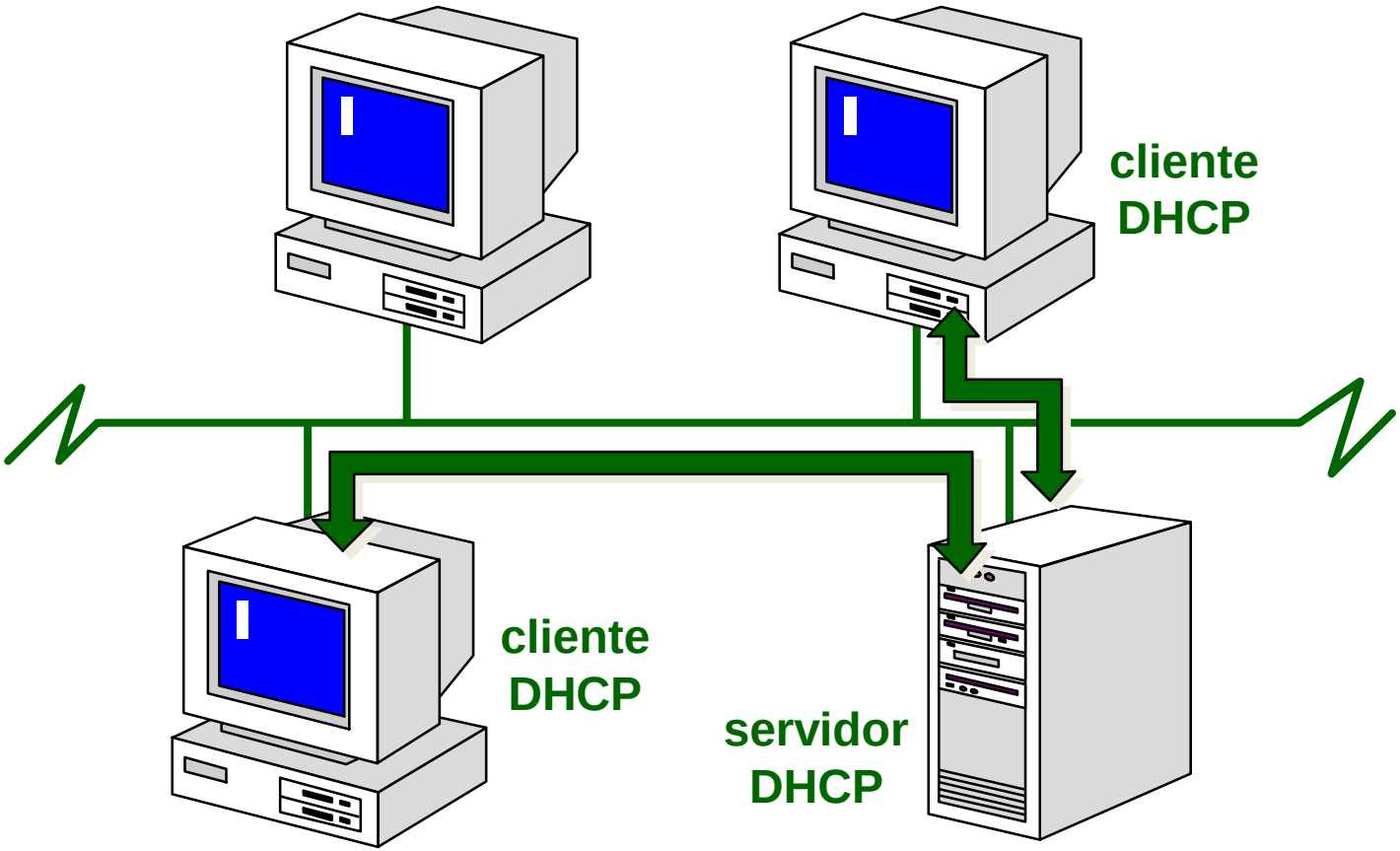
Asignación de direcciones a dispositivos

- Configuración manual
  - Trabajo administrativo, rutinario y propenso a errores
  - Muy complejo en redes grandes; dificultad para localizar la fuente de un problema
- Configuración dinámica: RARP, BOOTP, DHCP
  - Los clientes obtienen su dirección IP de manera automática de un servidor
  - Se minimizan los problemas de configuración
  - Soporte a usuarios “nómadas”

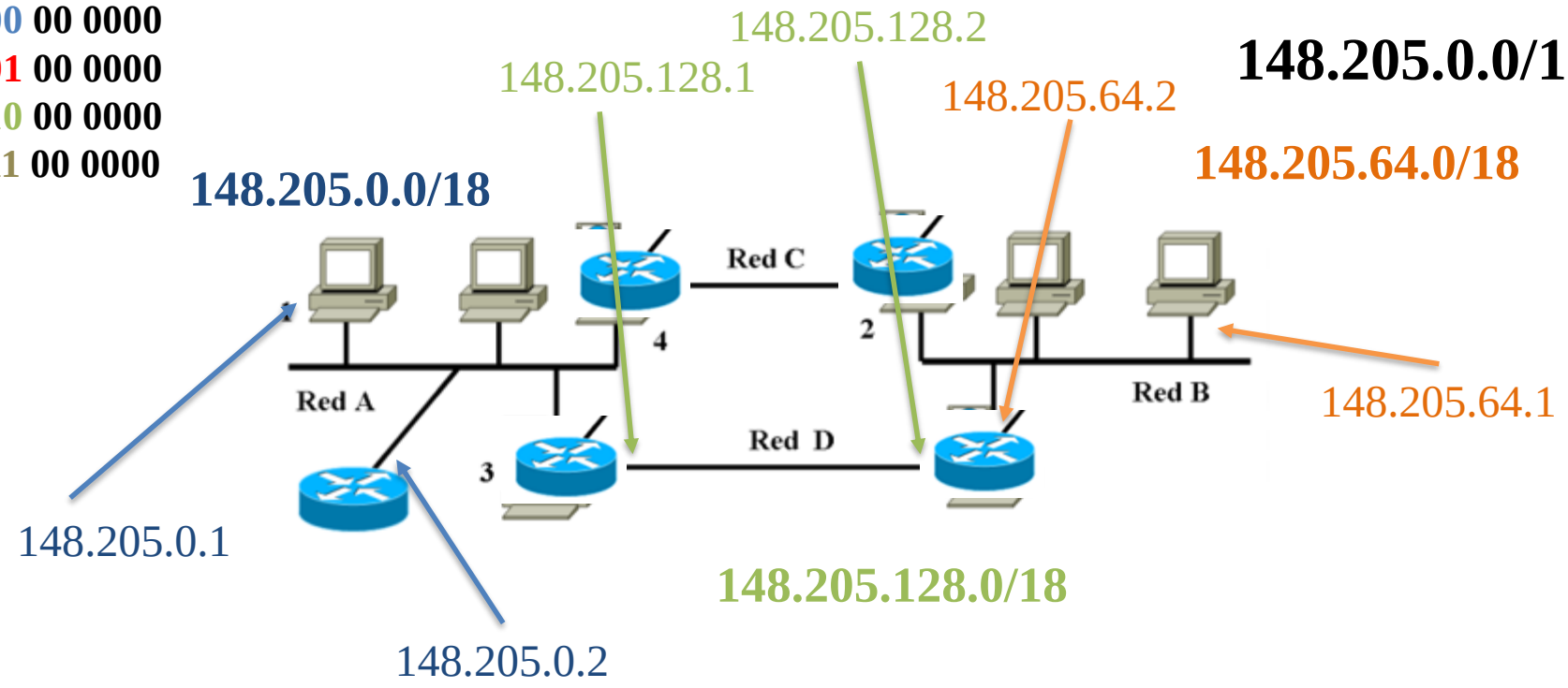
Dynamic Host Configuration Protocol

1. El cliente difunde un mensaje *discover* sobre su red local
2. Todos los servidores DHCP contestan con un mensaje *offer* proponiendo parámetros de configuración
3. El cliente selecciona una oferta y difunde un mensaje *request* que incluye la dirección del servidor seleccionado.
4. El servidor seleccionado responde con un mensaje *ACK.*
5. El cliente completa la asociación

DHCP



00 00 0000
01 00 0000
10 00 0000
11 00 0000



Direcciones privadas

- RFC 1918 asigna las siguientes direcciones para uso privado (*i.e.* no pueden ser anunciadas)
  - 10.0.0.0 a 10.255.255.255 (10/8)
  - 172.16.0.0 a 172.31.255.255 (172.16/12)
  - 192.168.0.0 a 192.168.255.255 (192.168/16)
- Traducir las direcciones internas en direcciones válidas vía proxies o Network Address Translation (NAT)
- El bloque 169.254.0.0/16 también ha sido reservado para hacer autoconfiguración DHCP

Network Address Translation

Pool de direcciones Internet : 200.1.1.1 a 200.1.1.5

Datagrama Intranet		Datagrama Internet
IP fuente: 10.1.2.3 IP dest. 198.9.8.7	→ NAT	IP fuente: 200.1.1.3 IP dest: 198.9.8.7
IP fuente: 198.9.8.7 IP dest: 10.1.2.3	← NAT	IP fuente: 198.9.8.7 IP dest: 200.1.1.3
IP fuente: 10.1.2.5 IP dest: 15.66.12.1	→ NAT	IP fuente: 200.1.1.1 IP dest: 15.66.12.1

Network Address Port Translation

Pool de direcciones Internet : 200.1.1.1 (solamente 1)

Datagrama Intranet		Datagrama Internet
IP/TCP fuente: 10.1.2.3/2345	→	IP /TCP fuente: 200.1.1.1/1024
IP /TCP dest: 198.9.8.7/80	PAT	IP /TCP dest: 198.9.8.7/80
IP /TCP fuente: 198.9.8.7/80	←	IP /TCP fuente: 198.9.8.7/80
IP /TCP dest: 10.1.2.3/2345	PAT	IP /TCP dest: 200.1.1.1/1024
IP /TCP fuente: 10.1.2.5/1234	→	IP /TCP fuente: 200.1.1.1/1025
IP /TCP dest: 15.66.12.1/80	PAT	IP /TCP dest: 15.66.12.1/80

Direcciones privadas

- Ventajas:
  - Seguridad
  - Flexibilidad para cambiar de ISP
  - Disminución de tablas de enrutamiento
- Desventajas:
  - Administración tercerizada no tiene acceso directo
  - Complejidad adicional ante fusiones, acceso a otras redes privadas, etc.
  - ¡Puede no funcionar!
  - Supone un modelo cliente/servidor. Complicaciones para aplicaciones entre pares
  - Modifica el principio de diseño E2E. Inhibe la creación de nuevas aplicaciones
  - Afecta el desempeño y la solidez de la red

Mecanismos para atravesar NATs

- Universal Plug and Play (UPnP)
  - Protocolo para que NAT notifique a las aplicaciones cliente la dirección y puerto que se estará utilizando
  - Requiere NATs y clientes compatibles (pocos en la actualidad)
  - Apoyado por Microsoft
  - Conveniente para uso residencial. En corporativos grandes se tienen dudas sobre la seguridad
- Configuración manual
  - Tanto en cliente como en NAT, mapeo estático de direcciones configuradas manualmente
  - Únicamente para redes muy pequeñas, hasta que UPnP se difunda más
- Simple Traversal of UDP over NATs (STUN)
  - Cliente envía solicitud a un STUN server quien le responde con la dirección IP pública del NAT y el número de puerto que se está utilizando.
  - Google Talk hace uso extensivo de STUN
  - Clientes también deben ser modificados (hay pocos)
  - No sirve para NATs simétricos, es decir, los que mapean direcciones y puertos tanto fuente como destino
- Traversal Using Relay NAT (TURN)
  - Muy similar a STUN pero ahora el servidor se inserta en la trayectoria de los flujos: en la DMZ del cliente o en la red de acceso del ISP.

Mecanismos para atravesar NATs

- Pasarela a nivel aplicación (ALG)
  - NAT o firewall que entiende la semántica a nivel aplicación y realiza las transformaciones correspondientes
  - Configuración compleja y soluciones costosas, limitan su uso a grandes organizaciones
- Túnel
  - Se crea un túnel entre la red privada y la red pública para atravesar el NAT. El servidor en la red pública actúa como pasarela mapeando direcciones privadas y puertos con su dirección pública
  - El servidor en la red pública puede representar una vulnerabilidad en la estrategia de seguridad
- UDP hole punching
  - A y B se comunican con un servidor en la internet pública. El servidor responde con las direcciones y puertos usados por A y B. Ahora éstos se comunican directamente con la esperanza de que el NAT conserve esos estados.
  - Una de las técnicas usadas por Skype

Protocolos auxiliares

Internet Control Message Protocol

- ICMP está definido en el RFC 792 y es utilizado por los enrutadores y nodos destino para informar al nodo emisor acerca de algunos errores durante el procesamiento del datagrama.

- ICMP reporta errores, mas no hace confiable a IP. La confiabilidad debe ser implementada por protocolos de alto nivel.

Principales mensajes ICMP

Tipos de mensajes	ICMP type	Descripción
- Destino no alcanzable	3	- Paquete no se entregó
-Tiempo excedido	11	-TTL = 0
-Problemas de parámetros	12	-Campo inválido en el encabezado
-Anuncio y solicitud de enrutador	9,10	-Detección del enrutador por omisión
-Redirección	5	-Aprendizaje de rutas
-Petición de eco	8	-Preguntar si una máquina está viva
-Respuesta eco	0	-Respuesta afirmativa de eco

Aplicaciones ICMP

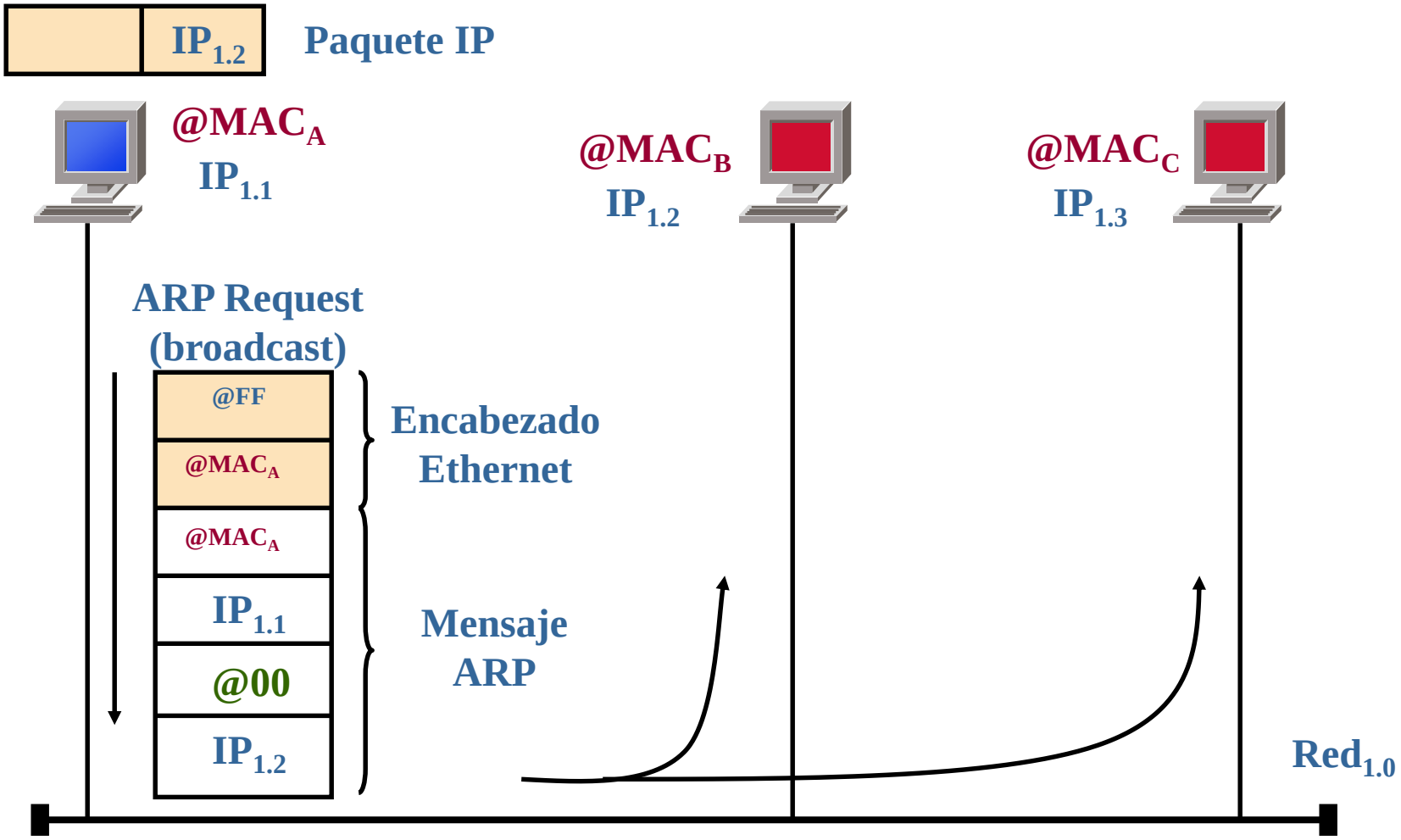
- Las dos aplicaciones más ampliamente usadas que se basan en mensajes ICMP son:
  - Ping.- Envía uno o más paquetes IP a un destino específico solicitando respuesta y midiendo el tiempo de viaje redondo.
  - Traceroute.- Determina la ruta completa que un datagrama IP sigue desde el nodo emisor hasta el receptor.

Address Resolution Protocol

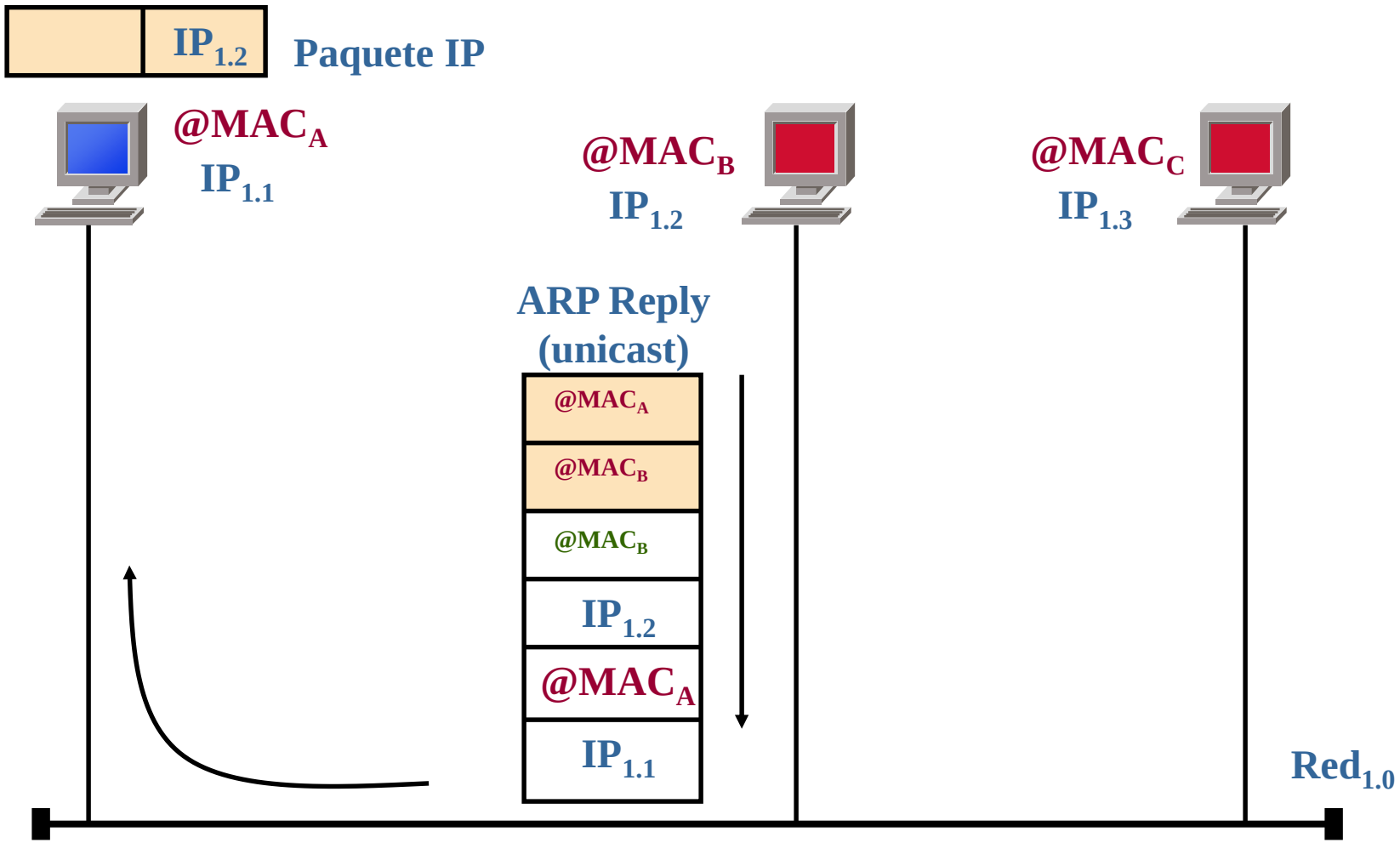
- La comunicación entre nodos dentro de una subred (o dominio de difusión) se realiza con base en las direcciones físicas o MAC.

- ARP, definido en el RFC 826, sirve para realizar el mapeo de direcciones IP a direcciones MAC dentro de una misma subred.

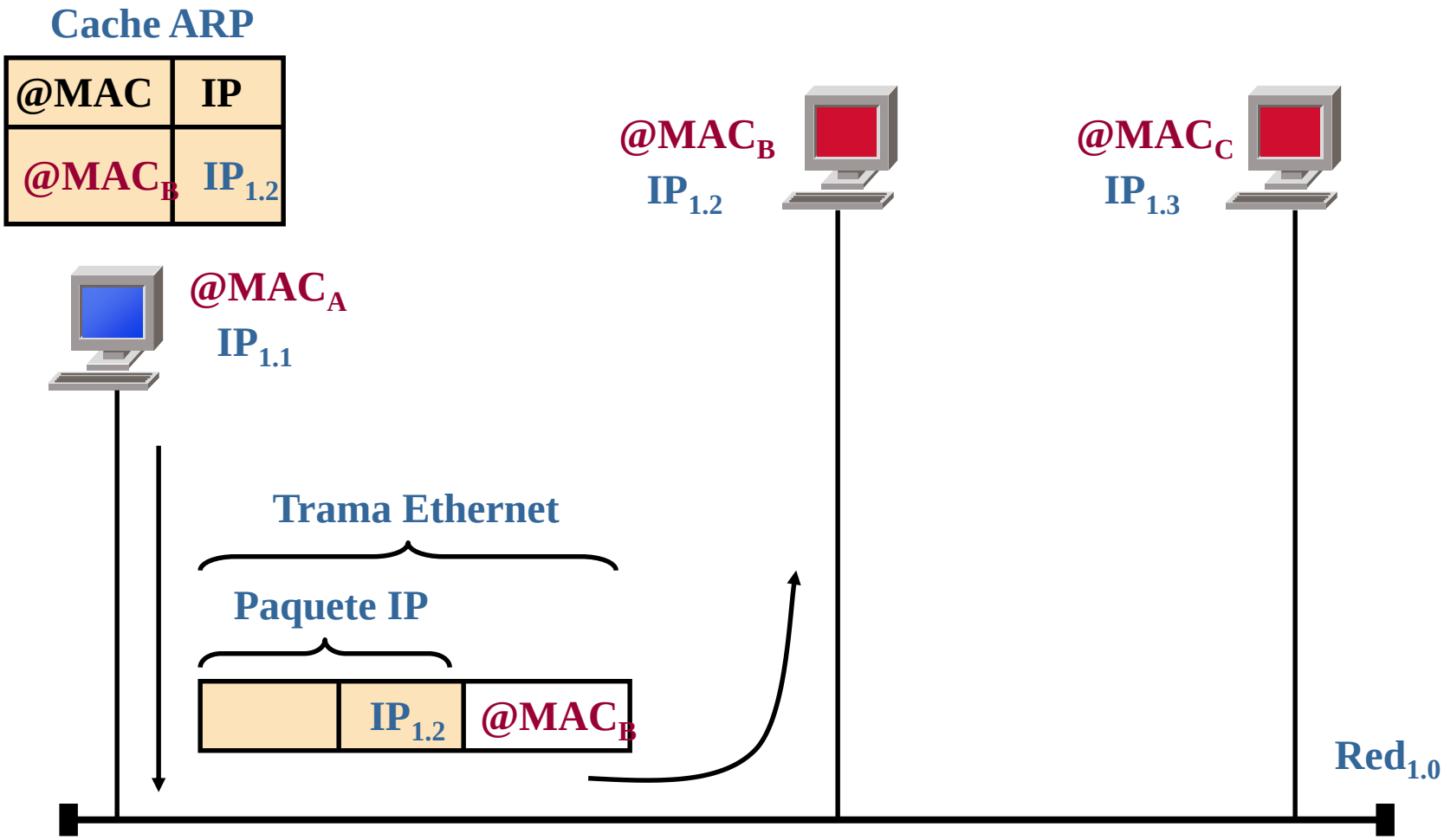
Modo de operación ARP (1)



Modo de operación ARP (2)



Modo de operación ARP (3)



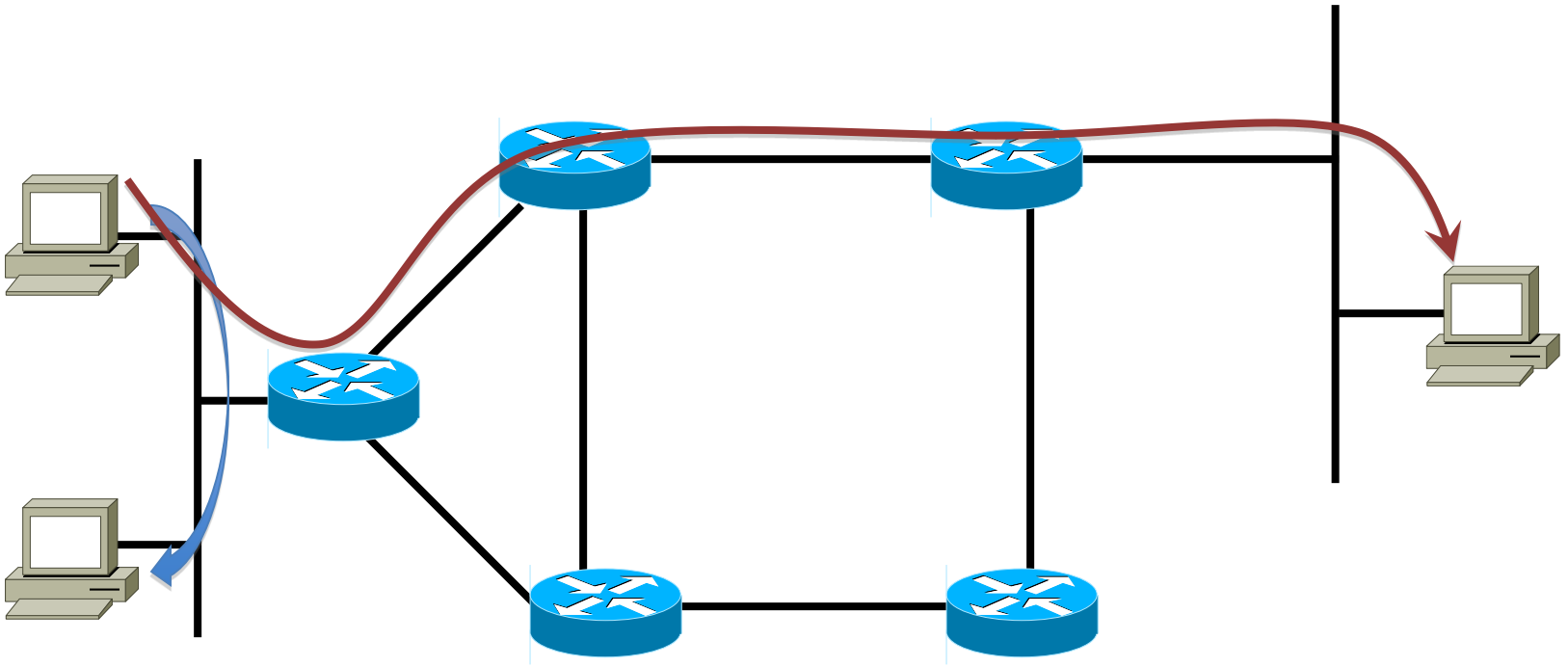
Enrutamiento

- Entrega directa de datagramas
  - La transmisión de un datagrama entre dos computadoras conectadas a la misma red IP no involucra enrutadores.
  - La fuente encapsula el datagrama en un paquete de la subred física, agrega la dirección “hardware” correspondiente y envía el paquete directamente al destino.

Enrutamiento

- Entrega indirecta de datagramas
  - La transmisión de un datagrama entre dos computadoras conectadas a diferentes redes IP involucra el uso de enrutadores.
  - La fuente envía el datagrama a un enrutador de su red IP encapsulándolo en un paquete de la subred física.
  - El datagrama pasa de enrutador a enrutador a través de diferentes subredes físicas hasta que llega a un enrutador directamente conectado a la red destino.
  - Este enrutador entrega directamente el datagrama al destino encapsulándolo en un paquete de la subred física.

Enrutamiento



Entrega directa

Entrega indirecta

Enrutamiento

- ¿Cómo sabe la fuente a qué enrutador enviar el datagrama?
- ¿Cómo saben los enrutadores la ruta por la que debe pasar el datagrama hasta llegar a la red destino?

Enrutamiento

- Tanto las computadoras como los enrutadores emplean tablas de enrutamiento que contienen una entrada por cada posible red IP destino en la que se indica:
  - que la entrega es directa, o
  - la dirección IP del enrutador que constituye el siguiente salto en la ruta hasta el destino

Enrutamiento

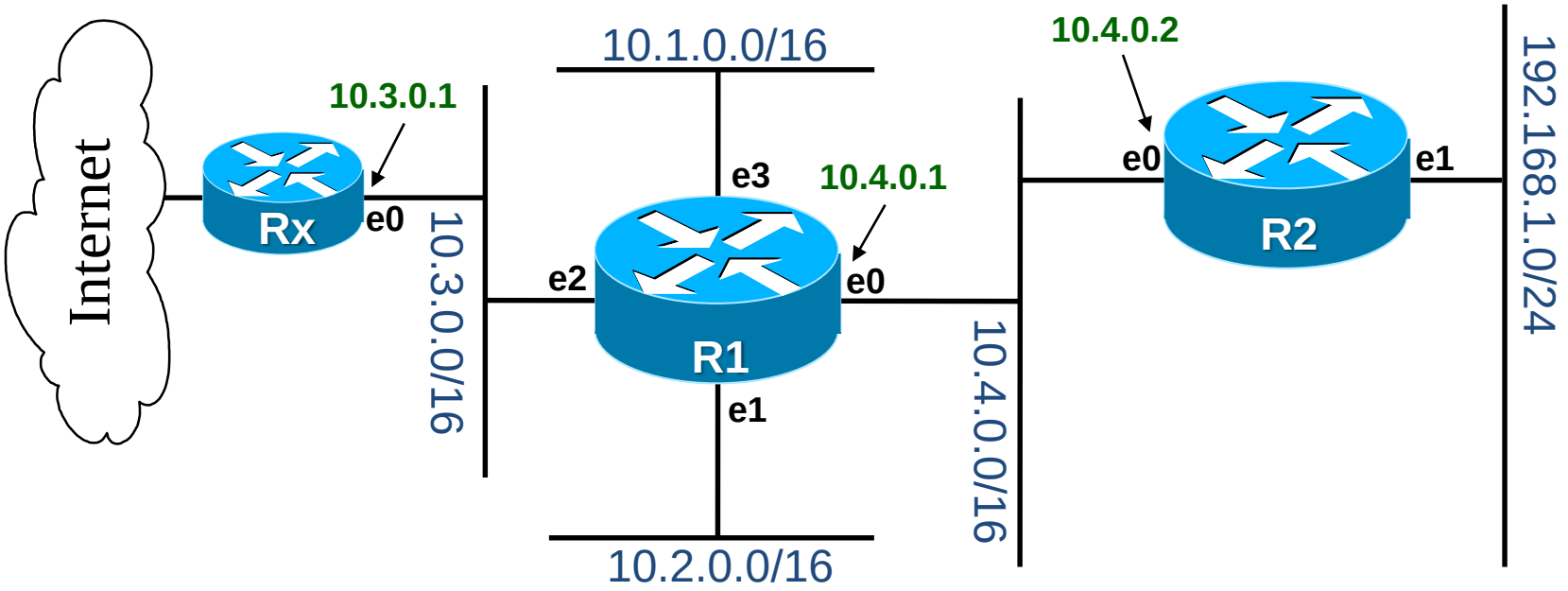
- En la tabla de enrutamiento también se indica para cada red destino qué interfaz de salida debe utilizarse.
- Cada interfaz de un enrutador tiene un identificador y una dirección IP distinta.
- La dirección de cada interfaz corresponde a la de la red IP a la cual se conecta.

Mecanismos de enrutamiento

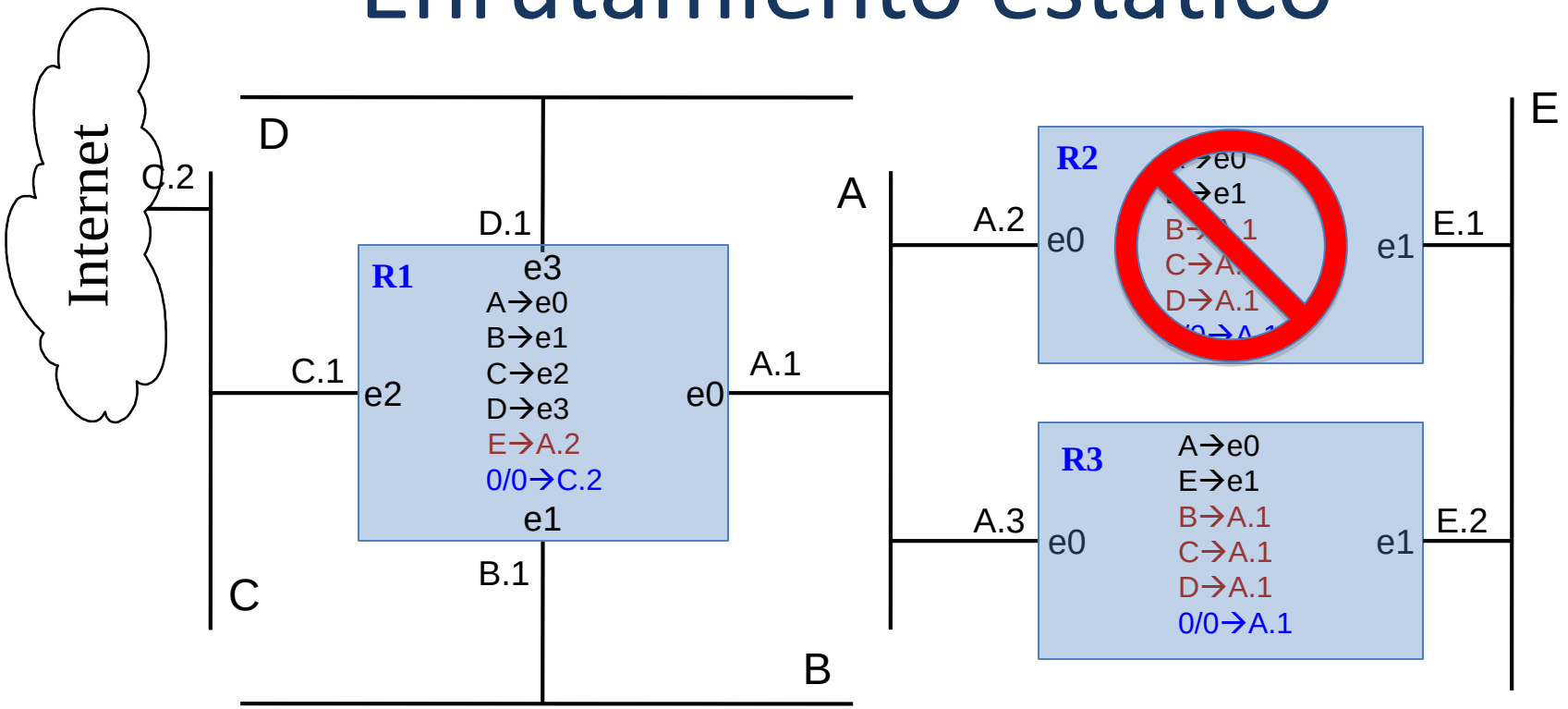
- Enrutamiento estático
- Protocolos de enrutamiento
  - Enrutamiento interno (a un Sistema Autónomo)
    - Basado en vector de distancias
    - Basado en estado del enlace
  - Enrutamiento externo
    - Basado en políticas

Enrutamiento estático

Red de referencia



Enrutamiento estático



- Simple de configurar (para redes pequeñas) pero propensa a errores (loops)
- No puede encontrar rutas alternativas en caso de fallos

Fuente: Toutain

Enrutamiento estático

- Comandos tipicos
  - BSD
    - route add 10.1.2.0/24 10.0.0.1
    - route add default 10.0.0.1
  - Linux
    - route add 10.1.2.0/24 gw 10.0.0.1
    - route add default gw 10.0.0.1
  - Cisco
    - ip route 10.1.2.0 255.255.255.0 10.0.0.1
    - ip route 0.0.0.0 0.0.0.0 10.0.0.1

Fuente: Toutain

Enrutamiento estático

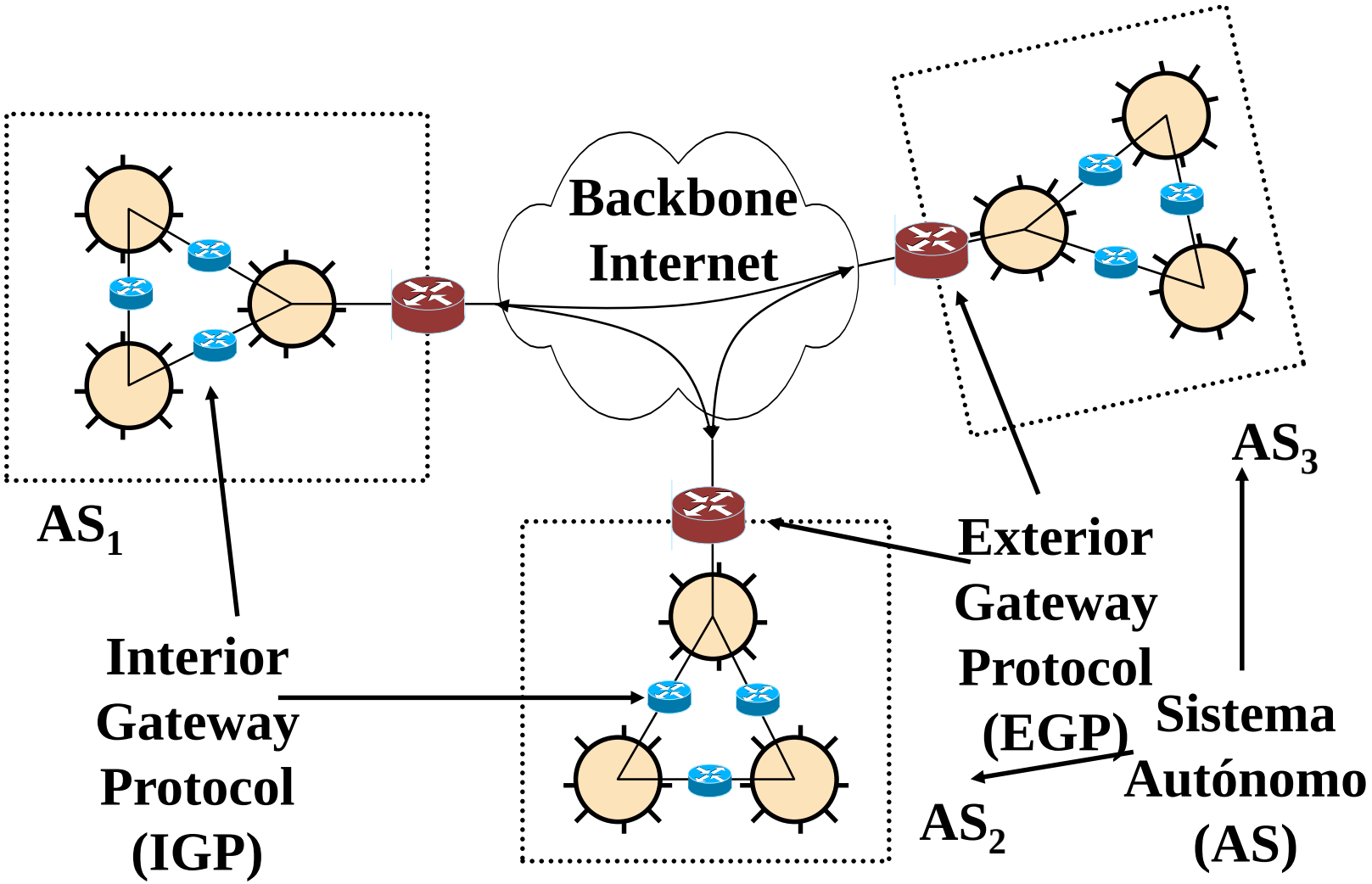
```
RouterB25#sh ip ro
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route


Gateway of last resort is 193.50.69.73 to network 0.0.0.0


B 193.52.74.0/24 [200/0] via 193.50.69.74, 1d05h
192.44.77.0/24 is variably subnetted, 2 subnets, 2 masks
B 192.44.77.0/24 [200/0] via 193.50.69.74, 1d05h
C 192.44.77.96/28 is directly connected, GigabitEthernet0/1.16
10.0.0.0/24 is subnetted, 6 subnets
S 10.1.1.0 [1/0] via 192.108.119.196
S 10.35.1.0 [1/0] via 192.108.119.205
S 10.35.4.0 [1/0] via 192.108.119.162
S 10.35.30.0 [1/0] via 192.108.119.160
C 10.51.0.0 is directly connected, GigabitEthernet0/1.51
C 10.49.0.0 is directly connected, GigabitEthernet0/1.49
192.108.119.0/24 is variably subnetted, 6 subnets, 4 masks
C 192.108.119.128/25 is directly connected, GigabitEthernet0/1.5
....
```

Fuente: Toutain

Jerarquía en el enrutamiento



Protocolos de enrutamiento

- Internet es una red formada por Sistemas Autónomos interconectados.
- Un Sistema Autónomo está constituido por un conjunto de subredes y enrutadores que tienen una administración común.
  - UNAM SA 278
  - ITAM SA 21520

Protocolos de enrutamiento

- Cada Sistema Autónomo
  - puede escoger su propio protocolo de enrutamiento
  - debe intercambiar información de enrutamiento con otros Sistemas Autónomos

Protocolos de enrutamiento

- IGP
  - Vectores de Distancias RIP-2 (RFC 2453)
  - Estado de Enlaces OSPF-2 (RFC 2328)
- EGP
  - Vectores de Ruta BGP-4 (RFC 1771)

Vector de distancias

RIP, RIPv2, IGRP

Algoritmo de vector de distancias

- BD de enrutamiento y FIB (forwarding information base) son iguales
  - Se asocia un costo (típicamente número de saltos) a cada prefijo
- Enrutador difunde periódicamente su FIB en cada enlace al que está conectado
- Si un enrutador difunde un nuevo prefijo o uno con menor costo
  - Esta entrada se agrega/modifica en la FIB
  - Siguiente salto es la dirección IP de quien difundió el anuncio
  - El costo se incrementa en uno

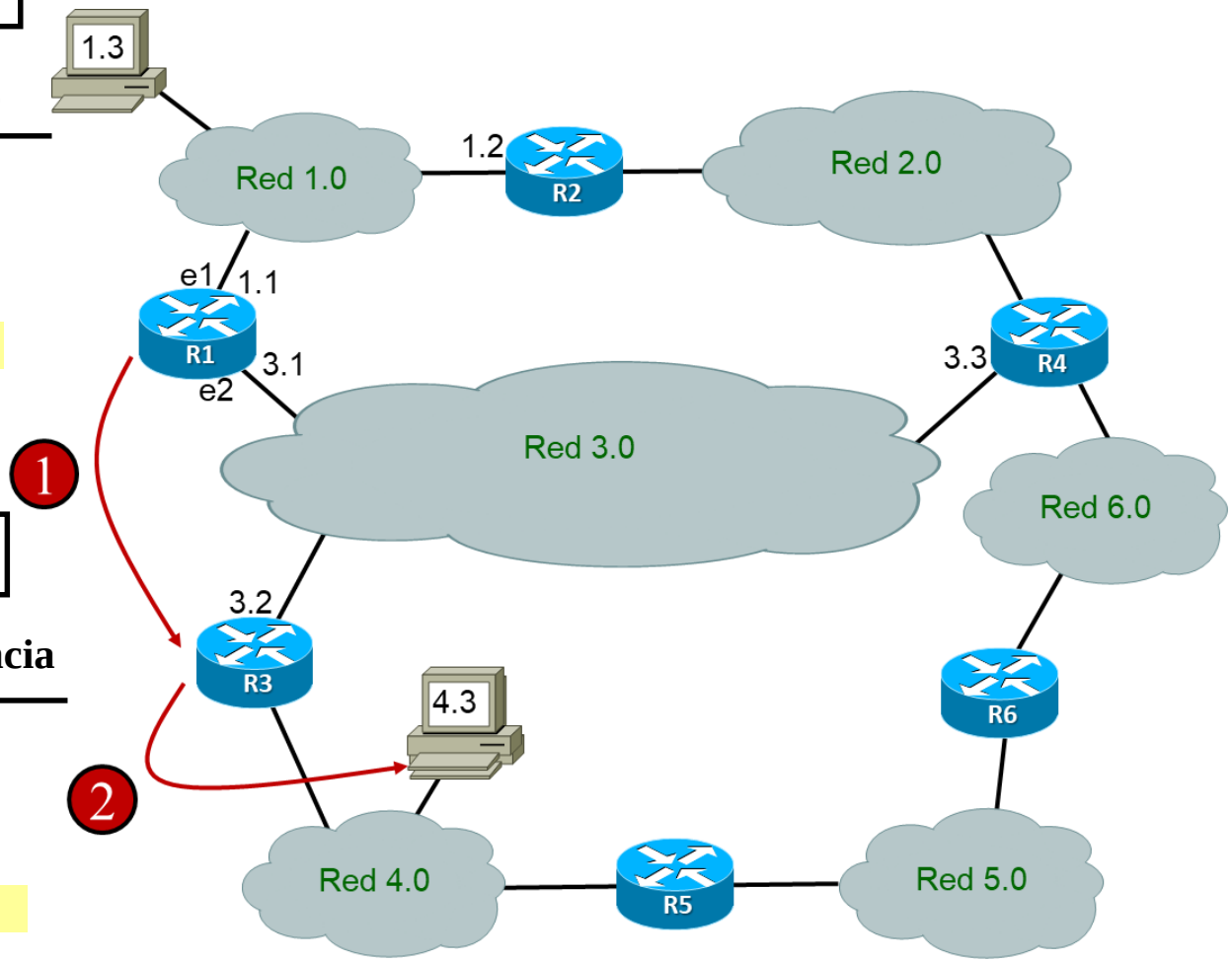
IGP (Algoritmo de Vector de distancias)

Tabla de distancias para R1

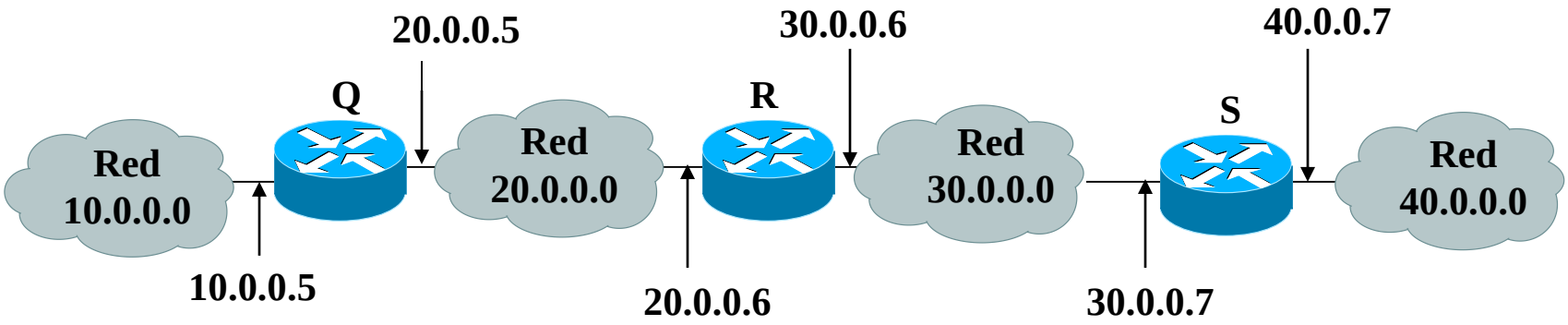
Red	R2 , 1	R3 , 2	R4 , 2
1 . 0	2	2	3
2 . 0	2	3	2
3 . 0	3	2	2
4 . 0	4	2	3
5 . 0	4	3	3
6 . 0	3	3	2

Tabla de ruteo para R1

Red	Sig.	Enlace	distancia
1 . 0	R1	1	1
2 . 0	R2	1	2
3 . 0	R1	2	1
4 . 0	R3	2	2
5 . 0	R3	2	3
6 . 0	R4	2	2



Enrutamiento



Red IP	Siguiente salto
20.0.0.0	entrega directa
30.0.0.0	entrega directa
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

RIP

- Cada enrutador mantiene en su tabla de enrutamiento la distancia, en saltos, que lo separa de cada destino.
- Envía a sus vecinos su vector de distancias cada 30 segundos.

Red IP	Distancia	Siguiente salto
20.0.0.0	1	entrega directa
30.0.0.0	1	entrega directa
10.0.0.0	2	20.0.0.5
40.0.0.0	2	30.0.0.7

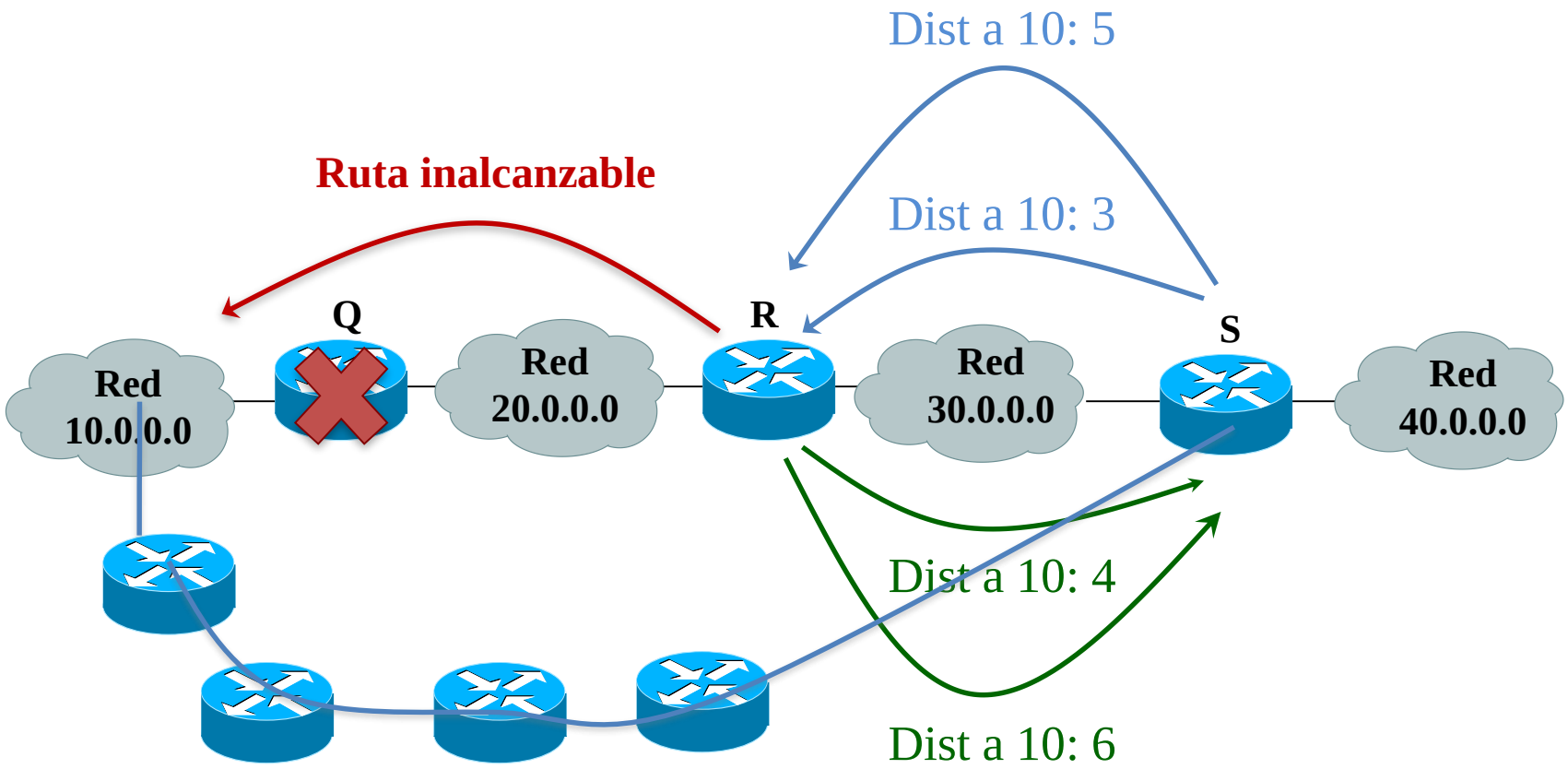
Red IP	Distancia
20.0.0.0	1
30.0.0.0	1
10.0.0.0	2
40.0.0.0	2

RIP

- Los mensajes RIP se encapsulan en datagramas UDP.
- En un mensaje RIP pueden enviarse hasta 25 entradas del vector de distancias.
- Para transportar vectores grandes se utilizan varios mensajes.
- Una entrada de la tabla se vuelve inválida si pasan X ciclos de refresco sin que sea vista
  - Típicamente X = 3 ó 6 => 90 ó 180 seg

RIP – Problema de convergencia

- Cuenta al infinito (entre R y S)



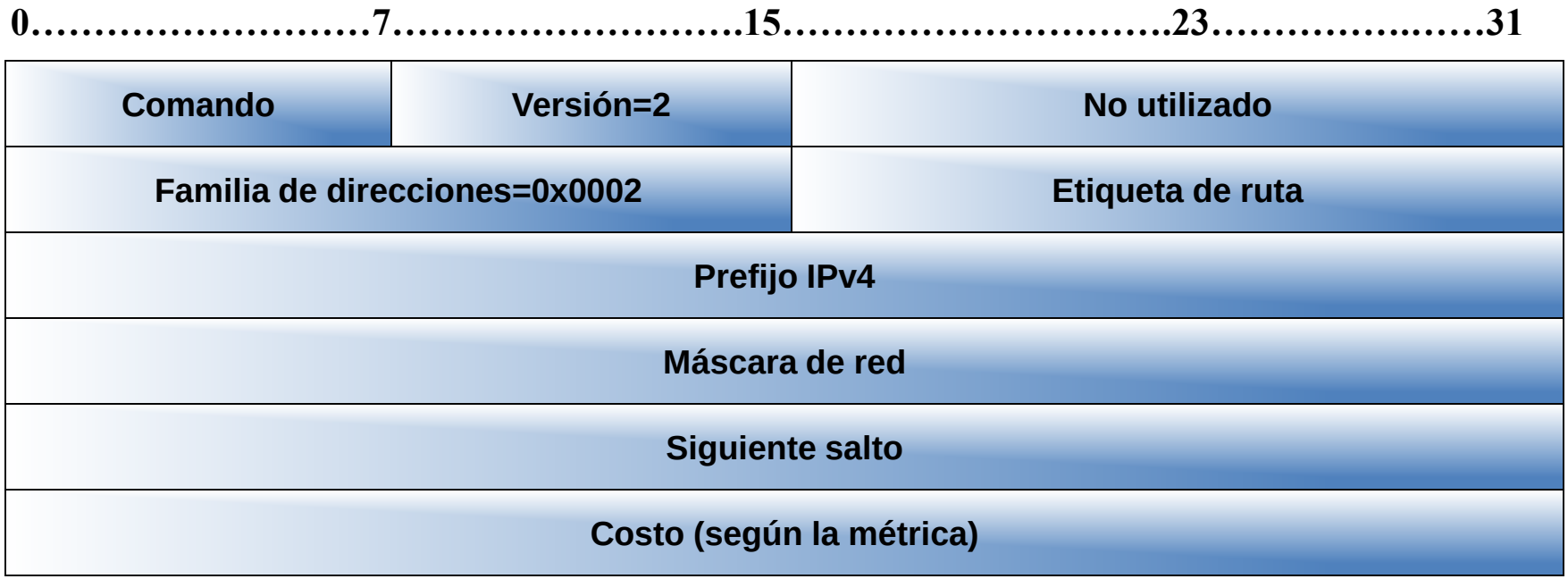
RIP – Formas de reducir este problema

- Distancia máxima entre dos dispositivos: 15 enrutadores (16=∞)
  - Después se considera ruta inalcanzable
- Envenenamiento hacia atrás
  - Al recibir una ruta inalcanzable (distancia infinita) se marca así en el vector de distancias
  - Se propaga inmediatamente a sus vecinos
- Split Horizon:
  - Si “S” piensa que puede llegar a 10.0.0.0 vía “R”, sus mensajes a R no deben incluir esta red

Vector de distancias

- Algoritmo muy simple de entender, administrar e implementar
- Desempeño es muy pobre:
  - Visión limitada de la red basada en el resumen hecho por los otros enrutadores
  - Puede crear loops o retrasos largos para reconectar partes de la red
  - La tabla de enrutamiento se envía periódicamente
    - Para detectar rutas caídas
    - Para detectar mejores trayectorias
- Genera carga en la red y de procesamiento
- Debe limitarse a la (auto)configuración de pequeñas redes

RIP-2

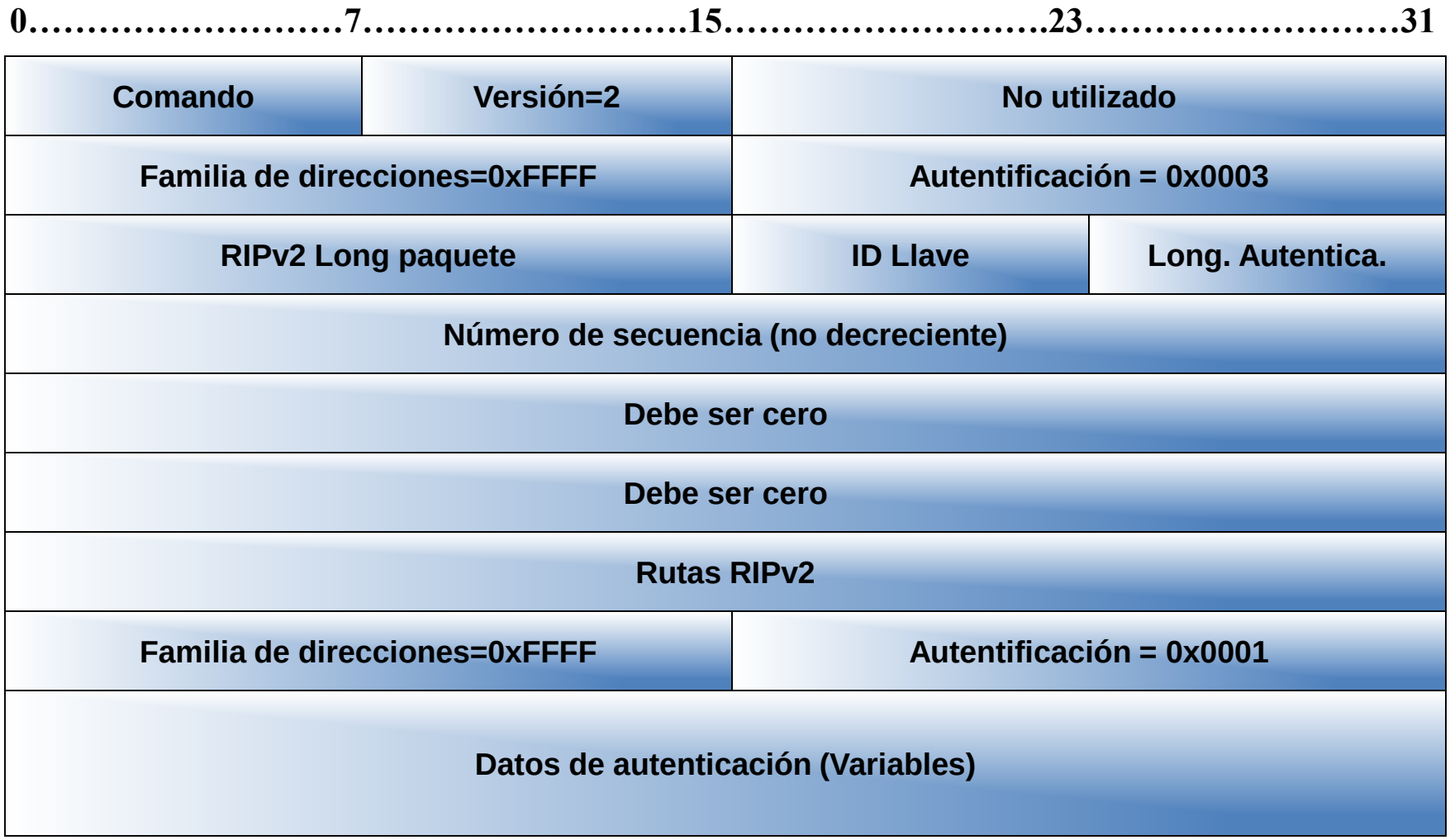


- Comando: 1= solicitud, 2= respuesta
- Dirección multicast: 224.0.0.9.. Puerto UDP 520
- Siguiente salto en vez de la dirección fuente en el encabezado
- Etiqueta de ruta diferencía entre rutas internas y externas (p.e. SA de quien anunció la ruta)

Seguridad en RIP-2

- Un atacante puede fácilmente anunciar una ruta al enrutador por omisión con un costo muy bajo, interceptando así todos los mensajes
- RIP-2 ofrece una autenticación sencilla firmando digitalmente los mensajes
  - Mecanismo original basado en MD5 (RFC 2082)
  - Hoy se recomienda SHA1 (RFC 4822)

Seguridad en RIP-2



IGRP

- Algoritmo propietario de Cisco que utiliza Vectores de Distancias
- El número de saltos no está limitado a 15
- Las actualizaciones se envían cada 90 segundos, por lo que se carga menos la red con información de enrutamiento
- Utiliza como distancia una métrica compuesta ponderada:
  - velocidad de transmisión, retardo, carga, tasa de error.
- Puede balancear la carga entre múltiples rutas que tienen una distancia equivalente.

IGRP

- Para evitar los ciclos que involucran más de dos enrutadores, un enrutador no toma en cuenta las actualizaciones recibidas para una ruta:
  - durante 90 segundos después de haberla considerado inaccesible (*hold down)*,
  - si el número de saltos ha crecido de manera importante (rutas envenenadas).

Estado de enlace

OSPF

Algoritmos de estado de enlace

- Consideran el *estado del enlace* para establecer la topología
  - Estado de enlace es la descripción de una interfaz en un enrutador (Dir. IP, máscara, tipo de red, …) y su relación con enrutadores vecinos
- Cada enrutador envía esta información y forman una base de datos a partir de la cual se estima la topología y se calculan trayectorias de costo mínimo

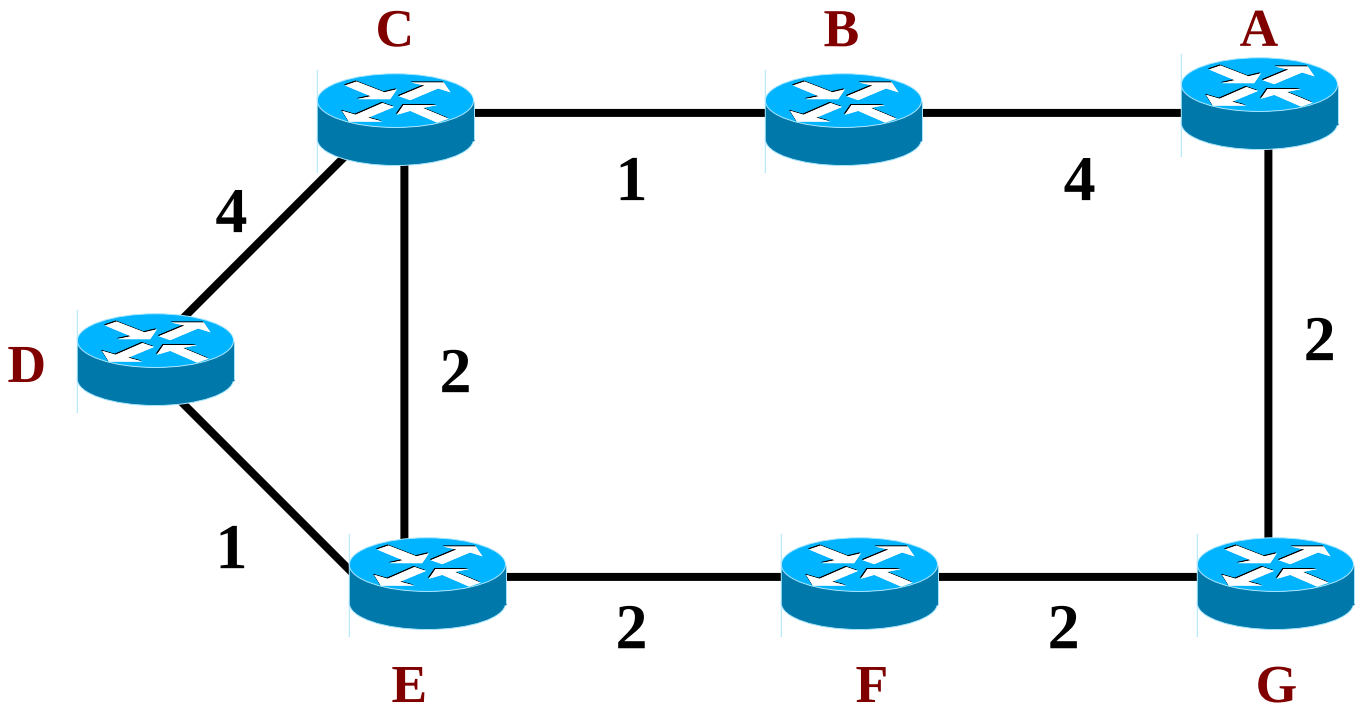
Algoritmo de Estado de enlace

1. Descubrir sus vecinos y aprender sus direcciones de red.
2. Medir el costo del enlace a cada uno de sus vecinos y anunciar la lista de vecinos y el costo asociado (LSA, link State Advertisements)
   - Lista de vecinos, no toda la tabla de enrutamiento
3. Crear una base de datos que describe la topología de la red (es la misma para cada enrutador)
4. Cada enrutador selecciona la ruta más corta a cada destino (algoritmo SPF, Shortest Path First)
5. Esta información se usa para actualizar las tablas de enrutamiento

Algoritmo SPF (Shortest Path First)

- Algoritmo propuesto por Dijikstra, tiene como objetivo encontrar la trayectoria de menor costo entre dos nodos (en este caso entre dos ruteadores)
- Componentes del algoritmo SPF:
  - Base de datos del estado de enlace creada mediante el intercambio de paquetes LSP (Link State Pakets).
  - Base de datos de alternativas, todas la tuplas (ID ruteador, costo, dirección) hacia todos los nodos.
  - Base de datos de trayectoria (las mejoras tuplas)
  - Base de datos de ruteo (tabla de ruteo) para la operación del ruteador.

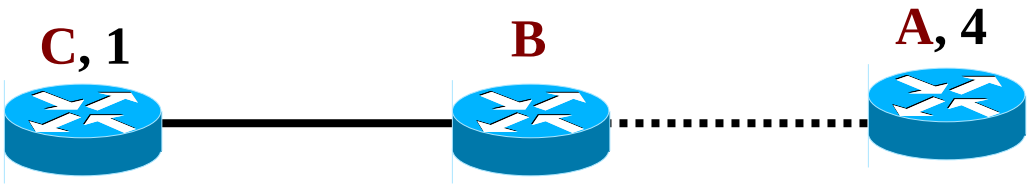
Algoritmo SPF (Ejemplo 1/7)



A		B		C		D		E		F		G	
B	4	A	4	B	1	C	4	C	2	E	2	A	2
G	2	C	1	D	4	E	1	D	1	G	2	F	2
				E	2			F	2				

Algoritmo SPF (Ejemplo 2/7)

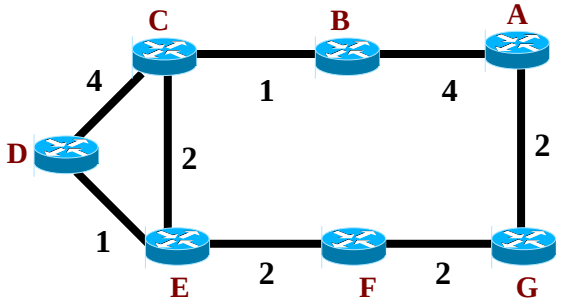
Algoritmo aplicado a B



Desconocidos: ~~A, B, C~~, D, E, F, G

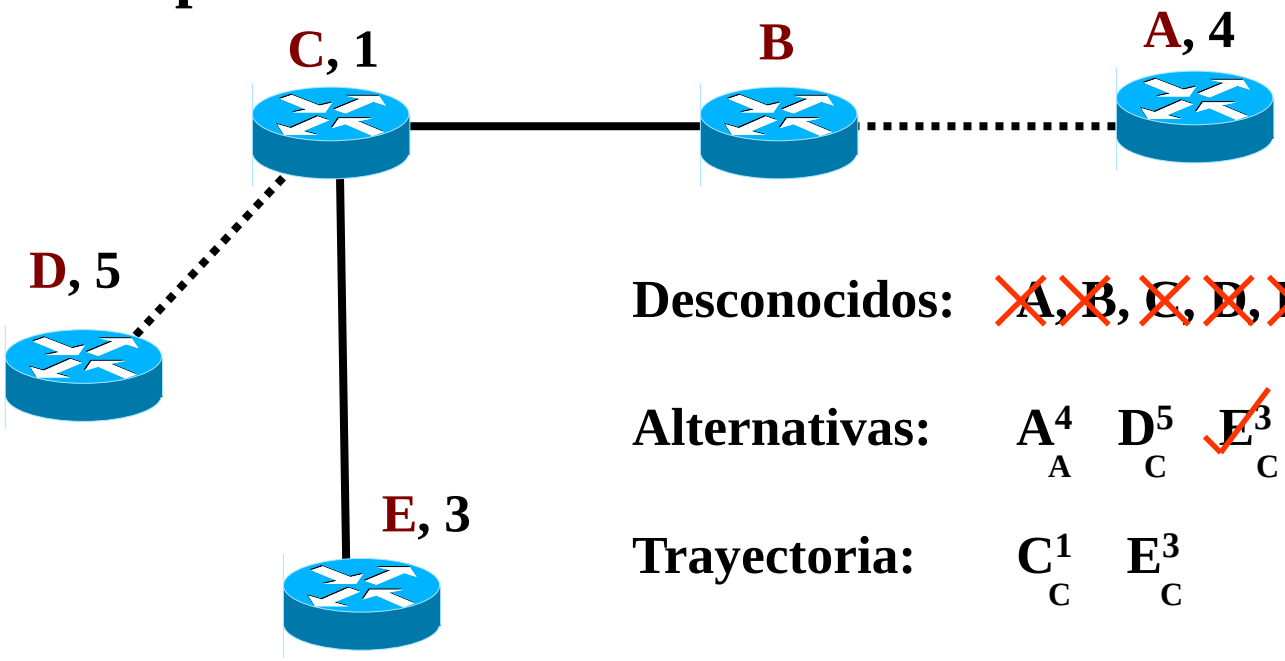
Alternativas: C^{1}_{C} A^{4}_{A}

Trayectoria: C^{1}_{C}



Algoritmo SPF (Ejemplo 3/7)

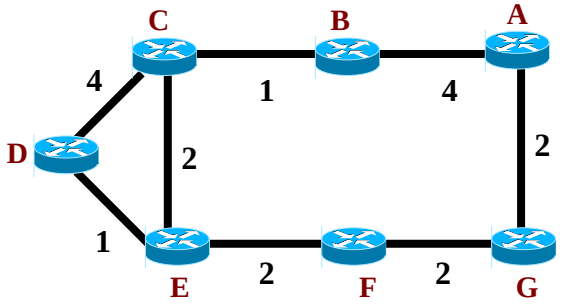
Algoritmo aplicado a B



Desconocidos: ~~A, B, C, D, E~~, F, G

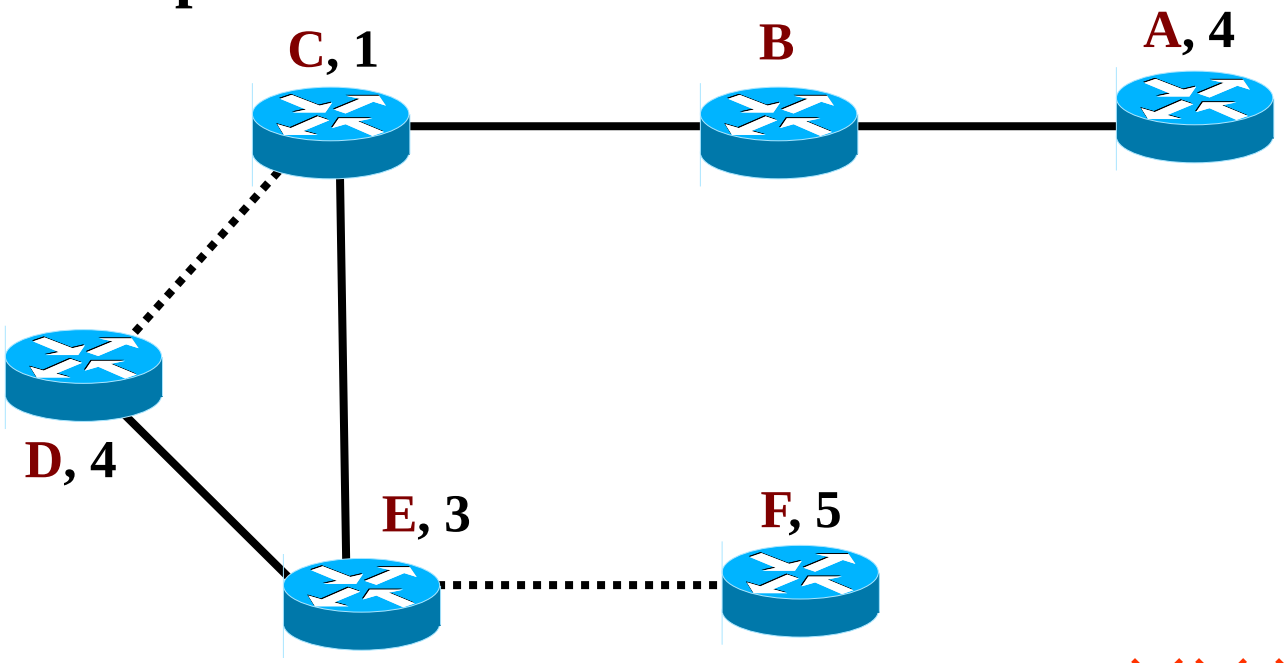
Alternativas: A^4_A D^5_C ~~E^3_C~~

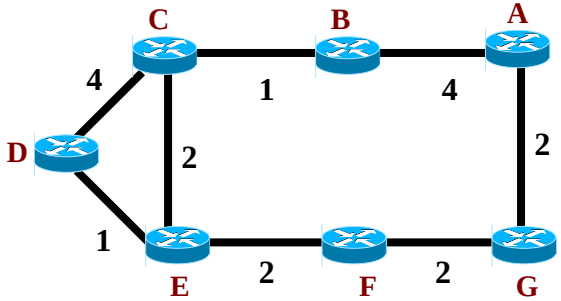
Trayectoria: C^1_C E^3_C



Algoritmo SPF (Ejemplo 4/7)

Algoritmo aplicado a B





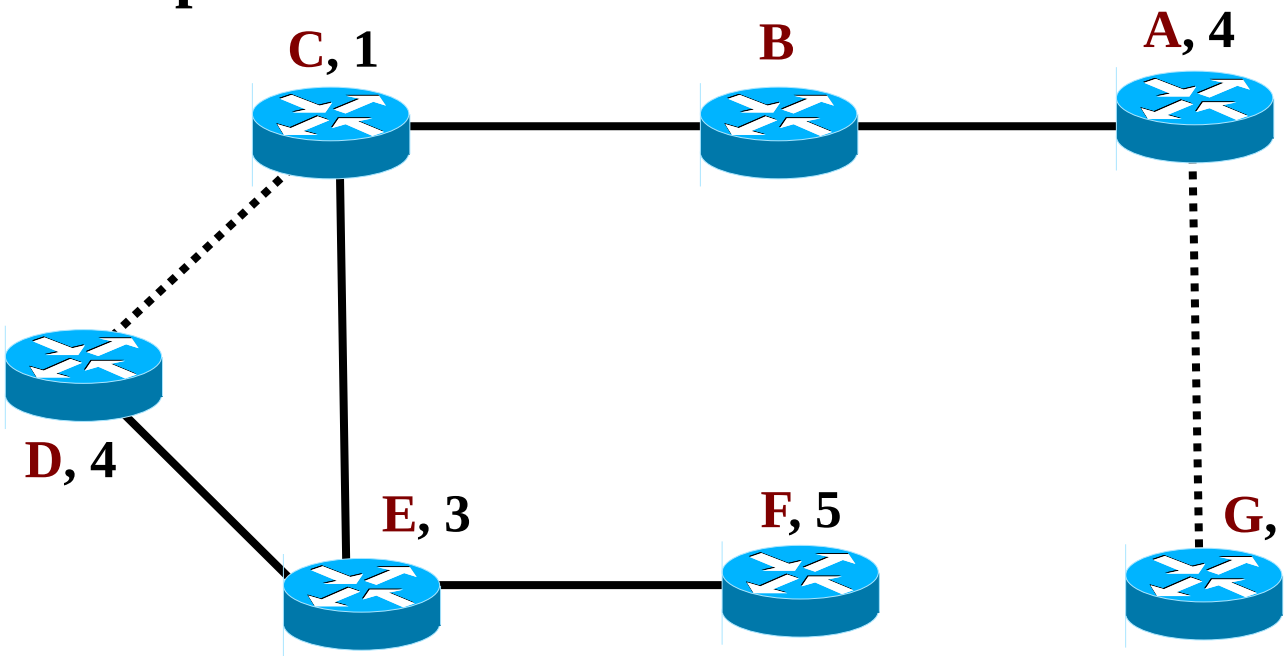
Desconocidos: ~~A, B, C, D, E, F,~~ G

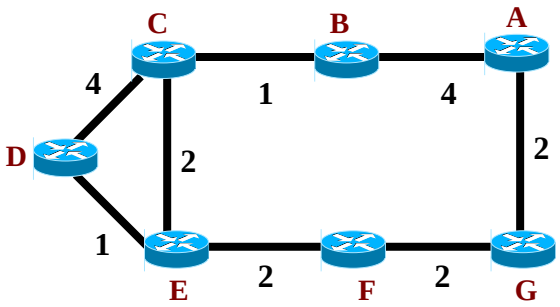
Alternativas: ~~A^4_A~~ D^5_C ~~D^4_C~~ F^5_C

Trayectoria: C^1_C E^3_C A^4_A D^4_C

Algoritmo SPF (Ejemplo 5/7)

Algoritmo aplicado a B





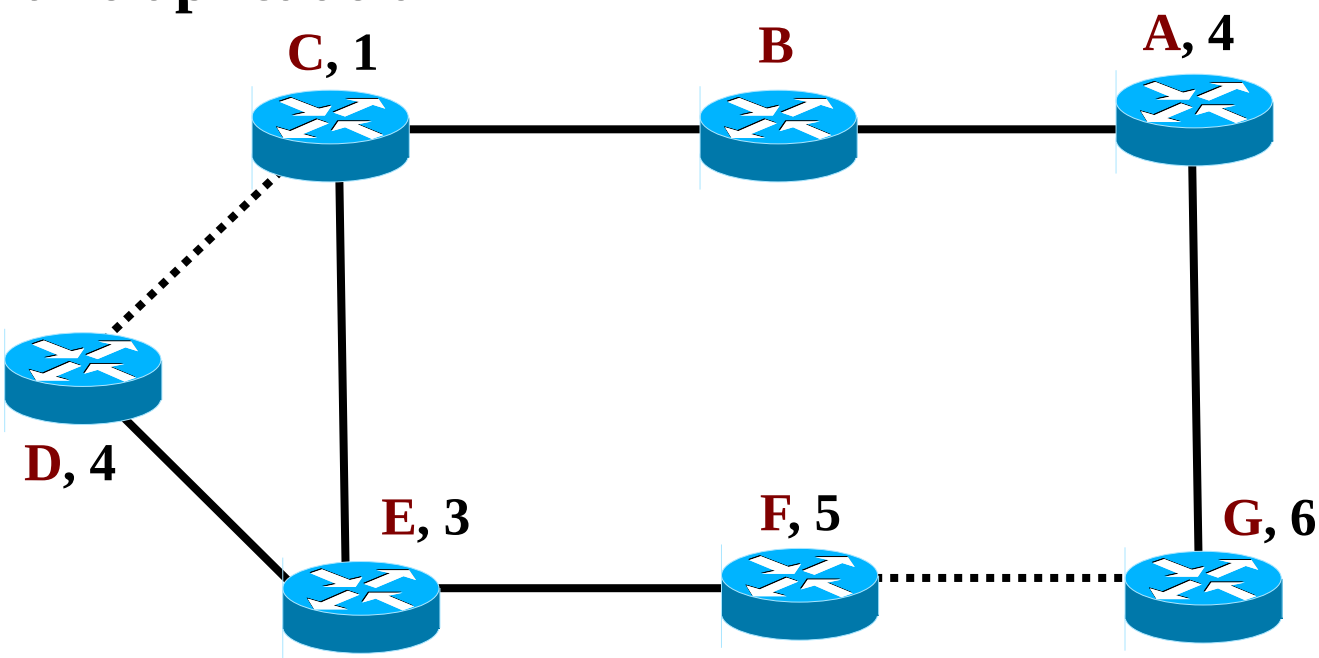
Desconocidos: ~~A, B, C, D, E, F, G~~

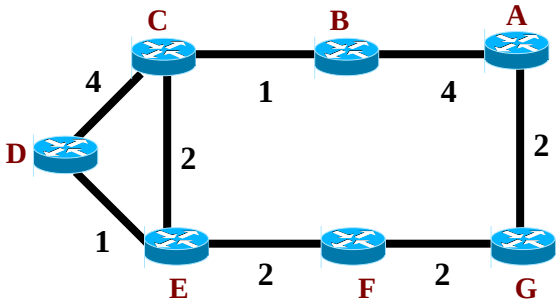
Alternativas: F^5_C G^6_A

Trayectoria: C^1_C E^3_C A^4_A D^4_C F^5_C

Algoritmo SPF (Ejemplo 6/7)

Algoritmo aplicado a B





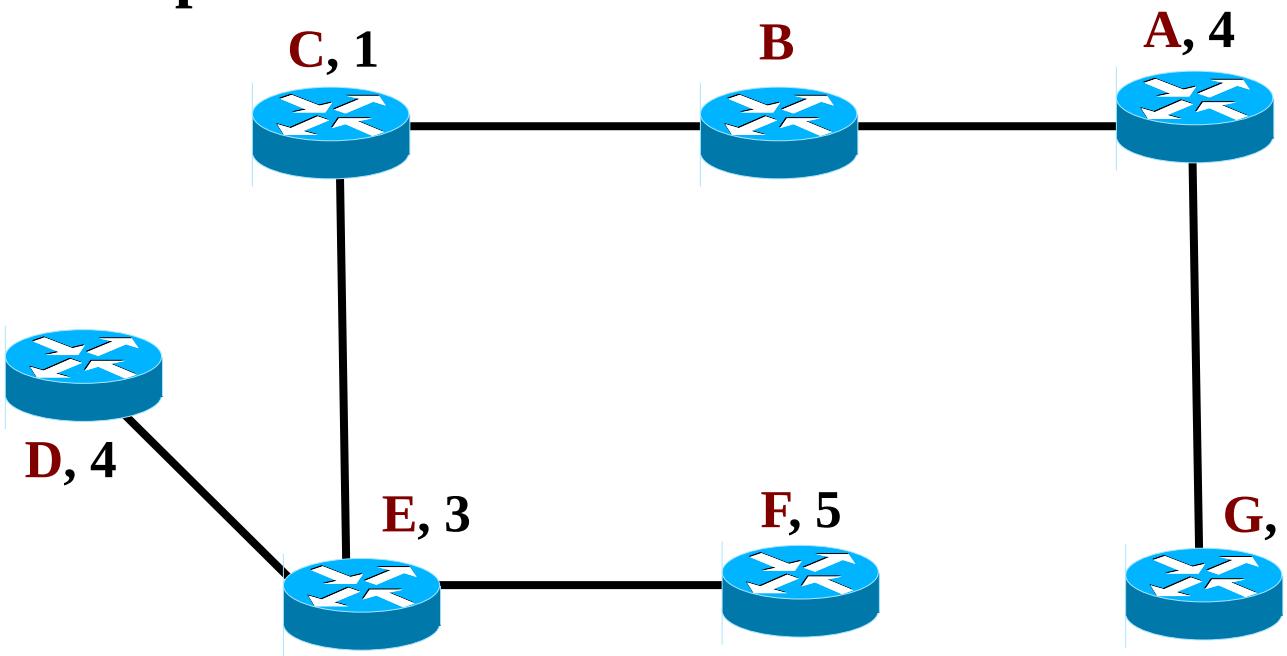
Desconocidos: ~~A, B, C, D, E, F, G~~

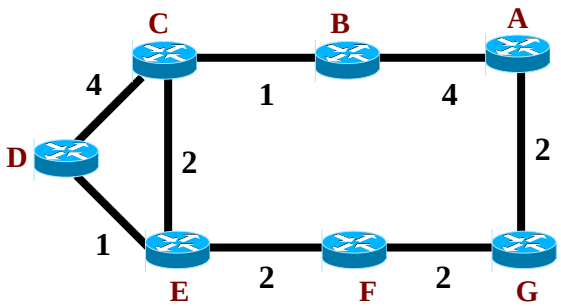
Alternativas: ~~G^6_A~~ G^7_C

Trayectoria: C^1_C E^3_C A^4_A D^4_C F^5_C G^6_A

Algoritmo SPF (Ejemplo 7/7)

Algoritmo aplicado a B





Desconocidos: ~~A, B, C, D, E, F, G~~

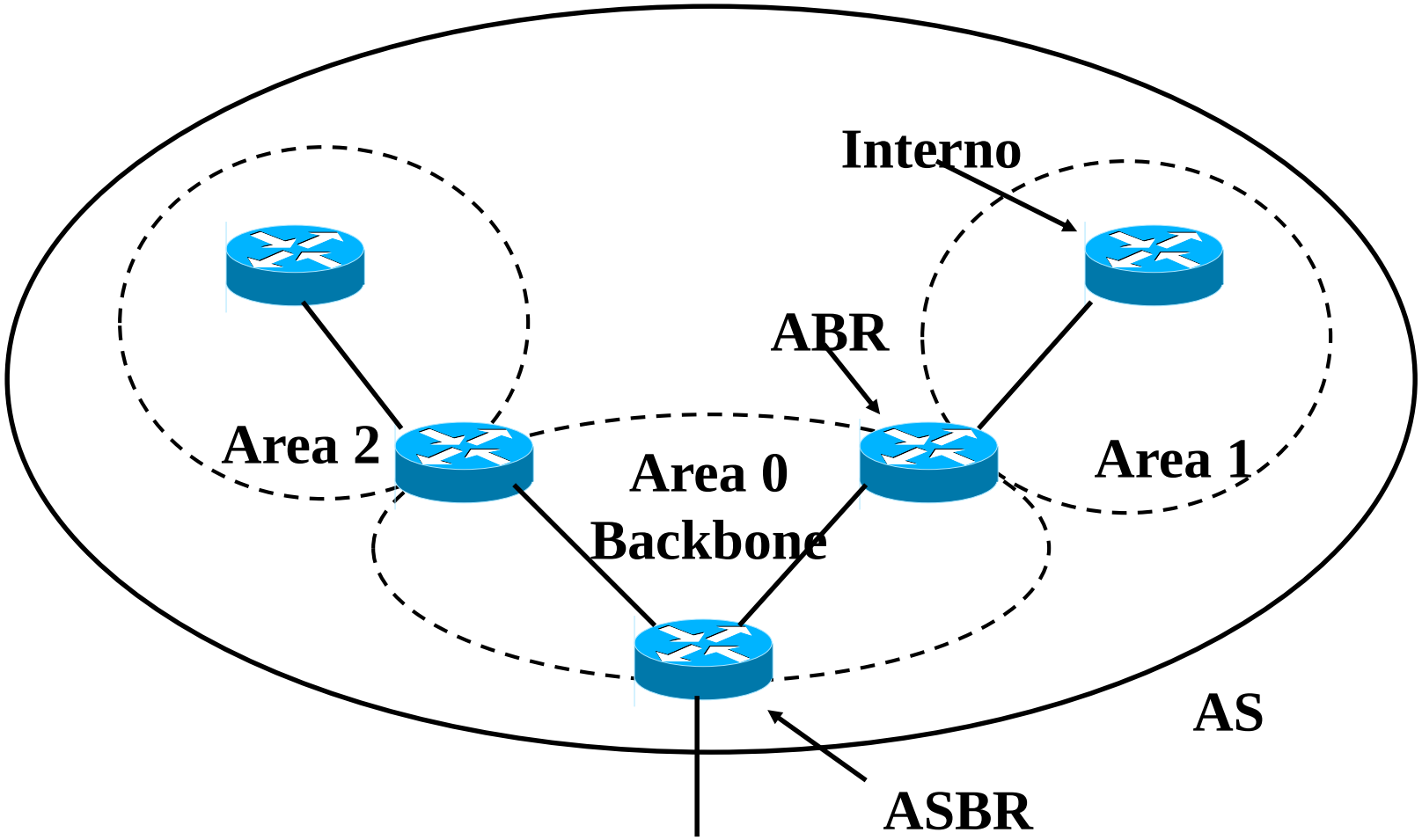
Alternativas:

Trayectoria: C^1_C E^3_C A^4_A D^4_C F^5_C G^6_A

OSPF (Open Shortest Path First)

- OSPF es una tecnología de estado de enlace
- Fue desarrollado por el IETF en 1988
- Escrito para cubrir las necesidades de redes grandes, ofrece mucho mayor escalabilidad que RIP
  - Velocidad de convergencia
  - Soporte de máscaras de longitud variable
  - Escalabilidad
  - Optimización del ancho de banda
  - Método para selección de rutas

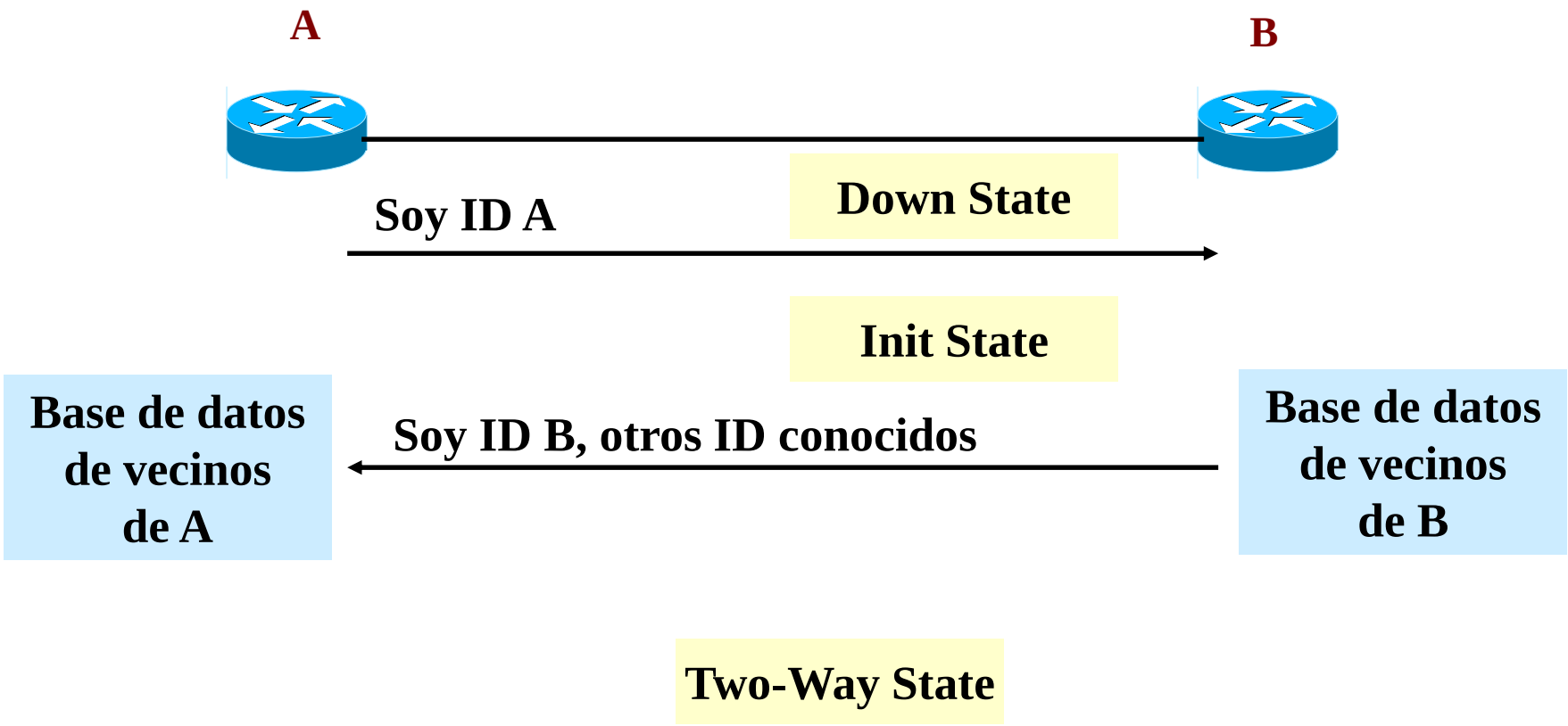
Elementos de OSPF



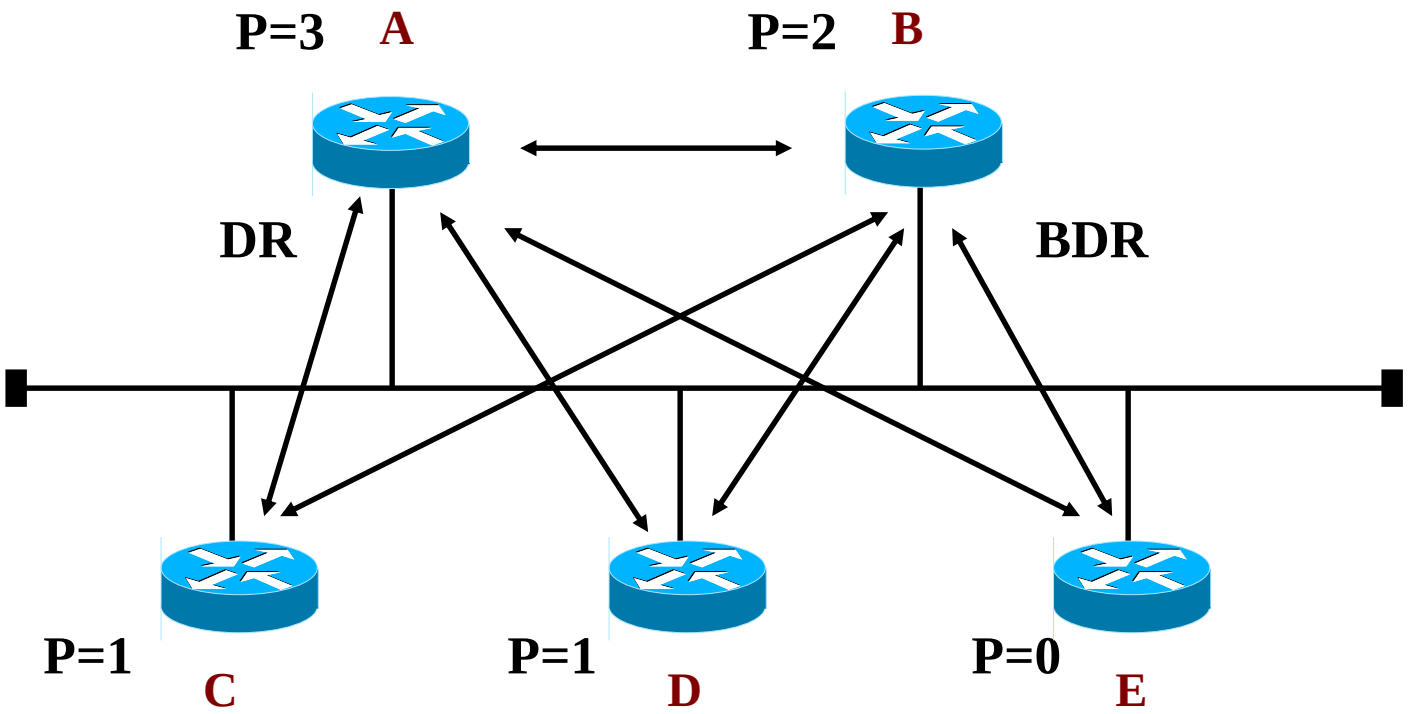
Operación de OSPF

- Paso 1.- Descubrir los enrutadores vecinos (protocolo Hello)
- Paso 2.- Seleccionar un enrutador designado (DR) y un enrutador de respaldo (BDR) por cada subred
- Paso 3.- Descubrimiento de rutas (LSP Link State Packets)
- Paso 4.- Selección de rutas (selección de la ruta de menor costo)
- Paso 5.- Mantenimiento de información de enrutamiento

Paso 1.- Reconocimiento de vecinos (protocolo Hello)

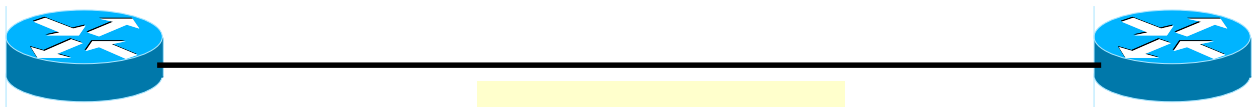


Paso 2.-Selección del enrutador designado



Recibe y reenvía la información de estado de enlace

Paso 3.- Descubrimiento de rutas



A **B** **DB**

Exchange State

Resumen de mi BD (DD)

LSAck

Loading State

LSR Requiere Info. Completa de por ej. C

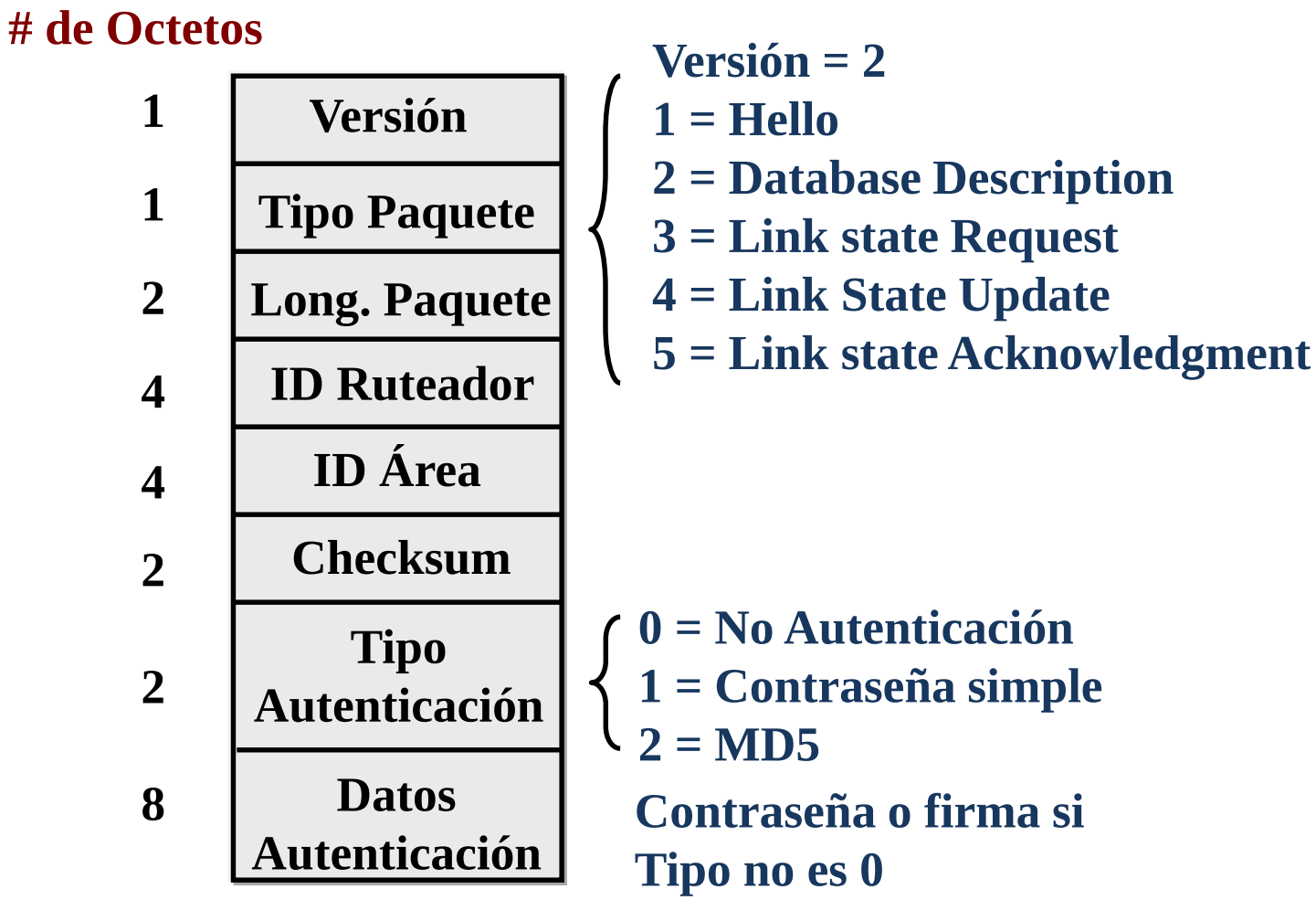
LSU Aquí está la información de C

LSAck

Full State

DD : Database Description
LSR : Link State Request
LSU : Link State Update

Tipo de paquetes OSPF



Paso 4.- Selección de rutas

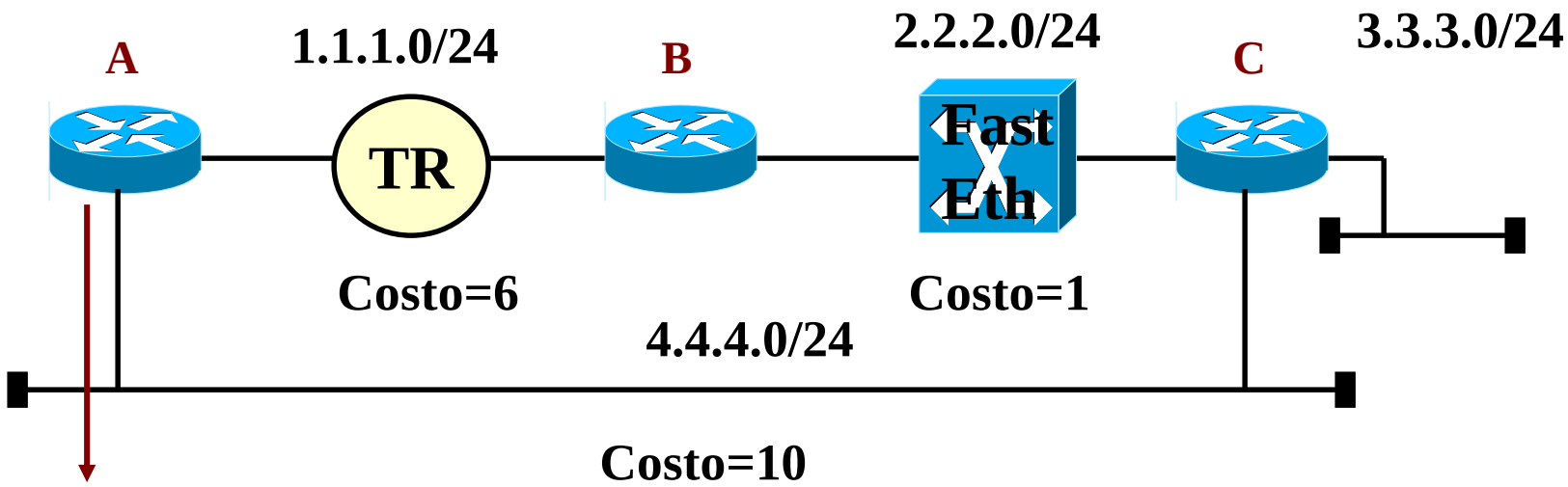
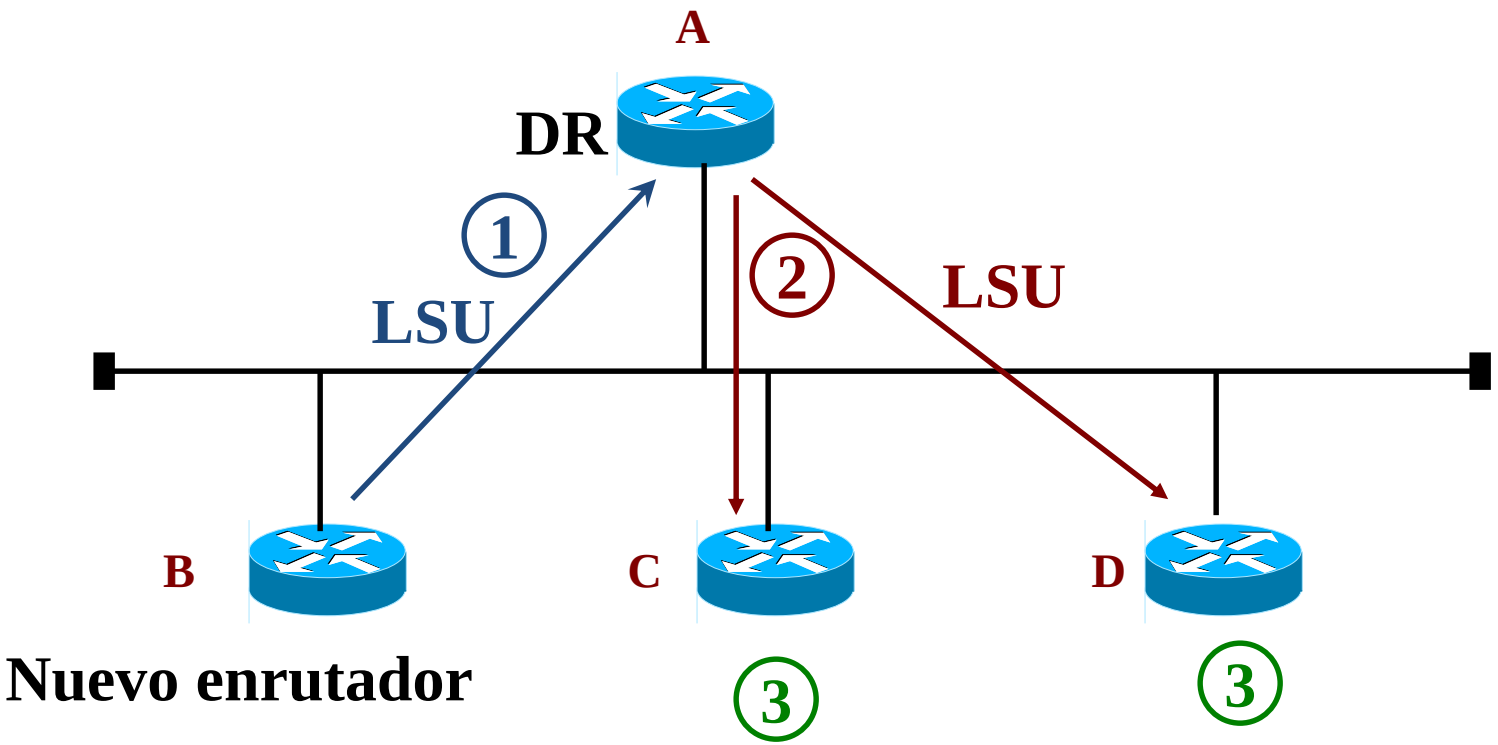


Tabla de Ruteo

Red	Costo
2.2.2.0	6
3.3.3.0	7
3.3.3.0	10

Costo = 100 Mbps / Ancho de Banda (Mbps)

Paso 5.- Mantenimiento de información de rutas



EGP
Vector de trayectorias

BGP

BGP – Border Gateway Protocol

- Es el (único) protocolo usado entre Sistemas Autónomos para intercambiar información de enrutamiento
- Reduce la cantidad de información intercambiada sumarizando rutas
- Utiliza un algoritmo de Vectores de Rutas
- Cubre tres objetivos:
  - Escalabilidad
  - Políticas. Los AS tienen libertad de decidir qué rutas anunciar y cómo
  - Cooperación bajo condiciones de competencia. Bajo varias opciones AS deciden hacia dónde enrutar

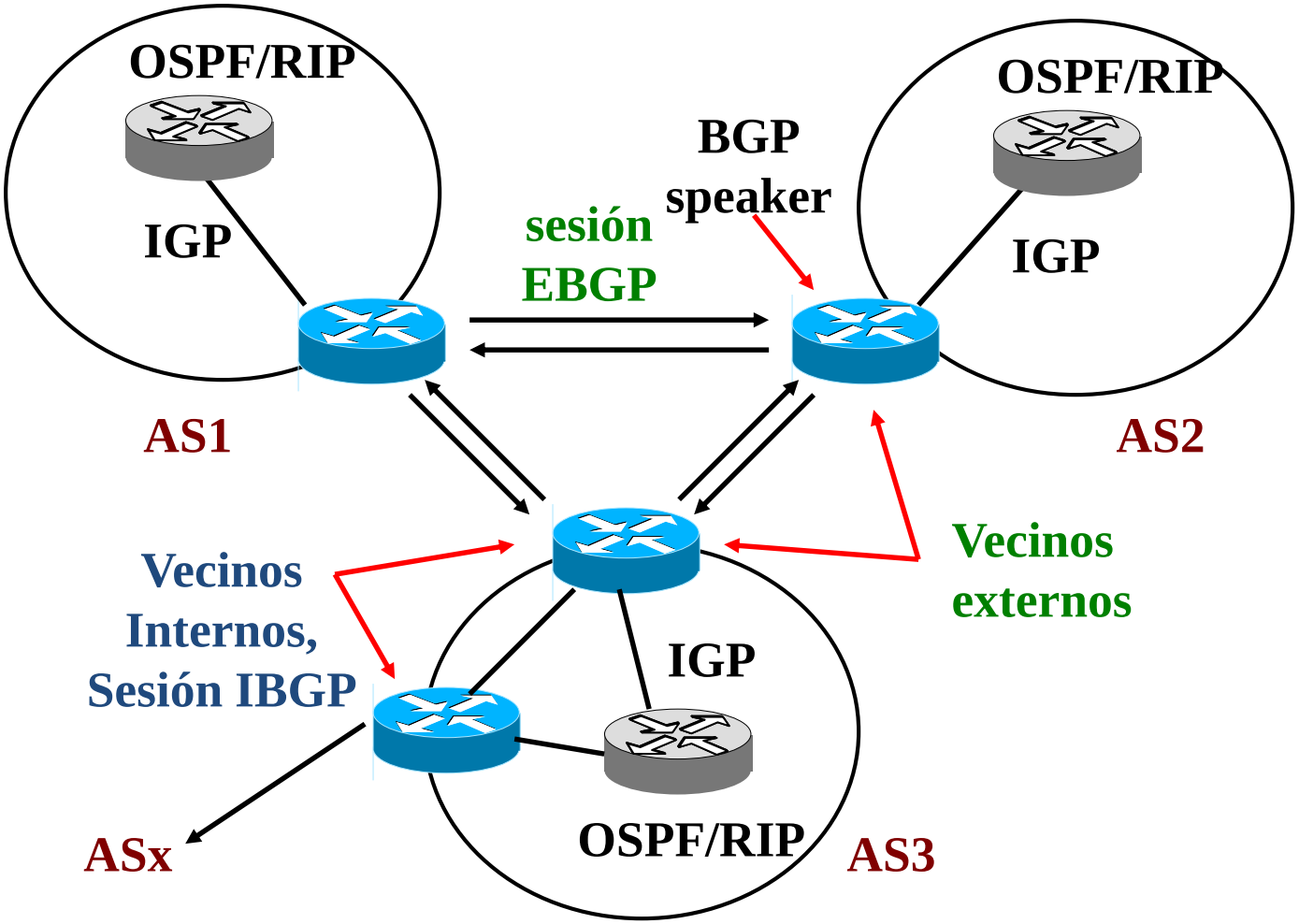
BGP

- Para tomar decisiones de enrutamiento, pueden tenerse en cuenta, por ejemplo, cuestiones políticas, económicas, de confiabilidad o de seguridad.
- Este tipo de consideraciones se configura manualmente en los enrutadores.

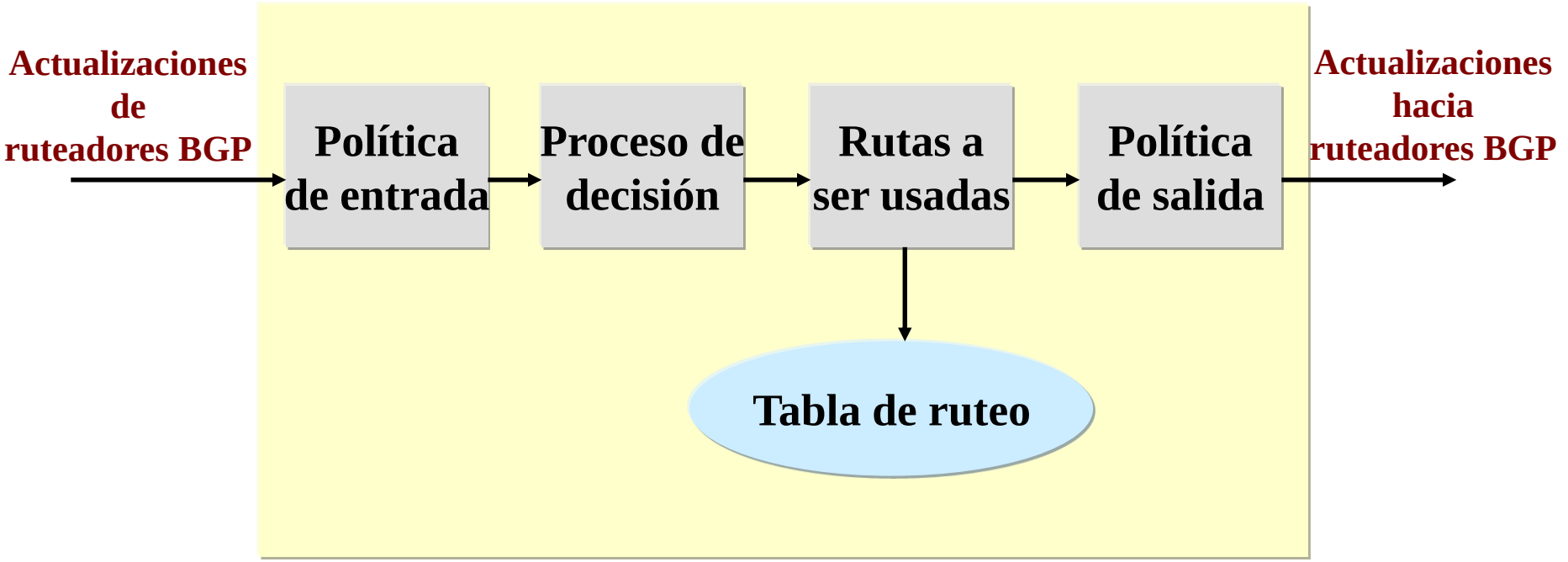
BGP

- Por ejemplo, en función del SA fuente o de la composición del AS_PATH, la configuración manual puede:
  - autorizar o no un anuncio
  - asignar diferente preferencia a diferentes anuncios

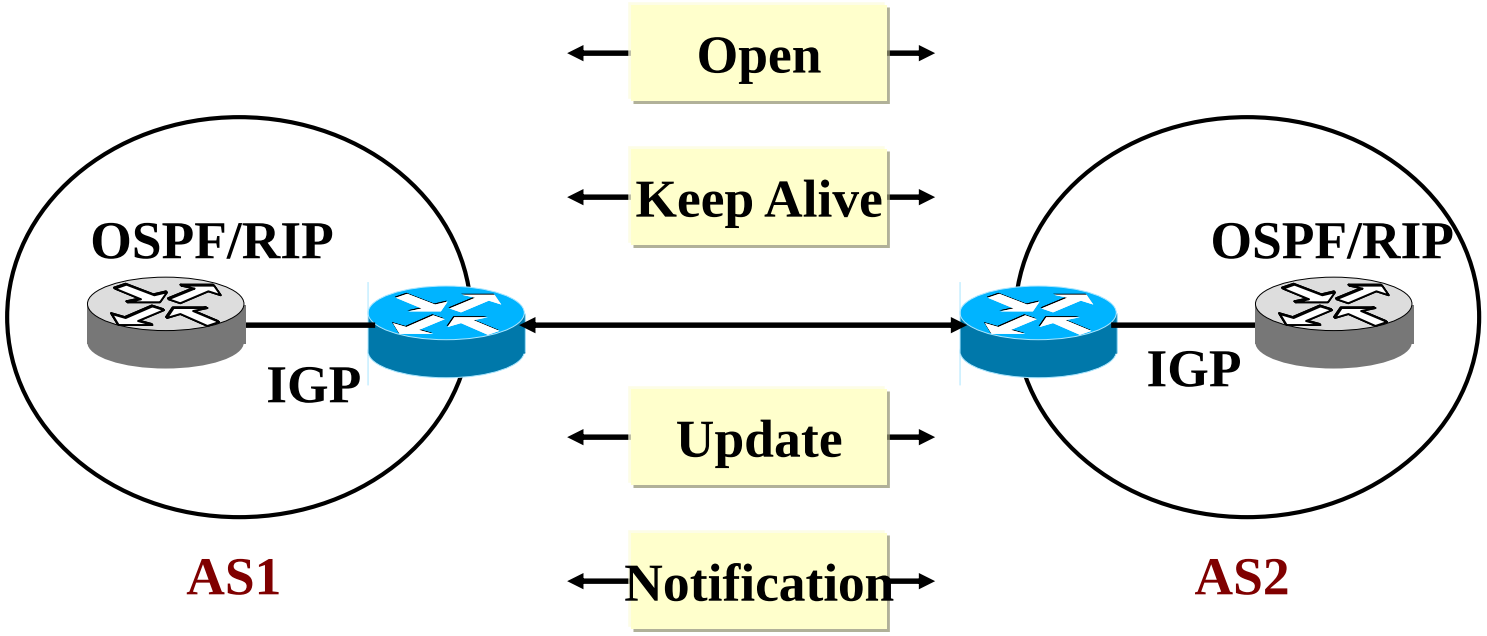
Componentes de BGP



Procesos de BGP y políticas de ruteo



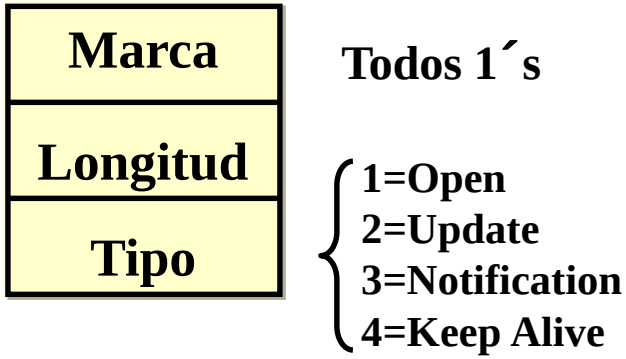
Protocolo BGP



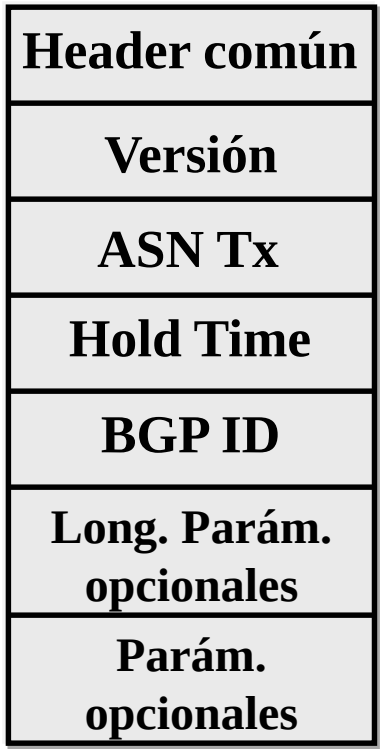
- Protocolo TCP en el puerto 179
  - (1) Apertura y confirmación; (2) Mantenimiento de la conexión; (3) Envío de información de rutas alcanzables; (4) Notificación de errores

Mensajes BGP (*open*)

Encabezado de mensaje BGP

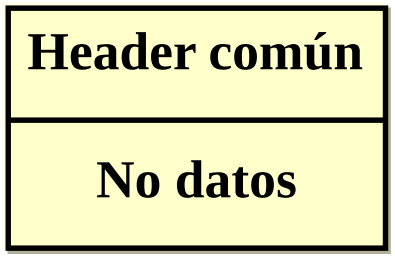


Mensaje Open BGP



Mensajes BGP (*keepalive* y *update*)

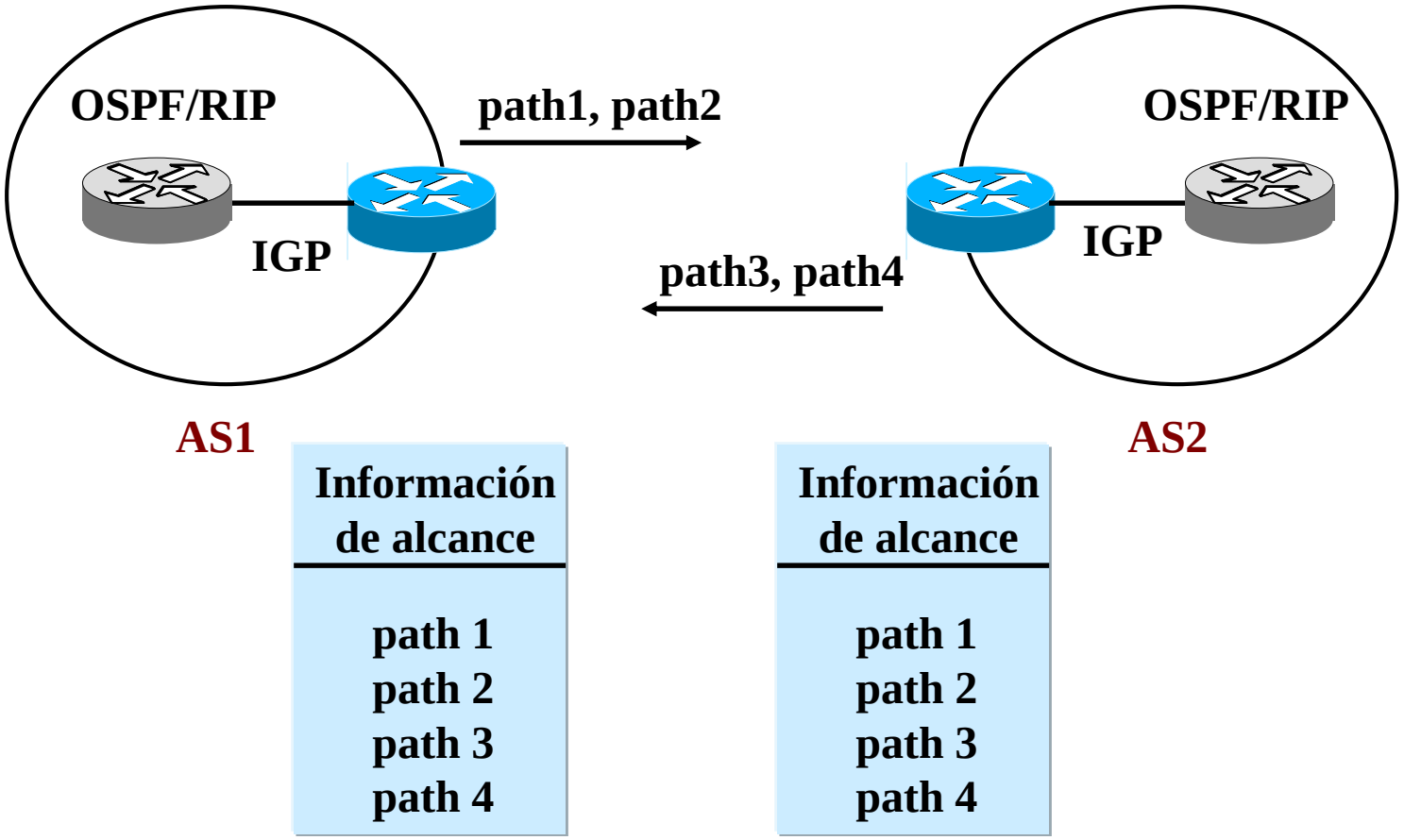
Mensaje de Keepalive BGP



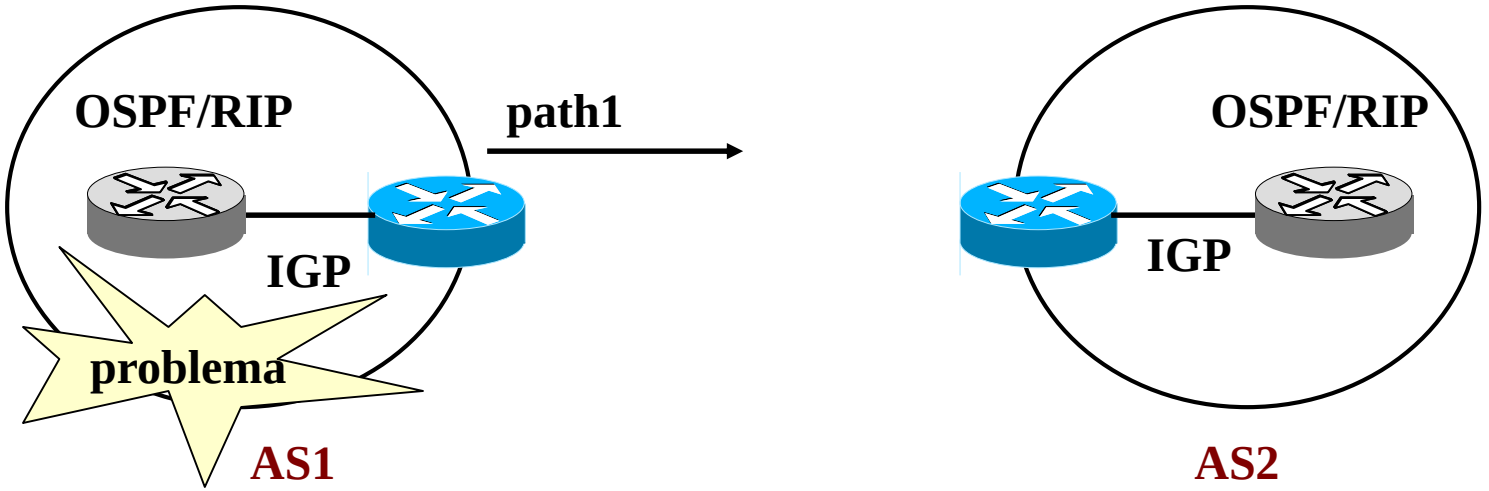
Mensaje de actualización BGP

NLRI: Network layer reachability information. Rutas alcanzables

Intercambio de NLRI



Intercambio de rutas retiradas



Información disponibilidad
path 2
path 3
path 4

Información disponibilidad
path 2
path 3
path 4