



TEMA 5: Capa de Red



UNIVERSITAT POLITÈCNICA DE VALÈNCIA
Escola Politècnica Superior de Gandia



Polimedias recomendados

- La cabecera de los paquetes IPv4

<https://youtu.be/NBKGQLErm2w>

- Tablas de Encaminamiento IP

https://youtu.be/gyRXRI_3gJ4



Tema 5: Secciones y objetivos

5.1 Protocolos de capa de red

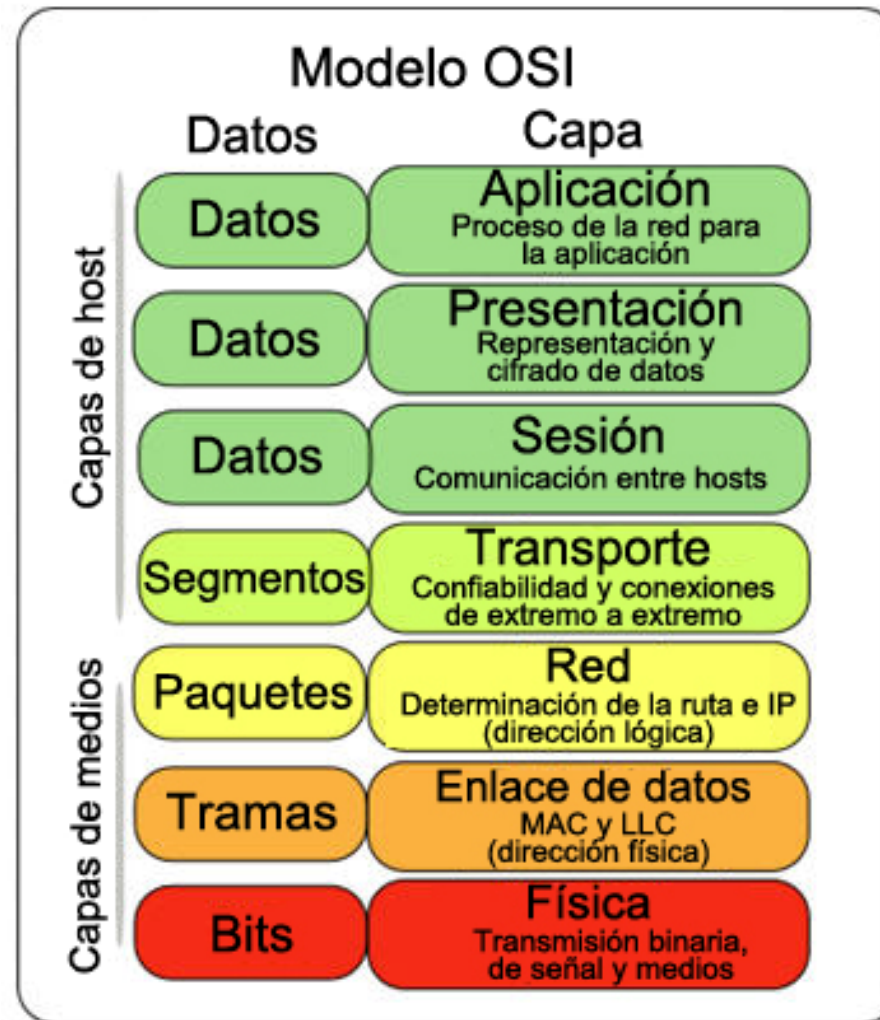
- Describir el propósito de la capa de red en la comunicación de datos.
- Explicar por qué el protocolo IPv4 requiere otras capas para proporcionar confiabilidad.
- Explicar la función de los principales campos de encabezado en los paquetes IPv4 e IPv6.

5.2 Enrutamiento

- Explicar la forma en que un dispositivo host utiliza las tablas de enrutamiento para dirigir paquetes a sí mismo, a un destino local o a un gateway predeterminado.
- Comparar una tabla de enrutamiento de un host con una tabla de enrutamiento de un router.

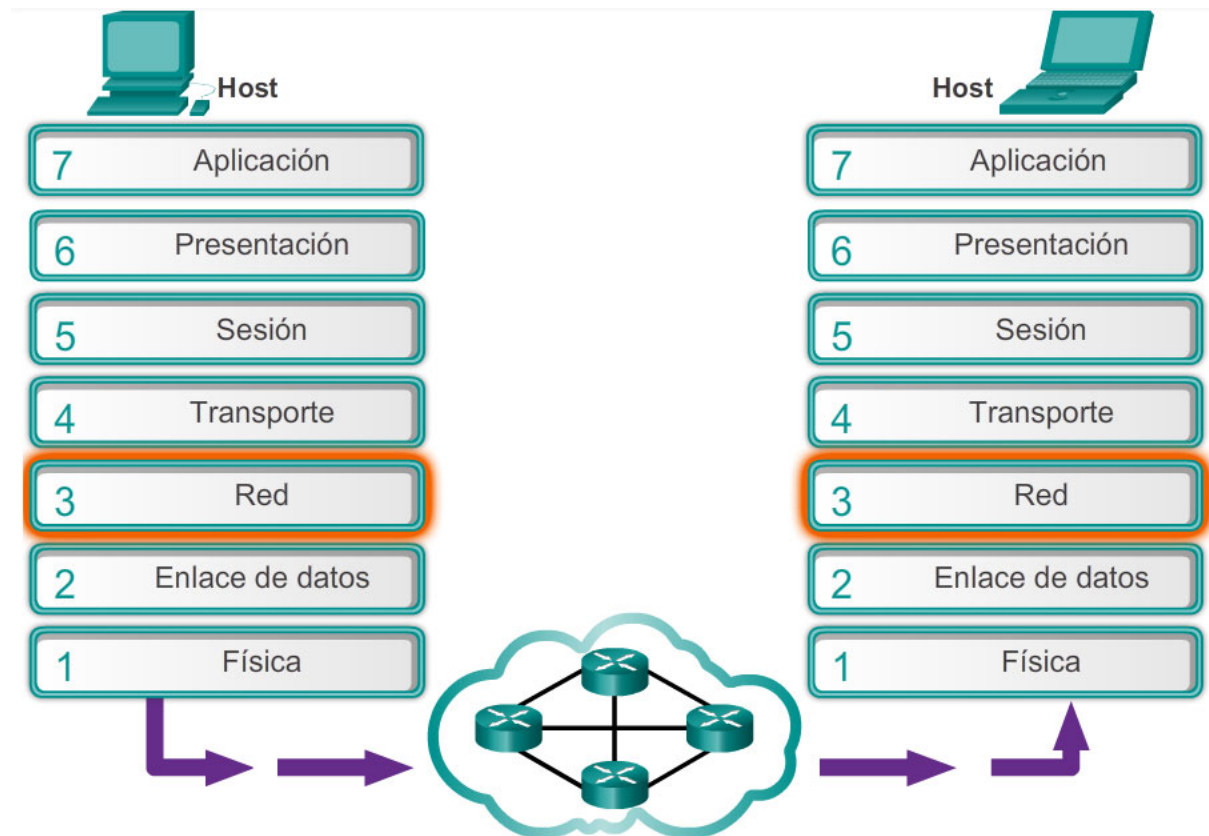
Capa de red

Capa de red



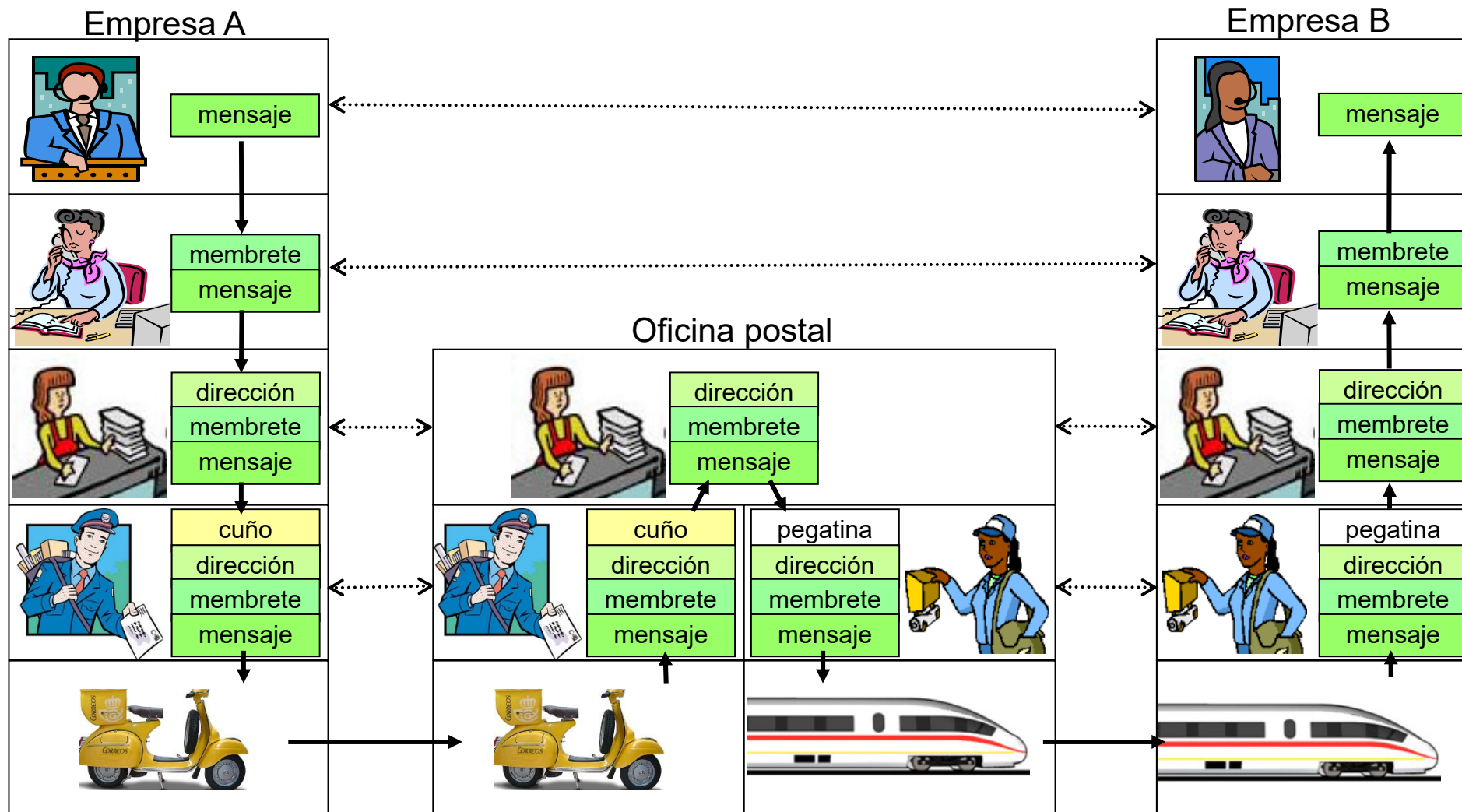
Protocolos de capa de red

La capa de red en la comunicación



Los protocolos de capa de red reenvían las PDU de la capa de transporte entre hosts.

Símil de las empresas





La capa de red en la comunicación

La capa de red

Función básica de la capa de red:

- Permitir el intercambio de paquetes a través de la red entre dos dispositivos finales

Tareas a resolver:

- Direccionamiento de dispositivos finales*
- Encapsulación en paquetes*
- Enrutamiento

*También en otras capas



La capa de red en la comunicación

La capa de red

- **Direccionamiento de terminales:** Los terminales se deben configurar con una **dirección IP** única para identificarlos en la red.
- **Encapsulamiento:** La capa de red encapsula segmentos o datagramas de la capa de transporte a un **paquete**. El proceso de encapsulamiento agrega información de encabezado IP, como la dirección IP de los hosts de origen y de destino.
- **Enrutamiento:** La capa de red permite dirigir paquetes a un host de destino en otra red. Para transferir un paquete a otras redes, debe procesarlo un **router**. La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina **"enrutamiento"**. Un paquete puede cruzar muchos dispositivos intermediarios antes de llegar al host de destino. Se denomina "salto" a cada router que cruza un paquete antes de alcanzar el host de destino.
- **Desencapsulamiento:** Cuando el paquete llega a la capa de red del host de destino, el host revisa el encabezado IP del paquete. Si la dirección IP de destino coincide con su propia dirección IP, se elimina el encabezado IP del paquete y se obtiene se transfiere al servicio apropiado (TCP o UDP) en la capa de transporte.



La capa de red en la comunicación

Protocolos de la capa de red

Protocolos de capa de red actuales:

- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)

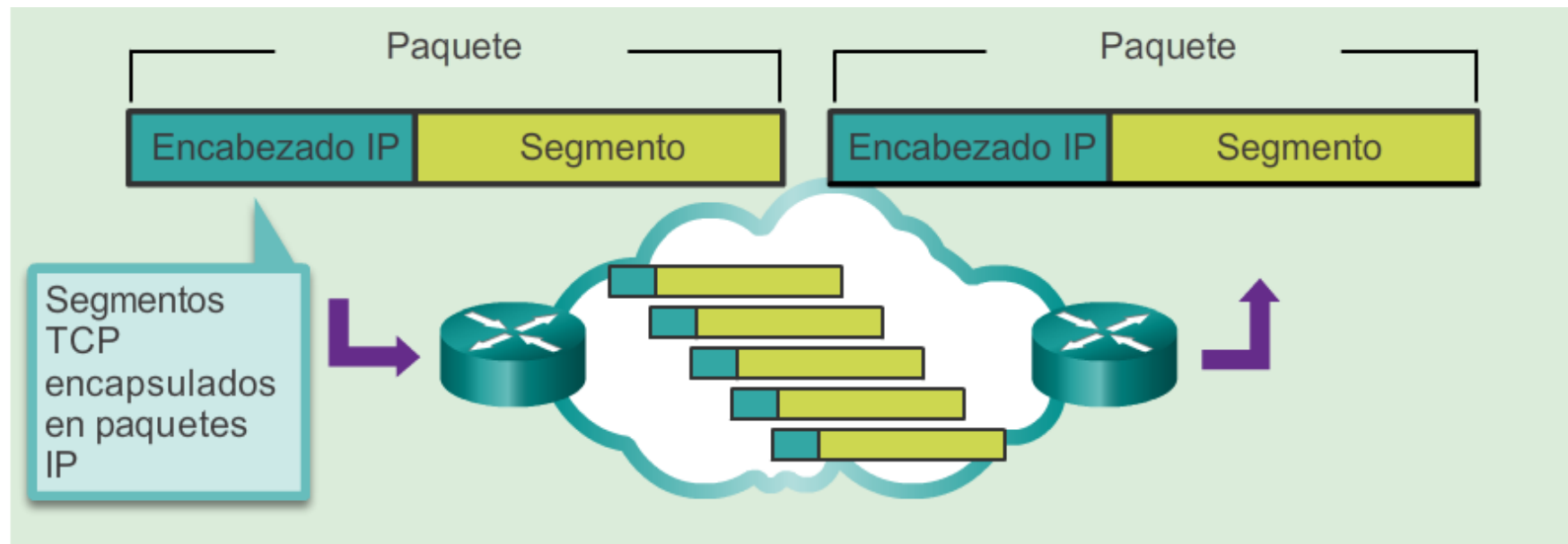
Protocolos de capa de red antiguos:

- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

Características del protocolo IP

Características de IP

- Sin conexión
- No confiable (poca sobrecarga)
- Independiente de los medios



Características del protocolo IP

IP: Sin conexión



Se envía una carta.

El emisor no sabe:

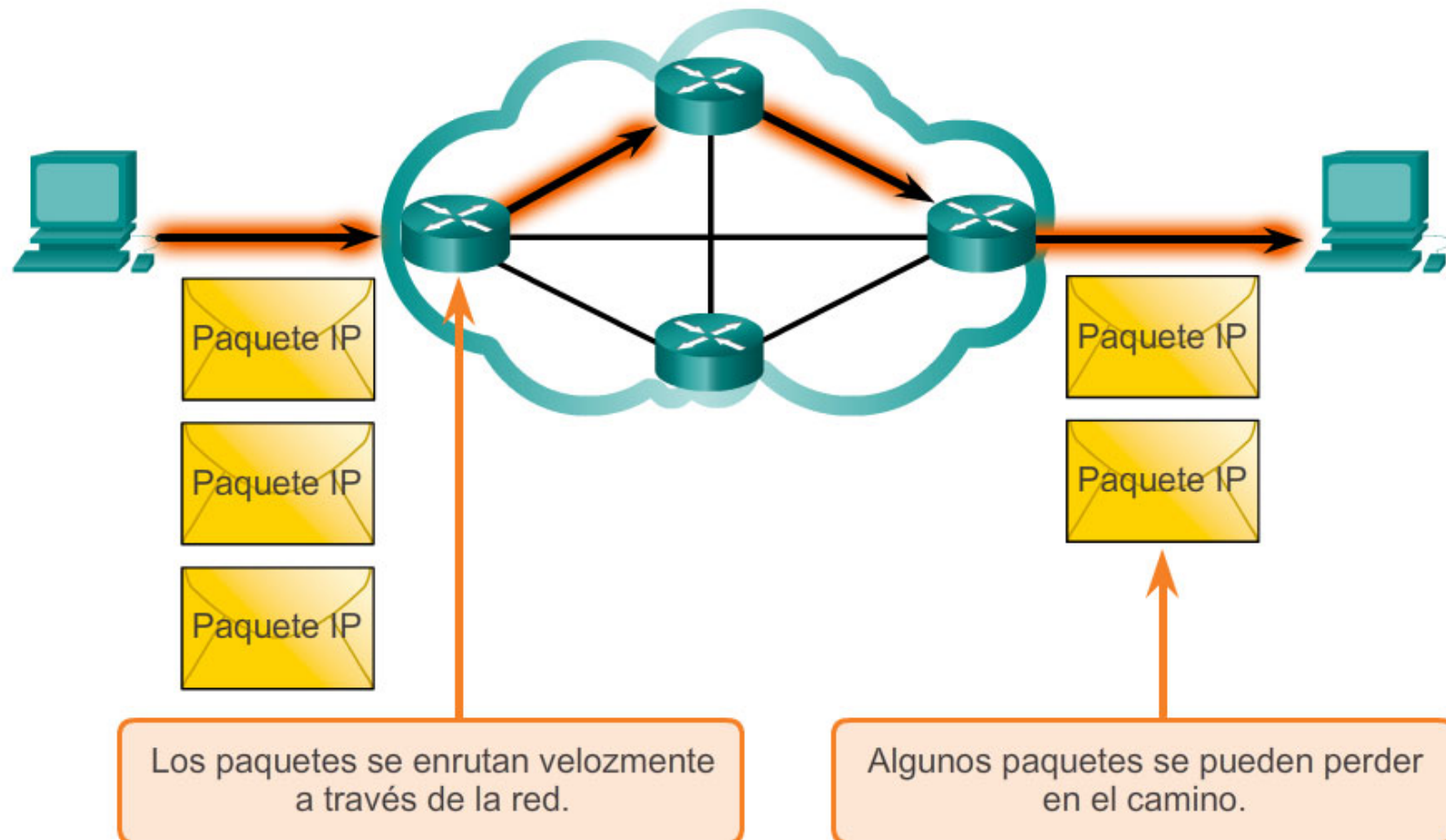
- Si el receptor está presente
- Si la carta llegó
- Si el receptor puede leer la carta

El receptor no sabe:

- Cuándo llegará

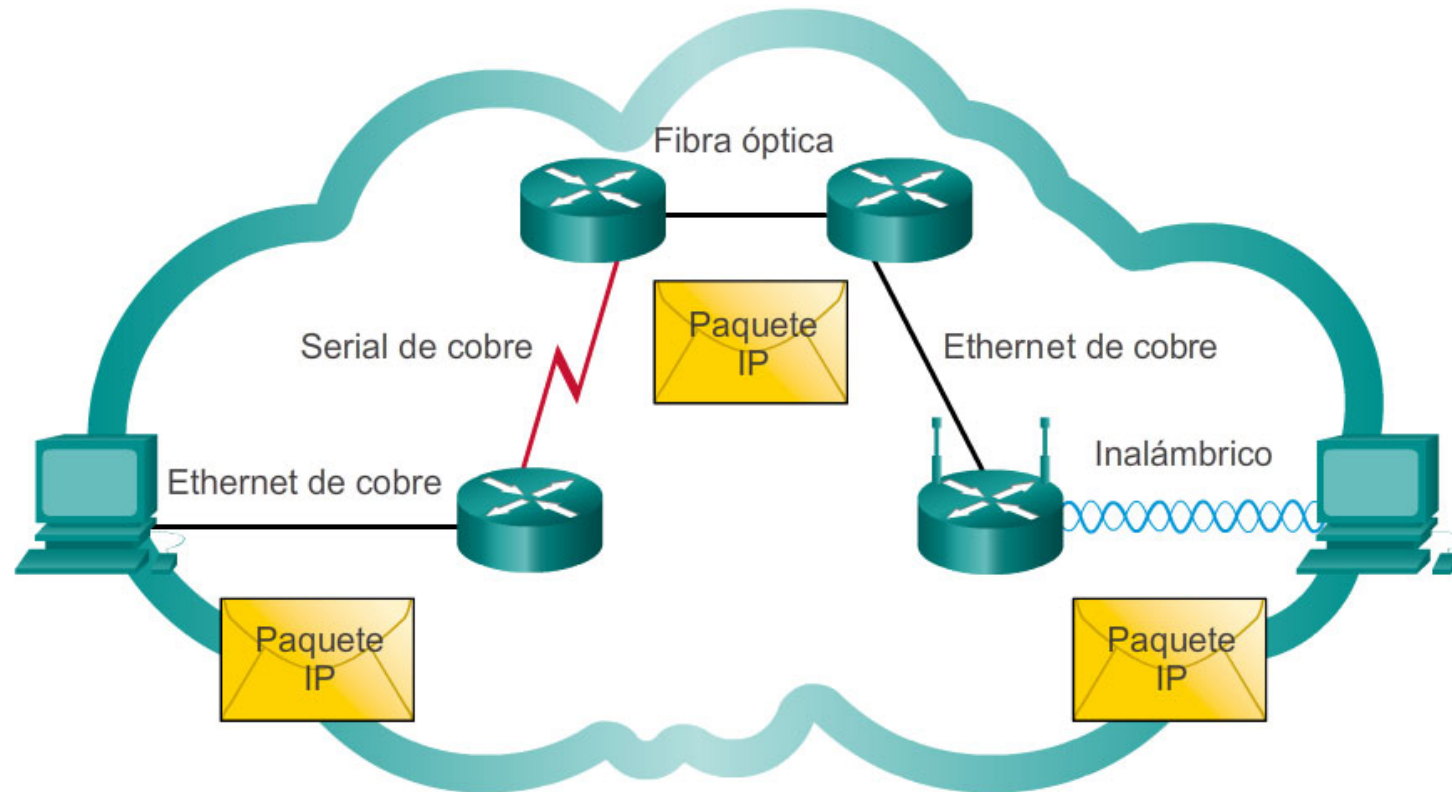
Características del protocolo IP

IP: No confiable (poca sobrecarga)



Características del protocolo IP

IP: Independiente de los medios





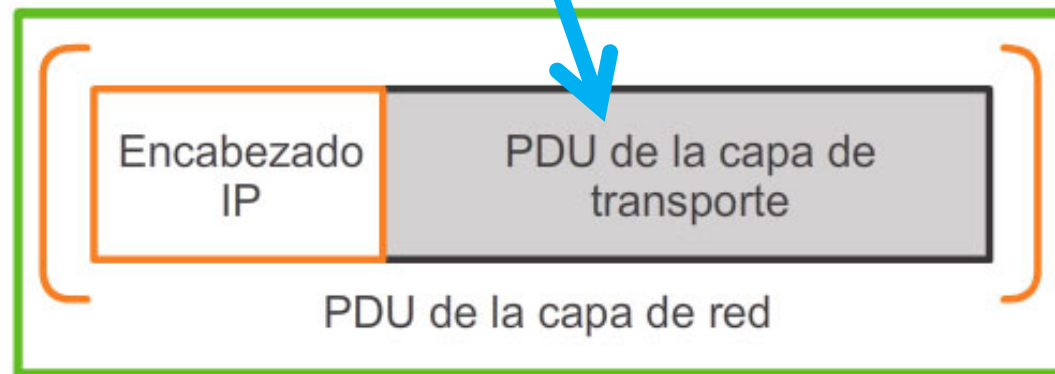
Paquetes IPv4

Encapsulación de IP

Encapsulación de la capa de transporte



Encapsulación de la capa de red

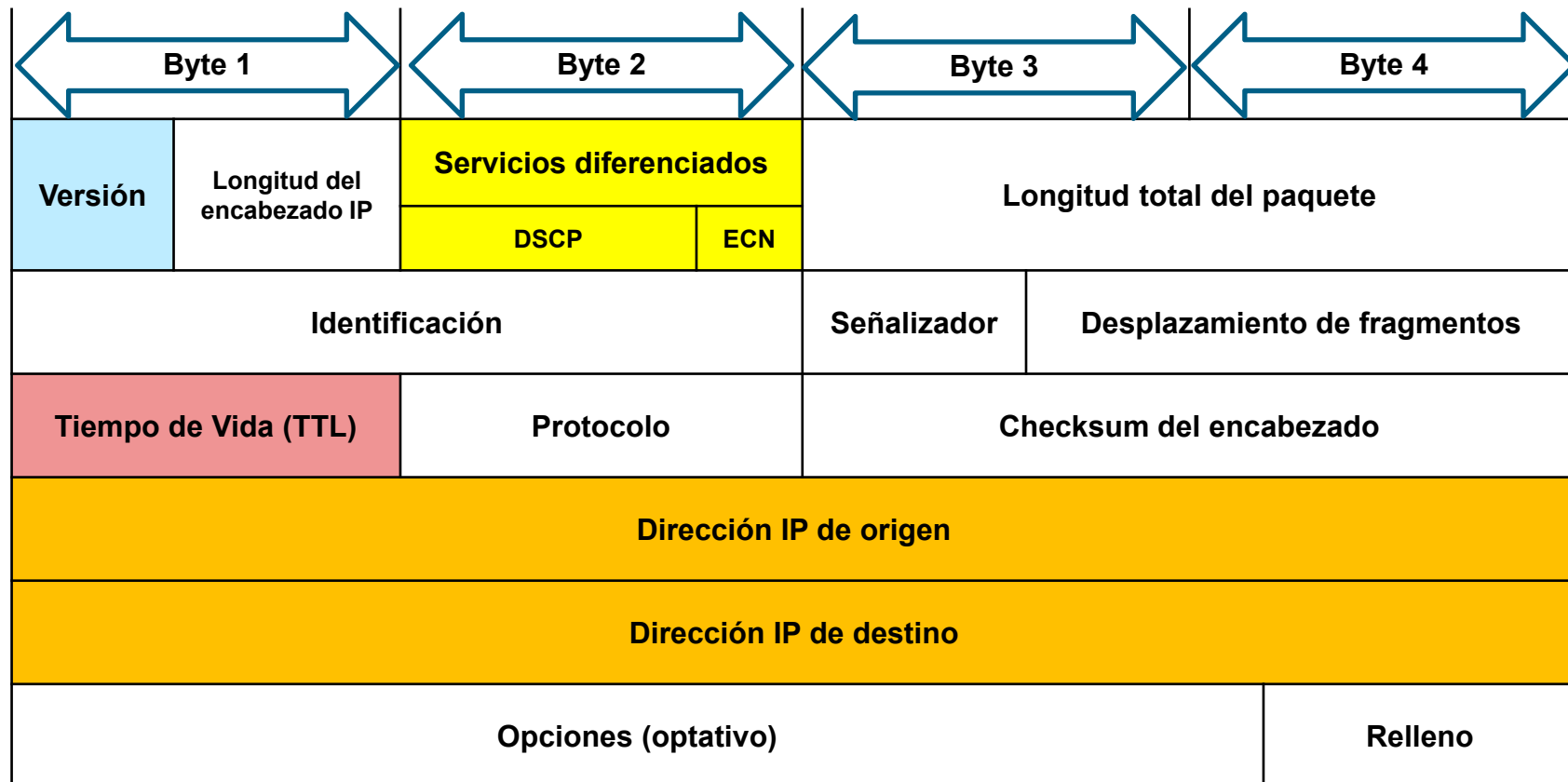


Paquete IP



Paquete IPV4

Encabezado de paquetes IPv4





Paquetes IPv4

Campos del encabezado de IPv4

- Versión (4 bits)
Número de la versión IP (**0100** para IP v4)
- Longitud del encabezado - IHL (4 bits)
Tamaño del encabezado del paquete (en general **20 bytes**, pero, si hay opciones, serán más)
- Tipo de servicio o servicios diferenciados (8 bits)
Prioridad del paquete. Mecanismo de Calidad del Servicio (QoS)
- **Longitud del paquete** (16 bits)
Tamaño en bytes del paquete, incluidos el encabezado + datos
- Identificación (16 bits)
Identifica el paquete IP original para poder unir los fragmentos
- Desplazamiento de fragmentos y señalizadores de frag. (16 bits)
A veces un router tiene que fragmentar un paquete cuando lo pasa a una red con tamaño de paquete menor



Paquetes IPv4

Campos del encabezado de IPv4

- **Tiempo de vida – TTL (Time To Live) (8 bits)**

Resto de vida que le queda al paquete. Se resta uno cada vez que el paquete pasa por un router. Cuando llega a cero, el router descarta el paquete. Es una protección frente a errores de enrutamiento

- **Protocolo (8 bits)**

Tipo de contenido que el paquete traslada para pasárselo al protocolo adecuado. (01-ICMP, 06-TCP, 17-UDP)

- **Checksum del encabezado (16 bits)**

Para controlar errores del encabezado del paquete. No resulta muy necesario hoy en día

- **Dirección origen (32 bits)**

- **Dirección destino (32 bits)**

- **Opciones y relleno:**

Rara vez utilizados (en este caso, serían más de 20 bytes de encabezado)



Paquetes IPv4

Identificación de paquetes y fragmentación

- Puede haber redes que admitan tamaños de paquetes más grandes y otras que admitan más pequeños

Ej: Ethernet admite tamaño máximo de 1500 bytes, y es un valor que actualmente se ha estandarizado
- Si llega un paquete demasiado grande para una red, hay que fragmentarlo
- Cada fragmento mantiene el mismo identificador de paquete, pero cambia el offset (desplazamiento)

El primer fragmento tiene offset 0

El segundo, tiene como offset el tamaño del primer fragmento,...
- El señalizador de fragmento indica si ese era el último fragmento



Paquetes IPv4

Encabezados de IPv4 de muestra

Microsoft: \Device\NPF_{7BB3C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	3.64050300	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128
17	3.64506800	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64
18	3.68215500	192.168.1.109	38.112.107.53	TCP	54	55502 > https [ACK] Seq=1 Ack=134 win=16661 Len=0
19	4.19945400	fe80::15ff:98d8:d28ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
20	4.60748800	fe80::15ff:98d8:d28ff02::c	fe80::b1ee:c4ae:a11	SSDP	453	HTTP/1.1 200 OK
21	4.64229900	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128
22	4.64509200	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64
23	4.73605200	192.168.1.109	255.255.255.255	DB-LSP	154	Dropbox LAN svnc Discovery Protocol

Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li_a0:d1:be (00:18:39:a0:d1:be)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 60
- Identification: 0x3704 (14084)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0x7ffe [correct]
- Source: 192.168.1.109 (192.168.1.109)
- Destination: 192.168.1.1 (192.168.1.1)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

Internet Control Message Protocol

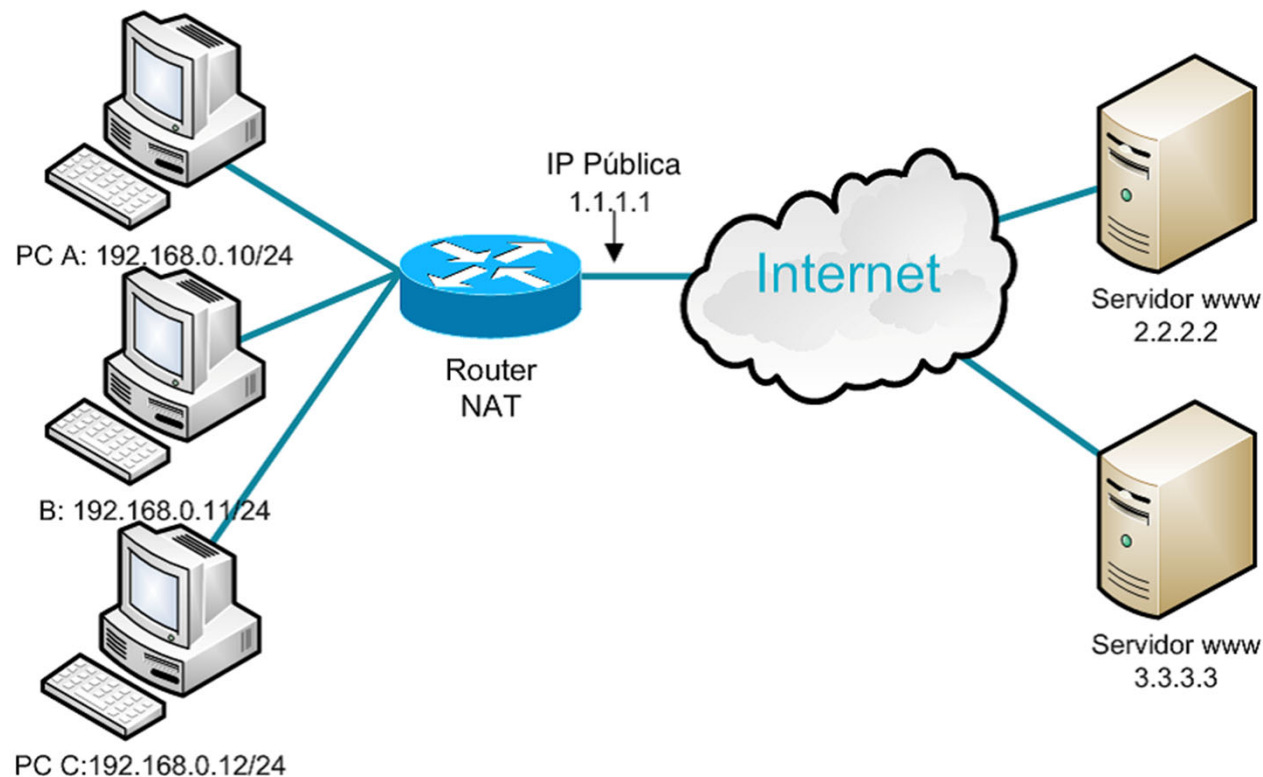
0000 00 18 39 a0 d1 be 24 77 03 45 5d c4 08 00 45 00 ..9...\$w .E]...E.
0010 00 3c 37 04 00 00 80 01 7f fe c0 a8 01 6d c0 a8 .<7.....m..
0020 01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66 ...MV..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Internet Protocol Version 4 (ip), 20 bytes Packets: 35 Displayed: 35 Marked: 0 Dropped: 0 Profile: Default

La capa de red en la comunicación

Limitaciones de IPv4

- Agotamiento de direcciones IP
- Las tablas de enrutamiento en IPv4 son complejas
- Varios ordenadores han de compartir la misma IP pública (uso de **NAT** en el gateway: **N**etwork **A**ddress **T**ranslation)





La capa de red en la comunicación

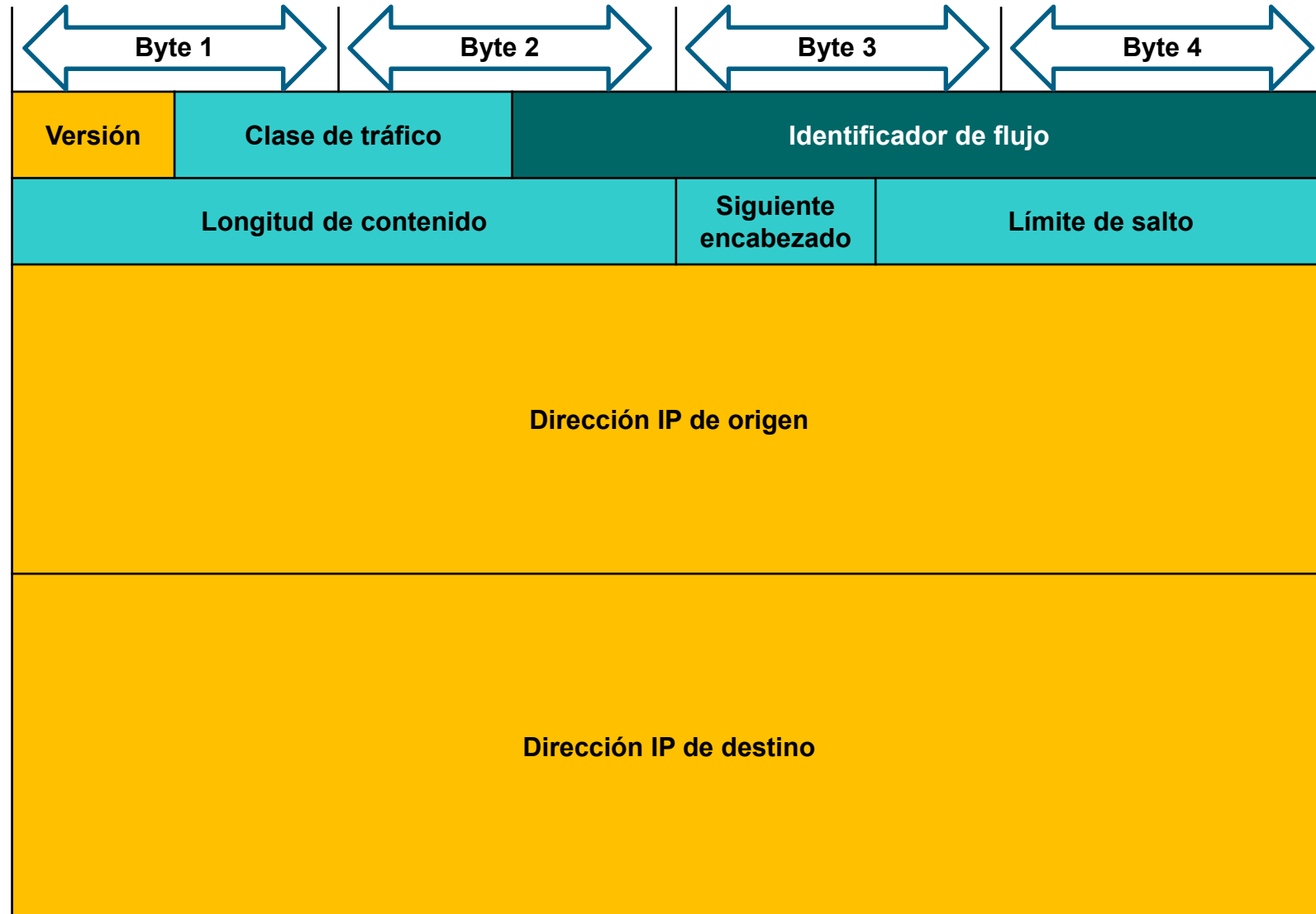
Introducción a IPv6

- Mayor espacio de direcciones
 - Mejor manejo de paquetes (menos campos)
 - Elimina la necesidad de NAT (compartir IP)
 - Nuevo campo de identificador de flujo
-
- 4000 millones de direcciones IPv4 (32 bits): $2^{32} = 4.000.000.000$
 - 340 sextillones de direcciones IPv6 (128 bits): $2^{128} = 340.000.000.000.000.000.000.000.000.000.000.000.000.000$



Paquetes IPv6

Encabezado de paquetes IPv6





Paquetes IPv6

Encabezado de paquetes IPv6

- **Versión:** (4 bits = **0110**).
- **Clase de tráfico:** (8 bits)
Prioridad del paquete. Notificación de congestión
- **Identificador de flujo:** (20 bits)
En aplicaciones en tiempo real (*streaming*, por ejemplo) para indicar al router que todos los paquetes sigan el mismo camino <<Nuevo>>
- **Longitud de contenido:** (16 bits)
Tamaño en bytes del contenido, solamente
- **Siguiente encabezado:** (8 bits)
Tipo de contenido del paquete (01-ICMP, 06-TCP, 17-UDP)
- **Límite de saltos** (8 bits)
Equivalente a TTL en IPv4
- **Dirección origen** (128 bits)
- **Dirección destino** (128 bits)




Paquetes IPv6

Encapsulación de IPv6

Encabezado de IPv4

Versión	IHL	Tipo de servicio	Longitud total	
Identificación			Señaladores	Desplazamiento de fragmentos
Tiempo de duración	Protocolo		Checksum del encabezado	
Dirección de origen				
Dirección de destino				
Opciones				Relleno




Leyenda

-  - Se conservan los nombres de campo de IPv4 a IPv6
-  - Cambian el nombre y la posición en IPv6
-  - No se conservan los campos en IPv6

Encabezado de IPv6

Versión	Clase de tráfico	Etiqueta de flujo	
Longitud de contenido		Encabezado siguiente	Límite de saltos
Dirección IP de origen			
Dirección IP de destino			

Leyenda

-  - Se conservan los nombres de campo de IPv4 a IPv6
-  - Cambian el nombre y la posición en IPv6
-  - Nuevo campo en IPv6

Longitud: 20-60 bytes

Longitud: 40 bytes



Paquetes IPv6

Encabezados de IPv6 de muestra

Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8) interface showing a packet capture of an IPv6 HTTP transaction.

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
47	325.030878	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:9ff:fee3:e8de	TCP	82	http > 59201 [SYN, ACK] Seq=0 Ack=1 win=6
48	325.031166	2001:6f8:102d:0:2d0:9ff:fee3:e8de	2001:6f8:900:7c0::2	TCP	74	59201 > http [ACK] Seq=1 Ack=1 win=5760 L
49	325.040411	2001:6f8:102d:0:2d0:9ff:fee3:e8de	2001:6f8:900:7c0::2	HTTP	314	GET / HTTP/1.0
50	325.045496	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:9ff:fee3:e8de	TCP	1506	[TCP segment of a reassembled PDU]
51	325.045525	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:9ff:fee3:e8de	HTTP	901	HTTP/1.1 200 OK (text/html)
52	325.045627	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:9ff:fee3:e8de	TCP	74	http > 59201 [FIN, ACK] Seq=2260 Ack=241

Frame 49: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)

- Ethernet II, Src: HsingTec_e3:e8:de (00:d0:09:e3:e8:de), Dst: Ibm_82:95:b5 (00:11:25:82:95:b5)
- Internet Protocol Version 6, Src: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de), Dst: 2001:6f8:900:7c0::2 (2001:6f8:900:7c0::2)
 - 0110 = Version: 6
 - 0000 0000 = Traffic class: 0x00000000
 - 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
 - Payload length: 260
 - Next header: TCP (6)
 - Hop limit: 64
 - Source: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de)
 - [Source SA MAC: HsingTec_e3:e8:de (00:d0:09:e3:e8:de)]
 - Destination: 2001:6f8:900:7c0::2 (2001:6f8:900:7c0::2)
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 59201 (59201), Dst Port: http (80), Seq: 1, Ack: 1, Len: 240
- Hypertext Transfer Protocol

Packet bytes:

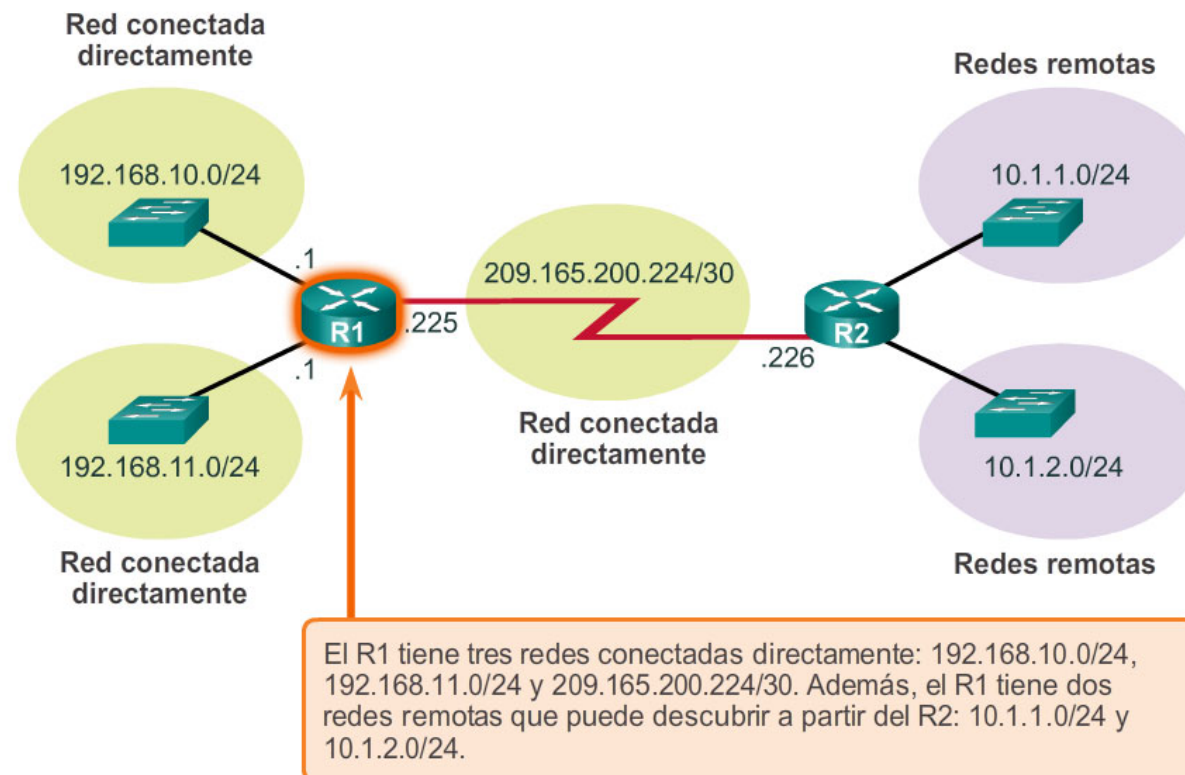
Offset	Hex	ASCII
0000	00 11 25 82 95 b5 00 d0 09 e3 e8 de 86 dd 60 00	...%.....
0010	00 00 01 04 06 40 20 01 06 f8 10 2d 00 00 02 d0@.....
0020	09 ff fe e3 e8 de 20 01 06 f8 09 00 07 c0 00 00A.P...a.J
0030	00 00 00 00 00 02 e7 41 00 50 ab dc d6 61 01 4a	S.P...H..GET /
0040	73 9f 50 18 16 80 f4 48 00 00 47 45 54 20 2f 20	HTTP/1.0 ..Host:
0050	48 54 54 50 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20	cl-1985. ham-01.d
0060	63 6c 2d 31 39 38 35 2e 68 61 6d 2d 30 31 2e 64	e.sixxs. net..Acc
0070	65 2e 73 69 78 78 73 2e 6e 65 74 0d 0a 41 63 63	

Internet Protocol Version 6 (IPv6), 40 bytes | Packets: 55 Displayed: 55 Mark... | Profile: Default

Enrutamiento

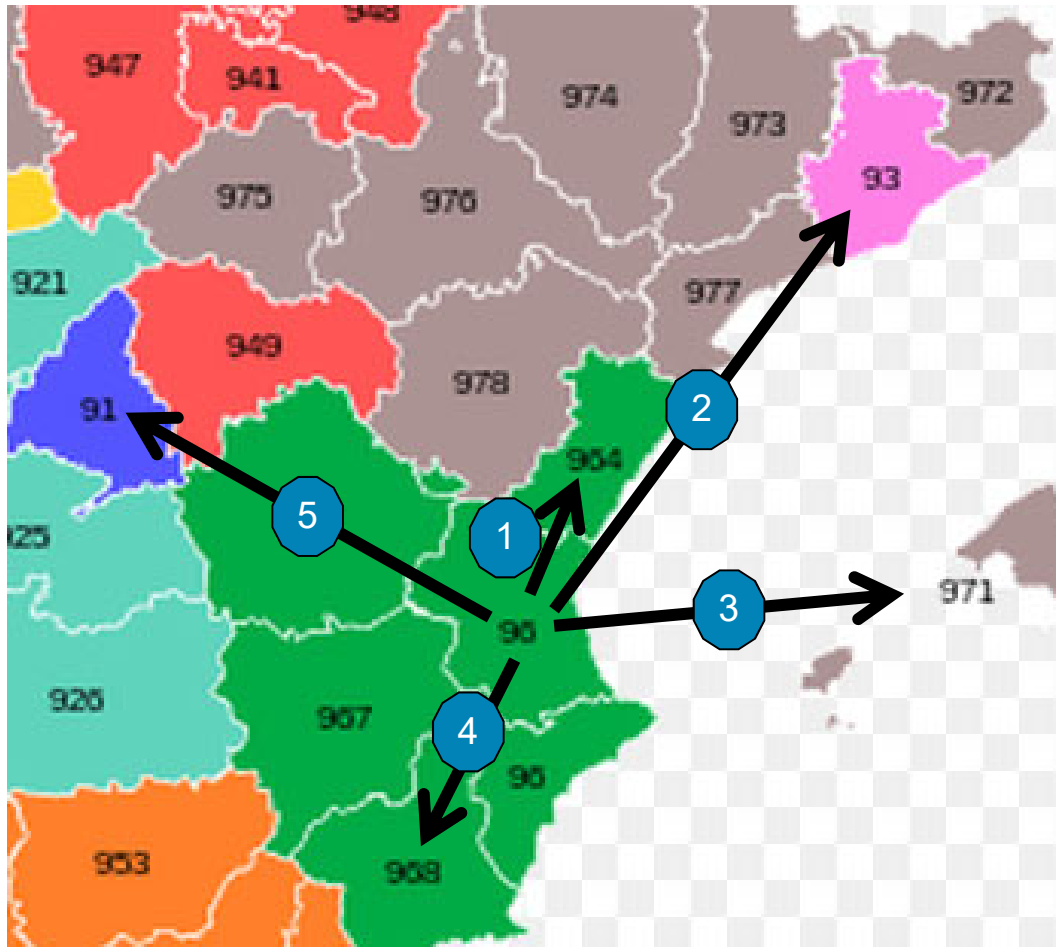
¿Qué es una tabla de enrutamiento?

- Cada vez que llega un paquete a un router, este ha de decidir por dónde retransmitirlo
- Esta tarea se realiza utilizando la tabla de enrutamiento



Enrutamiento

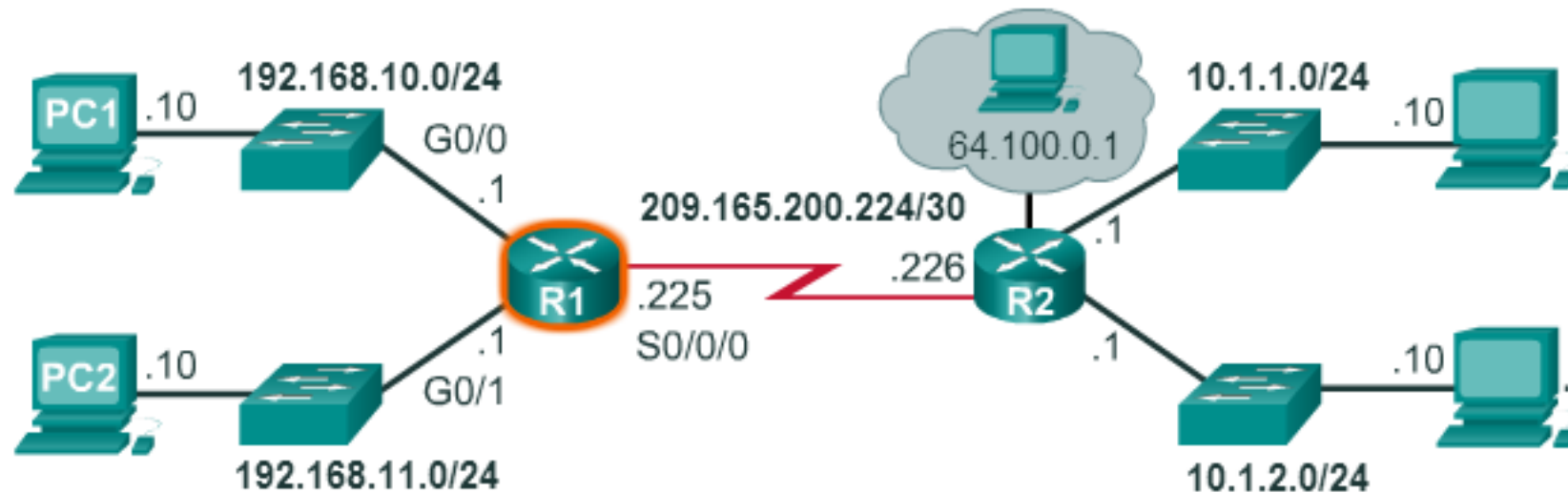
Símil con la (antigua) red telefónica



Prefijo	salida
<u>96</u> 4000000 /3	1
<u>93</u> 0000000 /2	2
<u>97</u> 1000000 /3	3
<u>96</u> 8000000 /3	4
000000000 /0	5

Enrutamiento

¿Qué es una tabla de enrutamiento?



Red destino		salida
192.168.10.0	/24	G0/0
192.168.11.0	/24	G0/1
209.165.200.224	/30	S0/0/0
10.1.1.0	/24	209.165.200.226
10.1.2.0	/24	209.165.200.226
0.0.0.0	/0	209.165.200.226

Redes directamente conectadas

Redes remotas

Ruta de salida por defecto



Enrutamiento

Proceso para crear una tabla de enrutamiento

- Paso 1: identificar las redes directamente conectadas a cada uno de los interfaces del router (siempre habrá dos o más)
- Paso 2: poner línea a línea cada una de las redes anteriores, indicando como salida el interfaz correspondiente (el nombre, no la IP)
- Paso 3: identificar las redes remotas (no conectadas directamente a ninguno de los interfaces del router)
- Paso 4: poner línea a línea cada una de las redes anteriores, indicando como salida la IP del siguiente salto (ha de ser una IP perteneciente a alguna de las redes directamente conectadas y que actuará como pasarela al resto de la red)
- Paso 5: poner 0.0.0.0/0 (es decir, resto de IPs) indicando como salida la ruta por defecto (esta también deberá ser una IP perteneciente a alguna de las redes directamente conectadas y que actuará como pasarela al resto de Internet)



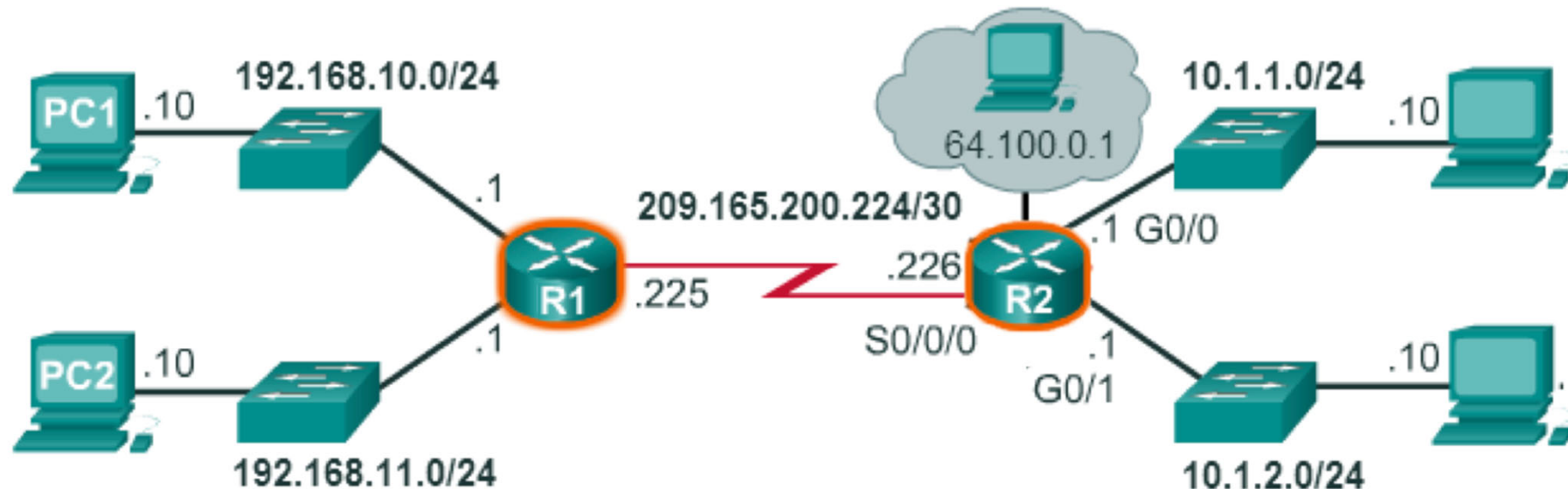
Ejercicio: tabla de enrutamiento R2



1. Enumera redes conectadas a R2
2. Indica, como salida, el interfaz
3. Enumera redes remotas
4. Indica ip de siguiente salto
5. Introduce 0.0.0.0 /0
6. Indica ip ruta por defecto

Enrutamiento

Solución: tabla de enrutamiento R2

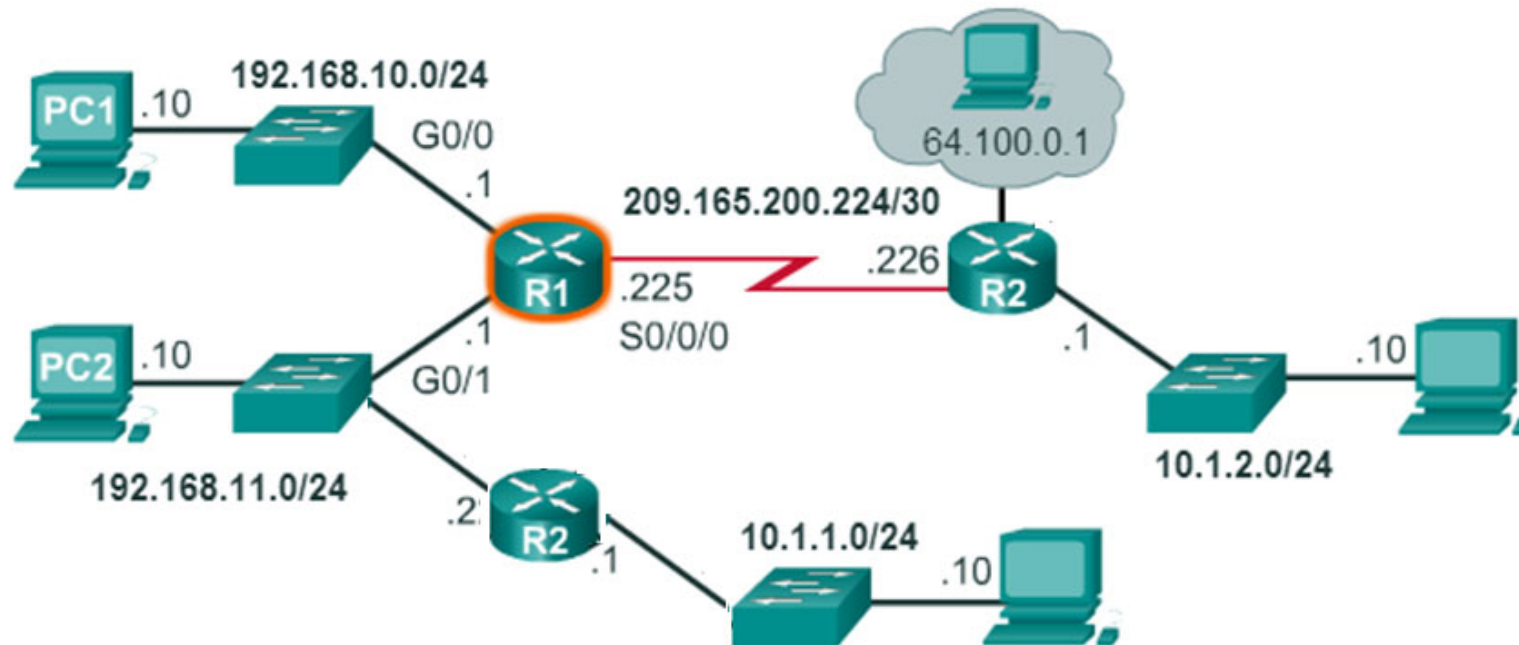


1. Enumera redes conectadas a R2
2. Indica, como salida, el interfaz
3. Enumera redes remotas
4. Indica ip de siguiente salto
5. Introduce 0.0.0.0 /0
6. Indica ip ruta por defecto

Red destino	salida
10.1.1.0/24	G0/0
10.1.2.0/24	G0/1
209.165.200.224/30	S0/0/0
192.168.10.0/24	209.165.200.225
192.168.11.0/24	209.165.200.225
0.0.0.0/0	64.100.0.1

Enrutamiento

Solución: tabla de enrutamiento R1



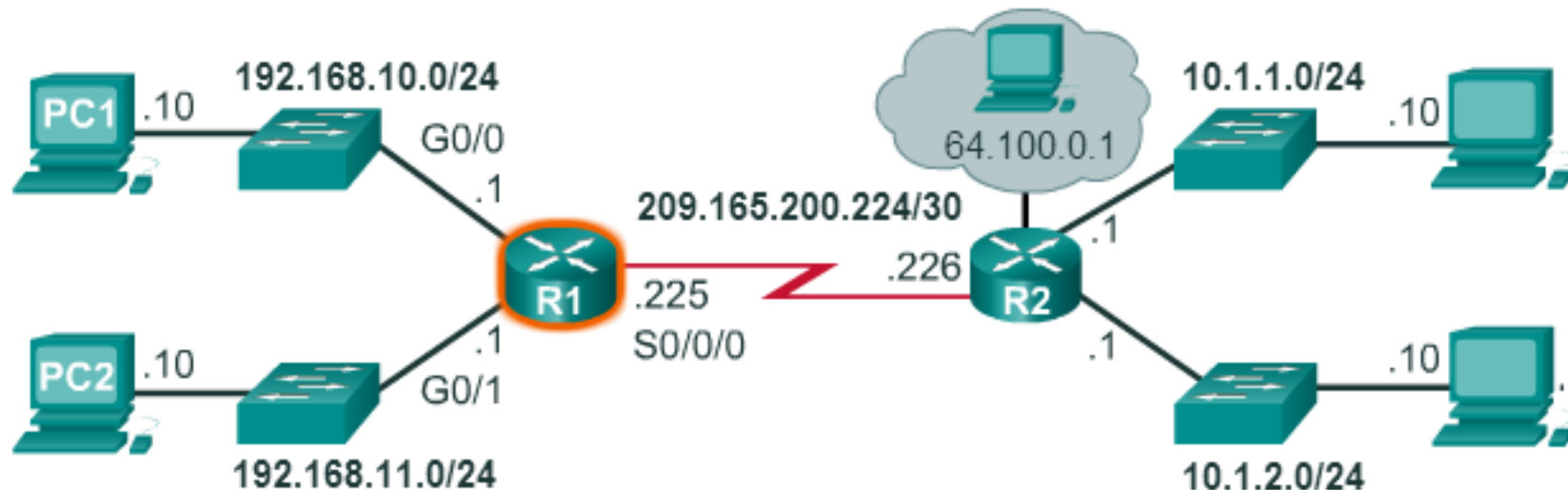
1. Enumera redes directamente conectadas a R1
2. Indica, como salida, el interfaz
3. Enumera redes remotas
4. Indica ip de siguiente salto
5. Introduce 0.0.0.0 /0
6. Indica ip ruta por defecto

Red destino	salida
192.168.10.0/24	G0/0
192.168.11.0/24	G0/1
209.165.200.224/30	S0/0/0
10.1.2.0/24	209.165.200.226
10.1.1.0/24	192.168.11.2
0.0.0.0/0	209.165.200.226 !!!

Enrutamiento

Aprendiendo la tabla de enrutamiento

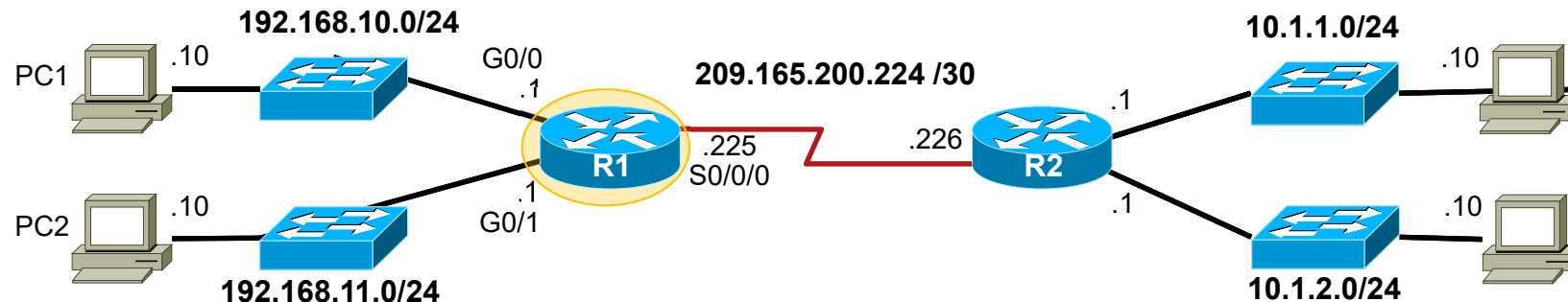
- Enrutamiento estático → las entradas de la tabla de enrutamiento se configuran manualmente
- Protocolo de enrutamiento → los routers comunican a otros routers las redes que pueden alcanzar.
 - Ejemplos: RIP, EIGRP, OSPF,... En esta asignatura no se verán.





Tablas de enrutamiento de router

Tabla de enrutamiento de router IPv4



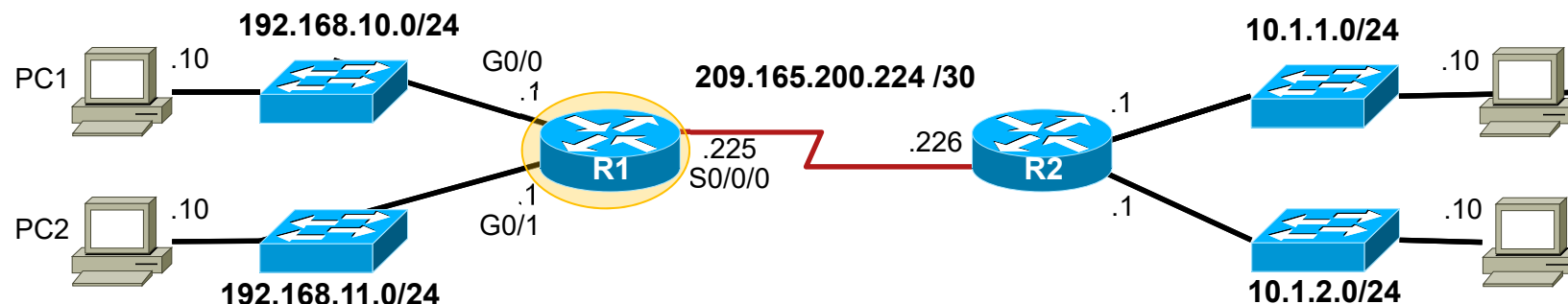
Supongamos que el PC1 con la dirección IP 192.168.10.10 desea enviar un paquete a PC2 con IP 192.168.11.10

Pasos:

1. El PC1 consulta la tabla de rutas IPv4 sobre la base de la dirección IP de destino
2. El PC1 descubre que el PC2 no está en la misma red y simplemente envía el paquete a su gateway predeterminado R1
3. El R1 recibe el paquete en su interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino
4. El R1 consulta la tabla de enrutamiento
5. El R1 busca en esa tabla la entrada que coincide con la dirección IP de destino, y descubre que esta corresponde a su interfaz local G0/1
6. El R1 retransmite el paquete IP por dicha interfaz

Tablas de enrutamiento de router

Tabla de enrutamiento de router IPv4



```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

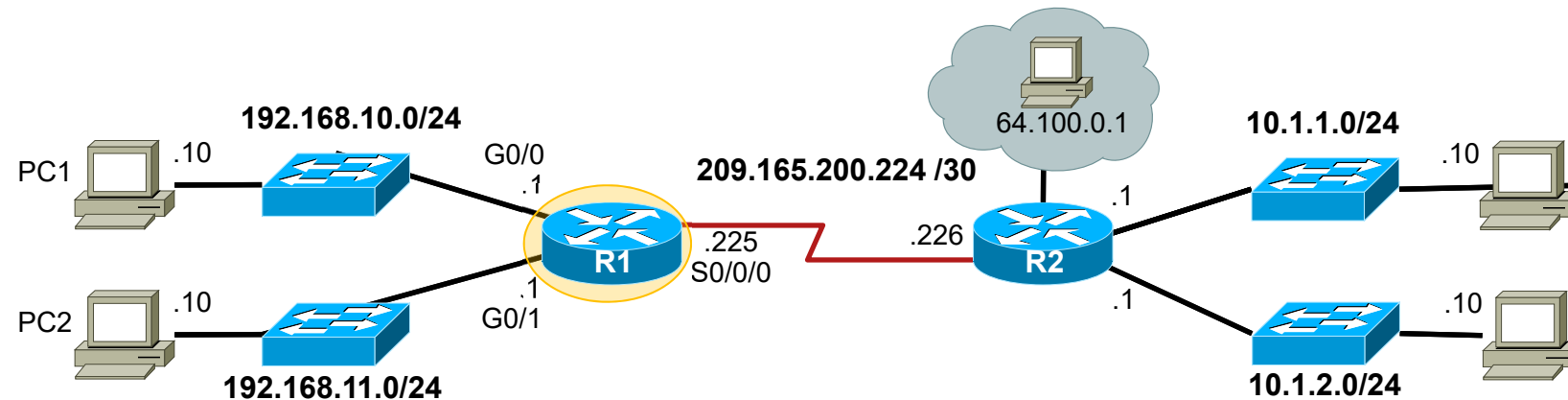
Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
D    10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/1
L    192.168.11.1/32 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C    209.165.200.224/30 is directly connected, Serial0/0/0
L    209.165.200.225/32 is directly connected, Serial0/0/0
```

- La tabla del router también tiene información sobre cómo se obtuvo la ruta, su confianza y su calificación.
- **C**: identifica a una red conectada directamente y creada automáticamente cuando se configura una interfaz y se activa.
- **L**: indica que se trata de una interfaz local. Esta es la propia dirección IPv4 del router en esa red.

Tablas de enrutamiento de router

Entradas de tabla de enrutamiento



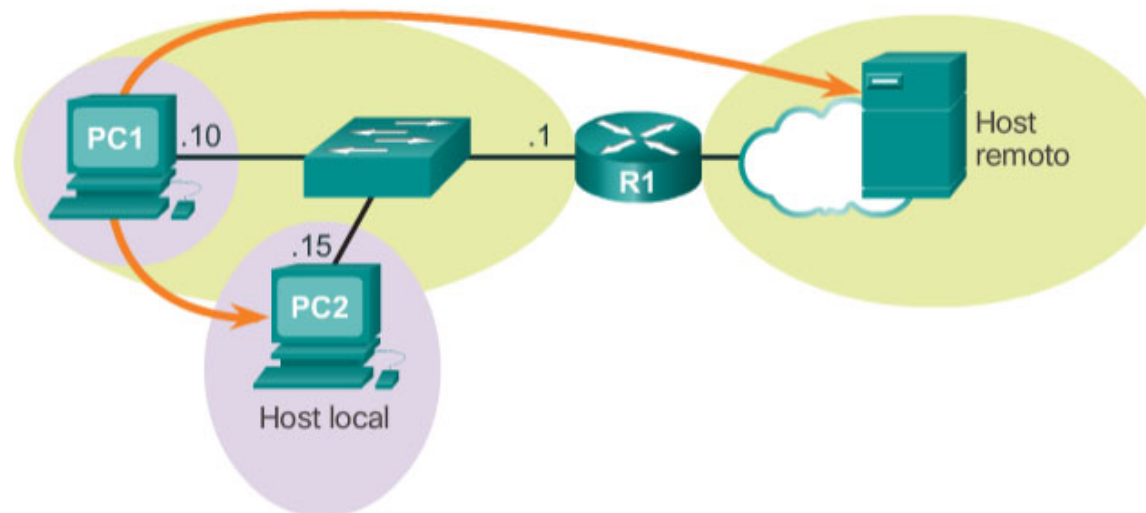
D	10.1.1.0/24	[90/2170112]	via	209.165.200.226,	00:00:05,	Serial10/0/0
---	-------------	--------------	-----	------------------	-----------	--------------

A	Identifica el modo en que el router descubrió la red
B	Identifica la red de destino
C	Identifica la distancia administrativa (confiabilidad) del origen de la ruta
D	Identifica la métrica para llegar a la red remota
E	Identifica la dirección IP del siguiente salto para llegar a la red remota
F	Identifica el tiempo transcurrido desde que se descubrió la red
G	Identifica la interfaz de salida en el router para llegar a la red de destino

Tablas de enrutamiento de host

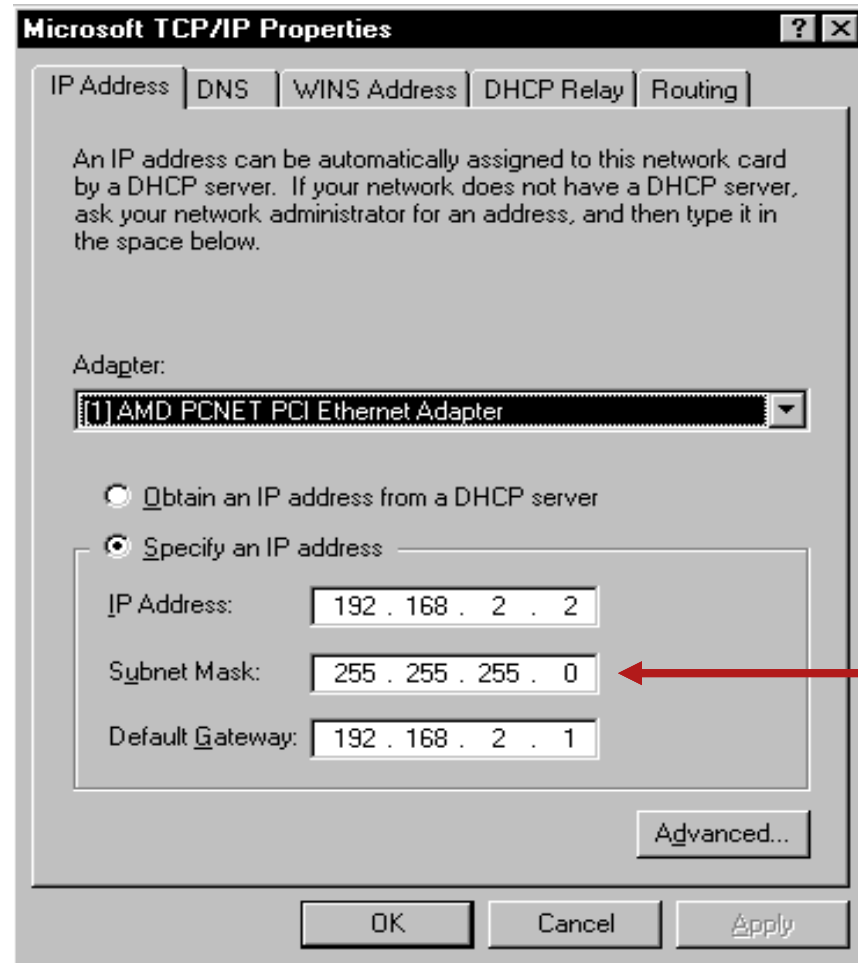
¿Cómo enrutan los hosts?

- Decisión de envío de paquetes en un host:
 - A sí mismo: 127.0.0.1
 - A un host local (de la misma red en la que se encuentra)
 - A un host remoto, a través de un router de su propia red que actuará como *gateway predeterminado*



Gateway predeterminado

- Gateway predeterminado:
 - Los hosts utilizarán el gateway predeterminado para enviar paquetes a redes remotas
 - Enruta el tráfico a otras redes
 - Tiene una dirección IP local en el mismo intervalo de direcciones que el host



Microsoft TCP/IP Properties

IP Address | DNS | WINS Address | DHCP Relay | Routing

An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:
(1) AMD PCNET PCI Ethernet Adapter

☐ Obtain an IP address from a DHCP server

☒ Specify an IP address

IP Address: 192 . 168 . 2 . 2

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 2 . 1

Advanced...

OK Cancel Apply

/24

Configuración del gateway predeterminado

Gateway predeterminado en un host

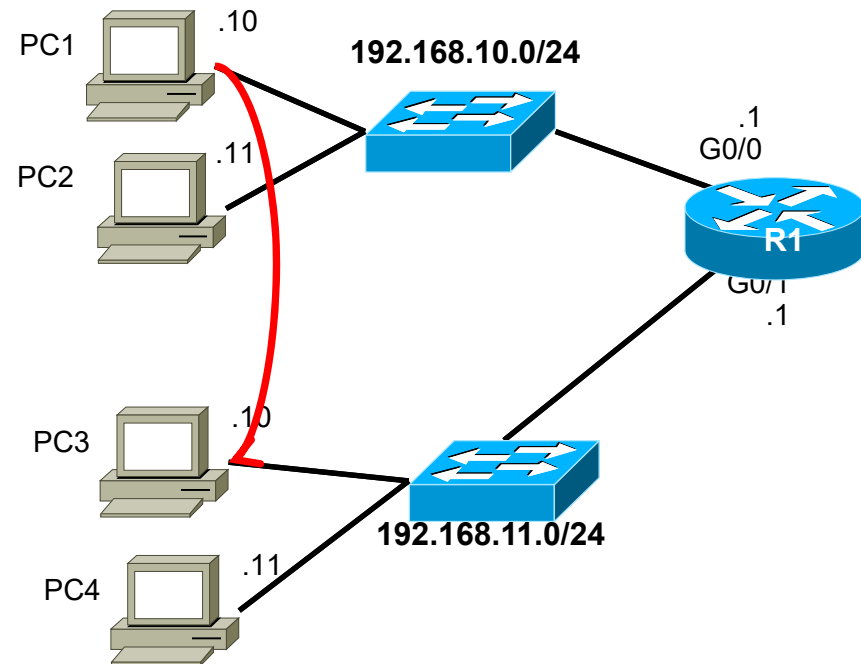
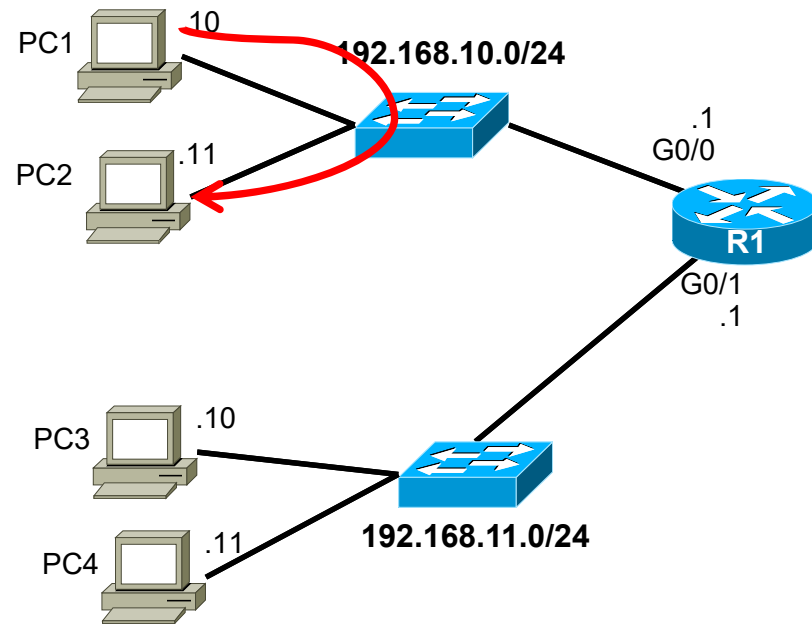
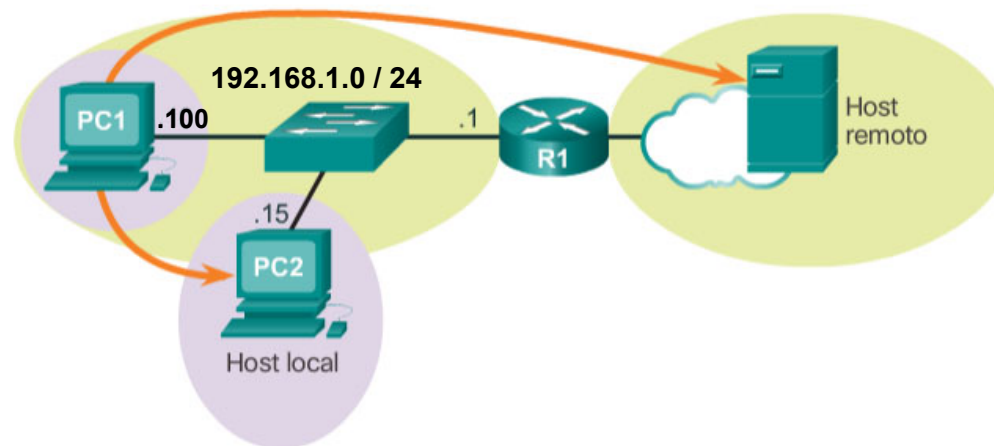




Tabla de enrutamiento de host IPv4

netstat -r muestra la tabla de enrutamiento de un host con Windows



```
C:\Documents and Settings\cisco>netstat -r
```

Route Table

A		B		C		D		E	
Active Routes:									
Network Destination		Netmask		Gateway		Interface		Metric	
0.0.0.0		0.0.0.0		192.168.1.1		192.168.1.100		20	
127.0.0.0		255.0.0.0		127.0.0.1		127.0.0.1		1	
192.168.1.0		255.255.255.0		192.168.1.100		192.168.1.100		20	
192.168.1.100		255.255.255.255		127.0.0.1		127.0.0.1		20	

- Host remoto
- A sí mismo
- A un host local
- A sí mismo



Enrutamiento

Tablas de enrutamiento de host

- En este ejemplo, se observa:
 - El host tiene la IP 192.168.1.100
 - La red a la que está conectada es 192.168.1.0/24
 - El gateway predeterminado (R1) tiene la IP 192.168.1.1

```
C:\Documents and Settings\cisco>netstat -r
```

```
Route Table
```

A		B	C	D	E
Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0		0.0.0.0	192.168.1.1	192.168.1.100	20
127.0.0.0		255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0		255.255.255.0	192.168.1.100	192.168.1.100	20
192.168.1.100		255.255.255.255	127.0.0.1	127.0.0.1	20

Routers

Anatomía de un router





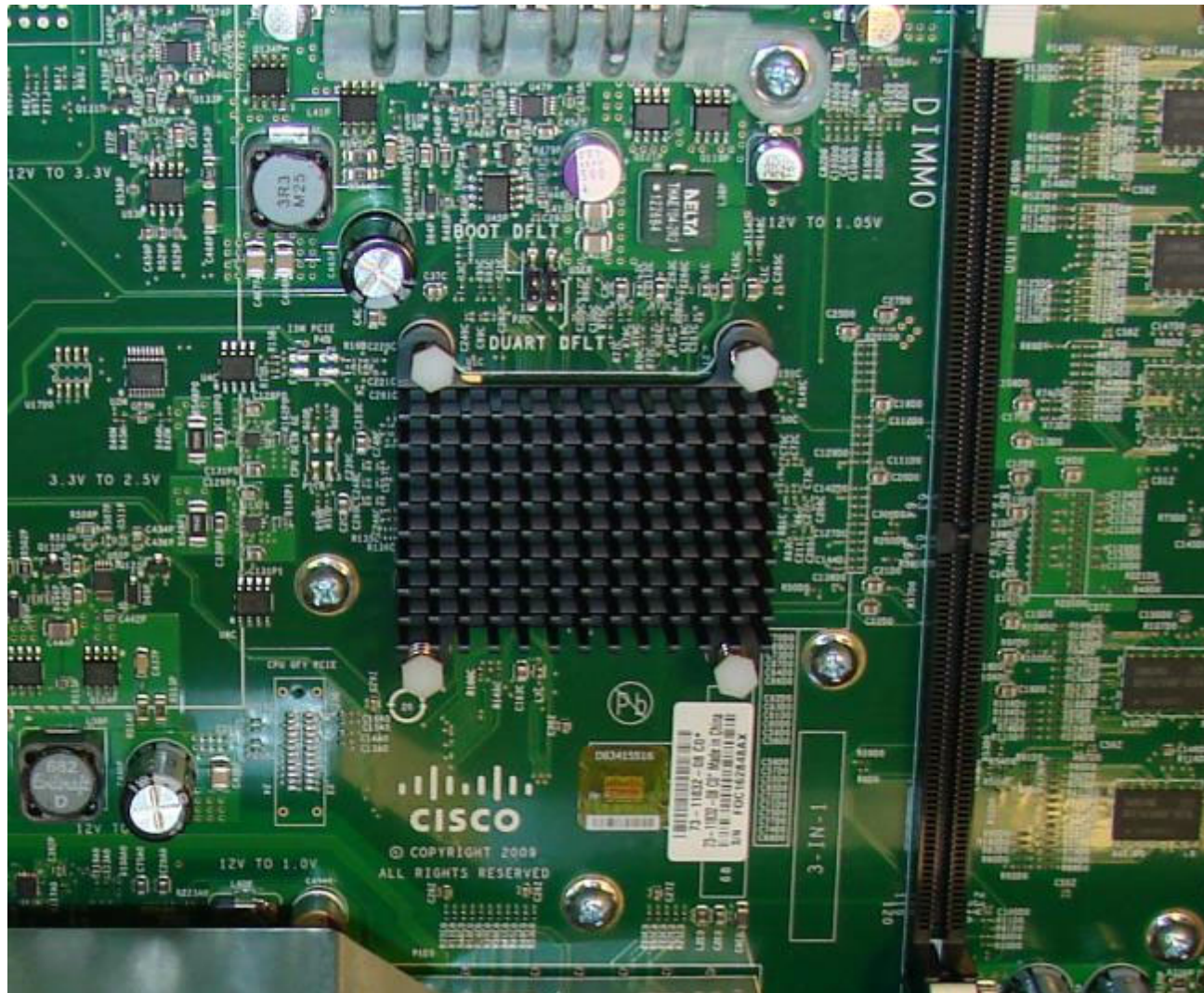
Anatomía de un router

Los routers son computadoras



Anatomía de un router

CPU y OS del router





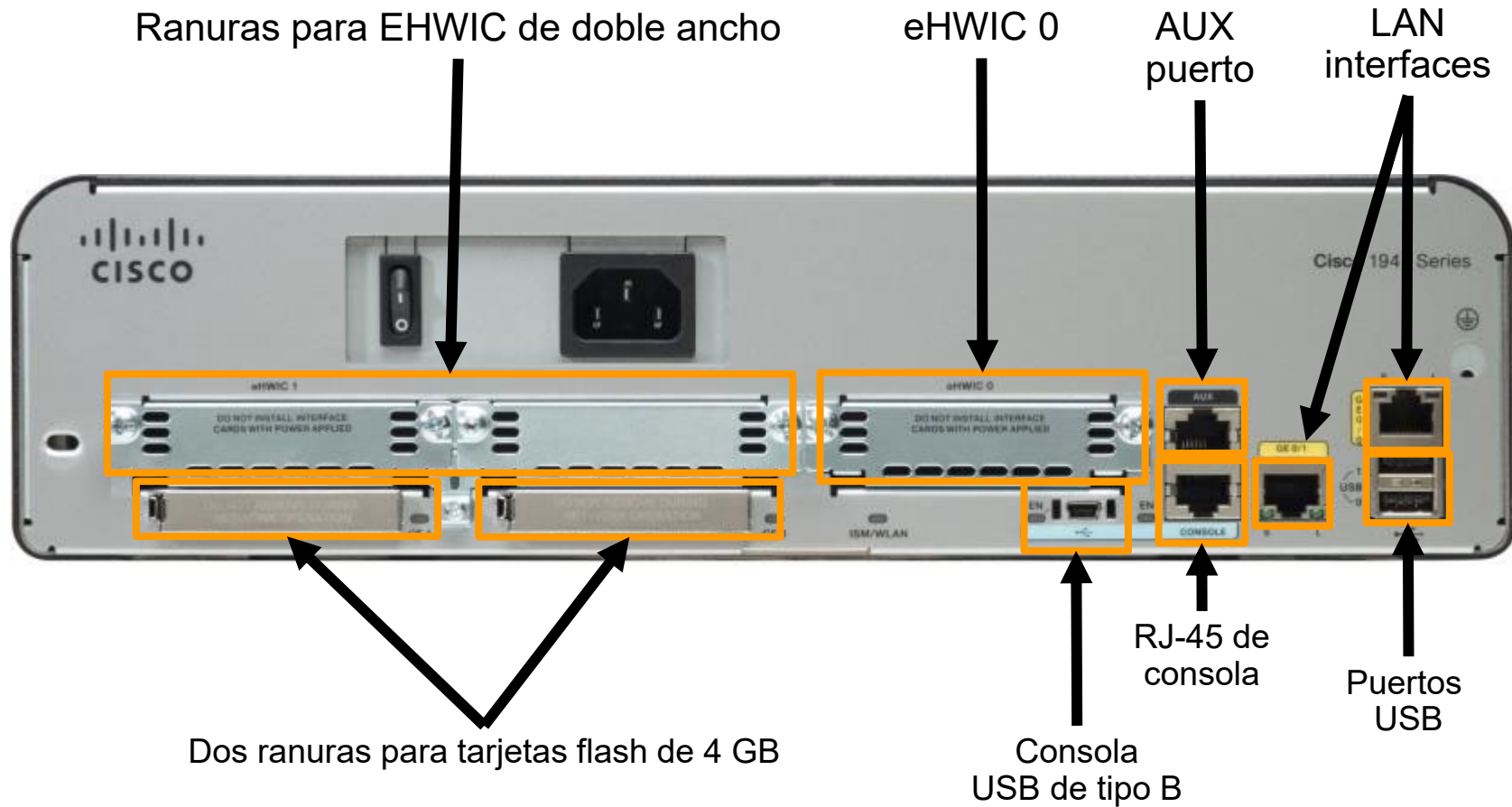
Anatomía de un router

Memoria del router

Memoria	Volátil / No volátil	Almacena
RAM	Volátil	<ul style="list-style-type: none">• IOS en ejecución• Archivo de configuración en ejecución• Tabla enrutamiento y tabla ARP• Buffer de paquetes
ROM	No volátil	<ul style="list-style-type: none">• Instrucciones de arranque• Software básico de diagnóstico• IOS limitado
NVRAM	No volátil	<ul style="list-style-type: none">• Archivo de configuración de inicio
Flash	No volátil	<ul style="list-style-type: none">• IOS (Sistema operativo de internetworking)• Otros archivos de sistema

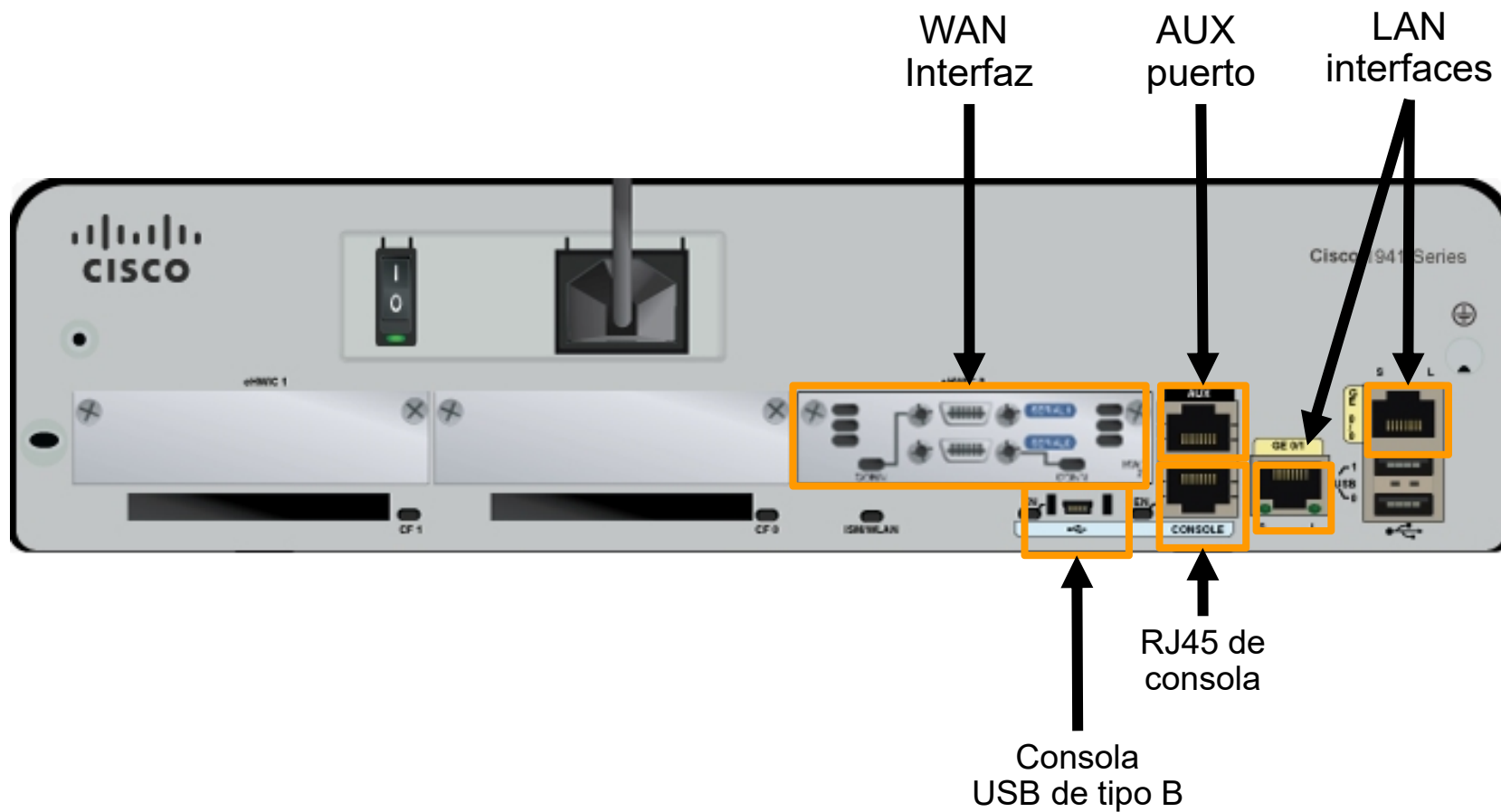
Anatomía de un router

Backplane del router



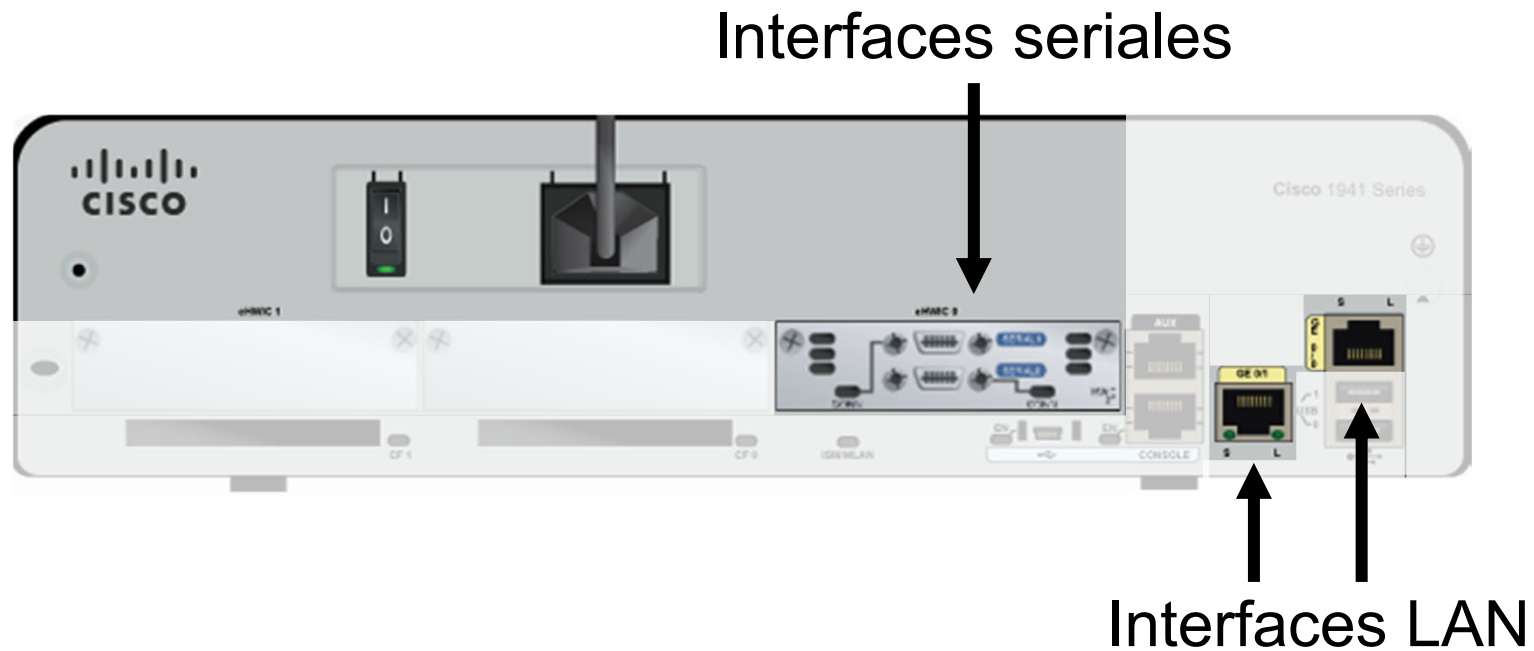
Anatomía de un router

Conexión al router



Anatomía de un router

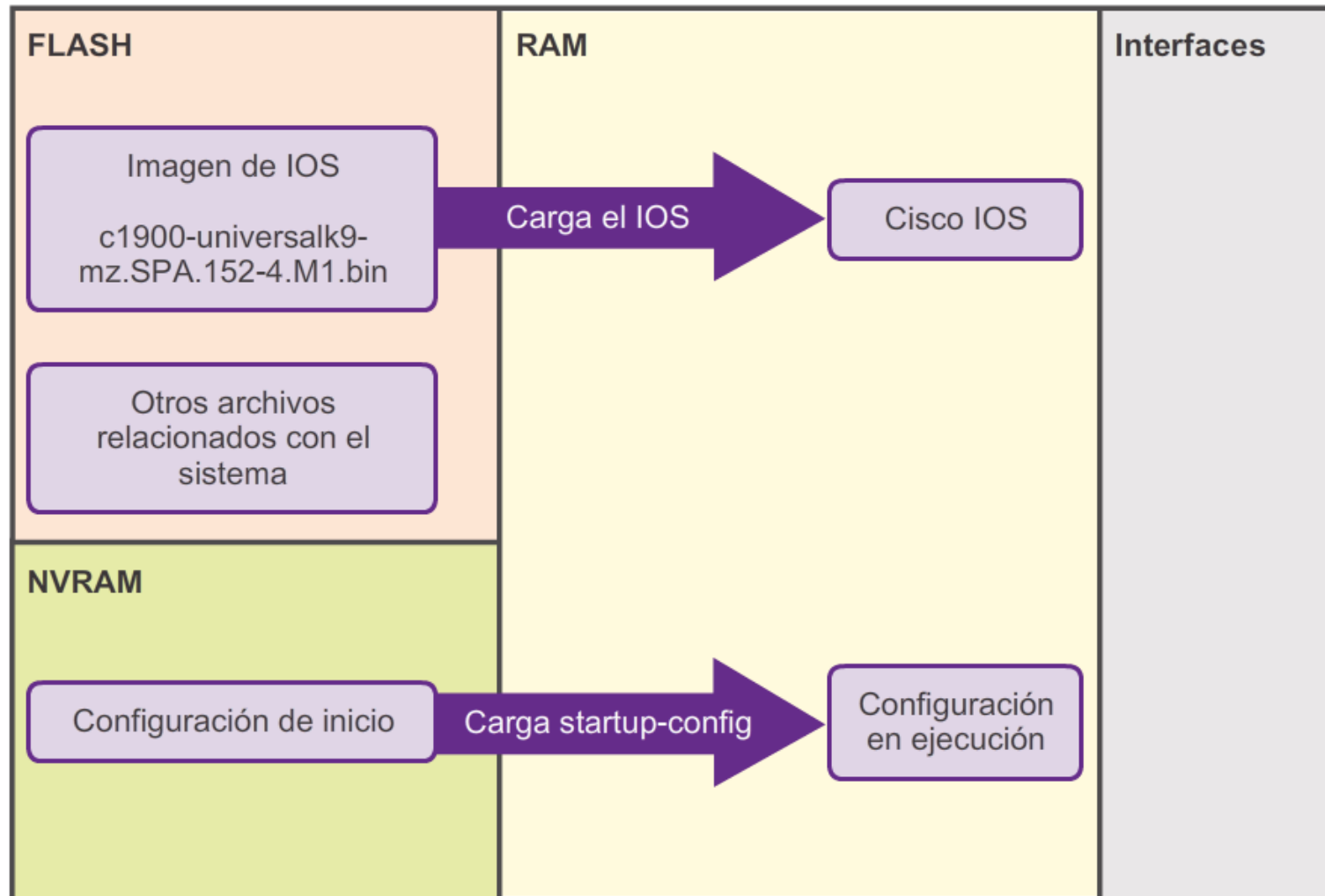
Interfaces LAN y WAN





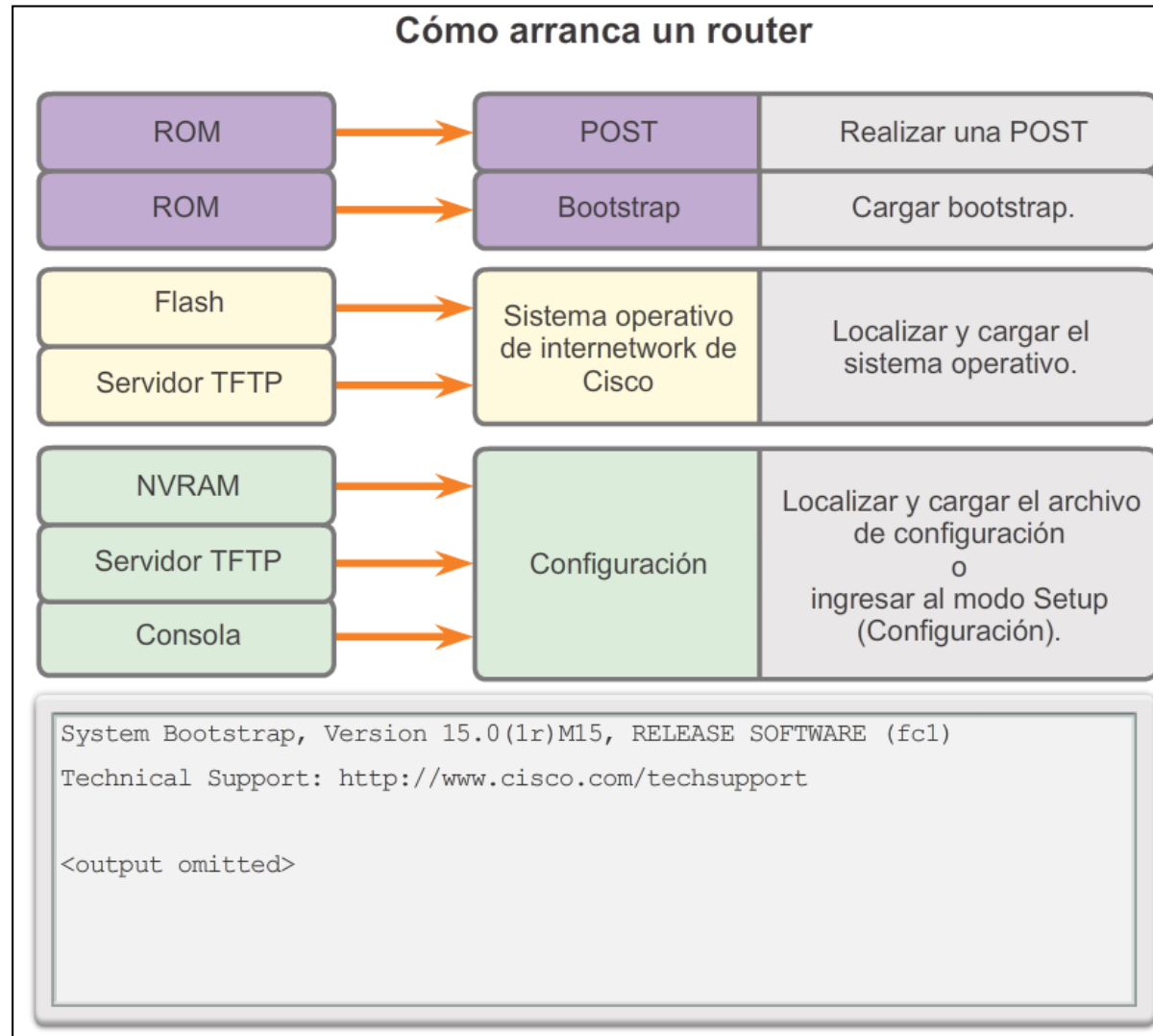
Arranque del router

Archivos Bootset



Arranque del router

Proceso de arranque del router



1. Realizar la POST y cargar el programa bootstrap.

2. Localizar y cargar el software Cisco IOS.

3. Localizar y cargar el archivo de configuración de inicio o ingresar al modo Setup.



Arranque del router

Resultado de Show version

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Soporte técnico: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team
```

```
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
```

```
Router uptime is 10 hours, 9 minutes
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: power-on
```

<Resultado omitido>

```
Cisco CISC01941/K9 (revision 1.0) with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)
```

<Resultado omitido>

Technology Package License Information for Module:'c1900'

Technology	Technology-package Current	Technology-package Type	Technology-package Next reboot
ipbase	ipbasek9	Permanent	ipbasek9
security	None	None	None
data	None	None	None

Configuration register is 0x2142 (will be 0x2102 at next reload)

Router#

Capa de red

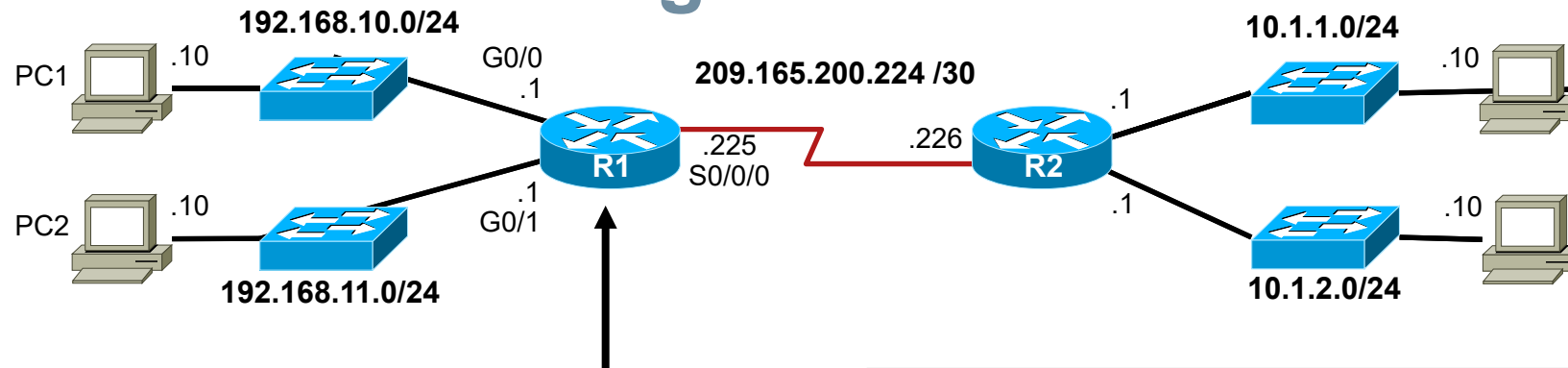
Configuración de un router Cisco





Configuración inicial

Pasos de configuración del router



```
Router> enable
Router# configure terminal
Ingrese los comandos de configuración, uno
por línea. Finalice con CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

O

```
Router> en
Router# conf t
Ingrese los comandos de configuración, uno
por línea. Finalice con CNTL/Z.
Router(config)# ho R1
R2(config)#
```

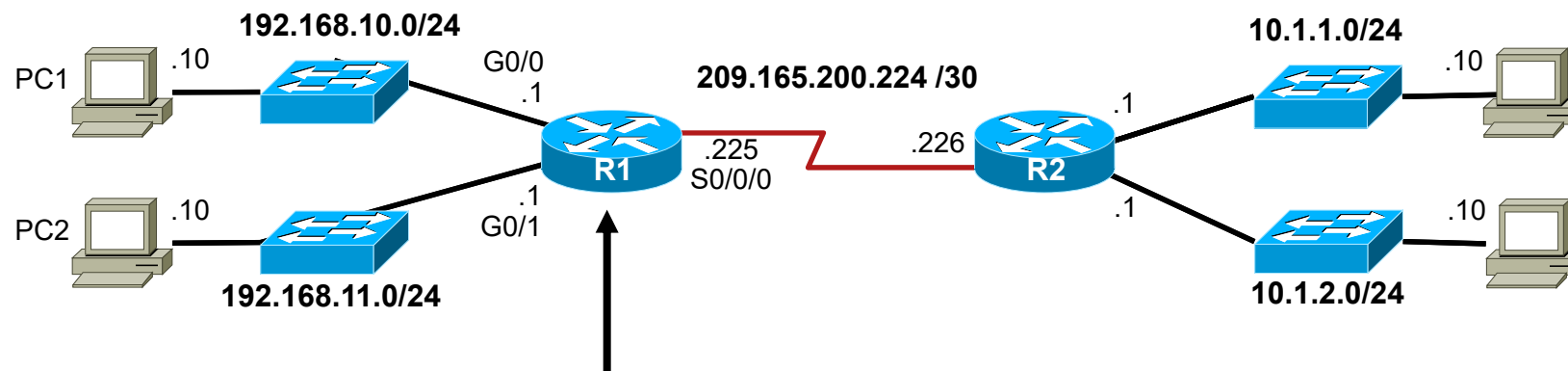
```
R1(config)# banner motd #
Ingrese mensaje de TEXTO. Finalice con el caracter
"#".
*****
WARNING: Unauthorized access is prohibited!
*****
#
R1(config)#
```

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```



Configuración de interfaces

Configuración de interfaces LAN

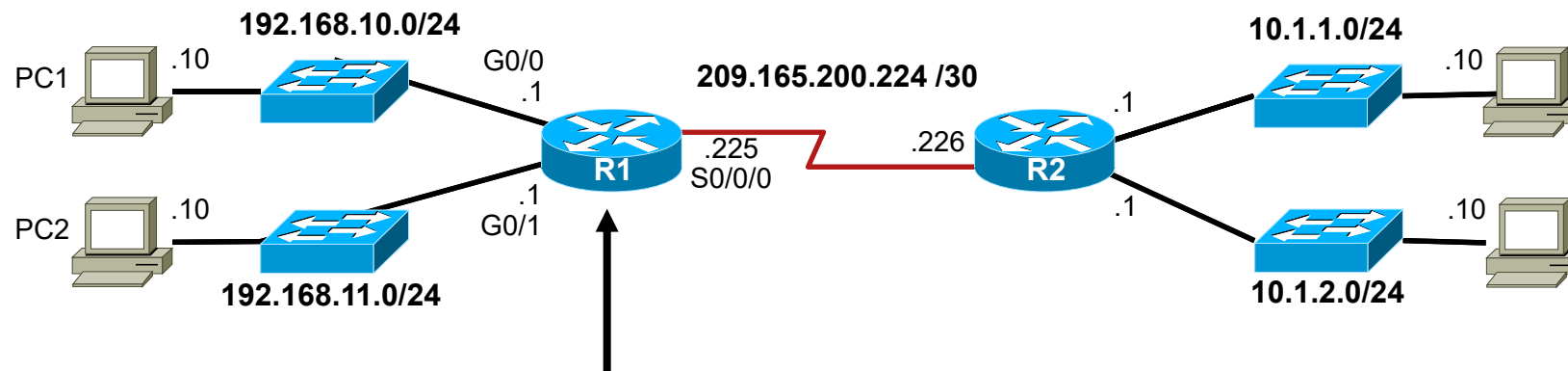


```
R1# conf t
Ingrese los comandos de configuración, uno por línea. Finalice con
CNTL/Z.
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description Link to LAN-10
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)# exit
R1(config)#
R1(config)# int g0/1
R1(config-if)# ip add 192.168.11.1 255.255.255.0
R1(config-if)# des Link to LAN-11
R1(config-if)# no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
R1(config-if)# exit
R1(config)#
```



Configuración de interfaces

Verificación de configuración de interfaz



```
R1# show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       192.168.10.1    YES manual  up          up
GigabitEthernet0/1       192.168.11.1    YES manual  up          up
Serial0/0/0               209.165.200.225 YES manual  up          up
Serial0/0/1               unassigned      YES NVRAM   administratively down down
Vlan1                     unassigned      YES NVRAM   administratively down down
R1#
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

R1#
```




Capa de red

Resumen

- La capa de red permite que los dispositivos finales intercambien paquetes a través de la red
- La capa de red utiliza: la encapsulación, el direccionamiento jerarquico de dispositivos finales y el enrutamiento
- IPv4 continúa siendo el protocolo que más se utiliza
- IPv6 ofrece varias ventajas: mayor eficacia de enrutamiento, encabezados simplificados y capacidad de proceso por flujo
- Cuando un paquete llega a un router:
 - Lo desencapsula
 - Mira su IP destino y busca en la tabla de enrutamiento
 - Lo encapsula y lo reenvia por la interfaz adecuada



Capa de red

Resumen

- En la tabla de enrutamiento de un router se almacena:
 - redes conectadas directamente → interfaz que lo conecta
 - redes remotas → IP del router de siguiente salto
 - ruta predeterminada → Si no existe ninguna entrada que coincida
- Enrutamiento estático → las entradas de la tabla de enrutamiento se pueden configurar manualmente
- Protocolo de enrutamiento → los routers comunican a otros routers las redes que pueden alcanzar
- Los hosts también tienen una tabla de enrutamiento para asegurarse de que los paquetes se dirijan a la red correcta
- La ruta predeterminada corresponde con la IP del router conectado a su red local