



# ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

FORMANDO PROFESIONALES DE ÉLITE



# FUNDAMENTOS DE REDES

## CLASE 7

Ing. ANDRÉS PÉREZ





# INTRODUCCIÓN A LA CLASE

1. Retroalimentación
2. Indicaciones generales
3. Objetivos de la clase



**ITSQMET**  
INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

# RETROALIMENTACIÓN

FORMANDO PROFESIONALES DE ÉLITE



## Objetivos de la clase:

1. Reconocer las características de la Capa de RED



# ÍNDICE

## UNIDAD II: DIRECCIONAMIENTO IP

- Capa de RED
- PAQUETE IPV4
- PAQUETE IPV6
- INTRODUCCIÓN AL ENRUTAMIENTO





**ITSQMET**  
INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

# CAPA DE RED

FORMANDO PROFESIONALES DE ÉLITE



# CAPA DE RED

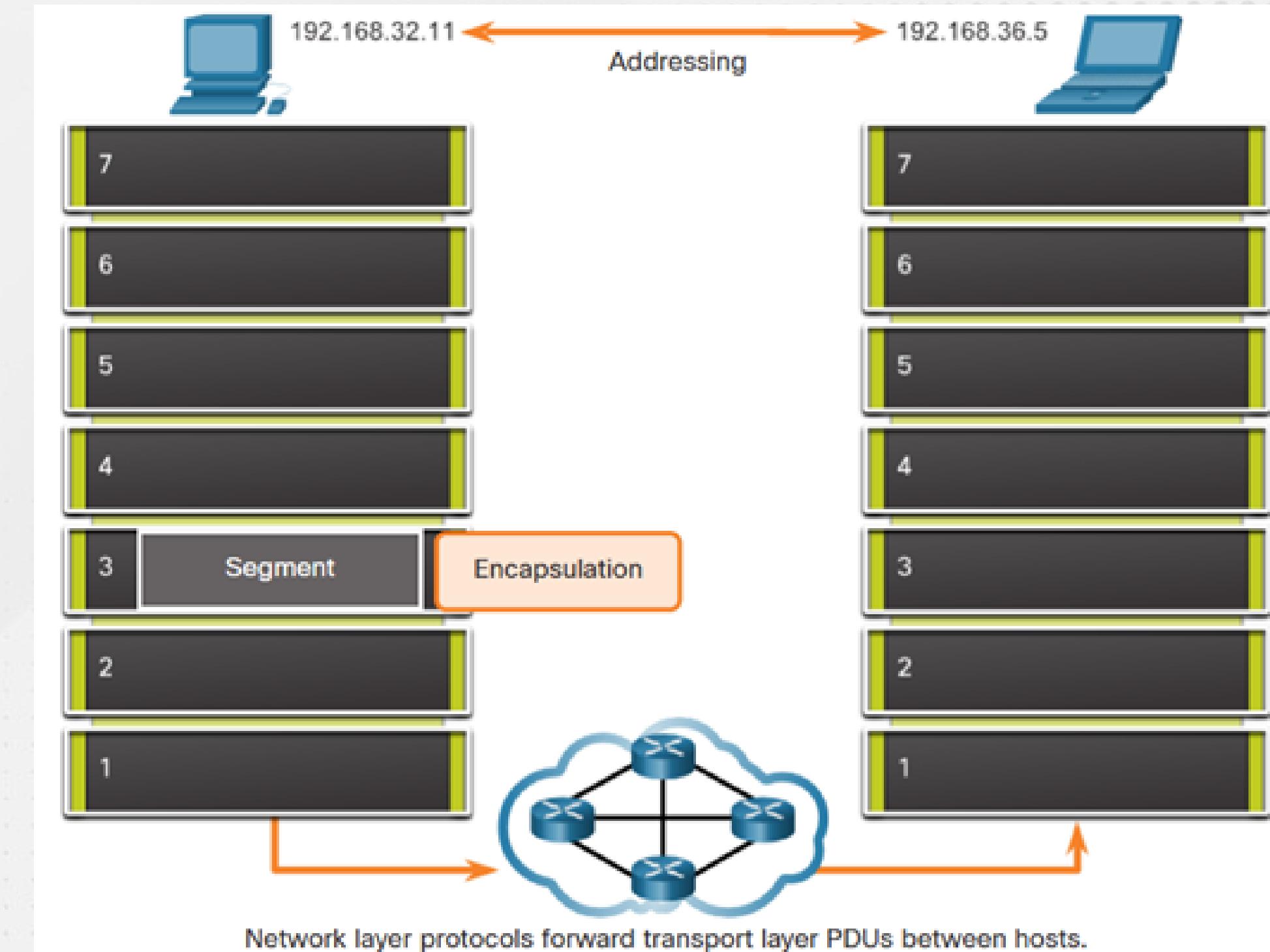


- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)



# CAPA DE RED

- Proporciona servicios para permitir que los dispositivos finales intercambien datos
- IP versión 4 (IPv4) e IP versión 6 (IPv6) son los principales protocolos de comunicación de la capa de red.
- La capa de red realiza cuatro operaciones básicas:
  - Direccionalamiento de terminales
  - Encapsulamiento
  - Routing
  - Desencapsulamiento



# Operaciones básicas de la Capa de Red

1. **Direccionamiento de dispositivos finales:** los dispositivos finales deben configurarse con una dirección IP única para la identificación en la red.
2. **Encapsulación:** La capa de red encapsula la unidad de datos de protocolo (PDU) de la capa de transporte en un paquete. El proceso de encapsulamiento agrega información de encabezado IP, como la dirección IP de los hosts de origen (emisores) y de destino (receptores).
3. **Enrutamiento:** La capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para transferir un paquete a otras redes, debe procesarlo un router.
  - Función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina "enrutamiento".
4. **Desencapsulación:** Cuando el paquete llega a la capa de red del host de destino, el host verifica el encabezado IP del paquete. Si la dirección IP de destino dentro del encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete.



© 2016 Cisco y/o sus filiales. Todos los derechos reservados.  
Información confidencial de Cisco

7

© 2016 Cisco y/o sus filiales. Todos los derechos reservados.  
Información confidencial de Cisco

Nº



- IP encapsula el segmento de la capa de transporte.
- IP puede utilizar un paquete IPv4 o IPv6 y no afectar al segmento de capa 4.
- El paquete IP será examinado por todos los dispositivos de capa 3 a medida que atraviese la red.
- El direccionamiento IP no cambia de origen a destino.

**Nota:** NAT cambiará el direccionamiento, pero se discutirá en un módulo posterior.

Encapsulamiento de la capa de transporte

Encabezado del segmento

Datos

PDU de la capa de transporte

Encapsulamiento de la capa de red

Encabezado IP

Datos

PDU de la capa de red

Paquete IP



# Características de la capa de red

## Características de IP

IP está destinado a tener una sobrecarga baja y puede describirse como:

- Sin conexión
- Servicio mínimo
- Independiente de los medios



# Características de la capa de red Sin conexión (Connectionless)

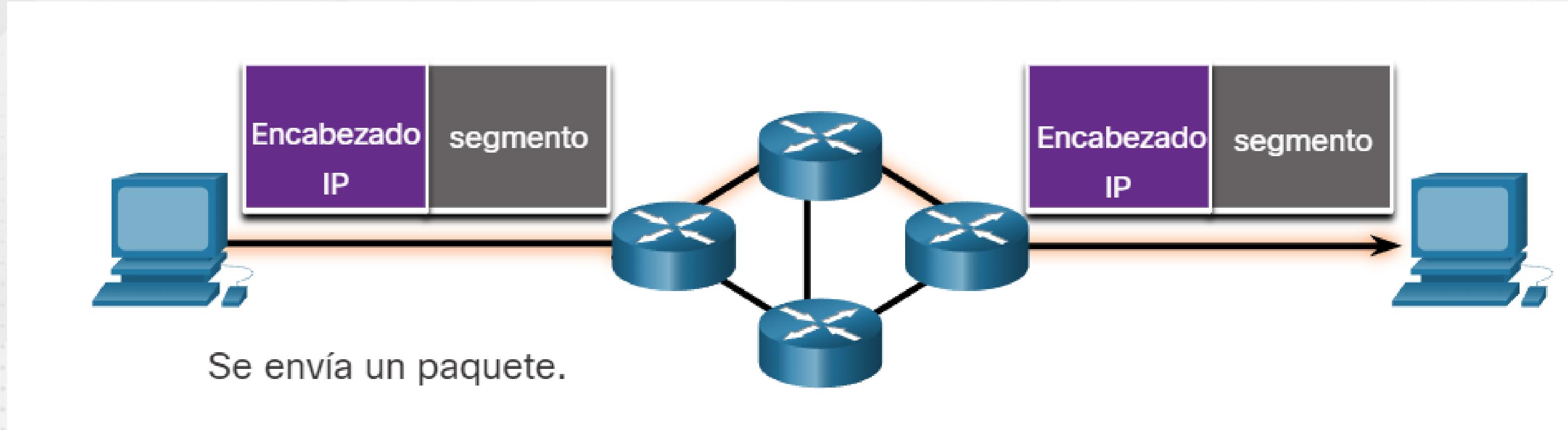
## IP Sin conexión (Connectionless)

- IP no establece ninguna conexión con el destino antes de enviar el paquete.
- No se necesita información de control (sincronizaciones, confirmaciones, etc.).
- El destino recibirá el paquete cuando llegue, pero no se envían notificaciones previas por IP.
- Si hay una necesidad de tráfico orientado a la conexión, otro protocolo manejará esto (normalmente TCP en la capa de transporte).





# Características de la capa de red Sin conexión (Connectionless)

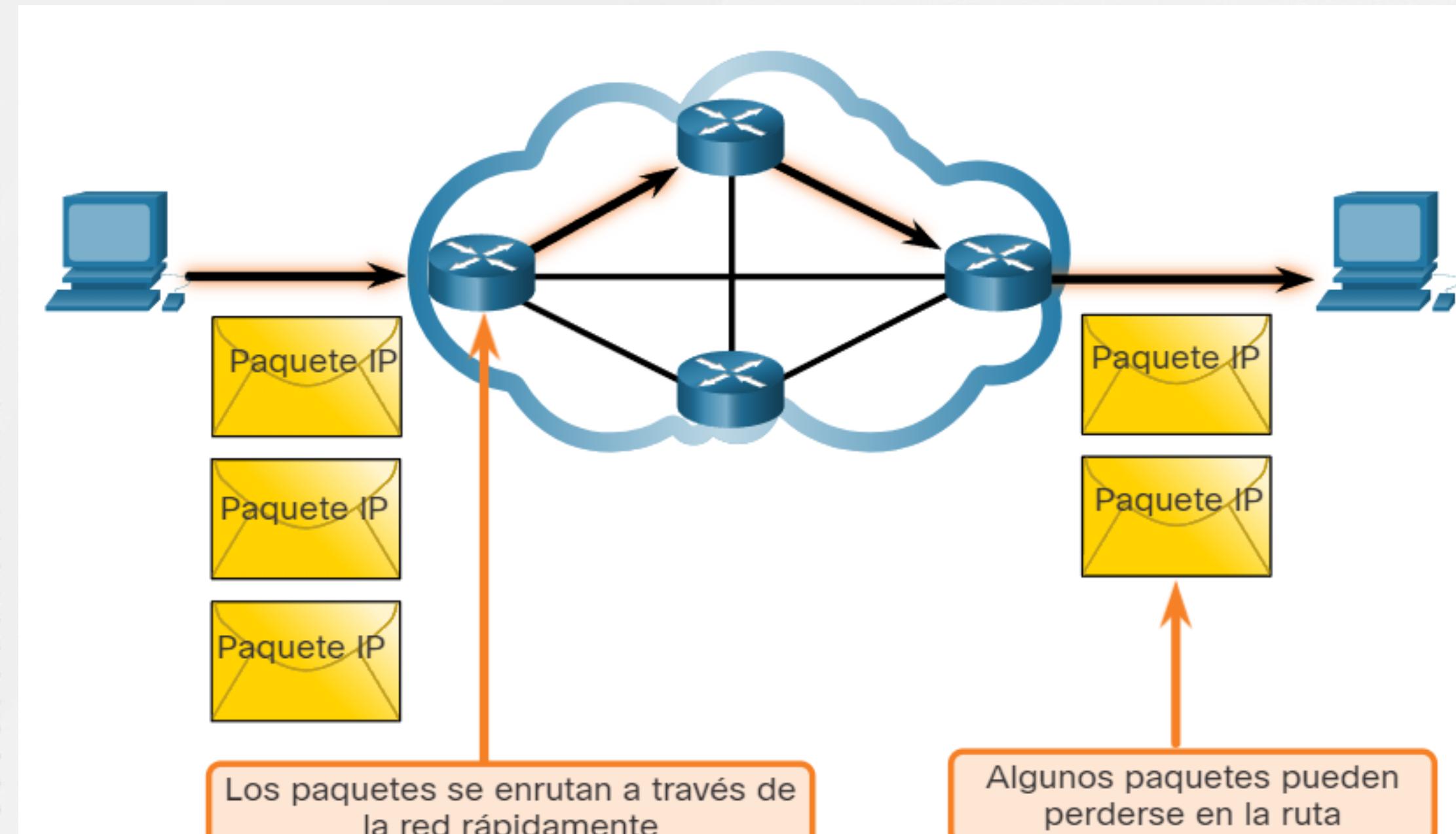




# Características de la Capa de Red Mejor esfuerzo (Best Effort)

IP is el mejor esfuerzo

- IP no garantizará la entrega del paquete.
- IP ha reducido la sobrecarga ya que no existe ningún mecanismo para reenviar datos que no se reciben.
- IP no espera reconocimientos.
- IP no sabe si el otro dispositivo está operativo o si recibió el paquete.





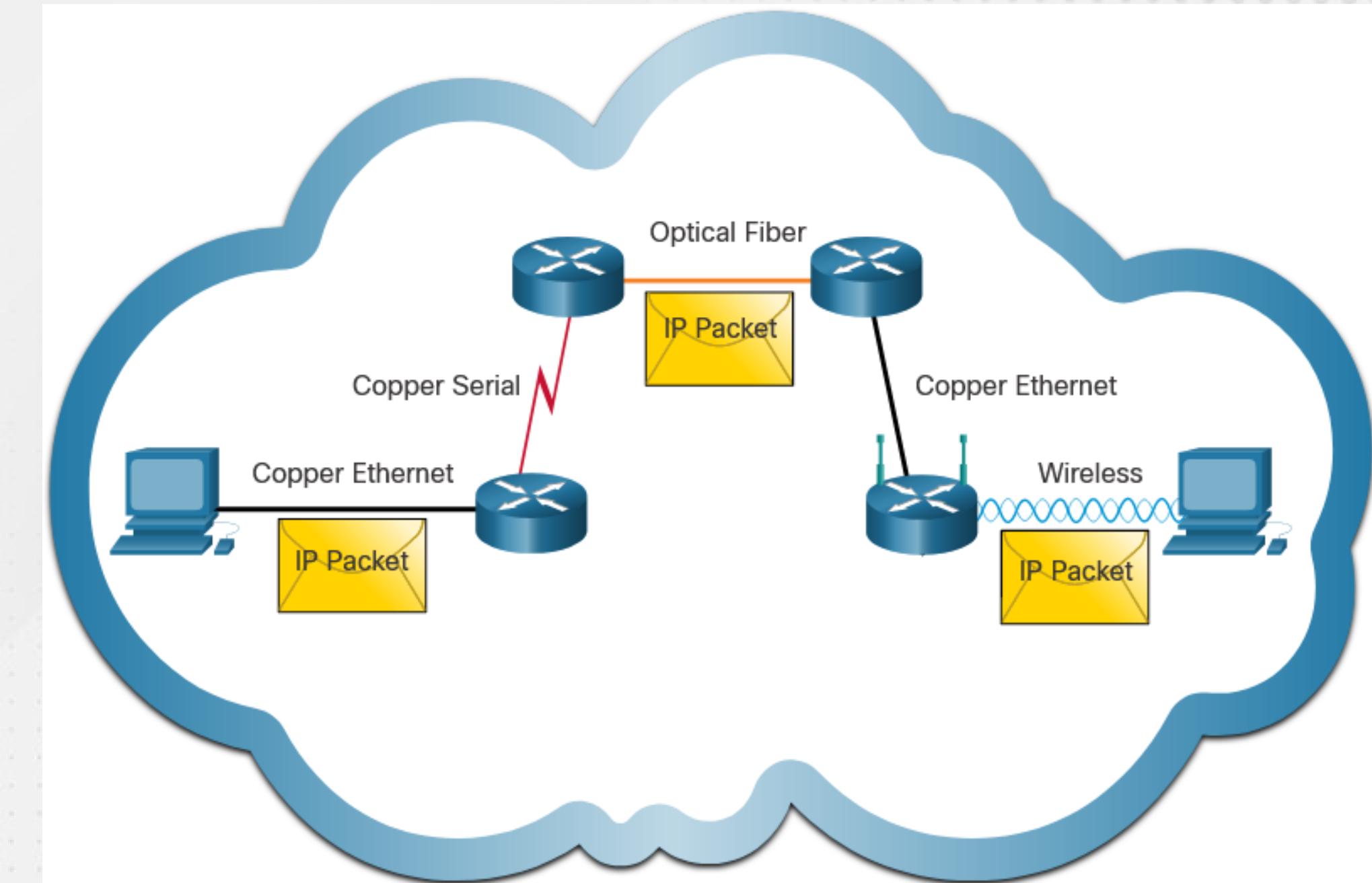
# Características de la capa de red Independencia de Medios

IP no es confiable:

- No puede administrar ni corregir paquetes no entregados o corruptos.
- IP no puede retransmitir después de un error.
- IP no puede realinear los paquetes de secuencia.
- IP debe depender de otros protocolos para estas funciones.

IP es independiente de los medios:

- IP no se refiere al tipo de trama requerido en la capa de enlace de datos ni al tipo de medio en la capa física.
- IP se puede enviar a través de cualquier tipo de medio: cobre, fibra o inalámbrica.





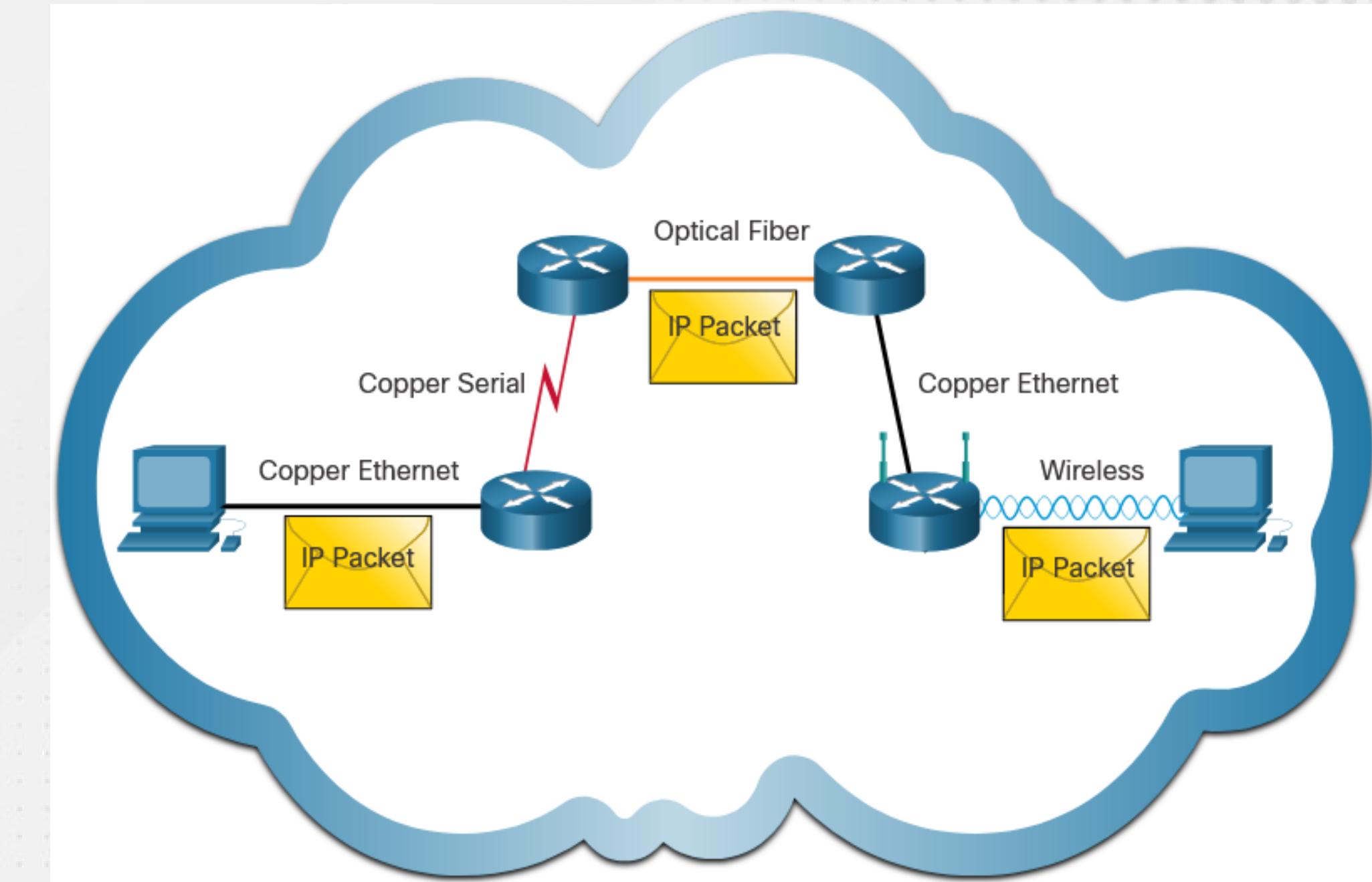
La capa de red establecerá la Unidad de Transmisión Máxima (MTU).

- La capa de red lo recibe de la información de control enviada por la capa de vínculo de datos.
- A continuación, la red establece el tamaño de MTU.

La fragmentación es cuando la Capa 3 divide el paquete IPv4 en unidades más pequeñas.

- Fragmentar provoca latencia.
- IPv6 no fragmenta paquetes.
- Ejemplo: El router pasa de Ethernet a una WAN lenta con una MTU más pequeña.

## Características de la capa de red Independencia de medios





**ITSQMET**  
INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

# PAQUETE IPV4

FORMANDO PROFESIONALES DE ÉLITE



## Paquete IPV4

# Encabezado de paquetes IPV4

IPv4 es el protocolo de comunicación principal para la capa de red.

El encabezado de red tiene muchos propósitos:

- Garantiza que el paquete se envía en la dirección correcta (al destino).
- Contiene información para el procesamiento de capas de red en varios campos.
- La información del encabezado es utilizada por todos los dispositivos de capa 3 que manejan el paquete



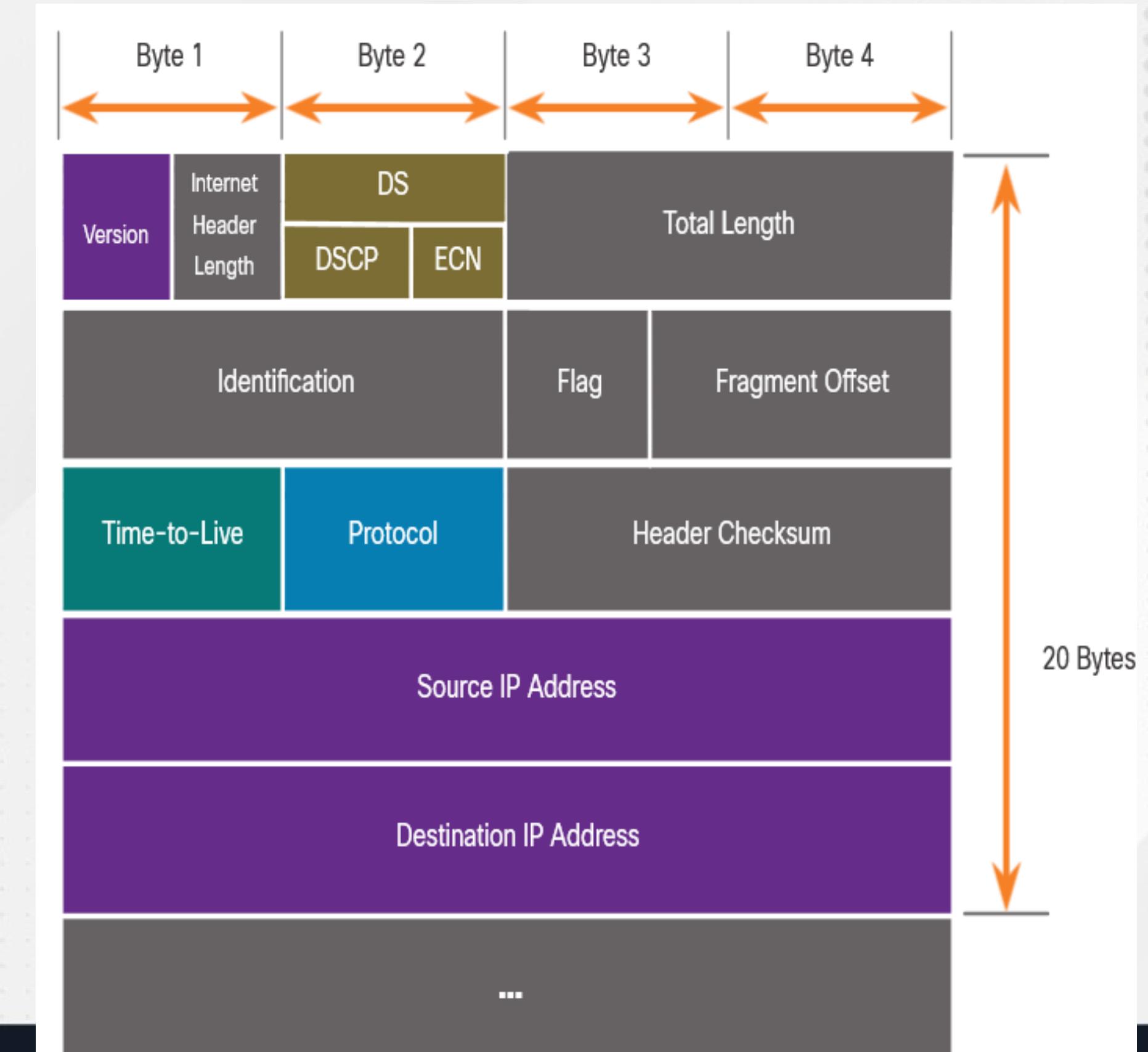
# Paquete IPV4

## Campos de encabezado de paquete IPV4

Características del encabezado de red IPv4:

- Está en binario.
- Contiene varios campos de información
- Diagrama se lee de izquierda a derecha, 4 bytes por línea
- Los dos campos más importantes son el origen y el destino.

Los protocolos pueden tener una o más funciones.





# Paquete IPV4

## Campos de encabezado de paquete IPV4

Campos significativos en el encabezado IPv4:

Función	Descripción
<b>Versión</b>	Esto será para v4, a diferencia de v6, un campo de 4 bits = 0100
<b>Servicios diferenciados</b>	Utilizado para QoS: campo DiffServ — DS o el anterior IntServ — ToS o Tipo de servicio
<b>Suma de comprobación del encabezado</b>	Detectar daños en el encabezado IPv4
<b>Tiempo de vida (TTL)</b>	Recuento de saltos de capa 3. Cuando se convierte en cero, el router descartará el paquete.
<b>de Internet</b>	Protocolo de siguiente nivel de ID: ICMP, TCP, UDP, etc.
<b>Dirección IPv4 de origen</b>	Dirección de origen de 32 bits
<b>Dirección IPV4 de destino</b>	Dirección de destino de 32 bits



**ITSQMET**  
INSTITUTO TECNOLÓGICO SUPERIOR  
QUITO METROPOLITANO

# PAQUETE IPV6

FORMANDO PROFESIONALES DE ÉLITE



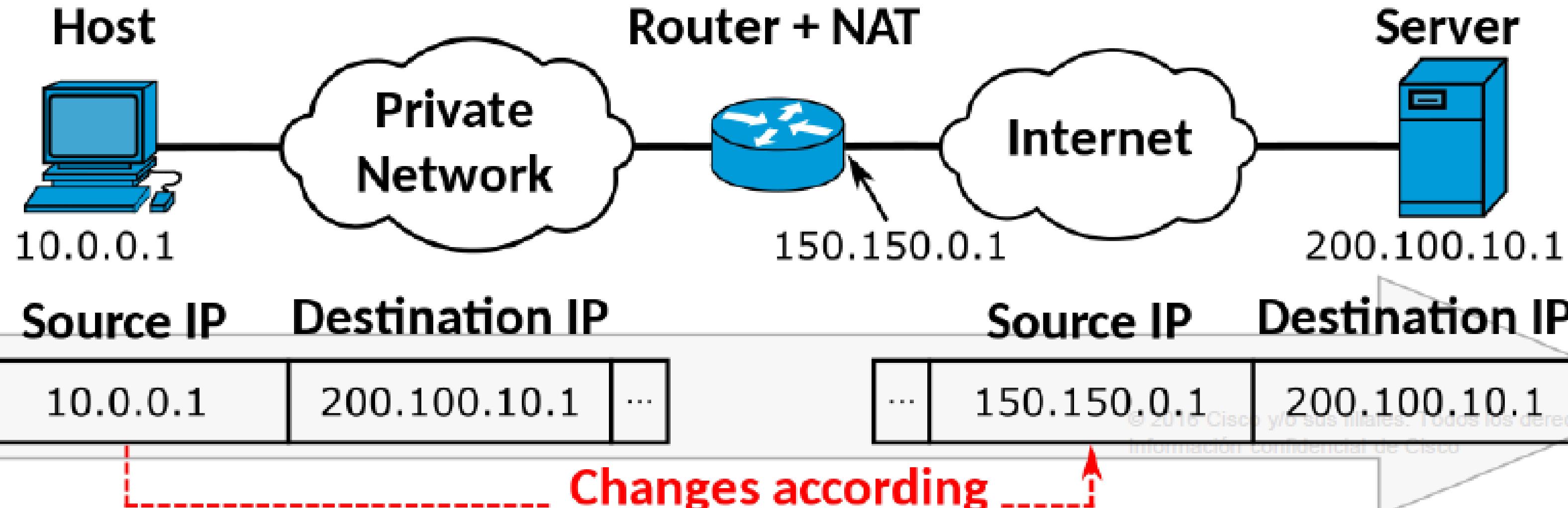
# Paquetes IPv6 Limitaciones de IPv4

IPv4 tiene tres limitaciones principales:

- Agotamiento de las direcciones IPv4: básicamente nos hemos quedado sin direccionamiento IPv4.
- Falta de conectividad de extremo a extremo: para que IPv4 sobreviva a este largo tiempo, se crearon direcciones privadas y NAT. Esto puso fin a las comunicaciones directas con el discurso público.
- Mayor complejidad de la red: NAT fue concebido como una solución temporal y crea problemas en la red como un efecto secundario de manipular los encabezados de red que direcciona. NAT provoca problemas de latencia y solucion de problemas.



# Paquetes IPv6 Limitaciones de IPv4





# Paquetes IPv6

## Introducción a IPv6

- IPv6 fué desarrollado por Internet Engineering Task Force (IETF).
- IPv6 vence las limitaciones de IPv4.
- Mejoras que proporciona IPv6:
  - **Mayor espacio de direcciones** : basado en la dirección de 128 bits, no en 32 bits
  - **Manejo mejorado de paquetes** – encabezado simplificado con menos campos
  - **Elimina la necesidad de NAT** : dado que hay una gran cantidad de direccionamiento, no es necesario utilizar direccionamiento privado internamente y asignarse a una dirección pública compartida



# Paquetes IPv6

## Introducción a IPv6

Nombre del número	Notación científica	Cantidad de ceros
Mil	$10^3$	1000
1 millón	$10^6$	1 000000
1000 millones	$10^9$	1000000000
1 billón	$10^{12}$	1000000000000
1000 billones	$10^{15}$	1000000000000000
1 trillón	$10^{18}$	1000000000000000000
1000 trillones	$10^{21}$	1000000000000000000000
1 cuatrillón	$10^{24}$	1000000000000000000000000
1000 cuatrillones	$10^{27}$	1000000000000000000000000000
1 quintillón	$10^{30}$	1000000000000000000000000000000
1000 quintillones	$10^{33}$	10000000000000000000000000000000000
1 sextillón	$10^{36}$	100

### Leyenda



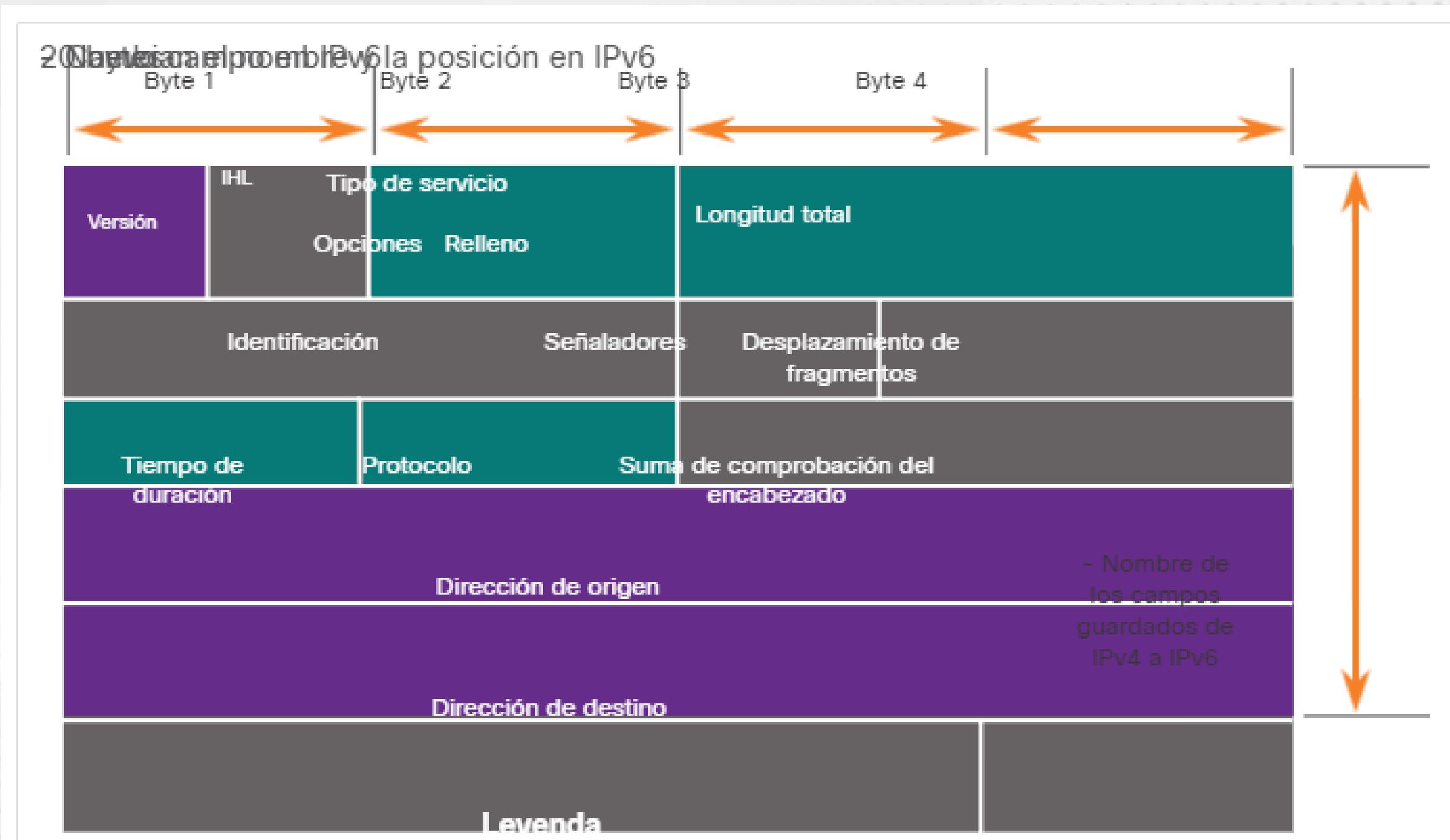
Hay 4000 millones de direcciones IPv4.

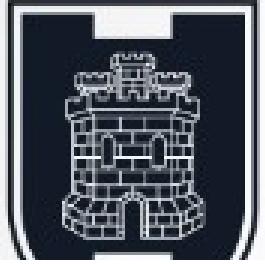


Hay 340 sextillones de direcciones IPv6.

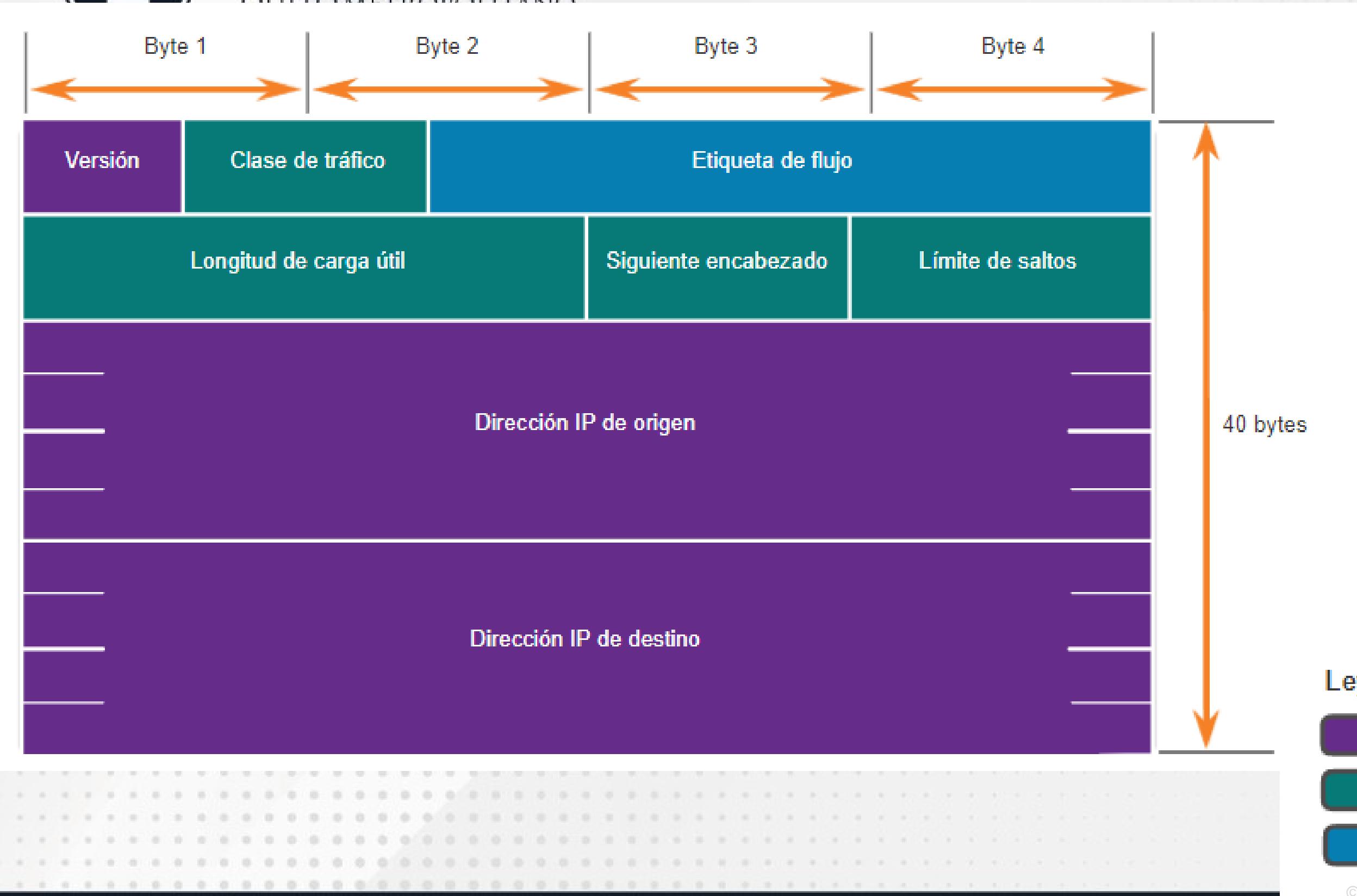


# Campos de encabezado de paquetes IPv4 en el encabezado de paquetes IPv6





# Paquetes IPv6 Encabezado de paquetes IPv6



## Paquetes IPV6

# Encabezado de paquetes IPV6

Campos significativos en el encabezado IPv4:

Función	Descripción
<b>Versión</b>	Esto será para v6, a diferencia de v4, un campo de 4 bits = 0110
<b>Clase de tráfico</b>	Utilizado para QoS: Equivalente al campo DiffServ — DS
<b>Etiqueta de flujo</b>	Informa al dispositivo para manejar etiquetas de flujo idénticas de la misma manera, campo de 20 bits
<b>Longitud de carga útil</b>	Este campo de 16 bits indica la longitud de la porción de datos o la carga útil del paquete IPv6
<b>Siguiente encabezado</b>	I.D.s de siguiente nivel protocolo: ICMP, TCP, UDP, etc.
<b>Límite de saltos</b>	Reemplaza el recuento de saltos de capa 3 del campo TTL
<b>Dirección IPv4 de origen</b>	Dirección de origen de 128 bits
<b>Dirección IPV4 de destino</b>	Dirección de destino de 128 bits



## Paquetes IPV6

# Encabezado de paquetes IPV6

El paquete IPv6 también puede contener encabezados de extensión (EH).

Características de los encabezados EH:

- proporcionar información de capa de red opcional
- son opcionales
- se colocan entre el encabezado IPv6 y la carga útil
- puede usarse para fragmentación, seguridad, soporte de movilidad, etc.

**Nota:** a diferencia de IPv4, los Routers no fragmentan los paquetes de IPv6.



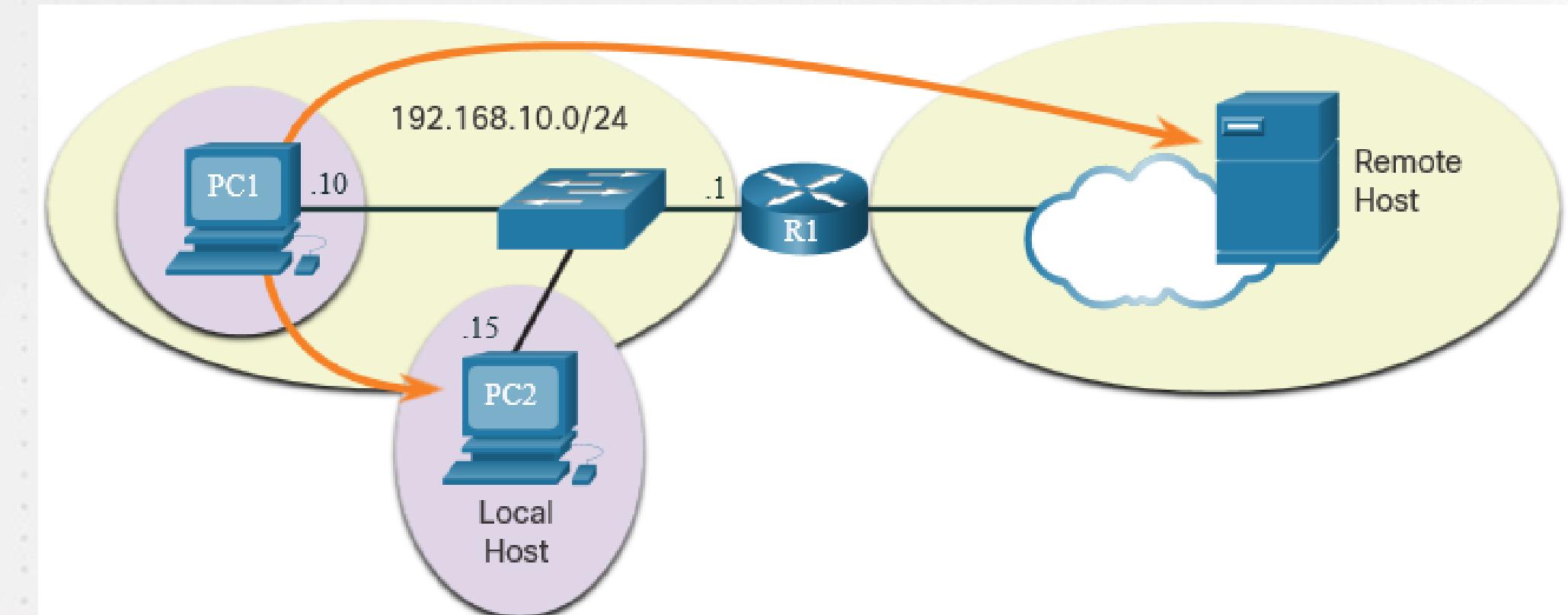
# INTRODUCCIÓN AL ENRUTAMIENTO



# Cómo se enruta un Host

## Decisión de reenvío de host

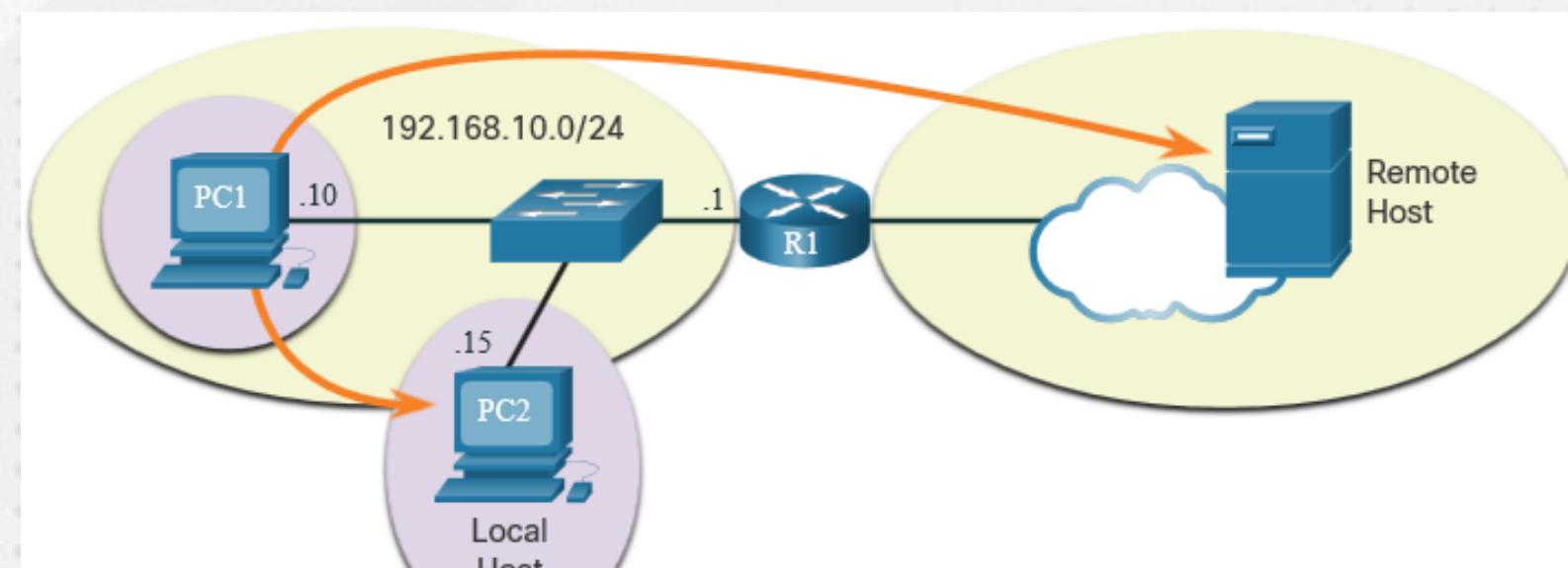
- Los paquetes siempre se crean en el origen.
- Cada dispositivo host crea su propia tabla de enrutamiento.
- Un host puede enviar paquetes a lo siguiente:
  - Sí mismo — 127.0.0.1 (IPv4), : :1 (IPv6)
  - Hosts locales: el destino está en la misma LAN
  - Hosts remotos: los dispositivos no están en la misma LAN





# Cómo se enruta un Host Decisión de reenvío de host (Cont.)

- El dispositivo de origen determina si el destino es local o remoto
- Método de determinación:
  - IPv4: el origen utiliza su propia dirección IP y máscara de subred, junto con la dirección IP de destino
  - IPv6: el origen utiliza la dirección de red y el prefijo anunciados por el enrutador local
- El tráfico local se desconecta de la interfaz de host para ser manejado por un dispositivo intermedio.
- El tráfico remoto se reenvía directamente a la puerta de enlace predeterminada de la LAN.





## Cómo se enrutan los host **Gateway Predeterminado**

Un enrutador o conmutador de capa 3 puede ser una puerta de enlace predeterminada.

Características de una puerta de enlace predeterminada (DGW):

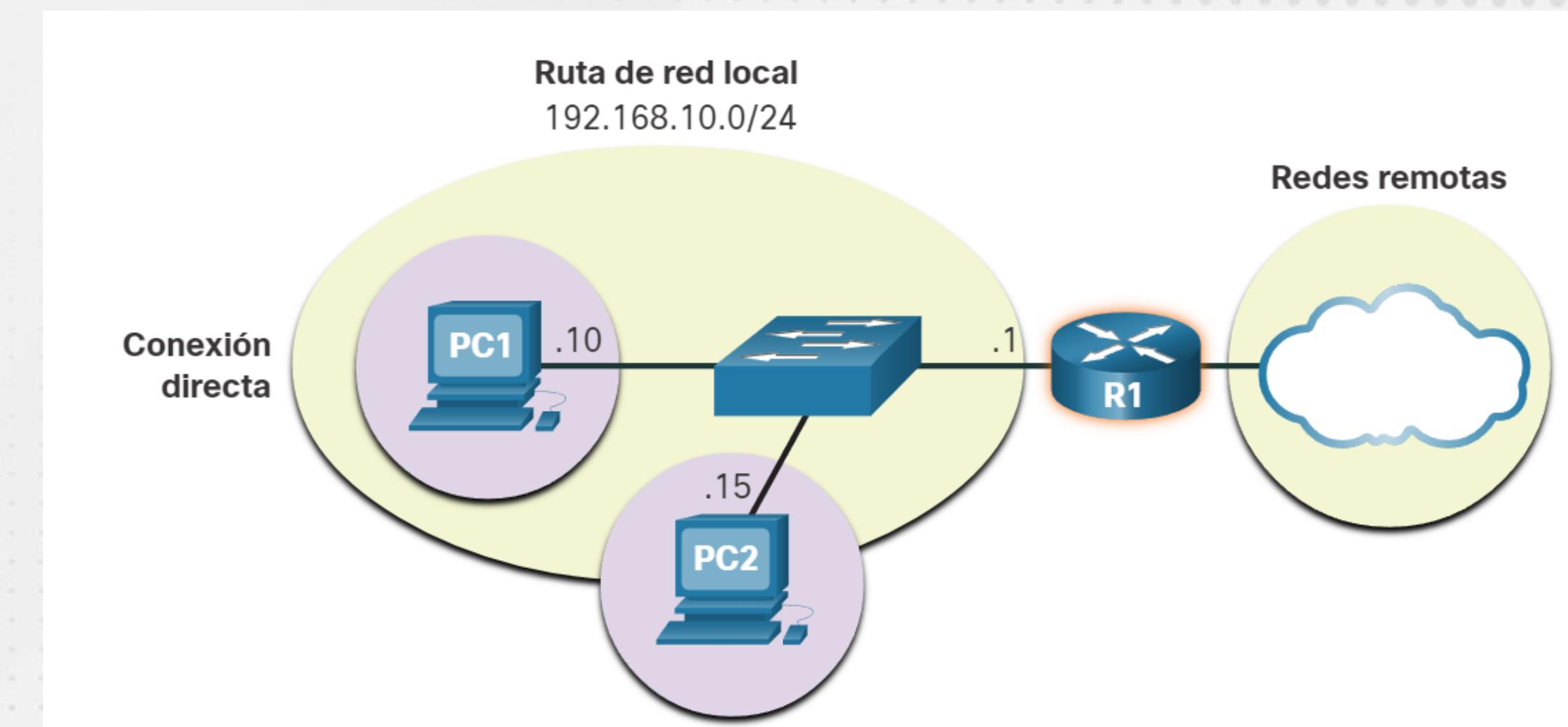
- Debe tener una dirección IP en el mismo rango que el resto de la LAN.
- Puede aceptar datos de la LAN y es capaz de reenviar tráfico fuera de la LAN.
- Puede enrutarse a otras redes.

Si un dispositivo no tiene una puerta de enlace predeterminada o una puerta de enlace predeterminada incorrecta, su tráfico no podrá salir de la LAN.



## Cómo se enrutan los host Un host enruta a la puerta de enlace predeterminada

- El host conocerá la puerta de enlace predeterminada (DGW) de forma estática o a través de DHCP en IPv4.
- IPv6 envía el DGW a través de una solicitud de un router (RS) o puede configurarse manualmente.
- Una DGW es una ruta estática que será una ruta de último recurso en la tabla de enrutamiento.
- Todos los dispositivos de la LAN necesitarán el DGW del roter si tienen la intención de enviar tráfico de forma remota.





# Cómo se enruta un Host

## Tablas de enrutamiento de Host



### IPv4 Routing Table for PC1

```
C:\Users\PC1> netstat -r
```

#### IPv4 Route Table

##### Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.10.0	255.255.255.0	On-link	192.168.10.10	281
192.168.10.10	255.255.255.255	On-link	192.168.10.10	281
192.168.10.255	255.255.255.255	On-link	192.168.10.10	281
224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	192.168.10.10	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	192.168.10.10	281

- En Windows, route print o netstat -r muestra la tabla de enrutamiento de PC
- Tres secciones mostradas por estos dos comandos:
  - Lista de interfaces: todas las interfaces potenciales y direccionamiento MAC
  - Tabla de enrutamiento IPv4
  - Tabla de enrutamiento IPv6.

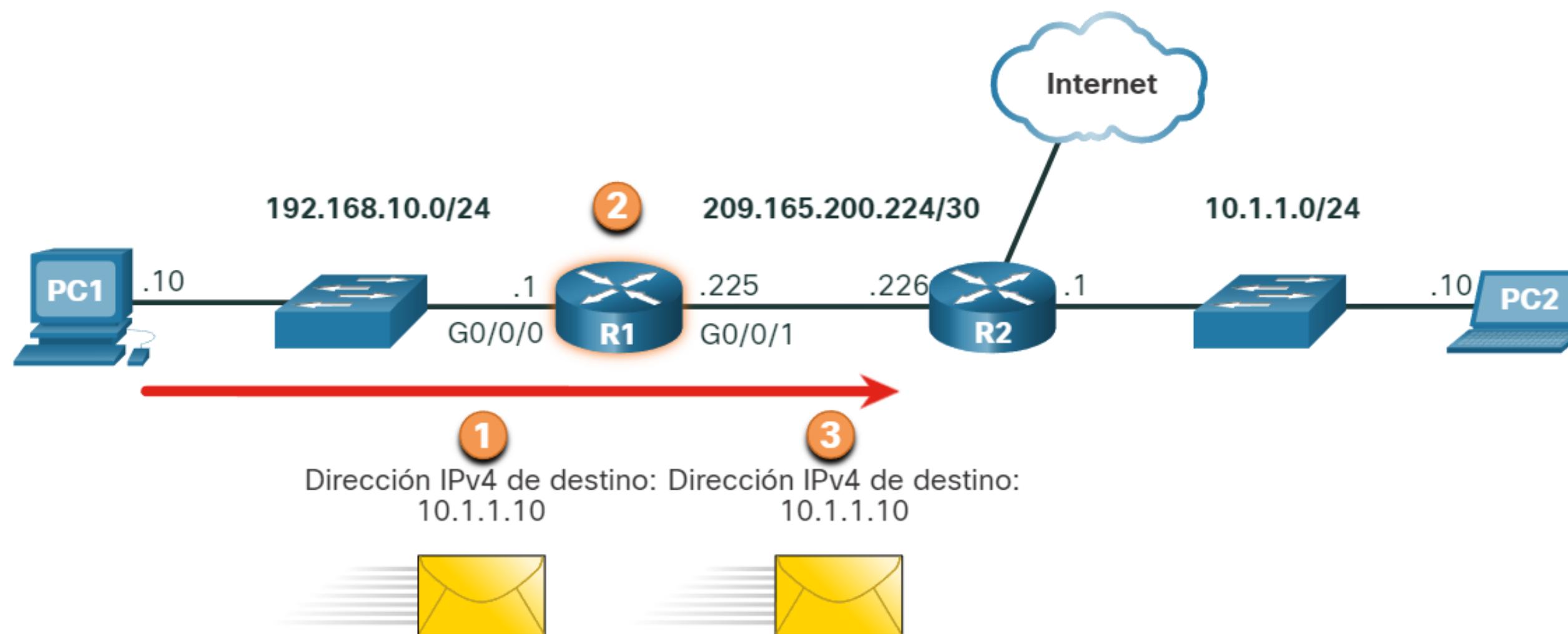


# Introducción al Enrutamiento

## Decisión de reenvío de paquetes del enrutador

¿Qué sucede cuando el enrutador recibe la trama del dispositivo host?

1. El paquete llega a la interfaz Gigabit Ethernet 0/0/0 del router R1. R1 desencapsula el encabezado Ethernet de Capa 2 y el remolque.
2. El router R1 examina la dirección IPv4 de destino del paquete y busca la mejor coincidencia en su tabla de enrutamiento IPv4. La entrada de ruta indica que este paquete se reenviará al router R2.
3. El router R1 encapsula el paquete en un nuevo encabezado Ethernet y remolque, y reenvía el paquete al siguiente router de salto R2.



R1 Routing Table

Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	vía R2
Default Route 0.0.0.0/0	vía R2



# Introducción al enrutamiento

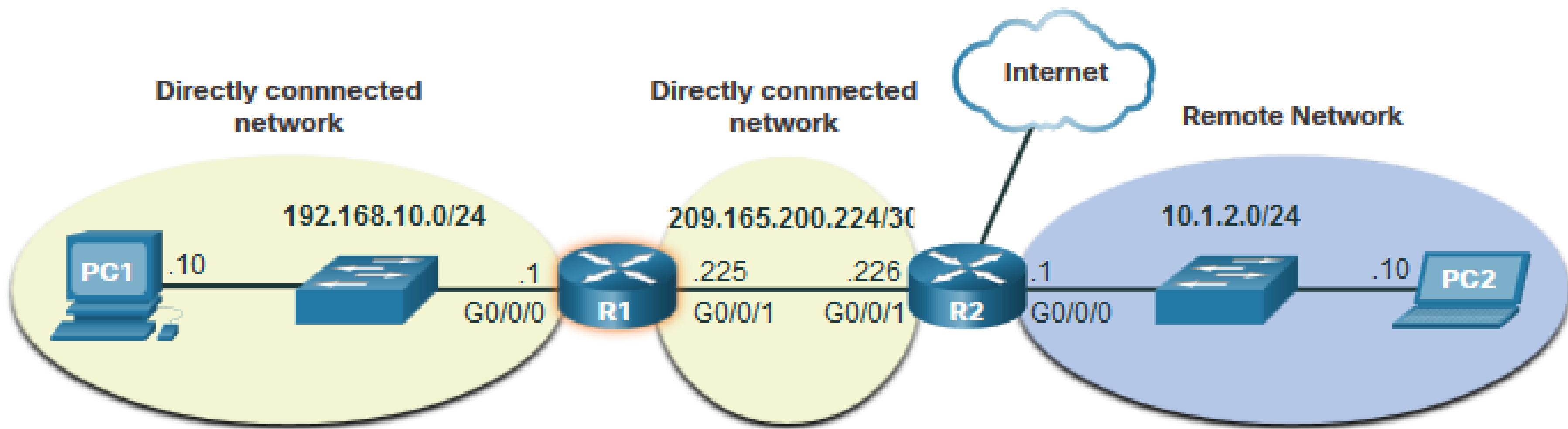
## Tabla de enrutamiento IP del router

Hay tres tipos de rutas en la tabla de enrutamiento de un enrutador:

- **Conectado directamente** — Estas rutas son agregadas automáticamente por el router, siempre que la interfaz esté activa y tenga direccionamiento.
- **Remoto** — Estas son las rutas que el router no tiene una conexión directa y se pueden aprender:
  - Manualmente — con una ruta estática
  - Dinámicamente: mediante el uso de un protocolo de enrutamiento para que los routers compartan su información entre sí
- **Ruta predeterminada** : reenvía todo el tráfico a una dirección específica cuando no hay coincidencia en la tabla de enrutamiento



# Introducción al enruteamiento **EJEMPLO**

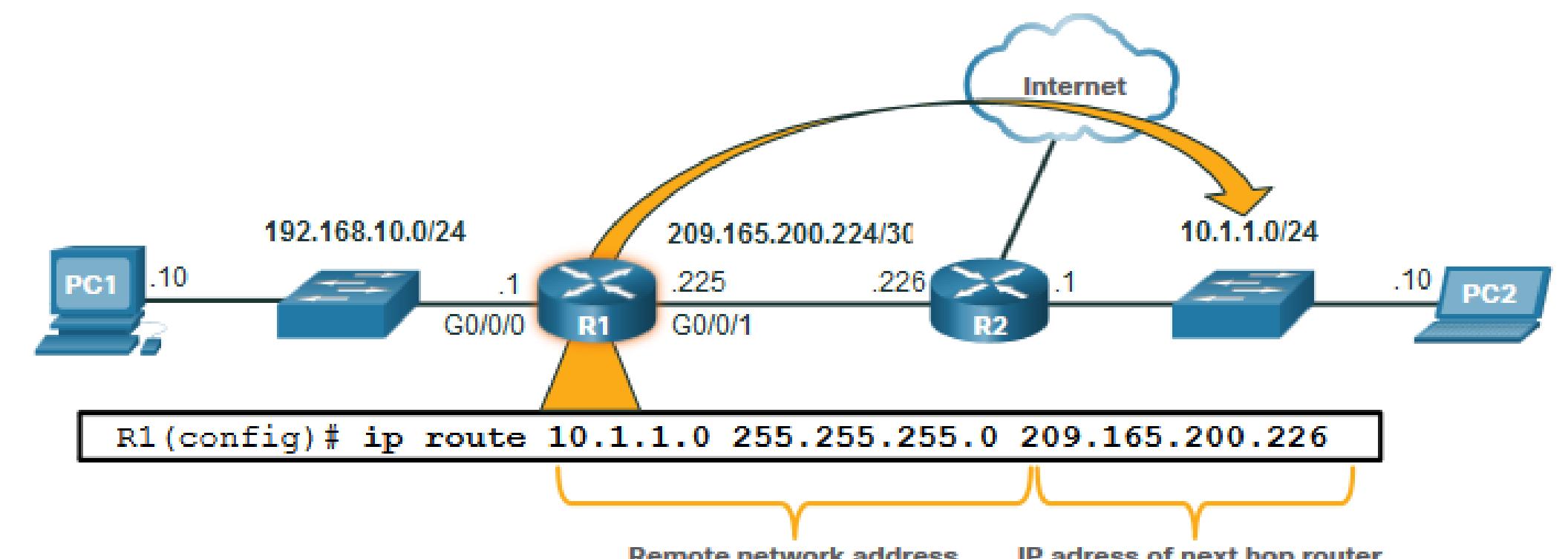




# Introducción al enrutamiento Enrutamiento estático

## Características de la ruta estática:

- Debe configurarse manualmente.
- Debe ser ajustado manualmente por el administrador cuando hay un cambio en la topología
- Bueno para redes pequeñas no redundantes
- Se utiliza a menudo junto con un protocolo de enrutamiento dinámico para configurar una ruta predeterminada

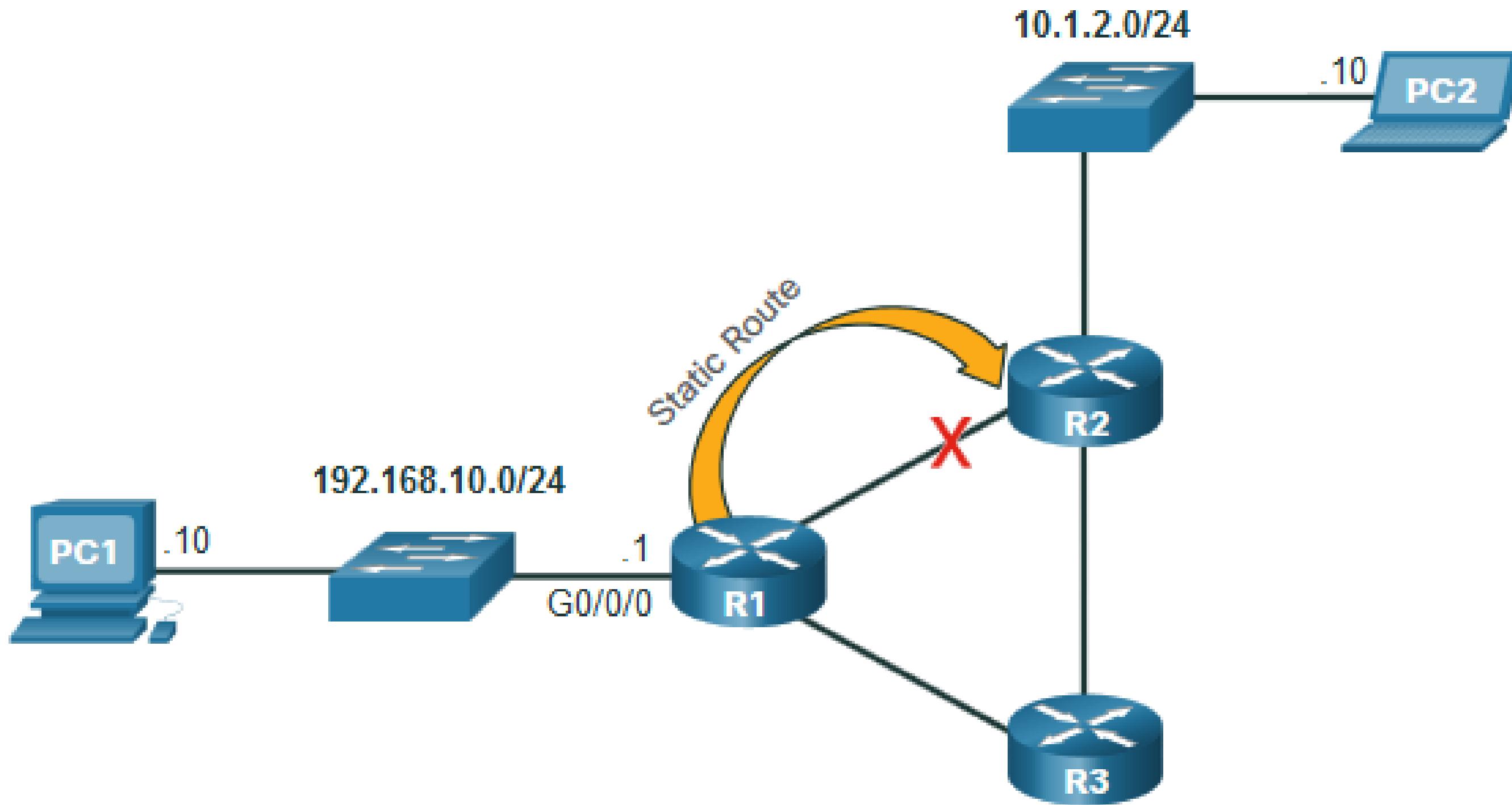


R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.



# Introducción al enrutamiento

## Enrutamiento estático



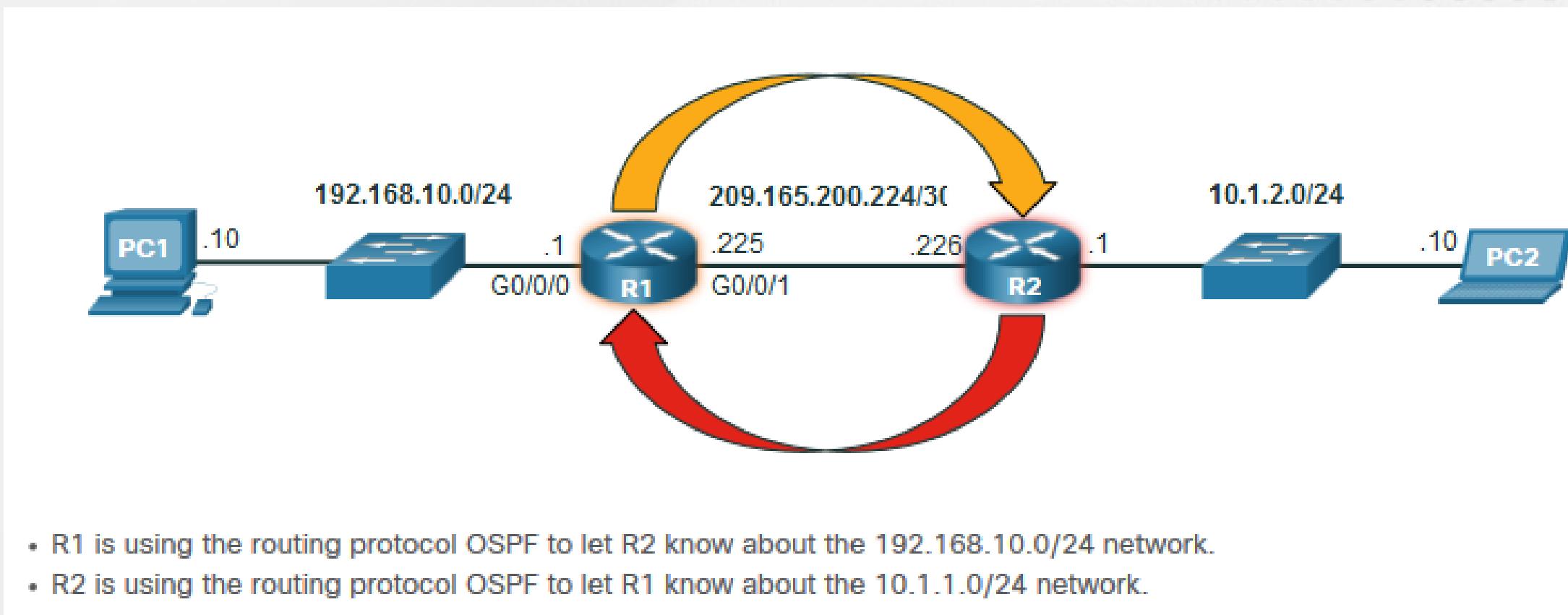


# Introducción al enrutamiento Enrutamiento dinámico

Rutas dinámicas automáticamente:

- Detectar redes remotas.
- Mantener información actualizada.
- Elija el mejor camino hacia las redes de destino
- Buscar nuevas rutas óptimas cuando hay un cambio de topología

El enrutamiento dinámico también puede compartir rutas estáticas predeterminadas con los otros routers.

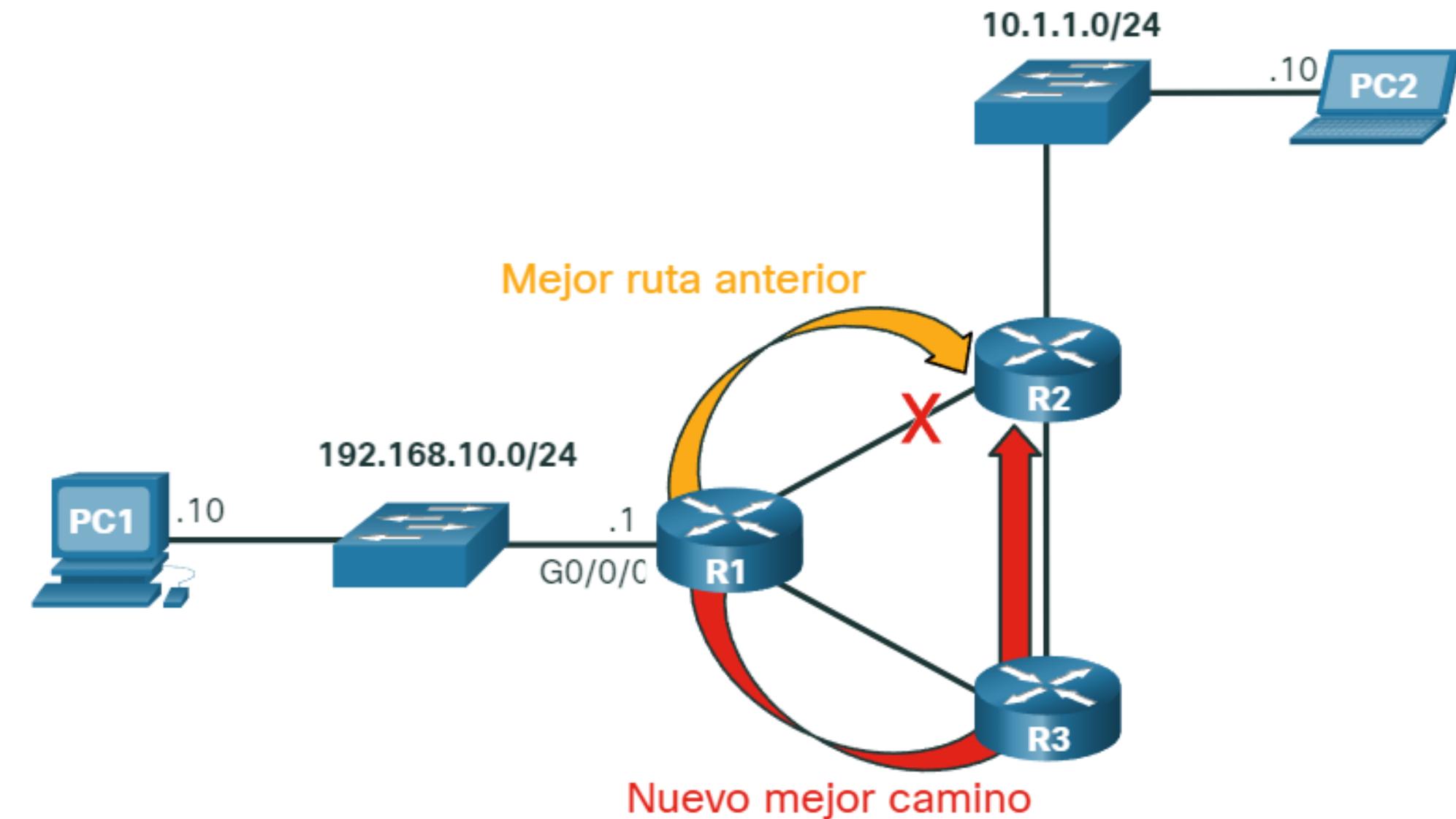




# Introducción al enrutamiento

## Enrutamiento dinámico

Cuando un router se configura manualmente con una ruta estática o aprende acerca de una red remota dinámicamente mediante un protocolo de enrutamiento dinámico, la dirección de red remota y la dirección de salto siguiente se introducen en la tabla de enrutamiento IP. Como se muestra en la figura, si hay un cambio en la topología de red, los routers se ajustarán automáticamente e intentarán encontrar una nueva mejor ruta.





El comando **show ip route** muestra los siguientes orígenes de ruta:

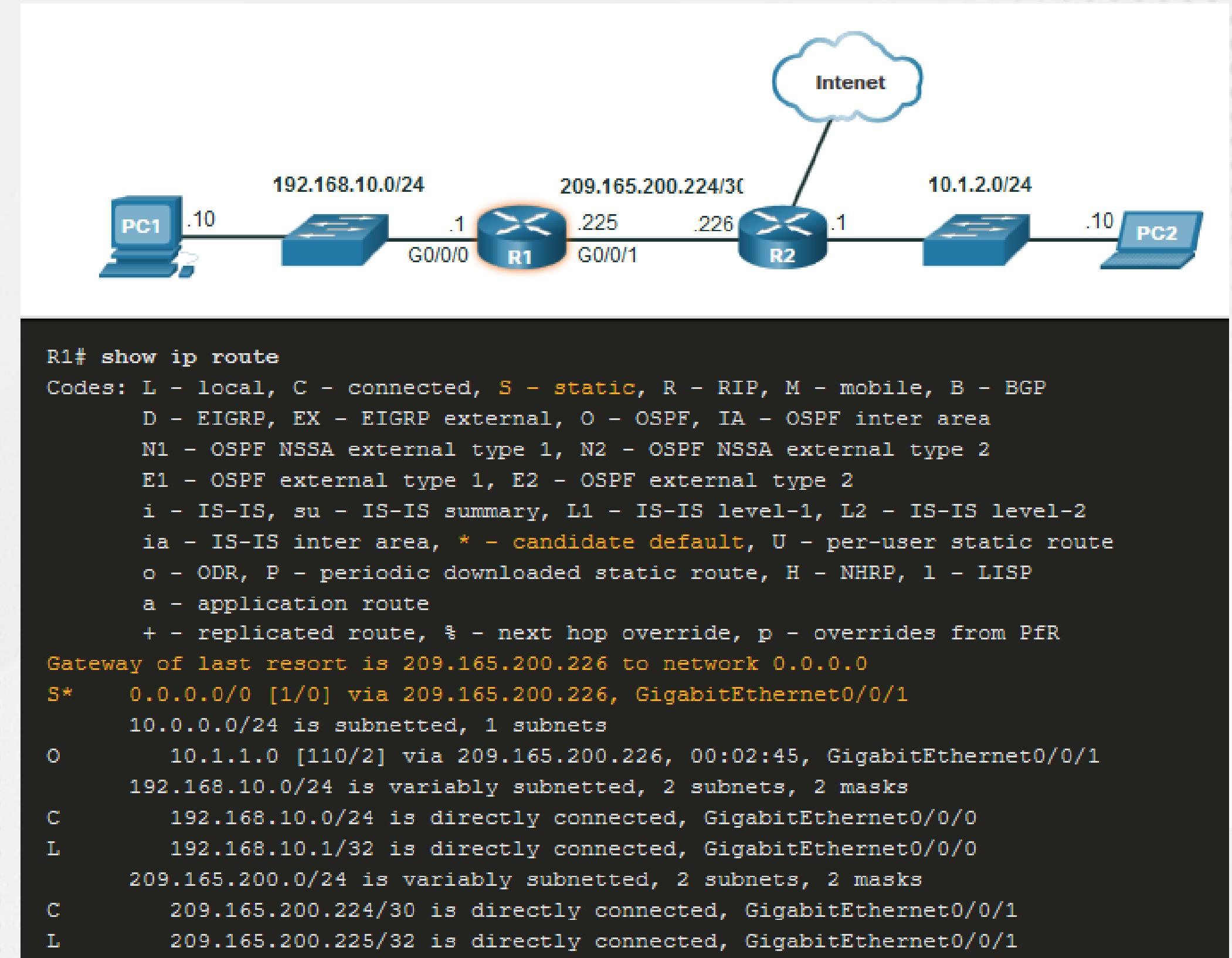
- **L** - Dirección IP de interfaz local conectada directamente
- **C** – Red conectada directamente
- **S** — La ruta estática fue configurada manualmente por un administrador
- **O** – OSPF
- **D** – EIGRP

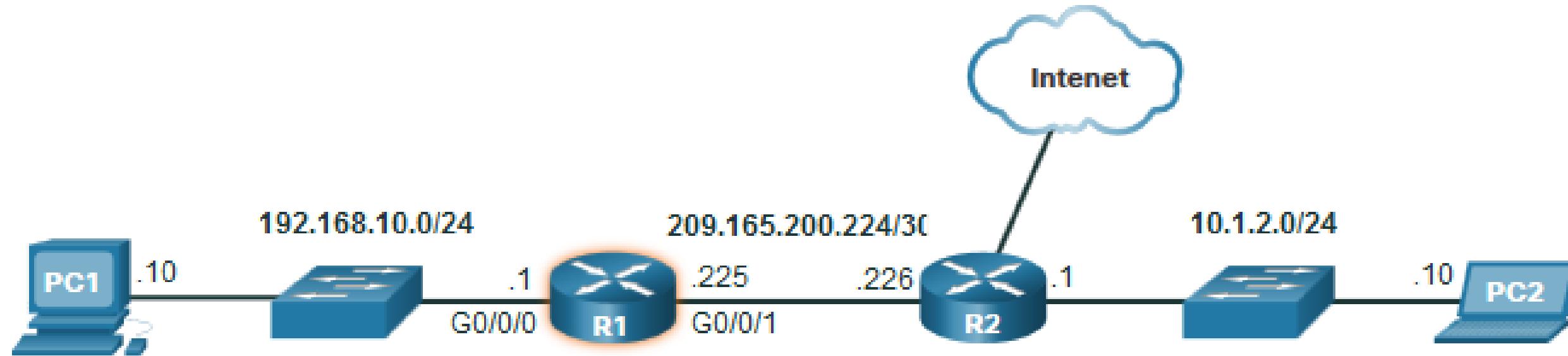
Este comando muestra los tipos de rutas:

- Conectado directamente – C and L
- Rutas remotas – O, D, etc.
- Rutas predeterminadas – S\*

# Introducción al enruteamiento

## Introducción a una tabla de enruteamiento 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
      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, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
        O     10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
        C     192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
        L     192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
        C     209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
        L     209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
```



# Capa de red Nuevos Términos y Comandos

- netstat –r
- route print
- interface list
- IPv4 Route Table
- IPv6 Route Table
- directly-connected routes
- remote routes
- default route
- **show ip route**
- route source
- destination network
- outgoing interface
- administrative distance
- metric
- next-hop
- route timestamp



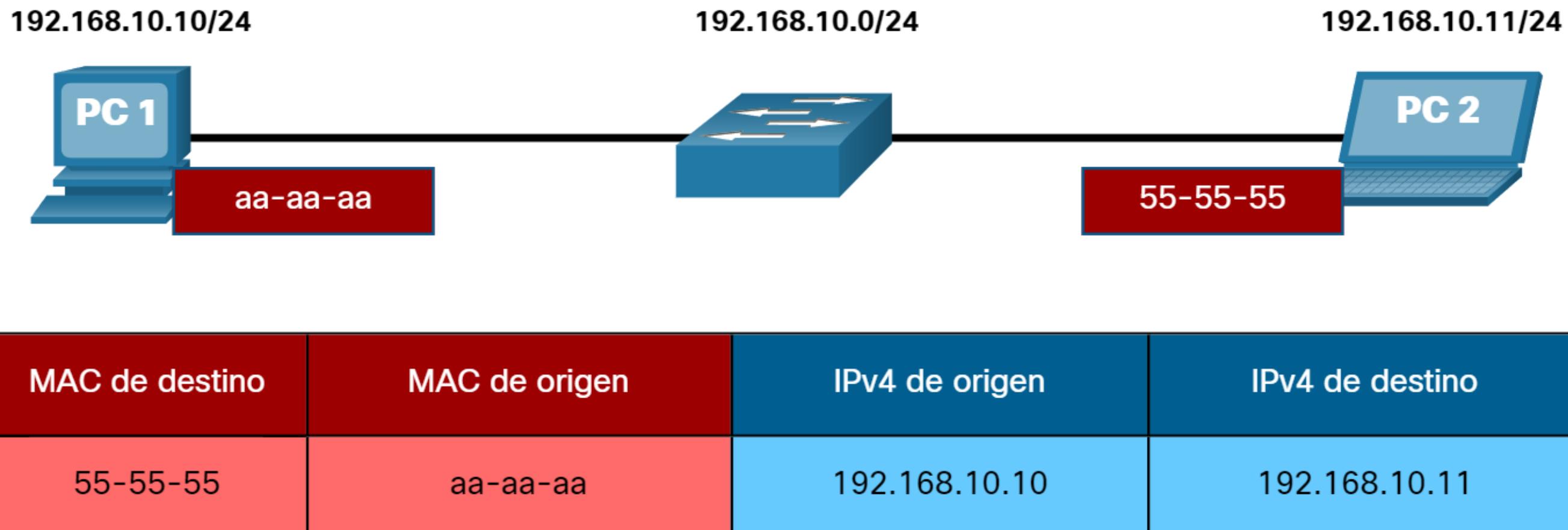
# RESOLUCIÓN DE DIRECCIÓN

# MAC e IP Destino en la misma red

Hay dos direcciones principales asignadas a un dispositivo en una LAN Ethernet:

- **Dirección física de capa 2 (la dirección MAC):**– se utiliza para comunicaciones NIC a NIC en la misma red Ethernet.
- **Dirección lógica de capa 3 (la dirección IP):**– Se utiliza para enviar el paquete desde el dispositivo de origen al dispositivo de destino.

Las direcciones de capa 2 se utilizan para entregar tramas desde una NIC a otra NIC en la misma red. Si una dirección IP de destino está en la misma red, la dirección MAC de destino será la del dispositivo de destino.

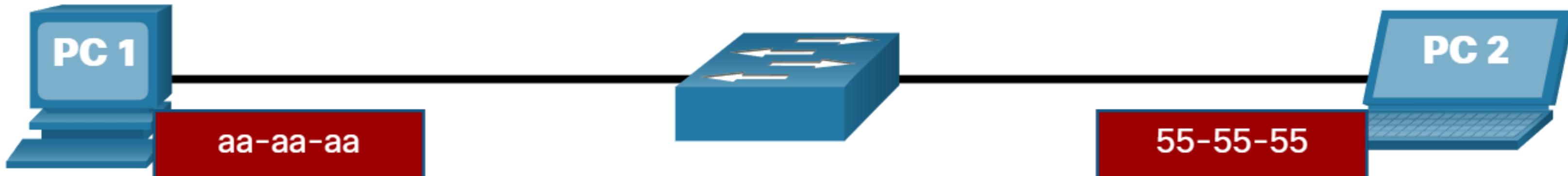




192.168.10.10/24

192.168.10.0/24

192.168.10.11/24

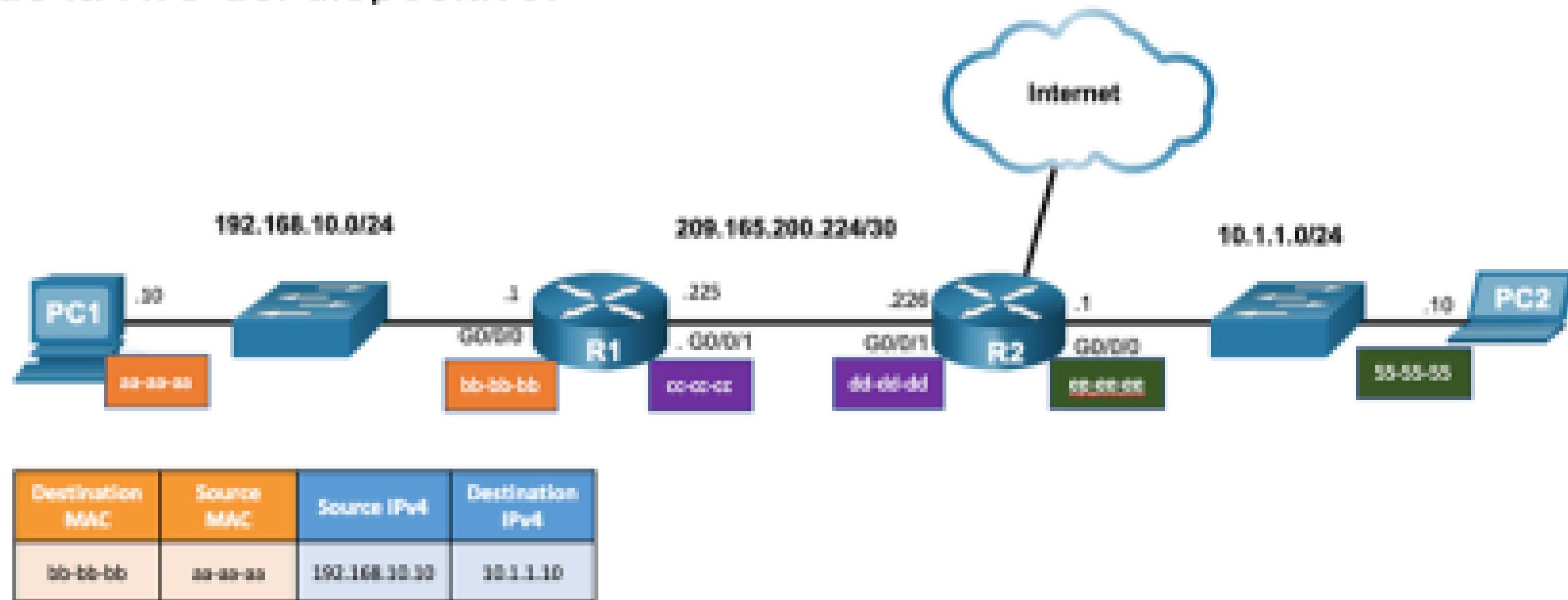


MAC de destino	MAC de origen	IPv4 de origen	IPv4 de destino
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

# MAC e IP Destino en una red remota

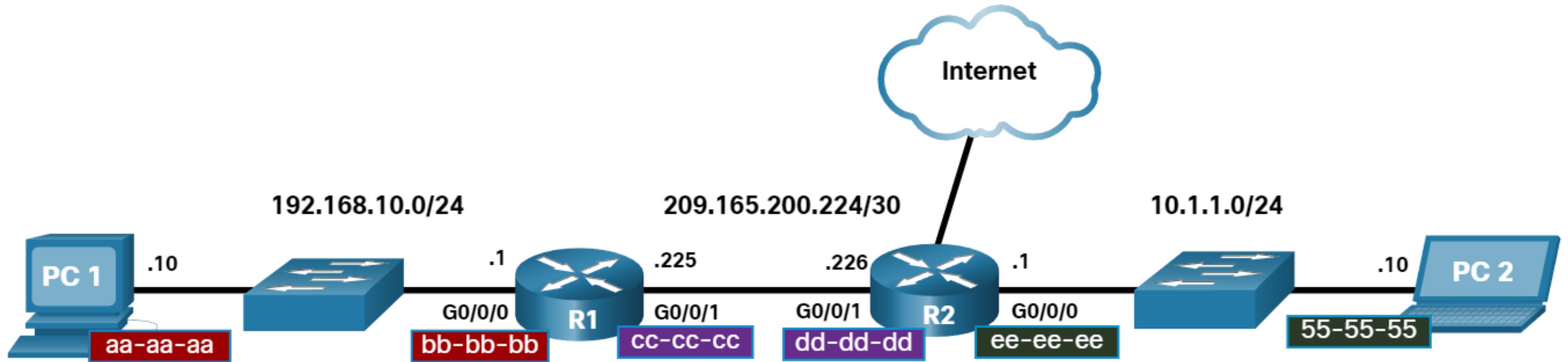
Cuando la dirección IP de destino está en una red remota, la dirección MAC de destino es la de la puerta de enlace predeterminada.

- IPv4 utiliza ARP para asociar la dirección IPv4 de un dispositivo con la dirección MAC de la NIC del dispositivo.
- IPv6 utiliza ICMPv6 para asociar la dirección IPv6 de un dispositivo con la dirección MAC de la NIC del dispositivo.



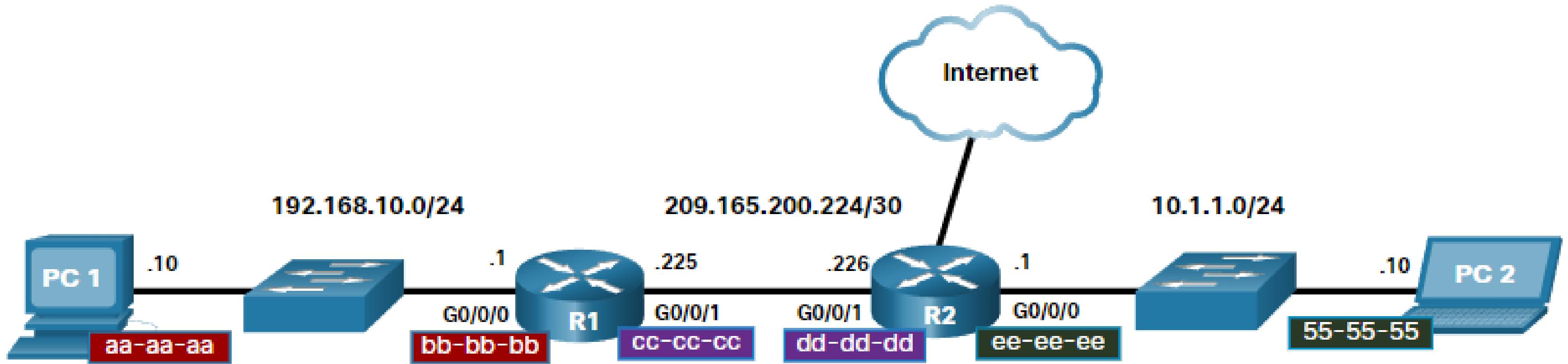
Información confidencial de Cisco

13



MAC de destino	MAC de origen	IPv4 de origen	IPv4 de destino
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

MAC de destino	MAC de origen	IPv4 de origen	IPv4 de destino
dd-dd-dd	cc-cc-cc	192.168.10.10	10.1.1.10



MAC de destino	MAC de origen	IPv4 de origen	IPv4 de destino
55-55-55	ee-ee-ee	192.168.10.10	10.1.1.10



# ¿PREGUNTAS?