

Redes y Sistemas Distribuidos

Tema 6.1

Nivel de Red



Contenidos

1. Introducción a las redes de computadores

- Concepto de Red
- Tipos de redes
- Direccionamiento
- Latencia

2. Redes de área local

- Concepto y tipos de redes locales
- Medios de transmisión
- Técnicas de contención

3. Red Ethernet

- Características
- Protocolos
- Estándares
- Direcciones
- Codificación

4. Interconexión de redes

- Modos de interconexión
- Puentes
- *Spanning Tree*
- Switches

5. Red WLAN

- Topologías
- Espectro
- Nivel físico
- Protocolos
- Seguridad

6.1 Nivel del Red Internet

- Encaminamiento
- Fragmentación y reensamblaje

6.2 Direccionamiento IP

7. Arquitectura TCP/IP

- Estructura TCP/IP
- Elementos
- Direcciones IP
- Funcionalidades
- Protocolos
- NAT

8. Sistemas distribuidos

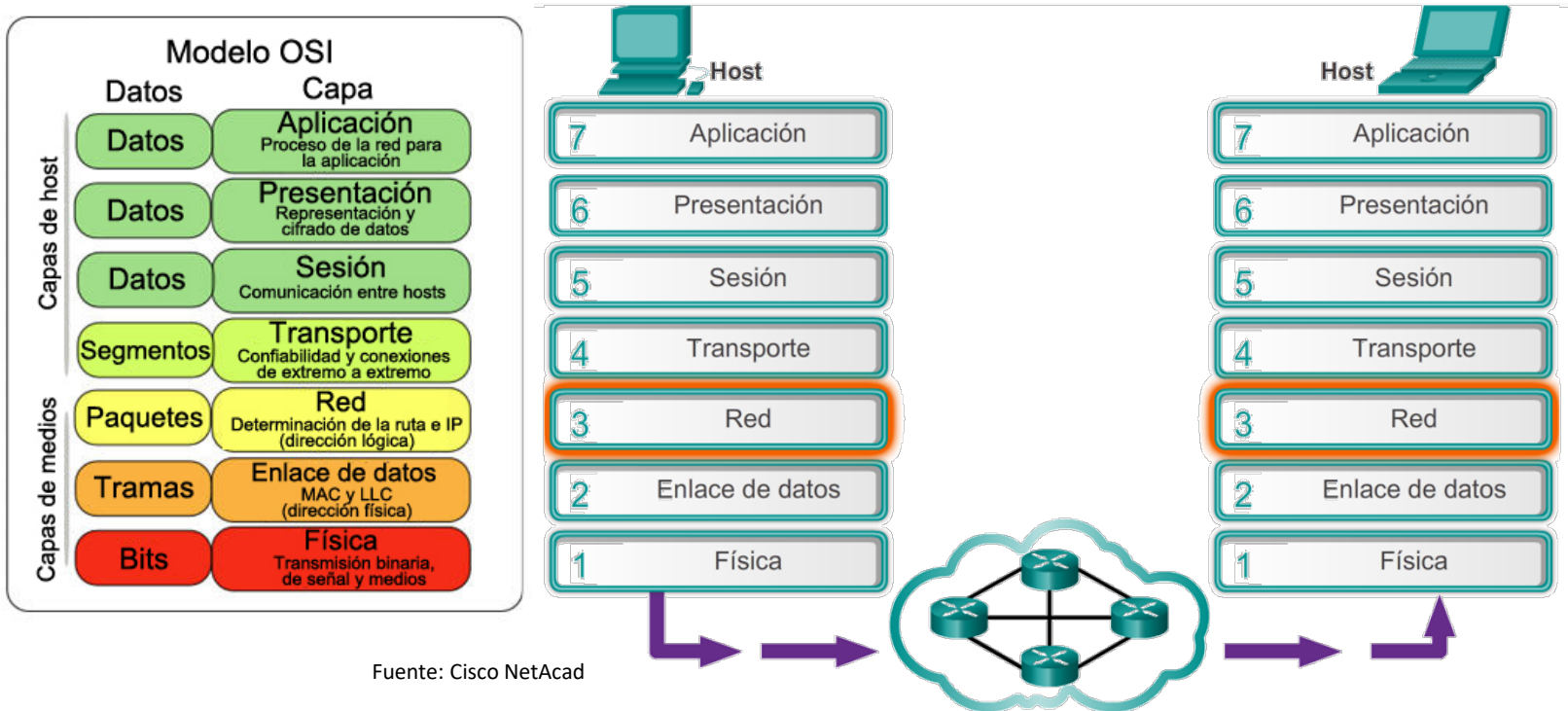
- Concepto
- Arquitectura cliente-servidor
- Arquitectura P2P

6.1 Nivel del Red Internet

- Introducción
 - Características de la capa de red
 - Formato de paquetes IPv4 e IPv6
- Encaminamiento
- Fragmentación y reensamblaje

La capa de red

La **capa de red** (capa 3 de OSI y TCP/IP) proporciona los servicios que permiten que los dispositivos finales intercambien datos a través de la red.



La capa de red

- 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 4 operaciones básicas:
 1. Direccionamiento de terminales
 2. Encapsulamiento
 3. Routing / Encaminamiento
 4. Desencapsulamiento

Características de IP

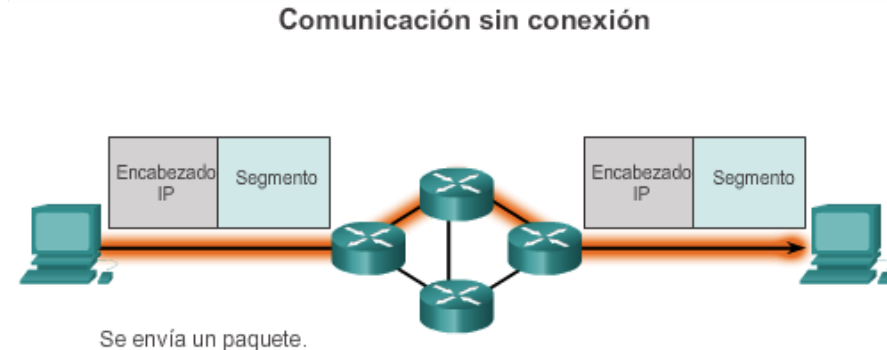
Características básicas del protocolo IP:

1. **Sin conexión:** NO se establece ninguna conexión con el destino antes de enviar los paquetes de datos.
2. **Máximo esfuerzo (no confiable):** La entrega de paquetes no está garantizada.
3. **Independiente de los medios:** La operación es independiente del medio que transporta los datos.

Características de IP: Sin conexión

1. Sin conexión (*Connectionless*)

- IP **no establece conexión** con el destino antes de enviar el paquete.
- No 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).



El emisor no sabe:

- Si el receptor está presente
- Si el paquete llegó
- Si el receptor puede leer el paquete

El receptor no sabe:

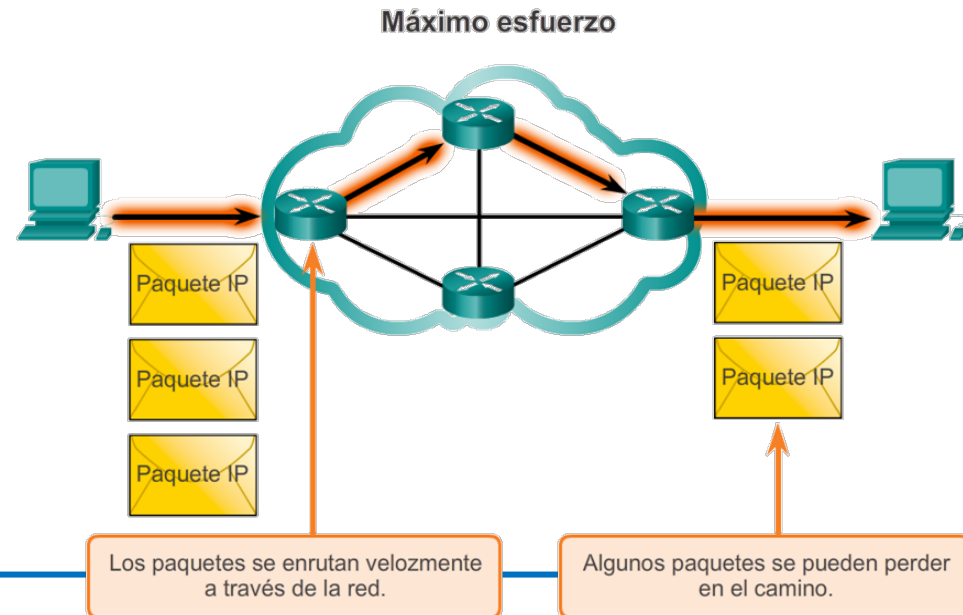
- Cuándo llegará

Fuente: Cisco NetAcad

Características de IP: Mejor esfuerzo

2. Mejor esfuerzo (*Best Effort*)

- 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.

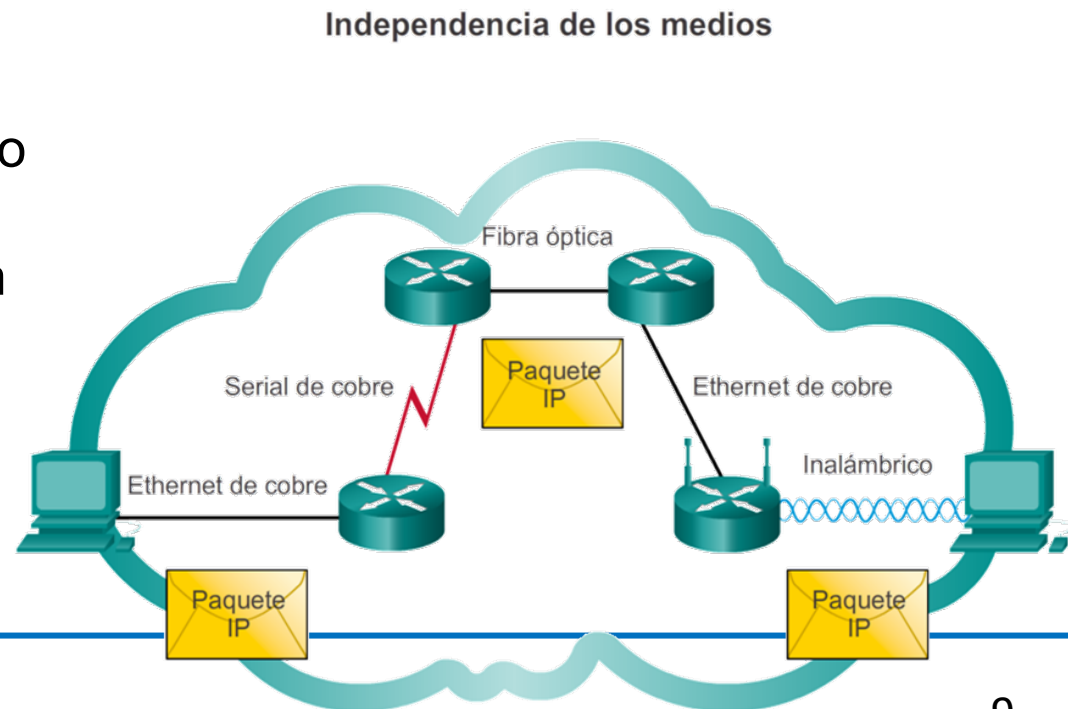


Fuente: Cisco NetAcad

Características de IP: Independencia de medios

3. Independencia de los medios

- Capa enlace prepara paquetes IP para transmisión por los medios.
- Tamaño máx. de PDU que medio puede transportar “unidad máxima de transmisión” (MTU).
- Dispositivos intermediarios dividen un paquete cuando reenvían de un medio a otro con MTU menor. Proceso denominado fragmentación de paquetes.

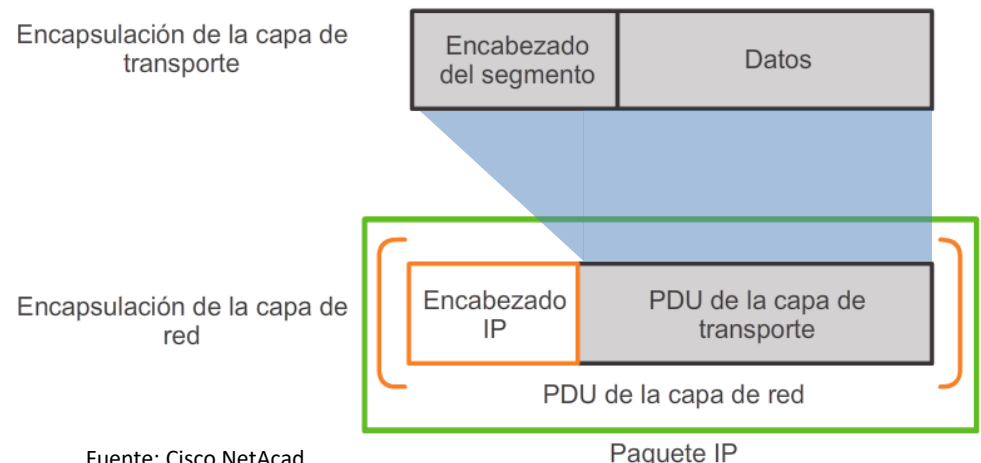


Encapsulación IP

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 (*Direccionamiento MAC en capa 2 – enlace si lo hacía*).

- **Nota:** NAT cambiará el direccionamiento, pero se discutirá más adelante



Formato de paquetes IPv4 e IPv6

Formato de los paquetes IPv4

Paquetes IPv4

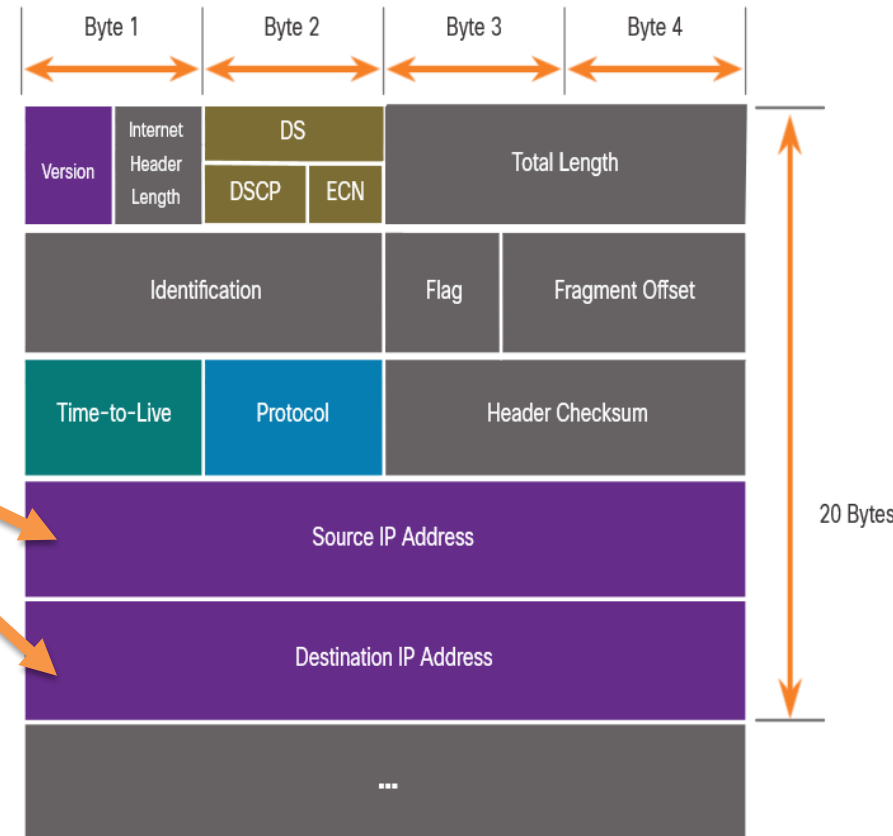
- IPv4 es el protocolo de comunicación principal de red.
- El encabezado de red tiene varios propósitos:
 - Garantiza que el paquete se envía en la dirección correcta.
 - Contiene información para el procesamiento de capas de red en varios campos.
 - La información del encabezado es utilizada por todos los dispositivos de capa 3 que manejan el paquete

Formato de los paquetes IPv4

Características encabezado IPv4:

- Está en binario
- Contiene varios campos
- 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.



Fuente: Cisco NetAcad

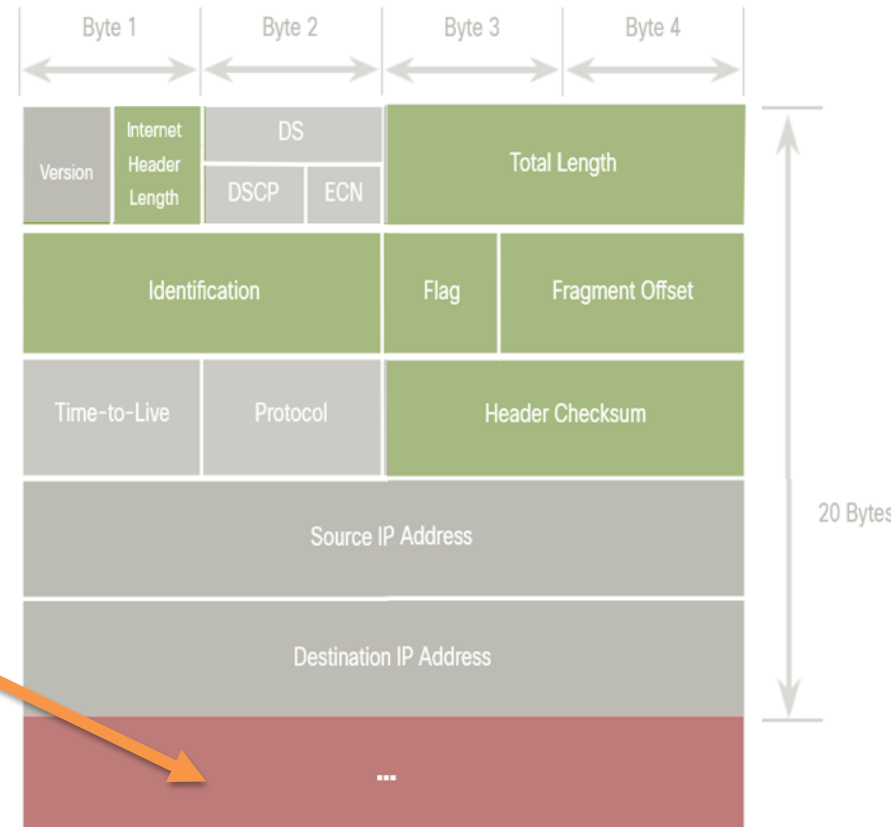
Campos de los paquetes IPv4

Campo	Descripción
Version	4 bits que identifican la <u>versión del paquete IP</u> . En IPv4, este campo siempre se establece en 0100
DS (Servicios diferenciados)	8 bits que determinan la <u>prioridad de cada paquete</u> . <ul style="list-style-type: none">• 6 bits: Punto de código de servicios diferenciados (DSCP), utilizado por un mecanismo de calidad de servicio (QoS).• 2 bits: Notificación explícita de congestión (ECN), utilizada para evitar descartar paquetes en momentos de congestión de la red
TTL (Tiempo de vida)	8 bits utilizados para limitar la <u>vida útil de un paquete</u> . Valor inicial de TTL disminuye un punto por cada salto, es decir, cada vez que el paquete es procesado por un router. Si el campo TTL disminuye a cero, el router descarta el paquete y envía un mensaje del protocolo de mensajes de control de Internet (ICMP) de Tiempo superado a IP de origen
Protocol	8 bits indica el <u>tipo de contenido de datos que transporta el paquete</u> , lo que permite que la capa de red pase los datos al protocolo superior correspondiente. ICMP (1), TCP (6) y UDP (17)

Formato de los paquetes IPv4

Los campos restantes se utilizan para identificar y validar el paquete, o para volver a ordenar un paquete fragmentado.

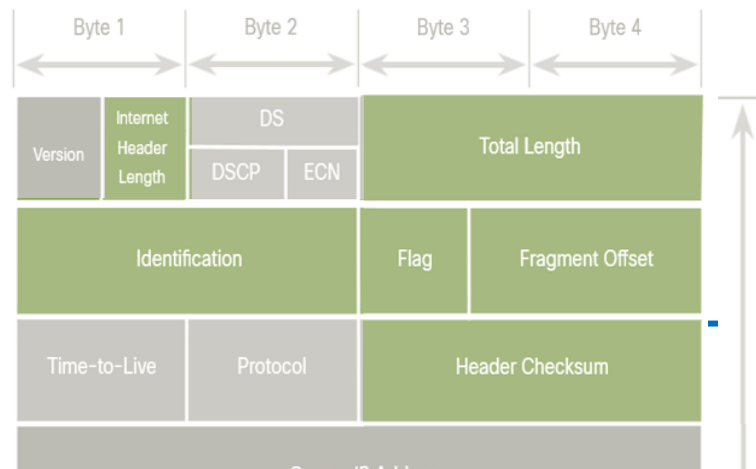
Nota: los campos Opciones y Relleno se utilizan con poca frecuencia.



Fuente: Cisco NetAcad

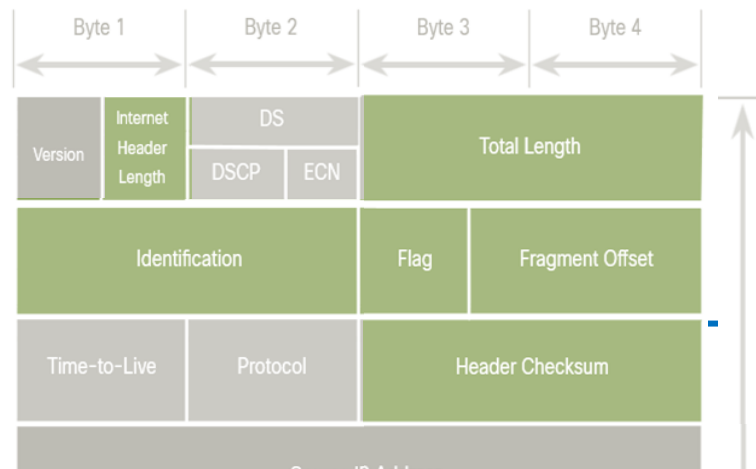
Campos de los paquetes IPv4

Campo	Descripción
IHL (Longitud del encabezado de Internet)	4 bits que identifica la <u>cantidad de palabras de 32 bits en el encabezado</u> . El valor de IHL varía según los campos Opciones y Relleno. <ul style="list-style-type: none"> - El valor mínimo para este campo es 5 ($5 \times 32 = 160$ bits = 20 bytes) - El máximo es 15 ($15 \times 32 = 480$ bits = 60 bytes)
Total Length	16 bits. Denominado también " <u>Longitud del paquete</u> ". Define el tamaño total en bytes del paquete (fragmento), incluidos encabezado y datos. <ul style="list-style-type: none"> - Longitud mínima es 20 bytes (encabezado 20 bytes + datos 0 bytes) - Longitud máxima es de 65.535 bytes
Header checksum	16 bits para la <u>verificación de errores del encabezado IP</u> . El checksum del encabezado se vuelve a calcular y se compara con el valor en el campo checksum. Si los valores no coinciden, se descarta el paquete



Campos de los paquetes IPv4

Campo	Descripción
Identification	16 bits identifican el <u>fragmento de un paquete IP original</u> .
Flag	3 bits identifican <u>cómo se fragmenta el paquete</u> . Se utiliza con los campos Fragment Offset e Identification para ayudar a reconstruir el paquete original con el fragmento.
Fragment Offset	13 bits identifican <u>orden en que se debe colocar el fragmento del paquete</u> en la reconstrucción del paquete original sin fragmentar.



Limitaciones de IPv4

IPv4 tiene **3 limitaciones** principales:

1. **Agotamiento de direcciones IPv4:** básicamente nos hemos quedado sin direccionamiento IPv4.
2. **Falta de conectividad de extremo a extremo:** Para permitir que IPv4 sobreviva todo este largo tiempo, se crearon direcciones privadas y NAT. Esto puso fin a comunicaciones directas.
3. **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 también un aumento de latencia.

Introducción a IPv6

Paquetes IPv6

IPv6 desarrollado por *Internet Engineering Task Force* (IETF) con la finalidad de superar limitaciones IPv4. Introduce mejoras:



- **Mayor espacio de direcciones:** Basado en la dirección de **128 bits** en lugar de las de **32 bits** de IPv4
- **Manejo mejorado de paquetes:** El encabezado se ha simplificado con menos campos
- **Elimina la necesidad de NAT:** Dado el amplio rango para direccionamiento, no es necesario utilizar direccionamiento privado internamente y direcciones públicas compartidas

Comparación espacio de direcciones IPv4 / IPv6

IPv4 and IPv6 Address Space Comparison

Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^3	1,000
1 Million	10^6	1,000,000
1 Billion	10^9	1,000,000,000
1 Trillion	10^{12}	1,000,000,000,000
1 Quadrillion	10^{15}	1,000,000,000,000,000
1 Quintillion	10^{18}	1,000,000,000,000,000,000
1 Sextillion	10^{21}	1,000,000,000,000,000,000,000
1 Septillion	10^{24}	1,000,000,000,000,000,000,000,000
1 Octillion	10^{27}	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^{30}	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^{33}	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^{36}	1,000,000,000,000,000,000,000,000,000,000,000,000

Legend

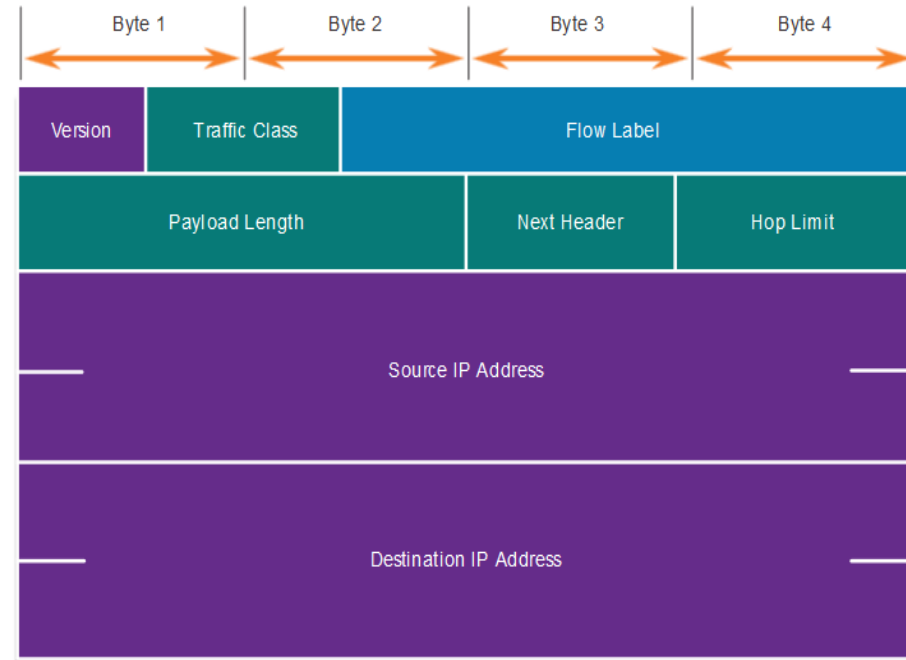
-  There are 4 billion IPv4 addresses
-  There are 340 undecillion IPv6 addresses

Fuente: Cisco NetAcad

Formato de los paquetes IPv6

Encabezado IPv6 se simplifica, pero no es más pequeño (40 Bytes frente a 20)

- Se eliminaron varios campos IPv4 para mejorar el rendimiento:
 - Identification
 - Fragment Offset
 - Header Checksum
- Puede contener encabezados de extensión (EH) opcionales
 - Proporcionar información de capa de red
 - Colocados entre encab. IPv6 y carga útil
 - Usados para seguridad, movilidad, etc.
- **Nota:** A diferencia de IPv4, los Routers no fragmentan los paquetes IPv6.



Fuente: Cisco NetAcad

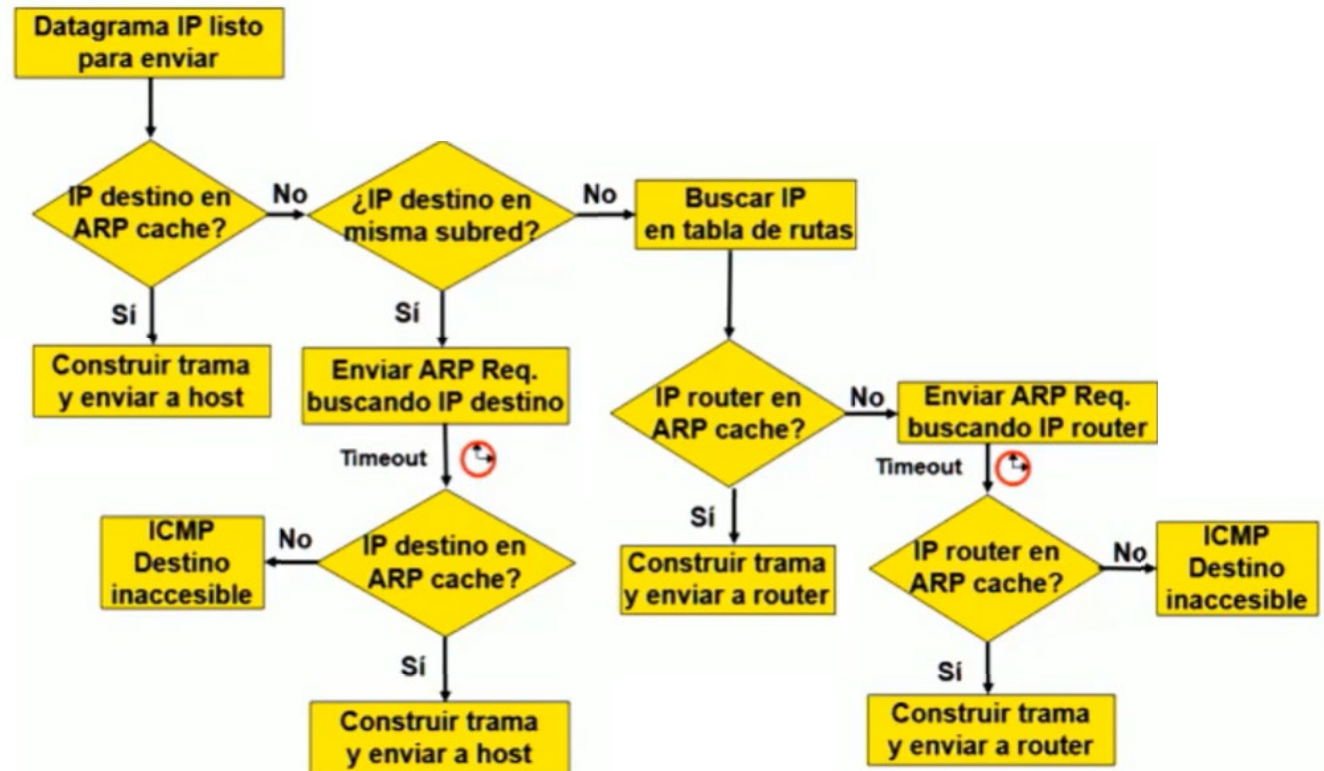
Campos de los paquetes IPv6

Campo	Descripción
Version	4 bits que identifican la <u>versión del paquete IP</u> . Para IPv6, este campo siempre se establece en 0110
Traffic Class	8 bits <u>equivalente a campo DS de IPv4</u> . <ul style="list-style-type: none">- Punto de código de servicios diferenciados (DSCP), 6 bits para clasificar paquetes- Notificación explícita de congestión (ECN), 2 bits para controlar la congestión del tráfico
Flow Label	20 bits proporcionan un <u>servicio especial para aplicaciones en tiempo real</u> . Para indicar a los routers y switches que deben mantener la misma ruta para el flujo de paquetes, a fin de evitar que estos se reordenen
Payload Length	16 bits equivalente a Total Length de IPv4. Define el <u>tamaño total del paquete</u> (fragmento)
Next Header	8 bits equiv. Protocol IPv4. Indica el <u>tipo de contenido de datos transportado</u> , permitiendo que la capa de red pase los datos al protocolo de capa superior correspondiente. <u>También usado para agregar encabezados de extensión optativos al paquete</u>
Hop Limit	8 bits <u>reemplaza TTL IPv4</u> . Cuando cada router reenvía un paquete, este valor disminuye en un punto. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje de ICMPv6 al host emisor en el que se indica que el paquete no llegó a destino

Encaminamiento Del HOST

Envío de un datagrama IP por un host

Envío de un datagrama IP por un host



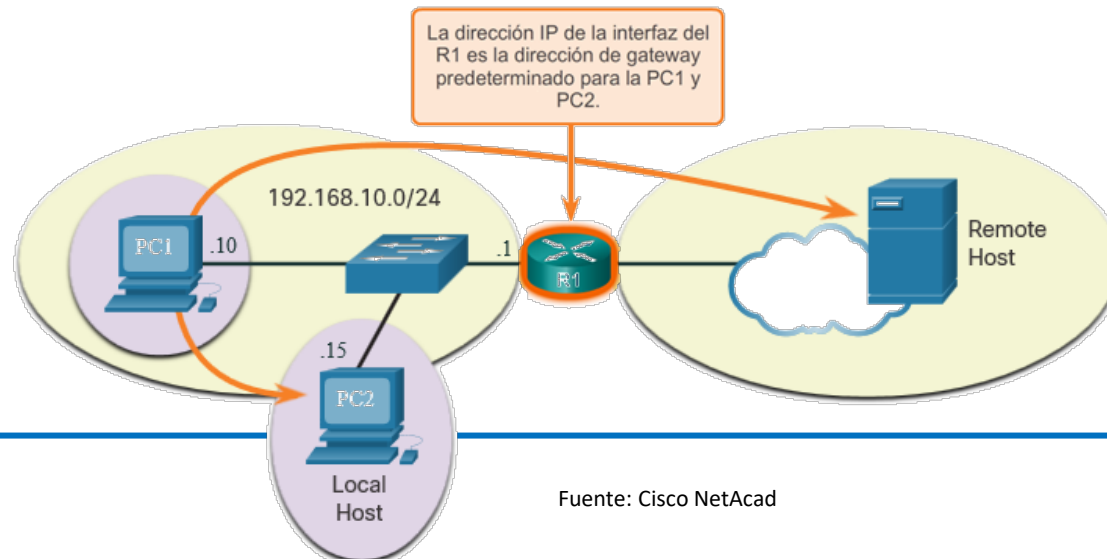
Rogelio Montañana



Decisión de reenvío de paquetes del Host

Host debe decidir que hacer con paquetes que envía

- 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:
 - **A sí mismo** — 127.0.0.1 (IPv4) y ::1 (IPv6)
 - **Hosts locales**: Destino está en la misma LAN
 - **Hosts remotos**: Dispositivos no están en la misma LAN



Decisión de reenvío de paquetes del Host

Host debe decidir que hacer con paquetes que envía

- 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 envía desde la interfaz de host para ser manejado por un dispositivo intermediario.
- El tráfico remoto se reenvía directamente a la puerta de enlace predeterminada de la LAN.

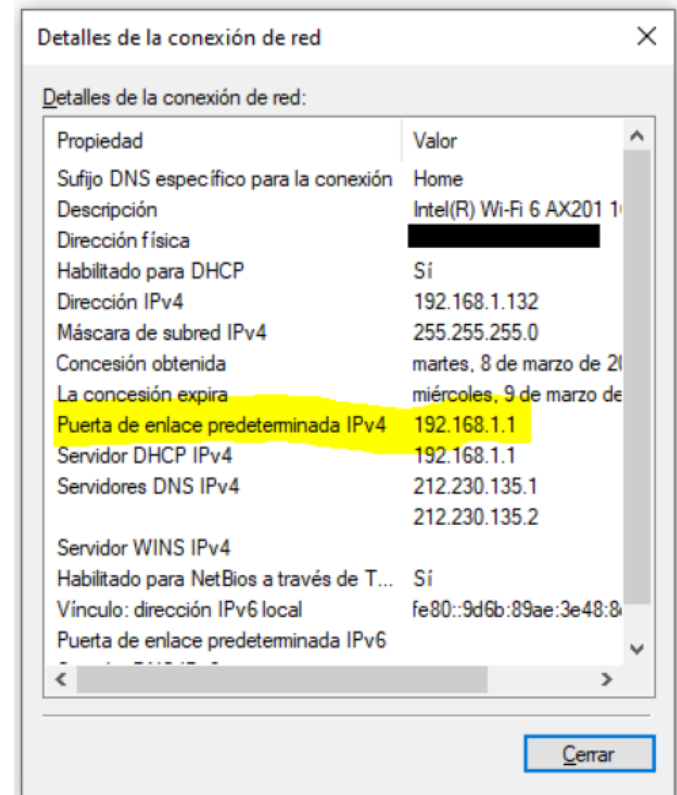
Gateway predeterminado para el Host

Router (capa 3) puede ser una **puerta de enlace predeterminada** (DGW).

Características DGW:

- Debe tener 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.

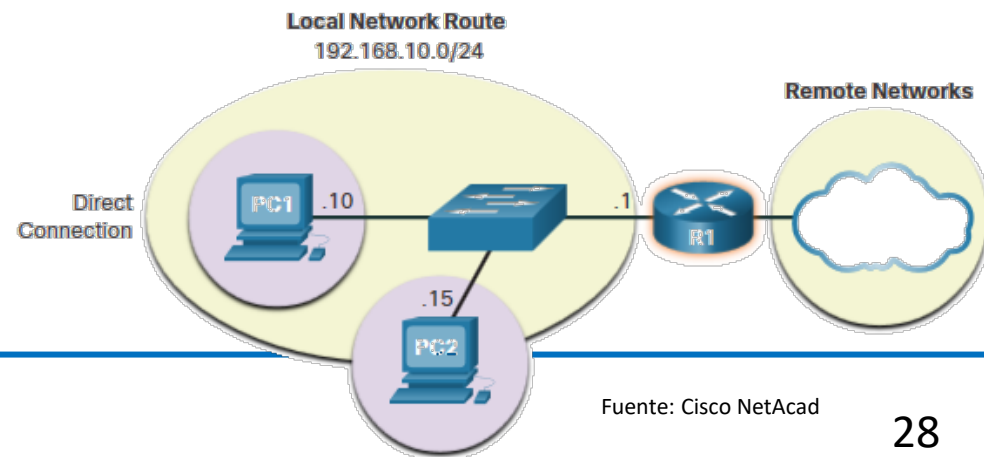
Si un dispositivo no tiene una puerta de enlace predeterminada o una puerta de enlace predeterminada incorrecta, su tráfico no podrá salir de la LAN.



Host enruta al DGW

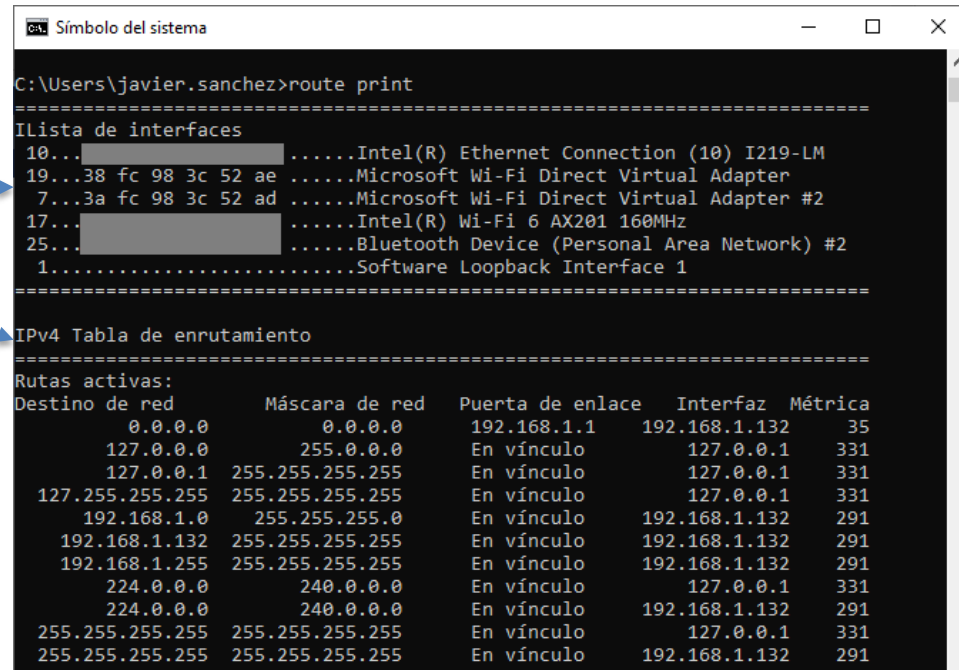
Envíos del Host al DWG

- 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 router si tienen la intención de enviar tráfico de forma remota.



Tablas de enrutamiento de Host

- En Windows, los comandos `route print` , `netstat -r` muestran la tabla de enrutamiento del equipo
- 3 secciones son mostradas:
 - Lista de interfaces: todas las interfaces potenciales y direccionamiento MAC
 - Tabla de enrutamiento IPv4
 - Tabla de enrutamiento IPv6



```
C:\Users\javier.sanchez>route print

=====
Lista de interfaces
10...[redacted] .....Intel(R) Ethernet Connection (10) I219-LM
19...38 fc 98 3c 52 ae .....Microsoft Wi-Fi Direct Virtual Adapter
7...3a fc 98 3c 52 ad .....Microsoft Wi-Fi Direct Virtual Adapter #2
17...[redacted] .....Intel(R) Wi-Fi 6 AX201 160MHz
25...[redacted] .....Bluetooth Device (Personal Area Network) #2
1.....Software Loopback Interface 1
=====

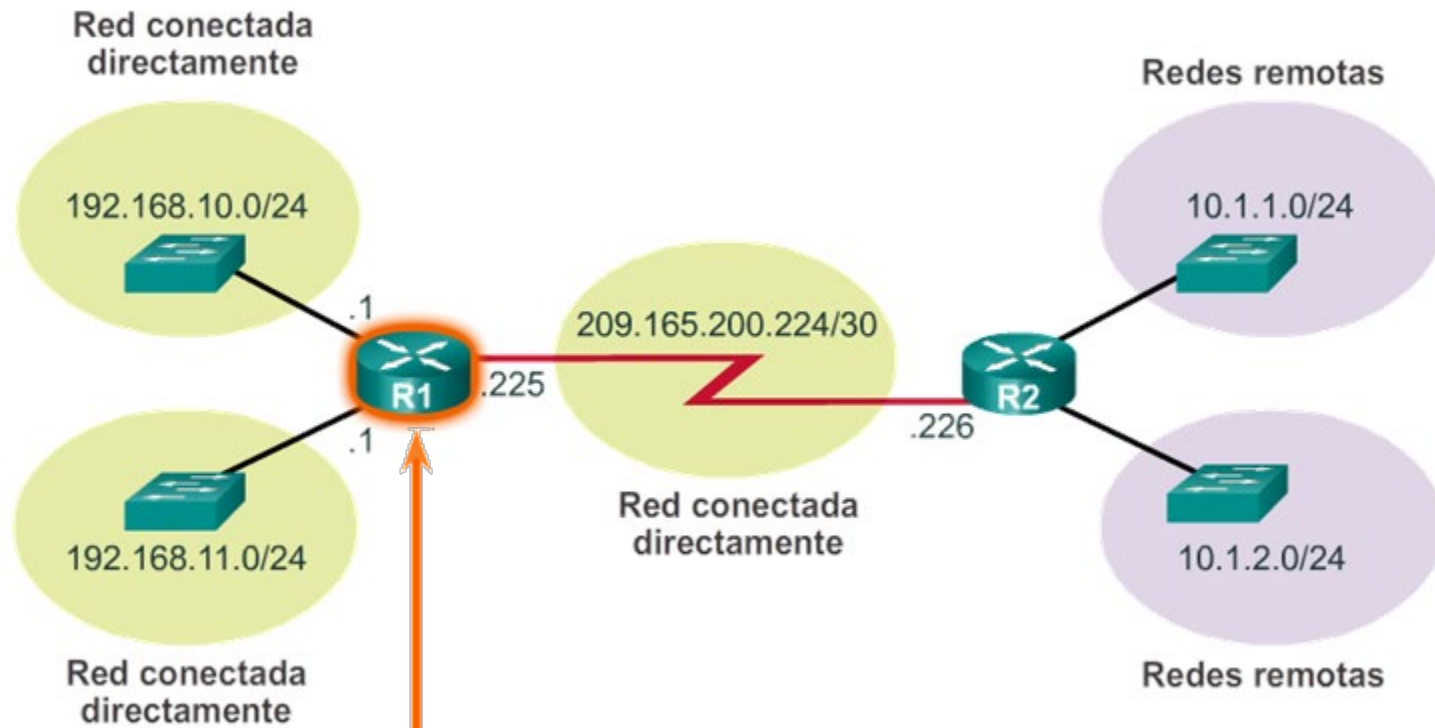
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace    Interfaz  Métrica
0.0.0.0             0.0.0.0             192.168.1.1         192.168.1.132    35
127.0.0.0           255.0.0.0           En vínculo          127.0.0.1        331
127.0.0.1           255.255.255.255     En vínculo          127.0.0.1        331
127.255.255.255     255.255.255.255     En vínculo          127.0.0.1        331
192.168.1.0         255.255.255.0       En vínculo          192.168.1.132    291
192.168.1.132       255.255.255.255     En vínculo          192.168.1.132    291
192.168.1.255       255.255.255.255     En vínculo          192.168.1.132    291
224.0.0.0           240.0.0.0           En vínculo          127.0.0.1        331
224.0.0.0           240.0.0.0           En vínculo          192.168.1.132    291
255.255.255.255     255.255.255.255     En vínculo          127.0.0.1        331
255.255.255.255     255.255.255.255     En vínculo          192.168.1.132    291
```

...

Encaminamiento ROUTER

Decisión de reenvío de paquetes del router

¿Qué sucede cuando el router recibe la trama de un dispositivo host?

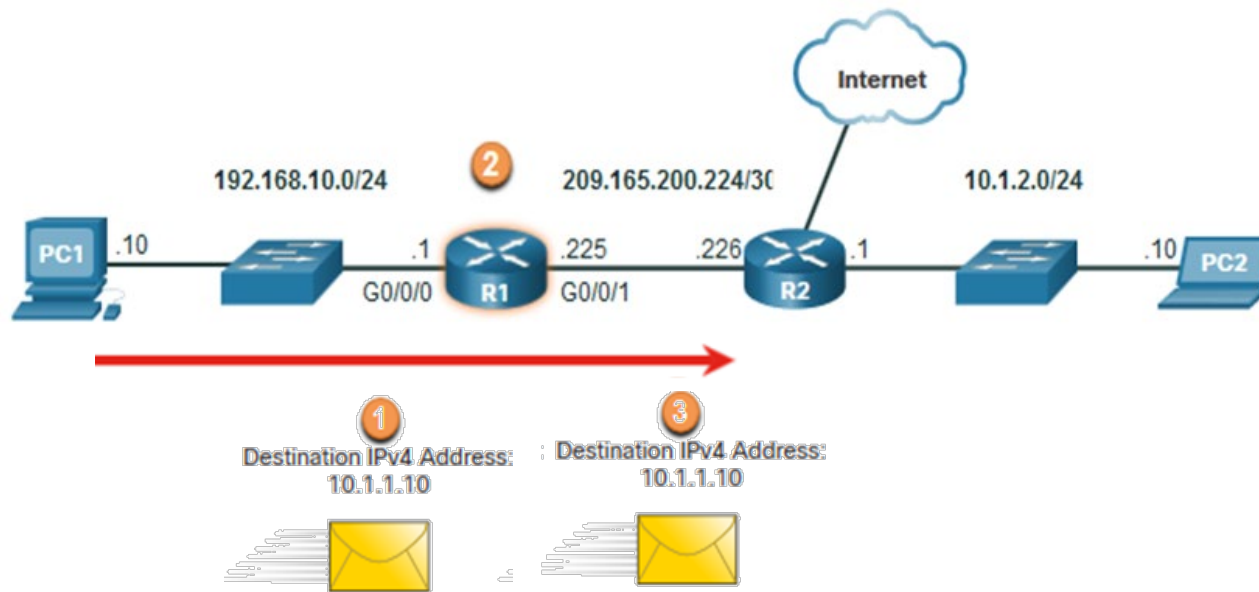


Fuente: Cisco NetAcad

El R1 tiene tres redes conectadas directamente: 192.168.10.0/24, 192.168.11.0/24 y 209.165.200.224/30. Además, el R1 tiene dos redes remotas que puede descubrir a partir del R2: 10.1.1.0/24 y 10.1.2.0/24.

Decisión de reenvío de paquetes del router

¿Qué sucede cuando el router recibe la trama de un dispositivo host?



R1 Routing Table

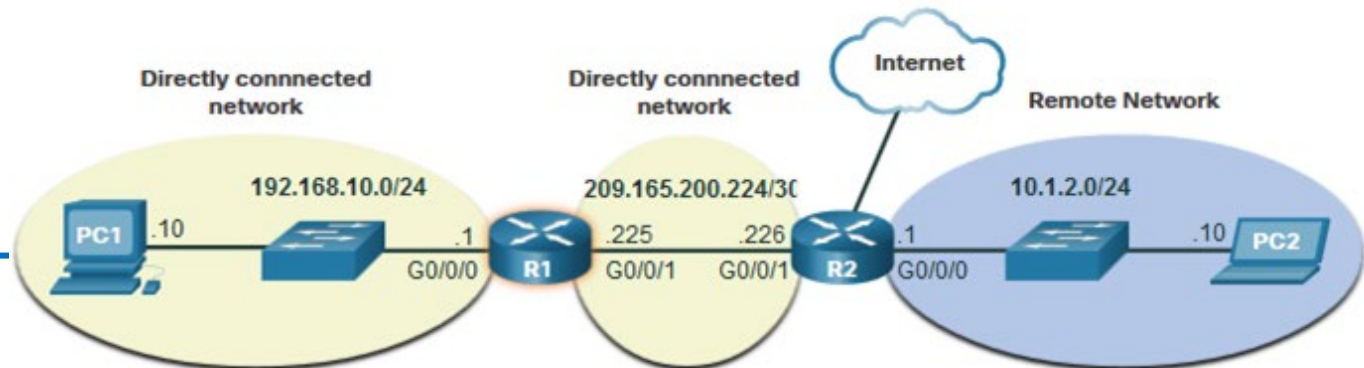
Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2
Default Route 0.0.0.0/0	via R2

1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

Tabla de enrutamiento IP del router

Hay tres tipos de rutas en la tabla de enrutamiento del router:

1. **Conectado directamente** — Estas rutas son agregadas automáticamente por el router, siempre que la interfaz esté activa y tenga direccionamiento.
2. **Remoto** — Estas son las rutas con las que el router no tiene una conexión directa. 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
3. **Ruta predeterminada** — reenvía todo el tráfico a una dirección específica cuando no hay coincidencia en la tabla de enrutamiento

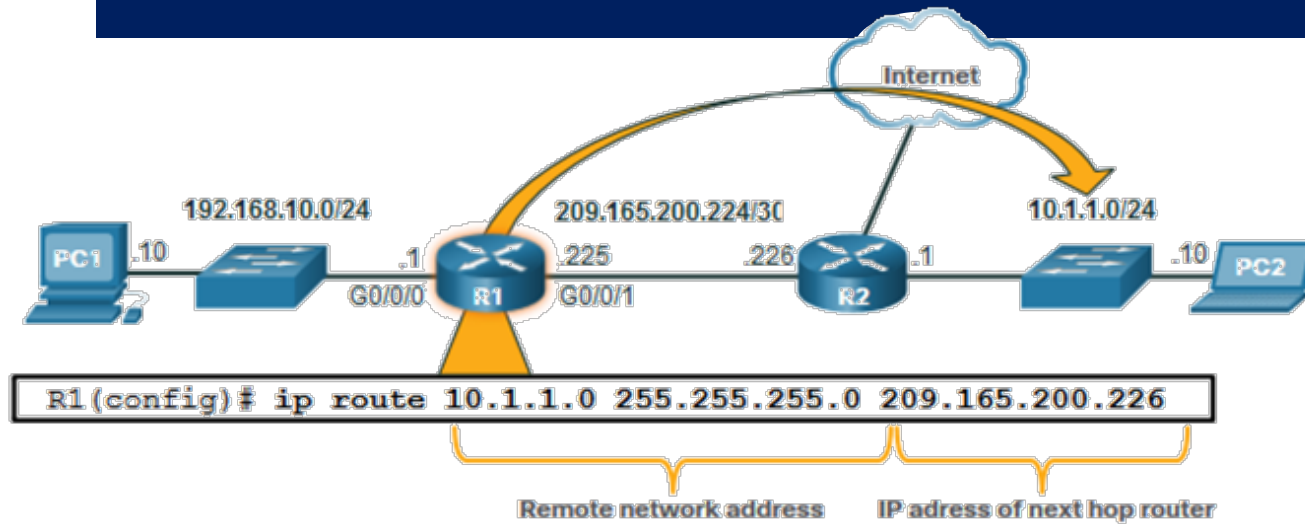


Enrutamiento estático

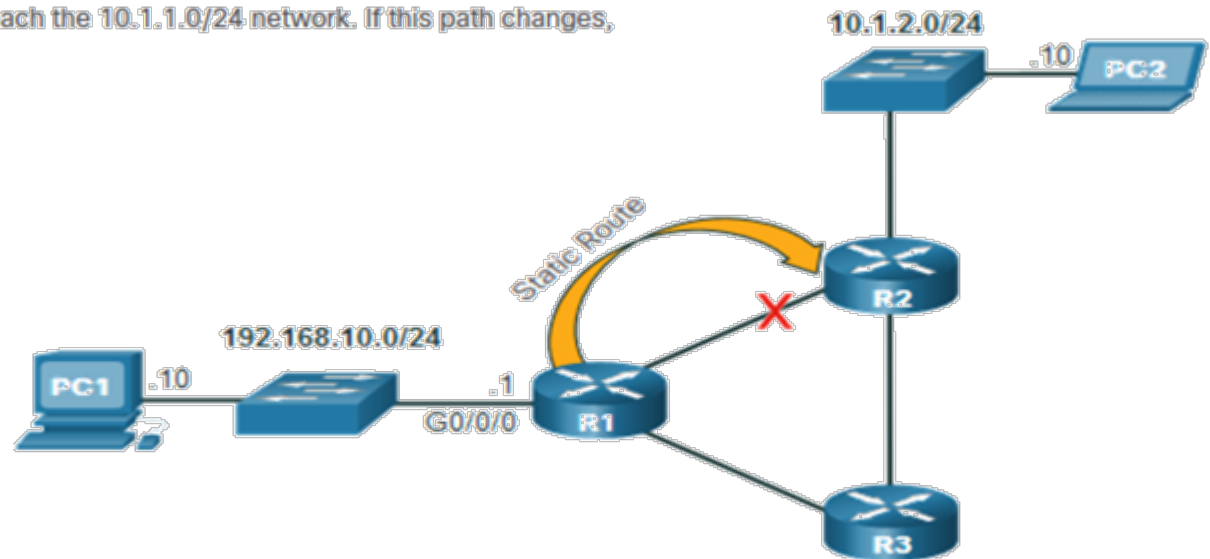
Características **rut**as estáticas:

- Deben configurarse manualmente.
- Deben ajustarse manualmente por el administrador cuando hay un cambio en la topología
- Buenas para redes pequeñas no redundantes
- Utilizadas a menudo junto con un protocolo de enrutamiento dinámico para configurar una ruta predeterminada

Enrutamiento estático



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.



Fuente: Cisco NetAcad

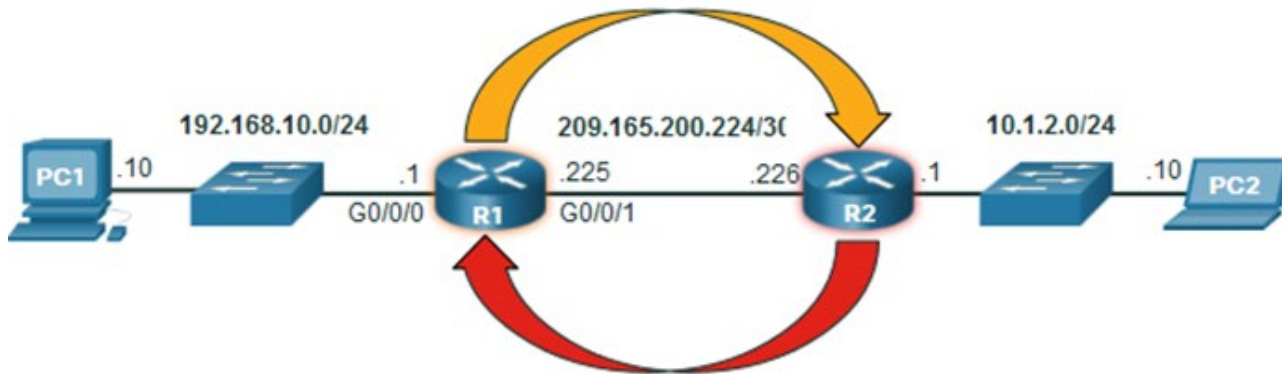
Enrutamiento dinámico

Características **rut**as dinámicas:

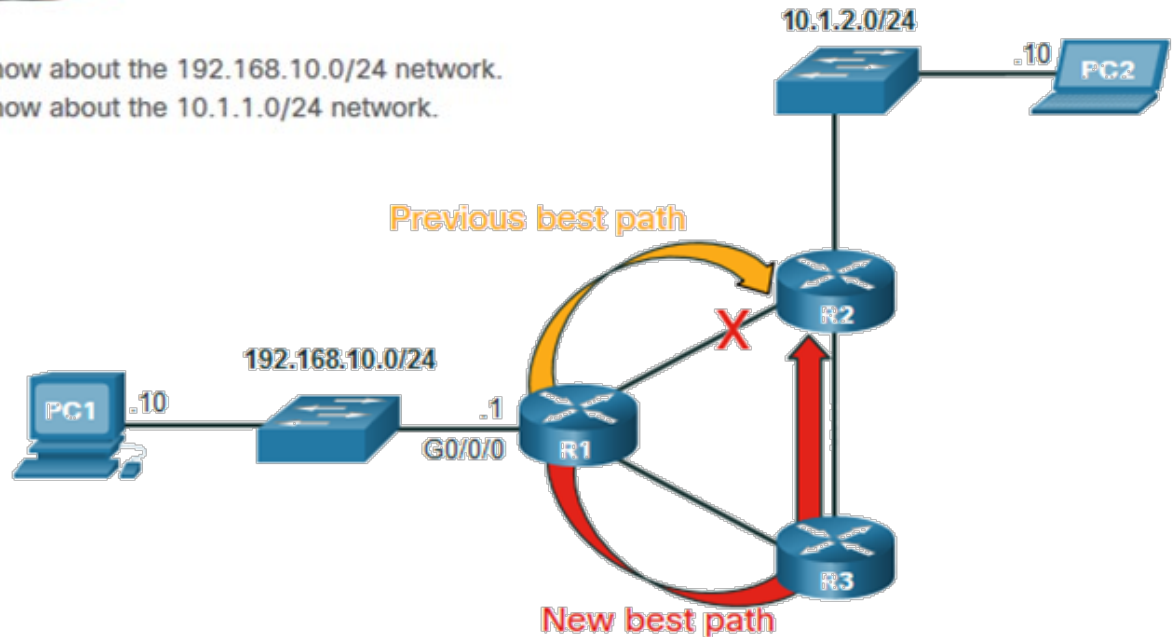
- Detectan redes remotas.
- Mantienen información actualizada.
- Eligen el mejor camino hacia las redes de destino.
- Buscan nuevas rutas óptimas cuando hay un cambio de topología.

Enrutamiento dinámico también puede compartir rutas estáticas predeterminadas con los otros routers

Enrutamiento dinámico



- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.



Fuente: Cisco NetAcad

R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

¿Estático o dinámico?

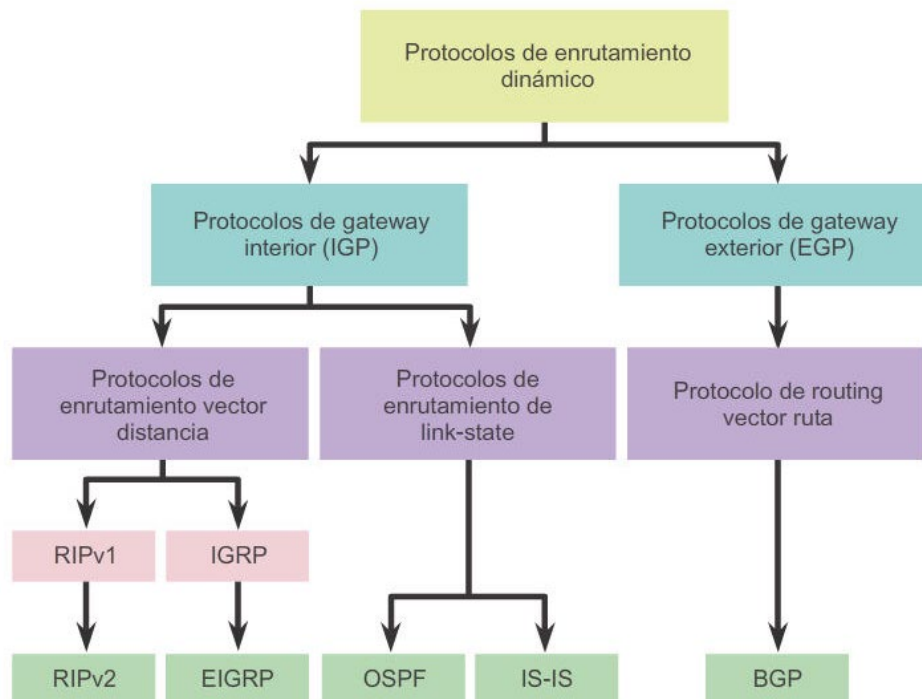
¿Cuándo conviene utilizar cada uno?

Suelen convivir ambos para aprovechar lo mejor de cada uno, según la topología

Característica	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Independiente del tamaño de la red	Aumenta cuando la red crece
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere intervención del administrador
Escalabilidad	Adecuado para topologías simples a complejas	Adecuado para topologías simples
Seguridad	La seguridad debe estar configurada	La seguridad es inherente
Uso de recursos	Usa CPU, memoria, ancho de banda de enlaces	No se necesitan recursos adicionales
Predictibilidad de Ruta	La ruta depende de la topología y el protocolo de enrutamiento utilizados	Definido explícitamente por el administrador

Más detalles sobre enrutamiento dinámico

[Ver Anexo al tema para más detalles]



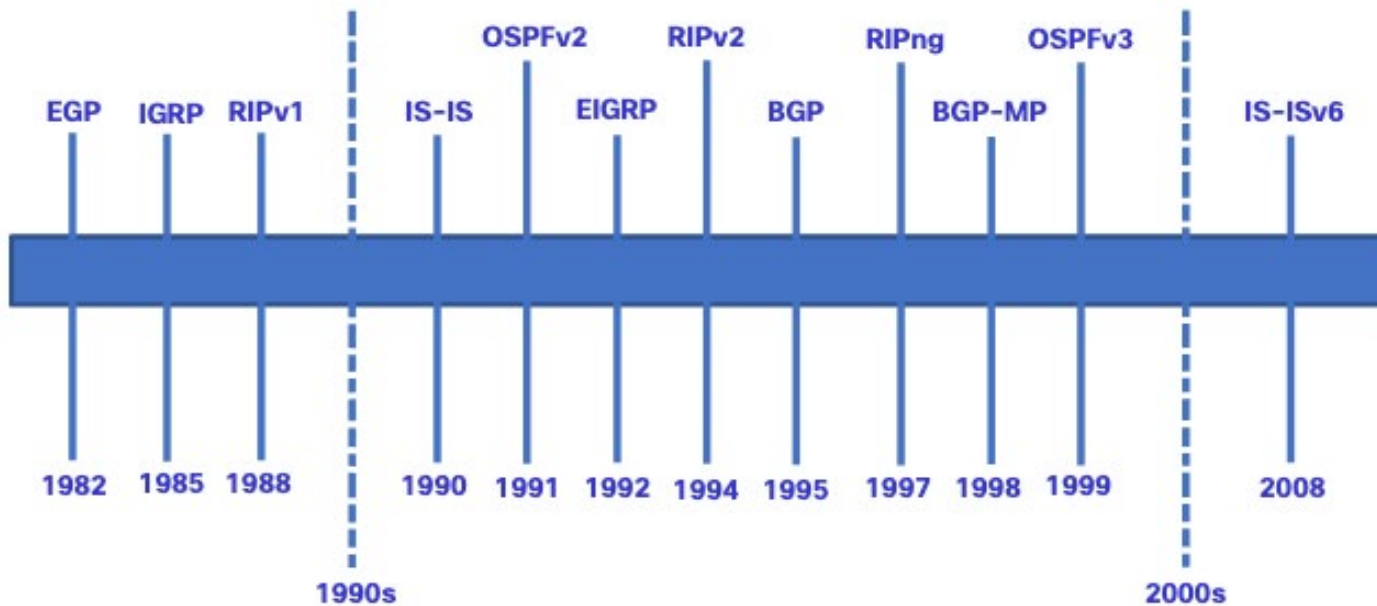
Los protocolos **vector distancia** utilizan routers como indicadores a lo largo de la ruta hacia el destino final

Protocolos de **estado de enlace** son parecidos a tener un mapa completo de la topología de la red. Los indicadores a lo largo de la ruta de origen a destino no son necesarios, debido a que todos los routers usan un mapa de la red idéntico. Un router de estado de enlace usa la información de estado de enlace para crear un mapa de la topología y seleccionar la mejor ruta hacia todas las redes de destino en la topología

Evolución del enrutamiento dinámico

[Ver Anexo al tema para más detalles]

Evolución del enrutamiento dinámico



Componentes de los protocolos dinámicos

Componentes de los protocolos de routing dinámicos:

- **Estructuras de datos:** Generalmente utilizan tablas o bases de datos para sus operaciones. Esta información se guarda en la RAM.
- **Mensajes del protocolo:** Usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de enrutamiento y realizar otras tareas para conservar información precisa acerca de ella.
- **Algoritmo:** Lista finita de pasos que se usan para llevar a cabo una tarea. Los protocolos de routing usan algoritmos para facilitar información de routing y para determinar el mejor camino.

Los protocolos de enrutamiento determinan la mejor ruta hacia cada red. Esta ruta es mostrada en la tabla de enrutamiento. La ruta se instalará en la tabla de enrutamiento, si no hay otra ruta con una distancia administrativa menor.

Más detalles sobre enrutamiento dinámico

Detalles sobre los protocolos de routing dinámicos más usados

Protocolo de enrutamiento	Métrica
Routing Information Protocol (RIP)	<ul style="list-style-type: none">• La métrica es el recuento de saltos• Cada router de una ruta agrega un salto al recuento de saltos.• Se permite un máximo de 15 saltos.
Open Shortest Path First (OSPF)	<ul style="list-style-type: none">• La métrica es el "Costo", basado en el ancho de banda acumulado de origen a destino.• A los enlaces más rápidos se les asignan costos más bajos en comparación con los enlaces más lentos (de mayor costo).
Enhanced Interior Gateway Routing Protocol (EIGRP)	<ul style="list-style-type: none">• Calcula una métrica basada en los valores de ancho de banda y retraso más lentos.• Confiabilidad y carga también se pueden incluir en el cálculo de la métrica.

Videos: Routing dinámico

Routing dinámico

Conceptos de enrutamiento dinámico (Aruma digital):

<https://www.youtube.com/watch?v=CKURHj2qn28>

Enrutamiento dinámico con RIP (Aruma digital):

https://www.youtube.com/watch?v=pZY_D7ASII0

Un MUY BUEN canal con videos sobre CCNA:

<https://www.youtube.com/playlist?list=PLC752553BD9C9C76C>

(Aruma digital)



Fuente: <https://sp.depositphotos.com/stock-photos/popcorn-box.html>

Fragmentación y reensamblaje

MTU de los enlaces de red

Cada red o enlace impone un tamaño máximo a sus paquetes (MTU). Estos límites tienen varias razones, entre ellas:

- El hardware (por ejemplo, el tamaño de una trama Ethernet).
- El sistema operativo (por ejemplo, todos los búferes son de 512 bytes).
- Los protocolos (por ejemplo, cantidad de bits del campo longitud de paquete).
- El cumplimiento de algún estándar (inter)nacional.
- El deseo de reducir las retransmisiones inducidas por errores.
- El deseo de evitar que un paquete ocupe el canal demasiado tiempo.

Resultado: Los diseñadores de redes no tienen la libertad de elegir cualquier tamaño máximo de paquetes que deseen.

Fuente: Redes de computadoras. Tanenbaum

Valores de MTUs habituales

Ejemplos de MTU para distintos protocolos usados en Internet*:

- **Ethernet** (802.3): 1500 bytes
- **WiFi** (802.11): 2272 bytes
- PPPoE: 1492 bytes
- ATM (AAL5): 9180 bytes
- FDDI: 4470 bytes
- **PPP**: 576 bytes

El protocolo IP permite paquetes de hasta 65515 bytes

Fuente: Wikipedia

Ventajas/Inconvenientes paquetes grandes

Ventajas

- Aumento de la eficiencia por reducción, en términos relativos, del tamaño de cabeceras.
- La menor tasa de procesamiento de tramas redunda en un alivio de la carga de la CPU.



Inconvenientes

- Se requiere mayor cantidad de memoria.
- La pérdida de un paquete es más traumática al perder mayor información.
- Introducción de retardos excesivos en líneas de baja velocidad.



Fragmentación en origen/ruta

Si el datagrama/paquete que se desea enviar es demasiado grande ha de fragmentarse para que entren en la MTU disponible.

La fragmentación puede hacerse:

- En **origen**: Es responsabilidad de los hosts cuando el paquete que han de enviar es mayor que la MTU de su interfaz.
- En **ruta**: Los routers son los encargados cuando por una interfaz les llega un paquete que es superior que la MTU de la interfaz por la que ha de salir.

La desfragmentación se realiza en el nivel de red del host receptor, nunca durante el transcurso de la comunicación a lo largo de la red.

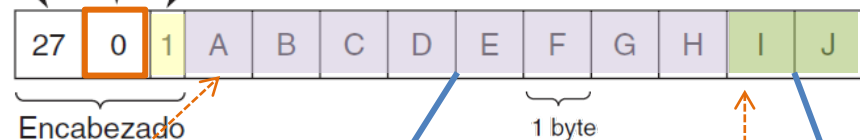
Fragmentación en origen/ruta

Número del primer fragmento elemental de este paquete - **Fragment Offset**

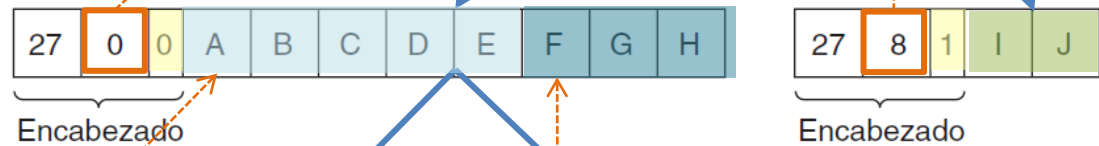
Identification - Número de paquete

Bit de fin de paquete = ! MF (equivalente negado MF)

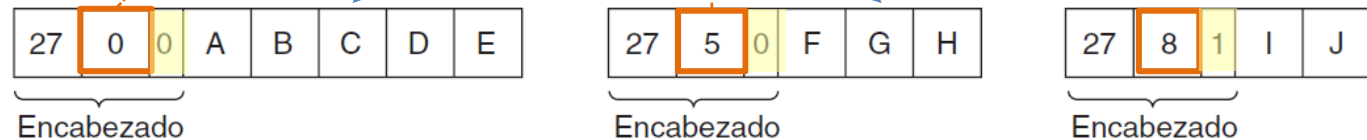
Paquete original con 10 bytes datos + encabezado.



Fragmentos después de pasar por red con **MTU** (tam. Máx. paquete) de **8 bytes datos + encabezado**.

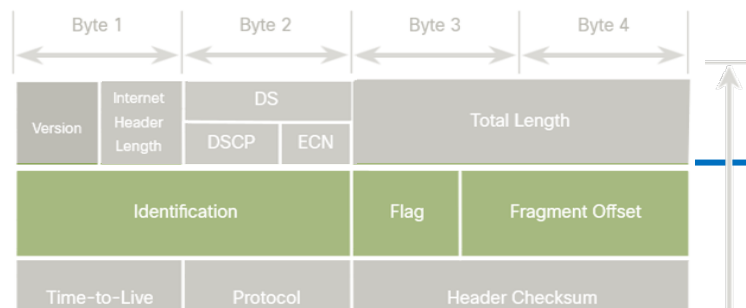


Fragmentos después de pasar por red con **MTU** de **5 bytes datos + encabezado**



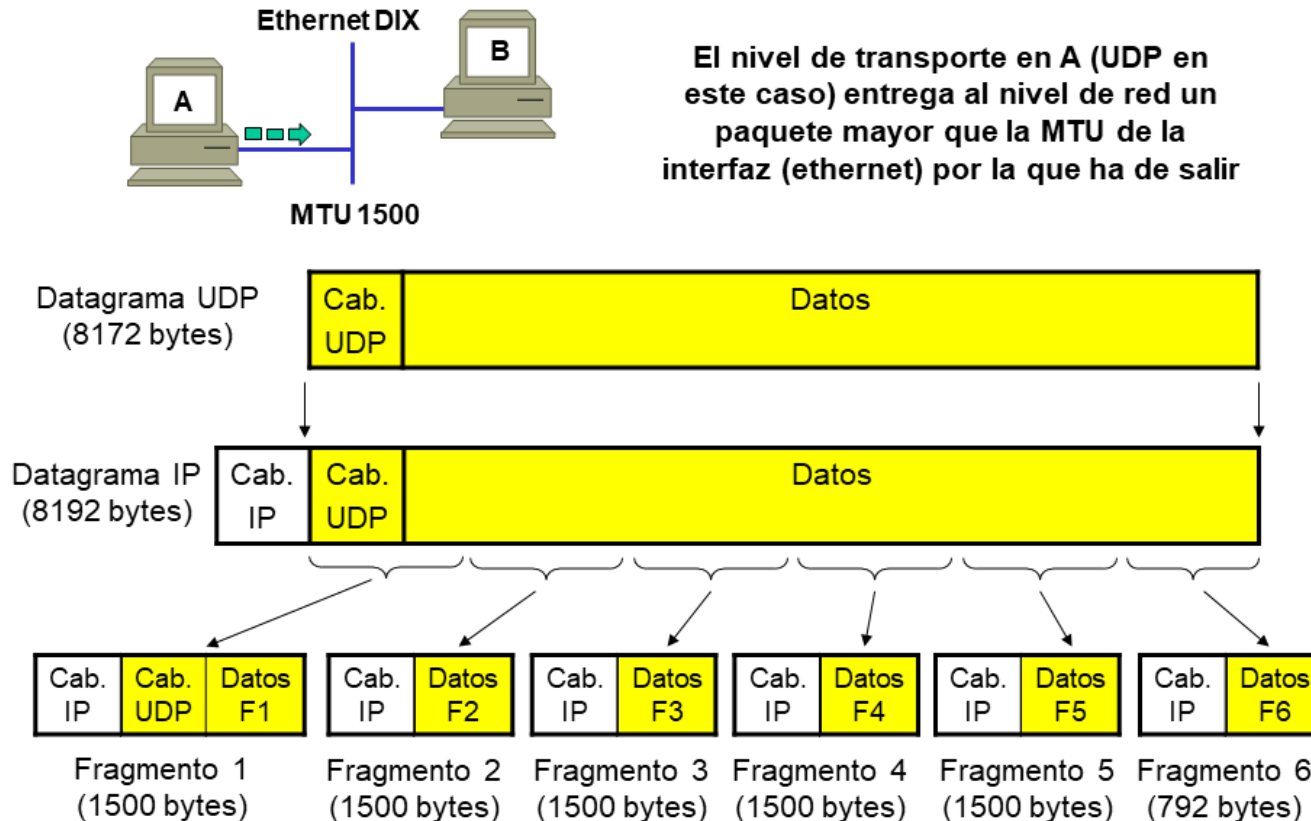
Campos (fragmentación) de paquetes IPv4

Campo	Descripción
Identification 16 bits	Identifican el <u>fragmento de un paquete IP original</u> . Dado un contador de cada envío, su valor es copiado a este campo en caso de ser necesario fragmentar. Mismo valor todos los fragmentos del mismo paquete.
Flag 3 bits	Identifican <u>cómo se fragmenta el paquete</u> . <ul style="list-style-type: none"> • Res: Reservado (no se usa) • DF: Indicador de fragmentación. Si el valor es 1 la máquina no debe fragmentar el datagrama. De manera que, si no puede pasar por alguna red física disponible se descarta el datagrama y se envía un mensaje ICMP de error al host origen. Si el valor es cero el datagrama puede ser fragmentado en caso de necesidad. • MF: Indicador de más fragmentos. Si el valor es 1 indica que el datagrama no es el último fragmento y un valor 0 indica que es el último o único fragmento.
Fragment Offset 13 bits	Identifican <u>orden en que se debe colocar el fragmento</u> del paquete en la reconstrucción del paquete original sin fragmentar. Es múltiplo de 8 bytes (consecuencia del tamaño del campo son 13 bits).



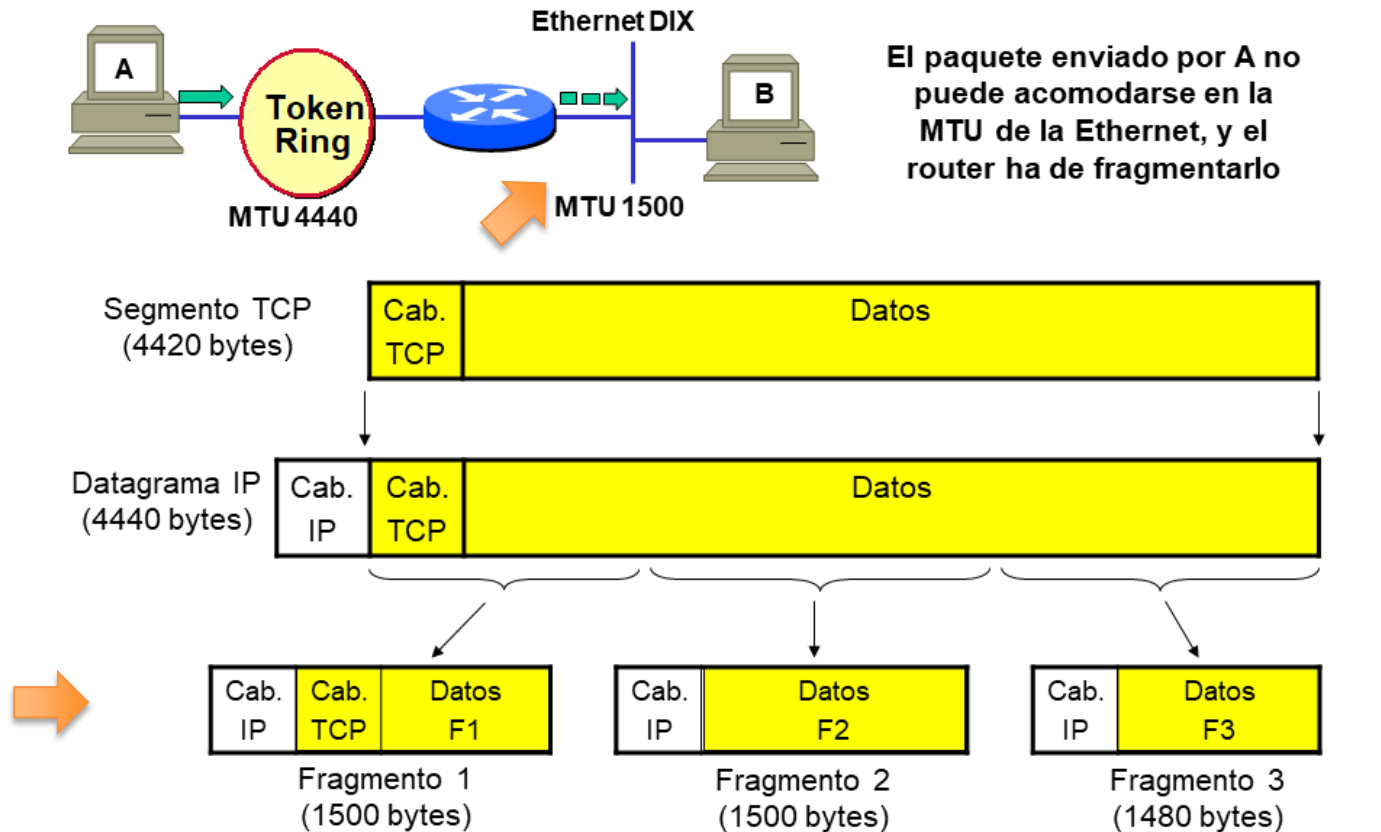
Fragmentación en Origen (Host)

Ejemplo de fragmentación en origen (host)



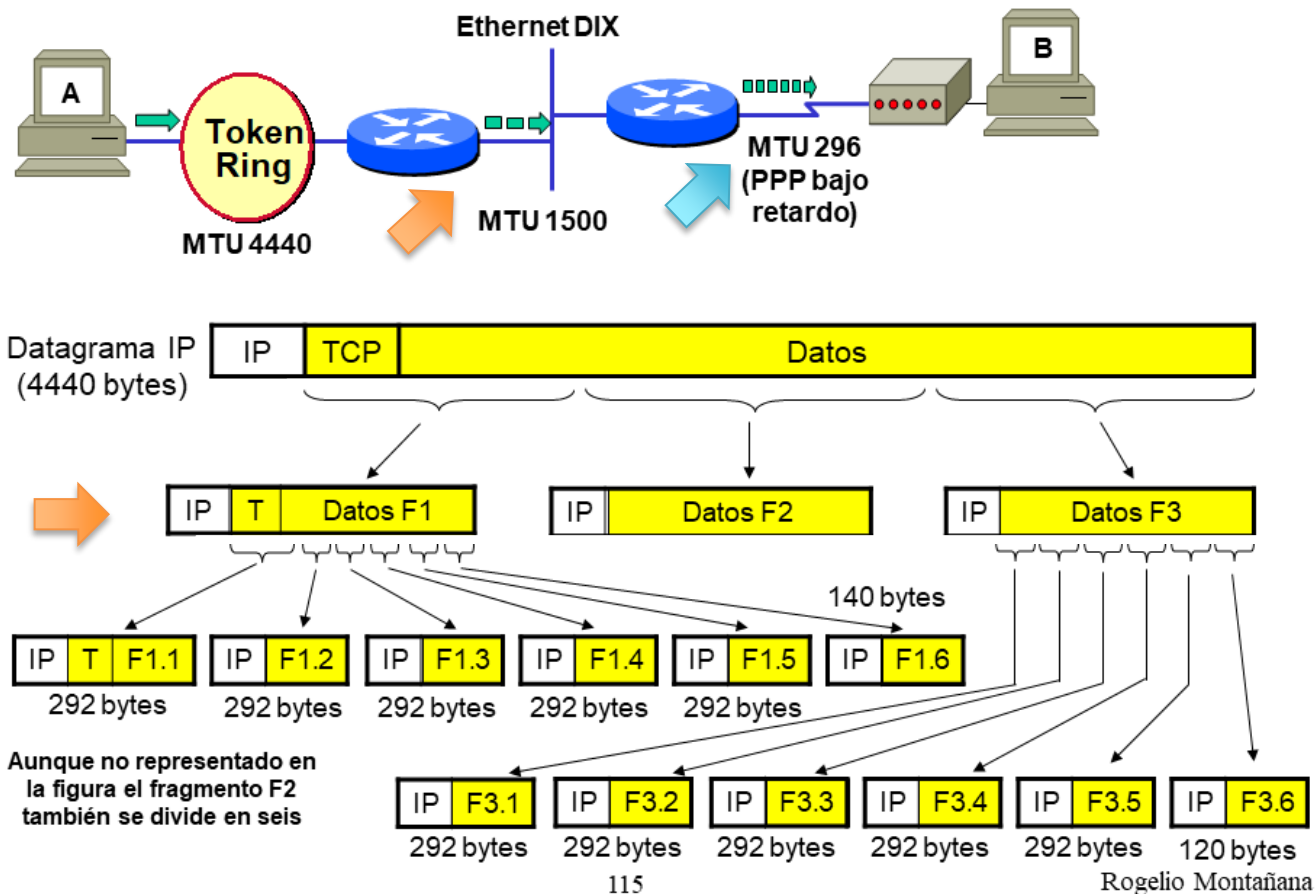
Fragmentación en Ruta

Ejemplo de fragmentación en ruta (router)

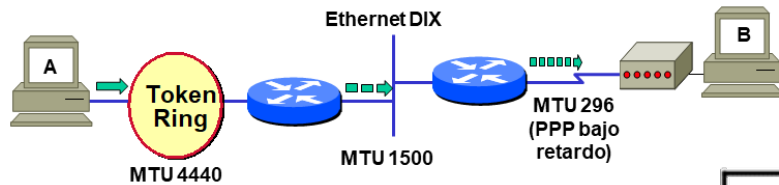


Fragmentación múltiple en Ruta I

Ejemplo de fragmentación múltiple en ruta



Fragmentación múltiple en Ruta II



Fragmentación múltiple

		Id.	Long	DF	MF	Desplaz.	Datos	
								4420 bytes
Token Ring	Datagrama Original	XXX	4440	0	0	0	ABCDEF GHIJKL MNOPQR	
E-net DIX	Fragmento 1	XXX	1500	0	1	0	ABCDEF	← 1480 bytes
	Fragmento 2	XXX	1500	0	1	185	GHIJKL	← 1480 bytes
	Fragmento 3	XXX	1480	0	0	370	MNOPQR	← 1460 bytes
PPP Bajo Retardo	Fragm. 3.1	XXX	292	0	1	370	M	← 272 bytes
	Fragm. 3.2	XXX	292	0	1	404	N	← 272 bytes
	Fragm. 3.3	XXX	292	0	1	438	O	← 272 bytes
	Fragm. 3.4	XXX	292	0	1	472	P	← 272 bytes
	Fragm. 3.5	XXX	292	0	1	506	Q	← 272 bytes
	Fragm. 3.6	XXX	120	0	0	540	R	← 100 bytes

El campo Desplaz. cuenta los bytes en grupos de 8 ($1480 / 8 = 185$)

Videos: Fragmentación de paquetes

Fragmentación de paquetes

Explicación completa con ejemplos:

Fragmentación (Rogelio Montaña)

<https://www.youtube.com/watch?v=6czsilKsZUg>

Otra explicación con su ejemplo:

Fragmentación en IPv4 (teoría)

<https://www.youtube.com/watch?v=yL28OKZ5E4U>

Fragmentación en IPv4 (ejercicio)

<https://www.youtube.com/watch?v=KaHpC2W9-l4>



Fuente: <https://sp.depositphotos.com/stock-photos/popcorn-box.html>

Actividad de clase: Configuración PT

¡ Vamos a jugar un poco con PT !

