La evolución del stack de Internet: IPv6 y QUIC

Carlos M. Martínez

@CagnazzoEng

Junio 2020

lacnic

www.lacnic.net

Acerca de mi

Gerente de Tecnología en LACNIC

- IPv6, RPKI, DNS, DNSSEC, Security

Antes:

- 15 años en operación de un ISP

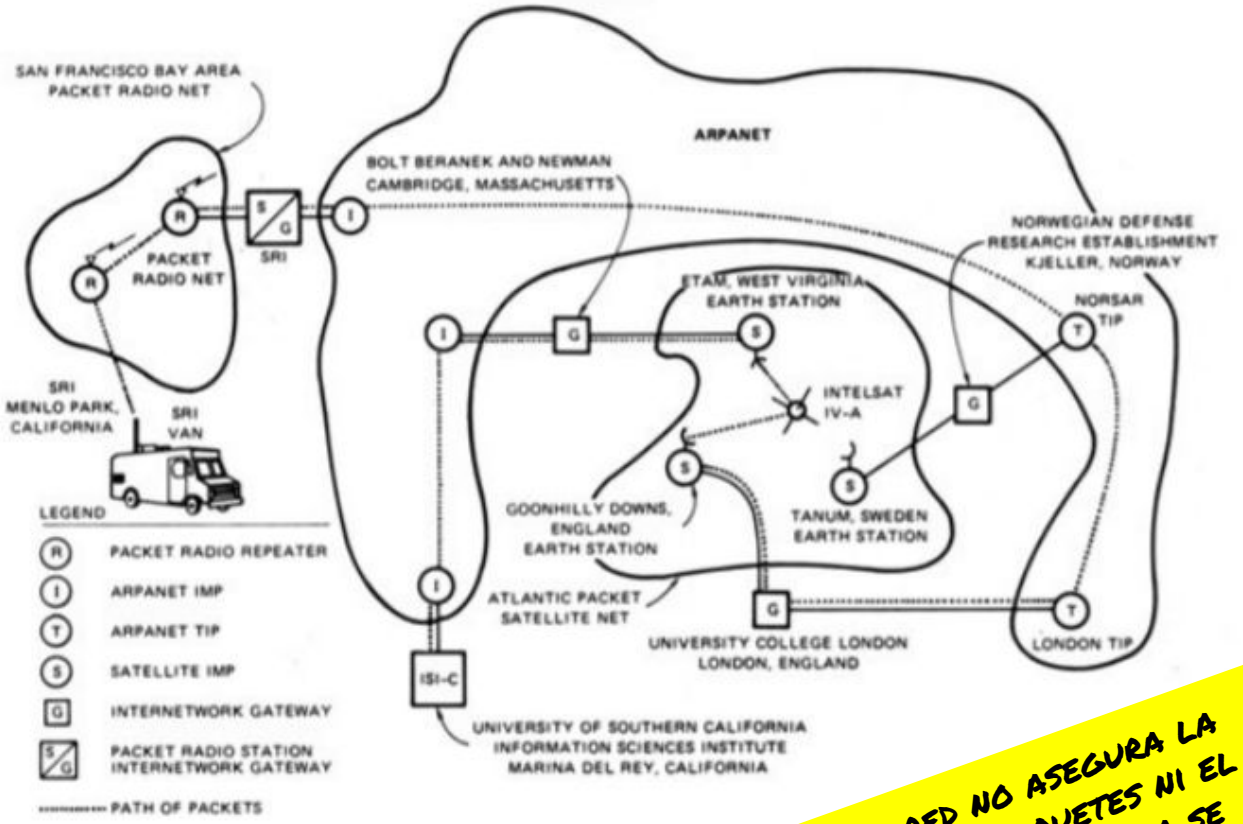
Además:

- Comité de Programa de LACNOG (Latin American and Caribbean Network Operators Group)
- Ceremonias de firma de la raíz del DNS (KSK)

Acerca de LACNIC

El *stack* de Internet

- Capas físicas/enlace heterogéneas
- Capa de red *best effort* basada en datagramas
- Transporte y aplicaciones sobre ellas



LA CAPA DE RED NO ASEGURA LA ENTREGA DE LOS PAQUETES NI EL ORDEN EN QUE ESA ENTREGA SE REALIZA

El stack de Internet

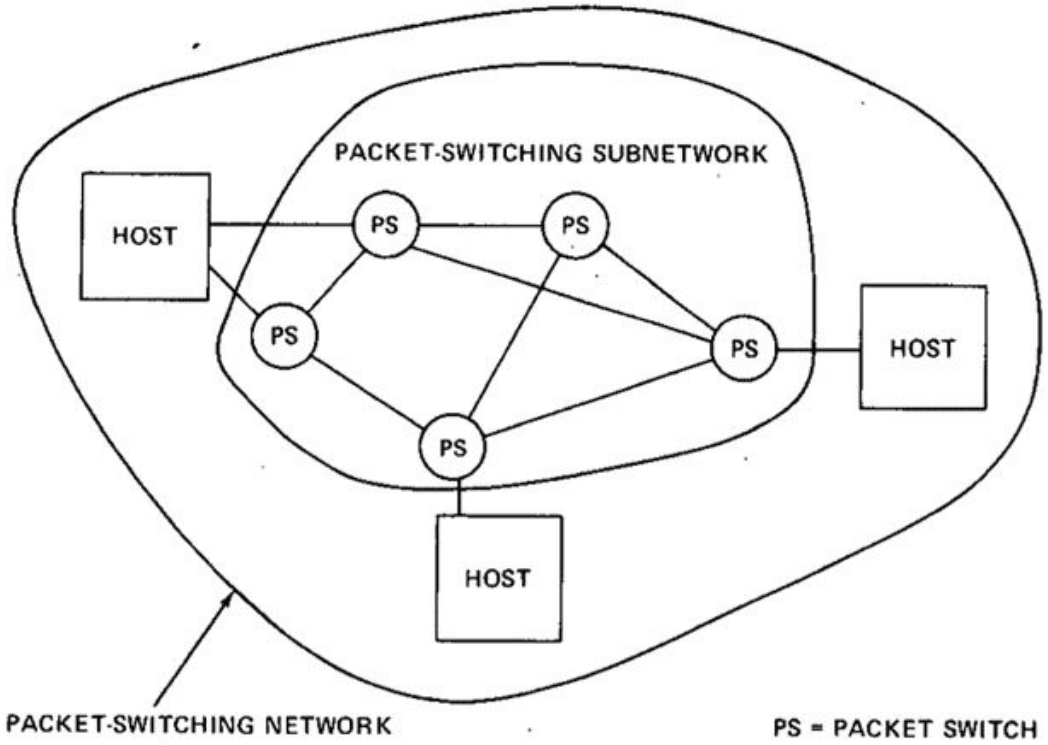
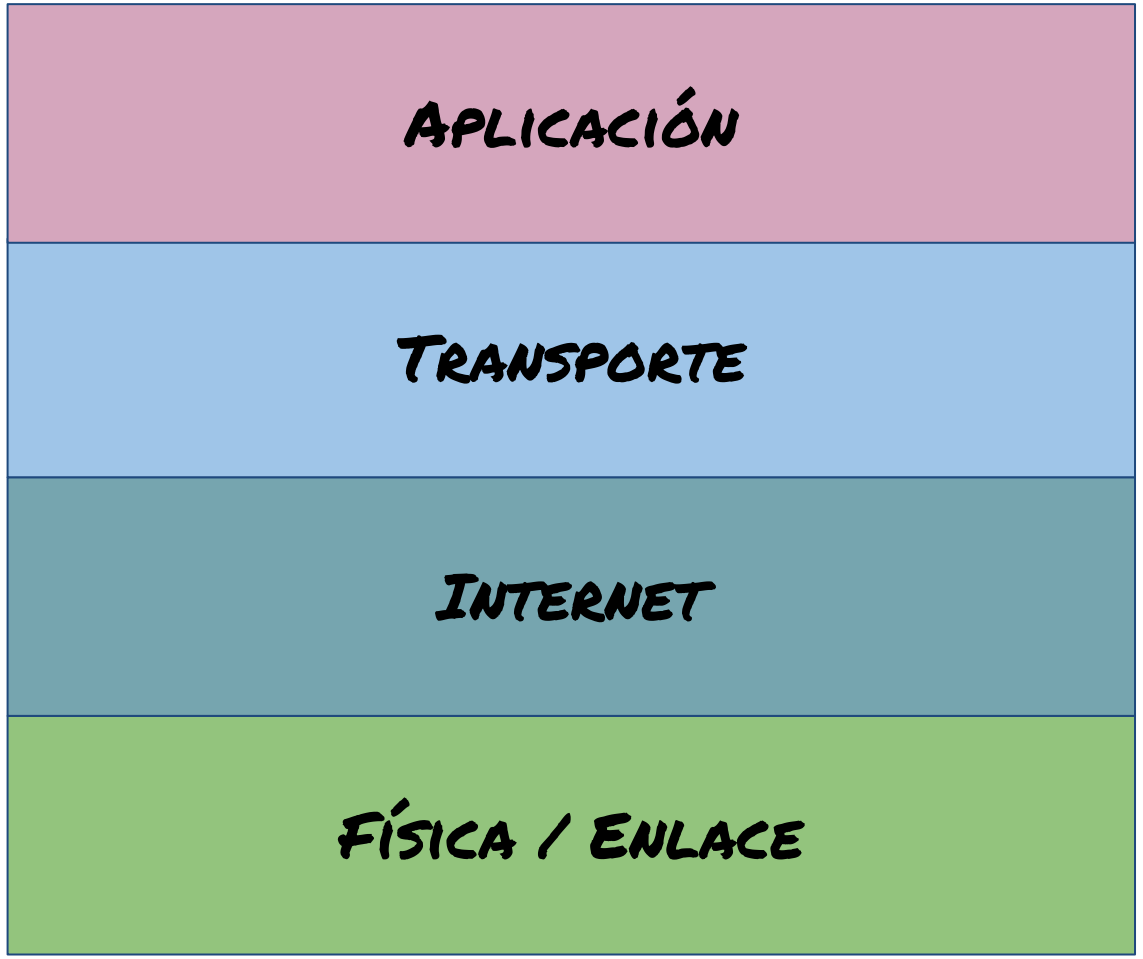
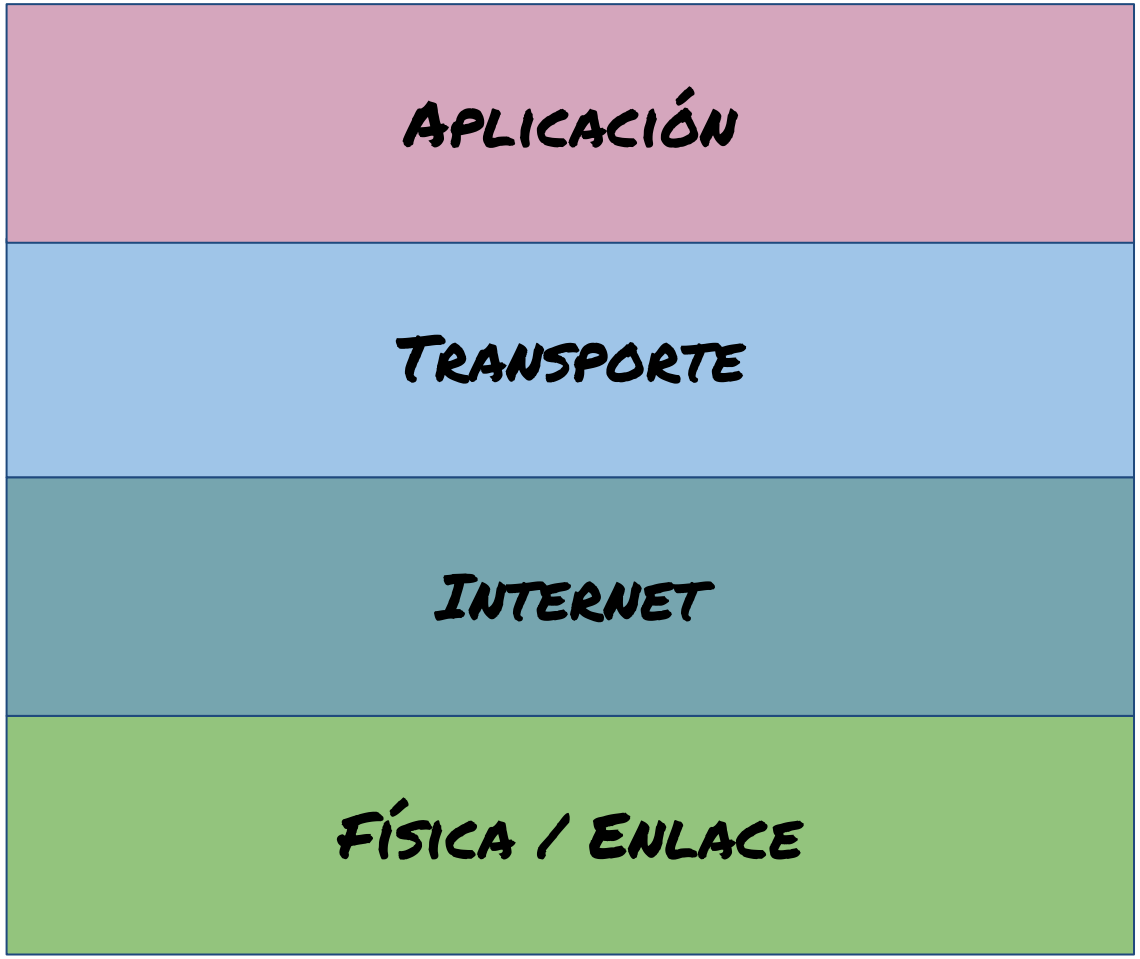


Fig. 1. Typical packet switching network.



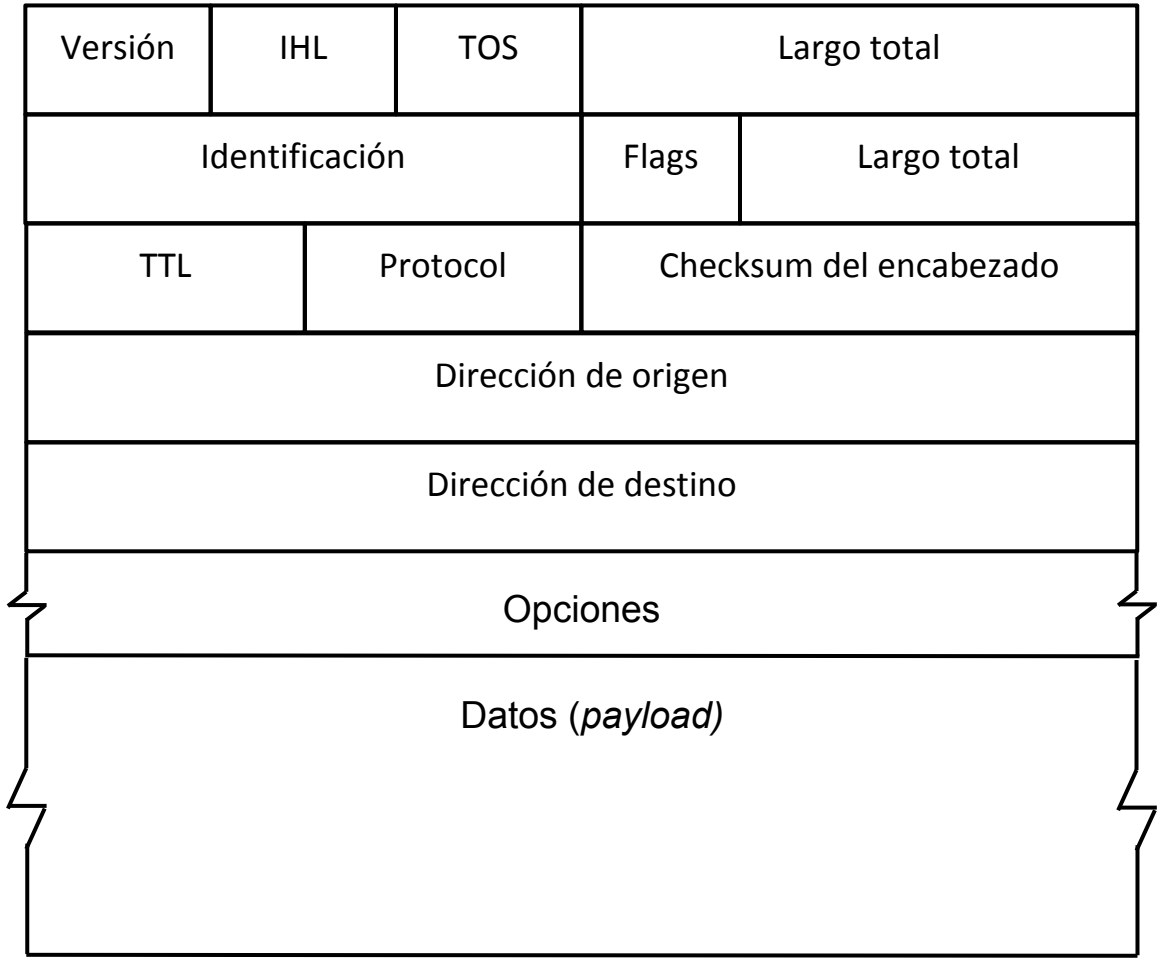
Estándares, estándares...



IP

IPv4:

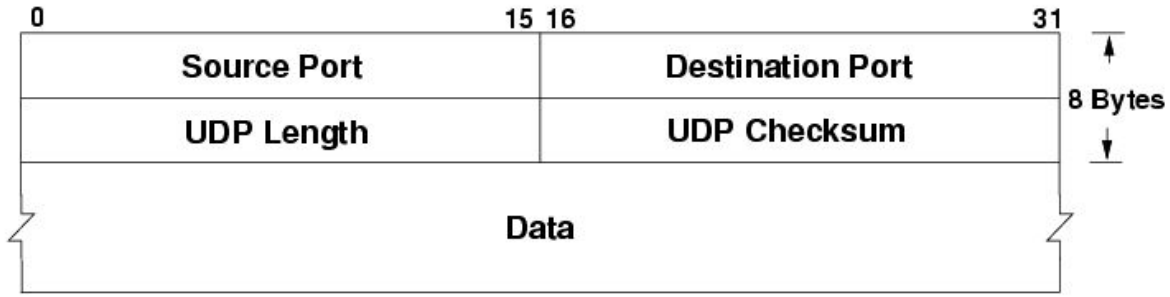
- direcciones de 32 bits
- TTL
- bloque fijo de 20 bytes más un bloque de largo variable de opciones
- fragmentación salto a salto posible
  - *cualquier nodo intermedio puede fragmentar*



UDP

UDP

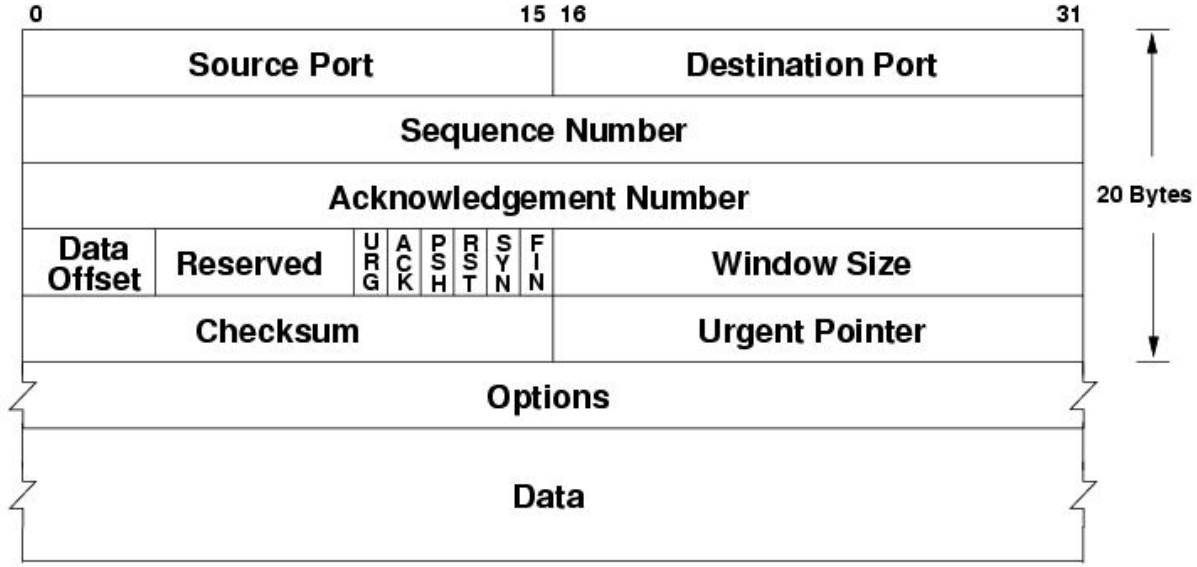
- servicio de datagramas (paquetes individuales) sin garantías de entrega u orden
- puerto de origen y destino
- largo de datagrama
- checksum

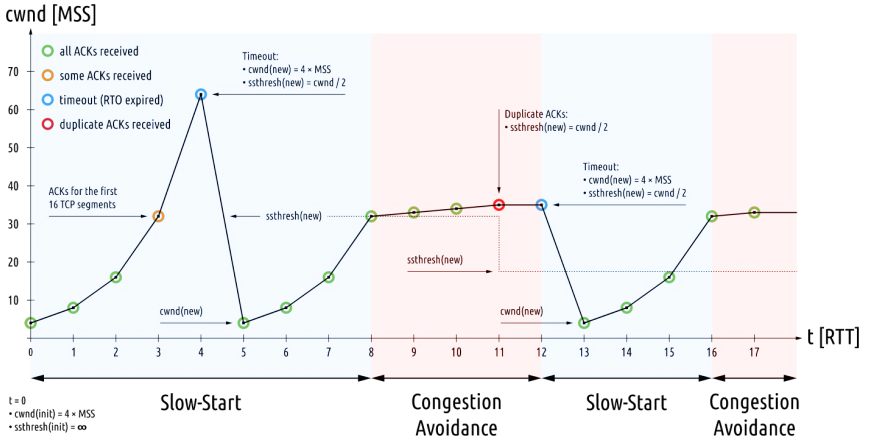


TCP

TCP

- entrega confiable y ordenada
- números de secuencia
- ventanas de retransmisión
- *slow start*
- *three-way handshake*
  - 2 RTT antes de poder transmitir información útil





Problemas en el stack actual

IP:

- Espacio de direccionamiento (agotamiento de IPv4)

TCP:

- SSL por conexión (múltiples negociaciones de cripto)
- Control de flujo asociado al concepto de *slow start* vinculado a la congestión
- No integrado con protocolos de capa superior (falta de *pipelining*)

Evolución en capa de red : IPv6

Un poco de historia:

- Cerca de 1994 ya se advierte el problema del posible agotamiento de IPv4
- Necesidad de un nuevo protocolo
- Se analizaron diferentes alternativas, lo que hoy conocemos como IPv6 fue la propuesta “ganadora” de este proceso

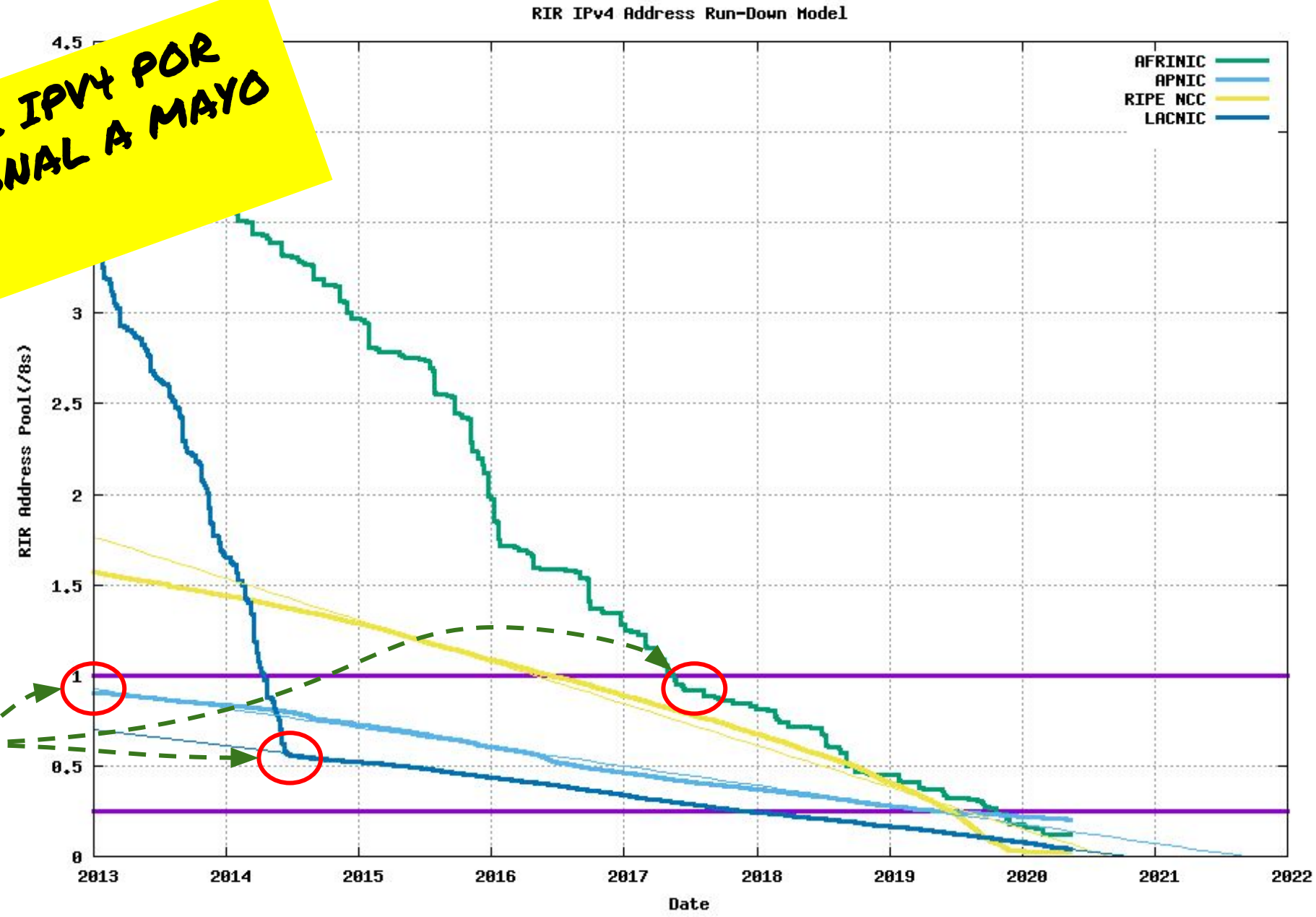
Agotamiento de IPv4

¡Situación ya percibida en 1994!

Medidas paliativas:

- eliminación del "*classful addressing*", introducción del concepto de máscara de red o largo de prefijo
- introducción del *Network Address Translation* o NAT
  - compartir direcciones públicas entre múltiples dispositivos
- introducción del encabezado "Host:" en HTTP 1.1
  - compartir la misma dirección pública en varios sitios web

AGOTAMIENTO DE IPV4 POR REGISTRO REGIONAL A MAYO DE 2020



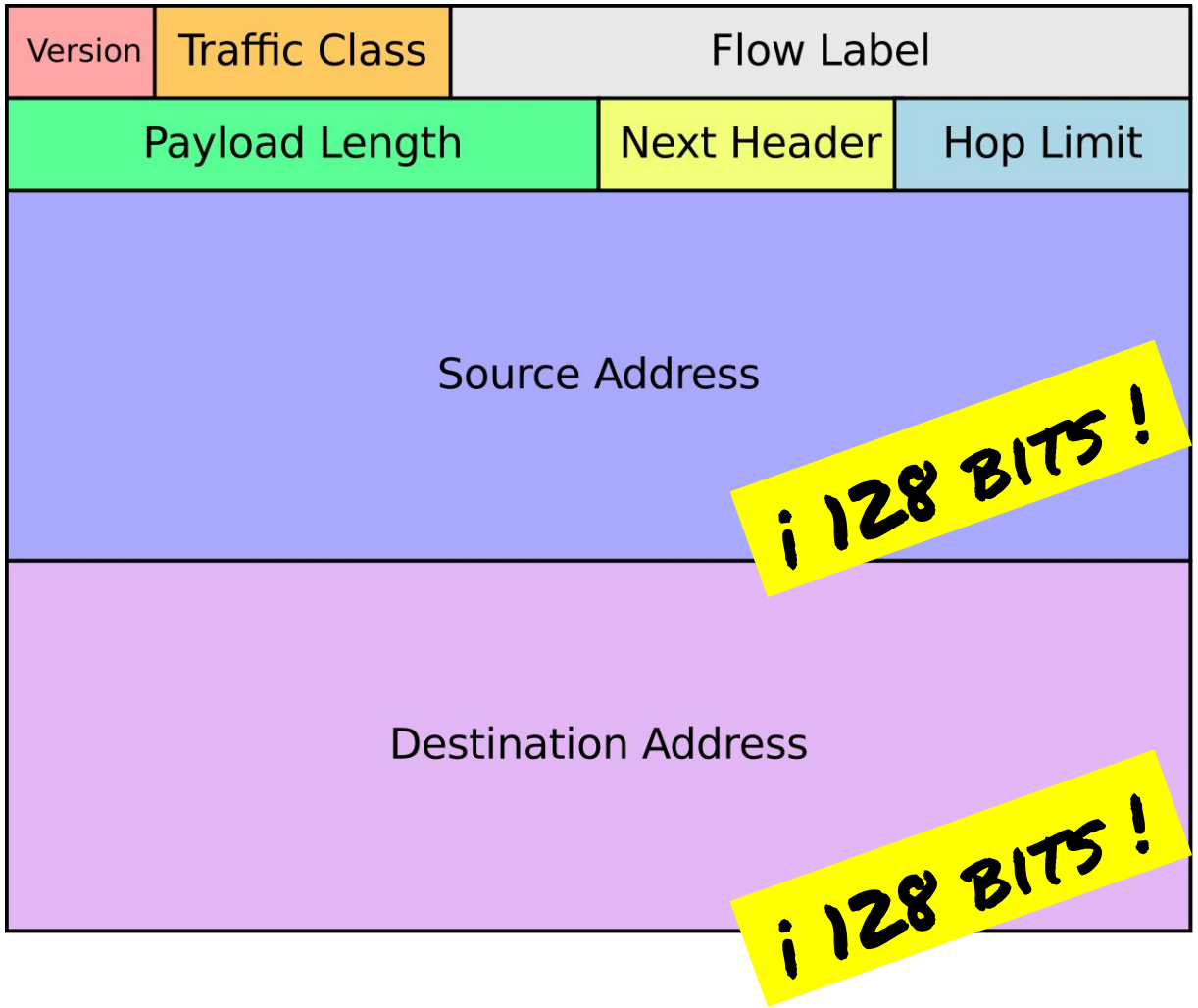
POLITICAS DE SOFT-LANDING

IPv6: Evolución de la capa de red

IPv6

Encabezado:

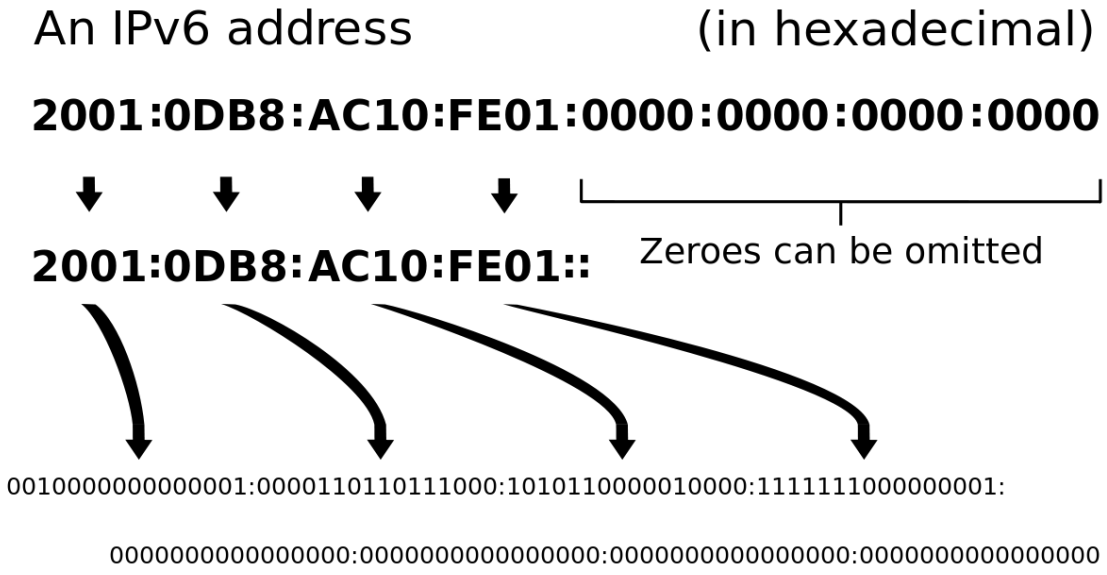
- simplificado con respecto a IPv4
- soporte de *encabezados de extensión*



IPv6: Direcciones

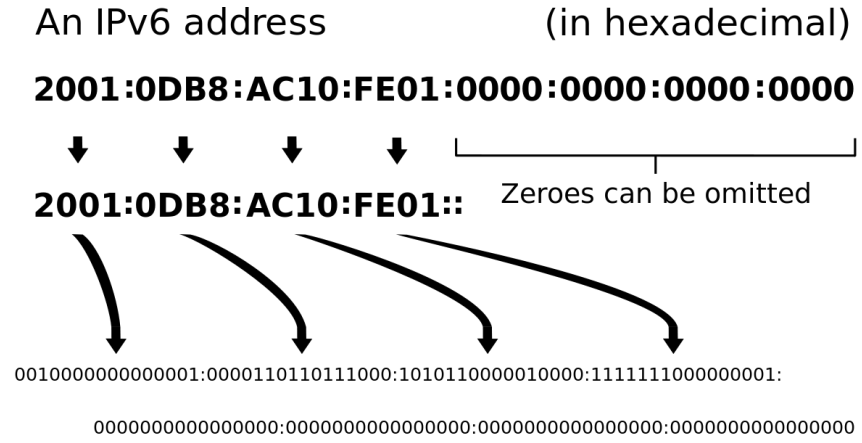
Notación:

- cada dígito representa 4 bits
- cada grupo 16 bits
- los ceros consecutivos se pueden omitir
- los ceros a la izquierda también se omiten



IPv6: *Scope* de las direcciones

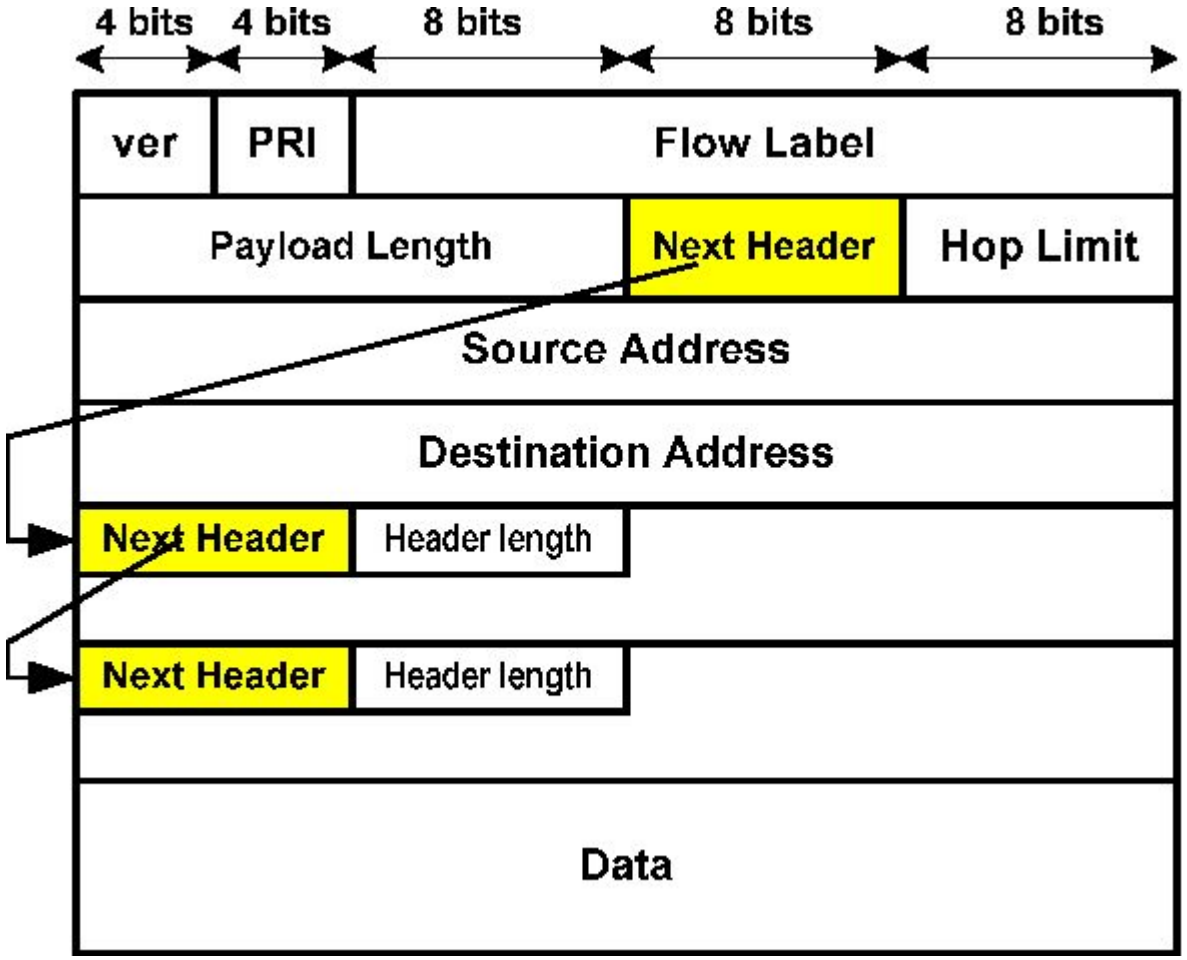
- Las direcciones en IPv6 tienen *scopes:*
  - Link local
    - Solo válidas en una misma LAN
    - Los routers no las reenvian
  - Global Unicast
    - Ruteables
    - ULAs*
  - Multicast



IPv6: Encabezados de extensión

Encabezados de extensión:

- end to end
- hop by hop



IPv6: ICMPv6

Protocolo de control para IPv6, resumiendo las funcionalidades de:

- ICMP
- IGMP
- ARP

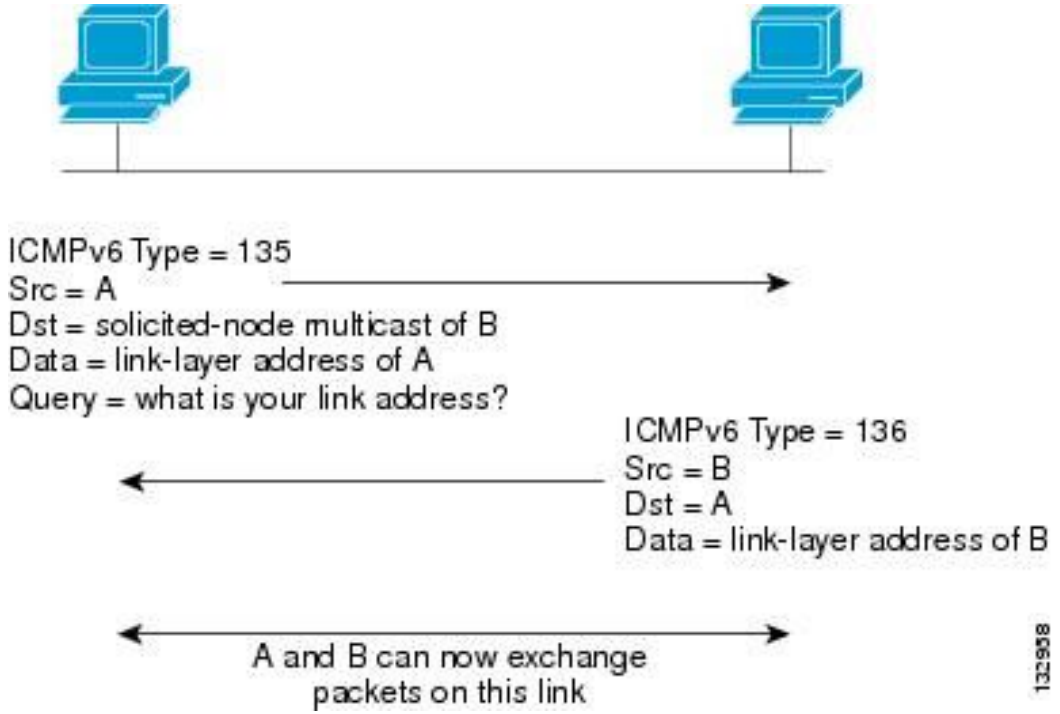
Además agrega funcionalidades:

- Autoconfiguración sin estado

IPv6: Neighbor Discovery

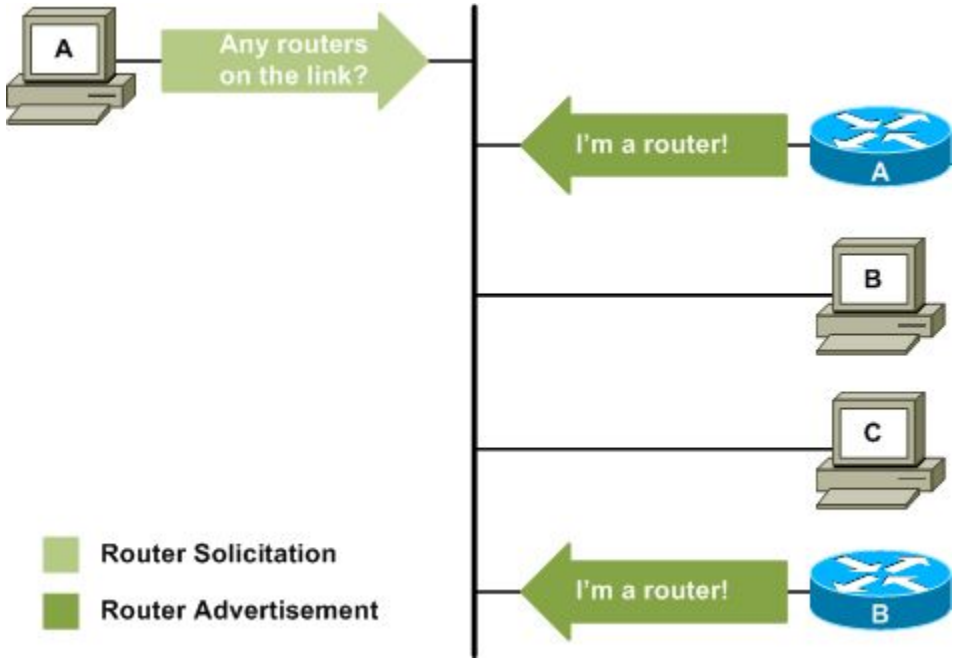
Descubrimiento de direcciones de capa de enlace

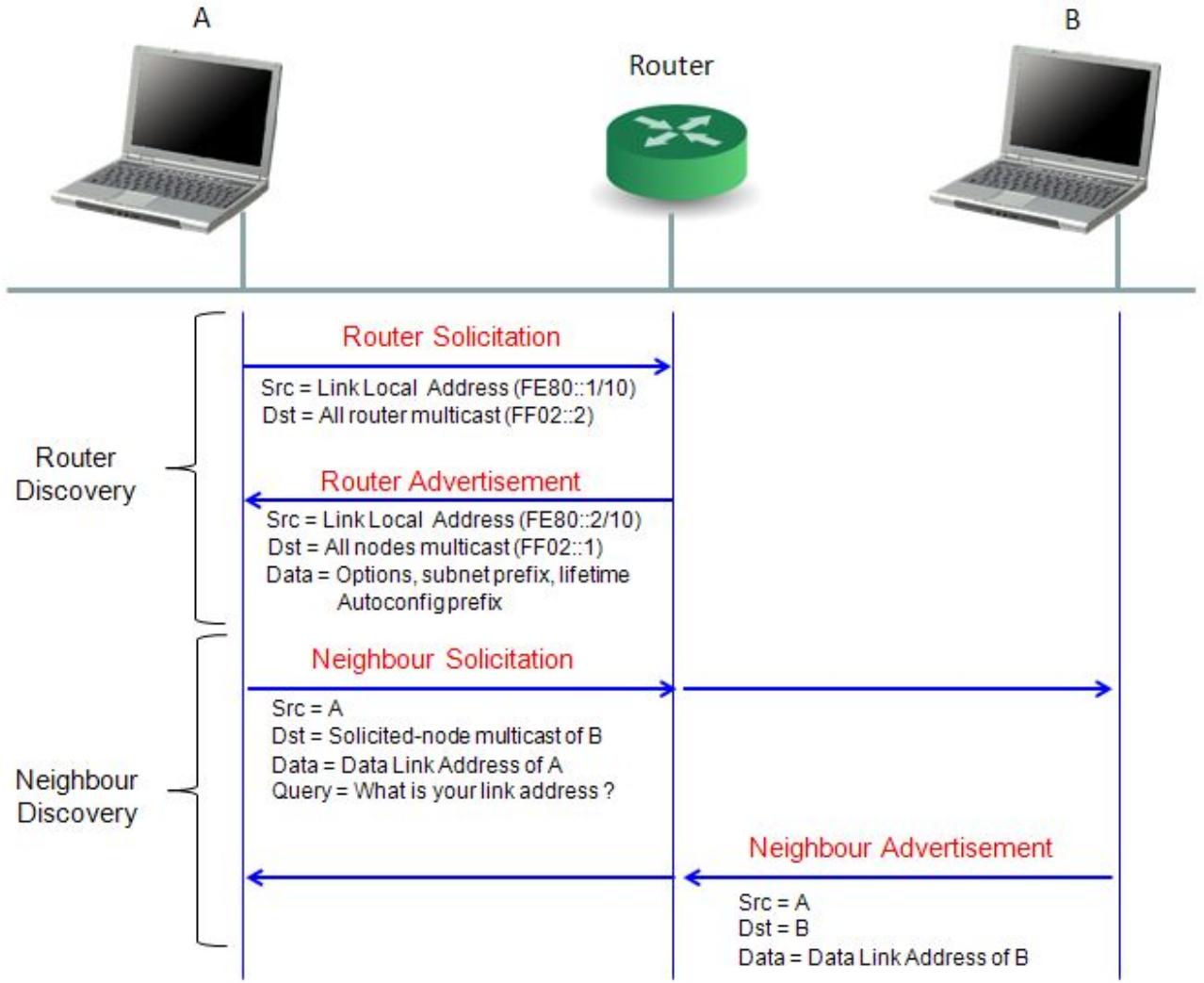
- Determina la dirección MAC de los vecinos del mismo enlace
- Reemplaza al protocolo ARP utilizando multicast
- El host envía un mensaje NS con su dirección MAC y pregunta la MAC del vecino



IPv6: Neighbor Discovery

Router discovery:





IPv6: Autoconfiguración de interfaces

- Mecanismo que permite atribuir direcciones unicast a los nodos
  - sin necesidad de realizar configuraciones manuales.
  - sin utilizar servidores adicionales.
  - con una configuración mínima de los routers.

- Genera direcciones IP a partir de información enviada por los routers y datos locales como la dirección MAC
- Genera una dirección para cada prefijo informado en los mensajes RA

QUIC: Evolución de la capa de transporte

QUIC: Evolución de la capa de transporte

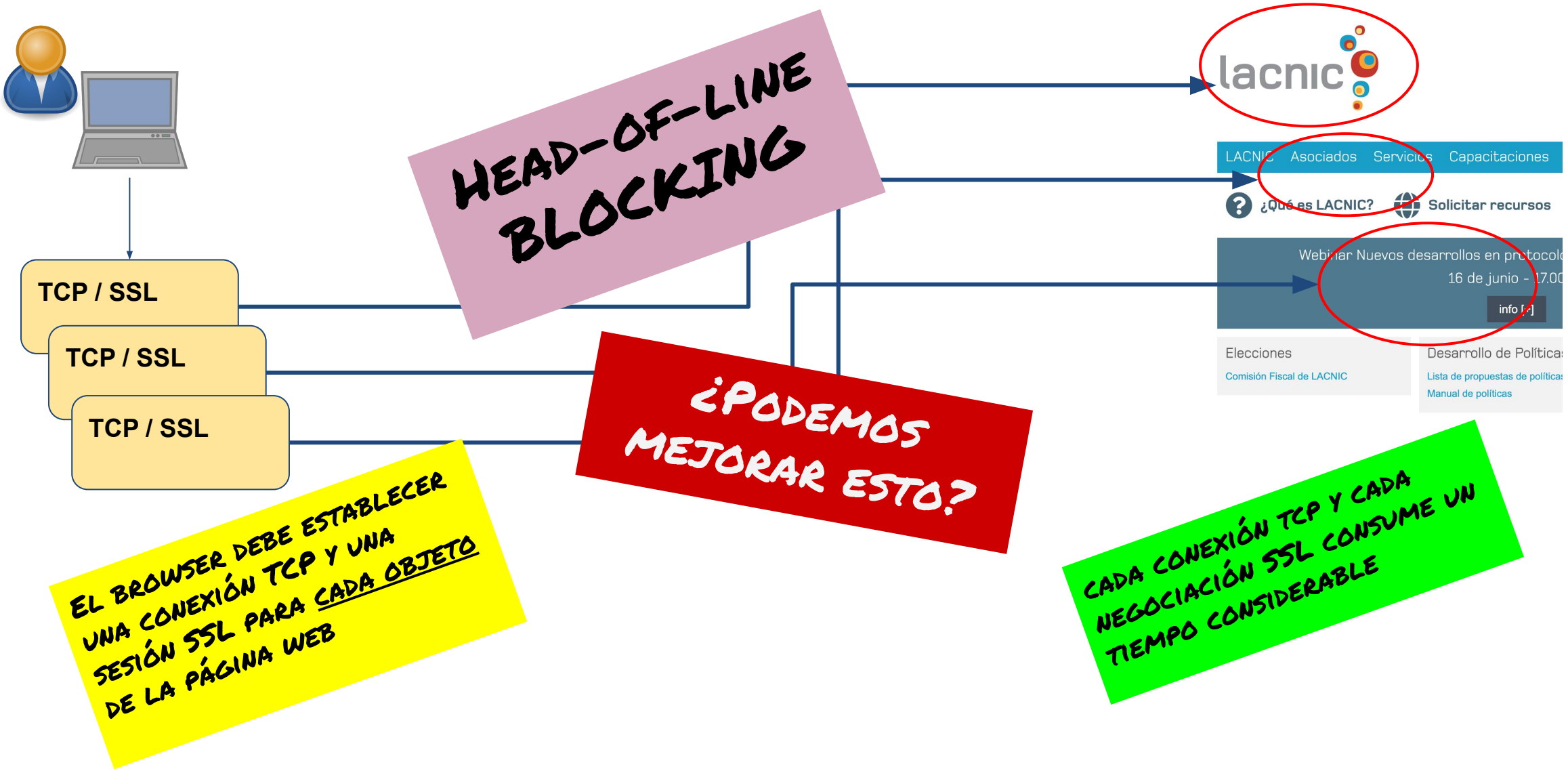
Capa de transporte:

- Modelo de servicio entre aplicaciones y la capa de red
- “*Confiable y ordenado*” vs “*No confiable*”

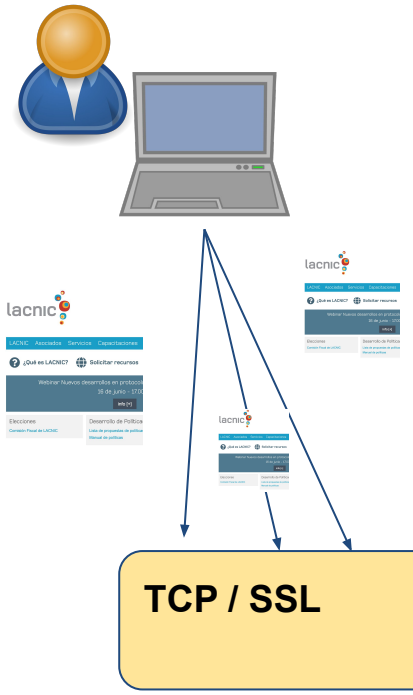
Un poco de historia:

- Experimento de Google (“Google QUIC”)
- Ahorrar tiempos de negociación SSL
- Incrementar performance a través de adaptar el control de flujo a la realidad de las redes de hoy

HTTP 1.1: *Hypertext Transport Protocol*



HTTP/2



TCP / SSL

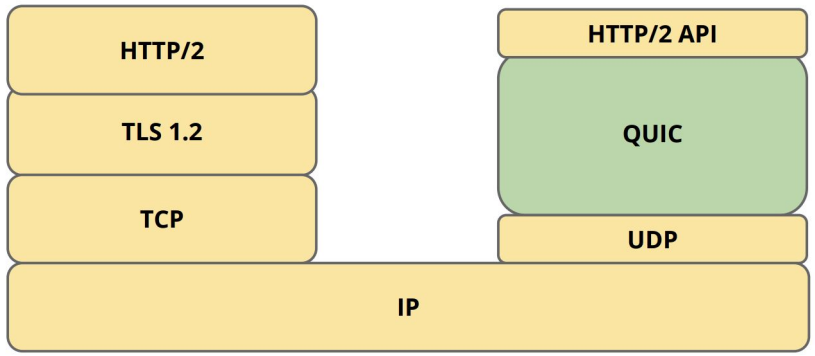
EL BROWSER ESTABLECE UNA ÚNICA CONEXIÓN TCP/SSL Y UTILIZA LOS "STREAMS" DE HTTP/2

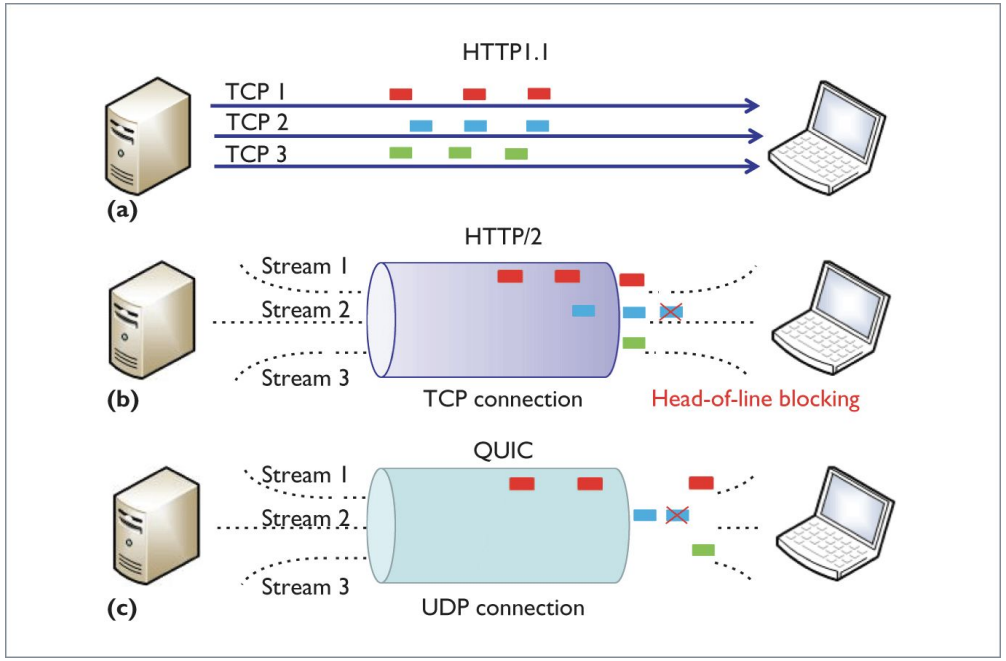
¿PODEMOS MEJORAR ESTO?

DE TODAS FORMAS, HAY HOL BLOCKING, PORQUE EL TRANSPORTE NO CONOCE A LOS STREAMS, NO TIENE NOCIÓN DE PARALELISMO EN LA APLICACIÓN.

QUIC

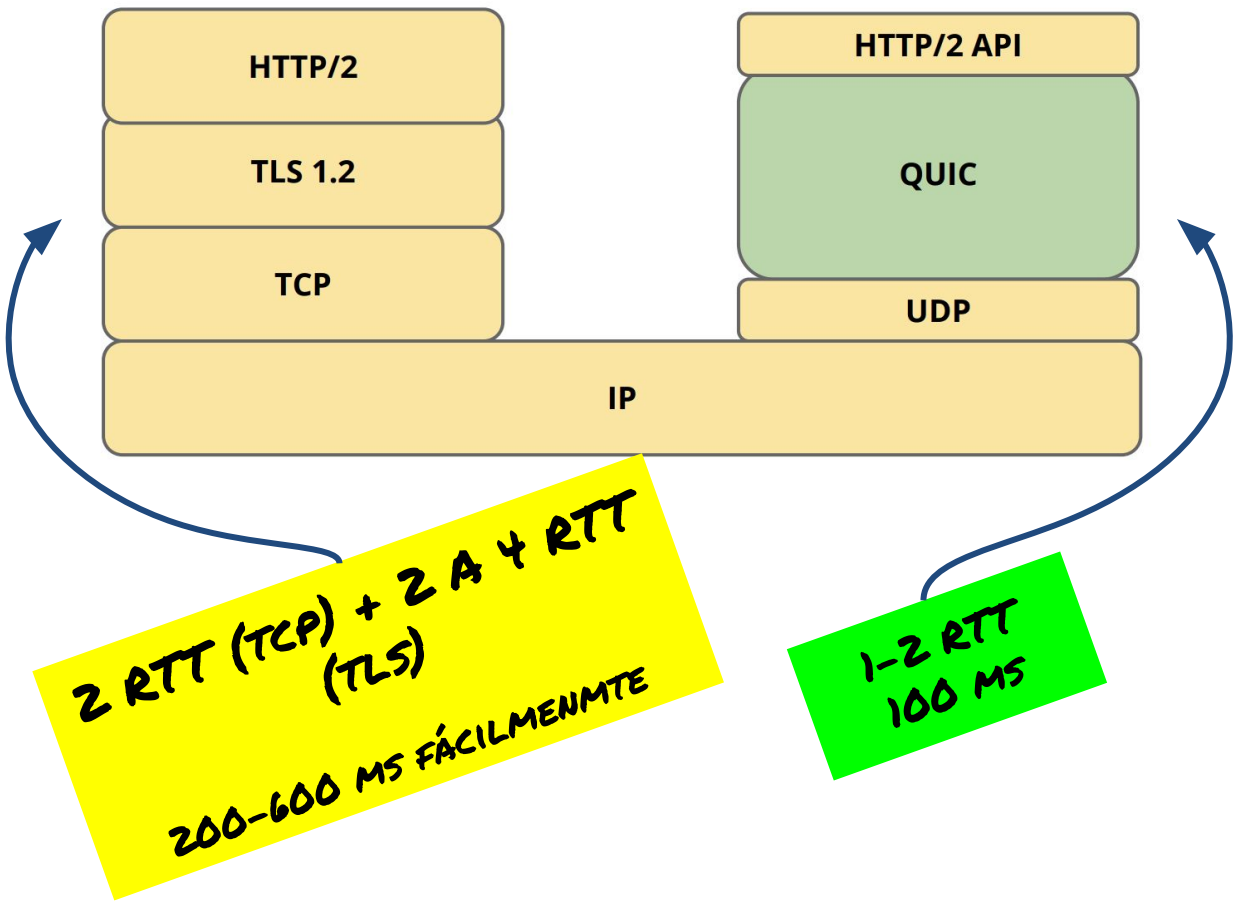
- **Q**uick **U**DP **I**nternet **C**onnections
- HTTP sobre QUIC





  - QUIC es:
    - cifrado por defecto, multiplexa conexiones, no sufre de NAT, basado en UDP (0-RTT connection establishment)

QUIC: *Quick UDP Internet Connections*



¿Por qué usar UDP?:

- *stack ossification***
- kernel space vs. user space
- no hay 3-way handshake
- Criptografía embebida:
  - TLS 1.3
  - 0 RTT handshake

QUIC

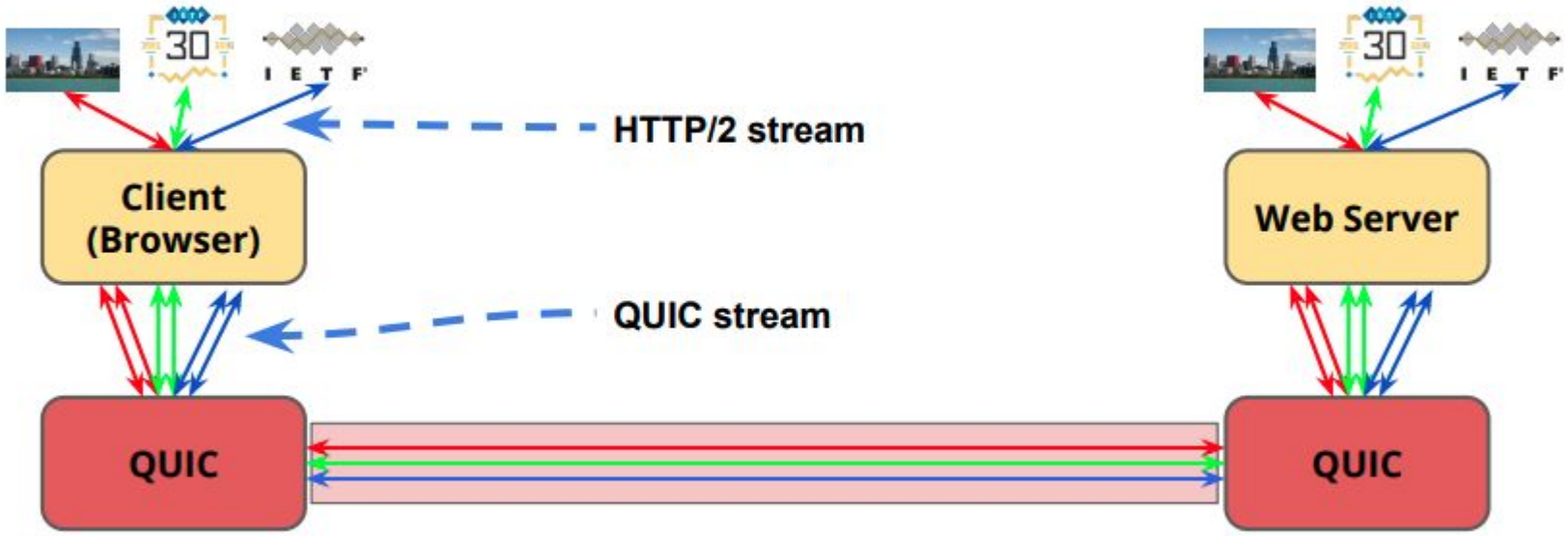
Establecimiento de conexiones:

- 0 RTT a un servidor “ya conocido”
- 1 RTT si las claves criptográficas no son recientes
- 2 RTT si la *versión* de QUIC debe ser negociada

Luego:

- Los pedidos / respuestas de HTTP fluyen dentro de la conexión QUIC

HTTP sobre QUIC



QUIC

Funcionalidades esperadas:

- Relativa facilidad para el despliegue y posterior evolución
- Bajas latencias en el establecimiento de las conexiones
- Streaming
- Mejores características de recuperación y mayor flexibilidad para implementar control de congestión
- **Resistencia al *NAT-Rebinding***
- Multipath para mayor resiliencia y balanceo de carga

QUIC

- El uso de UDP como base permite el despliegue pasando por las middleboxes actuales y permite la implementación a nivel usuario
- Negociación de versiones permite la evolución paulatina del protocolo
- Cifrado incluso hasta en los encabezados
  - problema en potencia para los operadores de red

Conclusiones

Después de casi 40 años del stack TCP/IP, estamos ante la necesidad de evolucionar el mismo.

En capa de red, IPv6 nos permite acceder a direcciones de 128 bits y un procesamiento simplificado de encabezados.

En la capa de transporte QUIC incorpora años de lecciones aprendidas y una serie de optimizaciones y mejoras de seguridad.

¡Muchas gracias por su atención!

¿Preguntas?

¡Muchas gracias por su atención!