



# Teoría de las Comunicaciones

Edición 65 oficial, pero en realidad desde que se comenzó a dictar (a.k.a Redes) es la edición 74. Este es el último cuatrimestre que se dicta.

**Dr. Claudio Enrique Righetti**

15 septiembre 2025

*Segundo Cuatrimestre*

**Departamento de Computación  
Facultad de Ciencias Exactas y Naturales  
Universidad de Buenos Aires  
Argentina**

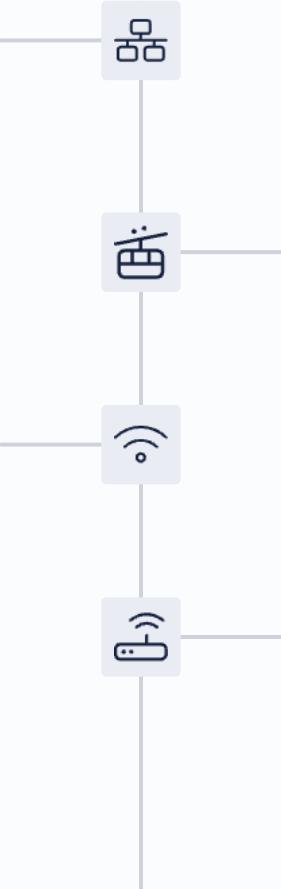
# Agenda : Módulos (1-4)

## Módulo 1: Fundamentos de Redes

Historia y evolución de redes, modelos OSI y TCP/IP, señales analógicas vs. digitales, teoría de la información y teoremas de Shannon. Práctica: cálculo de entropía, codificación Huffman y análisis de capacidad de canal.

## Módulo 3: Redes de Acceso y LAN

Tecnologías inalámbricas, Ethernet, switching y VLANs. Práctica: configuración de switches y análisis de tráfico con Wireshark.



## Módulo 2: Nivel Físico y Enlace

Técnicas de codificación y modulación, medios de transmisión, protocolos de enlace y mecanismos de ventana deslizante. Práctica: implementación de protocolos nivel 2, CRC y algoritmos Stop & Wait.

## Módulo 4: Nivel de Red

Redes Orientadas a conexión ( Circuitos Virtuales ) y sin Conexión ( Datagramas). **Protocolo IP**, tablas de ruteo, algoritmos Distance Vector y Link State. Práctica: direccionamiento IP, ICMP y configuración de RIP y OSPF.

Al finalizar estos cuatro módulos, se realizará el primer parcial para evaluar la comprensión de los conceptos fundamentales de redes. Estos módulos establecen las bases necesarias para abordar temas más avanzados en la segunda parte del curso.

# Estructura de Módulos (5-8)



## Módulo 5: Capa de Transporte



Análisis detallado del protocolo TCP, cálculo del RTO, mecanismos de control de flujo y errores. Práctica: comparación UDP vs. TCP, máquina de estados y análisis de conexiones.



## Módulo 6: Control de Congestión



Problema de congestión en redes, curvas de tráfico, taxonomía de soluciones y mecanismos de realimentación. Práctica: implementación de algoritmos Slow Start y Congestion Avoidance.



## Módulo 7: Capa de Aplicación



Arquitecturas cliente-servidor vs. peer-to-peer, servicios fundamentales como Web, correo electrónico y DNS. Práctica: herramientas de diagnóstico y protocolos HTTP, SMTP, POP3, IMAP.



## Módulo 8: Performance y Seguridad



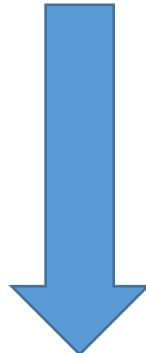
Análisis de rendimiento, factores que afectan el desempeño, algoritmos criptográficos y conceptos de seguridad. Práctica: configuración de firewalls, certificados digitales y protocolos seguros.

Estos módulos avanzados completan la formación integral en redes, abordando aspectos críticos como el transporte confiable de datos, la gestión de congestión, las aplicaciones de red y la seguridad. Al finalizar el curso, los estudiantes habrán adquirido tanto conocimientos teóricos sólidos como experiencia práctica en la implementación y análisis de redes.

# Recordemos que es Wi-Fi

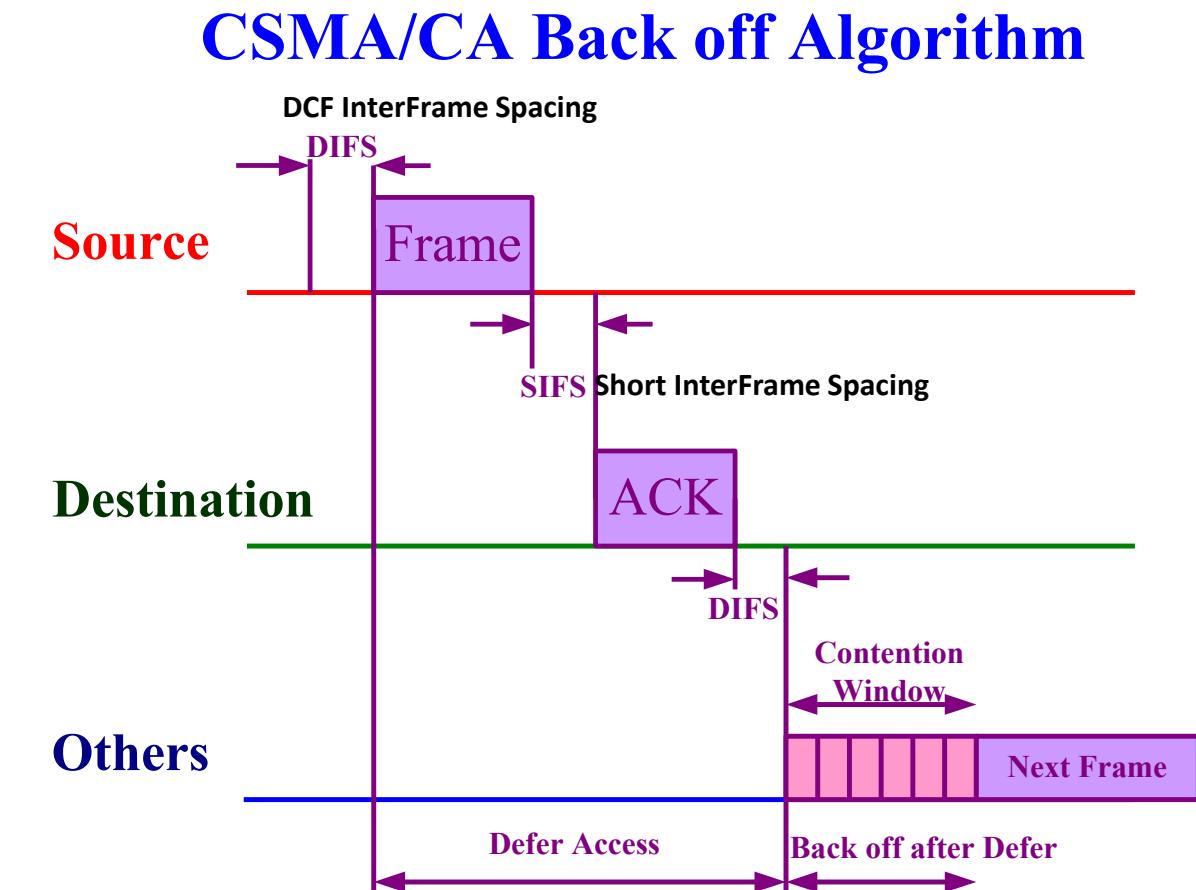
- El término "Wi-Fi" fue creado por la organización sin fines de lucro **Wi-Fi Alliance** y se refiere a un grupo de protocolos de redes inalámbricas que se basan en el estándar de red IEEE 802.11
- La tecnología Wi-Fi existe desde finales de los noventa, pero ha mejorado drásticamente en la última década

# El ecosistema de Wi-Fi: ¿cambio en los últimos 20 años?



# Listen Before-to-Talk y DCF MAC: La ventana de contención

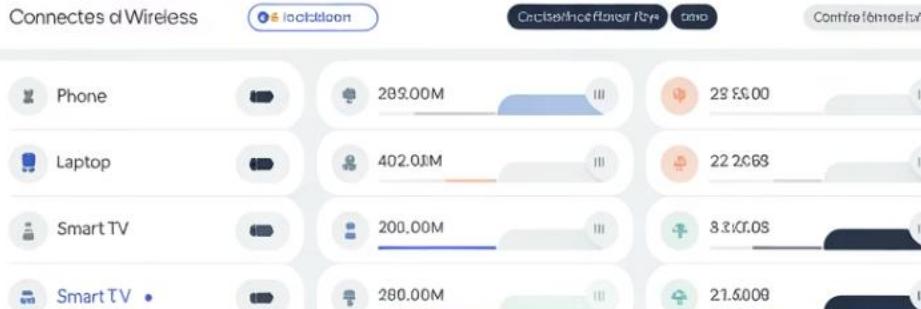
- Mientras el canal está libre el nodo decrementa el backoff counter (caso contrario se mantiene)
- Si backoff counter==0
  - El nodo TX el frame
- Si la TX no es exitosa (no ACK)
  - La *ventana de contención* (contention window) se selecciona de un intervalo random que es el doble del intervalo previo
  - este proceso se repite hasta que el canal esté libre



## Optimize your Wireless

Identify bottlenecks and Improve performance

Analyze Now



# Acceso Múltiple: El Reto del Aire Compartido



## Competencia por recursos

Múltiples dispositivos intentan usar el mismo canal inalámbrico simultáneamente.



## Problema de colisiones

Las transmisiones simultáneas generan interferencias y pérdida de datos.



## Necesidad de coordinación

Se requieren mecanismos que ordenen el acceso al medio compartido.



# ¿Qué es Listen Before Talk (LBT)?



## Escuchar

El dispositivo monitorea el canal para detectar actividad.



## Esperar

Si el canal está ocupado, pospone la transmisión.



## Transmitir

Envía datos sólo cuando detecta que el canal está libre.

# El Papel de DCF en Wi-Fi



## Función principal

Control de acceso al medio en redes IEEE 802.11



## Detección de portadora

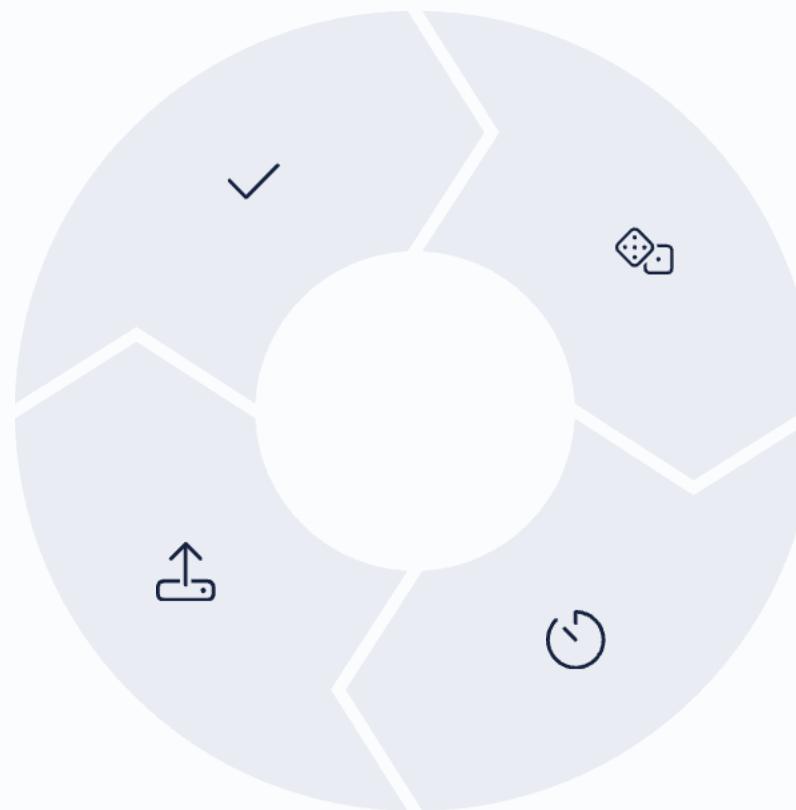
Basado en CSMA/CA: monitoreo continuo del canal



## Organización distribuida

Utiliza ventanas de contención para ordenar acceso

# La Ventana de Contención en DCF



**Canal libre**

El dispositivo detecta que no hay transmisiones activas

**Valor aleatorio**

Selecciona un número entre 0 y CW

**Transmisión**

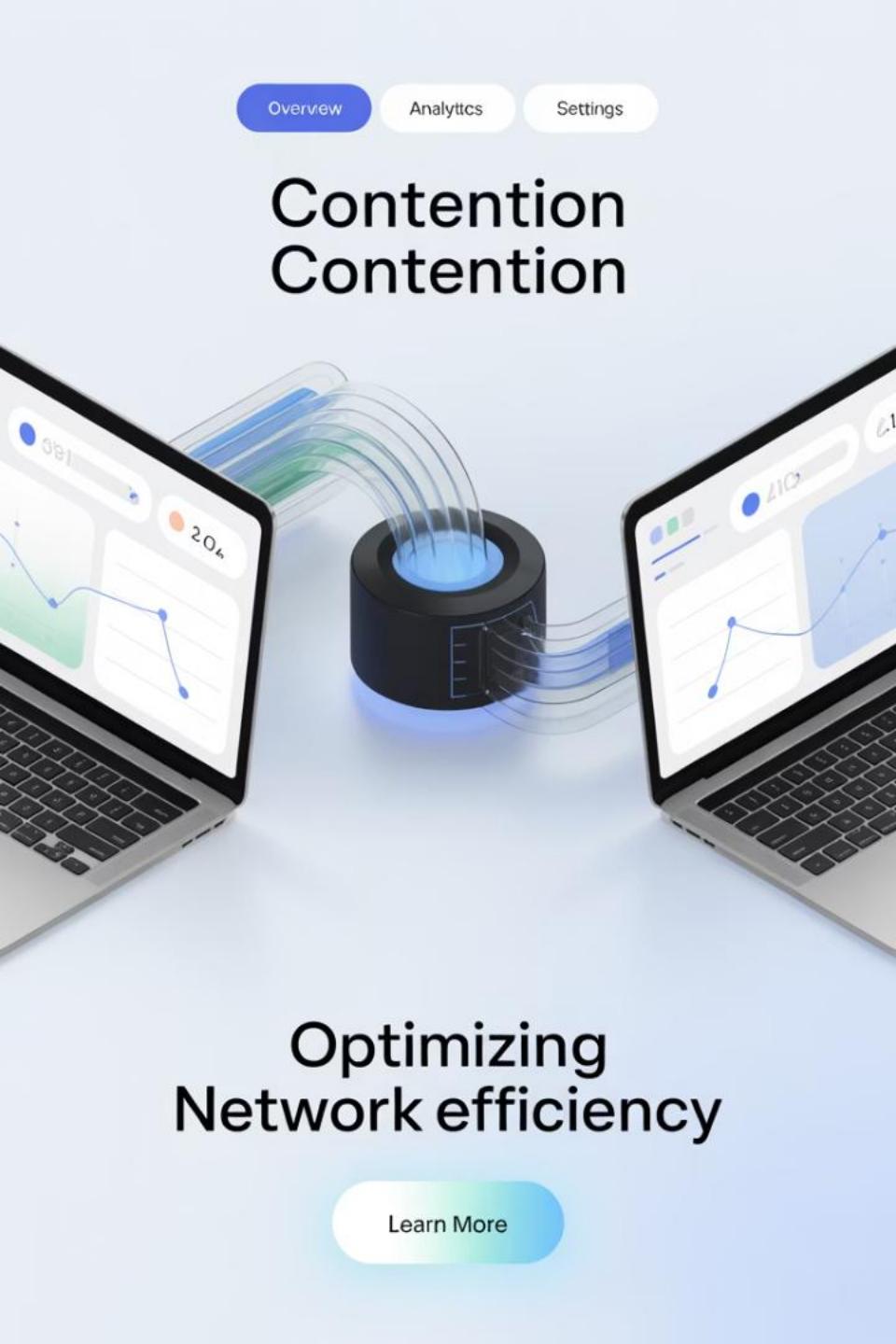
Envía datos cuando su contador llega a cero primero

**Cuenta regresiva**

Espera mientras el contador disminuye hasta cero

# Relación entre LBT y la Ventana de Contención





# Ejemplo Práctico: ¿Cómo Funciona en la Vida Real?

2

Dispositivos

Laptops intentando transmitir  
simultáneamente

1

Canal

Medio inalámbrico compartido entre  
ambos

0

Colisiones

Resultado ideal tras aplicar LBT y  
contención



**Seamless connectivity.  
Limitless potential.**

# Conclusiones y Tendencias Futuras

## Beneficios actuales

- Mayor eficiencia en redes congestionadas
- Reducción significativa de interferencias
- Mejor experiencia para usuarios finales

## Desafíos pendientes

- Saturación en entornos de alta densidad
- Optimización para aplicaciones en tiempo real
- Compatibilidad entre diferentes estándares

## Innovaciones futuras

- Algoritmos adaptativos de contención
- Integración con inteligencia artificial
- Coordinación multi-banda automatizada

# Anomalía de Wi-fi



- ▶ En WiFi los nodos de baja velocidad degradan el throughput de los nodos de alta velocidad
- ▶ Los nodos reducen su data rate cuando la potencia de la señal es baja (WiFi auto-rate)
- ▶ Los paquetes de los nodos de baja velocidad consuelen más “tiempo de aire”
  - ▶ Monopolizan el canal Half Duplex
- ▶ WiFi arbitra las transmisiones paquete a paquete
  - ▶ Los nodos de alta velocidad reciben menos “tiempo de aire”

Standard	Frequency (GHz)	Bandwidth (MHz)	Modulation	Max Data Rate
802.11b	2.4	22	DSSS	11 Mbps
802.11a	5	20	OFDM	54 Mbps
802.11g	2.4	20	OFDM	54 Mbps
802.11n	2.4, 5	20, 40	MIMO-OFDM	600 Mbps



# Anomalía de Velocidad en Redes 802.11

En el mundo de las redes inalámbricas, existe un fenómeno crítico conocido como la "anomalía de rendimiento" que afecta significativamente la velocidad de todas las terminales conectadas a una red Wi-Fi.

Este problema, presente desde los primeros estándares 802.11 desarrollados en 1997, puede causar una reducción del 40-60% en el rendimiento total de redes empresariales. El efecto, también denominado "efecto de estación lenta", representa uno de los desafíos más persistentes en las comunicaciones inalámbricas modernas.

# Fundamentos de la Anomalía 802.11

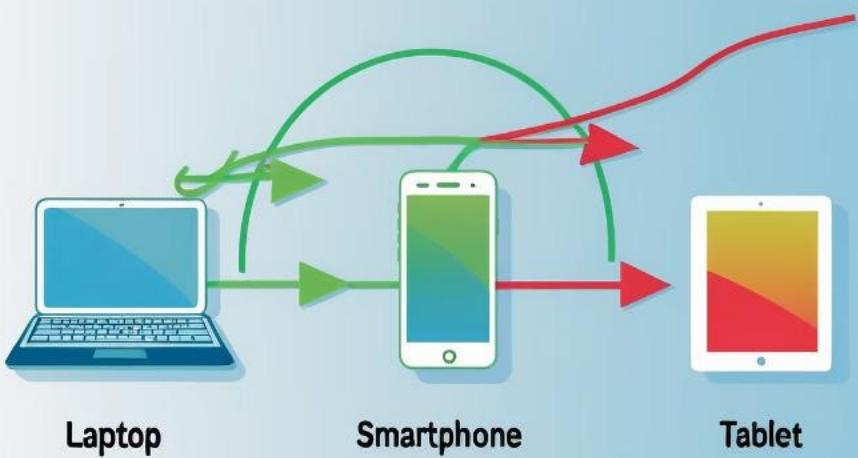
## Acceso Equitativo

El protocolo CSMA/CA otorga acceso equitativo por paquete a todas las terminales, independientemente de su velocidad de transmisión. Esto significa que cada dispositivo recibe la misma oportunidad para enviar datos, sin considerar el tiempo que tardará en hacerlo.

## Consumo Desproporcionado

Las terminales lentas consumen un tiempo desproporcionado de transmisión, pudiendo utilizar hasta 10 veces más tiempo de aire que las terminales rápidas para enviar la misma cantidad de datos. Este problema ha sido documentado desde la aparición del estándar 802.11b en 1999.

# Mecánica de la Anomalía



La raíz del problema reside en cómo el protocolo MAC (Control de Acceso al Medio) otorga igualdad de oportunidades a todas las estaciones, sin considerar su velocidad. Esta democracia en el acceso al medio se convierte en un obstáculo cuando las velocidades son muy dispares.



## Terminal Rápida (54 Mbps)

Transmite 1500 bytes en apenas 0.22 milisegundos



## Terminal Lenta (1 Mbps)

Necesita 12 milisegundos para transmitir los mismos 1500 bytes



## Factor de Diferencia

Una terminal a 1 Mbps ocupa el canal 54 veces más tiempo que una a 54 Mbps

# Impacto en Rendimiento de Red



El rendimiento global de la red Wi-Fi tiende a caer dramáticamente al nivel del dispositivo más lento conectado. Una sola terminal operando a baja velocidad puede reducir el throughput total en hasta un 80%, afectando a todos los usuarios.

Este efecto se ve agravado en ambientes con múltiples dispositivos compitiendo por el acceso al medio. Situaciones comunes que provocan este problema incluyen dispositivos alejados del punto de acceso, presencia de interferencias electromagnéticas o el uso de equipos antiguos con estándares obsoletos.

# Evolución de Soluciones en Estándares Wi-Fi

## Primeras Soluciones

Los primeros intentos de mitigación incluyeron técnicas básicas de gestión de ancho de banda y algoritmos de control de acceso al medio, pero con resultados limitados en los estándares originales.

## Protocolos QoS

La incorporación de mecanismos de calidad de servicio (QoS) desde Wi-Fi 4 permitió establecer prioridades entre diferentes tipos de tráfico, ofreciendo una solución parcial al problema.

## Tecnologías MIMO

El desarrollo de tecnologías MIMO (Multiple Input Multiple Output) y posteriormente MU-MIMO (Multi-User MIMO) ha sido clave en la reducción del impacto de la anomalía, permitiendo comunicaciones simultáneas.

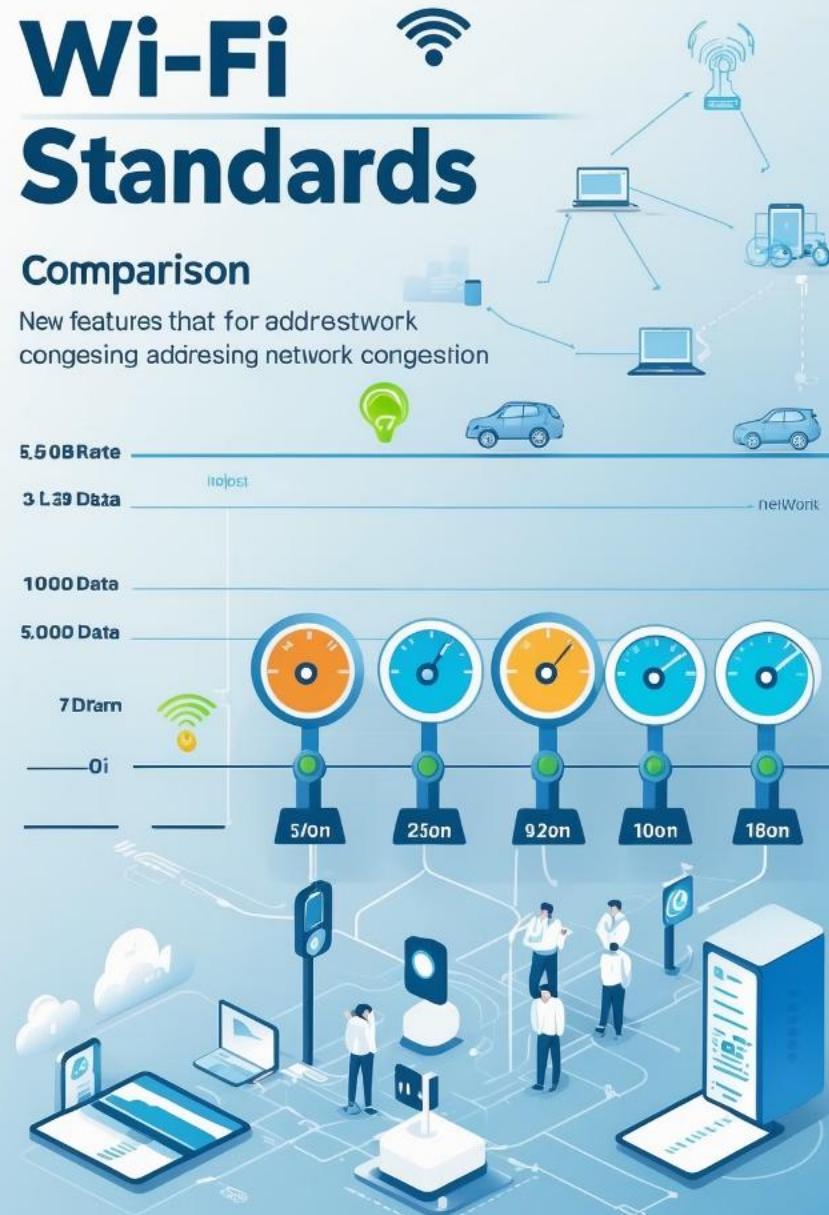
## Soluciones Avanzadas

Los estándares más recientes implementan técnicas sofisticadas como OFDMA y operaciones multi-enlace que abordan directamente el problema de la anomalía de rendimiento.

# Comparativa de Estándares Wi-Fi y Mitigación de Anomalía

Estándar	Año	Velocidad Máx.	Mitigación de Anomalía	Técnica Principal
Wi-Fi 4 (802.11n)	2009	600 Mbps	Parcial	Frame Aggregation
Wi-Fi 5 (802.11ac)	2014	6.9 Gbps	Media	MU-MIMO (DL)
Wi-Fi 6 (802.11ax)	2019	9.6 Gbps	Alta	OFDMA + Scheduling
Wi-Fi 7 (802.11be)	2024	46 Gbps	Muy Alta	Multi-Link Operation

La evolución de los estándares Wi-Fi muestra un progreso significativo en la capacidad para mitigar la anomalía de estación lenta. Cada nueva generación ha introducido mecanismos más sofisticados que permiten un uso más eficiente del espectro y reducen el impacto negativo de los dispositivos lentos.



# Soluciones Tecnológicas Implementadas

## OFDMA

Wi-Fi 6 introduce la tecnología OFDMA (Orthogonal Frequency Division Multiple Access) que divide el canal en pequeñas unidades de recursos, permitiendo que múltiples dispositivos transmitan simultáneamente, reduciendo drásticamente el impacto de terminales lentas.

## Schedulers Inteligentes

Los algoritmos avanzados de programación (scheduling) priorizan inteligentemente las terminales rápidas, optimizando el uso del tiempo de aire y evitando que dispositivos lentos monopolicen el canal de comunicación.

## Target Wake Time

Esta función permite programar con precisión cuándo los dispositivos deben despertar para transmitir datos, reduciendo la congestión y las colisiones en la red, particularmente útil en entornos con alta densidad de dispositivos.

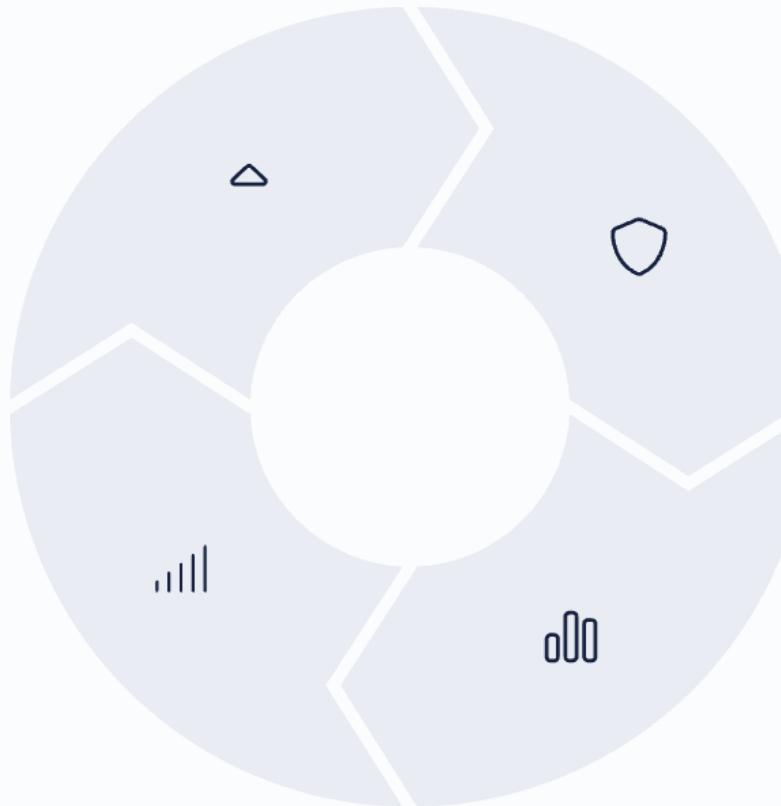
## BSS Coloring

La técnica de "coloreado" BSS minimiza la interferencia entre redes superpuestas, permitiendo transmisiones paralelas y reduciendo los tiempos de espera que exacerbán el problema de la anomalía de rendimiento.

# Recomendaciones Prácticas

**Actualizar Infraestructura**  
Implementar dispositivos compatibles con Wi-Fi 6 o superior cuando sea posible

**Banda de 5 GHz**  
Priorizar esta banda para dispositivos críticos que requieren mayor rendimiento



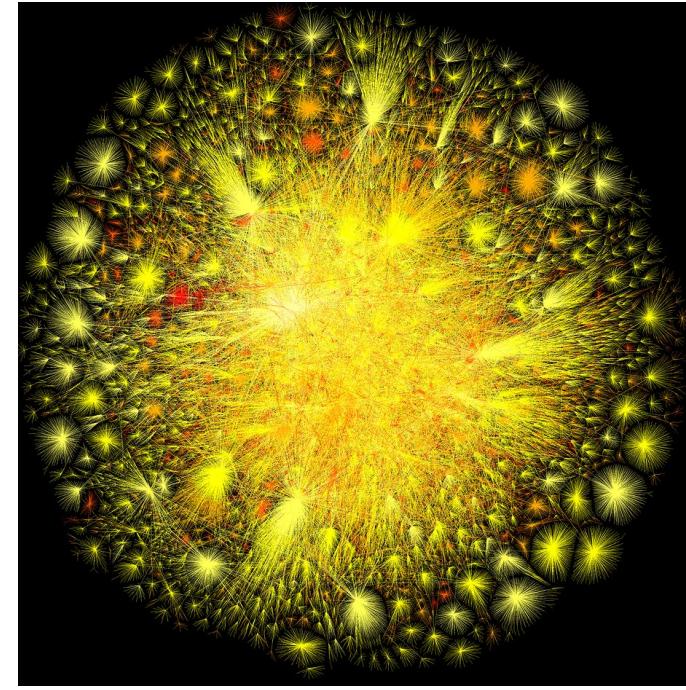
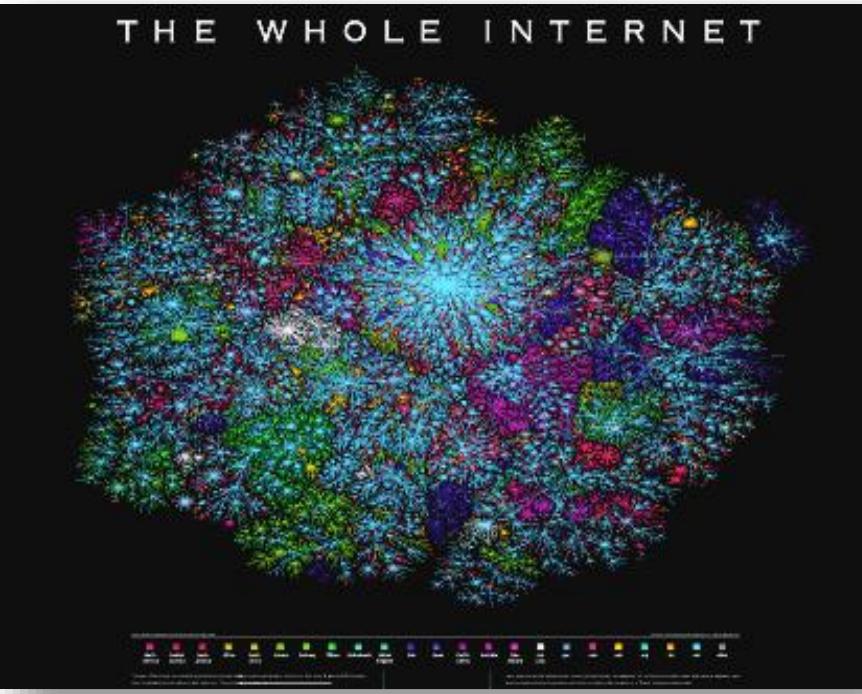
## Políticas de Banda

Configurar redes separadas o políticas específicas para dispositivos antiguos

## Monitoreo Continuo

Utilizar herramientas como Wireshark, Ekahau o AirMagnet para diagnóstico

Para mitigar efectivamente la anomalía de rendimiento en redes 802.11, es fundamental adoptar un enfoque proactivo en la gestión de la infraestructura Wi-Fi. La combinación de hardware moderno, configuración optimizada y monitoreo constante permitirá maximizar el rendimiento incluso en presencia de dispositivos con capacidades limitadas.

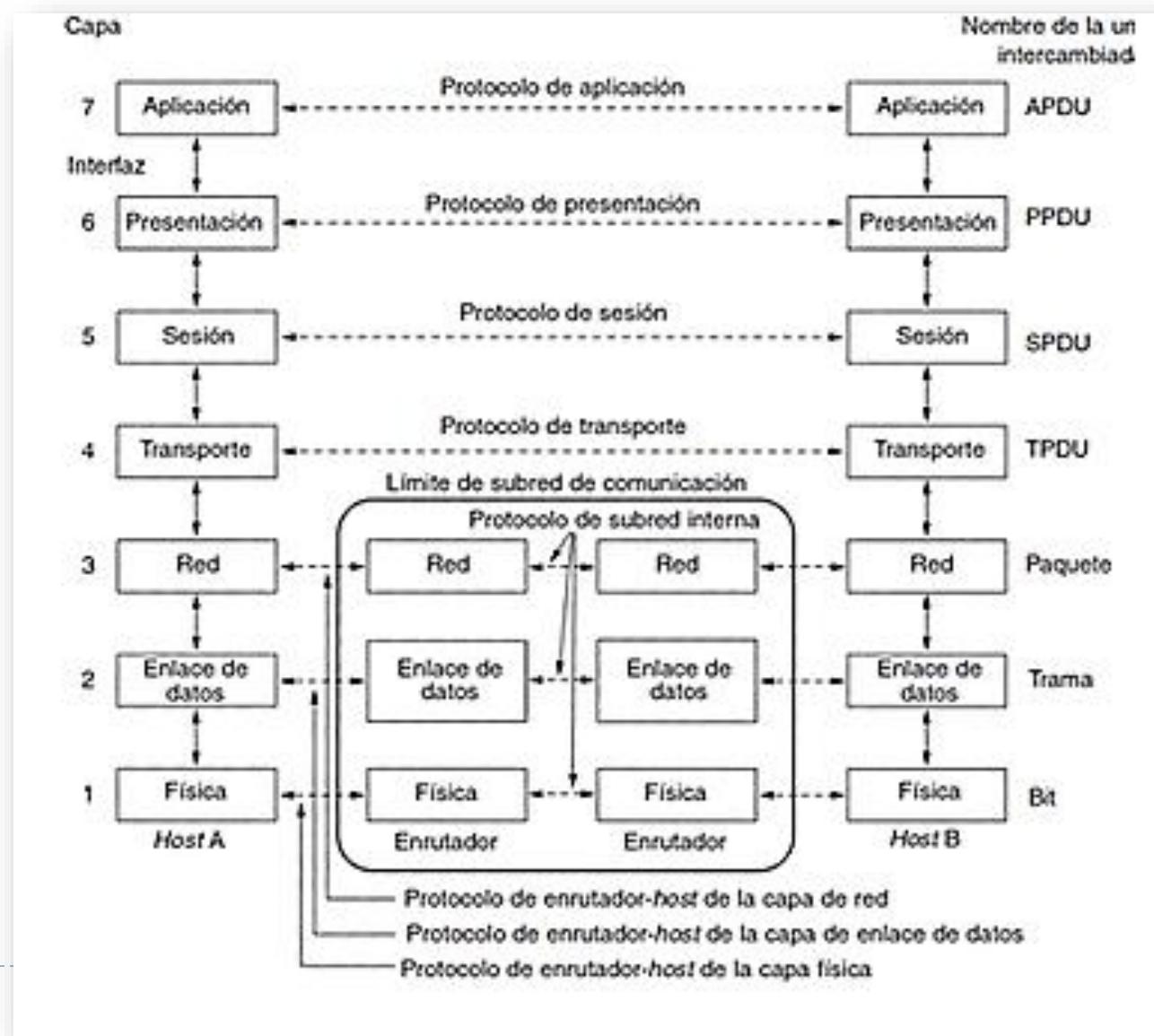


Nivel de Red

Introducción a IP

[http://www.?](http://www.)

# “El Modelo OSI”



# Agenda

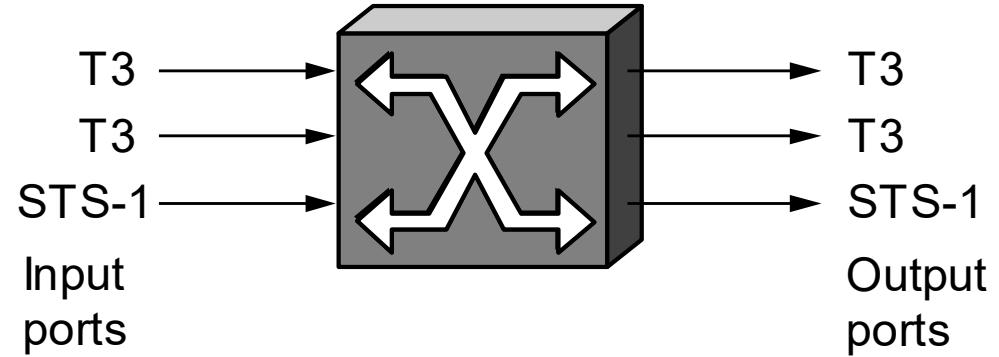
---

- ▶ Circuitos Virtuales
- ▶ Datagramas
- ▶ Introducción IP

# “Redes Escalables”

---

- ▶ Switch



# ¿Qué es un switch?

---

- ▶ Es una “*appliance*” que **interconecta enlaces** para formar redes más grandes.
- ▶ Un switch de datos es un dispositivo con múltiples entradas y múltiples salidas.
- ▶ Su trabajo es lograr que la mayor cantidad de paquetes que entran al switch vayan a la **salida apropiada**.
  - ▶ Envía paquetes, frames o celdas de un **puerto de entrada** a un **puerto de salida** (función conocida como **switching** ó **forwarding**)
  - ▶ El **puerto de salida** se **selecciona** utilizando una dirección que trae el header (encabezado) del paquete, frame o celda.
- ▶ Según el tipo de switch:
  - ▶ Para distribuir los paquetes, algunos utilizan **circuitos virtuales** y otros **comutación de paquetes**.
  - ▶ Pueden comutar paquetes de longitud variable o de longitud fija.

# El switch permite construir redes escalables

---

- ▶ Los switches permiten, al interconectarse unos con otros, cubrir mayores áreas geográficas.
  - ▶ Permiten construir redes más grandes
  - ▶ Ofrecen tolerancia a la latencia (mediante buffers)
- ▶ Pueden soportar un gran número de nodos (ancho de banda es escalable).
- ▶ Colocar un nuevo host a un switch no necesariamente carga más la red.



# Commutación de Paquetes: Dos grandes paradigmas



Orientado a Conexión vs. Sin Conexión

# Sin conexión: Datagramas

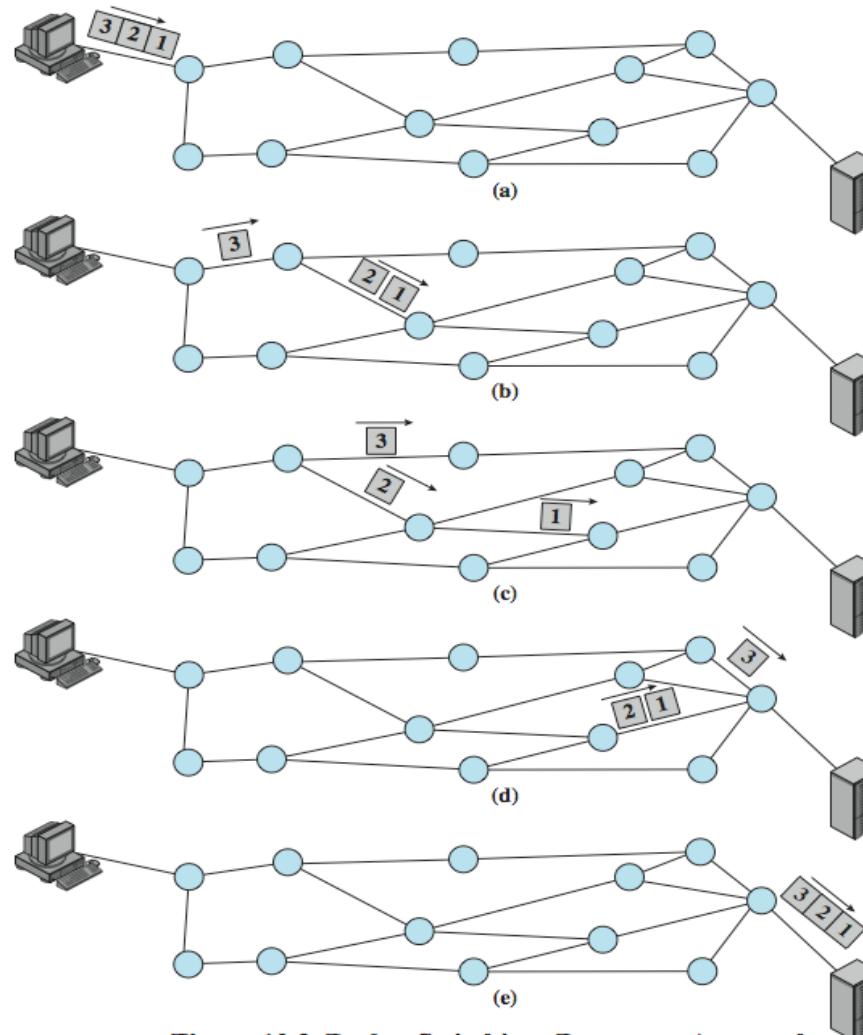


Figure 10.9 Packet Switching: Datagram Approach

# Orientado a Conexión: Circuito Virtual

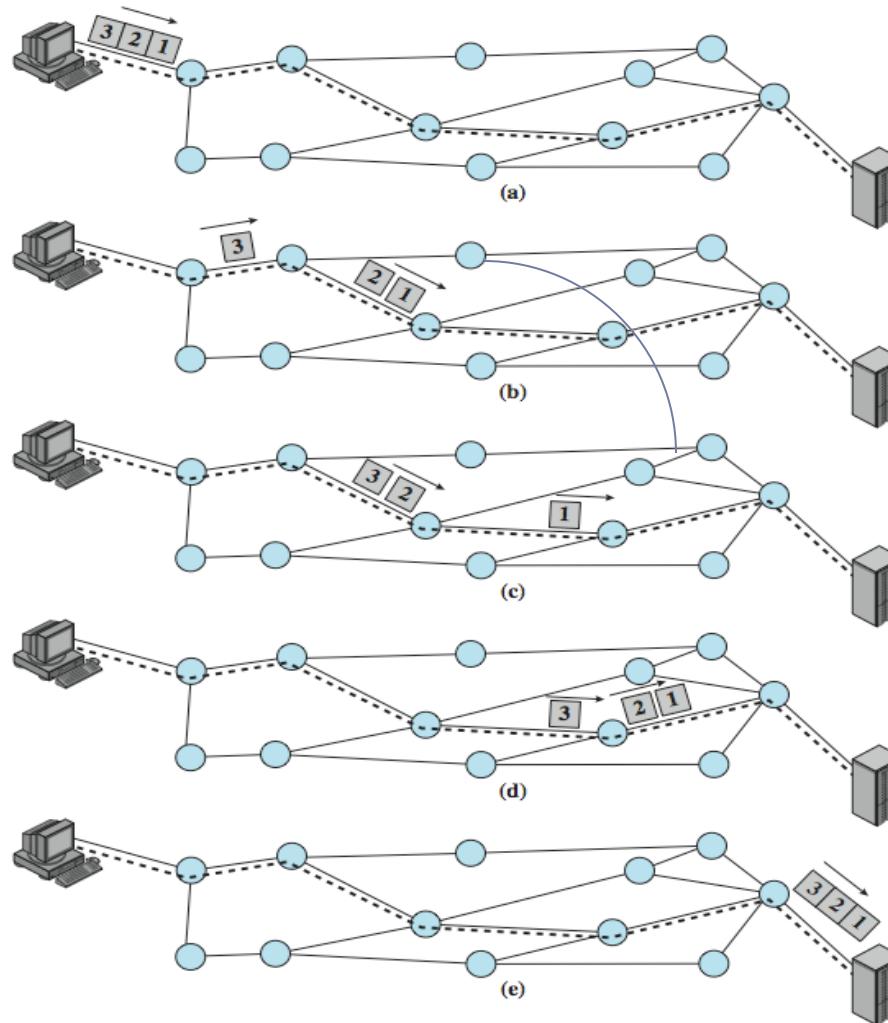
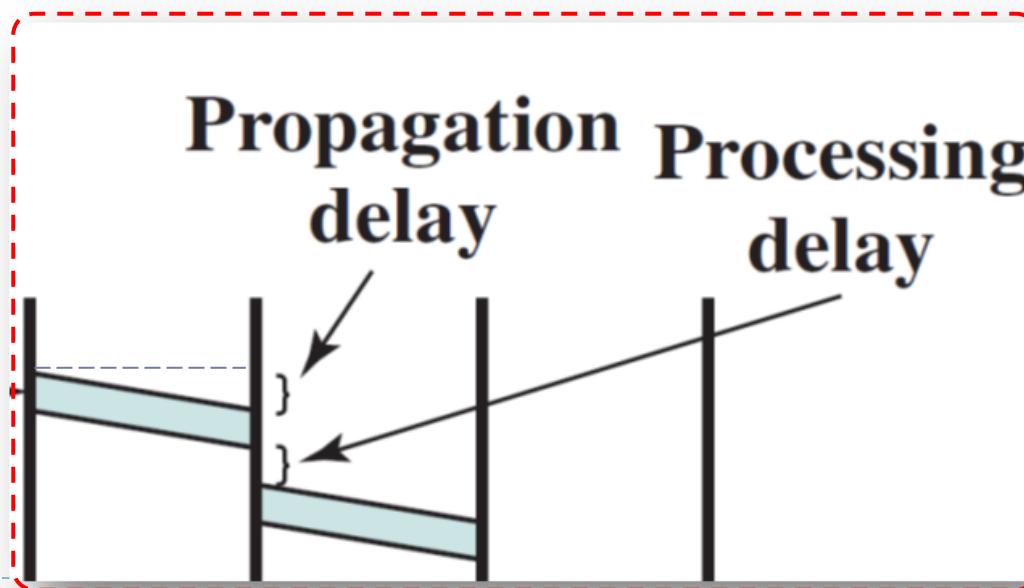


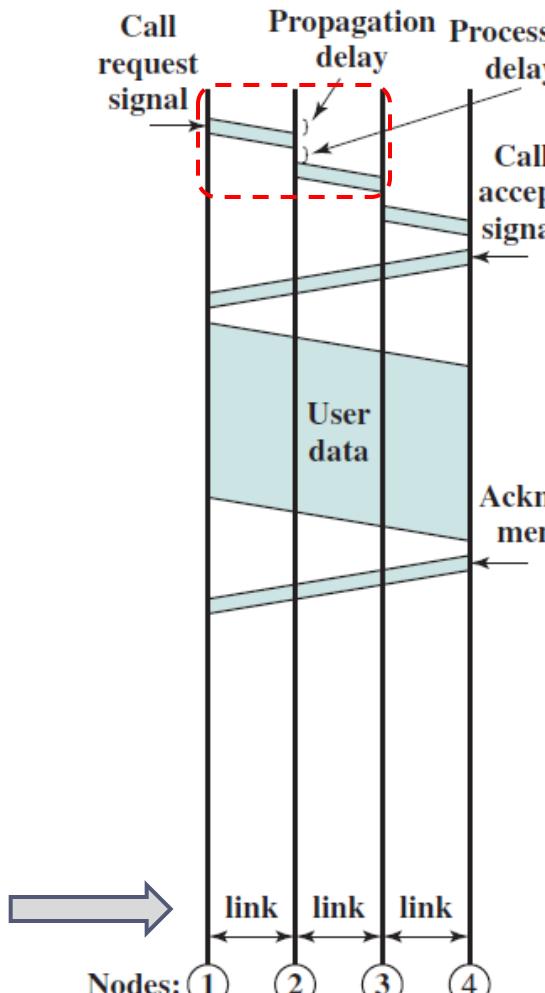
Figure 10.10 Packet Switching: Virtual-Circuit Approach

# Commutación de Circuitos vs. conmutación de Paquetes

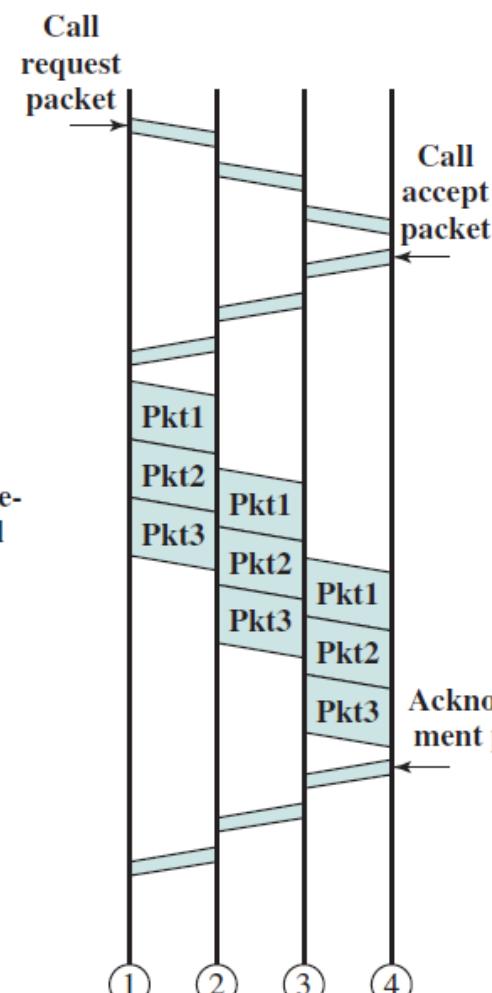
- ▶ La performance “punta a punta” depende de varios retardos:
  - ▶ Tiempo de procesamiento (en cada nodo)
  - ▶ Tiempo de transmisión (desde cada nodo)
  - ▶ Tiempo de propagación (en cada enlace físico)
- ▶ Otras características:
  - ▶ Overheads
  - ▶ “Transparencia”
    - ▶ Forward/Filter/Flood



# Temporización de eventos

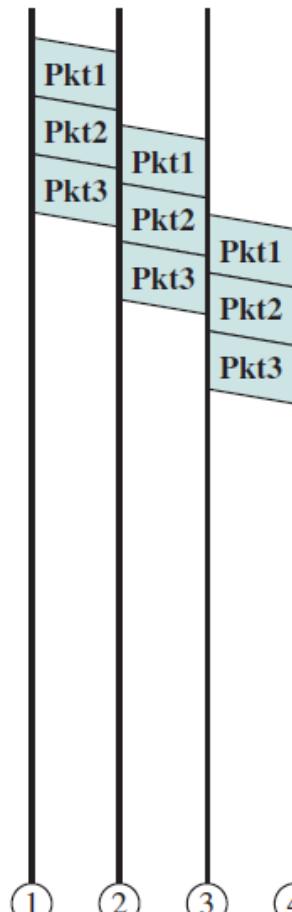


(a) Circuit switching



(b) Virtual circuit packet switching

esquema más utilizado



(c) Datagram packet switching

# Conmutación sin conexión (datagrama)

---

- ▶ Características

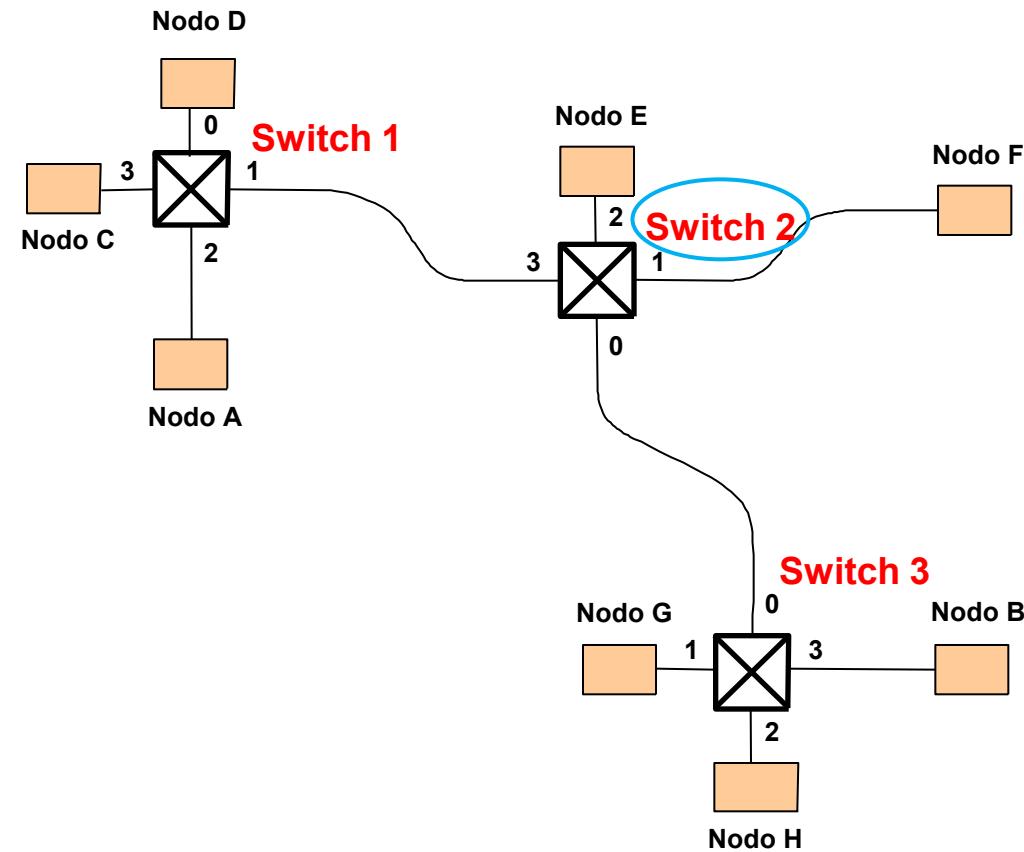
- ▶ No existe una fase para establecer una conexión
  - ▶ el nodo puede enviar el paquete “*cuando quiera*”.
- ▶ Cada paquete se envía independientemente
  - ▶ debe llevar **toda la información necesaria** para alcanzar su destino.

# Commutación sin conexión (datagrama)

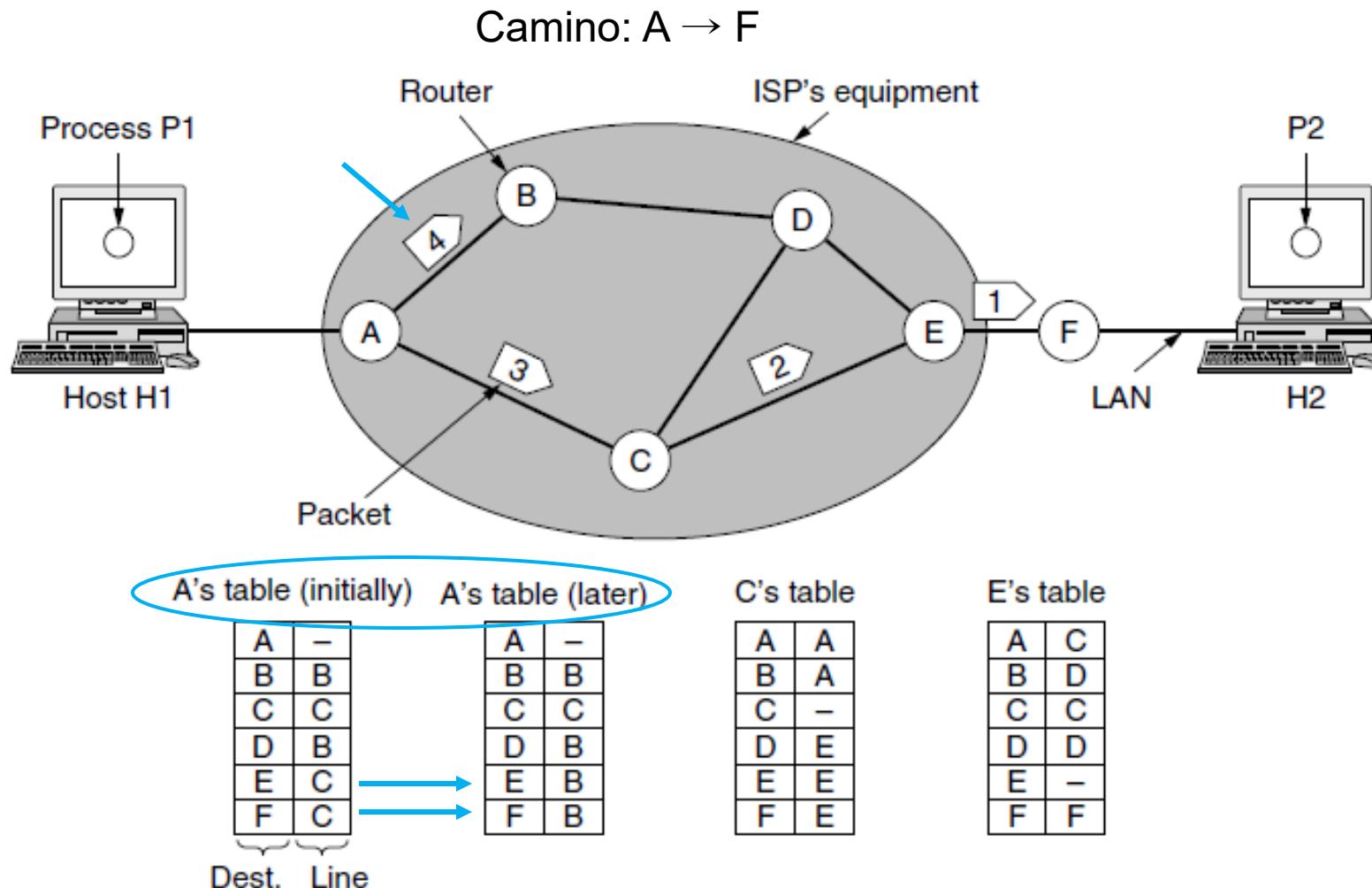
Analogía: sistema postal

Cada switch mantiene una tabla de *forwarding (routing)*

Tabla de commutación para el switch 2	
Destino	Puerto
A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0



# Enrutamiento en una red de datagramas



# Modelo de Datagrama

---

- ▶ No se debe esperar un RTT (*round trip time*) para establecer una conexión
  - ▶ Un nodo puede enviar datos tan pronto como este listo.
  - ▶ El nodo origen no tiene porque saber si la red es capaz de entregar un paquete o si el nodo destino está listo para recibir los datos.
- 
- ▶ Ya que los paquetes son tratados independientemente, es posible cambiar el camino
    - ▶ Por ejemplo para evitar enlaces y nodos que estén fallando
  - ▶ Ya que cada paquete lleva la dirección completa del nodo destino
    - ▶ la **información adicional de control (overhead)** que lleva es mucho mayor que la utilizada en el modelo orientado a conexión

# Conmutación orientada a conexión (o Circuito Virtual)

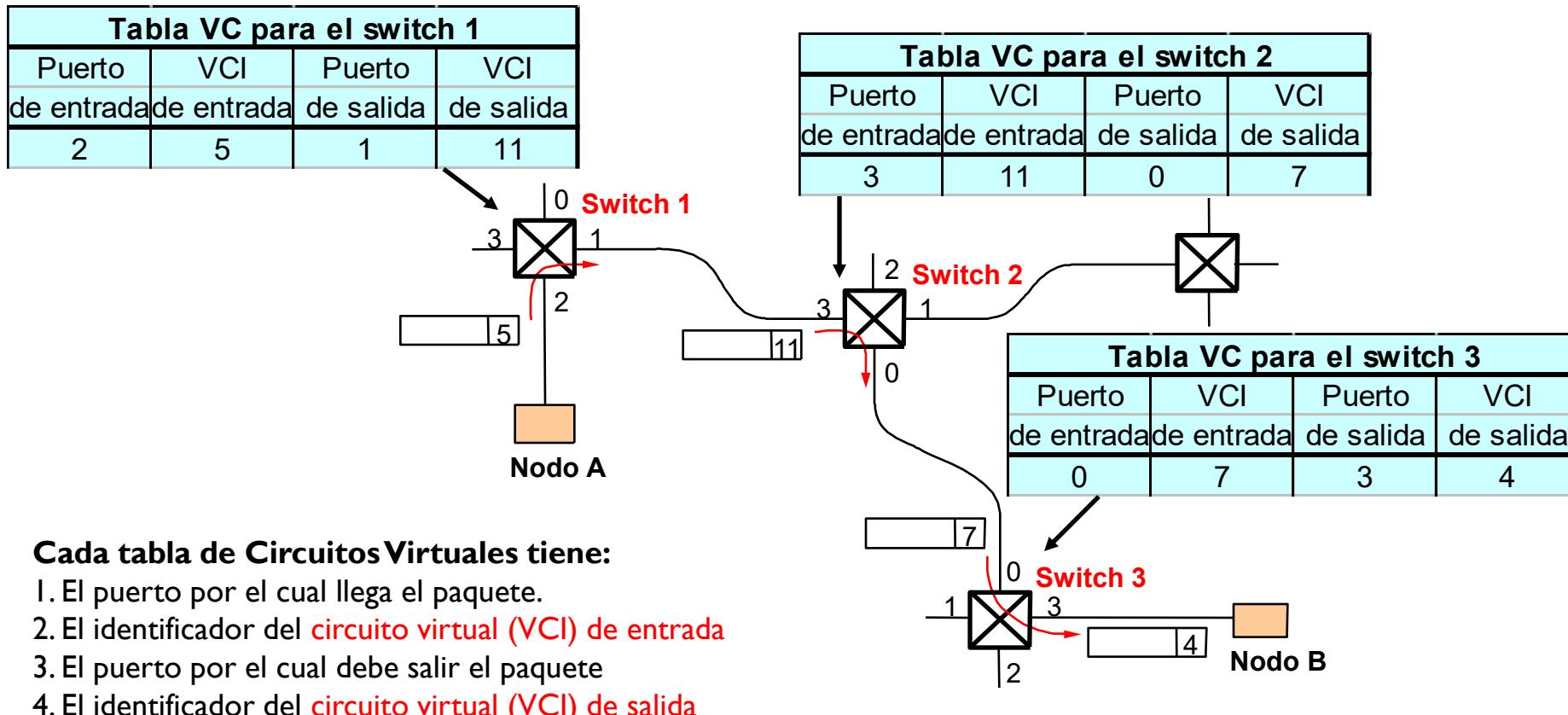
---

- ▶ Se requiere una **fase inicial** para establecer una conexión y **otra de finalización** de la conexión
  - ▶ Durante estas fases no se transporta datos del usuario
- ▶ Los paquetes que se transmiten después de establecer la conexión utilizan **siempre el mismo circuito**

# Comunicación orientada a conexión (o Circuito Virtual)

Analogía: llamada telefónica

Cada switch mantiene una tabla de **VC** (Virtual Circuits)

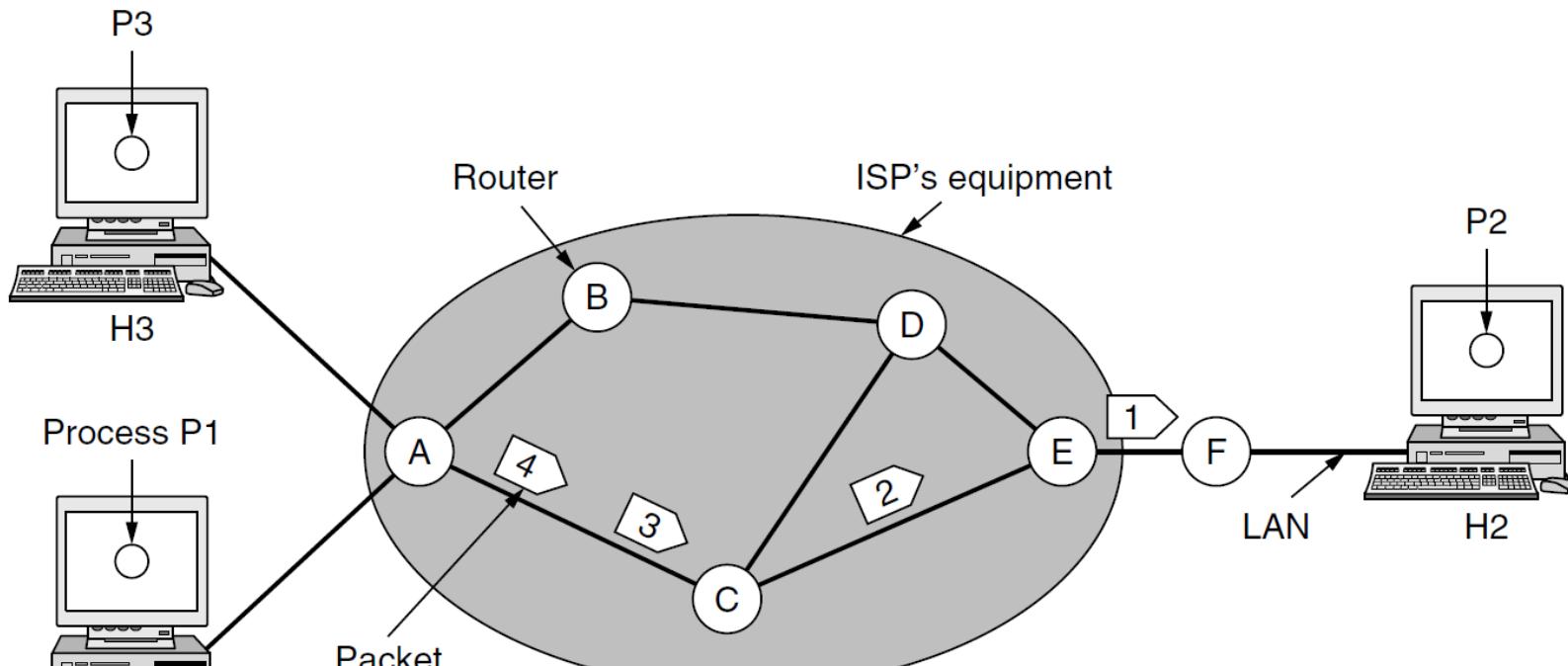


# Tipos de conexiones

---

- ▶ Conexión Permanente (PVC)
  - ▶ Este tipo de conexión la define y la finaliza el administrador de la red.
  - ▶ Una persona solicita a la red la creación de los registros en las tablas VC.
  - ▶ Despues de creado el circuito virtual ya se pueden enviar datos.
- ▶ Conexión por Solicitud (o comutado) (SVC)
  - ▶ Cuando el nodo A desea enviar datos al nodo B envía un mensaje de solicitud de conexión a la red.
  - ▶ Luego el switch que la recibe se lo envía al siguiente, hasta llegar al nodo B. Este último, si acepta la conexión, devolverá el identificador de circuito que desea utilizar (4 en el ejemplo anterior)
  - ▶ Esta “aceptación” se repite en todos los switches que se encuentran en el camino.
  - ▶ Despues de construir el Circuito Virtual se empieza a enviar datos.

# Comunicación orientada a conexión (circuito virtual)



Una forma de  
“label switching”

A's table		C's table		E's table	
H1   1		A   1	E   1	C   1	F   1
H3   1		A   2	E   2	C   2	F   2
In			Out		

# Finalización de la conexión

---

- ▶ Conexión Permanente (**PVC**)
  - ▶ El administrador de la red, una persona, solicita o hace las operaciones que permitan “bajar” el circuito virtual.
- ▶ Conexión por Solicitud (**SVC**)
  - ▶ Cuando el nodo A no desea enviar más datos al nodo B, **termina el circuito virtual** enviando un mensaje de finalización a la red.
  - ▶ El switch que recibe el mensaje **borra la línea de la tabla de VC** correspondiente a ese circuito
    - ▶ envía un mensaje de finalización **al siguiente switch** para que repita la misma acción y así hasta alcanzar al nodo B.
  - ▶ Si después de esto el nodo A envía un paquete a la red, **este puede ser descartado** pues ya no existe el circuito virtual.

# Modelo de circuito virtual

---

- ▶ Normalmente debe esperarse un RTT completo mientras se establece una conexión para poder enviar el primer paquete o celda.
- ▶ La **solicitud de conexión** debe llevar la dirección completa del nodo destino, pero los demás paquetes o celdas sólo tienen un identificador muy pequeño (el VCI)
  - ▶ Esto hace que **el overhead de transmisión sea pequeño**.
- ▶ Si un switch o un enlace falla, el circuito virtual falla y una nueva conexión debe establecerse.
  - ▶ Esto hace que **el overhead de recuperación ante errores sea grande**.
- ▶ Establecer una conexión de antemano permite además **reservar recursos en los switches** (espacio en los buffers).
  - ▶ Tecnologías “viejas” que utilizan hoy circuitos virtuales son: X.25, Frame Relay y ATM.

# Datagrama vs. Circuito Virtual

Asunto	Subred de datagramas	Subred de circuitos virtuales
Configuración del circuito	No necesaria	Requerida
Direccionamiento	Cada paquete contiene la dirección de origen y de destino	Cada paquete contiene un número de CV corto
Información de estado	Los enrutadores no contienen información de estado de las conexiones	Cada CV requiere espacio de tabla del enrutador por conexión
Enrutamiento	Cada paquete se enruta de manera independiente	Ruta escogida cuando se establece el CV; todos los paquetes siguen esta ruta
Efecto de fallas del enrutador	Ninguno, excepto para paquetes perdidos durante una caída	Terminan todos los CVs que pasan a través del enrutador
Calidad del servicio	Difícil	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV
Control de congestión	Difícil	Fácil si pueden asignarse por adelantado suficientes recursos a cada CV

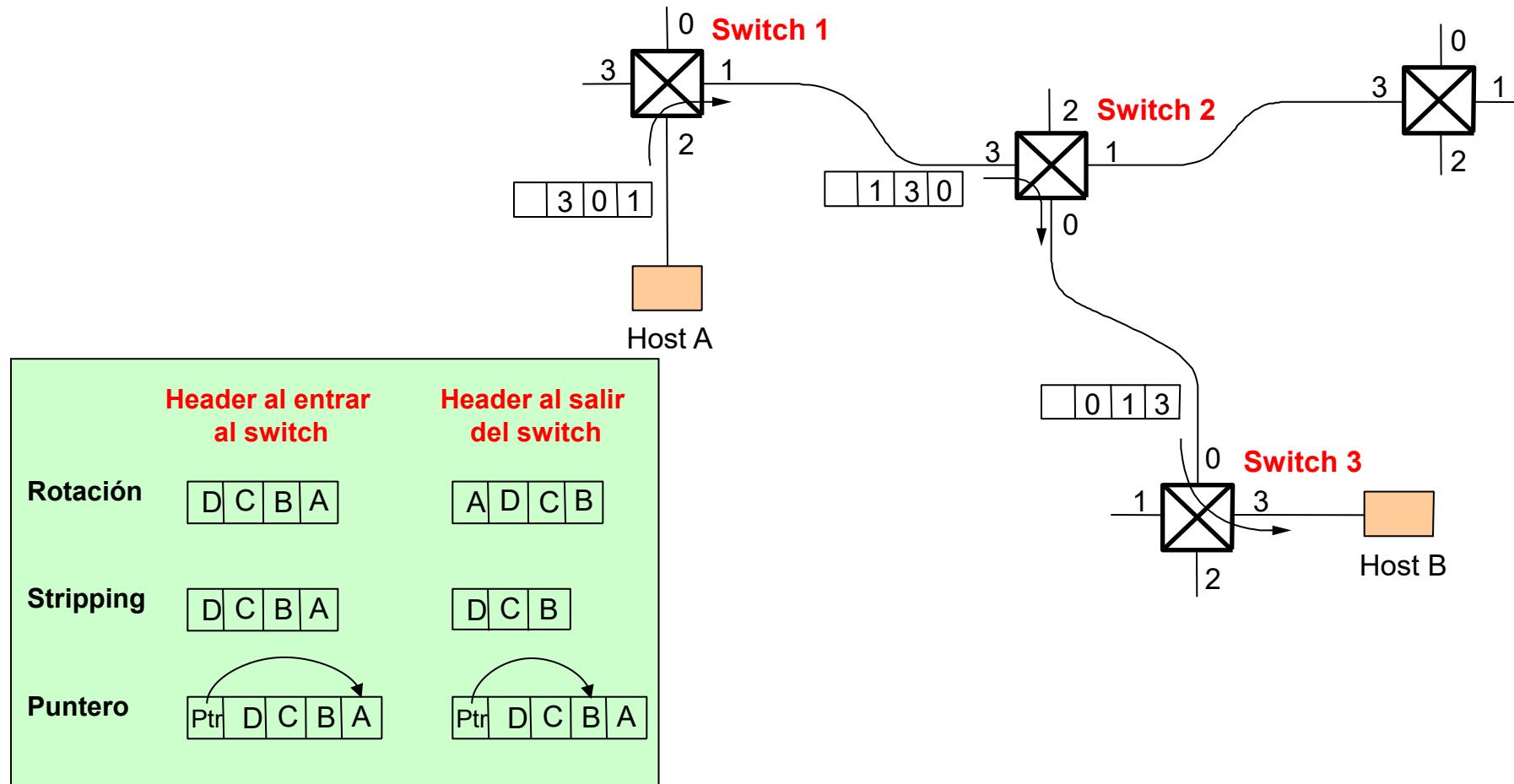
# Comutación *Source Routing*

---

- ▶ Toda la información sobre la topología de la red que se necesita para comutar los paquetes es proporcionada por el nodo origen.
- ▶ Existen varias formas de implementar Source Routing.
  - ▶ Rotación
  - ▶ Stripping
  - ▶ Pointer

# Commutación Source Routing

Ejemplo para Rotación



# Uso de Source Routing

---

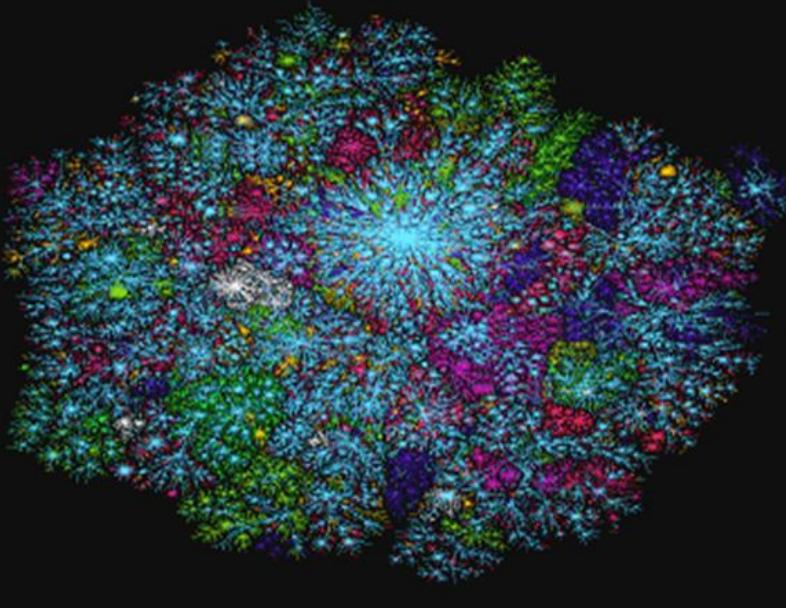
- ▶ La commutación basada en *Source Routing* puede ser utilizada en redes no orientadas a conexión (Datagrama) o en redes orientadas a conexión (Circuito Virtual).
- ▶ Por ejemplo:
  - ▶ IP (Internet Protocol), que es un protocolo no orientado a conexión, incluye una **opción para source routing** que permite que **ciertos paquetes seleccionados** puedan ser enrutados desde el origen.
  - ▶ En redes de Circuitos Virtuales, *source routing* significa **escoger de antemano** un trayecto especificado sobre la red.

# Internetworking

---

**Modelo de Servicio “Best Effort”: IP (Internet Protocol)**

THE WHOLE INTERNET



# Protocolo IP

Claudio E. Righetti

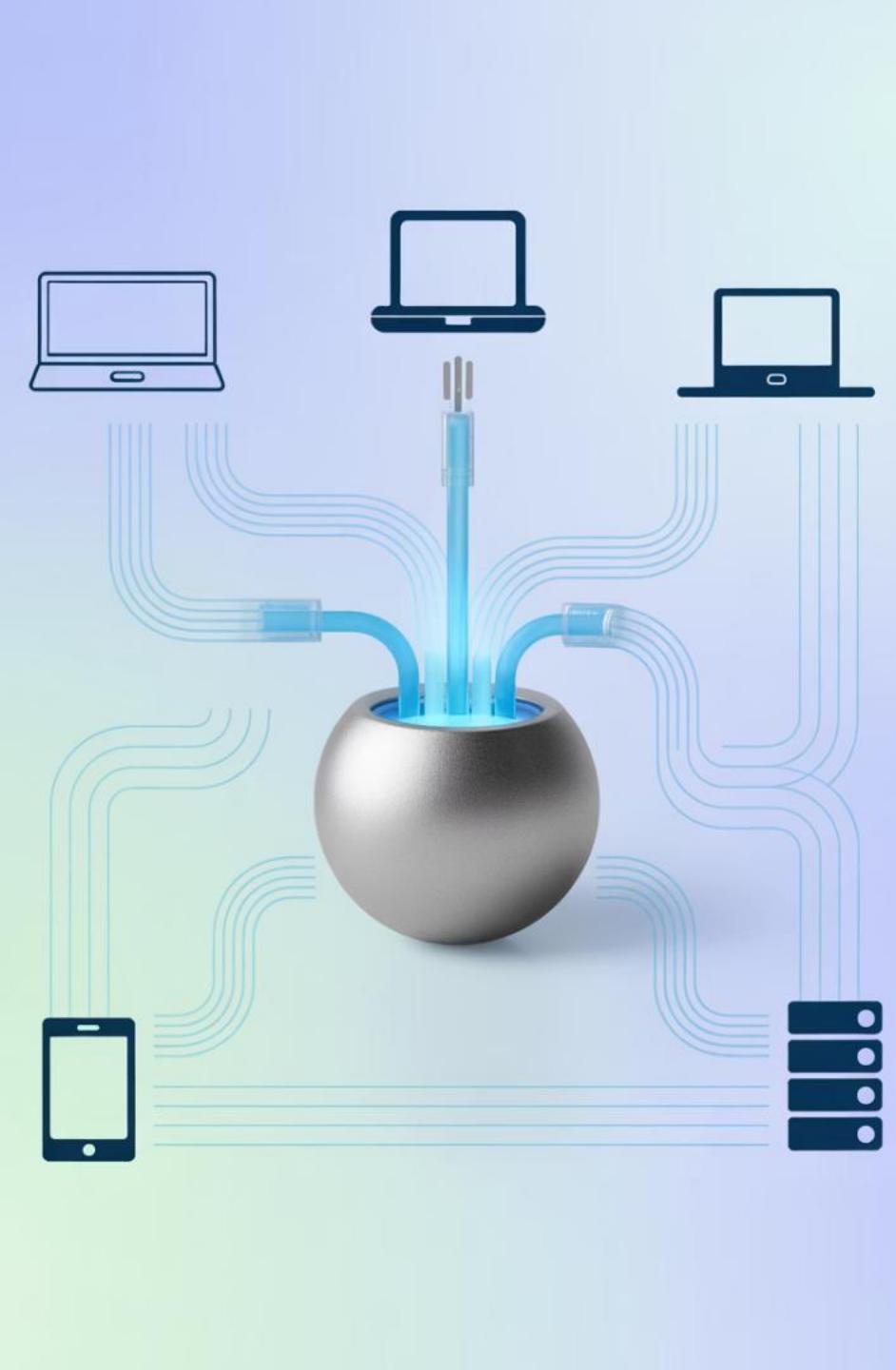
Miércoles 28 mayo 2025

Concurso de Renovación

Departamento de Computación  
Facultad de Ciencias Exactas y Naturales  
Universidad de Buenos Aires

# Introducción al Protocolo IP

## Clave para la Interconexión Global



# Introducción

68%

Conectividad Global

Porcentaje de la población mundial  
conectada a Internet actualmente

1983

Año Clave

Implementación oficial de TCP/IP en  
ARPANET

100 Mil Millones+

Dispositivos

Estimación de dispositivos conectados  
para 2030

El desafío de conectar redes diferentes fue resuelto gracias al Protocolo IP. Esta tecnología fundamental permite la interoperabilidad global.

# Orígenes: Paper de Cerf & Kahn (1974)



1974: Publicación

"A Protocol for Packet Network Intercommunication" establece los fundamentos teóricos.



1978: División TCP/IP

Se separa en dos protocolos para mayor flexibilidad.



1983: Implementación

ARPANET adopta TCP/IP como estándar oficial.

El problema principal era la heterogeneidad de redes incompatibles. La solución: crear capas de abstracción mediante encapsulamiento.



## A Protocol for Packet Network Intercommunication

VINTON G. CERF AND ROBERT E. KAHN,  
MEMBER, IEEE

*Abstract* — A protocol that supports the sharing of resources that exist in different packet switching networks is presented. The protocol provides for variation in individual network packet sizes, transmission failures, sequencing, flow control, end-to-end error checking, and the creation and destruction of logical process-to-process connections. Some implementation issues are considered, and problems such as internetwork routing, accounting, and timeouts are exposed.

### INTRODUCTION

IN THE LAST few years considerable effort has been expended on the design and implementation of packet switching networks [1]-[7],[14],[17]. A principle reason for developing such networks has been to facilitate the sharing of computer resources. A packet communication network includes a transportation mechanism for delivering data between computers or between computers and terminals. To make the data meaningful, computer and terminals share a common protocol (i.e., set of agreed upon conventions). Several protocols have already been developed for this purpose [8]-[12],[16]. However, these protocols have addressed only the problem of communication on the same network. In this paper we present a protocol design and philosophy that supports the sharing of resources that exist in different packet switching networks.

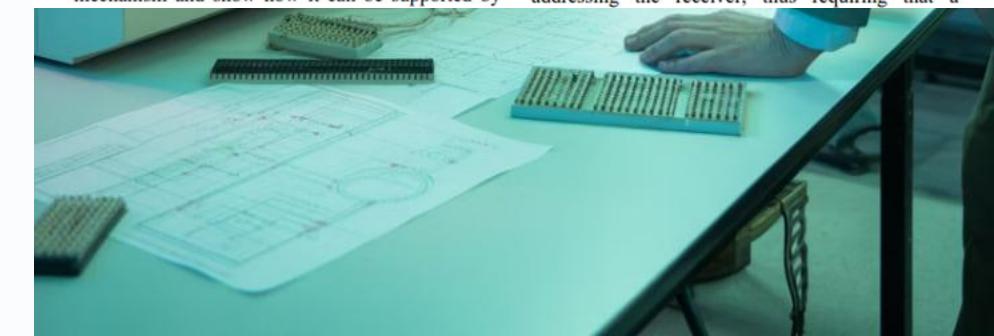
After a brief introduction to internetwork protocol issues, we describe the function of a GATEWAY as an interface between networks and discuss its role in the protocol. We then consider the various details of the protocol, including addressing, formatting, buffering, sequencing, flow control, error control, and so forth. We close with a description of an interprocess communication mechanism and show how it can be supported by

of one or more *packet switches*, and a collection of communication media that interconnect the packet switches. Within each HOST, we assume that there exist *processes* which must communicate with processes in their own or other HOSTS. Any current definition of a process will be adequate for our purposes [13]. These processes are generally the ultimate source and destination of data in the network. Typically, within an individual network, there exists a protocol for communication between any source and destination process. Only the source and destination processes require knowledge of this convention for communication to take place. Processes in two distinct networks would ordinarily use different protocols for this purpose. The ensemble of packet switches and communication media is called the *packet switching subnet*. Fig. 1 illustrates these ideas.

In a typical packet switching subnet, data of a fixed maximum size are accepted from a source HOST, together with a formatted destination address which is used to route the data in a store and forward fashion. The transmit time for this data is usually dependent upon internal network parameters such as communication media data rates, buffering and signalling strategies, routeing, propagation delays, etc. In addition, some mechanism is generally present for error handling and determination of status of the networks components.

Individual packet switching networks may differ in their implementations as follows.

1) Each network may have distinct ways of addressing the receiver, thus requiring that a



# ¿Qué es el Protocolo IP?



IP opera en la capa de red del modelo OSI. Fragmenta y encapsula datos en unidades llamadas datagramas IP.

# Independencia de la tecnología subyacente



## Ethernet

Redes cableadas tradicionales con velocidades de hasta 400 Gbps



## Wi-Fi

Redes inalámbricas que operan en bandas de 2.4 GHz y 5 GHz



## Fibra óptica

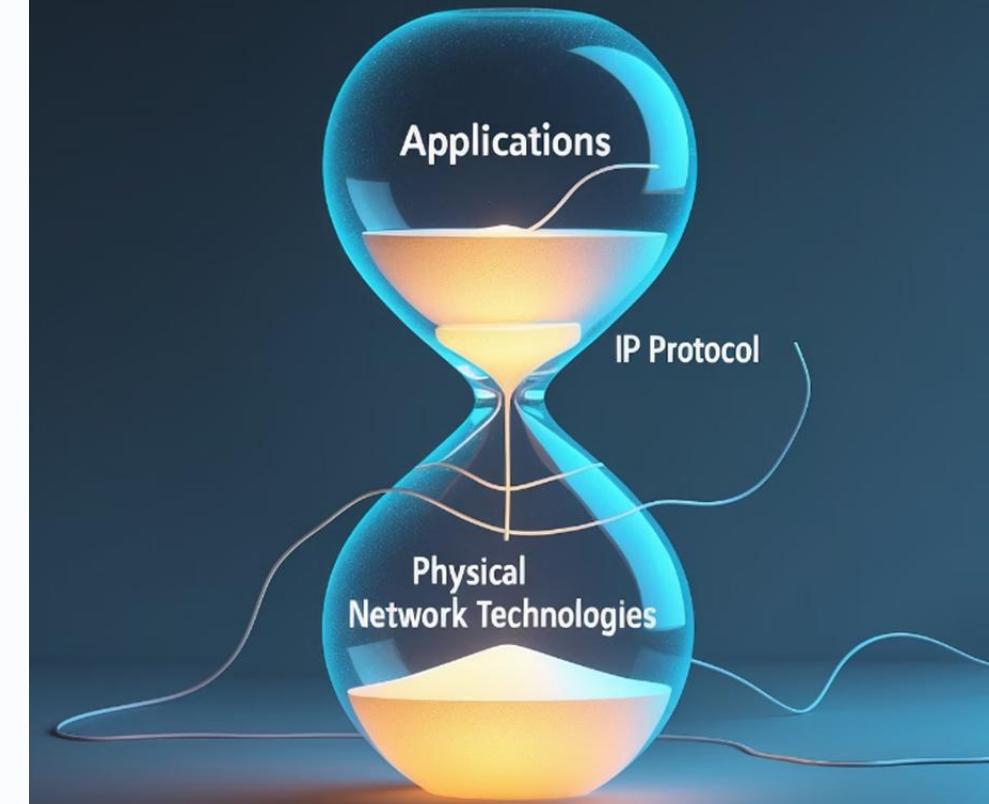
Transmisión mediante pulsos de luz a velocidades terabit



## 5G

Redes celulares de alta velocidad con baja latencia

IP actúa como capa intermedia que abstrae las diferencias. Esta independencia es fundamental para la versatilidad de Internet.





# Visión y Principio Clave



## Diseño de un único protocolo de red

Se diseña un único protocolo de red – **IP** – como punto de convergencia.



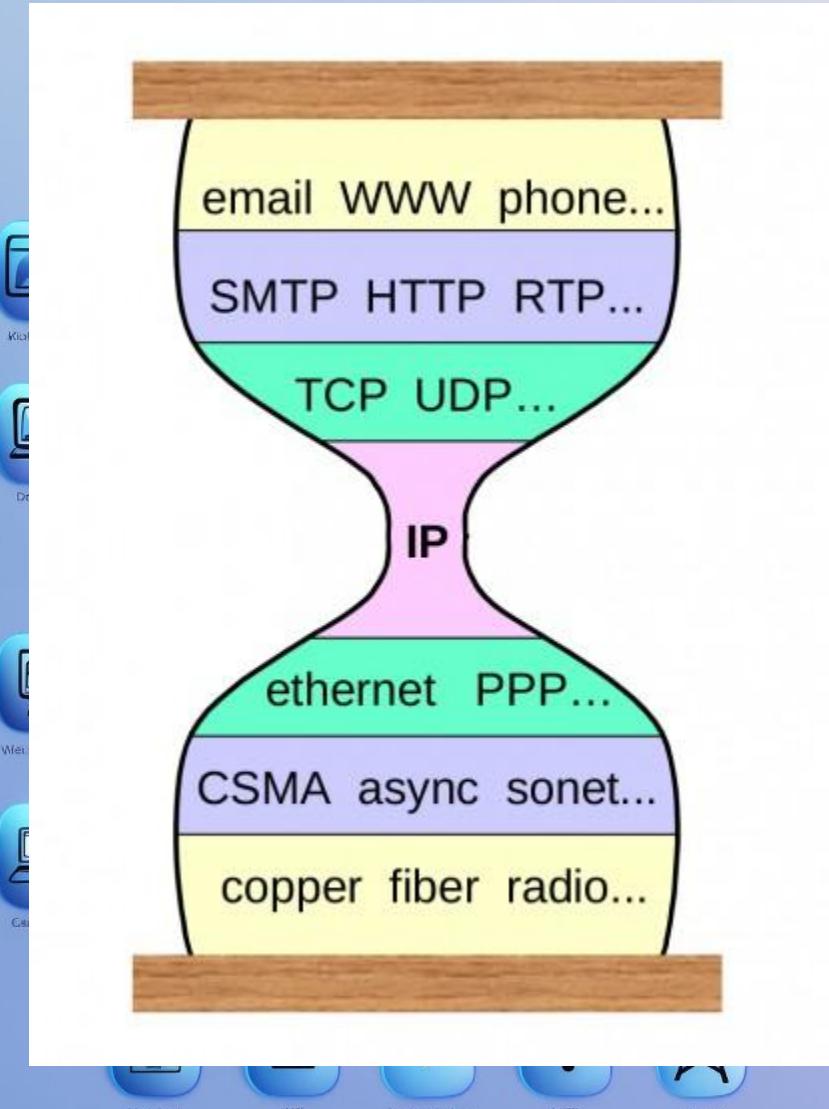
## Compatibilidad universal

Esto permite que cualquier aplicación funcione sobre cualquier tipo de red física, siempre que ambas hablen IP.



## Capa de abstracción universal

Es decir, **IP actúa como capa de abstracción universal**, que es lo suficientemente simple como para ser implementada sobre diversas tecnologías físicas y lo suficientemente poderosa para soportar una enorme variedad de aplicaciones.





# Funcionamiento de IP: Cómo viajan los paquetes



## Fragmentación

Los datos se dividen en paquetes manejables



## Etiquetado

Cada paquete recibe cabecera con direcciones origen y destino



## Enrutamiento

Los routers determinan el mejor camino disponible

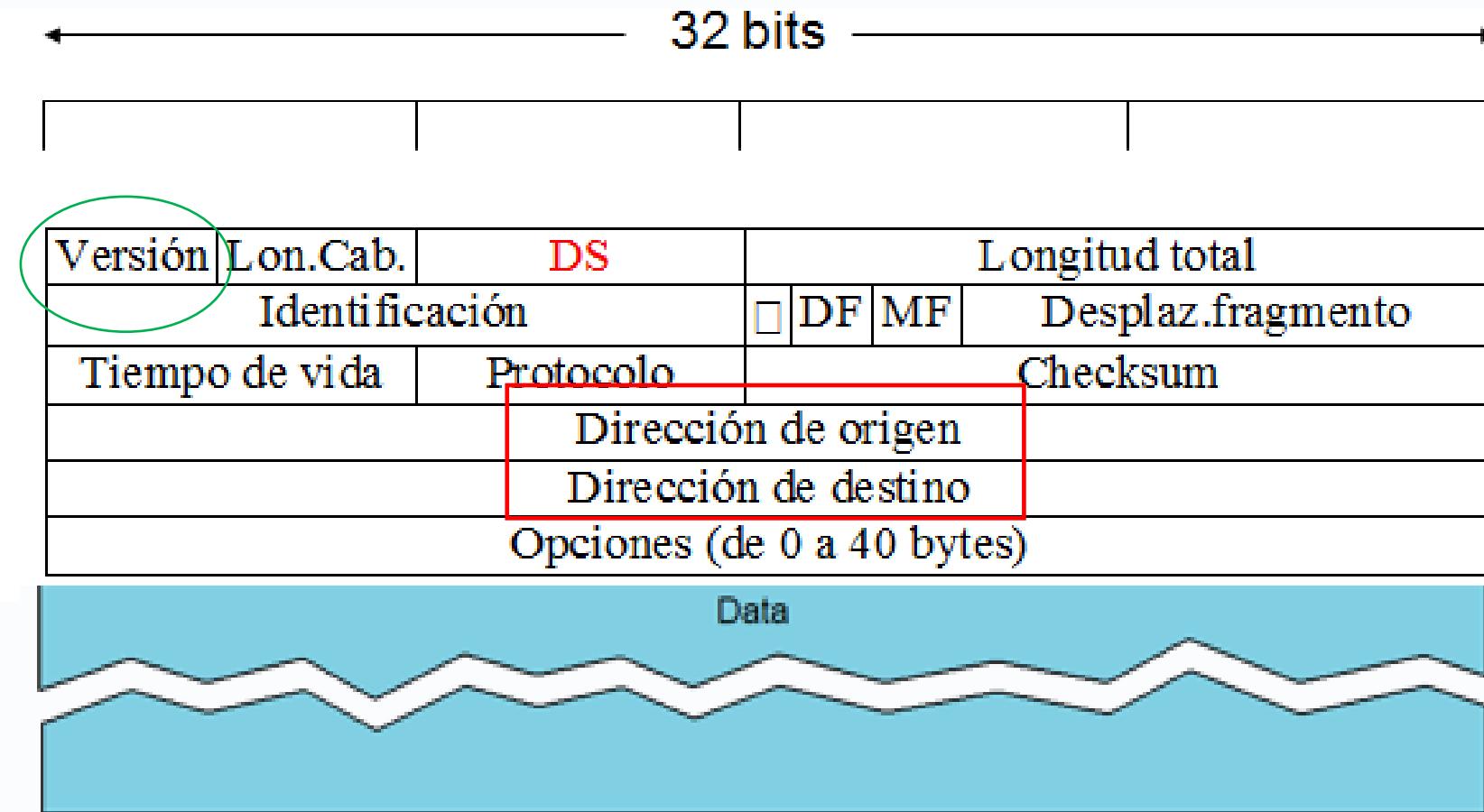


## Llegada

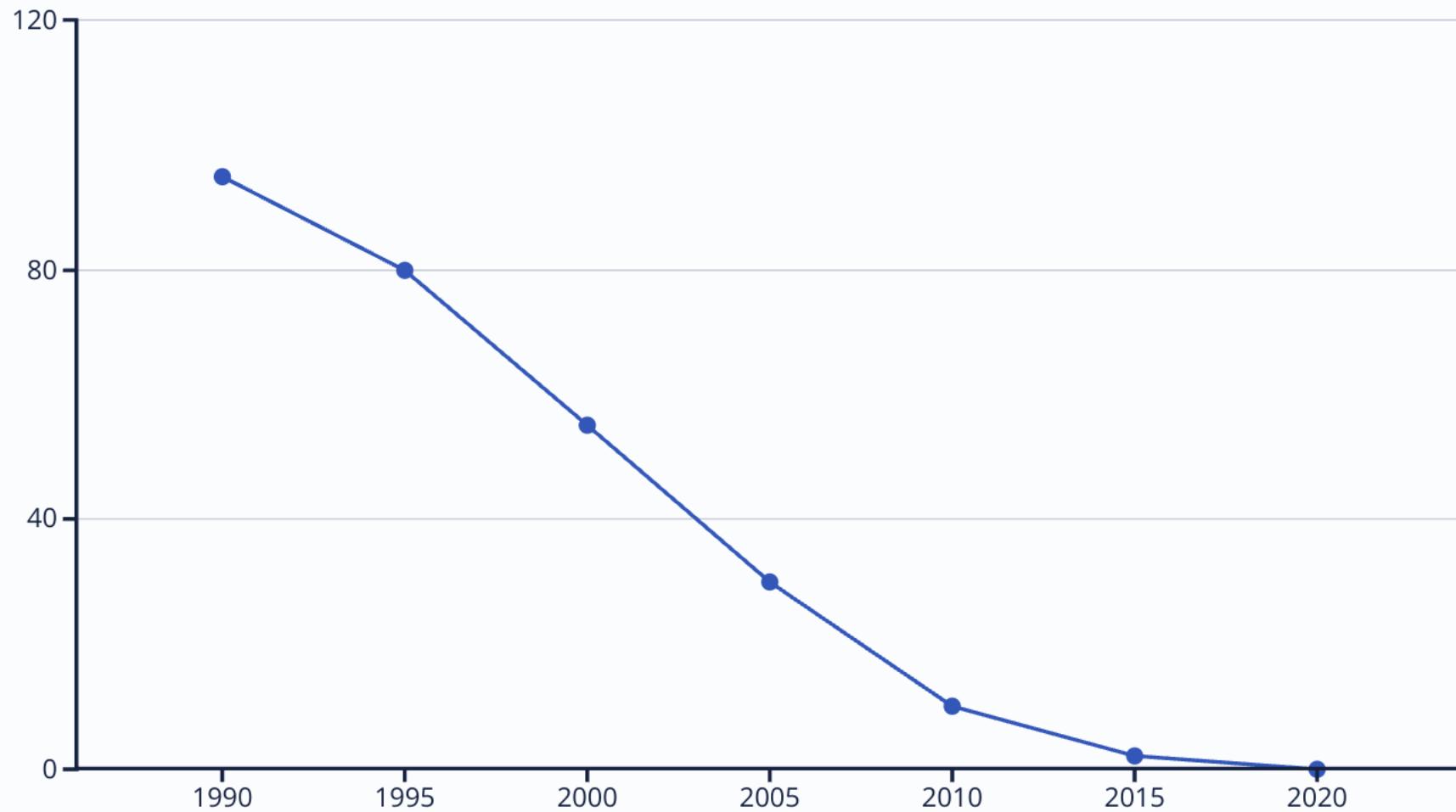
El destino reensambla los paquetes si es necesario

Cada paquete es independiente. Pueden tomar rutas distintas según la congestión de la red. IP no garantiza entrega ni orden.

# Cabecera IP ( Versión 4)

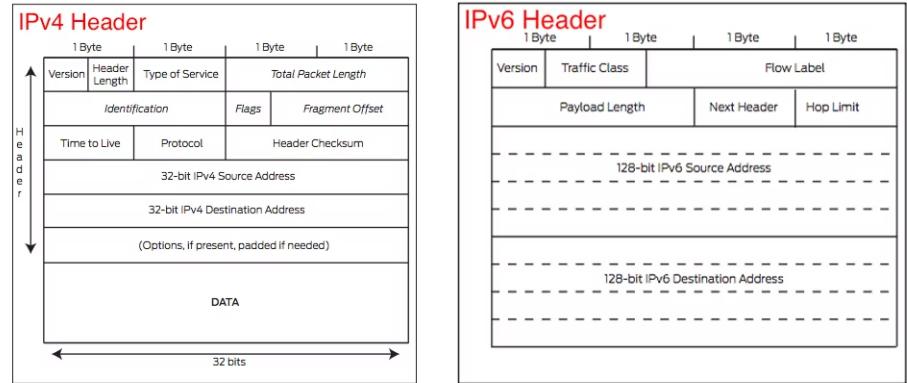


## Desafío: Agotamiento de IPv4



IPv4 usa direcciones de 32 bits. Esto limita el espacio a 4.294 millones de direcciones. IANA agotó sus reservas en 2011.

# La solución: IPv6



## Capacidad masiva

128 bits de direccionamiento: 340 sextillones de direcciones. Equivale a  $4.3 \times 10^{20}$  direcciones por cada milímetro cuadrado de la Tierra.

## Formato mejorado

Cabecera simplificada. Eliminación de checksums. Formato más eficiente para el procesamiento por routers.

## Seguridad integrada

IPsec incorporado desde el diseño. Mejor soporte para autenticación y cifrado de extremo a extremo.

## Autoconfiguración

Los dispositivos pueden generar direcciones automáticamente. Facilita la implementación de redes y dispositivos IoT.

IPv4 e IPv6 coexisten actualmente mediante mecanismos de transición como túneles y traducción.

$$2^{128} \approx 3.4 \times 10^{38}$$

# Conclusiones



## Fundamento de Internet

IP permitió la interconexión global



## Abstracción clave

Independiza comunicaciones de infraestructura



## Escalabilidad

Su diseño simple ( best-effort ) permitió crecimiento exponencial



## Futuro asegurado

IPv6 garantiza expansión continua

El protocolo IP demuestra cómo principios de diseño simples pero potentes pueden transformar el mundo. Su impacto en la sociedad es incalculable.



# 🎯 Ventajas del Modelo de Reloj de Arena



## Flexibilidad

Permite que nuevas tecnologías físicas (Wi-Fi, LTE, fibra, etc.) se integren fácilmente a Internet sin cambiar las capas superiores.



## Escalabilidad

Nuevas aplicaciones pueden surgir (Zoom, WhatsApp, Netflix) sin requerir cambios en la infraestructura subyacente.



## Interoperabilidad global

Cualquier dispositivo puede comunicarse con otro en cualquier parte del mundo si ambos entienden IP.



## Simplicidad y estabilidad

La capa IP es minimalista y estable, lo que asegura compatibilidad a lo largo del tiempo.

# Bibliografía y Referencias

- Peterson, L. L., & Davie, B. S. (2021). Computer Networks: A Systems Approach (6<sup>a</sup> ed.). Morgan Kaufmann
- ITU Launches Facts & Figures 2024 on global connectivity, digital inclusion and 5G coverage <https://www.uar-aub.org/single-post/itu-launches-facts-figures-2024-on-global-connectivity-digital-inclusion-and-5g-coverage>
- Cerf & Kahn Publish TCP: A Protocol for Packet Network Communication : History of Information <https://www.historyofinformation.com/detail.php?id=915>
- Peterson, Larry; Davie, Bruce (2025-04-26). What We Talk About When We Talk About Systems: Essays on the Systems Approach (English Edition) . Systems Approach LLC. Edición de Kindle.
- RFC 791 Internet Protocol ( 1981) <https://www.rfc-editor.org/rfc/rfc791.html>
- IPv4 Exhaustion FAQs | The Number Resource Organization <https://www.nro.net/about/rirs/internet-number-resources/ipv6/ipv4-exhaustion-faqs/>
- Agotamiento de direcciones IPv4 a nivel central - NIC Chile <https://www.nic.cl/anuncios/20110203-ipv4.html>

Gracias por su tiempo !

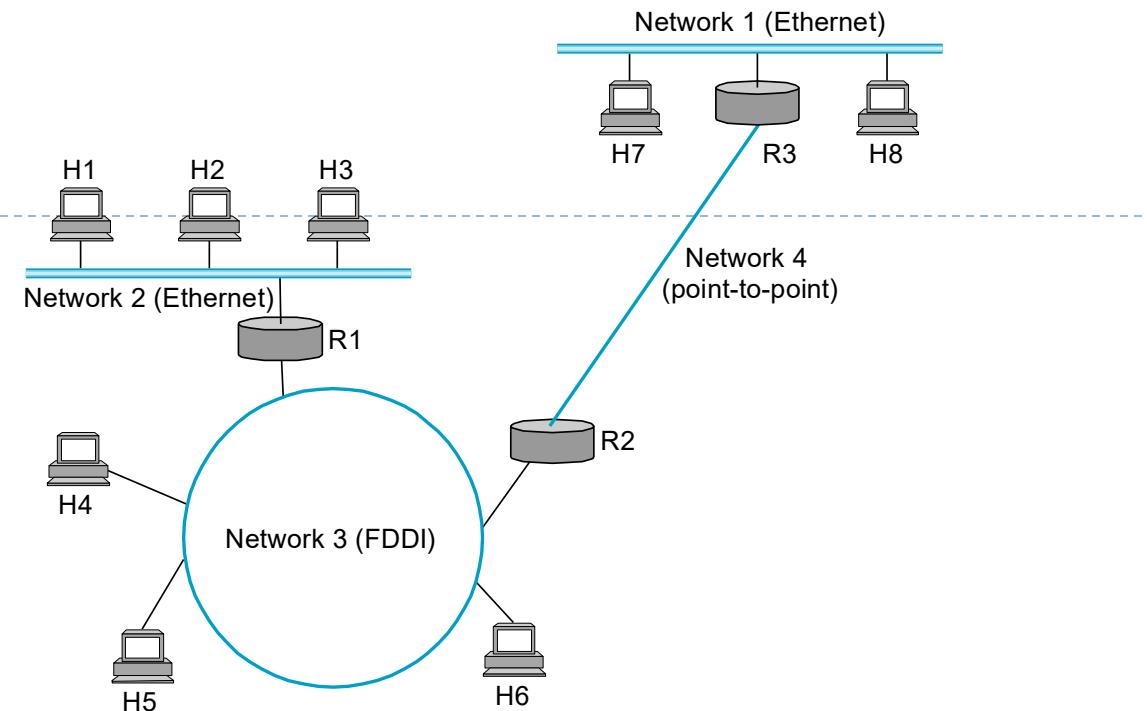
# Agenda

---

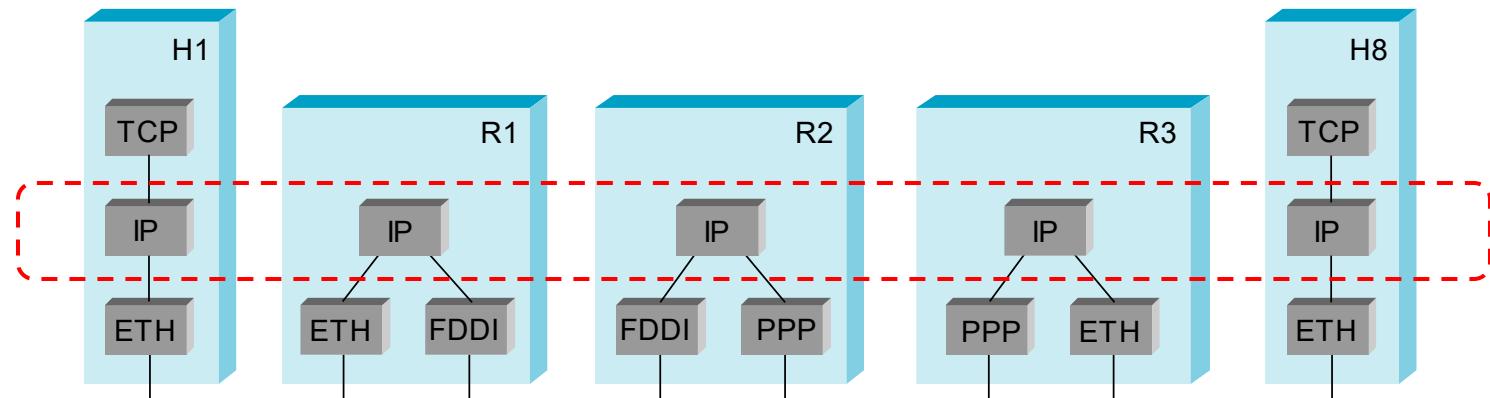
- ▶ Modelo de Servicio “Best Effort”
- ▶ Cabecera IP
- ▶ Fragmentación
- ▶ Direcccionamiento Global
- ▶ Forwarding

# IP en Internet

- ▶ Interconexión de Redes

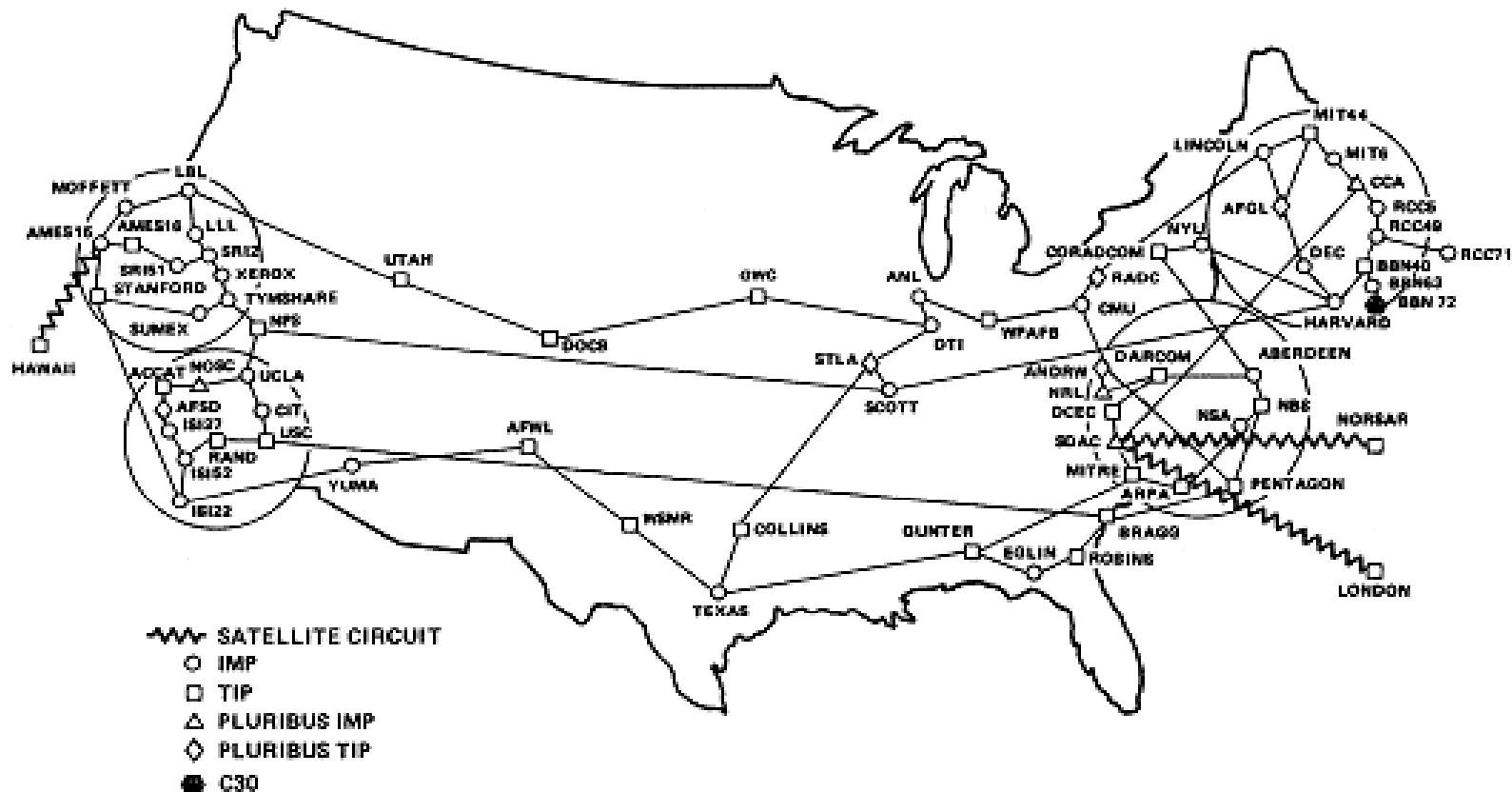


- ▶ Protocol Stack



# IP en Internet

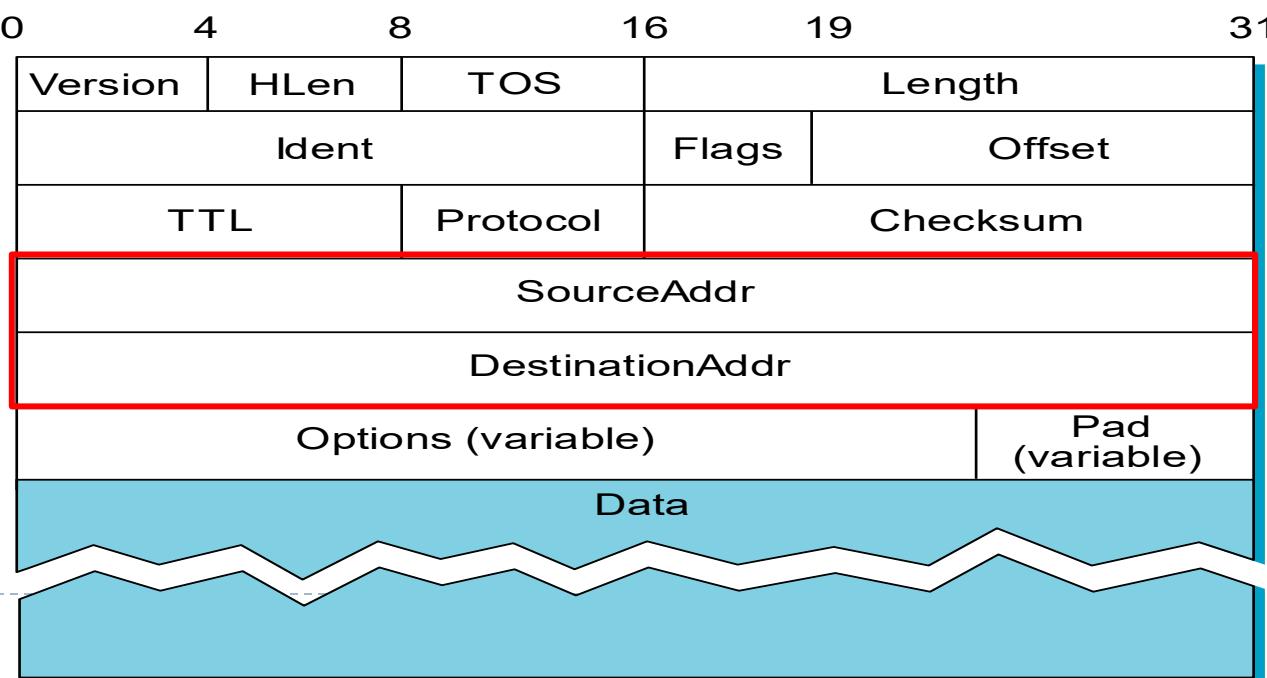
ARPANET GEOGRAPHIC MAP, OCTOBER 1980



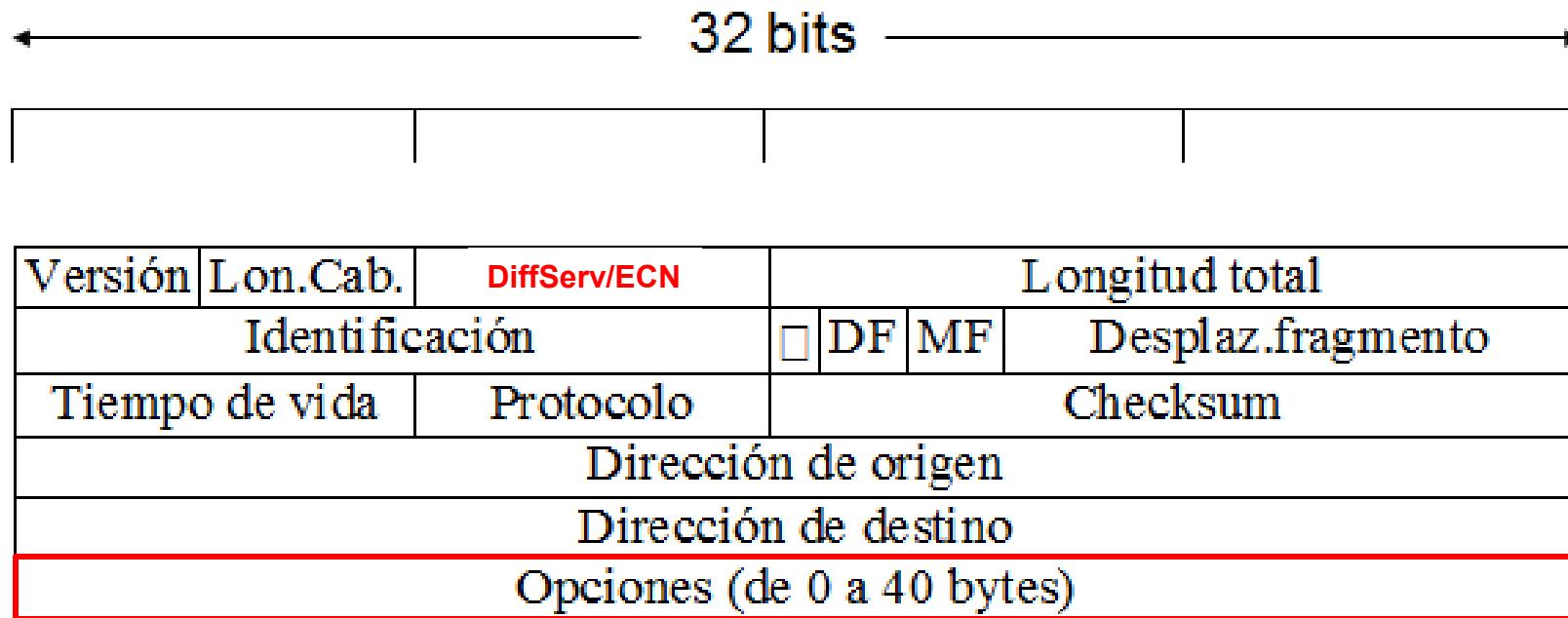
# Modelo de Servicio

- ▶ Connectionless (datagram-based)
- ▶ Best-effort (unreliable service). Los paquetes pueden:
  - ▶ Perderse
  - ▶ Llegar fuera de orden
  - ▶ Tener duplicados entregados
  - ▶ No tener una cota para el tiempo de entrega

- ▶ Formato



# Cabecera IP (versión 4)



- La cabecera de un datagrama IP contiene información que deben interpretar los routers.
- El tamaño de la cabecera es normalmente de **20 bytes**, pudiendo llegar hasta 60 si se utilizan todos los **campos opcionales**.

# Campos del header IP

---

- ▶ **Versión:** actualmente v4, comienzan los v6 pero el resto del formato del header no es el mismo en ambas versiones.
- ▶ **Longitud Cabecera:** en palabras de 32 bits (mínimo 5, máximo 15)
- ▶ **Longitud total:** en bytes, máximo de 65535 (incluye la cabecera)
- ▶ **Fragmentación:** Identificación, DF, MF, Desplazamiento.
- ▶ **Tiempo de vida:** contador de saltos hacia atrás (se descarta cuando es cero)
- ▶ **Checksum:** de toda la cabecera (no incluye los datos)
- ▶ **Dirección fuente y destino:** 32 bits
- ▶ **DiffServ/ECN:** Calidad de Servicio/Control Explícito de Congestión

# Algunos Valores de campo Protocol

Valor	Protocolo	Descripción
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management Protocol
3	GGP	Gateway-to-Gateway Protocol
4	IP	IP en IP (encapsulado)
5	ST	Stream
6	TCP	Transmission Control Protocol
8	EGP	Exterior Gateway Protocol
17	UDP	User Datagram Protocol
29	ISO-TP4	ISO Transport Protocol Clase 4
80	CLNP	Connectionless Network Protocol
88	IGRP	Internet Gateway Routing Protocol
89	OSPF	Open Shortest Path First

# Fragmentación y Reensamblado en IP

---

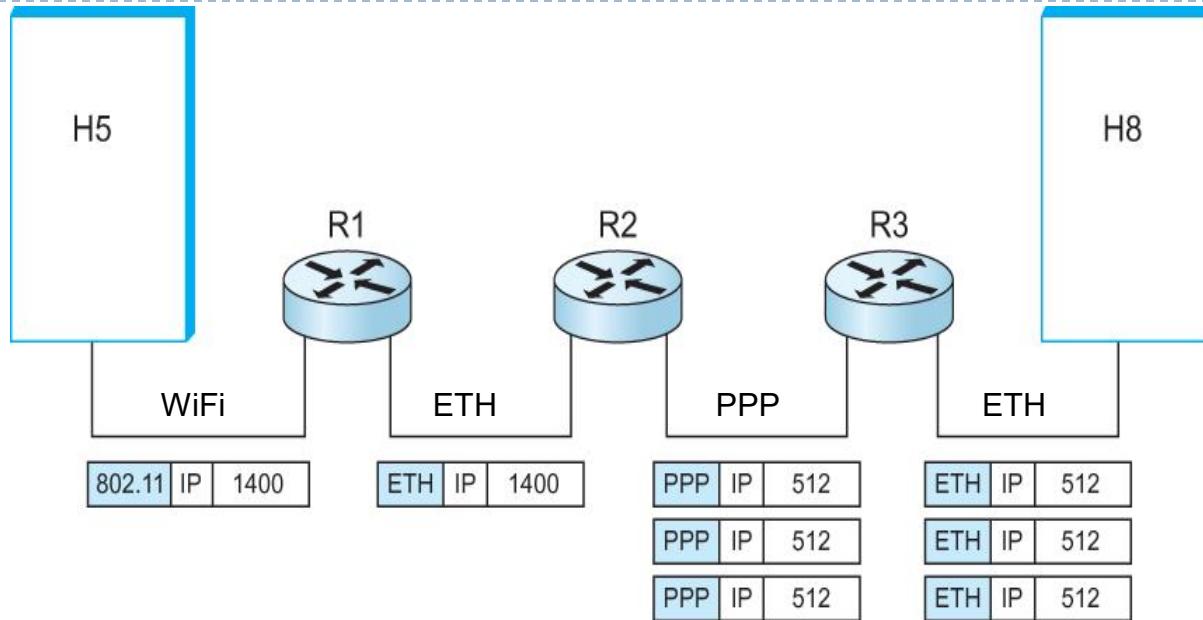
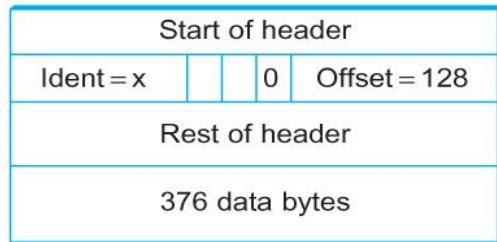
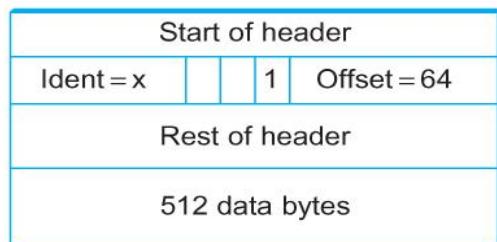
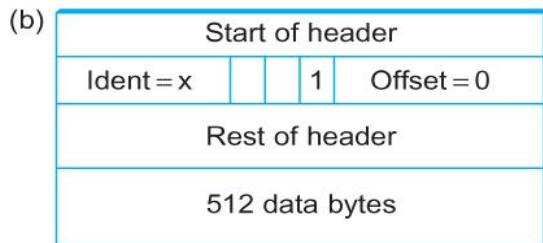
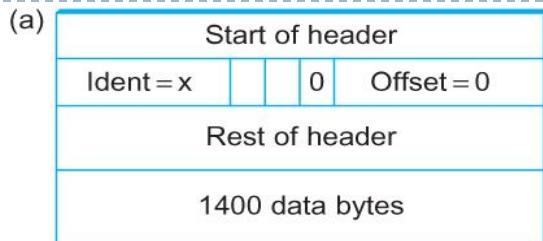
- ▶ Cada tecnología de red tiene, **en su nivel de enlace**, un MTU (Maximum Transmission Unit):
  - ▶ Ejemplos: Ethernet (1500 bytes), FDDI (4500 bytes)
- ▶ Estrategia:  
IP se “adapta” a la **tecnología de enlace subyacente**
  - ▶ **Fragmentación:** ocurre si **un router** recibe un datagrama que debe reenviar a una red donde  
 $MTU < \text{Tamaño\_datagrama}$
  - ▶ **Reensamblado:** se realiza en el **host destino**
    - ▶ Todos los **Fragmentos** tienen un **mismo identificador**
  - ▶ **Fragmentos:** son datagramas autocontenidos
    - ▶ IP no recupera fragmentos perdidos

# Fragmentación en IP

---

- ▶ Los **fragmentos** heredan la misma cabecera que el datagrama original
  - ▶ Excepto por los campos especiales: 'More Fragments' y 'Desplazamiento del Fragmento'.
- ▶ Los fragmentos de un mismo datagrama se identifican por el campo 'Identificación'.
- ▶ Todos los fragmentos, menos el último, tienen en I el bit MF (More Fragments).
- ▶ La unidad básica de fragmentación es 8 Bytes.
  - ▶ Los datos se reparten en tantos fragmentos como haga falta, todos múltiplos de 8 Bytes (salvo quizá el último).
- ▶ Toda red debe aceptar un MTU de al menos 68 Bytes
  - ▶ (60 de cabecera y 8 de datos).

# Fragmentación

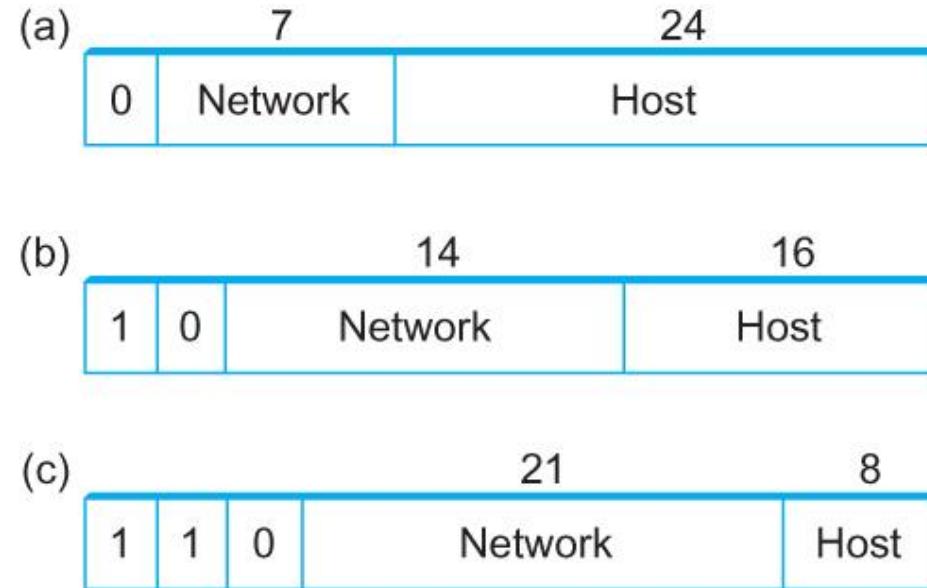


(a) Paquete sin Fragmentar

(b) Paquete fragmentado

# Direccionamiento Global

- ▶ Propiedades
  - ▶ Dirección **globalmente única**
  - ▶ **Jerárquica: red + host**
  - ▶ **32 bits:** ~4300 millones de IP addresses
  - ▶ Esquema “Classfull” (original): clases A, B y C
  - ▶ Problemas de escalabilidad



Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Start address	End address
A	0	8	24	128 ( $2^7$ )	16,777,216 ( $2^{24}$ )	0.0.0.0	127.255.255.255
B	10	16	16	16,384 ( $2^{14}$ )	65,536 ( $2^{16}$ )	128.0.0.0	191.255.255.255
C	110	24	8	2,097,152 ( $2^{21}$ )	256 ( $2^8$ )	192.0.0.0	223.255.255.255

Notación “Dot”: 10.3.2.4, 128.96.33.81, 192.12.69.77.

UBA: 157.92/16 (“máscara de red” de 16 bits, equiv. Clase B)

# Direccionamiento Privado

Rekhter, et al

Best Current Practice

[Page 3]

RFC 1918

Address Allocation for Private Internets February 1996

### 3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	-	10.255.255.255 (10/8 prefix)
172.16.0.0	-	172.31.255.255 (172.16/12 prefix)
192.168.0.0	-	192.168.255.255 (192.168/16 prefix)

We will refer to the first block as "24-bit block", the second as "20-bit block", and to the third as "16-bit" block. Note that (in pre-CIDR notation) the first block is nothing but a single class A network number, while the second block is a set of 16 contiguous class B network numbers, and third block is a set of 256 contiguous class C network numbers.

An enterprise that decides to use IP addresses out of the address space defined in this document can do so without any coordination with IANA or an Internet registry. The address space can thus be used by many enterprises. Addresses within this private address space will only be unique within the enterprise, or the set of enterprises which choose to cooperate over this space so they may communicate with each other in their own private internet.

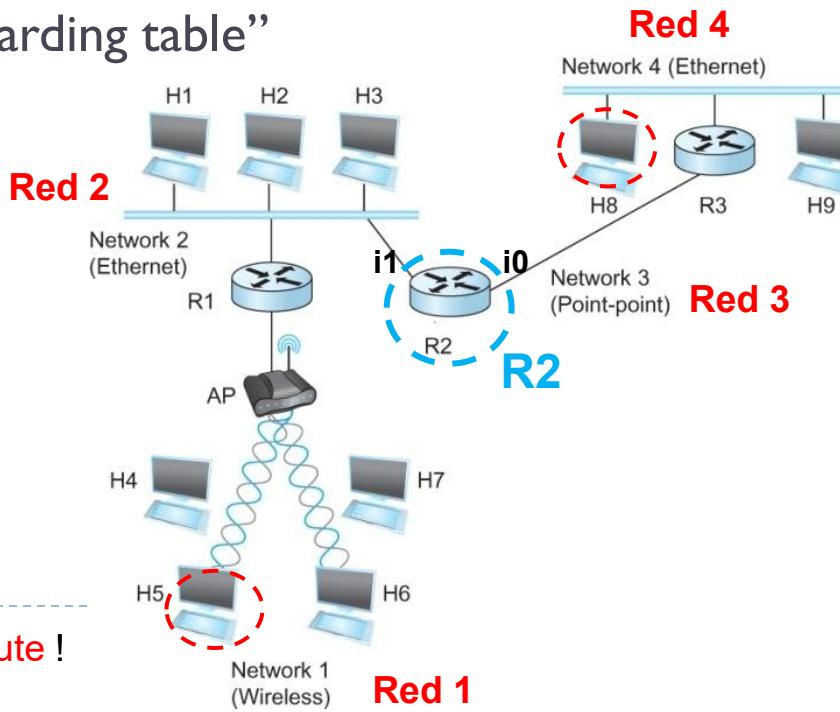
# IP Forwarding

- ▶ Estrategia
  - ▶ Cada datagrama tiene la **dirección destino**
  - ▶ Si **está** directamente conectado a la red destino => forward al host
  - ▶ Si **NO está** directamente conectado a la red destino => forward a otro router
  - ▶ **Forwarding table:** conecta un número de red al “next hop”
  - ▶ **Cada host** tiene un “default router”
  - ▶ **Cada router** mantiene una “forwarding table”
- ▶ **Forwarding Table** para **R2**

NetworkNum	NextHop
1	R1
2	Interface 1
3	Interface 0
4	R3

Elementos: **Red, Router e Interfaz:**

Nota: Esta tabla ya combinó **Forward** con **Route** !



# IP Forwarding

---

- ▶ Algoritmo

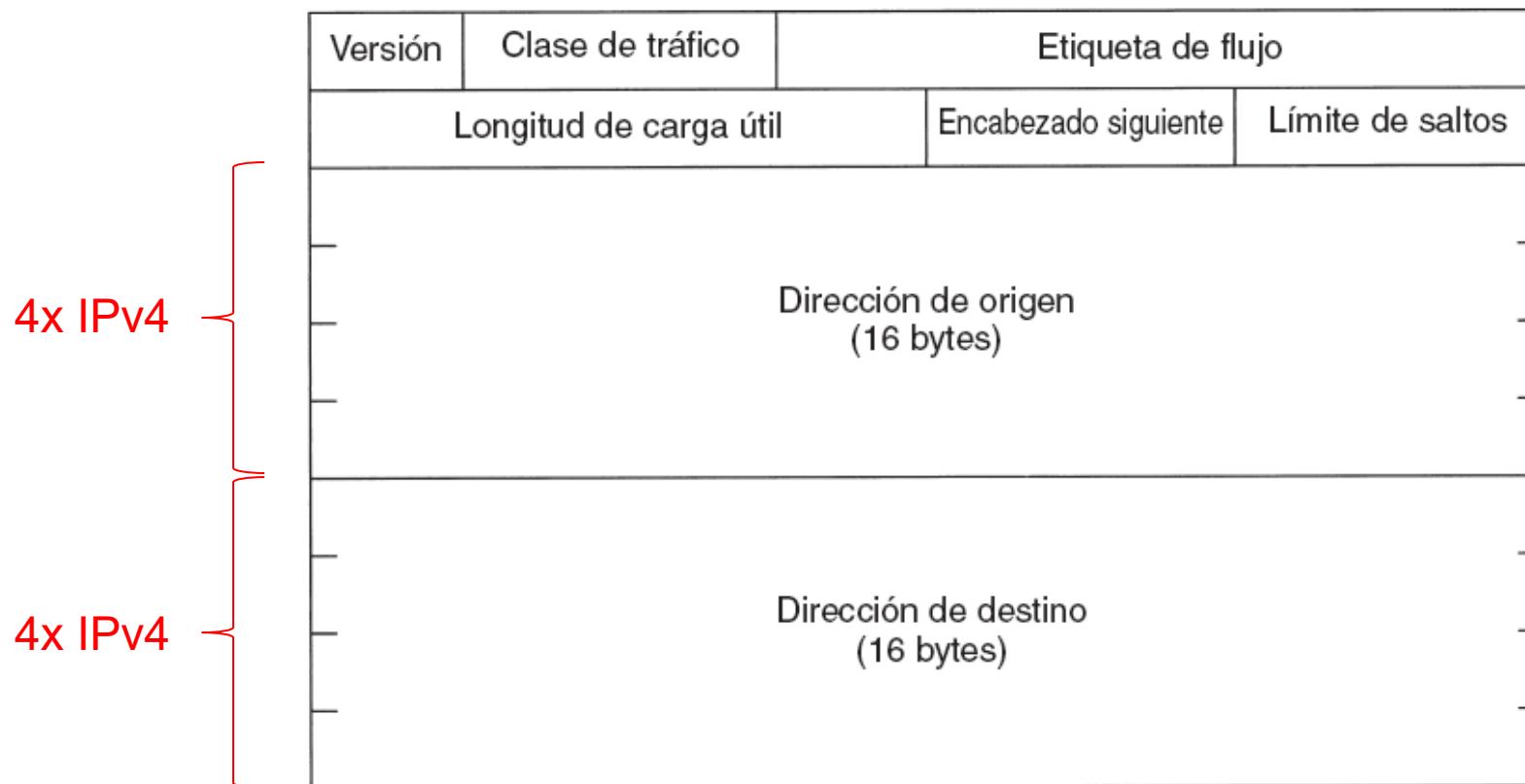
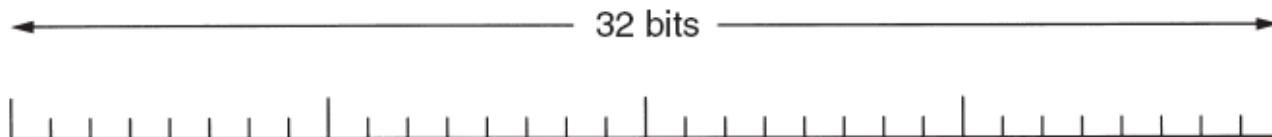
```
if (NetworkNum del Destino = NetworkNum de alguna de mis interfaces) then
    enviar datagrama al Destino por esa interface
else
    if (NetworkNum del Destino está en mi forwarding table) then
        enviar datagrama al NextHop router
    else
        enviar datagrama al Default router
```

¿En que caso el algoritmo de forwarding se reduce a lo siguiente?

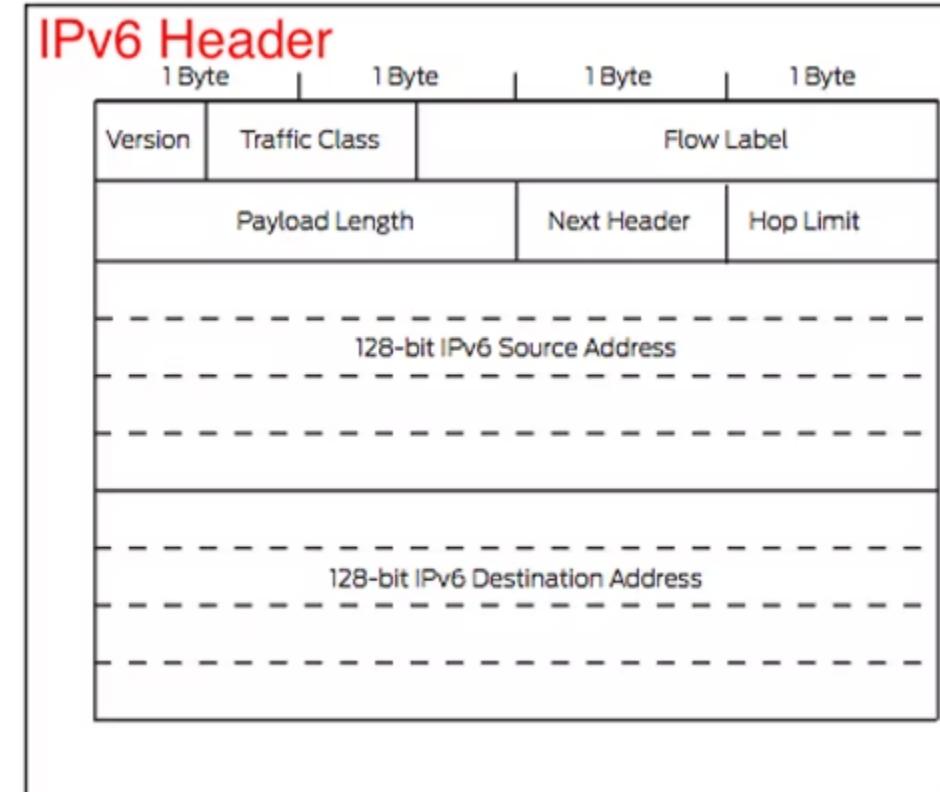
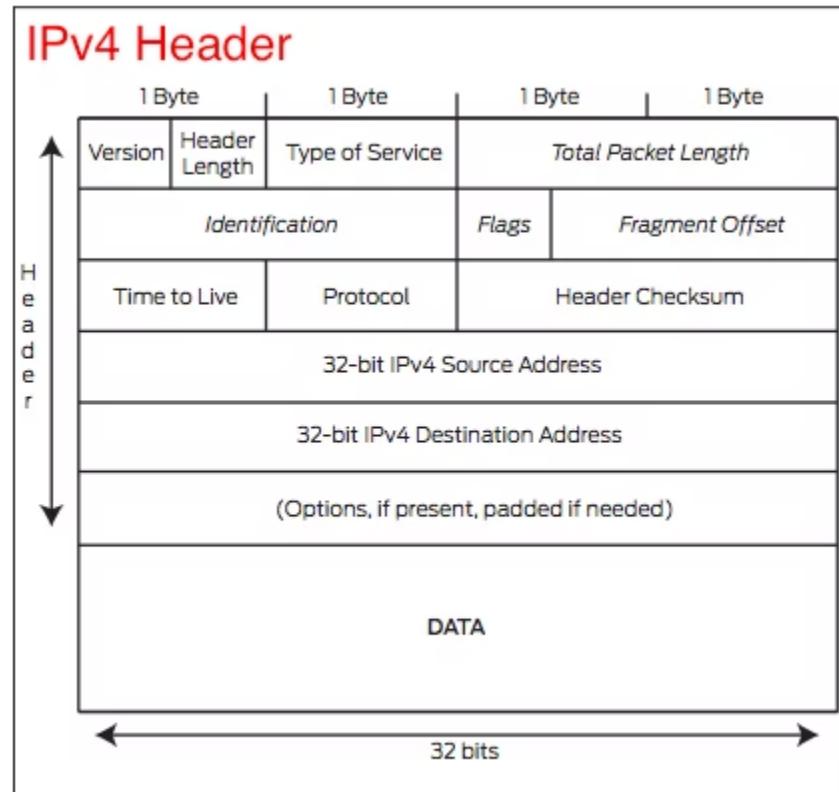
```
if (NetworkNum del Destino = mi NetworkNum) then
    enviar datagrama al Destino directamente
else
    enviar el datagrama al Default router
```

# IPv6

8000:0000:0000:0000:0123:4567:89AB:CDEF



# Header de IPv4 vs IPv6



# Tasa de adopción

