



UNCUYO
UNIVERSIDAD
NACIONAL DE CUYO



**FACULTAD
DE INGENIERÍA**

**Licenciatura en Ciencias de la
Computación**

Redes de Computadoras

Unidad 3

Capa de red



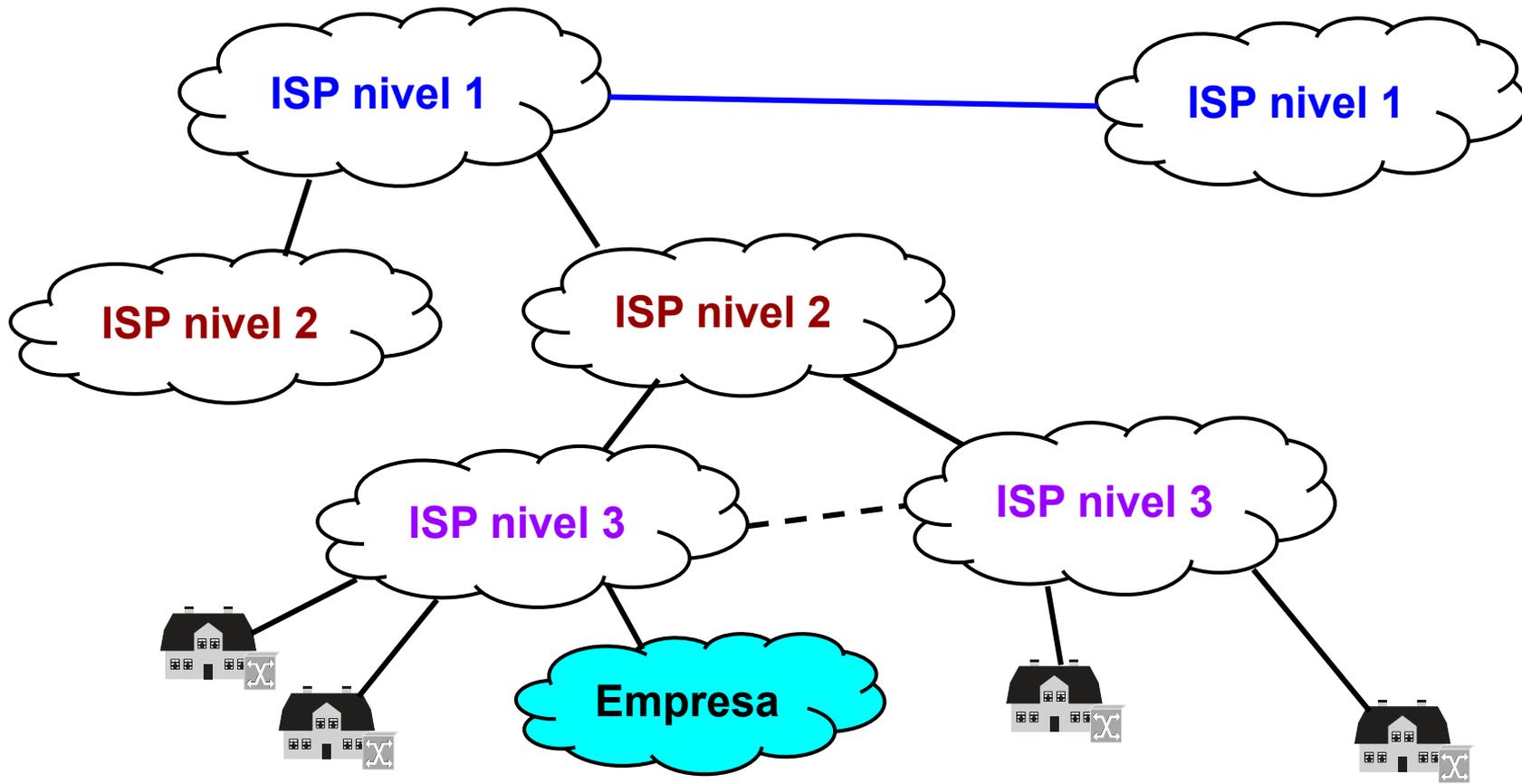
Temario

- ● **Introducción.**
 - **Repaso**
 - **Servicios proporcionados por la capa de red.**
 - **Tipos de servicios.**
 - **Interconexión de redes. Dificultades. Mecanismos**
 - **Descubrimiento del MTU de la ruta y fragmentación de paquetes.**
- **Congestión y calidad de servicio.**
- **IPv4**
- **IPv6**
- **Protocolos de control de Internet (ICMP)**
- **Conmutación basada en etiquetas (MPLS)**
- **Algoritmos de enrutamiento**

Capa de red

- **Llevar (Enrutar)** paquetes desde el origen al destino, pudiendo estar los mismos en **diferentes redes** de **diferentes tecnologías**, y pudiendo pasar por **muchas redes intermedias** de diferentes tecnologías.
- Nuevo componente: **enrutador**
- Requisitos de diseño:
 - Los servicios proporcionados por la capa de red deben ser **independientes** del enrutador.
 - La capa superior (capa de transporte) debe estar **aislada de los detalles de las redes subyacentes** (número y tecnología de routers, topologías de las redes, etc.)
 - Esquema de **direccionamiento uniforme**.

Arquitectura de Internet: niveles de ISPs

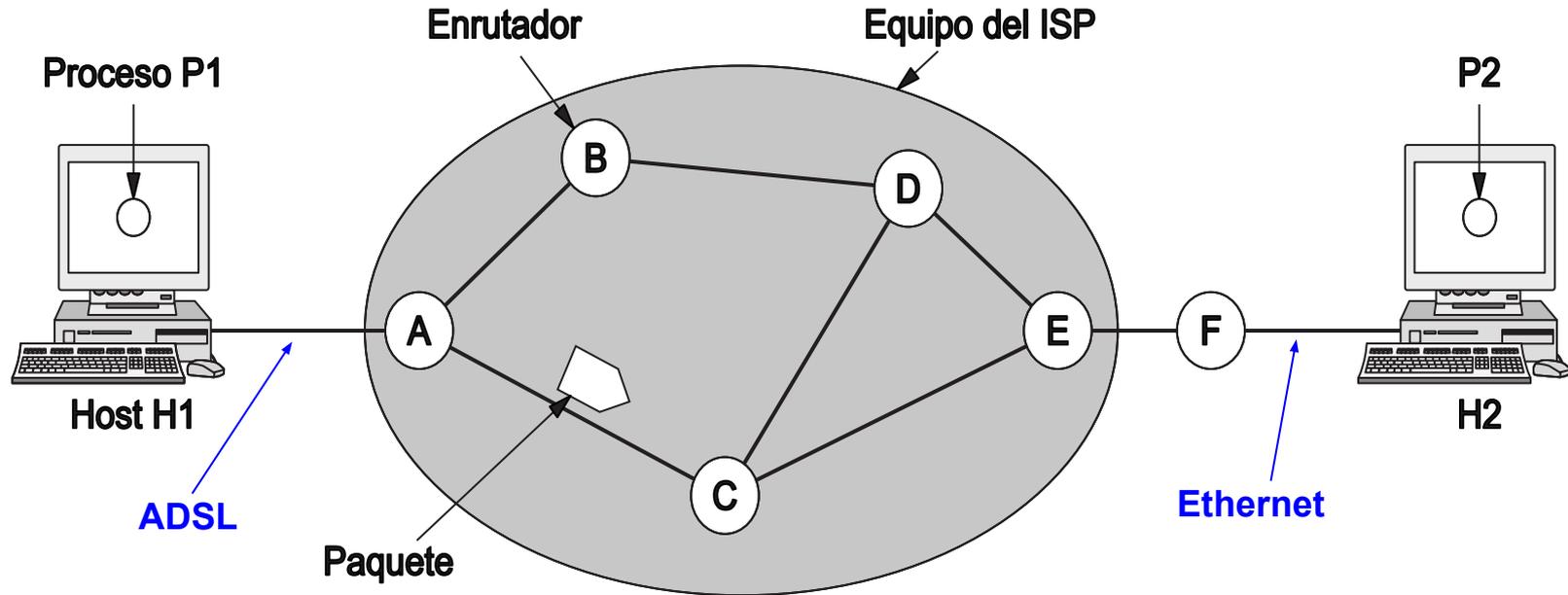


Capa de red

Problema a resolver por la capa de red:

¿Cómo llega el paquete de la máquina H1 a la máquina H2?

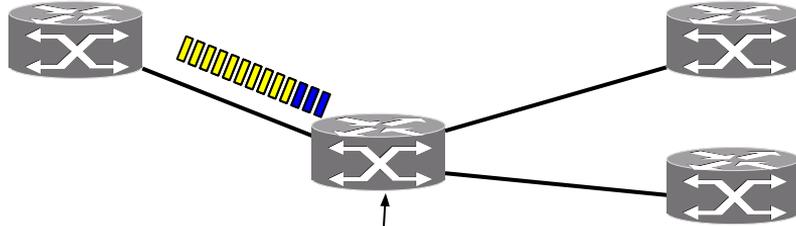
¿Cómo interconectar dos tipos de redes diferentes (de cualquier tipo)?



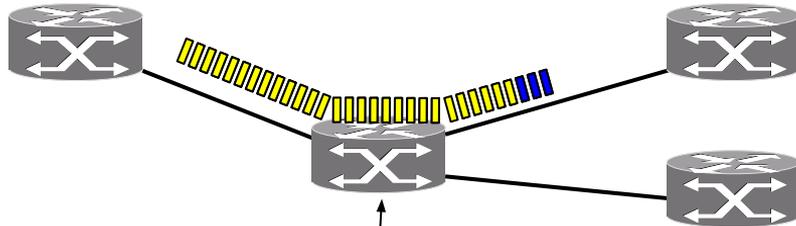


Conmutación por paquetes: con y sin almacenamiento

Sin almacenamiento

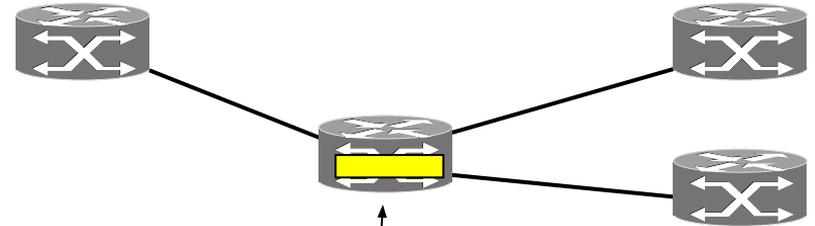
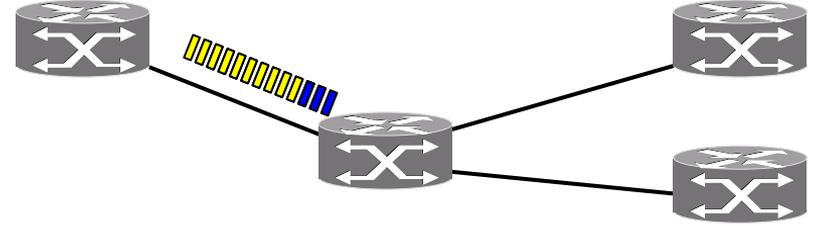


Detecta el destino a partir del encabezado

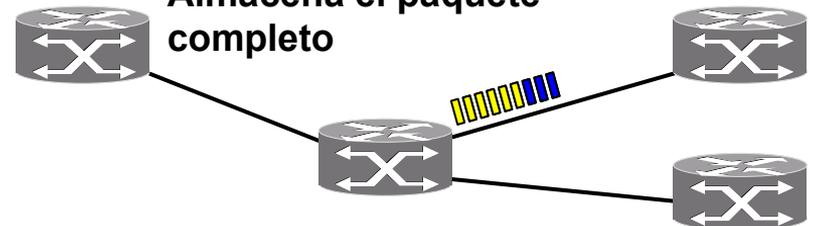


Envía los bits a medida que los recibe sin almacenarlos

Con almacenamiento



Almacena el paquete completo





Servicios sin conexión y orientados a conexión

- **Servicios sin conexión.**

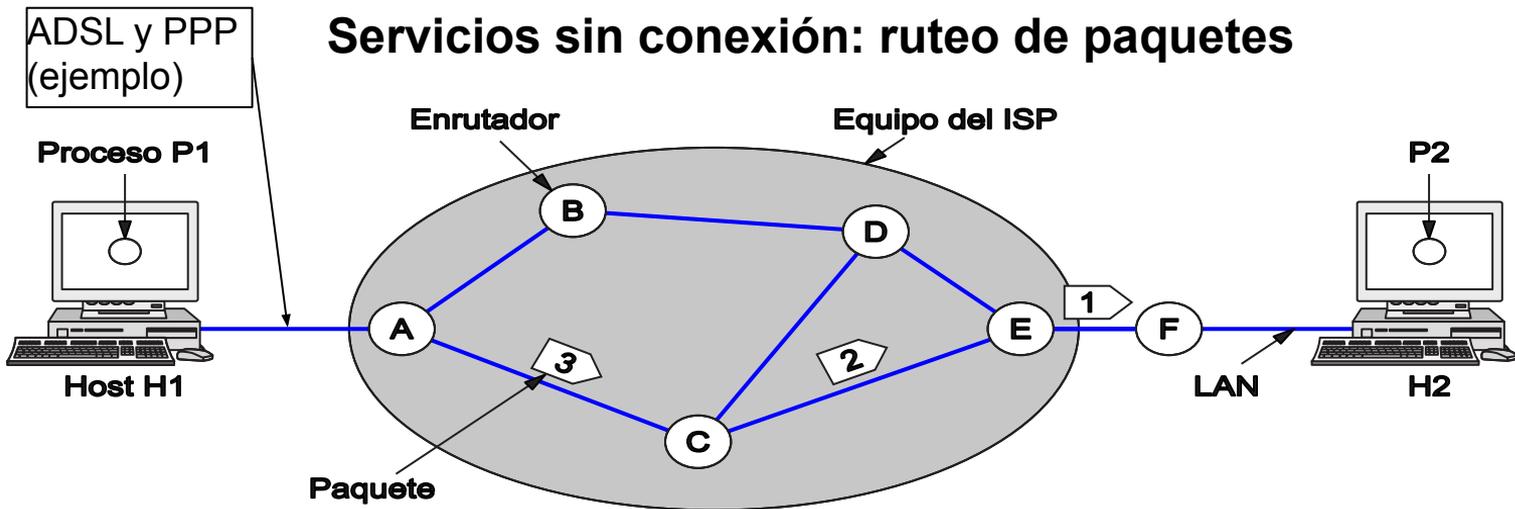
- No hay conexión: **Sin negociación** previa entre origen y destino.
- No se establece un circuito o ruta previa al envío de datos.
- Los paquetes de datos se **rutean por separado** y de manera independiente.
- La información de ruteo de los paquetes es la **dirección de destino**.
- Las **tablas de ruteo** asocian el **destino final** con el **siguiente** salto.
- Basado en el sistema de telegramas.



Un servicio sin conexión puede establecerse sobre una capa de nivel inferior orientada a conexión (por ejemplo, IP sobre ADSL), o sobre una red de redes que incluya ambos tipos de servicios (IP sobre una red de redes que incluya redes Ethernet, ADSL, SONET y PPP).



Servicios sin conexión: ruteo de paquetes



Paquete

Tabla de A

A	-
B	B
C	C
D	B
E	C
F	C

Destino Línea de salida o próximo salto

Tabla de C

A	A
B	A
C	-
D	E
E	E
F	E

Tabla de E

A	C
B	D
C	C
D	D
E	-
F	F

¿Cómo arman los routers estas tablas?: Algoritmos de ruteo (se verá al final de esta unidad)



Servicios sin conexión: ruteo de paquetes

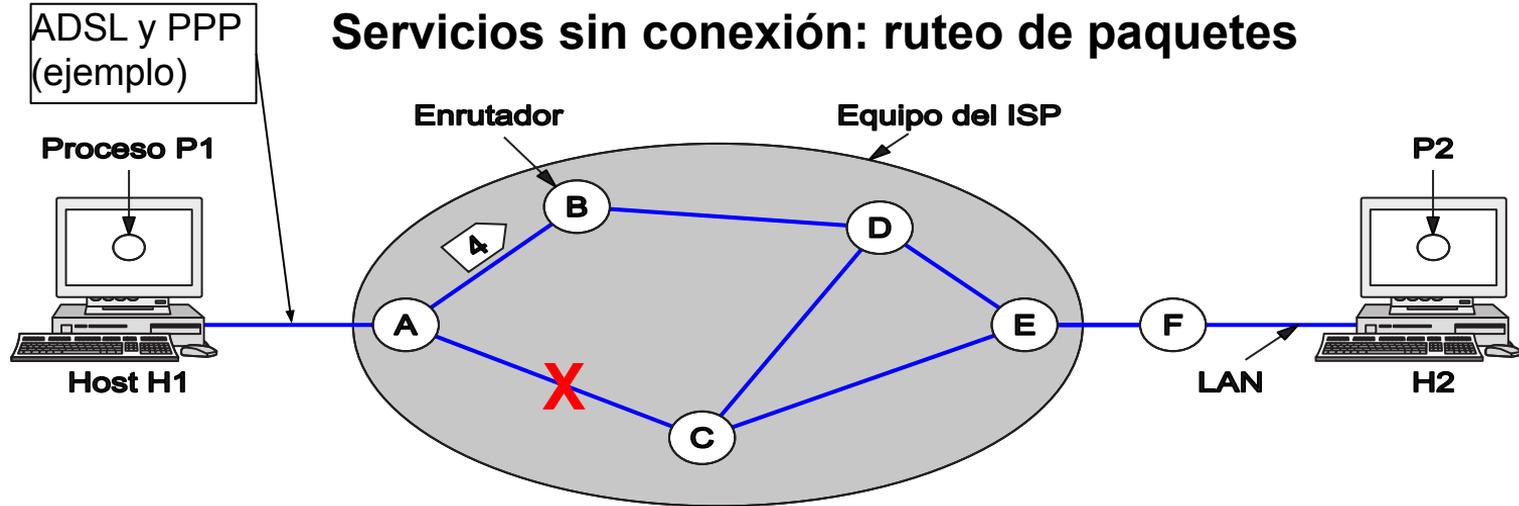


Tabla de A

A	-
B	B
C	C
D	B
E	B
F	B

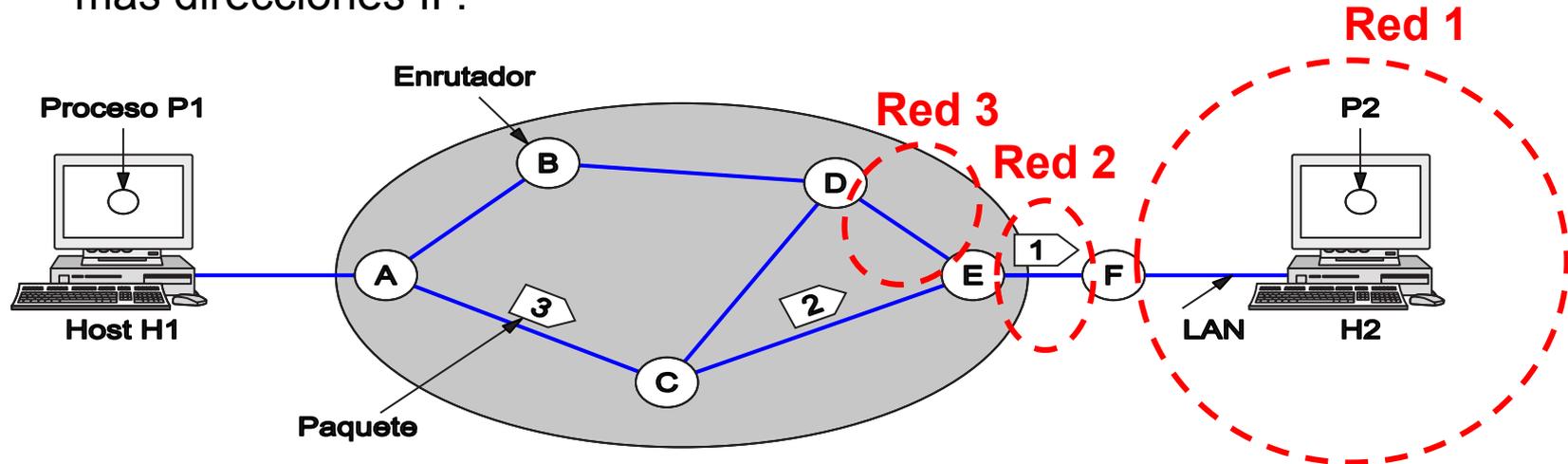
Ante una falla en el enlace A-C,
la tabla de ruteo del router A
puede actualizarse

Servicios sin conexión: ruteo de paquetes (explicación figura anterior)

- El proceso P1 necesita enviarle datos al proceso P2.
- La capa de red puede dividir los datos en paquetes (si la cantidad de datos es grande).
- Cada enrutador tiene una **tabla** con dos al menos dos datos:
 - **Destino final** (puede estar directamente conectado al enrutador o lejano).
 - **Línea de salida** o próximo salto (enrutador directamente conectado al cual enviar el paquete para que llegue al destino final).
- Las **tablas de ruteo son dinámicas, pueden cambiar** si se produce un problema en una ruta (fallo en la conexión, fallo en un enrutador, congestión en una ruta).
- **Algoritmo de enrutamiento: componente clave del sistema.** Determina la línea de salida de acuerdo al destino final. **Implementación distribuida.**

Notas sobre ruteo en IP:

- En IP, las tablas de ruteo indican las redes destino, no los host destinos.
 - Solo el último router entregará el paquete al host destino final.
- Las direcciones IP (prefijos de IPs) se asignan a redes (sistemas autónomos).
 - Los routers están conectados a 2 o más redes, por lo tanto tendrán dos o más direcciones IP.



Servicios sin conexión y orientados a conexión

- Servicios **orientados a conexión** o de circuitos virtuales
 - Se establece una **conexión**: **Con negociación** previa entre origen y destino.
 - Antes de enviar los paquetes, se **establecerse la ruta entre el origen y el destino** o **conexión** (física o virtual).
 - La información de ruteo de los paquetes es un **identificador de conexión** o **circuito virtual**.
 - Las tablas de ruteo asocian un **circuito de salida** con el **circuito de entrada**.
 - Basado en el sistema telefónico.



Un servicio orientado a conexión puede establecerse sobre servicios sin conexión. Ejemplo: TCP (servicio orientado a conexión), trabaja sobre IP (servicio sin conexión)



Servicios orientado a conexión: conmutación de circuitos virtuales

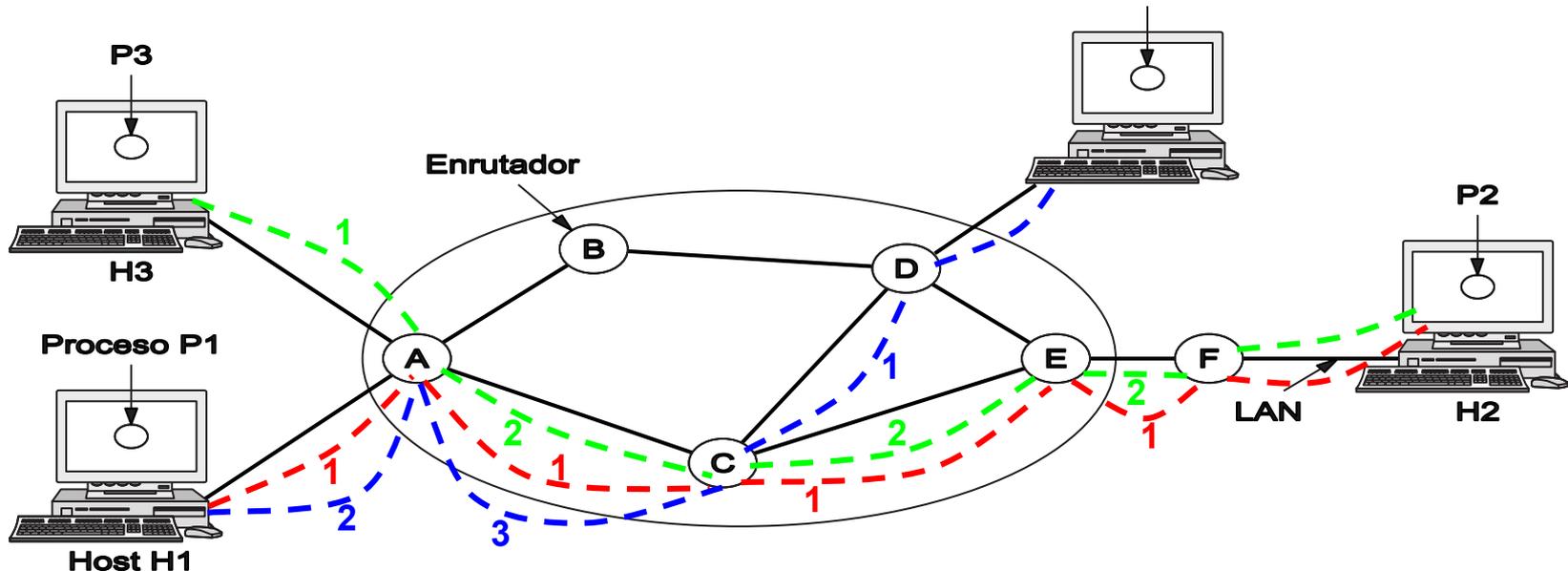


Tabla de A

H1	1	C	1
H3	1	C	2
H1	2	C	3

Entrada

Salida

Tabla de C

A	1	E	1
A	2	E	2
A	3	D	1

Tabla de E

C	1	F	1
C	2	F	2

Servicios orientado a conexión: conmutación de circuitos virtuales

- H1 quiere enviar datos a H2
- Cada tabla asocia el identificador de **circuito entrante y enrutador inmediato de origen** con el **identificador de circuito saliente y enrutador inmediato destino**.
- Cada identificador de circuito es análogo a un “cable” entre enrutadores.
 - En los sistemas telefónicos antiguos, el identificador de circuito era realmente un cable.
 - Actualmente puede ser una **ranura de tiempo** o simplemente una **etiqueta**.
- A no puede utilizar el mismo identificador de circuito de salida hacia C para diferentes conexiones, ya que C no podría diferenciar los circuitos entrantes desde A.
- Protocolo actual importante **MPLS**: MultiProtocol Label Switching (Conmutación Multiprotocolo Mediante Etiquetas).

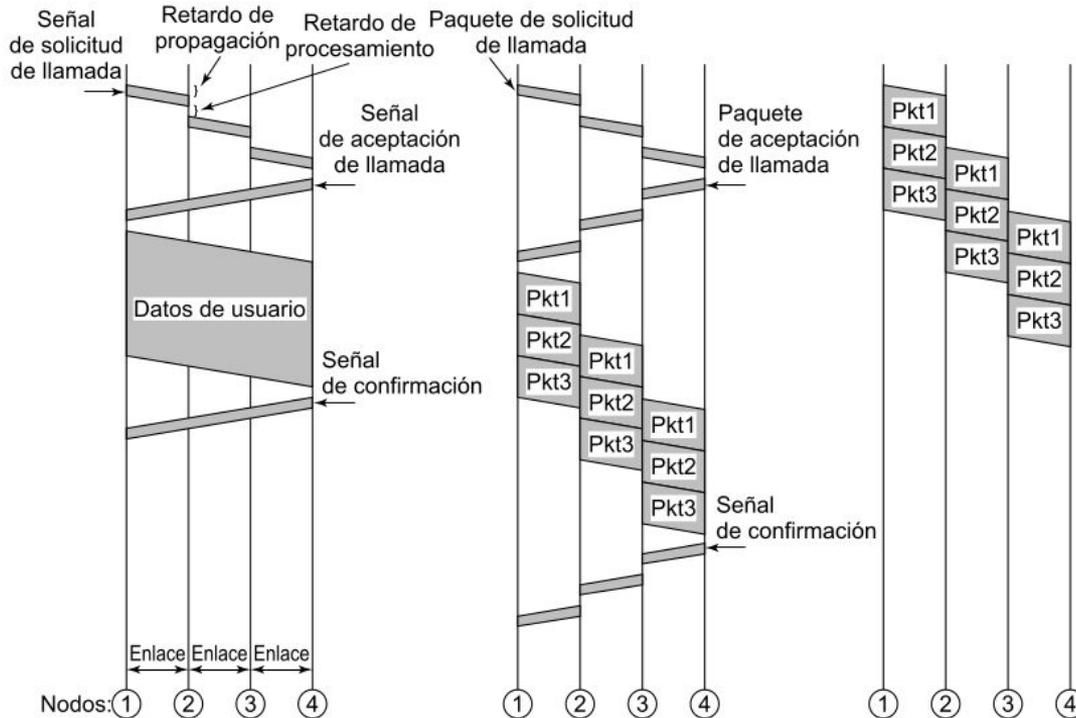
Servicios orientado a conexión vs servicios sin conexión

Asunto	Red sin conexión	Red de circuitos virtuales
Configuración del circuito	No necesaria.	Requerida. Necesidad de tiempo y recursos al comienzo. Más simple el ruteo posterior.
Direccionamiento	Cada paquete contiene la dirección de origen y de destino completas. Más bits. Tablas de ruteo mucho mayor (los destinos finales pueden ser muchos).	Cada paquete contiene un número de CV corto. Menos bits para direccionamiento. Tablas de ruteo menores.
Información de estado de las conexiones	Los enrutadores no contienen información de estado sobre las conexiones.	Cada CV requiere espacio de tabla del enrutador por cada conexión
Enrutamiento	Cada paquete se enruta de manera independiente	La ruta se elige cuando se establece el CV; todos los paquetes siguen esa ruta
Decisiones de ruteo	Todo el tiempo, en cada salto	Solo al principio.

Servicios orientado a conexión vs servicios sin conexión

Asunto	Red sin conexión	Red de circuitos virtuales
Efecto de fallas del enrutador	Ninguno, los paquetes pueden elegir otro camino (excepto para paquetes perdidos durante una caída).	Muy serio, terminan todos los CVs que pasaron por el enrutador defectuoso (aún cuando el router falle solo un segundo).
Calidad del servicio	Difícil (no pueden asegurarse recursos)	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV
Control de congestión	Difícil	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV
Aprovechamiento de recursos	Adaptable. Al no haber recursos asignados, no hay recursos perdidos por baja carga de datos.	Si hay baja carga de datos, los recursos asignados no utilizados se desaprovechan.
Adaptabilidad al nivel de carga	Muy adaptable. Los paquetes pueden enviarse por otros ruteadores si uno está saturado.	Poco adaptable. Si un circuito tiene mucha carga y otros poca, los paquetes seguirán siempre por esos circuitos.

Comparación entre conmutación de circuitos, conmutación de paquetes mediante circuitos virtuales y conmutación de paquetes mediante datagramas.



(a) Conmutación de circuitos

(b) Conmutación de paquetes
mediante circuitos virtuales

(c) Conmutación de paquetes
mediante datagramas

- Con circuitos virtuales la ruta no está dedicada a la conexión.



Interconexión de Redes

Dificultad: Existen muchos tipos de redes diferentes

Aspecto	Algunas posibilidades
Servicio ofrecido.	Sin conexión vs. orientado a conexión.
Direccionamiento.	Distintos tamaños, plano o jerárquico.
Difusión.	Presente o ausente (también multidifusión).
Tamaño de paquete.	Cada red tiene su propio valor máximo.
Ordenamiento.	Entrega ordenada y desordenada.
Calidad del servicio.	Presente o ausente; muchos tipos distintos.
Confiabilidad.	Distintos niveles de pérdida.
Seguridad.	Reglas de privacidad, cifrado, etcétera.
Parámetros.	Distintos tiempos de expiración, especificaciones de flujo, etcétera
Contabilidad.	Por tiempo de conexión, paquete, byte o ninguna.

Interconexión de Redes: Posibles mecanismos para interconectar las redes

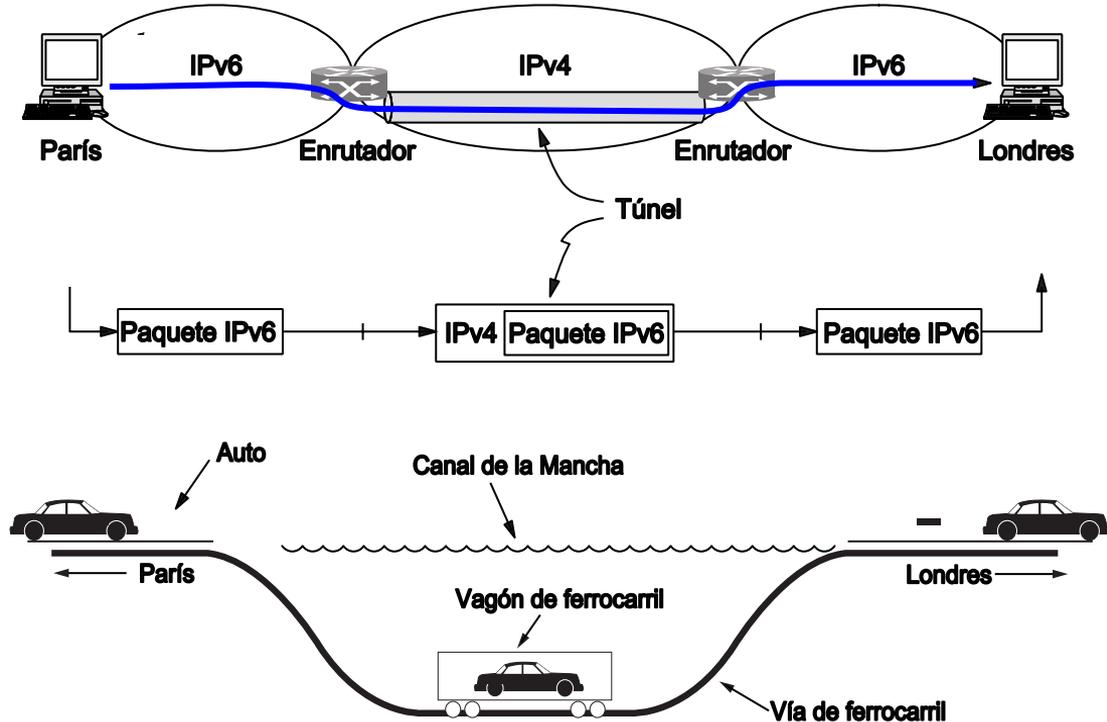
1. A nivel capa de enlace: mediante **Traductores/adaptadores** que traduzcan tramas y adapten diferentes tipos de redes. Por ejemplo: traductores Ethernet-Wifi, traductores Ethernet-SONET, Ethernet-ASDL, Ethernet10BaseT-Ethernet100BaseT etc.
 - a. Se requerirían gran cantidad de traductores (cantidad = $(n-1)(n)/2$).
 - b. Cada vez que se cree una nueva tecnología de capa de enlace o física, se requerirían traductores que permita conectar la nueva tecnología con todas las existentes.
 - c. No resuelve el problema del direccionamiento global.
2. **Tunelización.**
3. A nivel capa de red: Construir **otra capa** que permita la interconectividad. Los paquetes pasan a la capa de red y la misma se encarga.
 - a. Esta nueva capa se encarga del direccionamiento global.

2° mecanismo de Interconexión de Redes: Tunnelización

- Objetivo: Enviar un paquete entre un origen y un destino tal que:
 - El **origen** y el **destino** pertenecen al **mismo tipo de red** (red superpuesta u “overlay”).
 - Entre las redes origen y destino existen **redes de diferentes tipos**.
 - Todas las redes pueden ser del **mismo o diferente nivel**.
 - Se requieren **ruteadores multiprotocolo**.
 - **A nivel de datos, una trama o paquete se encapsula dentro de otro.**
 - Aplicaciones: VPN, MPLS, PPPoE (PPP sobre Ethernet), IPv6 sobre IPv4.

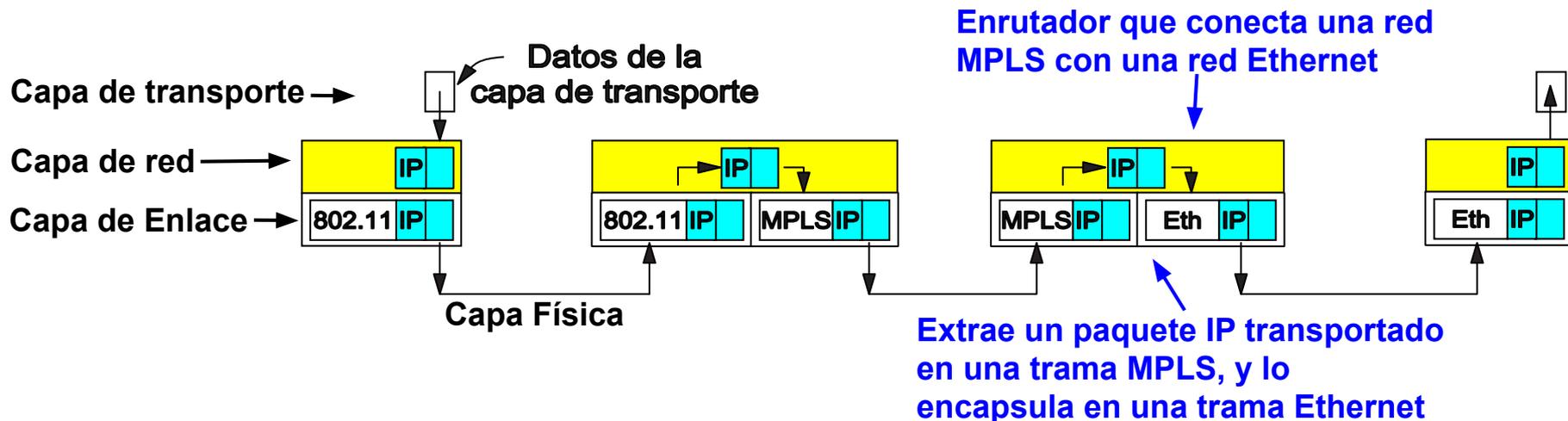
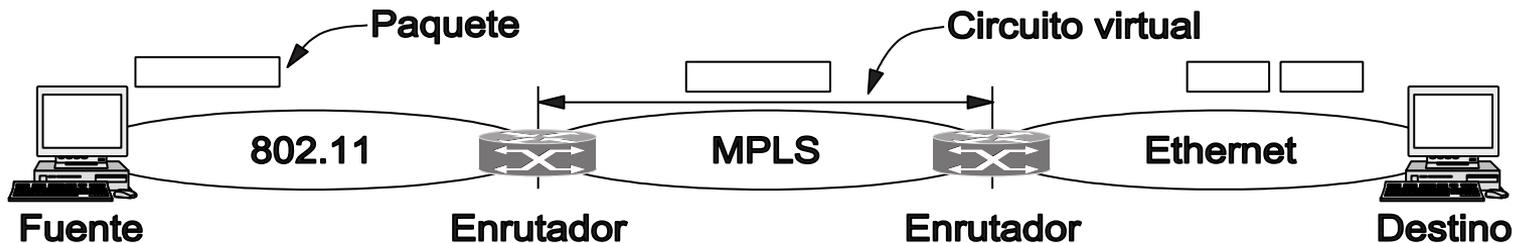


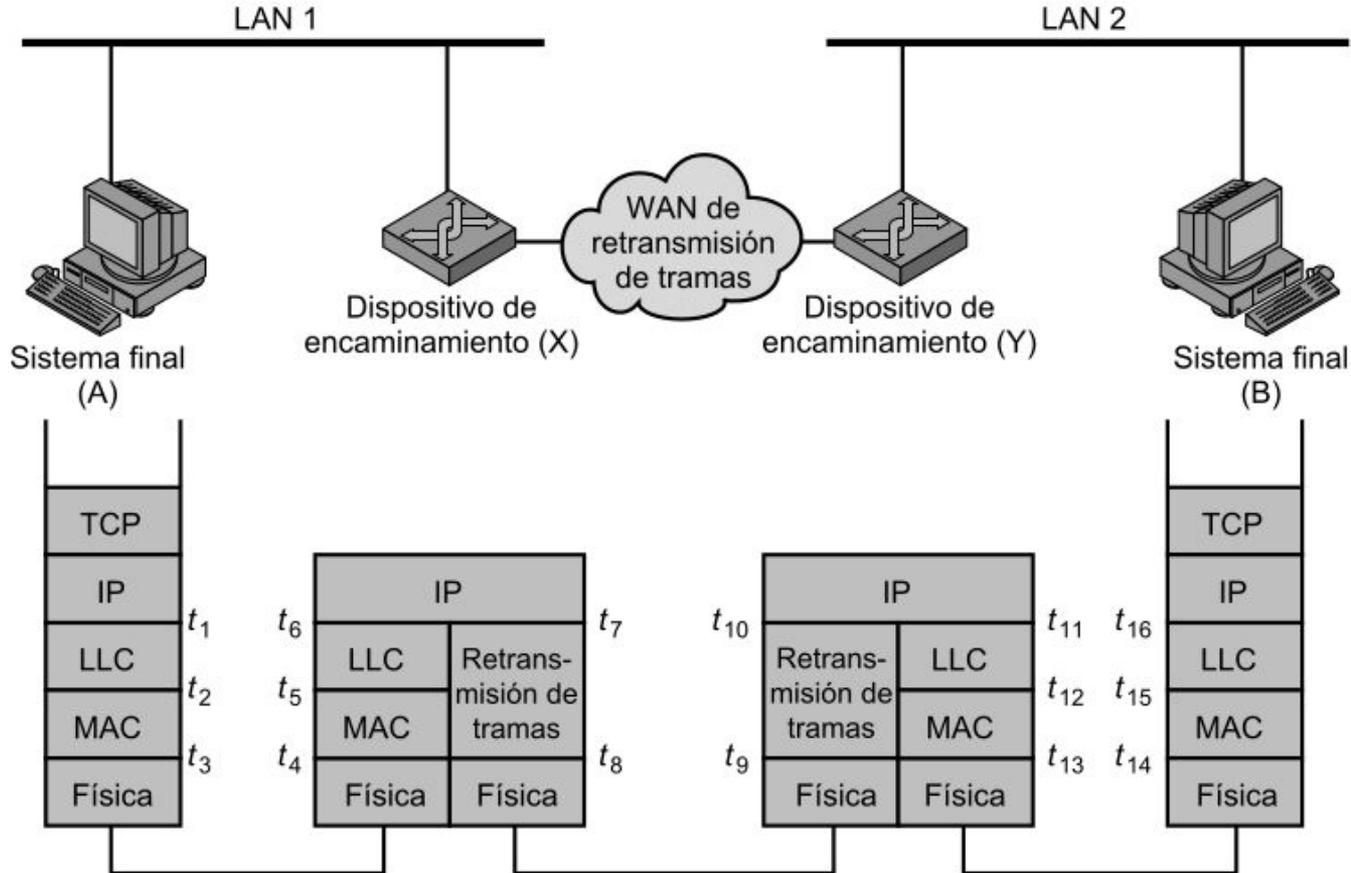
2° mecanismo de Interconexión de Redes: Tunnelización





3° mecanismo de Interconexión de Redes: Capa de Red





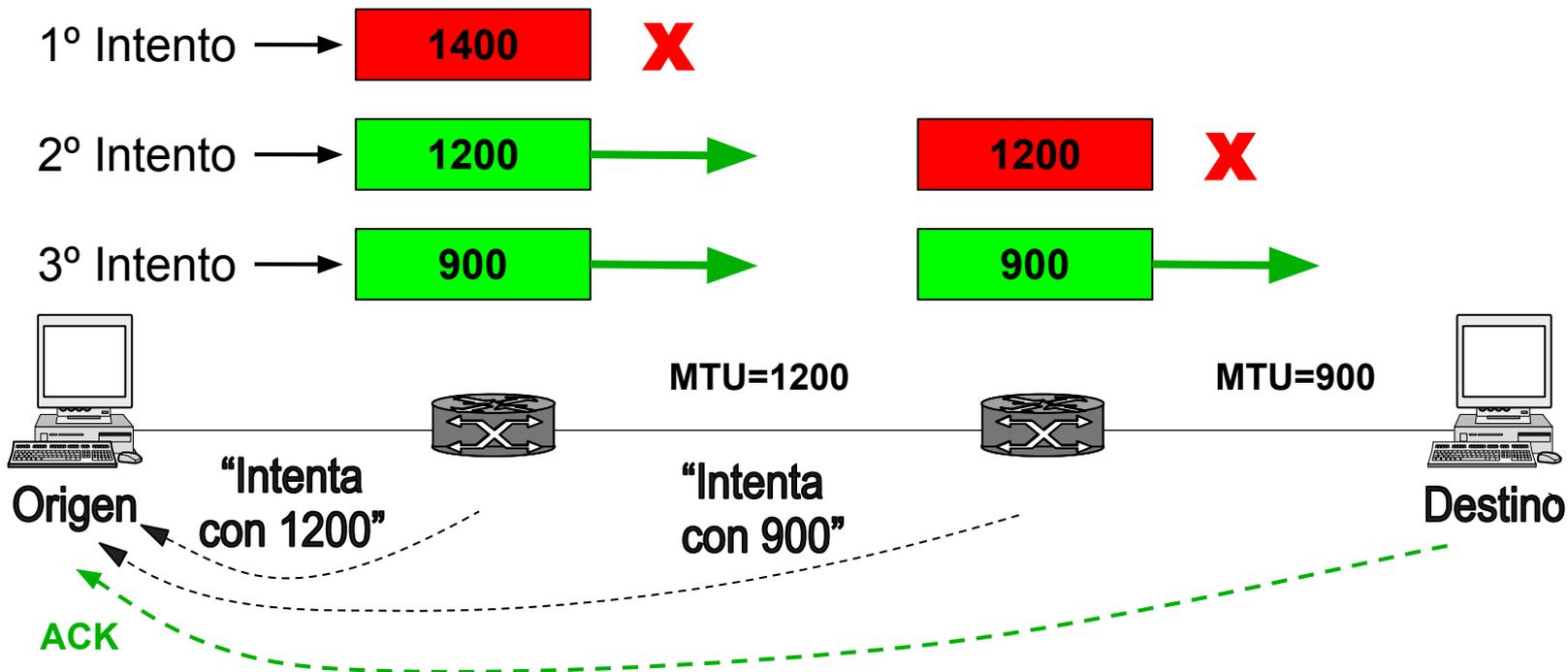
Interconexión de Redes: Diferentes Tamaño de paquetes

- Los protocolos imponen un **tamaño máximo de paquetes o MTU** (Maximum Transmission Unit o Unidad de Transmisión Máxima).
 - **Ventajas de mayor tamaño: menor sobrecarga.**
 - **Ventajas de menor tamaño: menor probabilidad de error.**
 - Ejemplo: Ethernet 1500 bytes, IEEE802.11 2272 bytes, IP 65515 bytes.
- Problema: Paquetes de tamaño N que tienen que transitar por una red con tamaño de **paquete menor**.
 - Solución 1: **Descubrimiento de MTU** de la ruta completa.
 - Solución 2: **Fragmentación** (permitir que los enrutadores dividan un paquete en fragmentos y enviar cada uno como un paquete separado).

Interconexión de Redes: Descubrimiento de MTU de la ruta

- Se envían **paquetes de prueba** con banderas indicando que **no se pueden fragmentar**.
- Si el paquete llega a una red con **MTU menor** al tamaño del paquete, el router **lo rechaza** y envía un mensaje de error.
- El origen recibe el mensaje de error y prueba con **paquetes más pequeños**.
- El proceso se repite si otros enrutadores con **MTU menor** reciben el paquete.
- Cuando el paquete **llega al destino**, este responde. El emisor **recibe el ack** y **obtiene el MTU de la ruta**.
- Si la **ruta cambia** y un paquete llega a una red con **MTU menor**, **el proceso se repite** (la MTU se adapta a diferentes rutas).

Interconexión de Redes: Descubrimiento de MTU de la ruta





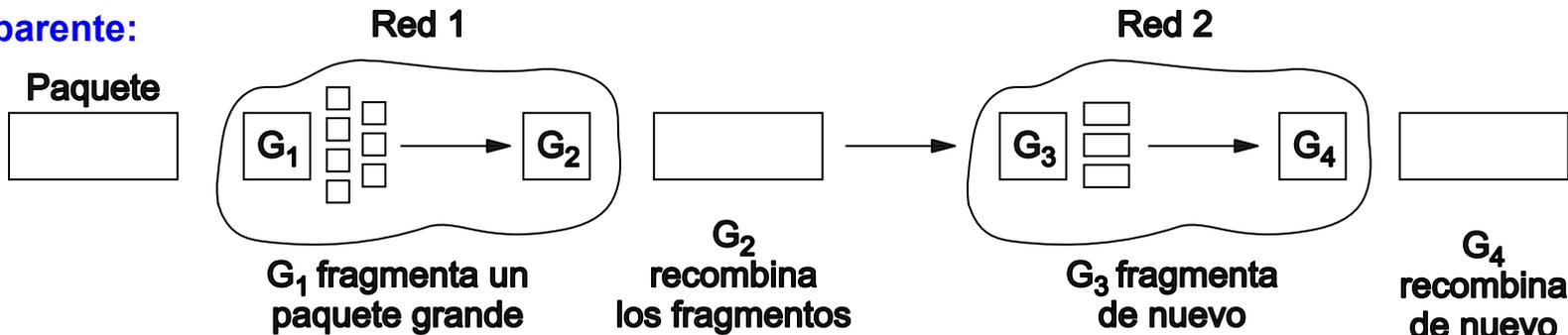
Interconexión de Redes: Fragmentación de paquetes

- Los enrutadores **dividen el paquete**.
- Dos enfoques:
 - **Fragmentación transparente**: El router de entrada a la red divide el paquete en fragmentos, y el router de salida los reensambla.
 - **Desventajas**:
 - Sobrecarga de enrutadores.
 - Uso de gran cantidad de memoria en los enrutadores.
 - Se restringen las rutas al tener que salir todos los paquetes por el mismo enrutador.
 - **Fragmentación no transparente**: una vez divididos, los fragmentos se comportan como paquetes independientes hasta el destino final.
 - **Ventaja: Menos sobrecarga en los enrutadores.**
 - **Usado por protocolo IP.**

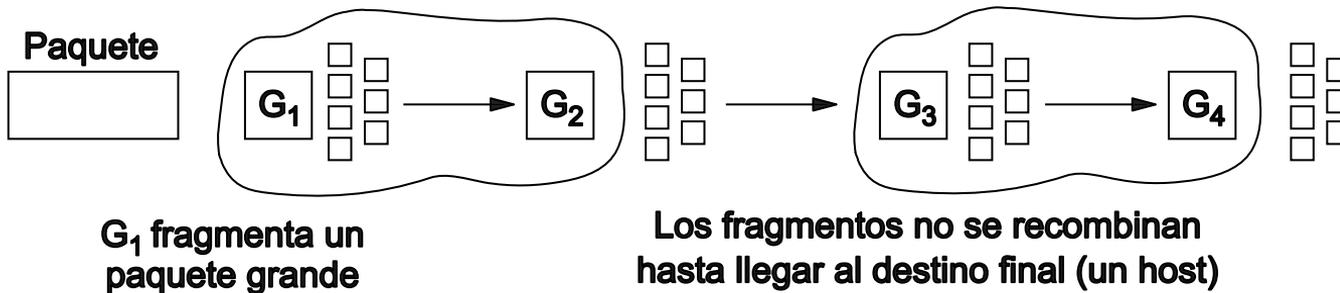


Interconexión de Redes: Fragmentación de paquetes

Transparente:

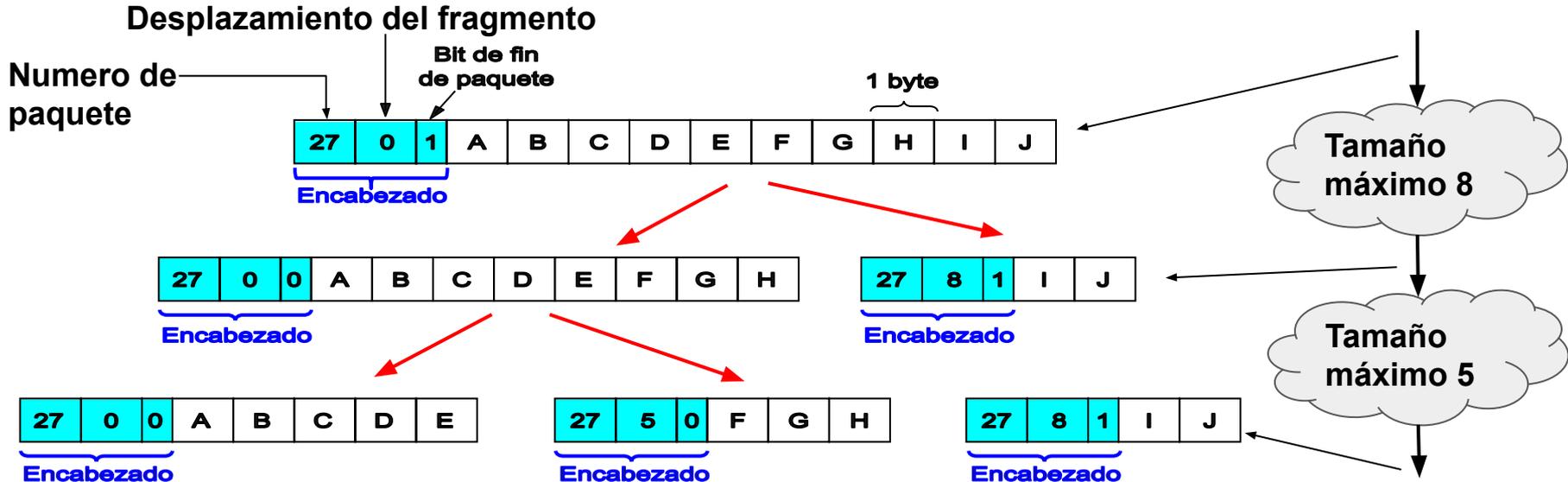


No transparente:



Interconexión de Redes: Fragmentación de paquetes

- Fragmentación no transparente. Necesidad de:
 - Número identificador de paquete.
 - Campo que indique el desplazamiento del fragmento dentro del paquete.
 - Agregar un indicador de fin del paquete.





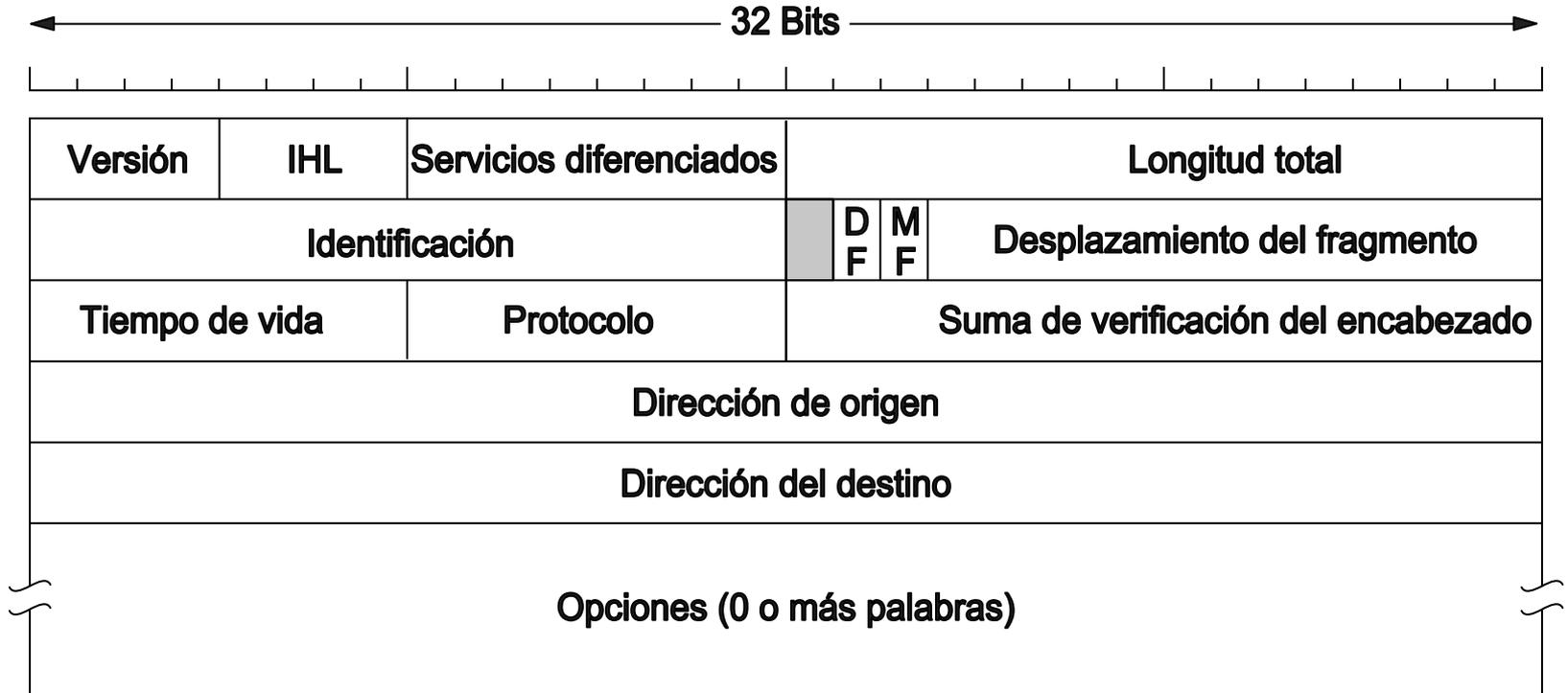
Temario

- Introducción.
- Congestión y calidad de servicio.
- ● **IPv4**
 - **Direcciones IP. Encabezado IPv4.**
 - **Subredes.**
 - **Direccionamiento basado en clases y sin clases. Superredes.**
 - **Agotamiento de direcciones IPv4. Soluciones. NAT**
 - **Multidifusión**
- IPv6
- Protocolos de control de Internet
- Conmutación basada en etiquetas (MPLS)
- Algoritmos de enrutamiento

Interconexión de Redes: IP (Internet Protocol)

- Diseñado para **interconectar redes**.
- Protocolo de **mejor esfuerzo**: **hace todo lo posible** para entregar un paquete, pero **no garantiza** la entrega.
- Tamaño máximo de paquetes: **65 KBytes**.
- **Rutea** paquetes entre diferentes redes:
 - Los paquetes pueden pasar entre diferentes niveles de ISPs.
 - Pueden pasar por ISPs y puntos de interconexión (IXP).
 - Pueden pasar por diferentes tecnologías de red.
- Protocolo **sin conexión**.

Interconexión de Redes: encabezado IPv4 (IP versión 4)



Interconexión de Redes: encabezado IP

- Versión: versión del protocolo IP (IPv4, IPv5, IPv6, etc.).
- IHL (Internet Header Length): Longitud del encabezado en palabras de 32 bits. El encabezado es de longitud variable.
- Servicios diferenciados: Calidad de servicio¹
 - Servicio expedito, servicio asegurado.
 - Notificación explícita de congestión.
 - Indicación de ocurrencia de congestión.
- Longitud total: Longitud de todo el paquete (en bytes).
- Identificación: Número o identificación de paquete al cual pertenece un fragmento.
- Bit sin uso: ¿?

¹ Anteriormente indicaba parámetros de fiabilidad, prioridad, retardo y rendimiento que raramente se usaban. Se sustituyó a “Servicios diferenciados”..

Interconexión de Redes: encabezado IP

- DF (Don't Fragment): Si se marca, el paquete no debe fragmentarse.
 - El paquete llegará sin fragmentarse o generará un mensaje de error.
 - Útil para encontrar la MTU de una ruta.
- MF (More Fragments): Para indicar si deben esperarse más fragmentos.
- Desplazamiento del fragmento: múltiplo de 8 bytes (el fragmento más pequeño puede tener 8 bytes). Pueden haber 8192 fragmentos.
- Tiempo de vida: Se decrementa en cada salto. Si llega a cero el paquete se descarta.
- Protocolo: identificación del protocolo de la capa de transporte (TCP, UDP, etc.). Listados en www.iana.org. (Internet Assigned Numbers Authority)
- Suma de verificación **del encabezado**: Se debe recalcular en cada salto
 - El campo tiempo de vida cambia en cada salto
 - Se evita que enrutadores posteriores ruteen paquetes dañados.



Interconexión de Redes: encabezado IP

- Dirección IP origen y dirección IP destino: 32 bits para IPv4.
- Opciones: Posibilita ampliaciones futuras del protocolo. Algunas opciones son:
 - Seguridad: Especifica que tan secreto que es el datagrama (actualmente no usado, permite a espías identificar paquetes importantes).
 - Enrutamiento estricto desde el origen: Proporciona la ruta completa a seguir como secuencia de direcciones IP. Sirve para hacer mediciones o recuperar tablas de ruteo.
 - Enrutamiento libre desde el origen: Proporciona una lista de enrutadores que no se deben omitir. Los paquetes deben pasar si o si por esos enrutadores (cuestiones políticas o económicas pueden imponer esos enrutadores).



Interconexión de Redes: encabezado IP

- Opciones + relleno (continuación):
 - Registrar ruta: Hace que cada enrutador adjunte su dirección IP al paquete. Sirve para analizar fallas de ruteo o tareas de investigación.
 - Estampa de tiempo: Hace que cada enrutador adjunte una estampa de tiempo al paquete (se usa en conjunto con “Registrar ruta” para tareas de medición o investigación).
 - Relleno: Se utiliza para asegurar que el encabezado posee una longitud múltiplo de 8 bits.
- **No todos los enrutadores procesan los campos opciones.**

Direcciones IP

- 32 bits ($2^{32}=4.29*10^9$).
- **Cada interfaz de red tiene su dirección IP.**
 - Una computadora conectada a dos redes necesita dos interfaces de red y dos direcciones IP.
 - Un enrutador tiene varias direcciones IP (al menos dos).
- Direcciones jerárquicas
 - **Primeros bits: Identifican la red (prefijo).**
 - **Últimos bits: Identificación del host (cada interfaz) dentro de la red.**
 - **Ventaja: Los ruteadores solo trabajan con la dirección de red, no con la IP completa. Menores longitudes de tablas de ruteo.**
 - Desventajas:
 - **La dirección IP depende de la ubicación de la computadora.**
 - **Desperdicio de direcciones.**

- Notación: **32 bits** = 4 bytes, se escriben **como 4 números decimales separados por un punto** (192.168.1.30 = 11000000 10101000 00000001 00011110)
- **Máscara de red** = conjunto de bits tal que al aplicar una AND con una dirección IP, permite obtener el prefijo (dirección de la red).
 - Ejemplo: 24 bits de prefijo (red) y 8 bits de host
 - Dirección IP: 192.168.1.30 = **11000000 10101000 00000001 00011110**
 - Máscara de red: 255.255.255.0 = 11111111 11111111 11111111 00000000
 - Prefijo (red) = 192.168.1.0 = **11000000 10101000 00000001 00000000**
- Otra notación: 192.168.1.30/**24** (/24 indica 24 bits usados para indicar el prefijo o dirección de red).
- ¿Quién asigna las direcciones IP?: Los 5 **RIR** (Regional Internet Registry), dependientes de IANA¹ e ICANN² e, en conjunto con los NIR y LIR.
 - LACNIC³: Registro de Direcciones de Internet de América Latina y Caribe (RIR que rige nuestros IPs).

¹Internet Assigned Numbers Authority ² Internet Corporation for Assigned Names and Numbers

³Latinoamérica y Caribe NIC (Network Information Center)

179.0.132.0/22 = 10110011.00000000.10000100.00000000 (IP de red de UNCuyo)

255.255.252.0 = 11111111.11111111.1111111100.00000000 (Máscara)

**Dirección de red o prefijo
de la UNCuyo. Lo asigna
LACNIC a la UNCuyo**

**Host dentro de la UNCuyo.
Los asigna la UNCuyo a sus
host ($2^{10}=1024$ host).**

179.0.133.131/22 = 10110011.00000000.10000101.00000000 (Ejemplo de IP de host dentro de UNCuyo)

255.255.252.0 = 11111111.11111111.1111111100.00000000 (Máscara)

179.0.132.0 = 10110011.00000000.10000100.00000000

Rango de IPs que pertenecen a la UNCuyo:

Desde 10110011.00000000.10000100.00000000 = 179.0.132.0

Hasta 10110011.00000000.10000111.11111111 = 179.0.135.255

(Ver <https://rdap-web.lacnic.net/ip/179.0.132.52>)

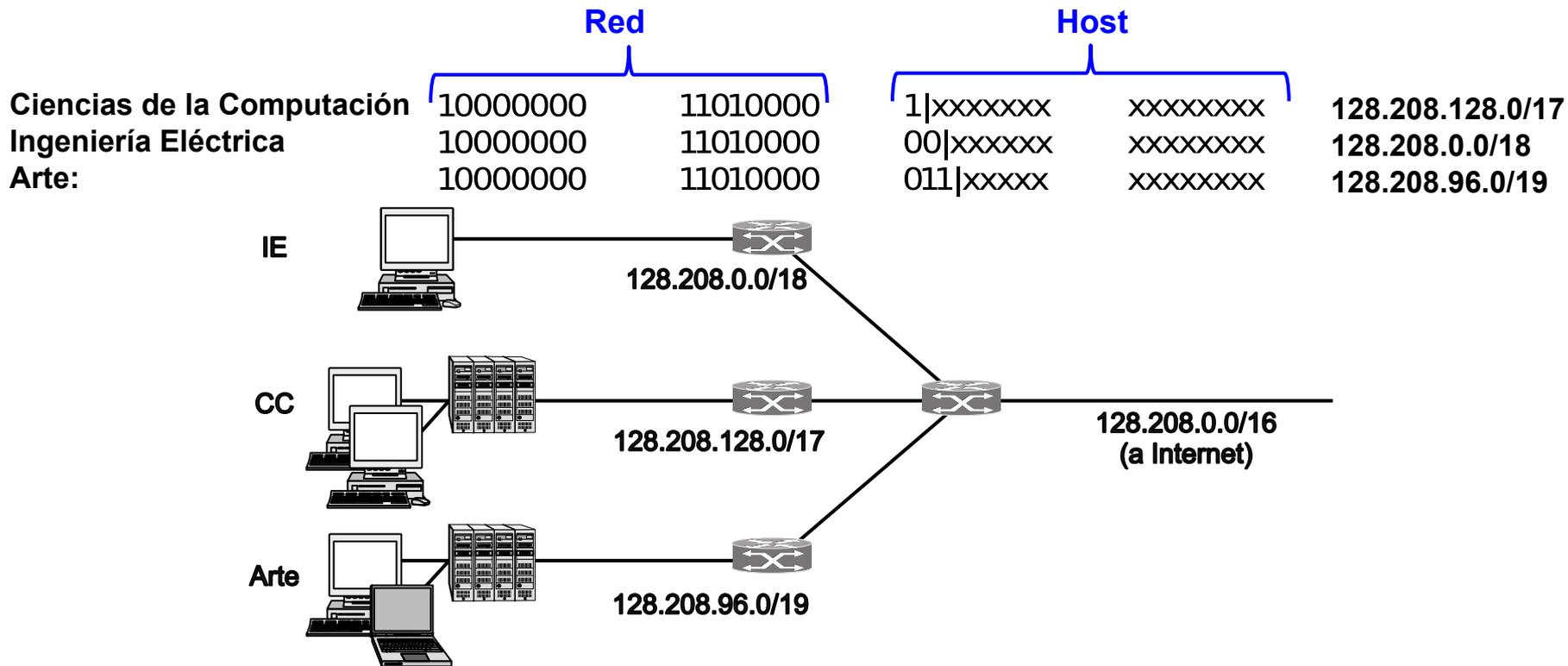
Direcciones IP: Subredes

- Si una empresa u organización posee una dirección IP de red, puede **dividir internamente su red en subredes**:
 - Hacia el exterior la red se sigue comportando como una sola.
 - Hacia el interior se pueden tener varias redes.
- **Ventaja: Mejor organización.**
- Se utilizan los primeros bits de host para identificar las subredes, junto a una máscara.
- El ruteador de entrada debe conocer las máscaras de red de cada subred.



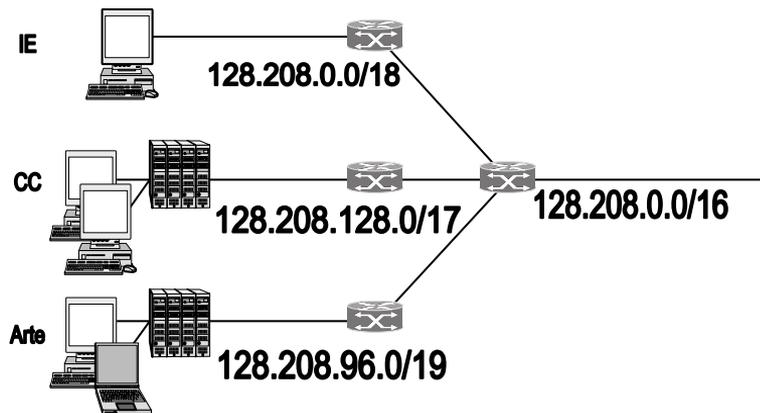


Direcciones IP: Subred



Direcciones IP: Subred Ejemplo

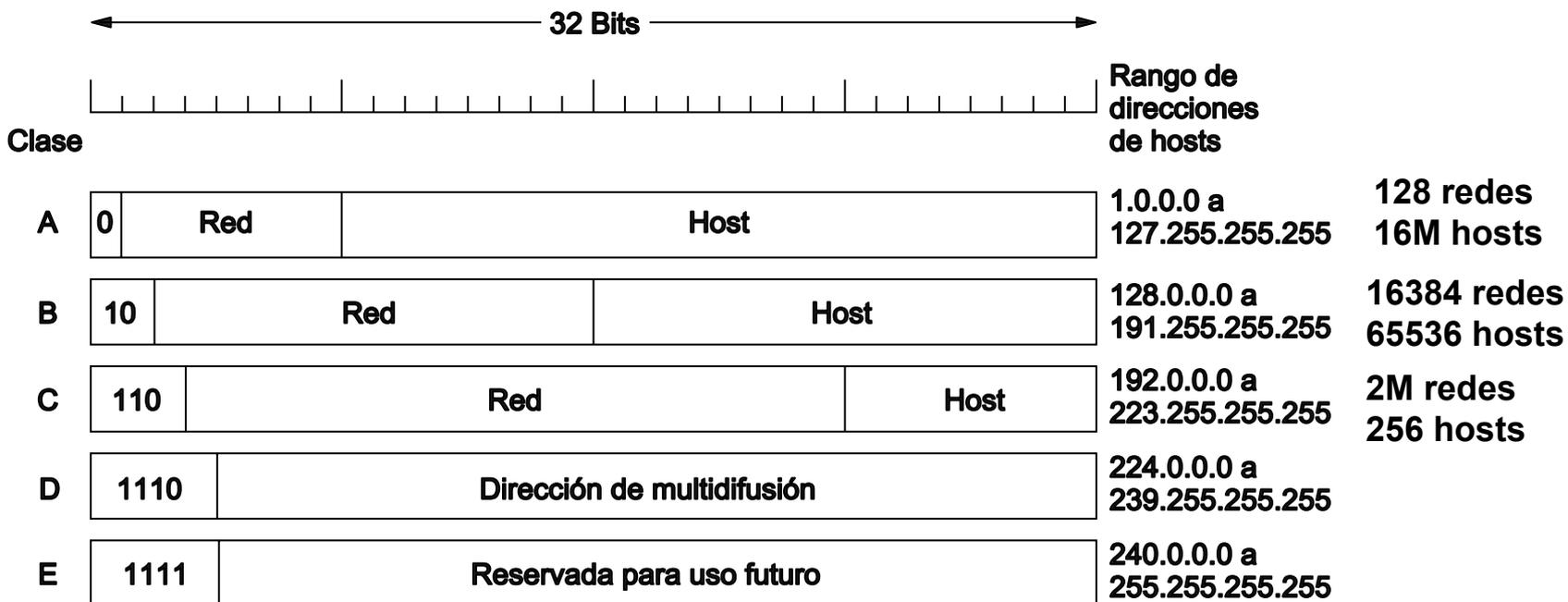
Red	Identificador Red	Máscara
IE	128.208.0.0/18	255.255.192.0
CC	128.208.128.0/17	255.255.128.0
Arte	128.208.96.0/19	255.255.224.0



- Llega el paquete **128.208.2.151**, ¿A cual red va?
 - ¿Va a CC?: $128.208.2.151 \text{ AND } 255.255.128.0 = 128.208.0.0$, **no** es la dirección de CC.
 - ¿Va a IE?: $128.208.2.151 \text{ AND } 255.255.192.0 = 128.208.0.0$, **SI** es la dirección de IE.



Direcciones IP: Direccionamiento basado en Clases



Direcciones IP: Direccionamiento basado en Clases

- Ruteo:
 - Se detecta la clase, y luego se busca en tablas de ruteo.
- **Ventaja: Al ser el número a comparar de tamaño fijo, el algoritmo es mucho más simple que si los números fueran variables.**
- **Problema: gran cantidad de direcciones IP desperdiciadas.**
 - Rara vez una empresa que pida una red tipo C tendrá exactamente 256 hosts, lo mismo una empresa que pide una red tipo B rara vez tendrá exactamente 65536 hosts.
 - **Agotamiento de direcciones IPv4**
 - **Por este motivo ya no se usa.**

Direcciones IP: Direccionamiento sin Clases CIDR (Classless InterDomain Routing)

- **Problema: Agotamiento de direcciones IP.**
 - **Causa 1: Asignación ineficiente de direcciones.**
- CIDR (Classless InterDomain Routing o Enrutamiento Inter dominio **sin Clases**). RFC 4632 (1993).
- Se pueden asignar direcciones de red de **cualquier longitud**. Ejemplos: 192.24.0.0/21, 192.24.16.0/20 (el /x es parte de las tablas de ruteo)
- **Agregación de direcciones**: Combinar prefijos de redes en prefijos más grandes llamados **superredes** (mayor números de host).
 - Mayor uso de jerarquías de redes y **reducción de tablas de ruteo**.
- Ventajas:
 - **Hace más eficiente en uso de las direcciones IP disponibles.**
 - **Disminuye la sobrecarga en los enrutadores**

Direcciones IP: Superredes

1 entrada en su tabla de ruteo que abarca a Cambridge, Oxford y Edimburgo

Nueva York



3 entradas en su tabla de ruteo

Londres



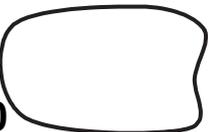
Cambridge



192.24.0.0/21

11000000.00011000.00000000.00000000

Oxford



192.24.16.0/20

11000000.00011000.00010000.00000000

Edimburgo



192.24.8.0/22

11000000.00011000.00001000.00000000

11000000.00011000.00000000.00000000

192.24.0.0/19

Coinciden en estos 19 bits
(pueden agruparse en una
sola dirección IP)

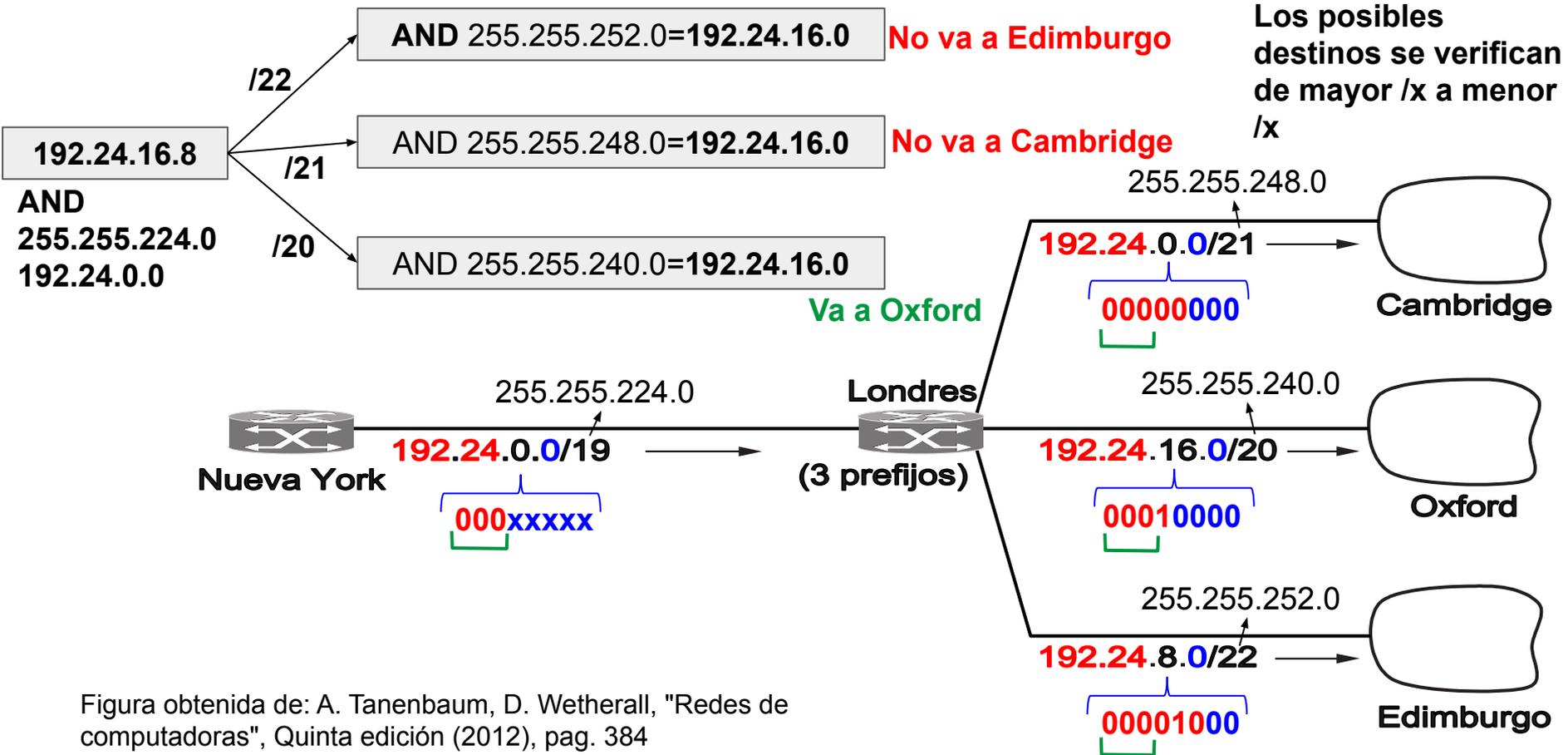


Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 384



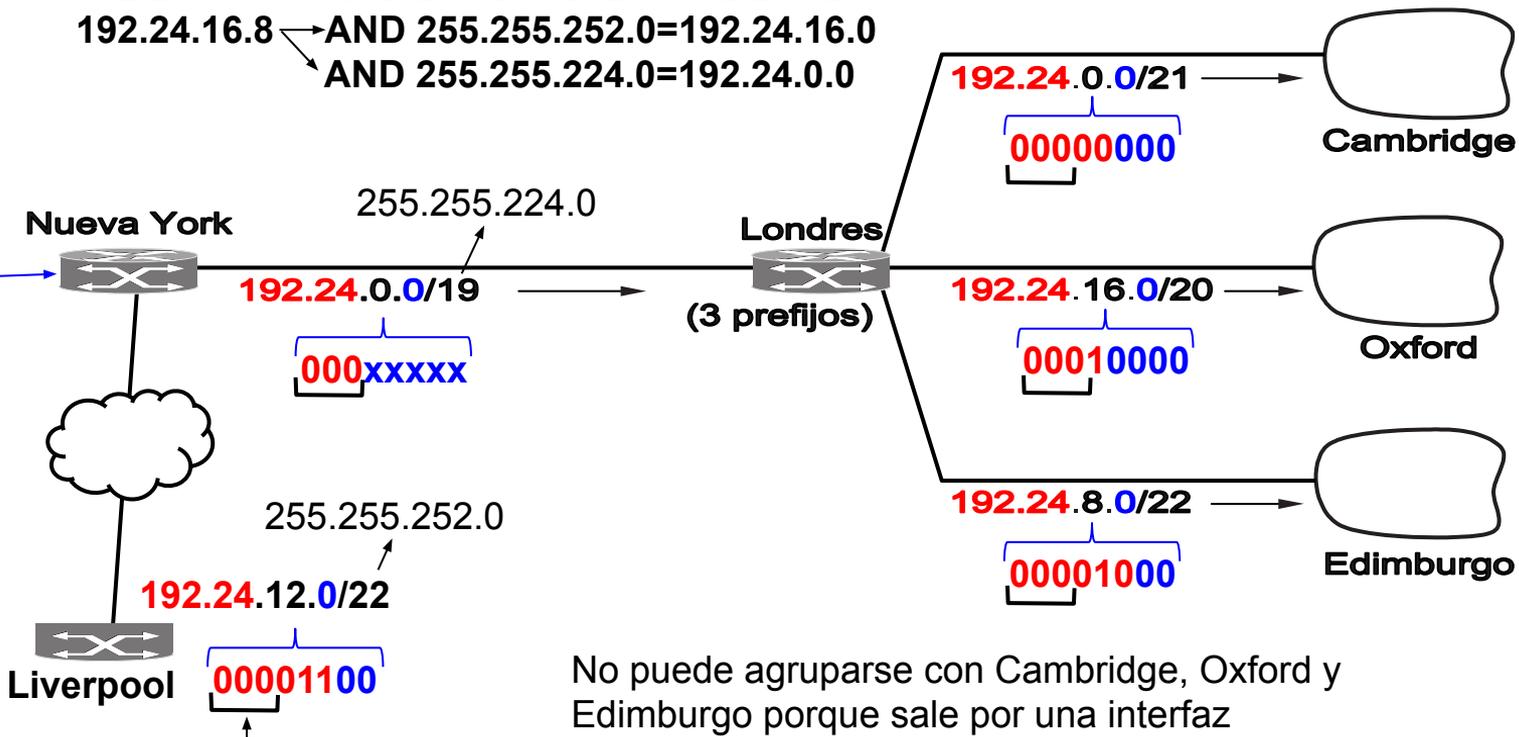
CIDR (Classless InterDomain Routing): traslape de prefijos

192.24.14.0 → AND 255.255.252.0 = 192.24.12.0
 192.24.16.8 → AND 255.255.252.0 = 192.24.16.0
 AND 255.255.224.0 = 192.24.0.0

Tabla Ruteo

.....
 192.24.12.0/22
 192.24.0.0/19

Primero se verifica
la dirección de red
más larga



No puede agruparse con Cambridge, Oxford y Edimburgo porque sale por una interfaz diferente del Router Nueva York

Agotamiento de direcciones IP

- Causas:
 - El número total direcciones IPv4 ($2^{32}=4.29*10^9$) **no fue suficientes**.
 - El empleo de **clases de direcciones (A, B, C)** hizo que hubiera gran número de direcciones asignadas pero **no utilizadas**.
 - Al principio, las direcciones IP **se distribuyeron de manera inadecuada**.
- Soluciones que ayudan a mitigar el problema:
 - **CIDR (ruteo sin clases)**
 - Hace más eficiente la asignación de direcciones de red.
 - **No incrementa el número de direcciones IP.**
 - **Reclamación de direcciones sin uso**
 - no todos las quieren devolver
 - **No incrementa el número de direcciones IP.**

Problema: Agotamiento de direcciones IP

- **Soluciones que ayudan a mitigar el problema (continuación...):**
 - **IP dinámica.**
 - Al conectarse una máquina a la red se le asigna una IP. Cuando se desconecta, esa IP queda libre para asignarse a otra máquina.
 - **No incrementa el número de direcciones IP.**
 - **Tendencia actual a mantenerse conectado todo el tiempo hace que pierda aplicabilidad.**
- **Soluciones que **resuelven** el problema:**
 - **NAT:** Network Address Translation. Permite conectar más de una interfaz (pocas o miles) a una sola IP (**RFC 3022**).
 - **IPv6:** Total direcciones IPv6: $2^{128}=3.40*10^{38}$ o $6.7*10^{17}$ direcciones por mm^2 de superficie de la tierra.

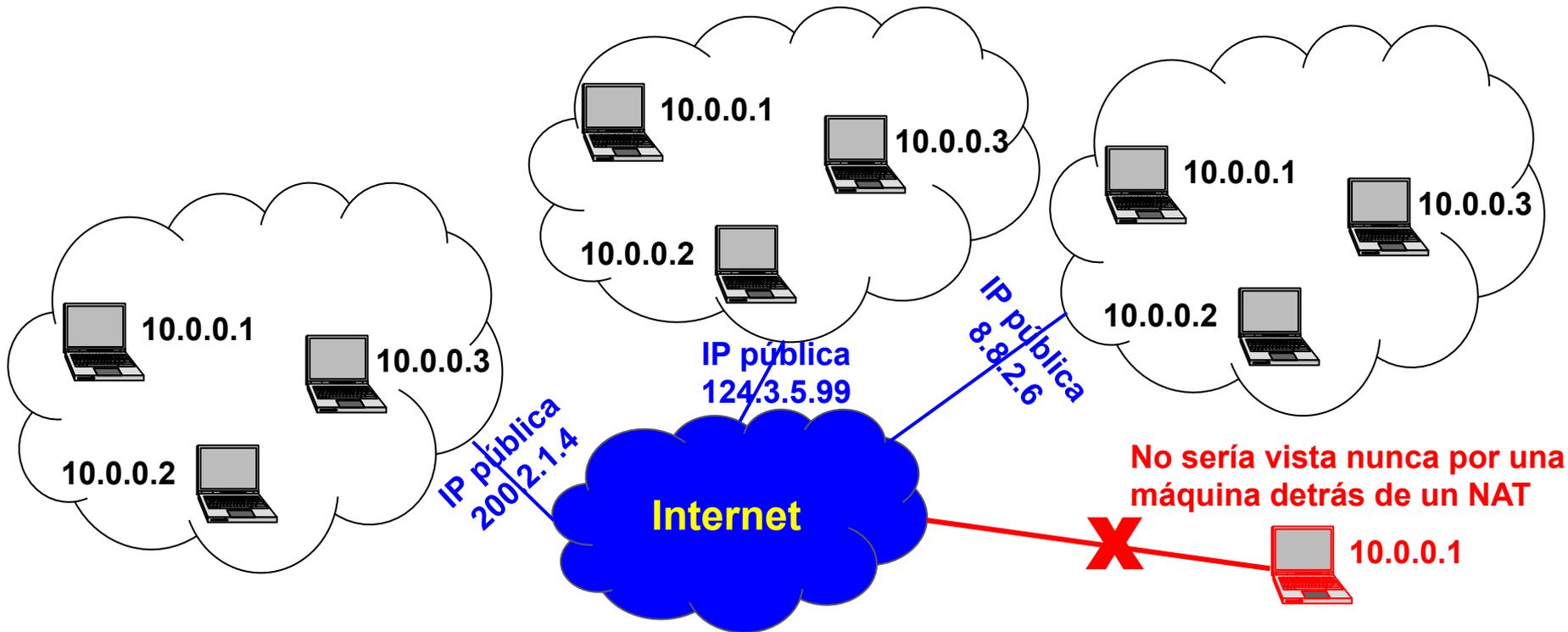
Protocolo IP: NAT (Network Address Translation) (Traducción de Dirección de Red)

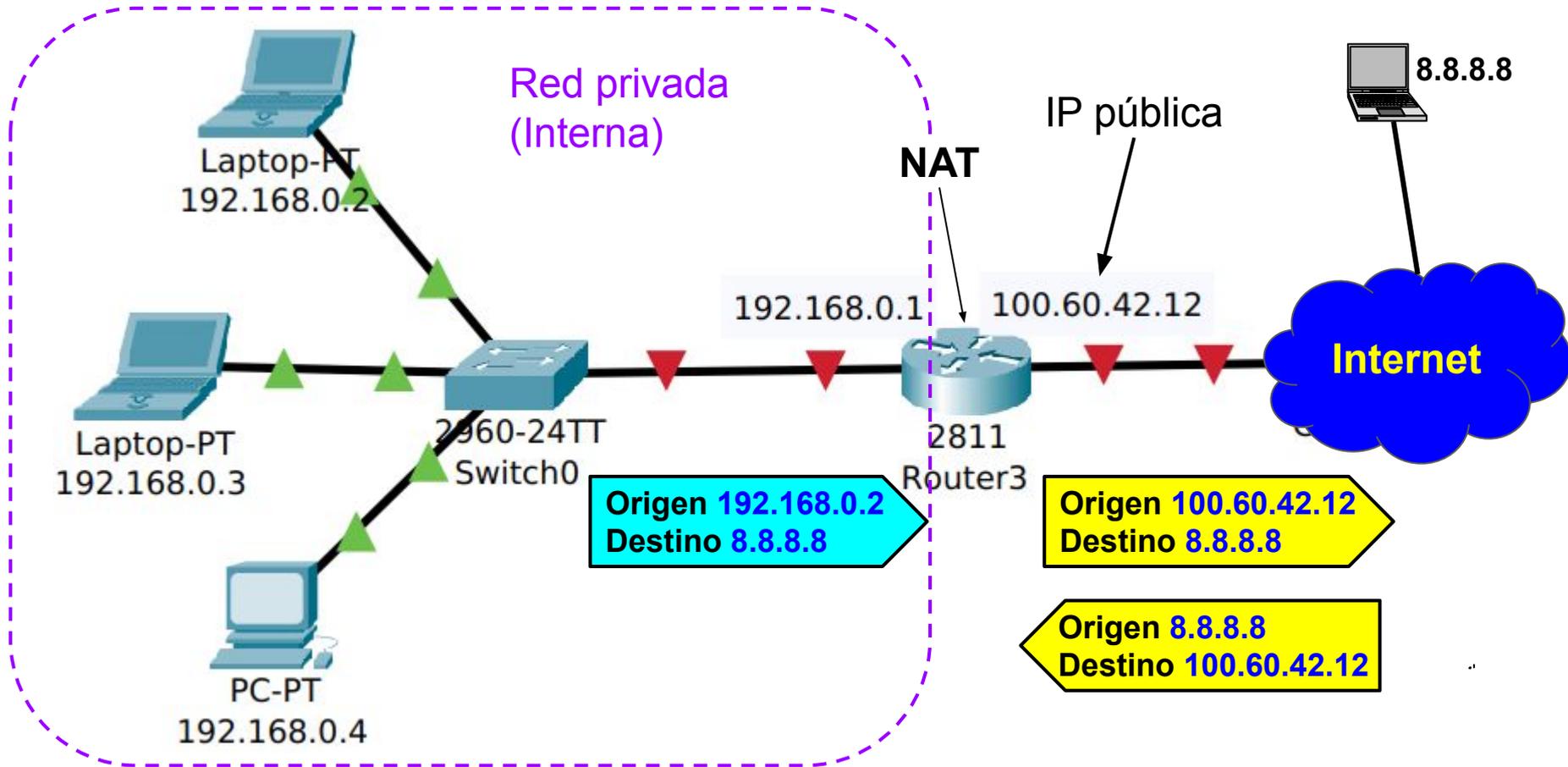
- Asignar a **una red** conectada a Internet una **única IP** (usualmente casas o empresas) llamada **IP pública**.
- La IP pública es **compartida** por **todas las computadoras** de la red.
- Dentro de la red, **cada computadora** tiene **una IP** que puede usar solo para **tráfico interno** en la red, llamada **IP privada** (RFC 1918).
- Si un paquete tiene que salir de la red cliente, su **IP privada se cambia por la IP pública**.
- **Una IP pública no puede usarse como IP privada.**
- Prefijos de direcciones IP que pueden utilizarse como **IP privada**:
 - **10.0.0.0/8** (10.0.0.0 - 10.255.255.255, 16M de direcciones).
 - **172.16.0.0/12** (172.16.0.0 - 172.31.255.255, 1M de direcciones).
 - **192.168.0.0/16** (192.168.0.0 - 192.168.255.255, 65k direcciones).
- **Una IP reservada para usarse como privada no puede usarse como pública**



Protocolo IP: NAT (Network Address Translation)

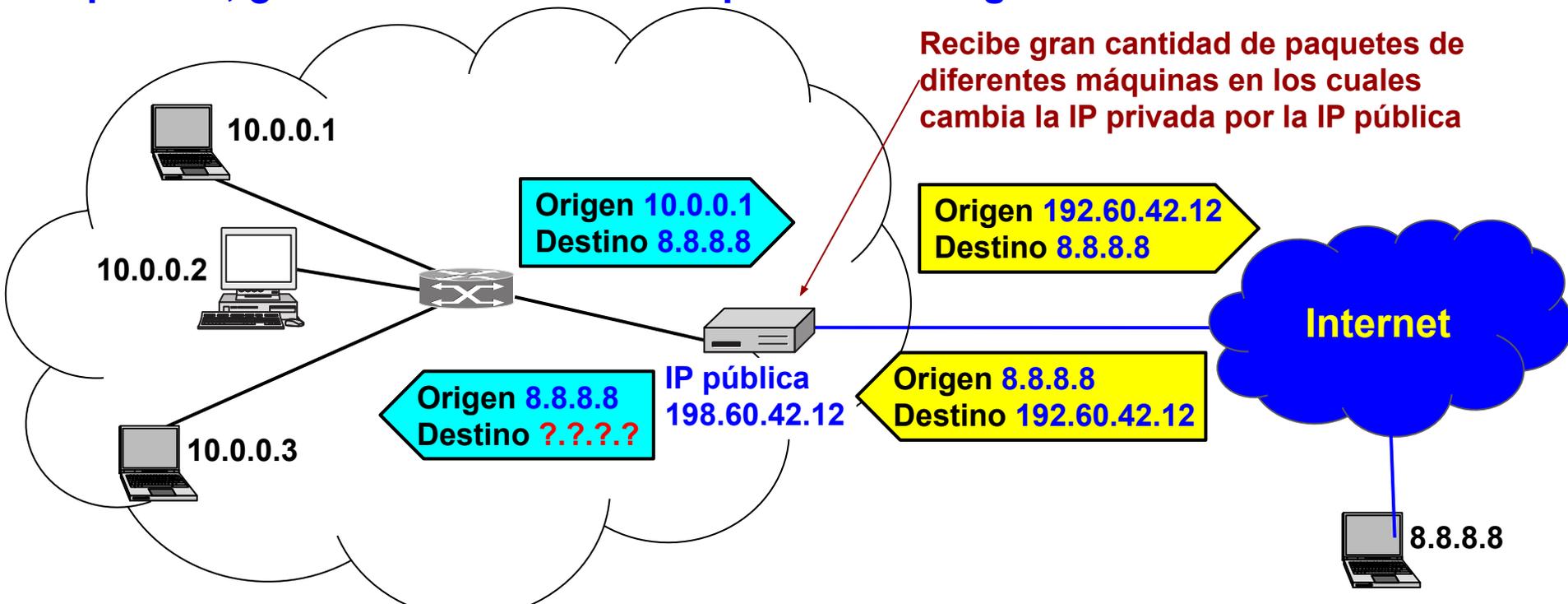
- Las **IP privadas** pueden **repetirse** en todas las redes privadas existentes.





Protocolo IP: NAT (Network Address Translation)

- Problema:** Cuando llega un paquete de respuesta, **tendrá como IP destino la IP pública, ¿Como sabe el NAT la IP privada de origen?**



Protocolo IP: NAT (Network Address Translation)

- **Solución: Se utiliza el campo puerto de origen TCP o UDP (capa transporte).**
 - Campo de 16 bits de los segmentos¹ generados por la capa de transporte.
 - Puerto origen: Identifica al proceso que genera el segmento TCP
 - Puerto destino: Identifica al proceso destino del segmento TCP.
- El NAT posee una “**tabla de traducciones de entrada**” con 65536 entradas.
 - Cada entrada de la tabla posee un **índice** y espacio para almacenar una **dirección IP** y un **puerto origen**.
- Se almacena en la tabla la dirección IP y puerto origen, y en el campo puerto origen se inserta el índice de la tabla donde se almacenó el IP y puerto.
- Se recalcula el CRC.

¹ Segmento: Nombre de las unidades de datos generados en la capa de transporte



IP origen	IP destino	CRC		Puerto Origen	Puerto Destino	
10.0.0.1	8.8.8.8	CRC		6000	80	

Paquete enviado dentro de la red privada.

IP pública	8.8.8.8	CRC		41	80	
------------	---------	-----	--	----	----	--

Paquete enviado fuera de la red privada.

8.8.8.8	IP pública	CRC		80	41	
---------	------------	-----	--	----	----	--

Paquete respuesta fuera de la red privada.

8.8.8.8	10.0.0.1	CRC		80	6000	
---------	----------	-----	--	----	------	--

Paquete respuesta dentro de la red privada.

Tabla de traducciones de entrada

Indice	IP privada origen	Puerto origen
....
41	10.0.0.1	6000

Protocolo IP: NAT: Desventajas, objeciones

- **Quebranta el modelo IP:** según IP, cada máquina conectada a Internet tiene un IP único. Con NAT puede hacer muchas máquinas con el mismo IP.
- **Una máquina detrás de un NAT no puede ser vista desde Internet** (solo puede llegarle una respuesta desde Internet si la máquina envió previamente un paquete de salida y sus datos se almacenaron en el NAT).
- **Si el NAT falla se pierden todos los paquetes desde el exterior destinados a la red privada** (por ejemplo: se pierden todas las conexiones TCP).
- **Requiere que el usuario utilice TCP o UDP** (protocolos de la capa de transporte con un campo de puerto).
- **Quebranta el principio de que una capa k no puede depender de la capa k+1, y mucho menos modificar campos de la capa k+1.**
- **Pero resuelve el problema del límite de usuarios que pueden acceder a Internet por agotamiento de direcciones IP** (la mayoría de los usuarios no necesitan una dirección IP, solo quieren acceder a Internet).
- **Seguridad:** Una máquina externa no puede llegar a una máquina con IP privada.

Carrier-grade NAT (CGNAT)

- También conocido como LSN (Large Scale NAT).
- Los clientes reciben IPs privadas desde los ISPs.
 - Permite a un ISP proveer Internet a un número grande de clientes con una cantidad reducida de IPs públicas.
- Se reservan IPs para ser utilizadas como IP privadas dentro de CGNATs (RFC 6598).
 - Rango: 100.64.0.0/10 (100.64.0.0 a la 100.127.255.255).



Temario

- Introducción.
- Congestión, reenvío de paquetes y calidad de servicio.
- IPv4
- ● **IPv6**
 - **Características. Encabezado. Encabezados de extensión.**
 - **Diferencias con IPv4.**
 - **Mecanismos de transmisión de IPv4 a IPv6.**
- Protocolos de control de Internet
- Conmutación basada en etiquetas (MPLS)
- Algoritmos de enrutamiento

IPv6

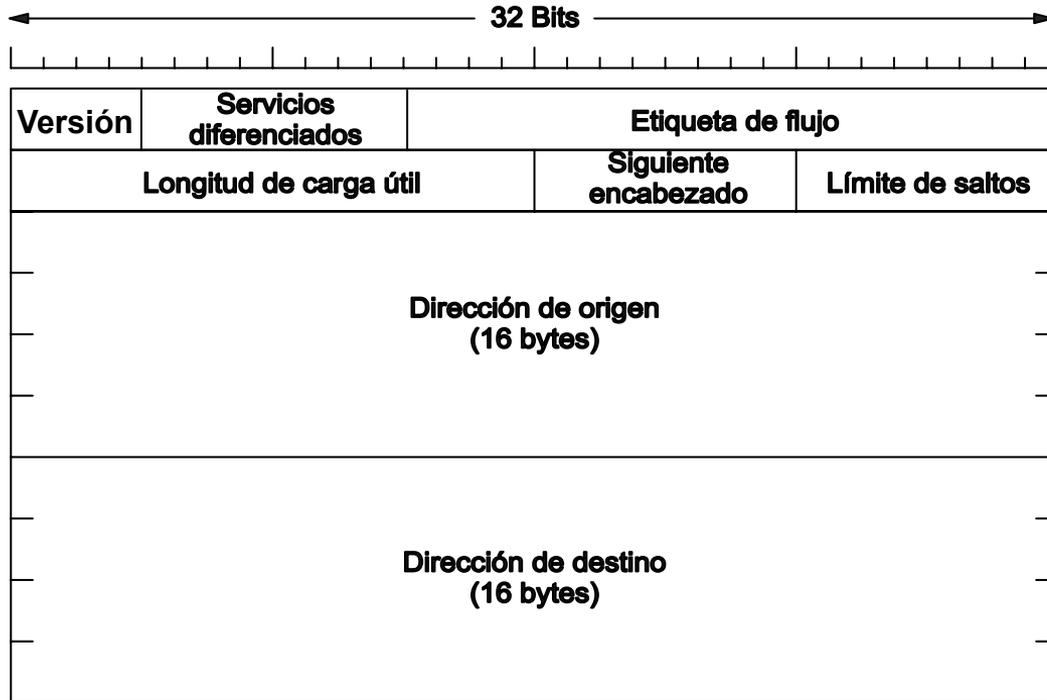
- Estándar desde 1998 (RFC 2460 - 2466).
- Características principales (algunas):
 - Campos de direcciones de **128 bits**¹ en lugar de los 32 de IPv4.
 - **Encabezado más simple** (7 campos en lugar de los 13 de IPv4) y de **tamaño fijo** (Su procesamiento es **más rápido**).
 - **Encabezados de extensión** en lugar de campos de opciones.
 - Esto permite que el encabezado tenga longitud fija.
 - **Mejoras en la seguridad.**
 - **Enrutamiento jerárquico y agregación de direcciones** (permite disminuir tamaño de tablas de ruteo).
 - Características mejoradas de **calidad de servicio**.
 - Muy importante para transmitir multimedia.

¹ $2^{128} = 3.40 \cdot 10^{38}$ o $6.7 \cdot 10^{17}$ direcciones por mm^2 de superficie de la tierra

IPv6

- Características principales (continuación):
 - Etiquetado de paquetes como pertenecientes a un **flujo** que requiere tratamiento especial (importante para video en tiempo real).
 - **Jumbogramas**: paquetes de hasta 4GB.
 - **No se fragmenta**: El tamaño del paquete se elige en el origen.
- No hay código para detección de errores.
 - Se confía en que la suma de verificación se calcula tanto en capa de enlace y en la de transporte.
 - Las redes actuales son en general muy confiables.
 - Quitar la suma de verificación aumenta el desempeño (no hay que recalcular la suma de verificación en cada salto).

Encabezado IPv6



No posee campos relacionados con:

- Fragmentación.
- Opciones (Puede poseer encabezados adicionales) .
- Longitud del encabezado (tamaño fijo).
- Suma de verificación.
- Identificación de paquete (No necesario si no hay fragmentación).

Encabezado IPv6: Campos

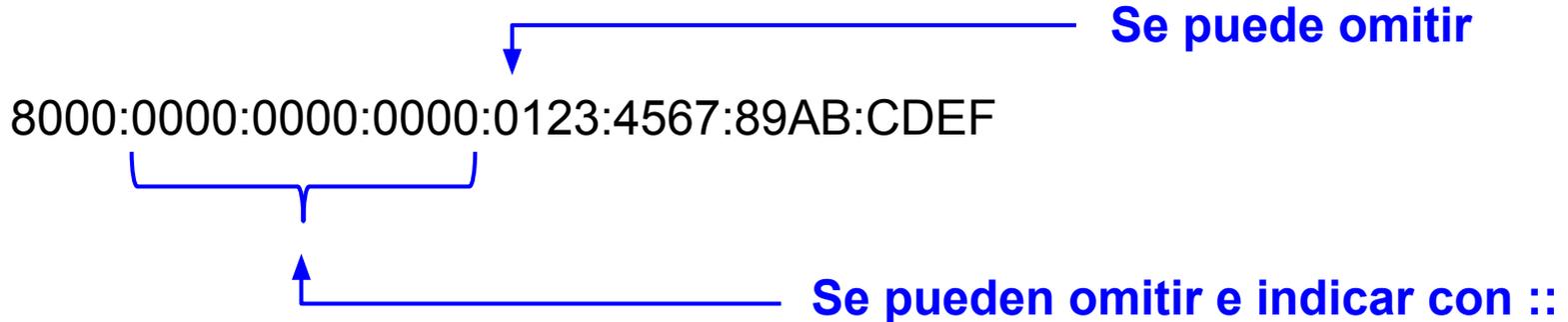
- Versión: Indica que es IPv6 (Los enrutadores necesitan saber si es IPv4 o IPv6).
- Servicios diferenciados: Identifica diferentes calidades de servicio o tipo de tráfico (Como IPv4).
- Etiqueta de Flujo: permite marcar grupos de paquetes como pertenecientes a un flujo, para que sean tratados de la misma manera (tengan los mismos requerimientos). Por ejemplo: baja latencia.
- Siguiendo encabezado:
 - El paquete IPv6 puede tener encabezados adicionales o de extensión (hay distintos tipos de encabezados de extensión).
 - Este campo puede indicar:
 - El tipo del siguiente encabezado de extensión (si lo hay).
 - Si no hay encabezado de extensión, indica el protocolo del datagrama de la capa de transporte.

Encabezado IPv6: Campos

- Límite de saltos: Evita que el paquete viva por siempre.

Notación de las direcciones IPv6

- Los bit se agrupan en 8 grupos de 4 números hexadecimales ($8 \cdot 4 \cdot 4 = 128$).

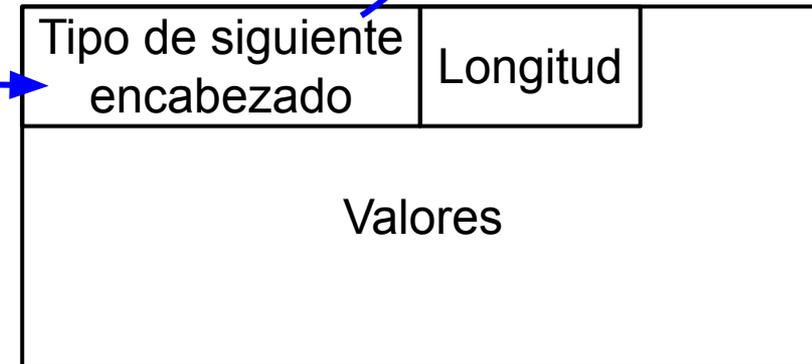


La dirección anterior simplificada quedaría como: 8000::123:4567:89AB:CDEF

Encabezados de Extensión

- Permiten agregar **opciones adicionales**.
- No son obligatorios, pero si están, su presencia se debe indicar en el campo “Siguiete Encabezado”.
- Algunos tienen tamaño fijo, otros tienen tamaño variable.
- Formato:

Versión	Servicios diferenciados	Etiqueta de flujo	
	Longitud de carga útil	Siguiete encabezado	Límite de saltos
	Dirección de origen (16 bytes)		
	Dirección de destino (16 bytes)		

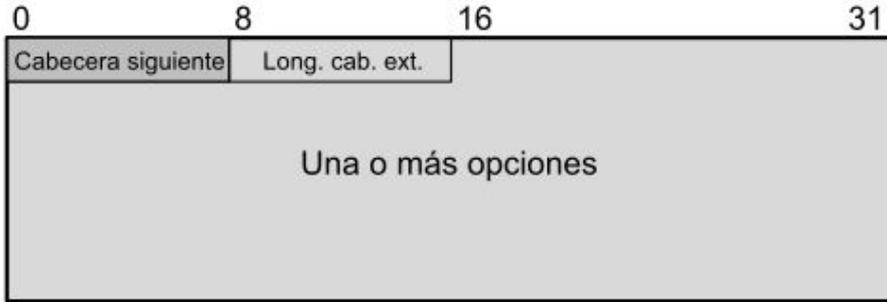




- **Tipo** (1 byte): indica el tipo de encabezado de extensión. Indicado en el encabezado anterior.
 - Los **dos primeros bits indican que hacer a los enrutadores que no sepan cómo procesar la información:**
 - Omitir la opción
 - Descartar el paquete enviando un mensaje ICMP (Protocolo de mensajes de control de Internet, se verá en esta unidad).
 - Descartar el paquete sin enviar mensajes ICMP.
- **Longitud** (1 byte): Indica la longitud del campo Valor.
- **Valor** (255 bytes).

Algunos tipos de encabezados de extensión

Encabezado de extensión	Descripción
Opciones salto por salto.	Información diversa para los enrutadores.
Opciones de destino.	Información adicional para el destino.
Enrutamiento.	Lista informal de los enrutadores a visitar.
Fragmentación.	Manejo de fragmentos de datagramas.
Autenticación.	Verificación de la identidad del emisor.
Carga útil de seguridad cifrada.	Información sobre el contenido cifrado.



(a) Cabecera de opciones salto a salto;
cabecera de opciones para el destino



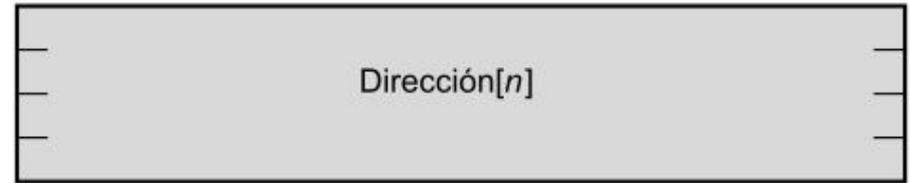
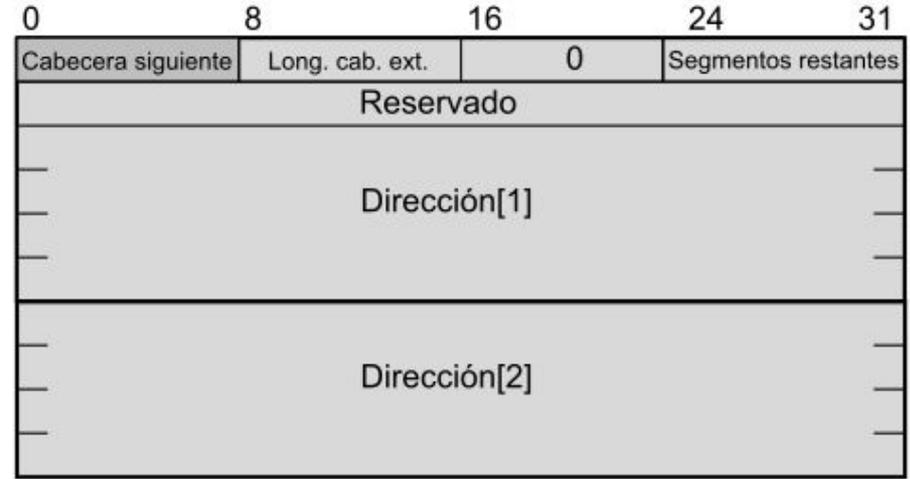
(b) Cabecera de fragmentación

Reservado y Res: reservado uso futuro.

M: Más fragmentos

Identificador: ID paquete original

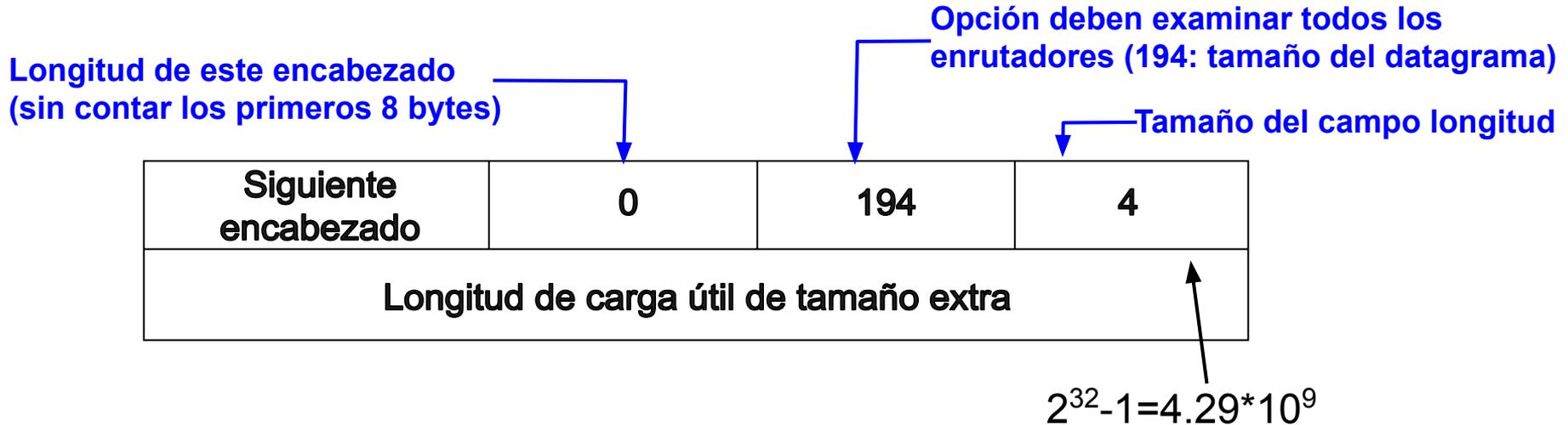
Segmentos restantes: número de nodos intermedios
explícitamente contenidos en la lista que falta visitar.



(d) Cabecera de encaminamiento tipo 0

Ejemplo: Envío de **paquetes de más de 64 Kb** o **jumbogramas**

- Utilizados en computación de alto rendimiento o video.
- Encabezado de extensión **Opciones salto por salto**.
 - Indica opciones que deben examinar todos los enrutadores a lo largo de la ruta.



Transición de IPv4 a IPv6

- **Mecanismos:**
 - **Tunelización** entre redes (o computadoras individuales) IPv6 conectadas por redes IPv4.
 - **Doble pila**: Cada host y router posea pilas IPv4 e IPv6.
 - **Traducción**: Para comunicar una máquina que solo emplee IPv4 con una que solo emplee IPv6.
- Estadísticas de adopción de Google:
 - <https://www.google.com/intl/en/ipv6/statistics.html> (se sugiere ver).



Temario

- Introducción.
- Congestión y calidad de servicio.
- IPv4
- IPv6
- ● **Protocolos de control de Internet (ICMP), ARP y DHCP.**
- Conmutación basada en etiquetas (MPLS)
- Algoritmos de enrutamiento

Protocolos de Control de Internet: ICMP (Internet Control Message Protocol)

- Aplicaciones:
 - Informar al emisor si ocurre un **error**.
 - Permitir obtener información sobre el **funcionamiento** de la red.
- Se encapsula en paquetes IP.

Protocolo ICMP: Ejemplos de mensajes

- **Destination unreachable** (Destino inaccesible):
 - Cuando el destino de un paquete no puede localizarse.
 - Cuando un paquete con el bit DF (Don't Fragment) seteado llega a una red con tamaño de paquetes más pequeño.

Protocolo ICMP: Ejemplos de mensajes

- **Echo and echo reply** (Eco y respuesta al eco): Mensaje para ver si un destino es alcanzable y está “vivo”. El emisor envía un mensaje “eco” y espera como respuesta el mensaje “respuesta al eco”.
 - Empleado por la **aplicación ping**.
 - Sugerencia: ver “ping --help” y “man ping”.
- **Time exceeded** (Tiempo excedido): Se envía cuando el campo tiempo de vida (o número de saltos máximo) de un paquete llega a 0.
 - Usado por **traceroute** (aplicación que encuentra todos los enrutadores hacia un destino).
- **Source quench** (Ralentización de fuente): Mensaje que se envía a un host para indicarle que está enviando demasiados paquetes.
 - Se esperaba que sería usado para regular congestiones. Pero hoy día la congestión se trata en la capa de transporte.

Protocolo ICMP: Ejemplos de mensajes

- **Redirect** (Redireccionar): Cuando un enrutador detecta un paquete mal enrutado, o la existencia de un camino más corto al destino final, envía este mensaje al emisor para que actualice la tabla de ruteo.
- **Parameter problem** (Problema de parámetros): Hay un valor ilegal en un parámetro del encabezado.
- **Timestamp request/reply** (Estampa de tiempo, Petición/respuesta): Similar a eco, pero con estampa de tiempo.
- **Router advertisement/solicitation** (anuncio de enrutador/solicitud de enrutador): usados por los host para buscar enrutadores.
- Otros: www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

Protocolo ARP (Address Resolution Protocol) (Protocolo de Resolución de Direcciones)

- **IP toma decisiones de ruteo**: decide cual es el host o enrutador inmediato al cual enviar un paquete para que llegue al destino final.
 - Si hay varias interfaces, decide la IP de la interfaz de salida.
- Una vez que IP conoce el destino inmediato (destino final o enrutador intermedio) IP entrega el paquete a la **capa de enlace** para que haga el envío.
- **Problema**: La capa de enlace **NO emplea direcciones IP**. En una red por **difusión** (Ethernet o IEEE 802.11), **se necesita conocer la dirección MAC del destino inmediato**.
- **ARP**: protocolo que asocia direcciones IP con direcciones MAC:



Protocolo ARP

Direcciones IP	Direcciones MAC
<ul style="list-style-type: none">● Configurables, jerárquicas.● Dependientes de la red, si la máquina se mueve a otra red, la dirección IP cambia.	<ul style="list-style-type: none">● Fijas y grabadas de fábrica para cada Interfaz.● Si la máquina se mueve a otra red, la dirección MAC NO cambia.

- IP decide el destino inmediato:
 - Si el destino final está en **la misma red**, el destino inmediato será el **destino final**.
 - Si el destino final está en **otra red**, el destino inmediato será un **router**.
- Funcionamiento de ARP:
 - Cada máquina posee una **tabla** que asocia direcciones IP a direcciones MAC.
 - Si se conoce la dirección MAC de destino, la capa de enlace envía el paquete al destino que **IP decidió**.

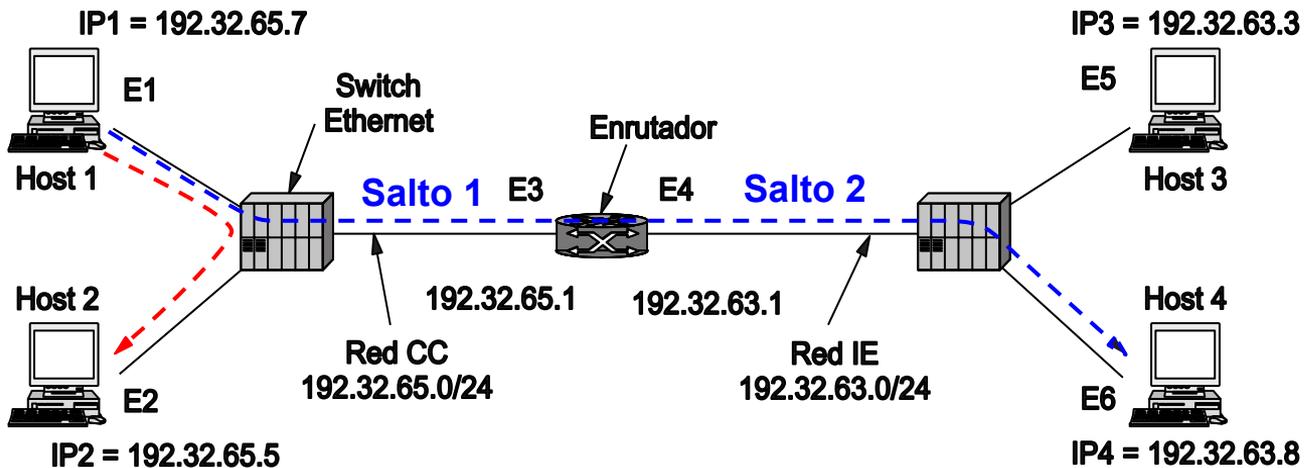


Funcionamiento de ARP (continuación):

- Si no se conoce la dirección MAC de destino:
 - El origen envía una pregunta por difusión (Ethernet o 802.11) preguntando: ¿Quién posee tal dirección IP?
 - Todas las máquinas de la red **reciben el paquete** y **verifican si es su IP**
- La máquina **dueña de la IP**, responde **enviando su dirección MAC**.
 - La máquina origen ya puede enviar el paquete.
- La información queda **almacenada** para **comunicaciones futuras**.
- La máquina origen de la consulta **envía su propia IP** para que el destino la almacene en su tabla ARP.
- Todas las máquinas que escuchan la consulta y la respuesta ARP, y almacenan las direcciones IP y MAC de las máquinas origen y destino en sus tablas ARP.
- Las asociaciones dirección IP - dirección MAC **expiran cada cierta cantidad de minutos**, para permitir adaptarse a cambios en la red.
- Cuando una máquina se **conecta**, envía **peticiones ARP buscándose a si misma**. Esto permite que otras máquinas agenden su IP y dirección MAC.



Protocolo ARP (Address Resolution Protocol) (Repaso de rutero)



	N° de Saltos	Salto	IP origen	IP destino	Eth origen	Eth destino
IP1 a IP2	1	1°	IP1	IP2	E1	E2
IP1 a IP4	2	1°	IP1	IP4	E1	E3
		2°	IP1	IP4	E4	E6

Protocolo DHCP (Dynamic Host Configuration Protocol) Protocolo de Configuración Dinámica de Host

- ¿Cómo obtienen direcciones IP las computadoras?
 - **Asignación estática** (Las asigna manualmente un administrador).
 - **Asignación dinámica** (automática) mediante DHCP (RFC 2131 y 2132)
- **Servidor DHCP**: es el encargado de asignar direcciones IP
- Al **encender** una máquina, no posee dirección IP.
 - La máquina difunde una petición de IP o **paquete DHCP Discover** (incluye la dirección MAC de la máquina origen).
 - El **servidor DHCP** le asigna una **dirección IP libre** y se la envía a la máquina a través de un paquete **DHCP offer**.
 - La asignación dura un tiempo determinado. Luego de ese tiempo, la máquina debe enviar una **petición de renovación** para conservar la IP.
 - DHCP **configura otros parámetros** (máscara de red, servidores DNS¹, etc.)

¹ Protocolo de la capa de aplicación. Se verá en la unidad 6



Temario

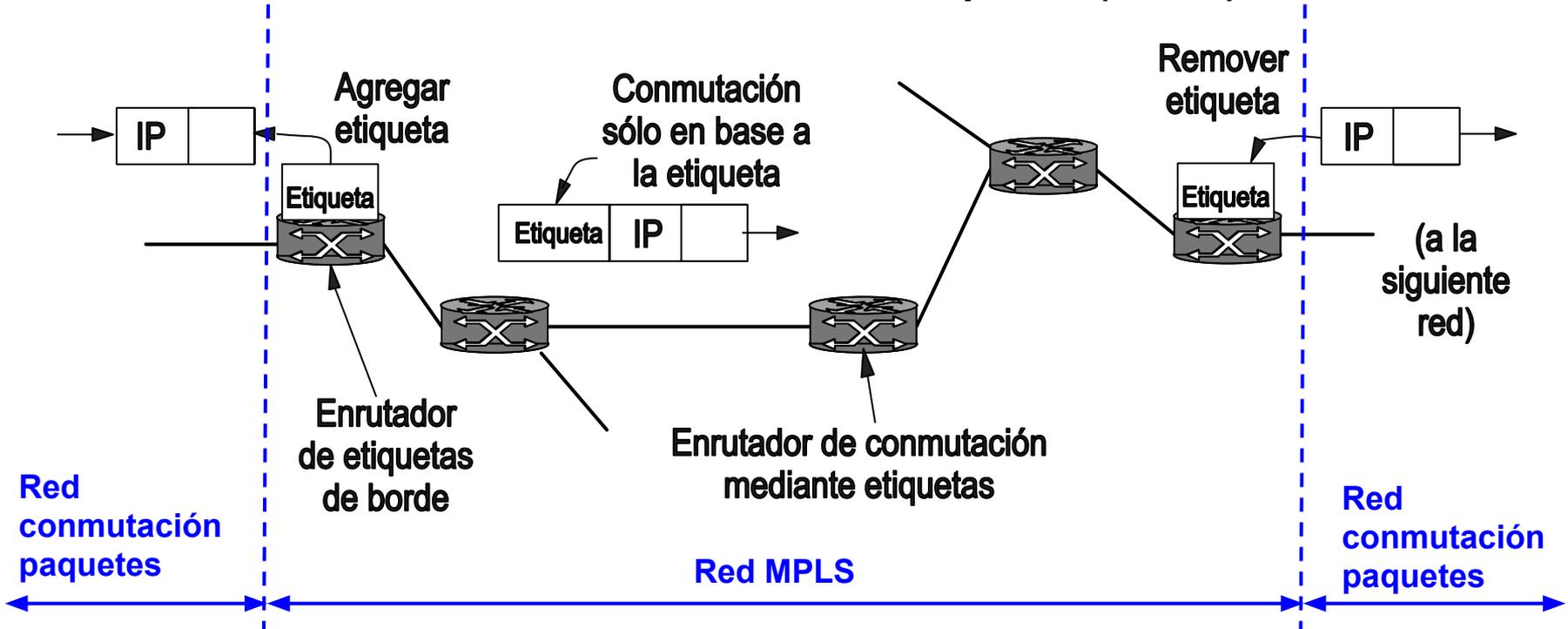
- Introducción.
- Congestión y calidad de servicio.
- IPv4
- IPv6
- Protocolos de control de Internet
- ● Conmutación basada en etiquetas (MPLS)
- Algoritmos de enrutamiento

Conmutación mediante etiquetas (MPLS)

- MPLS (MultiProtocol Label Switching) o conmutación mediante etiquetas multiprotocolo (RFC 3031).
- Protocolo **orientado a conexión** (circuitos virtuales) ¹.
 - Permite a los ISP ofrecer calidad de servicio mediante selección de los caminos que los paquetes siguen.
- Basado en **tunelización**: Cada paquete (puede ser IP u otro protocolo) se encapsula añadiendo un encabezado que contiene una etiqueta.
- **El ruteo que hace en base a esas etiquetas** o circuitos virtuales.
- Puede transportarse en otros protocolos de capa de enlace, por ejemplo PPP.
- Sucesor de Frame Relay y ATM.

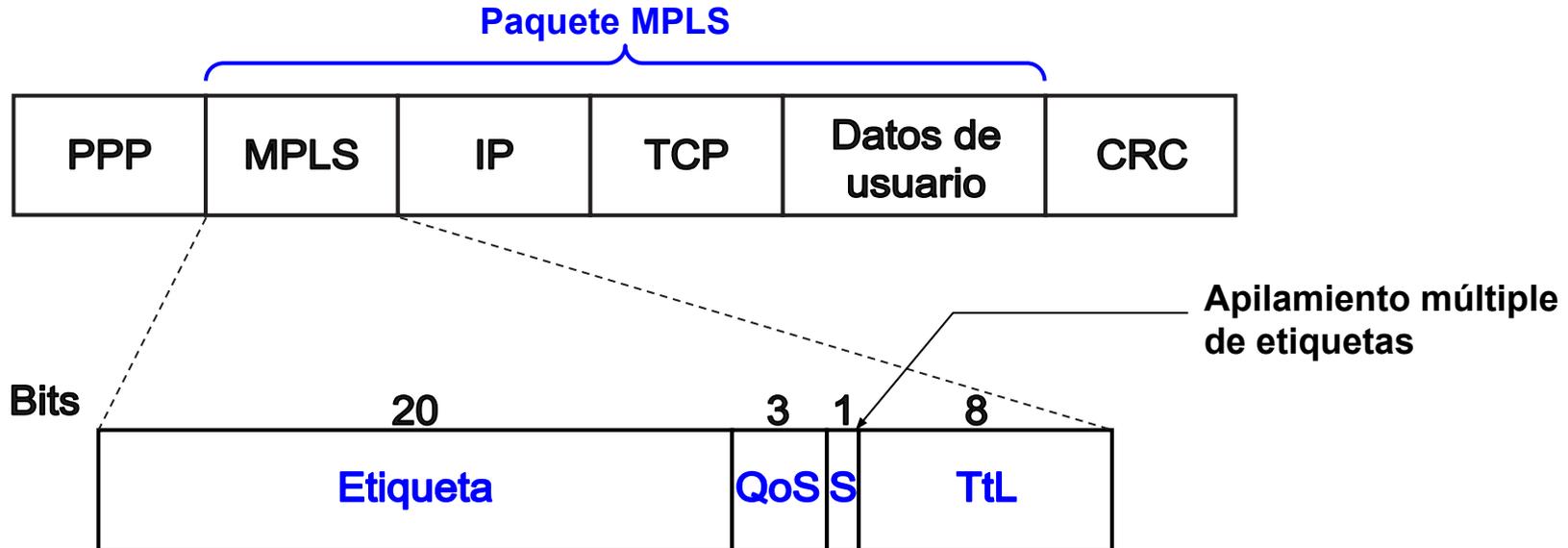
¹ Repaso (ver filmina 12): Requiere una negociación previa, en la cual se **preestablece la ruta** por la cual circularán los paquetes. Los ruteadores poseen tablas en las que se asocian circuitos virtuales (o etiquetas) de entrada con circuitos virtuales (o etiquetas) de salida.

Conmutación mediante etiquetas (MPLS)



Conmutación mediante etiquetas (MPLS)

- MPLS no es de capa de enlace (varios saltos, no un solo enlace) ni de red (depende de IP u otro protocolo de red). Se dice que es **capa 2.5**



Conmutación mediante etiquetas (MPLS)

- Características especiales:
 - Permite **agregación** de rutas.
 - Varios flujos que terminan en un mismo enrutador pueden utilizar la misma etiqueta.
 - Permite **múltiples niveles** (un paquete puede llevar varias etiquetas MPLS).
- Ventaja:
 - **Permite a un ISP brindar calidad de servicio.**



Temario

- Introducción.
- ● **Congestión y calidad de servicio.**
- IPv4
- IPv6
- Protocolos de control de Internet
- Conmutación basada en etiquetas (MPLS)
- Algoritmos de enrutamiento

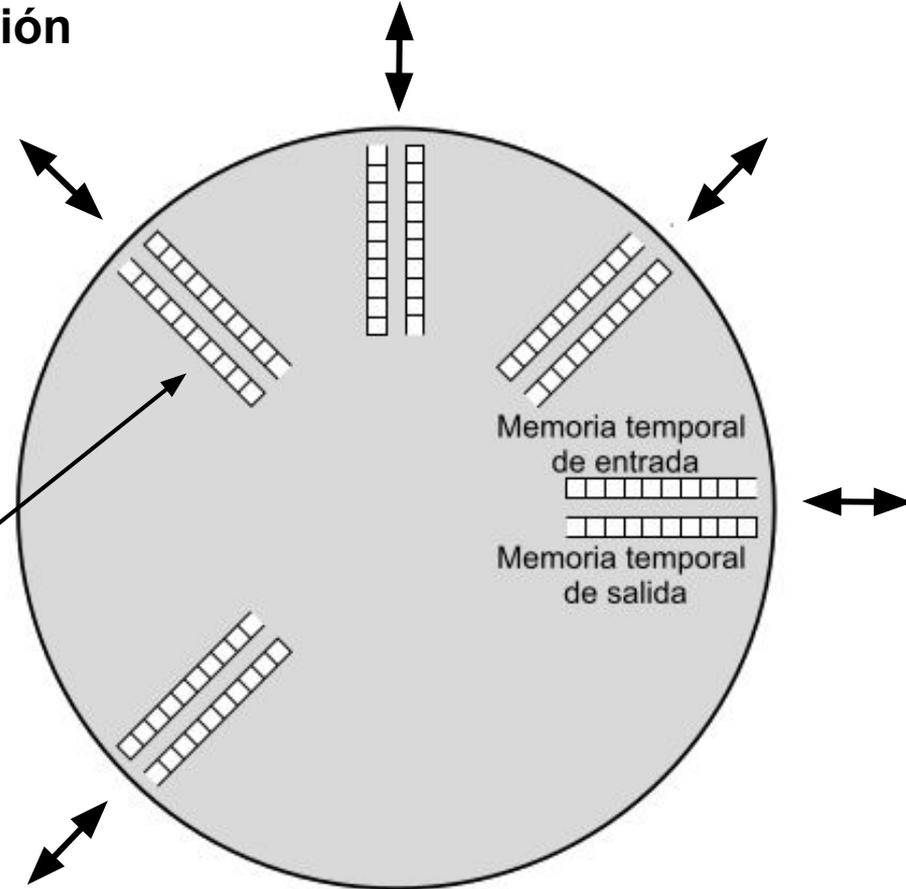


Algoritmos Control de Congestión

Congestión: Una red (o parte de ella) recibe más tráfico del que puede manejar.

- Comienzan a **llenarse los buffers** de los enrutadores.
- **Incremento de latencia.**
- **Incremento de paquetes perdidos** (por saturación de buffers o latencia muy grande), **duplicados o reenviados.**

Pueden existir varias colas para proporcionar calidad de servicio



Algoritmos Control de Congestión

Métodos de control de congestión en la capa de red (del más lento al más veloz)

- **1) Aprovisionamiento de la red**: mejorar equipamiento por el cual transita carga alta. **No es dinámico.**
 - Agregar memoria (**por experimentos: agregar memoria incrementa la cantidad de paquetes reenviados y duplicados**).
- **2) Enrutamiento consciente** del tráfico: Los routers reconocen congestión y desvían el tráfico por otras rutas.
 - Se ponderan los enlaces en función de sus capacidades y carga.
 - Parámetros fijos: Ancho de banda.
 - Parámetros variables: Latencia, carga.
 - **Puede congestionar otras redes o producir oscilaciones.**

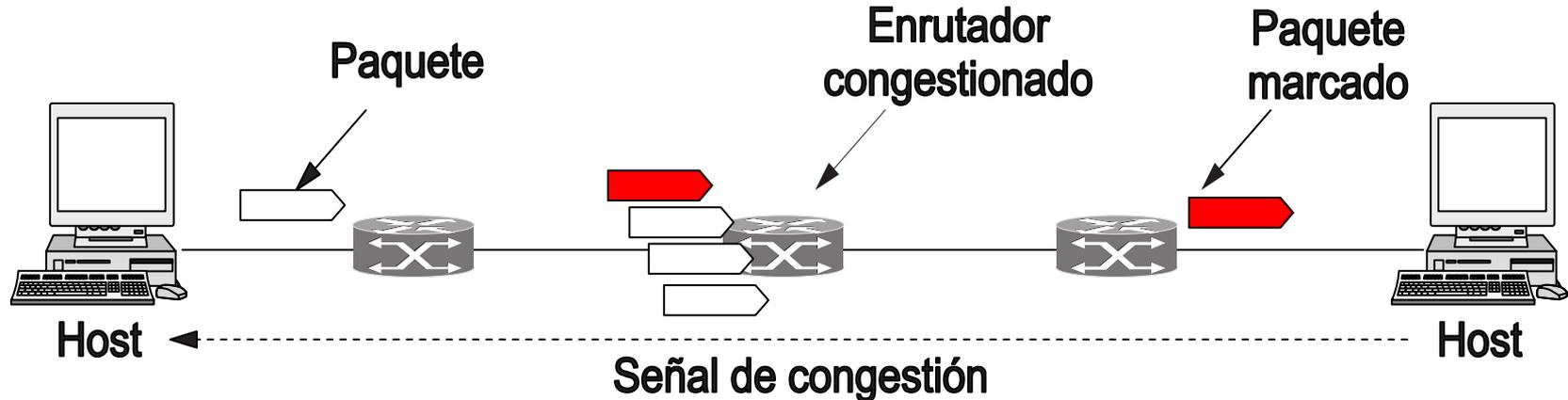
Algoritmos Control de Congestión (continuación...)

- **3) Control de admisión:** rechazar nuevas conexiones de circuitos virtuales si la red no los va a poder manejar.
 - **Aplicable solo en servicios con conexión.**
- **4) Regulación del tráfico:** Los ruteadores **detectan** una congestión inminente o ya se está produciendo y envían **mensajes** a las fuentes de datos para que disminuyan el tráfico que generan cuando una congestión es inminente.
 - **Primer paso: Detección** de congestión: medición de parámetros claves (paquetes en los buffers de los enrutadores, etc.).
 - **Segundo paso: Notificación:**
 - Envía **notificaciones de congestión** a los emisores que generan el problema para que reduzcan su velocidad de transmisión. **Genera más paquetes.**
 - **Etiquetar** paquetes: Mecanismo **ECN** (Explicit Congestion Notification) Usado en IP y TCP, RFC 3168 (ver filmina siguiente).

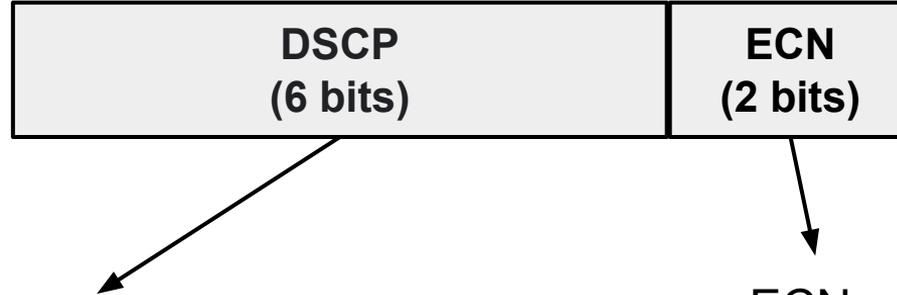
Algoritmos Control de Congestión (continuación...)

Algoritmo ECN (marcado de paquetes)

- Trabaja en **conjunto con TCP**.
- **Etiquetar** los paquetes que **producen la congestión** y dejar que sigan su camino.
- El destinatario recibirá los paquetes etiquetados y enviará sus **acuses de recibo TCP** indicando al emisor el problema.



Campo servicios diferenciados (IPv4v e IPv6):
A partir de la RFC 2474 (1998).



DSCP (Differentiated Services Code Point):
Códigos que indican diferentes calidades de
servicios. Definidos por IANA

ECN:
00: ECN no soportado
01 o 10: ECN soportado
11: Congestión



Algoritmos Control de Congestión (continuación...)

- **5) Desprendimiento de carga**
 - **Descartar paquetes:** Si se llenan los buffers de los enrutadores, inevitablemente los paquetes comenzarán a **perderse**.
- **Desprendimiento de carga y calidad de servicio:** Los paquetes a descartar dependen de la aplicación:
 - Transferencia de archivos: se descartan los paquetes más nuevos.
 - Para no obligar al receptor a almacenar en búffers paquetes nuevos hasta que los viejos descartados lleguen.
 - Tiempo real (voz, video): Los más viejos.
 - En tiempo real, un paquete fuera de tiempo no sirve.
- Funciona bien en combinación con TCP.

Calidad de Servicio

- Algunas aplicaciones requieren un **desempeño determinado** de la red para funcionar:
 - Parámetros importantes (cada aplicación requiere mantener uno o varios parámetros dentro de valores límites):
 - Ancho de banda (en bps)
 - Latencia
 - Variación de la latencia
 - Pérdida de paquetes
- **Solución más simple: sobreaprovisionamiento** (overprovisioning), construir la red de manera que sus prestaciones puedan tolerar la peor situación sin sufrir congestión ni otros tipos de problemas.
 - **Problemas:**
 - costo elevado
 - La mayor parte del tiempo habría desaprovechamiento de recursos.

Calidad de Servicio requerida según aplicaciones

Aplicación	Ancho de banda	Retardo	Variación del retardo	Pérdida
Correo electrónico.	Bajo	Bajo	Baja	Media
Compartir archivos.	Alto	Bajo	Baja	Media
Acceso a Web.	Medio	Medio	Baja	Media
Inicio de sesión remoto.	Bajo	Medio	Media	Media
Audio bajo demanda.	Bajo	Bajo	Alta	Baja
Video bajo demanda.	Alto	Bajo	Alta	Baja
Telefonía.	Bajo	Alto	Alta	Baja
Videoconferencias.	Alto	Alto	Alta	Baja

Calidad de servicio en la capa de Red

- Dos métodos para ofrecer calidad de servicio:
 - **Calidad de servicio basada en flujo o servicios integrados**
 - Reservar recursos (ancho de banda, espacio en buffers, etc) a lo largo de la ruta.
 - Útil en servicios orientados a conexión.
 - **Calidad de servicio basada en clase o servicios diferenciados**
 - Clasificar los paquetes en diferentes tipos según la aplicación y según los **Acuerdos de Nivel de Servicio** o SLA (acuerdo entre los ISP y los clientes).
 - Útil en servicios sin conexión.

Calidad de Servicio basada en clase

- También llamados “**servicios diferenciados**”.
- A cada paquete se le asigna una “**clase**” mediante un campo en su encabezado.
 - Campo DSCP: 6 bits. Hasta 64 clases.
- Los enrutadores **tratan cada paquete** según la **clase**. Según la clase los routers deciden:
 - Que paquete enviar primero (prioridades para el envío).
 - Los paquetes se almacenan en diferentes colas (buffers) según su prioridad.
 - Que paquete tienen mayor o menor probabilidad de ser descartado ante una congestión.
- Los ISPs pueden definir sus propias clases.
- Para permitir **interoperabilidad**, la **IANA define varias clases**.

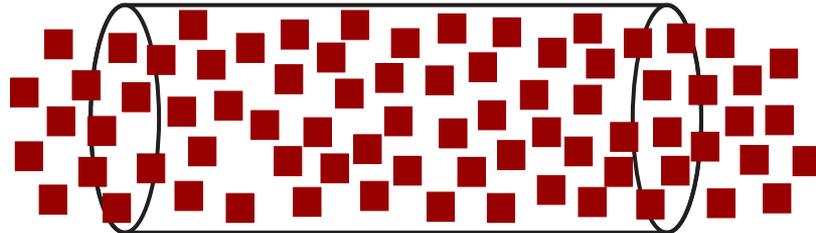
Calidad de Servicio basada en clase: reenvío expedito

- Clasificación en **Paquetes expeditos** (parámetros temporales con importantes) o **Paquetes regulares**. (Códigos DSCP: 101110 y 101100)
- Los enrutadores, para cada línea de salida, **tienen dos colas**, una para paquetes regulares y otra para paquetes expeditos.
 - La cola para paquetes expeditos tienen prioridad.

**Paquetes
expeditos**



**Paquetes
regulares**



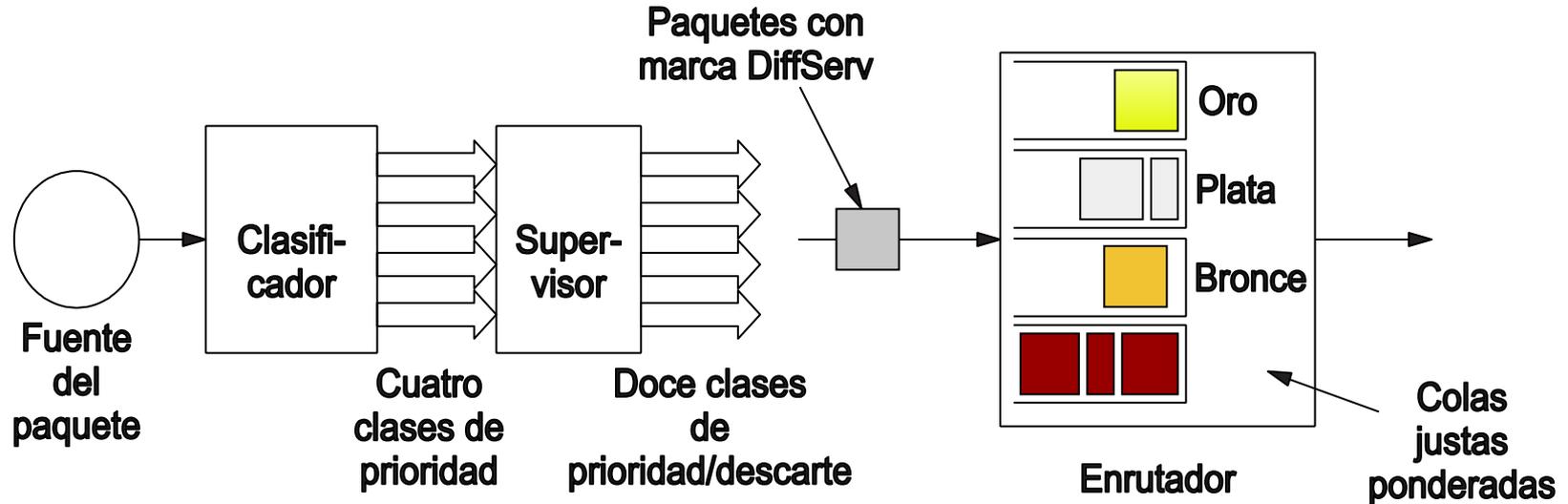
Calidad de Servicio basada en clase: reenvío asegurado

- Se definen cuatro clases de prioridades para los paquetes: **oro**, **plata**, **bronce** y **regular** (RFC 2597).
 - Las clases definen que paquetes tendrán **mayor prioridad** para ser reenviados en un **enrutador justo ponderado**.
 - Para cada clase, se definen **3 probabilidades** de descarte en caso de **congestión**.

Nota: los algoritmos que deciden que paquetes descartar son complejos. Toman decisiones en función de la clase de los paquetes, el tipo de tráfico (expedito o regular), los patrones de tráfico (ráfagas pequeñas, ráfagas extensas, etc).

Calidad de Servicio basada en clase: reenvío asegurado

- El enrutador de entrada puede limitar los paquetes con prioridades altas.



Temario

- **Introducción.**
- **Congestión, reenvío de paquetes y calidad de servicio.**
- **IPv4**
- **IPv6**
- **Protocolos de control de Internet**
- **Conmutación basada en etiquetas (MPLS)**
- ● **Algoritmos de enrutamiento:**
 - **Principio de optimización**
 - **Tipos de algoritmos de optimización**
 - **Enrutamiento jerárquico**
 - **Protocolos de Ruteo intradominio**
 - **Protocolos de Ruteo interdominio**

Interconexión de Redes: Enrutamiento en una internet



Concepto importante

- **Sistema Autónomo** (AS: Autonomous System): Red o grupo de redes que posee una **política** de enrutamiento propia e independiente:
 - Suele ser la red o red de redes de una organización. Todos los enrutadores suelen usar el mismo protocolo de encaminamiento.
 - Ejemplo de AS: Red de un ISP, Red de una Universidad, Red de grandes empresas (La UNCuyo es un AS).
 - **Las direcciones IP de red se asignan a AS.**
 - Internet es una gran colección de AS.
- Tipos de protocolos de enrutamiento:
 - Protocolos de enrutamiento **intradominio** o protocolo de puerta de enlace interior (RIP, OSPF, IS-IS, muchos otros propietarios), usado dentro de un AS.
 - Protocolos de enrutamiento **interdominio** o protocolo de puerta de enlace exterior (BGP: Border Gateway Protocol), usado para conectar AS.

Algoritmos y protocolos de Enrutamiento

- Toma la decisión del **camino que seguirá un paquete** para ir del origen al destino final (**arma y mantiene tablas de ruteo**).
- Tipos:
 - Algoritmos de enrutamiento **no adaptativo** o **estático**: Las rutas se calculan por adelantado.
 - Algoritmos de enrutamiento **adaptativo** o dinámico: Las rutas se deciden en función de mediciones o estimaciones de tráfico y topologías actuales.
- **Son algoritmos distribuidos.**
- Emplea conceptos de: teoría de grafos, electrónica (ruidos, latencias) y matemática.

Métrica de distancia

- **Métricas de “distancia”:**
 - **Número de saltos.** Fácil de medir. (redes cableadas).
 - **Distancia en metros o km.** Redes inalámbricas (Necesidad de algoritmos de posicionamiento).
 - **Latencia.** Medida con paquetes de prueba (se envían peticiones de eco y se mide el tiempo que tarda en volver la respuesta).
 - **Ancho de banda.**
 - **Trafico promedio.**
 -
- En general la distancia es una **función ponderada de varias de estas métricas.**



Ejemplos de Protocolos de enrutamiento Intradominio: RIP (Routing Information Protocol)

- Principal protocolo de ARPANET en sus comienzos.
- En todo algoritmo de ruteo: Al agregarse una red o ruta, el algoritmo lo anuncia a sus vecinos (mensajes Hello).
- Métricas: Número de saltos.
- Algoritmo de ruteo del tipo **vector de distancia**:
 - Cada router comparte toda su tabla de ruteo con los vecinos inmediatos.
 - La información se comparte periódicamente.
- Varias versiones: RIPv 1 para IPv4 con direccionamiento con clase, RIPv 2 para IPv4 sin clases, y RIPng para IPv6.



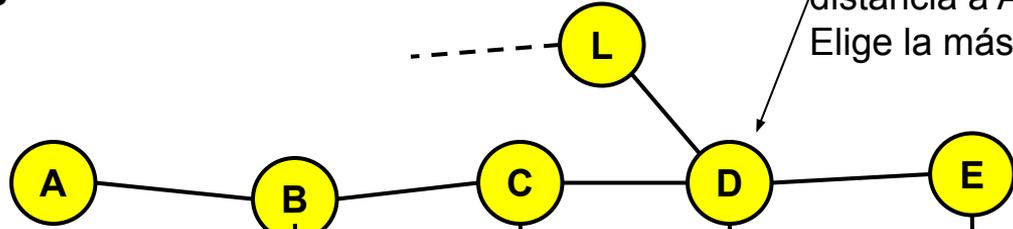
Ejemplos de Protocolos de enrutamiento Intradominio: RIP

- **Problemas:**
 - Converge muy lento ante cambios de la topología que involucran la desaparición de un nodo.
 - Conteo al infinito.
 - Su desempeño disminuye si el tamaño del sistema aumenta.
- **Ventaja: Funciona bien en sistemas pequeños.**



Vector de distancia: Propagación de tablas de ruteo

D recibe información de distancia a A de C y de L. Elige la más corta.



Se agrega el nodo A

B detecta a A y lo agrega a su tabla

B propaga su tabla a C. C agrega a A a su tabla

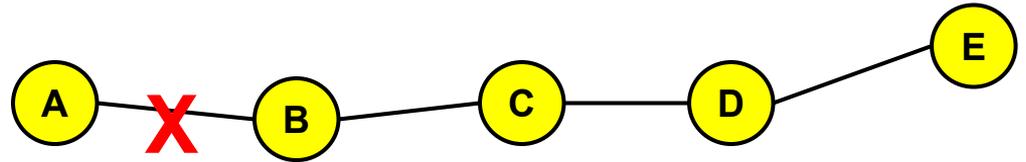
C propaga su tabla a D

D propaga su tabla a E

t_0	∞	∞	∞	∞
t_1	1	∞	∞	∞
t_2	1	2	∞	∞
t_3	1	2	3	∞
t_4	1	2	3	4

Distancia de cada nodo hacia el nodo A en saltos

Algoritmo de ruteo por vector de distancia: Problema conteo infinito



Se rompe el enlace AB

B deja de recibir tablas de ruteo desde A, pero recibe una tabla de ruteo desde C. B calcula erróneamente a partir de la tabla recibida desde C que A está a distancia 3

B propaga su tabla errónea hacia C. C calcula erróneamente desde B que A está a distancia 4

t_0	1	2	3	4
....
t_4	3	2	3	4
t_5	3	4	3	4
t_6	5	4	5	4
t_7	5	6	5	6
t_8	7	6	7	6
t_9	7	8	7	8
t_{10}	9	8	9	8

Hay varias propuestas para resolver el problema, pero ninguna eficiente



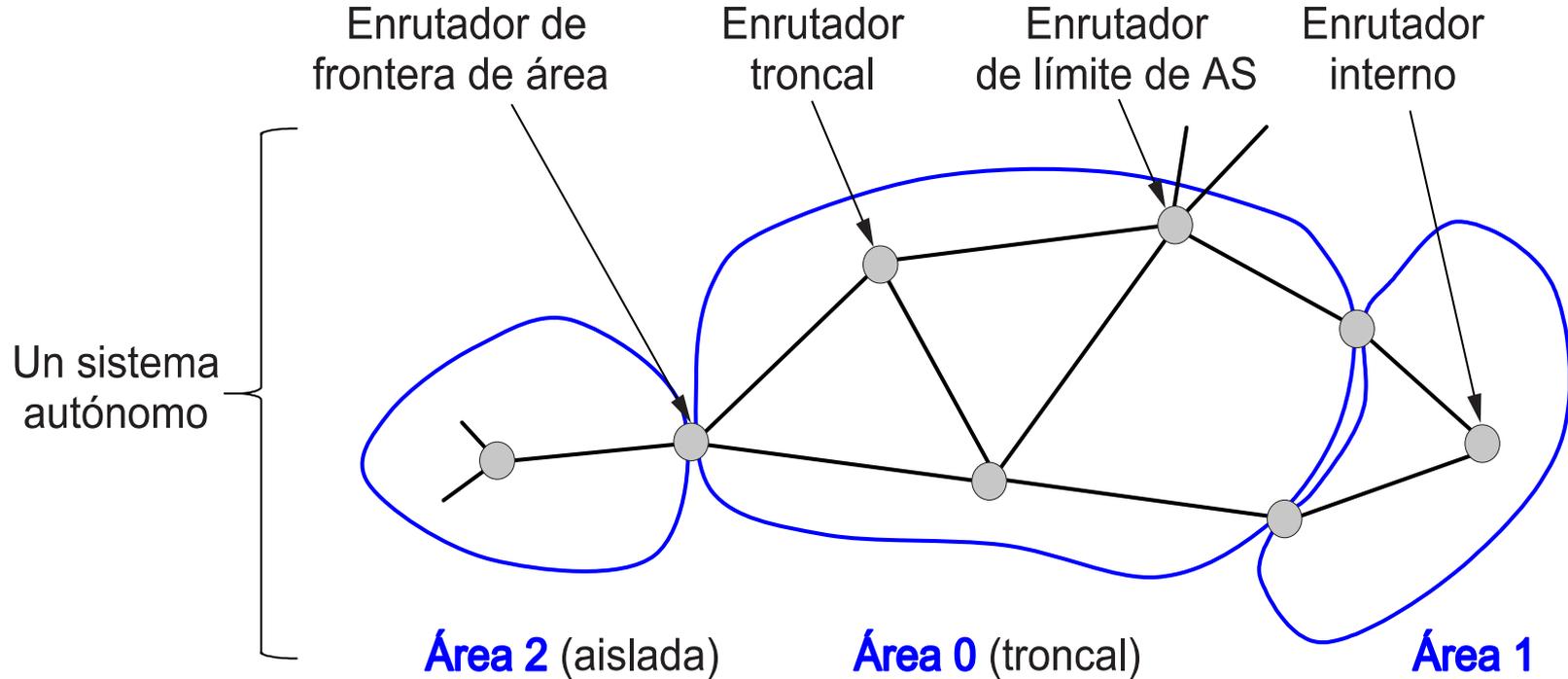
Ejemplos de Protocolos de enrutamiento Intradominio: OSPF (Open Shortest Path First o primero la ruta más corta “abierto”)

- Estandarizado por la **IETF** en 1990 (RFC 2328 versión 2).
- Se emplea en redes internas de empresas u organizaciones.
- Algoritmo de **estado de enlace**.
 - Cada router calcula la distancia a sus vecinos inmediatos.
 - **Cada router comparte con todos los router de la red las distancias a sus vecinos inmediatos.**
 - La información se comparte solo cuando hay un cambio.
 - **Requiere más memoria y poder de procesamiento** en cada router y **genera mayor tráfico de red** que el algoritmo de vector de distancia.
 - **Converge más rápido que vector de distancia.**
- Basado en **algoritmo de Dijkstra**.



Ejemplos de Protocolos de enrutamiento Intradominio: OSPF (Open Shortest Path First o primero la ruta más corta “abierto”)

- Soporte a enrutamiento con base en **tipo de servicio** (el primero).
- Balancea carga entre **múltiples rutas**.
- Soporte para **sistemas jerárquicos** (las redes eran muy grandes).
- Soporta enrutadores conectados mediante **enlaces punto a punto y por difusión** (ejemplo: Ethernet).
- Métrica para el costo del enlace:
 - Velocidad del enlace (bps).
 - Congestión.



Ejemplos de Protocolos de enrutamiento Intradominio: OSPF y áreas

- Mensajes empleados por OSPF (algunos):
 - **Hello**: Cuando un **enrutador se enciende y periódicamente**, envía un Hello a todos los routers de la LAN y espera respuestas para conocer a sus vecinos y que sus vecinos lo conozcan.
 - **Link state update (LSA)**(actualización de estado del enlace):
 - Contiene el **estado del enrutador y costos de los enlaces a sus vecinos inmediatos**.
 - Contiene número de secuencia.
 - Se envían a todos los routers mediante **árboles de expansión**.
 - **Link state ack**: Confirma la recepción de un Link state update.
 - **Link state request**: Solicitar información a otros enrutadores.



Ejemplos de Protocolos de enrutamiento Intradominio: OSPF y áreas

- **Temporizadores** (algunos):
 - Tiempo entre envío mensajes Hello.
 - Tiempo para considerar un router fuera de servicio si no se reciben mensajes de dicho router (Timeout).

Ejemplo del valor del costo para diferentes tipos de tecnologías con ancho de banda de referencia 10 Gbps.

- El administrador debe establecer un ancho de banda de referencia.
 - Usualmente el ancho de banda del enlace más rápido.

Tipo de interfaz	Ancho de banda de referencia en bps	Ancho de banda predeterminado en bps	Costo
10 Gigabit Ethernet 10 Gbps	10,000,000,000 ÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	10,000,000,000 ÷	1,000,000,000	10
Fast Ethernet 100 Mbps	10,000,000,000 ÷	100,000,000	100
Ethernet 10 Mbps	10,000,000,000 ÷	10,000,000	1000
Serial 1,544 Mbps	10,000,000,000 ÷	1,544,000	6477
Serial 128 kbps	10,000,000,000 ÷	128,000	78125
Serial 64 kbps	10,000,000,000 ÷	64,000	156250

Ejemplo del valor del costo para diferentes tipos de tecnologías con ancho de banda de referencia 1 Gbps.

Tipo de interfaz	Ancho de banda de referencia en bps	Ancho de banda predeterminado en bps	Costo
10 Gigabit Ethernet 10 Gbps	1,000,000,000	10,000,000,000	1
Gigabit Ethernet 1 Gbps	1,000,000,000	1,000,000,000	1
Fast Ethernet 100 Mbps	1,000,000,000	100,000,000	10
Ethernet 10 Mbps	1,000,000,000	10,000,000	100
Serial 1,544 Mbps	1,000,000,000	1,544,000	647
Serial 128 kbps	1,000,000,000	128,000	7812
Serial 64 kbps	1,000,000,000	64,000	15625

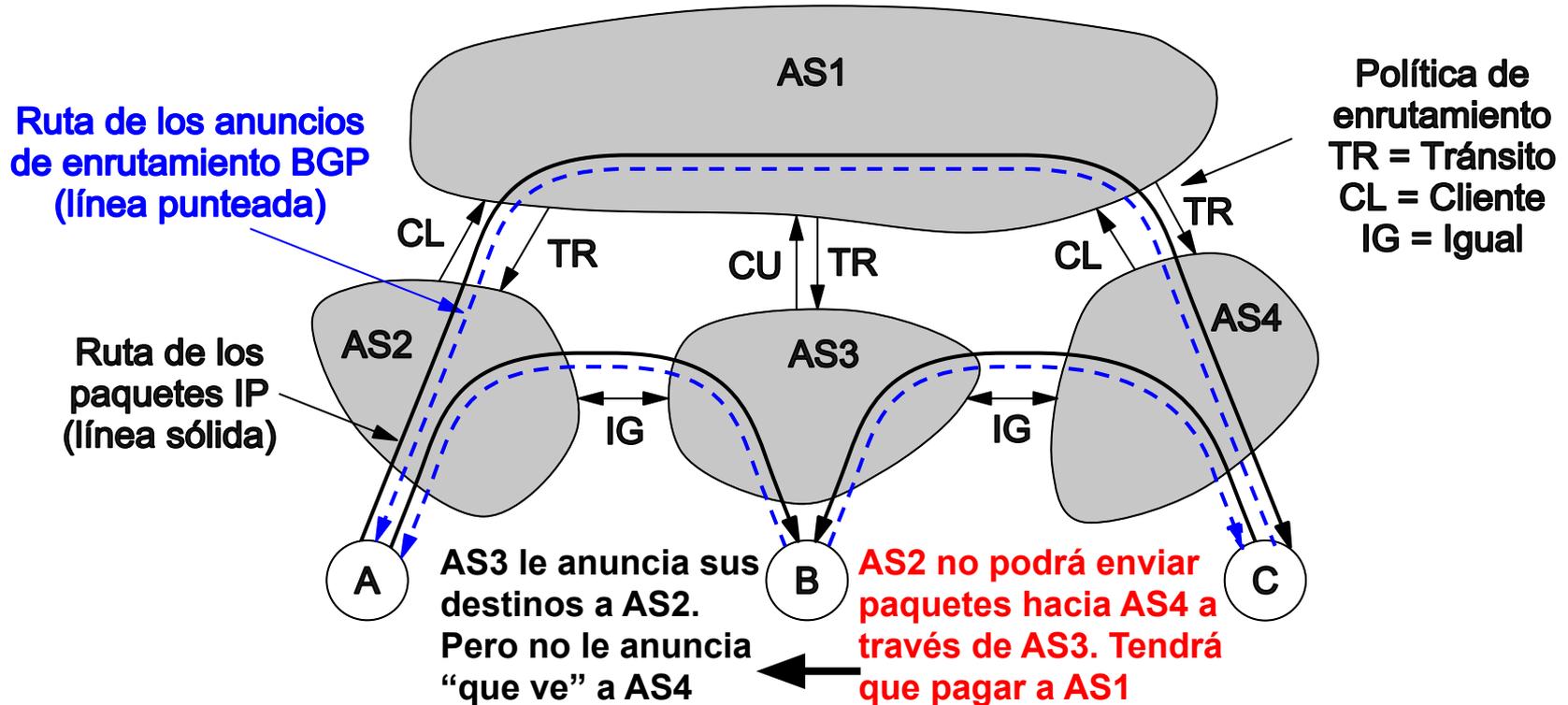
Figura obtenida de:
<https://community.cisco.com/>

Ejemplos de Protocolos de enrutamiento Interdominio: BGP (Border Gateway Protocol o Protocolo de Puerta de Enlace de Frontera)

- Algunos modelos:
 - **Servicio de tránsito o proveedor-cliente**: AS2, AS3 y AS4 (clientes) pueden pagar a un AS1 (proveedor) para que envíe sus paquetes a cualquier destino en Internet.
 - **AS1 debe anunciar todos los destinos alcanzables a sus clientes.**
 - **Los clientes deben anunciar sus destinos al proveedor.**
 - **Acuerdo** (o comunicación) **entre pares** (peering): Dos AS que intercambian mucho tráfico pueden acordar intercambiar paquetes **sin costo**.
 - **Deben enviarse anuncios de enrutamiento entre si.**
 - **No es transitiva**: si AS2 y AS3 tienen acuerdo, AS3 y AS4 tienen acuerdo, no significa que AS2 pueda enviar paquetes a AS4 a través de AS3 (AS3 anuncia sus destinos a AS4, pero no los destinos en AS2).
 - Algunos host (usualmente compañías) compran acceso a varios ISP.



Ejemplos de Protocolos de enrutamiento Interdominio: BGP





Ejemplos de Protocolos de enrutamiento Interdominio: BGP (Border Gateway Protocol o Protocolo de Puerta de Enlace de Frontera)

- RFC 4271.
- **Dificultades** de los protocolos de enrutamiento **interdominio**: **Políticas**.
 - Un AS puede no querer transportar paquetes que se originan en otro AS y tienen como destino un tercer AS.
 - Un AS puede tener acuerdo de pares con otro AS, pero no con un tercero.
 - Un AS podría cobrar una tarifa a otros AS para transportar su tráfico (empresas portadoras).
 - Un AS puede preferir determinado AS y no un tercero para enviar sus paquetes por ser el tercero más costoso.



Ejemplos de Protocolos de enrutamiento Interdominio: BGP

- Las **rutas** se definen **principalmente por políticas**, y en forma **secundaria por costos** (El costo es difícil calcularlo, depende de los protocolos intradominio, y algunos AS pueden no querer proporcionarlos).
- Protocolo basado en **vector de camino** (o de vector de distancia “modificado” o vector de ruta).
 - Los enrutadores BGP tienen información sobre los **destinos, costos a cada destino y ruta**.
 - **Ruta** se da en forma de **próximo salto** (próximo router BGP o de frontera) y **secuencia de AS**.
 - Si un enrutador recibe un anuncio de ruta, añade su número de AS al mensaje y lo reenvía al siguiente AS.
 - Si el enrutador detecta que su número de AS ya está en la ruta, **ha detectado un ciclo** y descarta el mensaje.

Ejemplos de Protocolos de enrutamiento Interdominio: BGP

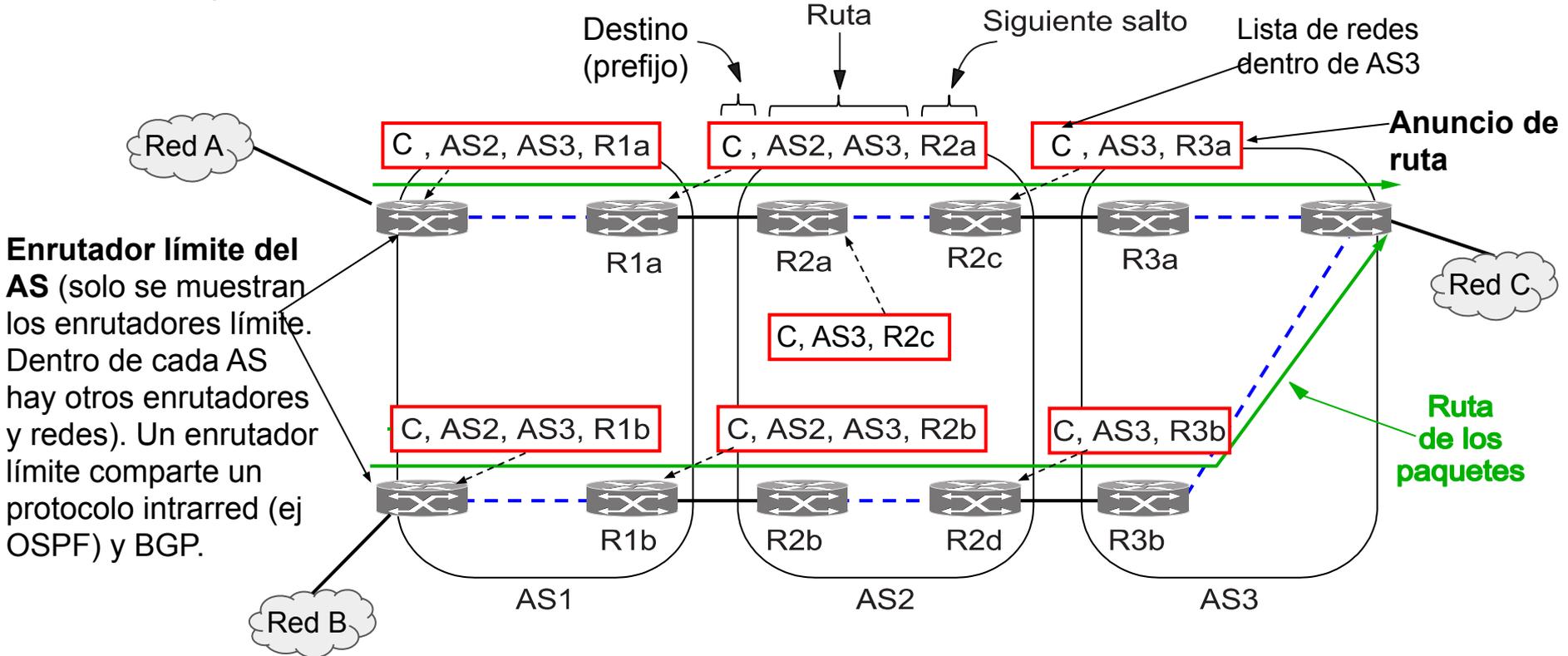


Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 413



Ejemplos de Protocolos de enrutamiento Interdominio: BGP (continuación)

- Los pares de enrutadores BGP se comunican mediante TCP.
- Si un router detecta un cambio en su base de datos (nueva ruta, ruta ya no existente, etc.), difunde un mensaje de actualización.
- Un router que se comunica con otro router de otro AS no necesariamente debe implementar BGP. Otro router del mismo AS que implemente BGP puede informar que dicho router es el “proximo salto” para llegar a otro destino.

Ejemplos de Protocolos de enrutamiento Interdominio: BGP

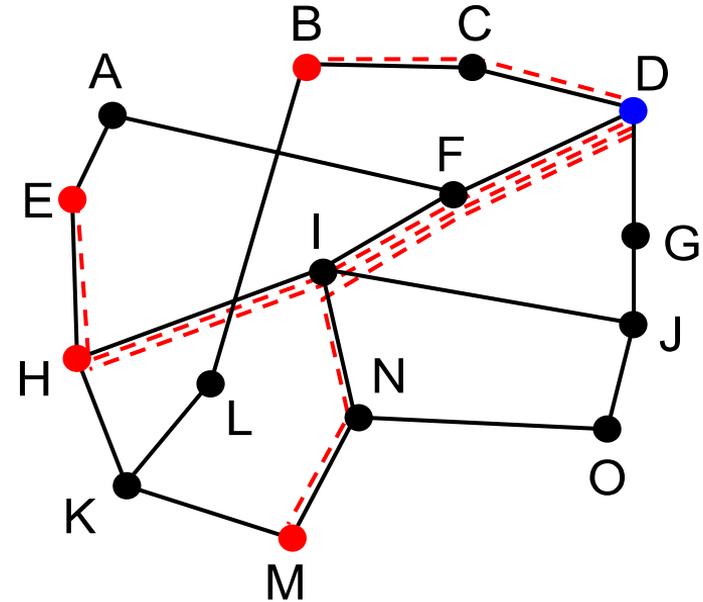
- ¿Cómo pasa un anuncio de ruta **BGP** a través de las **rutas internas de un AS** (por ejemplo, un ISP)?
 - **No se emplea el protocolo intradominio**, se emplea **iBGP** (internal BGP).
 - Cada enrutador límite (o de salida del AS) conoce la información contenida por todos los demás enrutadores límites del AS, de manera que saben cómo salir del AS.
 - Cada AS elige sus estrategias o políticas para rutear paquetes de tránsito:
 - Usar rutas con acuerdo entre pares (pueden ser gratuitas).
 - Dar preferencia a los que paguen.
 - En caso de dos rutas “iguales”: menor costo dentro del AS (o enrutamiento de la papa caliente).



Enrutamiento por difusión (Broadcasting)

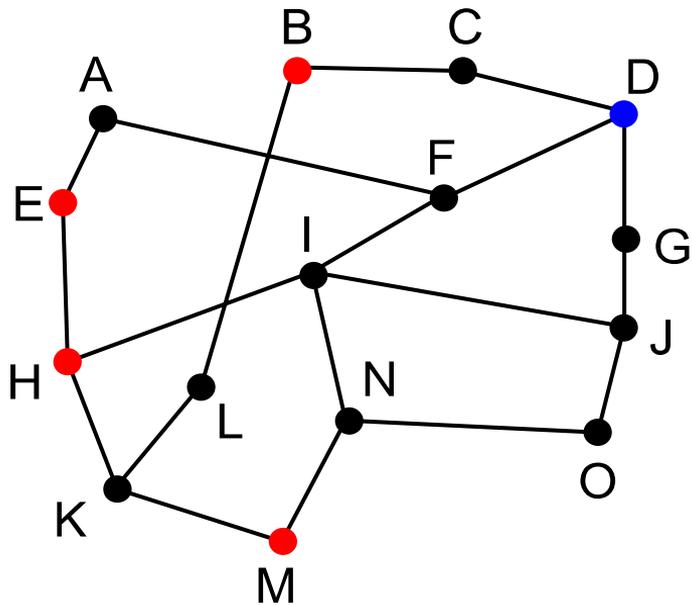
- Envío de mensajes a varias o todas las máquinas de una red (broadcast, multicast, anycast).
- Métodos (tanto para broadcast, multicast, anycast):
 - Enrutamiento multidestino: El paquete tiene múltiples destinos. El paquete solo se divide en dos copias cuando deben seguir diferentes rutas.
Sobrecarga en enrutadores.
 - Inundación. **Latencia grande.**
 - Enviar una copia del paquete a cada destino.
 - Árboles de expansión.

- Inundación
 - **No es necesario conocer la ubicación de los nodos finales.**
 - **Gran cantidad de tráfico innecesario.**
- Enviar una copia del paquete a cada destino.
 - **Es necesario conocer la ubicación de estos nodos.**
 - **Muchos paquetes con los mismos datos circulan por los mismos enlaces y routers.**
- Árboles de expansión (siguiente filmina).

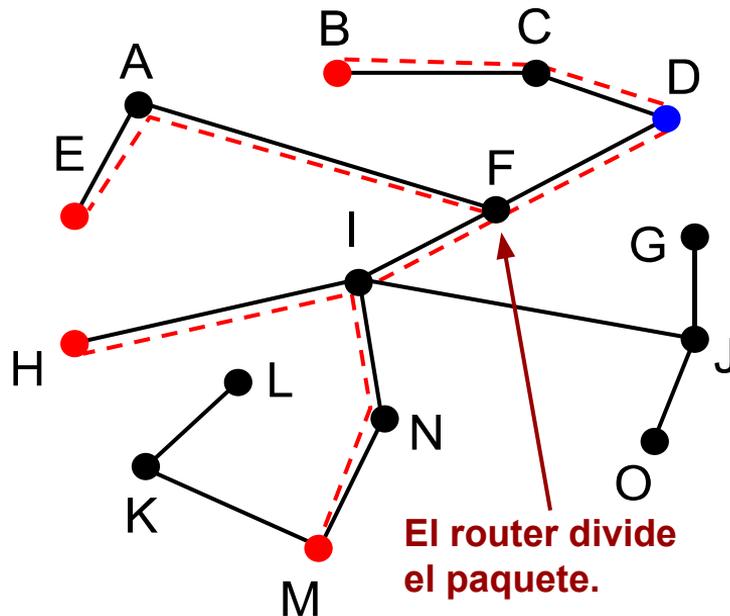




Enrutamiento por difusión: Ejemplo de ruteo por árbol de expansión



Red completa



árbol de expansión

Enrutamiento por difusión, ejemplos de uso

- **Broadcast:**

- Envío de mensajes a todos los nodos de la red.
- Ejemplo de aplicación:
 - Algoritmos de ruteo de Internet (BGP).
 - Algoritmos de estado de enlace (envío de paquetes de estado de enlace en protocolos como OSPF).

- **Multicast:**

- Envío de mensajes a todos los nodos de un grupo.
- Ejemplo de aplicación:
 - Enviar un flujo continuo de paquetes a un subgrupo de máquinas la red (no a toda la red).
 - Streaming.

Enrutamiento por difusión

- **Anycast:**

- El paquete se entrega al miembro más cercano de un grupo.
- Ejemplo aplicación: Cuando un grupo de nodos provee un **servicio**.
Temperatura promedio por zonas, DNS.

