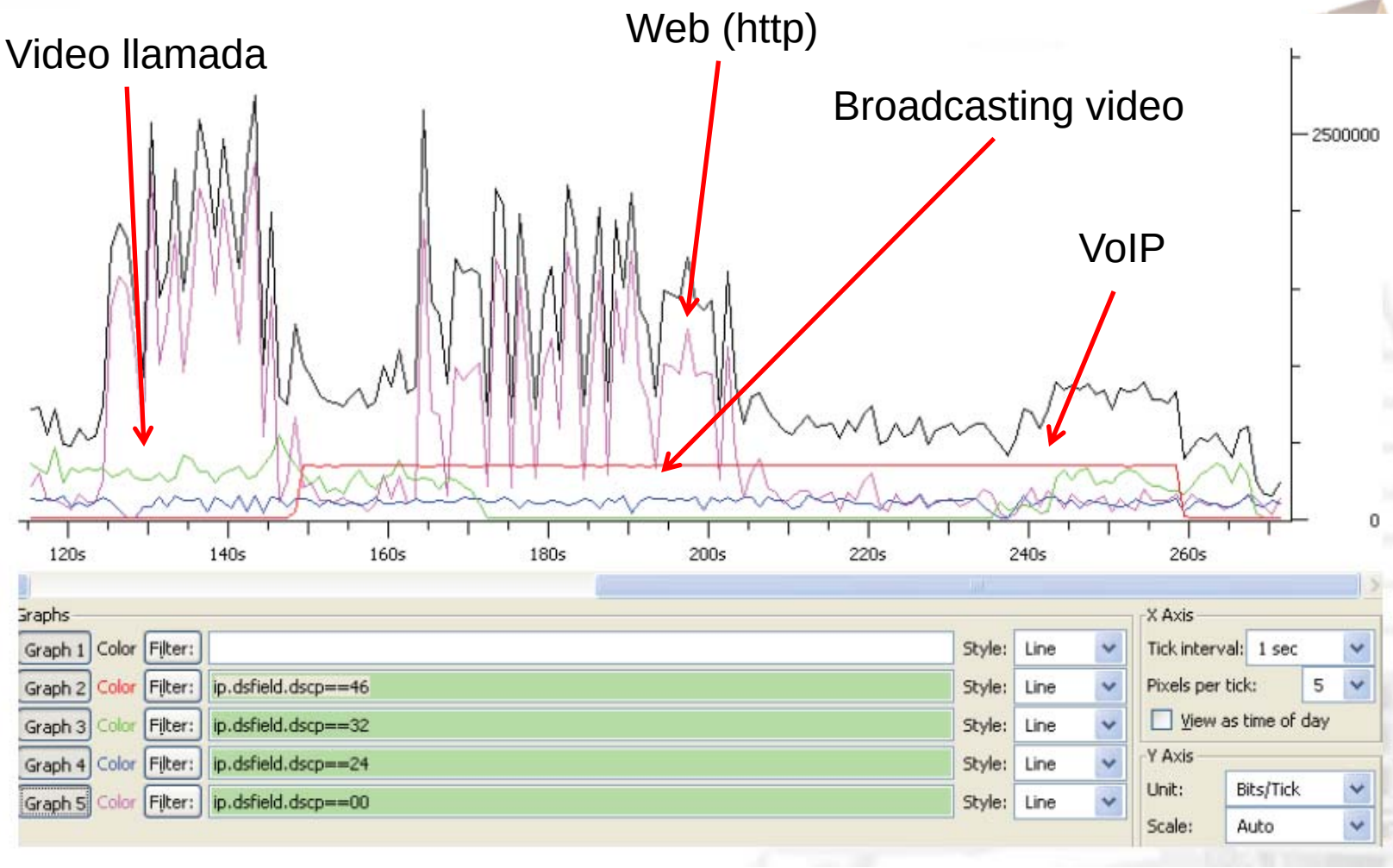
Jhon Jairo Padilla A. PhD.

Arquitectura de Routers y Switches

Requerimientos actuales

- Servicios:
  - Voz
  - audio
  - TV
  - Juegos
  - Web
  - Videos
- Usuarios:
  - Dispositivos móviles pequeños
  - Gran crecimiento del número de usuarios

Tráfico de diferentes aplicaciones



Requerimientos actuales

- Tráfico:
  - Voz, video, datos
  - Altos volúmenes de tráfico
  - Requerimientos de QoS altos
- Características internas de Routers y Switches:
  - Grandes tablas de enrutamiento
  - Procesamiento de paquetes a alta velocidad

Funciones Básicas

FUNCIONES DE UN ROUTER

Funciones del procesamiento de los paquetes

Funciones básicas

- Búsqueda de direcciones y re-envío de paquetes
- Detección y corrección de errores
- Fragmentación, segmentación y re-ensamble
- Demultiplexación de protocolos y tramas
- Seguridad: autenticación y privacidad

Funciones para soporte de QoS

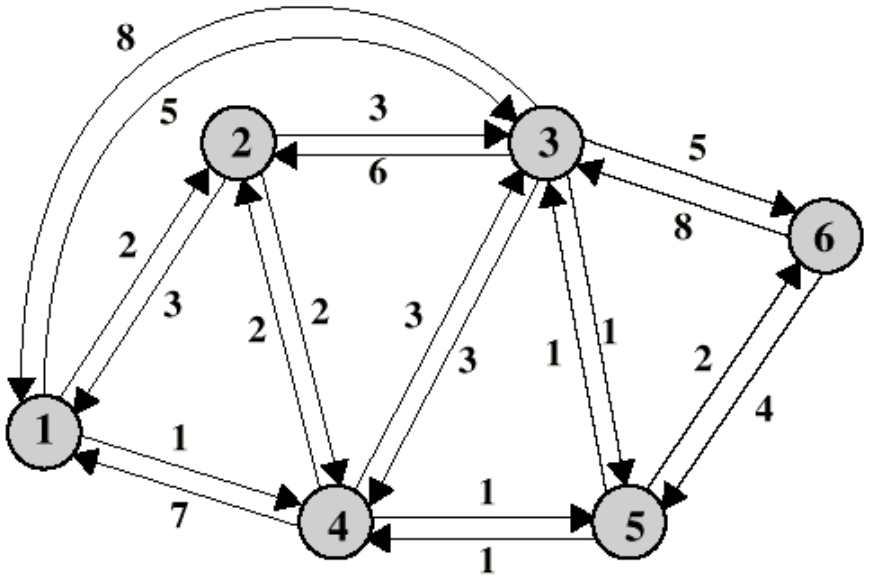
- Clasificación de paquetes
- Encolamiento y descarte de paquetes
- Planificación y temporización
- Medición de tráfico y control de políticas
- Recorte de tráfico

BUSQUEDA DE DIRECCIONES Y REENVÍO DE PAQUETES

Tablas de Enrutamiento

CENTRAL ROUTING DIRECTORY

To Node \ From Node	1	2	3	4	5	6
1	—	1	5	2	4	5
2	2	—	5	2	4	5
3	4	3	—	5	3	5
4	4	4	5	—	4	5
5	4	4	5	5	—	5
6	4	4	5	5	6	—



Node 1 Directory

Destination	Next Node
2	2
3	4
4	4
5	4
6	4

Node 2 Directory

Destination	Next Node
1	1
3	3
4	4
5	4
6	4

Node 3 Directory

Destination	Next Node
1	5
2	5
4	5
5	5
6	5

Node 4 Directory

Destination	Next Node
1	2
2	2
3	5
5	5
6	5

Node 5 Directory

Destination	Next Node
1	4
2	4
3	3
4	4
6	6

Node 6 Directory

Destination	Next Node
1	5
2	5
3	5
4	5
5	5

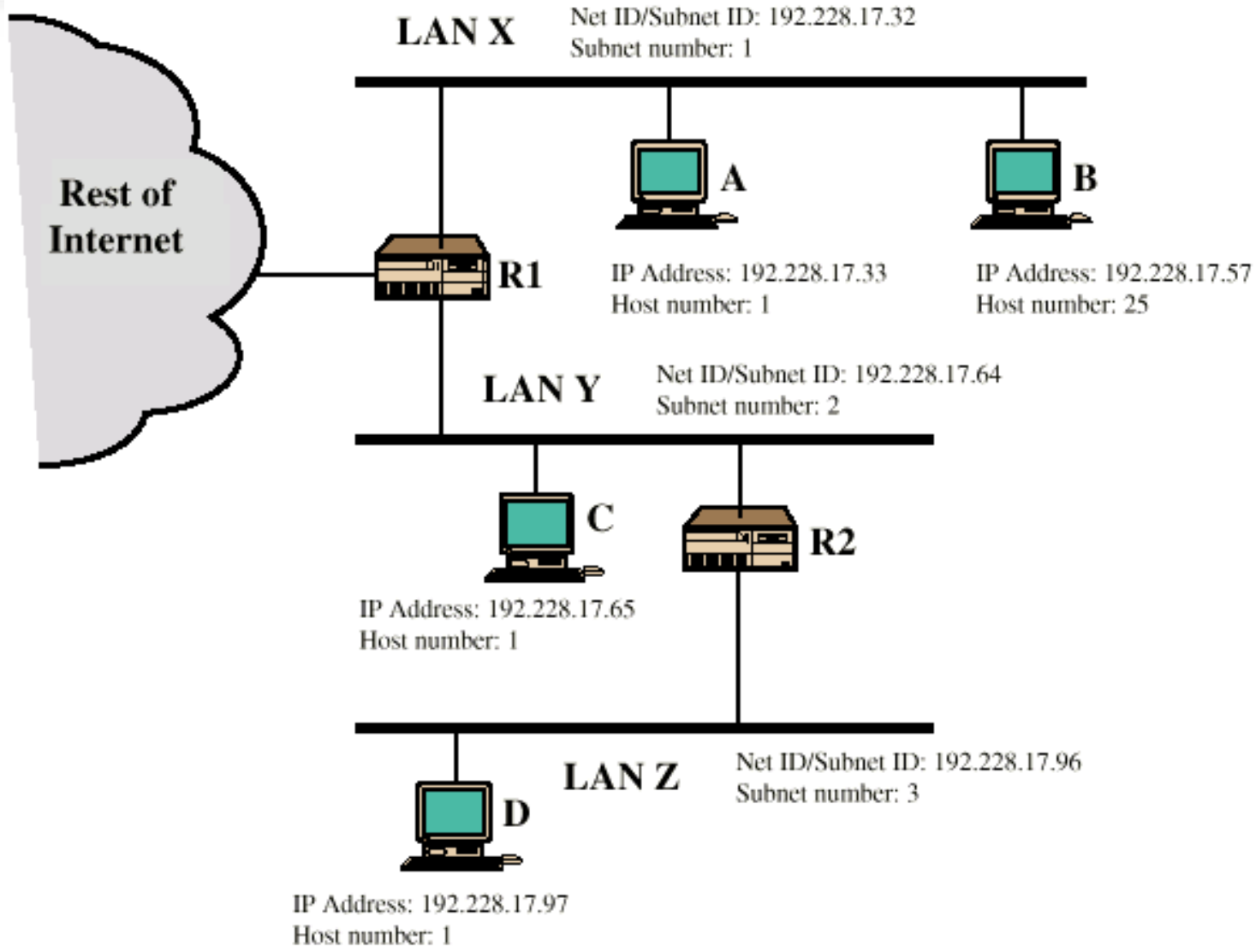
Búsqueda de Direcciones y re-envío de paquetes

- Búsqueda de direcciones (Address Lookup):
  - El sistema mantiene una tabla y usa la tabla de direcciones para buscar la dirección destino indicada en un paquete.
- Ejemplos:
  - Puente Ethernet:
    - Se busca la dirección MAC para determinar re-enviar el paquete
  - Router:
    - Se busca la dirección IP de destino.
  - Protocolo ARP:
    - Mantiene un caché que se consulta cuando se envía un datagrama IP

Re-envío de paquetes

- La búsqueda de direcciones está muy relacionada con el proceso de re-envío (forwarding)
- Forwarding:
  - Es el proceso de enviar un paquete hacia su destino.
  - Se debe decidir cuál es el enlace de salida.
  - Se requiere la búsqueda previa de direcciones en una tabla (address Lookup)
  - Este proceso puede suceder en la capa 2 (Puente) y en la capa 3 (Router).
- Ejemplo:
  - Puente:
    - La tabla de re-envío se construye extrayendo la información de las cabeceras de las tramas entrantes.
    - La búsqueda de direcciones requiere una coincidencia exacta (**exact match lookup**) de un ítem en la tabla.
  - Router IP:
    - La tabla es construida por una entidad separada
    - Cada entrada contiene una máscara de direcciones que no puede ser deducida de los paquetes.
    - En lugar de una coincidencia exacta, la búsqueda de direcciones IP requiere la coincidencia de un prefijo (**longest Prefix Match**).
  - Direccionamiento multicast:
    - El camino de salida de los paquetes depende tanto de la dirección fuente como de la dirección destino.

Enrutamiento usando Longest Prefix Match



Direcciones IP y máscara de subred

	Representación binaria	**Notación de Punto decimal**
Dirección IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de subred	11111111.11111111.11111111.11100000	255.255.255.224
Resultado And bit a bit	11000000.11100100.00010001.00100000	192.228.17.32
Número de subred	11000000.11100100.00010001.001	1
Número de computador	00000000.00000000.00000000.00011001	25

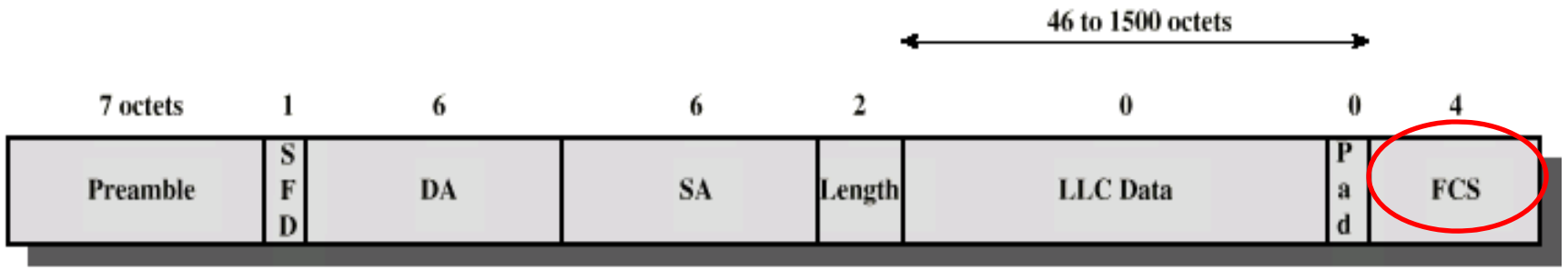
La máscara de subred sirve para determinar la dirección de subred y la identificación del Host

DETECCIÓN Y CORRECCIÓN DE ERRORES

Corrección y detección de errores

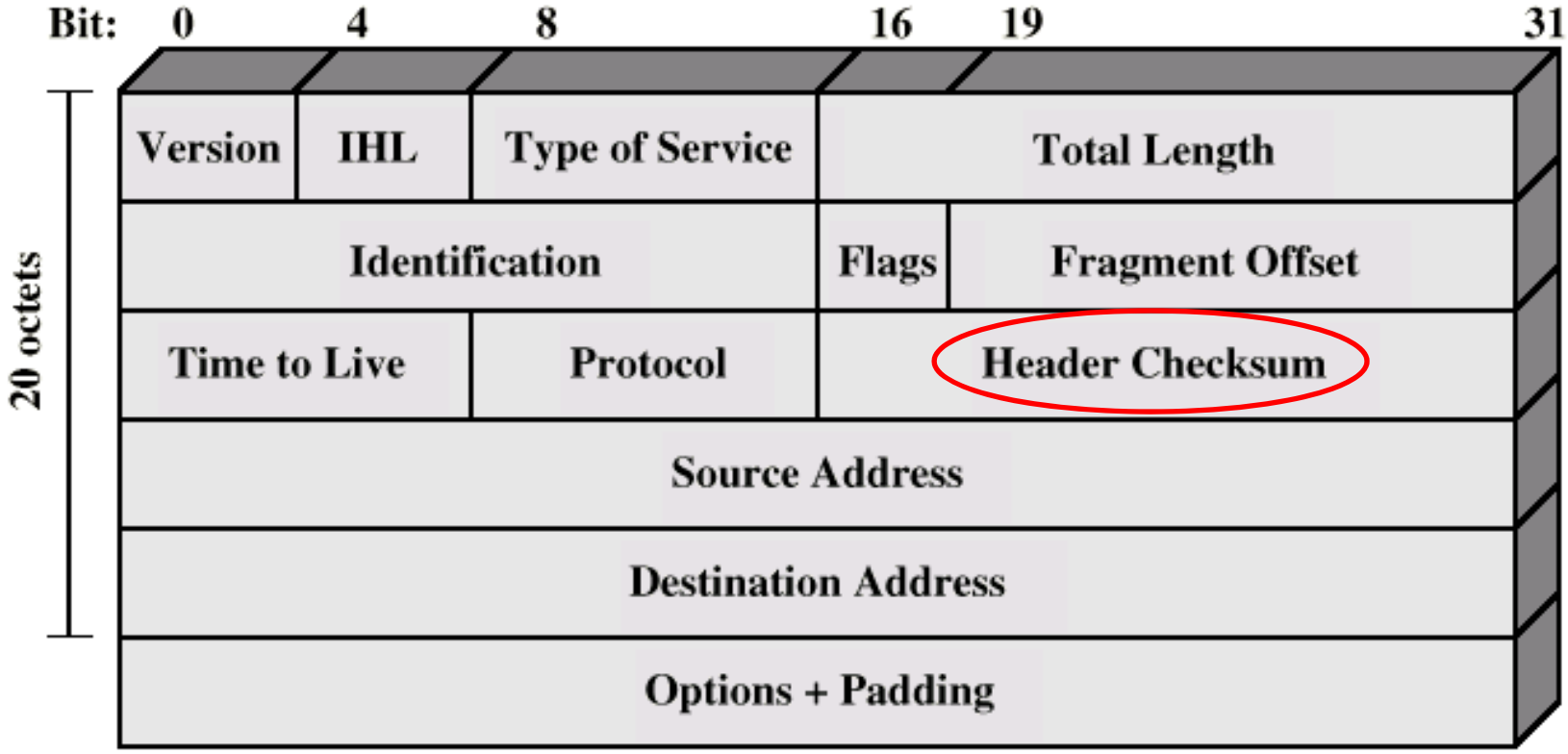
- Es posible que se dañen algunos bits de las tramas
- Causas: interferencia electromagnética, hardware que opera de forma incorrecta
- Solución:
  - Códigos detectores de error
  - Métodos de retransmisión de la información
  - Códigos correctores de errores (incluyen bits redundantes)
- Estas funciones se realizan agregando campos adicionales a los paquetes (FEC, Checksum)
- Capas encargadas:
  - Suelen ser la capa 2 (Acceso: LLC, HDLC, etc) y la capa 4 (Transporte: TCP)
  - La capa 3 (IP) hace detección de errores en los bits de la cabecera (no en los datos). Usa el protocolo ICMP para informar de estos errores.

Detección de Errores en trama MAC de IEEE 802.3 (Ethernet)



SFD = Start of frame delimiter
DA = Destination address
SA = Source address
FCS = Frame check sequence

Ejemplos: IPv4



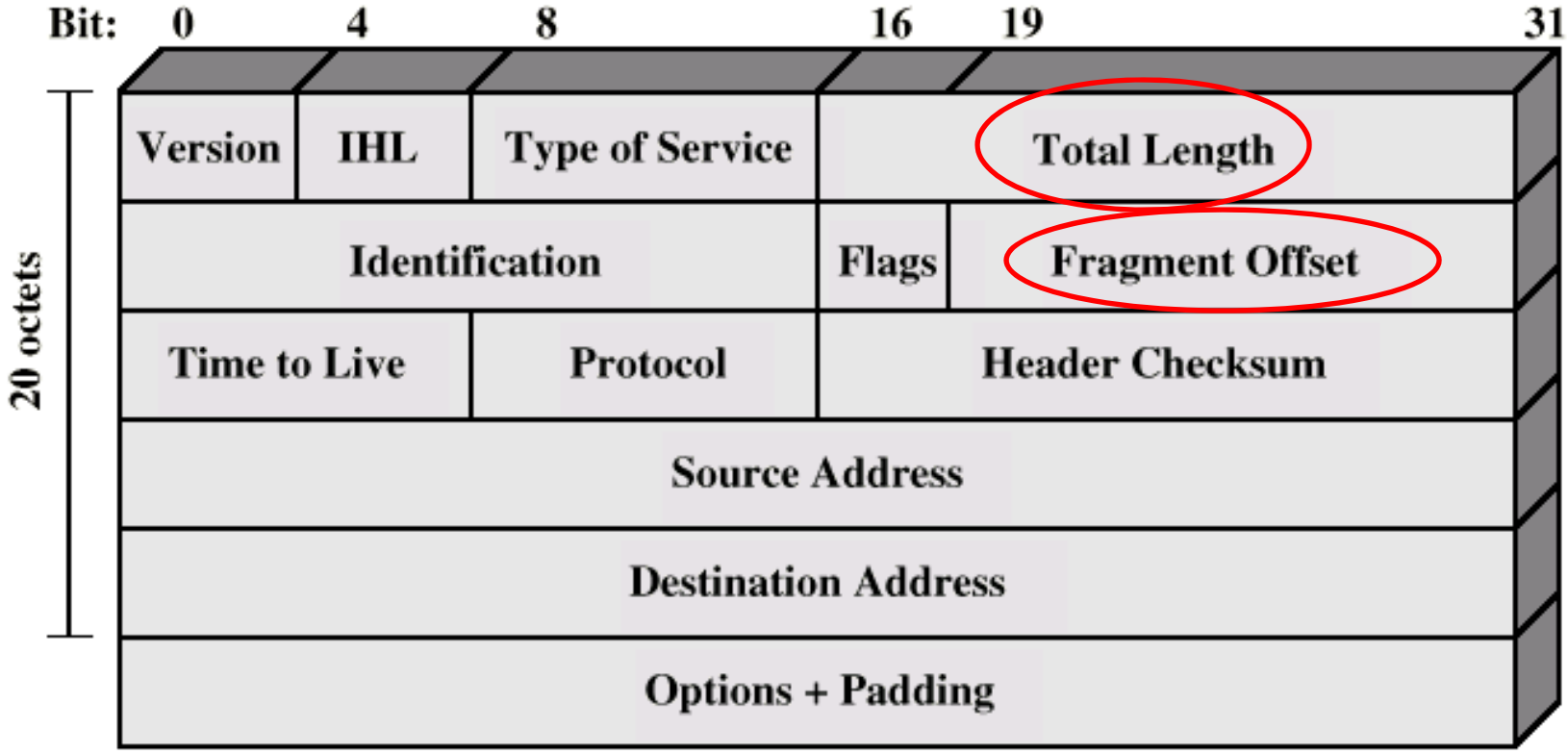
FRAGMENTACIÓN Y REENSAMBLE DE PAQUETES

Fragmentación, Segmentación y Re-ensamble

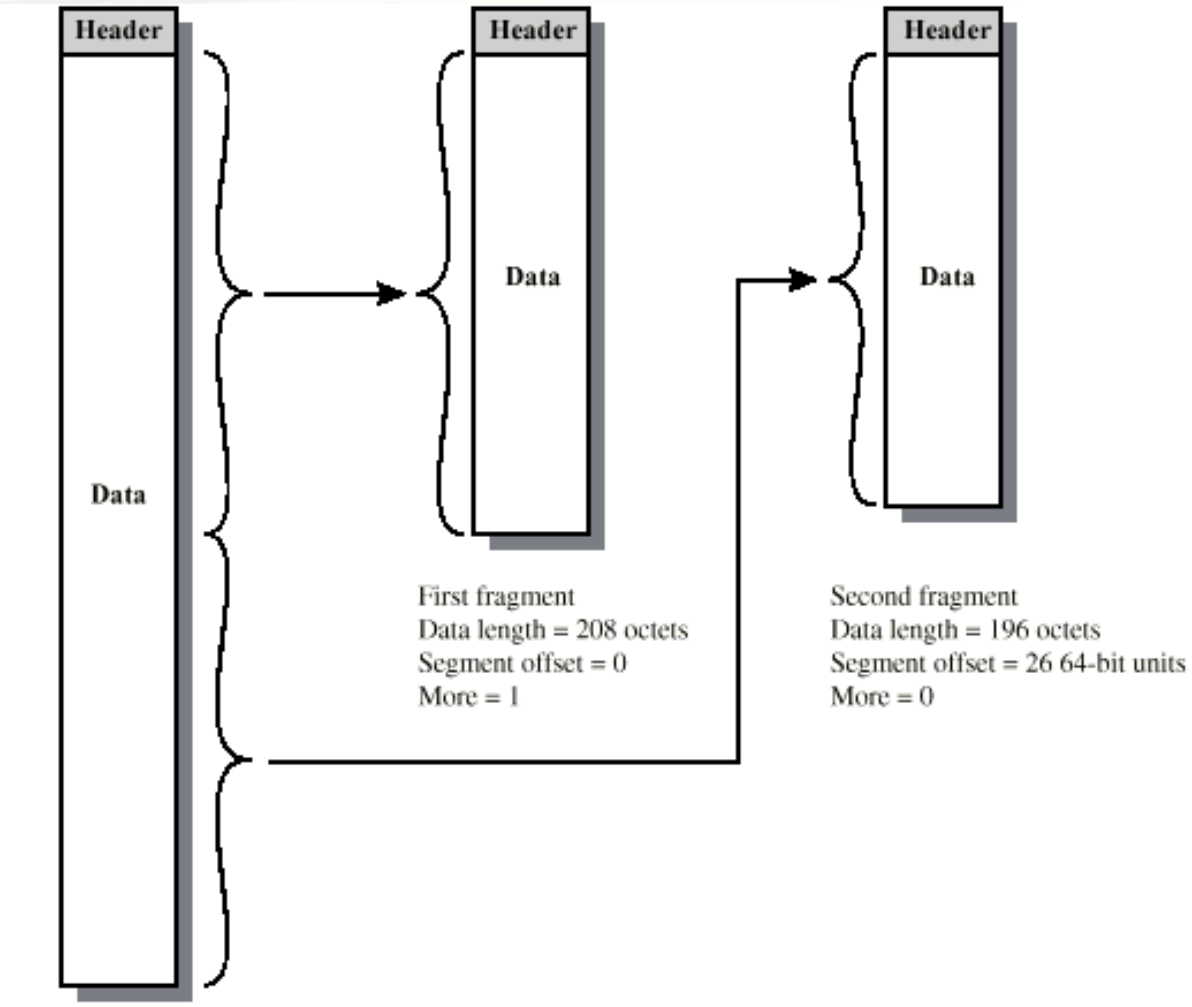
- **Segmentación:** Varias tecnologías de red requieren dividir un paquete grande en paquetes más pequeños (p.ej. IP, ATM)
- *El problema es el re-ensamblaje:* Las partes del paquete llegan asíncronamente.

- Re-ensamblaje:
  - Requiere almacenar las partes hasta que llega el paquete original completo.
  - Debe haber soluciones al problema de pérdida de algunas partes (cuándo asumir como perdido y avisar?).
  - El sistema que re-ensambla no conoce la longitud total del paquete original hasta que se recibe todo….Por tanto, si no se usan apuntadores en la memoria, se requeriría tener un espacio de memoria suficiente reservado para el paquete segmentado que se está recibiendo…Esto requiere grandes cantidades de memoria.

Protocolo IPv4: campos de la trama para la fragmentación/re-ensamblado

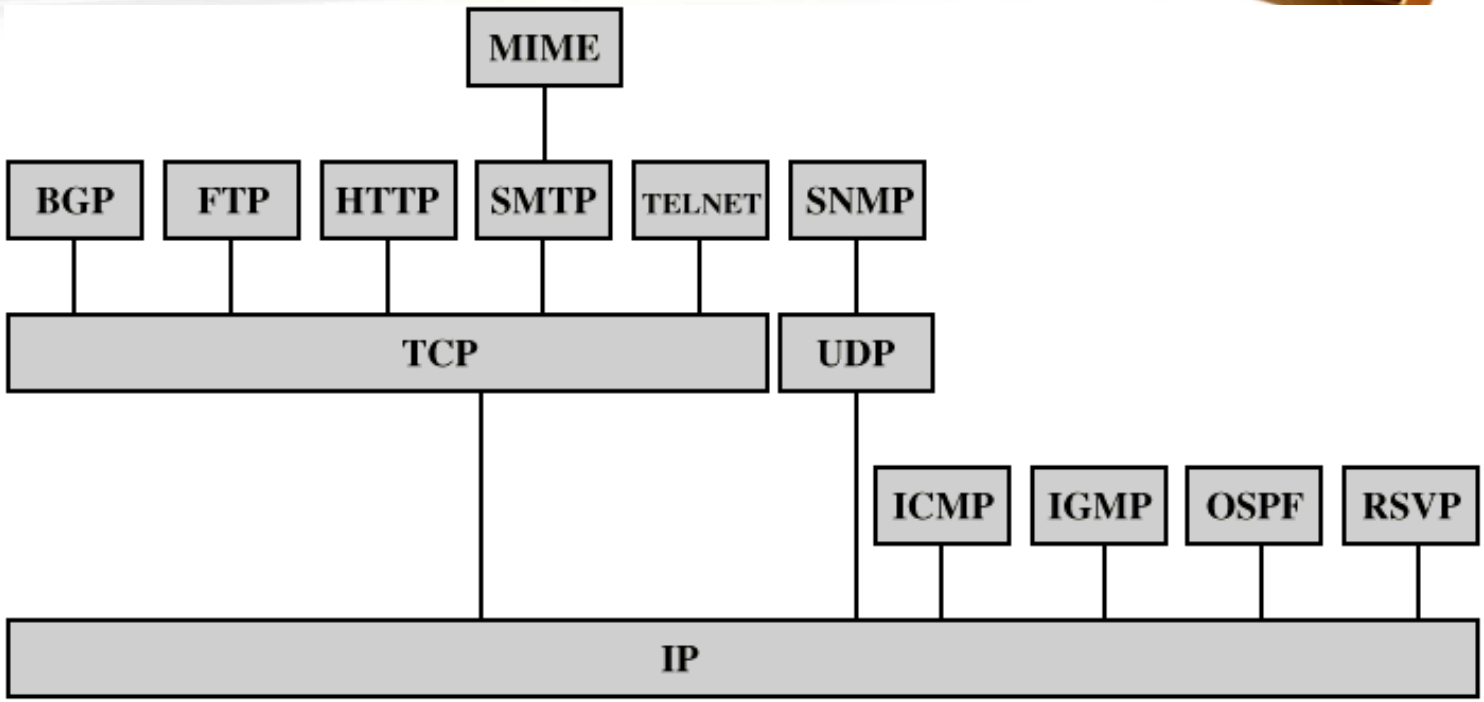


Ejemplo de Fragmentación



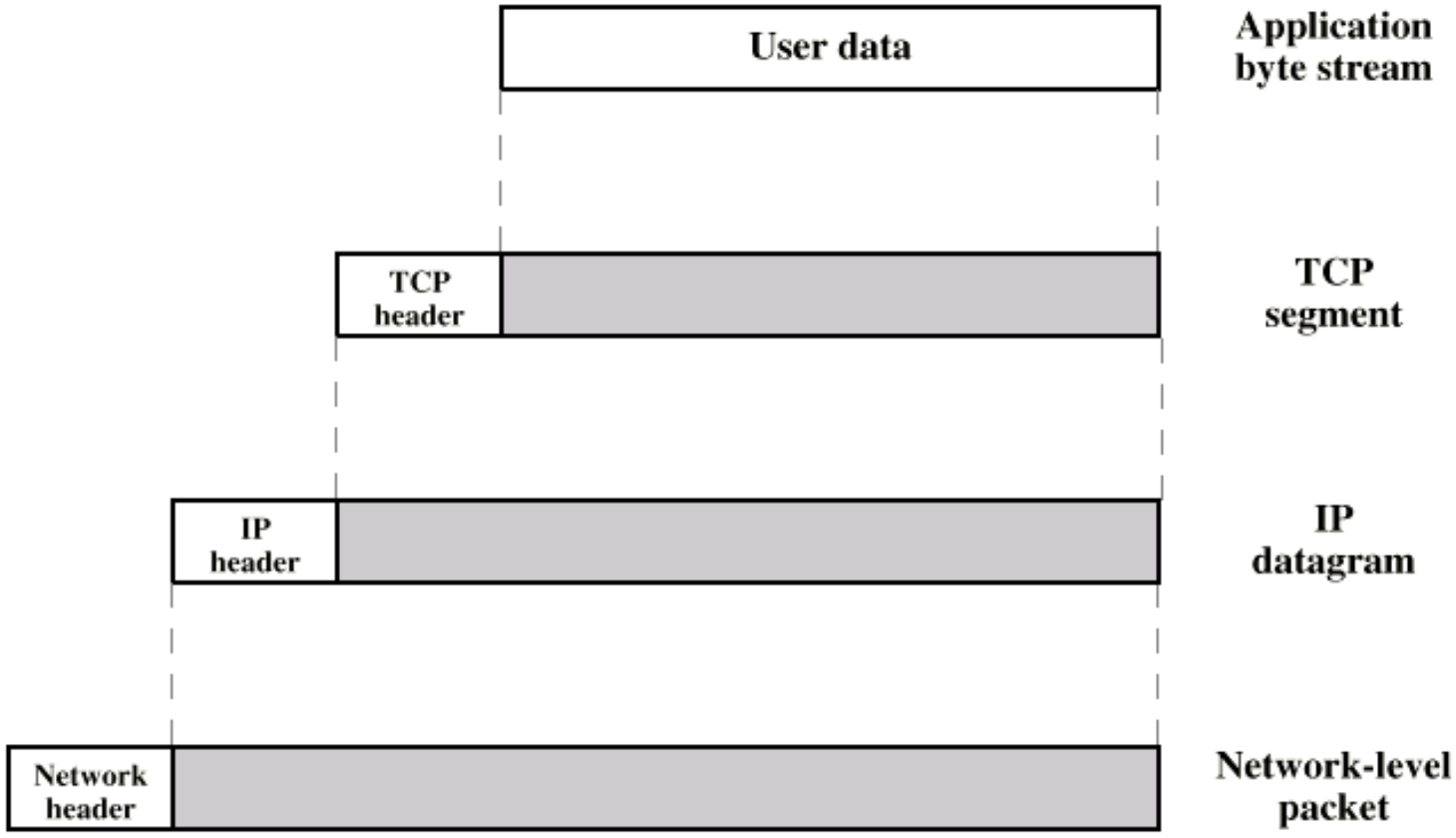
DEMULTIPLEXACIÓN DE TRAMAS Y PROTOCOLOS

Algunos protocolos en la arquitectura TCP/IP



BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

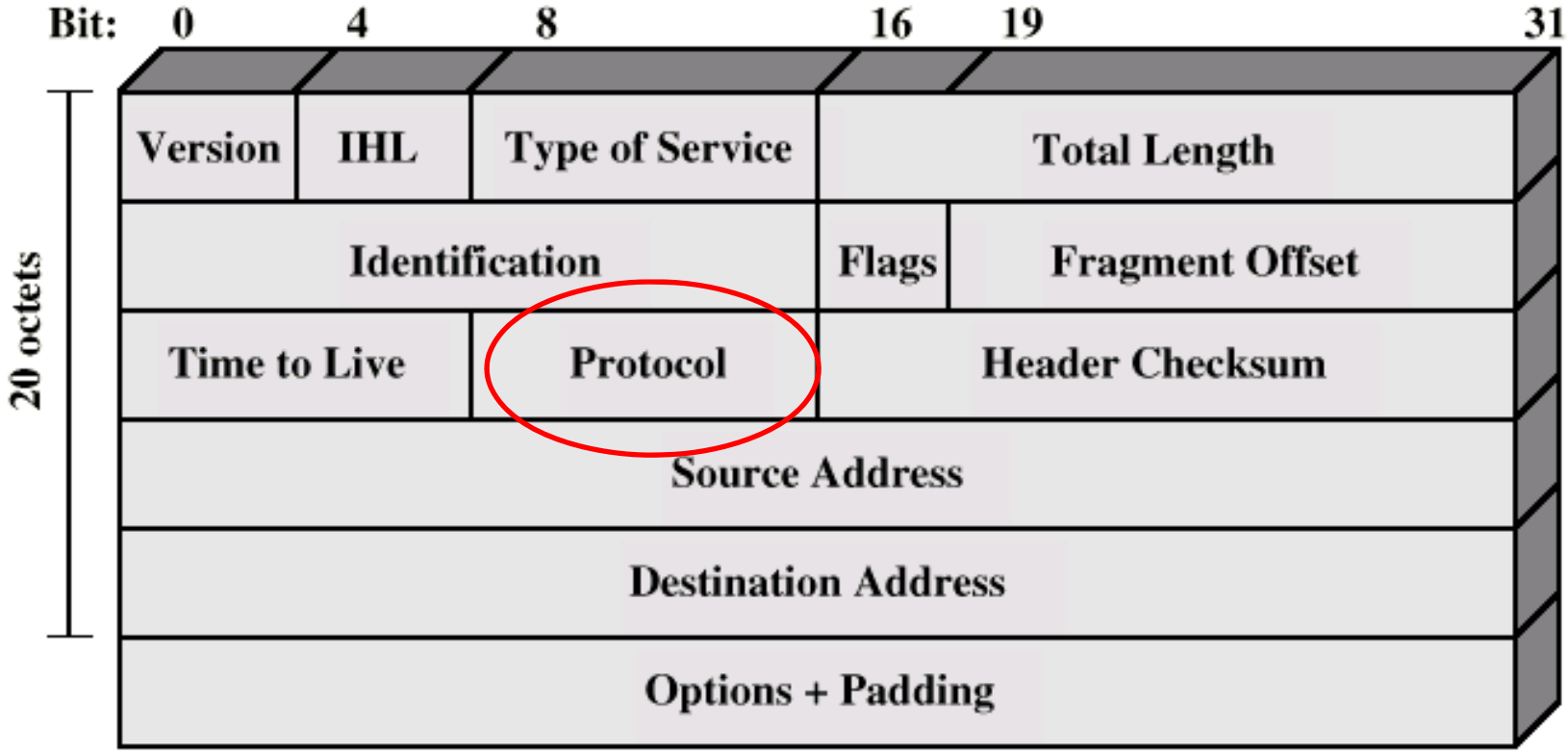
Encapsulamiento/Desencapsulamiento de paquetes



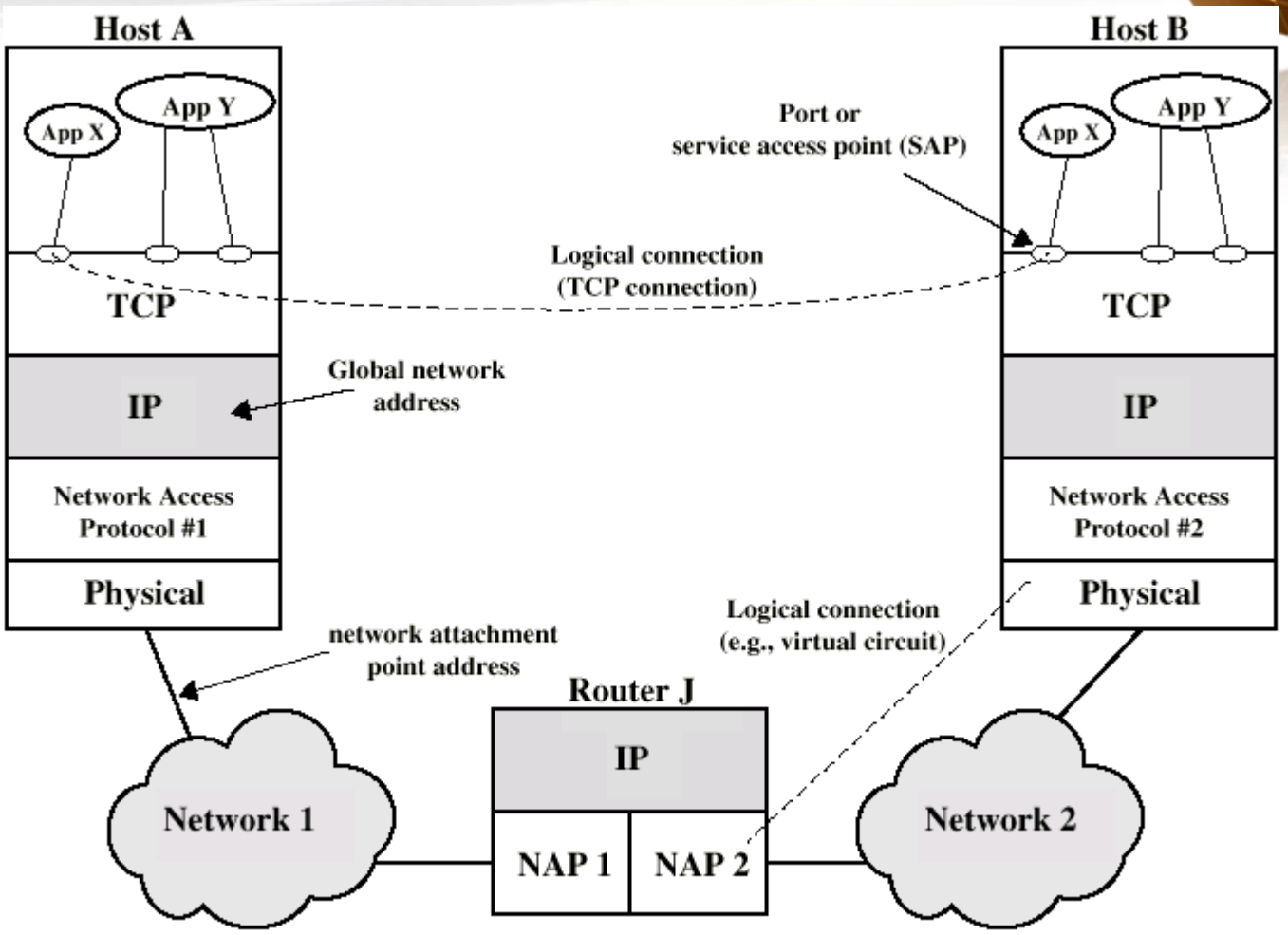
Demultiplexación de tramas y protocolos

- Demultiplexación de protocolos:
  - Escoger un protocolo que será usado para procesar un paquete.
  - Existen diferentes protocolos en la capa superior.
  - Cada capa hace el proceso de demultiplexación para determinar el protocolo de capa superior que debe procesar el paquete.
- Ejemplos:
  - Capa 2:
    - Cuando llega una trama a un Router, se usa la información de la trama para determinar si va hacia el protocolo ARP o IP.
  - Capa 3:
    - Si una trama contiene un paquete IP, el módulo IP usa información del paquete para determinar si el protocolo de transporte es TCP o UDP.
  - Capa 4:
    - El protocolo de capa de transporte debe demultiplexar su MTU entre múltiples aplicaciones (usa los puertos para ello).

IPv4: Campo usado para demultiplexación



Demultiplexación en capa de Transporte



Demultiplexación de tramas y protocolos

- Se requiere que en los enlaces de salida del router se haga el proceso inverso.
- Se debe agregar información en las cabeceras de cada capa para que se pueda hacer la demultiplexación en los enlaces de entrada.
- Ejemplo:
  - Cuando un router encapsula un datagrama en una trama Ethernet para su transmisión, un módulo IP fija el tipo de trama a 800H, lo que permite al router que recibe demultiplexar dicho paquete cuando llega.

SEGURIDAD

Funciones relacionadas

- Encriptación:
  - Resuelve el problema de escucha por parte de terceros (Privacidad)
  - Tanto el orígen como el destino conocen una clave para ingresar/extraer la información de la trama encriptada
- Autenticación:
  - Resuelve el problema de determinar si el otro extremo es quien dice ser.
  - También sirve para verificar la integridad de los datos
  - Se requiere una clave o firma digital del transmisor con la cual se genera un número que es comparado en el receptor

Recursos requeridos

- Se requiere poca información adicional
- Sin embargo, el procesamiento de las tramas para la autenticación y la privacidad es bastante fuerte
- Los sistemas que implementan encripción y autenticación requieren de una potencia extra de procesamiento

Planificación de procesos

- Los sistemas basados en procesadores (CPUs) requieren hacer varios procesos “simultáneamente”
- Se requiere distribuir el tiempo de CPU entre diferentes procesos.
- Se utilizan prioridades para los diferentes procesos
- Puede haber procesos realmente simultáneos, por lo que se requieren varios “hilos” (threads) para el procesamiento
- La planificación está relacionada con los temporizadores de diferentes tareas.

Gestión de los temporizadores

- Los temporizadores son fundamentales para el procesamiento de paquetes a diferentes niveles:
  - Lectura de bits
  - Inicio/fin de trama
  - Refresco del estado de diferentes protocolos
- Ejemplos de protocolos con temporización:
  - ARP (capa 2): retransmisión (para declarar un sistema no alcanzable) y manejo del caché (borra entradas al vencerse un temporizador)
  - IP (capa 3): re-ensamble de paquetes
  - TCP (capa 4): Para solicitar retransmisiones si no llegan paquetes

Funciones para el soporte de QoS

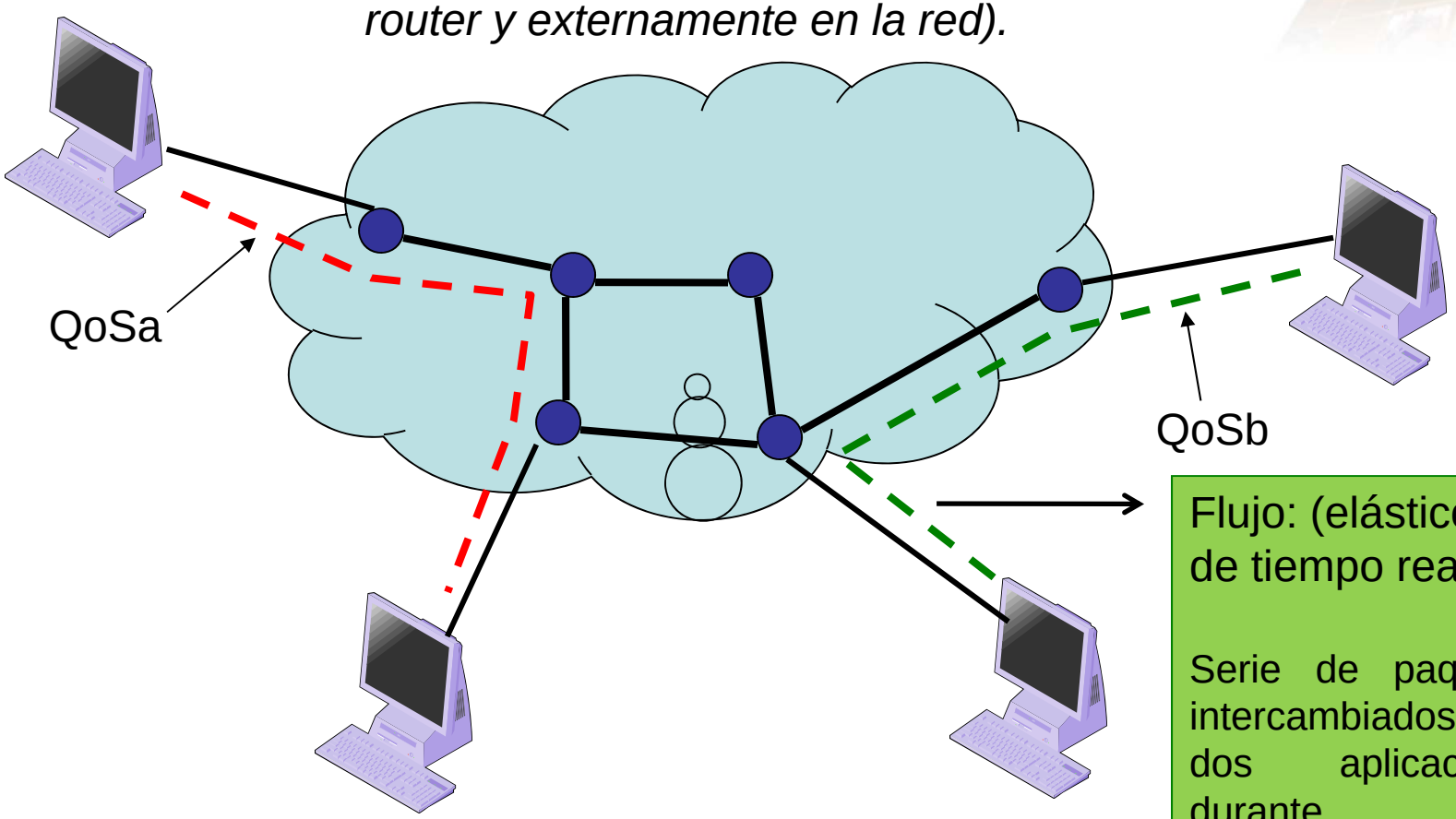
FUNCIONES DE UN ROUTER

CLASIFICACIÓN DE PAQUETES

Flujos en una red

Flujo:

Paquetes que tienen características similares fluirán sobre el mismo camino lógico (internamente en el router y externamente en la red).



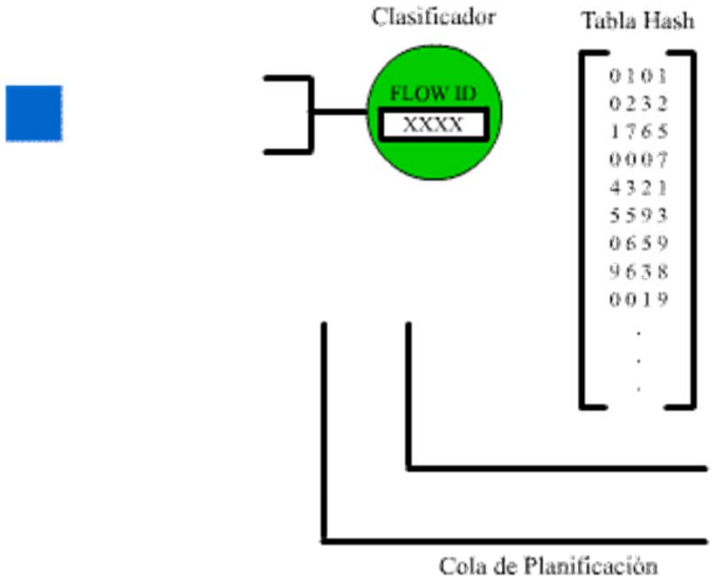
Flujo: (elástico o de tiempo real)

Serie de paquetes intercambiados por dos aplicaciones durante una conexión

Clasificación de paquetes

- Se refiere al proceso de mapear un paquete a uno de un conjunto finito de flujos o categorías.
- Clasificación Interna del router:
  - Un router puede clasificar los paquetes entrantes en 4 categorías:
    - Paquetes TCP
    - Paquetes UDP
    - Mensajes ICMP
    - Otros
  - Este conjunto de flujos es estático (no cambia): **Asignación de flujos estática.**
  - **Asignación dinámica de flujos:**
    - Se usan uno o varios campos de la cabecera IP para hacer la clasificación (Dir IP origen, Dir IP Destino, Puerto Origen, Puerto Destino, identificación protocolo)

Clasificación de paquetes



Tipos de Procesos

- **-Proceso sin Estado:**
  - El conjunto de posibles opciones (categorías de salida) es siempre el mismo.
  - La opción para un paquete dado depende sólo del contenido del paquete.

- **-Proceso con Estado:**
  - El sistema genera información (p.ej. Un valor numérico obtenido a partir de ciertas operaciones con algunos campos) a partir del paquete que llega.
  - El sistema usa esta información (estado) y la información que contiene el paquete para asignarlo a un flujo.
  - El reordenamiento de los paquetes genera un cambio de flujo (es importante la historia de los paquetes).

Demultiplexación vs. Clasificación

Característica	Demultiplexación	Clasificación
Estado	Siempre sin estado	Con estado/Sin estado
Variables	Globales: las conoce e interpreta igual el Tx y el Rx	No requieren ser globales. Los paquetes a clasificar en los flujos de salida pueden provenir de diferentes fuentes.
Capas	Usa datos de una sola capa	Usa datos de varias capas
Participación del Transmisor	Sí (significado de las variables debe ser el mismo en Tx y Rx)	No (Sólo el receptor toma datos de los campos del paquete sin ponerse de acuerdo con el transmisor)
Conjunto de flujos	Estático (siempre son los mismos protocolos de la capa superior)	Dinámico (los flujos aparecen y desaparecen con las comunicaciones)

Ventajas de la Clasificación

- Tiene la capacidad de eludir el procesamiento por capas
- Introduce la compresión de capas, examinando campos de múltiples capas en un solo paso

MANEJO DE COLAS

La situación

- store and forward:
  - Los routers almacenan los paquetes mientras son procesados y luego los re-envían
- Encolamiento:
  - Políticas, estructuras de datos y algoritmos relacionados con el almacenamiento y selección de los paquetes para el re-envío.

Tipos de colas

- FIFO: First-In-First-Out:
  - Es el caso más simple
  - Debe diseñarse para tener un acceso eficiente
  - Debe notificar al receptor cuando hay paquetes presentes
  - Debe manejar los casos extremos:
    - Cola vacía: No hay paquetes en la cola
    - Cola Llena: No pueden agregarse más paquetes a la cola.
  - El diseñador debe tener en cuenta:
    - Dónde ubicar la cola FIFO?
    - Qué tan larga debe ser la cola?

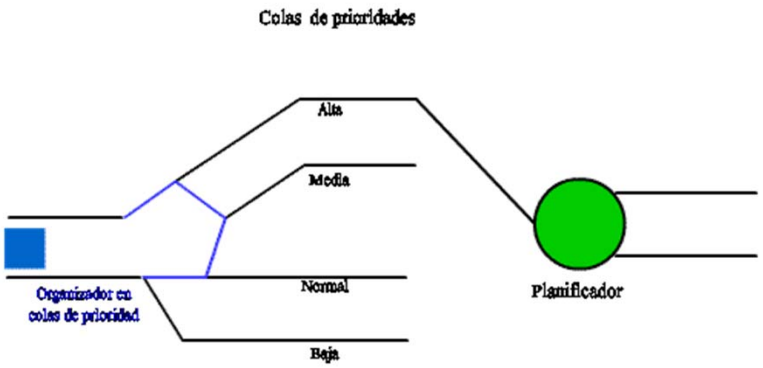
Tipos de colas

- Colas con Prioridades:
  - Son más complejas que la FIFO
  - Se favorecen unos paquetes sobre otros según diferentes criterios
    - Contenido de los paquetes
    - Identidad del orígen
    - Tamaño del paquete

Colas con prioridades

- Ejemplos más usados:
  - Priority Queueing (PQ)
  - Weighted Round Robin (WRR)
  - WFQ (Weighted Fair Queueing)

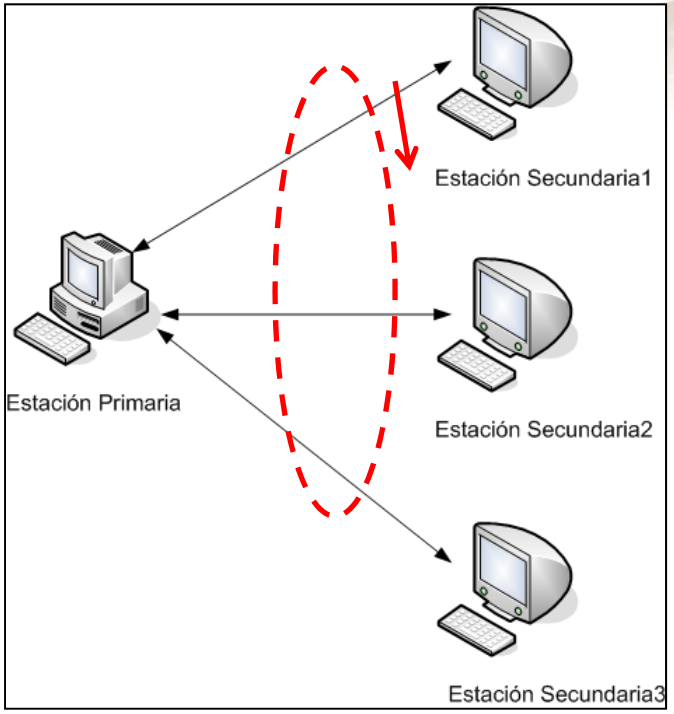
Priority Queueing (PQ)



- Hay varias colas, cada una con una prioridad diferente
- Mientras haya paquetes en una cola de alta prioridad, las demás colas deben esperar.
- **Hambruna:** La cola de menor prioridad podría no ser atendida en mucho tiempo.

Weighted Round Robin (WRR)

- Evita la hambruna
- RR: Round Robin
  - Se asigna a los clientes (flujos) un tiempo de servicio fijo (ranura de tiempo). Si el servicio no se completa durante este intervalo, el cliente (flujo) regresa a la cola, que es de tipo FCFS.
- WRR:
  - A un cliente se pueden asignar varias ranuras de tiempo según la prioridad que posea.
  - A mayor prioridad, más ranuras



WRR

Ventajas

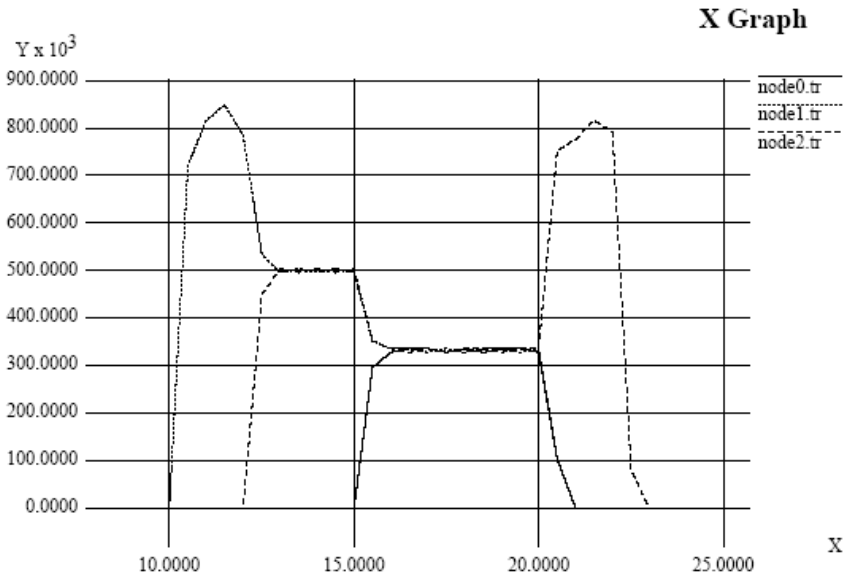
- Aisla las colas
- El tráfico excesivo en una cola no afecta el servicio de las otras

Desventajas

- Cálculos se hacen con base en el tamaño medio del paquete
- Si el tamaño de los paquetes varía mucho con respecto a la media, algunas colas podrían recibir más tiempo de servicio y otras menos de lo debido.

WFQ

- Weighted Fair Queueing: Encolamiento Justo por pesos
- El objetivo es dividir el ancho de banda de un enlace de salida entre los flujos de paquetes existentes de forma *justa*
- Evita la hambruna
- Asigna recursos de manera más precisa que *WRR.*

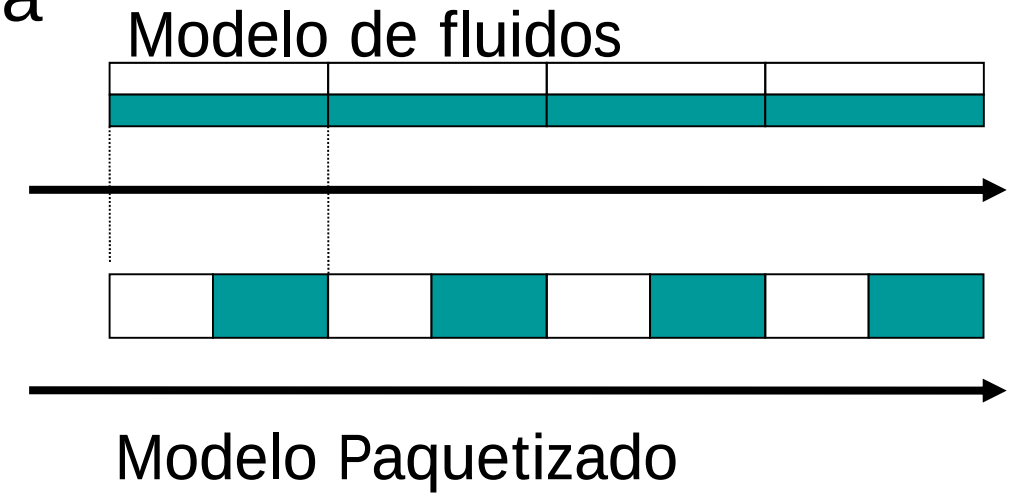


WFQ

- Está basado en el principio usado por GPS (Generalized Processor Sharing).
- La tasa de salida en bps es proporcional al peso asignado a cada flujo

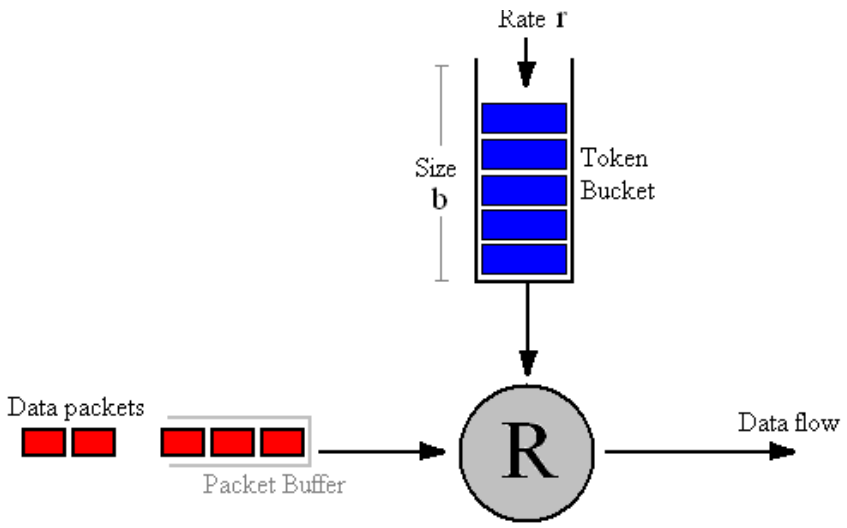
$$R_i = \frac{\phi_i}{\sum_{j=1}^{V} \phi_j} R$$

- GPS es un modelo de fluidos
- Pero se requiere un modelo paquetizado



Modelo paquetizado de WFQ

- PGPS: Packetized Generalized Processor Sharing
- Usa el Token Bucket:



WFQ

Ventajas

- Aisla las colas para evitar hambruna
- Opera sin conocimiento previo de las prioridades del tráfico, ni tampoco el tamaño de los paquetes
- Puede ser usado para garantizar el retardo límite de los paquetes

Desventajas

- Uso de los recursos:
  - Almacena información de estado
  - Requiere cálculos para cada paquete que llega
- No es escalable para un gran número de flujos o tasas de tráfico altas para los agregados de tráfico

DESCARTE DE PAQUETES

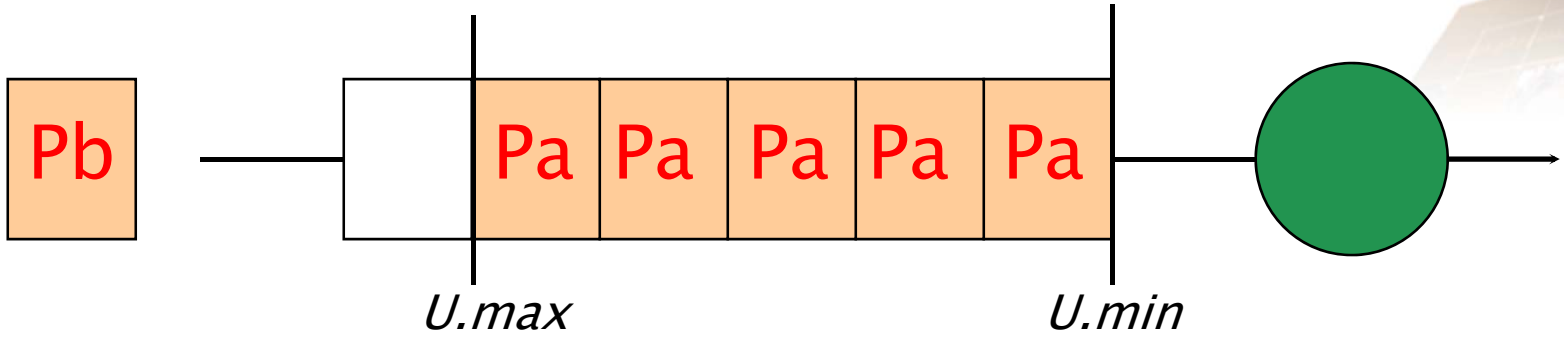
Objetivo

- El problema: Congestión
- Durante la congestión las colas de los routers se acercan a su máximo límite.
- Al llegar las colas a su máximo límite, no se pueden recibir más paquetes y se pierden
- Un método para reducir la congestión es EVITARLA mediante el descarte de paquetes cuando el sistema está cercano a la congestión.

Métodos para evitar la congestión

- Hay métodos básicos:
  - Tail drop:
    - Se desechan los paquetes que llegan cuando la cola está llena.
    - El problema es que se produce el efecto de **sincronización global** con las comunicaciones que usan TCP (por el control de congestió en TCP)
  - RED (Random Early Detection):
    - Después de cierto umbral de longitud de las colas, se desechan paquetes aleatoriamente con cierta probabilidad (a mayor longitud de colas, mayor probabilidad de descarte)
    - Esto evita la Sincronización global

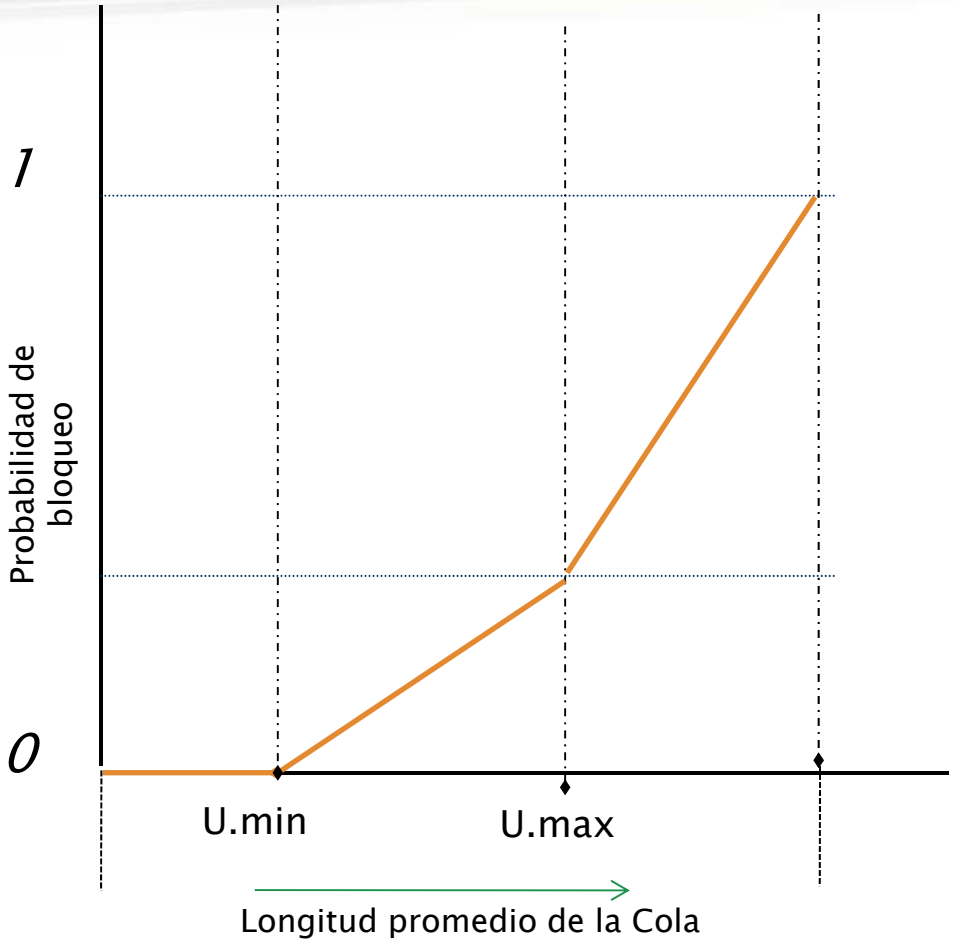
EARLY RANDOM DROP



•Si el tamaño promedio de la cola esta entre el mínimo y el máximo umbral, cada paquete que llegue es marcado con probabilidad *Pa.* Cuando el tamaño promedio de la cola excede el *U.max,* cada paquete que va llegando va siendo marcado con *Pb*.

•Esto reduce la sincronización global.

RED



Según se va aproximando el tamaño medio de la cola al umbral máximo, va bloqueando un número cada vez mayor de paquetes.

Cuando bloquea los paquetes, RED escoge de qué conexiones bloqueará los paquetes de una forma aleatoria.

SLA: Service Level Agreement

- En DiffServ los servicios se definen entre el cliente y el proveedor de servicios con un SLA (Service Level Agreement)
- Partes de un SLA:
  - TCA (Traffic conditioning Agreement)
  - Disponibilidad
  - Seguridad
  - Monitoreo
  - Auditoría
  - Contabilidad
  - Precio
  - Cobro

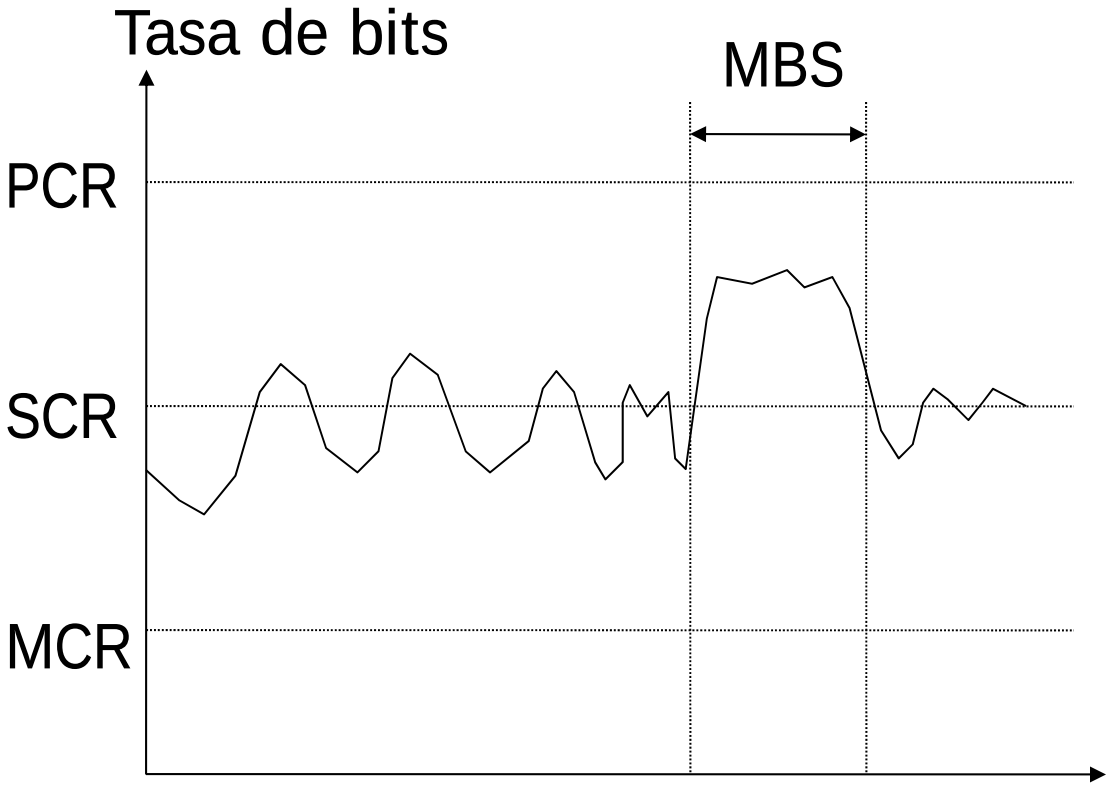
TCA

- Detalla parámetros de servicio para perfiles de tráfico y control de policía.
- Puede incluir:
  - Perfiles de tráfico, tales como parámetros del token bucket (difieren para c/clase)
  - Métricas de desempeño (throughput, retardo, prioridades)
  - Acciones para paquetes no-conformes
  - Servicios de marcación de paquetes y recorte suministrados por el proveedor.

Parámetros de QoS

Parámetro	Siglas	Significado
Tasa celdas pico	PCR	Tasa máxima a la que se enviarán las celdas
Tasa celdas sostenida	SCR	Tasa de celdas promedio a largo plazo
Tasa celdas mín.	MCR	Tasa celdas mínima aceptable
Tolerancia de variac. De retardo celdas	CVDT	Fluctuación de retardo máxima aceptable en las celdas
Tasa perdida celdas	CLR	Fracción de celdas que se pierden o entregan muy tarde
Retardo transf.celda	CTD	Tiempo que lleva la entrega (medio, máximo)
Variac.retardo celda	CDV	Variación tiempo de entrega de celdas
Tasa errores celdas	CER	Fracción celdas entregadas sin error

Parámetros de QoS



MBS: Maximum Burst Size; Cuánto tiempo se Puede trabajar Por encima del SCR

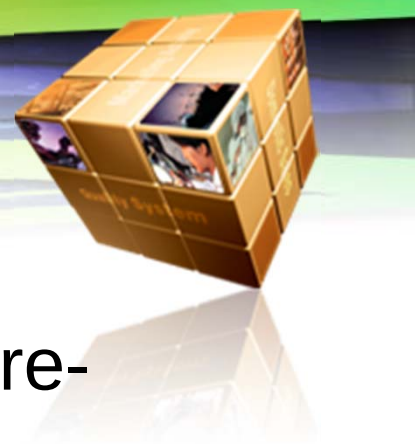
Arquitectura de servicios Diferenciados (DiffServ)

- Se crea un conjunto reducido de clases
- Hay grupos de usuarios
- Pocas clases (AF, EF, BF) manejadas por prioridades
- Ventaja: Escalable
- Requiere:
  - Control de admisión (CAC)
  - Control de Policía (UPC, uso de parámetros)
  - Manejo de troncales con QoS mediante MPLS

Forwarding Classes

- El tráfico en DiffServ se divide en unas pocas clases de re-transmisión (*forwarding classes*):
  - AF (Assured Forwarding)
  - EF (Express Forwarding)
  - BF (Best Effort Forwarding)
- Una clase de re-transmisión representa un tratamiento de re-transmisión predefinido en términos de:
  - Pérdidas de paquetes
  - Asignación de ancho de banda
- El tipo de clase de re-transmisión se codifica en un campo de la cabecera del paquete IP.

Tratamientos de retransmisión (Forwarding Classes)



- En DiffServ se definen tratamientos de re-transmisión y no servicios End-to-End.
- Los servicios pueden ser construidos combinando clases de re-transmisión y control de admisión.
- En IntServ se definen servicios (garantizado, carga controlada). El tratamiento de los paquetes no es parte de los estándares.

Confusión

- Suele confundirse el concepto de Servicio y el de Tratamiento de retransmisión
- *Tratamiento de retransmisión:* Se refiere a comportamientos de algoritmos implementados en los nodos.
- *Servicio:* Se refiere al desempeño total que un tráfico de un cliente tiene.
- Los tratamientos de retransmisión son la base para construir servicios.

Ejemplo

- Un tratamiento de retransmisión es el denominado *express forwarding*.
- *Express forwarding* es el tratamiento de los paquetes con prioridades (paquetes con prioridad alta se retransmiten primero que los de prioridad baja).
- Supongamos un servicio denominado *no-loss service*. Este garantiza a los clientes que no hay pérdidas de paquetes.

Ejemplo

Servicio	**Tratamiento de retransmisión usado**
No-loss service	Express forwarding (alta prioridad) + control de admisión (limita el número de paquetes de alta prioridad)
No-loss service	FCFS queuing + una red con recursos suficientes para atender todas las demandas de tráfico

Servicios vs. tratamientos

- No necesariamente hay una correspondencia 1 a 1.
- Un servicio cambia en el tiempo dependiendo de las demandas del mercado.
- Un tratamiento de retransmisión se implementa en los nodos y no es fácilmente cambiable.
- Los tratamientos de retransmisión envuelven acciones limitadas: marcado, recorte, reordenamiento.

Per-Hop Behaviors (PHBs)

- En DiffServ se le llama PHB al tratamiento de retransmisión externamente observable en un nodo.
- Cada PHB se codifica con un valor de 6 bits llamado DSCP (Differentiated Services code point).
- Todos los paquetes con el mismo codepoint pertenecen a un *agregado de comportamiento (behavior aggregate)*, y todos ellos reciben el mismo tratamiento.

DiffServ en IPv4

Campo TOS (Type of Service) de IPv4

Precedencia	D	T	R	0	0

Definición del campo *IP TOS*.

Bit	Descripción
0-2	Precedencia
3	0 = Retardo Normal 1 = Retardo Bajo
4	0 = Tasa de Transferencia Normal 1 = Tasa de Transferencia Alta
5	0 = Confiabilidad Normal 1 = Confiabilidad Alta
6-7	Reservado para uso futuro

Campo DSCP de DiffServ

DSCP	CU

- El estándar de *Servicios Diferenciados* redefine el campo existente *IP TOS* para indicar los *Comportamientos de Re-Transmisión*.
- El nuevo campo, denominado *DS* (*Differentiated Services*), vuelve obsoletas las definiciones existentes del octeto *TOS* y también el octeto *Clase de Tráfico* de *IPv6*.
- Los primeros 6 bits del campo *DS* son usados como un *DSCP* (*Differentiated Services Code Point*), es decir, un valor que se utiliza para codificar el *PHB* con que debe tratarse un paquete en cada nodo *DiffServ.*
- Los restantes dos bits (campo *CU*) no están siendo utilizados actualmente.

Per-Hop Behaviors (PHBs)

- Los PHBs son usados como bloques constitutivos para brindar asignación de servicios para diferentes servicios.
- Los servicios E2E pueden ser construidos combinando diferentes PHBs con acondicionamiento de tráfico y suministro de la red.
- Un PHB podría, por ejemplo, garantizar un mínimo de BW para un agregado de comportamiento.

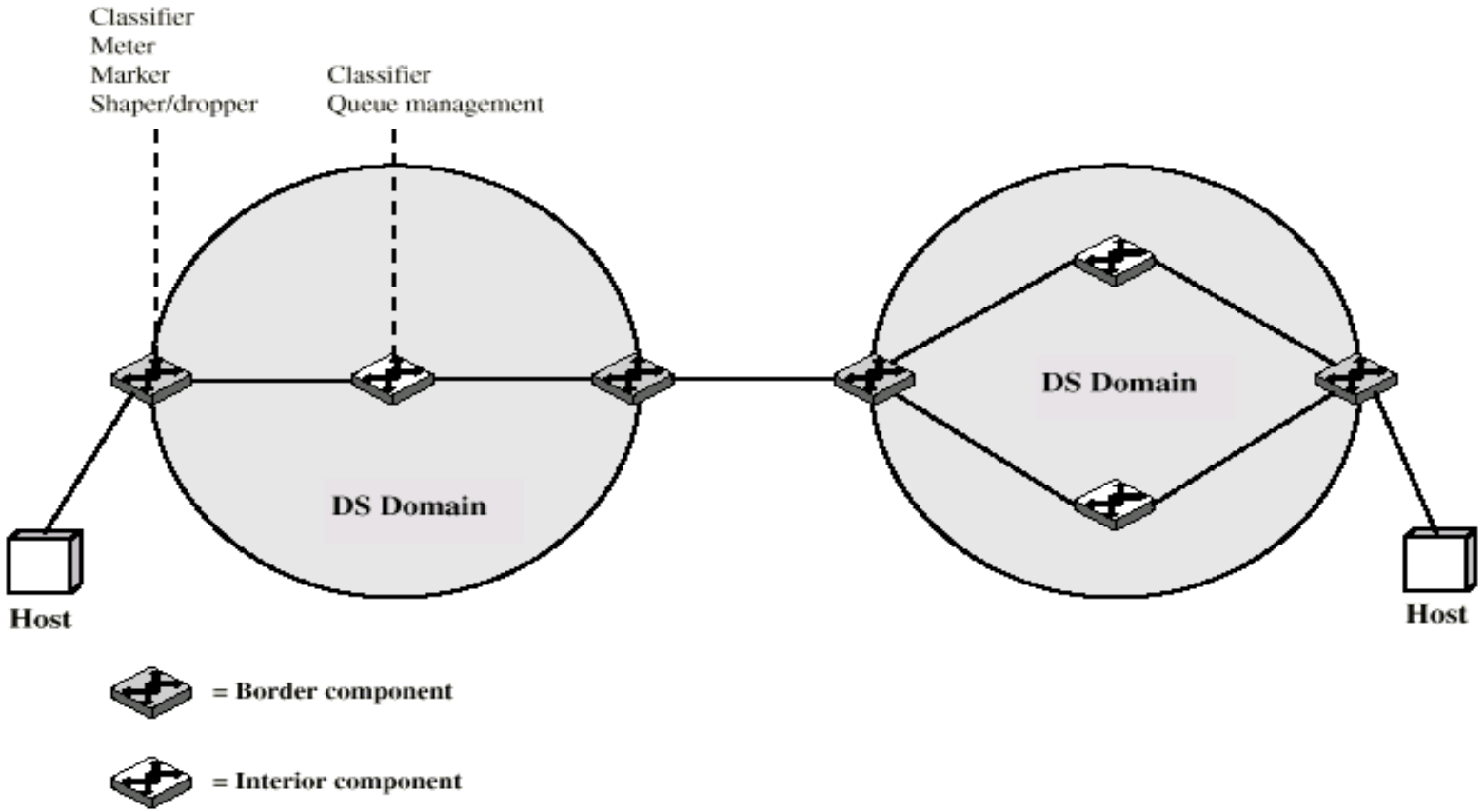
Per-Hop Behaviors (PHBs)

- Un PHB se implementa típicamente mediante la gestión de un buffer y la planificación de paquetes.
- Para un PHB particular, pueden usarse una variedad de mecanismos para obtener el mismo tratamiento de retransmisión.

Grupo PHB

- Un conjunto de PHBs podría formar un *grupo PHB*.
- Un grupo PHB es un conjunto de PHBs que comparten una restricción común (p.ej. probabilidad de pérdida o ancho de banda).
- Si en un mismo dominio DS existen varios grupos PHB, es necesario especificar la relación entre ellos.

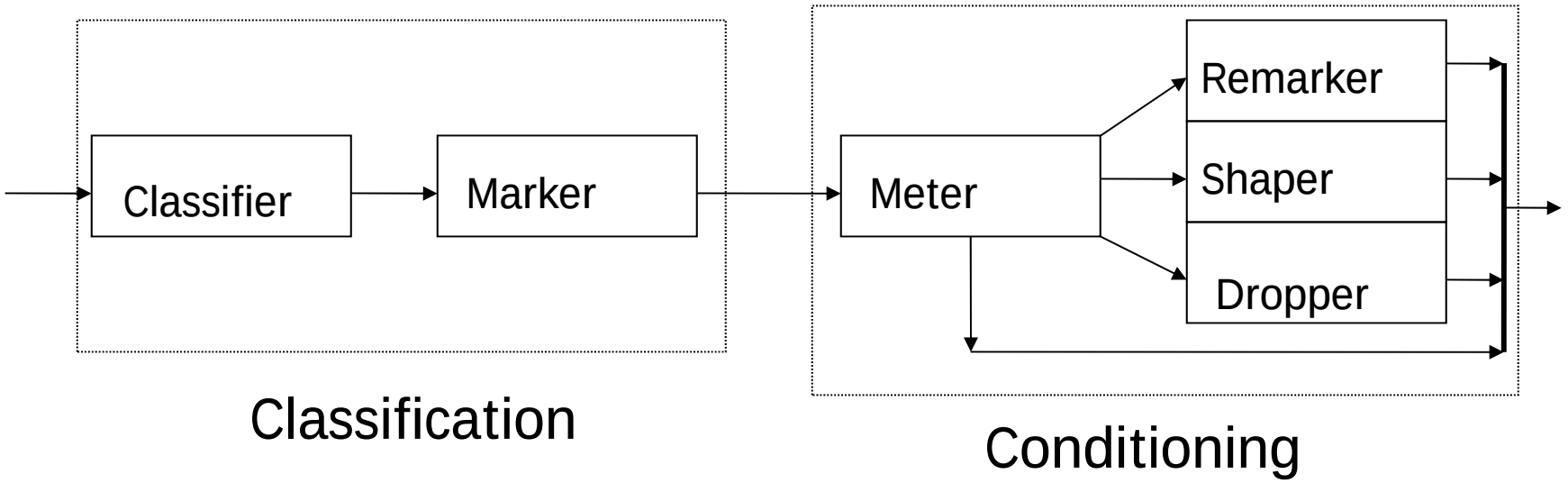
Arquitectura de una red DiffServ



Nodos Frontera y Nodos Interiores

- Funciones nodos frontera:
  - Mapeo de los paquetes a una de las clases de retransmisión soportadas en la red.
  - Asegurar que el tráfico está conforme al SLA para ese cliente específico.
- Una vez los paquetes pasan los nodos frontera hacia el interior de la red, la asignación de recursos en los Nodos Interiores es hecha con base en las clases de retransmisión.

Componentes de un nodo frontera



Componentes de un Nodo Frontera

Elemento	Función
Clasificador	Divide el flujo de paquetes entrante en múltiples grupos basándose en reglas predefinidas
Medidor (Meter)	Compara el flujo de tráfico de un cliente con su perfil de tráfico. Los paquetes que cumplen el perfil se dejan ingresar directo a la red. Los paquetes que no cumplen deben pasar por el acondicionamiento (marking, shaping, dropping)
Marcador (Marker)	Fija el campo DSCP (codepoint) a un valor particular. Así se incluye el paquete en una clase de retransmisión. Los paquetes marcados como no conformes podrían ser desechados por la red ante congestión.
Recortador (Shaper)	Un recortador no permite que el paquete pase hacia la red hasta que cumpla con el perfil de tráfico (retarda los paquetes)
Desechador (Dropper)	Desecha los paquetes no cumplientes con el perfil de tráfico

Clasificador

- **Función**: Divide el flujo de paquetes entrante en múltiples grupos basándose en reglas predefinidas.
- Hay dos tipos:
  - BA (Behavior Aggregate)
  - MF (Multifield)

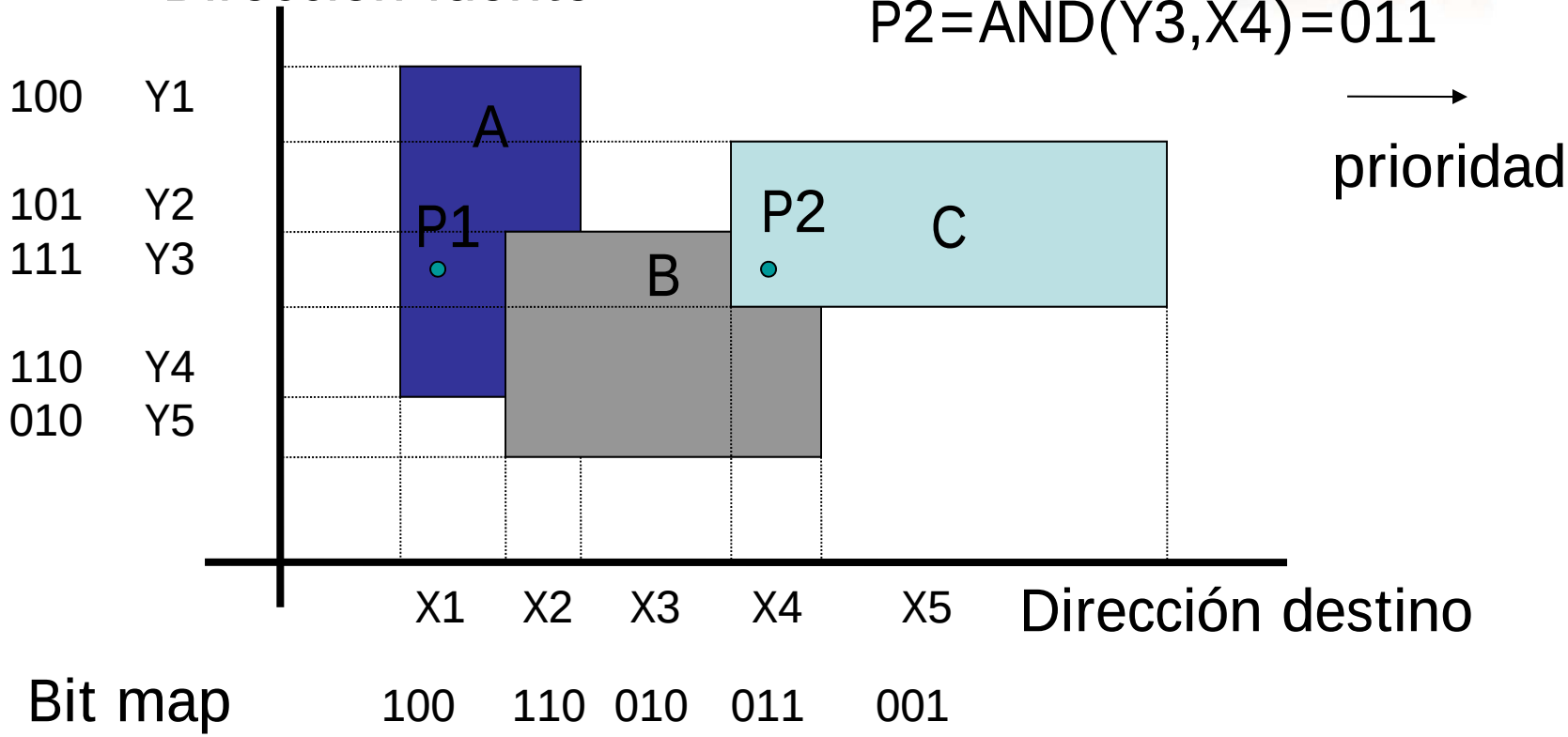
Clasificador BA

- Es el más simple
- Selecciona los paquetes basándose únicamente en el codepoint (DSCP).
- Para que esto funcione se requiere que los paquetes sean marcados (puesto el codepoint en un valor) antes de ingresar al clasificador.
- Dónde se marcan los paquetes?
  - Son marcados por la fuente
  - O Son marcados por el router de primer salto en la LAN
  - También podría hacerlo el mismo ISP

Clasificador MF

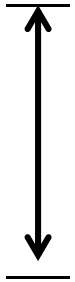
- Usa una combinación de uno o más campos de la quíntupla (dir.dest., dir. Orig.,pto orig, pto dest, id.protoc) en la cabecera del paquete para hacer la clasificación.
- Casos:
  - Marca paquetes con base en los tipos de aplicación (puertos). Ej: Telnet, FTP.
  - Marca paquetes con base en direcciones particulares de origen, destino o prefijos de red.
- Es más versátil pero es más complejo que el BA ya que es un problema multidimensional, mientras que el BA sólo clasifica por un parámetro (codepoint).

Clasificación MF



Acondicionador de tráfico

- Realiza funciones de policía de tráfico para asegurar el TCA entre clientes e ISP.
- Consiste de 4 elementos:
  - Medidor (Meter)
  - Marcador (Marker)
  - Recortador (Shaper)
  - Desechador (Dropper)

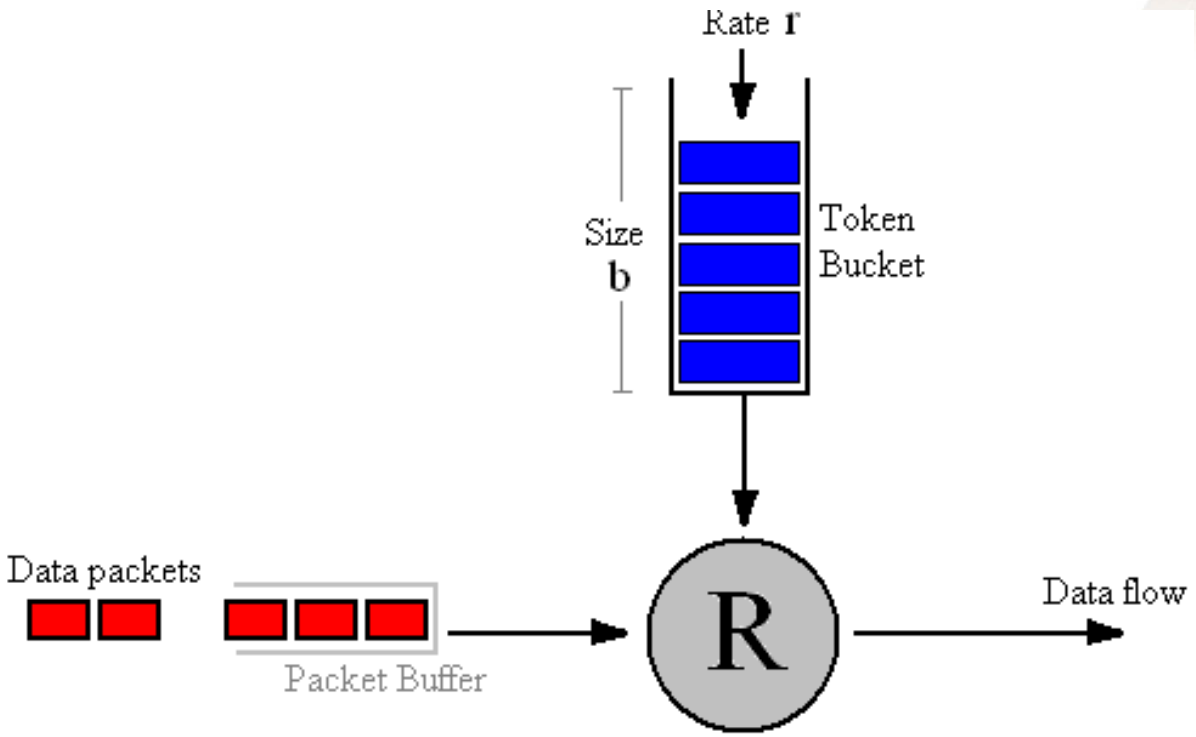


Acciones sólo para paquetes no conformes

Medidor (Meter)

- Compara el flujo de tráfico de un cliente con su perfil de tráfico.
- Los paquetes que cumplen el perfil se dejan ingresar directo a la red.
- Los paquetes que no cumplen deben pasar por el acondicionamiento (marking, shaping, dropping).
- La mayoría de medidores son implementados con Token Bucket, ya que los perfiles son descritos en los términos de este algoritmo.

Medición de tráfico conToken Bucket



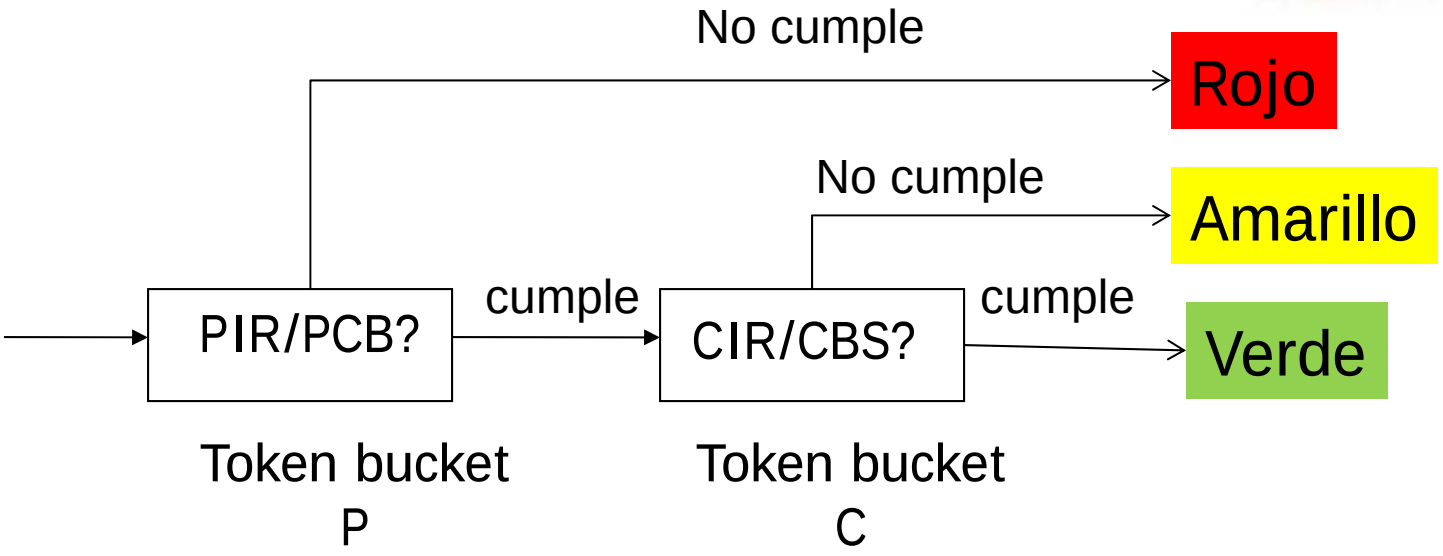
Marcador

- Fija el campo DSCP (codepoint) a un valor particular. Así se incluye el paquete en una clase de retransmisión.
- Podrían marcar paquetes no marcados o re-marcar paquetes ya marcados.
- También marcan paquetes no conformes con un valor especial de codepoint para indicar su no-conformidad.
- Los paquetes marcados como no conformes podrían ser desechados por la red ante congestión.

Marcador

- ¿Cuándo se re-marcan los paquetes?
  - Cuando hay cambio de dominio DS y en el nuevo dominio son paquetes no conformes.
  - Cuando hay cambio de dominio DS y hay diferentes codepoints en el nuevo dominio.
- Casos de cambio de PHB:
  - *Degradación de PHB*: El nuevo PHB es peor que el anterior (caso más común)
  - *Promoción de PHB:* El nuevo PHB es mejor que el anterior

Marcado de paquetes con Dual token algorithm



Recortador (Shaper)

- **Función:** Retarda los paquetes no-conformes hasta que cumplen con el perfil de tráfico.
- Un marcador sólo marca los paquetes pero los deja seguir a la red.
- Un recortador no permite que el paquete pase hacia la red hasta que cumpla con el perfil de tráfico.
- Puede requerirse un recortador al cambiar de dominio DS. El nodo de egreso debería recortar el tráfico para que cumpla con el perfil de tráfico apropiado para el siguiente dominio DS.

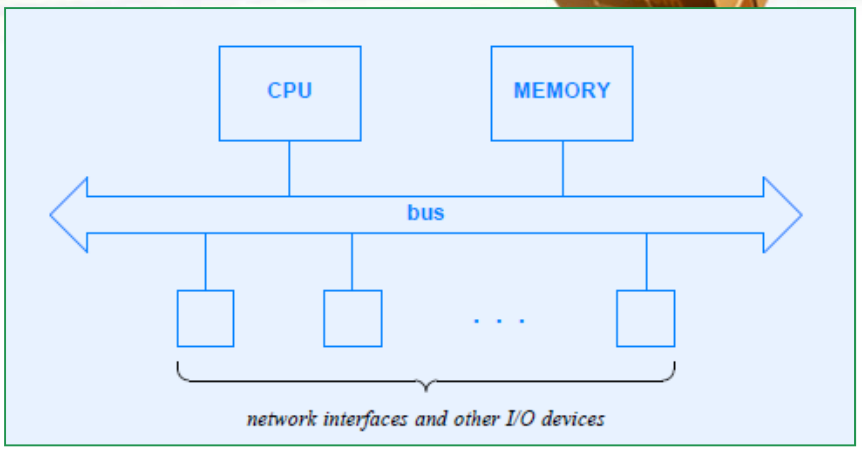
Desechador (Dropper)

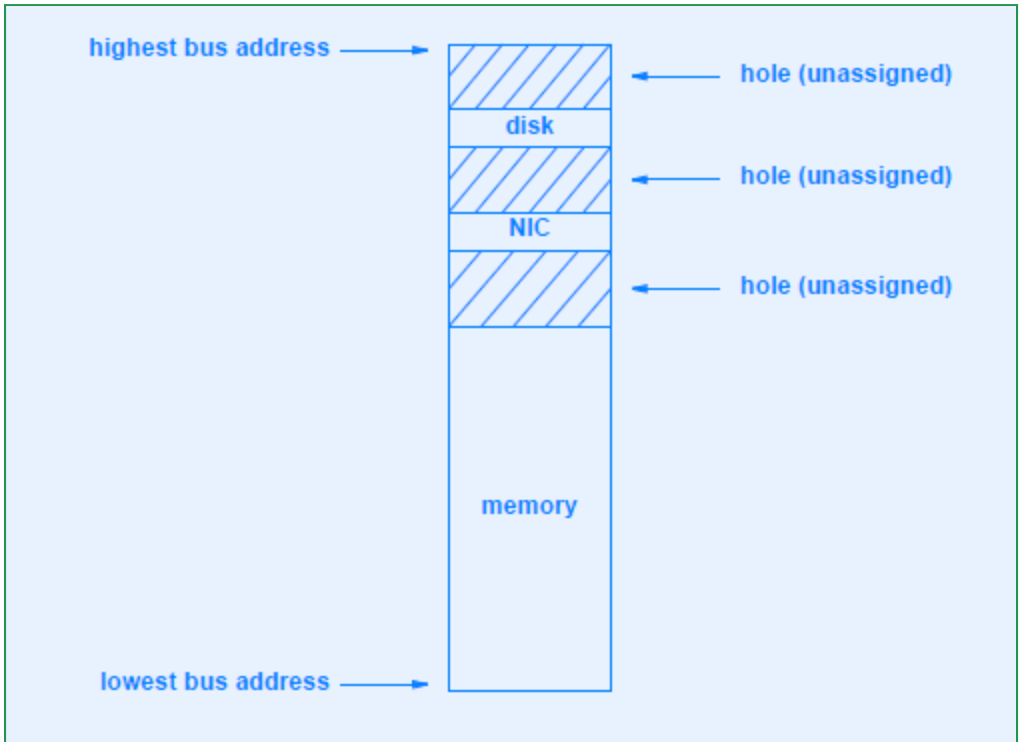
- Desecha los paquetes no cumplientes con el perfil de tráfico
- Es más fácil de implementar que un shaper, pues no requiere un buffer mientras que el shaper sí.

Evolución del Hardware de los Routers

1ª Generación de Routers

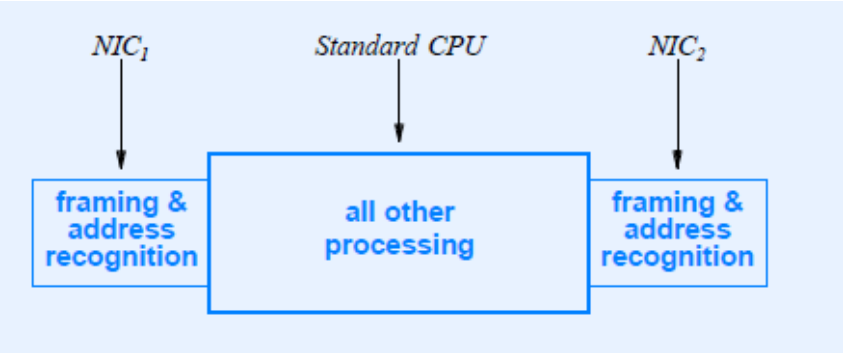
- Hasta los 80´s
- Arquitectura Von Neumann:
  - CPU
  - Periféricos (I/O), incluyen las Tarjetas de Red (NIC-Network Interface Card)
  - Memoria compartida
  - Sistemas de buses para comunicación I/O, memoria, CPU
  - Todo el procesamiento lo hace la CPU





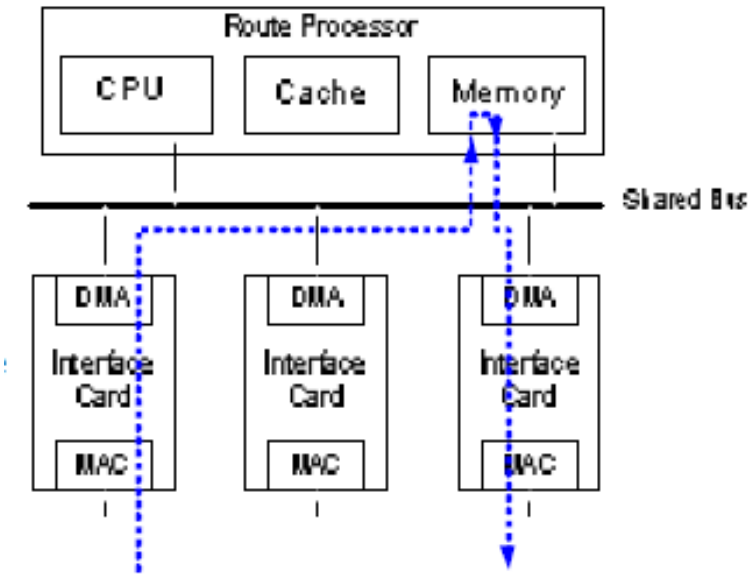
Procesamiento de Protocolos en Routers de 1ª Generación

- Un procesador de propósito general maneja la mayoría de tareas
- NICs: Entramado y reconocimiento de direcciones
- Es adecuado para sistemas de bajas velocidades



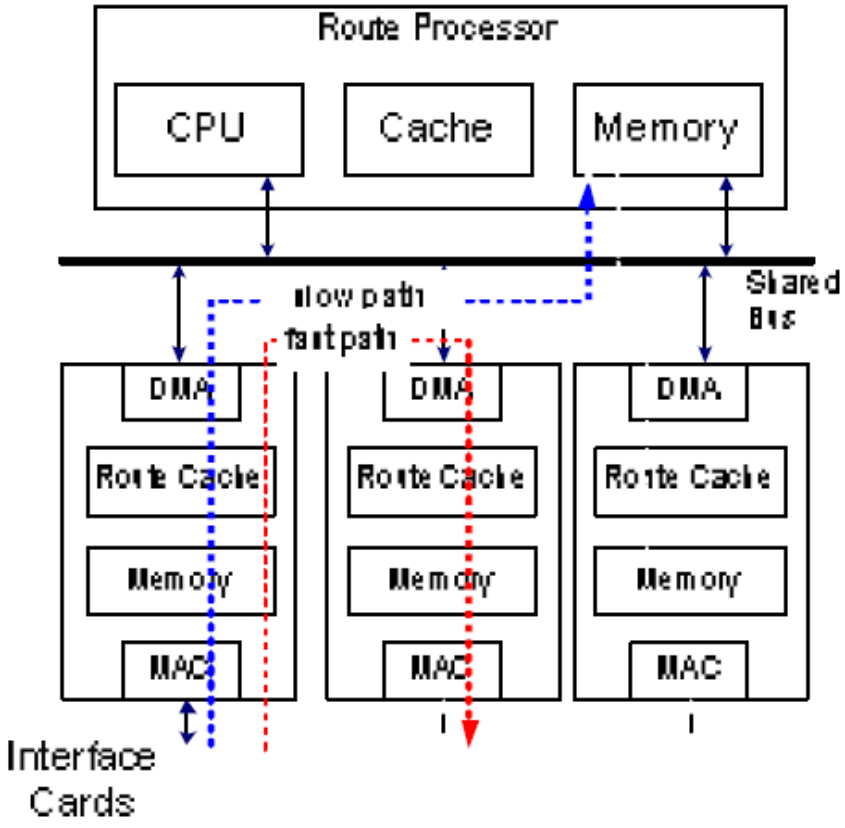
2ª Generación de Routers

- Primera mitad de los años 90s
- Se delegan funciones a las NICs
- Los paquetes que se reciben se envían a la memoria mediante DMA (Direct Memory Access)
- Buses de datos y direcciones compartidos
- CPU central tiene funciones de re-envío de paquetes
- El caché de memoria en la CPU puede acelerar la búsqueda de direcciones
- Desventajas:
  - Rendimiento del re-envío está limitado por la CPU
  - La capacidad del bus compartido limita el número de NICs que se pueden conectar



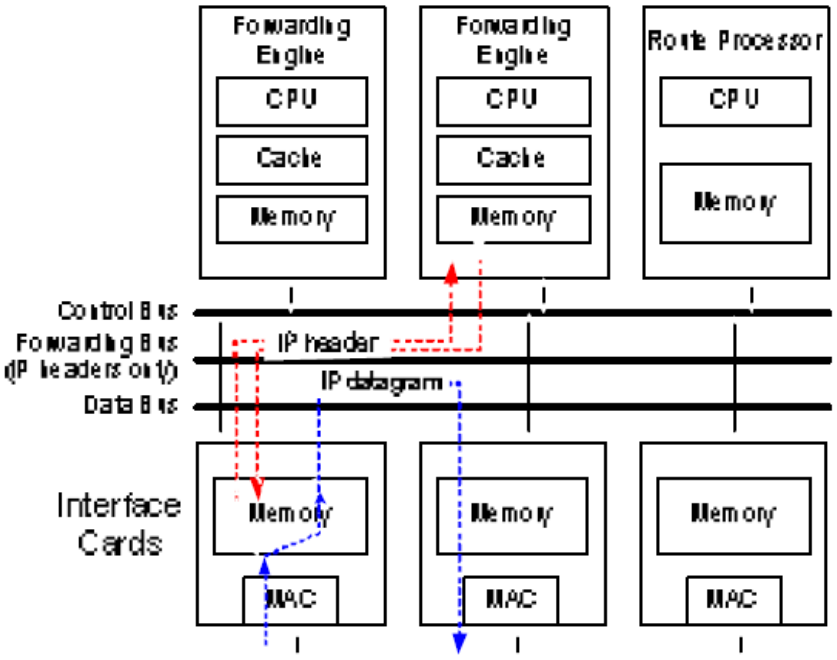
Routers 2ª Generación

- Posibles caminos:
  - **Camino rápido:** Los paquetes que se encuentran en el caché de la NIC de entrada se re-envían directamente a la NIC de salida sin pasar por el procesador.
  - **Camino lento:** Los paquetes que no están en el caché de la NIC de entrada, deben pasar por la CPU para su análisis.



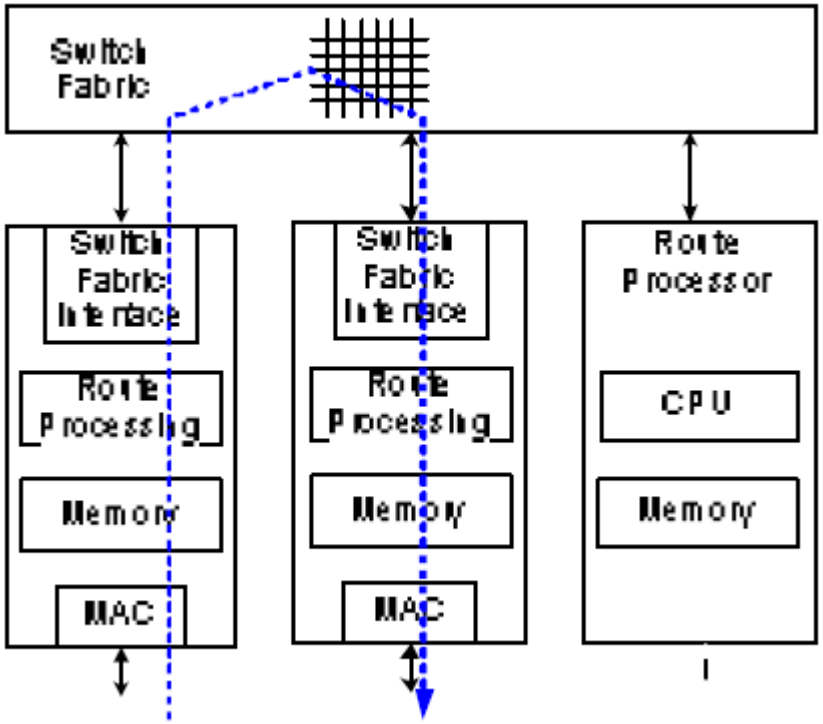
2ª Generación: Uso de Motores de Re-transmisión

- Los paquetes recibidos por una interfaz:
  - Se almacenan en la memoria local de la NIC
  - Se les extrae la cabecera IP
  - La cabecera IP se envía a un motor de re-transmisión
- Funciones del motor de re-transmisión:
  - Búsqueda de direcciones en la tabla de enrutamiento
  - Actualización de la cabecera IP
  - Envío de la cabecera IP a la interfaz de entrada nuevamente
- Los paquetes son reconstruidos en la NIC de entrada y se envían a la NIC de salida.



3ª Generación de Routers

- Segunda mitad de los 90s
- Se usa un conmutador de alta velocidad (p.ej. Conmutador Crossbar)
- Las NIC operan independientemente
- No hay procesamiento centralizado para la re-transmisión de paquetes IP
- Utilizan una arquitectura distribuida
- Agregan cientos de NICs y obtienen velocidades de 1Tbps



Arquitecturas de Hardware

- Router tradicional por software: Router con una sola CPU
- Router con procesadores en paralelo (paralelismo a nivel de instrucción)
- Router con múltiples procesadores idénticos y múltiples tareas: uso de Unix.
- Sistema Asimétrico: Router con múltiples procesadores, cada uno con tareas especializadas
- Sistema con Co-procesadores de propósito especial
- Sistemas con un procesador y varias tarjetas de red
- Líneas de procesamiento de paquetes (Data Pipelines)

Otras estrategias

- Cambiar los protocolos para tener:
  - Tamaño de paquete fijo (celda de ATM)
  - Direccionamiento relativo (ATM, FR, MPLS) en lugar de direccionamiento absoluto (IP)