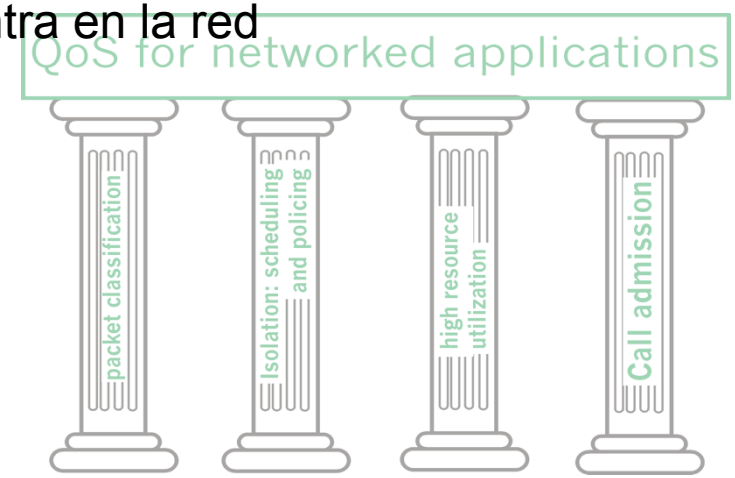
Clasificación, marcado, CAC policing y shaping

Área de Ingeniería Telemática
http://www.tlm.unavarra.es

Máster en Comunicaciones

Resumen anterior

- *Best Effort / IntServ / DiffServ*
- *Connection Admission Control (CAC)*
  - *¿Puede la red cursar el nuevo flujo de tráfico manteniendo los parámetros de QoS ofrecidos a todos los usuarios?*
- Planificación de recursos (*scheduling*)
  - El recurso normalmente es el enlace
  - ¿Cómo organizar a los paquete que deben enviarse?
  - ¿Dar prioridades? ¿Repartir la capacidad?
- *Traffic shaping* y *policing*
  - Marcar, descartar o retrasar el tráfico en exceso
- Monitorización
  - Analizar la cantidad de tráfico que entra en la red
- *QoS routing / Traffic Engineering*
- Clasificación
  - ¿Cómo distinguir entre flujos?
- Gestión de cola
  - ¿Qué paquetes tirar si se llena?



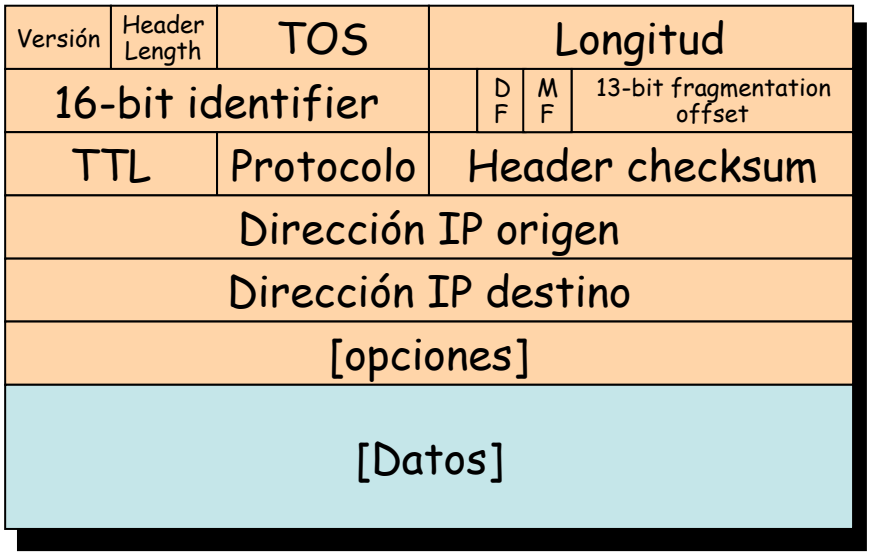
Objetivos

- Conocer los mecanismos de clasificación y marcado
- Conocer mecanismos de policing y shaping

Clasificación y marcado

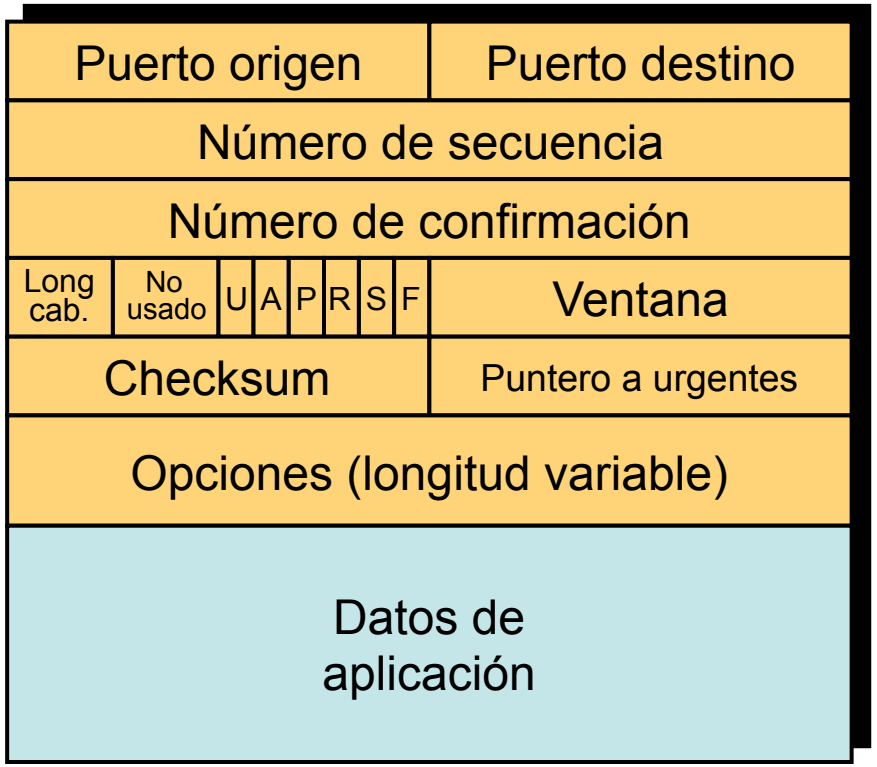
Identificación/clasificación de flujos

- En IPv4 (layer 3) la clasificación se suele hacer por:
  - Dirección IP de origen, dirección IP de destino
  - Protocolo de transporte utilizado (TCP o UDP)
- (...)



Identificación/clasificación de flujos

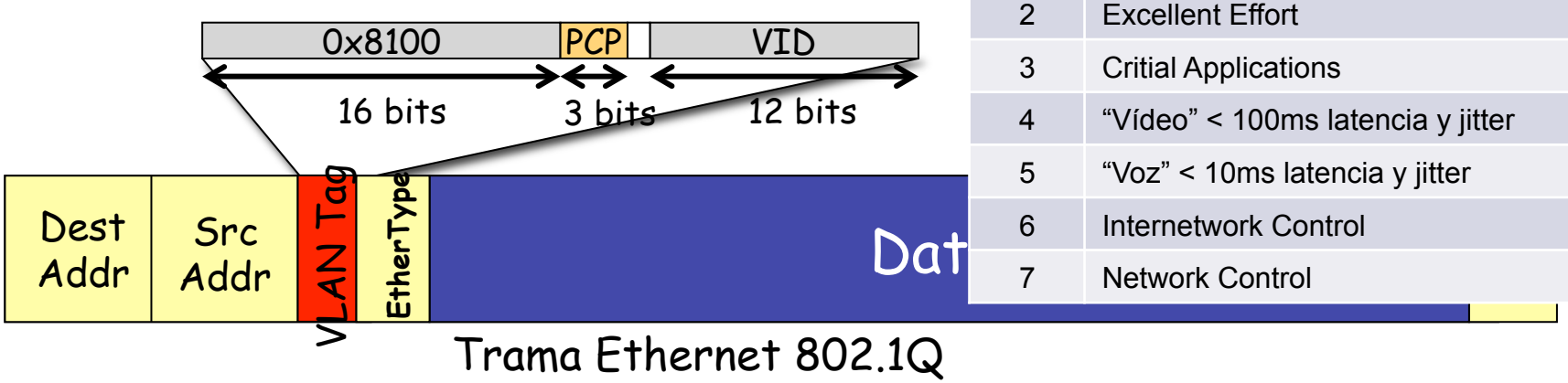
- En IPv4 (layer 3) la clasificación se suele hacer por:
  - Dirección IP de origen, dirección IP de destino
  - Protocolo de transporte utilizado (TCP o UDP)
- Puede incluir parámetros de nivel de transporte (puertos)
- Fragmentos IP pierden cabecera nivel 4 y se vuelven best effort
- (...)



Identificación/clasificación de flujos

- En IPv4 (layer 3) la clasificación se suele hacer por:
  - Dirección IP de origen, dirección IP de destino
  - Protocolo de transporte utilizado (TCP o UDP)
- Puede incluir parámetros de nivel de transporte (puertos)
- Fragmentos IP pierden cabecera nivel 4 y se vuelven best effort
- O información nivel físico (interfaz de entrada, PVC, etc)
- O de nivel de enlace
  - Ethernet: VLAN, direcciones MAC, Ethertype, bits de prioridad
  - (...)

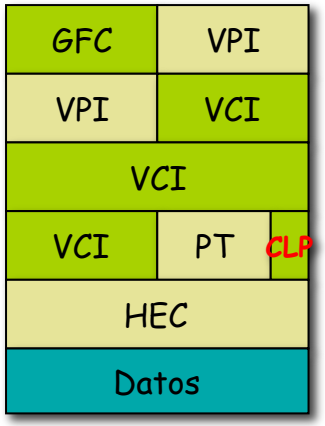
PCP	Tráfico recomendado (802.1Q-2005 Tabla G-2)
0	Best Effort
1	Background
2	Excellent Effort
3	Critial Applications
4	“Vídeo” < 100ms latencia y jitter
5	“Voz” < 10ms latencia y jitter
6	Internetwork Control
7	Network Control



Trama Ethernet 802.1Q

Identificación/clasificación de flujos

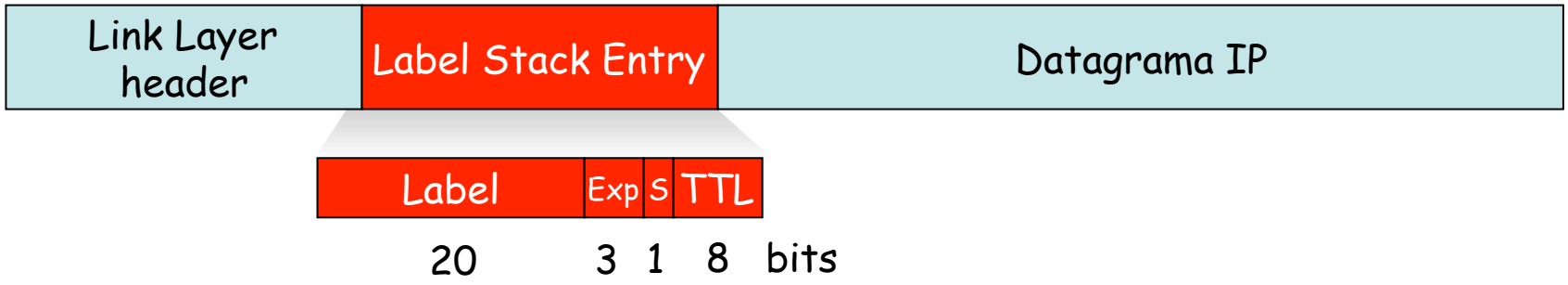
- En IPv4 (layer 3) la clasificación se suele hacer por:
  - Dirección IP de origen, dirección IP de destino
  - Protocolo de transporte utilizado (TCP o UDP)
- Puede incluir parámetros de nivel de transporte (puertos)
- Fragmentos IP pierden cabecera nivel 4 y se vuelven best effort
- O información nivel físico (interfaz de entrada, PVC, etc)
- O de nivel de enlace
  - Ethernet: VLAN, direcciones MAC, Ethertype, bits de prioridad
  - ATM: VPI/VCI, bit CLP
  - (...)



Celda ATM UNI

Identificación/clasificación de flujos

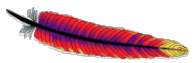
- En IPv4 (layer 3) la clasificación se suele hacer por:
  - Dirección IP de origen, dirección IP de destino
  - Protocolo de transporte utilizado (TCP o UDP)
- Puede incluir parámetros de nivel de transporte (puertos)
- Fragmentos IP pierden cabecera nivel 4 y se vuelven best effort
- O información nivel físico (interfaz de entrada, PVC, etc)
- O de nivel de enlace
  - Ethernet: VLAN, direcciones MAC, Ethertype, bits de prioridad
  - ATM: VPI/VCI, bit CLP
  - MPLS: Label, Exp bits
- (…)



Identificación/clasificación de flujos

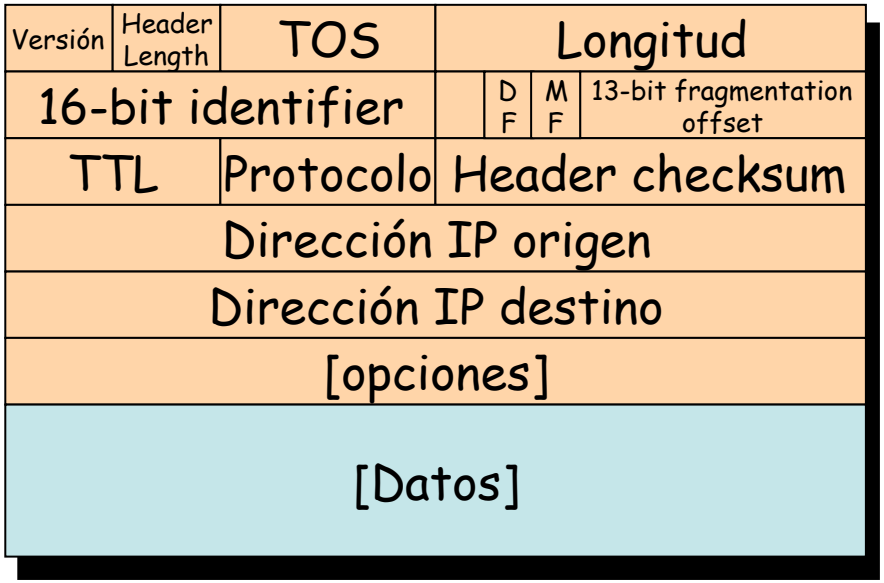
- En IPv4 (layer 3) la clasificación se suele hacer por:
  - Dirección IP de origen, dirección IP de destino
  - Protocolo de transporte utilizado (TCP o UDP)
- Puede incluir parámetros de nivel de transporte (puertos)
- Fragmentos IP pierden cabecera nivel 4 y se vuelven best effort
- O información nivel físico (interfaz de entrada, PVC, etc)
- O de nivel de enlace
  - Ethernet: VLAN, direcciones MAC, Ethertype, bits de prioridad
  - ATM: VPI/VCI, bit CLP
  - MPLS: Label, Exp bits
- O de nivel de aplicación (URL, MIME type, etc) usando DPI (*Deep Packet Inspection)* y SI (*Stateful Inspection*)

```
GET /~daniel/index.html HTTP/1.1
Host: www.tlm.unavarra.es
User-agent: Mozilla/4.0
Connection: close
Accept-language:es
```



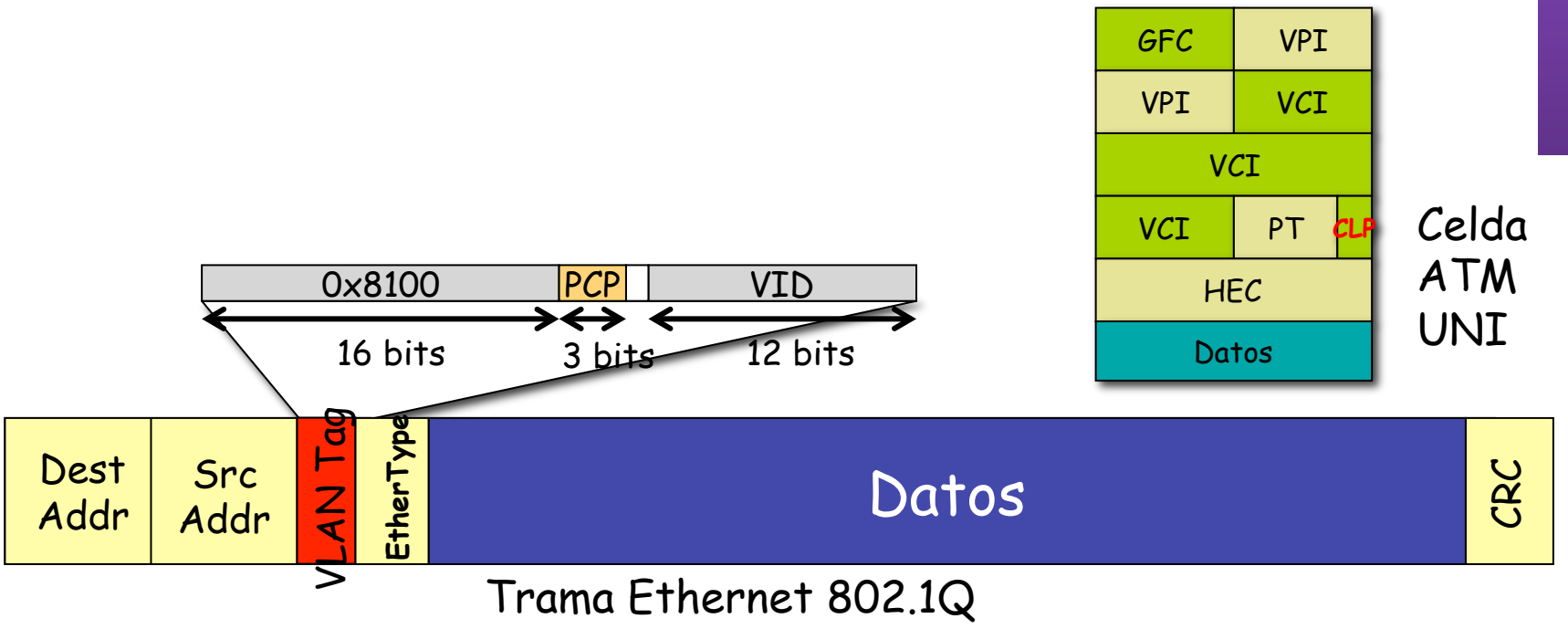
Marcado

- Marcar al paquete como perteneciente a un flujo o a una clase
- En base a la clasificación
- Simplifica la clasificación a partir de ese punto
- En IPv4 usar los bits de TOS (renombrados para DiffServ)
- (...)



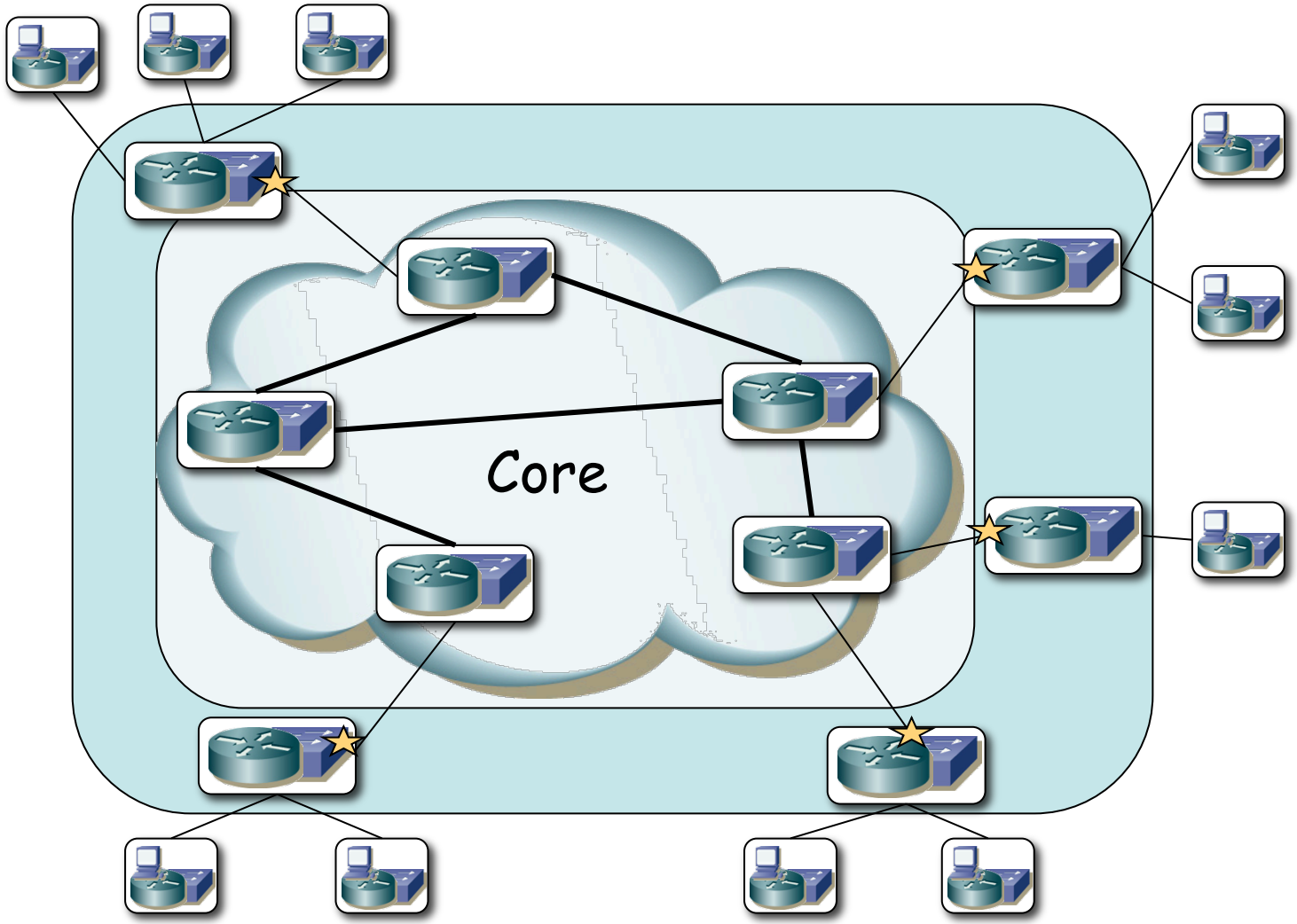
Marcado / Coloreado

- Marcar al paquete como perteneciente a un flujo o a una clase
- En base a la clasificación
- Simplifica la clasificación a partir de ese punto
- En IPv4 usar los bits de TOS (renombrados para DiffServ)
- En trama 802.1Q en los bits de prioridad
- En celda ATM en bit CLP



¿ Dónde = Quién ?

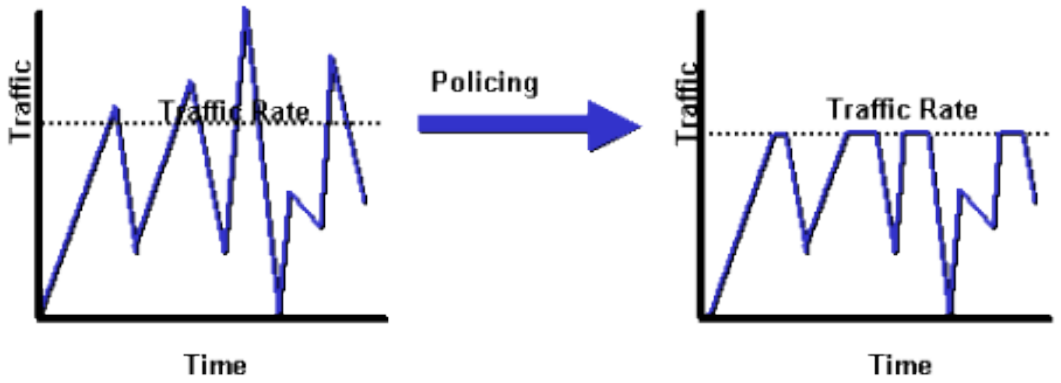
- Preferiblemente en los extremos (edge) de la red
- O en los propios generadores de los paquetes (ej. Teléfono IP)



Policing and Shaping

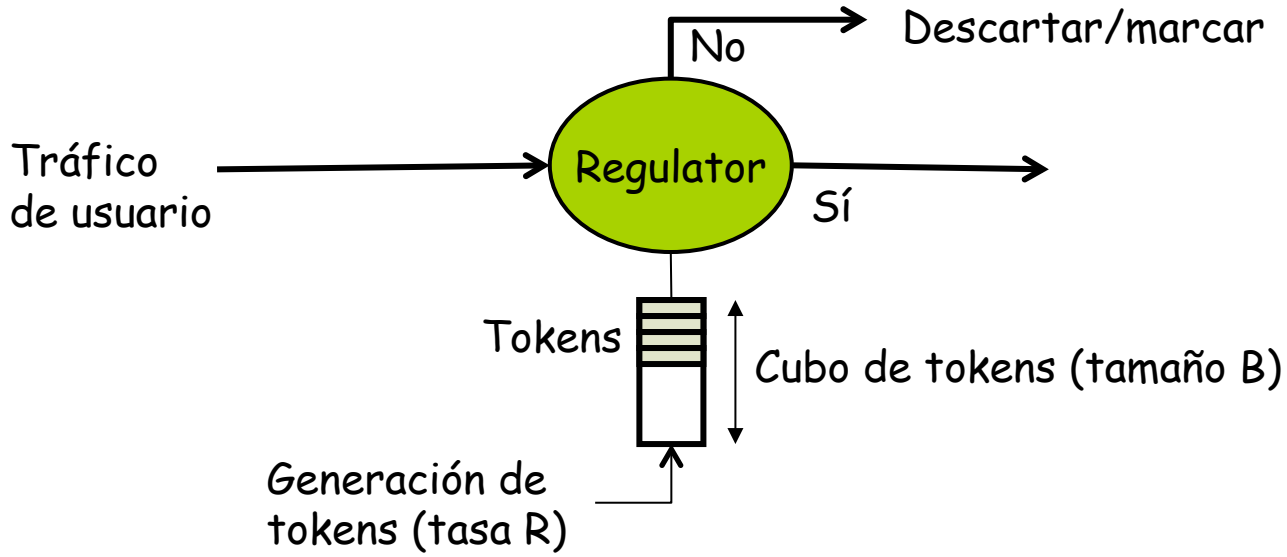
Policing

- **Objetivo**: Limitar el tráfico a la entrada a la red para que no exceda el declarado
- Su objetivo es un flujo o un agregado de flujos
- Los que excedan lo contratado (*nonconforming*) se descartan o marcan (*conditional marker*)
- No introduce delay o jitter adicional al tráfico que se acepta
- Características del tráfico
  - Tasa media (media a largo plazo)
  - Tasa de pico
  - Tamaño máximo de ráfaga: máx nº paquetes a tasa de pico



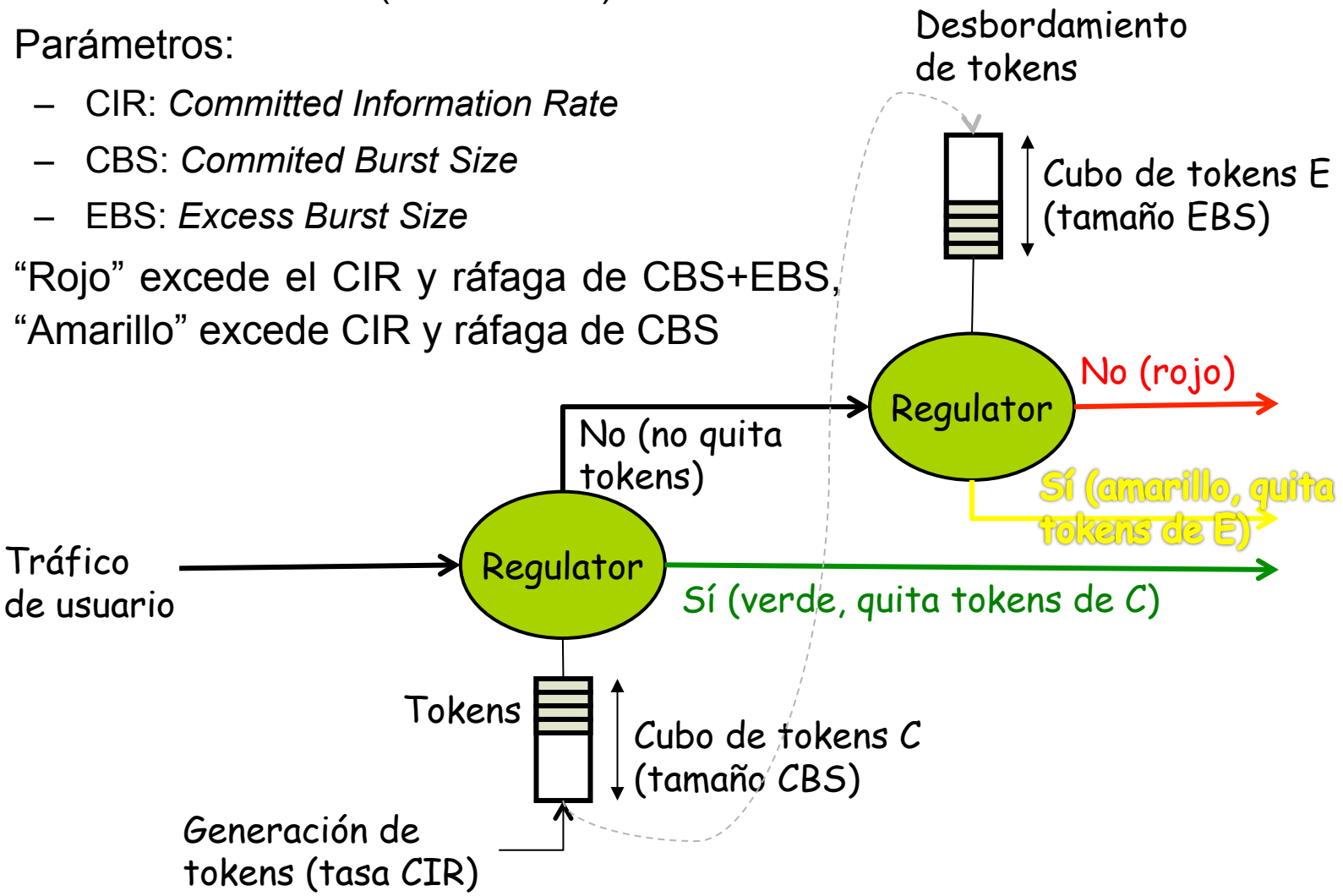
Token Bucket

- *One-rate token bucket policer*
- Tasa de llegada de tokens R
- Tamaño máximo del cubo de tokens B
- Llega un paquete te tamaño b
- ¿Hay al menos b tokens en el cubo?
  - Sí: paquete “conforme” al contrato. Retirar b del cubo
  - No: paquete “no conforme” al contrato. Descartar/marcar
- No retrasa el tráfico, el buffer es para los tokens



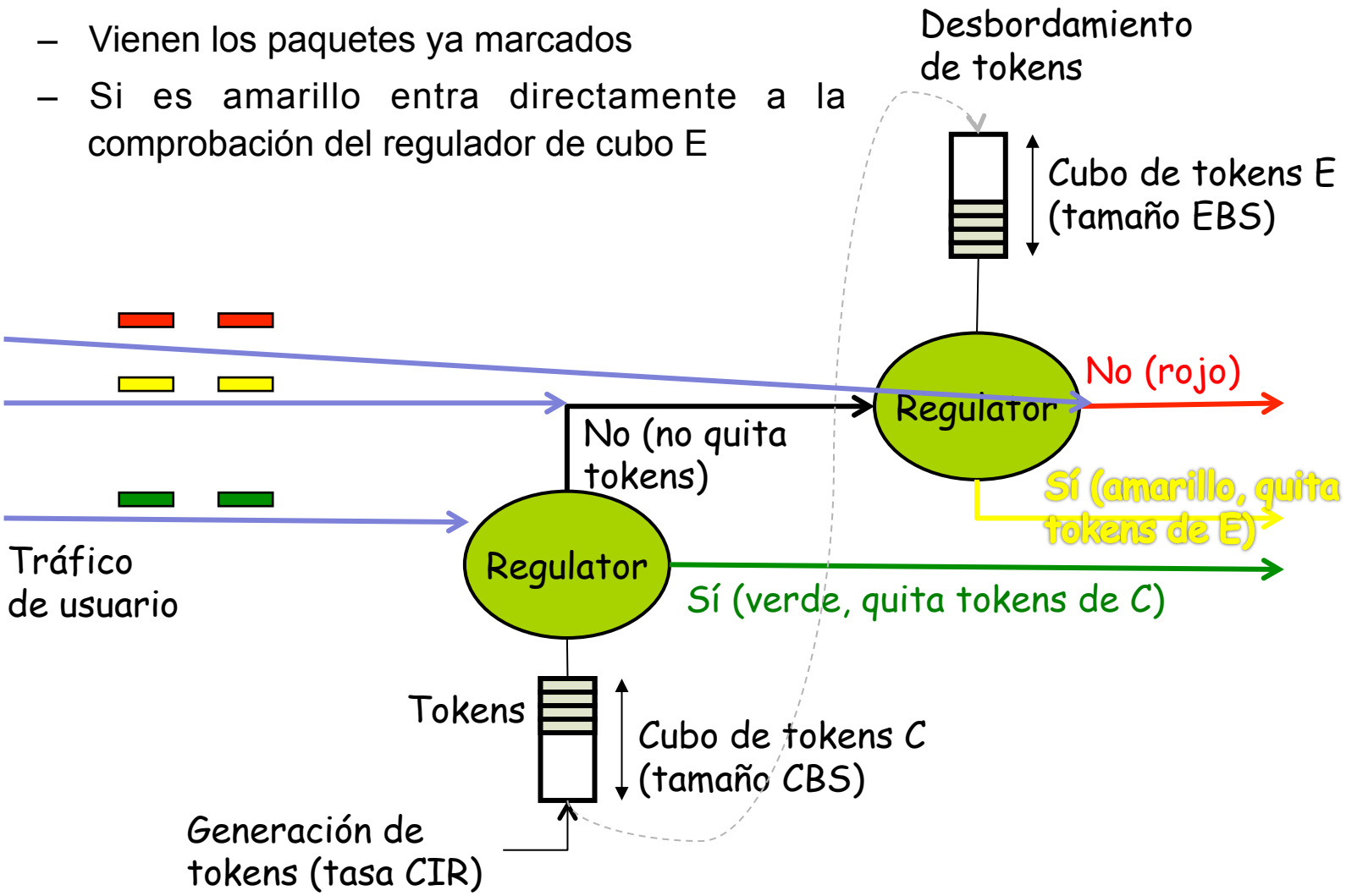
srTCM

- *single rate Three Color Marker (*RFC 2697)
- Dos *Token Buckets* (inicio llenos)
- Parámetros:
  - CIR: *Committed Information Rate*
  - CBS: *Commited Burst Size*
  - EBS: *Excess Burst Size*
- "Rojo" excede el CIR y ráfaga de CBS+EBS, "Amarillo" excede CIR y ráfaga de CBS



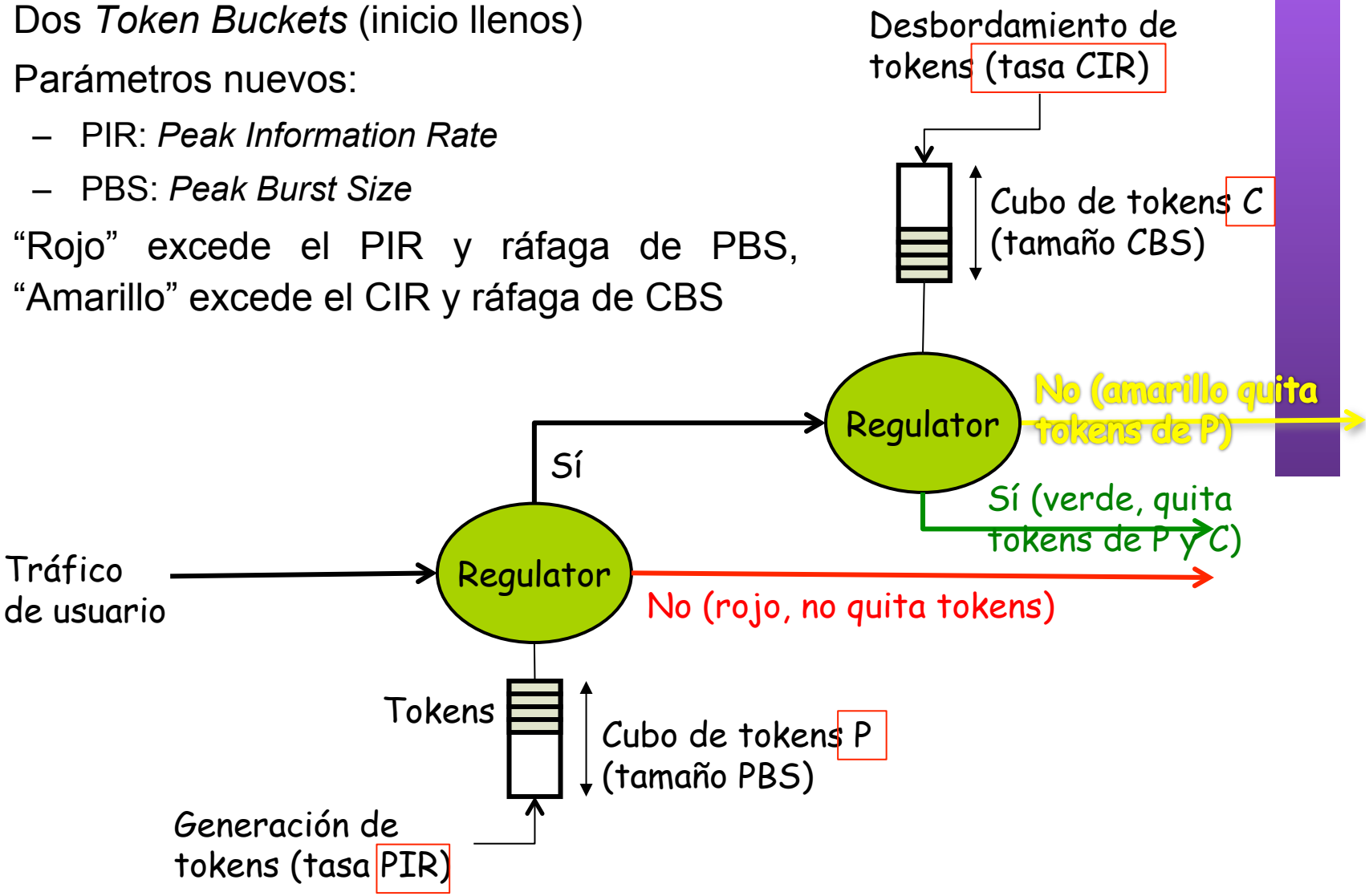
srTCM

- Eso era *color-blind*
- *Color-aware*:
  - Vienen los paquetes ya marcados
  - Si es amarillo entra directamente a la comprobación del regulador de cubo E



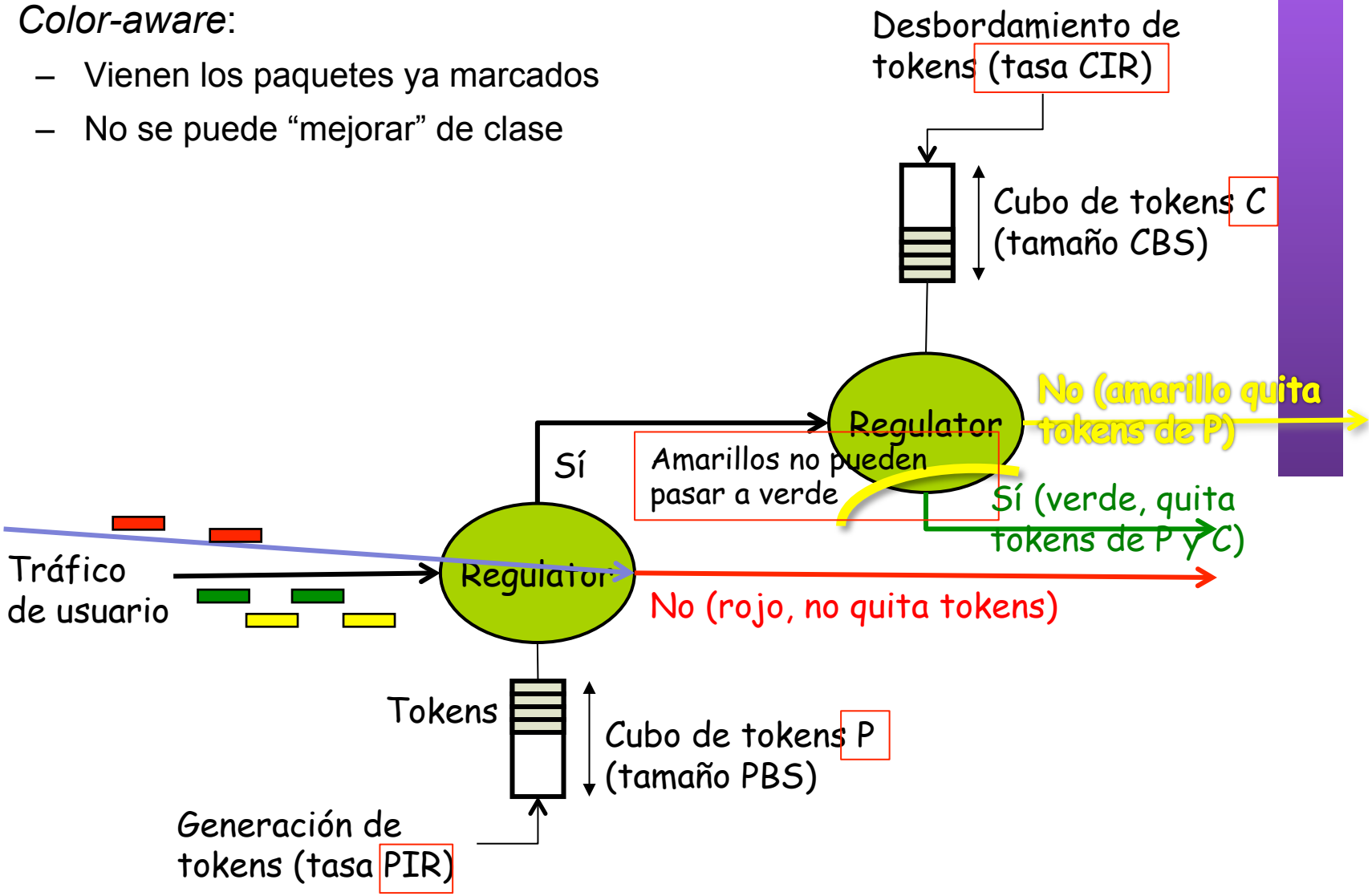
trTCM

- *two rate Three Color Marker (*RFC 2698)
- Dos *Token Buckets* (inicio llenos)
- Parámetros nuevos:
  - PIR: *Peak Information Rate*
  - PBS: *Peak Burst Size*
- "Rojo" excede el PIR y ráfaga de PBS, "Amarillo" excede el CIR y ráfaga de CBS



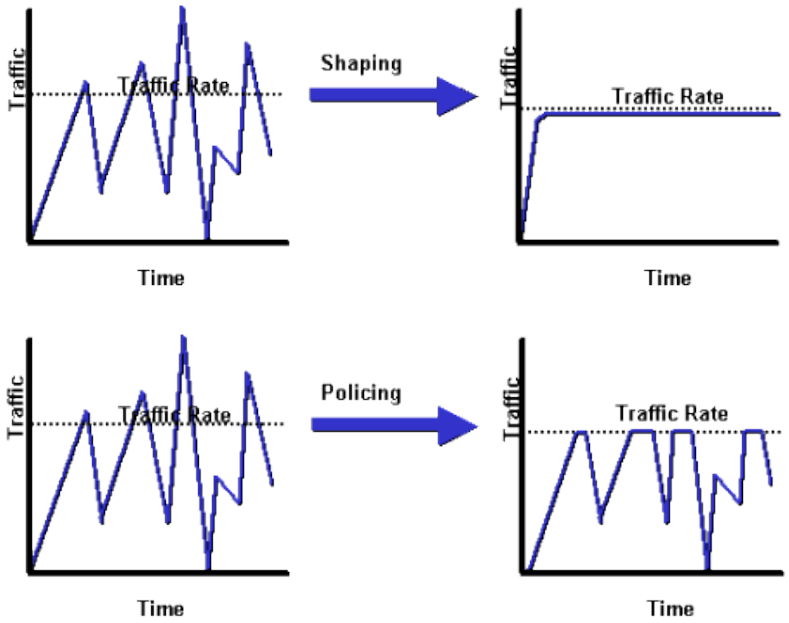
trTCM

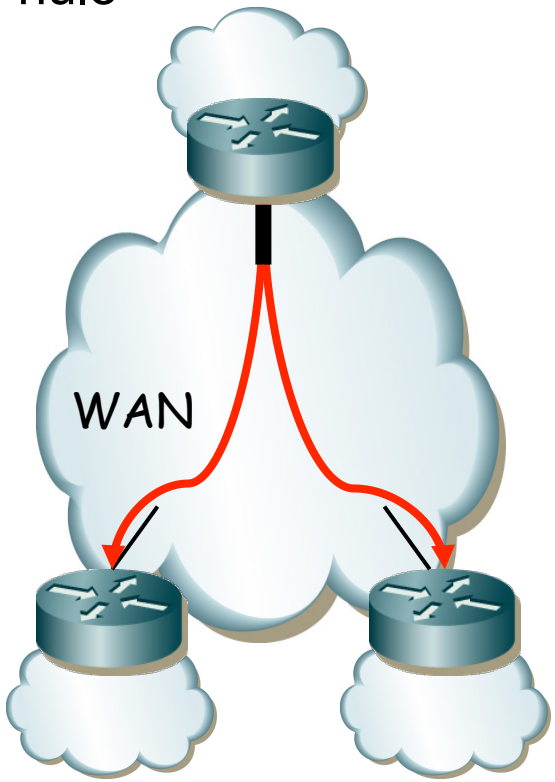
- Eso era *color-blind*
- *Color-aware*:
  - Vienen los paquetes ya marcados
  - No se puede "mejorar" de clase



Shaping

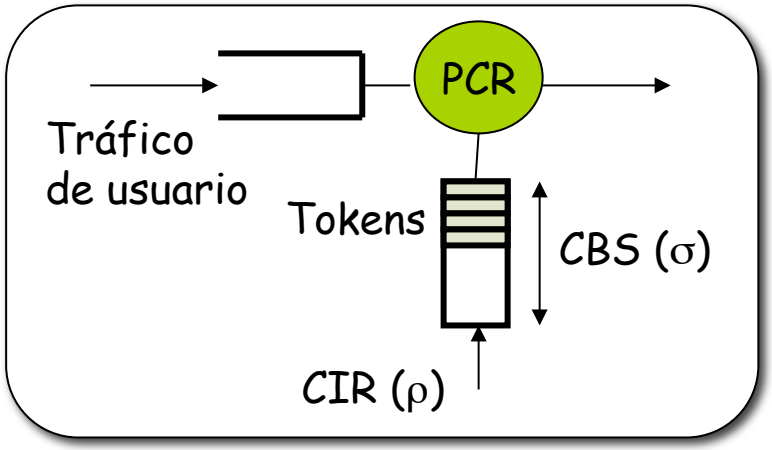
- Los que excedan no se descartan sino que se encolan
- Introduce delay y jitter
- Permite adaptar el tráfico ante diferentes velocidades en los extremos de una red
- Policing es similar a Shaping con buffer nulo

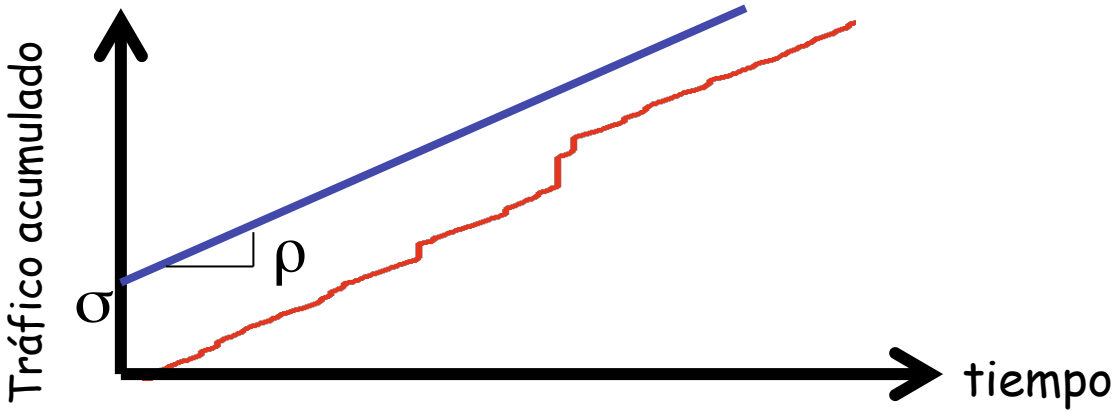




Ejemplo: *Single Leaky Bucket*

- Parámetros:
  - CIR = *Commited Information Rate* (bytes de paquetes IP por seg.)
  - CBS = *Commited Burst Size* (bytes)
- A(0,t) = tráfico cursado en intervalo (0,t)
- $A(0,t) \leq \rho t + \sigma$
- *"Restricción (σ, ρ)"* a la salida (LBAP, *Linear Bounded Arrival Process*)



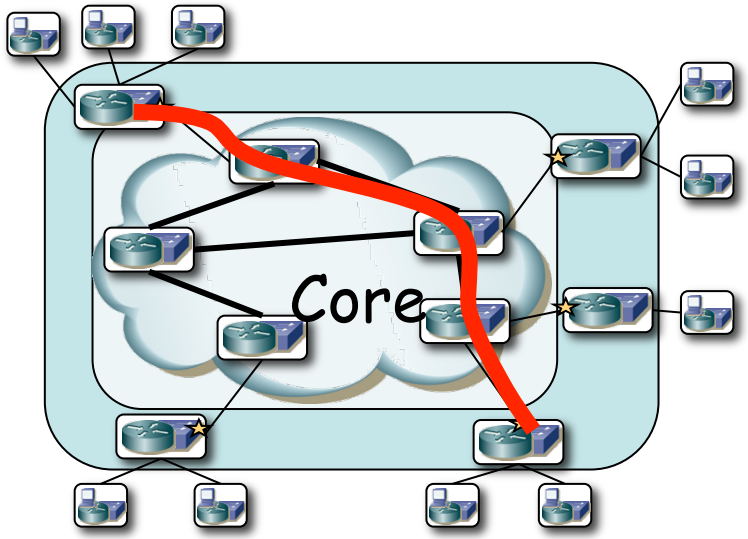


Connection Admission Control

CAC

Connection Admission Control

- Durante el establecimiento de la conexión
- Acciones para determinar si se permite o no
- Es lo correcto para flujos RT en vez de control de congestión
- Puede rechazar conexiones aunque haya capacidad suficiente, para asegurar dejar BW disponible para otras de mayor prioridad
- Sencillo para flujos que requieren QoS CBR
- Con flujos VBR debe basarse en caracterización estadística del agregado
- Puede permitir un grado de sobresubscripción para flujos VBR
- ¡Proteger tráfico RT del tráfico RT!
- "Call Admission Control"
- "Capacity Admission Control"



CAC para IP: Taxonomía

- *Endpoint measurement-based CAC*
  - Las decisiones son tomadas por las aplicaciones extremo
  - Se basan en medidas del tráfico a los destinos
  - Monitorización activa: se envían paquetes “sonda” (“probe”) para medir las características del camino
  - Monitorización pasiva: miden las características de flujos ya presentes entre esos extremos
  - Tiene el problema de que medidas pasadas pueden no ser un buen indicador de prestaciones futuras
  - No muy extendido
- *On-path network signaled CAC*
  - Los nodos en el camino de los datos son los responsables del CAC
  - Esto requiere que la señalización emplee el mismo camino que los datos
- *Off-path CAC*
  - La señalización puede llevar camino diferente a los datos
  - Puede ser mediante “bandwidth managers”

Resumen

- Clasificación en función de parámetros y características de layer 1-7
- Marcado, normalmente en cabeceras
- Token buckets