Università degli Studi di Bergamo

DIP. DI INGEGNERIA DELL'INFORMAZIONE E METODI MATEMATICI

RETI INTERNET MULTIMEDIALI

Internet Quality of Service

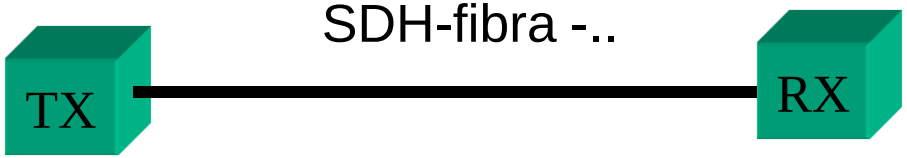
IL PROBLEMA DELLA QoS

Cosa è la QoS

- La QoS (Quality of Service) è un indice di qualità associato ai flussi informativi e influenzato da
  - Banda disponibile (compressione, rate di trasmissione)
  - Ritardi
  - Jitter dei ritardi
  - Packet dropping
  - Blocking probability
  - Set-up delay

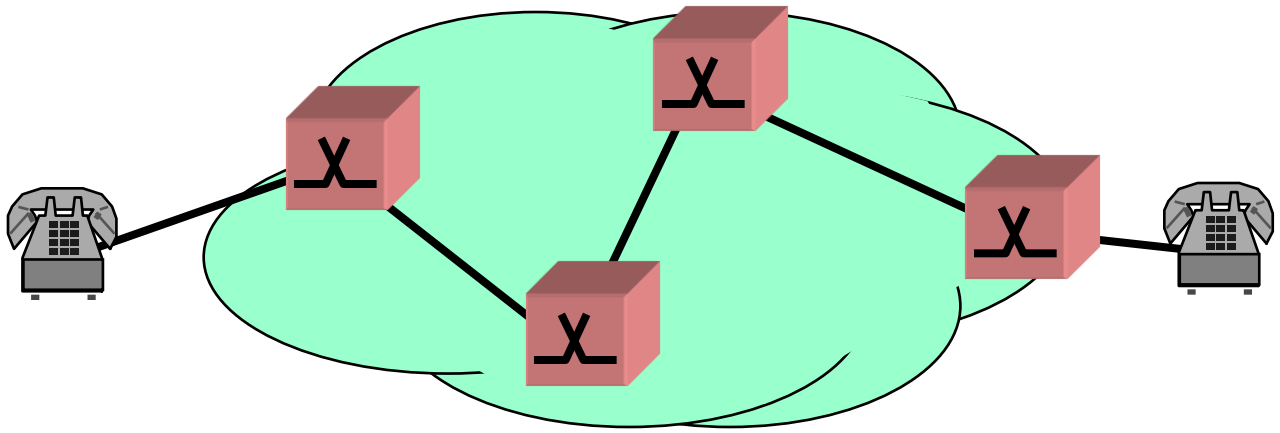
La Banda

- E’ la velocità di trasferimento (elaborazione) dell’informazione
  - E’ misurata in bit/s (byte/s, pacchetti/s,..)
  - Può essere variabile nel tempo
- I sistemi trasmissivi fisici hanno banda costante nel tempo



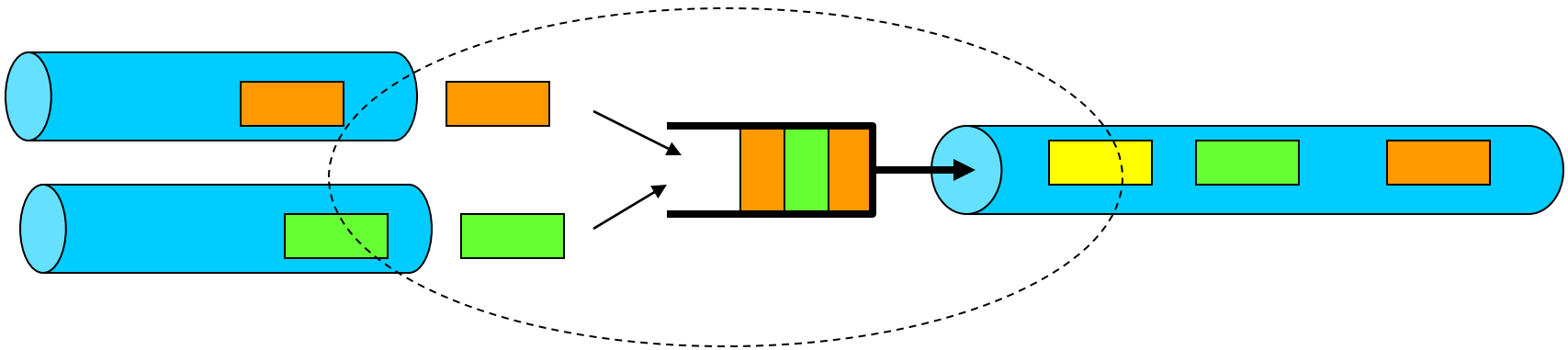
La Commutazione di Circuito

- Ritaglia un circuito a banda costante (64 kb/s) end-to-end
- Ogni bit è trasferito con la stessa velocità (servizio sincrono)
- (quasi) nessun jitter

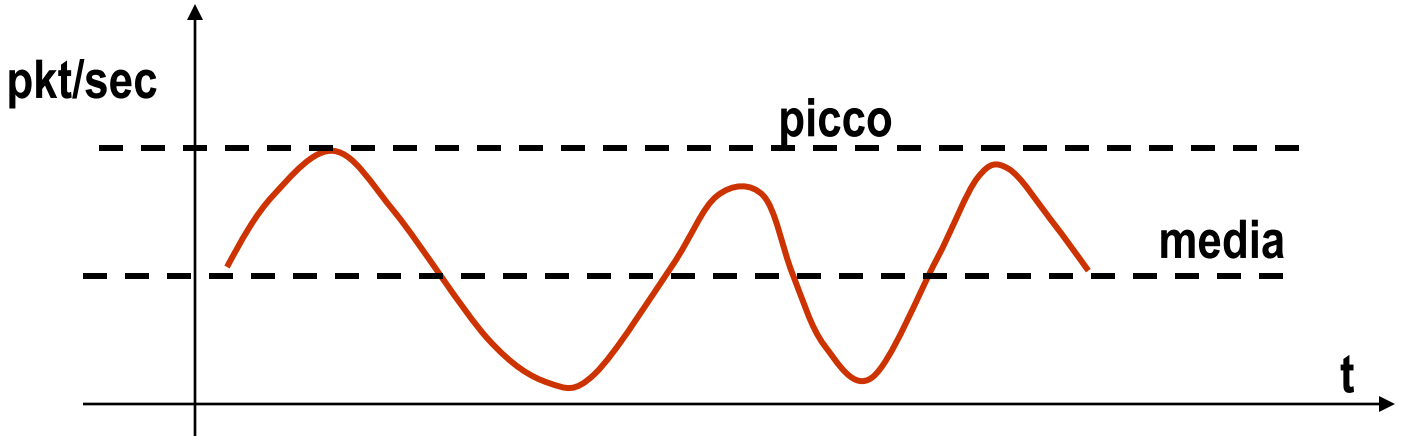


La Commutazione di Pacchetto

- Trasferisce pacchetti (trame, celle, ..) ossia unità di più bit
- Il trasferimento è asincrono
- Le variazioni di traffico variano la banda disponibile
- I conflitti introducono ritardi variabili (jitter)

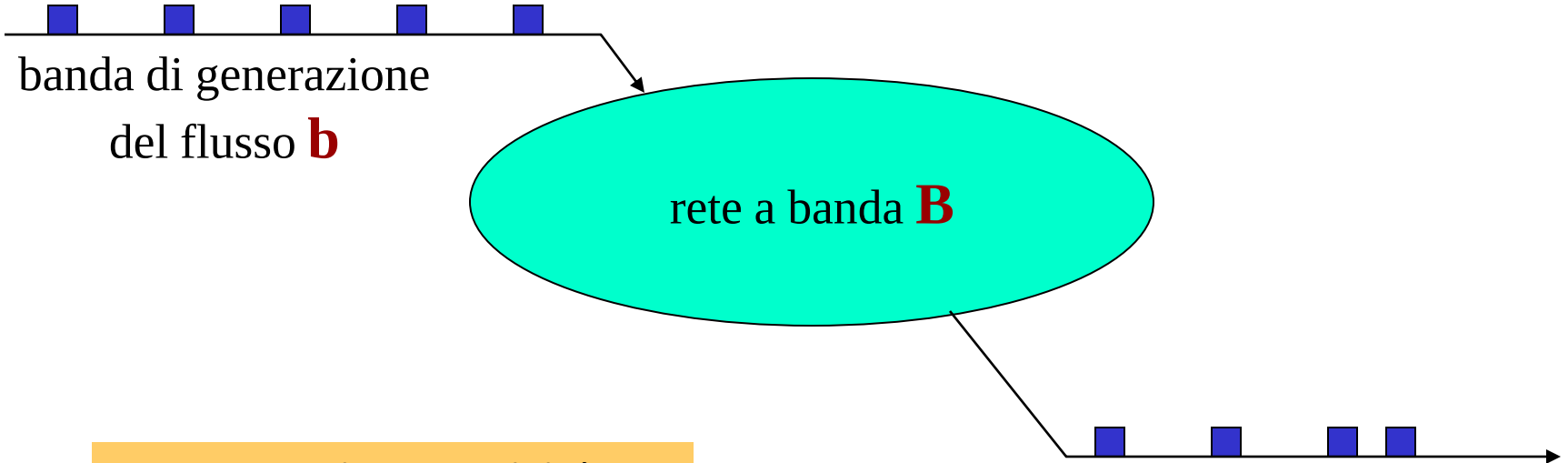


Banda Variabile

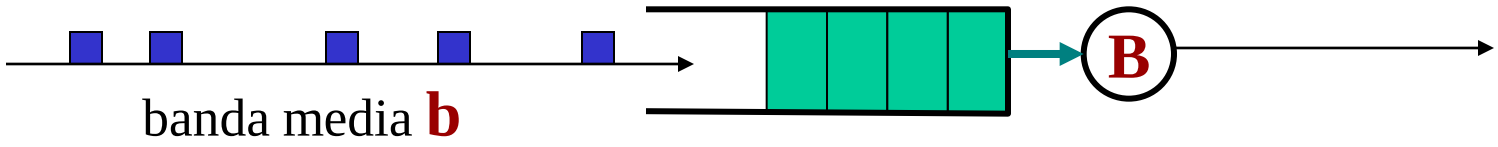


- Si definiscono
  - Banda media
  - Banda di picco
  - etc.

Banda Variabile



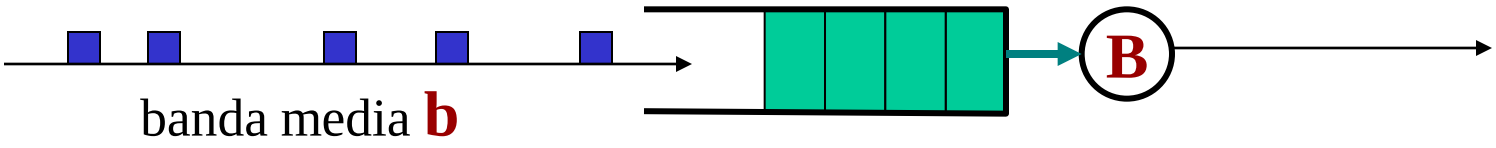
La rete introduce variabilità
anche nei flussi costanti



Modello di nodo di rete

Prestazioni

- Quale banda B assegnare al flusso b?
- Se **B < b**
  - si **perdono** pacchetti in rete
- Se **B > b**
  - si hanno **ritardi** tanto **minori** quanto più grande è B



Prestazioni

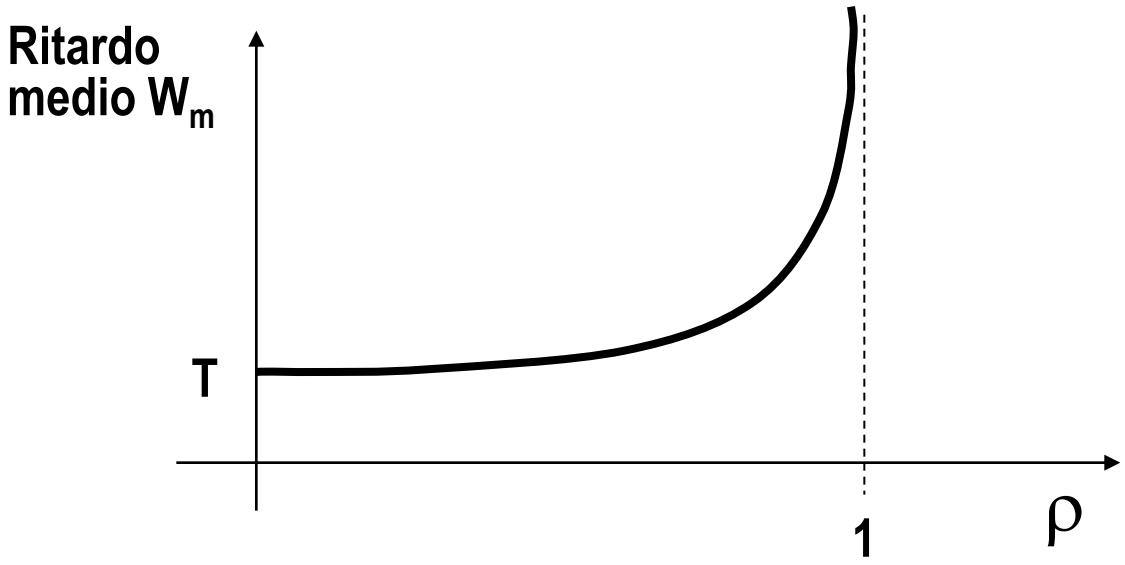
- Problema: quale banda B occorre assegnare per garantire i ritardi?
  - Non esiste una risposta univoca
  - Dipende dal tipo di flusso

Modello di Arrivi di Poisson

- Il modello degli arrivi di Poisson consente di calcolare i ritardi medi e i percentili

T = tempo di trasmissione dei pacchetti
b = banda media del flusso
B = banda costante del canale

$$W_m = \frac{\rho}{1-\rho}\left(\frac{T}{2} + \frac{\sigma_T^2}{2T}\right) + T$$

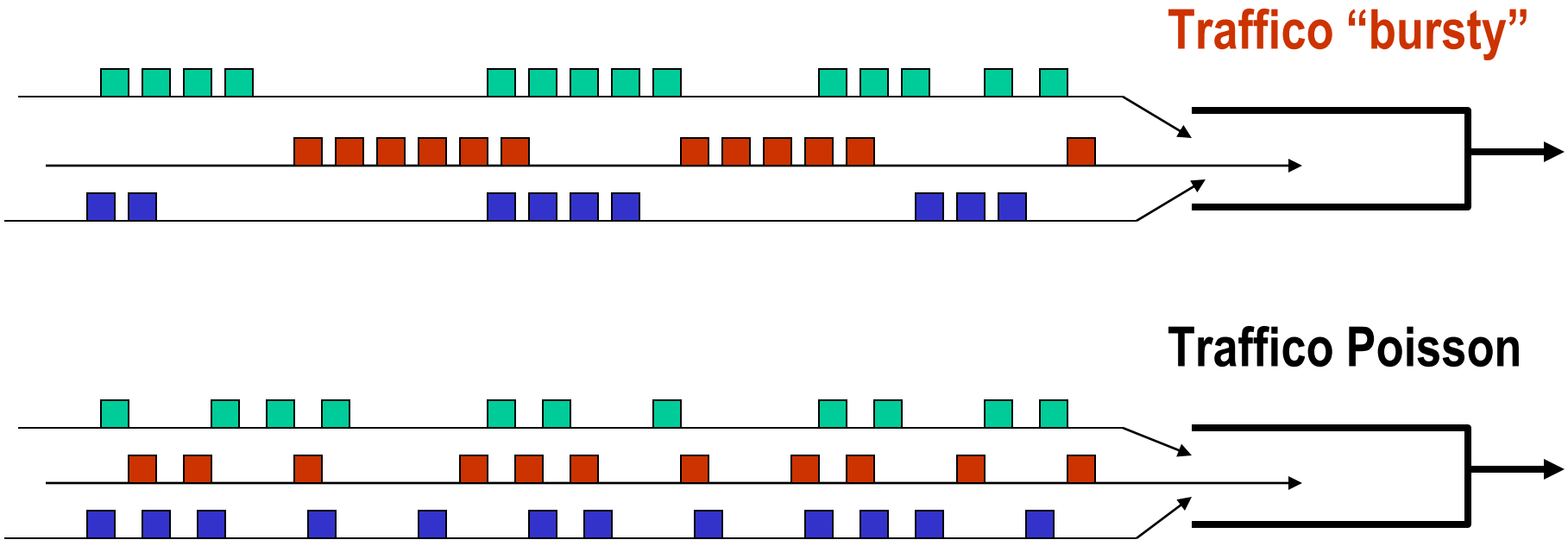


$$\rho = \frac{b}{B}$$

il ritardo massimo non è garantito

Burstiness

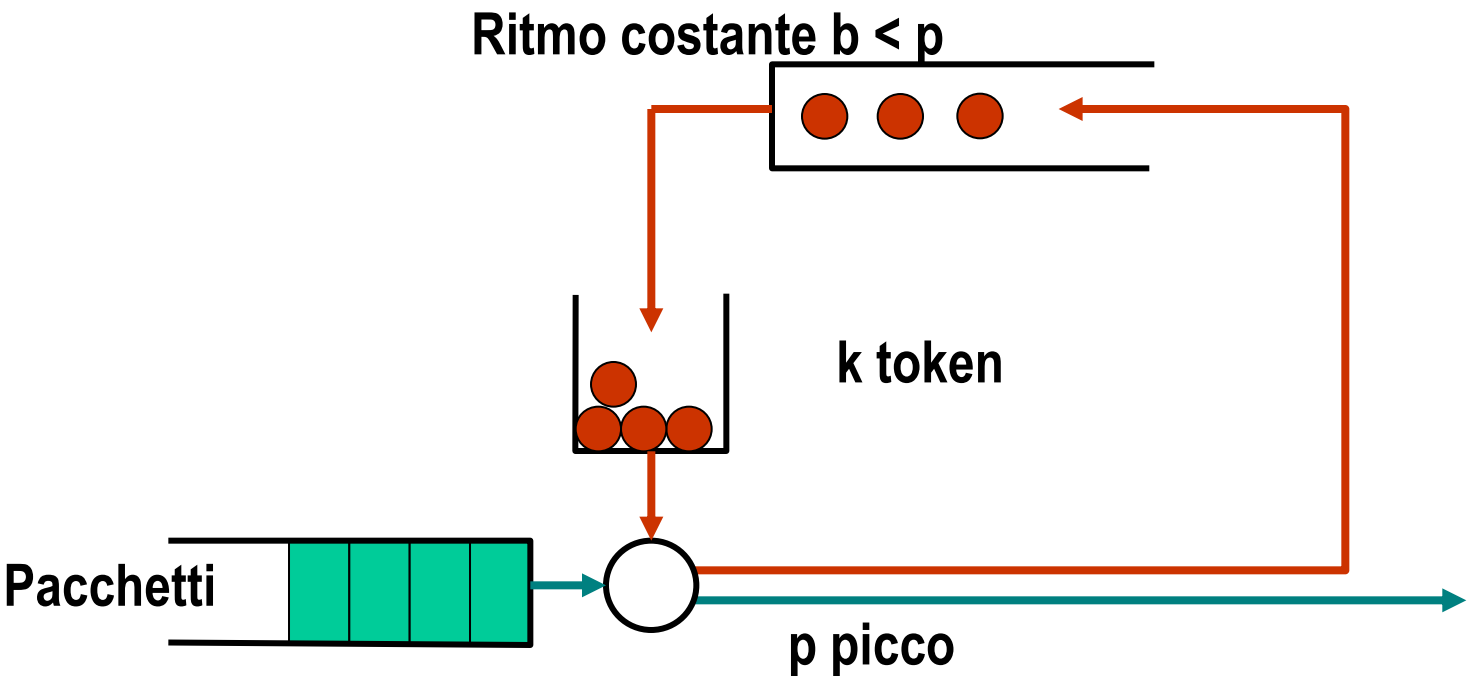
- I flussi reali si scostano dal modello di Poisson



- Per indagare i ritardi occorre definire la “variabilità” (burstiness) (si può fare solo in modo approssimato)

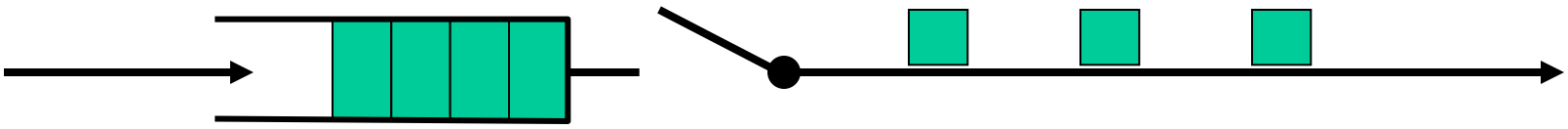
Modello Token Bucket

- Controlla il picco **p**, la media **b** e la lunghezza massima del burst **L**



Modello Token Bucket

- Con k=1 genera traffico CBR



- Con k>1 genera traffico bursty

$$pL = k + bL \longrightarrow L = \frac{k}{p-b}$$

Risultati per modello Token Bucket

- Il traffico è caratterizzato da k, p, b, e da M (maximum policed unit) e m (minimum policed unit)
- Si riesce a controllare il **ritardo massimo** W_M usando banda B

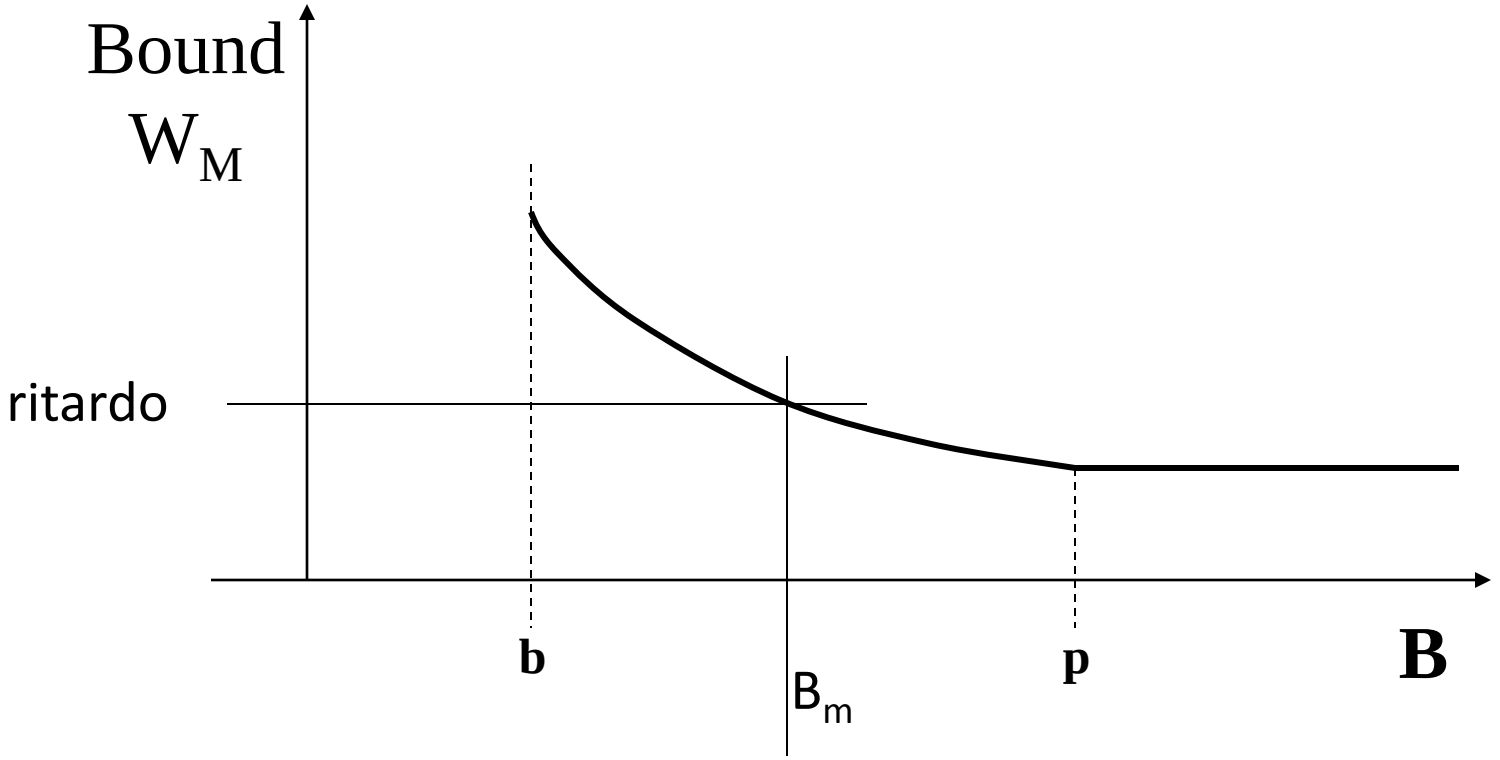
$$W_M \leq \frac{k-M}{B}\frac{p-B}{p-b} + \frac{M}{B} + \frac{C}{B} + D \quad \text{se} \quad B < p$$

tiene conto del burst

$$W_M \leq \frac{M}{B} + \frac{C}{B} + D \quad \text{se} \quad B > p$$

C e D costanti

Risultati per modello Token Bucket



- Fissato il massimo ritardo ammissibile si può ricavare il minimo B (B_m) che lo garantisce

Problema: B_m è molto spesso molto più grande di b

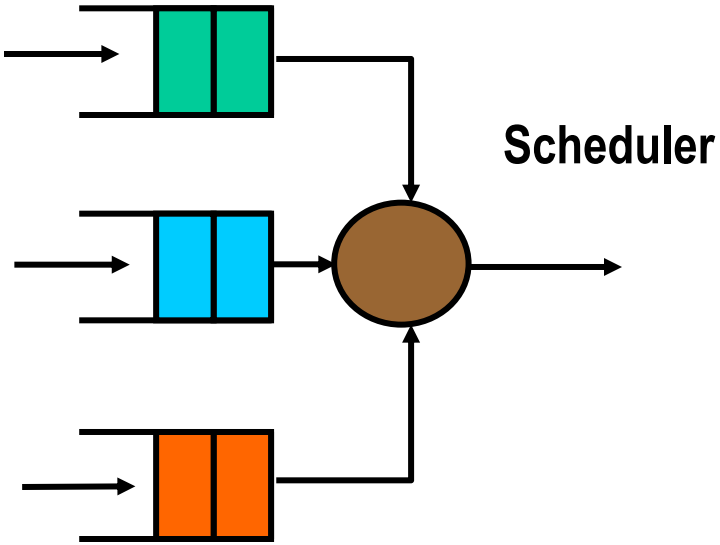
STRUMENTI PER GARANTIRE LA QoS

Strumenti per garantire la QoS

- Per garantire la QoS servono strumenti di identificazione dei flussi (label, virtual circuits, etc.) …

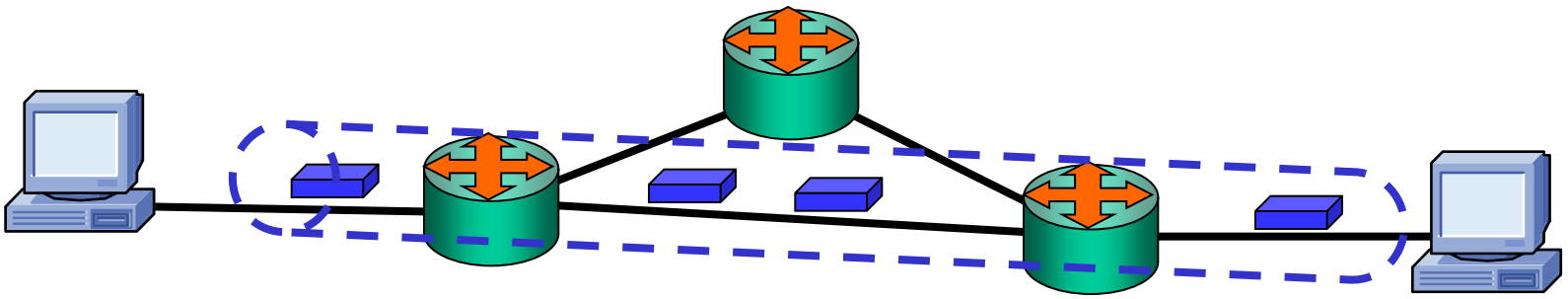
Strumenti per garantire la QoS

- … e servono strumenti per suddividere la banda nei router (tecniche di scheduling)



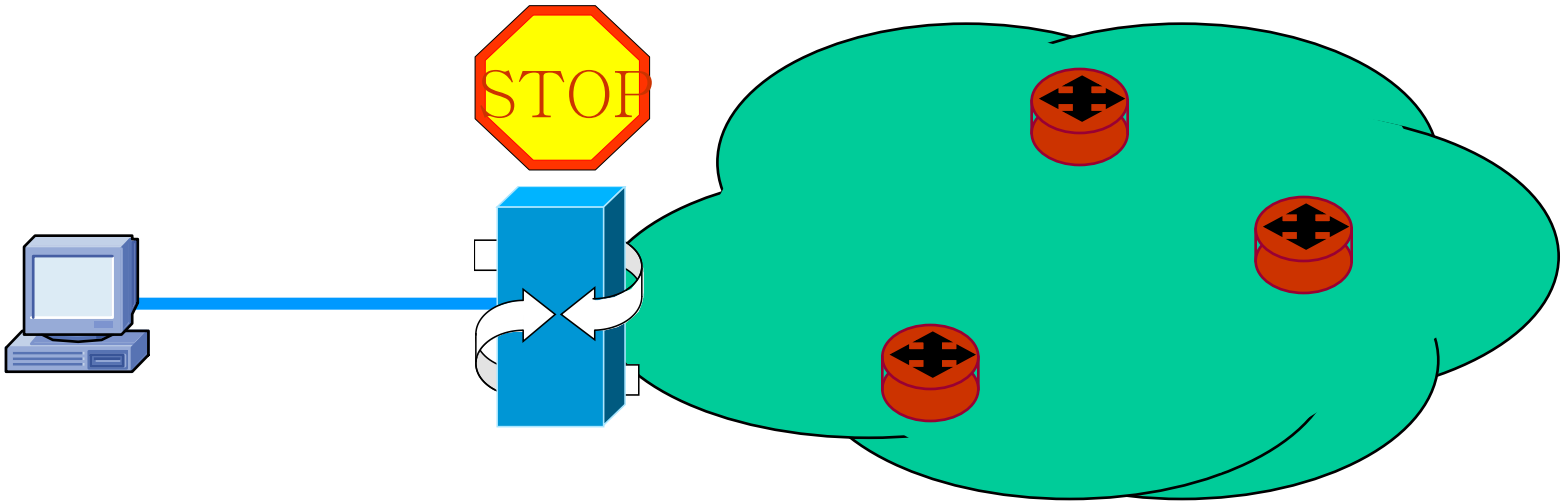
Strumenti per garantire la Banda

- Per garantire la banda occorrono strumenti per fissare i cammini in rete



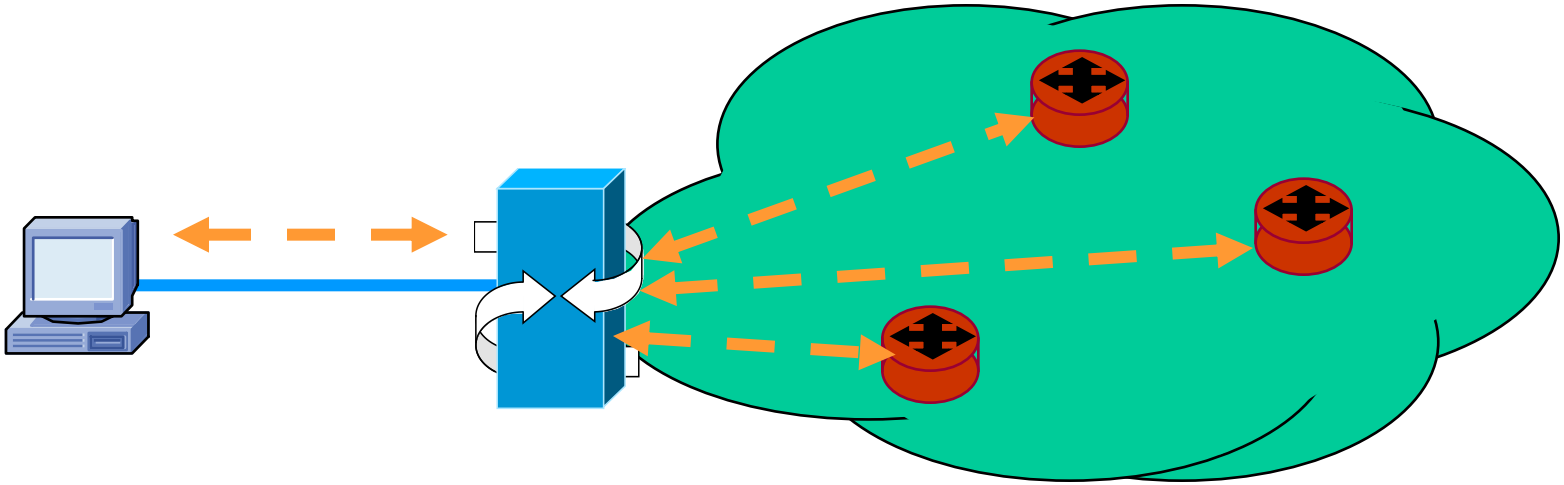
Garantire la Banda in modo dinamico

- Occorrono meccanismi di controllo delle risorse (CAC: Call and Admission Control)
  - che possano rifiutare la richiesta se la banda non è disponibile …



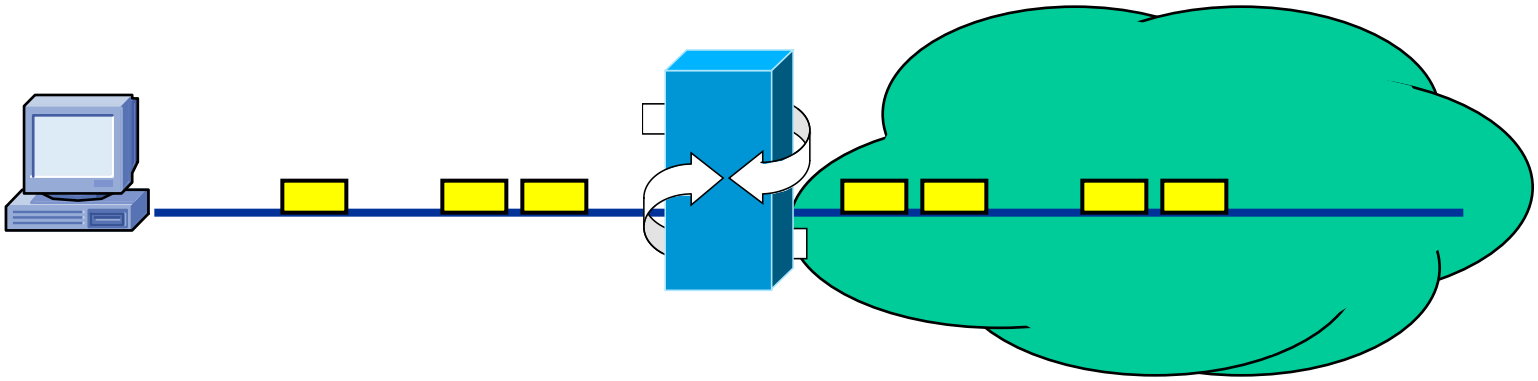
Garantire la Banda in modo dinamico

- ... e meccanismi di segnalazione delle risorse di rete (banda disponibile sui vari cammini)



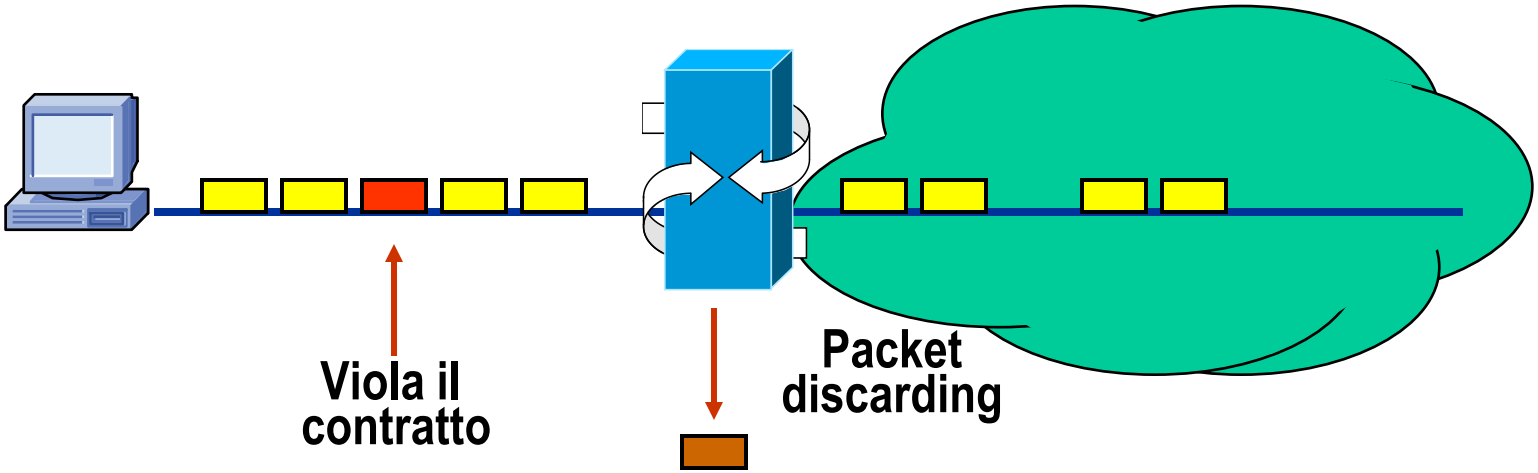
Controllo del traffico immesso

- Il traffico immesso non è vincolato dal mezzo fisico
  - è spesso variabile, con banda media b minore di quella di linea p (picco)
  - i contratti tengono conto della media e del picco (lunghezza del burst)



Strumenti di Policing

- Per evitare che la banda venga sottratta occorrono strumenti di policing
  - che controllino il traffico immesso
  - verifichino la conformità alle risorse
  - prendano provvedimenti in caso di violazione



Overprovisioning

- **Se la banda fosse infinita…**
  … la QoS non sarebbe un problema
- La banda non è infinita (ha un costo)
- Le richieste fluttuano nel tempo (si dimensiona sul picco?)
- Le richieste crescono col tempo (previsioni?)
- Le richieste prima o poi generano conflitti
- Che risultano in perdita di QoS, unfairness

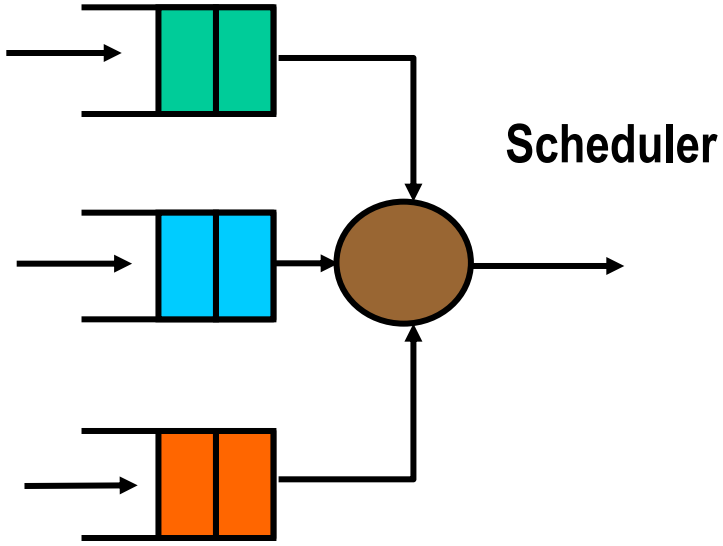
Traffic Engineering

- **Con il CAC la QoS può essere garantita su qualunque rete**
- Basta limitare il traffico ammesso a un livello sufficientemente basso
- Ma il traffico troppo basso scontenta i gestori
- Per questo in aggiunta si usano strumenti di traffic engineering che consentono di sfruttare meglio le risorse
- e quindi di spostare il livello di traffico a cui far intervenire il CAC a valori più elevati

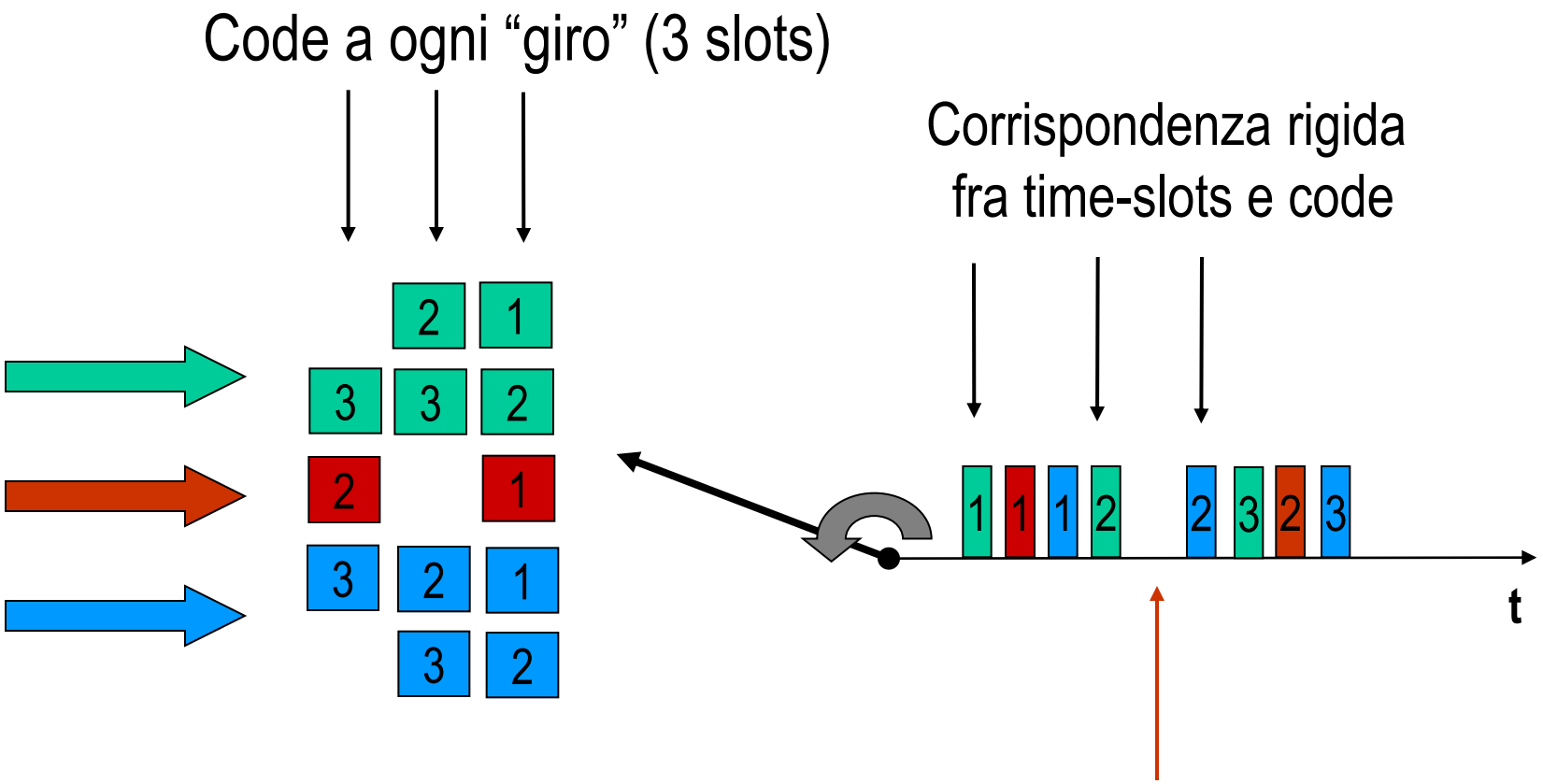
SUDDIVISIONE DELLA BANDA

Scheduling

- Strumenti per suddividere la banda nei router (tecniche di scheduling)



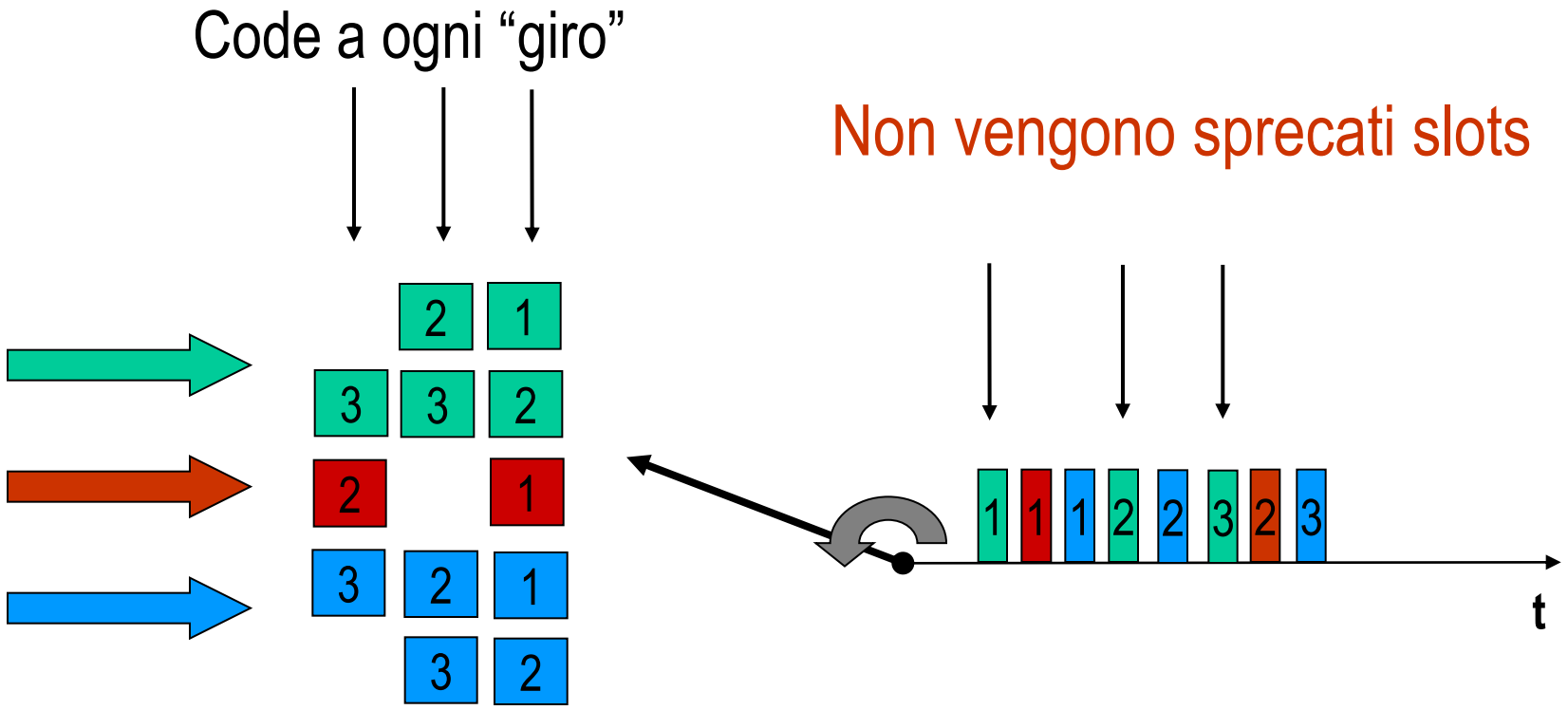
Time Division Multiplexing



Non consente il riutilizzo di risorse non usate da un flusso

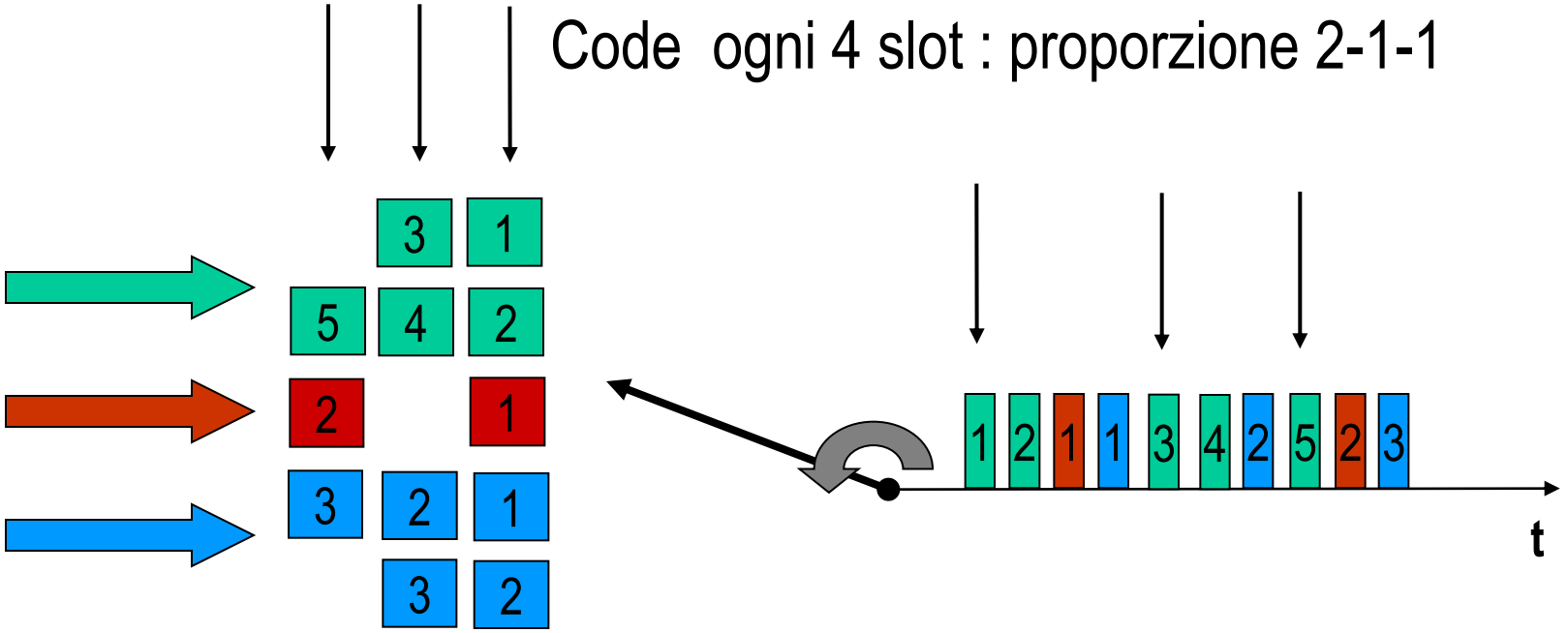
Round Robin (Fair Queuing)

- Suddivisione dinamica ed uguale della banda ottenuta trasmettendo un pacchetto per ogni flusso ciclicamente



Weighted Fair Queuing

- Suddivisione dinamica e proporzionale della banda ottenuta trasmettendo K_i pacchetti per ogni flusso “i” in modo pseudo ciclico.



Risultati per modello Token Bucket

- Il traffico è caratterizzato da k, p, b, e da M (maximum policed unit) e m (minimum policed unit)
- Si riesce a controllare il ritardo massimo W usando Weighted Fair Queuing che assegna banda B

$$W \leq \frac{k-M}{B}\frac{p-B}{p-b} + \frac{M}{B} + \frac{C}{B} + D \quad \text{se} \quad B < p$$

$$W \leq \frac{M}{B} + \frac{C}{B} + D \quad \text{se} \quad B > p$$

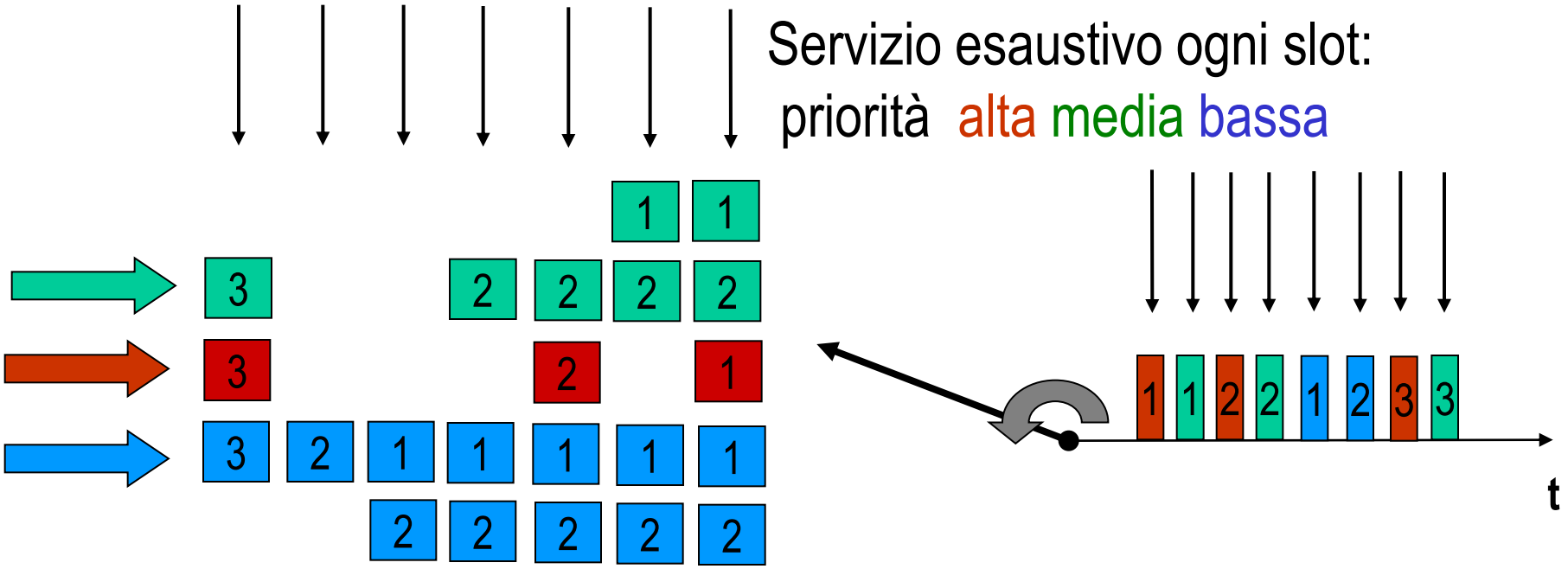
C e **D** costanti che dipendono dal tipo di algoritmo usato

Suddivisione della Banda

- I pacchetti sono unità intere di lunghezza variabile
- La suddivisione è quantizzata
  - a pacchetti
  - di lunghezza variabile
- E’ complicato suddividere esattamente
- Si introducono ritardi e jiitter

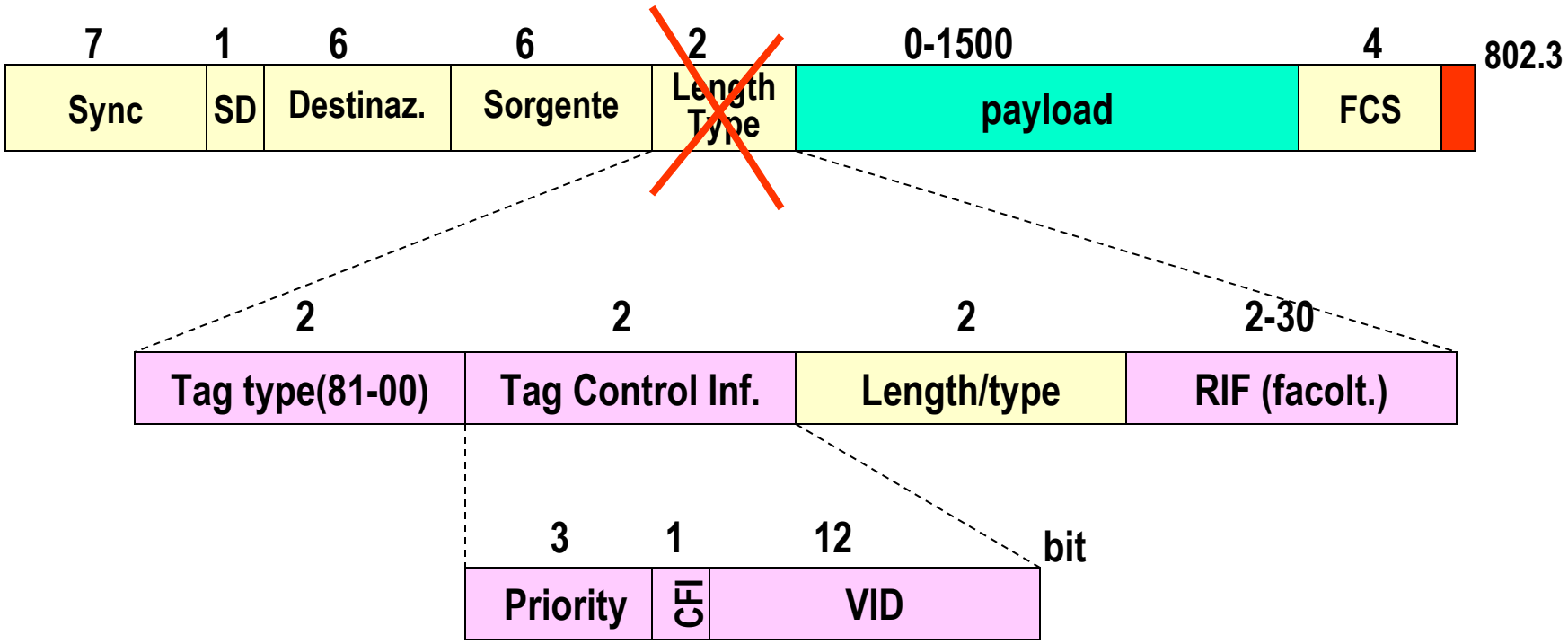
Priorità di Servizio

- Suddivisione dinamica preferenziale della banda.
- Non garantisce le priorità inferiori



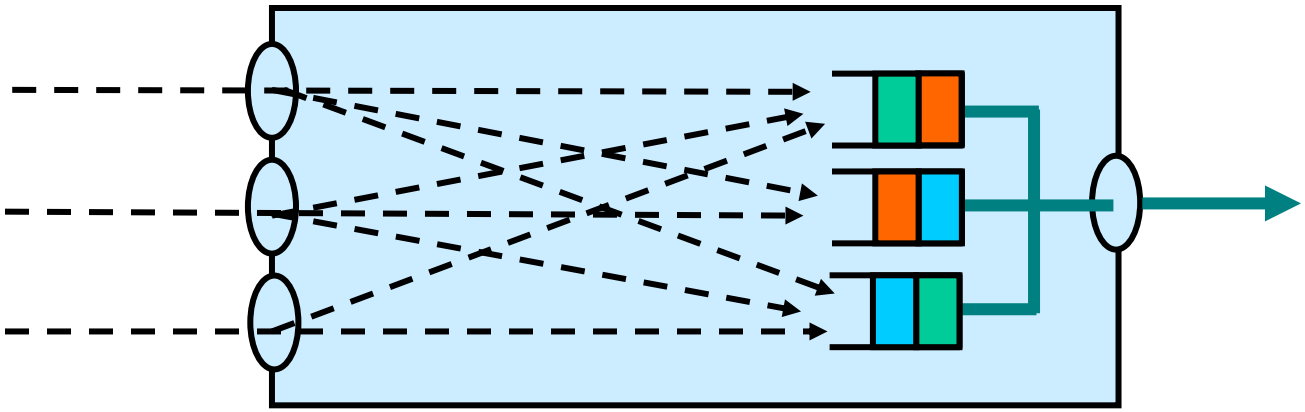
Priorità nelle LAN

- Lo standard IEEE 802.1Q (VLAN) introduce campi di priorità anche per 802.3 e 802.11 (che non servono per l'accesso multiplo)



Priorità nelle LAN

- Fino a 8 priorità di servizio sono state standardizzate in 802.1D
  - Mappano le priorità della trama MAC
- Queste sono impostate al momento dell'incapsulamento dei livelli superiori
  - in base alle priorità di questi
  - o alla VLAN di appartenenza
  - o al tipo di traffico trasportato (livelli 4)

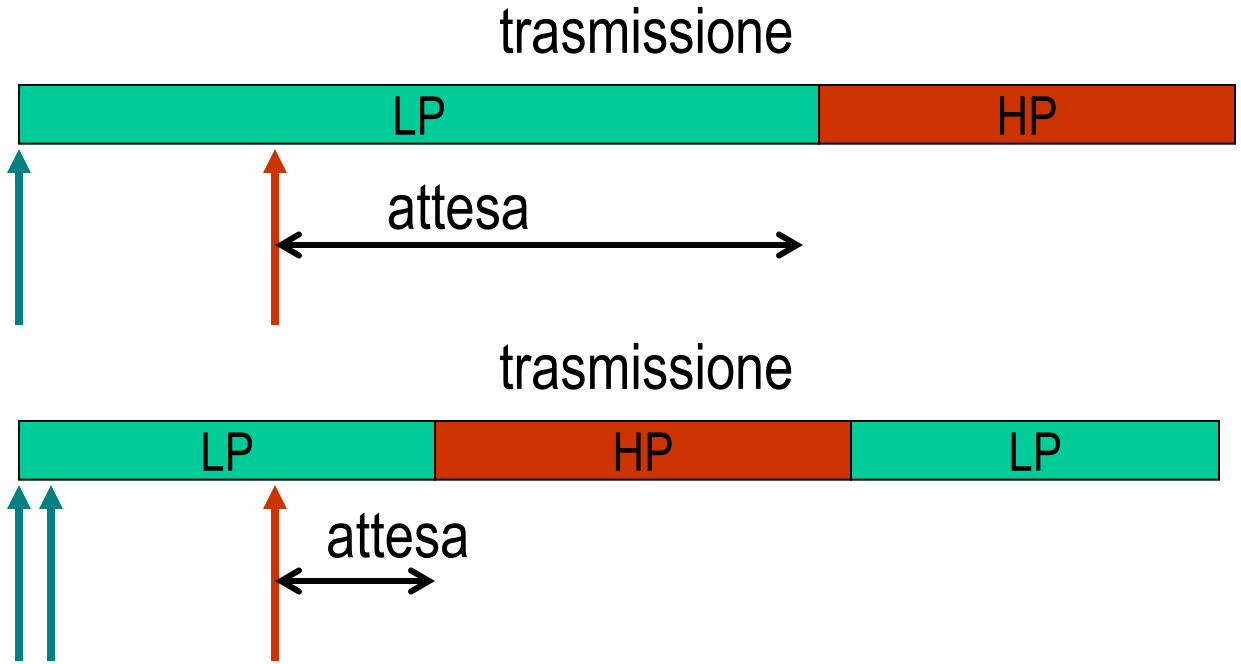


Priorità e Scheduling

- Priorità e scheduling vengono effettuate sulla base di pacchetti interi
  - non si possono interrompere le trasmissioni
- Se i pacchetti in trasmissione sono lunghi gli altri ne subiscono il ritardo

Priorità di Servizio

- Esempio:
  - **Rosso** alta priorità
  - Effetto di un pacchetto **verde lungo** e di **due verdi di lunghezza metà**



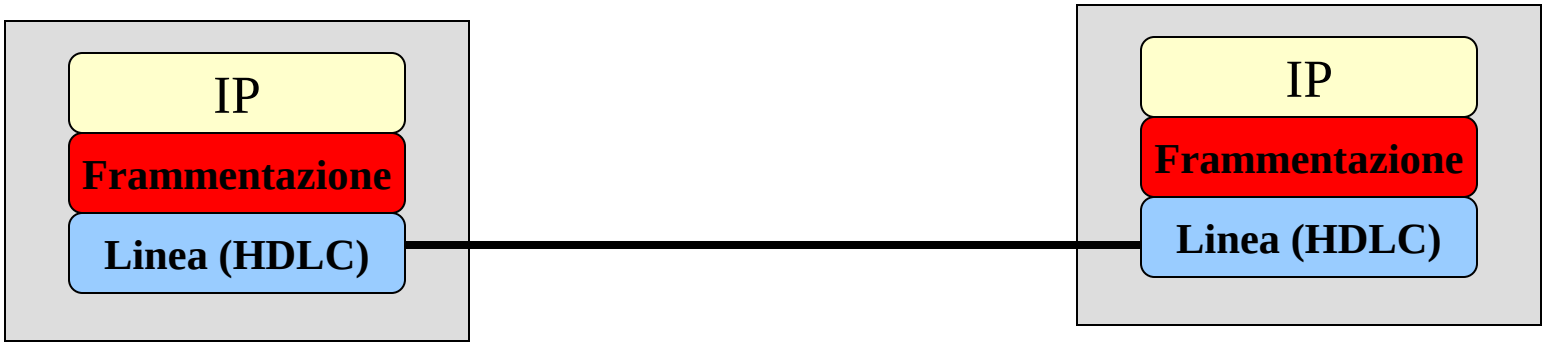
Trasmissione delle Trame

	1500 Byte (max Ethernet)	40 Byte (voce)
64 kb/s	187.5 ms	5 ms
128 kb/s	93.75 ms	2.5 ms
512 kb/s	23.4 ms	0.625 ms
2 Mb/s	6 ms	0.16 ms
10 Mb/s	1.2 ms	0.033 ms

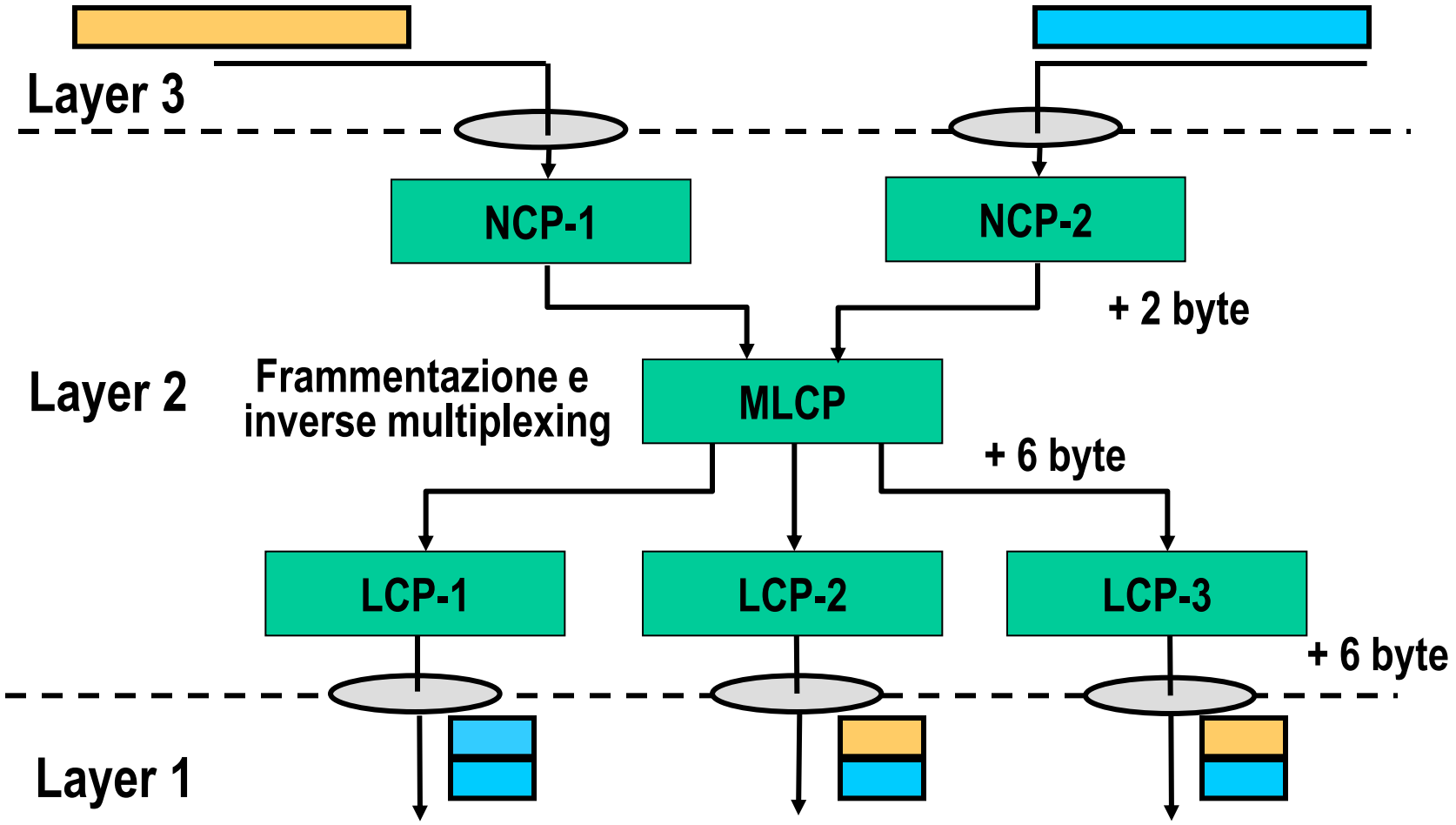
Necessità di frammentare su link poco veloci

Modalità di Frammentazione

- Ridurre la lunghezza di tutte le trame IP porta ad enormi inefficienze
- Si possono frammentare trame a livello IP solo su connessioni lente.
  - Ma poi IP non le ricostruisce che alla fine
- Occorre un meccanismo a livello 2 sulle connessioni lente che possa frammentare le trame lunghe in trasmissione e che le ricomponga in ricezione

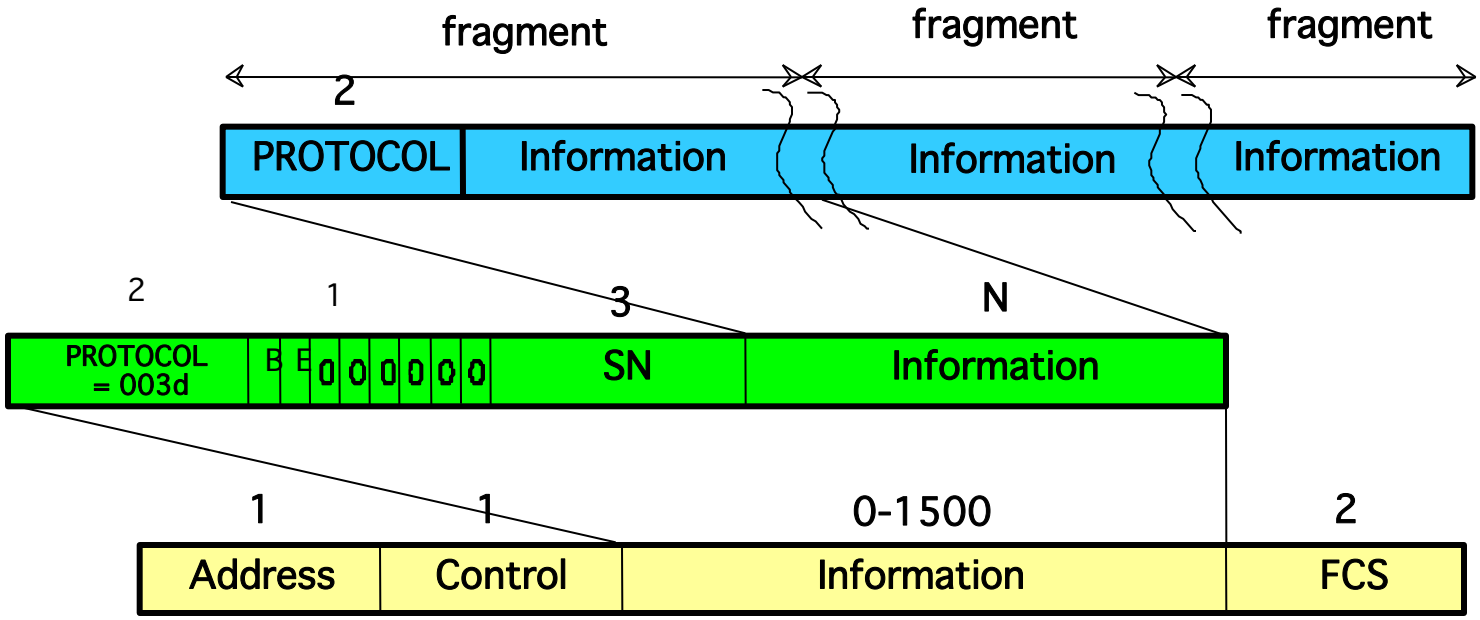


Il protocollo Multilink PPP

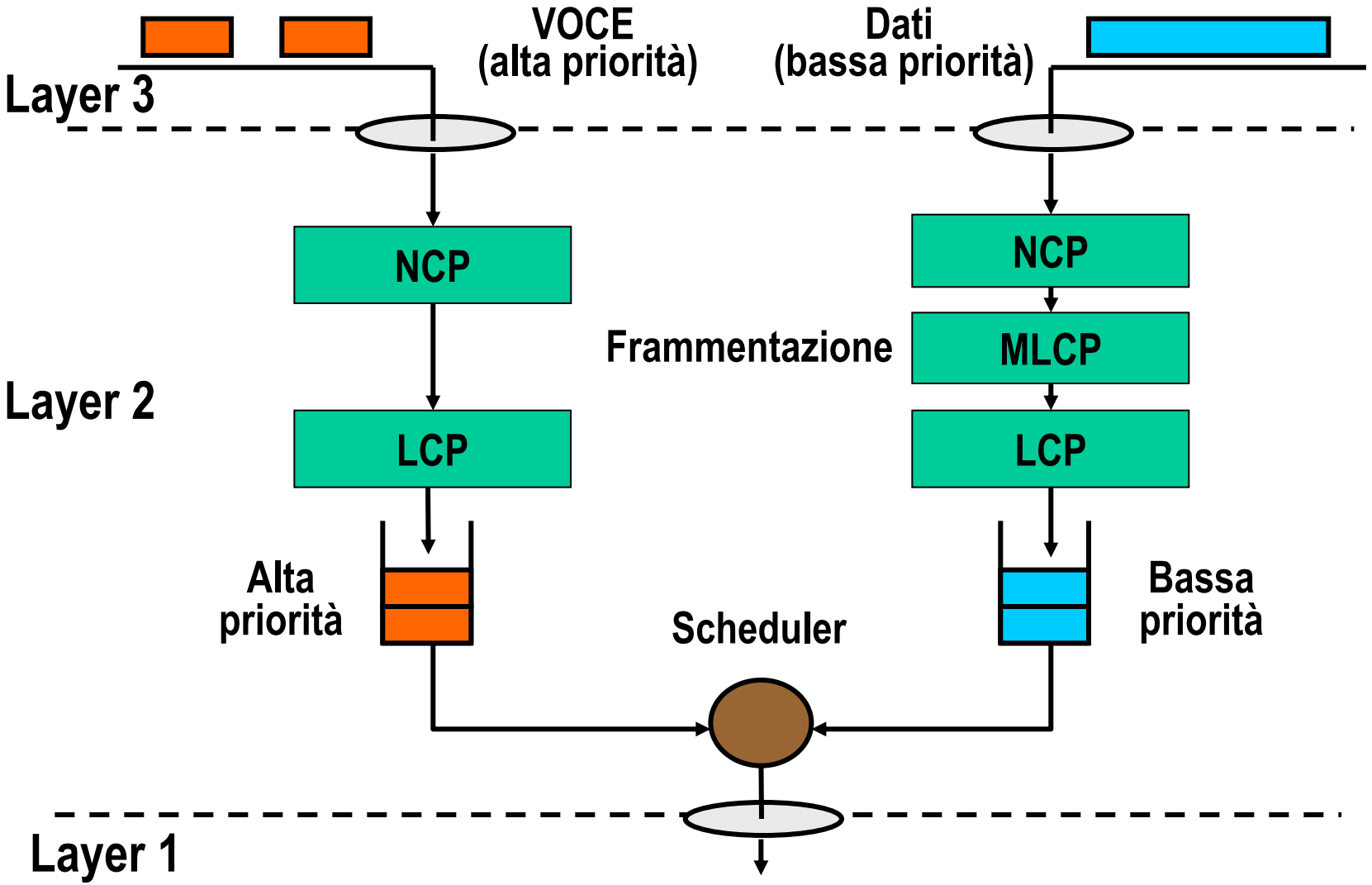


Il protocollo Multilink PPP

- Gli strati LCP e MLCP incapsulano nella loro trama il SAP del sottostrato superiore, cosicché in ricezione la catena viene ripercorsa a rovescio



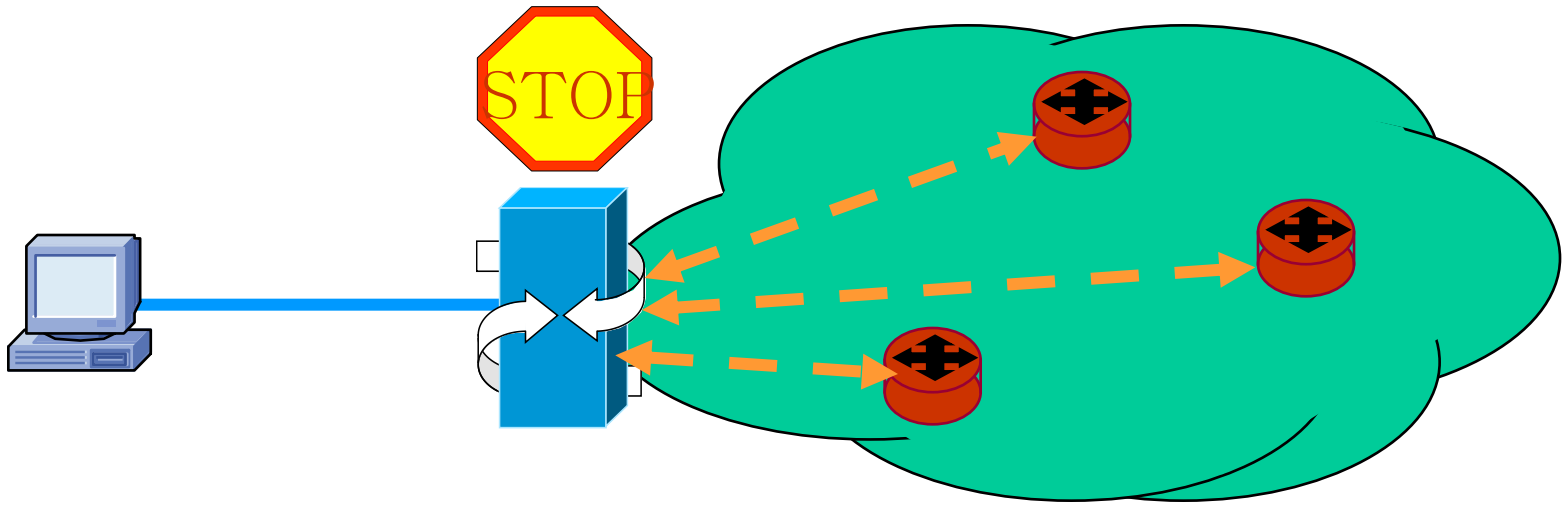
Utilizzo proprietario del protocollo PPP



IL CONTROLLO D’ACCESSO

Call and Admission Control

- Deve conoscere
  - la quantità di risorse richiesta
  - la quantità di risorse usata su ogni link
- Calcolare se esiste un cammino con tale disponibilità
- prenotare le risorse in caso di accettazione



Modalità di calcolo e prenotazione

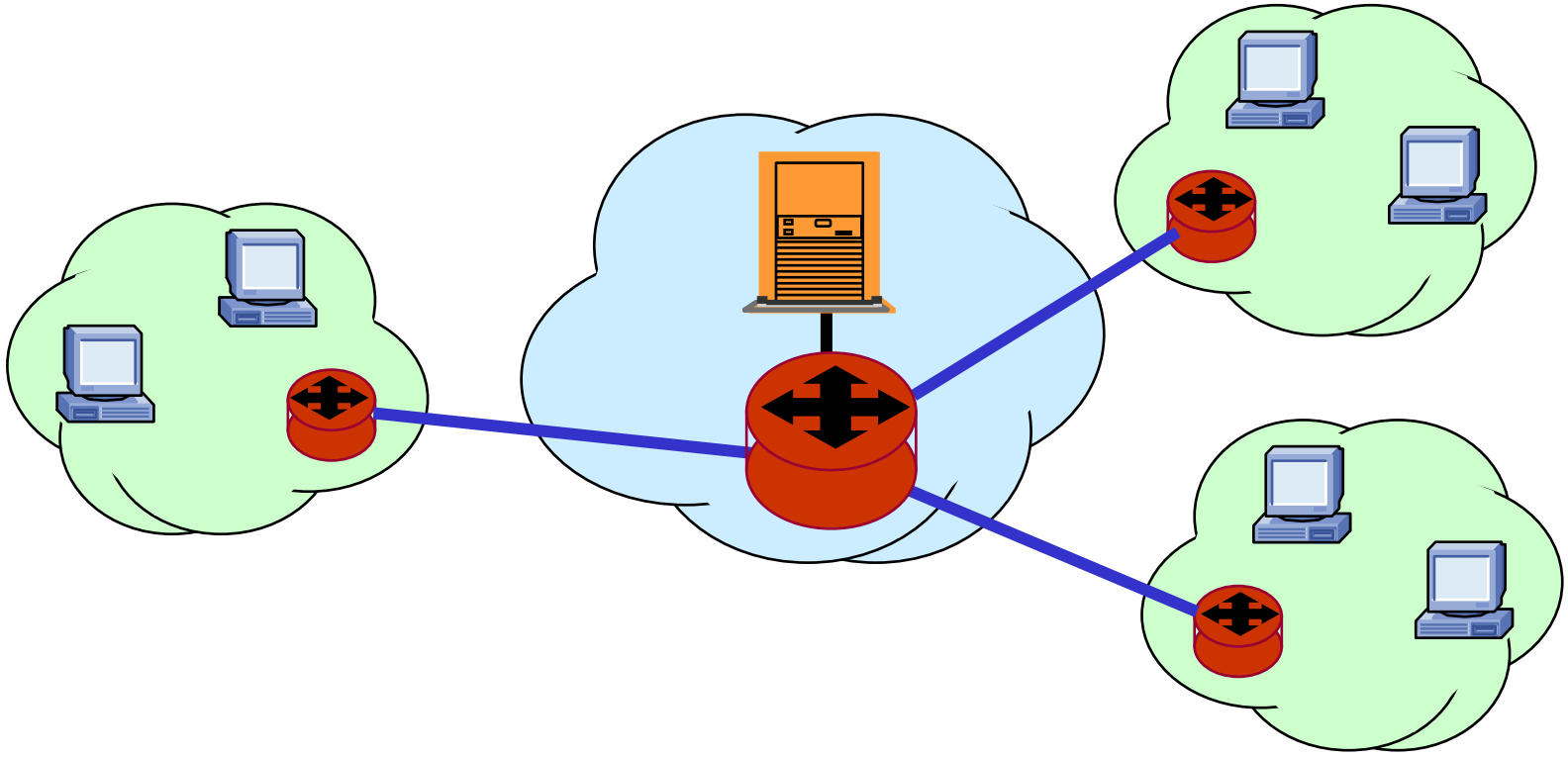
- Le modalità di calcolo e prenotazione possono essere suddivise in tre gruppi:
  - **Centralizzata**: il CAC viene effettuato da un server centrale
  - **Distribuita**: Ogni nodo concorre al CAC
  - **Mista**: tecnica che consente il CAC solo ai nodi d'ingresso della rete

Modalità Centralizzata

- Il CAC viene effettuato da un server centrale
  - Il server riceve tutte le richieste e conosce tutto
  - La segnalazione verso i nodi è semplificata (non sempre è necessaria)
  - Può essere determinato il cammino ottimale
- Svantaggi
  - Problemi di complessità, scalabilità, affidabilità e velocità
  - Non consona ad IP (se non per sistemi semplici)
  - Per il cammino ottimale occorre poter dominare e segnalare l'instradamento

Modalità Centralizzata

- Adatta a piccoli sistemi con server ridondati in reti di tipo Hub and Spoke



Modalità Distribuita

- Ogni nodo conosce le risorse occupate e concorre al CAC
- Caratteristiche
  - E’ un sistema robusto
  - Occorre un sistema di segnalazione per raccogliere la disponibilità dei nodi e prenotare (SS7, RSVP)
  - E’ molto complesso determinare il cammino ottimale

Modalità all'ingresso

- Il CAC è effettuato dai router all'ingresso
  - E' un sistema misto
  - Si può determinare il cammino ottimale (QoS Routing)
- Caratteristiche
  - Occorre un sistema di segnalazione per raccogliere lo stato di occupazione (estensioni di IGP, BGP)
  - Occorre un sistema di segnalazione per prenotare (RSVP)

IL CONTROLLO DELLE RISORSE

IntServ, DiffServ

Meccanismi di controllo delle risorse

- Il controllo delle risorse deve utilizzare meccanismi scalabili e distribuiti
- Ci sono due approcci in IETF che si differenziano per le garanzie che offrono e la complessità che presentano
  - Integrated Services (**IntServ**)
  - Differentiated Services (**DiffServ**)

INTEGRATED SERVICES

IntServ

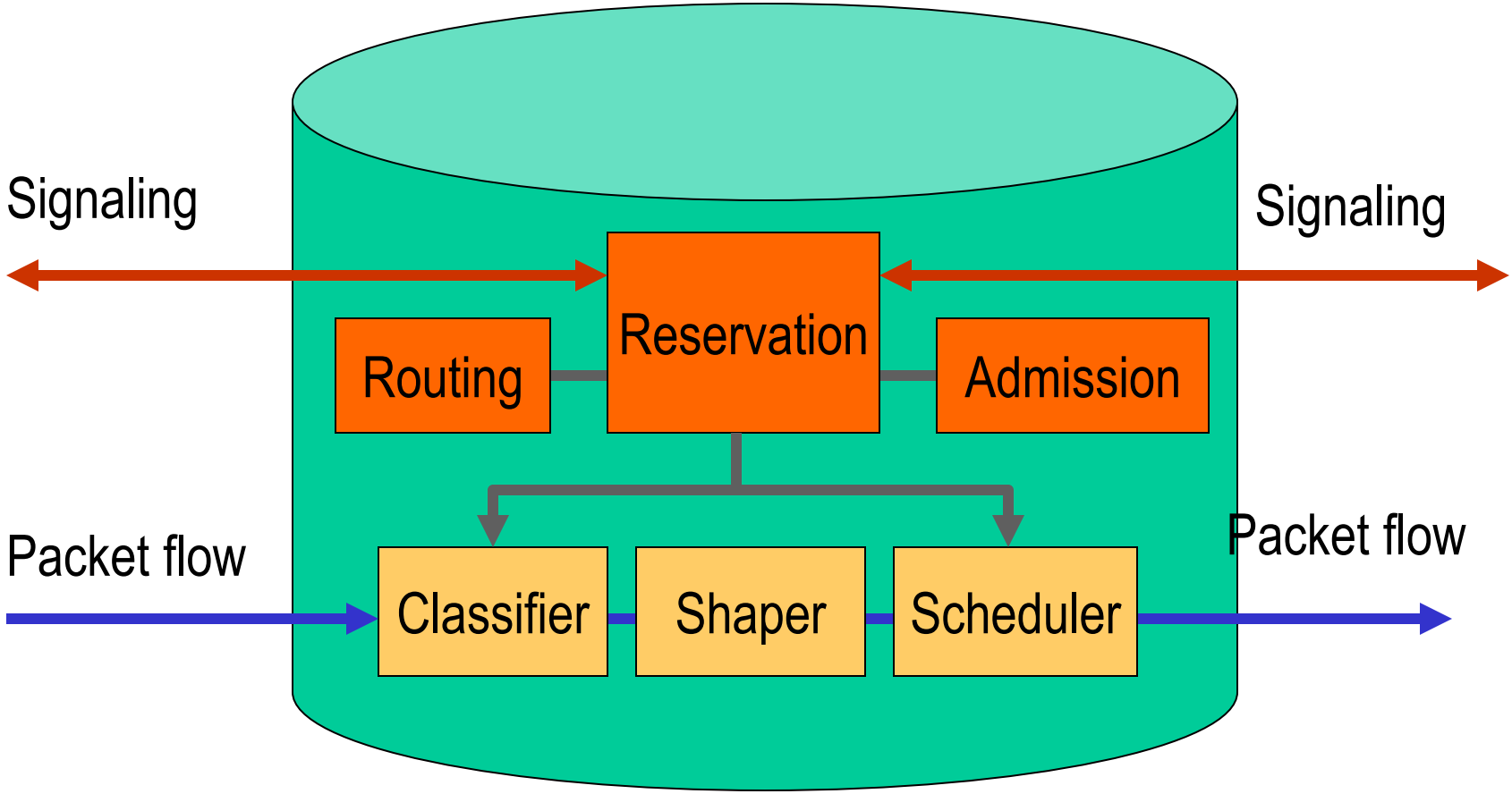
Integrated Services

- Introducono in IP una modalità di controllo dinamica e assoluta (RFC 2215) di ciascun flusso d'utente
- Offrono due classi di servizio oltre alla classe Best-Effort
  - Controlled Load (RFC 2211)
  - Guaranteed Service (RFC 2212)
- Si basano su modifiche sostanziali all'architettura dei router
- Utilizzano RSVP per prenotare le risorse (RFC 2210)

Modalità assoluta di controllo e assegnazione delle risorse

- E’ il paradigma da sempre utilizzato in telefonia:
  - Sistema di prenotazione flusso per flusso a blocco
  - Le risorse vengono richieste dall’utente
  - Se esistono vengono prenotate
  - Se non esistono la richiesta è rifiutata
- Miglioramenti introdotti con IP
  - Diverse classi di servizio (risorse)
  - Utilizzo di risorse prenotate ma non usate

IntServ: funzionalità dei routers

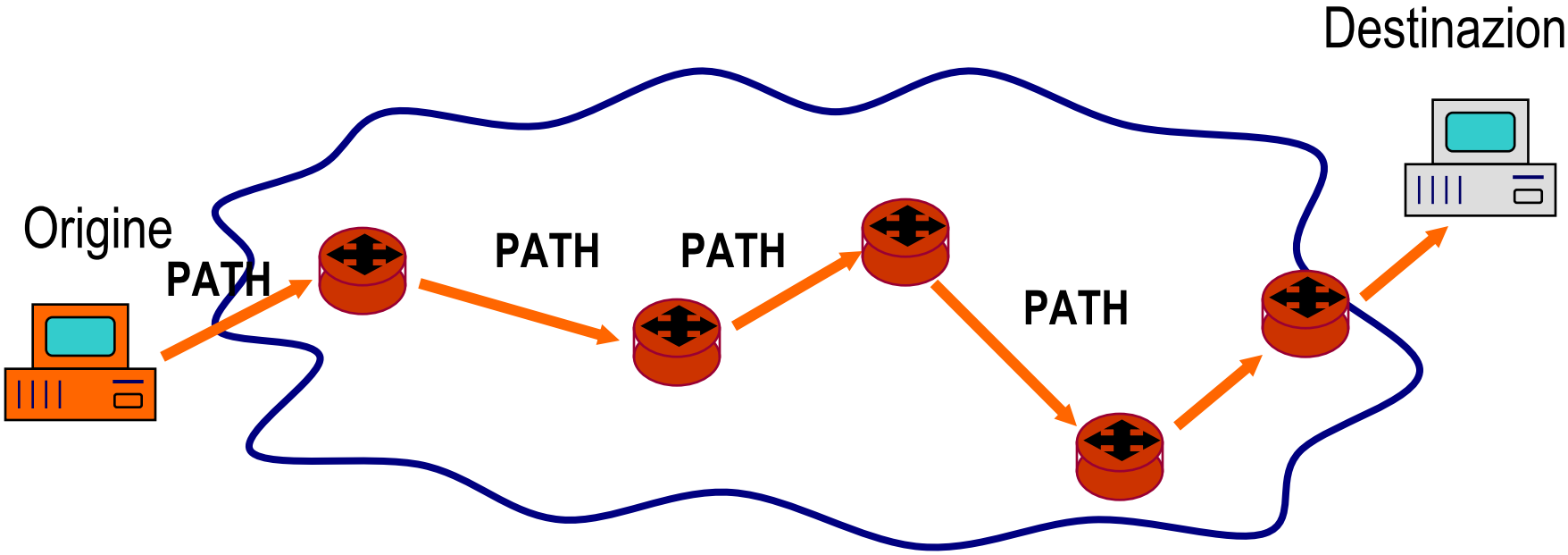


IntServ: prenotazione risorse

- RSVP (Resource reSerVation Protocol) - RFC 2205
- Trasmette ai router sul cammino informazioni di richiesta di risorse e QoS relative ogni flusso
- I routers valutano se le richieste possono essere accettate
- Se si, memorizzano le richieste delle chiamate accettate in modo da poterle soddisfare all'arrivo dei flussi
- Lo stato nei router ha una validità limitata nel tempo (soft state)

RSVP – PATH MESSAGE

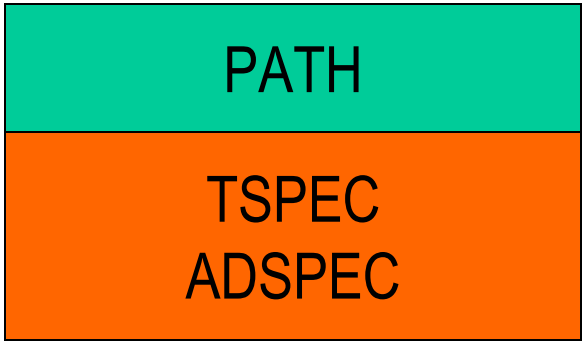
- Fissa il cammino su cui si effettua la riservazione



- La sorgente invia un messaggio di PATH verso la destinazione.
- Ciascun router che riceve un messaggio di PATH mantiene l'indirizzo del nodo precedente attraversato dal flusso.

RSVP – PATH MESSAGE

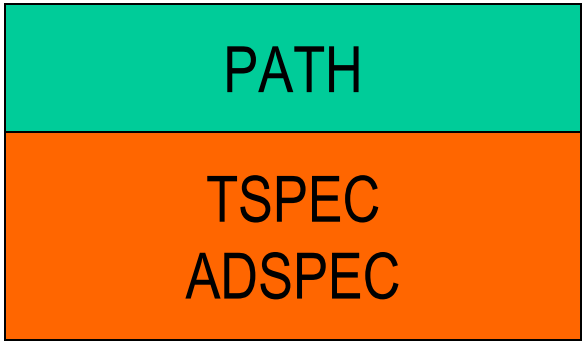
- Informa i router delle caratteristiche del flusso



- TSPEC contiene la descrizione del traffico generato dalla sorgente (per es. attraverso i parametri del token bucket)
- TSPEC non può essere modificato dai router

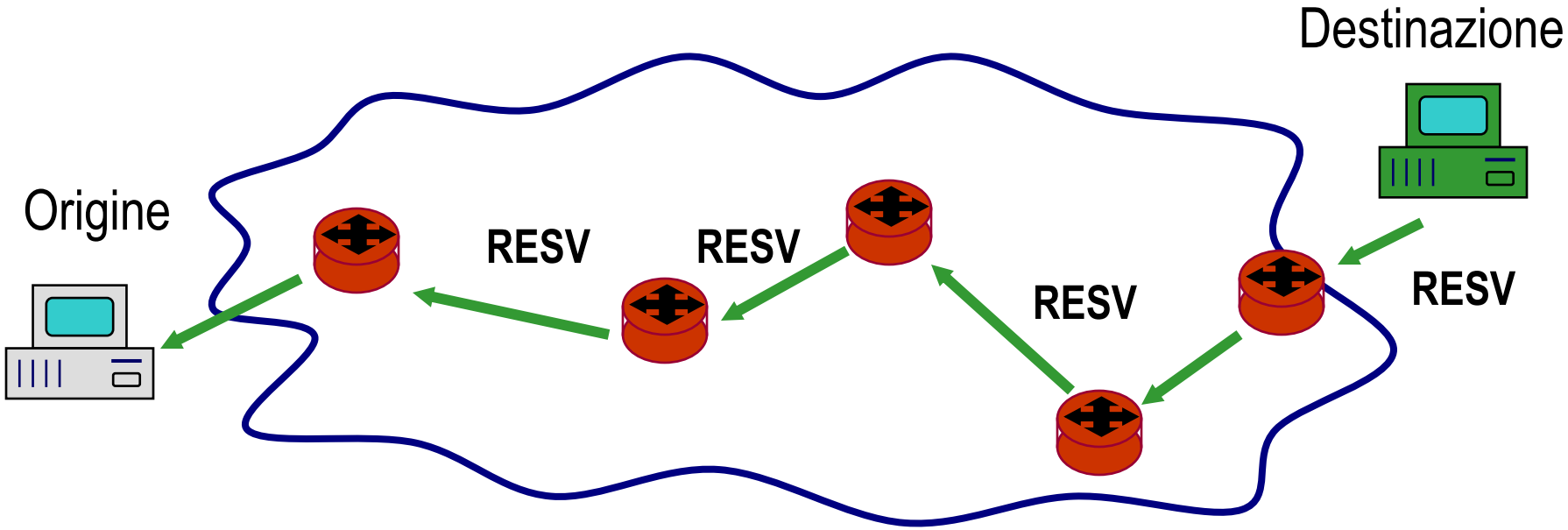
RSVP – PATH MESSAGE

- Raccoglie informazioni preliminari sulla QoS sul cammino



- ADSPEC, esaminato e opportunamente modificato ad ogni hop, sintetizza informazioni sulla QoS conseguibile sul cammino (es. se ci sono router non RSVP-compliant, se alcuni classi di servizio non sono supportate, la MTU minima sul cammino etc.)

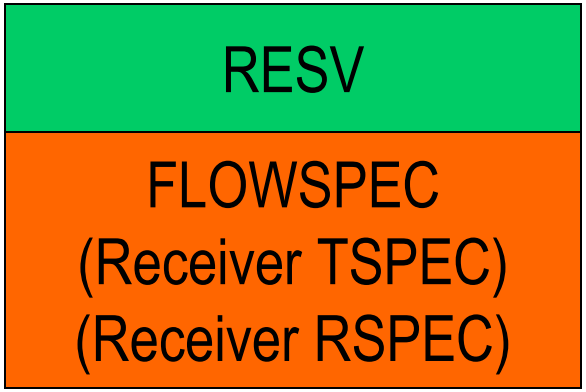
RSVP – PATH MESSAGE



- Sulla base del Sender TSPEC e del campo ADSPEC ricevuto, la destinazione stabilisce che richiesta di riservazione effettuare, e la invia nel campo FLOWSPEC del messaggio RESV verso la sorgente

RSVP – PATH MESSAGE

- Raccoglie informazioni preliminari sulla QoS sul cammino

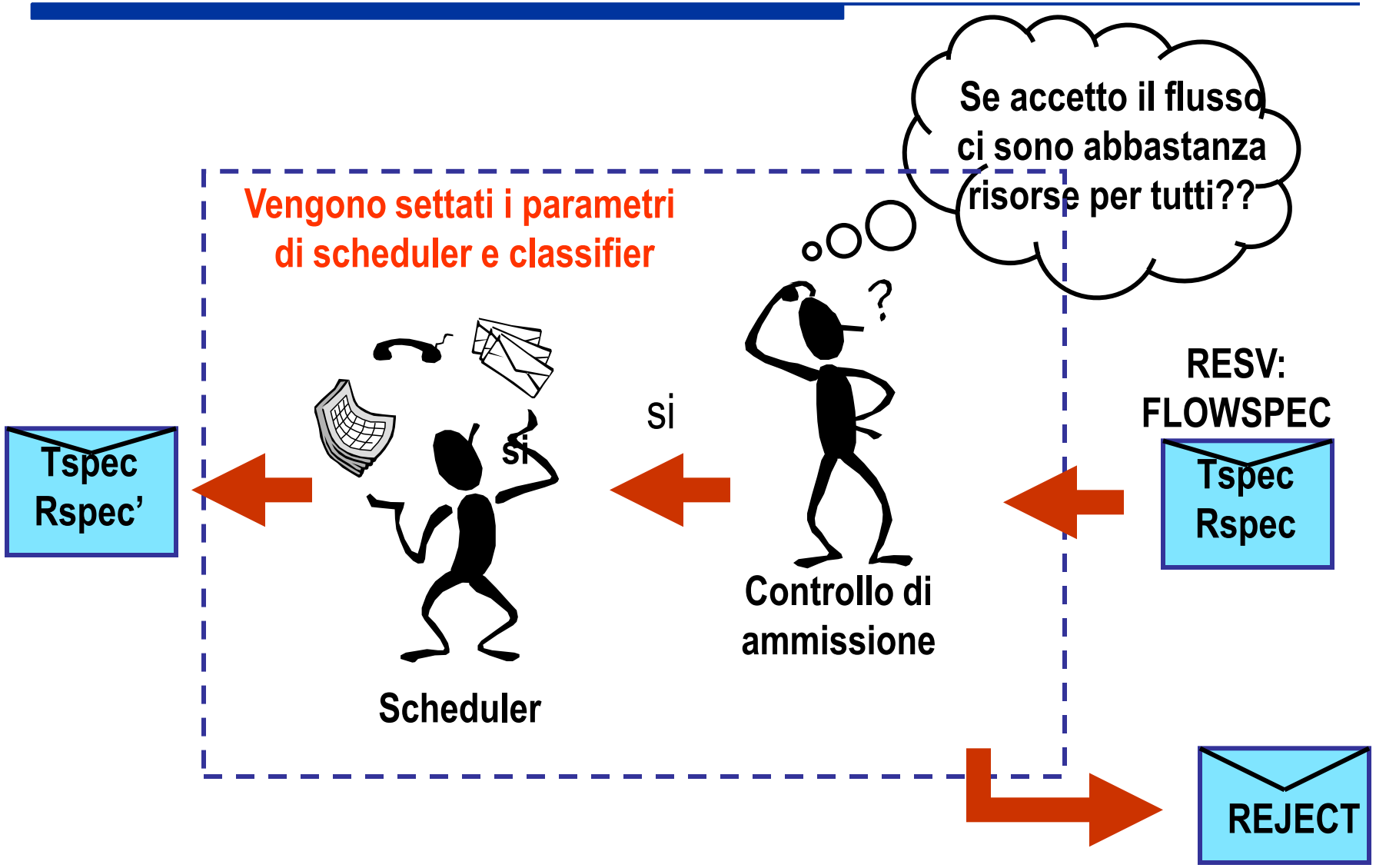


- In TSPEC sono contenute le descrizioni del traffico, eventualmente cambiate dal receiver
- In RSPEC sono contenute le descrizioni del tipo di servizio desiderato

Controllo di ammissione

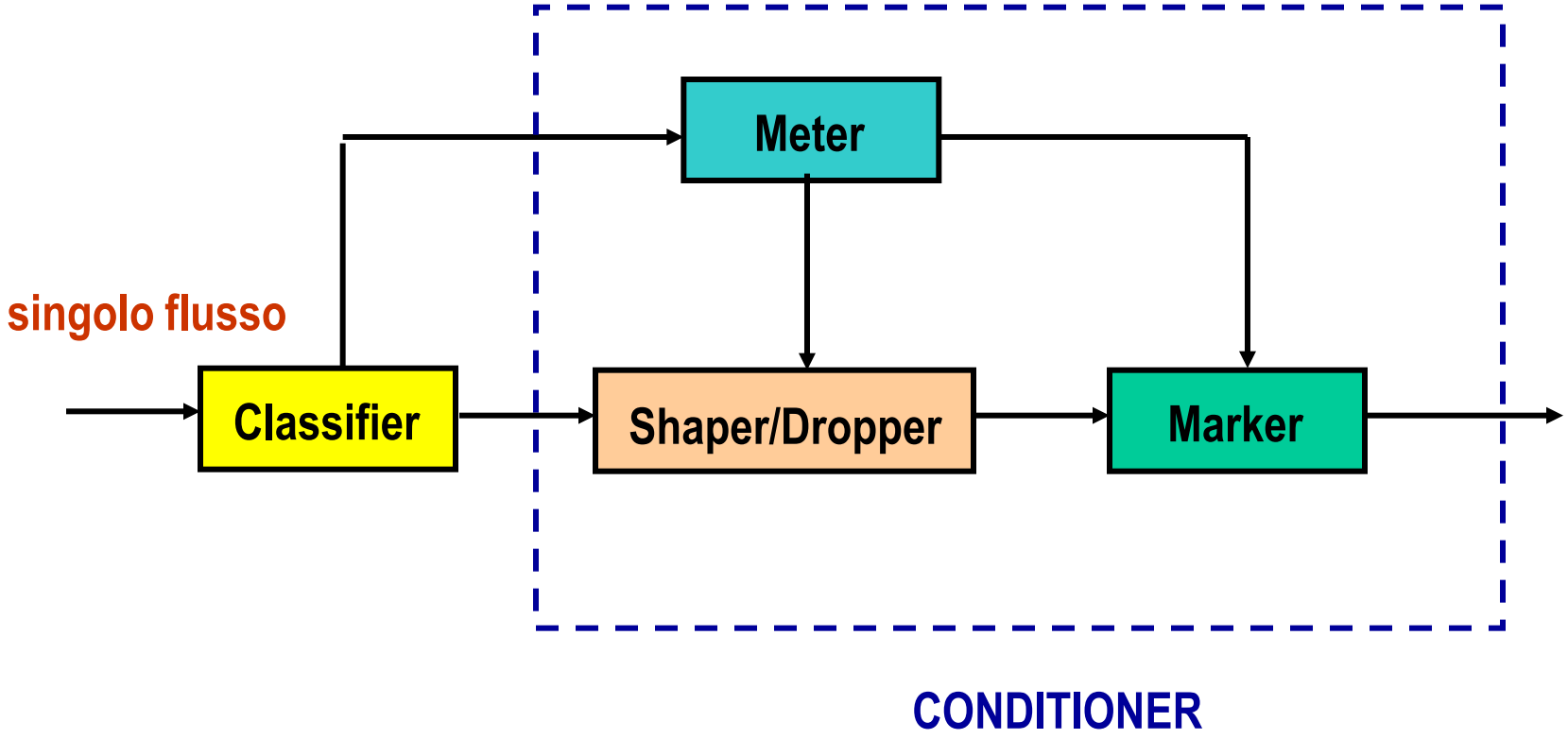
- Riceve in input informazioni sul nuovo flusso
  - **RSPEC:** definisce la QoS desiderata (Reserve Spec.)
  - **TSPEC:** descrive il flusso dati (Traffic Spec.)
- Conosce l'occupazione delle risorse dovuta a chiamate già accettate
  - Parametri di traffico 'a priori' delle chiamate accettate
  - 'misurazioni' della effettiva occupazione delle risorse
- Determina le risorse da assegnare alla nuova chiamata
  - Accetta il nuovo flusso se le risorse esistono
  - Altrimenti rigetta il flusso
- Determina nuove RSPEC da inviare a monte

RSVP – RESV MESSAGE
Decisione al router



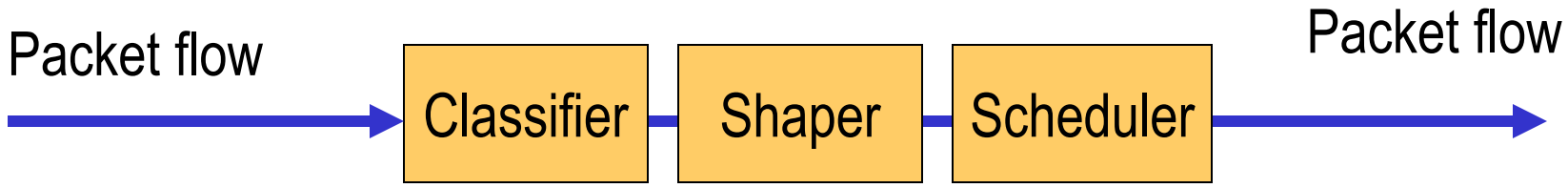
Controllo del traffico

- I Router di frontiera devono effettuare POLICING sui parametri dichiarati



Controllo del traffico

- I router interni effettuano
  - Classificazione dei pacchetti di ciascun flusso
  - Shaping nei casi richiesti per semplificare lo scheduler
  - Scheduling basato sulla QoS richiesta

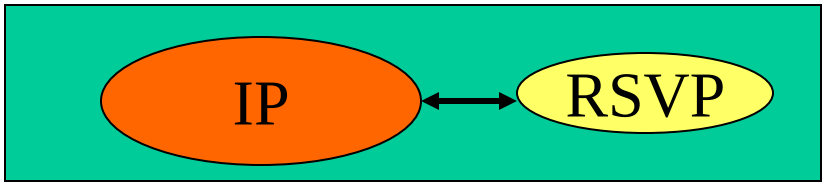


Soft State

- Lo stato nei router ha una validità limitata nel tempo e controllata da un timer. La sorgente e la destinazione inviano quindi periodicamente nuovi messaggi di PATH / RESV
- Vantaggi:
  - recupero da situazioni di errore
  - tolleranza alla perdita di pacchetti di segnalazione
  - buona adattabilità a cambiamenti del cammino tra sorgente e destinazione
- Svantaggio: segnalazione pesante

Il protocollo RSVP

- E’ un protocollo che si colloca a livello 3, anche se usa i servizi stessi di IP

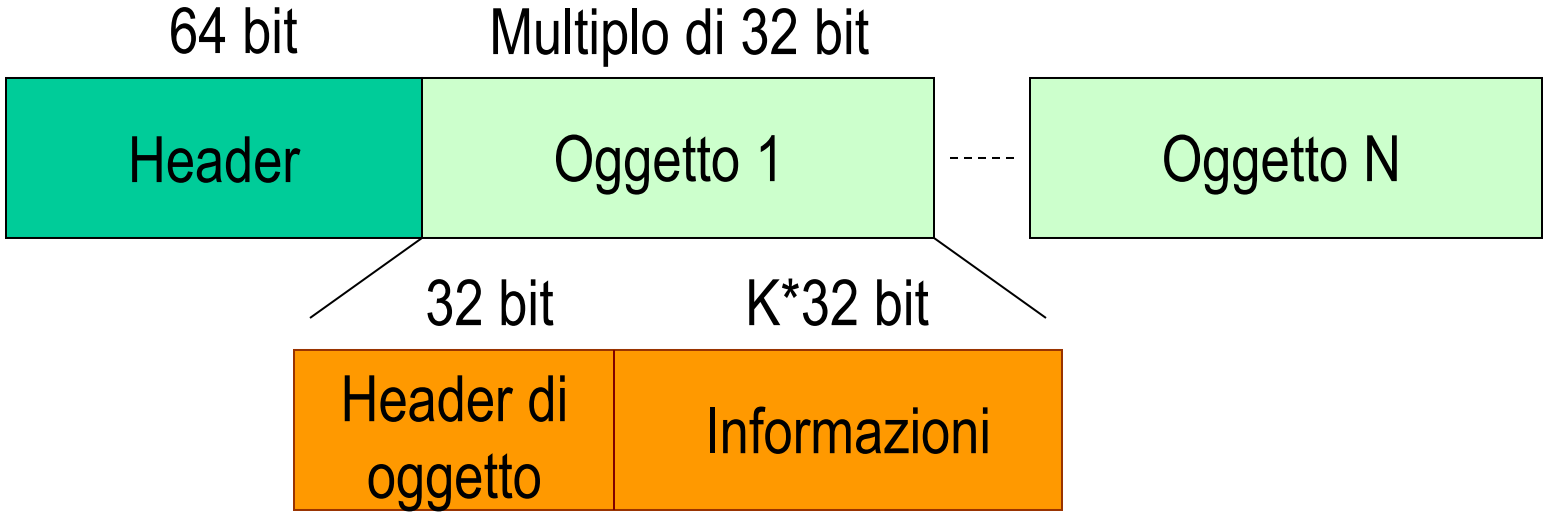


- I messaggi RSVP vengono trasmessi all’interno di un pacchetto IP con protocol ID 46
- E’ richiesto che venga limitata la congestione dei pacchetti di segnalazione, tramite o l’assegnazione di una quantità di banda per la segnalazione, o l’utilizzo di meccanismi a priorità

Messaggi RSVP

- PATH messaggio iniziale sul cammino di andata
- RESV messaggio di riservazione sul cammino di ritorno
- PATH ERR comunica l'identificazione di errori durante l'elaborazione del messaggio di PATH
- RESV ERR indica il fallimento della fase di riservazione
- PATH TEAR abbattimento dello stato instaurato nei router da un messaggio di PATH
- RESV TEAR abbattimento dello stato instaurato nei router da un messaggio di RESV
- RESV CONF è un messaggio inviato alla destinazione per confermare la riuscita della fase di riservazione delle risorse

Formato dei messaggi RSVP



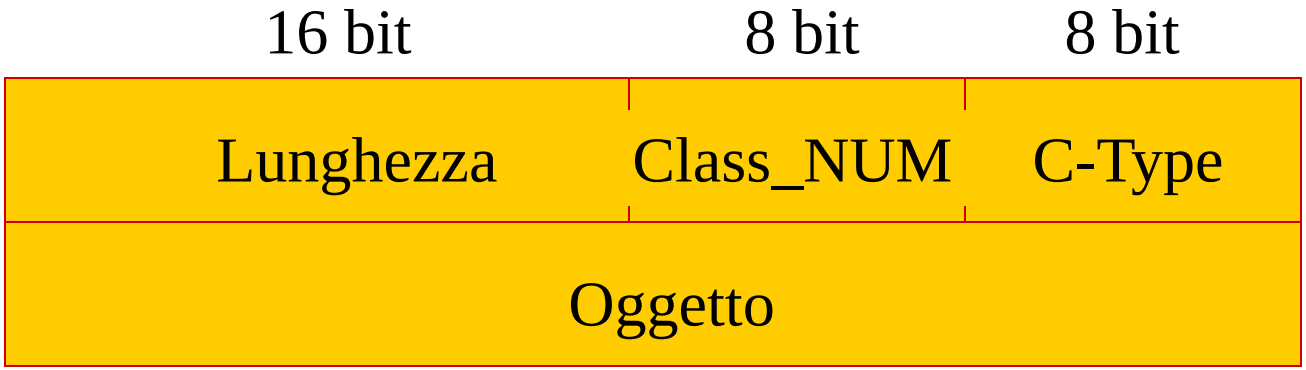
- Ciascun oggetto (multiplo di 32 bit) raggruppa informazioni di carattere simile trasportate dal messaggio (ad esempio la caratterizzazione del traffico, o dati di policing)

Header dei messaggi RSVP

Vers Flags	Msg Type	RSVP Checksum
Send_TTL	Reserved	RSVP Length

- Vers indica la versione del protocollo (attualmente 1)
- Flags non e' ancora specificato
- Msg Type contiene l' identificatore del tipo di messaggio (PATH, RESV, etc)
- RSVP Checksum verifica l'integrità del contenuto del messaggio
- Send_TTL (tramite il confronto con il TTL dell'header IP permette di individuare l'attraversamento di nodi non RSVP)
- RSVP Length indica la lunghezza del messaggio

Formato degli oggetti RSVP



- Lunghezza indica la lunghezza dell'oggetto in byte
- Class_NUM identifica un tipo di oggetto (Es. FILTER_SPEC, ADSPEC, SENDER_TSPEC, RSVP_HOP, TIME VALUES, etc.)
- C_Type identifica univocamente il tipo di formato usato per un tipo di oggetto (1 → IPv4, 2 → IPv6)

Formato dei messaggi di PATH

1	Flag	1	RSVP Checksum
Send_TTL		Reserved	RSVP Length
INTEGRITY (autentic. e integrità)			
SESSION (identifica la sessione)			
RSVP_HOP (ultimo nodo RSVP compatibile)			
TIME_VALUES (refresh)			
POLICY_DATA			
SENDER_TEMPLATE (identifica i flussi di ogni SENDER)			
TSPEC (caratteristiche del flusso)			
ADSPEC (stime raccolte)			

Formato dei messaggi di RESV

1	Flag	2	RSVP Checksum
Send_TTL		Reserved	RSVP Length
INTEGRITY (autentic. e integrità)			
SESSION (sessione di riferimento)			
RSVP_HOP (ultimo nodo RSVP compatibile)			
RSV_CONFIRM (rich. conferma alla destinaz)			
POLICY_DATA			
TIME_VALUES (refresh)			
SCOPE (sorgente a cui inviare resv)			
STYLE (res singola o multipla)			
FLOWSPEC			

Guaranteed Service (RFC 2212)

- E’ il primo fra due classi di servizio INTSERV (oltre al best effort) con assegnazione di risorse e blocco all’ammissione
- Emula il servizio a circuito con ritardi garantiti
- Garantisce
  - perdita nulla nei buffer di trasmissione
  - un upper bound al ritardo

Guaranteed service (RFC 2212)

- Si basa sulle formule già viste per il bound sul flusso i nel router j

$$W_i \le \frac{k - M}{B_i}\frac{p - B_i}{p - b} + \frac{M}{B_i} + \frac{C_i}{B_i} + D_i \qquad \text{se} \quad B_i < p$$

$$W_i \le \frac{M}{B_i} + \frac{Ci}{B_i} + D_i \qquad \text{se} \quad B_i > p$$

C_j e D_j dipendono solo dal router j

- **Teorema**: il bound sul ritardo end-to-end si ottiene semplicemente rimpiazzando C_j e D_j con

$$C_{tot} = \sum C_j \qquad D_{tot} = \sum D_j$$

Guaranteed service (RFC 2212)

- TSPEC contiene i parametri del token bucket
- ADSPEC contiene i campi C_{tot} e D_{tot} che vengono aggiornati di router in router

$$C_{tot} = \sum C_k \qquad D_{tot} = \sum D_k$$

Guaranteed service (RFC 2212)

- Il ricevitore sulla base di ADSPEC determina la banda B_j che i router devono assegnare al flusso j e lo Slack

  S = bound(R) - bound_desiderato

- e li invia come RSPEC
- Se S è positivo, i router a monte possono ridurre B_j e S e aggiornare RSPEC
- Se la banda B_j non è disponibile la chiamata viene rifiutata
- Costa in complessità negli apparati dei router (classifier, shaper, scheduler) che devono gestire flusso per flusso
- E' il più adatto alla telefonia

Controlled load service (RFC 2211)

- Offre un servizio che emula il “best effort” in una rete non congestionata:

  A very high percentage of transmitted packets will be successfully delivered by the network to the receiving end-nodes. (The percentage of packets not successfully delivered must closely approximate the basic packet error rate of the transmission medium).

  The transit delay experienced by a very high percentage of the delivered packets will not greatly exceed the minimum transmit delay experienced by any successfully delivered packet. (This minimum transit delay includes speed-of-light delay plus the fixed processing time in routers and other communications devices along the path.)

Controlled load service (RFC 2211)

- Controlled Load Service (CLS) utilizza un meccanismo di shaping solo all'ingresso
- Non garantisce ritardi
- La gestione nei nodi è più semplice
- Lascia ampio spazio a varianti di implementazione

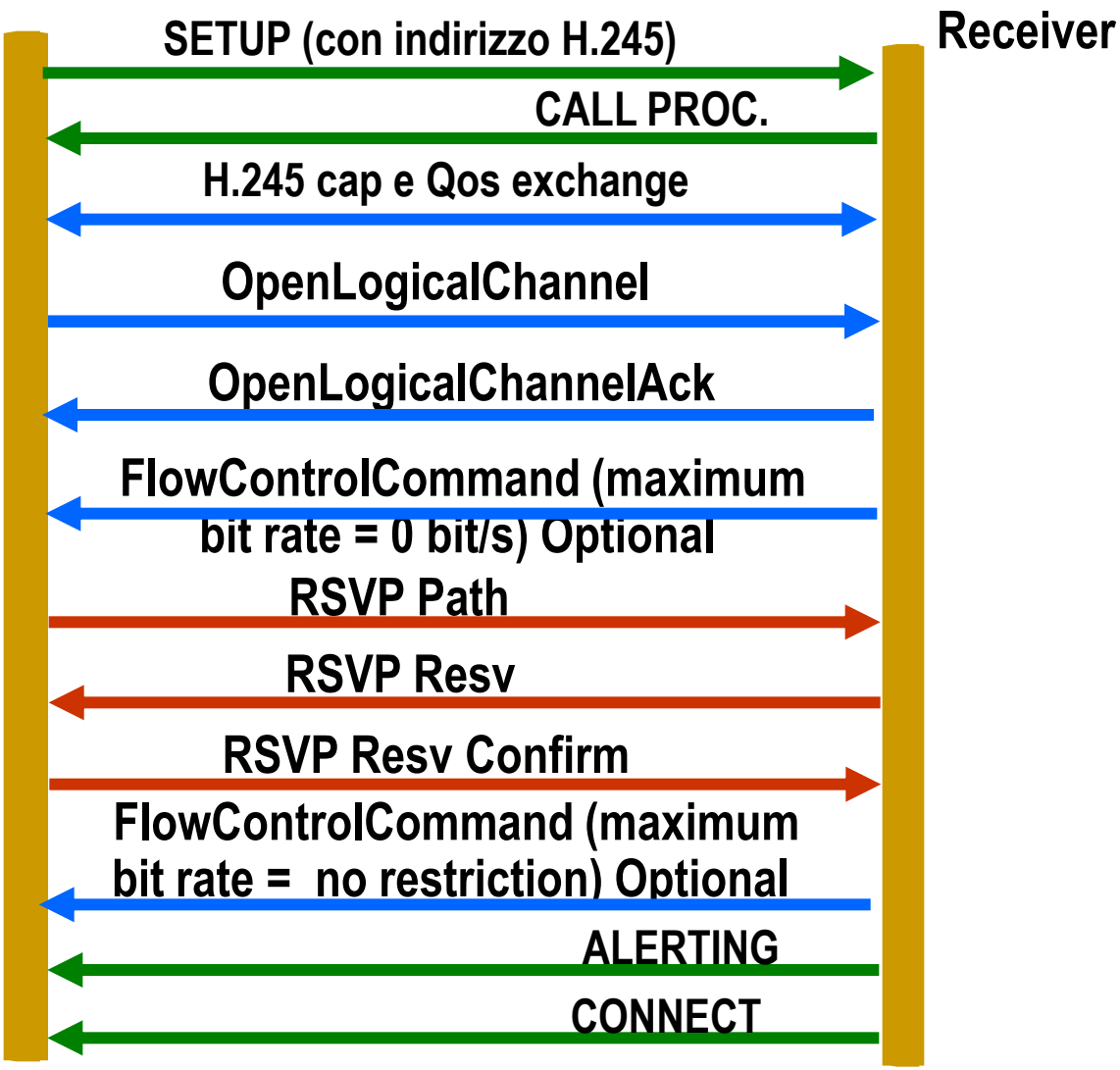
Controlled load service (RFC 2211)

- TSPEC contiene la descrizione del token bucket
- ADSPEC è privo di parametri QoS
- FLOWSPEC non contiene RSPEC
- In pratica ogni router decide il rate B_i indipendentemente in base a una politica predeterminata
- Deve essere $B_i > b$
- … ma si può fare overbooking

Sincronizzazione H.323-RSVP

Le fasi di Reservation vanno eseguite per ogni canale

E' possibile usare Fast Connect



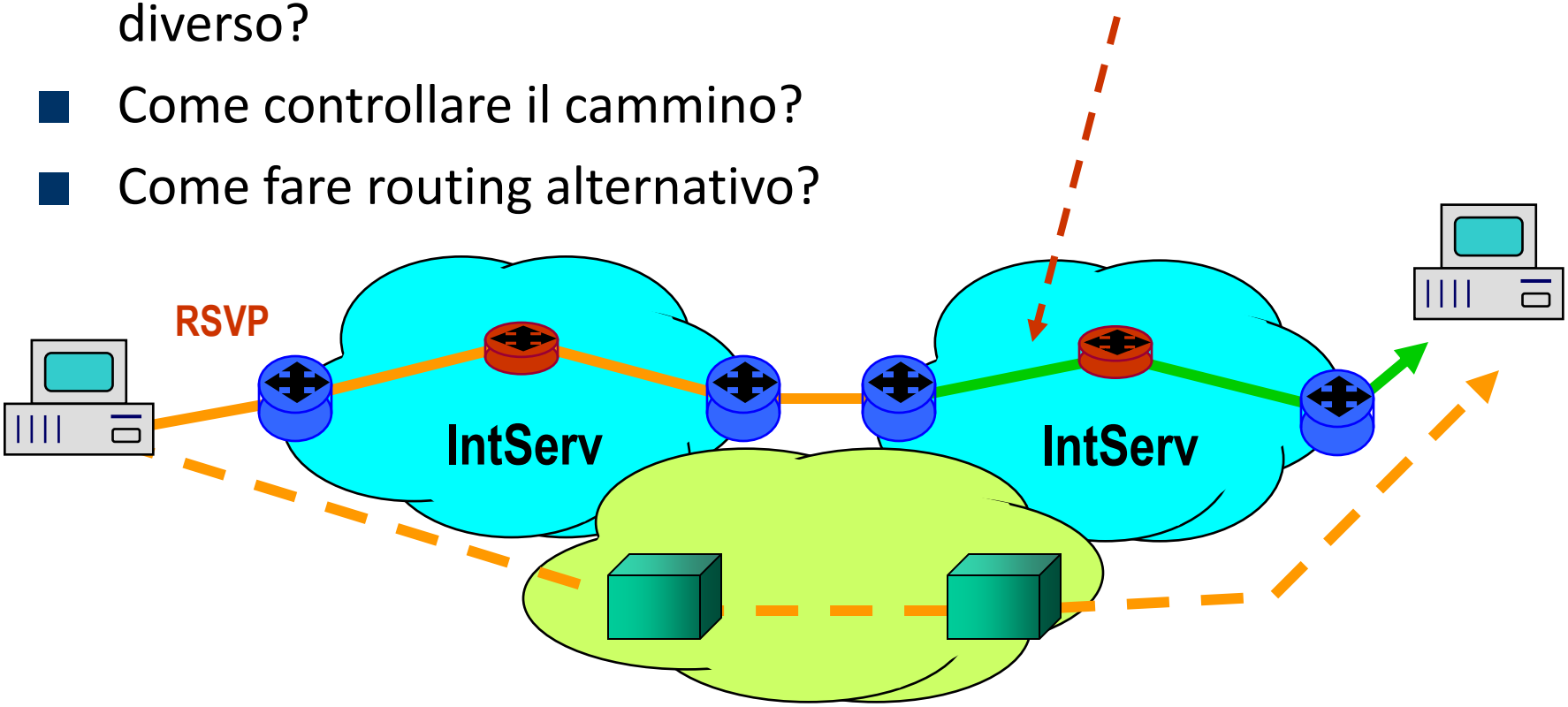
Integrated Services: problemi

- Richiedono di mantenere nei router uno stato per ciascun flusso
- Scarsa scalabilità
- Segnalazione pesante
- Forte impatto sull'architettura di rete esistente

Buona soluzione per la rete di accesso

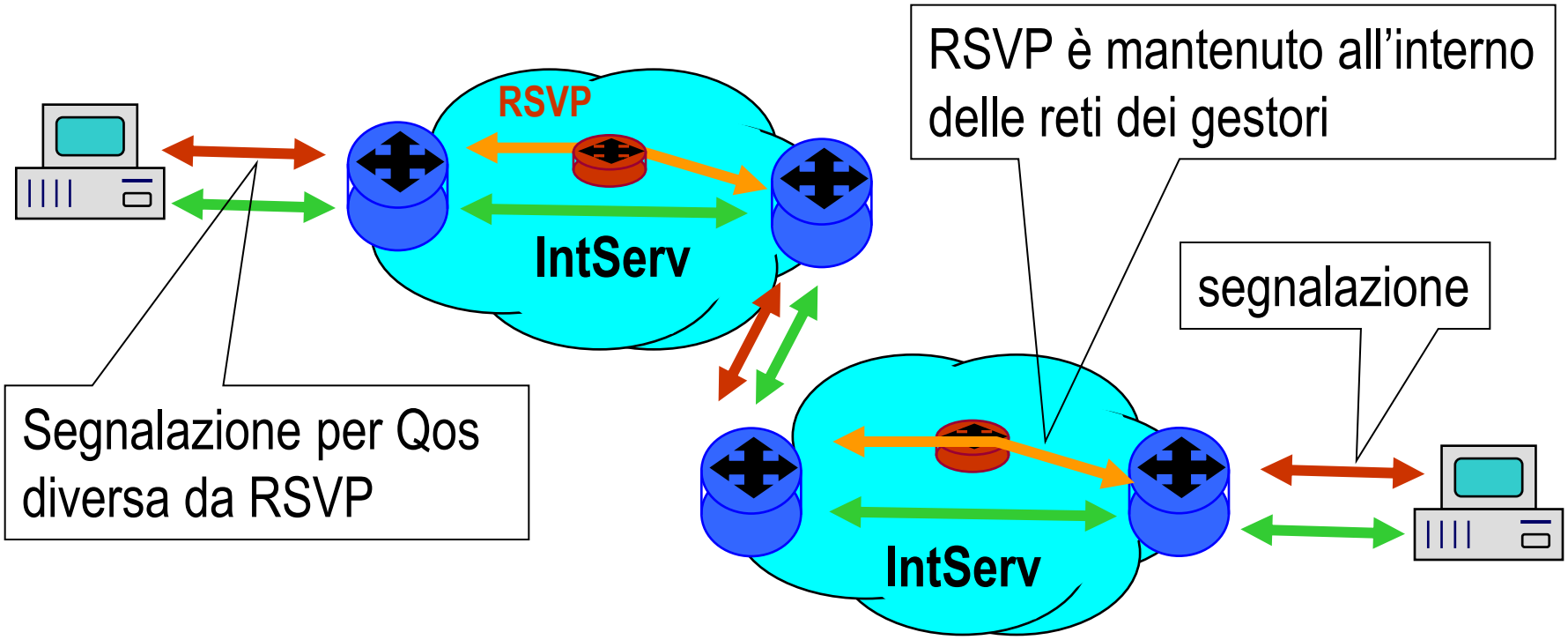
IntServ: problemi non risolti

- I gestori possono lasciare passare la prenotazione RSVP in modo trasparente (o meno)?
- Come riservare risorse per tratte compresse in modo diverso?
- Come controllare il cammino?
- Come fare routing alternativo?



IntServ: problemi non risolti

- L'alternativa è quella di utilizzare dei router d'accesso, gateways IP-IP, o application servers, che terminano le connessioni, effettuano la prenotazione, rerouting, conversione di formato



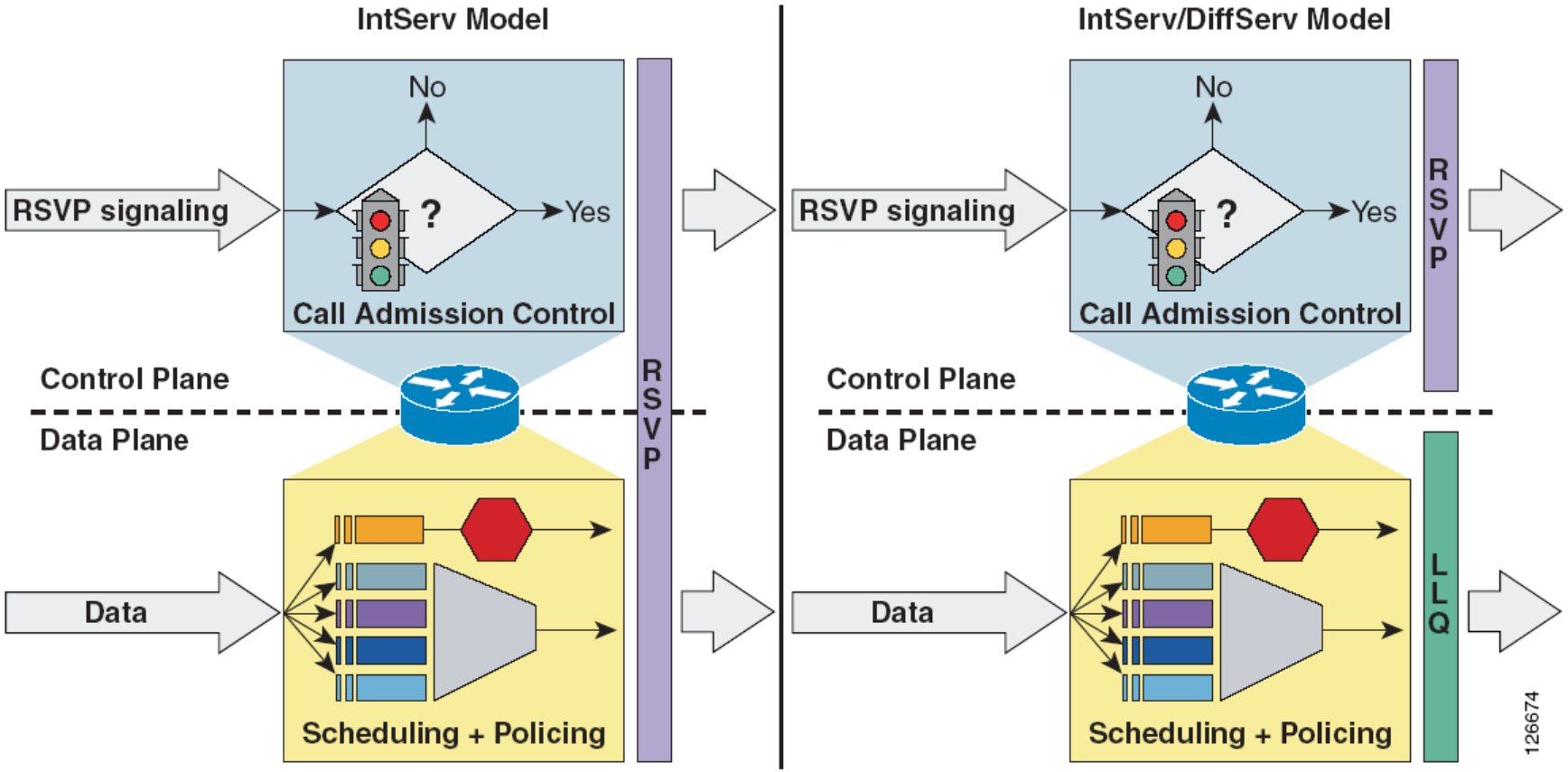
DIFFERENTIATED SERVICES

DiffServ

Differentiated Services

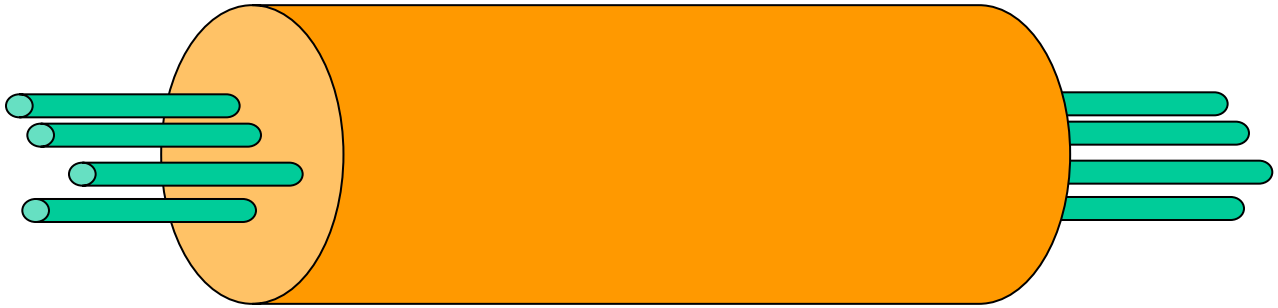
- Perseguono una soluzione semplice, scalabile e di basso costo
- Si rinuncia al controllo stretto flusso per flusso nel forwarding dei router
- Si dimensiona la classe di servizio collettivamente all'interno di un singolo router
- Le reservations possono ancora essere fatte flusso per flusso attraverso RSVP

RSVP e Differentiated Services



Microflussi senza controllo

- I microflussi non possono essere controllati
- Il traffico che eccede sottrae QoS a tutti



- A livello microflusso (es. per telefonia) occorre una gestione esterna ai DiffServ, che controlli lo stato di allocazione delle pipes DiffServ

Differentiated Services (RFC 2475)

Come

- Le operazioni complesse e il controllo dei microflussi sono compito esclusivamente dei bordi della rete.
- I router di rete devono essere solo in grado di applicare forwarding differenziati a poche differenti classi di traffico
  - Non richiedono modifiche significative, ed in particolare non necessitano di mantenere uno stato per flusso o gestire segnalazione).

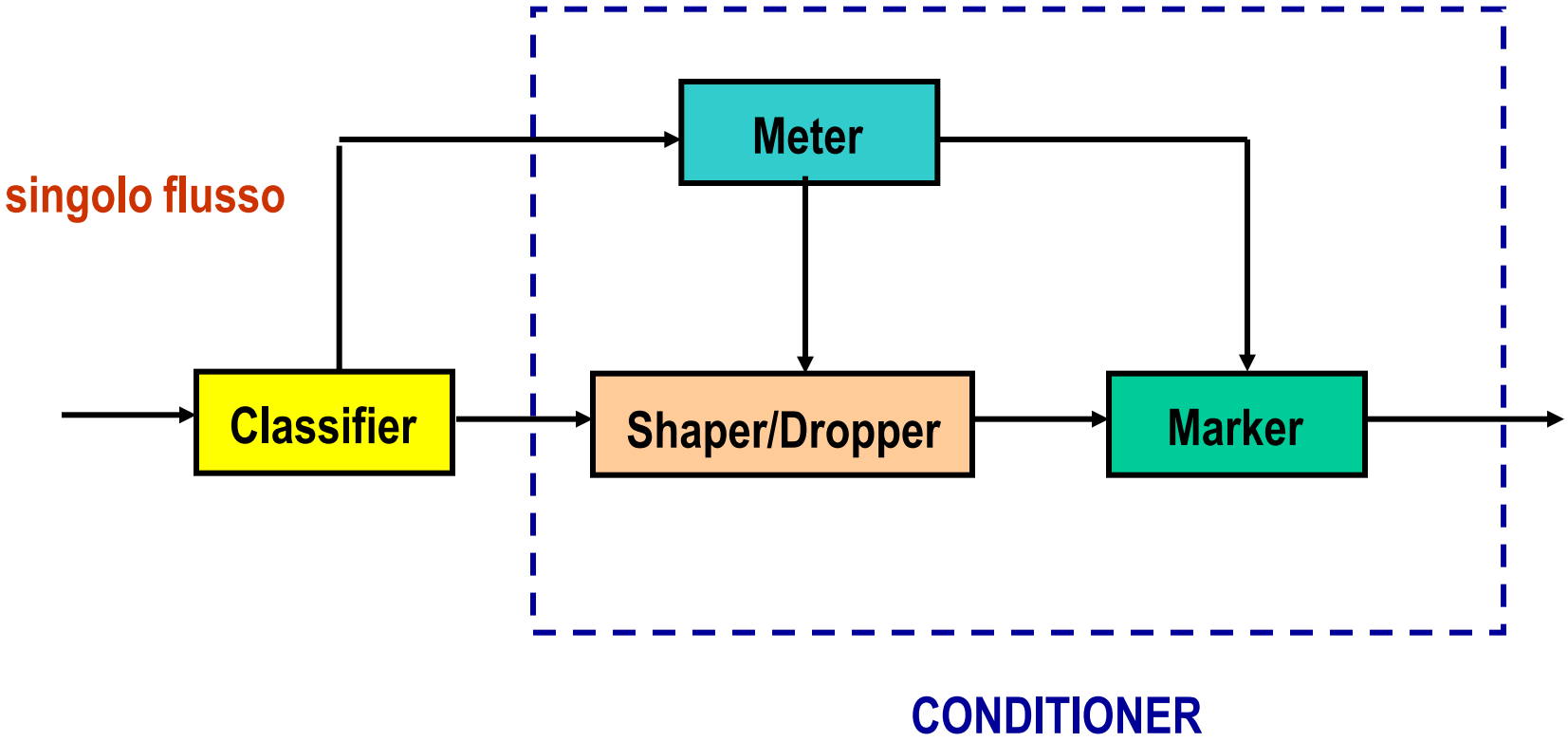
Differenziazione dei flussi

- Viene usato il campo (DS) dell'header IP corrisponde al TOS (Type Of Service) byte di IPv4 o al Traffic Class byte di IPv6
- 6 bit sono utilizzati per specificare il Differentiated Service Code Point (DSCP), mentre i rimanenti due bit non sono utilizzati
- Il DSCP viene usato dai router per selezionare il tipo di servizio (o Per-Hop-Behavior o PHB) da applicare (Es. 0X00 standard per best effort forwarding)

Controllo d’accesso

- E’ basato su un contratto, Service Level Specification, che specifica il servizio statico offerto al traffico globale generato dall’utente
  - Tipo di servizio e prestazioni
  - ‘Scope’ del servizio (se il servizio e’ applicato a tutto il traffico o solo alla porzione di traffico tra particolari gateway di accesso e di uscita).
  - Profilo di traffico concordato (Es: parametri del token bucket)
  - Disposizioni per il traffico che eccede il profilo di traffico

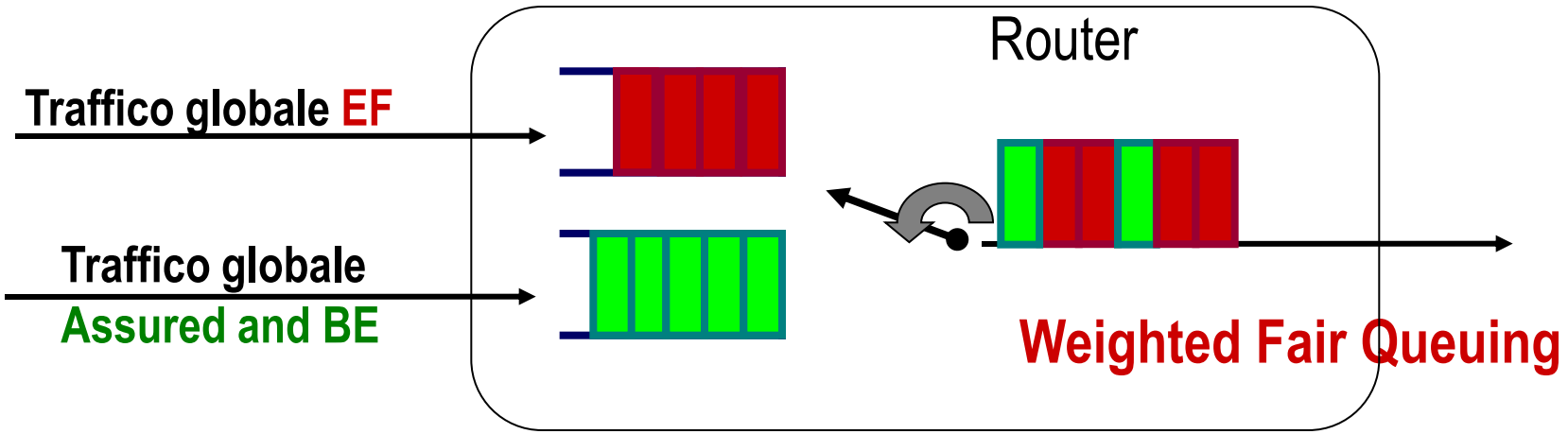
Gateway di accesso



- I router di frontiera gestiscono aggregati di traffico e verificano la coerenza con gli SLA interdominio

Possibili PHB (servizi)

- Per Hop Behavior (PHB)
  - **Expedited Forwarding** per applicazioni a basso ritardo
  - **Assured Forwarding** service per applicazioni che richiedono affidabilità di consegna
  - **Best Effort** service, nessuna garanzia



Expedited Forwarding (RFC 2598)

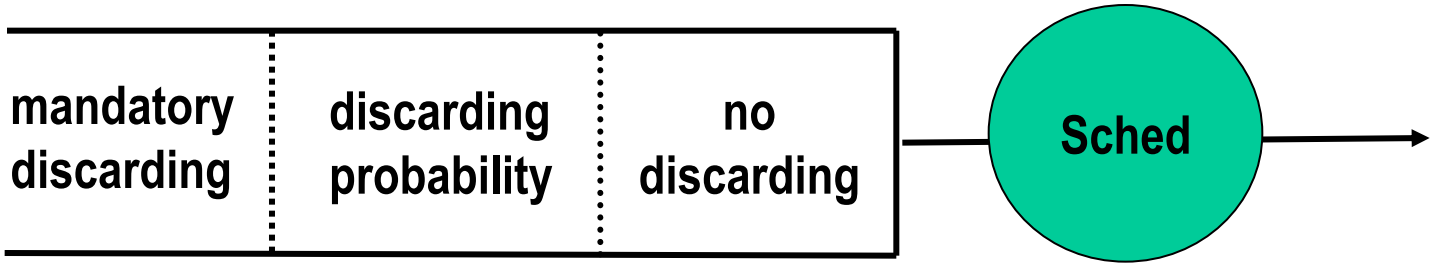
- Expedited Forwarding vuole emulare una linea dedicata:
  - Gli utenti richiedono una quantità di banda per la comunicazione tra due punti
  - Se il traffico non eccede quanto stabilito, i ritardi e la percentuale di pacchetti persi devono essere molto bassi
  - Il traffico va condizionato e controllato. Quello in eccesso non viene immesso in rete.
  - Codepoint 101110

Assured Forwarding (RFC 2597)

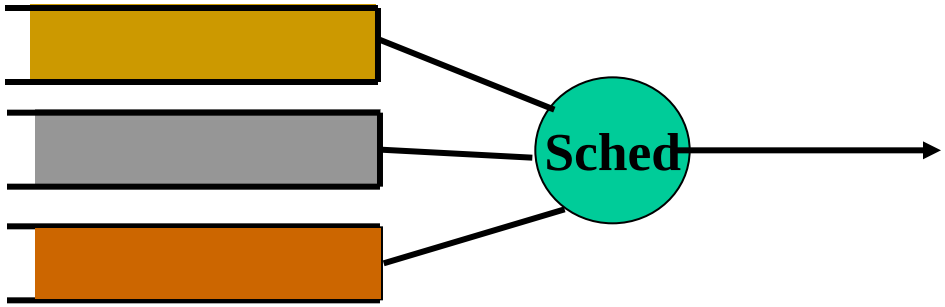
- Assured Forwarding fornisce differenti livelli di garanzie di forwarding (banda e spazio nelle code) (4-livelli)
- Si propone di evitare situazioni di congestione
  - di breve termine con l'accodamento nei buffer
  - di lungo termine tramite un discarding preventivo
  - e differenziato dei pacchetti
- Si introducono così diversi livelli di probabilità di discarding (almeno 3)

Assured Forwarding

- Il discarding dei pacchetti deve avvenire in modo dolce
- Una possibilità è usare RED (per ciascun livello)



RED (Random Early Discarding)

Esempio di Assured forwarding

- Olimpic service: tre di flusso, ciascuna con tre probabilità di discarding
  - **Gold service**: dimensionato con basso carico
  - **Silver service**: dimensionato con medio carico
  - **Bronze service**: dimensionato con medio-alto carico