



Università di Verona
Dipartimento di Informatica



Metodi di rete per garantire la Qualità del Servizio su rete a pacchetto

Davide Quaglia

**(materiale tratto dalle lezioni del prof. J. C. De Martin -
Politecnico di Torino)**

Sommario

- Definizione del problema
- Modello Best Effort
- Parametri di Qualità del Servizio
 - QoS per vari tipi di applicazioni
 - funzione utilità
- Policing e shaping
- Resource reservation protocol (RSVP)
- Modello a Servizi Integrati
- Modello a Servizi Differenziati
- Multi-Protocol Label Switching

Definizione del problema

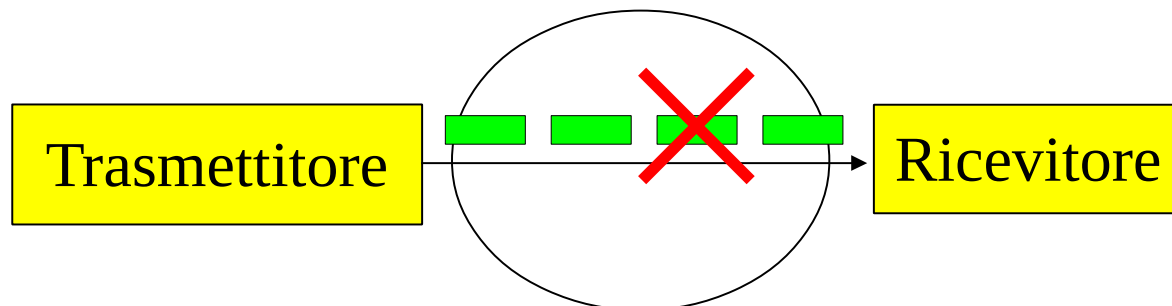
- Le reti a commutazione di circuito avevano una intrinseca garanzia di qualità del servizio (QoS)
- La rete IP tradizionalmente non fornisce garanzie di QoS → modello best effort
- Si può assicurare agli utenti una QoS ?
- Nota: la gestione della QoS non crea banda dal nulla
 - se qualche utente verrà trattato meglio rispetto alla media, qualcun altro verrà trattato peggio

Modello Best Effort

- La rete non assicura nulla all'utente
- La QoS istantanea dipende da
 - carico della rete
 - politiche di traffic engineering e routing
 - controllo di congestione end-to-end (TCP)
 - meccanismi di scheduling e dimensione dei buffer

Parametri di Qualità del Servizio

- Variazione max del ritardo end-to-end
- Frazione max di pacchetti persi oppure Throughput minimo
- Ritardo end-to-end max



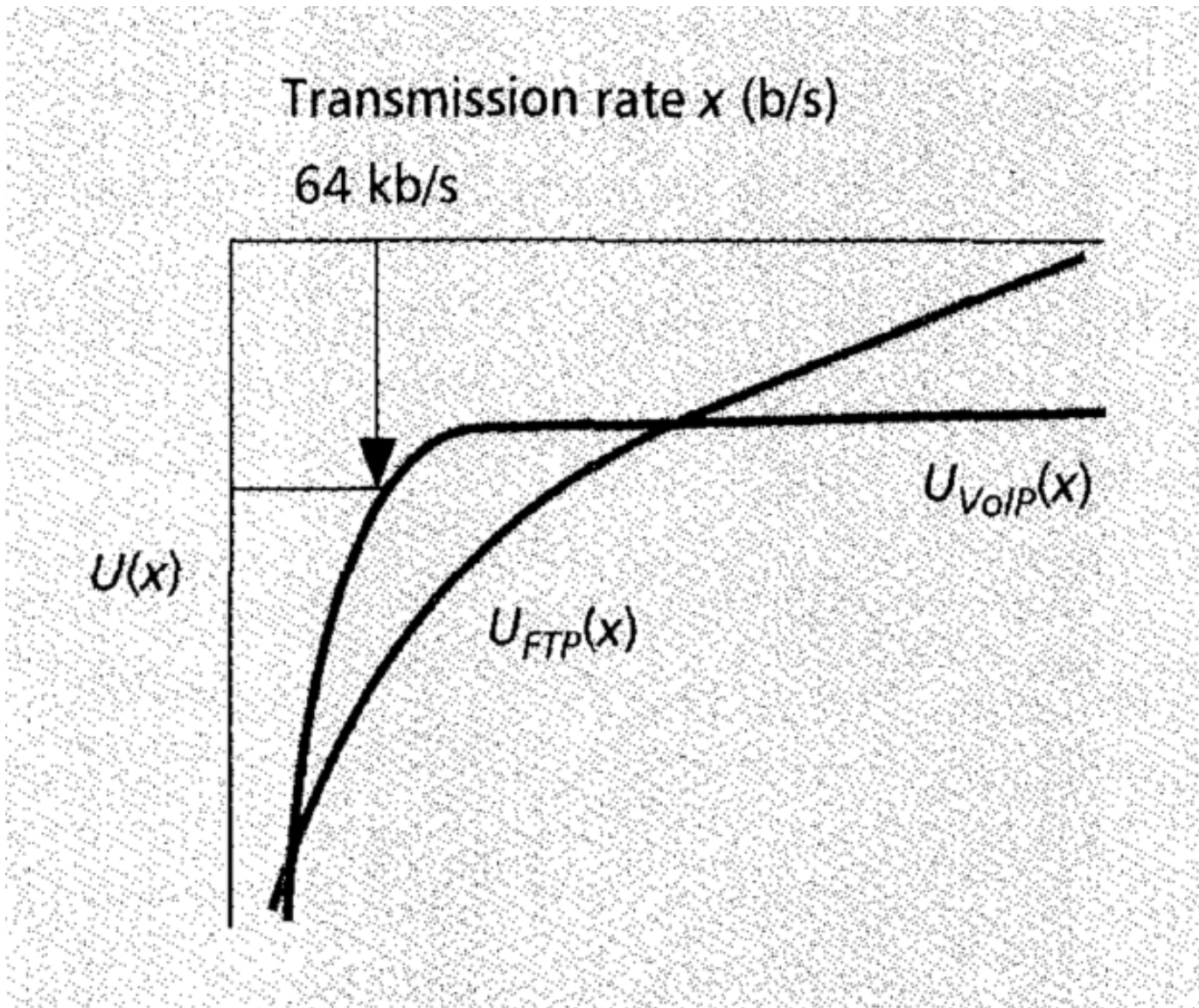
QoS e applicazioni

Error tolerant	Conversational voice and video	Voice messaging	Streaming audio and video	Fax
Error intolerant	Telnet, interactive games	E-commerce, WWW browsing,	FTP, still image, paging	E-mail arrival notification
	Conversational (delay $\ll 1$ sec)	Interactive (delay approx 1 sec)	Streaming (delay < 10 sec)	Background (delay > 10 sec)

QoS e applicazioni interattive

Medium	Application	Degree of symmetry	Data rate	Key performance parameters and target values		
				End-to-end One-way Delay	Delay Variation within a call	Information loss
Audio	Conversational voice	Two-way	4-25 kb/s	<150 msec preferred <400 msec limit Note 1	< 1 msec	< 3% FER
Video	Videophone	Two-way	32-384 kb/s	< 150 msec preferred <400 msec limit Lip-synch : < 100 msec		< 1% FER
Data	Telemetry - two-way control	Two-way	<28.8 kb/s	< 250 msec	N.A	Zero
Data	Interactive games	Two-way	< 1 KB	< 250 msec	N.A	Zero
Data	Telnet	Two-way (asymmetric)	< 1 KB	< 250 msec	N.A	Zero

Funzione utilita'



Modelli di traffico

Parametri caratterizzanti

- Bitrate
 - Bitrate istantaneo
 - Bitrate medio
 - Bitrate di picco
- Inter-packet gap
- Burstiness
- Packet size
- Packet arrival time
- Packet arrival rate

Bitrate

- Istantaneo $B(t)$
 - Numero di bit che passano sul canale nell'unita' di tempo
- Dato un intervallo T di osservazione
 - Bitrate medio

$$\frac{1}{T} \int_0^T B(t) dt$$

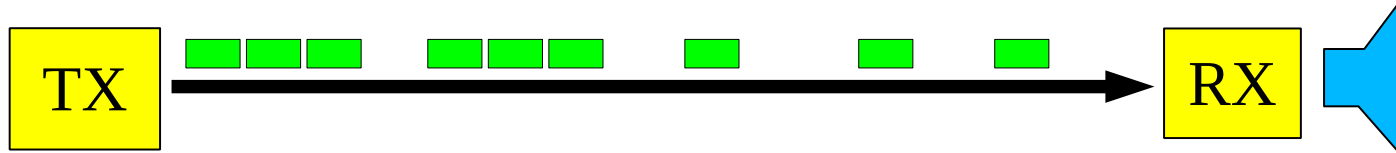
- Bitrate di picco

$$\max_T (B(t))$$

Altri parametri

- Inter-packet gap
 - distanza temporale tra 2 pacchetti successivi
- Burstiness
 - lunghezza media (su un intervallo di osservazione) delle sequenze di pacchetti aventi inter-packet gap nullo
- Packet size
 - dimensione in byte del pacchetto
- Packet arrival time
 - istante di arrivo di un pacchetto al ricevitore
- Packet arrival rate
 - numero medio (su un intervallo di osservazione) di pacchetti che arrivano al RX nell'unità di tempo

Calcolo della burstiness: esempio

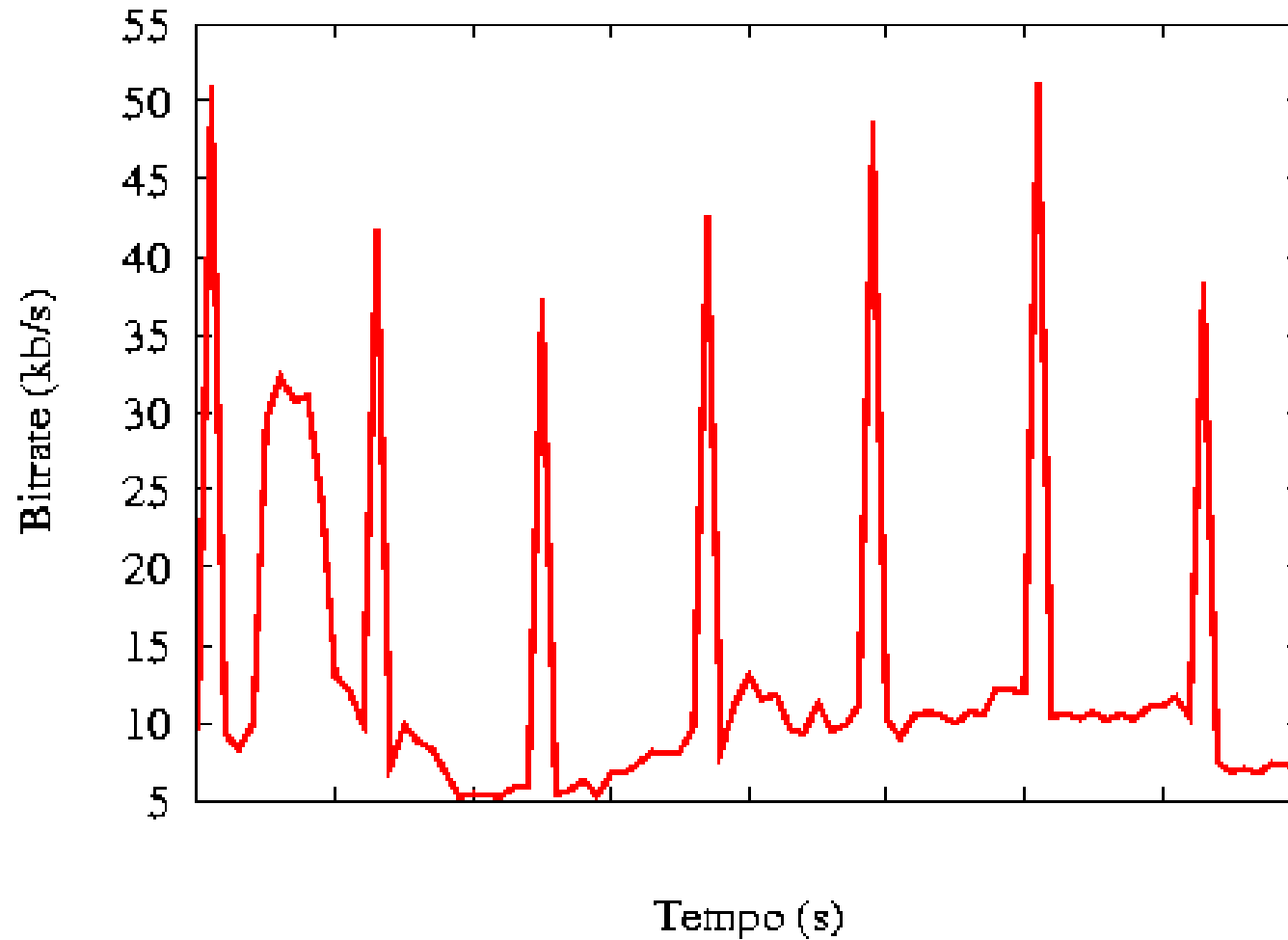


$$\text{lunghezza media del burst} = \frac{(3 + 3 + 1 + 1 + 1)}{5}$$
$$= \frac{9}{5} = 1.8$$

Tipi di modelli di traffico

- **Flussi Constant Bit Rate (CBR)**
 - bitrate istantaneo costante e uguale al bitrate medio
 - Esempio:
 - conversazione telefonica tradizionale (64kb/s)
- **Flussi Variable Bit Rate (VBR)**
 - bitrate istantaneo variabile nel tempo
 - caratterizzato da un bitrate medio e di picco
 - Esempio:
 - traffico dati su una linea dialup
 - flusso di bit prodotto da un codificatore video MPEG

Traffico VBR di MPEG



Gli utenti e la rete

- Gli utenti
 - generano traffico avente certe caratteristiche
 - possono chiedere alla rete di assicurare una certa QoS per il proprio traffico
- La rete
 - accetta traffico dagli utenti
 - recapita i pacchetti verso le destinazioni
 - puo' concordare con l'utente che, a fronte di un traffico con certe caratteristiche, garantira' certi valori di QoS (Service Level Agreement - SLA)
 - puo' **riservare risorse** a certi utenti dotati di SLA
 - Spazio nelle code
 - Capacità sui link

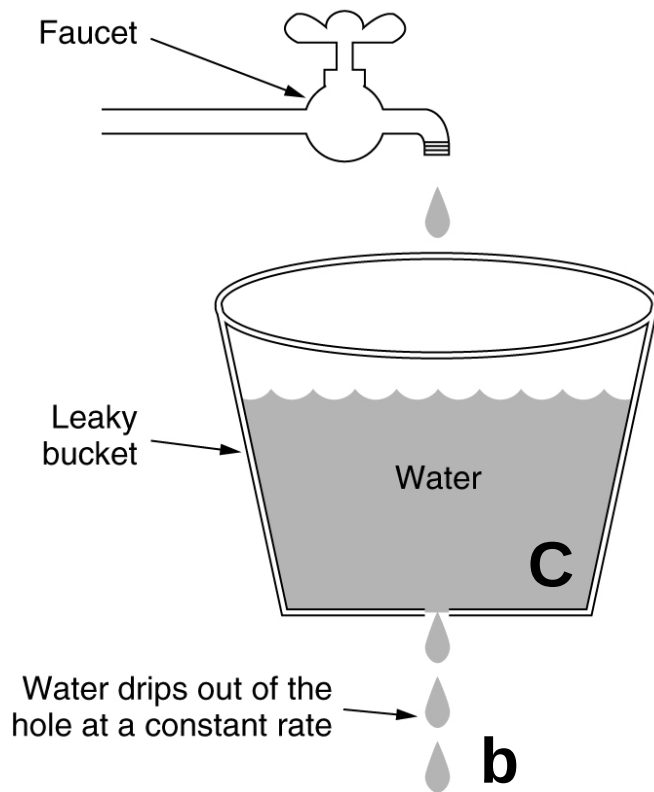
Policing

- La rete deve verificare che l'utente rispetti il SLA
 - Si mette un filtro davanti al traffico in ingresso prodotto dall'utente.
 - Solo i pacchetti che passano il filtro rispettano il SLA e quindi avranno QoS garantita
 - I pacchetti che vengono scartati dal filtro possono subire diversi trattamenti a seconda del provider
 - Venire scartati
 - Subire trattamento best effort
 - Agendo su alcuni parametri del filtro si riproducono i valori del SLA specifico
- Tipi di filtro
 - Leaky bucket
 - Token bucket

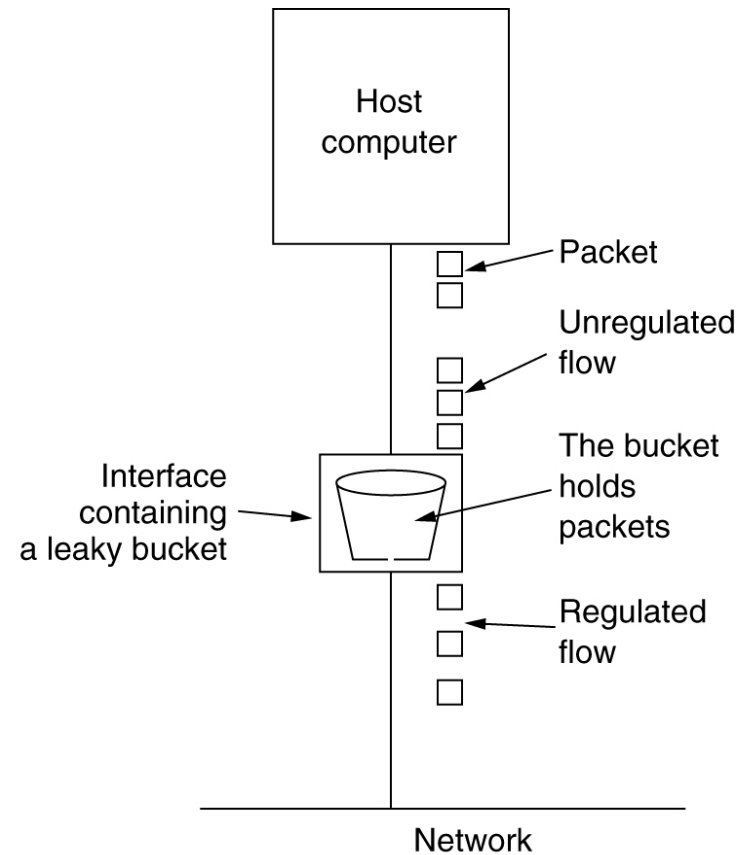
Shaping

- L'utente usa un filtro analogo e gli stessi parametri usati dal gestore per il policing
- L'utente “modella” (to shape) il suo traffico in modo che rispetti il SLA
 - Solo per i pacchetti che passano il filtro (e quindi rispettano il SLA) si è sicuri della QoS e quindi si possono inviare senza dubbi
 - I pacchetti che vengono scartati dal filtro
 - Se **non** sono importanti vengono inviati comunque lasciando la decisione al gestore di rete
 - Se sono importanti vengono ritardati in modo da rientrare nella quota assegnata (possibili problemi per applicazioni multimediali interattive)
 - Viene sempre generato un avviso per l'applicazione che li ha generati

Leaky bucket



(a)



(b)

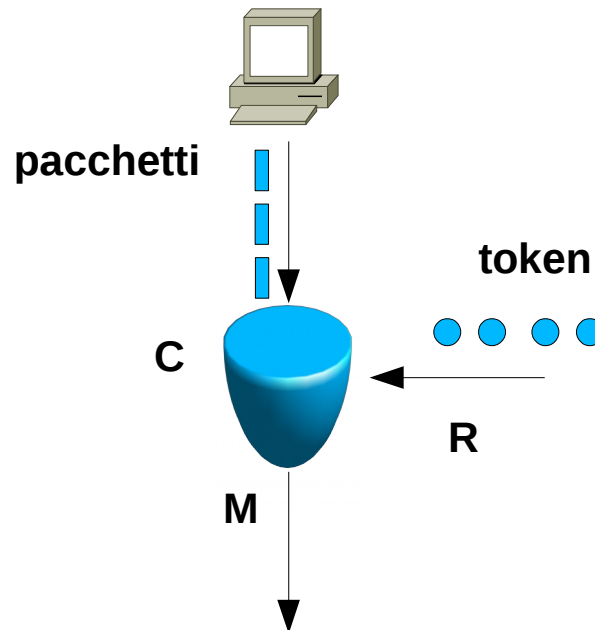
- C = capacità del bucket
- b = bitrate in uscita

Leaky bucket

- Permette di verificare solo che i pacchetti ricevuti abbiano un andamento a bitrate medio b (su una finestra di osservazione C/b)

Token bucket

- Un cesto di capacità C [bit] riceve token di 1 bit ogni $1/R$ secondi
- Un pacchetto in arrivo viene ammesso se
 - ci sono token sufficienti per la sua dimensione nel cesto
 - il bitrate in quel momento è inferiore a M

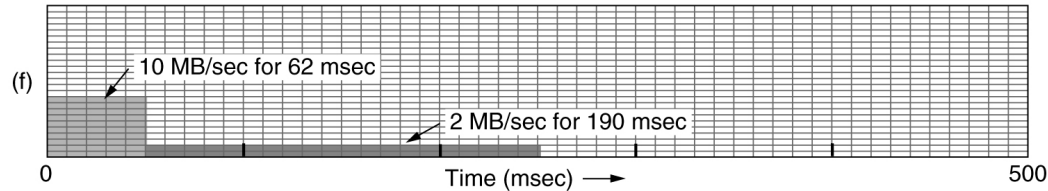
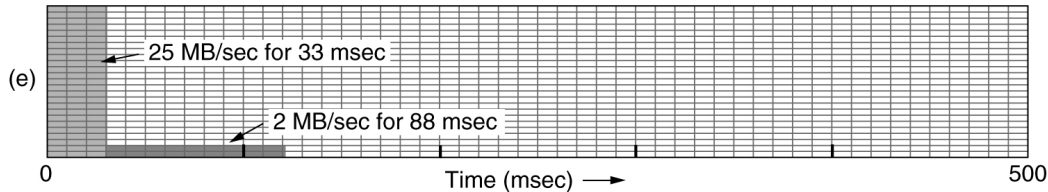
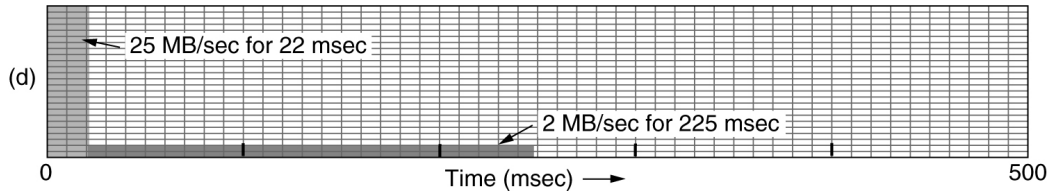
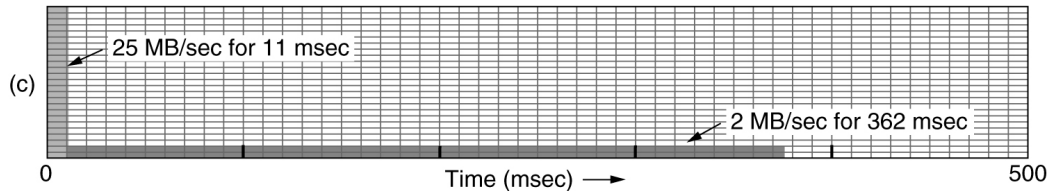
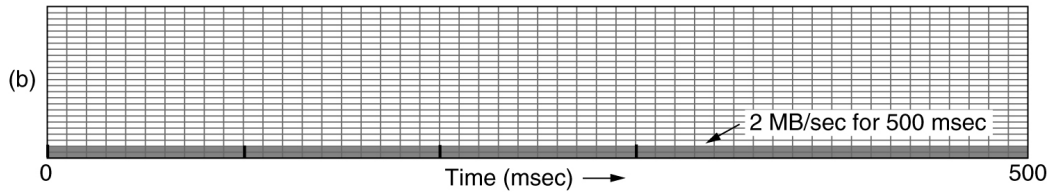
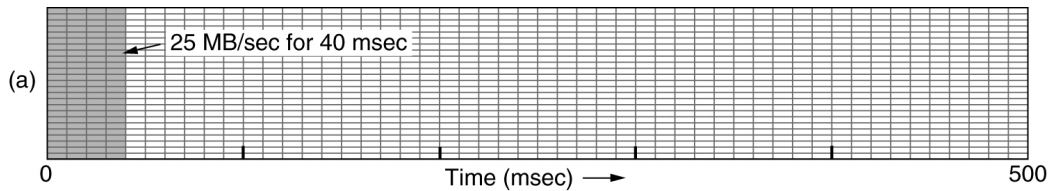


Token bucket (2)

- Il token bucket ammette in uscita un traffico dato da
 - un bitrate medio R
 - un bitrate di picco M
 - la massima lunghezza di un burst al rate di picco pari a

$$\frac{C}{(M - R)}$$

Leaky bucket vs. Token bucket



(a) Ingresso a leaky bucket.

(b) Uscita da leaky bucket.

(c,d,e) Uscita da token bucket con capacità di 250 KB, 500 KB, 750 KB

(f) Uscita da token bucket di 500KB che alimenta un leaky bucket da 10MB/sec.

Resource reservation Protocol (RSVP)

**Un protocollo per la prenotazione di risorse
in Internet**

Requisiti di progetto

- Deve supportare applicazioni unicast, multicast uno-a-molti e molti-a-molti
- Deve usare le risorse in modo efficiente
- Deve supportare ricevitori eterogenei
- Deve seguire principi di progetto dello stack TCP/IP
 - robustezza rispetto a perdite di pacchetti o guasti
 - adattamento ai cambiamenti di topologia
- Deve rappresentare un'integrazione dell'architettura tradizionale non una modifica

RSVP nell'architettura esistente

- Messaggi incaspolati in IP
 - PATH (unicast o multicast)
 - RESV (unicast)
 - TEARDOWN (unicast o multicast)
- Per la propagazione dei messaggi si usano le normali informazioni di routing unicast o multicast
- Ad ogni “hop” interagisce con il Controllo di Ammissione del router e, se esistono le risorse, le prenota altrimenti avverte il richiedente dell'insuccesso

Cosa RSVP non fa

- routing
- controllo di ammissione
- classificazione dei pacchetti
- schedulazione dei pacchetti

RSVP: sommario

- Prenota risorse per ciascun flusso di dati di livello 4
- E' il ricevitore del flusso di dati a decidere se prenotare e quanto prenotare
- Non occorre conferma **end-to-end** di avvenuta prenotazione ma solo di fallimento

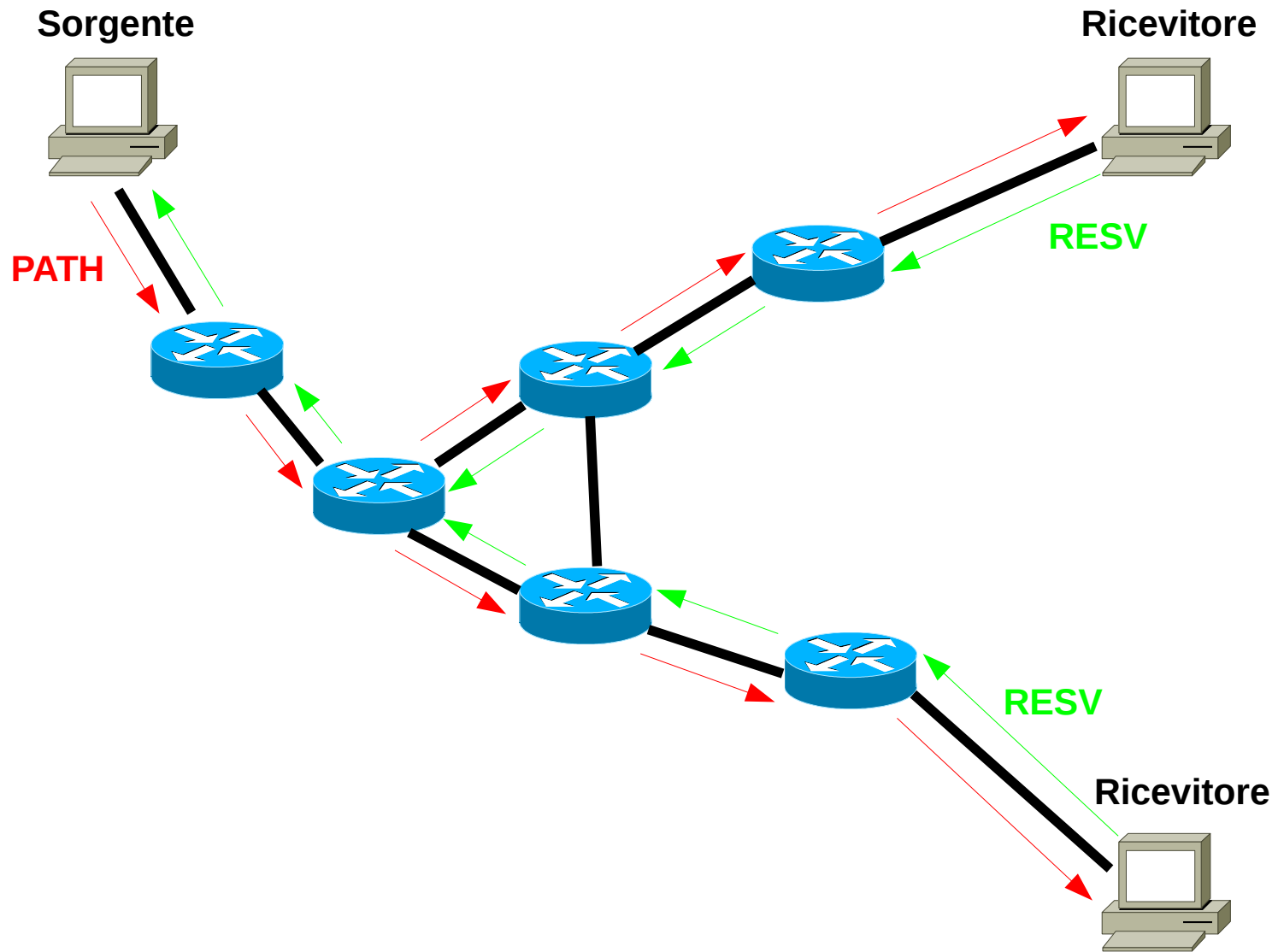
RSVP: operazioni (1)

- Esempio: audioconferenza su gruppo multicast con una sorgente e molteplici ricevitori appartenenti al gruppo
- La sorgente invia periodicamente messaggi PATH al/ai ricevitore/i
- Ciascun ricevitore, in risposta ad un messaggio PATH, invia verso la sorgente un messaggio RESV con cui richiede la prenotazione di risorse.
- I messaggi RESV seguono il percorso inverso rispetto ai messaggi PATH.

RSVP: operazioni (2)

- I messaggi RESV, hop per hop, portano la richiesta di prenotazione di risorse del ricevitore a ciascun router e alla sorgente del messaggio PATH.
 - se un router non ha sufficienti risorse informa il ricevitore
 - se due o piu' messaggi RESV (quindi provenienti da ricevitori diversi) richiedono risorse per la stessa sorgente allora le richieste vengono fuse prima di essere propagate verso la sorgente
- Quando il messaggio RESV arriva alla sorgente questa è sicura che tutte le risorse sono state prenotate con successo
- Alla fine della sessione, sorgente e ricevitori inviano un messaggio di TEARDOWN

Esempio



Cambiamenti di topologia

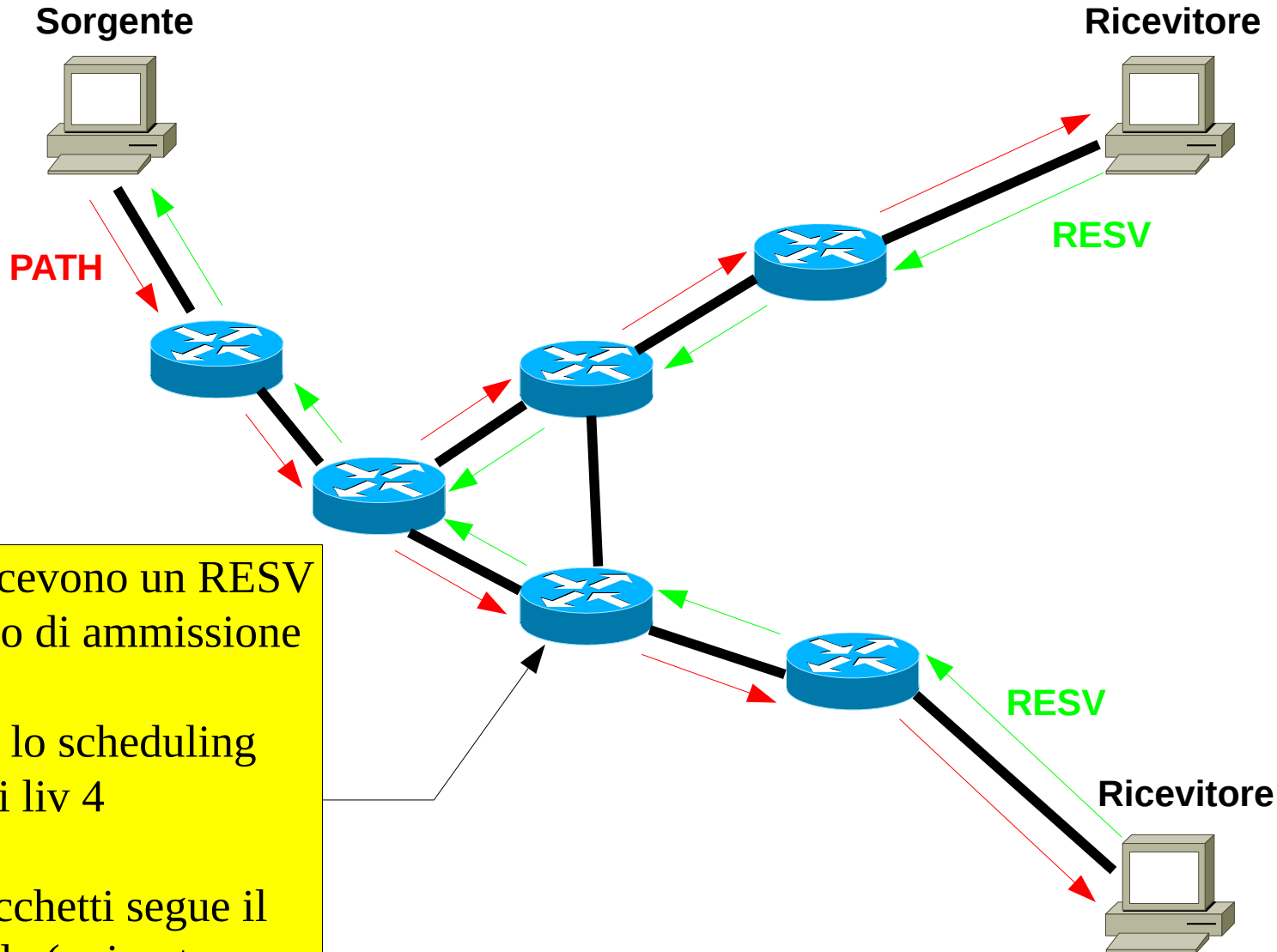
- RSVP è robusto ai cambiamenti di topologia della rete in quanto i messaggi PATH e RESV vengono inviati periodicamente
 - in assenza di cambi di percorso i messaggi periodici rinfrescano semplicemente le prenotazioni
 - quando ci sono dei cambiamenti di topologia i messaggi PATH identificano i nuovi percorsi e i messaggi RESV li seguono a ritroso
 - le prenotazioni non piu' rinfrescate scadono liberando le risorse del router

Modello a Servizi Integrati (IntServ)

Concetti fondamentali

- Applicazioni specifiche richiedono QoS
 - garanzie sui ritardi max
 - garanzie sul throughput minimo
- La QoS viene fornita a flussi di livello 4
 - ogni flusso è identificato da IP sorgente, IP destinazione, porta sorgente, porta destinazione, protocollo (UDP/TCP)
 - ogni flusso informa la rete delle sue richieste (RSVP)
 - la rete accetta o rifiuta in base al tipo di richiesta e alle risorse disponibili
- Supporto QoS per flussi unicast e multicast
- Flussi QoS possono coesistere con flussi best effort
- I router mantengono info per ogni flusso

Esempio

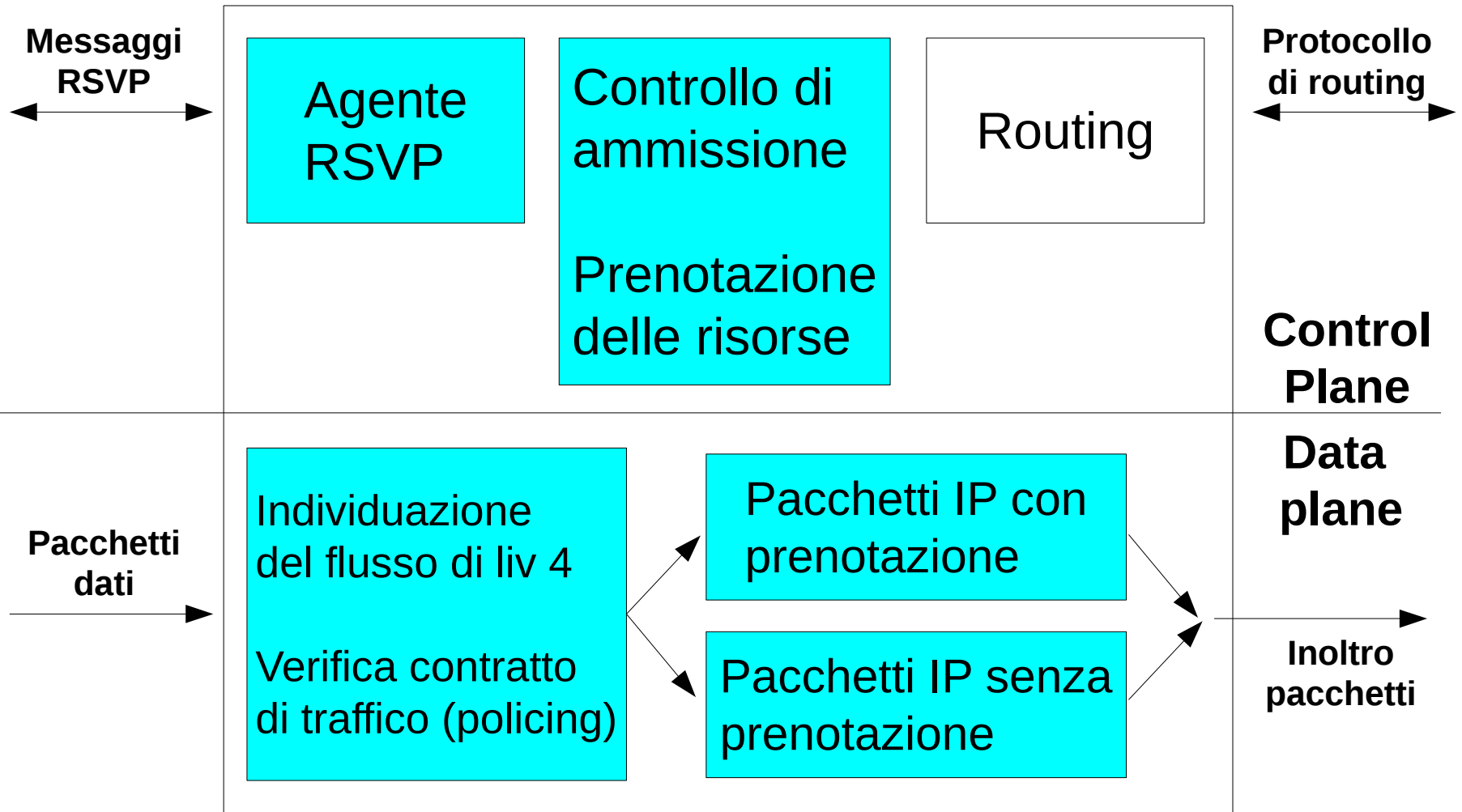


I router quando ricevono un RESV eseguono controllo di ammissione

I router applicano lo scheduling a ciascun flusso di liv 4

Il percorso dei pacchetti segue il routing tradizionale (unicast e multicast)

Schema di router IntServ



Controllo di ammissione

- Messaggio RESV relativo ad un certo flusso di livello 4
 - definizione della QoS richiesta (banda, ritardo)
 - caratterizzazione del traffico che invierà in rete (parametri token bucket)

Classi di servizio IntServ

- Due classi di servizio standardizzate da IETF
 - Guaranteed Service (GS)
 - Controlled Load (CL)
- Riferimenti
 - Shenker, S., Partridge, C., and R. Guerin, "Specification of Guaranteed Quality of Service", RFC 2212, September 1997
 - Wroclawski, J., "Specification of the Controlled-Load Network Element Service", RFC 2211, September 1997

Guaranteed Service

- Garanzie fornite a pacchetti conformi
 - conformita' definita tramite Token Bucket
 - Upper bound su ritardo di rete end-to-end
 - Nessuna garanzia sul ritardo medio
 - Nessuna garanzia sul jitter del ritardo
 - Nessuna perdita per overflow del buffer del router
 - lo spazio nei router viene prenotato
- I pacchetti non conformi sono trattati come traffico best effort

Controlled Load

- Principio
 - fornire un servizio come in una rete best effort con basso carico e senza congestioni
- Garanzie
 - Nessuna garanzia sulle perdite
 - ...ma le perdite devono essere basse come in GS
 - Nessuna garanzia su ritardi e jitter
 - ...ma il ritardo di accodamento deve essere basso

Bibliografia

- R. Hunt, A review of quality of service mechanisms in IP-based networks - integrated and differentiated services, multi-layer switching, MPLS and traffic engineering, Elsevier CompComm Mag., 2002
- P. P. White, RSVP and Integrated Services in the Internet: a Tutorial, IEEE Communication Magazine, Maggio 1997
- <http://ieeexplore.ieee.org> (down. da dentro la facoltà)

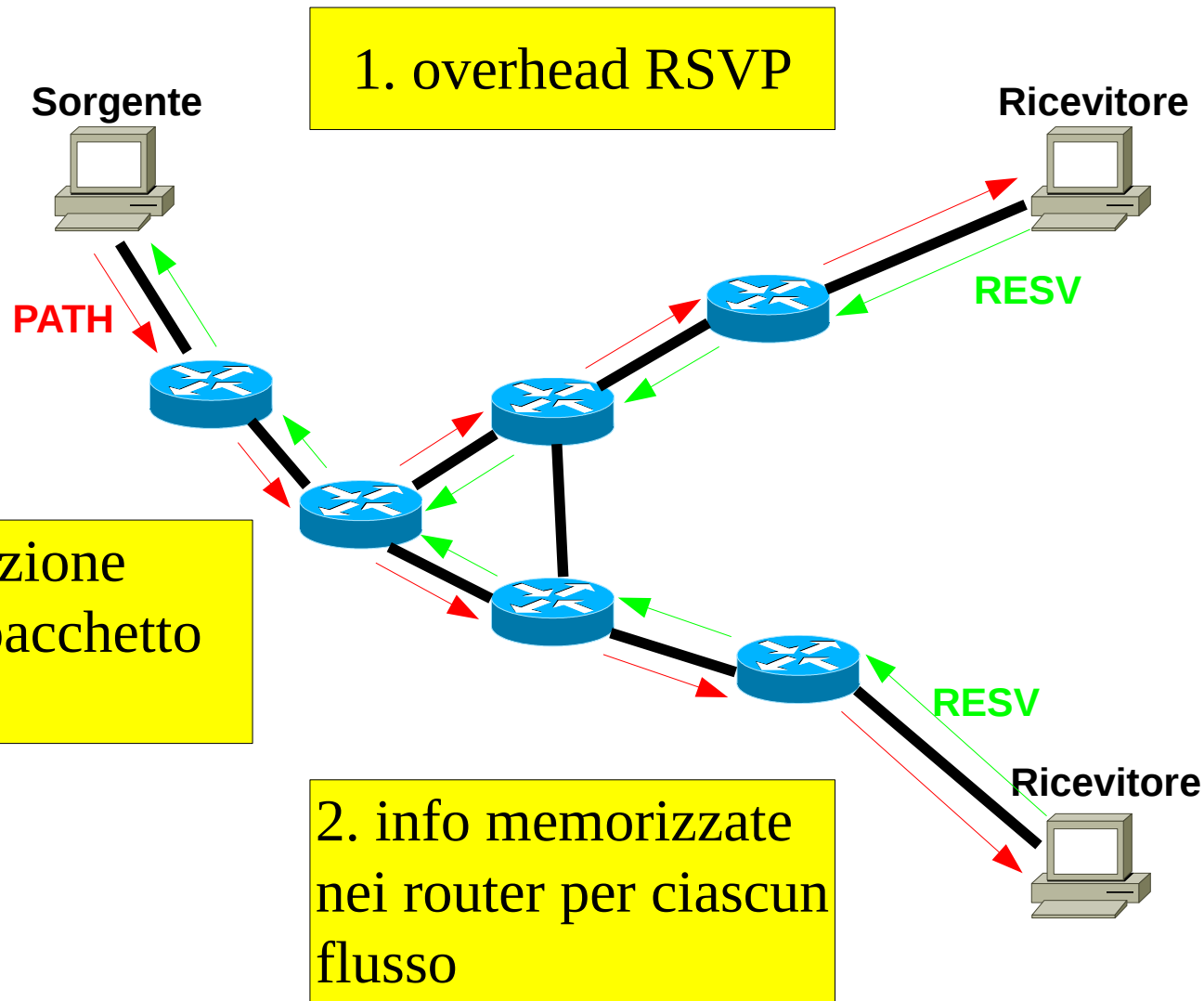
Bibliografia

- <http://www.ietf.org>
 - RFC 1633: Integrated Services in the Internet Architecture: an Overview, 1994
 - RFC 2205: Resource ReSerVation Protocol (RSVP), 1997
 - RFC 2210: The Use of RSVP with IETF Integrated Services, 1997
 - RFC 2750, RFC 3936, RFC 4495, RFC 5946: aggiornamenti a RSVP

Commento

- Vantaggi
 - garanzie fornite a ciascun flusso di livello 4
- Svantaggi
 - complessità in tutti i router della rete
 - ogni router in ogni parte della rete deve tenere info per ogni flusso di livello 4 (scalabilità)
 - gestione del protocollo RSVP
 - identificazione dei flussi di livello 4 (spacchettamento)
 - policing/queueing/scheduling dei flussi di livello 4
 - definizione delle caratteristiche del traffico in uscita da ogni applicazione
 - certe applicazioni potrebbero non saperlo

Problemi di scalabilita' di IntServ



Problemi di scalabilità di IntServ (2)

- Overhead RSVP
 - elaborazione di una coppia PATH/RESV per ogni flusso per ogni periodo di refresh
- Info memorizzate per ciascun flusso
 - identificazione dei flussi (IP sorg, IP dest, porta sorg, porta dest, protocollo)
 - identificazione dell'hop precedente (per inoltrare RESV)
 - stato della prenotazione
 - risorse prenotate
- Elaborazione per ogni pacchetto in arrivo
 - associazione ad un flusso
 - verifica della prenotazione
 - verifica del contratto

Modello a Servizi Differenziati (DiffServ)

Limiti del modello IntServ

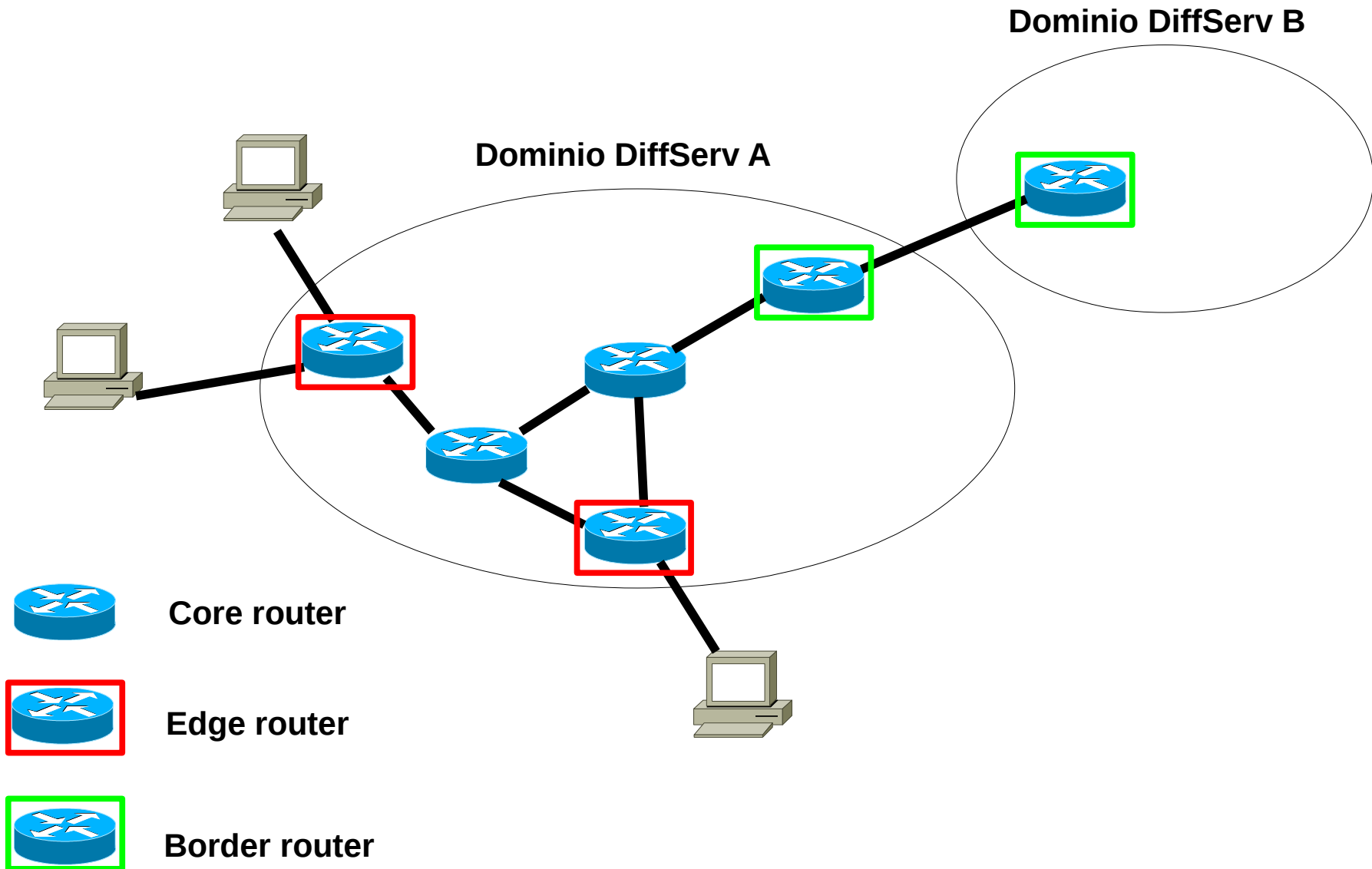
- Prenotazione risorse per singole sessioni
 - simile ad un modello a commutazione di circuito (contro la filosofia di Internet)
 - su Internet le sessioni sono spesso molto brevi → eccessivo overhead
- Prenotazione lungo tutto il percorso del flusso dati
 - Internet e' una connessione di reti diverse sotto amministrazioni diverse
- Complessità nel centro della rete
 - Internet ha sempre confinato la complessità ai bordi della rete mantenendo il “core” semplice ed efficiente

Un approccio semplificato

- Permettere agli utenti di specificare SLA per alcune classi di traffico
 - Best effort, better effort, real-time
 - diverse garanzie su banda e ritardi per ogni tipo di classe

Error tolerant	Conversational voice and video	Voice messaging	Streaming audio and video	Fax
Error intolerant	Telnet, interactive games	E-commerce, WWW browsing,	FTP, still image, paging	E-mail arrival notification
	Conversational (delay <<1 sec)	Interactive (delay approx 1 sec)	Streaming (delay <10 sec)	Background (delay >10 sec)

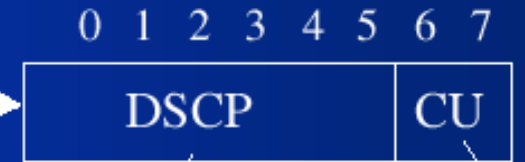
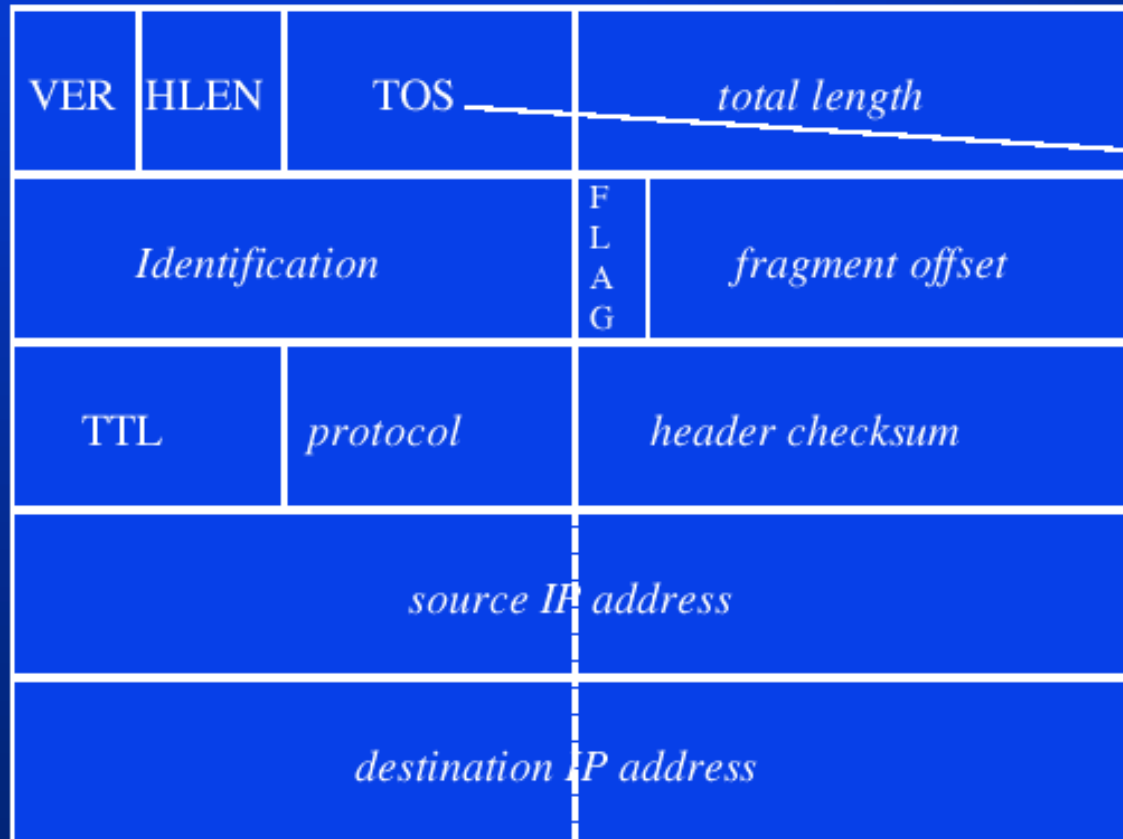
Architettura



Architettura (2)

- Dominio DiffServ: rete IP con amministrazione omogenea della QoS da fornire alle varie classi
- Edge router: tra host e rete DiffServ
- Border router: tra domini DiffServ
- Il tipo di classe a cui appartiene il pacchetto è indicato in un campo dell'header IP
 - elaborazione a livello 3 e non 4 come in IntServ !
- La marcatura dei pacchetti può essere fatta
 - negli host
 - negli edge router
 - nei border router

Marcatura dei pacchetti IP



Riservato ad uso
Futuro (ECN)

DiffServ Code Point

Usato per specificare come la
Rete deve trattare il pacchetto
Default DSCP 000000
Significa "best-effort"

Ruolo dei router

- Gli Edge router marciano il traffico proveniente dall'host in base al SLA oppure fanno il policing dei flussi già marcati
 - possono anche fare traffic shaping
- I Border router hanno il compito di mappare le classi di un dominio DiffServ in quelle di un altro dominio
 - l'amministratore potrebbe aver usato DSCP diversi per le stesse classi oppure accorpato più classi
- I Core router gestiscono ciascun pacchetto dati in base alla classe di appartenenza
 - code diverse per classi diverse (es. corsia preferenziale, cassa veloce al supermercato)

Vantaggi

- La complessità computazionale è confinata il più possibile ai bordi della rete
 - (re)marking, policing, (re)shaping
- La differenziazione di trattamento nei core router è più leggera
 - livello 3 invece che 4
 - poche info di stato (solo parametri QoS delle classi)
 - la complessità dipende dal numero di classi e non dal numero di flussi di livello 4
 - il numero di classi solitamente non è molto alto
- La QoS può essere anche assicurata su parte dell'intero tragitto (diversamente da IntServ)

Per-hop behavior (PHB)

- Comportamento che i core router applicano a ciascun pacchetto in base alla classe di appartenenza
- PHB standard
 - best effort
 - expedited forwarding (RFC 3246)
 - bassa percentuale di perdita
 - basso delay
 - basso jitter
 - assured forwarding (RFC 2597)
 - bassa percentuale di perdita
 - 4 sotto-classi servite indipendentemente

Expedited forwarding (EF)

- Simile alla posta prioritaria
- Adatta per applicazioni multimediali interattive
- In ogni nodo, l'amministratore deve configurare parte della banda per il traffico EF
 - Il traffico EF deve usufruire della banda indipendentemente dall'intensità di altro traffico attraverso il nodo
 - la banda usata dai pacchetti EF dovrebbe essere, in media, pari almeno alla banda garantita durante qualsiasi intervallo di tempo uguale o più lungo del tempo per inviare un pacchetto di dimensione massima al rate pari alla banda

Multiprotocol Label Switching (MPLS)

Sommario

Introduzione

- Forwarding equivalence classes

Multi-Protocol Label Switching

- principi

- vantaggi

- gestione delle etichette

Utilizzi

- Traffic engineering per Virtual Private Network (VPN)

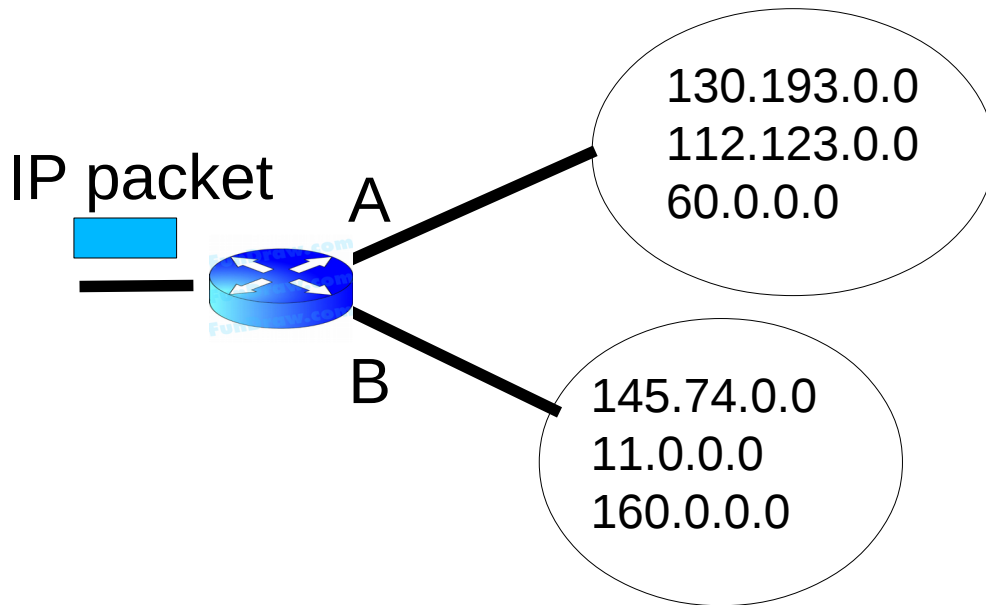
- Load Balancing in Server Farm

- Voice over MPLS

Bibliografia

Introduzione

Nel protocollo IP ogni router che riceve un pacchetto decide su quale interfaccia farlo uscire in base indirizzo IP destinazione
tabella di routing (statica o compilata attraverso protocollo di routing)

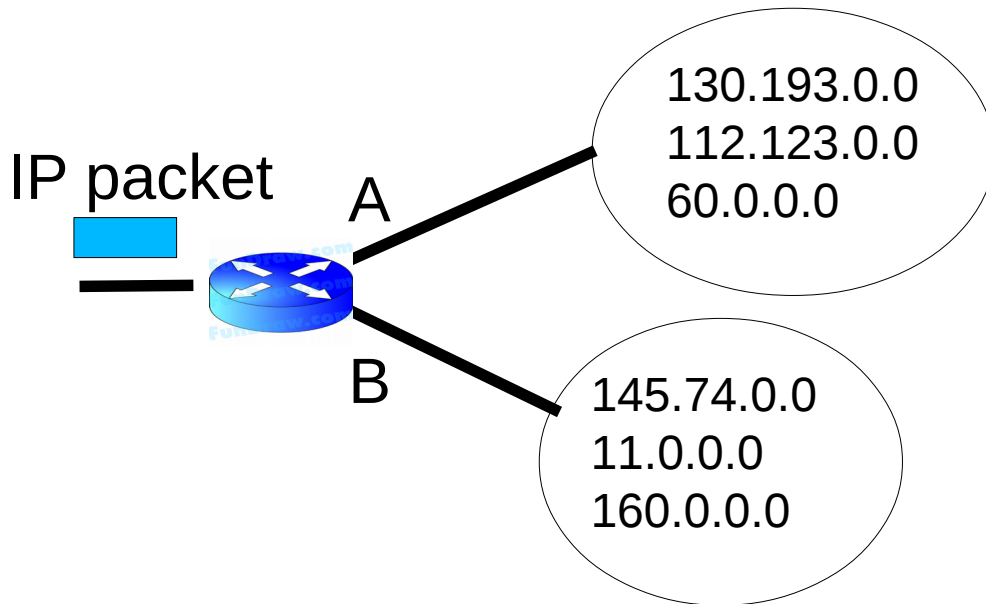


Routing table

130.193.0.0		A
112.123.0.0		A
60.0.0.0		A
145.74.0.0		B
11.0.0.0		B
160.0.0.0		B

Forwarding Equivalence Classes (FEC)

Tutti i pacchetti IP che escono dalla stessa interfaccia appartengono alla stessa Forwarding Equivalence Class



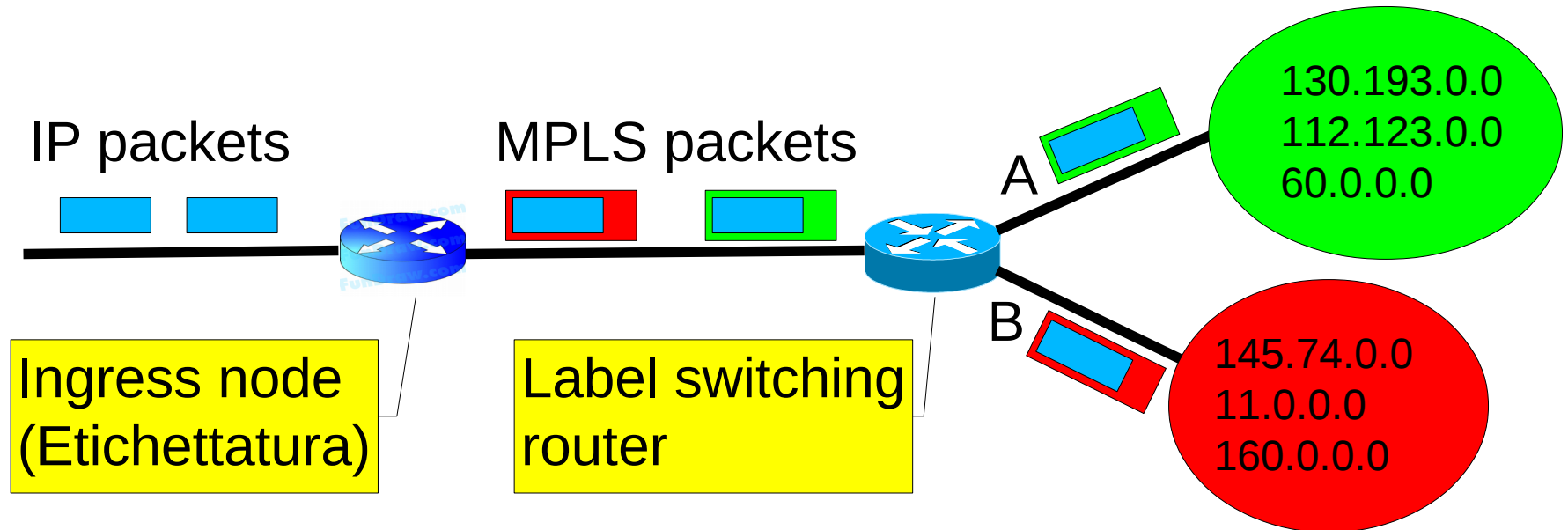
Routing table

130.193.0.0		A	} FEC_0
112.123.0.0		A	
60.0.0.0		A	
145.74.0.0		B	} FEC_1
11.0.0.0		B	
160.0.0.0		B	

Multi-Protocol Label Switching

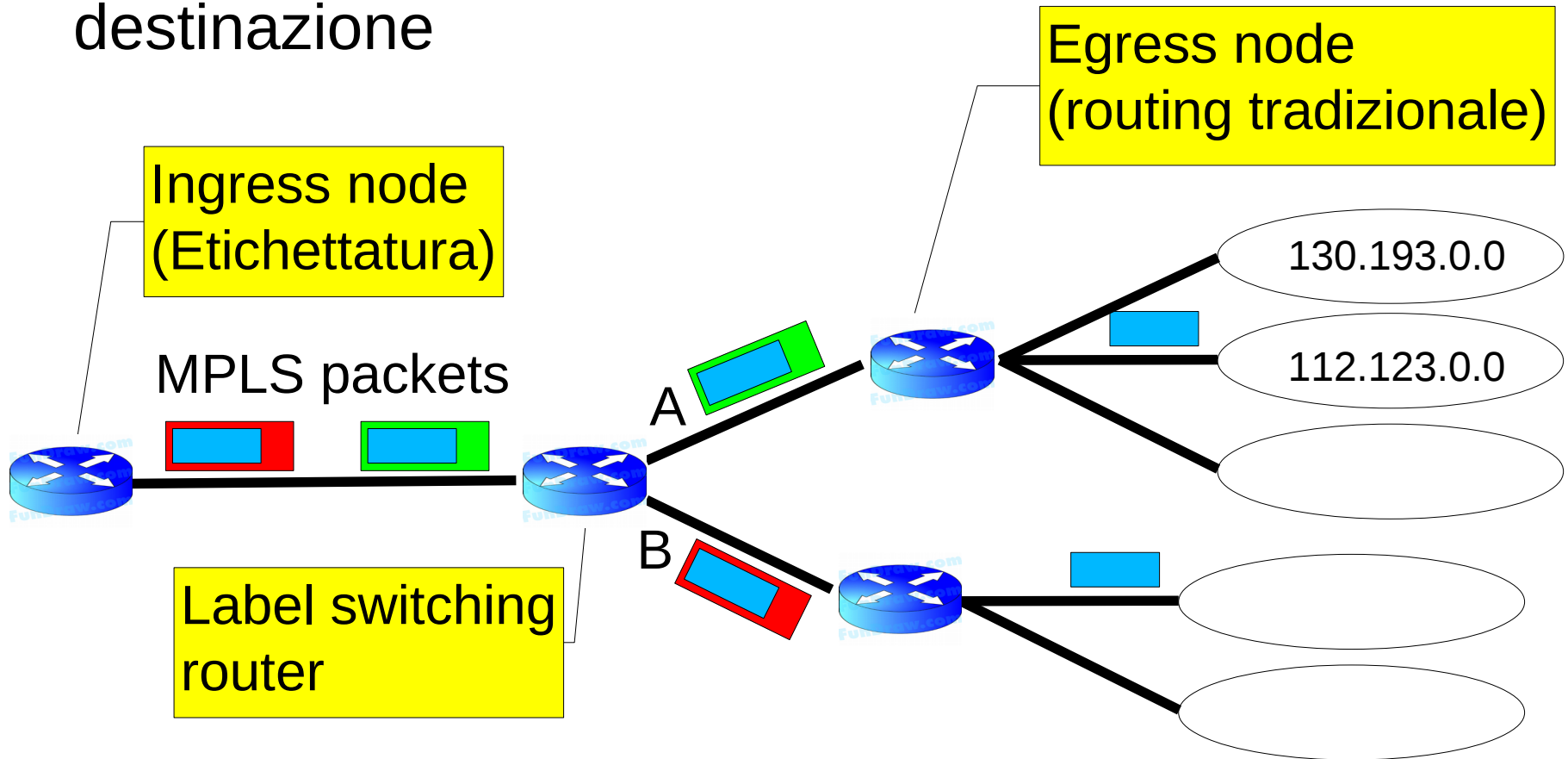
Il router che funge da *Ingress node* appone la *label* in base ad una certa politica (ad es. IP destinazione)

Il *label switching router* esegue una semplice commutazione in base all'etichetta (switch)



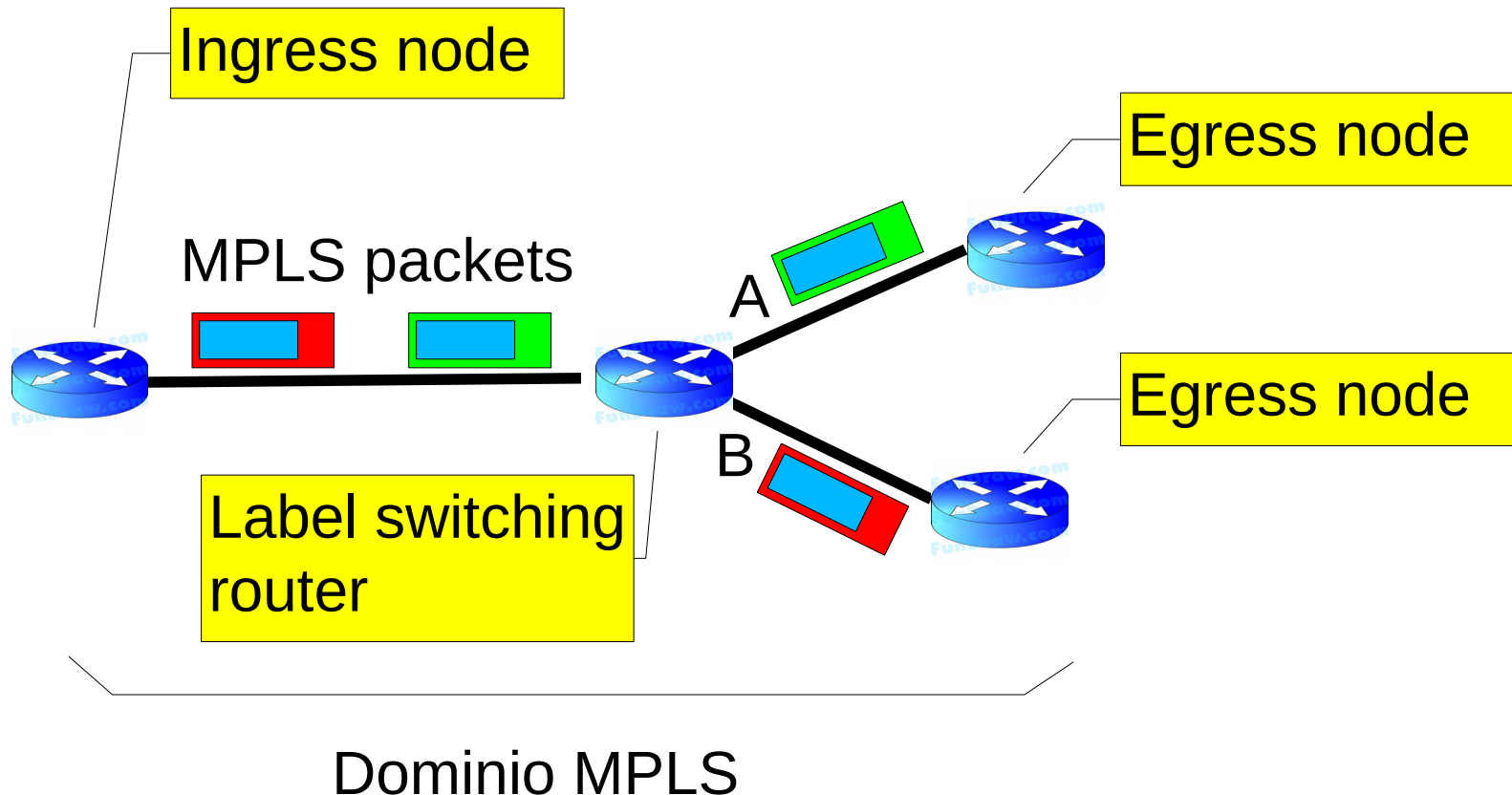
Multi-Protocol Label Switching (2)

Il router che funge da *Egress node* elimina la *label* ed effettua il forwarding tradizionale in base all'IP destinazione



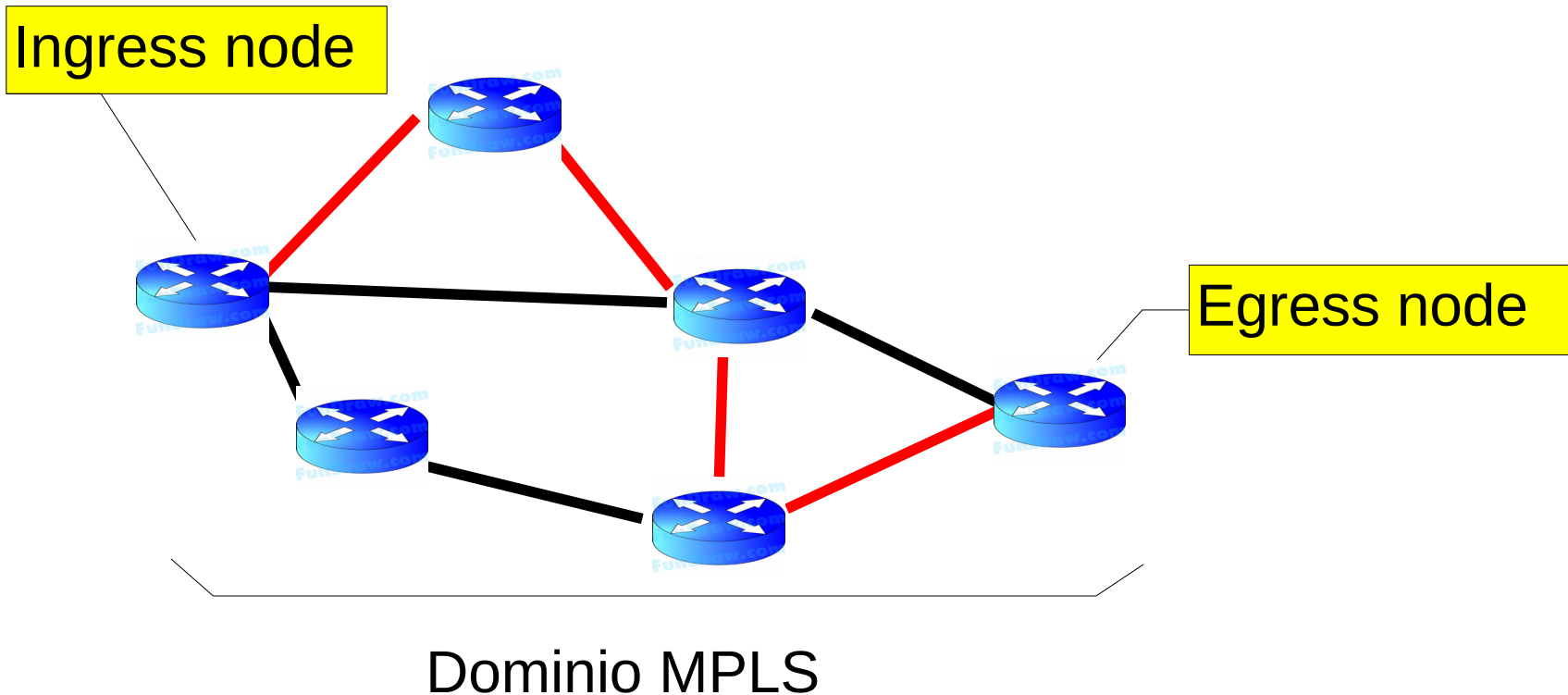
Dominio MPLS

Il router che funge da *Egress node* elimina la *label* ed effettua il forwarding tradizionale in base all'IP destinazione



Dominio MPLS (2)

Usando il label switching si puo' far fare ad un insieme di pacchetti (determinato all'ingresso) sempre una certa strada (magari comoda per assicurare una QoS)



Vantaggi

I label switching router operano in maniera veloce senza guardare dentro i pacchetti IP (come gli switch di livello 2)

L'etichetta serve per

- decidere l'interfaccia di uscita

- decidere che priorit  assegnare al pacchetto (Qos)

Si puo' forzare un certo insieme di pacchetti a seguire sempre un certo percorso senza ricorrere al source routing

Vantaggi (2)

Gli Ingress node possono assegnare le etichette in base a politiche piu' sofisticate del semplice IP destinazione

- interfaccia di arrivo del pacchetto

- tipo di applicazione

- QoS che si vuole assegnare al flusso

Gli Ingress node possono diventare molto sofisticati e complicati ma i router interni rimangono sempre semplici switch

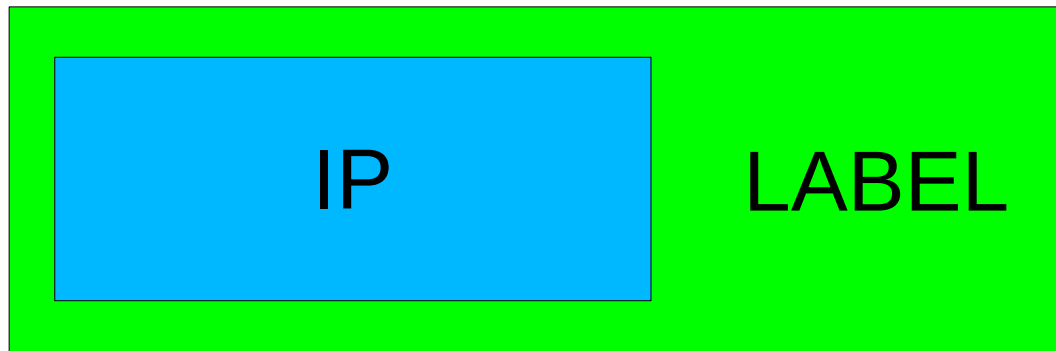
Label

L'etichetta e' una sequenza di bit
corta

di lunghezza fissa in tutto il dominio MPLS

L'etichetta e' contenuta in un pacchetto che contiene
il pacchetto IP come payload

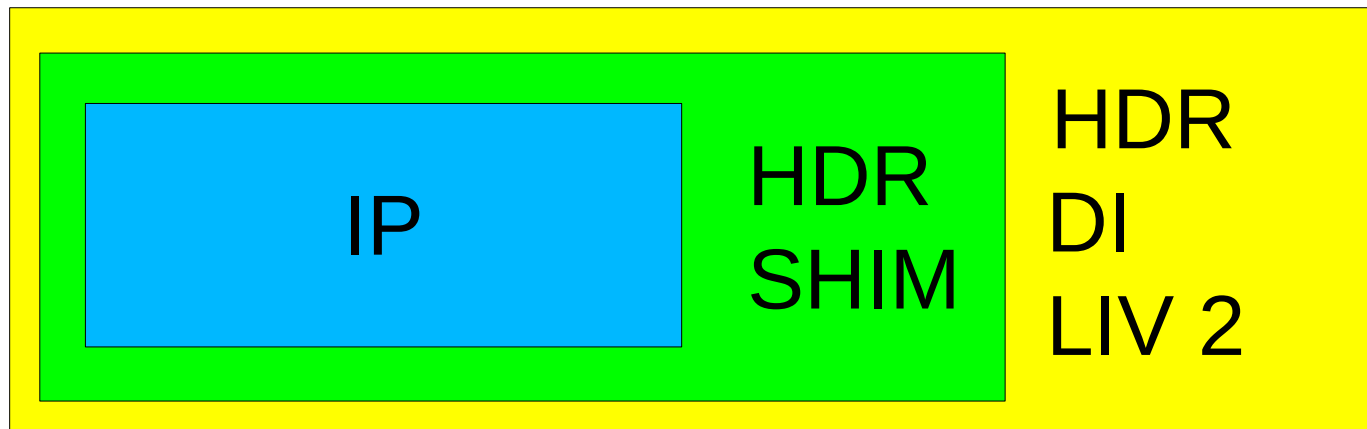
si puo' considerare una specie di frame di livello 2



Label (2)

In RFC 3032 e' stato definito un pacchetto "shim" che si interpone tra il livello 2 vero e il livello IP

In realta' dentro il pacchetto shim puo' stare un qualsiasi tipo di pacchetto di livello 3
da qui il nome "Multi-Protocol"



Label (3)

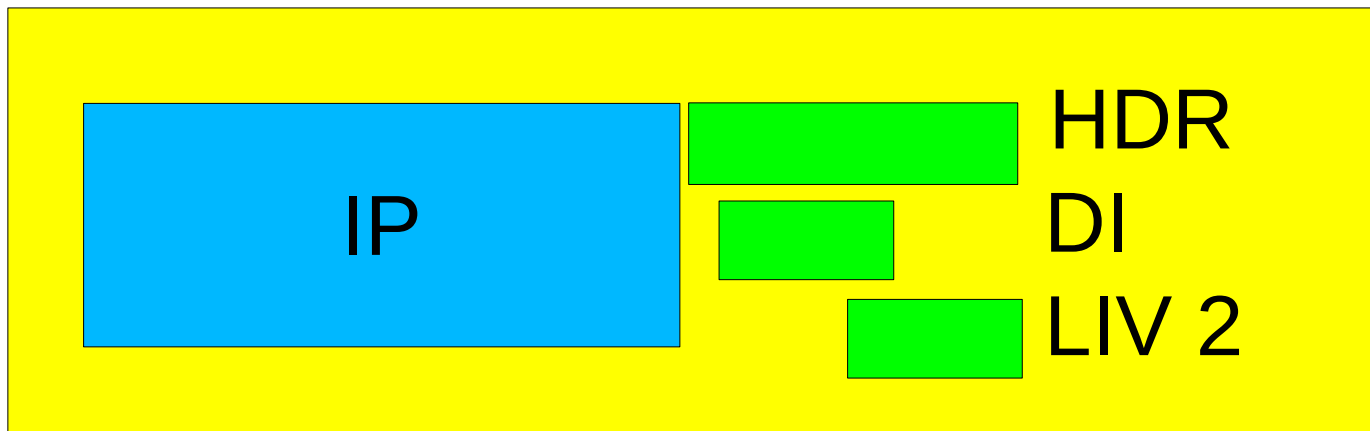
E' prevista una modalita' senza il pacchetto shim

La label viene ricavata da campi del frame di liv. 2

identificatori di path e circuito di ATM

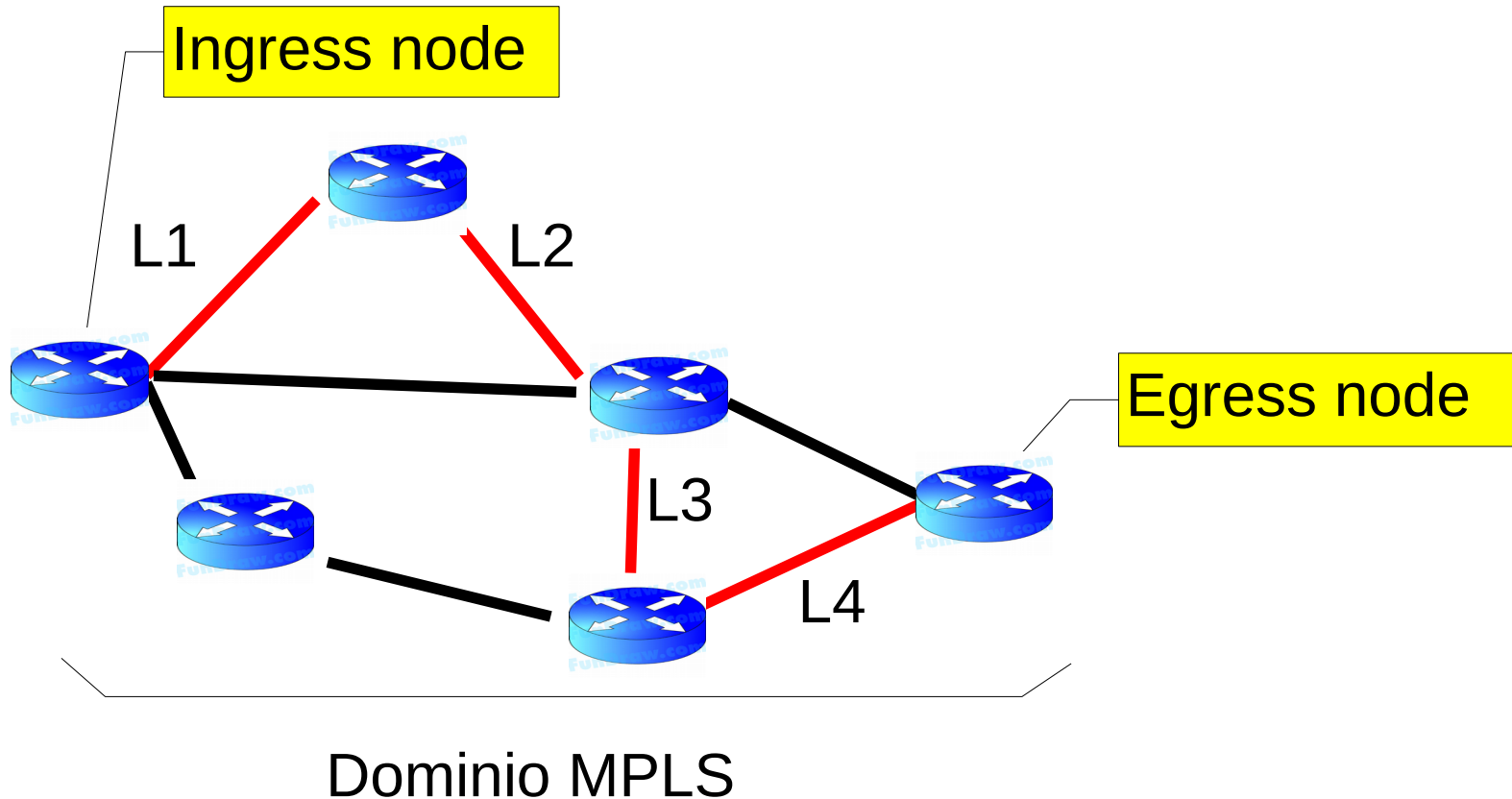
identificatori di circuito di Frame Relay

Utile per mappare direttamente circuiti virtuali ATM e Frame Relay in flussi MPLS



Label Swapping

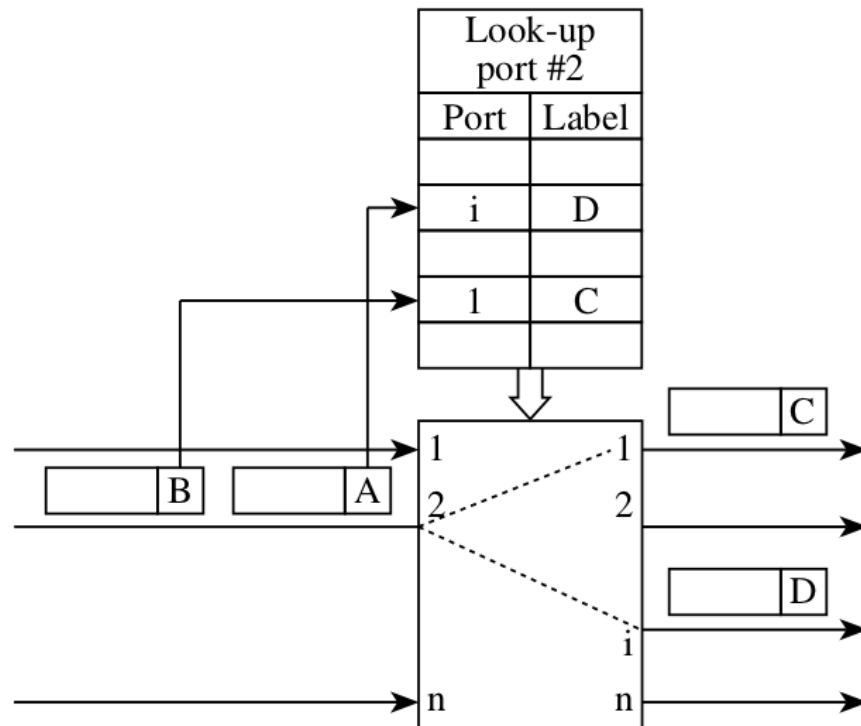
Dato un certo flusso MPLS non e' necessario che il valore della sua etichetta sia costante su tutto il tragitto; basta che lo sia su ogni tratta.



Label Swapping (2)

L'etichetta puo' venire sostituita ad ogni nodo

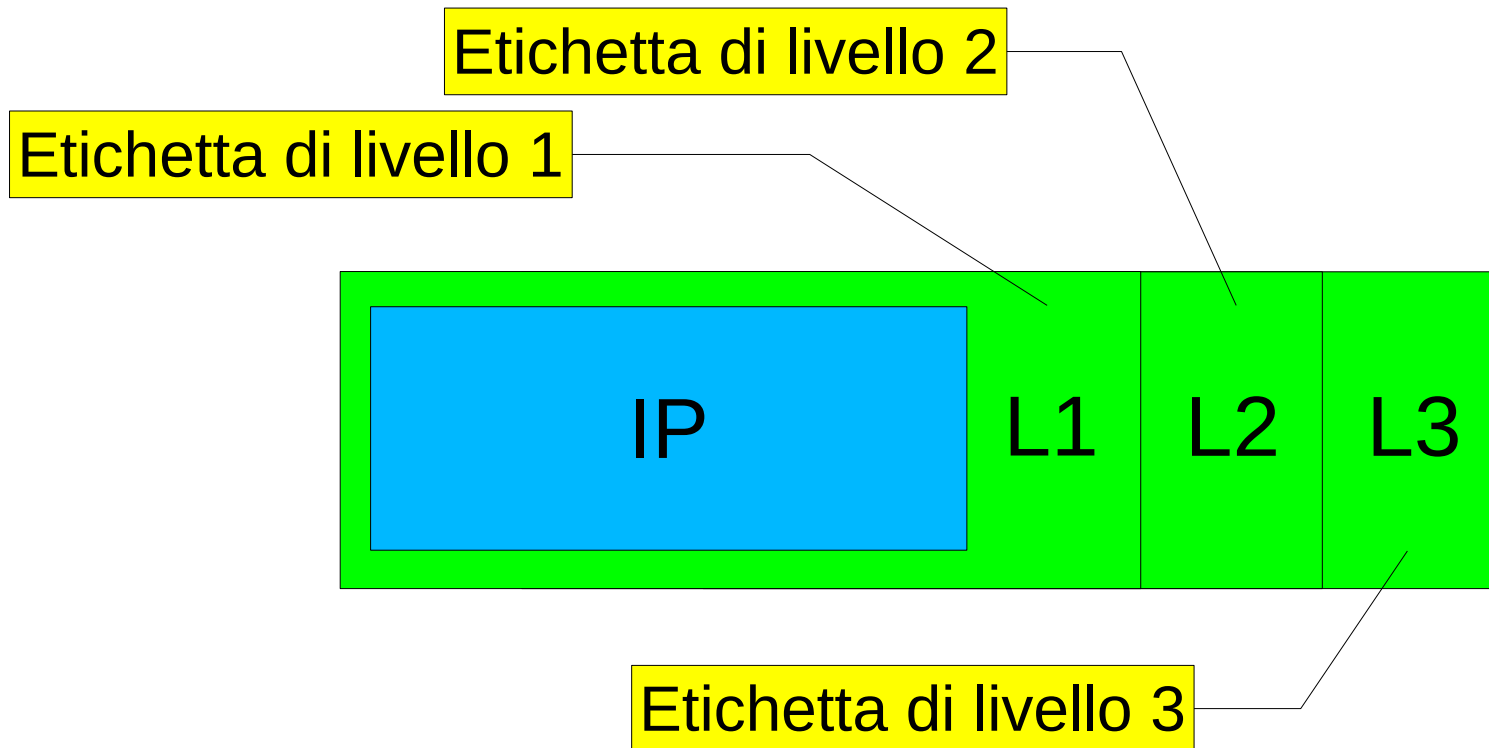
All'arrivo del pacchetto nel nodo il valore dell'etichetta e' usato per accedere ad una tabella che contiene l'interfaccia di uscita e la nuova etichetta



Stack di etichette

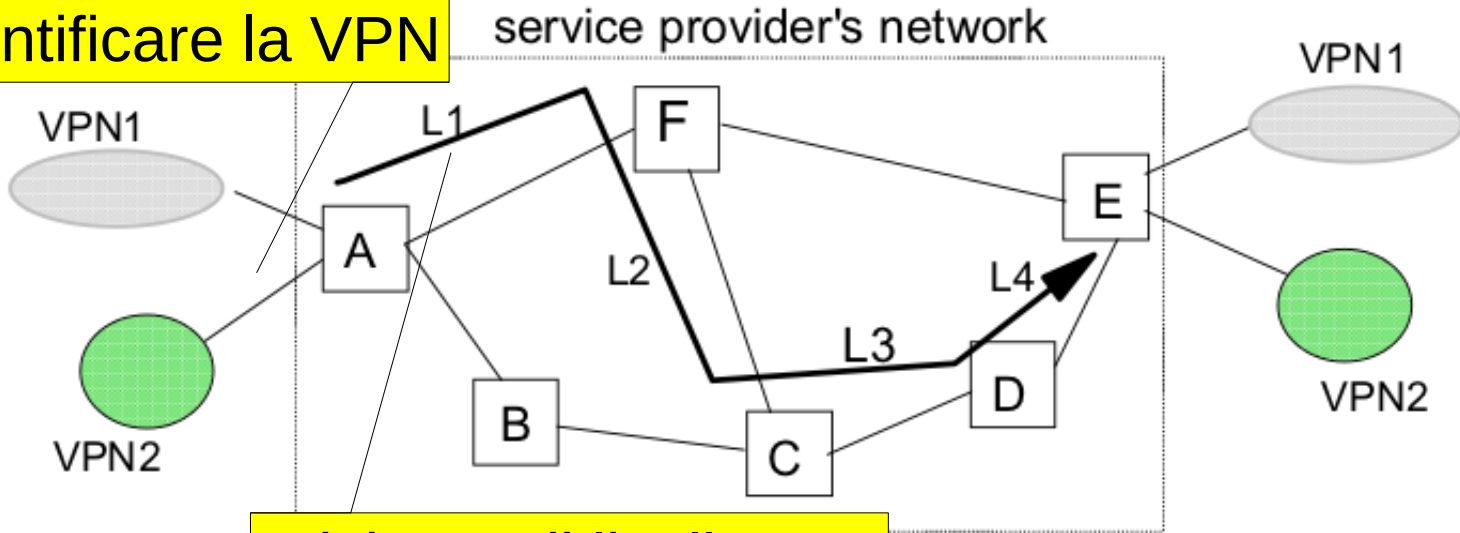
Si possono creare pile di etichette per definire flussi MPLS annidati

Le etichette vengono aggiunte/rimosse in ordine LIFO

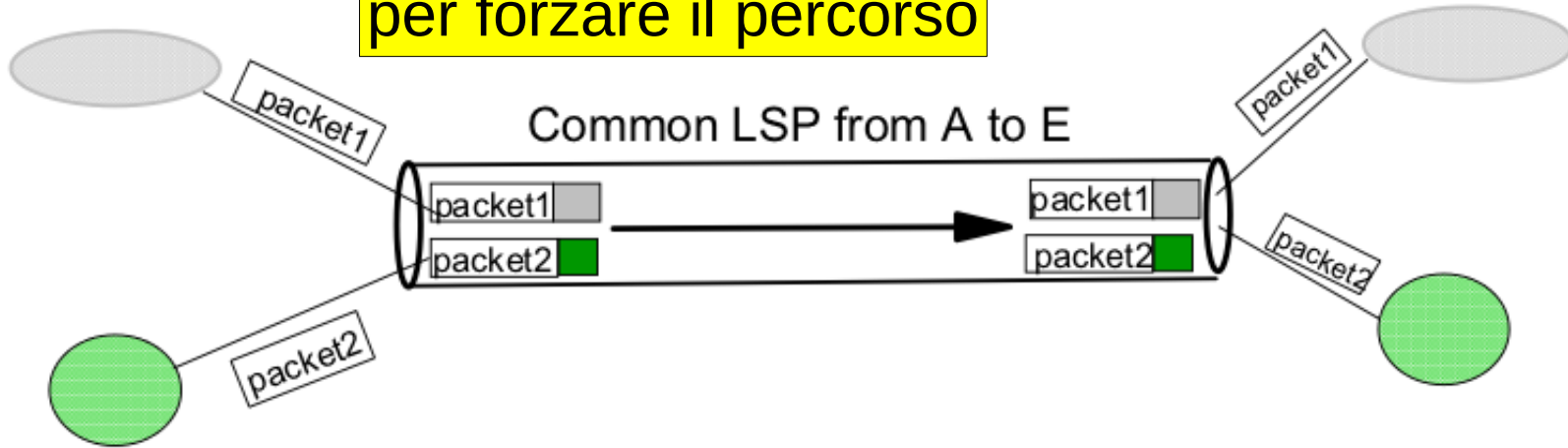


Stack di etichette: esempio

Etichetta di livello 1
per identificare la VPN



Etichetta di livello 2
per forzare il percorso



Assegnazione delle etichette

Statica

effettuata dall'amministratore del dominio MPLS

Dinamica

i label switch router si scambiano le informazioni tramite un protocollo

Label Distribution Protocol

Il nodo downstream comanda l'assegnazione dell'etichetta al nodo upstream



Utilizzo di MPLS

Creazione di percorsi fissi a QoS garantita

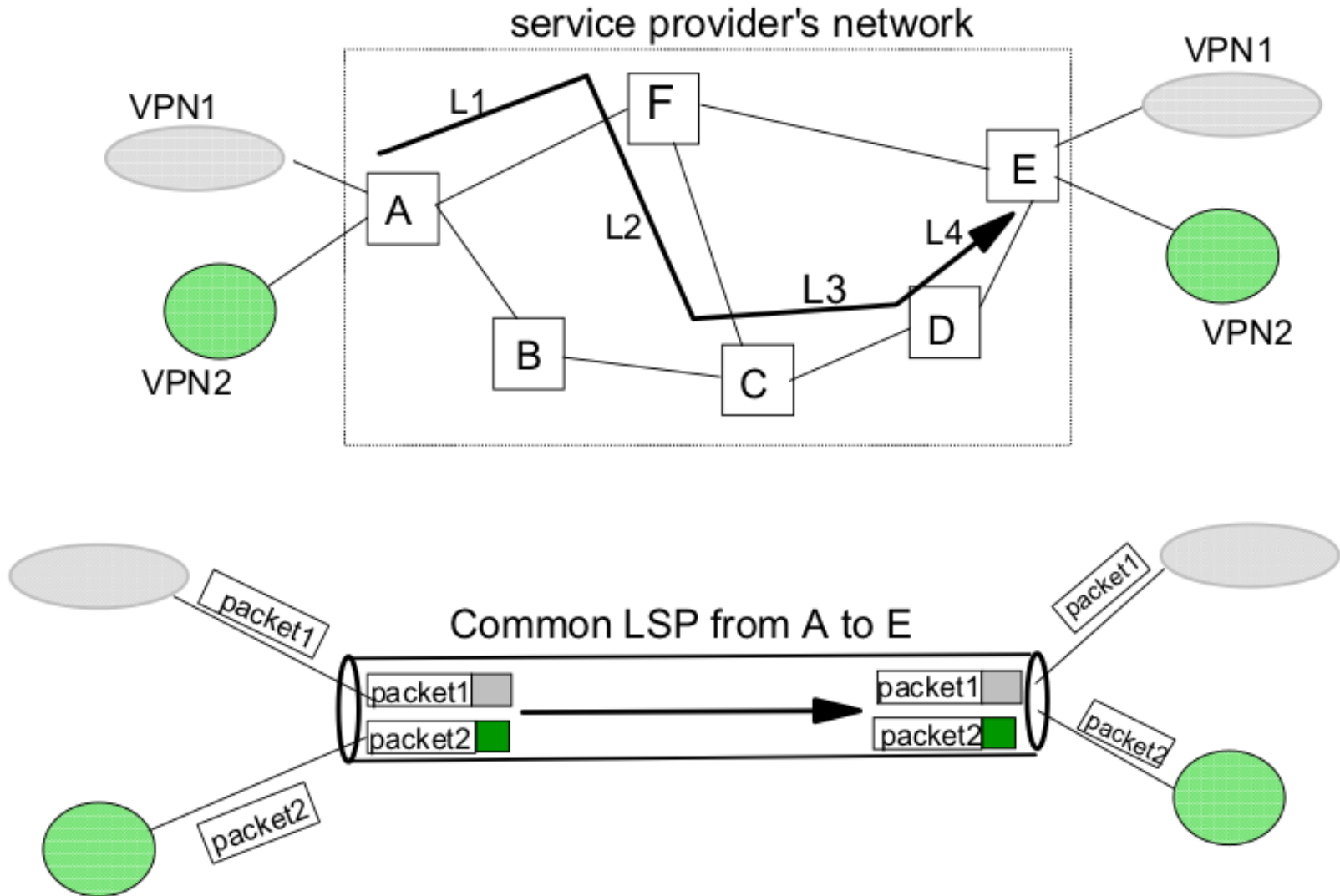
Identificatori per Virtual Private Network (VPN)

routing privato e routing pubblico non interferiscono

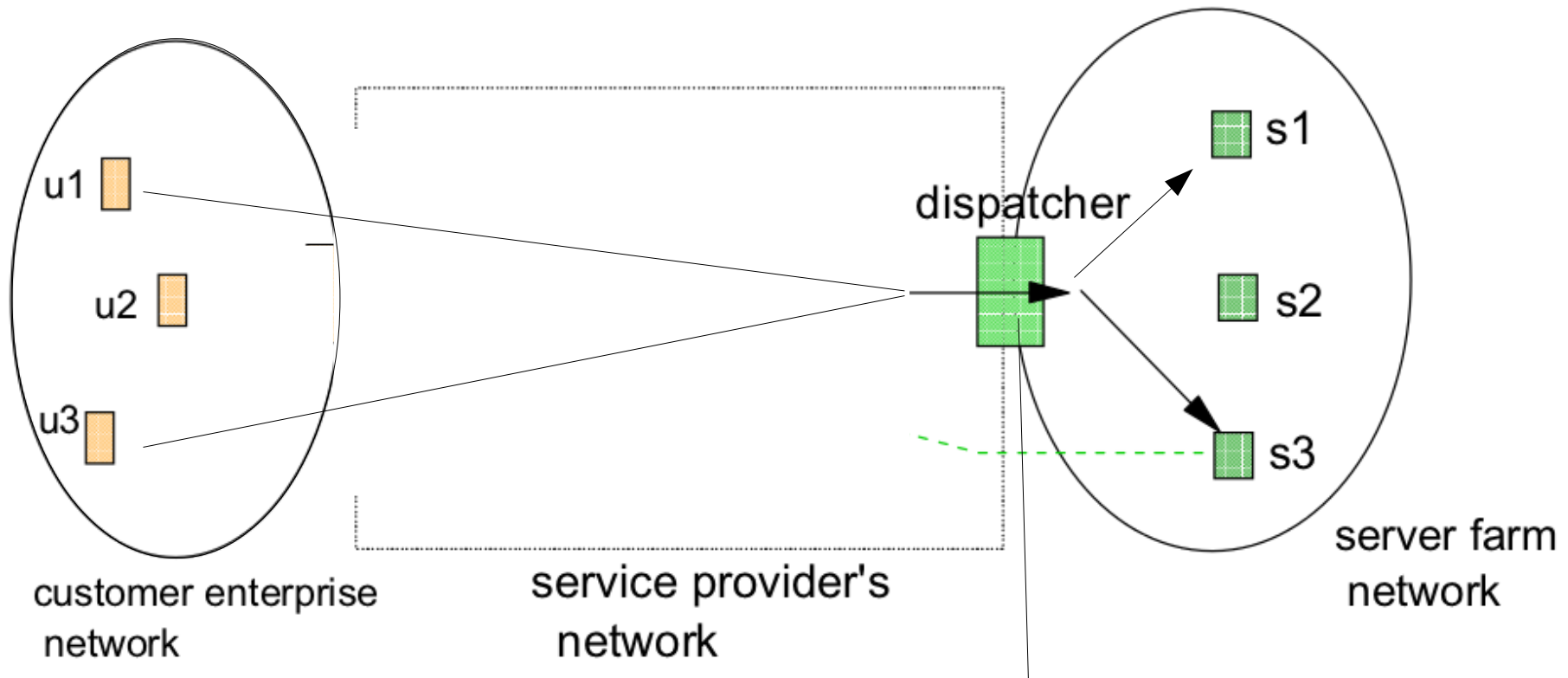
Load balancing di server farm

Trasmissione voce (Voice over MPLS - VoMPLS)

Virtual Private Network

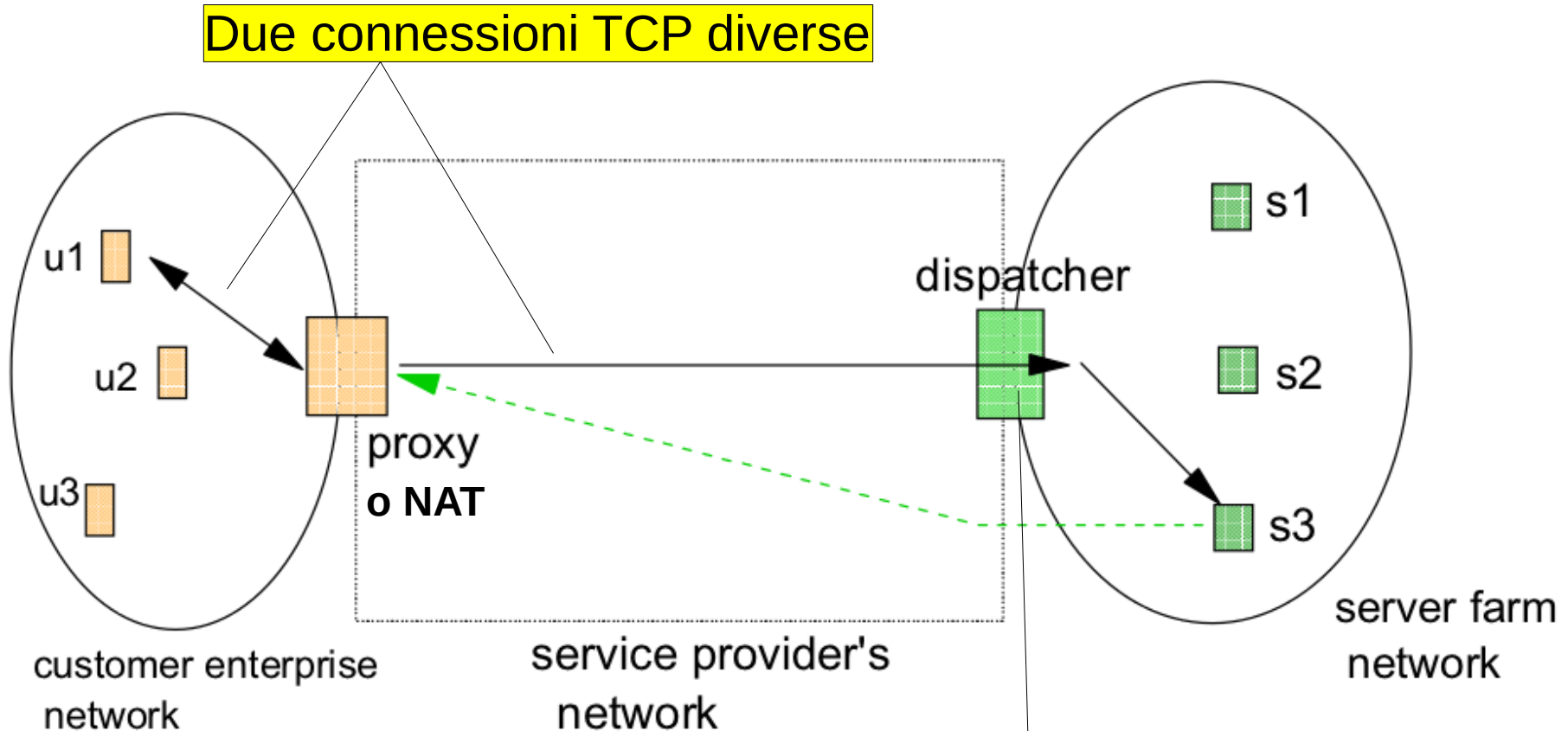


Server Farm: scenario senza proxy



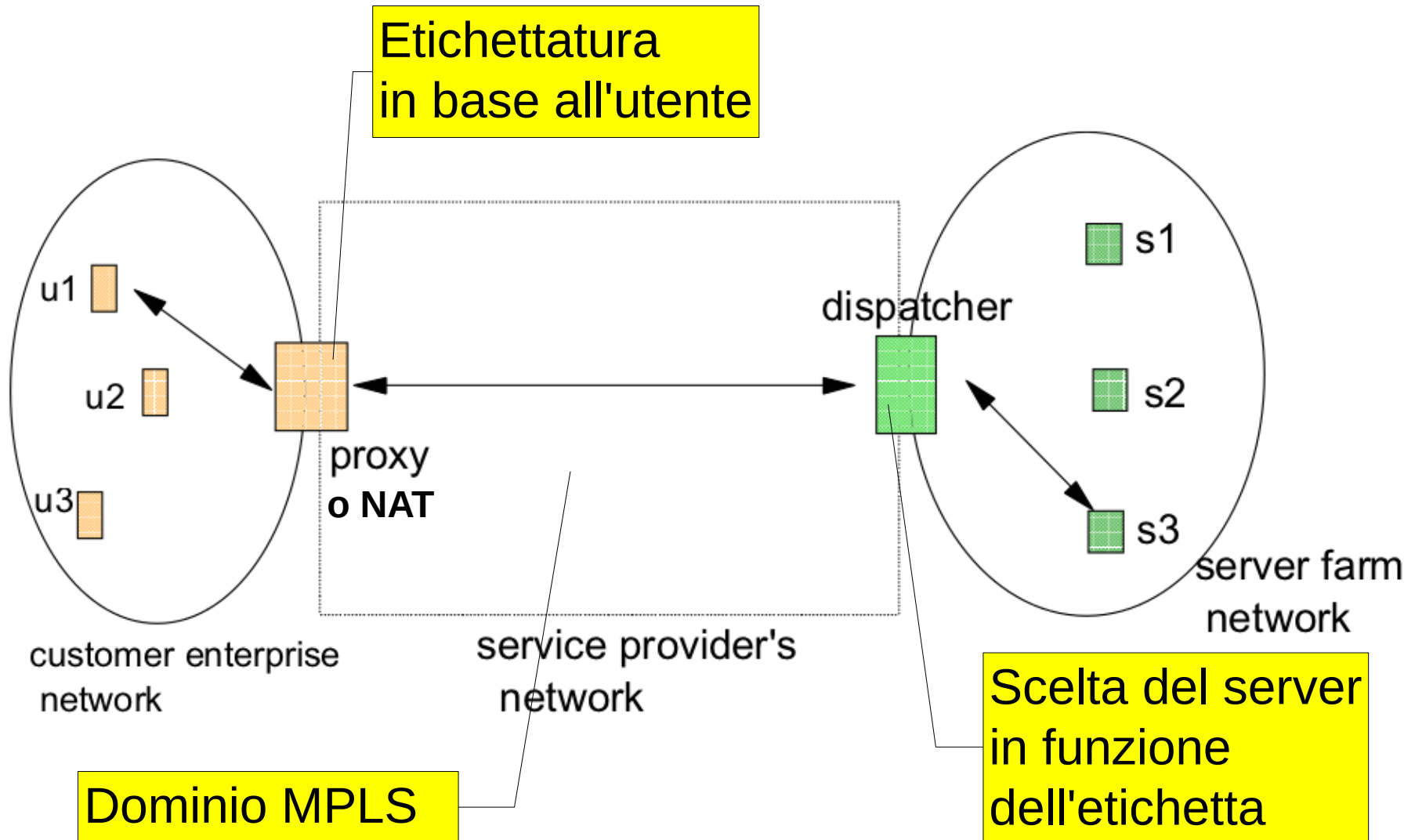
La scelta del server avviene in funzione dell'IP del client in modo che tutte le richieste dello stesso client vadano allo stesso server

Server Farm: scenario con proxy



Tutte le richieste arrivano dal proxy
o tutto va ad s3
o necessita' di guardare dentro il TCP

Server Farm con MPLS



Voice over MPLS

Si utilizza una label per identificare ogni connessione voce

Si risparmiano $20+8+12$ byte di header IP/UDP/RTP

Il traffico voce riceve priorità nei router MPLS

Bibliografia

R. Hunt, A review of quality of service mechanisms in IP-based networks - integrated and differentiated services, multi-layer switching, MPLS and traffic engineering, Elsevier CompComm Mag., 2002

<http://www.ietf.org>

RFC 3031: Multiprotocol Label Switching Architecture, 2001

RFC 3032: MPLS Label Stack Encoding, 2001

Assured forwarding (AF)

- Simile alla lettera raccomandata
- Obiettivo: dare priorità all'accesso alla banda
 - utenza “business”
 - utenza dial-up a pagamento
 - utenza dial-up gratis
- Ogni classe usa ciò che rimane della banda e lascia il resto alla classe più bassa

DiffServ: considerazioni finali

- assegnare tutto il traffico ad una stessa classe significa tornare al modello best-effort
- Es: rete IP con traffico dati + multimedia real-time
 - best-effort per il traffico dati
 - expedited e assured forwarding per multimedia
- Oggi con pochi servizi multimediali funziona
- Cosa succederà quando il traffico multimediale pareggerà o supererà il traffico dati ?
- Possibile soluzione
 - non tutti i pacchetti multimediali alle classi nobili (cercare un punto ottimo)
 - torna il compromesso rate (risorse) - distortion

Bibliografia

- R. Hunt, A review of quality of service mechanisms in IP-based networks - integrated and differentiated services, multi-layer switching, MPLS and traffic engineering, Elsevier Comp. Comm. Mag., 2002
- B. E. Carpenter, K. Nichols, Differentiated Services in the Internet, Proceedings IEEE, vol. 90, n. 9, settembre 2002
- <http://ieeexplore.ieee.org>

Bibliografia

- <http://www.ietf.org>
 - RFC 2638: A Two-bit Differentiated Services Architecture for the Internet, 1999
 - Riporta le idee pre-rfc2474, utile la versione pdf con figure
 - RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, 1998
 - RFC 2475: An Architecture for Differentiated Services, 1998
 - RFC 2597: Assured Forwarding PHB Group, 1999
 - RFC 3246: Expedited Forwarding PHB Group, 2002
 - RFC 3260: New Terminology and Clarifications for Diffserv, 2002
 - RFC 2998: A Framework for Integrated Services Operation over Diffserv Networks, 2000