TIZIANO TOFONI

# Servizi MPLS


Edizioni REISS ROMOLI

**Copyright © REISS ROMOLI S.r.l.**

Via E. Berlinguer 3, 67100 L'Aquila (Italy)

Tel./Fax : +39 0862 452401

e-mail : info@ssgrr.com

**www.reissromoli.com**

Tutti i diritti sono riservati a norma di legge e a norma delle convenzioni internazionali

**ISBN 978-88-905806-9-7**

Prima Stampa: Ottobre 2020

Stampato in Italia da:

FABRESCHI PRINTING
Via della Forma, 22
00028 Subiaco RM

# INDICE

# Prefazione

Nel lontano 2003 ho scritto il primo (e forse unico, in lingua Italiana) libro sullo standard MPLS. Molti anni sono passati da allora, e dalle prime pionieristiche applicazioni MPLS ha fatto molta strada, divenendo uno standard utilizzato ormai da tutti i *Service Provider* medio-grandi del mondo e da molte reti *Enterprise*. Ho ritenuto che era ora di un ampio "tagliando" alla prima edizione, poiché nel frattempo MPLS ha avuto una sua evoluzione. Sono nati molti nuovi servizi che lo utilizzano sul piano dati, che oggi fanno parte dell'offerta di quasi tutti i *Service Provider*, e che sono utilizzati anche nelle reti *Enterprise*.

MPLS è oggi un protocollo maturo, che presumibilmente non subirà grosse modifiche negli anni a venire, se non nel piano di controllo, che sarà semplificato. Per cui, arrivato ormai alla fine della mia vita professionale, che ho dedicato in una parte non trascurabile allo studio e alle applicazioni pratiche delle tecnologie utilizzate nei grandi *backbone* dei *Service Provider*, ho deciso di raccogliere la mia esperienza in una seconda edizione del libro, che spero potrà essere utile alle future generazioni di *networkers*. Ho deciso anche di cambiare il titolo, passando da “MPLS: fondamenti e applicazioni alle reti IP" della prima edizione, a "Servizi MPLS". Il perché il lettore lo scoprirà leggendo il libro, ma una prima anticipazione voglio darla: MPLS è diventato importante perché attraverso di questo è possibile ampliare e di molto la gamma di servizi offerti dalle reti IP tradizionali. E credo che i servizi MPLS rimarranno nei prossimi anni il fulcro dell’offerta dei *Service Provider* verso i loro clienti.

Il libro, per come è concepito, richiede per la sua lettura solide basi dell’architettura TCP/IP, ed in particolare delle basi del protocollo BGP. Inoltre, poiché sono illustrati vari aspetti di configurazione sia in ambiente Cisco (IOS/IOS-XE/IOS-XR) che Juniper (JUNOS), è richiesta una conoscenza di base di questi Sistemi Operativi. È comunque mia ferma opinione che la conoscenza o meno di un particolare Sistema Operativo non sia poi così importante, una volta compresi bene i concetti che sono dietro al protocollo e ai suoi servizi. Passare da una tecnologia ad un’altra è solo questione di apprendere i comandi fondamentali e capire come il protocollo è stato implementato dal particolare costruttore, con quest’ultimo aspetto che è molto importante nell’interlavoro di macchine diverse.

Il libro può considerarsi in generale di livello medio-alto, mentre per ciò che riguarda MPLS può essere letto sia da chi ne abbia già le conoscenze di base e voglia approfondirne i concetti, sia da chi non ha alcuna conoscenza dello standard. Esso è rivolto al vasto pubblico di esperti di *Internetworking* sia lato reti *backbone* (ad esempio, le grandi reti dei *Service Provider*), che lato reti *Enterprise* (vedi tutti gli enti come Banche, Industrie, Pubblica Amministrazione, molti dei quali hanno le loro Reti Aziendali basate su *backbone* IP/MPLS).

Mi auguro che la sua lettura consenta ai lettori, al di là della comprensione dei fondamenti teorico-pratici dello standard, di capire l’utilità di integrare MPLS nelle reti IP.

***Tiziano Tofoni***

# Presentazione

La rivoluzione digitale, iniziata alla fine degli anni ’80 e basata sul successo oltre ogni previsione del fenomeno Internet, ha portato all’introduzione di nuovi attori e di nuove tecnologie.

Queste nuove tecnologie hanno permesso di aumentare di molto il *throughput* e la gamma dei servizi a disposizione per gli utilizzatori finali e di introdurre nuovi paradigmi, come ad esempio la virtualizzazione, il *Cloud Computing*, i *Data Center*, che stanno rivoluzionando l’essenza stessa delle reti e la loro architettura.

Paradossalmente, al di la di tutto questo fermento, le fondamenta su cui si poggia l’Internet sono basate ancora sull’architettura TCP/IP, sviluppata tra la fine degli anni ’70 e gli inizi degli anni ’80 da personaggi ormai divenuti celebri come Vinton Cerf, Bob Khan, Leo Kleinrock e Jonathan (Jon) Postel. Tra l’altro anche prima di molte tecnologie che oggi sono considerate ormai obsolete, come ad esempio l’ATM (*Asynchronous Transfer Mode*), sviluppato tra la fine degli anni ’80 e i primi anni ’90. Allo stesso modo, l’altro grande pilastro dello sviluppo delle reti IP, lo standard Ethernet, ha visto i suoi albori agli inizi degli anni ’70, grazie agli studi pionieristici di Bob Metcalfe.

Per gli *Internet Service Provider* (ISP) l’evoluzione delle reti si è invece realizzata nel decennio successivo ed un aiuto fondamentale alla rete IP di “base” (con i suoi intramontabili protocolli OSPF, IS-IS e BGP) è arrivato dall’introduzione, alla fine degli anni ’90, dello standard *Multi Protocol Label Switching* (MPLS). Questo protocollo nacque quando i router non erano ancora dotati di una grande velocità di calcolo, per accelerare l’elaborazione dei pacchetti IP disaccoppiando il calcolo dell’instradamento dal piano di *forwarding*, quest’ultimo ridotto ad una semplice Commutazione di Etichetta (*Label Swapping)*.

Ma la vera fortuna di MPLS non fu tanto legata al motivo originale per cui venne ideato, quanto alle sue caratteristiche di grande versatilità, flessibilità e scalabilità, costituendo per gli operatori di tutto il mondo un elemento abilitante per la realizzazione di reti IP moderne, integrate e multiservizio.

MPLS è infatti oggi implementato con successo nei *backbone* IP di quasi tutti gli ISP ed in reti *Enterprise*, anche di dimensioni medio-piccole, che ne utilizzano le funzionalità per offrire servizi di Rete Privata Virtuale sia di Livello 3 (L3VPN) che di Livello 2 (L2VPN), servizi di trasporto del traffico IPv6 con i modelli 6PE e 6VPE, e perfino servizi per il trasporto del traffico telefonico più tradizionale.

TIM è stata decisamente un pioniere in questo campo, avendo già iniziato nel lontano 2001, tra i primi al mondo, ad offrire ai suoi Clienti *Executive* e *Business* i servizi L3VPN sulla sua rete IP/MPLS e avendo, l’anno seguente, intrapreso con successo la migrazione del trasporto del traffico telefonico di Rete Fissa, e successivamente anche di Rete Mobile, dalla Rete a Commutazione di Circuito tradizionale sul suo Backbone Nazionale IP/MPLS (per inciso, quando ingegnerizzammo MPLS per la rete di Telecom Italia di allora, il mio collega Simeone Mastropietro ed io non avremmo mai e poi mai immaginato tutto ciò).

Tornando alla tecnologia, MPLS ha avuto sicuramente una sua metamorfosi negli anni anche se il paradigma di fondo, il piano di *forwarding* basato sull'uso estensivo delle etichette, è rimasto invariato. Per il futuro, quantomeno per la sua componente di trasporto, MPLS sarà ancora un pilastro fondamentale per le reti degli ISP e di molte reti *Enterprise*.

Come dimostra la continua estensione con nuove funzionalità di protocolli quali MP-BGP, di supporto alla realizzazione di servizi basati su MPLS, si continuerà senza dubbio ad avere un'evoluzione sul piano di controllo ed i protocolli classici come LDP e RSVP-TE (ampiamente trattati nel libro) saranno tendenzialmente sostituiti dal *Segment Routing* (anche questo trattato nel libro); ma il piano dati rimarrà comunque sempre quello originale basato sul paradigma della Commutazione di Etichetta e soprattutto i servizi di oggi, basati su MPLS, non scompariranno affatto ma continueranno piuttosto ad arricchirsi di nuovi casi di uso come l'ingegnerizzazione del traffico sulla base di requisiti di latenza o la definizione della topologia di rete in funzione del servizio (*slicing*); e lo stesso titolo del libro sintetizza tutto ciò (Servizi e non solo Tecnologia).

Il libro nasce quindi con la finalità di illustrare in modo esaustivo le caratteristiche sia classiche che avanzate di MPLS ed evidenziarne le applicazioni maggiormente caratterizzanti. Oltre ai fondamenti dello standard, l'enfasi del libro è giustamente sui Servizi che l'aggiunta di MPLS alle reti IP consente di realizzare in modo flessibile e scalabile.

Oltre a tali obiettivi, altri aspetti premianti sono il rigore tecnico ed i riferimenti continui alle specifiche ufficiali, ma soprattutto l'attenzione rivolta agli aspetti pratici ed applicativi. Infatti, per ciascun servizio trattato, è stato dato ampio spazio alle modalità di configurazione degli apparati ed alla implementazione di MPLS sugli stessi, con numerosi ed interessanti esempi, per altro sia su tecnologia Cisco che Juniper.

Questo libro è quindi di grande utilità per tutti coloro che vogliano avvicinarsi al mondo di MPLS ed in generale alle problematiche avanzate delle reti IP, ma costituisce una lettura unica, per la sua impostazione, per coloro che sono chiamati ad operare su reti che forniscono servizi MPLS, sia negli aspetti di implementazione e gestione, che nel campo della progettazione e vendita dei servizi.

Ora mi permetto di chiudere con una breve nota personale; per me è un grande onore scrivere la presentazione di questo libro: Tiziano è stato nostro docente alla *Scuola Superiore Guglielmo Reiss Romoli* nei primi anni '90 e le sue lezioni ci lasciavano già allora a bocca aperta; non esisteva ancora l'IP, si parlava di Erlang e di Teoria delle Code e delle emergenti tecnologie a commutazione di pacchetto (come l'ormai preistorico X.25). Sono passati tanti anni, ma ciò non ha di certo intaccato la competenza, la professionalità e soprattutto la passione di Tiziano e infatti mi dicono tutti che le sue lezioni hanno sulle nuove leve lo stesso effetto che fece a noi quasi trenta anni fa.

A Tiziano i miei più sinceri complimenti per l'egregio lavoro svolto ed ai lettori un augurio per una interessante e proficua lettura.

***Alberto Maria Langellotti***

***Responsabile IP, Transport & SDN in TIM***

# Ringraziamenti

Durante la realizzazione di questo lavoro ho potuto beneficiare dell'aiuto di molte persone che mi ritengo fortunato di poter avere come Amici (con la A maiuscola), e alle quali va la mia sincera gratitudine.

In particolare desidero ringraziare tutte quelle persone che hanno letto in anteprima parti del libro, dandomi suggerimenti preziosi per il suo miglioramento: Moreno Granzotto di Insiel, Nicola Modena, consulente indipendente e Marco Serra di RFI.

Inoltre, desidero ringraziare i molti amici di TIM, tra cui Alberto Langellotti, Antonio Soldati, Carlo Cianfarani, Tiziano Ionta e Simeone Mastropietro, con i quali negli anni ho avuto interessanti scambi di idee sul ruolo di MPLS e sulle sue applicazioni reali nella rete di un grande ISP.

Infine, *last but not least*, come per ogni libro che ho scritto. ringrazio le due donne di casa, Vicky e Fiammix (Maria Vittoria e Fiammetta). Senza la loro stanchezza serale (che mi permetteva di concentrarmi sul lavoro) e senza la loro pazienza a sopportare le mie continue assenze mentali, probabilmente questo libro non avrebbe mai visto la luce. A loro dedico questo lavoro.

La teoria è quando si sa tutto e non funziona niente.
La pratica è quando tutto funziona e nessuno sa il perché.
Noi abbiamo messo insieme la teoria e la pratica:
non c'è niente che funzioni, e nessuno sa il perché!
**Albert Einstein**

# 1 – ROUTING NELLE RETI ISP

MPLS è un protocollo utilizzato nei *backbone* delle reti IP, siano esse i grandi *backbone* delle reti degli *Internet Service Provider* (ISP), che i *backbone* generalmente più piccoli delle reti *Enterprise*. Per questo, prima di vedere il funzionamento di MPLS e i principi su cui si basa, è bene inquadrare il ruolo delle tre componenti chiave dei moderni *backbone* IP: il protocollo di routing interno (IGP), il protocollo BGP e MPLS. In questo capitolo introduttivo tratteremo i due seguente aspetti:

- Il ruolo dei protocolli IGP (OSPF oppure IS-IS) ed EGP (in pratica del BGP, che è l'unico protocollo di tipo EGP adottato universalmente nelle reti IP).
- Il ruolo di MPLS e il suo contributo nell'architettura di routing complessiva e nella realizzazione di nuovi servizi di rete.

Il primo aspetto è importante per capire l'interazione tra i protocolli di routing presenti nei moderni *backbone* IP e quale è il compito svolto dalle due tipologie di protocolli (IGP ed EGP) in una architettura di routing che sia flessibile e soprattutto scalabile.

Il secondo aspetto ci permetterà invece di avere una visione generale del ruolo di MPLS all'interno dell'architettura di routing dei moderni *backbone* IP, e soprattutto perché è importante utilizzarlo. A questo proposito deve essere chiaro un punto, forse qualche servizio di rete oggi realizzato con MPLS potrebbe essere realizzato in qualche altro modo, ad esempio utilizzando una rete IP senza l'ausilio di MPLS. Ma il prezzo da pagare sarebbe molto alto, sia in termini di complessità di configurazione, che di flessibilità e soprattutto di scalabilità (ossia, la possibilità di fornire il servizio a un numero molto elevato di clienti).

Infine, il capitolo si concluderà con una visione sulle motivazioni che oggi dovrebbero spingere un progettista di una rete IP a inserire MPLS nel proprio *backbone*.

## 1.1 ARCHITETTURA DELLE RETI ISP

Le reti degli ISP o anche delle grandi compagnie *enterprise*, come tutte le reti IP, sono caratterizzate da tre elementi fondamentali:

- La *topologia*.
- Il *piano di numerazione*.
- L'*architettura di routing*.

Questi sono anche i tre aspetti che guidano le scelte progettuali per realizzare reti stabili, scalabili e facilmente espandibili in funzione delle esigenze di traffico.

In questo paragrafo daremo dei cenni ai primi due elementi, mentre al terzo sarà dedicato il successivo Paragrafo 1.2.

### 1.1.1 Topologia: Accesso, Aggregazione, *Backbone*

La realizzazione di una topologia di rete che sia scalabile, stabile e facilmente espandibile, segue delle linee guida di progetto, che possono essere riassunte nei seguenti punti:

- *Gerarchia*: è questo il modo più semplice per realizzare reti scalabili. Per gerarchia si intende la possibilità di dividere la rete in aree di accesso e commutazione locale, tipicamente definite su base geografica, e la presenza di un livello gerarchico superiore che fa da "collante" tra le varie aree.
- *Modularità*: nel progetto di una rete è necessario tener conto dei futuri sviluppi, e quindi è bene adottare una architettura di rete che sia facilmente estendibile. Una topologia modulare minimizza i costi di espansione, rende più semplice la predizione del traffico e aumenta l'efficienza del *troubleshooting* in caso di fuori servizio.
- *Ridondanza*: poiché gli apparati utilizzati dalla rete, siano essi di trasmissione o di commutazione, sono soggetti a fuori servizio, è opportuno progettare una topologia di rete che tenga conto di fuori servizio multipli. Una rete quindi, deve essere sufficientemente magliata in modo da garantire comunque la connettività fisica tra gli apparati di commutazione (router), anche in presenza di uno scenario simile. È anche bene tener presente, per contro, che una magliatura troppo fitta risulta non economica e potrebbe causare rallentamenti del tempo di convergenza dei protocolli di routing (maggiore è la magliatura, maggiore è il numero di cammini disponibili, e quindi maggiore è il tempo per determinare i percorsi ottimi).
- *Semplicità*: un progetto semplice risulta in configurazioni degli apparati più semplici e standardizzabili, in un numero minore di errori umani nella fase di configurazione della rete, in una maggiore capacità di automazione e in una maggiore velocità di risoluzione dei problemi.

Le reti IP di dimensione medio-grandi hanno spesso architetture gerarchiche basate su tre livelli:

- *Livello di accesso*: è il livello responsabile della connettività verso i clienti esterni. Il livello di accesso può essere su rete fissa o rete mobile ed è svolto da nodi particolari (es. Stazioni Radio Base, *DSLAM*, *OLT* per gli accessi in fibra ottica, ecc.), che vengono spesso indicati come nodi di accesso (*AN, Access Node*).
- *Livello di aggregazione (backhauling)*: è un livello intermedio che serve, nelle reti di grandi dimensioni, a ridurre la complessità dell'interconnessione tra le varie aree di accesso. In reti di medie dimensioni a volte coincide con il livello di transito, portando di fatto ad una topologia basata su due livelli piuttosto che su tre. A svolgere le funzioni del livello di aggregazione, trascurando quelle *legacy* basate su *Frame Relay* o *ATM*, sono nelle reti attuali *switch Ethernet multilayer*, che in funzione delle strategie adottate, possono essere utilizzati o come semplici e puri *switch Ethernet*, oppure come *router* di Livello 3 (IP), eventualmente con in aggiunta delle funzionalità MPLS, fermo restando che in questo caso il collegamento tra i *router* avviene con tecnologia *Ethernet*, che viene utilizzata come pura e semplice tecnologia di trasporto di Livello 1 e 2 della pila OSI. La preferenza è verso questa ultima soluzione poiché consente di evitare tutte le problematiche legate all'utilizzo del protocollo *Spanning Tree*, necessario nelle reti *switched Ethernet* per evitare pericolosi problemi di *forwarding loop* (spreco di banda, percorsi non ottimi, ecc.). I nodi del livello di aggregazione vengono spesso indicati come *Transport Node* (*TN*), poiché svolgono essenzialmente funzioni di trasporto tra la rete di accesso e il livello superiore (*Core network*). I router del livello di

aggregazione hanno due tipi di collegamenti: *uplink*, verso i router della *Core network*, *downlink* verso i nodi del livello di accesso. Nelle architetture più comuni, i *router/switch* del livello di aggregazione hanno uno o due collegamenti *uplink* verso uno o due router del livello di transito, e più collegamenti *downlink* verso i nodi del livello di accesso.

- *Core network*: è un livello che ha una duplice funzione: attivazione dei servizi richiesti dal cliente (es. Reti Private Virtuali, accesso all'Internet IPv4/IPv6, emulazione di circuito, ecc.) e interconnessione tra i livelli di aggregazione. I servizi dei clienti sono attivati nei nodi di frontiera con la rete di aggregazione, per questo questi nodi vengono spesso indicati come *Provider Edge* (*PE*) oppure più in generale *Service Node* (*SN*). Poiché il ruolo primario dei nodi di frontiera è quello dell'attivazione dei servizi, è opportuno da un punto di vista progettuale che questi nodi siano adeguati alla quantità di servizi che devono offrire, e che offrano un sufficiente livello di scalabilità del piano di controllo. Nella *Core network* sono poi presenti dei nodi di puro transito, che vengono spesso indicati come router *Provider* (*P*) oppure più in generale anche questi *TN*. Poiché il ruolo primario dei nodi di transito, è quello di smaltire grossi volumi di traffico, è opportuno, da un punto di vista progettuale, evitare che questi svolgano funzioni complesse. La loro configurazione dovrebbe essere mantenuta al massimo livello di semplicità, assegnando al piano di controllo le sole funzioni indispensabili, come ad esempio la gestione delle informazioni di routing, e, solo nel caso di implementazione dello standard MPLS, della gestione delle etichette MPLS e dell'attivazione di eventuali percorsi MPLS espliciti. A questo livello sono applicate le funzioni più complesse come le politiche di *routing* del traffico da e verso il cliente, il controllo del traffico, eventuali politiche di Qualità del Servizio (es. classificazione e/o colorazione del traffico, *scheduling*, *policing/shaping*, ecc.). La *Core network* ha un ruolo di primaria importanza, per cui è necessario che sia costituita da router di adeguata potenza, da collegamenti trasmissivi ad elevata capacità e altamente affidabili, e da una topologia con una magliatura sufficiente ad evitare partizioni della rete, anche in presenza di fuori servizio multipli.

Oltre ai router appartenenti ai tre livelli gerarchici descritti, le reti degli ISP possono anche avere, soprattutto se molto grandi, anche router dedicati a funzioni particolari, come *Route Reflection*, *BGP peering* verso *Upstream Provider* e altri ISP con cui si hanno semplici accordi di *peering* e *Shadow Router*, ossia router dedicati a rilevare misure prestazionali sulla rete. In funzione del ruolo svolto, è necessario che questi abbiano adeguata potenza elaborativa. Ad esempio, i *Route Reflector* sono spesso dedicati al solo lavoro di gestione degli annunci BGP e non svolgono il ruolo di smaltimento del traffico (o perlomeno, non dovrebbero farlo in una rete progettata correttamente!), per cui sono sufficienti anche router di capacità di *forwarding* modesta. Per contro, devono essere router dotati di molta memoria poiché è da loro che transitano tutti gli annunci *BGP* da e verso l'*Autonomous System* (AS).

La Figura 1.1 seguente riassume l'architettura basata sui tre livelli gerarchici appena descritti.

### 1.1.2 Piano di numerazione

Il progetto di un piano di numerazione, anche se all'apparenza semplice, deve essere eseguito con cura, tenendo conto di fattori quali la sicurezza, la semplicità in fase di *troubleshooting*, l'estendibilità a fronte di crescita in dimensioni della rete.

Il piano di numerazione della rete di un ISP deve occuparsi principalmente di assegnare indirizzi IP (v4 oppure v6):

- Alle interfacce di *Loopback* di ciascun router. Le interfacce di *Loopback*, anche se teoricamente non indispensabili, sono una componente molto importante in un progetto "elegante" di rete. Queste vengono utilizzate soprattutto come estremi di sessioni iBGP (iBGP=*internal* BGP) e possibilmente, dipende dalle scelte di configurazione, come identificativo in alcuni protocolli di routing e di distribuzione delle etichette MPLS.
- Alle interfacce fisiche dell'infrastruttura interna di rete (es. interfacce LAN, collegamenti punto-punto).
- Per scopi gestionali (applicazioni *Telnet*, interfacce verso i centri di gestione).

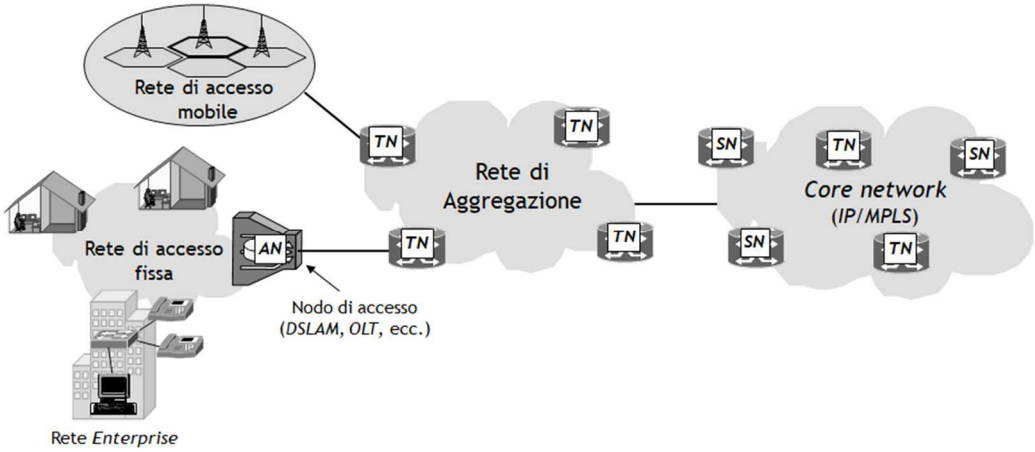


**Figura 1.1** - Esempio di architettura di rete di un grande ISP.

Come *best-practice* di configurazione, le interfacce di *Loopback* dovrebbero sempre essere /32 nel caso di indirizzamento IPv4 o /128 nel caso di indirizzamento IPv6, mentre per le interfacce fisiche si possono utilizzare:

- Per i collegamenti punto-punto, nel caso di indirizzamento IPv4 prefissi /30 o meglio ancora /31 (se supportati). Nel caso di indirizzamento IPv6 si possono utilizzare prefissi /127 (consigliato), o per maggiore semplicità, /64.
- Per i segmenti di rete *broadcast* (LAN), nel caso di indirizzamento IPv4 un prefisso con *subnet mask* di lunghezza funzione del numero di router del segmento, sempre tenendo in mente futuri ampliamenti. Nel caso di indirizzamento IPv6 si utilizzano tipicamente, per vari motivi che esulano dallo scopo di questa trattazione, prefissi /64.

Una prima scelta da fare, quando si affronta la definizione di un piano di numerazione, è se utilizzare indirizzi pubblici o privati (*unique-local* nel gergo IPv6). Su questo aspetto ci sono diversi punti di vista tra i vari ISP, ma molti convergono sull'opportunità di utilizzare indirizzi privati, e vi sono stati casi di migrazione da piani di numerazione pubblici a privati.

La motivazione principale della scelta di utilizzare indirizzi privati è la maggiore sicurezza, dovuta al fatto che i router pubblici non accettano pacchetti IP con indirizzo destinazione privato (come si dice nel gergo del *Networking IP*, gli indirizzi privati sono *non routable*). Questo rende praticamente impossibile ad eventuali *hacker*, di prendere il controllo di un router e mettere in crisi l'intera rete. In

realtà, anche utilizzando indirizzi pubblici, questo potrebbe essere reso praticamente impossibile: sarebbe sufficiente non propagare all'esterno dell'AS il blocco di indirizzi utilizzato per il piano di numerazione, e inserire meccanismi di sicurezza perimetrale, impedendo a pacchetti destinati a un indirizzo del blocco di entrare nella rete. Ma questo comporta maggiore complessità nelle configurazioni, mentre utilizzando indirizzi privati, molti aspetti sono risolti automaticamente dai filtri standard applicati dagli ISP nei router pubblici. Infatti, questi di norma impediscono annunci BGP dei prefissi *non routable* e filtrano sul piano dati tutto il traffico destinato a indirizzi IP privati.

L'utilizzo di indirizzi privati non comporta alcuna difficoltà operativa, poiché il routing interno alla rete dell'ISP, in una rete ben progettata, va tenuto completamente isolato dal mondo esterno. In altre parole, il processo di routing che regola la determinazione dei percorsi interni (tipicamente OSPF o IS-IS, vedi il successivo Paragrafo 1.2), non deve avere alcuna adiacenza con router esterni all'AS.

## 1.2 ARCHITETTURA DI ROUTING DELLE RETI ISP

L'idea fondamentale per la costruzione di una rete scalabile, è quella di mantenere al più basso livello di complessità possibile il protocollo di routing IGP. Una cosa assolutamente da evitare, ad esempio, è quella di iniettare nel processo di routing IGP un numero elevato di prefissi, poiché ciò porta facilmente alla saturazione delle risorse di memoria anche in router di grandi dimensioni. Per questo scopo è più adatto il BGP, progettato sin dall'inizio per gestire grossi volumi di prefissi IP.

Le reti moderne utilizzano protocolli IGP di tipo *Link State*, in particolare le scelte ricadono su OSPF o IS-IS. OSPF e IS-IS sono protocolli con caratteristiche simili, anche se IS-IS è più semplice e ha qualche vantaggio in termini di scalabilità. Ma non è questo che guida la scelta degli ISP, piuttosto, ciò che maggiormente interessa è tipicamente il grado di esperienza del personale, nella configurazione e nella risoluzione di problemi del protocollo.

L'architettura di routing interna di una grande rete ISP si basa su un modello che può essere riassunto come segue:

- Il protocollo IGP trasporta esclusivamente informazioni di routing interne della rete (prefissi delle interfacce di *Loopback* e prefissi IP utilizzati per numerare l'infrastruttura interna).
- Una maglia di sessioni iBGP tra ciascun router *PE* e tutti gli altri router della rete (*P* e *PE*).
- Un insieme di sessioni eBGP per lo scambio di informazioni di routing con i propri clienti o con altri ISP. Lato clienti possono essere utilizzati anche altri protocolli di routing (es. OSPF, IS-IS, EIGRP, RIP), anche se oggi il protocollo preferito, soprattutto in scenari *fault-tolerant*, è il BGP.

La maglia di sessioni iBGP è il punto debole di questo modello. Infatti, in reti di grandi dimensioni, il numero di sessioni iBGP potrebbe essere troppo elevato, e quindi di difficile gestione. Il calcolo del numero esatto di sessioni iBGP necessarie è presto fatto. Indicando con $N$ il numero totale di router della rete, e con $NP$ il numero dei router $P$, il numero di sessioni iBGP è pari a:

$$N.ro\ sessioni\ iBGP = [N \cdot (N\text{-}1) - NP \cdot (NP - 1)] / 2$$

dove il termine sottratto tiene conto del fatto che le sessioni iBGP tra router $P$ non servono.

Ad esempio, in una rete con 200 router *PE* e 72 router *P*, sono richieste 0,5*[272*(272–1) – 72*(72–1)] = 34.300 sessioni iBGP. Da ciascun router *PE*, in particolare, devono essere configurati 271 *BGP peer*. Esistono varie soluzioni che consentono una drastica riduzione del numero delle sessioni iBGP. Le più note e più applicate nelle reti in esercizio sono la funzionalità di *Route Reflection* (vedi Sezione

1.2.2), e l'introduzione di MPLS (vedi Sezione 1.2.3). Le due soluzioni non sono alternative, ma di norma vengono utilizzate congiuntamente, per creare una architettura di routing ottimale, sulla quale sono basati tutti i servizi di rete più importanti (vedi Sezione 1.2.3).

### 1.2.1 Ruoli del protocollo IGP e del BGP

Il modello di routing basato sull'utilizzo di un protocollo IGP e del BGP, si poggia su una regola molto semplice: propagare i prefissi esterni all'AS all'interno della rete, tramite il protocollo BGP, e non tramite una redistribuzione nel protocollo IGP.

Questa semplice regola definisce chiaramente il ruolo dei due protocolli:

- Il protocollo BGP serve a propagare all'interno della rete tutti i prefissi appresi dall'esterno dell'AS, ossia, i prefissi dei propri clienti (sia privati che eventuali piccoli ISP), e quelli comunicati dagli altri ISP.
- Il protocollo IGP serve a creare percorsi ottimi interni alla rete, in particolare tra le interfacce utilizzate per le sessioni iBGP, che è buona pratica che siano interfacce di *Loopback*.

Vediamo ora, con un esempio, l'interazione tra il protocollo IGP e il BGP all'interno della rete di un ISP, e come avviene l'instradamento di un pacchetto. La Figura 1.2 seguente riporta lo schema di propagazione degli annunci BGP e il percorso ottimo determinato dal protocollo IGP.

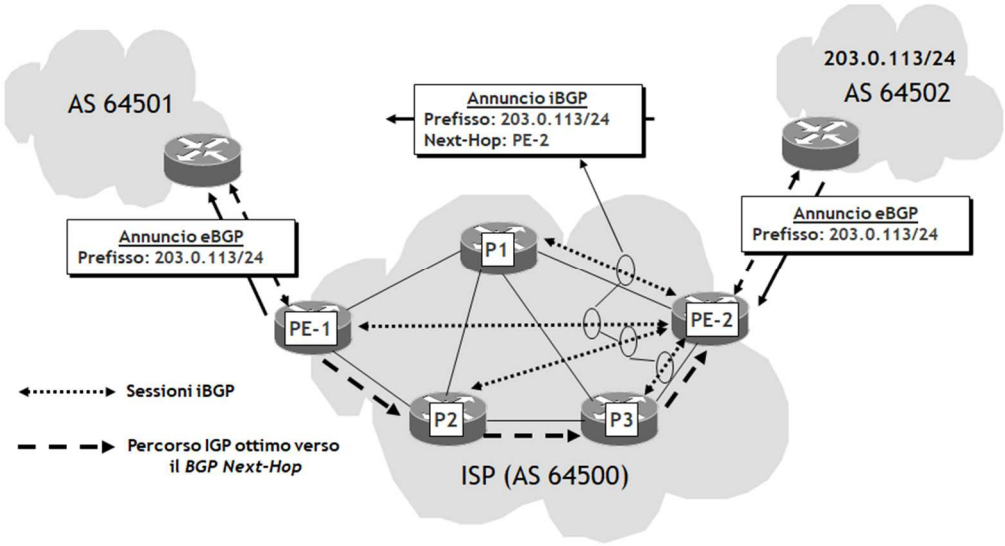


**Figura 1.2** - Propagazione degli annunci BGP e percorso verso il *BGP Next-Hop*.

L'ISP (AS 64500), ha due sessioni eBGP verso un cliente privato (AS 65002) e verso un altro ISP (AS 64501). Dall'AS 65002 riceve, sul router PE-2, un annuncio eBGP del prefisso 203.0.113/24, che propaga ai router P1, P2, P3 e PE-1 attraverso le sessioni iBGP tra PE-2 e questi router. Nella propagazione sulle sessioni iBGP, è buona regola cambiare, via configurazione, la gestione di *default* dell'attributo BGP NEXT_HOP, inserendo nell'attributo l'indirizzo IP utilizzato per la sessione iBGP (nella figura è schematizzato semplicemente con il nome del router, nella pratica è bene che sia l'indirizzo IP di un'interfaccia di *Loopback*).

A fronte di questa propagazione, PE-1 installerà nella propria RIB il prefisso 203.0.113/24 con *Next-Hop* PE-2. Poiché il *Next-Hop* PE-2 è contenuto nell'annuncio iBGP, chiameremo questo il *BGP Next-Hop*. Il protocollo IGP permetterà inoltre di installare nella RIB di PE-1, il *Next-Hop* verso il *BGP Next-Hop*. Chiameremo questo l'*IGP Next-Hop*. L'annuncio viene infine propagato verso l'ISP che ha AS=64501, tramite la sessione eBGP con questo.

Ora, vedi la Figura 1.3 seguente, supponiamo che PE-1 riceva dall'AS 64501 un pacchetto diretto verso l'*host* 203.0.113.1, parte del prefisso 203.0.113/24. PE-1 effettua un primo *lookup* sulla propria RIB, dal quale evince che per raggiungere il prefisso 203.0.113/24 il *Next-Hop* è PE-2 (=*BGP Next-Hop*). Ora, poiché il *BGP Next-Hop* non è direttamente connesso, PE-1 è costretto ad effettuare un secondo *lookup* sulla propria RIB, per trovare un percorso (ottimo) verso il *BGP Next-Hop* PE-2. Compito di trovare questo percorso è del protocollo IGP, che stabilisce che la via migliore per raggiungere PE-2, è transitare attraverso P2 (*IGP Next-Hop*).

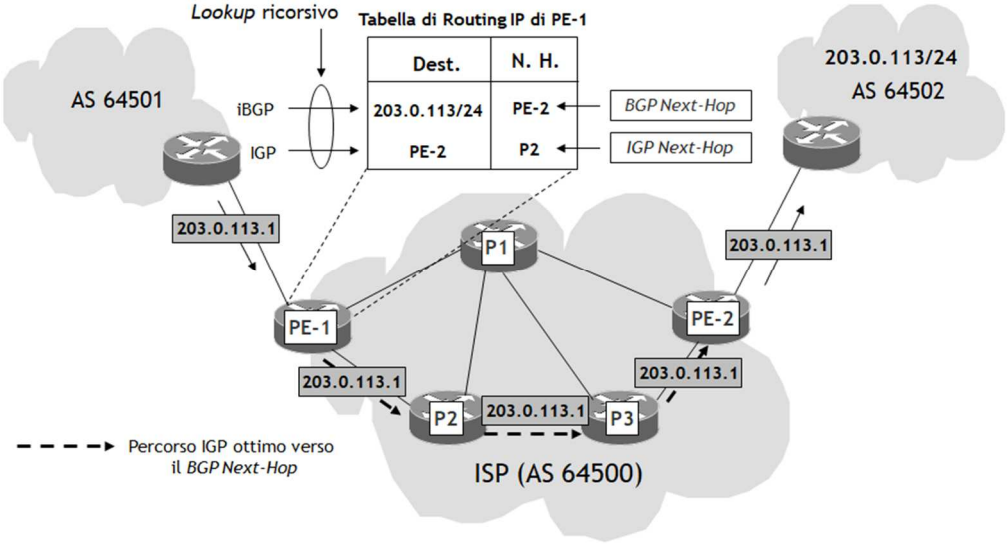


**Figura 1.3** - Instradamento di un pacchetto nell'architettura di routing IGP+BGP.

Il pacchetto IP viene quindi inviato a P2. P2 ripete esattamente le stesse operazioni, inviando il pacchetto al suo *IGP Next-Hop* verso PE-2, ossia P3, e così via fino a quando il pacchetto non raggiunge PE-2. Quando PE-2 riceverà il pacchetto, lo inoltrerà verso l'AS 65002, poiché è da questo che ha ricevuto, via eBGP, l'annuncio del prefisso 203.0.113/24.

**NOTA**: il doppio *lookup* effettuato sulla RIB viene indicato come *lookup ricorsivo*. Nella realtà i router, per evitare per ciascun pacchetto da instradare un *lookup ricorsivo*, determinano in anticipo il *Next-Hop* effettivo (=*IGP Next-Hop*). Questa informazione viene quindi trasferita attraverso un protocollo interno (tipicamente proprietario), alla Tabella di *Forwarding* (anche nota come FIB, *Forwarding Information base*), realizzata in *hardware*. I router utilizzano quindi le informazioni contenute nella FIB per instradare i pacchetti.

Questa architettura di routing, benché richieda due protocolli, invece del solo protocollo IGP come in passato, ha il vantaggio di mantenere ad un livello minimo la complessità del protocollo IGP. Questo infatti ha il compito di propagare internamente i soli prefissi IP che vengono utilizzati per il piano di

numerazione interno della rete (interfacce di *Loopback*, collegamenti *punto-punto* e *Broadcast*), con evidenti benefici in termini di consumo di memoria e soprattutto di maggiore velocità di convergenza. Una regola aurea da seguire, quando si progetta l'implementazione del protocollo IGP, è che questo, per ragioni di sicurezza, debba essere completamente isolato dall'esterno, ossia, non deve avere alcuna interazione con protocolli di routing esterni all'AS. Per questa ragione è buona norma cambiare, via configurazione, la gestione di *default* dell'attributo NEXT_HOP, da parte del BGP.

### 1.2.2 Riduzione del numero di sessioni iBGP

Il punto debole del modello di routing basato su un protocollo IGP e sul BGP, come abbiamo già detto, è l'elevato numero di sessioni iBGP necessarie. A livello di protocollo BGP, esistono due tecniche che permettono di risolvere il problema:

- Utilizzare il concetto di *Route Reflection*.
- Utilizzare una *Confederazione BGP*.

I grandi ISP preferiscono utilizzare la prima soluzione, anche se questa comporta l'aggiunta alla rete di ulteriori router (o anche *server* dedicati), i *Route Reflector* (RR). In realtà, le funzioni di *Route Reflection* potrebbero essere svolte anche da alcuni router della rete, ma per evitare sovraccarichi della CPU, si preferisce utilizzare router o server dedicati.

Il risparmio di sessioni iBGP utilizzando i RR è elevatissimo. Riprendendo l'esempio visto nell'introduzione a questo Paragrafo, e ipotizzando per affidabilità, due sessioni iBGP verso due diversi RR per ciascun router *P* o *PE*, le sessioni iBGP necessarie diventano 2x272 = 544, più poche decine di sessioni tra i RR (il numero esatto dipende da quanti sono i RR installati), contro le 34.300 richieste senza RR.

**NOTA**: il lettore interessato ad approfondire i concetti di *Route Reflection* o più in generale del protocollo BGP, può consultare il libro "T. Tofoni, *BGP*: *dalla teoria alla pratica*, Ed. Reiss Romoli, Maggio 2011".

### 1.2.3 Architettura di routing BGP/MPLS

Una ulteriore riduzione del numero di sessioni iBGP si può ottenere attraverso l'introduzione in rete dello standard MPLS. Anche se ancora non abbiamo introdotto alcunché di MPLS, per capire ciò che andremo qui a dire, è sufficiente illustrare una delle proprietà fondamentali di MPLS, che sarà ampiamente sviluppata nel Capitolo 3. MPLS è una tecnologia del piano dati che utilizza il ben noto concetto di commutazione di etichetta (*label switching*), ossia la commutazione, al pari dei vecchi e ormai desueti standard *Frame Relay* e *ATM*, avviene utilizzando una etichetta (ossia, un semplice numeretto) presente da qualche parte nell'intestazione del pacchetto. Il router che esegue la commutazione avrà quindi una "Tabella di *forwarding* MPLS", che a ciascuna etichetta in ingresso, fa corrispondere una etichetta uscente e un *IP Next-Hop*. L'architettura di routing risultante viene denominata BGP/MPLS.

L'idea di fondo si basa sull'osservazione che il ruolo dei router *P* è quello di fare solamente da transito per il traffico tra due *PE*, uno d'ingresso e uno di uscita del traffico. Infatti, un esame critico della situazione descritta nelle Figure 1.2 e 1.3, consente di dedurre che il lavoro che i router *P* effettivamente svolgono, è quello di trasferire pacchetti da un router *PE* d'ingresso ad un router *PE* di uscita. Perché allora propagare tutti i prefissi esterni all'AS anche nelle Tabelle di Routing IP dei router *P*? Esiste qualche modo di eliminare questa conoscenza superflua, alleviando così il lavoro fatto

da questi router (che poi sono quelli che dovrebbero dedicare la maggior parte della loro potenza elaborativa allo smaltimento del traffico)?

In effetti, il problema potrebbe essere risolto mettendo in piedi dei *tunnel* che colleghino tra loro i router *PE* ingresso/uscita, mascherando ai router *P* gli indirizzi IP destinazione dei pacchetti IP. Questi *tunnel* potrebbero essere realizzati, ad esempio, da percorsi MPLS, ossia percorsi dove il traffico viene commutato sulla base di una etichetta e non sulla base dell'indirizzo IP destinazione.

La Figura 1.4 seguente descrive l'idea di fondo. I prefissi esterni, appresi da un *PE* attraverso un qualsiasi protocollo di routing (sia esso statico o dinamico), e redistribuiti nel processo BGP, vengono propagati ai soli altri router *PE*, e non ai router *P*. Quindi, alla fine saranno solo i router *PE* quelli che avranno nella loro RIB tutti i prefissi esterni; il collegamento tra i router *PE* è assicurato da una maglia completa di percorsi MPLS, che hanno quindi lo scopo di "congiungere" logicamente i router *PE*.

L'architettura di routing BGP/MPLS riduce ulteriormente il numero delle sessioni iBGP da configurare; infatti, non sono più necessarie le sessioni iBGP tra i router *PE* e i router *P* (che sono in numero di *NPE*NP*, dove *NPE* è il numero dei router *PE* e *NP* il numero dei router *P*). Inoltre, in aggiunta al vantaggio dell'ulteriore riduzione delle sessioni iBGP, ha innegabili vantaggi in termini di scalabilità in quanto nei router *P*:

- Non è più necessario propagare via BGP i prefissi esterni. In realtà, nei router *P* non è più necessario attivare un processo BGP.
- Si velocizza la ricerca del *Next-Hop*, essendo l'inoltro dei pacchetti basato sulle etichette MPLS, ed essendo queste in numero limitato (una per ciascun *PE*, in una configurazione ottimale!).
- Si risparmia memoria, poiché non è necessario memorizzare grandi quantità di annunci BGP.

Il punto chiave che consente all'architettura BGP/MPLS di inoltrare comunque il traffico, senza dover propagare gli annunci dei prefissi esterni ai router *P*, è che i router *P* effettuano la commutazione del pacchetto non sulla base dell'indirizzo IP destinazione, ma sulla base di una etichetta MPLS, corrispondente al percorso MPLS che collega il router *PE* che riceve il pacchetto dall'esterno (*PE* di ingresso, nella figura PE[*i*]), al router *PE* che inoltra il pacchetto al di fuori della rete dell'ISP (PE di uscita, nella figura PE[*u*]). Ulteriori dettagli dell'architettura di routing BGP/MPLS saranno trattati nel Paragrafo 4.4.

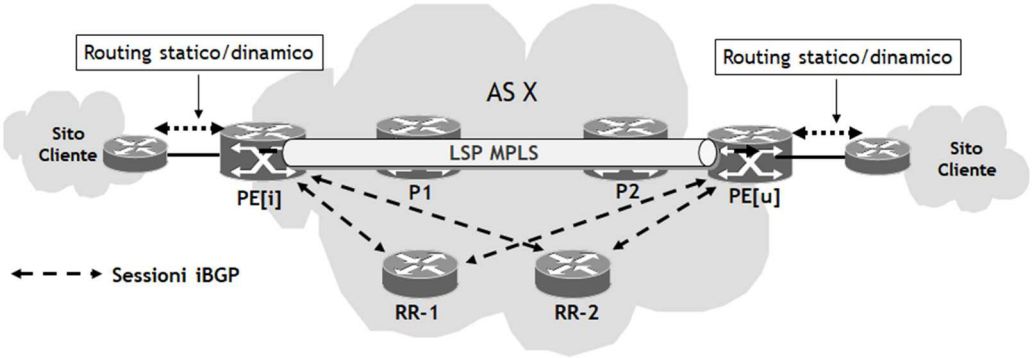


**Figura 1.4** - Schema logico dell'architettura di routing BGP/MPLS.

### 1.2.4 *Best-practice* di configurazione

La configurazione di una rete che voglia utilizzare l'architettura di routing BGP/MPLS, richiede l'attivazione di tre componenti fondamentali:

- Un protocollo di routing IGP. Nelle applicazioni pratiche si utilizzano protocolli di tipo *Link State* (OSPF o IS-IS).
- Il protocollo BGP. In particolare, è necessaria una maglia completa di sessioni iBGP tra tutti i router *PE*. La maglia completa può essere realizzata, per maggiore scalabilità, mediante *Route Reflector* oppure *Confederazioni BGP*.
- Il meccanismo di *forwarding* MPLS. In particolare è necessario realizzare una maglia completa di percorsi MPLS tra tutti i router *PE*.

Le linee guida, per una elegante ed efficiente implementazione pratica di una architettura di routing BGP/MPLS, sono le seguenti:

- Configurare, su ciascun router *P*, *PE*, ed eventuali RR, delle interfacce di *Loopback*, che indicheremo brevemente con *Lo0*.
- Attivare un protocollo IGP interno (OSPF o IS-IS), che permetta la raggiungibilità reciproca di tutte le interfacce *Lo0*. In particolare, nel caso si utilizzino, per maggiore scalabilità, dei RR, è importante che vi sia connettività IP tra le interfacce *Lo0* di ciascun router PE e le interfacce *Lo0* dei RR.
- Su ciascun router *PE*, configurare almeno una sessione iBGP verso un RR (Nota: nella pratica, è bene che vi siano, per motivi di affidabilità, almeno due sessioni iBGP verso due diversi RR). In funzione dei servizi offerti, è possibile attivare sessioni iBGP di tipo multiprotocollo (MP-iBGP), indispensabili ad esempio per servizi quali *L2VPN* e *L3VPN*.
- Realizzare una maglia completa di percorsi MPLS tra tutti i router *PE*, o attivando il protocollo *LDP* (vedi Paragrafo 4.2) su tutti i router *P* e *PE* (soluzione tipicamente consigliata), oppure attraverso la configurazione manuale di percorsi MPLS espliciti tra ogni coppia di *PE* (Nota: poiché i percorsi MPLS sono unidirezionali, questo comporterebbe la configurazione di *NPE**(*NPE*-1) percorsi MPLS espliciti). La seconda soluzione, oltre a comportare una configurazione molto lunga, ha il difetto che l'aggiunta di un nuovo *PE*, comporta la configurazione di *NPE*-1 nuovi percorsi espliciti.

Una rete così configurata può essere utilizzata, con aggiunte minori, per importanti servizi come ad esempio le Reti Private Virtuali IP BGP/MPLS, l'accesso ad Internet, il trasporto di trame di Livello 2 (ad esempio trame *PPP*, *Ethernet*, ecc.), l'emulazione di *LAN Ethernet*, il trasporto di pacchetti IPv6 su reti IPv4/MPLS, ecc.

## 1.3 L'EVOLUZIONE VERSO LE RETI IP/MPLS: CENNI STORICI

La crescita esponenziale del traffico Internet, iniziata nella metà degli anni '90, ha aperto la strada ad una innovazione tecnologica senza precedenti delle reti IP. Queste sono di fatto diventate il mezzo "universale" su cui far transitare diversi tipi di traffico, essenzialmente voce, video e dati, permettendo di realizzare il vecchio sogno dei gestori di reti di telecomunicazione: trasportare qualsiasi tipo di traffico su una sola piattaforma.

Tra i tentativi più importanti di integrazione del trasporto del traffico ricordiamo lo standard ATM (*Asynchronous Transfer Mode*), sviluppato tra la fine degli anni '80 e inizi anni '90 e che, secondo le

intenzioni iniziali, sarebbe dovuto diventare la tecnologia "universale" delle reti di telecomunicazione. ATM è uno standard sicuramente sofisticato, con caratteristiche molto interessanti, tra cui:

- Elevata velocità di commutazione.
- Possibilità di differenziare la Qualità del Servizio.
- Meccanismi di controllo e gestione del traffico molto efficienti.

Proprio queste caratteristiche si sono rivelate però il suo tallone di Achille. Infatti, la realizzazione pratica delle funzionalità appena citate ha reso lo standard molto complesso, e quindi di difficile utilizzo nelle applicazioni pratiche.

L'introduzione, a partire dai primi anni '90, di nuove applicazioni (es. il servizio WWW) basate su una piattaforma semplice e standardizzata come l'architettura protocollare TCP/IP e la loro vasta accettazione da parte del mercato, ha di fatto cambiato lo scenario tecnologico spostando l'attenzione, sia da parte dei costruttori di apparati, sia da parte dei gestori delle reti, all'ottimizzazione delle reti IP. Si è passati così da un mercato *technology driven* a nuove tecnologie *market driven*.

Tutto questo ha avuto importanti riflessi nell'evoluzione delle tecnologie dei *backbone* IP, basate fino ad allora su standard certamente non adatti al nuovo scenario. Tra i punti deboli delle reti IP tradizionali ricordiamo:

- *Impossibilità di differenziare la Qualità del Servizio offerta*: le reti IP offrono una sola classe di servizio, convenzionalmente chiamata *Best-Effort*, dove non viene offerta alle applicazioni alcuna garanzia di Qualità del Servizio. Se ciò potrebbe non essere importante per applicazioni tipo *e-mail* o *World Wide Web*, la stessa cosa non si può dire per il traffico *real-time* (es. voce e video) dove sono necessari requisiti stringenti in termini di perdita dei pacchetti, ritardo massimo *end-to-end*, variabilità del ritardo (*jitter*).
- *Impossibilità di ingegnerizzare il traffico sulla rete*: nelle reti IP il traffico viene instradato secondo algoritmi di ricerca del cammino a costo minimo, basati su determinate metriche associate ai collegamenti. Questi algoritmi sono basati su una visione topologica della rete e non sul traffico che effettivamente scorre sui collegamenti costituenti i cammini. Ciò potrebbe portare a situazioni in cui alcuni percorsi sulla rete sono fortemente congestionati (a causa del forte traffico su uno o più collegamenti) mentre altri sono scarsamente utilizzati, creando di fatto un utilizzo non ottimo della rete.
- *Scarsa scalabilità nell'offerta dei servizi*: servizi come le Reti Private Virtuali basate su piattaforma IP creano seri problemi di gestione qualora vengano offerti a migliaia di Clienti ciascuno dei quali con diverse centinaia di siti da collegare.

A partire dalla metà degli anni '90 c'è stato un forte impulso a migliorare le reti IP cercando di renderle più veloci, scalabili e sicure. Il primo tentativo verso questa direzione è stato quello di utilizzare la migliore tecnologia di rete a quel momento disponibile, ossia ATM. L'integrazione IP/ATM, nella sua versione originale del modello *overlay* , benché sia stata un salto tecnologico notevole in termini di prestazioni della rete, ha però ben presto rivelato dei limiti che ne hanno bloccato lo sviluppo.

**NOTA**: il modello *overlay* utilizza il modello *IP classico su ATM* specificato nella RFC 1483. In particolare, viene utilizzata la versione con Connessioni Virtuali Permanenti (PVC, *Permanent Virtual Connection*). Nell'applicazione tipica, i router comunicano tra di loro attraverso un insieme di PVC ATM, che quindi funzionano come circuiti logici che garantiscono la connettività tra i router della rete IP. I router non conoscono la topologia fisica della rete ATM, hanno conoscenza soltanto dei PVC, che

appaiono quindi a loro come semplici collegamenti virtuali punto-punto. Viene attivato su ciascun PVC un protocollo di routing in modo che i router possano stabilire delle "adiacenze" e scambiarsi le informazioni di routing.

Si è passati così ad un modello diverso di integrazione IP/ATM, il modello *integrato*, che ha permesso di eliminare alcuni difetti del modello *overlay*, ma non alcuni problemi intrinseci del trasporto di IP su ATM. I principali costruttori mondiali hanno sviluppato, a partire dalla metà degli anni '90, interessanti soluzioni proprietarie basate sul concetto di modello integrato, soluzioni però non interoperabili essendo per l'appunto proprietarie. Tutte queste soluzioni avevano un denominatore comune: l'utilizzo di ATM come tecnologia di trasporto.

**NOTA**: l'idea alla base del modello integrato è la riduzione del numero delle adiacenze che il protocollo di routing IP deve mantenere. Per raggiungere questo scopo, l'idea è quella di far si che anche gli *switch* ATM diventino, dal punto di vista dell'instradamento, dei router IP. Ciò comporta che la rete risultante sia una semplice rete IP in cui però i pacchetti IP vengono trasportati sotto forma di celle ATM su collegamenti virtuali che seguono un percorso che però è determinato da un protocollo di routing IP (es. OSPF, IS-IS), o da altre tecniche.

La validità del modello integrato fu subito riconosciuta dalla comunità IP. In particolare Cisco, nel 1997, annunciò l'intenzione di standardizzare la sua tecnologia proprietaria *Tag Switching* già implementata nei suoi router. Lo scopo era di eliminare gli svantaggi residui del modello integrato e definire un nuovo standard basato in massima parte sulla tecnologia *Tag Switching*. Fu così costituito in ambito IETF, (*Internet Engineering Task Force*, è l'organismo di standardizzazione "tecnica" delle reti IP) agli inizi del 1997, un gruppo di lavoro ad hoc con l'obiettivo di armonizzare ed integrare le varie soluzioni proprietarie di modello integrato in modo da produrre uno standard *multivendor*, che potesse essere impiegato su qualsiasi tecnologia di trasporto.

Il gruppo di lavoro, riunitosi per la prima volta nell'Aprile 1997, decise di chiamare la nuova tecnologia da sviluppare *Multi Protocol Label Switching (*MPLS*)*. Il processo di standardizzazione, nella sua parte più importante, si è concluso agli inizi del 2001 e ha permesso la definizione di una tecnica in grado di soddisfare tutti gli obiettivi preposti, con in più il vantaggio di essere molto generale, aperta a futuri sviluppi e di applicabilità molto ampia.

### 1.3.1 Dal modello integrato a MPLS

L'idea di MPLS parte dal modello integrato IP/ATM e cerca di risolverne i problemi più evidenti. L'obiettivo dell'intero processo di standardizzazione è stato di sviluppare uno standard in grado di:

- Recepire le idee alla base del modello integrato.
- Funzionare con differenti tecnologie di livello 2 (quindi, non solo ATM).
- Far evolvere il routing IP verso nuove funzionalità, come ad esempio la possibilità di ingegnerizzare il traffico.
- Rendere le reti IP più scalabili, ossia in grado di smaltire traffici di grandi dimensioni e di offrire servizi avanzati a un parco clienti vasto e differenziato.
- Supportare i modelli di Qualità del Servizio sviluppati in ambito IETF.

Riportiamo testualmente dal documento IETF *draft-ietf-mpls-framework*:

**"The primary goal of the MPLS working group is to standardise a base technology that integrates the label swapping forwarding paradigm with network layer routing. This base technology (label swapping) is expected to improve the price/performance of network layer routing, improve the scalability of the network layer, and provide greater flexibility in the delivery of (new) routing services (by allowing new routing services to be added without a change to the forwarding paradigm)"**

L'idea alla base di MPLS è quella di introdurre nelle reti IP il concetto di commutazione di etichetta tipico delle reti a commutazione di pacchetto *connection-oriented*, come nei vecchi standard X.25, *Frame Relay*, ATM, e quindi di inserire in un mondo *connection-less*, come quello IP, il concetto di connessione virtuale. Ciò avviene associando a tutti i pacchetti un breve identificativo di lunghezza fissa, l'etichetta (*label*), che gli apparati di rete possono utilizzare per effettuare un instradamento veloce. È bene sgombrare il campo subito da un possibile equivoco: *MPLS non è un nuovo protocollo di routing, ma solo una nuova tecnica di commutazione (forwarding) dei pacchetti IP*.

Al pari del modello integrato, MPLS richiede l'introduzione in rete di un nuovo *protocollo per la distribuzione delle etichette* da associare a un percorso, che nelle reti MPLS può essere quello definito dal protocollo di routing IP oppure un percorso *esplicito* diverso da questo.

Uno dei molti punti di forza di MPLS è legato alla sua flessibilità, poiché non legato ad una particolare tecnologia di trasporto (a differenza ad esempio del modello integrato, basato sul solo trasporto ATM). Inoltre, MPLS è anche molto generale per quanto riguarda il "contenuto" del trasporto, poiché in grado di trasportare qualsiasi cosa, sia esso un pacchetto di livello 3 (IPv4, IPv6, IPX, ecc.) o una trama di livello 2 (PPP, Ethernet, Frame Relay, ATM, ecc.). In un certo senso si può affermare che MPLS è totalmente "ignaro" su ciò che trasporta. Tutto questo spiega la parte *Multi Protocol* dell'acronimo MPLS.

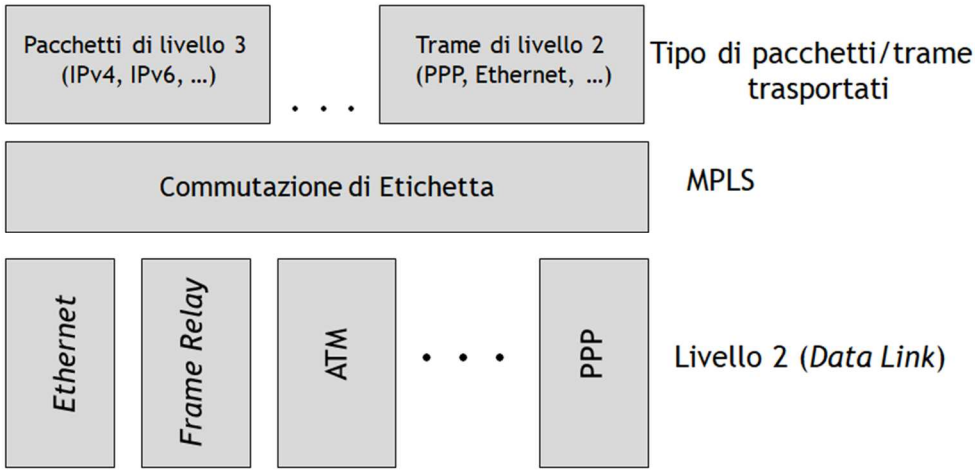


**Figura 1.5** - Perché MPLS è *Multi Protocol*.

**NOTA**: per chi è abituato a pensare in termini di architetture di comunicazione, sorge spontanea la domanda di identificare a quale livello del modello a strati ISO/OSI si colloca MPLS. Osserviamo innanzitutto che MPLS non può collocarsi a Livello 2 poiché è indipendente dal protocollo di Livello 2

utilizzato (vedi Figura 1.5). Non è d'altra parte nemmeno collocabile a Livello 3 in quanto mancano a MPLS le funzionalità di routing e indirizzamento che il modello ISO/OSI assegna a questo livello. MPLS viola anche altre caratteristiche del modello ISO/OSI sulle quali non ci soffermiamo. Allora, quale è la risposta alla domanda iniziale? La verità è che MPLS non è classificabile in alcun livello del modello di riferimento ISO/OSI. Il modello ISO/OSI è appunto un modello di "riferimento"; il fatto che MPLS abbia guadagnato un così vasto consenso suggerisce che a volte può esistere un modello "reale" che non è schematizzabile tramite un modello teorico di "riferimento".

## 1.4 MPLS TRA MITI E REALTÀ

Ci sono alcuni miti riguardo il ruolo di MPLS nei backbone IP, che è bene sfatare subito.

**1° mito:** MPLS è stato sviluppato per trasformare *switch* ATM in router ad alte prestazioni.

Sebbene questo sia stato uno degli obiettivi originari delle soluzioni proprietarie nella metà degli anni '90, i progressi nella tecnologia del silicio consentono di effettuare (attraverso ASIC dedicati) una lettura della FIB a velocità comparabile a quella su una tabella di instradamento ATM.

**2° mito:** MPLS è stato progettato per eliminare completamente la necessità del routing IP convenzionale.

Ciò non è esattamente vero in quanto l'analisi di un pacchetto a Livello 3 (e Livelli superiori) è fondamentale ad esempio per la sicurezza. Inoltre, MPLS non viene implementato, a meno di casi molto particolari, nel dominio dei "clienti"; quindi i pacchetti IP provenienti da un router esterno al dominio MPLS devono essere elaborati a Livello 3 (almeno) dal primo router. Infine, l'ultimo router del dominio MPLS dovrà necessariamente esaminare il pacchetto a Livello 3.

**3° mito:** MPLS è stato progettato per fornire Qualità del Servizio alle reti IP.

Questo non è assolutamente vero. MPLS supporta il modello *Differentiated Services* per la Qualità del Servizio nelle reti IP, ma di suo non introduce alcuna nuova funzionalità di QoS.

Per contro, MPLS ha indubbi vantaggi rispetto al routing convenzionale. Tra questi, quello principale è che consente a un ISP di offrire nuovi servizi che non possono essere supportati semplicemente attraverso le tecniche convenzionali. Di questi servizi si parlerà ampiamente nel resto del libro.

## SOMMARIO

La crescita esponenziale del traffico Internet ha determinato un forte impulso per il miglioramento delle reti IP. Le tecnologie di *backbone* sono evolute passando dapprima per l'integrazione IP/ATM, e quindi per il nuovo paradigma MPLS.

L'integrazione IP/ATM si è basata nella metà degli anni '90 sul modello *overlay*. Questo si è però ben presto dimostrato insufficiente in termini di scalabilità e supporto dei servizi. Si è passati così al nuovo modello integrato, che ha permesso di risolvere alcuni dei problemi insiti nel trasporto di IP su ATM, restando comunque sempre legato al trasporto ATM e a tutti gli svantaggi che ciò comportava in termini di spreco di banda trasmissiva e scalabilità. Questo, insieme al fatto che i costruttori che hanno adottato questo modello hanno prodotto macchine non interoperabili, ha dato il via al processo di standardizzazione del nuovo paradigma MPLS.

MPLS recepisce le idee chiave del modello integrato IP/ATM, estendendone l'utilizzo sia nel trasporto del tipo di contenuto (non solo IP), che nell'utilizzo del livello 2 (non solo ATM). Inoltre, consente di realizzare in rete in modo scalabile, servizi molto importanti (vedi prossimo Capitolo 2).

## Cosa è importante ricordare:

1. L'architettura di routing di una rete ISP
2. Il ruolo dei protocolli IGP e del protocollo BGP
3. L'architettura di routing BGP/MPLS e il ruolo di MPLS