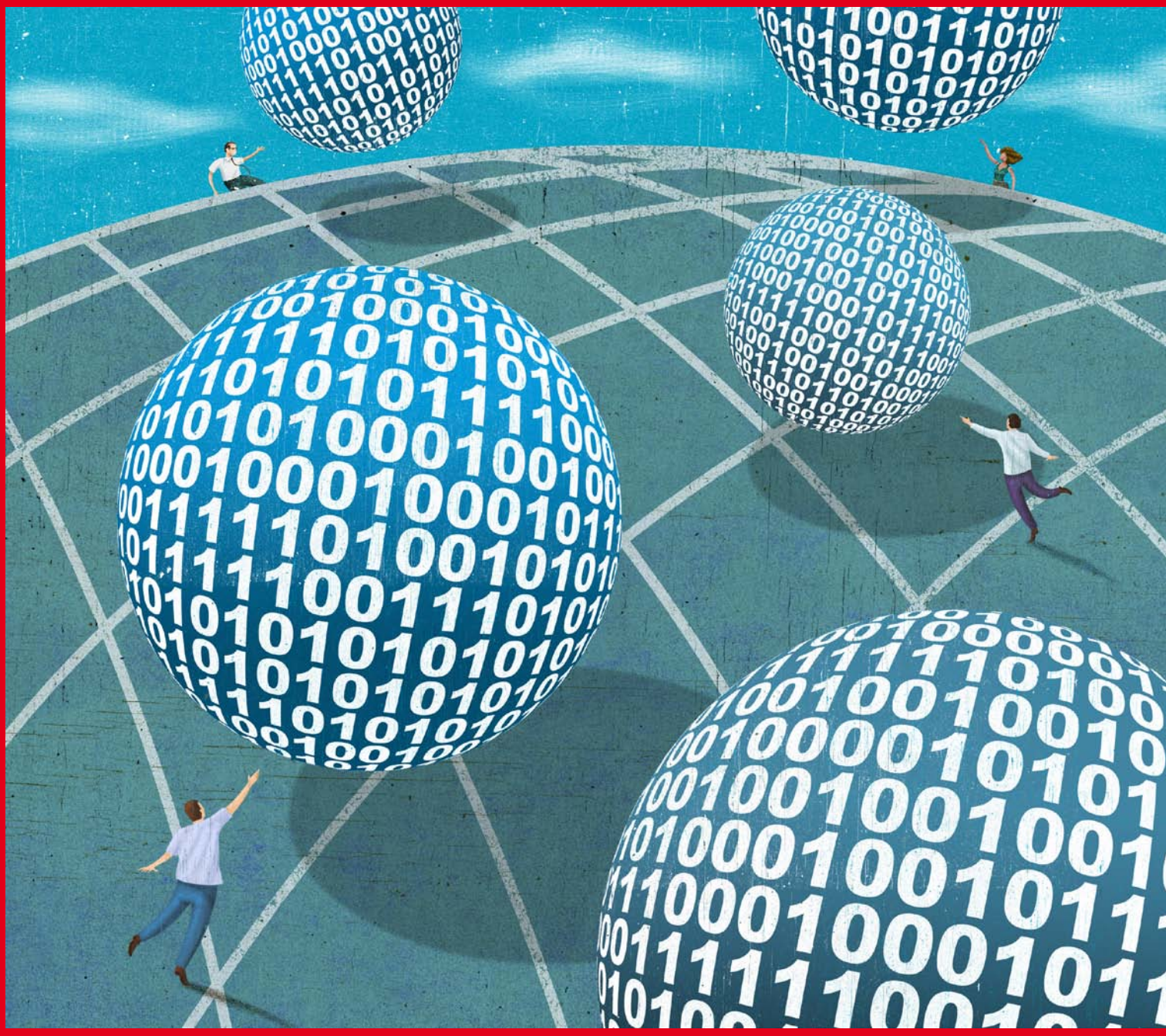
RETE DATI FISSA DI TELECOM ITALIA

Paolo Fasano, Domenico Marocco, Giovanni Picciano



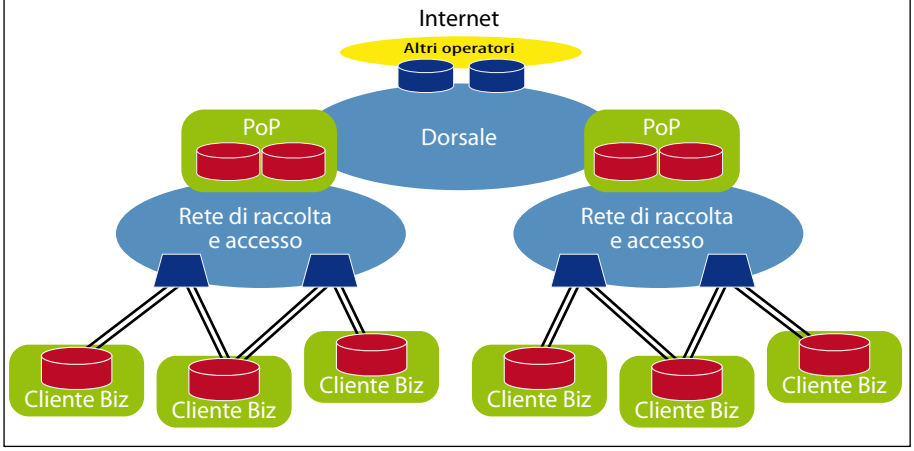
La rete dati fissa di Telecom Italia si è sviluppata nel corso dell'ultimo ventennio. Partita inizialmente come rete dedicata per servizi di nicchia, è ora divenuta la piattaforma di rete su cui si prevede la convergenza di tutte le tipologie di offerte di servizio.
Questo articolo descrive la rete dati fissa di Telecom Italia con particolare attenzione a quella parte di rete denominata Edge IP, in cui sono presenti gli apparati che mantengono configurazioni specifiche per i singoli clienti e interagiscono in maniera privilegiata con le piattaforme di Controllo dei servizi di rete.

1 Introduzione

Telecom Italia dispone di una rete a pacchetto rappresentata schematicamente in Figura 1. In prima approssimazione essa si compone di 4 segmenti:

- La *dorsale* o *Backbone* fornisce connettività in forma aggregata a livello nazionale tra i PoP (*Point of Presence*) della rete IP. La principale rete dorsale di Telecom Italia denominata OPB (*Optical Packet Backbone*) è realizzata in tecnologia IP/MPLS direttamente su un'infrastruttura fotonica. Essa è inoltre collegata ad altri operatori per realizzare i collegamenti alla rete Internet su scala globale.
- La *rete di accesso e raccolta* è costituita dai nodi di accesso (principalmente DSLAM), situati nella maggior parte delle centrali Telecom Italia per terminare lato rete le linee cliente, e nodi di aggregazione e trasporto che realizzano il collegamento tra i nodi di accesso e i PoP. La prima tecnologia utilizzata in questo segmento è stata la tecnologia ATM (*Asynchronous Transfer Mode*). Più recentemente è stata sviluppata una rete in tecnologia Carrier Ethernet IP/MPLS (*Multi-Protocol Label Switching*) denominata OPM (*Optical Packet Metro*)[1], che oggi costituisce lo stato dell'arte per le reti di aggregazione Metro-Regionali. La rete poggia su un infrastruttura di trasporto ottica e SDH (*Synchronous Digital Hierarchy*) anch'essa in evoluzione.
- La *terminazione in sede cliente* che può essere controllata da parte di Telecom Italia; in questo caso il servizio include anche le funzioni realizzabili su tale apparato.
- La *corona di Edge IP* costituita da un insieme di nodi collocati nei PoP su cui sono concentrate le funzioni di rete necessarie per servire ciascun singolo cliente. In particolare tali nodi

Figura 1 - Schema della rete dati



mantengono uno stato specifico per ogni cliente che lo caratterizza in termini di tipo di connettività richiesta, prestazioni, etc.

In questo articolo viene dapprima descritta la modalità realizzativa dei servizi dati oggi a portafoglio per clienti business e clienti residenziali. Si presentano poi gli enti di standardizzazione in cui sono sviluppate le soluzioni architetturali e di protocollo per i servizi di rete fissa. Nella seconda parte di questo lavoro si apre lo sguardo alle innovazioni che si presentano all'orizzonte: prima da un punto di vista tecnologico, si analizzano i trend evolutivi per gli apparati impiegati in questo segmento, e infine da un punto di vista di architetture di rete si guarda al modello denominato *Seamless MPLS* come ad una promettente direzione di sviluppo.

2 I Servizi Dati

2.1 Clienti Business

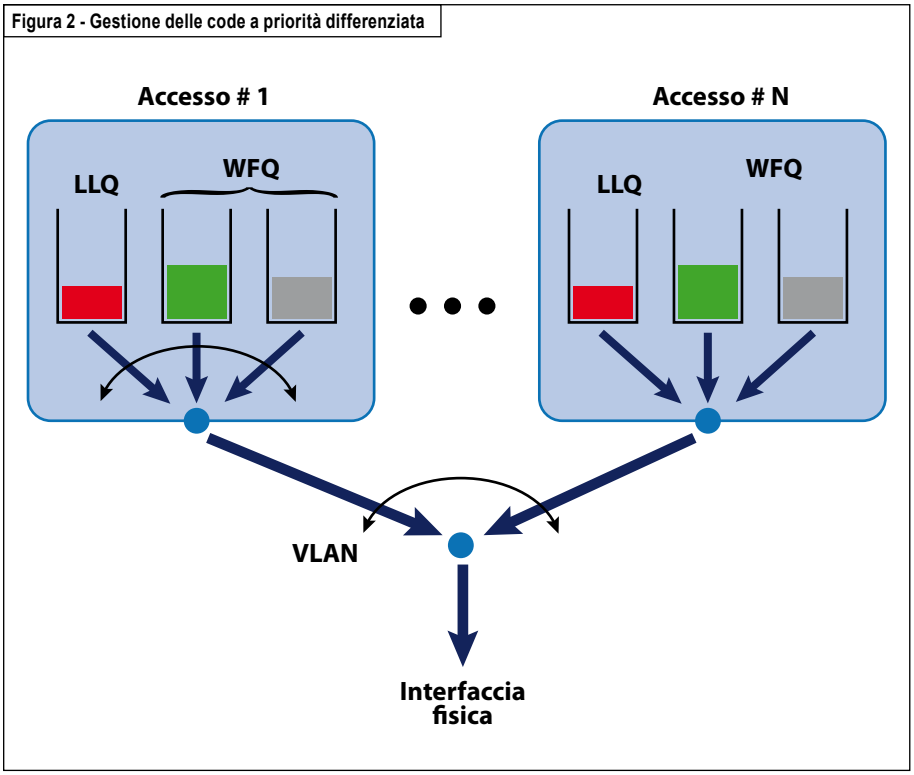
I clienti affari di fascia media e alta vengono serviti mediante una piattaforma di Edge dedicata. Ciò consente di realizzare funzioni e prestazioni adatte a questa fascia di clientela, quali VPN (*Virtal Private Network*), garanzia di banda, differenziazione su base classe QoS (*Quality of Services*) e accessi con protezione in ridondanza.

L'elemento di rete su cui si concentrano le funzioni necessarie a servire tali clienti è un router IP denominato PE (*Provider Edge*). Tale elemento è inserito nella rete IP/MPLS di Telecom Italia, ed in particolare sfrutta la connettività realizzata dalla dorsale per offrire servizi dati nazionali e internazionali. L'impiego di MPLS è di particolare rilevanza, perché fornisce uno strato protocollare con cui i PE possono incapsulare il traffico cliente. In questo modo è possibile fornire servizi di VPN IP, consentendo ai clienti multi-sede (tipicamente grandi aziende) una piena autonomia nell'indirizzamento, oltre che un ambiente chiuso e protetto. MPLS consente inoltre ai PE di trasportare protocolli diversi da IPv4 (l'unico di livello 3 direttamente trattato dalla dorsale). È possibile fornire una connettività Ethernet mediante il servizio VPLS (*Virtual Private LAN service*), con cui si realizza una VPN di livello 2. Un altro esempio in questo senso è la realizzazione di servizi IPv6 (un'evoluzione del protocollo IPv4, quello su cui è stata costruita Internet, che consente di superarne i limiti sull'indirizzamento). La soluzione così realizzata consente di limitare l'aggiornamento ai nodi di Edge (e solo a quelli interessati) e ai nodi di collegamento alla Internet IPv6. Analogamente è possibile un servizio di VPN IPv6.

Verso l'accesso il PE sfrutta un servizio di connettività punto-punto realizzato dalla rete di aggregazione e accesso: nel caso di OPM tale collegamento è ottenuto mediante VLAN (*Virtual Local area Network*) Ethernet.

La gestione della banda operata sui PE consente di modulare le risorse allocate per ciascun cliente e di offrire diverse classi di servizio. Tale meccanismo è attivato sulle porte di collegamento del PE verso OPM, che diventano quindi il punto di controllo della banda e della qualità di servizio. La Figura 2 mostra il modello di QoS operato da tali apparati, che avviene mediante una gestione multilivello della capacità trasmissiva contesa tra clienti diversi e classi di servizio (meccanismo chiamato Hierarchical QoS, HQoS).

Figura 2 - Gestione delle code a priorità differenziata



IPv6 LaunchDay

L'ISOC (Internet Society), l'ente la cui missione è promuovere lo sviluppo aperto, l'evoluzione e l'uso di Internet a beneficio di chiunque nel mondo, sta monitorando da tempo e con apprensione lo sviluppo della rete Internet. Con il sempre crescente consumo di indirizzi IPv4, la preoccupazione sale. Come poter continuare a garantire lo sviluppo costante della Rete? Ogni computer connesso alla rete viene identificato con un indirizzo numerico, che può essere statico (sempre lo stesso) oppure dinamico (quando ci si connette, ce ne viene dato uno temporaneo). Il default in questi decenni è dato dal protocollo IPv4 (IP versione 4): un indirizzo è formato da quattro byte, 32 bit, scrivibili come stringa di 8 caratteri esadecimali (ma più spesso rappresentati come sequenza di 4 interi da 0 a 255 ciascuno) e permetterebbe in teoria di avere quattro miliardi di indirizzi diversi, anche se in pratica se ne possono usare molti meno dato che gli indirizzi sono assegnati a gruppi. Purtroppo ormai non ci sono più indirizzi IPv4 di scorta: una soluzione è necessaria nel più breve tempo possibile.

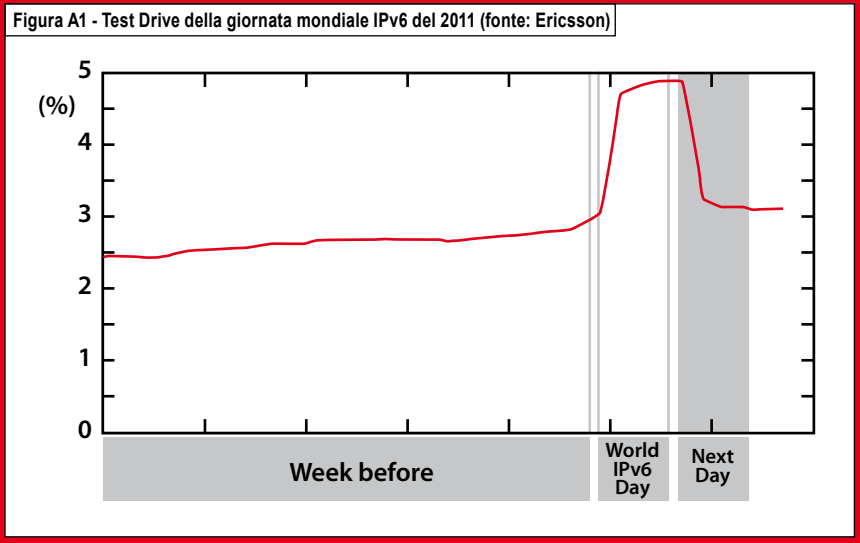
La soluzione identificata è quella che prevede il passaggio al protocollo IPv6. IPv6 ha a disposizione uno spazio di indirizzamento infinitamente più elevato di quello IPv4, si passa infatti da 32 bit a 128 bit: da poco più di 4 miliardi a circa $3{,}4 \times 10^{38}$ indirizzi!

Nonostante i molti anni di vita di questo protocollo (è stato introdotto a livello di standard internazionale già alla fine degli anni '90), la sua diffusione è tuttora molto ridotta, sia presso i Service Provider sia tra i Content Provider, anche perché non è compatibile con l'attuale IPv4. Tuttavia recentemente l'esaurimento degli indirizzi IPv4 è diventato una minaccia concreta, e IPv6 è prepotentemente diventato di attualità.

Lo scorso anno ISOC ha promosso una giornata dedicata all'IPv6: l'*IPv6 World Day*, che si è svolto l'8 Giugno 2011. In tale occasione Service Provider e Content Provider hanno utilizzato IPv6 per la connettività e la navigazione, realizzando un trial planetario della durata di ventiquattro ore.

I risultati sono stati sostanzialmente positivi: il traffico IPv6 in rete è cresciuto per poi riabbassarsi la giornata successiva, ma attestandosi a valori più elevati rispetto al trend rilevato fino al 5 Giugno, come indicato nella Figura A1.

Figura A1 - Test Drive della giornata mondiale IPv6 del 2011 (fonte: Ericsson)



Visti i buoni risultati (non sono stati rilevati disservizi particolari durante la giornata e la partecipazione è stata soddisfacente: Google, Yahoo, Facebook erano raggiungibili in IPv6), ISOC ha deciso di promuovere una nuova giornata per il 6 giugno 2012: *IPv6 LaunchDay* (*www.worldipv6launch.org*). "Questa volta è per davvero", recita il sottotitolo dell'evento. Infatti, l'obiettivo di questa giornata è quello di dare il via all'utilizzo continuativo di IPv6, lasciandolo attivo e offerto ai clienti come opzione reale per la connettività ad Internet.

Sono molte le adesioni all'evento, specie tra gli operatori americani (AT&T, Comcast e Time Warner Cable e molte università). In Italia aderisce il GARR (il consorzio che gestisce la rete dell'università e della ricerca). Anche i Content Provider ci sono quasi tutti: Google, Yahoo, Facebook, Netflix e tanti altri, per un totale di più di mille siti aderenti all'iniziativa.

L'IPV6 Day per Telecom Italia

Telecom Italia ha seguito fin dall'inizio la nascita e la crescita di IPv6. Traendo spunto dall'evento del 6 Giugno 2012, Telecom Italia ha predisposto una soluzione tecnica che consente a un qualsiasi cliente residenziale di poter sperimentare la connettività IPv6. Tra le varie soluzioni possibili, se ne è scelta una che privilegia la velocità di dispiegamento in campo e la possibilità di essere utilizzata da tutti gli utenti, indipendentemente dall'area geografica e dalla tipologia di attestazione alla rete (mediante DSLAM Ethernet e/o ATM).

Lo schema della rete è riportato nella Figura A2.

Nello specifico sono stati configurati due BNAS (*Broadband Network Access Server*) centralizzati con funzione LNS

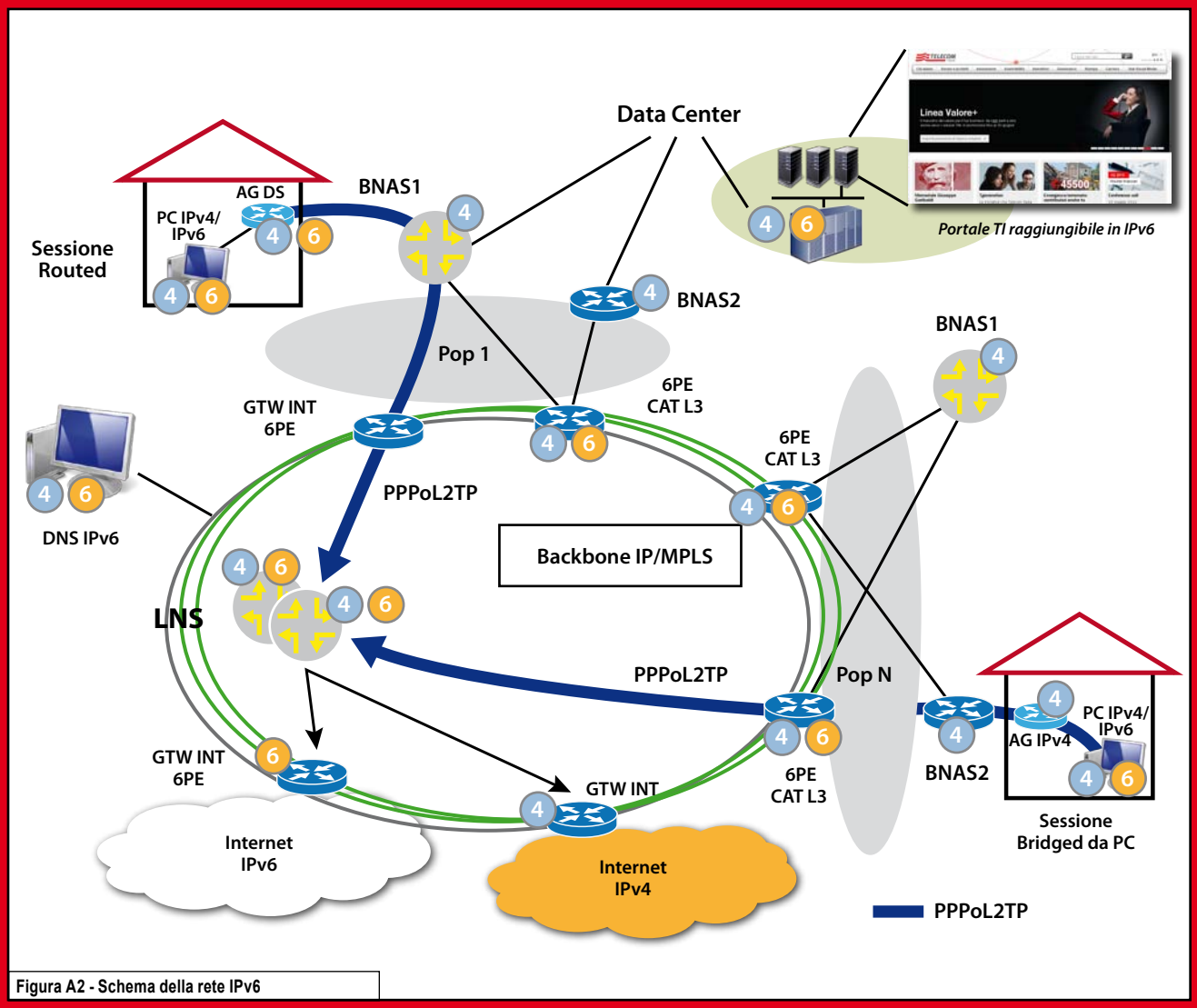


Figura A2 - Schema della rete IPv6

(*L2TP Network Server*) all'interno di due PoP di Telecom Italia, che sono in grado di gestire in contemporanea sia traffico IPv4 sia traffico IPv6. Il cliente che vuole utilizzare IPv6 può farlo in modalità *Routed* o in modalità *Bridged*. Per poter attivare una sessione *Routed* IPv4 e IPv6, deve disporre di un AG (*Access Gateway*) *Dual Stack* e di un PC dotato di un sistema operativo che lo supporti (Windows 7, MacOS X o una versione recente di Linux); per attivare una sessione *Bridged* direttamente dal PC è sufficiente un PC con i sistemi operativi sopraelencati, senza requisiti particolari per quanto riguarda l'Access Gateway. Seguendo le procedure manuali pubblicate al link *http://assistenzatecnica.telecomitalia.it/at/Informazioni_privati/ipv6* si può procedere alla configurazione del modem o del PC. Tale configurazione dovrà essere manuale: in questa fase non sono ancora disponibili procedure automatizzate di *pre-provisioning* o *provisioning*, che tuttavia saranno predisposte non appena il servizio sarà consolidato.

Tra gli Access Gateway commercializzati da Telecom Italia, il Fritzbox 7270 di AVM con le release in usodispone di tutte le funzionalità necessarie per poter garantire il collegamento alla rete in *Dual Stack*. Tra i prodotti acquistabili liberamente sul mercato, alcuni sono già predisposti per il supporto della modalità Dual Stack (DLink, Netgear, Zyxel e Linksys), ma il cliente deve procedere ancora in maniera autonoma alla configurazione.

Il modello di servizio è molto semplice: consiste nell'apertura di una sessione

PPP (come avviene oggi), ma con il supporto per IPv4 e IPv6. Il BNAS di attestazione, riconosciuta la richiesta, prolungherà la sessione verso i BNAS centralizzati in grado di offrire il servizio. In questo modo, nel caso della sessione *Routed*, l'AG otterrà un indirizzo IPv4 pubblico per la connessione punto-punto con il BNAS (come succede già nelle attuali connessioni) e due prefissi pubblici IPv6, uno per la connessione punto-punto e uno per la *home network*. Inoltre saranno comunicati e configurati automaticamente una coppia di server DNS (*Domain Name System*) IPv4 e una coppia IPv6. Il PC del cliente affiancherà quindi all'indirizzo IPv4 (che appartiene allo spazio di indirizzamento privato e che viene "nattato", cioè trasformato in indirizzo pubblico, dall'Access Gateway per la connettività Internet) anche un indirizzo IPv6 pubblico (per il quale non saranno necessarie le funzioni di NAT dell'AG), che consentirà di accedere direttamente alla rete Internet IPv6. Nel caso invece della sessione *Bridged,* il PC del cliente otterrà due indirizzi pubblici, uno per IPv4 e uno per IPv6.

A seconda della destinazione inserita nel *browser*, il PC dell'utente utilizzerà il protocollo IPv4 o quello IPv6 per la visualizzazione della pagina richiesta, in modo trasparente all'utilizzatore.

Sono inoltre stati aperti all'accesso IPV6 anche alcuni portali istituzionali, *www.telecomitalia.com*, *www.avoicomunicare.it* e *www.telecomitaliahub.it*.

Il cliente si potrà accorgere di essere collegato in IPv6 grazie alla presenza di un Pop-up che indica il prefisso IPv6 utilizzato ■

andrea.garzia@telecomitalia.it

chiara.moriondo@telecomitalia.it

In sintesi il nodo opera secondo i seguenti criteri:

- Su ogni accesso (realizzato mediante una interfaccia logica) viene applicata una limitazione a livello di BP (*Banda di Picco*), che opera anche in condizioni di rete scarica. Tale limite solitamente corrisponde alla capacità massima della linea di accesso del cliente (ad es. 2 Mbit/s).
- In caso di congestione il PE ripartisce la banda tra gli accessi rispettando un parametro contrattuale chiamato BMG (*Banda Minima Garantita*). Tale parametro consente di differenziare accessi che con lo stesso tipo di collegamento (ad es. un ADSL a 7 Mbit/s, su cui si applica una BMG di 256 kbit/s oppure di 512 kbit/s) e quindi avere una maggiore ricchezza di offerta.
- All'interno della banda disponibile per un accesso (BP se non c'è congestione, oppure un valore compreso tra BMG e BP) il traffico viene accodato in maniera differenziata. Nel caso di accodamento standard si hanno tre classi, una prioritaria a bassa latenza (RT (*Real Time*), gestita con tecnica di LLQ (*Low Latency Queuing*)) ma con limitazione ad un a valore massimo contrattualizzato (BRT, minore di BMG), e due classi dati (DEFAULT e MC (*Mission Critical*)) gestite in ripartizione di banda pesata (ad esempio 30:70, su cui si applica un algoritmo di tipo WFQ (*Weighted Fair Queuing*). È anche prevista una ulteriore classe non disponibile al traffico cliente ma riservata per protocolli di routing e gestione NC (*Network Control*).

Sull'apparato posto in sede cliente, chiamato TIR (*Terminazione Intelligente di Rete*) viene effettuata la differenziazione in classi come indicato nel punto precedente. Non è invece richiesta la gestione della BMG e solitamente neppure della limitazione a livello di BP (poiché questa corrisponde alla velocità fisica della interfaccia di collegamento). La TIR è però responsabile della classificazione del traffico che può avvenire secondo criteri anche personalizzabili e relativamente sofisticati. In questo modo un cliente può scegliere quale tipo di traffico e, con alcuni modelli di TIR, anche quali applicazioni vengono classificati con DEFAULT, MC o RT. La TIR è anche un elemento impiegabile per fornire servizi ulteriori, quali i servizi di sicurezza (Firewall), servizi di fonia realizzata con tecnologia VoIP e connettività LAN mediante porte in rame o WiFi.

Per i clienti che lo richiedono sono disponibili anche diverse opzioni di ridondanza. Tra queste citiamo la ridondanza di TIR e di collegamento e la possibilità di avere bilanciamento su due vie, anche attestate su PE distinti. A questo scopo tra TIR e PE si realizza una comunicazione che verifica continuativamente la disponibilità del collegamento di accesso e, in caso di rilevazione di guasto, scatena le necessarie azioni (re-instradamento del traffico ed eventuale attivazione di collegamenti "on-demand"). Il protocollo impiegato è BGP che consente normalmente di individuare un guasto entro 30 secondi; sono anche possibili soluzioni più reattive (basate ad esempio sul protocollo BFD – Bidirectional Forwarding Detection, appositamente sviluppato per questo scopo).

2.2 Clienti Residenziali e Small Business

La clientela Residenziale MM (*Mass Market*) e Small Business SoHo (*Small Office–Home Office*), che generalmente utilizza accessi ADSL e AG (*Access Gateway*), viene gestita da una piattaforma di Edge dedicata. Molti di questi clienti utilizzano AG forniti da Telecom Italia, per i quali è prevista una procedura automatizzata di configurazione dell'accesso alla rete. La tariffazione applicata è di tipo flat o a tempo.

L'elemento di rete sul quale sono concentrate le funzionalità necessarie a fornire i servizi per questi clienti è denominato BNAS (*Broadband Network Access Server*) o BNG (*Broadband Network Gateway*). Tale elemento, inserito nella rete Telecom Italia come ad esempio nella configurazione di Figura 3, è il primo nodo di trattamento dell'*Internet Protocol* del cliente verso Internet. Questo tipo di apparato deve essere caratterizzato da alta scalabilità e, necessariamente, alta affidabilità data la concentrazione su uno stesso apparato di un bacino di utenza significativa (fino a 128 K/256 K utenti per le tecnologie più recenti).

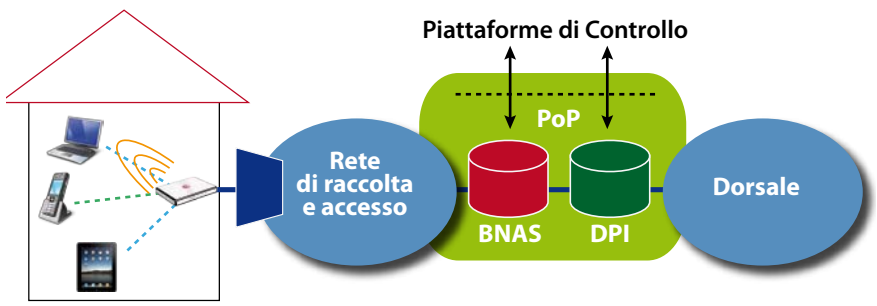
Indipendentemente dalla rete di aggregazione utilizzata, Carrier Ethernet come nel caso di OPM o ATM, il modello di connettività si basa sull'uso di PPP (*Point-to-Point Protocol*). Questo protocollo permette di realizzare una connessione punto-punto tra il terminale del cliente e il BNAS oppure tra l'AG e il BNAS. Nel primo caso si parla di accesso di tipo *Bridged* e l'AG opera essenzialmente come un modem terminatore di linea ADSL. Nel secondo caso si parla di accesso *Routed*; l'AG opera anche come router IP vero e proprio.

Le sessioni PPP, a partire da casa cliente, vengono aggregate sui nodi di accesso DSLAM (*Digital Subscriber Line Access Multiplexer*) per essere trasportate verso un'interfaccia del BNAS. Il BNAS termina le sessioni PPP ed esegue un insieme di funzioni denominate *Subscriber Management*, che potremmo tradurre con Gestione del Cliente. Queste funzioni comprendono:

- **AAA** (*Autenticazione, Autorizzazione e Accounting*);
- assegnazione degli indirizzi IP;
- applicazione di regole di trattamento dei pacchetti IP (*Policy Enforcement*).

Il BNAS esegue le funzioni di *Subscriber Management* grazie all'interazione con le piattaforme di controllo che detengono le informazioni di profilo contrattuale dei clienti e sono coinvolte in un fitto scambio di informazioni con il BNAS stesso.

Figura 3 - Catena impiantistica per clienti MM



2.2.1 *Autenticazione, Autorizzazione e Accounting (AAA)*

Nel corso della costruzione della sessione PPP è prevista una procedura di autenticazione del cliente. I messaggi di controllo di PPP trasportano le credenziali del cliente:

- una chiave tecnica inserita dal DSLAM che identifica la linea cliente;
- username e password inseriti dal cliente.

La chiave tecnica rappresenta una credenziale molto affidabile e quindi consente un livello di sicurezza della procedura di autenticazione molto forte. Essa consente di autenticare la linea cliente; username e password possono essere utilizzati per individuare più specificatamente l'utente che desidera accedere a servizi particolari.

Il BNAS, ricevute queste credenziali, interroga un server di autenticazione per verificarne la correttezza. Per farlo utilizza il protocollo RADIUS (*Remote Authentication Dial-In User Service*); se la verifica ha esito positivo, essa si conclude con l'autorizzazione del cliente ad accedere al servizio richiesto.

Ulteriore compito di RADIUS è quello di *Accounting* ovvero di fornire la "documentazione" relativa all'attività del Cliente. Tale documentazione è utile per vari scopi:

- registrazione degli istanti di inizio e fine della connessione in rete degli utenti, in ottemperanza agli obblighi di legge;
- tariffazione (per i clienti che abbiano sottoscritto un contratto su base consumo);
- realizzare uno strumento per la verifica della *presence*, ovvero un database che contiene istan-

te per istante la lista dei clienti "on line".
In pratica RADIUS viene utilizzato per inviare dei Cartellini sia al momento dell'instaurazione della connessione sia al momento della disconnessione (ad esempio quando il Cliente spegne il modem). Questi Cartellini, prodotti dal BNAS, permettono di correlare informazioni quali: identità del Cliente, indirizzo IP assegnato, data ora di inizio e fine della connessione e volume di traffico scambiato durante la sessione.

2.2.2 *Assegnazione degli indirizzi IP*

Per consentire al cliente autorizzato di poter accedere al servizio richiesto, è necessario assegnare un indirizzo IP alla terminazione PPP lato cliente (il suo terminale o l'AG). Questa assegnazione può essere permanente (il Cliente ottiene sempre lo stesso indirizzo IP) o temporanea (l'indirizzo IP assegnato al Cliente cambia ogni volta che si connette, ad esempio quando accende il modem).
L'attribuzione di un indirizzo permanente è considerato un plus in quanto consente al Cliente di essere raggiunto sempre con lo stesso indirizzo IP. Questa caratteristica è utile, ad esempio, a quei Clienti, tipicamente Business, che dietro la loro connettività IP vogliono esporre un sito web. La macro distinzione è quindi: ai Clienti Business vengono attribuiti indirizzi IP permanenti mentre ai Clienti consumer vengono assegnati indirizzi IP temporanei. In entrambi i casi l'assegnazione avviene in modalità dinamica, sfruttando le funzioni di RADIUS e PPP.
L'utilizzo di indirizzi IP assegnati temporaneamente consente all'operatore di realizzare una gestione più efficiente degli indirizzi IP. Se su un BNAS sono stati configurati 100 Clienti ed ad ognuno si vuole poter assegnare un indirizzo IP per il tempo in cui richiede mantenersi *on-line*, non è necessario predisporre 100 indirizzi ma un numero inferiore in considerazione del "fattore di contemporaneità".
L'utilizzo efficiente degli indirizzi IP diviene ancora più importante in una fase in cui le scorte a livello mondiale si stanno esaurendo. Per questo motivo si tende a non "sprecare" indirizzi IP pubblici per servizi completamente richiusi all'interno della rete dell'operatore. È questo il caso dei servizi di tipo ToIP (*Telephony over IP*) e dei servizi di telegestione degli AG forniti direttamente da Telecom Italia: per questi servizi vengono assegnati indirizzi IP privati.
Inoltre, ci si sta preparando all'offerta di servizi basati su IPv6. Questo comporterà l'assegnazione di indirizzi IPv6 in aggiunta a quelli IPv4.

2.2.3 *Policy enforcement*

La sessione cliente autorizzata e che ha ottenuto il suo indirizzo IP viene caratterizzata sulla base di parametri definiti in sede di contratto (banda allocata, QoS, eventuali restrizioni all'accesso,...). Per ogni accesso sul BNAS viene configurata una limitazione a livello di Banda di Picco, sempre attiva in presenza o meno di congestione. Tale limite corrisponde alla capacità massima del valore contrattuale del collegamento del cliente (es. Alice 7Mega, Alice 20Mega). Altri elementi caratterizzanti e distintivi del profilo cliente prevedono ad esempio:

- per clienti Small Business la configurazione di una Banda Minima Garantita, ripartita dal BNAS tra gli accessi in caso di congestione;
- per clienti Residenziali la configurazione di restrizioni all'accesso verso i server di Telecom Italia nel caso dei servizi ToIP e di telegestione e l'eventuale redirezione verso portali Telecom Italia per comunicazioni importanti alla clientela.

Una volta assegnato il profilo di connettività, questo rimane normalmente immutato per tutta la durata della connessione (e più in generale per tutta la durata del contratto). È tuttavia possibile cambiare "in corsa" le caratteristiche del profilo cliente per realizzare servizi a richiesta. Un esempio in fase di studio è un servizio di tipo "Turbo button", grazie al quale un cliente con una banda di picco di 7 Mbps potrebbe accedere ad un portale e richiedere in tempo reale un incremento di velocità passando a 20 Mbps; pagherà in modo differente il periodo di tempo in cui ha usufruito della velocità più alta.
Questa variazione viene realizzata tramite funzionalità specifiche del protocollo RADIUS denominate CoA (*Change of Authorisation*). A comandare questa variazione di profilo è chiamata una piattaforma di controllo denominata Policy Manager (vedi BOX).

2.2.4 *Deep Packet Inspection*

In Figura 3 si può osservare come tra il BNAS e i router del backbone IP/MPLS siano collocati apparati di DPI (*Deep Packet Inspection*), in grado di classificare il traffico su base protocollo e specifica ap-

Policy Control

La realizzazione di servizi evoluti e caratterizzati da un elevato grado di dinamicità richiede un'orchestrazione complessiva delle funzionalità di controllo messe a disposizione dai dispositivi di rete deputati all'effettivo instradamento del traffico. Scopo del *Policy Control* è appunto quello di assicurare questo coordinamento, nel rispetto di politiche di gestione dei servizi specificate dall'operatore e realizzando logiche di ottimizzazione nell'utilizzo delle risorse trasmissive.

Il *Policy Control* si basa sulla disponibilità di un sistema, genericamente denominato *Policy Manager*, che, agendo a livello di piano di controllo, sia in grado di interagire in real-time con i nodi di rete e di modificare (su base richiesta utente o su base condizione di rete) le politiche di trattamento del traffico da questi attuate.

Nel contesto dei servizi legati al *Policy Control*, è quindi compito del *Policy Manager* controllare gli elementi di rete, forzando l'applicazione di regole di trattamento del traffico rispondenti al servizio o alla prestazione di rete desiderati.

Si rende così possibile la realizzazione di politiche di *Traffic Management* differenziate su base caratteristiche statiche (ad esempio: profilo utente, terminale in uso, ...) e dinamiche (ad esempio: localizzazione, tipo di copertura radio, ...) relative alla specifica sessione trattata. È inoltre possibile l'attuazione di politiche di servizio dinamiche su base richiesta esplicita da parte dell'utente (ad esempio incremento di banda su richiesta).

La soluzione di *Policy Manager* realizzata da Telecom Italia è denominata CPM (*Common Policy Manager*). Al CPM è affidata la gestione dei servizi fissi e mobili di utenza Residenziale, Business e Top, come illustrato nella Figura 2A.

La scelta di avere una soluzione di *policy management* comune tra le reti fissa e mobile offre numerosi vantaggi, tra cui:

- abilita la definizione sinergica di servizi convergenti fisso/mobile;
- minimizza l'*effort* di dispiegamento della soluzione;
- ottimizza l'utilizzo degli *skill* acquisiti;
- rappresenta un trend tecnologico sempre più evidente tra i vendor di soluzioni di *policy management*.

Il dispiegamento attuale della soluzione CPM prevede l'interfacciamento di questa piattaforma con i nodi GGSN per il controllo dei servizi di rete mobile e con le sonde DPI ed i nodi BNAS per la realizzazione di quelli di rete fissa.

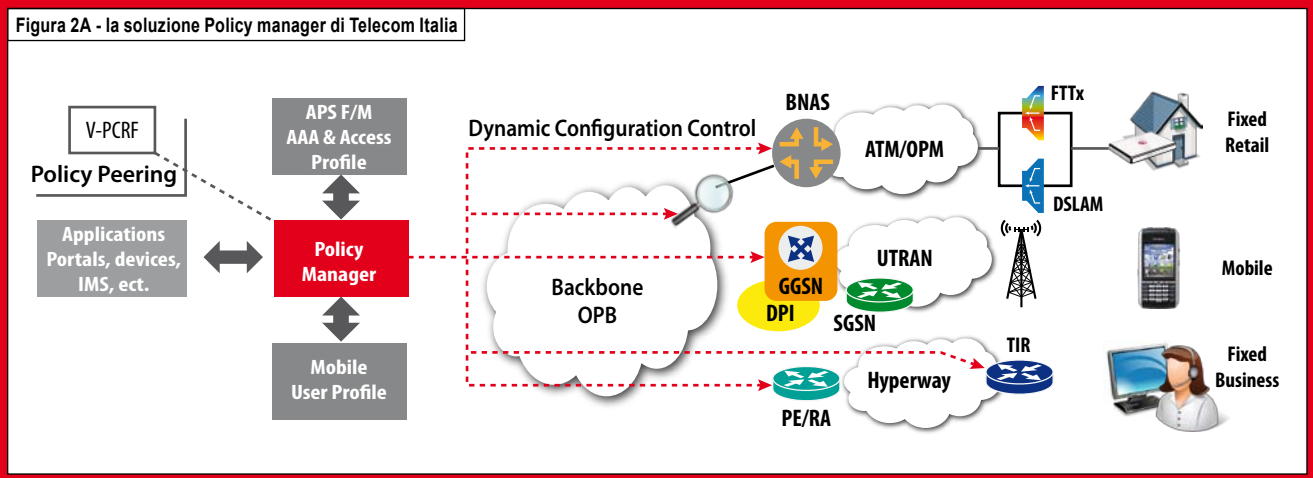
La funzionalità DPI riveste un ruolo molto importante nella realizzazione dei servizi legati al *Policy Control*, rendendo possibile l'attuazione di *policy* che agiscano selettivamente solo su specifiche tipologie di traffico, di applicazioni o di utenti.

Un esempio di prestazione realizzata è la limitazione della banda di alcune applicazioni o di alcuni utenti nei casi di congestione di rete, per migliorare la fruibilità dei servizi da parte di tutti gli utenti.

Nella rete mobile, è realizzato il controllo ed eventuale limitazione del volume totale del traffico dei clienti per specifiche offerte ("*Unlimited*") oppure per evitare l'utilizzo (che può essere molto costoso) della rete dopo l'esaurimento del credito ■

angelo.garofalo@telecomitalia.it
massimo1.sassi@telecomitalia.it

Figura 2A - la soluzione Policy manager di Telecom Italia



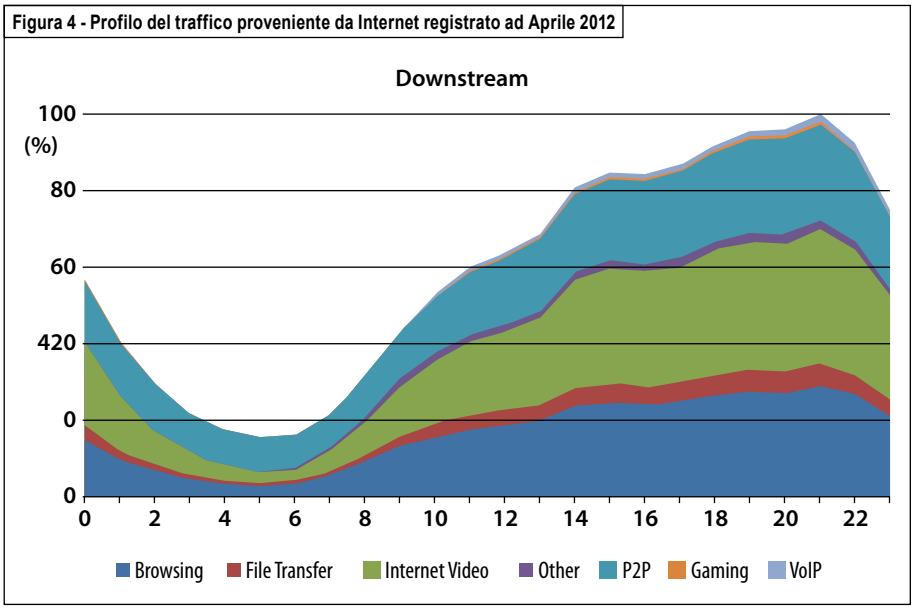
plicazione. Tale classificazione fine consente un efficace monitoraggio del traffico: è possibile in questo modo misurare l'incidenza dei diversi tipi di applicazioni utilizzati dai clienti sul traffico totale trasportato in rete, come mostrato in Figura 4.
Inoltre gli apparati di DPI consentono di effettuare un efficace *Traffic Management* volto a garantire un uso equo delle risorse di rete a tutti i clienti. Con questo scopo gli apparati DPI sono impiegati nella prevenzione dei disagi dovuti a fenomeni di congestione sui collegamenti tra alcuni DSLAM di più vecchia generazione e la rete di aggregazione ATM (sui siti Telecom Italia viene riportata l'evidenza delle centrali, aree e fasce orarie interessati dalla soluzione): per i clienti attestati a questi DSLAM viene realizzata una limitazione selettiva del traffico di applicazioni Peer-to-Peer nelle fasce orarie di massimo carico a beneficio delle applicazioni caratterizzate da una minore richiesta di banda (ad es. web browsing o e-mail), che risulterebbero, altrimenti, penalizzate dalle prime.

La soluzione TI di *Traffic Management* mette in pratica una *Fair Use Policy*, che permette alla totalità dei clienti un utilizzo soddisfacente della rete. Le funzionalità presenti in rete su piattaforma DPI consentono di non penalizzare il traffico di specifici clienti, ma di applicare la limitazione di banda all'insieme dei clienti simultaneamente utilizzatori di applicazioni P2P, gestiti in modalità anonima.

3 Gli Enti di standardizzazione

A differenza di quanto avviene per la rete mobile, non vi è un modello realizzativo univoco per i servizi di rete fissa. Sono infatti emersi nelle implementazioni degli operatori vari modelli che fanno tutti riferimento a meccanismi e protocolli standard, a volte standardizzati dopo che erano già stati adottati da qualche *early adopter*. Vi sono differenze nella scelta tipo sessione (PPP per molti, ma altri hanno adottato il modello delle cosiddette sessioni IP), nei protocolli di autenticazione (RADIUS è certamente la scelta più diffusa, ma non l'unica possibile), addirittura nell'architettura: alcuni operatori hanno scelto un approccio denominato *Single Edge*, in cui tutti i servizi sono gestiti da un'unica piattaforma di Edge, mentre altri hanno seguito l'approccio *Multiple Edge*, dove esistono piattaforme di Edge dedicate per ciascun servizio.
La diversità di scelta è dipesa da vari fattori: il target di clientela a cui ci si rivolge, i modelli di tariffazione, l'organizzazione interna delle strutture tecniche degli operatori, ecc.
Questa situazione ha radici nella natura del coordinamento tecnico di Internet, basata su pochi e fondamentali principi architetturali e rivolta alla standardizzazione delle soluzioni a specifici problemi puntuali, a volte anche di più soluzioni per uno stesso problema. L'ente di standardizzazione di riferimento per i protocolli di Internet è l'IETF (*Internet Engineering Task Force*) [2]: nello spirito dei pionieri di Internet l'IETF non fornisce indicazioni implementative sugli apparati, né modelli di servizio end-to-end.
Per colmare questa lacuna si è invece affermato più recentemente il BBF (*BroadBand Forum*) [3]. La sua attività si concentra sulle architetture e sugli apparati, con l'obiettivo di garantire l'interoperabilità end-to-end delle catene si servizio, pur in uno scenario in cui sono possibili più modelli realizzativi per lo stesso servizio.

Figura 4 - Profilo del traffico proveniente da Internet registrato ad Aprile 2012



3.1 IETF

L'IETF è un ente internazionale che si occupa della standardizzazione dei protocolli per la rete Internet.

Ciò che differenzia l'IETF da enti ed organizzazioni di standardizzazione più tradizionali è la sua struttura aperta: il lavoro viene svolto da gruppi di lavoro che operano soprattutto tramite *mailing list*, aperte alla partecipazione di chiunque sia interessato. Al lavoro svolto dall'IETF contribuiscono esperti tecnici e ricercatori provenienti dai principali costruttori di apparati di rete, dai maggiori operatori e dalle principali università del mondo.
I gruppi di lavoro si occupano ciascuno di uno specifico argomento tecnico e sono organizzati in aree tematiche, in modo da coprire tutte le aree scientifiche e tecnologiche dalla rete: *Applications, Internet, Operations and Management, Routing, Security, Transport*, ecc.
Il risultato del lavoro di ogni gruppo IETF è costituito da documenti denominati RFC (*Request For Comments*). Dalla sua nascita (1986) ad oggi l'IETF ha prodotto più di 6000 RFC contenenti le specifiche di tutti i protocolli utilizzati nella rete Internet: dai protocolli di base come IP, TCP, UDP ai protocolli di routing *unicast* e *multicast*, ai protocolli MPLS per applicazioni VPN e *Pseudowire*. L'IETF sta inoltre lavorando da diversi anni alla definizione del protocollo IPv6: ovvero il successore del protocollo IPv4 oggi utilizzato per l'indirizzamento della rete Internet, in quanto lo spazio di indirizzi IPv4 disponibili è stato esaurito all'inizio dello scorso anno. Le specifiche IPv6 di base sono ormai consolidate; negli ultimi tre anni l'IETF si è concentrata sulla definizione di tecniche di migrazione e coesistenza IPv4/IPv6 basate su meccanismi di *tunneling* IPv6 su IPv4 e IPv4 su IPv6 o di traduzione di protocollo.
Le RFC costituiscono l'elemento fondamentale su cui si basano le specifiche tecniche della maggior parte degli apparati di rete. Le RFC vengono solitamente citate da Telecom Italia nei requisiti delle gare per i nuovi apparati. Telecom Italia partecipa da anni all'IETF ed è tra gli autori di alcune RFC e di numerosi documenti di lavoro (*internet drafts*) sulle tematiche IPv6, IP/MPLS e *performance monitoring*.

3.2 Broadband Forum

Il BBF è l'ente che si occupa della standardizzazione dell'architettura della rete *broadband* di accesso, aggregazione e Edge IP. Questo ente, nato originariamente come *DSL Forum* in quanto focalizzato sulle tecnologie di livello fisico in rete di accesso, si è negli anni evoluto fino a coprire tematiche architetturali *end-to-end* sui differenti segmenti di rete, grazie anche alla fusione con l'IP/MPLS Forum, che tradizionalmente si occupava della definizione delle architetture per reti IP/MPLS.
Al BBF partecipano costruttori di apparati dei differenti segmenti di rete e operatori provenienti da tutto il mondo.
Le aree tematiche di competenza del BBF si possono logicamente suddividere in tre categorie :

- **Broadband Network**: definizione di architetture e requisiti di apparato per la rete di accesso, di aggregazione ed Edge al fine di garantire soluzioni di rete di interoperabili e scalabili a livello *end-to-end*;
- **Broadband User**: specifiche degli apparati *Residential Gateway* per la *home network*;
- **Broadband Management**: specifiche per la gestione degli apparati della *home network*.

Nel corso degli ultimi anni il BBF ha guidato l'evoluzione della rete Broadband con la pubblicazione di documenti di specifica per i BNAS/BNG e per i nodi di accesso. In particolare il BBF ha dapprima specificato i requisiti base per i BNG in termini di routing, *Subscriber Manager* per sessioni PPP e QoS, per poi affrontare le problematiche connesse con la migrazione ATM-Ethernet. Tra i temi più recenti, vi è la migrazione IPv4/IPv6. Il passo successivo nell'evoluzione della rete Broadband è costituito dalla definizione dell'architettura e dei requisiti dei nodi (nodi di accesso, BNG e nodi di aggregazione) per la rete Broadband Multi-servizio.

4 L'evoluzione delle tecnologie di Edge

Una linea guida importante nell'evoluzione dei router di Edge IP è determinata dalla necessità di ridurre i costi a seguito del rallentamento del tasso di crescita dei servizi broadband nei paesi più evoluti, dell'incremento della banda per linea cliente e della diminuzione dei ricavi per unità di banda.
In questo contesto si assiste da parte dei principali costruttori alla razionalizzazione delle linee di prodotto con l'offerta di apparati sempre più *general purpose* al posto di apparati dedicati per segmento di clientela e/o funzionalità di rete. In particolare i nuovi apparati di Edge IP business e residenziale sono realizzati a partire da *switch* IP/MPLS, inizialmente proposti per il segmento metro, equipaggiati con schede dotate

di *packet processor* evoluti molto flessibili, che permettono lo sviluppo di funzionalità complesse di *Subscriber Management*.
Le nuove soluzioni di Edge IP sono caratterizzate da un sostanziale incremento della capacità di commutazione per scheda e per apparato: essendo piattaforme pensate per la rete di aggregazione, sono già in grado oggi di gestire *throughput* per scheda nell'ordine di 100 Gbps, con *throughput* per macchina che raggiungono e superano 1 Tbps; capacità destinate a raddoppiare nell'arco di un anno. La scalabilità di questi apparati cresce inoltre in modo sensibile anche in termini di numero di utenti gestiti (128 k sessioni di utenti residenziali per apparato, con un target di 256 k, circa 5 k sessioni BGP con un target di 10-12k).
L'impiego della stessa tipologia di apparati a livello di Edge e a livello di aggregazione Metro, lascia per altro la possibilità di una scelta architetturale nuova: collassare le funzionalità di Edge e di aggregazione in un solo apparato, "soluzione Edge distribuito", che è di particolare interesse in contesti, in cui il traffico è più localizzato e/o è economicamente conveniente una redistribuzione capillare di contenuti attraverso soluzioni di *caching* o di *content delivery*.
In ogni caso, sia optando per una architettura di rete tradizionale, con separazione tra Edge ed aggregazione, sia optando per la soluzione Edge distribuito, l'aspettativa è che l'evoluzione tecnologica permetta una sostanziale riduzione del numero di apparati complessivi in rete (e quindi del *Total Cost of Ownership*).
Una direzione evolutiva importante per gli apparati di Edge IP è quella che permette di fornire funzionalità di servizio di livello 4-7 attraverso l'integrazione di schede di elaborazione general purpose, eventualmente modulari in termini di CPU e memoria. L'integrazione di queste schede è oggi considerata per tre applicazioni specifiche:
- **Carrier Grade NAT**, per gestire la scarsità di indirizzi IPv4 attraverso l'assegnazione agli utenti di indirizzi privati e lo spostamento della funzionalità di NAT in rete per accesso a Internet;
- **Deep Packet Inspection**, per realizzare servizi che richiedano qualità differenziata su base applicazione e/o analisi statistiche sul traffico generato dagli utenti a livello applicativo;
- **Caching/Content Distribution** di contenuti video, per ottimizzare il traffico in rete a fronte di richieste multiple per lo stesso contenuto.

Queste funzioni sono oggi normalmente realizzate da apparati dedicati inseriti all'interno del PoP. L'integrazione sugli apparati di Edge riduce il numero totale di apparati e di interfacce in rete, portando quindi a una possibile riduzione dei costi di investimento e dei costi operativi. Un altro beneficio atteso è la semplificazione nella configurazione dei servizi, in quanto si ha sempre un unico punto in rete in cui sono configurate tutte le funzionalità di *Subscriber Management*: una maggiore segmentazione dell'offerta richiede ad esempio di fornire funzionalità di NAT o di Content Distribution solo ad un sotto-insieme dei clienti, operazione che può risultare complessa se realizzata su apparati diversi da quelli che autenticano il cliente e ne gestiscono il profilo di connettività.
Per contro l'integrazione di queste funzioni sul nodo di Edge presenta due problemi principali:
- la de-ottimizzazione nell'utilizzo delle risorse rispetto al caso di apparati dedicati che possono essere condivise tra più apparati di Edge,
- possibili problemi di scalabilità sulle macchine di Edge stesse dovute al numero di schede *general purpose* equipaggiabili e alle capacità di queste ultime che potrebbero essere inferiori a quelle di apparati dedicati.

L'integrazione di funzionalità di *processing* all'interno dei nodi di Edge, in alcune visioni evolutive ha un ruolo che va oltre le semplici funzionalità precedentemente descritte: diventa un elemento che permette una migliore integrazione dei servizi di Telecomunicazione con i Servizi IT ed in ultima analisi uno dei fattori abilitanti per una fase evoluta del *Cloud Computing* (da alcuni anche denominato in questo contesto *Fog Computing*), in cui le risorse informatiche da centralizzate si distribuiscono in maniera sempre più capillare.
Un ulteriore aspetto evolutivo di interesse è la progressiva introduzione di soluzioni che permettono di utilizzare più apparati in *cluster* come un unico apparato logico, prevedendo un'integrazione a livello di piano di controllo e di gestione. Su questo aspetto in assenza di standard di riferimento le soluzioni proposte dai costruttori non sono completamente in linea tra loro e assumono anche denominazioni diverse come *Virtual Chassis* (soluzione proposta ad esempio da Juniper e Cisco) o *Virtual Router* (soluzione proposta ad esempio da ALU). A titolo di esempio, si considera in questo contesto la sola soluzione *Virtual*

Chassis, che genericamente prevede:

- collegamento tra gli apparati sul piano dati attraverso interfacce standard di livello 2;
- almeno un *Route Processor* per apparato con gestione in ridondanza calda (unico processo di routing e unica tabella di *forwarding* per i due apparati); a seconda dell'implementazione può essere richiesto un collegamento tra i *Route Processor* distinto dal collegamento sul piano dati;
- gestione delle schede di interfaccia in modo trasparente rispetto all'apparato su cui sono fisicamente inserite;
- possibilità di gestire con il protocollo LAG (*Link Aggregation Group*) interfacce inserite su apparati differenti.

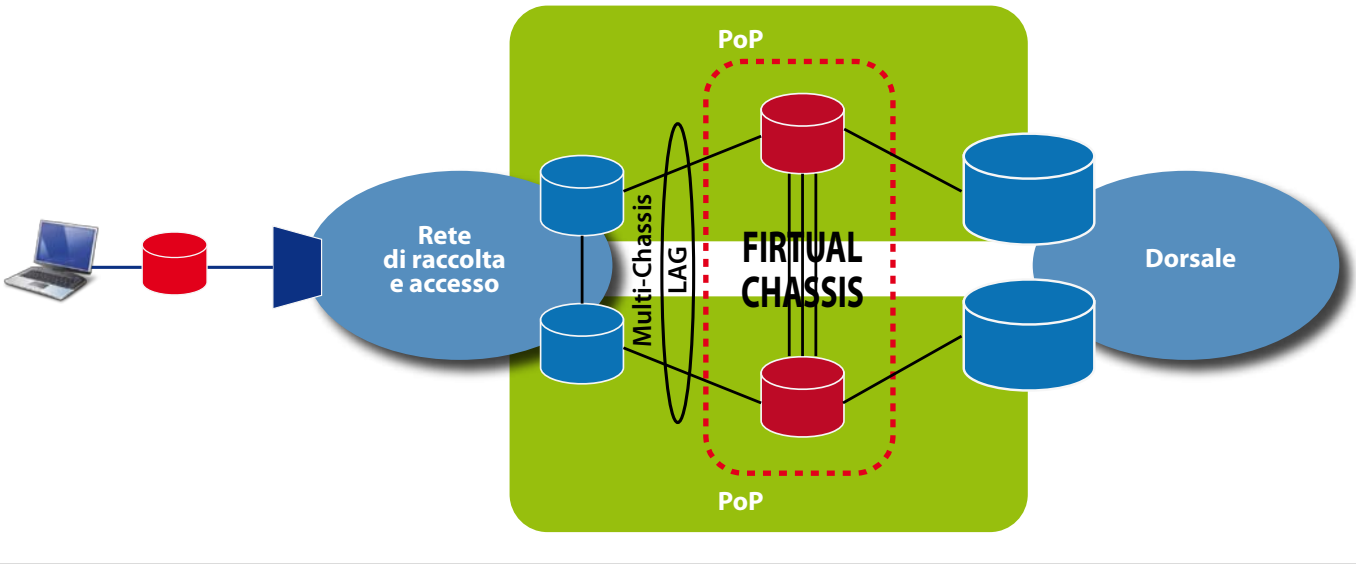
Si noti che non è richiesto che gli apparati siano collocati nella stessa sede: il funzionamento viene garantito anche nel caso siano in sedi separate da qualche centinaio di chilometri. Questa soluzione è quindi promettente per realizzare una architettura di rete che permetta di garantire continuità di servizio anche in caso di guasto catastrofico che coinvolga un'intera sede. Nel caso di apparati collocati nella stessa sede il vantaggio affidabile, pur non nullo, è di entità modesta.

Per contro la necessità di collegamenti tra i due apparati sul piano dati è un punto debole proprio nel caso di diversificazione di sede, avendo un impatto significativo sui costi: nel caso di due apparati i collegamenti devono essere dimensionati almeno al 50% del traffico aggregato, in quanto i router di backbone bilanceranno il traffico sulle interfacce verso i due apparati indipendentemente dal posizionamento fisico delle interfacce d'accesso.

Un esempio del contesto di rete in cui può essere inserita la funzionalità *Virtual Chassis* è riportato in Figura 5, dove il Nodo di Edge è un BNAS distribuito su due PoP che termina sessioni PPP e fornisce servizi di connettività IP a clientela residenziale e small business: nel caso di guasto dell'intera sede A, le connessioni PPP sono protette sulla sede B.

Passando dal breve al lungo termine, le linee di sviluppo del livello di Edge IP non sono ancora chiaramente definite: ampio dibattito è in corso sulla necessità/opportunità di dotare i router di interfacce aperte sul piano di controllo che permettano di istanziare politiche di routing complementari o sostitutive rispetto a quelle tradizionali, basate su protocolli di comunicazione tra gli apparati. Questo nuovo approccio alle reti dati, che è conosciuto come SDN (*Software Defined Networking*) [4] ed è embrionalmente sperimentato da qualche anno con sviluppi essenzialmente guidati da un ambito accademico (si vedano le iniziative legate al protocollo *Openflow* [5]), trova potenzialmente nei nodi di Edge il punto di naturale applicazione: fattibilità, scalabilità ed effettiva rispondenza alle esigenze del mercato sono tuttavia ancora incognite. Per contro alternative che portino ad una estrema semplificazione dell'offerta di servizio e quindi delle funzionalità dei nodi di Edge, al fine di **minimizzare** i costi, non possono esser escluse.

Figura 5 - Configurazione di ridondanza geografica



5 Il Modello Seamless MPLS

La tecnologia IP/MPLS è utilizzata da più di dieci anni all'interno delle reti dorsali dei principali operatori a livello mondiale. Telecom Italia, con la rete OPB è stata pioniera nell'adozione di IP/MPLS per il trasporto sia del traffico dati sia del traffico di fonia nei collegamenti a livello di dorsale. L'esperienza operativa sviluppata ha reso evidente l'elevata maturità tecnologica di IP/MPLS, sia a livello di standard sia per l'ampia disponibilità di prodotti.
Questa maturità consente oggi la realizzazione di reti a pacchetto estese in grado di offrire funzionalità che fino a qualche anno fa erano considerate tipiche delle sole reti di trasporto SDH quali: strumenti gestionali evoluti, possibilità di monitoraggio costante della qualità del servizio di trasporto, meccanismi di re-instradamento molto veloci. Oltre a questi benefici le reti IP/MPLS presentano il grande vantaggio di disporre di un piano di controllo automatico che consente una drastica semplificazione delle attività operative, nonché il vantaggio di trasportare in maniera molto efficiente ed affidabile, rispetto ad altre soluzioni, i servizi *video live* (tramite funzionalità di *multicast*) e servizi per reti private virtuali *any-to-any* a livello Ethernet e IP.
Per questi motivi, l'utilizzo della tecnologia IP/MPLS è stato adottato anche nella maggior parte delle reti di aggregazione realizzate dai principali Operatori in tutto il mondo. Non fa eccezione la rete metro regionale OPM di Telecom Italia, realizzata inizialmente nel 2005 a supporto del lancio dei Servizi *Triple Play* (dati, voce, IPTV), in sostituzione della infrastruttura di raccolta ATM che iniziava a manifestare limitazioni nella possibilità di fornitura di servizi più avanzati, è diventata oggi una robusta rete multi-servizio in grado di raccogliere il traffico di servizi di rete fissa e mobile della clientela residenziale e business sia di Telecom Italia sia di altri operatori.
La rete OPM, è stata realizzata fin dall'inizio con apparati *multilayer switch*, in grado di trattare il traffico sia al livello 2 (*switching* Ethernet) sia a livello IP, sia a livello MPLS. Questo elevato grado di flessibilità ne ha consentito una graduale evoluzione a partire da una fase iniziale in cui la rete era utilizzata come infrastruttura di raccolta di puro livello 2 per la maggior parte dei servizi, privilegiando gli aspetti legati alla semplicità dei protocolli Ethernet, ad una fase successiva in cui si è passati ad un utilizzo sempre più spinto di soluzioni di trasporto IP e MPLS per far fronte ai limiti riscontrati nella tecnologia Ethernet costituiti principalmente dalla scalabilità in termini di massimo numero di identificativi di VLAN (12 bit disponibili nel formato di una frame Ethernet) e dai ridotti meccanismi automatici di ripristino dai guasti (tempi di convergenza dei protocolli *Spanning Tree e Rapid Spanning Tree*).
Il modello oggi adottato per OPM è basato sulla tecnologia Ethernet over MPLS per il trasporto dei flussi Ethernet e sulla tecnologia IP per il routing di alcuni servizi direttamente a livello IP: in generale quindi il Piano di Controllo (ossia l'insieme dei protocolli che regolano l'instradamento dei servizi in rete) è di tipo IP/MPLS.
Una possibile direzione evolutiva della rete di Telecom Italia prevede l'estensione di questa omogeneità tecnologica basata su IP/MPLS fino ai nodi di accesso (DSLAM) e ai nodi di Edge IP (BNAS e PE). Questo modello architetturale prende il nome di *Seamless MPLS* [6][7] e si pone l'obiettivo di creare una soluzione di rete uniforme per tutti i segmenti di rete (dall'accesso, all'aggregazione, al PoP e alla dorsale), in grado di sfruttare i benefici della tecnologia IP/MPLS con il suo piano di controllo omogeneo su tutta la rete, per offrire differenti tipi di servizio in modo uniforme, flessibile e scalabile.
Nell'architettura *Seamless MPLS* i nodi di Edge IP sono denominati SN (*Service Node*) mentre i router della rete di aggregazione (nel caso di Telecom Italia, OPM) e della rete dorsale (nel caso di Telecom Italia OPB) sono denominati TN (*Transport Node*); i nodi di accesso sono denominati AN (*Access Node*).
La soluzione *Seamless MPLS* sfrutta il piano di controllo IP/MPLS per la creazione automatica di una magliatura di LSP (*Label Switched Path*), utilizzati per garantire la connettività tra i nodi appartenenti al dominio MPLS, mentre utilizza gli PW (*Pseudowire*) per realizzare le direttrici di servizio.
In Figura 6 sono riportate, a titolo di esempio, tre diverse tipologie di collegamenti logici di tipo PW, questi ultimi permettono di stabilire in modo semplice ed uniforme, mediante configurazioni limitate ai soli punti terminali del collegamento, la connettività necessaria all'erogazione dei vari servizi.
Scendendo più neI dettaglio, per il piano di controllo, il modello *Seamless MPLS* utilizza i seguenti protocolli di routing:

- **OSPF** (*Open Shortest Path First)*: per consentire la mu-

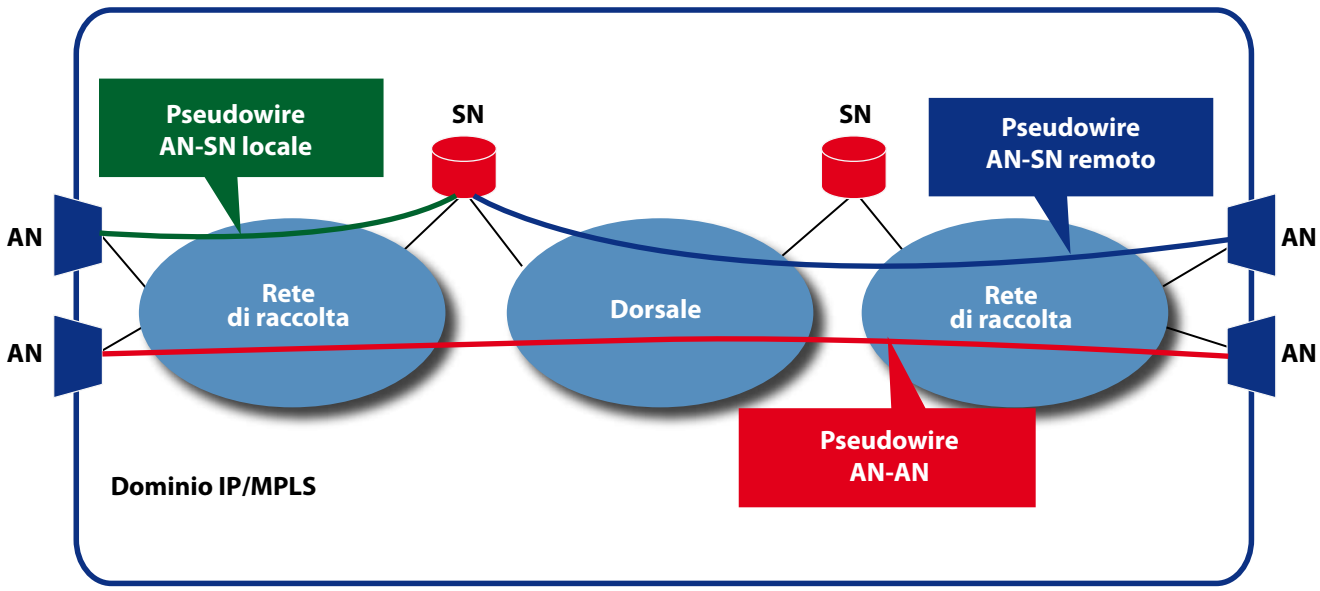


Figura 6 - Architettura *Seamless MPLS*

tua raggiungibilità IP tra tutti i nodi intermedi e i Service Node;

- **BGP** (*Border Gateway Protocol*): per propagare all'interno della rete gli indirizzi IP degli Access Node; l'impiego del BGP si rende necessario per motivi di scalabilità, in quanto il numero di AN può essere molto elevato e quindi non gestibile con il protocollo OSPF;
- Routing statico: tra l'Access Node ed il Transport Node a cui è attestato. L'obiettivo è minimizzare il numero di requisiti per l'Access Node escludendo l'impiego di protocolli di routing dinamici e limitando il più possibile il numero di prefissi IP da memorizzare. L'impiego del routing statico è sufficiente in quanto l'AN rappresenta un nodo terminale all'interno della rete, con grado di connettività molto basso (uno o due al massimo).

Per quanto riguarda la distribuzione delle label MPLS la soluzione Seamless si avvale dei seguenti protocolli:

- LDP (*Label Distribution Protocol*): utilizzato per la segnalazione delle label MPLS e la creazione degli LSP tra tutti i TN e i SN;
- LDP **DoD** (*Downstream-on-Demand*): utilizzato esclusivamente tra un AN e il TN a cui è attestato, per limitare la complessità dell'AN fa sì che quest'ultimo istanzi esclusivamente gli LSP verso i nodi a cui deve inviare traffico;
- BGP (*Border Gateway Protocol*): utilizzato per la segnalazione delle *label* MPLS associate agli indirizzi IP degli Access Node. Le sessioni BGP utilizzate nel piano di routing sono in realtà sessioni IPv4+Label secondo RFC 3107 [8].

Il protocollo di segnalazione per la creazione di uno Pseudowire è T-LDP (*Targeted-LDP*), cioè la versione di LDP che permette l'instaurazione di sessioni LDP tra nodi non adiacenti. La sessione T-LDP è creata direttamente tra i punti terminali dello Pseudowire. La Figura 7 rappresenta schematicamente gli elementi del Piano di Controllo del modello Seamless MPLS.

Il modello *Seamless MPLS* permette di disaccoppiare logicamente l'infrastruttura della rete di trasporto dall'architettura logica di servizio, consentendo una più elevata flessibilità nella collocazione dei nodi di servizio, in funzione di fattori quali la tipologia del servizio stesso, la fase di sviluppo ed il grado di penetrazione previsto. Oltre al beneficio di unificazione di tutti i servizi offerti su una stessa tecnologia IP/MPLS, con conseguente semplificazione dei processi di attivazione dei servizi stessi, i vantaggi salienti della soluzione *Seamless MPLS* sono legati alle funzionalità del piano di controllo IP/MPLS. Quest'ultimo consente di realizzare e mantenere in modo automatico e scalabile la connettività *any-to-any* tra qualunque coppia di nodi

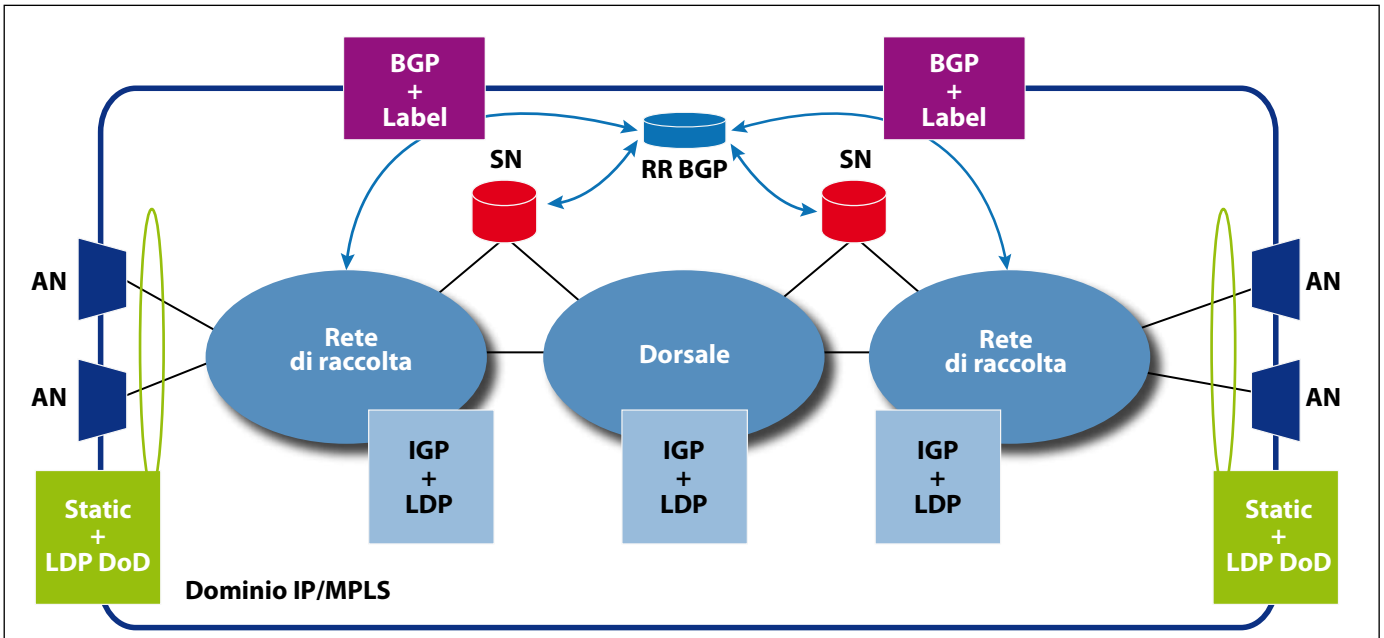


Figura 7 - Piano di controllo della soluzione *Seamless MPLS*

in rete ed è in grado di sfruttare la presenza di cammini multipli tra *sorgente* e *destinazione* sia per distribuire i flussi di traffico tra i vari percorsi (bilanciamento del traffico) e quindi ottimizzare l'utilizzo delle risorse disponibili, sia per re-instradare automaticamente il traffico in caso di guasto in modo rapido (con tempi di re-instradamento anche inferiori a 50ms). L'utilizzo di MPLS nella rete di accesso e aggregazione consente inoltre di superare i limiti di scalabilità legati al numero massimo di identificativi di VLAN disponibili (vale a dire dei servizi trasportabili) ed introduce la possibilità di estendere meccanismi di protezione *end-to-end*, basati su *Pseudowire* fino ai nodi di accesso.

Come emerge da queste considerazioni, l'architettura *Seamless MPLS* mira ad estendere i benefici della tecnologia IP/MPLS ai nodi Accesso, mantenendo però limitata la complessità e di conseguenza i costi di questi apparati, tradizionalmente semplici e presenti in numero molto elevato in rete.

Inoltre il modello *Seamless MPLS* favorisce la creazione di reti *multi-vendor*, grazie alla collaudata interoperabilità del piano di controllo IP/MPLS. Proprio per le sue caratteristiche di semplicità e scalabilità, unite alla possibilità di convergere verso un approccio uniforme nell'erogazione dei servizi di rete, mantenendo allo stesso tempo una notevole flessibilità nel loro dispiegamento, questo modello ha registrato un significativo interesse da parte dell'industria. Alcuni tra i principali Service Provider europei (es. DT, FT-Orange) ed i maggiori costruttori del settore (es. Cisco, Juniper, ALU) si stanno infatti muovendo in questa direzione. L'interesse generale per questo modello architetturale è anche testimoniato dalle numerose attività in corso, in ambito di standardizzazione su questo tema [9] [10][11].

Conclusioni

Le tecnologie per il segmento di Edge IP hanno un ruolo fondamentale nello sviluppo della rete dati fissa. Le evoluzioni tecnologiche e architetturali previste sono importanti per affrontare i problemi che anni e anni di continua crescita hanno inevitabilmente portato.

La sfida principale che gli operatori hanno di fronte è quella di semplificare il PoP. La stratificazione di diverse generazioni tecnologiche ha lasciato in eredità una notevole numerosità di apparati e configurazioni molto articolate. Altro aspetto particolarmente delicato è legato all'esigenza di incrementare l'affidabilità di questo segmento di rete.

Apparati di nuova generazione dotati di grande scalabilità, integrazione di funzioni e soluzioni innovative per gestire la ridondanza sono certamente di grande aiuto in questa sfida. Così come il

modello *Seamless MPLS* può aiutare a definire una soluzione di networking omogenea e più agevole da gestire ■

Acronimi

AAA	Authentication, Authorization & Accounting
ADSL	Asymmetric Digital Subscriber Line
AG	Access Gateway
ATM	Asynchronous Transfer Mode
BBF	BroadBand Forum
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BMG	Banda Minima Garantita
BNAS	Broadband Network Access Server
BNG	Broadband Network Gateway
BP	Banda di Picco
BRT	Banda Real-Time
DoD	Downstream on Demand
DPI	Deep Packet Inspection
DSLAM	Digital Subscriber Line Access Multiplexer
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LDP	Label Distribution Protocol
LLQ	Low Latency Queueing
LSP	Label Switched Path
MC	Mission Critical
MM	Mass Market
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
NC	Network Control
OPB	Optical Packet Backbone
OPM	Optical Packet Metro
OSPF	Open Shortest Path First
PE	Provider Edge
PoP	Point of Presence
PPP	Point-to-Point Protocol
PW	Pseudowire
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RT	Real-Time
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Networking
SOHO	Small Office – Home Office
TIR	Terminazione Intelligente di Rete
ToIP	Telephony over IP
VLAN	Virtual LAN
VPLS	(Virtual Private LAN Service)
VoIP	Voice over IP
VPN	Virtual Private Network
WFQ	Weighted Fair Queueing

Bibliografia

[1] M. Bianchetti, G. Picciano, L. Venuto, "NGN2: la parte metro", Notiziario tecnico Telecom Italia, Anno 17, numero 2, agosto 2008.
[2] http://www.ietf.org
[3] http://www.broadband-forum.org/
[4] https://www.opennetworking.org/
[5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner, "OpenFlow: enabling innovation in campus networks", ACM SIGCOMM Computer Communication Review, Volume 38 Issue 2, April 2008.
[6] M. Billotti, "Come cambiano le piattaforme di rete", Notiziario tecnico Telecom Italia, Anno 19, numero 2, 2010.
[7] K. Kompella, "MPLS in the access", 11th MPLS Conference 2008, Washington, Ottobre 2008.
[8] Y. Rekhter, E. Rosen, "Carrying Label Information in BGP-4", RFC3107, 2001
[9] N. Leymann, B. Decraene, C. Filsfils, M. Konstantynowicz, D. Steinberg, "Seamless MPLS Architecture", draft-ietf-mpls-seamless-mpls-01, 2012
[10] Broadband Forum, "Multi-service Broadband Network Functional Modules and Architecture", WT-145
[11] Broadband Forum, "Multi-service Broadband Network Architecture and Nodal Requirements", WT-178

paolo2.fasano@telecomitalia.it
domenico.marocco@telecomitalia.it
giovanni.picciano@telecomitalia.it

Paolo Fasano
dottore di Ricerca in Ingegneria Elettronica, è in azienda dal 1993 e ha dedicato la propria attività lavorativa all'innovazione delle reti a pacchetto.
Si è inizialmente occupato di reti e servizi a larga banda partecipando alle prime sperimentazioni geografiche a livello europeo di reti in tecnologia ATM (*Asynchronous Transfer Mode*).
Ha spostato successivamente i suoi interessi sui servizi di rete basati sull'Internet Protocol (IP); dal 1995 al 2001 ha partecipato attivamente a numerosi gruppi di lavoro dell'IETF (Internet Engineering Task Force) ed è stato pioniere sul tema IPv6 in Telecom Italia.
È oggi il responsabile della funzione Data Networks Innovation che si occupa dell'innovazione relativa al backbone IP/MPLS, alla rete metro regionale multi-servizio e alle piattaforme di Edge IP fisso, residenziale e business.

Domenico Marocco
laureato in Ingegneria Elettronica, è entrato in Azienda nel 1987. Ha collaborato a diversi progetti sia in ambito Rete che nell'allora Direzione Business, contribuendo allo sviluppo delle maggiori reti dati pubbliche (ATM, Interbusiness, OPB, GBE, ecc.) e dell'Intranet aziendale (Rete Dati di Gruppo - Dacon).
Dopo aver ricoperto diversi ruoli, oggi è responsabile della Funzione IP Edge & Services Engineering in ambito Tilab.

Giovanni Picciano
ingegnere elettronico, presso l'Università La Sapienza di Roma, dal 1996 opera nell'area Technology della Direzione Generale di Telecom Italia dove fino al 2002 ha curato le attività di industrializzazione dei sistemi di gestione per le reti di trasporto (SDH e WDM) e successivamente ha coordinato le attività di industrializzazione degli apparati per reti metropolitane e regionali in tecnologia xWDM, Ethernet, IP e MPLS. Nel 2006 ha assunto la responsabilità della funzione Wireline Access Engineering, in ambito Telecom Italia Lab, con il compito di assicurare le attività di ingegnerizzazione della rete di accesso e di aggregazione metro-regionale di Telecom Italia (OPM). Dal 2011 Oggi è responsabile della funzione Wireline Access Innovation and Engineering che include anche la responsabilità delle attività di innovazione in rete di accesso principalmente in ambito NGAN e nuove tecniche di trasmissione su portanti rame.