
**UNIVERSITÀ POLITECNICA DELLE MARCHE**

---

**Corso di Laurea in Ingegneria Elettronica**

# Evoluzione di reti intranet in ambito aziendale

# Enterprise intranet evolution

Relatore:
Prof. **Ennio Gambi**

Tesi di laurea di:
**Mario Federici**

Correlatore
Ing**. Adelmo De Santis**

---

*A.A. 2018/2019*

INDICE DEGLI ARGOMENTI

1. INTRODUZIONE ..... 8

1.1 INTRANET INTESO A LIVELLO LOGICO ..... 8

1.2 INTRANET INTESO A LIVELLO INFRASTRUTTURALE ..... 9

2. LE PRIME RETI INTRANET DAL 1994 AL 2000 ..... 11

2.1 LAN (LOCAL-AREA NETWORK) ..... 11

2.2 PRIME LAN A BUS SU MEZZO FISICO ..... 12

2.3 LAN ATTESTATE SU APPARATI ..... 13

3. MODELLO DI RIFERIMENTO PER INTERCONNESSIONE FRA SISTEMI ..... 16

3.1 PROTOCOLLI DI COMUNICAZIONE A LIVELLO 2 ..... 18
3.1.1 CONNESSIONE PUNTO-PUNTO CON PROTOCOLLO HDLC ..... 18
3.1.2 RETI GEOGRAFICHE CON PROTOCOLLO FRAME-RELAY ..... 18
3.1.3 RETI GEOGRAFICHE CON PROTOCOLLO ATM ..... 21

4. LE WAN E LA COMUNICAZIONE IN UN TERRITORIO ..... 26

4.1 RETE DATI GEOGRAFICA ..... 26
4.1.1 ROUTER ..... 29

5. MPLS PER LA RAZIONALIZZAZIONE DELLE RETI ..... 32

5.1 MOLTEPLICITÀ DI RETI GEOGRAFICHE ..... 32

5.2 COME NASCE MPLS ..... 33

5.3 ARCHITETTURA MPLS ..... 34
5.3.1 COMMUTAZIONE DI ETICHETTA: LA COMPONENTE DI FORWARDING ..... 35
5.3.2 COMMUTAZIONE DI ETICHETTA IN MPLS: LA COMPONENTE DI CONTROLLO ..... 38
5.3.3 LABEL SWITCHED PATH ..... 40
5.3.4 CENNI SU MECCANISMO EQUIVALENTE MPΛS (MULTIP. LAMBDA SWITCHING) ..... 41

5.4 APPLICAZIONI ..... 41
5.4.1 MPLS TRAFFIC ENGINEERING ..... 42
5.4.2 RETI PRIVATE VIRTUALI MPLS/IP ..... 42
5.4.3 MPLS E LA DIFFERENZIAZIONE DEI SERVIZI (DIFFSERV) ..... 47
5.4.4 IL RIPRISTINO VELOCE DI MPLS (FAST REROUTING) ..... 49
5.4.5 SERVIZI CHE UNA TELCO PUÒ OFFRIRE CON USO DI MPLS) ..... 50
5.4.6 ARCHITETTURA INTRANET CON VPN MPLS ..... 50

6. LE RETI DATI VERSO RETI “FULL IP” ..... 52

6.1 LA SUDDIVIZIONE IN SEGMENTI DELLE RETI DATI ..... 53

6.2 I SERVIZI DATI ..... 54
6.2.1 CLIENTI BUSINESS ..... 55

6.2.2 CLIENTI RESIDENZIALI E SMALL BUSINESS ..... 57

6.3 EVOLUZIONE DEGLI APPARATI E NUOVE ARCHITETTURE DI RETE ..... 60
6.3.1 EVOLUZIONE DELLE TECNOLOGIE EDGE ..... 60
6.3.2 MODELLO SEAMLESS MPLS ..... 61

7. INTEGRAZIONE FRA LA RETE IP E LA RETE DI TRASPORTO OTTICA ..... 66

7.1 LA RETE IP E LA RETE DI TRASPORTO OTTICA ..... 66

7.2 L'INTEGRAZIONE DELLA RETE IP CON LA RETE OTTICA ..... 68

7.3 IMPIEGO DI INTERFACCE OTTICHE COLORATE SUI ROUTER ..... 69

7.4 INTEGRAZIONE A LIVELLO DI PIANO DI CONTROLLO CON GMPLS UNI ..... 71
7.4.1 L'INTERFACCIA GMPS UNI ..... 72

7.5 INTEGRAZIONE MEDIANTE TRANSPORT SDN ..... 73

8. RICONFIGURABILITÀ NELLE RETI ACCESS E METRO ACCESS ..... 76

8.1 L'EVOLUZIONE DEL TRAFFICO NELLE RETI DI ACCESS ..... 76

8.2 RICONFIGURABILITÀ A LIVELLO FISICO ..... 76

8.3 CONVERGENZA METRO-ACCESS ..... 79

9. ARCHITETTURE DI RETE DI ACCESSO FISSO ..... 82

9.1 TECNOLOGIE IN RAME INNOVATIVE IN RETE DI ACCESSO ..... 84

9.2 TECNOLOGIE OTTICHE INNOVATIVE IN RETE DI ACCESSO ..... 87

10. LE RETI AZIENDALE E LE NUOVE TECNOLOGIE. ..... 90

10.1 SOLUZIONI PER COLLEGARE LE SEDI DISTRIBUITE NEL TERRITORIO ..... 90
10.1.1 CANALI DIRETTI NUMERICI CDN ..... 90
10.1.2 CANALI CIFRATI ALL'INTERNO DELLA INTERNET (VPN IPSec ) ..... 91
10.1.3 RETE MPLS (MULTI PROTOCOL LABEL SWITCHING) ..... 92

10.2 CONSIDERAZIONI CHE PORTANO A PREFERIRE LA SOLUZIONE IP MPLS. ..... 92

10.3 IP MPLS: OFFERTE COMMERCIALI PROPOSTE DALLE TELCO ..... 93
10.3.1 PROPOSTE COMMERCIALI PER SERVIZIO MPLS OFFERTE DA TIM ..... 95
10.3.2 PROPOSTE COMMERCIALI PER SERVIZIO MPLS DA FASTWEB ..... 95

LISTA DEGLI ACRONIMI

| | |
|---|---|
| AAA | Authentication, Authorization & Accounting |
| AAL ATM | Adaptation Layer |
| ADSL | Asymmetric Digital Subscriber Line |
| AG | Access Gateway |
| API | Application Programming Interface |
| AS | Assigned Number |
| ATM | Asynchronous Transfer Mode |
| ARIS: | Aggregate Route-Based Switching |
| BB | BackBone |
| BBF | BroadBand Forum |
| BFD | Bidirectional Forwarding Detection |
| BGP | Border Gateway Protocol |
| BGPv4 | Border Gateway Protocol version 4 |
| BGP-LS | Border Gateway Protocol – Link State |
| BMG | Banda Minima Garantita |
| BNAS | Broadband Network Access Server |
| BNG | Broadband Network Gateway |
| BP | Banda di Picco |
| BRT | Banda Real-Time |
| CE | Customer Edge |
| CO | Central Office |
| CoS | Class of Service |
| CPE | Customer Premises Equipment |
| CR-LDP | Constraint-based Routing – LDP |
| DCE | Data Communications Equipment |
| DLCI | Data Link Connection Identifier |
| DTE | Data Terminal Equipment |
| DoD | Downstream on Demand |
| DPI | Deep Packet Inspection |
| DSLAM | Digital Subscriber Line Access Multiplexer |
| E-LSP | Exp. inferred Label Switched Path |
| E-LSR | Edge-Label Switch Router |
| ER | Explicit Route |
| ERO | Explicit Route bject O |
| FCS | Frame Check Sequence |
| FEC | Forwarding Equivalence Class |
| FEC | Forward Error Correction |
| FT | Forwarding Table |

| | |
|---|---|
| GMPLS | Generalized MultiProtocol Label Switching |
| IETF | Internet Engineering Task Force |
| IGP | Interior Gateway Protocol |
| IGRP | Interior Gateway Routing Protocol |
| IP | Internet Protocol |
| IPLPDN | IP over Large Public Data Network |
| ISP | Internet Service Provider |
| ITU | International Telecommunications Union |
| LAG | Link Aggregation Group |
| LAN | Local Area Network |
| LDP | Label Distribution Protocol |
| LIB | Label Information Base |
| LIFO | Last In uFtirst O |
| LMP | Link Management Protocol |
| LLQ | Low Latency Queueing |
| LSP | Label Switched Path |
| L-LSP | Label inferred Label Switched Path |
| LSR | Label Switch Router |
| MAC | Medium Access Control |
| MAN | Metropolitan Area Network |
| MC | Mission Critical |
| MM | Mass Market |
| API | Application Program Interface |
| AWG | Array Waveguide Grating |
| BoD | Bandwidth on Demand |
| CDN | Content Delivery Network |
| CMOS | Complementary Metal Oxide Semiconductor |
| CO | Central Office |
| CPE | Customer Premises Equipment |
| DWDM | Dense Wavelength Division Multiplexing |
| DPU | Distribution Point Unit |
| EDFA | Erbium Doped Fiber Amplifier |
| FEC | Forward Error Correction |
| FEXT | Far End Cross Talk |
| FTTCab | Fiber To The Cabinet |
| FTTdp | Fiber To The distribution point |
| FTTE | Fiber To The Exchange |
| FTTH | Fiber To The Home |
| GPON | Gigabit-capable Passive Optical Network |
| IaaS | Internet as a Service |
| IoT | Internet of Things |
| IPoWDM | Internet Protocol over Wavelength Division Multiplexing |

| | |
|---|---|
| LAN | Local Area Network |
| LCoS | Liquid Crystal on Silicon |
| LTE | Long Term Evolution |
| LTE-A | Long Term Evolution – Advanced |
| MARIN | Metro Access Rings Integrated Network |
| MEMS | Micro Electro Mechanical Systems |
| MP-BGP | MultiProtocol BGP |
| MPLS | MultiProtocol Label Switching |
| MP□S | MultiProtocol Lambda Switching |
| MPOA | MultiProtocol Over ATM |
| NAT | Network Address Translation |
| NC | Network Control |
| NE | Network Element |
| NFV | Network Functions Virtualization |
| NGCN | Next Generation Core Network |
| NHLFE | Next Hop Label Forwarding Entry |
| NHRP | Next Hop Resolution Protocol |
| NMS | Network Management System |
| NNI | Network to Network Interface |
| OAM | Operation Administration and Management |
| OBS | Optical Burst Switching |
| OCS | Optical Channel Switching |
| OEO | Optical/Electrical/Optical |
| OFS | Optical Flow Switching |
| OLS | Optical Label Switching |
| OLT | Optical Line Termination |
| OMP | Optimized MultiPath |
| ONF | Open Networking Forum |
| ONT | Optical Network Termination |
| ONU | Optical Network Unit |
| OPB | Optical Packet Backbone |
| OpEx | Operational Expenditures |
| OPM | Optical Packet Metro |
| OSPF | Open Shortest Path First |
| OPS | Optical Packet Switching |
| OSS | Operation Support System |
| P | Provider (Router) |
| PCE | Path Computation Element |
| PCEP | Path Computation Element Protocol |
| PE | Provider Edge (Router) |
| PHB | Per Hop Behaviour |
| PON | Passive Optical Network |

| | |
|---|---|
| PoP | Point of Presence |
| PPP | Point to Point Protocol |
| PVC | Permanent Virtual Circuit |
| QoE | Quality of Experience |
| QoS | Quality of Service |
| RD | Route Distinguisher |
| REST | REpresentational State Transfer |
| RFC | Request For Comment |
| RN | Remote Node |
| ROADM | Reconfigurable Optical Add Drop Multiplexer |
| ROLC | Routing Over Large Clouds |
| RPF | Reverse Power Feeding |
| RSOA | Reflective Semiconductor Optical Amplifier |
| RSVP | Resourse reSerVation Protocol |
| RSVP-TE | ReSerVation Protocol – Traffic Engineering |
| SARDANA | Scalable Advanced Ring Dense Access Network Architecture |
| SDN | Software Defined Network |
| SOI | Silicon On Insulator |
| SRLG | Shared Risk Link Group |
| TCP | Transmission Control Protocol |
| TDM | Time Division Multiplexing |
| TE | Traffic Engineering |
| TED | Traffic Engineering Database |
| TOS | Type Of Service |
| T-SDN | Transport Software Defined Network |
| TDD | Time Division Duplexing |
| UDP | User Datagram Protocol |
| UNI | User to Network Interface |
| VDSL | Very-high speed Digital Subscriber Line |
| VLAN | Virtual Local Area Network |
| VNF | Virtual Network Function |
| VNTP | Virtual Network Topology Manager |
| VPI/VCI | Virtual Path Identifier / Virtual Circuit Identifier |
| VPN | Virtual Private Network |
| VRF | Virtual Routing Forwarding |
| WAN | Wide Area Network |
| WDM | Wavelength Division Multiplexing |
| WSS | Wavelength Selective Switch |

# 1. INTRODUZIONE

Il concetto di intranet risale al 1994, anno in cui Steven Telleen concepì il termine. Alcuni anni dopo, in un'intervista, il ricercatore dirà: "Quando coniugai il termine IntraNet alla Amdahl, nell'estate del 1994, questo sembrava più un Web interno, che un'Internet interna. Infatti il termine che usavamo tra di noi, prima, era l'ingombrante Enterprise Wide Web. Si è usata la parola intranet per definire un'infrastruttura, basata sugli standard e sulle tecnologie di Internet, che condivide informazioni e contenuti all'interno di un gruppo limitato e ben definito. L'infrastruttura si riferiva alla matrice organizzativa e gestionale volta a creare, gestire e condividere i contenuti. L'unica limitazione tecnica era che la rete fisica doveva basarsi sull'Internet Protocol (IP)".

Due modi di intendere il termine intranet.

## 1.1 INTRANET INTESO A LIVELLO LOGICO

Il termine intranet inteso a livello logico, si riferisce alla rete di servizi, al sistema di siti che formano uno spazio web interno (ad esempio a un'azienda o ad una organizzazione). Il termine può essere anche inteso come il sistema di informazioni e servizi di utilità generale accessibili dalla rete interna.

Nella concezione più comune di intranet viene previsto un Corporate Portal come punto di ingresso ad applicazioni specifiche, quali:

- Publishing: pubblicazione, personalizzazione e visualizzazione dei contenuti sull'intranet, realizzando la comunicazione monodirezionale di contenuti verso il personale;
- Document management: supporto all'acquisizione ed alla gestione della conoscenza esplicita, con funzioni di archiviazione, indicizzazione, correlazione e ricerca;
- Community: supporti alla comunicazione e all'interazione tra utenti attraverso servizi interattivi (forum, mailing list, instant messaging, chat etc), finalizzati alla gestione della conoscenza implicita all'interno dell'azienda;
- Collaborative work: supporto alla collaborazione e al teamworking (ad esempio groupware, e-room, videoconferenze etc);
- Legacy integration: supporto all'accesso ai sistemi informativi aziendali, ai dati e alle procedure dei sistemi gestionali e di tutti gli altri applicativi in azienda;
- Self Service: funzionalità in grado di erogare servizi interattivi ai dipendenti, come e-learning, rubrica del personale, modulistica, help desk informatico etc.

Nel rapporto 2006 dell'Osservatorio permanente sulle Intranet della School of Management del Politecnico di Milano, emerge come le Intranet mostrano segnali di evoluzione verso una prospettiva nuova ed ambiziosa. Pur conservando la loro natura di strumenti incentrati sulla persona, le Intranet avanzate integrano nuovi strumenti di comunicazione e collaborazione e si fondono con altri Sistemi Informativi tradizionali per creare i Virtual Workspace in cui scambiare idee/documenti e collaborare su progetti. La intranet favorisce la comunicazione interna, cosa necessaria specie quando si dispone di telelavoratori, lavoratori fuori sede, dipendenti che si spostano di frequente. Una intranet è il mezzo ideale per pubblicare rapporti settimanali, promemoria; per dare vita a bacheche virtuali, messaggistica immediata e chat moderate. Intranet rappresenta la concezione della comunicazione in azienda, della trasparenza dei processi burocratici, della condivisione della conoscenza, della riduzione del lavoro inutile.

Le intranet divengono così uno dei pilastri della ristrutturazione organizzativa, sia per facilitare altri cambiamenti e sia per migliorare la velocità e la flessibilità dell'azienda stessa.

## 1.2 INTRANET INTESO A LIVELLO INFRASTRUTTURALE

Il termine intranet inteso a livello a livello infrastrutturale si riferisce a una rete aziendale privata che utilizza il protocollo TCP/IP e può estendersi con collegamenti WAN e VPN. Spesso tale rete o è completamente isolata dalla Rete Internet esterna (es. LAN), rimanendo a solo uso interno, oppure comunica eventualmente con la rete esterna e le altre reti, attraverso opportuni sistemi di comunicazione e relativa protezione (come ad esempio un firewall).

Quando una parte della intranet viene resa accessibile a clienti venditori, fornitori, partner o altre entità esterne all'organizzazione, tale quota parte diventa una extranet che si configura quindi come un sottoinsieme di una intranet.

A distanza di quasi 25 anni dall'avvento della prima intranet, stiamo assistendo a una sua ristrutturazione con l'ausilio di nuove tecnologie per crearne una versione più efficiente.

Le prime intranet nella seconda metà degli anni 90' complicate, e poco sicure richiedevano un server separato, assistenza, manutenzione costante.

In questo documento ci si propone di mostrare come la struttura della rete intranet si sia evoluta nel corso di questi 25 anni e indicare quali siano le prospettive di sviluppo, considerando l'evoluzione

degli apparati che ne costituiscono i nodi di rete , quello del trasporto che permette le connessioni tra i nodi e quello dei sistemi informativi cui fa riferimento la rete.

.

# 2. LE PRIME RETI INTRANET DAL 1994 AL 2000

## 2.1 LAN (LOCAL-AREA NETWORK)

Una LAN è un sistema di comunicazione condiviso che permette ad apparecchiature indipendenti di comunicare tra di loro entro un'area delimitata, utilizzando un unico canale fisico a velocità elevata e con basso tasso di errore.

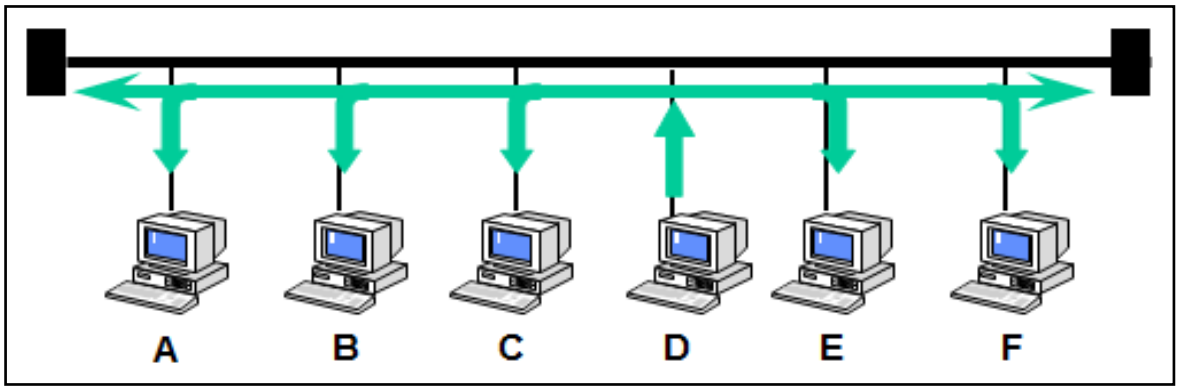



Figura 1 – Apparati su messo trasmissivo condiviso

Il termine LAN (local-area network) definisce una tipologia di rete, o di parte di una rete, in cui i vari dispositivi che ne fanno parte sono tutti dislocati nell'ambito dello stesso edificio o al massimo in più edifici contigui (distanze nell'ordine delle centinaia di metri).

Le LAN hanno dimensioni contenute il che favorisce il tempo di trasmissione che è noto. Le LAN tradizionali lavorano tra 10 Mbps a 100 Mbps, hanno bassi ritardi e pochissimi errori. Mentre le LAN recenti operano fino a 100 Gbps.

Le LAN sono configurabili con differenti tipologie. Le due più utilizzate sono:

- Bus;
- Anello.

Nella LAN a bus, quella che ha avuto la massima diffusione, in ogni istante è master (quindi può trasmettere) una sola macchina, tutte le altre devono attendere che il bus si liberi. Una tipica rete a bus è la Ethernet che è una rete broadcast con controllo non centralizzato.

Per regolamentare l'accesso al mezzo trasmissivo era stato adottato un protocollo di tipo CSMA/CD (Carrier Sense Multiple Access / Collision Detect).

Dove la funzione Collision Detect evita di perdere i messaggi nel caso in cui due apparecchiature inizino a trasmettere nello stesso istante

## 2.2 PRIME LAN A BUS SU MEZZO FISICO

Le prime reti LAN erano basate sulla condivisione del un mezzo fisico rappresentato dal cavo coassiale al quale venivano riportati gli host e un eventuale server.

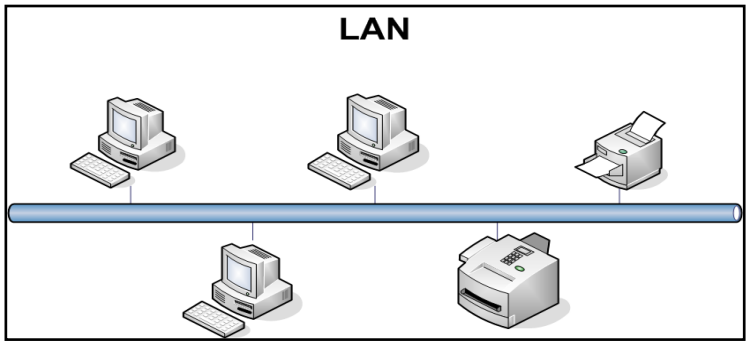



Figura 2 - LAN con host connessi a un cavo Coassiale (detto: BUS).

Per collegare l'host al cavo coassiale si usava una derivazione a T terminata BNC.

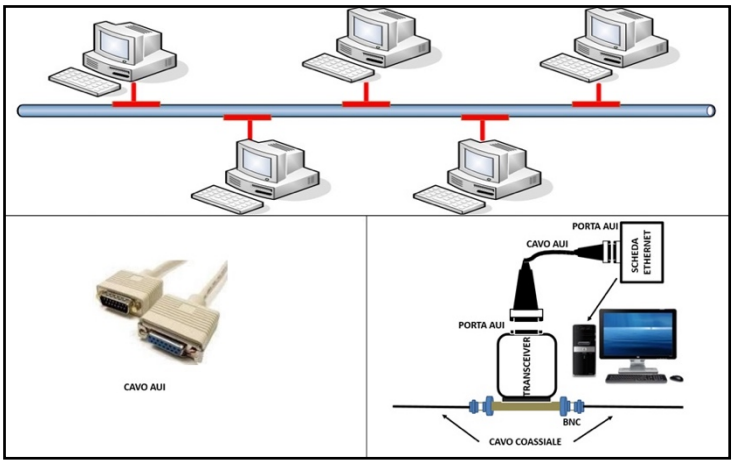



Figura 3 – Connessione degli host alla lan 10Base5 con connettore a T

La rete prendeva la denominazione di "10 Base 5" dove "5" indicava che 500 metri era la massima lunghezza per ciascun segmento.

Il Transceiver veniva innestato sul cavo coassiale e si occupava di trasmettere e ricevere le trame sul mezzo fisico e rilevare le collisioni.

Si riportano in fig. 4 i diversi standard di livello fisico nei quali si fa uso di transceiver.

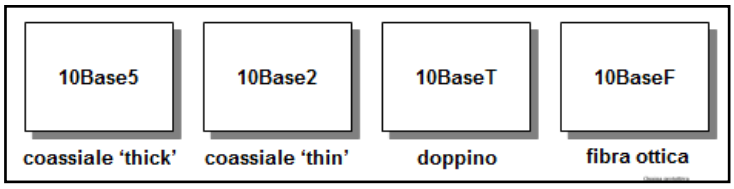



Figura 4 - Standard di livello fisico

Il livello fisico del modello ISO/OSI, 802.3 prevede esclusivamente trasmissioni via cavo in banda base, a velocità di 10, 100 e 1000 Mbps, su cavi coassiali, doppini intrecciati (schermati e non) e fibre ottiche. Queste e altre caratteristiche sono riassunte negli acronimi usati per le varie implementazioni del livello fisico, tutti del tipo NBaseA, essendo N la velocità di trasmissione, Base indica che l'implementazione opera in banda base, ed A è una sigla legata al tipo di cavo utilizzato e ad altre caratteristiche salienti.

Di seguito sono illustrate brevemente alcune di queste implementazioni:

- 100Base-TX - (Fast Ethernet);
- 100Base-FX - come 100Base-TX, ma su fibra ottica multimodale in prima finestra;
- 1000Base-SX - Fibra ottica multimodale in prima finestra, distanze fino a 275m o 550m a seconda del tipo di fibra;
- 1000Base-LX - Fibra ottica monomodale in seconda finestra, distanze fino a 5km (secondo lo standard) o 10km (secondo molti produttori);
- 1000Base-T.

## 2.3 LAN ATTESTATE SU APPARATI

Presto si passa dalla condivisione di un mezzo fisico (bus) alla condivisione di apparati. Il cavo coassiale aveva problemi di gestione, era difficile da stendere ed era costoso. La ricerca ha portato un sistema più pratico: l'HUB.

L'HUB mette a disposizione prima porte BNC poi porte RJ45 su cui collegare gli apparati.

Figura 5 - hub 8 porte RJ45

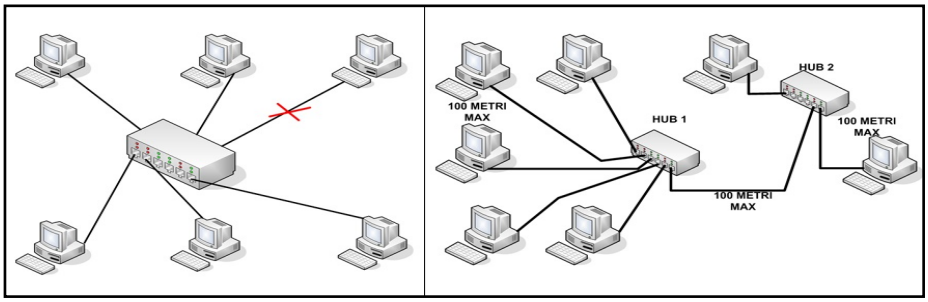



Figura 6 – Connessione di host mediante uno o più hub

La distanza massima del cavo UTP tra il computer e l'hub o fra due hub è di 100 metri, e la rete LAN che si ottiene appartiene al proprio Dominio di Collisione (Collision-Domain). Uno dei vantaggi è che si interrompe un ramo della LAN non pregiudica il resto. L'HUB è un apparato che smista dati di una comunicazione ancora organizzata con tipologia logica a bus.

Le sue funzioni principali sono le seguenti:

- ripete le frames ricevute su un segmento e le trasmette sugli altri segmenti;
- decodifica le frames ricevute su una porta e le ricodifica sulle altre porte ritemporizzando quindi tutti i bit da trasmettere;
- si occupa della gestione delle collisioni;
- può opzionalmente isolare una porta, per un determinato periodo di tempo, quando su questa si verificano più di 30 collisioni consecutive.

L'evoluzione porta alla sostituzione dell'hub con lo switch, apparato che trasmette la trama ricevuta da una qualsiasi delle proprie porte, solo su quella che permette di raggiungere il destinatario della trama stessa (identificato dall'indirizzo MAC).

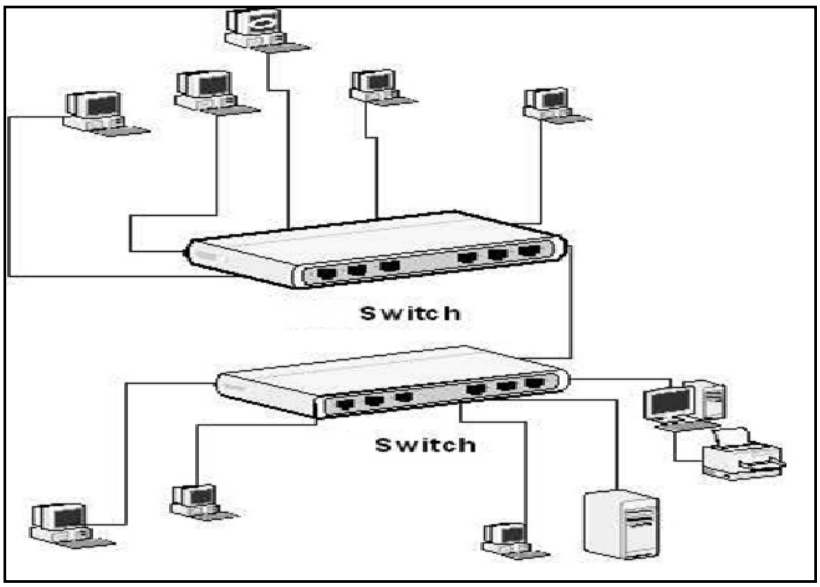



Figura 7 - Connessione di host mediante uno o più switches

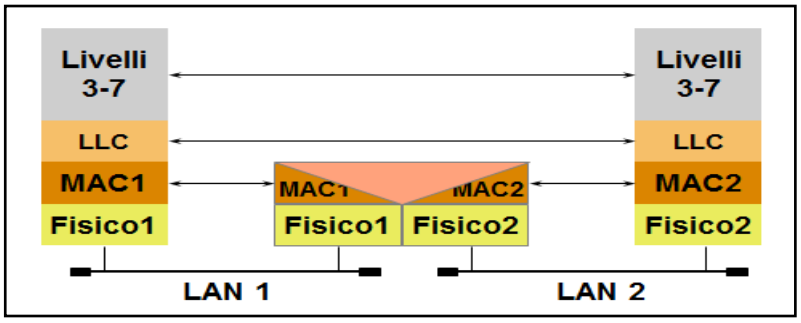



Figura 8 – Switch su cui coesistono due domini di collisione

## 3. MODELLO DI RIFERIMENTO PER INTERCONNESSIONE FRA SISTEMI

Per sviluppare gli standard di interconnessione fra Sistemi (Sistemi = insiemi di elaboratori, relativo software, periferiche, terminali, processi ecc.) si fa uso di un modello come base comune: il Modello di riferimento OSI (Open System Interconnection, vedi fig. 9 e tab. 1).

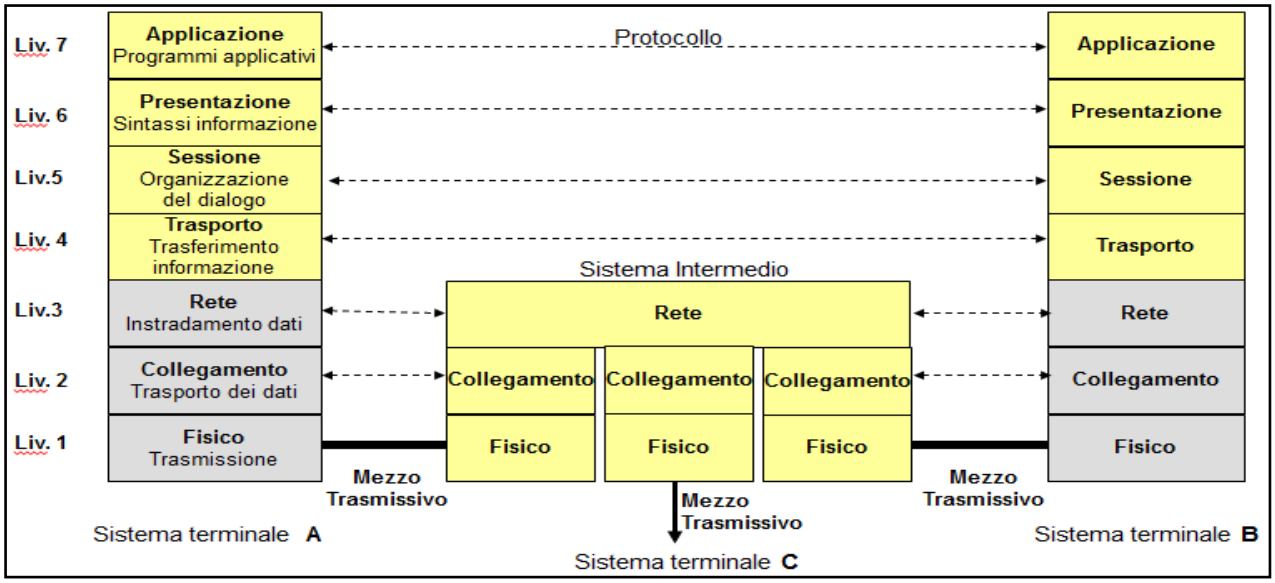



Figura 9 – Modello OSI

Tab 1 – Descrizione dei livelli del Modello OSI

| Liv. | Denominazione | Descrizione |
|---|---|---|
| 7 | Applicazione | E' il livello dei programmi applicativi attraverso i quali l'utente finale utilizza la rete. Esempi di tali applicativi: VT (Terminale Virtuale) cioè connessione ad un elaboratore remoto; X.400 (la posta elettronica) |
| 6 | Presentazione | Gestisce la sintassi dell'informazione da trasferire (ad esempio codifica ASCII o esadecimale). |
| 5 | Sessione | Questo livello è responsabile dell'organizzazione del dialogo tra due applicativi e del conseguente scambio di dati. |
| 4 | Trasporto | Provvede a fornire il trasporto dei dati con la massima affidabilità, esegue la rilevazione e correzione di errori. |
| 3 | Rete | Il livello 3 offre la connettività e la selezione del percorso dei dati. A questo livello avviene l'instradamento. |
| 2 | Data Link | Al livello 2 si preparano i dati da trasmettere in rete su mezzo fisico. Effettua la verifica di eventuali errori gestisce la correzione di tali errori tramite ritrasmissioni. |

| | | |
|---|---|---|
| 1 | Fisico | In questo livello avviene la trasmissione delle sequenze binarie sul canale di comunicazione. Vengono definite le specifiche elettriche, meccaniche e funzionali dei collegamenti fisici tra sistemi. |

IEEE ha prodotto diversi standard per le LAN, collettivamente noti come IEEE 802, tra i quali:

- Specifiche generali del progetto (802.1);
- Logical Link Control, LLC (802.2);
- CSMA/CD (802.3).

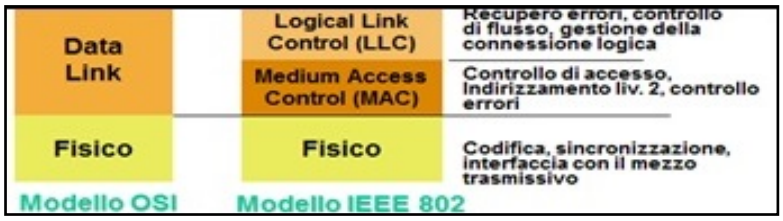



Figura 10 - Confronto IEEE 802 con la pila OSI

Il livello MAC è di fondamentale importanza nelle reti di tipo broadcast, in cui ogni sistema riceve tutte le trame inviate dagli altri.

Trasmettere in broadcast implica la soluzione di due problemi:

- in trasmissione: per determinare chi deve/può utilizzare il canale si usa protocollo di tipo CSMA/CD (Carrier Sense Multiple Access / Collision Detect);
- in ricezione: per discriminare quali messaggi sono destinati alla stazione si fa uso di indirizzi MAC.

## 3.1 PROTOCOLLI DI COMUNICAZIONE A LIVELLO 2

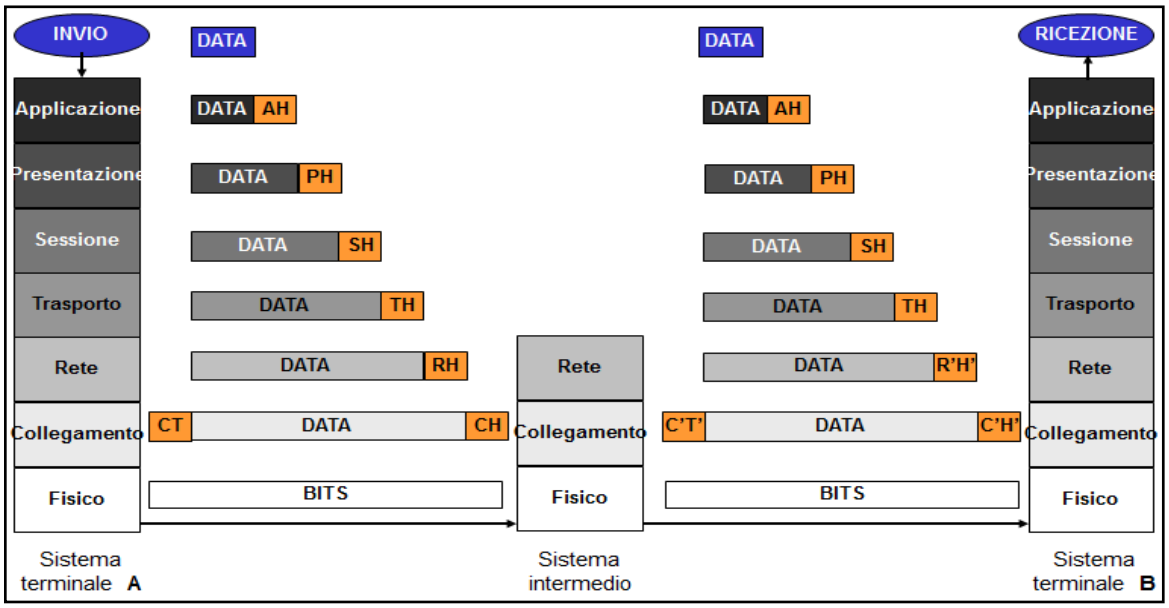



Figura 11 – Livelli OSI e Protocolli di comunicazione.

Al livello 2, Data Link (collegamento e trasporto dei dati), si fa uso dei protocolli:

- HDLC;
- Frame Relay;
- ATM.

### 3.1.1 CONNESSIONE PUNTO-PUNTO CON PROTOCOLLO HDLC

Il protocollo HDLC è utilizzato per le connessioni punto-punto;

### 3.1.2 RETI GEOGRAFICHE CON PROTOCOLLO FRAME-RELAY

Il protocollo FR realizza il collegamento logico tra l'interfaccia di utente e quella di rete. Non necessita di instaurazione di chiamata in quanto tutte le connessioni sono di tipo permanente. Periodicamente (normalmente ogni 10 secondi) l'utente richiede l'integrità del protocollo verso la porta di rete. Non implementa nessun contatore quindi non riscontra mai l'arrivo del messaggio a destinazione.

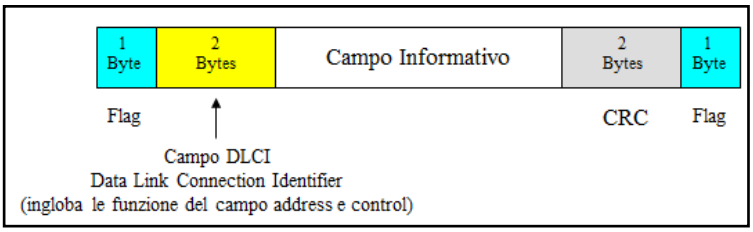



Figura 12 – Trama Frame-Relay

La lunghezza del campo informativo è variabile fino ad un massimo di 4096 bytes.

Il servizio Frame Relay usa una struttura di protocolli che prevede le seguenti funzioni:

- Livello 1:

il livello fisico del Frame Relay rappresenta ancora l'integrità del collegamento elettrico e meccanico tra il terminale d'utente e la terminazione di rete

La velocità massima di esercizio è di 2Mbit/sec. Consente di avere molteplici soluzioni n*64Kbit/sec. sino al completo riempimento del 2Mbit/sec.

- Livello 2:

Il livello Data-Link o Frame Relay, prevede il trasferimento di trame Frame-Relay tra due DTE. Le suddette trame vengono instradate secondo un indirizzo di trama denominato DLCI (Data Link Connection Identifier). Non essendo previsti riscontri, non c'è richiesta di ritrasmissione, non esiste una numerazione sequenziale delle trame, Il trasmittente inserisce un campo di controllo FCS in modo che il DTE ricevitore possa verificare l'integrità di trama (la trama non conforme viene scartata), in caso di congestione la trama viene scartata, nessuna notifica degli errori. L'abolizione dei meccanismi di riscontro e/o rigetto consente di raggiungere velocità elevate.

Ciascuna trama viene instradata all'interno della rete in base al suo DLCI.

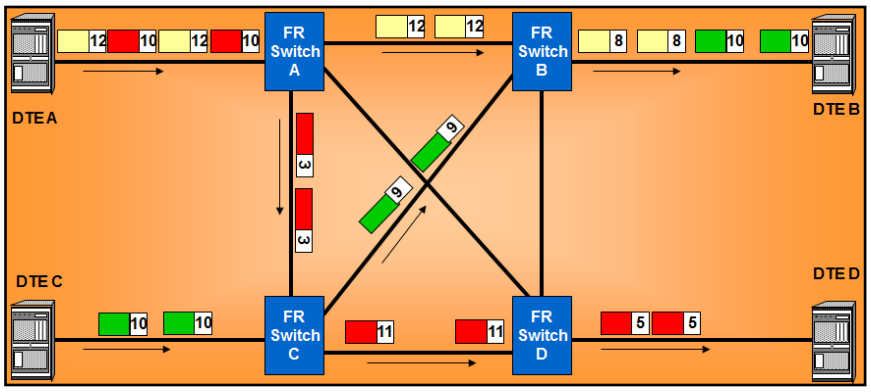



Figura 13 - Trame instradate secondo un indirizzo di trama denominato DLCI

Il DLCI ha validità solamente locale utente-rete, quindi un PVC tra un utente A ed utente B, può essere caratterizzato da un DLCI diverso sulle due interfacce. È compito della rete instradare correttamente i DLCI.

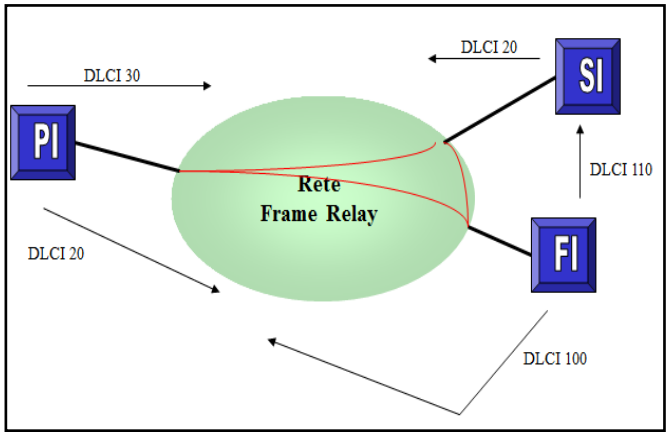



Figura 14 - Tipo di indirizzamento e la commutazione dei DLCI

I numeri dei DLCI da utilizzare vengono stabiliti all'atto della sottoscrizione del PVC. Le connessioni Frame Relay si possono multiplare; all'interno della trama il campo DLCI caratterizza quella particolare connessione logica nel collegamento utente-rete.

L'accesso di livello 1 (o circuito trasmissivo) è del tipo permanente, quindi la connessione fisica viene stabilita su base contrattuale. La rete è responsabile del mantenimento della connessione fisica. Il protocollo di livello 1 è regolato dalle raccomandazioni della serie V e precisamente:

- V.24 per velocità fino a 9600 bit/sec;
- V.35 per velocità superiori fino a 2Mbit/sec;
- G.703 / G.704 per velocità n*64 fino a 2Mbit/sec.

Generalmente ogni N scambi di messaggi "Status Enquiry"/ "Status" il DTE invia alla rete una richiesta di "Full Status Enquiry", alla quale il DCE risponde con "Full Status". Tale scambio dei messaggi serve oltre che a verificare lo stato del link UNI, anche a riportare lo stato dei DLCI configurati sull'interfaccia UNI (User to Network Interface).

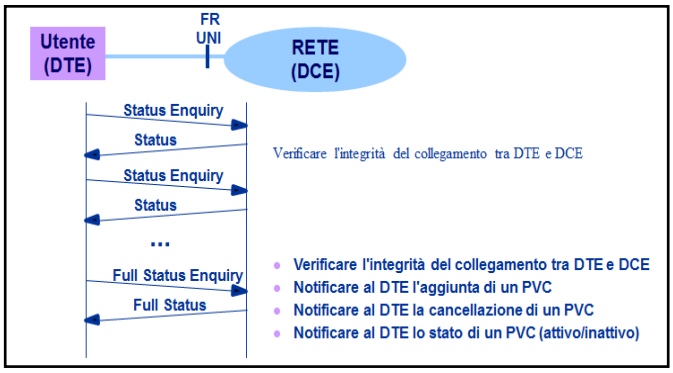



Figura 15 - Scambio di messaggi "Status Enquiry"/"Status"

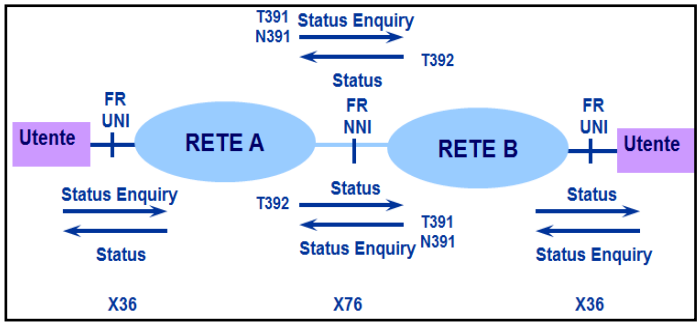



Figura 16 – Connessione fra utenti attraverso reti FR

I messaggi di PVC Management sono trasmessi su DLCI riservati in base allo standard implementato:

- ANSI T1.617 Annex D (Canada ed USA) DLCI = 0
- ITU-T Q.933 Annex A (Europa) DLCI = 0
- LMI (Cisco) DLCI = 1023

### 3.1.3 RETI GEOGRAFICHE CON PROTOCOLLO ATM

La crescita di applicazioni multimediali e delle esigenze degli utilizzatori, già nei primi anni 2000, ha reso necessario un adeguamento delle prestazioni di rete, in termini di velocità e banda passante.

Si osservava già un numero crescente di LAN che necessariamente dovevano essere collegate tra loro con reti geografiche.

Si era alla ricerca di buone prestazioni in termini di basso ritardo, alta velocità ed affidabilità.

L'implementazione del protocollo Frame-Relay aveva parzialmente risolto il problema di interconnessione a lunga distanza, ma la limitazione della velocità a 2Mb/s non permetteva l'accesso se non ad un numero ristretto di utenti.

In questo contesto si è inserito ATM (Asyncronous Transfer Mode) che unitamente alla velocità più elevata, permetteva di gestire (mezzo fisico permettendo) in maniera ottimale i ritardi di trasmissione. A differenza del protocollo FR dove la lunghezza dei messaggi era variabile, nel protocollo ATM ogni messaggio aveva una lunghezza fissa stabilita dagli enti di standardizzazione in 53 bytes, denominata "cella".

Il controllo di errore era effettuato solo sull'intestazione della cella ATM, mentre il recupero degli stessi era demandato ai livelli di adattamento superiori.

Tutte le suddette caratteristiche hanno fatto di ATM un protocollo estremamente potente e veloce.

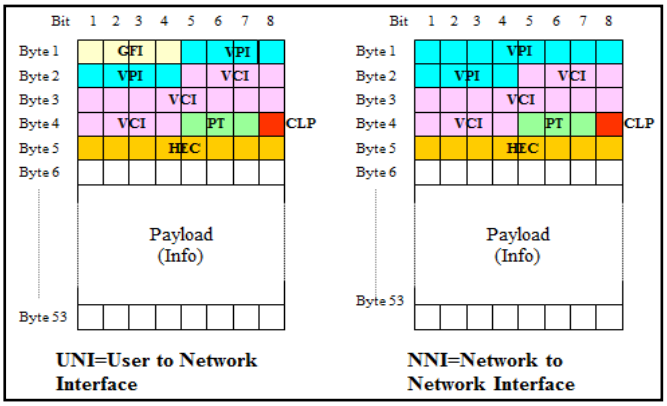



Figura 17 - Protocollo ATM – Formato Celle UNI - NNI

I campi riportati in fig. 17 hanno il significato:

| Campo | significato |
|---|---|
| GFI | General Format Identifier ; non ancora utilizzato dagli enti di standardizzazione |
| VPI | Virtual Path Identifier ; percorso virtuale, identifica un gruppo di canali logici virtuali |
| VCI | Virtual Channel Identifier ; canale logico virtuale |
| PT | Payload Type ; tipo di traffico trasportato all'interno del payload, specifica se traffico dati, real-time, fonia, video…oppure riservata per la gestione della rete |
| CLP | Cell Loss Priority ; priorità allo scarto, indica se la cella è a bassa o alta priorità (analogo al bit DE del protocollo FR) |
| HEC | Header Checksum ; controllo dell'errore solo sull'intestazione della cella |

ATM effettua un multiplazione di tipo asincrona dove i flussi informativi vengono riportati in celle di lunghezza fissa pari a 53 Bytes ( 5 bytes intestazione + 48 bytes dati ) con allocazione di banda dinamica.

L'instradamento della cella viene eseguito dal commutatore analizzando i campi VPI/VCI contenuti nell'etichetta della cella in ingresso i quali vengono usati per puntare una tabella di transcodifica ( look-up ) che contiene la nuova etichetta da inserire alla cella sulla linea di uscita.

Campo Indirizzo ( VPI / VCI ):

- Il Virtual Channel indica un instradamento per il trasporto di celle ATM. A ciascun canale è assegnato un identificatore VCI;
- Il Virtual Path indica un fascio di Virtual Channel a cui è assegnato l'identificatore VPI.

L'insieme "VPI / VCI" forma l'etichetta della cella.

Commutazione di celle ATM

Nei Nodi ATM le connessioni (cross-connection) possono essere di due tipi:

- VPC = Virtual Path Connection che serve a connettere un VPI di un'interfaccia di ingresso con un VPI di un'interfaccia di uscita;
- VCC = Virtual Channel Connection che serve a connettere un VPI/VCI di un'interfaccia di ingresso con un VPI/VCI di un'interfaccia di uscita.

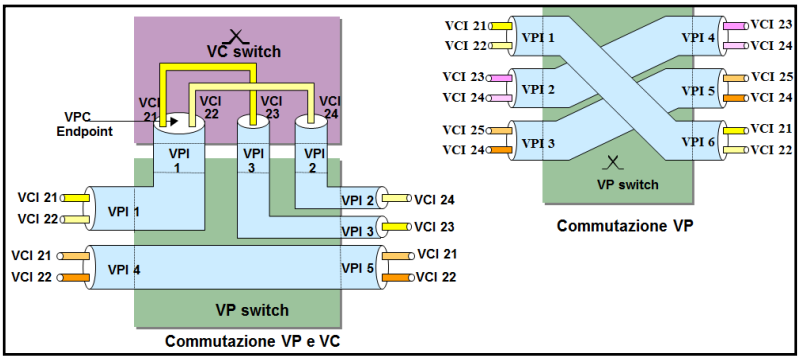



Figura 18 – I due tipi di commutazione delle celle ATM

Categorie di servizio:

- Una grande varietà di applicazioni possono essere supportate in una rete ATM;

- Queste applicazioni richiedono diversi comportamenti della rete dipendenti dalla natura delle applicazioni.
- In conseguenza il traffico è stato raggruppato per tipi e sono state definite le seguenti categorie di servizio.

| Categorie di servizio | Descrizione | Applicazioni |
|---|---|---|
| CBR | Costant Bit Rate<br>(velocità di bit costante) | Voce, video, ISDN, circuiti PDH |
| rt-VBR | Real Time Variable Bit Rate<br>(velocità di bit variabile in tempo reale) | Voce e video no CBR (jpeg) |
| nrt-VBR | Non Real Time Variable Bit Rate<br>(velocità di bit variabile non in tempo reale) | Canale D, X.25, Frame Relay |
| ABR | Available Bit Rate<br>(velocità di bit disponibile) | Interc. LAN, TCP/IP, SMDS |
| UBR | Unspecified Bit Rate<br>(velocità di bit non specificata) | FTP, Posta Elettronica |

Livello di adattamento "AAL

Essendo il livello ATM non adatto ad essere direttamente interfacciato con le attuali applicazioni è stato introdotto un livello di adattamento "AAL" che fornisce servizi diversi a seconda dell'applicazione utilizzata, isolando il livello ATM dall'applicazione stessa.

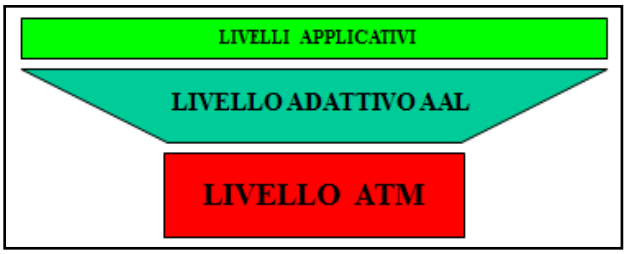



Figura 19 - Livello di adattamento “AAL

Le funzioni principali del livello AAL sono perciò:

- Gestione degli errori;
- Gestione dei problemi relativi alla frammentazione;
- Gestione della perdita o inserzione di celle;
- Gestione del controllo di flusso e della temporizzazione tre sorgente e destinazione.

La fig. 20 mostra  come una trama FR venga frammentata e inserita sulle celle di trasporto ATM, di dimensione fissa di 53 Byte, dal livello di adattamento AAL-5.

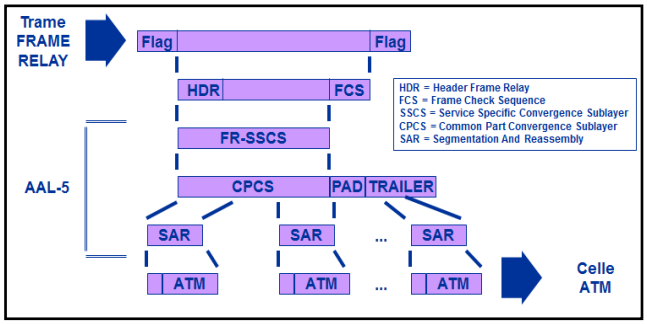



Figura 20 - Inserimento trame FR su celle ATM

# 4. LE WAN E LA COMUNICAZIONE IN UN TERRITORIO

Abbiamo visto che nel caso di LAN la comunicazione avviene tra dispositivi dislocati nell'ambito dello stesso edificio o edifici limitrofi con limiti fisici che non possono essere superati (con i cavi UTP occorre restare entro i 100 metri). Si aveva la necessità di superare tali limiti e realizzare connessioni tra reti/apparati distribuiti sul territorio.

## 4.1 RETE DATI GEOGRAFICA

La Rete Dati Geografica rappresenta l'insieme delle risorse di commutazione e di trasmissione che consentono il trasferimento dell'informazione a distanza.

L'interconnessione avviene:

- utilizzando i mezzi trasmissivi della rete di telecomunicazione PSTN (Public Switched Telephone Network), CDA, CDN;
- utilizzando Reti Dati specializzate (Rete ATM ….);

Le LAN sono connesse tra loro attraverso la WAN (Wide Area Network).

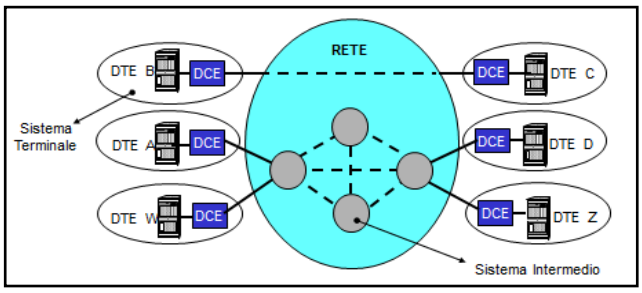



Figura 21 – Host inseriti in rete

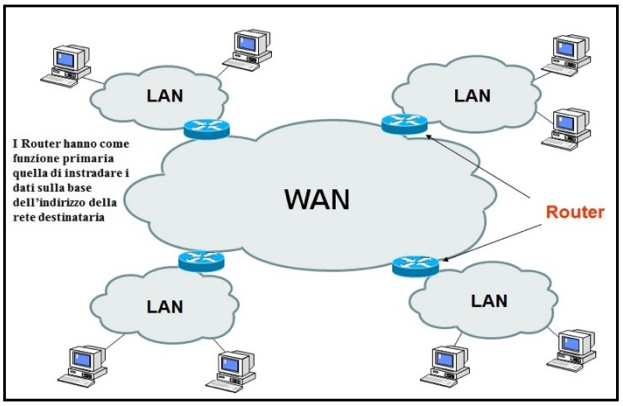



Figura 22 – Esempio di rete geografica

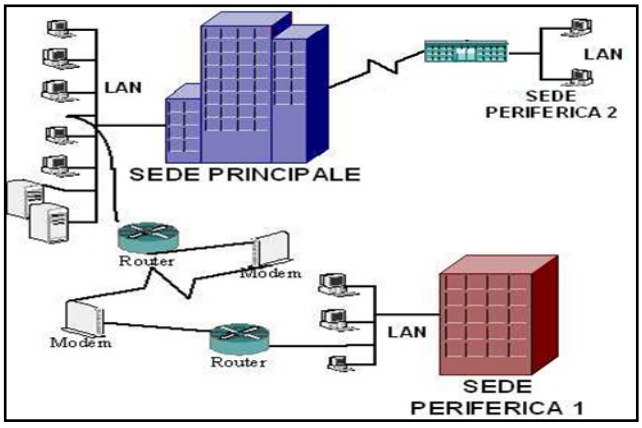



Figura 23 – WAN che permette la connessione fra sedi con circuiti dedicati.

In figura 23 è rappresentata la tipica situazione di una azienda con più sedi distribuite in diverse località. Basandoci sulla rappresentazione figura 23 potremmo rivedere la definizione di WAN come: "una rete costituita da più reti LAN separate geograficamente ed interconnesse grazie a dispositivi che consentono di superare le limitazioni relative alle LAN".

L'architettura di rete WAN aziendale assume la struttura di tipo "hub and spoke", con le funzioni hub svolte dalla sede principale che vede allocati i server e il management della rete mentre la parte spoke è rappresentata delle sedi periferiche.

Le reti dati quindi possono essere classificate a seconda della architettura in :

- LAN Rete Locale Rete Dati in ambito Edificio;
- MAN Rete Metropolitana Rete Dati in ambito Urbano;
- WAN Rete Geografica Rete Dati in ambito extra Urbano.

Con il trasporto ATM posso realizzare connessioni fra utenti FR o fra utenti FR e utenti ATM. La seconda situazione era utilizzata in una INTRANET aziendale per raccogliere sedi periferiche normalmente caratterizzate da collegamenti n x 64 Kb/s fino a 2 Mb/s e concentrarle, con trasporto ATM, verso la sede principale fig. 24 e 25.

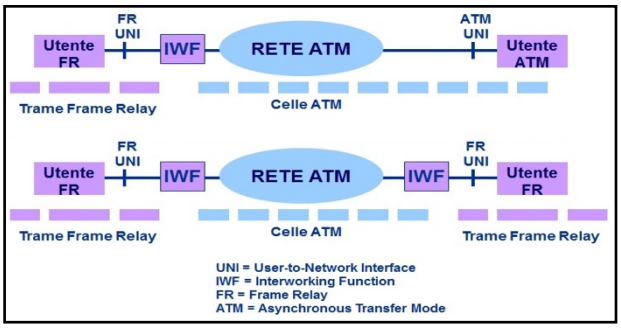



Figura 24 - Reti geografica con trasporto su rete ATM

In fig. 24 nella connessione tra utente FR e rete ATM viene utilizzato il protocollo FR fino all'apparato IWF che ha la funzione di effettuare la transcodifica dal protocollo FR a quello ATM.

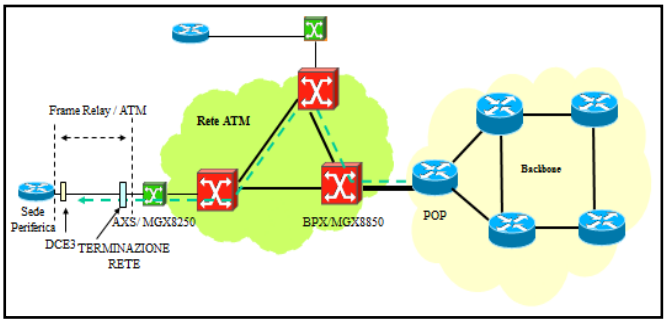



Figura 25 – Esempio di connessione di una sede periferica al BackBone Intranet con trasporto su rete ATM

Nell'uscita dalla rete ATM dove il traffico viene convogliato verso il POP di accesso al backbone intranet si utilizza un collegamento ATM di velocità maggiore, tipicamente 34 Mb/s o 155 Mb/s. La fig. 25 mostra un POP di raccolta sedi periferiche, parimenti altri POP possono connettersi ad altri nodi del Backbone. Sempre sul Backbone possono essere connesse sedi master che erogano i servizi per la intranet, tra cui l'accesso alla rete internet.

ATM e Frame Relay hanno quindi consentito di interconnettere più sedi aziendali creando reti private su scala geografica, ma a costi accessibili solo alle grandi aziende.

Una modalità di realizzazione del networking WAN a costi accessibili è quella che permette di sfruttare le risorse condivise di un ISP per la propria VPN basata su IPSec. In una rete basata su VPN IPSec, la connessione sicura avviene tramite un tunnel cifrato che attraversa internet che per essere attivato necessita dell'installazione di apparecchiature presso la sede del cliente.

Le TELCO simultaneamente fornivano accessi ADSL alla clientela residenziale con connettività basata sull'uso di protocollo PPP (Point-to-Point Protocol) per realizzare la connessione punto-

punto tra il terminale del cliente e il NAS (Network Access Server). Le sessioni PPP, a partire da casa cliente, venivano aggregate sui nodi di accesso DSLAM-ATM (Digital Subscriber Line Access Multiplexer) per essere trasportate sulla rete ATM verso un'interfaccia del NAS. Dove il NAS esegue un insieme di funzioni per la Gestione del Cliente tra le quali AAA (Autenticazione, Autorizzazione e Accounting), assegnazione degli indirizzi IP, applicazione delle policy tra cui la limitazione della banda secondo il contratto del cliente.

### 4.1.1 ROUTER

Per la realizzazione delle reti geografiche sono fondamentali gli elementi nodi di rete presenti nelle fig. 21 e 22. Questi sono i router, apparati che lavorano al livello 3 OSI (livello di rete). Separano le reti in domini di broadcast differenti facendo uso dell'Internet Protocol (IP).

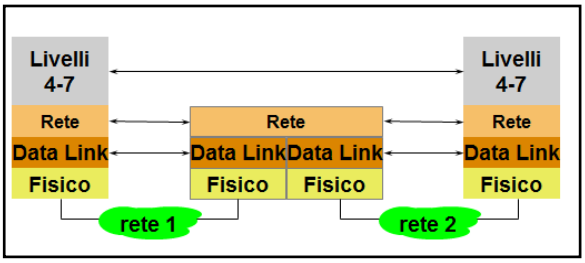



Figura 26 – Connessione fra domini di broadcast differenti.

IP è un protocollo di interconnessione di reti (Inter-Networking Protocol), nato per interconnettere reti eterogenee per tecnologia, prestazioni, gestione.

- Il protocollo IP fornisce un servizio datagram connectionless (senza connessione) ed inaffidabile
- Il termine inaffidabile significa che non ci sono garanzie che un pacchetto IP giunga a destinazione
- Il termine connectionless significa che il protocollo IP non mantiene alcuna informazione di stato circa i pacchetti inoltrati. Ciascun pacchetto è trattato indipendentemente da tutti gli altri. Questo significa anche che i datagrammi IP possono essere consegnati fuori sequenza
- L'Internet Protocol (IP) è un protocollo di rete a pacchetto; secondo la classificazione ISO/OSI è di livello rete (3).

- La versione correntemente usata del protocollo IP è detta anche IPv4 per distinguerla dalla più recente IPv6, nata dall'esigenza di gestire meglio il crescente numero di computer connessi ad Internet.

In fig. 27 la rappresentazione del pacchetto IP.

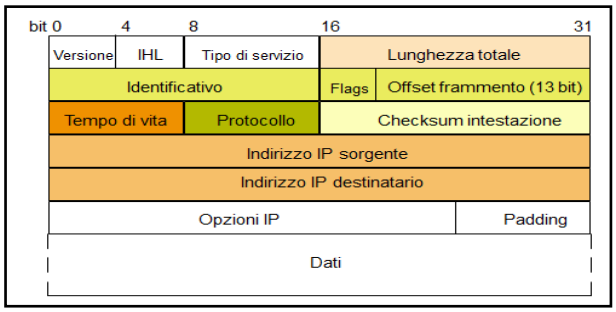



Figura 27 – Pacchetto IP

Allora facendo riferimento alla Fig. 9 del Modello OSI, scendendo dal livello 3 al livello 2, il pacchetto IP viene imbustato su una trama di livello 2, fig. 28.

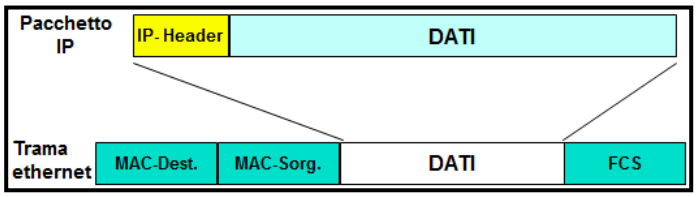



Figura 28 - Imbustamento di un pacchetto IP su una trama di livello 2.

Salendo nel Modello OSI, e passando al livello 4 di trasporto, i protocolli di trasporto sono soprattutto TCP e UDP:

<u>TCP - Transmission Control Protocol</u>

Garantisce la trasmissione End-to-End

- Connection Oriented
- Rilevamento errori
- Controllo di flusso
    - Numerazione sequenze e gestione della finestra (quantità di dati trasferibili in un singolo segmento)
    - Riconoscimento End to End

UDP - User Datagram Protocol

Non garantisce la tramissione End-to-End

- Connectionless
- Rilevamento errori
- Nessun controllo di flusso

# 5. MPLS PER LA RAZIONALIZZAZIONE DELLE RETI

## 5.1 MOLTEPLICITÀ DI RETI GEOGRAFICHE

La tradizionale architettura delle reti IP (connectionless-oriented, paradigma best-effort), aveva contribuito ad una straordinaria crescita e diffusione. Le moderne tecnologie avevano trasformato le reti geografiche in reti private con funzionalità, sicurezza e prestazioni simili alle reti locali. La crescita delle reti aveva stimolato la ricerca di nuove soluzioni di interconnessione e contribuito a diversificare e incrementare la tipologia di applicazioni e servizi offerti (video on-demand, real-time, Voice over IP). Alle prime intranet aziendali se ne erano affiancate altre dedicate ai servizi: office automation, gestione apparati, controllo accessi, sicurezza fig. 29.

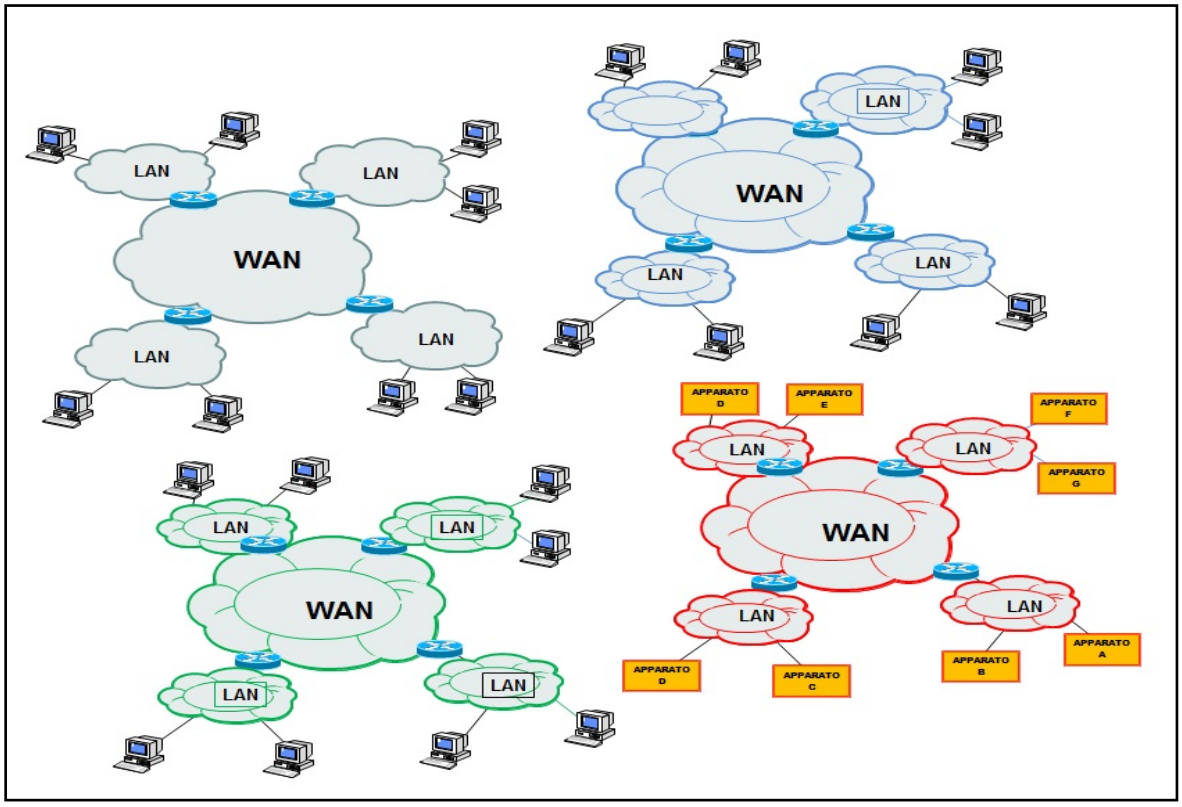



Figura 29 - Molteplicità di INTRANET sulle stesse sedi territoriali.

La gestione di reti distinte era divenuta onerosa e occorreva adattare l'architettura protocollare delle reti IP in un contesto di traffico altamente variegato dove il modello di servizio best-effort non consentiva di rispondere alle esigenze dei clienti. Per rispondere alle nuove esigenze verso la fine degli anni '90 l'attività dell'IETF portava alla definizione del protocollo MPLS (MultiProtocol

Label Switching). Nasceva così come tentativo di risolvere i problemi dovuti alla proliferazione di reti multiservizio il protocollo MPLS. L'architettura MPLS è più articolata di un'architettura IP ed è stata introdotta per realizzare servizi VPN IP (Virtual Private Network IP).

## 5.2 COME NASCE MPLS

Nella prima metà degli anni Novanta per far fronte al crescente sviluppo della rete Internet, in termini di diversità dei servizi gestibili e della banda offerta agli utilizzatori, si era convinti che occorresse coniugare le tecniche basate su IP con le soluzioni di trasporto ATM. Si pensava alla possibilità di riuscire a mappare l'architettura IP su una rete ATM. La prima soluzione proposta era, perciò, di tipo overlay, ossia con livelli separati e sovrapposti, in cui, di fatto, i protocolli d'instradamento a livello IP e ATM agivano indipendentemente, con una netta distinzione tra la rete IP e quella ATM (fig. 30).

Nell'applicazione tipica del modello overlay, i router IP comunicano tra loro attraverso un insieme di PVC (Permanent Virtual Circuit) ATM, che funzionano, perciò, come un insieme di circuiti logici che garantiscono la connettività tra i nodi terminali (edge). In questo caso, se N è il numero dei router di dorsale, per ottenere una soluzione funzionante ed efficace, sarebbe necessario magliare completamente la rete (full mesh) e, quindi, configurare un numero di PVC proporzionale al quadrato del numero N dei nodi. Una dorsale IP basata su ATM presenta, dunque, alcune limitazioni di rilievo: la necessità di mantenere la gestione delle due reti ATM e IP sovrapposte e i problemi di crescita modulare e, cioè, di scalabilità (N-squared problem) causati dall'impiego dei protocolli d'instradamento IP - in genere di tipo OSPF (Open Shortest Path First) - su una magliatura di PVC

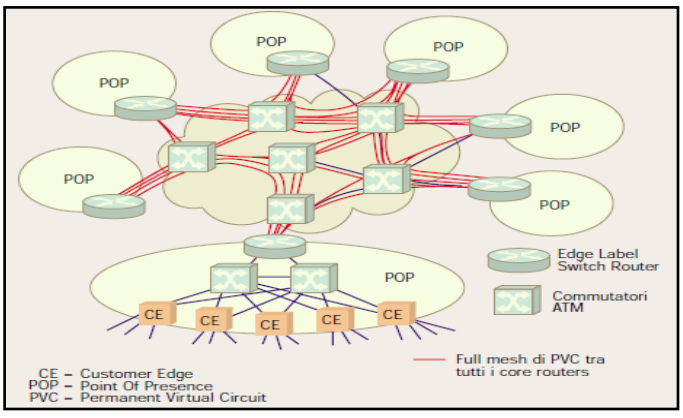



Figura 30 - Integrazione IP/ATM, modello overlay.

Per questi motivi, al modello overlay si contrappose, in un secondo tempo, il modello integrato, introdotto con lo scopo di eliminare le difficoltà di indirizzamento e le ridondanze delle caratteristiche funzionali presenti nelle reti IP e ATM per permettere l'inoltro delle informazioni. Si passa attraverso proposte proprietarie dei diversi vendor con il limite principale di queste tecnologie rappresentato dal fatto che le varie soluzioni non sono tra loro interoperabili e quasi tutte richiedono, come tecnologia di trasporto, l'ATM. Proprio a partire da questo contesto, nel 1997 l'IETF ha costituito l'MPLS Working Group, assegnandogli l'obiettivo di armonizzare e di integrare le proposte, in modo da produrre uno standard multivendor impiegabile su qualsiasi tecnologia di trasporto. L'idea architetturale di base riguarda l'associazione a tutti i datagrammi IP di una breve etichetta (label) di lunghezza fissa, con cui gli apparati di rete possono effettuare un instradamento veloce basato sulla commutazione dell'etichetta stessa (label swapping). La tecnologia risultante è di fatto così in grado di "appoggiarsi" a qualsiasi protocollo di trasporto e di utilizzare qualsiasi protocollo di rete con la possibilità di poter fornire nuovi servizi. Gli sviluppi si sono poi orientati verso un'architettura di rete MPLS trasportata da sistemi SDH, piuttosto che verso MPLS su ATM. Questa scelta vede in prospettiva, la semplificazione dei livelli di rete e la convergenza verso soluzioni che consentono di instradare direttamente IP sui portanti ottici.

## 5.3 ARCHITETTURA MPLS

Il concetto fondamentale di MPLS [9] è, dunque, quello di associare un'etichetta a ciascun pacchetto che attraversa la rete, seguendo a livello architetturale di nodo il criterio della separazione delle due componenti dell'instradamento: la decisione d'instradamento, gestita dai protocolli IP, e l'effettiva attuazione (*forwarding*) dello smistamento dei flussi di pacchetti, gestita tramite la commutazione di etichetta.

La componente di decisione ( che comprende l'insieme dei moduli demandati all'allocazione e alla distribuzione delle etichette tra nodi adiacenti) e l'intelligenza di livello 3 (*IP addressing, IP routing*), è del tutto indipendente da quella di attuazione (*inoltro dei pacchetti secondo il paradigma label switching*). L'assenza di vincoli permette di realizzare differenti protocolli su qualsiasi mezzo (*multiprotocol*) e di evitare, come nel caso di overlay del livello IP su ATM, configurazioni completamente magliate di percorsi, LSP *(Label Switched Path*), fra i router della dorsale.

### 5.3.1 COMMUTAZIONE DI ETICHETTA: LA COMPONENTE DI FORWARDING

Nel modello di layer 3 forwarding tradizionale [10], ciascun router di rete consulta la propria IP FT (*Forwarding Table*) e seleziona, così, il nodo successivo verso cui inviare i pacchetti (*next hop*) sulla base dell'indirizzo IP di destinazione contenuto nell'intestazione di livello 3.

La scelta del next hop è data dalla combinazione di due funzioni: la prima suddivide l'intero insieme dei possibili pacchetti IP in sottoinsiemi denominati FECs (Forwarding Equivalence Classes); la seconda associa ciascuna FEC a un determinato indirizzo IP di next hop. Il processo è conosciuto come *hop by hop forwarding*.

Con la tecnologia MPLS, l'analisi dell'intestazione IP e l'assegnazione conseguente di un pacchetto a una determinata FEC (che può essere effettuata sulla base di numerose informazioni quali IP precedence, indirizzo di sorgente e di destinazione, tipo di applicazione) è eseguita una sola volta in corrispondenza dell'E-LSR (Edge-Label Switch Router), posto nei punti di ingresso della rete. La FEC alla quale il pacchetto è assegnato è codificata con un'etichetta di lunghezza fissa che è anteposta all'intero pacchetto. Il pacchetto "esteso" è, quindi, inviato verso il next hop, che questa volta realizza lo smistamento unicamente in base alle informazioni contenute nell'etichetta, piuttosto che sull'analisi delle informazioni dell'intestazione di livello 3 [11].

Nel punto di uscita dalla rete MPLS, il corrispondente E-LSR rimuove l'etichetta e consegna il pacchetto IP al sito del Cliente finale. In questo modo l'intero processo di trasporto MPLS in rete rimane del tutto trasparente per i siti posti presso le sedi dei clienti.

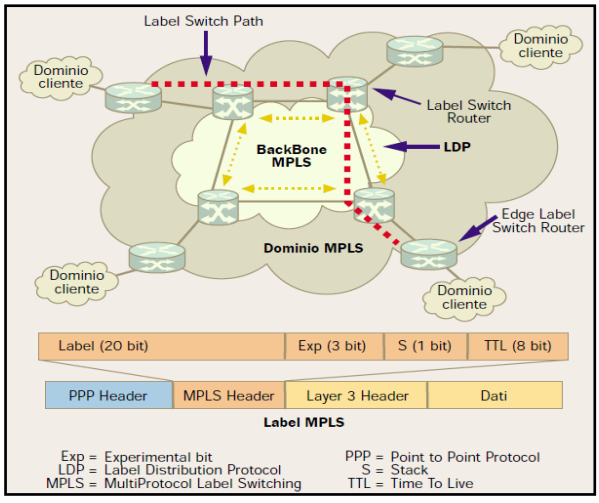



Figura 31 - Architettura di rete e struttura dell'intestazione MPLS.

Nella struttura tipica di una rete MPLS (fig 31) gli elementi base che possono essere riconosciuti sono i seguenti:

- Dominio MPLS: porzione di rete costituita da apparati che riconoscono e che sono in grado di dialogare con la rete MPLS;
- Dorsale di rete MPLS: porzione interna del dominio MPLS in cui l'inoltro dei pacchetti avviene unicamente attraverso la commutazione di etichetta MPLS;
- Dominio cliente: insieme di siti della rete di un Cliente connessi al backbone MPLS;
- Edge LSR (Edge Label Switch Router): router posti alla terminazione (frontiera) della rete, utilizzati per assegnare e per togliere le etichette ai datagrammi e per eseguire l'operazione conseguente di inoltro verso il dominio MPLS;
- LSR (Label Switch Router): dispositivi collocati in genere all'interno del dominio MPLS capaci di inoltrare i pacchetti unicamente sulla base del contenuto informativo di un'etichetta (paradigma Label Switching);
- LSP (Label Switched Path): percorso attraverso uno o più LSRs seguito da un pacchetto appartenente a un certo flusso di dati;
- LDP (Label Distribution Protocol): protocollo utilizzato, insieme con quelli d'instradamento;
- IP classici, per definire e per distribuire le etichette;
- Router Ru e Rd: Ru è detto upstream LSR se un pacchetto, rispetto al processo di distribuzione delle etichette, è inoltrato da un router Ru ad uno Rd; analogamente Rd è chiamato downstream LSR.

La fig. 31 mostra anche la struttura di una generica trama MPLS consegnata al livello 2 sottostante per il trasporto. Il payload è costituito da un pacchetto IP preceduto da una sequenza di intestazioni MPLS. Ogni intestazione MPLS è composta da 32 bit dove:

- Label (20 bit);
- Stack (1 bit): è il campo che indica l'eventuale presenza di più etichette messe in sequenza (ovvero in stack) per consentire, lo smistamento in reti realizzate su più livelli MPLS;
- TTL (8 bit): è il campo Time-to-Live.

La label di 20 bit sopra specificata ha un valore locale nell'interfaccia utilizzata per l'inoltro dei pacchetti e sintetizza diverse informazioni riguardanti il pacchetto cui essa si riferisce:

- destinazione;
- precedenza;
- appartenenza a VPN (Virtual Private Network);

- QoS (Quality of Service);
- informazioni di TE (Traffic Engineering).

Tra i valori assegnabili alcuni sono riservati:

- valore 0 - IPv4 Explicit NULL. Questo valore indica che l'etichetta non contiene effettive informazioni d'instradamento. Il pacchetto deve, quindi, essere inoltrato seguendo le informazioni contenute nell'intestazione di livello 3, che in questo caso è del tipo IPv4;
- valore 2 - IPv6 Explicit NULL: analogamente al caso precedente, con livello 3, che in questo caso è del tipo IPv6;
- valore 3 - Implicit NULL. Questo valore è impiegato nel protocollo LDP (Label Distribution Protocol) per la distribuzione delle etichette tra nodi.

Un pacchetto nel caso più generale, quando ad esempio si debbano attraversare aree multibackbone, vale a dire, aree gestite da differenti ISP, non trasporta una sola etichetta, ma una serie di etichette, organizzate in sequenza (a stack) di tipo LIFO (Last In First Out).

L'analisi dello stack in ogni nodo MPLS, LSR (Label Switching Router), avviene, allora, in maniera indipendente dal livello della gerarchia e sempre guardando l'etichetta posta in cima, senza considerare che altre etichette possono essere state inserite in precedenza "sotto di essa". Può essere rilevato che un pacchetto, a cui non sia stata ancora associata un'etichetta, abbia lo stack vuoto, mentre se un pacchetto possiede m etichette, quella posta in cima allo stack è definita di livello (o di gerarchia) m. Quando un pacchetto è ricevuto, viene analizzata l'etichetta di livello più elevato nello stack e da questa lettura, sempre operando sulla base della tabella NHLFE (Next Hop Label Forwarding Entry), si ricavano le informazioni necessarie per agire correttamente nell'inoltro del pacchetto stesso, in pratica il next-hop da utilizzare, e le successive azioni da eseguire sullo stack, tra cui, ad esempio:

- sostituire l'etichetta posta in cima allo stack con una nuova;
- leggere lo stack delle etichette;
- inserire nuove etichette.

Per inoltrare, invece, un pacchetto privo di etichetta, in un LSR si analizza direttamente l'intestazione di livello 3 e, sempre dalla tabella NHLFE, si valuta dove instradare il pacchetto e quale etichetta inserire.

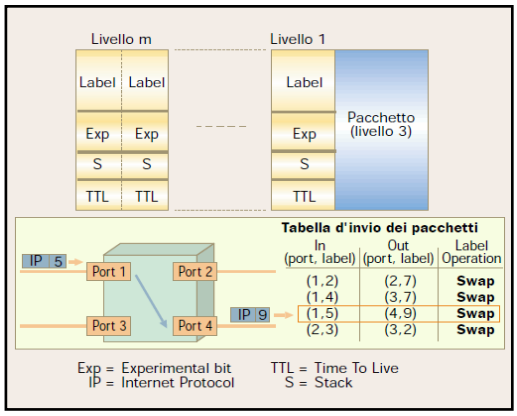



Figura 32 - Stack di etichette MPLS e paradigma di commutazione di etichetta.

La fig. 32 mostra un esempio di come avvenga una generica propagazione di un pacchetto IP, a cui sia stata applicata l'etichetta MPLS, quando attraversa un nodo MPLS. Secondo quanto riportato nella tabella d'instradamento del nodo rappresentato, un pacchetto proveniente dalla porta 1, con etichetta di ingresso pari a 5, deve essere inviato alla porta di uscita 4, dopo che gli sia stata associata un'etichetta di uscita pari a 9. Quando anche l'ultima etichetta posta nello stack è letta, l'inoltro del pacchetto avviene unicamente sulla base dell'intestazione IP.

### 5.3.2 COMMUTAZIONE DI ETICHETTA IN MPLS: LA COMPONENTE DI CONTROLLO

Le funzioni d'instradamento sono suddivise in due componenti: attuazione e controllo. Per effettuare il controllo devono essere inserite nuove prestazioni, legate alla distribuzione delle informazioni d'instradamento tra nodi LSR e alle procedure (algoritmi) che gli stessi nodi eseguono per costruire e per aggiornare le tabelle d'instradamento utilizzate, in modo da assegnare e da modificare le etichette. Può essere utilizzato a questo scopo il protocollo BGP (Border Gateway Protocol) ma l'IETF ha, però, definito anche un nuovo protocollo, l'LDP (Label Distribution Protocol) [13] [14], con l'obiettivo di fissare l'insieme delle procedure attraverso le quali un LSR informa un altro LSR sulle etichette create e sulle associazioni tra percorsi d'instradamento ed etichette. Due LSR che stabiliscano una comunicazione mediante LDP sono detti label distribution peers. Le operazioni caratteristiche per l'allocazione e per la distribuzione delle etichette MPLS sono tre:

- Downstream Label Allocation;
- Downstream Label Allocation on Demand;
- Upstream Allocation.

Per un corretto funzionamento del meccanismo è necessario attivare nella rete MPLS un protocollo di routing come quello IGP (Interior Gateway Protocol), che governa il popolamento delle tabelle d'instradamento dei singoli LSR.

*Downstream Label Allocation*

Nel Downstream Label Allocation, un LSR, nel momento in cui un particolare prefisso, il FEC (*Forwarding Equivalence Class*), è stato appreso tramite messaggi che provengono dal protocollo di routing IGP, associa un'etichetta al prefisso e ad un percorso d'instradamento, la inserisce nella sua tabella d'instradamento, stabilisce un riferimento a essa nel proprio elenco di etichette valide, la LIB (*Label Information Base*), e comunica, poi, agli LSR adiacenti la relazione tra etichetta d'ingresso e percorso d'instradamento.

Quando un LSR riceve, dal nodo successivo su un dato percorso d'instradamento, l'informazione che consente di stabilire su quel percorso un'associazione tra FEC ed etichetta (permette di effettuare cioè il cosiddetto label-binding), l'LSR pone l'etichetta tra quelle d'uscita della LIB che si riferiscono allo stesso percorso. In caso contrario, si limita ad associare un'etichetta a ciascun percorso disponibile.

*Downstream Label Allocation on Demand*

Nel Downstream Label Allocation on Demand un LSR identifica per ciascun percorso d'instradamento un nodo subito "a valle" (next hop). Invia, poi, una richiesta (via LDP) per associare un'etichetta a quel percorso. Quando il nodo next hop riceve la richiesta, crea un'etichetta e la memorizza nel proprio archivio di etichette valide (nella propria LIB), producendo un'azione successiva che dipende dal modo di funzionamento che può essere di tipo indipendente o ordinato.

*Upstream Label Allocation*

Con la procedura di Upstream Label Allocation, un LSR alloca alcune etichette per ciascun percorso, contenuto nella propria tabella d'instradamento e raggiungibili da una delle sue interfacce. Aggiorna poi la propria LIB ponendo l'etichetta tra quelle in uscita e informa il nodo successivo su quel percorso dell'avvenuta associazione.

Il nodo di next hop, dopo aver ricevuto questa informazione, mette questa etichetta tra quelle in ingresso nella propria LIB. Dopo aver inserito sia l'etichetta d'ingresso sia quella di uscita, l'LSR

può inoltrare i pacchetti sul percorso individuato, utilizzando l'algoritmo di commutazione di etichetta.

Ogni volta che un LSR crea una nuova associazione tra un percorso e un'etichetta, aggiorna sia la tabella d'instradamento sia la LIB.

Quest'operazione permette di associare etichette anche ai pacchetti a cui non era stata assegnata in precedenza alcuna etichetta e, quindi, ai pacchetti che arrivano in ingresso alla rete MPLS dall'esterno.

### 5.3.3 LABEL SWITCHED PATH

Il cammino seguito da un pacchetto nel backbone MPLS prende il nome di LSP (*Label Switched Path*) e, genericamente, può essere definito di livello *m* per un particolare datagramma se si tratta di una sequenza di router R1…Rn con le proprietà di seguito elencate:

- inizia con un LSR (*LSP Ingress*) che inserisce nel pacchetto un'etichetta di gerarchia *m* (come descritto al precedente par. 5.3.2);
- tutti gli LSR intermedi nel LSP prendono le decisioni di label switching basandosi solo sull'etichetta di *livello m;*
- termina (*LSP Egress*) quando viene deciso di effettuare lo smistamento, basandosi su un'etichetta di livello differente (pari a m-k, con k > 0), o quando la decisione dello smistamento non è basata sulla procedura di *label switching*.

L'operazione di eliminazione dell'etichetta di livello *m* può essere eseguita dal *LSP Egress*, ma, in genere, risulta più efficiente se essa è eseguita dal penultimo LSR di un LSP. A livello architetturale questo comportamento risulta, infatti, perfettamente appropriato in quanto l'etichetta di gerarchia *m* ha la funzione di instradare il pacchetto sino a Rn, e, quando Rn-1 ha deciso di indirizzarlo correttamente, non è più necessario il trasporto dell'etichetta. L'utilizzo di questa tecnica, che prende il nome di *Penultimate Hop Popping*, evita, di fatto, la necessità di far eseguire per due volte dall'*LSP Egress* l'operazione di decisione d'instradamento: dapprima sulla base dell'etichetta di livello *m*, e poi dall'esame della parte restante del datagramma in modo da consentire l'instradamento verso la destinazione finale.

Per quanto concerne il modo per selezionare un LSP per una particolare FEC, il protocollo MPLS supporta due possibili meccanismi di *route selection:*

- *Hop by Hop Routing;*
- *Explicit Routing.*

Nel caso di un *Hop by Hop Routing* ciascun nodo sceglie il proprio *next-hop* in maniera indipendente dagli altri, sulla base delle informazioni contenute nella propria tabella d'instradamento, popolata ad esempio dalle rotte distribuite attraverso il protocollo *OSPF (Open Shortest Path First).*

In un *Explicit Route* LSP, invece, ogni LSR non esegue la scelta del *next hop* in maniera indipendente. Un singolo LSR, tipicamente l'LSP Ingress o l'LSP Egress, specifica in modo completo *(strictly),* o quasi *(loosely),* l'intero LSP.

Questo meccanismo può essere utile per molte ragioni, prima fra tutte, la possibilità di utilizzare MPLS a scopi di corretto bilanciamento del traffico sulle varie direttrici interne alla rete MPLS, in base, cioè, al *TE (Traffic Engineering).*

### 5.3.4 CENNI SU MECCANISMO EQUIVALENTE MPΛS (MULTIP. LAMBDA SWITCHING)

Uno degli obiettivi più attraenti dell'MPLS riguarda oggi la possibilità di utilizzare un meccanismo equivalente *MPλS (MultiProtocol Lambda Switching)* [17], per riuscire a portare IP direttamente sulle reti ottiche, e quindi a realizzare i sistemi di commutazione ottica attraverso i meccanismi d'instradamento IP riducendo, in particolare, il numero dei livelli tipici delle attuali reti per dati (da IP/ATM/SDH/WDM a IP/WDM) via via che si estenda l'impiego della rete *WDM (Wavelength Division Multiplexing).* In sostanza, MPλS si propone di combinare i vantaggi che MPLS introduce in termini di *Traffic Engineering* (a livello, quindi, di piano di controllo) con le tecnologie emergenti di commutazione fotonica e ottica, per realizzare reti capaci di fornire in tempo reale servizi di trasporto attraverso canali ottici.

## 5.4 APPLICAZIONI

L'introduzione dell'architettura e delle funzionalità MPLS in una rete IP può consentire di:

a) gestire le funzioni di Traffic Engineering per un impiego ottimale delle risorse di rete da parte degli ISP;

b) realizzare *VPN (Virtual Private Network)* IP, ossia realizzare infrastrutture di Intranet e di Extranet, gestite dagli ISP per conto dei siti clienti, che spesso sono reti Internet estese;
c) consentire la predisposizione di nuove *CoS (Classes of Service)* con relativa QoS, nell'ambito della fornitura di servizi differenziati, attraverso la realizzazione del modello *Diffserv c*ongiuntamente a meccanismi di Traffic Engineering;
d) garantire un rapido reinstradamento *(fast rerouting)* per migliorare l'affidabilità, la robustezza e la qualità dei servizi offerti dalle reti IP.

### 5.4.1 MPLS TRAFFIC ENGINEERING

Le funzioni di Traffic Engineering consentono a un ISP di instradare un certo flusso di traffico lungo un percorso differente da quello individuato dai normali protocolli d'instradamento, in modo da utilizzare, qualora sia necessario, un percorso fisico meno congestionato.

Lo sviluppo delle funzionalità di *Traffic Engineering* su MPLS attraverso un'integrazione delle tecnologie di livello 2 e 3:

- permette il calcolo degli LSP sulla base delle risorse disponibili nella rete in quel momento tenendo presente le caratteristiche specifiche richieste dal particolare flusso di dati che si deve trasportare attraverso la rete;
- possiede un meccanismo adattativo rispetto ai mutamenti della rete a livello topologico, dovuti a guasti o all'inserimento di nuovi nodi.

### 5.4.2 RETI PRIVATE VIRTUALI MPLS/IP

Una Rete Privata Virtuale, o *VPN (Virtual Private Network),* è costituita da un insieme di siti di Clienti la cui connettività è basata su una struttura condivisa, dotata delle stesse politiche amministrative applicabili a una struttura privata (ad esempio piano di indirizzamento individuale, traffico limitato ai siti dei clienti). Sia dal punto di vista dell'instradamento, che da quello della riservatezza, la rete può, infatti, essere classificata come privata, nel senso che per una VPN tutte le altre sono "trasparenti", vale a dire non può essere utilizzata da utenti esterni, e che l'instradamento e il piano di indirizzamento interno ( eventualmente privato ) sono completamente indipendenti dall'instradamento e dal piano di indirizzamento di tutte le altre reti.

La rete è, invece, virtuale nel senso che l'utilizzo del mezzo fisico è in realtà condiviso fra più utilizzatori *(VPN customer)* ciascuno dei quali desidera disporre di una propria VPN, mentre il fornitore è tipicamente una terza parte che può essere definito come *VPN service provider*.

Nel caso più generale, una VPN è costituita da una serie di siti interconnessi tra loro, a cui è possibile applicare diversi criteri di connessione anche se operano all'interno di una medesima struttura amministrativa. Si può anche fare in modo che un sito, appartenente a una certa VPN, comunichi solo con un sottoinsieme di altri siti appartenenti a un'altra VPN.

Nel primo caso si può parlare di *Intranet VPN,* mentre nel secondo di *Extranet VPN*. In virtù di questa definizione risulta chiaro che un determinato sito può appartenere a una o più VPN.

Prima dell'applicazione dell'MPLS la maggior parte delle tecniche utilizzate per la realizzazione di VPN era basata sul modello *overlay* [9], nel quale ciascun sito ha uno o più router connessi agli altri siti ( o eventualmente a un loro sottoinsieme ) mediante collegamenti punto-punto (tipicamente realizzati con tecnologia *Frame Relay* o ATM, in ogni caso a livello 2). Soluzione che richiedeva una magliatura completa o parziale di collegamenti punto-punto.

Il modello MPLS VPN/IP basato sul concetto del "peer" [9] consente, invece, di superare la maggior parte delle precedenti limitazioni e, in particolare, consente ai *VPN service provider* di fornire VPN su larga scala, permettendo, al contempo, di offrire il servizio agli utenti senza richiedere un'esperienza a livello d'instradamento IP in quanto si riduce notevolmente il numero complessivo delle connessioni di livello 2 necessarie.

In tal modo risulta decisamente semplificata la fornitura di servizi VPN rispetto al numero di siti connessi e si riesce a ottenere una connettività *any-to-any* altamente scalabile per Intranet estese e per Extranet che offrano nuovi servizi a valore aggiunto. Le MPLS VPN consentono, anche, di raggiungere livelli di sicurezza e di riservatezza delle informazioni affidabili e di offrire più classi di servizio, sia all'interno della stessa VPN che fra più VPN.

Si descrivono ora le caratteristiche più significative dell'architettura del modello MPLS VPN/IP .

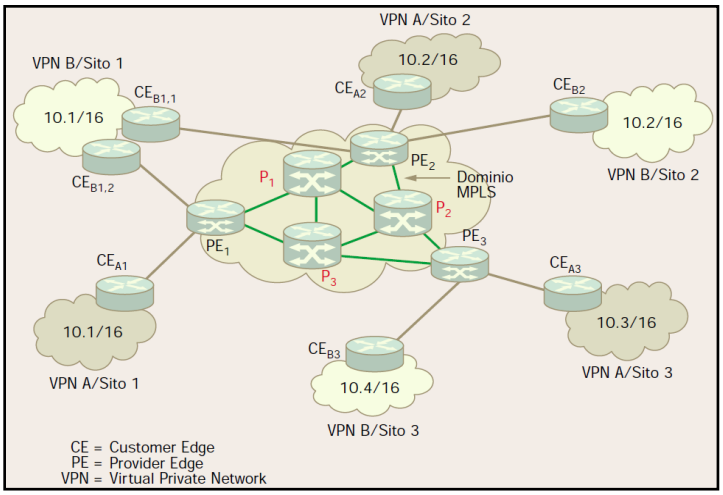



Figura 33 - *Architettura di una VPN MPLS.*

La struttura tipica di un'area MPLS VPN/IP è rappresentata nella fig. 33 dove gli elementi fondamentali sono:

• *PE (Provider Edge router):* sono i router utilizzati dai clienti per accedere all'area MPLS;

• *CE (Customer Edge router):* sono i router che raggruppano l'insieme dei siti del Cliente e sono collegati direttamente con i PE router per accedere alla rete MPLS pur ignorando completamente la struttura del dominio MPLS;

• *P (Provider router):* sono i router dell'area interna di una MPLS VPN.

In una MPLS VPN/IP il router del Cliente, il *CE (Customer Edge)* è connesso al router di accesso del provider *(PE)* con una logica di interconnessione indipendente dal particolare tipo di tecnologia utilizzata per il livello fisico e per il collegamento. Il meccanismo di controllo della connettività fra i siti è realizzato mediante una *constrained distribution of routing information*, con uno schema, cioè, di distribuzione delle informazioni d'instradamento che può essere decomposto in cinque passi:

a) le informazioni d'instradamento sono, dapprima, avviate dal Cliente (nodo CE) al Service Provider al nodo *PE (Provider Edge)* attraverso uno dei quattro criteri riportati di seguito: instradamento statico; RIPv2; BGPv4; OSPF;

b) sul nodo PE le informazioni d'instradamento sono esportate nel protocollo *BGP (Border Gateway Protocol)* del Service Provider;

c) le informazioni d'instradamento sono poi propagate, tramite *I-BGP (Internal BGP),* tra i nodi PE a cui sono attestati i siti di una stessa VPN;

d) le informazioni precedenti d'instradamento sono importate dal protocollo di routing BGP nel nodo PE di uscita (fase esattamente complementare a quella del punto b prima indicata);

e) le informazioni d'instradamento sono propagate dal Service Provider (nodo PE) al client (nodo CE) (fase complementare a quella del punto a).

In una struttura di questo tipo, i router definiti come PE ricevono e memorizzano le informazioni d'instradamento relative solo alle VPN direttamente connesse. Il numero delle informazioni d'instradamento mantenute sul PE è, quindi, direttamente proporzionale al numero di VPN direttamente connesse a ciascuno di essi. Inoltre, ogni nodo CE mantiene informazioni sui *peer* di tipo PE ai quali è direttamente connesso, trascurando tutti gli altri siti di Clienti della VPN di appartenenza.

È proprio grazie a tale meccanismo che questa soluzione risulta decisamente più scalabile rispetto a quella *overlay*, non solo per quanto riguarda il numero di connessioni risparmiate (è, infatti, evitata la realizzazione di una magliatura completa fra i CE), ma anche perché, per aggiungere o per eliminare un sito da una VPN, è semplicemente necessario aggiornare il database del PE al quale un proprio CE risulta direttamente connesso (indipendentemente dal numero totale di siti presenti in rete). I router PE non possiedono un'unica tabella d'instradamento per gestire questo meccanismo, ma ne gestiscono differenti, ognuna delle quali - relativa a una particolare VPN - prende il nome di *VRF (VPN Routing Forwarding table)* e, come le normali tabelle d'instradamento IP, si compone di due sottotabelle: la *VRF IP routing table,* nella quale sono contenute le informazione d'instradamento verso le destinazioni appartenenti alla VPN, e la *VRF IP forwarding table*, nella quale sono comprese le informazioni relative alla commutazione dei pacchetti da un'interfaccia entrante a una uscente dal router. L'associazione di un sito a una determinata VPN avviene, quindi, in base all'interfaccia logica di attestazione del CE al PE.

È importante sottolineare che, mentre non è necessario stabilire una relazione uno-a-uno fra siti di utente e VPN, un sito può però essere associato solo a una VRF, che contiene tutte le possibili rotte disponibili al sito e poste all'interno della VPN al quale esso appartiene. Può essere definita una sola istanza VRF su ciascuna interfaccia, mentre è consentito associare la stessa VRF a più interfacce (questo è il caso in cui più siti della stessa VPN siano connessi allo stesso PE su interfacce distinte).

Sulla base delle informazioni contenute nella *VRF IP routing table* e nella *VRF forwarding table*, i pacchetti sono consegnati alla loro destinazione attraverso un meccanismo di inoltro MPLS, che consente di superare il problema relativo all'utilizzo di cammini espressi in termini di *VPN IP*

*address:* a questo scopo è, infatti, disaccoppiata l'informazione utilizzata per l'instradamento dei pacchetti (etichetta MPLS) da quella contenuta nell'intestazione IP.

Sono, in pratica, elaborati e stabiliti alcuni cammini sulla base delle informazioni d'instradamento private contenute nelle singole VRF ed i pacchetti sono successivamente inoltrati lungo questi percorsi mediante MPLS.

Dal punto di vista delle caratteristiche peculiari di un MPLS, un router PE non è altro che un *LSR (Label Switch Router)* di tipo *Egress* che esegue l'operazione di assegnazione delle etichette ai pacchetti che ne sono sprovvisti e di eliminazione, sempre delle etichette, a quelli diretti verso i router CE.

In realtà, per migliorare la modularità e l'espandibilità della rete, un PE quando riceve un pacchetto non etichettato da uno dei CE direttamente connessi, gli assegna una coppia di etichette gerarchiche. Quella di primo livello *(interna)* è associata a un percorso verso il PE di destinazione, e di conseguenza garantisce il corretto instradamento da un PE di ingresso a uno di uscita, mentre quella di secondo livello *(esterna)* controlla l'inoltro dei pacchetti MPLS sino al penultimo PE, prima cioè del PE di destinazione (vedi fig. 34). L'utilizzo di questa tecnica permette ai router dei *provider* P della dorsale MPLS di non memorizzare informazioni riguardanti direttamente l'instradamento interno alle singole VPN, ma di registrare solo quelle relative all'inoltro dei pacchetti mediante MPLS (ossia mediante il LIB) verso i router a essi direttamente connessi.

Le etichette di primo livello sono tipicamente distribuite mediante sessioni *BGP (Border Gateway Protocol)* insieme con i percorsi VPN/IP; quelle di secondo livello mediante *LDP (Label Distribution Protocol)* (come mostrato nella fig. 34).

Per avere un'idea concreta del guadagno che si ottiene in termini di scalabilità utilizzando una tecnica MPLS gerarchica basta considerare l'esempio di un service provider che possiede duecento router (PE e P) e che gestisce 10mila VPN, ciascuna mediamente con 100 route. Senza l'ausilio della tecnica MPLS gerarchica, ogni provider (P) router dovrebbe mantenere 10mila X 100 = 1 milione di rotte, mentre con MPLS sono sufficienti per ogni P router, duecento rotte verso tutti gli altri router della dorsale.

Le informazioni d'instradamento sono, dunque, mantenute nella VRF che ne garantisce la sicurezza, prevenendo che vadano indebitamente fuori della VRF informazioni che devono rimanere all'interno, e che pacchetti esterni siano instradati a un router interno alla VPN.

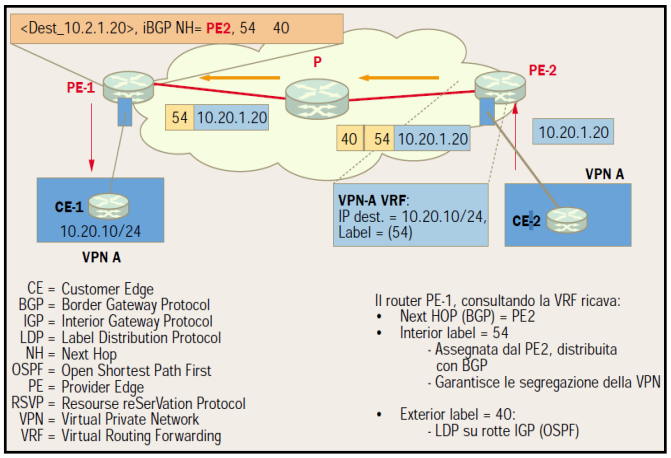



Figura 34 - *Esemplificazione del funzionamento delle VPN MPLS con doppia gerarchia di etichette.*

Gli stessi meccanismi associati alle VRF consentono, anche, di poter ripetere indirizzi di utenti (tipicamente privati) all'interno di VPN differenti. Non è, infatti, necessario che un utente, per partecipare a due VPN, debba avere due indirizzi IP differenti, dal momento che sono esclusi a priori eventuali conflitti: anche se uno stesso indirizzo è presente in due tabelle d'instradamento VRF, essendo queste tabelle del tutto indipendenti tra loro, non si può verificare alcuna ambiguità.

Per la gestione degli spazi di indirizzamento sovrapposti è definita una nuova famiglia di indirizzi IP estesi (per mezzo del meccanismo del *route distinguisher*), mentre per la propagazione delle relative informazioni d'instradamento tra i vari router terminali PE sono utilizzate le estensioni del *Multi Protocol BGP (MP-BGP)* [28].

### 5.4.3 MPLS E LA DIFFERENZIAZIONE DEI SERVIZI (DIFFSERV)

La realizzazione di VPN attraverso MPLS permette, già intrinsecamente, ai *service provider* che le offrono di poter differenziare, almeno parzialmente, i servizi offerti garantendo differenti livelli di QoS per le diverse classi di traffico presenti in rete. È infatti possibile realizzare meccanismi che consentano di distinguere la QoS all'interno delle singole VPN, separando, ad esempio, il traffico *VoIP (Voice-over-IP)* che dovrebbe ricevere un trattamento che assicuri un fissato ritardo massimo di trasmissione, da quello dell'*e-commerce* che dovrebbe, invece, ricevere una banda minima garantita (senza vincoli espressi sul ritardo di consegna).

Il MultiProtocol-BGP

Il MP-BGP (definito nella RFC 2283[37]) consente di annunciare univocamente le rotte IPv4 dei clienti, in un ambiente in cui gli indirizzi IP non sono unici, utilizzando un apposito formato denominato VPN-IPv4.

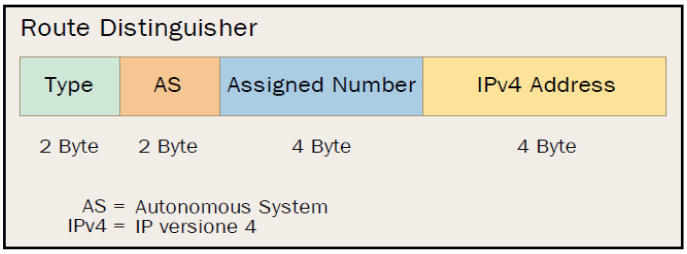



Figura 35 - *Formato Route Distinguisher.*

Come rappresentato in fig. 35, un indirizzo VPN-IPv4 è costituito da un campo *RD(Route Distinguisher)* di lunghezza pari a 64 bit e da un indirizzo IP tradizionale.

Il formato del RD comprende tre sottocampi:

- *Type:* ha la lunghezza di due byte e determina la lunghezza degli altri due campi e la semantica del campo *Autonomous System*;
- *AS (Autonomous System):* contiene un numero identificativo dell'Authority preposta a fissare il valore dell'*Assigned Number* per una determinata applicazione;
- *Assigned Number:* è direttamente fissato dal VPN service provider (in genere uno per ogni VPN servita dal medesimo provider, anche se in realtà può essere pure utilizzato per identificare un particolare sito del cliente).

Impiegando un formato come quello mostrato in figura per l'RD, si è certi dell'unicità totale degli indirizzi VPN-IPv4, in quanto il campo AS è unico rispetto all'insieme dei provider, mentre quello relativo all'*Assigned Number*, per definizione, è unico all'interno dell'ambito relativo al singolo provider.

La tecnica MPLS dovrebbe però essere in grado di gestire anche un modello architetturale del tipo *DiffServ* [29] per il controllo della QoS. Sono aperti a questo scopo alcuni *Internet Draft* che ne prescrivono le caratteristiche [30]. In questo caso i pacchetti entranti nella rete sarebbero raggruppati in classi, ciascuna della quali è contraddistinta da una determinata tipologia di servizio offerto. I pacchetti di traffico VoIP possono essere, ad esempio, inseriti nella classe a priorità più elevata, mentre quelli HTTP e-commerce in una classe "gold" e così via. Per differenziare ciascuna classe all'interno di ogni singolo router, ognuna di esse è associata a un determinato colore (una

particolare sequenza di bit del campo MPLS Experimental dell'etichetta MPLS) il che consente di rendere il modello assai scalabile e garantisce che anche nel nucleo della rete vengano rispettati i vincoli sulla banda e il ritardo per il traffico trasmesso. L'associazione è realizzata quando un pacchetto entra nella rete ed è marcato in base ai criteri di classificazione applicati.

I router di frontiera possono anche eseguire il controllo sul traffico effettuando *shaping e/o policing*.

Essi, ad esempio, effettuano la cancellazione dei pacchetti che eccedono la capacità concordata o eventuali operazioni di *re-marking*. Ciascun nodo della dorsale applica poi differenti criteri di classificazione del traffico, sia per ciò che concerne la gestione delle code, sia per l'eliminazione di alcuni pacchetti, a seconda di come questi siano stati marcati. Gli approcci utilizzati per poter marcare il traffico MPLS al fine di realizzare un modello DiffServ sono due. Il problema che si pone in questo caso è, infatti, quello di associare alla trama MPLS le informazioni relative alla classe di servizio cui appartiene un flusso di dati.

Una prima soluzione, definita *EXP Infrared-LSP* (E-LSP) [30], consiste nell'utilizzare un unico LSP per tutte le classi di servizio trasportate e "colorare" le varie trame MPLS utilizzando il campo EXP dell'intestazione MPLS. Questo meccanismo consente di poter definire otto differenti classi di servizio, mentre attraverso il campo *TOS (Type Of Service)* dell'intestazione di livello IP in realtà possono esserne definite sino a 64 classi, mediante l'impiego di otto bit. Questa discrepanza è motivata dal fatto che l'etichetta MPLS è stata definita prima della standardizzazione del campo TOS e la sua brevità si giustifica con l'intento di non appesantirla troppo.

È, però, opinione comune che otto classi di servizio potrebbero essere più che sufficienti in futuro per diversificare tutto il traffico presente in rete.

### 5.4.4 IL RIPRISTINO VELOCE DI MPLS (FAST REROUTING)

Un'importante applicazione di MPLS riguarda la possibilità di reagire a condizioni di guasto della rete, quali, ad esempio, fuori servizio di un collegamento, di un nodo, oppure di entrambe queste parti della rete, con tempi di ripristino molto bassi (dell'ordine di 50 ms), tipici dei meccanismi di protezione delle reti SDH.

La tecnica in questione, che prende il nome di *Fast Rerouting* [32] [33], è ottenuta attraverso meccanismi definiti all'interno dell'architettura MPLS-TE che consentono di mantenere per il traffico interessato adeguati livelli di qualità del servizio. Più in particolare, grazie al *Fast Rerouting*, si può anche predisporre l'opzione di utilizzare i percorsi di protezione solo per il

traffico con priorità più elevata, lasciando che il *best-effort* continui a essere gestito dai protocolli tradizionali di routing e garantendo l'immissione dei pacchetti in un *Fast Reroute Path* mediante l'impiego di una classificazione di tipo *Diffserv*.

In una rete MPLS con funzionalità TE di *Fast Rerouting* i tempi necessari per l'instaurazione dei tunnel alternativi e per il ripristino da una condizione di guasto a una nuova possibile sono minimi, in quanto il percorso di riserva è pre-calcolato e pre-allocato direttamente, durante la fase di instaurazione dell'LSP primario. In aggiunta in questo caso sono utilizzati meccanismi di rilevazione dell'anomalia stati definiti tre diversi meccanismi di protezione:

a) *Link Protection,* in grado di reagire a un malfunzionamento su di una connessione.

b) *Node Protection,* che consentono di rispondere a un malfunzionamento su di un nodo.

c) *Path Protection,* in grado di proteggere un intero percorso in seguito a un'anomalia che si presenti su di esso.

### 5.4.5 SERVIZI CHE UNA TELCO PUÒ OFFRIRE CON USO DI MPLS)

Una dorsale di rete IP con questa architettura permette ad una TELCO di offrire ai propri clienti un servizio di VPN IP con qualità di servizio garantita all'interno della singola VPN. Fornire servizi esterni, come accesso alla rete pubblica (Internet), colloquio affidabile fra differenti VPN (Extranet), accesso ad aree legate alla fornitura di servizi a valore aggiunto (E-mail, Web caching, Web hosting, DNS, content delivery, database, …). Si ha la possibilità di offrire ai propri Clienti, grazie alla presenza di MPLS nella propria dorsale IP. Si ha la possibilità di offrire servizi a qualità differenziata e con elevata affidabilità per il trasporto di differenti tipi di traffico (real-time, Voice over IP, telefonico). In questo contesto sono certamente significative le funzionalità di TE e Fast Rerouting

### 5.4.6 ARCHITETTURA INTRANET CON VPN MPLS

Con l'architettura IP-MPLS le Telco possono rispondere alle nuove esigenze dovute allo sviluppo disordinato di reti a seguito della crescente richiesta di servizi, sviluppo che ha portato al proliferare di reti specializzate e distribuite sullo stesso territorio. La situazione è già stata descritta al capitolo 5.1 fig. 29. Avvalendosi della nuova architettura IP-MPLS nelle singole sedi possono essere attivate

le varie reti che in fig. 36 sono rappresentate come appartenenti alle VPN A, B, C, D e condividere con accesso ai PE lo stesso dominio IP-MPLS.

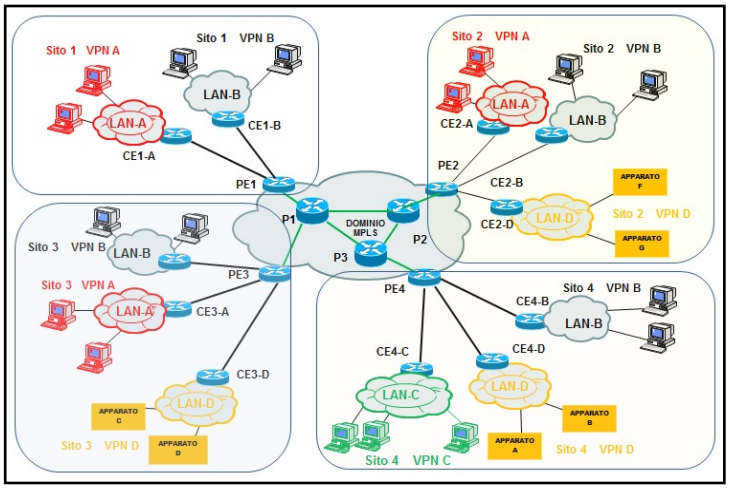



Figura 36 – Architettura intranet VPN MPLS

## Bibliografia


[1] Laubach, M.; Halpern, J.: *Classical IP and ARP Over ATM.* RFC 2225, aprile 1998.

[9] Davie, B.; Rekhter, Y.: *MPLS Technology and Applications.* Morgan Kaufman Ed., aprile 2000.

[10] Comer, D.: *Internetworking with TCP/IP: Principles, Protocols, Architecture.* Prentice Hall, 1995.

[11] Rosen, E.; Viswanathan, A.; Callon, R.: *Multiprotocol Label Switching Architecture.* RFC 3031, gennaio 2001.

[13] Andersson, L.; Doolan, P.; Feldman, N.; Fredette, A.; Thomas, B.: *LDP Specification.* RFC 3036, gennaio 2001.

[14] Thomas, B.; Gray, E.: *LDP Applicability.* RFC 3037, gennaio 2001.

[17] Awduche, D. et al.: *MultiProtocol Lambda Switching: Combining MPLS Traffic Engineering Control With Optical Crossconnects.* Internet draft-awduche-mpls-te-optical-03.txt, aprile 2001.

[28] Rosen, C. et al.: *BGP/MPLS VPNs.* Internet draft-ietf-ppvpn-rfc2547bis-00.txt, luglio 2001.

# 6. LE RETI DATI VERSO RETI “FULL IP”

Le TELCO sono aziende che offrono servizi digitali attraverso lo sviluppo di piattaforme di rete con architettura convergente verso uno scenario Full IP Cloud Based e con Accessi UBB [1] e progressivo abbandono di tecnologie e servizi legacy. Nello scenario ”All-IP”, la totalità dei servizi e delle applicazioni utilizzate dagli End Users e dalle Aziende, attraverso terminali fissi e mobili, saranno basate su IP (Internet Protocol [2, 3]), e la totalità del traffico nelle reti sarà costituito da pacchetti IP; ciò ha conseguenze importanti per le scelte architetturali e tecnologiche. Infatti, le reti attuali sono il frutto di un pluridecennale processo di “stratificazione” ed “affiancamento” di architetture e tecnologie, nate per trattare servizi e comunicazioni che originariamente non erano basate su IP, ma su traffico “a circuito”. Inoltre, alle reti che offrivano servizi solo verso terminazioni “fisse”, si sono successivamente affiancate reti concepite per connettere terminali mobili; nel tempo sono progressivamente aumentate le “parti in comune” fra reti fisse e reti mobili (ad es. molte infrastrutture di trasmissione, e la “rete dati dorsale - backbone” che trasporta il traffico a livello interregionale).

Anche se ancora oggi coesistono soluzioni specializzate per “il fisso” e per “il mobile”, l’evoluzione dei servizi si sta velocemente spostando verso il concetto dell’*access independent*, ossia i servizi sempre più sono richiesti e fruiti da qualunque tipo di accesso e su qualunque tipo di *device*. Le tipologie di servizio sempre più risiedono nel Cloud, alcuni esempi sono servizi IoT e la distribuzione dei servizi video verso il singolo End User nel momento da lui scelto.

L’evoluzione verso l’All-IP è caratterizzata da un altro cambiamento fondamentale.

- In passato i “servizi” di telecomunicazione erano sostanzialmente offerti “nella” rete; il servizio telefonico era realizzato direttamente dagli apparati esistenti nelle centrali; di fatto, il servizio *coincideva* con la rete.
- Con l’ALL-IP, l’End User utilizza invece, applicazioni disponibili su Internet, realizzate da Server che sono “fuori” dalla rete e gestiti da soggetti diversi dai Telco, gli OTT (Over The Top) cher erogano servizi quali Skype, googleVoice, WhatsApp……

In una rete “Full-IP”, un’infrastruttura unica, condivisa tra tutti i flussi di traffico che la attraversano, tratta indistintamente, a livello di protocollo IP qualsiasi tipo di traffico (video, posta elettronica, browsing, …), come richiesto dalle regole definite per Net Neutrality/Open Internet [4]. Gli End Users tipicamente scambiano traffico IP con “Server” accessibili sulla Internet Globale, e le

prestazioni fornite dall'IP dipendono essenzialmente dalla topologia della rete (numero di router attraversati) e dal tipo di router. Ne consegue che per alcuni servizi le prestazioni offerte dal puro trasporto IP non sono in grado di garantire i livelli di qualità richiesti dai servizi e dalle applicazioni degli End Users (QoE – Quality of Experience).

Occorre migliorare:

- il *Throughput* a livello applicativo cioè l'effettiva velocità di trasferimento delle informazioni quando l'utente finale utilizza un'applicazione o accede ad un contenuto sul WEB;
- Il "Download Time", cioè il tempo necessario per accedere e scaricare le "informazioni" da Internet; questa grandezza dipende dall'efficienza della completa suite protocollare utilizzata.

## 6.1 LA SUDDIVIZIONE IN SEGMENTI DELLE RETI DATI

Le TELCO si sono dotate di reti a pacchetto rappresentate schematicamente in Figura 37. In prima approssimazione esse si compongono di 4 segmenti [5]:

- La *dorsale* o *Backbone* di una TELCO fornisce connettività in forma aggregata a livello nazionale tra i PoP (*Point of Presence*) della rete IP. La principale rete dorsale è realizzata in tecnologia IP/MPLS direttamente su un'infrastruttura ottica. 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 di una TELCO 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 ma dalla prima decade degli anni 2000 a questa viene affiancata una rete di accesso in tecnologia Carrier Ethernet IP/MPLS (Multi-Protocol Label Switching) denominata OPM (Optical Packet Metro) [6], che ora 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) che è in evoluzione.
- *La terminazione in sede cliente* che può essere controllata da parte di una TELCO; 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 mantengono uno stato specifico per ogni cliente che lo caratterizza in termini di tipo di connettività richiesta, prestazioni, etc.

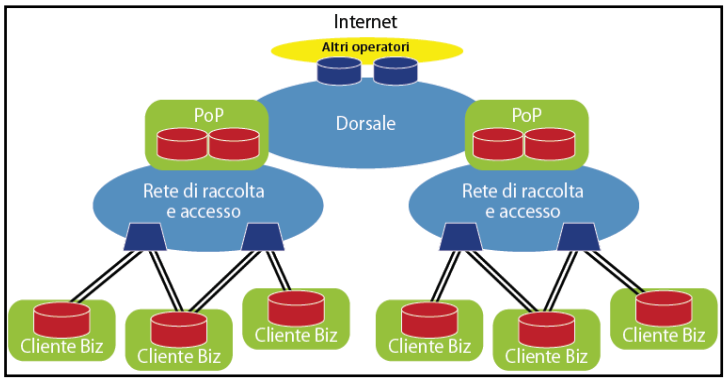



Figura 37 - Schema della rete dati

Si descrivono nei paragrafi seguenti la modalità realizzativa dei servizi dati messi a disposizione di clienti business e clienti residenziali.

## 6.2 I SERVIZI DATI

Fra gli operatori TELCO, per i servizi di rete fissa, non vi è un modello realizzativo univoco. Sono infatti emersi nelle implementazioni degli operatori vari modelli e vi sono differenze fra operatori 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.
Allo scopo di proporre modelli di riferimento si sono affermati gli enti di standardizzazione in cui sono sviluppate le soluzioni architetturali e di protocollo per i servizi di rete fissa:

- L' IETF è un ente internazionale che si occupa della standardizzazione dei protocolli per la rete Internet;
- BBF (BroadBand Forum) [8] è l'ente che si occupa della standardizzazione dell'architettura della rete broadband di accesso, aggregazione e Edge IP. La sua attività si concentra sulle architetture e sugli apparati, con l'obiettivo di garantire l'interoperabilità end-to-end delle catene di servizio, pur in uno scenario in cui sono possibili più modelli realizzativi per lo stesso servizio.

Nei due paragrafi che seguono ci poniamo nella veste degli operatori che hanno scelto l'approccio *Multiple Edge*, dove esistono piattaforme di Edge dedicate per ciascun servizio.

### 6.2.1 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*) inserito nella rete IP/MPLS e che 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 IPv4 di livello 3.

È possibile fornire una connettività Ethernet mediante il servizio VPLS (*Virtual Private LAN service*), con cui si realizza una VPN di livello 2. 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 38 mostra il modello di QoS operato da tali apparati, che avviene mediante una gestione multi-livello della capacità trasmissiva contesa tra clienti diversi e classi di servizio (meccanismo chiamato Hierarchical QoS, HQoS).

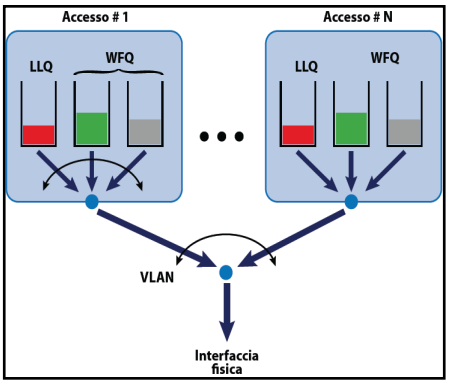


Figura 38 - Gestione delle code a priorità differenziata

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 la 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).

### 6.2.2 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.

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*). Tale elemento, inserito nella rete TELCO come ad esempio nella configurazione di Figura 39, 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).

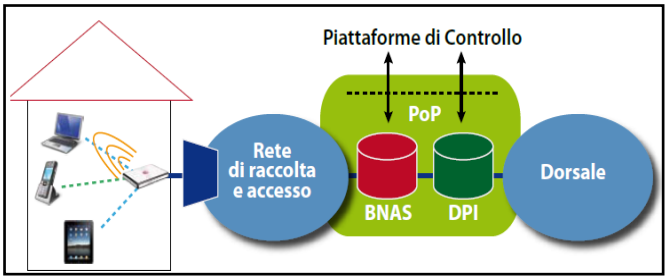



Figura 39 - Catena impiantistica per clienti MM

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 il terminale del cliente opera essenzialmente come un modem terminatore di linea ADSL. Nel secondo caso si parla di accesso *Routed* e 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 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.

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*);
    - *Autenticazione:* per autenticare la linea cliente Il BNAS, ricevute le credenziali del cliente, interroga un server di autenticazione per verificarne la correttezza e lo fa utilizzando il protocollo RADIUS (*Remote Authentication Dial-In User Service*);
    - *Autorizzazione: se la procedura di Autenticazione ha* esito positivo, essa si conclude con l'*autorizzazione* del cliente ad accedere al servizio richiesto;
    - *Accounting:* consiste nel fornire la "documentazione" relativa all'attività del Cliente

- 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). L'assegnazione avviene in modalità dinamica, sfruttando le funzioni di RADIUS e PPP.
    - *ai Clienti Business* vengono attribuiti indirizzi IP permanenti, questa modalità è considerato un plus in quanto consente al Cliente di essere raggiunto sempre con lo stesso indirizzo IP. Questa caratteristica è utile al Cliente che dietro la propria connettività IP voglia esporre un sito web.
    - *ai Clienti consumer* vengono assegnati indirizzi IP temporanei.

- applicazione di regole di trattamento dei pacchetti IP (*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. 7Mega, 20Mega).
- Ci sono altri elementi caratterizzanti e distintivi del profilo cliente, ad esempio per clienti Small Business è prevista la configurazione di una Banda Minima Garantita.
- 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. *Policy Control* interviene allo scopo 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 [10].

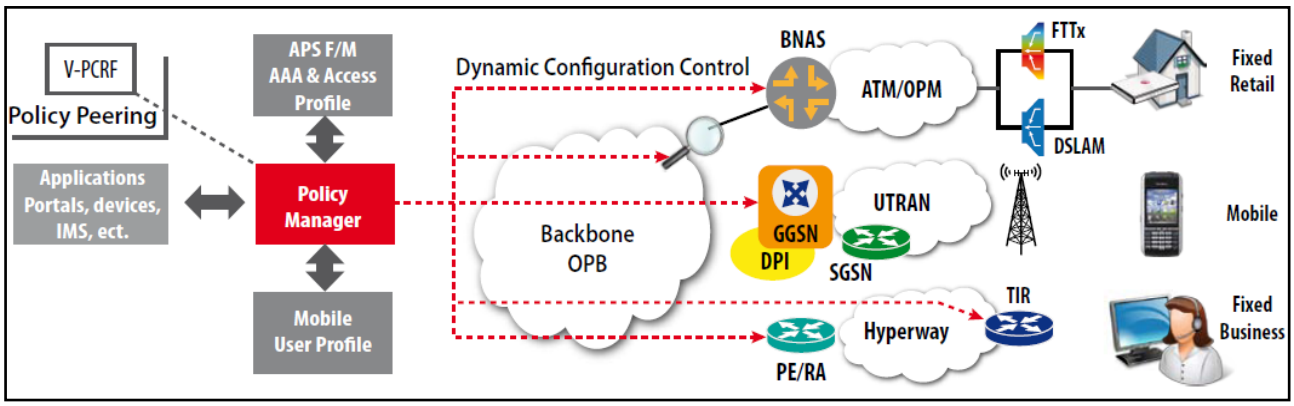



Figura 40 - La soluzione Policy manager [10].

• Deep Packet Inspection;

- In Figura 39 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 applicazione. Tale classificazione fine consente un efficace monito-

raggio 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 41. 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. La soluzione di *Traffic Management* mette in pratica una *Fair (giusta) Use Policy*, che permette alla totalità dei clienti un utilizzo soddisfacente della rete.

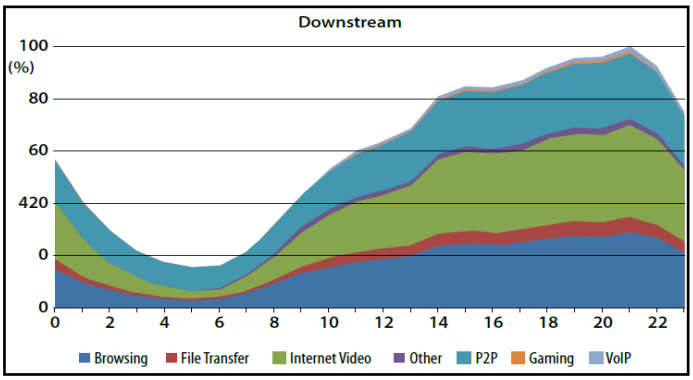



Figura 41 - Profilo del traffico proveniente da Internet registrato ad Aprile 2012

## 6.3 EVOLUZIONE DEGLI APPARATI E NUOVE ARCHITETTURE DI RETE

Nel secondo decennio degli anni 2000 si presentano delle innovazioni che dal punto di vista tecnologico, sono funzione dei trend evolutivi degli apparati, e dal punto di vista di architetture di rete vedono una promettente direzione di sviluppo in un modello denominato Seamless MPLS. I risultati dell'evoluzione degli apparati sono la semplificazione del PoP e l'incremento dell'affidabilità della rete.

### 6.3.1 EVOLUZIONE DELLE TECNOLOGIE EDGE

La necessità di ridurre i costi per i servizi broadband e il contemporaneo incremento della banda per linea cliente porta i 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

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).

### 6.3.2 MODELLO SEAMLESS MPLS

La tecnologia IP/MPLS è utilizzata dall'inizio degli anni 2000 all'interno delle reti dorsali dei principali operatori a livello mondiale e in Italia da Telecom Italia, con la rete OPB. L'elevata maturità tecnologica di IP/MPLS ha consentito la realizzazione di reti a pacchetto estese in grado di offrire funzionalità quali: strumenti gestionali evoluti, possibilità di monitoraggio costante della qualità del servizio di trasporto, meccanismi di re-instradamento molto veloci.

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 e anche dalla rete metro regionale OPM di Telecom Italia che dal 2005 sta sostituendo l'infrastruttura di raccolta ATM e oggi costituisce una robusta rete multi-servizio in grado di raccogliere il traffico di servizi di rete fissa e mobile della clientela residenziale e business. 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 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* [11][12] 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*);
- 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;
- utilizza gli PW (*Pseudowire*) per realizzare le direttrici di servizio.

In Figura 42 sono riportate, a titolo di esempio, tre diverse tipologie di collegamenti logici di tipo PW, che 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.

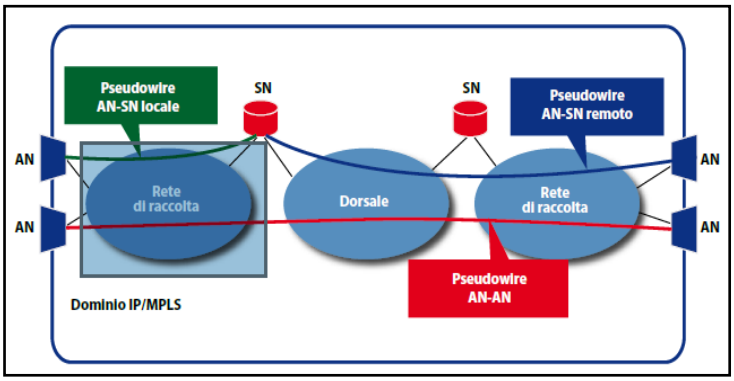



Figura 42 - Architettura Seamless MPLS

Scendendo più nel dettaglio, per il piano di controllo, il modello *Seamless MPLS* utilizza i seguenti protocolli di routing:

- OSPF (*Open Shortest Path First)*: per consentire la mutua 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 [13].

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 44 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 SN, 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.

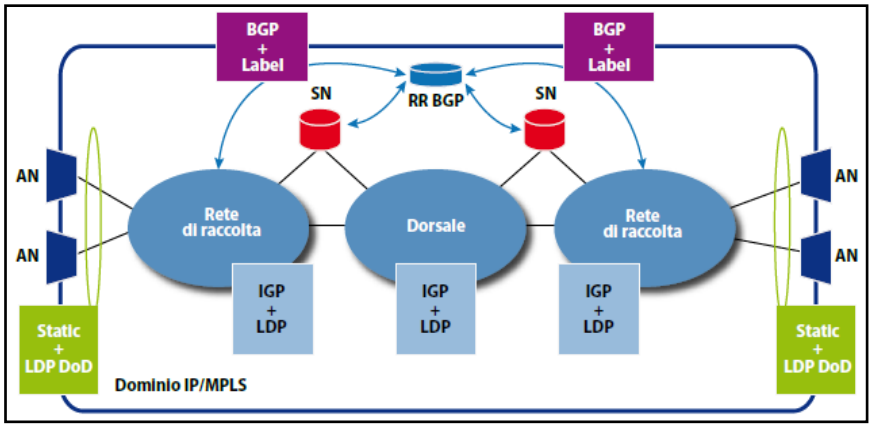



Figura 43 - Piano di controllo della soluzione *Seamless MPLS*

Quest'ultimo consente di realizzare e mantenere in modo automatico e scalabile la connettività *any-to-any* tra qualunque coppia di nodi 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.

## Bibliografia

[1] G. Catalano, D. Franceschini, A. Pavese, D. Roffinella, "Il paradigma Full IP a supporto della Digital Telco Network", Notiziario tecnico Telecom Italia, Anno 25, numero 1, agosto 2016.

[2] http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

[3] http://www.cisco.com/en/US/docs/security/vpn5000/manager/reference/guide/appA.html

[4] http://www.agcom.it/-/avvio-di-un-indagine-conoscitiva-concernente-lo-sviluppo-delle-piattaforme-digitalie-
dei-servizi-di-comunicazione-elettronica-delibera-n-357-15-cons-

[5] P. Fasano, D. Marocco, G. Picciano, "Rete Dati di Telecom Italia: Network", Notiziario tecnico Telecom Italia, Anno 21, numero 2, 2012.

[6] M. Bianchetti, G. Picciano, L. Venuto, “NGN2: la parte metro”, Notiziario tecnico Telecom Italia, Anno 17, numero 2, agosto 2008.
[7] http://www.ietf.org
[8] http://www.broadband-forum.org/
[9] https://www.opennetworking.org/
[10] 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.
[11] M. Billotti, “Come cambiano le piattaforme di rete”, Notiziario tecnico Telecom Italia, Anno 19, numero 2, 2010.
[12] K. Kompella, “MPLS in the access”, 11th MPLS Conference 2008, Washington, Ottobre 2008.
[13] Y. Rekhter, E. Rosen, “Carrying Label Information in BGP-4”, RFC3107, 2001

# 7. INTEGRAZIONE FRA LA RETE IP E LA RETE DI TRASPORTO OTTICA

## 7.1 LA RETE IP E LA RETE DI TRASPORTO OTTICA

Nel corso degli ultimi anni si sono verificati due fenomeni che stanno portando ad una trasformazione della rete. Da un lato, come abbiamo descritto in Cap. 6, già il protocollo IP si sta affermando come l'unico protocollo utilizzato sia per la rete fissa che per quella mobile, per tutti i tipi di servizio (voce, video, dati, ecc.) e per tutti i tipi di clientela (residenziale business e wholesale). Dall'altro, la continua crescita del traffico richiede una rete in grado di fornire sempre più capacità a costi contenuti.La rete geografica (Wide Area Network, WAN) che costituisce l'infrastruttura di connessione della rete multi-servizio figure 37 e 43, ha una struttura gerarchica e risulta composta da due segmenti distinti [1]:

- il segmento metro/regionale (*rete di accesso e raccolta*) che aggrega il traffico proveniente dalla rete di accesso verso i PoP nei quali sono presenti i nodi di servizio SN;
- la rete di lunga distanza (*dorsale* o *Backbone*) che collega i PoP fra loro e ai gateway internazionali verso Internet.

La progressiva convergenza di tutti i servizi su IP sta portando ad una semplificazione della WAN che, a tendere, sarà costituita essenzialmente da due livelli:

- uno strato a pacchetto, con lo scopo di effettuare una aggregazione efficiente del traffico;
- uno strato ottico che ottimizza l'uso della fibra ottica, fornendo una serie di connessioni a banda molto elevata mediante la multiplazione a divisione di lunghezza d'onda (WDM).

Infatti, oggi la rete backbone di TIM è costituita da uno strato IP/MPLS, chiamato OPB, che si appoggia sulla rete ottica Kaleidon. Analogamente, nelle zone metropolitane a più alta densità di traffico, esiste uno strato IP/MPLS, chiamato OPM, che si appoggia, almeno in parte, su reti Metro WDM (figura 44).

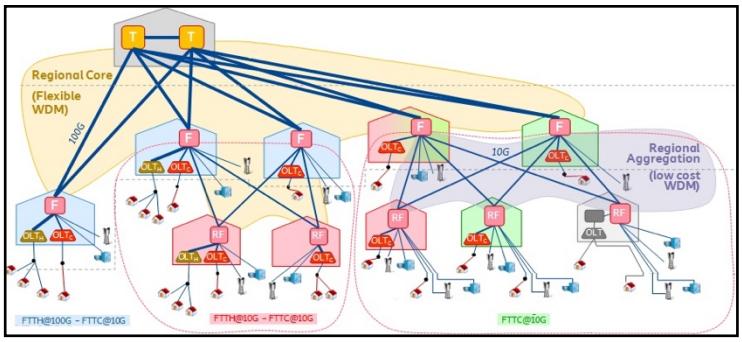



Figura 44 – rete metro/regionale OPM su reti Metro WDM.

La decisa crescita del traffico prevista richiede che la capacità della rete OPB e delle MAN OPM riesca a scalare progressivamente. Su OPB è stato avviato un processo di rinnovamento, denominato NGCN (Next Generation Core Network), che porterà a un'architettura gerarchica costituita da PoP Principali e PoP Secondari. I PoP Principali, equipaggiati con una nuova generazione di router saranno collegati fra loro con canali ottici a 100 Gbit/s. La trasformazione del livello IP è accompagnata da cambiamenti anche nel livello ottico: l'introduzione di lunghezze d'onda a 100 Gbit/s su Kaleidon per supportare le interconnessioni fra i PoP primari di NGCN e una progressiva introduzione di apparati ROADM, analoghi a quelli già presenti su Kaleidon, anche sulle reti Metro WDM per aumentarne la flessibilità. Allo stato attuale nella rete di TIM, come in quelle dei principali operatori, lo strato IP e quello Ottico sono separati e fra essi esiste una relazione di tipo client/server, ma non esiste alcuna interazione a livello di controllo e gestione, come mostrato nello schema di principio di figura 45.

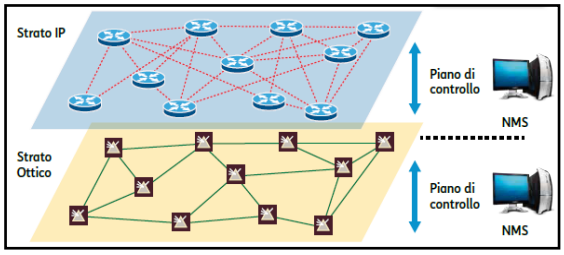



Figura 45 - Relazione fra lo strato IP e lo strato ottico

I router dello strato IP sono connessi fra loro da link secondo una certa topologia logica, che dipende essenzialmente dalle principali direttrici di traffico e dalla necessità di avere percorsi alternativi che consentano la sopravvivenza in caso di guasto. Ciascun link è ottenuto mediante un canale ottico fornito dalla rete WDM sottostante. La topologia della rete WDM è invece di tipo

fisico, perché dipende strettamente dalla disposizione dei cavi. Essa è quindi diversa dalla topologia dello strato IP.

Ciascuno dei due strati dispone di un proprio piano di controllo e di propri sistemi OSS per la gestione di rete, ma non c'è comunicazione fra i piani di controllo e gli OSS dei due strati. La separazione fra i due strati di rete esiste anche a livello di processi aziendali. Infatti, la pianificazione delle due reti avviene in modo separato e l'unico legame è costituito dal fatto che i link della rete IP sono un input alla pianificazione della rete ottica. Analogamente, l'esercizio delle due reti avviene in modo indipendente e con metodologie diverse. Per lo strato IP è fondamentale la presenza del piano di controllo che automatizza le funzioni di instradamento. Per lo strato ottico, invece è fondamentale l'uso del sistema di gestione OSS centralizzato per svolgere tutte le attività di creation, provisioning ed assurance, mentre il piano di controllo GMPLS ha un ruolo meno importante.

## 7.2 L'INTEGRAZIONE DELLA RETE IP CON LA RETE OTTICA

In passato la rete di trasporto ottica aveva il compito di fornire connettività a più reti client diverse e ciascuna di esse richiedeva connessioni velocità nettamente inferiori rispetto a quelle delle lunghezze d'onda presenti sui sistemi WDM[1]. L'adattamento fra la velocità delle connessioni richieste dalle reti client (ad esempio 1 o 2.5 Gbit/s) su lunghezze d'onda a più alta velocità (ad es. 40 o 100 Gbit/s) veniva ottenuto mediante multiplazione TDM.

La veloce crescita del traffico IP ha cambiato radicalmente questa situazione.

Oggi, infatti, la rete IP è il client principale della rete ottica e le porte dei router operano a velocità comprese fra 10 e 100 Gbit/s, le stesse delle lunghezze d'onda presenti sulla rete ottica. Si tende quindi ad avere sempre più una corrispondenza uno a uno fra i link dello strato IP e le lunghezze d'onda dello strato ottico. Diventa, quindi, sempre più importante progettare la rete ottica in modo da ottimizzare il suo client principale che è la rete IP. Questa tendenza ha portato allo studio dei possibili benefici derivanti da una progressiva integrazione fra questi due strati che, in generale, può essere ottenuta in modi diversi: a livello di piano dati, di piano di controllo e/o di piano di gestione.

I principali benefici attesi da questa integrazione rientrano nelle seguenti categorie:

- riduzione dei costi complessivi derivante da una ottimizzazione congiunta delle risorse di rete sui due strati;
- automazione del set-up di nuove lunghezze d'onda fra i router;

- miglioramento delle prestazioni per alcune categorie di servizi attraverso una scelta ottimizzata dell'instradamento;
- miglioramento dell'affidabilità per i servizi basati su IP attraverso instradamenti che tengono conto della topologia fisica dello strato ottico e tecniche di multi-layer resilience.

## 7.3 IMPIEGO DI INTERFACCE OTTICHE COLORATE SUI ROUTER

Le reti ottiche si basano sulla multiplazione WDM, cioè sul concetto di trasmettere più canali su di una stessa fibra, associandoli a diverse lunghezza d'onda [1].

Le prestazioni trasmissive di un sistema WDM vengono sinteticamente indicate da tre parametri:

- il numero di canali utilizzabili,
- la massima velocità (bit rate) di ciascun canale
- la massima distanza raggiungibile senza rigenerazione (per tipo bit rate e per un tipo di fibra).

Attualmente gli standard relativi alle reti ottiche regolano il tipo di interfacce disponibili fra il sistema WDM e gli apparati client, ad esempio router, in modo da garantire un'interoperabilità fra costruttori diversi. Il segnale ottico su questa interfaccia è detto "grigio", poiché lo standard non specifica un particolare "colore", cioè una lunghezza d'onda precisa. Per garantire questa interoperabilità, ciascun canale di un sistema WDM è dotato di un dispositivo, detto trasponder, che esegue una conversione ottico/elettrico/ottica (OEO). Lo schema di principio di un trasponder è mostrato in figura 46. Esso riceve in ingresso il segnale grigio dell'apparato client, lo riporta in formato elettrico e poi genera un nuovo segnale ottico colorato, avente la lunghezza d'onda, il formato di modulazione e tutte le altre caratteristiche necessarie per essere multiplato e trasmesso con le prestazioni volute lungo la linea.

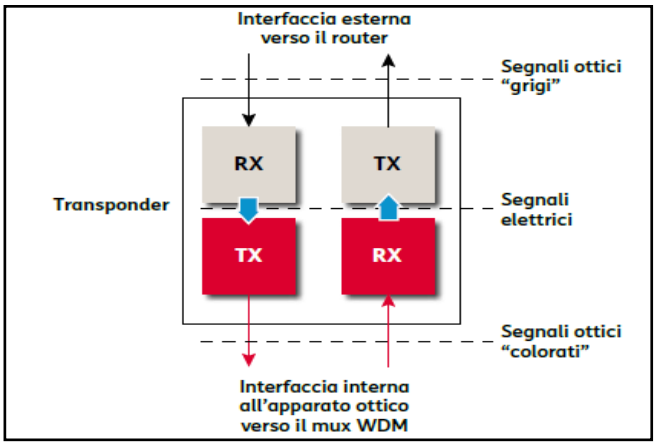



Figura 46 - Schema di principio di un trasponder

A livello di linea, invece, ciascun costruttore è libero di agire come meglio crede sui parametri fisici dei segnali ottici:

- formato di modulazione;
- livello di potenza;
- codice correttore di errori (FEC),

in modo da ottimizzarne le prestazioni. Questo impedisce l'interoperabilità fra sistemi WDM forniti da costruttori diversi. In ITU si sta lavorando ad un nuovo standard che consenta l'interoperabilità anche a livello di linea, ma questo può comportare una riduzione delle prestazioni del sistema, perché si riducono i gradi di libertà a disposizione del costruttore per ottimizzare le prestazioni complessive.

Quindi è ragionevole che questo tipo di interoperabilità sarà possibile solo per i sistemi Metro WDM, per i quali la massima distanza raggiungibile senza rigenerazione non è un parametro troppo importante, mentre l'interoperabilità non verrà garantita per i sistemi long haul, che devono proprio essere ottimizzati per raggiungere grandi distanze. In figura 47 è visibile uno schema semplificato dell'interconnessione fra una coppia di router ottenuta attraverso un sistema WDM. La figura 47a mostra la situazione attuale, che prevede l'utilizzo del trasponder per adattare ogni segnale ottico che entra nel sistema WDM: per ogni link fra due router sono necessari due trasponder. Il tipo di integrazione IP/Ottico concettualmente più semplice consiste nell'inserire l'interfaccia colorata direttamente sulle porte dei router, eliminando la necessità di usare i trasponder sul sistema WDM, come mostrato in figura 47b. Il vantaggio di questa soluzione è il risparmio di una coppia di trasponder, che si traduce sia in un minore investimento per l'acquisto di hardware sia in un risparmio di consumi elettrici e di spazi.

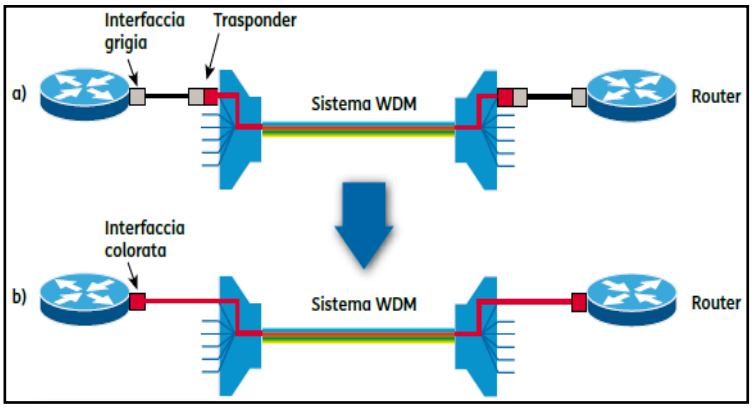


Figura 47 - Schema di interconnessione dei router alla rete ottica con trasponder (a) e senza trasponder (b)

Questa soluzione presenta però alcuni problemi:

- l'interoperabilità fra le interfacce colorate di router forniti da costruttori diversi non è garantita per l'assenza di standard a livello di linea;
- la rete ottica perde le funzionalità di performance monitoring su questa lunghezza d'onda perché queste funzioni sono localizzate all'interno dei ricevitori che ora si trovano nei router, al di fuori della rete ottica; per questo motivo una lunghezza d'onda di questo tipo viene anche detta "alien wavelenght".

Oggi la soluzione di integrazione IP/Ottico mediante interfacce colorate sul router funziona bene in un ambiente mono-vendor, nel quale tutti i router e gli apparati ottici sono forniti dallo stesso costruttore. La sua applicazione ad un ambiente multi-vendor verrà favorita dai nuovi standard ITU sull'interoperabilità a livello di linea di un sistema WDM, almeno nel caso di reti ottiche di piccole dimensioni come quelle Metro WDM.

La disponibilità delle informazioni di performance trasmissive sulla porta del router consente, d'altra parte, di mettere in atto strategie di proactive protection nelle quali lo strato IP/MPLS re-instradi rapidamente il traffico non appena rilevi un degrado delle prestazioni del link, in modo da minimizzare l'impatto sui servizi.

## 7.4 INTEGRAZIONE A LIVELLO DI PIANO DI CONTROLLO CON GMPLS UNI

Un altro tipo di integrazione fra strato IP e strato ottico è quello a livello di piano di controllo ottenuto mediante l'interfaccia GMPLS UNI [1]. Lo strato IP ha un proprio piano di controllo basato sull'impiego di un insieme di protocolli di instradamento e segnalazione definiti da IETF ed indicati sinteticamente come piano di controllo IP/MPLS.

IETF ha generalizzato i protocolli del piano di controllo IP/MPLS per renderli adatti anche a reti di trasporto basate su multiplazione di tipo TDM e WDM. È nato così il piano di controllo GMPLS.

È poi stata definita un'interfaccia di segnalazione fra i due piani di controllo che consente allo strato IP/MPLS di richiedere l'attivazione automatica di una nuova connessione (lunghezza d'onda) fra le porte di due router. Questa interfaccia è detta UNI User Network Interface, perché consente allo uno strato client IP (user) di chiedere alla rete ottica (network) una funzione di provisioning automatico.

L'interfaccia UNI è limitata perché non consente di specificare caratteristiche importanti della nuova connessione. Ad esempio, non è possibile richiedere che la nuova connessione abbia un percorso fisicamente separato da quello di un'altra connessione già esistente, requisito molto importante per garantire che i meccanismi di recovery del livello IP/MPLS funzionino correttamente quando si verifica un guasto a livello di rete ottica. Per colmare questo vuoto, vari costruttori hanno sviluppato estensioni proprietarie dell'interfaccia UNI che non sono mai state standardizzate. In particolare, quelle più interessanti dal punto di vista dell'integrazione IP/Ottico sono:

- estensioni che consentono alla rete ottica di comunicare al piano IP/MPLS la topologia fisica dei collegamenti e la presenza di SRLG cioè di punti nei quali un unico guasto fisico interrompe più connessioni (ad esempio, perché due cavi diversi si trovano per un certo tratto nella stessa tubazione);
- estensioni che consentono allo strato IP/MPLS di richiedere connessioni con vincoli sull'instradamento.

L'impiego della GMPLS UNI standard consente l'interoperabilità fra router di un costruttore e rete ottica di un costruttore diverso, ma non offre grandi vantaggi a causa delle sue funzioni limitate. D'altra parte, le estensioni proprietarie alla UNI rendono le possibilità di integrazione fra i due strati di rete più interessanti, ma funzionano solo in un ambiente mono-vendor.

### 7.4.1 L'INTERFACCIA GMPS UNI

La GMPLS UNI (*Generalized Multi-Protocol LabelSwitching User to Network Interface*) permette il provisioning automatico di connessioni tra router IP/MPLS attraverso una rete ottica di trasporto ed è stata definita con l'obiettivo di fornire uno strumento per ridurre i tempi ed i costi necessari per

realizzare tali connessioni[2]. L'interfaccia UNI rappresenta un chiaro punto di demarcazione tra la rete IP/MPLS e quella di trasporto ottica, come mostrato in figura 48.

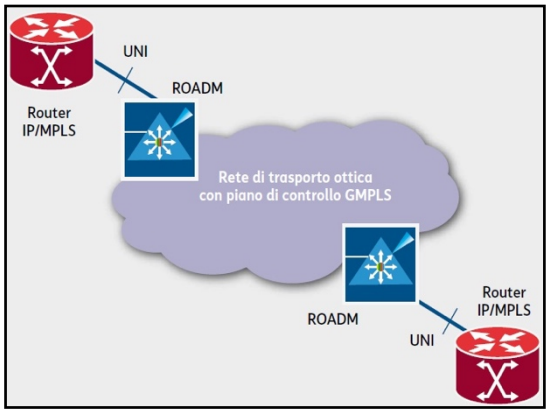



Figura 48 – Interfaccia GMPS UNI

Essa è stata specificata da IETF nella RFC 4208 "GMPLS (*Generalized Multiprotocol Label Switching*) UNI (*User-Network Interface*): RSVP-TE (*Resource ReserVation Protocol-Traffic Engineering*)". Il modello della GMPLS UNI è basato su un approccio overlay, secondo il quale il piano di controllo della rete IP/MPLS è trasportato in modo trasparente dalla rete ottica che, a sua volta, è controllata da un piano di controllo GMPLS indipendente da quello IP/MPLS. Questo implica che i router IP/MPLS non siano a conoscenza della topologia interna della rete di trasporto, ma che possano essere informati circa la raggiungibilità degli altri router attestati alla rete ottica. La specifica RFC 4208 definisce i messaggi attraverso i quali un router può richiedere alla rete ottica l'instaurazione di una connessione, ma non definisce in dettaglio alcuni importanti parametri addizionali che possono caratterizzare una connessione (ad es.: la banda, la priorità, il tipo di protezione o la diversità di percorso rispetto ad altre connessioni). Questi parametri addizionali sono stati implementati da molti costruttori di apparati in modo proprietario, rendendo di conseguenza molto difficile l'interoperabilità tra le diverse implementazioni.

## 7.5 INTEGRAZIONE MEDIANTE TRANSPORT SDN

Il concetto di SDN (Software Defined Network)[1] trova applicazione in diverse parti della rete di un operatore:

- per la gestione del networking all'interno dei Data Center utilizzati per il Cloud Computing e per ospitare funzioni di rete virtualizzate;
- per il Flexible Service Chaining all'interno dei PoP, che consente la creazione di servizi attraverso la concatenazione di una serie di blocchi elementari da utilizzare su richiesta del cliente;
- per il controllo della WAN.

Con il termine Transport SDN si intende l'applicazione dei concetti SDN ad una WAN, in particolare, all'insieme della rete IP e della rete ottica che costituiscono l'infrastruttura di connessione di una rete multiservizio.

L'impiego di T-SDN consente un'integrazione fra i due strati di rete a livello di piano di controllo, questa volta centralizzato, che supera le limitazioni della GMPLS UNI. Infatti, un controllore T-SDN che implementi la funzione di multi-layer Path Computation Element (PCE) è in grado di vedere sia la topologia della rete IP che quella della rete ottica e, quindi, di gestire i percorsi in modo ottimizzato in entrambi gli strati di rete.

Le applicazioni di un multi-layer PCE sono molteplici. Quella probabilmente più semplice è la creazione automatica delle lunghezze d'onda che collegano fra loro i router, come con la GMPLS UNI. La conoscenza della topologia dello strato ottico, inclusi gli SRLG, può inoltre consentire di calcolare percorsi di traffic engineering per lo strato IP che siano ottimizzati sulla base di criteri come la minima latenza o l'affidabilità. L'integrazione dei piani di controllo abilita anche soluzioni di multi-layer resilience, nelle quali lo strato IP e lo strato ottico collaborano per la protezione contro i guasti. Anche nel caso della T-SDN la sfida principale consiste nel realizzare un controllore che sia in grado di operare su entrambi gli strati di rete in un ambiente multi-vendor. Al momento iniziano ad essere disponibili controllori SDN sia per lo strato ottico che per lo strato IP, ma non esistono ancora controllori in grado di operare su di una rete multi-layer. Per lo strato IP, grazie all'attività di standardizzazione svolta da IETF, alcuni controllori SDN hanno già dimostrato in "prove di laboratorio" di essere in grado di interoperare con router di costruttori diversi. Per lo strato ottico esistono due tipi di problemi che rendono più difficile l'interoperabilità:

- i lavori di standardizzazione dell'interfaccia southbound del controllore T-SDN sono in uno stadio meno avanzato;
- il PCE dello strato ottico deve conoscere le caratteristiche fisiche della rete per poter calcolare gli instradamenti delle lunghezze d'onda (deve tenere conto dei cosiddetti physical impairments) e queste non sono standard.

Questi problemi possono essere superati utilizzando, anziché un singolo controllore SDN per l'intera rete IP/Ottica, un'architettura gerarchica di controllori "come mostrato in figura49".

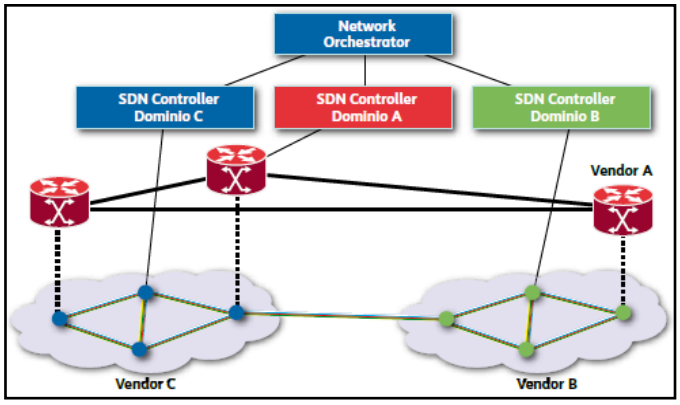



Figura 49 - Architettura SDN gerarchica per il controllo di una rete IP/Ottico multi-vendor

In questa architettura, la rete è suddivisa in domini con caratteristiche diverse ciascuno dotato di un proprio controllore SDN. Ad esempio, si potrebbero avere diversi domini a livello ottico, uno per ciascun costruttore, ed un solo dominio multi-vendor a livello IP. L'interazione fra i diversi controllori di dominio è gestita da un livello di intelligenza superiore che svolge funzioni di orchestrazione di rete. Per l'integrazione della rete IP con la rete di trasporto ottica l'impiego di T-SDN è lo strumento più promettente, anche se esistono ancora alcuni problemi da risolvere per ottenere un buon livello di interoperabilità, che consenta un vero controllo congiunto dello strato IP e dello strato ottico in un ambiente multi-vendor. L'approccio previsto per l'introduzione della T-SDN prevede di partire dal backbone e di procedere con un'integrazione a fasi successive.

In una prima fase, il controllore SDN dello strato IP potrà disporre in sola lettura delle informazioni topologiche dello strato ottico, per ottimizzare gli instradamenti.

## Bibliografia

[1] A. Calvi, G. Ferraris, "Integrazione fra la rete IP e la rete di trasporto ottica", Notiziario tecnico Telecom Italia, Anno 25, numero 1, 2016.

[2] C. Cavazzoni, "L'interfaccia GMPS UNI", Notiziario tecnico Telecom Italia, Anno 25, numero 1, 2016.

# 8. RICONFIGURABILITÀ NELLE RETI ACCESS E METRO ACCESS

## 8.1 L'EVOLUZIONE DEL TRAFFICO NELLE RETI DI ACCESS

Con il termine "riconfigurabile" si intende la possibilità per una rete di adattarsi dinamicamente, anche in tempo reale, alle variazioni delle condizioni nelle quali la rete stessa si trova ad operare, rispondendo in modo efficace ed efficiente a mutevoli requisiti di capacità, sicurezza e di QoS/QoE) [1].

L'esigenza di rendere riconfigurabili le reti è avvertita prevalentemente a livello di reti *core* e reti di *data center*. In tali contesti si è affacciata negli ultimi anni la proposta di un nuovo paradigma, il SDN (*Software Defined Networking*), che in estrema sintesi realizza un disaccoppiamento tra il *Control Plane*, cioè il sistema che stabilisce il *routing* del traffico coordinato da un *controller* centralizzato, ed il *Data Plane*, ovvero il sistema sottostante che effettua il *forwarding* del traffico.

La necessità dell'utilizzo del concetto di riconfigurabilità al segmento di accesso è dovuta, fra l'altro, all'avanzamento di nuovi servizi *bandwidth hungry* raccolti dalle nuove reti d'accesso ottiche che comportano una crescita del traffico secondo la legge di Nielsen (aumento del 50% all'anno).

## 8.2 RICONFIGURABILITÀ A LIVELLO FISICO

La dinamicità richiesta comporta, dal punto di vista dei componenti e dei sistemi *hardware*, dei requisiti cruciali che sono la flessibilità e la programmabilità. In altre parole, sarà necessario sviluppare sistemi fotonici, i cui parametri chiave siano riconfigurabili via *software*: le reti riconfigurabili e *software defined SDN*, in definitiva, richiedono lo sviluppo di un nuovo approccio tecnologico, la *software defined photonics*. Le proposte presenti nella letteratura scientifica riconducibili, direttamente o indirettamente, a questa tematica, sono numerosissime e riconducono per gran parte all'impiego su larga scala della fotonica del silicio (*Silicon Photonics*) in circuiti integrati fotonici. Si potrebbero sintetizzare, a grandi linee, in quattro macro-aree non mutuamente esclusive:

1) *transceiver* flessibili;

2) griglie WDM flessibili;

3) tecniche di *routing* a livello fisico;

4) tecniche di *switching* a livello ottico.

Per *transceiver* flessibili si intendono essenzialmente trasmettitori e ricevitori riconfigurabili installati "a bordo" delle OLT e ONU/ONT. Come mostrato in figura 50, per esempio, si potrebbero modificare in *real-time* i seguenti parametri:

- il *bit-rate*,
- la potenza trasmessa,
- la tecnica e/o la cardinalità della modulazione,
- la tecnica di codifica,
- la lunghezza d'onda della portante ottica,
- il *payload* del FEC.

Per far ciò è necessario intervenire sulla sorgente laser, sull'elettronica di pilotaggio della sorgente o su un modulatore ottico esterno.

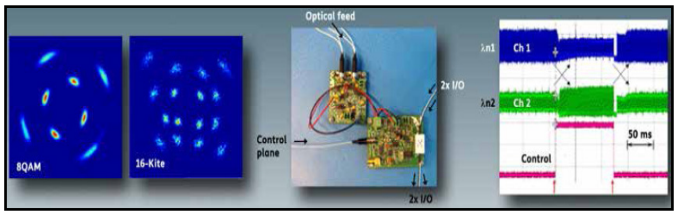



Figura 50 - Transceiver flessibili ed esempi di costellazioni 8-QAM e 16- QAM.

Le griglie WDM flessibili sono già da qualche anno una possibilità concreta per le reti *backbone*. Come si può notare in figura 51, se la spaziatura tra le portanti ottiche di un sistema di multiplazione a divisione di lunghezza d'onda non è strettamente vincolata ad una griglia prestabilita (per esempio quella DWDM), è evidente che la banda allocabile per ciascuna portante può essere gestita in modo dinamico ottimizzando l'efficienza spettrale. L'estensione della modulazione WDM alle reti PON [3] renderà opportuno utilizzare tecniche come questa per adeguare la capacità del link alle esigenze degli utenti.

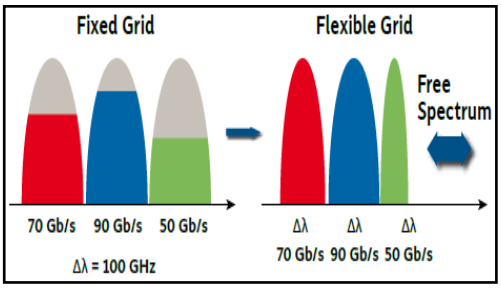



Figura 51 – Schematizzazione dei vantaggi nell'applicazione di griglie WDM flessibili

Il *routing* di lunghezze d'onda è un modo per instradare il traffico senza ricorrere a conversioni elettro-ottiche. Nelle reti *backbone* degli operatori sono già presenti da alcuni anni nodi ROADM in grado di operare tale funzione impiegando tecnologie MEMS o LCoS [4]. Il *routing* di lunghezza d'onda è solo una delle possibilità per instradare il traffico in una rete WDM riconfigurabile; dal punto di vista concettuale, si tratta di una "semplice" commutazione di circuito ottico, denominata OCS (*Optical Channel Switching*).

Tecniche di *switching* a livello ottico, sono tecniche più sofisticate, sintetizzate in figura 52 che permetterebbero di adattare la rete in modo più "granulare" ed efficiente alle variazioni del traffico.

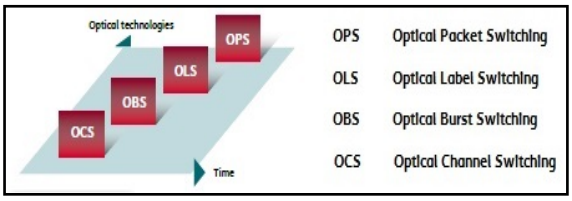



Figura 52 - Tecnologie di switching ottico ordinate in base alla complessità implementativa e alle fasi in cui se ne prevede l'impiego

L'approccio ideale sarebbe teoricamente la OPS (*Optical Packet Switching*), ovvero una commutazione di pacchetto eseguita interamente nel dominio ottico. L'implementazione a livello ottico della commutazione di pacchetto consentirebbe l'applicazione del concetto di IPoWDM, che semplificherebbe notevolmente la pila protocollare, riducendo i costi operativi della rete. Poiché le tecnologie attuali non consentono questa possibilità, un approccio pratico per implementare la OPS è rappresentato dalla OLS (*Optical Label Switching*) in cui solo l'*header* del pacchetto (l'etichetta, appunto) viene processato elettronicamente. Una soluzione meno sofisticata ma più facilmente implementabile è rappresentata dalla OBS (*Optical Burst Switching*) che non ha la pretesa di

instradare i singoli pacchetti ma gruppi di pacchetti (*burst*) processando un segnale *out-of-band* che contiene le informazioni per l'indirizzamento.

## 8.3 CONVERGENZA METRO-ACCESS

L'impiego dei ROADM e delle evolute tecniche di *switching* descritte finora consentirebbe di integrare in un'unica rete *all-optical* i segmenti *access* e *metro*: molte delle architetture proposte che realizzano tale convergenza consistono in un anello *metro* che raccoglie il traffico da un certo numero di alberi PON (Passive Optical Network) collegati all'anello mediante ROADM) [1].

L'utilizzo di architetture basate sulla WDM in rete di accesso, ritenuto un verosimile scenario a medio e lungo termine [3], estenderà il campo di applicazione delle PON rispetto agli attuali standard GPON (Gigabit-capable PON) [5]. La riduzione delle perdite di inserzione degli splitter (sostituiti dagli AWG) con conseguente incremento del *power budget* e quindi del *reach*, abiliterà infatti l'utilizzo delle tecnologie PON nelle reti *metro-access* unificate.

Tali reti dovranno supportare tre applicazioni principali:

- accesso ottico residenziale condiviso;
- accesso ottico dedicato per i clienti *business;*
- *backhauling* dei nodi della rete radiomobile (4G/5G).

Tali applicazioni potrebbero essere fornite da un'infrastruttura unificata ibrida WDM/TDM-PON [6].

Una possibile soluzione *cost-effective* potrebbe essere quella di utilizzare la WDM nel segmento metro e la TDM nel segmento di accesso. Ovviamente ci sarebbero sfide tecnologiche da affrontare: per ampliare il *reach* potrebbero essere necessari amplificatori ottici nei RN; andrebbe anche gestita la trasmissione *burst-mode* implicita della TDM.

L'architettura SARDANA, proposta nel 2011 da un consorzio internazionale di operatori, *vendor* e istituti di ricerca, è forse l'esempio più noto di convergenza *metro-access*. Tale architettura, raffigurata in figura 53, prevede un anello bidirezionale WDM a 32 lunghezze d'onda che si interfaccia con degli alberi TDM PON a 10 Gbps mediante RN (Remote Node) che effettuano l'*add/drop* dei canali. Si tratta di nodi ottici passivi, poiché tutta l'elettronica risiede in un unico nodo di controllo, ovvero un CO (Central Office) sede di OLT localizzato sull'anello WDM. Ciascun RN è equipaggiato con uno splitter, per la distribuzione sulla relativa PON, ed un EDFA con una pompa laser remota localizzata nel CO, per estendere il *reach*.

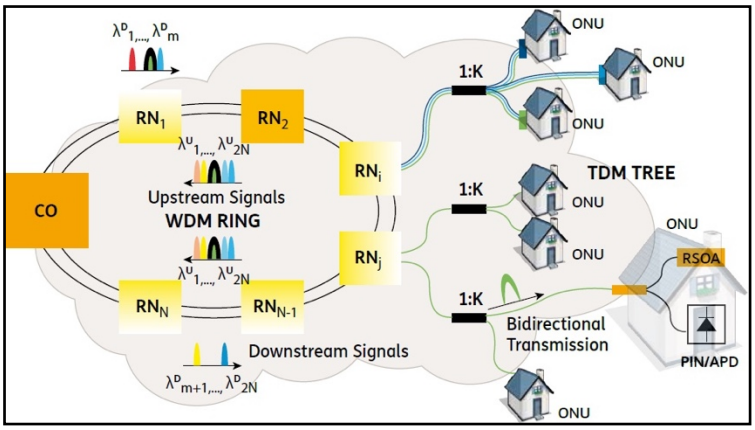



Figura 53 - Architettura di rete metro-access SARDANA.

Le ONT sono equipaggiate con transceiver colorless basati su RSOA (Reflective Semiconductor Optical Amplifier) che riflettono e rimodulano il segnale ottico ricevuto in downstream per generare il traffico *upstream*. La topologia ad anello è chiaramente strategica dal punto di vista della resilienza della rete, considerando che garantisce due vie di collegamento tra l'OLT e ciascuna ONT con un tempo di ripristino, in caso di eventuale guasto, inferiore a 50 ms [8].

Recentemente sono state proposte altre architetture *metro-access* riconfigurabili. Particolarmente interessante è quella presentata da Schrenk *et al*. basata su nodi ROADM passivi che effettuano uno *switching* ottico dinamico utilizzando meccanismi di "*energy scavenging*": tali dispositivi, infatti, non necessitano di alimentazione elettrica locale ma si auto-alimentano mediante segnali ottici a -10 dBm che potrebbero anche essere i segnali di traffico, piuttosto che un segnale di pompa [9].

In figura 54 la struttura del GPON Albero PON che vede l'ONT dell'utente con una singola fibra dedicata a partire dall'apparato OLT in sede CO.

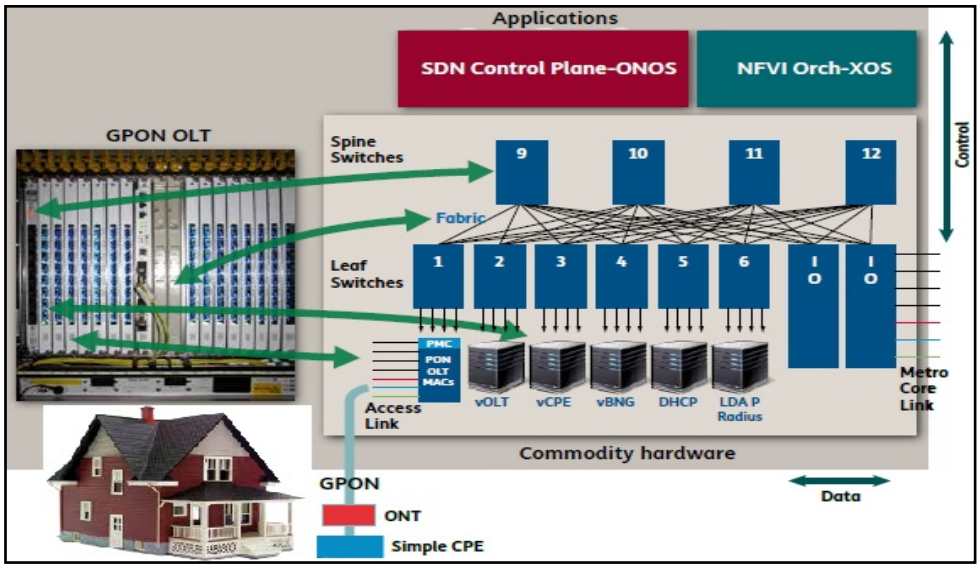



Figura 54 – GPON

Bibliografia

[1] T. Muciaccia, S. Pileri, "Riconfigurabilità nelle reti di accesso metro-access", Notiziario tecnico Telecom Italia, Anno 25, numero 1, agosto 2016.

[2] A. Amokrane, J. Hwang, J. Xiao, N. Anerousis, "*Software defined enterprise passive optical network*", 10th International Conference on Network and Service Management (CNSM), Rio de Janeiro, 2014..

[3] T. Muciaccia, S. Pileri, "*Reti WDM PON: principali sfide*", Notiziario Tecnico - Telecom Italia, N. 2, pp. 126-139, 2014.

[4] S. Augusto, V. Brizi, R. Tavilla, "*L'evoluzione della trasmissione ottica*", Notiziario Tecnico - Telecom Italia, N. 1, pp. 60-89, 2009.

[5] GPON (Gigabit-capable PON): specifiche contenute nelle Recommendation ITU-T, serie G.984. Bit rate massima di 1.25Gbps in upstream, 2.5Gbps in downstream.downstream.

[6] S. Pato, J. Pedro, J. Santos, H. Silva, J. Pires, P. Monteiro, "*All-Optical Remote Node for Cost-Effective Metro-Access Convergence*", Conf. on Telecommunications (ConfTele), S.ta Maria Feira, Portugal, 2009.

[7] S. Wong, W. Shaw, K. Balasubramanian, N. Cheng, L. Kazovsky, "*MARIN: Demonstration of a Flexible and Dynamic Metro-Access Integrated Architecture*", IEEE Global Telecommunications Conference (GLOBECOM '07), Washington (DC), 2007.

[8] J. Hoover, J. Van Horne, "*SARDANA Tackles The Bandwidth Challenge*", Broadband Communities, October 2011.

[9] B. Schrenk, F. Laudenbach, R. Lieger, T. Lorünser, P. Bakopoulos, A. Poppe, M. Stierle, H. Avramopoulos, H. Leopold, "*Passive ROADM Flexibility in Optical Access With Spectral and Spatial Reconfigurability*", IEEE Journal On Selected Areas In Communications, Vol. 33, No. 12, pp. 2837-2845, 2015.[24]

# 9. ARCHITETTURE DI RETE DI ACCESSO FISSO

L'evoluzione delle tecnologie di accesso [10] è caratterizzata da una progressiva introduzione della fibra ottica, con l'obiettivo di raggiungere nel lungo periodo gli utenti direttamente in fibra.

Questo obiettivo tuttavia verrà raggiunto gradualmente, valorizzando il più possibile l'attuale rete di distribuzione in rame, che costituisce ancora un patrimonio e un asset strategico per gli operatori del settore (per quanto riguarda il contesto italiano basti pensare ai 570 mila km di cavo, ai 102 milioni di coppie in rame o ai 152 mila armadi ripartilinea), grazie alla sua capillarità; al di là dell'aspetto economico, l'adozione di architetture che sfruttano la rete in rame esistente, costituisce un importante vantaggio in termini di mercato, consentendo di accelerare i tempi di sviluppo e dispiegamento della rete così da raggiungere nel più breve tempo possibile il maggior numero di potenziali clienti.

Il naturale percorso evolutivo che si è venuto a delineare pertanto vede un progressivo avvicinamento dell'infrastruttura in fibra al cliente finale associato all'adozione di tecnologie trasmissive in rame che, sfruttando le distanze via via più brevi da coprire, consentono di assecondare la richiesta di connettività a velocità sempre maggiori; tale percorso evolutivo si articola nei seguenti passi:

- FTTE (Fiber To The Exchange);
- FTTCab (Fiber To The Cabinet);
- FTTdP (Fiber To The distribution Point);
- FTTH (*Fiber To The Home*).

L'architettura FTTE è stata adottata nella seconda metà anni '90 primi anni di introduzione sul mercato di accessi a larga banda, ed associata alla tecnologia ADSL ha consentito a milioni di utenti iniziare a sperimentare le opportunità offerte dai servizi a larga banda; le lunghe tratte di rete in rame e lo stato della tecnologia (ADSL 20/1 Mbit/s Downstream/Upstream rispettivamente) tuttavia, non consentiva di raggiungere i target di prestazioni che il mercato andava chiedendo.

Negli anni successivi (a partire circa dal 2010) lo sviluppo della tecnologia VDSL ha consentito una prima importante evoluzione architetturale che prevede l'installazione dell'elettronica a livello di armadio ripartilinea; l'architettura FTTCab prevede infatti di raggiungere un'unità remota ONU (*Optical Network Unit*) con un collegamento in fibra ottica dedicato in grado di portare fino a 1 Gbit/s simmetrico. La tratta in rame da coprire in questo caso è solo quella della rete di

distribuzione secondaria a valle dell'armadio ripartilinea e le velocità raggiungibili crescono in modo significativo, consentendo di avvicinarsi ai target imposti dall'agenda digitale Europea.

In questo periodo di tempo le soluzioni di collegamento puramente in fibra (architetture FTTH) sono state marginali in termini di consistenza, ma molto rilevanti in termini di mercato, essendo queste rivolte a un'utenza particolarmente pregiata (es. collegamenti punto-punto dedicati per utenza business, applicazioni di Backhauling di stazioni radiobase della rete mobile, …), oppure per clientela residenziale in aree selezionate e circoscritte del territorio (collegamenti punto-multi-punto con tecnologia trasmissiva GPON). Inoltre nell'immediato futuro è previsto un forte allargamento del bacino di utenza a cui offrire connettività FTTH, adottando una topologia di distribuzione ottica punto-multipunto PON (*Passive Optical Network*) basata su diramatori ottici passivi a divisione di potenza (power splitter) associata alla tecnologia GPON e alle sue evoluzioni (XG-PON/XGSPON/NG-PON2: vedi paragrafo 9.2).

Questa ulteriore evoluzione architetturale potrà assecondare le richieste di connettività presenti e future, consentendo di andare anche oltre gli attuali obiettivi previsti dall'Agenda Digitale Europea, e costituirà anche un importante elemento di sinergia tra lo sviluppo della rete di accesso fissa e mobile, offrendo a quest'ultima gli strumenti trasmissivi ed infrastrutturali necessari per il backhauling/fronthauling di micro/nano celle diffuse capillarmente sul territorio.

Un'altra architettura che sta raccogliendo sempre maggiore interesse tra gli Operatori è quella FTTdP (*Fiber To The distribution Point*): questa è caratterizzata dall'adozione di un'unità attiva nelle immediate prossimità dell'utente (es. all'ultimo distributore della rete in rame, alla base dell'edificio o sul marciapiede o in un pozzetto subito al di fuori di un edificio). L'ultima tratta della rete in rame da coprire in questo caso sarà molto breve (50-150m) e potrà pertanto essere adottata un'innovativa tecnologia trasmissiva in rame in fase di sviluppo (G.fast) ottimizzata per queste brevi distanze. Un altro elemento caratterizzante l'architettura FTTdP è l'adozione dell'alimentazione dell'apparato direttamente da casa del cliente RPF(*Reverse Power Feeding*): in questo caso il singolo cliente eroga dalla propria abitazione l'energia necessaria ad alimentare l'interfaccia trasmissiva in rame a lui dedicata e contribuisce all'alimentazione delle parti comuni dell'apparato. L'interesse per questa architettura discende dal fatto che consente di superare i problemi legati ad eventuali difficoltà impiantistiche nel realizzare in fibra ottica l'ultimo tratto di rete (rete di edificio e/o rete in casa utente), e supera l'esigenza di predisporre un punto di fornitura di energia elettrica per strada o in aree comuni alla base dell'edificio.

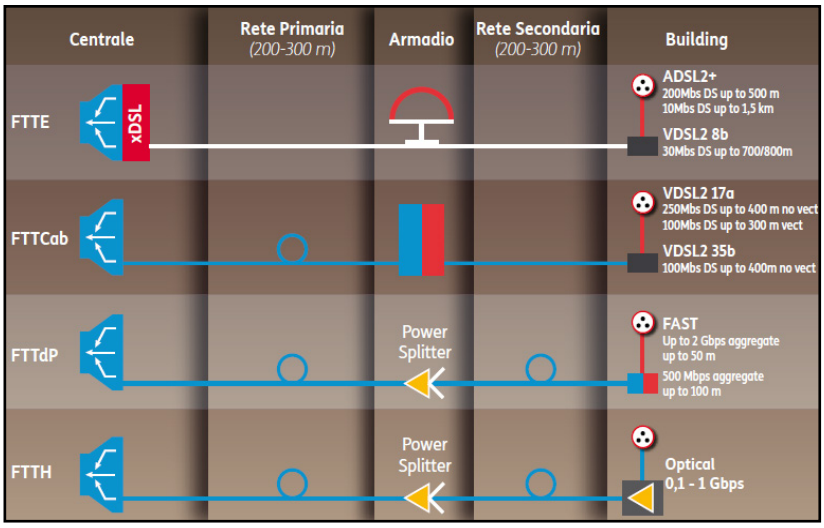


Figura 55 - Architetture di rete di accesso fisso

## 9.1 TECNOLOGIE IN RAME INNOVATIVE IN RETE DI ACCESSO

Le architetture descritte per la rete di accesso [11] tendono a sfruttare, quando possibile l'infrastruttura in rame esistente, che grazie alla sua capillarità e all'evoluzione delle tecnologie trasmissive permette di raggiungere velocità elevate su distanze medio corte, e concentrare gli investimenti per un deployment FTTH/FTTdp inizialmente nelle aree più strategiche. Naturalmente, maggiore è la velocità che si vuole offrire sulla tratta in rame e più esteso deve essere lo spettro utilizzato dal sistema trasmissivo. Purtroppo sia l'attenuazione sia la diafonia sono fenomeni che peggiorano al crescere della frequenza, perciò per poter sfruttare le frequenze elevate è necessario accorciare la lunghezza della tratta in rame [7].

La tecnologia VDSL2, come definita dallo standard ITU-T G.993.2, rappresenta l'evoluzione naturale dell'ADSL/2+, e ne incrementa la velocità di linea, utilizzando uno spettro molto più ampio, che si sfrutta bene su lunghezze di collegamento più corte, dell'ordine di alcune centinaia di metri. Questa tecnologia, che utilizza tecniche di frequency duplexing FDD (Frequency Division Duplexing) per separare le trasmissioni upstream da quelle downstream, prevede più profili, ottimizzati per l'utilizzo in scenari diversi:

- profili fino a 8MHz e 12 MHz per l'utilizzo da centrale, dove le linee sono mediamente più lunghe;
- profili fino a 17MHz e 35MHz (di recente definizione) per l'utilizzo da cabinet, dove le linee sono più corte.

Il profilo a 17MHz è già diffusamente utilizzato in campo per le offerte ultrabroadband FTTCab degli operatori italiani, e permette di offrire velocità downstream intorno ai 50-100M, a seconda della lunghezza del collegamento, mentre per il dispiegamento da centrale, tipicamente per le linee in rete rigida (linee che non transitano attraverso un armadio ripartilinea, ma sono collegate direttamente in centrale), si utilizza il profilo a 8MHz, con velocità intorno ai 30-50Mbit/s su linee mediamente più lunghe.

Nel corso del 2015 è stato approvato in ITU un nuovo profilo VDSL2, denominato Enhanced VDSL2 (AnnexQ dell'Amendment 1 alla Raccomandazione G.993.2 "Enhanced data rate 35 MHz VDSL2 vectoring compatible with profile 17a"), con spettro fino a 35MHz, nato dall'esigenza di sfruttare al massimo le potenzialità del rame e gli investimenti fatti dagli operatori al cabinet, e contemporaneamente di mantenere la compatibilità con i profili 17MHz in campo, anche in presenza di vectoring, grazie alla spaziatura delle portanti a 4kHz. Con questo nuovo profilo si stima che in rete italiana siano possibili velocità ben superiori a 100Mbit/s per distanze inferiori ai 150-200m, e che si possa incrementare significativamente la percentuale di clienti a cui si potrà offrire 100Mbit/s, anche in assenza di vectoring.

Poiché come si è detto al crescere della frequenza il disturbo di diafonia aumenta, e diventa su distanze medio brevi il fattore principale del degrado delle prestazioni, negli ultimi anni è stata standardizzata la tecnologia del Vectoring (ITU-T G.993.5), una soluzione che, grazie al coordinamento dei segnali trasmessi nello stesso ambiente cavo e alla preventiva valutazione delle caratteristiche di diafonia del cavo, permette di pre-compensare i segnali trasmessi in downstream, sottraendo in anticipo il contributo di rumore di telediafonia (FEXT) che questi riceveranno durante la trasmissione nel cavo. Una elaborazione in post processing viene applicata invece ai segnali ricevuti in direzione upstream, in modo da concentrare la complessità elaborativa del vectoring sull'apparato di rete (ONU). Questa soluzione permette di cancellare il rumore FEXT prodotto dai sistemi omologhi presenti nel cavo, e di ottenere dunque prestazioni più elevate ed indipendenti dal riempimento del cavo. Il vectoring può essere applicato alla tecnologia VDSL, ma anche alle evoluzioni successive delle tecnologie trasmissive su rame, come il FAST.

La tecnologia FAST rappresenta un ulteriore salto tecnologico, ed è stata specificata per lavorare in maniera ottimale fino a circa 100m (su doppino da 0.5mm di diametro) e raggiungere target prestazionali compresi tra i 500Mbit/s e il 1Gbit/s aggregati (download + upload). Standardizzato nel corso del 2014 (Raccomandazioni ITU-T G.9700 e G.9701), il FAST a differenza delle tecnologie DSL (FDD), è un sistema a divisione di tempo (TDD - Time Division Duplexing). Questa scelta ha permesso di semplificare il design e la complessità del transceiver e di contenerne i

consumi. Inoltre attraverso l'uso del TDD, gli operatori possono ottenere una ripartizione tra banda downstream e upstream più flessibile, in modo da poter definire un portafoglio servizi broadband più ampio. A livello spettrale, il FAST può utilizzare frequenze comprese tra 2MHz e 106MHz, ma sono già previste, in future evoluzioni dello standard, ulteriori estensioni che permetteranno l'utilizzo di frequenze fino a 212MHz. Per garantire la coesistenza nello stesso ambiente cavo con sistemi DSL legacy (figura 56), quali il VDSL2 dispiegato da cabinet, la frequenza da cui il FAST è abilitato a trasmettere può essere opportunamente configurata e sono stati introdotti opportuni meccanismi in grado di limitare i disturbi arrecati dal FAST nello spettro di frequenze utilizzate per le trasmissioni radio in FM. Nel corso del 2015 si sono resi disponibili i primi prototipi di DPU(Distribution Point Unit) e CPE (Customer Premises Equipment) in tecnologia FAST, che hanno dimostrato velocità aggregate superiori a 800Mbit/s su collegamenti di 50m (distanze tipiche per il dispiegamento in FTTdp). Il numero di porte dei primi apparati disponibili è fino a 16, poiché i requisiti espressi dalla maggior parte degli operatori, prevedono applicazioni dalla base degli edifici, in architettura FTTdp (Fiber To The Distribution Point), con modularità di 8/16 porte. Date le altre frequenze di lavoro, il FAST è particolarmente sensibile al crosstalk di linee omologhe sviluppate dallo stesso sito: in presenza di rumore le prestazioni del FAST possono risultare particolarmente basse, simili a quelle che si otterrebbero con un sistema VDSL2. A tale scopo quindi è stato reso obbligatorio dallo standard l'utilizzo di tecniche di vectoring in grado di cancellare il rumore di FEXT presente sulle linee.

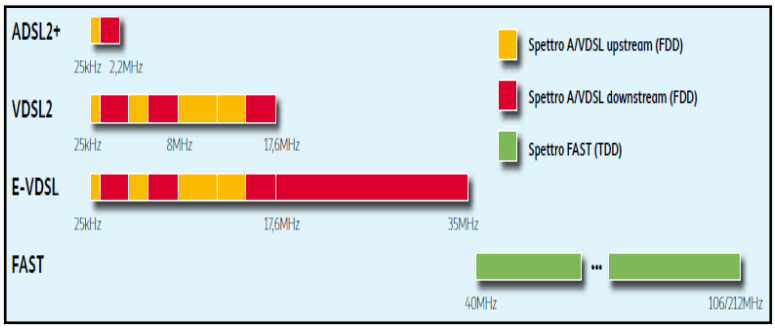


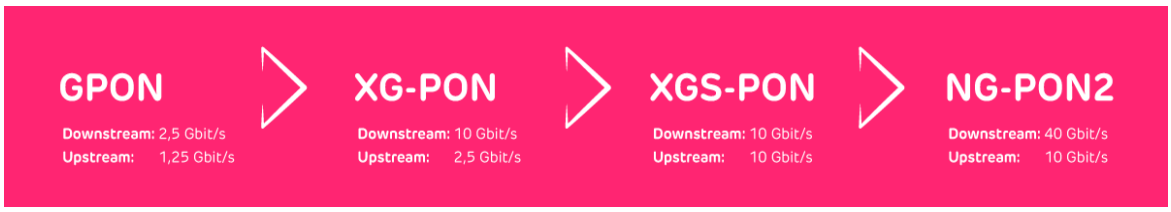

Figura 56 - occupazione spettrale delle tecnologie DSL per la compatibilità nello stesso ambiente cavo

## 9.2 TECNOLOGIE OTTICHE INNOVATIVE IN RETE DI ACCESSO

E' universalmente riconosciuto che le tecnologie ottiche innovative in rete di accesso [12] si basano su un'infrastruttura ottica passiva punto-multipunto (PON – Passive Optical Network) operanti su rete di distribuzione ottica con topologia ad albero, basata su diramatori ottici passivi (power splitter): questo indirizzo discende dall'opportunità di condividere la stessa infrastruttura ottica e l'interfaccia ottica di centrale tra più utenti, con ovvie ricadute in termini di contenimento del costo per cliente, inoltre si rende possibile una flessibile allocazione delle risorse trasmissive (ad esempio in termini di banda per cliente) tra utenti con requisiti differenti.

La standardizzazione dei sistemi PON è in corso da numerosi anni (a partire dagli anni '90) in ambito ITU-T ed ha visto susseguirsi la definizione di diverse generazioni via via più performanti di sistemi PON; una prima generazione dei sistemi GPON consente di disporre di 2,5/1,25 Gbit/s rispettivamente downstream/upstream da condividersi tra gli utenti attestati allo stesso albero ottico. Successivamente (2010) è stata definita in ambito ITU-T una seconda generazione denominata XG-PON che ha consentito di ottenere un forte incremento di capacità trasmissiva rispetto alla precedente generazione dei sistemi GPON (10/2,5 Gbit/s rispettivamente DS/US): tali sistemi XG-PON, sono disponibili già da qualche anno sebbene non molto diffusi. La ragione della scarsa diffusione di questi ultimi sistemi probabilmente è da ricercare da un lato nella attuale mancanza di richiesta di servizi di massa con requisiti di banda particolarmente spinti e da un maggior costo di questi sistemi rispetto ai molto più diffusi sistemi GPON tradizionali.

Rete di accesso FTTH e tecnologia GPON.




| | |
|---|---|
| GPON | (2,5G/1,25G) |
| XG-PON | (10G/2,5G) |
| XGS-PON | (10G/10G) |
| NG-PON2 | (40G/10G) , (80G /20G) e anche (80G /80G) |

Tra parentesi è indicata la velocità massima in Downstream e Upstream.

Negli ultimi anni (a partire dal 2012) si è avviata la definizione in ambito ITU-T di una successiva generazione di sistemi denominata NG-PON2 che prevede due possibili opzioni, denominate TWDM PON e PtP WDM PON: la prima specifica un sistema in cui ciascun canale ottico è condiviso tra più utenti, la seconda un sistema in cui ciascun canale ottico è dedicato al singolo utente (punto-punto logico su rete punto-multipunto).

In linea di principio il sistema TWDM PON consiste nella sovrapposizione di più sistemi (fino a 8) XG-PON operanti a lunghezze d'onda differenti, realizzando quindi un sistema di trasmissione ottica multi-canale in grado di offrire sul singolo albero ottico fino a 8 volte la capacità trasmissiva di un singolo sistema XG-PON (80/20 Gbit/s rispettivamente DS/US e opzionalmente anche 80/80 Gbit/s). Ulteriori dettagli sul funzionamento dei sistemi NG-PON 2 possono essere consultati in [6].

Un'importante caratteristica, voluta da tutti gli Operatori, che accomuna tutte le generazioni di sistemi PON è quella di poter coesistere tra loro sulla stessa infrastruttura in fibra ottica, grazie all'utilizzo di una differente allocazione di lunghezze d'onda; questo consente all'Operatore di introdurre gradualmente in rete i sistemi di nuova generazione, anche ove sia già stata adottata la consolidata tecnologia GPON, per offrire il servizio a maggior capacità solo dove necessario, senza arrecare disservizio ad altri utenti che condividono la stessa infrastruttura in fibra. In figura 57 è riportata l'allocazione spettrale delle varie generazioni di sistemi PON, dalla quale si può vedere come l'utilizzo di porzioni disgiunte di spettro consente la coesistenza sullo stesso albero PON di sistemi di differente generazione.

E' attualmente in fase di approvazione in ITU-T lo standard di un'ulteriore tipologia di sistema PON che si colloca tecnologicamente a metà strada tra i sistemi XG-PON ed i sistemi NG-PON2: tale sistema, denominato XGS-PON, consiste in una versione "simmetrica" del sistema XG-PON (capacità trasmissiva 10/10 Gbit/s rispettivamente DS/US); l'interesse verso questo sistema discende dal fatto che essendo tecnologicamente più semplice dei sistemi NG-PON2 (non essendo multicanale) si stima possa raggiungere rapidamente la maturità ed essere commercialmente disponibile in tempi brevi.

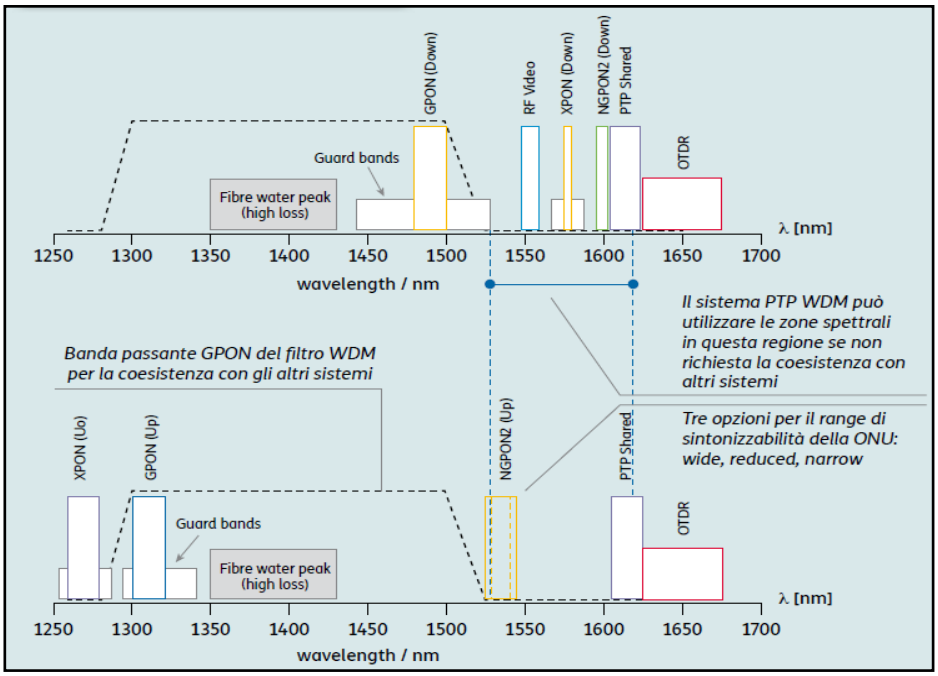



Figura 57 - Allocazione spettrale dei sistemi PON

Bibliografia

[1] Tecnologia VDSL2 e Enhanced VDSL2: "*Very high speed digital subscriber line transceivers 2 (VDSL2)*", Raccomandazione ITU-T G.993.2, Gennaio 2015 e Amendment 1, Novembre 2015.

[2] Vectoring: "*Self-FEXT cancellation (vectoring) for use with VDSL2 transceivers*", Raccomandazione ITU-T

G.993.5, Aprile 2010.

[3] Sistemi GPON: serie di Raccomandazioni ITU-T G.984.1 – G.984.7, G.988

[4] Sistemi XG-PON: serie di Raccomandazioni ITU-T G.987, G.987.1 – G.987.4, G.988

[5] Sistemi NG-PON2: serie di Raccomandazioni ITU-T G.989, G.989.1-G.989.3

[6] "*Le reti ottiche e la loro evoluzione negli standard*", G. Ferraris, L. Pesando, M. Valvo - Notiziario Tecnico TI 2/2015

[7] "*Evoluzione tecnologica per la rete NGAN*", P. Cinato, F. Marigliano, M. Valvo – Notiziario Tecnico TI 2/2012

[8] Tecnologia FAST: serie di Raccomandazioni ITU-T G9700-9701

[9] Sistemi XGS-PON: Raccomandazione ITU-T G.9807.1

[10] M. Caretti, P. Cinato, U. Ferrero, R. Mercinelli, "Evoluzione dell'accesso", Notiziario tecnico Telecom Italia, Anno 25, numero 1, agosto 2016.

[11] Umberto Eula, "Evoluzione dell'accesso: Tecnologie in rame innovative in rete di accesso", Notiziario tecnico Telecom Italia, Anno 25, numero 1, agosto 2016.

[12] Maurizio Valvo, "Evoluzione dell'accesso: Tecnologie ottiche innovative in rete di accesso", Notiziario tecnico Telecom Italia, Anno 25, numero 1, agosto 2016.

# 10. LE RETI AZIENDALE E LE NUOVE TECNOLOGIE.

## 10.1 SOLUZIONI PER COLLEGARE LE SEDI DISTRIBUITE NEL TERRITORIO

Possiamo avere il caso un'organizzazione ad alta distribuzione geografica caratterizzata da poli remoti a banda medio bassa ma anche la situazione in cui c'è la necessità di connettere divisioni aziendali di grandi dimensioni con filiali situate in una regione geografica. Un'azienda distribuita su varie sedi richiede un ambiente di business basato sulla condivisione sicura delle informazioni che ottimizzi le comunicazioni con i clienti, i partner ed i fornitori autorizzati ad accedere le basi dati.

L'orientamento alla condivisione richiede una tecnologia di networking sicura, scalabile e flessibile. Occorre interconnettere più sedi aziendali creando reti private su scala geografica, ma a costi accessibili. Per creare una rete sicura, ovvero al riparo per quanto possibile da possibili intercettazioni, per un'azienda distribuita che prevede filiali e sede principale, è possibile fare uso di:

- canali Diretti Numerici (CDN)
- canali cifrati all'interno della rete Internet (VPN = Virtual Private Network)
- una rete MPLS

Tali soluzioni sono rappresentate nei paragrafi che seguono.

### 10.1.1 CANALI DIRETTI NUMERICI CDN

Si tratta del noleggio di alcune linee telefoniche dedicate per collegare le diverse filiali alla sede centrale dell'azienda. Una CDN collega due reti fisicamente, non virtualmente, senza utilizzare la rete Internet (come invece fanno le VPN). La soluzione CDN è molto costosa con costi di noleggio delle linee elevati già per una singola linea da 2Mbit/s che crescono con la distanza, per questi motivi è ora assai poco utilizzata.

Caratteristiche:

- si tratta di linee ad uso esclusivo dell'azienda e quindi non ci sono possibilità per estranei di intercettare i dati trasmessi; pertanto non serve crittografare i dati trasmessi;
- i costi di noleggio delle linee possono essere piuttosto elevati;

- tutta la banda di trasmissione delle linee è ad uso esclusivo dell'azienda. Tipicamente si considerano collegamenti costituiti da una o più linee a 2 Mbit/s;
- si possono usare indirizzi IP privati in quanto non ci sono collegamenti con Internet;
- se voglio anche la connessione ad Internet, si può mettere un ulteriore Router nella sede centrale per il collegamento al provider. Dalle altre sedi si può andare in Internet passando per la sede centrale.

### 10.1.2 CANALI CIFRATI ALL'INTERNO DELLA INTERNET (VPN IPSec )

Il collegamento avviene tramite la rete Internet, che però è accessibile da tutti e pertanto è opportuno, anzi necessario, crittografare i dati trasmessi per ottenere una "privatezza virtuale". A tal fine si utilizza il protocollo IPSec del livello 3 OSI. Ogni sede dell'azienda si collega ad un Internet Service Provider e pertanto ha bisogno di avere un indirizzo IP pubblico da assegnare all'interfaccia verso l'esterno del proprio Router. I costi sono molto bassi e dipendono dalla velocità della linea che si utilizza. Per le filiali si faceva uso di linee ADSL che sono asimmetriche e caratterizzate fino a qualche anno fa da velocità di 20 Mbit/s (download) e 1 Mbit/s (upload) ma che ora raggiungono, con le tecniche VDSL2 e Vectoring velocità superiori ai 100 Mbit/s (download). Si utilizzano anche le tecniche in fibra GPON descritte al paragrafo 9.2. Per la sede centrale dove c'è il server dati i collegamenti erano caratterizzati fino a qualche anno fa da modem simmetrici HDSL a 8 Mbit/s download e upload ora sono accessibili anche i collegamenti GPON simmetrici sempre visti al al paragrafo 9.2. In figura 58 si riporta un esempio di connessione multisede che fa uso di VPN IPSec.

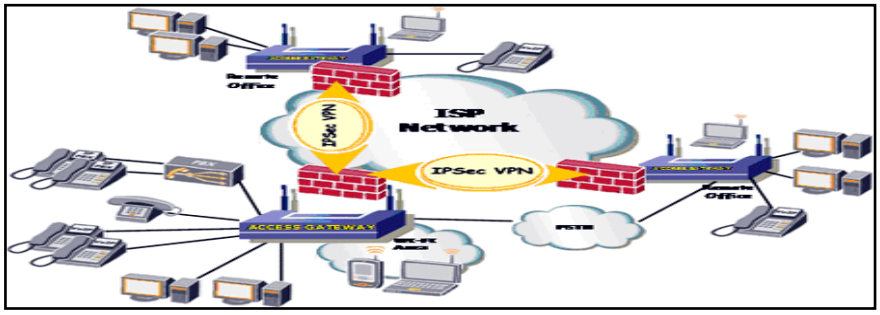



Figura 58 – Connessioni in Internet con uso di VPN IPSec e CPE di tipo Access.

### 10.1.3 RETE MPLS (MULTI PROTOCOL LABEL SWITCHING)

Per la connessione di centrostella e sedi periferiche principali si utilizza la rete dati messa a disposizione dalle Telco: la rete IP MPLS con la quale si attivano le VPN MPLS. Con il suo utilizzo risulta possibile differenziare i servizi **e** il loro trattamento qualitativo all'interno della rete, ovvero applicare politiche di QoS (Quality of Service) ad esempio per dare maggiore priorità al traffico VOIP (Voice over IP) e al traffico di Streaming Video e minore priorità al traffico dati, web e alla posta elettronica. Si migliora nel complesso la qualità del servizio di trasmissione dati percepita dall'utente finale. La rete IP dati MPLS presenta requisiti impliciti di sicurezza con canali "virtualmente privati" VPN MPLS senza necessità di crittografare. La rete IP MPLS offre servizi, con costi accettabili rispetto le altre soluzioni. L'attestazione della sede dell'impresa alla rete dati Telco avviene con utilizzo di una fibra dedicata che connette il NTE della sede utente direttamente con una porta dell'apparato della rete di aggregazione (in TIM l'apparato Remote Feeder della rete OPM). L'NTE della sede utente può utilizzare indirizzi IP privati. Per la connettività a Internet si fruisce dell'accesso a Internet della sede principale connessa con un apposito indirizzo IP pubblico e solo su questa occorrerà impostare le policy sul firewall.

Un accesso a un Data Center permetterà di fruire servizi di Backup as a Service o meglio di Disaster Recovery.

## 10.2 CONSIDERAZIONI CHE PORTANO A PREFERIRE LA SOLUZIONE IP MPLS.

Tra le soluzioni esposte la soluzione CDN risulta quella obsoleta, insufficiente in termini di banda vista la crescente richiesta per i nuovi servizi e fuori mercato per i costi elevati e quindi destinata solamente a usi particolari.

La soluzione che prevede l'attivazione di VPN IPSec rende il networking WAN più accessibile. Si sfruttano le risorse condivise di un ISP che attiva un tunnel cifrato che attraversa internet per ottenere una "privatezza virtuale". La VPN IPSec ha un costo decisamente inferiore rispetto ad una linea dedicata CDN e viene utilizzata per la connessione di piccole sedi piccole e per lo "smart working".

La vera soluzione per creare una intranet aziendale, è quella basata sulle reti dati IP MPLS. Le Telco offrono reti dati supportate da moderne tecnologie che permettono connessioni a banda larga

e trasformano le reti geografiche in reti private con logiche funzionali, sicurezza e prestazioni simili alle reti locali. Gli utenti di rete, hanno accesso ai servizi di rete remoti come se fossero logicamente erogati da server locali.

Il servizio VPN MPLS è quindi la soluzione principe per la realizzazione di reti geografiche private.

## 10.3 IP MPLS: OFFERTE COMMERCIALI PROPOSTE DALLE TELCO

Le TELCO sviluppano le reti dati e su queste dispongono servizi di rete con uso di features quali: SDN una nuova modalità di creare e gestire le reti geografiche private in tempi rapidi (time to market); pseudowire utilizzati per creare connessioni tipo punto-punto nella rete di accesso e aggregazione tra nodi di accesso e nodi PE. In questo contesto le TELCO riescono a fornire offerte commerciali affinché le imprese possano realizzare le reti geografiche private.

In una rete geografica aziendale IP-MPLS:

- la sede centrale dovrà avere un accesso (link) MPLS per essere connessa con tutte le sedi secondarie.
- ogni sede periferica avrà un accesso MPLS che utilizzerà per connettersi con la rete aziendale.
- ogni sede, sia centrale che periferica, avrà un accesso MPLS attestato alla rete metro regionale di accesso e aggregazione (in TIM rete OPM) sull'apparato di aggregazione di competenza territoriale (in TIM Remote Feeder). In fig. 59 è riportato un esempio di attestazione al RF di apparati NTE Intranet Enterprise.
- la sede principale (o "*centro stella*") viene dotata di un accesso ad internet (*opportunamente dimensionato)*, *che sarà a disposizione dell'intera azienda e di tutte le sedi* secondarie (accesso ad internet centralizzato).
- tutte le sedi dovranno essere fornite dallo stesso provider, ovvero non è possibile usare reti MPLS di fornitori diversi.

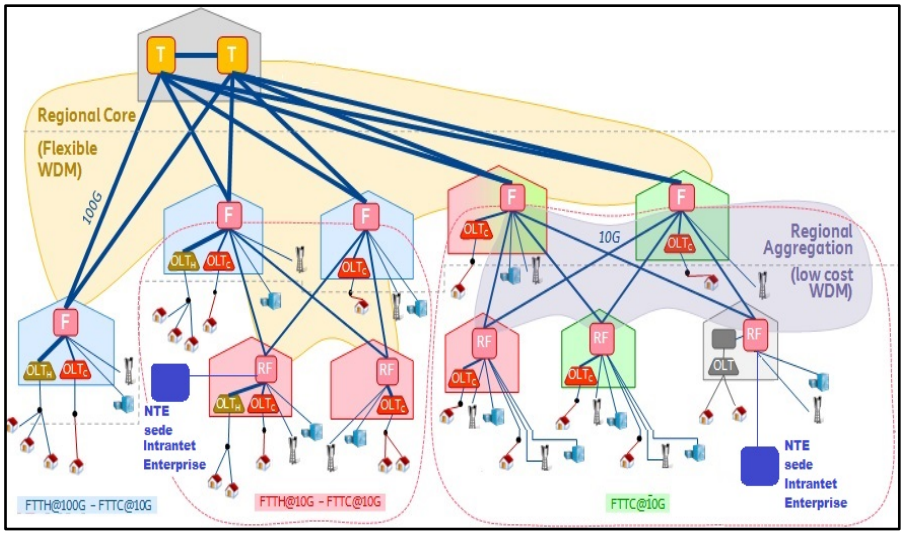



Figura 59 – Accesso alla rete metro regionale OPM di apparati NTE Intranet Enterprise

Possiamo distinguere due modalità di realizzazione della intranet:

- la prima fornisce una connettività livello 2 trasparente fra sedi cliente attestate alla stessa MAN.

- la seconda fornisce una connettività metropolitana terminata a livello 3 sulle singole NTE fra sedi cliente attestate alla stessa MAN.
  - Le CPE del Cliente appartengono a sottoreti differenti in ciascuna sede di appartenenza, consentendo di mantenere la compatibilità con piani d'indirizzamento IP preesistenti.
  - Indirizzamento di livello 3 IP privato nelle sottoreti del Cliente.
  - La soluzione è basata su routing IP dinamico realizzato nelle NTE per consentire la connettività fra le CPE appartenenti alle differenti sottoreti del Cliente.

Ci sono inoltre offerte specifiche per attivare la connettività verso internet a partire dal centrostella.

Proponiamo di seguito esempi di offerte commerciali Telco per la realizzazione della rete IP MPLS aziendale.

### 10.3.1 PROPOSTE COMMERCIALI PER SERVIZIO MPLS OFFERTE DA TIM

Piattaforma Ethernity:

La piattaforma Ethernity consente l'accesso alla Rete MPLS di TIM per la realizzazione di reti geografiche e la connessione ad Internet ad alta velocità.

Il servizio Ethernity offre alle aziende una infrastruttura di eccellenza per le applicazioni come: Interconnessione LAN e WAN, Disaster Recovery e Business Continuity, Sincronizzazione di DB e collegamenti Server ad alta velocità. Il servizio Fibra Ethernity supporta lo standard MEF (Managed Extensibility Framework), e offre performances garantite con parametri definiti e predicibili come: Packet Loss: < 10 -4, Max Latenza Media: 30 ms, Jitter Max: 40 ms.

Il servizio Fibra Ethernity comprende diverse architetture di connessione con profilo:

- Giga Hyperway per realizzare la rete geografica IP-MPLS, offre una soluzione di interconessione fra le sedi (Banda MPLS). In funzione del tipo di profilo Ethernity contrattualizzato dal cliente, la banda MPLS è disponibile in modalità standard a 10/100 Mbps e si arricchisce con i nuovi tagli di 200, 300, 500, 600 Mbps e 1Gbps;
- GigaBusiness offre una soluzione di accesso ad Internet in fibra ottica su interfacce GBE a partire da 10M e con possibilità di configurare la banda di accesso ad Internet a partire da 2M e si arricchisce con i nuovi tagli di 200, 300, 500, 600 Mbps e 1Gbps. L'infrastruttura in fibra di accesso alla rete IP è realizzata mediante il servizio ETHernity, attraverso uno qualsiasi dei profili di connettività disponibili: Silver o Gold.

### 10.3.2 PROPOSTE COMMERCIALI PER SERVIZIO MPLS DA FASTWEB

FASTCompany è l'Offerta di VPN MPLS per connettere diverse sedi Aziendali compreso il centrostella a banda larga sicura che presenta le seguenti caratteristiche:

- Scalabilità e flessibilità delle offerte;
- Affidabilità e Prestazioni elevate;
- Quality of Service (QOS);
- Sicurezza: la comunicazione fra le sedi collegate tramite VPN è protetta e la rete non è attaccabile con tecniche intrusive.

Fast Company Mobile è il servizio per accedere in mobilità alla rete VPN Aziendale o ad Internet, senza alcuna necessità di passare da Internet e di dotarsi della infrastruttura richiesta per l'accesso da remoto. Il servizio è integrato con la rete VPN MPLS fissa (FastCompany).

Fast Company Mobile presenta le seguenti caratteristiche:

- Flessibilità d'offerta;
- Affidabilità e alte performance;
- Gestione semplificata: non è necessario predisporre e manutenere apparati hardware e software;
- Sicurezza delle soluzioni Mobile VPN l'utente non è raggiungibile da reti pubbliche ed il traffico non transita mai da reti non sicure.

FLEX COMPANY. La soluzione SDWAN, basata sul paradigma delle SDNs (Software Defined Network), consiste in una nuova modalità di creare e gestire le reti geografiche private. Prevede l'accesso ad un'infrastruttura dedicata alla Clientela business e completamente integrata nella rete di trasporto di Fastweb, garantendo SLA e prestazioni ottimizzate per il traffico e le applicazioni Mission Critical del Cliente.

La soluzione SDWAN presenta le seguenti caratteristiche:

- Gestione e controllo semplificato del traffico.
- Flessibilità: l'integrazione nativa con la rete MPLS permette di scegliere su quali sedi attivare il servizio.
- Sicurezza: possibilità di segregare il traffico e di applicare l'encryption.