Le misure di rete (o oggettive) sono state effettuate mediante il software ETHEREAL che permetteva di misurare parametri come throughput, jitter e data lost. Per la misurare invece la QoS in termini percettivi (o soggettivi), ci si è basati sul giudizio fornito da un gruppo di valutatori inseriti in una camera silente a cui erano mostrati degli streaming audio-video. Per maggiori informazioni si può andare al sito www.iscom.gov.it. I valutatori erano in possesso di un dispositivo con un cursore che azionavano durante la visione di un filmato, dispositivo che permette di esprimere il compiacimento del valutatore fornendo una curva che poteva variare da 0 (pessima immagine) a 100 (ottima immagine). E' evidente che nel caso di un filmato percepito con una ottima qualità la curva emessa dal dispositivo è una linea che nel tempo rimane fissa ad un valore prossimo a quello massimo (100 nel nostro caso). Particolare rilevanza è stata data alla correlazione tra misure oggettive e soggettive.

I primi test avevano riguardato l'utilizzo della tecnica DiffServ over MPLS per garantire la QoS nel caso di rete che veniva saturata con un generatore di traffico. I risultati mostravano l'importanza di una etichettatura di tipo Expedited Forwarding come già mostrato nel sito www.iscom.gov.it.

I risultati presentati in questo contributo si riferiscono alle degradazioni che sono subite da filmati in alta definizione quando la rete presenta 2 tipi di degradazione: a) l'interruzione di un collegamento (link failure), e b) la saturazione della banda nella connessione di accesso. Come riferimento è stato preso in considerazione l'unico documento che ad oggi definisce degli standard minimi di QoE (Qualità of Experience), il WT-126 del DSL Forum.

I flussi video utilizzati nei test di ***durata pari a 28 secondi*** erano tutti codificati in MPEG2 sia Video che Audio:

- MPEG2 720x576p 16/9, 9,29 Mbit/s di media, 29.97 fps, 30 MB per 24500 pks IP
- MPEG2 1280x720p 16/9, 18,94 Mbit/s di media, 60 fps, 65 MB per 45000 pks IP
- MPEG2 1920x1080i 16/9, 20 Mbit/s di media, 29.97 fps, 80MB per 62000 pks IP
- Audio: In tutti i casi si è utilizzato l'MP2 192 Kbit/s e 48 kHz.

Vediamo i risultati delle indagini:

a) Link failure. Per i *test sulla rete* nel caso di link failure si è inviato un flusso dati da un un punto ad un altro della rete e successivamente si è manualmente disattivato un link costringendo i routers interessati ad un ricalcalo del percorso. Mediante un software, Ethereal, si è potuto catturare lato destinazione tutti i pacchetti IP entranti ed in base al loro tempo di interarrivo si è potuto valutare il tempo impiegato dalla rete per il ripristino del collegamento. Lo stesso test è stato condotto prima con il ripristino in OSPF e successivamente in MPLS; i routers interessati sono stati i Juniper M10. Nel caso OSPF il tempo medio sulle quindici prove ripetute si è assestato sui 170 ms di gap,

l'MPLS mediante i meccanismi di *link protection* e *standby secondary path* (MPLS LP+SSP) ha registrato tempi medi di 50 ms. La tecnica OSPF è risultata subito inadeguata a causa del lungo tempo di ripristino richiesto e quindi l'analisi della QoS è stata basata solo sulla tecnica MPLS LP+SSP.

Sono stati analizzati tutti e tre i flussi, 576p, 720p e 1080i: il numero di pacchetti persi in 50 ms è crescente con la risoluzione ma la percentuale sul totale dei pacchetti costituenti il flusso rimane identica per i tre filmati comportando un livellamento degli effetti nei tre casi considerati. Il danno rimane comunque contenuto intaccando si il filmato ma preservando l'intellegibilità dei contenuti.

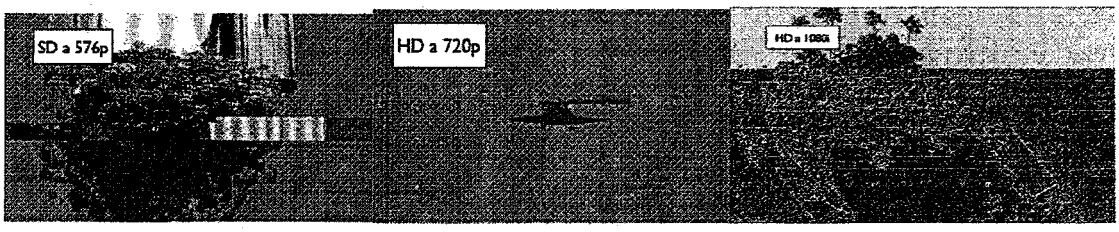


Fig. 6: Immagini da filmati video (SD, HD 720p e HD 1080i da sinistra a destra) durante un processo di ripristino MPLS LP+SSP. La degradazione avveniva per un tempo brevissimo (meno di 1 secondo).

b) *Saturazione della banda nel collegamento di accesso*. In questa analisi si sono ricreate le condizioni di saturazione del collegamento verso l'utente finale. Si è avviato il download di dati da un web server durante la ricezione di uno streaming video in alta definizione di 18 Mbit/s di bitrate medio. Per quel che riguarda la connessione in ADSL2+ si è settato il collegamento alla massima banda disponibile di 24 Mbit/s. I flussi ricevuti erano quindi di due tipi, UDP nel caso video e TCP per i dati.

Non appena si è dato il via al download di dati in TCP il flusso video ha subito una perdita di pacchetti continuata nel tempo rendendo la fruizione del filmato impossibile.

Si è cercata quindi una possibile soluzione che permettesse di continuare a vedere il filmato durante il download di dati: la più semplice soluzione che è stato possibile implementare è stata quella di etichettare i traffico video UDP come Expedited Forwarding applicando quindi una forma di QoS basata su DiffServ. Per fare ciò si è costruita una policy ad hoc sul router Cisco al quale era direttamente connesso il PC che funzionava da video server. Tramite il software Ethereal si è potuto verificare il funzionamento della soluzione trovata e i risultati sono riportati in fig. 7.

Come si può verificare all'applicazione della policy il traffico dati si stabilizza ad un bitrate medio più basso. Questo streaming è stato mostrato ai valutatori che lo hanno valutato con il dispositivo per la misura della qualità percepita. I valori mediati sui 20 utenti sono stati riportati nel grafico di figura 4, ciascuno in corrispondenza del throughput misurato in fig. 3.

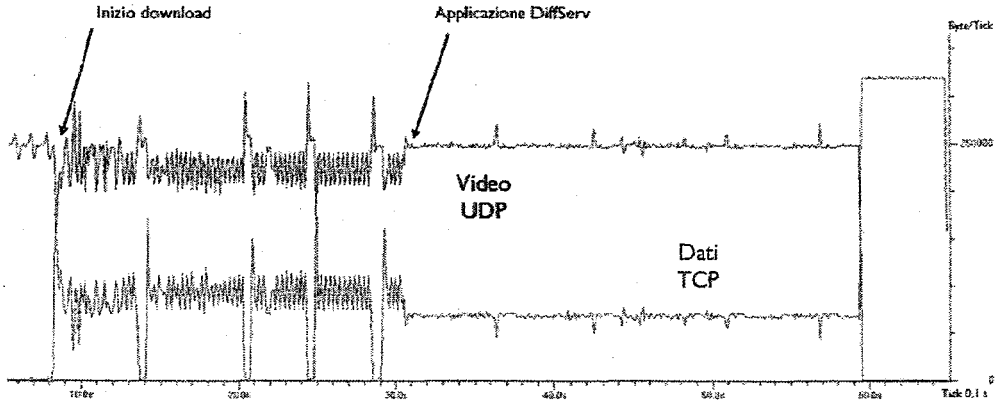


Figura 7 – Ethereal: Grafico dei pacchetti ricevuti con (secondo intervallo) e senza (prima intervallo) etichettatura dei pacchetti DiffServ

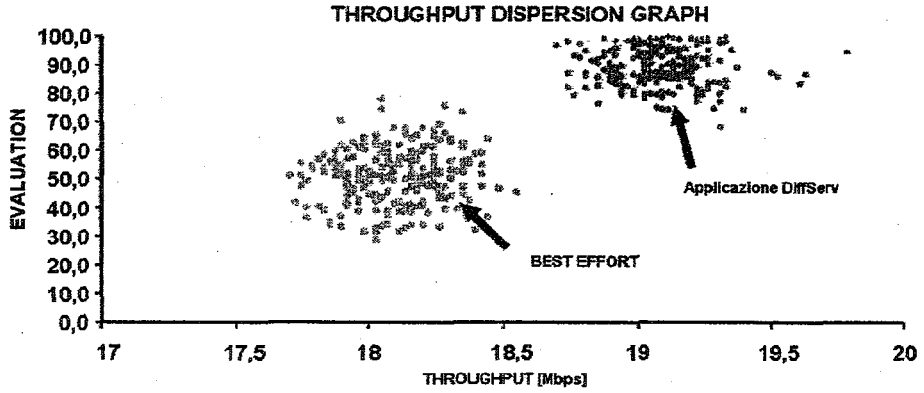


Figura 8: grafico a dispersione del throughput con e senza etichettatura dei pacchetti con tecnica DiffServ

3.1.2.2. Virtual private network automatizzate in reti di trasporto multi-vendor

Le Virtual Private Networks (VPN) sono servizi di rete che stanno riscuotendo un sempre crescente successo tra le aziende e gli operatori telefonici grazie alle loro caratteristiche di sicurezza e flessibilità. Attualmente la creazione di una VPN richiede un attento esame da parte di un operatore dello stato dei nodi di reti interessati dal servizio ed una successiva configurazione degli stessi con tempi, in genere, dell'ordine di giorni. Un tale processo può essere estremamente velocizzato ed automatizzato dall'introduzione di opportune estensioni all'architettura ASON/GMPLS che permetterebbero agli operatori di configurare automaticamente e con tempi ridotti i nodi di rete in ambiente multi-dominio e multi-vendor ed agli utenti di effettuare richieste di VPN ai loro operatori.

La fornitura di servizi VPN

Una VPN (Virtual Private Network) è un servizio di rete che permette di emulare su di una rete condivisa, l'esclusività fisica propria di una rete locale consentendo, al contempo, politiche di QoS e sicurezza. I maggiori vantaggi di una VPN rispetto ad una rete fisica dedicata risiedono nella dinamicità di creazione e nel basso costo di realizzazione al punto da essere ad oggi la soluzione preferita dalle aziende per l'interconnessione delle loro LAN dislocate in aree geografiche diverse. Le tipologie di VPN maggiormente diffuse attualmente sono quelle che coinvolgono tecnologie classificabili nello strato 2 e 3 della pila OSI, sebbene si preveda in futuro la diffusione di VPN che utilizzano tecnologie di strato 1, con granularità pari alla lunghezza d'onda in una fibra ottica, grazie in particolare ai progressi ottenuti della tecnologia WDM.

Un esempio di tecnologia VPN di livello 3 basato sul protocollo di trasporto IP è il "BGP/MPLS IP Virtual Private Network (VPN)" o VPN L3. Questo servizio di rete permette la creazione di una rete privata virtuale in un ambiente multi-dominio in maniera scalabile e sicura grazie all'utilizzo dell'architettura di rete MPLS e del protocollo BGP. L'MPLS è utilizzato come protocollo di "tunnelling" per ottenere una connettività tra i nodi di bordo della rete con percorso prestabilito e possibilità di ingegnerizzare il traffico grazie alla creazione di Label Switched Path (LSP).

Il protocollo BGP è utilizzato per la creazione e lo scambio di tabelle di instradamento dei pacchetti specifiche per la VPN allo scopo di permettere la coordinazione tra i bordi della rete collegati dagli LSP. In particolare, in una VPN L3 l'instradamento dei pacchetti IP tra i bordi della rete è ottenuto con l'utilizzo dello spazio di indirizzamento tipico del protocollo di trasporto IP, mentre l'evoluzione del protocollo BGP, denominata BGP V4, permette di distinguere su di uno stesso nodo di rete più VPN L3 in quanto crea uno spazio di indirizzamento privato e distinto, rispetto all'IP e al BGP standard.

Il maggior vantaggio dell'utilizzo delle VPN L3 è che è facilmente realizzabile con dispositivi di rete commerciali che supportano la suite MPLS. In particolare, l'intelligenza delle VPN L3 risiede solo nei router di bordo, detti Provider Edge (PE), perché essi gestiscono l'instaurazione degli LSP e la coordinazione tra le tabelle di routing BGP private appartenenti a differenti VPN L3. I router interni non sono a conoscenza delle configurazioni necessarie all'instaurazione delle VPN, rendendo le VPN L3 scalabili al crescere delle dimensioni della rete.

Il principale svantaggio dell'uso delle VPN L3 risiede nella complessità necessaria per la configurazione e la gestione dei protocolli BGP e MPLS in maniera coordinata tra i nodi di bordo. Attualmente le VPN L3 sono gestite da un operatore in maniera centralizzata, senza meccanismi automatizzati. Inoltre il costante fiorire di specifiche di protocolli non ancora standardizzati ufficialmente ma già operativi sugli apparati di produttori diversi pone delle serie questioni di

interoperatività quando le VPN L3 devono essere create in reti multi–dominio.

L'architettura ASON/GMPLS è stata dotato di un piano funzionale denominato Service Plane (SP) [2], capace di colloquiare con i nodi di bordo del piano di controllo allo scopo di permettere l'automatizzazione della gestione dei servizi di rete (creazione, abbattimento, modificazione). Il SP è costituito da una entità centralizzata chiamata "Centralized Service Element" (CSE) e da più elementi, chiamati "Distributed Service Element" (DSE) associati a ciascun PE della rete. L'elemento CSE è addetto al controllo dell'identità di chi chiede un servizio, e alla gestione del database che memorizza i contratti detti "Service Level Agreement" (SLA) stipulati con i clienti della rete. Il DSE è una entità distribuita in grado di accettare richieste di servizi di rete da applicazioni tramite l'interfaccia denominata User to Service Interface (USI). Queste richieste sono trasformate in maniera completamente automatizzata in una serie di direttive al piano di controllo tramite la "User to Network Interface" (UNI) e distribuite ai PE coinvolti nel servizio stesso grazie ai protocolli di segnalazione CSE-DSE e DSE-DSE. Importante sottolineare che il SP non è un gestore distribuito perché non gestisce direttamente le risorse di rete. Il principale vantaggio del SP risiede nel fatto che il suo utilizzo non comporta modifiche agli apparati di rete e non si sostituisce all'uso della UNI e del sistema di gestione ma estende le capacità della rete di fornire servizi di rete complessi in maniera automatizzata e distribuita riducendo l'intervento umano a semplice supervisore delle attività della rete.

Il valore aggiunto del SP nel caso di fornitura di servizi VPN L3 risiede nella constatazione che i parametri identificativi necessari per creare quel servizio di rete sono molto diversi se visti dalla prospettiva dell' utente oppure dalla prospettiva di rete. Infatti un utente richiede una VPN L3 in termini di banda e di indirizzi IP degli "host" o delle LAN private che devono essere interconnesse. In particolare la banda richiesta viene tradotta dal SP nella banda da richiedere alla rete tenendo conto della granularità che la stessa è in grado di supportare (ad esempio VC4 nel caso di reti SDH). Inoltre gli indirizzi IP elencati dagli utenti vengono risolti dal SP negli indirizzi dei PE che servono il traffico degli host o le LAN dell'utente stesso. Tuttavia questi parametri passati dagli utenti non sono sufficienti, a livello di rete, per creare il servizio poichè i router coinvolti nell'instaurazione della VPN necessitano di direttive specifiche per quanto riguarda la configurazione dei protocolli espresse in maniera differente a seconda del linguaggio utilizzato. Al fine di instaurare la VPN, è necessario configurare per ogni nodo: il protocollo BGP, utile allo scambio delle tabelle VRF (VPN Routing and Forwarding Table), l'MPLS per la prenotazione di banda tramite gli LSP, e soprattutto una istanza privata di protocollo di instradamento costruita ad hoc per la VPN. I parametri necessari all'instaurazione della VPN L3 vengono ottenuti dal SP in modo trasparente all'utente in funzione della topologia della rete e delle risorse disponibili ed infine tradotti in un insieme di direttive UNI

ad opportuni nodi di bordo del piano di controllo per la creazione degli LSP e delle configurazione dei protocolli di rete necessari alla creazione della VPN.

Il testbed

Il testbed di fig. 1 è stato configurato come riportato in fig. 6, realizzato per validare l'instaurazione automatica di una VPN L3 da parte di un prototipo di Service Plane, e valutare l'interoperabilità tra apparati di rete di differenti produttori (vendor).

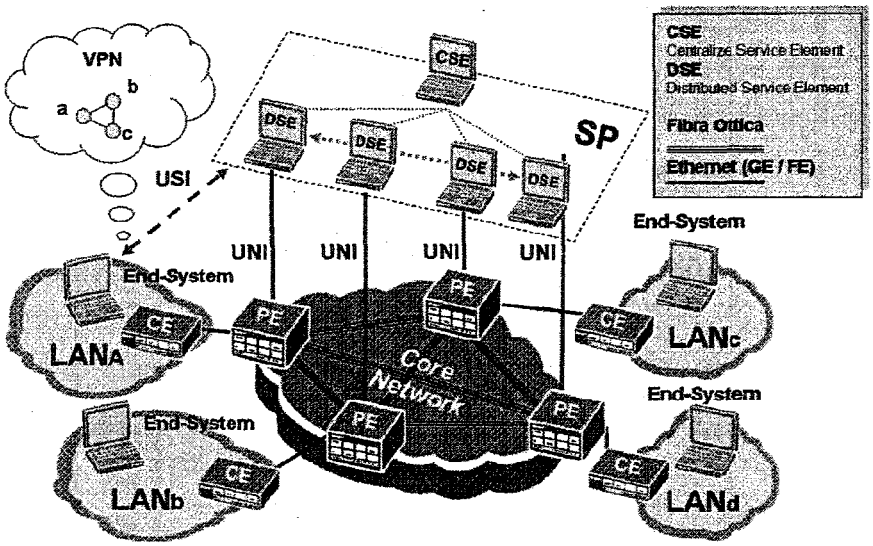


Figura 9. Il testbed

Il testbed utilizza l'anello ottico sperimentale Roma-Pomezia di 50 km di lunghezza complessiva ed è formato da sette router di differenti vendor, interconnessi in maniera completamente magliata allo scopo di poter creare topologie virtuali differenti. In particolare nella scelta delle topologie si è tenuto conto delle diverse situazioni riscontrabili in una rete multi-vendor, considerando che gli elementi nevralgici, sui quali andranno caricate dinamicamente le configurazioni, sono i PE. Il ruolo del PE, ovvero del router di bordo, viene coperto alternativamente da router dei diversi vendor in modo da ottenere genericità sui test. I nodi interni della rete non necessitano di configurazioni "ad hoc" per le VPN L3, ovvero questi elementi sono trasparenti alle configurazioni presenti ai bordi della rete quindi senza perdita di generalità possiamo ignorare la scelta del vendor nei nodi interni. Come protocollo di comunicazione tra i router della LAN che si interfacciano con la rete di trasporto, detti Customer Edge (CE), ed i PE è stato scelto l'OSPF in quanto questa è la soluzione più diffusa tra le LAN di tipo aziendale.

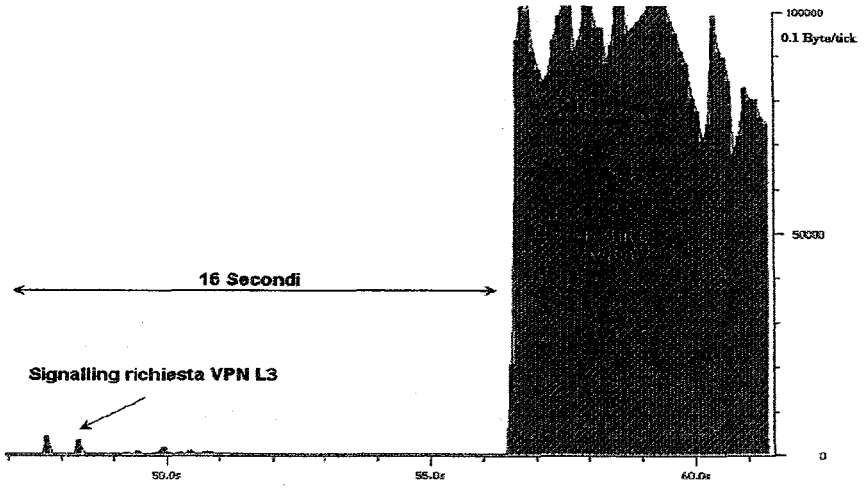


Figura 10. Tempo di instaurazione VPN L3

E' stato valutato il tempo di instaurazione e si è verificata l'effettiva connettività della VPN L3 dopo la richiesta (on-demand) da parte di una applicazione al SP. Dal grafico di fig. 7 si può notare come il tempo di instaurazione della VPN L3, comprensivo del signaling effettuato dal SP, sia di circa 16 secondi dalla richiesta. Questo risultato è assai rilevante specialmente se confrontato con i tempi dell'ordine dei giorni che un operatore impiega oggi per instaurare lo stesso servizio.

3.1.2.3. Ripristino a livello GbE

Il ripristino nelle reti ottiche Ethernet, può esserre trattato con tecniche proprie dell'IP, che però richiedono tempi molto lunghi se non vengono utilizzate particolari metodologie. Per esempio l'utilizzo di un meccanismo di protezione/ripristino del tipo Fast Reroute gestito dall'MPLS può fortemente migliorare la velocità del ripristino raggiungendo tempi confrontabili con quello tipico dell'SDH. Una via alternativa per ottenere un ripristino molto efficiente e veloce in reti GbE è quella di far ricorso a tecniche hardware basate sulla commutazione del traffico affetto da guasto, verso un cammino fisico alternativo, commutazione che è direttamente comandata dal rilevamento della mancanza segnale (LoL - Loss of Light) da parte dei router. In genere lo svantaggio di un meccanismo di protezione e/o di ripristino basato su un percorso fisico alternativo è la necessità di avere un cavo alternativo, il cui costo non sarebbe compatibile con l'economicità che deriva dalla tecnica di trasmissione GbE. Per questa ragione, in questo lavoro, si propone un meccanismo di ripristino che prevede di commutare e accoppiare (multipare) la lunghezza d'onda λ presente in un collegamento che è stato affetto da guasto su un collegamento alternativo già esistente. In questo modo, oltre a registrare una consistente riduzione dei tempi di ripristino del traffico in caso di guasto si riesce anche ad aumentare la potenzialità dei collegamenti in fibra ottica coinvolti nelle

reti, rendendo questi più efficienti in termini di capacità trasportata. Questo meccanismo di protezione/ripristino, da noi denominato AWP (Alternative Wavelength Path), è stato verificato su un test-bed di rete IP e i risultati ottenuti in termini di "tempi di ripristino" sono stati confrontati con quelli ottenibili con altri meccanismi di protezione /restoration basati sui protocolli standard di instradamento (OSPF) e di segnalazione (RSVP-TE) gestiti dall' ASON/GMPLS.

Il citato meccanismo di protezione/restoration (fig. 8), è basato sul principio che quando si verifica un guasto nel collegamento tra due router, questi sono in grado di rilevare una segnalazione di allarme per mancanza segnale (LoL). Tale segnalazione di allarme viene poi utilizzata per far commutare uno switch ottico all'uscita del Router LAB1 e quindi instradare il traffico associato alla lunghezza d'onda λ_1, dal percorso (a) ai percorsi (b)+(c), su cui già viaggiano rispettivamente le lunghezze d'onda λ_2 e λ_3.

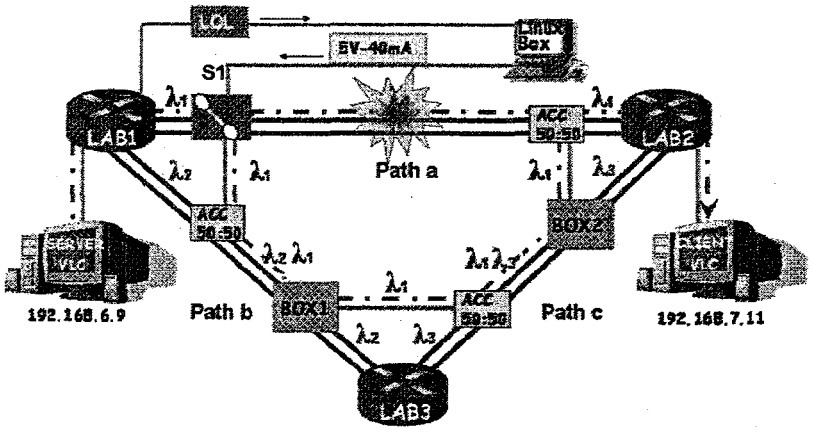


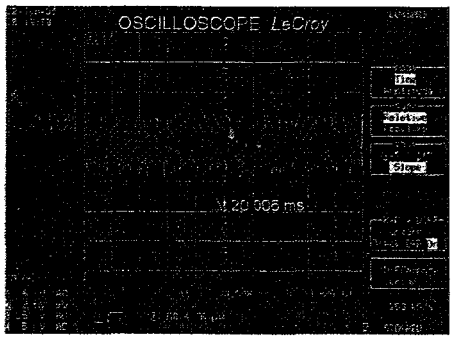
Fig.11: Procedura di ripristino basata sul percorso alternativo costituito da una lunghezza d'onda. Sui terminali VLC viene verificata la qualità di filmati DVD trasmessi in rete.

Il citato meccanismo di ripristino è stato sperimentato sul test bed riportato nella seguente Fig. 11. Questo è essenzialmente costituito da 3 core router con interfacce 1.25 GbE, operanti a 1550 nm (λ_1, λ_2, e λ_3 sono 1550.40, 1551.43 e 1553.36 nm) su lunga distanza. I router sono tra loro connessi con le fibre ottiche del cavo Roma-Pomezia (25 km), giuntate a Pomezia in modo tale da realizzare delle connessioni lunghe 50 km. Le modalità con cui è stata realizzata la rete sono tali da garantire la QoS con tecnica DiffServ su MPLS.

Risultati

Nella fig.12 è riportato l'andamento del segnale ottico registrato all'ingresso del router LAB2 prima della rilevazione del LoL per rottura del collegamento (a), durante la fase di commutazione ottica e dopo il reinstradamento del segnale stesso (λ_1) dal collegamento (a) al collegamento (b) + (c). La

rottura del collegamento è ottenuta mediante uno switch, messo dopo S1, comandato da PC in modo da calcolare accuratamente i tempi di ripristino. Dalla fig.9 si può notare una interruzione del segnale di circa 20 ms.



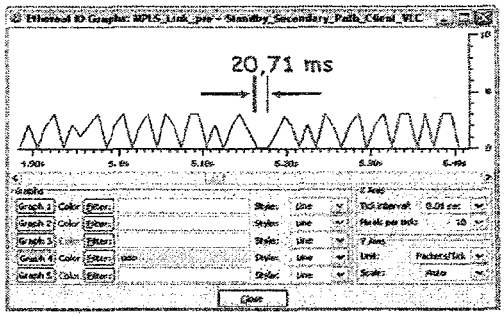


Fig. 12: segnale ottico all'ingresso di LAB2 Fig.13: Comportamento del segnale in LAB2

Oltre che al controllo del segnale ottico abbiamo anche analizzato il flusso dei pacchetti per mezzo del Software "Etheareal", che conferma la perdita di pacchetti per soli 20 ms (fig. 13).

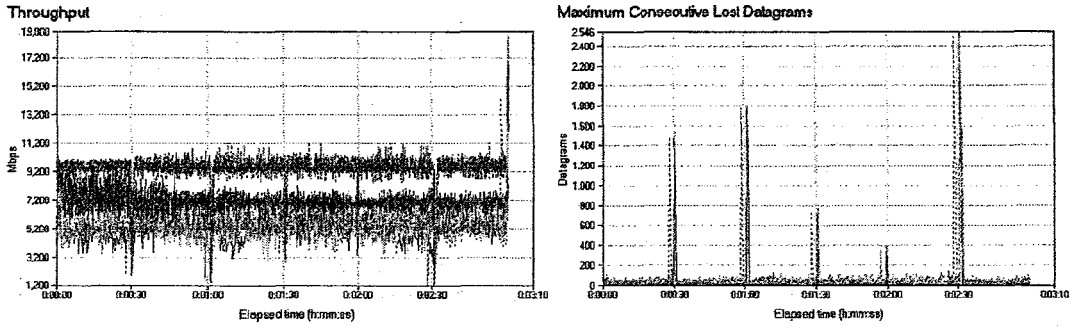


Fig.14: andamento del throughput (a sinistra) e del jitter (a destra) in corrispondenza di 5 interruzioni.

Sono state fatte anche prove di throughput e data lost, effettuando 5 rotture consecutive ed i risultati sono riportati in fig. 14, che confermano che la diminuizione del throughput e le perdite di pacchetti avvengono per brevissimi intervalli (20 ms) durante le operazioni di ripristino. Viceversa è stato verificato che nel processo di commutazione (ritorno) alla via working (a) iniziale non si verificava alcuna perdita percettibile dei dati dal momento che questa commutazione avveniva con tempi ancora più rapidi (circa 3 ms) in quanto era una operazione che non richiedeva il processo con il segnale LoL. Questo è un punto fondamentale per le future reti ottiche perché mostra come i processi di riconfigurazione della rete (operazioni di add/drop, cambio di lunghezze d'onda, ecc...) possono rendere trascurabile la degradazione del traffico se fatti con tempi estremamente brevi.

Oltre a verificare il comportamento della rete con prove oggettive sono state realizzate anche delle prove percettive per verificare la soddisfazione dell'utente per questa procedura di ripristino. Allo scopo sono stati mostrati ad un gruppo di valutatori dei filmati da DVD che circolavano nella rete durante le operazioni di ripristino. Il risultato è stato che i valutatori non percepivano alcun degrado nelle immagini mostrate.

Per completezza abbiamo confrontato la nostra procedura con le tecniche di ripristino offerte dai protocolli per reti Ethernet basate su IP, come l'OSPF (Open Short Path First) e l'MPLS (Multi Protocol Label Switching). Per quanto concerne l'MPLS, che ad oggi è il protocollo più efficiente per il ripristino, abbiamo confrontato l'AWP oltre che con le configurazioni tradizionali anche con due configurazioni ottimizzate per il ripristino a seguito di link failure che vanno sotto il nome di MPLS-LP ed MPLS-LP+SSP. La prima MPLS - LP (LP sta per Link Protection) pre-alloca le risorse per la protezione del link a seguito ad esempio di una rottura; la seconda MPLS LP+SSP (SSP sta per Stand by Secondary Path) in aggiunta alla allocazione delle risorse per la link protection prevede l'instaurazione di un LSP secondario che faccia da back up a quello in esercizio. Come si può ben notare, risulta chiaro il vantaggio che si può ottenere con il meccanismo AWP in termini di tempo di ripristino.

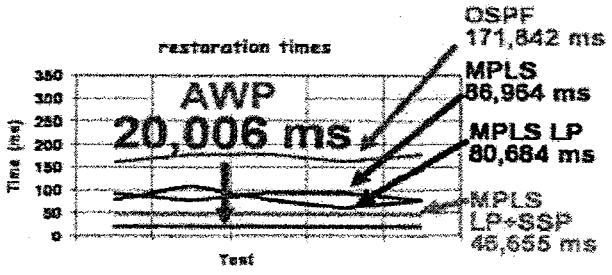


Fig.15: Confronto tra la nostra tecnica AWP e altre tecniche di ripristino OSPF e MPLS.

3.1.2.4. Sistemi optical wireless.

Anche nel 2006 è continuata, in collaborazione con l'ISCOM, l'attività sui sistemi optical wireless. In particolare si è studiata la possibilità di inviare tutto il contenuto informativo presente in una fibra ottica (che potrebbe essere costituito da molte lunghezze d'onda ad alto bit rate) ad essere inviato in un collegamento optical wireless. Questo potrebbe essere molto importante ai fini di connettere tratti di backbone, dove non ci sia però un collegamento in fibra o in caso di un disastroso evento naturale.

Sono stati svolti diversi esperimenti sia in laboratorio che all'aperto con apparati montati sull'edificio del Ministero delle Comunicazioni e sull'edificio di Poste Italiane. I sistemi full duplex

sono costituiti da apparati commerciali che in trasmissione utilizzano un laser VCSEL (Vertical Cavity Surface Emitting Laser) operante a 850 nm, seguito da un gruppo di lenti telescopiche, che forniscono al fascio una divergenza angolare di 4mrad, e in ricezione un fotodiodo a valanga. Questo sistema permette una trasmissione fino a 4 km.

Fig. 16 gli apparati optical wireless presso l'ISCOM.

Nei primi mesi del 2006 gli studi sui sistemi optical wireless sono stati concentrati sulla trasmissione WDM. Nella figura 14 riportiamo il set up sperimentale costituito da tre sorgenti (Laser DFB su tre lunghezze d'onda a 1500 nm, due modulate a 2.5 Gb/s e una a 40 Gb/s. Il cammino ottico in aria era regolato da un attenuatore variabile per simulare l'attenuazione dovuta alle condizione metereologiche sfavorevoli.

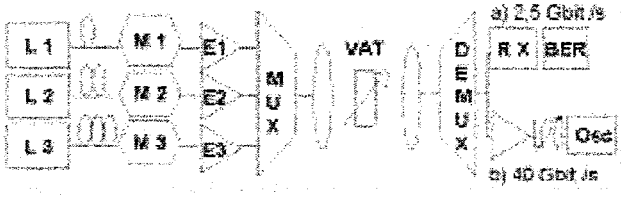


Fig. 17: Set-up sperimentale

Nella fig. 15 riportiamo il fattore Q per il canale a 40 Gb/s in funzione della potenza ricevuta, in presenza dei 2 canali a 2.5 Gb/s (2int) e in loro assenza (0 in). E' chiaro che nessuna interfenza è prodotta dai due canali e quindi la tecnica WDM nello spazio libero si dimostra una grande opportunità.

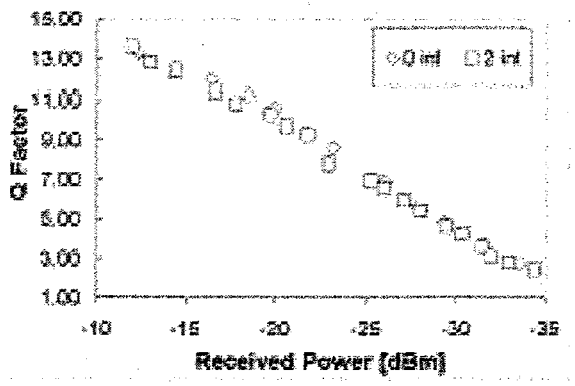


Fig. 18: prestazioni di un sistema a 40 Gb/s in optical wireless

Tra le principali applicazioni che pensiamo alla tecnica del WDM per l'optical wireless pensiamo ad azioni di disaster recovery, dove a causa di una improvvise rottura di un cavo di una dorsale che trasporta molti canali WDM si potrebbero avere danni catastrofici dal punto di vista delle telecomunicazioni, con tempi di ripristino troppo elevati se basati sulla ricostruzione dell'opera. Il montaggio di un sistema optical wireless può essere fatto nel giro di qualche ora.

3.1.2.5. Quality of Experience per servizi IP-TV

Sulla base delle risultanze della ricerca eseguita l'anno precedente in collaborazione con Fast-Web e ISCOM, la Fondazione ha proseguito la sua attività di ricerca nel campo della Quality of Experience (QoE), ovvero negli studi orientati alla valutazione dei requisiti di utente (ovvero degli Operatori del settore telecomunicazioni) e del livello di "soddisfazione" dell'utente finale per servizi televisivi erogati attraverso canali internet.

L'attività descritta si è svolta nell'arco dell'anno 2006 e sta proseguendo nell'anno corrente.

Sulla base delle risultanze degli studi eseguiti nel 2005, si è cercato di individuare meglio i requisiti di utente in relazione anche a quanto individuato dall'organismo internazionale DSL-Forum. Il Forum DSL è un consorzio nato nel 1994 e composto da circa 200 industrie leader del settore delle telecomunicazioni (operatori, manifatturiere, gestori di reti ecc.) che si prefigge lo scopo di introdurre e facilitare la penetrazione di nuovi servizi, impieganti piattaforme e modalità di sviluppo comuni e tali da rendere i servizi facilmente scalabili e economicamente profittevoli. L'acronimo DSL deriva dalla definizione della linea di utente digitale (Digital Subscriber Line) ed è conforme con I princiapli risultati del gruppo che hanno portato alla standardizzazione internazionale delle tecnologie ADSL, SHDSL, VDSL, ADSL2plus.

Da qui la possibilità per operatori di rete fissa (una volta confinati al settore della telefonia classica) di evolvere verso servizi noti come "triple play", ovvero telefono, internet e TV.

La Fondazione ha rivolto la propria attenzione verso questo organismo anche in ragione del fatto che il DSL-Forum ha accettato i risultati ottenuti durante la ricerca eseguita nel 2005 e li ha inseriti in un rapporto tecnico pubblicato sul proprio sito internet (TR-126).

Visto il successo della ricerca del 2005; si è deciso di proseguire le indagini cercando di affinare i risultati ottenuti precedentemente.

I primi dati non permettono ancora la stesura di un modello sufficientemente accurato da meritare una pubblicazione, ma costituiscono una incoraggiante base teorico sperimentale verso la preparazione di una proposta di standardizzazione internazionale (ITU).

In pratica si sta cercando di determinare le condizioni per cui alcune configurazioni di perdita di segnale in un servizio IPTV (in pratica perdita di pacchetti IP) comportano un impatto significativo sulla QoE, ovvero sul livello di soddisfazione dell'utente finale.

Queste misurazioni vengono fortemente influenzate anche da scelte eseguite dagli operatori, come ad esempio la scelta del terminale di utente(Set Top Box – STB), e alcune funzionalità che esso fornisce, in termini di controllo della QoS (Qualità of Service). Infatti, nel caso di utilizzo di STB che non applicano strategie di "error concealment", la tipologia degli artifatti introdotti da perdite di servizio è confrontabile con quelli rilevabili da un utente che fruisce il servizio TV attraverso il satellite; al contrario la presenza di strategie di "error concealment" nei STB per IP-TV abbassa sensibilmente l'impatto dei disservizi rendendoli meno visibili all'utente finale e, di conseguenza, innalzando il livello della "QoE". Un altro aspetto di sicuro interesse, che sarà oggetto di studio nel prossimo anno, è rappresentato dall'utilizzo di nuovi protocolli di trasmissione dati, che permettono un'ottimizzazione della gestione delle informazioni perse anche per servizi in "tempo reale" come l'IP-TV. L'avvento di queste nuove strategie sarà reso possibile grazie anche alla sempre maggiore capacità di banda che le nuove tecnologie DSL renderanno disponibile nei collegamenti su rame.

In fine va rilevato che gli studi soprastati avranno impatto anche nei lavori che la Fondazione presenterà al neo-costituito gruppo "IPTV Focus Group" (FG IPTV) la cui missione comprende il coordinamento e la promozione dello sviluppo di standard globali per il servizio IPTV tenendo conto delle attuali attività dell'ITU (International Telecommunication Union) così come di tutti gli altri Enti Internazionali di Standardizzazione, i Forum ed i Consorzi ceh operano nel settore.

3.1.3 Ipotesi per la diffusione della Larga banda nelle zone rurali

Dalla esperienza sperimentale sul test bed di rete IP la FUB ha effettuato alcuni studi sulle metodologie e i costi per portare la larga banda nelle zone meno sostenibili dal punto di visto economico. Tra queste zone quelle a cui abbiamo dedicato il maggiore interesse è quello delle Comunità Montane e alcuni casi particolari sono stati studiati nell'area dell'Alta Sabina.

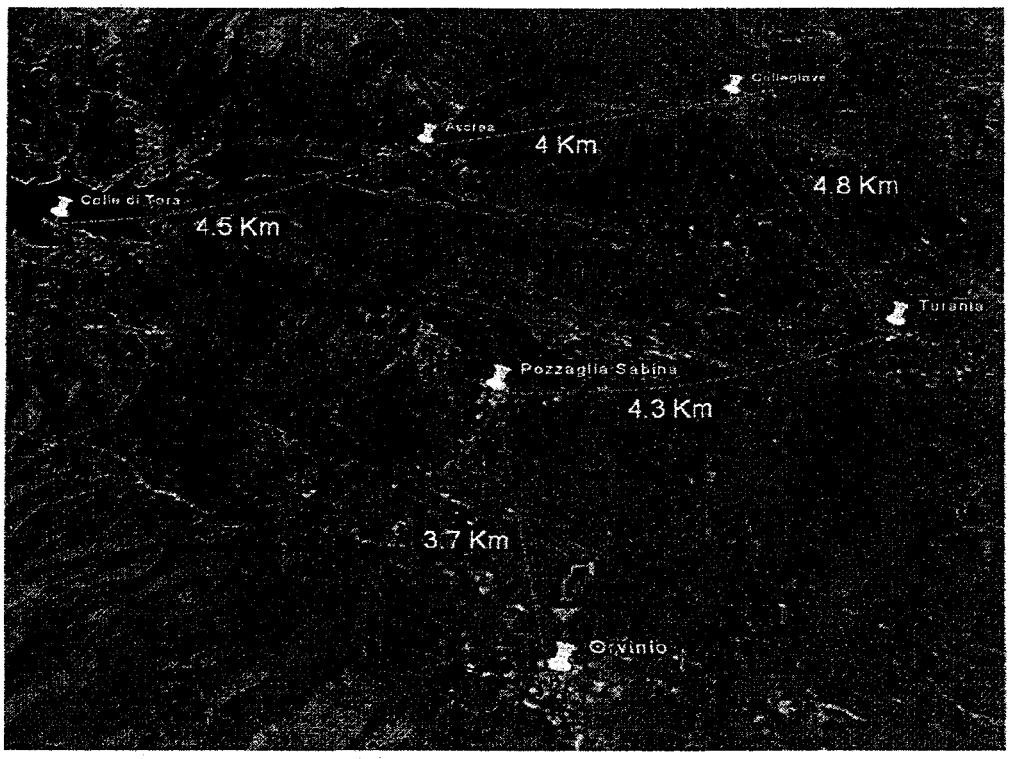


Fig. 19: Un esempio di zona rurale: l'Alta Sabina

Le Comunità montane sono costituite da centri rurali, come piccoli comuni, centri agricoli, gruppi di fabbricati che non hanno a disposizione connessioni a larga banda (se non tramite satellite). In genere comunque possiedono una copertura telefonica PSTN e questo è un vantaggio perché esiste una minima infrastruttura di rete. Gli utenti sono connessi alla centrale telefonica in doppino con distanze che possono raggiungere anche i 2 o i 3 chilometri. Le centrali sono connesse principalmente mediante ponti radio alla rete PSTN, ed in particolare la fibra ottica in genere raggiunge il comune più grande (o il più facilmente raggiungibile) che rappresenta la base di una certa zona. Nel comune raggiunto dalla fibra è montata la centrale di commutazione che serve anche ad alimentare i ponti radio che serviranno i comuni adiacenti. Come esempio riportiamo la zona dell'Alta Sabina rappresentata dalla figura, dove la fibra raggiunge il Comune di Orvinio. La connessione in fibra consiste in un classico anello ottico a 4 fibre a 155 Mbit/s (STM-1). Il cablaggio è effettuato tramite cavo multifibra a 10 fibre (6 di queste sono spente e sono utilizzabili per sostituire eventuali fibre danneggiate o per realizzare altri collegamenti o estensioni). Nella centrale telefonica di Orvinio sono attestate circa 100 linee POTS e 4 linee ISDN. I paesi riportati nella figura sono connessi alla centrale di Orvinio mediante ponti radio a 34 Mb/s.

Il nostro studio parte dalla considerazione che dovendo comunque affrontare degli investimenti

assai rilevanti, conviene pensare ad un progetto che duri nel tempo e quindi alla possibilità di una fruizione di servizi che possa essere esauriente almeno per i prossimi 10 anni. Questo significa fare delle scelte in grado di fornire la IPTV, possibilmente anche con modalità HDTV. Per questo pensiamo ad una tecnica con DLAM ADSL2+ in centrale e che permette quindi di offrire 20 Mb/s agli utenti che distano meno di 500 m dalla centrale (e quindi abilitati anche per la IPTV HD) e 6 Mb/s per quelli che distano fino a 2 km dalla centrale (abilitati quindi con la IPTV convenzionale). Si pensa quindi di installare in ciascun comune, nella centrale, un DSLAM in grado di coprire almeno il 20% della popolazione. Considerato la bassa densità di popolazione in queste aree possiamo dire che i DSLAM si possono limitare ad un numero di 16-32 porte con costi intorno ai 2000-4000 Euro.

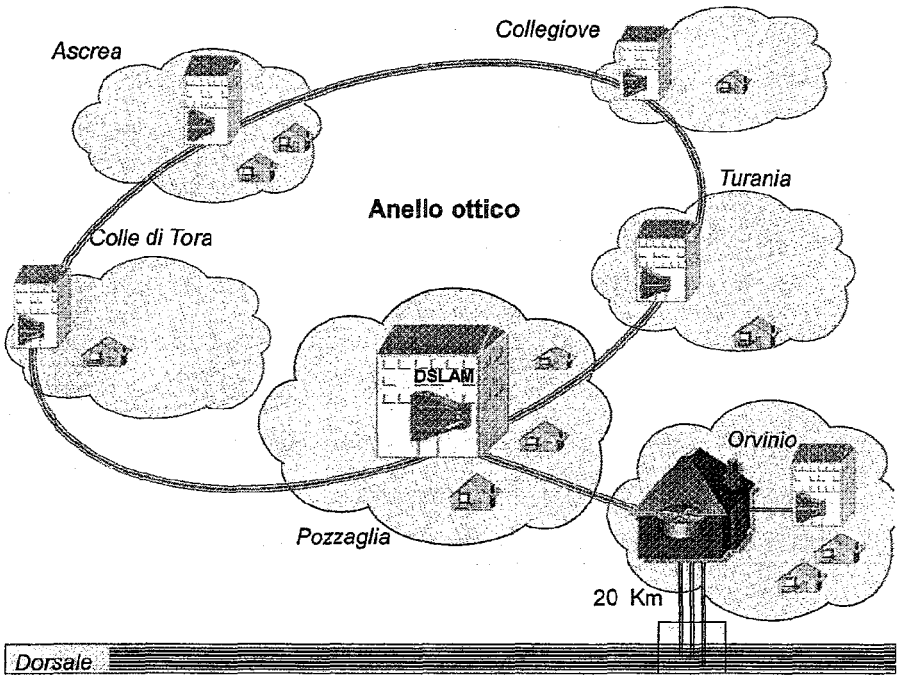


Fig 20: Schema dell'anello ottico per l'alta sabina.

Per la realizzazione di una infrastruttura a larga banda per una comunità come quella in fig.19, cercando di ottimizzare i costi il più possibile noi pensiamo ad una LAN molto estesa costituita da un doppio anello in fibra che collega tutti i comuni, un router nel comune in cui arriva la fibra dalla dorsale e uno switch in ogni altro comune. Il Router e gli switch dovranno avere 4 porte ottiche GbE (ciascuna porta ha un ingresso e una uscita), più porte FE (100 Mb/s) per connettere questi dispositivi ai DSLAM.

Possiamo quindi dire che il costo di una infrastruttura di questo tipo è circa:

Costo infrastruttura LB= costo router + (n-1)x(costo switch) + n x costo DSLAM+ Lcosto fibra

dove n è il numero dei comuni. Il costo del router può aggirarsi intorno ai 100 Meuro, quello dello switch intorno ai 10 Keuro, mentre il costo della installazione della F.O. si aggira intorno ai 30 Keuro/km, per uno scavo in microtrincea. Nel caso riportato nella figura il costo complessivo della rete si aggirerebbe intorno al milione di Euro (circa 170 Meuro a comune), dove il costo principale è proprio data dalla cablatura in fibra. Soluzioni molto più economiche potrebbero essere utilizzate pensando ad esempio di utilizzare cavidotti o palificazioni già presenti.

Nel caso in cui due comuni avessero una distanza inferiore ai 2 km e fossero in visività (LOS) si potrebbe pensare ad una trasmissione optical wireless, che hanno un costo intorno ai 30 Keuro, anche se bisognerebbe prendere in considerazione i fuori servizio che potrebbero essere causati dalle cattive condizioni atmosferiche (specialmente la nebbia); un costo quindi minore (2 km di installazione in fibra costano circa 60 Keuro), ma certamente meno affidabile e soprattutto non comaparabile in termini di banda rispetto alla fibra ottica.

Rimane inoltre da segnalare la futura possibilità di utilizzare la tecnica WIMAX al posto delle connessioni ottiche. Certamente il WIMAX sarebbe molto più economico rispetto alla cablatura in fibra e più affidabile rispetto all'optical wireless. Tuttavia per far dei confronti economici occorre prendere in considerazione anche i costi dovuti alle licenze del WIMAX.

La nostra opinione è che nella realizzazione delle infrastrutture per larga banda in aree rurali, ai fini di non precludere l'utenza verso servizi ad alta capacità, conviene realizzare, almeno per alcuni segmenti, connessioni in fibra ottica, anche se altamente costosi. In questo modo si metterebbe a disposizione dell'area una infrastruttura in grado di sostenere tutte le evoluzioni che le TLC possono avere. Per alcuni segmenti di rete, specialmente quelli con minor traffico, possono esser utilizzate soluzioni alternative, come sistemi radio (WIMAX soprattutto) e sistemi optical wireless (per brevi distanze, 2 km).

3.1.4 Il protocollo IPv6.

La FUB ha svolto alcuni studi, parallelamente ad un confronto tecnico tra aziende e operatori, sul tema dell'IPv6 e su questo tema ha realizzato il Quaderno di Telema "La domanda di comunicazione chiede di aggiornare Internet" pubblicato a dicembre 2006. Riportaimo nel seguito i principali risultati.

Le reti attuali sono basate sulla versione 4 di questo protocollo (IPv4), che per molti versi risulta inadeguata già per le esigenze attuali. Ecco quindi la versione 6 (IPv6) che è già disponibile, ma non è ancora chiaro quando questa entrerà profondamente nella rete. Come mostrato dal Quaderno di Telema (febbraio 2006) l'IPv6 ha oggi un alto grado di maturità, è in grado di rispondere a tutte le esigenze di comunicazione, che sono prevedibili per i prossimi anni, specialmente quelle legate