Per motivi di affidabilità è tipico collegare i router CE attraverso un doppio collegamento allo stesso PE oppure a due PE distinti.

Sono anche possibili configurazioni che prevedano siti VPN collegati attraverso due router CE a due router PE.

Consideriamo per primo il caso di un router CE con un collegamento di accesso ad un router PE di tipo "multi-link", ossia un router CE connesso con più collegamenti fisici al PE; questa soluzione trova applicazione soprattutto quando si vuole garantire al cliente VPN un accesso fisico di velocità intermedia tra due valori standard (es. N x 2 Mbit/s).

La politica più conveniente di ripartizione del traffico entrante ed uscente sui collegamenti è quella a "divisione equa del carico"; questa può essere raggiunta sfruttando le possibilità offerte dalla maggior parte dei protocolli di routing di dividere equamente il traffico su cammini di eguale metrica **(Equal Cost Multipath).**

Una semplice configurazione per ottenere questo obiettivo è quella che prevede delle route statiche di default che dal router CE puntino verso le interfacce di attestazione dei collegamenti sul router PE ed un protocollo di routing dinamico (ad es. RIP) che permetta al router PE, in caso di fuori servizio di un collegamento di inviare tutto il traffico verso il CE sui collegamenti funzionanti.

Il caso più frequente di configurazione ***fault-tolerant*** è quello che prevede un doppio collegamento su due PE diversi (dual-homing).

Le politiche di ripartizione del traffico sui due collegamenti dipendono dalla particolare applicazione e possono essere:

- a ripartizione equa
- a riserva fredda: il traffico (in ingresso ed in uscita) viene tutto instradato su un collegamento definito come primario e quindi deviato automaticamente sul collegamento secondario (backup) in caso di fuori servizio del collegamento primario.

In questi casi, oltre a prevedere la possibilità di politiche di ripartizione del traffico sia sull'accesso che all'interno della rete BGP MPLS, è necessario fare attenzione al formarsi di possibili loop ed a situazioni che comportino un instradamento non ottimo del traffico.

Situazioni non ottimo del traffico dipendono spesso dal valore di "distanza amministrativa", ricordando che di norma i protocolli utilizzati sui collegamenti PE-CE hanno sempre distanza amministrativa inferiore rispetto a MP-iBGP, possono verificarsi loop oppure percorsi non ottimali con maggiore salti di router.

Il protocollo BGP di regola non distribuisce mai annunci verso AS già attraversati e quindi utilizzando BGP nei collegamenti PE-CE si evitano automaticamente il formarsi di eventuali loop, a meno che nei PE non sia configurata la funzionalità AS override oppure nei CE il comando "neighbor..allowas-in ".

In entrambi i casi gli annunci BGP verrebbero propagati verso i CE portando di nuovo a pericoli di loop. Il problema viene risolto tramite un nuovo attributo BGP di tipo *Extended_Communities* denominato **SOO** (Site Of Origin).

In pratica il SOO identifica il sito che ha originato l'annuncio e previene il ritorno di questo allo stesso sito.