ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΜΕΛΕΤΗ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ GMPLS»

ΑΝΑΣΤΑΣΙΟΣ Ν. ΜΠΙΚΟΣ
Α. Μ 2686

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ:
Χρήστος Μπούρας, Καθηγητής

ΕΠΙΒΛΕΠΟΝΤΕΣ
Κωσταντίνος Στάμος

ΠΑΤΡΑ 2010

ΠΕΡΙΛΗΨΗ

Από τα μέσα της δεκαετίας 1990 ξεκίνησε μια ραγδαία αύξηση της κλιμάκωσης του Διαδικτύου σε φυσικό επίπεδο και ιδιαίτερα στο IP Service Layer. Πλέον η νέα εποχή των προηγμένων ευρυζωνικών διαδικτυακών υπηρεσιών σηματοδοτείται από τα Ιδιωτικά Εικονικά Δίκτυα –Virtual Private Networks μεταξύ οργανισμών, μετάδοση πολυμεσικών δεδομένων όπως IPTV και Voice over IP, υπηρεσίες τηλεματικής καθώς και δέσμευση ταχύτητας αλλά και συνδέσεων κατ'απαίτηση. Ειδικότερα τα τελευταία δε θα μπορούσαν να υλοποιηθούν διαφορετικά χωρίς την ύπαρξη συγεκριμένων διαφοροποιημένων υπηρεσιών – differentiated services όπως: Ποιότητα Υπηρεσίας (QoS), Service–Level Agreements (SLAs), μηχανισμών κατανομής bandwidth και γενικότερα traffic engineering.

Με την αξιοποίηση της οπτικής ίνας για δικτύωση απομακρυσμένων σταθμών και την εισαγωγή ποικίλων τεχνικών πολυπλεξίας κίνησης, αναπτύχθηκε μία νέα γενιά οπτικών και φωτονικών συσκευών καθώς και αρχιτεκτονικών γιά οπτικά δίκτυα δεδομένων, που οραματίζονταν να κάνουν πράξη τις προκλήσεις του Broadband Internet. Η απαίτηση τόσο για ενοποιημένη πρόσβαση σε ετερογενείς backbone–core αρχιτεκτονικές, όσο και για μεγαλύτερη αυτοματοποίηση της διαχείρησης των transport networks, οδήγησαν στην μετάβαση σε μια νέα Intelligent Optical Networking αντίληψη, οπού οι νέες υπηρεσίες θα μπορούν να εφαρμοστούν με επιτυχία τόσο σε όλα τα δίκτυα μεταγωγής κυκλώματος όσο και σε πολλαπλούς network clients. Η παραδοσιακή μέχρι τότε MPLS υποδομή κορμού έπρεπε, γι'αυτό το σκοπό, να γενικευτεί και να εξελιχθεί σε ένα νέο framework που θα είχε στόχο ένα ενοποιημένο πεδίο διαχείρησης ελέγχου του δικτύου, καθώς και σε τελικό στάδιο τη σύγκλιση του Data με το IP –Data–IP Convergence.

Στη διπλωματική αυτή επιχειρήται μια θεωρητική προσέγγιση και μελέτη του γενικευμένου πρωτοκόλλου επιπέδου 2.5 GMPLS, σενάρια υλοποίησης του σε πραγματικές συνθήκες, όπως στα πλαίσια του AutoBAHN συστήματος του ευρωπαικού προγράμματος GN2, και παράλληλα εκτέλεση πειραματικών μετρήσεων και συγκριτική αξιολόγηση των αποτελεσμάτων με βάση τους δύο δημοφιλέστερους και πλέον εξιδικευμένους δικτυακούς εξομειωτές για το συγκεκριμένο framework: τον NS–2.1, και τον GLASS.

Είναι ευρέως αποδεκτό οτι το GMPLS θα αποτελέσει τεχνολογία κλειδί για την εξέλιξη της νέας γενιάς αξιόπιστων IP backbone δικτύων κορμού υψηλών ταχυτήτων. Το Generalized επεκτείνει την αντίληψη του MPLS traffic engineering (MPLS–TE) προσφέροντας παρόμοιους μηχανισμούς ελεγχου με το MPLS για δίκτυα που υλοποιούν ενιαίες στρατηγικές μηχανισμού κίνησης για όλες τις υποστηριζόμενες τεχνικές διαχωρισμού όπως packet, TDM, wavelength και fiber switching. Οι πλατφόρμες νέας γενιάς που θα υποστηρίζουν την λειτουργικότητα του GMPLS θα προσφέρουν στους service providers την δυνατότητα να μετοικίσουν σε μια αρχιτεκτονική που:

1. Θα εξελισσει τα επικαλυπτόμενα –overlay δίκτυα: TDM, Packet, Cell, Lambda σε ενα ενοποιημένο με κοινό πεδίο διαχείρησης ελέγχου –control plane.

2. Θα επιτρέπει την απο άκρου σε άκρου τροφοδοσία –provisioning των υπηρεσιών από το δικτυο προσβασης μέχρι και το δίκτυο κορμού.

3. Θα επιτρέπει στους παρόχους να χτίζουν πολλαπλά δίκτυα με διαφορετικές ροές κίνησης πάνω στο ίδιο πεδίο μεταφοράς δεδομένων –data plane.

Εφόσον τα πεδία λειτουργικότητας του GMPLS μπορούν να ειναι φυσικά ανεξάρτητα, κάτι τέτοιο άλλωστε ήταν και το όραμα της κοινότητας του Generalized, νέοι μηχανισμοί έχουν υλοποιηθεί ώστε να παρέχουν βιωσιμότητα μέσω σχημάτων προστασίας και αποκατάστασης σε περιπτώσεις κατάρρευσης γραμμής –link failure. Αυτοί οι μηχανισμοί των πρωτοκόλλων σηματοδοσίας RSVP–TE και CR–LDP του GMPLS θα πρέπει να υποστηρίζουν νέες τεχνικές όπως out–of–band signaling (σηματοδοσία σε ξεχωριστό κανάλι), παράλληλες συνδέσεις –link bundling, και προώθηση πληροφοριών γειτνίασης –forwarding adjacencies.

Στόχος, σε πειραματικό επίπεδο της διπλωματικής μου εργασίας είναι αφενός η δέσμευση on demand ενός μονοπατιού σε ένα GMPLS/Optical δίκτυο και μετάδοση διαφορετικών ροών δεδομένων σε αυτό με τεχνικές multiplexing, και αφετέρου η σύγκριση υπαρχόντων μηχανισμών αποκατάστασης και επανάκτησης μετά από αστοχία σύνδεσης, η μελέτη της επιρροής του control plane failure στους QoS μηχανισμους κίνησης, καθώς και η δυναμική διαχείριση των μονοπατιών μετά από κατάρευση. Τέλος, παρουσιάζονται και νέοι βελτιωμένοι μηχανισμοί επανάκτησης στο πεδίο λειτουργικότητας ελέγχου και δεδομένων στα πλαίσια του ASONS Simulator στον ns–2.

EXECUTIVE SUMMARY

Since the mid–1990s a rapid increase in Internet scaling begun in the physical and more particularly in the IP service layer. From that point, the new era of advanced broadband internetworking services is marked by Virtual Private Networks between organizations, transmission of multimedia data like IPTV and Voice over IP, telematic services and even reservation of bandwidth and circuit on demand. The last, in particular, could not be implemented differently without the existence of specific differentiated services like Quality of Service (QoS), Service–Level Agreements (SLA's), bandwidth allocation mechanisms and generally traffic engineering.

With the deployment of optical fiber medium for interconnecting remote stations and the introducing of multiple traffic division multiplexing techniques, a new generation of optical and photonic applications as well as optical architectures emerged, that was visioning to illustrate the challenges of Broadband Internet. The demand for a common access to heterogenous backbone–core architectures, as well as for more automazation of the management of the trasnport networks, lead to the transition to a new Intelligent Optical Networking perception, where the new services could be deployed with success in any circuit–switched network as well as in multiple network clients. The conventional, up until then, MPLS core infostructure should, for that purpose, generalize and evolve into a new framework that would target a common control plane and even in final stage the complete convergence of Data with IP.

In this Diploma thesis, i attempt to give a theoretical approach and study of the Generalized Layer 2.5 Protocol GMPLS, implementation of real world scenarios, like in the context of AutoBAHN system, and in addition, execution of experimental measurements and comparing evaluation of the statistical results based on the two most popular and specifically designed for this framework network simulators: NS–2.1, and GLASS.

It is widely accepted that GMPLS (Generalized MPLS) will be a key technology in the evolution of the next generation of reliable Internet Protocol (IP) backbone networks. The GMPLS extends the MPLS traffic engineering concept by providing the MPLS–based common control mechanisms for multi–layer network which allow implementing common traffic engineering strategy for all supported switching techniques like packet, TDM, wavelength and fiber switching. New generation platforms supporting GMPLS functionality will give service providers an opportunity to migrate a new network architecture that will:

1. Allow overlay networks (TDM, Packet, Cell, and Lambda) to evolve to a single layered architecture with a common control plane.

2. Allow end–to–end provisioning of services extending from the access network to the core.

3. Allow service providers to build multi–vendor networks with many of the

Integration and flow through issues simplified.

Since the functional planes of GMPLS could be independent from the first place, something which had always benn the vision of the Generalized community, new mechanisms have been implemented to offer resiliency through protection and restoration schemes in case of link failure. These mechanisms of the GMPLS signaling protocols RSVP–TE and CR–LDP should support new techniques like out–of–band signaling, link bundling and forwarding adjacencies.

The aim of this Diploma Thesis, in experimental level, is on the first place to reserve a lightpath on demand in a GMPLS/Optical network and transmit different traffic flows on it with various multiplexing techniques, and on the second to compare existing restoration schemes after a link failure, the case study of the impact of control plane failure on the QoS traffic mechanisms, and the dynamic provision of backup paths as well. Finally, new and improved survivability schemes are being presented in the context of ASONS simulator on ns–2.

ΠΡΟΛΟΓΟΣ

Ολοκληρώνοντας την παρούσα διπλωματική εργασία θα ήθελα να απευθύνω ευχαριστίες στα άτομα που με βοήθησαν στον ευρύτερο Πανεπιστημιακό χώρο, ο καθένας με τη δική του συμβολή, που χωρίς τη βοήθειά τους πιθανόν να μην ήταν δυνατή η εκπόνησή της.

Κατ' αρχάς, θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κ. Χρήστο Μπούρα (Καθηγητής τμήματος Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής του Πανεπιστημίου Πατρών) για την επίβλεψη της εργασίας, την εμπιστοσύνη που έδειξε στο πρόσωπό μου στην ανάθεσή της, και για τη δυνατότητα που μου παρείχε ν' ασχοληθώ με ένα τόσο ενδιαφέρον ερευνητικό αντίκειμενο όπως αυτό των οπτικών δικτύων.

Ακόμα θα ήθελα να απευθύνω ιδιαίτερες ευχαριστίες στον Δρ. Κώστα Στάμο γιατί η βοήθειά του, η υπομονή του και η διάθεσή του να με υποστηρίξει υπήρξε καταλυτική στην εκπόνηση της διπλωματικής μου εργασίας.

Κλείνοντας, θα ήθελα να ευχαριστήσω την οικογένεια μου που χωρίς την ψυχική και υλική βοήθειά τους και την αμέριστη συμπαράστασή τους όποτε τη χρειαζόμουν, δεν θα ήταν δυνατό να ολοκληρώσω τις προπτυχιακές μου σπουδές.

Πάτρα, Άυγουστος 2010

Αναστάσιος Ν. Μπίκος

Στην οικογένειά μου

"Equations are more important to me, because politics is for the present, but an equation is something for eternity."

Albert Einstein

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΑΚΡΩΝΥΜΑ

Αγγλικοί όροι

AAL	ATM Adaptation Layer
ASON	Automatically Switched Optical Network
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
EGP	Exterior Gateway Protocol
GMPLS	Generalized MultiProtocol Label Switching
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
ITU	International Telecommunication Union
LER	Label Edge Router
LSR	Label Switch Router
MPLS	Multiprotocol Label Switching
NNI	Network to Network Interface
NS2	Network Simulator 2
OSPF	Open Shortest Path First
QoS	Quality of Service
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
UNI	User to Network Interface
WWW	World Wide Web

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

ΕΙΣΑΓΩΓΗ

Από τα μέσα της δεκαετίας 1990 ξεκίνησε μια ραγδαία αύξηση της κλιμάκωσης του Διαδικτύου σε φυσικό επίπεδο και ιδιαίτερα στο IP Service Layer. Πλέον η νέα εποχή των προηγμένων ευρυζωνικών διαδικτυακών υπηρεσιών σηματοδοτείται από τα Ιδιωτικά Εικονικά Δίκτυα –Virtual Private Networks μεταξύ οργανισμών, μετάδοση πολυμεσικών δεδομένων όπως IPTV και Voice over IP, υπηρεσίες τηλεματικής καθώς και δέσμευση ταχύτητας αλλά και συνδέσεων κατ'απαίτηση. Ειδικότερα τα τελευταία δε θα μπορούσαν να υλοποιηθούν διαφορετικά χωρίς την ύπαρξη συγεκριμένων διαφοροποιημένων υπηρεσιών – differentiated services όπως: Ποιότητα Υπηρεσίας (QoS), Service–Level Agreements (SLAs), μηχανισμών κατανομής bandwidth και γενικότερα traffic engineering.

Με την αξιοποίηση της οπτικής ίνας για δικτύωση απομακρυσμένων σταθμών και την εισαγωγή ποικίλων τεχνικών πολυπλεξίας κίνησης, αναπτύχθηκε μία νέα γενιά οπτικών και φωτονικών συσκευών καθώς και αρχιτεκτονικών γιά οπτικά δίκτυα δεδομένων, που οραματίζονταν να κάνουν πράξη τις προκλήσεις του Broadband Internet. Η απαίτηση τόσο για ενοποιημένη πρόσβαση σε ετερογενείς backbone–core αρχιτεκτονικές, όσο και για μεγαλύτερη αυτοματοποίηση της διαχείρησης των transport networks, οδήγησαν στην μετάβαση σε μια νέα Intelligent Optical Networking αντίληψη, οπού οι νέες υπηρεσίες θα μπορούν να εφαρμοστούν με επιτυχία τόσο σε όλα τα δίκτυα μεταγωγής κυκλώματος όσο και σε πολλαπλούς network clients. Η παραδοσιακή μέχρι τότε MPLS υποδομή κορμού έπρεπε, γι'αυτό το σκοπό, να γενικευτεί και να εξελιχθεί σε ένα νέο framework που θα είχε στόχο ένα ενοποιημένο πεδίο διαχείρησης ελέγχου του δικτύου, καθώς και σε τελικό στάδιο τη σύγκλιση του Data με το IP –Data–IP Convergence.

Στη διπλωματική αυτή επιχειρήται μια θεωρητική προσέγγιση και μελέτη του γενικευμένου πρωτοκόλλου επιπέδου 2.5 GMPLS, σενάρια υλοποίησης του σε πραγματικές συνθήκες, όπως στα πλαίσια του AutoBAHN συστήματος του ευρωπαικού προγράμματος GN2, και παράλληλα εκτέλεση πειραματικών μετρήσεων και συγκριτική αξιολόγηση των αποτελεσμάτων με βάση τους δύο δημοφιλέστερους και πλέον εξιδικευμένους δικτυακούς εξομειωτές για το συγκεκριμένο framework: τον NS–2.1, και τον GLASS. Στόχος, σε πειραματικό επίπεδο της διπλωματικής μου εργασίας είναι αφενός η δέσμευση on demand ενός μονοπατιού σε ένα GMPLS/Optical δίκτυο και μετάδοση διαφορετικών ροών δεδομένων σε αυτό με τεχνικές multiplexing, και αφετέρου η σύγκριση υπαρχόντων μηχανισμών αποκατάστασης και επανάκτησης μετά από αστοχία σύνδεσης, η μελέτη της επιρροής του control plane failure στους QoS μηχανισμους κίνησης, καθώς και η δυναμική διαχείριση των μονοπατιών μετά από κατάρευση. Επιπλέον, παρουσιάζονται και νέοι βελτιωμένοι μηχανισμοί επανάκτησης στο πεδίο λειτουργικότητας ελέγχου και δεδομένων στα πλαίσια του ASONS Simulator στον ns–2. Συγκεκριμένα, προτείνεται ένας νέος link–delay constrainted αλγόριθμος ο οποίος λαμβάνοντας υπόψιν τον αριθμό των οπτικών συνδέσεων που διατρέχει κάθε σύνδεσμο, καθορίζει ένα πιό βέλτιστο και ασφαλές μονοπάτι προστασίας είτε πρίν (pre–planned protection), είτε μετά την πρόκληση της αστοχίας (dynamic restoration). Το αποτέλεσμα είναι η αύξηση του επιπέδου βιωσιμότητας – Resilience level στο δίκτυο, η μείωση πιθανότητας εμφάνισης νέων αστοχιών καθώς και του αριθμού των απωλεσθέντων πακέτων. Ο αλγόριθμος δοκιμάστηκε μέσω προσωμοιώσεων με

χρήση του προσωμοιωτή NS–2 και τα παραπάνω αποτελέσματα επιβεβαιώνονται και πειραματικά.

Στο κεφάλαιο 2 αναφερόμαστε στην ανάγκη μετάβασης στην νέα γενιά Intelligent Optical Networking για την υποστήριξη των προηγμένων πλέον telecom services, καθώς και στις διάφορες τεχνικές διαχωρισμού κίνησης απαραίτητες για τη μετάδοση πληροφοριών μεγέθους έως και Terabit/s. Επιπλέον, μελετώνται οι υπαρχοντες μηχανισμοί Traffic Shapping και Traffic Engineering, ενώ, τέλος, κλείνουμε με μια αναλυτική αναφορά στα προβλήματα κοινής πρόσβασης ετερογενών δικτύων κορμού καθώς και μεθόδους διαχείρισής τους, για να καταλήξουμε στο όραμα του Generalized σχετικά με την ενοποίηση του πεδίου λειτουργικότητας ελέγχου πάνω σε διαφορετικές backbone τεχνολογίες πρόσβασης.

Στο κεφάλαιο 3 ξεκινάμε με μια σύντομη παρουσίαση του προκατόχου του GMPLS, το MultiProtocol Label Switching (MPLS), καθώς και των βασικών του αρχιτεκτονικών χαρακτηριστικών απαραίτητων για την μετάβαση στο Generalized. Περνάμε έπειτα στο GMPLS framework όπου αναλύουμε εκτενώς την αρχιτεκτονική του, τα πεδία λειτουργικότητάς του, αλγόριθμους δρομολόγησης καθώς και τα σχήματα αποκατάστασης μετά από αστοχία. Κλείνοντας, αναφερόμαστε στον υπάρχοντα εμπορικό εξοπλισμό που υποστηρίζει το συγκεκριμένο πολυπρωτόκολλο, ενώ περιγράφουμε σενάρια υλοποίησής του σε πραγματικές συνθήκες, όπως στα πλαίσια του Ευρωπαικού προγράμματος AutoBAHN του GN2.

Στο κεφάλαιο 4 παρουσιάζουμε εντελώς συνοπτικά τους βασικότερους ανταγωνιστές του πρωτοκόλλου στα πλάισια τυποποιήσεων του ITU–T, ενώ αναφερόμαστε στις προοπτικές εξέλιξης του GMPLS τόσο σε ενσύρματα backbone δίκτυα, όσο και σε ασύρματες δικτυακές υποδομές.

Στο κεφάλαιο 5 γίνεται περιγραφή των πειραματικών μετρήσεων στα πλαίσια της διπλωματικής αυτής εργασίας και στους δύο δικτυακούς προσωμοιωτές που αναφέραμε, παρουσίαση των τοπολογιών καθώς και σχετικών συνθηκών που χρησιμοποιήθηκαν στα πλαίσια της εξομοίωσης.

Στο κεφάλαιο 6 αξιολογούνται τα αποτελέσματα των πειραματικών μετρήσεων και παρουσιάζονται τα συμπεράσματα της διπλωματικής εργασίας.

Στο κεφάλαιο 7 παρουσιάζεται ο νέος link–delay constrainted αλγόριθμος αποκατάστασης. Με βάση, τώρα, τον μηχανισμό λειτουργίας του υλοποιούνται και αξιολογούνται βελτιωμένοι μηχανισμοί προστασίας και αποκατάστασης στο πεδίο λειτουργικότητας δεδομένων του GMPLS, στα πλαίσια του περιβάλλοντος προσωμοίωσης του ns–2. Τέλος αναλύονται και τα συμπεράσματα από την χρήση του μηχανισμού αυτού.

Στο Κεφάλαιο 8 , τέλος, παρουσιάζονται η βιβλιογραφία και οι σχετικοί δικτυακοί τόποι που αναφέρονται στη διπλωματική αυτή εργασία.

ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΣΥΝΕΔΡΙΑ:

An Improved GMPLS Survivability Mechanism Using Link Delay – Constrained Algorithm

International Conference on Data Communication Networking - DCNET 2011, Seville, Spain, A. Bikos, C. Bouras, K. Stamos, July 18-21 2011, pp. 45 – 50

http://ru6.cti.gr/ru6/publications/4685DCNET_2011_2_CR.pdf

ΚΕΦΑΛΑΙΟ 2: ΑΠΑΙΤΗΣΗ ΓΙΑ ΕΝΟΠΟΙΗΣΗ ΤΩΝ BACKBONE ΑΡΧΙΤΕΚΤΟΝΙΚΩΝ ΣΤΑ ΠΕΔΙΑ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ

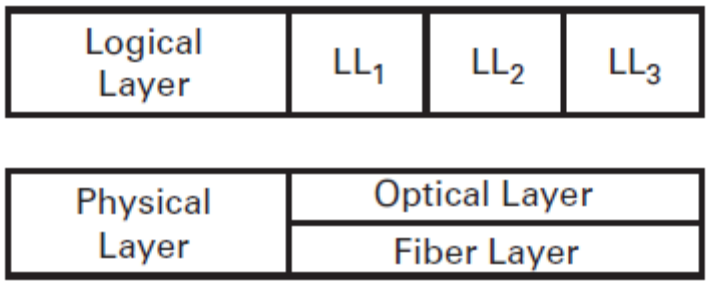
2.1.1 Η ΑΝΑΓΚΗ ΓΙΑ ΟΠΤΙΚΑ ΔΙΚΤΥΑ:ΣΥΓΚΡΙΣΗ OPTICAL ΚΑΙ ELECTRONIC SWITCHING

Τα επόμενης γενιάς δίκτυα κορμού – IP Core/Backbone networks, δηλαδή το σύνολο εκείνων των επικοινωνιακών υποδομών που ανταλλάσουν τη μαζικότερη κίνηση ανάμεσα σε κεντρικούς κόμβους και σημεία πρόσβασης, οφείλουν να πληρούν ορισμένες βασικές προυποθέσεις απόδοσης και αξιοπιστίας. Μερικές από αυτές είναι η αυξημένη συνδεσιμότητα με δυνατότητα υποστήριξης παράλληλων γραμμών, υψηλή χωρητικότητα και ταχύτητα με χαμηλό ποσοστό σφάλματος, ευκολία κλιμάκωσης και ολοκληρωμένους μηχανισμούς διαχείρισης και ανάκαμψης μετά από αστοχία. Οι Backbone ISP's –Internet Service Providers αναζητούν πιό αποτελεσματικές, ευέλικτες και υψηλότερης κλιμάκωσης λύσεις μεταφοράς δεδομένων ώστε να καλύψουν τις συνεχώς αυξανόμενες απαιτήσεις στο εύρος ζώνης κορμού εξαιτίας της εμφάνισης νέων IP εφαρμογών και υπηρεσιών, όπως B2B, B2C, broadband multimedia και content distribution. Επιπρόσθετα τα οικονομικά βιώσιμα και σύγχρονα δίκτυα κορμού ειναι υποχρεωμένα να παρέχουν υποστήριξη για μεταφορά υπηρεσιών της τάξης των 2.5 Gbit/s, 10 Gbit/s, 40 Gbit/s και σύντομα των 100 Gbit/s. Έχει παρατηρηθεί μάλιστα οτι ειδικά τα Internet Backbones χτίζονται με τέτοιο ραγδαίο ρυθμό, ώστε πολλαπλασιάζουν το απαιτούμενο bandwidth 2 ως και 10 φορές το χρόνο. Τέλος εξαιτίας του ιστορικού διαχωρισμού μεταξύ δικτύου πρόσβασης και δικτύου κορμού δημιουργείται σοβαρό αντίκτυπο σε μεγάλο αριθμό τελικών χρηστών στις περιπτώσεις των αστοχίων δικτύου –network failures, ενώ αυξάνονται τόσο η πολυπλοκότητα όσο και οι προκλήσεις μιας ενιαίας διαχείρησης της υποδομής.

Οι οπτικές ίνες μπορούν αναμφισβήτητα να θεωρηθούν ως ένας απο εκείνους τους μηχανισμούς που ικανοποιούν τις προηγούμενες απαιτήσεις καθώς και ένα εξαιρετικό μέσο μετάδοσης εξαιτίας προηγμένων ιδιοτήτων όπως:χαμηλή απόσβεση, τεράστιο εύρος ζώνης και ανοχή στις ηλεκτρομαγνητικές παρεμβολές. Μέσω εξελιγμένων τεχνικών πολυπλεξίας κίνησης όπως WDM –Wavelength Division Multiplexing, γρήγορα καθιερώθηκαν σαν πρότυπο για συνδέσεις υψηλής χωρητικότητας πρώτα σε optical point–to–point επίπεδο και ύστερα σε μορφή All–optical networks. Έτσι σαν αποτέλεσμα οι οπτικές/φωτονικές τεχνολογίες αλλάζουν διαρκώς κάθε τομέα των δημόσιων δικτυακών υποδομών και ιδιαίτερα αυτών των δικτύων κορμού. Πλέον ο μελλοντικός εξοπλισμός των IP Core δικτύων θα επιτρέπει την ιεραρχηση του συνολικού εύρους ζώνης να γίνεται πιό έγκαιρα, αφαιρώντας τα όποια επίπεδα προκαλούσαν καθυστέρηση, όπως το ATM aggregation layer, συνεισφέροντας έτσι στην δημιουργία μιας αρχιτεκτονικής δικτύου υψηλής κλιμάκωσης δυο επιπέδων. Το δίκτυο μεταφοράς αποτελούμενο από Dense WDM –DWDM τεχνικές πολυπλεξίας και οπτικούς μεταγωγείς –optical cross–connects θα μεταφέρει terabits εύρους ζώνης το οποίο θα μπορεί να επεξεργάζεται αυτούσια στο routing layer. Νέες τεχνολογίες ηλεκτρονικής δρομολόγησης –electrical routing και οπτικής μεταγωγής –optical switching οδηγούν αυτή την ραγδαία εξέλιξη. Τα optical switches δουλεύουν με DWDM συστήματα ώστε να κάνουν διαθέσιμα προς επεξεργασία terabits πληροφορίας στους electrical routers, οι οποίοι με τη σειρά τους παρέχουν την υποδομή να δρομολογούν πακέτα μεταξύ οποιοδήποτε αποστελέα και παραλήπτη στο Διαδίκτυο. Αυτές οι δύο συμπληρωματικές ηλεκτρονικές και οπτικές τεχνολογίες αναμένεται σύντομα να συγκλίνουν σε ένα ενιαίο σύστημα.

Πιο συγκεκριμένα αναφερόμενοι σε ένα καθαρά οπτικό φυσικό επίπεδο, μέχρι αυτή τη στιγμή τουλάχιστον, υπάρχει πλήρης διαχωρισμός ανάμεσα στην οπτική/φωτονική τεχνολογία, από το ένα άκρο, και στην ηλεκτρονική, από το άλλο. Οι σταθμοί μέσα στο Optical Domain είναι υπεύθυνοι να προσφέρουν τις βασικές λειτουργίες όπως το να φωτίζουν τις ίνες με μήκη κύματος –lasers και να τις εξάγουν μέσω φωτοανιχνευτών. Όταν

τα σήματα είναι σε οπτική μορφή η υπάρχουσα οπτική τεχνολογία είναι επαρκής να πραγματοποιεί ορισμένες απλές λειτουργίες routing και switching μέσα στους κόμβους. Με τις φωτονικές συσκευές είναι σχετικά εύκολο , επίσης, να υλοποιηθούν τεχνικές υπέρθεσης, διαχωρισμού, φιλτραρίσματος, πολύπλεξης και απόπλεξης στο πεδίο της συχνότητας των οπτικών σημάτων. Από την άλλη ωστόσο, στο Electric Domain η πληροφορία ελέγχου που μεταδίδεται in–band (στο ίδιο κανάλι με τα δεδομένα) τόσο σε IP Packet Based ή ATM Cell Based networks, δεν μπορεί να χρησιμοποιηθεί όσο το σήμα είναι σε οπτική μορφή. Για το γεγονός αυτό το οπτικο φυσικό επίπεδο από μόνο του δε μπορεί να πραγματοποιήσει τις αναγκαίες λειτουργίες του packet–switching.



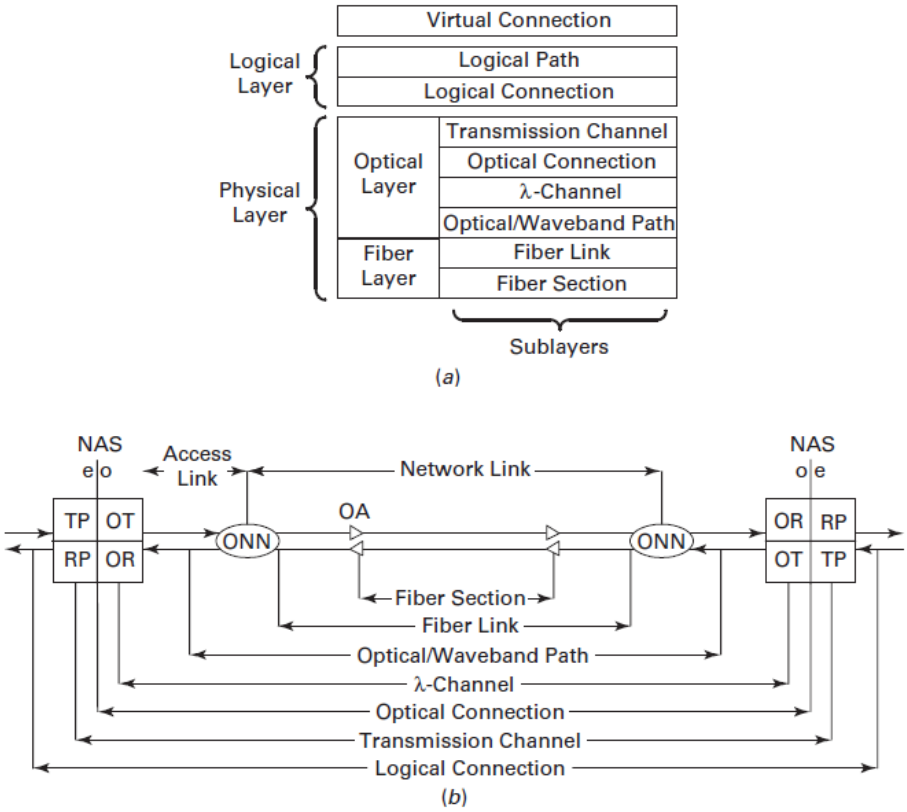
Εικόνα 1. Επιπεδοποιημένη –layered όψη ενός οπτικού δικτύου

2.1.2 Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΩΝ MULTILAYER ΟΠΤΙΚΩΝ ΔΙΚΤΥΩΝ

Με βάση την επιπεδοποιημένη προσέγγιση –layered view, ένα σύνθετο σύνολο απο συστατικά δικτύου καθώς και οι αλληλεπιδράσεις τους μπορούν να ειδωθούν σαν μια μικρότερη και ευκολότερα διαχειρίσιμη ιεραρχία επιπέδων. Όπως φαίνεται στην Εικόνα 1, υπάρχει σαφής διαχωρισμός μεταξύ του φυσικού –οπτικού επιπέδου και του λογικού –ηλεκτρονικού. Το μεν φυσικό στρώμα υποδιαιρείται στο Optical Layer, που περιλαμβάνει τις διασυνδέσεις των οπτικών ινών, και στο Fiber Layer, που αποτελείται απο τον φωτονικό εξοπλισμό όπως Switches, Optical Cross Connects, και φωτοανιχνευτές. Το λογικό στρώμα, από την άλλη, παρέχει τις λεγόμενες λογικές συνδέσεις –logical links ενώ είναι υπεύθυνο για όλες τις διαδικασίες routing και circuit switching, όπως τον καθορισμό εικονικών κυκλωμάτων –virtual circuits στη περίπτωση του ATM.

Για την καλλίτερη κατανόηση της προσέγγισης των οπτικών δικτύων πολλαπλών επιπέδων –multilayer παρουσιάζουμε το πιό σύνθετο σχήμα της Εικόνας 2.a. Όπως εξηγήθηκε προηγουμένως τα κατώτερα στρώματα –sublayers έχουν διακριτές και ανεξάρτητες λειτουργίες. Εαν θεωρήσουμε για παράδειγμα, σε υψηλότερο επίπεδο, ένα packet–cell switched δικτυο που αντιπροσωπεύει ενα ATM ή IP core network και που περιλαμβάνει υποχρεωτικά και ένα επίπεδο εικονικής σύνδεσης –virtual connection layer, τότε θα μπορούσε να ειπωθεί οτί το φυσικό στρώμα αποτελείται από δυο network clients:το IP δίκτυο και το IP over ATM over WDM. Ξεκινώντας από το φυσικό στρώμα της Εικόνας 2.a και έχοντας υπόψιν τις συνδέσεις σημείου–προς–σημείο της Εικόνας 2.b, παρατηρούμε οτι το όριο μεταξύ των Logical και Physical υποστρωμάτων είναι τα NAS–Network Access Stations. Ειναι εμφανές οτι τα στοιχεία αυτά λειτουργούν ως σύνορα

μεταξύ του Optical και Electric Domain. Έτσι από την οπτική μεριά συνδέονται μέσω μίας γραμμής πρόσβασης (που αποτελείται από ένα σύνολο από ζεύγη οπτικών καλωδιώσεων) με ένα ONN–Optical Network Node, ενώ από την ηλεκτρική με λογικές συνδέσεις δημιουργώντας έτσι τα λογικά μονοπάτια. Μια οπτική σύνδεση μπορεί να περιλαμβάνει οπτικούς ενισχυτές/αναγεννητές σήματος OA's–Optical Amplifiers στη πορεία της, ενώ διακρίνεται σε μονόδρομη (αν έχουμε κίνηση προς μία κατεύθυνση) και αμφρίδρομη(αν υπάρχει κίνηση και προς τις δύο κατευθύνσεις). Στο συγκεκριμένο σχήμα έχουμε ζεύγη μονόδρομων οπτικών ινών.



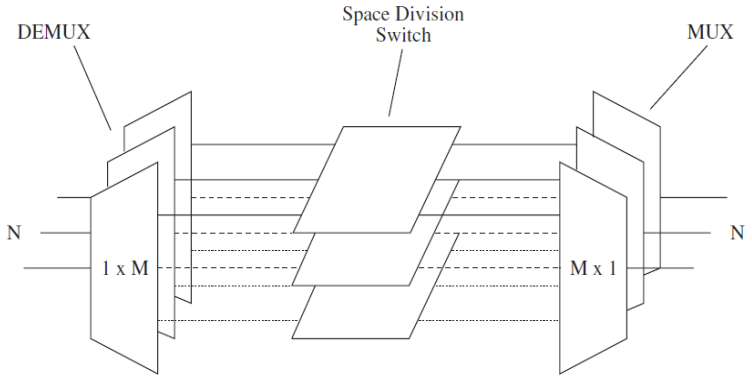
Εικόνα 2. Επιπεδοποιημένη –layered όψη οπτικών συνδέσεων

Οι πιο θεμελιώδεις ποσότητες στο κομμάτι του Optical layer domain είναι τα μήκη κύματος lambdas ή λ–channels. Είναι οι βασικότεροι φορείς πληροφορίας στο φυσικό στρώμα, ενώ γίνονται routed και switched μέσω τεχνικών πολυπλεξίας κίνησης από τα ONN's. Αφού εγκαθιδρυθεί το οπτικό μονοπάτι –optical path, το κανάλι μετάδοσης πραγματοποιεί λειτουργίες μετατροπής του λογικού σήματος σε σήμα μετάδοσης. Αυτή η διαδικασία εκτελείται στον Transmission Processor –TP του NAS ενώ η ανάποδη λειτουργία λαμβάνει χώρα στον Reception Processor –RP. Οι Optical Transmitters και Receivers –OT και –OR , τέλος, λειτουργούν σαν οπτικοί πομπο–δέκτες.

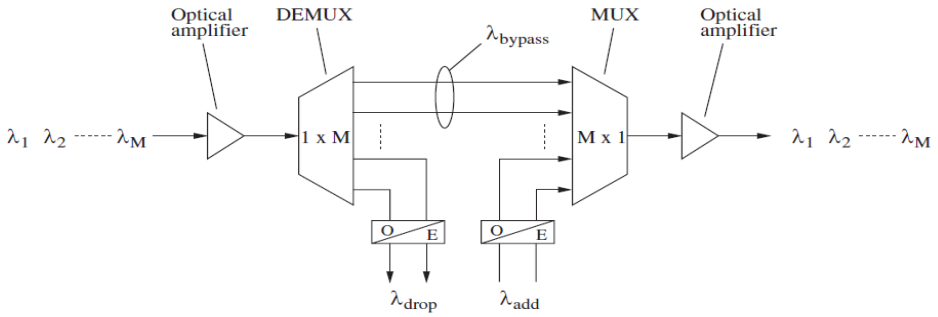
Να σημειώσουμε οτί στο ανώτερο επίπεδο των multilayer οπτικών δικτύων, δηλαδή στο Virtual Connection Layer, μια εικονική σύνδεση μεταξύ ενός ζεύγους συστημάτων μεταφέρεται πάνω σε ένα logical path –λογικο μονοπάτι που αποτελείται από δυο logical hops –LC's. Παρώτι πρόκειται για point–to–point συνδέσεις, τα ίδια ακριβώς μπορούν να επεκταθούν και σε optical multipoint γραμμές.

Τα Wavelength Division Multiplexing οπτικά δίκτυα αποτελούνται από οπτικές ίνες που κάνουν διαχωρισμό στο πεδίο της συχνότητας της μεταδιδόμενης πληροφορίας και που σαν αποτέλεσμα μπορούν να μεταφέρουν περισσότερα από ένα wavelength καναλια στο ίδιο οπτικο μονοπάτι. Τα οπτικά δίκτυα γενικότερα διακρίνονται σε E–O–E networks – Electronic–to–Optical–to–Electronic, οπού μεσολαβούν ενδιάμεσες μετατροπές από ηλεκτρική σε οπτική μορφή και αντίστροφα, όπως για παράδειγμα στο σχήμα της Εικονας 2b, και σε AON's –All Optical Networks, οπού δεν υπάρχει καμία οπτικο–ηλεκρονική μετατροπή και η κίνηση διατηρείται στο optical domain.

Στα AON's οι οπτικοί κόμβοι καλούνται Optical Add–Drop Multiplexers (OADM) και Optical Cross–Connects (OXC's), ενώ οι οπτικές point–to–point συνδέσεις καλούνται οπτικά μονοπάτια –lightpaths. Και οι δύο αυτές συσκευές παρέχουν μηχανισμούς προστασίας και παραμετροποίησης του δικτύου ώστε να ανταπεξέλθει στις αλλαγές του φόρτου κίνησης, και να ανακάμψει μετά από αστοχία γραμμής ή και κόμβου στο δίκτυο.



Εικόνα 3. Optical Cross–connect (OXC) με N οπτικές ίνες, οπού κάθε μια μεταφέρει M wavelengths



Εικόνα 4. Optical add–drop multiplexer (OADM) με 1 οπτική ίνα, οπού μεταφέρει M wavelengths

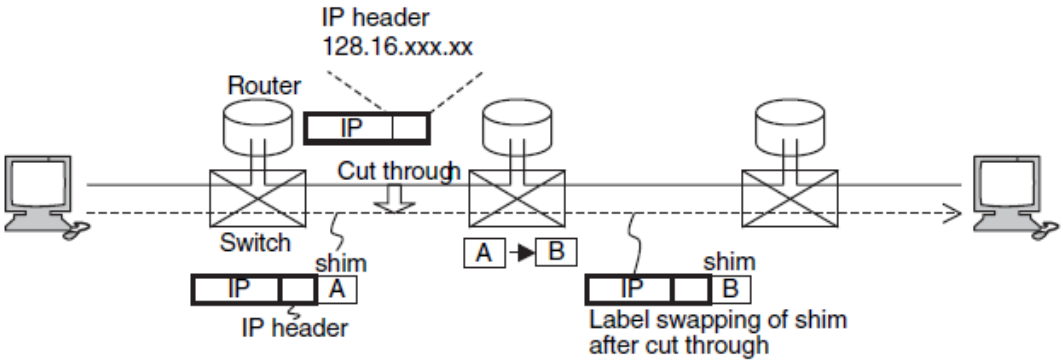
2.1.3 ΣΥΝΔΕΣΜΟΣΤΡΕΦΕΙΣ BACKBONE ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ATM

Το International Telecommunication Union (ITU) έχει επιλέξει τον ασύγχρονο τρόπο μεταφοράς –ATM (Asynchronous Transfer Mode) ως μία κυρίαρχη διαδικτυακή τεχνολογία γιά την υλοποίηση των broadband ενοποιημένων υπηρεσιών (B–ISDN), καθώς

και για μετάδοση δεδομένων τόσο πραγματικού χρόνου όσο και μη σε μία υπάρχουσα δικτυακή υποδομή. Κατά την αλληλεπίδραση του ATM με παραδοσιακά IP δίκτυα συναντάμε μηχανισμούς QoS και κλάσεις διαφοροποιημένων υπηρεσιών IP Diffserv, που καθιστούν την τεχνολογία αυτή ιδιαίτερα χρήσιμη για τις σημερινές απαιτήσεις στα broadband networks μιας και ένα από τα βασικότερα πλεονεκτήματα της ATM επικοινωνίας είναι τα εξαιρετικά Traffic Engineering χαρακτηριστικά της. Αυτό το πλαίσιο είναι απαραίτητο για την παιρετέρω βέλτιστη κατανόηση του MPLS πρωτοκόλλου και κατ'επεκτασιν του GMPLS.

Η βάση των τηλεπικοινωνιακών συστημάτων είναι η δημιουργία ενός μονοπατιού επικοινωνίας για την ανταλλαγή πληροφοριών. Υπάρχουν δύο τρόποι να εγκαθιδρυθεί ένα μονοπάτι:ο συνδεσμοστρεφής –connection–oriented και ο ασυνδεσμικός –connectionless. Η πρώτη μέθοδος είναι ανώτερη της δεύτερης καθώτι σε αυτήν γίνεται εγκατάσταση της σύνδεσης πριν την μετάδοση ή λήψη πληροφορίας, ενώ δεσμεύονται από πριν οι απαραίτητοι επικοινωνιακοί πόροι όπως bandwidth, κτπ. Έτσι διατηρείται ένα επιθυμητό επίπεδο ποιότητας επικοινωνίας. Στην άλλη περίπτωση ωστόσο η προς μετάδοση πληροφορία μετατρέπεται σε πακέτα, όπου το καθένα φέρει και μία διεύθυνση προορισμού, κάνοντας έτσι στα πακέτα αυτά, ταξιδεύοντας στο δίκτυο, να πραγματοποιούνται αποφάσεις δρομολόγησης σε κάθε κόμβο του. Η δευτερη περίπτωση μοίαζει με τη διακίνηση των γραμμάτων του ταχυδρομείου, ενώ η πρώτη με το τηλέφωνικό σύστημα. Ο connection–oriented μηχανισμός χρησιμοποιείται κατεξοχήν στο ATM, ενώ οι connectionless επικοινωνίες εφαρμόζονται στο παραδοσιακό IP packet forwarding των IP δικτύων όπως το Internet.

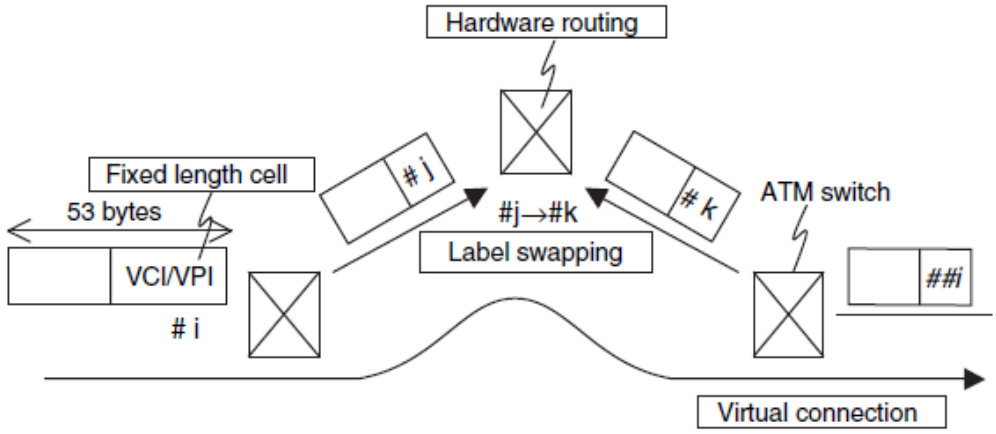
Η MPLS επικοινωνία συνδυάζει τα χαρακτηριστικά και την λειτουργικότητα και των δύο τύπων IP μετάδοσης:ATM και IP, όπως φαίνεται και στην εικόνα 5. Συγκεκριμένα όπως παρατηρούμε και στο σχήμα μεταξύ των δύο απομακρυσμένων κόμβων μεσολαβούν διάφοροι δρομολογητές και switches. Οι μεν Routers κάνουν, μέσω των έντονων χρωματισμένα γραμμών μετάδοσης, το παραδοσιακό IP Forwarding στα μεταδιδόμενα πακέτα, δηλαδή hop–by–hop μεταφορά βάση της διεύθυνσης προορισμού τους, ενώ αντίθετα τα switches , στις διακεκομμένες γραμμές, πραγματοποιούν την τεχνική του **Label Swapping:** Σε μία ροή κίνησης IP πακέτων, οπού είναι ευκολότερο να μεταχειρίζεται συνολικά ειδικά εαν διαθέτει μία μοναδική διεύθυνση προορισμού για πολλά πακέτα, εισάγεται στον ingress –σημείου εισόδου switch (label switch router) μια ετικέτα label με ένα ζεύγος από μία διεύθυνση αποστολής και μια προορισμού, ενω η ίδια ετικέτα αφαιρείται στον egress –σημείου εξόδου switch. Η μεταφορά εκτελείται με απλή μεταγωγή ετικέτας –label swapping (A B), μέσω της τεχνικής του **cut–through**. Σε αυτήν τη τεχνική μόλις φθάσει το IP header του επόμενου προορισμού –και όχι ολόκληρο το πακέτο ακόμη, γίνεται label swapping, ενώ τα πακέτα στο MPLS δίκτυο μεταδίδονται από ένα μόνο μονοπάτι το οποίο είναι δυνατόν να επιλεγεί ρητά –**explicit route**. Το πλεονέκτημα του (connection–oriented) cut–through αντί του παραδοσιακού (connectionless) store–and–forward είναι η παροχή επαρκούς εύρους ζώνης ώστε το δίκτυο να εγγυηθεί μία δεδομένη ποιότητα υπηρεσιών QoS –Quality Of Service, μιας και στο IP Forwarding κάτι τέτοιο δεν είναι εφικτό λόγω του ενδεχομένου τα πακέτα να ακολουθήσουν διαφορετικά μονοπάτια.



Εικόνα 5. Βασικός Μηχανισμός του MPLS

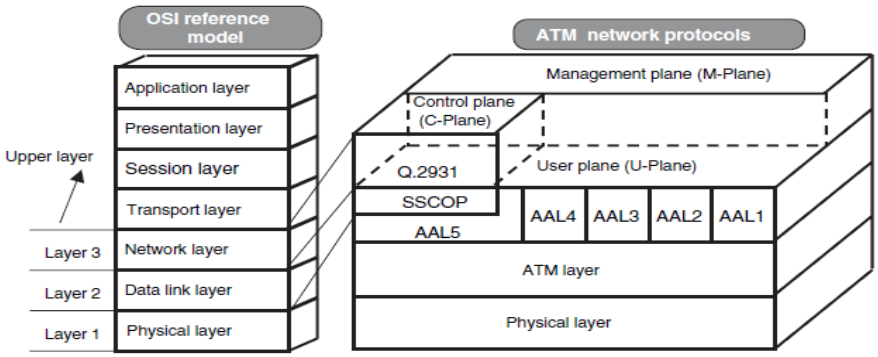
Παρατηρούμε επομένως οτί το ATM αποτελεί τον συνδεσμοστρεφή μηχανισμό μεταφοράς του πρωτοκόλλου MPLS. Πιο συγκεκριμένα το MPLS εκτελεί IP Forwarding ως την αρχική διαδικασία μετάδοσης, και ειδικότερα στην εγκαθίδρυση του νοητού μονοπατιού –virtual connection, καθώτι οι διευθύνσεις του αποστολέα και παραλήπτη πρέπει να είναι εκ των προτέρων γνωστές, ενώ στην συνέχεια κάνει cut–through μέσω του label–swapping για λόγους αποφυγής συμφόρησης στο δίκτυο, μέσω επιλογής διαφορετικών μονοπατιών.

Εξετάζοντας μάλιστα συνοπτικά την αρχιτεκτονική του ATM, παρατηρούμε οτί έχει όντως και από τη σειρά της αρκετά κοινά με τη φιλοσοφία του MPLS. Αρχικά εγκαθιδρύεται και εδώ ένα νοητό μονοπάτι το οποίο μεταφέρει πακέτα μέσω της εναπόθεσης μίας VCI/VPI ετικέτας –Virtual Channel Identifier/Virtual Path Identifier στην επικεφαλίδα του ATM. Πακέτα ή κυψέλες σταθερού μήκους 53 bytes χρησιμοποιούνται για τη μετάδοση της πληροφορίας, ενώ κάθε ATM κόμβος πραγματοποιεί αποφάσεις δρομολόγησης βάση της εκάστοτε VPI/VCI κατάστασης. Η διαδικασία αυτή του VPI/VCI relaying μοιάζει σε μεγάλο βαθμό με το label swapping στο MPLS, όπως φαίνεται και την εικόνα 6.



Εικόνα 6. Βασικός Μηχανισμός του ATM

Ενδεικτικά αναφέρουμε οτι το ATM δικτυακό πρωτόκολλο αποτελείται πέρα από τα επίπεδα OSI από τρία ανεξάρτητα πεδία λειτουργικότητας:user plane, control plane και management plane. Το πρώτο πραγματοποιεί μετάδοση των δεδομένων του χρήστη, το δεύτερο παρέχει συνδέσεις ελέγχου, ενώ το τελευταίο συντονίζει όλα τα layers και προσφέρει λειτουργίες διαχείρησης.



Εικόνα 7. ATM Αρχιτεκτονική

Όπως αναφέρθηκε το ATM διαθέτει διάφορους μηχανισμούς γιά την υποστήριξη QoS εγγύησεων μεταξύ τελικών χρηστών. Όταν εγκαθιδρύεται μία μία ATM σύνδεση, ο χρήστης και το δίκτυο συμφωνούν να τηρήσουν ένα συμβόλαιο κίνησης –traffic contract, το οποίο αποτελείται από δύο μέρη:τον traffic descriptor, που περιγράφει τα χαρακτηριστικά κίνησης τα οποία ο χρήστης οφείλει να ικανοποιεί, και τον QoS descriptor που περιλαμβάνει τις QoS εγγυήσεις που οφείλει να ικανοποιεί το δίκτυο για τη συγκεκριμένη σύνδεση(Εικόνα 8). Τα πιο ενδεικτικά από το πρώτο μέρος είναι τα εξής:

Peak Cell Rate (PCR): Το PCR ορίζει το μέγιστο ρυθμό με τον οποίο η πηγή μπορεί να στέλνει κυψέλες στο δίκτυο στη συγκεκριμένη σύνδεση.

Sustainable Cell Rate (SCR): Το SCR ορίζει το άνω όριο του μέσου ρυθμού αποστολής κυψέλης στο δίκτυο. Εαν ο μέσος αυτός ρυθμός ξεπερνάει το SCR η πηγή θα παραβιάζει τότε το συμβόλαιο κίνησης.

Minimum Cell Rate (MCR): Το MCR ειναι ο ελάχιστος ρυθμός κυψελών πού ζητείται από το δίκτυο.

Maximum Burst Size (MBS): Το MBS είναι ο μέγιστος αριθμός κυψελών που μπορούν να σταλούν πίσω στο μέγιστο ρυθμό.

Maximum Frame Size (MFS): Το MFS είναι το μέγιστο μέγεθος ενός frame που μεταδίδεται στο ATM.

Από το δεύτερο μέρος τηρούνται οι ακόλουθοι QoS παράμετροι:

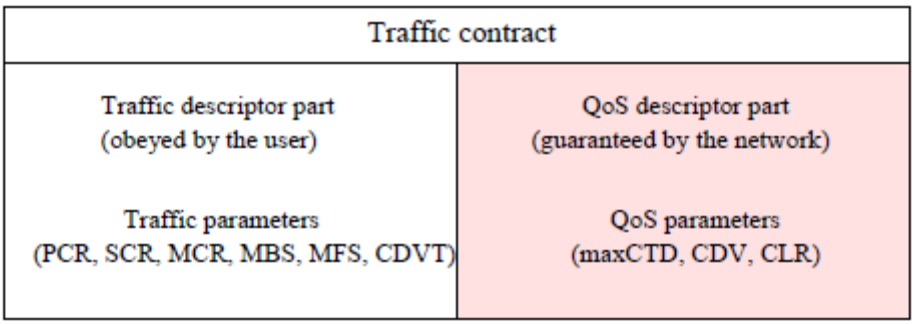
Maximum Cell Transfer Delay (maxCTD): Είναι ο μέγιστος χρόνος που δαπανάται από μία κυψέλη στο δίκτυο εξαιτίας των όποιων καθυστερήσεων όπως propagation, switching, και queuing delays.

Cell Delay Variation (CDV): Είναι η διαφορά ανάμεσα στη καλλίτερη και χειρότερη περίπτωση του CTD.

Cell Loss Ratio (CLR): Είναι το ποσοστό των απωλεσθέντων προς τις συνολικές κυψέλες.

Παράλληλα σε συνδυασμό με την υποστήριξη 5 διαφορετικών service classes όπως: Constant Bit Rate **(CBR),** Variable Bit Rate **(VBR),** Available Bit Rate **(ABR),** Unspecified Bit Rate **(UBR)** , και Guaranteed Frame Rate **(GFR)**, το ATM μέσω του υποεπιπέδου προσμαρμογής ATM AAL–ATM Adaptation Layer, το οποίο επιτρέπει σε οποιοδήποτε πρωτόκολλο ή υπηρεσία να συνδέεται με τη συγκεκριμένη τεχνολογία, παρέχει 4 επίπεδα υπηρεσιών για την κάλυψη διαφορετικών κάθε φορά απαιτήσεων όπως καθυστέρησης, διαμεταγωγής, και χρονισμού. Αυτά είναι τα:

- AAL1 για μεταδόσεις σταθερού ρυθμού όπως η 64 Kbps φωνή.
- AAL2 για μετάδοση μεταβλητού ρυθμού πληροφορίας όπως video MPEG–2
- AAL3/4 για μετάδοση πληροφορίας από συνδεσμοστρεφή packet–switched δίκτυα.
- AAL5 για υποστήριξη connectionless μεταφορών, όπως TCP/IP



Εικόνα 8. ATM QoS

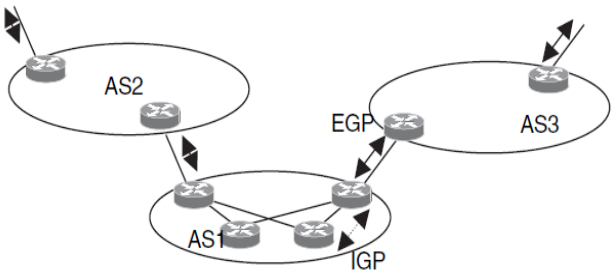
Τελος αναφέρουμε ενδεικτικά οτι εξαιτίας διαφόρων περιπτώσεων ασυμβατότητας ανάμεσα στα δίκτυα IP και ATM όσον αφορά στις αντιστοιχήσεις –mappings των QoS χαρακτηριστικών που αναφέρθησαν, το πρωτόκολλο Multiprotocol Label Switching (MPLS) παρουσιάζεται , όπως θα δούμε και στη συνέχεια, πιό ελκυστικό γιά την υποστήριξη QoS και Diffserv πάνω σε ATM και IP δίκτυα.

2.1.4 ΤΟ INTERNET PROTOCOL (IP)

Όπως αναφέρθηκε και στην προηγούμενη ενότητα το MPLS συνδυάζει στην επικοινωνία του δύο τύπους IP μεταφοράς –ATM και IP– , οπού ο μεν πρώτος είναι συνδεσμοστρεφής και ο δεύτερος ασυνδεσμικός. Με αυτό το τρόπο καταφέρνει να αποκτά τα πλεονεκτήματα και των δύο τύπων, όπως καθορισμό πολιτικών κίνησης –Traffic Engineering στις συνδέσεις, καλλίτερη υποστήριξη broadband υπηρεσιών και εξοικονόμηση εύρους ζώνης, απο τη μεριά του ATM, ενώ εξασφαλίζει την αξιοπιστία και ευρωστία στο δίκτυο μέσω μιας αυτόνομα κατανεμημένης διαχείρησης και ελέγχου, από τη μεριά του IP. Εξετάζοντας συνοπτικά το Internet Protocol (IP) παρατηρούμε οτι είναι ένα επιπέδου 3 πρωτόκολλο που αποτελείται από ένα IP forwarding πρωτόκολλο προώθησης και ένα IP routing πρωτόκολλο δρομολόγησης. Το πρώτο δημιουργεί έναν πίνακα δρομολόγησης, ενώ το δεύτερο μεταδίδει τα IP πακέτα σύμφωνα με αυτό τον πίνακα.

Στο IP layer, ένας κόμβος μέσα στο δίκτυο καλείται δρομολογητής –router. Τα πακέτα ταξιδεύουν στο δίκτυο ανάμεσα στους δρομολογητές hop–by–hop δηλαδή από κόμβο σε κόμβο. Ο router δε χρειάζεται να γνωρίζει όλη τη πληροφορία δρομολόγησης μέχρι τη διεύθυνση προορισμού. Το μόνο που αρκεί είναι ποιοι γειτονικός δρομολογητής είναι ο πλησιέστερος έτσι ώστε να του προωθήσει τα αντίστοιχα πακέτα. Με αυτό το τρόπο στη παγκόσμια κλίμακα του Internet τα IP πακέτα μεταφέρονται στην διεύθυνση προορισμού τους. Κάθε δρομολογητής εκτελεί το hop–by–hop routing βάσει ενός πίνακα προώθησης –forwarding table. Ο πινακας αυτός περιέχει πεδία όπως (1) διεύθυνση προορισμού, (2) IP διεύθυνση του επόμενου γειτονικού κόμβου, (3) ένα network interface number για κάθε καταχώρηση. Η αναζήτηση στον πίνακα προώθησης γίνεται βάσει της διευθυνσης προορισμού η οποία χρησιμοποιείται ως κλειδί. Αν αντί της κλασσικής διευθυνσιοδότησης με κλάσεις , όπου χρησιμοποιώντας πολλαπλές διευθύνσεις class C δημιουργείται το πρόβλημα της περιττής αύξησης καταχωρήσεων στα routing tables, κάνουμε χρήση της CIDR –Classless Interdomain Routing τεχνικής, τότε πολλαπλές IP διευθύνσεις ενοποιούνται σε ένα ενιαίο πίνακα δρομολόγησης μέσω της χρήσης προθέματος –prefix και μιας 32–bit μάσκας δικτύου. Η διεύθυνση του επόμενου hop στα IP routing tables προσδιορίζεται μέσω της longest–prefix matching μεθόδου, βάσει της οποίας εκτελείται ένα λογικό AND ανάμεσα στη διεύθυνση προορισμού του αφιχθέντος IP header και της μάσκας δικτύου bit με bit, και λαμβάνεται η καταχώρηση που ταιριάζει στα περισσότερα δυαδικά ψηφία. Μάλιστα με την αύξηση των καταχωρήσεων στους πίνακες δρομολόγησης εισάγονται νέες μέθοδοι αναζήτησης όπως το 'Patricia tree', που είναι ένα είδος δυαδικού δέντρου.

Από την οπτική γωνία τώρα του IP Routing, που θα μας απασχολήσει περισσότερο στα πλαισια της εργασίας, είναι προφανές οτι ειδικά για μεγάλα δίκτυα όπως το Internet, δεν είναι πρακτικό αλλά και εφικτό να δημιουργούμε έναν πίνακα δρομολόγησης οπού θα υπάρχει μια μόνο κεντρική διαχείρηση της διεύθυνσης προορισμού. Γι αυτό το λόγο αναπτύχθηκε ένα routing protocol ως ένας μηχανισμός δημιουργίας πίνακα δρομολόγησης αυτόνομα και κατανεμημένα. Το πρωτόκολλο αυτό δημιουργεί καταρχήν ένα routing table το οποίο αλλάζει και προσαρμόζεται δυναμικά ανάλογα με τις αλλάγες στο δίκτυο, και έπειτα ένα πίνακα προώθησης γιά τη μεταφορά των IP πακέτων. Εξετάζοντας τα routing πρωτόκολλα ως προς την ιεραρχία τους, παρατηρούμε καταρχήν οτί σε κάθε Αυτόνομο Σύστημα –Autonomous System που αποτελεί και ένα ξεχωριστό domain δικτύου, αυτα διακρίνονται σε inside–AS και ονομάζονται IGP –Interior Gateway Protocols, και σε inter–AS που καλούνται EGP –Exterior Gateway Protocols.



Εικόνα 9. IGP και EGP

Οι συνοριακοί δρομολογητές των γειτονικών AS ανταλλάσουν πληροφορίες δρομολόγησης χρησιμοποιώντας το EGP. Εσωτερικά σε ένα AS γινεται χρήση του IGP. Συγκεκριμένα το IGP είναι ένα πρωτόκολλο δρομολόγησης που δημιουργεί ένα routing table μέσα σε ένα AS, βάσει του οποίου τα IP πακέτα μεταδίδονται στο προορισμό τους ακολουθώντας το συντομότερο μονοπάτι. Τυπικά τέτοια πρωτόκολλα είναι τα RIP, IGRP, OSPF, IS–IS (Intermediate System to Intermediate System) κτπ. Το πιό δημοφιλές EGP protocol είναι το BGP–4 (Border Gateway Protocol).

Ανάλογα με τη λειτουργία τους τα routing protocols διακρίνονται σε:

Distance vector Αναζήτηση του επόμενου hop στο συντομότερο μονοπάτι μέσω της ανταλλαγής ενός distance–vector πινακα. Χρησιμοποιείται ο αλγόριθμος Bellman–Ford. Παράδειγμα είναι τα RIP, IGRP.

Path Vector Επιλογή του μονοπατιού με το μικρότερο μήκος και ταυτόχρονη αποφυγή routing loop μέσω ανταλλαγής ενός path vector πίνακα.

Link State Κάθε κόμβος περιέχει πληροφορία τοπολογίας για γειτονικούς κόμβους. Ο υπολογισμός του συντομότερου μονοπατιού γίνεται με την ανταλλαγή link states με τις συγκεκριμένες πληροφορίες.

Το δημοφιλέστερο ίσως Link State πρωτόκολλο είναι το OSPF –Open Shortest Path First. Έχοντας τυποποιηθεί απο τον IETF το 1998, κατόρθωσε να αντικαταστήσει γρήγορα το RIPv2 και σήμερα εφαρμόζεται σε όλες τις μεγάλες IP υποδομές με σκοπό τη παιρετέρω μείωση του κόστους δρομολόγησης. Κάθε OSPF δρομολογητής διατηρεί μία ταυτοτική βάση δεδομένων που περιγράφει τη τοπολογία του αυτόνομου συστήματος. Από αυτή τη τοπολογία υπολογίζεται ένας πίνακας δρομολόγησης με τη κατασκευή ενός δέντρου συντομότερου μονοπατιού. Το OSPF επαναπροσδιορίζει γρήγορα τα μονοπάτια στα όποια ενδεχόμενα αλλαγών της τοπολογίας, ελαχιστοποιώντας έτσι το επιπλέον φορτίο της routing κίνησης, και διασφαλίζοντας την δρομολόγηση. Επιπλέον έχει επιλεγεί για το GMPLS με σκοπό την υλοποίηση Traffic Engineering λειτουργιών χρησιμοποιώντας Link State Advertisements –LSA's.

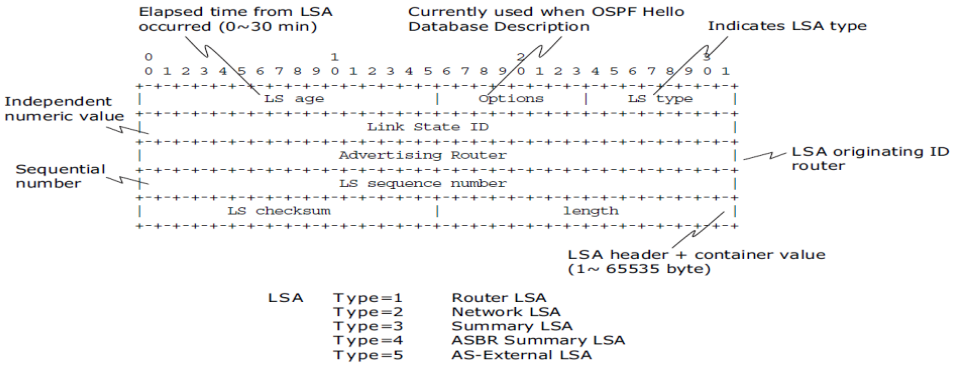
Το OSPF υπολογίζει το συντομότερο μονοπάτι από τη πηγή στο προορισμό κάνοντας χρήση του αλγορίθμου **Dijkstra**. Συνοπτικά ο αλγόριθμος λειτουργεί ως εξής:Πρώτα αναζητά το κόμβο με το χαμηλότερου κόστους μονοπάτι, έπειτα αναζητά και βρίσκει τον επόμενο με την ίδια ιδιότητα μέχρι να καταλήξει στο προορισμό. Αυτό επαφίεται γιά το κόμβο, κάθε φορά, που έχει το μικρότερο κόστος ανάμεσα σε όλους τους υπόλοιπους που φθάνουν στον ίδιο κόμβο–προορισμό. Η διαδικασία αυτή επαναλαμβάνεται μέχρι να έχουν δοκιμαστεί ολά τα hops. Απο προηγουμένως όμως το OSPF έχει ήδη 'πλημμυρίσει' –κάνει flooding το δίκτυο με τα LSA's με σκοπό τη δημιουργία της βάσης δεδομένων της τοπολογίας. Πιο συγκεκριμένα το link state εκφράζει τη πληροφορία των συνδέσμων που εκτείνονται από έναν router. Ο δρομολογητής που κάνει flooding τα link states στο δίκτυο καλείται LSA router. Κατά τη διάρκεια της διαδικασίας αυτής τα link–state packets αποστέλονται απο τον LSA router σε όλους τους γειτονικούς του routers. Επειδή όμως συχνές αλλαγές της τοπολογίας δημιουργούν την ανάγκη να αναγνωρίζονται τα πιο πρόσφατα link states, ο LSA router εισάγει ένα sequence number σε αυτά και κάνει flooding στη συνέχεια. Οι υπόλοιποι δρομολογητές αποδέχονται τα πακέτα με το μεγαλύτερο sequence number ως τα πιο πρόσφατα link states.

```
DIJKSTRA (G,s) /* for the single source shortest paths problem */
 1.  do for every v ∈ V
 2.     d[v] = ∞, π[v] = NIL
 3.  d[s] = 0
 4.  L = 0, U = V
 5.  do while U! = 0
 6.     u = EXTRACT_MIN_KEY_ENTRY(U)
 7.     L = L + u
 8.     do for each arc a(u, v) ∈ Originating[u] /* Originating[u] = arcs originating from vertex u */
 9.     if v∈U && d[v] > d[u] + w(a)
10.     then d[v] = d[u] + w(a), π[v] = u, DECREASE_ENTRY_KEY(U, v)
```

Εικόνα 10. Ο Αλγόριθμος Dijkstra

Σε ένα OSPF δίκτυο το ίδιο link state μπορεί να παραμείνει σε αυτό μέχρι να ξεπεράσει κάποιο προκαθορσμένο χρονικό όριο. Εαν δεν υπάρχει καμία αλλαγή στο περιεχόμενο του LSA μέσα σε αυτό το χρονικό διάστημα, τότε αυτό ανανεώνεται και αποστέλλεται ξανά, ενώ το sequence number αυξάνεται κατά 1. Προκαθορισμένα ένα link state διαφημίζεται κάθε 30 λεπτά. Εάν μετά από 1 ώρα δεν έχει ανανεωθεί, διαγράφεται από τη βάση δεδομένων του router.

Τέλος στο σχήμα 10 παρουσιάζεται ενδεικτικά η δομή ενός LSA header. Αυτό αποτελείται από πεδία όπως: LS age και LS sequence number (χρησιμοποιούνται για λόγους συγχρονισμού), LS type (περιγράφει το τύπο του LSA: type 1 για router LSA, type 2 για network LSA), link state ID.



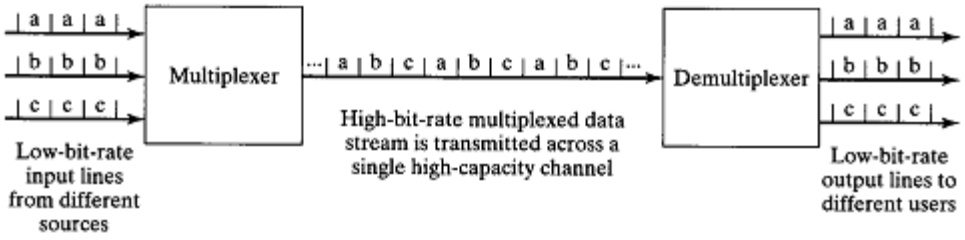
Εικόνα 11. LSA Header

2.1.5 ΤΕΧΝΙΚΕΣ ΠΟΛΥΠΛΕΞΙΑΣ ΚΙΝΗΣΗΣ ΣΤΑ MULTILAYER ΟΠΤΙΚΑ ΔΙΚΤΥΑ

Δεδομένης της τεράστιας χωρητικότητας των οπτικών ινών, όπως εξετάσαμε στην ενότητα 1. 1. 1, είναι απίθανο ένας μονο χρήστης ή κάποια εφαρμογή να απαιτήσει ολόκληρο το προσφερόμενο bandwidth. Αντίθετα, η όλη κίνηση στο δίκτυο από πολλαπλές διαφορετικές πηγές θα πρέπει να διαμοιράζεται το συνολικό οπτικό εύρος ζώνης μέσω μηχανισμών πολυπλεξίας –multiplexing. Το Multiplexing είναι μία τεχνική που επιτρέπει πολλαπλές πηγές κίνησης να μοιράζονται ένα κοινό μέσο μετάδοσης. Στο πλαίσιο των οπτικών δικτύων, τρείς κυρίως multiplexing προσεγγίσεις επικρατούν για το διαμοίρασμα

του bandwidth των οπτικών ινών: (1) **time division multiplexing (TDM),** (2) **space division multiplexing (SDM),** και (3) **wavelength division multiplexing (WDM)**.

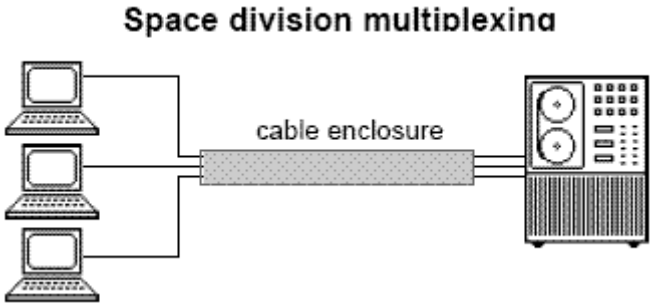
- **Time division multiplexing:** Το παραδοσιακό TDM είναι μία πολύ καταξιωμένη τεχνική και έχει χρησιμοποιηθεί κατ'εξοχήν σε ηλεκτρονικές διαδικτυακές αρχιτεκτονικές εδώ και περισσότερο από 50 χρόνια. Σε αυτό το τύπο πολυπλεξίας δύο ή περισσότερα σήματα από ροές bits μεταδίδονται ταυτόχρονα ως υποκανάλια σε ένα κανάλι επικοινωνίας, παίρνοντας σειρά μετάδοσης κάθε φορά στο κανάλι. Το πεδίο του χρόνου υποδιαιρείται σε αρκετά ταυτόχρονα timeslots καθορισμένου μήκους ένα για κάθε υποκανάλι. Ένα block δεδομένων από το υποκανάλι 1 μεταδίδεται κατα τη διάρκεια του timeslot 1, το υποκανάλι 2 από το timeslot 2, κτπ. Ένα TDM frame περιέχει ένα timeslot ανά υποκανάλι. Μετά τη μετάδοση του τελευταίου υποκαναλιού, ξεκινάει ξανά ο δεύτερος κύκλος με τη μετάδοση του δεύτερου block από το 1ο υποκανάλι, κτπ. Ενδεικτικά ο μηχανισμός φαίνεται στο σχήμα 13.



Εικόνα 12. Time Division Multiplexing

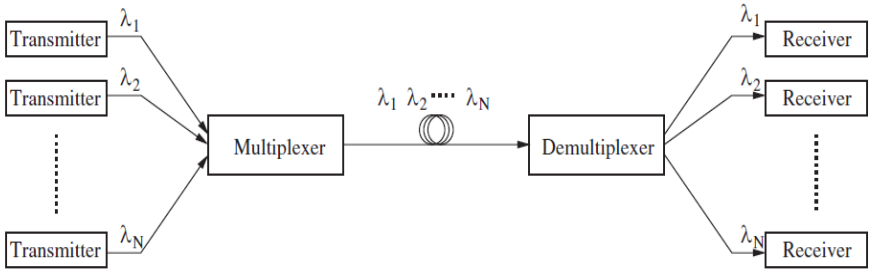
Το TDM ωστόσο αντιμετωπίζει σήμερα διάφορα προβλήματα οσον αφορά την πλήρη αξιοποίηση του τεράστιου εύρους ζώνης των δικτύων οπτικών ινών. Συγκεκριμένα ένα από αυτά είναι οτι το οπτικό TDM σήμα μεταφέρει την συνολική κίνηση από πολλαπλούς χρήστες και κάθε TDM κόμβος πρέπει να είναι ικανός να λειτουργεί στο συνολικό ρυθμό γραμμής παρά στο subrate που αντιστοιχεί σε κάθε υποκανάλι με το δικό του timeslot. Πρακτικά το συνολικό rate δε μπορεί να ανταποκριθεί σε μεγάλες τιμές αλλά περιορίζεται στις δυνατότητες της ηλεκτρονικής μετάδοσης και επεξεργασίας.

- **Space division multiplexing** Για την αποφυγή όποιων τέτοιων προβλημάτων στα πλαίσια πάντα των δικτύων οπτικών ινών, καθιερώνεται ο μηχανισμός SDM οπού πολλαπλές ίνες χρησιμοποιούνται παράλληλα αντί για μία μόνο. Κάθε μια από αυτές μπορεί να λειτουργεί σε οποιοδήποτε απαιτητικό, υποστηριζόμενο πάντα, ρυθμό μετάδοσης. Το SDM είναι επαρκές γιά μεταδόσεις μικρών αποστάσεων αλλά καθίσταται ασύμφορο οικονομικά για μεγαλύτερες αποστάσεις λόγω του κόστους εγκατάστασης παράλληλων γραμμών.



Εικόνα 13. Space Division Multiplexing

- **Wavelength division multiplexing** Το WDM εμφανίζεται ως η πιό πολλά υποσχόμενη τεχνική πολυπλεξίας κίνησης για τη βέλτιστη διαχείρηση του τεράστιου bandwidth των δικτύων οπτικών ινών αποφεύγοντας τα όποια προβλήματα που παρουσίαζαν οι δύο προηγούμενοι μηχανισμοί. Συγκεκριμένα το multiplexing εδώ μπορεί να θεωρηθεί ως ένα οπτικό frequency division multiplexing, οπού η κίνηση από κάθε client στέλνεται σε διαφορετικό φορέα συχνότητας. Οπως φαίνεται και στην εικόνα 14 στα οπτικά WDM δίκτυα κάθε transmitter i αποστέλνει μετάδοση σε ξεχωριστό μήκος κύματος λi. Στη μεριά της μετάδοσης ένας πολυπλέκτης μήκους κυματος συλλέγει όλα τα lambdas –μήκη κύματος και τα τροφοδοτεί σε μία και μόνο ίνα. Στη μεριά της λήψης γίνεται το αντίστροφο. Ένας αποπλέκτης κάνει το διαχωρισμό στα χρώματα και τα αποστέλει στους αντίστοιχους χρήστες. Σε αντίθεση , τέλος, με το SDM η πολυπλεξία μήκους κύματος δεν απαιτεί την τοποθέτηση παράλληλων γραμμών και άρα είναι πιό οικονομική για μεγάλες αποστάσεις.



Εικόνα 14. Wavelength Division Multiplexing

Το GMPLS όπως θα δούμε και στην συνέχεια εφαρμόζεται όχι μόνο στα παραδοσιακά packet–switched networks, αλλά κάνει ενοποιημένο switching στα πεδία του χρόνου (TDM) , της ίνας (SDM), και της συχνότητας (WDM), επομένως και optical switching.

2.2.1 ΔΙΑΦΟΡΟΠΟΙΗΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΠΟΛΙΤΙΚΕΣ ΚΙΝΗΣΗΣ

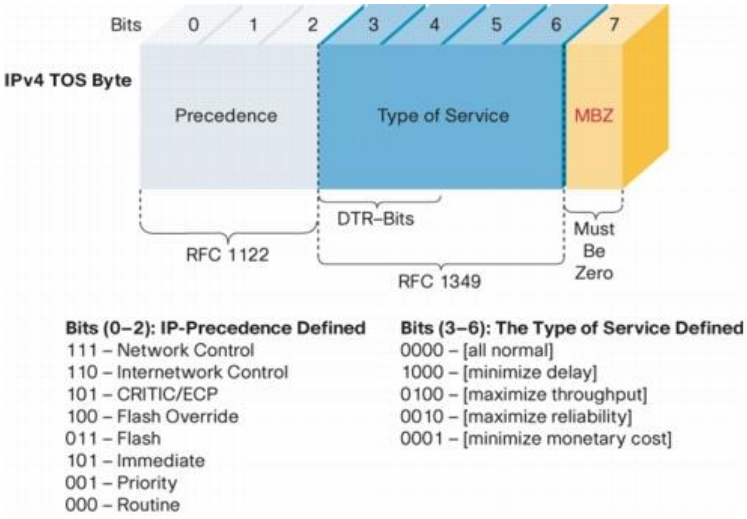
Η βασική επιτυχία του Internet στηρίζεται στο πρωτόκολλο IP. Το IP –Internet Protocol σχεδιάστηκε να προσφέρει best–effort υπηρεσίες για τη μετάδοση πακέτων δεδομένων και για να εκτελείται θεωρητικά σε κάθε διαδικτυακό μέσο και πλατφόρμα. Η αυξανόμενη δημοτικότητα του IP άλλαξε την αντίληψη του «IP over everything» σε «everything over IP». Για να διαχειριστεί την αυξανόμενη πολυπλοκότητα εφαρμογών όπως ροή βίντεο, Voice over IP (VoIP), e–commerce, Enterprise Resource Planning (ERP), και άλλα το δίκτυο απαιτεί Ποιότητα Υπηρεσιών –Quality of Service (QoS) σε συνδυασμό με best–effort υπηρεσίες. Διαφορετικές εφαρμογές έχουν κυμαινόμενες απαιτήσεις για καθυστέρηση, διακύμανση καθυστέρησης –jitter, εύρος ζώνης, απώλεια πακέτων και διαθεσιμότητα. Αυτές οι παράμετροι είναι η βάση του QoS. Το IP όφειλε, και τελικά κατάφερε, να σχεδιαστεί με βάση αυτά τα QoS constraints –χαρακτηριστικά.

Για την υλοποίηση μιας πραγματικής end–to–end QoS υπηρεσίας σε ένα IP–δίκτυο το IETF –Internet Engineering Task Force έχει ορίσει δύο μοντέλα:το Integrated Services (IntServ) και το Differentiated Services (DiffServ). Το πρώτο ακολουθεί το signaled–QoS μοντέλο, οπού οι τελικοί hosts σηματοδοτούν τις δικές τους QoS απαιτήσεις στο δίκτυο, ενώ το δεύτερο λειτουργεί στο provisioned QoS μοντέλο, όπου κάθε στοιχείο στο δίκτυο εγκαθιστά πολλαπλές κλάσεις υπηρεσιών κίνησης με κυμαινόμενα QoS χαρακτηριστικά. Το Diffserv συγκεκριμένα ικανοποιεί την απαίτηση της απλής και διευρημένης μεθόδου κατηγοριοποίησης κίνησης σε διαφορετικές κλάσεις, που καλούνται Class Of Service (CoS), και παράλληλα εφαρμόζει τις QoS παραμέτρους σε αυτές τις κλάσεις. Για την επίτευξη αυτής της απαίτησης τα πακέτα διαιρούνται σε κλάσεις με το μαρκάρισμα του Type of Service (ToS) byte στην IP επικεφαλίδα. Ένα 6–bit πεδίο (που καλείται Differentiated Services Code Point [DSCP]) στην IPv4 ToS οκτάδα χρησιμοποιείται όπως φαίνεται στην εικόνα 15.

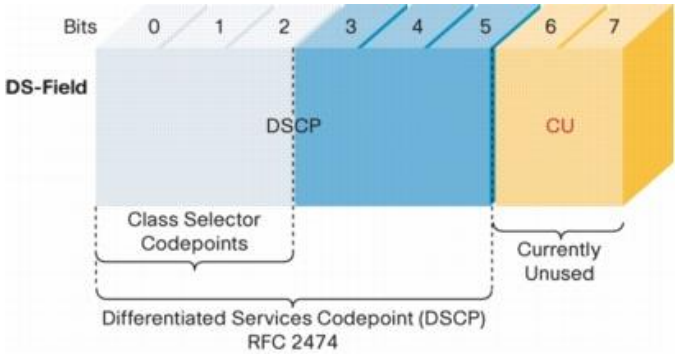
Όταν τα πακέτα κατηγοριοποιούνται στα όρια του δικτύου, συγκεκριμένες πολιτικές μεταχείρισης, που καλούνται χαρακτηριστικά Per–Hop–Behavior (PHB), εφαρμόζονται σε κάθε στοιχείο του δικτύου προσφέροντας έτσι σε κάθε πακέτο την κατάλληλη καθυστέρηση, διακύμανση καθυστέρησης, bandwidth, κτπ. Στο Diffserv , σε αντίθεση με το IntServ, η σηματοδοσια για το QoS μειώνεται, καθώς και ο αριθμός των states –καταστάσεων που πρέπει να διατηρούνται σε κάθε στοιχείο δικτύου περιορίζεται δραστικά, έχοντας σαν αποτέλεσμα μία διευρημένη και απόλυτα κλιμακούμενη QoS λειτουργικότητα.

Όπως παρατηρούμε στην ToS οκτάδα, 6 bits χρησιμοποιούνται για την κατηγοριοποίηση των πακέτων. Αυτά τα bits καλούνται Differentiated Services Codepoint (DSCP). Με το DSCP σε οποιδήποτε κόμβο στο δίκτυο μέχρι και 64 διαφορετικές κλάσεις μπορούν να υποστηριχθούν. Πιο αναλυτικά ένα σύνολο πακέτων πού έχουν την ίδια DSCP τιμή και που ακολουθούν μια συγκεκριμένη κατεύθυνση ονομάζονται–αποτελούν ένα Behavior Aggregate –BA. Το Per–Hop–Behavior που επισημάνθηκε προηγουμένως αναφέρεται στην συμπεριφορά προγραμματισμού –scheduling, αναμονή ουρας –queuing, πολιτικής και κίνησης πακέτου ενός κόμβου πού ανήκει σε ένα BA, όπως καθορίζεται και από ένα Service Level Agreement –SLA. Σήμερα τέσσερις προκαθορισμένες πολιτικές PHB είναι διαθέσιμες για την υλοποίηση ενός Diffserv–enabled δικτύου και για την υποστήριξη QoS και CoS.

IPv4 και IPv6 Headers



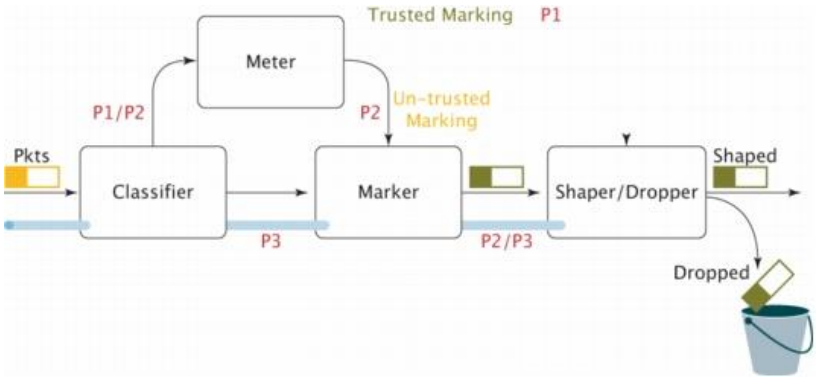
Η οκτάδα IPv4 ToS



Diffserv Codepoint πεδίο

Εικόνα 15. IP και Diffserv

Επιπρόσθετα στο Diffserv η όλη κίνηση μπορεί να διαιρεθεί σε gold, silver και bronze κλάσεις, με την πρώτη να κατανέμει το 50% του διαθέσιμου ευρους ζώνης της γραμμής, τη δεύτερη το 30% και τη Τρίτη το 20%. Το AFxy PHB ορίζει τέσσερις AFx κλάσεις: AF1 , AF2 , AF3 και AF4. Κάθε κλάση αποκτά ένα συγκεκριμένο buffer space και interface bandwidth, βάσει της εκάστοτε SLA πολιτικής. Μέσα σε κάθε AFx κλάση είναι δυνατό να ορίσουμε τρεις packet drop τιμές. Εάν υπάρχει συμφόρηση σε ένα κόμβο και τα πακέτα μιας συγκεκριμένης κλάσης, π. χ. AF1, πρέπει να γίνουν dropped , τότε τα τα συνολικά πακέτα στην AFxy απορρίπτονται με τέτοιο τρόπο ώστε να ισχύει: **dP(AFx1) <= dP(AFx2) <= dp(AFx3)**, όπου dP(AFxy) είναι η πιθανοτητα απόρριψης των πακέτων της AFxy κλάσης. Φυσικά η μεταβλητή y δηλώνει την ακολουθία απόρριψης των πακέτων. Για παράδειγμα πακέτα στην κλάση AF13 θα γίνουν dropped πριν από τα πακέτα της AF12, και αυτά με τη σειρά τους πριν από την κλάση AF11. Αυτή ακριβώς η ακολουθία είναι χρήσιμη για την απαγόρευση των ροών κίνησης που υπερβαίνουν το συνολικό bandwidth.



Εικόνα 16. Diffserv Traffic Conditioner Block

Τέλος αναφέρουμε τα συστατικά ενός Diffserv router που αποτελούν τα λεγόμενα Traffic Conditioners. Ο συνδυασμός τους απλοποιεί την δημιουργία κλιμακούμενων Diffserv δικτύων. Μάλιστα όπως φαίνεται και στην εικόνα 16 μέσω αυτών των components τα πακέτα ακολουθούν ένα συγκεκριμένο path για την υλοποίηση των Traffic Shaping πολιτκών στο δίκτυο. Συγκεκριμένα υπάρχουν:

• **Classifier:** Επιλέγει ένα πακέτο σε μία ροή κίνησης βασει κάποιας τιμής του packet header.

• **Meter:** Ελέγχει τη συμβατότητα σε κάποιες παραμέτρους κίνησης (π.χ. Token bucket) και περνάει τα αποτελέσματα στον marker και shaper.

• **Marker:** Θέτει και επαναθέτει το DSCP value

• **Shaper:** Καθυστερέι ορισμένα πακέτα ώστε να είναι συμβατά με το προφίλ κίνησης.

Είναι προφανές οτι οι αλγόριθμοι ελέγχου κίνησης –traffic control algorithms, καθώς και οι μηχανισμοί ποιότητας υπηρεσιών και πολιτικών traffic shaping μπορούν σε μεγάλο βαθμό να βελτιστοποιήσουν τους δικτυακούς πόρους στην ανάπτυξη GMPLS δικτύων. Γι'αυτό άλλωστε και εξετάζονται συνοπτικά στα πλαίσια της εργασίας.

2.2.2 ΚΛΑΣΕΙΣ ΠΟΙΟΤΗΤΑΣ ΥΠΗΡΕΣΙΩΝ QOS

Όπως ακριβώς αναφέραμε και στην προηγούμενη ενότητα η ανάπτυξη μεγάλης κλίμακας δικτύων GMPLS απαιτεί μηχανισμούς bandwidth management και πολιτικές καθορισμού κίνησης –traffic shaping. Μαλιστα όπως θα δούμε και στην συνέχεια η Traffic Engineering αντίληψη γενικότερα αποτελεί αναπόσπαστο κομμάτι της αρχιτεκτονικής του πεδίου λειτουργικότητας ελέγχου του Generalized. Σαν αποτέλεσμα της σπουδαιότητας αυτής, το MPLS υποστηρίζει οκτώ κλάσεις Ποιότητας Υπηρεσιών –QoS, ενώ το πρωτόκολλο σηματοδοσίας του GMPLS –RSVP (Resource Reservation Protocol) εντάσσει στην νέα TE επέκταση του (RSVP–TE) αμιγή χαρακτηριστικά Quality of Service.

Έχουμε αναφέρει και προηγουμένως οτι τα σύγχρονα επικοινωνικά ευρυζωνικά δίκτυα με τις εκατοντάδες απαιτητικές εφαρμογές σε ζητήματα όπως εύρος ζώνης, καθυστέρηση και αξιοπιστία, απαιτούν μία προσυμφωνημένα εγγυημένη ποιότητα υπηρεσιών προκειμένου να ανταποκριθούν σωστά. Αυτή ακριβώς η συμφωνία ή αλλιώς το συμβόλαιο κίνησης –traffic contract δεσμεύει το δίκτυο να κατανείμει από πριν τους απαραίτητους επικοινωνιακούς πόρους όπως:**bit rate, delay, jitter, packet dropping probability, bit error rate**. Όταν το δίκτυο υποστηρίζει τέτοιους μηχανισμούς Ποιότητας Υπηρεσιών, οι οποίοι έχουν φυσικά νόημα μόνο γιά περιπτώσεις περιορισμένων δικτυακών πόρων ύστερα απο συμφόρηση –congestion, εγγυάται την βέλτιστη εξυπηρέτηση των clients αλλά με προτεραιότητα (βάση της εφαρμογής). Σε αντίθετη περίπτωση αναφερόμαστε σε δίκτυα **best–effort**, οπού δεν εγγυώνται την παροχή βέλτιστης ποιότητας υπηρεσίας, αλλά θα κάνουν όμως οτι μπορούν για να γίνει όσο το δυνατόν αυτό εφικτό.

Network QoS Parameters

Category	*Parameters*
Timeliness	Delay
	Response time
	Jitter
Bandwidth	Systems-level data rate
	Application-level data rate
	Transaction rate
Reliability	Mean time to failure (MTTF)
	Mean time to repair (MTTR)
	Mean time between failures (MTBF)
	Percentage of time available
	Packet loss rate
	Bit error rate

Εικόνα 17. QoS παράμετροι

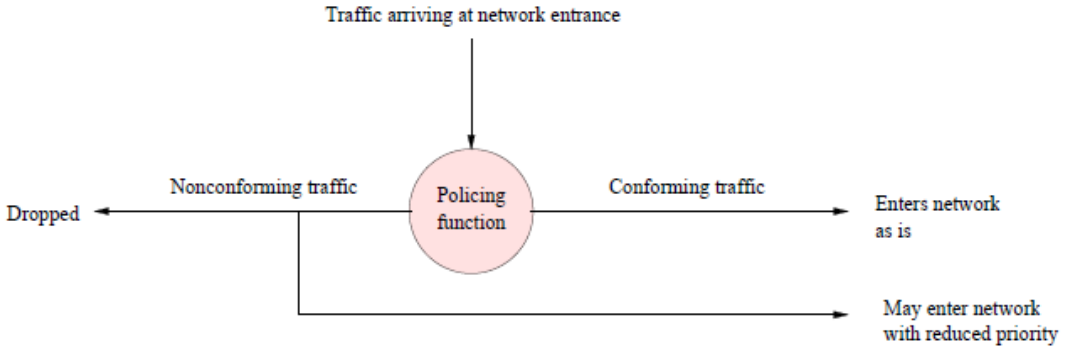
Network Type	*Bandwidth (Mbps)*
Ethernet	10
Fast Ethernet	100
100VG–ANYLAN	100
Token Ring	4 to 16
Wireless LANs	1 to 11
Fiber distributed data interface (FDDI)	100
Distributed queue dual bus (DQDB)	45 to 140
Integrated services digital network (ISDN)	64 to 2.048
Asynchronous transfer mode (ATM)	155 to 622
Switched multimegabit data services	1 to 34
Frame relay	2

Εικόνα 18. Ενδεικτικά bandwidth ranges σύγχρονων δικτύων

Επειδή το Internet αποτελείται στη πράξη απο ετερογενή δίκτυα, η παροχή ποιότητας υπηρεσιών απο άκρου σε άκρου είναι εντελώς απρόβλεπτη. Οι παραμετροι της Εικόνας 18 διακυμαίνονται τόσο χρονικά όσο και ανάλογα με τους προορισμούς. Όταν μάλιστα η ζήτηση υπερβαίνει τους διαθέσιμους πόρους στο δίκτυο είναι λογικό να δημιουργούνται ουρές και άρα καθυστέρηση. Εδώ αποκτά σημασία το Quality Of Service. Οι πόροι στο δίκτυο , όταν υπάρχει συμφόρηση, γίνονται αντικείμενο ανταγωνισμού από τους διαφορετικούς clients. Με τον καθορισμό πολιτικών προτεραιότητας στην κίνηση δημιουγείται μία κατάσταση 'δικαιοσύνης' στο μοιρασμα του aggregate traffic και εξυπηρετούνται ταυτόχρονα πολλές εφαρμογές.

Οι πιό σημαντικοί πόροι που δεσμέυονται απο πριν για το καθορισμό του traffic contract –συμβολαίου κίνησης είναι το εύρος ζώνης γραμμής και ο χώρος ενδιάμεσης αποθήκευσης. Το reservation αυτό στο μεν bandwidth επιτρέπει την τήρηση των delay και jitter απαιτήσεων για σημαντικές κλήσεις υπηρεσιών, ενώ αυτό του ενδιάμεσου χώρου για την τήρηση ενός ορίου απόρριψης πακέτων στο δίκτυο. Εαν δεν υπάρχει σηματοδοσία, π. χ. στη περίπτωση του Diffserv, η δέσμευση πόρων ανά κλήση γίνεται από ειδικά πρωτόκολλα όπως το RSVP–Resource Reservation Protocol. Από κει και πέρα ένας αλγόριθμος καθορισμού πολιτικής κίνησης θα πρέπει να τηρεί τους ακόλουθους περιορισμούς:

- Δε θα πρέπει να απορρίπτει ή να μειώνει την προτεραιότητα των πακέτων που δεν παραβιάζουν το συμβόλαιο κίνησης.
- Οφείλει να ανιχνεύει οποιοδήποτε πακέτο που παραβιάζει το συμβόλαιο και να το απορρίπτει.
- Θα πρέπει να είναι απλό και να λειτουργεί σε πραγματικό χρόνο.



Εικόνα 19. Πολιτική Κίνησης στο QoS δίκτυο

Οι πιό χαρακτηριστικοί μηχανισμοί διαχείρισης εύρους ζώνης στα πλαίσια του QoS ειναι:

- Τεχνικές **traffic shaping** ή **rate limiting**:
  - **Token Bucket**, αλγόριθμος που επιτρέπει τον έλεγχο του πλήθους μεταδιδόμενων πακέτων ανάλογα με την ύπαρξη ή όχι tokens σε έναν κάδο.
  - **Leaky Bucket**, αλγόριθμος που επιτρέπει την μετάδοση πακέτων στο δίκτυο βάση ενός αυξανόμενου μετρητή ο οποίος όταν ξεπεράσει κάποιο όριο αρχίζει να απορρίπτει πακέτα.
  - **Ολισθαίνων TCP παράθυρο**

- Αλγόριθμοι δρομολόγησης **Scheduling Algorithms:**
  - **Weighted Fair Queuing (WFQ)**. Σε κάθε ροή κίνησης αντιστοιχείται μια FIFO ουρά που έχει δικό της βάρος –προτεραιότητα υπηρεσίας.
  - **Class Based Queuing (CBQ).** Υποστηρίζει την κατηγοριοποίηση της κίνησης σε κλάσεις ανάλογα με κάποιες παραμέτρους για κοινή χρήση του aggregate bandwidth.
  - **Weighted Round Robin (WRR).** Εκ περιτροπής εξυπηρέτηση των γεμάτων από πακέτα ουρών σε συγκεκριμένα χρονικά διαστήματα –κβάντα.
  - **Deficit weighted round robin** (**DWRR**) Μία μέγιστη τιμή μεγέθους πακέτου αφαιρείται από το μήκος του εκάστοτε πακέτου, και τα πακέτα που υπερβαίνουν αυτόν τον αριθμό απορρίπτονται.
  - **Hierarchical Fair Service Curve** (**HFSC**) Συνδυασμός και των τριών παρακάτω χαρακτηριστικών όπως: εγγυημένο real–time, adaptive best–effort, και hierarchical link–sharing services.
- Αποφυγή Συμφόρησης
  - Ρητή αποφυγή συμφόρησης
  - Πολιτικές κίνησης
  - Buffer tuning

Στην εικόνα 20 βλέπουμε τις κλάσεις Ποιότητας Υπηρεσιών QoS με κυμαινόμενη προτεραιότητα, όπου 0 η χαμηλότερη και ανταποκρινόμενη σε best–effort κίνηση, και 7 η υψηλότερης προτεραιότητας πιό κατάλληλη για real time εφαρμογές, όπως IPTV και VoIP.

0 (lowest)	**Best Effort**
1	**Background**
2	**Standard (Spare)**
3	**Excellent Load** **(Business Critical)**
4	**Controlled Load** **(Streaming Multimedia)**
5	**Voice and Video** **(Interactive Media and Voice)** **[Less than 100ms latency and jitter]**
6	**Layer 3 Network Control Reserved Traffic** **[Less than 10ms latency and jitter]**
7 (highest)	**Layer 2 Network Control Reserved Traffic** **[Lowest latency and jitter]**

Εικόνα 20. Κλάσεις QoS

2.2.3 ΕΦΑΡΜΟΓΗ ΤΩΝ DIFFERENTIATED SERVICES ΣΤΑ ΟΠΤΙΚΑ ΔΙΚΤΥΑ

Το Traffic Engineering θα πρέπει να θεωρείται ως επέκταση της routing και switching υποδομής, το οποίο παρέχει πρόσθετη πληροφορία για την προώθηση κίνησης ανάμεσα σε εναλλακτικά μονοπάτια στο δίκτυο, και που προσπαθεί να βελτιστοποιήσει την προσφερόμενη ποιότητα υπηρεσιών με την αποφυγή της όποιας συμφόρησης. Το Traffic Engineering είναι απαράιτητο στα σύγχρονα δίκτυα επειδή τα τωρινά δυναμικά πρωτόκολλα δρομολόγησης κάνουν χρήση του συντομότερου μονοπατιού για την προώθηση της κίνησης. Αυτή η πρακτική έχει ως αποτέλεσμα την δέσμευση δικτυακών πόρων, αλλά παράλληλα προκαλεί την υπερβολική χρήση ορισμένων ενώ κάποιοι άλλοι παραμένουν αναξιοποίητοι. Επιπλέον τα routing πρωτόκολλα δεν λαμβάνουν υπόψιν τους συγκεκριμένες απαιτήσεις ροών κίνησης όπως εύρος ζώνης και Quality of Service.

Όταν μία traffic–engineering εφαρμογή υλοποιεί τα σωστά απαιτούμενα χαρακτηριστικά, οφείλει να παρέχει ακριβή έλεγχο στην αντιστοίχηση των ροών κίνησης σε ένα routing και switching domain, να αποκτά καλλίτερη χρήση του δικτύου και μεγαλύτερη διαχειρισιμότητά του. Μία τέτοια λύση συμβατή με οπτικά δίκτυα θα πρέπει να αποτελείται από τις εξής βασικές λειτουργίες:

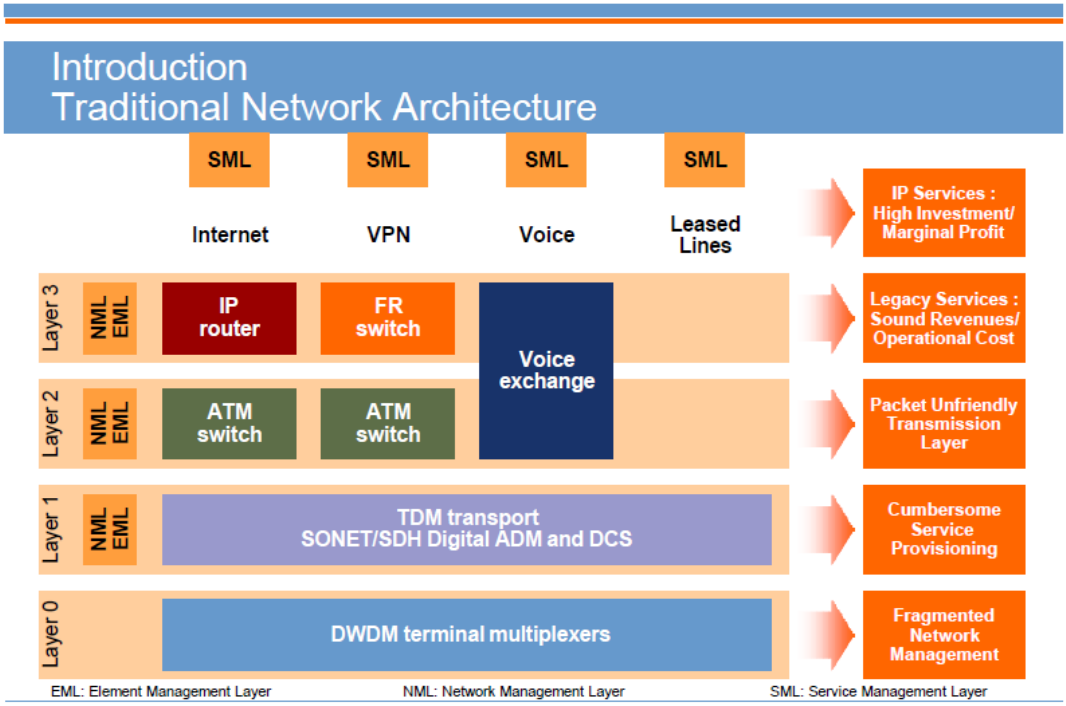
- **Traffic monitoring, analysis, και aggregation** Αυτή η λειτουργικότητα συλλέγει στατιστικά κίνησης από τα διάφορα στοιχεία του δικτύου, όπως για παράδειγμα τα OXCs –Optical Cross Connects. Έπειτα τα στοιχεία αυτά αναλύονται και αθροίζονται ώστε να ετοιμάσουν τις TE αποφάσεις και ενέργειες.
- **Bandwidth demand projection** Το Bandwidth demand projection εκτιμά τις απαιτήσεις σε εύρος ζώνης στο κοντινό μέλλον βασισμένο σε τωρινές και προγούμενες μετρήσεις.
- **Reconfigurations trigger** Αυτή η μεταβλητή αποτελείται από ένα σύνολο πολιτικών που αποφασίζουν διάφορες ενέργειες, όταν πραγματοποιείται μια παραμετροποίηση στο δίκτυο, βάση κάποιων χαρακτηριστικών όπως: μετρήσεις κίνησης, πρόβλεψη εύρους ζώνης, κτπ.
- **Topology design** Παρέχει μία δικτυακή τοπολογία βασισμένη στις μετρήσεις κίνησης και προβλέψεις. Αυτή η διαδικασία μπορεί να ειδωθεί ως η βελτιστοποίηση ενός γράφου (π. χ. ενός OXC που συνδέεται με lightpaths στο WDM επίπεδο) για συγκεκριμένους σκοπούς (π. χ. μεγιστοποίηση throughput), και για κάποια συγκεριμένα constraints (π. χ. χωρητικότητα interface).
- **Topology migration** Αποτελείται από αλγόριθμους που συντονίζουν την μετάβαση από μία παλιά τοπολογία σε μία νεότερη. Επειδή η WDM παραμετροποίηση σχετίζεται με μεγάλης χωρητικότητας κανάλια, αλλάζοντας την κατανομή των πόρων καναλιών επηρεάζεται μεγάλος αριθμός ροών κίνησης τελικών χρηστών. Οι ροές αυτές οφείλουν να προσαρμόζονται στις αλλαγές των οπτικών μονοπατιών σε κάθε φάση μετάβασης.

Παραδοσικά η όλη διαχείρηση των οπτικών δικτύων απαιτούσε χειρωνακτικό προγραμματισμό και οργάνωση, κάτι που είχε ως αποτέλεσμα μέρες ή και εβδομάδες χρόνου εργασίας. Τα τελευταία χρόνια με την εξέλιξη των πρωτοκόλλων ελέγχου –control protocols, καθίσταται εφικτή η δυναμική τροφοδοσία –provisioning και παραμετροποίηση των οπτικών δικτύων, ειδικά στα δίκτυα τελευταίας γενιάς τα ASON/ASTN –Automatically Switched Optical Networks. Πλέον η τελευταία ίσως πρόκληση είναι η ανάπτυξη ενός ενιαίου πεδίου λειτουργικότητας ελέγχου, που θα περιλαμβάνει όλους εκείνους τους αλγορίθμους και τα πρωτόκολλα ελέγχου, για τον δυναμικό έλεγχο των οπτικών πόρων και μάλιστα με περισσότερο κατανεμημένο τρόπο.

2.3.1 ΤΑ ΠΡΟΒΛΗΜΑΤΑ ΤΩΝ ΕΤΕΡΟΓΕΝΩΝ BACKBONE ΤΕΧΝΟΛΟΓΙΩΝ

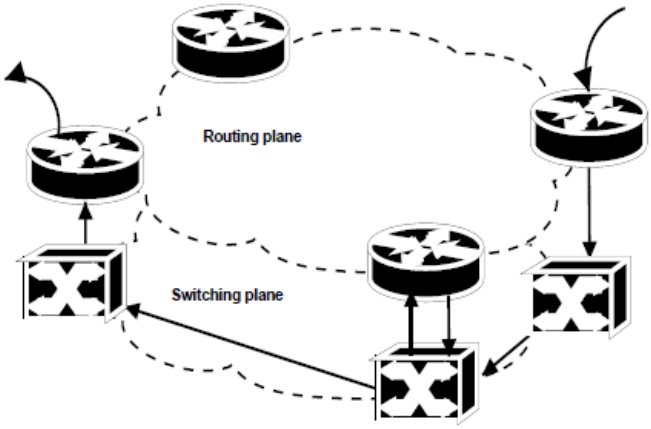
Όπως φαίνεται και στην Εικόνα 21 η παραδοσιακή αρχιτεκτονική δικτύων στα μεριά των backbone–core συστημάτων είναι multi–layer –πολλαπλών επιπέδων. Αποτελείται από το φυσικό στρώμα –layer 0, οπού πραγματοποιούνται στοιχειώδεις διαδικασίες optical switching , στα πλαίσια της WDM τεχνικής multiplexing, στο επίπεδο TDM μεταφοράς 1, στο 2ο layer οπού πραγματοποιείται το VPI/VCI relaying στα ATM switches, και το επίπεδο 3 που αποτελεί το κλασσικό επίπεδο δρομολόγησης IP. Στο υψηλότερο layer

βρίσκονται οι διάφορες υπηρεσίες και web εφαρμογές, όπως Voice, Internet, και VPN's. Παρατηρούμε οτί επειδή ακριβώς υπάρχουν πολλά διαφορετικά επίπεδα αυξάνεται αφενός το διαχειριστικό κόστος της όλης αρχιτεκτονικής, αφετέρου δεν υπάρχει ένας ενοποιημένος και κατανεμημένος έλεγχος με αποτέλεσμα να απουσιάζει ο συντονισμός ανάμεσα στο IP και Optical domain και να δημιουργούνται μη φιλικά προς τη μετάδοση πακέτων δεδομένων επίπεδα μεταφοράς. Αν λάβουμε υπόψιν και τις ετερογενείς διαδικτυακές τεχνολογίες που συνδέονται και λειτουργούν η μια πανω στην άλλη π. χ. ATM/IP ή MPLS/ATM/IP είναι εμφανές οτι απουσιάζει μια ενιαία υποδομή που θα παρέχει αλληλεπίδραση ανάμεσα στις τεχνολογίες πακέτων και στον οπτικό πυρήνα.



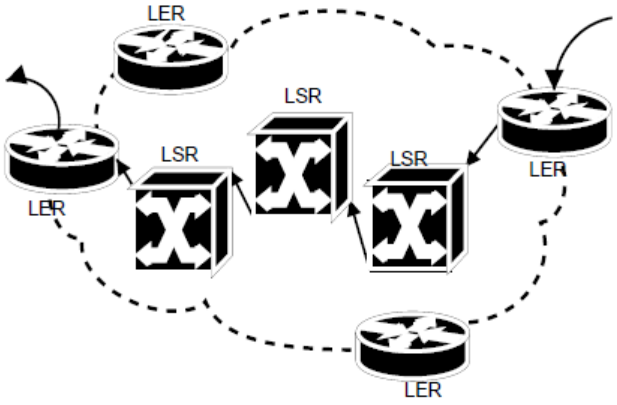
Εικόνα 21. Παραδοσιακή Δικτυακή Αρχιτεκτονική

Η μέχρι πρώτινος καθιέρωση της τεχνολογίας ATM στην υποδομή των δικτύων κορμού συναντούσε σταδιακά πολλά προβήματα ειδικά οσον αφορά την εξέλιξη των δικτύων μετάδοσης και την εμφάνιση νέων πιό απαιτητικών εφαρμογών όπως μετάδοση φωνής. Ειδικότερα τα IP πακέτα που μεταφέρονται σε ένα ATM δίκτυο υφίστανται μεταβαλλόμενη καθυστέρηση διάδοσης –propagation delay. Μια μέθοδος αποφυγής του προβλήματος είναι η διασύνδεση κάποιων συνοριακών –border IP routers με PVC's –Private Virtual Circuits. Δυστηχώς αυτή η διαδικασία απαιτεί κάθε πακέτο να δρομολογείται σε κάθε κόμβο μέσα στο δίκτυο, κάτι που εντέλει αυξάνει και άλλο το propagation delay, με αποτέλεσμα τα πακέτα αυτά να ακολουθούν τις PVC οδηγίες και όχι τη τοπολογία του δικτύου.



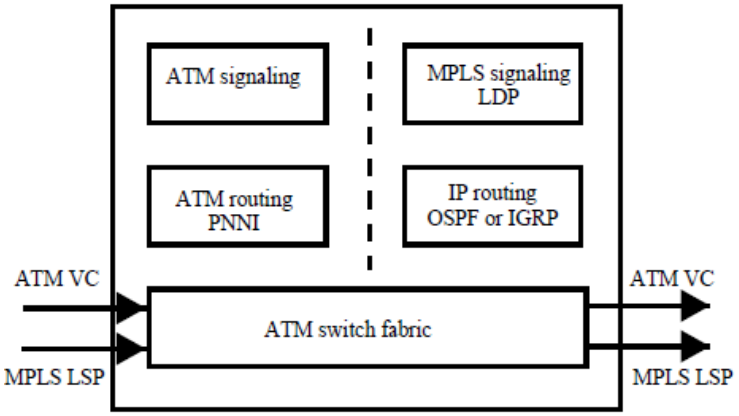
Εικόνα 22. Παραδοσιακή τοπολογία IP over ATM

Λύση στο πρόβλημα δόθηκε με την ανάπτυξη του MPLS . Με το πρωτόκολλο αυτό τα πακέτα δρομολογούνται στα όρια του δικτύου και γίνονται switched μόνο στον πυρήνα, αποφεύγοντας έτσι την παιρετέρω αύξηση του round trip time και άρα του propagation delay μεταξύ διαδοχικών κόμβων.



Εικόνα 23. Δίκτυο MPLS

Επιπρόσθετα το ATM και IP layer έχουν και τα δύο με τη σειρά τους λειτουργικότητα δρομολόγησης –routing functionality. Αυτό προκαλεί προβλήματα όταν κάποια φυσική σύνδεση καταρρεύσει. Το IP routing Protocol (IGRP) θα αρχίσει να ανταλλάσει πληροφορίες δρομολόγησης και να εγκαθιστά νέα μονοπάτια γιά τα πακέτα. Από την άλλη μεριά ταυτόχρονα το PNNI –Private Network to Network Interface πρωτόκολλο του ATM layer θα ξαναεγκαθιδρύει νέο μονοπάτι γιά τις κυψέλες. Μόλις αυτο το μονοπάτι δημιουργηθεί, το IP routing layer πρέπει να ξαναυπολογίσει την πληροφορία δρομολόγησης. Αυτο το φαινόμενο έιναι γνωστό ως 'IGRP stress'. Μία λύση είναι η καθιέρωση static routes κάτι όμως που θα αύξανε το κόστος. Έτσι με την εισαγωγή του MPLS , το πρόβλημα λύνεται με το πεδίο λειτουργικότητας ελέγχου του MPLS λειτουργεί ταυτόχρονα και χωρίς παρεμβολή με αυτό του ATM, όπως φαίνεται και στην εικόνα 24.

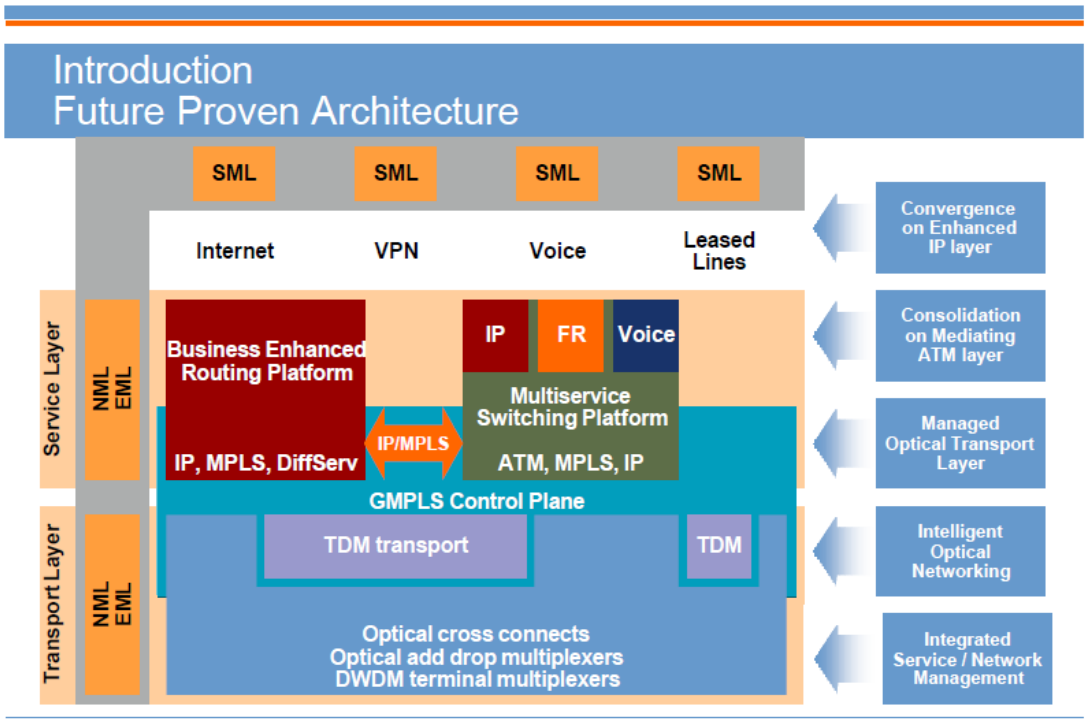


Εικόνα 24. MPLS και ATM control planes

Δυστηχώς όμως τα προβλήματα δεν σταματούν και εδώ. Με την μετάβαση σε cell switched MPLS, δεν επιλύεται το μεγάλο ζήτημα του ATM cell overhead. Δημιουργείται δηλαδή επιπλέον επιβάρυνση φορτίου στις κυψέλες, όπως επίσης και η εξάντληση του χώρου ετικέτας –label space. Η καθιέρωση τέλος διαφορετικών τεχνικών πολυπλεξίας κίνησης , όπως στο πεδίο του χρόνου TDM, στο μήκος κύματος WDM, κτπ, η δεδομένη χρήση δικτύων οπτικών ινών και η απαίτηση για ενοποίηση των πεδίων λειτουργικότητας για λόγους μεγαλύτερης διαχείρησης και κλιμάκωσης, δεν αφήνουν σήμερα πλέον πολλά περιθώρια εξέλιξης ακόμη και για το MPLS. Έτσι το φυσικό επακόλουθο για την κάλυψη αυτών των απαιτήσεων είναι η Γενίκευση του στο Generalized.

2.3.2 Η ΑΠΑΙΤΗΣΗ ΓΙΑ ΕΝΑ ΕΝΟΠΟΙΗΜΕΝΟ CONTROL PLANE

Κρίνοντας από τις τρέχουσες εξελίξεις των δικτύων μεταφοράς καθώς και από την εμφάνιση νέων πρωτοκόλλων ελέγχου, η αποδεδειγμένη μελλοντική αρχιτεκτονική που θα αντιπροσωπεύει τα σύγχρονα δίκτυα επικοινωνιών είναι αυτή της εικόνας 25.



Εικόνα 25. Μελλοντική Τάση Αρχιτεκτονικής Δικτυών

Παρατηρώντας την εικόνα συμπεραίνουμε οτι τα τέσσερα επίπεδα –layers της προηγούμενης αρχιτεκτονικής μειώνονται συνολικά σε δύο:στο στρώμα μεταφοράς –Transport layer, και στο στρώμα υπηρεσιών –Service layer. Το μεν πρώτο αφορά καθαρά τα στοιχεία εκείνα του δικτύου που σχετίζονται με τη μεταφορά των πακέτων δεδομένων αλλά και τις στοιχειώδεις διαδικασίες optical switching, όπως τους οπτικούς πολυπλέκτες/αποπλέκτες, τα τερματικά οπτικών δικτύων και τα OXC's. Είναι επίσης εμφανές οτι καθένα απο αυτά τα επίπεδα χωρίζεται και σε υποστρώματα –sublayers, κάτι που ισχύει και για το πρώτο επίπεδο. Έτσι στο ανωτερο υπόστρωμα του 1ου layer επικρατεί Time Division Multiplexing μεταφορά, δηλαδή στο πεδίο διαχωρισμού του χρόνου. Ανεβαίνοντας επίπεδο συναντάμε τις διαφορετικές switching δικτυακές πλατφόρμες όπως ATM, MPLS και Frame Relay, με ταυτόχρονη υποστήριξη Diffserv χαρακτηριστικών και IP δρομολόγησης. Μάλιστα παρατηρούμε οτι ο συγκερασμός των δύο αυτών επιπέδων συντελείται στο πεδίο λειτουργικότητας ελέγχου του GMPLS –GMPLS Control Plane. Ο λόγος που επιλέγεται η Generalized επέκταση του MPLS είναι διότι αυτή ακριβώς εμφανίζεται καταλληλότερη για την υλοποίηση του Intelligent Optical Networking concept, με χαρακτηριστικά όπως μεγαλύτερο συντονισμό ανάμεσα στον IP και Optical domain, βελτιωμένες τεχνικές προστασίας και αποκατάστασης γραμμής, καθώς και νέες υπηρεσίες όπως O–VPN's –Optical Virtual Private Networks, διαφοροποιημένα κυκλώματα μετάδοσης, και bandwidth on demand. Είναι προφανές οτι η επικρατούσα τάση δεν είναι άλλη από την συγκλιση του Data με το IP. Αυτο δεν είναι τυχαίο καθώτι με αυτό το τρόπο επιτυγχάνεται πιο κατανεμημένος διαχειριστικός έλεγχος στο δίκτυο, μειώνεται το λειτουργικό κόστος και αυξάνεται η βιωσιμότητα και η στιβαρότητά του. Δεν είναι τυχαία επίσης η επιλογή του GMPLS ως το framework εκείνο που με τις επεκτάσεις σηματοδοσίας και τα TE constraints που έτσι και αλλιώς υποστήριζε το MPLS, κατορθώνει να κάνει πράξη αυτή τη προοπτική.

Για την κάλυψη των απαιτήσεων του Intelligent Optical Networking και για να φτάσουμε σε αυτή την αρχιτεκτονική υπήρξαν κάποιες αυστηρές προυποθέσεις για ένα εξυπνότερο και πιό λειτουργικό control plane:

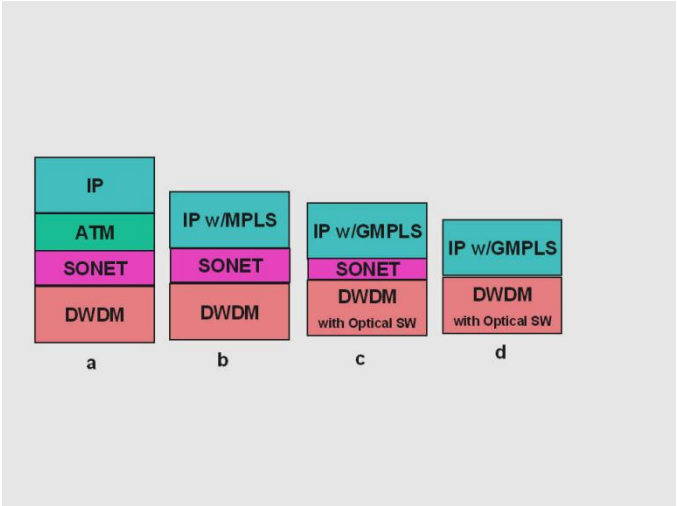
- ✓ Οφείλει να είναι ικανό και επαρκές προκειμένου να προσαρμόζεται σε διαφορετικά μοντέλα υπηρεσιών, με το να καθιερώνει υβριδικούς αντί για ανταγωνίσιμους μηχανισμούς, π. χ. Peer και Overlay αντί για Peer–vs–Overlay.
- ✓ Οφείλει να είναι εφαρμόσιμο σε όλα τα circuit–switched δίκτυα όπως OTN, SONET/SDH, και PDH.
- ✓ Οφείλει να υποστηρίζει πολλαπλούς network clients (IP, ATM, …)
- ✓ Οφείλει να απλοποιεί τις διαδικασίες μετάβασης και συνεργασίας μεταξύ δικτύων με διαφορετικά πεδία λειτουργικότητας δεδομένων –data planes.
- ✓ Οφείλει να επεκτείνει τους μηχανισμούς IP Traffic Engineering σε ένα ενιαίο optical control plane.

Επιπλέον είναι σημαντικό το πρωτόκολλο ελέγχου να είναι ιδιαίτερα αποτελεσματικό σε περιπτώσεις κατάρρευσης γραμμής μετά απο αστοχία, καθώς σε αυτή τη περίπτωση απαιτουνται πολύπλοκες ενέργειες όπως αποκατάσταση σε κλιμακα μεγάλης απόστασης και όχι τοπικής, αποφυγή μελλοντικών link failures, και προβλημάτων IP δρομολόγησης.

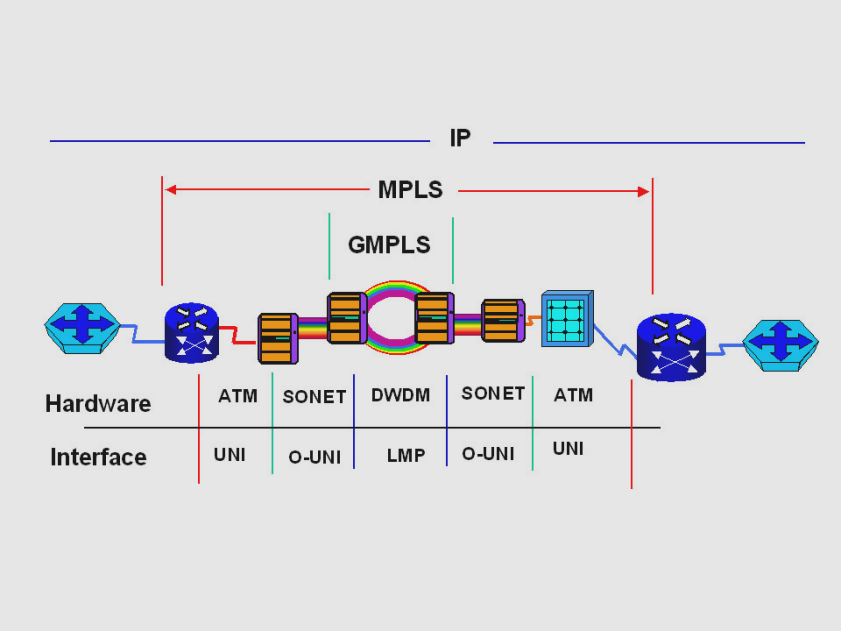
2.3.3 ΤΟ ΟΡΑΜΑ ΤΟΥ GMPLS ΣΥΓΚΛΙΣΗ DATA ΚΑΙ IP

Ο πυρήνας της λειτουργικότητας του GMPLS στηρίζεται στις ακόλουθες νέες αντιλήψεις:

- ❖ Τη μετάβαση από ένα παραδοσικά αποκεντρωμένο πεδίο διαχείρισης – Management Plane (MP), σε ένα ενοποιημένο και ανεξάρτητο πεδίο λειτουργικότητας ελέγχου –control plane (CP). Κάτι τέτοιο είναι προφανές οτί αυξάνει την βιωσιμότητα και ευρωστία του δικτύου μειώνοντας ταυτόχρονα το λειτουργικό κόστος[Εχει αποδειχθεί στη πράξη μείωση του κόστους έως και 50%].
- ❖ Ένα μοντέλο ελέγχου πλήρως εφαρμόσιμο σε οπτικά δίκτυα πολλαπλών επιπέδων με διαφορετικές αρχιτεκτονικές όπως SONET/SDH, OTN, WDM , κτπ.
- ❖ Εξειδικευμένα πρωτόκολλα ελέγχου μέσω επεκτάσεων σηματοδοσίας , π. χ. RSVP–TE και CR–LDP, για δέσμευση πόρων συνδέσμων που κατανέμονται στα LSP's, routing και switching λειτουργίες για δυναμικό υπολογισμό μονοπατιού –path computation.
- ❖ Την εισαγωγή του LMP –Link Management Protocol το οποίο είναι υπεύθυνο για την ανίχνευση και παραμετροποίηση διεπαφών των transport και control planes.
- ❖ Καθιέρωση εξειδικεύμενων μηχανισμών Traffic Engineering.
- ❖ Υπηρεσίες αποκατάστασης και επανάκτησης.



Εικόνα 26. Η υπόσχεση του GMPLS – Σύγκλιση Data IP

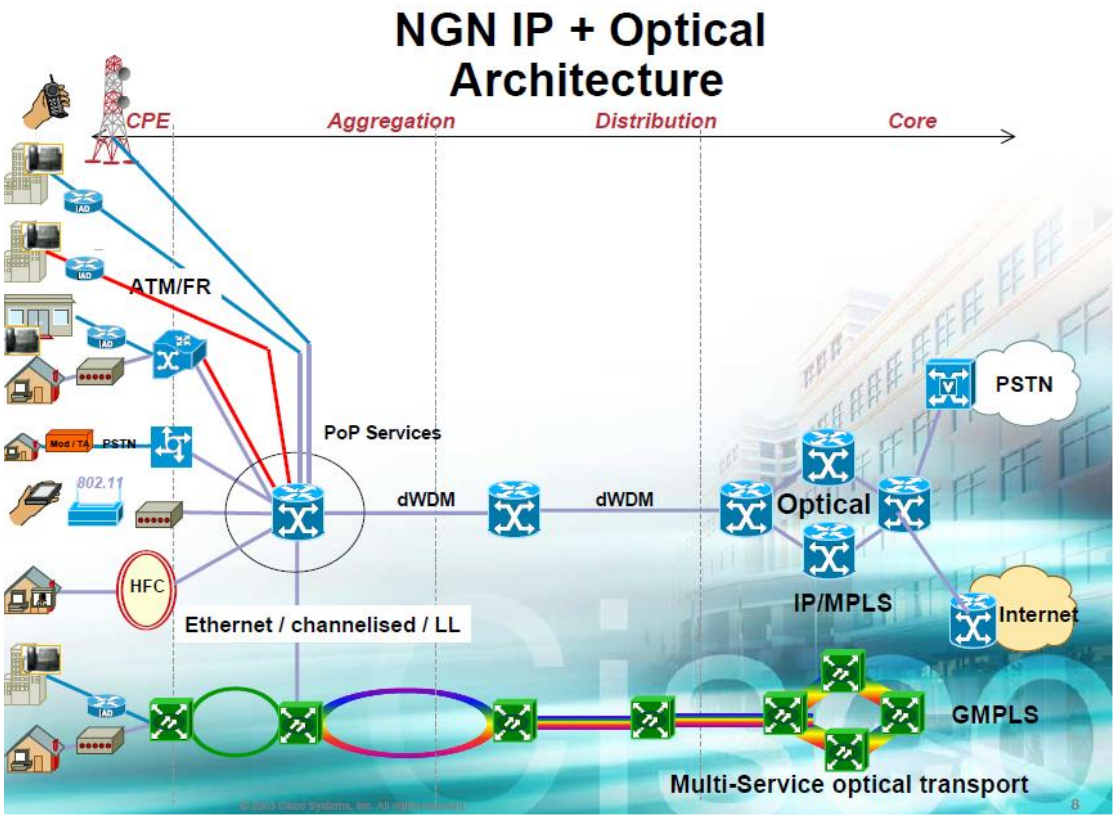


Εικόνα 27. Η αρχιτεκτονική του GMPLS

Το GMPLS βασισμένο στην επιτυχία του προκατόχου του MPLS, επεκτείνει τα IGP – Interior Gateway Protocols πρωτόκολλα δρομολόγησης που ήταν ήδη συμβατά για TE. Παράλληλα εισάγει νέους μηχανισμούς προστασίας εξειδικευμένα γιά κάθε link, όπως 1+1, 1:N, υποστηρίζει πολλαπλούς τύπους φορτίων Payload types ανάλογα με τον κάθε client, καθώς και κωδικοποιήσεις μονοπατιών LSP's για SONET/SDH. Πιο αναλυτικά οφείλει να ικανοποιεί τις ακόλουθες προκλήσεις σε επίπεδο διαχείρισης δικτύου:

- Οφείλει όχι μόνο να να προωθεί πακέτα σε δρομολογητές, αλλά και να πραγματοποιεί αποφάσεις μεταγωγής –switching στο πεδίο διαχωρισμού χρόνου, μήκους κύματος και φυσικών διεπαφών –ports.
- Είναι υποχρεωμένο να διαχειρίζεται με μεγάλη ακρίβεια τον οπτικό domain καθως αποτελείται απο χιλιάδες χρώματα φωτός που απαιτουν το κάθε ένα έλεγχο, σε αντίθεση με τον IP domain.

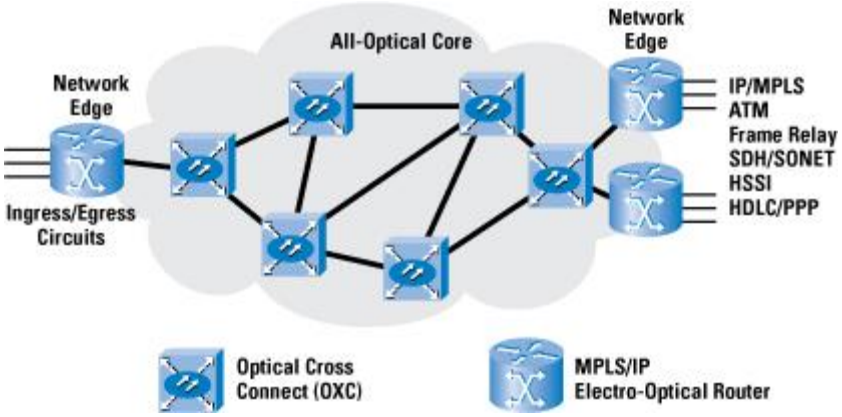
- Υπάρχει συνήθως μεγαλύτερη καθυστέρηση στην εγκαθίδρυση ενος LSP μονοπατιού σε έναν optical switch παρά σε έναν IP router. Το GMPLS οφείλει να προσαρμόζεται αντίστοιχα.
- Τα SDH/SONET συστήματα είναι ικανά να αποκαθίστανται σε λιγότερο από 50ms ύστερα από αστοχία γραμμής. Ο πίνακας ελέγχου του GMPLS οφείλει να λαμβάνει υπόψιν αυτή τη δυνατότητα.



Εικόνα 28. Δίκτυα Επόμενης Γενιάς –Next Generation Networks βασισμένα στο GMPLS

Η σύγχρονη υποδομή μεταφοράς του Internet μπορεί να ειδωθεί στο φυσικό επίπεδο σαν ένα πολυσύνθετο σύνολο από διασυνδεδεμένα οπτικά και ηλεκτρονικά –ETDM υποδίκτυα, όπου κάθε ενα αποτελείται από αρκετές ετερογενείς routing και switching συσκευές με τις δικές τους πολιτικές ελέγχου και control plane λειτουργικότητες. Με αυτούς τους διαφορετικούς τύπους συσκευών, ολες οι αποφάσεις προώθησης θα βασίζονται σε ένα συνδυασμό από πακέτα, κυψέλες, timeslots, μήκη κύματος, και διεπαφές, ανάλογα με τον ρόλο και την θέση της εκάστοτε switching συσκευής. Νέες οπτικές συσκευές όπως Dense–WDM πολυπλέκτες, Add/Drop πολυπλέκτες (ADM), και Optical Cross–Connects (OXC's), κάνουν εφικτή την intelligent all–optical core λογική, όπου τα πακέτα δρομολογούνται στο δίκτυο χωρίς να φεύγουν από τον optical domain. Όπως φαίνεται και ξεκάθαρα στην εικόνα 29, το οπτικό δίκτυο και τα γειτονικά IP δίκτυα είναι ανεξάρτητα μεταξύ τους. Ο οπτικός domain είναι υπεύθυνος για την εγκατάσταση των μονοπατιών φωτός –lightpaths ανάμεσα στους edge IP routers. Το κλειδί για την εγγύηση των επιθυμητών ταχυτήτων και της σωστής λειτουργικής συμπεριφοράς είναι τα δίκτυα αυτά να

διατηρούν το σήμα σε καθαρά οπτική μορφή, αποφεύγοντας έτσι την πρόκληση overhead από τις ενδιάμεσες μετατροπές από και πρός ηλεκτρονική μορφή. Το GMPLS κατορθώνει να κάνει πράξη τις προηγούμενες προκλήσεις καθώς προσφέρει ένα οπτικό πεδίο λειτουργικότητας ελέγχου το οποίο παραμετροποιεί αυτόματα και δυναμικά οποιοδήποτε στοιχείο δικτύου, ακόμη και οπτικές συσκευές όπως αυτές που αναφέραμε.



Εικόνα 29. Η Υποδομή Οπτικής Μεταφοράς

Ο πινακας ελέγχου –control plane του GMPLS υποστηρίζει διαχείριση συνδέσμων ενώ παρέχει μηχανισμούς προστασίας και αποκατάστασης. Είναι υποχρεωμένος ειδικά για τα οπτικά δίκτυα να ανιχνεύει τη τοπολογία του δικτύου και να ενημερώνει για την κατάσταση των δικτυακών πόρων. Δύο πρωτόκολλα εκπληρώνουν αυτό το έργο:

- **Routing protocols** τα οποία είναι υπεύθυνα για την διαφήμιση της τοπολογίας του οπτικού δικτύου, τον καθορισμό των περιοχών δρομολόγησης και την ενημέρωση των διαθέσιμων πόρων ανάμεσα στους διάφορους domains.
- **Signaling protocols** είναι υπεύθυνα με τη σειρά τους γιά τη τροφοδοσία, διατήρηση και αποδέσμευση των συνδέσμων. Τα οπτικά δίκτυα χαρακτηρίζονται από συνδεμοστραφείς τεχνικές που απαιτούν πρωτόκολλα δέσμευσης πόρων –resource reservation protocols. Με τον πλήρη διαχωρισμό μάλιστα του data από το control plane που υλοποιεί έτσι και αλλιώς το GMPLS, καθιερώνονται hard state reservation protocols χωρίς περιοδική ανανέωση στους κόμβους ώστε να περιορίζεται η συνέπεια της ενδεχόμενης κατάρρευσης του control plane.

Μαλιστα η όλη υποδομή του Generalized control plane κατορθώνει να υπολογίζει τα optical paths σε διάστημα μερικών δευτερολέπτων αντί για ώρες ολόκληρες όπως συνέβαινε παλιότερα, όπως επίσης και την δέσμευση κυκλωμάτων κατ'απαίτησιν με συγκεκριμένα χαρακτηριστικά bandwidth και Traffic Engineering. Τέλος επιλύει το γνωστό traffic–grooming πρόβλημα που συναντάμε στα οπτικά δίκτυα με το να λειτουργεί σε ένα επίπεδο δύο στρωμάτων [το είδαμε στην εικόνα 26] ανάμεσα στους κόμβους:δηλαδή ένα καθαρά οπτικό –pure optical wavelength routed δίκτυο και ενα οπτικο–ηλεκτρονικό TDM από πάνω του. Το πρώτο υπόστρωμα εγκαθιστά μονοπάτια φωτός –lightpaths ανάμεσα σε κόμβους που μάλιστα φαίνονται ως διαδοχικοί –adjacent απο το ανώτερο στρώμα. Το δέυτερο με τη σειρά του πραγματοποιεί σύνθετες διαδικασίες πολύπλεξης/απόπλεξης σε ένα wavelength μονοπάτι μέσω τεχνικών διαχωρισμού στο χρόνο, στην ίνα, κτπ. Παρομοιώς υλοποιεί και διαδικασίες remultiplexing για σύνθετα traffic demands που απαιτούν

παρόμοια μεταχείριση. Αυτό είναι εφικτό χάρις στην γενικευμένη και πολυεπίπεδη φύση του GMPLS control plane.

ΚΕΦΑΛΑΙΟ 3: ΑΠΟ ΤΟ MPLS ΣΤΟ GENERALIZED MPλS:GMPLS

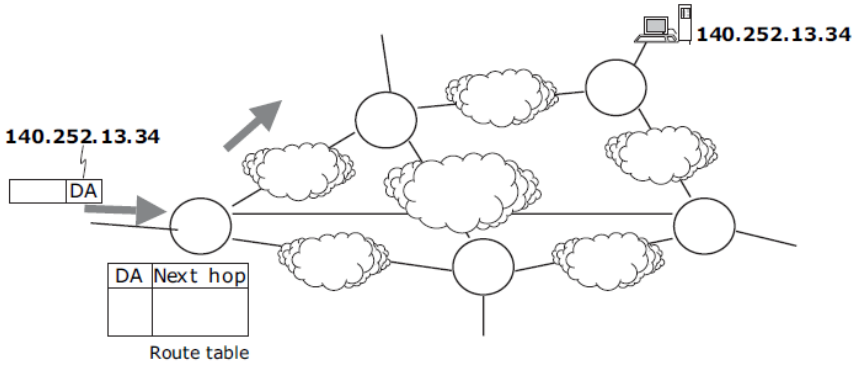
3.1.1 MULTI–PROTOCOL LABEL SWITCHING (MLPS)

Το πρωτόκολλο **MPLS –Multi–Protocol Label Switching** ξεκίνησε να αναπτύσσεται στα μέσα της δεκαετίας του 90 με στόχο την κάλυψη δύο αντικειμενικών απαιτήσεων:η πρώτη ήταν η βελτιωμένη αλληλεπίδραση του ATM με το IP μέσω της παροχής ενός μοναδικού πεδίου λειτουργικότητας ελέγχου –control plane που θα συνδύαζε τόσο τα ATM switches όσο και τους IP routers. Η δεύτερη απαίτηση αφορούσε την προσθήκη στο IP control plane επιπλέον χαρακτηριστικών λειτουργικότητας όπως traffic engineering κάνοντας χρήση της constrained–based δρομολόγησης που ήταν έτσι και αλλιώς υπάρχουσα στο πεδίο λειτουργικότητας του ATM. Η ιδέα ενός ενοποιημένου control plane για τα ATM switches και IP routers οδήγησε , λίγο αργότερα, στην γέννηση του Generalized Multi Protocol Label Switching –GMPLS που παρείχε ενιαίο πεδίο λειτουργικότητα ελέγχου όχι μόνο για ATM και IP αλλά και για οπτικές συσκευές επίσης , όπως optical cross connects –OXC's.

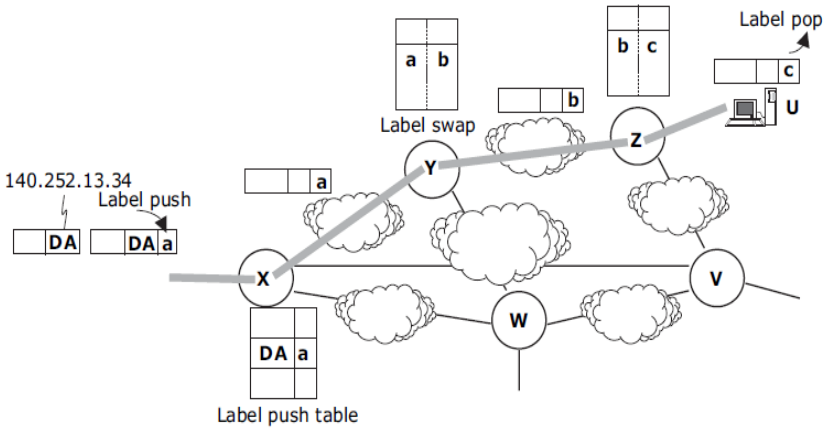
Στην ενότητα 2.1.4 αναφέραμε συνοπτικά τους πιο αντιπροσωπευτικούς τρόπους υπολογισμού του επόμενου hop δρομολόγησης στο ip routing table κατά την μετάδοση IP πακέτων. Ένας από αυτούς είναι η longest–prefix match μέθοδος. Ωστόσο όταν το IP routing table γίνεται μεγάλο, κάτι που ισχύει κατα κόρον για τα σημερινά δίκτυα δεδομένων , όσο μάλιστα κλιμακώνονται περισσότερο, η μέθοδος αυτή χρησιμοποιεί την τεχνική του **Patricia tree** για αναζήτηση στο πίνακα δρομολόγησης. Κάτι τέτοιο όμως αποδυκνείεται ασύμφορο απο αποψη ταχύτητας για τους δρομολογητές. Για την επίλυση του συγκεκριμένου προβλήματος εισήγχθη η αντίληψη του MPLS στην IP μετάδοση πακέτων.

Στο MPLS αντί να γίνεται αναζήτηση στο πίνακα δρομολόγησης βάσει μίας διεύθυνσης προορισμού στην IP επικεφαλίδα σαν κλειδί, **μια ετικέτα –label εισάγεται σε κάθε πακέτο** και η επόμενη διεύθυνση προσδιορίζεται ψάχνοντας για αυτή την ετικέτα σε έναν πίνακα μετάδοσης. Σε αντίθεση με το IP που είναι ασυνδεσμικό –connectionless, το MPLS είναι συνδεσμοστεφής τεχνολογία –connection–oriented. Εγκαθιστά κατ'αρχήν μια εικονική σύνδεση –virtual connection ανάμεσα στα start και end points, και εκτελεί μετάδοση πακέτων πάνω σε αυτή την εικονική σύνδεση. Το Label χρησιμοποιείται για να αναγνωρίσει την σύνδεση αυτή. Στην εικόνα 30(a) διακρίνεται η βασική αρχή της IP datagram επικοινωνίας (connectionless). Η δεύθυνση προορισμού (DA = 140. 252. 13. 34) γράφεται στην επκεφαλίδα του πακέτου. Συγκεκριμένα η διεύθυνση αυτή προσδιορίζει μια μοναδική τιμή σε ολόκληρο το δίκτυο, ενώ διαφορετική τιμή αποδίδεται σε κάθε κόμβο του δικτύου. Κάθε δρομολογητής διατηρεί έναν δικό του πίνακα δρομολόγησης οπού η σχέση ανάμεσα στη διεύθυνση προορισμού και τον επόμενο κόμβο καταγράφεται. Όταν ένα πακέτο φθάσει στον router, αυτός ψάχνει τον πίνακα του χρησιμοποιώντας το destination address που εξάγεται απο την IP επικεφαλίδα του πακέτου ως κλειδί αναζήτησης, και προσδιορίζει τον επόμενο hop. Εκτελώντας αυτή τη διαδικασία επαναληπτικά σε κάθε δρομολογητή, το πακέτο παραλαμβάνεται από τον τελικό παραλήπτη.

Σε αντίθεση με αυτή τη διαδικασία, στην Εικόνα 30(b) παρατηρούμε τον βασικό μηχανισμό της συνδεσμοστρεφούς επικοινωνίας βασισμένης στο εικονικό κύκλωμα.



(a) Βασική αρχή της IP datagram επικοινωνίας (connectionless)



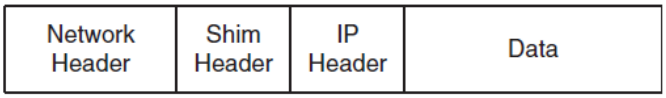
(b) Μηχανισμός της συνδεσμοστρεφούς επικοινωνίας μέσω εικονικού κυκλώματος

Εικόνα 30. Σύγκριση IP και MPLS μεταφοράς

Σε αυτή τη περίπτωση μια ετικέτα εισάγεται στην επικεφαλίδα ενός πακέτου. Αυτή η ετικέτα –label δεν απαιτείται να είναι μοναδική σε όλο το δίκτυο;αντίθετα είναι δυνατό να είναι μοναδική στην εκάστοτε γραμμή σύνδεσης. Εδώ θα πρέπει να τονιστεί οτι στην datagram επικοινωνία μια διεύθυνση χρησιμοποιείται για να αναγνωριστεί ένας host, ενώ στις virtual circuit επικοινωνίες μέσω μιας ετικέτας αναγνωρίζεται μια ροή κίνησης –traffic flow. Μάλιστα στη τελευταία περίπτωση κάθε κόμβος που αναλαμβάνει καθήκοντα δρομολόγησης καλείται μεταγωγέας –switch σε αντιδιαστολή με τους routers στις IP επικοινωνίες. **Το switch ψάχνει τον πινακα ετικέτας του χρησιμοποιώντας το εξαγόμενο label απο το πακέτο που φθάνει στην σύνδεση εισόδου, ως κλειδί αναζήτησης. Έπειτα αντικαθιστά την ετικέτα της επικεφαλίδας του πακέτου με αυτήν της γραμμής εξόδου, και μεταφέρει το πακέτο στον επόμενο hop.**

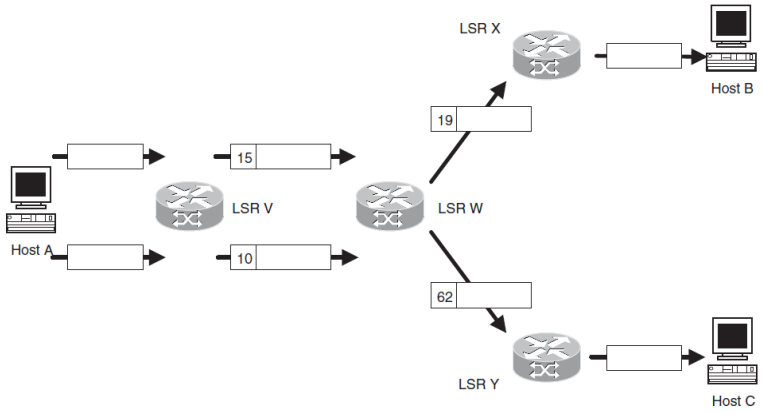
Εκείνο που αναδυκνείει τη σημασία του μηχανισμού του MPLS είναι η άψογη συνεργασία του με τη παραδοσιακή IP datagram επικοινωνία. Όταν πακέτα εισέρχονται από ένα IP σε ένα MPLS δίκτυο, μια ετικέτα εισάγεται σε αυτά ώστε να μεταδοθούν με τον μηχανισμό virtual circuit. Αργότερα κατα την έξοδό τους απο το MPLS δίκτυο αυτή η ετικέτα **αφαιρείται**, και η ασυνδεσμική μετάδοση επανέρχεται. Σε ένα MPLS δίκτυο κάθε κόμβος καλείται **label–switch router (LSR)**. Μάλιστα ένας LSR που βρίσκεται στα σύνορα του δικτύου καλείται **label–edge router (LER)**, ενώ μία εικονική σύνδεση ονομάζεται **label–switch path (LSP)**.

Μια MPLS ετικέτα εισάγεται δυναμικά κάθε φορά που εγκαθιδρύεται ένα LSP μονοπάτι. Μάλιστα ο πινακας ετικετών κάθε LSP περιέχει όλες τις απαραίτητες πληροφορίες ενός μονοπατιού καθώς και τις ετικέτες για τον διαχωρισμό των LSP's, που στις περισσότερες περιπτώσεις είναι κάποιος αριθμός για την αναγνώριση των εικονικών κυκλωμάτων. Ως αποτέλεσμα καθίσταται εφικτό να γίνεται αναζήτηση στο label table χρησιμοποιώντας την ετικέτα ως κλειδί, και έτσι να διευκολύνεται η ταχεία εύρεση στον πίνακα δρομολόγησης. Έτσι μέθοδοι όπως longest–prefix match και patricia tree για αναζήτηση στους IP πίνακες δρομολόγησης γίνονται λιγότερο απαραίτητοι. Η MPLS ετικέτα αποτελεί ενα μικρού μεγέθους, και καθορισμένου μήκους label , που εισάγεται σε κάθε πακέτο προς μετάδοση ώστε να προωθήται εύκολα στο δίκτυο. Αυτή η επιπρόσθετη ποσότητα πληροφορίας που εισάγεται καλείται **shim header**, είναι 20–bit, και τοποθετείται ανάμεσα στο Network Protocol Header και στο IP Header, όπως φαίνεται και στην εικόνα 31. Ο πίνακας ετικετών που προαναφέραμε καλείται **Label Forwarding Information Base –LFIB** και περιέχει αντιστοιχήσεις της μορφής {incoming interface, incoming label} σε {outgoing interface, outgoing label}. Η μόνη πολυπλοκότητα υπάρχει στον ingress –σημείου εισόδου LER , οπού θα πρέπει να κατηγοριοποιήσει κάθε πακέτο ανάλογα με τον προορισμό του και την αντίστοιχη παρεχόμενη πολιτική ποιότητας υπηρεσιών. Σε όλους τους υπόλοιπους κόμβους η διαδικασία είναι προβλεπόμενη καθώτι οι αντιστοιχήσεις στους πίνακες LFIB's που αναφέραμε είναι στατικές, και εκ των προτέρων γνωστές.



Εικόνα 31. Το σημείο εισόδου του shim header στο IP πακέτο

Στην εικόνα 32 έχουμε τωρα ενα παράδειγμα δύο Label Switched Path μονοπατιών. Το MPLS δίκτυο αποτελείται απο τέσσερις LSR's που προωθούν τα πακέτα. Ο Host A στέλνει IP πακέτα στον LSR V. Ο συγκεκριμένος είναι ingress LSR κάνει την κατηγοριοποίηση των πακέτων βάσει του τελικού τους προορισμού, τα αντιστοιχίζει σε ένα LSP, και εισάγει σε αυτά ετικέτα. Απο τα πακέτα που στέλνει ο Host A, αυτά που προορίζονται για τον Host B αποκτούν την ετικέτα 15, ενώ αυτά για τον Host C την ετικέτα 10. Στον LSR W εξετάζονται οι αντιστοιχήσεις του πίνακα ετικετών του, για τον προσδιορισμό της εξερχόμενης ετικέτας και interface. Τα labels που είχαν εισαγχθεί προηγουμένως τώρα αντικαθίστανται με καινούργια, γίνονται swapped, και προωθούνται στα αντιστοιχα interface εξόδου. Έτσι τα πακέτα με το label 15 οδηγούνται στον LSR X με νέα ετικέτα την 19, ενώ αυτά με label 10 στον LSR Y με καινούργιο label το 62. Τέλος οι LSR's αυτοί είναι egress, δηλαδή αφαιρούν το shim header, και προωθούν τα πακέτα στο IP επίπεδο.



Εικόνα 32. Label Switch Paths (LSP's)

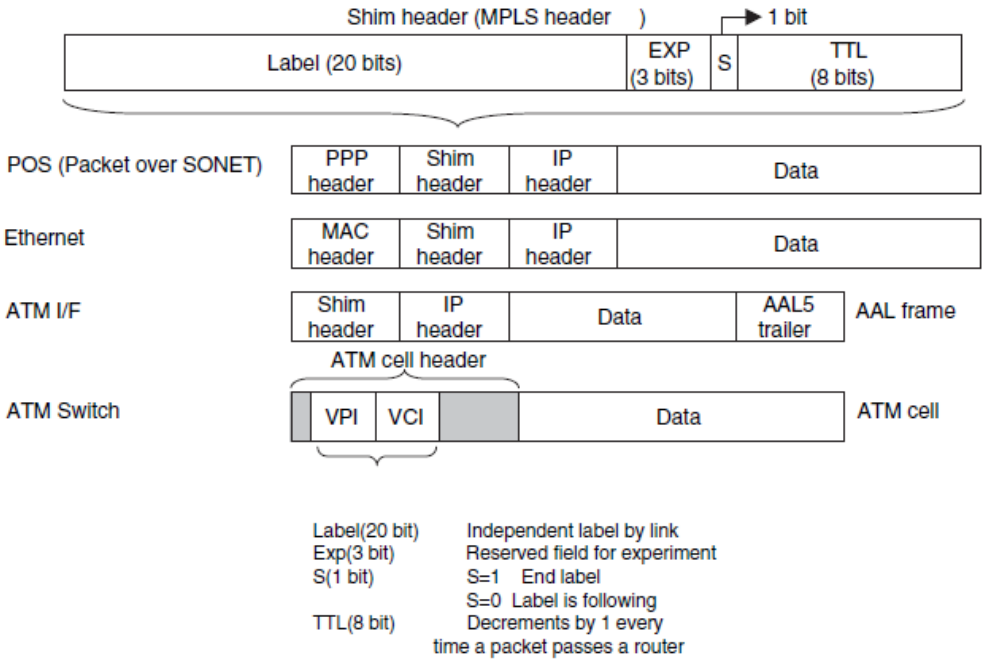
Πακέτα με την ίδια ετικέτα –label μεταχειρίζονται με την ίδια διαδικασία μετάδοσης σε ένα MPLS δίκτυο. Αυτή η διαδικασία καλείται **κλάση ισοδύναμης προώθησης – Forwarding Equivalence Class (FEC)**. Όταν πακέτα εισέρχονται στο δίκτυο, ο ingress label switch router αποφασίζει σε ποιά κλάση ισοδύναμης προώθησης ανήκουν αυτά τα πακέτα. Αυτά που θα προωθηθούν στο ίδιο egress σημείο, πάνω στο ίδιο μονοπάτι και με την ίδια διαδικασία μεταφοράς λέμε οτι ανήκουν στην ίδια κλάση FEC. Μάλιστα είναι δυνατόν να αλλάξουμε τον μηχανισμό αυτό μεταφοράς , π. χ. σε TCP πρωτόκολλο, προσδιορίζοντας ένα εκάστοτε TCP/UDP port number ανά εφαρμογή για κάθε FEC , όπως φαίνεται και στο πίνακα 32, κάτι βέβαια που φάνταζε δύσκολο να υλοποιηθεί στην συμβατική IP datagram επικοινωνία.

	SA	DA	SP	DP	PID
FEC 1	—	141.72.168.0/24	—	—	—
FEC 2	192.168.32.6/24	141.72.168.0/24	—	—	—
FEC 3	192.168.32.0/24	141.72.168.0/24	—	80	TCP

Εικόνα 33. Παραδείγματα FEC

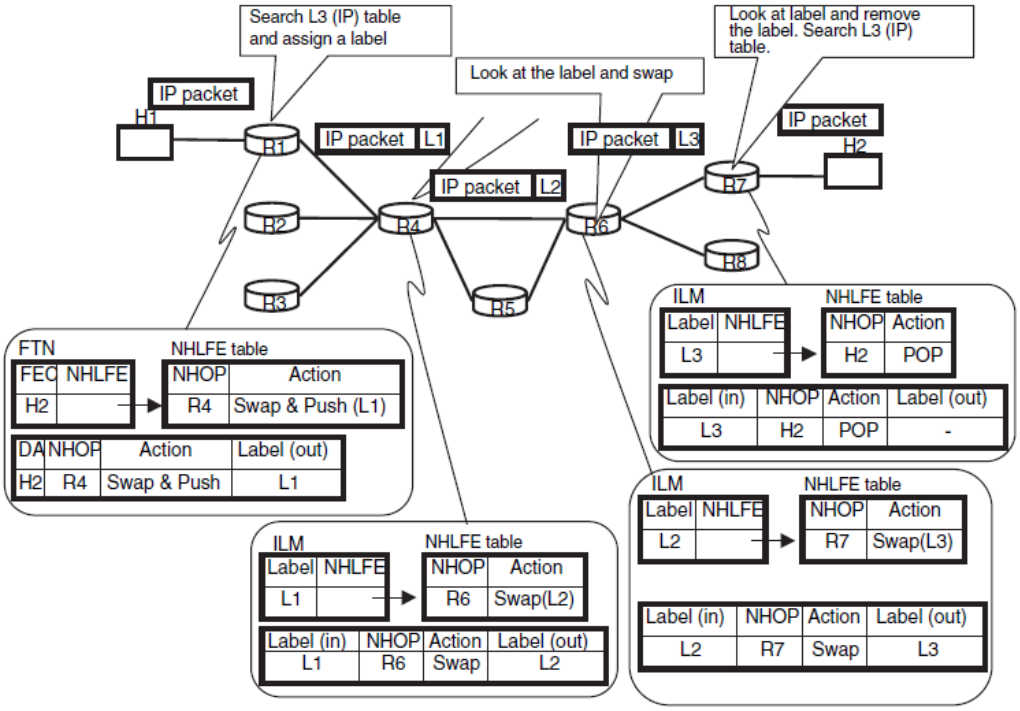
Όπως επισημάνθηκε και προηγουμένως μια MPLS ετικέτα επισυνάπτεται σε ένα πεδίο που καλείται Shim header, που είναι μία 32–bit επικεφαλίδα τοποθετούμενη με τη σειρά της στο IP πακέτο. Αυτή η επιπρόσθετη ποσότητα πληροφορίας αποτελείται από το περιεχόμενο της ετικέτας **label value** (20 bits), ένα **Exp** bit (3 bits), ένα **stack–indication** bit (1 bit), και το **TTL** πεδίο (8 bits). Το EXP bit είναι δεσμευμένο για μελλοντική χρήση και χρησιμοποιείται για αντιστοίχηση κλάσεων υπηρεσιών κατά τον προσδιορισμό της ποιότητας υπηρεσιών QoS σε ένα IP/MPLS δίκτυο. Το stack–indication bit χαρακτηρίζει την σωρό ετικετών. Είναι εφικτό να δημιουργήσουμε αυτή τη σωρό με το να αντιστοιχηθούν πολλαπλές ετικέτες σε ένα IP πακέτο. Εάν αυτό το bit έχει τεθεί η ετικέτα βρίσκεται στο τέλος της σωρού. Το TTL πεδίο έχει τον ίδιο ρόλο με αυτόν στο IP πακέτο, και χρησιμοποιείται να εμποδίζει τα πακέτα από το να κυκλοφορούν επ'άπειρον στο δίκτυο έπειτα από πρόκληση transmission loops –βρόχων μετάδοσης. Κάθε φορά που εισέρχεται ένα πακέτο στο MPLS δίκτυο, το TTL περιεχόμενο της MPLS επικεφαλίδας μειώνεται κατά 1 , σε κάθε μετάδοση του πακέτου, μέχρι να μηδενιστεί, οπότε και απορρίπτεται από το

δίκτυο. Τέλος, στη περίπτωση που χρησιμοποιήσουμε τη τεχνολογία ATM στο επίπεδο 2, είναι δυνατό να πάρουμε το VPI/VCI πεδίο ως MPLS ετικέτα, ενώ εάν κάνουμε χρήση Frame Relay, μπορούμε να πάρουμε το DLCI.



Εικόνα 34. Ενθυλάκωση MPLS ετικέτας στα παραδοσιακά πρωτόκολλα μεταφοράς

Υπάρχουν τρείς τύποι πινάκων ετικετών: **NHLFE, FTN** και **ILM**. Ο πρώτος τύπος NHLFE –Next Hop Label Forwarding Entry είναι ένας πίνακας που περιγράφει την σχετιζόμενη με τα MPLS πακέτα διαδικασία. Σε κάθε καταχώρηση στον πίνακα αυτόν πληροφορία όπως ο επόμενος κόμβος και πως να επεξεργαστεί η εκάστοτε ετικέτα καταγράφεται. Οι διαθέσιμες επιλογές για την επεξεργασία της ετικέτας είναι: **label exchanging, label hopping, και label pushing.** Ο δεύτερος τύπος FTN –FEC–to–NHLFE αποτελεί ένα πίνακα που αντιστοιχίζει το FEC στο NHLFE, και χρησιμοποιείται να αποδίδει ετικέτα σε ένα πακέτο που δεν διαθέτει ακόμα. Ο τελευταίος πίνακας ILM – Incoming Label Mapping αντιστοιχίζει την ετικέτα στο NHLFE και αποφασίζει τον διαθέσιμο τρόπο επεξεργασίας της. Στην εικόνα 35 βλέπουμε ένα παράδειγμα και των τριών τρόπων επεξεργασίας ετικέτας. Οι R1 και R7 είναι LER's, ενώ οι R4 και R6 LSR's. Ο H1 μεταδίδει IP πακέτα που προορίζονται στον R1 και H2, ενώ ο R1 αρχικά κάνει αναζήτηση στον FTN πίνακα και αποφασίζει την NHLFE καταχώρηση που αντιστοιχεί στην κλάση ισοδύναμης προώθησης FEC με προορισμό τον H2. Σε αυτή τη καταχώρηση καταγράφεται οτι ο επόμενος κόμβος NHOP είναι ο R4, και οτι πρέπει να τοποθετηθεί η ετικέτα L1 (Swap&Push(L1)). Έτσι ο R1 με βάση αυτές τις πληροφορίες μεταφέρει τα IP πακέτα στον R4. Στους επόμενους δύο ενδιάμεσους κόμβους R6 και R7 επαναλαμβάνεται η ίδια διαδικασία αλλά με ενέργειες επεξεργασίας Swapping στις αντίστοιχες ετικέτες, αυτή τη φορά. Τέλος η τελευταία διαδικασία που εκτελείται πάνω στην ετικέτα είναι μία πράξη Pop , δηλαδή αφαίρεση ετικέτας απο τον Edge Router R7. Εδώ να σημειώσουμε οτί στο MPLS είναι εφικτό να τοποθετηθούν οποιοσδήποτε αριθμός από ετικέτες στα IP πακέτα. Με αυτόν τον τρόπο δημιουργείται ένα ιεραρχικό LSP δίκτυο μέσω του label stacking , δηλαδή του σωρού ετικετών.



Εικόνα 35. Label Stack επεξεργασία (Exchange, Push, and Pop)

Στο σημείο εξόδου –egress στο MPLS δίκτυο, δύο τύποι αναζήτησης απαιτούνται:label–table αναζήτηση και IP route–table αναζήτηση. Για την επιτάχυνση της διαδικασίας αυτής έχει προταθεί μία μέθοδος που καλείται Penultimate–hop popping (PHP). Στον αμέσως προηγούμενο κόμβο πριν τον LER εξόδου, αφού γίνει η αναζήτηση στον πίνακα ετικετών, τοποθετείται η ετικέτα εξόδου και τα πακέτα προωθούνται στον egress router. Επειδή έτσι και αλλιώς η διαδικασία Popping πραγματοποιείται στον LER ταυτόχρονα με το IP routing table searching, για μείωση του επιπλέον φορτίου κίνησης και άρα για αύξηση της ταχύτητας προτείνεται η αφαίρεση της ετικέτας να γίνεται στον LSR ένα hop πριν τον exit–side LER, και η IP αναζήτηση να πραγματοποιείται κανονικά στον τελευταίο.

Τέλος να αναφέρουμε οτί υπάρχουν δύο τύποι μονοπατιών που μπορούν να εγκατασταθούν γιά ένα LSP :hop–by–hop τύπος LSP, και explicit–route τύπος LSP. Στην πρώτη κατηγορία σε οποιαδήποτε αλλαγή της τοπολογίας στο δίκτυο, ή σε αλλαγή της πολιτικής δρομολόγησης, το LSP μονοπάτι μπορεί να αλλάξει. Στο explicit–route αντιθετα LSP το μονοπάτι είναι προκαθορισμένο. Αυτός ο τύπος χρησιμοποιείται κυρίως για μηχανισμούς και πολιτικές traffic engineering.

Μέχρι στιγμής έχουμε δεί πώς το MPLS χρησιμοποιεί ετικέτες για την πραγματοποίηση του forwarding των πακέτων, αλλά μένει ακόμη να ξεκαθαρίσουμε πώς οι δεσμεύσεις μεταξύ labels και FECs διανέμονται σε ολόκληρο το δίκτυο. Εφόσον η μη αυτόματη παραμετροποίηση δεν είναι η βέλτιστη επιλογή, είναι ξεκάθαρη η ανάγκη για την εύρεση ενός πρωτοκόλλου ώστε να ανακτά αυτή τη πληροφορία. Από μία πρακτική οπτική γωνία υπάρχουν 2 επιλογές: (α) να υλοποιηθεί ένα νέο πρωτόκολλο που θα διανέμει τις δεσμεύσεις ετικετών ή (β) να επεκταθεί ένα ήδη υπάρχον που θα μεταφέρει τις ετικέτες μαζί

με πληροφορία δρομολόγησης. Για την επίτευξη ενός μεγαλύτερου συμβιβασμού, η κοινότητα τυποποίησης εφείυρε το πρωτόκολλο LDP –Label Distribution Protocol, και ταυτόχρονα επέκτεινε δυο προυπάρχοντα το RSVP –Resource Reservation Protocol και το BGP –Border Gateway Protocol.

Το Label Distribution Protocol είναι προιόν εργασίας του MPLS Working Group της IETF. Αντίθετα με τα υπάρχοντα RSVP και BGP που επεκτάθηκαν ώστε να υποστηρίζουν label distribution, το LDP είναι σχεδιασμένο εξειδικευμένα γι'αυτό το σκοπό. Το πρωτόκολλο αυτό δεν επιχειρεί να πραγματοποιήσει λειτουργίες δρομολόγησης και γι'αυτούς τους ρόλους βασίζεται σε ένα Interior Gateway Protocol –IGP. Μάλιστα στην αρχική του έκδοση ορίστηκε να εγκαθιδρύει LSP's για κλάσεις ισοδύναμης προώθησης FEC που αναπαριστούσαν IPv4 ή IPv6 διευθύνσεις. Ο πυρήνας λειτουργικότητας του LDP βασίζεται σε ανταλλαγή μυνημάτων μεταξύ κόμβων του δικτύου. Οι υποψήφιοι γείτονες ανιχνεύονται αυτόματα μέσω της πολυεκπομπής HELLO μηνυμάτων σε μια καθορισμένη UDP θύρα. Μόλις ένας υποψήφιος γείτονας ανακαλυφθεί, μία TCP σύνδεση εγκαθιδρύεται και η περίοδος LDP ξεκινάει. Έπειτα από την φάση αρχικοποίησης μεταξύ των κόμβων, αυτοί ανταλλάσουν πληροφορία σχετικά με τις δεσμεύσεις των ετικετών με τις κλάσεις FEC's πάνω στην TCP σύνδεση αυτή. Στην απουσία περιοδικής πληροφορίας ανάμεσα στους κόμβους, αποστέλλονται μυνήματα keepalive για την συντήρηση της σύνδεσης. Ο κυρίαρχος κανόνας της λειτουργίας του LDP είναι οτι εάν για παράδειγμα ο LSR A λάβει την αντιστοίχηση της ετικέτας L για την FEC κλάση F από τον γειτονικό του κόμβο LSR B, θα χρησιμοποιήσει την ετικέτα αυτή γιά λόγους προώθησης αν και μόνο αν ο B ανήκει στο IGP συντομότερο μονοπάτι με προορισμό το F. Φυσικά ο κύριος λόγος της διανομής των δεσμεύσεων αυτών μεταξύ ετικετών και FEC's είναι η εγκαθίδρυση των LSP's μονοπατιών στο δίκτυο. Είναι προφανές οτι η επιλογή των FEC's που θα διανεμηθούν καθορίζει και την επιλογή του αντίστοιχου LSP που θα εγκατασταθεί. Γι'αυτο το σκοπό έχουν προταθεί διάφορες πολιτικές που μπορούν μάλιστα να συνυπάρχουν στην ίδια τοπολογία.

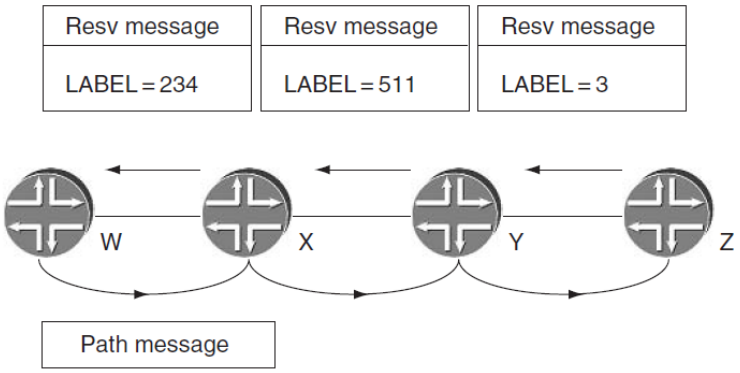
Ένα πολύ σημαντικό ζήτημα όσον αφορά το ποιός αναθέτει τις ετικέτες, δηλαδή το label distribution mode, είναι οτι κατά το χτίσιμο του πίνακα πρόωθησης , εάν θα πρέπει να παίρνουμε το τοπικά επιλεγόμενο label ως εισερχόμενη ή εξερχόμενη ετικέτα. Η MPLS αρχιτεκτονική κάνει χρήση του downstream label assignment, που σημαίνει οτι ο router περιμένει να λάβει τη κίνηση με την ετικέτα που πήρε από το τοπικό πίνακα. Στο MPLS δίκτυο η κίνηση κατευθύνεται προς την αντίθετη πορεία από την διανομή ετικετών. Αυτή άλλωστε είναι και η downstream λογική που εξηγήσαμε.

Ένας εναλλακτικός μηχανισμός για την διανομή ετικετών στα LSP's μονοπάτια μεταφορών βασίζεται στο **Resource Reservation Protocol –RSVP**. Το συγκεκριμένο πρωτόκολλο επινοήθηκε πριν ακόμη γεννηθεί το MPLS και χρησιμοποιήθηκε αρχικά σαν ένα σχήμα για τη δημιουργία δεσμέυσεων εύρους ζώνης για μεμονωμένες ροές κίνησης σαν μέλος του λεγόμενου **int–serv** μοντέλου. Παρά ωστόσο τα αρχικά προβλήματα κλιμάκωσής του, στο περιεχόμενο του MPLS, το RSVP επεκτάθηκε ώστε να υποστηρίζει την δημιουργία και συντήρηση των LSP's , και να πραγματοποιεί τις αντίστοιχες δεσμεύσεις ταχύτητας. Τα όποια θέματα κλιμάκωσης που παρουσιάζονταν αρχικά, τώρα εμφανίζουν μειωμένη βαρύτητα επειδή η όλη κίνηση αντιστοιχίζεται πλέον σε ένα μοναδικό LSP, το οποίο με τη σειρά του απαιτεί μόνο μια RSVP σύνοδο που περιλαμβάνει πολλές end–to–end ροές. Το σημαντικό εκείνο σημείο που διακρίνει το RSVP είναι οτι ένα LSP σηματοδοτούμενο με το συγκεκριμένο πρωτόκολλο ελέγχου, δεν ακολουθεί κατ'ανάγκην τις απαιτήσεις καθορισμού μονοπατιού από το IGP. Το RSVP διαθέτει αποκλειστικές ιδιότητες δρομολόγησης στο βαθμό που ο ingress router καθορίζει ολόκληρο το απο άκρου σε

άκρου μονοπάτι που πρέπει να ακολουθήσει το LSP, ή τους ενδιάμεσους κόμβους που πρέπει να διασχίσει.

Η δημιουργία του RSVP–σηματοδοτούμενου LSP μονοπατιού ξεκινάει από τον ingress LER. Αυτός στέλνει το RSVP path μύνημα. Η διεύθυνση προορισμού του μυνήματος αυτού είναι ο egress LER. Ενδεικτικά τα πεδία που περιέχει το Path message είναι τα ακόλουθα:

1. **Label Request Object**. Κάνει αίτηση για μία MPLS ετικέτα για το μονοπάτι. Σαν αποτέλεσμα ο egress και οι ενδιάμεσοι routers κάνουν κατανομή της ετικέτας για το συγκεκριμένο LSP.
2. **Explicit Route Object (ERO)**. Το ERO πεδίο περιέχει τις διευθύνσεις των κόμβων που περνάει το LSP.
3. **Record Route Object (RRO)**. Το RRO απαιτεί την καταγραφή των διευθύνσεων των transit hops από τα οποία περνάει το LSP μονοπάτι. Με αυτό το τρόπο ένας router μπορεί να εντοπίσει routing loops –ατέρμονους βρόχους δρομολόγησης σε περίπτωση που εντοπίσει την διεύθυνσή του στο RRO.
4. **Sender TSpec**. Το πεδίο αυτό ζητάει από τον ingress router να ζητήσει δεσμεύσεις bandwidth.



Εικόνα 36. Ανταλλαγή RSVP Path και Resv μυνημάτων

Σε απάντηση στο Path message, ο egress router στέλνει ένα Resv μύνημα. Εδώ να σημειώσουμε οτι ο router αυτός απευθύνει το μύνημα στους διαδοχικούς του κόμβους με τρόπο upstream –ανοδικό, αντί να το αποστέλλει κατ'ευθείαν στη πηγή. Με αυτό το τρόπο κάθε LSR που ανήκει στο συγκεκριμένο μονοπάτι επαναλαμβάνει την ίδια διαδικασία. Το RSVP απαιτεί περιοδικά ανταλλαγή μυνημάτων από τη στιγμή που εγκαθιδρυθεί ένα LSP μονοπάτι ώστε να συντηρεί –refresh τη κατάστασή του. Αυτό επιτυγχάνεται με την εκατέρωθεν αποστολή Path και Resv μηνυμάτων για κάθε ενεργό μονοπάτι. Εαν ο router δεν λάβει ένα συγκεκριμένο αριθμό μυνημάτων για ένα καθορισμένο LSP, τότε το θεωρεί μη απαραίτητο (ενεργό), και αφαιρεί όλες τις καταστάσεις του όπως πίνακες προώθησης και δεσμεύσεις bandwidth. Μάλιστα το RSVP διαθέτει και ένα μηχανισμό ανίχνευσης αστοχίας κόμβου, κατα τον οποίο hello μυνήματα στέλνονται περιοδικά μεταξύ των κομβων του δικτύου. Με την πάροδο κάποιου χρονικού διαστήματος, συνήθως μεγάλου, ένας κόμβος ανιχνεύει την κατάρρευση κάποιου γείτονά του μέσα από το timeout –χρονική λήξη των RSVP συνόδων.

3.1.2 TRAFFIC ENGINEERING ΚΑΙ MPLS (MPLS–TE)

Η διαδικασία ελέγχου του μονοπατιού μέσα από το οποίο διακινείται η κίνηση στο δίκτυο καλείται Traffic Engineering –TE. Υπάρχουν πολλοί λόγοι γιατί οι διαχειριστές δικτύων επιθυμούν να επηρεάζουν τα χαρακτηριστικά ενός μονοπατιού, ένας από τους οποίους είναι η βελτιστοποίηση της χρήσης των δικτυακών πόρων. Ο σκοπός είναι απλός:**αποφυγή της κατάστασης όπου ορισμένα τμήματα του δικτύου παρουσιάζουν συμφόρηση όταν άλλα υποχρησιμοποιούνται**. Άλλοι σημαντικοί λόγοι είναι το μονοπάτι να διαθέτει ορισμένους περιορισμούς –constraints (παράδειγμα να μην κάνει χρήση συνδέσμων μεγάλης καθυστέρησης) , ώστε σε περιπτώσεις κατάρρευσης γραμμής να εξασφαλίζεται δίκαιη προτεραιότητα κατά τη διανομή της κίνησης. Μέσα από τη διαδικασία αυτή του Traffic Engineering προσφέρονται νέες υπηρεσίες με εκτεταμένες εγγυήσεις ποιότητας υπηρεσιών, ενώ μειώνονται οι επενδύσεις σε νέους δικτυακούς πόρους, όπως εύρος ζώνης, μέσω της βελτιστοποίησης της χρήσης ήδη υπαρχόντων. Έχει αποδειχθεί στη πράξη οτι η τεχνολογία του MPLS , και κατ'επέκτασιν ο διάδοχος του το Generalized, προσφέρουν την απαιτούμενη επιχειρησιακή ευελιξία ταυτόχρονα με την απλότητα για την υλοποίηση πολύπλοκων πολιτικών TE.

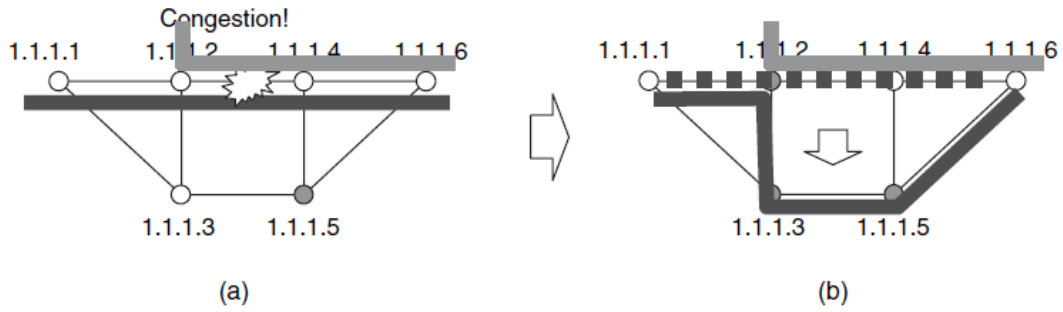
Ανεξάρτητα με το όποιο σενάριο κίνησης απαιτηθεί σε ένα MPLS δίκτυο, ο μηχανισμός του Traffic Engineering υλοποιείται σε δύο στάδια:υπολογισμός του μονοπατιού που ικανοποιεί ένα σύνολο από constraints, και προώθηση της κίνησης μέσα από αυτό το μονοπάτι. Το MPLS–TE χρησιμοποιεί LSP priorities ώστε να μαρκάρει κάποια Label Switched Paths ως περισσότερο σημαντικά σε σχέση με κάποια άλλα, ώστε τα πρώτα να δεσμεύσουν πόρους από τα τελευταία. Μέσα από αυτό εξασφαλίζονται τα ακόλουθα:

1. Σε περίπτωση απουσίας των περισσότερο σημαντικών LSP's, οι πόροι μπορούν να δεσμευτούν από τα λιγότερο σημαντικά.
2. Ένα σημαντικό LSP εγκαθιδρύεται πάντα μέσα από το συντομότερο μονοπάτι που ικανοποιεί τους περιορισμούς, ανεξάρτητα από υπάρχουσες δεσμεύσεις.
3. Όταν LSP's χρειάζεται να αλλάξουν μονοπάτι, ύστερα από κατάρρευση γραμμής, τα περισσότερο σημαντικά από αυτά έχουν μεγαλύτερη πιθανότητα να ανακαλύψουν το εναλλακτικό μονοπάτι.

Όσον αφορά τις προτεραιότητες των LSP's το MPLS–TE καθορίζει 8 επίπεδα, με το 0 ως το βέλτιστο και το 7 ως το χειρότερης προτεραιότητας. Ένα LSP διαθέτει δύο priorities:το **setup priority** και το **hold priority**. Ο πρώτος τύπος προτεραιότητας είναι υπεύθυνος για τον έλεγχο των πόρων τη στιγμή που ένα μονοπάτι εγκαθιδρύεται, ενώ ο δεύτερος πραγματοποιεί έλεγχο της πρόσβασης στους πόρους σε ένα LSP που έχει ήδη εγκαθιδρυθεί. Όταν ένα μονοπάτι αρχικοποιείται εάν δεν υπάρχουν διαθέσιμα αρκετά resources, το setup priority του νέου LSP συγκρίνεται με το hold priority των ήδη υπαρχόντων μονοπατιών που κάνουν χρήση των πόρων στο δίκτυο , ώστε να διαπιστωθεί αν πράγματι μπορεί να κάνει preempt τα υπάρχοντα LSP's και να πάρει τους πόρους τους. Εάν κάτι τέτοιο επιτευχθεί τα υπόλοιπα LSP's αποτρέπονται. Έχει αποδειχθεί μάλιστα οτι αναθέτοντας ένα σημαντικό hold priority, έστω 0, και ένα λιγότερο σημαντικό setup priority, έστω 7, σε ένα LSP, κάτι τέτοιο εξασφαλίζει δικτυακή σταθερότητα. Αυτό είναι το αποτέλεσμα του ανταγωνισμού των μονοπατιών για πόρους σε ένα δικτυακό περιβάλλον, ιδιαίτερα μάλιστα ύστερα από περιπτώσεις αστοχίας όπως κατάρρευση γραμμής.

Όπως αναφέρθηκε και σε προηγούμενες ενότητες στο IGP(Interior Gateway Protocol) σύνολο πρωτοκόλλων, όπως στο **OSPF(Open Shortest Path First)** ή **IS–IS (Intermediate System to Intermediate System)**, ένα μονοπάτι επιλέγεται με τέτοιο

τρόπο ώστε το άθροισμα του συνολικού κόστους που κατανέμεται σε κάθε σύνδεσμο να είναι το ελάχιστο. Το μονοπάτι αυτό δεν αλλάζει ακόμη και όταν οι συνθήκες κίνησης στο δίκτυο αλλάξουν, και τα πακέτα μεταφέρονται κατα μήκος του ακόμη και με τη παρουσία συμφόρησης. Στην εικόνα 37(α) διακρίνουμε ένα παράδειγμα όπου κίνηση από τον δρομολογητή 1. 1. 1. 2 στον δρομολογητή 1. 1. 1. 6, και αντίστοιχα από τον 1. 1. 1. 4 στον 1. 1. 1. 6, συγκρούονται, δημιουργώντας συμφόρηση. Σε αυτή τη περίπτωση είναι εφικτό να αποφύγουμε τη δημιουργία αυτής της συμφόρησης με το να αλλάξουμε το μονοπάτι από τον 1. 1. 1. 1 router στον 1. 1. 1. 6 όπως φαίνεται στην εικόνα 37(β). Επειδή ωστόσο η δρομολόγηση στα IGP πρωτόκολλα καθορίζεται από τη διεύθυνση προορισμού των πακέτων, είναι αδύνατον να αλλάξουμε το μονοπάτι των πακέτων με την ίδια διεύθυνση παραλήπτη. Στο IGP δεν υπάρχει καμία λειτουργικότητα να γίνεται αλλαγή της πορείας του μονοπατιού δυναμικά σε εξάρτηση με τις συνθήκες κίνησης στο δίκτυο, ακόμη και όταν υπάρχει συμφόρηση σε ένα σύνδεσμο και τα πακέτα ακολουθούν το συντομότερο μονοπάτι. Έτσι η διαδικασία της μεταγωγής μονοπατιού ώστε να λαμβάνονται υπόψιν οι συγκυρίες κυκλοφορίας στο δίκτυο, τεχνική που καλείται όπως είπαμε Traffic Engineering, είναι αδύνατη στο συγκεκριμένο πρωτόκολλο.

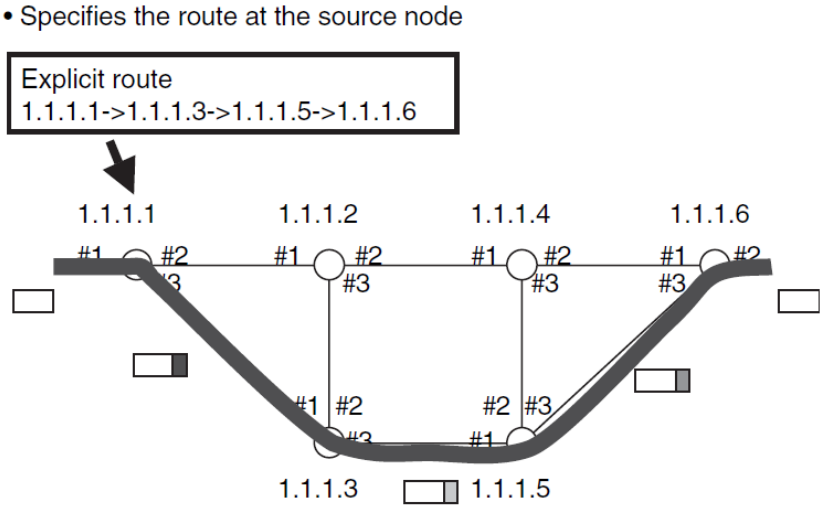


Εικόνα 37. Διαχειριστικά προβλήματα του IGP

Είχαμε τονίσει και σε προηγούμενες ενότητες οτί το MPLS framework συνδυάζει τις λειτουργικότητες της connection–oriented και connectionless συμπεριφοράς. Τα πακέτα στο δίκτυο προωθούνται με βάση ενός πίνακα ετικετών –label table που υπάρχει σε κάθε LSR της διαδρομής. Στο MPLS είναι εφικτό να εγκαθιδρύσουμε ένα LSP μονοπάτι με το να διευθετήσουμε τον πίνακα ετικετών σε κάθε LSR της διαδρομής ύστερα από τον καθορισμό του μονοπατιού αυτού. Με αυτή την οπτική αντιλαμβανόμαστε οτι **η προώθηση των πακέτων (forwarding) και ο έλεγχος της δρομολόγησης (route control) είναι ξεχωριστές διεργασίες**. Αν το συγκρίνουμε τώρα με το συμβατικό IP πρωτόκολλο θα δούμε οτι στο τελευταίο οι ίδιες διαδικασίες είναι ενοποιημένες.

Η τεχνική του Source Routing έγκειται στην εγκατάσταση ενός LSP πάνω σε ένα προκαθορισμένο μονοπάτι στο MPLS για την αποφυγή συμφόρησης. Η εγκαθίδρυση του LSP πάνω σε ένα μονοπάτι μπορεί να γίνει είτε λαμβάνοντας κάποιες μετρήσεις–συμβάσεις στον κόμβο προέλευσης **(source routing)**, είτε με τον καθορισμό της πληροφορίας δρομολόγησης μέσω μυνημάτων σηματοδοσίας **(explicit route –ER)**. Στην εικόνα 38 διακρίνουμε τους δύο μηχανισμούς. Το μονοπάτι **1. 1. 1. 1–>1. 1. 1. 3–>1. 1. 1. 5–>1. 1. 1. 6** που εγκαθίσταται με αυτό το τρόπο καλείται **Explicit Route LSP –ER–LSP**. Τέλος υπάρχουν 2 τρόποι να καθορίσουμε ένα μονοπάτι:ο **loose** και ο **strict**. Στον πρώτο καθορίζουμε συγκεκριμένους κόμβους, δίκτυα ή αυτόνομα συστήματα σε ένα μονοπάτι, ενώ στον τελευταίο επιλέγουμε όλα τα στοιχεία του δικτύου. Ένα παράδειγμα ώστε να διακρίνουμε τη διαφορά αυτών των δύο τεχνικών είναι το μονοπάτι 0–1(s)–2(s)–3(s)–4,

όπου το γράμμα 's' δηλώνει το strict και οτι στη περίπτωση του 1(s), ο γειτονικός κόμβος πρέπει να είναι ο 1. Αντίθετα στο μονοπάτι 0–2(l)–4, το γράμμα 'l' σημαίνει loose και το 2 οτι ο γειτονικός κόμβος δε θα πρέπει να είναι ο 2.



Εικόνα 38. Source και Explicit Routing

Traffic Trunk καλείται το σύνολο–άθροισα των ροών κίνησης της ίδιας κλάσης ισοδύναμης προώθησης και μεταφέρεται πάνω σε ένα ER–LSP. Διακρίνουμε τα ακόλουθα χαρακτηριστικά ενός traffic trunk:

Traffic Parameter. Δείχνει τα χαρακτηριστικά της κίνησης ενός trunk, όπως bit rate, average bit rate, burst size, κτπ

Generic Path Selection and Management. Το path selection rule αποφασίζει το συντομότερο μονοπάτι που επιλέγει το IGP, καθώς και εαν η επιλογή του μονοπατιού θα πρέπει να βασίζεται σε συνθήκες πολιτικών ή διαθέσιμων πόρων, ενώ το path management rule καθορίζει εαν το επιλεγμένο μονοπάτι θα πρέπει να ανακατασκευάζεται δυναμικά σύμφωνα με τις αλλαγές στη κατάσταση του δικτύου.

Resource–class affinity. Δείχνει ποιά κλάση διαθέσιμων πόρων θα πρέπει να χρησιμοποιηθεί ή να αφαιρεθεί. Μα αυτό το τρόπο πολιτικέ καθορισμού κίνησης μπορούν εύκολα να υλοποιηθούν.

Adaptivity. Δείχνει τον βαθμό προσαρμοστικότητας στις ενδεχόμενες αλλαγές των συνθηκών δικτύου. Με αυτό το τρόπο μπορεί να εγκαθιδρυθεί ένα LSP ώς το βέλτιστο μονοπάτι κάθε φορά που ένας πόρος καθίσται διαθέσιμος ή όταν κάποιος αποδεσμεύεται.

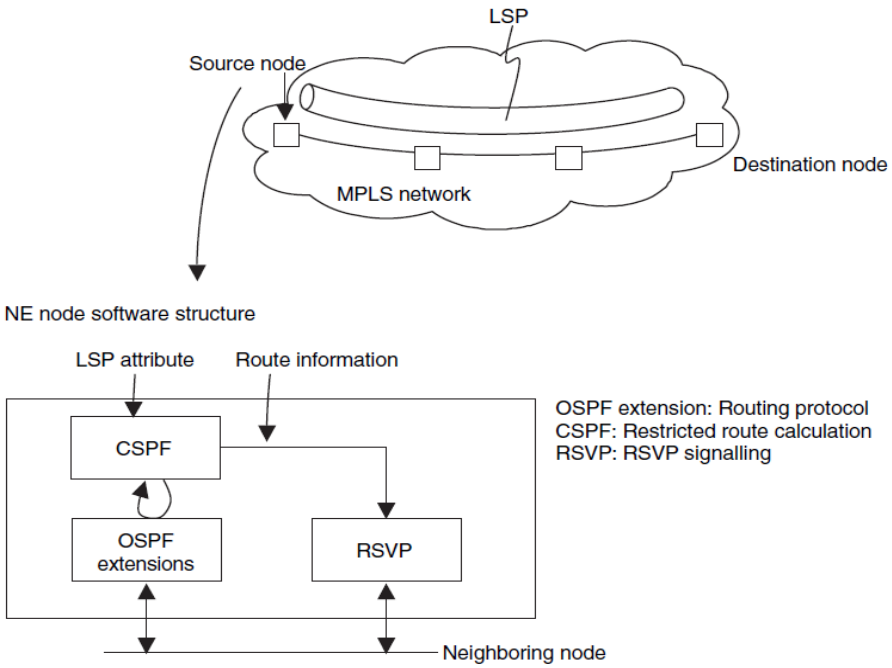
Priority. Καθορίζει τη προτεραιότητα των traffic trunks

Preemption. Είναι πεδίο που καθορίζει εαν κάποιο LSP μπορεί τόσο να αποδεμεύσει κάποιο άλλο LSP, όσο να αποδεσμευτεί και αυτό.

Resilience. Καθορίζει εαν θα επιτρέπεται η αλλαγή μονοπατιού –detour σε περίπτωση αστοχίας στο δίκτυο.

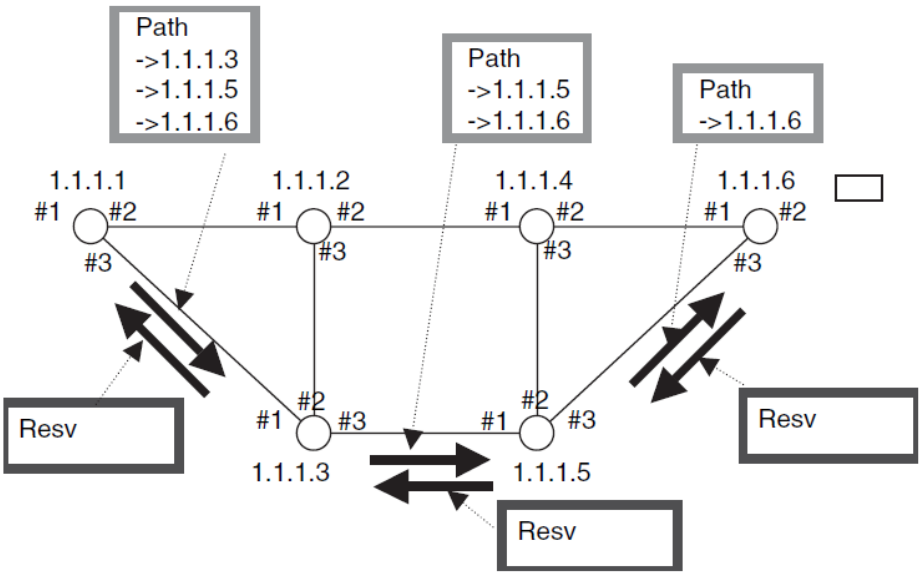
Μια πολύ ενδεικτική εικόνα είναι η 39. Όταν το attribute ενός traffic trunk, ενός πόρου, καθώς και οποιαδήποτε άλλη πληροφορία σχετιζόμενη με τη τοπολογία και κατάσταση της κάθε γραμμής δίνεται, το μονοπάτι που ικανοποιεί τις συνθήκες αυτές υπολογίζεται. Έτσι

μπορούμε να θεωρήσουμε την διαδικασία κατασκευής ενός μονοπατιού ως έναν αλγόριθμο–λευκό κουτί που δέχεται ως είσοδο–δεδομένα τα attributes και τη τοπολογία του δικτύου, και με βάση τα route–computation πρωτόκολλα Constraint–Based Shortest Path First (CSPF), καθώς και link–state OSPF και IS–IS, παράγει το τελικό μονοπάτι. Στο CSPF, ένα μονοπάτι , με βάση πάντα και τα attribute constraints, επιλέγεται εκτελώντας αλγόριθμους συντομότερου μονοπατιού όπως τον Dijkstra. Τέλος τις πληροφορίες για τη χρησιμοποίηση πόρων των συνδέσμων, οι διάφοροι κόμβοι τις αποκτούν μέσω των επεκτάσεων των link state πρωτοκόλλων OSPF και IS–IS.



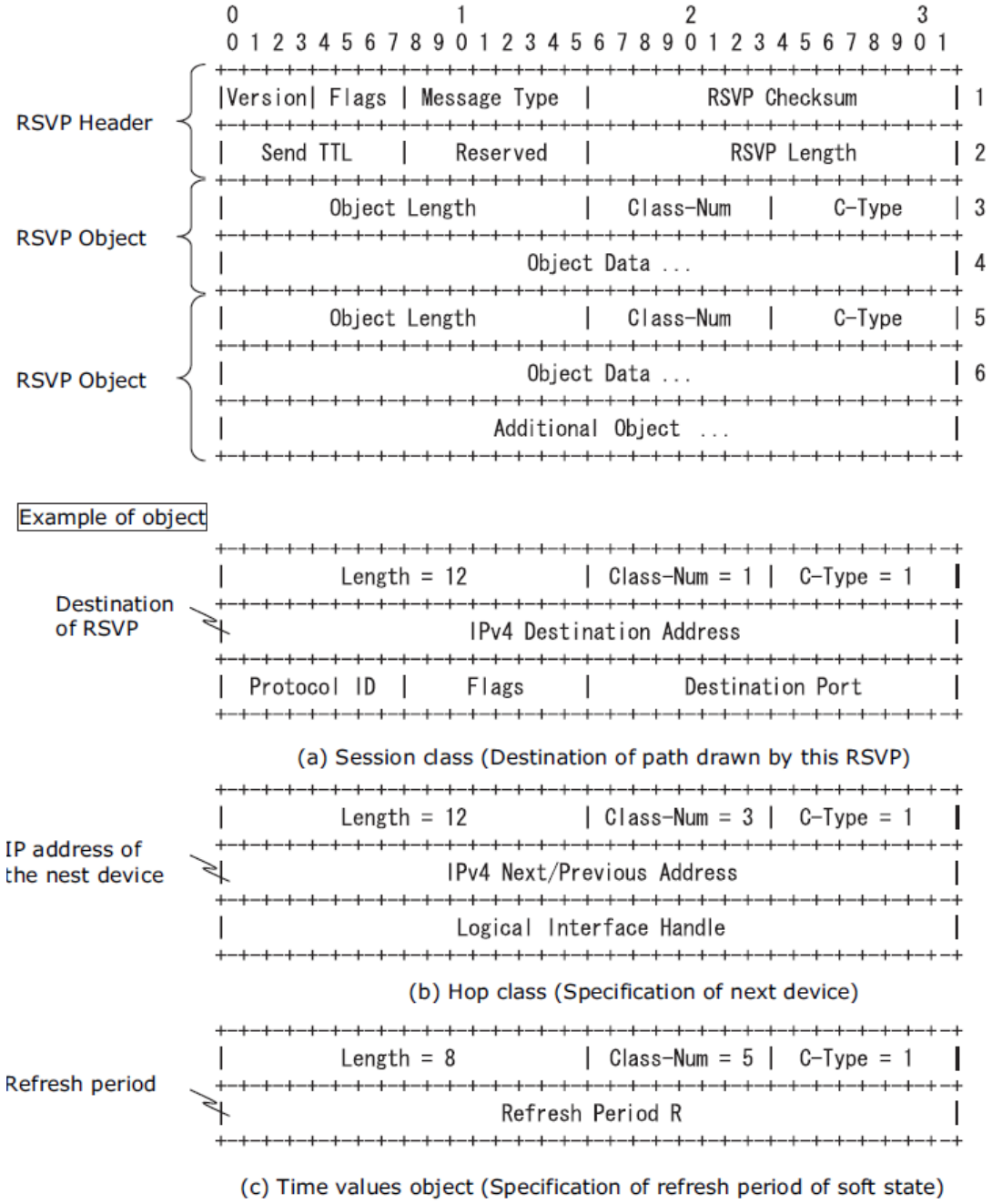
Εικόνα 39. Ο αλγόριθμος κατασκευής μονοπατιού

Στη συνέχεια θα περιγράψουμε τη διαδικασία σηματοδοσίας που χρησιμοποιείται κατα την εγκαθίδρυση ενός LSP. Υπάρχουν 2 πρωτόκολλα σηματοδοσίας:**RSVP–TE** και **CR–LDP**. Με την χρήση του πρωτοκόλλου RSVP–TE ένας αριθμός κόμβου κατά μήκος του μονοπατιού αντιστοιχίζεται σε ένα αντικείμενο που καλείται ERO –Explicit Route Object. Παίρνοντας για παράδειγμα την εικόνα 40, ο κόμβος 1. 1. 1. 1 δημιουργεί ένα PATH μύνημα που απευθύνεται στο κόμβο 1. 1. 1. 6, ώστε να εγκαθιδρύσει ένα ER–LSP μονοπάτι σε αυτόν. Σε αυτό το σημείο εισάγει το υποψήφιο μονοπάτι στο αντικείμενο ERO και το στέλνει στον επόμενο κόμβο 1. 1. 1. 3. Ο κόμβος αυτός αφού λάβει το PATH μύνημα, επεξεργάζεται το ERO πεδίο(δηλαδή το 1. 1. 1. 1–>1. 1. 1. 3–>1. 1. 1. 5–>1. 1. 1. 6), και αφού διακρίνει το δικό του αριθμό –id, το αφαιρεί από το ERO, και το προωθεί στον επόμενο γειτονικό κόμβο. Η ίδια διαδικασία επαναλαμβάνεται μέχρι τον κόμβο προορισμό. Όταν ο τελευταίος κόμβος αντιληφθεί οτι η διεύθυνση προορισμού του PATH μυνήματος ήταν αυτός, στέλνει με τη σειρά του ένα RESV message ξανά πίσω στον αρχικό κόμβο.



Εικόνα 40. Εγκατάσταση ER–LSP με το RSVP–TE

Να σημειώσουμε εδώ οτι το RSVP–TE είναι ένα πρωτόκολλο που επεκτείνει το παραδοσιακό RSVP. Το τελευταίο είναι ένα soft–state πρωτόκολλο σηματοδοσίας επιπέδου πάνω από το IP layer, με αριθμό 46. Η εικόνα 41 δείχνει το format των πακέτων του RSVP–TE. Ένα RSVP packet αποτελείται από ένα RSVP header και ένα RSVP object. Πολλαπλά RSVP objects μπορούν να συμπεριληφθούν σε ένα μοναδικό πακέτο. Τα ενδεικτικά πεδία που αποτελείται το header είναι: **Version, Flag, Message Type, RSVP Checksum, , TTL, RSVP Length.** Ο τύπος του RSVP object καθορίζεται στην επικεφαλίδα με βάσει τα πεδία class number και class type.



Εικόνα 41. RSVP message format

Να σημειώσουμε εδώ οτι στο PATH μύνημα περιλαμβάνεται το ERO object, και στο RESV το ERO και RRO –Record Route Object. Ενδεικτική είναι και η εικόνα 42 οπού διακρίνουμε τους διάφορους τύπους μυνημάτων RSVP.

TABLE 6.2
Message Type of RSVP

Value	Message Type
1	Path
2	Resv
3	PatrErr
4	ResvErr
5	PathTear
6	ResvTear
7	RescConf

Εικόνα 42. Τύποι μυνημάτων RSVP

Ας δούμε τώρα ένα παράδειγμα της διαδικασίας επεξεργασίας αντικειμένων RRO κατα τη φάση εγκατάστασης μονοπατιού. Όπως φαίνεται και στην εικόνα 40, για τη δημιουργία του LSP μονοπατιού από το κόμβο 0 στον κόμβο 4, ο πρώτος κόμβος θέτει το αντικείμενο 'label recording flag to session attribute' του PATH μυνήματος και καταγράφει το 0 ως το δικό του αριθμό κόμβου. Εαν ο επόμενος κόμβος είναι ο 1, όταν αυτός λάβει το PATH message, καταγράφει το 1 ως το δικό του αριθμό κόμβου στο RRO. Η διαδικασία αυτή επαναλαμβάνεται μέχρι και τον κόμβο προορισμού, οπότε και αυτός αποστέλλει με τη σειρά του ένα RESV μύνημα πίσω πάλι στον γειτονικό του κόμβο. Την ίδια στιγμή ο κόμβος 4 καταγράφει τον αριθμό του στο RRO. Όταν ληφθεί το RESV message απο τον επόμενο γειτονικό κόμβο, αυτός πάλι καταγράφει τον δικό του αριθμό στοαντικείμενο RRO. Και πάλι η ιδια διαδικασία πραγματοποιείται μέχρι τον αρχικό κόμβο. Με αυτούς τους 2 τρόπους ολοκληρώνεται η συλλογή της πληροφορίας δρομολόγησης του LSP. Τέλος να σημειώσουμε οτι κάθε ενδιάμεσος κόμβος στο μονοπάτι μπορεί με αυτές τις 2 διαδικασίες να συλλέξει τόσο ανοδική –upstream πληροφορία δρομολόγησης, όσο και καθοδική –downstream.

Το Traffic Trunk ενός LSP εγκαθίσταται κάνοντας χρήση του RSVP–TE. Το συγκεκριμένο αναγνωρίζεται με ένα tunnel identifier (Tunnel–ID). Συχνά είναι επιθυμητό ένα LSP να αντικαθίσταται από άλλο LSP κατά μήκος ενός μονοπατιού. Αυτό συμβαίνει όταν πρέπει να αλλάξουμε κάποια TE attributes–constraints με κάποια άλλα. Ένα LSP αναγνωρίζεται από το LSP identifier(LSP–ID). Το Tunnel–ID καταγράφεται στο Session object, ενώ το LSP–ID στο Session_Template Object. Το Session object τοποθετείται ρητά στα PATH και RESV μυνήματα, ενώ το Session_Template Object μόνο στο PATH message.

3.1.3 MPLS DIFFSERV–TE

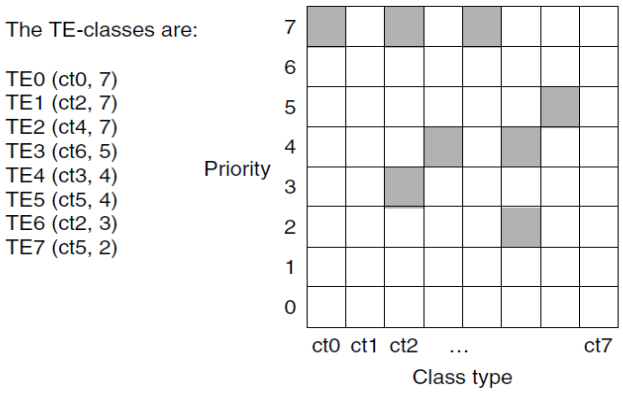
Στην προηγούμενη ενότητα είδαμε πώς ο μηχανισμός MPLS–TE επιτρέπει στους χρήστες να δημιουργούν μονοπάτια από σημείο–σε–σημείο μέσα στο δίκτυο με δεσμεύσεις εύρους ζώνης. Κάτι τέτοιο εγγυάται οι διαθέσιμοι πόροι που θα μεταφέρουν την όλη κίνηση θα είναι μικρότεροι ή ίσοι αυτών των δεσμεύσεων. Ένα σημαντικό μοινέκτημα, ωστόσο, του μοντέλου MPLS–TE είναι οτι δεν είναι ενήμερο των διαφορετικών κλάσεων DiffServ, που λειτουργούν στο συνολικό επίπεδο. Το συγκεκριμένο κείμενο κάνει μια μικρή εισαγωγή στο DiffServ ενημερωμένο MPLS–TE, που επεκτείνει το προηγούμενο μοντέλο με το να

επιτρέπει στις δεσμεύσεις αυτές του εύρους ζώνης να μεταφέρονται στο δίκτυο ανα επίπεδο κλάσεων. Το αποτέλεσμα είναι η ικανότητα του δικτύου να αποδίδει αυστηρές QoS εγγυήσεις, καθώς και βέλτιστη χρήση των πόρων του. Αυτό με τη σειρά του δίνει τη δυνατότητα στους διαχειριστές δικτύων να προσφέρουν υπηρεσίες με υψηλή απαίτηση σε πόρους, όπως φωνή, κινούμενη εικόνα, και σε τελική ανάλυση την ενοποίηση και σύγκλιση των πεδίων λειτουργικότητας που όπως θα δούμε στη συνέχεια κάνει εφικτή το GMPLS.

Οι σύγχρονες και πλέον απαιτητικές υπηρεσίες IP ζητούν αυστηρότερα επίπεδα SLA's – Service Layer Agreements, από ότι στα παραδοσιακά IP/MPLS δίκτυα. Τα SLA's ορίζουν την ποιότητα υπηρεσιών που διασταθμίζεται ανάλογα με τη συμπεριφορά κίνησης στο δίκτυο, και εκφράζεται με όρους όπως καθυστέρηση, διακύμανση καθυστέρησης (jitter), εγγυήσεις εύρους ζώνης και τεχνικές αποκατάστασης. Οι απαιτήσεις των SLA's μεταφράζονται σε δύο συνθήκες: (α) διαφορετικό χρονοπρογραμματισμό, πολιτικές ουράς, και συμπεριφορά απόρριψης πακέτων και (β) εγγυήσεις εύρους ζώνης βασισμένες σε κατηγορίες εφαρμογών. Βέβαια σε πρακτικό επίπεδο, με το να μαρκάρουν οι διαχεριστές δικτύων τις διάφορες εφαρμογές σε ξεχωριστές κλάσεις ποιότητας υπηρεσιών , ειδικά όταν η κίνηση ακολουθεί ένα συμφορημένο μονοπάτι δημιουργούνται διάφορα ζητήματα που θίγουν παραδοσιακές αντιλήψεις και στερεότυπα. Μιά εξ αυτών είναι οτι για να λυθεί η συμφόρηση πρέπει να 'ρίξουμε' περισσότερο bandwidth σε περιπτώσεις κατάρρευσης κόμβου ή και γραμμής. Κάτι τέτοιο αποδυκνείεται από σύγχρονες πρακτικές οτι κάθε άλλο παρα δίνει λύσεις. Λύση είναι η έξυπνη διαχείριση των διαθέσιμων πόρων, οι τεχνικές προστασίας των LSP's, οι μηχανισμοί reroute και το αυξημένο provisioning.

Στο μοντέλο DiffServ συναντάμε δύο τύπους κίνησης:best effort και guaranteed bandwidth. Το guaranteed bandwidth πρέπει να είναι συμβατό με ενα δεδομένο SLA. **Ο σκοπός είναι να προσφέρουμε το απαιτούμενο επίπεδο υπηρεσιών στο εγγυημένο εύρος ζώνης και ταυτόχρονα να κάνουμε traffic engineering στη best–effort κίνηση**. Η βασική απαίτηση του DiffServ–TE είναι να αντιστοιχούμε ξεχωριστές δεσμεύσεις εύρους ζώνης σε ξεχωριστές κλάσεις κίνησης. Για το σκοπό της αποθήκευσης του διαθέσιμου bandwidth για κάθε τύπο κίνησης το RFC3564 εισάγει την έννοια του τύπου κλάσης class type –CT. Επειδή το PHB –Per Hop Behavior καθορίζεται από τη προτεραιότητα ουράς και απόρριψης, ένα CT μπορεί να μεταφέρει κίνηση από περισσότερα από μία DiffServ κλάση υπηρεσιών. Μια πιθανή υλοποίηση είναι να αντιστοιχίζεται η κίνηση που μοιράζεται την ίδια συμπεριφορά χρονοπρογραμματισμού στο ίδιο CT. Τα IETF standards υποστηρίζουν μέχρι και 8 CT's αναφερόμενα από CT0 ως CT7. Κατά σύμβαση η best–effort κίνηση αντιστοιχίζεται στο CT0.

Στη προηγούμενη ενότητα είδαμε πως το CSPF υπολογίζει ένα μονοπάτι που συμμορφώνεται με καθοριζόμενα από το χρήστη constraints, όπως εύρος ζώνης και και χαρακτηριστικά συνδέσμων. Το DiffServ–TE προσθέτει το διαθέσιμο bandwidth σε καθε ένα από τα 8 CT's ώς ένα δεδομένο περιορισμό που μπορείνα εφαρμοσθεί σε ένα μονοπάτι. Για να επιτευχθεί ο υπολογισμός του μονοπατιού το διαθέσιμο bandwidth ανα CT σε όλα τα επίπεδα προτεραιότητας πρέπει να είναι γνωστό για καθε γραμμή. Αυτό σημαίνει οτι τα link–state IGP πρωτόκολλα οφείλουν να διαφημίζουν το διαθέσιμο εύρος ζώνης ανα CT σε καθε priority level σε κάθε γραμμή. Εφόσον υπάρχουν 8 επίπεδα προτεραιότητας και 8 CT's, συνολικά θα πρέπει να διαφημίζονται 64 τιμες απο τα link–state protocols. Ενδεικτικά αναφέρουμε οτι για λόγους απλότητας και εξοικονόμησης χρόνου, το IETF αποφάσισε να περιορίσει τον αριθμό των advertisements σε 8, και αυτα φαίνονται με τα σκιασμένα κελιά στο πίνακα 41.



Εικόνα 43. Διαλογή 8 ΤΕ κλάσεων από 64 συνολικούς συνδυασμούς

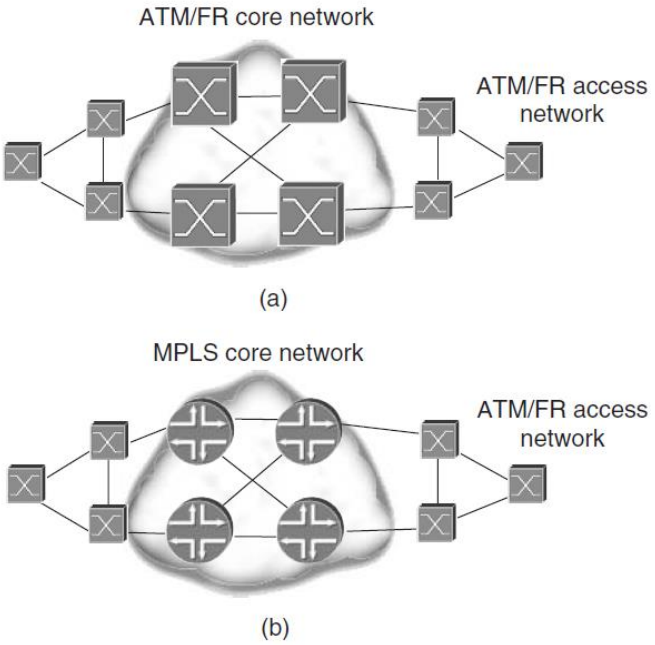
Στην συνέχεια αφού το μονοπάτι εγκατασταθεί σηματοδοτείται. Αναγκαίες επεκτάσεις στα ήδη υπάρχοντα πρωτόκολλα σηματοδοσίας είναι απαραίτητα, όπως το RSVP–TE και CR–LDP, έτσι ώστε να δημιουργούνται μονοπάτια με δεσμεύσεις εύρους ζώνης ανά CT. Η CT πληροφορία για ένα LSP μεταφέρεται στο πεδίο Class Type Object μέσα στο RSVP path μύνημα, και καθορίζει το CT από το οποίο απαιτείται η δέσμευση εύρους ζώνης. Βεβαίως το ερώτημα που τίθεται είναι πώς υπολογίζεται το διαθέσιμο bandwidth για κάθε απαιτούμενο Class Type. Γι'αυτό το θέμα έχουν προταθεί διάφοροι μηχανισμοί–μοντέλα όπως:

- **Maximum Allocation Model (MAM).** Το πλεονέκτημα του MAM είναι οτι απομονώνει εντελώς διαφορετικά CT's. Γι'αυτο ακριβώς οι προτεραιότητες δεν λαμβάνονται υπόψιν ανάμεσα σε LSP's που μεταφέρουν κίνηση από διαφορετικά CT's. Ο υπολογισμός του bandwidth γίνεται ως εξής: Για το CTn με προτεραιότητα p, αφαιρείται από το εύρος ζώνης που κατανέμεται στο CTn το άθροισμα όλων των bandwidth που κατανέμονται για τα LSP's των CTn σε όλα επίπεδα προτεραιότητας που είναι καλλίτερα ή ισα με το p. Το πρόβλημα με το μηχανισμό αυτό είναι οτι επειδή είναι αδύνατο να μοιραστούμε αχρησιμοποίητο εύρος ζώνης μεταξύ των CT's, το bandwidth μπορεί να σπαταλιέται αντί να χρησιμοποιείται για τη μεταφορά των άλλων CT.
- **Russian Dolls Model (RDM).** Το συγκεκριμένο μοντέλο βελτιώνει την αποτελεσματικότητα εύρους ζώνης του MAM με το να επιτρέπει CT's να μοιράζονται το bandwidth. Το CT7 αντιστοιχεί στην κίνηση με τις αυστηρότερες QoS απαιτήσεις και το CT0 είναι η best–effort κίνηση. Ο βαθμός της κοινής χρήσης του bandwidth κυμαίνεται ανάμεσα σ ε δύο άκρα:Από τη μια το BC7 είναι ένα σταθερό ποσοστό του εύρους ζώνης γραμμής που δεσμέυεται για κινηση από το CT7 μόνο. Από την άλλη το BC0 αντιπροσωπεύει ολόκληρο το link bandwidth και μοιράζεται από όλα τα CT's. Ανάμεσα σε αυτά τα δύο διακρίνουμε διάφορες διαβαθμίσεις όπως το BC6, BC5 κτπ.

3.1.4 ΜΕΤΑΦΟΡΑ ΕΠΙΠΕΔΟΥ 2 ΣΕ MPLS ΚΑΙ VPNS

Η μεταφορά επιπέδου 2 πάνω σε MPLS δίκτυα είναι στοιχείο κλειδί των multiservice networks, καθώς επιτρέπει στους διαχειριστές να μετοικίσουν από τεχνολογίες όπως Frame Relay, ATM και μισθωμενές γραμμές σε MPLS προσεγγίσεις, διατηρώντας παράλληλα τα χαρακτηριστικά υπηρεσιών από την οπτική γωνία του τελικού χρήστη. Η υποστήριξη layer 2 transport σε MPLS είναι καταλυτική για την εγκαθίδρυση Ιδιωτικών Εικονικών Δικτύων Virtual Private LAN –VLAN υπηρεσιών στο MPLS, όσο και για την νέα γενιά οπτικών εικονικών δικτύων, τα OVPN's –Optical Virtual Private Networks, μέσω του Generalized MPLS , όπως θα δούμε στη συνέχεια. Για τη πραγματοποιήση αυτής της μεταφοράς, δύο πρωτόκολλα σηματοδοσίας προσφέρονται:το LDP –Label Distribution Protocol, και το BGP –Border Gateway Protocol. Στα πλαίσια του πίνακα προώθησης –forwarding plane, αυτές οι δύο προσεγγίσεις είναι ίδιες. Ωστόσο από τη μεριά του πεδίου λειτουργικότητας ελέγχου –control plane διαφέρουν σημαντικά. Ένα μοναδικό σημείου–προς–σημείο Layer 2 στοιχείο σύνδεσης σε ένα MPLS δίκτυο καλείται ψευδοκύκλωμα –pseudowire , έτσι ώστε να ικανοποιείται η αρχή οτι το δίκτυο αυτό θα πρέπει τελικά να παραμένει αόρατο στο τελικό χρήστη.

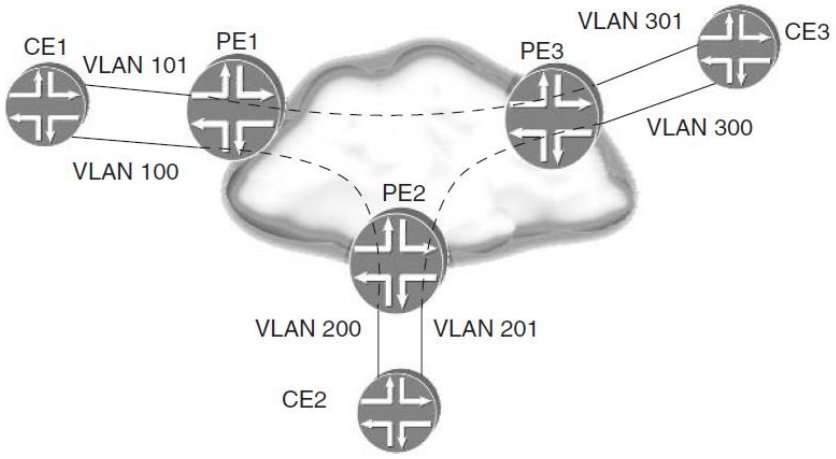
Οι Layer 2 υπηρεσίες υπήρχαν στο προσκήνιο για αρκετά χρόνια, βασισμένες στο Frame Relay ή ATM. Αυτές χρησιμοποιούνται από τους οργανισμούς να χτίζουν το εταιρικό τους Layer 2 VPN μέσω της διασύνδεσης των διαφόρων LAN's σε κλίμακα ευρείας περιοχής. Οι Service Providers προσφέρουν στους πελάτες τους τις IP υπηρεσίες σε παγκόσμια εμβέλεια, μέσω της μεταφοράς ATM cells ή Frame Relay frames πάνω στην ευρεία περιοχή με ένα συμφωνημένο bit–rate για κάθε κύκλωμα. Άλλες φορές πάλι οι υπηρεσίες αυτές μεταφέρουν κίνηση με περισσότερο αυστηρά επίπεδα SLA's στο δίκτυο, όπως video, voice over IP, τηλεματικές υπηρεσίες. Με την μετοίκιση τώρα των υπηρεσιών αυτών σε MPLS και κατ'επέκτασιν σε GMPLS δίκτυα(εφόσον υπάρχει οπτικός φορέας), μειώνονται τα λειτουργικά και επιχειρησιακά έξοδα του Service Provider, συγκρινόμενα με το να τρέχει τις ίδιες υπηρεσίες σε προηγούμενης γενιάς τεχνολογίες μέσω ξεχωριστών δικτύων Layer 2 και Layer 3 συνδεσιμότητας. Ένα άλλο πολύ σημαντικό δέλεαρ της μετάβασης αυτής στο MPLS είναι οι Ethernet υπηρεσίες επιπέδου 2, οι οποίες όταν χρησιμοποιούνται για την διασύνδεση των εταιρικών LAN's, μπορούν να θεωρηθούν σαν φυσική τους επέκταση σε ευρεία κλίμακα διατηρώντας μάλιστα την ευελιξία, απόδοση και φιλικότητα στο χρήστη που διακατέχει το Layer 2 πρωτόκολλο αυτό. Ακόμη και σε point–to–point Ethernet υπηρεσίες , όπως και σε multipoint –VLAN's, πάντα σε Layer 2 επίπεδο, τα MPLS δίκτυα εξασφαλίζουν την υποστήριξη μηχανισμών DiffServ–TE που δίνουν προτεραιότητα στη κίνηση κάθε κόμβου και παρέχουν πολιτικές προστασίας και αποφυγής συμφόρησης.



Εικόνα 44. Μετάβαση ATM ή FR core σε MPLS core: (a)πριν τη μετάβαση και (b)μετά

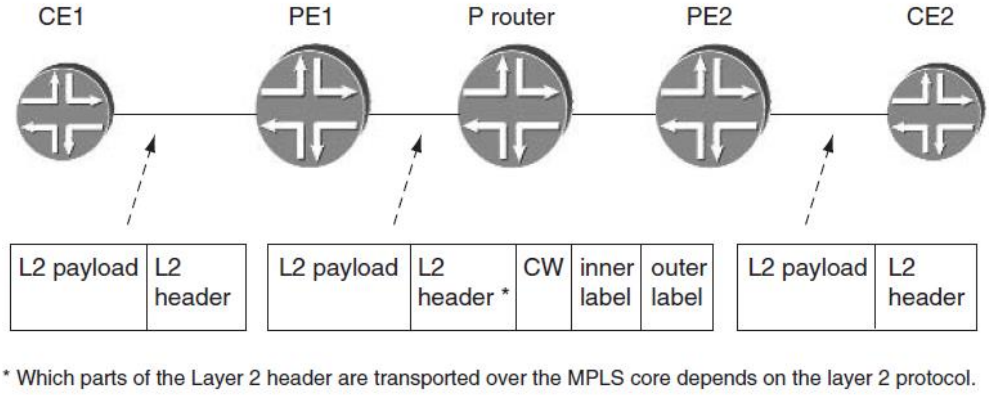
Να αναφέρουμε στο σημείο αυτό οτι υπάρχουν δύο μοντέλα για την VPN συνδεσιμότητα:το ομότιμο –peer και το μοντέλο επικάλυψης –overlay. Τα BGP/MPLS βασισμένα Layer 3 VPN's ανήκουν στο peer μοντέλο. Αντίθετα τα Layer 2 VPN αντιστοιχούν στη κατηγορία των overlay δικτύων. Υπάρχουν αρκετές διαφορές ανάμεσα στα VPN επιπέδου 2 και 3, και γι'αυτό το λόγο αλλά και για τη κάλυψη των ευρύτερων αγοραστικών απαιτήσεων, οι διαχειριστές υπηρεσιών προσφέρουν ταυτόχρονα Layer 2 και 3 υπηρεσίες στις MPLS υποδομές τους.

Στην εικόνα 45 διακρίνουμε ένα σενάριο όπου ο service provider χρησιμοποιεί το MPLS δίκτυό του για να προσφέρει Layer 2 υπηρεσίες σε έναν πελάτη. Παρατηρούμε οτι και οι τρείς πελάτες πλήρως συνδεδεμένοι μεταξύ τους –fully meshed μέσω κυκλωμάτων που ανταποκρινονται στην εκάστοτε τεχνολογία όπως ATM, Ethernet, κτπ. Οι PE's – Provider Edges ανήκουν στο service provider, και οι CE's –Customer Edges στον customer, έτσι ώστε τα σύνορα μεταξύ τους να αποτελούν εν τέλει τα κυκλώματα πρόσβασης VLAN. Ένα σημαντικό σημείο που πρέπει να παρατηρήσουμε είναι οτι εαν ένα πακέτο φθάσει στον PE1 από τον CE1 στο VLAN 100, ο PE1 πρέπει να προωθήσει το πακέτο αυτό στον PE2, και ο PE2 με τη σειρά του στο CE2 πάνω στο VLAN 200. Αυτή η λειτουργία δε θα μπορούσε να υλοποιηθεί χωρίς τα αναφερθέντα πρωτόκολλα σηματοδοσίας πάνω στο πεδίο λειτουργικότητας ελέγχου.



Εικόνα 45. Παράδειγμα Layer 2 VPN

Στην εικόνα 46 διακρίνουμε πολύ ενδεικτικά την λειτουργικότητα του πεδίου προώθησης στην Layer 2 μεταφορά πάνω σε MPLS. Η μέθοδος ενθυλάκωσης των πακέτων είναι πανομοιότυπη ανεξάρτητα από το ποιό από τα δύο πρωτόκολλα σηματοδοσίας ελέγχου χρησιμοποιούνται, δηλαδή το BGP ή το LDP.



Εικόνα 46. Λειτουργικότητα του πεδίου προώθησης στο MPLS Layer 2 VPN

Η μεγαλύτερη διαφορά ανάμεσα στα δύο αυτά σχήματα, είναι οτι το BGP πρωτόκολλο διαθέτει αυτοανιχνευτικές ιδιότητες παρόμοιες με αυτές των L3 VPN's. Αυτο κάνει , σαν αποτέλεσμα, το provisioning να είναι πιο άμεσο και τα ψευδοκυκλώματα να δημιουργούνται αυτόματα αντί της ατομικής παραμετροποίησης. Ο LDP μηχανισμός αντίθετα δεν διαθέτει αντίληψη των VPN και απαιτεί χειρωνακτικό έλεγχο των pseudowires ανάμεσα στους Provider Edges. Τέλος να αναφέρουμε ενδεικτικά οτι ως προς το μέγεθος της κλίμακας, το BGP σχήμα είναι περισσότερο κατάλληλο για μεγαλύτερες υλοποιήσεις.

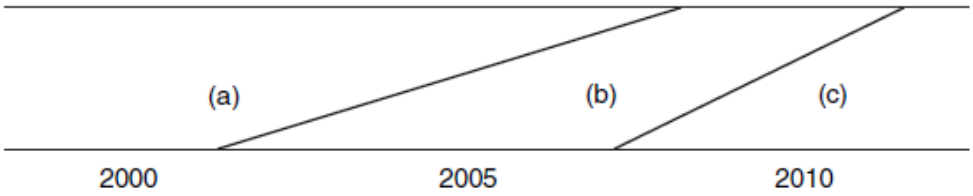
3.2.1 ΤΟ FRAMEWORK GENERALIZED–MPLS (GMPLS)

Το GMPLS είναι μία σουίτα πρωτοκόλλων (παρά ένα μεμονωμένο πρωτόκολλο) που εφαρμόζεται στο TDM (Time Domain Multiplexing) layer –επίπεδο–, στο wavelength–path layer και στο fiber layer, μέσω της γενίκευσης της αντίληψης της ετικέτας, που με αρκετή επιτυχία εφαρμόζεται στο MPLS για τη μεταφορά IP πακέτων πάνω από το packet layer. Το GMPLS επιτρέπει τον κατανεμημένο έλεγχο πάνω στο δίκτυο, κάτι που οδηγεί στη περαιτέρω απλούστευσή του, καθώς και τον έλεγχο της όλης κίνησης βάσει της πληροφορίας δρομολόγησης κάθε επιπέδου. Με τέτοιες προηγμένες τεχνικές Traffic Engineering , που καθιερώνει το framework αυτό, βελτιώνεται ακόμη περισσότερο η χρήση πόρων του δικτύου.

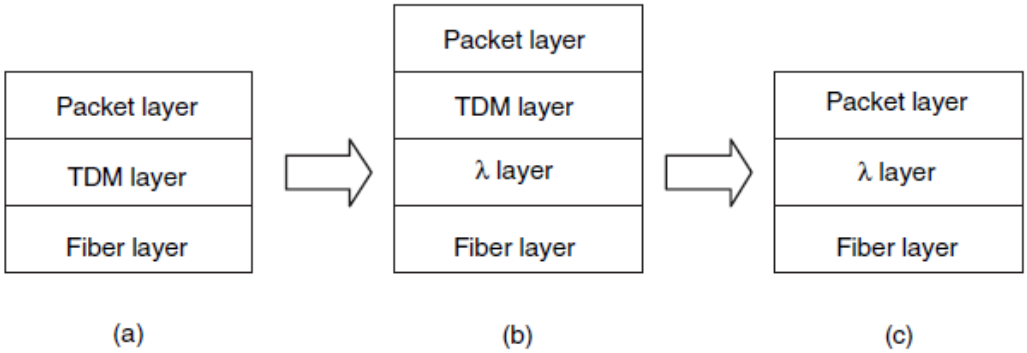
Στις παραδοσιακές μεταφορές οπτικών ινών, τα δεδομένα μεταδίδονταν κάνοντας χρήση ενός μοναδικού μήκους κύματος (ή ενός χρώματος) πάνω σε ένα μοναδικό οπτικό μέσο ανάμεσα σε δύο κόμβους. Με την αύξηση της απαίτησης για ακόμη μεγαλύτερη χωρητικότητα δεδομένων στα οπτικά δίκτυα, καθώς και για ακόμη περισσότερο εύρος ζώνης, κάτι τέτοιο φάνταζε αρκετά ασύμφορο οικονομικά από τη μια και μη πρακτικό από την άλλη. Έτσι καθιερώθηκαν διάφορες τεχνικές πολυπλεξίας και διαχωρισμού της κίνησης για την ταυτόχρονη μετάδοση διαφορετικών ροών δεδομένων. Μία από αυτές βασίζεται στο διαχωρισμό στο πεδίο μήκους κύματος –Wavelength Division Multiplexing, όπου η χωρητικότητα μεταφοράς αυξάνεται ανάλογα με τον αριθμό των χρωμάτων μέσα στην ίδια οπτική ίνα, καθιστώντας τη ιδιαίτερα χρήσιμη για τη μεταφορά μεγάλου όγκου δεδομένων.

Στην Εικόνα 47 παρουσιάζεται η σταδιακή μετάβαση της αρχιτεκτονικής διαστρωμάτωσης των επιπέδων δικτύου από το IP/MPLS στο MPλS/GMPLS . Συγκεκριμένα ένα IP/MPLS δίκτυο χτίζεται στο SDH/SONET (Synchronous Digital Hierarchy/Synchronous Digital Network) επίπεδο σύνδεσης, ενώ τα περισσότερα SDH/SONET δίκτυα χτίζονται σε φυσικό επίπεδο οπτικής ίνας. Σε κάθε οπτική διασύνδεση εφαρμόζεται μία τεχνολογία WDM. Η αναφερθείσα αρχιτεκτονική διαστρωμάτωση του MPLS δικτύου παρουσιάζεται στην Εικόνα 48. Μέχρι τώρα υπάρχουν τρία διαφορετικά layers: το **fiber layer**, το **TDM layer** και το **IP packet layer**. Με την αύξηση των απαιτήσεων σε κίνηση στο δίκτυο καθώς και την αύξηση του αριθμού των χρωμάτων που απαιτούν πολυπλεξία, η βελτιστοποίηση της χρήσης των πόρων του δικτύου μπορεί να αυξηθεί με το να χρησιμοποιηθεί ένα μήκος κύματος , από το διαθέσιμο οπτικό εύρος συχνοτήτων, σαν οπτικό μονοπάτι (μονοπάτι με μία λογική έννοια σαν αθροισμα δηλαδή οπτικών φυσικών συνδέσεων). Αυτό φαίνεται στο σχήμα (b) της Εικόνας 48. Με τη τεχνική αυτή είναι εφικτό να μειωθεί το συνολικό λειτουργικό κόστος του δικτύου, μέσω της εισαγωγής ενός επιπλέον επιπέδου, που καλείται λ–layer, ανάμεσα στο Fiber και TDM –SDH/SONET– layer. Ο κόμβος που εκτελεί καθήκοντα μεταγωγής –switching στα δύο πρώτα επίπεδα, καλείται **OXC –Optical Cross–Connect** και **DXC –Digital Cross–Connect**. Συγκριτικά με μεγάλους όγκους δεδομένων, το OXC πλεονεκτεί του DXC. Με την παιρετέρω διαχρονική αύξηση της μεταδιδόμενης IP κίνησης στα οπτικά δίκτυα μεταφορών, καθώς και την καθιέρωση κάποιων στανταρτς, προτάθηκε η αφαίρεση του TDM layer και η τάση προς τη μελλοντική οργανωση επιπέδων του σχήματος (c), με στόχο την αύξηση της απόδοσης. Έτσι καθιερώθηκε ένα μιγαδικό πρωτόκολλο, το **MPλS**, που όπως αναφέραμε ασκεί τον κατανεμημένο έλεγχο της MPLS τεχνολογίας στο IP packet layer με σκοπό την διαχείρηση του λ–layer δικτύου. Στο MPλS, ένα λ –χρώμα ή μήκος κύματος μεταχειρίζεται ως ετικέτα , όπως ακριβώς στο MPLS. Μαλιστα είναι εφικτό να χτιστεί ένα οπτικό LSP μονοπάτι συνδέοντας το εισερχόμενο με το εξερχόμενο wavelength σε κάθε OXC. Κατά την εγκαθίδρυση του μονοπατιού , όπως ακριβώς και στο MPLS, ανταλλάσονται πληροφορίες σύνδεσης ανάμεσα σε γειτονικούς κόμβους μέσω ενός

πρωτοκόλλου δρομολόγησης, και ελέγχου μέσω κατάλληλου πρωτοκόλλου σηματοδοσίας. Έτσι μπορούμε να πούμε οτι το MPλS είναι ένα πρωτόκολλο που γενικεύει την έννοια της ετικέτας στο λ–layer. Προχωρώντας ακόμη περισσότερο, ένα Γενικευμένο MPLS Πρωτόκολλο –**GMPLS**, θα γενικεύει ακόμη την έννοια της ετικέτας τόσο στο TDM όσο και στο fiber layer. **Έτσι, φτάσαμε στο GMPLS.**



Εικόνα 47. Milestones εξέλιξης του MPλS



Εικόνα 48. Οργάνωση επιπέδων δικτύου

Σύμφωνα με το RFC 3031, ένα LSR καθορίζεται ως ένας κόμβος ο οποίος διαθέτει ένα πεδίο λειτουργικότητας μεταφοράς που είναι ικανό να αναγνωρίζει τα πεδία ενός IP πακέτου ή κυψελίδας με τοποθετημένη μια MPLS ετικέτα, και να εκτελεί μεταφορά δεδομένων ανάλογα με το περιεχόμενο της επικεφαλίδας του πακέτου. Στο GMPLS απο την άλλη, ένα LSR περιλαμβάνει όχι μόνο τον κόμβο που εκτελεί χρέη μεταφοράς αλλά και μία συσκευή που μεταδίδει πακέτα βάσει της πληροφορίας του time slot, wavelength και physical port του οπτικού domain. Έτσι το LSR interface του GMPLS κατηγοριοποιείται σε τέσσερις τύπους ανάλογα με την ικανότητα μεταγωγής του:**PSC (Packet–Switch Capable), TDM (Time–Division–Multiplex Capable), LSC (Lambda–Switch Capable) και FSC (Fiber–Switch Capable)**.

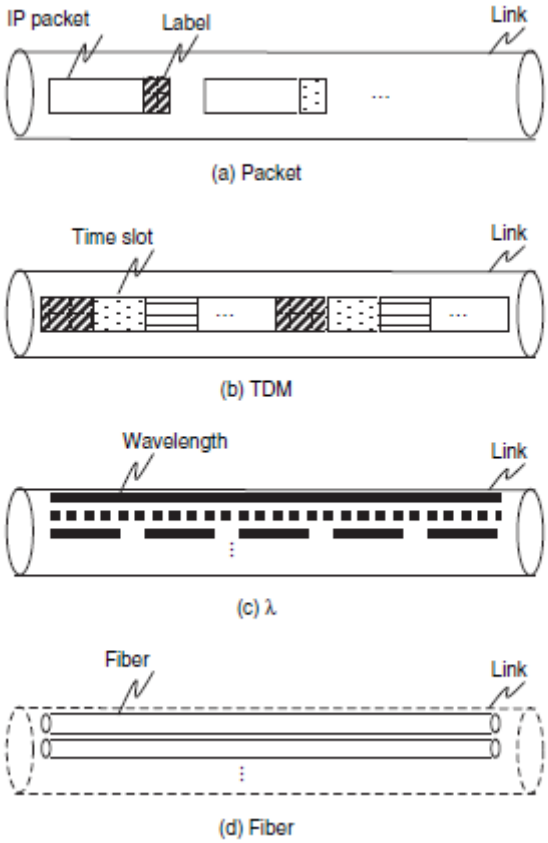
PSC: Η διεπαφή PSC είναι ικανή να αναγνωρίσει τα όρια ενός IP πακέτου ή κυψέλης και εκτελεί μετάδοση δεδομένων ανάλογα με το περιεχόμενο της επικεφαλίδας τους. Όπως φαίνεται και στην Εικόνα 49(a), μια ετικέτα εισάγεται σε κάθε πακέτο ώστε να καθορίζει το εκάστοτε LSP. Ο σύνδεσμος της Εικόνας αντιστοιχεί σε ένα link που καθορίζεται μεταξύ δύο LSRs για τη μεταφορά των IP πακέτων.

TDM: Η διεπαφή TDM επαναλαμβάνεται περιοδικά και εκτελεί μετάδοση πακέτων ανάλογα με ένα time slot. Στο TDM layer της Εικόνας 49(b) η ετικέτα αντιστοιχεί σε ένα time slot. Σαν παράδειγμα TDM interface, υπάρχει ένα DXC στο οποίο το TDM path ή

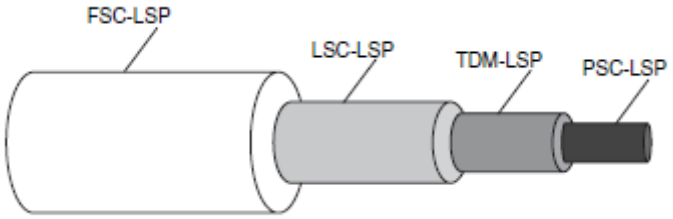
SDH/SONET path σχηματίζεται συνδέοντας το time slot του σημείου εισόδου με αυτό της εξόδου.

LSC: Η συγκεκριμένη διεπαφή εκτελεί τη μετάδοση ανάλογα με το μήκος κύματος – wavelength μέσα στην οπτική ίνα μέσα από το οποίο μεταφέρονται τα πακέτα. Όπως φαίνεται και στην Εικόνα 49(c), στο λ–layer η ετικέτα αντιστοιχεί στο μήκος κύματος. Σαν παράδειγμα LSC interface αναφέρουμε ένα OXC το οποίο εκτελεί μεταγωγή στο πεδίο διαχωρισμού μήκους κύματος, συνδέοντας το wavelength εισόδου με αυτό της εξόδου.

FSC: Το FSC interface μεταδίδει πακέτα στο πεδίο διαχωρισμού του χώρου, δηλαδή του physical port –fiber, όπως φαίνεται και στην Εικόνα 49(d). Η ετικέτα στην περίπτωση αυτή αντιστοιχεί στην εκάστοτε οπτική ίνα. Παράδειγμα υλοποίησης της τεχνικής είναι ένα OXC με ικανότητα μεταγωγής –switching στο πεδίου διαχωρισμού του χώρου –Space Division Multiplexing.



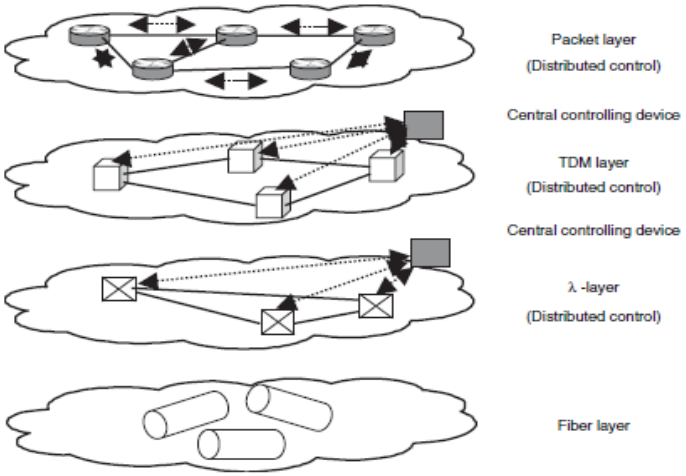
Εικόνα 49. Οι όψεις της ετικέτας στο GMPLS



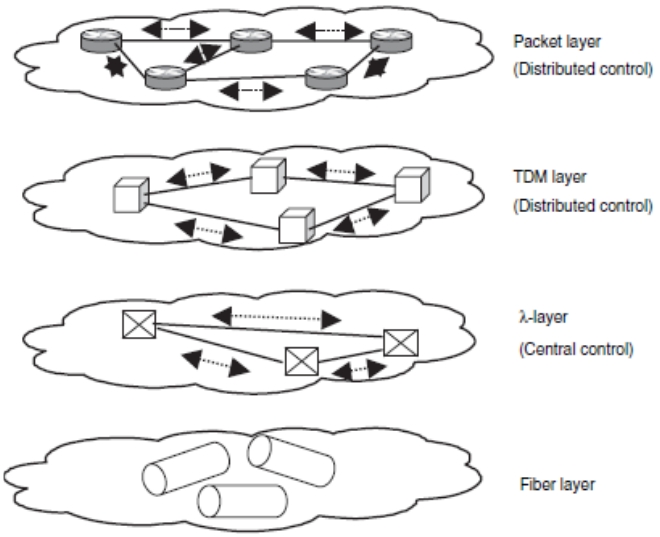
Εικόνα 50. Ιεράρχηση των LSPs

Όπως φαίνεται και στην Εικόνα 50, είναι εφικτό στο GMPLS να υπάρχει μία ιεραρχία των τεχνικών αυτών μεταγωγής. Όπου μάλιστα υπάρχει και το εκάστοτε interface, αυτό λέμε οτι αντιστοιχεί σε ένα κατάλληλο layer ή συγκεκριμένη περιοχή. Έτσι η περιοχή ανάμεσα στα PSC interfaces καλείται PSC layer, οι TDM διεπαφές σχηματίζουν ένα TDM–LSP σε ένα TDM layer, κτπ.

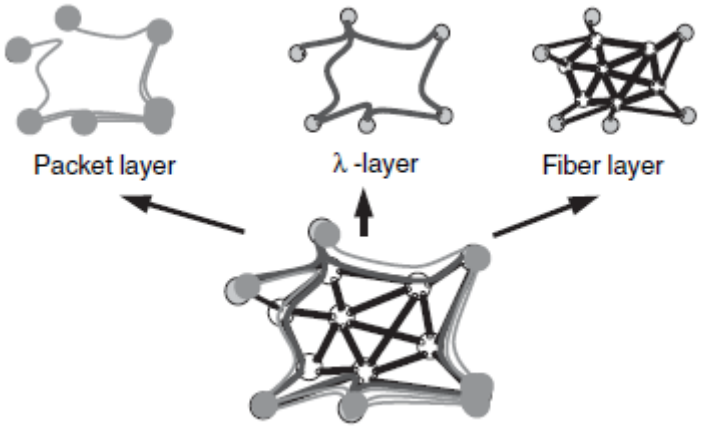
Το GMPLS , όπως θα δούμε και στην συνέχεια, προσφέρει αρκετά πλεονεκτήματα σε σύγκριση με το MPLS. Στην μέχρι πρώτινος αρχιτεκτονική δικτύου του IP/MPLS υπήρχε κατανεμημένος έλεγχος στο packet layer κάνοντας χρήση ενός πρωτοκόλλου δρομολόγησης ή σηματοδοσίας. Στα υπόλοιπα επίπεδα όπως το TDM, λ–layer ο έλεγχος είναι κεντρικός μέσω της εγκαθίδρυσης του μονοπατιού. Σε αυτό το περιβάλλον οι διαχειριστές όφειλαν να αντιμετωπίζουν καθε layer με ξεχωριστό τρόπο λόγω των διαφορετικών τεχνικών ελέγχου που εφαρμόζεται σε καθε ένα. Αντίθετα στο GMPLS μέσω της επέκτασης της MPLS ετικέτας και στα υπόλοιπα επίπεδα (πλην βέβαια του φυσικού), είναι πλέον εφικτός ο κατανεμημένος έλεγχος και διαχείρηση και σε αυτά. Έτσι εκεί που οι διαχειριστικές λειτουργικότητες συντελούνταν σε κάποιο απομακρυσμένο κεντρικό κόμβο, τώρα κατανέμονται σε καθε κόμβο του δικτύου και ελέγχονται ανεξάρτητα. Καθίσταται πιο εύκολη η δημιουργία νέων κόμβων, η διαγραφή ήδη υπαρχόντων, όπως βέβαια και συνδέσμων–μονοπατιών. Το αποτέλεσμα είναι η ακόμα πιό βέλτιστη χρήση πόρων του δικτύου. Εκείνο που πραγματικά επιτυγχάνει το GMPLS είναι η ενοποίηση των upper layers (Packet+TDM+λ–layer)σε ενα ενιαίο επίπεδο με κατανεμημένο έλεγχο και διαχείρηση, μια τεχνική που καλείται **multilayer traffic engineering**.



Εικόνα 51.Υπάρχουσα αρχιτεκτονική IP/MPLS



Εικόνα 52. Αρχιτεκτονική GMPLS με κατανεμημένο έλεγχο σε κάθε επίπεδο

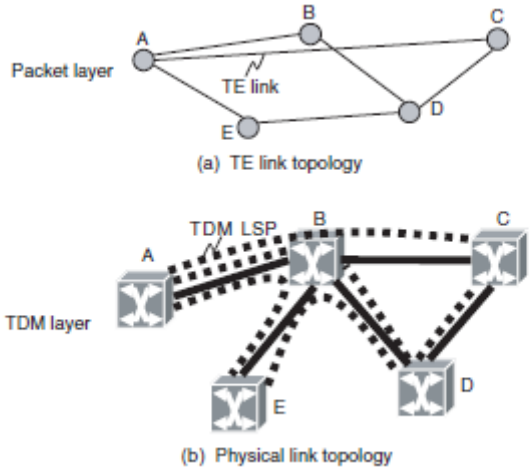


Εικόνα 53. Multilayer Traffic Engineering

Ένα απο τα βασικότερα χαρακτηριστικά του GMPLS είναι ο διαχωρισμός του πεδίου λειτουργικότητας μεταφοράς –data plane από το πεδίο λειτουργικότητας ελέγχου –control plane. Στο IP/MPLS δίκτυο είναι καθολικά αποδεκτό οτί όλοι οι κόμβοι διαθέτουν ένα interface που μπορεί να αναγνωρίσει και να επεξεργαστεί τα πακέτα. Με αυτό το τρόπο τα πακέτα ελέγχου του πρωτοκόλλου δρομολόγησης ή σηματοδοσίας μεταφέρονται πάνω από το ίδιο φυσικό μέσο με τα πακέτα δεδομένων. Αντίθετα στο GMPLS δεν έχουν όλα τα layers την δυνατότητα και το interface να αναγνωρίζουν πακέτα. Έτσι η μετάδοση των πακέτων ελέγχου εκτελείται λογικά χρησιμοποιώντας διαφορετικό μέσο απο αυτό για τη μετάδοση δεδομένων. Επικρατεί επομένως στο GMPLS λογικός διαχωρισμός ανάμεσα στο data και control plane.

Τα πιό ευρέως χρησιμοποιούμενα πρωτόκολλα δρομολόγησης στο GMPLS είναι το **OSPF (Open Shortest Path First)** και το **IS–IS (Intermediate System to Intermediate System)**. Στα GMPLS δίκτυα το OSPF πρωτόκολλο επεκτείνεται με νέα χαρακτηριστικά και λειτουργικότητες όπως:**traffic–engineering link (TE), hierarchization of the LSP, unnumbered links, link bundling** και **LSA(Link–State**

Advertisements). Ως προς το πρώτο χαρακτηριστικό, όπως διακρίνεται και στην Εικόνα 52, ένα LSP κατώτερου επιπέδου –layer μπορεί να γίνει σύνδεσμος για ένα upper–layer LSP. Για παράδειγμα όταν ένα LSP μονοπάτι εγκαθιδρύεται σε ένα καθορισμένο TDM μονοπάτι, το τελευταίο συμπεριφέρεται σαν ένας σταθερός σύνδεσμος που διατηρείτο εκεί για αρκετό χρόνο. Όταν το LSP κατωτέρου επιπέδου εγκατασταθεί, ο κόμβος προέλευσης του μονοπατιού αυτού, από την όψη ενός ανωτερου layer, διαφημίζεται στο δίκτυο σαν upper–layer link. Αυτο το LSP καλείται TE link. Ένα παράδειγμα αυτού που ανφέραμε φαίνεται στην Εικόνα 54. Οι διακεκκομμένες γραμμές αντιστοιχούν σε TDM paths. Στο TDM layer το TDM–LSP συμπεριφέρεται σαν TE link. Όταν το PSC–LSP εγκατασταθεί, το μονοπάτι επιλέγεται ανάλογα με τη τοπολογία που χτίζεται απο τους TE συνδέσμους. Παρώτι το TE link αντιμετωπίζεται ως ένα αφηρημένο –abstract link, στη περίπτωση επιλογής μονοπατιού LSP, στην ουσία αναφέρεται σε κάθε τοπολογία που δημιουργείται μέσω του traffic engineering;δεν υπάρχει δηλαδή διαχωρισμός ανάμεσα σε φυσικούς και λογικούς συνδέσμους.



Εικόνα 54. Traffic Engineering και GMPLS

Στη περίπτωση, στη συνέχεια, των unnumbered links, είναι γνωστό οτι συνήθως σε κάθε σύνδεσμο –link σε ένα δίκτυο MPLS, αποδίδεται και μια IP διεύθυνση. Με βάση αυτή τη διεύθυνση είναι εφικτό να αναγνωρίσουμε τη γραμμή μέσα στο δίκτυο. Επειδή , ωστόσο, στα GMPLS δίκτυα λόγω της πιθανότητας να κατανέμονται μέχρι και 100 ή περισσότερα χρώματα –lambdas σε κάθε οπτική ίνα, ο αριθμός των απαιτούμενων IP διευθύνσεων στη περίπτωση αυτή θα ήταν τεράστιος. Έτσι η λύση που προτάθηκε ήταν να αποδίδεται σε κάθε TE link interface ένα link identifier (link ID). Παρόλο που μια IP διεύθυνση πρέπει και πάλι να αποδίδεται καθολικά, το link ID είναι εξίσου καλό εαν είναι μοναδικό μέσα στο Router. Όταν ένας σύνδεσμος εκφράζεται ως συνδυασμός του Router ID και του link ID καλείται unnumbered link, με την έννοια οτι δεν έχει αποδωθεί σε αυτόν IP διεύθυνση.

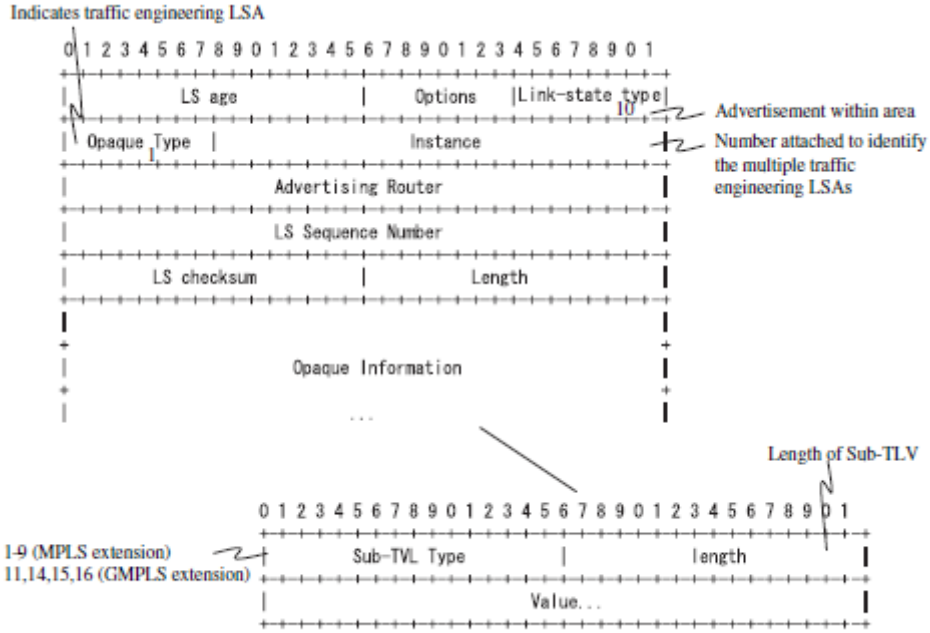
Έπειτα εξετάζουμε τη τεχνική του link–bundling, όπου πολλαπλές γραμμές με τα ίδια TE χαρακτηριστικά ενοποιούνται και αντιμετωπίζονται ως ένα ενιαίο TE link. Οι συνθήκες ομοιότητας που πρέπει να πληρούνται είναι:(1) Οι γραμμές να βρίσκονται ανάμεσα σε κοινούς κόμβους, (2) Οφείλουν να είναι του ιδίου τύπου (point–to–point ή point–to–multipoint), (3) Να διαθέτουν τις ίδιες TE μετρικές, (4) Να ανήκουν στην ίδια κλάση διαθέσιμων πόρων δικτύου. Ο κύριος σκοπός του link bundling είναι η βελτίωση της κλιμάκωσης της δρομολόγησης μέσω της μείωσης του ποσοστού των link advertisements για κάθε σύνδεσμο.

Σε ένα IP/MPLS δίκτυο, τα link states –πληροφορίες συνδέσμων ανάμεσα στους δρομολογητές διαφημίζονται χρησιμοποιώντας έναν LSA router τύπου 1 –LSA type–1. Για να διαφημιστεί το link state ενός TE link στο GMPLS δίκτυο, χρησιμοποιείται το λεγόμενο 'opaque' LSA –Link State Advertisement. Το format του φαινεται στην Εικόνα 55. Η λέξη 'opaque' έχει περισσότερο την έννοια του 'αβέβαιου'. Στο GMPLS , που και αυτή τη στιγμή ακόμη τυποποιείται στο IETF, χρησιμοποιείται LSA type–10 επειδή έχει να κάνει με intra–domain πρωτόκολλο δρομολόγησης. Το opaque LSA διαφημίζεται ανάλογα με το format αποθήκευσης του TLV (type, length, value). Υπάρχουν δύο τύποι TLV format. Ο ένας είναι ο TLV δρομολογητής που εκφράζει τη πληροφορία δρομολόγησης, και ο άλλος είναι ο TLV συνδέσμου που εκφράζει με τη σειρά του τη πληροφορία σύνδεσης. Στις απαραίτητες επεκτάσεις του πρωτοκόλλου OSPF για το GMPLS, για το sub–TLV του TLV συνδέσμου, όπως φαίνεται και στην Εικόνα 56, καθορίζονται 9 τύποι, από Type–1 έως Type–9, ως επεκτάσεις Traffic Engineering. Επιπρόσθετα με αυτές τις επεκτάσεις, ακολουθούν άλλες 4 ειδικά για το GMPLS OSPF–TE.

- **Sub–TLV = 11 (Link local/remote identifier):** Το μήκος του είναι 8 bytes. Το link local identifier και το link remote identifier έχουν μέγεθος 4 οκτάδες αντίστοιχα. Το local σημαίνει το κόμβο της μεριάς του συνδέσμου, ενώ το remote το κόμβο από την άλλη μεριά του συνδέσμου. Το πεδίο αυτό χρησιμοποιείται στη περίπτωση των unnumbered links. Εαν το απομακρυσμένο TE link identifier είναι άγνωστο, τίθεται στο 0.
- **Sub–TLV = 14 (Link protection type):** Έχει μήκος 4 οκτάδες. Το πεδίο αυτό υποδυκνείει τον βαθμό αξιοπιστίας της γραμμής. Η πρώτη οκτάδα έχει τυποποιηθεί με βάση τους ακόλουθους τύπους προστασίας:
  0 × 01 (Extra traffic type): Χρησιμοποιείται ως γραμμή προστασίας για τα υπόλοιπα links. Best–effort κίνηση τρέχει συνήθως σε αυτό το σύνδεσμο. Όταν συμβεί κάποια αστοχία στην προστατευόμενη σύνδεση, τα LSP δεδομένα στην άλλη προστατευόμενη γραμμή, περνούν τώρα σε αυτήν.
  0 × 02 (Unprotected): Αυτή η γραμμή δεν προστατεύεται. Όταν συμβεί μία αστοχία, τα LSP δεδομένα της χάνονται.
  0 × 08 Shared Type: Υπάρχουν 1 ή περισσότερα extra–traffic–type συνδέσεις που προστατεύουν την γραμμή αυτή. Το μονοπάτι του shared–type link και το μονοπάτι του extra–traffic type link είναι ανεξάρτητα το ένα του άλλου.
  0 × 08 1:1 type: Υπάρχει μόνο ένα extra–traffic type link που προστατεύει ένα 1:1 τύπο. Και πάλι τα δύο μονοπάτια τους είναι ανεξάρτητα το ένα του άλλου.
  0 × 08 1+1 type: Υπάρχει ένα dedicated–independent–μονοπάτι που προστατεύει ένα 1+1 τύπο. Το θέμα είναι όμως οτι δεν μπορεί να επιλέξει με τη σειρά του το LSP route διότι δεν διαφημίζεται ως link state.

0 × 20 Enchanced type: Είναι πιό αξιόπιστο από τον προηγούμενο τύπο. Υπάρχουν εδώ 2 ή και περισσότερα dedicated και independent μονοπάτια που προστατεύουν τον 1+1 τύπο.

- **Sub–TLV = 15 (Interface switching capability identifier):** Το μήκος του πεδίου είναι μεταβλητό. Υπάρχει μια οκτάδα που υποδυκνείει την ικανότητα μεταγωγής, άλλη μια τον τύπο κωδικοποίησης, και η τελευταία περιέχει το μέγιστο LSP bandwidth για κάθε προτεραιότητα. Ο μέγιστος αριθμός προτεραιοτήτων είναι 8. Ένα από τα χαρακτηριστικά του GMPLS είναι οτι κάθε interface έχει και διαφορετική ικανότητα μεταγωγής. Μπορει για παράδειγμα ένα interface ενός συγκεκριμένου link να μην αναγνωρίσει ένα πακέτο, είναι ωστόσο ικανό να το προωθήσει και να το μεταγάγει. Υπάρχουν διάφοροι τύποι μεταγωγής: PSC, TDM, LSC, και FCS. Οι τύποι κωδικοποίησης περιλαμβάνουν τα πακέτα, Ethernet, λ, ίνα, κτπ. Τέλος τα X και Y στο (X, Y) δηλώνουν την ικανότητα μεταγωγής και στα δύο άκρα του interface. Έτσι έχουμε:
  (PSC, PSC), (TDM, TDM), (LSC, LSC), (PSC, TDM), (PSC, LSC), (TDM, LSC), (PSC, PSC+LSC).
- **Sub–TLV = 16 (Risk–shared link group –SRLG):**Και πάλι το μήκος είναι μεταβλητό. Το SRLG είναι ένα σύνολο από συνδέσμους που επηρεάζονται από ένα συγκεκριμένο σφάλμα. Για παράδειγμα, όταν πολλαπλά χρώματα –lambdas ανήκουν σε μία οπτική ίνα, και πολλαπλά LSC–LSPs εγκαθιδρύονται ως μονοπάτι χρησιμοποιώντας ένα μήκος κύματος από την ίδια ίνα, κατα την πραγματοποίηση μιας αστοχίας οι LSC–LSP γραμμες επηρεάζονται διαδοχικά. Εαν στο ανωτερο επίπεδο, το TDM, κάθε μια από αυτές αντιμετωπίζεται ως μια ανεξάρτητη γραμμή, τότε η αξιοπιστία του TDM layer δεν είναι εξασφαλισμένη. Έτσι στο GMPLS, κάθε γραμμή στα πλαίσια της προστασίας της μπορεί να επιλέξει ένα ανεξάρτητο μονοπάτι λαμβάνοντας πάντα υπόψιν το πεδίο SRLG, εάν αυτό το μονοπάτι ανήκει σε κάποιο SRLG group. Το SRLG group εκφράζεται με 4 οκτάδες.



Εικόνα 55. Opaque LSA format

Sub-TLV Type	Length	Name	
1	1	Link type	
2	4	Link ID	
3	4	Local interface IP address	
4	4	Remote interface IP address	
5	4	Traffic engineering metric	
6	4	Maximum bandwidth	
7	4	Maximum reservable bandwidth	
8	32	Unreserved bandwidth	
9	4	Administrative group	
11	8	Link Local/Remote Identifiers	← Added for GMPLS
14	4	Link Protection Type	← Added for GMPLS
15	variable	Interface Switching Capability Descriptor	← Added for GMPLS
16	variable	Shared Risk Link Group	← Added for GMPLS

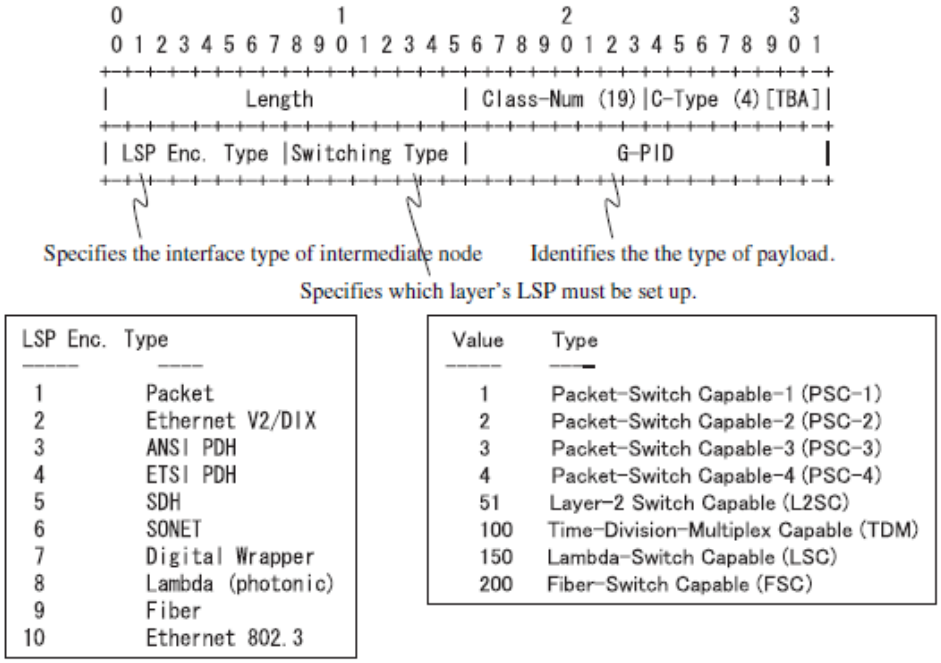
Εικόνα 56. Sub–TLV του Opaque LSA στο GMPLS OSPF–TE

Το πρωτόκολλο σηματοδοσίας είναι ένα πρωτόκολλο που εγκαθιδρύει το LSP και διαχειρίζεται την όλη φάση εγκατάστασής του. Την στιγμή που γράφεται το παρών κείμενο γίνονται εκτεταμένες προσπάθειες από τον IETF για την τυποποίηση του επεκτεταμένου πρωτοκόλλου RSVP–TE, το οποίο αποτελεί το δημοφιλέστερο πρωτόκολλο σηματοδοσίας του GMPLS. Στη συνέχεια περιγράφουμε τις Traffic Engineering επεκτάσεις του πρωτοκόλλου αυτού. Όπως είχαμε ξαναπεί, όταν ένα LSP εγκατασταθεί, ο κόμβος προέλευσης μεταδίδει ένα PATH μήνυμα {Παρεπιπτόντως η ίδια διαδικασία ακολουθείται και στο ASON module του NS–2, για τις ανάγκες των πειραματικών προσωμειώσεων του GMPLS}, το οποίο φτάνει στον κόμβο προορισμού μέσω των ενδιάμεσων hops του μονοπατιού. Σε αυτό το μήνυμα εισάγεται μια ετικέτα σε κάθε (οπτικό) σύνδεσμο του μονοπατιού. Όταν ο κόμβος προορισμού λάβει το PATH μήνυμα, μεταδίδει προς τα πίσω ένα RESV μήνυμα με την αντίστροφη σειρά. Κατα την μετάδοση και λήψη τώρα του RESV μηνυματος από κάθε ενδιαμέσο κόμβο, ξεκινώντας βέβαια από τον κόμβο προορισμού,

σχηματίζονται και τυπικά τα Label Forwarding Tables σε κάθε hop, ενώ δεσμέυεται και το απαιτούμενο bandwidth μαζί με άλλα TE constraints. Η διαδικασία αυτή εκτελείται τόσο σε upstream όσο και σε downstream επίπεδο. Στη περίπτωση του RSVP–TE, για την διαχείρηση της κατάστασης εγκατάστασης του LSP, και για την διατήρηση αυτής της κατάστασης, ο κόμβος προορισμού, μετά την δημιουργία του μονοπατιού, μεταδίδει PATH ή RESV μηνύματα περιοδικά. Αυτά καλούνται refresh messages. Το state του LSP υποδυκνείεται απο αυτά τα refresh messages. Εάν ένας συγκεκριμένος κόμβος δεν λάβει το μήνυμα ανανέωσης μετά από ένα καθορισμένο time interval, ο αντίστοιχος σχετικός κόμβος κρίνει οτι έχει συμβεί μια αστοχία ή σφάλμα, και διαγράφει το state του LSP, ενώ παράλληλα μεταδίδει ένα Path ERROR μήνυμα και ένα Path TEAR μήνυμα τόσο σε upstream όσο και downstream φορά. Στη συνέχεια ο κόμβος που λαμβάνει το PATH μήνυμα διαγράφει και θέτει disconnected το state του LSP. Αυτή η μέθοδος διαχείρισης της κατάστασης του μονοπατιού ανάλογα με τα μηνύματα ανανέωσης καλείται "management by soft state".

Η RSVP–TE σηματοδοσία ενός MPLS δικτύου επεκτείνεται και στη περίπτωση του GMPLS. Η εγκατάσταση του μονοπατιού σημαίνει να γίνεται μεταγωγή των πακέτων βάση του πίνακα προώθησης ετικετών σε κάθε κόμβο. Στο MPLS η ανάθεση ετικέτας εκτελείται μόνο για την εγκαθίδρυση του LSP, αλλά όχι και για την ανάθεση εύρους ζώνης ή άλλων δικτυακών πόρων. Όπως είδαμε προηγουμένως στην ίδια ενότητα, στο GMPLS μια ετικέτα αντιστοιχεί σε time slot στο TDM layer, σε χρώμα–lambda στο λ–layer, και σε φυσική οπτική ίνα στο fiber layer. Επομένως αναθέτοντας ετικέτα στο GMPLS σημαίνει ανάθεση δικτυακών πόρων ταχύτητας και εύρος ζώνης σε κάθε επίπεδο, πλην βέβαια του packet layer. Κάποια βασικά χαρακτηριστικά του RSVP–TE που θα δούμε στη συνέχεια , όπως Label Request, Dual Direction Path Signaling, Label Setting και Architectural signaling, σχετίζονται με την έννοια αυτής της ανάθεσης στο GMPLS.

Στα MPLS δίκτυα ένα LSP μονοπάτι απευθύνεται μόνο σε Packet Switched Capable – PSC interfaces, με αντίστοιχη τεχνική μεταγωγής προορισμένη για IP πακέτα. Αντίθετα στο GMPLS, το RSVP–TE εγκαθιστά μονοπάτια στα TDM–, LSC– και FSC– interfaces πέραν του PSC, και ταυτόχρονα διαχειρίζεται τη κατάστασή τους. Κατά την αίτηση για ετικέτα με το PATH μήνυμα, το τελευταίο διαθέτει ένα label–request object. Η διαδικασία αίτησης ετικέτας στο GMPLS απαιτεί ουσιαστικά μια γενικευμένη ετικέτα. Έτσι σαν επεκτάσεις για το label request object προστέθηκαν τα πεδία: **LSP Encoding Type, Switching Type,** και **G–PID (Generalized Payload ID)**. Στην Εικόνα 57 διακρίνουμε το format του label request object.



Εικόνα 57. Format του Label Request Object

LSP encoding type: Αναπαριστάνεται με ένα 8–bit πεδίο. Υποδυκνείει σε ποιο interface ενός ενδιάμεσου κόμβου του LSP μονοπατιού, ποια συγκεκριμένη τεχνολογία κωδικοποίησης πρέπει να υποστηριχθεί. Παραδείγματα τέτοιων τεχνικών κωδικοποίησης είναι τα πακέτα, Ethernet, SDH, digital wrapper, λ και ίνα. Όταν υπάρχει μια δεδομένη κωδικοποίηση, το interface ενός hop είναι ικανό να αναγνωρίζει και να επεξεργάζεται τα αντίστοιχα format πακέτων.

Switching type: Και πάλι παριστάνεται με ένα 8–bit πεδίο. Καθορίζει ποιανού επιπέδου –layer ετικέτα πρέπει να χρησιμοποιηθεί. Τα switching types ειναι PCS, TDM, LSC και FCS. Έτσι στη περίπτωση για παράδειγμα που ο τύπος μεταγωγής είναι TDM, απαιτείται time slot σαν ετικέτα, ενώ όταν είναι LSC απαιτείται μήκος κύματος ή lambda.

G–PID: Αναπαριστάνεται με ένα 16–bit πεδίο. Είναι ένα αναγνωριστικό πεδίο του φορτίου που μεταδίδει το LSP. Υποδυκνείει δηλαδή την αντίστοιχη τεχνολογία που θα πρέπει βάση της οποίας ο κόμβος προέλευσης και προορισμού να επεξεργαστεί το φορτίο αυτό. Στην Εικόνα 58 διακρίνουμε όλους τους τύπους του G–PID. Να σημειώσουμε εδώ οτι εάν τα interfaces σε κάθε σημείο του LSP δεν υποστηρίζουν το ίδιο G–PID, το φορτίο δεν μπορεί να αποκωδικοποιηθεί και η επικοινωνία στο LSP δεν εκτελείται.

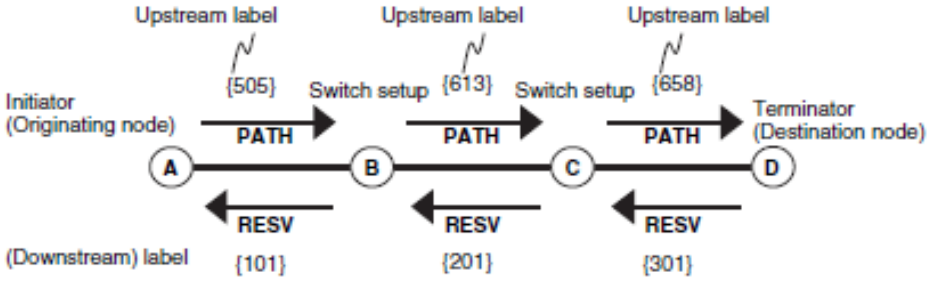
Value	Type	Technology
0	Unknown	All
1	Reserved	
2	Reserved	
3	Reserved	
4	Reserved	
5	Asynchronous mapping of E4	SDH
6	Asynchronous mapping of DS3/T3	SDH
7	Asynchronous mapping of E3	SDH
8	Bit synchronous mapping of E3	SDH
9	Byte synchronous mapping of E3	SDH
10	Asynchronous mapping of DS2/T2	SDH
11	Bit synchronous mapping of DS2/T2	SDH
12	Reserved	
13	Asynchronous mapping of E1	SDH
14	Byte synchronous mapping of E1	SDH
15	Byte synchronous mapping of 31 * DS0	SDH
16	Asynchronous mapping of DS1/T1	SDH
17	Bit synchronous mapping of DS1/T1	SDH
18	Byte synchronous mapping of DS1/T1	SDH
19	VC-11 in VC-12	SDH
20	Reserved	
21	Reserved	
22	DS1 SF Asynchronous	SONET
23	DS1 ESF Asynchronous	SONET
24	DS3 M23 Asynchronous	SONET
25	DS3 C-Bit Parity Asynchronous	SONET
26	VT/LOVC	SDH
27	STS SPE/HOVC	SDH
28	POS - No Scrambling, 16 bit CRC	SDH
29	POS - No Scrambling, 32 bit CRC	SDH
30	POS - Scrambling, 16 bit CRC	SDH
31	POS - Scrambling, 32 bit CRC	SDH
32	ATM mapping	SDH
33	Ethernet	SDH, Lambda, Fiber
34	SONET/SDH	Lambda, Fiber
35	Reserved (SONET deprecated)	Lambda, Fiber
36	Digital Wrapper	Lambda, Fiber
37	Lambda	Fiber

Εικόνα 58. Τύποι G–PID

Ένα LSP στα MPLS δίκτυα συνήθως αποτελεί ένα μονόδρομο μονοπάτι. Ωστόσο όταν η επικοινωνία επεκτείνεται στο TDM layer, λ–layer και fiber layer στο GMPLS δίκτυο, επειδή τα SONET/SDH μονοπάτια, τα wavelength μονοπάτια και τα fiber , επίσης, είναι αμφίδρομα, η σηματοδοσία πρέπει να επεκταθεί ώστε να υποστηρίζει αυτή την αμφίδρομη κίνηση. Μία προσέγγιση για την υλοποίηση της αμφίδρομης σηματοδοσίας στο GMPLS είναι να εφαρμόσουμε διαφορετική μονόδρομη σηματοδοσία σε κάθε κατεύθυνση. Μία τέτοια λύση , ωστόσο, δεν έχει γίνει αποδεκτή για πολλούς λόγους, όπως για το αυξημένο μέγεθος του setup time, το διπλασιασμό των μηνυμάτων σηματοδοσίας, κτπ. Έτσι αυτό που εντέλει καθιερώθηκε είναι ένα αμφίδρομο μονοπάτι να εγκαθίσταται με το να αναγκάζει τη σηματοδοσία να πηγαίνει και να επιστρέφει ανάμεσα στο κόμβο προορισμού και προέλευσης με χρήση PATH και RESV μηνυμάτων μέσω μιας upstream ετικέτας. Στη συνέχεια θα περιγράψουμε ένα μικρό παράδειγμα δημιουργίας αμφίδρομου μονοπατιού με χρήση αυτής της αντίστοιχης σηματοδοσίας. Όπως βλέπουμε και στην Εικόνα 59, ο κόμβος που μεταδίδει το PATH μήνυμα καλείται "initiator" και ο κόμβος που μεταδίδει το RESV

μήνυμα καλείται "terminator". Το LSP που μεταφέρει δεδομένα από τον κόμβο προέλευσης στον κόμβο προορισμού καλείται "downstream path", και αντίστοιχα το άλλο LSP καλείται "upstream path". Πριν ο κόμβος Α μεταδώσει το PATH μήνυμα στον κόμβο Β, το 505 ανατίθεται ως τιμή ετικέτας για το μονοπάτι ανόδου ανάμεσα στον κόμβο Α και Β. Ο Α τοποθετεί την upstream τιμή ετικέτας 505 στο PATH μήνυμα και το μεταδίδει στον Β. Αυτός με τη σειρά του θέτει την ετικέτα με τιμή 613 για τον σύνδεσμο ανάμεσα στους Β και C στο label conversion table, και εκτελεί την εγκατάσταση της μεταγωγής για το μονοπάτι ανόδου ανάλογα με αυτόν τον πίνακα. Μόλις η διαδικασία αυτή ολοκληρωθεί στον κόμβο D, αυτός μεταδίδει το μονοπάτι ανόδου στον Α. Κατα την φάση αυτή της εγκατάστασης του καθοδικού μονοπατιού, ακολουθείται η ίδια διαδικασία και η ετικέτα του μονοπατιού αυτού περιλαμβάνεται στο RESV μήνυμα.

Κάνοντας χρήση αυτής της διαδικασίας σηματοδοσίας, καθίσταται εφικτό να δημιουργούμε ένα αμφίδρομο μονοπάτι σε ένα round–trip του PATH και RESV μηνύματος.



Εικόνα 59. Ετικέτα ανόδου –upstream

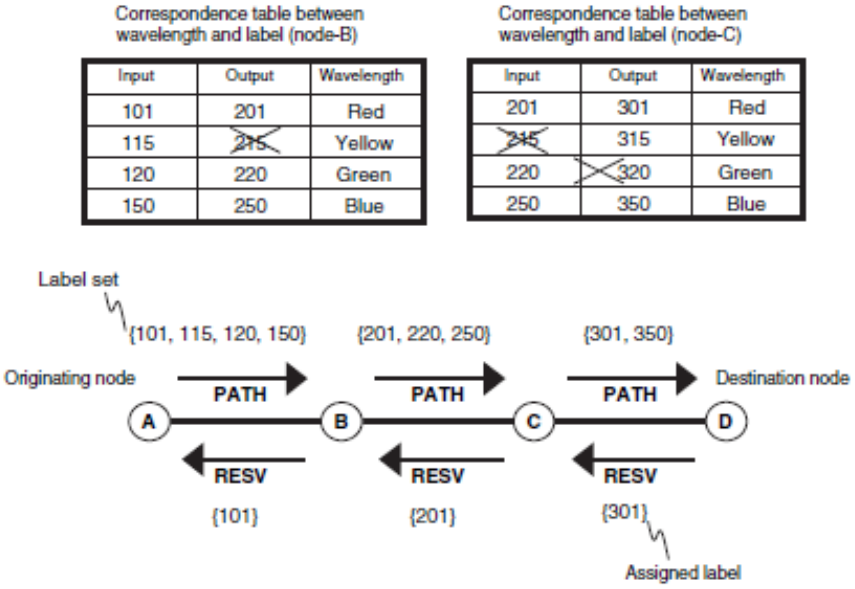
Η τεχνική του **label setting** εισάγεται για να εφαρμόζουμε τη σηματοδοσία στο λ–layer επίπεδο. Σε αυτή τη περίπτωση η ετικέτα αντιστοιχεί σε χρώμα ή μήκος κύματος. Αυτό το γεγονός ωστόσο εισάγει και κάποια πιθανά προβήματα όπως:

Η περίπτωση όπου μια συσκευή μετάδοσης του κόμβου ανοδικής πορείας δεν υποστηρίζει το μήκος κύματος που αντιστοιχεί στην τιμή της ετικέτας την οποία έχει προσδιορίσει ο κόμβος καθοδικής πορείας. Lasers μεταβλητού μήκους κύματος είναι ακριβά, ενώ τα χρώματα εξόδου είναι περιορισμένα.

Η περίπτωση όπου υπάρχει περιορισμός στη διαδικασία μετατροπής μήκους κύματος σε έναν ενδιάμεσο κόμβο. Σε αυτή τη περίπτωση δεν είναι δυνατόν να ρυθμίσουμε τη διαδικασία που θα αντιστοιχεί την εισερχόμενη με εξερχόμενη ετικέτα. Είναι απαραίτητος δηλαδή ένας wavelength–conversion μεταγωγέας με ορισμένους αναγκαίους περιορισμούς.

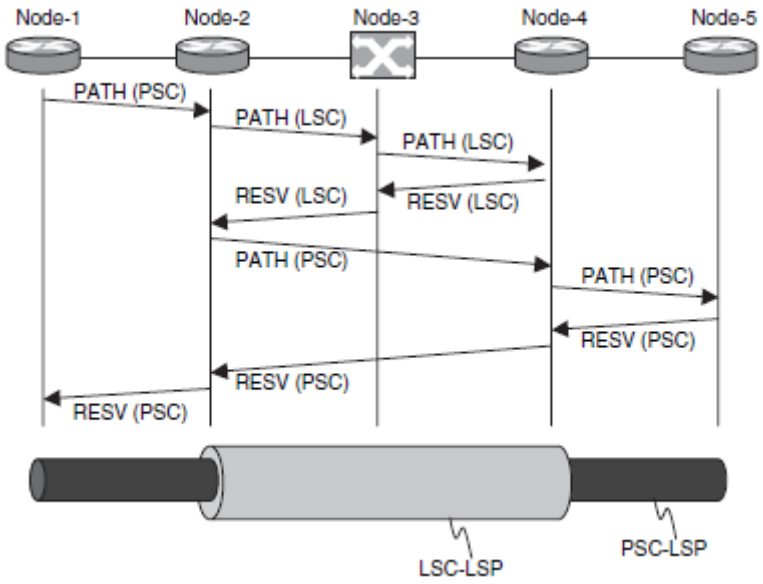
Κατά τη φάση της ανάθεσης ετικέτας στο λ–layer επίπεδο, επειδή όπως είχαμε τονίσει υπάρχει και η έννοια της ανάθεσης και του αντίστοιχου δικτυακού πόρου, γεννάται αναπόφευκτα ένας περιορισμός στον wavelength–conversion μεταγωγέα. Σε αυτή τη περίπτωση ο ανοδικός κόμβος είναι υποχρεωμένος να προβάλλει έναν περιορισμό στη τιμή της ετικέτας στον καθοδικό κόμβο, όταν ο upstream node μεταφέρει το PATH μήνυμα. Δίνουμε στη συνέχεια ένα παράδειγμα της διαδικασίας ανάθεσης ετικέτας στη περιπτωση αυτή. Στην Εικόνα 60 ο κόμβος Α είναι κόμβος προέλευσης, ενώ τα χρώματα –μήκη κύματος που μπορούν να μεταδοθούν είναι κόκκινο, κίτρινο, πράσινο και μπλε με αντίστοιχα label values τις τιμές 101, 115, 120 και 150. Ο κόμβος Α μεταδίδει το PATH μήνυμα, συμπεριλαμβάνοντας το σύνολο τιμών ετικετών (101, 115, 120, 150) ως τους περιορισμούς των μηκών κύματος που θα υποστηρίζει ο μεταδότης, στον κόμβο Β. Επειδή ο τελευταίος δεν διαθέτει το κίτρινο μήκος κύματος στο δικό του wavelength–conversion

function, και μπορεί έτσι να μεταδίδει μόνο κόκκινο, πράσινο ή μπλε, στέλνει στον γειτονικό του κόμβο το σύνολο ετικετών (201, 220, 250). Η διαδικασία αυτή επαναλαμβάνεται μέχρι και τον τελευταίο κόμβο D. Οταν αυτός λάβει το label set (301, 320), μπορεί να επιλέξει μόνο μια ετικέτα από αυτό. Στο παράδειγμά μας επιλέγει την ετικέτα 301 και μεταδίδει το RESV μήνυμα , συμπεριλαμβανομένης αυτής της τιμής, στον κόμβο C. Έπειτα ο κόμβος C επιλέγει την ετικέτα 201 από το σύνολο (201, 220, 250) ώστε να δημιουργήσει το LSP του κόκκινου χρώματος –μήκους κύματος. Παρόμοια ο κόμβος B επιλέγει την ετικέτα 101 και ενημερώνει τον γειτονικό του κόμβο A σχετικά, με ένα RESV μήνυμα. Το αποτέλεσμα όλης αυτής της διαδικασίας είναι η δημιουργία ενός LSP μονοπατιού ανάμεσα στους κόμβους A και D.



Εικόνα 60. Label set

Με βάση τα όσα τονίσαμε προηγουμένως, σε ένα GMPLS δίκτυο όταν εισάγεται η αντίληψη της ιεραρχίας του LSP καθώς και η έννοια της κατανεμημένης σηματοδοσίας, καθίσταται εφικτό να εγκαθιδρύσουμε ένα LSP σε χαμηλότερο layer με το να ενεργοποιήσουμε ένα LSP setup αίτημα σε υψηλότερο επίπεδο. Αυτό καλείται **"hierarchical signaling"**. Παράδειγμα της τεχνικής αυτής διακρίνουμε στην Εικόνα 61.



Εικόνα 61. Ιεραρχικοποίηση ενός LSP

Για τη διαχείριση των συνδέσμων μεταξύ γειτονικών κόμβων, ένα **Link Management Protocol (LMP)** έχει εισαγχθεί ως ένα GMPLS πρωτόκολλο. Ώς γνωστόν τα πεδία λειτουργικότητας δεδομένων και ελέγχου είναι ξεχωριστά και ανεξάρτητα στο GMPLS. Αυτό ισχύει και για τα καναλια ελέγχου και δεδομένων. Όταν συμβεί μια αστοχία –failure στο κανάλι δεδομένων, είναι εξαιρετικά αναγκαίο να αναγνωρισθεί και να εντοπισθεί το ακριβές σημείο της βλάβης όσο το δυνατόν γρηγορότερα ώστε να επιτευχθεί άμεση ανάκαμψη. Ωστόσο στα παραδοσιακά πρωτόκολλα στα οποία τα δύο αυτά κανάλια δεν είναι ανεξάρτητα, δεν είναι καθόλου δυνατόν να εντοπιστεί μια πιθανή βλάβη στον σύνδεσμο μετάδοσης δεδομένων. Έτσι οι κύριες υπευθυνότητες ενός LMP πρωτοκόλλου είναι: (α) να αντιστοιχεί τον TE σύνδεσμο στον σύνδεσμο δεδομένων που ανήκει σε σχετικό TE constraint set ανάμεσα σε γειτονικούς κόμβους, (β) να αντιστοιχεί τη φυσική διεπαφή ενός τοπικού κόμβου στη αντίστοιχη διεπαφή ενός απομακρυσμένου για τον αντίστοιχο σύνδεσμο δεδομένων που τους συνδέει, και (γ) να εντοπίζει την ακριβή θέση της αστοχίας.

Το LMP διαθέτει τέσσερις κύριες λειτουργικότητες:

Control–channel management

Link–property correlation

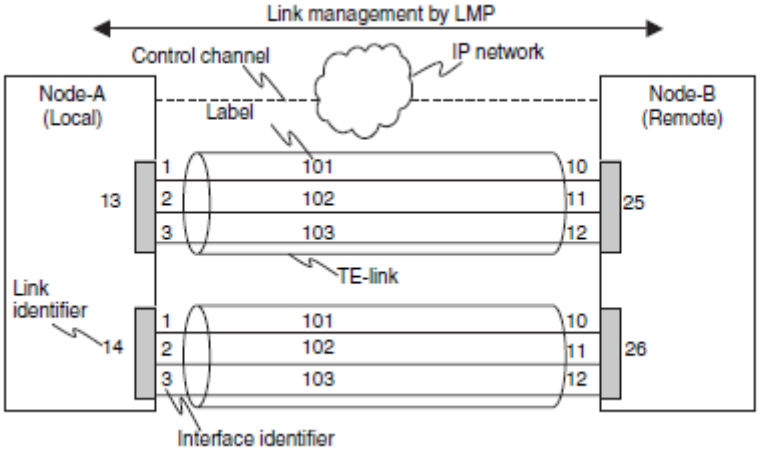
Connectivity certification (προαιρετική)

Failure management (προαιρετική)

Εξετάζουμε συνοπτικά κάθε μια απο αυτές.

Control–channel management. Για να λειτουργήσει σωστά το LMP, θα πρέπει υπάρχει τουλάχιστον ένα αμφίδρομο κανάλι ελέγχου ανάμεσα στους δύο κόμβους που συνδέονται με ένα TE link. Κατα τη δημιουργία ενός τουλάχιστον τέτοιου καναλιού, οι γειτονικοί κόμβοι καλούνται "LMP neighbors". Η κύρια υπευθυνότητα της συγκεκριμένης λειτουργικότητας του LMP είναι η εγκαθίδρυση και η διαχείριση του καναλιού αυτού. Όπως βλεπουμε και στην Εικόνα 62, η επικοινωνία των δεδομένων ελέγχου ανάμεσα σε γειτονικούς κόμβους εκτελείται με ένα IP πρωτόκολλο. Όλα τα LMP πακέτα συμπεριφέρονται ως UDP (User Datagram Protocols) πακέτα έχοντας ένα LMP port number. Το κανάλι ελέγχου κάθε κατεύθυνσης ταυτοποιείται με έναν αναγνωριστή

καναλιού–ελέγχου –control channel identifier. Με την εγκαθίδρυση του καναλιού, ενεργοποιείται το LMP HELLO πρωτόκολλο. Αυτό με τη σειρά του ανταλλάσσει HELLO μηνύματα μεταξύ δύο γειτονικών κόμβων και επιβεβαιώνει την ομαλή λειτουργία του καναλιού ελέγχου.



Εικόνα 62. Link Management Protocol

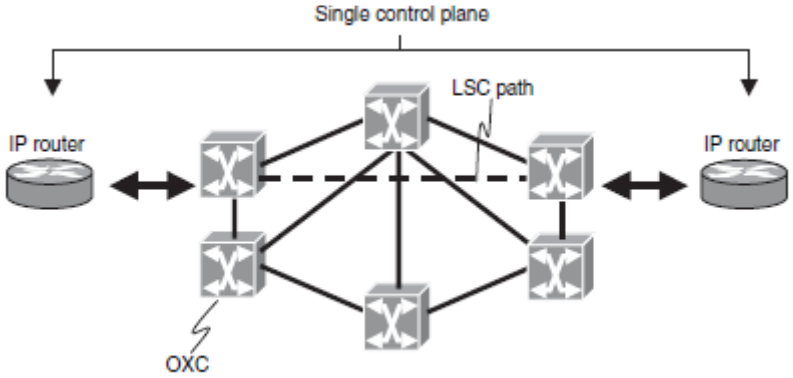
Link–property correlation: Η τεχνική του Link–property correlation εκτελείται για το συγχρονισμό ενός TE συνδέσμου ανάμεσα σε γειτονικούς κόμβους, με το να αντιστοιχίζονται πολλαπλές γραμμές δεδομένων στο TE link αυτό. Κάτι τέτοιο μπορεί να γίνει ύστερα απο χειρωνακτική εγκατάσταση του TE link, είτε ύστερα από μια αυτόματη (σε αυτή τη περίπτωση χρησιμοποιείται η λειτουργικότητα connectivity–verification του LMP). Όπως φαινεται και στην Εικόνα 62, όταν υπάρχουν περισσότερες από μια TE γραμμές, κάθε μια από αυτές διαθέτει ένα link identifier, ενώ κάθε interface της γραμμής διαθέτει και ένα ξεχωριστό interface identifier. Αυτά τα δύο αναγνωριστικά μπορούν να δέχονται IPv4, IPv6 διευθύνσεις ή να είναι unnumbered.

Connectivity certification: Χρησιμοποιείται μόνο κατά την αυτόματη εγκαθίδρυση του TE link. Επειδή ακριβώς είναι εξαιρετικά πολυπλοκο να επιβεβαιώσουμε την συνδεσιμότητα μιας γραμμής δεδομένων αναμεσα σε κόμβους που στέλνουν και λαμβάνουν οπτικά σήματα, χωρίς πρώτα να τα μετατρέψουμε σε ηλεκτρονική μορφή, είναι απαραίτητο η διαδικασία αυτή να γίνει πριν ακόμη μεταδοθοθεί η κίνηση του χρήστη. Κάτι τέτοιο είναι εφικτό με το να γίνεται switched η γραμμή δεδομένων σε μια κατάλληλη συσκευή η οποία μεταδίδει και λαμβάνει ηλεκτρικά σήματα σε κάθε κατεύθυνση, και στη συνέχεια να γίνεται μετάδοση ενός Test μηνύματος στη γραμμή για την τελική επιβεβαίωση της συνδεσιμότητάς της. Παράδειγμα τέτοιων Test μηνυμάτων είναι τα: **BeginVerify, BeginVerifyAck, BeginVerifyNack, End–Verify, EndVerifyAck, TestStatusSuccess, Test, TestFailure, TestStatusAck**.

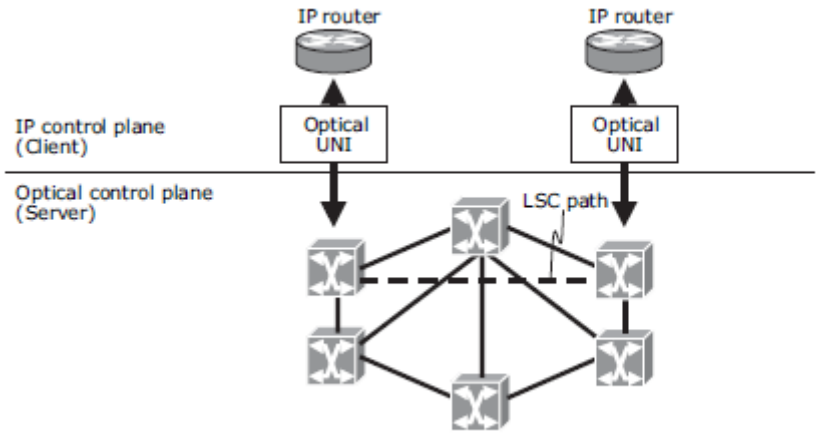
Failure management: Η ικανότητα εντοπισμού μιας βλάβης σε έναν TE σύνδεσμο, καθώς και της ακριβούς θέσης του, καθιστά το δίκτυο επαρκές και ικανό για δυνατότητα εκτεταμένης προστασίας και ανάκαμψης. Ο μηχανισμός αυτός υλοποιείται με μηνύματα όπως: **ChannelStatus, ChannelStatusAck, ChannelStatusRequest, ChannelStatusResponse**. Όταν συμβεί μια αστοχία είναι συχνά πιθανό όλοι οι καθοδικοί κόμβοι του LSP να ανιχνεύουν τη βλάβη, και να παράγουν πολλαπλά alarms χωρίς να εντοπίζουν το ακριβές σημείο της. Για την αποφυγή αυτής της περίπτωσης, υλοποιείται μια ξεχωριστή failure–notification λειτουργικότητα στο LMP. Για τον εντοπισμό , τώρα, της

θέσης της αστοχίας, οι καθοδικοί κόμβοι που ανιχνεύουν την βλάβη ειδοποιούν αντίστοιχα τους ανοδικούς κόμβους, χρησιμοποιώντας ένα ChannelStatus μήνυμα. Ο ανοδικός κόμβος εξετάζει εαν ανιχνεύεται ένα σφάλμα ανοδικής γραμμής ή όχι, και εαν επικρατεί η τελευταία περίπτωση στέλνει ένα ChannelStatus μήνυμα που υποδυκνείει οτι η γραμμή λειτουργεί κανονικά. Στην αντίθετη περίπτωση, εαν δηλαδή ο καθοδικός κόμβος δεν λάβει κάποιο ChannelStatus μήνυμα από τον ανοδικό, στέλνει σε αυτόν ένα ChannelRequest μήνυμα. Αφού στη συνέχεια εντοπιστεί το ακριβές σημείο της βλάβης, εκτελείται η διαδικασία ανάκαμψης από το πρωτόκολλο σηματοδοσίας.

Τέλος να αναφέρουμε στην εισαγωγική αυτή ενότητα για το GMPLS, οτι από τη μεριά του Network Interface, το συγκεκριμένο framework υποστηρίζει δύο τύπους (μοντέλα): το ομότιμο –**peer**, και το επικαλυπτόμενο –**overlay**. Στο πρώτο μοντέλο, όλοι οι IP δρομολογητές και τα OXC's υπάρχουν στο δίκτυο ως ομότιμοι κόμβοι, ενώ διαχειρίζονται απο ένα ενιαίο control plane. Ένα από τα κύρια πλεονεκτήματα του peer μοντέλου είναι οτι μπορεί να εκτελεί end–to–end προστασία και ανάκαμψη ακόμη και όταν υπάρχουν πολλαπλά layers. Τέλος το overlay μοντέλο διαχωρίζεται σε ένα IP control plane και σε ένα optical control plane, και με τα δύο να διασυνδέονται μέσω ενός UNI (User Network Interface). Το IP layer δε μπορεί να γνωρίζει τα χαρακτηριστικά του psychical layer, όπως τοπολογία, πληροφορία δρομολόγησης, και αντίστροφα τα OXC δε μπορούν να γνωρίζουν τις πληροφορίες του IP επιπέδου. Το μοντέλο αυτό μπορούμε να το χαρακτηρίσουμε καλλίτερα ως client–server μοντέλο λογω των ιδιοτήτων του αυτών. Ένα απο τα βασικότερα πλεονεκτήματά του είναι οτι εκμεταλλεύεται πλήρως τα οφέλη του GMPLS, όπως multilayer traffic engineering.



Εικόνα 63. Peer μοντέλο



Εικόνα 64. Overlay μοντέλο

3.2.2 GMPLS ΣΗΜΑΤΟΔΟΣΙΑ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΣΥΝΔΕΣΜΩΝ

Η σηματοδοσία –signaling είναι η διαδικασία εκείνη της ανταλλαγής μηνυμάτων μέσα στο πεδίο λειτουργικότητας ελέγχου –control plane, για την εγκαθίδρυση, συντήρηση, τροποποίηση και τερματισμό των μονοπατιών μετάδοσης δεδομένων του data plane. Στα πλαίσια του GMPLS, αυτά τα μονοπάτια δεδομένων καλούνται LSPs. Η συλλογή όλων των μηνυμάτων σηματοδοσίας και των κανόνων επεξεργασίας τους είναι γνωστά ως πρωτόκολλο σηματοδοσίας –signaling protocol. Τα μηνύματα ελέγχου ανταλάσσονται συνήθως ανάμεσα σε συστατικά λογισμικού στο δίκτυο που καλούνται **signaling controllers**. Κάθε ένας απο αυτούς είναι υπεύθυνος για τη διαχείριση των συστατικών των πεδίων λειτουργικότητας δεδομένων για ένα ή περισσότερους μεταγωγείς –data switches. Στο GMPLS αυτοί οι μεταγωγείς καλούνται **Label Switch Routers –LSRs**. Υπαρχουν δύο προοπτικές για τους ελεγκτές αυτούς: Στη πρώτη ο signaling controller μπορεί να είναι φυσικά ανεξάρτητος από το data switch, με ένα κατάλληλο πρωτόκολλο να χρησιμοποιείται για την μεταξύ τους επικοινωνία, και στη δεύτερη ένας μοναδικός τέτοιος ελεγκτής να διαχειρίζεται περισσότερους από έναν μεταγωγείς –switches.

Οι signaling controllers επικοινωνούν με τους γειτονικούς τους μέσω καναλιών ελέγχου στο control plane. Ένα κανάλι ελέγχου είναι ένας σύνδεσμος, που μπορεί να είναι φυσικός ή λογικός, ανάμεσα σε ελεγκτές υπεύθυνους για διαδοχικά συνδεδεμένους μεταγωγείς στο data plane. Τα κανάλια ελέγχου μπορούν να χρησιμοποιούν τις συνδέσεις δεδομένων ανάμεσα σε ένα ζεύγος από LSRs. Σε αυτή τη περίπτωση, τα μηνύματα ελέγχου και δεδομένων αναμειγνύονται, και το κανάλι ελέγχου χαρακτηρίζεται ως **in band**. Στα οπτικά δίκτυα είναι ασύνηθες να συνδυάζουμε τη κίνηση της σηματοδοσίας και του χρήστη, διότι κάτι τέτοιο θα απαιτούσε από τον εκάστοτε μεταγωγέα να εξετάζει την ροή της κίνησης και να εξάγει τα αντίστοιχα μηνύματα ελέγχου. Αυτή η λειτουργία αφενός θα απαιτούσε ακριβό εξοπλισμό από τη μια, από την άλλη θα ήταν μη πρακτική σε ορισμένες συσκευές όπως OXCs. Έτσι τα μηνύματα ελέγχου θα πρέπει να μεταφέρονται με κάποιον άλλο τρόπο. Μια επιλογή θα ήταν να κάναμε χρήση επιπρόσθετου φορτίου σε ορισμένες κωδικοποιήσεις δεδομένων (όπως TDM), και να μεταφέραμε τη σηματοδοσία μαζί με τα δεδομένα. Κάτι τέτοιο μοιάζει ρεαλιστικό, αλλά απαιτεί κόστος σε bandwidth.

Ένας προτιμότερος μηχανισμός θα ήταν μια **in–fiber–out–of–band** υποστήριξη καναλιού ελέγχου, όπου αφιερώνεται ένα ξεχωριστό κανάλι δεδομένων για την κίνηση σηματοδοσίας. Αυτό μπορέι να είναι dedicated wavelength, ένα timeslot, και χαρακτηρίζεται ως optical supervisory channel –OSC. Ο μόνος περιορισμός είναι οτι το OSC θα πρέπει να τερματίζεται σε κάθε switch, ώστε η κίνηση να παραδίδεται στους κατάλληλους signaling controllers. Εναλλακτικά, θα μπορούσε η συνδεσιμότητα καναλιού ελέγχου να εξυπηρετούνταν από μια διαφορετική φυσική σύνδεση (όπως Ethernet, ή copper καλώδιο). Με αυτήν την **out–of–fiber–out–of–band** τεχνική το όλο κύκλωμα ελέγχου θα χρησιμοποιεί μια φυσική τοπολογία εντελώς ανεξάρτητη από το data plane, και έτσι θα δρομολογήται από ξεχωριστό δίκτυο. Το πλεονέκτημα του GMPLS είναι οτι μπορεί να συνδυάσει τέτοιους διαφορετικούς μηχανισμούς σηματοδοσίας ώστε να παρέχει ευελιξία, ασφάλεια και προστασία.

Μία καθοριστική απαίτηση της σηματοδοσίας είναι η ικανότητά της να αναγνωρίζει τους συνδέσμους και τους κόμβους οι οποίοι θα αποτελέσουν το LSP μονοπάτι στο πεδίο λειτουργικότητας δεδομένων. Αυτό σημαίνει οτι τα στοιχεία αυτά θα πρέπει να διαθέτουν ορισμένα μοναδικά αναγνωριστικά. Την ίδια στιγμή, τα μηνύματα σηματοδοσίας και ελέγχου θα πρέπει να παραδίνονται στους σωστούς ελεγκτές, άρα και αυτοί με τη σειρά τους θα πρέπει να διαθέτουν τέτοια αναγνωριστικά ώστε να είναι δρομολογήσιμοι. Τα αναγνωριστικά αυτά πεδία που χρησιμοποιούνται στο GMPLS είναι στην ουσία IP διευθύνσεις. Η διαχωρισιμότητα , επίσης, του data από το control plane υποδυκνείει οτι θα πρέπει να υπάρχει διαχωρισμός και στην διευθυνσιοδότησή τους. Στο πεδίο λειτουργικότητας ελέγχου χρησιμοποιούνται όλοι εκείνοι οι μηχανισμοί και πρωτόκολλα του IP addressing , και έτσι το control plane αποτελεί ουσιαστικά ένα IP δίκτυο.

Όπως έχουμε ξαναπεί και σε προηγούμενες ενότητες, τα δύο δημοφιλέστερα πρωτόκολλα σηματοδοσίας του GMPLS είναι το **RSVP–TE (Resource Reservation Protocol – with Traffic Engineering Extensions),** και το **CR–LDP (Constraint–based Routed Label Distribution Protocol)**. Στον IETF , τα τελευταία χρόνια, γίνεται εκτεταμένη προσπάθεια να αναγνωριστεί το γεγονός οτι μόνο ένα signaling πρωτόκολλο είναι στην ουσία απαραίτητο.

Στα πλαίσια του RSVP, σύνοδος ή session είναι το σύνολο των ροών κίνησης για έναν προκαθορισμένο προορισμό. Η σύνοδος αναγνωρίζεται με ένα IP address (IPv4 ή IPv6) identifier του προορισμού, και από ένα identifier θύρας στο οποίο θα μεταφερθεί η όλη κίνηση. Εκείνο που κάνει τόσο σημαντική την έννοια της συνόδου είναι οτι οι ροές που τη μοιράζονται, μπορούν τελικά να μοιραστούν πόρους μέσα στο δίκτυο. Έτσι ευνοείται η μετάδοση πακέτων δεδομένων διαφόρων υπηρεσιών –όπως video conferencing σε αντίστοιχες συνόδους οι οποίες μοιράζονται κοινούς πόρους.

Το RSVP–TE εισάγει την έννοια του **MPLS tunnel**. Ένα tunnel διαθέτει μια είσοδο και μια έξοδο. Με εξαίρεση τις περιπτώσεις αστοχιών στο δίκτυο, η είσοδος στο tunnel καθορίζει και την αντίστοιχη έξοδο, ενώ η εισαγωγή δεδομένων εγγυάται την μετάδοσή τους στην έξοδο του tunnel. Στα πλαίσια του Traffic Engineering, το tunnel αποτελεί το βασικό δομικό κομμάτι για τη μεταφορά πακέτων, καθώς οι εφαρμογές ενδιαφέρονται μόνο για τη παράδοση δεδομένων ανάμεσα στα end–points του, ενώ λεπτομέρειες όπως η υποστήριξη του και οι πόροι που πρέπει να διαχειρίζεται εναπόκεινται στο δίκτυο. Κάθε tunnel διαθέτει ένα μοναδικό αναγνωριστικό πεδίο που καλείται **Tunnel Identifier (16–bit)**, και το οποίο χρησιμοποιείται για να ξεχωρίσει διαφορετικά tunnels τα οποία μοιράζονται κοινούς πόρους από πολλαπλές συνόδους.

Ο πυρήνας της λειτουργικότητας του GMPLS είναι η παροχή end–to–end υπηρεσιών στο δίκτυο, κάτι το οποίο μπορεί να θεωρηθεί και ως tunnel. Μία σύνοδος , ωστόσο, δεν είναι αρκετή για τη μεταφορά των δεδομένων. Χρειαζόμαστε LSPs για αυτή τη μεταφορά. Και επειδή η έννοια των μονοπατιών στα πλαίσια του GMPLS είναι ιδιαίτερα αφαιρετική, τα LSPs διαθέτουν , ουσιαστικά, τις ιδιότητες των tunnels και άρα γι'αυτό ονομάζονται και **LSP tunnels**. Επιπλέον, μια υπηρεσία μπορεί να υποστηρίζεται από περισσότερα από ένα LSP. Σε τέτοιες περιπτώσεις αυτά τα LSP μονοπάτια χαρακτηρίζονται παράλληλα, επειδή ακριβώς το ίδιο ζεύγος πηγής και προορισμού χρησιμοποιείται για την εξυπηρέτηση πολλαπλών υπηρεσιών. Τέλος, να αναφέρουμε οτι η έννοια του LSP σχετίζεται όχι μόνο με το πεδίο λειτουργικότητας δεδομένων αλλά και ελέγχου. Στη τελευταία περίπτωση , όπως θα δούμε και στη συνέχεια, χρησιμοποιούνται LSP tunnels για την μετάδοση των control plane μηνυμάτων ελέγχου.

Το LSP –Label Switched Path είναι ένα μονοπάτι στο δίκτυο που σχηματίζεται από cross–connected ετικέτες (που στα πλαίσια του GMPLS αποτελούν πόρους δικτύου) σε μια σειρά από data plane συνδέσμους. Το μονοπάτι που χρησιμοποιεί το LSP μπορεί να επιλεγεί με τρείς διαφορετικούς τρόπους ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής. Ο καθορισμός , έπειτα, του μονοπατιού αυτού είναι απόλυτα εξαρτημένος από τις πληροφορίες που διανέμονται από τα GMPLS πρωτόκολλα δρομολόγησης.

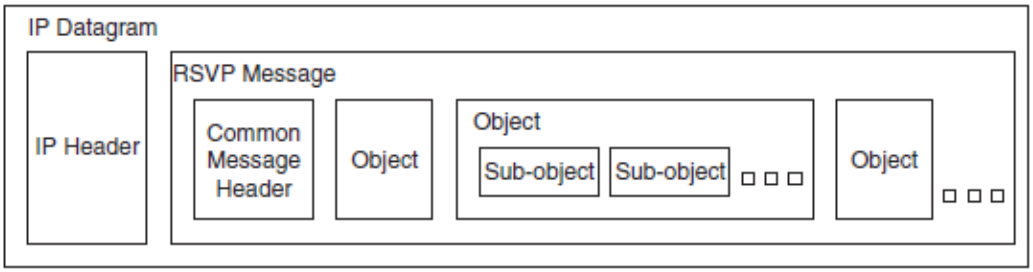
- Το μονοπάτι μπορεί να αφεθεί εντελώς στα πλαίσια του δικτύου να επιλεγεί. Σε αυτή τη περίπτωση, η εφαρμογή που κάνει αίτηση για το LSP απλά καθορίζει το προορισμό, και το μονοπάτι επιλέγεται σε μια hop–by–hop βάση όσο τα μηνύματα σηματοδοσίας δρομολογούνται στο δίκτυο. Σε κάθε LSR το περισσότερο βέλτιστο επόμενο πεδίο λειτουργικότητας δεδομένων προς τον προορισμό επιλέγεται και τα μηνύματα προωθούνται ανάλογα. Αυτή η τεχνική δεν αποτελεί την καλσσική IP δρομολόγηση, αλλά κάνει χρήση του Traffic Engineering Database (TED).
- Το μονοπάτι του LSP μπορεί να προσδιορίζεται πλήρως από την εφαρμογή ή τον διαχειριστή. Εάν ο τελευταίος επιθυμεί να τοποθετήσει ένα LSP πάνω σε ένα μονοπάτι με συγκεκριμένους πόρους, τότε μπορεί να εισάγει ένα explicit path στο control plane. Τα μηνύματα σηματοδοσίας θα επιχειρήσουν να εγκαταστήσουν το LSP σε αυτό το route.
- Εναλλακτικά, ο διαχειριστής ή η εφαρμογή μπορούν να αφήσουν την επιλογή του μονοπατιού στο control plane, αλλά με τη ταυτόχρονη απαίτηση για καθορισμό του μονοπατιού με ορισμένους περιορισμούς –constraints. Σε αυτή τη περίπτωση γίνεται χρήση Constraint–based path computation (CSPF) αλγορίθμων από το πεδίο λειτουργικότητας ελέγχου.

Κατά τη φάση εγκατάστασης του μονοπατιού, το καθοδικό LSR κατανέμει μια ετικέτα ανάλογα με τους διαθέσιμους πόρους και τον εκάστοτε τύπο μεταγωγής. Απαιτείται να ενημερώσει το ανοδικό LSR γι'αυτή την επιλογή, και αυτό το πραγματοποιεί με το να στέλνει πίσω την επιλεγμένη ετικέτα σε ένα Generalized Label object. Αυτό το αντικείμενο είναι απλά μια raw ακολουθία από bits που κωδικοποιεί την ετικέτα, και κανένα Label type δεν της έχει ανατεθεί. Οι περισσότερες ετικέτες (packet, lambda, fiber) κωδικοποιούνται σε ένα 32–bit πεδίο. Η ετικέτα πακέτων , για παράδειγμα, κάνει χρήση των 20 λιγότερων σημαντικών bits.

Η εγκαθίδρυση του LSP αρχικοποιείται από το ingress LSR, το οποίο βρίσκεται στο ανοδικό ρεύμα του εκάστοτε LSP. Το LSP αποκτά αίτηση εγκατάστασης κάνοντας χρήση ενός LSP setup μηνύματος, και επιβεβαιώνεται από το καθοδικό LSR χρησιμοποιώντας ένα LSP confirm μήνυμα. Αστοχίες και λάθη μπορούν να ανιχνευτούν είτε ανοδικά είτε καθοδικά μέσω της χρήσης των LSP Downstream ή LSP Upstream messages. Ένα LSP μπορεί να απελευθερωθεί από ένα οποιοδήποτε LSR του μονοπατιού μέσω των LSP Upstream Release και LSP Downstream Release messages αντίστοιχα. Τέλος, πληροφορίες για την κατάσταση του πεδίου λειτουργικότητας δεδομένων ενός μονοπατιού μπορεί να εξαχθεί από ένα LSP Notify μήνυμα. Στις Εικόνες 63 και 64 διακρίνουμε αντίστοιχα τα RSVP–TE protocol μηνύματα και το format ενός από αυτά.

Abstract message	RSVP-TE Protocol message
LSP Setup	Path
LSP Accept	Resv
LSP Confirm	ResvConfirm
LSP Upstream error	PathErr
LSP Downstream error	ResvErr
LSP Downstream release	PathTear
LSP Upstream release	PathErr
LSP Notify	Notify

Εικόνα 65. RSVP–TE μηνύματα ελέγχου



Εικόνα 66. Format του GMPLS RSVP–TE μηνύματος

Μόλις το LSP μονοπάτι εγκατασταθεί, θέλουμε να παραμείνει ενεργό μέχρι η αντίστοιχη υπηρεσία (το GMPLS tunnel) να μην είναι πλεον απαραίτητη. Γι'αυτόν ακριβώς το λόγο, το RSVP καθορίζει τα PATH μηνύματα να επαναμεταδίδονται περιοδικά (refreshed) καθώς και να ακολουθούν τα ίδια μονοπάτια προς τον προορισμό όπως και οι γραμμές δεδομένων. Σε αυτή τη περίπτωση, εάν υπάρξει κάποια αλλαγή στο δίκτυο, τα PATH μηνύματα θα προσαρμοστούν στις νέες αλλαγές, νέα RESV μηνύματα θα επιστραφούν και οι πόροι θα καθιστούν διαθέσιμοι στα νέα μονοπάτια. Συγκεκριμένα, το RSVP καθορίζει οτι εαν ο ανοδικός router επαναμεταδίδει PATH messages, ο καθοδικός δρομολογητής μπορεί να θεωρήσει οτι οι πόροι (που έχει δεσμεύσει) δεν είναι πλεον απαραίτητοι εαν δεν λάβει κάποιο μήνυμα μετά από κάποιο χρονικο interval. Παρομοίως το RSVP πρωτόκολλο καθορίζει οτι το RESV μήνυμα θα πρέπει να επαναμεταδίδεται έστι ώστε να ανιχνεύει αλλαγές και αστοχίες στο δίκτυο. Το γεγονός αυτό καθιστά το RSVP ως ένα soft state πρωτόκολλο, κάτι που μπορεί να δημιουργήσει, δηστυχώς, φαινόμενα κακής κλιμάκωσης ειδικά οταν ο router διαχειρίζεται χιλιάδες ροές.

Ας δούμε τώρα λίγο συνοπτικά τις περιπτώσεις σηματοδοσίας ελέγχου έπειτα από κατάρρευση μονοπατιών. Στο GMPLS χρησιμοποιείται κατα κόρον το LSP Upstream Error μήνυμα κατά τη φάση αστοχιών. Συγκεκριμένα, αποκτά ιδιαίτερο ρόλο όταν ένα LSP Request μήνυμα εγκαθίδρυσης μονοπατιού δεν μπορεί να ικανοποιηθεί. Για παράδειγμα, μπορεί να μην υπάρχουν διαθέσιμοι πόροι για να ικανοποιήσουν το αίτημα, ή να είναι αδύνατο να δρομολογηθεί το μονοπάτι βάση του explicit route που παρέχεται. Το LSP Upstream Error message αποστέλλεται σαν απάντηση στο LSP Request και μπορεί να παρέχει σημαντικές πληροφορίες ώστε να επιτρέπει επαναδρομολόγηση του LSP. Το LSP Upstream Error μήνυμα μπορεί να χρησιμοποιείται και για αναφορά αστοχιών ή προβλημάτων με προεγκατεστημένα LSPs. Σε τέτοιες περιπτώσεις ενημερώνεται το control plane για τη βλάβη, και με κατάλληλες ενέργειες το LMP –Link Management Protocol πετυχαίνει την απομόνωσή της.

Οι GMPLS κόμβοι μπορεί να συνδέονται μεταξύ τους με πολλαπλά κανάλια δεδομένων και συνδέσμους. Κάθε κανάλι μπορεί να είναι οπτική ίνα, αλλά είναι πιθανό σε κάθε ίνα να υπάρχουν εξίσου πολλοί σύνδεσμοι , όπως για παραδειγμα διαφορετικά χρώματα –lambdas. Ένα ζεύγος από γειτονικούς κόμβους θα πρέπει να είναι ικανό να αναφέρεται σε κάθε τέτοιο κανάλι δεδομένων με διακριτό τρόπο. Αυτό μπορεί να επιτευχθεί μέσω της παραμετροποίησης κάθε LSR, αλλά όσο ο αριθμός των καναλιών δεδομένων αυξάνει, δημιουργείται επιπλέον φόρτος στο δίκτυο. Το πρόβλημα αντιμετωπίζεται με το Πρωτόκολλο Διαχείρισης Συνδέσμων –Link Management Protocol (LMP), το οποίο βοηθάει τους δρομολογητές να αναγνωρίζουν το είδος και τη κατάσταση των συνδέσμων τους, όπως και τον εντοπισμό και απομόνωση πιθανών αστοχίων στο δίκτυο.

Το LMP πρωτόκολλο είναι ένα point–to–point πρωτόκολλο εφαρμογών που τρέχει πάνω σε UDP χρησιμοποιώντας τη θύρα 701. Απαιτεί την προκαθορισμένη παραμετροποίηση των διευθύνσεων των καναλιών δεδομένων σε κάθε κόμβο, ενώ για την διατήρηση της LMP γειτνίασης είναι απαραίτητη η ύπαρξη ενός καναλιού ελέγχου. Απαιτείται παράλληλα η ύπαρξη ενός μοναδικού αναγνωριστικού σε κάθε κόμβο, που καλείται Control Channel ID (CCID). Το πρωτόκολλο διαθέτει ορσμένα διακριτά λειτουργικά τμήματα:

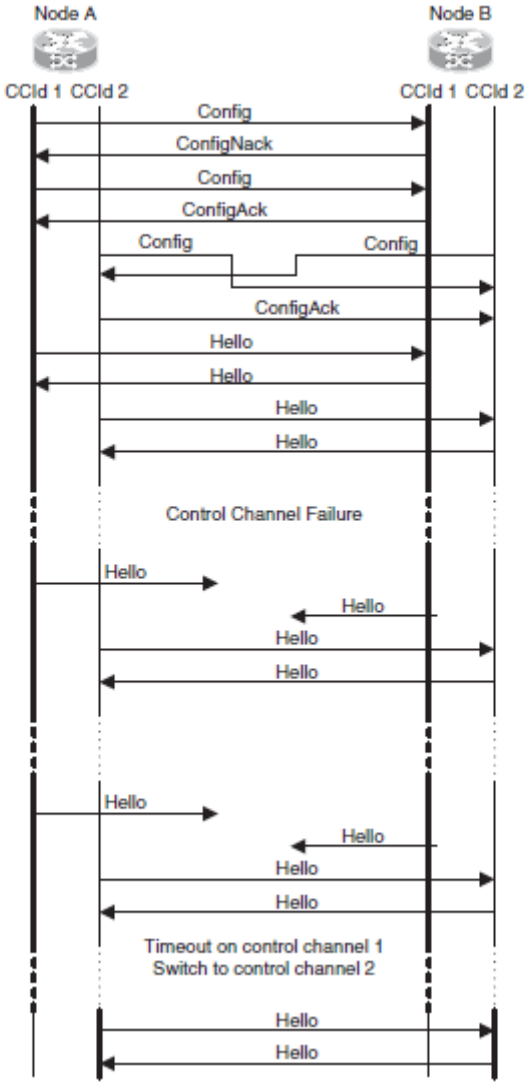
- Η διαχείριση του καναλιού ελέγχου –Control Channel Management ξεκινάει με την φάση της Αρχικοποίησης, κατά την διάρκεια της οποίας οι LMP γείτονες ανταλλάσουν HELLO μηνύματα ώστε να ενεργοποιήσουν το κανάλι ελέγχου και να εγκαθιδρύσουν τα αναγνωριστικά τους.
- Η φάση ανίχνευσης γραμμής –Link Discovery βοηθάει το LSR να ανιχνεύσει την ύπαρξη, συνδεσιμότητα και τύπο των συνδέσμων δεδομένων από και προς τους γείτονες του. Αρχικά ο κόμβος αυτός γνωρίζει την ύπαρξη τέτοιων γειτόνων αλλά όχι και την κατάστασή τους. Όλες αυτές οι ερωτήσεις λύνονται με την ανταλλαγή κατάλληλων μηνυμάτων.
- Η φάση της ανταλλαγής δεδομένων των Ικανοτήτων του συνδέσμου μπορεί να ακολουθεί την προηγούμενη φάση, ώστε το εκάστοτε LSR να γνωρίζει τα ειδικά χαρακτηριστικά των γραμμών δεδομένων , οπως την ύπαρξη TE συνδέσεων για το χτίσιμο της αντίστοιχης τοπολογίας.
- Η φάση της επιβεβαίωσης των συνδέσμων μπορεί να εκτελείται περιοδικά για την ανίχνευση της κατάστασης και συνδεσιμότητας των γραμμών ιδιαίτερα μετά από περιπτώσεις αστοχίας.

- Η φάση της απομόνωσης βλαβών. Είναι η κυριότερη λειτουργικότητα του πρωτοκόλλου καθώς ανιχνεύονται αστοχίες και λάθη σε φυσικό επίπεδο , όπως φαινόμενα loss of light LOS, διατάραξη σήματος και προβλήματα framing, κυρίως από τον καθοδικό κόμβο –downstream node.
- Η φάση της επιβεβαίωσης. Είναι σημαντικό να τονίσουμε οτι στα πλαίσια του LMP υπάρχουν όλες εκείνες οι διαδικασίες που εγγυώνται οτι οι LMP ομότιμοι κόμβοι επικοινωνούν μεταξύ τους με έγκυρα μηνύματα και λειτουργίες.

Τα LMP μηνύματα κατασκευάζονται από ένα κοινό μήνυμα επικεφαλίδας που αναγνωρίζει τον τύπο και το μήκος του μηνύματος αυτού, ακολουθούμενο από ένα σύνολο από message objects. Κάθε τέτοιο αντικείμενο αναγνωρίζεται από μια κλάση που υποδυκνείει τον τύπο του object και έναν τύπο κλάσης που καθορίζει την χρήση του αντικειμένου. Το object μεταφέρει ένα πεδίο μήκους με το μέγεθος του αντικειμένου, ενώ το υπόλοιπο κομμάτι του αφιερώνεται στη μετάδοση των δεδομένων. Εφόσον το LMP μεταφέρεται μέσω του UDP πρωτοκόλλου μεταφοράς, πρέπει να λαμβάνει ορισμένα μέτρα που θα εγγυώνται ασφαλή παραλαβή των δεδομενών, όπως ειδικά αναγνωριστικά και επιβεβαιώσεις.

Ας δούμε λίγο συνοπτικά μερικές από τις πιό πάνω λειτουργικότητες του LMP. Ένα LMP κανάλι ελέγχου γίνεται λειτουργικό όταν το ένα άκρο του στέλνει ένα **Config** μήνυμα. Το μήνυμα αυτό αναγνωρίζει το τοπικό άκρο του καναλιού αυτού (με ένα CCID –Control Channel Identifier), και μεταφέρει κατάλληλες παραμέτρους για να εφαρμοστούν ανάμεσα στους δύο τελικούς κόμβους. Ο παραλήπτης του Config μηνύματος απαντάει με ένα **ConfigAck** μήνυμα ώστε να δεχθεί τις παραμέτρους αυτές και να παράσχει τους δικούς του identifiers. Το ConfigAck μήνυμα περιλαμβάνει τον κόμβο, το κανάλι ελέγχου, και τους message identifiers από το λαμβανόμενο Config message. Εαν ο παραλήπτης αυτός επιθυμεί να διαπραγματευτεί την όλη παραμετροποίηση, στέλνει ένα **ConfigNack** μήνυμα πίσω στον αρχικό κόμβο. Η Config/ConfigAck ανταλλαγή προσδιορίζει ένα LMP peer ως τον αρχικό κόμβο και έναν άλλο ως τον αποδέκτη. Πολλαπλά κανάλια ελέγχου μπορούν να είναι ενεργά την ίδια χρονική στιγμή ανάμεσα σε ένα ζεύγος από LMP peers. Αυτοί πραγματοποιούν τα ίδια βήματα αρχικοποίησης που προαναφέρθησαν σε κάθε αντίστοιχο κανάλι. Το πλεονέκτημα αυτής τη φάσης είναι οτι στη περίπτωση που καταρρεύσει ένα κανάλι ελέγχου, η LMP επεξεργασία μπορεί να μεταφερθεί σε άλλο κανάλι. Τα control channels παραμένουν ενεργά μέσω της περιοδικής ανταλλαγής HELLO μηνυμάτων. Το HELLO interval είναι μια από αυτές τις παραμέτρους που αποτελεί αντικείμενο διαπραγμάτευσης στην Config ανταλλαγή μηνυμάτων. Εαν μετά απο το HELLO dead interval, οποισδήποτε κόμβος δεν λάβει το αντίστοιχο HELLO μήνυμα, μαρκάρει το κανάλι ελέγχου ως νεκρό–ανενεργό, και ξεκινάει τις διαδικασίες ενεργοποίησης νέου καναλιού.

Η Εικόνα 67 δείχνει την εγκατάσταση δύο καναλιών ελέγχου ανάμεσα στα LSRs A και B. Το πρώτο control channel (CCID 1) ενεργοποιείται από το LSR A. Το LSR B απορρίπτει τις παραμέτρους κάνοντας χρήση ενός ConfigNack μηνύματος, και ο LSR A ξαναστέλνει ένα νέο Config μήνυμα που αυτή τη φορά αποδέχεται από τον B. Το δεύτερο κανάλι ενεργοποιήται ταυτόχρονα και από τα δύο LSRs, αλλά επειδή ο κόμβος B έχει μεγαλύτερο node ID από τον A, αυτός (ο B) καθίσταται ως ο αρχικός LMP κόμβος.

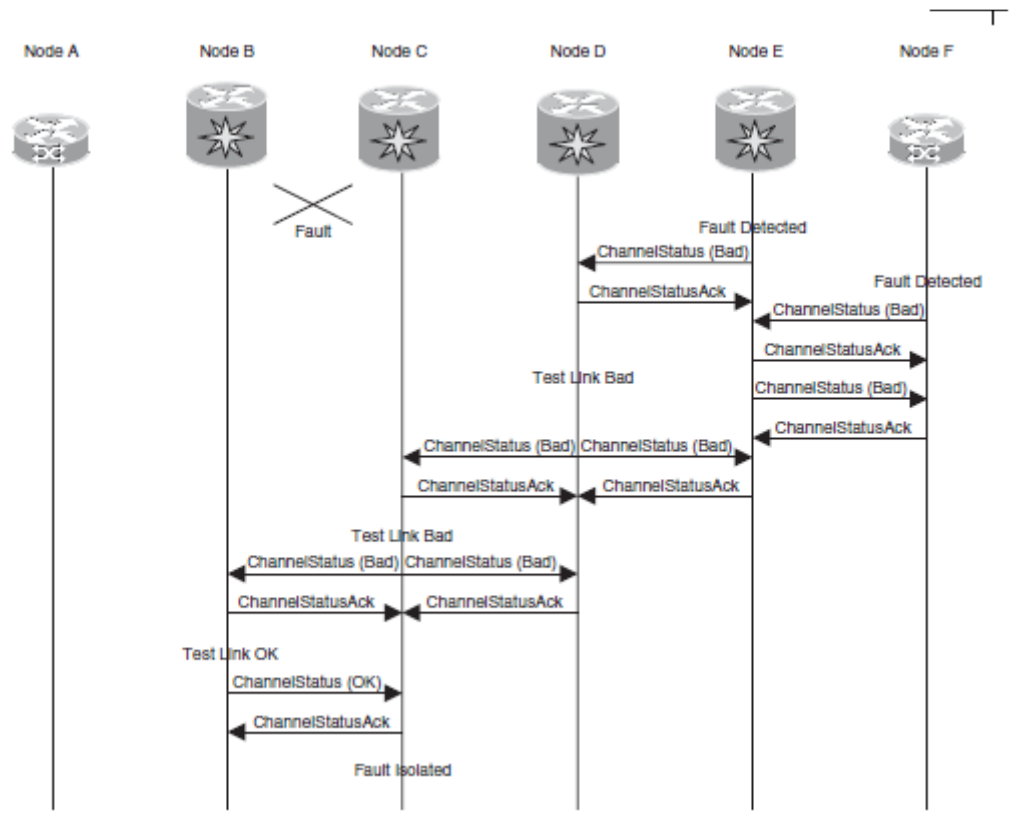


Εικόνα 67. Εγκατάσταση δύο καναλιών ελέγχου στο LMP

Η ανίχνευση και επιβεβαίωση σύνδεσης είναι ταυτοτικές διαδικασίες που οδηγούν στην ανακάλυψη της συνδεσιμότητας των data links ανάμεσα σε ένα ζεύγος από κόμβους. Αρχικά ένας κόμβος γνωρίζει τα τοπικά αναγνωριστικά του για τις συνδέσεις που πιστεύει οτι τον ενώνουν με έναν διαδοχικό κόμβο, αλλά ωστόσο δεν γνωρίζει την κατάστασή τους καθώς και τους απομακρυσμένους identifiers των άλλων κόμβων. Στο GMPLS, τα LSRs χρησιμοποιούν τις interface ID αντιστοιχήσεις που καθορίζονται από την LMP επιβεβαίωση γραμμής, ώστε να σηματοδοτήσουν ποιά γραμμή να μεταφέρει το LSP. Η πληροφορία αυτή είναι εξίσου απαράιτητη για τα TE συστατικά του δικτύου ώστε να συγχρονίσουν τα advertisements σε όλους τους συνδέσμους τους. Η διαδικασία

επιβεβαίωσης βασίζεται στην ανταλλαγή **BeginVerify/beginVerifyAck** και **EndVerify/EndVerifyAck** μηνυμάτων.

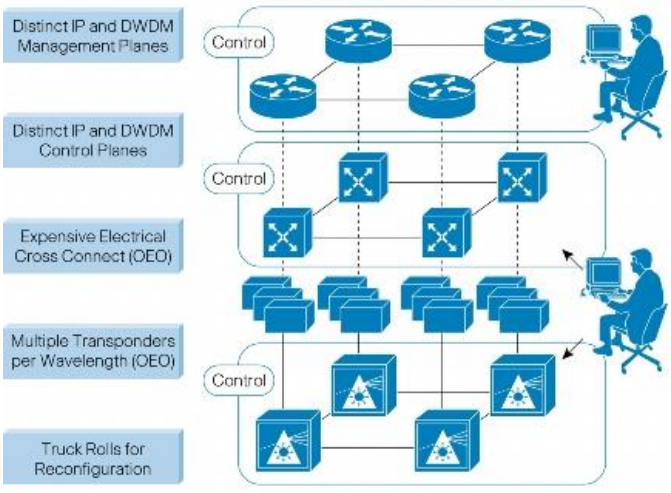
Τέλος, αξίζει να σημειώσουμε οτι αν και προαιρετικώς, το LMP διαθέτει έναν μηχανισμό απομόνωσης βλαβών –fault isolation στο δίκτυο. Επειδή ακριβώς τα συστατικά του οπτικού δικτύου είναι transparent, δηλαδή κάνουν switching στα δεδομένα χωρίς να τα εξετάζουν, σε περιπτώσεις αστοχιών θα είναι εξαιρετικά δύσκολο να πραγματοποιηθεί αφενός ο ακριβής εντοπισμός της βλάβης, αφετέρου να λειτουργήσει αποδοπτικά ο μηχανισμός απομόνωσής της. Γι'αυτο το λόγο, το LMP διαθέτει μια διαδικασία όπου αρχικοποιείται από έναν καθοδικό κόμβο ο οποίος εντοπίζει το πρόβλημα σε ένα σύνδεσμο δεδομένων. Ο κόμβος στέλνει ένα **ChannelStatus** message ανοδικά, κάνοντας χρήση του καναλιού ελέγχου και αμέσως λαμβάνει μια επιβεβαίωση. Ο ανοδικός κόμβος που λαμβάνει το μήνυμα θεωρεί πλέον οτι είναι ασφαλές να εξετάσει το σήμα δεδομενων, ενώ παράλληλα ελέγχει εαν λαμβάνει ικανοποιητικό σήμα από τον γειτονικό του κόμβο. Στη περίπτωση που το λαμβάνει, η αστοχία έχει απομονωθεί και στέλνει αμέσως ένα ChannelStatus μήνυμα που αναφέρει οτι η σύνδεση είναι ασφαλής. Στην αντίθετη περιπτωση αποστέλλει ένα μήνυμα που περιγράφει λεπτομερειακά το πρόβλημα.



Εικόνα 68. Ο LMP μηχανισμός εντοπισμού και απομόνωσης βλαβών

3.2.3 ΤΟ ΠΕΔΙΟ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ ΕΛΕΓΧΟΥ ΤΟΥ GMPLS (GMPLS CONTROL PLANE)

Όσο τα IP δίκτυα μεταφοράς εξελίσσονταν –επηρεασμένα από τις διαφορετικές απαιτήσεις σε χρονικό και χρηστικό επίπεδο–, ανέπτυξαν ανεξάρτητους και ασύμβατους μεταξύ τους μηχανισμούς ελέγχου για την μετάδοση της πληροφορίας ανάμεσα σε πηγή και προορισμό. Τα δίκτυα μεταφοράς σήμερα βασίζονται αποκλειστικά σε προκαθορισμένα μονοπάτια τα οποία παραμετροποιούνται είτε με διάφορα πεδία λειτουργικότητας –panels, είτε μέσω προ–εγκατεστημένων κυκλωμάτων στους οπτικούς μεταγωγείς κατα την σύνδεση της θύρας εισόδου και εξόδου. Σε ορισμένες περιπτώσεις κάποιο μικρό ποσοστό του εύρους ζώνης κατανέμεται για την επικοινωνία της σηματοδοσίας ελέγχου ώστε να αυτοματοποιηθεί σε κάποιο βαθμό η διαδικασία εγκαθίδρυσης μονοπατιού. Ωστόσο η τοπολογία του δικτύου δεν ανανεώνεται σε πραγματικό χρόνο στα συστήματα διαχείρισης, κάτι που έχει ως αποτέλεσμα ογκώδεις βάσεις δεδομένων και μεγάλους χρόνους διεκπεραίωσης. Μεγάλης κλίμακας δίκτυα μπορεί να απαιτήσουν και εβδομάδες να παραμετροποιηθούν, επειδή νέα wavelengths χρειάζονται ειδική επίβλεψη ανάμεσα στα τελικά σημεία. Τα IP/MPLS δίκτυα έχουν εξελιχθεί με έναν περισσότερο αυτοματοποιημένο τρόπο, ο οποίος εφαρμόζεται στα περισσότερα packet–based networks, και έτσι ανταλλάσουν πληροφορία ελέγχου κάνοντας χρήση πρωτοκόλλων όπως BGP και LDP. Η χρήση αυτών των πρωτοκόλλων προσφέρει την απαιτούμενη ευφυεία για την αυτο–διαχείριση και αυτο–βελτίωση της κίνησης, βασισμένη σε δυναμικές συνθήκες και χαρακτηριστικά στο δίκτυο.



Εικόνα 69. Η σημερινή αρχιτεκτονική των πεδίων λειτουργικότητας δικτύων

Στη συγκεκριμένη θεματική ενότητα θα εστιάσουμε σε όλες εκείνες τις τεχνολογικές προεκτάσεις της GMPLS σηματοδοσίας για τον έλεγχο των Οπτικών Δικτύων Μεταφορών –Optical Transport Networks (OTN). Ως γνωστόν το Generalized framework επεκτείνει το ήδη υπάρχον MPLS πρωτόκολλο με το να υποστηρίζει πέραν των Packet Switching Capable (PSC) interfaces, και άλλους τέσσερις επιπλέον τύπους όπως Layer–2 Switching (L2SC), Time–Division Multiplex (TDM), Lambda Switch (LSC), και Fiber–Switch (FSC) Capable. Είναι απαραίτητο να επισημανθούν όλες εκείνες οι επεκτάσεις σηματοδοσίας που σχετίζονται με το G. 709 Optical Transport Network, όπως καθορίζονται από το προιον τυποποίησης ITUT–G709. Οι παράμετροι αυτοί κίνησης οφείλουν να χρησιμοποιούνται όταν η ετικέτα κωδικοποιήται όπως καθορίζεται στο παρών κείμενο.

Το ITUT–G709 καθορίζει διάφορα επίπεδα δικτύου που σχηματίζουν την ιεραρχία οπτικής μεταφοράς:

— Με πλήρη λειτουργικότητα:
  - **Optical Transmission Section (OTS)**
  - **Optical Multiplex Section (OMS)**
  - **Optical Channel (OCh)**
— Με περιορισμένη λειτουργικότητα:
  - **Optical Physical Section (OPS)**
  - **Optical Channel με περιορισμένη λειτουργικότητα (OChr)**

Επιπλέον καθορίζει δύο επίπεδα που σχηματίζουν την ιεραρχία ψηφιακής μετάδοσης:

— **Optical Channel Transport Unit (OTUk)**
— **Optical Channel Data Unit (ODUk)**

Όπως αναφέρθηκε και σε προηγούμενες ενότητες το LSP Encoding Type, το Switching Type, και το Generalized Protocol Identifier (Generalized–PID) καθιστούν τμήμα του Generalized Label Request –αιτήματος γενικευμένης ετικέτας. Επειδή οι G. 709 συστάσεις καθορίζουν δύο νέα επίπεδα δικτύου (ODUk και OCh), το LSP Encoding Type αντικατοπτρίζει αυτά τα επίπεδα ως "Digital Wrapper" και "Lambda" κώδικα αντίστοιχα. Ως αποτέλεσμα οι ακόλουθες νές οδηγίες καθορίζονται για το LSP Encoding Type:

Value	Type
12	G. 709 ODUk (Digital Path)
13	G. 709 Optical Channel

Το Switching Type υποδεικνείει τον τύπο της μεταγωγής που θα πρέπει να εφαρμόζεται στο σημείο τερματισμού της αντίστοιχης γραμμής. Στην προκειμένη περίπτωση καμία επιπρόσθετη switching type πληροφορία δεν χρειάζεται να επιβληθεί διότι η ODUk μεταγωγή ανήκει στην TDM κλάση, και η OCh αντίστοιχα ανήκει στην Lambda κλάση.

Το GPID (16–bit πεδίο) υποδυκνείει το φορτίο που μεταφέρεται από ένα LSP, και μπορεί να λάβει τις ακόλουθες τιμές όταν τα πακέτα του χρήστη μεταφέρονται από το Digital Path Layer:

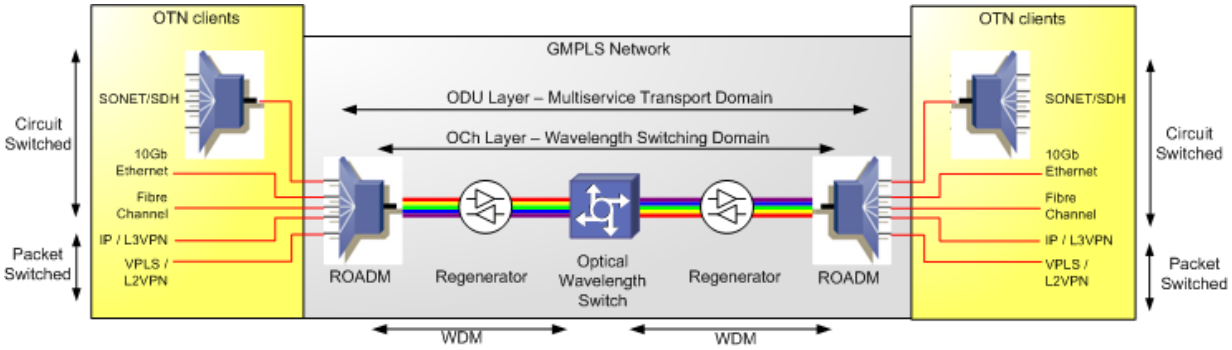
- CBRa: asynchronous Constant Bit Rate (i. e. , mapping of STM-16/OC-48, STM-64/OC-192 and STM-256/OC-768)
- CBRb: bit synchronous Constant Bit Rate (i. e. , mapping of STM-16/OC-48, STM-64/OC-192 and STM-256/OC-768)
- ATM: mapping at 2. 5, 10 and 40 Gbps
- BSOT: non-specific client Bit Stream with Octet Timing (i. e. , Mapping of 2. 5, 10 and 40 Gbps Bit Stream)
- BSNT: non-specific client Bit Stream without Octet Timing (i. e., Mapping of 2. 5, 10 and 40 Gbps Bit Stream)
- ODUk: transport of Digital Paths at 2. 5, 10 and 40 Gbps

- ESCON: Enterprise Systems Connection
- FICON: Fiber Connection

Τέλος ο ακόλουθος πίνακας περιλαμβάνει τις τιμές του GPID αναφορικά με το LSP Encoding Type.

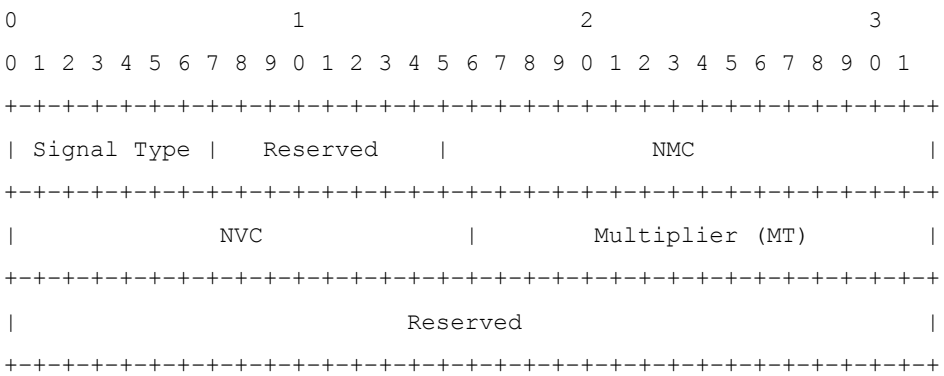
Value	G-PID Type	LSP Encoding Type
47	G. 709 ODUj	G. 709 ODUk (with k > j)
48	G. 709 OTUk (v)	G. 709 OCh ODUk mapped into OTUk (v)
49	CBR/CBRa	G. 709 ODUk, G. 709 OCh
50	CBRb	G. 709 ODUk
51	BSOT	G. 709 ODUk
52	BSNT	G. 709 ODUk
53	IP/PPP (GFP)	G. 709 ODUk (and SDH)
54	Ethernet MAC (framed GFP)	G. 709 ODUk (and SDH)
55	Ethernet PHY (transparent GFP)	G. 709 ODUk (and SDH)
56	ESCON	G. 709 ODUk, Lambda, Fiber
57	FICON	G. 709 ODUk, Lambda, Fiber
58	Fiber Channel	G. 709 ODUk, Lambda, Fiber

Όταν το G. 709 Digital Path Layer ή το G. 709 Optical Channel Layer καθορίζεται στο πεδίο LSP Encoding Type, η επιπλέον αυτή πληροφορία θα πρέπει να συμπεριληφθεί στο αίτημα γενικευμένης ετικέτας.



Εικόνα 70. Το G. 709 OTN Μοντέλο

Οι παράμετροι κίνησης του G. 709 καθορίζονται ως εξής:



Σε αυτό το πλαίσιο, το **NMC** σημαίνει **Number of Multiplexed Components – αριθμός πολυπλεγμένων στοιχείων**, **NVC Number of Virtual Components** –αριθμός εικονικών στοιχείων, και **MT** για **Multiplier –πολλαπλασιαστή**.

Συγκεκριμένα, το πρώτο πεδίο Signal Type (8–bit) υποδυκνείει τον τύπο του G. 709 σήματος για την εγκαθίδρυση του LSP μονοπατιού. Ακολουθούν οι επιτρεπτές τιμές:

Value	Type
0	Not significant
1	ODU1 (i. e., 2. 5 Gbps)
2	ODU2 (i. e., 10 Gbps)
3	ODU3 (i. e., 40 Gbps)
4	Reserved (for future use)
5	Reserved (for future use)
6	OCh at 2. 5 Gbps
7	OCh at 10 Gbps
8	OCh at 40 Gbps
9–255	Reserved (for future use)

Εαν για παράδειγμα ο τύπος κωδικοποίησης του LSP περιέχει σαν τιμή το G. 709 Digital Path Layer, τότε οι έγκυρες τιμές του είναι τα ODUk σήματα (k = 1, 2, 3). Εαν είναι σαν τιμή το G. 709 Optical Channel Layer, τότε παίρνει τα OCh στα 2. 5, 10 ή 40 Gbps.

Από την άλλη ο αριθμός πολυπλεγμένων στοιχείων (NMC) (16–bit πεδίο) παριστάνει τον αριθμό των ODU θυρών που χρησιμοποιούνται από ένα ODUj οταν πολυπλέκονται σε ένα ODUk (k > j), για το απαιτούμενο LSP. Στη συνέχεια, το NVC πεδίο (16–bit) υποδυκνείει τον αριθμό των ODU1, ODU2 ή ODU3 πρωτότυπων σημάτων τα οποία είναι απαραίτητο να συνενωθούν εικονικά για τη δημιουργία ενό ODUk–Xv σήματος. Εξ' ορισμού αυτά τα σήματα πρέπει να είναι του ιδίου τύπου. Τέλος, ο πολλαπλασιαστής Multiplier (MT) υποδυκνείει τον αριθμό των ταυτοτικών ήδη διαμορφωμένων ή πρωτότυπων σημάτων που είναι απαραίτητα για την εγκαθίδρυση του LSP, και που σχηματίζουν το τελικό σήμα ελέγχου.

Τέλος, θα αναφερθούμε στις αναγκαίες επεκτάσεις του RFC3473 πρωτοκόλλου για την χρήση των G. 709 παραμέτρων κίνησης. Αυτοί οι παράμετροι μεταφέρονται στα G. 709 SENDER_TSPEC και FLOWSPEC αντικείμενα. Χρησιμοποιείται το ίδιο ακριβώς format και για τα δύο objects, ενώ περιέχουν τις ακόλουθες κλάσεις και τύπους:

– G. 709 SENDER_TSPEC Object: Class = 12, C–Type = 5

– G. 709 FLOWSPEC Object: Class = 9, C–Type = 5

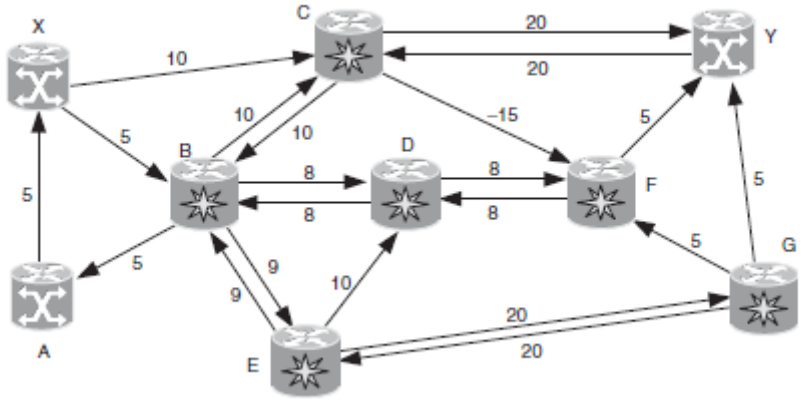
Για έναν συγκεκριμένο αποστολέα σε μία RSVP σύνοδο, τα περιεχόμενα του FLOWSPEC αντικειμένου που λαμβάνονται σε ένα RESV μήνυμα **θα πρέπει να είναι παρόμοια** με τα περιεχόμενα του SENDER_TSPEC object τα οποία λαμβάνονται στο Path μήνυμα. Εαν τα αντικείμενα αυτά δεν ταιριάζουν, ένα ResvErr μήνυμα με τιμή **"Traffic Control Error/Bad Flowspec value"** μήνυμα σφάλματος θα πρέπει να πυροδοτείται. Τέλος, οι ενδιάμεσοι κόμβοι καθώς και οι κόμβοι σημείου εξόδου (egress) οφείλουν να επιβεβαιώνουν οτι ο αντίστοιχος κόμβος καθως και τα interfaces που θα εγκατασταθεί το LSP, μπορούν να υποστηρίξουν τις προηγούμενες τιμές των Signal Type, NMC και NVC.

3.2.4 GMPLS ΑΛΓΟΡΙΘΜΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ

Στο σημερινό, ιδιαίτερα απαιτητικό και ανταγωνιστικό περιβάλλον των Service Providers, οι χρήστες απαιτούν ιδιαίτερα υψηλή ποιότητα και στάνταρτς από τις επικοινωνιακές υπηρεσίες που αγοράζουν. Πιό συγκεκριμένα, δεν ανέχονται διακοπή της πρόσβασης τους σε υπηρεσίες για χρονικά διαστήματα περισσότερο από μερικά δεκάδες χιλιοστά του δευτερολέπτου. Η πραγματικότητα είναι ωστόσο οτι τα δικτυακά στοιχεία των Παρόχων παθαίνουν αστοχίες. Έτσι ο μόνος τρόπος να εγγυηθούμε ομαλή λειτουργία στη παροχή υπηρεσιών είναι κάποιας μορφής προστασία. Μια υπηρεσία συνήθως αντιστοιχίζεται σε περισσότερα του ενός μονοπάτια, έτσι ώστε όταν ένα από αυτά καταρρεύσει ένα δευτερεύον μονοπάτι να λειτουργήσει ως ενναλακτικό. Ακόμη και σε αυτή τη περίπτωση βέβαια μια διατάραξη της υπηρεσίας θα είναι αναπόφευκτη. Το μέγεθός της θα είναι σαφώς μικρότερο από την κατάσταση οπού δεν υπάρχει καμία προστασία και απαιτούνται εκ του μηδενός διαδικασίες καθορισμού μονοπατιού και σηματοδοσίας. Τα μονοπάτια αυτά θα πρέπει να είναι διακριτά –να χειρίζονται δηλαδή διακριτούς δικτυακούς πόρους –. Γι'αυτόν ακριβώς τον λόγο ο καθορισμός μονοπατιού είναι καθολικής σημασίας στο GMPLS. Σε αυτή τη θεματική ενότητα θα περιγράψουμε τους δημοφιλέστερους path computation αλγορίθμους.

Ο καθορισμός μονοπατιού –path computation είναι η διαδικασία της επιλογής εκείνου του μονοπατιού που απαιτείται βάσει των ζητούμενων προδιαγραφών της εκάστοτε δικτυακής υπηρεσίας. Υπάρχουν δύο τρόποι να επιτευχθεί χρονικα: κατά τη διάρκεια της επίβλεψης της υπηρεσίας (on–line path computation), και έπειτα από αυτη (off–line path computation). Εαν όλα τα μονοπάτια μιας υπηρεσίας υπολογίζονται σε ένα μόνο κόμβο, αυτός ο καθορισμός καλείται centralized. Στην άλλη περίπτωση έχουμε τον κατανεμημένο υπολογισμό μονοπατιού –distributed path computation, όταν πολλές δικτυακές οντότητες συνεργάζονται για να ικανοποιήσουν ένα μοναδικό αίτημα καθορισμού μονοπατιού.

Ένα δίκτυο μεταφοράς αναπαριστάνεται συνήθως από ένα συνεκτικό γράφημα με βάρη–κόστη στις πλευρές–ακμές του. Παράδειγμα τέτοιου γραφήματος έχουμε στην Εικόνα 71.



Εικόνα 71. Δίκτυο Μεταφοράς ως Γράφος με κόστη

Ως γνωστόν από τη θεωρία των Γράφων, το μονοπάτι είναι ένα σύνολο από διαδοχικές ακμές που διασυνδέουν ένα ζεύγος κορυφών. Ένα μονοπάτι μπορεί να είναι απλό ή θεμελιώδες όταν δεν περιέχει βρόχους, ή και το αντίθετο, όταν συναντά μια κορυφή περισσότερο από μια φορά. Για κάθε ακμή του γράφου συναντάμε έναν ακέραιο δείκτη σε αυτή ο οποίος καλείται κόστος της. Συνήθως επιλέγουμε ως ακμές ενός μονοπατιού αυτές με το ελάχιστο κόστος, και η λογική αυτή αποτελεί τη πεμπτουσία όλων των path computation αλγορίθμων του GMPLS. Διακρίνουμε τα ακόλουθα προβλήματα που μπορούν να επιλυθούν με τη μέθοδο του καθορισμού μονοπατιού:

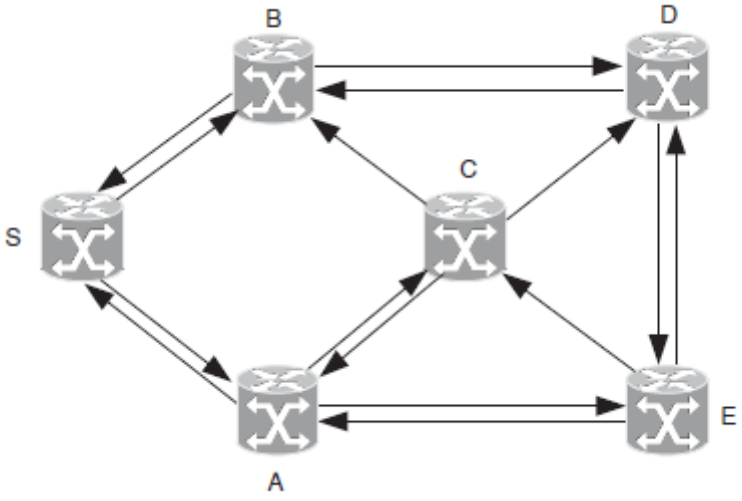
- **Single–source shortest path problem:** Είναι στην ουσία ο υπολογισμός των συντομότερων μονοπατιών από ένα δεδομένο κόμβο σε όλους τους υπόλοιπους.
- **Single–destination shortest path problem:** Είναι ο υπολογισμός συντομότερων μονοπατιών σε έναν δεδομένο κόμβο από όλους τους υπόλοιπους.
- **Single–pair shortest path problem:** Ο υπολογισμός του κοντινότερου μονοπατιού μεταξύ δύο κορυφών.
- **All–pairs shortest path problem:** Η αναζήτηση των κοντινότερων μονοπατιών ανάμεσα σε κάθε ζεύγος κορυφών.

Στην Βιβλιογραφία υπάρχει πραγματικά μια μεγάλη ποικιλία από single source αλγόριθμους. Αυτοί συχνά αναφέρονται και ως Short Path First (SPF) αλγόριθμοι. Οι τέσσερις πιο δημοφιλείς από αυτούς είναι ο **Bellman–Ford**, ο **Dijkstra**, ο **τροποποιημένος Dijkstra**, και ο **Breadth First Search** αλγόριθμος.

Εξετάζοντας πρώτα τον Bellman–Ford αλγόριθμο, παρατηρούμε οτι για ένα δεδομένο γράφημα G(V, A) παράγει συντομότερα μονοπάτια από ένα οποιοδήποτε κόμβο s σε οποιοδήποτε άλλους κόμβους προσβάσιμους από τον s. Επιπλέον, επιτρέπει να υπάρχουν αρνητικές μετρικές–κόστη στις ακμές του γράφου, με τη μόνη προυπόθεση να μην δημιουργούν αρνητικούς βρόχους προσβάσιμους από τον s. Έτσι η πιο σημαντική ιδιότητά του είναι οτι μπορεί να ανιχνεύει τέτοιους βρόχους, από το να θεωρεί οτι απουσιάζουν εντελώς. Στο σχήμα 70 παρουσιάζεται ο αλγόριθμος. Ακολούθως στις Εικόνες 71 διακρίνουμε ένα παράδειγμα γράφου για τον συγκεκριμένο αλγόριθμο, στην 72 τον πίνακα με τα βάρη κάθε ακμής του, και τέλος στην 73 την συνολική εξέλιξη του Bellman–Ford αλγορίθμου. Να σημειώσουμε εδώ οτι σκοπός του παραδείγματός μας είναι ο καθορισμός των συντομότερων μονοπατιών από τον κόμβο S σε όλους τους άλλους κόμβους.

```
BELLMAN-FORD (G,s)
1.  do for every vertex v ∈ V
2.     d[v] = ∞; π[v] = NIL
3.  d[s] = 0
4.  do for every i ∈ (0, 1, . . . ,|V| − 1)
5.     do for every arc a(u, v) ∈ A
6.     if d[v] > d[u] + w(a) then d[v] = d[u] + w(a); π[v] = u
7.  do for every arc a(u, v) ∈ A
8.     if d[v] > d[u] + w(A) then return FALSE /* negative loop is present */
9.  return TRUE /* no negative loops */
```

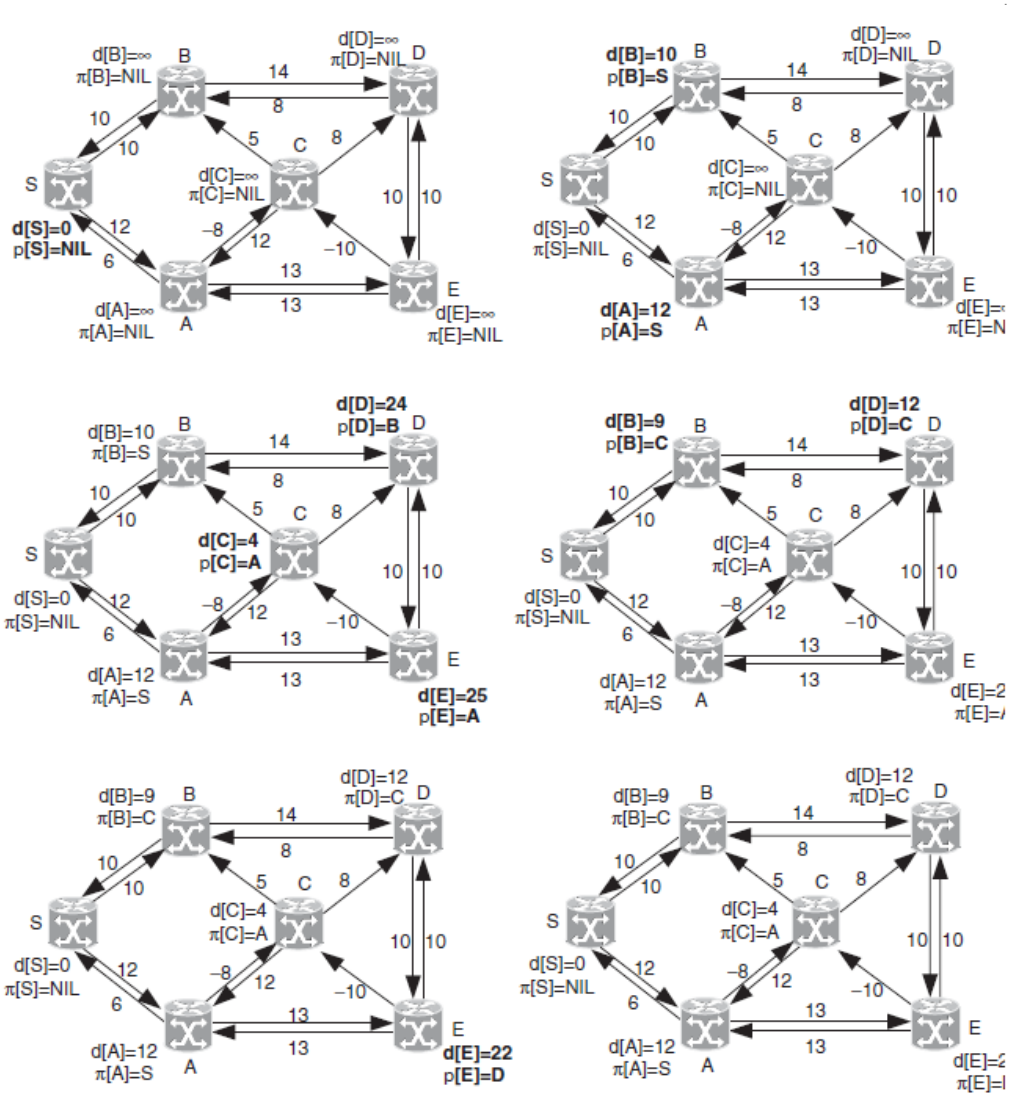
Εικόνα 72. Ο αλγόριθμος Bellman–Ford



Εικόνα 73. Γράφος Δικτύου για τον Bellman–Ford αλγόριθμο

Arc Originating Vertex	Arc Terminating Vertex	Arc Weight
B	D	14
D	B	8
D	E	10
E	D	10
C	B	5
C	D	8
E	C	–10
E	A	13
A	E	13
A	C	–8
C	A	12
A	S	6
S	A	12
S	B	10
B	S	10

Εικόνα 74. Τα κόστη των ακμών του Γράφου Εικόνας 71



Εικόνα 75. Η πορεία εκτέλεσης του Bellman–Ford αλγορίθμου

Ο αλγόριθμος Dijkstra έχει εξεταστεί σε προηγούμενη θεματική ενότητα. Το μοιονέκτημά του είναι οτι αποτυγχάνει στις περιπτώσεις που κάποιες ακμές του γράφου έχουν αρνητικά βάρη. Έτσι προτάθηκε ο τροποποιημένος αλγόριθμος Dijkstra ο οποίος μεταχειρίζεται τις ακμές με αρνητικά βάρη με το να επιτρέπει σε κορυφές οι οποίες έχουν μαρκαριστεί και αφαιρεθεί από την ουρά U, να ξαναεισέρχονται σε αυτήν. Ο αλγόριθμος παρουσιάζεται σε μορφή ψευδοκώδικα στην Εικόνα 76.

```
MODIFIED DIJKSTRA (G,s)
1.  do for every v ∈ V
2.     d[v] = ∞; π[v] = NIL
3.  d[s] = 0
4.  L = 0, U = V
5.  do while U! = 0
6.     u = EXTRACT_MIN_KEY_ENTRY(U)
7.     L = L + u
8.     do for each arc a(u, v) ∈ Originating[u]
9.     if d[v] > d[u] + w(a) then
10.    d[v] = d[u] + w(a), π[v] = u
11.    if v ∈ U
12.    then DECREASE_ENTRY_KEY(U, v)
13.    else L = L − v, INSERT_ENTRY (U, v)
```

Εικόνα 76. Ο αλγόριθμος Modified Dijkstra

Ο αλγόριθμος Breadth First Search (BFS) είναι ένας άλλος σχετικά απλός SPF αλγόριθμος που για έναν δεδομένο γράφο παράγει τα συντομότερα μονοπάτια από οποιαδήποτε κορυφή s σε όλες τις άλλες κορυφές προσβάσιμες από την s. Επιτρέπει την ύπαρξη αρνητικών μετρικών στις ακμές του γράφου, με την προυπόθεση οτι δεν παράγουν αρνητικούς βρόχους. Έτσι, αντίθετα με τον Bellman–Ford δεν μπορεί να ανιχνεύσει τέτοιους βρόχους, ενώ δεν ξαναμαρκάρει –re–label κορυφές στην ουρα ελάχιστης προτεραιότητας U. Ο αλγόριθμος παρουσιάζεται στην Εικόνα 77.

```
BFS (G,s)
1.  do for every vertex v ∈ V
2.     d[v] = ∞; π[v] = NIL
3.  d[s] = 0, F = s
4.     do while F! = 0
5.     do for every u ∈ F
6.     do for every arc a(u, v) ∈ A
7.     F = F − u
8.     if d[v] > d[u] + w(a)
9.     then d[v] = d[u] + w(a), π[v] = u, F = F + v
```

Εικόνα 77. Ο Breadth First Search αλγόριθμος

Υπάρχουν περιπτώσεις οπου χρειάζεται να καθορίσουμε μονοπάτια ανάμεσα σε όλα τα ζεύγη κορυφών u, v ε V, δεδομένου ενός γραφήματος G(V, A). Αυτό είναι το γνωστό **all–pairs shortest path** πρόβλημα. Ο αλγόριθμος Johnson επιλύει το πρόβλημα αυτό καλώντας αντίστοιχα τους Dijkstra και Bellman–Ford. Ο αντίστοιχος αλγόριθμος φαίνεται στην Εικόνα 78.

```
JOHNSON (G)
1.  create new vertex s
2.  G′ = G + s; A′ = A
3.  do for every v ∈ V
4.      create a(s, v) with w(s, v) = 0, A′ = A′ + a
5.  if (BELLMAN-FORD(G′, s) = = FALSE)
6.      then exit /* negative loop is detected */
7.  do for every a ∈ A
8.    w(a) = w(a) + d′[u] − d′[v] /* d′[u] and d′[v] are distance estimates of u and v determined
        by BELLMAN-FORD */
9.  do for every v ∈ V
10.   DIJKSTRA(G, v)
11.     do for every u ∈ V store δ[v, u] /* shortest path from v to u computed by DIJKSTRA */
```

Εικόνα 78. Ο αλγόριθμος Johnson

Στη πράξη υπάρχουν πολυάριθμα constraints και προτιμήσεις για έναν χρήστη ώστε να επιλέξει το βέλτιστο μονοπάτι για μια υπηρεσία: διαθέσιμο εύρος ζώνης για κάθε επιλεγμένο link, ποιότητα προστασίας σύνδεσης, καθώς και ένας μικρός αριθμός από optical–electronic–optical (OEO) μετατροπές. Μπορεί παράλληλα κάποιο συντομότερο μονοπάτι να μην ικανοποιεί ορισμένους περιορισμούς, ενώ κάποιο λιγότερο σύντομο να το επιτυγχάνει. Ένας από τους πλέον αποδοτικούς τρόπους να επιλέξουμε ένα μονοπάτι υποκείμενο σε ορισμένα constraints, είναι να υπολογίσουμε διάφορα συντομότερα μονοπάτια ανάμεσα στο κόμβο προέλευσης και προορισμού, και να διαλέξουμε εν τέλει εκείνο που ικανοποιεί όλους τους περιορισμούς αυτούς. Έτσι τίθεται το **k (k = 1, 2, 3, …)shortest path (KSP)**πρόβλημα – καθόρισε τα k συντομότερα μονοπάτια ανάμεσα σε ένα ζευγάρι από κόμβους ταξινομημένα ως προς το κόστος τους κατά αύξοντα τρόπο.

Ο αλγόριθμος απίλυσης του προβλήματος αποτελείται από τα επόμενα βήματα:

1. Επέλεξε ενα single–pair shortest path αλγόριθμο.
2. Υπολόγισε και επέστρεψε το πρώτο συντομότερο μονοπάτι με την εκτέλεση του αλγορίθμου στον αρχικό γράφο.
3. Εαν k > 1, υπολόγισε το επόμενο συντομότερο μονοπάτι μετα την αφαίρεση μιας ακμής a από τον γράφο. Επανέλαβε αυτό το βήμα μέχρι να υπολογιστούν k διακριτά μονοπάτια με το ελάχιστο κόστος.

3.2.5 CONSTRAINT–BASED ΚΑΘΟΡΙΣΜΟΣ ΜΟΝΟΠΑΤΙΟΥ

Ο μηχανισμός καθορισμού μονοπατιού του GMPLS αναμένεται να λαμβάνει υπόψιν όλες τις προτιμήσεις των χρηστών αναφορικά τόσο με την επιλογή των working paths, όσο και των βέλτιστων εκείνων μονοπατιών που θα καθίστανται διαθέσιμα μετά από μια αστοχία κάποιου δικτυακού πόρου. Οι αλγόριθμοι δρομολόγησης που επισημάνθηκαν στη προηγούμενη ενότητα έχουν το πρόβλημα οτι επιτρέπουν πολύ μικρό έλεγχο του χρήστη πάνω στην επιλογή του μονοπατιού. Για παράδειγμα, αυτοί επιστρέφουν μόνο συντομότερα μονοπάτια, ενώ για τον χρήστη σημασία μπορεί να έχουν κάποια paths τα οποία αποφεύγουν εσκεμμένα ορισμένους κόμβους και ακμές είτε λόγω των επιλεγμένων πολιτικών τοπολογίας, είτε επειδή κάποιες απο αυτές ενδεχομένως έχουν υποστεί βλάβη. Ακόμη και σε αυτή τη περίπτωση, για όλους αυτούς τους λόγους, περισσότερο νόημα για το χρήστη μπορεί να έχει ένα λιγότερο σύντομο μονοπάτι.

Ένας δεύτερος λόγος οπού ένα μονοπάτι που επιστρέφεται από τους προηγούμενους αλγορίθμους δεν είναι η καταλληλότερη επιλογή για μια υπηρεσία, είναι οτι καποιες ακμές του μπορεί να μην έχουν επαρκείς πόρους να μεταφέρουν την κίνηση ανάμεσα σε διαδοχικούς κόμβους. Καθίσταται επομένως επιτακτική η ανάγκη για constraint–based αλγορίθμους καθορισμού μονοπατιού, οι οποίοι επιτρέπουν σε έννοιες όπως διαθέσιμο εύρος ζώνης γραμμής, ικανότητες προστασίας σύνδεσης, και διαθέσιμοι πόροι να λαμβάνονται σημαντικά υπόψιν κατα την επιλογή του μονοπατιού.

Μέχρι τώρα, ο μοναδικός περιορισμός –constraint που εισάγαμε για τον καθορισμό του μονοπατιού ήταν το κόστος της σύνδεσης που αναπαρίστανε το βάρος μίας ακμής στον αντίστοιχο γράφο. Επειδή είναι πρακτικά αδύνατο να εκφραστούν όλες οι απαιτήσεις των χρηστών με μια μόνο μεταβλητή, ένα σύνολο από πολλαπλά attributes πρέπει να σχετιστεί με μία TE γραμμή, και να διαφημιστεί από το κατάλληλο TE πρωτόκολλο δρομολόγησης (OSPF–TE ή ISIS–TE). Συνήθως οι ακόλουθοι χαρακτηρισμοί σχετίζονται με μια σύνδεση:

- **Τύπος προστασίας**. Αυτό το πεδίο περιγράφει ποιές τεχνικές προστασίας είναι εφαρμόσιμες σε μία σύνδεση, ώστε η επιλογή μονοπατιού να περιορίζεται σε συνδέσμους με κάποιο αποδεκτό επίπεδο προστασίας και ανάκαμψης.
- **Shared Risk Link Groups (SRLGs)**. Ένα σύνολο από γραμμές μπορεί να ανήκει στο ίδιο SRLG όπου αντιστοιχίζεται ένας πόρος του οποίου η αστοχία μπορεί να επηρεάσει όλες αυτές τις συνδέσεις. Έτσι ο περιορισμός της επιλογής του μονοπατιού καθορίζεται από τους συνδέσμους που δεν μοιράζονται κοινούς πόρους.
- **Τεχνικές μεταγωγής γραμμής**. Ο τρόπος καθορισμού του μονοπατιού εξαρτάται απο τις εκάστοτε τεχνικές με τις οποίες μεταχείριζονται τα πακέτα δεδομένων οι διάφοροι σύνδεσμοι, για παράδειγμα Ethernet πακέτα, SDH φορτίο, κ. τ. π.
- **Data encoding type**. Αυτός ο χαρακτηρισμός επιτρέπει να επιλέγεται το path κατά τέτοιο τρόπο ώστε να λαμβάνει υπόψιν τα δεδομένα του χρήστη με ένα συγκεκριμένο format.
- **Maximum Unreserved LSP Bandwidth**. Είναι ένα πεδίο που υποδυκνείει πόσο διαθέσιμο εύρος ζώνης υπάρχει σε μια σύνδεση για μια νέα υπηρεσία με συγκεκριμένο επίπεδο προτεραιότητας.

- **Resource Class**. Υποδυκνείει ορισμένα χαρακτηριστικά ποιότητας του συνδέσμου στον μηχανισμό καθορισμού του μονοπατιού ώστε να επιλέγεται το path εκείνο ενός συγκεκριμένου τύπου τέτοιων χαρακτηριστικών.

Στη πράξη, επιθυμούμε να καθορίσουμε μονοπάτια τα οποία δεν είναι απλά βέλτιστα μόνο από την οπτική μεριά πολλαπλών κριτηρίων, αλλά που καταναλώνουν τους ελάχιστους πόρους και είναι επαρκή για τις περισσότερες δικτυακές υπηρεσίες.

Να σημειώσουμε σε αυτό το σημείο οτι ειδικά στα πλαίσια του GMPLS πρωτοκόλλου, επειδή ακριβώς επιλέγουμε συνήθως οπτικά μονοπάτια, υπάρχουν ορισμένες προδιαγραφές οι οποίες πρέπει να πληρούνται για τον καθορισμό ενός optical path.

Η ποιότητα ενός οπτικού σήματος χαρακτηρίζεται από δύο μετρικές: **optical signal noise ratio (OSNR)**, και **end–to–end διασπορά –dispersion (εύρος οπτικού παλμού)**. Οι δύο αυτές παράμετροι επηρεάζουν άμεσα το service bit error rate (BER), που είναι η QoS παράμετρος ορατή από το χρήστη. Άλλες επίσης σημαντικές μετρικές που πρέπει να λαμβάνονται υπόψιν είναι:

- **Attenuation (power loss)**. Κάθε φορά που το οπτικό σήμα περνάει στον παθητικό carrier (ίνα, οπτικό πολυπλέκτη, cross–connect), χάνει κάποιο ποσοστό ενέργειας λόγω της απορρόφησης φωτός.
- **Amplified spontaneous emission (AES) θόρυβος**. Μέσω της ενίσχυσης του οπτικού σήματος από κατάλληλους ενισχυτές καταπολεμάμε την απώλεια ενέργειας. Αυτή η λύση ωστόσο γεννά θόρυβο ο οποίος συσσωρεύεται και δημιουργεί το παρών φαινόμενο.
- **Διασπορά**. Το φαινόμενο αυτό προκαλεί διαπλάτυνση του εύρους των οπτικών παλμών, και σαν αποτέλεσμα διαδοχικά bits αλληλοπαρεμβάλονται με αποτέλεσμα την αλλοίωση της μεταδιδόμενης πληροφορίας.
- **Cross–Talk**. Είναι η αλληλοπαρεμβολή άλλων γειτονικών οπτικών σημάτων με το μεταδιδόμενο σήμα σε μια ίνα.

3.2.6 GMPLS ΚΑΙ ΜΗΧΑΝΙΣΜΟΙ ΑΠΟΚΑΤΑΣΤΑΣΗΣ

Σε πραγματικά σενάρια εκτέλεσης οι πόροι των δικτύων μεταφορών τυχαίνει πολλές φορές να αποτυγχάνουν. Οι οπτικές ίνες καταστρέφονται ενώ τα optical cross–connects, οι οπτικοί ενισχυτές και οι ελεγκτές δικτύου τίθενται εκτός υπηρεσίας εντελώς ξαφνικά. Αν λάβουμε υπόψιν τον τεράστιο όγκο δεδομένων που μεταφέρεται από τα δίκτυα αυτά, μια και μονο αστοχία, ακόμη και για μικρό χρονικό διάστημα, είναι ικανή να προκαλέσει μεγάλη ζημιά στις χρηστικές υπηρεσίες. Ακόμη και αν οι πάροχοι υπηρεσιών κατορθώσουν να μεταφέρουν τις υπηρεσίες από το σημείο της αστοχίας σε κάποιο άλλο περισσότερο λειτουργικό, μέσω ενός provisioning του δικτύου, κάτι τέτοιο δεν είναι αρκετό. Απαιτείται , επιπλέον, μια ικανότητα του πεδίου λειτουργικότητας ελέγχου στο δίκτυο η οποία θα εντοπίζει άμεσα και θα απομονώνει τις βλάβες –fault localization, όπως και θα μεταφέρει τις ενεργές υπηρεσίες μακριά από αυτές. Παρομοίως θα πρέπει το control plane να υποστηρίζει μια έξυπνη λειτουργικότητα για τον καθορισμό τόσο των κυρίων όσο και των εναλλακτικών μονοπατιών, ώστε μια αστοχία να μην επηρεάζει και τα δύο.

Οι δύο κυρίαρχοι τύποι βλαβών στα δίκτυα μεταφοράς συγκαταλέγονται σε αστοχίες του control plane, και αστοχίες του data plane. Βλάβες της πρώτης κατηγορίας καθιστούν τις υπηρεσίες μη διαχειρίσιμες, ενώ της τελευταίας επηρεάζουν άμεσα τη λειτουργικότητά τους. Επιπλέον, ανάλογα με το τύπο του συστατικού δικτύου που έχει υποστεί βλάβη, η αστοχία μπορεί να χαρακτηριστεί ως hardware, software ή αστοχία παραμετροποίησης. Τα σύγχρονα δίκτυα μεταφορών οφείλουν να χειρίζονται τις αστοχίες κατά τέτοιο τρόπο ώστε αυτές να προκαλούν την ελάχιστη διατάραξη, αν όχι και καθόλου, για τις υπηρεσίες των χρηστών. Με άλλα λόγια τα δίκτυα θα πρέπει να είναι ικανά να επιβιώνουν ύστερα από απλές ή και πολλαπλές βλάβες στους πόρους τους.

Η όλη διαδικασία αποκατάστασης ή αλλιώς ο κύκλος επανάκαμψης υπηρεσιών – **recovery operation stage** στο δίκτυο περιλαμβάνει αρκετά στάδια ή βήματα. Ο συνολικός χρόνος διεκπεραίωσής της ισούται με:

T = Td + Th + Tl + Tc + Tn + Tr + Tt

Όπου

Td – fault detection time

Th – hold–off time

Tl – fault localization time

Tc – fault correlation time

Tn – fault notification time

Tr –recovery operation time

Tt – traffic recovery time

Τα πρώτα πεντε στάδια καλούνται διαχείριση σφάλματος –fault management. Η ανίχνευση σφάλματος είναι το μόνο στάδιο το οποίο δεν μπορεί να υλοποιηθεί χωρίς την αλληλεπίδρασή του με το data plane –όλα τα υπόλοιπα βήματα πραγματοποιούνται είτε μέσα από το πεδίο λειτουργικότητας ελέγχου ή και δεδομένων.

Όταν μια αστοχία συμβεί, οι γειτονικοί κόμβοι στη γραμμή ή κόμβο που έχει καταρρεύσει δεν εντοπίζουν την βλάβη στιγμιαία. Απαιτείται κάποιος χρόνος για το υλισμικό που αφιερώνεται στην ανίχνευση σφαλμάτων να εντοπίσει πρώτα το λανθάνων συστατικό στο δίκτυο, να προσδιορίσει την ακριβή κατάσταση του σφάλματος, και τέλος να ειδοποιήσει την οντότητα που είναι υπεύθυνη για τη διαχείριση σφαλμάτων (π. χ. το πεδίο λειτουργικότητας ελέγχου του GMPLS). Ο χρόνος ανίχνευσης σφάλματος εξαρτάται καθολικά από τη τεχνολογία κατασκευής του data plane (TDM, WDM), ποσο αναλυτικός είναι κάθε κόμβος στην επεξεργασία των σημάτων, και γενικά στις χρησιμοποιούμενες τεχνικές επεξεργασίας ψηφιακών/οπτικών σημάτων.

Η οντότητα διαχείρισης σφαλμάτων συνήθως δεν αντιδρά στην ειδοποίηση για αστοχία αμέσως. Πρώτα μεταφέρει την υπηρεσία σε μια fault hold–off κατάσταση. Αυτό είναι απαραίτητο διότι ένα χαμηλότερο επίπεδο δικτύου μπορεί να διαθέτει έναν δικό του μηχανισμό επανάκτησης, και είναι γενικά μη επιθυμητό να έχουμε πολλαπλά layers να προσπαθούν να ανακάμψουν από την ίδια αστοχία αφού κάτι τέτοιο θα προκαλούσε διατάραξη στο δίκτυο. Εαν μετά από το hold–off χρονικό interval η ειδοποίηση σφάλματος ακόμη δεν έχει αποσυρθεί, η διαδικασία επανάκαμψης μεταφέρεται στο επόμενο στάδιο –αυτό της απομόνωσης λαθών. Σε ορισμένες τεχνολογίες μεταφορών (SONET/SDH) η απομόνωση σφαλμάτων υποστηρίζεται από το πεδίο λειτουργικότητας δεδομένων. Σε καποιες άλλες απαιτούνται κάποιες out–of–band τεχνικές όπως αυτές που

προσφέρει το LMP πρωτόκολλο στο GMPLS framework. Η διαδικασία της σωστής απομόνωσης των αστοχιών στο δίκτυο απαιτεί όλους τους κόμβους που ανιχνεύουν την βλάβη να την αναφέρουν σε μια οντότητα που λαμβάνει τις αποφάσεις ανάκαμψης, η οποία με τη σειρά της θα κάνει τοπικό το χαρακτήρα της βλάβης μέσω της ανάλυσης των TE βάσεων δεδομένων και επηρεασμένων μονοπατιών. Τεχνικές , ωστόσο, απομόνωσης που χτίζονται στο control plane σημαίνουν οτι η αστοχία μπορεί να εντοπιστεί πιό εύκολα, οι υπηρεσίες να ανακάμψουν πιο γρήγορα και με περισσότερη ακρίβεια.

Κατά την λήψη του fault notification message ο κύκλος επανάκαμψης στο δίκτυο αντιδρά από το να μην κάνει καμία απολύτως ενέργεια (για μη προστατευόμενες υπηρεσίες), στο να καθορίζει και να εγκαθιδρύει εναλλακτικά μονοπάτια και να μεταγάγει την κίνηση σε αυτά (full re–routing).

Το διαθέσιμο σχήμα προστασίας –recovery scheme διακρίνεται στα ακόλουθα δύο είδη:

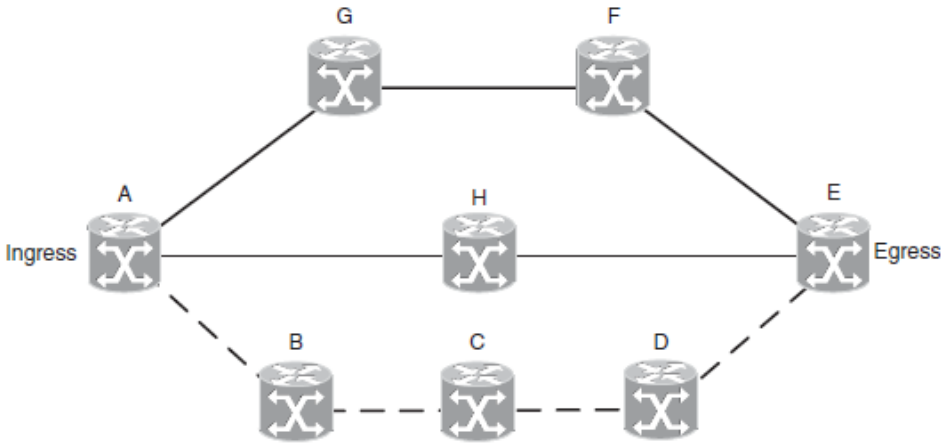
- **End–to–End recovery**. Σε αυτή τη περίπτωση, ένα εναλλακτικό μονοπάτι που ξεκινάει και τελειώνει στο ίδιο ζεύγος κόμβων με το κυρίως μονοπάτι, προσφέρει προστασία από οποιαδήποτε μορφής αστοχία σε κόμβο ή γραμμή σε αυτό.
- **Local Recovery**. Δύο μέθοδοι υλοποιούν αυτό το σχήμα προστασίας: **fast re–route (FRR)**, και **path segment recovery**. Στο FRR μοντέλο, όπου κάθε πόρος ενός μονοπατιού προστατεύται από ένα ξεχωριστό backup tunnel, το χαρακτηριστικό είναι οτι το σημείο που τα δύο μονοπάτια {κυρίως και εναλλακτικό}συγκλίνουν{PLR}, για κάθε domain προστασίας, είναι εγγυημένο να βρίσκεται σε ένα πεδίο λειτουργικότητας δεδομένων ενός μόνο hop οποιουδήποτε σημείου αστοχίας. Επιπλέον το σημείο που τα backup μονοπάτια συγκλίνουν με το κυρίως είναι πολύ κοντά στους πόρους που προστατεύονται. Αυτή ακριβώς η ιδιότητα καθιστά το μοντέλο αυτό ικανό για αρκετά γρήγορους χρόνους επανάκαμψης.

Από δω και στο εξής θα εξετάσουμε την αποκατάσταση υπηρεσιών –service recovery σε επίπεδο καθαρά μονοπατιού –δηλαδή αποκατάσταση ολόκληρου του LSP (End–to–End recovery) ή ατομικών τμημάτων των LSPs (fast reroute). Κάθε LSP μπορεί να διαθέτει άκρου–σε–άκρου αποκατάσταση μονοπατιού από ενός από τους ακόλουθους τύπους:

- **Μονόδρομη 1 + 1 προστασία**
- **Αμφίδρομη 1 + 1 προστασία**
- **1 : N προστασία με extra traffic shaping**
- **Pre–planned re–routing προστασία χωρίς extra traffic shaping**
- **Full re–routing**
- **Χωρίς προστασία**

Μονόδρομη 1 + 1 προστασία

Σε αυτό το σχήμα, το άκρο ενός προστατευόμενου LSP υπολογίζει δύο συνδέσμους/κόμβους/ή SRLGs, ένα για το κυρίως μονοπάτι και ένα για το εναλλακτικό ή backup. Το μονοπάτι προστασίας εγκαθιδρύεται πλήρως την ίδια χρονική στιγμή με το προστατευόμενο LSP. Στο πεδίο λειτουργικότητας δεδομένων, καθε ένας από τους ingress και egress κόμβους διοχετεύουν την κίνηση και στα δύο μονοπάτια, ενώ επιλέγουν την εισερχόμενη κίνηση από το μονοπάτι με το πιο βέλτιστο σήμα. Όταν μια αστοχία συμβεί στο κυρίως LSP οι αντίστοιχοι αυτοί κόμβοι μεταγάγουν την κίνηση στο λειτουργικό –μη λανθάνων μονοπάτι. Καμία ειδοποίηση σφάλματος ή συγχρονισμός δεν είναι απαραίτητος σε αυτό το σχήμα. Επειδή το LSP προστασίας χρησιμοποιείται μόνιμα για μεταφορά κίνησης, οι πόροι του δεν μπορούν να μοιράζονται από LSPs που προστατεύουν άλλα LSPs. Έτσι το σχήμα αυτό προστασίας δεν είναι επαρκές, παρά την ιδιαίτερη αμεσότητα και απλότητά του.



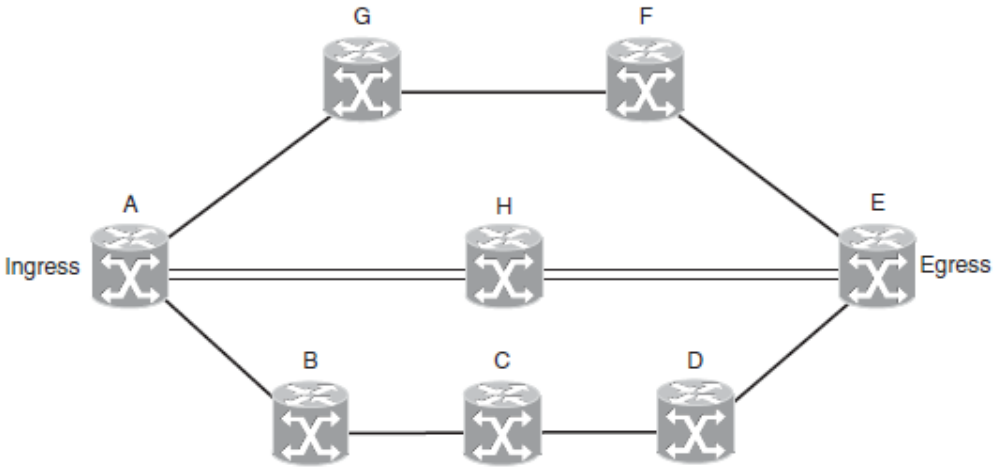
Εικόνα 79. End–to–end 1 + 1 προστασία

Αμφίδρομη 1 + 1 προστασία

Αυτός ο μηχανισμός λειτουργεί ακριβώς όπως και ο προηγούμενος με μια μόνο εξαίρεση: Οι ingress και egress κόμβοι διαλέγουν κίνηση από το ίδιο κανάλι. Αυτό σημαίνει οτι μετά από την αστοχία, οι κόμβοι αυτοί λαμβάνουν την κίνηση από το δεύτερο κανάλι ακόμη και αν η βλάβη επηρέασε μόνο μια κατεύθυνση του προστατευόμενου μονοπατιού. Αυτός ο συγχρονισμός απαιτεί κατάλληλη σηματοδοσία ανάμεσα στους κόμβους.

1 : N προστασία με extra traffic shaping

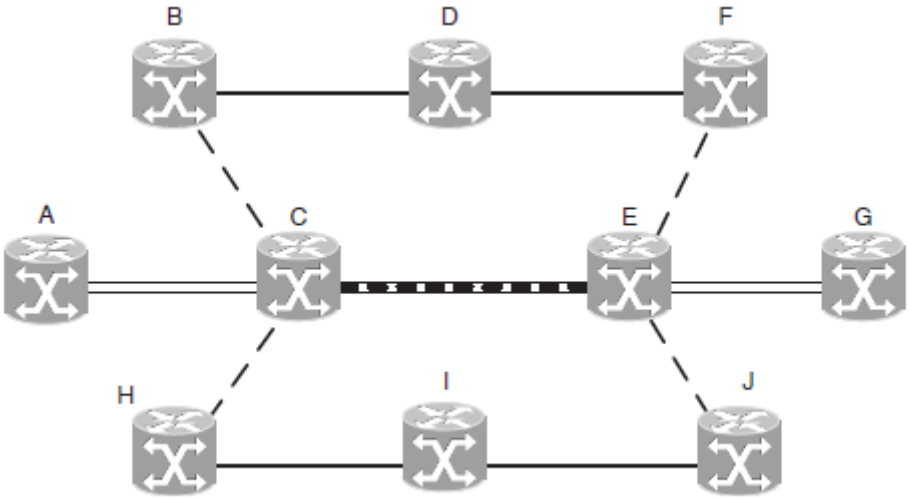
Σε αυτό το μοντέλο, ένα ακρου–προς–άκρου μονοπάτι προστασίας σηματοδοτείται πάνω σε ένα path που αποτελείται από διαδοχικούς κόμβους, συνδέσμους, SRLGs πολλαπλών προστατευόμενων LSPs. Ας υποθέσουμε οτι έχουμε ένα ζεύγος από υπηρεσίες που μεταφέρουν κίνηση πάνω στα μονοπάτια A–B–C–D–E και A–G–F–E (Εικόνα 79) τα οποία απαιτούν προστασία. Το LSP που προστατεύει και τα δύο, μπορεί να εγκαθιδρυθεί στο path A–H–E. Το μονοπάτι προστασίας δεν μεταφέρει ακόμη καμία κίνηση των άλλων δύο μονοπατιών. Όταν συμβεί μια αστοχία σε ένα από τα δύο προστατευόμενα μονοπάτια, οι αντίστοιχοι κόμβοι τους μεταγάγουν αμέσως την κίνηση στο μονοπάτι προστασίας. Υπάρχει, βέβαια, και το ενδεχόμενο περισσότερα από ένα μονοπάτια να ζητήσουν πόρους από το LSP που τα προστατεύει. Σε αυτή τη περίπτωση, το μονοπάτι με τη μεγαλύτερη TE προτεραιότητα είναι αυτό που θα δεσμεύσει τους πόρους του backup LSP.



Εικόνα 80. End–to–end 1 + 1 προστασία με extra traffic shaping

Pre–planned re–routing προστασία χωρίς extra traffic shaping

Αυτό το σχήμα υποθέτει οτι ένα LSP προστασίας προ–σηματοδοτείται ώστε να είναι ξεχωριστό –disjoint ενός ή και περισσοτέρων προστατευόμενων LSPs. Σε αντίθεση με όλους τους προηγούμενους μηχανισμούς προστασίας, οι πόροι στο backup LSP κατανέμονται αλλά δεν δεσμεύονται από τα OXCs. Έτσι το LSP προστασίας δεν μπορεί να μεταφέρει extra κίνηση. Επιπλέον μετά από μια αστοχία, θα πρέπει πρώτα να ενεργοποιηθεί ώστε να δεσμευτούν οι πόροι του από τα cross–connects. Η χρησιμότητα αυτού του μηχανισμού, παρώτι πετυχαίνει χειρότερους χρόνους επανάκαμψης από τα προηγούμενα σχήματα, είναι οτι μπορέι να δεσμεύει –preplan πόρους και για LSPs που δεν τερματίζονται από τα ίδια egress και ingress στοιχεία των αρχικών προστατευόμενων μονοπατιών. Επομένως μπορεί να λειτουργήσει ως μηχανισμός προστασίας ΚΑΙ για περισσότερες γραμμές.



Εικόνα 81. Pre–Planned Rerouting χωρίς extra traffic shaping

Full re–routing

Το συγκεκριμένο σχήμα αποκατάστασης μονοπατιού δεν προυποθέτει καμία προ–σηματοδοσία και επίβλεψη ενός LSP προστασίας, πριν την εμφάνιση κάποιας αστοχίας στο κυρίως μονοπάτι. Ας θεωρήσουμε την Εικόνα 79. Υποθέτουμε οτι υπάρχει ένα μη προστατευόμενο μονοπάτι που διατρέχει τους κόμβους A, B, D, και E. Κάποια στιγμή μια αστοχία εμφανίζεται στην γραμμή BD. Ο end–to–end μηχανισμός Full re–routing λειτουργεί τότε ως εξής:

- Ο κόμβος ανίχνευσης αστοχίας (B ή D) στέλνει ένα FIS (Fault Indication Signal) μήνυμα στον ingress κόμβο του LSP (τον A).
- Ο κόμβος αυτός υπολογίζει ένα εναλλακτικό μονοπάτι ή επιλέγει ένα προκαθορισμένο. Το μονοπάτι αυτό θα πρέπει να μην περιέχει φυσικά τον ελαττωματικό κόμβο.
- Ο ingress κόμβος επαναδρομολογεί –re–route το αρχικό LSP στο νέο μονοπάτι, κάνοντας χρήση της make–before–break τεχνικής ώστε να δεσμεύσει κοινόχρηστους πόρους στο μονοπάτι.
- Εαν για κάποιο λόγο αποτύχει η επαναδρομολόγηση, ο αρχικός κόμβος υπολογίζει ένα νέο εναλλακτικό μονοπάτι.

Ο μηχανισμός αυτός, συγκρινόμενος με όλους τους υπόλοιπους, προσφέρει χειρότερους χρόνους αποκατάστασης. Αυτό συμβαίνει διότι απαιτείται σημαντικά επιπλέον χρόνος για τον καθορισμό μονοπατιού και την εγκαθίδρυσή του μέσω κατάλληλης σηματοδοσίας και μηνυμάτων ελέγχου. Ωστόσο έχει και σημαντικά πλεονεκτήματα. Πρώτον, αποτελεί το πιο βέλτιστο σχήμα από άποψη διαχείρισης πόρων. Αυτό ισχύει διότι δεν δεσμεύει πόρους για λόγους επανάκαμψης πρωτού συμβεί μια αστοχία. Δεύτερον, είναι ένας ικανός μηχανισμός για αντιμετώπιση οποιοδήποτε τύπου αστοχίας, ακόμη και για ταυτόχρονη εμφάνιση αστοχιών στο δίκτυο. Τέλος, δεν απαιτείται το LSP προστασίας και το προστατευόμενο LSP να είναι πλήρως ξεχωριστά συνδεδεμένα –disjoint.

Να σημειώσουμε σε αυτό το σημείο οτι μετά από το switch–over μιας υπηρεσίας στο backup LSP, το τελευταίο στις περισσότερες περιπτώσεις παρέχει μια κατώτερης ποιότητας υπηρεσία. Το πιό σημαντικό είναι οτι το μονοπάτι προστασίας τώρα δεν προστατεύται και εαν καταρρεύσει και αυτό η υπηρεσία μεταφοράς διαταράσσεται σημαντικά.

Πριν κλείσουμε, να αναφέρουμε και την περίπτωση της αστοχίας και ανάκαμψης του πεδίου λειτουργικότητας ελέγχου. Ως γνωστόν, στο GMPLS τα data και control planes είναι ανεξάρτητα. Μια συνέπεια αυτού του γεγονότος είναι οτι μπορούν να καταρρεύσουν ξεχωριστά.

Στο πεδίο λειτουργικότητας δεδομένων, οι βλάβες ανιχνεύονται από τις ενδείξεις υλισμικού των οπτικών συσκευών διασύνδεσης. Αντίθετα, στο control plane οι ίδιοι οι ελεγκτές ελέγχου ανιχνεύουν τις διάφορες αστοχίες μέσω της απουσίας συγχρονισμού των μηνυμάτων σηματοδοσίας ανάμεσα σε γειτονικούς κόμβους. Με άλλα λόγια, αλλιώς ερμηνεύονται οι αστοχίες σε επίπεδο data plane και αλλιώς σε control plane. Τις περισσότερες φορές συμβάντα όπως: λάθη παραμετροποίησης, αλλαγή ή τροποποίηση διεπαφών ελέγχου, bugs ή και λανθασμένη χρήση πρωτοκόλλων οδηγούν σε αυτό που ονομάζουμε control plane failures –αστοχίες επιπέδου control plane. Εκείνο που είναι σημαντικό να τονίσουμε είναι οτι η επανάκαμψη του control plane δεν σημαίνει μόνο αποβολή των συνθηκών που προκάλεσαν την βλάβη, αλλά και μια διαδικασία

επανασυγχρονισμού του πεδίου λειτουργικότητας ελέγχου για όλα τα LSPs που αποτελούν το data plane. Υπάρχουν αρκετοί τρόποι να επιτευχθεί ο συγχρονισμός αυτός.

Ενας από αυτούς είναι μέσω της σηματοδοσίας ελέγχου. Αυτό πραγματοποιείται θαυμάσια μέσω του RSVP–TE πρωτοκόλλου. Συγκεκριμένα κατά την φάση επανεγκατάστασης των πληροφοριών γειτνίασης ανάμεσα στους κόμβους του δικτύου (μέσω της ανταλλαγής των GMPLS RSVP Hello μηνυμάτων), ο ελεγκτής ελέγχου που ανακάμπτει, έχει το δικαίωμα να επανασυγχρονίσει τις πληροφορίες ελέγχου για όλα τα LSPs. Μόλις λάβει πάλι όλες τις πληροφορίες αυτές για τα states των LSPs, ο κόμβος αυτός ανανεώνει τις εγγραφές στο data plane, επανασυχρονίζει το control plane, και κάνει επαναδεύσμευση των πόρων –resources για τα ενεργά μονοπάτια. Με αυτό το τρόπο, έπειτα από μια αστοχία, πετυχαίνεται πλήρης αποκατάσταση του control plane status.

Ένας λίγο πιο διαφορετικός τρόπος είναι να αποθηκεύουμε τις pre–failure –προ–αστοχίας control plane καταστάσεις σε αντίστοιχες τοπικές βάσεις δεδομένων κάθε LSR. Ωστόσο με τη μέθοδο αυτή ποτέ δεν θα είμαστε εντελώς ακριβείς διότι πάντα θα απουσιάζει κάποια αναγκαία πληροφορία από τις εγγραφές αυτές, επειδή ακριβώς δεν γνωρίζουμε τον χρόνο της αστοχίας. Μια πιο αποδοτική προσέγγιση θα ήταν εαν αποθηκεύαμε στις βάσεις δεδομένων μόνο τα μηνύματα ελέγχου που λαμβάνονται ή αποστέλλονται από κάθε controller. Σε κάθε περίπτωση, ένας τέτοιος μηχανισμός απαιτεί επιπλεόν χρόνο επεξεργασίας και δεν είναι πρακτικός.

Ο μόνος αξιόπιστος τρόπος για την πλήρη αποκατάσταση του πεδίου λειτουργικότητας ελέγχου είναι να χρησιμοποιήσουμε την LSP πληροφορία που παρέχεται απο το data plane. Το control plane κάνοντας χρήση της πληροφορίας για LSP εύρος ζώνης, τύπο κωδικοποιήσης δεδομένων, και οργάνωση πακέτων, μπορεί να χτίσει με τη σειρά του το LSP Setup μήνυμα (RSVP Path). Να σημειώσουμε εδώ, οτι ο εκάστοτε ελεγκτής δεν χρειάζεται να γνωρίζει τον προορισμό του LSP ή και το μονοπάτι που επιλέγεται από αυτό. Αυτό που πρέπει να κάνει είναι να καθορίσει το εξερχόμενο link ID και τη ταυτότητα του απομακρυσμένου controller στο άκρο της σύνδεσης. Αυτή η πληροφορία συνήθως εξάγεται από το πρωτόκολλο LMP. Έχοντας προσδιορίσει τον επόμενο hop, αυτός λαμβάνει το LSP Setup μήνυμα, υπολογίζει με τη σειρά του όλες τις αναγκαίες πληροφορίες, και η διαδικασία επαναλαμβάνεται μέχρι τον egress κόμβο του LSP.

3.3.1 TRAFFIC ENGINEERING ΚΑΙ GENERALIZED–MPLS

Οι Service Providers έχουν πλεον πειστεί για την σημαντικότητα των τεχνικών traffic engineering, επειδή με τη σωστή εφαρμογή τους επιτρέπεται να βελτιστοποιούν την χρήση των δικτυακών πόρων και να τους προσφέρονται έτσι αρκετά οφέλη. Άλλωστε ένας από τους σημαντικότερους λόγους της επιτυχίας του MPLS πρωτοκόλλου ως τεχνολογίας, είναι η ικανότητα να προσφέρει traffic engineering χαρακτηριστικά σε ιδιαίτερα χαμηλό λειτουργικό κόστος. Ο δυναμικός υπολογισμός των βέλτιστων μονοπατιών, η δυναμική διαχείριση των tunnels, καθώς και ο τρόπος κατανομής της κίνησης ανάμεσά τους είναι παραδείγματα του πώς το MPLS κατορθώνει να μετατρέψει το δίκτυο από μια παραδοσιακά αποκεντρωμένη μορφή σε μια σύγχρονης αντίληψης, intelligent core και TE ικανή υποδομή. Στη συγκεκριμένη θεματική ενότητα θα διαπιστώσουμε αναλυτικά πως εφαρμόζεται η τεχνική του Traffic Engineering στα GMPLS–ελεγχόμενα δίκτυα μεταφοράς, καθώς και τις εφαρμογές της σε δίκτυα που ενώνουν πολλαπλά αυτόνομα συστήματα και διαφορετικούς domains.

Όπως αναφέρει το RFC 2702, Requirements for Traffic Engineering Over MPLS, το traffic engineering είναι μια τεχνολογία που σχετίζεται με την βελτιστοποίηση της απόδοσης στα δίκτυα δεδομένων. Πιο γενικά, αποτελεί ένα σύνολο από εφαρμογές, μηχανισμούς, εργαλεία και συμβάσεις τα οποία επιτρέπουν την μέτρηση, μοντελοποίηση, χαρακτηρισμό και έλεγχο της βασισμένης σε πακέτα κίνησης του χρήστη, ώστε να επιτευθούν συγκεκριμένοι στόχοι απόδοσης. Το ερώτημα που τίθεται είναι ποιοί ακριβώς είναι αυτοί οι στόχοι. Υπάρχουν δύο κλάσεις:

Η πρώτη κλάση είναι βασισμένη στη κίνηση –traffic–oriented και άρα ορατή στους τελικούς χρήστες. Οι αντικειμενικοί σκοποί αυτής της κλάσης περιλαμβάνουν προσθήκες Ποιότητας Υπηρεσιών –Quality of Service στις ροές κίνησης, ελαχιστοποίηση της απώλειας δεδομένων και της καθυστέρησης, καθώς και μεταχείριση των ροών με υψηλή προτεραιότητα σε περιπτώσεις οπού κάποιες γραμμές παρουσιάζουν συμφόρηση.

Η δεύτερη κλάση των στόχων απόδοσης είναι resource–oriented, βασισμένη δηλαδή στους πόρους. Αυτοί οι στόχοι απόδοσης είναι σημαντικοί μόνο στους Παροχείς Υπηρεσιών και όχι στους τελικούς χρήστες. Για να καταλάβουμε καλλίτερα τη χρησιμότητά τους, αυτοί απαντούν σε ερωτήματα όπως: Δεδομένων κάποιων δικτυακών πόρων, με ποιό τρόπο όλοι οι χρήστες θα εξυπηρετούνται βέλτιστα?, Πως θα προωθούνται νέες υπηρεσίες χωρίς να επηρεάζεται η απόδοση στους υπάρχοντες χρήστες?, και Πως θα προστατευτούν οι ροές κίνησης από περιπτώσεις κατάρρευσης γραμμής ή άλλων αστοχιών στο δίκτυο?

Το Traffic Engineering είναι μια ιδιαίτερα σημαντική λειτουργικότητα του πεδίου ελέγχου στο δίκτυο. Παραδοσιακά, εισάγεται για τη καταπολέμηση της συμφόρησης σε υπερφορτωμένες γραμμές εξαιτίας των πρωτοκόλλων δρομολόγησης τους (και ειδικότερα λόγω του shortest–path χαρακτήρα τους).

Δύο είναι οι κύριες αιτίες για την πρόκληση συμφόρησης.

- Το δίκτυο είναι υπο–διαχειριζόμενο –under–provisioned. Αυτό σημαίνει οτι δεν υπάρχουν ενναλλακτικά μονοπάτια για την μετάδοση των πακέτων από τον αποστολέα στον παραλήπτη.
- Η όλη κίνηση αντιστοιχίζεται σε μονοπάτια που χρησιμοποιούν υπερφορτωμένους συνδέσμους, ανεξάρτητα απο την ύπαρξη ή όχι ενναλλακτικών μονοπατιών. Η πρόκληση συμφόρησης στις περιπτώσεις αυτές συμβαίνει διότι τα πρωτόκολλα δρομολόγησης προσδιορίζουν τα μονοπάτια με το ελάχιστο μετρικό κόστος συνδέσμων.

Όπως τονίζεται και από το RFC 2702, η τεχνική του traffic engineering είναι χρήσιμη όταν ένα μονοπάτι υπολογίζεται δυναμικά, και υπάρχουν περισσότερα του ενός μονοπάτια για την αποστολή της κίνησης στο δίκτυο. Διαχρονικά, το Traffic Engineering έχει υποστεί σημαντική εξέλιξη. Οι πιο απαιτητικοί τομείς που καλείται να απαντήσει είναι:

1. Πως να πραγματοποιεί τον έλεγχο σε μονοπάτια που δεσμεύονται απο υπηρεσίες χωρίς να επιβαρύνει σημαντικά τα Internet πρωτόκολλα δρομολόγησης.
2. Πως να εξασφαλίζει οτι ένα λειτουργικό μονοπάτι θα προσφέρει πάντα QoS εγγυήσεις όχι σε χειρότερο επίπεδο από το προσυμφωνημένο από το Service Level Agreement.
3. Πως να εξασφαλίζει οτι η βιωσιμότητα των υπηρεσιών απέναντι σε δικτυακές αστοχίες δεν είναι χειρότερη από την προεγκατεστημένη.

4. Εαν ενα εναλλακτικό μονοπάτι καθίσταται διαθέσιμο μετα από την εγκαθίδρυση μιας υπηρεσίας, πως θα κάνει την υπηρεσία αυτή να προωθείται σε αυτό το μονοπάτι με την μικρότερη δυνατή επιβάρυνση στο δίκτυο.
5. Πως θα χρεώνονται οι υπηρεσίες ώστε οι χρήστες να επιβαρύνονται περισσότερο για πιό βέλτιστες υπηρεσίες.

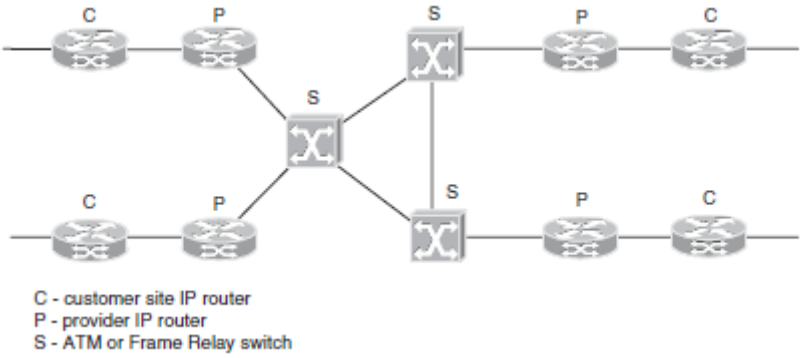
Στη συνέχεια, διακρίνουμε τις ακόλουθες μεθόδους Traffic Engineering:

Traffic Engineering μέσω τροποποιήσιμων μετρικών δικτυακών συνδέσμων. Σύμφωνα με την προσέγγιση αυτή, ο έλεγχος των ροών κίνησης γίνεται τροποποιώντας τις μετρικές–κόστη που αντιστοιχούν σε κάθε γραμμή. Ωστόσο στη περίπτωση αυτή, και δεδομένου ενός γραφήματος με κόστη μιας δικτυακής τοπολογίας, για την εφαρμογή των πολιτικών καθορισμού κίνησης το πρόβλημα δημιουργείται στο ποιές μετρικές να τροποποιηθούν, πότε και πόσο. Αποφασίζοντας είτε περισσότερο καθυστερημένα είτε λιγότερο για τις αλλαγές αυτές, δημιουργούνται εύκολα καταστάσεις συμφόρησης και κακής διαχείρησης του δικτύου.

Traffic Engineering μέσω ECMP. Σε περιπτώσεις που σε κάποιο δίκτυο υπάρχουν δύο ή και περισσότερα εναλλακτικά μονοπάτια με το ίδιο κόστος, ο πιο αποδοτικός τρόπος μεταφοράς είναι η κατανομή της όλης κίνησης με τέτοιο τρόπο ώστε τα πολλαπλά μονοπάτια να εναλλάσονται με χρήση μεθόδου Round–Robin. Η τεχνική που χρησιμοποιείται για την έξυπνη αυτή κατανομή της κίνησης ανάλογα με τις διευθύνσεις αποστολής και προορισμού, DiffServ πολιτικών, και ροών κίνησης καλείται **Equal Cost Multi–Path Forwarding**. Και πάλι ωστόσο δεν εξαλείφονται εύκολα τα φαινόμενα congestion.

Traffic Engineering μέσω Service Type Based Routing. Το επόμενο εγχείρημα για την επίτευξη των στόχων του Traffic Engineering είναι η ξεχωριστή δρομολόγηση ροών κίνησης που σχετίζονται με διαφορετικούς τύπους υπηρεσιών. Παράδειγμα τέτοιων υπηρεσιών είναι το Voice Over IP (VoIP), όπου καθορίζονται υψηλές απαιτήσεις όσον αφορά την καθυστέρηση, καθυστέρηση από άκρου σε άκρου, και διακύμανση καθυστέρησης, όπως και το WEB browsing που απαιτείται υψηλή ταχύτητα και χαμηλό κόστος. Μέσω της τεχνικής αυτής αντιστοιχίζεται σε κάθε σύνδεσμο και από ένας τύπος εφαρμογής, ενώ σε κάθε κόμβο ο πίνακας προώθησης ενημερώνεται για το αντίστοιχο service type. Παρόλο που κατορθώνουμε να πετυχαίνουμε τις QoS εγγυήσεις καθώς και τους προσυμφωνημένους τύπους SLA, είναι πολύ πιθανό να δημιουργούνται rooting loops στο δίκτυο εξαιτίας των διαφορετικών (ίσως) αποφάσεων δρομολόγησης σε κάθε κόμβο.

Traffic Engineering χρησιμοποιώντας Overlays. Στην Εικόνα 82 έχουμε ένα παράδειγμα IP overlay δικτύου. Εκείνο που καθιστά αυτή τη μορφή δικτύου σε τόσο αποδοτική είναι οτι κάθε ροή κίνησης μπορεί να δρομολογηθεί ανεξάρτητα, ακόμα και αν σχετίζεται με κάποιο άλλο τύπο υπηρεσίας. Τα εισερχόμενα πακέτα στο δίκτυο κατηγοριοποιούνται ανάλογα με το φορτίο τους και τις διευθύνσεις, και στη συνέχεια προωθούνται στα εικονικά κανάλια. Οι αποφάσεις δρομολόγησης λαμβάνονται μόνο μια φορά και έτσι αποφεύγονται τα rooting loops, ενώ σε περιπτώσεις αστοχιών η κίνηση μετάγεται σε αντίστοιχα εικονικά κανάλια που είναι ξεχωριστά από αυτά που επηρεάζονται απο τη βλάβη. Το μοιονέκτημα αυτής της προσέγγισης είναι το υψηλό διαχειριστικό κόστος και η χαμηλή δυνατότητα κλιμάκωσης.



Εικόνα 82. IP Overlay δίκτυο

Traffic Engineering βασισμένο στο MPLS. Τα MPLS traffic engineering πρωτόκολλα επιτρέπουν στους κόμβους να διαφημίζουν όχι μόνο τη δικτυακή τους παρουσία και τοπολογική πληροφορία, αλλά και τα χαρακτηριστικά των συνδέσμων τους. Το γεγονός αυτό διευκολύνει την δυναμική εγκαθίδρυση υπηρεσιών, τον off–line καθορισμό μονοπατιού, καθώς και την αυτόματη τροφοδοσία τους. Όταν ένα πιό βέλτιστο μονοπάτι καθίσταται διαθέσιμο για μια υπηρεσία, το τελευταίο μπορεί να επαναδρομολογηθεί με μικρή επιρροή στο όλο δίκτυο. Είναι αναμφισβήτητο οτι ο μηχανισμός του Traffic Engineering στα MPLS δίκτυα κορμού αποτελεί τη πιο βέλτιστη και αποδοτική προσέγγιση στη κατηγορία αυτή λόγω των πλεονεκτημάτων προστασίας και ανάκαμψης που προσφέρει το MPLS και της άνετης εφαρμογής του σε ετερογενή δίκτυα.

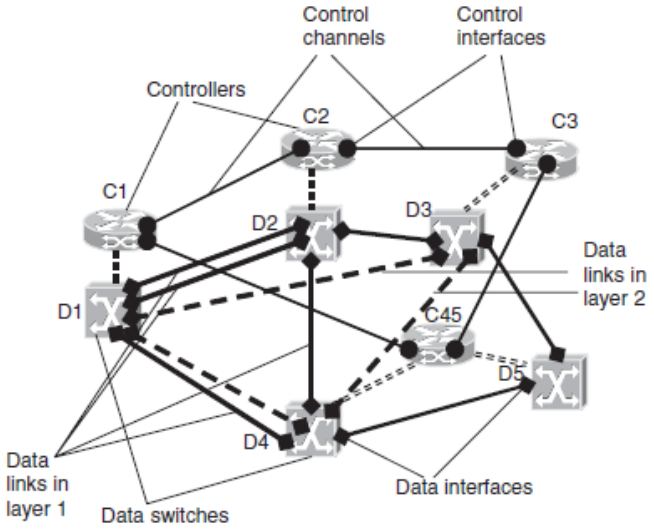
Σύγχρονες Απαιτήσεις Traffic Engineering Δικτύων Μεταφορών

Διακρίνουμε τα ακόλουθα constraints που πρέπει να λαμβάνει υπόψιν ένα σύγχρονο πρωτόκολλο TE:

1. **Οι σύνδεσμοι μεταφοράς είναι συνήθως αμφίδρομοι.**
2. **Οι ετικέτες αναγνωρίζουν και διαχειρίζονται πόρους (GMPLS).**
3. **Το εύρος ζώνης κατανέμεται σε μικρότερο βαθμό.**
4. **Ο υπολογισμός μονοπατιού απαιτεί περισσότερα constraints.**
5. **Τα πεδία λειτουργικότητας ελέγχου και δεδομένων είναι διαχωρισμένα.**
6. **Χρήση Ιεραρχικών LSP's.**

Όπως είδαμε κάθε τεχνολογική προσέγγιση έχει τα θετικά αλλά και τα αρνητικά της στη περίπτωση του Traffic Engineering. Το GMPLS από την άλλη είναι μια τεχνολογία που συνδυάζει όλα τα προηγούμενα θετικά οφέλη και μπορει να εφαρμοσθεί άνετα και στη περίπτωση των packet switching δικτύων –περαν φυσικά των optical switching.

Ας θεωρήσουμε τώρα την τοπολογία της Εικόνας 83. Πέραν των συνδέσμων δεδομένων, των διαφόρων διεπαφών και των καναλιών ελέγχου, διακρίνουμε και άλλα δικτυακά στοιχεία όπως τους Controllers και τα data switches. Τα μεν πρώτα περιέχουν όλη τη ευφυή λειτουργικότητα του πεδίου ελέγχου του GMPLS (δρομολόγηση, πρωτόκολλα σηματοδοσίας και TE, στοιχεία καθορισμού μονοπατιού). Τοπικά, διασυνδέονται μέσω καναλιών ελέγχου και αντίστοιχων διεπαφών. Τα δεύτερα γνωστά και ως κόμβοι μεταφοράς, αποτελούν δομικά στοιχεία του GMPLS που είναι ικανά να τερματίζουν μια ροή δεδομένων και να την προωθούν στο μονοπάτι του προορισμού της.



Εικόνα 83. Δομικά στοιχεία δικτύου GMPLS

Στα πλαίσια τώρα του Traffic Engineering, διακρίνουμε τα ακόλουθα **TE link attributes** ενός δικτύου GMPLS:

- **Link type**
- **Link ID**
- **Local interface IP address (για numbered TE links)**
- **Remote interface IP address (για numbered TE links)**
- **Local link identifier (για unnumbered links)**
- **Remote link identifier (για unnumbered links)**

Το Link type attribute αναγνωρίζει τον τύπο της TE γραμμής. Δύο τύποι καθορίζονται μέχρι αυτή τη στιγμή **(1: point–to–point; 2: multi–access)**. Τυπικά μόνο ο πρώτος τύπος έχει πρακτική εφαρμογή για τα δίκτυα μεταφοράς, εφόσον τα multi–access οπτικά ή TDM δίκτυα δεν έχουν ακόμη αναπτυχθεί.

Το Link ID χαρακτηριστικό έχει πολλαπλή σημασία. Για τις point–to–point συνδέσεις καθορίζει την διεύθυνση του δρομολογητή ενός controller που αντιστοιχίζεται στο άλλο άκρο της γραμμής. Τυπικά θα μπορούσε να χαρακτηριστεί ως ένα πεδίο για ένα IP, ικανό για δρομολόγηση, data switch.

Τα υπόλοιπα πεδία–χαρακτηριστικά έχουν ήδη εξηγηθεί σε προηγούμενες ενότητες.

Τέλος τα επόμενα GMPLS–TE link attributes είναι καθορισμένα για χρήση σε constraint–based καθορισμό μονοπατιού:

- **Traffic Engineering metric**. Το attribute αυτό χρησιμοποιείται ως κόστος που αντιπροσωπεύει την αντίστοιχη TE γραμμή στον γράφο.
- **Administrative group**. Είναι 32–bit αριθμός που διαφημίζεται για κάθε γραμμή και αναπαριστάνει την ποιότητα της σύνδεσης, ώστε η διαδικασία καθορισμού μονοπατιού να αποκτά δεσμεύσεις ως προς κάποια TE links με συγκεκριμένα χρώματα, ανάλογα με το είδος της υπηρεσίας.
- **Link protection type**. Παρουσιάζει τις ικανότητες προστασίας ενός TE συνδέσμου(Έχει επεξηγηθεί σε προηγούμενη ενότητα).

- **Shared Risk Link Group (SRLG)**. Είναι 32–bit αριθμός που αντιπροσωπεύει όλα τα SRLGs οπου ανήκει ένας σύνδεσμος. Για παράδειγμα πολλαπλά links μπορούν να αποτελούν ένα SRLG εαν διαμοιράζονται έναν συγκεκριμένο πόρο δικτύου του οποίου κάποια αστοχία μπορεί να επηρεάσει ενδεχομένως όλες αυτές τις γραμμές στο δίκτυο. Το πεδίο αυτό είναι ιδιαίτερα χρήσιμο για τον καθορισμό των μονοπατιών ανάκαμψης.
- **Interface Switching Capability descriptor**. Αντίθετα με τα προηγούμενα attributes, το ISC περιγράφει τα χαρακτηριστικά όχι ενός TE συνδέσμου αλλά μιας διεπαφής μεταφοράς δεδομένων. Η ακόλουθη πληροφορία είναι ενδεικτική του τι περιλαμβάνει αυτό το πεδίο:
  - **Interface switching capability type.** Το συγκεκριμένο πεδίο υποδυκνείει με ποιό τρόπο και με ποιά οργάνωση πακέτων, τα δεδομένα θα γίνονται switched από/προς τα αντίστοιχα interfaces.
  - **Data encoding type**. Προσφέρει τις απαιτούμενες πληροφορίες για το είδος της κωδικοποίησης που υποστηρίζεται απο το αντίστοιχο interface.
  - **Minimum/Maximum LSP bandwidth.**
  - **Interface Maximum Transmit Unit (MTU).**
  - **SONET/SDH indicator.**

Οι ελεγκτές στο δίκτυο είναι υποχρεωμένοι να ανταλλάσουν μηνύματα ελέγχου ώστε να λειτουργήσουν τα πρωτόκολλα σηματοδοσίας για την εγκαθίδρυση των μονοπατιών στο data plane. Γι'αυτό το σκοπό, ενθυλακώνουν τα μηνύματα αυτά μέσα στα IP πακέτα και χρησιμοποιούν την IP υποδομή για τη παράδοσή τους. Η παραδοσιακή IP μεταφορά απαιτεί την ύπαρξη IP πινάκων προώθησης σε όλους τους ελεγκτές, ώστε να γνωρίζει ο καθένας πως να προωθεί τα πακέτα. Αυτοί οι πίνακες θα πρέπει να χτίζονται και να διαχειρίζονται με δυναμικό τρόπο από κατάλληλα link–state IP routing πρωτόκολλα, όπως το OSPF ή το IS–IS, σε κάθε ελεγκτή. Συγκεκριμένα, κάθε ελεγκτής διαφημίζει όλη την απαιτούμενη πληροφορία για τον ίδιο και τα κανάλια ελέγχου του. Αυτά τα advertisements διανέμονται σε όλους τους υπόλοιπους ελεγκτές, και ο καθένας χτίζει με τη σειρά του μια Βάση Δεδομένων από συνδέσμους –Link State Database που παρέχει μια πληρη εικόνα της τοπολογίας. Από εκεί και έπειτα κάθε controller τρέχει έναν αλγόριθμο συντομότερου μονοπατιού στο LSD, και προσδιορίζει τα συντομότερα IP μονοπάτια για όλους τους υπόλοιπους.

Ένας ελεγκτής που εφαρμόζει πολιτικές Traffic Engineering απαιτεί μια ιδιαίτερα ακριβή αναπαράσταση του δικτύου τόσο από την μεριά των data switches όσο και TE links. Για τον σκοπό αυτό ειδικά στα πλαίσια του MPLS πρωτοκόλλου, τα Traffic Engineering πρωτόκολλα (OSPF–TE και ISIS–TE) διανέμουν τις TE πληροφορίες στο TE layer, με τον ίδιο τρόπο που προηγουμένως προωθούνταν τα IP based advertisements. Εξετάζουμε συνοπτικά τα δύο αυτά πρωτόκολλα.

Το **OSPF–TE** κάνει χρήση του OSPF opaque LSA option το οποίο εισάγεται στο RFC 2370. TE–βασισμένες πληροφορίες ενθυλακώνονται σε OSPF διαφανή –opaque LSAs και μεταφέρονται μέσω του OSPF μηχανισμού μεταφοράς. Τα TE LSAs είναι τύπου 10, και έτσι «πλημμυρίζουν» μόνο την OSPF περιοχή του LSA προέλευσης. Το αντίστοιχο TE layer είναι υπεύθυνο για την δημιουργία του γραφήματος με κόμβους τα data switches, και ακμές τα αντίστοιχα TE links. Αυτό θα είναι το γράφημα στη συνέχεια, οπού θα υπολογίσει τα μονοπάτια στο δίκτυο για υπηρεσίες μεταφοράς (LSPs).

Όπως έχουμε ξαναδεί, το TE LSA φορτίο δομείται ως ένα σύνολο από Type–Length–Value blocks (TLVs)Αυτό με τη σειρά του αποτελείται από:

- **Router Address TLV**
- **TE Link TLV**

Τέλος να αναφέρουμε οτι έχουν προταθεί, στα πλαίσια του GMPLS, επιπλέον επεκτάσεις στο OSPF–TE με τη μορφή νέων sub–TLVs.

Το πρωτόκολλο ISIS–TE επιτελεί τον ίδιο ακριβώς ρόλο με το OSPF–TE. Η επιλογή ανάμεσα στα δύο εξαρτάται αποκλειστικά από ποιό πρωτόκολλο δρομολόγησης χρησιμοποιείται στη πράξη στο πεδίο λειτουργικότητας ελέγχου. Για να διαφημίσουν την δικτυακή πληροφορία τους, οι ISIS ελεγκτές χρησιμοποιούν Link State Protocol Data Units που αποτελούνται από πολλαπλά TLVs. Αυτή τη φορά το ISIS καθορίζει δύο νέους τύπους TLVs: το **Traffic Engineering Router ID TLV**, και το **Extended IS Reachability TLV**. Και πάλι το GMPLS εισάγει καινούργιες επεκτάσεις για να διαφημίσει TE link attributes όπως: local and remote identifiers, link protection types, SRLGs.

Ο καθορισμός μονοπατιού στο GMPLS με χρήση περιορισμών –constraint based, απαιτεί να διαφημίζεται περισσότερη TE πληροφορία από ότι στο MPLS, κάτι που προκαλεί σημαντικά ζητήματα κλιμάκωσης. Η τεχνική του TE link bundling είναι μια μέθοδος για τη μείωση του όγκου αυτής της διαφημιζόμενης πληροφορίας αλλά και για την καλλίτερη διαχείριση του LSP. Μία γραμμή δεδομένων μέσα στο bundle καλείται component link. Τα component link IDs έχουν ουσία μόνο για τους ελεγκτές που χειρίζονται τα switches και στις δύο μεριές του bundle, ενώ για τα υπόλοιπα στοιχεία στο δίκτυο δεν είναι σημαντικά. Θα πρέπει να ισχύουν οι ακόλουθες προυποθέσεις για να είναι δύο ή περισσότερα component links μέρος μέρος του ίδιου bundle:

- Θα πρέπει να αρχίζουν και να τελειώνουν στο ίδιο ζεύγος των data switches.
- Θα πρέπει να ανήκουν στο ίδιο network layer; να έχουν δηλαδή τον ίδιο ISC ενδείκτη.
- Θα πρέπει να έχουν κοινές TE μετρικές.
- Θα πρέπει να ανήκουν στο ίδιο γκρουπ διαχείρισης.

Τα component links μπορούν να προσφέρουν διαφορετικές τεχνικές προστασίας, SRLGs, κτπ. Τέλος όπως και οι απλές TE γραμμές, τα TE bundles μπορεί να είναι αριθμημένα ή μη αριθμημένα. Ακόμη, τα παράλληλα TE–LSPs μπορούν να ενοποιηθούν σε bundles αρκεί να τηρούνται οι προηγούμενες συνθήκες.

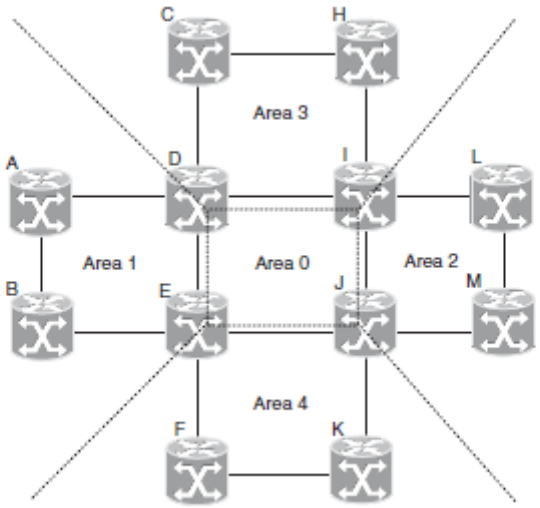
Ένα GMPLS LSP είναι ικανό να ενώνει διαφορετικές περιοχές δρομολόγησης ή ακόμη και διαφορετικούς διαχειριστικούς domains. Από την οπτική γωνία του Traffic Engineering, η τροφοδοσία και επίβλεψη των inter–domain LSPs υποννοεί την ύπαρξη ενός περιβάλλοντος από κατανεμημένους TE domains. Ας θεωρήσουμε την Εικόνα 84, οπού διακρίνουμε το παράδειγμα ενός δικτύου πολλαπλών περιοχών–domains. Υποθέτουμε οτι απαιτείται η εγκαθίδρυση υπηρεσίας από τον κόμβο A στον κόμβο M. Το πρόβλημα είναι , ωστόσο, οτι ο A δεν μπορεί να υπολογίσει το πλήρες μονοπάτι μέχρι και αυτό το προορισμό διότι γνωρίζει τα όρια μονο του δικού του domain. Υπάρχουν δύο τρόποι να καθοριστεί εν τέλει το μονοπάτι:

- Χρήση κατανεμημένου τρόπου καθορισμού μονοπατιού –distributed path computation.
- Χρήση στοιχείων για τον απομακρυσμένο υπολογισμό μονοπατιού –remote path computation element(s).

Ως προς τη πρώτη μέθοδο, ο ingress κόμβος A ζητάει από το τοπικό σύστημα δρομολόγησής του τη λίστα των κόμβων που διαφημίζουν την IP προσβασιμότητα μέχρι και τον ζητούμενο κόμβο προορισμού. Εαν η λίστα επιστραφεί κενή, τα path computation και service setup αίτηματα αποτυχαίνουν με το κωδικό σφάλματος "unknown service destination". Τότε ο κόμβος αυτός σημείου εισόδου υπολογίζει τα TE μονοπάτια σε εκείνους τους συνοριακούς κόμβους του (εδώ τους D και E), και επιλέγει το συντομότερο μονοπάτι να σηματοδοτήσει το LSP setup μήνυμα. Οταν το μήνυμα φτάσει στον ζητούμενο κόμβο του επόμενου γειτονικού domain, η ίδια διαδιακασία επαναλαμβάνεται, σε κάθε επόμενο domain, μέχρι να καθοριστεί πλήρως το μονοπάτι έως και τον τελικό κόμβο M. Για τον μηχανισμό προστασίας τώρα, και την επιλογή των μονοπατιών ανάκαμψης, η μέθοδος αυτή λειτουργεί ως εξής:

- Ο ingress κόμβος υπολογίζει διαδοχικά μονοπάτια γιά όλους τους συνοριακούς κόμβους που επιστρέφονται από το σύστημα δρομολόγησης.
- Έπειτα, ο ίδιος επιλέγει τον συντομότερο συνοριακό κόμβο (με την μικρότερη απόσταση), και στέλνει το LSP μήνυμα σε αυτόν.
- Το συγκεκριμένο μήνυμα περιλαμβάνει το προηγούμενο επιλεγμένο μονοπάτι ως το κυρίως λειτουργικό, όπως επίσης και μονοπάτια σε όλους τους συνοριακούς κόμβους ως εναλλακτικά.

Η δεύτερη μέθοδος χρησιμοποιεί remote path computation elements (PCEs) για τον καθορισμό του μονοπατιού. Στο συγκεκριμένο παράδειγμα, ας υποθέσουμε οτι ο κόμβος A μαθαίνει οτι μπορεί να χρησιμοποιήσει τους D και E ως απομακρυσμένα PCEs. Για τον καθορισμό των εναλλακτικών μονοπατιών, μπορεί να στείλει path computation αίτημα είτε στον D είτε στον E, είτε και στους δύο. Όταν ο κόμβος A λάβει τα αιτήματα αυτά από όλους τους PCEs, επιλέγει το βέλτιστο σύνολο μονοπατιών και εγκαθιδρύει τα μονοπάτια ανάκαμψης.



Εικόνα 84. Multi–Area Network

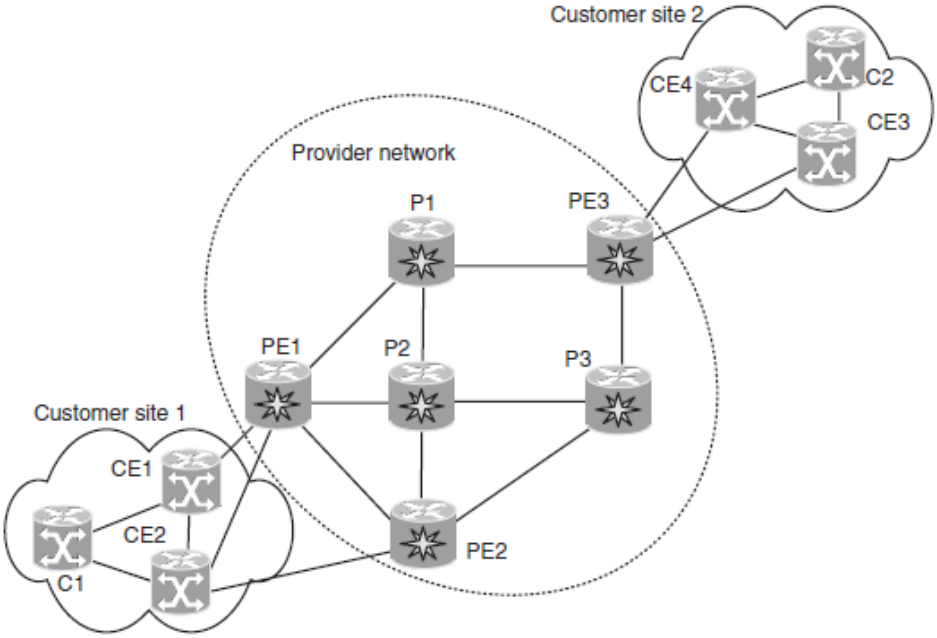
Ειδικά όταν ένα service LSP setup μήνυμα φθάσει σε έναν συνοριακό κόμβο, ο τελευταίος είναι υποχρεωμένος να πραγματοποιήσει μια ενοποίηση των LSP segments που ανήκουν σε γειτονικούς domains. Η διαδικασία αυτή καλείται **horizontal LSP integration**. Όταν και οι δύο domains τρέχουν τα ίδια πρωτόκολλα σηματοδοσίας, ο συνοριακός κόμβος θα εκτελεί την διαδικασία αυτή ως ένα συνεχόμενο –contiguous LSP, χωρίς παιρετέρω ενοποιήσεις. Σε διαφορετική περίπτωση, όταν ο συνοριακός κόμβος λάβει το setup μήνυμα επιτελεί τις ακόλουθες διαδικασίες:

- Πραγματοποιεί αντιστοίχηση, σε επίπεδο πεδίου λειτουργικότητας δεδομένων, του inter–domain LSP με το intra–domain LSP.
- Κάνει tunneling το μήνυμα αυτό που λαμβάνει στον γειτονικό συνοριακό κόμβο του επόμενου domain, ώστε να επαναληφθεί ξανά η ίδια διαδικασία.

3.3.2 ΕΙΚΟΝΙΚΑ ΔΙΚΤΥΑ ΕΠΙΠΕΔΟΥ 1 (LAYER 1 VPNS)

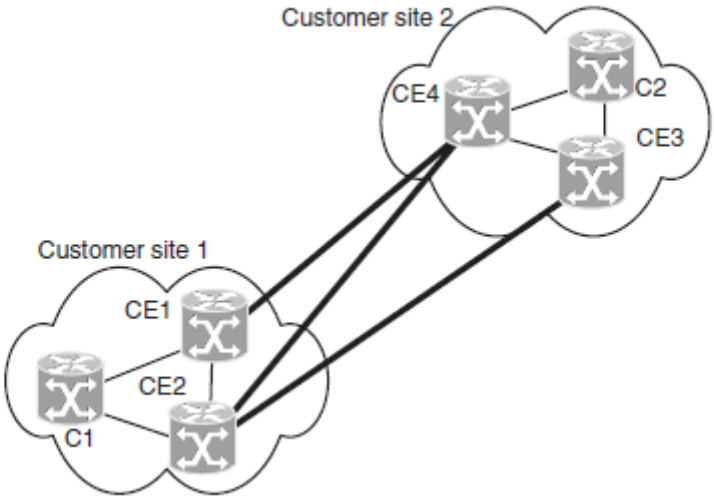
Το GMPLS είναι ένα ιδιαίτερα ικανό πρωτόκολλο στο να μετατρέπει πολλαπλές εφαρμογές σε βασισμένες σε μετάδοση δικτυακές υπηρεσίες. Όπως έχουμε τονίσει και σε προηγούμενες ενότητες μια υπηρεσία μεταφοράς –transport service είναι ένας τρόπος να προσφέρουμε σε έναν χρήστη (Customer) κίνηση με συγκεκριμένα χαρακτηριστικά και απαιτήσεις ανάμεσα σε δύο συνορικά σημεία ενός δικτύου παροχής υπηρεσιών (Provider Edge's), και με ένα προσυμφωνημένο επίπεδο ποιότητας υπηρεσιών, πολιτικής προστασίας και βαθμού ανθεκτικότητας σε δικτυακές αστοχίες. Έτσι, ο πελάτης αντιλαμβάνεται την υπηρεσία αυτή ως ένα σύνολο από τις ακόλουθες βασικές υπηρεσίες:

- Συνδεσιμότητα στο πεδίο λειτουργικότητας δεδομένων ανάμεσα σε δύο σημεία πελατών (Customer Sites).
- Χωρητικότητα σε bit rate.
- Format του τύπου κωδικοποίησης δεδομένων.
- Quality of Service.
- Διαθεσιμότητα.



Εικόνα 85. Layer one συστατικά δικτύου

Από την οπτική γωνία , τώρα, του Traffic Engineering, οι υπηρεσίες μεταφοράς κάνουν χρήση γραμμών TE ανάμεσα στα συνδεδεμένα CEs –Customer Edges (σημεία πελατών). Ας υποθέσουμε οτι υπάρχουν τρείς υπηρεσίες μεταφοράς οι οποίες συνδέουν το CE1 με το CE4, το CE2 με το CE4, και το CE2 με το CE3 αντίστοιχα, όπως φαίνεται στην Εικόνα 86.



Εικόνα 86. Ο TE γράφος δικτύου του παραδείγματός μας

Μια υπηρεσία μεταφοράς μπορεί να αντιστοιχηθεί σε μόνιμα –permanent, ημιμόνιμα –soft–permanent, και σε switched LSPs. Για τα μόνιμα μονοπάτια, το πεδίο λειτουργικότητας ελέγχου δεν συμμετέχει στην LSP επίβλεψη και διαχείρηση ούτε στο σημείο Πελάτη, ούτε στο σημείο Παρόχου. Αυτό που πραγματοποιείται σε επίπεδο διαχείρησης είναι τα NMSs –Network Management Systems και στα δύο αυτά σημεία να συμφωνούν στις παραμέτρους του LSP μονοπατιού και να επιβλέπουν τις περιοχές τους τοπικά.

Τα switched LSPs , από την άλλη, επιβλέπονται από άκρου–σε άκρου μέσω της συνεργασίας των πεδίων λειτουργικότητας ελέγχου των Customer και Provider σημείων, με μηδενική συμμετοχή των επιπέδων διαχείρισής τους. Στη περίπτωση των ημιμόνιμων LSPs, οι υπευθυνότητες ανάμεσα στα δύο αυτά πεδία λειτουργικότητας διαμοιράζονται με τον ακόλουθο τρόπο: οι PE–PE (PE–Provider Edge)περιοχές διαχειρίζονται από το control plane του Παρόχου, ενώ οι CE–PE σύνδεσμοι επιβλέπονται από το επίπεδο διαχείρησης –management plane.

Από δω και στο εξής ας θεωρήσουμε μια υπηρεσία επιπέδου ένα –Layer One service, ως ένα πλήρες σύνολο υπηρεσιών που μπορεί να προσφέρεται από το δίκτυο Παροχής. Αυτό το σύνολο περιλαμβάνει και λειτουργικότητες τόσο στο control όσο και στο data plane. Έτσι, μια υπηρεσία μεταφοράς μπορεί να θεωρηθεί ως ένα data plane συστατικό μιας υπηρεσίας Layer One. Μια απαίτηση γι'αυτές τις υπηρεσίες είναι τα κανάλια ελέγχου να είναι ικανά να εγκαθιδρύουν πληροφορίες σηματοδοσίας (RSVP–TE), συνόδους LMP, και να εκτελούν οποιοδήποτε πρωτόκολλο ανάμεσα στα σημεία πελατών.

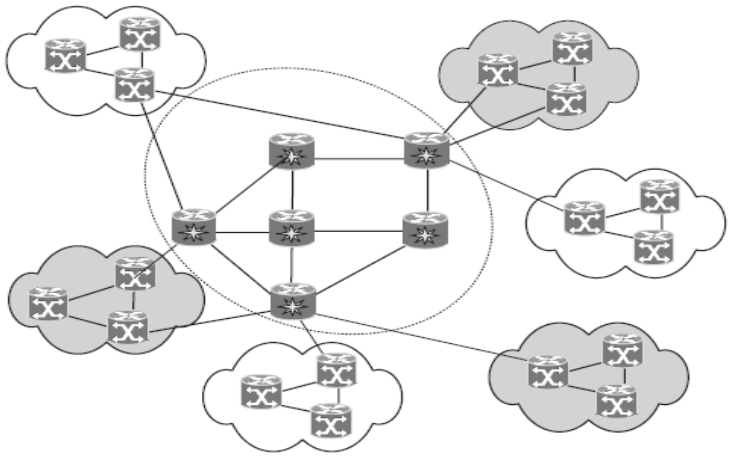
Το ITU–T έχει καθορίσει δύο κατηγορίες υπηρεσιών επιπεδου 1:

- Κατηγορία 1: Απλή υπηρεσία (Ένας πελάτης, δύο CEs)
- Κατηγορία 2: Πολλαπλή υπηρεσία (Ένας πελάτης, τρία ή περισσότερα CEs)

Επιπλέον, το L1VPN καθορίζεται ως υπηρεσία επιπέδου ένα της κατηγορίας 2, με τις ακόλουθες προσθήκες:

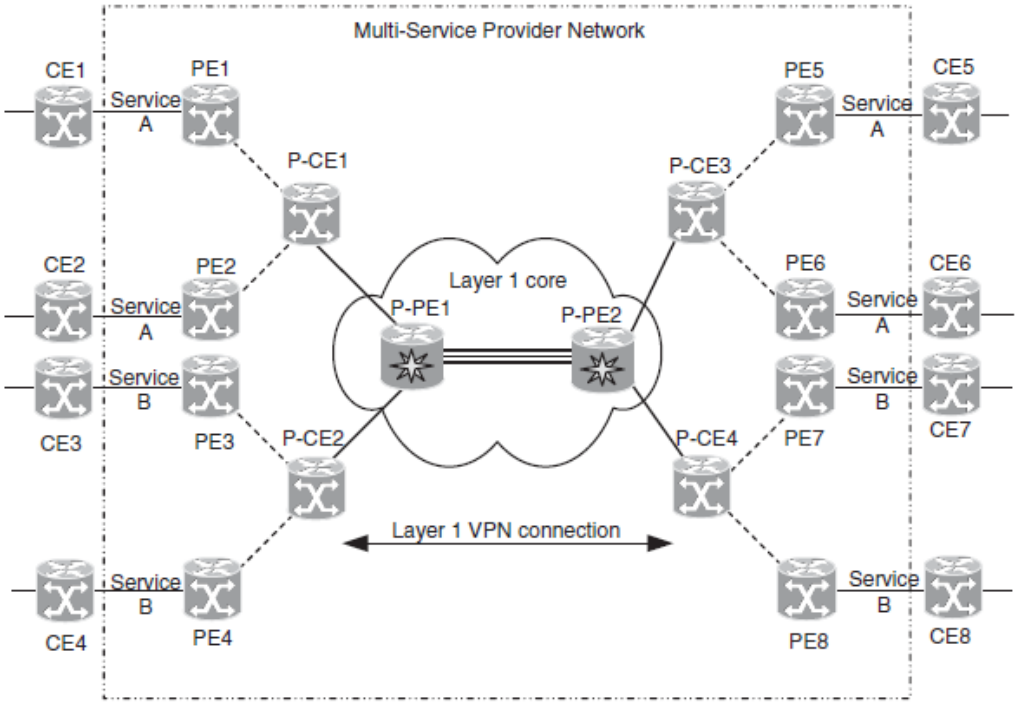
- Το σύνολο των CEs που ανήκουν σε έναν συγκεκριμένο Πελάτη μπορούν να συνδεθούν μόνο εάν είναι μέλη του ίδιου VPN.
- Η πληροφορία συνδρομής των υπηρεσιών διανέμεται ανάμεσα στα CEs
- Μια ξεχωριστή per–service based πολιτική θα μπορούσε να εφαρμοσθεί από τον Πελάτη, που θα καθόριζε για παράδειγμα τον τύπο της προστασίας απέναντι στις αστοχίες.

Ένα L1VPN θα μπορούσε να θεωρηθεί ως ένα VPN του οποίου το πεδίο λειτουργικότητας δεδομένων λειτουργεί σε επίπεδο ένα. Μια σύνδεση ανάμεσα σε CEs που βρίσκονται σε διαφορετικά σημεία ενός L1VPN καλείται Layer One VPN σύνδεσμος. Παράδειγμα δύο L1VPNs φαίνεται στην Εικόνα 87.



Εικόνα 87. Layer One VPNs

Ας θεωρήσουμε, τώρα, ένα μεγάλο δίκτυο Παροχής που προσφέρει πολλαπλού τύπου υπηρεσίες στους Πελάτες του (Εικόνα 88).



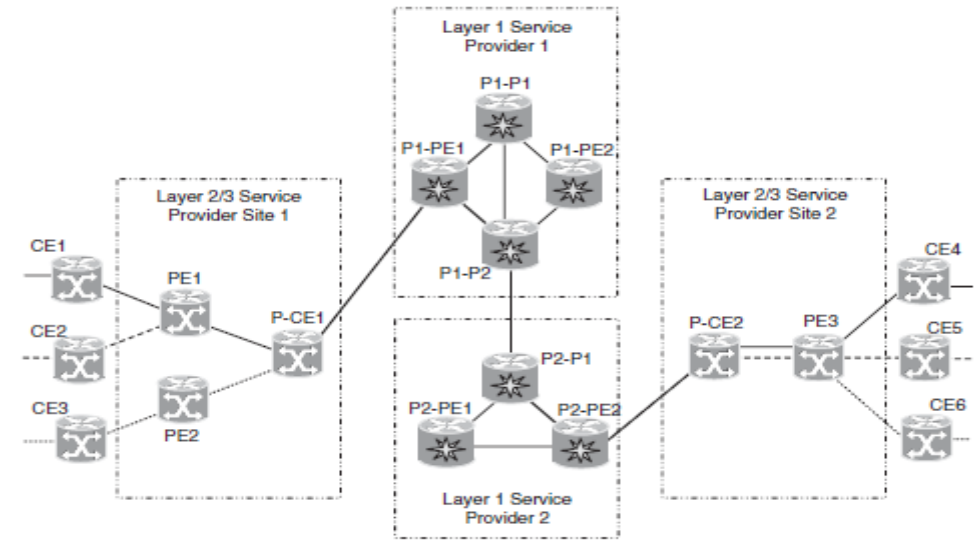
Εικόνα 88. Παράδειγμα Multi–Service δικτύου κορμού

Ένας τρόπος να διαχειριστούμε αποδοτικά ένα τέτοιο δίκτυο είναι να το διαιρέσουμε σε διάφορα τμήματα –segments. Υποθέτουμε οτι το τμήμα Α είναι υπεύθυνο για να προσφέρει υπηρεσίες τύπου Α (π. χ. TDM) στους πελάτες του, ενώ το Β προσφέρει υπηρεσίες IP. Επιπλέον θεωρούμε οτι ένα τρίτο τμήμα –Layer One Core– προσφέρει υπηρεσίες επιπέδου ένα στα τμήματα Α και Β ώστε να μεταφέρουν κίνηση ανάμεσα στους φυσικούς τους προορισμούς. Η κίνηση που μεταδίδεται πάνω στο κορμό επιπέδου ένα μπορεί να είναι οποιοδήποτε τύπου, και έτσι οι ίδιοι πόροι μεταφοράς μπορούν να μοιράζονται ανάμεσα σε πολλαπλές υπηρεσίες υψηλότερων επιπέδων.

Θα εξετάσουμε, τώρα, την σημασία των L1VPN υπηρεσιών στην αποδοτική μεταφόρα κίνησης ανάμεσα σε ένα δίκτυο κορμού. Ας υποθέσουμε οτι θέλουμε να μεταφέρουμε IP κίνηση ανάμεσα στους κόμβους CE4 και CE8. Με την προυπόθεση ότι όλοι οι κόμβοι είναι GMPLS συμβατοί, ο PE4 θα υπολόγιζε ενα multi–layer μονοπάτι από τον εαυτό του στον PE8. Η διαδικασία του LSP Setup θα πυροδοτούσε την εγκαθίδρυση ενός ιεραρχικού LSP μονοπατιού (H–LSP), καθώς και την διαφήμιση του αντίστοιχου TE συνδέσμου ανάμεσα στα P–CE2 και P–CE4 στοιχεία. Μάλιστα, το ίδιο το H–LSP θα μπορούσε να μεταφέρει κίνηση και από άλλα εξίσου μονοπάτια, π. χ. από το PE3 στο PE7.

Υπάρχουν διάφοροι λόγοι για τους οποίους είναι αποδοτικότερη η χρήση των L1VPN. Οι σύνδεσμοι μεταφοράς πάνω στο δίκτυο κορμού επιπέδου ένα εγγυώνται μόνο συνδεσιμότητα επιπέδου δεδομένων, και έτσι η ρύθμιση της λειτουργικότητας πεδίου ελέγχου απαιτεί επιπλέον υπηρεσίες, παραμετροποιήσεις, και φυσικά πόρους. Το L1VPN από την άλλη παρέχει ένα ευρή σύνολο υπηρεσιών που περιλαμβάνει και την ανταλλαγή control plane δεδομένων ανάμεσα σε Πελάτες που ανήκουν στο ίδιο VPN. Ένας δεύτερος λόγος για την χρήση των L1VPN είναι η ευελιξία που προσφέρουν στην εφαρμογή διαφορετικών πολιτικών σε κάθε εικονικό δίκτυο που βρίσκονται. Για παράδειγμα διαφορετικά εικονικά δίκτυα προσφέρουν διαφορετικούς τύπους προστασίας ανάλογα με τα σημεία πελατών που συνδέουν. Τέλος, το L1VPN αφαιρεί κάθε απαίτηση για ενοποίηση και ύπαρξη ομοιογένειας του πεδίου λειτουργικότητας ελέγχου κατά την διαχείριση διαφορετικών/ετερογενών δικτύων.

Στην Εικόνα 89 διακρίνουμε ένα παράδειγμα **εμφωλεύσιμου –nesting** L1VPN σε ένα ιδεατό σενάριο. Με τον όρο αυτό εννοούμε μια υπηρεσία που παρέχει συνδεσιμότητα σε επίπεδο data και control plane ανάμεσα σε δύο σημεία –sites με την ταυτόχρονη υποστήριξη και μιας δεύτερης υπηρεσίας. Στο παράδειγμά μας ανάμεσα στα σημεία P–CE1 και P–CE2, διακρίνουμε πρακτικά δύο διαφορετικές υπηρεσίες: Service Provider 1 και Service Provider 2.



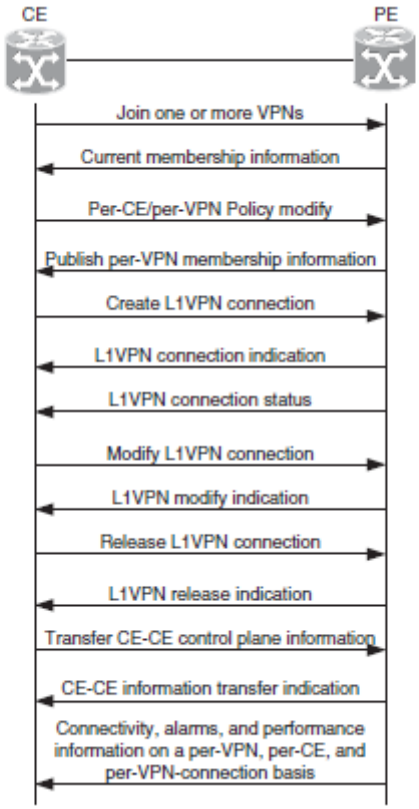
Εικόνα 89. Εμφωλεύσιμο Layer One VPN

Ως προς την διαδικασία της διανομής των πόρων ανάμεσα σε διαφορετικά εικονικά δίκτυα, σε επίπεδο data plane, διακρίνουμε τα ακόλουθα μοντέλα:

- **Shared.** Σε αυτό το μοντέλο οποιοσδήποτε πόρος του δικτύου παροχής μπορεί να κατανεμηθεί σε οποιοδήποτε VPN.
- **Dedicated.** Εδώ οι πόροι διαχωρίζονται στατικά και προκαθορισμένα ανάμεσα στα εικονικά δίκτυα, και μπορούν να χρησιμοποιηθούν για να υποστηρίξουν L1VPN υπηρεσίες μόνο για τα VPNs που προορίζονται.
- **Hybrid.** Υπάρχει ένα σύνολο από διαμοιραζόμενους πόρους προς χρήση από οποιδήποτε εικονικό δίκτυο, καθώς και πόροι εξειδικευμένοι προς χρήση απο συγκεκριμένα VPNs.

Στη συνέχεια, θα εξετάσουμε συνοπτικά την διαδικασία εγκατάστης ενός L1VPN. Υπάρχουν τρία μοντέλα για την συγκεκριμένη υλοποίηση:

- **Management–based**. Στο συγκεκριμένο μηχανισμό, ο Πελάτης και ο Πάροχος επικοινωνούν μέσω του πεδίου λειτουργικότητας διαχείρησης. Συγκεκριμένα, το NMS του Πελάτη στέλνει αιτήσεις στο NMS του Παρόχου για την εγκαθίδρυση L1VPN συνδέσεων ανάμεσα σε ένα ζεύγος από CEs. Το σύστημα διαχείρισης του Παρόχου απαντά με πληροφορίες για την κατάσταση του υπάρχοντος L1VPN, όπως εάν έχει επιτύχει η εγκατάστασή του, εάν όχι ποιοί είναι οι λόγοι αποτυχίας του, σε ποιές αστοχίες αυτή αποδίδεται, καθώς και εαν οι QoS παράμετροι κίνησης πλέον ικανοποιούν τα προσυμφωνημένα επιπεδα SLAs.
- **Signaling Only**. Εδώ το CE χρησιμοποιεί το User–Network Interface (UNI) για την δυναμική αίτηση, τροποποίηση, και απελευθέρωση L1VPN συνδέσεων. Δεν υπάρχει ανταλλαγή πληροφορίας σε επίπεδο control plane πάνω στα UNI.
- **Signaling and Routing**. Το συγκεκριμένο μοντέλο υπηρεσίας είναι και το περισσότερο ενδιάφερον, καθώς το UNI ανάμεσα στα CE και PE χρησιμοποιείται για όλες τις L1VPN συνδέσεις. Η αναταλλαγή μηνυμάτων δρομολόγησης ανάμεσα στα CE και PE είναι ο κυρίαρχος τρόπος για ένα CE να μάθει τους γειτονικούς του στο ίδιο εικονικό δίκτυο, καθώς και να ανταλλάξει πληροφορίες δρομολόγησης και TE από απομακρυσμένα σημεία.



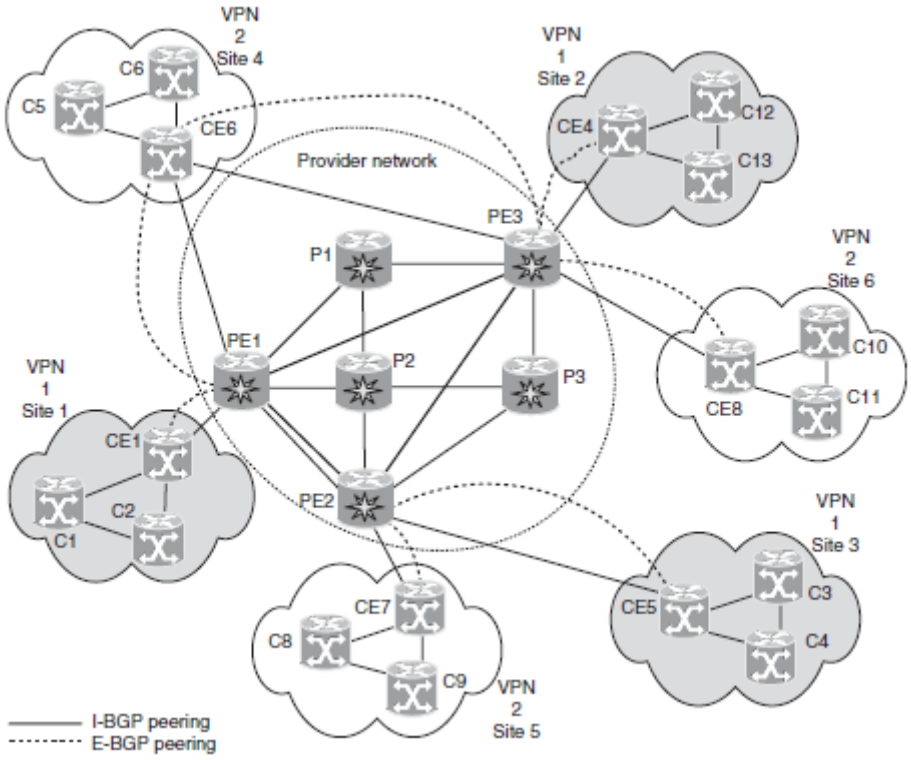
Εικόνα 90. Ανταλλαγή μηνυμάτων ανάμεσα στα CE και PE κατά την εγκατάσταση ενός L1VPN

Κλείνοντας την παρούσα ενότητα θα περιγράψουμε συνοπτικά τις δύο περισσότερο δημοφιλείς, βασισμένες στο GMPLS, L1VPN προσεγγίσεις: τα **Generalized Virtual Private Networks (GVPNs)**, και **GMPLS Overlays**. Οι δύο αυτές προσεγγίσεις διαθέτουν πολλά κοινά χαρακτηριστικά επειδή και οι δύο βασίζονται στο GMPLS. Αυτά περιλαμβάνουν την διευθυνσιοδότηση CE–PE σύνδεσης, την σηματοδοσία της, καθώς και την δυναμική επίβλεψη των PE–PE τμημάτων των CE–CE L1VPN συνδέσεων. Η κυριότερη διαφορά τους έγγυται στον μηχανισμό αυτοανίχνευσης του εικονικού δικτύου: πως τα PEs μαθαίνουν για απομακρυσμένα CEs, σε ποια VPNs πραγματικά ανήκουν, και ποιά PEs είναι συνδεδεμένα σε αυτά.

Για κάθε VPN, ένα PE διατηρεί έναν πίνακα συσχετίσεων με αντιστοιχίσεις ανάμεσα σε τριάδες <CE_ID, PE_VPN_ID, PE_ID> και την κατάσταση των CE–PE συνδέσεων που έχει ανιχνεύσει τοπικά.

Κάθε μια από τις πιο πάνω προσεγγίσεις κάνει χρήση του GMPLS πρωτοκόλλου για τη εκτέλεση της σηματοδοσίας μεταξύ των CE και PE με σκοπό την αρχικοποίηση, τροποποίηση, και απελευθέρωση L1VPN συνδέσεων με τα απομακρυσμένα CEs. Επιπλέον, το GMPLS πεδίο λειτουργικότητας ελέγχου χρησιμοποιείται σε κάθε περίπτωση για οτιδήποτε απαιτείται ως προς την επίβλεψη και συντήρηση των PE–PE τμημάτων του L1VPN, καθορισμό μονοπατιών, προστασία από αστοχίες, κ.τ.π.

Θα δούμε αρχικά τα GVPNs. Η ιδέα πίσω από αυτή τη προσέγγιση είναι η επέκταση του BGP–VPN framework πάνω στο L1VPN. Υποτίθεται οτι το BGP –Border Gateway Protocol πρωτόκολλο δρομολόγησης τρέχει τουλάχιστον ανάμεσα στη περιοχή του Παρόχου (I–BGP) και μεταξύ των CEs και PEs (E–BGP). Στην Εικόνα 91 διακρίνουμε ένα παράδειγμα δικτύου με GVPNs.



Εικόνα 91. Generalized VPNs (GVPNs)

Στα πλαίσια του GVPN, ο πίνακας που περιέχει τις CE–PE αντιστοιχίσεις μαζί με τη κατάσταση των CE–PE συνδέσμων καλείται **Generalized Virtual Switching Instance (GVSI)**. Τα GVSIs διατηρούνται από τα PEs σε μια per–VPN βάση. Ο πίνακας αυτός ενημερώνεται από δύο πηγές: Πληροφορίες που σχετίζονται με τοπικές CE–PE συνδέσεις παρέχονται από τα συνδεδεμένα CEs μέσω του E–BGP πρωτοκόλλου, ενώ πληροφορίες για απομακρυσμένα CE–PE links παρέχονται από τον βασισμένο στο BGP μηχανισμό αυτοανίχνευσης των VPNs.

Το ζήτημα είναι σε αυτό το σημείο πως ένα CE θα μαθαίνει για τη διαθεσιμότητα άλλων CEs μέσα σε ένα συγκεκριμένο L1VPN. Μια λύση θα ήταν η εφαρμογή BGP επεκτάσεων γι'αυτό το σκοπό. Τα PEs θα πρέπει να εγκαθιδρύουν E–BGP συνόδους με όλα τα συνδεδεμένα CEs και να τα χρησιμοποιούν για να αποστέλλουν ενημερωμένες VPN πληροφορίες. Για να γίνει αυτό εφικτό, θα πρέπει το δίκτυο Παροχής να συμμετάσχει στην VPN δρομολόγηση. Οφείλει:

- Να εγκαθιδρύσει IGP (π. χ. OSPF) συνδέσεις ανάμεσα στα PEs και CEs.
- Να χρησιμοποιήσει αυτές τις συνδέσεις για τη διαφήμιση των TE δεσμεύσεων για όλες τις PE–CE γραμμές που ανήκουν σε ένα συγκεκριμένο VPN.
- Να "πλημμυρίσει" –flood τις TE πληροφορίες ανάμεσα στα συνοριακά VPNs.

Σε κάθε περίπτωση, ο μηχανισμός μεταφοράς γι'αυτές τις συνδέσεις είναι IP tunnels μέσα στο πεδίο λειτουργικότητας ελέγχου, τα οποία μπορούν να εγκαθιδρύονται κάθε φορά που ένα GVSI μαθαίνει για την ύπαρξη ενός νέου GVSI.

Περνάμε, τέλος, στη δεύτερη προσέγγιση, στα **GMPLS overlays**. Ως γνωστόν το BGP είναι ένα distance–vector πρωτόκολλο δρομολόγησης σχεδιαμένο για την διανομή πληροφορίας γειτνίασης σε μεγάλα IP δίκτυα. Για τα πεδία λειτουργικότητας ελέγχου των Packet Switched Capable –PSC δικτύων , ωστόσο, δεν θεωρείται κομμάτι τους, και έτσι άλλα link state IGP πρωτόκολλα , όπως OSPF και IS–IS, είναι πιο αποτελεσματικά και πιο κατάλληλα για τις απαιτήσεις του Traffic Engineering. Το BGP από την άλλη είναι ένα ιδιαίτερα πολύπλοκο πρωτόκολλο και δύσκολο στην διαχείρισή του. Το γεγονός αυτό καθιστά τα GVPN λιγότερο ελκυστικά στους Παρόχους Υπηρεσιών επιπέδου ένα.

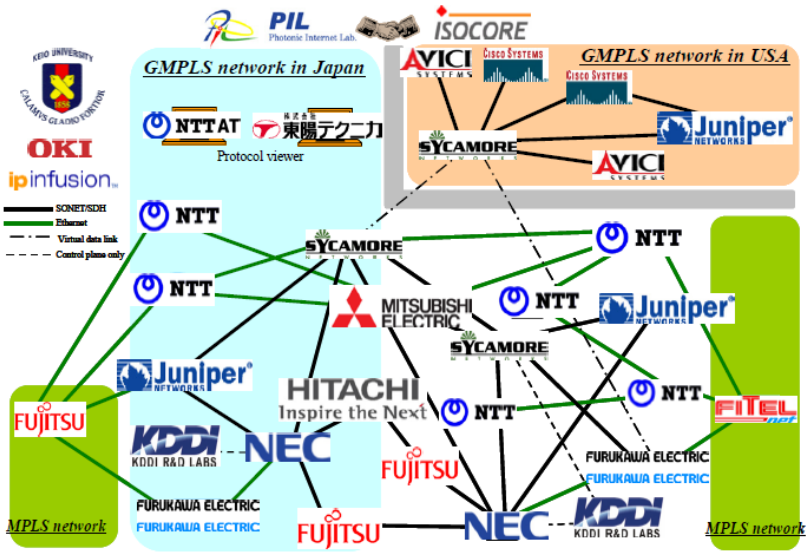
Έτσι ερχόμαστε στα GMPLS overlays (γνωστά και ως GMPLS UNI) που προσφέρουν μια διαφορετική προσέγγιση για τα L1VPNs. Ο συγκεκριμένος μηχανισμός μοντελοποιεί το δίκτυο Παροχής ως ένα δίκτυο κορμού και τα Εικόνικά Δίκτυα ως επικαλυπτόμενα δίκτυα ή overlays. Τα overlays συνδέονται με το δίκτυο κορμού στο πεδίο λειτουργικότητας δεδομένων μέσω CE–PE συνδέσεων και στο πεδίο λειτουργικότητας ελέγχου μέσω CE–PE καναλιών ελέγχου. Τα CE–PE κανάλια χρησιμοποιούνται για ανταλλαγή μηνυμάτων σηματοδοσίας ανάμεσα στα CEs και PEs. Το CE–PE πρωτόκολλο σηματοδοσίας είναι πλήρως συμβατό με το κλασσικό GMPLS RSVP. Επιπλέον, η CE–PE TE διευθυνσιοδότηση γραμμής είναι ακριβώς ίδια με το GVPN. Για τον σκοπό του υπολογισμού μονοπατιών των PE–PE τμημάτων των CE–CE συνδέσεων, κάθε PE πρέπει να είναι ικανός να μεταφράζει την CE διεύθυνση προορισμού σε μια egress PE διεύθυνση. Αυτό επιτυγχάνεται μέσω και παλι ενός πίνακα αντιστοιχίσεων, ενώ είναι δυνατόν μέσω κατάλληλων TE επεκτάσεων στα χρησιμοποιούμενα πρωτόκολλα δρομολόγησης (OSPF–TE, IS–IS–TE) να πραγματοποιούμε λειτουργίες αυτο–ανίχνευσης και διαφήμισης πληροφοριών γειτνίασης.

Στο επίπεδο τώρα του πεδίου λειτουργικότητας ελέγχου, επειδή σε ορισμένες περιπτώσεις το overlay δίκτυο είναι σε διαφορετικό επίπεδο μεταγωγής –switching layer από το δίκτυο κορμού, είναι εφικτό να γίνεται ενθυλάκωση της control plane κίνησης μέσα στην L1VPN σύνδεση. Είναι εξίσου εφικτό να κάνουμε tunneling την διαδικασία ανταλλαγής πληροφορίας δρομολόγησης ώστε όλα τα overlays να συμμετέχουν πρακτικά στο ίδιο IGP.

3.4.1 ΕΜΠΟΡΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ GMPLS

Το **PIL (Photonic Internet Laboratory) organization** ιδρύθηκε το Σεπτέμβριο του 2002 με σκοπό την προώθηση της έρευνας και την ανάπτυξη των φωτονικών δικτύων επόμενης γενιάς, καθώς και για εκτεταμένες προσπάθειες τυποποίησης διαφόρων σχετικών τεχνολογιών σε διεθνές επίπεδο. Ο PIL οργανισμός σήμερα διαθέτει έξι πωλητές και ακαδημαικά ιδρύματα:**Keio University, NTT, NEC Corporation, Fujitsu Laboratories Ltd. , The Furukawa Electric Co. , Ltd. , Mitsubishi Electric Corporation, Oki Electric Industry Co. , Hitachi, Ltd. και IPinfusion**. Συγκεκριμένα προωθεί την εξάπλωση του εξελιγμένου photonic–GMPLS framework, το οποίο κάνει χρήση ευρυζωνικής, οικονομικά αποδοτικής οπτικής τεχνολογίας ώστε να υλοποιεί IP κεντρικά δίκτυα. Επομένως, αποτελεί το PIL ενα consortium για εκτεταμένη έρευνα πάνω στο GMPLS πρωτόκολλο καθώς και για προώθηση της τυποποίησης πάνω σε αυτή τη περιοχή.

Ιστορικά να αναφέρουμε οτι τα μέλη του PIL οργανισμού NTT, NEC Corporation, Fujitsu Laboratories Ltd. , The Furukawa Electric Co. , Ltd. , και Mitsubishi Electric Corporation, κατόρθωσαν τον Οκτώβριο του 2003 να ολοκληρώσουν επιτυχημένα τα πρώτα παγκοσμίως MPLS–GMPLS τεστ διαλειτουργικότητας, κάνοντας χρήση multi–layer multi–route GMPLS πρωτοκόλλων σηματοδοσίας και ελέγχου. Να σημειώσουμε οτι στο συγκεκριμένο event συμμετείχαν πάνω από 600 σύνεδροι από γνωστές εταιρίες Παρόχων Υπηρεσιών, carrier και network system vendors.



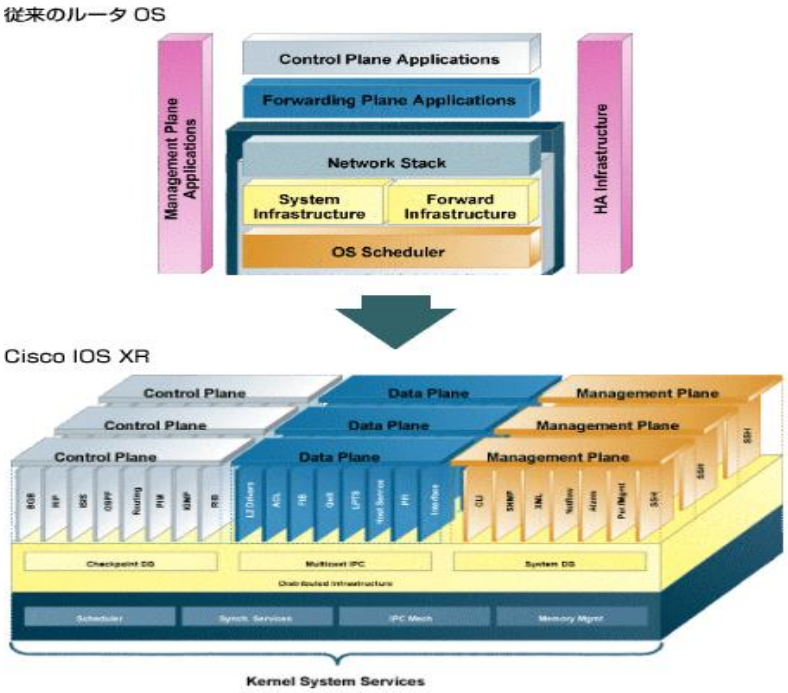
Εικόνα 92. GMPLS vendor's και παροχείς υπηρεσιών το 2005

Στη συνέχεια θα αναφέρουμε συνοπτικά τον GMPLS εξοπλισμό των πέντε μεγαλύτερων players στο συγκεκριμένο μερίδιο αγοράς IT υπηρεσιών.

Αποτέλεσμα της συνεργασίας της εταιρίας CISCO Systems με την FUJITSU ήταν η εμπορική διάθεση των GMPLS δρομολογητών της σειράς XR12000 **(Fujitsu and Cisco XR12000)**, με πιό πρόσφατη αυτή της XR12800 **(Fujitsu and Cisco XR12800)**.

Στην Εικόνα 93 διακρίνουμε έναν Cisco XR 12000 Router με 8XFE–TX, 5X1GE, 2XOC48–POS/RPR, και 1XCHSTM1/OC–3 SPAs, ενώ στην Εικόνα 94 φαίνεται η χρησιμοποιούμενη αρχιτεκτονική στα διάφορα πεδία λειτουργικότητας.

Εικόνα 93. Cisco XR 12000 Router



Εικόνα 94. Αρχιτεκτονική του Cisco XR 12000 Router

Ο συγκεκριμένος δρομολογητής υποστηρίζει Layer 2/Layer 3 VPNs over MPLS, 1 εκατομμύριο IPv4/MPLS ή 512, 000 IPv6 καταχωρήσεις δρομολόγησης, και μηχανισμούς και πολιτικές QoS. Κάνει χρήση των δημοφιλέστερων πρωτοκόλλων δρομολόγησης επιπέδου 3, όπως BGPv4, OSPFv3, IS–IS και EIGRP, ενώ παρέχει τα συμβατά με το GMPLS πρωτόκολλα σηματοδοσίας RSVP–TE και CR–LDP. Τέλος προσφέρει την ευέλικτη λειτουργικότητα διεπαφής του γνωστού Cisco IOS® Software και Cisco IOS XR Software command–line interface (CLI).

Περνάμε έπειτα στους οπτικούς μεταγωγείς της εταιρείας Sycamore, και συγκεκριμένα της σειράς **SN 3000 (Optical Edge Switch)** και την πλατφόρμα **DNX Cross Connect**.

Η πρώτη επιτυγχάνει οπτική μεταγωγή σε επίπεδο δικτύου κορμού μέσω της χρησιμοποίησης πολλαπλών λειτουργιών όπως ADM, DCS, Ethernet, και οπτική μεταφορά. Μεταχειρίζεται τις υπηρεσίες με μέγιστη αποτελεσματικότητα και απόδοση σε ταχύτητες που περνάνε από το DS3 και E1 στο OC–192/STM–64. Ορισμένα ενδεικτικά χαρακτηριστικά διεπαφών της:

- **24 x DS3**
- **21 x E1**
- **8 x OC–3/STM–1**
- **4 x OC–12/STM–4**
- **4 x OC–48/STM–16**
- **1 x OC–192/STM–64**
- **4 x Gigabit Ethernet, rate control**
- **DWDM multiplexers**
- **Integrated transport optics (from 1310nm SR to 15xxnm LR–2+)**

Παρέχει ASON/GMPLS συμβατό πεδίο λειτουργικότητας ελέγχου, MPLS based σηματοδοσία και πρωτόκολλα δρομολόγησης. Τέλος, προσφέρει τους ακόλουθους εξιδεικευμένους μηχανισμούς προστασίας από αστοχία:

- **Linear, Ring, Mesh, and Hybrid**
- **Per port software configurable**
- **1+1 Linear APS/MSP**
- **UPSR/SNCP**
- **2– and 4–fiber BLSR/MS–SPRing**
- **1+1 Path Protected**
- **1:n PDH Protection**
- **Dynamic Mesh Restoration**
- **Gateway between SONET and SDH**
- **IP–based and OSI–based DCC interoperability**

Τέλος, η οπτική πλατφόρμα cross–connect DNX υποστηρίζει με τη σειρά της τόσο επεξεργασία/μεταγωγή κυκλώματος και πακέτου όσο και εξελιγμένες τεχνικές αποκατάστασης στον οπτικό πυρήνα.

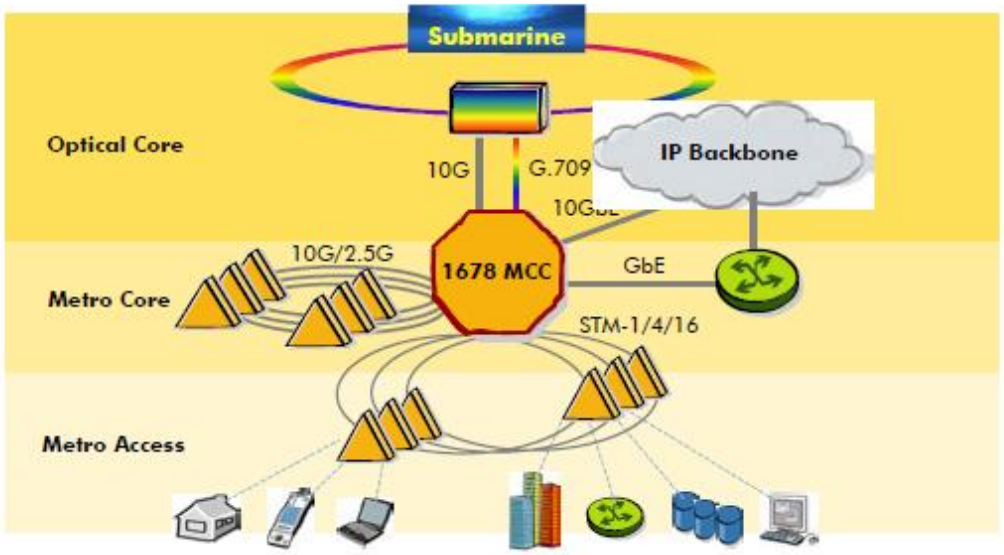
Περνάμε και στον τέταρτο πιο δημοφιλή πωλητή GMPLS δρομολογητών, την εταιρεία JUNIPER Networks.

Εδώ, θα παρουσιάσουμε τον **T640 core router**, ο οποίος διακρίνεται και στην Εικόνα 95. Πρόκειται για ένα ολοκληρωμένο σύστημα δρομολόγησης που παρέχει Gigabit Ethernet, SONET/SDH και άλλα high–speed interfaces για μεγάλης κλίμακας δικτυακές υπηρεσίες και ISPs. Υποστηρίζει μέχρι και 128 SONET/SDH OC48/STM16, 32 SONET/SDH OC192/STM64, ή 128 Gigabit Ethernet θύρες, με μέγιστη χωρητικότητα τα 320 Gbps, full duplex. Τέλος, μέσω του διαχωρισμού του πεδίου λειτουργικότητας ελέγχου από την όλη διαδικασία του packet forwarding επιτυγχάνει μεγαλύτερη απόδοση και αξιοπιστία.

Εικόνα 95. Juniper T640 gmpls core router

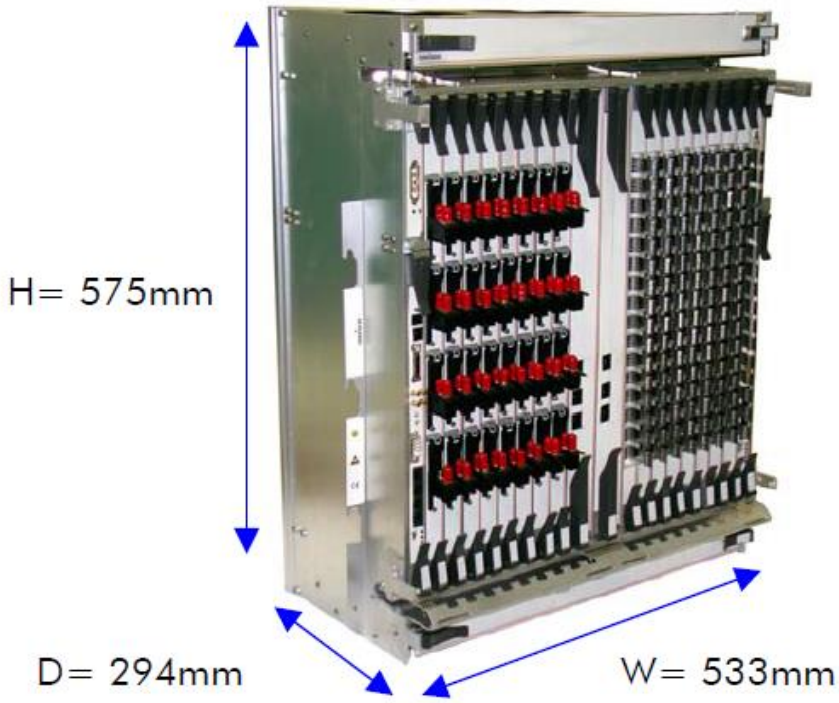
Ο πέμπτος πιο δραστήριος πωλητής δρομολογητών και υπηρεσιών GMPLS είναι η εταιρεία ALCATEL με τη σειρά των **1678 Metro Core Connect (MCC)**. Πρόκειται για μια νέα γενιά Optical Multiband πλατφόρμας με ευρυζωνικές (SDH/Sonet) αλλά και OTN και L2 (Ethernet) λειτουργικότητες. Ξεκινώντας με χωρητικότητα μεταγωγής τα 640Gbps, η συγκεκριμένη αρχιτεκτονική απευθύνεται σε πληθώρα υπηρεσιών από metro σε backbone δίκτυα μέχρι και full mesh τοπολογίες βασισμένες στο πεδίο λειτουργικότητας ελέγχου GMPLS/ASON. Εκπληρώνει με βέλτιστο τρόπο όλες τις σύγχρονες απαιτήσεις των οπτικών δικτύων επόμενης γενιάς όπως:

- Απλοποίηση και βελτιστοποίηση δικτύου.
- Ελαχιστοποίηση κόστους.
- Υποστήριξη broadband υπηρεσιών.
- Ευκολία επέκτασης και δυνατότητα κλιμάκωσης.



Εικόνα 96. Η Alcatel 1678 MCC λειτουργικότητα

Ο συγκεκριμένος GMPLS κόμβος είναι έτοιμος για μελλοντική επέκταση στα 160 Gbit/s και μέχρι 5 Tbit/s στην ευρυζωνική λειτουργία.



Εικόνα 97. Ο Alcatel 1678 MCC κόμβος

Διαθέτει τα ακόλουθα interfaces:

- 4x STM-64 port
  - 4x I-64.1 port (VSR)
  - 4x S-64.2 port (with XFP technology)
- 1x STM-64 port
  - 1x I-64.1 port (VSR)
  - 1x S-64.2 port
  - 1x L-64.2 port
  - 1x STM-64 VLH port
  - 1x STM-64 ULH port
- 4x STM-64 USR port
- 16x STM-16 unit
- 16x STM-4/1 unit
- 16x GBE SX/LX unit

Το GMPLS–based πεδίο λειτουργικότητας ελέγχου στον Alcatel 1678 MCC υλοποιείται με το GMRE λογισμικό (Generalized MPLS Routing Engine). Το GMRE διαχειρίζεται το UNI/NNI πρωτόκολλο με in–band σηματοδοσία και επιτρέπει την δυναμική εγκατάσταση μονοπατιού καθώς και την άμεση αποκατάσταση μετά από αστοχία.

Τέλος να τονίσουμε οτι πρόκειται για έναν Lambda aware κόμβο, καθώς διαθέτει την ικανότητα 'έξυπνης' επεξεργασίας και μεταγωγής χρωμάτων μέσω της DWDM τεχνολογίας σε πολυ υψηλές ταχύτητες.

3.4.2 ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΕΝΟΣ PHOTONIC MPLS ROUTER

Η ποσότητα της μεταδιδόμενης κίνησης IP δεδομένων έχει αυξηθεί δραματικά τα τελευταία χρόνια. Για την αντιμετώπιση αυτής της ραγδαίας αύξησης καθώς και των απαιτήσεων που αναμφισβήτητα γεννάει έχουν προταθεί μεγάλης κλίμακας δρομολογητές, ευέλικτοι μηχανισμοί ελέγχου καθώς και εξελιγμένη οπτική τεχνολογία. Το Multiprotocol Label Switching (MPLS) framework έχει αποδειχθεί ιδιαίτερα αποδοτική και αξιόπιστη λύση στο παραπάνω πρόβλημα. Αρχικά, είχε προταθεί ως το πεδίο λειτουργικότητας ελέγχου –control plane για συστήματα βασισμένα σε πλαίσια ή κυψέλες όπως ATM, Frame Relay, Ethernet, και Point–to–Point Protocol/High Level Data Link Control (PPP/HDLC). Μερικά χρόνια πρίν, προτάθηκαν διάφορες τυποποιήσεις για την χρησιμοποίηση του MPLS σαν μηχανισμός ελέγχου για τα οπτικά δίκτυα, όπως για παράδειγμα Multiprotocol Lambda Switching (MPLambdaS ή MPλS). Όλες αυτές οι διεργασίες οδήγησαν τελικά στην αναγκαστική πλέον μετάβαση στο Generalized MPLS (GMPLS).

Στη συγκεκριμένη θεματική ενότητα θα παρουσιάσουμε συνοπτικά έναν μεγάλης χωρητικότητας φωτονικό MPLS δρομολογητή **(HIKARI router)**, ο οποίος κάνει χρήση ενός εξειδικευμένου MPλS πρωτοκόλλου μαζί με ένα σχήμα με shared link–group constraints (SRLG), που καλείται weighted–SRLG (WSRLG).

Ο HIKARI δρομολογητής αποτελεί έναν multilayer router με ικανότητες μεταγωγής όχι μόνο σε Lambdas (LSC–Lambda Switching capability), αλλά και σε packet (PSC–Packet Switching capability). Είναι γνωστό οτι τα κλασσικά Optical Cross Connects διαθέτουν LSC ικανότητα μεταγωγής ή και FSC–Fiber Switching capability. Οι παραδοσιακοί MPLS δρομολογητές, από την άλλη, διαθέτουν μόνο την PSC λειτουργικότητα. Ο HIKARI router καταφέρνει και συνδυάζει και τις δύο τεχνικές μεταγωγής: LSC και PSC, και έτσι προσφέρει τα οφέλη τόσο της packet–switched τεχνολογίας όσο και της circuit–switched.

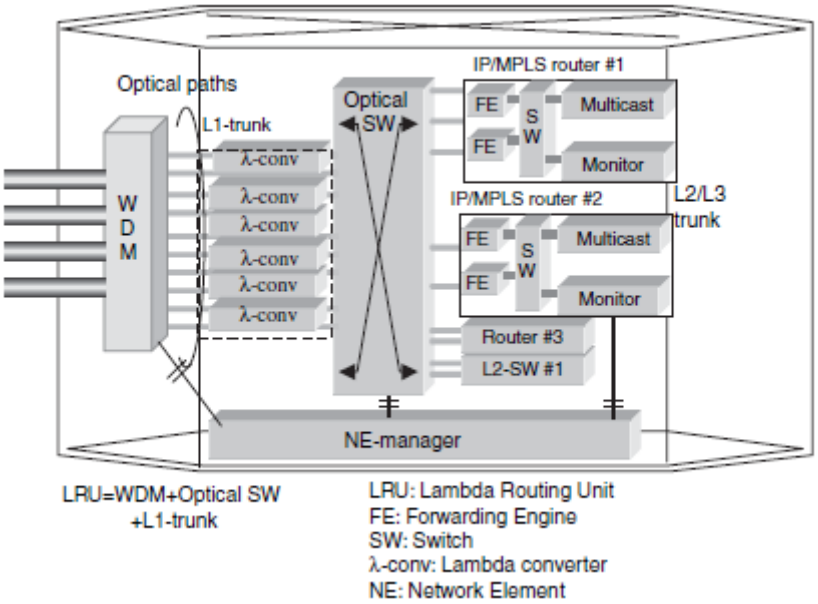
Ο συγκεκριμένος δρομολογητής εγκαθιδρύει IP δίκτυα πάνω σε οπτικά με κατανεμημένο έλεγχο. Μέσω της επικοινωνίας του με άλλους routers, κάθε HIKARI δρομολογητής ελέγχει το OLSP –OpticalLSP. Ο συγκεκριμένος δρομολογητής μπορεί να διαχειριστεί ταυτόχρονα τόσο τα LSPs όσο και τα OLSPs, επειδήτα πρώτα χειρίζονται από την PSC τεχνική μεταγωγής και τα δεύτερα από την LSC. Τα LSPs διασυνδέονται από OLSPs, ενώ ορισμένες φορές εμφανίζονται και ως σύνολο, σχηματίζοντας έτσι μια ιεραρχία μονοπατιών. Αναπτύσσοντας τα OLSPs, βελτιώνεται το throughput στα δίκτυα μέσω της εκμετάλλευσης της τεχνικής του cut–through.

Όπως φαίνεται και στην Εικόνα 98, ο HIKARI δρομολογητής αποτελείται από πέντε διακριτές μονάδες: ένα συστατικό WDM, ένα optical switch unit, ένα L1 trunk unit, ένα

L2/L3 trunk unit, καθώς και ένα network element manager (NE manager). Η μονάδα LRU (Lambda–routing unit) αποτελεί την ένωση των WDM, optical switch, και L1 trunk units. Η LRU μπορεί να κάνει μεταγωγή και add/drop τα OLSPs, ενώ η μετατροπή μήκους κύματος πραγματοποιείται από τις μονάδες λ–conv στα L1 trunks. Οι HIKARI δρομολογητές είναι σε θέση να ανταλλάξουν μηνύματα μέσω του optical–supervisory channel (OSC). Τα OSC και οπτικά μονοπάτια πολυπλέκονται στις WDM μονάδες. Ο NE διαχειριστής παρακολουθεί όλα τα κυκλώματα σε κάθε κόμβο, επιβλέπει απομακρυσμένους οπτικούς ενισχυτές σήματος, καταγράφει την ποιότητα των σημάτων, και διαχειρίζεται τα μονοπάτια.

Επιπλέον, τα L1 trunks μπορούν να αντικατασταθούν με λ–conv λειτουργίες, μονάδες ενίσχυσης και αναγέννησης σήματος, και οπτικής μεταγωγής. Τα L2/L3 trunks, από την άλλη, είναι σε θέση να αντικαθίστανται με λειτουργικότητες IP δρομολόγησης, MPLS δρομολόγησης, και layer–2 μεταγωγής . Τέλος, είναι εφικτό να τεθεί σε ισχύ ένα L3 packet forwarding, όταν βέβαια χρησιμοποιείται στη πράξη.

Εικόνα 98. Ο HIKARI δρομολογητής



Εικόνα 99. Λειτουργικές μονάδες του HIKARI δρομολογητή

Η Εικόνα 100 δείχνει τα χαρακτηριστικά του συγκεκριμένου φωτονικού router. Ο HIKARI δρομολογητής είναι ένα κατεξοχήν IP σύστημα δρομολόγησης. Έτσι, η τεχνικές επεξεργασίας πακέτων είναι και οι πιό σημαντικές. Η εμπορική έκδοση του router σχεδιάστηκε να επιτυγχάνει το μέγιστο χωρητικότητα 5 gigapackets per second (5 Gpps). Κάποια σύνολα των εισερχόμενων πακέτων επεξεργάζονται στα L3 trunks με PSC τεχνικές μεταγωγής, ενώ κάποια άλλα στην LRU μονάδα σε LSC βάση.

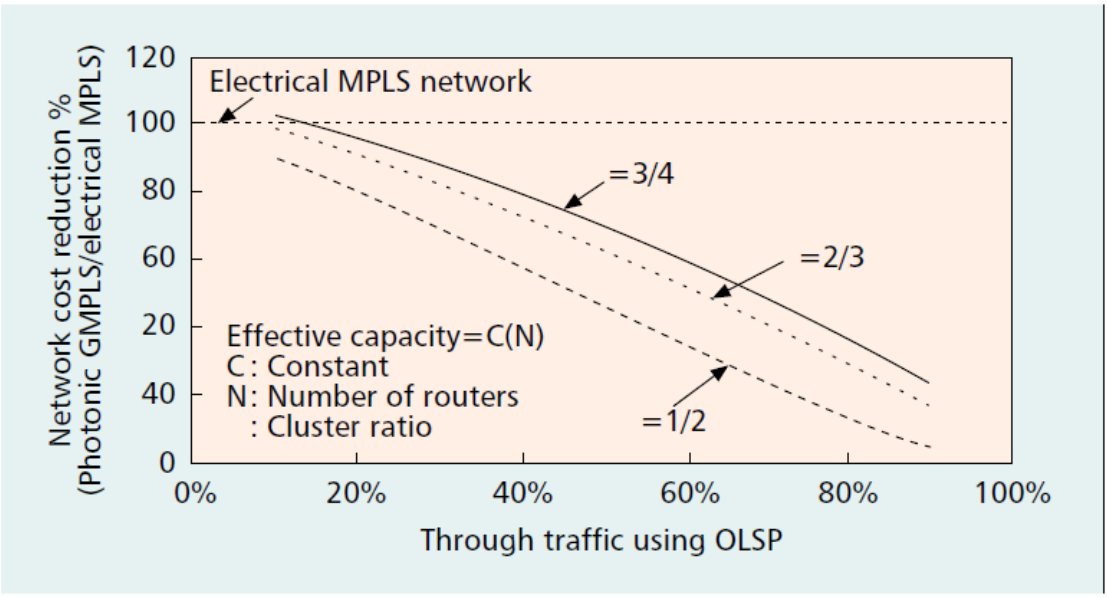
Η μονάδα LRU κάνει χρήση ενός ευφειούς, βασισμένου στην οπτική μεταγωγή, Optical Cross Connect, ο οποίος εγκαθιδρύει τόσο τα οπτικά μονοπάτια όσο και πραγματοποιεί επίσης τις διάφορες τεχνικές μεταγωγής. Η σχεδιαστική του φιλοσοφία είναι τέτοια που μειώνει το διαχειριστικό κόστος, την κατανάλωση ενέργειας και το ποσοστό αστοχιών. Η χωρητικότητα της μονάδας είναι 128 αμφίδρομα οπτικά μονοπάτια, με υποστηριζόμενο optical interface το SONET OC–48c. Έτσι η μέγιστη χωρητικότητα διαμεταγωγής φθάνει τα 640 Gbps. Εαν οι διεπαφές αυτές αναβαθμίζονταν σε OC–192c ή GbE, η χωρητικότητα θα άγγιζε τα 2. 56 Tbps.

Items	Specifications
Switch architecture	DC-SW scheme
Operating wavelength range	1550-nm band (C-band)
Optical channel speed	2.5 Gb/s (upgradable to 10 Gb/s)
Maximum number of wavelengths	32
Number of fiber ports	8 (maximum)
Cross-connection	256 channels
System throughput	640 Gb/s (upgradable to 2.56 Tb/s)
Modular unit	8 channels
Optical channel allocation	Even assignment on 50-GHz grid Anchored at 193.100 THz
Fiber type	Single-mode fiber (G.652 [9])
Optical supervisory channel (OSC)	OTS/OMS-OH [10] transport and high-speed DCC

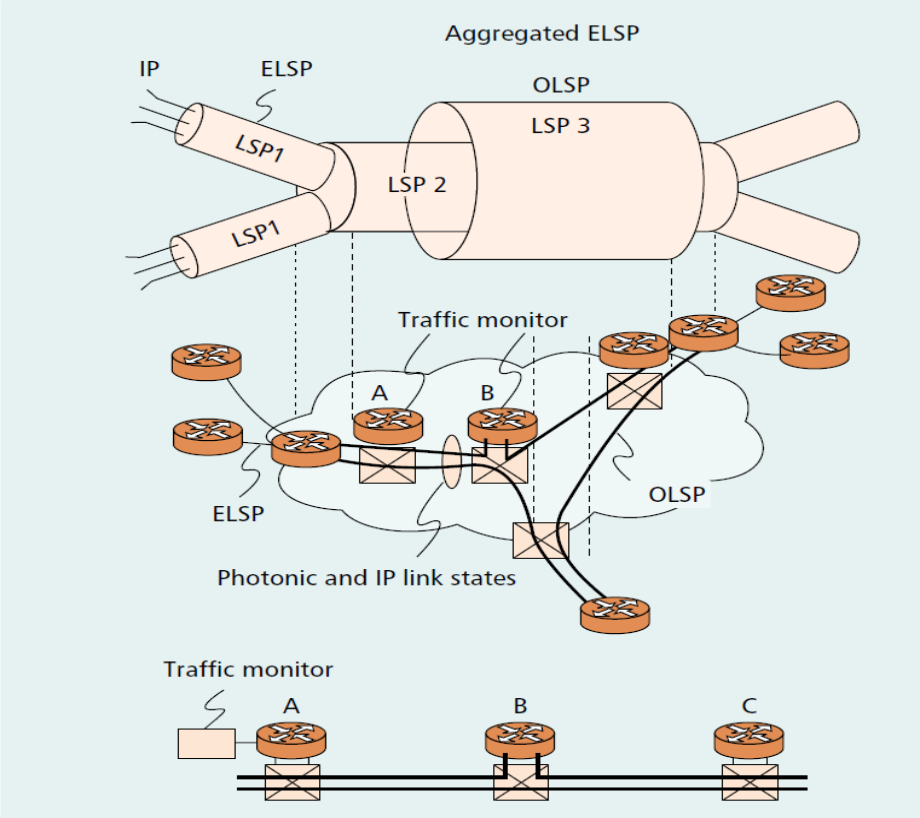
Εικόνα 100. Τα χαρακτηριστικά του HIKARI δρομολογητή

Το υποστηριζόμενο optical–channel (Och) frame format ήταν μέχρι πρώτινος ένα τροποποιημένο SDH G. 707 frame. Το συγκεκριμένο θα αλλάξει σε OTN G. 709 frame. Το Optical supervisory channel (OSC) μεταφέρει το επιπλεόν φορτίο –overhead της οπτικής μεταφοράς (OTS–OH), της μονάδας οπτικής πολυπλεξίας (OMS–OH), καθώς και ένα υψηλής ταχύτητας κανάλι μετάδοσης δεδομένων (DCC). Το τμήμα επιπλέον φορτίου του OSC χρησιμοποιείται για το DCC. Τα OTS–OH και OMS–OH χρησιμοποιούνται για να διαχειριστούν WDM γραμμές. Το DCC χρησιμοποιείται ως κανάλι διαχείρισης δικτύου και MPλS κανάλι σηματοδοσίας.

Η μονάδα διαχείρισης NE από την άλλη είναι υπεύθυνη για τον έλεγχο και καταγραφή των διαφόρων στοιχείων υλισμικού, και πραγματοποιεί την επικοινωνία ανάμεσα σε άλλα NEs ώστε να ανταλλάξει MPλS μηνύματα σηματοδοσίας, μέσω του CR–LDP πρωτοκόλλου, και OA&M μηνύματα. Συνήθως, το SNMP –Simple Network Management Protocol χρησιμοποιείται για την διαχείριση των HIKARI δρομολογητών.

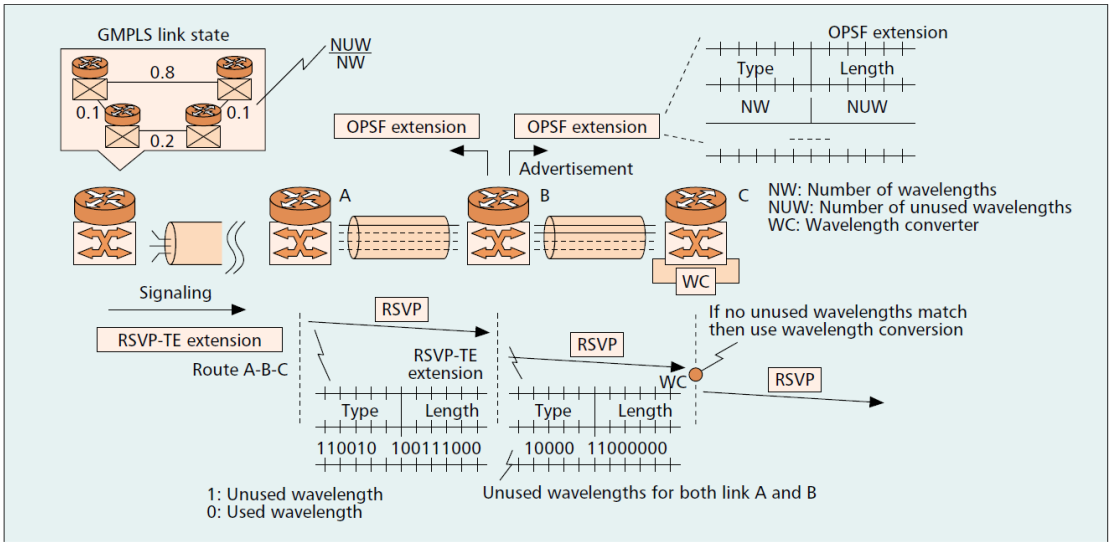


Εικόνα 101. Τα οφέλη της χρησιμοποίησης της τεχνικής cut–through για εγκατάσταση μονοπατιού

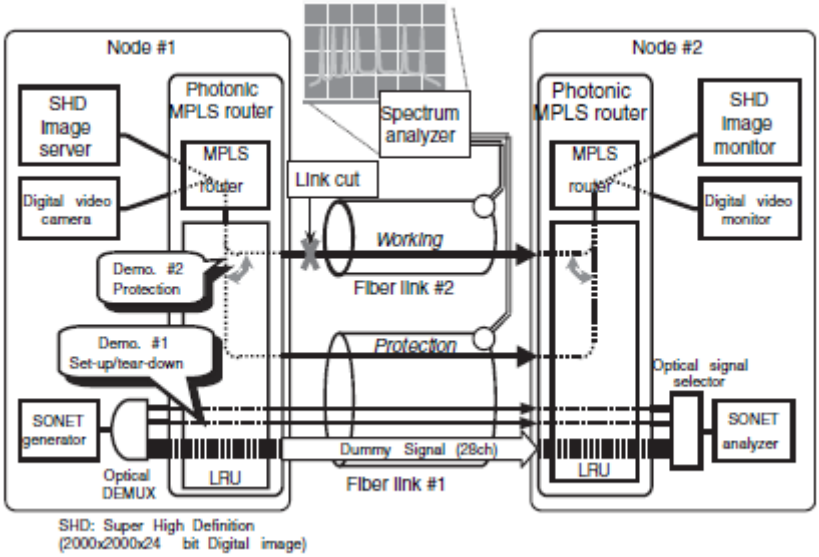


Εικόνα 102. Εγκαθίδρυση μονοπατιού με τη τεχνική του cut–through

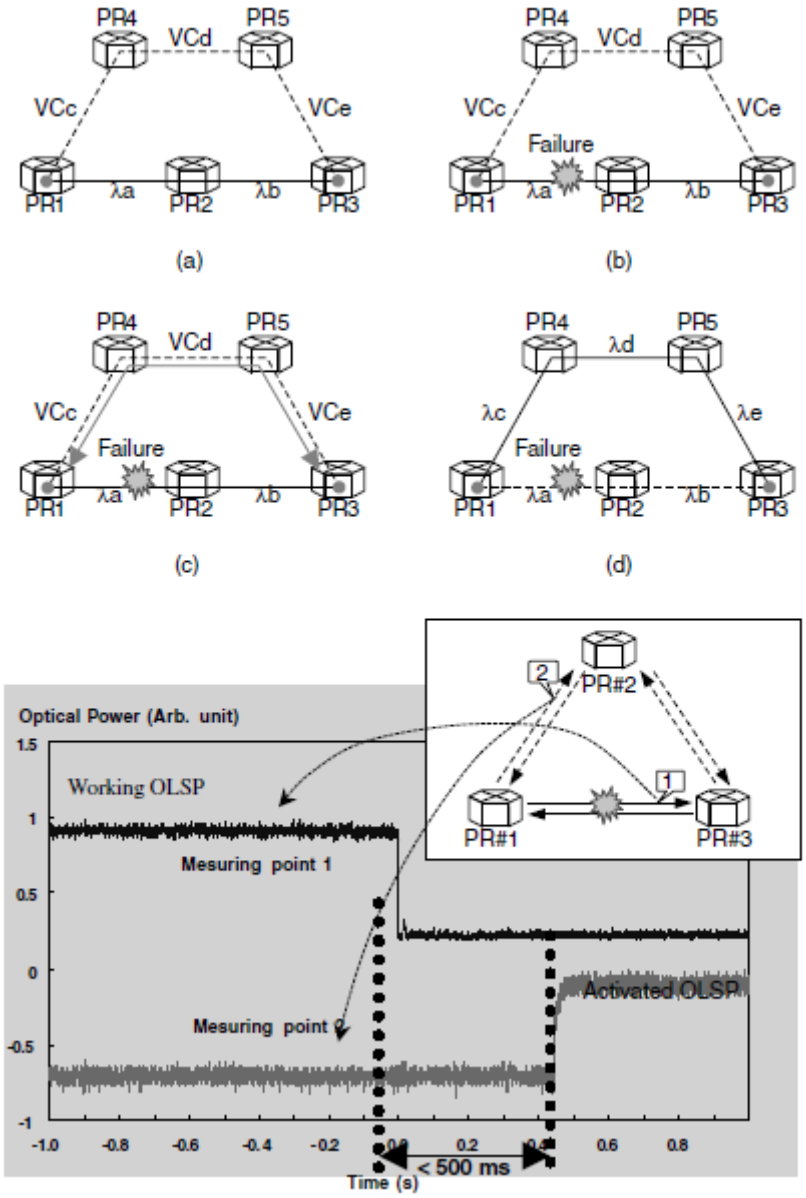
Το OLSP πεδίο λειτουργικότητας ελέγχου –control plane ενός HIKARI router βασίζεται στο CR–LDP πρωτόκολλο με κατάλληλες επεκτάσεις για επίβλεψη οπτικών δικτύων. Στην εκτεταμένη αυτή έκδοση, τα LSPs μεταχειρίζονται ως αμφίδρομα μονοπάτια, κατά την αλληλεπίδρασή τους με τα OLSPs. Ο δρομολογητής HIKARI προσφέρει αρκετούς τύπους προστασίας και επανάκαμψης από αστοχίες, κάνοντας χρήση 1+1 προστασίας, 1:1 προστασίας, ανάκαμψης –restoration ή και καμίας. Για την επίτευξη ταχείας αποκατάστασης μετά από βλάβη στο δίκτυο, γίνεται χρήση ενός disjoint–path–selection αλγορίθμου, του WSRLG σχήματος. Στην Εικόνα 105 διακρίνουμε την όλη διαδικασία επανάκαμψης σε επίπεδο πραγματικού σεναρίου, μετά από αστοχία συνδέσμου.



Εικόνα 103. Επεκτάσεις σηματοδοσίας στο CR–LDP πρωτόκολλο για το OLSP control plane



Εικόνα 104. Τυπική συνδεσμολογία HIKARI δρομολογητών



Εικόνα 105. Η πλήρης διαδικασία αποκατάστασης (a) – (d) και πειραματικές μετρήσεις

3.5.1 GMPLS ΚΑΙ GN3

Το σύστημα **AutoBAHN –Automated Bandwidth Allocation across Heterogeneous Networks** προσφέρει την κατάλληλη διεπαφή για την εγκατάσταση δυναμικών κυκλωμάτων πάνω σε παγκόσμιες ερευνητικές και ακαδημαικές δικτυακές υποδομές. Το όλο σύστημα έχει αναπτυχθεί ως πιλοτικό στα πλαίσια του GN2 project. Η δυναμική επίβλεψη κυκλωμάτων είναι κυρίαρχο ζήτημα στις προσπάθειες ανάπτυξης του δικτύου επόμενης γενιάς GEANT2, χρησιμοποιώντας τεχνολογίες μεταφοράς που παρέχουν νέες υπηρεσίες σε συνδυασμό με IP based services (AutoBAHN). Στη παρούσα θεματική ενότητα θα περιγράψουμε τις επεκτάσεις και προσθήκες που σχεδιάζονται για το AutoBAHN σύστημα κατά την διάρκεια του κύκλου ζωής του GN3 project.

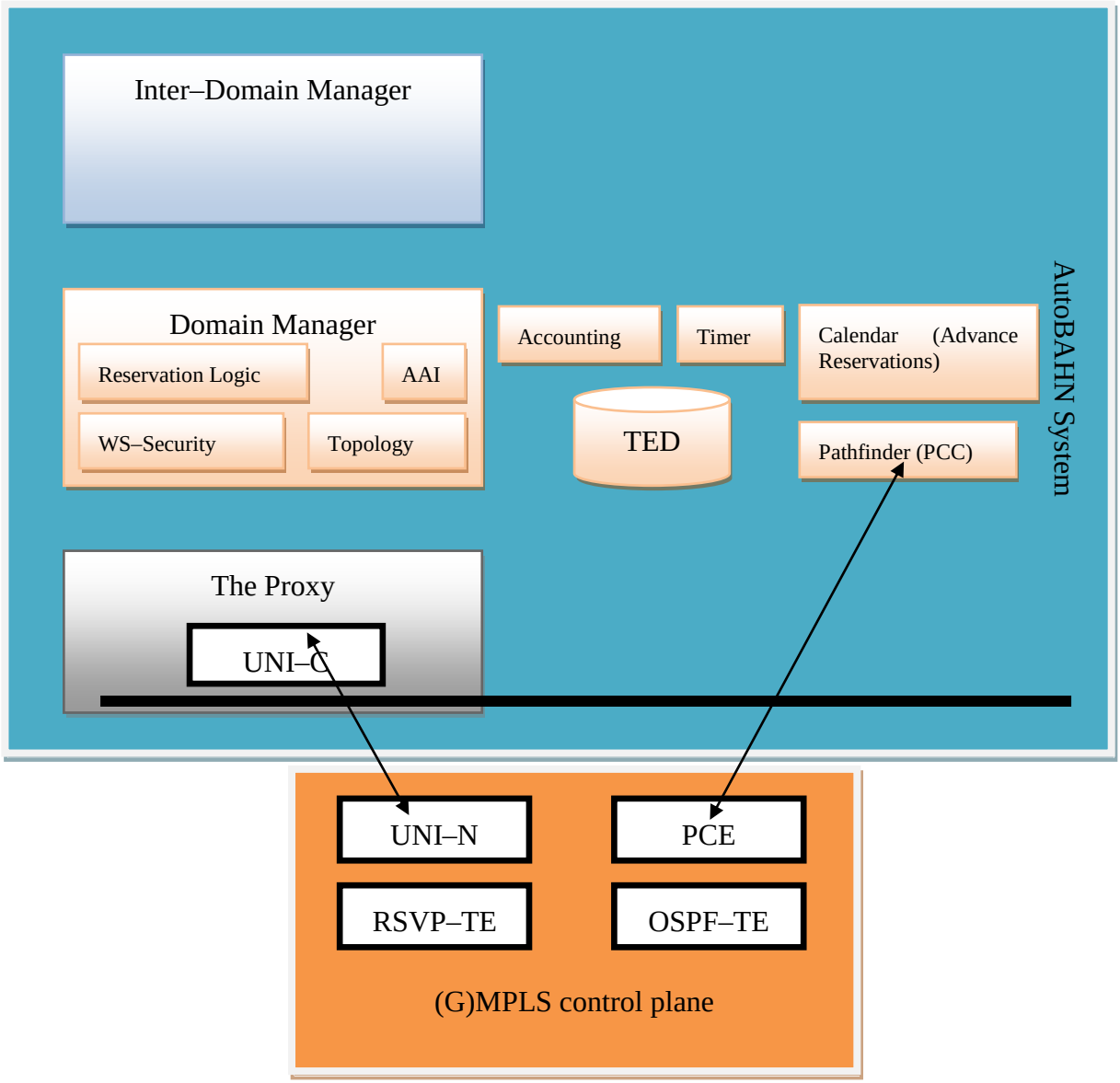
Το AutoBAHN μπορεί να αλληλεπιδρά με ένα GMPLS δίκτυο κάνοντας χρήση ενός επικαλυπτόμενου –overlay ή ομότιμου –peer μοντέλου. Στο overlay μοντέλο, το επίπεδο ορατότητας του δικτύου περιορίζεται σε όρους τοπολογίας ή χρήσης πόρων, και έτσι διαφορετικοί μηχανισμοί θα πρέπει να υλοποιούνται για την υποστήριξη των προχωρημένων λειτουργιών στο GMPLS. Από την άλλη, ένα peer μοντέλο θα επέτρεπε στο AutoBAHN να γίνει μέρος του GMPLS Signaling Communication network (SCN) και να διαμοιράζεται την όλη πληροφορία πόρων μέσω της υλοποίησης των πρωτοκόλλων σηματοδοσίας και δρομολόγησης του AutoBAHN/GMPLS δικτύου. Το επικαλυπτόμενο μοντέλο θεωρείται πιό ασφαλές από το ομότιμο καθώς δεν εκθέτει την εσωτερική του τοπολογία, και έτσι διασφαλίζει την ιδιωτικότητα και αξιοπιστία. Ωστόσο αυτό έχει το μοιονέκτημα της χαμηλότερης ευελιξίας. Στην Εικόνα 106 διακρίνουμε την συνολική αρχιτεκτονική του Overlay μοντέλου συμπεριλαμβανομένου και του GMPLS control plane και AutoBAHN.

Το GMPLS κάνει χρήση ενός δυναμικού link–state IGP πρωτοκόλλου δρομολόγησης ώστε να πλημμυρίσει το όλο δίκτυο με πληροφορίες για τους κόμβους και γραμμές. Αυτή η πληροφορία συλλέγεται από όλους τους hops ώστε να χτιστεί αυτό που αποκαλούμε Traffic Engineering Database (TED). Αυτή η βάση δεδομένων είναι ουσιαστικά η όλη πληροφορία τοπολογίας που περιλαμβάνει τις παραμέτρους κατάστασης όπως για παράδειγμα τη διαθεσιμότητα ή και την χρησιμοποίηση του εύρους ζώνης. Στο GMPLS , κάθε εμπλεκόμενος κόμβος αναπτύσσει ένα στιγμιότυπο του εκάστοτε πρωτοκόλλου δρομολόγησης ώστε να ανταλλάξει πληροφορία δρομολόγησης. Για παράδειγμα το OSPF–TE κάνει χρήση link state advertisements γι'αυτό το σκοπό.

Στο Overlay μοντέλο, η πληροφορία δρομολόγησης πρέπει να παραμετροποιείται χειρωνακτικά στο AutoBAHN και να ανανεώνεται ανάλογα με τις αλλαγές της τοπολογίας. Δύο περιπτώσεις διακρίνουμε εδω:

- Edge + Border: Το AutoBAHN παραμετροποιείται με τα edge και border σημεία του GMPLS δικτύου. Με αυτό το τρόπο το όλο δίκτυο μπορεί να ειδωθεί ως ένα νέφος δικτύου με σημεία εισόδου και εξόδου (ingress και egress). Σε αυτή τη περίπτωση το GMPLS σύννεφο θεωρείται fully meshed.
- Full topology: Το AutoBAHN παραμετροποιείται με την πλήρη τοπολογία του GMPLS δικτύου ώστε να έχει πλήρη εικόνα όλων των κόμβων και συνδέσμων.

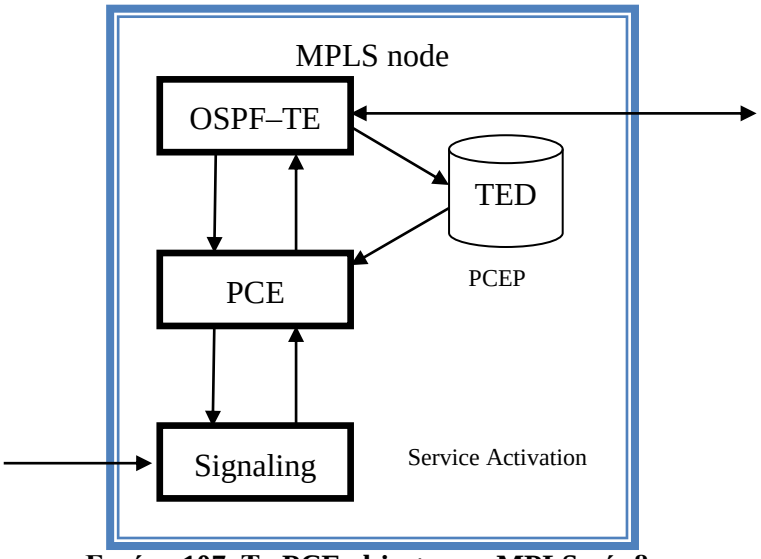
Η αναζήτηση μονοπατιού –Path finding στο ASON πραγματοποιείται από τον ελεγκτή δρομολόγησης –routing controller. Στα πλαίσια του IETF ένα Path Computation Element (PCE) είναι υπεύθυνο για την υλοποίηση ενός αλγορίθμου δρομολόγησης (RWA) και για τον καθορισμό του βέλτιστου μονοπατιού βάσει κάποιων παραμέτρων εισόδου όπως προέλευση, προορισμός, εύρος ζώνης και άλλα constraints. Η αίτηση φθάνει από τον Path Computation Client (PCC), που υλοποιείται συνήθως στον Connection Controller (CC) και μετά επεξεργάζεται στο PCE. Πολλαπλά ή μόνο ένα PCE μπορούν να αναπτύσσονται σε ένα GMPLS δίκτυο, αλλά όλα αυτά τα στιγμιότυπα είναι υποχρεωμένα να προσπελαύνουν ένα ενημερωμένο TED, από πληροφορίες πόρων δικτύου. Ανάλογα με την εκάστοτε αρχιτεκτονική και το επίπεδο πληροφορίας διαθέσιμο σε κάθε PCE , ένας ή και περισσότεροι PCEs συμμετέχουν στον καθορισμό μονοπατιού. Η ακριβής θέση των PCEs καθορίζεται σε συνάρτηση με τα υπόλοιπα PCCs.



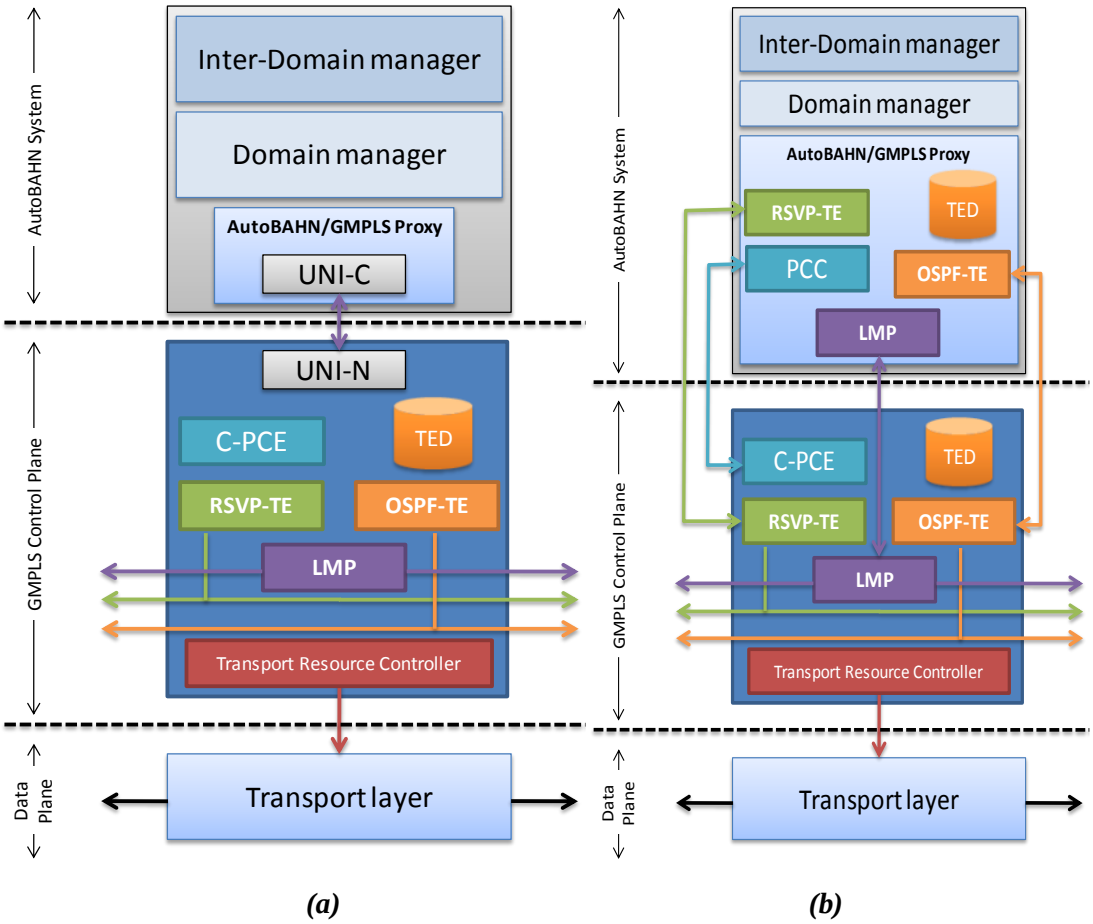
Εικόνα 106. Η αρχιτεκτονική του Επικαλυπτόμενου –Overlay μοντέλου

— Στο επικαλυπτόμενο μοντέλο, η αναζήτηση μονοπατιού πραγμοτεποιείται σε ένα PCE μέσα στο GMPLS νέφος καθώς το OIF UNI δεν επιτρέπει την σηματοδοσία ενός Explicit μονοπατιού.

— Στο ομότιμο μοντέλο, το AutoBAHN/GMPLS θα μπορούσε να υλοποιήσει ένα PCC να επικοινωνεί με το διαθέσιμο PCE στο GMPLS δίκτυο ή να χρησιμοποιήσει το TED για τον καθορισμό του μονοπατιού. Αφότου υπολογιστεί το μονοπάτι, η αίτηση σηματοδοσίας που περιλαμβάνει το καθορισμένο μονοπάτι στο Explicit Route Object (ERO), προωθείται μέσω του RSVP πρωτοκόλλου.



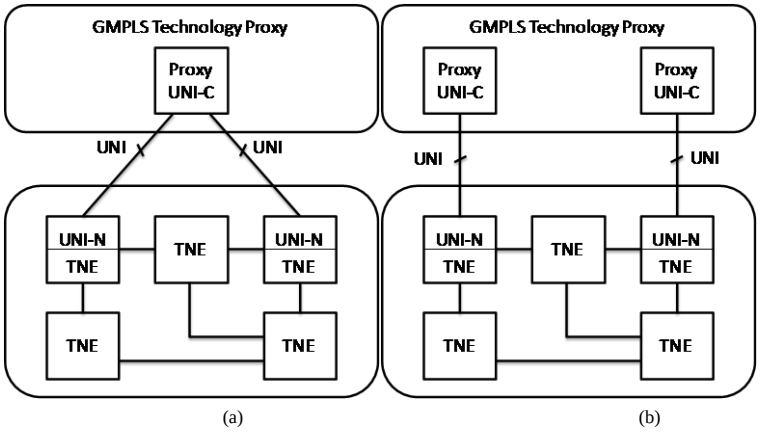
Εικόνα 107. Το PCE object στον MPLS κόμβο



Εικόνα 108. (a) Αρχιτεκτονική Overlay (b) Αρχιτεκτονική Peer

Το OIF UNI (User–Network Interface) υποστηρίζει διάφορες ετερογενείς λειτουργικότητες πάνω στην διεπαφή αυτή. Για τον σχεδιασμό του AutoBAHN GMPLS proxy οι πιο χαρακτηριστικές συνδέονται με την εγκαθίδρυση των συνδέσεων, την διαγραφή τους και τις διαδικασίες ανταλλαγής καταστάσεων και σηματοδοσίας. Το OIF UNI υποστηρίζει επίσης λειτουργίες αυτοανίχνευσης των δυνατοτήτων του δικτύου. Τα δύο ουσιαστικά σημεία του UNI είναι τα UNI–C και UNI–N. Το UNI–C ανήκει στην συσκευή του πελάτη και το UNI–N εγκαθίσταται στο Transport Network Element (TNE). Η UNI σηματοδοσία υποστηρίζει διαφορετικούς τύπους συνδέσεων όπως SONET/SDH, OTN ή Ethernet.

Το κανάλι μέσα από το οποίο μεταφέρονται τα μηνύματα σηματοδοσίας μεταξύ των UNI–C και UNI–N είναι το κανάλι ελέγχου. Το κανάλι ελέγχου μπορεί να είναι in–fiber (ίδια γραμμή με το κανάλι δεδομένων), ή out–fiber (dedicated γραμμή). Η τεχνολογία GMPLS οφείλει να κάνει χρήση μιας out–of–fiber προσέγγισης εαν πρόκειται να υλοποιηθεί στο AutoBAHN σύστημα.



Εικόνα 109. GMPLS τεχνολογικές προεσεγγίσεις στο OIF UNI

Αναφορικά με την διευθυνσιοδότηση, τα UNI–C και UNI–N πρέπει να διαθέτουν ένα Node identifier ώστε να αναγνωρίζουν τα τερματικά σημεία της UNI control plane συνόδου. Ένα Transport Network Address (TNA), που ανατίθεται σε ένα ή περισσότερα data links, τίθεται στα τερματικά σημεία της σύνδεσης και πρέπει να είναι καθολικά μοναδική διεύθυνση. Για την αναγνώριση ξεχωριστών συνδέσμων δεδομένων μέσα σε ένα TNA , δύο Logical Port identifiers χρησιμοποιούνται και είναι μοναδικοί στον κόμβο.

Τέλος, το OIF UNI καθορίζει αφαιρετικά μηνύματα για τους βασικότερους μηχανισμούς σηματοδοσίας οι οποίοι μπορούν να υλοποιηθούν με τα RSVP ή LDP πρωτόκολλα. Για το AutoBAHN σύστημα θα θεωρήσουμε ως κυρίαρχο το RSVP.

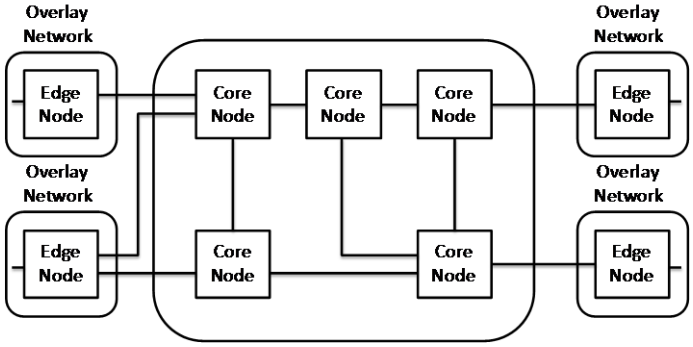
Message No.	Abstract Message Description	Message Direction	RSVP Message
1	Connection Create Request	UNI–C→UNI–N & UNI–N→UNI–C	Path
2	Connection Create Response	UNI–N→UNI–C & UNI–C→UNI–N	Resv, PathErr
3	Connection Create Confirmation	UNI–C→UNI–N & UNI–N→UNI–C	ResvConf

4	Connection Delete Request	UNI–C→UNI–N & UNI–N→UNI–C	Path or Resv with ADMIN_STATUS bit
5	Connection Delete Response	UNI–N→UNI–C & UNI–C→UNI–N	PathErr with Path_State_Removed flag, PathTear
6	Connection Status Enquiry	UNI–C→UNI–N & UNI–N→UNI–C	Implicit
7	Connection Status Response	UNI–N→UNI–C & UNI–N→UNI–C	Implicit
8	Notification	UNI–N→UNI–C	PathErr, ResvErr

Εικόνα 110. OIF UNI αφαιρετικά μηνύματα

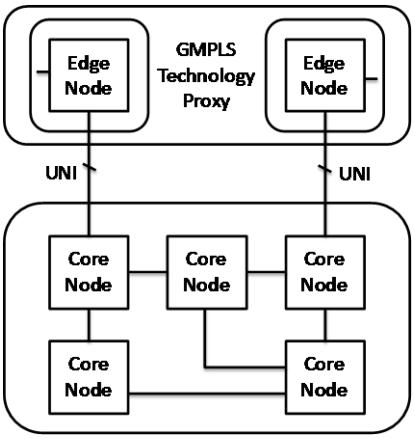
Είναι σημαντικό να τονίσουμε οτι τα Connection Status μηνύματα βασίζονται στο RSVP πρωτόκολλο μέσω περιοδικής ανταλλαγής refresh μηνυμάτων.

Το GMPLS IETF UNI, από την άλλη, αναφέρεται στην διεπαφή μεταξύ του επικαλυπτόμενου δικτύου και του δικτύου κορμού. Σε αυτή τη περίπτωση, ο κόμβος με ένα TE–Link στο δίκτυο κορμού είναι ο **edge node**, ενώ ο κόμβος στην άλλη πλευρά του TE συνδέσμου είναι ο **core node**.



Εικόνα 111. GMPLS IETF UNI μοντέλο

Με αυτή τη λογική, η τεχνολογία AutoBAHN θα αναπαρίστανε κανονικά τους ακραίους κόμβους προέλευσης και προορισμού, ενώ ο κόμβος στο GMPLS δίκτυο στον οποίο συνδέεται θα αποτελούσε έναν κόμβο κορμού –core node. Το επικαλυπτόμενο μοντέλο όπως καθορίζεται από το ASON απαιτεί διαχωρισμό ανάμεσα στην UNI και NNI σηματοδοσία. Το GMPLS UNI , αντίθετα, επιτρέπει την διατήρηση της ίδιας συνόδου ανάμεσα στα NNI, **εαν και μόνο εαν** τα UNI και NNI είναι GMPLS RSVP–based.



Εικόνα 112. Αρχιτεκτονική GMPLS IETF UNI

Η διευθυνσιοδότηση ανάμεσα σε έναν ακραίο κόμβο και έναν κόμβο κορμού θα πρέπει να ανήκει στο ίδιο address space. Εαν ένας edge node συνδέεται με τον core node μέσω ενός ή περισσοτέρων συνδέσμων, κάθε ένας από αυτούς ανατίθεται έναν TE Link identifier. Για τη δημιουργία της σύνδεσης, ένα Path μήνυμα αποστέλλεται από τον edge node στον core node, ενώ για τη διαγραφή της σύνδεσης ένα PathTear ή PathErr μήνυμα με την Path_State_Removed σημαία μπορεί να χρησιμοποιηθεί.

Το πρωτόκολλο που ενεργοποιεί την επικοινωνίας ανάμεσα στα PCC και PCE καλείται Path Computation Element Communication Protocol [RFC 5440]. Πριν ένα PCC απαιτήσει καθορισμό μονοπατιού από το PCE, μια σύνοδος ανάμεσα σε αυτά τα δύο πρέπει να εγκαθιδρυθεί. Το OPEN object [RFC 5440, 7. 3] χρησιμοποιείται γι'αυτό το σκοπό. Είναι σκόπιμο να γνωρίζουμε οτι οι PCEP σύνοδοι μπορούν να εγκαθιδρύονται και να διατηρούνται ενεργές καθώς και να αποδεσμεύονται κατα απαίτηση. Εαν απαιτήσουμε μόνιμες συνδέσεις με ένα PCE, η διασφάλιση της PCEP ενεργής κατάστασης θα απαιτούσε μια περιοδική αποστολή KeepAlive μηνυμάτων. Για την αποδέσμευση των συνόδων ένα CLOSE object αποστέλλεται.

Το PCEP είναι ένα αμφίδρομο πρωτόκολλο κάτι που σημαίνει οτι το PCC όχι μόνο μπορεί να αποστέλλει αιτήσεις αλλά και να λαμβάνει ειδοποιήσεις διαφόρων γεγονότων, όπως PCC ακυρώσεις υπολογισμού μονοπατιών αλλά και επιβεβαιώσεις. Το NOTIFICATION object χρησιμοποιείται για να μεταφέρει αυτό το τύπο πληροφορίας.

Το PCE διαθέτει ένα πολύ ισχυρό σύνολο χαρακτηριστικών όταν πρόκειται για καθορισμό μονοπατιού με δεσμεύσεις. Απλές ή πολλαπλές εντολές υπολογισμού μονοπατιού καθορίζονται στο PCReq μήνυμα, και τα διάφορα constraints μπορεί να αποτελούνται από:

- **Endpoints**
- **LSP attributes**
- **Bandwidth**
- **Μετρικές**
- **Καταγεγραμμένο Route Object**
- **Συμπεριλαμβανομένο Route Object**
- **Load balancing**
- **SVEC**

Η ανθεκτικότητα –Resiliency αποτελεί την ικανότητα επιβίωσης απέναντι σε δικτυακές αστοχίες. Οφείλει να περιλαμβάνει και κάποια λειτουργικότητα ώστε να παρέχεται αδιάκοπτη συνέχεια στην υπηρεσία σε βαθμό που είναι διαφανής στους χρήστες. Ας δούμε τα υποστηριζόμενα επίπεδα προστασίας στα δύο αυτά UNIs.

Στη περίπτωση του OIF UNI ο όλος μηχανισμός ικανότητας αντοχής σε βλάβες δεν μπορεί να κληθεί άμεσα από το συγκεκριμένο interface. Γι'αυτό το λόγο το σύστημα AutoBAHN θα πρέπει να βασιστεί σε άλλους τρόπους ανίχνευσης αστοχιών στο δίκτυο, ώστε σε περίπτωση βλάβης το σύστημα να επανακαθορίσει τους διαθέσιμους πόρους που έχουν επηρεαστεί. Το αντικείμενο RP (Request Parameters) που ενθυλακώνεται στο PCReq object υποδυκνείει τον επιθυμητό τύπο προστασίας και αποκατάστασης.

Στο IETF UNI οι διάφορες αστοχίες ανιχνεύονται και απομονώνονται, ενώ ειδοποιήσεις παραδίδονται μέσω του IETF UNI (RSVP Notify), η κίνηση μεταγάγεται αυτόματα και ξανατρέχει πάλι κανονικά. Για την αναγνώριση των μονοπατιών που επιλέγονται μετά από μια αποκατάσταση, το PCC θα μπορούσε να εκδώσει ένα PCReq μήνυμα με το Synchronization sub–object (SVEC) στο PCE.

ΚΕΦΑΛΑΙΟ 4: ΜΕΛΛΟΝΤΙΚΗ ΕΞΕΛΙΞΗ ΤΟΥ GMPLS ΚΑΙ ΑΝΤΑΓΩΝΙΣΤΕΣ

4.1 ASON – ASTN

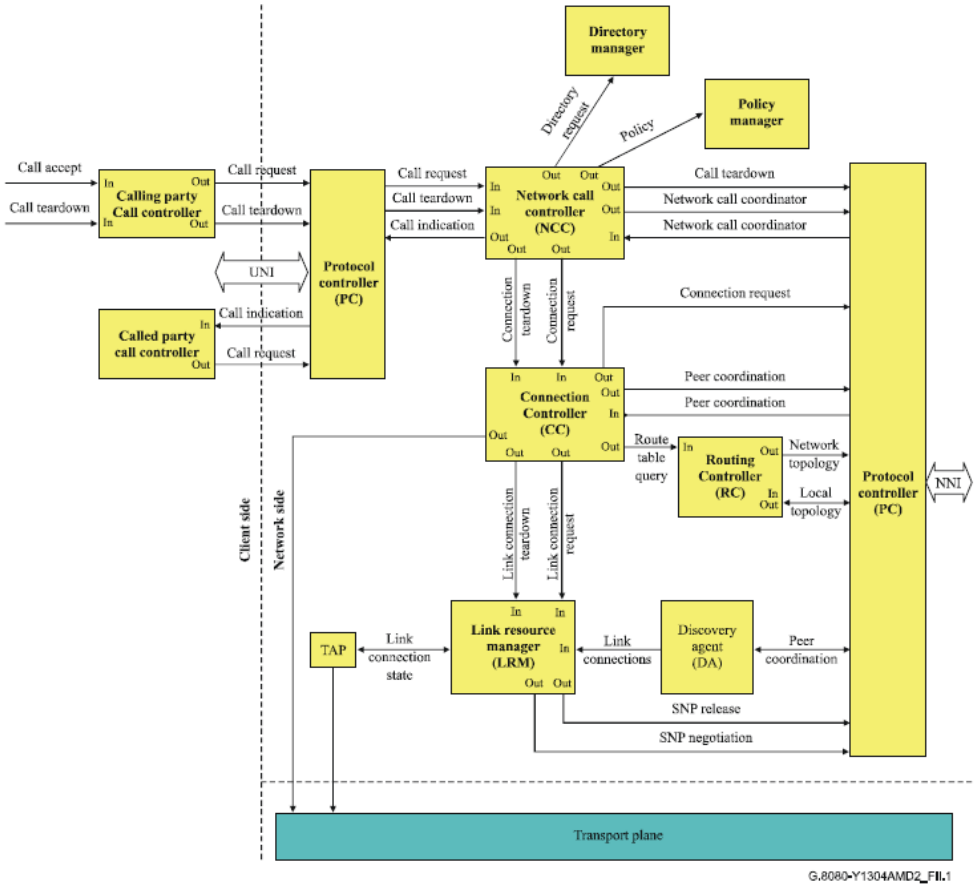
Το **ASTN (Automatic Switched Transport Network)** framework επιτρέπει στα μονοπάτια κίνησης να εγκαθιδρύονται μέσω ενός switched δικτύου αυτόματα. Ο όρος ASTN αντικαθιστά τον **ASON (Automatically Switched Optical Network)** και χρησιμοποιείται εναλλακτικά με το GMPLS. Αυτό ωστόσο δεν είναι απόλυτα σωστό διότι το GMPLS είναι σουίτα πρωτοκόλλων, ενώ το ASON/ASTN αποτελεί μια αρχιτεκτονική οπτικής μεταφοράς. Οι διάφορες απαιτήσεις της αρχιτεκτονικής αυτής μπορούν να ικανοποιηθούν χρησιμοποιώντας τα GMPLS πρωτόκολλα όπως αυτά έχουν τυποποιηθεί από την IETF και ITU. Επιπλέον, τα GMPLS πρωτόκολλα είναι εφαρμόσιμα τόσο σε οπτικά όσο και σε μη οπτικά δίκτυα μεταφοράς (packet, frame κ. τ. π.), και έτσι το GMPLS αποτελεί μια γενικότερη αντίληψη από το ASTN.

Παραδοσιακά, η δημιουργία μονοπατιών κίνησης μέσω ενός συνόλου από στοιχεία δικτύου έχει συμπεριλάβει την παραμετροποίηση ξεχωριστών Optical Cross–Connects σε καθένα από αυτά. Το ASTN επιτρέπει σε ένα χρήστη να καθορίσει το αρχικό σημείο, τελικό σημείο και απαιτούμενο εύρος ζώνης, και ο ASTN agent στα διάφορα στοιχεία δικτύου θα κατανείμει το path, θα το επιβλέψει, θα κάνει δέσμευση πόρων και εύρους ζώνης κατ'απαίτηση. Το πραγματικό μονοπάτι στο δίκτυο δεν θα είναι επιλεγμένο από το τελικό χρήστη. Οι διάφορες αλλαγές στο δίκτυο (προσθήκη/κατάρρευση κόμβων ή συνδέσμων) θα λαμβάνουν νόημα από τους Agents αλλά όχι από τον χρήστη. Με αυτόν τον τρόπο προσφέρεται ευελιξία στο δίκτυο και μεγαλύτερη αξιοπιστία.

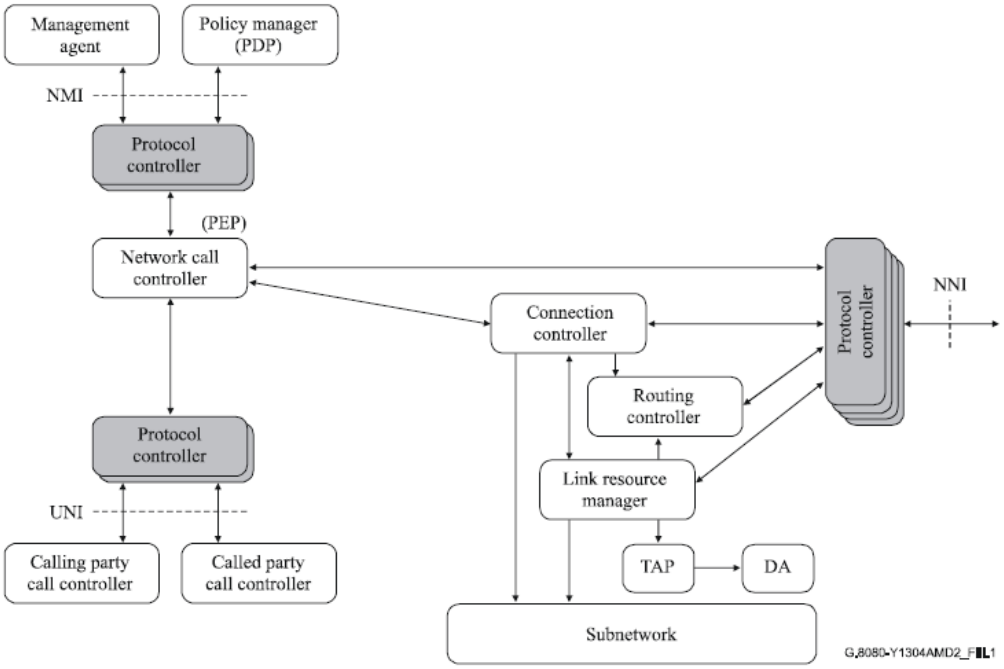
Διακρίνουμε τις ακόλουθες αρχιτεκτονικές απαιτήσεις για το ASON/ASTN από την ITU–T:

- **G. 8080/Y. 1304**, Architecture for the automatically switched optical network (ASON)
- **G. 807/Y. 1302**, Requirements for automatic switched transport networks (ASTN) Call and Connection Management
- **G. 7713/Y. 1704**, Distributed call and connection management (DCM)
- **G. 7713. 1/Y. 1704. 1**, DCM signaling mechanism using PNNI/Q. 2931
- **G. 7713. 2/Y. 1704. 2**, DCM signaling mechanism using GMPLS RSVP–TE
- **G. 7713. 3/Y. 1704. 3**, DCM signaling mechanism using GMPLS CR–LDP Discovery and Link Management
- **G. 7714/Y. 1705**, Generalized automatic discovery techniques
- **G. 7715/Y. 1706**, Architecture and requirements of routing for automatic switched transport network
- **G. 7716/Y. 1707**, Architecture and requirements of link resource management for automatically switched transport networks
- **G. 7717/Y. 1708**, ASTN connection admission control. Other Related Recommendations
- **G. 872**, Architecture of optical transport networks
- **G. 709/Y. 1331**, Interface for the optical transport network (OTN)
- **G. 959. 1**, Optical transport network physical layer interfaces
- **G. 874**, Management aspects of the optical transport network element
- **G. 874. 1**, Optical transport network (OTN) protocol neutral management information model for the network element view.
- **G. 875**, Optical transport network (OTN) management information model for the network element view
- **G. 7041/Y. 1303**, Generic framing procedure (GFP)
- **G. 7042/Y. 1305**, Link capacity adjustment scheme (LCAS) for virtual concatenated signals
- **G. 65x**, series on optical fiber cables and test methods

- **G. 693**, Optical interfaces for intra–office systems
- **G. 7710/Y. 1701**, Common equipment management function requirements
- **G. 7712/Y. 1703**, Architecture and specification of data communication network.
- **G. 806**, Characteristics of transport equipment. Description methodology and generic functionality. [1]



Εικόνα 113. Παράδειγμα διασύνδεσης των συστατικών δικτύου ASON



Εικόνα 114. Το ASON/ASTN Control Plane

Ως γνωστόν τα οπτικά δίκτυα κορμού, βασισμένα σε SDH/SONET και WDM τεχνολογίες, είναι σχεδιασμένα κυρίως για εφαρμογές φωνής και δεν καλύπτουν τις σύγχρονες απαιτήσεις της ραγδαίας αύξησης της κίνησης χρηστών. Οι διαθέσιμοι πόροι δεν μπορούν να κατανεμηθούν σωστά εξαιτίας της έλλειψης ευελιξίας ή και της μη αυτόματης επίβλεψης μεγάλης κλίμακας οπτικών δικτύων. Το πρόβλημα αυτό μπορεί να λυθεί μέσω της χρήσης ενός πεδίου λειτουργικότητας ελέγχου που πραγματοποιεί τις λειτουργίες ελέγχου κλήσης και σύνδεσης σε πραγματικό χρόνο. Μια από τις πιό πολλά υποσχόμενες λύσεις είναι η αντίληψη του ASON δικτύου με την ικανότητά του για δυναμική επίβλεψη του control plane.

Τα σύγχρονα οπτικά δίκτυα, παρώτι προσφέρουν τεράστια χωρητικότητα εύρους ζώνης, είναι μη ευέλικτα σε σύγκριση με τους IP ανταγωνιστές τους. Οι περισσότεροι περιορισμοί τους οφείλονται στο γεγονός οτι διαχειρίζονται μη αυτόματα ή από εξαιρετικά αργά συστήματα διαχείρισης. Τα κυριότερα προβλήματα που συναντάμε στα οπτικά δίκτυα είναι:

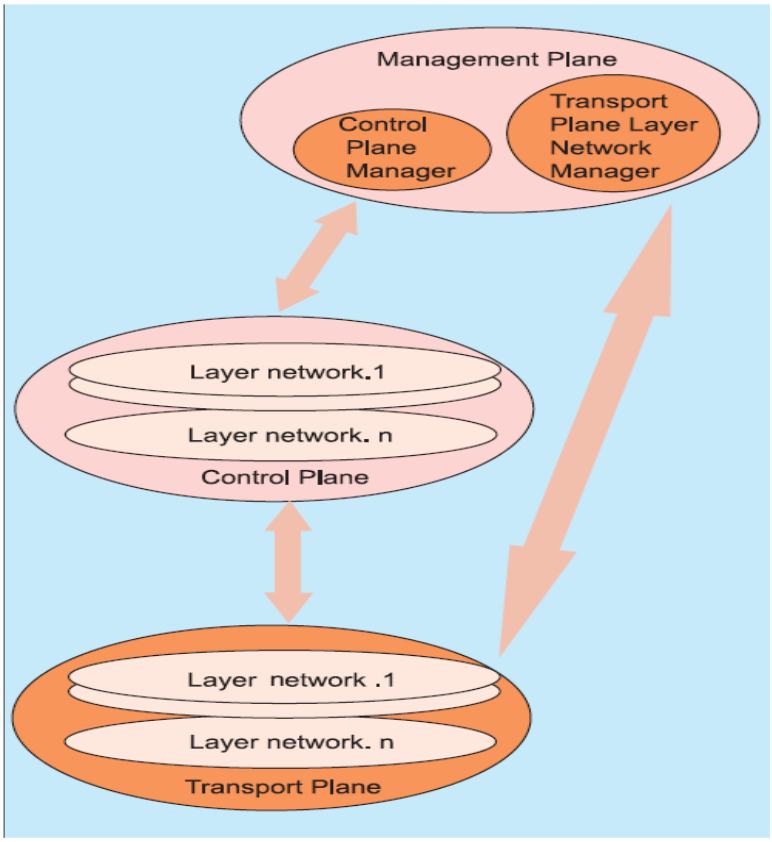
- Μη αυτόματη και επιρρεπής σε λάθη επίβλεψη.
- Μεγάλοι χρόνοι επίβλεψης.
- Ανεπαρκής χρήση πόρων.
- Δύσκολη διαλειτουργικότητα ανάμεσα σε packet client networks και circuit–switched optical networks.
- Πολύπλοκη δικτυακή διαχείριση.
- Δύσκολη διαλειτουργικότητα ανάμεσα σε δίκτυα ετερογενών τεχνολογιών.
- Έλλειψη επαρκών μηχανισμών προστασίας και αποκατάστασης.

Από την άλλη τα ASON δίκτυα προσφέρουν όλα εκείνα τα χαρακτηριστικά που τα καθιστούν ικανά για τις σύγχρονες δικτυακές απαιτήσεις, όπως: κλιμάκωση, αποδοτικότητα, ευελιξία και προστασία.

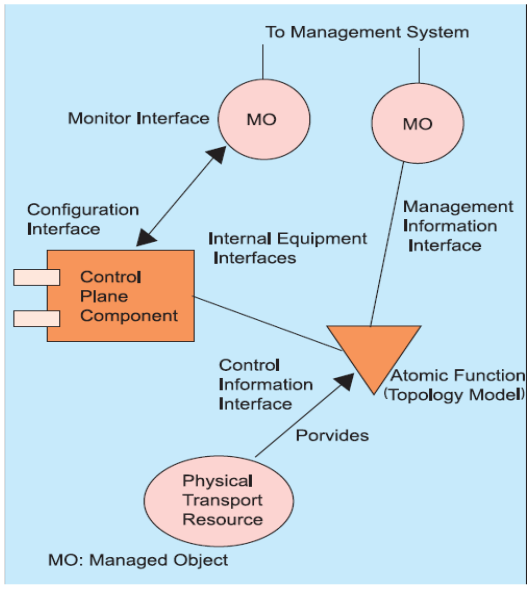
Η δημιουργία ξεχωριστού πεδίου λειτουργικότητας ελέγχου θα έχει ιδιαίτερη βαρύτητα στη δικτυακή διαχείριση και επίβλεψη. Από δω και στο εξής οι συνδέσεις θα μπορούν να εγκαθίστανται σε ένα multi–vendor και multi–carrier περιβάλλον χωρίς να βασίζονται σε ζητήματα διαλειτουργικότητας ανάμεσα σε διαφορετικά συστήματα διαχείρισης. Θα είναι ικανά επίσης να ανταποκρίνονται σε αλλαγές της τοπολογίας, κάτι που θα προσφέρει κλιμάκωση και ευελιξία στο δίκτυο. Νέοι μηχανισμοί προστασίας και αποκατάστασης θα βελτιώνουν την αξιοπιστία και δικτυακή απόδοση, και λαμβάνοντας υπόψιν τις πολύ υψηλές ταχύτητες μεταγωγής στα οπτικά δίκτυα, θα καθιστούν ιδιαίτερα ικανό ένα πεδίο λειτουργικότητας ελέγχου που με τη σειρά του θα επιτρέπει τη βέλτιστη διαχείριση πόρων, θα ανταποκρίνεται γρήγορα στις αστοχίες και θα εκμεταλλεύεται βέλτιστα τα πρωτόκολλα σηματοδοσίας.

Στην Εικόνα 115 διακρίνουμε τα πεδία λειτουργικότητας του ASON. Η μεταφορά πληροφορίας μπορεί να είναι μονόδρομη ή αμφίδρομη. Επίσης το πεδίο μεταφοράς μπορεί να μεταδίδει κάποιας μορφής πληροφορία ελέγχου ή και διαχείρισης. Ένα layer network μέσα στο πεδίο μεταφοράς είναι ένα συστατικό τοπολογίας που περιλαμβάνει τόσο τις οντότητες μεταφοράς όσο και τις λειτουργίες που περιγράφουν την δημιουργία, μεταφορά και τερματισμό των σημάτων που μεταδίδονται στο δίκτυο. Το πεδίο λειτουργικότητας ελέγχου πραγματοποιεί τις διαδικασίες ελέγχου κλήσης και σύνδεσης. Αυτές βασίζονται σε μια ευφυή λειτουργικότητα που περιλαμβάνει αυτόματη ανίχνευση, δρομολόγηση και σηματοδοσία.

Το πεδίο λειτουργικότητας διαχείρισης από την άλλη πραγματοποιεί όλες εκείνες τις διαδικασίες επίβλεψης του πεδίου μεταφοράς και ελέγχου, και συντονίζει όλα τα επίπεδα. Παρώτι κάθε πεδίο είναι ανεξάρτητο, υπάρχει στη πράξη ορισμένη αλληλεπίδραση μεταξύ τους. Αυτή φαίνεται στην Εικόνα 116.



Εικόνα 115. Τα πεδία λειτουργικότητας του ASON



Εικόνα 116. Αλληλεπίδραση των πεδίων λειτουργικότητας του ASON

Όπως φαίνεται και στην Εικόνα, μια ατομική λειτουργία –atomic function αντιπροσωπεύει την λειτουργικότητα των συστατικών στοιχείων μεταφοράς μέσα στο δίκτυο. Μια τέτοια ατομική λειτουργία δεν μπορεί να διαιρεθεί σε απλούστερες. Τόσο τα αντικείμενα διαχείρισης όσο και η πληροφορία διαχείρισης βρίσκονται φυσικά ενταγμένα στους πόρους μεταφοράς. Επιπλέον, η λειτουργία του control plane μοιάζει αυτόνομη με αυτήν του management plane και αντίστροφα, με αποτέλεσμα να μην γνωρίζει η μια την ύπαρξη της άλλης, αλλά με ύπαρξη ταυτόσιμων πληροφοριών και στις δύο. Κάθε συστατικό του πεδίου λειτουργικότητας ελέγχου διαθέτει ένα σύνολο από διεπαφές που χρησιμοποιούνται για την καταγραφή και ρύθμιση διαφόρων πολιτικών. Θα πρέπει να τονίσουμε οτι το management plane δεν αποκτά πρόσβαση στους πόρους μέσω των συστατικών του control plane αλλά μονάχα τους διαχειρίζεται.

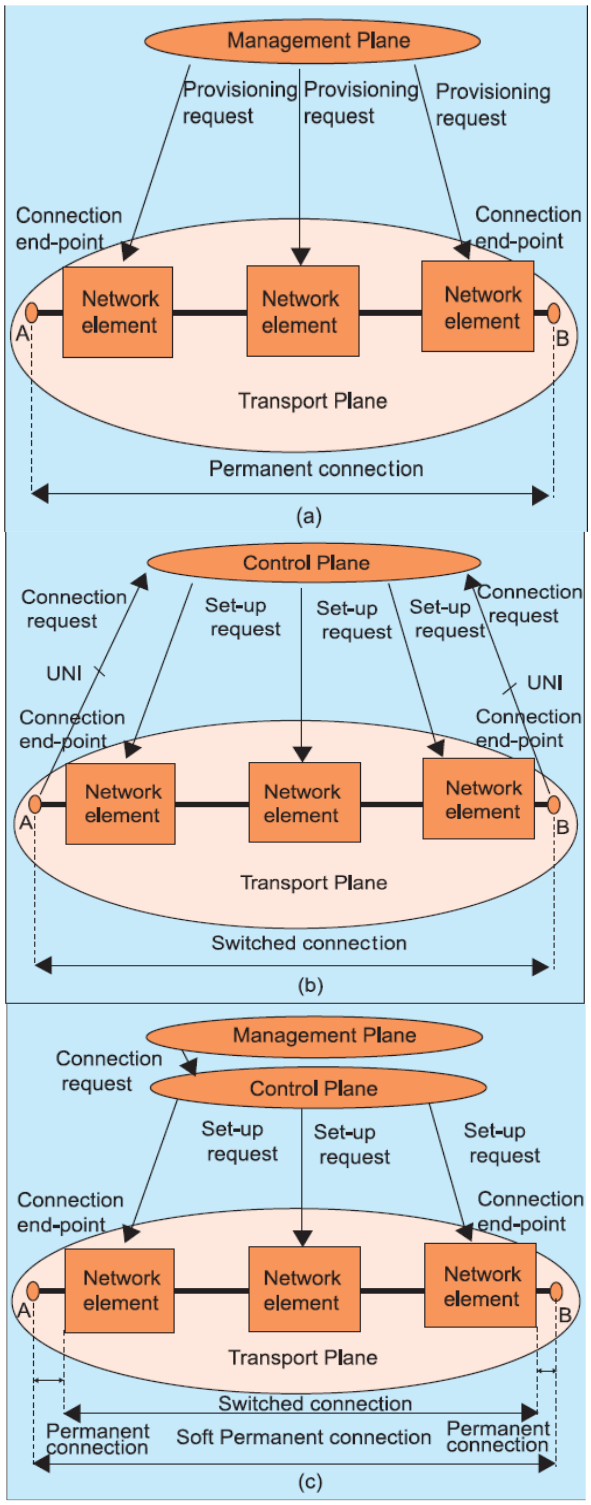
Ως πρός τις οπτικές συνδέσεις, υποστηρίζονται τρείς κυρίως τύποι , όπως καθορίζονται απο το G. 807:

- Μονόδρομη point–to–point σύνδεση.
- Αμφίδρομη point–to–point σύνδεση.
- Μονόδρομη point–to–multipoint σύνδεση.

Επιπλέον στο ASON τρείς κυρίαρχοι τύποι συνδέσμων υποστηρίζονται:

- Permanent.
- Switched.
- Soft permanent.

Οι μόνιμες συνδέσεις εγκαθίστανται είτε από ένα σύστημα διαχείρισης ή μέσω μη αυτόματης επίβλεψης. Κατά συνέπεια μια τέτοια σύνδεση δεν απαιτεί παρέμβαση του control plane και δεν εμπλέκει αυτόματη δρομολόγηση ή σηματοδοσία. Συνήθως πρόκειται για μια στατική σύνδεση που κρατάει μεγάλο χρονικό διάστημα, από μήνες έως και χρόνια. Η switched σύνδεση εγκαθιδρύεται κατ'απαίτηση –on demand από τα τερματικά σημεία με τη χρησιμοποίηση δυνατοτήτων δρομολόγησης και σηματοδοσίας του control plane. Αυτός ο τύπος σύνδεσης απαιτεί ένα user–network signaling interface (UNI), ενώ η εγκατάστασή του μπορεί να είναι ευθύνη του τελικού χρήστη. Τέλος, οι ημιμόνιμες συνδέσεις εγκαθιδρύονται μέσω του καθορισμού δύο μόνιμων συνδέσμων στα άκρα του δικτύου, και της ρύθμισης μιας switched σύνδεσης ανάμεσα στις δύο προηγούμενες συνδέσεις. Ο συγκεκριμένος τύπος σύνδεσης αποτελεί έναν υβριδικό και δεν απαιτεί UNI. Από όλους αυτούς τους τύπους συνδέσεων, ο switched εμπλέκει το control plane και μπορεί να ενεργοποιηθεί σε μερικά δευτερόλεπτα. Εμπεριέχει υπηρεσίες όπως bandwidth on demand. Από την άλλη, οι ημιμόνιμες συνδέσεις υποστηρίζουν μηχανισμούς traffic engineering και αποκατάστασης μονοπατιών, ενώ ρυθμίζονται από το control plane.



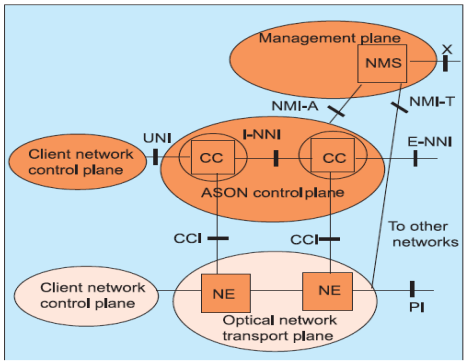
Εικόνα 117. Παραδείγματα συνδέσων μεταφοράς στο ASON

Σύμφωνα με τις G. 8080 ITU–T συστάσεις, η διασύνδεση ανάμεσα σε domains, περιοχές δρομολόγησης και σε ορισμένες περιπτώσεις συστατικά ελέγχου περιγράφεται με τον όρο σημείο αναφοράς –reference point. Ένα reference point αντιπροσωπεύει την συλλογή των υπηρεσιών που παρέχονται από ένα ή περισσότερα συστατικά δικτύου. Η ανταλλαγή πληροφορίας ανάμεσα στα σημεία αναφοράς περιγράφεται από τις διάφορες διεπαφές ανάμεσα στα συστατικά ελέγχου. Μάλιστα, η φυσική διασύνδεση παρέχεται από αυτές τις διεπαφές. Μία φυσική διεπαφή παρέχεται μέσω της αντιστοίχισης μιας αφαιρετικής διεπαφής σε κάποιο πρωτόκολλο. Μία λογική άποψη της ASON αρχιτεκτονικής δίνεται στην Εικόνα 118. Η ASON/ASTN τυποποίηση καθορίζει τρείς λογικές διεπαφές και τα αντίστοιχα σημεία αναφοράς τους στο πεδίο λειτουργικότητας ελέγχου.

- **User–Network Interface (UNI):** Ένα αμφίδρομο interface σηματοδοσίας ανάμεσα σε μια οντότητα πεδίου ελέγχου αίτησης υπηρεσιών και μια εξυπηρέτησής της.
- **Internal Network–Network Interface (I–NNI):** Μια αμφίδρομη διεπαφή σηματοδοσίας ανάμεσα σε οντότητες πεδίου ελέγχου που ανήκουν σε ένα ή περισσότερους domains.
- **External Network–Network Interface (E–NNI):** Ένα αμφίδρομο signaling interface ανάμεσα σε control plane οντότητες που ανήκει σε διαφορετικούς domains.

Μερικές από τις υποχρεωτικές υπηρεσίες που πρέπει να υποστηρίζουν τα interfaces αυτά είναι: **μηνύματα υπηρεσίας σύνδεσης**, που περιλαμβάνουν έλεγχο κλήσης, έλεγχο σύνδεσης και επιλογή σύνδεσης, **διεύθυνση ακραίου σημείου** και **πληροφορίες δρομολόγησης**, καθώς και **έλεγχο δικτυακών πόρων**.

Οι τυποποιήσεις του ASON παρέχουν την δυνατότητα του **multi–homing**: την υποστήριξη δηλαδή περισσοτέρων από ένα συνδέσμων ανάμεσα σε έναν χρήστη ή πελάτη δικτύου και το οπτικό δίκτυο. Αυτή ακριβώς η τεχνική προσφέρει ανθεκτικότητα σε αστοχίες και λάθη ενώ εξισορροπεί το φορτίο κίνησης.



CC: Connection Controller
CCI: Connection Control Interface
E-NNI: External Network-Network Interface
I-NNI: Internal Network-Network Interface
NE: Network Element
NMI-A: Network Management Interface-ASON control plane
NMI-T: Network Management Interface-Transport control plane
NMS: Network Management System
PI: Physical Interface

Εικόνα 118. Λογική άποψη της ASON αρχιτεκτονικής

Το πεδίο λειτουργικότητας ελέγχου είναι ένα σύνολο από οντότητες που είναι υπεύθυνες για την εγκατάσταση από άκρου σε άκρου συνδέσεων, την απελευθέρωσή τους και την συντήρησή τους. Στην ASON λειτουργικότητά του το πεδίο ελέγχου είναι υπεύθυνο για τον έλεγχο κλήσης και σύνδεσης. Μία κλήση είναι μια συσχέτιση ανάμεσα σε ακραία σημεία που υποστηρίζουν μια εκάστοτε υπηρεσία, ενώ η σύνδεση είναι μια οντότητα μεταφοράς ικανή να μεταφέρει πληροφορία. Η διαδικασία ελέγχου κλήσης είναι με τη σειρά της υπεύθυνη για τη πραγματοποίηση μίας άκρου σε άκρου συμφωνίας συνόδου, εγκαθίδρυση της και συντήρησή της. Από την άλλη η διαδικασία ελέγχου σύνδεσης απασχολείται με την αρχικοποίηση και απελευθέρωση των συνδέσμων καθώς και τον έλεγχο της κατάστασής τους. Ο λογικός διαχωρισμός του ελέγχου κλήσεων και συνδέσεων επιτρέπει την μείωση πληροφορίας ελέγχου κλήσης στους κόμβους του δικτύου, αφού αυτός πραγματοποιείται στο UNI και E–NNI και όχι στο I–NNI.

Το πεδίο λειτουργικότητας ελέγχου πραγματοποιεί τις ακόλουθες κυριότερες υπηρεσίες:

- **Αυτόματη ανίχνευση γειτονικών κόμβων, διαθέσιμων πόρων και συνδέσμων.**
- **Ανάθεση και απελευθέρωση διευθύνσεων.**
- **Σηματοδοσία.**
- **Δρομολόγηση.**

Τέλος, υπάρχουν και ορισμένες απαιτήσεις για την ομαλή λειτουργικότητα του πεδίου ελέγχου. Κάποιες από αυτές είναι ένα αποδεκτό προσυμφωνημένο επίπεδο Service Level Agreement για τις διαθέσιμες υπηρεσίες στο δίκτυο, ο έλεγχος και η επιβεβαίωση της ύπαρξης επαρκών πόρων για την εγκαθίδρυση μιας σύνδεσης τόσο στα circuit–switched δίκτυα όσο και στα packet–switched, η υποστήριξη multi–homing τεχνικών για αύξηση του resilience καθώς και ο διαχωρισμός του control plane σε πολλαπλούς domains.

Οι κυριότερες λειτουργίες του control plane συνοψίζονται ως εξής:

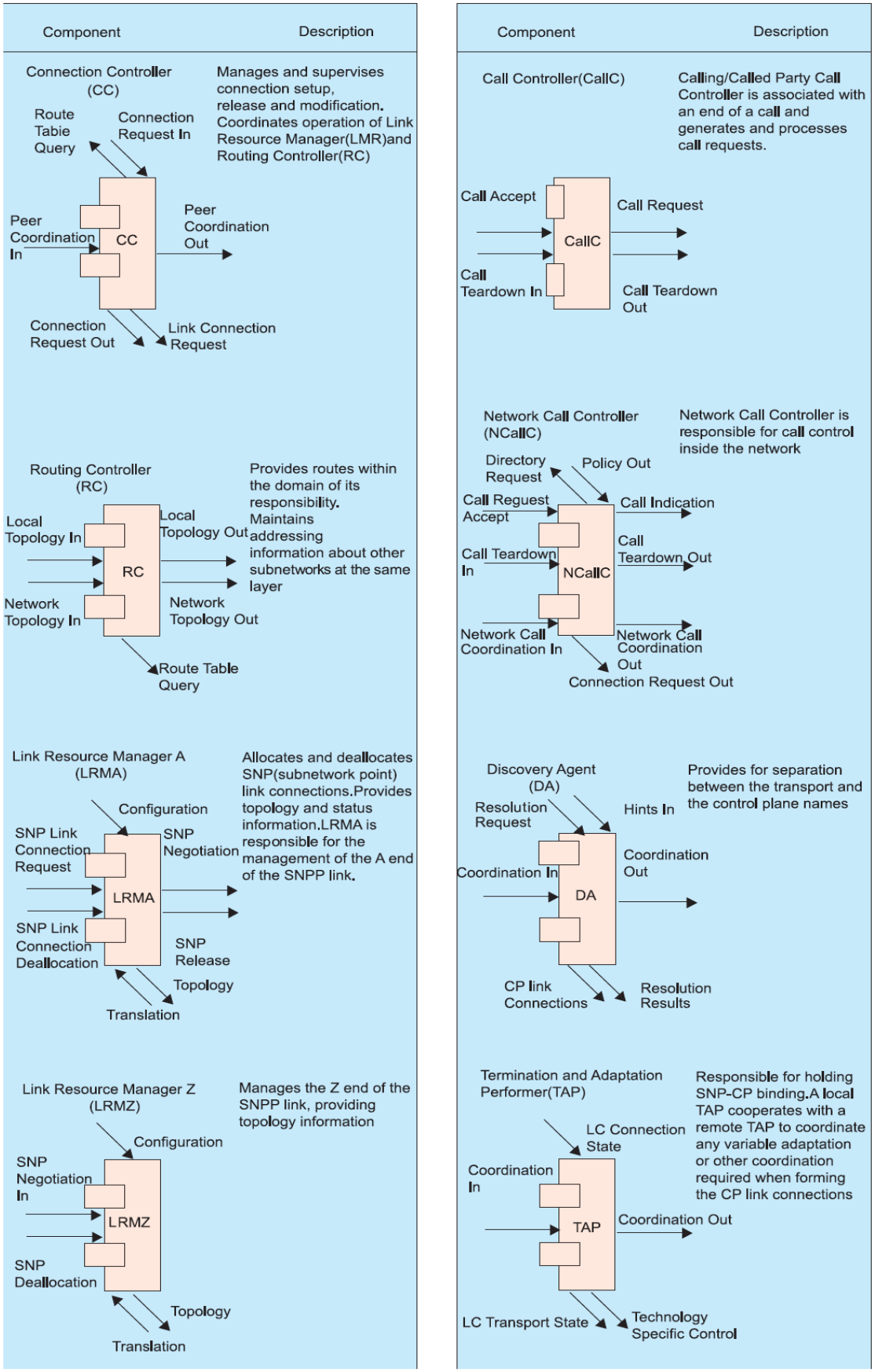
Ανίχνευση

Η αυτόματη ανίχνευση μειώνει δραματικά την ανάγκη για αποκλειστική –explicit παραμετροποίηση. Οι ακόλουθες τρείς κατηγορίες των λειτουργιών ανίχνευσης μπορούν να διακριθούν:

- **Ανίχνευση γειτόνων.**
- **Ανίχνευση πόρων.**
- **Ανίχνευση υπηρεσιών.**

Δρομολόγηση

Η διαδικασία της δρομολόγησης συνίσταται από την επιλογή των βέλτιστων μοπατιών για την πραγματοποίηση των συνδέσεων στο δίκτυο. Επειδή ακριβώς η οπτική μετάδοση είναι μια αναλογική και όχι ψηφιακή τεχνολογία, θα πρέπει επιπρόσθετες πληροφορίες να λαμβάνονται υπόψιν στον καθορισμό των μονοπατιών. Η ASON αρχιτεκτονική υποστηρίζει ιεραρχική, source–based, και βήμα–προς–βήμα δρομολόγηση με κατανεμημένο τρόπο.



Εικόνα 119. Συστατικά του ASON control plane

Σηματοδοσία

Η σηματοδοσία περιλαμβάνει την μεταφορά μηνυμάτων ελέγχου ανάμεσα σε όλες τις οντότητες που επικοινωνούν στο control plane του δικτύου. Είναι σημαντικό να υπάρχει ποικιλία από διαφορετικά πρωτόκολλα σηματοδοσίας τα οποία να λειτουργούν σε ένα multi–domain περιβάλλον.

Διαδικασίες ελέγχου κλήσης και σύνδεσης

Μηχανισμοί Αποκατάστασης

Η μεγαλύτερη δικτυακή αξιοπιστία στο ASON επιτυγχάνεται μέσω της χρησιμοποίησης διαφόρων μηχανισμών προστασίας. Η όλη διαδικασία αποκατάστασης στο ASON εμπλέκει και τα τρία πεδία λειτουργικότητας.

4.2 ΕΥΡΩΠΑΙΚΟ PROJECT PHOSPHORUS: GRID–GMPLS CONTROL PLANE ΥΠΟΣΤΗΡΙΞΗ ΓΙΑ ΥΠΗΡΕΣΙΕΣ ΔΙΚΤΥΩΝ GRID

Τα τελευταία χρόνια έχει γίνει σχεδόν καθολική η αναγνώριση οτι οι τοπικοί υπολογιστικοί πόροι δεν μπορούν να ανταποκριθούν στις ολοένα και αυξανόμενες απαιτήσεις των χρηστών/εφαρμογών, και γι'αυτό έχει προταθεί η προσέγγιση της κατανεμημένης επεξεργασίας κάνοντας χρήση του Grid computing ως λύση του προβλήματος. Ένα τέτοιο παράδειγμα εφαρμογής που απαιτεί μαζική επεξεργασία είναι η περιοχή του επιστημονικού υπολογισμού, η οποία κάνει χρήση high–end συστημάτων και πόρων σε παγκόσμια κλίμακα για την επίλυση της. Η διασύνδεση αυτών των πόρων , σε καθαρά δικτυακό επίπεδο, μπορεί να αποδειχθεί αρκετά πολύπλοκη διαδικασία, καθιστώντας απαραίτητη την ύπαρξη αυστηρών δικτυακών προδιαγραφών. Τα οπτικά δίκτυα δείχνουν να είναι οι περισσότερο ικανές υποδομές να υποστηρίξουν αυτή τη μαζική απαίτηση σε Εύρος Ζώνης και άλλους πόρους και μάλιστα σε συνδυσμό με το πεδίο λειτουργικότητας ελέγχου του GMPLS κατορθώνουν την έγκαιρη και έγκυρη επίβλεψη των συνδέσεων ανάμεσα σε ετερογενείς και multidomain τοπολογίες. Το κοινοτικό πρόγραμμα **PHOSPHORUS** (Lambda User Controlled Infrastructure for European Research) είναι ένα IT επιδοτούμενο Project από την Ευρωπαική Ένωση που απευθύνεται να επιλύσει τις προκλήσεις που προαναφέρθησαν. Πιό συγκεκριμένα, η όλη αντίληψη του δικτύου, οι υλοποιήσεις των control plane λειτουργιών, καθώς και η ανάπτυξη του project θα καθιστούν τις υπηρεσίες ενήμερες για τους συνολικούς διαθέσιμους πόρους του δικτύου Grid (τόσο υπολογιστικούς όσο και δικτυακούς), ενώ θα κάνουν βέλτιστη χρήση των διάφορων ετερογενών υποδομών. Σαν κομμάτι αυτού του εγχειρήματος, το έργο PHOSPHORUS επικεντρώνεται στην ανάπτυξη ενός ενιαίου και ανεξάρτητου πεδίου λειτουργικότητας ελέγχου για την Grid υποδομή, στην οποία οι οπτικοί και υπολογιστικοί πόροι θα ελέγχονται από το ίδιο control plane για λόγους αυξημένης προστασίας και ανοχής σε αστοχίες δικτύου. Στο παρών κείμενο θα δώσουμε μια πολύ συνοπτική αναφορά στις απαραίτητες επεκτάσεις του GMPLS (Grid–GMPLS), καθώς και στη περιγραφή της αρχιτεκτονικής και οργάνωσης του εγχειρήματος.

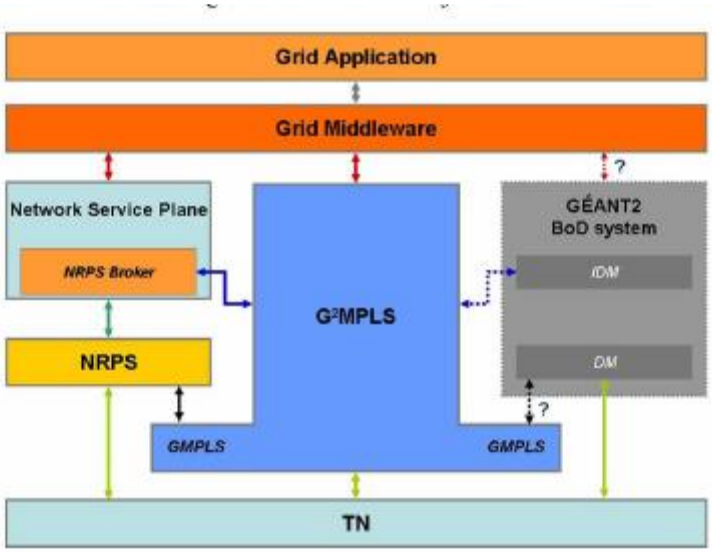
Οι υπολογιστικές εφαρμογές μαζικών απαιτήσεων του 21ου αιώνα θα πρέπει να αντιμετωπίζουν ζητήματα και δεσμεύσεις όπως εγγυημένο επίπεδο υπηρεσιών QoS, μεγάλους όγκους μεταφοράς δεδομένων, και απαιτήσεις καθυστέρησης τα οποία είναι συνήθως επιτεύξιμα μόνο από την σύγχρονη οπτική τεχνολογία (lambdas). Είναι πλέον αποδεκτό οτι τα υψηλής χωρητικότητας οπτικά δίκτυα επικοινωνιών μπορούν να ικανοποιούν αυτές τις απαιτήσεις σε κίνηση, αλλά στα πλαίσια αυτού του Ευρωπαικού προγράμματος θα πρέπει να αναπτυχθούν και εργαλεία λογισμικού καθώς και frameworks τα οποία θα καθιστούν εφικτή την επίβλεψη των πόρων στο δίκτυο σε συντονισμό με τους υπόλοιπους υπολογιστικούς πόρους. Το Project PHOSPHORUS είναι ένα μεγάλο κοινοτικό έργο που περιλαμβάνει 19 partners από 9 χώρες με σκοπό αυτή ακριβώς την ενοποιημένη αλληλεπίδραση ανάμεσα στο δίκτυο κορμού και τους πόρους του Grid δικτύου μέσα πάντα από την επίβλεψη ενός ενοποιημένου control plane. Το έργο, κάνοντας χρήση του επεκτεταμένου πρωτοκόλλου GMPLS (Grid–GMPLS), προσφέρει 3 πεδία λειτουργικότητας: το Service Plane, το Network Resource Provisioning System (NRPS), και το Control Plane, δίνοντας έτσι την δυνατότητα στους διαχειριστές να δεσμεύουν συγκεκριμένους δικτυακούς πόρους για τις απαιτήσεις του Grid Computing. Το συνολικό task με το έργο περιλαμβάνει την υλοποίηση διεπαφών ανάμεσα σε διαφορετικά NRPS ώστε να επιτρέπει την multi–domain συμπεριφορά, ενώ το πεδίο λειτουργικότητας ελέγχου θα προσφέρει την διαλειτουργικότητα των GMPLS–domains με τους NRPS–domains. Να τονίσουμε εδώ οτι το project θα συνεργάζεται με υπάρχοντα δικτυακά προγράμματα και test–beds όπως το GEANT2.

Στο καθολικό τώρα πρόβλημα της αλληλεπίδρασης των δικτυακών και Grid υπηρεσιών προτείνεται η αξιοποίηση του G2MPLS Control Plane καθώς προσφέρει τα ακόλουθα πλεονεκτήματα:

- Αποτελεί μια αμφίδρομη προσέγγιση με υποστήριξη στα δίκτυα Grid καθώς και στη παραμετροποίηση των δικτυακών πόρων.
- Οι Grid κόμβοι μπορούν να μοντελοποιούνται ως κόμβοι δικτύου με τους grid πόρους επιπέδου κόμβου να προβάλλονται και να παραμετροποιούνται, κάτι που αποτελεί πυρηνικό κομμάτι της λειτουργικότητας του GMPLS.
- Επιτρέπει την ενσωμάτωση χρήσιμων GMPLS χαρακτηριστικών όπως crankback και recovery.

Σε αυτό το σημείο να επισημάνουμε οτι το control plane του G2MPLS αν και προτείνεται ως πιό ισχυρό από το παραδοσιακό ASON/GMPLS για εφαρμογή στο έργο, ενσωματώνει αρκετά παρόμοια πλεονεκτήματα με το Generalized.

Στην Εικόνα 120 διακρίνουμε τα βασικά επίπεδα της αρχιτεκτονικής PHOSPHORUS.

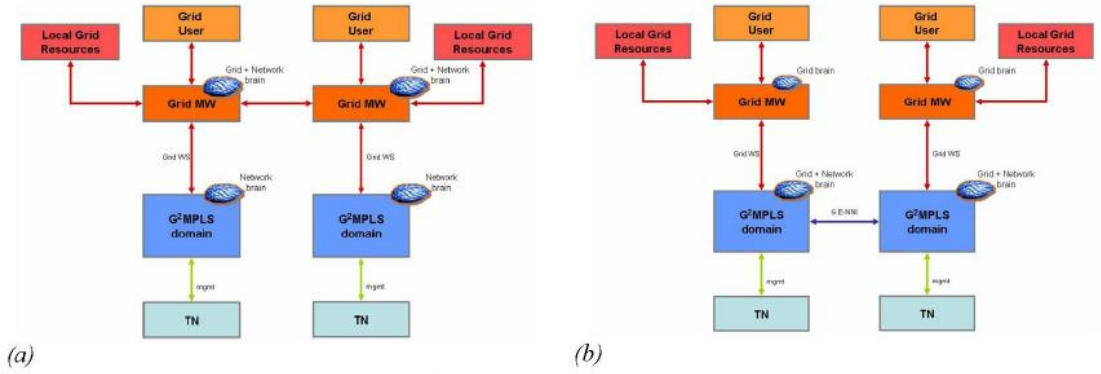


Εικόνα 120. Η θέση του G2MPLS framework στο έργο PHOSPHORUS που περιλαμβάνει και το GEANT2 Project

Στο χαμηλότερο επίπεδο, το Transport Plane επικομείζεται όλα τα δεδομένα, τους οπτικούς εξοπλισμούς και τις ρυθμίσεις των διεπαφών. Το G2MPLS Network Control Plane προσφέρει την ανίχνευση και διαφήμιση των Grid δυνατοτήτων και πόρων των συμμετεχόντων Grid sites (Vsites), την εγκατάσταση των υπηρεσιών και την επίβλεψή τους, καθώς και όλο το αυτοματοποιημένο network provisioning. Το επίπεδο Grid απευθύνεται στην ρύθμιση ενός συμβιβασμού ανάμεσα στις εφαρμογές Grid και middleware. Η λειτουργικότητα του G2MPLS μπορεί να αναπτυχθεί στο συγκεκριμένο έργο είτε ως peer style μοντέλο, είτε ως over lay style. Από τη μεριά του όλου framework το G2MPLS προσφέρει:

— Ταχύτερες δυναμικές εγκατάστασης υπηρεσιών.
— Υποστήριξη από το προγενέστερο GMPLS/ASON αξιόπιστων ρουτινών για Traffic Engineering και ανεκτικότητα σε λάθη.
— Ενοποιημένο interface για τον χρήστη του Grid.

Στο G2MPLS Overlay μοντέλο, το Grid layer έχει πλήρη αντίληψη των Grid και δικτυακών πόρων, ώστε να παρέχει παραμετροποίηση και επίβλεψη των resources. Το G2MPLS λειτουργεί απλά ως ένας πληροφοριακός domain για την όλη διαδικασία, ενώ ο πυρήνας της υπολογιστικής λειτουργικότητας διατηρείται στο Grid layer. Στο άλλο μοντέλο, τώρα, οι περισσότερες ευθύνες περνούν στο G2MPLS το οποίο καθίσταται υπεύθυνο για διαδικασίες δρομολόγησης και προγραμματισμού.



Εικόνα 121. G2MPLS overlay (a) και peer (β) μοντέλα

Περνώντας, τώρα, στις αναγκαίες επεκτάσεις στο GMPLS για την συμβατότητά του με το Grid διακρίνουμε τις ακόλουθες διαδικασίες:

— Ανίχνευση και διαφήμιση των Grid δυνατοτήτων και πόρων των συμμετεχόντων Grid πελατών.

— Εγκατάσταση υπηρεσιών και συντήρηση:

- Συντονισμός, κατανομή, και παραμετροποίηση των Grid και δικτυακών πόρων.
- Ανάκαμψη των υπηρεσιών έπειτα από αστοχία.

— Επιτήρηση υπηρεσιών: καταγραφή της κατάστασης των Grid λειτουργιών και δικτυακών συνδέσμων.

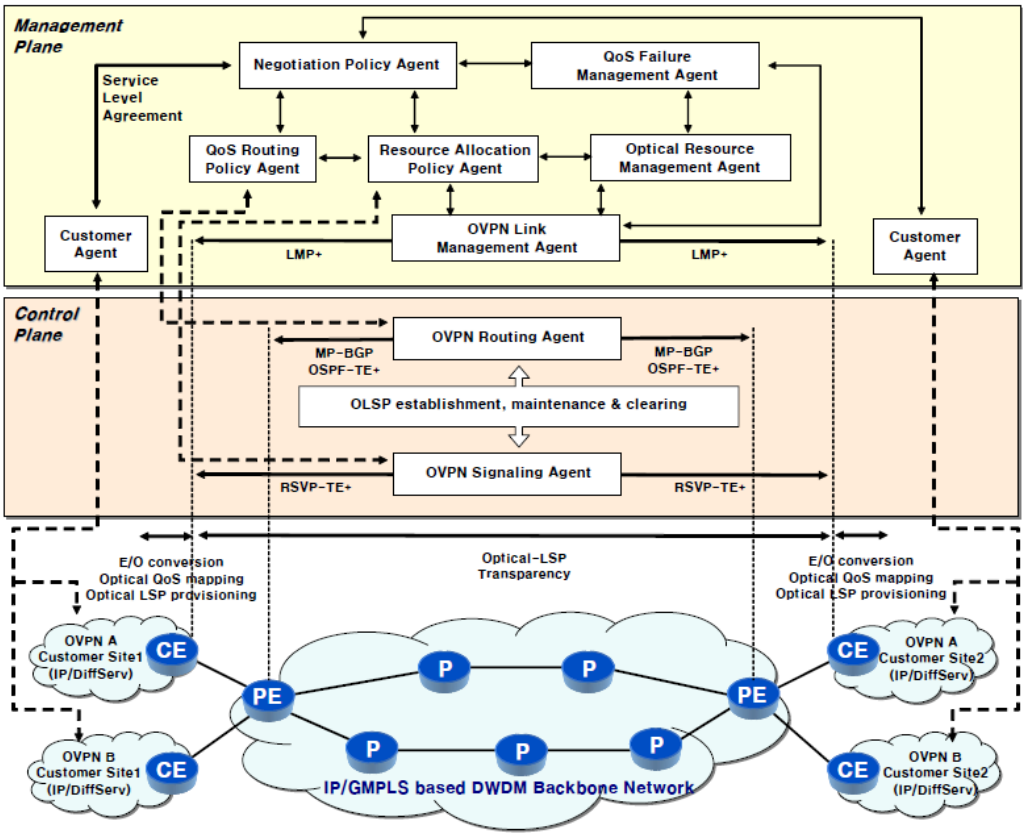
Τέλος, κατά την άφιξη αιτήματος δημιουργίας μονοπατιού, οι καθορισμένες από τον χρήστη παράμετροι που μεταφέρονται στην LSP αίτηση μετατρέπονται σε constraints μέσα στο εκάστοτε PCE –Path Computation Element το οποίο αναλαμβάνει την υπευθυνότητα της δημιουργίας του επιθυμητού άκρου–σε–άκρου μονοπατιού. Ο αλληλοσυντονισμός των Grid εφαρμογών απαιτεί την ταχύτατη ανίχνευση των καθορισμένων συνδέσμων που είναι αποτέλεσμα μιας πραγματικά πολύπλοκης διαδικασίας καθορισμού μονοπατιού. Το PCE κάνει χρήση των τοπικών βάσεων δεδομένων –TED σε κάθε κόμβο ώστε να υπολογίσει το βέλτιστο μονοπάτι. Από αυτά τα Grid constraints το κάθε PCE κατασκευάζει μια αφαιρετική τοπολογία του δικτύου βασισμένη σε κατάλληλους routing και wavelength assignment αλγόριθμους υπολογισμού μονοπατιού.

4.3 OPVN's – OPTICAL VIRTUAL PRIVATE NETWORKS

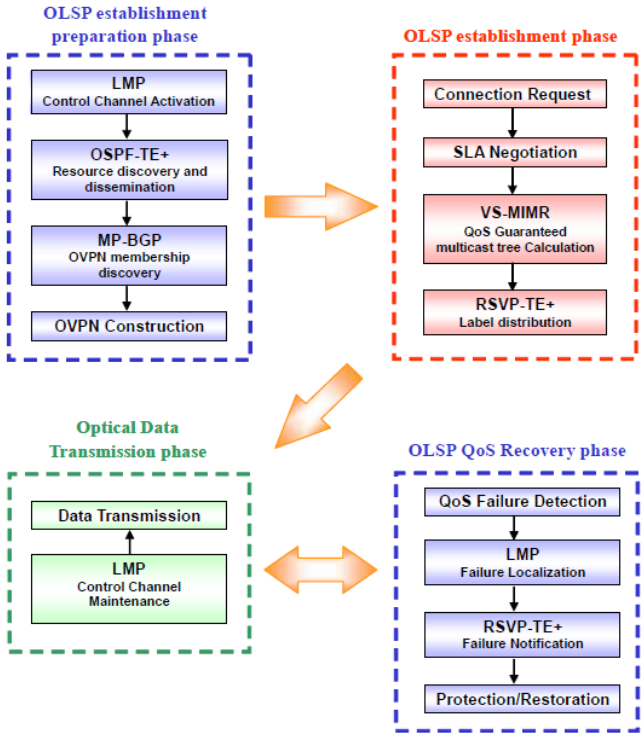
Τα οπτικά εικονικά ιδιωτικά δίκτυα –**Optical Virtual Private Networks** αναμένεται να αποτελέσουν μια από τις βασικότερες εφαρμογές των οπτικών δικτύων του μέλλοντος. Γι'αυτον ακριβώς τον λόγο η OVPN over IP/GMPLS over DWDM τεχνολογία έχει προταθεί ως μια επιτυχημένη προσέγγιση για την πραγματοποίηση των επόμενης γενιάς VPN υπηρεσιών. Τα OVPN θα πρέπει να προσεγγίζονται ανάλογα με τον τύπο των υπηρεσιών είτε ως unicast είτε ως multicast. Στη unicast μέθοδο, ένα βέλτιστο οπτικό μονοπάτι ανάμεσα σε πηγή και προορισμό θα πρέπει να εγκαθιδρύεται για μια point–to–point σύνδεση. Στην άλλη περίπτωση, τα οπτικά μονοπάτια οφείλουν να εγκαθίστανται για point–to–multipoint συνδέσεις στην multicast μέθοδο. Τα πλεονεκτήματα και οφέλη της multicast μεθόδου έγγυνται στην οικονομία εύρους ζώνης και δυνατότητα κλιμάκωσης.

Για την εγκαθίδρυση του multicast OLSP –Optical Label Switched Path, στο σημείο Πελάτη, ένας Customer Agent απαιτεί μια CE (Client Edge)–to–CE OLSP εγκατάσταση με προσυμφωνημένα επίπεδα SLA. Μόλις ο Agent που είναι υπεύθυνος για την ρύθμιση των πολιτικών αυτών, λάβει την ειδοποίηση σε κάποιο ingress PE (Provider Edge) για την εγκαθίδρυση του OLSP, εμπλέκει τον υπεύθυνο Agent για QoS πολιτικές δρομολόγησης, να πραγματοποιήσει ανάθεση της πληροφορίας δρομολόγησης και μήκους κύματος που εξάγεται από το αίτημα αυτό. Σε αυτή τη διαδικασία για να υπολογιστεί το βέλτιστο QoS–εγγυημένο μονοπάτι, είναι σημαντικό για κάθε οπτικό κόμβο να κάνει broadcast κάθε τοπικά διαθέσιμο πόρο, χρησιμοποιώντας πληροφορίες γειτνίασης και κατάστασης, σε όλη τη τοπολογία.

Ο OVPN Agent δρομολόγησης στο GMPLS βασισμένο OVPN πεδίο λειτουργικότητας ελέγχου κάνει χρήση OSPF–TE ή IS–IS επεκτάσεων για την ανταλλαγή πληροφοριών δρομολόγησης και συνδρομής σε CE–PE και PE–PE επίπεδο αντίστοιχα, μέσω των IGP και MP–BGP πρωτοκόλλων.



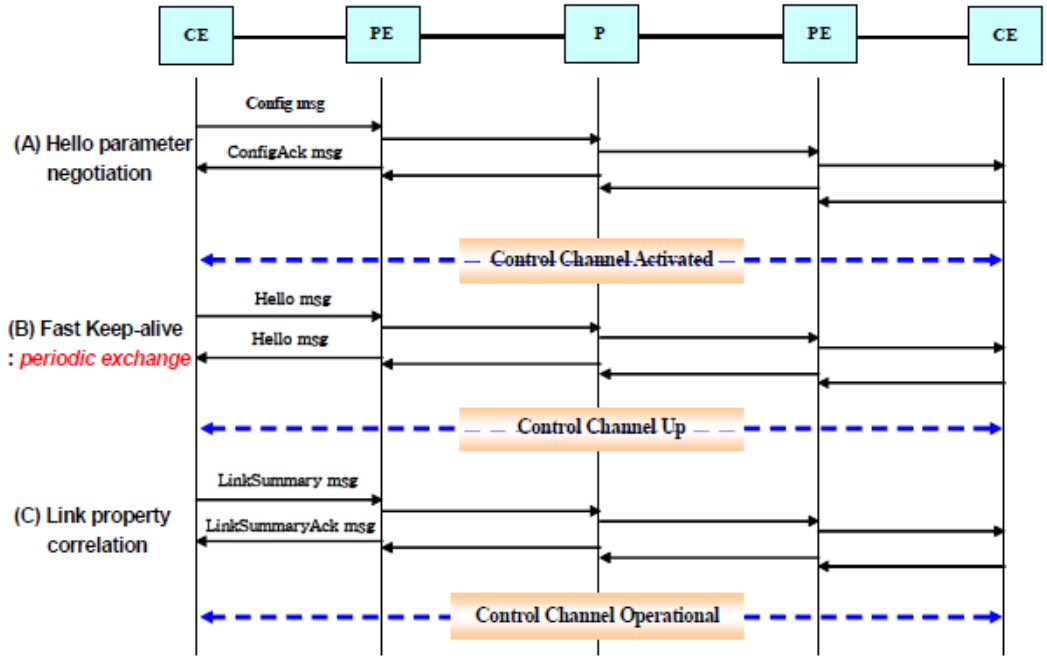
Εικόνα 122. Η αρχιτεκτονική λειτουργικότητα του QoS guaranteed OVPN



Εικόνα 123. Ο μηχανισμός ελέγχου του OVPN για παροχή QoS εγγύσεων

Βασισμένα στην αρχική παραμετροποίηση, τα παραπάνω πρωτόκολλα δρομολόγησης μπορούν να χρησιμοποιήσουν τους μηχανισμούς ανίχνευσης γειτόνων ώστε να εντοπίσουν την OVPN συνδεσιμότητα, μέσω της χρήσης πληροφορίας πόρων, όπως για παράδειγμα τον αριθμό των θυρών, τους ομότιμους κόμβους, τον αριθμό των χρωμάτων ή μηκών κύματος ανα ίνα, καθώς και την χωρητικότητα του καναλιού. Βάσει της OVPN πληροφορίας συνδρομής και πόρων, ο OVPN Routing Agent υπολογίζει τις QoS εγγυήσεις για το χτίσιμο του multicast OLSP. Αμέσως μετά, ο OVPN Signaling Agent στο πεδίο λειτουργικότητας ελέγχου εμπλέκεται στο να δεσμεύσει τους οπτικούς πόρους μέσω του κατάλληλου GMPLS πρωτοκόλλου σηματοδοσίας όπως RSVP–TE ή CR–LDP.

Για την διατήρηση του QoS, η διαχείριση προστασίας και αποκατάστασης περιλαμβάνει τέσσερις λειτουργικές μονάδες**: ανίχνευση αστοχίας, απομόνωση βλάβης, ειδοποίηση και αποκατάσταση**.

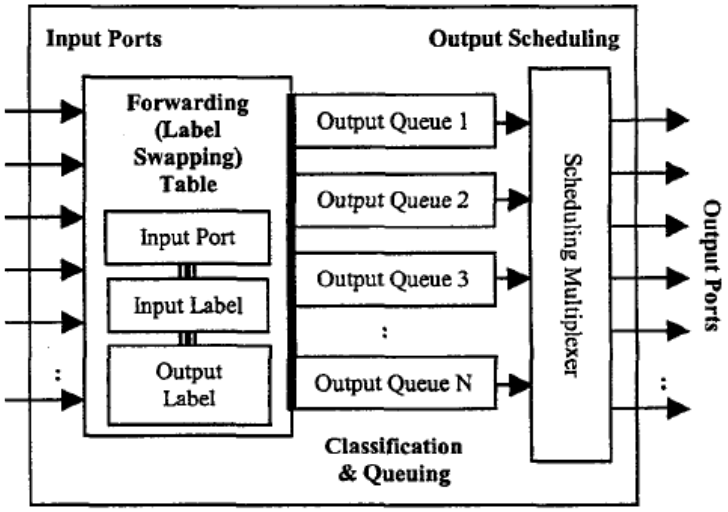


Εικόνα 124. Διαδιακασία εγκατάστασης καναλιού ελέγχου του OVPN

4.4 WIRELESS MULTIPROTOCOL LABEL SWITCHING (WMPLS)

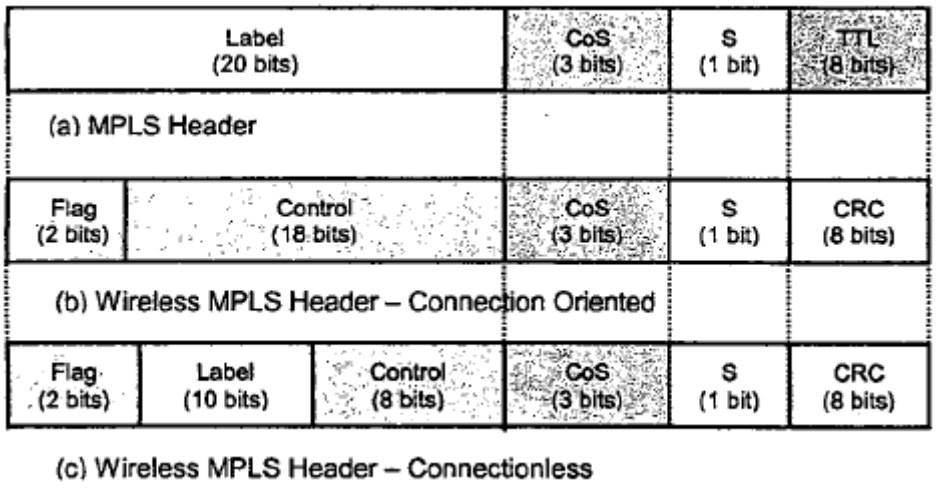
Το framework της wireless multiprotocol label switching (WMPLS) τεχνολογίας, με εφαρμογή στις ασύρματες ευρυζωνικές συνδέσεις, έχει σχεδιαστεί ώστε να αποτελεί ένα ομογενές πρωτόκολλο στα multiprotocol label switching (MPLS), Generalized MPLS (GMPLS), και MPLambdaS, τα οποία είναι οι ισχυρότεροι υποψήφιοι για τα δίκτυα επόμενης γενιάς (Next Generation Networks). Το format του WMPLS μοιάζει αρκετά με τη παραδοσιακή αρχιτεκτονική του MPLS πρωτοκόλλου μαζί με κάποιες απαραίτητες επεκτάσεις για αυξημένη αξιοπιστία ασύρματης επικοινωνίας.

Τα τρία frameworks που προαναφέρθησαν (MPLS, GMPLS, MPLambdaS) ήταν αυτά που ώθησαν τελικά στην ανάπτυξη του WMPLS ως μια ασύρματη έκδοση τους. Η επιτυχημένη εφαρμογή των πολιτικών QoS στις ενσύρματες διασυνδέσεις καθώς και των διαφοροποιημένων υπηρεσιών για τον καθορισμό της βέλτιστης κίνησης στο δίκτυο, έδωσε τα ινία για την δημιουργία και ασύρματων Traffic Engineering λειτουργιών μέσα από το WMPLS πρωτόκολλο. Το MPLS, ως γνωστόν, συνδυάζει τις τεχνολογίες switching επιπέδου 2 (data link layer), με τις τεχνικές δρομολόγησης επιπέδου 3 (network layer). Ο κύριος σκοπός της MPLS τυποποίησης είναι να παρέχει μια ευέλικτη δικτυακή αρχιτεκτονική που προσφέρει αυξημένη απόδοση και κλιμάκωση. Ο MPLS label switch router (LSR) που πραγματοποιεί τις διαφοροποιημένες υπηρεσίες απαιτείται να υλοποιεί μια διαδικασία τριών φάσεων για την ενεργοποίηση του Traffic Engineering. Αυτή ακριβώς η διαδικασία (CQS) φαίνεται στην Εικόνα 125.

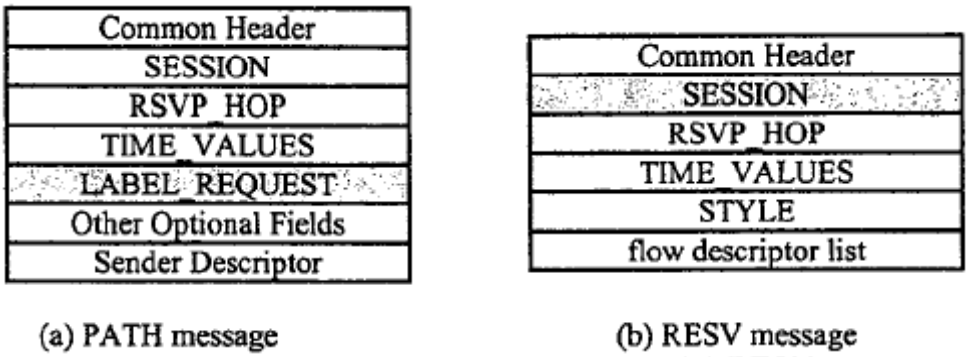


Εικόνα 125. Η LSR CQS λειτουργικότητα

Το WMPLS κάνει χρήση δύο θεμελιωδών επικεφαλίδων πρωτοκόλλων όπως φαίνεται στην Εικόνα 126. Επιπλέον, χρησιμοποιεί σαν πρωτόκολλα σηματοδοσίας το constraint–based routed label distribution protocol (CR–LDP), καθώς και επεκτάσεις στο RSVP (E–RSVP).



Εικόνα 126. Δομή πρωτοκόλλου WMPLS

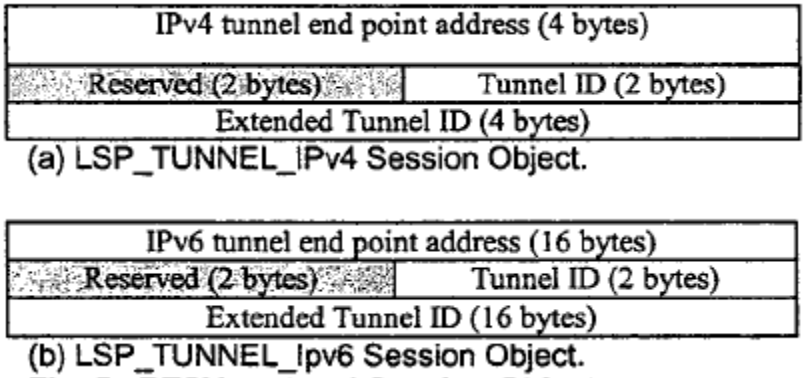


Εικόνα 127. Δομή των PATH και RESV μηνυμάτων

Εικόνα 128. Label Request Object

Τέλος, στην Εικόνα 130 διακρίνουμε τις αναγκαίες επεκτάσεις στο CR–LDP για να ικανοποιεί τις απαιτήσεις του CoS και πληροφορίας ετικέτας από το WMPLS δίκτυο. Συμπερασματικά, κλείνοντας καταλήγουμε στα ακόλουθα πλεονεκτήματα χρήσης του WMPLS:

— Ενοποιώντας και επεκτείνοντας τα MPLS, GMPLS και MPLambdaS στις ασύρματες εκδόσεις τους, το WMPLS κάνει ουσιαστικά χρήση των ίδιων πρωτοκόλλων σηματοδοσίας με αυτά τα frameworks.



Εικόνα 129. RESV protocol session objects

— Το βασικό format του πρωτοκόλλου όπως είδαμε είναι αρκετά όμοιο με αυτό του MPLS/GMPLS.
— Τα base stations το μόνο που θα κάνουν είναι μια απλή μετατροπή των MPLS/GMPLS ετικετών σε WMPLS αντίστοιχα, αυξάνοντας μα αυτό το τρόπο την κλιμάκωση στο δίκτυο.
— Ουσιαστικά με αυτή την επέκταση του GMPLS στον wireless core οι ασύρματοι κόμβοι θα φαίνονται ως τμήματα του LSP μονοπατιού.
— Επεκτείνονται οι πολιτικές των differentiated services στο ασύρματο επίπεδο.

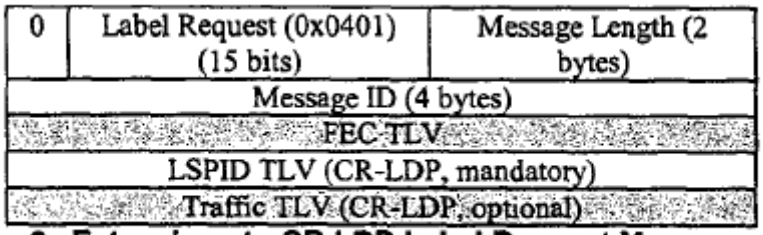


Fig. 6. Extensions to CR-LDP Label Request Message.

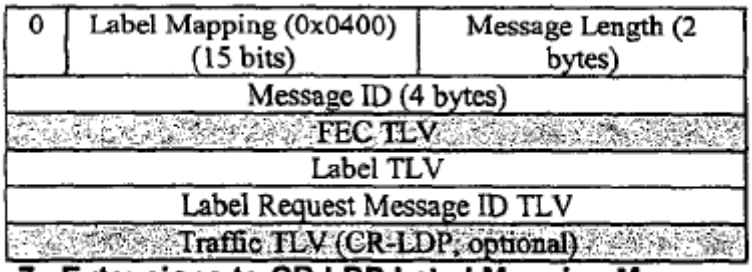


Fig. 7. Extensions to CR-LDP Label Mapping Message.

Εικόνα 130. Επεκτάσεις στο CR–LDP

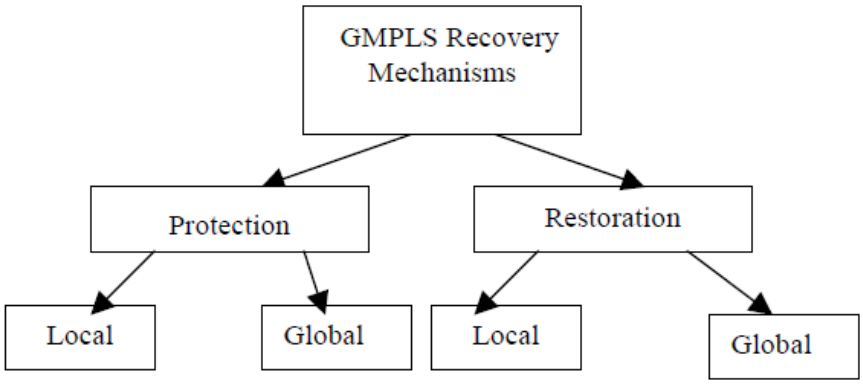
ΚΕΦΑΛΑΙΟ 5: ΠΕΙΡΑΜΑΤΙΚΕΣ ΜΕΤΡΗΣΕΙΣ

5.1 ΠΕΙΡΑΜΑΤΙΚΕΣ ΜΕΤΡΗΣΕΙΣ

Στα προηγούμενα κεφάλαια μελετήσαμε συνοπτικά το θεωρητικό και ερευνητικό σκέλος του γενικευμένου πρωτοκόλλου GMPLS. Εξετάσαμε ακόμη και τα περιθώρια επέκτασης και βελτιστοποίησης των υπαρχόντων μηχανισμών αποκατάστασης στο πεδίο λειτουργικότητας δεδομένων στα πλαίσια του ASONS patch στον ns–2, μέσω του καθορισμού ενός ακόμη πιο βέλτιστου μονοπατιού, όχι μόνο απο άποψη απόστασης αλλά και άλλων TE χαρακτηριστικών δεσμεύσεων όπως για παράδειγμα καθυστέρησης γραμμής –link delay.

Αντικείμενο του παρόντος κεφαλαίου είναι σε πειραματικό επίπεδο αφενός η δέσμευση on demand ενός μονοπατιού σε ένα GMPLS/Optical δίκτυο και η μετάδοση διαφορετικών ροών δεδομένων σε αυτό με τεχνικές multiplexing, και αφετέρου η σύγκριση υπαρχόντων μηχανισμών αποκατάστασης και επανάκτησης μετά από αστοχία σύνδεσης, η μελέτη της επιρροής του control plane failure στους QoS μηχανισμους κίνησης, καθώς και η δυναμική διαχείριση των μονοπατιών μετά από κατάρευση –dynamic provisioning. Για τις ανάγκες αυτές χρησιμοποιούμε τρείς εξομοιωτές: τον **NIST GLASS 2. 0. 2 –GMPLS Lightwave Agile Switching Simulator**, και τον NS**–2.1b9a –Network Simulator** με ενσωματωμένο το ASONS Patch. Να σημειώσουμε οτι οι δύο πρώτοι δικτυακοί εξομοιωτές είναι ανοικτού κώδικα –open source και άρα διατίθενται δωρεάν.

Ως γνωστόν, ένα από τα σημαντικότερα ζητήματα στο GMPLS είναι ο μηχανισμός αποκατάστασης μετά από αστοχία. Υπάρχουν δύο τύποι τέτοιων μηχανισμών: εκείνοι της **προστασίας** –protection και της **επανάκτησης –restoration**. Ένα dedicated μονοπάτι προστασίας εγκαθιδρύεται για μια δεδομένη σύνδεση a priori. Όταν συμβεί μια αστοχία στο κυρίως μονοπάτι, η σύνδεση αλλάζει από το λειτουργικό μονοπάτι σε αυτό της προστασίας (backup). Στους τυπικούς μηχανισμούς επανάκτησης η διαδικασία δημιουργίας του backup path δεν πραγματοποιείται παρά μόνο αφ'ότου προκληθεί η βλάβη στο κυρίως μονοπάτι. Μετά την αστοχία η κίνηση μεταφέρεται στο μονοπάτι προστασίας. Οι μηχανισμοί προστασίας και επανάκτησης είναι διαφορετικοί μηχανισμοί. Λειτουργούν σε διαφορετική χρονική κλιμάκωση: η προστασία απαιτεί πλεονάζοντες πόρους, ενώ η επανάκτηση βασίζεται στην δυναμική δέσμευση των πόρων αυτών. Στην Εικόνα 131 διακρίνουμε την κατηγοριοποίηση των GMPLS μηχανισμών προστασίας.

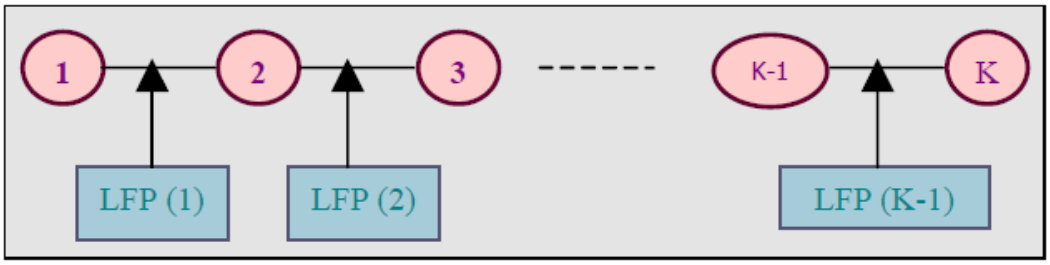


Εικόνα 131. GMPLS μηχανισμοί αποκατάστασης

Το αντικείμενο της τοπικής αποκατάστασης είναι η προστασία απέναντι σε αστοχία σύνδεσης καθώς και η ελαχιστοποίηση του χρόνου που απαιτείται για την ειδοποίηση σφαλμάτων. Η διαδιακασία αυτή ενεργοποιείται από τον ανοδικό κόμβο του προβληματικού link, ο οποίος μπορεί να είναι μεταβατικός κόμβος ή ο αρχικός κόμβος του LSP. Από την άλλη, ο σκοπός της καθολικής αποκατάστασης είναι η προστασία απέναντι σε οποιοδήποτε link fault σε LSP ή τμήμα LSP. Αυτή η αποκατάσταση καλείται και end–to–end path recovery επειδή μόνο οι κόμβοι πηγής και προορισμού αρχικοποιούν την διαδιακασία. Οι μηχανισμοί αυτοί αποκατάστασης μπορούν να χρησιμοποιηθούν σε οποιοδήποτε δίκτυο το οποίο διαθέτει διαφορετικές τεχνικές μεταγωγής σε κάθε επίπεδο της GMPLS ιεραρχίας, όπως για παράδειγμα ATM, IP, Optical. Τα GMPLS δίκτυα υποστηρίζουν τους ακόλουθους μηχανσιμούς αποκατάστασης:

- **Global backup model**: Σε αυτό το μοντέλο, ο ingress κόμβος έχει την ευθύνη της αποκατάστασης από αστοχία. Εδώ η προστασία είναι πάντα ενεργοποιημένη στον κόμβο αυτόν ανεξάρτητα από το πού θα συμβεί η βλάβη στο κυρίως μονοπάτι, ενώ κάθε λειτουργικό μονοπάτι διαθέτει και ένα εναλλακτικό backup. Υπάρχει απώλεια πακέτων ανάλογη με τον απαιτούμενο χρόνο αποκατάστασης, κάτι το οποίο βέβαια είναι κοινό για όλους τους μηχανισμούς.
- **Reverse backup model**: Εδώ ο κύριος σκοπός του συγκεκριμένου μοντέλου είναι η αντιστροφή της κίνησης στο σημείο της αστοχίας πίσω στον αρχικό κόμβο του προστατευόμενου μονοπατιού μέσω ενός reverse backup LSP. Υπάρχει προεγκατεστημένο εναλλακτικό μονοπάτι ώστε να αποφεύγεται η απώλεια πακέτων. Επιπλεόν, μόλις συμβεί μια αστοχία και ταυτόχρονα εντοπισθεί, το LSR στο ingress σημείο του προβληματικού link κάνει επαναδρομολόγηση της κίνησης και τα πακέτα συνεχίζουν να αποστέλλονται πάνω στο κυρίως μονοπάτι αλλά με αντίστροφη πορεία μέσα στο εναλλακτικό μονοπάτι.
- **Local backup model**: Προσφέρει χαμηλό χρόνο αποκατάστασης με αποτέλεσμα μικρότερο packet loss. Σε αυτό το μοντέλο, η αποκατάσταση ξεκινάει από το σημείο της αστοχίας. Διαθέτει σημαντικά μεγαλύτερους χρόνους αποκτάστασης από τις υπόλοιπες μεθόδους, αλλά είναι πιό δύσκολο να συντηρούνται και να δημιουργούνται πολλαπλά LSP backup μονοπάτια, διότι κάτι τέτοιο θα προκαλούσε χαμηλή χρησιμοποίηση πόρων και υψηλή πολυπλοκότητα διαχείρισης.
- **Segment backup model**: Αποτελεί μια ενδιάμεση λύση του τοπικού backup. Προσφέρει χαμηλότερο χρόνο αποκατάστασης, με αποτέλεσμα μικρότερο packet loss, από το global/reverse μοντέλο.
- **1+1 model**: Εδώ υπάρχουν δύο working μονοπάτια. Μετά από την αστοχία, ο υπεύθυνος LSR ανιχνεύει μόνο ένα μονοπάτι και το επιλέγει αυτό ως το κυρίως μονοπάτι. Ο μηχανισμός αυτός δεν έχει χρόνους ειδοποίησης και απώλειας πακέτων, χρησιμοποιεί ωστόσο υψηλή κατανάλωση πόρων.

Ο υπολογισμός της ακριβούς πιθανότητας αστοχίας ενός τμήματος δικτύου είναι πολύπλοκος, ωστόσο μια τέτοια τιμή μπορεί να προκύψει. Θεωρούμε στην Εικόνα 132 ένα LSP με K διαφορετικά links –συνδέσμους.



Εικόνα 132. LSP πιθανότητα αστοχίας

Η LSP πιθανότητα βλάβης (LSP_FP) υπολογίζεται ως εξής:

$$1 - LSP\_FP = \prod_{i=1}^{K-1} (1 - LFP_i)$$

Υποθέτουμε οτι όλα τα LSPs είναι εκ των προτέρων γνωστά και ανεξάρτητα μεταξύ τους. Όταν τα LFPs όλων των συνδέσμων είναι απείρως μικρά (LFP<<1), και ο αριθμός των συνδέσμων (K) δεν είναι μεγάλος, η πιθανότητα αστοχίας του LSP υπολογίζεται ως εξής:

$$1 - LSP\_FP = \prod_{i=1}^{K-1} (1 - LFP_i) \approx 1 - \sum_{i=1}^{K-1} LFP_i$$

Είναι εξίσου σημαντικό να τονίσουμε οτι κατά την αλλαγή της κίνησης στο backup μονοπάτι, θα πρέπει να προστατεύεται όχι μόνο η κίνηση, με το μικρότερο δυνατό βαθμό απώλειας πακέτων, αλλά και οι QoS δεσμεύσεις που έχουμε απο πριν κατοχυρώσει. Επιπρόσθετα, ακόμη και το switch–over interval, ο χρόνος μετάβασης από το κυρίως στο εναλλακτικό μονοπάτι παίζει καθοριστικό ρόλο για το προσφερόμενο επίπεδο υπηρεσιών. Για την εκπλήρωση αυτού του σκοπού προτείνονται δύο end–to–end μηχανισμοί:

- Εγκαθίδρυση πολλαπλών διαδοχικών backup LSPs με χρήση προτεραιοτήτων. **(υποστηρίζεται από τον GLASS)**
- Εγκατάσταση backup για ένα νέο λειτουργικό μονοπάτι –το οποίο θα γίνεται switched στο εναλλακτικό μετά την αστοχία. **(υποστηρίζεται από τον NS–2)**

Ο πρώτος μηχανισμός επιτρέπει την παροχή μιας υπηρεσίας προστασίας που πληρεί τις πολιτικές του παρόχου, και εγγυάται ικανοποιητικό επίπεδο προστασίας. Ωστόσο καταναλώνει πολλούς πόρους και είναι δύσκολο να διαχειριστεί. Η δεύτερη επιλογή απαιτεί σαφώς λιγότερους πόρους αλλά το επίπεδο προστασίας που προσφέρει μπορεί να μην είναι επαρκές.

Δεν είναι δύσκολο να καταλάβουμε οτι η μέθοδος προστασίας που θα επιλέξουμε εν τέλει για το δίκτυο μας εναπόκειται σε μια γενικότερη στρατηγική αποκατάστασης – protection strategy παρά σε μια μεμονωμένη τακτική. Οι ακόλουθες στρατηγικές προστασίας προτίνονται για την μετάβαση από το κυρίως στο backup μονοπάτι:

— preestablished protection strategy **(υποστηρίζεται από τον GLASS)**
— on–demand protection strategy **(υποστηρίζεται από τον NS–2)**
— precalculated protection strategy

Στη πρώτη περίπτωση, μετά από το switch–over το νέο dedicated backup μονοπάτι εγκαθιδρύεται και κατανέμενται. Αυτό το νέο μονοπάτι μπορεί να προστατέυται με τον ίδιο ή άλλο τρόπο. Στη δεύτερη περίπτωση, το νέο LSP δημιουργείται την χρονική στιγμή της αστοχίας (όταν φυσικά αυτή ανιχνευτεί). Αυτή η μέθοδος προσφέρει το χαμηλότερο επίπεδο QoS, αλλά απαιτεί λιγότερους πόρους. Τέλος, στη τελευταία περίπτωση κατά την χρονική στιγμή του switch–over το νέο backup μονοπάτι υπολογίζεται αλλά δεν κατανέμεται. Στην πιθανότητα να εμφανιστεί αστοχία και στο εναλλακτικό μονοπάτι, ένα νέο LSP εγκαθιδρύεται βάσει του υπολογισμένου αυτού μονοπατιού.

Level of QoS	Primary protection	Protection strategy
Highest	Preestablished	Preestablished
High	Preestablished	On-demand
Average	On-demand	On-demand
Low	Preestablished	None
Lowest	On-demand	None

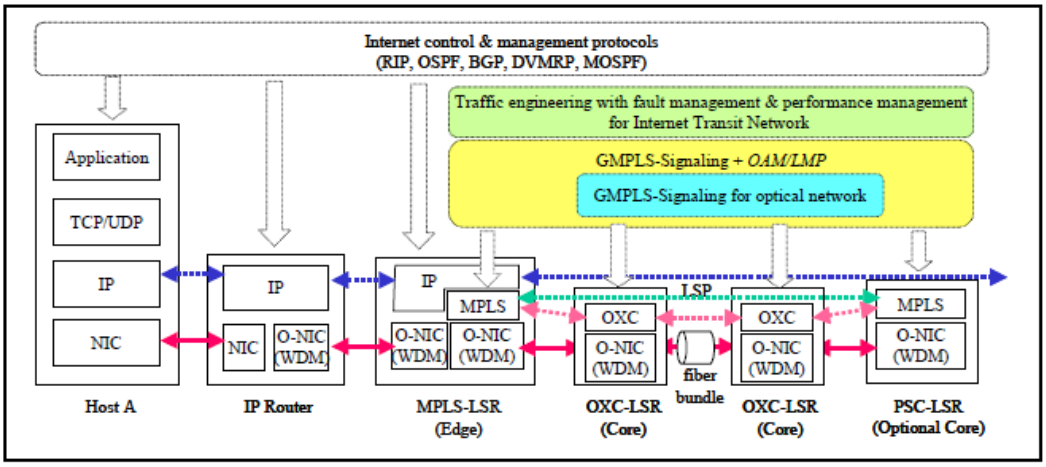
Εικόνα 133. Σχήματα Μηχανισμών προστασίας

Στις πειραματικές μετρήσεις που ακολουθούν, οι ενδογενείς μηχανισμοί αποκτάστασης των εξοιμοιωτών GLASS και NS–2 ακολουθούν , αντίστοιχα, τα μοντέλα προστασίας που προαναφέραμε.

Ας δούμε τώρα λίγο τις αρχιτεκτονικές των δύο αυτών εξομοιωτών, καθώς και το πώς υποστηρίζουν την οργάνωση των πεδίων λειτορυγικότητας του GMPLS.

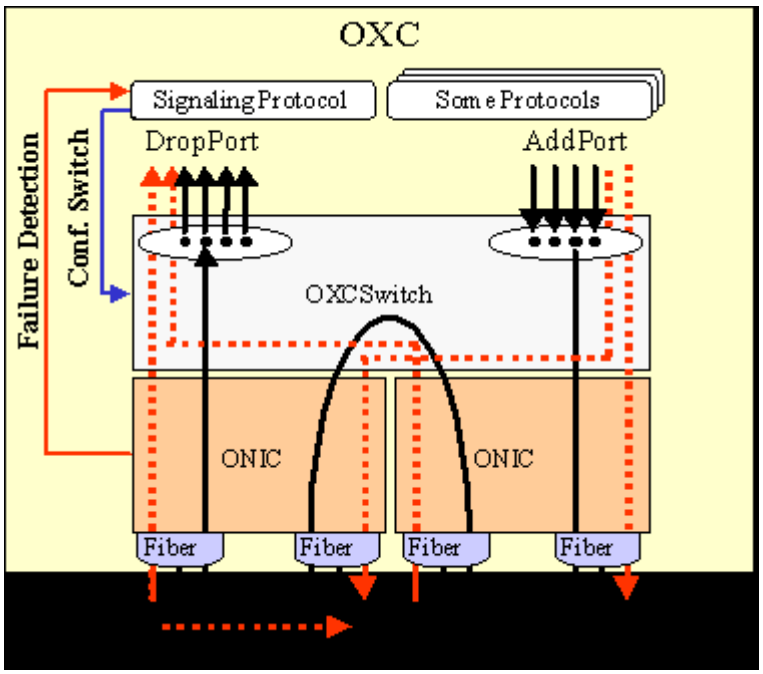
[1] Προφίλ GLASS

Ο εξομοιωτής NIST GLASS υλοποιείται σε γλώσσα προγραμματισμού JAVA πάνω στην SSFNet (Scalable Simulation Framework Network) πλατφόρμα προσομείωσης.



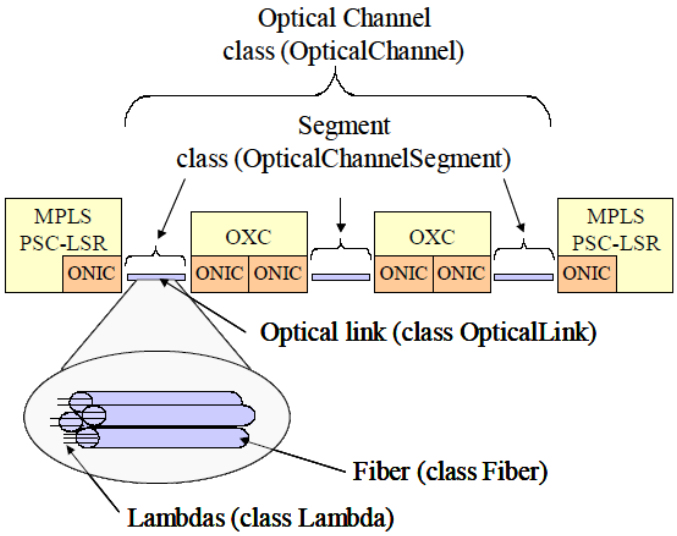
Εικόνα 134. Τα GMPLS επίπεδα αρχιτεκτονικής

Ο συγκεκριμένος εξομοιωτής μοντελοποιεί πλήρως τον οπτικό πυρήνα ενός Optical Network μέσω ενός OXC και OXCEdgeRouter δομικού στοχείου (Optical Cross–Connect), καθώς και των απαραίτητων συνδέσεων οπτικών ινών με Lambdas και Fibers. Επιπλεόν διαθέτει την λειτουργικότητα της MPLS αρχιτεκτονικής με την παροχή του LSR (MPLS node) στοιχείου.



Εικόνα 135. Το Optical Cross Connect (OXC) στον GLASS

Στην Εικόνα 135 διακρίνουμε την οργάνωση ενός OXC στον GLASS. Το συγκεκριμένο στοιχείο δικτύου προσφέρει ταυτόχρονα O/O/O Switching και O/E/O Switching. Η O/E/O μεταγωγή υλοποιείται μέσω της χρήσης της Add/Drop ικανότητας ώστε να μεταφέρει τα εισερχόμενα μηνύματα στο ανώτερο layer και να στέλνει τα εξερχόμενα μέσω του switch στο αντίστοιχο fiber. Η όλη παραμετροποίηση του switch πραγματοποιείται εξωτερικά από το κατάλληλο πρωτόκολλο σηματοδοσίας. Ο GLASS υποστηρίζει και τα δύο signaling protocols του GMPLS: το RSVP–TE και το CR–LDP.

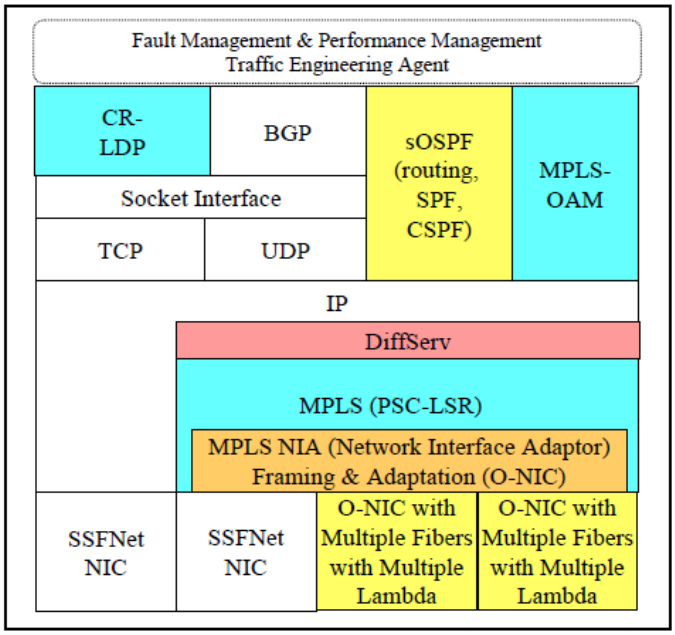


Εικόνα 136. Optical Links στον GLASS

Στον GLASS η οπτική σύνδεση είναι ένα λογικό σύνολο από πολλαπλές οπτικές ίνες. Μια οπτική σύνδεση μπορεί να είναι μονόδρομη ή αμφίδρομη. Κάθε ίνα μπορεί να είναι μονόδρομη ή αμφίδρομη επίσης. Η οπτική ίνα διαθέτει τα χρώματα, ή μήκη κύματος ή Lamdas. Αυτά οργανώνονται σε data lambdas και signaling lambdas. Το γεγονός αυτό γίνεται για τις ανάγκες υπολογισμού του οπτικού εύρους ζώνης.

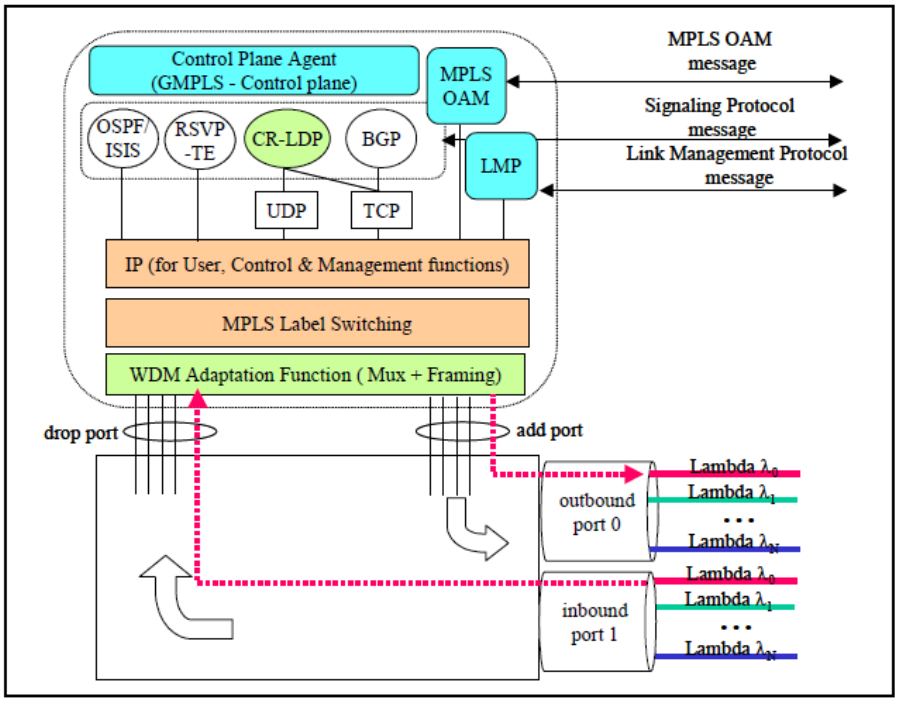
Ο συγκεκριμένος εξοιμειωτής προσφέρει τη δυνατότητα να καταγράφεται η όλη κίνηση της σύνδεσης σε κάθε κατεύθυνση τόσο εισερχόμενη όσο και εξερχόμενη. Αυτό καθίσταται δυνατόν μέσω της τοποθέτησης κάποιων ειδικών monitors στα ONIC –Optical Network Interface Cards, και της καταγραφής των αποτελεσμάτων καθώς και ποικίλων στατιστικών από ειδικούς players στο πρόγραμμα.

Να σημειώσουμε στο σημείο αυτό οτι ο GLASS υποστηρίζει πολυπλεξία κίνησης στο πεδίο διαχωρισμού μήκους κύματος –DWDM.



Εικόνα 137. MPLS–LSR στον GLASS

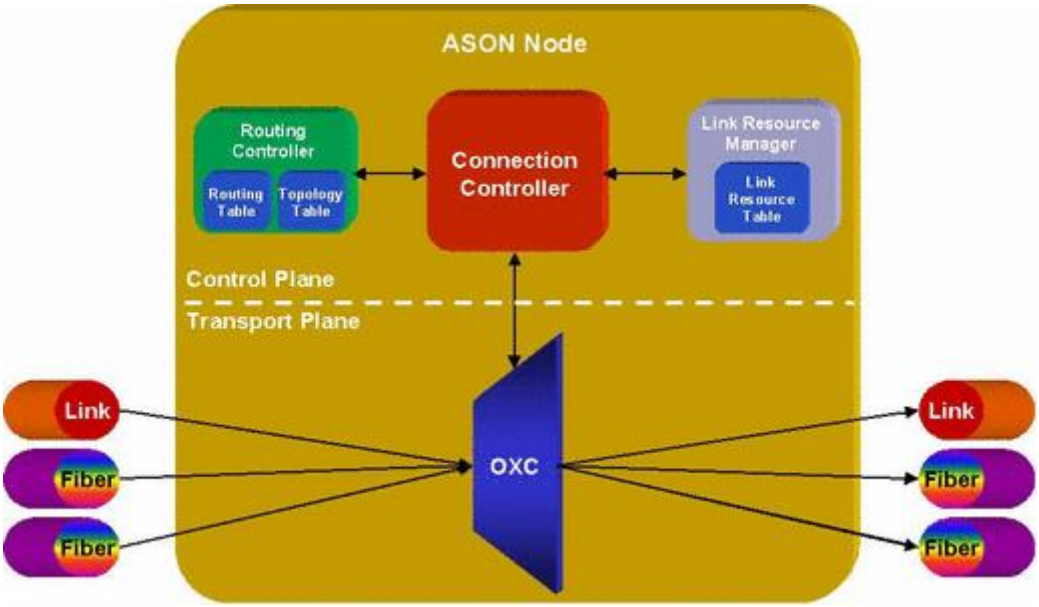
Ως προς τους μηχανισμούς αποκατάστασης , τέλος, να αναφέρουμε οτι χρησιμοποιούνται backup paths τα οποία είναι pre–established, δημιουργούνται πριν δηλαδή την εμφάνιση της αστοχίας, και σε αυτά μετάγεται η κίνηση μόλις συμβεί η βλάβη.



Εικόνα 138. OXC node model στον GLASS

[2] Προφίλ NS–2

Χωρίς το asons Patch δε θα μπορούσαμε αλλιώς να εξομοιωσουμε το οπτικό επίπεδο στον NS–2. Χτισμένο για τις δικές μας ανάγκες στον NS–2.1, ο εξομοιωτής asons υποστηρίζει τις κυριότερες συμβάσεις των G. 8080 τυποποιήσεων. Η όλη αρχιτεκτονική του διακρίνεται στην ακόλουθη Εικόνα:



Εικόνα 139. Αρχιτεκτονική asons στον NS–2

Τα δομικά συστατικά στοιχεία του asons είναι:

- **Optical Cross Connect (OXC)**. Περιλαμβάνει το πεδίο λειτουργικότητας δεδομένων –Transport Plane του ASON και χειρίζεται την μεταγωγή της κίνησης και την ανίχνευση του Loss of Light (LoL).
- **Connection Controller (CC)**. Είναι ο πυρήνας του ASON Control Plane. Κάνει επίβλεψη του signaling, της δημιουργίας και ανανέωσης των Topology Tables, της δημιουργίας και διαγραφής των οπτικών συνδέσμων και αποκατάστασης μετά από αστοχία.
- **Routing Controller (RC)**. Διατηρεί το the Topology Table (TT) και το Routing Table (RT) του ASON network.
- **Link Resource Manager (LRM)**. Κρατάει στατιστικά της κατάστασης των διαθέσιμων πόρων του κάθε κόμβου στο δίκτυο (fiber links, wavelengths) σε ένα Link Resource Table (LRT).
- **WDM fibers**

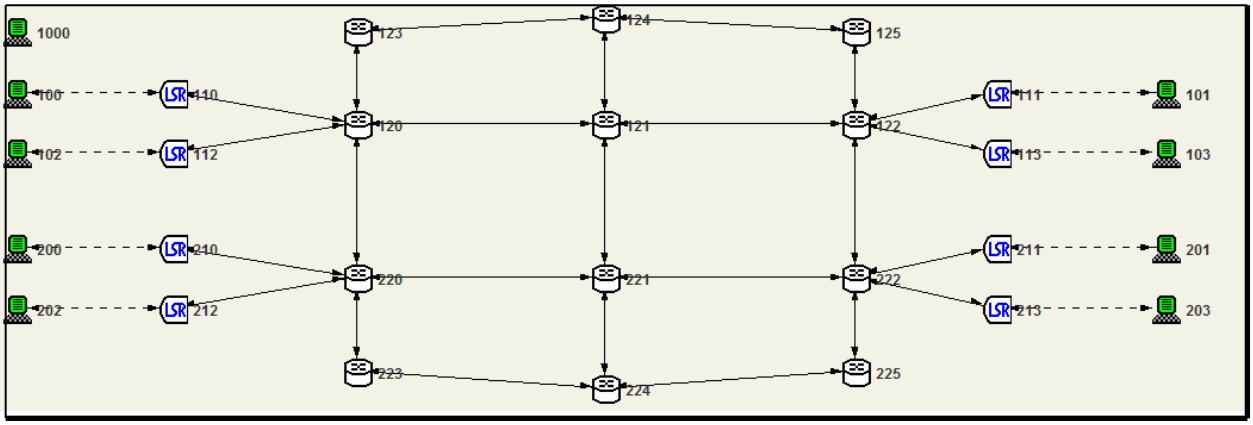
Υποστηρίζει τις ακόλουθες υπηρεσίες:

- **Overlay/Augmented network layering model**
- **Dynamic unidirectional lightpath creation**
- **Out–of–band NNI signaling**
- **Fiber failures**
- **Single and Multilayer Restoration, using two methods:**

- **Hold–off Timer**
- **Recovery Token Signal**

Περνάμε, τώρα, στο δικτυακό σενάριο των πειραμάτων μας.

Η ακολουθούμενη τοπολογία και στους δύο εξομοιωτές παρουσιάζεται στην ακόλουθη Εικόνα:



Εικόνα 140. Η δικτυακή τοπολογία των πειραμάτων μας

ΕΠΕΞΗΓΗΣΗ ΣΥΜΒΟΛΩΝ

OXC ή ASON Node **Πρόκειται για τον GMPLS Router που πραγματοποιεί WDM Multiplexing (στο πεδίο διαχωρισμού μήκους κύματος).**

LSR ή MPLS Node **Είναι ο MPLS Router ή Label Switch Router.**

IP Host **Είναι ο IP Host; Μπορεί να είναι Server ή Client της κίνησης.**

Ethernet **Η συνδεσμολογία (με διακεκομμένες γραμμές) είναι η κλασσική Ethernet σύνδεση.**

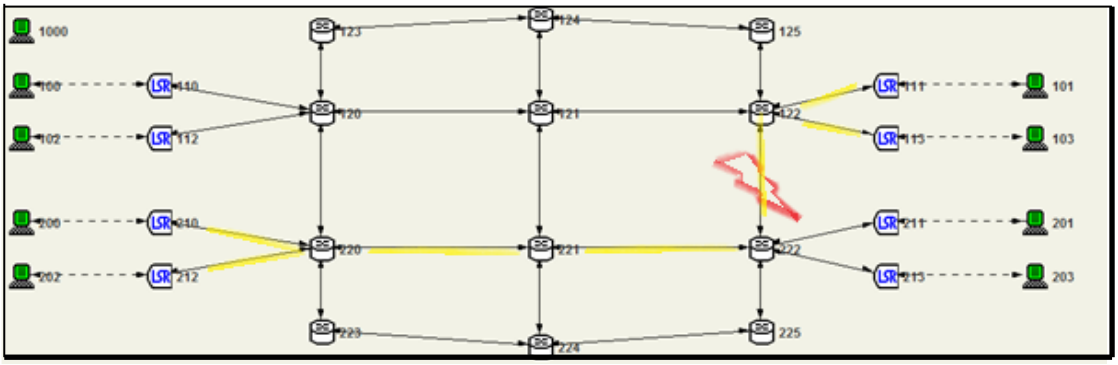
Optical Fiber **Η συνδεσμολογία (συνεχής γραμμή) είναι η οπτική ίνα.**

Σκοπός του σεναρίου μας και στους δύο εξομοιωτές είναι η δέσμευση ενός οπτικού μονοπατιού με συγκεκριμένα χαρακτηριστικά εύρους ζώνης, delay και QoS πολιτικών για την μετάδοση IP κίνησης από δύο διαφορετικές πηγές σε δύο διαφορετικούς προορισμούς, πάνω στο ίδιο αυτό μονοπάτι. Ουσιαστικά υλοποιείται πλήρως η λειτουργικότητα του GMPLS αφού πρόκειται για multiplexing διαφορετικών ροών κίνησης σε on–demand pre–established μονοπάτι. Μεταδίδεται κίνηση:

- **Από τον κόμβο 210 στον κόμβο 111.**
- **Από τον κόμβο 212 στον κόμβο 113.**

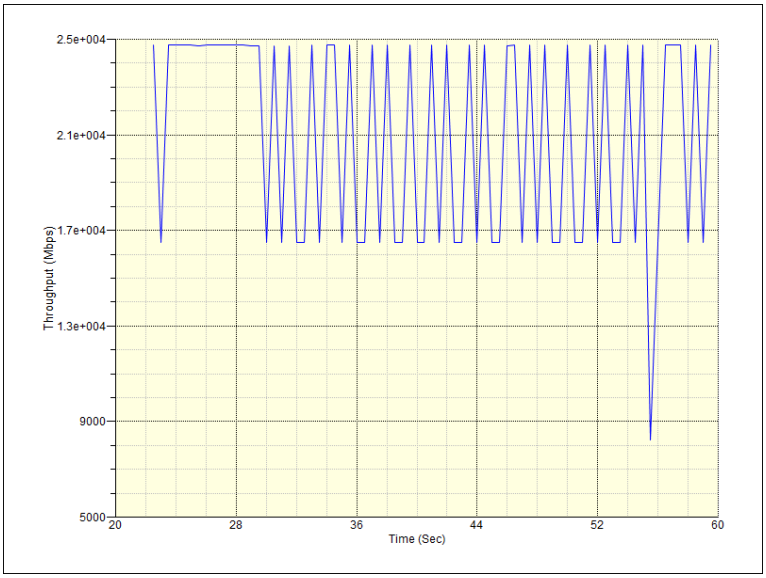
Ακολουθείται το (οπτικό) μονοπάτι: 220 – 221 – 222 – 122

Το πείραμα διαρκεί 60 sec, η μετάδοση της κίνησης ξεκινάει στα 20 sec, ενώ στα 35 sec συμβαίνει αστοχία σύνδεσης **(συγκεκριμένα της γραμμής ανάμεσα στους κόμβους 122 και 222)**. Από κεί και πέρα ενεργοποιούνται οι μηχανισμοί προστασίας και στους δύο εξομοιωτές με σκοπό την άμεση αποκατάσταση και επανάκαμψη της κίνησης.



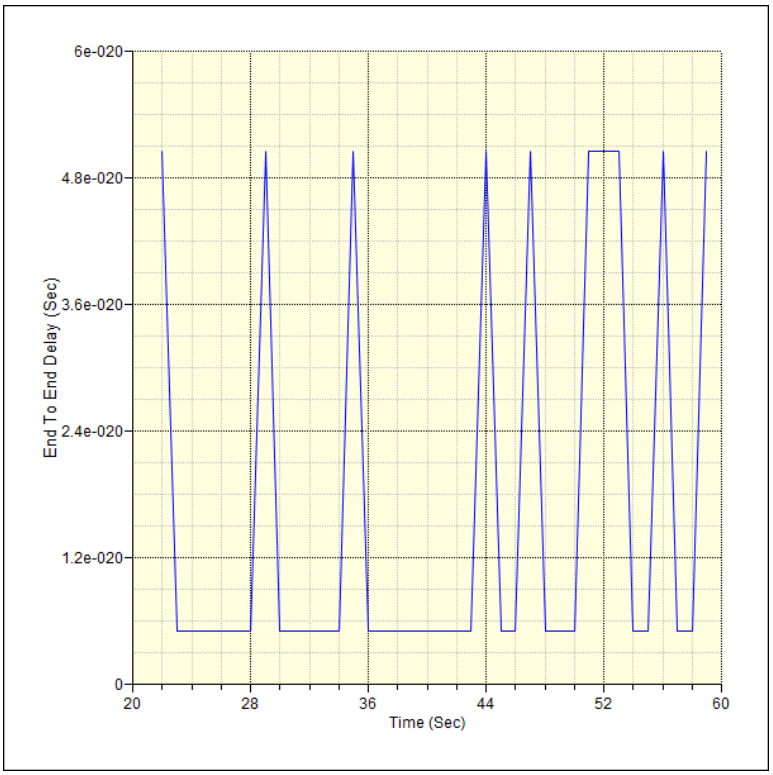
Εικόνα 141. Το ακολουθούμενο μονοπάτι και το σημείο της αστοχίας των πειραμάτων μας

Ακολουθούν τα στατιστικά του **Στιγμιαίου Εύρους ζώνης (Throughput), καθυστέρησης από άκρου σε άκρου (End–to–End Delay)** και **διακύμανσης καθυστέρησης (Jitter)** στον GLASS, καθώς και δύο γράφοι του συνολικού αριθμού των εξερχόμενων πακέτων από αντίστοιχους κόμβους για όλη τη διάρκεια του πειράματος.



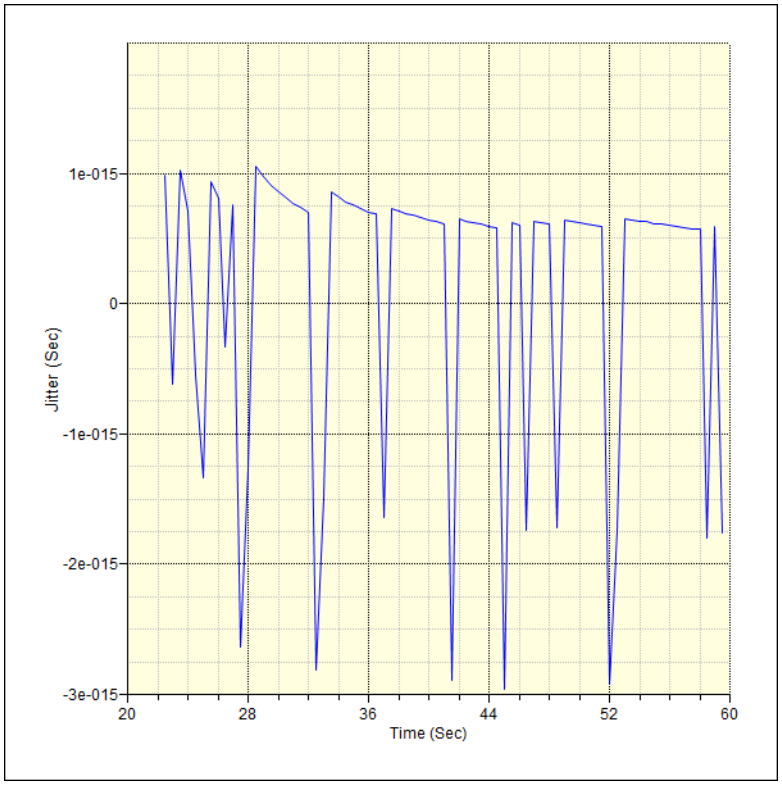
Εικόνα 142. Εύρος ζώνης (Throughput) [GLASS]

Είναι σχεδόν εμφανές και στην Εικόνα, οτι στο 35 sec οπου και πραγματοποιείται η αστοχία υπάρχει εμφανής μείωση του συνολικού Throughput στο δίκτυο. Μέχρι να αποκατασταθεί η κίνηση από το(α) backup μονοπάτι(α), το εύρος ζώνης κινείται στη περιοχή των 17 Gbps. Μετά την αποκατάσταση επανέρχεται στα αρχικά επίπεδα (25 Gbps). Οι εμφανιζόμενες ακμές στο γράφημα είναι αποτέλεσμα της ακαριαίας κατάρρευσης του οπτικού μας συνδέσμου.



Εικόνα 143. Καθυστέρηση από άκρου σε άκρου (End–to–End Delay) [GLASS]

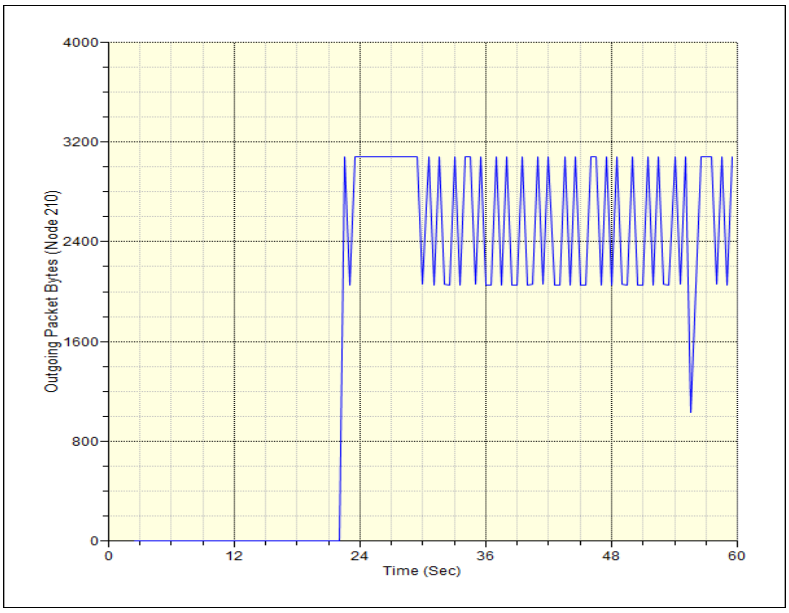
Παρομοίως και εδω στη περίπτωση της καθυστέρησης από άκρο σε άκρο φαίνεται ξεκάθαρα στην Εικόνα οτι στο 35 sec υπάρχει μια απότομη αιχμή, άρα μεγαλύτερη καθυστέρηση, εξαιτίας της αστοχίας στο δίκτυο. Έπειτα από κάποιο μικρό χρονικό διάστημα που κρατάει το switch–over στο backup μονοπάτι, η καθυστέρηση δείχνει να ομαλοποιείται (σχεδόν μηδενική) για αρκετά μεγάλο διάστημα (από 36 – 43 sec).



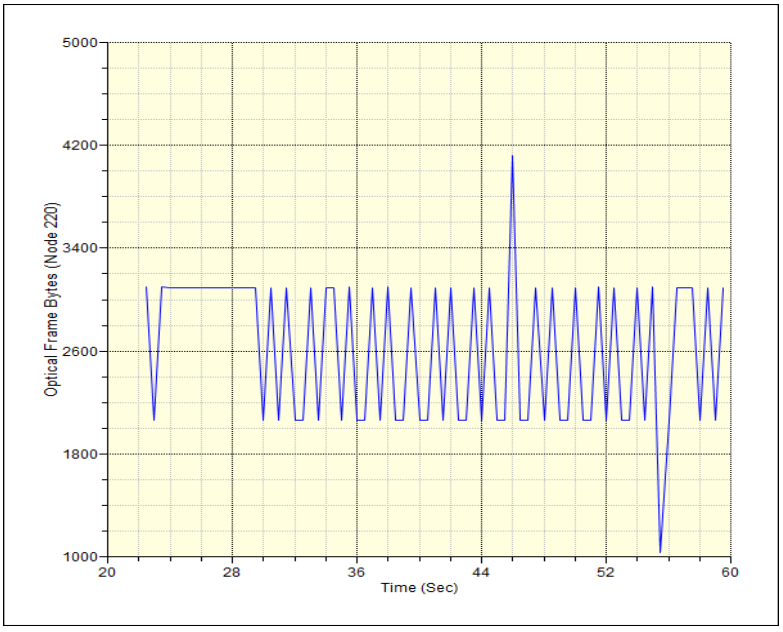
Εικόνα 144. Διακύμανση καθυστέρησης (Jitter) [GLASS]

Στη περίπτωση του Jitter, τώρα, φαίνεται και πάλι καθαρά στην Εικόνα οτι στην χρονική στιγμή της αστοχίας (35 sec) υπάρχει μια απότομη αιχμή προς τα κάτω, δείγμα της αύξησης της καθυστέρησης ανάμεσα σε αποστολέα και παραλήπτη αμέσως μετά την κατάρρευση της γραμμής. Η κλίση του Jitter δείχνει να ομαλοποιείται αμέσως μετά την αποκατάσταση της τοπολογίας.

Τέλος, παραθέτουμε δύο ακόμη στατιστικά γραφήματα που προβάλλουν τον συνολικό αριθμό των εξερχόμενων πακέτων (σε bytes) από τους κόμβους , αντίστοιχα, 210 και 220. Στον πρώτο κόμβο αναφερόμαστε σε IP πακέτα που δεν έχουν ακόμη ενθυλακωθεί (δεν έχει τοποθετηθεί ακόμη το Optical Frame GMPLS Label), ενώ στον δεύτερο έχουμε καθαρά οπτικά πακέτα που μεταδίδονται στον οπτικό φορέα.

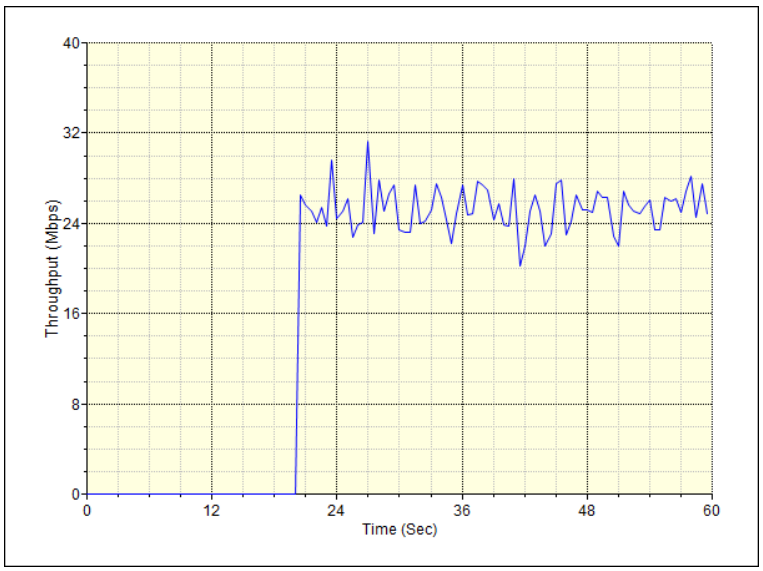


Εικόνα 145. Εξερχόμενα IP Πακέτα από τον κόμβο 210 [GLASS]



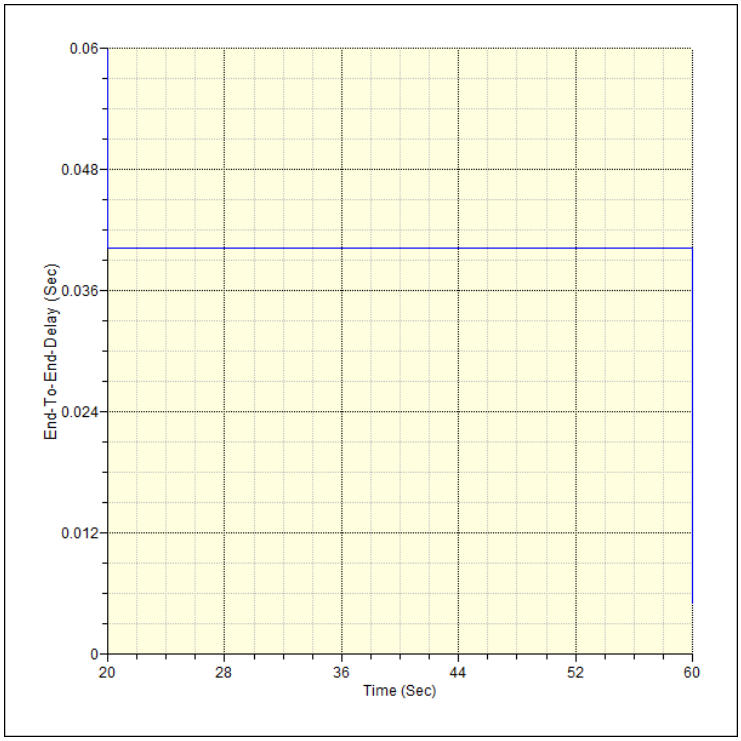
Εικόνα 146. Εξερχόμενα Optical Frame Packets από τον GMPLS κόμβο 220 [GLASS]

Περνάμε, τέλος, στα αντίστοιχα στατιστικά στοιχεία του NS–2.



Εικόνα 147. Εύρος ζώνης (Throughput) [NS–2]

Ακριβώς στο 35 sec έχουμε μια απότομη πτώση του bandwidth που κρατάει σύντομο χρονικό διάστημα, και μετά την αποκατάσταση επανέρχεται στα 25Gbps, όπως ακριβώς και στον GLASS.

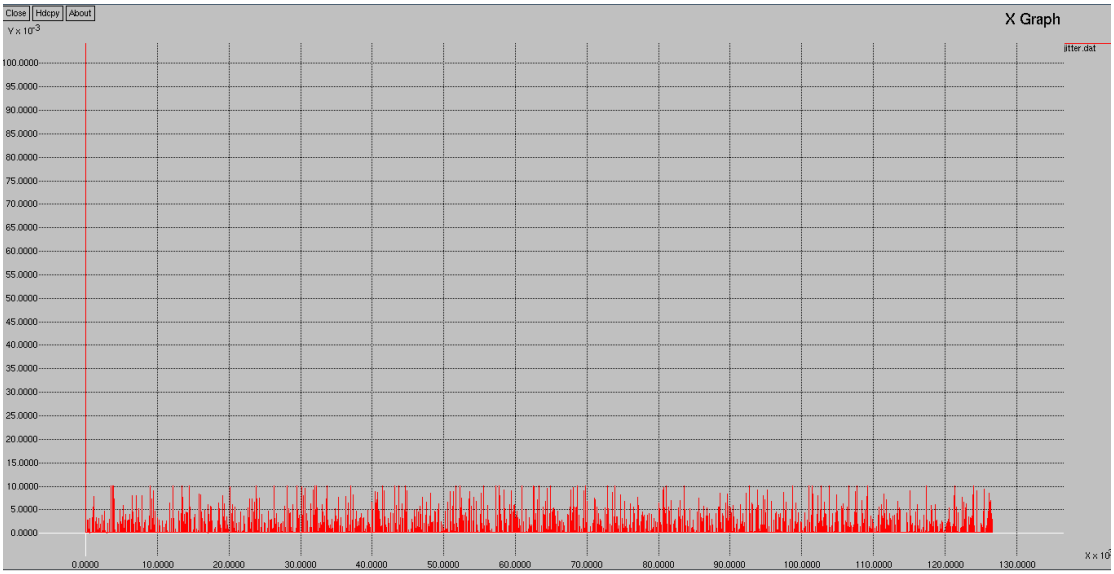


Εικόνα 148. Καθυστέρηση από άκρου σε άκρου (End–to–End Delay) [NS–2]

Από άποψη καθυστέρησης παρατηρούμε οτι εαν εξαιρέσουμε τις όποιες αιχμές στο γράφημα του GLASS, συναντάμε την ίδια ακριβώς περιοχή τιμών (0, 04979 sec) και στον NS–2. Από κεί και πέρα ο NS φαίνεται να μην επηρεάζεται σημαντικά από την αστοχία της σύνδεσης στο ζήτημα του end–to–end delay αν και παρατηρούνται κάποιες μεταπτώσεις σε περισσότερη λεπτομέρεια στο γράφημα.

Τέλος, στην έξοδο του script τυπώνονται τα ακόλουθα:

(1η Ροή) Number of packets sent: 126560 received: 126330 and lost: 230
(2η Ροή) Number of packets sent: 123415 received: 123193 and lost: 222



Εικόνα 149. Διακύμανση καθυστέρησης (Jitter) [NS–2]

ΚΕΦΑΛΑΙΟ 6: ΑΞΙΟΛΟΓΗΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

6.1 ΑΞΙΟΛΟΓΗΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο Κεφάλαιο 6 εξηγήσαμε τη διαφορά ανάμεσα στους μηχανισμούς Προστασίας (Protection Mechanisms) και Αποκατάστασης (Restoration Mechanisms). Στη πρώτη περίπτωση, το εκάστοτε δίκτυο εφαρμόζει μια pre–established protection στρατηγική, βάση της οποίας ΠΡΙΝ ακόμη από την αστοχία επιλέγεται το backup μονοπάτι προστασίας. Το γεγονός αυτό αλλά και γενικότερα αυτή η στρατηγική έχει το πλεονέκτημα της μικρότερης απώλειας πακέτων και διατήρησης των βέλτιστων QoS Constraints, καθώς μετά την αστοχία δεν χρειάζεται να δημιουργηθεί εκ νέου ένα νέο μονοπάτι αλλά απλά να γίνει ένα switch–over από το κυρίως (που έχει υποστεί την αστοχία) στο εναλλακτικό. Στη δεύτερη περίπτωση, ακολουθείται μια on–demand protection στρατηγική όπου ΜΕΤΑ την αστοχία το δίκτυο λαμβάνει την αίτηση να δημιουργήσει καινούργιο μονοπάτι κίνησης, ώστε να αντικαταστήσει το ελαττωματικό. Εδώ, ναι μεν αυξάνεται η απωλεστικότητα των πακέτων, καθώς η διαδικασία δημιουργίας νέου μονοπατιού δαπανά κάποιο παραπάνω χρονικό διάστημα, ωστόσο υπάρχει ένα συγκριτικό πλεονέκτημα σε σχέση με τον προηγούμενο μηχανισμό: Την χρονική στιγμή της αστοχίας το δίκτυο λαμβάνει υπόψιν τις τωρινές συνθήκες (εκείνη ακριβώς τη στιγμή), όπως Εύρος ζώνης, καθυστέρηση και διακύμανση, ώστε να καθορίσει ένα ακόμη πιό βέλτιστο καινούργιο μονοπάτι που θα εξυπηρετεί ορισμένα constraints. Εαν το δίκτυο λαμβάνει υπόψιν αυτό το πλεονέκτημα ο μηχανισμός αυτός καθίσταται αρκετά ωφέλιμος. Άλλωστε, να τονίσουμε εδώ οτι ο πρώτος μηχανισμός μπορεί αναμφισβήτητα να "κερδίζει" σε undropped πακέτα, ωστόσο δαπανά σημαντικούς δικτυακούς πόρους αφού σε κάποιες περιπτώσεις απαιτεί επίβλεψη περισσότερων από ένα ταυτόχρονων μονοπατιών.

Αξιολογώντας τώρα συνοπτικά τα πειράματά μας, διακρίνουμε οτι πράγματι όπως είχαμε πεί και προηγουμένως, ο GLASS ακολουθεί την στρατηγική του Protection Mechanism – Δηλαδή εγκαθιδρύει από πριν το εναλλακτικό μονοπάτι (μάλιστα αυτό φαίνεται και στο σενάριο του εξομοιωτή **– αρχείο: GMPLSFINALSCENARIO. dml –** Γραμμές: 29 – 187), όπου παραμετροποιείται το LSP Backup Tunnel με συγκεκριμένα TE Constraints (π. χ. Weighted Fair Queuing Scheduler, και συγκεκριμένα Traffic Parameters) με αρχή και προορισμό τους κόμβους 210 και 111 αντίστοιχα. **Το γεγονός αυτό επιβεβαιώνεται και στις πειραματικές μας μετρήσεις:** Μετά την αστοχία της γραμμής η κίνηση μεταδίδεται αμέσως (switch–over) στο Backup LSP. Δεν δαπανάται άλλος χρόνος για τη δημιουργία ενός νέου οπτικού μονοπατιού. Ως αποτέλεσμα το στιγμιαίο Εύρος ζώνης και η καθυστέρηση δεν μεταβάλλονται καθοριστικά. Έτσι, και ο βαθμός της απώλειας των πακέτων είναι σχεδόν αμελητέος.

Περνώντας στον NS–2, συμπεραίνουμε από τις μετρήσεις και πάλι, οτι ακολουθεί τον μηχανισμό Αποκατάστασης –Restoration Mechanism, όπου το εναλλακτικό μονοπάτι θα δημιουργείται εκ νέου ΜΕΤΑ την αστοχία. Εκείνο που διακρίνουμε καθαρά στα γραφήματα είναι μια καθυστέρηση της τάξης μερικών δεκάδων msec για την δημιουργία του Backup LSP αμέσως μετά την πρόκληση της βλάβης. Ως εκ τούτου, χάνονται και μερικά πακέτα ένα ποσοστό περίπου της τάξης του 0, 0002%. Στο debugging που ακολουθεί φαίνεται η ακριβής χρονική στιγμή αποκατάστασης στον NS–2:

```
35. 0000: CC(25): Failure detected upstream, I am EGRESS, no NOTIF. upstream, I am EGRESS, no NOTIF.
35. 0048: CC(26): Failure detected downstream, lightpath 0: OFF, sent NOTIF upstream. . .
downstream, lightpath 1: OFF, sent NOTIF upstream. . .
35. 0096: CC(22): Received NOTIF, lightpath 0: OFF, sending further upstream. . .
35. 0096: CC(22): Received NOTIF, lightpath 1: OFF, sending further upstream. . .
35. 0124: CC (18): Received NOTIF, I am INGRESS, lightpath 0: OFF.
35. 0124: CC(18): Initiating lightpath 10 —> 12, outgoing port found, wavelength found.
35. 0124: CC(18): Sending PATH downstream. . .
35. 0124: CC(18): Received NOTIF, I am INGRESS, lightpath 1: OFF.
35. 0124: CC(18): Initiating lightpath 11 —> 13, outgoing port found, wavelength found.
35. 0124: CC(18): Sending PATH downstream. . .
35. 0153: CC(17): Received PATH, outgoing port found, wavelength found.
35. 0153: CC(17): Sending PATH downstream. . .
35. 0153: CC(17): Received PATH, outgoing port found, wavelength found.
35. 0153: CC(17): Sending PATH downstream. . .
35. 0182: CC(21): Received PATH, outgoing port found, wavelength found.
35. 0182: CC(21): Sending PATH downstream. . .
35. 0182: CC(21): Received PATH, outgoing port found, wavelength found.
35. 0182: CC(21): Sending PATH downstream. . .
35. 0211: CC(25): Received PATH, outgoing port found, it is electrical, we are EGRESS.
35. 0211: CC(25): Sending RESV_CONF upstream. . .
35. 0211: CC(25): Received PATH, outgoing port found, it is electrical, we are EGRESS.
35. 0211: CC(25): Sending RESV_CONF upstream. . .
35. 0240: CC(21): Received RESV_CONF, forwarding RESV_CONF upstream. . .
35. 0240: CC(21): Received RESV_CONF, forwarding RESV_CONF upstream. . .
35. 0268: CC(17): Received RESV_CONF, forwarding RESV_CONF upstream. . .
35. 0268: CC(17): Received RESV_CONF, forwarding RESV_CONF upstream. . .
35. 0297: CC(18): Received RESV_CONF, forwarding RESV_CONF upstream. . .
35. 0297: CC(18): Received RESV_CONF, lightpath from 11 to 13 CREATED!
```

Από τα προηγούμενα, φαίνεται οτι πλεονεκτεί ο μηχανισμός προστασίας –Protection Mechanism όπως υλοποιείται από τον εξομοιωτή GLASS, τόσο από άποψη failure resilience όσο και restoration efficiency έναντι του σχήματος Restoration που λειτουργεί σαν προεπιλεγμένος μηχανισμός προστασίας στον NS–2. Ωστόσο, εάν λάβουμε υπόψιν μας έναν Βελτιώμενο Μηχανισμό Αποκατάστασης στον NS–2 **(Κεφάλαιο 7)**, τότε μάλλον υπάρχει μεγαλύτερο πλεονέκτημα στον τελευταίο, καθώτι λαμβάνονται υπόψιν οι τωρινές συνθήκες στο δίκτυο (link delay) για την επιλογή ενός ακόμη πιο βέλτιστου μονοπατιού. Μάλιστα κατορθωνουμε να υλοποιήσουμε σε αυτόν και τους τέσσερις μηχανισμούς προστασίας του GMPLS καθιστώντας την λειτουργικότητα του εξομοιωτή NS σχεδόν εφάμιλλη του GLASS ως προς την ικανότητα παροχής προστασίας από αστοχίες.

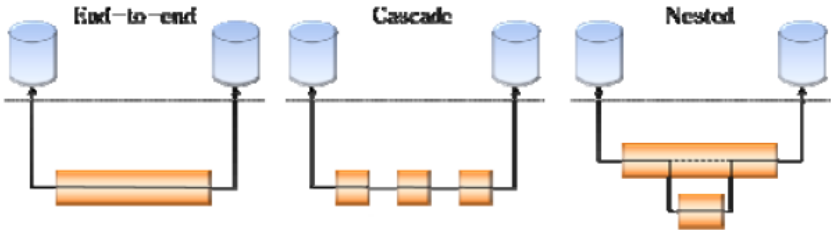
ΚΕΦΑΛΑΙΟ 7: ΠΑΡΟΥΣΙΑΣΗ ΝΕΟΥ LINK-DELAY CONSTRAINED ΑΛΓΟΡΙΘΜΟΥ ΑΠΟΚΑΤΑΣΤΑΣΗΣ

7.1 ΠΑΡΟΥΣΙΑΣΗ ΝΕΟΥ LINK-DELAY CONSTRAINED ΑΛΓΟΡΙΘΜΟΥ ΑΠΟΚΑΤΑΣΤΑΣΗΣ

Όπως είδαμε και στο θεωρητικό κομμάτι της εργασίας, το Generalized MPLS (GMPLS) framework προσφέρει ταχύτατους μηχανισμούς για αποκατάσταση από αστοχίες μέσω της εγκαθίδρυσης λειτουργικών Label Switched Paths ως backup paths. Με αυτά τα μονοπάτια προστασίας η κίνηση μπορεί πάντοτε να ανακατευθύνεται έπειτα από βλάβη δικτύου.

Το αντικείμενο του παρόντος κεφαλαίου είναι η βελτίωση ορισμένων από τους υπάρχοντες μηχανισμούς προστασίας του MPLS/GMPLS, ώστε να υποστηρίζονται ομαλά οι απαιτήσεις προστασίας των νέων υπηρεσιών Internet. Θα εξεταστούν πειραματικά πρώτα σε επίπεδο περιβάλλοντος εξομοίωσης NS–2 οι προκαθορισμένοι μηχανισμοί προστασίας – Protection Mechanisms του GMPLS όπως 1+1, 1:1, 1+N, και M:N, στα πλαίσια του εξειδικευμένου για το συγκεκριμένο πρωτόκολλο περιβάλλοντος **ASONS**. Έπειτα, προτείνεται ένας βελτιωμένος μηχανισμός αποκατάστασης –Restoration Mechanism για το Generalized, ο οποίος εξομοιώνεται πλήρως στον κώδικα του **ASONS** περιβάλλοντος και που κάνει χρήση της καθυστέρησης γραμμής –link delay, ως QoS constraint, σαν εναλλακτική παράμετρος καθορισμού βέλτιστου μονοπατιού με σκοπό την αύξηση του resilience και της ταχύτητας αποκατάστασης. Θα εξεταστεί η ακρίβεια του νέου μηχανισμού με συγκεκριμένες πειραματικές μετρήσεις και αξιολόγησή τους.

Η δικτυακή βιωσιμότητα **–Network Survivability** υποδυκνείει τον βαθμό του κατά πόσο μια υπηρεσία είναι σε θέση να αντέχει σε δικτυακές αστοχίες στα WDM/ROADM/PXC–βασισμένα δίκτυα. Αυτή ακριβώς μπορεί να κατηγοριοποιηθεί στα τρία ακόλουθα σχήματα:



Εικόνα 150. Σχήματα Network Survivability

1. **End–to–End:** Κάνει χρήση ενός μόνο σχήματος βιωσιμότητας.
2. **Cascaded:** Χρησιμοποιεί πολλά σχήματα βιωσιμότητας σειριακά. Εδώ, κάθε επιμέρους σχήμα περιέχει ένα αντικείμενο που χειρίζεται αστοχίες σε έναν συγκεριμένο sub–domain.
3. **Nested:** Πολλαπλοί μηχανισμοί βιωσιμότητας λειτουργούν κάτω από έναν συγκεκριμένο sub–domain. Λειτουργούν σε cascaded ή end–to–end μορφές.

Το συχνό φαινόμενο της αποσύνδεσης οπτικών καλωδίων και η αναπόφευκτη απώλεια πακέτων εξαιτίας αυτού του γεγονότος έχουν αυξήσει την απαίτηση να λαμβάνονται σοβαρά υπόψιν κατά το σχεδιασμό του δικτύου οι διάφοροι μηχανισμοί βιωσιμότητας. Οι δικτυακές αστοχίες κατηγοριοποιούνται είτε σαν βλάβη γραμμής ή βλάβη κόμβου. Όταν συμβεί μια αστοχία στο κυρίως μονοπάτι, η ανάκαμψη γίνεται με την παραμετροποίηση ενός backup μονοπατιού ώστε να αποκατασταθεί το κυρίως μονοπάτι στην αρχική κατάσταση. Τα σχήματα ανάκαμψης διακρίνονται σε προστασίας και αποκατάστασης.

Μηχανισμοί Προστασίας – Protection Mechanisms

(1) 1 + 1 προστασία. Η 1+1 προστασία καθορίζει ένα backup μονοπάτι το οποίο διαθέτει τους ίδιους πόρους με το κυρίως μονοπάτι και όταν η κίνηση στέλνεται στο κυρίως path, η ίδια ακριβώς στέλνεται επίσης και στο backup ταυτόχρονα. Κατά συνέπεια η παραμετροποίηση του κυρίως μονοπατιού απαιτεί διπλάσιους δικτυακούς πόρους, μειώνοντας την αποτελεσματικότητα χρήσης των πόρων αλλά προσφέροντας προστασία απέναντι σε απώλεια πακέτων και αστοχίες.

(2) 1 : 1 προστασία. Παρομοίως με το προηγούμενο σχήμα, παραμετροποιείται ένα backup μονοπάτι ίδιο ακριβώς με το κυρίως (ως προς τους πόρους), αλλά η κίνηση, τώρα, αποστέλεται μόνο από το κυρίως και όχι από το εναλλακτικό path. Όταν συμβεί μια αστοχία στο κυρίως μονοπάτι, ένα μήνυμα λαμβάνεται από τον κόμβο που ανίχνευσε την βλάβη και η κίνηση στέλνεται στο εναλλακτικό μονοπάτι, κάτι που μειώνει αισθητά την απώλεια πακέτων.

(3) 1 + N προστασία. Σε αυτή τη περίπτωση ένα μοναδικό μονοπάτι προσφέρει προστασία σε πολλά κυρίως paths. Μέσω της υποστήριξης πολλαπλών κυρίως μονοπατιών με ένα μοναδικό backup path, η χρήση πόρων βελτιστοποιείται, αλλά η δέσμευση είναι οτι το LSR μετάδοσης και το LSR λήψης πρέπει να είναι το ίδιο και ότι μόνο ένα κυρίως μονοπάτι μπορεί να ανακαμφθεί όταν συμβεί μια αστοχία σε δύο ή περισσότερα κυρίως από αυτά μονοπάτια.

(4) M : N προστασία. Το σχήμα στο οποίο M αριθμός από backup μονοπάτια και N αριθμός από κυρίως παραμετροποιούνται με τέτοιο τρόπο ώστε οποιαδήποτε αριθμός των εναλλακτικών μονοπατιών να προστατεύει οποιαδήποτε αριθμό κυρίως μονοπατιών. Θα υπάρχει σίγουρα σπατάλη πόρων εφόσον εναλλακτικά μονοπάτια δε θα χρησιμοποιούνται μέχρι να συμβεί η αστοχία.

Αυτοί οι μηχανισμοί κάνουν χρήση προκαθορισμένων backup μονοπατιών και ένα ή περισσότερα οπτικά μονοπάτια προστασίας προκαθορίζονται για ένα ή περισσότερα κυρίως μονοπάτια.

Μηχανισμοί Αποκατάστασης – Restoration Mechanisms.

Είναι μια μέθοδος στην οποία η χρησιμοποίηση των οπτικών πόρων του δικτύου αυξάνεται μέσω της παραμετροποίησης ενός backup μονοπατιού , σε περίπτωση αστοχίας, και ενός νέου μονοπατιού, μετά από την εμφάνιση της βλάβης αυτής. Παρότι ο μηχανισμός αποκατάστασης προσφέρει αποτελεσματική χρήση πόρων μέσω της μη άμεσης δημιουργίας προκαθορισμένου μονοπατιού, διατηρεί έναν αργότερο μηχανισμό ανάκαμψης σε σύγκριση με τα προηγούμενα σχήματα εξαιτείας του καθορισμού του backup μονοπατιού μετά την πρόκληση της αστοχίας. Το πλεονέκτημα του ωστόσο είναι οτι ο αλγόριθμος δρομολόγησης μπορεί να προσαρμόζει το δίκτυο επαρκώς στις διάφορες αλλαγές και συνθήκες και να υπολογίζεται το backup μονοπάτι αναλόγως.

Εξετάζουμε στη συνέχεια θεωρητικά τον βελτιωμένο μηχανισμό Restoration. Η φιλοσοφία του βασίζεται σε έναν link state αλγόριθμο επιλογής βέλτιστου backup μονοπατιού. Κατά την παραμετροποίηση του εναλλακτικού μονοπατιού, ο link state αλγόριθμος επιλέγει το path βασισμένο στις απαιτήσεις εύρους ζώνης και κόστους της κίνησης. Όταν η απόδοση μιας συγκεκριμένης γραμμής είναι ανώτερη από άλλες γειτονικές, η σύνδεση θα αφοσιωθεί σε εκείνη τη συγκεκριμένη γραμμή. Μια δεδομένη σύνδεση που έχει πολλά οπτικά μονοπάτια σημαίνει οτι περνάει πάνω της μεγάλη κίνηση, και μια ενδεχόμενη αστοχία σε εκείνη τη σύνδεση θα ήταν περισσότερο καταστροφική για το δίκτυο από τις υπόλοιπες γειτονικές. Αρα συμπεραίνουμε οτι περισσότερες συνδέσεις σε μια γραμμή σημαίνει και αντίστοιχα και υψηλότερη πιθανότητα αστοχίας, κάτι που οδηγεί σε αύξηση του αριθμού μονοπατιών προστασίας μειώνοντας έτσι την απόδοση του δικτύου. Στη περίπτωση μας το στοιχείο εκείνο που θα μας οδηγήσει να συγκρίνουμε την απόδοση γειτονικών γραμμών είναι το **link delay –καθυστέρηση γραμμής**.

Ο κύριος σκοπός ενός αλγορίθμου δρομολόγησης είναι να εντοπίσει ένα επαρκές μονοπάτι από άποψη εύρους ζώνης και QoS περιορισμών ώστε να επιτύχει ικανοποιητική εκμετάλλευση των διαθέσιμων πόρων. Για την βελτιστοποίηση της δικτυακής απόδοσης, οι QoS αλγόριθμοι δρομολόγησης χρησιμοποιούν δύο τεχνικές. Η πρώτη είναι να επιλέξουν το μονοπάτι εκείνο με τον μικρότερο αριθμό hops, άρα το συντομότερο, με σκοπό την μείωση της κατανάλωσης των πόρων, και η δεύτερη είναι να εξισορροπήσουν το φορτίο στο δίκτυο με αποτέλεσμα να επιλέγεται το λιγότερο φορτωμένο μονοπάτι. Ένα μονοπάτι με το μικρότερο μήκος δεν σημαίνει κατ'ανάγκην οτι είναι και το βέλτιστο από άποψη διαχείρισης πόρων και μετρικών QoS. Το γεγονός αυτό έχει άμεσο αντίκτυπο στην επιλογή του αλγορίθμου δρομολόγησής μας. **Προτείνεται στην συγκεκριμένη περίπτωση να επιλέγεται το μονοπάτι(α) εκείνο που ανάμεσα σε όλα τα υπόλοιπα ικανοποιεί σε μεγαλύτερο βαθμό κάποιο TE constraint , όπως link delay, bandwidth, jitter, κ.τ.π. , και έπειτα μέσω του αλγορίθμου δρομολόγησης Dijkstra να καθορίζεται από τα υποψήφια αυτά μονοπάτια το τελικό optimal backup path. Το επιπλέον backup μονοπάτι(α), σε ενδεχόμενη νέα αστοχία, θα επιλέγεται ως το disjoint του προηγούμενου**.

Ως γνωστόν, το εγγυημένο επίπεδο ποιότητας υπηρεσιών –Quality of Service (QoS) της μεταδιδόμενης κίνησης είναι ένας καθοριστικός παράγοντας για τον υπολογισμό του αντίκτυπου της αστοχίας στο δίκτυο. Προτείνεται να διαιρεθεί σε δύο συστατικά: τον χρόνο αποκατάστασης –recovery time και απώλεια πακέτων –packet loss. Κάθε μηχανισμός αποκατάστασης προσφέρει διαφορετικά επίπεδα recovery time. Προτείνεται η κατηγοριοποίηση της Εικόνας 151.

Level of protection	Recovery Time (T_{REC})
Very low	> 1 min
Low	200 ms – 1 min
Medium	50 ms – 200 ms
High	20 ms – 50 ms
Very High	< 20 ms

Εικόνα 151. Κατηγοριοποίηση των χρόνων αποκατάστασης

Όπως βλέπουμε και στην Εικόνα, ορισμένοι μηχανισμοί αποκατάστασης στο GMPLS, ανάλογα πάντα με τον τρόπο που γίνονται λειτουργικοί στο δίκτυο καθώς και τον τύπο της δικτυακής βιωσιμότητας που εφαρμόζεται, διαθέτουν μεγάλους έως και πολύ μεγάλους χρόνους επανάκτησης. Κάθε ένας από αυτούς τους χρόνους βέβαια εξαρτάται και από τις εκάστοτε συνθήκες στο δίκτυο, π.χ. τύπο αστοχίας και συχνότητά της, διάρκεια αστοχίας, τις όποιες παραμετροποίησεις κάνουμε σε ζητήματα ανάκαμψης, αλλά και τον εκάστοτε εξοπλισμό GMPLS που χρησιμοποιούμε.

Στα MPLS–based δίκτυα η πιό συνηθισμένη μέθοδος για επανάκτηση μετά από αστοχία είναι η χρησιμοποίηση ενός εναλλακτικού και διαδοχικού μονοπατιού στο κυρίως μονοπάτι. Η εγκαθίδρυση του μπορεί να γίνει με πολλούς διαφορετικούς τρόπους. Στην Εικόνα 152 διακρίνουμε τις φάσεις αποκατάστασης μετά από αστοχία σε ένα GMPLS δίκτυο, καθώς και μια συνοπτική εξήγησή τους. Αυτές οι μέθοδοι μπορούν να είναι προκαθορισμένα (pre–routed και pre–signaled) backup μονοπάτια ή από την άλλη μια δυναμική εγκαθίδρυσή τους, για παράδειγμα μετά από την πρόκληση της αστοχίας. Οι πόροι μπορούν να κατανεμένονται a priori, ή αλλιώς, στην περίπτωση των δυναμικών σχημάτων, μετά την εμφάνιση της αστοχίας. Ολόκληρος ο κύκλος αποκατάστασης ξεκινάει μόλις ανιχνευτεί η αστοχία και ολοκληρώνεται όταν η κίνηση έχει αποκατασταθεί πίσω στο αρχικό λειτουργικό μονοπάτι (διαδικασία κανονικοποίησης).

Κατά συνέπεια, ο συνολικός χρόνος αποκατάστασης T_{REC_N} από την στιγμή που λαμβάνει χώρα μια αστοχία μέχρι να αποκατασταθεί πλήρως η κίνηση στο αρχικό μονοπάτι προκύπτει από τον ακόλουθο τύπο:

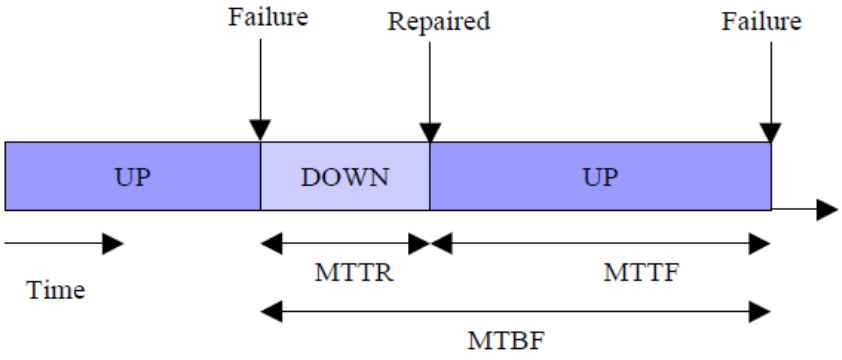
$$T_{REC\_N} = T_{DET} + T_{HOF} + T_{NOT} + T_{BR} + T_{BS} + T_{BA} + T_{SW} + T_{CR} + T_{RDET} + T_{RNOT} + T_{SWB}$$

Κατά την διάρκεια αυτής της διαδικασίας επανάκτησης υπάρχει μια αναπόφευκτη απώλεια πακέτων. Ωστόσο ο βαθμός αυτής της απώλειας δεν είναι ανάλογος του προηγούμενου τύπου. Μόλις συμβεί μια αστοχία, τα πακέτα χάνονται μέχρι η κίνηση να γίνει switched στο αρχικό μονοπάτι. Το χρονικό αυτό διάστημα T_{REC_PL} υπολογίζεται ως εξής:

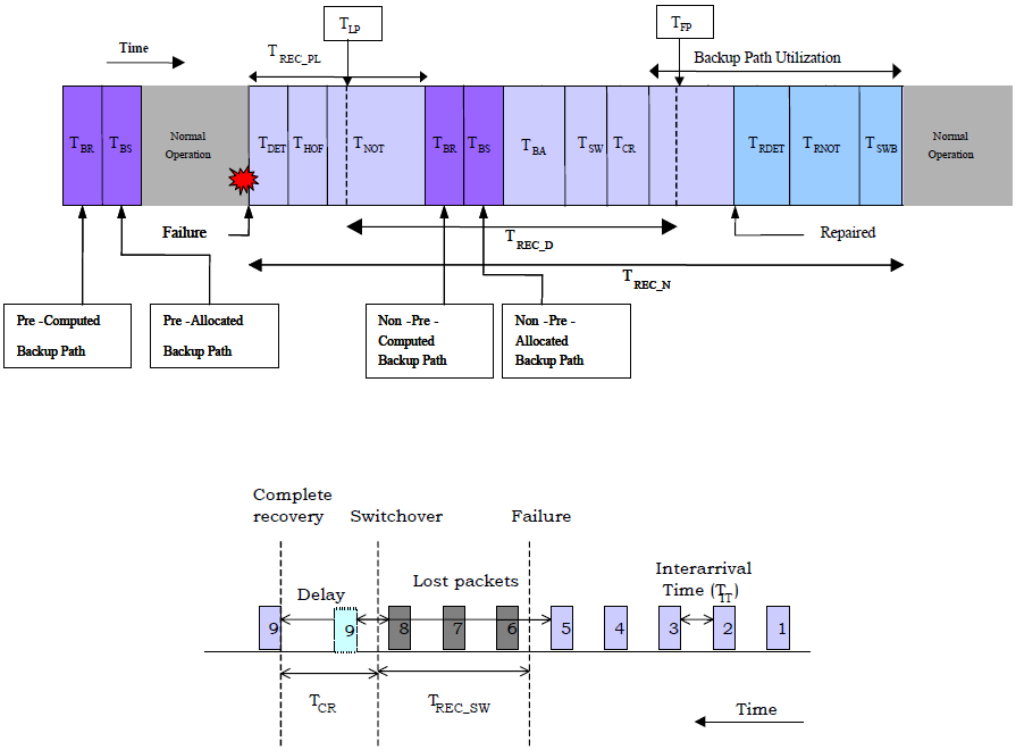
$$T_{REC\_PL} = T_{DET} + T_{HOF} + T_{NOT}$$

Ουσιαστικά η απώλεια πακέτων (P_{LS}) είναι ευθέως ανάλογη του T_{REC_PL} και του Transmission Rate (R_{TR}). Εαν μάλιστα λάβουμε υπόψιν και την απώλεια πακέτων στην γραμμή που έχει καταρρεύσει P_{FL}, παίρνουμε τον ακόλουθο τύπο:

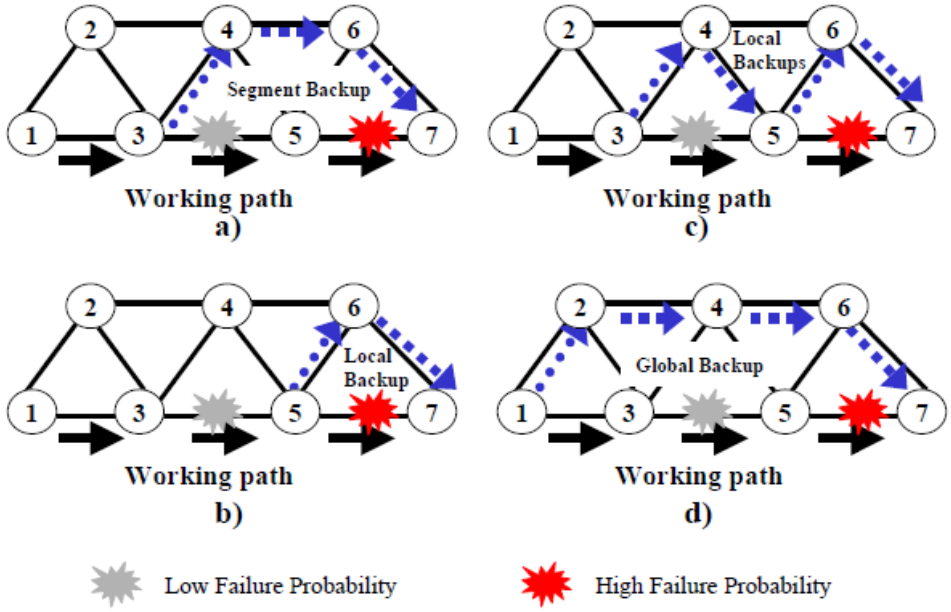
$$P_{LS} = R_{TR} \cdot T_{REC\_PL} + P_{FL}$$



Εικόνα 152. Η διαδικασία ανανέωσης

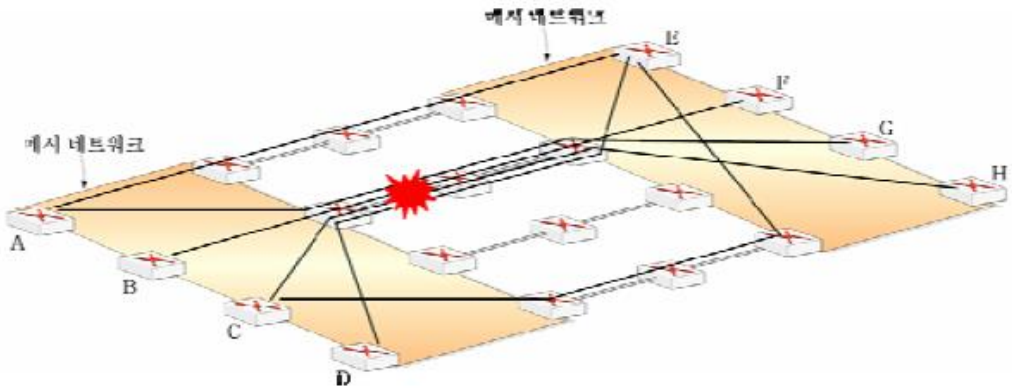


Εικόνα 153. Η χρονική εξέλιξη της διαδικασίας αποκατάστασης



Εικόνα 154. Σημεία με υψηλότερη συχνότητα αστοχίας

Στην Εικόνα 155 διακρίνουμε την περίπτωση όπου περισσότερες από μια συνδέσεις περνούν πάνω από μια γραμμή. Όπως επισημάναμε και προηγουμένως όσο περισσότερες συνδέσεις σε μία γραμμή τόσο πιό καταστροφικά τα αποτελέσματα σε ενδεχόμενο δικτυακής αστοχίας.

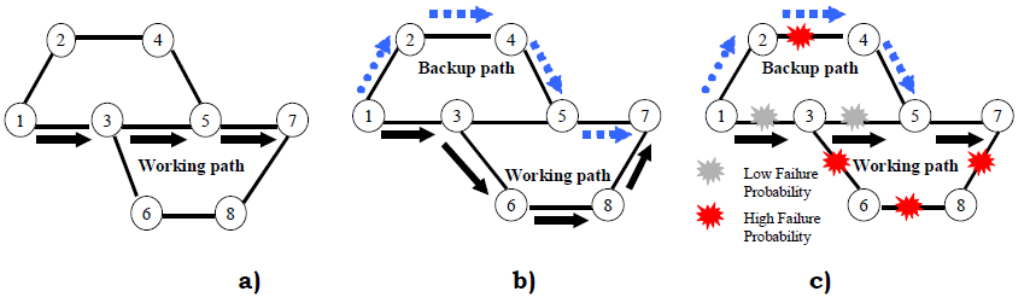


Εικόνα 155. Βλάβη σε μονοπάτι με πολλές συνδέσεις

Acronym	Component	Description
T_{DET}	Failure detection time	The time required to detect the fault (for instance, an alarm from lower levels or a 'hello' protocol)
T_{HOP}	Hold-off time	The time required to allow failure recovery at lower layer mechanisms (if necessary)
T_{NOT}	Failure notification time	The time required to inform (i.e. signaling-based or flooding-based notification) the node responsible for switchover
T_{BR}	Backup routing time	The time required for new backup creation, routing (TBR) and signaling (TBS)
T_{BS}	Backup signaling time	
T_{BA}	Backup Activation	The time required to activate (signaling/cross connection) the backup path before the switchover
T_{SW}	Switchover time	The time required for traffic switchover from the active path to the backup path
T_{CR}	Complete recovery time	The time required to complete the fault recovery (the time it takes the first packet to arrive from the backup path to the egress node)
T_{RDET}	Initial path recovery detection time	The time required to detect the working path restoration (time for the WP recovery detection)
T_{RNOT}	Initial path recovery notification time	The time required to notify of the working path recovery (time for the WP recovery notification)
T_{SWB}	Switchback time	The time required to switch the traffic back from the backup path to the working path

Εικόνα 156. Περιγραφή συστατικών διαδιακασίας αποκατάστασης

Η διαδικασία του νέου μηχανισμού Restoration στην περίπτωσή μας βασίζεται στην εγκαθίδρυση του εναλλακτικού μονοπατιού, κάτι που μπορεί να γίνει σε δύο φάσεις: Πρώτα υπολογίζεται το backup διαδοχικό μονοπάτι που ικανοποιεί το QoS constraint του μικρότερου link delay και στη συνέχεια μέσω ενός αλγορίθμου δρομολόγησης κατασκευάζεται. Αποδυκνείεται πειραματικά οτι **είναι προτιμότερο από άποψη απόδοσης και ανθεκτικότητας σε αστοχίες να επιλέγουμε ως εναλλακτικό μονοπάτι αυτό που ικανοποιεί κάποια QoS constraints και δεν είναι κατ'ανάγκην το μικρότερου μήκους, παρά να επιλέγουμε το συντομότερο μονοπάτι με χειρότερα επίπεδα Traffic Engineering.** Ο ισχυρισμός αυτός επιβεβαιώνεται με την Εικόνα 157.



Εικόνα 157. Καθορισμός disjoint paths

Ουσιαστικά κάνουμε χρήση ενός constraint–based αλγορίθμου δρομολόγησης ο οποίος καθορίζει το βέλτιστο backup μονοπάτι, αμέσως μετά την εμφάνιση της αστοχίας, βάσει του βαθμού ικανοποίησης ορισμένων ΤΕ μετρικών (στην περίπτωση μας του link delay), και όχι μόνο του συντομότερου μήκους του. **Ουσιαστικά για κάθε (οπτικό) σύνδεσμο l ενός κόμβου ελέγχεται ποιός έχει το μικρότερο έως εκείνη τη στιγμή delay, και στη συνέχεια με τη βοήθεια του τροποποιημένου αλγορίθμου Dijkstra επιλέγεται εκείνος ο σύνδεσμος με τη μικρότερη καθυστέρηση και αποκλείονται όλοι οι υπόλοιποι γειτονικοί του**. Η διαδικασία αυτή επαναλαμβάνεται σε κάθε κόμβο hop από τη πηγή μέχρι τον προορισμό, καθώς οι δύο ρουτίνες (Link_Delay_Constraint_Search και Dijkstra) καλούνται αναδρομικά σε κάθε κόμβο. Έτσι σταδιακά χτίζεται το μονοπάτι. Η διαδικασία αυτή περιγράφεται στη συνέχεια με τη μορφή ψευδοκώδικα:

```
L ←—— Set of Links (l)

Function Link_Delay_Constraint_Search(L)

1.  FOR each link l in L
2.    IF l has many connections
3.      L := L substraction {l}
4.    END IF
5.  END FOR

Return L

End
```

Εικόνα 158. Αναζήτηση συνδέσμων που ικανοποιούν κάποια constraints

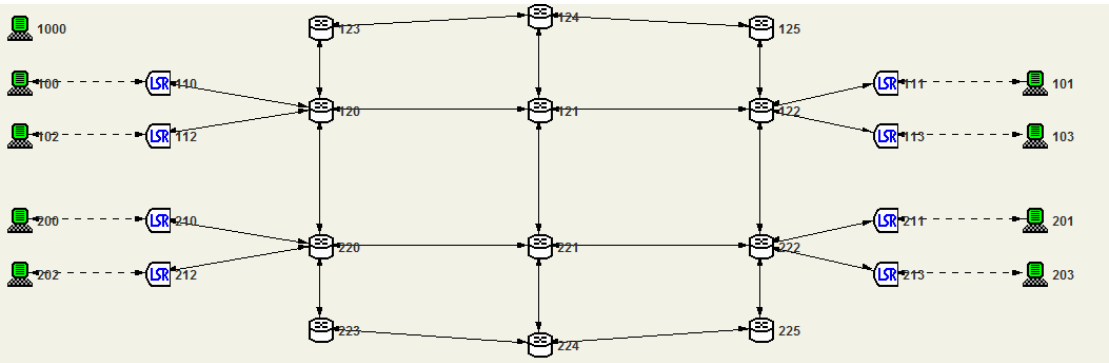
```
L <- The set of Links(l)
P <- The set of Paths
t <- Destination

Function Dijkstra(G, w, s, t)
1. FOR each vertax v in V[G]
2.          d[v] := infinity
3.          previous[v] := undefined
4.       d[s] := 0
5.       S := empty set
6.       Q := set of all vertices
7.       L := Constraint_set (Q)
8.       WHILE L is not an empty set
9.            u := Path_Num_Min(L)
10.           S := S union {u}
11.           FOR each edge (u,v) outgoing from u
12.                IF d[v] > d[u] + w(u,v)
13.                     d[v] := d[u] + w(u,v)
14.                          previous[v] := u
15.           END IF
16.         END FOR
17.           IF u = t
18.             P := empty sequence
19.             n := t
20.                  WHILE defined n in S
21.                     insert n to the beginning of P
22.                     n := previous[n]
23.               END WHILE
24.                    Return P
25.         END IF
26.     END WHILE
27. END FOR
END
```

Εικόνα 159. Τροποποιημένος Αλγορίθμος Dijkstra

Παρουσιάζουμε στη συνέχεια τις πειραματικές μας μετρήσεις και την αξιολόγησή τους. Χρησιμοποιούμε την πλατφόρμα της Αρχιτεκτονικής **ASONS** στο περιβάλλον του **NS–2.1b9a**, αφού φυσικά προβούμε στις απαραίτητες τροποποιήσεις στο κώδικα του **ASONS** patch αλλά και στον πυρήνα του ns–2.

Η ακολουθούμενη τοπολογία στον NS–2 παρουσιάζεται στην Εικόνα 160.



Εικόνα 160. Η δικτυακή τοπολογία των πειραμάτων μας

Τα πειράματα διαρκούν **10 sec**, η μετάδοση της κίνησης ξεκινάει στο **1ο sec**, ενώ στα **5 sec** συμβαίνει αστοχία οπτικής σύνδεσης. Από κεί και πέρα ενεργοποιούνται οι αντίστοιχοι μηχανισμοί προστασίας και αποκατάστασης με σκοπό την άμεση επανάκαμψη της κίνησης. Εξετάζουμε τους ακριβείς χρόνους αποκτάστασης σε κάθε πείραμα για την αξιολόγηση κάθε μηχανισμού.

Έτσι, εκτελούμε το παραπάνω δικτυακό γράφημα σε 5 διαδοχικά σενάρια:

(α) – Αξιολόγηση του μηχανισμού προστασίας 1 + 1.

(b) – Αξιολόγηση του μηχανισμού προστασίας 1 : 1.

(c) – Αξιολόγηση του μηχανισμού προστασίας 1 + N.

(d) – Αξιολόγηση του μηχανισμού προστασίας M : N.

(e) – Αξιολόγηση του βελτιωμένου μηχανισμού Restoration (Constraint–based Restoration Scheme).

[A] 1 + 1 Protection Scheme

Τυπικά, και στη πρώτη αυτή περίπτωση επιλέγεται με τον ίδιο τρόπο (μονοπάτι με το κριτήριο του ελάχιστου delay) ένα προκαθορισμένο –pre–established backup path ως διαδοχικό –disjoint του κυρίως λειτουργικού. Όταν συμβεί η αστοχία, απλώς η κίνηση ακολουθείται από το εναλλακτικό path και έτσι δεν προβαίνουμε σε διαδικασίες δημιουργίας νέου lightpath που θα προκαλούσαν περισσότερη επιβάρυνση και απώλεια πακέτων. Στο σενάριο μας επιλέγεται να λειτουργήσει 1 κυρίως οπτικό μονοπάτι: **200 101**. Η αστοχία συμβαίνει στον οπτικό σύνδεσμο **220 (node 18) 221 (node 22)**. **Συμπερασματικά, ο χρόνος αποκατάστασης είναι άμεσος:**

5. 0026: CC(18): Failure detected downstream, I am INGRESS, no NOTIF.

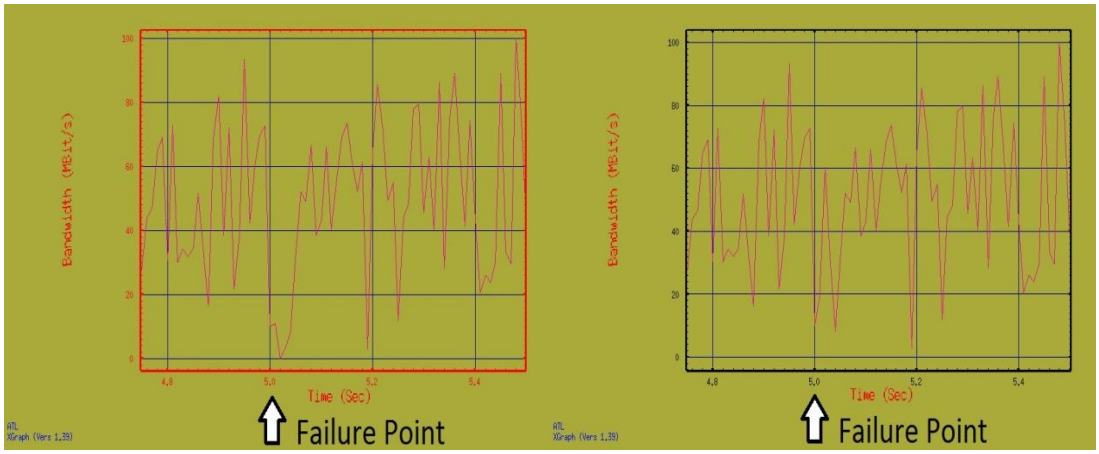
5. 0026: CC(18): Following Backup lightpath 10 —> 12. (1+1 Protection Scheme)

5. 0026: CC(22): Failure detected upstream, lightpath 0: OFF, sent NOTIF downstream. . .

5. 0052: CC(26): Received NOTIF, lightpath 0: OFF, sending further downstream. . .

5. 0078: CC(25): Received NOTIF, lightpath 0: OFF, sending further downstream. . .

5. 0103: CC(24): Received NOTIF, I am EGRESS, lightpath 0: OFF.



(a) **(b)**

Εικόνα 161. Σύγκριση Bandwidth meters ανάμεσα στον νέο μηχανισμό προστασίας 1+1 (b) και τον προκαθορισμένο του ASONS (a)

[B] 1 : 1 Protection Scheme

Στη δεύτερη αυτή περίπτωση, αμέσως μετά την αστοχία [**220 (node 18)** με **221(node 22)**] η κίνηση γίνεται switched στο backup μονοπάτι. Παρατηρούμε οτι η διαδικασία αποκατάστασης είναι άμεση, όπως μάλιστα βλέπουμε στο debug του ns–2, καθώς η κίνηση στο εναλλακτικό μονοπάτι απλώς ενεργοποιείται με την εντολή: **n_. sm(). setRecord(ON, newlpid_)**, από τότε που θα προκληθεί η βλάβη, αντί να προβούμε στη διαδικασία δημιουργίας νέου LightPath. Τα στοιχεία της κίνησης και τα μονοπάτια είναι ακριβώς ίδια με το προηγούμενο σενάριο.

5. 0047: CC(18): Failure detected downstream, I am INGRESS, no NOTIF.

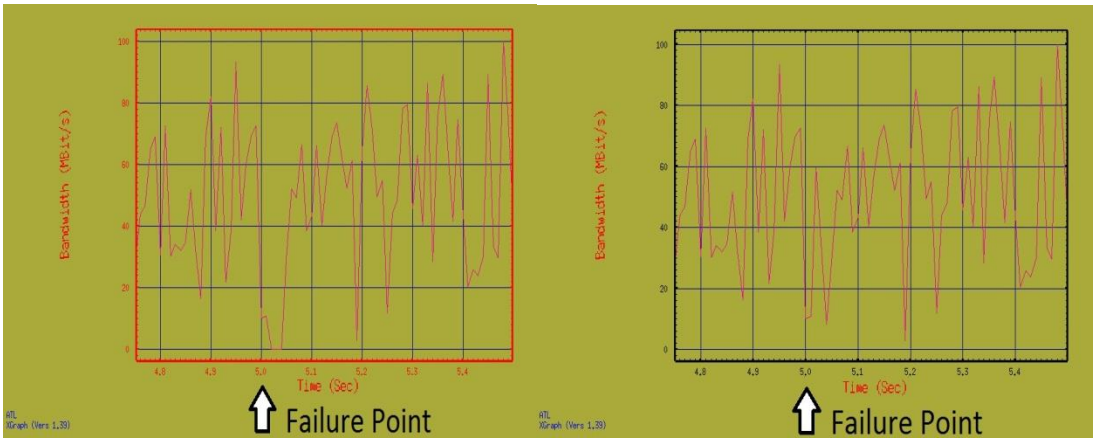
5. 0047: CC(18): Following Backup lightpath 10 —> 12. (1:1 Protection Scheme)

5. 0047: CC(22): Failure detected upstream, lightpath 0: OFF, sent NOTIF downstream. . .

5. 0095: CC(26): Received NOTIF, lightpath 0: OFF, sending further downstream. . .

5. 0142: CC(25): Received NOTIF, lightpath 0: OFF, sending further downstream. . .

5. 0186: CC(24): Received NOTIF, I am EGRESS, lightpath 0: OFF.



(a) **(b)**

Εικόνα 162. Σύγκριση Bandwidth meters ανάμεσα στον νέο μηχανισμό προστασίας 1:1 (b) και τον προκαθορισμένο του ASONS (a)

[C] 1 + N Protection Scheme

Έχοντας τώρα δύο διαφορετικές ροές δεδομένων (**200 101** και **202 103**) και οπτικά μονοπάτια αντίστοιχα, με ακριβώς το ίδιο σημείο αστοχίας με τα προηγούμενα 2 σενάρια, επιλέγουμε ένα μόνο προκαθορισμένο backup path ως disjoint των προηγούμενων, και μόλις εμφανιστεί η αστοχία και πάλι η κίνηση περνάει –switched στο εναλλακτικό μονοπάτι. Αυτή τη φορά ο χρόνος αποκατάστασης άμεσος.

5. 0043: CC(18): Failure detected downstream, I am INGRESS, no NOTIF.

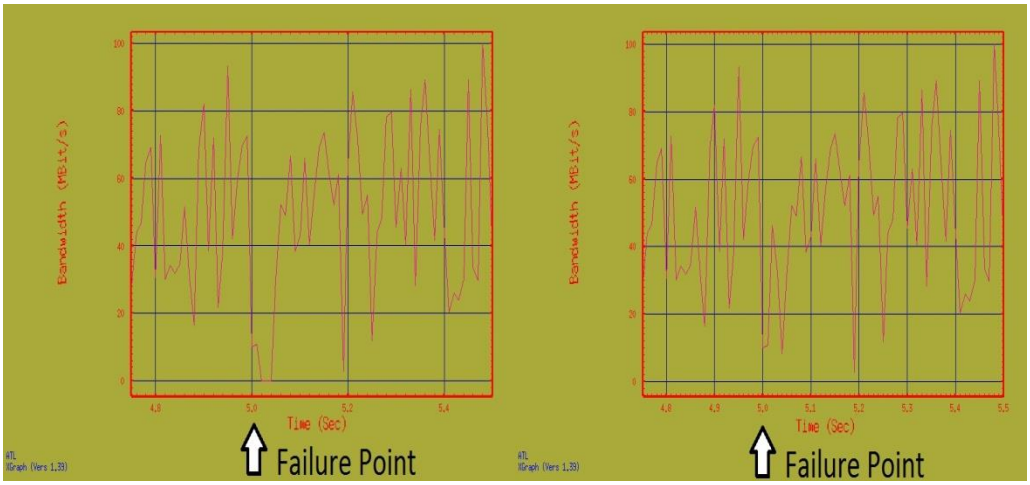
5. 0043: CC(18): Following Backup lightpath 10 —> 12. (1+N Protection Scheme)

5. 0043: CC(22): Failure detected upstream, lightpath 0: OFF, sent NOTIF downstream. . .

5. 0085: CC(26): Received NOTIF, lightpath 0: OFF, sending further downstream. . .

5. 0124: CC(25): Received NOTIF, lightpath 0: OFF, sending further downstream. . .

5. 0163: CC(24): Received NOTIF, I am EGRESS, lightpath 0: OFF.



(a) **(b)**

Εικόνα 163. Σύγκριση Bandwidth meters ανάμεσα στον νέο μηχανισμό προστασίας 1+N (b) και τον προκαθορισμένο του ASONS (a)

[D] M : N Protection Scheme

Έχοντας **N = 3** κυρίως οπτικά μονοπάτια [**100 – 101**, **200 – 101** , **202 – 101**] και **M = 2** εναλλακτικά, παρατηρούμε οτι τώρα η διαδικασία αποκατάστασης ξανά είναι σχεδόν ακαριαία, καθώς με αστοχία στους οπτικούς συνδέσμους **220 – 221** και **223 – 224**, ακολουθούνται τα backup οπτικά μονοπάτια (0) και (1) αντίστοιχα. Αυτά ενεργοποιούνται ξανά με την εντολή **n_. sm(). setRecord()**, αντί να κατασκευάζονται από την αρχή.

5. 0044: CC(18): Failure detected downstream, I am INGRESS, no NOTIF.

5. 0044: CC(18): Initiating lightpath 10 —> 12, outgoing port found,

wavelength found.

5. 0044: CC(18): Sending PATH downstream. . .

. . .

Impossible!!!

CC(18): MPLS will be signalled when HOT expires!

5. 0044: CC(22): Failure detected upstream, lightpath 1: OFF, sent NOTIF downstream. . .

5. 0044: CC(19): Failure detected downstream, I am INGRESS, no NOTIF.

5. 0044: CC(19): Following (0) Backup lightpath 11 —> 12. (M:N Protection Scheme)

downstream, I am INGRESS, no NOTIF.

5. 0044: CC(19): Following (1) Backup lightpath 10 —> 12. (M:N Protection Scheme)

downstream, I am INGRESS, no NOTIF.

5. 0044: CC(19): Following (2) Backup lightpath 8 —> 12. (M:N Protection Scheme)

5. 0044: CC(23): Failure detected upstream, lightpath 2: OFF, sent NOTIF downstream. . .

upstream, lightpath 4: OFF, sent NOTIF downstream. . .

upstream, lightpath 5: OFF, sent NOTIF downstream. . .

5. 0089: CC(17): Received PATH, outgoing port found, wavelength found.

5. 0089: CC(17): Sending PATH downstream. . .

5. 0089: CC(26): Received NOTIF, lightpath 1: OFF, sending further downstream. . .

5. 0089: CC(27): Received NOTIF, lightpath 2: OFF, sending further downstream. . .

5. 0089: CC(27): Received NOTIF, lightpath 4: OFF, sending further downstream. . .

5. 0089: CC(27): Received NOTIF, lightpath 5: OFF, sending further downstream. . .

5. 0133: CC(21): Received PATH, outgoing port found, wavelength found.

5. 0133: CC(21): Sending PATH downstream. . .

5. 0133: CC(25): Received NOTIF, lightpath 1: OFF, sending further downstream. . .

5. 0133: CC(26): Received NOTIF, lightpath 2: OFF, sending further downstream. . .

5. 0133: CC(26): Received NOTIF, lightpath 4: OFF, sending further downstream. . .

5. 0133: CC(26): Received NOTIF, lightpath 5: OFF, sending further downstream. . .

5. 0178: CC(25): Received PATH, outgoing port found, wavelength found.

5. 0178: CC(25): Sending PATH downstream. . .

5. 0178: CC(24): Received NOTIF, I am EGRESS, lightpath 1: OFF.

5. 0178: CC(25): Received NOTIF, lightpath 2: OFF, sending further downstream. . .

5. 0178: CC(25): Received NOTIF, lightpath 4: OFF, sending further downstream. . .

5. 0178: CC(25): Received NOTIF, lightpath 5: OFF, sending further downstream. . .

5. 0223: CC(24): Received PATH, outgoing port found, it is electrical, we are EGRESS.

5. 0223: CC(24): Sending RESV_CONF upstream. . .

5. 0223: CC(24): Received NOTIF, I am EGRESS, lightpath 2: OFF.

5. 0223: CC(24): Received NOTIF, I am EGRESS, lightpath 4: OFF.

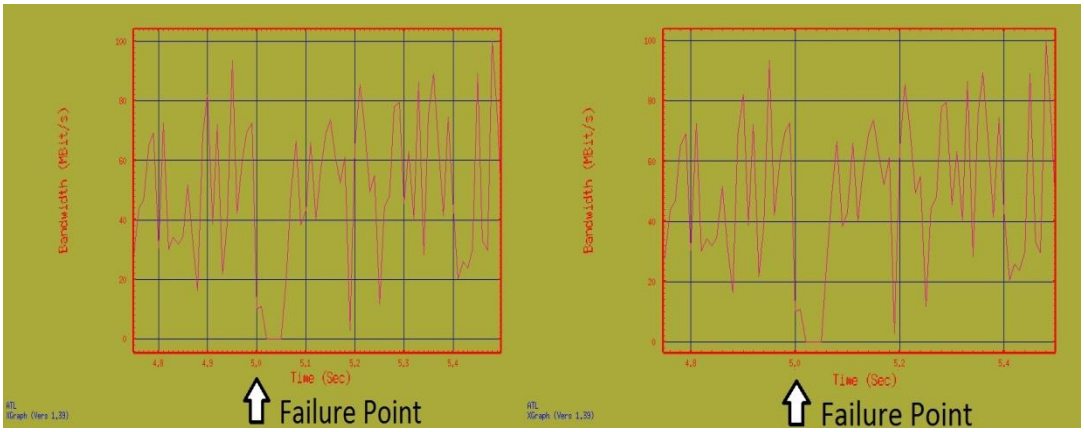
5. 0223: CC(24): Received NOTIF, I am EGRESS, lightpath 5: OFF.

5. 0267: CC(25): Received RESV_CONF, forwarding RESV_CONF upstream. . .

5. 0312: CC(21): Received RESV_CONF, forwarding RESV_CONF upstream. . .

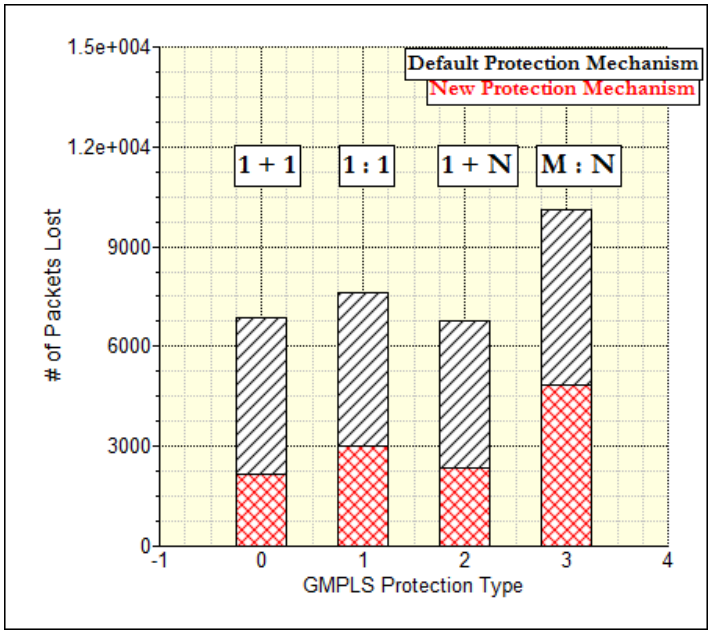
5. 0357: CC(17): Received RESV_CONF, forwarding RESV_CONF upstream. . .

5. 0401: CC(18): Received RESV_CONF, lightpath from 10 to 12 CREATED!



(a) **(b)**

Εικόνα 164. Σύγκριση Bandwidth meters ανάμεσα στον νέο μηχανισμό προστασίας M:N (b) και τον προκαθορισμένο του ASONS (a)



Εικόνα 165. Σύγκριση αριθμών απώλειας πακέτων ανάμεσα στους 4 νέους μηχανισμούς προστασίας και τον προκαθορισμένο του ASONS

[E] Improved Restoration Scheme

Τώρα, κάνουμε χρήση 6 οπτικών μονοπατιών:

[a] – **200 ◄► 202 (x 1)**

[b] – **200 ◄► 101 (x 2)**

[c] – **200 ◄► 100 (x 1)**

[c] – **200 ◄► 102 (x 2)**

Είναι προφανές οτι ο σύνδεσμος **220 – 120 θα έχει τώρα δύο διαφορετικές ροές οπτικής κίνησης, ενώ ο 220 – 221 επίσης δύο και ο 220 – 223 μόνο μία**. Από άποψη delay είναι εύλογο να θεωρήσουμε οτι την στιγμή της αστοχίας θα επιλεγεί ως βέλτιστο μονοπάτι το: **220 – 223 – 224 – 225 – 222 – 122 – 125**, και πράγματι αυτό συμβαίνει. Ο αλγόριθμος μας προσαρμόζεται στις τωρινές δικτυακές συνθήκες και υπολογίζει το μονοπάτι με τη μικρότερη καθυστέρηση. Αυτό γίνεται την χρονική στιγμή 5. 0 οπότε και καταρρέει ο σύνδεσμος **220 – 221**. Ο χρόνος αποκατάστασης κυμαίνεται στα 500 msec. Εκείνο βέβαια που είναι το σημαντικό πλεονέκτημα του **Improved Restoration Scheme** σε σχέση με όλους τους άλλους μηχανισμούς, έχει να κάνει οτι αποφεύγει τους συνδέσμους με υψηλότερη συχνότητα αστοχίας λόγω της ύπαρξης σε αυτά περισσότερων ροών κίνησης. Μάλιστα αυξάνεται η πιθανότητα πρόκλησης αστοχίας στον οπτικό σύνδεσμο 220 – 120, ο οποίος έχει δύο διαφορετικές ροές. Εαν επιλέγαμε αυτόν σαν το εναλλακτικό μονοπάτι μας θα υπήρχε σαφώς νέα κατάρρευση και άρα μεγαλύτερη απώλεια πακέτων. Αυτό ευτυχώς το αποφεύγουμε. Έτσι προσαρμοζόμαστε στις τωρινές συνθήκες στο δίκτυο και επιλέγουμε βέλτιστα QoS χαρακτηριστικά για το εναλλακτικό μας μονοπάτι.

5. 0041: CC(18): Failure detected downstream, I am INGRESS, no NOTIF.

5. 0041: CC(18): Selecting lightpath with minimum delay (QoS delay constraint). . . Might not be minimum.

. . .

5. 0041: CC(18): Lightpath with minimum delay succesfully selected.

5. 0041: CC(18): Initiating lightpath 10 —> 12, outgoing port found,

wavelength found.

5. 0041: CC(18): Sending PATH downstream. . .

. . .

Impossible!!!

CC(18): MPLS will be signalled when HOT expires!

downstream, I am INGRESS, no NOTIF.

downstream, I am INGRESS, no NOTIF.

5. 0041: CC(22): Failure detected upstream, lightpath 1: OFF, sent NOTIF downstream. . .

5. 0083: CC(19): Received PATH, outgoing port found, wavelength found.

5. 0083: CC(19): Sending PATH downstream. . .

5. 0083: CC(26): Received NOTIF, lightpath 1: OFF, sending further downstream. . .

5. 0124: CC(23): Received PATH, outgoing port found, wavelength found.

5. 0124: CC(23): Sending PATH downstream. . .

5. 0124: CC(25): Received NOTIF, lightpath 1: OFF, sending further downstream. . .

5. 0166: CC(27): Received PATH, outgoing port found, wavelength found.

5. 0166: CC(27): Sending PATH downstream. . .

5. 0166: CC(24): Received NOTIF, I am EGRESS, lightpath 1: OFF.

5. 0208: CC(26): Received PATH, outgoing port found, wavelength found.

```
5. 0208: CC(26): Sending PATH downstream. . .
5. 0249: CC(25): Received PATH, outgoing port found, wavelength found.
5. 0249: CC(25): Sending PATH downstream. . .
5. 0291: CC(24): Received PATH, outgoing port found, it is electrical, we are EGRESS.
5. 0291: CC(24): Sending RESV_CONF upstream. . .
5. 0332: CC(25): Received RESV_CONF, forwarding RESV_CONF upstream. . .
5. 0374: CC(26): Received RESV_CONF, forwarding RESV_CONF upstream. . .
5. 0416: CC(27): Received RESV_CONF, forwarding RESV_CONF upstream. . .
5. 0457: CC(23): Received RESV_CONF, forwarding RESV_CONF upstream. . .
5. 0499: CC(19): Received RESV_CONF, forwarding RESV_CONF upstream. . .
5. 0540: CC(18): Received RESV_CONF, lightpath from 10 to 12 CREATED!
```

ΚΕΦΑΛΑΙΟ 8: ΠΑΡΑΠΟΜΠΕΣ ΚΑΙ ΑΝΑΦΟΡΕΣ

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]. GMPLS Architecture And Applications By Farrel, Bryskin

[2]. GMPLS Technologies: Broadband Backbone Networks And Systems By Yamanaka, Shiomoto, Oki

[3]. Rick Gallaher's MPLS Training Guide:Building Multi Protocol Label Switching Networks

[4]. Optical Switching Networks By Martin Maier

[5]. MPLS – Enabled Applications: Emerging Developments And New Technologies By Ina Minei And Julian Lucek

[6]. Next Generation Transport Networks: Data, Management, And Control Planes By Ellanti, Gorshe , Raman, Grover

[7]. Multiwavelength Optical Networks Architectures, Design, And Control By Thomas E. Stern, Giorgios Ellinas, Krishna Bala

[8]. Optical WDM Networks By Biswanath Mukherjee

[9]. Engineering Internet QoS By Sanjay Jha, Mahbub Hassan

[10]. Traffic Grooming for Optical Networks: Foundations, Techniques and Frontiers By Rudra Dutta , Ahmed E. Kamal , George N. Rouskas

[11]. A new GMPLS Survivability Mechanism By ZengZhi, Zhao

[12]. Analysis Of The GMPLS Control Plane Security By Clement, Zavarsky, Lindskog

[13]. GMPLS Technology And Its Application In WDM Optical Network By Zhang, Bao

[14]. GMPLS Based Multi – Constrained Recovery Algorithm By Qu, Zhao

[15]. GTEP:Generalized Traffic Engineering Protocol For Multi-Layer GMPLS Networks By Shimazaki, Shiomoto

[16]. Optical CDMA For All-Optical Sub-Wavelength Switching In Core GMPLS Networks By Khattab, Alnuweiri

[17]. Performance Analysis Of Infrastructure Service Provision With GMPLS Based Traffic Engineering By Tomic, Jucan

[18]. Analysis Of GMPLS Architectures, Topologies And Algorithms By Chung, Khan, Soo , Reyes, Cho

[19]. Implementation Of IPV6 Services Over A GMPLS – Based IP/Optical Network By Tatipamula, M. Le Faucheur, F. Otani, T. Esaki, H.

[20]. Traffic Engineering Of IP/GMPLS Over WDM By Shaaya, Ibrahim, Din

[21]. Enhanced Fault Recovery Methods For Protected Traffic Services In GMPLS Networks By Eusebi CALLE ORTEGA

[22]. LSA Expansion for Fault Recovery in GMPLS Network By Changwoo Nam, Kwangsub Go, Minki Noh, Seunghae Kim Hyuncheol Kim, Jaeyong Lee, Jinwook Chung

[23]. Aspects Of Network Migration From ATM To MPLS By Adrian Minta

[24]. Analysis Of Generalized MPLS-based Recovery Mechanisms (including Protection and Restoration) By Dimitri Papadimitriou, Eric Mannie
[25]. Control Mechanism For QoS Guaranteed Multicast Service In OVPN Over IP/GMPLS Over DWDM By Jeong-Mi Kim, Oh-Han Kang, Jae-Il Jung, Sung-Un Kim
[26]. A New Fault Tolerant Routing Algorithm For GMPLS/MPLS Networks By Mohammad HossienYaghmae, Fahimeh Jafari
[27]. End-to-end protection strategies in the GMPLS networks By Paweł Rózycki, Janusz Korniak
[28]. From MPLS to GMPLS: Adopting An Evolution Approach To Intelligent Core Networking By Mark.Vanderhaegen
[29]. Specification Of Enhancements And Developments For The AutoBAHN System By R.Krywania
[30]. Dynamic Path Management With Resilience Constraints Under Multiple Link Failures In MPLS/GMPLS Networks By Park, Tae, Nah, Wook, Hyuk
[31]. Overview Of Enhancements To RSVP-TE To Increase Control Plane Resilience By Komolafe, Sventek
[32]. Impact Of GMPLS Control Message Loss By Komolafe, Sventek
[33]. Benefits Of Future GMPLS Controlled Ethernet Switches With Tunable Laser Modules By Szegedi
[34]. Implementation Of Signaling Tunnel In The GMPLS Control Plane By Korniak, Rozycki
[35]. The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols - RFC 3468
[36]. Generalized Multi-Protocol Label Switching (GMPLS) Architecture - RFC 3945
[37]. Link Management Protocol (LMP) - RFC 4204
[38]. Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE for Point-to-Multipoint TE Label Switched Paths (LSPs) - RFC 4875
[39]. RSVP-TE: Extensions to RSVP for LSP Tunnels - RFC 3209
[40]. Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls - RFC 4974
[41]. Emulation Of GMPLS – Controlled Ethernet Label Switching By Tavernier, Papadimitriou, Colle, Pickavet, Demeester
[42]. OPNET Modeler and Ns-2: Comparing the Accuracy Of Network Simulators for Packet-Level Analysis using a Network Testbed By Gilberto Flores Lucio, Marcos Paredes-Farrera, Emmanuel Jammeh, Martin Fleury, Martin J. Reed
[43]. Design and Implementation of MPLS Network Simulator Supporting LDP and CR-LDP By Gaeil Ahn and Woojik Chun
[44]. GLASS (GMPLS Lightwave Agile Switching Simulator) -A Scalable Discrete Event Network Simulator for GMPLS-based Optical Internet By Youngtak

Kim, Eunhyuk Lim, Chul Kim, Kwangil Lee, Douglas Montgomery,Oliver Borchert, Richard Rouil, David Su

[45]. MPLS Based Recovery Mechanisms By Johan Martin Olof Petersson

[46]. GMPLS - simulation tools By Janusz Korniak, Paweł Ró_ycki

[47]. Overview of the RSVP-TE Network Simulator: Design and Implementation By D. Adami, C. Callegari, S. Giordano, F. Mustacchio, M. Pagano, F. Vitucci

[48]. Metro/Core Routing Information Exchange In Optical Networks By Dongmei Wang, John Strand, Jennifer Yates, Charles Kalmanek, Guangzhi Li, and Albert Greenberg

[49]. ASON Training By Alcatel – Lucent

[50]. 1678MCC Rel. 4.3 GMPLS/GMRE Command Line Interface User Guide By Alcatel – Lucent

[51]. Specification Of Enhancements And Developments For The AutoBAHN System By R. Krzywania

[52]. Alcatel 1678MCC Rel. 4.1 OPTICAL MULTIBAND PLATFORM By Alcatel – Lucent

[53]. **GLASS - GMPLS Lightwave Agile Software Simulator:**
http://snad.ncsl.nist.gov/glass/
http://snad.ncsl.nist.gov/glass/doc/api_2.0/index.html

[54]. **NS-2 Manual - Network Simulator 2 Manual:**
The *ns* Manual
Kannan Varadhan
August 24, 2000

[55]. **NS-2 - Network Simulator 2:**
http://www.isi.edu/nsnam/ns/ns-build.html

[56]. **Opnet Modeler 14.5:**
http://www.opnet.com/solutions/network_rd/modeler.html

[57]. **asons** - **An Automatically Switched Optical Network Simulator** By George Kylafas, Dr.John Soldatos
http://www.telecom.ntua.gr/asons/index.html

[58]. Davide Adami, Christian Callegari, Stefano Giordano, Michele Pagano "A new NS2 module for the simulation of MPLS networks with Point-to-Multipoint LSPs support" IEEE International Conference on Communications (ICC 2009), June 14-18, Dresden, Germany
http://netgroup.iet.unipi.it/software/mtens/

[59]. An Improved GMPLS Survivability Mechanism Using Link Delay – Constrained Algorithm *International Conference on Data Communication Networking - DCNET 2011, Seville, Spain*, A. Bikos, C. Bouras, K. Stamos, July 18-21 2011, pp. 45 – 50

ΤΕΛΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ