ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΡΑΙΑ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
Π.Μ.Σ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
ΜΟΡΑΝΤΖΗΣ ΣΤΑΥΡΟΣ 09047

ΘΕΜΑ

Μελέτη της τεχνολογίας MPLS
(Multi Protocol Label Switching)
με βάση τις προηγμένες δικτυακές υπηρεσίες

ΠΡΟΛΟΓΟΣ

Σκοπός της πτυχιακής αυτής είναι η ανάλυση και μελέτη της τεχνολογίας MPLS. Πάνω στο περιβάλλον αυτό παρέχονται κάποιες υπηρεσίες, οι οποίες αναλύονται και γίνεται μελέτη των μηχανισμών και της αρχιτεκτονικής τους. Επιπλέον στόχος μας είναι και η μελέτη των νέων τεχνολογιών και δυνατοτήτων, όπως για παράδειγμα τα ιδεατά εικονικά δίκτυα βασισμένα στην τεχνολογία του MPLS (MPLS VPNs).

Έτσι το βιβλίο αυτό είναι νοητά χωρισμένο σε τρεις θεματικές ενότητες :

α) Κεφάλαιο 1-3 όπου περιγράφονται λεπτομερώς η ανάγκη δημιουργίας του MPLS ,τα συστατικά μέρη αυτής της τεχνολογίας καθώς και ο τρόπος λειτουργίας και επικοινωνίας των στοιχείων αυτών.

β) Κεφάλαιο 4-5 όπου αναλύονται οι μηχανισμοί και η αρχιτεκτονική των υπηρεσιών που μπορεί να προσφέρει το MPLS (QoS/CoS και Traffic Engineering) και πως αυτές μπορούν να αξιοποιηθούν από έναν φορέα παροχής υπηρεσιών Internet.

γ) Κεφάλαιο 6 όπου γίνεται μελέτη της νέας τεχνολογικής δυνατότητας του MPLS VPN.

ΠΕΡΙΕΧΟΜΕΝΑ

VPN Βασισμένα στην MPLS Τεχνολογία

Κεφάλαιο 1 - Εισαγωγή

Κατά την διάρκεια των τελευταίων χρόνων το Internet έχει εισβάλει δυναμικά στην ζωή μας και έχει προκαλέσει την δημιουργία και εξέλιξη ενός πλήθους εφαρμογών στους τομείς των επιχειρήσεων και των καταναλωτικών αγορών. Οι νέες αυτές εφαρμογές έχουν αυξήσει τις απαιτήσεις σε εγγυημένο εύρος ζώνης στον κορμό των δικτύων. Παράλληλα με τις παραδοσιακές υπηρεσίες δεδομένων , που παρέχονται σήμερα μέσω του Internet , νέες υπηρεσίες (εικόνας και ήχου) διαρκώς εξελίσσονται και επεκτείνονται .Το Internet έχει προκύψει ως το κατάλληλο δίκτυο που θα υποστηρίξει και αυτές τις νέες υπηρεσίες . Παρόλα αυτά οι απαιτήσεις που δημιουργούνται σε όρους ταχύτητας και εύρους ζώνης έχουν εξαντλήσει τους πόρους της υπάρχουσας δομής Internet . Αυτός ο μετασχηματισμός του παραδοσιακού δικτύου (πακέτων / πλαισίων) υποδομής έχει εισαγάγει την αβεβαιότητα παρόλο που μέχρι σήμερα ήταν αρκετά ικανοποιητικό.

Εκτός από το ζήτημα των περιορισμών των πόρων , μια ακόμη πρόκληση σχετίζεται με το πώς θα μεταφέρονται τα δεδομένα στο δίκτυο κορμού ώστε να παρέχονται διαφοροποιημένες κατηγορίες υπηρεσιών στους χρήστες.. Η ταχύρρυθμη αύξηση του αριθμού των χρηστών , με αποτέλεσμα την αύξηση της κίνησης ενισχύει το πρόβλημα. Θέματα Κατηγοριοποιημένης υπηρεσίας (CoS) και ποιότητας υπηρεσίας (QoS) πρέπει να ληφθούν υπόψη ώστε να υποστηριχτούν οι διάφορες απαιτήσεις του μεγάλου αριθμού χρηστών δικτύου.
Την λύση έρχεται να δώσει η τεχνολογία MPLS. Σε συνδυασμό με κάποιες αλλαγές, το MPLS θα έχει ένα πολύ σημαντικό ρόλο στην δρομολόγηση (routing) , μεταφορά (switching) και προώθηση πακέτων στις νέες γενιές δικτύων ώστε να ικανοποιούνται οι απαιτήσεις υπηρεσιών των χρηστών των δικτύων.

1.1 Ιστορική αναδρομή

Το MPLS είναι μια τεχνολογία που έχει καθοριστεί από την IETF (Internet Engineering Task Force) και προσβλέπει στον αποδοτικό προσδιορισμό, δρομολόγηση, προώθηση, και μεταγωγή της ροής της κυκλοφορίας μέσα στο δίκτυο.

Το MPLS είναι βασισμένο στην λογική της διαχείρισης ετικετών (labels): μια ανεξάρτητη και μοναδική "ετικέτα" προστίθεται σε κάθε πακέτο στοιχείων και αυτή χρησιμοποιείται για να μεταφέρει και να δρομολογήσει το πακέτο μέσω του

δικτύου. Η ετικέτα είναι απλή - ουσιαστικά μια σύντομη έκδοση πληροφοριών της κεφαλίδας (header) του πακέτου - έτσι ο εξοπλισμός δικτύων μπορεί να βελτιστοποιηθεί γύρω από την επεξεργασία της ετικέτας και την προώθηση της κυκλοφορίας. Αυτή η λογική υπήρχε γύρω από τα συστήματα μεταφοράς δεδομένων για χρόνια.. Οι τεχνολογίες X.25, Frame Relay και ATM είναι παραδείγματα των τεχνολογιών μετατροπής ετικετών. Διάφορες πρωτοβουλίες διαχείρισης ετικετών προέκυψαν στα μέσα της δεκαετίας του '90 για να βελτιώσουν την απόδοση των δρομολογητών IP και να παρέχουν ποιότητα υπηρεσίας (QoS). Μεταξύ αυτών ήταν IP switching (Ipsilon/Nokia), tag switching (Cisco), και ARIS (IBM). Στις αρχές του 1997, ανατέθηκε στην υπεύθυνη για τέτοια θέματα ομάδα εργασίας μηχανικών διαδικτύου (Internet Engineering Task Force - IETF) να τυποποιήσει την τεχνολογία μετατροπής ετικετών. Η IETF ανέπτυξε το MPLS με πρότυπα σχεδίων που το καθιστούν την σημαντικότερη δικτυακή ανάπτυξη των τελευταίων χρόνων

Το MPLS προέκυψε από αυτήν την προσπάθεια ως μία ακόμη τεχνολογία που χρησιμοποιούσε label, αλλά με το ευδιάκριτο πλεονέκτημα να χρησιμοποιεί τις υπάρχουσες τεχνολογίες δρομολόγησης και διευθυνσιοδότησης με το προϋπάρχον IP πρωτόκολλο που έχει κατακλύσει την πλειοψηφία των δικτύων. Σήμερα το MPLS καθορίζεται από ένα σύνολο αιτημάτων προς την IETF για σχόλια (RFCs) και προδιαγραφές σχεδίων .

Έτσι παρόλο που το MPLS αρχικά παρουσιάστηκε ως ένας τρόπος βελτίωσης της ταχύτητας προώθησης των Router σήμερα αναδεικνύετε ως κρίσιμη τεχνολογία που προσφέρει νέες δυνατότητες για υψηλής κλίμακας IP δίκτυα.

Η υποστήριξη Traffic engineering , VPN (Εικονικά Ιδιωτικά Δίκτυα) και QoS είναι παραδείγματα υπηρεσιών όπου το MPLS είναι ανώτερο από οποιαδήποτε υπάρχουσα IP τεχνολογία . Παρόλο που το MPLS επινοήθηκε ώστε να είναι ανεξάρτητο από το Επίπεδο 2 , ένα μεγάλο μέρος του ενδιαφέροντος προς το MPLS περιστρέφεται γύρω από την υπόσχεση του να παρέχει αποτελεσματικότερα IP δίκτυα βασισμένα σε ATM WAN δίκτυα κορμού.

1.2 Παραδοσιακή δρομολόγηση (IP)-προβλήματα

Μέχρι σήμερα ο παραδοσιακός τρόπος δρομολόγησης, της αποθήκευσης και προώθησης, εξυπηρετεί ικανοποιητικά τις κλασσικές εφαρμογές του IP (ftp, telnet, mail). Όμως η ραγδαία εξάπλωση του Internet και η επιθυμία για χρήση του πρωτοκόλλου IP και για άλλες πιο απαιτητικές εφαρμογές (video, audio, videoconference) έφερε στην επιφάνεια τις εγγενείς αδυναμίες του παραδοσιακού τρόπου δρομολόγησης.

Αυτό συμβαίνει για τρεις κυρίως λόγους:

1. Οι παραδοσιακοί δρομολογητές έχουν γίνει στενωποί (bottlenecks). Το γεγονός ότι κάθε δρομολογητής παίρνει μια απόφαση δρομολόγησης ανεξάρτητα από τους άλλους δρομολογητές δημιουργεί επικάλυψη τόσο στον χρόνο όσο και στον χώρο.

α) Η απόφαση ενός δρομολογητή για την δρομολόγηση ενός πακέτου σε κάποιο προορισμό είναι ανεξάρτητη από την ίδια απόφαση του που θα χρειαστεί να πάρει μεταγενέστερα για κάποιο άλλο πακέτο το οποίο έχει ακριβώς τον ίδιο προορισμό. Έτσι ο δρομολογητής αυτός θα επαναλάβει ακριβώς τις ίδιες ενέργειες, σπαταλώντας τον ίδιο χρόνο, και θα καταλήξει στην ίδια απόφαση και για τα δύο πακέτα.

β) Οι αποφάσεις που θα πάρουν δύο ή περισσότεροι δρομολογητές οι οποίοι βρίσκονται στο ίδιο μονοπάτι που ακολουθεί κάποιο πακέτο είναι ανεξάρτητες μεταξύ τους παρόλο ότι υπάρχει η προφανής αλληλοεπικάλυψη της πορείας των πακέτων. Όλοι οι δρομολογητές θα κάνουν ακριβώς τα ίδια πράγματα για να αποφασίσουν πως θα δρομολογήσουν ένα πακέτο της ίδιας ροής.

2. Οι παραδοσιακοί δρομολογητές δεν προσφέρουν τεχνικές traffic engineering. Αυτό οφείλεται στο γεγονός ότι δεν υπάρχει η δυνατότητα για ρητή (explicit) δρομολόγηση άλλα όλα τα πακέτα ακολουθούν το ίδιο μονοπάτι από την αφετηρία προς τον προορισμό μη εξετάζοντας την κατάσταση του δικτύου (φόρτος, καθυστέρηση κλπ). Αυτό έχει ως αποτέλεσμα να υπάρχουν κόμβοι και γραμμές του δικτύου στους οποίους υπάρχει συμφόρηση ενώ άλλοι κόμβοι και γραμμές του δικτύου να υποχρησιμοποιούνται.

3. Το παραδοσιακό IP δεν περιέχει αξιόλογους μηχανισμούς παροχής ποιότητας υπηρεσίας. Αντιμετωπίζει κάθε πακέτο κατά τον ίδιο (απόλυτα δίκαιο) τρόπο με συνέπεια την ύπαρξη μιας και μόνο κλάσης υπηρεσίας τη best effort. Δεν διαθέτει μηχανισμό δέσμευσης πόρων και δεν διαχωρίζει της ροές μεταξύ τους έτσι όλα τα πακέτα ανεξαρτήτως προορισμού και αφετηρίας έχουν την ίδια αντιμετώπιση. Αφού λοιπόν δεν μπορεί να εγγυηθεί καμία ποιότητα υπηρεσίας το παραδοσιακό IP δεν είναι ικανό να υποστηρίξει τις νέες υπηρεσίες (video, audio, videoconference) οι οποίες ολοένα και περισσότερο χρησιμοποιούνται και απαιτούν αυστηρή εγγύηση της ποιότητας υπηρεσίας.

1.3 Λύση MPLS - διαφορές MPLS-IP

Όλα τα προβλήματα που αναφέρθηκαν παραπάνω για το συμβατικό IP πηγάζουν από το γεγονός ότι:

1. οι δρομολογητές είναι stateless, κάθε δρομολογητής δεν κρατάει καμία πληροφορία για τον τρόπο που δρομολογεί τα πακέτα, αφού δρομολογήσει ένα πακέτο επιστρέφει στην αρχική κατάσταση και δρομολογεί οποιοδήποτε άλλο πακέτο ανεξάρτητα.
2. δρομολογούνται πακέτα (σε αντίθεση π.χ. με το ATM όπου δρομολογούνται ροές). Πάντως τεχνολογίες όπως το flow switching και το CEF της Cisco προσομοιώνουν κάποιες από τις λειτουργίες αυτές του ATM.

Όπως έχουμε δει, σε ένα δρομολογητή κάθε πακέτο προωθείται ανεξάρτητα από τα υπόλοιπα με μόνο κριτήριο τον προορισμό του με μία επαναλαμβανόμενη ενέργεια για κάθε πακέτο που αποτελείται από δύο διαδικασίες την δρομολόγηση και την μεταγωγή.

Η λύση που προσφέρει το MPLS βασίζεται στον διαχωρισμό των δύο διαδικασιών της δρομολόγησης και της μεταγωγής (switching) σε ένα δρομολογητή. Το νέο μηχάνημα ονομάζεται Label Switching Router ο οποίος κάνει την προώθηση των πακέτων βασισμένος σε ένα label το οποίο υπάρχει στην κεφαλή του πακέτου χωρίς να χρειάζεται να κάνει επιπλέον επεξεργασία του πακέτου (όπως ακριβώς γίνεται και στο ATM, όπου η δρομολόγηση γίνεται στην αρχή και φτιάχνονται τα μονοπάτια (VCs) και στην συνέχεια η μεταγωγή γίνεται μόνο με βάση ένα label, το VPI/VCI). Η διαφορά είναι ότι σε ένα LSR η μεταγωγή με label γίνεται σε επίπεδο 3 (επίπεδο δικτύου) ενώ στο ATM γίνεται στο επίπεδο 2. Είναι δηλαδή οι LSRs δρομολογητές που χρησιμοποιούν το πρωτόκολλο MPLS και δανείζονται χαρακτηριστικά τόσο από το IP όσο και από το ATM. Συνδυάζουν τα παραδοσιακά πρωτόκολλα του IP για να φτιάξουν τους πίνακες δρομολόγησης αλλά παράλληλα χρησιμοποιούν τον τρόπο μεταγωγής που χρησιμοποιεί ένας μεταγωγέας ATM.

Είναι σημαντικό να καταλάβουμε τις διαφορές στον τρόπο που το MPLS και IP προωθούν τα δεδομένα διαμέσου του δικτύου. Η παραδοσιακή δρομολόγηση πακέτων στο IP δίκτυο χρησιμοποιεί την διεύθυνση προορισμού που βρίσκεται στο header του πακέτου και γίνεται ανεξάρτητη δρομολόγηση σε κάθε δρομολογητή (router) του δικτύου. Οι αποφάσεις δρομολόγησης (hop by hop) βασίζονται στα πρωτόκολλα δρομολόγησης όπως το OSPF (Open Shortest Path First) ή το BGP (Border Gateway Protocol). Αυτά τα πρωτόκολλα δρομολόγησης σχεδιάστηκαν ώστε να βρίσκουν το συντομότερο μονοπάτι μέσα στο δίκτυο χωρίς να λαμβάνουν υπόψη άλλες παραμέτρους όπως λανθάνουσα κατάσταση ή κυκλοφοριακή συμφόρηση.

Το MPLS δημιουργεί ένα μοντέλο επικοινωνίας “connection-based” πάνω στο παραδοσιακό “connectionless” IP δίκτυο πλαισίων. Συνδυάζει την μεταγωγή

με label και την παραδοσιακή δρομολόγηση του IP με στόχο να αυξήσει την ευελιξία και την απόδοση πρωτοκόλλου IP και ταυτόχρονα να δώσει την δυνατότητα για την παροχή υπηρεσιών στο Internet. Έτσι ενώ το MPLS συνεργάζεται με τα υφιστάμενα πρωτόκολλα επιτρέπει την μεταγωγή με κύκλωμα στο Internet. Η μεταγωγή με label επιτυγχάνεται τοποθετόντας στην αρχή κάθε πακέτου, είσοδο του στο δίκτυο MPLS, μια ετικέτα (label) και σε κάθε δρομολογητή απόφαση για το πως θα δρομολογηθεί το πακέτο εξαρτάται μόνο από αυτό και όχι από την IP διεύθυνση στο header. Η ετικέτα απομακρύνεται κατά την έξοδο του πακέτου από το δίκτυο MPLS. Αυτή η αρχιτεκτονική ανοίγει τον δρόμο σε νέες δυνατότητες για την διαχείριση της κίνησης σε ένα IP δίκτυο, συνδυάζοντας τη νοημοσύνη της δρομολόγησης, που είναι θεμελιώδης στη λειτουργία του διαδικτύου και των σημερινών δικτύων IP, με την υψηλή απόδοση του switching .

1.4 Πλεονεκτήματα MPLS

Παρακάτω αναφέρονται τα πλεονεκτήματα για τα οποία το MPLS είναι γνωστό και διαδεδομένο.

- Το MPLS ενεργοποιεί ένα ενιαίο δίκτυο για να υποστηρίξει και τις νέες εφαρμογές αλλά και τις παλαιότερες παραδοσιακές υπηρεσίες, δημιουργώντας ένα αποδοτικό δίκτυο σε μια IP-βασισμένη υποδομή. Το MPLS διαχειρίζεται και τις κλασσικές (DS3, SONET) αλλά και τις νέες (10/100/1000/10G Ethernet) υποδομές καθώς και τις διάφορες τεχνολογίες δικτύων (IP, ATM, Frame Relay, Ethernet, και TDM).

- Multiprotocol και Multilink υποστήριξη. Η διαδικασία προώθησης Label δεν καθορίζεται για ένα συγκεκριμένο επίπεδο δικτύου. Για παράδειγμα, το ίδιο τμήμα αποστολής (router ,switch) θα μπορούσε να χρησιμοποιηθεί για την μεταφορά label και με IP αλλά και με IPX. Το MPLS είναι ικανό να διαχειριστεί εικονικά οποιοδήποτε πρωτόκολλο στο επίπεδο δεδομένων (data link),παρόλο που αρχικά δημιουργήθηκε δίνοντας έμφαση στο ATM.

- Το MPLS υποστηρίζει την παράδοση των υπηρεσιών με την χρήση των εγγυήσεων υπηρεσιών (QoS). Τα πακέτα μπορούν να μαρκαριστούν για την υψηλή ποιότητα, επιτρέποντας στους προμηθευτές να διατηρήσουν μια προσυμφωνημένη καθυστέρηση-λανθάνουσα κατάσταση για φωνή και βίντεο.

- Χρησιμοποιούνται τεχνικές traffic engineering κατά την δρομολόγηση έτσι επιτυγχάνεται να αποσταλούν περισσότερα δεδομένα στο διαθέσιμο εύρος ζώνης

- Το MPLS μειώνει τις απαιτήσεις υψηλής επεξεργασίας των δρομολογητών, δεδομένου ότι οι δρομολογητές διαβιβάζουν απλά τα πακέτα βασισμένα στις σταθερές ετικέτες.

- Το MPLS παρέχει το κατάλληλο επίπεδο ασφάλειας για να καταστήσει την IP τόσο ασφαλή όσο το Frame Relay στο WAN, μειώνοντας την ανάγκη για την κρυπτογράφηση στα δημόσια δίκτυα IP.

- Τα MPLS-VPNs κλιμακώνονται καλύτερα απ' ότι τα VPN που βασίζονται στον πάροχο όπου μειώνεται η δυνατότητα διαχείρισης των προϋποθέσεων και ρυθμίσεων για τον πελάτη

- Παρέχεται η δυνατότητα να διαβιβαστούν τα πακέτα πέρα από το κριτήριο της συντομότερης διαδρομής, δηλ. παρέχει την υπηρεσία μεταγωγής κυκλώματος σε ένα hop-by-hop δίκτυο δρομολογητών.

- Για τα μη βασισμένα στο IP πρωτόκολλο δίκτυα όπως το Frame Relay και το ATM , παρέχει ένα βασισμένο στην IP τεχνολογία σχέδιο ελέγχου (δρομολόγηση, επιλογή πορειών) αντί των συγκεκριμένων προεπιλεγμένων τεχνικών ελέγχου (π.χ. PNNI). Έτσι το MPLS παρέχει μια ενοποιημένη αρχιτεκτονική ελέγχου και για τις connectionless αλλά και τις connection-oriented τεχνολογίες.

- Οι ετικέτες έχουν καθοριστεί για τις περισσότερες τεχνολογίες επιπέδου 2 και κατά συνέπεια, οι υπηρεσίες MPLS μπορούν να προσφερθούν για μία σειρά ετερογενών δικτύων.

- Παρέχεται ένας μηχανισμός ομαδοποίησης των συσχετισμένων μεταξύ τους πακέτων ώστε να τους ανατίθεται κοινή ετικέτα και να απομονώνεται η μία ομάδα πακέτων από την άλλη. Έτσι μπορεί να εγκατασταθεί ένα μονοπάτι μεταγωγής ετικετών (LSP) παρέχοντας μια γενική υπηρεσία Tunneling όπως :
    - Σύνδεση των τμημάτων ενός VPN πέρα από ένα δημόσιο δίκτυο
    - Υπερσύνδεση δύο μη – IP βασισμένων δικτύων
    - Αντιστοίχηση κοινών κανόνων αποστολής για τα πακέτα με κοινή ετικέτα π.χ κατηγοριοποίηση υπηρεσιών (CoS)

- Το αρχικό κίνητρο για MPLS ήταν η ενεργοποίηση της γρήγορης μεταγωγής, με την αντικατάσταση του ελέγχου διαδρομών για μια διεύθυνση προορισμού IP μεταβλητού μήκους , με μια ακριβή αντιστοιχία ενός σταθερού, προκαθορισμένου αριθμού κομματιών. Εντούτοις, με την εμφάνιση των

γρήγορων αλγορίθμων και υλικού (hardware) δρομολόγησης η χρησιμότητα του MPLS ήταν πλέον περιορισμένη. Βεβαίως, η χρήση των ετικετών για να προσδιορίσει ρητά μια κοινή ομάδα πακέτων μπορεί να είναι χρήσιμη και σε άλλα πεδία που απαιτείται γρήγορη ταξινόμηση σε έναν πλαίσιο κανόνων. Παραδείγματος χάριν, τα πακέτα που λαμβάνουν μια κοινή υποψία ασφάλειας μπορούν να προσδιοριστούν με μια κοινή ετικέτα ή σε ένα σύστημα εξισορρόπησης φόρτου οι συνδέσεις που ανήκουν σε μια κοινή σύνοδο θα μπορούσαν να χαρακτηριστούν από μια κοινή ετικέτα έτσι ώστε τα πακέτα για εκείνη την σύνοδο να καθοδηγούνται στον ίδιο κεντρικό υπολογιστή (server)

- Δεδομένου ότι η ερμηνεία των ετικετών είναι ανεξάρτητη από τα πρωτόκολλα ελέγχου, νέα πρωτόκολλα θα μπορούν εύκολα να υποστηριχθούν.

1.5 Προκλήσεις σύγχρονης σχεδίασης

Οι σημερινοί σχεδιαστές δικτύων αντιμετωπίζουν τεχνολογικές προκλήσεις που έμοιαζαν με όνειρο πριν μερικά χρόνια όταν πρωτοεμφανίστηκε το IP γύρω στο 1970.Τα σύγχρονα δίκτυα καλούνται να υποστηρίξουν συνεχώς υψηλότερες ποσότητες δεδομένων πάνω στον παραδοσιακό τρόπο διαδικτύωσης (file transfer, email, www access). Καλούνται επίσης να διαφοροποιήσουν σε πολλές κατηγορίες την απόδοσης κυκλοφορίας . Οι traffic engineering δυνατότητες του MPLS επιτρέπουν έναν βαθμό ελέγχου πάνω στο δίκτυο σε αντίθεση με τις IP τεχνολογίες.
Έτσι με τις αυξημένες ανάγκες και των πελατών οι σχεδιαστές καλούνται να αντιμετωπίσουν διάφορες προκλήσεις όπως :

α) **Λειτουργικότητα**. Το Label switching παρέχει νέες λειτουργίες που ήταν στο παρελθόν είτε μη διαθέσιμες ή ανεπαρκής με την παραδοσιακή δρομολόγηση. Η explicit (ρητή) δρομολόγηση είναι ένα παράδειγμα . Η επιλογή μιας διαδρομής βάσει των ιδιοτήτων εκτός της διεύθυνσης προορισμού ,όπως γίνεται στο QoS, είναι επίσης απαραίτητο.

β) **Εξελισιμότητα**. Τα μελλοντικά δίκτυα χρειάζεται να είναι εικονικά απεριόριστα σε μέγεθος. Οι πληροφορίες δρομολόγησης αυξάνονται πολύ γρήγορα καθώς το δίκτυο αυξάνεται, και μπορούν τελικά να υπερφορτώσουν έναν δρομολογητή. Οι τρέχουσες τεχνικές διαστρωμάτωσης των IP δικτύων στην κορυφή των ATM ή Frame Relay εικονικών κυκλωμάτων επιδεινώνουν το πρόβλημα. Το MPLS απαιτεί από τις επιπέδου-2 συσκευές (π.χ ATM switches) να είναι ικανές να εκτελούν το IP πλάνο έλεγχου που περιορίζει αυτό το πρόβλημα . Το traffic engineering , υπό την έννοια ότι επιτρέπει την

αποδοτικότερη χρήση των πόρων δικτύων ,βοηθά επίσης στην εξέλιξη του δικτύου.

γ) **Αφομοίωση**. Μία από τις μεγαλύτερες προκλήσεις είναι η αφομοίωση των αλλαγών και της ανάπτυξης χωρίς σημαντικές διασπάσεις του δικτύου. Οι καθορισμένες υπηρεσίες πρέπει να επιστρωθούν επάνω στο μη καθορισμένο δίκτυο IP, οι πολλαπλάσιοι τύποι κυκλοφορίας IP πρέπει να γίνουν αποδεκτοί, και τα ιδεατά ιδιωτικά δίκτυα πρέπει να καθιερωθούν. Ενώ ο πυρήνας του δικτύου είναι αυτός που πρέπει να αυξήσει στην ικανότητα μεταφοράς (switching) , ένα μεγάλο μέρος της εξέλιξης οδηγείται στις συσκευές άκρων- το σημείο οριοθέτησης προμηθευτών χρηστών. Μια συσκευή μεταφορέας που ενσωματώνει τις νέες ικανότητες IP σε ένα τυποποιημένο πρότυπο βιομηχανίας είναι ουσιαστική.

δ) **Ολοκλήρωση (**Integration). Η δημιουργία εφαρμογής για την IP τηλεφωνία είναι ένα παράδειγμα της ολοκλήρωσης συστημάτων και η επικάλυψη του δικτύου IP πάνω σε μια υποδομή μεταφορέων του ATM είναι ένα εύστοχο παράδειγμα της ολοκλήρωσης των δικτύων. Η ολοκλήρωση σε όλα τα επίπεδα είναι μια απαίτηση σχεδίου για ένα αποτελεσματικό δίκτυο

MPLS και στοιχεία MPLS

2.1 Τι είναι το MPLS

Το MPLS είναι ένα καθορισμένο από την IETF πλαίσιο εργασίας το οποίο παρέχει αποδοτική σχεδίαση ,δρομολόγηση , προώθηση και μεταφορά (switching) της ροής της κίνησης μέσα στο δίκτυο.

Το MPLS έχει τις παρακάτω ιδιότητες –αρμοδιότητες

- Καθορίζει μηχανισμούς για την διαχείριση της κίνησης επιλύνοντας προβλήματα διαφόρων τύπων όπως διακίνηση πληροφοριών ανάμεσα σε συσκευές διαφορετικού υλικού (hardware) , διαφορετικών μηχανημάτων , ακόμα και διαφορετικών εφαρμογών

- Παραμένει ανεξάρτητο από τα επιπέδου 2 και 3 πρωτόκολλα

- Παρέχει μέσα για να χαρτογραφηθούν οι IP διευθύνσεις σε απλούστερες , μειωμένου μήκους ετικέτες (labels) χρησιμοποιώντας διαφορετικές τεχνολογίες προώθησης και μεταφοράς πακέτων

- Συνεργάζεται με τα υπάρχοντα πρωτόκολλα δρομολόγησης όπως το RSVP (Resource Reservation Protocol) και το OSPF (Open Short Path First)

- Υποστηρίζει τα IP ,ATM και Frame Relay επιπέδου 2 πρωτόκολλα

Στο MPLS, η μετάδοση δεδομένων γίνεται στα LSPs (label-switched paths). Τα LSPs είναι μια ακολουθία ετικετών σε κάθε κόμβο κατά μήκος της πορείας από την πηγή στον προορισμό. Τα LSPs δημιουργούνται είτε πρίν την μετάδοση των δεδομένων (control driven) ή μετά τον εντοπισμό μιας ροής δεδομένων (data-driven). Τα labels που είναι ειδικοί προσδιοριστές διανέμονται χρησιμοποιώντας το LDP (label distribution protocol) ή το RSVP ή βασίζονται σε προϋπάρχοντα πρωτόκολλα δρομολόγησης όπως το BGP και το OSPF. Κάθε πακέτο δεδομένων ενθυλακώνει και μεταφέρει τα labels κατά την διάρκεια του ταξιδιού από την πηγή στον προορισμό. Η υψηλή μεταφορά των δεδομένων είναι πιθανή επειδή τα labels εισάγονται στην αρχή του πακέτου ή πλαισίου και μπορεί να χρησιμοποιηθούν από τις συσκευές για την γρήγορη μεταφορά ανάμεσα στις συνδέσεις.

Ας δούμε όμως αναλυτικά τα στοιχεία και τα χαρακτηριστικά που απαρτίζουν ένα MPLS δίκτυο καθώς και τις λειτουργίες τους :

2.2 LSRs και LERs

Οι συσκευές που συμμετέχουν στους μηχανισμούς του MPLS μπορούν να κατηγοριοποιηθούν σε Label Edge Routers (LERs) και Label switching routers (LSRs). Λόγω της θέσης τους στο δίκτυο χαρακτηρίζονται και ως κόμβοι.

Ο LSR είναι μία υψηλής ταχύτητας συσκευή δρομολόγησης που βρίσκεται στον πυρήνα ενός MPLS δικτύου και συμμετέχει

α) στην δημιουργία των LSPs χρησιμοποιώντας το κατάλληλο πρωτόκολλο σηματοδοσίας ετικέτας

β)στην υψηλή ταχύτητα μεταγωγής της κίνησης των δεδομένων πάνω στα δημιουργημένα μονοπάτια

Ο LER είναι μία συσκευή η οποία λειτουργεί στο άκρο του δικτύου πρόσβασης και MPLS δικτύου. Οι LERs υποστηρίζουν πολλαπλές πόρτες συνδεδεμένες σε διαφορετικής τεχνολογίας δίκτυα (όπως Frame relay, ATM και

Ethernet) και προωθούν την κίνηση στο MPLS δίκτυο αφού ενεργοποιηθούν τα LSPs, χρησιμοποιώντας το πρωτόκολλο σηματοδοσίας ετικετών στην είσοδο και στη συνέχεια διανέμουν την κίνηση πίσω στα δίκτυα πρόσβασης στην έξοδο. Ο LER παίζει έναν πολύ σημαντικό ρόλο στην ανάθεση και απομάκρυνση των ετικετών κατά την διάρκεια εισόδου και εξόδου της κίνησης στο MPLS δίκτυο.

Μία συσκευή μπορεί να είναι edge (LER) και core (LSR) ταυτόχρονα. Για παράδειγμα ένας edge κόμβος, σημείο έναρξης η τερματισμού ενός LSP, μπορεί να είναι παράλληλα core κόμβος σε κάποιο LSP και να κάνει μεταγωγή για τα πακέτα που χρησιμοποιούν το συγκεκριμένο μονοπάτι. Το πιο σημαντικό είναι η διάκριση των λειτουργιών του κόμβου για κάθε LSP και όχι η κατάταξη των κόμβων ενός δικτύου σε μια από τις δύο κατηγορίες.

2.3 Label Distribution Protocol (LDP)

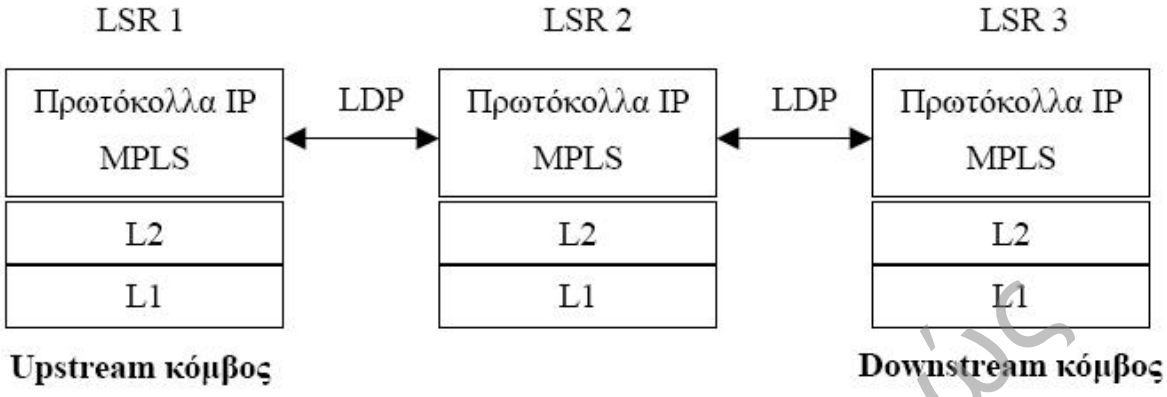
Το LDP είναι ένα νέο πρωτόκολλο διανομής πληροφοριών, που αφορούν τις συσχετίσεις των label, στα LSRs στο MPLS δίκτυο. Χρησιμοποιείται για την χαρτογράφηση των label σε FECs που με τη σειρά τους δημιουργούν τα LSPs. Οι LDP σύνοδοι πραγματοποιούνται μεταξύ των LDP peer στο MPLS δίκτυο. Οι peers ανταλλάσσουν τους εξής τύπους LDP μηνυμάτων :

- **Μηνύματα ανακάλυψης** – αναγγείλουν και διατηρούν την παρουσία ενός LSR μέσα σ' ένα δίκτυο
- **Μηνύματα συνόδου** – πραγματοποιούν ,διατηρούν και τερματίζουν τις συνόδους μεταξύ των LDP peer
- **Μηνύματα διαφήμισης** – δημιουργία, αλλαγή και διαγραφή label χαρτογράφησης για τα FEC
- **Μηνύματα ειδοποίησης** – παρέχουν συμβουλευτικές πληροφορίες και πληροφορίες λαθών σηματοδοσίας

2.4 Λειτουργία LSR

Το LDP εφαρμόζεται μεταξύ δύο διαδοχικών LSRs όπως φαίνεται και στο παρακάτω σχήμα, όπου ο πρώτος κόμβος (LSR 1) καλείται Upstream γείτονας του κεντρικού κόμβου (LSR 2) ενώ ο τρίτος κόμβος (LSR 3) Downstream γείτονας του κεντρικού κόμβου. Γενικά σε μια ροή πακέτων από ένα κόμβο A σε

ένα κόμβο Β όπου έχει γίνει δέσμευση μιας ετικέτας Ε ο Α καλείται Upstream και ο Β Downstream κόμβος.



Επικοινωνία μεταξύ LSRs

Όπως φαίνεται από το σχήμα. κάθε LSR υποστηρίζει στο επίπεδο 3 τόσο τα παραδοσιακά IP πρωτόκολλα όσο και το πρωτόκολλο MPLS. Η LDP επικοινωνία μεταξύ δύο LSR χωρίζεται σε τρεις φάσεις:

1. Αρχικά γίνεται ανίχνευση των γειτονικών LSRs, με την αποστολή 'DISCOVERY' μηνυμάτων. Μηνύματα ανταλλάσσονται επίσης περιοδικά για την συντήρηση της επικοινωνίας.

2. Ακολούθως οι γειτονικοί LSRs ανοίγουν ένα LDP session χρησιμοποιώντας το πρωτόκολλο TCP, ώστε να εξασφαλιστεί η αξιόπιστη παράδοση, το οποίο θα χρησιμοποιηθεί για την ανταλλαγή των πληροφοριών μεταγωγής.

3. Τέλος ανταλλάσσονται μια σειρά από LDP μηνύματα ώστε α) να συμφωνηθούν διάφορες παράμετροι και επιλογές της επικοινωνίας και β) να διαφημιστούν οι πληροφορίες δέσμευσης μεταξύ IP διευθύνσεων και labels Κατά αυτό τον τρόπο ένας LSR γνωρίζει τόσο με ποια labels θα του προωθεί ο upstream κόμβος πακέτα όσο και με ποια labels και σε ποιους κόμβους ο ίδιος θα τα προωθεί.

Οι LSRs έχουν δύο σημαντικές διαφορές από τους παραδοσιακούς δρομολογητές. Πρώτον η πληροφορία που ανταλλάσσουν μεταξύ τους δεν αφορά μόνο την δρομολόγηση αλλά επιπλέον και πληροφορία σχετικά με τον τρόπο προώθησης των πακέτων (δηλαδή τα labels). Δεύτερον, ενώ οι παραδοσιακοί δρομολογητές εφαρμόζουν την διαδικασία μεταγωγής ξεχωριστά για κάθε πακέτο, με αποτέλεσμα να παίρνουν τις ίδιες αποφάσεις πολλές φορές, οι LSRs κάνουν μεταγωγή σε ροές (flows). Αυτό έχει ως αποτέλεσμα να

μειώνεται η επικάλυψη, άρα και ο απαιτούμενος χρόνος, στις αποφάσεις που παίρνονται.

Επιπλέον οι LSRs ενσωματώνουν τα πλεονεκτήματα της IP και ATM τεχνολογίας και δεν κληρονομούν τα μειονεκτήματα αυτών. Έχουν χαμηλότερο κόστος κατασκευής από τα ATM switches γιατί δεν χρησιμοποιούν τα πολύπλοκα πρωτόκολλα σηματοδοσίας και δρομολόγησης του ATM και επίσης έχουν καλύτερη απόδοση από τους παραδοσιακούς IP δρομολογητές.

2.5 Μορφή label

Label (20 bits)	Exp (3 bits)	S (1 bit)	TTL (8 bits)

Η μορφή συγκρότησης ενός label

Ένα label , στην απλούστερη μορφή του , καθορίζει το μονοπάτι όπου ένα πακέτο θα έπρεπε να περάσει. Ένα label μεταφέρεται ή ενθυλακώνεται μέσα σε μια επιπεδου-2 κεφαλή (header) μαζί με το πακέτο. Ο παραλήπτης δρομολογητής εξετάζει το πακέτο για τα περιεχόμενα του label ώστε να συμπεράνει το επόμενο hop – πέρασμα. Αν στο πακέτο έχει προστεθεί label , το ταξίδι του μέσα στο δίκτυο κορμού βασίζεται στην μεταφορά (switching) βάση των label. Τα στοιχεία των label είναι σημαντικά μόνο τοπικά, δηλαδή χρησιμοποιούνται μόνο για τα περάσματα ανάμεσα στα LSRs.

Κάθε ετικέτα περιλαμβάνει τα εξής πεδία:

Bottom of Stack (S). Η τιμή του πεδίου τίθεται σε τιμή 1 για την ετικέτα που βρίσκεται στη βάση της στοίβας.

Time to Live (TTL). Συνήθως χρησιμοποιείται κατά ισοδύναμο τρόπο όπως το αντίστοιχο πεδίο του IP header. Κατά την εισαγωγή του πακέτου στο δίκτυο αντιγράφεται εδώ η τιμή IP TTL. Δέχεται την ανάλογη επεξεργασία σε κάθε κόμβο και τέλος κατά την έξοδο του από το δίκτυο MPLS αντιγράφεται πίσω στο IP TTL.

Experimental Use (Exp). Για πειραματική χρήση. Μία πιθανή εφαρμογή είναι για την διάκριση 8 διαφορετικών κατηγοριών υπηρεσίας.

Label Value (Label). Ουσιαστικά πρόκειται για την «πραγματική» τιμή της ετικέτας.

Ορισμένες τιμές ετικέτας (Label Value) έχουν δεσμευτεί για ειδικούς λόγους όπως για παράδειγμα η τιμή μηδέν (0) που έχει νόημα μόνο στη βάση της στοίβας και δηλώνει το “IPv4 Explicit NULL Label”. Ότι δηλαδή η ετικέτα

πρέπει να αφαιρεθεί και η προώθηση του πακέτου να γίνει με βάσει τη διεύθυνση στο IPv4 header.

Ένας LSR διαβάζοντας μία ετικέτα, πάντα από την κορυφή της στοίβας, μαθαίνει:

Που θα προωθήσει το πακέτο (next hop).

Την λειτουργία που θα εκτελέσει πριν από την προώθηση του, που είναι μία από τις ακόλουθες:

1. Να αντικαταστήσει την ετικέτα στην κορυφή της στοίβας με μια άλλη, ή
2. Να αφαιρέσει την ετικέτα της κορυφής από την στοίβα, ή
3. Να αντικαταστήσει την ετικέτα της κορυφής με κάποια άλλη και να προσθέσει μία ή περισσότερες ετικέτες στη στοίβα.

2.6 Forward Equivalence Class (FEC) – Label Information Base (LIB)

Το FEC είναι μια εκπροσώπηση μίας ομάδας πακέτων τα οποία έχουν τις ίδιες απαιτήσεις για την μεταφορά τους . Όλα τα πακέτα που ανήκουν σε μια τέτοια ομάδα αντιμετωπίζονται ομοίως κατά την δρομολόγηση τους. Αντίθετα με την συνηθισμένη προώθηση των IP πακέτων , στο MPLS η εγγραφή ενός πακέτου σε ένα FEC γίνεται μία μόνο φορά ,καθώς το πακέτο εισέρχεται στο δίκτυο. Τα FECs βασίζονται στις απαιτήσεις υπηρεσιών είτε μιας συγκεκριμένης ομάδας πακέτων ή στην απαίτηση ενός συγκεκριμένου προορισμού. Το κάθε LSR δημιουργεί τον δικό του πίνακα ώστε να καθορίσει πως ένα πακέτο πρέπει να προωθηθεί. Αυτός ο πίνακας ,που ονομάζεται Label Information Base (LIB) – βάση πληροφοριών ετικέτας, αποτελείται από αντιστοιχίες FEC-Label.

2.7 Αντιστοιχίες Label

Όταν το πακέτο κατηγοριοποιηθεί σε μία νέα ή προυπάρχουσα FEC , ένα label συνδέεται στο πακέτο. Οι τιμές των label μεταφέρονται από το επίπεδο-2 (στρώμα δεδομένων). Για τεχνολογίες επιπέδου-2 (π.χ ATM , Frame Relay),οι

προσδιοριστές επιπέδου 2 (DLCIs για Frame Relay ,VCIs στην περίπτωση του ATM) μπορούν να χρησιμοποιηθούν απευθείας ως label. Τα πακέτα τότε προωθούνται βασισμένα στην τιμή του label τους.

Οι ετικέτες είναι συνδεδεμένες σε ένα FEC ως αποτέλεσμα κάποιου γεγονότος ή πολιτικής που δείχνει ανάγκη για μια τέτοια σύνδεση. Αυτά τα γεγονότα μπορεί να είναι είτε ομαδοποίηση λόγω δεδομένων (**Data-driven bindings**) ή ομαδοποίηση λόγω ελέγχου (**control-driven bindings**). Το δεύτερο είναι προτιμότερο λόγω των προχωρημένων ιδιοτήτων που μπορούν να χρησιμοποιηθούν στο MPLS.

Η ανάθεση των label μπορεί να βασίζεται στα παρακάτω κριτήρια προώθησης :

- Προορισμός δρομολόγησης
- Traffic engineering
- Δρομολόγηση πολλαπλής διανομής
- Ιδεατά Εικονικά Δίκτυα (VPN)
- Ποιότητα υπηρεσίας (QOS)

2.8 Συγχώνευση -Κατακερματισμός Label

Σε μια σύνδεση του επιπέδου μεταφοράς μια ροή χαρακτηρίζεται από την τετράδα <διεύθυνση αφετηρίας, πόρτα αφετηρίας, διεύθυνση προορισμού, πόρτα προορισμού>. Αν για κάθε τέτοια πιθανή τετράδα δεσμεύεται ένα διαφορετικό label τότε χρειάζεται ένας πολύ μεγάλος αριθμός labels, κυρίως στα μεγάλα δίκτυα των ISPs. Αυτό μπορεί να έχει ως αποτέλεσμα την εξάντληση του αριθμού των διαθέσιμων labels, αφού χρησιμοποιείται ένα πεδίο σταθερού μήκους 32 bits, εκ των οποίων μόνο τα 20 bits είναι αφιερωμένα για την διάκριση των labels.

Μια εναλλακτική προσέγγιση είναι η δέσμευση ενός label για κάθε δυάδα <διεύθυνση αφετηρίας, διεύθυνση προορισμού>. Δηλαδή όλες οι ροές οι οποίες έχουν την ίδια αφετηρία και τον ίδιο προορισμό θα δρομολογούνται μέσα από το ίδιο μονοπάτι (LSP). Σε αυτήν την περίπτωση γίνεται μία συνάθροιση (aggregation) των ροών που έχουν την ίδια <διεύθυνση αφετηρίας, διεύθυνση προορισμού>. Ανάλογα με τον βαθμό ενοποίησης (ή συνάθροισης) που έχει επιλεχθεί καθορίζεται και ο βαθμός κατακερματισμού (granularity) των labels.
Είναι δυνατόν να γίνει ακόμη μεγαλύτερη συνάθροιση ροών, συνεπώς οικονομία labels, με την δέσμευση ενός label για κάθε προορισμό. Σε αυτήν την περίπτωση

όλα τα πακέτα που έχουν ως προορισμό κάποια συγκεκριμένη διεύθυνση θα έχουν το ίδιο label.

Το μειονέκτημα της ενοποίησης των ροών είναι ότι δεν μπορεί να υποστηριχθεί ποιότητα υπηρεσίας για την κάθε ροή ξεχωριστά, ιδιαίτερα σημαντικό στοιχείο για την παροχή αυστηρής ποιότητας υπηρεσίας.
Επιπλέον, σε κάθε μορφή συνάθροισης που επιλέγεται θα πρέπει να είναι ικανός ο προορισμός να διαχωρίζει τις διαφορετικές ροές που έχουν ενοποιηθεί. Γι' αυτόν τον λόγο είναι πολύ σημαντικό όλοι οι κόμβοι του δικτύου να έχουν επιλέξει τον ίδιο τρόπο ενοποίησης / συνάθροισης για τα LSPs. Γι αυτό μεταξύ των κόμβων αφετηρίας και προορισμού θα πρέπει να υπάρχει απόλυτη συμφωνία ως προς την επιλογή του βαθμού συνάθροισης των ροών διαφορετικά ο προορισμός δεν θα είναι ικανός να διαχωρίσει τις διαφορετικές ροές.

2.9 Δημιουργία Label

Υπάρχουν διάφοροι τρόποι και μέθοδοι που χρησιμοποιούνται για την δημιουργία των Label:

- Μέθοδος βασισμένη στην τοπολογία –χρησιμοποιεί επεξεργασία πρωτοκόλλων δρομολόγησης (όπως OSPF και BGP)
- Μέθοδος βασισμένη στις αιτήσεις – γίνεται επεξεργασία βάση των αιτημάτων ελέγχου κίνησης (όπως το RSVP)
- Μέθοδος βασισμένη στην κίνηση – χρησιμοποιεί την υποδοχή ενός πακέτου για να προκαλέσει την ανάθεση και τη διανομή μιας ετικέτας

Οι δύο πρώτοι τρόποι δημιουργίας των Label είναι παραδείγματα control-driven bindings ,ενώ η τρίτη μέθοδος είναι παράδειγμα Data-driven bindings

2.10 Label-Switched Paths (LSPs)

Μία συλλογή από MPLS συσκευές αποτελούν ένα MPLS domain. Μέσα στο MPLS domain εγκαθίσταται ένα μονοπάτι- διαδρομή (LSP), για να ταξιδέψει ένα πακέτο , βασισμένο σε ένα FEC. Το LSP εγκαθίσταται πριν ξεκινήσει η μετάδοση δεδομένων. Το MPLS διαθέτει τους παρακάτω δύο τρόπους για την δημιουργία ενός LSP:

- Hop-by-hop δρομολόγηση –Κάθε LSR ανεξάρτητα διαλέγει το επόμενο άλμα (hop) για ένα δοσμένο FEC. Αυτή η μεθοδολογία είναι όμοια με αυτή που χρησιμοποιείται στα IP δίκτυα. Ο LSR χρησιμοποιεί κάθε διαθέσιμο πρωτόκολλο δρομολόγησης όπως το OSFP,PNNI κλπ.

- Ρητή δρομολόγηση (explicit)- είναι παρόμοια με την δρομολόγηση πόρων. Οι LSR εισόδου (δηλαδή οι LSR που βρίσκονται εκεί που ξεκινάει η ροή δεδομένων του δικτύου) καθορίζουν την λίστα των κόμβων απ' όπου τα ER-LSP περνούν . Το μονοπάτι που καθορίζεται μπορεί να μην είναι απαραίτητα το ταχύτερο. Διαμέσου της διαδρομής οι πόροι μπορεί να διατηρηθούν ώστε να εξασφαλίζουν ποιότητα υπηρεσίας (QoS) στην διακίνηση δεδομένων. Αυτό διευκολύνει το traffic engineering στο δίκτυο και μπορεί να γίνει παροχή διαφοροποιημένων υπηρεσιών χρησιμοποιώντας ροές βασισμένες σε πολιτικές ή μεθόδους διαχείρισης δικτύου.

Υπάρχουν τρεις εναλλακτικές τεχνικές για την έναρξη της LSPs ή αλλιώς για την ανταλλαγή labels μεταξύ των LSRs :

- Τεχνική data-driven. Η ανταλλαγή των labels και η δημιουργία των LSPs προκαλείται από την έναρξη της ροής πακέτων μέσα στο δίκτυο. Αφού ολοκληρωθεί το μονοπάτι (LSP) ακολουθεί η προώθηση των πακέτων.
- Τεχνική topology-driven. Η ανταλλαγή των labels και η δημιουργία των LSPs αρχίζει αυτόματα μετά την ολοκλήρωση της τοπολογίας του δικτύου. Με αυτόν τον τρόπο τα LSPs δημιουργούνται εξαρχής και παραμένουν μέχρι να αλλάξει η τοπολογία του δικτύου.
- Τεχνική request-driven. Η ανταλλαγή των labels και η δημιουργία των LSPs πραγματοποιείται μετά από ρητή εντολή του χρήστη.

Ένα μειονέκτημα των τεχνικών data-driven και request-driven είναι ότι ο χρόνος για την εγκαθίδρυση του LSP εμφανίζεται ως καθυστέρηση πριν από την έναρξη της αποστολής των πακέτων σε αντίθεση με την topology-driven τεχνική όπου τα LSPs προϋπάρχουν. Η καθυστέρηση αυτή είναι αρκετά ενοχλητική κυρίως για ροές μικρής διάρκειας εξαιτίας του χρόνου που χρειάζεται για την δημιουργία των LSPs. Συνήθως ο χρόνος που θα χρειαστεί για την μεταφορά των πακέτων θα είναι περίπου ο ίδιος που θα ήταν και στο παραδοσιακό IP.
Μειονέκτημα της τεχνικής topology-driven είναι ότι χρησιμοποιούνται περισσότερα labels, αφού εξαρχής κατασκευάζονται όλες οι πιθανές διαδρομές .

2.11 Διανομή των Label

Η αρχιτεκτονική του MPLS δεν χρησιμοποιεί μία μόνο μέθοδο σηματοδοσίας για την διανομή των label. Τα προϋπάρχον πρωτόκολλα δρομολόγησης (όπως το BGP) έχουν ενισχυθεί ώστε να κουβαλήσουν τις πληροφορίες των Label μέσα στο περιεχόμενο τους. Το RSVP έχει επίσης επεκταθεί για να υποστηρίξει τις ανταλλαγές των label. Η IETF έχει επίσης καθορίσει το νέο γνωστό πρωτόκολλο Label Distribution Protocol (LDP) για ρητή σηματοδοσία και διαχείριση του διαστήματος του Label . Έχουν ακόμα καθοριστεί επεκτάσεις στο LDP για την υποστήριξη της ρητής (explicit) δρομολόγησης βασιζόμενη σε απαιτήσεις QOS και COS. Αυτές οι προεκτάσεις έχουν συμπεριληφθεί στο νεότερο CR-LDP πρωτόκολλο.

Ακολουθεί μια περίληψη των διαφόρων σχεδίων ανταλλαγής Label :

- LDP – χαρτογραφεί τους unicast IP προορισμούς μέσα στα Label
- RSVP, CR-LDP – χρησιμοποιούνται για traffic engineering και κατοχύρωση των πόρων
- Protocol-Independent multicast (PIM) – χρησιμοποιείται για την χαρτογράφηση multicast προορισμών στα label
- BGP– εξωτερικά Label (VPN)

Υπάρχουν πέντε μέθοδοι ανταλλαγής των labels μεταξύ των LSRs

Downstream allocation. Ο Downstream κόμβος δεσμεύει ένα label και στην συνέχεια ενημερώνει τον Upstream κόμβο για την δέσμευση αυτή καθώς και την πληροφορία για τον τύπο δέσμευσης προορισμού. Ο τύπος αυτός καθορίζει αν η δέσμευση του label αντιστοιχεί για παράδειγμα απλά σε κάποιον προορισμό ή σε ένα ζεύγος αφετηρίας – προορισμού. Ο Upstream κόμβος δεσμεύει το δικό του label για αυτόν τον τύπο προορισμού και ενημερώνει με την σειρά του τον δικό του Upstream κόμβο [π.χ. στην υλοποίηση του MPLS από την Cisco σε δρομολογητές έχουμε δει downstream allocation].

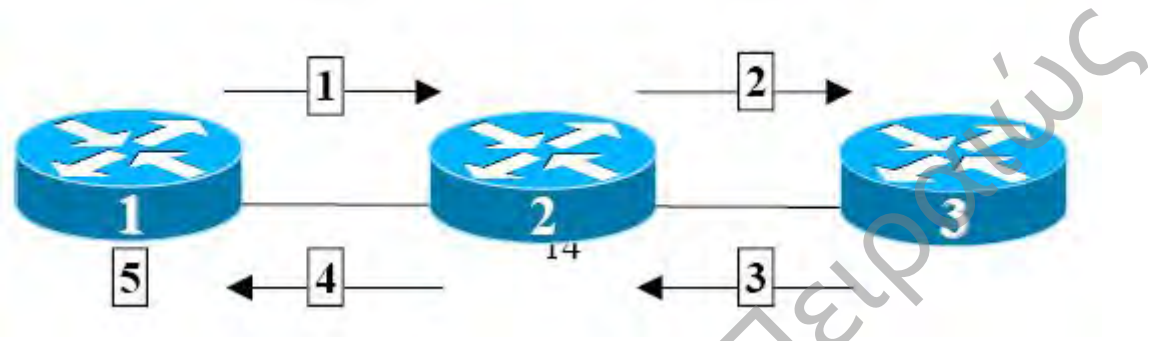
Downstream-on-demand allocation. Ο Upstream κόμβος ζητά από τον Downstream κόμβο να του δεσμεύσει ένα label για κάποιο τύπο προορισμού. Ο Downstream κόμβο προωθεί το μήνυμα στον δικό του Downstream κόμβο. Όταν το μήνυμα φτάσει στον προορισμό ακολουθείται η αντίστροφη διαδικασία η οποία είναι όμοια με την Downstream allocation.

Upstream allocation. Ο Upstream κόμβος δεσμεύει ένα label για κάποιο τύπο προορισμού και στην συνέχεια το στέλνει στον Downstream κόμβο. Η διαδικασία επαναλαμβάνεται μέχρι το μήνυμα να φτάσει στον Downstream κόμβο προορισμό.

Upstream-on-demand allocation. Ο Downstream κόμβος ζητάει από τον Upstream κόμβο να δεσμεύσει ένα label για κάποιο προορισμό και ακολουθείται η διαδικασία της μεθόδου Upstream allocation.

Implicit Upstream allocation. Το πρώτο πακέτο της κάθε ροής μεταφέρει το label το οποίο θα χρησιμοποιηθεί από τα υπόλοιπα πακέτα της ροής.

Στο παρακάτω Σχήμα παρουσιάζεται ενδεικτικά η ανταλλαγή των labels όταν χρησιμοποιείται η τεχνική Downstream-on-demand allocation.



Downstream-on-demand allocation

1. Ο Upstream κόμβος (κόμβος 1) ζητά από τον Downstream (κόμβος 2) να δεσμεύσει ένα label (για κάποιο τύπο προορισμού).

2. Ο Downstream κόμβος (κόμβος 2) ζητά από τον δικό του Downstream (κόμβος 3) να δεσμεύσει ένα label για τον ίδιο τύπο προορισμού.

3. Ο κόμβος 3 (ως προορισμός) δεσμεύει ένα label, ενημερώνει την LIB του και μεταβιβάζει το label στον Upstream κόμβο 2.

4. Ο κόμβος 2 ενημερώνει την LIB του, δεσμεύει και στέλνει ένα label στον Upstream κόμβο (κόμβο 1).

5. Ο κόμβος 1 ενημερώνει την LIB του.

Είναι φανερό ότι η επιλογή της τεχνικής έναρξης δημιουργίας LSPs περιορίζει τις μεθόδους ανταλλαγής των labels, και αντίστροφα. Για παράδειγμα αν επιλέξουμε την data-driven δεν μπορούμε να χρησιμοποιήσομε την downstream allocation αφού το LSP δημιουργείται όταν αρχίσει η ροή των δεδομένων (από την αφετηρία – upstream κόμβο). Όμοια όταν χρησιμοποιούμε την topology driven δεν μπορούμε να χρησιμοποιήσουμε την implicit upstream allocation για προφανή λόγο.

Στον παρακάτω πίνακα, παρουσιάζονται οι επιτρεπόμενοι συνδυασμοί μεταξύ των τρόπων ανταλλαγής των labels και των μεθόδων έναρξης της δημιουργίας των LSPs

	Upstream allocation	**Upstream-on-demand allocation**	**Downstream allocation**	**Downstream-on-demand allocation**	**Implicit upstream**
Topology driven	X	X	X		
Data driven	X			X	X
Request driven	X	X	X	X	X

Αντιστοίχηση μεθόδων ανταλλαγής των labels με μεθόδους δημιουργίας LSPs

2.12 Διαστήματα Label

Τα label που χρησιμοποιούνται από ένα LSR για FEC-ομαδοποίηση Label κατηγοριοποιούνται ως εξής :

- **Ανά πλατφόρμα**- οι τιμές των label είναι μοναδικές για όλο το LSR. Τα Label διατίθενται από μία κοινή πηγή. Δεν υπάρχει περίπτωση σε δύο διαφορετικές διεπαφές τα label να έχουν την ίδια τιμή.

- **Ανά διεπαφή** – Το τιμές των Label σχετίζεται με τις διεπαφές. Πολλαπλές πηγές Label καθορίζονται, μία για κάθε διεπαφή .Έτσι σε κάθε διεπαφή αποστέλλονται labels από διαφορετική πηγή, επομένως υπάρχει πιθανότητα σε διαφορετικές διεπαφές να υπάρχουν ίδιες τιμές label.

2.13 Διατήρηση Label

Το MPLS καθορίζει την αντιμετώπιση των ομαδοποιημένων label-FEC που λαμβάνονται από LSRs τα οποία δεν είναι "γειτονικά". Δύο τρόποι υπάρχουν :

- **Συντηρητικός** – εδώ οι συσχετίσεις μεταξύ label και FEC που λαμβάνονται από τα μη γειτονικά LSR καταργούνται. Αυτός ο τρόπος απαιτεί έναν LSR να διατηρεί λιγότερα label. Η μέθοδος αυτή είναι και η προτεινόμενη για τα ATM-LSRs

- **Ελεύθερος** - εδώ οι συσχετίσεις μεταξύ label και FEC που λαμβάνονται από τα μη γειτονικά LSR διατηρούνται. Αυτή η μέθοδος επιτρέπει γρηγορότερη υιοθέτηση των αλλαγών της τοπολογίας και επιτρέπει τη μεταγωγή (switching) κίνησης σε άλλα LSPs σε περίπτωση αλλαγών

2.14 Έλεγχος Label

Το MPLS καθορίζει δύο τρόπους διανομής των label στα γειτονικά LSRs

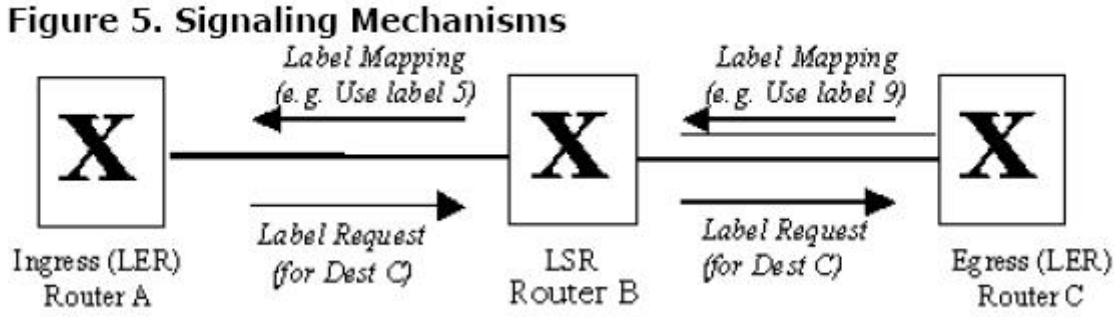
- **Ανεξάρτητος –** εδώ ένας LSR αναγνωρίζει ένα ιδιαίτερο FEC και παίρνει την απόφαση να εισαγάγει ένα label στο FEC ανεξάρτητα , χωρίς να ανακοινώσει αυτή την εισαγωγή στους άλλους peers. Τα νεα FECs αναγνωρίζονται όταν νέες διαδρομές γίνονται ορατές στον δρομολογητή.

- **Διαταγμένος** – εδώ ένα LSR εισάγει ένα label σε ένα συγκεκριμένο FEC αν και μόνο αν είναι εξωτερικός router ή αν έχει λάβει μία συσχέτιση label για το FEC από το LSR του επόμενου άλματος. Αυτή η μέθοδος προτείνεται για τα ATM-LSRs.

2.15 Μηχανισμοί σηματοδοσίας

- **Αιτήσεις Label –** χρησιμοποιώντας αυτόν τον μηχανισμό , ένας LSR ζήταει ένα label από το κατώτερο γειτονικό LSR έτσι ώστε να μπορεί να το συνδέσει σε ένα συγκεκριμένο FEC. Αυτός ο μηχανισμός μπορεί να εφαρμόζεται αλυσιδωτά προς τα κάτω μέχρι τον LSR εξόδου (μέχρι το σημείο που το πακέτο εξέρχεται από το την περιοχή του MPLS)

- **Χαρτογράφηση Label –** σε απάντηση μίας αίτησης label , κατώτερος LSR θα στείλει ένα label στον ανώτερο LSR χρησιμοποιώντας τον μηχανισμό χαρτογράφησης

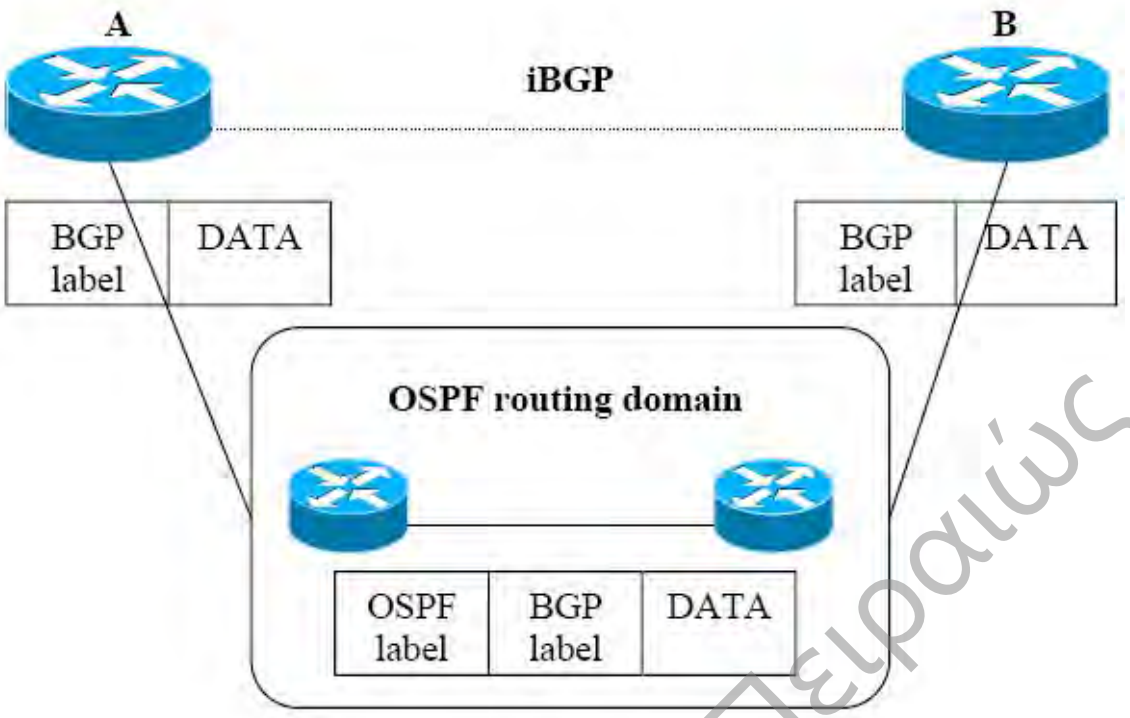


2.16 Στοίβα Label (label stack)

Ο μηχανισμός label stack επιτρέπει την ιεραρχική λειτουργία μέσα στην MPLS περιοχή. Βασικά επιτρέπει στο MPLS να χρησιμοποιείται ταυτόχρονα για δρομολόγηση σε χαμηλό επίπεδο (π.χ μεταξύ ανεξάρτητων router μέσω ενός παροχέα internet [ISP]) και σε ένα υψηλότερο επίπεδο (π.χ domain-by-domain). Κάθε επίπεδο στο Label Stack αναφέρεται σε κάποιο ιεραρχικό επίπεδο. Αυτό διευκολύνει την λειτουργία του Tunneling στην εφαρμογή του MPLS.

MPLS tunnels

Ένα ιδιαίτερα ενδιαφέρον αποτέλεσμα της τεχνικής στοίβας ετικετών είναι η δημιουργία tunnels κατά τρόπο όμοιο των γνωστών tunnels που δημιουργούνται μέσω netwotk layer encapsulation. Εδώ το tunnel υλοποιείται ως ένα LSP μεταγωγής με ετικέτα. Είναι επίσης σημαντικό να πούμε ότι τα LSP tunnels μπορούν να οργανωθούν σε ιεραρχίες, όπου κάθε ιεραρχία αντιστοιχεί σε ένα επίπεδο της στοίβας ετικετών. Ως ένα παράδειγμα μιας ιδιαίτερα χρήσιμης εφαρμογής των MPLS tunnels είναι τα IP-VPNs.
Για παράδειγμα έστω ένα δίκτυο όπου οι εσωτερικοί δρομολογητές εντός του domain τρέχουν OSPF και γνωρίζουν μόνο πως να φτάσουν σε προορισμούς εντός του OSPF domain. Το domain αυτό μπορεί να έχει αρκετούς AS δρομολογητές (Autonomous System Border Routers - ASBRs) που μεταξύ τους να μιλούν BGP (iBGP). Έστω επίσης ότι το BGP δεν διανέμεται στο OSPF και οι LSRs που δεν είναι στα άκρα δεν τρέχουν BGP.



Labelled tunnel

Μεταξύ των ακραίων δρομολογητών (ASBRs) χρησιμοποιείται μια επέκταση του BGP-4 για την ανταλλαγή ετικετών μεταξύ των γειτονικών (ως προς το BGP) δρομολογητών. Στο εσωτερικό δίκτυο την ανταλλαγή των ετικετών αναλαμβάνει το LDP.

Έστω ένα IP πακέτο χωρίς ετικέτα φτάνει στον κόμβο A, αυτός προσθέτει στη στοίβα μία ετικέτα, αυτή έχει νοήμα μόνο για τον γειτονικό του (ως προς BGP) κόμβο B, θυμηθείτε ότι η ανταλλαγή των ετικετών εδώ έγινε μέσω του BGP. Όταν το πακέτο εισέρχεται στο δίκτυο OSPF, ο κόμβος εισόδου του OSPF δικτύου προσθέτει μία ακόμη ετικέτα στη στοίβα, ένα OSPF label. Στην συνέχεια το προωθεί στο επόμενο κόμβο. Όταν το πακέτο φτάσει στο κόμβο εξόδου του OSPF δικτύου, αυτός θα αφαιρέσει το OSPF label από τη στοίβα και θα προωθήσει το πακέτο στον κόμβο B ο οποίος και θα δει το BGP label.

2.17 Traffic Engineering

Το traffic engineering είναι μία λειτουργία η οποία ενισχύει την συνολική απόδοση του δικτύου προσπαθώντας να δημιουργήσει μία ομοιόμορφη ή διαφοροποιημένη διανομή της κίνησης μέσα στο δίκτυο. Ένα σημαντικό αποτέλεσμα αυτής της διαδικασίας είναι η αποφυγή συμφόρησης σε οποιοδήποτε κανάλι. Είναι απαραίτητο να γνωρίζουμε ότι η διαδικασία του traffic engineering δεν επιλέγει απαραίτητα το μικρότερο κανάλι μεταξύ δύο συσκευών. Είναι

δυνατό για δύο ροές πακέτων δεδομένων να επιλεχθούν δύο τελείως διαφορετικές διαδρομές ακόμα και αν η πηγή προέλευσης των δεδομένων και ο προορισμός είναι ίδια. Μ' αυτόν τον τρόπο τα λιγότερα εκτεθειμένα – χρησιμοποιημένα στοιχεία δικτύου μπορεί να χρησιμοποιηθούν και να εφαρμοστούν διαφοροποιημένες υπηρεσίες.

Στο MPLS, το traffic engineering εγγενώς παρέχεται χρησιμοποιώντας ρητές (explicit) καθοδηγημένες πορείες. Τα LSPs δημιουργούνται ανεξάρτητα , καθορίζοντας διαφορετικές διαδρομές που βασίζονται σε διευκρινισμένες από τον χρήστη πολιτικές. Βέβαια αυτό ίσως απαιτεί εκτενής επεμβάσεις του διαχειριστή. Το RSVP και CR-LDP είναι δύο λύσεις που παρέχουν δυναμικά υπηρεσίες traffic engineering και ποιότητας υπηρεσίας στο MPLS.

2.18 CR - Constraint-based Routing

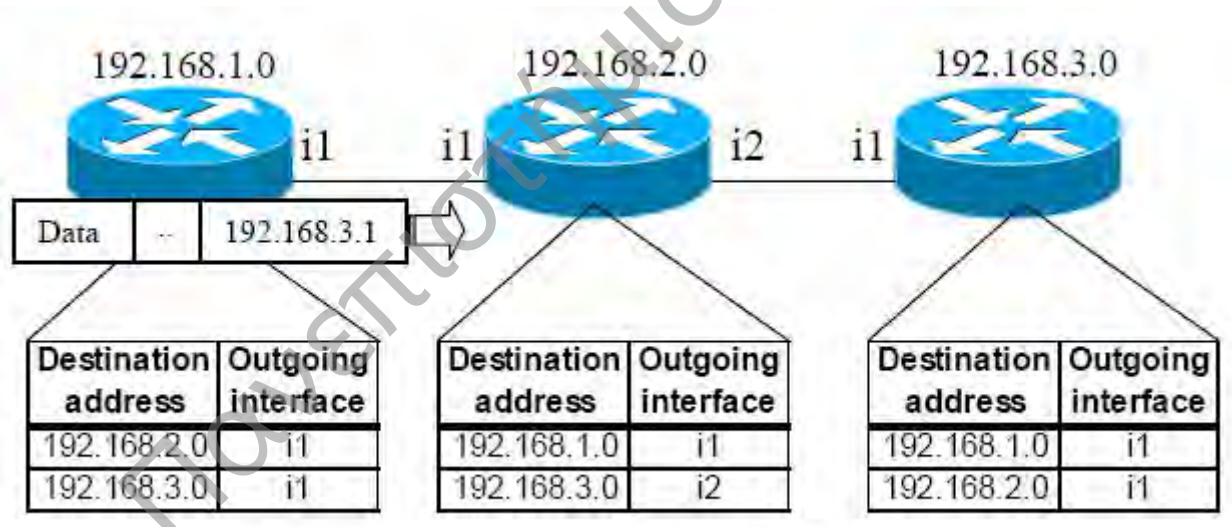
Η βασισμένη σε περιορισμούς δρομολόγηση (CR) αναλογίζεται παραμέτρους όπως χαρακτηριστικά γραμμής (εύρος ζώνης , καθυστερήσεις , κλπ) , αρίθμηση περασμάτων (hop count) και ποιότητα υπηρεσίας (QoS).Τα LSPs που καθιερώνονται μπορεί να είναι CR-LSPs, όπου οι περιορισμοί για παράδειγμα να είναι συγκεκριμένες απαιτήσεις QoS ή προκαθορισμένος αριθμός hop. Οι απαιτήσεις QoS υπαγορεύουν ποιες γραμμές και ποιοι μηχανισμοί αναμονής ή σχεδιασμού θα εφαρμοστούν για τη ροή δεδομένων.

Χρησιμοποιώντας την δρομολόγηση CR είναι πολύ πιθανό να επιλέγονται μακρύτερες αλλά λιγότερο φορτωμένες διαδρομές. Παρόλο που το CR αυξάνει την χρηστικότητα του δικτύου προσθέτει πολυπλοκότητα στους υπολογισμούς δρομολόγησης , καθώς η διαδρομή που επιλέγεται πρέπει να ικανοποιεί τις QoS απαιτήσεις του LSP. Το CR μπορεί να χρησιμοποιείται στο MPLS για την εγκατάσταση των LSPs. Η IETF έχει καθορίσει το CR-LDP στοιχείο για να διευκολύνει τις CR διαδρομές **.**

Κεφάλαιο 3 - Λειτουργία του MPLS

3.1 Προώθηση στο MPLS

Η διαδικασία προώθησης σε ένα δίκτυο MPLS χωρίζεται σε δύο μέρη. Στο πρώτο μέρος εκτελούνται τα παραδοσιακά πρωτόκολλα δρομολόγησης και δημιουργούνται οι γνωστοί πίνακες δρομολόγησης. Στην συνέχεια, οι LSRs για κάθε εγγραφή του πίνακα δρομολόγησης επικοινωνούν με τους γειτονικούς τους κόμβους (σύμφωνα με ορισμένα κριτήρια) για την ανταλλαγή των labels τα οποία θα χρησιμοποιηθούν για την μεταγωγή των πακέτων.

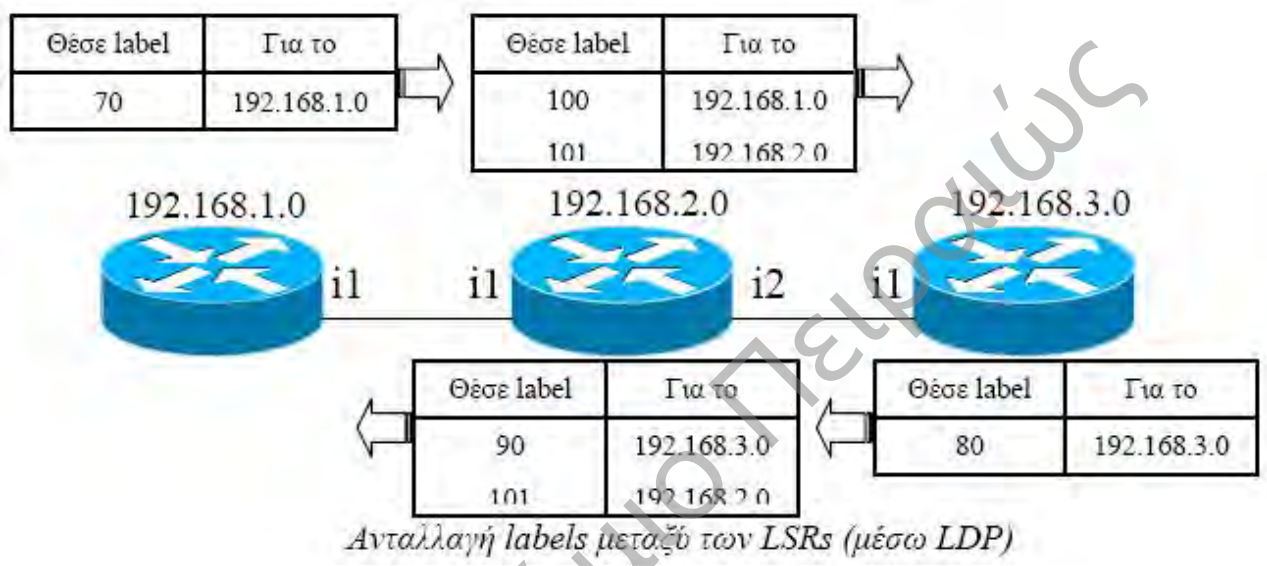


Η δρομολόγηση στους παραδοσιακούς IP δρομολογητές

Σχήμα 3.1

Σύμφωνα με τον παραδοσιακό τρόπο δρομολόγησης (Βλ. Σχήμα 3.1), πρώτα φτιάχνονται οι πίνακες δρομολόγησης από συγκεκριμένα πρωτόκολλα (RIP, OSPF κλπ) και στην συνέχεια τα δεδομένα αποστέλλονται σε πακέτα με την διεύθυνση προορισμού στην κεφαλή κάθε ενός από αυτά.

Στο παράδειγμα,(Σχήμα 3.2), ο κόμβος 192.168.1.0 ενημερώνει τον Up/Down stream κόμβο 192.168.2.0 ότι πακέτα που προορίζονται για το 192.168.1.0 να φέρουν το label 70. Ο κόμβος αυτός (192.168.2.0) με την σειρά του ενημερώνει τον Up/Down stream κόμβο 192.168.3.0 ότι πακέτα με προορισμό τα 192.168.1.0 και 192.168.2.0 να φέρουν τα labels 100 και 101 αντίστοιχα.



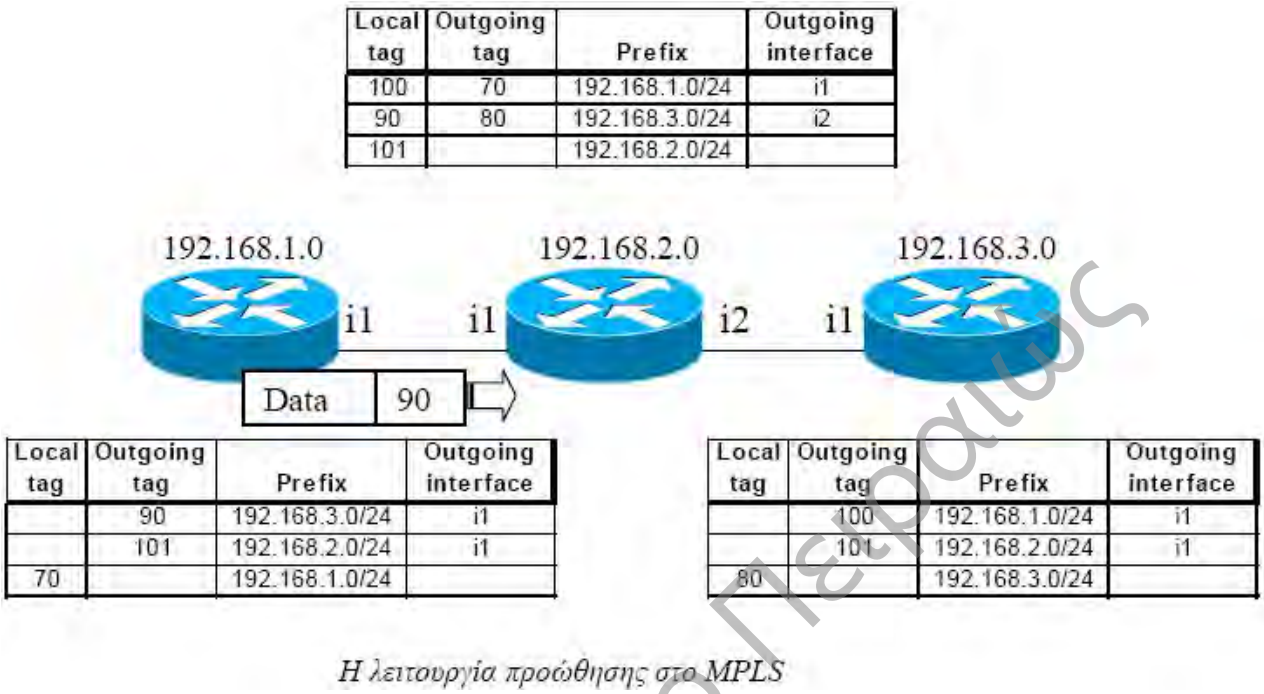
Ανταλλαγή labels μεταξύ των LSRs (μέσω LDP)

Σχήμα 3.2

Οι διαδρομές αυτές, γνωστές ως FECs (Forwarding Equivalence Classes), δημιουργούνται μόνο προς την μία κατεύθυνση. Η αντίστροφη διαδικασία, στο παράδειγμα από τον κόμβο 192.168.3.0 προς τον κόμβο 192.168.1.0, είναι απαραίτητη για ολοκλήρωση της διαδικασίας. Οι δύο κατευθύνσεις (FECs) μιας διαδρομής μεταξύ δύο κόμβων μπορεί να διέρχονται από διαφορετικούς ενδιάμεσους κόμβους.

Όταν ο κόμβος 192.168.1.0 θέλει να στείλει ένα πακέτο στον κόμβο 192.168.3.0, αυτό το πακέτο πλαισιώνεται από το MPLS σύμφωνα με τα στοιχεία του πίνακα προώθησης (Forwarding Information Base – FIB). Στο παράδειγμα, Σχήμα 3.3 τοποθετείται το label 90 στην κεφαλή του πακέτου και προωθείται στον επόμενο κόμβο διαμέσου του interface i1. Όταν ο ενδιάμεσος κόμβος 192.168.2.0 παραλάβει ένα πακέτο με label 90 χρησιμοποιεί την τιμή του label (και μόνο αυτή) ως δείκτη στον δικό του πίνακα προώθησης για να αποφασίσει πως θα προωθήσει το πακέτο αυτό. Στη προκείμενη περίπτωση, μεταβάλει την τιμή του label (από 90 σε 80) και προωθεί το πακέτο κατάλληλα.

Στον κόμβο εξόδου, 192.168.3.0, το label απομακρύνεται και το πακέτο παραδίδεται στον προορισμό του.



Η λειτουργία προώθησης στο MPLS

Σχήμα 3.3

Γενικά, σε κάθε πακέτο που εισέρχεται στο MPLS δίκτυο ανατίθεται ένα label (π.χ. για δρομολογητές μία σταθερού και μικρού μήκους τιμή μεγέθους 32bits) το οποίο τοποθετείται στην κεφαλή του πακέτου. Η ανάθεση γίνεται στον κόμβο εισόδου του δικτύου. Στην συνέχεια το πακέτο προωθείται στον επόμενο κόμβο μαζί με την ετικέτα αυτή. Σε κάθε ενδιάμεσο κόμβο γίνεται επεξεργασία μόνο της ετικέτας του πακέτου (σε επίπεδο δικτύου) με τρόπο ώστε η ετικέτα να χρησιμοποιείται ως δείκτης μέσα στον πίνακα μεταγωγής (Label Information Base –LIB). Στο πίνακα αυτό κάθε πλειάδα έχει την μορφή <ετικέτα εισόδου, διεπαφή εισόδου, διεπαφή εξόδου, ετικέτα εξόδου>. Η παλιά ετικέτα αντικαθίσταται από μία νέα ετικέτα και προωθείται στον επόμενο κόμβο. Στους κλασικούς IP δρομολογητές η κεφαλή του πακέτου υφίσταται επεξεργασία σε επίπεδο δικτύου όχι μόνο για να προωθηθεί το πακέτο στον επόμενο κόμβο αλλά και για να καθοριστεί η κλάση υπηρεσίας στην οποία ανήκει το πακέτο αυτό (π.χ. στα Integrated και Differentiated Services). Το MPLS επιτρέπει την μεταφορά όλης αυτής της πληροφορίας στην ετικέτα (αφού τα χαρακτηριστικά της κλάσης και οι διαδρομές έχουν εξαρχής προκαθοριστεί, όπως ισοδύναμα συμβαίνει στα δίκτυα ATM) και έτσι δεν χρειάζεται περαιτέρω επεξεργασία η κεφαλή του πακέτου σε επίπεδο 3.

Η παρουσία μιας LIB σε κάθε κόμβο επιτρέπει την δημιουργία ιδεατών μονοπατιών από κάθε κόμβο προς οποιοδήποτε άλλον κόμβο. Ένα τέτοιο μονοπάτι είναι μια ακολουθία από labels η οποία ξεκινάει από ένα LSR εισόδου και τελειώνει σε ένα LSR εξόδου. Τα LSPs μοιάζουν πολύ με τα μονής κατεύθυνσης VP/VCs του ATM. Η αντιστοίχηση μεταξύ ενός παραδοσιακού πίνακα δρομολόγησης και μιας LIB είναι της μορφής «ένα προς πολλά» αφού σε κάθε κόμβο μπορούμε να δεσμεύσουμε πολλά labels για τον ίδιο προορισμό όχι όμως το ίδιο label για διαφορετικούς προορισμούς. Μια εγγραφή στην LIB αντιστοιχεί σε μία και μόνο μια εγγραφή του παραδοσιακού πίνακα δρομολόγησης έτσι εξασφαλίζεται η μοναδικότητα ενός label για κάθε προορισμό πράγμα απαραίτητο αφού πλέον η δρομολόγηση γίνεται αποκλειστικά με βάση τα labels.

Το γεγονός ότι σε κάθε πακέτο που μπαίνει στο δίκτυο ανατίθεται μια ετικέτα επιτρέπει την εφαρμογή μιας αποτελεσματικής τεχνικής προώθησης. Επιπλέον ο διαχωρισμός, μέσω του MPLS, των λειτουργιών της μεταγωγής και της δρομολόγησης δίνει την δυνατότητα να υποστηριχθούν διαφορετικές πολιτικές δρομολόγησης οι οποίες θα ήταν δύσκολο ή αδύνατον να εφαρμοστούν στα συμβατικά πρωτόκολλα δρομολόγησης τα οποία κάνουν την προώθηση των πακέτων σε επίπεδο δικτύου (χωρίς να διαχωρίζουν την δρομολόγηση από την προώθηση, με αποτέλεσμα να μην είναι δυνατή η εναλλακτική δρομολόγηση).

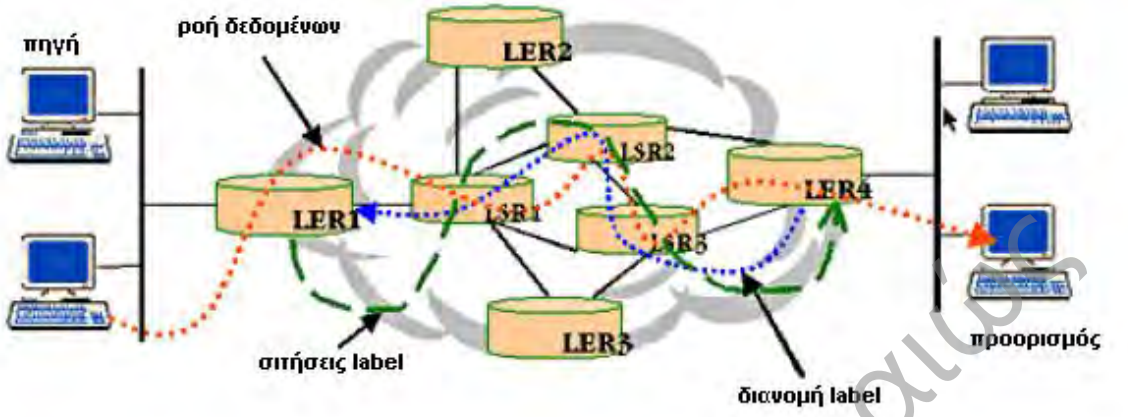
Ένα άλλο πλεονέκτημα, στην περίπτωση του MPLS over ATM, του διαχωρισμού της λειτουργίας της δρομολόγησης από την λειτουργία της μεταγωγής είναι ότι μας επιτρέπει να εφαρμόσουμε την λειτουργία της προώθησης σε επίπεδο 2, το οποίο έχει ως αποτέλεσμα να έχουμε σημαντική βελτίωση των επιδόσεων.

3.2 Ροή δεδομένων στο MPLS

Τα βήματα που γίνονται για να ταξιδέψει ένα πακέτο μέσω της MPLS περιοχής είναι τα εξής :

1. Δημιουργία Label και διανομή
2. Δημιουργία πινάκων σε κάθε δρομολογητή
3. Δημιουργία των LSPs
4. Εισαγωγή των label/Συμβουλή από πίνακες
5. Προώθηση πακέτου

Η πηγή στέλνει τα δεδομένα της στον προορισμό. Σ' ένα MPLS δίκτυο δεν είναι απαραίτητο όλη η κίνηση να μεταδοθεί από το ίδιο μονοπάτι. Εξαρτώμενα από τα χαρακτηριστικά της κίνησης Δημιουργούνται διαφορετικά LSPs που μπορεί να έχουν και διαφορετικές CoS απαιτήσεις.



Σχήμα 3.4
Δημιουργία και διανομή πακέτων διαμέσω ενός MPLS δικτύου

Ο παρακάτω πίνακας παραθέτει τις λειτουργίες που γίνονται στα πακέτα δεδομένων στο MPLS δίκτυο

Ενέργειες MPLS	**Περιγραφή**
Δημιουργία Label και Διανομή Label	**Πριν οποιαδήποτε κίνηση ξεκινήσει οι δρομολογητές παίρνουν την απόφαση να συσχετίσουν ένα label σ' ένα συγκεκριμένο FEC και να δημιουργήσουν τους πίνακες τους** **Με τη χρήση του LDP οι δρομολογητές ξεκινούν την διανομή των label και την FEC ομαδοποίηση** **Επιπλέον, τα χαρακτηριστικά της κίνησης και οι δυνατότητες του MPLS διαπραγματεύονται χρησιμοποιώντας το LDP** **Ένα αξιόπιστο πρωτόκολλο μεταφοράς χρησιμοποιείται για το πρωτόκολλο σηματοδοσίας .Το LDP χρησιμοποιεί TCP.**
Δημιουργία πίνακα	**Με την παραλαβή των συσχετίσεων label κάθε LSR κάνει εισαγωγές στην βάση πληροφοριών label (LIB).** **Τα περιεχόμενα του πίνακα θα καθορίσουν την χαρτογράφηση label-FEC.** **Η χαρτογράφηση ανάμεσα σε θύρα εισαγωγής και πίνακα εισόδου label** **σε θύρα εξαγωγής και πίνακα label εξόδου.**

	Τα δεδομένα ενημερώνονται σε κάθε επαναδιαπραγμάτευση που γίνεται στις συσχετίσεις των label.
Δημιουργία των LSPs	**Όπως φαίνεται από τις διακεκομμένες μπλε γραμμές στο παραπάνω σχέδιο τα LSPs δημιουργούνται στην ανάποδη κατεύθυνση σε σχέση με την δημιουργία εισαγωγών της LIB.**
Εισαγωγή των label Συμβουλή από πίνακες	**Ο πρώτος δρομολογητής (LER 1 στο σχέδιο) χρησιμοποιεί τον LIB πίνακα για να βρει το επόμενο hop και να ζητήσει ένα label για το συγκεκριμένο FEC.** **Οι ενδιάμεσοι δρομολογητές απλά χρησιμοποιούν το label για να βρουν το επόμενο πέρασμα.** **Όταν το πακέτο θα φτάσει το LSR εξόδου(LER 4),το label απομακρύνεται και το πακέτο παρέχεται στον προορισμό .**
Προώθηση πακέτου	**Αναφερόμενοι στο παραπάνω σχέδιο ας εξετάσουμε τη διαδρομή ενός πακέτου από το LER1 (LSR εισόδου) στο LER4 (LSR εξόδου).** **Το LER1 ίσως δεν έχει κάποιο label γι' αυτό το πακέτο καθώς είναι η πρώτη εμφάνιση τέτοιας αίτησης. Σ' ένα IP δίκτυο , θα βρεί τη πιο μακροχρόνια αντιστοιχία διευθύνσεων για να βρεί το επόμενο άλμα (hop). Το LSR1 θα είναι το επόμενο άλμα για το LER1.** **Το LER1 θα κάνει μία αίτηση label προς το LSR1.** **Αυτή η αίτηση θα διαδοθεί μέσω του δικτύου όπως φαίνεται και από τις πράσινες γραμμές.** **Κάθε επόμενος LSR (πχ LSR! και LSR3) θα εξετάσει το label στο πακέτο που παρέβαλε , θα το αντικαταστήσει με το label εξόδου και θα το προωθήσει** **Όταν το πακέτο φτάσει στον LER4 θα του αφαιρεθεί το label, επειδή φευγει από το MPLS δίκτυο , και θα μεταφερθεί (το πακέτο) στον προορισμό** **Το μονοπάτι δεδομένων διαφαίνεται με τις κόκκινες γραμμές**

Παράδειγμα ροής δεδομένων

Το παρακάτω σχέδιο παρουσιάζει ένα MPLS Δίκτυο και άμεσα συνδεδεμένα στοιχεία του. Το κεντρικό σύννεφο εκπροσωπεί το αυτούσιο MPLS

δίκτυο. Όλη η κίνηση δεδομένων μέσα στο σύννεφο αυτό γίνεται με την τεχνολογία MPLS , αντίθετα η κίνηση ανάμεσα στο σύννεφο και στα δίκτυα των πελατών γίνεται μέσω κάποιου άλλου πρωτοκόλλου –τεχνολογίας (πχ IP) . Οι δρομολογητές που ανήκουν στον πελάτη (Customer Edged (CE)) συνδέονται με τους δρομολογητές του παρόχου (Provider Edge (PE) ή Label Edge Routers (LERs)). Στην είσοδο του MPLS δικτύου οι PE δρομολογητές προσθέτουν labels στα πακέτα . Αντίθετα στην έξοδο του MPLS δικτύου οι PE δρομολογητές αφαιρούν τα labels. Μέσα τώρα στο MPLS σύννεφο οι P(Provider) δρομολογητές (οι γνωστοί μας label Switching Routers (LSRs)), μεταφέρουν την κίνηση από πέρασμα σε πέρασμα (hop by hop)

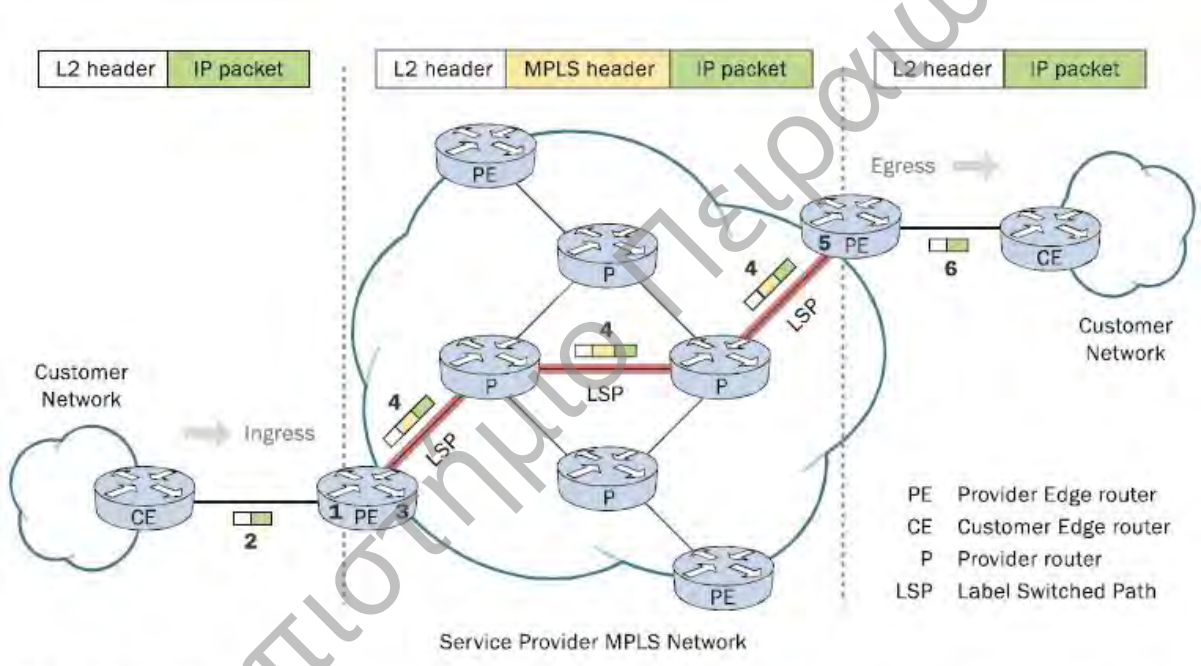


Figure 2. MPLS network.

Για την καλύτερη κατανόηση της MPLS διαδικασίας ακολουθούν τα βήματα ροής δεδομένων σύμφωνα με το παραπάνω σχέδιο

1.Πριν γίνει η προώθηση της κίνησης στο MPLS δίκτυο, ο ι PE δρομολογητές καθορίζουν τα LSPs προς τους απομακρυσμένους PE δρομολογητές

2.Η μη MPLS κίνηση (Frame Relay, ATM, Ethernet, κλπ.) διαβιβάζεται από το δίκτυο του πελάτη μέσω του CE δρομολογητή στην είσοδο του MPLS δικτύου και συγκεκριμένα στον PE δρομολογητή εισόδου του πάροχου

3.Ο PE δρομολογητής εξετάζει τις πληροφορίες του πακέτου ώστε να το κατηγοριοποιήσει ,να το συνδέσει , σε ένα FEC.Ύστερα προσθέτει τα κατάλληλα MPLS label(s) στο πακέτο

4.Το πακέτο ταξιδεύει στο LSP του , με κάθε ενδιάμεσο δρομολογητή P να ανταλλάσσει τις ετικέτες όπως διευκρινίζεται από τις πληροφορίες του LIB , για να οδηγηθεί το πακέτο στο επόμενο πέρασμα (hop)

5.Στον PE δρομολογητή εξόδου, απομακρύνεται το τελευταίο MPLS label και το πακέτο προωθείται πλέον με τους παραδοσιακούς μηχανισμός δρομολόγησης.

6.Το πακέτο φτάνει στον προορισμό CE (δρομολογητής πελάτη) και στο δίκτυο του πελάτη.

Κεφάλαιο 4 - MPLS Traffic Engineering (εφαρμοσμένη μηχανική κυκλοφορίας)

Το MPLS Traffic Engineering (MPLS TE) είναι μια αναπτυσσόμενη εφαρμογή στα σημερινά δίκτυα των φορέων παροχής υπηρεσιών. Η υιοθέτηση του MPLS στα δίκτυα αυτά έχει αυξηθεί λόγω των έμφυτων TE ικανοτήτων. Το MPLS TE επιτρέπει στο MPLS δίκτυο να ξεδιπλωθεί και να επεκταθεί επάνω στις ικανότητες TE των ATM και FRAME RELAY δικτύων (επίπεδο 2).
Το MPLS χρησιμοποιεί την ικανότητα να λαμβάνει πληροφορίες που παρέχονται από τα πρωτόκολλα δρομολόγησης επιπέδου3 και λειτουργεί όπως το επιπέδου 2 δίκτυο ATM.

Με το MPLS, οι TE ικανότητες είναι ενσωματωμένες στο στρώμα 3, οι οποίες μπορούν να εφαρμοστούν για την αποδοτικότερη χρησιμοποίηση εύρους ζώνης μεταξύ των δρομολογητών στο δίκτυο του των φορέων παροχής υπηρεσιών. Τα δίκτυα αυτά απαιτούνται να κάνουν υψηλή χρήση της δυνατότητας μετάδοσης και πρέπει να είναι πολύ «ελαστικά», ώστε να μπορούν να αντιμετωπίσουν αποτυχίες συνδέσεων και κόμβων.

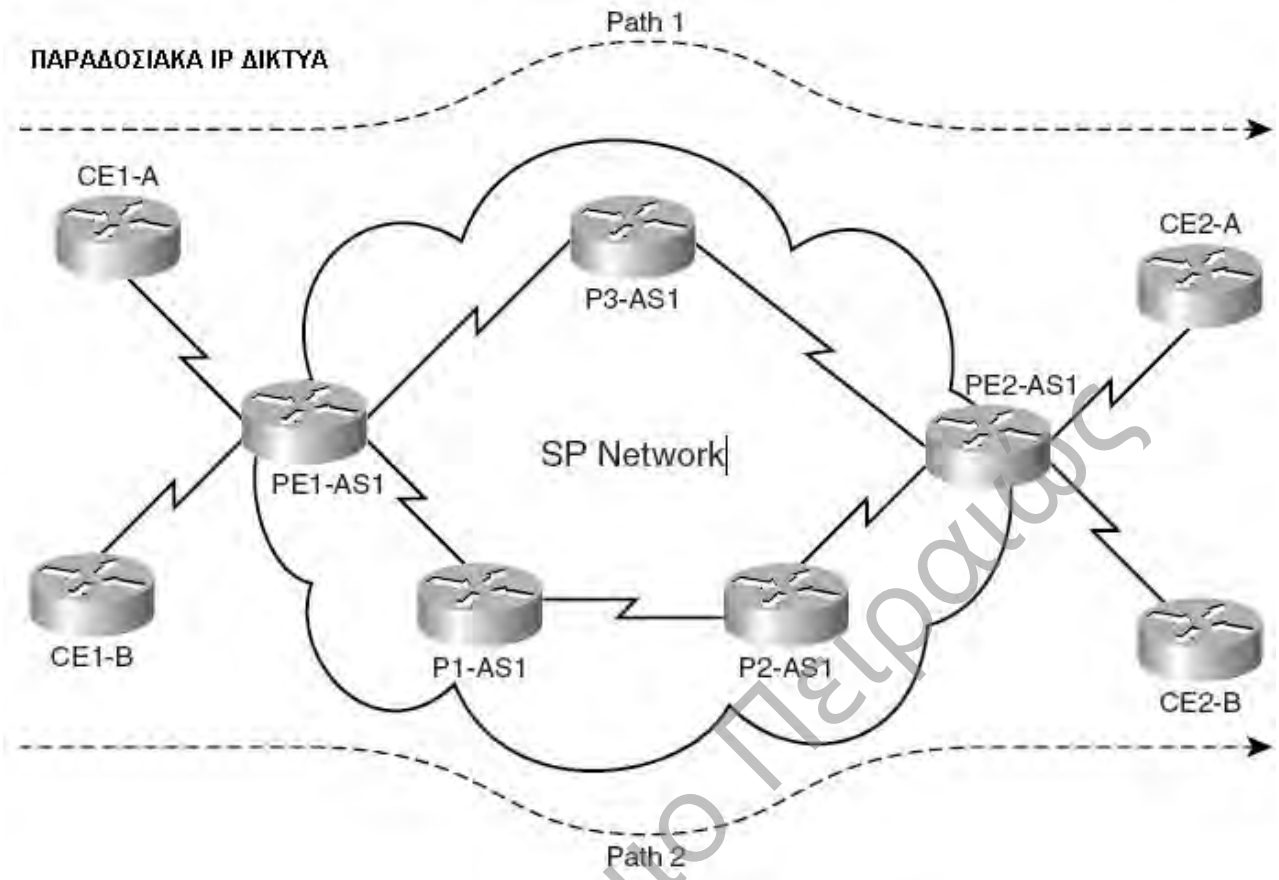
4.1 Τα βασικά περί Traffic Engineering

Traffic Engineering είναι η διαδικασία κατά την οποία η κίνηση κατευθύνεται πάνω στο κεντρικό δίκτυο (backbone) ώστε να γίνει η αποδοτικότερη δυνατή χρήση του διαθέσιμου εύρους ζώνης μεταξύ δύο δρομολογητών.
Πριν την εφαρμογή του MPLS TE, η λειτουργία traffic engineering γινόταν είτε από το IP η από το ATM, εξαρτιόταν από το πρωτόκολλο που χρησιμοποιούταν ανάμεσα στους 2 εξωτερικούς (edge) δρομολογητές στο δίκτυο.

Έτσι αν και ο όρος «traffic engineering» έγινε ιδιαίτερα γνωστός με την τεχνολογία MPLS , το παραδοσιακό TE πρωτοεμφανίστηκε στα IP και ATM δίκτυα.

Το TE στο IP κυρίως εφαρμόστηκε για την διαχείριση του κόστους των διεπαφών (interfaces) όταν υπήρχαν πολλαπλά μονοπάτια ανάμεσα σε δύο άκρα σε ένα δίκτυο. Αντίθετα οι στατικές διαδρομές ενεργοποιούσαν την κατεύθυνση της κίνησης πάνω σε ένα συγκεκριμένο μονοπάτι προς έναν προορισμό. Το Σχήμα 4.1 περιγράφει ένα βασικό IP δίκτυο με δύο πελάτες (A και B) συνδεδεμένους στον ίδιο φορέα παροχής υπηρεσιών. Όπως φαίνεται υπάρχουν δύο διαδρομές ανάμεσα στα router των πελατών (CE1-A και CE2-A) μέσω του SP δικτύου. Αν το κόστος όλων των συνδέσεων ήταν ίδιο μεταξύ των router (σχέδιο 4.1), το προτιμότερο μονοπάτι μεταξύ των router (CE1-A και CE2-A) θα ήταν αυτό με το μικρότερο κόστος (μέσω των router PE1-AS1, P3-AS1, και PE2-AS1) ή PATH1. Το ίδιο θα εφαρμοστεί για τους δρομολογητές του πελάτη B (CE1-B και CE2-B). Αν όλες οι συνδέσεις ήταν τύπου T3, σε μια περίπτωση όπου ο CE1-A στέλνει 45 Mbps κίνηση και ο CE1-B ταυτόχρονα στέλνει με 10 Mbps, μερικά πακέτα θα χαθούν λόγω σύγκρουσης στο PE1-AS1 επειδή η ταχύτερη πορεία και για τους δύο πελάτες είναι το PATH1. Η διαδρομή PATH2 δεν θα χρησιμοποιηθεί για την προώθηση της κίνησης , έτσι, το TE μπορεί να χρησιμοποιήσει αυτό το διαθέσιμο εύρος. Για να εφαρμοστεί TE στο IP πρωτόκολλο όπου οι διαδρομές PATH1 και PATH2 θα είναι είτε ίσα φορτωμένες ή θα χρησιμοποιούνται ομοίως , θα πρέπει να εφαρμόσουμε τα χαρακτηριστικά γνωρίσματα του IGP (όπως μέγιστες πορείες με διαφορά ή αλλαγή του κόστους) που σχετίζονται με την εναλλακτική πορεία,. Σε ένα περιβάλλον SP (service provider) δικτύου αυτό είναι συχνά δυσκίνητο για να εφαρμοστεί δεδομένου ότι ο αριθμός δρομολογητών είναι πολύ μεγαλύτερος.

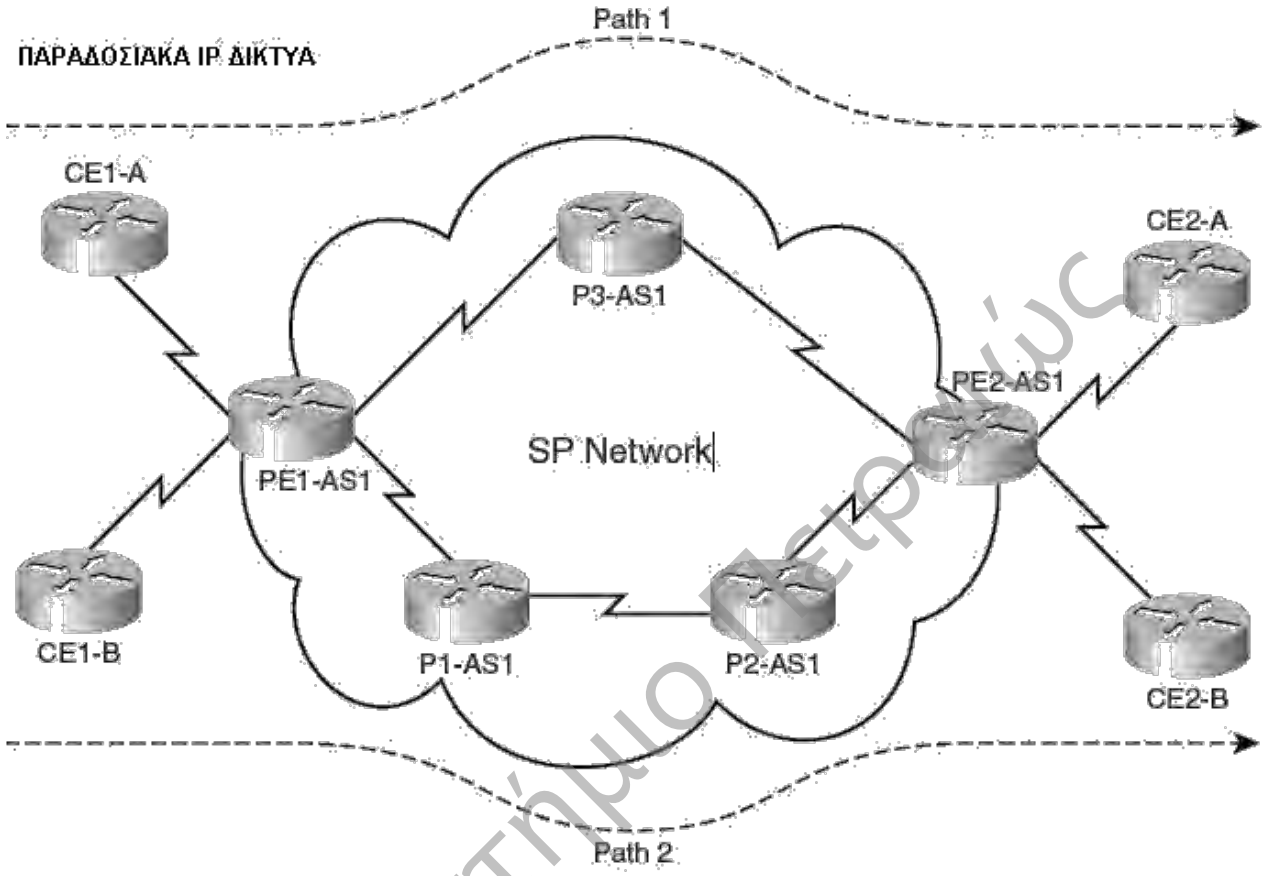
Σχήμα 4.1



Στα ATM δίκτυα ,η λύση είναι πιο εφικτή : PVCs μπορούν να ρυθμιστούν μεταξύ των router PE1-AS1 και PE2-AS1 με το ίδιο κόστος , αλλά αυτό θα δημιουργούσε ένα πλήρες πλέγμα από PVCs μεταξύ μιας ομάδας δρομολογητών. Από την άλλη πλευρά η εφαρμογή TE για ATM έχει ένα έμφυτο πρόβλημα όταν καταρρέει μία σύνδεση ή ένας κόμβος. Κατά την αποτυχία σύνδεσης ή κόμβου σε συνδυασμό με το TE ,μηνύματα πλημμυρίζουν το δίκτυο. Η Τοπολογία στρώματος 3 πρέπει να είναι κυρίως πλήρους πλέγματος για να εκμεταλλευτεί την επιπέδου 2 TE εφαρμογή.

Συχνά αυτό μπορεί να αποδειχθεί περιορισμός εξελισιμότητας για την χρήση του IGP, λόγω των ζητημάτων επαναφοράς στο επίπεδο 3. Το κυριότερο πλεονέκτημα της εφαρμογής MPLS TE είναι ότι παρέχει έναν συνδυασμό από τις δυνατότητες ATM's TE με την class of service (CoS) διαφοροποίηση του IP. Στο MPLS TE, ο επικεφαλής router στο δίκτυο ελέγχει την διαδρομή που θα ακολουθήσει η κίνηση προς ένα συγκεκριμένο προορισμό στο δίκτυο. Η απαίτηση εφαρμογής ενός πλήρους πλέγματος VCs ,όπως στο ATM, δεν υφίσταται όταν εφαρμόζεται MPLS TE. Σαν συνέπεια , όταν εφαρμόζεται MPLS TE στο IP δίκτυο ,που εμφανίζεται στο Σχήμα 4.1, μεταμορφώνεται σε περιοχή μεταφοράς label, όπως φαίνεται στο Σχήμα 4.2, όπου τα μονοπάτια μεταφοράς TE label (TE tunnels) (Tunnel1 and Tunnel2) καθορίζουν τις διαδρομές που μπορεί να χρησιμοποιηθούν για κίνηση μεταξύ των PE1-AS1 και PE2-AS1.

Σχήμα 4.2



4.2 MPLS TE – Γενικά

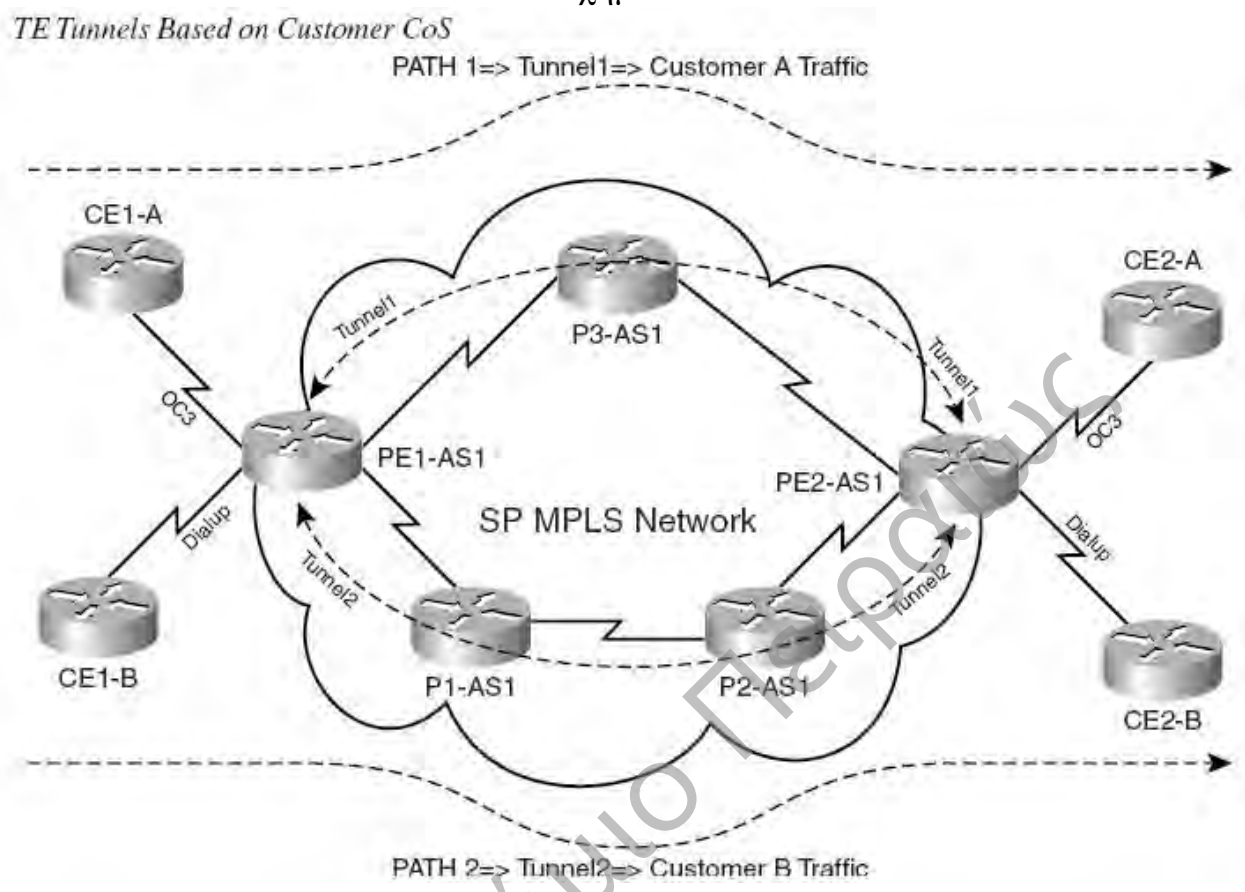
Στην περίπτωση της παραδοσιακής IP προώθησης, τα πακέτα προωθούνται ανά «άλμα» (hop) όπου γίνεται έλεγχος διαδρομής σε κάθε δρομολόγηση από την πηγή στον προορισμό. Όπως αναφέρεται και νωρίτερα η προώθηση βασισμένη στον προορισμό οδηγεί στη μειωμένη χρήση του διαθέσιμου εύρους ζώνης ανάμεσα σε δύο δρομολογητές του φορέα παροχής υπηρεσιών. Έτσι οι διαδρομές υποχρησιμοποιούνται στα IP δίκτυα. Για να αποφευχθούν οι πτώσεις πακέτων λόγω της ανεπαρκούς χρήσης του διαθέσιμου εύρους ζώνης και για την παροχής καλύτερης απόδοσης, εφαρμόζεται traffic engineering για να κατευθυνθεί μέρος της κίνησης από την κατάλληλη διαδρομή ώστε να ενεργοποιείται η καλύτερη διαχείριση και χρήση του διαθέσιμου εύρους ανάμεσα σε ένα ζεύγος δρομολογητών. Ως εκ τούτου το TE διευκολύνει προσωρινά την συμφόρηση στον πυρήνα του δικτύου πάνω στις αρχικές ή εναλλακτικές συνδέσεις

Το ΤΕ χαρτογραφεί τις ροές μεταξύ δύο δρομολογητών για να επιτρέψει κατάλληλα την αποδοτική χρήση του ήδη διαθέσιμου εύρους ζώνης στον πυρήνα του δικτύου. Το κλειδί για την εφαρμογή μιας εξελικτικής και αποδοτικής μεθοδολογίας ΤΕ στον πυρήνα του δικτύου είναι να συγκεντρωθούν οι πληροφορίες για τα σχέδια κυκλοφορίας (δεδομένου ότι διαπερνούν τον πυρήνα του δικτύου) έτσι ώστε οι εγγυήσεις εύρους ζώνης να μπορούν να καθιερωθούν. Όπως φαίνεται στο Σχήμα 4.3 τα ΤΕ τούνελ (Tunnel 1 και Tunnel 2), μπορεί να καθοριστούν στον δρομολογητή PE1-AS1 και να διαχωρίζουν τα πακέτα σε ξεχωριστά μονοπάτια (PATH1, PATH2), ενεργοποιώντας έτσι την αποδοτικότερη χρήση του διαθέσιμου εύρους.

Τα ΤΕ tunnels που καθορίζονται στους δρομολογητές είναι μονής κατεύθυνσης. Έτσι για να επιτευχθούν διπλής κατεύθυνσης ΤΕ τούνελ ανάμεσα στους δρομολογητές PE1-AS1 και PE2-AS1 (Σχήμα 4.3) ένα ζεύγος τούνελ πρέπει να καθοριστεί επίσης στον PE2-AS1 ομοίως με το Tunnel 1 και Tunnel 2 που ορίστηκαν στο PE1-AS1. Σε ένα MPLS δίκτυο , όλες οι σχετικές διαμορφώσεις τούνελ εκτελούνται πάντα στους δρομολογητές άκρων (PE) του παρόχου . Τα ΤΕ τούνελ ή LSPs θα χρησιμοποιηθούν για να συνδέσουν τους δρομολογητές ακρών μέσα από τον πυρήνα του δικτύου φορέων παροχής υπηρεσιών.

Το MPLS ΤΕ μπορεί επίσης να καταταχτεί σε ορισμένες κατηγορίες κυκλοφορίας σε σχέση με τους προορισμούς. Αν οι δρομολογητές του πελάτη A (CE routers) είναι συνδεδεμένοι στο δίκτυο του φορέα παροχής (SP) χρησιμοποιώντας τύπου OC3 σύνδεση και ο πελάτης B συνδέεται επίσης με το δίκτυο SP με 64 K dialup link, μπορεί να εφαρμοστεί προνομιακή μεταχείριση στα ΤΕ tunnels ώστε το ΤΕ Tunnel 1 να μεταφέρει την κίνηση του πελάτη A και το Tunnel 2 αντίστοιχα την κίνηση του πελάτη B.

Σχήμα 4.3



Έτσι τα TE tunnels είναι ροές δεδομένων μεταξύ μιας συγκεκριμένης πηγής και ενός προορισμού και μπορεί να διακατέχουν ορισμένες ιδιότητες. Οι ιδιότητες αυτές που έχει ένα tunnel, εκτός από τα σημεία εισόδου και εξόδου του δικτύου, μπορεί να περιλαμβάνουν απαιτήσεις εύρους ζώνης και COS για τα δεδομένα που θα προωθηθούν. Η κίνηση προωθείται μέσω της διαδρομής που καθορίζεται ως TE tunnel, με τη χρήση του MPLS. Ως εκ τούτου για τα TE tunnels ορίζονται συγκεκριμένα LSPs στο δίκτυο από την πηγή στον προορισμό, τα οποία είναι συνήθως συνδεδεμένα στα PE routers. Τα MPLS LSPs έχουν μια προς μία συσχέτιση με τα TE tunnels, και τα TE tunnels δεν είναι συνδεδεμένα με μια συγκεκριμένη διαδρομή μέσω του SP δικτύου προς ένα PE router. Αν δεν καθοριστούν ρητά (explicitly), τα TE tunnels μπορούν να επαναδρομολογήσουν πακέτα μέσω οποιασδήποτε διαδρομής στο δίκτυο συσχετισμένης με ένα MPLS LSP. Αυτό το μονοπάτι μπορεί να καθοριστεί από το IGP που χρησιμοποιείται στον πυρήνα. Ο κύριος λόγος εφαρμογής του MPLS TE είναι να ελέγχονται τα μονοπάτια από τα οποία διακινείται η κίνηση μέσα στο δίκτυο .Το MPLS TE παραχωρεί μία ελαστική σχεδίαση στην οποία μια εναλλακτική πορεία μπορεί να χρησιμοποιηθεί όταν αποτυγχάνει η βασική πορεία μεταξύ δύο δρομολογητών σε ένα δίκτυο. Σε ένα πακέτο που φτάνει σε έναν PE δρομολογητή από έναν CE του εφαρμόζονται labels και προωθείται στους PE δρομολογητές εξόδου. Εκεί

γίνεται αφαίρεση των labels και προωθείται προς στον κατάλληλο προορισμό ως IP πακέτο πλέον.

Τα πρωτόκολλα OSPF ή IS-IS με TE «προεκτάσεις» χρησιμοποιούνται για να μεταφέρουν πληροφορίες σχετικά με τα τούνελ που έχουν καθοριστεί σε έναν δρομολογητή. Αυτές οι προεκτάσεις περιέχουν πληροφορίες σχετικά με τους διαθέσιμους πόρους για την δημιουργία ενός τούνελ, όπως το εύρος ζώνης μίας σύνδεσης. Ως αποτέλεσμα, μια σύνδεση που δεν έχει τους απαιτούμενους πόρους δεν επιλέγεται να γίνει μέρος του LSP ή TE τούνελ. Η σηματοδοσία σε ένα MPLS TE περιβάλλον χρησιμοποιεί πρωτόκολλα κατοχύρωσης πόρων (όπως το RSVP) με τις κατάλληλες προεκτάσεις ώστε να υποστηρίζονται τα χαρακτηριστικά των TE τούνελ. Ο δρομολογητής εισόδου στο MPLS δίκτυο χρειάζεται να ξέρει πληροφορίες σχετικά με την διαθεσιμότητα των πόρων για κάθε σύνδεση ικανή να γίνει μέλος του MPLS TE tunnel. Αυτές οι πληροφορίες παρέχονται από τα IGPs όπως το OSPF και το IS-IS λόγω της έμφυτης τους λειτουργίας να πλημμυρίζουν με πληροφορίες σχετικά με τις συνδέσεις όλους τους δρομολογητές του IGP domain.. Έτσι ο δρομολογητής εισόδου συλλέγει πληροφορίες για όλους τους διαθέσιμους πόρους στο δίκτυο καθώς και την τοπολογία , που περιγράφει τα τούνελ μέσα στο δίκτυο μεταξύ των MPLS δρομολογητών.

Η βάση του MPLS TE είναι η δρομολόγηση βάση περιορισμών (*Constraint Based Routing (CBR)*), όπου λαμβάνεται υπόψη η πιθανότητα ύπαρξης πολλαπλών διαδρομών, μεταξύ μιας πηγής και ενός προορισμού σε ένα δίκτυο. Με το CBR, η λειτουργία ενός IP δικτύου ενισχύεται ώστε να δημιουργείται η μικρότερη σε κόστος διαδρομή και να ευνοούνται οι ήδη διαθέσιμες διαδρομές. Το CBR απαιτεί ένα IGP, όπως το OSPF ή το IS-IS, για τη λειτουργία του. Το CBR είναι ο κορμός του TE tunnel και καθορίζεται στον δρομολογητή εισόδου της MPLS περιοχής όταν εφαρμόζουμε MPLS TE. Η διαθεσιμότητα των πόρων και οι πληροφορίες κατάστασης των συνδέσεων μέτριουνται χρησιμοποιώντας τον CSPF υπολογισμό όπου μεταβλητές όπως εύρος ζώνης , πολιτικές και τοπολογία λαμβάνονται υπόψη για να καθοριστούν οι πιθανές διαδρομές από μια πηγή σε έναν προορισμό. Τα αποτελέσματα του CSPF υπολογισμού μαζί με ένα καθορισμένο σύνολο IP διευθύνσεων που υποδεικνύουν την διεύθυνση των δρομολογητών ,του επόμενου άλματος (hop), δημιουργούν ένα LSP. Αυτό το σύνολο των IP καθορίζεται από τον επικεφαλή δρομολογητή και διαδίδεται στους άλλους δρομολογητές από το LSP. Έτσι οι ενδιάμεσοι δρομολογητές δεν εκτελούν την διαδικασία επιλογής μονοπατιού . Το RSVP με TE προεκτάσεις χρησιμοποιείται για να κατοχυρώσει πόρους στο LSP και να αντιστοιχίσει label στο TE τούνελ.

Η λειτουργία του RSVP για το MPLS TE παρουσιάζεται παρακάτω

4.3 RSVP

4.3.1 RSVP με TE προεκτάσεις

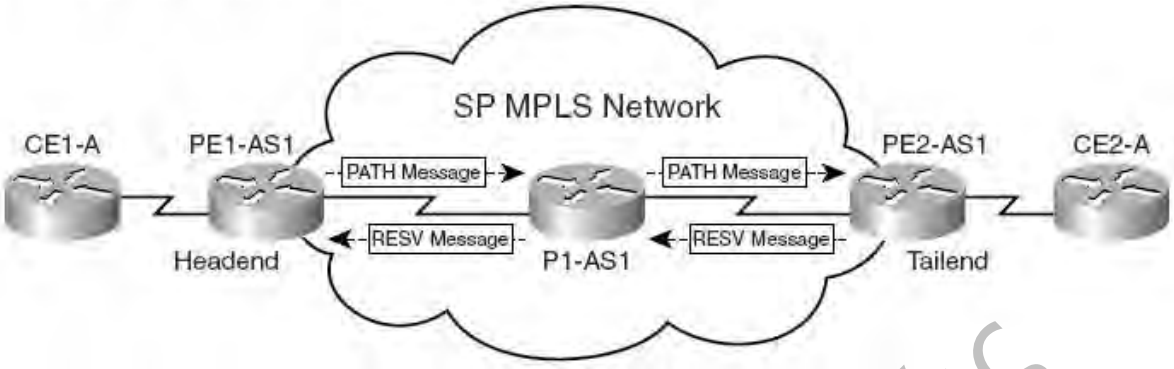
Το RSVP καταλαμβάνει κάποιο εύρος ζώνης πάνω σε ένα κανάλι απο μια πηγή σε έναν προορισμό. Τα RSVP μηνύματα στέλνονται, από τον δρομολογητή άνω άκρου (επικεφαλής), στο δίκτυο για να προσδιορίσουν την διαθεσιμότητα των πόρων πάνω στην διαδρομή πηγής - προορισμού. Ο επικεφαλής δρομολογητής είναι πάντα η πηγή στο MPLS TE tunnel , και ο ακραίος δρομολογητής είναι αυτός που λειτουργεί ως σημείο τερματισμού. Αφού σταλούν τα RSVP μηνύματα , οι πληροφορίες κατάστασης των δρομολογητών (διαθεσιμότητα πόρων) αποθηκεύονται στα μηνύματα πορείας (path messages) καθώς διαπερνούν το δίκτυο. Έτσι το RSVP ενημερώνει το δίκτυο για τις απαιτήσεις μιας συγκεκριμένης ροής κίνησης και συλλέγει πληροφορίες για το πότε οι απαιτήσεις αυτές μπορεί να εκπληρωθούν από το δίκτυο.
Τα 4 κύρια μηνύματα που χρησιμοποιούνται στην εφαρμογή του RSVP είναι Τα εξής :

- RSVP PATH message (μηνύματα πορείας)
- RSVP RESERVATION message (μηνύματα κράτησης)
- RSVP error messages (μηνύματα σφάλματος)
- RSVP tear messages.

Στο MPLS TE, το RSVP χρησιμοποιείται για να εξασφαλίσει και να ελέγξει την διαθεσιμότητα πόρων , όπως επίσης και να εφαρμόσει τα MPLS labels ώστε να ορίσει το MPLS TE LSP ανάμεσα στους δρομολογητές στο δίκτυο:

• **RSVP PATH message**— δημιουργείται από τον επικεφαλή δσρομολογητή και προωθείται μέσω του δικτύου πάνω από την διαδρομή του μελλοντικού TE LSP. Σε κάθε άλμα (hop) , το message ελέγχει την διαθεσιμότητα των απαιτούμενων πόρων και αποθηκεύει αυτές τις πληροφορίες.
Στο δίκτυο του παραδείγματος μας (σχέδιο 4.4), το PATH message δημιουργείται από τον δρομολογητή PE1-AS1(επικεφαλής) , και προωθείται προς τα κάτω όπου ελέγχεται η διαθεσιμότητα πόρων σε κάθε hop (P1-AS1 και PE2-AS1).Το RSVP PATH message λειτουργεί ως αίτημα label στην MPLS TE περιοχή.

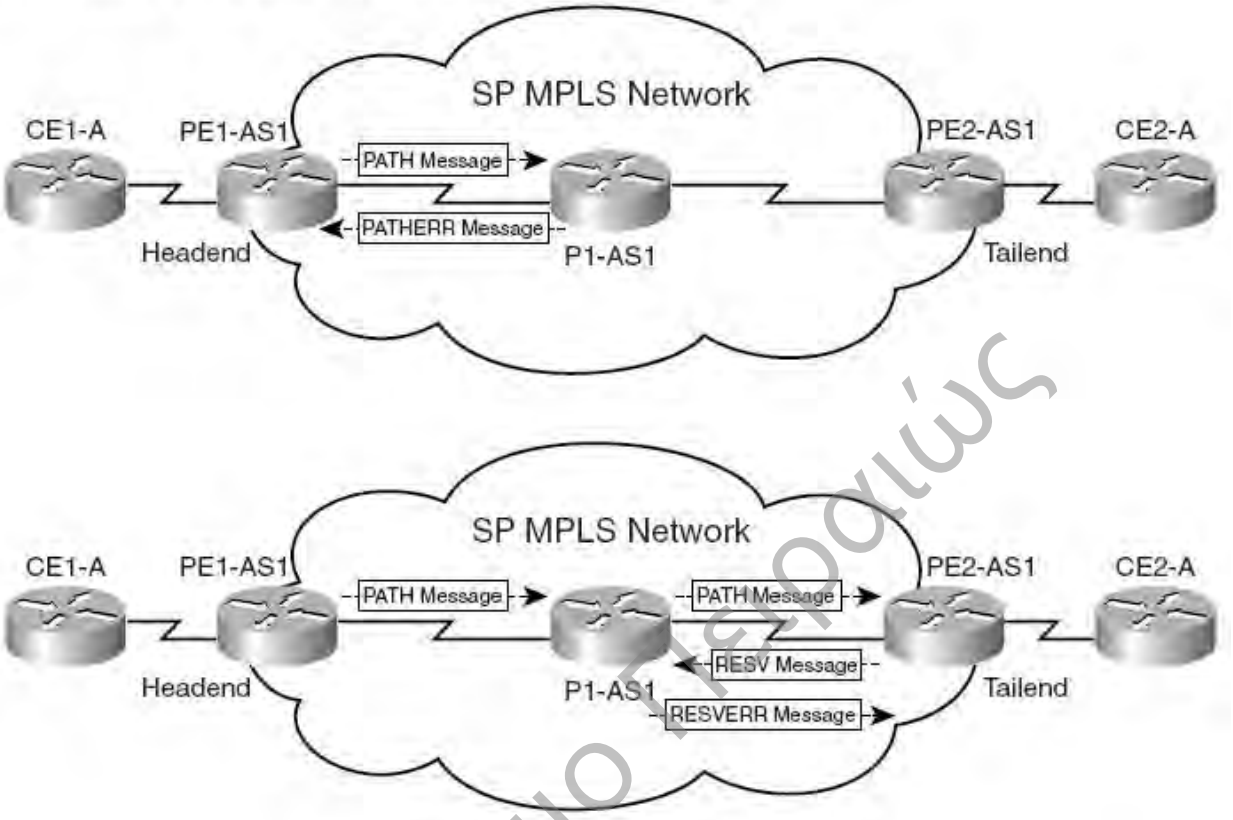
ΣΧΕΔΙΟ 4 *RSVP PATH and RESERVATION Messages*



• **RSVP RESERVATION message**—Δημιουργείται από τον ακραίο router στην MPLS TE περιοχή και χρησιμοποιείται για να επιβεβαιώσει την κατοχύρωση των απαιτήσεων που είχαν αποσταλεί νωρίτερα με τα PATH messages. Στο δίκτυο που απεικονίζεται στο σχέδιο 4.4 ο PE2-AS1 θα δημιουργήσει το RSVP RESERVATION μήνυμα σε απάντηση του PATH message. Έτσι τα PATH messages λειτουργούν σαν αιτήσεις κατοχύρωσης και τα RESERVATION messages λειτουργούν σαν επιβεβαίωση της κατοχύρωσης για την διαθεσιμότητα των απαιτούμενων πόρων. Το RSVP RESERVATION message εκτελεί την λειτουργία της ανάθεσης των label για την χαρτογράφηση ενός συγκεκριμένου LSP στο TE tunnel. Καθώς η κατανομή των label γίνεται με την downstream-on-demand μέθοδο, η αντιστοιχία τους σε ένα TE LSP πρώτα πραγματοποιείται από τον ακραίο LSR και στην συνέχεια μεταδίδονται προς τα πάνω . Αυτή η διαδικασία επαναλαμβάνεται σε κάθε άλμα (hop) όπου εφαρμόζεται τοπική αντιστοίχηση label σε ένα TE tunnel και μεταδίδεται προς τα πάνω μέχρι να φτάσουμε στον επικεφαλή δρομολογητή.

• **RSVP error messages**—Στην περίπτωση την ανεπάρκειας των ζητούμενων πόρων, ο δρομολογητής παράγει RSVP error μηνύματα και τα στέλνει στον router απ' οπου έγιναν οι αιτήσεις. Στο σχέδιο 4.5 αν ο Router P1-AS1 δεν μπορεί να διαθέσει τους ζητούμενους πόρους όπως καθορίζονται από το PATH message του PE1-AS1 (επικεφαλής router), τότε παράγει ένα PATH ERROR μήνυμα και το στέλνει προς τα πάνω στον LSR PE1-AS1.

ΣΧΕΔΙΟ 5 *RSVP PATH Error and RESERVATION Error Messages*



Αν το RSVP PATH μήνυμα φτάσει επιτυχώς στον ακραίο (tailend) router, αυτός με τη σειρά του (ο PE2-AS1) παράγει ένα RESERVATION μήνυμα. Αν ο P1-AS1 επιβεβαιώσει έλλειψη πόρων ,ανάμεσα στο διάστημα της στιγμής που λαμβάνει ο το PATH message από τον PE1-AS1 και της στιγμής που λάβει το RESERVATION message από τον PE2-AS1, τότε θα στείλει ένα RESERVATION ERROR (RESVERR) μήνυμα στον LSR PE2-AS1 για άρνηση της κράτησης (reservation)
Σχέδιο 4.5

• **RSVP tear messages**—Το RSVP δημιουργεί 2 είδη τέτοιων μηνυμάτων ονομαζόμενα, **PATH tear message** και **RESERVATION tear message**. Τα μηνύματα αυτά καθαρίζουν τις καταστάσεις PATH ή RESERVATION αντίστοιχα. Η λειτουργία καθαρισμού αυτών των καταστάσεων χρησιμοποιώντας τα tear μηνύματα ενεργοποιεί την δυνατότητα επαναχρησιμοποίησης των πόρων στον δρομολογητή για επόμενες απαιτήσεις.

4.3.2 Η Λειτουργία του RSVP στο MPLS TE

Όπως προαναφέρθηκε το αποτέλεσμα ενός CSPF ή CBR υπολογισμού στον επικεφαλή δρομολογητή είναι μια λίστα με IP διευθύνσεις που καθορίζουν τα επόμενα άλματα μέσα στο TE tunnel ή LSP. Αυτή η λίστα των δρομολογητών υπολογίζεται και είναι γνωστή μόνο στον επικεφαλή δρομολογητή ο οποίος είναι η πηγή του TE tunnel. Οι υπόλοιποι δρομολογητές στην ομάδα (domain) δεν εκτελούν υπολογισμούς CBR. Ο επικεφαλής δρομολογητής παρέχει πληροφορίες στους άλλους δρομολογητές στο TE tunnel μέσω της RSVP σηματοδοσίας για να ζητήσει και να επιβεβαιώσει την διαθεσιμότητα πόρων για την εγκαθίδρυση ενός tunnel.

Το RSVP με προεκτάσεις TE καταλαμβάνει τους απαραίτητους πόρους σε κάθε LSR στη διαδρομή που καθορίζεται απο τον επικεφαλή router και ορίζει labels στο TE tunnel LSP.

Οι επεκτάσεις του RSVP για ενεργοποίηση σε περιβάλλον MPLS παρουσιάζονται στον παρακάτω πίνακα (πίνακας 4.1) μαζί με τις λειτουργίες τους.

Object	**Message**	**Λειτουργία**
LABEL_REQUEST	PATH	**Χρησιμοποιείται για να ζητηθεί χαρτογράφηση label στο TE tunnel ή LSP; Δημιουργείται απο τον επικεφαλή δρομολογητή στο PATH message.**
LABEL	RESERVATION	**Χρησιμοποιείται για να διαθέσει τα Labels στο TE tunnel ή LSP: Δημιουργούνται απο τον ακριανό δρομολογητή (tailend router) στο RESERVATION message και διαδίδεται προς τα πάνω (upstream).**
EXPLICIT_ROUTE	PATH	**Μεταφέρεται μεσα στα PATH messages και χρησιμοποιείται είτε για αίτηση ή για επιβεβαίωση μιας συγκεκριμένης διαδρομής του tunnel.**
RECORD_ROUTE	PATH, RESERVATION	**Προστίθεται στο PATH ή RESERVATION message για να δηλώσει το δημιουργημένο κόμβο για την πραγματική διαδρομή την οποία χρησιμοποιεί το LSP TE tunnel .**
SESSION_ATTRIBUTE	PATH	**Χρησιμοποιείται για να καθορίσει συγκεκριμένες παραμετους συνόδου τοπικά στο TE LSP tunnel.**

Πίνακας 4.1

Κατά τη διάρκεια εγκατάστασης διαδρομής για τα LSP TE tunnels, Τα RSVP μηνύματα περιλαμβάνουν μία ή περισσότερες αυτών των προεκτάσεων για να καθορίσουν τη σημασία του κάθε τύπου μηνύματος και του περιεχόμενου του.

Το path message περιλαμβάνει τις πληροφορίες που αναφέρονται στον κάτωθι πίνακα (πίνακας 4.2).

Object	**Message**
SESSION	**Καθορίζει την πηγή και προορισμό του LSP tunnel. Συνήθως καθορίζεται απο τις IP διευθύνσεις των αντίστοιχων interfaces του επικεφαλή και των ακραίοων δρομολογητών**
SESSION_ATTRIBUTE	**Καθορίζει τα χαρακτηριστικά του συγκεκριμένου LSP tunnel, όπως τις απαιτήσεις εύρους ζώνης και πόρων οι οποίες χρειάζονται να διατεθούν για το tunnel.**
EXPLICIT_ROUTE	**Γνωστοποιείται με την λίστα επόμενων hops που καθορίζεται είτε προσωπικά η υπολογίζεται χρησιμοποιώντας constraint-based SPF. Το προηγούμενο hop ορίζεται στο interface (ip) εξόδου του router. Το Record_Route (RRO) ορίζεται επίσης στην ίδια διεύθυνση.**
RECORD_ROUTE	**Δημιουργείται στο interface εξόδου στη διαδρομή του LSP tunnel.**
SENDER_TEMPLATE	**Σε αντίθεση με τις αναφερθείσες ιδιότητες, το αντικείμενο sender template στο the path message απεικονίζει τη διεύθυνση του interface που θα χρησιμοποιηθεί σαν LSP-ID για το tunnel. Αυτή η τιμή καθορίζεται απο τον επικεφαλή router**

Πίνακας 4.2

Παράδειγμα

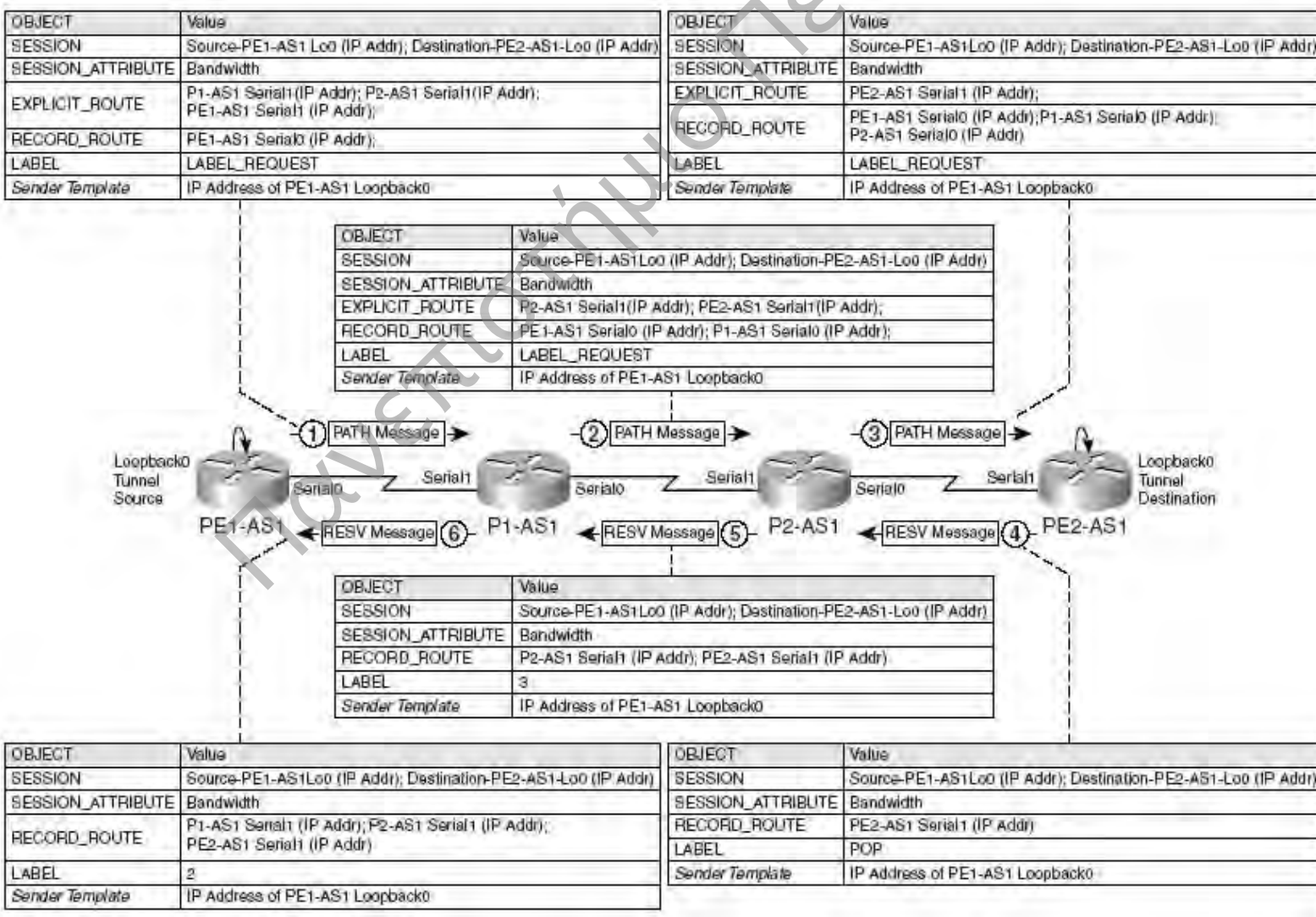
Θα παρουσιαστούν τα βήματα διάδοσης των PATH και RESV μηνυμάτων σε συνδυασμό με το σχέδιο 4.6 που ακολουθεί

Βήμα 1 Οι κατάλληλες τιμές για τα πεδία που ορίζονται στον πίνακα 4.1 εφαρμόζονται από τον επικεφαλή δρομολογητή (PE1-AS1) και το PATH message στέλνεται στο επόμενο άλμα (next-hop router) της LSP tunnel διαδρομής.

Βήμα 2 Όταν ο P1-AS1 παραλάβει αυτό το PATH message, ο δρομολογητής ελέγχει το αντικείμενο EXPLICIT_ROUTE για να δει αν το επόμενο άλμα είναι απευθείας συνδεδεμένο. Αυτό ελέγχεται στο *L-bit* του RSVP path message. Αν

τοL-bit έχει οριστεί, ο τοπικός δρομολογητής (local router) δεν είναι απευθείας συνδεδεμένος με το επόμενο hop στην LSP tunnel διαδρομή. Σε αυτή την περίπτωση ο δρομολογητής θα εκτελέσει ένα CSPF (βάση περιορισμών) υπολογισμό για να ορίσει το επόμενο άλμα στο Tunnel.Αν το L-bit είναι κενό ο δρομολογητής P1-AS1 γνωρίζει ότι είναι απευθείας συνδεδεμένος με το επόμενο άλμα της LSP tunnel διαδρομής. Έπειτα αναιρεί όλες τις εγγραφές του EXPLICIT_ROUTE που σχετίζονται με τον P1-AS1 και προωθεί το PATH message στο επόμενο άλμα όπως καθορίζεται από το EXPLICIT_ROUTE object. Επιπλέον ο P2-AS1 ενημερώνει το RECORD_ROUTE object για να παρουσιάσει το τοπικό Interface εξόδου στη διαδρομή του LSP tunnel. Στο σχέδιο 4.6 παρουσιάζονται οι τιμές του PATH message καθώς αυτό προωθείται από το P1-AS1 στο P2-AS1 αφού οι κατάλληλες τιμές ενημερωθούν. Όπως προαναφέρθηκε, ο P1-AS1 αφαιρεί τις αναφορές στο τοπικό του interface στο EXPLICIT_ROUTE.object και προσθέτει το εξωτερικό interface στο RECORD_ROUTE object.

Σχήμα 4.6



Βήμα 3 Η διαδικασία επαναλαμβάνεται στον P2-AS1 του οποίου οι αναφορές στο τοπικό του interface στο EXPLICIT_ROUTE object αφαιρέθηκαν και επισυνάπτηκε το interface εξόδου στο RECORD_ROUTE object.

Βήμα 4 Αφού το RSVP PATH message παραληφθεί από τον ακραίο Router PE2-AS1, ωθείται η δημιουργία ενός RESERVATION message. Η βασική έννοια είναι η διαδικασία κατανομής των ετικετών να ξεκινάει στον ακραίο δρομολογητή επάνω στην παραγωγή του RESERVATION message . Έτσι, όταν ο PE2-AS1 δημιουργεί ένα RESERVATION message, ο δρομολογητής ορίζει ένα POP label στο LSP tunnel.
Το RESERVATION μήνυμα έχει τώρα το RECORD_ROUTE object να δείχνει τα interface εξόδου από τον ακραίο μέχρι και τον επικεφαλή δρομολογητή.
Τέλος το RECORD_ROUTE object ξαναξεκινάει στο RESERVATION message. Οι τιμές εμφανίζονται στο σχέδιο 4.6.

Βήμα 5 Όταν το reservation message φτάσει στον P2-AS1,το RECORD_ROUTE είναι ενημερωμένο με το interface εξόδου και η τοπική χαρτογράφηση label στο LSP, έχει επίσης δημιουργηθεί και ενημερώσει το LABEL object. Μία αυθαίρετη τιμή 3 για το πεδίο value LABEL (σχέδιο 4.6).

Βήμα 6 Αυτή η διαδικασία επαναλαμβάνεται στον P1-AS1 και το RESERVATIONmessage παραλαμβάνεται από τον PE1-AS1.

Βήμα 7 Όταν ο PE1-AS1 παραλάβει το RESERVATION message, το RECORD_ROUTE καθορίζει το LSP, στο οποίο έχει εφαρμοστεί traffic engineering, και συνδέεται με μια συγκεκριμένη απαίτηση εύρους ζώνης και πόρων στο SESSION object.

Στην εφαρμογή του RSVP για MPLS TE, το RSVP ζητά όσο και επιβεβαιώνει το LSP, διατηρεί τους πόρους όπως ζητούνται σε όλους τους δρομολογητές της LSP διαδρομής και εφαρμόζει τα MPLS labels για να διαμορφώσει το MPLS LSP μέσα στο δίκτυο. Να σημειωθεί ότι οι δρομολογητές αποθηκεύουν ένα αντίγραφο της PATH αίτησης καθώς αυτή προωθείται στο επόμενο (next-hop) LSR.Αυτή η πληροφορία καθορίζει την διεπαφή καθώς τα reservation messages λαμβάνονται στο ίδιο LSR στο interface εξόδου του επικεφαλή δρομολογητή.

Στην επόμενη παράγραφο θα γίνει περιγραφή της λειτουργίας υπολογισμού του SPF βάση περιορισμών και η ανάγκη χρήσης ενός πρωτοκόλλου κατάστασης-σύνδεσης για την δυναμική ενεργοποίηση του MPLS TE στο κεντρικό δίκτυο ενός φορέα παροχής υπηρεσιών.

4.4 Δρομολόγηση βάση περιορισμών και η εφαρμογή του στο MPLS TE

Η σημαντικότερη απαίτηση του TE είναι τα χαρακτηριστικά των συνδέσεων του δικτύου, όπως και η διαθεσιμότητα των πόρων, να αναπαράγονται μέσα στο δίκτυο ώστε να γίνεται ικανοποιητική επιλογή μεταξύ των TE LSP διαδρομών. Στα πρωτόκολλα δρομολόγησης κατάστασης δικτύου (link-state), η επιλεγμένη διαδρομή συνεχίζει τα λαμβάνει υπ' όψη το εύρος ζώνης μεταξύ δύο δρομολογητών ώστε να υπολογίσει το κόστος που σχετίζεται με αυτή πριν από την κατανομή των επιλεγμένων διαδρομών. Ενεργοποιώντας τη χρήση των link-sate πρωτοκόλλων για να διασωθούν αποτελεσματικά οι πληροφορίες που σχετίζονται με την διαθεσιμότητα των πόρων, οι ανανεώσεις των διαδρομών εκτελούνται από πρόσθετες προεκτάσεις της βασικής λειτουργίας του πρωτοκόλλου κατάστασης σύνδεσης.

Οι μηχανισμοί λειτουργίας ενός link-state πρωτοκόλλου περιλαμβάνουν την διαρκή μετάδοση ανανεώσεων στο δίκτυο σχετικά με την κατάσταση σύνδεσης ή των μετρικών αλλαγών ή ορθότερα της διαθεσιμότητας εύρους ζώνης μιας TE προοπτικής.

Οι δρομολογητές πλημμυρίζουν τις ιδιότητες των πόρων στο δίκτυο ώστε να τους κάνουν διαθέσιμους στον επικεφαλή router του TE tunnel κατά την διάρκεια υπολογισμού της LSP διαδρομής (δυναμικά tunnels).Οι ανακοινώσεις κατάστασης σύνδεσης μεταφέρουν πληροφορίες που εμπεριέχουν τους ¨γειτονικούς δρομολογητές¨, τα άμεσα συνδεδεμένα δίκτυα, πληροφορίες σχετικά με τους πόρους του δικτύου και άλλες σχετικές πληροφορίες αναφορικά με την πραγματική διαθεσιμότητα πόρων που μπορεί αργότερα να ζητηθεί ώστε να γίνει ένας constraint-based SPF υπολογισμός.

Τα OSPF και IS-IS παρέχονται με προεκτάσεις ώστε να ενεργοποιείται η χρήση τους σε ένα MPLS TE περιβάλλον για να αναπαράγουν πληροφορίες που αφορούν τη διαθεσιμότητα πόρων και την δυναμική επιλογή LSP διαδρομής.

4.5 Μέγιστο και Διαθέσιμο Εύρος Ζώνης

Το Διαθέσιμο Εύρος(AB) είναι μια τιμή κλειδί που λαμβάνεται υπ' όψη κατά την διαδικασία υπολογισμού της LSP διαδρομής όπου ορίζεται η καλύτερη διαδρομή για το TE tunnel.Το διαθέσιμο εύρος ζώνης σε κάθε interface ρυθμίζεται βάση προτεραιοτήτων. Ο αριθμός της προτεραιότητας σε συνδυασμό με το διαθέσιμο εύρος ζώνης μπορεί να κυμαίνεται από 0 μέχρι 7, όπου το 0 εκπροσωπεί την υψηλότερη προτεραιότητα. Όταν οριστεί το διαθέσιμο εύρος για την τιμή μιας προτεραιότητας σε ένα interface, αφαιρείται από το ολικό διαθέσιμο εύρος για κάθε interface με χαμηλότερο επίπεδο προτεραιότητας.

Αν ο δρομολογητής PE1-AS1 έχει ένα σειριακό interface (T1-1.544 Mbps), ένα Ethernet interface (10 Mbps) και ένα Fast Ethernet interface (100 Mbps), τα πραγματικά bandwidths που αντιστοιχούν ανά interface εξαρτώνται από το μέγιστο bandwidth (MB) που διατίθεται από τις αντίστοιχες συνδέσεις (γραμμές).Το διαθέσιμο bandwidth είναι συνήθως το εύρος ζώνης της απαιτούμενης κράτησης αφαιρούμενο από το μέγιστο bandwidth. Παρόλα αυτά κάτι τέτοιο δεν ισχύει αν το διαθέσιμο εύρος ορίζεται μεγαλύτερο από το μέγιστο εύρος της γραμμής. Αν και το διαθέσιμο εύρος μπορεί να οριστεί υψηλότερο από το μέγιστη τιμή , οι κρατήσεις αυτές απορρίπτονται.

Όταν ο Router PE1-AS1 αρχικά μεταδίδει τις πληροφορίες σχετικά με το μέγιστο και το διαθέσιμο bandwidth σε όλες του τις γραμμές ,οι τιμή για το διαθέσιμο bandwidth σε κάθε επίπεδο προτεραιότητας για κάθε γραμμή θα είναι ίση με την τιμή του μέγιστου εύρους ζώνης (1.544 Mbps για το serial, 10 Mbps για Ethernet και 100 Mbps για το Fast Ethernet).
Όταν μία αίτηση tunnel γίνει αποδεκτή και το ανάλογο εύρος αφαιρεθεί από το διαθέσιμο bandwidth με μία δεδομένη προτεραιότητα ,τότε επίσης αφαιρείται και από όλες τις προτεραιότητες που είναι χαμηλότερες από αυτή που έκανε την αίτηση.

Αν η δημιουργία ενός LSP tunnel στον PE1-AS1 καταναλώνει 40 Mbps του εύρους ζώνης στο Fast Ethernet interface με μία προτεραιότητα επιπέδου 5, θα άλλαξει η διαθέσιμη τιμή εύρους ζώνης για τις προτεραιότητες με τιμή ίση ή χαμηλότερη του 5 στο Fast Ethernet interface από 100 σε 60 Mbps (100 – 40 = 60 Mbps).

Έστω ότι έχουμε την παρακάτω σειρά αιτήσεων:

1 Αίτηση για 10 Mbps bandwidth στο Ethernet interface με προτεραιότητα 1
2 Αίτηση για 20 Mbps bandwidth στο Fast Ethernet interface με προτεραιότητα 0
3 Αίτηση για 1 Mbps bandwidth στο serial interface με προτεραιότητα 0
4 Αίτηση για 2 Mbps bandwidth στο Ethernet interface με προτεραιότητα 3

Αυτή η σειρά θα μειώσει τις τιμές του διαθέσιμου εύρους όπως φαίνεται στον πίνακα 4.3

Interface	AB P = 0 (Mbps)	AB P = 1 (Mbps)	AB P = 2 (Mbps)	AB P = 3 (Mbps)	AB P = 4 (Mbps)	AB P = 5 (Mbps)	AB P = 6 (Mbps)	AB P = 7 (Mbps)
Serial	1.544 – 1 = .544	1.544 – 1 = .544	1.544 – 1 = .544	1.544 – 1 = .544	1.544 – 1 = .544	1.544 – 1 = .544	1.544 – 1 = .544	1.544 – 1 = .544
Ethernet	10	10 – 10 = 0	10 – 10 = 0	10 – 10 = 0	10 – 10 = 0	10 – 10 = 0	10 – 10 = 0	10 – 10 = 0
Fast Ethernet	100 – 20 = 80	100 – 20 = 80	100 – 20 = 80	100 – 20 = 80	100 – 20 = 80	60 – 20 = 40	60 – 20 = 40	60 – 20 = 40

Πίνακας 4.3: Μέγιστο και Διαθέσιμο εύρος ζώνης

Στα στοιχεία του πίνακα 4.3 δεν παρουσιάζεται το αίτημα για 2 Mbps bandwidth στο Ethernet interface με priority 3. Αυτό το αίτημα απορρίπτεται εξαιτίας της μη διαθεσιμότητας bandwidth για αυτό το επίπεδο προτεραιότητας την συγκεκριμένη στιγμή. Οι ενημερώσεις κατάστασης-γραμμής σχετικά με την διαθεσιμότητα των πόρων, πλημμυρίζουν το δίκτυο όταν η κατάσταση του καναλιού αλλάζει είτε λόγω χειροκίνητων αλλαγών των παραμέτρων(που σχετίζονται με την διαθεσιμότητα πόρων),είτε λόγω περιοδικών ανανεώσεων των συνδέσεων και της κατάστασης τους ή λόγω αποτυχίας εγκαθίδρυσης της LSP διαδρομής λόγω έλλειψης πόρων.

Αν οι πόροι που σχετίζονται με την γραμμή αλλάζουν συνεχώς αυτό θα ενεργοποιήσει την διαρκή παραγωγή μηνυμάτων ενημέρωσης , κατάσταση η οποία πρέπει να αποφευχθεί. Σ' αυτή την περίπτωση ο επικεφαλής δρομολογητής μπορεί να δει τη γραμμή ως μια πιθανή LSP διαδρομή. Έτσι αυτή η πιθανώς μη ανανεωμένη σύνδεση μπορεί να χρησιμοποιηθεί στον υπολογισμό διαδρομής ακόμα και αν αυτή δεν διαθέτει τους πόρους που απαιτούνται για την εγκαθίδρυση της LSP διαδρομής.

Έτσι μετά τον υπολογισμό LSP διαδρομής όταν επιχειρείται η εγκατάσταση της , ο δρομολογητής που διαχειρίζεται την σύνδεση με τους μη διαθέσιμους πόρους παράγει μία ενημέρωση με πληροφορίες επιβεβαιώνοντας την έλλειψη.

Οι γεννήτριες μηνυμάτων ανανέωσης μπορεί να εγκατασταθούν είτε βάση interface ή βάση γραμμής σε ένα router όπου εκεί δημιουργούνται με ένα προκαθορισμένο εύρος διαθεσιμότητας πόρων. Έτσι το ανώτερο όριο ,όπως και το κατώτερο, όταν πραγματοποιείται μια ανανέωση , μπορεί να προκαθοριστεί.

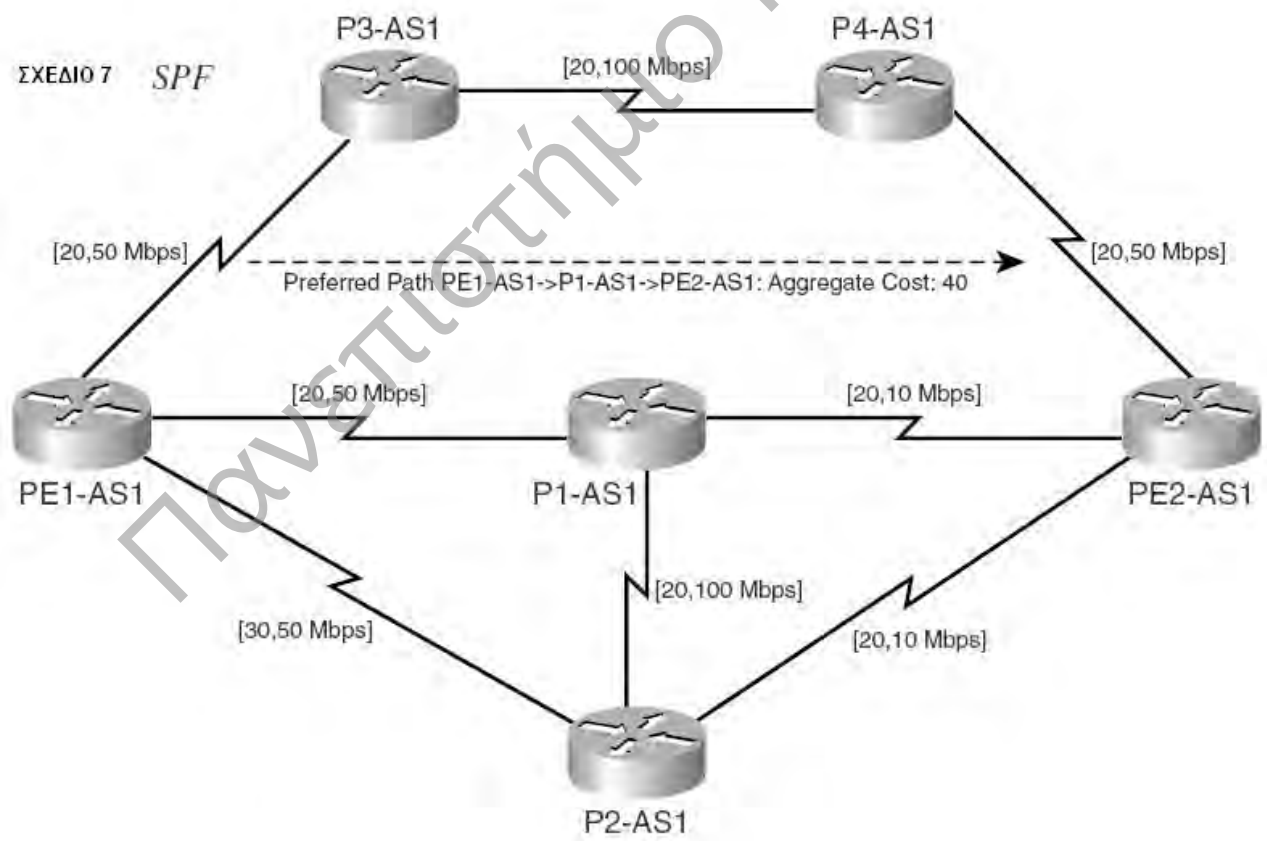
Για παράδειγμα αν το κατώτερο όριο οριστεί να είναι στο 50% του εύρους σύνδεσης με βήμα 60, 70, 80, και 90 με μέγιστο όριο ορισμένο στο 100%, οι ανανεώσεις που αφορούν την διαθεσιμότητα εύρους σύνδεσης, παράγονται και πλημμυρίζουν το δίκτυο όταν το 50%, 60%, 70%, 80%, 90%, και 100% του bandwidth επιτευχθεί.

4.6 Constraint-Based (βάση περιορισμών) SPF

Στην κανονική διαδικασία του SPF υπολογισμού, ένας δρομολογητής τοποθετείται στην κορυφή του δέντρου και οι ελάχιστες διαδρομές (shortest paths) υπολογίζονται σε κάθε προορισμό, λαμβάνοντας υπόψη μόνο τη μικρότερη τιμή κόστους της διαδρομής προς τον προορισμό.
Κατά την διάρκεια της απλής SPF λειτουργίας στο δίκτυο ,όπως φαίνεται και στο σχέδιο 4.7, μόνο το κόστος λαμβάνεται υπόψη στους υπολογισμούς της διαδρομής , όπου στο παράδειγμα μας για την απόσταση PE1-AS1 --- PE2-AS1 είναι η
PE1-AS1→P1-AS1→PE2-AS1. Σ' αυτόν τον υπολογισμό η βασική λογική είναι ότι δεν λαμβάνεται υπόψη το εύρος ζώνης των συνδέσεων των άλλων πιθανών διαδρομών, συγκεκριμένα των
PE1-AS1→P3-AS1→P4-AS1→PE2-AS1 και PE1-AS1→P2-AS1→ PE2-AS1

Στο παρακάτω σχέδιο αναφέρεται το κόστος και το εύρος ζώνης ανά γραμμή.

Σχέδιο 4.7

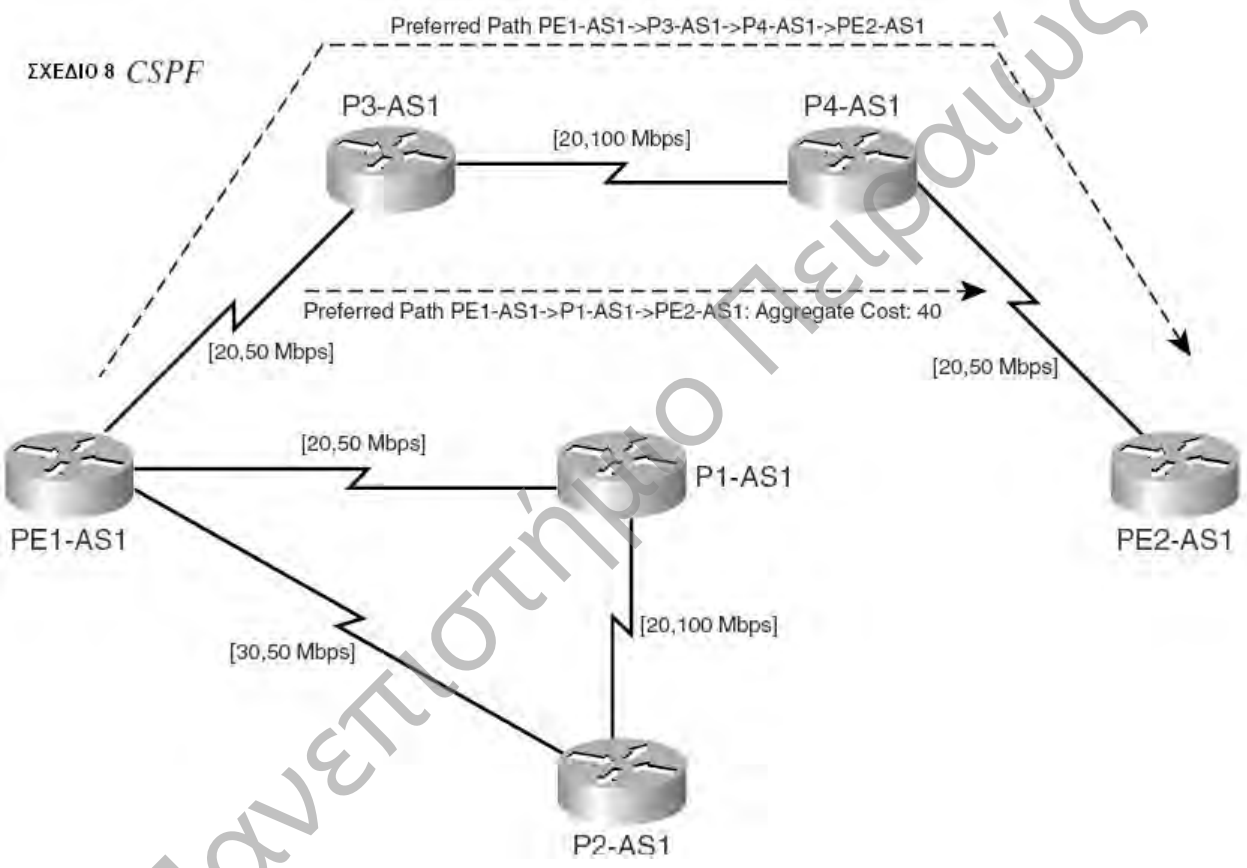


Αν δεν είναι μοναδική παράμετρος το ελάχιστο κόστος ,στην επιλογή διαδρομής, αλλά τεθεί επίσης ως επιπλέον παράμετρος να υποστηρίζεται εύρος ζώνης 50 Mbps στο δίκτυο του σχεδίου 4.7, μπορούμε να ελαχιστοποιήσουμε τις δυνατές

συνδέσεις . Έτσι το δίκτυο του παραδείγματος, που θα μπορούσε να υποστηρίξει αυτές τις απαιτήσεις, διαμορφώνεται ως εξής (σχέδιο 4.8)

Βάση λοιπόν των περιορισμών ,η μόνη ικανή διαδρομή που είναι ικανή να χρησιμοποιηθεί για ένα LSP με TE είναι PE1-AS1→ P3-AS1→ P4-AS1→ PE2-AS1. Αν οποιαδήποτε άλλη σύνδεση θα μπορούσε να υποστηρίξει εύρος ζώνης ανώτερο του προαπαιτούμενου θα μπορούσε να γίνει μέρος της CSPF δενδροειδής δομής .

Σχέδιο 4.8



Με το CSPF, χρησιμοποιούμε περισσότερους παράγοντες (εκτός του κόστους) για να καθορίσουμε τις πιθανές διαδρομές που μπορεί μα χρησιμοποιηθούν για το TE LSP. Η απόφαση ,για το ποια διαδρομή θα χρησιμοποιηθεί, λαμβάνεται στον επικεφαλή δρομολογητή αφού πρώτα «απορριφθούν» οι συνδέσεις οι οποίες δεν διαθέτουν συγκεκριμένα κριτήρια, όπως απαιτήσεις εύρους ζώνης και κόστος γραμμής.

Το αποτέλεσμα του CSPF υπολογισμού είναι ένα σύνολο IP διευθύνσεων που αντιστοιχούν στους next-hop δρομολογητές και συνθέτουν το TE LSP. Έτσι πολλαπλά TE LSPs θα μπορούσαν να χρησιμοποιηθούν στον υπολογισμό CSPF ώστε να καθοριστούν οι πιθανές συνδέσεις στο δίκτυο που ικανοποιούν τα κριτήρια. Επιπλέον ο διαχειριστής μπορεί να καθορίσει ένα στατικό TE tunnel ή

LSP ,τον επικεφαλή δρομολογητή, που θα υποδεικνύει τα επόμενα hops στην TE LSP διαδρομή όπου θα χρησιμοποιείται ως εναλλακτικό LSP στην περίπτωση όπου το κύριο TE LSP αποτύχει.

Έπειτα το αποτέλεσμα του CSPF υπολογισμού μεταδίδεται στην RSVP λειτουργία ώστε να ξεκινήσει το RSVP αίτημα και η διαδικασία κράτησης όπως περιγράφεται στην προηγούμενη ενότητα. Έτσι το RSVP χρησιμοποιείται σε συνδυασμό με το αποτέλεσμα του υπολογισμού CSPF or η των προκαθορισμένων ρυθμίσεων του διαχειριστή. Το TE LSP που δημιουργείται από αυτή την διαδικασία είναι μονής κατεύθυνσης στην πραγματικότητα.

Το CSPF κατά την διάρκεια των υπολογισμών μπορεί να χρησιμοποιήσει παράγοντες που ορίζει είτε ο διαχειριστής ή να λάβει υπόψη το IGP metric (γνωστό και ως TE metric). Για την σύγκριση των διαδρομών αυτή με το μεγαλύτερο εύρος ζώνης παίρνει προβάδισμα και σε συνδυασμό με τον αριθμό των hops γίνεται η επιλογή. Αν υπάρχει ισοβαθμία το CSPF επιλέγει τυχαία μια διαδρομή η οποία παραμένει και ως προεπιλογή.

Έτσι η σειρά των βημάτων στην δημιουργία ενός MPLS TE tunnel LSP στο δίκτυο είναι η εξής:

Βήμα 1 Πραγματοποιείται ο CSPF υπολογισμός από τον επικεφαλή δρομολογητή βάση των περιορισμών που καθορίζονται από τον προσδιορισμό και τις απαιτήσεις του tunnel.Αυτός ο υπολογισμός γίνεται από το IGP με τη χρήση είτε του OSPF ή του IS-IS πρωτοκόλλου.

Βήμα 2 Μετα τον υπολογισμό της LSP διαδρομής το αποτέλεσμα της CSPF διαδικασίας ,που είναι το σύνολο των IP διευθύνσεων που αντιστοιχούν στα επόμενα hop,προωθούνται στο RSVP.

Βήμα 3 Το RSVP με τη σειρά του πραγματοποιεί τις αιτήσεις κατοχύρωσης και επιβεβαίωσης των πόρων στο LSP όπως ορίζεται από την CSPF διαδικασία , για να προσδιορίσει αν το LSP εκπληρώνει τις απαιτήσεις συγκεκριμένων πόρων που ζητούνται κατά τον καθορισμό ενός tunnel.

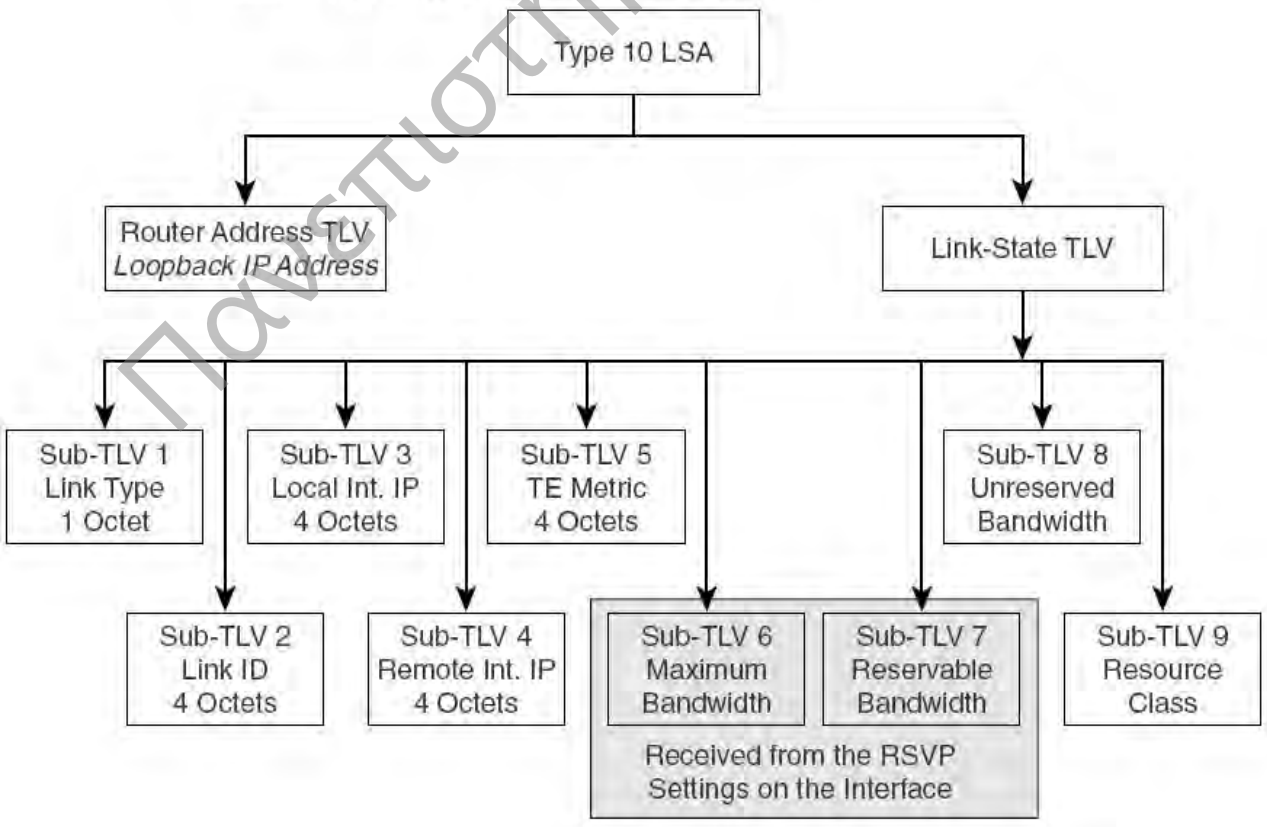
Βήμα 4 Αφού η RSVP διαδικασία παραλάβει ένα reservation μήνυμα δίνει σήμα ότι το LSP έχει πλέον δημιουργηθεί.

Βήμα 5 Σ’ αυτήν την χρονική στιγμή το TE tunnel είναι διαθέσιμο στο IGP για χρήση. Ως προεπιλογή οι πληροφορίες του tunnel δεν προστίθενται στον πίνακα δρομολόγησης ὁ βεβαίως κάτι τέτοιο μπορεί να ρυθμιστεί.

4.7 OSPF προεκτάσεις για MPLS TE

Το OSPF μπορεί να χρησιμοποιηθεί ως πρωτόκολλο κατάστασης δικτύου στο MPLS TE για την πλημμύρα του δικτύου με πληροφορίες κατανομής των πόρων χρησιμοποιώντας ως εργαλείο τις προεκτάσεις του OSFP ή των διαφανή *LSAs(link stare advertisements)*. Ο τύπος του LSA που χρησιμοποιείται καθορίζεται από τον σκοπό της ενημέρωσης . Επίσης το OSPF επεξεργάζεται τις ιδιότητες TLV και sub-TLV οι οποίες μπορεί να ρυθμιστούν να αναπαράγουν πληροφορίες διαθεσιμότητας πόρων στις ενημερώσεις κατάστασης σύνδεσης. Τα «διαφανή» LSAs είναι τύπου 9,10 και 11και διαφέρουν όπως προαναφέρθηκε στον σκοπό ενημέρωσης. Τα τύπου 9 LSAs δεν μεταδίδονται πέρα του τοπικού υποδικτύου και έχουν αρμοδιότητα τοπικής-σύνδεσης. Τα τύπου 10 LSAs δεν μεταδίδονται πέρα του ABR και έχουν αρμοδιότητα τοπικής-περιοχής. Τα τύπου 11 LSAs μεταδίδονται μέσα σε όλο το αυτόνομο σύστημα(AS). Η τεχνολογία που εφαρμόζει η Cisco σήμερα υποστηρίζει τα LSAa τύπου 10. Τα LSA τύπου 10, τα οποία σήμερα χρησιμοποιούνται στο MPLS TE, έχουν ένα σύνολο από TLV και sub-TLV τιμές τα οποία περιγράφουν συγκεκριμένους πόρους σε μία TE περιοχή (domain).Το σχέδιο 4.9 εμφανίζει τις TLV και sub-TLV τιμές και τις κατάλληλες τιμές που απαιτούνται για ενεργοποιήσουν το OSPF να κάνει χρήση MPLS TE.

ΣΧΕΔΙΟ 9 *OSPF TLV/Sub-TLV TE Extensions*



Οι πιο σημαντικές sub-TLV τιμές που αφορούν το to TE είναι οι 6, 7και 8. Οι τιμές 6 και 7 λαμβάνονται από την διαμόρφωση του RSVP για το συγκεκριμένο interface.Η τιμή 8 καθορίζει το διαθέσιμο εύρος για κράτηση σε κάθε μία από τις 8 προτεραιότητες.

4.8 IS-IS προεκτάσεις για MPLS TE

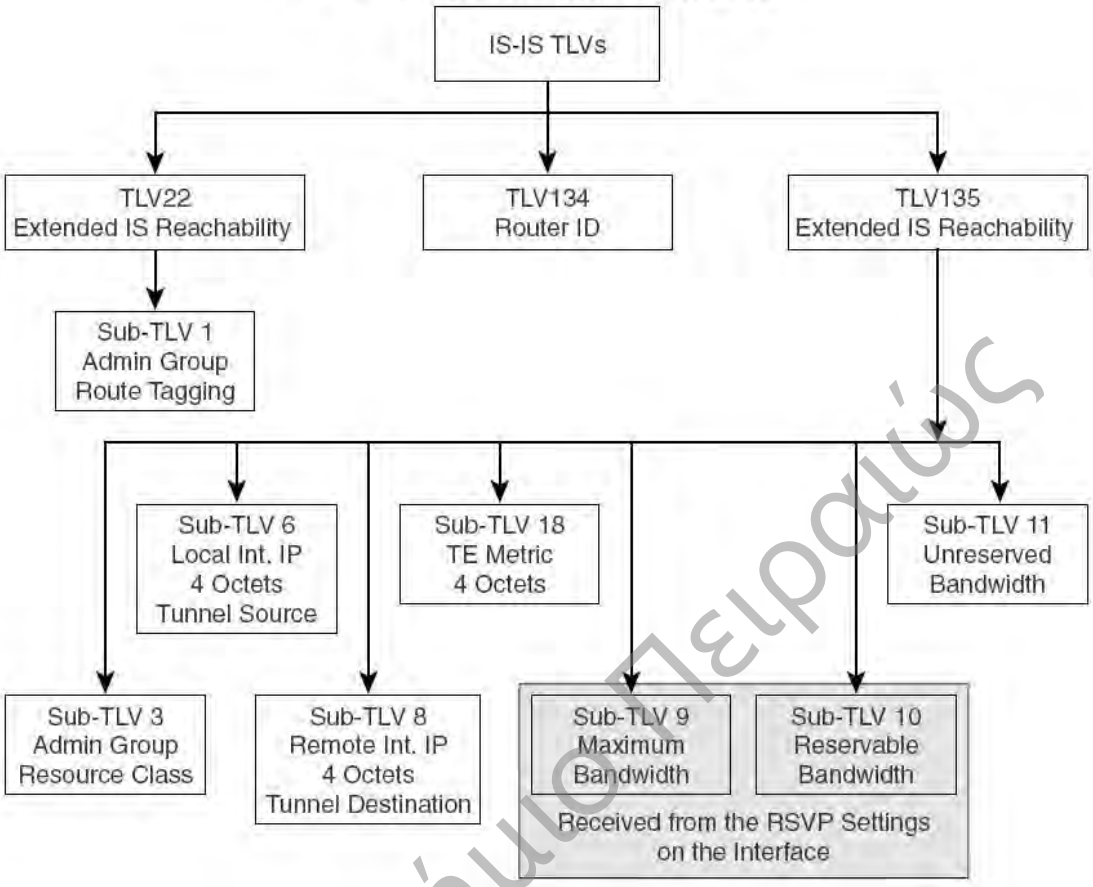
Ομοίως με το OSPF,το IS-IS μπορεί επίσης να χρησιμοποιηθεί σαν πρωτόκολλο κατάστασης σύνδεσης στην TE περιοχή. Το IS-IS με προεκτάσεις και τα πρόσφατα καθορισμένα TLVs μπορούν να χρησιμοποιηθούν για να αναπαράγουν πληροφορίες που σχετίζονται με την κατοχύρωση πόρων σε μία MPLS TE περιοχή. Τα παρακάτω TLVs έχουν καθοριστεί για την χρήση τους στο IS-IS ως κατάστασης σύνδεσης IGP σε μια MPLS TE περιοχή:

• **TLV22: Extended IS reachability**—Αυτό το TLV παράγει πληροφορίες σχετικά με την κατάσταση των γραμμών μέσα στο δίκτυο και επιτρέπει την χρήση των "ευρέων" μετρικών. Επιπλέον αυτό το TLV παρέχει πληροφορίες σχετικά με την διαθεσιμότητα πόρων ,όπως εύρος ζώνης.

• **TLV134: Router ID**—Αυτό το TLV χρησιμοποιείται για να καθορίσει τον δρομολογητή μια σαφή IP διεύθυνση. Η IP διευθύνσεις πηγής και προορισμού, που χρησιμοποιούνται για να υποδείξουν τα σημεία εκκίνησης και τερματισμού του tunnel πρέπει να συνδυάζονται με το router ID.

• **TLV135: Extended IP reachability**—Αυτό το TLV χρησιμοποιεί τα "ευρέως" μετρικά και προσδιορίζει αν ένα prefix είναι επιπέδου-1 ή επιπέδου-2. Επίσης επιτρέπει την κατάρρευση διαδρομών όταν ένα prefix μετατρέπεται από επιπέδου 2 σε επίπεδο 1.
Επιπλέον τα sub-TLVs έχουν καθοριστεί να προσθέτουν πληροφορίες που σχετίζονται με την κατανομή των TE πόρων στις ανανεώσεις. Κάθε sub-TLV αποτελείται από 3 οκτάδες εκτός από αυτές που παρουσιάζονται στο σχέδιο 4.10. το σχέδιο 4.10 εμφανίζει τα TLVs και sub-TLVs που χρησιμοποιούνται από το IS-IS για να υποστηρίξει MPLS TE

ΣΧΕΔΙΟ 10 *IS-IS TLV/Sub-TLVs for MPLS TE*



Τα σημαντικά TLVs είναι τα Sub-TLV 6 και 8, τα οποία υποδεικνύουν τα άκρα του tunnel ή τις IP διευθύνσεις πηγής και προορισμού, τα Sub-TLV 9 και 10,τα οποία συσχετίζουν τις RSVP ρυθμίσεις με κάποιο συγκεκριμένο interface και το Sub-TLV 11,το οποίο αντιστοιχίζει το ελεύθερο εύρος ζώνης ανά προτεραιότητα σε ένα interface αφού έχει γίνει η δέσμευση των πόρων για τις ενεργές συνδέσεις .

Κεφάλαιο 5 - Quality of Service(QoS) στα MPLS Δίκτυα (Ποιότητα Υπηρεσίας)

Κατά τη διάρκεια των προηγούμενων ετών, πολυάριθμοι μηχανισμοί έχουν εμφανιστεί για την παροχή ποιότητας εξυπηρέτησης (QoS). Ο στόχος αυτών των μηχανισμών είναι να παρασχεθεί βελτιωμένη εξυπηρέτηση στις εφαρμογές στα άκρα του δικτύου. Στη συνέχεια αναλύονται εν συντομία τα οφέλη του QoS, οι διαθέσιμοι μηχανισμοί QoS και πώς αυτοί επικοινωνούν.

5.1 Γενικά περί QoS

5.1.1 Τα οφέλη του QoS

Τα τελευταία χρόνια είμαστε μάρτυρες μιας ταχύτατης αύξησης στην κυκλοφορία της πληροφορίας μέσω των δικτύων υπολογιστών. Οι διαχειριστές των δικτύων αγωνίζονται για να συμβαδίσουν με τη συνεχώς αυξανόμενη ζήτηση με το να προσθέτουν χωρητικότητα στα δίκτυά τους. Παρόλα αυτά, οι πελάτες των δικτύων είναι συχνά δυσαρεστημένοι με την απόδοση του δικτύου. Η αύξηση χρήσης των «πεινασμένων για πόρους» (resource hungry) εφαρμογών πολυμέσων φαίνεται να επιδεινώνει την κατάσταση. Οι μηχανισμοί QoS παρέχουν ένα σύνολο εργαλείων που μπορεί να χρησιμοποιηθεί από το Network administrator για να διαχειριστεί τη χρήση των πόρων των δικτύων με έναν ελεγχόμενο και αποδοτικό τρόπο.

5.1.2 Προσδιορισμός της έννοιας QoS

Ο όρος QoS αναφέρεται στην ικανότητα ενός δικτύου να παρέχει τη δυνατότητα για καλύτερη και εγγυημένη εξυπηρέτηση επί του κυκλοφοριακού φόρτου του φορτίου χρησιμοποιώντας διάφορες τεχνολογίες (Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet και 802.1 δίκτυα, SONET, και IP-routed δίκτυα).

Με απλούστερα λόγια, Quality of Service (QoS) σημαίνει την παροχή σταθερού, προβλέψιμου ρυθμού μεταφοράς δεδομένων. Ή αλλιώς η ικανοποίηση των απαιτήσεων των εφαρμογών του πελάτη.
Ο βασικός στόχος του QoS είναι να μπορεί να διαθέσει συγκεκριμένο εύρος, ελεγχόμενο jitter και καθυστέρηση, καθώς επίσης και βελτιωμένα χαρακτηριστικά απωλειών.

Ο στόχος του QoS είναι:

• *έλεγχος επί των πόρων*—(bandwidth, εξοπλισμός, wide-area facilities, και ου το καθεξής)

• *αποδοτικότερη χρήση των πόρων του δικτύου* —με τη χρήση των εργαλείων του QoS γίνεται δυνατή η παρακολούθηση χρήσης του δικτύου και η καλύτερη δυνατή εξυπηρέτηση της κρίσιμης κυκλοφορίας

• *η δημιουργία κατηγοριών υπηρεσιών(cos)*—κατηγοριοποίηση των προσφερόμενων προς τους πελάτες υπηρεσιών, για την καλύτερη εξυπηρέτησή τους.

• συνύπαρξη *κρίσιμων εφαρμογών*—οι μηχανισμοί QoS εξασφαλίζουν την ικανοποιητικότερη δυνατή χρήση του δικτύου από τις κρίσιμες εφαρμογές, ότι θα τηρηθούν οι περιορισμοί σε εύρος και καθυστέρηση που επιβάλλονται από «απαιτητικές» εφαρμογές όπως οι εφαρμογές πολυμέσων και φωνής, αλλά και ότι οι υπόλοιπες εφαρμογές θα εξυπηρετηθούν χωρίς να αναμιχθούν με τις κρίσιμες εφαρμογές.

Η ικανοποίηση αυτών των στόχων θα έχει ως αποτέλεσμα τη βελτίωση των προσφερόμενων υπηρεσιών, ενώ ταυτόχρονα θα καλυφθεί η απαιτούμενη ζήτηση σε χωρητικότητα. Με άλλα λόγια, το QoS μπορεί να βοηθήσει στη βελτίωση των υπηρεσιών που προσφέρονται στους χρήστες δικτύων, μειώνοντας ταυτόχρονα τις δαπάνες για αυτές τις υπηρεσίες. Η επίτευξη του QoS απαιτεί τη συνεργασία όλων των επιπέδων του δικτύου, από πάνω προς τα κάτω, καθώς και κάθε στοιχείου του δικτύου, από άκρο σε άκρο.

Σαν αποτέλεσμα το επιτευκτό QoS είναι μόνο τόσο καλό όσο η πιο αδύνατη σύνδεση στη "αλυσίδα" μεταξύ του πομπού και του δέκτη.

Το QoS δεν παράγει εύρος ζώνης (bandwidth). Δεν είναι δυνατόν το δίκτυο να αποδώσει κάτι που δεν έχει. Έτσι, το υπάρχον εύρος αποτελεί έναν περιοριστικό παράγοντα. Το QoS απλά διαχειρίζεται το bandwidth σύμφωνα με τις απαιτήσεις των εφαρμογών και τις ρυθμίσεις διαχείρισης του δικτύου. Επομένως, QoS με εγγυημένο επίπεδο υπηρεσίας απαιτεί κατανομή πόρων σε κάθε ανεξάρτητη ροή δεδομένων. Βασικό στοιχείο της προσπάθειας των σχεδιαστών του QoS ήταν να βεβαιωθούν ότι η κυκλοφορία καλύτερης προσπάθειας (best effort traffic) θα μπορεί να εξυπηρετείται, αφού γίνουν όλες οι δεσμεύσεις. Οι εφαρμογές υψηλής προτεραιότητας δε θα πρέπει να καταστήσουν ανέφικτη τη χρήση εφαρμογών χαμηλής προτεραιότητας.

5.1.3 Γιατί απαιτείται η ύπαρξη του QoS

Οι εφαρμογές παράγουν κυκλοφορία σε διάφορους ρυθμούς και γενικά απαιτούν ότι τα δίκτυα θα είναι σε θέση να μεταφέρουν τον όγκο της πληροφορίας τον οποίο αυτές παράγουν. Επιπλέον, οι εφαρμογές μπορεί να είναι ανεκτικές ή όχι στις κυκλοφοριακές καθυστερήσεις του δικτύου και στις μεταβολές της. Ορισμένες εφαρμογές μπορούν να ανεχτούν κάποιο βαθμό απώλειας κυκλοφορίας, ενώ άλλες δεν μπορούν. Εάν υπήρχαν άπειροι πόροι δικτύων διαθέσιμοι, όλη η πληροφορία που θα παρήγαγε η κάθε εφαρμογή θα μπορούσε να μεταφερθεί με τον απαιτούμενο από την εφαρμογή ρυθμό, με μηδενική καθυστέρηση και χωρίς απώλεια πακέτων. Εντούτοις, οι πόροι των δικτύων δεν είναι άπειροι. Κατά συνέπεια, υπάρχουν μέρη του δικτύου στα οποία οι πόροι των δικτύων δεν είναι αρκετοί για να ικανοποιήσουν τις απαιτήσεις.

Τα δίκτυα χτίζονται με τη σύνδεση των συσκευών δικτύων όπως οι διακόπτες και οι δρομολογητές. Αυτοί διαβιβάζουν την κυκλοφορία μεταξύ τους χρησιμοποιώντας τις διεπαφές (interfaces). Εάν ο ρυθμός με τον οποίο η κυκλοφορία φθάνει σε μια διεπαφή υπερβαίνει τον ρυθμό με τον οποίο μπορεί αυτή να την προωθήσει στην επόμενη συσκευή εμφανίζεται συμφόρηση. Κατά συνέπεια, η ικανότητα μιας διεπαφής να προωθήσει την κυκλοφορία είναι ένα θεμελιώδες στοιχείο της συμπεριφοράς του κάθε δικτύου. Οι QoS μηχανισμοί λειτουργούν με το να διανείμουν αυτούς τους πόρους κατά προτίμηση σε συγκεκριμένη κυκλοφορία.

Προκειμένου να γίνει αυτό, είναι πρώτα απαραίτητο να προσδιοριστεί η διαφορετική κυκλοφορία. Η κυκλοφορία που φθάνει στις συσκευές των δικτύων είναι χωρισμένη στις ευδιάκριτες ροές μέσω της διαδικασίας της ταξινόμησης πακέτων. Η κυκλοφορία από κάθε ροή κατευθύνεται έπειτα σε μια αντίστοιχη ουρά αναμονής στη διεπαφή διαβίβασης. Οι ουρές αναμονής σε κάθε διεπαφή εξυπηρετούνται σύμφωνα με κάποιο αλγόριθμο. Ο αλγόριθμος αναμονής-εξυπηρέτησης ουράς καθορίζει το ρυθμό με τον οποίο η κυκλοφορία από κάθε ουρά αναμονής προωθείται, και έτσι καθορίζει τους πόρους που θα διατίθενται σε κάθε ουρά και στις αντίστοιχες ροές. Κατά συνέπεια, προκειμένου να παρασχεθεί QoS στο δίκτυο, είναι απαραίτητο να προσδιορισθούν οι :

1. Πληροφορίες ταξινόμησης με βάση τις οποίες οι συσκευές θα χωρίζουν το συνολικό όγκο της πληροφορίας σε ροές.
2. Αλγόριθμοι ουρών αναμονής και εξυπηρέτησης αυτών που θα χειρίζονται την κυκλοφορία από τις χωριστές ροές.

Θα αναφερθούμε σε αυτά συνολικά ως μηχανισμούς χειρισμού κυκλοφορίας. Μεμονωμένα, οι μηχανισμοί χειρισμού κυκλοφορίας δεν είναι χρήσιμοι. Πρέπει να ορίζονται ή να διαμορφώνονται με έναν συντονισμένο τρόπο που να παρέχει χρήσιμες από άκρη σε άκρη (end-to-end) υπηρεσίες μέσω ενός δικτύου. Για να φανεί λεπτομερέστερα η ανάγκη για QoS ας δούμε την περίπτωση των IP δικτύων.

5.2 Το QoS στα IP δίκτυα

Το πρωτόκολλο (IP) του Διαδικτύου, και η ίδια η αρχιτεκτονική του, είναι βασισμένα στο απλό σκεπτικό ότι τα datagrams (πακέτα-διαγράμματα δεδομένων) με τις διευθύνσεις πηγής και προορισμού μπορούν να διαπεράσουν ένα δίκτυο δρομολογητών (IP) ανεξάρτητα, χωρίς τις οδηγίες του πομπού ή του δέκτη τους. Το Διαδίκτυο στηρίχτηκε ιστορικά στην έννοια ενός «χαζού» δικτύου, με τα «έξυπνα» κομμάτια του σε κάθε άκρο του (στον πομπό και το δέκτη).

Υπάρχει, εντούτοις, ένα κόστος για αυτήν την απλότητα. Ο λόγος που το IP είναι τόσο απλό είναι επειδή δεν παρέχει πολλές υπηρεσίες. Το IP παρέχει τη διευθυνσιοδότηση και αυτή επιτρέπει την ανεξαρτησία του κάθε datagram. Το IP μπορεί να τεμαχίσει τα datagrams (στους δρομολογητές) και να τα συναρμολογήσει εκ νέου (στο δέκτη), και αυτό τους επιτρέπει να κινούνται μέσω των διαφορετικών δικτύων. Αλλά το IP δεν παρέχει την αξιόπιστη παράδοση δεδομένων. Οι δρομολογητές επιτρέπεται να απορρίψουν IP datagrams καθ' οδόν, χωρίς να ενημερώσουν τον πομπό ή το δέκτη. Το IP στηρίζεται σε υψηλότερου επιπέδου «μεταφορικά μέσα» (π.χ. TCP) για την παρακολούθηση των datagrams και την απόφαση να αναμεταδοθούν κάποια από αυτά, ανάλογα με τις ανάγκες. Και αυτοί οι μηχανισμοί "αξιοπιστίας" μπορούν μόνο να βεβαιώσουν την παράδοση δεδομένων; ούτε το IP ούτε τα υψηλού επιπέδου πρωτόκολλά της δεν μπορούν να εξασφαλίσουν έγκαιρη παράδοση ή να παρέχουν οποιεσδήποτε εγγυήσεις για τη ρυθμαπόδοση δεδομένων. Το IP παρέχει αυτό που καλείται υπηρεσία "καλύτερης προσπάθειας". Δεν μπορεί να δώσει καμία εγγύηση για το πότε περίπου θα φθάσουν τα δεδομένα ή πόσα μπορεί να παραδώσει.

Αυτός ο περιορισμός δεν είναι πρόβλημα για τις παραδοσιακές εφαρμογές Διαδικτύου όπως το WEB, το ηλεκτρονικό ταχυδρομείο, η μεταφορά αρχείων και άλλες όμοιες. Αλλά η νέα «φυλή» εφαρμογών, συμπεριλαμβανομένης της ηχητικής και τηλεοπτικής ροής, απαιτεί υψηλή ικανότητα ρυθμαπόδοσης δεδομένων (εύρος ζώνης) και έχει απαιτήσεις χαμηλής καθυστέρησης όταν χρησιμοποιούνται διπλής κατεύθυνσης επικοινωνίες (δηλ. σύσκεψη και

τηλεφωνία). Τα δημόσια και ιδιωτικά δίκτυα IP χρησιμοποιούνται επίσης όλο και περισσότερο για την παράδοση κρίσιμων πληροφοριών που δεν μπορούν να ανεχτούν απρόβλεπτες απώλειες.

Αντίθετα από τις τεχνολογίες "καθαρών εικονικών κυκλωμάτων" όπως τα ATM και τα Frame Relay, τα οποία άλλωστε εμπεριέχουν την έννοια του QoS, το IP δεν κάνει αυστηρές κατανομές των πόρων. Αυτό παρέχει αποδοτικότερη χρήση του διαθέσιμου εύρους ζώνης και το καθιστά πιο εύκαμπτο. Η χαρακτηριστική κυκλοφορία IP δικτύων είναι bursty (με εξάρσεις) παρά συνεχής. Το IP βασίζεται στα datagrams ώστε να χρησιμοποιεί το διαθέσιμο εύρος ζώνης όσο το δυνατόν αποτελεσματικότερα, με τη διανομή αυτού που είναι διαθέσιμου όπως απαιτείται. Αυτό επιτρέπει επίσης στο IP να προσαρμόζεται πιο εύκολα στις εφαρμογές με ποικίλες ανάγκες. Εντούτοις, οδηγεί επίσης σε κάποια μη προβλεψιμότητα στην παρεχόμενη υπηρεσία.

5.3 Συγκεκριμένα παραδείγματα

Οι ακόλουθες παράγραφοι περιγράφουν διάφορα συγκεκριμένα παραδείγματα των οφελών που μπορούν να αναμένονται ως αποτέλεσμα της επέκτασης του QoS

- Βελτιωμένη απόδοση των κρίσιμων εφαρμογών αποστολής επί **WAN** Δικτύων

  Εφαρμογές συνδέσεων όπως το SAP και PeopleSoft που χρησιμοποιούνται συχνά για να παρέχουν τις κρίσιμες υπηρεσίες πέρα από την ευρείας περιοχής intranets. Αυτές οι συνδέσεις είναι ιδιαίτερα ευαίσθητες στη συμφόρηση, η οποία οδηγεί σε αργούς χρόνους απόκρισης ή και σε διακοπές επικοινωνίας, οι οποίοι μπορούν να είναι δαπανηροί. Το QoS επιτρέπει στον network administrator για να δώσει προτεραιότητα στην «κρίσιμη» κυκλοφορία, έτσι ώστε να είναι απρόσβλητη από τη συμφόρηση στις **WAN** συνδέσεις. Αυτό μπορεί να επιτευχθεί με ελάχιστο κόστος στις λιγότερο σημαντικές, ανταγωνιστικές εφαρμογές. Η λύση του QoS είναι ανάλογη με την παροχή εναλλακτικών γραμμών, παράλληλα με τις απασχολημένες «λεωφόρους» μεταφοράς των πληροφοριών. Η κρίσιμη κυκλοφορία κατευθύνεται από αυτές τις “lanes.”

- Έλεγχος του αντίκτυπου της πολυμεσικής κυκλοφορίας στο δίκτυο

  Πολυμεσικές εφαρμογές όπως τα Windows Media™ Technologies, NetMeeting® λογισμικό σύσκεψης, RealAudio, και οι εφαρμογές

βασισμένες σε TAPI 3,0 κερδίζουν συνεχώς δημοτικότητα μεταξύ των χρηστών δικτύων. Αυτές παράγουν μεγάλο όγκο UDP κυκλοφορίας. Αυτή η κυκλοφορία δεν είναι «φιλική» προς το δίκτυο υπό την έννοια ότι δεν "υποχωρεί" παρά τη συμφόρηση. Λόγω του πιθανού αντικτύπου αυτού του τύπου κυκλοφορίας στους πόρους του δικτύου, οι network administrators προσπαθούν να περιορίσουν την επέκταση των εφαρμογών πολυμέσων στα δίκτυά τους. Οι μηχανισμοί QoS επιτρέπουν στον network administrator να ελέγξουν τον αντίκτυπο αυτών των εφαρμογών στο δίκτυο.

• Επιτρέποντας τα πολυμέσα

Στο προηγούμενο παράδειγμα, αναλύθηκε η χρήση QoS για να ελεγχθεί το αντίκτυπο των εφαρμογών αυξημένης ροής πληροφορίας στους πόρους των δικτύων χωρίς να ανησυχούμε για τις υπηρεσίες που παρέχονται πραγματικά στις εφαρμογές πολυμέσων. Το QoS μπορεί να εφαρμοσθεί για να εγγυηθεί συγκεκριμένη ποιότητα υπηρεσιών σε κάθε εφαρμογή πολυμέσων. Το QoS επιτρέπει σε αυτήν την περίπτωση την αληθινή σύγκλιση των δικτύων πολυμέσων και δεδομένων. Τα οφέλη μιας τέτοιας σύγκλισης περιλαμβάνουν (μεταξύ άλλων) τη χρησιμοποίηση IP τηλεφωνίας με ισόμετρη μείωση του κόστους.

5.4 Ποια είναι τα επιχειρησιακά οφέλη από το QoS

5.4.1 Τα οφέλη για τις επιχειρήσεις

Τα δίκτυα χρησιμοποιούνται ολοένα και περισσότερο ως επιχειρηματικά μέσα και οι προσδοκίες για τη διασφάλιση της ποιότητας είναι υψηλές. Το Διαδίκτυο χρησιμοποιείται για να ενδυναμώσει τα intranets μέσα στην επιχείρηση και τα extranets που επιτρέπουν το ηλεκτρονικό εμπόριο με τους επιχειρησιακούς συνεργάτες. Καθώς η επιχείρηση χρησιμοποιεί όλο και περισσότερο τα δίκτυα (και ιδίως τον Ιστό), γίνεται όλο και σημαντικότερο να διασφαλιστεί ότι αυτά τα δίκτυα προσδίδουν τα κατάλληλα επίπεδα ποιότητας. Η ποιότητα των τεχνολογιών υπηρεσιών (QoS) παρέχει τα εργαλεία για τους IT διευθυντές να το εξασφαλίσουν αυτό.

5.4.2 Τα οφέλη για τις εφαρμογές

Οι εφαρμογές παράγουν απαιτήσεις. Οι κρίσιμες εφαρμογές που εκτείνονται επί των διαφόρων δικτύων απαιτούν όλο και περισσότερο την ποιότητα, την αξιοπιστία, και τις διαβεβαιώσεις ελαχιστοποίησης του απαιτούμενου χρόνου. Ειδικότερα, οι εφαρμογές που χρησιμοποιούν φωνή, video ή πολυμέσα πρέπει να διαχειριστούν προσεκτικά μέσα σε κάθε δίκτυο για να συντηρήσουν την ακεραιότητά τους. Η διαχείριση QoS γίνεται όλο και πιο δύσκολη επειδή πολλές εφαρμογές εμφανίζουν απρόβλεπτες εκρήξεις κυκλοφορίας. Παραδείγματος χάριν, η συμπεριφορά του ηλεκτρονικού ταχυδρομείου και των εφαρμογών μεταφοράς αρχείων είναι ουσιαστικά αδύνατη να προβλεφθεί, όμως οι διευθυντές δικτύων πρέπει να είναι σε θέση να υποστηρίξουν τις κρίσιμες εφαρμογές ακόμη και κατά τη διάρκεια των περιόδων αιχμής. Οι QoS τεχνολογίες επιτρέπουν στους διευθυντές IT και τους διευθυντές δικτύων:

- Να διαχειριστούν τις ευαίσθητες στο jitter εφαρμογές, όπως ηχητικά και το βίντεο playbacks
- Να διαχειριστούν την ευαίσθητη στην καθυστέρηση κυκλοφορία, όπως η φωνή πραγματικού χρόνου
- Να ελέγξουν την απώλεια σε περιόδους της αναπόφευκτης συμφόρησης

5.4.3 Τα οφέλη στους φορείς παροχής υπηρεσιών

Οι φορείς παροχής υπηρεσιών που μπορούν να προσφέρουν τις διασφαλίσεις ποιότητας για την από άκρη σε άκρη επιχειρησιακή κυκλοφορία θα κερδίσουν περισσότερους πελάτες. οι τεχνολογίες QoS θα επιτρέψουν στους φορείς παροχής υπηρεσιών να προσφέρουν περισσότερες υπηρεσίες, όπως η σε πραγματικό χρόνο υποστήριξη κυκλοφορίας ή οι συγκεκριμένες κατανομές εύρους ζώνης, για να χτίσουν ένα χαρτοφυλάκιο SLA. Αυτό δημιουργεί νέα εισοδήματα για τους φορείς παροχής υπηρεσιών, προσφέροντας περισσότερες υπηρεσίες στις επιχειρήσεις.

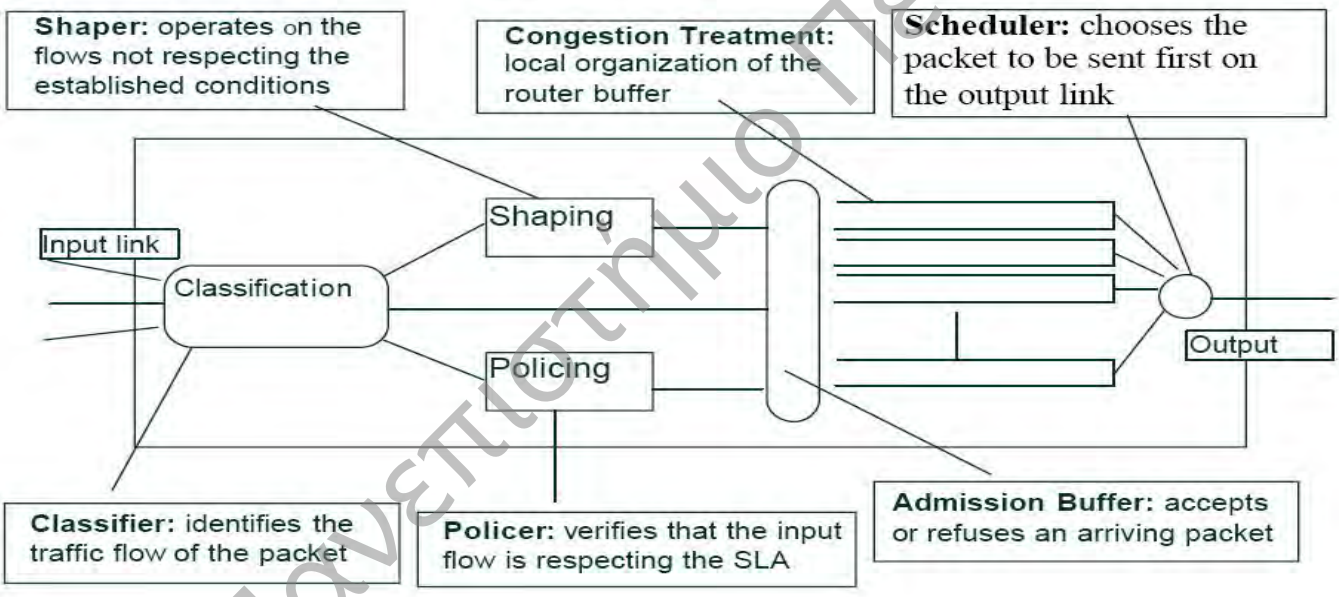
5.5 Μηχανισμοί QoS

Για να επιτευχθεί η διαφοροποίηση υπηρεσιών απαιτείται η εφαρμογή διαφόρων κατάλληλων μηχανισμών για την διαχείριση της κίνησης.
Οι βασικές λειτουργίες που πραγματοποιούνται από τους δρομολογητές όπως καθορίζονται από την IETF είναι οι εξής :

- Κατηγοριοποίηση πακέτων : προσδιορίζεται η κυκλοφοριακή ροή του πακέτου.

• Έλεγχος κίνησης: σχετίζεται με όλες τις λειτουργίες εισόδου της κίνησης και επαλήθευσης εφαρμογής των SLA. Οι λειτουργίες του ελέγχου κίνησης είναι 4. 3 είναι υποχρεωτικοί και 1 προαιρετικός

- Αλγόριθμος ελέγχου εισόδου: επιβεβαιώνει, με αίτηση του πελάτη, αν είναι δυνατό να δοθεί το QoS που απαιτείται χωρίς να απαιτούνται οι υπηρεσίες που δίνονται στις άλλες ροές κίνησης.
- Αλγόριθμος συμμόρφωσης: πρόκειται για ένα test για να απομονωθεί η κίνηση η οποία δεν συμμορφώνεται με τα πρότυπα που απαιτούνται από τον πελάτη.
- Επιτηρητής (Policer): είναι η διαδικασία που εμπλέκεται στην μεταχείριση της κίνησης εκτός συμμόρφωσης: συνήθεις πράξεις είναι ο αποχαρακτηρισμός ή απόρριψη της συγκεκριμένης κίνησης.
- Μεταμορφωτής (Shaper): είναι μία προαιρετική διαδικασία η οποία «μεταμορφώνει» την κίνηση ώστε να πληρεί τα προκαθορισμένα πρότυπα.



• Σχέδιο (προγραμματισμός μετάδοσης) πακέτου (Packet Scheduling): εγγυάται ότι το QoS διαχειρίζεται την προώθηση των πακέτων μέσω ξεχωριστού μηχανισμού διαχείρισης ουράς. Κάθε δρομολογητής έχει μια ξεχωριστή διαδικασία σχεδίασης για να αποφασίζει από στιγμή σε στιγμή ποια ροή κίνησης πρέπει να μεταδίδεται . (Παράδειγμα ο αλγόριθμος Weighted Round Robin).

• Αντιμετώπιση συμφόρησης : είναι απαραίτητο να αποφεύγονται περιπτώσεις υψηλής δικτυακής συμφόρησης : Η πιο συνηθισμένη τεχνική είναι η απόρριψη πακέτων όταν κάποιο threshold καθυστερήσει . Ένας μηχανισμός που συνήθως χρησιμοποιείται είναι ο Random Early Detection (RED).

5.6. Οι βασικές παράμετροι του QoS

Καθυστέρηση (latency)

Ο χρόνος μεταξύ της αποστολής μηνύματος από ένα κόμβο και της παραλαβής του μηνύματος από έναν άλλο κόμβο. Αυτό καλύπτει την καθυστέρηση σε ένα μονοπάτι μετάδοσης ή σε μια συσκευή μέσα σε ένα μονοπάτι μετάδοσης. Σε έναν δρομολογητή, η καθυστέρηση είναι το χρονικό διάστημα μεταξύ της λήψης ενός πακέτου δεδομένων και της αναμετάδοσης του. Επίσης αναφέρεται και ως καθυστέρηση διάδοσης (propagation delay).

Jitter («τρεμούλιασμα»)

Μια παρέκκλιση που εμφανίζεται όταν διαβιβάζεται το βίντεο ή η φωνή μέσω ενός δικτύου και κάποια πακέτα δεν φθάνουν στον προορισμό τους με τη σωστή κατάταξη ή εγκαίρως, δηλ. ποικίλλουν οι καθυστερήσεις. Η διαστρέβλωση ενός σήματος όπως προωθήθηκε μέσω του δικτύου, όπου το σήμα διαφέρει από τον αρχικό συγχρονισμό αναφοράς του. Στα packet-switched δίκτυα, το jitter είναι μια διαστρέβλωση των χρόνων μεταξύ των αφίξεων των πακέτων έναντι των χρόνων που μεσολαβούσαν μεταξύ των πακέτων κατά την αρχική μετάδοση. Αυτή η διαστρέβλωση είναι ιδιαίτερα επιζήμια στην κυκλοφορία πολυμεσικών εφαρμογών. παραδείγματος χάριν, η ακρόαση των ηχητικών ή τηλεοπτικών δεδομένων μπορεί να έχει μια ταραγμένη ή τρεμάμενη ποιότητα.

Εύρος ζώνης

Ένα μέτρο της ικανότητας μετάδοσης δεδομένων, που εκφράζεται συνήθως σε kilobits ανά δευτερόλεπτο (Kbps) ή megabits ανά δευτερόλεπτο (Mbps). Το εύρος ζώνης δείχνει τη θεωρητική μέγιστη ικανότητα μιας σύνδεσης, αλλά καθώς το θεωρητικό εύρος ζώνης προσεγγίζεται, οι αρνητικοί παράγοντες όπως η καθυστέρηση μετάδοσης μπορούν να προκαλέσουν επιδείνωση στην ποιότητα. Εάν αυξάνεται το εύρος ζώνης, μπορούν να μεταφερθούν περισσότερα δεδομένα. Το εύρος ζώνης δικτύων μπορεί να απεικονιστεί ως σωλήνας που μεταφέρει τα δεδομένα: Όσο μεγαλύτερος ο σωλήνας, τόσο περισσότερα δεδομένα μπορούν να σταλούν μέσω αυτού.

Απώλεια πακέτων

Η βαρύτητα αυτής της παραμέτρου για την κίνηση «πραγματικού χρόνου», είναι ξεκάθαρη. Η συγκεκριμένη κίνηση χρησιμοποιεί το UDP ως πρωτόκολλο μεταφοράς το οποίο δεν δίνει καμία εγγύηση για την παράδοση του πακέτου. Έτσι κάθε πακέτο που χάνεται αντιστοιχεί σε απώλεια δεδομένων ,σε μια πραγματικού χρόνου εφαρμογή, από την πλευρά του παραλήπτη. Επομένως είναι πολύ σημαντικό να εγγυάται μια πολύ μικρή τιμή απώλειας πακέτων

(Παράδειγμα:1% ή λιγότερη μηνιαία μέση απώλεια πακέτων σε ολόκληρο το δίκτυο.) αν θέλουμε να μιλάμε για QoS.

Διαθεσιμότητα

Πρόκειται για το ποσοστό μετάδοσης, δεδομένα που παραλήφθηκαν σε σχέση με δεδομένα που πραγματικά στάλθηκαν κατά τη μετάδοση. Αυτή η παράμετρος δεν περιλαμβάνει μόνο την κίνηση «πραγματικού χρόνου» αλλά και την TCP κίνηση ,συγκεκριμένα το TCP είναι προσαρμόσιμο ως προς την διαθεσιμότητα, έτσι όσο μεγαλύτερη είναι η διαθεσιμότητα ανάλογα μεγαλύτερη είναι και η TCP κίνηση, με προφανές αποτέλεσμα ταχύτερες εφαρμογές (πχ οι ιστοσελίδες ανοίγουν γρηγορότερα, οι Peer-to-Peer εφαρμογές ανταλλάσουν περισσότερα δεδομένα, κα).

Μια σύγχυση που συνήθως υπάρχει σχετικά με το MPLS και την ποιότητα υπηρεσίας (QoS) είναι ότι η προώθηση του πρώτου οδηγείται κυρίως από το δεύτερο. Σε σύγκριση με τους άλλους παράγοντες όπως IP VPNs και Traffic Engineering η ποιότητα υπηρεσίας δεν έχει καθοριστικό βάρος στην απόφαση υλοποίησης του MPLS. Η περισσότερη δουλειά στο χώρο γίνεται κυρίως στο πλαίσιο υποστήριξης υφιστάμενων χαρακτηριστικών ή/και τεχνικών για IP QoS σε ένα δίκτυο που τυγχάνει να είναι MPLS. Σκεφτείτε ακόμη ότι το MPLS δεν είναι ένα end-to-end πρωτόκολλο σε αντίθεση με το IP όπου και η ποιότητα υπηρεσίας έχει νόημα.

Συνεπώς ο ρόλος του MPLS είναι πρώτο να βοηθήσει κυρίως τους ISPs να προσφέρουν υπηρεσίες IP με QoS και δεύτερο να υποστηριχθούν QoS ικανότητες εντός των δικτύων των ISPs έστω και αν δεν είναι end-to-end (LSPs με εγγύηση ποιότητας).

Το πρωτόκολλο IP παρέχει δύο διαφορετικά μοντέλα QoS: Διαφοροποιημένες Υπηρεσίες (Differentiated Services) και Ολοκληρωμένες Υπηρεσίες (Integrated Services) συνυφασμένες με το RSVP.

5.7 Ολοκληρωμένες υπηρεσίες

Το πλαίσιο για τις ολοκληρωμένες υπηρεσίες (Integrated Services) είναι στενά συνδεδεμένο με τον ορισμό νέων κλάσεων υπηρεσιών και με την δέσμευση πόρων. Στις ολοκληρωμένες υπηρεσίες υπάρχουν δύο κατηγορίες υπηρεσιών επιπλέον της best-effort, αυτές είναι οι Guaranteed και Controlled-load.

Επειδή οι ολοκληρωμένες υπηρεσίες κάνουν δέσμευση πόρων χρειάζονται κάποιο signaling πρωτόκολλο, αυτό είναι σήμερα το RSVP. Αξίζει να σημειωθεί εδώ ότι σε κάθε μία από τις πρόσθετες δύο κατηγορίες των ολοκληρωμένων υπηρεσιών μπορούν να οριστούν άπειρες υπηρεσίες (π.χ. Guaranteed 5Mbps και end-to-end delay 2ms ή Guaranteed 5Mbps και end-to-end delay 10ms). Δηλαδή ο κατακερματισμός (granularity) των δύο αυτών κατηγοριών είναι θεωρητικά άπειρος.

5.7.1 Guaranteed service

Στην Guaranteed υπάρχει αυστηρή εγγύηση όσον αφορά την καθυστέρηση και το εύρος ζώνης που παρέχετε σε μια ροή. Η ιδέα στην οποία βασίζεται αυτή η υπηρεσία είναι ότι ο χρήστης περιγράφει στο δίκτυο την κυκλοφορία που πρόκειται να στείλει, στην συνέχεια κάθε δρομολογητής του δικτύου υπολογίζει τις παραμέτρους που δείχνουν πως θα συμπεριφερθεί στο δίκτυο μια τέτοια κυκλοφορία. Αθροίζοντας τις διάφορες παραμέτρους που θα επιστραφούν από τους υπόλοιπους δρομολογητές που βρίσκονται σε κάποιο μονοπάτι μπορούμε να υπολογίσουμε την μέγιστη δυνατή καθυστέρηση που μπορεί να αντιμετωπίσει ένα πακέτο που θα ταξιδεύει σε αυτό το μονοπάτι. Η συνολική καθυστέρηση που θα έχει κάποιο πακέτο είναι το άθροισμα της καθυστέρησης που οφείλεται στην μετάδοση των δεδομένων μέσα από το φυσικό μέσο και της καθυστέρησης λόγω ενταμίευσης (buffering).

Στην Guaranteed service δεσμεύομε πόρους για κάθε ροή σε όλο το μήκος του μονοπατιού που θα χρησιμοποιήσουμε. Με αυτόν τον τρόπο σε κάθε σύνδεσμο του μονοπατιού που χρησιμοποιούμε έχουμε δεσμεύσει R bandwidth το οποίο είναι αποκλειστικά για την συγκεκριμένη ροή. Όταν μια ροή τηρεί το συμβόλαιο της τότε το δίκτυο της παρέχει το προκαθορισμένο εύρος ζώνης, της εγγυάται ένα ανώτατο όριο όσον αφορά την καθυστέρηση των πακέτων και τέλος της εγγυάται ότι δεν θα έχει απώλεια πακέτων. Αυτή η υπηρεσία απευθύνεται σε εφαρμογές που έχουν αυστηρούς περιορισμούς ότι ένα πακέτο πρέπει να φτάσει στον δέκτη μέσα σε κάποιο περιορισμένο χρονικό διάστημα αλλιώς η πληροφορία είναι άχρηστη. Για παράδειγμα πολλές εφαρμογές audio καθιστούν άχρηστα όσα πακέτα φτάνουν μετά από κάποιο χρονικό περιθώριο.

5.7.2. Controlled-load service

Στην Controlled-load το μόνο που εγγυόμαστε είναι ότι οι ροές οι οποίες ανήκουν σε αυτήν την κατηγορία θα έχουν την ίδια μεταχείριση που θα είχαν αν άνηκαν στην best-effort και δεν υπήρχε συμφόρηση στο δίκτυο. Αυτό το εγγυόμαστε ανεξαρτήτου φόρτου του δικτύου. Αυτή η κατηγορία υπηρεσίας

είναι κατάλληλη και για εφαρμογές πραγματικού χρόνου οι οποίες έχουν δείξει ότι λειτουργούν καλά όταν το δίκτυο δεν είναι φορτωμένο αλλά χάνουν την λειτουργικότητα τους σε συνθήκες συμφόρησης.

Ο χρήστης που επιλέγει την Controlled load θα αντιλαμβάνεται την εξής συμπεριφορά όσον αφορά την μεταφορά των δεδομένων του:

• Τα περισσότερα πακέτα του (η μεγάλη πλειοψηφία) θα φτάνουν στον προορισμό τους. Το ποσοστό των πακέτων που δεν θα φτάνουν στον δεκτή θα είναι σχεδόν ίσο με το ποσοστό των πακέτων που χάνονται εξαιτίας λαθών που συμβαίνουν στο φυσικό επίπεδο.

• Η καθυστέρηση που θα αντιμετωπίζουν τα περισσότερα πακέτα δεν θα είναι πολύ μεγάλη και δεν θα οφείλεται κατά κύριο λόγο στο buffering. Δηλαδή η καθυστέρηση που θα έχουν τα περισσότερα πακέτα θα είναι περίπου ίση με το άθροισμα της καθυστέρησης που υπάρχει για την μεταφορά των πακέτων μέσα από το μέσο διάδοσης και της καθυστέρησης λόγω της επεξεργασίας στους μεταγωγείς και τα άλλα στοιχεία του μονοπατιού.

Για να μπορέσει το δίκτυο να εγγυηθεί αυτή την ποιότητα υπηρεσίας ο χρήστης θα πρέπει να δηλώσει ορισμένα χαρακτηριστικά της κυκλοφορίας που πρόκειται να περάσει μέσα από το δίκτυο. Αυτό γίνεται με την χρήση του Tspec και έχει σαν αποτέλεσμα την δέσμευση πόρων από το δίκτυο έτσι ώστε να είναι σε θέση(το δίκτυο) να παρέχει την απαιτούμενη ποιότητα υπηρεσίας για το ποσό της κυκλοφορίας που ζήτησε ο χρήστης. Το Tspec περιλαμβάνει της εξής παραμέτρους: τις Token bucket παραμέτρους(rate r, bucket depth b), το peak rate p, το ελάχιστο policed unit m και το μέγιστο policed unit M.

5.7.3 Ολοκληρωμένες υπηρεσίες και MPLS

Εξετάζοντας κανείς τη σχέση του MPLS με τις ολοκληρωμένες υπηρεσίες αρκεί όπως καταλαβαίνετε να δει πώς το RSVP συνεργάζεται με το MPLS.

Έχουμε ήδη συναντήσει το RSVP και ορισμένες επεκτάσεις του κατά την περιγραφή του Constrain-based routing (§Error! Reference source not found.). Εδώ δίνονται ορισμένες πρόσθετες πληροφορίες σχετικά με το ρόλο του RSVP για την υποστήριξη QoS.

Πρωταρχικός στόχος είναι να δώσουμε την ικανότητα στους LSRs να αναγνωρίζουν τις ροές πακέτων για τις οποίες έγινε κάποια δέσμευση πόρων, εδώ μέσω RSVP, καθώς θα ταξινομούν τα πακέτα εξετάζοντας μόνο την ετικέτα.

Αυτό επιτυγχάνεται με την συσχέτιση ροών (RSVP δεσμεύσεις πόρων) και ετικετών (LSPs) και διανομή τους στο MPLS δίκτυο.

Είδαμε ήδη την σχετική επέκταση του RSVP που συμπεριέλαβε δύο νέα αντικείμενα: "LABEL" και "LABEL_REQUEST" τα οποία μεταφέρονται στο μήνυμα PATH.

Η λειτουργία δέσμευσης ετικετών, μετά την επιτυχημένη αποστολή του PATH μηνύματος στο προορισμό, έχει ως ακολούθως: Ο LSR (προορισμός) δεσμεύει τοπικά μία διαθέσιμη ετικέτα, ενημερώνει τη LIB του - συμπληρώνει το πεδίο εισερχόμενης ετικέτας με την δεσμευμένη - και στέλνει το μήνυμα RESV ενσωματώνοντας σε αυτό το Label Object. Η LIB περιέχει και πληροφορίες για τους τοπικούς διαθέσιμους πόρους που θα χρησιμοποιηθούν π.χ. εύρος ζώνης, ουρές. Η πληροφορία αυτή μεταφέρεται επίσης στο RSVP μήνυμα. Κάθε ενδιάμεσος LSR προωθεί το RESV μήνυμα μέχρι αυτό να φτάσει στον προορισμό του (αφετηρία).

Στην περίπτωση που υπάρχει MPLS πάνω από ATM είναι αναγκαία η αντιστοίχηση των τριών κλάσεων του πλαισίου των ολοκληρωμένων υπηρεσιών στις πέντε κλάσεις υπηρεσίας του ATM. Η αντιστοίχηση που έχει προταθεί είναι η εξής:

- οι ροές οι οποίες ανήκουν στην Guaranteed να αντιστοιχηθούν σε VCs τα οποία θα είναι CBR ή rt-VBR. Αυτή η αντιστοίχηση είναι λογική γιατί όλες οι ροές που ανήκουν στην Guaranteed έχουν αυστηρές απαιτήσεις σε εύρος ζώνης και καθυστέρηση. Οι υπόλοιπες τρεις κλάσεις υπηρεσίας του ATM δεν παρέχουν τις εγγυήσεις που θέλουν αυτές οι ροές.
- για την controlled load υπηρεσίας έχει προταθεί όσες ροές ανήκουν σε αυτήν να παίρνανε από nrt-VBR ή ABR VCs. Βέβαια μπορούν να περνούν και από CBR ή rt-VBR VCs αλλά αυτό θα ήταν σπατάλη πόρων.
- για την Best effort χρησιμοποιούμε UBR VCs

5.8 Διαφοροποιημένες υπηρεσίες

Το πλαίσιο των διαφοροποιημένων υπηρεσιών (Differentiated Services) υποστηρίζει ένα διακριτό μοντέλο για διαχωρισμό των υπηρεσιών, δηλαδή έχουμε ένα πεπερασμένο σύνολο από κατηγορίες υπηρεσιών. Τα διάφορα πακέτα κατηγοριοποιούνται και μαρκάρονται κατάλληλα στις άκρες του δικτύου με την χρήση του πεδίου DSCP (Differentiated Services Code Point), αποτελεί ένα 6-bits τμήμα του γνωστού ToS. Στην συνέχεια ανάλογα με το μαρκάρισμα τα πακέτα έχουν διαφορετική αντιμετώπιση (παροχή QoS) στο δίκτυο.

Το πεδίο DSCP προσδιορίζει μία “per-hop behavior” (PHB) σε ένα κόμβο. Μία PHB είναι μια καλά ορισμένη συμπεριφορά που εφαρμόζεται στα πακέτα. Συνεπώς τα 6 bits του DSCP ενός πακέτου επιλέγουν μοναδικά μία εκ των 64 πιθανών PHBs. Υπάρχουν ορισμένες τυποποιήσεις PHBs όπως:

Defaut: Καμία ειδική μεταχείριση, ισοδυναμεί με best effort.

Expedited forwarding (EF). Πακέτα μαρκαρισμένα ως EF προωθούνται με ελάχιστη καθυστέρηση και υπόκεινται σε χαμηλή απώλεια.

Assured forwarding (AF). Εδώ ορίζεται ένα σύνολο από AF PHBs ως {AFxy}, όπου η τιμή x αναφέρεται ως AS class και συνήθως επιλέγει κάποια ουρά για το πακέτο, ενώ η τιμή y προσδιορίζει το drop preference του πακέτου. Για παράδειγμα πακέτα που μαρκάρονται με A11, A12 και A13 εξυπηρετούνται από την ίδια ουρά αλλά τα A13 θα απορριφθούν πρώτα (πριν από τα A11, A12) σε καταστάσεις συμφόρησης. Συνίσταται ο αριθμός των διαφορετικών AF PHBs να είναι 12, οργανωμένος σε 4 κλάσεις (x=1,2,3,4) με τρία επίπεδα drop preference σε κάθε μία.

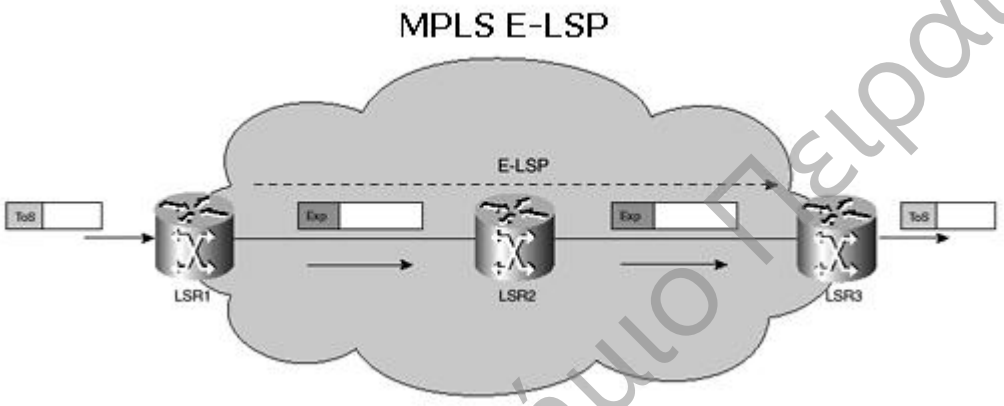
Ένα μειονέκτημα των διαφοροποιημένων υπηρεσιών είναι ότι δεν έχουν πρωτόκολλο για δέσμευση πόρων. Αυτό σημαίνει ότι δεν μπορούν να παρέχουν αυστηρή εγγύηση όσον αφορά την ποιότητα υπηρεσίας. Απλώς τα πακέτα που ανήκουν σε διαφορετικές κατηγορίες έχουν διαφορετική μεταχείριση. Πιο συγκεκριμένα οι πόροι του δικτύου κατανέμονται στις διάφορες κλάσεις υπηρεσίας (CoSs) και τα πακέτα της κάθε μίας από αυτές χρησιμοποιούν τους πόρους της συγκεκριμένης κλάσης. Αν δεν υπάρχουν διαθέσιμοι πόροι τότε δεν θα εξυπηρετηθεί το πακέτο. Αν δεν υπάρχουν άλλα πακέτα που να ανήκουν σε αυτήν την κατηγορία τότε το συγκεκριμένο πακέτο θα πάρει όλους τους πόρους.

5.8.1 MPLS και Diff-Serv

Το σημαντικό για την υποστήριξη των διαφοροποιημένων υπηρεσιών σε ένα δίκτυο MPLS είναι να εξασφαλιστεί πως πακέτα μαρκαρισμένα με πεδία DSCP θα απολαμβάνουν την κατάλληλη ποιότητα υπηρεσίας (QoS) σε κάθε LSR στο δίκτυο. Η δυσκολία έγκειται στο ότι η πληροφορία DSCP μεταφέρεται στη κεφαλή του IP πακέτου και ως γνωστό δεν εξετάζεται από έναν LSR όταν προωθούνται τα πακέτα. Συνεπώς η πληροφορία αυτή πρέπει να γνωστοποιηθεί στο LSR διαμέσου της ετικέτας με κάποια μέθοδο. Παρακάτω αναφέρονται σε συντομία οι δύο εναλλακτικοί τρόποι για να γίνει η μεταφορά της πληροφορίας στο label.

5.8.1.1 E-LSP

Ο πιο απλός είναι η αντιγραφή μέρους του πεδίου DSCP στο πεδίο Exp,. Θυμηθείτε ότι το πεδίο Exp έχει μέγεθος 3 bits και άρα μπορεί να εξυπηρετήσει μόνο 8 από τις 64 ενδεχόμενες κατηγορίες υπηρεσίας στο DSCP. Σε αυτή την περίπτωση οι διαφορετικές κλάσεις υπηρεσίας διέρχονται από το ίδιο LSP και το πεδίο Exp προσδιορίζει ποια PHB θα εφαρμοστεί στο πακέτο. Ουσιαστικά η ετικέτα (πεδίο Label) λέει σε ένα LSR που να προωθήσει το πακέτο και το πεδίο Exp ποιος PHB θα το χειριστεί. Τα LSPs που έχουν στηθεί υπό αυτές τις συνθήκες καλούνται E-LSPs, όπου το E προέρχεται από το Exp.

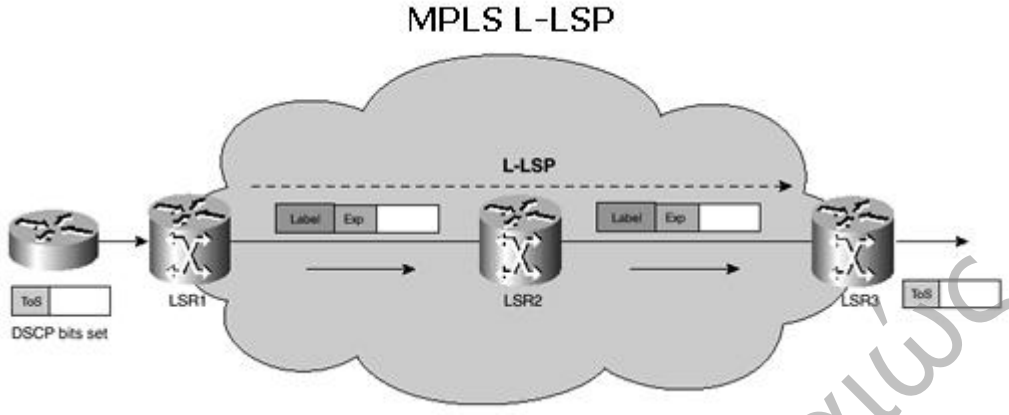


5.8.1.2 L-LSP

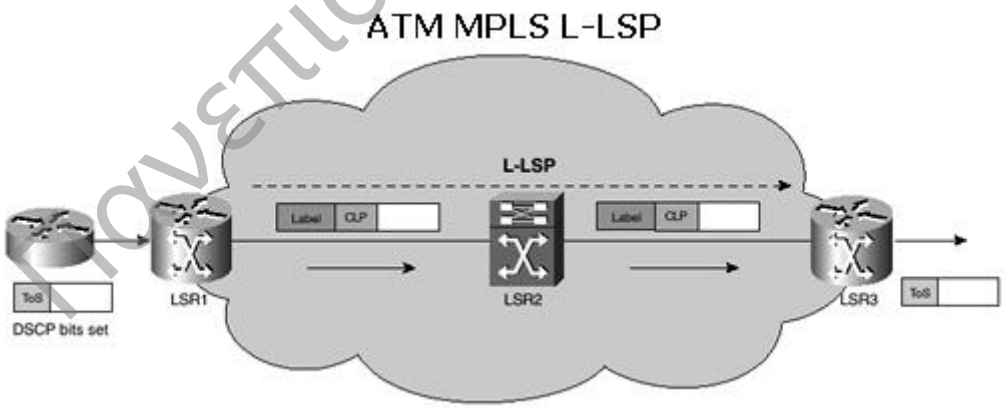
Ο δεύτερος τρόπος καλύπτει α) την περίπτωση που θέλουμε να υλοποιήσουμε πέραν των 8 διαφορετικών κατηγοριών υπηρεσίας και β) είδη συνδέσμων όπου δεν εμφανίζεται το πεδίο Exp στο label, όπως οι σύνδεσμοι ATM.

Αυτό που χρειάζεται είναι μια σχετική επέκταση των μηχανισμών διανομής των ετικετών ώστε μια ετικέτα να καθορίζει τόσο κάποιο LSP όσο και κάποιο PHB. Για παράδειγμα στο LDP το μήνυμα αίτησης ενός label περιλαμβάνει εκτός από το prefix και το PHB (<prefix, PHB>). Έτσι ένα LSP προσδιορίζεται εκτός από το label και από ένα PHB. Στη περίπτωση που η κίνηση χαρακτηρίζεται ως AF, θυμηθείτε ότι οργανώνεται ένα σύνολο AF PHBs {AFxy}, το LSP μπορεί να μεταφέρει ένα AF class (τιμή x) αλλά να τι γίνεται με τα διαφορετικά επίπεδα drop preference; Η επιλογή του επιπέδου drop preference (τιμή y) γίνεται με τη χρήση του πεδίου Exp έτσι ώστε τελικά σε κάθε LSP να μπορεί να αντιστοιχηθεί σε μία AFxy κλάση (2 –3 διαφορετικοί PHBs).

Τα LSPs που έχουν στηθεί υπό αυτές τις συνθήκες καλούνται L-LSPs, όπου το L προέρχεται από το Label.



Στην περίπτωση που υπάρχει MPLS πάνω από ATM η υποστήριξη διαφοροποιημένων υπηρεσιών θα πρέπει να κάνει αντιστοίχηση των κλάσεων υπηρεσίας στις κλάσεις υπηρεσίας του ATM.Οι διαφοροποιημένες υπηρεσιών αντιστοιχούν κυρίως στις κλάσεις υπηρεσίας ABR και nrt-VBR του ATM. Αυτό είναι λογικό γιατί στις διαφοροποιημένες υπηρεσίες δεν υπάρχει αυστηρή εγγύηση της υπηρεσίας, π.χ. την καθυστέρηση που θα έχουν τα πακέτα του. Για την υποστήριξη κίνησης AF και διαχωρισμού των επιπέδων drop preference (τιμή y) χρησιμοποιείται το πεδίου CLP του ATM header για να προσδιορίσει όμως δύο μόνο επίπεδα.



5.8.1.3 Συγκριση E-LSP και L-LSP

E-LSP	L-LSP
Το PHB προσδιορίζεται από το πεδίο Exp	Το PHB προσδιορίζεται από την ετικέτα μετά την ολοκλήρωση των LSP και το πεδίο Exp/CLP
Δεν απαιτείται κάποια τροποποίηση των μηχανισμών δέσμευσης ετικετών	Απαιτεί επέκταση των μηχανισμών δέσμευσης ετικετών ώστε να γίνει η σήμανση του κατά την εγκαθίδρυση
Συγκροτείται μία αντιστοίχηση Exp -> PHB	Η αντιστοίχηση Label -> PHB γίνεται μέσω σήμανσης Επιπλέον αντιστοίχηση Exp/CLP -> PHB για AF
Απαιτείται ετικέτα της μορφής 'shim' (Σχήμα 7.), δεν έχει δηλαδή εφαρμογή σε ATM, Frame Relay	Είναι κατάλληλο για όλους τους τύπους
Επιτρέπει μέχρι οκτώ PHBs σε κάθε LSP	Ένας PHB για κάθε LSP, για κίνηση AF 2 –3 διαφορετικοί PHBs σε ένα LSP.

Κεφάλαιο 6
VPN Βασισμένα στην MPLS Τεχνολογία

Εισαγωγή

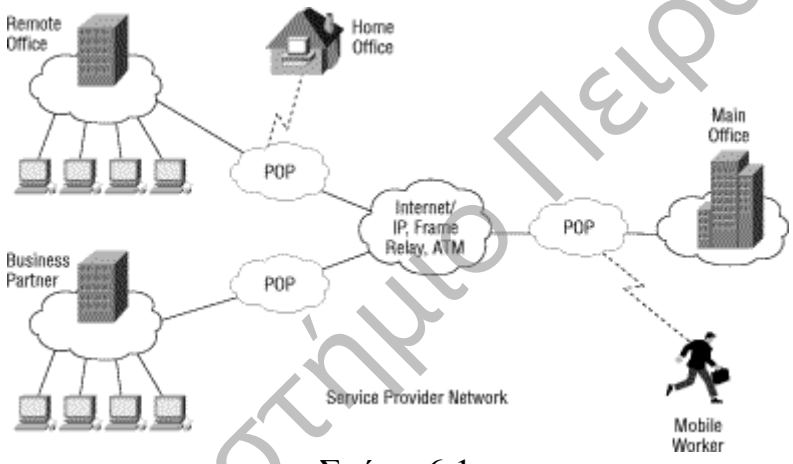
Η εξάπλωση της δικτυωμένης οικονομίας έχει επιφέρει ουσιαστικές αλλαγές στον τρόπο λειτουργίας των επιχειρήσεων. Οι ομάδες εργασίας δεν ορίζονται πλέον τόσο από τον τόπο στον οποίο δουλεύουνε αλλά από την αποδοτικότητά τους στο έργο με το οποίο ασχολούνται. Ο ανταγωνισμός σε πολλές βιομηχανίες έχει οδηγήσει σε συμμαχίες και συνεταιρισμούς μεταξύ των επιχειρήσεων που όσο εκτεταμένες και αν είναι πάντα προβάλλονται ενιαία όταν έρχονται σε συναλλαγές με τους πελάτες τους. Αυτές οι εξελίξεις έχουν μεν αυξήσει την παραγωγικότητα και την κερδοφορία πολλών επιχειρήσεων, έχουν όμως ταυτόχρονα δημιουργήσει νέες απαιτήσεις για τις επιχειρήσεις αυτές. Ένα δίκτυο που επικεντρώνεται στο να συνδέει απλά σταθερά σημεία των συνεργαζόμενων επιχειρήσεων δεν είναι πλέον εφικτό για πολλές επιχειρήσεις. Οι απομακρυσμένοι χρήστες του δικτύου των επιχειρήσεων, όπως οι τηλε-εργαζόμενοι ή "μαχητές του δρόμου" και άλλοι εξωτερικοί συνεργάτες απαιτούν πλέον πρόσβαση στους πόρους του δικτύου της επιχείρησης. Το κλασικό WAN πρέπει λοιπόν να επεκταθεί ώστε να συμπεριλάβει και αυτού του τύπου τους εργαζόμενους. Συνεπώς ,πολλές επιχειρήσεις στρέφονται προς τα δίκτυα VPN για να συμπληρώσουν την υπάρχουσα WAN υποδομή τους.

Σήμερα σχεδόν το 100% των επιχειρήσεων συμπληρώνουν την υποδομή των WAN τους με VPNs. Από την οπτική γωνιά της αρχιτεκτονικής του δικτύου το κίνητρο είναι προφανές—τα VPN μπορούν να ανταποκριθούν καλύτερα στις σημερινές ποικίλες ανάγκες σύνδεσης. Τα πλεονεκτήματα των VPN είναι ορατά και στη τελική ανάλυση. Τα VPN είναι λιγότερο δαπανηρά στη λειτουργία τους από τα ιδιωτικά δίκτυα από άποψη διαχείρισης, εύρους ζώνης και κεφαλαίου. Κατά συνέπεια ο χρόνος απόσβεσης ενός VPN μετράται συνήθως σε μήνες αντί σε χρόνια. Ίσως ,το πιο σημαντικό πλεονέκτημα από όλα να είναι το ότι τα VPN επιτρέπουν στις επιχειρήσεις να επικεντρωθούν στο αντικείμενο ενασχόλησής τους και όχι στο πώς να κρατήσουν το δίκτυό τους ζωντανό και αποδοτικό.

6.1 Τι είναι τα VPN

Έχει αναπτυχθεί μία αρκετά μεγάλη φιλολογία γύρω από το τι είναι τα VPN , ποια η λειτουργία τους και ποια η θέση τους στην αρχιτεκτονική των δικτύων. Για να το θέσουμε απλά το VPN είναι ένα δίκτυο επιχείρησης ανεπτυγμένο σε μία διανεμημένη υποδομή και έχει την ίδια ασφάλεια, διαχείριση

και υφίσταται την ίδια πολιτική σε όλο το μήκος του σαν να επρόκειτο για ιδιωτικό δίκτυο. Τα VPN είναι μία εναλλακτική λύση της υποδομής που παρέχουν τα WAN και που αντικαθιστούν ή επαυξάνουν τα υπάρχοντα ιδιωτικά δίκτυα που χρησιμοποιούν μισθωμένες γραμμές ή Frame Relay/ATM δίκτυα που ανήκουν στην επιχείρηση. Τα VPN δεν έχουν άλλες απαιτήσεις από αυτές των WAN όπως υποστήριξη πολλαπλών πρωτοκόλλων, υψηλή αξιοπιστία και εκτεταμένη διαβάθμιση, απλά ικανοποιούν αυτές τις απαιτήσεις λιγότερο δαπανηρά. Ένα VPN μπορεί να αξιοποιήσει τις πιο γνωστές τεχνολογίες μεταφοράς που υπάρχουν σήμερα : το δημόσιο Internet, IP backbones διαφόρων παροχέων υπηρεσιών όπως επίσης και τα Frame Relay και ATM δίκτυά τους. Η λειτουργικότητα του VPN καθορίζεται κυρίως από τον εξοπλισμό που είναι ανεπτυγμένος στο δίκτυο και την ολοκλήρωση των χαρακτηριστικών του WAN και όχι από το πρωτόκολλο μεταφοράς που αυτό χρησιμοποιεί.



Σχήμα 6.1

Τα VPN χωρίζονται σε τρεις κατηγορίες: απομακρυσμένης πρόσβασης ,intranets και extranets.

Τα remote access VPNs συνδέουν τηλεργαζόμενους, κινούμενους χρήστες ή ακόμα και μικρότερα απομακρυσμένα γραφεία με περιορισμένη κίνηση από και προς το WAN της επιχείρησης και των συλλογικών υπολογιστικών της πόρων.

Τα intranet VPNs συνδέουν σταθερά σημεία , παρακλάδια και γραφεία σπιτιών με το WAN της επιχείρησης.

Τα extranet VPNs επεκτείνουν την περιορισμένη πρόσβαση στους υπολογιστικούς πόρους της επιχείρησης στους διαφόρους συνεργάτες της που μπορεί να είναι προμηθευτές ή πελάτες επιτρέποντας πρόσβαση σε διαμοιράσιμη πληροφορία.

Κάθε τύπος VPN έχει διαφορετικά θέματα ασφάλειας και ποιότητας παρεχόμενων υπηρεσιών να αντιμετωπίσει.

6.2 Λόγοι Επιλογής των VPN από Επιχειρήσεις

Τα VPN προσφέρουν πολλά πλεονεκτήματα σε σχέση με τα παλιά – παραδοσιακά δίκτυα μισθωμένων γραμμών. Μερικά από αυτά είναι :

- **Μικρότερο κόστος από αυτό των ιδιωτικών δικτύων** : το ολικό κόστος ιδιοκτησίας μειώνεται μέσο μικρότερου κόστους του εύρους ζώνης, backbone εξοπλισμού και των λειτουργικών αναγκών—σύμφωνα με μελέτη της Infonetics (εταιρία διαχείρισης δικτύων και παροχής συμβουλευτικών υπηρεσιών) το κόστος LAN-to-LAN σύνδεσης μειώνεται κατά 20% με 40% σε σχέση με αυτό των δικτύων μισθωμένων γραμμών. Επιπλέον η αντίστοιχη μείωση του κόστους για απομακρυσμένη πρόσβαση πέφτει κατά 60% με 80%.

- **Ενίσχυση της Οικονομίας του Internet** : Τα VPN είναι αρχιτεκτονικές δικτύωσης περισσότερο ευέλικτες και διαβαθμισμένες από τα κλασικά WAN δίνοντας έτσι την ευχέρεια στις επιχειρήσεις να επεκτείνουν τη διασύνδεσή τους εύκολα και γρήγορα επιτυγχάνοντας σύνδεση και αποσύνδεση απομακρυσμένων γραφείων , σημείων σε όλη την υδρόγειο , τηλεργαζόμενους, περιπλανώμενους κινούμενους χρήστες και εξωτερικούς συνεργάτες κατά τις επιταγές και τις ανάγκες της επιχείρησης.

- **Μειωμένα έξοδα διαχείρισης** συγκρινόμενα με αυτά της ιδιοκτησίας και λειτουργίας ιδιωτικού δικτύου. Οι επιχειρήσεις μπορούν να αναθέσουν τη λειτουργία μέρους ή και όλου του WAN τους σε κάποιον παροχέα υπηρεσιών έτσι ώστε να επικεντρωθούν στη δουλειά τους και να μην διαχειρίζονται το WAN δίκτυο ή αυτό που παρέχει δυνατότητα απομακρυσμένης πρόσβασης. Ενημερώνεται

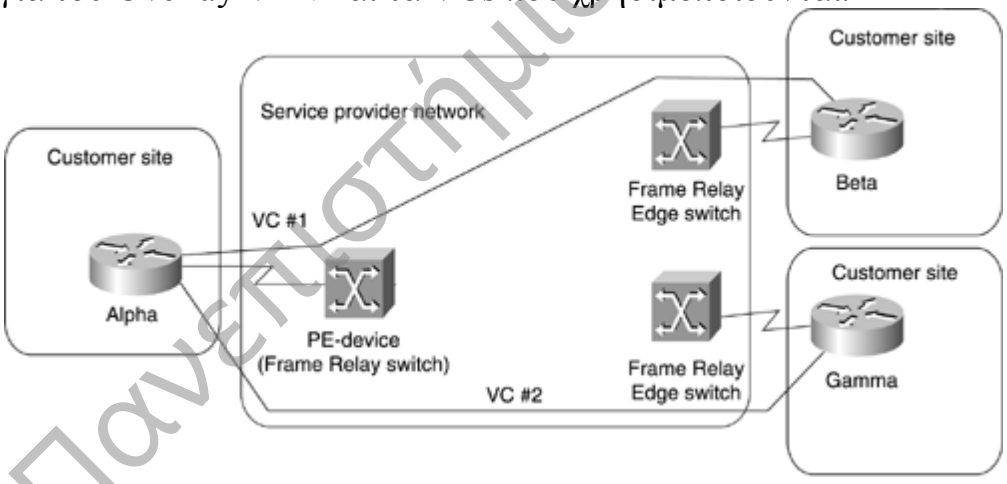
- **Απλοποίηση των δικτυακών τοπολογιών** μειώνοντας έτσι το φόρτο διαχείρισης: η χρησιμοποίηση ενός IP backbone μειώνει δραστικά τα μόνιμα εικονικά κυκλώματα (PVCs) που σχετίζονται με πρωτόκολλα σύνδεσης όπως τα Frame Relay και ATM δημιουργώντας μια εντελώς μπερδεμένη δικτυακή τοπολογία την ίδια στιγμή που μειώνουν τη συνθετότητα και το κόστος του δικτύου.

6.3 Τα μοντέλα Επικαλυπτόμενου VPN & Ομότιμων Οντοτήτων

Δύο μοντέλα υλοποίησης VPN έχουν ευρεία χρήση
• **Το μοντέλο επικάλυψης (Overlay Model)**, όπου ο πάροχος υπηρεσίας εξασφαλίζει εξομοιούμενες μισθωμένες γραμμές στο πελάτη.
• **Το peer-to-peer μοντέλο**, όπου ο πάροχος υπηρεσίας και ο πελάτης ανταλλάσσουν πληροφορία διαδρομής του Επιπέδου 3 και ο πάροχος μεταδίδει τα δεδομένα μεταξύ των τοποθεσιών του πελάτη από το βέλτιστο κατά περίπτωση μονοπάτι μεταξύ των τοποθεσιών, χωρίς την ανάμιξη του πελάτη.

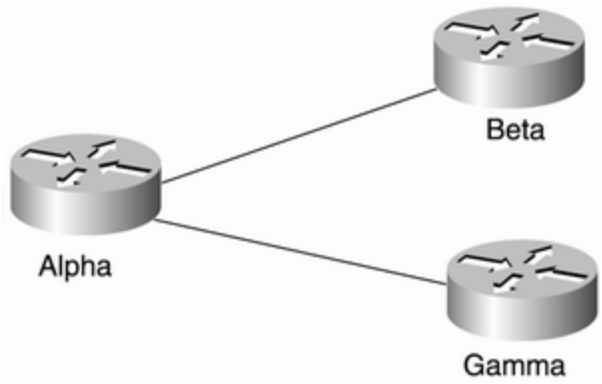
6.3.1 Το Επικαλυπτόμενο (Overlay) VPN Μοντέλο

Το VPN μοντέλο επικάλυψης είναι από τα πιο απλά επειδή εξασφαλίζει πολύ καθαρή διάκριση ανάμεσα στις ευθύνες του πελάτη και του παρόχου υπηρεσίας. Ο πάροχος υπηρεσίας προμηθεύει τον πελάτη με μια ομάδα από εξομοιούμενες μισθωμένες γραμμές. Αυτές οι γραμμές λέγονται VCs και μπορεί να είναι είτε μόνιμα διαθέσιμες ή εγκατεστημένες. Το Σχήμα 6.2 δείχνει την τοπολογία του Overlay VPN και τα VCs που χρησιμοποιούνται.



Σχήμα 6.2 παράδειγμα Overlay VPN δικτύου

Ο πελάτης εγκαθιστά μια router-to-router επικοινωνία ανάμεσα στις CPE συσκευές στα VCs που είναι εφοδιασμένο από τον πάροχο υπηρεσίας. Στη συνέχεια το πρωτόκολλο δρομολόγησης δεδομένων ανταλλάσσει πληροφορία μεταξύ των συσκευών του παρόχου, και ο πάροχος υπηρεσίας δεν γνωρίζει τίποτα για την εσωτερική δομή του δικτύου του πελάτη. Το Σχήμα 6.3 δείχνει την τοπολογία του VPN δικτύου. Οι QoS εγγυήσεις του VPN μοντέλου συνήθως εκφράζονται σε όρους εγγυημένου εύρους ζώνης ανά VC (Committed Information Rate – CIR) και σε μέγιστο εύρος ζώνης διαθέσιμο σε συγκεκριμένο VC (Peak Committed Information Rate – PIR).



Σχήμα 6.3
Η δρομολόγηση στο δείγμα του Overlay VPN δικτύου

Το δεσμευμένο εγγυημένο εύρος ζώνης εξαρτάται από την στρατηγική υπερδέσμευσης των υπαρχόντων συνδέσεων του παρόχου υπηρεσίας. Αυτό σημαίνει ότι ο δεσμευμένος ρυθμός δεν είναι πρακτικά εγγυημένος αν και ο πάροχος υπηρεσίας μπορεί να εγγυηθεί ένα ελάχιστο ρυθμό πληροφορίας (Minimum Information Rate – MIR) που δεσμεύεται αποτελεσματικά διαμέσου της υποδομής του επιπέδου δικτύου.

Τα Overlay VPN μπορούν να υλοποιηθούν με χρήση διαφόρων Switched WAN τεχνολογιών επιπέδου 2, συμπεριλαμβανομένων των X.25,frame relay, SMDN ή ATM. Τα τελευταία χρόνια στα Overlay VPN έχουν επίσης εφαρμοστεί με χρήση IP-to-IP tunneling, είτε μαζί σε ιδιωτικά IP backbones είτε πάνω στο δημόσιο ιστό (internet). Οι πιο κοινές IP-to-IP Tunneling τεχνολογίες είναι το Generic Route Encapsulation (GRE) και το IP Encryption.

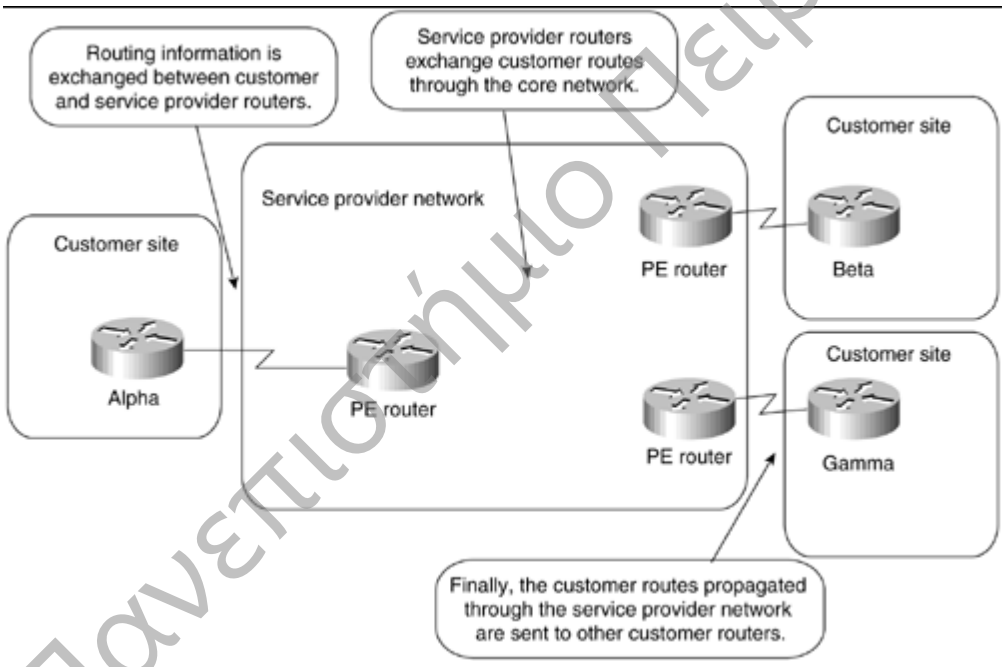
Αν και είναι σχετικά εύκολο να καταλάβει κανείς και να υλοποιήσει το Overlay VPN μοντέλο, υπάρχουν μια σειρά από μειονεκτήματα όπως:

• Πρόβλημα διαχειρισιμότητας. Είναι επαρκές για μη πλεονάζουσες διατάξεις (nonredundant) με λίγες κεντρικές τοποθεσίες και πολλές απομακρυσμένες, αλλά γίνεται υπερβολικά δύσκολο στη διαχείριση σε μια περισσότερο πολύπλοκη & σύνθετη διάταξη.
• Μερική γνώση & πρόβλεψη κίνησης. Η σωστή δημιουργία των VC με τις απαραίτητες χωρητικότητες, απαιτεί λεπτομερή γνώση της site-to-site κίνησης που είναι συνήθως δεν είναι διαθέσιμη κατά τη δημιουργία των VCs.
• Γραμμικό κόστος ανά αριθμό διασυνδέσεων για κάνε νέο κόμβο. Το κόστος εφαρμογής μεγαλώνει γραμμικά σε σχέση με τον αριθμό από point-to-point συνδέσεις στο δίκτυο, όχι με τον αριθμό των νέων δικτυακών τοποθεσιών που μπαίνουν στο VPN.
• Υποστήριξη πολύπλοκη επιχειρηματικού μοντέλου από τους παροχείς δικτυακών υπηρεσιών. Τέλος αλλά όχι λιγότερα σημαντικό αποτελεί το γεγονός

ότι το Overlay VPN μοντέλο, όταν εφαρμόζεται με Layer 2 τεχνολογίες, εισάγει ένα ακόμα ενδιάμεσο επίπεδο πολυπλοκότητας στο επιχειρηματικό μοντέλο παροχής υπηρεσιών δικτύου το οποίο είναι περισσότερο προσανατολισμένο στην παροχή υπηρεσιών επιπέδου 3 (IP-based), έτσι αυξάνεται το κόστος απόκτησης και λειτουργίας ενός τέτοιου δικτύου.

6.3.2 Το VPN Μοντέλο των ομότιμων (Peer-to-peer) οντοτήτων

Το Peer-to-Peer VPN μοντέλο εισήχθη τα τελευταία χρόνια για να ανακουφίσει τα μειονεκτήματα του Overlay VPN μοντέλου. ΣτοP-P μοντέλο η Provider Edge (PE) συσκευή είναι ένας δρομολογητής (PE router) που ανταλλάσσει πληροφορία δρομολόγησης (routing information) με τον CPE δρομολογητή. Το παρακάτω σχήμα δείχνει ένα παράδειγμα P-P VPN.



Σχήμα 6.4 παράδειγμα Peer-to-Peer VPN

Το P-P παρέχει κάποια πλεονεκτήματα σε σχέση με το παραδοσιακό Overlay μοντέλο :

• Η δρομολόγηση (από την πλευρά του πελάτη) γίνεται ιδιαίτερα απλή καθώς ο δρομολογητής του πελάτη ανταλλάσσει πληροφορία δρομολόγησης με μόνο ένα (ή λίγους) PE δρομολογητή, ενώ αντιθέτως, στο Overlay VPN δίκτυο ο αριθμός των γειτονικών δρομολογητών μπορεί να αυξηθεί σε έναν μεγάλο αριθμό.

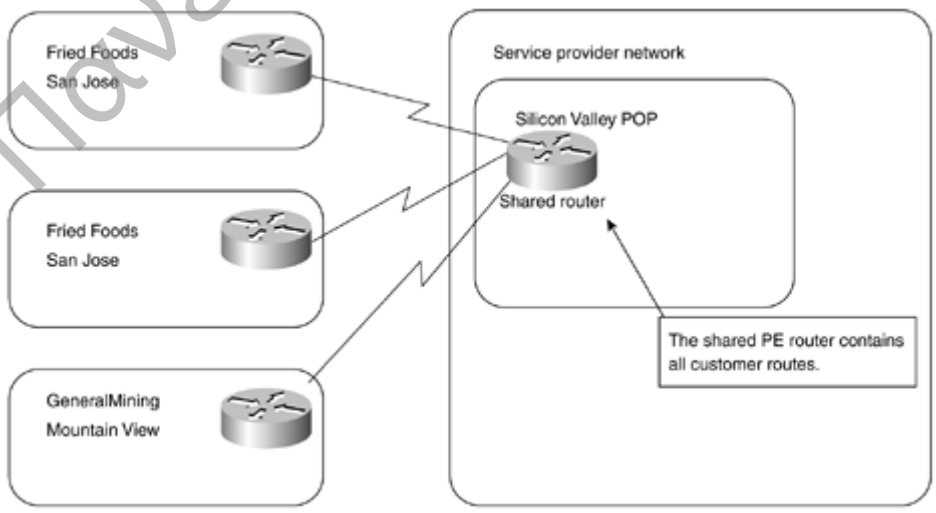
• Η δρομολόγηση μεταξύ των τοποθεσιών του πελάτη είναι πάντα η βέλτιστη, αφού οι δρομολογητές του παρόχου γνωρίζουν την τοπολογία του δικτύου του

πελάτη και έτσι μπορούν να εγκαταστήσουν το καλύτερο μονοπάτι δρομολόγησης ανάμεσα στις υπηρεσίες.
• Η ανάθεση εύρους ζώνης είναι απλούστερη επειδή ο πελάτης μπορεί να καθορίσει μόνο το εσωτερικό και εξωτερικό εύρος ζώνης Committed Access Rate (CAR) και Committed Delivery Rate (CDR) και όχι το ακριβές site-to-site προφίλ κίνησης.
• Η πρόσθεση μια καινούργιας τοποθεσίας είναι απλούστερη επειδή ο πάροχος υπηρεσίας δημιουργεί μόνο μια επιπρόσθετη τοποθεσία και αλλάζει τους πίνακες δρομολόγησης στον συνδεόμενο PE. Αντίθετα στο Overlay VPN μοντέλο ο πάροχος υπηρεσίας πρέπει να παράσχει μια ολόκληρη ομάδα από VCs που να συνδέει τη νέα τοποθεσία σε όλες τις άλλες τοποθεσίες του πελάτη VPN.

6.3.2.1 Shared-Router Approach P-P VPN Model

Στη προσέγγιση του διαμοιραζόμενου δρομολογητή (shared router), πολλαπλοί πελάτες μπορεί να είναι συνδεδεμένοι στον ίδιο PE δρομολογητή. Οι λίστες πρόσβασης πρέπει να είναι διαμορφωμένες για κάθε VPN PE-to-CE διεπιφάνεια πάνω στον PE δρομολογητή έτσι ώστε να κατοχυρώνεται ο διαχωρισμός μεταξύ των VPN πελατών, και να εμποδίζεται ένας VPN πελάτης να παραβιάζει ένα άλλο VPN δίκτυο ή να εκτελεί μια επίθεση άρνησης υπηρεσίας σε έναν άλλο VPN πελάτη. Το Σχήμα 6.5 απεικονίζει ένα παράδειγμα διαμοιραζόμενου δρομολογητή.

Για να κατοχυρώσει το διαχωρισμό μεταξύ των πελατών η διάταξη θα πρέπει να έχει διαμορφωθεί κατάλληλα η λίστα πρόσβασης του POP δρομολογητή στο Σχήμα 6.5

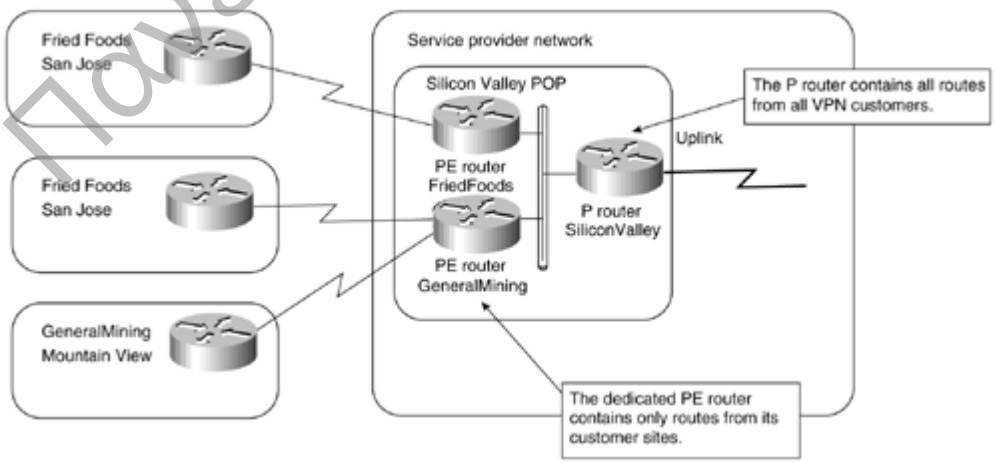


Σχήμα 6.5 Peer-to-Peer VPN μοντέλο: Διάταξη διαμοιραζόμενου δρομολογητή

6.3.2.2 Dedicated-router Approach P-P VPN Model

Στην προσέγγιση του αποκλειστικού δρομολογητή (dedicated router) για το P-P μοντέλο κάθε VPN πελάτης έχει τους δικούς του αποκλειστικούς PE δρομολογητές και, με αυτόν τον τρόπο, έχει πρόσβαση μόνο στους δρομολογητές που εμπεριέχονται μέσα στο routing table αυτού του δρομολογητή. Το μοντέλο αποκλειστικού δρομολογητή χρησιμοποιεί πρωτόκολλα δρομολόγησης για να δημιουργήσει πίνακες μεταγωγής ανά VPN στους PE δρομολογητές. Οι πίνακες δρομολόγησης στους PE δρομολογητές περιέχουν τους δρομολογητές που γνωστοποιούνται από τον VPN πελάτη που είναι συνδεδεμένος σε αυτούς, έχοντας σαν αποτέλεσμα ένα σχεδόν τέλεια απομονωμένο μεταξύ των VPN πελατών. Η μεταγωγή στο μοντέλο αποκλειστικού δρομολογητή μπορεί να υλοποιηθεί όπως παρακάτω:

• Κάθε πρωτόκολλο μεταγωγής «τρέχει» μεταξύ του PE δρομολογητή και του CE δρομολογητή.
• Το BGP «τρέχει» μεταξύ του PE και του P
• Ο PE ανακατανέμει τους δρομολογητές που παρελήφθησαν από τον CE στον BGP, σημειωμένοι με τον πελάτη ID (BGP «κοινωνία»),και μεταδίδει τις διαδρομές στους P. Οι P με αυτόν τον τρόπο συμπεριλαμβάνουν όλες τις διαδρομές από όλους τους δρομολογητές
• Οι P-δρομολογητές διαδίδουν μόνο διαδρομές με την κατάλληλη BGP «κοινωνία» στους PE-δρομολογητές. Οι PE-δρομολογητές με αυτόν τον τρόπο παραλαμβάνουν μόνο τις διαδρομές που προέρχονται από τους PE-δρομολογητές στο δικό τους VPN σχετικά τμήματα του PE-router και της διάταξης P-router για τον πάροχο υπηρεσίας Point- of- Presence (POP) που απεικονίζονται στο Σχήμα 6.6



Σχήμα 6.6 Peer-to-Peer VPN: Γιάταξη εξειδικευμένου Γρομολογητή

6.3.2.3 Σύγκριση των Peer-to-Peer Μοντέλων

Όπως πολύ εύκολα μπορούμε να συμπεράνουμε από την προηγούμενη περιγραφή, το μοντέλο διαμοιραζόμενου δρομολογητή είναι αρκετά δύσκολο να διατηρηθεί επειδή αυτό απαιτεί την ανάπτυξη της αποτελεσματικότητας μακριών και πολύπλοκων λιστών πρόσβασης σε κάθε σχεδόν αλληλεπίδραση δρομολογητή. Η προσέγγιση της αποκλειστικής δρομολόγησης, αν και απλούστερη στη διαμόρφωση και διατήρηση, γίνεται πολύ ακριβή για τον πάροχο υπηρεσίας, όταν προσπαθεί να εξυπηρετήσει έναν μεγάλο αριθμό πελατών με γεωγραφικά διασκορπισμένες υπηρεσίες.
Και τα δύο P-P μοντέλα εμφανίζουν κάποια κοινά μειονεκτήματα που εμποδίζουν την ευρεία διάδοση τους.
• Όλοι οι πελάτες μοιράζονται την ίδια περιοχή IP διευθύνσεων, εμποδίζοντας έτσι τους πελάτες στο να αναπτύξουν ιδιωτικές IP διευθύνσεις. Έτσι οι πελάτες πρέπει να χρησιμοποιήσουν είτε κοινές IP διευθύνσεις ή ιδιωτικές IP διευθύνσεις διανεμημένες σε αυτούς από τον πάροχο υπηρεσίας.
• Οι πελάτες δεν μπορούν να εισάγουν τη δική τους δρομολόγηση πακέτων μέσα στο VPN τους. Αυτός ο περιορισμός εμποδίζει τη βελτιστοποίηση της δρομολόγησης και εμποδίζει τους πελάτες από το να έχουν πρόσβαση στο Internet και από άλλο πάροχο υπηρεσίας δικτύου (ISP).
Επιπρόσθετα στα δύο προηγούμενα μειονεκτήματα, το μοντέλο διαμοιραζόμένου δρομολογητή υποφέρει από επιπρόσθετη πολυπλοκότητα, όταν οι πελάτες χρησιμοποιούν διαφορετικά πρωτόκολλα δρομολόγησης (RIP, RIPv2, BEP, IS-IS).

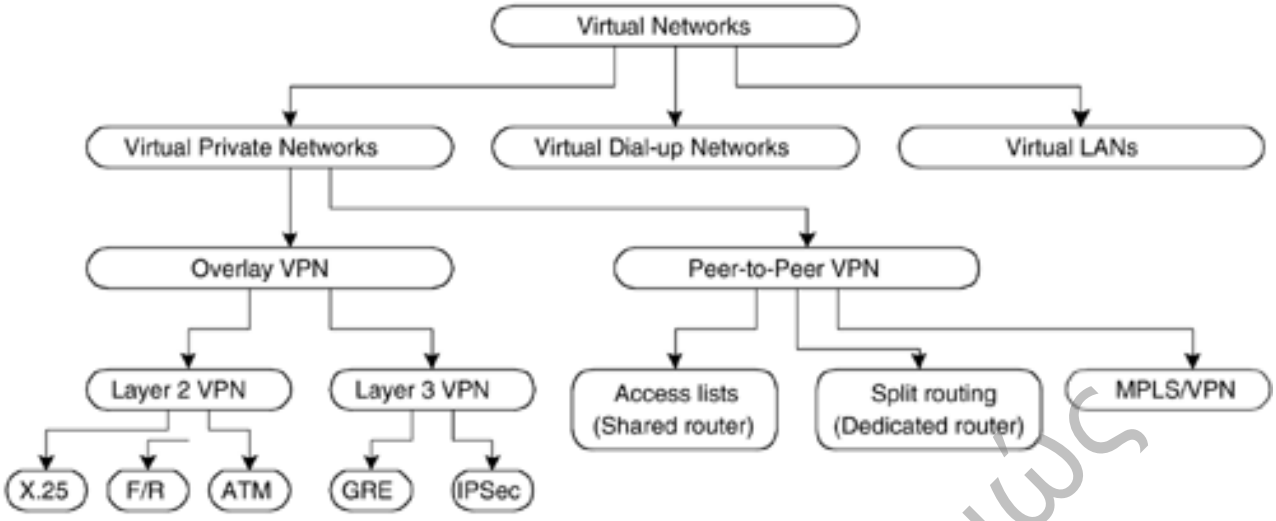
6.4 Τυπικές τοπολογίες VPN

Η VPN τοπολογία που απαιτείται από έναν οργανισμό πρέπει να καλύπτει της απαιτήσεις της επιχείρησης. Παρόλα αυτά, υπάρχουν διάφορες πολύ γνωστές τοπολογίες που αξίζει να αναφερθούν. Οι ίδιες τοπολογίες μπορούν να λύνουν μια ποικιλία από διαφορετικά θέματα επιχείρησης ανάλογα με τις απαιτήσεις ης αγοράς αλλά και του επιχειρηματικού κλάδου στον οποίο δραστηριοποιούνται.
Οι VPN τοπολογίες που θα περιγραφούν μπορούν να διαιρεθούν σε τρεις μεγάλες κατηγορίες.
• Τοπολογίες επηρεασμένες από το Overlay VPN μοντέλο. Συγκεκριμένα προκειται για τις:
Hub and Spoke τοπολογίες, partial ή full mesh τοπολογία και hybrid τοπολογία.
• Extranet τοπολογίες, και συγκεκριμένα τα any-to-any Extranet και Central Services Extranet

• Ειδικού σκοπού (Special Purpose) τοπολογίες, όπως οι VPDN backbone και Manager Network τοπολογία

6.5 Κατηγοριοποίηση VPN

Τα VPN γίνεται να κατηγοριοποιηθούν με μια σειρά από κριτήρια. Η ευρύτερη τεχνολογική ιεράρχηση είναι βασισμένη πάνω στο τρόπο που η πληροφορία δρομολόγησης ανταλλάσσεται μέσα στο VPN. Στο peer-to-peer VPN μοντέλο η πληροφορία δρομολόγησης του πελάτη ανταλλάσσεται μεταξύ των δρομολογητών του πελάτη και των δρομολογητών του προμηθευτή υπηρεσίας. Στο Overlay VPN μοντέλο ο προμηθευτής υπηρεσίας εξασφαλίζει μόνο τα VCs (λογικές μισθωμένες γραμμές) και η πληροφορία δρομολόγησης ανταλλάσσεται επακριβώς μεταξύ των ακριανών δρομολογητών του πελάτη. Τα δυο μοντέλα μπορεί να είναι συνδυασμένα σε ένα μεγάλο δίκτυο παρόχου υπηρεσίας: Το Peer-to-Peer ίσως να χρησιμοποιεί Overlay VPN μοντέλο στα τμήματα πρόσβασης (για παράδειγμα, οι πελάτες συνδέονται στους δρομολογητές ακριανού παρόχου μέσα από το Frame Relay) ή στο πυρήνα του.Η πιο λεπτομερή VPN ιεράρχηση (απεικονίζεται στο Σχήμα 6.7) εστιάζει πάνω στη υποκείμενη τεχνολογία που χρησιμοποιείται στα πακέτα μεταφοράς του Επιπέδου 3 πάνω στο VPN. Το Overlay VPN μοντέλο μπορεί να υλοποιηθεί με Επιπέδου 2 WAN τεχνολογίες μεταγωγής (X.25, SMDN, Frame Relay, ATM) ή tunneling τεχνολογίες Επιπέδου 3 (IP-over-IP,IPSec). Το Peer-to-Peer VPN μοντέλο μπορεί να υλοποιείται παραδοσιακά με χρήση πολύπλοκων τεχνικών δρομολόγησης ή IP λίστες εισόδου, έχοντας και τα δύο έναν αριθμό από ελαττώματα που έχουν περιγραφεί στην παράγραφο «Peer-to-Peer VPN μοντέλο». Το MPLS based VPN συμπληρώνει τις αδυναμίες άλλων Peer-to-Peer VPN τεχνολογιών. Αφήνοντας τους παρόχους υπηρεσίας να συνδυάζουν τα προτερήματα του Peer-to-Peer μοντέλου (απλούστερη δρομολόγηση, απλούστερη εφαρμογή των απαιτήσεων του πελάτη) με την ασφάλεια και την απομόνωση που κληρονομούνται από το Overlay VPN μοντέλο.



Σχήμα 6.7

6.6 Υπηρεσίες των MPLS VPNs

Τα MPLS VPNs επιτρέπουν στους παροχείς υπηρεσιών να διαθέτουν μία ποικιλία προστιθέμενων υπηρεσιών όπως:

• Μη προσανατολισμένες στην σύνδεση – ασυνδεσμικές - υπηρεσίες (Connectionless Service): ένα τεχνικό πλεονέκτημα των MPLS VPN είναι ότι είναι ασυνδεσμικά, που σημαίνει ότι δεν χρειάζεται εκ των προτέρων εγκατάσταση καναλιού επικοινωνίας ανάμεσα σε δύο σημεία. Αυτό έρχεται σε πλήρη ευθυγράμμιση με την λογική λειτουργίας του ίδιου του internet το οποίο βασίζεται στο πρωτόκολλο TCP/IP που είναι επίσης ασυνδεσμικό.
Έτσι αποφεύγεται επιπλέον πολυπλοκότητα στην λειτουργία του δικτύου.

• Κεντρικός έλεγχος υπηρεσιών (Centralized service): τα VPNs δίνουν την δυνατότητα στους παροχείς υπηρεσιών να παρέχουν αρκετές υπηρεσίες σε ομάδες χρηστών. Οι χρήστες μπορούν να χρησιμοποιούν αυτές τις υπηρεσίες, ιδιωτικώς, μέσα στα δικά τους intranets και extranets. Επειδή τα MPLS VPNs «φαίνονται» σαν ιδιωτικά intranets μπορούν να χρησιμοποιήσουν και τις νέες IP υπηρεσίες όπως:

• πολυεκπομπή
• ποιότητας υπηρεσιών (QoS)
• τηλεφωνία εντός του VPN
• φύλαξη ιστοσελίδων (Web hosting)

Πολλές από αυτές τις υπηρεσίες μπορούν ακόμα και να συνδυαστούν μεταξύ τους ώστε να ικανοποιήσουν και τις πιο ιδιαίτερες ανάγκες των χρηστών.

• Δυνατότητα αναβάθμισης (Scalability): σε αντίθεση με τα άλλα είδη VPN (Frame Relay,ATM κλπ.) που χρησιμοποιούν προσανατολισμένες στην σύνδεση υπηρεσίες, η ασυνδεσμικότητα του MPLS δίνει την δυνατότητα της εύκολης αναβάθμισης. Τα MPLS χρησιμοποιούν το λεγόμενο ομότιμο (peer) μοντέλο για να πετύχουν αυτήν την αναβάθμιση. Σύμφωνα με αυτό, το site ενός πελάτη το μόνο που χρειάζεται είναι να «συνδεθεί» (peer) με την άκρη ενός δρομολογητή του παροχέα (provider edge – PE – router) και όχι με όλους τους υπόλοιπους δρομολογητές που είναι μέλη του VPN. Η ασυνδεσμική του αρχιτεκτονική επιτρέπει τέτοιου είδους συνδέσεις χωρίς την ανάγκη δημιουργίας κρυπτογραφικών tunnels ή μόνιμων εικονικών κυκλωμάτων VCs.

Επίσης την δυνατότητα αναβάθμισης διευκολύνει και ο διαχωρισμός των δρομολογητές του παροχέα σε δύο κατηγορίες

• PE δρομολογητής: είναι αυτοί που συντηρούν τα VPN δρομολόγια στα VPN που είναι μέλος ο δρομολογητής

• P δρομολογητής: είναι αυτοί που δεν συντηρούν VPN δρομολόγια

• Ασφάλεια (Security): τα MPLS προσφέρουν το ίδιο επίπεδο ασφάλειας με τα προσανατολισμένα στην σύνδεση VPNs. Πακέτα συγκεκριμένου VPN δεν μπορούν χωρίς λόγο να βρεθούν σε άλλο VPN.

Η ασφάλεια παρέχεται

• από την πλευρά του παροχέα, ο οποίος εξασφαλίζει τα πακέτα ενός πελάτη να πηγαίνουν στο σωστό VPN

• από το δίκτυο κορμού (backbone) του παροχέα: η κυκλοφορία των VPN πακέτων γίνεται ξέχωρα από άλλα πακέτα. Κάθε προσπάθεια παράνομης προσπέλασης αυτών είναι σχεδόν αδύνατη, διότι είναι πακέτα IP που φέρουν μοναδική ετικέτα του VPN δικτύου για το οποίο προορίζονται.

• Εύκολη δημιουργία (Easy Creation): για να γίνει πλήρη εκμετάλλευση της τεχνολογίας των VPN, πρέπει να παρέχεται ευκολία στους πελάτες να δημιουργήσουν νέα VPN και κοινότητες χρηστών. Εξαιτίας της ασυνδεσμικότητας των MPLS VPN δεν χρειάζονται συγκεκριμένες σημείου προς σημείο αντιστοιχήσεις συνδέσεων και τοπολογιών. Μπορούμε να προσθέσουμε εύκολα νέα sites στα intranets και στα extranets του VPN καθώς και να δημιουργήσουμε κλειστές ομάδες χρηστών. Έτσι δίνεται η δυνατότητα σε ένα site να είναι μέλος σε πολλά VPN αυξάνοντας την ευελιξία στην δημιουργία intranets και extranets.

• Ευέλικτη διευθυνσιοδότηση (Flexible Addressing): για να αυξήσουμε την προσπελασιμότητα ενός VPN, πελάτες ενός παροχέα υπηρεσιών μπορούν να

σχεδιάσουν το δικό τους χώρο διευθύνσεων ανεξάρτητα από άλλους πελάτες του ίδιου παροχέα. Είναι αρκετοί αυτοί που χρησιμοποιούν τις δικές τους ιδιωτικές διευθύνσεις και δεν θέλουν να σπαταλήσουν χρόνο και χρήμα για να τις μετατρέψουν σε δημόσιες IP διευθύνσεις. Τα MPLS επιτρέπουν στους πελάτες να συνεχίσουν να χρησιμοποιούν τον δικό τους χώρο διευθύνσεων χωρίς να γίνει μετάφραση αυτών (NAT) παρέχοντας έτσι μια δημόσια και μια ιδιωτική προβολή των διευθύνσεων. Μετάφραση γίνεται μόνο όταν δύο VPN με επικαλυπτόμενες διευθύνσεις θέλουν να επικοινωνήσουν. Συνοψίζοντας, στα MPLS VPNs οι πελάτες χρησιμοποιούν άφοβα τις δικές τους ιδιωτικές διευθύνσεις και επικοινωνούν ελεύθερα πάνω από τα δημόσια IP δίκτυα.

• Υποστήριξη κλάσεων υπηρεσιών (Class of Service –CoS- support): Η CoS είναι σημαντική απαίτηση για πολλούς πελάτες των VPN. Παρέχει την δυνατότητα να ικανοποιηθούν δύο βασικές παράμετροι των VPN
• Πρόβλεψη απόδοσης και πολιτική υλοποίησης
• Υποστήριξη πολλαπλών επιπέδων υπηρεσιών στα MPLS VPNs

• Άμεση εξάπλωση (Straightforward migration): Οι παροχείς υπηρεσιών για να αναπτύξουν γρήγορα τις υπηρεσίες ενός VPN χρησιμοποιούν ένα ευθύ και άμεσο μονοπάτι εξάπλωσης.

Τα MPLS είναι μοναδικά επειδή μπορούν να χτιστούν πάνω σε πολλές και διαφορετικές αρχιτεκτονικές δικτύων όπως IP, Frame Relay, ATM κλπ. Η εξάπλωση μέχρι τον τελικό χρήστη είναι απλή γιατί δεν είναι απαραίτητο να γίνει κάποια αλλαγή ούτε στον δρομολογητή CE του πελάτη, ούτε στο intranet που δουλεύει ώστε να υποστηρίξουν το MPLS

6.7 Αρχιτεκτονική των MPLS/VPN Δικτύων

Η υλοποίηση MPLS VPNs σήμερα έχει βρει λύση στην συνεργασία δύο γνωστών τεχνολογιών MPLS και BGP όπου το MPLS χρησιμοποιείται για την προώθηση των πακέτων στο δίκτυο και το BGP για την διανομή των διαδρομών (κατ' επέκταση των ετικετών).

Γενικά για να γίνει αυτό εφικτό απαιτούνται
• Ελεγχόμενη διανομή των πληροφοριών δρομολόγησης (Constrained distribution)
• Πολλαπλοί πίνακες προώθησης
• Νέοι τύποι διευθύνσεων, οι VPN-IP
• Οι μηχανισμοί προώθησης του MPLS

Μία σχετική ορολογία που χρησιμοποιείται της τεχνολογίας MPLS VPNs

• Customer Edge device (CE). Πρόκειται για την ακραία συσκευή ενός πελάτη που ανήκει σε ένα VPN και συνδέεται σε μία η περισσότερες συσκευές του παρόχου. Θεωρητικά μπορεί να είναι ένας μεμονωμένος εξυπηρετητής, ένας μεταγωγέας ή στη συνηθέστερη και μια πρακτική μορφή ένας δρομολογητής.
• Provider Edge device (PE). Είναι ο ακραίος δρομολογητής του δικτύου του παρόχου στον οποίο συνδέονται οι CE δρομολογητές.
• Provider device (P). Κάθε ενδιάμεσος δρομολογητής του δικτύου του παρόχου.
Είναι σημαντικό να τονιστεί ότι το μοντέλο MPLS VPNs δεν ταυτίζεται με κάποιο είδος "overlay" στο δίκτυο του παρόχου, συνεπώς δεν υπάρχει κάποια ένοια ιδεατού δικτύου κορμού για τον πελάτη. Κάθε CE δρομολογητής ενός πελάτη έχει μία ομότιμη σχέση διασύνδεσης με τον PE δρομολογητή του παρόχου και όχι με κάποιον άλλον CE δρομολογητή του σε ένα άλλον σημείο παρουσίας, ουσιαστικά δεν γνωρίζει όσο αφορά την δρομολόγηση, την ύπαρξη άλλων CE δρομολογητών

6.7.1 Ελεγχόμενη διανομή των πληροφοριών δρομολόγησης

Με έλεγχο του τρόπου διανομής των πληροφοριών δρομολόγησης (πίνακες δρομολόγησης) ελέγχουμε ουσιαστικά την ροή των δεδομένων στο δίκτυο.

1. Η διανομή των πληροφοριών δρομολόγησης γίνεται ως ακολούθως: Η πληροφορία διαδίδεται από τον CE δρομολογητή στον PE δρομολογητή με τον οποίο είναι συνδεδεμένος. Αυτό μπορεί να γίνει με RIP, OSPF, static routes, BGP.

2. Από τον εισερχόμενο PE η πληροφορία αναδιανέμεται στο BGP του παρόχου.

3. Η πληροφορία δρομολόγησης διανέμεται ανάμεσα στους υπόλοιπους PE δρομολογητές του δικτύου.

4. Στους εξερχόμενους PE δρομολογητές η πληροφορία δρομολόγησης εισάγεται από το BGP του παρόχου.

5. Η πληροφορία δρομολόγησης αποστέλλεται από τον PE δρομολογητή εξόδου στον CE δρομολογητή. Αυτό μπορεί να γίνει με RIP, OSPF, static routes, BGP.

Η ελεγχόμενη διανομή των πληροφοριών δρομολόγησης γίνεται με χρήση της τεχνικής φιλτραρίσματος με βάση την ιδιότητα / χαρακτηριστικό Community του BGP. Στο βήμα 2 της παραπάνω διαδικασίας ο PE δρομολογητής εισάγει μία

κατάλληλη τιμή στο πεδίο Community πριν εξάγει τις πληροφορίες δρομολόγησης στο BGP. Στο βήμα 4 ο PE δρομολογητής εξόδου χρησιμοποιώντας τη τιμή του BGP Community ελέγχει την διανομή των πληροφοριών δρομολόγησης στον CE δρομολογητή. Σημειώστε ότι η λειτουργία αυτή ελέγχεται αποκλειστικά από τον πάροχο και ο πελάτης δεν χρειάζεται να γνωρίζει κάτι η να εμπλακεί με κάποια σχετική ενέργεια.
Όσο αφορά τα μεγέθη, επειδή το πεδίο BGP Community έχει μέγεθος 32 bits εκ των οποίων ένα τμήμα των 16 bits κρατά το Autonomous System Number, επιτρέπει 216 διαφορετικές communities ή αλλιώς το πολύ 216 VPN πελάτες. Για ένα παγκόσμιο πάροχο αυτό μάλλον είναι περιοριστικό οπότε έχει εισαχθεί η έννοια των Extended Communities όπου τα 16 bits του AS Number χρησιμοποιούνται για την διάκριση 232 communities αφού στα ιδιωτικά VPNs τα AS Numbers έχουν εντελώς τοπική σημασία.

6.7.2 Πολλαπλοί πίνακες προώθησης

Επειδή ένας PE δρομολογητής θα έχει συνήθως πολλά διαφορετικά VPNs η διατήρηση ενός κοινού πίνακα δρομολόγησης για όλα τα ιδιωτικά δίκτυα αποτρέπει τον διαχωρισμό της πληροφορίας δρομολόγησης με αποτέλεσμα να είναι πιθανή η προώθηση πακέτων μεταξύ διαφορετικών VPNs.
Το πρόβλημα αυτό αντιμετωπίζεται με την υποστήριξη πολλαπλών πινάκων δρομολόγησης σε κάθε PE δρομολογητή. Ειδικότερα συντηρείται ένας πίνακας δρομολόγησης για κάθε ένα VPN.

6.7.3 Διευθύνσεις VPN-IP

Το πρωτόκολλο δρομολόγησης BGP, όπως και τα υπόλοιπα, προϋποθέτουν για να λειτουργήσουν, χρήση μοναδικών IP διευθύνσεων. Αντίθετα στα MPLS VPNs μπορούν να συνυπάρχουν τόσο επικαλύψεις διευθύνσεων μεταξύ διαφορετικών VPNs όσο και χρήση των ιδιωτικών διευθύνσεων (π.χ. διευθύνσεις 10.0.0.0). Το πρόβλημα αντιμετωπίζεται με τη δημιουργία ενός νέου τύπου διευθύνσεων, των IP-VPNS.

Μία IP-VPN διεύθυνση κατασκευάζεται με την παράθεση ενός πεδίου με σταθερό μήκος, Route Distinguisher, και μιας συνηθισμένης IP διεύθυνσης. Το πεδίο Route Distinguisher παράγεται μοναδικά από το VPN πάροχο, ακόμα και για VPNs που κατανέμονται μεταξύ διαφορετικών παρόχων, και περιλαμβάνει

τρία πεδία: Type (2 octets), Autonomous System Number (4 octets), Assigned Number (4 octets).

Το πεδίο Autonomous System Number περιέχει τον AS Number του παρόχου του VPN και το Assigned Number ένα μοναδικό αριθμό για αυτό το VPN που εκχωρείται από τον πάροχο.

Συνεπώς ο Route Distinguisher είναι όχι μόνο τοπικά μοναδικός, στα πλαίσια του παρόχου, αλλά και καθολικά. Κατά συνέπεια οι IP-VPN διευθύνσεις είναι καθολικά μοναδικές, αφού φέρουν μοναδικό Route Distinguisher έστω και αν χρησιμοποιούν κοινές ή ιδιωτικές απλές IP διευθύνσεις.

Η διαχείριση των διευθύνσεων αυτών από το BGP είναι εφικτή λόγω τις ικανότητας του multiprotocol BGP να χειρίζεται δρομολογήσεις για multiple-address families. Η χρήση των διευθύνσεων αυτών, IP-VPNs, περιορίζεται αποκλειστικά στους PE δρομολογητές του παρόχου, ο πελάτης, CE δρομολογητής, είναι άσχετος με αυτό το μοντέλο.

Σημειώστε ότι οι IP-VPNs διευθύνσεις χρησιμοποιούνται και μεταφέρονται μόνο από τα πρωτόκολλα δρομολόγησης (εδώ το BGP) και όχι στο header του πακέτου IP.

6.8 Οι μηχανισμοί προώθησης του MPLS-VPN

Το καθοριστικό πλεονέκτημα του MPLS, στην προκειμένη περίπτωση, είναι ο διαχωρισμός της πληροφορίας προώθησης (ετικέτα) από τη περιεχόμενο του header (IP διεύθυνση) του IP πακέτου που εφαρμόζει.

Για την υποστήριξη των IP-VPN διευθύνσεων από το MPLS χρησιμοποιείται πολύ έξυπνα η τεχνική του label stack. Πρόκειται για στοίβα δύο επιπέδων (δηλαδή κάθε πακέτο φέρει δύο ετικέτες) όπου:

• η ετικέτα στην κορυφή της στοίβας (δεύτερο επίπεδο) συσχετίζεται με τους PE δρομολογητές εισόδου / εξόδου και υλοποιεί έτσι το μηχανισμό προώθησης από ένα PE δρομολογητή εισόδου σε ένα PE δρομολογητή εισόδου. Η διανομή των ετικετών αυτού του επιπέδου μπορεί να γίνει είτε με LDP είτε με CR-LDP ή RSVP αν απαιτείται Traffic Engineering.

• η ετικέτα του πρώτου επιπέδου ελέγχει την προώθηση στο PE δρομολογητή ειξόδου. Οι ετικέτες αυτού του επιπέδου διανέμονται αποκλειστικά μέσω του BGP μαζί με τις IP-VPN διευθύνσεις.

Είναι πολύ σημαντικό μα τονιστεί ότι όταν μία IP-VPN διεύθυνση (ουσιαστικά διεύθυνση πελάτη) διανέμεται μέσω του BGP μεταφέρει ως τιμή next-hop τη διεύθυνση του PE που τη δημιούργησε (και όχι τη διεύθυνση του CE όπως κανείς θα μπορούσε να φανταστεί). Αυτή η next-hop διεύθυνση του PE είναι

προφανώς μία συνηθισμένη IP διεύθυνση του δικτύου του παρόχου και δρομολογείται σύμφωνα με τις συνήθεις διαδικασίες δρομολόγησης (π.χ. OSPF).

6.9 Πλεονεκτήματα χρήσης των MPLS VPNs

Γενικά τα IP VPNs είναι μία ελκυστική λύση γιατί:
1. μειώνουν το κόστος σύνδεσης των γραφείων μιας εταιρίας η οργανισμού, των τηλεπικοινωνιακών συσκευών και των κινητών χρηστών μέσα σε ένα intranet που λειτουργεί πάνω από μια δημόσια υποδομή του internet

2. είναι πιο οικονομικά από τα δημόσια δίκτυα που χρησιμοποιούν μισθωμένες γραμμές Επίσης τα συνηθισμένα είδη VPN δικτύων, αναβαθμίζονται πολύ δύσκολα. Αυτό συμβαίνει διότι βασίζονται σε πλήρεις τοπολογίες από κρυπτογραφικά tunnels ή από μόνιμα εικονικά κυκλώματα γεγονός που καθιστά την προσθήκη νέων πελατών εξαιρετικά δύσκολη. Τέτοιου είδους VPN είναι τα εξής:
• IPSec
• Layer 2 tunneling protocol (L2TP)
• Layer 2 forwarding protocol (L2F)
• Generic routing encapsulation (GRE)
• Frame relay
• ATM protocols

Η επιπλέον πληροφορία (overhead) που πρέπει να προστίθεται ώστε να εξασφαλιστούν οι προσανατολισμένες στην σύνδεση υπηρεσίες των παραπάνω VPN, δημιουργεί ανυπέρβλητα προβλήματα σε έναν παροχέα που πρέπει να υποστηρίζει εκατοντάδες ή και χιλιάδες VPNs, καθένα από τα οποία μπορεί να έχει εκατοντάδες ή και χιλιάδες sites και χιλιάδες η δεκάδες χιλιάδες δρομολόγια. Τα MPLS VPNs τα οποία είναι πρωτόκολλα επιπέδου 3, μη προσανατολισμένα στην σύνδεση (ασυνδεσμικά) είναι ουσιαστικά περισσότερο αναβαθμίσιμα και πιο εύκολο να δημιουργηθούν και να διαχειριστούν, από ότι τα συμβατικά VPN. Επιπλέον κάθε MPLS VPN μπορεί να παρέχει προστιθέμενης αξίας υπηρεσίες όπως φύλαξη δεδομένων και εφαρμογών, δίκτυα επιχειρήσεων και τηλεφωνικές υπηρεσίες.

Συνοψίζοντας τα MPLS VPNs προσφέρουν:

• Μια πλατφόρμα για την ταχύτατη ανάπτυξη προστιθέμενης αξίας IP υπηρεσιών όπως intranets, extranets, φωνή, πολυμέσα και δικτυακές επιχειρήσεις.

• **Ιδιωτικότητα και ασφάλεια** αντίστοιχη των Layer-2 VPNs περιορίζοντας τις VPN διαδρομές μόνο ανάμεσα σε εκείνους τους δρομολογητές που είναι μέλη του VPN.

Ασφάλεια. Τα VPNs που δημιουργούνται με την τεχνολογία MPLS παρέχουν αυξημένη προστασία των εταιρικών δεδομένων από τον κίνδυνο της υποκλοπής καθώς η κίνηση ανάμεσα στα σημεία που ανήκουν στο VPN είναι παντελώς απομονωμένη από την κίνηση άλλων VPNs. Για να επιτύχει τον στόχο της απομόνωσης, το πρότυπο MPLS προβλέπει ότι κάθε MPLS VPN έχει δικό του πίνακα δρομολόγησης (routing table) καθώς και πόρτες που έχουν καθορισθεί άμεσα ότι ανήκουν σε αυτό. Συνεπώς δεν είναι εφικτή η επικοινωνία ανάμεσα σε δύο MPLS VPNs χωρίς την άμεση παρέμβαση του παρόχου. Μελέτη του IETF (Internet Engineering Task Force), του φορέα που είναι υπεύθυνος για την διαχείριση του συνόλου των προτύπων που αφορούν στο Internet (RFCs), αναφέρει ότι η τεχνολογία MPLS προσφέρει το ίδιο επίπεδο ασφάλειας στα εταιρικά δίκτυα, με εκείνη που προσφέρεται από παραδοσιακές τεχνολογίες όπως Frame Relay και ATM

• **Ευελιξία.** Οι υπηρεσίες MPLS IP-VPN δίνουν τη δυνατότητα δημιουργίας κλειστών ιδιωτικών δικτύων των οποίων τα μέλη μπορεί να συνδέονται μεταξύ τους με οποιαδήποτε λογική τοπολογία είναι επιθυμητή. Με αυτόν τον τρόπο διευκολύνεται η εξυπηρέτηση διαφορετικών επιχειρησιακών διαδικασιών πάνω από το ίδιο δίκτυο, π.χ. η εξυπηρέτηση της φωνητικής επικοινωνίας των σημείων παρουσίας μίας εταιρείας απαιτεί άμεση διασυνδεσιμότητα ενός σημείου με οποιοδήποτε άλλο σημείο της τράπεζας (full mesh λογική τοπολογία). Κάτι τέτοιο δεν είναι επιθυμητό για το δίκτυο δεδομένων της τράπεζας το οποίο μπορεί να επιλέξει τοπολογία αστέρα ή partial mesh. Με τη χρήση MPLS VPN και οι δύο λύσεις μπορούν να συνυπάρξουν πάνω από ένα ενιαίο δίκτυο. Η ευελιξία του MPLS VPN θα δώσει την δυνατότητα ενσωμάτωσης των μελλοντικών απαιτήσεων που μπορεί να προκύψουν από το δυναμικό εξελισσόμενο επιχειρησιακό περιβάλλον, σε μικρό χρόνο και με ελεγχόμενο κόστος.

• Ενσωμάτωση των intranets των πελατών, χωρίς καμία περικοπή.

• Αυξημένη δυνατότητα αναβάθμισης έτσι ώστε, να μπορούν να φιλοξενηθούν χιλιάδες sites ανά VPN και δεκάδες ή και χιλιάδες VPN ανά παροχέα.

• Ευέλικτο σχήμα διευθυνσιοδότησης. Με τη χρήση των υπηρεσιών MPLS IP-VPN παρέχεται η δυνατότητα διατήρησης του σχήματος διευθυνσιοδότησης το οποίο έχει υιοθετήσει εσωτερικά μειώνοντας με αυτόν τον τρόπο σημαντικά το κόστος υιοθέτησης της νέας τεχνολογίας.

• IP - Class of Service (CoS), υποστήριξη πολλών κλάσεων υπηρεσιών και προτεραιοτήτων εντός του VPN ή ανάμεσα στα VPNs. Δίνουν τη δυνατότητα δημιουργίας πολιτικής επιπέδου υπηρεσιών από άκρο σε άκρο, διασφαλίζοντας με αυτόν τον τρόπο ότι τα ευαίσθητα επιχειρησιακά δεδομένα πχ μιας τράπεζας θα τυγχάνουν προνομιακής μεταχείρισης σε όλα τα στάδια της μετάβασής τους από το δίκτυο του παρόχου.

• Εύκολη διαχείριση των μελών ενός VPN.

• Κλιμακωτή διασύνδεση εξωτερικών intranets και extranets που περικλείουν πολλές επιχειρήσεις.

Βιβλιογραφία

1. MPLS: Conformance and Performance Testing — IXIA (www.ixiacom.com)
2. MPLS — The International Engineering Consortium (www.iec.org)
3. MPLS — Ennovate Networks, Inc. (www.techguide.com)
4. MPLS Traffic Engineering — Cisco (www.cisco.com)
5. Traffic Engineering Solutions for Core Networks — Alcatel (www.alcatel.com)
6. An MPLS-based Quality of Service Architecture for Heterogeneous Networks (Master Thesis) — Srihari Raghavan (Virginia State University)
7. Cisco MPLS Controller Software Configuration Guide — Cisco Systems, Inc (www.cisco.com)
8. Advanced MPLS VPN Solutions (AMVS)-volume1 — Cisco Systems, Inc (www.cisco.com)
9. Advanced MPLS Design and Implementation — Cisco Systems, Inc (www.cisco.com)
10. Cisco Press CCIP MPLS and VPN Architectures — Cisco Systems, Inc (www.cisco.com)